Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

メモ: メモは、デバイスをより有用に使うための重要な情報を説明しています。

注意: ハードウェアの損傷またはデータの損失の可能性を示唆し、問題を回避する方法を説明しています。

警告: **警告は、物的損害、けが、または死亡の原因となる可能性があることを示します。**

2003 年 11 月 Rev. A01

メモ、注意および警告

PowerConnect 3324/3348 スイッチの設定

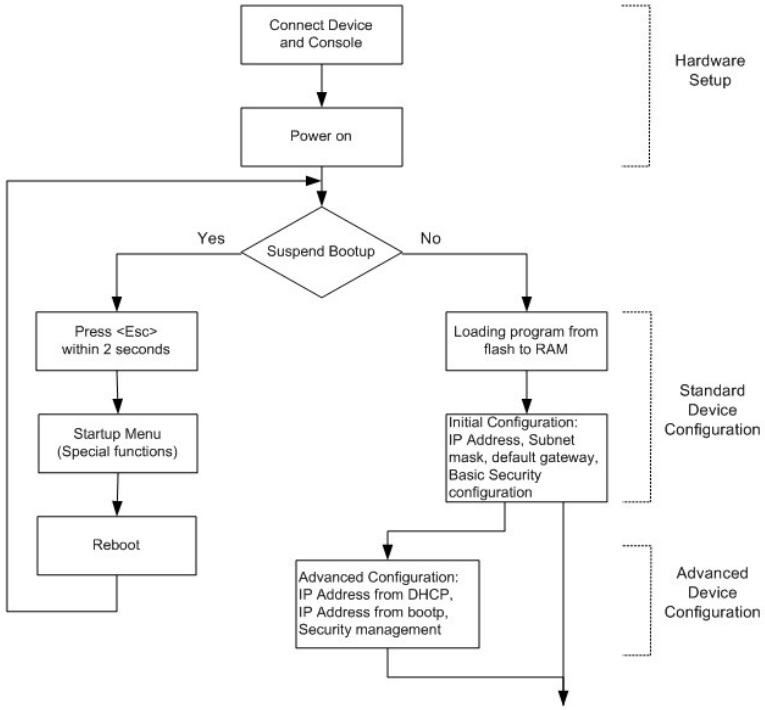
Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

設定の概要

この項では、以下の項目を含むデバイスの初期設定について説明します。

- デバイスの初期起動
- 設定作業前要件
- スタッキングの設定

すべてのデバイス外部接続が完了した後、起動およびその他の手続きを監視するために、コンピュータターミナルをデバイスに接続する必要があります。インストールと設定の手順を次のフローチャートに示します。



デバイスとハードウェアのセットアップについては、前の項で説明しています。初めてインストールする場合は、標準デバイスインストールが実行されます。これ以外の特別な機能を実行することもできますが、そうするとインストールプロセスが中断され、システムが再起動します。このオプションについては、本項で後ほど説明します。

全般設定情報

Dell™ PowerConnect™ 3324/3348 には、定義済みの実装機能とセットアップ設定が用意されています。

自動ネゴシエーション

自動ネゴシエーションにより、デバイスが動作モードを通知できるようになり、同じポイントツーポイントリンクセグメントを使用するデバイスと情報を共有できます。これにより、両方のデバイスがそれぞれの能力を最大限に活用できるよう自動的に設定されます。

自動ネゴシエーションは、リンク初期化時に完全に物理レイヤ内で実行され、MAC や上位プロトコルレイヤに余分なオーバーヘッドをかけません。自動ネゴシエーションにより、ポートで以下のことを実行できます。

- それぞれの能力を通知する。
- 両方のデバイスが共有する共通動作モードの受信を確認し理解する。
- 両方のデバイスで共有していない動作モードの使用を拒否する。
- 両方のポートがサポートできる上位動作モード用に各ポートを設定する。

スイッチのポートを、自動ネゴシエーションをサポートしていない、または自動ネゴシエーションが設定されていない、ワークステーションまたはサーバーのネットワークインタフェースコントローラ (NIC) に接続する場合は、ウェブブラウザインタフェースまたは CLI コマンドを使用し、スイッチングポートと NIC の両方を、同じ速度および二重モードに手動で設定する必要があります。

注意： リンクの片方の端のステーションが手動で全二重モードに設定されているポートと自動ネゴシエーションを試みる場合、そのステーションの自動ネゴシエーションは半二重モードになります。この不一致は大きなフレームロスにつながる場合があります。これは自動ネゴシエーション標準に固有のものです。

スイッチングポートのデフォルト設定

以下の表に、ポートのデフォルト設定を示します。

ポートのデフォルト設定

機能	デフォルト設定
ポートの速度およびモード	10/100M 銅製ポート 自動ネゴシエーション 1000M 自動ネゴシエーション
ポートの転送状態	有効
ポートのタグ付け	No tagging （タグなし）
Head of line ブロック保護	On （有効）
Flow Control	消灯
Back Pressure	消灯

以下に、CLI コマンドを使用してポート 1/e5 のポート速度を変更する例を示します。

```
console> enable

console# configure

Console (config)# interface ethernet 1/e5

Console (config-if)# speed 9600
```

以下に、CLI コマンドを使用してポート 1/e5 のフロー制御を有効にする例を示します。

```
console> enable

console# configure

Console (config)# interface ethernet 1/e5

Console (config-if)# flowcontrol on
```

以下に、CLI コマンドを使用してポート 1/e5 の Back Pressure を有効にする例を示します。

```
console> enable
```

```
console# configure

Console (config)# interface ethernet 1/e5

Console (config-if)# back-pressure
```

[ボーレート]

ボーレートは、手動で以下の値のいずれかに変更できます。

- 2400
- 4800
- 9600
- 19,200
- 38,400
- 57,600
- 115,200

メモ: デフォルトのボーレートは 9600 です。

メモ: デバイスを閉じても、デフォルトのボーレートは返されません。明示的に設定する必要があります。

メモ: 設定モードに入るには、管理レベル 15 特権を指定する必要があります。

以下に、CLI コマンドを使用してデフォルトのボーレートを変更する例を示します。

```
console> enable

console# configure

console(config)# line console

console(config-line)# speed 9600

console(config-if)# exit

console(config)# exit
```

ターミナル接続の設定

PowerConnect 3324/3348 の設定では、以下のターミナル接続パラメータが必要です。

- パリティなし
- 1 ストップビット
- 8 データビット

その他の設定要件

組み込みソフトウェアをダウンロードしてデバイスを設定するには、以下のものが必要です。

- ユニットの背面パネルのシリアルポートに接続されている ASCII ターミナル（またはエミュレーション）
- Telnet、SSH などを使用してデバイスをリモートコントロールするための、PowerConnect 3324/3348 の割り当て IP アドレス

メモ: 設定手順は、1 つのポートのみを定義します。

デバイスの起動

ローカルターミナルが接続された状態で電源をオンにすると、デバイスに対して POST (Power On Self Test) が実行されます。この内蔵電源テストは、デバイスが初期化されるたびに実行されます。POST は、起動が完了する前にハードウェアコンポーネントを調べて、デバイスが完全に動作可能な状態になっているかを確認します。

重大な問題が検出されると、プログラムのフローが停止します。POST が正常に完了すると、コードが RAM メモリに圧縮されます。

POST メッセージがコンピュータターミナルに表示され、テストの成否を示します。

デバイスを起動するには、次の手順を実行します。

1. ASCII ケーブルがコンピュータターミナルに接続されているか確認します。
2. デバイスに電源を接続すると、デバイスの起動プロセスが開始されます。起動テストは、まず利用可能なデバイスメモリを計算し、起動を続けます。以下に、POST テストの画面表示例を示します。

```
------ Performing the Power-On Self Test (POST) ------


UART Channel Loopback Test......PASS

Testing the System Cache.......PASS

Testing the System SDRAM.......PASS
```

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

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

Flash Image Validation Test......PASS

Testing CPU PCI Bus Device Configuration...PASS



BOOT Software Version 1.30.11 Built 27-JAN-2003 10:06:03

Processor:MPC8245 Rev 0.12, 250 MHz (Bus:100MHz), 32 MByte SDRAM.

I-Cache 16 KB, linesize 32.D-Cache 16 KB, linesize 32.

Cache Enabled.

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

POST の最後に表示される自動起動メッセージ (最後の行) は、起動中に問題が発生しなかったことを示します。

このときユーザー入力を行って Startup メニューを表示し、メニュー内の特定の機能を実行することができます。Startup メニューに入るには、自動起動メッセージが表示されてから 2 秒以内に **<Esc>** または **<Enter>** キーを押してください。Startup メニューに関する詳細については、Startup （スタートアップ） メニューの機能 を参照してください。

ユーザー入力が行われない場合は、コードを RAM に圧縮して動作を続行します。RAM からのコードの実行が開始され、使用可能なポート番号の一覧とそれぞれの状態 (動作中または停止中) が表示されます。

メモ: 以下の画面は設定の例です。アドレス、バージョン、および日付は各デバイスで異なることがあります。

```
Preparing to decompress.

Decompressing SW from RSCOD_2

85e000

OK

Running from RAM.
```

**Running SW Ver.3.30 Date 03-Feb-2003 Time 10:10:37
****

HW version is X.X

Base Mac address is: 00:01:02:03:04:05

Dram size is:32M bytes

Dram first block size is:20M bytes

Dram first PTR is:0xB70000

Flash size is:8M

STAND ALONE

The BCM5625_A1 0 initiate successfully

The BCM5625_A1 1 initiate successfully

02-Jan-2000 01:01:11%SSHD-W-NOHOSTKEY:SSHG_init:The SSH daemon cannot listen

for incoming connections, because a host key has not been generated.

The service will start automatically when a host key is generated.

01-Jan-2000 01:01:11 %INIT-I-InitCompleted:Initialization task is completed

console> 01-Jan-2000 01:01:12 %PS-I-PSUP:Power Supply #1 is up

01-Jan-2000 01:01:12%PS-W-PSDOWN:Power Supply #2 is down

01-Jan-2000 1:01:12%LINK-W-Up:1/e1

01-Jan-2000 01:01:12%LINK-W-UP:1/e2

```
01-Jan-2000 1:01:12%LINK-W-Up:1/e3

01-Jan-2000 01:01:12%LINK-W-UP:1/e4

01-Jan-2000 1:01:12%LINK-W-Up:1/e5

01-Jan-2000 01:01:13%LINK-W-Up:1/e9
```

デバイスの起動が成功した後、システムプロンプト (console>) が表示され、設定プロセスを開始できます。設定はローカルターミナルで実行できます。

デバイス設定について

設定には、2 つのタイプまたはレベルがあります。初期設定は、基本的なセキュリティ要件を考慮した基本的な設定機能です。拡張設定には動的 IP 設定が含まれ、より高度なセキュリティ要件を考慮しています。

注意： 設定を変更した後、再起動する前に新しい設定を保存する必要があります。
設定を保存するには、以下のコマンドを入力します。

```
console> enable

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

初期設定

初期設定は、デバイスが正常に起動した後開始します。初期設定は、以下のデバイスを対象としています。

- 静的 IP アドレスとサブネットマスク
- デフォルトゲートウェイ
- リモート管理を行う場合は、ユーザー名と特権レベルを設定する必要があります。

SNMP ベースの管理ステーションからデバイスを管理する場合は、SNMP コミュニティストリングも設定する必要があります。

静的 IP アドレスとサブネットマスク

PowerConnect 3324/3348 デバイスでは、各ポートで IP インタフェースを設定でき、その数に制限はありません。設定コマンドを入力した後、"show ip interface" コマンドを入力して、ポートに IP アドレスが設定されていることを確認してください。

注意： IP アドレスを割り当てることのできる VLAN は 1 つだけです。別の VLAN にアドレスを割り当てた場合は、新しいアドレスが元の IP アドレスを上書きします。

VLAN 上にインタフェースを設定するには、以下の例のようにシステムプロンプトでコマンドを入力します。

```
console> enable

console# configure

console(config)# interface vlan 1

console(config-if)# ip address 100.1.1.1 /8

console(config-if)# exit

console(config)# exit

console# show ip interface


Gateway IP Address Activity status

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


IP Address I/F

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

100.1.1.1/8 vlan 1


console#
```

ポート上にインタフェースを設定するには、以下の例のようにシステムプロンプトでコマンドを入力します。

```
console> enable

console# configure
```

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

console(config-if)# ip address 10.1.1.1 255.0.0.0

console(config-if)# exit

console(config)# exit

console# show ip interface


Gateway IP Address Activity status

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


IP Address I/F

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

10.1.1.1/8 1/e1


console#
```

デフォルトゲートウェイ

リモートネットワークから PowerConnect 3324/3348 デバイスを管理する場合は、デフォルトゲートウェイ (特定のゲートウェイが指定されない場合にデバイスが使用するゲートウェイ) を設定する必要があります。設定されるゲートウェイ IP アドレスは、デバイス IP インタフェースのうちの 1 つと同じサブネットに属する必要があります。

デフォルトゲートウェイを設定するには、例のようにシステムプロンプトでコマンドを入力します。

```
console> enable

console# configure
```

```
console(config)# ip default-gateway 100.1.1.100

console(config)# exit
```

ユーザー名、パスワード、特権レベル

重要:リモートターミナルまたはウェブ管理インタフェースからデバイスを管理する場合は、ユーザー名、パスワード、および最高の権限レベル (15) を入力する必要があります。(最高レベルでは、CLI 設定コンテキストにアクセスできます。) 特権レベルの詳細については、「CLI リファレンスガイド」を参照してください。

設定したユーザー名は、リモート管理セッションのログイン名として入力します。ユーザー名と特権レベルを設定するには、以下の例のようにシステムプロンプトでコマンドを入力します。

```
console> enable

console# configure

console(config)# username admin password admin level 15

console(config)# exit
```

SNMP コミュニティストリング

SNMP（Simple Network Management Protocol）はネットワークデバイスの管理メソッドを提供します。SNMP 対応デバイスは、ローカルソフトウェア（エージェント） を実行します。SNMP エージェントは、デバイスの管理に使用される変数の一覧を保持します。変数は MIB（Management Information Base）で定義されます。MIB はエージェントによって管理される変数を表示します。SNMP エージェントは、MIB 指定フォーマットおよびネットワーク全体にわたる情報にアクセスするためのフォーマットを定義します。SNMP エージェントへのアクセス権は、アクセスストリングおよび SNMP コミュニティストリングによって制御されます。

デバイスは SNMP 準拠です。デバイスには、標準および専用 MIB 変数のセットをサポートする SNMP エージェントが含まれています。管理ステーションの開発者は、MIB ツリーの完全な構造を必要とし、MIB を管理するために完全な専用 MIB 情報を受け取ります。

SNMP 管理ステーションの IP アドレスおよびコミュニティ (コミュニティ名とアクセス権) を除き、どの SNMP 管理プラットフォームからもすべてのパラメータを管理できます。コミュニティストリングが存在しない場合、SNMP 管理によるデバイスへのアクセスは無効になります。デバイスは、コミュニティストリングが設定されていない状態で提供されます。

以下に、デフォルトデバイス設定の画面表示例を示します。

```
console# enable

console# show snmp
```

```
Community-String Community-Access IP address

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

Traps are enabled.

Authentication-failure trap is enabled.
```

コミュニティストリング、コミュニティアクセス、および IP アドレスは初期設定時にローカルターミナルを使用して設定できます。

SNMP 設定オプションは次のとおりです。

- コミュニティストリング
- アクセス権オプション: ro (読み取り専用)、rw (読み書き)、または su (super)。
- IP アドレスを設定するかどうか: IP アドレスを設定しない場合は、同じコミュニティ名を持つすべてのコミュニティメンバに同じアクセス権が与えられます。

通常は、デバイスに 2 つのコミュニティストリングを使用します。ひとつ
(public コミュニティ) は読み取り専用アクセス、もうひとつ (private コミュニティ)
は読み書きアクセスです。

- Public このストリングを使用すると、認証を受けた管理ステーションは MIB オブジェクトを検出できます。
- Private このストリングを使用すると、認証を受けた管理ステーションは MIB オブジェクトを検出し、変更できます。

初期設定時に、SNMP ベースの管理ステーションの使用について、ネットワーク管理要件に基いてデバイスを設定することをお勧めします。

SNMP ステーション IP アドレスおよびコミュニティストリングを設定するには、次の手順を実行します。

1. コンソールプロンプトで、**Enable** と入力します。プロンプト（#）が表示されます。
2. **configure**と入力して、<Enter>を押します。
3. 以下の例のように、設定モードで、コミュニティ名 (private)、コミュニティアクセス権 (読み書き)、および IP アドレスを含むパラメータを使用して、SNMP 設定コマンドを入力します。

```
console> enable

config# configure

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

config(config)# exit

config# show snmp
```

```
Community-String Community-Access IP address

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

private readWrite 11.1.1.2

Traps are enabled.

Authentication-failure trap is enabled.

Trap-Rec-Address Trap-Rec-Community Version

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

System Contact:

System Location:
```

これにより、ローカルターミナルからの初期設定が完了します。設定したパラメータによって、離れた場所からデバイス設定を実行できます。

詳細設定

この章では、IP アドレスの動的割り当ておよび AAA (Authentication, Authorization and Accounting: 認証、承認、アカウント) に基くセキュリティ管理機構について説明します。この章には以下のトピックがあります。

- DHCP を利用した IP アドレスの設定。
- BOOTP を利用した IP アドレスの設定。
- セキュリティ管理とパスワード設定。

DHCP および BOOTP を使用して IP アドレスを設定または取得する場合、これらのサーバーから取得する設定には、IP アドレスのほかに、サブネットマスクとデフォルトゲートウェイが含まれる場合があります。

DHCP サーバーからの IP アドレスの取得

DHCP プロトコルを使用して IP アドレスを取得する場合、デバイスは DHCP クライアントとして動作します。

DHCP サーバーから IP アドレスを取得するには、次の手順を実行します。

1. IP アドレスを取得するため、いずれかのポートを選択し、DHCP サーバー、または DHCP サーバーを有するサブネットに接続します。
2. 選択したポートを使用して IP アドレスを取得するには、例に示すようにコマンドを入力します。

```
console> enable

console# configure

console(config)# interface vlan 1

console(config-if)# ip address dhcp hostname <string>

console(config-if)# exit

console(config)# exit
```

3. デバイスは IP アドレスを自動的に取得します。

IP アドレスを確認するには、次の手順を実行します。

1. システムプロンプトで **show ip interface** と入力します。以下の例を参照してください。

```
console> enable

console# show ip interface


Gateway IP Address Activity status

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


IP Address I/F

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

10.1.1.1/8 vlan1


console#
```

メモ: DHCP サーバーの IP アドレスを取得するためにデバイス設定を削除する必要はありません。

BOOTP サーバーからの IP アドレスの取得

デバイスが自身の IP ホスト設定をインターネット上のあらゆる標準的な BOOTP サーバーから自動的にダウンロードできるよう、標準的な BOOTP プロトコルがサポートされています。この場合、デバイスは BOOTP クライアントとして動作します。

BOOTP サーバーから IP アドレスを取得するには、次の手順を実行します。

1. IP アドレスを取得するため、いずれかのポートを選択し、BOOTP サーバー、または BOOTP サーバーを有するサブネットに接続します。
2. Startup configuration をフラッシュから削除するため、システムプロンプトで delete startup configuration コマンドを入力します。デバイスは設定なしで再起動し、60 秒経過すると BOOTP リクエストの送信を開始します。
3. デバイスは IP アドレスを自動的に取得します。

メモ: "delete startup configuration" が開始された後、ASCII ターミナルまたはキーボードで入力を実行すると、設定プロセスが完了前に自動的に中断され、デバイスは BOOTP から IP アドレスを取得できません。

以下にプロセスの例を示します。

```
console> enable

console# delete startup-config
```

以下に、IP アドレス検証の例を示します。

```
console> enable

console# show ip interface


Gateway IP Address Activity status

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



IP Address I/F

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

10.1.1.1/8 vlan1
```

```
console#
```

これでデバイスに IP アドレスが設定されました。

BOOTP サーバーから IP アドレスを取得するには、デバイス設定を削除する必要があります。

セキュリティ管理とパスワード設定

システムセキュリティは、ユーザーアクセス権、特権、および管理方法を制御する AAA (認証、承認、アカウント) 機構によって処理されます。AAA はローカルおよびリモートのユーザーデータベースを使用します。データの暗号化は SSH 機構によって処理されます。

システムにはデフォルトのユーザー名やパスワードはあらかじめ設定されていません。すべてのユーザー名およびパスワードはユーザーが定義する必要があります。ユーザー定義パスワードが分からなくなった場合は、Startup メニューからパスワードのリカバリ手続きを実行できます。この手続きはローカルターミナルにのみ適用でき、パスワードを入力せずに 1 度だけローカルターミナルからデバイスにアクセスすることを許可します。

メモ: 自分のユーザー名とパスワードを入力する際は、常に管理レベル 15 特権を含めてください。

セキュリティパスワードの設定

セキュリティパスワードは、次のサービスに対して設定できます。

- Console
- Telnet
- SSH
- HTTP
- HTTPS

メモ: パスワードはユーザーが定義します。

メモ: ユーザー名を作成する際のデフォルトの優先度は 「1」 で、アクセスは許可されますが、設定権限はありません。デバイスへのアクセスと設定権限を有効にするには、優先度 「15」 を設定する必要があります。

パスワードの制限については、「ネットワークセキュリティの設定」を参照してください。

初期コンソールパスワードの設定

初期コンソールパスワードを設定するには、以下のコマンドを入力します。

```
console> enable
```

```
console# configure
```

```
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 console

console(config-line)# exit

console(config)# exit
```

- コンソールセッションを介してデバイスに初めてログオンする際は、パスワードプロンプトで console と入力します。
- デバイスのモードを enable に変更するには、パスワードプロンプトで console と入力します。

初期 Telnet パスワードの設定

初期 Telnet パスワードを設定するには、以下のコマンドを入力します。

```
console> enable

console# configure

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 admin
```

```
console(config-line)# exit

console(config)# exit
```

- Telnet セッションを介してデバイスに初めてログオンする際は、telnet と入力します。
- デバイスモードを enable に変更するには、admin と入力します。

初期 SSH パスワードの設定

初期 SSH パスワードを設定するには、以下のコマンドを入力します。

```
console> enable

console# configure

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 admin

console(config-line)# exit

console(config)# exit
```

- SSH セッションを介してデバイスに初めてログオンする際は、パスワードとして admin と入力します。
- デバイスモードを enable に変更するには、パスワードとして admin と入力します。

初期 HTTP パスワードの設定

初期 HTTP パスワードを設定するには、以下のコマンドを入力します。

```
console> enable

console# configure

console(config)# ip http authentication local

console(config)# username admin password admin level 15

console(config)# exit
```

初期 HTTPS パスワードの設定

初期 HTTPS パスワードを設定するには、以下のコマンドを入力します。

```
console> enable

console# configure

console(config)# ip https authentication local

console(config)# username admin password admin level 15

console(config)# exit
```

HTTPS セッションを使用するには、コンソール、Telnet、または SSH セッションを設定する際に、以下のコマンドを一回だけ入力します。

メモ: ページのコンテンツを表示するには、ウェブブラウザ内で SSL 2.0 以上を有効化します。

```
console> enable

console# configure

console(config)# crypto certificate generate key-generate

console(config)# ip https server

console(config)# exit
```

初めて HTTP または HTTPS セッションを有効にする際は、ユーザー名に admin、パスワードに user1 と入力します。

メモ: HTTP および HTTPS サービスではレベル 15 のアクセスが必要であり、設定レベルアクセスに直接接続します。

設定プロセス例

この章では、PowerConnect 3324/3348 デバイスとの間にリモートネットワーク管理接続を確立するための基本的な手順を紹介します。デバイスで使用できる各種の設定や関連コマンドについては説明しません。

この章では、出荷時の設定と定義の状態で、デバイスに最初にアクセスする方法を説明します。以前行った設定によって問題が発生している場合、起動設定ファイル (電源をオンにしたときのデバイスの設定) を消去して、デバイスを再起動する必要があります。デバイスのデフォルト設定 を参照してください。

デバイスのセットアップ要件

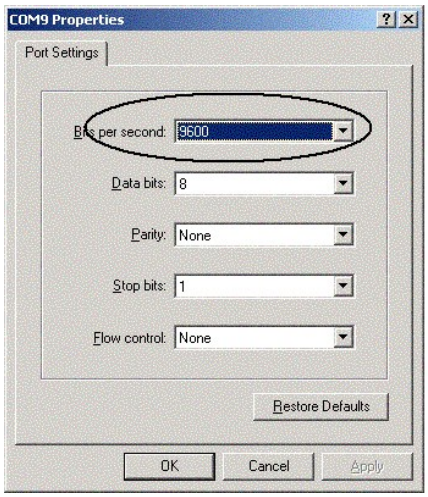
この例では、次のコンポーネントが必要となります。

- PowerConnect 3324/3348 デバイス
- 以下がインストールされた PC ワークステーション
  - NIC (ネットワークアダプタ) カード
  - ASCII ターミナルアプリケーション
    (® Windows® MS Hyper Terminal または Procomm Plus Terminal など)
  - ブラウザアプリケーション
- Null Modem F2F ケーブル 1 本
- ストレートまたはクロスの UTP (cat 5) ケーブル

最初の接続

最初に接続する際は、次の手順を実行します。

1. PowerConnect 3324/3348 デバイスを、ASCII ターミナルとして動作しているコンピュータの RS232 インタフェースに接続します。
2. ASCII ターミナルに以下の設定を行い、適切な COM ポートを選択します (この例では、 Windows Hyper Terminal アプリケーションを使用しています)。



メモ: 9600 は新しいデバイスのデフォルトボーレートです。9600 ボーレートを使用してもデバイスターミナルが表示されない場合は、ほかのボーレート設定を試してみてください (デバイスが異なるボーレートに設定されている可能性があります)。

3. F2F Null Modem ケーブルを使用して、ASCII ターミナルを実行している PC をデバイスに接続します。
4. デバイスの電源コードをコンセントに差し込み、デバイスの電源をオンにします。次の画面が表示されます。

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

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

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


Booting...


------ Performing the Power-On Self Test (POST( ------

UART Channel Loopback Test.....................PASS

Testing the System Cache.......................PASS

Testing the System SDRAM.......................PASS

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

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

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

Testing CPU PCI Bus Device Configuration.........PASS



BOOT Software Version 1.0.0.13 Built 11-May-2003 14:58:20

Processor:MPC8245 Rev 0.14, 250 MHz (Bus:100MHz), 32 MByte SDRAM.

I-Cache 16 KB, linesize 32.D-Cache 16 KB, linesize 32.

Cache Enabled.



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

Preparing to decompress...
```

イメージファイルが解凍されると、デバイス情報、SW/HW バージョン、既存のすべてのインタフェースのステータス (実行中/停止中) を示す以下のような画面が表示されます。

```
Decompressing SW from image-2

8cc000

OK

Running from RAM...



Update Host params for stand-alone



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

*** Running SW Ver.1.0.0.52 Date 29-Jun-2003 Time 19:04:06 ***
```

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



HW version is 00.00.01


Base Mac address is:00:06:5b:ff:59:4d


Dram size is:32M bytes


Dram first block size is:20M bytes


Dram first PTR is:0xB20000


Flash size is:8M



STAND ALONE


The BCM5615_A1 0 initiate successfully


01-Jan-2000 01:01:10 %SSHD-W-NOHOSTKEY:SSH has been enabled but an encryption key was not found.


For key generation use the 'crypto key generate' commands.The service will start automatically when a host
key is generated.


01-Jan-2000 01:01:11 %INIT-I-InitCompleted:Initialization task is completed



console> 01-Jan-2000 01:01:11 %BOX-I-PSUP:Power Supply #1 is up


01-Jan-2000 01:01:11 %BOX-W-PSNOTPRES:Power Supply #2 is not present


01-Jan-2000 01:01:11 %LINK-W-Down:1/e1


01-Jan-2000 01:01:11 %LINK-W-Down:1/e2


01-Jan-2000 01:01:11 %LINK-W-Down:1/e3


.....
```

```
.....

Jan-2000 01:01:13 %LINK-W-Down:1/e2

01-Jan-2000 1:01:13 %LINK-W-Down:1/e23

01-Jan-2000 1:01:13 %LINK-W-Down:1/e24

01-Jan-2000 1:01:13 %LINK-W-Down:1/g1

01-Jan-2000 1:01:13 %LINK-W-Down:1/g2

01-Jan-2000 01:01:14 %LINK-I-Up:Vlan 1

01-Jan-2000 01:01:14 %LINK-I-Up:1/e1


console>
```

これでデバイスを設定する準備ができました。

デバイスのデフォルト設定

デバイスのデフォルト設定に戻るには、特権モードプロンプト (#) で **delete startup-config** コマンドを実行して、デバイスを再起動します。デバイスが再ロードされると、デフォルト設定が適用されます。

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

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

.

.

.

.
```

リモート管理アクセス

リモートデバイス管理 (Telnet、ウェブなど) を許可するには、次の手順を実行します。

1. 以下のように、コンソールで **enable** コマンドを実行して、Privileged EXEC 画面モードに入ります。

```
console>enable

console#
```

2. CAT5 Cable を使用し、Ethernet ポートのいずれかを介して (またはデバイスに接続されたネットワークを介して) 管理ステーション (PC) をデバイスに接続します。この例ではポート e1 です。ASCII ターミナルで、インタフェースのステータスが "up" に変更されたことと、STP ステータスが転送 (30 秒後に) されることを確認します。

```
console>enable

Console#

01-Jan-2000 1:43:03 %LINK-I-Up:Vlan 1
```

```
01-Jan-2000 1:43:03 %LINK-I-Up:1/e1


01-Jan-2000 01:43:34 %STP-I-PORTSTATUS:Port 1/e1:STP status Forwarding
```

3. 以下のように、コンソールで **configure** コマンドを実行して、Configuration 画面モードに入ります。

```
console> enable


console# configure


console(config)#
```

4. 以下のように、コンソールで **interface ethernet** コマンドを実行して、VLAN1 を介して Device Configuration 画面モードに入ります。

```
console> enable


console# configure


console(config)# interface vlan 1


console(config)# exit
```

5. 管理ステーションに接続されたインタフェースに IP アドレスを割り当てることによって、デバイス上で IP アドレスを定義します (この例では 50.1.1.1)。管理ステーションがインタフェースに直接接続されている場合、インタフェースの IP アドレスは、管理ステーションと同じサブネットを持っている必要があります。

```
console> enable


console# configure


console(config)#


console(config-if)# ip address 50.1.1.2 /8


01-Jan-2000 1:48:37 %LINK-W-Down:Vlan 1


console(config-if)# exit


console(config)# exit
```

6. 管理ステーションがインタフェースに直接接続されていない場合 (リモートネットワークのメンバー) は、デバイス上でデフォルトゲートウェイを管理します。ゲートウェイが設定した IP アドレスは、デバイスに接続されたルータインタフェースの IP です。

```
console> enable

console# configure

console(config-if)#

console(config-if)# exit

console(config)# ip default-gateway 50.1.1.100

console(config)# exit
```

7. デバイスから管理ステーションを ping して、接続が確立されていることを確認します (これを実行する前に、ポートが STP 転送に入るため 30 秒間待ってください)。この例では、管理ステーション IP は 50.1.1.3 です。

```
console> enable

console# configure

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#
```

8. リモートユーザー (telnet、Web Server など) に完全な (特権レベル 15) デバイスアクセスを許可するため、ユーザー名とパスワードを定義します。この例では、ユーザー名とパスワードは "Dell" です。

```
console#


console# configure


console(config)# username Dell password Dell level 15


console(config)#
```

9. Console、Telnet、SSH、HTTP、および HTTPS セキュリティパスワードを設定します。

```
console> enable


console# configure


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 admin


console(config-line)# exit


console(config)# aaa authentication login default line


console(config)# aaa authentication enable default line


console(config)# line telnet


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

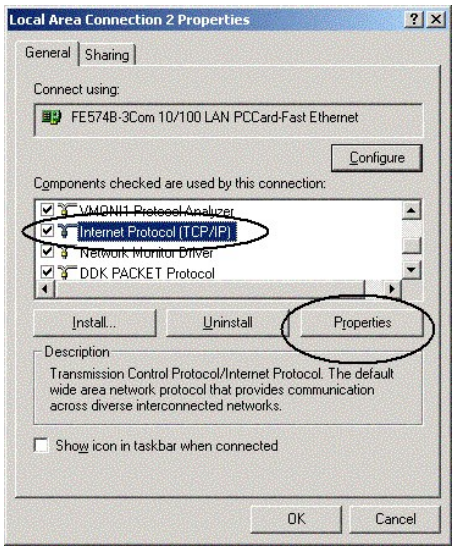
```
console(config-line)# enable authentication default

console(config-line)# password admin

console(config-line)# exit

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 admin

console(config-line)# exit

console(config)# ip http authentication local

console(config)# username admin password admin 15

console(config)# ip https authentication local

console(config)# username admin password admin 15

console(config)# crypto certificate generate key-generate

console(config)# ip https server

console(config)# exit

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

これでデバイスの設定が完了し、ウェブ管理インタフェースを実行する準備ができました。

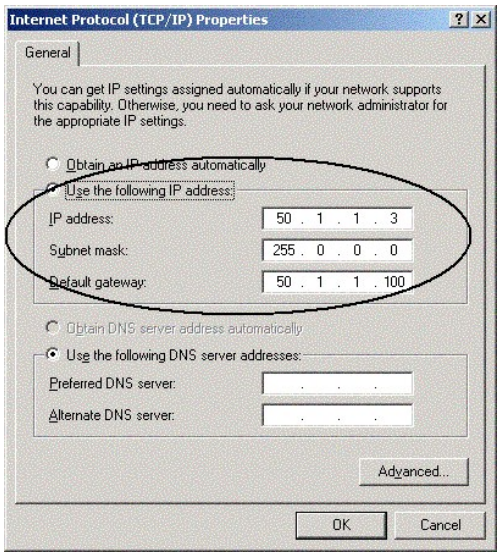
管理ステーションの実行開始

デバイス起動するには、次の手順を実行します。

1. リモート管理ステーションとして使用する PC に IP アドレスを定義します。Windows で、**スタート → 設定 → ネットワークとダイヤルアップ接続**を選びます。
2. 管理に使用するネットワーク接続を右クリックします。接続プロパティウィンドウが表示されます。



3. インターネットプロトコル (TCP/IP) を設定するオプションを選択して、**プロパティ**をクリックします。インターネットプロトコル (TCP/IP) プロパティウィンドウが表示されます。



4. **Use the following IP address** オプションを選択します。
5. インターネットプロトコル (TCP/IP) プロパティウィンドウで、IP アドレス、マスク、および PC のデフォルトゲートウェイを DHCP を介してでなく静的に定義します。

メモ: PC が、PowerConnect 3324/3348 デバイスに直接でなく、ルータに接続されている場合は、PC に接続されたルータインタフェースの IP アドレス (PowerConnect デバイスに接続する) として、デフォルトゲートウェイを設定する必要があります。

Telnet アクセス

Telnet を介してデバイスにアクセスするには、Windows または DOS のコマンドラインを使用するか、または Telnet アプリケーションを使用します。パスワードは正しく入力してください。接続は、デバイスに定義された IP アドレスで実行されます。

アクセスが許可された後は、デバイスを直接管理する際と同様にコマンドを使用できます。

1. Windows で、**スタート** → **ファイル名を指定して実行**をクリックし、cmd コマンドを入力します。標準の Windows コマンドラインインタフェースが表示されます。
2. **Telnet** コマンドとデバイス IP アドレスを入力します。

```
Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.

C:\>telnet 50.1.1.2

01-Jan-2000 02:40:23 %MSCM-I-NEWTERM:New TELNET connection from 50.1.1.2

User Name:Dell

Password:****

console# show ip interface

Gateway IP Address Activity status

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

50.1.1.100 inactive

IP Address I/F
```

```
---------------------- ----------------------


50.1.1.1/8 vlan 1



console#
```

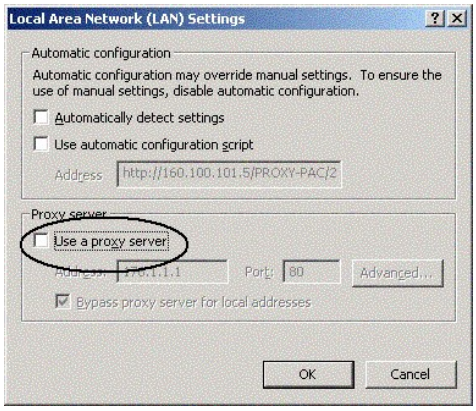
ASCII ターミナルで、デバイスが Telnet セッションのステータスを示していることに注意してください。

```
console> 01-Jan-2000 02:39:04 %MSCM-I-NEWTERM:New TELNET connection from 50.1.1.3


01Jan-2000 02:39:11 %MSCM-I-TERMTERMINATED:TELNET connection from 50.1.1.3 terminated
```

ウェブアクセス (HTTP サーバー)

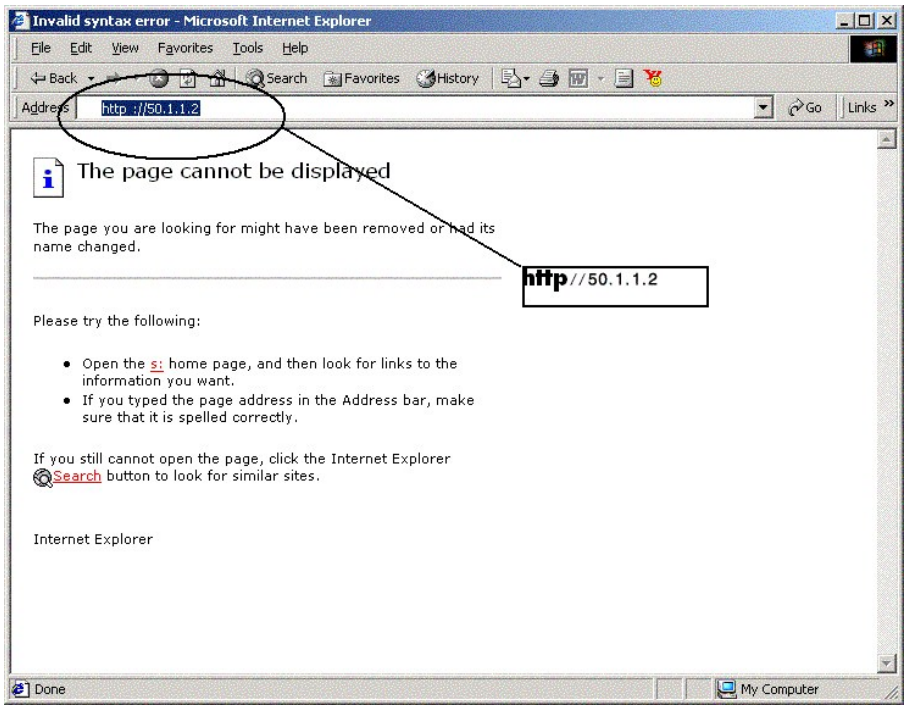
デバイスにウェブアクセスするには、次の手順を実行します。

1. HTTP プロキシサーバー使用時の特有の問題を回避するには、ブラウザのプロキシ設定を無効化 (チェックを外す) します (Microsoft Internet Explorer では、ツール → インターネットオプション → 接続 → LAN の設定)。



プロキシウィンドウの無効化

2. デバイスに設定した IP を、ブラウザウィンドウで入力します (http:// あり、またはなしで)。

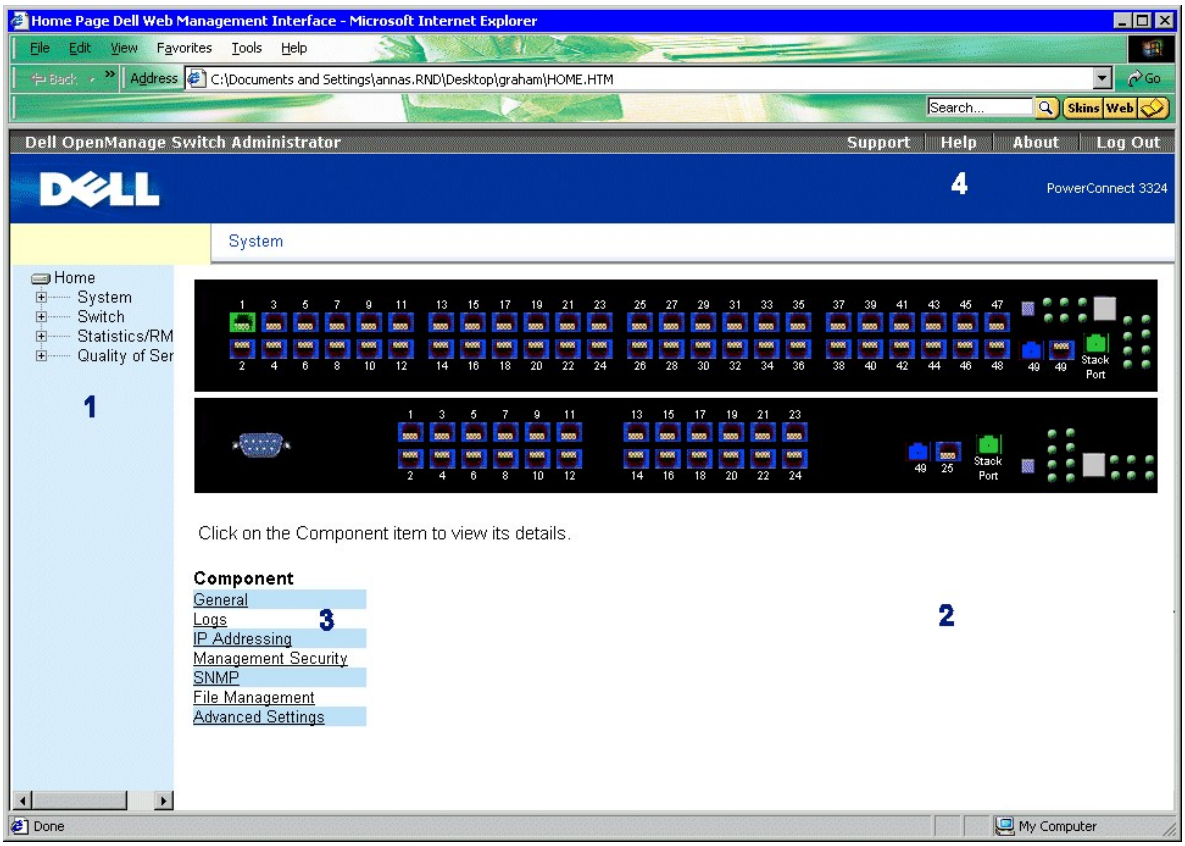


ログオンインタフェース

3. 認証ウィンドウが表示されたら、ユーザー名とパスワードを入力します。

パスワードプロンプト

デバイスのウェブ管理インタフェースが表示されます。



PowerConnect 3324/3348 ウェブ管理インタフェース

PowerConnect 3324/3348 Interface Components Table では、インタフェースコンポーネントとそれに対応する数字を一覧表示します。

スタッキングの設定

スタッキングの概要

スタックされている PowerConnect 3324/3348 ユニットは、単一のシステムとして動作します。各スタックには、マスターユニットが 1 つと、最大で 5 つのメンバーユニットがあります。マスターユニットは、以下の用途に使用されます。

- すべてのメンバーデバイスのセットアップの管理
- メンバーポートの設定
- メンバーコンテキストで発生するイベントの管理

スタックされているすべてのユニットのイベントログは、選択されたマスターユニットで報告され管理されます。各メンバーユニットには、それぞれの ASCII ターミナル （RS-232 ポート） を介してアクセスできますが、メンバーユニットはマスターユニットを介してアクセスできます。

スタッキング要件

スタックを構築する前に、以下のスタッキング要件を実行します。

- 各ユニットにスタックリンクモジュールが挿入されているか確認します。
- すべてのケーブルが適切に接続されているか確認します。
- すべてのユニットの電源を入れます。数秒後、Unit ID LED が点滅します。
- 各メンバーユニットは Unit ID を持ちます。Unit ID の選択の詳細については、「スタック ID ボタン」 を参照してください。

スタックの設定

この項では、スタックの設定手順について説明します。スタックを設定するには、次の手順を実行します。

メモ: スタックユニット ID は、15 秒以内に選択する必要があります。

1. 選択したマスターユニットに接続します。デバイスが起動を始めます。
2. スタッキング LED 1 が選択されるまで、**Stack ID** ボタンを使用して、Unit 1 を選びます。選択したユニットが Stack Master である場合、LED は 15 秒以内に点滅を停止します。

メモ: スタッキング LED が点滅を停止しない場合、マスターユニットはグループに接続されていません。

3. 選択したメンバーユニットに接続します。デバイスが起動を始めます。
4. **Stack ID** ボタンを使用して、15 秒以内に Unit 2 を選択します。
5. 手順 3 と手順 4 を、すべてのスタッキングメンバーで繰り返します。

メモ: ユニットは、Unit ID に応じてスタックします。たとえば、マスターユニットを最初にスタックし、Unit 2 をマスターユニットのすぐ下にスタックします。

スタックの拡張

この項では、スタッキングメンバーの追加手順について説明します。スタックを拡張するには、次の手順を実行します。

メモ: スタックユニット ID は、15 秒以内に選択する必要があります。

1. スタックが正常に動作しているか確認します。
2. 下部スタッキングコネクタを追加するスタッキングメンバーユニットに接続します。
3. 新しいスタッキングユニットに接続します。デバイスが起動を始めます。
4. **Stack ID** ボタンを使用して、15 秒以内にユニットメンバーを選択します。
5. 新しいメンバーごとに、既存のリングを開いて、新しいメンバーのスタッキングケーブルを接続します。

スタッキングメンバーの交換および Unit ID の再割り当てについては、「スタックメンバーの交換」 を参照してください。

デバイスの再起動

メモ: デバイスを再起動する前に、デバイス設定を保存します。デバイスをリセットすると、保存されていない設定の変更はすべて失われます。

1. CLI モードを起動します。以下のプロンプトが表示されます。

```
Console > enable
```

2. Reload と入力します。以下のメッセージが表示されます。

```
>reload

This command will restart the whole system and disconnect your current session.Do you want to continue?
```

3. Y と入力します。デバイスが再起動します。

Startup （スタートアップ） メニューの機能

Startup メニューから、追加のデバイス設定機能が実行できます。Startup メニューは、以下の設定機能を表示します。

- ソフトウェアのダウンロード
- フラッシュファイルの消去
- フラッシュセクターの消去

以下に、Startup メニューを示します。

```
[1] Download Software

[2] Erase Flash File

[3] Erase Flash Sectors

[4] Password Recovery Procedure

[5] Enter Diagnostic Mode

[6] Back

Enter your choice or press 'ESC' to exit:Startup Menu
```

ソフトウェアのダウンロード

Startup メニューを使用する

デバイスソフトウェアは、起動プロセス中に Startup メニューにアクセスして、そこからダウンロードできます。

CLI モードからソフトウェアのダウンロードを開始するには、次の手順を実行します。

1. CLI モードを起動します。以下のプロンプトが表示されます。

```
console>
```

2. reload と入力します。以下のメッセージが表示されます。

```
console>reload

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

3. Y と入力します。デバイスが再起動します。
4. 2 秒以内に <Return> または <Esc> を押します。**Startup** メニューが表示されます。

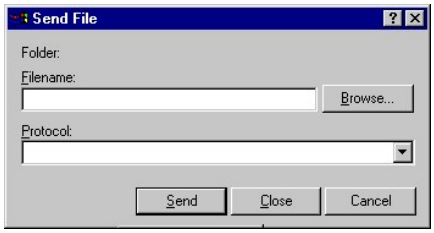
メモ: **Startup** メニューを表示するには、<Return> または <Esc> キーを 2 秒以内に押す必要があります。

メモ: 何も選択されない場合、デバイスは 35 秒後にタイムアウトします。CLI を使用してタイムアウト期間を再設定できます。

5. 1 と入力します。以下のプロンプトが表示されます。

```
Downloading code using XMODEM.
```

6. VT100 エミュレータを使用して、ダウンロードファイルオプションを選択します。 **Send File** ウィンドウが表示されます。**Send** ボタンをクリックします。



Send File ウィンドウ

7. Configuration ファイルのファイルパスを入力します。
8. プロトコルが Xmodem に定義されていることを確認します。
9. **Send** をクリックします。ソフトウェアがダウンロードされます。

デバイスは自動的に再起動します。

メモ: ソフトウェアをダウンロードする前に、TFTP サーバーを設定する必要があります。

フラッシュファイルの消去

デバイス設定は、ASCII ターミナルを使用して消去することができます。設定が消去されると、すべての IP ホストパラメータおよび CLI、ウェブ管理インタフェース、または SNMP を介して設定されたパラメータは、再設定する必要があります。

デバイス設定を消去するには、次の手順を実行します。

1. ASCII ターミナルがデバイスに接続されていることを確認します。
2. 電源ケーブルを接続します。デバイスが起動し、**Startup** メニューが表示されます。デバイスが起動を始めます。
3. 2 秒以内に <Esc> を押して終了するか、または <Enter> を押します。
   Startup メニューが表示されます。
4. 希望の数字を入力するか、<Esc> を押して終了します。2 秒以内に 2 と入力します。次のメッセージが表示されます。

```
Warning!About to erase the file from flash Are you sure (Y/N)?
```

5. Y と入力します。 以下のメッセージが表示されます。

```
? Flash file name (8 characters, Enter for none.)
```

6. フラッシュファイル名として config と入力します。設定は消去されスイッチは再起動します。最初の IP パラメータ設定については、「デバイス設定について」 を参照してください。

フラッシュセクターの消去

フラッシュメモリは、実行可能なイメージ、CDB （MIB ファイル）、およびログファイルなどの追加ファイルを保存します。

注意： フラッシュを消去すると、すべてのソフトウェアファイルをダウンロードしなおして、再インストールする必要があります。

1. ASCII ターミナルがデバイスに接続されていることを確認します。
2. 電源ケーブルを接続します。デバイスが起動し、Startup メニューが表示されます。
3. 希望の選択を入力するか、または <Esc> を押して終了します。2 秒以内に 3 と入力します。次のメッセージが表示されます。

```
Warning!About to erase Flash Memory!FLASH size = 16252928. blocks = 64 Are you sure (Y/N)?
```

4. Y と入力して確認します。次のメッセージが表示されます。

```
Enter First flash block (1 - 64):
```

5. 消去する最初のフラッシュブロックを入力して、<Enter> を押します。値の範囲は、1 ～ 64 です。 以下のメッセージが表示されます。

```
Enter Last flash block (1 - 64):
```

6. 消去する最後のフラッシュブロックを入力して、<Enter> を押します。次のメッセージが表示されます。

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

7. Y と入力して確認します。次のメッセージが表示されます。

```
Erasing flash blocks 1 - 1:Done.
```

パスワードの復元

Access Method パスワードを復元するには、次の手順を実行します。

1. デバイスを起動または再起動して、2 秒以内に <Enter> を押します。
   Startup メニューが表示されます。以下に Startup メニューを示します。

```
Startup menu

[1] Download sw

[2] Erase from flash

[3] Erase Flash

[4] Password Recovery Procedure
```

2. 4 と入力して<Enter>キーを押します。アクセスメソッドがリセットされます。

メモ: デバイスのセキュリティを確認するには、Console Access Method パスワードを再定義します。

ユーザーパスワード設定の詳細については、『*CLI User's Guide*』を参照してください。

診断プログラムの実行

このオプションを使用する前に、デルのテクニカルサポートにお問い合わせください。「Dell の連絡先」を参照してください。

スタッキングユニットへのソフトウェアのダウンロード

以下の方法のうちの 1 つを使用して、TFTP サーバーからすべてのスタッキングユニットにソフトウェアをダウンロードします。

- CLI を順番に使用する
- CLI を個別に使用する
- Dell OpenManage™ Switch Administrator を使用する

CLI を順番に使用したソフトウェアのダウンロード

1. マスターユニットの 1 つ以上のポートに IP アドレスが割り当てられていることを確認します。
2. `console# show version` と入力して、各ユニットでソフトウェアのどのバージョンが実行されているか確認します。以下に表示される情報の例を示します。

```
Unit SW version Boot version HW version
```

```
----------------------------------------------------

1 1.0.0.52 1.0.0.13 00.00.01

2 1.0.0.52 1.0.0.13 00.00.01
```

各ユニットのソフトウェアのバージョン、起動バージョン、およびハードウェアのバージョンが表示されます。上記の例では、ユニットの起動バージョンとハードウェアのバージョンが異なり、ソフトウェアのバージョンは同じです。

3. console# show bootvar と入力して、どのユニットでどのイメージバージョンが現在アクティブか確認します。以下に表示される情報の例を示します。

```
Unit Active image Selected for next boot

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

1 image-2 image-2

2 image-1 image-1
```

アクティブなイメージファイルとデバイスのリセット後にアクティブになるイメージファイルの両方がすべてのユニットで表示されます。

4. console# copy tftp://*{tftp address}*/*{file name}* image と入力して、ソフトウェアをマスターユニットにコピーします。ファイルはコピーされますが、デバイスがリセットされファイルが Active Image ファイルとして選択されるまでアクティブになりません。以下に、表示される情報の例を示します。

```
console# copy tftp://176.215.31.3/332448-10018.dos image

Erasing file image-1...done.

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

メモ： 各 ! は、10 個のパケットが正常に転送されたことを示します。

```
Copy:2739187 bytes copied in 0:01:13 [hh:mm:ss]
```

5. console# copy tftp://50.1.1.2/332448-10018.dos unit://2/image と入力します。デバイスソフトウェアは、スタッキングメンバー 2 にコピーされます。 unit://2/image は、ソフトウェアのコピー先のスタッキングメンバー Unit ID を示します。以下に、表示される情報の例を示します。

```
...................Unit 2:Erased image-1

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

```
Copy:2744590 bytes copied in 0:01:41 [hh:mm:ss]


console# 01-Jan-2000 1:01:55 %COPY-W-TRAP:The copy operation was completed successfully
```

6. 各スタッキングメンバーで手順 5 を繰り返します。正しいスタッキングメンバー Unit ID にソフトウェアがコピーされたか確認します。
7. console# boot system image-2 と入力して、デバイスがリセットされた後に使用する Image ファイルを設定します。
8. console# boot system unit 2 image-1 と入力します。これは再起動後に、デバイスがイメージ 1 から起動されることを示します。
9. console# reload と入力します。以下のメッセージが表示されます。

```
This command will reset the whole system and disconnect your current


session.Do you want to continue (y/n) [n] ?
```

10. Y と入力します。デバイスが再起動します。
11. 手順 2 と手順 3 を繰り返して、どのイメージファイルがアクティブか確認します。

CLI を個別に使用したソフトウェアのダウンロード

この項では、各スタッキングメンバーに個別にデバイスソフトウェアをダウンロードする手順について説明します。

- TFTP サーバーからマスターユニットへ
- マスターユニットからメンバーユニットへ

1. マスターユニットの 1 つ以上のポートに IP アドレスが割り当てられていることを確認します。
2. console# show version と入力して、各ユニットでソフトウェアのどのバージョンが実行されているか確認します。以下に、表示される情報の例を示します。

```
Unit SW version Boot version HW version


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


1 1.0.0.52 1.0.0.13 00.00.01


2 1.0.0.52 1.0.0.13 00.00.01
```

各ユニットのソフトウェアのバージョン、起動バージョン、およびハードウェアのバージョンが表示されます。上記の例では、ユニットの起動バージョンとハードウェアのバージョンが異なり、ソフトウェアのバージョンは同じです。

3. console# show bootvar と入力して、どのユニットでどのイメージバージョンがアクティブか確認します。以下に表示される情報の例を示します。

```
Unit Active image Selected for next boot


----------------------------------------------------
```

```
1 image-2 image-2


2 image-1 image-1
```

アクティブなイメージファイルとデバイスのリセット後にアクティブになるイメージファイルの両方がすべてのユニットで表示されます。

4. console# copy tftp://*{tftp address}*/*{file name}* image と入力して、ソフトウェアをマスターユニットにコピーします。ファイルはコピーされますが、デバイスがリセットされファイルが Active Image ファイルとして選択されるまでアクティブになりません。以下に、表示される情報の例を示します。

```
console# copy tftp://176.215.31.3/332448-10018.dos image


Erasing file image-1...done.


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


Copy:2739187 bytes copied in 0:01:13 [hh:mm:ss]
```

5. console# boot system image-1 と入力して、デバイスがリセットされた後に使用する Image ファイルを設定します。
6. console# reload と入力します。以下のメッセージが表示されます。

```
This command will reset the whole system and disconnect your current


session.Do you want to continue (y/n) [n] ?
```

7. Y と入力します。デバイスが再起動します。
8. 手順 3 を繰り返してどのイメージファイルがアクティブか確認します。
9. console# copy image unit://2/image と入力します。以下に表示される情報の例を示します。

```
console# copy image unit://2/image


...................Unit 2: Erased image-2


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


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


Copy:2883576 bytes copied in 00:01:35 [hh:mm:ss]


console# 01-Jan-2000 01:08:59 %COPY-W-TRAP:The copy operation was completed successfully
```

10. `console# boot system unit {unit number} image-{file name}` と入力します。
11. 各スタッキングユニットで手順 9 を繰り返します。
12. `console# reload` と入力します。以下のメッセージが表示されます。

```
This command will reset the whole system and disconnect your current

session.Do you want to continue (y/n) [n] ?
```

13. Y と入力します。デバイスが再起動します。
14. 手順 2 と手順 3 を繰り返して、正しい Image ファイルがアクティブになっているか確認します。

PowerConnect 3324/3348 Dell OpenManage Switch Administrator を介したソフトウェアのダウンロード

OpenManage Switch Administrator を介したソフトウェアのダウンロード手順については、「ファイルの管理」 を参照してください。

SNMP の設定の定義

SNMP（Simple Network Management Protocol）はネットワークデバイスの管理メソッドを提供します。SNMP をサポートするデバイスは、ローカルソフトウェア（エージェント）を実行します。

SNMP エージェントは、デバイスの管理に使用される変数の一覧を保持します。変数は MIB（Management Information Base）で定義されます。MIB はエージェントによって管理される変数を表示します。SNMP エージェントは、MIB 仕様フォーマットだけでなくネットワーク上で情報にアクセスするのに使用されるフォーマットも定義します。

SNMP エージェントへのアクセス権は、アクセスストリングによって制御されます。デバイスと通信を行うには、内蔵 Web サーバで有効なコミュニティストリングを送信して、認証を受ける必要があります。

PowerConnect デバイスのデフォルトのコミュニティストリングには、以下のものがあります。

- Public ― このストリングを使用すると、認証を受けた管理ステーションは MIB オブジェクトを検出できます。
- Private ― このストリングを使用すると、認証を受けた管理ステーションは MIB オブジェクトを検出し、変更できます。

SNMP が使用されていない場合、次の手順を実行します。

- デフォルトのコミュニティストリングを変更して、PowerConnect デバイスへの不正なアクセスを防ぎます。
- 両方のデフォルトのコミュニティストリングを削除します。コミュニティストリングがない場合、PowerConnect デバイスへの SNMP 管理アクセスは無効になります。

ストリングを削除するには、次の手順を実行します。

メモ: 設定コンテキストを使用するには、ユーザーは特権レベル 15 を割り当てられている必要があります。

1. Enable と入力します。プロンプトは、# サインを表示します。
2. Privileged Exec レベルグローバル設定コンテキストが有効でない場合、configure と入力して、<Enter> を押します。
3. no snmp-server community private と入力し、<Enter> を押して、**private** コミュニティストリングを削除します。
4. no snmp-server community public と入力し、<Enter> を押して、**public** コミュニティストリングを削除します。
5. exit と入力します。これで設定コンテキストを終了します。
6. copy running-config startup-config と入力し、<Enter> を押して、設定の変更を保存します。

デバイスの接続

PowerConnect デバイスに IP アドレスを割り当てた後に、デバイスを PowerConnect の正面パネルの RJ45 コネクタに接続します。

注意： RJ-45 ポートのオートネゴシエイションが無効になっている場合は、オート MDI/MDI-X ピンの信号設定も無効です。

SFP トランシーバポートにデバイスを接続するには、次の手順を実行します。

1. ケーブル要件を確認して、適切な SFP トランシーバタイプを使用します。
2. SFP トランシーバ（別売り）を SFP トランシーバスロットに挿入します。
3. 適切なネットワーク配線を使用して、デバイスを SFP トランシーバのコネクタに接続します。

注意： SFP トランシーバにリンクが確立した場合、関連する内蔵 10/100/1000BASE-T ポートは無効になります。

すべての装置のスイッチを切るには、電源ケーブルを電源ソケットから抜きます。電源ソケットは装置の近くにあり、容易にアクセスできる必要があります。

保護マーク「B」が付いている場合は、その装置が PN-93/T-42107 および PN-EN 55022:1996 規格の保護使用要件に準拠していることを表しています。

メモ、注意および警告

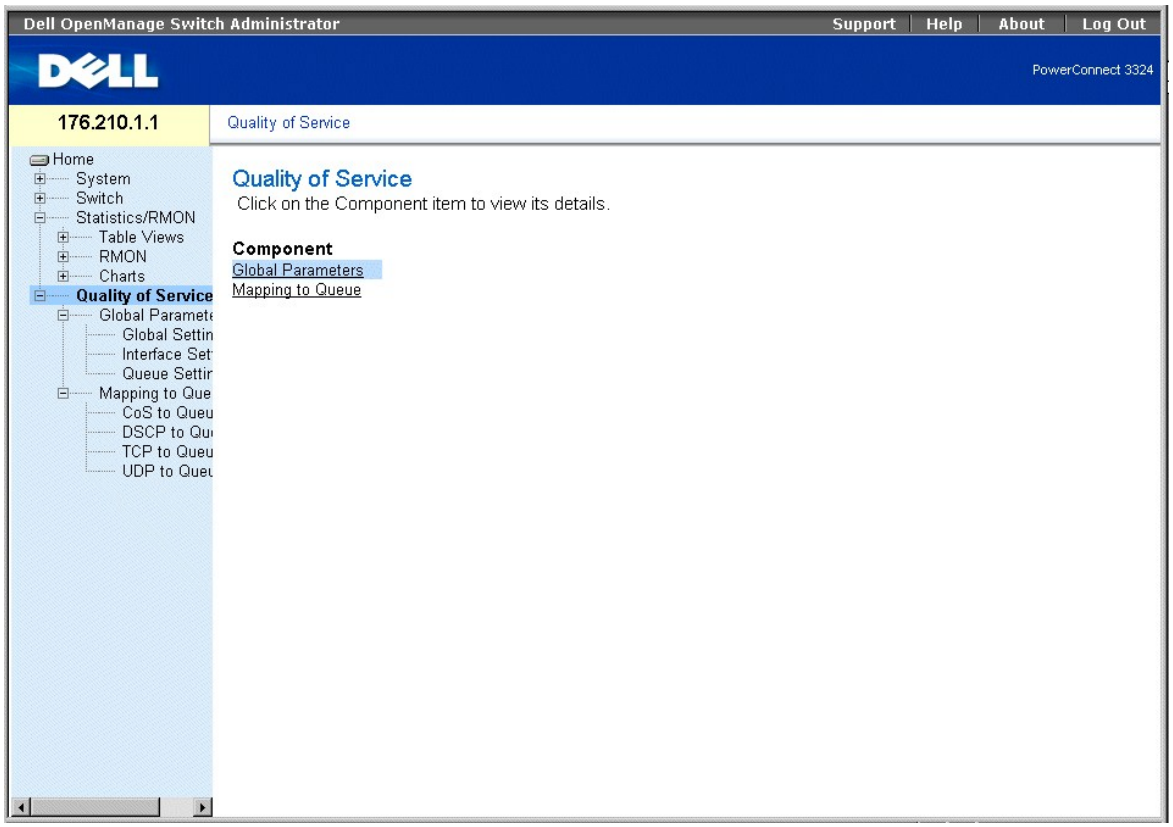
メモ、注意および警告

Quality of Service（サービスのクオリティ）の設定

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

この項では、QoS（Quality of Service）パラメータの定義および設定について説明します。

- Tree View で、**Quality of Service** をクリックします。**Quality of Service** ページが開きます。



Quality of Service ページ

この項には以下のトピックがあります。

- QoS（Quality of Service）の概要
- QoS グローバルパラメータの定義
- キューへのマッピング

QoS（Quality of Service）の概要

QoS（Quality of Service）は、ネットワーク内に QoS および優先度キューを導入する機能を提供します。QoS は、ポリシー、フレームカウンタ、およびコンテキスト

にもとづくネットワークトラフィックを向上させます。

QoS には、高優先度キューを割り当てることができる音声、ビデオ、およびリアルタイムトラフィックなどのトラフィックを含み、他のトラフィックに低優先度キューを割り当てることができます。結果として、要求度の高いトラフィックのトラフィックフローが向上します。

QoS は、以下で定義されます。

- Classification — どのパケットが特定の値と一致するかを指定します。ユーザーが定義した設定に一致するすべてのパケットは、一緒に分類されます。
- Action — 転送されるパケットがパケット情報および VPT（VLAN 優先度）や DSCP（DiffServ Code Point）などのパケットフィールド値に基づく場合の、トラフィック管理を定義します。
- Prioritization — トラフィックには、転送用の適切な優先度およびキューが割り当てられています。

CoS（Class of Service）の情報

8 つの CoS 値は、4 つの転送キューのうちの 1 つにマップすることができます（Queue 1 ～ 4）。各キューには、異なる優先度があります。1 番目のキューの転送優先度は最低です。4 番目のキューの転送優先度は最高で、デフォルトでマップされません。

メモ: スタッキング構成では、Queue 4 は転送スタッキングトラフィックに使用されます。そのため、Queue 4 にトラフィックを追加すると、スタック制御を妨害する可能性があります。

3 つのマッピングテーブルがあります。

- CoS to Queue Mapping Table
- DSCP to Queue Mapping Table
- TCP/UDP to Queue Mapping Table。TCP/UDP Table は、デフォルトで空です。

Cos to Queue Mapping Table には、キュー値を転送するデフォルトの CoS マッピングがあります。

CoS値	転送するキュー値
0	q2
1	q1（最低の優先度 = ベストエフォート）
2	q1（最低の優先度 = ベストエフォート）
3	q2
4	q2
5	q3
6	q3
7	q3

CoS to Queue Mapping Table のデフォルト値

CoS マッピングは、システムごとに有効にします。CoS 値の順番は 0 ～ 7 で、0 が最低の優先度を持ち、7 が最高の優先度を持ちます。

DSCP 値は、優先度キューにマップすることができます。**DSCP to Queue Mapping Table Default Values Table** には、キュー値を転送するデフォルトの DSCP マッピングが含まれています。

DSCP to Queue Mapping Table のデフォルト値

DSCP 値	転送するキュー値
0-7	q1（最低の優先度）

8-15	q1
16-23	q2
24-31	q2
32-39	q2
40-47	q3
48-55	q3
55-63	q3（最高の優先度）

DSCP マッピングは、システムごとに有効にします。

QoS Services（QoS のサービス）

特定のキューにパケットを割り当てた後、QoS サービスをキューに割り当てることができます。出力キューには、以下の方法のうちの 1 つを使用してスケジュールスキームを設定することができます。

- Strict Priority — 時間に依存するアプリケーションは、常に迅速なパスを介して転送されます。Strict Priority を使用して、ネットワーク管理者は、重要なミッションの、時間に依存したトラフィックを時間に依存しないアプリケーションに優先させることができます。たとえば、Strict Priority では、IP を介した音声トラフィックは FTP または E メール（SMTP）トラフィックの前に転送されます。Strict Priority キューは、残りのキューのトラフィックが転送される前に空になります。

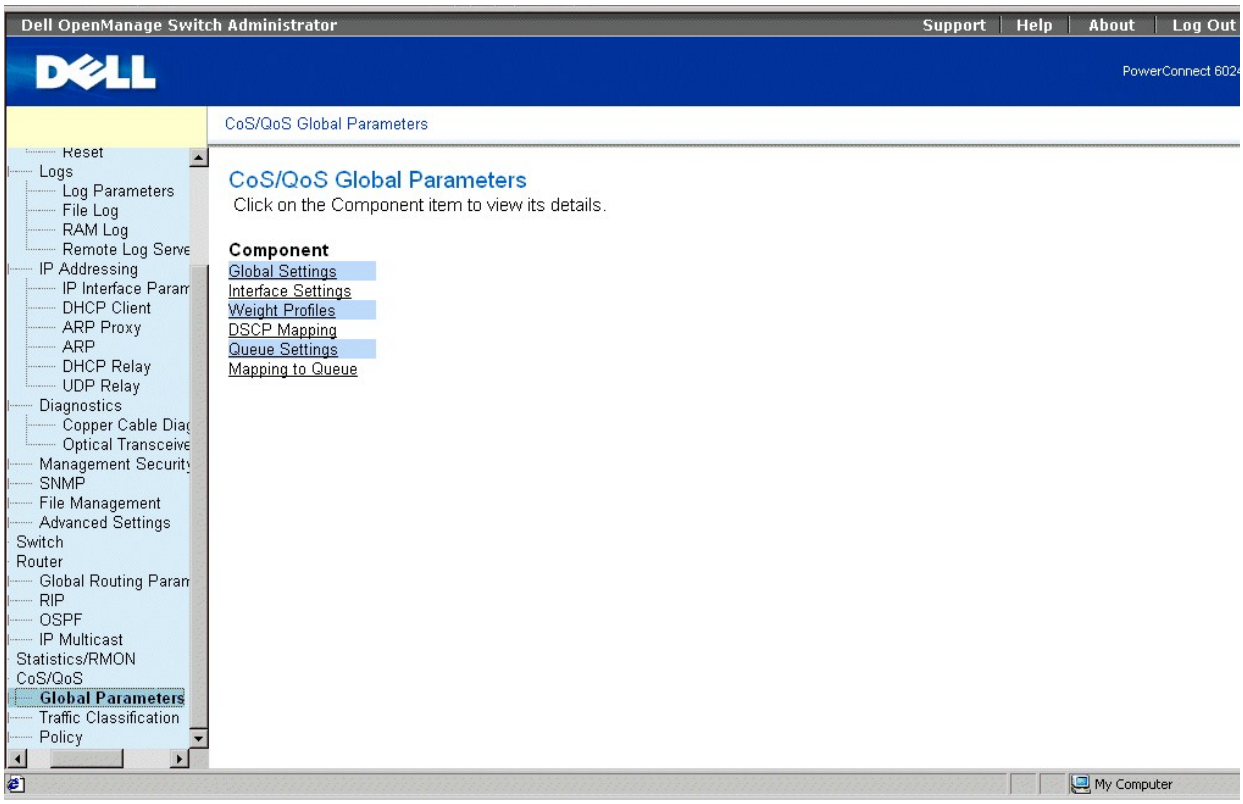
- Weighted Round Robin — PowerConnect 3324/3348 の転送容量が 1 つのアプリケーションに占有されないように設定します。WRR（Weighted Round Robin）は、round robin order のすべてのキューを転送します。キュー優先度はキューの長さで定義されます。キューが長いほどキューの転送優先度が高くなります。
  たとえば、4 つのキューが 1、2、3、および 4 の weight を持つ場合、最高の転送優先度を持つパケットに Queue 4 が割り当てられ、最低の転送優先度を持つパケットに Queue 1 が割り当てられます。Queue 4 に最高の転送優先度を提供することで、WRR はより高い優先度のトラフィックを持ち、低い優先度のトラフィックが十分に転送されるようにします。

スケジュールスキームは、全システムで有効になります。Strict Priority ポリシーに割り当てられたキューは、自動的に最高の優先度キューに割り当てられます。デフォルトで、すべての値は Strict Priority にセットされています。WRR モードを変更する際、デフォルトの weight 値は 1 です。キュー weight 値は、WRR を使用してどんな順番でも割り当てることができます。WRR 値は、システム毎に割り当てられます。ベストエフォートトラフィックは、常に 1 番目のキューに割り当てられます。キュー 1 がベストエフォートになるように、WRR 値を割り当てる必要があります。

QoS グローバルパラメータの定義

QoS グローバルパラメータは、QoS Global Parameter ページで設定します。**QoS Global Parameters** ページを開くには、次の手順を実行します。

- Tree View で、**Quality of Service** → **Global Parameters** とクリックします。**CoS/QoS Global Parameters** ページが開きます。



CoS/QoS Global Parameters ページ

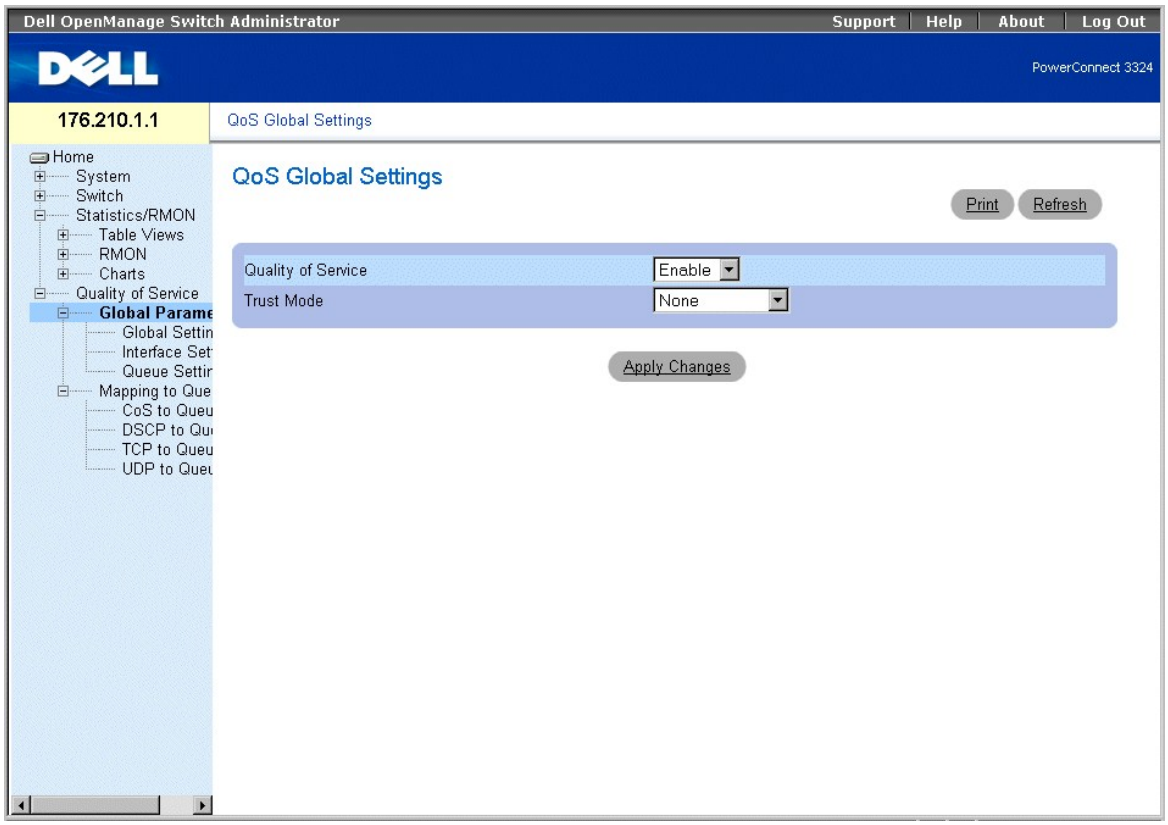
CoS/QoS Global Parameters ページには、以下のリンクがあります。

- グローバル QoS の設定
- QoS インタフェースの設定の定義
- キューの設定の定義

グローバル QoS の設定

QoS Global Settings ページを使用して、ユーザーは QoS を有効または無効にすることができます。また、**Trust** モードを選ぶこともできます。このモードは、パケットの定義済みフィールドに基づいて出力キューを決定するため、パケットのサービスを決定します。**QoS Global Settings** ページを開くには、次の手順を実行します。

- Tree View で、**Quality of Service** → **Global Parameters** → **Global Settings** とクリックします。**QoS Global Settings** ページが開きます。



QoS Global Settings ページ

QoS Global Settings ページには、以下のフィールドが含まれています。

- **Quality of Service** — QoS を使用したネットワークトラフィックの管理を有効にします。フィールド値のオプションには、以下のものがあります。
  - **Enable** — デバイスで QoS を有効にします。
  - **Disable** — デバイスで QoS を無効にします。
- **Trust Mode** — スイッチに入るパケットの分類にどのパケットフィールドを使用するか決定します。どのルールも定義されていない場合、定義済みのパケットフィールド（CoS、DSCP、または TCP/UDP ポート）を含むトラフィックは、対応する Trust Mode テーブルに基づいてマップされます。定義済みのパケットフィールドを持たないトラフィックは、ベストエフォートにマップされます。可能な Trust Mode フィールド値には、以下のものがあります。
  - **CoS** — 出力キュー割り当てが IEEE802.1p VPT（VLAN 優先度タグ）またはポートに割り当てられたデフォルト VPT で決定されることを示します。
  - **DSCP** — 出力キュー割り当てが DSCP フィールドで決定されることを示します。
  - **TCP/UDP** — 出力キュー割り当てが TCP/UDP ポートで決定されることを示します。

メモ: インタフェースの **Trust** 設定は、グローバル **Trust** 設定に優先します。

Quality of Service を有効にするには、次の手順を実行します。

1. **QoS Global Settings** ページを開きます。
2. **Quality of Service** フィールドで、**Enable** を選びます。
3. **Apply Changes** をクリックします。デバイスで、**Quality of Service** が有効になります。

Trust を有効にするには、次の手順を実行します。

1. **QoS Global Settings** ページを開きます。
2. **Trust Mode** フィールドで、Trust 設定を選びます。

3. **Apply Changes** をクリックします。デバイスで、Trust が有効 / 無効になります。

CLI コマンドを使用した Trust の有効化

次の表に、**QoS Global Settings** ページでの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
qos trust [cos | dscp | tcp-udp-port]	システムを基本的なモードおよび Trust ステートに設定します。
qos	デバイスで、QoS を有効にします。
no qos trust	非 Trust 状態に戻します。

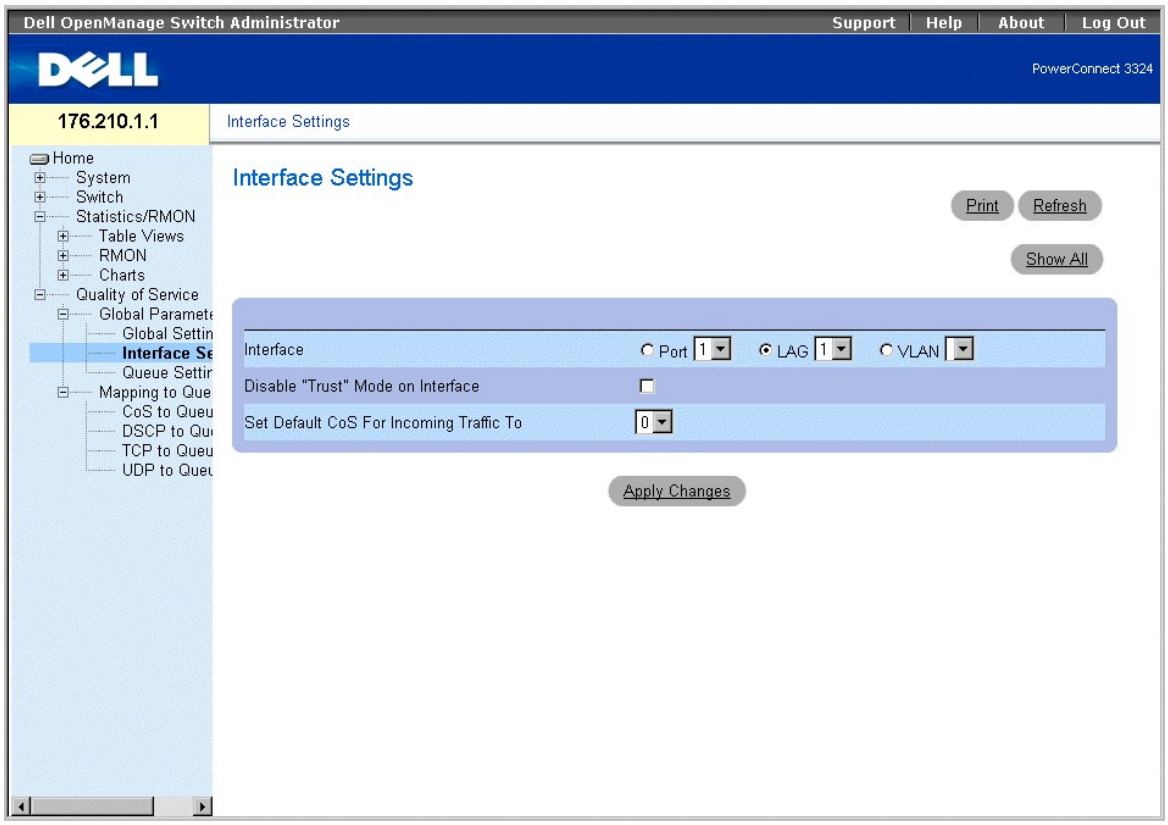
以下に、CLI コマンドの例を示します。

```
Console (config)# qos

Console (config)# qos trust dscp
```

QoS インタフェースの設定の定義

ユーザーは **QoS Interface Settings** ページを使用して、選択した Trust Mode をアクティブにするかどうかをポートごとに設定できます。タグなし受信パケットのデフォルト優先度も、**QoS Interface Settings** ページで選択します。**Interface Settings** ページを開くには、次の手順を実行します。

- Tree View で、**Quality of Service** → **Global Parameters** → **Interface Settings** とクリックします。**Interface Settings** ページが開きます。



Interface Settings ページ

Interface Settings ページには、以下のフィールドが含まれています。

- **Interface** — Trust Mode が適用される特定のインタフェースを示します。Trust Mode は、以下に適用されます。
  - **Port** — ポート番号を指定します。
  - **LAG** — LAG 番号を示します。
  - **VLAN** — VLAN 番号を示します。
- **Disable "Trust" Mode on Interface** — デバイスで、Trust 値を無効にします。パスワードの制限については、「グローバル QoS の設定」を参照してください。
- **Set Default CoS For Incoming Traffic To** — タグなしパケットのデフォルトの CoS タグ値を設定します。CoS タグ値は、0 ～ 7 です。デフォルト値は **0** です。

インタフェースに QoS/CoS 設定を割り当てるには、次の手順を実行します。

1. **QoS Interface Settings** ページを開きます。
2. **Interface** フィールドで、インタフェースを選びます。
3. 特定のインタフェースで Trust Mode を無効にする場合、**Disable "Trust" Modeon Interface** チェックボックスにチェックマークを付けます。
4. **Default CoS For Incoming Traffic** を必要な値に設定します。
5. **Apply Changes** をクリックします。QoS/CoS 設定がインタフェースに割り当てられます。

CLI コマンドを使用した QoS/CoS インタフェースの割り当て

次の表に、**Interface Settings** ページでのフィールドの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
qos trust	それぞれで Trust 状態を有効にします。
qos cos *default-cos*	デフォルトのポートの CoS 値を設定します。
no qos trust	各ポートで Trust 状態を無効にします。

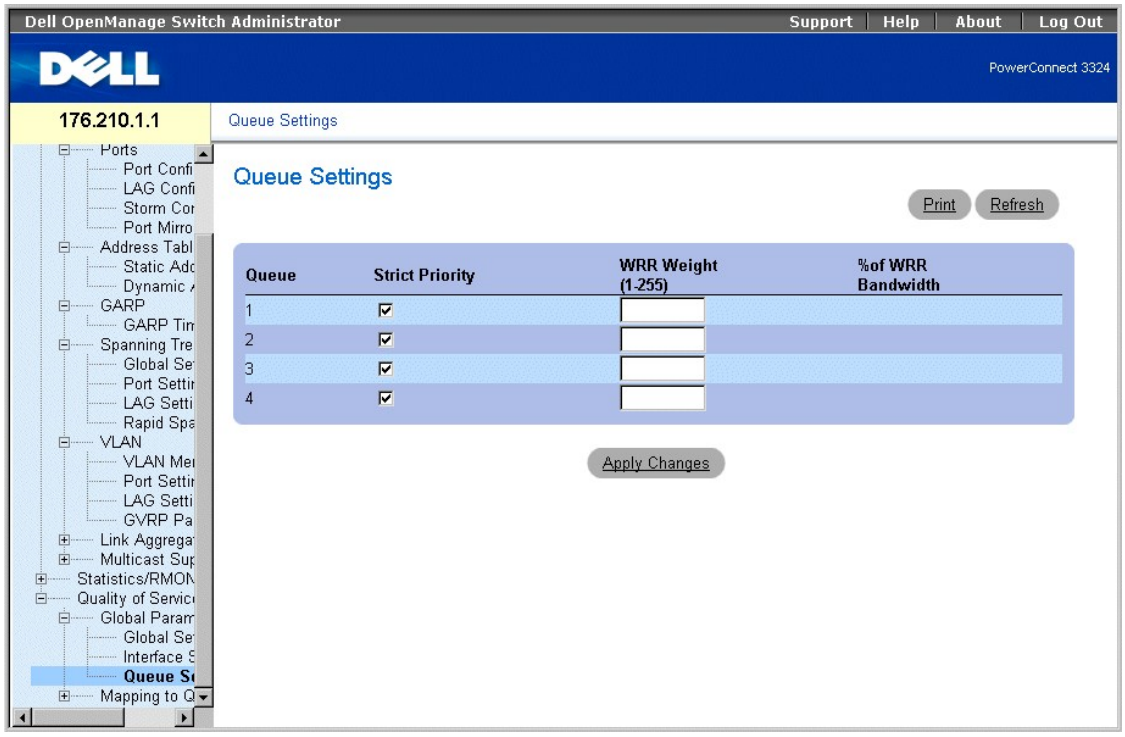
以下に、CLI コマンドの例を示します。

```
Console (config)# interface ethernet 1/e5

Console (config-if)# qos trust

Console (config-if)# qos cos 3
```

キューの設定の定義

Queue Settings ページを使用して、ネットワーク管理者は、WRR（Weighted Round Robin）の設定だけでなく、キューにバンド幅を割り当てることができます。各キューは、異なる WRR および WRED（Weighted Random Early Detection）値で設定されています。**Queue Settings** ページを開くには、次の手順を実行します。

- Tree View で、**Quality of Service** → **Global Parameters** → **Queue Settings** とクリックします。**Queue Settings** ページが開きます。



Queue Setting ページ

Queue Settings ページには、以下のフィールドが含まれています。

- **Queues** — キューの番号を示します。

メモ: キューの過負荷はネットワークの混雑の原因になることがあります。

- **Strict Priority** — トラフィックスケジュールが、キュー優先度のみに基づいているか特定します。デフォルトは Enabled です。
- **WRR** — キューのトラフィックスケジュールが、WRR スキームに基づいているか特定します。
- **WRR Weight** — WRR weight を送信キューに割り当てます。可能なフィールド値は 1 ～ 255 で、1 が最低値で 255 が最高値です。
- **% of WRR Bandwidth** — WRR に割り当てられたバンド幅の量を示します。

Queue Settings を定義するには、次の手順を実行します。

1. **Queue Settings** ページを開きます。
2. **Scheduling**、**WRR Weight**、および **Bandwidth** フィールドを定義します。
3. **Apply Changes** をクリックします。**Queue Settings** ページおよびデバイスがアップデートされます。

CLI コマンドを使用した Queue Setting の割り当て

次の表に、**Queue Settings** ページでのフィールドの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
wrr-queue bandwidth *weight1 weight2 . weight_n*	WRR（Weighted Round Robin）weight を送信キューに割り当てます。
show qos interface [*interface-id***] [queuing]**	インタフェースの QoS データを表示します。

以下に、CLI コマンドの例を示します。

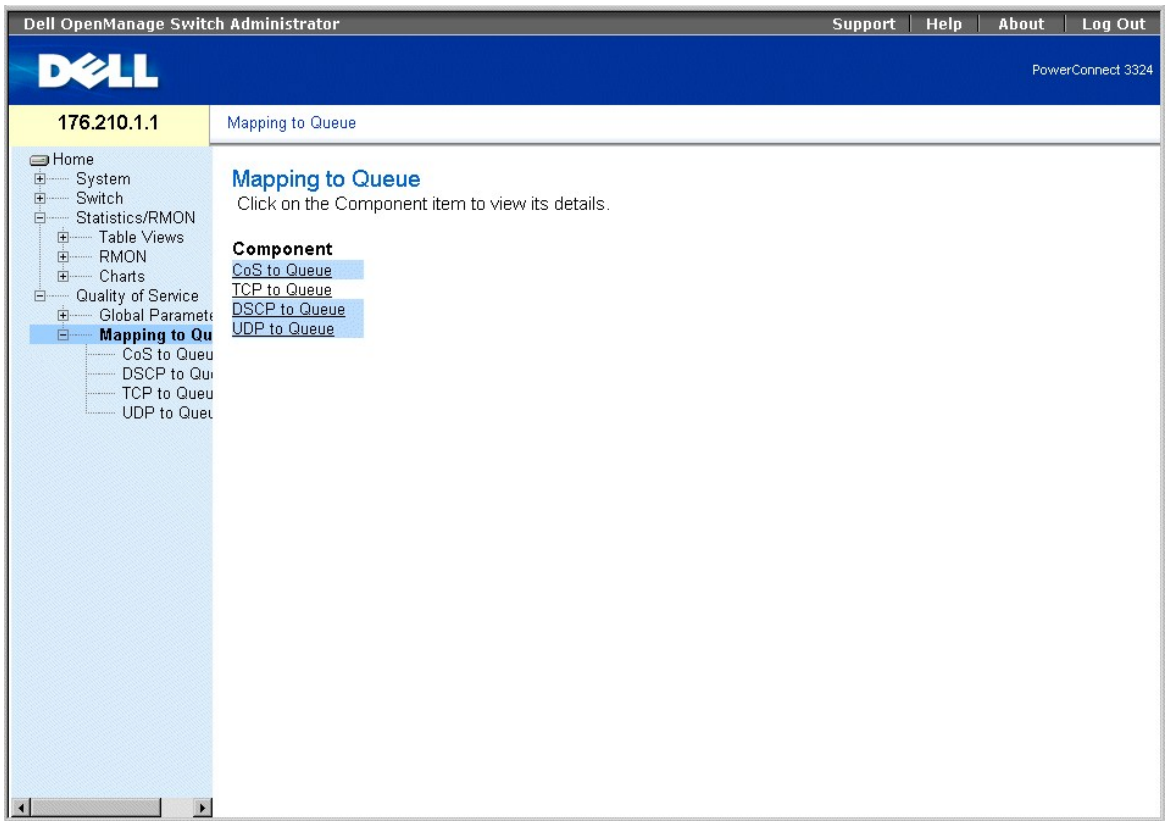
```
Console (config)# wrr-queue bandwidth 10 20 30 40

Console (config)# exit

Console # exit

Console> show qos interface ethernet 1/e3 queueing

Ethernet 1/e3

wrr bandwidth weights and EF priority:

qid-weights Ef - Priority

1 — 10 dis- N/A

2 — 20 dis- N/A
```

```
3 — 30 dis- N/A

4 — 1 dis- N/A

Cos-queue map:

cos-qid

0 - 2

1 - 1

2 - 1

3 - 2

4 - 2

5 - 3

6 - 3

7 - 3
```

キューへのマッピング

Mapping to Queue ページには、CoS および DSCP 値の QoS キューへのマッピングページだけでなく TCP および UDP ポートの QoS キューへのマッピングページへのリンクがあります。**Mapping to Queue** ページを開くには、次の手順を実行します。

1. **Quality of Service → Mapping to Queue** を選びます。**Mapping to Queue** ページが開きます。



Mapping to Queue ページ

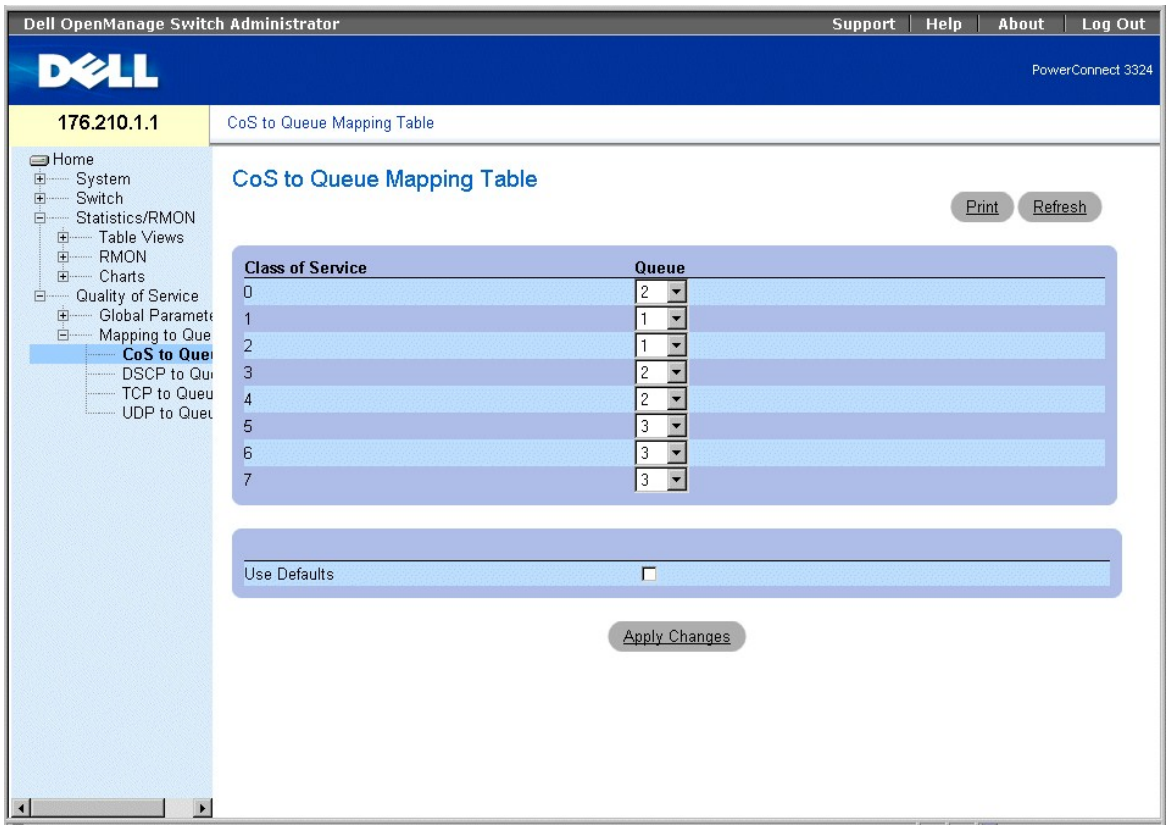
Mapping to Queue ページには、以下のトピックへのリンクがあります。

- CoS 値のキューへのマッピング
- TCP ポート値のキューへのマッピング
- DSCP 値のキューへのマッピング
- UDP ポート値のキューへのマッピング

CoS 値のキューへのマッピング

CoS to Queue ページを使用して、ネットワーク管理者は CoS 設定をトラフィックキューに分類することができます。**CoS to Queue Mapping Table** ページを開くには、次の手順を実行します。

- Tree View で、**Quality of Service** → **Mapping to Queue** → **CoS to Queue** とクリックします。**CoS to Queue Mapping Table** ページが開きます。



CoS to Queue Mapping Table ページ

CoS to Queue Mapping Table ページには、以下のフィールドが含まれています。

- **Class of Service** — CoS 優先度タグ値を指定します。0 が最低値で、7 が最高値です。
- **Queue** — CoS 優先度がマップされるトラフィック転送キューを示します。4 つのトラフィック優先度キューに対応しています。

メモ: スタッキング構成では、Queue 4 は転送スタッキングトラフィックに使用されます。そのため、Queue 4 にトラフィックを追加すると、スタック制御を妨害する可能性があります。

- **Use Defaults** — CoS 値の転送キューへのマッピングにデバイスのデフォルトを使用します。

CoS 値をキューにマッピングするには、次の手順を実行します。

1. **CoS to Queue** ページを開きます。
2. CoS エントリを選びます。
3. **Queue** フィールドで、キュー番号を定義します。
4. **Apply Changes** をクリックします。CoS 値はキューにマップされ、デバイスがアップデートされます。

CLI コマンドを使用した CoS 値のキューへの割り当て

次の表に、**Mapping CoS Values to Queues Table** ページでのフィールドの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
wrr-queue cos-map *queue-id* **cos1.cosn**	割り当てられた CoS 値を送信キューにマップします。

以下に、CLI コマンドの例を示します。

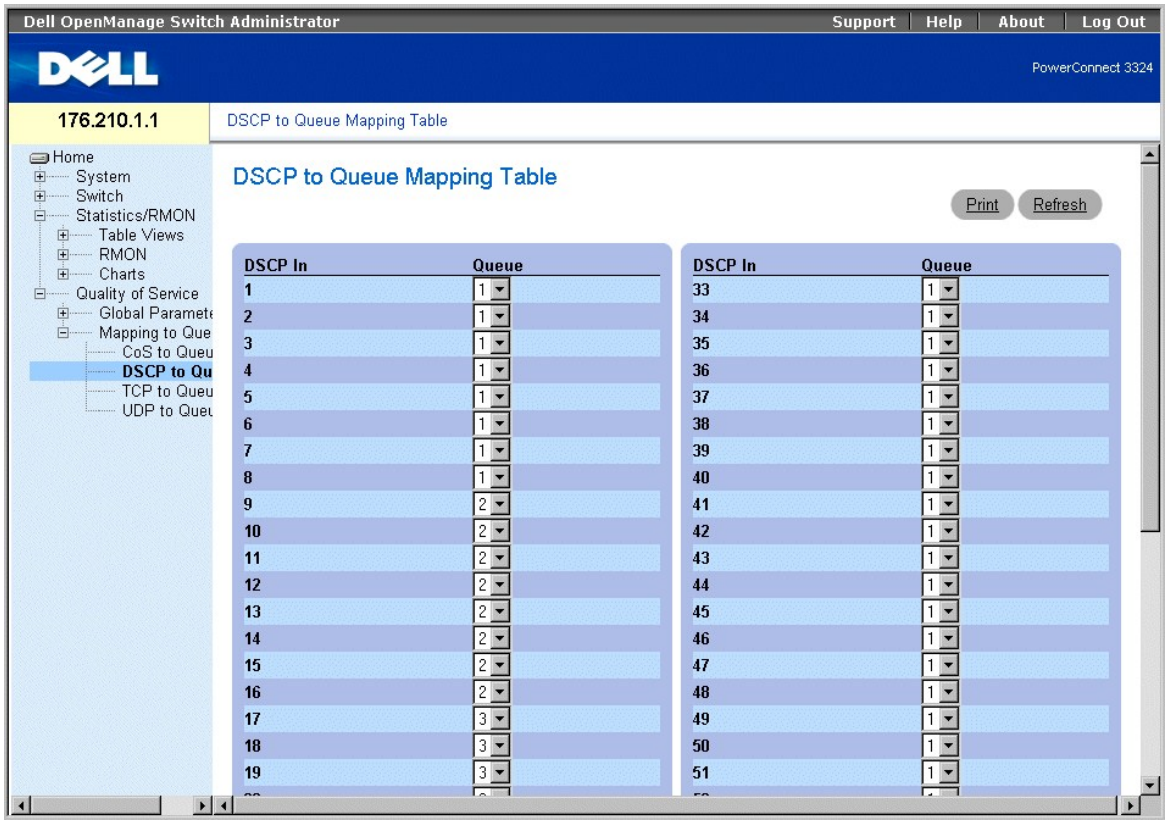
```
Console (config)# wrr queue cos-map 4 7
```

DSCP 値のキューへのマッピング

DSCP Mapping ページを使用して、ネットワーク管理者は特定の DSCP フィールドごとに割り当てられた出力キューを決定することができます。**DSCP Mapping** ページを開くには、次の手順を実行します。

メモ: DSCP のデフォルトのキュー設定については、「DSCP to Queue Mapping Table のデフォルト値」を参照してください。

- Tree View で、**Quality of Service** → **Global Parameters** → **Global Settings** → **DSCP Mapping** とクリックします。**DSCP to Queue Mapping Table** ページが開きます。



DSCP to Queue Mapping Table ページ

DSCP のデフォルトのキュー設定のリストには、以下のフィールドが含まれています。

メモ: スタッキング構成では、Queue 4 は転送スタッキングトラフィックに使用されます。そのため、Queue 4 にトラフィックを追加すると、スタック制御を妨害する可能性があります。

- **DSCP In** — 受信パケット内の DSCP フィールドの値を示します。
- **Queue** — 特定の DSCP 値のパケットが割り当てられているキューを示します。
  値は 1 ～ 4 で、1 が最低値で 4 が最高値です。

DSCP 値をマッピングして優先度キューを割り当てるには、次の手順を実行します。

1. **DSCP to Queue Mapping Table** ページを開きます。
2. **DSCP In** コラムで、値を選択します。
3. **Queue** フィールドを定義します。
4. **Apply Changes** をクリックします。DSCP は上書きされず、値は転送キューに割り当てられます。

CLI コマンドを使用した DSCP 値の割り当て

次の表に、**DSCP to Queue Mapping Table** ページでのフィールドの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
qos map dscp-queue *dscp-list to queue-id*	DSCP をキューマッピングに変更します。

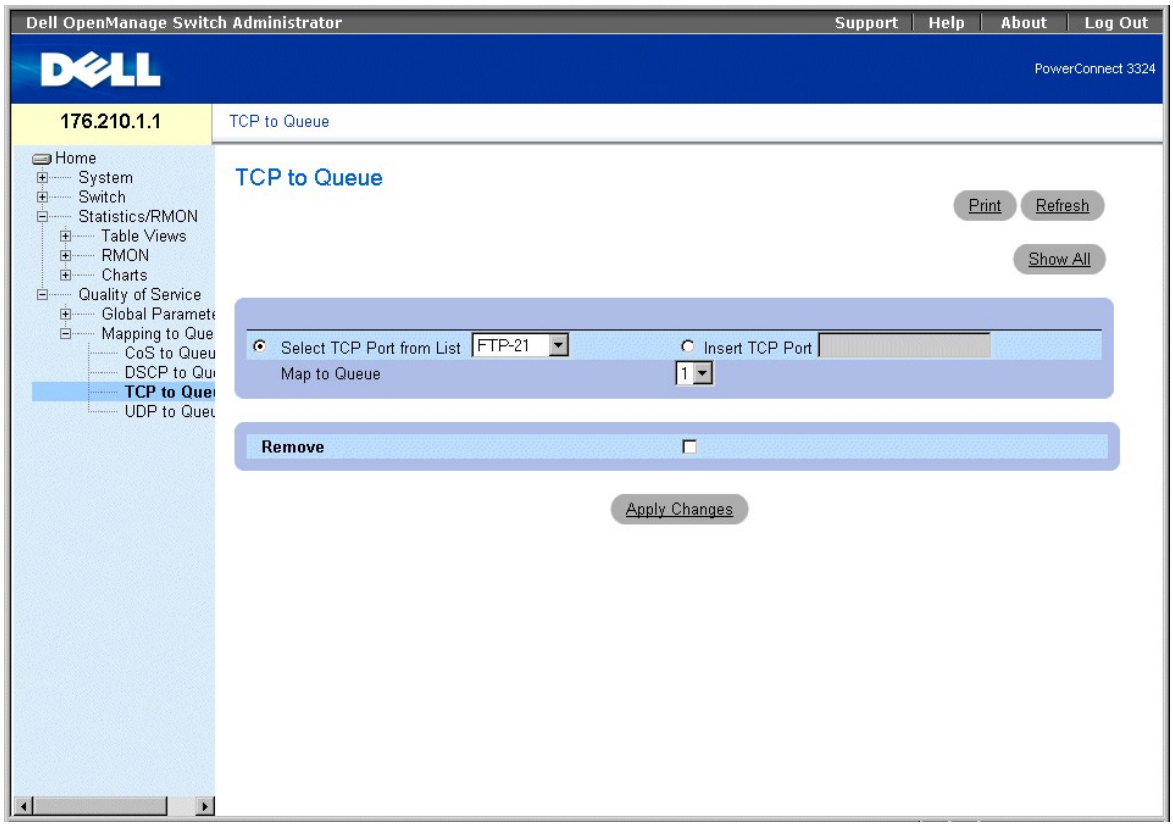
以下に、CLI コマンドの例を示します。

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

TCP ポート値のキューへのマッピング

TCP to Queue ページを使用して、ネットワーク管理者は特定の TCP の目的ポートトラフィックをキューに分類できます。**TCP to Queue** ページを開くには、次の手順を実行します。

- Tree View で、**Quality of Service** → **Mapping to Queue** → **TCP to Queue** とクリックします。**TCP to Queue** ページが開きます。



TCP to Queue ページ

TCP to Queue ページには、以下の情報が含まれています。

- **Select TCP Port from List** — 定義済みの共通して使用されている TCP ポートドロップダウンリストを提供します。
- **Insert TCP Port** — 新しい TCP ポートの定義を有効にします。
- **Map to Queue** — TCP ポートが割り当てられているトラフィックキューを示します。

メモ: スタッキング構成では、Queue 4 は転送スタッキングトラフィックに使用されます。そのため、Queue 4 にトラフィックを追加すると、スタック制御を妨害する可能性があります。

- **Remove** — TCP ポートマッピングを削除します。
  - **Checked** — 特定の TCP ポートマッピングを削除します。
  - **Unchecked** — TCP ポートマッピングを保持します。

TCP ポートをトラフィックキューへ割り当てるには、次の手順を実行します。

1. **TCP to Queue** ページを開きます。
2. **TCP Port List** で、ポートを選びます。

   または

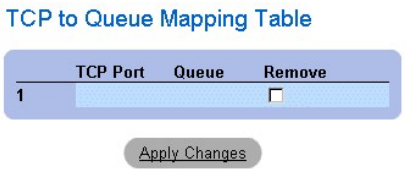
   Insert TCP Port チェックボックスにチェックマークを付けます。**New TCP Port** フィールドが有効になります。新しい TCP ポートを定義します。
3. **Map to Queue** ドロップダウンリストで、キュー番号を選びます。
4. **Apply Changes** をクリックします。TCP ポートに転送キューが割り当てられます。

TCP ポートをトラフィックキュー設定に変更するには、次の手順を実行します。

1. **TCP to Queue** ページを開きます。
2. **TCP Port List** ドロップダウンリストで、ポートを選びます。**Map to Queue** ドロップダウンリストに、ポートを割り当てられたキューが表示されます。
3. **Map to Queue** ドロップダウンリストで、新しいトラフィックキューを選びます。
4. **Apply Changes** をクリックします。TCP ポートは、異なるトラフィックキューに再割り当てされます。

TCP to Queue Mapping Table を表示するには、次の手順を実行します。

1. **TCP to Queue** ページを開きます。
2. **Show All** をクリックします。**TCP to Queue Mapping Table** ページが開きます。



TCP to Queue Mapping Table

TCP to Queue Mapping Table から TCP ポートマッピングを削除するには、次の手順を実行します。

1. **TCP to Queue** ページを開きます。
2. **Show All** をクリックします。**TCP to Queue Mapping Table** ページが開きます。
3. **TCP Port List** ドロップダウンリストで、ポートを選びます。**Map to Queue** ドロップダウンリストに、ポートを割り当てられたキューが表示されます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。TCP ポートがトラフィックキューから削除されます。

CLI コマンドを使用した TCP ポートのキューへの割り当て

次の表に、**TCP to Queue** ページでのフィールドの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
qos map tcp-port-queue *port1.port8 to queue-id*	TCP ポートをキューに変更します。
show qos map tcp-port-queue	TCP ポートをキューに表示します。
no qos map tcp-port-queue	TCP ポートをキューから削除します。

以下に、CLI コマンドの例を示します。

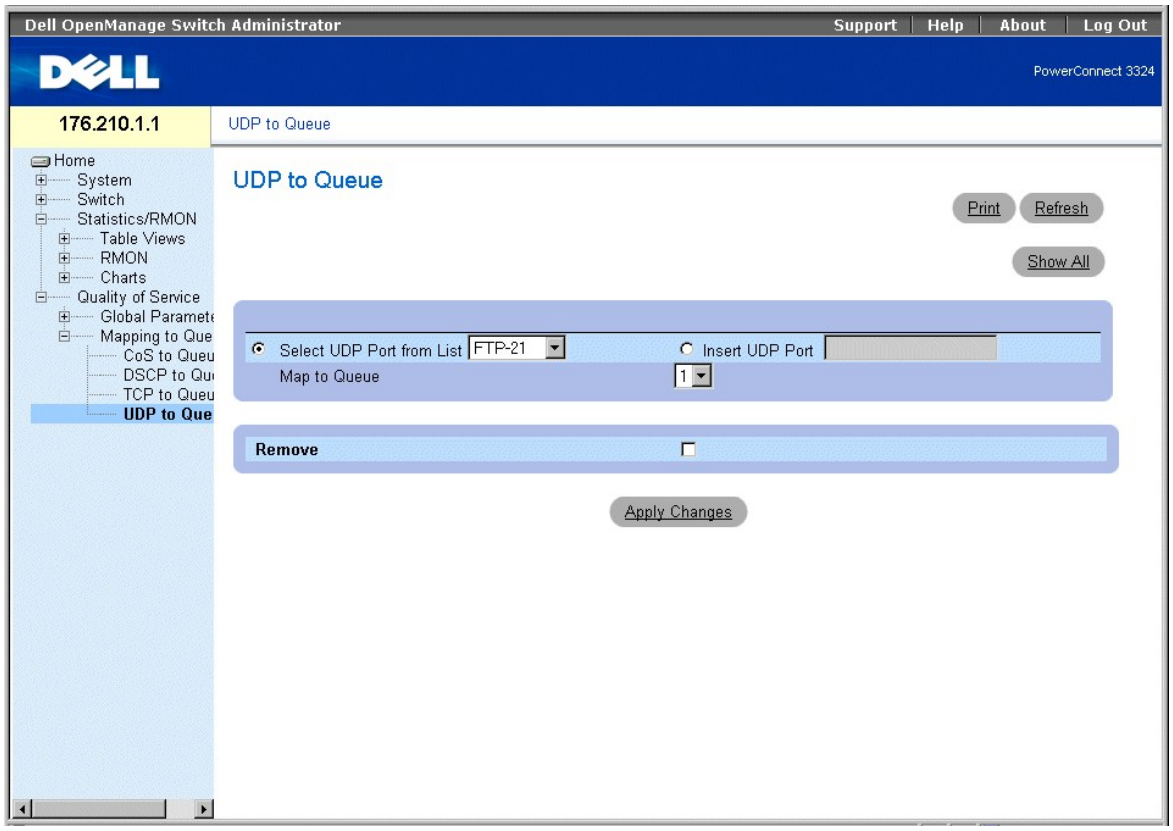
```
Console (config)# qos map tcp-port-queue 6001 to 2

Console (config)# exit

Console # exit
```

```
Console (config)# show qos map tcp-port-queue

Tcp port-queue map:

Port queue

----- ------

6000 1

6001 2

6002 3
```

UDP ポート値のキューへのマッピング

UDP to Queue ページを使用して、ネットワーク管理者は特定の UDP ポートトラフィックをキューに分類できます。**UDP to Queue** ページを開くには、次の手順を実行します。

- Tree View で、**Quality of Service** → **Mapping to Queue** → **UDP to Queue** とクリックします。**UDP to Queue** ページが開きます。



UDP to Queue ページ

UDP to Queue ページには、以下のフィールドが含まれています。

- **Select UDP Port from List** — 定義済みの共通して使用されている UDP ポートのドロップダウンリストを提供します。
- **Insert UDP Port** — 新しい UDP ポートを定義します。
- **Map to Queue** — UDP ポートが割り当てられているトラフィックキューを示します。

メモ: スタッキング構成では、Queue 4 は転送スタッキングトラフィックに使用されます。そのため、Queue 4 にトラフィックを追加すると、スタック制御を妨害する可能性があります。

- **Remove** — UDP ポートマッピングを削除します。
  - **Checked** — UDP ポートマッピングを削除します。
  - **Unchecked** — UDP ポートマッピングを保持します。

UDP ポートをトラフィックキューへ割り当てるには、次の手順を実行します。

1. **UDP to Queue** ページを開きます。
2. **UDP Port List** で、ポートを選びます。

   または

   Insert UDP Port チェックボックスにチェックマークを付けます。**New UDP Port** フィールドが有効になります。

   新しい UDP ポートを定義します。
3. **Map to Queue** ドロップダウンリストで、キュー番号を選びます。
4. **Apply Changes** をクリックします。UDP ポートに転送キューが割り当てられます。

UDP ポートをトラフィックキュー設定に変更するには、次の手順を実行します。

1. **UDP to Queue** ページを開きます。
2. **UDP Port List** ドロップダウンリストで、ポートマッピングを選びます。**Map to Queue** ドロップダウンリストに、ポートを割り当てられたキューが表示されます。
3. **Map to Queue** ドロップダウンリストで、新しいトラフィックキューを選びます。
4. **Apply Changes** をクリックします。UDP マッピングは、異なるトラフィックキューに再度割り当てされます。

UDP to Queue Mapping Table から UDP ポートマッピングを削除するには、次の手順を実行します。

1. **UDP to Queue** ページを開きます。
2. **UDP Port List** ドロップダウンリストで、ポートマッピングを選びます。**Map to Queue** ドロップダウンリストに、ポートを割り当てられたキューが表示されます。
3. **Remove** チェックボックスにチェックマークを付けます。
4. **Apply Changes** をクリックします。UDP ポートマッピングは、UDP to the Traffic Mapping Table から削除されます。

CLI コマンドを使用した UDP ポートのキューへの割り当て

次の表に、**UDP to Queue** ページでのフィールドの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
qos map udp-port-queue *port1.port8 to queue-id*	UDP ポートをキューに変更します。
show qos map udp-port-queue	UDP ポートをキューに表示します。
no qos map udp-port-queue	UDP ポートをキューから削除します。

以下に、CLI コマンドの例を示します。

```
Console (config)# qos map udp-port-queue 2000 80 to 2
```

```
Console (config)# show qos map udp-port-queue
```

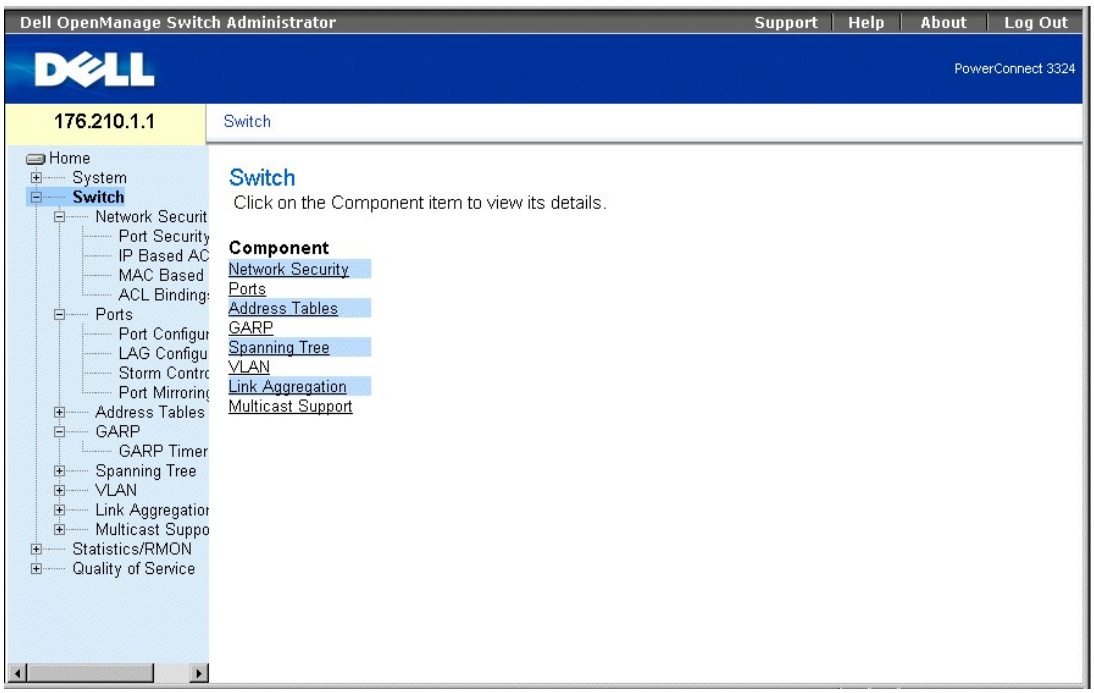
メモ、注意および警告

メモ、注意および警告

スイッチ情報の設定

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

この項では、ネットワークセキュリティ、ポート、アドレステーブル、GARP、VLAN、Spanning Tree、ポート集合、およびマルチキャストサポートに関するシステムの運用および一般的な事柄について説明します。



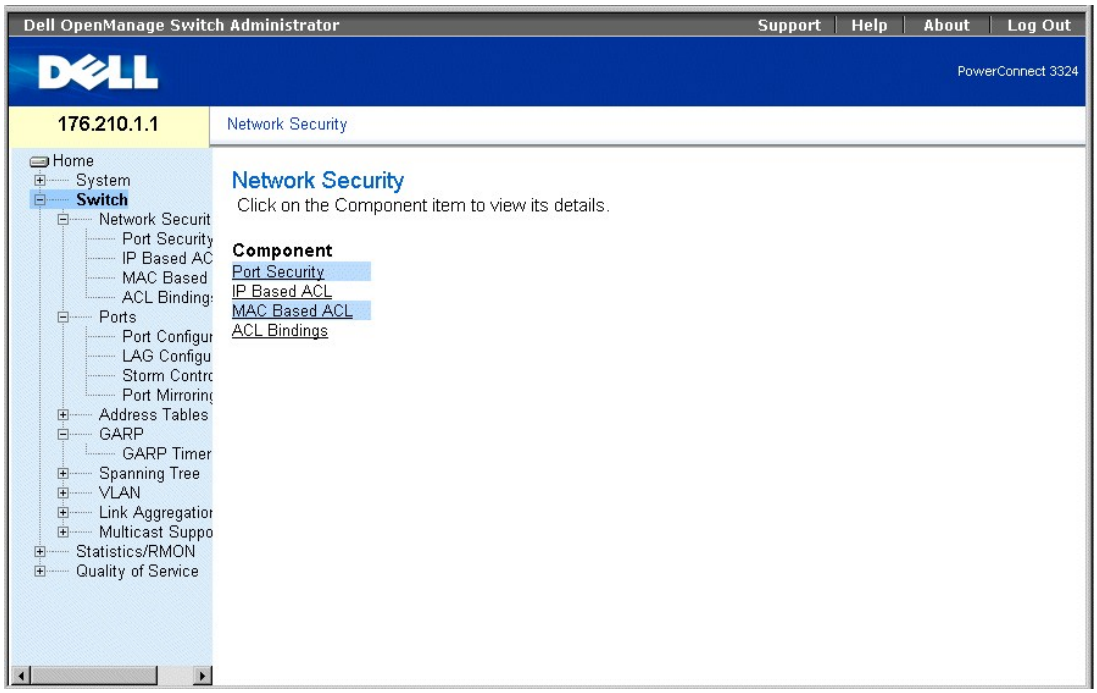
Switch ページ

ネットワークセキュリティの設定

Dell™ PowerConnect™ 3324/3348 を使用して、ネットワーク管理者は Access Control Lists および Locked Ports の両方を介してネットワークセキュリティを設定できます。

Network Security ページを開くには、次の手順を実行します。

1. Switch → **Network Security** と選びます。**Network Security** ページが開きます。



Network Security ページ

Network Security ページには、以下のトピックへのリンクがあります。

- ネットワークセキュリティの概要
- ポートセキュリティの設定
- IP ベースの ACL の定義
- MAC ベースの ACL の定義
- ACL のバインド

ネットワークセキュリティの概要

ACL (アクセス制御リスト) を使用して、ネットワーク管理者は特定の進入ポートに対する分類アクションとルールを定義できます。ACL には複数の分類ルールとアクションが含まれています。分類ルールとアクションは、ACE (Access Control Element) です。ACE は、トラフィックをフィルタして分類を決定します。パケットは、以下の ACE と一致します。

- Protocol
- Destination Port
- Source IP Address
- Destination IP Address
- Wild Card Masks
- Match DSCP
- Match IP-Precedence
- Source MAC Address

- Destination MAC Address
- VLAN ID

たとえば、ネットワーク管理者は、ポート番号 20 は TCP パケットを受信できるが、UDP パケットを受信するとそのパケットは破棄される、という ACL ルールを定義することができます。

1 つの ACL は、複数の ACE を含むことができます。ACL 内の ACE は、最初に一致するものに適用されます。ACE は、最初の ACE から順番に処理されます。パケットが ACE 分類に一致すると、ACE アクションが実行され、ACL 処理が停止します。一致するものが見つからない場合、デフォルトのアクションではパケットは破棄されます。複数の ACL が処理される場合、すべての ACL が処理されてからデフォルトのアクションが適用されます。デフォルトの破棄アクションは、Telnet、HTTP、SNMP などの管理トラフィックを含むすべての許可されているトラフィックをスイッチに転送します。

ネットワーク管理者は、2 つのタイプの ACL を定義できます。

- IP ACL — IP パケットにのみ適用します。すべての分類フィールドは IP パケットに関連します。
- MAC ACL — 非 IP を含むすべてのパケットに適用します。分類フィールドは、L2 フィールドにのみ基づきます。

アクティブな ACL で進入ポートに入るパケットは、以下のように処理されます。

- パケットは転送されます。
- パケットは破棄され、トラップが送信されます。
- パケットは破棄され、トラップが送信され、進入ポートが無効になります。

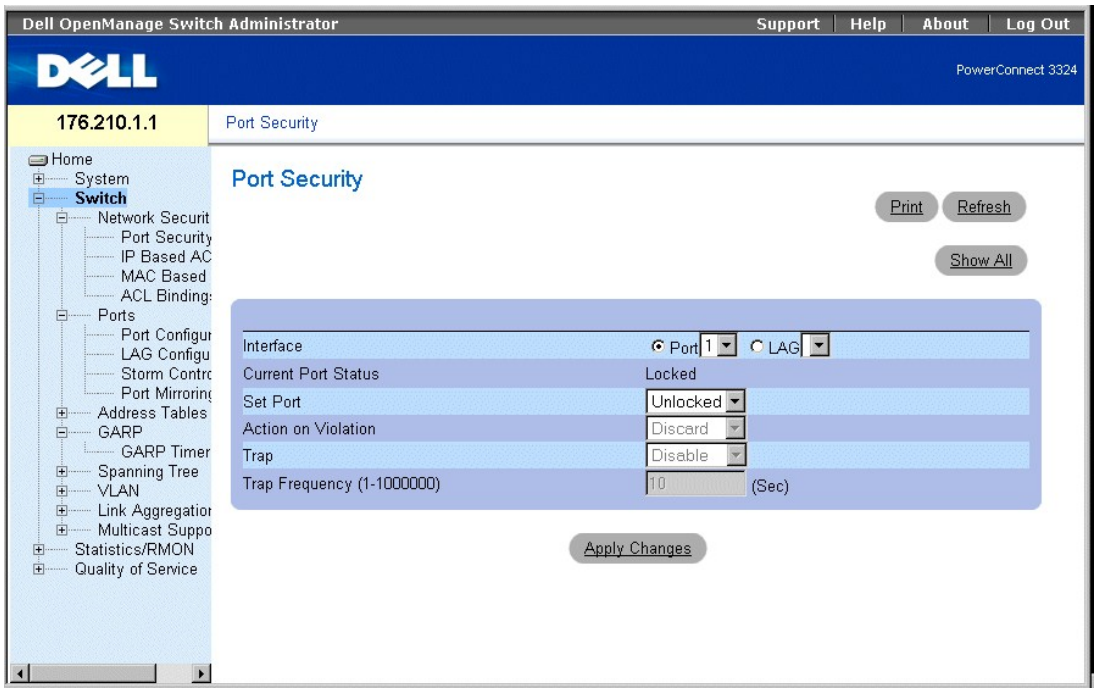
PowerConnect 3324/3348 は、最大で 128 の ACL をサポートします。PowerConnect 3324/3348 は、1 つの FE ポートに最大で 248 の ACE をサポートし、1 つの GE ポートに最大で 120 の ACE を定義できます。

ポートセキュリティの設定

ネットワークユーザーを、特定のポートまたは Locked Port で LAG に制限することができます。Locked Port は、特定の MAC アドレスを持つユーザーに制限されています。Locked Port は、静的 MAC アドレスでのみ有効にできます。また、Locked Port セキュリティオプションを使用して、Configuration ファイル内に MAC アドレスのリストを保存することができます。MAC アドレスリストは、デバイスのリセット後に復元できます。MAC アドレスは、動的または静的に学習されます。

Locked Port に着いたパケットは、転送されるか破棄され、あるいはパケットが破棄され、トラップが送信されて、進入ポートが無効になります。無効になったポートは、**Port Parameters** ページでアクティブにできます。「ポートパラメータの定義」を参照してください。**Port Security** ページを開くには、次の手順を実行します。

- **Switch** → **Network Security** → **Port Security** と選びます。**Port Security** ページが開きます。



Port Security ページ

Port Security ページには、以下のフィールドが含まれています。

- **Interface** — Locked Port が有効になっている選択されたインタフェースタイプを示します。
  - **Port** — 選択されたインタフェースのタイプがポートであることを示します。
  - **LAG** — 選択されたインタフェースのタイプがスタックメンバーであることを示します。
- **Current Port Status** — 現在のポートのステータスを示します。
- **Set Port** — ポートが Locked または Unlocked であることを示します。可能なフィールド値には、以下のものがあります。
  - **Unlocked** — ポートのロックを解除します。これはデフォルト値です。
  - **Locked** — ポートをロックします。
- **Action on Violation** — ロックされたポートに着いたパケットに適用されるアクションを示します。可能なフィールド値には、以下のものがあります。
  - **Forward** — 不明な送信元からのパケットを転送しますが、MAC アドレスは学習されません。
  - **Discard** — 学習されていない送信元からのパケットを破棄します。これはデフォルト値です。
  - **Shutdown** — 学習されていない送信元からのパケットを破棄し、ポートをロックします。ポートは、アクティブにするか、デバイスがリセットされるまでロックされたままです。
- **Trap** — トラップの送信を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — ロックされたポートでパケットが受信されると、トラップの送信を有効にします。
  - **Disable** — ロックされたポートでパケットが受信されると、トラップの送信を無効にします。これはデフォルト値です。
- **Trap Frequency (1-1000000)** — トラップの間隔を秒で示します。このフィールドはロックされたポートにのみ適用されます。デフォルト値は 10 秒です。

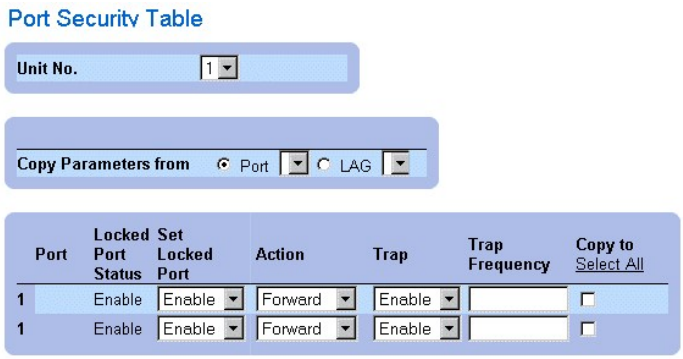
Locked Port を定義するには、次の手順を実行します。

1. **Port Security** ページを開きます。
2. インタフェースタイプと番号を選びます。

3. **Set Port**、**Action on Violation**、 および **Trap** フィールドを定義します。
4. **Apply Changes** をクリックします。ロックされたポートが **Port Security Table** に追加され、デバイスがアップデートされます。

Locked Port Table を表示するには、次の手順を実行します。

1. **Port Security** ページを開きます。
2. **Show All** をクリックします。**Port Security Table** ページが開きます。**Port Security Table** 内のフィールドは、**Port Security** ページのフィールドと同じです。 Locked Ports は **Port Security** ページだけでなく **Locked Ports Table**からも定義できます。



Port Security Table ページ

Port Security ページ で表示されるフィールドに加えて、**Port Security Table** ページには、以下のフィールドも含まれています。

- **Unit No.** — ポートのセキュリティ情報が表示されているユニット番号を示します。

CLI コマンドを使用した、Locked Port セキュリティの設定

次の表に、 Port Security ページ で表示される Locked Port の設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
shutdown	インタフェースを無効にします。
set interface active {ethernet *interface* **| port-channel** *port-channel-number***}**	ポートのセキュリティの理由でシャットダウンされたインタフェースをアクティブに戻します。
port security <*options***>** *trap frequency*	インタフェースでの新しいアドレスの学習をロックします。
show ports security	ポートロックの状態を表示します。

以下に、CLI コマンドの例を示します。

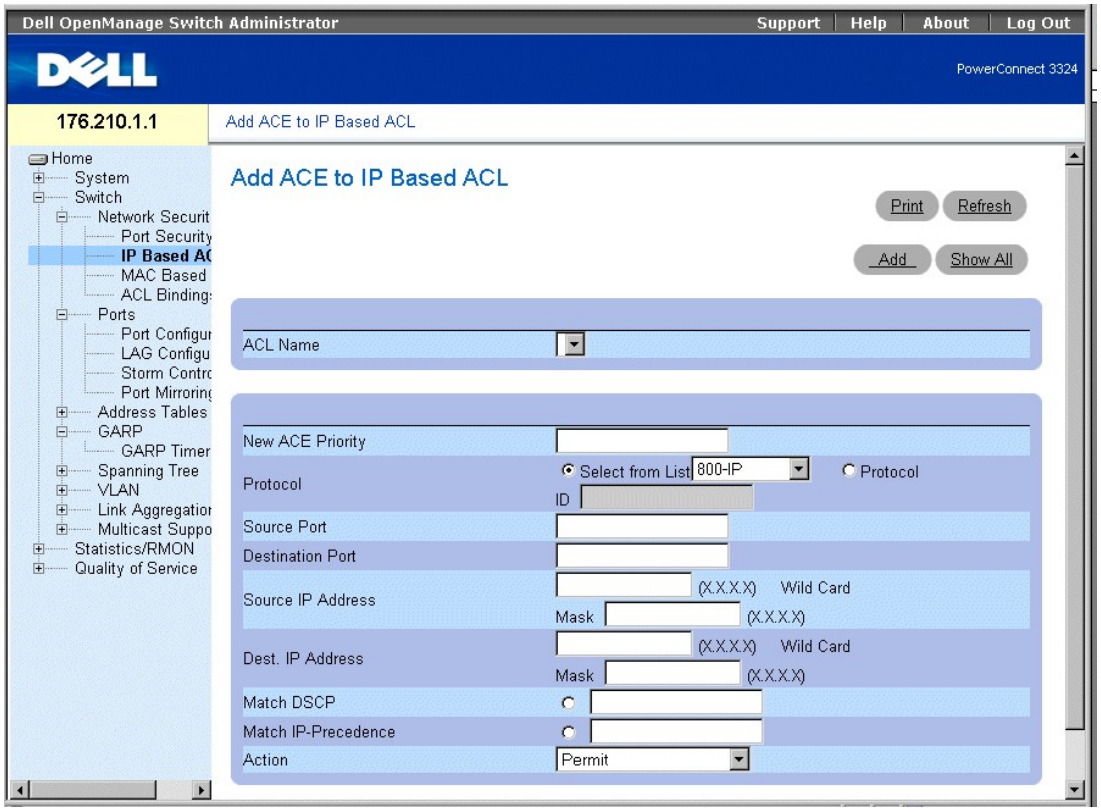
```
From 18.1.16 Console # show ports security

Port Action Trap Frequency Counter

-------------------------------------------
```

```
5/7 Discard Enable 100 88


7/8 Discard Disable
```

IP ベースの ACL の定義

Add ACE to IP Based ACL ページで、ネットワーク管理者は IP ベースの ACL および ACE (Access Control Entries) を定義することができます。ACE は、パケットを転送条件に一致させるフィルタとして動作します。**Add ACE to IP Based ACL** ページを開くには、次の手順を実行します。

- **Switch** → **Network Security** → **IP based ACL** と選びます。**Add IP Based ACL** ページが開きます。



Add ACE to IP Based ACL ページ

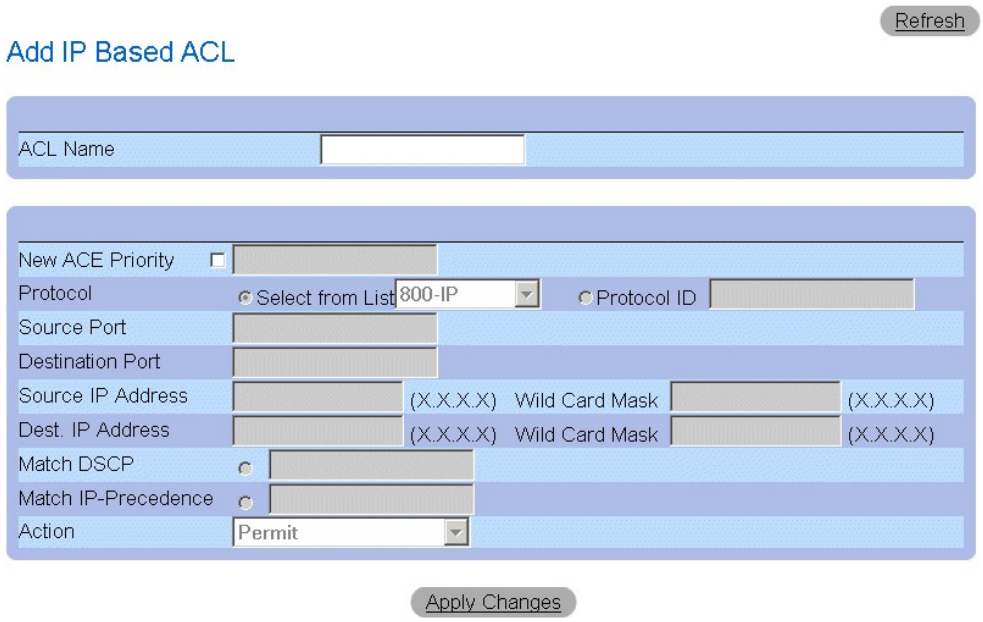
Add ACE to IP Based ACL ページには、以下のフィールドが含まれています。

- **ACL Name** — ユーザー定義の ACL リストがあります。
- **New ACE Priority** — ACE 優先度を定義します。ACE は、最初に一致したものをもとにチェックされます。ACE 優先度は、ACL リスト内の ACE 順序を定義します。
- **Protocol** — 特定のプロトコルに基づく ACE を作成できます。
- **Source Port** — 一致したパケットの送信元のポートを示します。Protocol リストで TCP または UDP が選択されている場合にのみ有効になります。
- **Destination Port** — 一致したパケットの送信先のポートを示します。
  Protocol リストで TCP または UDP が選択されている場合にのみ有効になります。
- **Source IP Address** — パケットの送信元の IP アドレスを ACE と一致させます。

- **Wild Card Mask** — 送信元の IP アドレスのワイルドカードマスクを示します。ワイルドカードは、すべて、または一部の送信元の IP アドレスのマスクに使用されます。ワイルドカードマスクは、どのビットが使われ、どのビットが無視されるかを指定します。255.255.255.255 のワイルドカードマスクは、どのビットも重要ではないことを示します。00.00.00.00 のワイルドカードは、すべてのビットが重要であることを示します。たとえば、送信元の IP アドレスが 149.36.184.198 で、ワイルドカードマスクが 255.36.184.00 の場合、IP アドレスの最初の 2 ビットは無視されますが、最後の 2 ビットは使われます。
- **Dest. IP Address** — パケットの送信先の IP アドレスをパケットの宛先 ACE と一致させます。
- **Wild Card Mask** — 送信先の IP アドレスのワイルドカードマスクを示します。ワイルドカードは、すべてまたは一部の送信先の IP アドレスのマスクに使用されます。ワイルドカードマスクは、どのビットが使われ、どのビットが無視されるかを指定します。255.255.255.255 のワイルドカードマスクは、どのビットも重要ではないことを示します。00.00.00.00 のワイルドカードは、すべてのビットが重要であることを示します。たとえば、送信先の IP アドレスが 149.36.184.198 で、ワイルドカードマスクが 255.36.184.00 の場合、IP アドレスの最初の 2 ビットは使われますが、最後の 2 ビットは無視されます。
- **Match DSCP** — パケットの DSCP 値を ACE と一致させます。DSCP 値または IP Precedence 値が、パケットを ACE に一致させるために使用されます。
- **Match IP-Precedence** — パケットの IP Precedence 値を ACE と一致させます。DSCP 値または IP Precedence 値が、パケットを ACE に一致させるために使用されます。
- **Action** — ACE 転送アクションを示します。可能なフィールド値には、以下のものがあります。
  - **Permit** — ACE 条件に合うパケットを転送します。
  - **Deny** — ACE 条件に合うパケットを破棄します。
  - **Deny and Disable Port** — ACE 条件に合うパケットを破棄し、パケットの送信先のポートを無効にします。ポートは Port Configuration からアクティブに戻すことができます。「ポートパラメータの定義」 を参照してください。

IP ベース の ACL を追加するには、次の手順を実行します。

1. **Add ACE to IP Based ACL** ページを開きます。
2. **Add** （追加）をクリックします。**Add IP Based ACL** ページが開きます。



Add IP Based ACL ページ

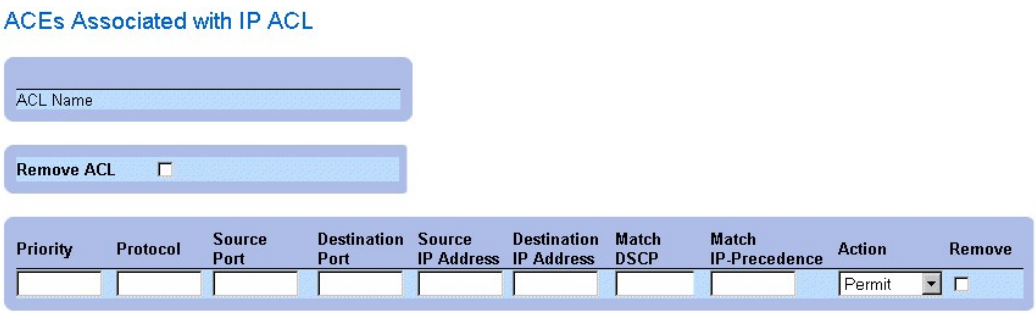
3. **ACL Name**、**New Ace Priority**、**Protocol**、**Source and Destination Port**、**Source and Destination IP Address**、**Match DSCP** または **Match IP Precedence**、および **Action** フィールドを定義します。
4. **Apply Changes** をクリックします。IP ベースの ACL が定義されます。新しい ACE 優先度を定義した場合、新しい ACL に追加されます。

ACE を IP ベース の ACL に割り当てるには、次の手順を実行します。

1. **Add ACE to IP Based ACL** ページを開きます。
2. **ACL Name** ドロップダウンリストで ACL を選びます。
3. **New ACE Priority** フィールドを定義します。
4. **ACE No.**、**Protocol**、**Source and Destination Port**、**Source and Destination IP Address**、**Match DSCP** または **Match IP Precedence**、および/または **Action** フィールドを定義します。
5. **Apply Changes** をクリックします。ACE が IP ベースの ACL に割り当てられます。

ACL に特定の ACE を表示するには、次の手順を実行します。

1. **Add ACE to IP Based ACL** ページを開きます。
2. **Show All** をクリックします。**ACEs Associated with IP ACL** ページが開きます。



ACEs Associated with IP ACL

IP ベース の ACE を変更するには、次の手順を実行します。

1. **Add ACE to IP Based ACL** ページを開きます。
2. Show All をクリックします。**ACEs Associated with IP ACL** ページが開きます。
3. **ACL Name**、**New Ace Priority**、**Protocol**、**Source and Destination Port**、**Source and Destination IP Address**、**Match DSCP** または **Match IP Precedence**、および **Action** フィールドを変更します。
4. **Apply Changes** をクリックします。IP ベースの ACE が変更され、デバイスがアップデートされます。

ACL を削除するには、次の手順を実行します。

1. **Add ACE to IP Based ACL** ページを開きます。
2. **Show All** をクリックします。**ACEs Associated with IP ACL** ページが開きます。
3. ACL を選びます。
4. **Remove ACL** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。IP ベースの ACL が削除され、デバイスがアップデートされます。

ACE を削除するには、次の手順を実行します。

1. **Add ACE to IP Based ACL** ページを開きます。
2. **Show All** をクリックします。**ACEs Associated with IP ACL**

ページが開きます。

3. ACE を選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。IP ベースの ACE が削除され、デバイスがアップデートされます。

CLI コマンドを使用した ACL への IP ベースの ACE の割り当て

次の表に、**Add ACE to IP Based ACL** ページで表示される ACL への IP ベースの ACE の割り当てに対応する CLI コマンドをまとめます。

CLI コマンド	説明
ip access-list *name*	IP アクセスリスト設定モードを起動します。
permit {any | *protocol*`}` **{any | {**`source source-wildcard`**}} {any | {**`destination destination-wildcard`**}} [dscp** `dscp number` **| ip-precedence** `ip-precedence`**]**	許可ステートメントで定義された条件に合う場合、トラフィックを許可します。
deny [disable-port] {any| *protocol*`}` **{any | {**`source source-wildcard`**}} {any | {**`destination destination-wildcard`**}} [dscp** `dscp number` **| ip-precedence** `ip-precedence`**]**	拒否ステートメントで定義された条件に合う場合、トラフィックを許可しません。

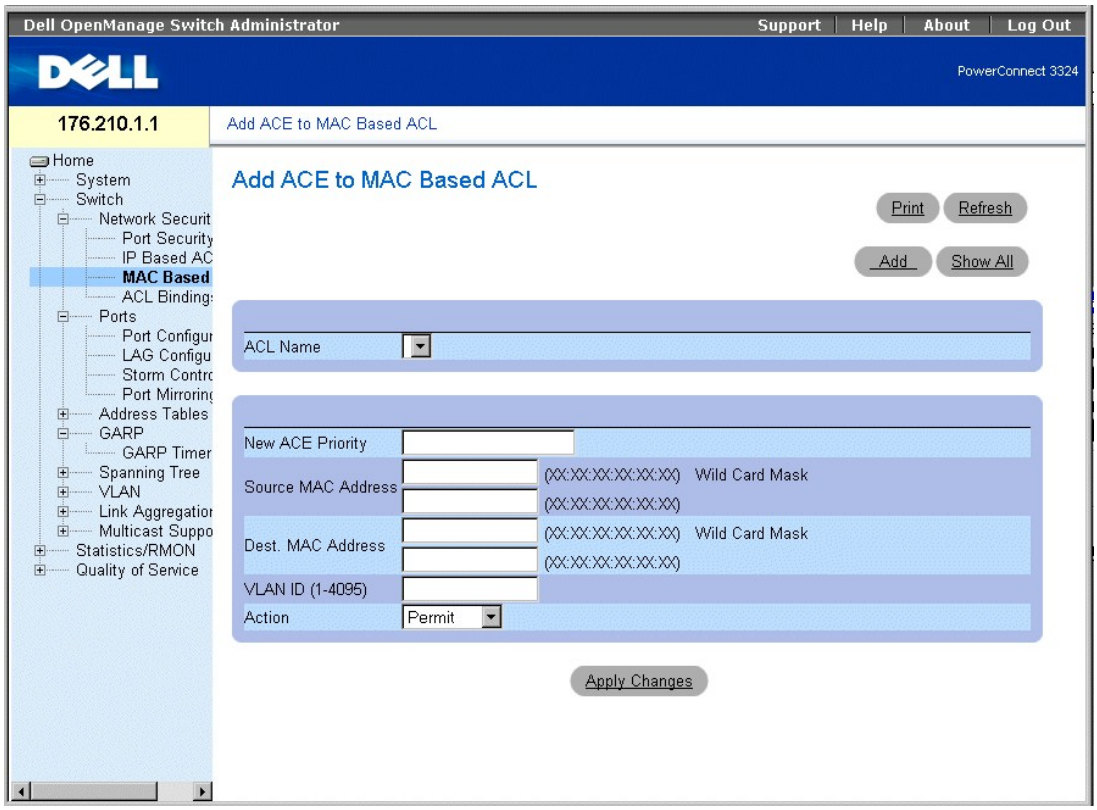
以下に、CLI コマンドの例を示します。

```
Permit 00:00:bo:11:11:11 0:0:0:0:0:0 any VLAN 4

deny 00:00:bo:11:11:11 0:0:0:0:0:0 any VLAN 4
```

MAC ベースの ACL の定義

Add ACE to MAC Based ACL ページを使用して、ネットワーク管理者は MAC ベースの ACE (**Access Control Entry**) および ACL (**Access Control Lists**) を定義することができます。ACE は、パケットを転送条件に一致させるフィルタとして動作します。**Add ACE to MAC Based ACL** ページを開くには、次の手順を実行します。

- **Switch → Network Security → MAC Based ACL** と選びます。
  Add ACE to MAC Based ACL ページが開きます。



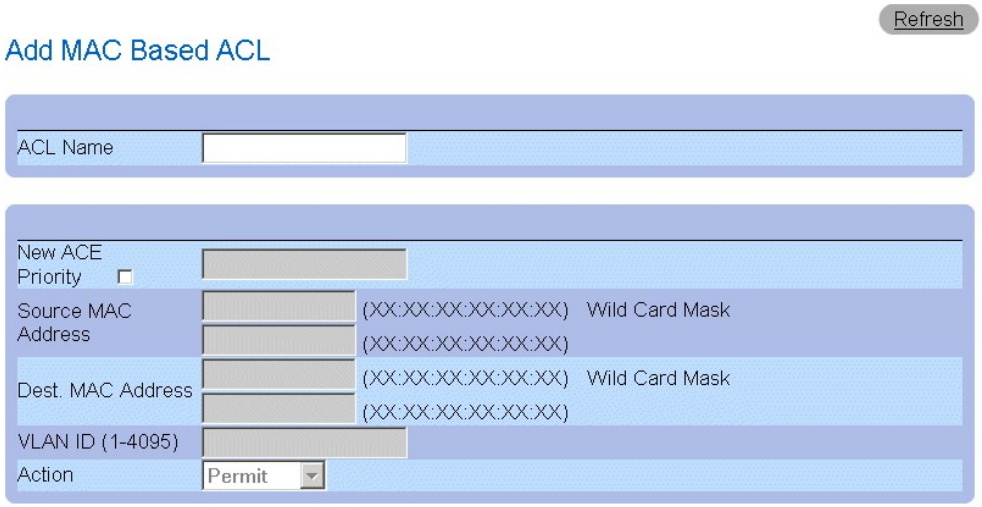
Add ACE to MAC Based ACL ページ

Add ACE to MAC Based ACL ページには、以下のフィールドが含まれています。

- **ACL Name** — ユーザー定義の ACL リストがあります。
- **New ACE Priority** — 新しい ACE の作成を有効にして、ACE 優先度を示します。
- **Source MAC Address** — パケットの送信元の MAC アドレスを ACE と一致させます。
- **Wild Card Mask** — 送信元の MAC アドレスのワイルドカードマスクを示します。ワイルドカードは、すべてまたは一部の送信元の MAC アドレスのマスクに利用されます。ワイルドカードマスクは、どのビットが使われ、どのビットが無視されるかを指定します。FF:FF:FF:FF:FF:FF のワイルドカードマスクは、どのビットも重要ではないことを示します。00.00.00.00.00.00 のワイルドカードは、すべてのビットが重要であることを示します。たとえば、送信元の MAC アドレスが E0:3B:4A:C2:CA:E2 で、ワイルドカードマスクが 00:3B:4A:C2:CA:FF の場合、MAC の最初の 2 ビットは使用されますが、最後の 2 ビットは無視されます。
- **Dest. MAC Address** — パケットの送信先の MAC アドレスを ACE と一致させます。
- **Wild Card Mask** — 送信先の MAC アドレスのワイルドカードマスクを示します。ワイルドカードは、すべてまたは一部の送信先の MAC アドレスのマスクに使用されます。ワイルドカードマスクは、どのビットが使われ、どのビットが無視されるかを指定します。FF:FF:FF:FF:FF:FF のワイルドカードマスクは、どのビットも重要ではないことを示します。00.00.00.00.00.00 のワイルドカードは、すべてのビットが重要であることを示します。たとえば、送信先の MAC アドレスが E0:3B:4A:C2:CA:E2 で、ワイルドカードマスクが 00:3B:4A:C2:CA:FF の場合、MAC の最初の 2 ビットは使用されますが、最後の 2 ビットは無視されます。
- **VLAN ID (1-4095)** — パケットの VLAN ID を ACE と一致させます。
- **Action** — ACE 転送アクションを示します。可能なフィールド値には、以下のものがあります。
  - **Permit** — ACE 条件に合うパケットを転送します。
  - **Deny** — ACE 条件に合うパケットを破棄します。
  - **Shutdown** — ACE 条件に合うパケットを破棄し、パケットの送信先のポートを無効にします。ポートは Port Configuration からアクティブに戻すことができます。「ポートパラメータの定義」 を参照してください。

MAC ベースの ACL を追加するには、次の手順を実行します。

1. **Add ACE to MAC Based ACL** ページを開きます。
2. **Add** （追加）をクリックします。**Add MAC Based ACL** ページが開きます。



ACEs Associated with Mac-Based ACLs

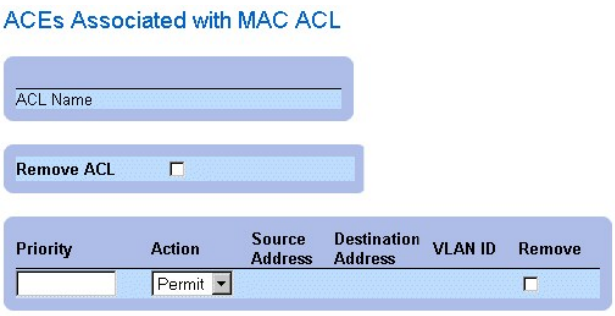
3. **ACL Name**、**Source and Destination Address**、および **Action** フィールドを定義します。
4. **Apply Changes** をクリックします。MAC ベースの ACL が定義され、デバイスがアップデートされます。

ACE を MAC ベースの ACL に割り当てるには、次の手順を実行します。

1. **Add ACE to MAC Based ACL** ページを開きます。
2. **ACL Name** ドロップダウンリストで ACL を選びます。
3. **New ACE Priority** フィールドを定義します。
4. **ACL Name**、**VLAN ID**、**Source and Destination Address**、および **Action** フィールドを定義します。
5. **Apply Changes** をクリックします。ACE が MAC ベースの ACL に割り当てられます。

ACL に特定の ACE を表示するには、次の手順を実行します。

1. **Add ACE to MAC Based ACL** ページを開きます。
2. **Show All** をクリックします。**ACEs Associated with MAC ACL** ページが開きます。



ACEs Associated with MAC ACL

MAC ベースの ACE を変更するには、次の手順を実行します。

1. **Add ACE to MAC Based ACL** ページを開きます。
2. **Show All** をクリックします。**ACEs Associated with MAC ACL** ページが開きます。
3. **ACL Name**、**Source and Destination Address**、および **Action** フィールドを修正します。
4. **Apply Changes** をクリックします。MAC ベースの ACE が変更され、デバイスがアップデートされます。

ACL を削除するには、次の手順を実行します。

1. **Add ACE to MAC Based ACL** ページを開きます。
2. **Show All** をクリックします。**ACEs Associated with MAC ACL** ページが開きます。
3. ACL を選びます。
4. **Remove ACL** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。MAC ベースの ACL が削除され、デバイスがアップデートされます。

ACE を削除するには、次の手順を実行します。

1. **Add ACE to MAC Based ACL** ページを開きます。
2. **Show All** をクリックします。**ACEs Associated with MAC ACL** ページが開きます。
3. ACE を選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。MAC ベースの ACE が削除され、デバイスがアップデートされます。

CLI コマンドを使用した MAC ベースの ACE の ACL への割り当て

以下に例を示します。ステーション A はポート 5 に接続され、ステーション B はポート 9 に接続されています。 ステーション A の MAC アドレスは、00-0B-CD-35-6A-00 （IP アドレスは、10.0.0.1 255.255.255.0） です。ステーション B の MAC アドレスは、00-06-6B-C7-A1-D8 （IP アドレスは、10.0.0.2 255.255.255.0） です。

ポート 5 に MAC ACL を導入して、すべてのトラフィックがステーション A からステーション B に移動できるようにするには、以下の CLI コマンドを入力します。

```
permit source mac address destination mac address
```

```
permit 00-0B-CD-35-6A-00 0.0.0.0.0.0 00-06-6B-C7-A1-D8 0.0.0.0.0.0
```

ACL に一致するすべてのトラフィックは通過され、その他のトラフィックはすべて許可されません。（deny all を ACL の後ろに追加すると、すべて許可されません。）

上記の例では、ステーション A は ICMP ECHO をステーション B に送信しようとしますが、MAC ACL で許可されていても、ICMP は失敗します。問題は、ステーション A が ICMP ECHO をステーション B に送信しようとしていますが、ARP テーブルにエントリがないことです。ステーション A は、ステーション A の送信元 MAC (00-0B-CD-35-6A-00) と送信先ブロードキャスト (FF.FF.FF.FF.FF.FF) のブロードキャストフレームである ARP 要求でステーション B の MAC アドレスを取得しようとします。このフレームは、ポート 5 で設定された MAC ACL と一致しないので、サイレントで破棄されます。

この問題を解決するには、ユーザーは permit のラインを追加して、ブロードキャストフレームを許可する必要があります。

```
permit 00-0B-CD-35-6A-00 0.0.0.0.0.0 FF.FF.FF.FF.FF.FF 0.0.0.0.0.0
```

メモ: ユーザーが MAC アドレス A から MAC アドレス B のトラフィックを許可しようとしても、ICMP などの単純なトラフィックでは別のブロードキャストが考慮されないため、実行できません。

次の表に、**Add ACE to MAC Based ACL** ページで表示される MAC ベース の ACE の ACL への割り当てに対応する CLI コマンドをまとめます。

CLI コマンド	説明
mac access-list *name*	Layer 2 MAC ACL を作成し、MAC アクセスリスト設定モードを起動します。
permit {any | {host *source source-wildcard***} any | {***destination destination-wildcard***}}[vlan** *vlan-id***]**	許可ステートメントで定義された条件に合う場合、トラフィックを許可します。
deny [disable-port] {any | {*source source- wildcard***} any | {***destination destination- wildcard***}}[vlan** *vlan-id***]**	許可ステートメントで定義された条件に合う場合、トラフィックを許可します。

以下に、CLI コマンドの例を示します。

```
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
```

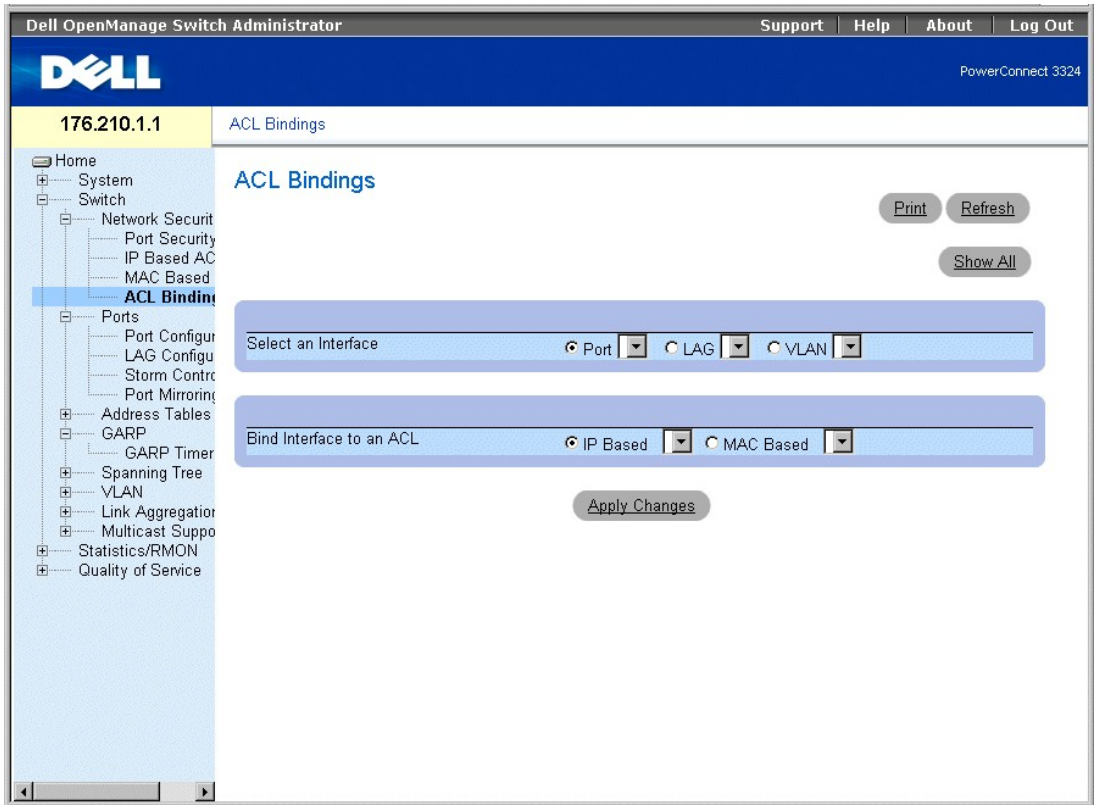
```
Console (config-mac-al)# deny 6.6.6.6.6.6 0.0.255.255.255.255
```

ACL のバインド

ACL Bindings ページを使用して、ネットワーク管理者は ACL リストをインタフェースに割り当てることができます。**ACL Bindings** ページを開くには、次の手順を実行します。

1. **Switch → Network Security → ACL Bindings** と選びます。
   ACL Bindings ページが開きます。

メモ: インタフェースに接続されていない限り、ACL は影響しません。



ACL Bindings ページ

ACL Bindings ページには、以下のフィールドが含まれています。

- **Select an Interface** — ACL が割り当てられているインタフェースとインタフェースタイプを示します。可能なフィールド値には、以下のものがあります。
  - **Port** — ACL が割り当てられているポート番号を示します。
  - **LAG** — ACL が割り当てられている LAG を示します。
  - **VLAN** — ACL が割り当てられている VLAN を示します。
- **Bind Interface to an ACL** — 受信パケットが一致する ACL 名を示します。パケットは、IP ベースの ACL か MAC アドレスベースの ACL のどちらかに一致できます。可能なフィールド値には、以下のものがあります。
  - **IP Based** — 受信パケットが IP ベースの ACL に一致することを示します。
  - **MAC Based** — 受信パケットが MAC ベースの ACL に一致することを示します。

ACL をインタフェースに割り当てるには、次の手順を実行します。

1. **ACL Bindings** ページを開きます。
2. **Select ACL** フィールドで、ACL タイプを選びます。
3. **Attach ACL to an Interface** フィールドで、ACL が割り当てられているインタフェースを定義します。
4. **Apply Changes** をクリックします。ACL がインタフェース割り当てられます。

CLI コマンドを使用した ACL メンバーシップの割り当て

次の表に、**ACL Bindings** ページで表示される ACL メンバーシップの割り当てに対応する CLI コマンドをまとめます。

CLI コマンド	説明
class-map *class-map-name* **[match-all | match-any]**	クラスマップを作成し、クラスマップ設定モードを起動します。
match access-group ACL *name*	トラフィックを分類するための一致条件を定義します。
show class-map [*class-map-name***]**	デバイスで定義されているすべてのクラスマップを表示します。

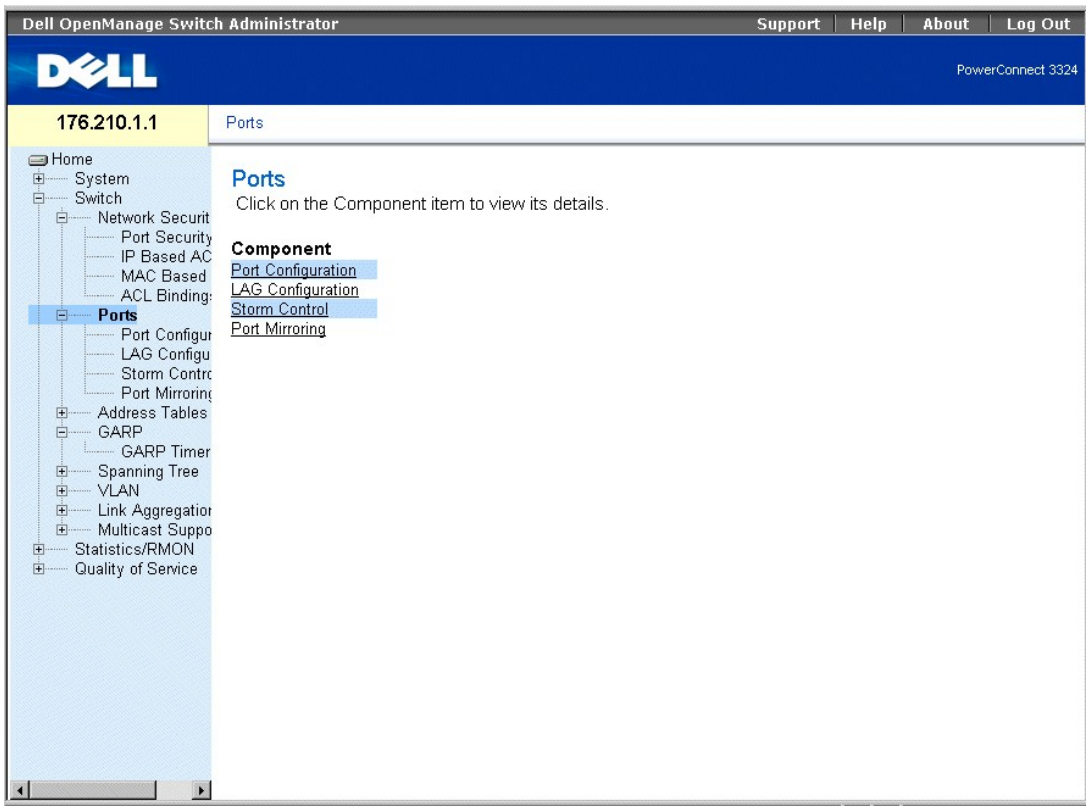
以下に、CLI コマンドの例を示します。

```
Console (config)# class-map class1 match-any

Console (config-cmap)# match access-group dell

Console (config-cmap)# exit

Console (config)# exit

Console # exit

Console> show class-map class1

Class Map match-any class1 (id4)
```

ポートの設定

この項では、ストーム制御やポートのミラリングなどの詳細機能を含む、ポートの機能とその設定方法を説明します。**Ports** ページを開くには、次の手順を実行します。

- **Switch** → **Ports** と選びます。**Ports** ページが開きます。



Ports ページ

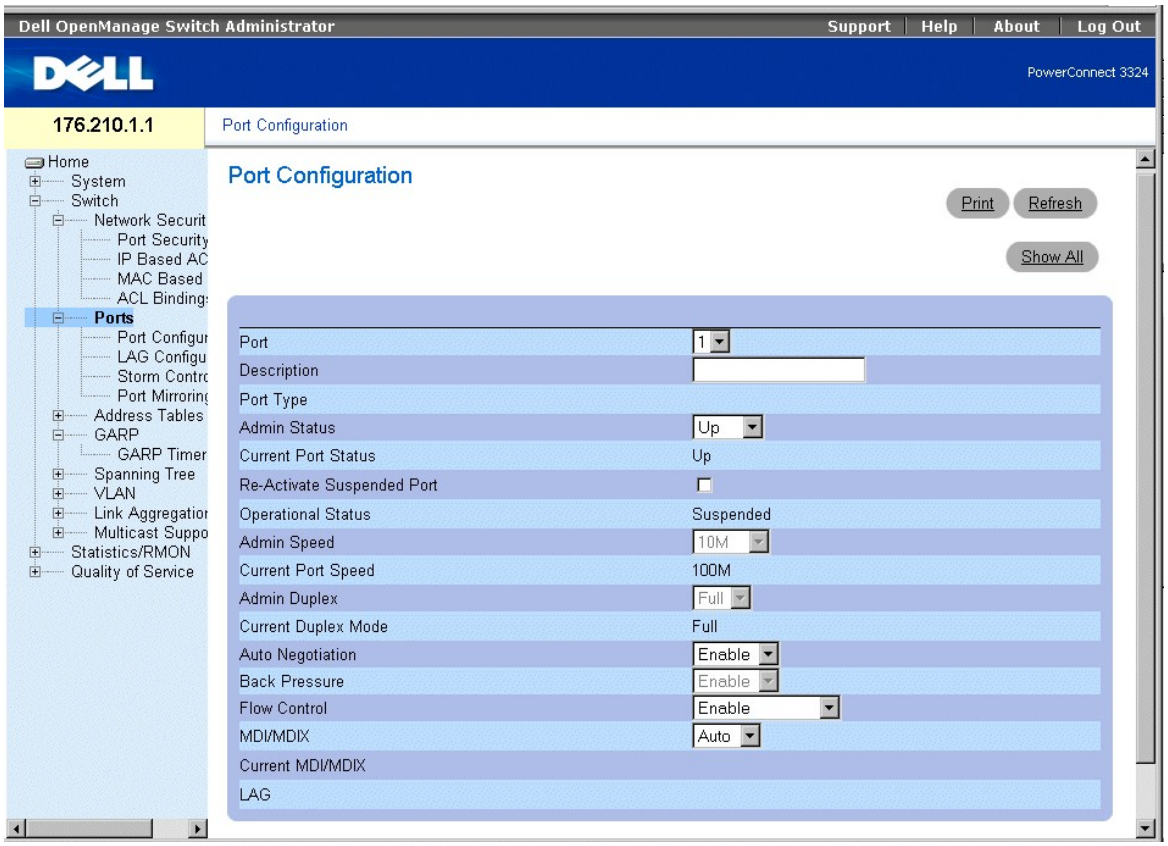
この項には以下のトピックがあります。

- ポートパラメータの定義
- LAG パラメータの定義
- ストーム制御の有効化
- ポートミラリングセッションの定義

ポートパラメータの定義

Port Configuration ページを使用して、ネットワーク管理者はポートパラメータの定義ができます。**Port Configuration** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Ports** → **Port Configuration** とクリックします。**Port Configuration** ページが開きます。



Port Configuration ページ

Port Configuration ページには、以下のフィールドが含まれています。

- **Port** — ポート番号を指定します。
- **Description** — Ethernet などのインタフェースの簡単な説明を提供します。
- **Port Type** — ポートタイプを示します。可能なフィールド値には、以下のものがあります。
  - Ethernet
  - Fast Ethernet
  - GE
- **Admin Status** — 選択されたポートトラフィックを制御します。デフォルトで、このパラメータは **Enable** に設定されています。可能なフィールド値には、以下のものがあります。
  - **Up** — ポートを介したトラフィック転送を有効にします。
  - **Down** — ポートを介したトラフィック転送を無効にします。
- **Current Port Status** — ポートの動作状態を示します。可能なフィールド値には、以下のものがあります。
  - **Up** — ポートが現在機能していることを示します。
  - **Down** — ポートが現在機能していないことを示します。
- **Re-Activate Suspended Port** — **Locked Port** または **ACL** セキュリティオプションでポートが無効になっている場合、ポートをアクティブに戻します。
- **Operational Status** — ポートの機能状態を示します。
- **Admin Speed** — ポートの速度を示します。この値は、ポートが無効になっている場合にのみ指定できます。可能なフィールド値には、以下のものがあります。

- 10M
- 100M
- 1000M

- **Current Port Speed** — 同期化されているポート速度を bps で指定します。可能なフィールド値には、以下のものがあります。
  - **10M**
  - **100M**
  - **1000M**
- **Admin Duplex** — 同期化されているポートの二重方式モードを bps で指定します。Admin Duplex が全二重に設定されている場合、Head-of-Line ブロッキングが選択されたポートで機能しています。可能なフィールド値には、以下のものがあります。
  - **Full** — インタフェースは、デバイスとクライアント間の同時双方向の通信をサポートします。これはデフォルト値です。
  - **Half** — インタフェースは、デバイスとクライアント間で一度に一方向のみの通信をサポートします。
- **Current Duplex Mode** — 同期化されているポートの二重方式モードを指定します。可能なフィールド値には、以下のものがあります。
  - **Full**
  - **Half**
- **Auto Negotiation** — デバイスで自動ネゴシエーションを有効にします。自動ネゴシエーションは、ポートがそれぞれのパートナーに送信速度、二重方式モード、フロー制御能力を通知できる 2 つのリンクパートナー間のプロトコルです。可能なフィールド値には、以下のものがあります。
  - **Enable** — ポートで自動ネゴシエーションを有効にします。
  - **Disable** — ポートで自動ネゴシエーションを無効にします。
    これはデフォルト値です。
  - **Current Auto Negotiation** — 自動ネゴシエーションの動作状態を示します。
- **Back Pressure** — デバイスで Back Pressure モードを有効にします。Back Pressure モードは、ポートのメッセージ受信を無効にするために半二重モードで使用されます。Back Pressure が有効な場合、Head-of-Line ブロッキングは有効に設定されていても動作しません。
- 可能なフィールド値には、以下のものがあります。
  - **Enable** — ポートで Back Pressure を有効にします。
  - **Disable** — ポートで Back Pressure を無効にします。これはデフォルト値です。
  - **Current Back Pressure** — Back Pressure の動作状態を示します。
- **Flow Control** — ポートで Flow Control が有効になっているかを示します。デバイスが二重方式モードの場合、Flow Control は有効になっています。また、Flow Control が有効になっている際は、Head-of-Line は選択されたポートで無効になっています。Flow Control が有効になっている際は、Head-of-Line ブロッキングは有効に設定されていても動作しません。可能なフィールド値には、以下のものがあります。
  - **Enable** — デバイスで Flow Control が有効になっていることを示します。
  - **Disable** — デバイスで Flow Control が無効になっていることを示します。これはデフォルト値です。
  - **Current Flow Control** — Flow Control の動作状態を示します。
  - **Auto-negotiation** — ポートで Flow Control の自動ネゴシエーションを有効にします。
  - **Tx Only** — 出口ポートの自動ネゴシエーションを有効にします。
  - **Rx Only** — 進入ポートの自動ネゴシエーションを有効にします。
- **MDI/MDIX** — デバイスは、クロスケーブルと非クロスケーブルを識別できます。1 つのハブおよびスイッチは、意図的にエンドステーションの配線と逆に配線されていますので、ハブまたはスイッチがエンドステーションに接続されている場合、ストレートスルーの Ethernet ケーブルが使用でき、ペアが正常に一致します。2 つのハブ / スイッチが相互接続されている場合、または 2 つのエンドステーションが相互接続されている場合、クロスオーバケーブルを使用して正しいペアが接続されるようにします。標準のケーブル配線には、以下のものがあります。
  - ハブおよびスイッチ用の MDIX (Media Dependent Interface with Crossover)
  - エンドステーション用の MDI (Media Dependent Interface)

メモ: 自動ネゴシエーションが無効な場合、自動 MDIX は FE ポートで動作しません。

以下の表では、ポートの設定に必要なパラメータコンビネーション設定を示します。これらの設定で、設定機能を確実に維持することができます。

	自動ネゴシエーション	
	有効	無効
Auto	適	不適
MDI	適	適
MDIX	適	適

- **Current MDI/MDIX** — Indicates the MDIX の動作状態を示します。可能なフィールド値には、以下のものがあります。
  - **MDI**
  - **MDIX**
  - **Auto** — 値は自動的に設定されることを示します。
- **LAG** — ポートが LAG の一部であるかどうかを指定します。

Port Parameters を定義するには、次の手順を実行します。

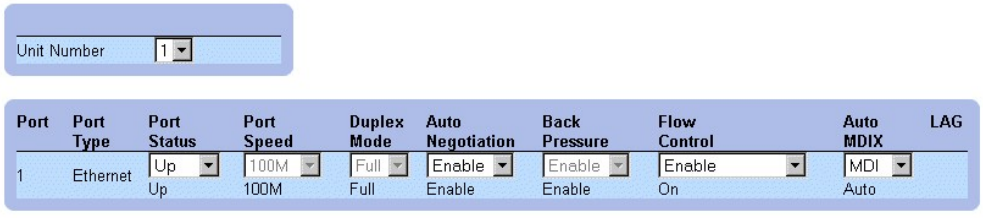
1. **Port Configuration** ページを開きます。
2. **Port** フィールドで、ポートを選びます。
3. **Description**、 **Admin Status**、**Admin Speed**、**Admin Duplex**、**Auto Negotiation**、**Back Pressure**、**Admin Auto MDIX**、および/または**Admin Flow Control** フィールドを定義します。
4. **Apply Changes** をクリックします。ポートパラメータがデバイスに保存されます。

ポートパラメータを変更するには、次の手順を実行します。

1. **Port Configuration** ページを開きます。
2. **Port** フィールドで、ポートを選びます。
3. **Description**、 **Admin Status**、**Admin Speed**、**Admin Duplex**、**Auto Negotiation**、**Back Pressure**、**Admin Auto MDIX**、および/または**Admin Flow Control** フィールドを変更します。
4. **Apply Changes** をクリックします。ポートパラメータがデバイスに保存されます。

Port Configuration Table を表示するには、次の手順を実行します。

1. **Port Configuration** ページを開きます。
2. **Show All** をクリックします。**Port Configuration Table** が開きます。



Ports Configuration Table

Port Configuration ページのフィールドに加えて、**Port Configuration Table** には以下のフィールドも表示されます。

- **Unit Number** — ポート情報が表示されているスタッキングユニット

番号を表示します。

CLI コマンドを使用したポート設定

以下の例は、ポートを MDIX または MDI モードに設定する方法について説明しています。ポートを MDIX モードに設定するには、システムプロンプトで以下を入力します。

```
console(config-if)# mdix on
```

以下のメッセージが表示されます。

```
console # show inter config ethernet 1/e1

Flow Admin Back Mdix
Port Type Duplex Speed Neg Control State Pressure Mode

.....................................................

1/e1 100M-Copper Enabled Off Up Disabled On
```

ポートを MDI モードに設定するには、システムプロンプトで以下を入力します。

```
console(config)# inter eth 1/e1

console(config-if)# no mdix
```

以下のメッセージが表示されます。

```
console # show inter config ethernet 1/e1

Flow Admin Back Mdix
Port Type Duplex Speed Neg Control State Pressure Mode

.....................................................

1/e1 100M-Copper Enabled Off Up Disabled Off
```

次の表に、**Port Configuration** ページで表示されるポートの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明

interface ethernet *interface*	Ethernet タイプのインタフェースを設定するインタフェース設定モードを起動します。
description *string*	インタフェース設定に説明を追加します。
shutdown	現在設定されているコンテキストの一部であるインタフェースを無効にします。
set interface active {ethernet *interface* **| port-channel** *port-channel-number***}**	セキュリティの理由でシャットダウンされたインタフェースをアクティブに戻します。
speed {10 | 100 | 1000}	自動ネゴシエーションを使用していない場合、特定の Ethernet インタフェースの速度を設定します。
duplex {half | full}	自動ネゴシエーションを使用していない場合、特定の Ethernet インタフェースの全二重 / 半二重動作を設定します。
negotiation	特定のインタフェースの速度と二重方式パラメータに対する自動ネゴシエーション動作を有効にします。
back-pressure	特定のインタフェースで Back-Pressure を有効にします。
flowcontrol {auto | on | off | rx | tx}	特定のインタフェースの Flow Control を設定します。
mdix {on | auto}	特定のインタフェースまたはポートチャネルの自動クロスオーバを有効にします。
show interfaces configuration [ethernet *interface* **| port-channel** *port-channel-number***]**	すべての設定インタフェースの設定を表示します。
show interfaces status [ethernet *interface* **| port-channel** *port-channel-number***]**	すべての設定インタフェースのステータスを表示します。
show interfaces description [ethernet interface | port-channel *port-channel-number***]**	すべての設定インタフェースの説明を表示します。

以下に、CLI コマンドの例を示します。

```
Console (config)# interface ethernet 1/e5

Console (config-if)#

Console (config-if)# description RD SW#3

Console (config-if)# shutdown

Console (config-if)# no shutdown

Console (config-if)# speed 100

Console (config-if)# duplex full

Console (config-if)# negotiation

Console (config-if)# back-pressure

Console (config-if)# flowcontrol on
```

```
Console (config-if)# mdix auto

Console (config-if)# exit

Console (config)# exit

Console# show interfaces configuration

Port Type Duplex Speed Neg Flow Back MDIX Admin

Cont Pres Mode State

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

1/e1 1g-combo-c Full 1000 Auto On Enable Auto Up

2/e1 100-copper Full 1000 Off Off Disable off Up

2/e2 1g-Fiber Full 1000 Off Off Disable on Up


Neg :Negotiation

Flow Cont:Flow Control

Back Pres:Back Pressure

Console# show interfaces status


Port Port Duplex Speed Neg Flow Back MDI Link

Cont Pres Mode State

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

2/e1 100-copper Full 1000 off Off Disable Off Down*
```

```
Legend

Neg :Negotiation

Flow Cont:Flow Control

Back Pres:Back Pressure

*: The interface was suspended by the system.

Router# show interfaces description



Port Description

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

1/e1 Port that should be used for management only

2/e1

2/e2



Port Channel Description

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

1 dell

2 projects
```

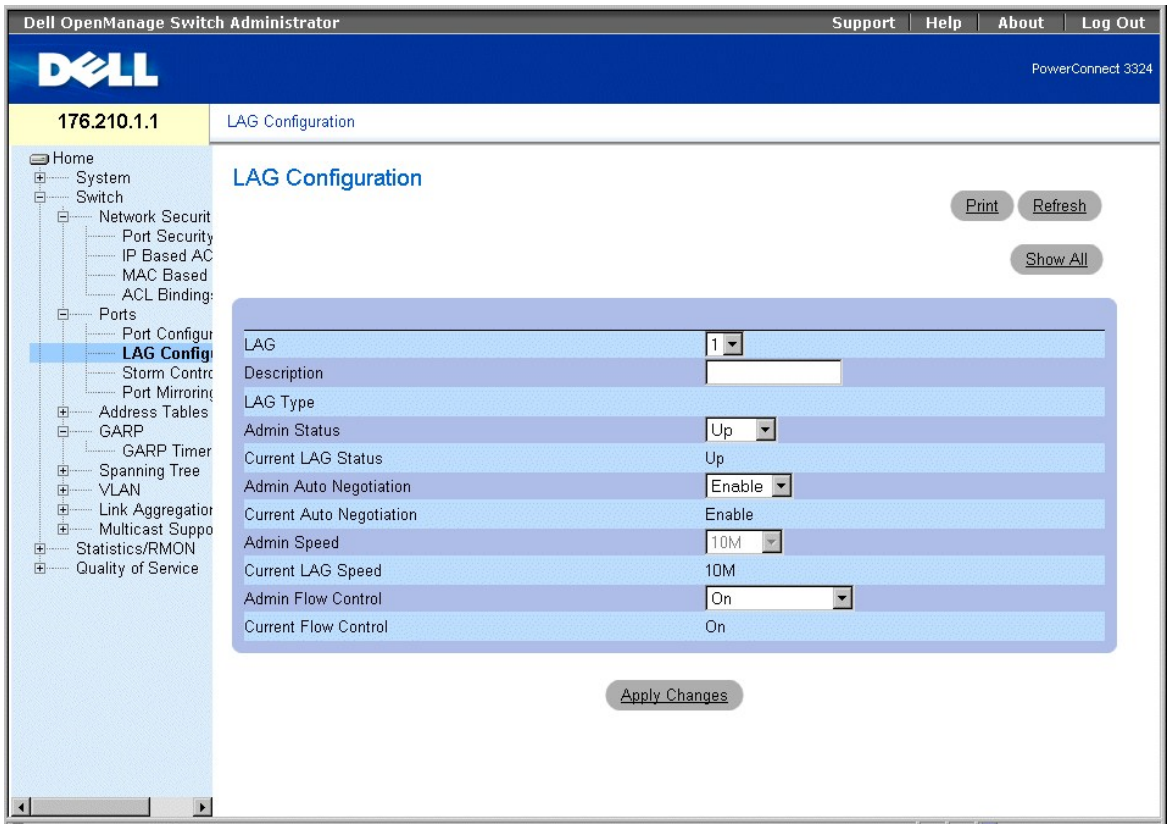
LAG パラメータの定義

LAG Configuration ページを使用して、ネットワーク管理者は設定されている LAG のパラメータを設定できます。PowerConnect 3324/3348 は、1 つの LAG に最大で 8 つまでのポート、1 つのシステムで 6 つまでの LAG に対応しています。システムは 6 つの恒久的な LAG を提供します。LAG (Link Aggregated Group) および LAG へのポートの割り当ての詳細については、「 ポートの集合」 を参照してください。

LAG Configuration ページを開くには、次の手順を実行します。

メモ: ポートが LAG メンバーである間にポート設定が変更された場合、設定の変更は LAG からそのポートが削除されてから有効になります。

- Tree View で、**Switch** → **Ports** → **LAG Configuration** とクリックします。**LAGConfiguration** ページが開きます。



LAG Configuration ページ

LAG Configuration ページには、以下のフィールドが含まれています。

- **LAG** — LAG 番号を示します。
- **Description** — ユーザー定義の LAG の説明を提供します。
- **LAG Type** — LAG の最大速度を示します。
- **Admin Status** — 選択された LAG からのトラフィックを制御します。デフォルトで、このパラメータは **Up** に設定されています。可能なフィールド値には、以下のものがあります。
  - **Up** — LAG を介したトラフィック転送を有効にします。
  - **Down** — LAG を介したトラフィック転送を無効にします。
- **Current LAG Status** — LAG のステータスを指定します。可能なフィールド値には、以下のものがあります。
  - **Up** — LAG が現在機能していることを示します。
  - **Down** — LAG が現在機能していないことを示します。
- **Admin Auto Negotiation** — LAG の自動ネゴシエーションを有効にします。自動ネゴシエーションは、LAG がそれぞれのパートナーに送信速度、二重方式モード、フロー制御能力 （Flow Control はデフォルトで無効になっています） を通知できる 2 つのリンクパートナー間のプロトコルです。可能なフィールド値には、以下のものがあります。

- **Enable** — LAG で自動ネゴシエーションを有効にします。
- **Disable** — LAG で自動ネゴシエーションを無効にします。

- **Current Auto Negotiation** — 現在の自動ネゴシエーションの設定を示します。可能なフィールド値には、以下のものがあります。
  - **Enable**
  - **Disable**
- **Admin Speed** — LAG の動作速度を示します。この値は、LAG が無効な場合にのみ入力できます。可能なフィールド値には、以下のものがあります。
  - **10M**
  - **100M**
  - **1000M**
- **Current LAG Speed** — 同期化されている LAG 速度を bps で指定します。
  可能なフィールド値には、以下のものがあります。
  - **10M**
  - **100M**
  - **1000M**
- **Current Duplex Mode** — LAG 通信タイプを指定します。可能なフィールド値には、以下のものがあります。
  - **Full** — インタフェースは、デバイスとクライアント間の同時双方向の通信をサポートします。
  - **Half** — インタフェースは、デバイスとクライアント間で一度に一方向のみの通信をサポートします。
- **Admin Current Duplex Mode** — LAG 通信タイプを指定します。可能なフィールド値には、以下のものがあります。
  - **Full** — インタフェースは、デバイスとクライアント間の同時双方向の通信をサポートします。
  - **Half** — インタフェースは、デバイスとクライアント間で一度に一方向のみの通信をサポートします。
- **Flow Control** — LAGで Flow Control が有効になっていることを示します。可能な値は以下のとおりです。
  - **Off** — LAGの Flow Control を無効にします。これはデフォルト値です。
  - **On** — LAGの Flow Control を有効にします。
  - **Auto-negotiation** — LAG で Flow Control の自動ネゴシエーションを有効にします。
- **Current Flow Control** — Flow Control の現在の設定を示します。可能な値は以下のとおりです。
  - **Off**
  - **On**
  - **Auto-negotiation**

LAG パラメータを定義するには、次の手順を実行します。

1. **LAG Configuration** ページを開きます。
2. **LAG** フィールドで、LAG を選びます。
3. **Description**、**Admin Status**、**Port Speed**、**Admin Auto Negotiation**、 **Admin Speed**、および/または**Admin Flow Control**フィールドを定義します。
4. **Apply Changes** をクリックします。LAG パラメータがデバイスに保存されます。

LAG パラメータを変更するには、次の手順を実行します。

1. **LAG Configuration** ページを開きます。
2. **LAG** フィールドで、LAG を選びます。

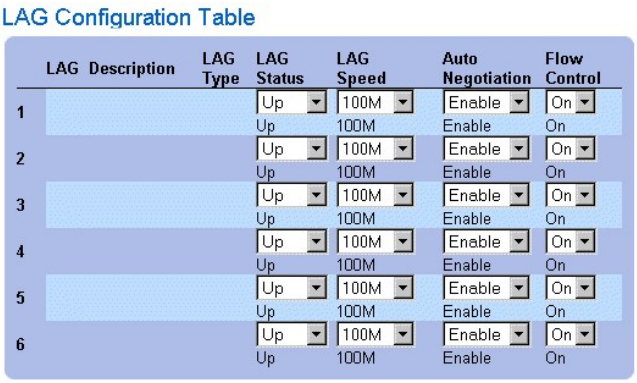
3. **Description**、**Admin Status**、**Port Speed**、**Admin Auto Negotiation**、 **Admin Speed**、および/または**Admin Flow Control**フィールドを変更します。

4. **Apply Changes** をクリックします。LAG パラメータがデバイスに保存されます。

LAG Configuration Table を表示するには、次の手順を実行します。

1. **LAG Configuration** ページを開きます。

2. **Show All** をクリックします。**LAG Configuration Table** が開きます。



LAG Configuration Table

CLI コマンドを使用した LAG 設定

以下に、自動ネゴシエーションを無効、100Full の設定で LAG を設定する方法の例を示します。

システムプロンプトで以下を入力して、静的リンク集合をセットアップします。

```
console> en

console# config

console(config)# interface port-channel 1

console(config-if)# no neg

console(config-if)# speed 100

console(config-if)# exit

console(config)# interface range ethernet 1/e23-24
```

```
console(config-if)# no mdix

console(config-if)# no neg

console(config-if)# speed 100

console(config-if)# duplex full

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

console(config-if)# end
```

以下のメッセージが表示されます。

```
console# sh interfaces status port-channel 1

Flow Link Back
ch Type Duplex Speed Neg Control State Pressure

.....................................................

ch1 100M Full 100 Disabled Off Up Disabled
```

次の表に、**LAG Configuration** ページで表示される LAG の設定に対応する CLI コマンドをまとめます。

CLI コマンド	**説明**
interface port-channel *port-channel-number*	ポートチャネルを作成し、ポートチャネル設定モードを起動します。
channel-group *port-channel-number* **mode {on | auto}**	ポートにポートチャネルを関連付けます。
show interfaces port-channel [*port-channel-number***]**	ポートチャネル情報を表示します （どのポートがポートチャネルのメンバーで、現在アクティブかどうかの情報）。

以下に、CLI コマンドの例を示します。

```
Console (config)# interface ethernet 1/e5

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

Console (config-if)# exit
```

```
Console (config-if)# exit

Console # show interfaces port-channel

Channel Port

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

1 Active 1/e5, 2/e2 Inactive 3/e3

2 Active 1/e2

3 Inactive 3/e8
```

ストーム制御の有効化

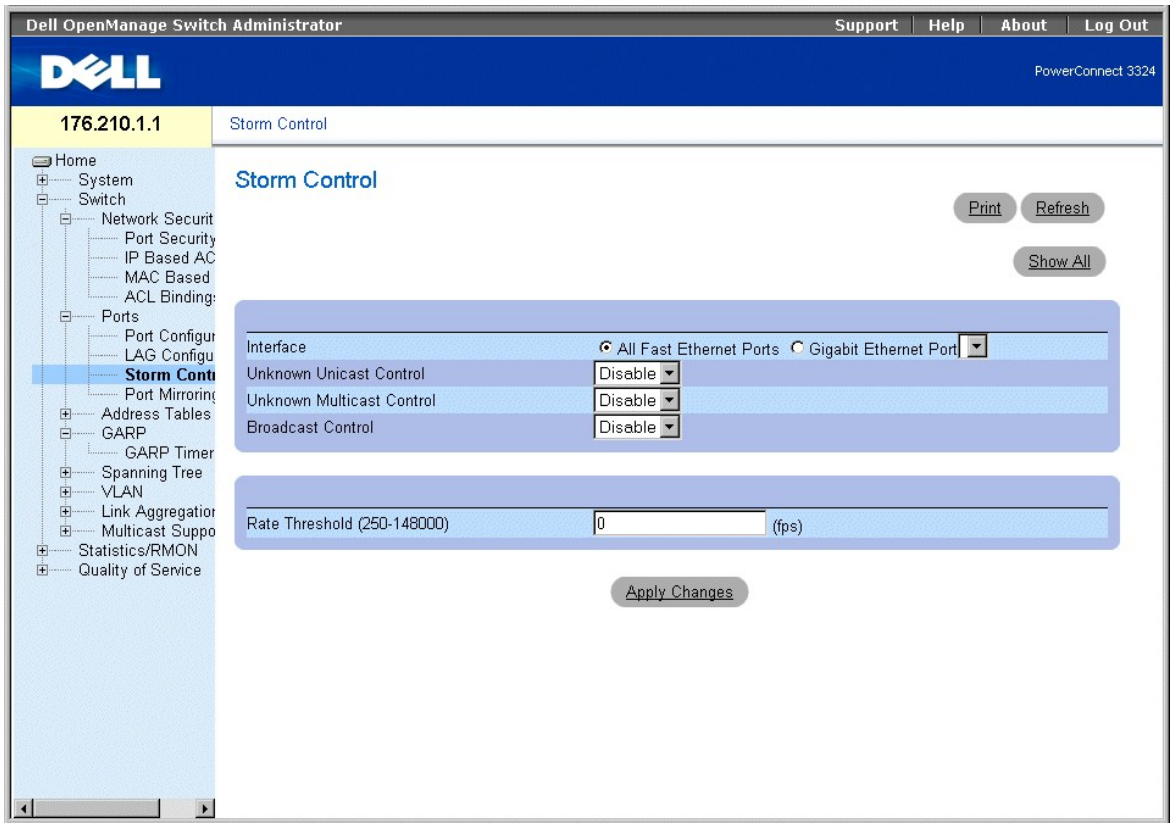
ブロードキャストストームは、1 つのポートがネットワーク上で同時に送信するブロードキャストメッセージ量の過多が原因で起こります。転送されたメッセージ応答は、ネットワークにロードされ、ネットワークリソースの不足や、ネットワークのタイムアウトを引き起こします。

ストーム制御は、パケットタイプとパケットの送信速度を定義することにより、すべての Fast Ethernet ポートまたは Giga ポートに有効になります。ポートも、グループ全体に対してストーム保護を提供するためにグループ化できます。

システムは、受信ブロードキャスト、マルチキャスト、および不明なフレームの速度を各ポートで個別に測定し、速度がユーザー定義の速度を上回る場合、フレームを破棄します。

Storm Control ページを使用してネットワーク管理者は、ストーム制御を有効にしたり設定することができます。**Storm Control** ページを開くには、次の手順を実行します。

- Tree View で、**Switch → Ports → Storm Control** とクリックして、**StormControl** ページを開きます。



Storm Control ページ

Storm Control ページには、以下のフィールドが含まれています。

- **Interface** — Storm Control が設定されているインタフェースを示します。
  - **All Fast Ethernet Ports** — Storm Control がすべての FE ポートに有効になっていることを示します。Storm Control は、GE ポートに個別に適用できます。
  - **Gigabit Ethernet Port** — 選択された Gigabit Ethernet ポートで、Storm Control が有効になっていることを示します。Storm Control は、すべての FE ポートに対して有効、または無効になっています。
- **Unknown Unicast Control** — デバイスで不明なユニキャストパケットの抑制を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — デバイスで不明なユニキャストパケットの抑制を有効にします。
  - **Disable** — デバイスで不明なユニキャストパケットの抑制を無効にします。
- **Unknown Multicast Control** — デバイスで不明なマルチキャストパケットの抑制を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — デバイスで不明なユニキャストパケットの抑制を有効にします。
  - **Disable** — デバイスで不明なマルチキャストパケットの抑制を無効にします。
- **Broadcast Control** — 不明なブロードキャストパケットの抑制を有効にします。
  可能なフィールド値には、以下のものがあります。
  - **Enable** — ブロードキャストパケットの抑制を有効にします。
  - **Disable** — ブロードキャストパケットの抑制を無効にします。
- **Rate Threshold (250-148000)** — ストーム制御用にブロードキャストパケット速度の限度を設定します。FE ポートでは、範囲は 250 ～ 148,000 で、GE ポートでは、範囲は 250 ～ 262,143 パケットです。FE ポートでのデフォルトは 148,000 で、GEポートでのデフォルトは 262,143 です。

デバイスで Storm Control を有効にするには、次の手順を実行します。

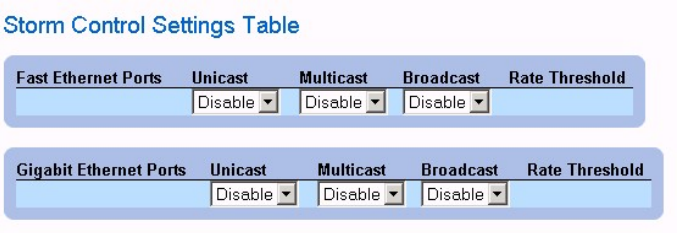
1. **Storm Control** ページを開きます。
2. ストーム制御を導入するインタフェースを選びます。
3. **Unknown Unicast Control**、**Unknown Multicast Control**、**Broadcast Control**、および **Rate Threshold (250-148000)** フィールドを定義します。
4. **Apply Changes** をクリックします。Storm Control がデバイスで有効になります。

Storm Control ポートパラメータを変更するには、次の手順を実行します。

1. **Storm Control** ページを開きます。
2. **Unknown Unicast Control**、**Unknown Multicast Control**、**Broadcast Control**、および **Rate Threshold (250-148000)** フィールドを変更します。
3. **Apply Changes** をクリックします。Storm Control ポートパラメータがデバイスに保存されます。

Storm Control Settings Table を表示するには、次の手順を実行します。

1. **Storm Control** ページを開きます。
2. **Show All** をクリックします。**Storm Control Settings Table** が開きます。



Storm Control Settings Table

CLI コマンドを使用したストーム制御の設定

次の表に、**Storm Control** ページで表示されるストーム制御の設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
port storm-control enable {unknown | broadcast | multicast} {fastethernet | gigaethernet *interface***}**	ユニキャスト、マルチキャスト、およびブロードキャストパケットに対してブロードキャストストーム制御を有効にします。
port storm-control rate gigaethernet *interface rate.*	最大ブロードキャスト速度を設定します。
show ports storm-control	ストーム制御設定を表示します。

以下に、CLI コマンドの例を示します。

```
Console(config)# port storm-control rate fastethernet 300

Console(config)# port storm-control enable fastethernet
```

```
Console# show ports storm-control

Port Unknown Broadcast Multicast Rate
[Packets/sec]
-------------- -------- --------- -------- -----------
Gigaethernet 1 Enabled Disabled Enabled 2000
Gigaethernet 2 Enabled Enabled Enabled 2000
FastEthernet Enabled Enabled Enabled 1000
```

ポートミラリングセッションの定義

ポートのミラリングは、ポートから監視ポートに送受信パケットのコピーを転送して、ネットワークトラフィックの監視とミラーをおこないます。ポートのミラリングは、診断ツールまたはデバッグ機能として利用することができます。ポートのミラリングは、スイッチ性能の監視も可能にします。

ネットワーク管理者は、すべてのパケットをコピーする特定のポート、およびパケットのコピー元と別のポートを選んで、ポートのミラリングを設定します。ポートのミラリングを設定する前に、以下のことに注意します。

- 監視されているポートは、監視しているポートより高速で動作できません。
- すべての RX/TX パケットは、同じポートで監視する必要があります。
- PowerConnect 3348 は、同じユニット内のポート 1 ～ 24 およびポート 25 ～ 48 間をミラーします。ミラリングは、ポート 25 ～ 48 間、および別の PowerConnect 3348 のポート 25 ～ 48 間、またはどの PowerConnect 3324 のポートでも可能です。
- PowerConnect 3348 は、ミラー元のポートが G2 ポートではない限り、どの PowerConnect 3324 ユニットにでもミラーできます。PowerConnect 3348 は、ポートが PowerConnect の 25 ～ 48 ポートの範囲にある限り、別の PowerConnect 3348 ユニットとミラーできます。

以下の制限が、ミラー先のポートとして設定するポートに適用されます。

- ポートはミラー元として設定できないこと。
- ポートは LAG メンバーでないこと。
- IP インタフェースは、ポートで設定されていないこと。
- GVRP は、ポートで有効でないこと。
- ポートは、VLAN のメンバーでないこと。
- ミラー先には 1 つのポートのみ定義できます。

以下の制限が、ミラー元のポートとして設定するポートに適用されます。

- ミラー元ポートは LAG メンバーでないこと。
- ポートはミラー先としては設定できないこと。

- すべてのパケットは、ミラー先ポートから送信される時にタグ付けされます。

以下の制限が、ミラー元のポートとして設定するポートに適用されます。

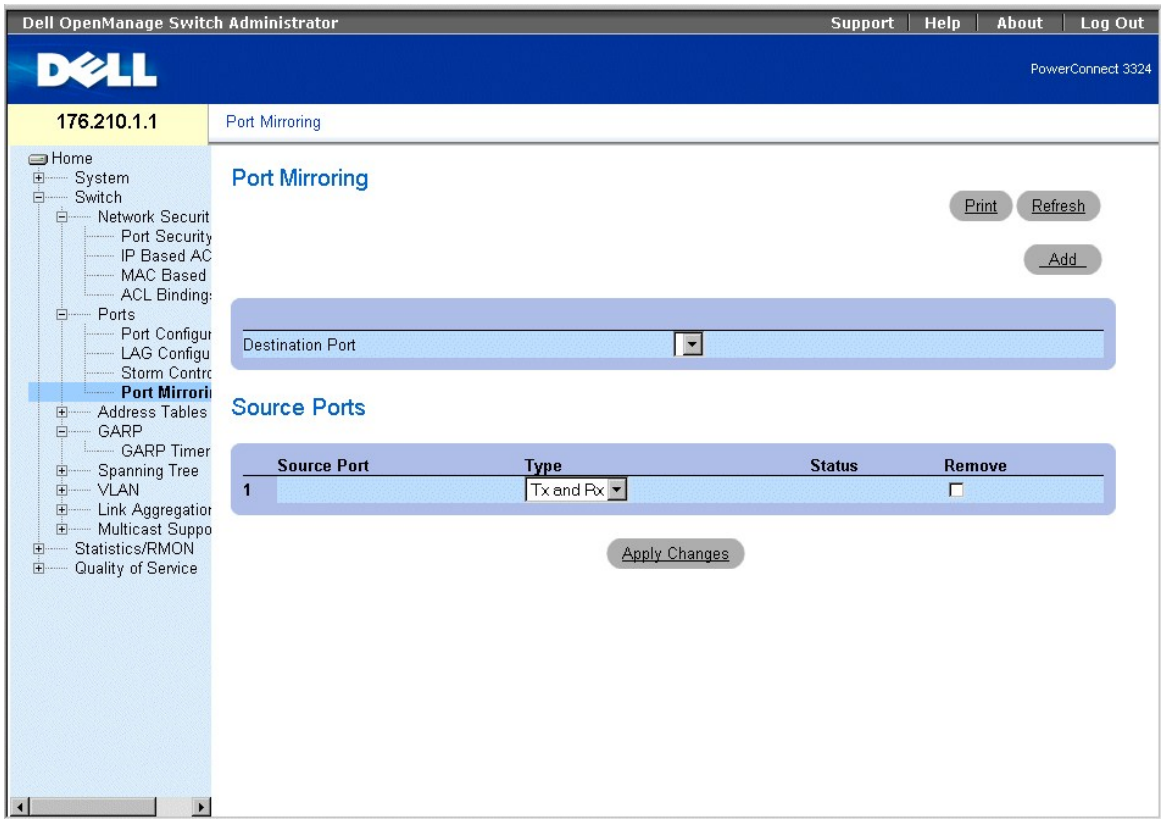
- タグなしのパケットがミラー元のポートで受信された場合、パケットはミラー先ポートに送信される際に、ミラー元のポートのデフォルト PVID でタグ付けされます。

すべての RX/TX パケットは、同じポートで監視する必要があります。

Port Mirroring ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Ports** → **Port Mirroring** とクリックします。**PortMirroring** ページが開きます。

メモ: ポートが、ポートミラリングセッションのターゲットポートに設定されている場合、このポート上のすべての通常の動作は一時停止されます。この動作は、Spanning Tree と LACP を含みます。



Port Mirroring ページ

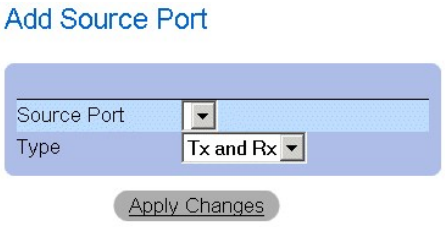
- **Destination Port** — ポートトラフィックのミラー先のポート番号を定義します。コピーポートは、自分自身をミラーできません。 また、ミラー元のポート VLAN 以外の VLAN メンバーであってはいけません。 IP インタフェースで設定することもできません。ミラー元のポートのすべてのトラフィックはタグ付けされます。
- **Source Port** — ポートトラフィックのコピー元のポート番号を定義します。最大で 8 ポートが 1 つのミラリングポートにミラーできます。
- **Type** — ミラーされるポートのトラフィックタイプを指定します。可能なフィールド値には、以下のものがあります。
  - **RX** — 受信トラフィックがミラーされていることを示します。
  - **TX** — 送信トラフィックがミラーされていることを示します。

- **Both** — 送受信トラフィックの両方がミラーされていることを示します。

- **Status** — ポートの状態を示します。可能なフィールド値には、以下のものがあります。
  - **Active** — ポートが有効になっていて、ネットワークトラフィックの受信 / 転送をおこなっていることを示します。
  - **Not Active** — ポートが無効になっていて、ネットワークトラフィックの受信 / 転送をおこなっていないことを示します。
- **Remove** — ポートミラリングセッションを削除します。可能なフィールド値には、以下のものがあります。
  - **Checked** — ポートミラリングセッションを削除します。
  - **Unchecked** — ポートミラリングセッションを保持します。

ポートミラリングセッションを追加するには、次の手順を実行します。

1. **Port Mirroring** ページを開きます。
2. **Add** （追加）をクリックします。**Add Source Port** ページが開きます。



Add Source Port ページ

3. **Source Port** および **Type** フィールドを定義します。
4. **Apply Changes** をクリックします。新しいミラー元ポートが定義され、デバイスがアップデートされます。

ポートミラリングセッションからコピーポートを削除するには、次の手順を実行します。

1. **Port Mirroring** ページを開きます。
2. **Remove** チェックボックスにチェックマークを付けます。
3. **Apply Changes** をクリックします。ポートミラリングセッションが削除され、デバイスがアップデートされます。

CLI コマンドを使用したポートミラリングセッションの設定

次の表に、**Port Mirroring** ページで表示されるポートミラリングセッションの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
port monitor *src-interface* **[rx | tx]**	ポートコピーの状態を表示します。
show ports monitor	ポート監視セッションを開始します。

以下に、CLI コマンドの例を示します。

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

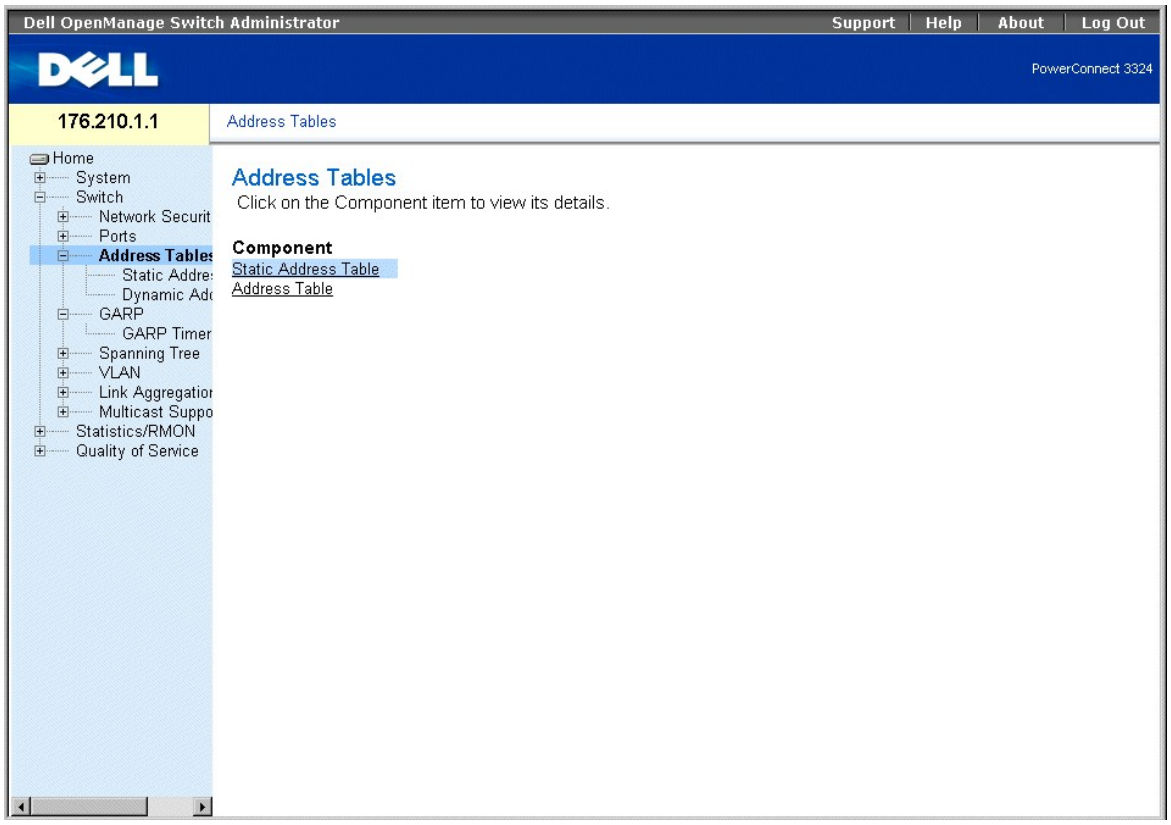
```
Console(config-if)# port monitor 1/e8

Console# show ports monitor

Source port Destination Port Type Status

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

1/e1 1/e8 RX, TX Active

1/e2 1/e8 RX Active
```

アドレステーブルの設定

MAC アドレスは、Static Address データベースまたは Dynamic Address データベースのどちらかに保存されます。データベースに保存された送信先に向けたパケットは、ただちにポートに転送されます。Static Address Table および Dynamic Address Table は、インタフェース、VLAN、およびインタフェースタイプ別に並べ替えができます。ミラー元からのパケットがスイッチに着くと、MAC アドレスは動的に学習されます。アドレスは、フレームの送信元のアドレスからポートを確認してポートに関連付けられます。どのポートにも関連していない、送信先の MAC アドレス向けフレームは、関連 VLAN のすべてのポートにフラッドされます。静的アドレスは、手動でユーザーによって設定されます。ブリッジテーブルのオーバーフローを防ぐため、一定期間トラフィックのない動的 MAC アドレスは削除されます。

Address Tables ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Address Tables** とクリックします。
  Address Tables ページが開きます。



Address Tables ページ

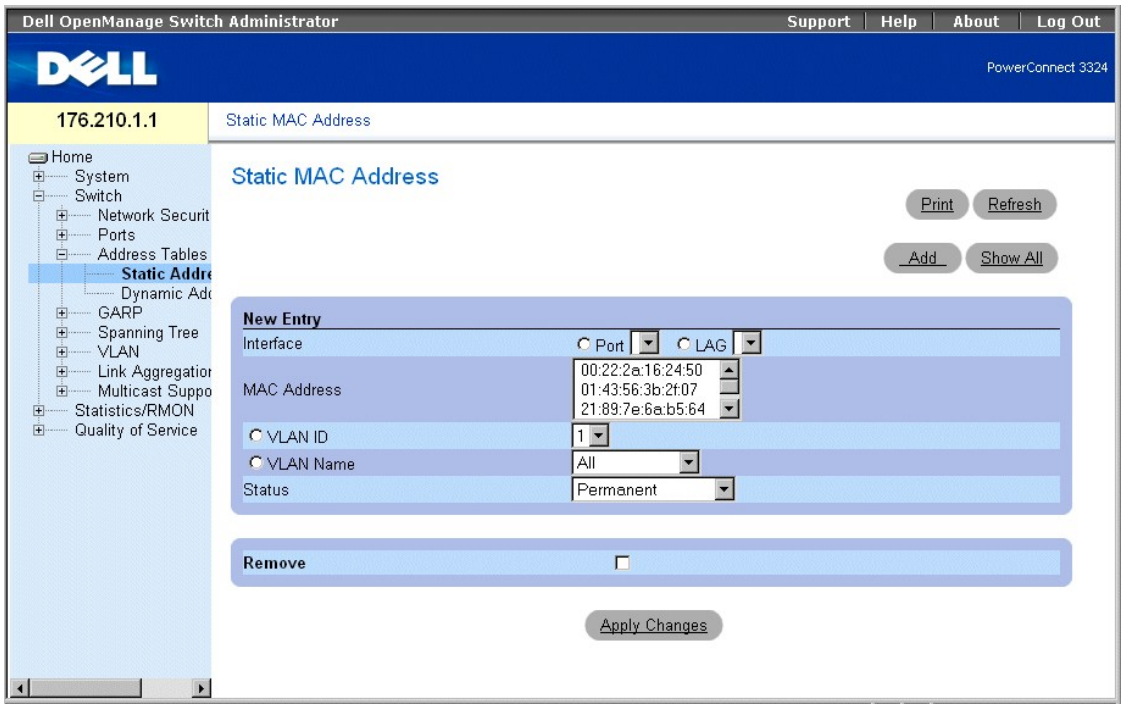
Address Tables ページには、以下へのリンクがあります。

- 静的アドレスの定義
- 動的アドレスの表示

静的アドレスの定義

Static MAC Address ページには、静的 MAC アドレスの一覧が含まれています。静的アドレスは、**Static MAC Address** ページから追加したり削除できます。また、複数の MAC アドレスを 1 つのポートに定義できます。**Static MAC Address** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Address Tables** → **Static Address** とクリックします。**Add Static MAC Address** ページが開きます。



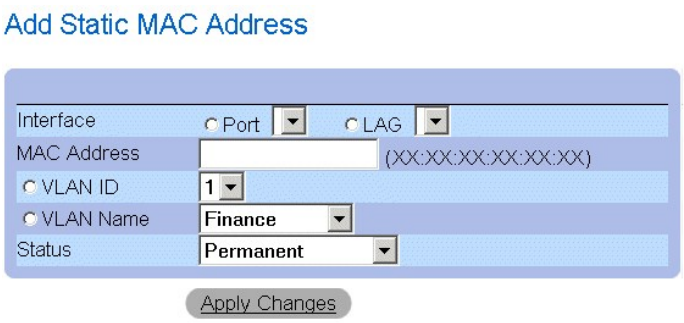
Add Static MAC Address ページ

Add Static MAC Address ページには、以下のフィールドが含まれています。

- **Interface** — 静的 MAC アドレスが追加される特定のインタフェースを示します。
  可能なフィールド値には、以下のものがあります。
  - **Port** — MAC アドレスが追加される特定のポートを示します。
  - **LAG** — MAC アドレスが追加される特定の LAG を示します。
- **MAC Address** — **Current Static Address List** に一覧表示されている MAC アドレスを指定します。
- **VLAN ID** — MAC アドレスに付加されている VLAN ID 値を示します。
- **VLAN Name** — ユーザー定義の VLAN 名を示します。
- **Status** — Static MAC Address のステータスを定義します。可能なフィールド値には、以下のものがあります。
  - **Permanent** — 恒久的な MAC アドレスであることを示します。
  - **Delete on Reset** — デバイスがリセットされる際に、MAC アドレスが削除されることを示します。
  - **Timeout** — デバイスがタイムアウトする際に、MAC アドレスが削除されることを示します。
  - **Secure** — Locked Port MAC アドレスは削除されません。Secure MAC アドレスは、Port Security ページから削除されます。

Static Address Table に静的アドレスを追加するには、次の手順を実行します。

1. **Static Address Table** を開きます。
2. **Add**（追加）をクリックします。**Add Static MAC Address** ページが開きます。



Add Static MAC Address ページ

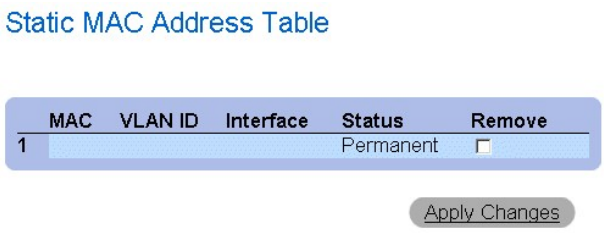
3. **Interface**、**MAC Address**、**VLAN ID** または **VLAN Name**、および **Status** フィールドを定義します。
4. **Apply Changes** をクリックします。Static Address Table に新しい静的アドレスが追加され、デバイスがアップデートされます。

Static Address Table の静的アドレスを変更するには、次の手順を実行します。

1. **Static Address Table** を開きます。
2. **Port**、**MAC Address**、および**VLAN** フィールドを変更します。
3. **Apply Changes** をクリックします。静的アドレスが変更され、デバイスがアップデートされます。

Static Address Table を表示するには、次の手順を実行します。

1. **Static Address Table** を開きます。
2. **Show All** をクリックします。**Static MAC Address Table** が開きます。



Static MAC Address Table

Static Address Table から静的アドレスを削除するには、次の手順を実行します。

1. **Static Address Table** を開きます。
2. **Show All** をクリックして、**Static MAC Address Table** を開きます。
3. 1 つまたは複数のテーブルエントリを選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。静的アドレスが削除され、デバイスがアップデートされます。

CLI コマンドを使用した静的アドレスパラメータの設定

次の表に、**Add Static MAC Address** ページで表示される静的アドレスパラメータの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
bridge address *mac-address* **{ethernet** *interface* **| port-channel** *port-channel-number***} [permanent | delete-on-reset | delete-on-timeout| secure]**	静的 MAC レイヤステーションの送信元のアドレスをブリッジテーブルに追加します。
show bridge address-table static [vlan *vlan***] [ethernet** *interface* **| port-channel** *port-channel-number***]**	ブリッジ転送データベースに静的に入力されたエントリのクラスを表示します。

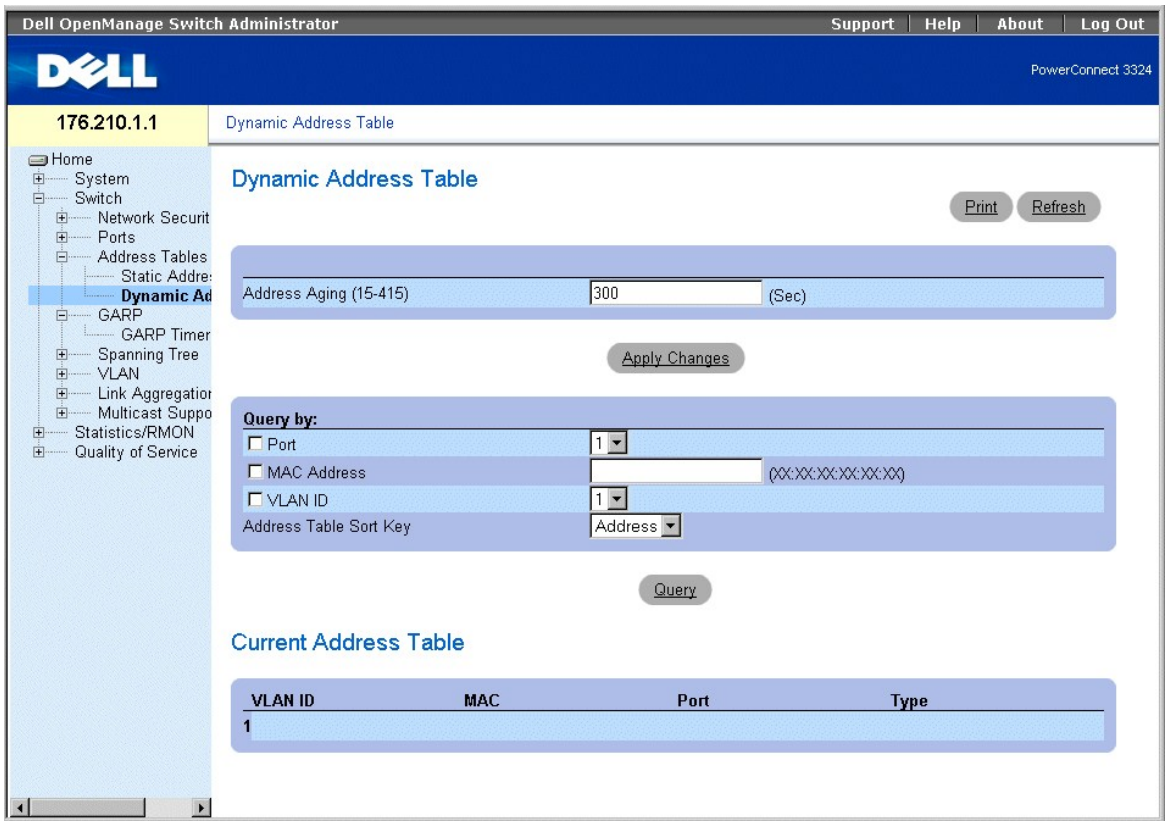
以下に、CLI コマンドの例を示します。

```
Console (config-vlan)# bridge address 168.210.0.10 ethernet 1/e8 permanent

Console# show bridge address table static

Aging time is 300 sec

vlan mac address port type

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

200 0010.0D48.37FF 5/9 delete-on-reset
```

動的アドレスの表示

Dynamic Address ページには、インタフェースタイプ、MAC アドレス、VLAN、およびテーブルの並べ替えなどの **Dynamic Address Table** の照会についての情報が含まれています。Address Tables に保存されているアドレスに転送されたパケットは、直接これらのポートに転送されます。**Dynamic Address Table** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Address Tables** → **Dynamic Addresses** とクリックします。**Dynamic Address Table** ページが開きます。



Dynamic Address Table ページ

Dynamic Address Table ページには、以下のフィールドが含まれています。

- **Address Aging (15-415)** — 送信元からのトラフィックが検出されない場合、タイムアウトまで **Dynamic Address Table** にMAC アドレスが残る時間を指定します。デフォルト値は 300 秒です。
- **Port** — テーブルが照会されるポート番号を指定します。
- **MAC Address** — テーブルが照会される MAC アドレスを指定します。
- **VLAN ID** — テーブルが照会される VLAN ID を指定します。
- **Address Table Sort Key** — Dynamic Address Table が並べ替えられる方法を指定します。可能なフィールド値には、以下のものがあります。
  - **Address** — 指定された MAC アドレスに対する照会結果を並べ替えます。
  - **VLAN** — 照会結果を VLAN ID で並べ替えます。
  - **Interface** — インタフェースで照会結果を並べ替え、指定されたポートで学習されたすべての MAC アドレスを表示します。

Query Results Table ページには、以下のコラムが含まれています。

- **VLAN ID** — VLAN ID タグ値を示します。
- **MAC** — MAC アドレスを示します。
- **Port** — ポートが動的 MAC アドレスに付与されていることを示します。
- **Type** — MAC アドレスタイプを示します。

エージングタイムを再定義するには、次の手順を実行します。

1. **Dynamic Address Table** を開きます。

2. **Address Aging (15-415)** フィールドを定義します。
3. **Apply Changes** をクリックします。エージングタイムが変更され、デバイスがアップデートされます。

Dynamic Address Table を照会するには、次の手順を実行します。

1. **Dynamic Address Table** を開きます。
2. **Dynamic Address Table** を照会するパラメータを定義します。 **Dynamic Address Table** エントリは、インタフェース、MAC アドレス、または VLAN で照会することができます。
3. **Query** をクリックします。**Dynamic Address Table** が照会されます。照会結果は、選択した **Address Table Sort Key** フィールド値で並べ替えられます。

CLI コマンドを使用した動的アドレスの照会と並べ替え

次の表に、**Dynamic Address Table** ページで表示される動的アドレスの照会と並べ替えの実行に対応する CLI コマンドをまとめます。

CLI コマンド	説明
bridge aging-time *seconds*	アドレステーブルのエージングタイムを設定します。
show bridge address-table [vlan *vlan*] **[ethernet** *interface* **| port-channel** *port-channel-number*]	ブリッジ転送データベースに動的に作成されたエントリのクラスを表示します。

以下に、CLI コマンドの例を示します。

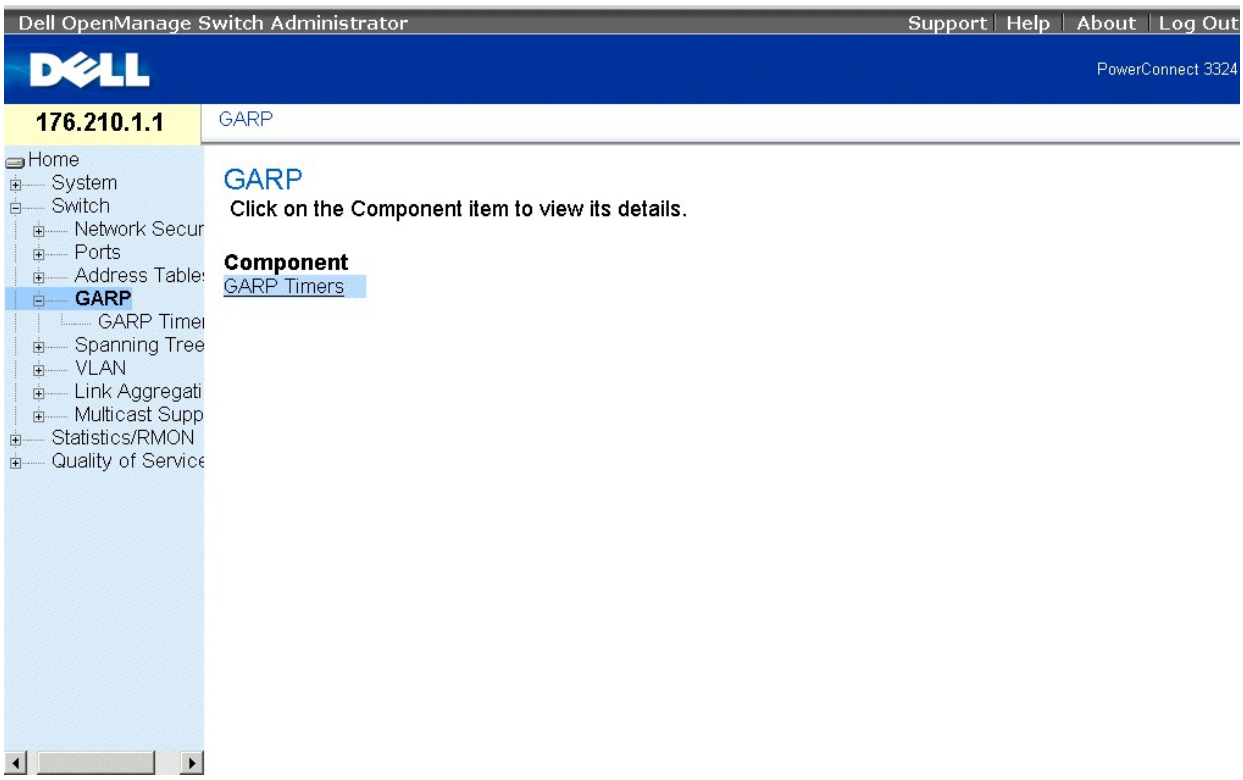
```
Console (config)# bridge aging-time 250

Console (config)# exit

Console# show bridge address table


Aging time is 250 sec


vlan mac address port type

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

1 0060.704C.73FF 5/e8 dynamic

1 0060.708C.73FF 5/e8 dynamic
```

```
200 0010.0D48.37FF 5/e9 static
```

GARP の設定

GARP (Generic Attribute Registration Protocol) プロトコルは、ネットワーク接続またはメンバーシップスタイル情報を登録する汎用プロトコルです。GARP は、VLAN やマルチキャストアドレスなど、特定のネットワーク属性に関連するデバイスのセットを定義します。**GARP** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **GARP** とクリックします。**GARP** ページが開きます。



GARP ページ

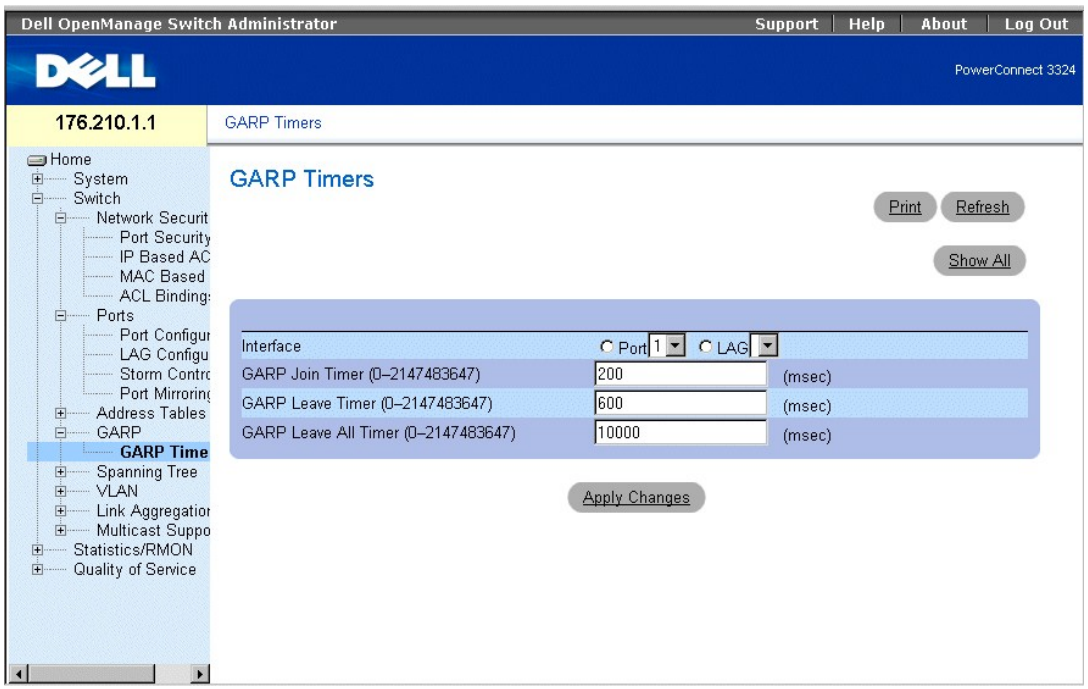
この項には、以下のトピックが含まれています。

- GARP タイマーの定義

GARP タイマーの定義

GARP Timers ページには、デバイスで GARP を有効にするためのパラメータが含まれています。**GARP Timers** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **GARP** → **GARP Timers** とクリックします。**GARPTimers** ページが開きます。



GARP Timers ページ

GARP Timers ページには、以下のフィールドが含まれています。

- **Interface** — GARP Timer が表示されるインタフェースのタイプを示します。
  可能なフィールド値には、以下のものがあります。
  - **Port** — GARP Timer が表示されるポートを示します。
  - **LAG** — GARP タイマーが表示される LAG を示します。
- **GARP Join Timer (10-2147483647)** — PDU が送信される時間をミリ秒で示します。
- **GARP Leave Timer (10-2147483647)** — デバイスが GARP 状態でなくなるまで待つ時間をミリ秒で示します。**GARP Leave Timer** は、**GARP Leave All Timer** メッセージの送受信によってアクティブになり、**GARP Join Timer** メッセージの受信でキャンセルされます。デフォルトは、600 ミリ秒です。
- **GARP Leave All Timer (10-2147483647)** — VLAN 内のポートを確認するのに使用します。メッセージの送信間隔のミリ秒での時間です。デフォルトは、10000 ミリ秒です。

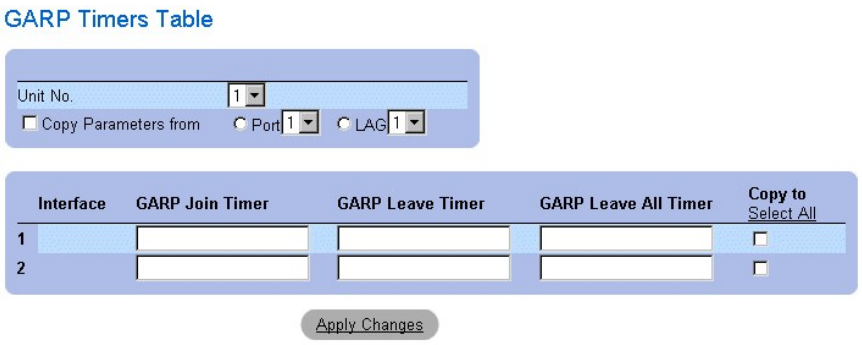
メモ: 様々なタイマー値間では、次の関係を維持する必要があります — Leave Time は、 Join Time の 3 倍以上である必要があります。Leave-all Time は、Leave Time 以上である必要があります。

GARP タイマーを定義するには、次の手順を実行します。

1. **GARP Timers** ページを開きます。
2. **Interface**、**GARP Join Time**、 **GARP Leave Timer**、および **GARP Leave All Timer** を定義します。
3. **Apply Changes** をクリックします。GARP パラメータがデバイスに保存されます。

GARP Timers Table を表示するには、次の手順を実行します。

1. **GARP Timers** ページを開きます。
2. **Show All** をクリックします。**GARP Timers Table** が開きます。



GARP Timers Table ページ

GARP Timers ページのフィールドに加えて、**GARP Timers Table** ページには以下のフィールドも表示されます。

- **Unit No.** — スタッキングユニットの番号を示します。
- **Copy Parameters From** — ポート GVRP パラメータを **Copy to** フィールドで指定されたインタフェースにコピーします。
- **Copy To** — GVRP Timer がコピーされるインタフェースを示します。

GARP 情報をコピーするには、次の手順を実行します。

1. **GARP Timers** ページを開きます。
2. **Show All** をクリックします。**GARP Timers Table** が開きます。
3. **Copy Parameters from** フィールドで、インタフェースを選びます。
4. **Copy To** フィールドで、GARP タイマー情報をコピーするインタフェースを選びます。

CLI コマンドを使用した GARP タイマーの定義

次の表に、**GARP Timers** ページで表示される GARP タイマーの定義に対応する CLI コマンドをまとめます。

CLI コマンド	説明
garp timer {join | leave | leaveall} *timer_value*	GARP アプリケーションの join、leave、および leaveall GARP タイマー値を設定します。

以下に、CLI コマンドの例を示します。

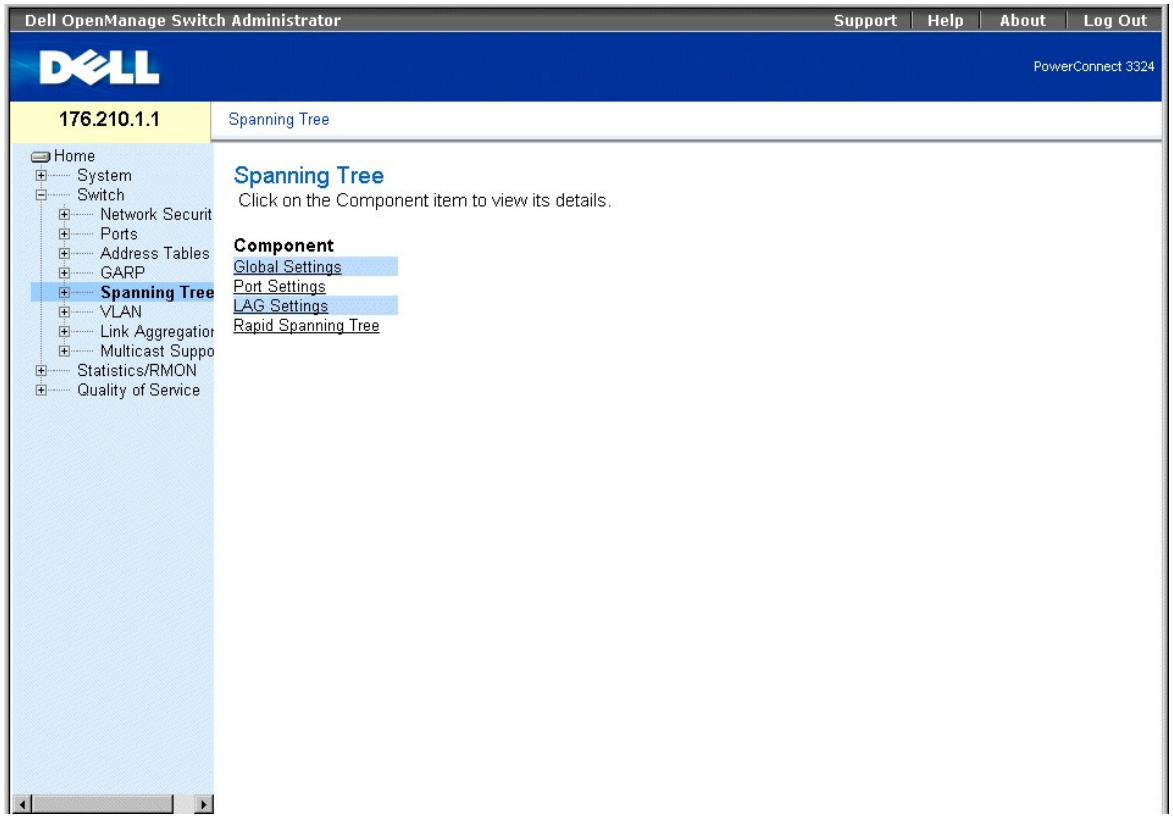
```
Console (config)# interface ethernet 1/e8

Console (config-if)# garp timer leave 900
```

Spanning Tree Protocol の設定

STP (Spanning Tree Protocol) は、Layer 2 ネットワーク上のエンドステーション間に単一のパスを提供し、ループを解消します。

ループは、ホスト間に代替ルートが存在する場合に発生します。拡張ネットワーク内のループにより、ブリッジは永続的にトラフィックを転送し、トラフィックの増加とネットワーク性能の低下の原因となることがあります。**Spanning Tree** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Spanning Tree** とクリックします。**Spanning Tree** ページが開きます。



Spanning Tree ページ

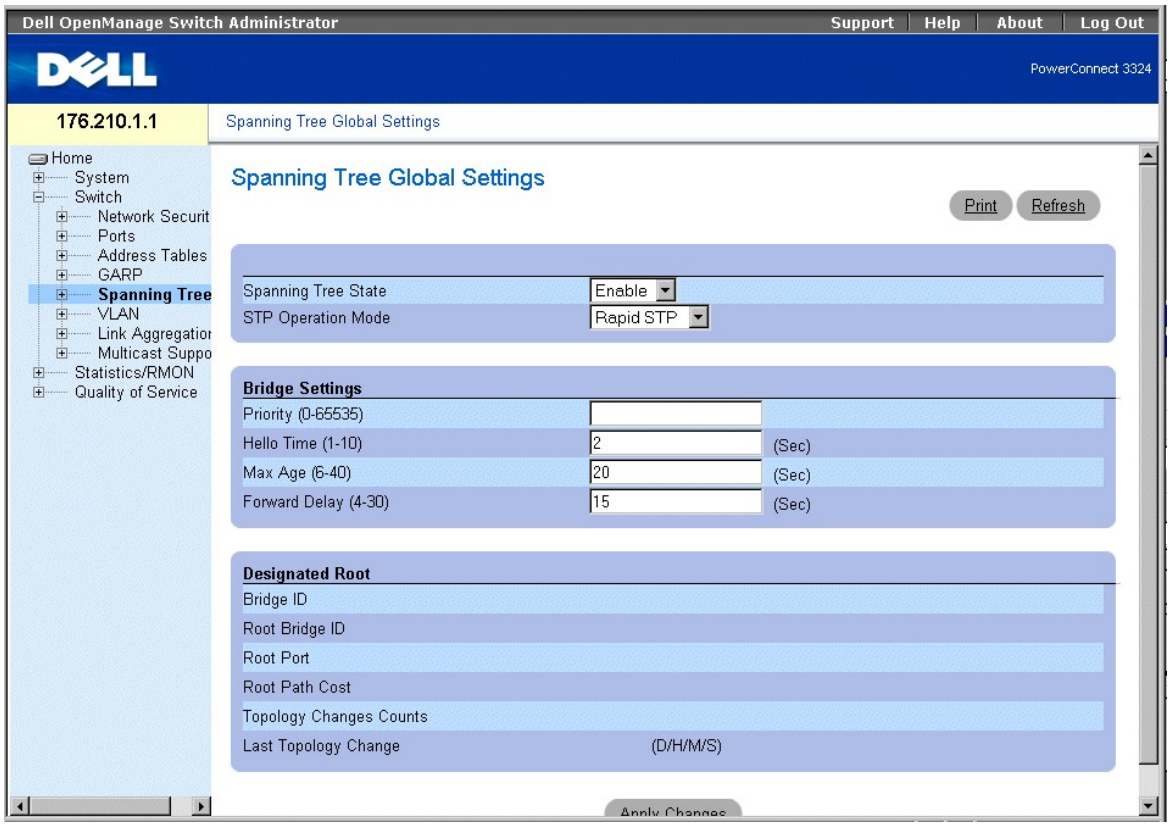
この項には、以下のトピックがあります。

- STP グローバル設定の定義
- Defining STP Port Settings
- STP LAG 設定の定義
- Rapid Spanning Tree の設定

STP グローバル設定の定義

Spanning Tree Global Settings ページには、デバイスで STP 動作を有効にしたり、設定するためのパラメータが含まれています。**Spanning Tree Global Settings** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Spanning Tree** → **Global Settings** とクリックします。**Spanning Tree Global Settings** ページが開きます。



Spanning Tree Global Settings ページ

Spanning Tree Global Settings ページには、以下のフィールドが含まれています。

- **Spanning Tree State** — デバイスで STP を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — デバイスで STP を有効にします。
  - **Disable** — デバイスで STP を無効にします。
- **STP Operation Mode** — デバイスで有効になっている STP の STP モードを示します。可能なフィールド値には、以下のものがあります。
  - **Classic STP** — デバイスで Classic STP を有効にします (IEEE 802.1D)。
  - **Rapid STP** — デバイスで Rapid STP を有効にします (IEEE 802.1w)。ドライバの詳細は、「Rapid Spanning Tree の設定」を参照してください。
- **Priority (0-65535)** — ブリッジ優先度値を指定します。スイッチまたはブリッジが STP を実行している際、個々に優先度が割り当てられています。BPDU の交換後、最低の優先度値のスイッチが Root Bridge になります。デフォルト値は、32768 です。 ポート優先度値は、16、32、64、80 のように 16 の倍数で増えていきます。
- **Hello Time (1-10)** — スイッチの Hello Time を指定します。Hello Time は、ルートブリッジが設定メッセージの間に待つ時間を秒で示します。デフォルトは 2 秒です。
- **Max Age (6-40)** — スイッチの Maximum Age Time を指定します。Maximum Age Time は、ルートブリッジが設定メッセージを送信するまでに待つ時間を秒で示します。デフォルトの Maximum Age Time は、20 秒です。
- **Forward Delay (4-30)** — スイッチ転送遅延時間を指定します。転送遅延時間は、ブリッジがパケットを転送するまで、Listening と Learning 状態でいる時間を秒で示します。デフォルトは 15 秒です。
- **Bridge ID** — ブリッジ優先度および MAC アドレスを示します。
- **Root Bridge ID** — Root Bridge 優先度および MAC アドレスを示します。
- **Root Port** — このブリッジから Root Bridge への一番低いコストパスを提供するポート番号を示します。ブリッジがルートでない場合、非常に重要です。デフォルトは、ゼロです。
- **Root Path Cost** — このブリッジからルートへのコストパスを示します。

- **Topology Changes Counts** — STP 状態変更の合計回数を示します。
- **Last Topology Change** — ブリッジが初期化またはリセットされ、最後のトポロジ関連の変更が発生してからの時間を示します。2 日間 5 時間 10 分 4 秒などのように、日数、時間、分、秒の形式で表示されます。

STP グローバルパラメータを定義するには、次の手順を実行します。

1. **Spanning Tree Global Settings** ページを開きます。
2. **Spanning Tree State** フィールドで、**Enable** を選びます。
3. **STP Operation Mode** フィールドで、**Classic STP** を選びます。
4. **Apply Changes** をクリックします。STP がデバイスで有効になります。

STP グローバルパラメータを変更するには、次の手順を実行します。

1. **Spanning Tree Global Settings** ページを開きます。
2. **STP Operation Mode**、**Bridge Priority**、**Hello Time (Sec)**、**Max Age (Sec)**、および **Forward Delay (Sec)** フィールドを定義します。
3. **Apply Changes** をクリックします。STP パラメータが変更され、デバイスがアップデートされます。

CLI コマンドを使用した STP グローバルパラメータの定義

次の表に、**Spanning Tree Global Settings** ページで表示される STP グローバルパラメータの定義に対応する CLI コマンドをまとめます。

CLI コマンド	説明
spanning-tree	Spanning Tree 機能を有効にします。
spanning-tree mode {stp | rstp}	現在実行中の Spanning Tree Protocol を設定します。
spanning-tree priority *priority*	Spanning Tree 優先度を設定します。
spanning-tree hello-time *seconds*	スイッチが他のスイッチに Hello メッセージを送信する頻度を示す Spanning Tree ブリッジの Hello Time を設定します。
spanning-tree max-age *seconds*	ポートに受信されたプロトコル情報をスイッチに保存しておく期間を示す Spanning Tree ブリッジの Max Age を設定します。
spanning-tree forward-time seconds	Spanning Tree ブリッジ転送時間を設定します。 これは、ポートが転送状態に入るまでに Listening と Learning 状態でいる時間です。
show spanning-tree [ethernet *interface* **| port-channel** *port-channel-number***]**	Spanning Tree 設定を表示します。

以下に、CLI コマンドの例を示します。

```
Console(config)# spanning-tree

Console(config)# spanning-tree mode rstp

Console(config)# spanning-tree priority 12288
```

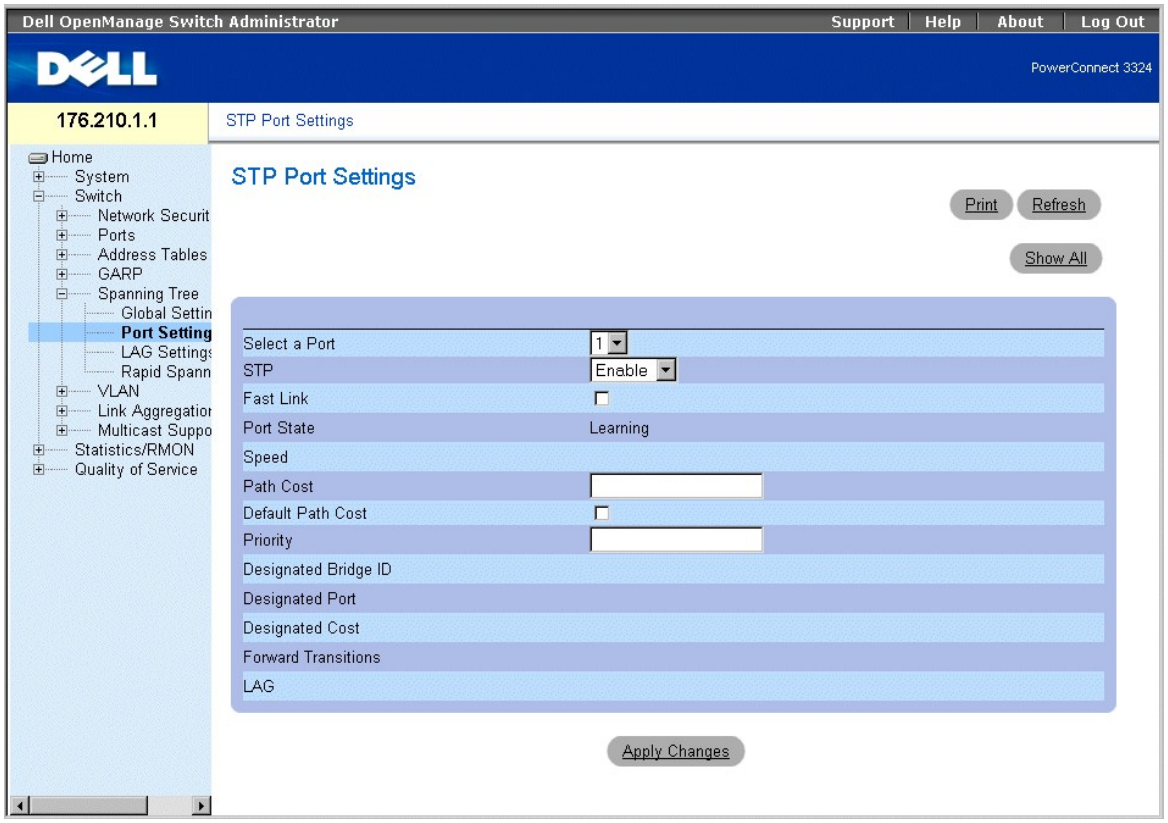
```
Console(config)# spanning-tree hello-time 5

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 X.X.X.X.X.X

Cost 57

Port 1/e1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769

Address X.X.X.X.X.X

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 2 last change occurred 00:23:56 ago

Times:hold 1, topology change 35, notification 2

hello 2, max age 20, forward delay 15


Interface Port ID Designated Port ID

Name Prio Cost Sts Cost Bridge ID Prio.Nbr
```

```
-------- ------ --- --- -------------------- ------

1/e1 128 19 FWD 38 8000 00:30:94:41:62c1 80 001

1/e2 128 19 FWD 57 8000 00:02:4b:29:7a:00 80 002

ch1 128 19 FWD 57 8000 00:02:4b:29:7a:00 80 003
```

Defining STP Port Settings

STP Port Settings ページを使用して、ネットワーク管理者は STP プロパティを個々のポートに割り当てることができます。**STP Port Settings** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Spanning Tree** → **Port Settings** とクリックします。**STP Port Settings** ページが開きます。



STP Port Settings ページ

STP Port Settings ページには、以下のフィールドが含まれています。

- **Select a Port** — STP 統計が表示されるポートを示します。
- **STP** — ポートで STP を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — ポートで STP を有効にします。

- **Disable** — ポートで STP を無効にします。

- **Fast Link** — ポートで Fast Link モードを有効にします。ポートで Fast Link モードが有効な場合、ポートリンクが立ち上がると、ポートは自動的に **Forwarding** 状態に入ります。Fast Link モードは、STP プロトコルが収束するまでにかかる時間を最適化します（STP 収束は大規模ネットワークでは 30 ～ 60 秒かかることがあります）。

- **Port State** — ポートの現在の STP 状態を示します。有効な場合、Port State はトラフィックの転送アクションを決定します。可能なフィールド値には、以下のものがあります。

  - **Disabled** — ポートリンクが現在ダウンしていることを示します。

  - **Blocking** — ポートは現在ブロックされ、トラフィックの転送や MAC アドレスの学習に使用できません。

  - **Listening** — ポートは現在 Listening モードです。ポートはトラフィックの転送ができず、MAC アドレスの学習もできません。

  - **Learning** — ポートは現在 Learning モードです。ポートはトラフィックの転送はできませんが、新しい MAC アドレスの学習はできます。

  - **Forwarding** — ポートは現在 Forwarding モードです。ポートはトラフィックの転送ができ、新しい MAC アドレスの学習ができます。

- **Speed** — ポートの速度を示します。可能なフィールド値には、以下のものがあります。

  - **10M**

  - **100M**

  - **1000M**

- Path Cost — このポートが Root Path Cost に使用される量を示します。Path Cost 値は高く、または低く調整することができ、再経路指定されたパスにトラフィックを転送したり、トラフィックが行かないようにできます。パスコストには、1 ～ 65,535 の値があります。

- **Default Path Cost** — デフォルト Path Cost を指定します。

- **Priority** — ポートの優先度値を示します。優先度値は、ブリッジに同じ LAN 上のループに接続されたポートが 2 つある場合、ポートの選択に影響します。優先度値は、0 ～ 255 の間です。

- **Designated Bridge ID** — 指定されたブリッジの優先度と MAC アドレスを示します。

- **Designated Port** — 指定されたブリッジで選択されたポートの優先度と MAC アドレスを示します。

- **Designated Cost** — STP トポロジに参加している指定ポートのコストを示します。

- **Forward Transitions** — ポートが **Blocking** 状態から **Forwarding** に変更された回数を示します。

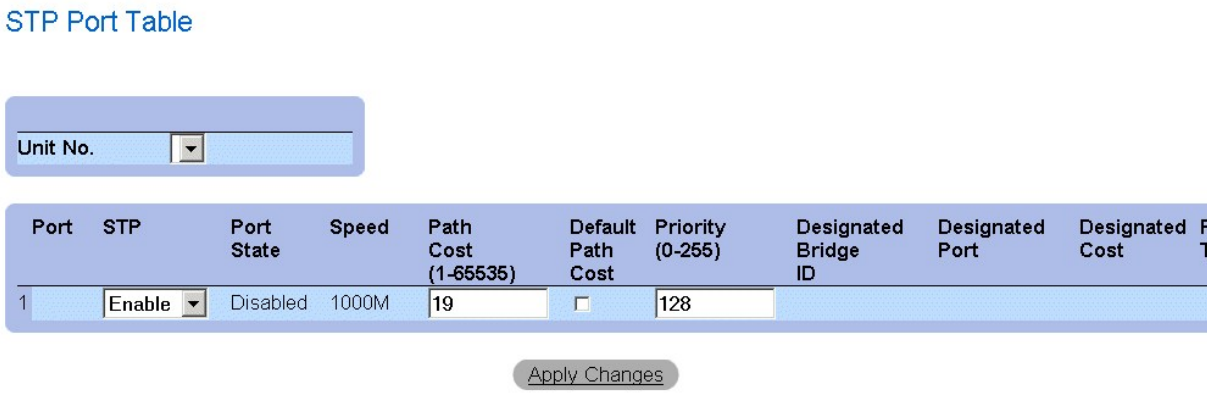
- **LAG** — ポートが接続されている LAG を示します。

ポートで STP を有効にするには、次の手順を実行します。

1. **STP Port Settings** ページを開きます。
2. STP フィールドで **Enabled** を選びます。
3. **Priority**、**Path Cost**、**Default Path Cost**、および **Fast Link** フィールドを定義します。
4. **Apply Changes** をクリックします。STP がポートで有効になります。

STP ポートのプロパティを変更するには、次の手順を実行します。

1. **STP Port Settings** ページを開きます。
2. **Priority**、**Path Cost**、**Default Path Cost**、および **Fast Link** フィールドを変更します。
3. **Apply Changes** をクリックします。STP ポートパラメータが変更され、デバイスがアップデートされます。



STP Port Table ページ

CLI コマンドを使用した STP ポートパラメータの定義

次の表に、 **STP Port Settings** ページで表示される STP ポートパラメータの定義に対応する CLI コマンドをまとめます。

CLI コマンド	説明
spanning-tree disable	特定のポートで Spanning Tree を無効にします。
spanning-tree cost *cost*	ポートの Spanning Tree ポートコストを設定します。
spanning-tree port-priority priority	ポート優先度を設定します。
show spanning-tree [ethernet *interface* **| port-channel** *port-channel-number*]	Spanning Tree 設定を表示します。
spanning-tree portfast	PortFast モードを有効にします。

以下に、CLI コマンドの例を示します。

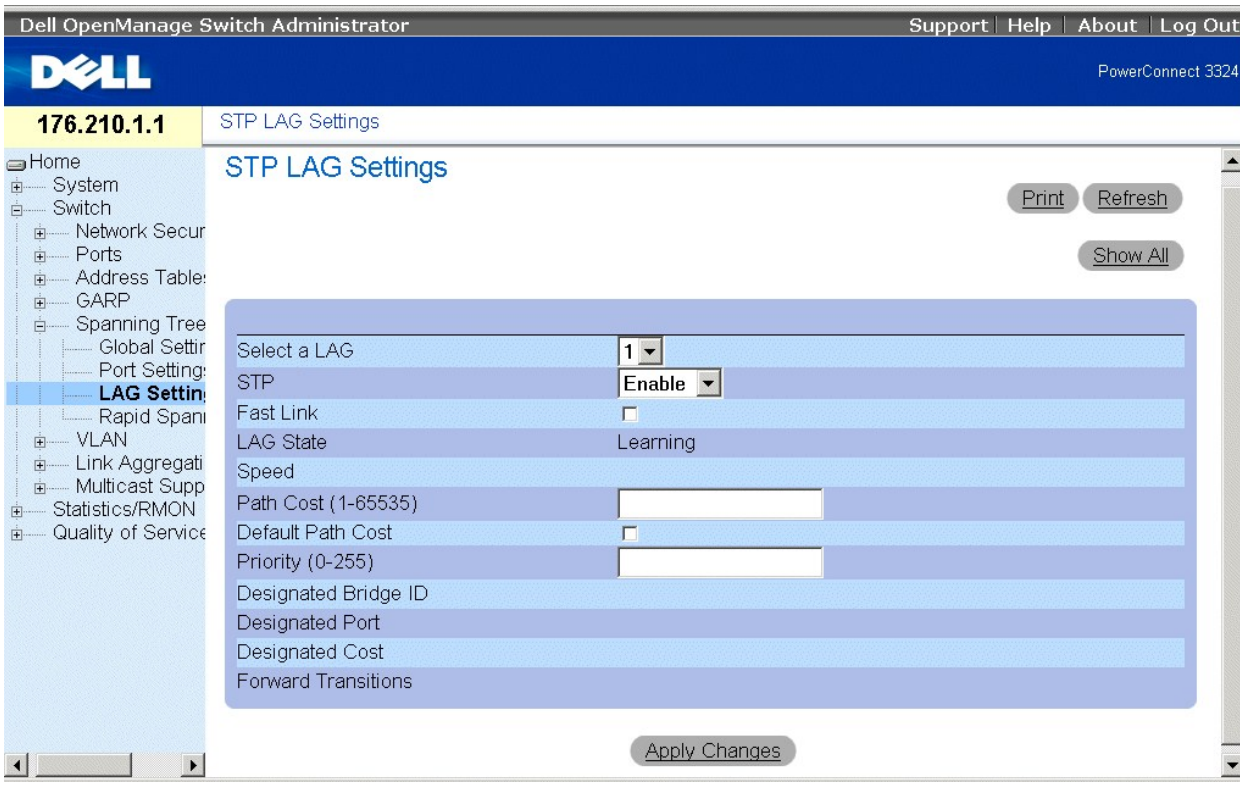
```
Console (config)# interface ethernet 1/e5

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console (config-if)# exit

Console (config)# exit

Console# show spanning-tree ethernet 1/e5
```

```
Console# show spanning-tree ethernet 1/e5

Interface Port ID Designated Port ID

Name Prio Sts Enb Cost Cost Bridge ID Prio.Nbr

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

1/e5 128 DSBL True 100 0 8000 xx.xx.xx.xx.xx.xx 80 001

Spanning tree enabled

Port Fast:no (configured:no)

éÌó\xde :point-to-point (configured:auto)

Number of transitions to forwarding state: 1

BPDU:sent 2, received 120638
```

STP LAG 設定の定義

STP LAG Settings ページを使用して、ネットワーク管理者は LAG の STP パラメータの割り当てができます。**STP LAG Settings** ページを開くには、次の手順を実行します。

1. Tree View で、**Switch** → **Spanning Tree** → **LAG Settings** とクリックします。**STP LAG Settings** ページが開きます。



STP LAG Settings ページ

STP LAG Settings ページには、以下のフィールドが含まれています。

- **Select a LAG** — ユーザー定義の LAG を示します。このプログラムの詳細は、「LAG メンバーシップの定義」を参照してください。
- **STP** — LAG で STP を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — LAG で STP を有効にします。
  - **Disable** — LAG で STP を無効にします。
- **Fast Link** — LAG で Fast Link を有効にします。Fast Link が LAG で有効な場合、LAG は自動的に **Forwarding** 状態になります。Fast Link は、STP プロトコルが収束するまでにかかる時間を最適化します （STP 収束は大規模ネットワークでは 30 ～ 60 秒かかることがあります）。

メモ: **Fast Link** オプションは、デバイスがエンドステーションの STP ネットワークトポロジのリーフである場合など、適切な場合にのみ使用してください。

- **LAG State** — LAG の現在の STP 状態を示します。有効な場合、LAG State はトラフィックの転送アクションを決定します。ブリッジが誤動作している LAG を検出した場合、LAG は **Disabled** 状態になります。可能なフィールド値には、以下のものがあります。
  - **Disabled** — 現在リンクがダウンしていることを示します。
  - **Blocking** — LAG は現在ブロックされ、トラフィックの転送や MAC アドレスの学習に使用できません。
  - **Listening** — LAG は現在 Listening モードです。LAG はトラフィックの転送や MAC アドレスの学習はできません。
  - **Learning** — LAG は現在 Learning モードです。LAG はトラフィックの転送はできませんが、新しい MAC アドレスの学習はできます。
  - **Forwarding** — LAG は現在 Forwarding モードです。LAG はトラフィックの転送ができ、新しい MAC アドレスの学習ができます。
- **Speed** — LAG を構成しているポートの速度です。
- **Path Cost (1-65535)** — この LAG が Root Path Cost に使用される量を示します。Path Cost 値は高く、または低く調整することができ、再経路指定されたパスにトラフィックを転送したり、トラフィックが行かないようにできます。パスコストには、1～ 65,535 の値があります。
- **Default Path Cost** — デフォルト Path Cost を指定します。LAG のデフォルト Path Cost は 4 です。

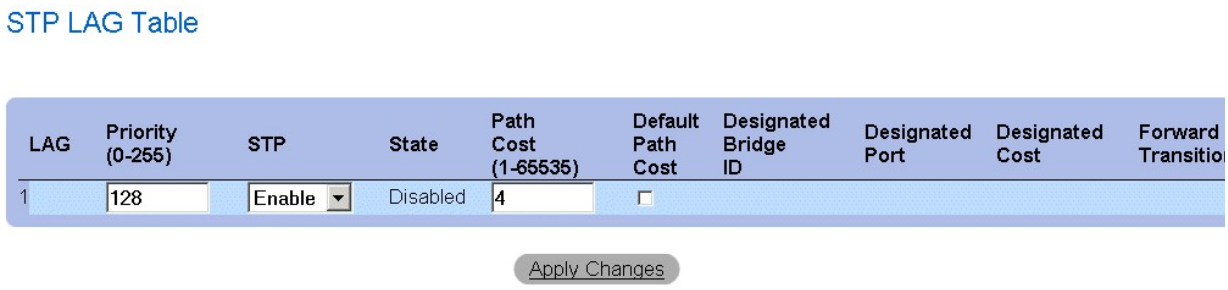
- **Priority (0-255)** — LAG の優先度値を示します。優先度値は、ブリッジに同じ LAN 上のループに接続されたポートが 2 つある場合、 LAG の選択に影響します。優先度値は、0 ～ 255 の間です。
- **Designated Bridge ID** — 指定されたブリッジの優先度および MAC アドレスを示します。
- **Designated Port** — 選択されたポートの優先度および MAC アドレスを示します。
- **Designated Cost** — 指定されたコストを示します。
- **Forward Transitions** — ポートが **Blocking** 状態から **Forwarding** に変更された回数を示します。

LAG で STP を有効にするには、次の手順を実行します。

1. **STP LAG Table** ページを開きます。
2. STP フィールドで **Enabled** を選びます。
3. **Fast Link**、**Path Cost (1-65535)**、**Default Path Cost** および **Priority (0- 255)** フィールドを定義します。
4. **Apply Changes** をクリックします。LAG で STP が有効になり、デバイスがアップデートされます。

LAG STP パラメータを変更するには、次の手順を実行します。

1. **STP LAG Table** ページを開きます。
2. **Fast Link**、**Path Cost (1-65535)**、**Default Path Cost** および **Priority (0-255)** フィールドを変更します。
3. **Apply Changes** をクリックします。STP LAG パラメータが変更され、デバイスがアップデートされます。



STP LAG Table ページ

CLI コマンドを使用した STP LAG パラメータの定義

次の表に、 **STP LAG Settings** ページで表示される STP LAG パラメータの定義に対応する CLI コマンドをまとめます。

CLI コマンド	説明
interface port-channel *port-channel-number*	ポートチャネル設定モードを起動します。
spanning-tree port-priority *priority*	LAG 優先度を設定します。

以下に、CLI コマンドの例を示します。

```
console(config)# interface port-channel 1

console(config-if)# spanning-tree port-priority 16
```

Rapid Spanning Tree の設定

Classic Spanning Tree は、一般的なネットワークトポロジでの L2 転送ループを防ぎます。ただし、収束には 30 ～ 60 秒かかることがあります。収束にかかる時間は、多くのアプリケーションで長すぎると考えられます。ネットワークトポロジで可能な場合は、より速い収束が可能な場合もあります。RSTP (Rapid Spanning Tree Protocol) は、転送ループを作成することなく、スパニングツリーの収束時間を短くできるネットワークトポロジを検索して、使用します。

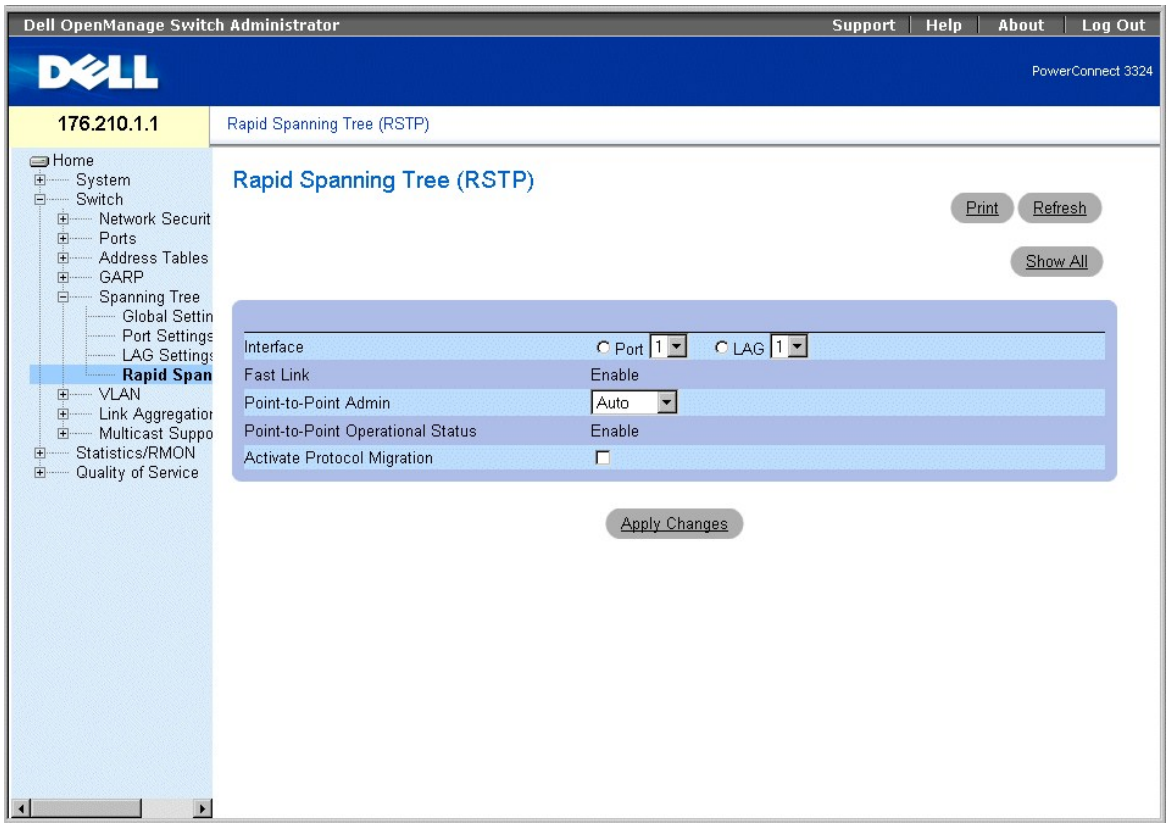
STP には、以下の異なるポート状態があります。

- Listening
- Learning
- Blocking
- Forwarding

Listening ポートは、指定ポートまたはルートポートで、転送状態への移行を処理しています。ただし、ポートが Forwarding 状態になったら、ポートがルートポートまたは指定ポートかを確認することはできません。RSTP は、ポートの役割と状態を切り離すことによってこの問題に対処します。**Spanning Tree Global Settings** ページを使用して、RSTP を有効にします。

Rapid Spanning Tree (RSTP) ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Spanning Tree** → **Rapid Spanning Tree** とクリックします。**Rapid Spanning Tree (RSTP)** ページが開きます。



Rapid Spanning Tree (RSTP) ページ

Rapid Spanning Tree (RSTP) ページには、以下のフィールドが含まれています。

- **Interface** — RSTP が有効になっているインタフェース番号を示します。
- **Fast Link** — Fast Link が有効になっているかどうかを示します。

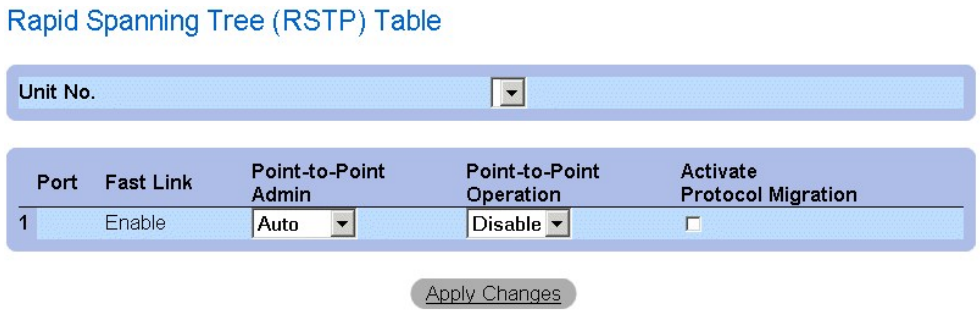
メモ: Fast Link は、**STP Port Settings** ページまたは **STP LAG Settings** ページで有効になります。Fast Link の有効化の詳細については、「Defining STP Port Settings」または「STP LAG 設定の定義」を参照してください。

- **Point-to-Point Admin** — ポートリンクタイプをポイントツーポイントに指定します。可能なフィールド値には、以下のものがあります。
  - **Auto** — デバイスは自動的にポイントツーポイントリンクを検出できます。
  - **Enable** — ポイントツーポイントリンクを確立できます。
  - **Disable** — ポイントツーポイントリンクを確立できません。
- **Point-to-Point Operational Status** — ポイントツーポイント動作の状態を示します。
- **Activate Protocol Migration** — プロトコル移行をアクティブにします。プロトコル移行を使用して、ポートが RSTP に移行できるかをテストし、プロトコルの周囲のスイッチとの再ネゴシエーションが可能になります。可能なフィールド値には、以下のものがあります。
  - **Checked** — プロトコル移行をアクティブにします。
  - **Unchecked** — プロトコル移行を無効にします。

Rapid STP を有効にするには、次の手順を実行します。

1. **Rapid Spanning Tree (RSTP)** ページを開きます。
2. **Point-to-Point Admin**、**Protocol Operation**、および **Activate Protocol Migration**フィールドを定義します。

3. **Apply Changes** をクリックします。RSTP が有効になり、デバイスがアップデートされます。



Rapid Spanning Tree (RSTP) Table

CLI コマンドを使用した Rapid STP パラメータの定義

次の表に、**Rapid Spanning Tree (RSTP)** ページで表示される RSTP パラメータの定義に対応する CLI コマンドをまとめます。

CLI コマンド	説明
spanning-tree link-type {point-to-point | shared}	デフォルトのリンクタイプ設定を置き換えます。 これは、ポートの二重方式モードで決定され、RSTP (Rapid Spanning-Tree Protocol) は、Forwarding 状態へ移行できるようになります。
spanning tree mode {stp |rstp}	現在実行されている RSTP を設定します。
clear spanning-tree detected-protocols	プロトコル移行プロセスを再開します。
show spanning-tree [ethernet interface | port-channel port-channel-number]	RSTP 設定を表示します。

以下に、CLI コマンドの例を示します。

```
Console (config)# interface ethernet 1/e5

Console(config-if)# spanning-tree link-type shared
```

VLAN の設定

VLAN は、ハードウェアソリューションの定義によるものではなく、ソフトウェアが作成した LAN (ローカルエリアネットワーク) の論理サブグループです。VLAN は、接続されている物理的な LAN セグメントに関係なく、ユーザーステーションとネットワークデバイスを 1 つのドメインに統合します。VLAN を使用して、ネットワークトラフィックがサブグループ内でより効率的に流れるようになります。ソフトウェアで管理されている VLAN は、ネットワークへの変更が導入される時間を低減します。

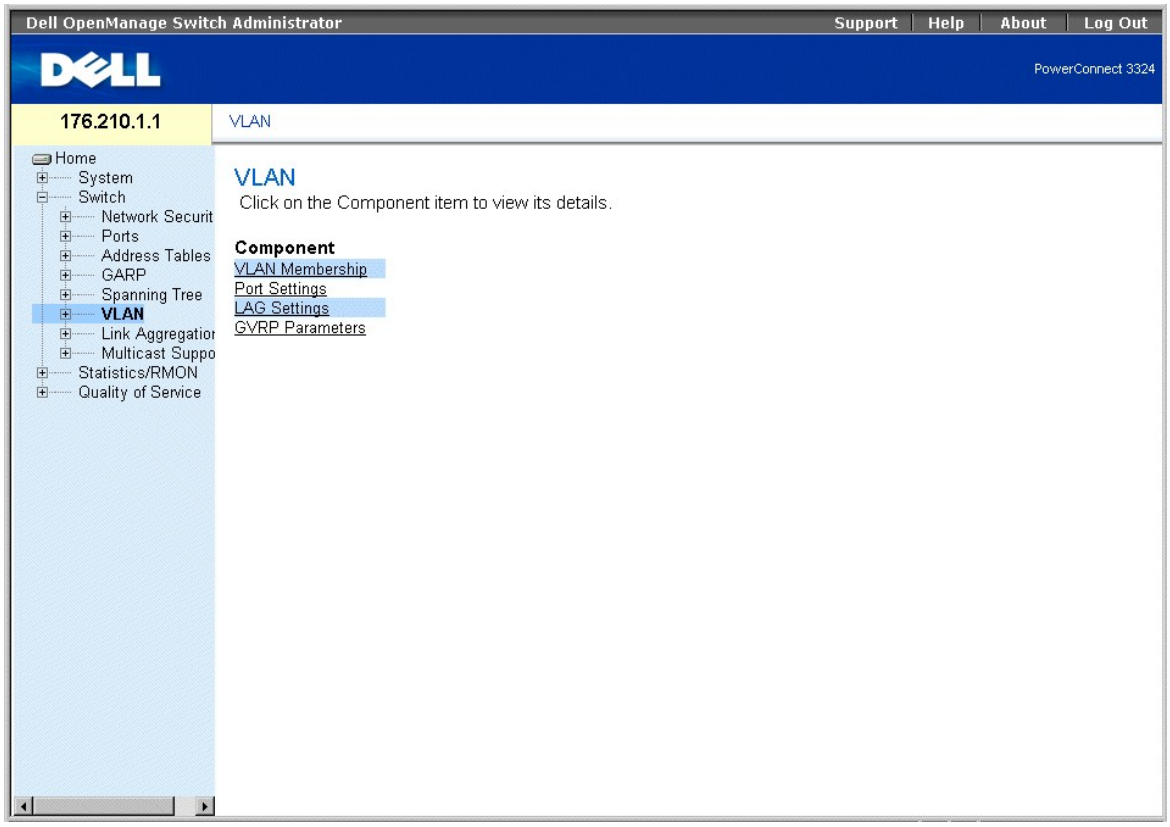
VLAN はソフトウェアベースで、物理的な属性で定義されていません。その結果、VLAN にポートを無限に設定することができ、ユニット、デバイス、スタック、またはその他の論理接続の組み合わせごとに VLAN を作成することができます。

VLAN は Layer 2 で動作します。 VLAN は VLAN 内でトラフィックを分離しますので、VLAN 間でトラフィックが流れるように Layer 3 で動作しているルータが必要です。Layer 3 ルータはセグメントを認識し、VLAN と調整します。VLAN はブロードキャストおよびマルチキャストドメインです。ブロードキャストおよび

マルチキャストトラフィックは、トラフィックが生成される VLAN でのみ送信されます。

VLAN のタグ付けは、VLAN グループ間の VLAN 情報の伝達方法を提供します。VLAN のタグ付けは、パケットのヘッダーに 4 バイトのタグを付けます。VLAN タグは、どの VLAN にパケットが属するかを示します。VLAN タグは、エンドステーションまたはネットワークデバイスのどちらかで、パケットに付けられています。VLAN タグは、VLAN ネットワーク優先度情報も含んでいます。VLAN と GVRP を組み合わせることにより、ネットワーク管理者は、VLAN 情報を自動的に伝えることができます。 **VLAN** ページを表示するには、次の手順を実行します。

- Tree View で、**Switch** → **VLAN** とクリックします。**VLAN** ページが開きます。



VLAN ページ

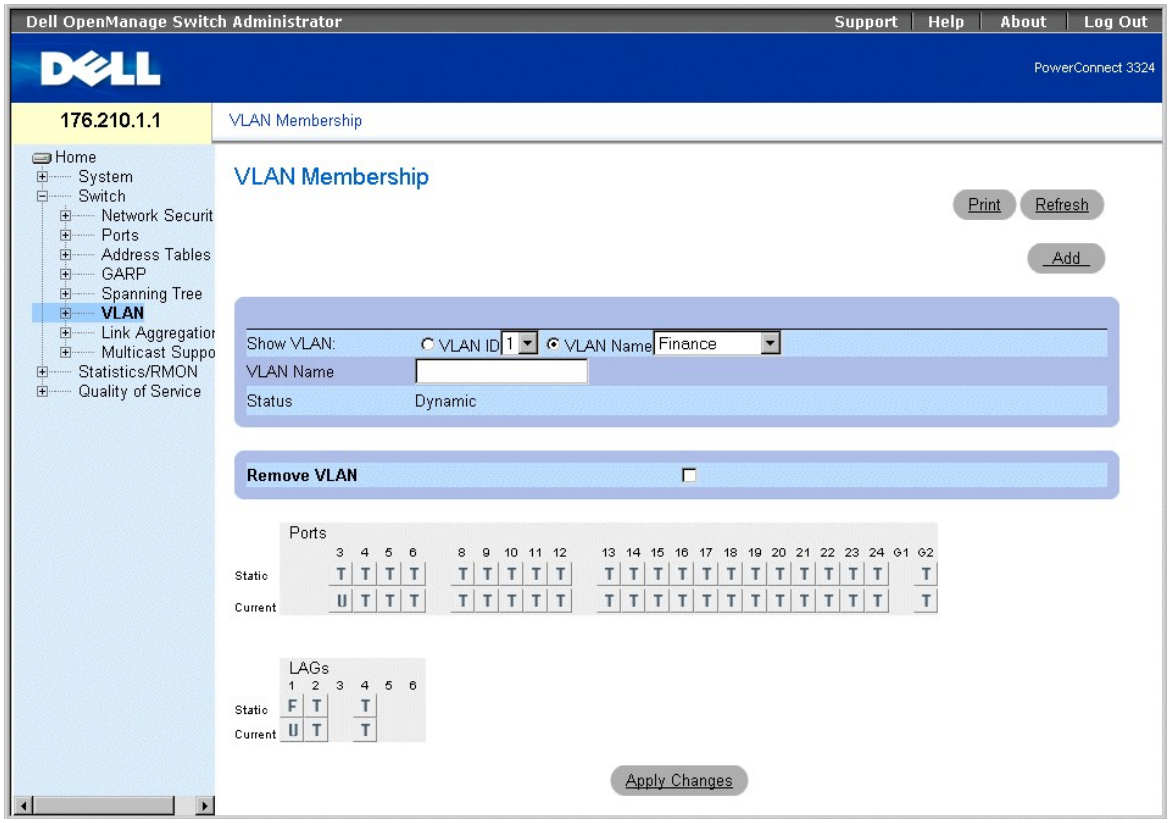
VLAN ページには、以下のものを定義するリンクが含まれています。

- VLAN メンバーの定義
- VLAN ポート設定の定義
- VLAN LAG 設定の定義
- GVRP の設定

VLAN メンバーの定義

VLAN Membership ページを使用して、ネットワーク管理者は、VLAN グループを定義できます。**VLAN Membership** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **VLAN** → **VLAN Membership** とクリックします。**VLAN Membership** ページが開きます。



VLAN Membership ページ

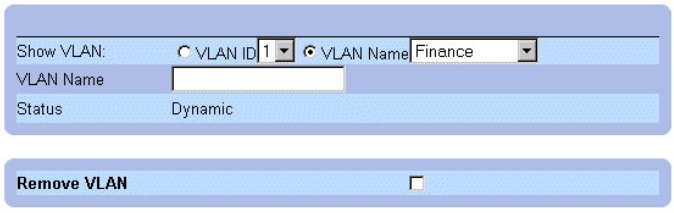
VLAN Membership ページは、以下の項目に分かれています。

- VLAN メンバーシップ
- VLAN ポートメンバーシップテーブル
- VLAN LAG 設定の定義

VLAN メンバーシップ

VLAN Membership セクションには、ポートに VLAN メンバーシップを割り当てるためのパラメータが含まれています。PowerConnect 3324/3348 は、最大で 256 の VLAN に対応しています。

メモ: すべてのポートに、定義済みの PVID が必要です。他の値が設定されていない場合、デフォルトの VLAN PVID を使用します。



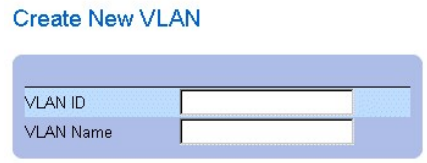
VLAN メンバーシップ

VLAN Membership セクションには、以下のフィールドが含まれています。

- **Show VLAN** — 以下に従って特定の VLAN 情報を一覧表示します。
  - **VLAN ID** — VLAN IDで VLAN を表示します。 VLAN のデフォルト ID は 1 です。 VLAN に 現在のポートデフォルト VLAN ID（PVID） である ID があり、その ID がポートから削除された場合、PVID は 1 に設定されます。VLAN 番号 1 はシステムから削除できません。 VLAN の範囲は 1 ～ 4095 です。 VLAN 4095 は Discard VLAN です。
  - **VLAN Name** — VLAN 名で VLAN を表示します。
- **VLAN Name** — VLAN のユーザー名を表示、または定義します。
- **Status** — VLAN タイプを示します。VLAN は、ユーザー定義 （恒久的） で、GVRP で作成されるかまたはデフォルトの VLAN です。可能なフィールド値には、以下のものがあります。
  - **Dynamic** — VLAN が動的に GVRP を介して作成されたことを示します。
  - **Static** — VLAN がユーザー定義であることを示します。
  - **Default** — VLAN はデフォルトの VLAN であることを示します。
- **Remove VLAN** — VLAN を **VLAN Membership Table** から削除します。可能なフィールド値には、以下のものがあります。
  - **Checked** — VLAN グループを VLAN Membership Table から削除します。
  - **Unchecked** — VLAN グループを VLAN Membership Table で保持します。

新しい VLAN を追加するには、次の手順を実行します。

1. **VLAN Membership** ページを開きます。
2. **Add** （追加）をクリックします。**Create New VLAN** ページが開きます。



Create New VLAN ページ

3. **VLAN ID** および **VLAN Name** フィールドを定義します。
4. **Apply Changes** をクリックします。新しい VLAN が追加され、デバイスがアップデートされます。

VLAN 名グループを変更するには、次の手順を実行します。

1. **VLAN Membership** ページを開きます。
2. **Show VLAN** フィールドで VLAN を選びます。
3. **VLAN Name** フィールドを変更します。
4. **Apply Changes** をクリックします。VLAN メンバーシップ情報が変更され、デバイスがアップデートされます。

VLAN を削除するには、次の手順を実行します。

1. **VLAN Membership** ページを開きます。
2. **Show VLAN** フィールドで VLAN を選びます。
3. **Remove** チェックボックスにチェックマークを付けます。

4. **Apply Changes** をクリックします。VLAN が削除され、デバイスがアップデートされます。

CLI コマンドを使用した VLAN メンバーシップグループの定義

次の表に、**VLAN Membership** ページで表示される VLAN メンバーシップの定義に対応する CLI コマンドをまとめます。

CLI コマンド	説明
vlan database	インタフェース設定 （VLAN） モードを起動します。
vlan {*vlan-range***}**	VLAN を作成します。
name *string*	VLAN に名前を付けます。

以下に、CLI コマンドの例を示します。

```
Console # vlan database

Console (config-switch)#

Console (config-switch)# vlan 1972

Console (config-switch)# exit

Console (config)# interface vlan 19

Console (config-if)# name Marketing
```

VLAN ポートメンバーシップテーブル

VLAN Port Membership Table には、VLAN へのポートの割り当て用のポートテーブルが含まれています。ポートには、ポート制御設定の切り替えを介して、 VLAN メンバーシップが割り当てられています。ポートは、以下の値を持つことができます。

VLAN ポートメンバーシップ制御設定

ポート制御	定義
T	インタフェースは VLAN のメンバーです。インタフェースが転送したすべてのパケットはタグ付けされます。パケットには VLAN 情報が含まれています。
U	インタフェースはこのメンバーのメンバーです。インタフェースが転送したパケットはタグ付けされません。
F	インタフェースは、GVRP を介した VLAN へのメンバーシップが認められていません。
消灯	インタフェースはこの VLAN のメンバーではありません。VLAN に関連したパケットは転送されません。

メモ： LAG メンバーのポートは、VLAN Port Membership Table には表示されません。

VLAN Port Membership Table は、ポート、ポートの状態、および LAG を表示します。

VLAN ポートメンバーシップテーブル

ポートを VLAN グループに割り当てるには、次の手順を実行します。

1. **VLAN Membership** ページを開きます。
2. **Show VLAN** ドロップダウンリストから VLAN を選びます。
3. **Port Membership Table** でポートを選び、ポートに値（**v**、**t**、**f**、または **Blank**) を割り当てます。
4. **Apply Changes** をクリックします。ポートが VLAN グループに割り当てられ、デバイスがアップデートされます。

VLAN を削除するには、次の手順を実行します。

1. **VLAN Membership** ページを開きます。
2. **Show VLAN** ドロップダウンリストから VLAN を選びます。
3. **Remove** チェックボックスにチェックマークを付けます。
4. **Apply Changes** をクリックします。VLAN グループが削除され、デバイスがアップデートされます。

CLI コマンドを使用したポートの VLAN グループへの割り当て

次の表に、 **VLAN Membership** ページで表示されるポートのVLAN グループへの割り当てに対応する CLI コマンドをまとめます。

CLI コマンド	説明
vlan database	インタフェース設定 （VLAN） モードを起動します。
vlan {*vlan-range***}**	VLAN を作成または削除します。
interface vlan *vlan-id*	インタフェース設定 （VLAN） モードを起動して、既存の VLAN を設定します。
name *string*	VLAN に名前を付けます。
interface range ethernet {*port-range* **| all}**	同時に複数のポートでコマンドを実行できます。
switchport forbidden vlan {add vlan-list | remove vlan-list}	ポートへの特定の VLAN の追加ができなくなります。

以下に、CLI コマンドの例を示します。

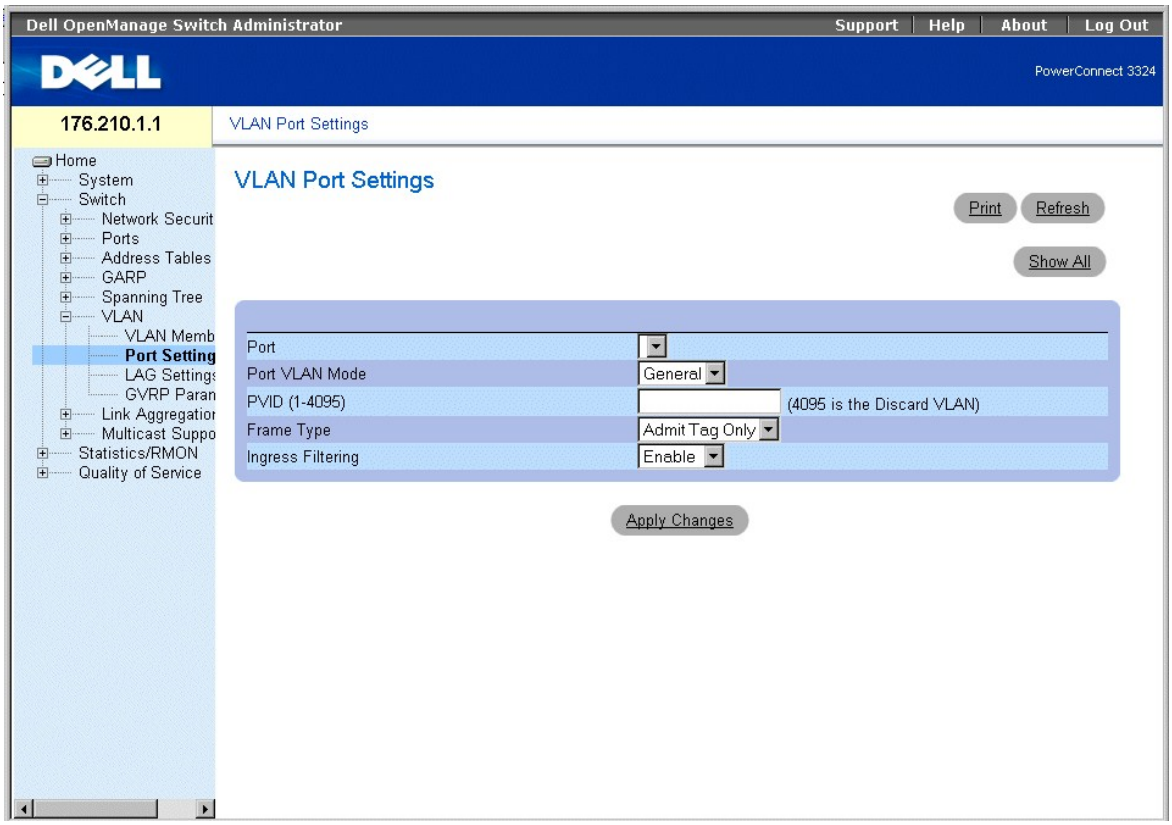
```
Console # vlan database

Console (config-vlan)# vlan 1972

Console (config-vlan)# exit

Console (config)# interface vlan 1972

Console (config-if)# name Marketing

Console (config-if)# exit

Console (config)# interface range ethernet 1/e18 - e20
```

VLAN ポート設定の定義

VLAN Port Settings ページでは、VLAN の一部である管理ポートのパラメータを提供します。

Port Default VLAN ID (PVID) は、**VLAN Port Settings** ページで設定されます。
デバイスに着いたすべてのタグなしパケットは、ポートの PVID でタグ付けされます。**VLANPort Settings** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **VLAN** → **Port Settings** とクリックします。**VLANPort Settings** ページが開きます。



VLAN Port Settings ページ

VLAN Port Settings ページには、以下のフィールドが含まれています。

- **Port** — VLAN に含まれているポート番号を示します。
- **Port VLAN Mode** — ポート VLAN モードを指定します。 可能なフィールド値には、以下のものがあります。
  - **General** — ポートが 1 つまたは複数の VLAN に属していて、各 VLAN はユーザーによってタグ付きまたはタグなしと定義されていることを示します (完全 802.1Q モード)。Ingress Filtering は、一般モードポートでのみ無効にできます。
  - **Access** — ポートは、単一のタグなし VLAN に属することを示します。ポート VLAN モードをアクセスに定義すると、ポートはすべてのタグなしフレームと、ポートの PVID として現在設定されている VID でタグ付けされているフレームすべてを受け入れます。アクセスモードポートは、特にエンドステーションが VLAN タグを生成できない際、エンドステーションとシステム間にリンクを確立するようになっています。Ingress Filtering が有効になっています。
  - **Trunk** — ポートは、すべてのフレームがタグ付けされる VLAN に属していることを示します。Ingress Filtering は、トランクモードポートで有効になっています。
- **PVID (1-4095)** — VLAN ID をタグなしパケットに割り当てます。これは、一般モードポートでのみ実行されます。可能なフィールド値の範囲は、1 ～ 4095 です。

メモ: VLAN 4095 は、Discard VLAN です。

- **Frame Type** — ポートで受け入れられるパケットタイプを示します。可能なフィールド値には、以下のものがあります。
  - **Admit Tag Only** — タグ付きパケットのみがポートで受け入れられることを示します。
  - **Admit All** — タグ付きおよびタグなしパケットの両方がポートで受け入れられることを示します。
- **Ingress Filtering** — ポートで Ingress Filtering を有効にします。Ingress Filtering は、進入ポートを含まない VLAN に関連するパケットを破棄します。可能なフィールド値には、以下のものがあります。
  - **Enable** — ポートで Ingress Filtering を有効にします。
  - **Disable** — ポートで Ingress Filtering を無効にします。

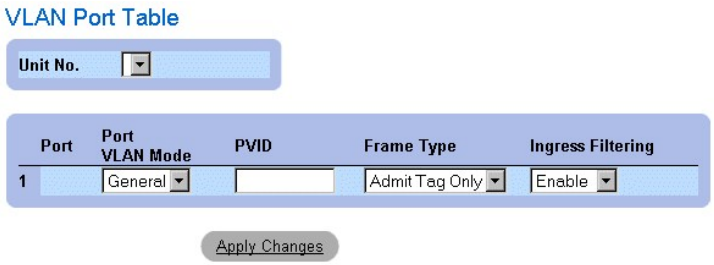
ポート設定を割り当てるには、次の手順を実行します。

メモ: Ingress Filtering は、一般 VLAN モードに設定されているポートでのみ無効にできます。

1. **VLAN Port Settings** ページを開きます。
2. **LAG VLAN Mode**、**PVID (1-4095)**、**Frame Type**、および **Ingress Filtering** フィールドを定義します。
3. **Apply Changes** をクリックします。VLAN ポートパラメータが定義され、デバイスがアップデートされます。

VLAN Port Table を表示するには、次の手順を実行します。

1. **VLAN Port Settings** ページを開きます。
2. **Show All** をクリックします。**VLAN Port Table** ページが開きます。



VLAN Port Table ページ

VLAN Port Settings ページのフィールドに加えて、**VLAN Port Table** ページには以下のフィールドも表示されます。

- **Unit No.** — ポート情報が表示されている VLAN のスタッキングユニット番号を表示します。

CLI コマンドを使用したポートの VLAN グループへの割り当て

次の表に、**VLAN Port Settings** ページで表示される VLAN グループへのポートの割り当てに対応する CLI コマンドをまとめます。

CLI コマンド	説明
interface ethernet *interface*	Ethernet タイプのインタフェースを設定するインタフェース設定モードを起動します。
switchport mode {access | trunk | general}	ポート VLAN メンバーシップモードを設定します。
switchport general pvid *vlan-id*	インタフェースが一般モードの際に、Port VLAN ID (PVID) を設定します。
switchport general allowed vlan add *vlan-list* **[tagged | untagged]**	VLAN を一般ポートに追加します。
switchport general allowed vlan remove *vlan-list*	VLAN を一般ポートから削除します。

switchport general ingress-filtering disable	Ingress Filtering を無効にします。

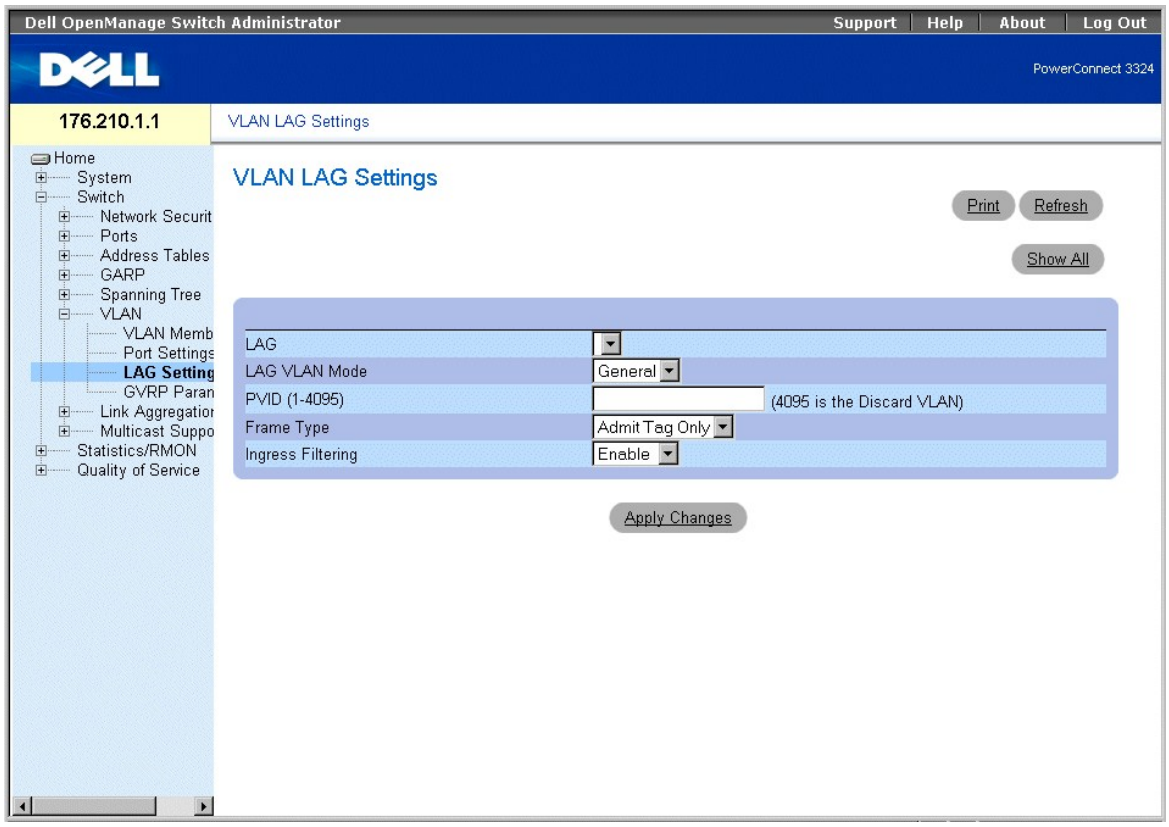
以下に、CLI コマンドの例を示します。

```
Console (config)# interface range ethernet 1/e18 - e20

Console (config-if)# switchport mode access

Console (config-if)# switchport general pvid 234

Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged

Console (config-if)# switchport general ingress-filtering disable
```

VLAN LAG 設定の定義

VLAN LAG Settings ページでは、VLANの一部である LAG の管理のパラメータを提供します。VLAN は、個々のポートまたは LAG で構成されています。LAG のスイッチに入ってくるタグなしパケットは、LAG の PVID で指定されたタグでタグ付けされます。**VLANLAG Settings** ページを開くには、次の手順を実行します。

- Tree View で、**Switch → VLAN → LAG Settings** とクリックします。**VLANLAG Settings** ページが開きます。



VLAN LAG Setting ページ

VLAN LAG Settings ページには、以下のフィールドが含まれています。

- **LAG** — VLAN に含まれている LAG 番号を示します。
- **LAG VLAN Mode** — ポートモードを示します。可能なフィールド値には、以下のものがあります。
  - **General** — LAG が 1 つまたは複数の VLAN に属していて、各 VLAN はユーザーによってタグ付きまたはタグなしと定義されていることを示します (完全 802.1Q 準拠)。
  - **Access** — LAG は、単一のタグなし VLAN に属することを示します。
  - **Trunk** — LAG が、すべてのフレームがタグ付けされる VLAN に属していることを示します （オプションの単一のネイティブ VLAN は除きます）。
- **PVID (1-4095)** — VLAN ID をタグなしパケットに割り当てます。LAG が PVID を割り当てるには、LAG は**VLAN Port Membership Table** でタグなしと定義されている必要があります。
- **Frame Type** — LAG で受け入れられるパケットタイプを示します。可能なフィールド値には、以下のものがあります。
  - **Admit Tag Only** — タグ付きパケットのみが LAG で受け入れられることを示します。
  - **Admit All** — タグ付きおよびタグなしパケットの両方が LAG で受け入れられることを示します。
- **Ingress Filtering** — LAG で Ingress Filtering を有効にします。Ingress Filtering は、進入ポートを含まないパケットを破棄します。可能なフィールド値には、以下のものがあります。
  - **Enable** — LAG で Ingress Filtering を有効にします。
  - **Disable** — LAG で Ingress Filtering を無効にします。

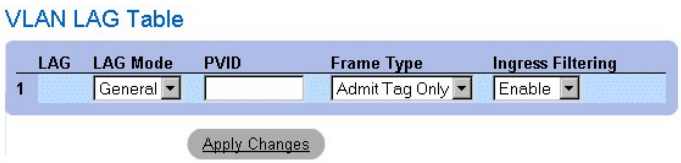
LAG 設定を割り当てるには、次の手順を実行します。

1. **VLAN LAG Settings** ページを開きます。

2. **LAG VLAN Mode**、**PVID (1-4095)**、**Frame Type**、および **Ingress Filtering** フィールドを定義します。
3. **Apply Changes** をクリックします。VLAN LAG パラメータが定義され、デバイスがアップデートされます。

VLAN LAG Table を表示するには、次の手順を実行します。

1. **VLAN LAG Settings** ページを開きます。
2. **Show All** をクリックします。**VLAN LAG Table** が開きます。



VLAN LAG Table

CLI コマンドを使用した LAG の VLAN グループへの割り当て

次の表に、**VLAN LAG Settings** ページで表示される LAG の VLAN グループへの割り当てに対応する CLI コマンドをまとめます。

CLI コマンド	説明
switchport mode {access | LAG | general}	ポート VLAN メンバーシップモードを設定します。
switchport LAG native vlan *vlan-id*	指定された VLAN のメンバーとして LAG を定義し、VLAN ID を 「ポートデフォルト VLAN ID (PVID)」 として定義します。
switchport general pvid *vlan-id*	インタフェースが一般モードの際に、Port VLAN ID (PVID) を設定します。
switchport general allowed vlan add *vlan-list* **[tagged | untagged]**	VLAN を一般ポートに追加します。
switchport general allowed vlan remove *vlan-list* **[tagged | untagged]**	VLAN を一般ポートから削除します。
switchport general acceptable-frame-types tagged-only	進入時にタグなしフレームを破棄します。
switchport general ingress-filtering off	Ingress Filtering を無効にします。

以下に、CLI コマンドの例を示します。

```
Console (config)# interface port channel 1 1/e8

Console (config-if)# switchport mode access

console (config-if)# switchport LAG 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-types tagged-only
```

```
Console (config-if)# switchport general ingress-filtering disable
```

GVRP の設定

GVRP (GARP VLAN Registration Protocol) プロトコルは、VLAN 認識ブリッジへの VLAN メンバーシップ情報の自動通知のために提供されています。GVRP を使用して、VLAN 認識ブリッジは、VLAN を自動的に学習し、個々にブリッジを設定する必要なくポートマッピングのブリッジをおこない、VLAN メンバーシップを登録します。

GVRP プロトコルを実行中のメモリ必要量を最小限にするため、2 つの調整変数が標準変数に追加されています。

- **Maximum number of GVRP VLANs** — GVRP 動作に参加できる GVRP VLAN の数を表示します。
- **Maximum number of GVRP VLANs after Reset** — GVRP VLAN および調整に使用される別の値を設定します。この値は、リセット後にのみ有効になります。

GVRP VLAN の最大数には、静的または動的 VLAN にかかわらず、GVRP 動作に参加しているすべての VLAN が含まれます。

リセット後の GVRP VLAN の最大数を設定して、GVRP に参加している VLAN の最大数を指定する際に、以下のことを考慮する必要があります。

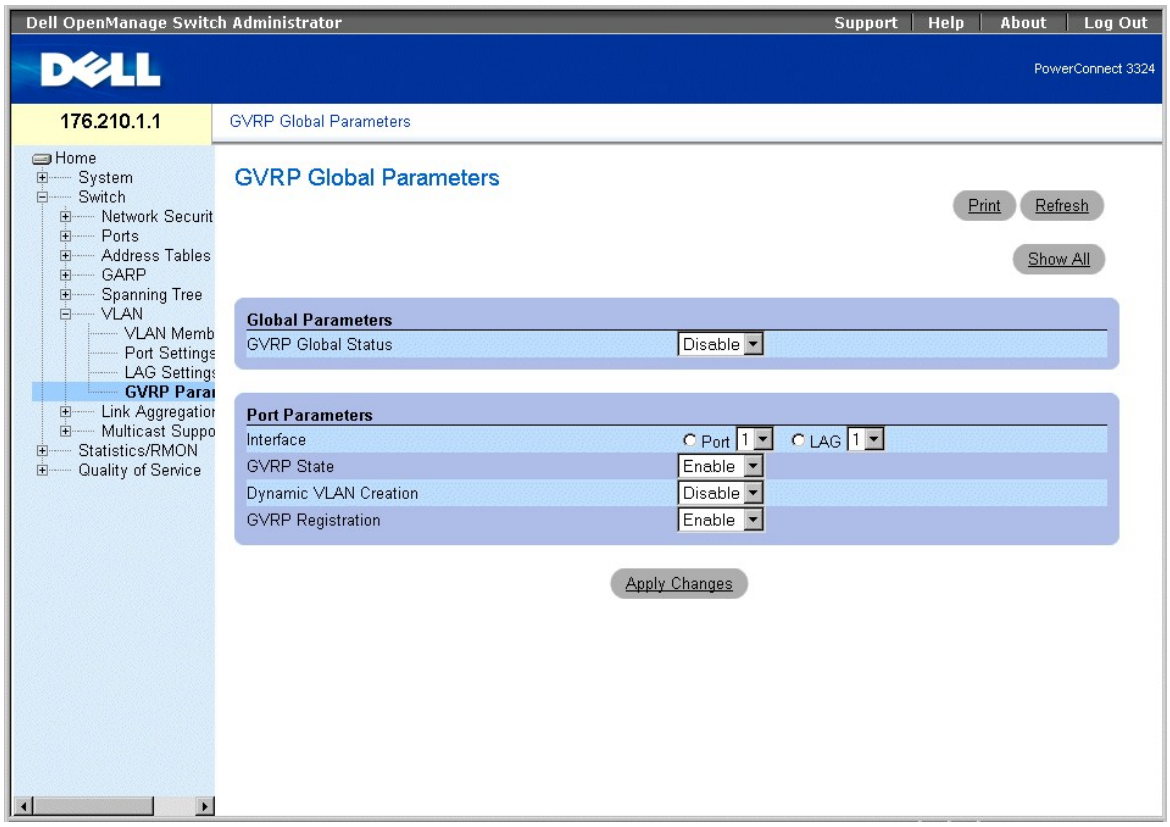
- デフォルトの GVRP VLAN の最大数は、メモリによる制限のため、128 です。
- VLAN の最大数 （Max VLANs MIB 変数で管理されます） は、GVRP VLAN の最大数を制限します。

GVRP プロトコルが正しく機能するように、GVRP VLAN の最大数を以下の合計を大きく超えた値に設定するようお勧めします。

- 現在設定されているものと、今後設定する予定のすべての静的 VLAN の数
- 現在設定されているもの （動的 GVRP VLAN の初期値は 128 です） と、今後設定する予定の GVRP に参加しているすべての動的 VLAN の数

GVRP VLAN の最大数を上記の合計より大きくすると、GVRP を実行でき、大量の GVRP LAN を受信するためにデバイスをリセットする必要がありません。たとえば、3 つの VLAN があり、VLAN の静的または動的登録の結果として別の 2 つの VLAN を設定する予定である場合、リセット後の GVRP VLAN の最大数を 10 に設定します。 **GVRP Global Parameters** ページを開くには、次の手順を実行します。

- Tree View で、**Switch → VLAN → GVRP Parameters** とクリックします。**GVRP Parameters** ページが開きます。



GVRP Global Parameters ページ

GVRP Global Parameters ページには、以下のフィールドが含まれています。

- **GVRP Global Status** — デバイスで GVRP を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enabled** — デバイスで GVRP が有効になっていることを示します。
  - **Disabled** — デバイスで GVRP が無効になっていることを示します。
    このフィールド値は、デフォルトです。
- **Interface** — GVRP が有効になっている特定のインタフェースを示します。
  可能なフィールド値には、以下のものがあります。
  - **Port** — GVRP が有効になっている特定のポートを示します。
  - **LAG** — GVRP が有効になっている特定の LAG を示します。
- **GVRP State** — GVRP がポートで有効かどうかを示します。可能なフィールド値には、以下のものがあります。
  - **Enable** — インタフェースで GVRP を有効にします。
  - **Disable** — インタフェースで GVRP を無効にします。これはデフォルト値です。
- **Dynamic VLAN Creation** — GVRP を介した VLAN の作成を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — GVRP を介した VLAN の作成を有効にします。
  - **Disable** — GVRP を介した VLAN の作成を無効にします。
- **GVRP Registration** — GVRP 登録ステータスを有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — GVRP を介した VLAN 登録を有効にします。
  - **Disable** — GVRP を介した VLAN 登録を無効にします。

デバイスで GVRP を有効にするには、次の手順を実行します。

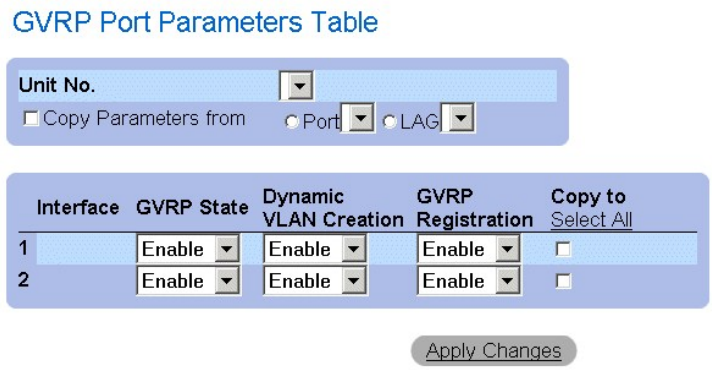
1. **GVRP Global Parameters** ページを開きます。
2. **GVRP Global Status** フィールドで、**Enable** を選びます。
3. **Apply Changes** をクリックします。GVRP がデバイスで有効になります。

GVRP ポートを定義するには、次の手順を実行します。

1. **GVRP Global Parameters** ページを開きます。
2. **Show All** をクリックします。**GVRP Parameters** ページが開きます。**GVRP Port Parameters** には、ポートで GVRP を有効にし、GVRP を使用してポートが VLAN 登録に参加できるよう許可するパラメータが含まれています。また、**GVRP Port Parameters Table** にも VLAN 登録モードについての情報が含まれています。特定のポートを、VLAN 登録または VLAN での使用からブロックすることもできます。
3. ポートを選びます。
4. **GVRP State**、**Dynamic VLAN Creation**、**VLAN Registration** および **GVRP Registration** フィールドを定義します。
5. **Apply Changes** をクリックします。GVRP がポートで有効になり、パラメータが定義され、デバイスがアップデートされます。

GVRP Port Parameters Table を表示するには、次の手順を実行します。

1. **GVRP Global Parameters** ページを開きます。
2. **Show All** をクリックします。**GVRP Port Parameters Table** ページが開きます。



GVRP Port Parameters Table ページ

GVRP Global Parameters ページで表示されるフィールドに加えて、**GVRP Port Parameters Table** ページには以下のフィールドも表示されます。

- **Unit No.** — GVRP 情報が表示されているスタッキングユニット番号を表示します。
- **Copy Parameters from** — GVRP パラメータのコピー元のインタフェースを示します。
- **Copy To** — GVRP パラメータのコピー先のポートを示します。

CLI コマンドを使用した GVRP の設定

次の表に、**GVRP Global Parameters** ページで表示される GVRP の設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明

gvrp enable	GVRP をグローバルに有効にします。
gvrp enable	GVRP をインタフェースで有効にします。
gvrp vlan-creation-forbid	動的 VLAN 作成を有効または無効にします。
gvrp registration-forbid	すべての VLAN の登録を解除し、ポートでの動的 VLAN の作成または登録ができないようにします。
show gvrp configuration [ethernet interface | port-channel *port-channel-number*]	タイマー値、GVRP と動的 VLAN の作成が有効かどうか、およびどのポートが GVRP を実行しているかなどの GVRP 設定情報を表示します。
gvrp max-vlan number	GVRP が有効になっている際の VLAN の最大数を設定します。

以下に、CLI コマンドの例を示します。

```
Console (config)# gvrp enable

Console (config)# interface ethernet 1/e8

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 switch.

Maximum VLANs:256, Maximum VLANs after reset: 256.

Port(s)Status Registration Dynamic VLAN Timers (milliseconds)

Creation Join Leave Leave All

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

2/1 Enabled Normal Enabled 200 600 10000

4/4 Enabled Normal Enabled 200 600 10000
```

ポートの集合

ポート集合は、ポートのグループをリンクして 1 つの LAG (Link Aggregated Group) を形成し、ポートの使用を最適化します。ポート集合は、デバイス間のバンド幅を拡大し、ポートの柔軟性を増し、リンクの冗長性を提供します。PowerConnect 3324 および PowerConnect 3348 の両方が最大で 6 つの LAG、および各スタックまたはスタンドアロンユニットの LAG 1 つに付き 8 つのポートに対応しています。

各 LAG は、同じ速度のポートで構成され、全二重方式動作に設定されています。LAG のポートの速度が同じであれば、異なるメディアタイプ （UTP / ファイバー、または異なるファイバータイプ） でも動作します。

集合リンクは、関連リンクで LACP (Link Aggregation Control Protocol) を有効にすることにより、手動または自動で割り当てることができます。PowerConnect 3324/3348 は、送信元の MAC アドレスと送信先の MAC アドレスの両方に基づいた LAG Load Balancing を提供します。

集合リンクは、システムで単一の論理ポートとして扱われます。具体的には、集合リンクは自動ネゴシエーション、速度、二重方式などの非集合ポートに似たポート属性を持っています。

PowerConnect 3324/3348 は、静的 LAG および LACP (Link Aggregation Control Protocol) LAG の両方に対応しています。LACP LAG は、異なるデバイスにある他の LACP ポートと集合ポートリンクをネゴシエートします。他のデバイスポートも LACP ポートである場合、デバイスは、LACP の間に LAG を確立します。

スタンドアロンまたはスタッキング構成でポートを LAG に追加する際は、以下のガイドラインに従ってください。

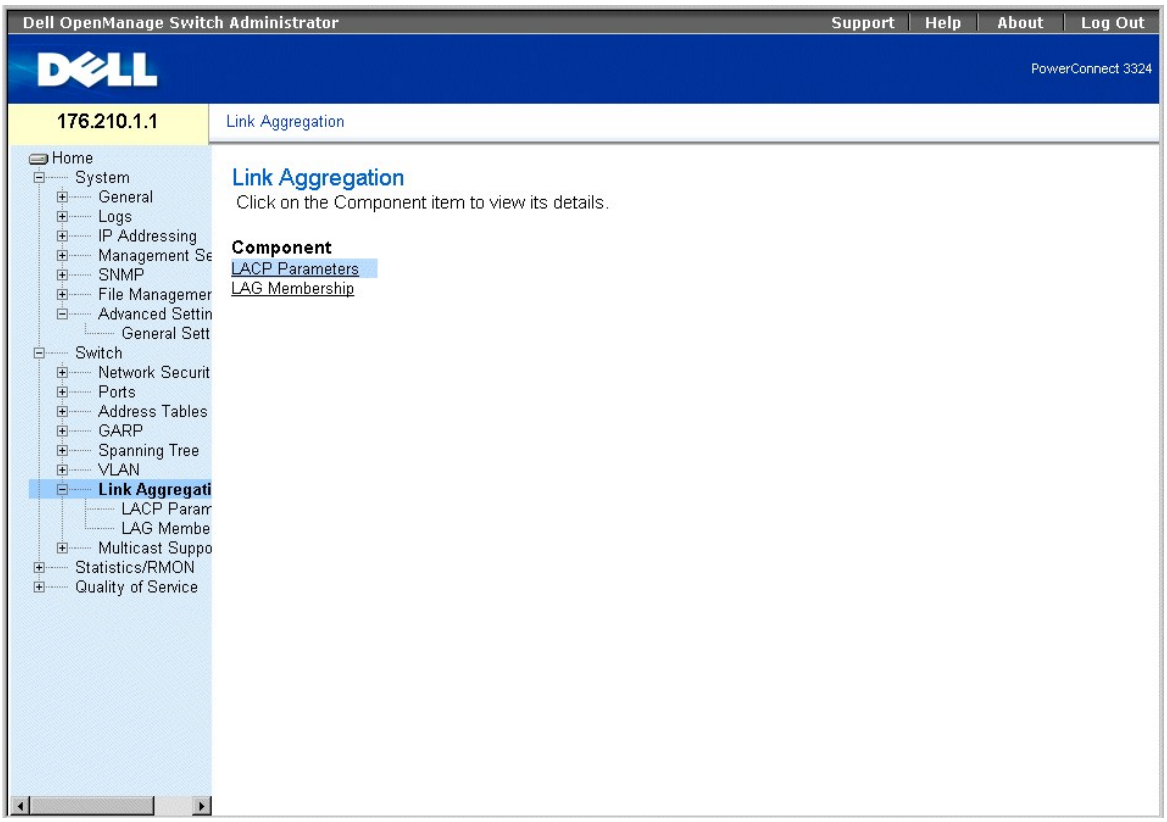
- Layer 3 インタフェースがポートで定義されていないこと。
- ポートがどの VLAN にも属さないこと。
- ポートが他のどの LAG にも属さないこと。
- ポートがミラーポートではないこと。
- ポートの 802.1p 優先度が LAG の 802.1p 優先度と同じであること。
- ACL がポートで定義されていないこと。
- QoS Trust がポートで無効化されていないこと。
- GVRP が有効化されていないこと。

メモ: ポートは、ポートが以前に設定された LAG の一部でない場合にのみ、 LACP ポートとして設定できます。

PowerConnect 3324/3348 は、ハッシュ機能を使用してどのフレームがどの集合リンクメンバーに運ばれているかを決定します。ハッシュ機能は、統計的に集合リンクメンバーの負荷のバランスを取ります。PowerConnect 3324/3348 は、集合リンクを単一の論理ポートとみなします。

各集合リンクには、Gigabit Ethernet ポートや Fast Ethernet ポートなどの集合リンクポートタイプがあります。ポートタイプが同じ場合にのみ、ポートを集合リンクに追加できます。ポートが集合リンクから削除される際、ポートは元のポート設定に戻ります。**LinkAggregation** ページを開くには、次の手順を実行します。

- Tree View で、**Switch → Link Aggregation** とクリックします。**LinkAggregation** ページが開きます。



Link Aggregation ページ

この項には以下のトピックがあります。

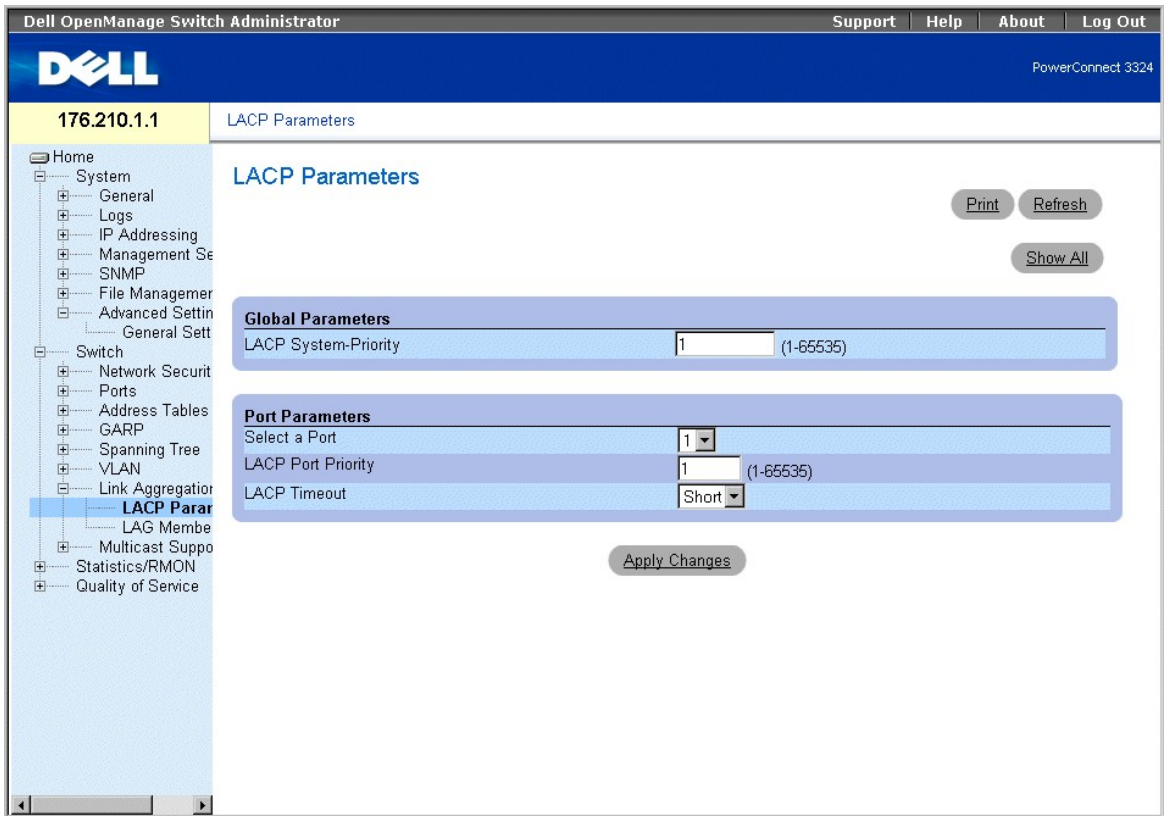
- LACP パラメータの定義
- LAG メンバーシップの定義

LACP パラメータの定義

LACP Parameters ページには、LACP LAG の設定についての情報が含まれています。集合ポートは、リンク集合ポートグループにリンクできます。各グループは、同じ速度のポートで構成されています。

集合リンクは、関連リンクで LACP (Link Aggregation Control Protocol) を有効にすることで、手動で設定または自動的に確立することができます。**LACP Parameters** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Link Aggregation** とクリックします。**LACPParameters** ページが開きます。



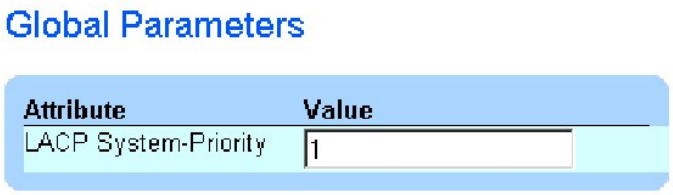
LACP Parameters ページ

LACP Parameters ページには、以下の項目が含まれています。

- Global Parameters ページ
- Port Parameters Table

Global Parameters ページ

Global Parameters には、LACP 優先度割り当ての情報が含まれています。集合ポートは、リンク集合ポートグループにリンクできます。LAG は、ユーザーの明示的な割り当てで手動で設定することができ、関連 LAG で LACP (Link Aggregation Control Protocol) を確立して自動で設定することもできます。



グローバルパラメータ

Global Parameters セクションには、以下のフィールドが含まれています。

- **LACP System-Priority** — LACP 優先度値を示します。可能な範囲は

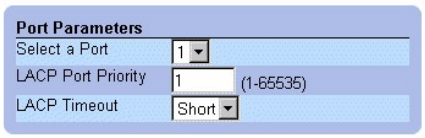
1 ～ 65535 で、デフォルト値は 1 です。

Global Parameters を定義するには、次の手順を実行します。

1. **LACP Parameters** ページを開きます。
2. **Global Parameters** セクションにスクロールします。
3. **LACP System Priority** および **LACP Timeout** フィールドを定義します。
4. **Apply Changes** をクリックします。Global Parameters が定義され、デバイスがアップデートされます。

Port Parameters Table

Port Parameters Table には、LACP 優先度とタイムアウト値のポートへの割り当てについての情報が含まれています。



ポートパラメータテーブル

Port Parameters Table には、以下のフィールドが含まれています。

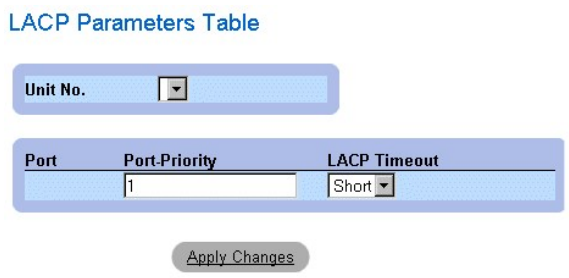
- **Select Port** — ポート番号を指定します。
- **LACP Port Priority** — ポート LACP 優先度値を示します。デフォルトは 1 です。
- **LACP Timeout** — 管理用の LACP タイムアウトを割り当てます。 可能なフィールド値には、以下のものがあります。
  - **Short** — 短いタイムアウト値を指定します。
  - **Long** — 長いタイムアウト値を指定します。

Port Parameters を定義するには、次の手順を実行します。

1. **LACP Parameters** ページを開きます。
2. **Link Aggregation Port Parameters Table** にスクロールします。
3. **LACP System Priority** および **LACP Timeout** フィールドを定義します。
4. **Apply Changes** をクリックします。Link Aggregation Global Parameters が定義され、デバイスがアップデートされます。

LACP Parameters Table を表示するには、次の手順を実行します。

1. **LACP Parameters** ページを開きます。
2. **Show All** をクリックします。**LACP Parameters Table** ページが開きます。



LACP Parameters Table ページ

LACP Parameters ページのフィールドに加えて、**LACP Parameters Table** には以下のフィールドも表示されます。

- **Unit No.** — LACP 情報が表示されているスタッキングユニット番号を表示します。

CLI コマンドを使用した LACP パラメータの設定

次の表に、**Link Aggregation** ページで表示される LACP パラメータの設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
lacp system-priority *value*	システム優先度を設定します。
lacp port-priority *value*	物理ポートの優先度値を設定します。
lacp timeout {long | short}	管理用の LACP タイムアウトを割り当てます。
show lacp ethernet *interface* **[parameters | statistics | protocol-state]**	Ethernet ポートの LACP 情報を表示します。
show lacp port-channel **[port_channel_number]**	ポートチャネルの LACP 情報を表示します。

以下に、CLI コマンドの例を示します。

```
Console (config)# lacp system-priority 120

Console (config)# interface ethernet 1/e8

Console (config-if)# lacp port-priority 247

Console (config-if)# lacp timeout long

Console (config-if)# exit

Console# show lacp ethernet 1/e1 statistics

Port 1/e1 LACP Statistics:
```

```
LACP PDUs sent:2


LACP PDUs received:2
```

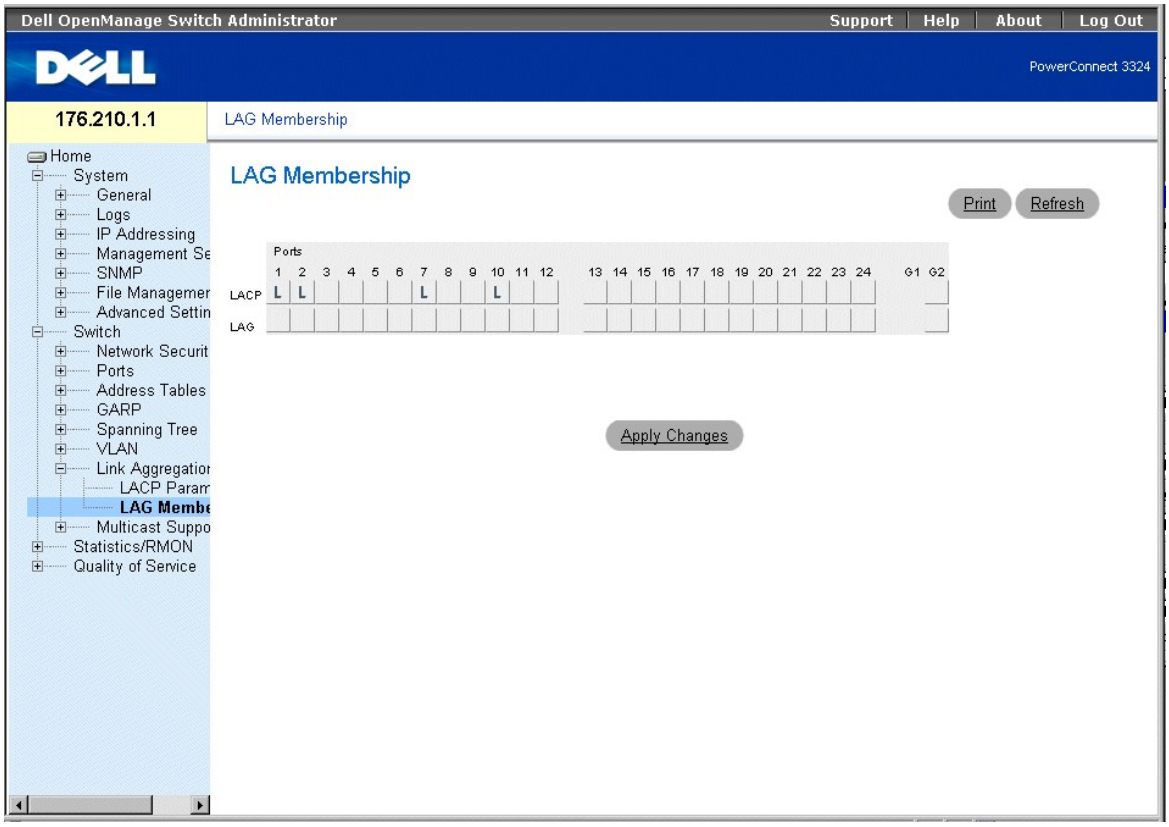
LAG メンバーシップの定義

LAG Membership ページを使用して、ネットワーク管理者は LAG へのポートの割り当てができます。LAG には最大で 8 つのポートを含むことができます。現在、PowerConnect 3324/3348 は、デバイスがスタンドアロンデバイスまたはスタック内にあっても、各システムで 6 つの LAG に対応しています。**LAG Membership Table** には、以下の項目が含まれています。

- **LACP** — ポートが LAG メンバーになるのを許可して、動的であるかを示します。
- **LAG** — ポートを LAG に追加して、ポートが属している特定の LAG を示します。

LAG Membership ページを開くには、次の手順を実行します。

- Tree View で、Switch → Link Aggregation → LAG Membership Tab とクリックします。**LAG Membership** ページが開きます。



LAG Membership ページ

LAG にポートを追加するには、次の手順を実行します。

1. **LAG Membership** ページを開きます。

2. ポート番号で切り替えて、LAG 設定と番号を割り当てます。
3. **Apply Changes** をクリックします。ポートが LAG に追加され、デバイスがアップデートされます。

CLI コマンドを使用した ポート の LAG への割り当て

次の表に、**LAG Membership** ページで表示されるポートの LAG への割り当てに対応する CLI コマンドをまとめます。

CLI コマンド	説明
channel-group port-channel-number mode {on | auto}	ポートをポートチャネルに設定します。
show interface port_channel	LAG に接続されているインタフェースを表示します。

以下に、CLI コマンドの例を示します。

```
Console# channel-group port-channel-number mode on auto 1

Port-Channel 1:Port Type 1000 Ethernet

Actor

System Priority:1

MAC Address:000285:0E1C00

Admin Key: 29

Oper Key: 29

Partner

System Priority:0

MAC Address: 000000:000000

Oper Key: 14
```

マルチキャスト転送サポート

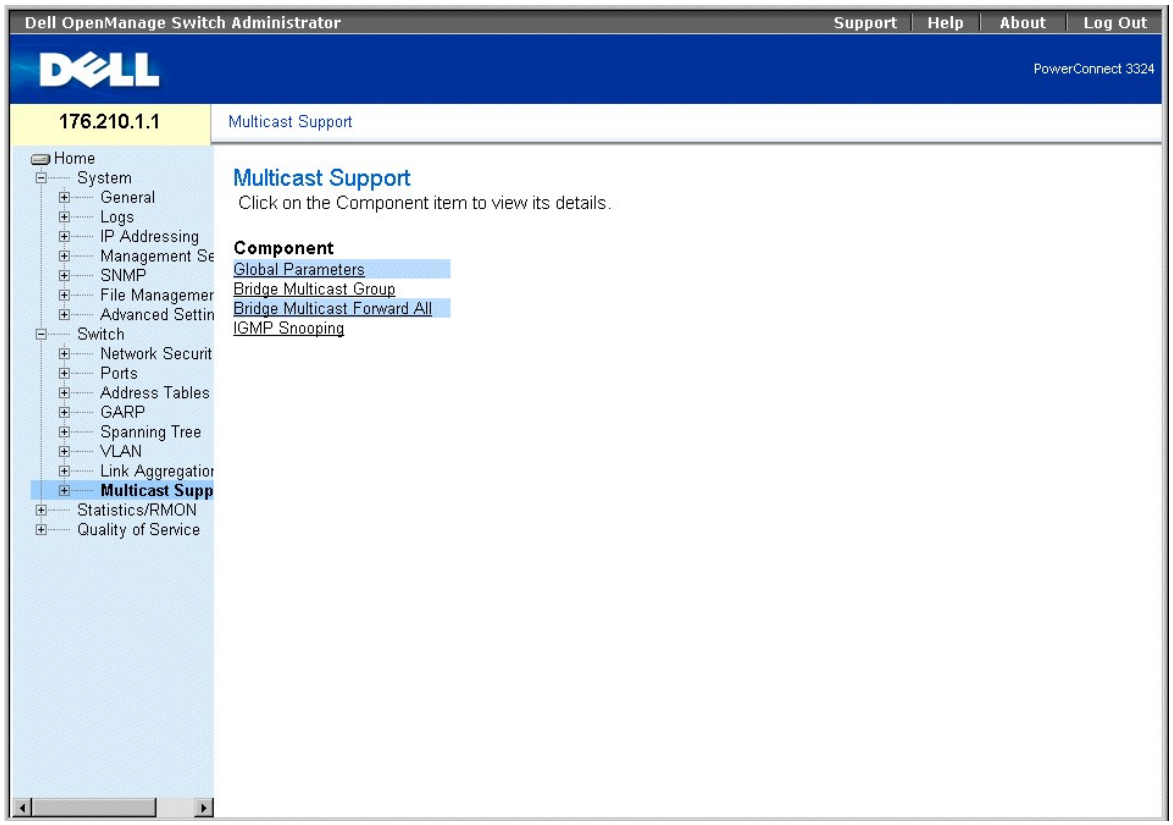
マルチキャスト転送を使用して、1 つのパケットを複数の送信先に転送することができます。L2 マルチキャストサービスは、特定のマルチキャストアドレスに宛てられた 1 つのパケットを受信する L2 スイッチに基づいています。マルチキャスト転送は、パケットのコピーを作成し、パケットを関連ポートに送信します。

PowerConnect 3324/3348 は、以下の両方に対応しています。

- **Forwarding L2 Multicast Packets** — デフォルトで有効になっています。
- **Filtering L2 Multicast Packets** — L2 パケットのポート VLAN への転送を有効にします。Multicast Filtering が無効な場合、マルチキャストパケットはすべての関連 VLAN ポートにフラッドされます。

Multicast Support ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Multicast Support** とクリックします。**MulticastSupport** ページが開きます。



Multicast Support ページ

Multicast Support ページには、以下のトピックへのリンクがあります。

- IGMP スヌーピング設定の定義
- ブリッジマルチキャストグループメンバーの追加
- Multicast Forward All パラメータの割り当て
- IGMP スヌーピングの有効化

IGMP スヌーピング設定の定義

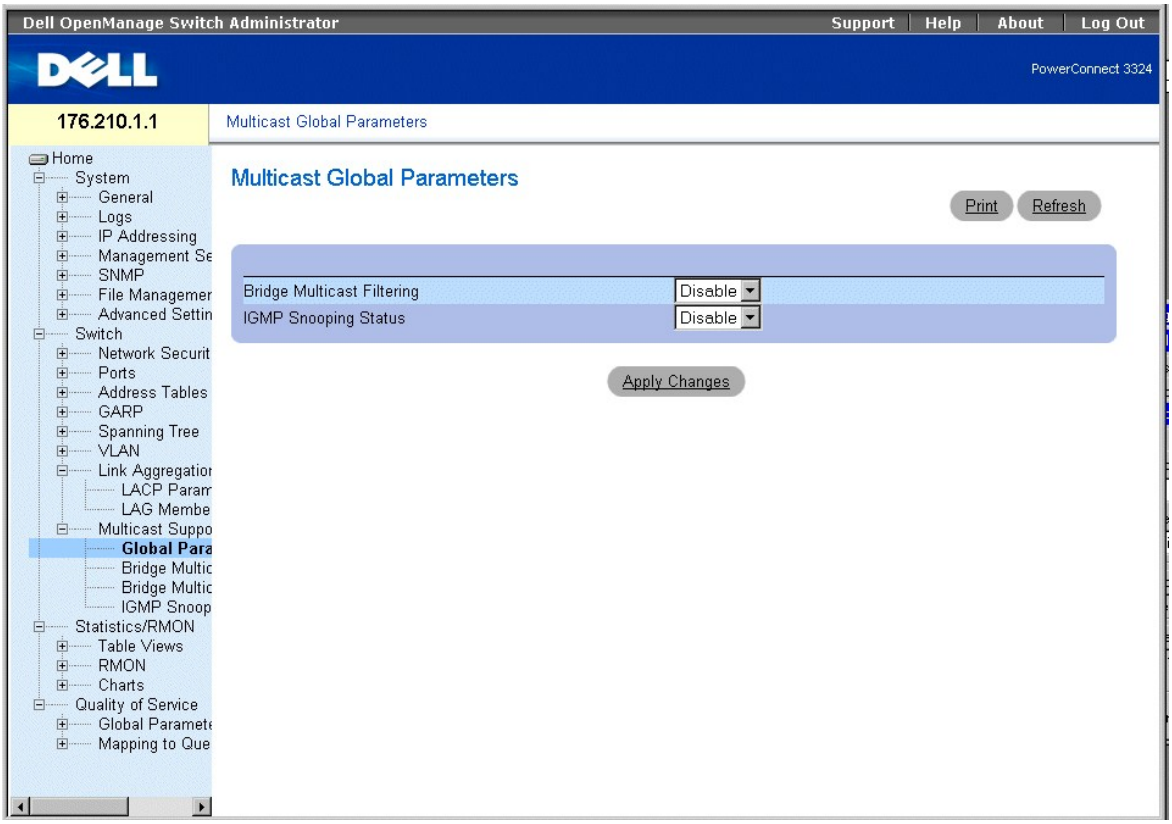
Layer 2 スイッチングはデフォルトで、パケットをマルチキャストパケットとして扱い、すべての関連 VLAN ポートにマルチキャストパケットを転送します。このタイプのトラフィック転送は機能的ですが、関連のないポートもマルチキャストトラフィックを受信し、ネットワークトラフィックが増加します。

IGMP スヌーピングは、ステーションからマルチキャストルータへ転送される際に IGMP フレームを確認して、不要なマルチキャストトラフィックを解消します。

IGMP スヌーピングがグローバルで有効になっている際、スイッチング ASIC は、すべての IGMP フレームを CPU に転送するようにプログラムされています。CPU は受信フレームを分析し、どのポートがどのマルチキャストグループに参加したいのか、どのポートが IGMP 照会を生成しているマルチキャストルータを持っているのか、どの Routing プロトコルがパケットおよびマルチキャストトラフィックを転送しているのかを決定します。特定のマルチキャストグループに参加を希望しているポートは、そのマルチキャストグループを指定する IGMP レポートを発行します。

Multicast Global Parameters ページを使用して、ネットワーク管理者はデバイスで全般的な IGMP スヌーピングおよび Multicast Filtering を有効にできます。**Multicast Global Parameters** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Multicast Support** → **Global Parameters** とクリックします。**Multicast Global Parameters** ページが開きます。



Multicast Global Parameters ページ

Multicast Global Parameters ページには、以下のフィールドが含まれています。

- **Bridge Multicast Filtering** — デバイスで、Bridge Multicast Filtering が有効になっているかを示します。可能なフィールド値には、以下のものがあります。
  - **Enabled** — デバイスで、Bridge Multicast Filtering を有効にします。
  - **Disabled** — デバイスで、Bridge Multicast Filtering を無効にします。これはデフォルト値です。
- **IGMP Snooping Status** — デバイスで IGMP スヌーピングが有効かどうかを示します。可能なフィールド値には、以下のものがあります。

- **Enabled** — 特定の VLAN で IGMP スヌーピングを有効にします。
- **Disabled** — 特定の VLAN で IGMP スヌーピングを無効にします。これはデフォルト値です。

デバイスで Bridge Multicast Filtering を有効にするには、次の手順を実行します。

1. **Multicast Global Parameters** ページを開きます。
2. **Bridge Multicast Filtering** フィールドで **Enable** を選びます。
3. **Apply Changes** をクリックします。**Bridge Multicast** がデバイスで有効になります。

デバイスで IGMP スヌーピングを有効にするには、次の手順を実行します。

1. **Multicast Global Parameters** ページを開きます。
2. **IGMP Snooping Status** フィールドで **Enable**を選びます。
3. **Apply Changes** をクリックします。IGMP スヌーピングがデバイスで有効になります。

CLI コマンドを使用したマルチキャスト転送および IGMP スヌーピングの有効化

次の表に、 **Multicast Support** ページで表示されるマルチキャスト転送および IGM スヌーピングの有効化に対応する CLI コマンドをまとめます。

CLI コマンド	説明
bridge multicast filtering	マルチキャストアドレスのフィルタリングを有効にします。
ip igmp snooping	IGMP (Internet Group Management Protocol) スヌーピングを有効にします。

以下に、CLI コマンドの例を示します。

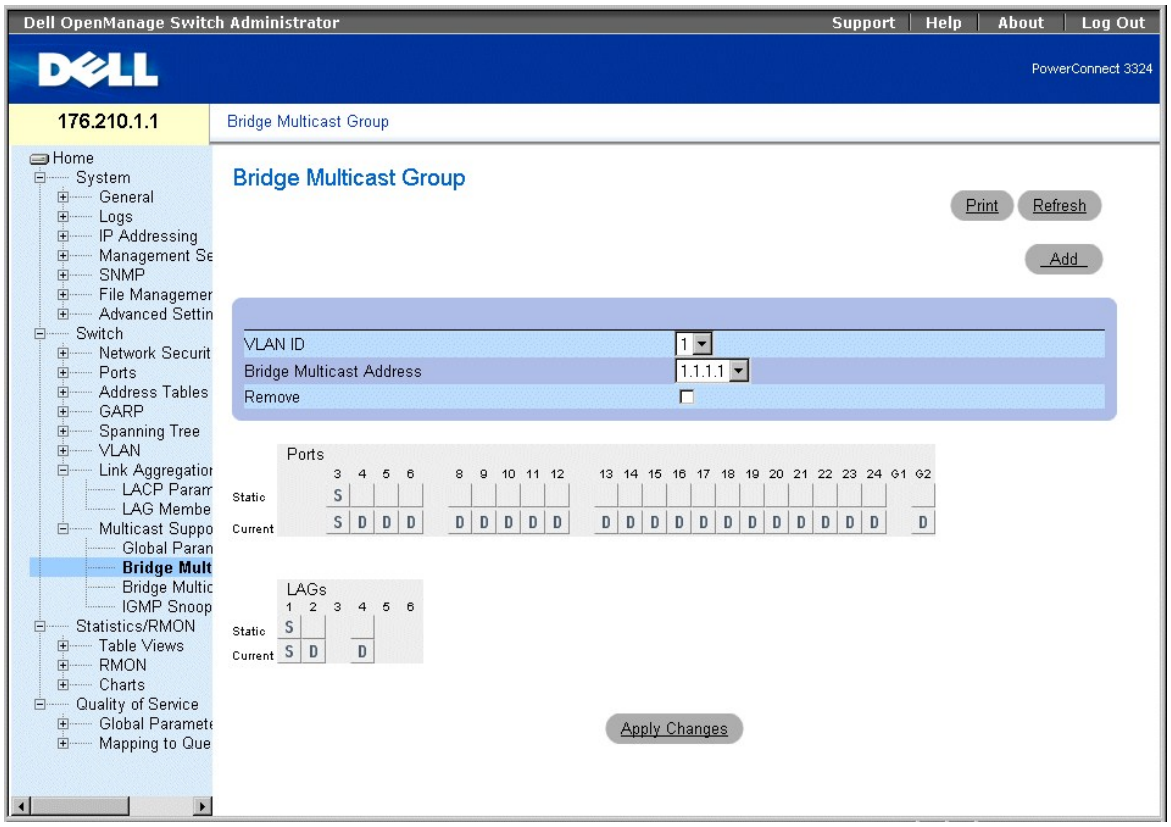
```
Console (config)# bridge multicast filtering
```

```
Console (config)# ip igmp snooping
```

ブリッジマルチキャストグループメンバーの追加

Bridge Multicast Group ページでは、**Port** および **LAG Table** にあるマルチキャストサービスグループに接続しているポートと LAG を表示します。Port および LAG テーブルは、ポートまたは LAG がマルチキャストグループに参加している方法も反映します。ポートは、既存のグループまたは新しいマルチキャストサービスグループに追加することができます。**Bridge Multicast Group** ページで、新しいマルチキャストサービスグループを追加することができます。**Bridge Multicast Group** ページでは、特定のマルチキャストサービスアドレスグループにポートを割り当てることもできます。**Bridge Multicast Group** ページを開くには、次の手順を実行します。

1. Tree View で、**Switch** → **Multicast Support** → **Bridge Multicast Group** とクリックします。**Bridge Multicast Group** ページが開きます。

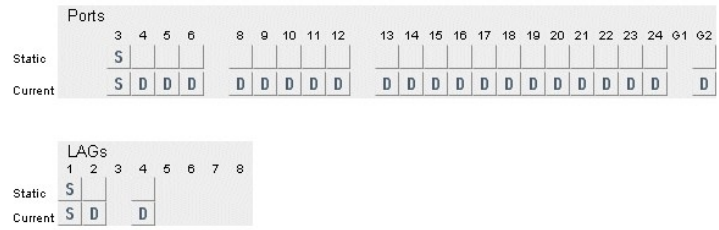


Bridge Multicast Group ページ

Bridge Multicast Group ページには、以下のフィールドが含まれています。

- **VLAN ID** — VLAN を示します。
- **Bridge Multicast Address** — マルチキャストグループの IP アドレスを示します。
- **Remove** — アドレスで指定されたブリッジマルチキャストグループを削除します。
  - **Checked** — ブリッジマルチキャストアドレスを削除します。
  - **Unchecked** — ブリッジマルチキャストアドレスを保持します。
- **Ports Table** — マルチキャストサービスに追加できるポートを一覧表示します。
- **LAGs Table** — マルチキャストサービスに追加できる LAG を一覧表示します。

IGMP Port/LAG Members Table は、 IGMP Port/LAG メンバーステータスを表示します。



IGMP Port/LAG Members Table

IGMP Port/LAG Members Table Control Settings Table には、IGMP ポートおよび LAG メンバーを管理する設定が含まれています。

IGMP Port/LAG Members Table 制御設定

ポート制御	定義
D	ポート / LAG が **Current** 行のマルチキャストグループに動的に参加したことを示します。
S	**Static** 行の静的メンバーとしてポートをマルチキャストグループに接続します。ポート / LAG が **Current** 行のマルチキャストグループに静的に参加したことを示します。
F	ポートがこのマルチキャストグループに参加できないことを示します。
消灯	ポートがこのマルチキャストグループに接続されていないことを示します。

マルチキャストサービスを受信するためにポートを定義するには、次の手順を実行します。

1. **Bridge Multicast** ページを開きます。
2. **VLAN ID** および **Bridge Multicast Address** フィールドを定義します。
3. 選択したマルチキャストグループにポートを参加させるにはポートを **S** に切り替え、マルチキャストグループにポートが参加できないようにするには **F** に切り替えます。
4. **Apply Changes** をクリックします。ポートがマルチキャストグループに割り当てられ、デバイスがアップデートされます。

マルチキャストサービスを受信するために LAG を割り当てるには、次の手順を実行します。

1. **Bridge Multicast** ページを開きます。
2. **VLAN ID** および **Bridge Multicast Address** フィールドを定義します。
3. 選択したマルチキャストグループに LAG を参加させるには LAG を **S** に切り替え、マルチキャストグループにポートが参加できないようにするには **F** に切り替えます。
4. **Apply Changes** をクリックします。LAG がマルチキャストグループに割り当てられ、デバイスがアップデートされます。

CLI コマンドを使用したマルチキャストサービスメンバーの管理

次の表に、**Bridge Multicast Group** ページで表示されるマルチキャストサービスメンバーの管理に対応する CLI コマンドをまとめます。

CLI コマンド	説明
bridge multicast address {*mac-multicast-address* **|** *ip-multicast-address***} {add | remove} {ethernet** *interface-list* **| port-channel** *port-channel-number-list***}**	MAC レイヤのマルチキャストアドレスをブリッジテーブルに登録し、静的ポートをグループに追加します。
show bridge multicast address-table [vlan *vlan-id***] [address** *mac-multicast-address* **|** *ip-multicast-address***] [format ip | mac]**	マルチキャスト MAC アドレステーブル情報を表示します。

以下に、CLI コマンドの例を示します。

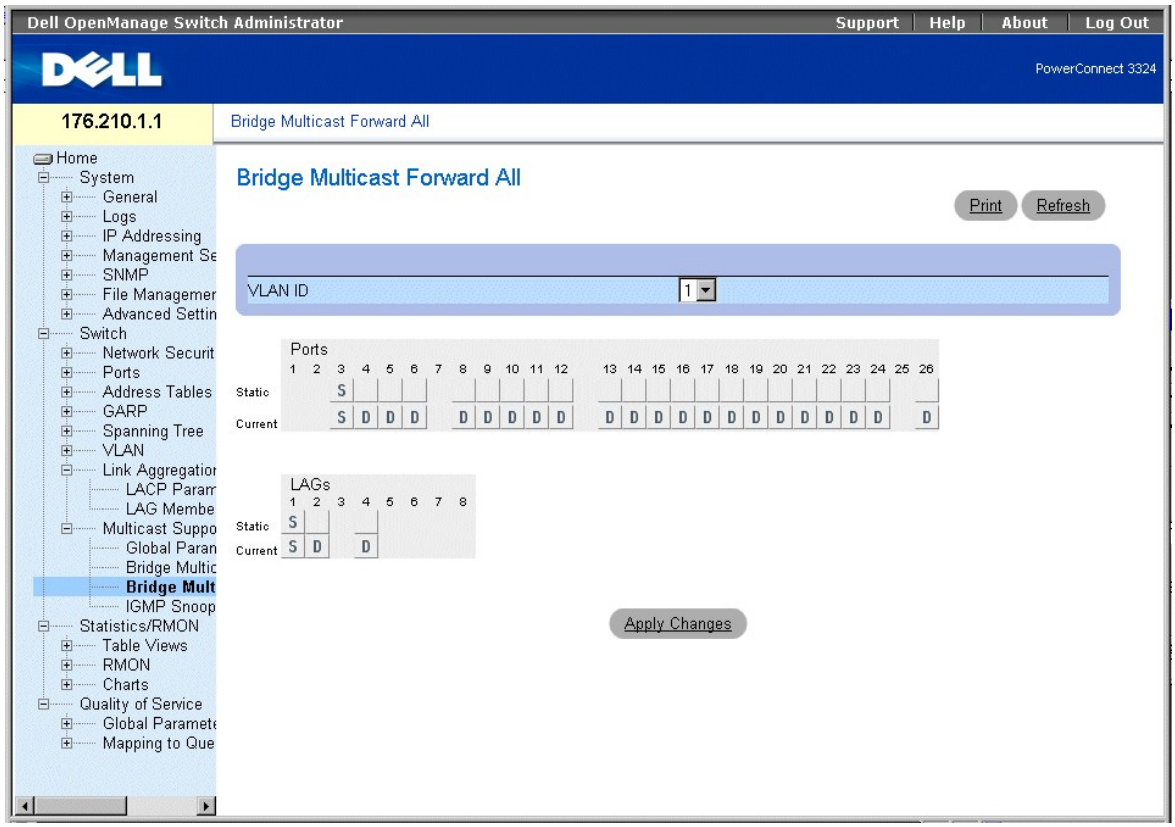
```
Console (config)# interface vlan 8

bridge multicast address 0100.5e02.0203
```

```
bridge multicast address 0100.5e02.0203 add ethernet 1/e1, 2/e2

Console (config-if)# Exit

Console # show bridge multicast address-table



Vlan MAC Address type Ports

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

1 0100.5e02.0203 static 1/e1, 2/e2

19 0100.5e02.0208 static 1/e1-8

19 0100.5e02.0208 dynamic 1/e9-11



Forbidden ports for multicast addresses:

Vlan MAC Address Ports

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

1 0100.5e02.0203 2/e8

19 0100.5e02.0208 2/e8
```

Multicast Forward All パラメータの割り当て

Bridge Multicast Forward All ページを使用して、ネットワーク管理者はポートまたは LAG を周囲のマルチキャストルータ / スイッチに接続しているスイッチに接続することができます。IGMP スヌーピングが有効になると、マルチキャストパケットは適切なポートまたは VLAN に転送されます。

- Tree View で、**Switch → Multicast Support → Bridge Multicast → Bridge Multicast Forward All Tab** とクリックします。**Bridge Multicast Forward All** ページが開きます。



Bridge Multicast Forward All ページ

Bridge Multicast Forward All ページには、以下のフィールドが含まれています。

- **VLAN ID** — フレーム VLAN を示し、マルチキャストグループアドレスについての情報が含まれています。
- **Ports Table** — マルチキャストサービスに追加できるポートを一覧表示します。
- **LAGs Table** — マルチキャストサービスに追加できる LAG を一覧表示します。

Bridge Multicast Forward All ページには、スイッチやポートの設定を管理する設定が含まれています。

Bridge Multicast Forward All ルータ / ポート制御設定

ポート制御	定義
D	ポートをマルチキャストルータまたはスイッチに動的ポートとして接続します。
S	ポートをマルチキャストルータまたはスイッチに静的ポートとして接続します。
F	ポートがマルチキャストグループに参加できないことを示します。
消灯	ポートがマルチキャストルータまたはスイッチに接続されていないことを示します。

ポートをマルチキャストルータまたはスイッチに接続するには、次の手順を実行します。

1. **Bridge Multicast Forward All** ページを開きます。
2. **VLAN ID** フィールドを定義します。
3. **Multicast Router Port Table** でポートを選び、ポートに値を割り当てます。
4. **Apply Changes** をクリックします。マルチキャストルータまたはグループに接続しているポートがアップデートされます。

LAG をマルチキャストルータまたはスイッチに接続するには、次の手順を実行します。

1. **Bridge Multicast Forward All** ページを開きます。
2. **VLAN ID** フィールドを定義します。
3. **Multicast Router Port Table** で LAG を選び、LAG に値を割り当てます。
4. **Apply Changes** をクリックします。マルチキャストルータまたはグループに接続している LAG がアップデートされます。

CLI コマンドを使用したマルチキャストルータに接続されている LAG およびポートの管理

次の表に、**Bridge Multicast Forward All** ページで表示されるマルチキャストルータに接続されている LAG およびポートの管理に対応する CLI コマンドをまとめます。

CLI コマンド	説明
show bridge multicast filtering *vlan-id*	マルチキャスト設定を表示します。
bridge multicast forbidden forward-all	マルチキャストパケットの転送をポートで無効にします。
bridge multicast forward-all {add | remove} {ethernet interface-list | port-channel port-channel-number-list}	すべてのマルチキャストパケットの転送をポートで有効にします。

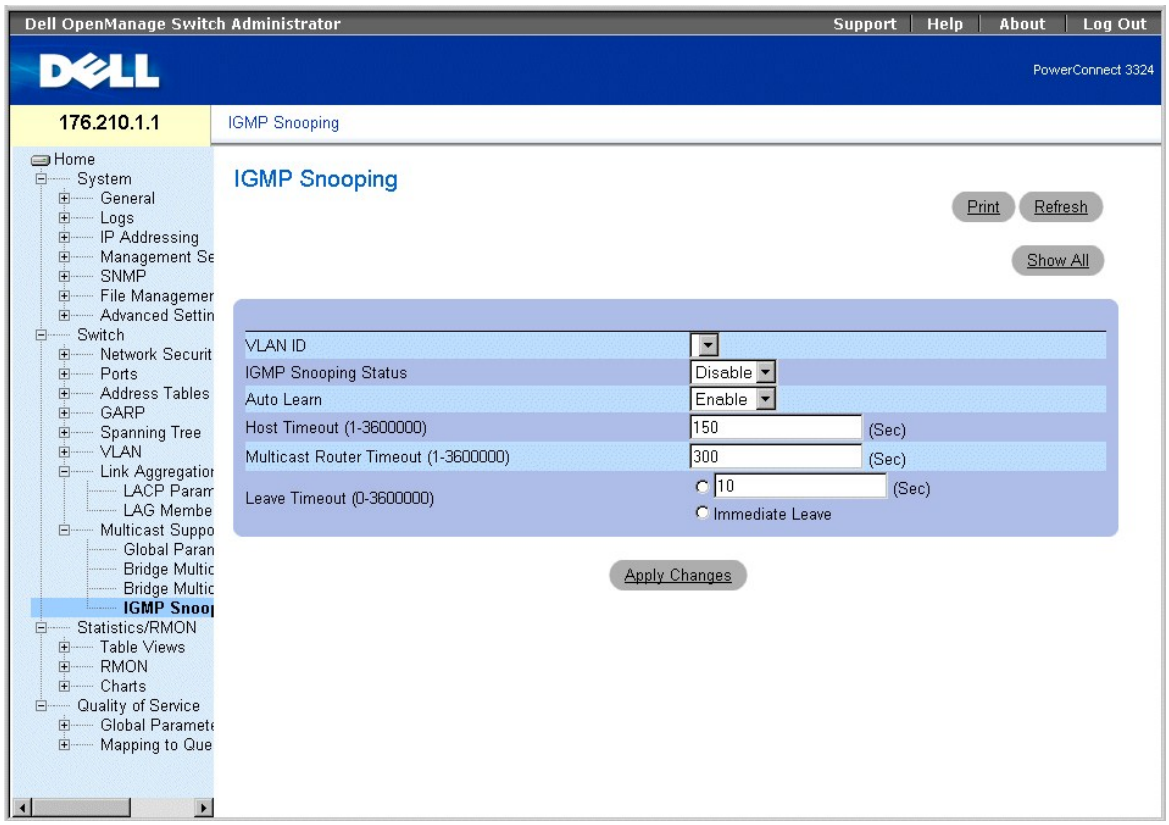
以下に、CLI コマンドの例を示します。

```
Console # show bridge multicast filtering

Filtering:óLå¯

VLAN: 1

Port Forward-All

Static Status

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

1/e1 Forbidden Filter

1/e2 Forward Forward(s)

1/e3 - Forward(s)
```

IGMP スヌーピングの有効化

IGMP Snooping ページを使用して、ネットワーク管理者は IGMP メンバーを追加することができます。 **IGMP Snooping** ページを開くには、次の手順を実行します。

- Tree View で、**Switch** → **Multicast Support** → **IGMP Snooping** とクリックします。**IGMP Snooping Table** が開きます。



IGMP Snooping ページ

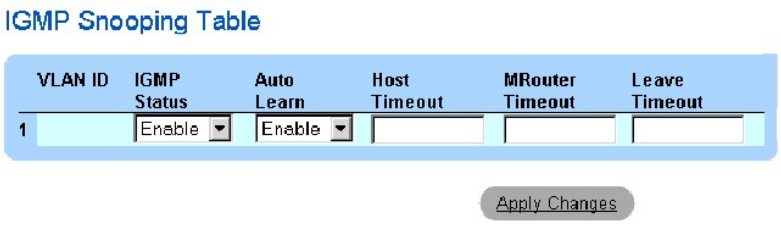
IGMP Snooping ページには、以下の情報が含まれています。

- **VLAN ID** — VLAN IDを指定します。
- **IGMP Snooping Status** — デバイスで IGMP スヌーピングを有効にします。
  可能なフィールド値には、以下のものがあります。
  - **Enabled** — デバイスで IGMP スヌーピングを有効にします。
  - **Disabled** — デバイスで IGMP スヌーピングを無効にします。
- **Auto Learn** — 新しいマルチキャストグループメンバーの自動的な学習を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — 新しいマルチキャストグループメンバーの自動的な学習を有効にします。
  - **Disable** — 新しいマルチキャストグループメンバーの自動的な学習を無効にします。
- **Host Timeout (1-3600000)** — IGMP スヌーピングエントリがエージアウトするまでの時間を示します。デフォルト値は **150** 秒です。
- **Multicast Router Timeout (1-3600000)** — マルチキャストルータエントリがエージアウトするまでの時間を示します。デフォルト値は **300** 秒です。
- **Leave Timeout (1-3600000)** — ポート Leave メッセージが受信された後、マルチキャストルータエントリがエージアウトするまでの時間を秒で指定します。可能なフィールド値には、以下のものがあります。

- **User-Defined** — ユーザー定義の Leave Timeout 値を示します。
- **Immediate Leave** — 即時の Leave Timeout 値を示します。

IGMP Snooping Table を表示するには、次の手順を実行します。

1. **IGMP Snooping** ページを開きます。
2. **Show All** をクリックします。**IGMP Snooping Table** が開きます。



IGMP Snooping Table

CLI コマンドを使用した IGMP スヌーピングの設定

次の表に、**IGMP Snooping** ページで表示される IGMP Snooping の設定に対応する CLI コマンドをまとめます。

CLI コマンド	説明
ip igmp snooping	IGMP (Internet Group Management Protocol) スヌーピングを特定の VLAN で有効にします。
ip igmp snooping mrouter learn-pim-dvmrp	特定の VLAN コンテキストでマルチキャストルータポートを自動的に学習できるようにします。
ip igmp snooping host-time-out *time-out*	Host Timeout を設定します。
ip igmp snooping mrouter-time-out *time-out*	Mrounter Host Timeout を設定します。
ip igmp snooping leave-time-out {*time-out* **| immediate-leave}**	Leave Timeout を設定します。
show ip igmp snooping mrouter [interface *vlan-id***]**	動的に学習されたマルチキャストルータインタフェースの情報を表示します。

以下に、CLI コマンドの例を示します。

```
Console (config)# interface vlan 2

Console (config-if)# ip igmp snooping

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 300
```

```
Console (config-if)# exit

Console (config)# interface vlan 2

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console (config)# exit

Console # show igmp snooping mrouter interface 1000

VLAN Ports

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

200 1/e1, 2/e1
```

メモ、注意および警告

メモ、注意および警告

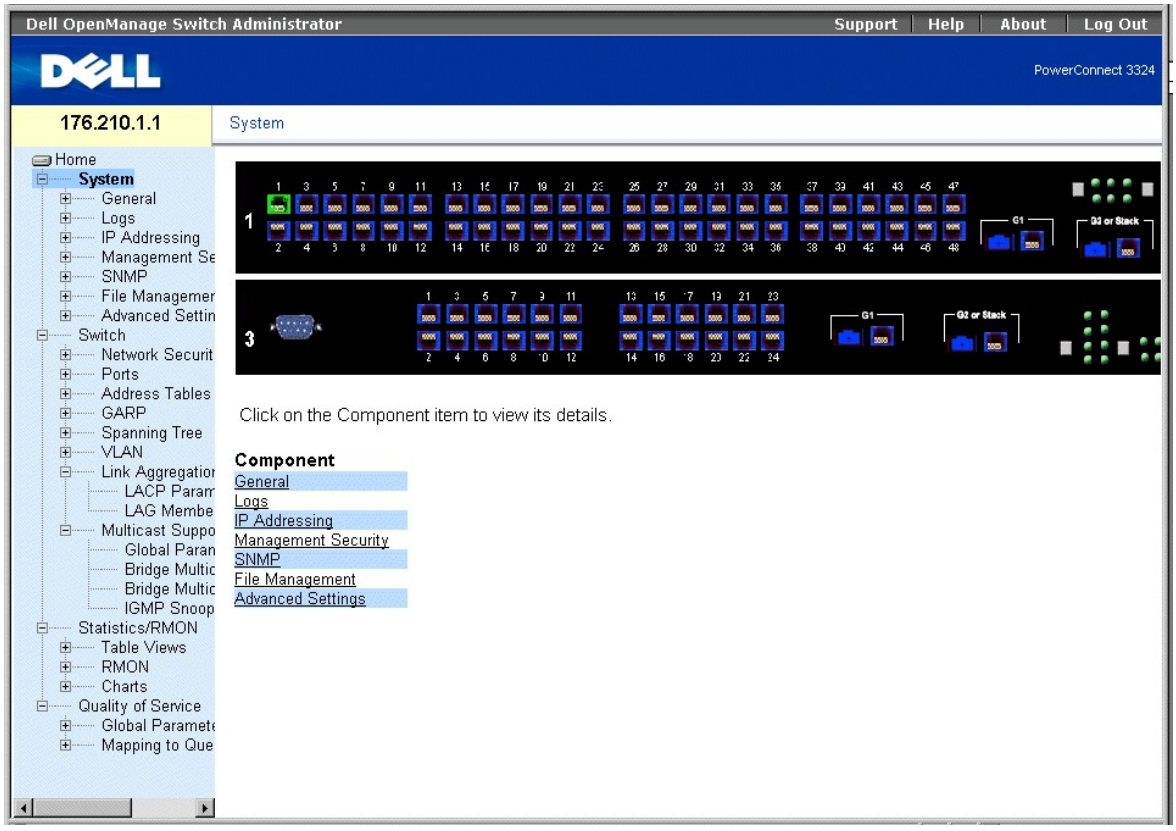
システム情報の設定

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

- 全般的なデバイス情報の定義
- ログの管理
- デバイスの IP アドレスの定義
- デバイスのセキュリティ管理
- SNMP パラメータの定義
- ファイルの管理
- 詳細設定の定義

この項では、セキュリティ機能、デバイスソフトウェアのダウンロード、デバイスのリセットを含むシステムパラメータの定義方法について説明します。**System** ページを開くには、次の手順を実行します。

1. Tree View で、**System** をクリックします。**System** ページが開きます。

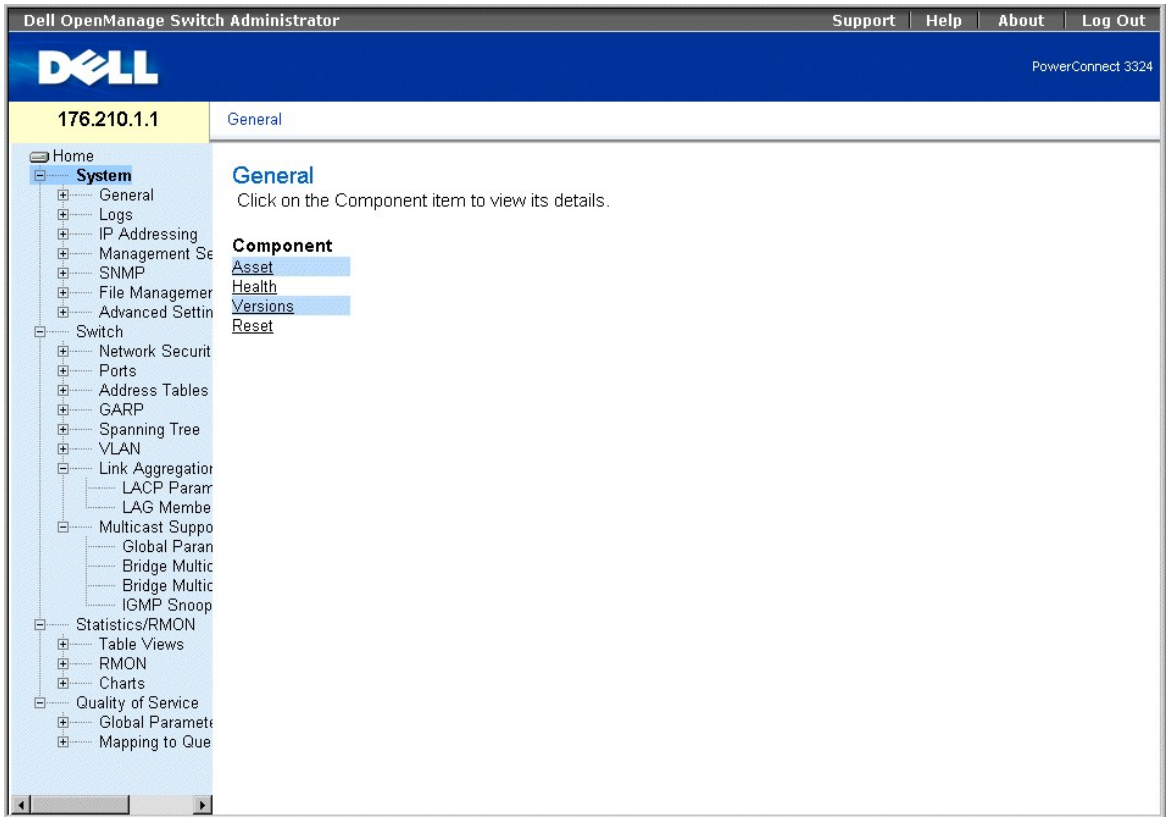


System ページ

全般的なデバイス情報の定義

General ページの様々なページへのリンクを使用して、ネットワーク管理者は、以下のようなデバイスパラメータを設定できます。

- 資産ページの表示
- システムの動作状態情報の表示
- バージョンページの表示
- デバイスのリセット

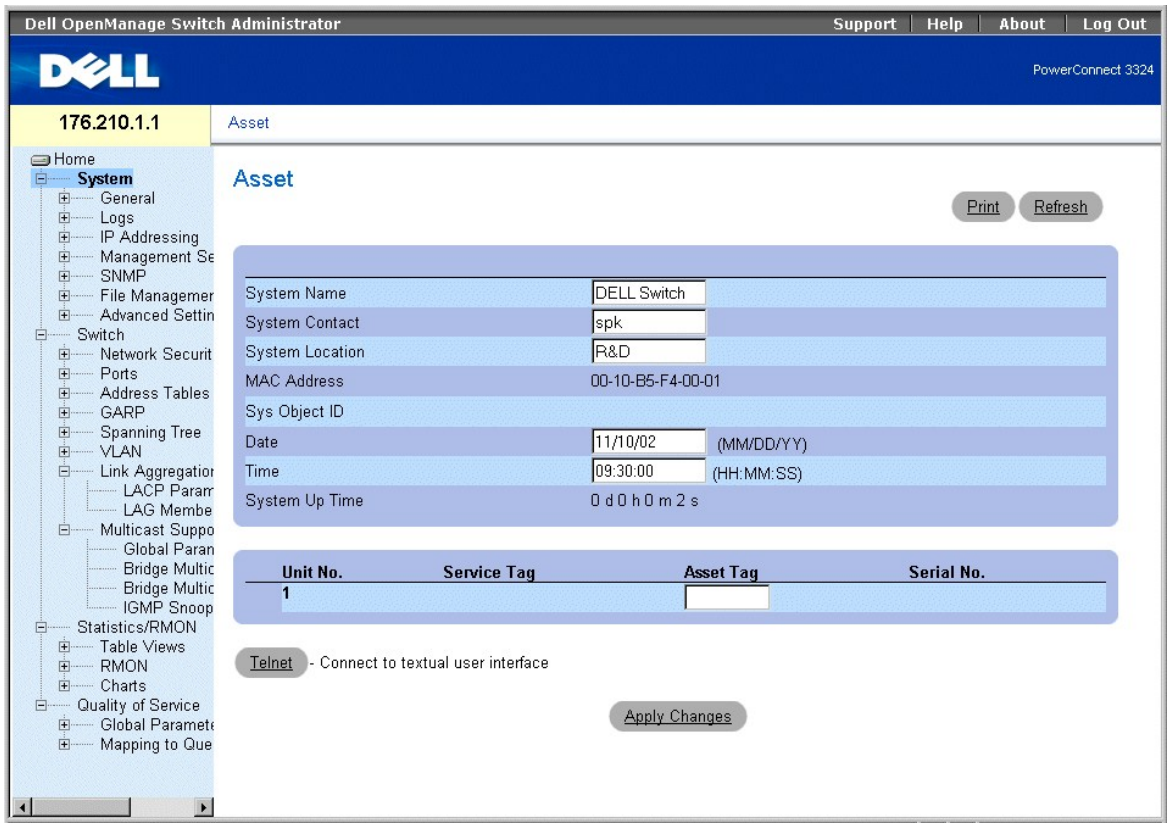


General ページ

資産ページの表示

Asset ページには、システム名、場所、連絡先、システムの MAC アドレス、システムオブジェクトの ID、日付、時間、システムのアップタイムなどの全般的なデバイス情報の設定用パラメータが含まれています。**Asset** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **General** → **Asset** とクリックします。**Asset** ページが開きます。



Asset ページ

Asset ページには、以下のフィールドが含まれています。

- **System Name** — ユーザー定義のデバイス名を定義します。
- **System Contact** — 担当者名を指定します。
- **System Location** — システムが現在稼動している場所を示します。
- **MAC Address** — スイッチの MAC アドレスを指定します。
- **Sys Object ID** — MIB の OID を識別します。
- **Date (MM/DD/YY)** — 現在の日付を示します。形式は月/日/年です。 たとえば、11/10/02 は、2002 年 11 月 10 日です。
- **Time (HH:MM:SS)** — 時刻を指定します。形式は、時間:分:秒です。 たとえば、20:12:03 は、午後 8 時 12 分 3 秒です。
- **System Up Time** — 最後のデバイスリセットからの経過時間を示します。システムの時間は、日数、時間、分、秒の形式で表示されます。たとえば、41 日 2 時間 22 分 15 秒などです。
- **Unit No.** — スタッキングユニットの番号を示します。
- **Service Tag** — デバイスを修理する際に使用されるサービスリファレンス番号を示します。
- **Asset Tag** — ユーザー定義のデバイスリファレンス番号を定義します。
- **Serial No.** — デバイスのシリアルナンバーを示します。

システム情報を定義するには、次の手順を実行します。

1. **Asset** ページを開きます。
2. **System Name**、**System Contact**、**System Location**、**Date**、**Asset Tag**、および **Time** フィールドを定義します。
3. **Apply Changes** をクリックします。システムパラメータが定義され、デバイスがアップデートされます。

Telnet セッションを開始するには、次の手順を実行します。

1. **Asset** ページを開きます。
2. **Telnet** をクリックします。Telnet セッションが開始します。

CLI コマンドを使用したデバイス情報の設定

次の表に、**Asset** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
hostname *name*	デバイスのホスト名を指定または変更します。
snmp-server contact *text*	システムの担当者名を設定します。
snmp-server location *text*	デバイスの場所の情報を入力します。
clock set *hh:mm:ss day month year*	システムクロックおよび日付を手動で設定します。日付の形式が異なっていますのでご注意ください。
show clock	システムクロックから時刻と日付を表示します。
show system id	サービスタグ情報を表示します。
show system	システム情報を表示します。
管理タグ	デバイスの管理タグを表示します。

以下に、CLI コマンドの例を示します。

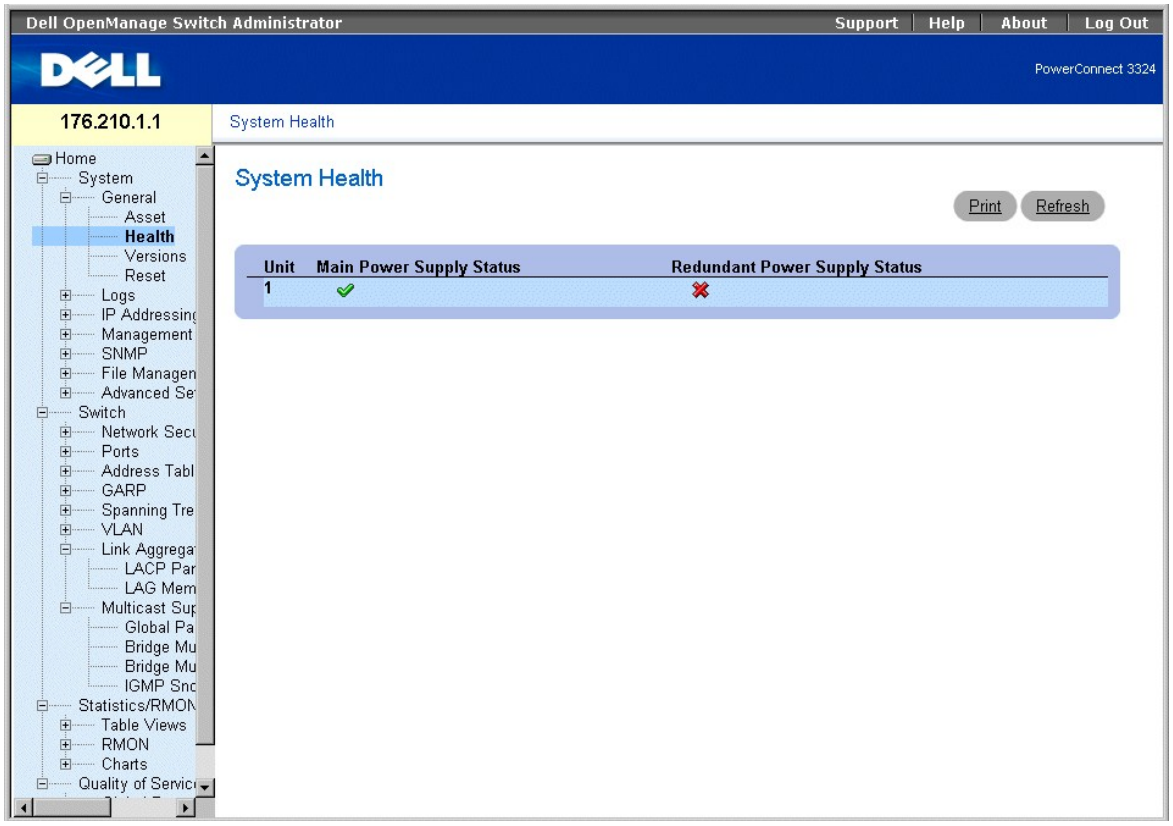
```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_York

Console (config)# exit

Console # exit

Console (config)# asset-tag lqwepot

Console> clock set 13:32:00 7 Mar 2002

Console> show clock

13:32:00 7 Mar 2002
```

```
     console# show system

     System Description:Ethernet Stackable Switching System

     System Up Time (days,hour:min:sec): 0,00:30:58

     System Contact:Dell_Tech_Supp

     System Name:dell

     System Location:New_York

MAC Address:00:00:b0:22:33:44

     Sys Object ID: 1.3.6.1.4.1.674.10895.3004

     Power supply Source Status

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

     Internal Power Supply Internal redundant OK unit1

     External Power Supply External OK unit1

     Internal PowerSupply Internal redundant OK unit2

     External PowerSupply External OK unit2

     Internal PowerSupply Internal redundant OK unit3

     External PowerSupply External OK unit3

     Internal PowerSupply Internal redundant OK unit6

     External PowerSupply External OK unit6
```

システムの動作状態情報の表示

System Health ページでは、物理的なデバイスのハードウェア情報が表示されます。**System Health** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **General** → **Health** とクリックします。 **SystemHealth** ページが開きます。



System Health ページ

System Health ページには、以下のフィールドが含まれています。

- **Unit** — スタッキングユニット番号を示します。
- **Main Power Supply Status** — 主電源装置の状態を示します。可能なフィールド値には、以下のものがあります。
  - — 指定されたユニットの主電源装置が正常に動作していることを示します。
  - — 指定されたユニットの主電源装置が正常に動作していないことを示します。
  - **Not Present** — 指定されたユニットの電源装置がないことを示します。
- **Redundant Power Supply Status** — 冗長電源装置の状態を示します。可能なフィールド値には、以下のものがあります。
  - — 指定されたユニットの冗長電源装置が正常に動作していることを示します。
  - — 指定されたユニットの冗長電源装置が正常に動作していないことを示します。
  - **Not Present** — 指定されたユニットの電源装置がないことを示します。

CLI コマンドを使用したシステムの動作状態情報の表示

次の表に、**System Health** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
show system	システム情報を表示します。

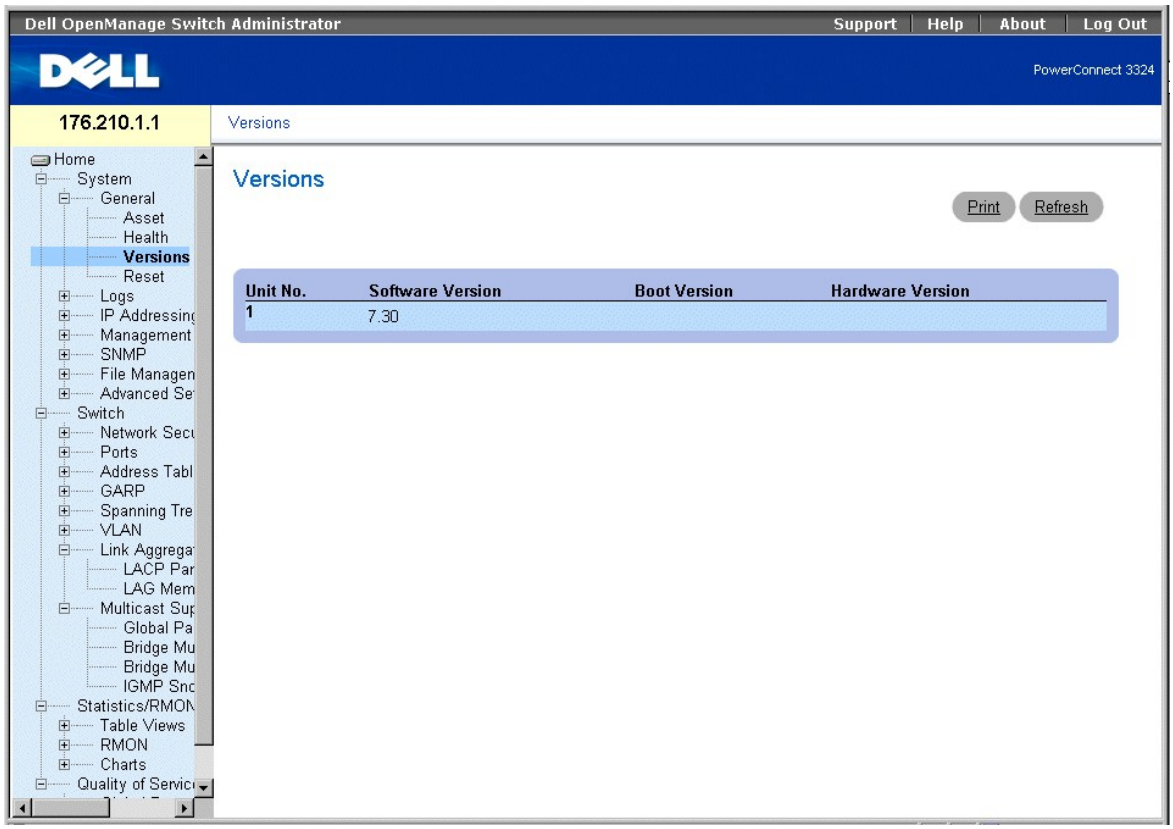
以下に、CLI コマンドの例を示します。

```
Console> show system

System Description:Ethernet Stackable Switching System

System Up Time (days,hour:min:sec): 0,00:08:56

System Contact:Dell_Tech_Supp

System Name:dell

System Location:New_York
```

バージョンページの表示

Versions ページには、現在動作中のハードウェアとソフトウェアのバージョンについての情報が含まれています。**Versions** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **General** → **Versions** とクリックします。
  Versions ページが開きます。



Versions ページ

Versions ページには、以下の情報が含まれています。

- **Unit No.** — スタッキングユニットの番号を示します。
- **Software Version** — 特定のスタッキングユニットで実行している現在のソフトウェアバージョンを表示します。
- **Boot Version** — 特定のスタッキングユニットで実行している現在の Boot バージョンを表示します。
- **Hardware Version** — 特定のスタッキングユニットで動作している現在のハードウェアバージョンを表示します。

CLI を使用したデバイスバージョンの表示

次の表に、**Versions** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
show version	システムのバージョン情報を表示します。

以下に、CLI コマンドの例を示します。

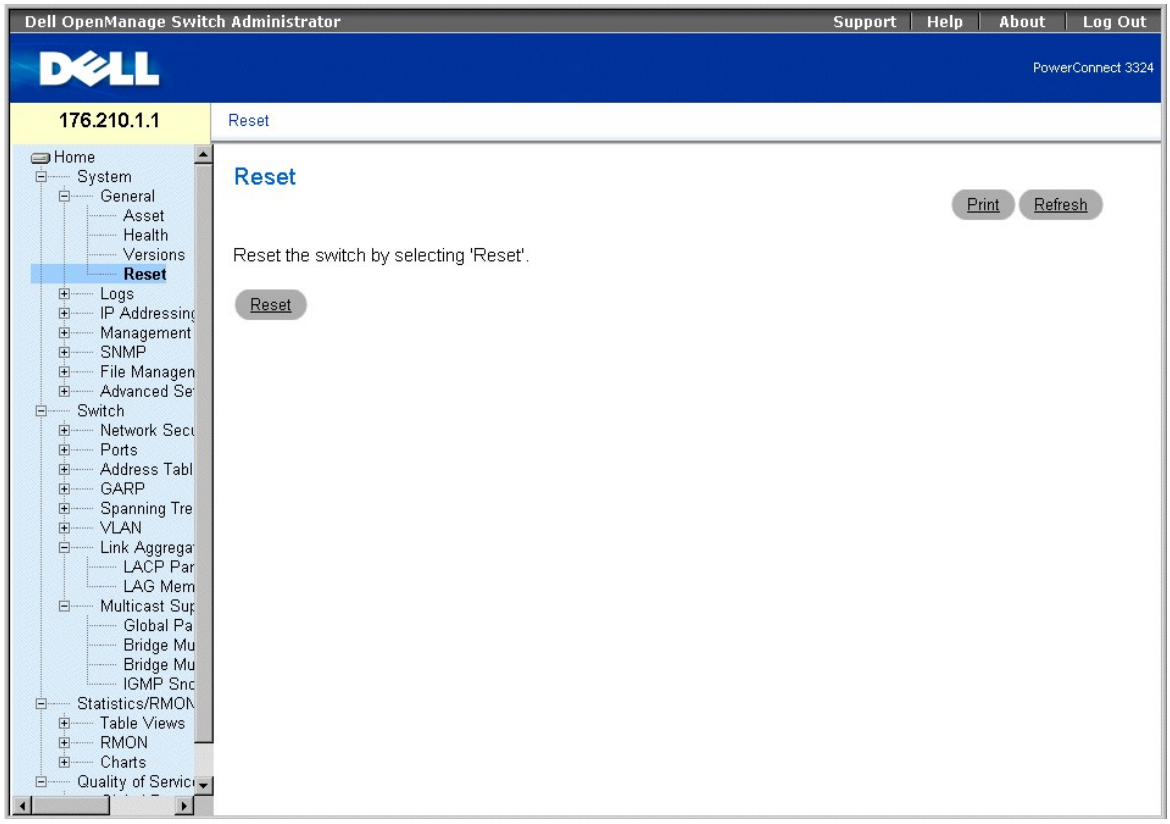
```
Console> show version


SW version 1.0.0.01 (date 14-Feb-2003 time 14:42:16 )
```

```
Boot version 1.30.11 ( date 27-Jan-2003 time 10:06:02 )


HW version 01.01.01
```

デバイスのリセット

Reset ページを使用して、ユーザーは離れた場所からデバイスをリセットできます。**Reset** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **General** → **Reset** とクリックします。
  Reset ページが開きます。



Reset ページ

メモ: 現在のデバイス設定を失わないよう、デバイスをリセットする前に、**Running Configuration** ファイルに変更をすべて保存してください。Configuration ファイルの保存については、「ファイルの管理」を参照してください。

デバイスをリセットするには、次の手順を実行します。

1. **Reset** ページを開きます。
2. **Reset**（リセット）をクリックします。確認メッセージが表示されます。

デバイスリセットの確認メッセージ

3. **OK**をクリックします。デバイスがリセットされます。デバイスがリセットされた後に、ユーザー名とパスワードを入力するよう求められます。

CLI を使用したデバイスのリセット

次の表に、**Reset** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
reload	オペレーティングシステムをリロードします。

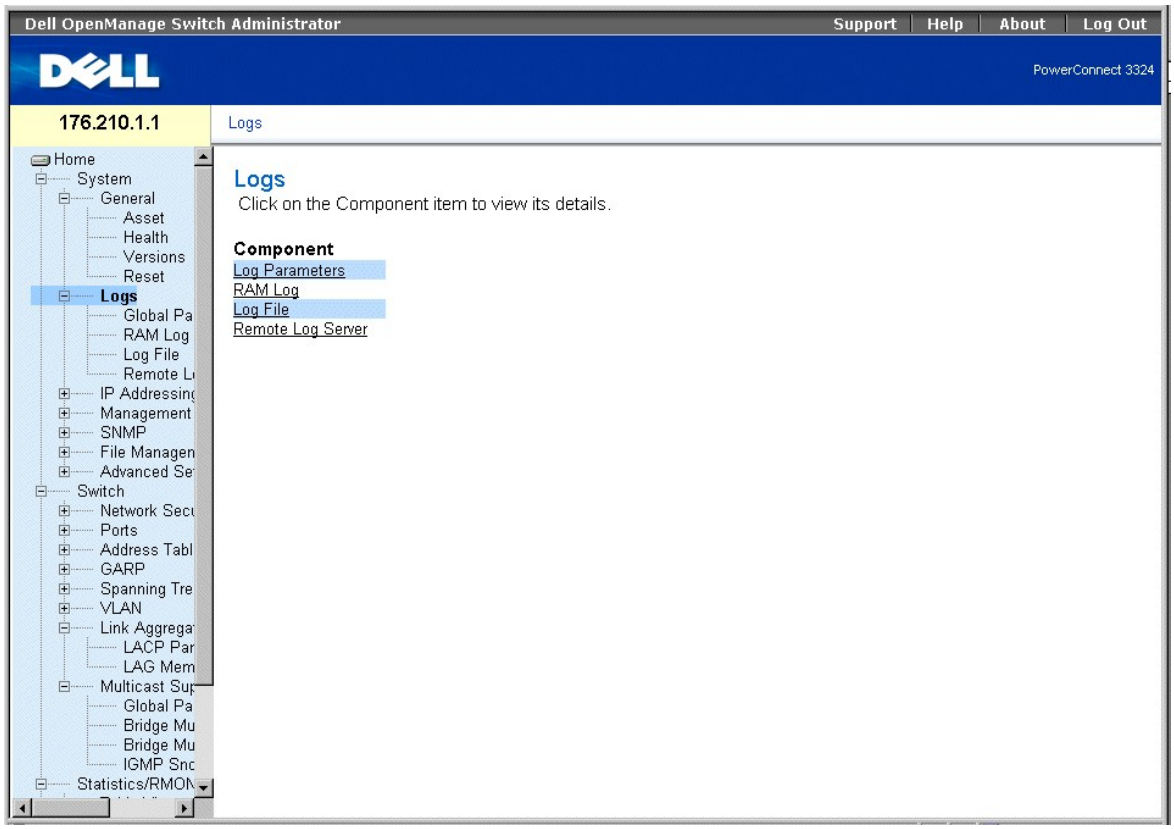
以下に、CLI コマンドの例を示します。

```
Console >reload

This command will reset the whole system and disconnect your current

session.Do you want to continue (y/n) [n] ?
```

ログの管理

Logs ページには、様々なログページへのリンクがあります。**Logs** ページを開くには、次の手順を実行します。

1. Tree View で、**System** → **Logs** をクリックします。**Logs** ページが開きます。



Logs ページ

Logs ページには、以下のページへのリンクがあります。

- グローバルログパラメータの定義
- RAM ログテーブルの表示
- ログファイルテーブルの表示
- リモートログサーバーの設定ページの表示

グローバルログパラメータの定義

System Log を使用して、重要なイベントのリアルタイムでの表示と今後のためにイベントを記録しておくことができます。この機能は、イベントのログと管理およびエラーの報告機能を提供します。

イベントメッセージは、Syslog+ local device reporting のように、すべてのエラー報告用の SYSLOG RFC 推奨メッセージ形式に基づいた固有の形式で示されます。メッセージには重要度コードが割り当てられ、メッセージ記憶用コードが含まれていますので、メッセージを生成したソースアプリケーションを特定できます。メッセージは、緊急度または関連度によってフィルタされます。各メッセージの重要度に応じて、メッセージが各イベントロギングデバイスに対して送信されるイベントロギングデバイスのセットが決定されます。以下の表に、ログ重要度レベルを示します。

ログ重要度レベル

重要度タイプ	重要度レベル	説明
Emergency	0	システムが機能していないことを示します。
警告	1	システムに対する作業がただちに必要であることを示します。
Critical	2	システムが危険な状態にあることを示します。

エラー	3	システムエラーが発生したことを示します。
Warning	4	システム警告が発生したことを示します。
Notice	5	システムは正常に機能していますが、システム注意が発生したことを示します。
Informational	6	デバイス情報を提供します。
Debug	7	ログについての詳細情報を提供します。

Global Log Parameters ページでは、どのイベントをどのログに記録するかを定義することができます。ログをグローバルに有効にするフィールドおよびログパラメータの定義用のパラメータが含まれています。Severity ログメッセージは重要度の高いものから低いものの順番で表示されています。**Global Log Parameters** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Logs** → **Global Parameters** とクリックします。**Global Log Parameters** ページが開きます。

Global Log Parameters ページ

Global Log Parameters ページには、以下のフィールドが含まれています。

- **Logging** — Cache、File、および Server Logs に対してデバイスのグローバルログを有効にします。Console ログはデフォルトで有効で、無効にすることはできません。可能なフィールド値には、以下のものがあります。
  - **Enable** — Cache (RAM)、File (フラッシュ)、および External Server へのログの保存を有効にします。
  - **Disable** — ログの保存を無効にします。Console ログは無効にできません。
- **Severity** — 利用可能な重要度ログには以下のものがあります。
  - **Emergency** — 最も高い警告レベルを示します。デバイスがダウンまたは適切に機能していない場合、緊急ログメッセージが指定されたロギング場所に保存されます。
  - **Alert** — 2 番目に高い警告レベルを示します。Alert ログは、すべてのデバイスの機能がダウンした場合などの深刻なデバイスの不具合が起こった場合に保存されます。

- **Critical** — 3 番目に高い警告レベルを示します。Critical ログは、2 つのデバイスポートが機能せず、残りのデバイスポートは機能している場合などの重要なデバイスの不具合が起こった場合に保存されます。
- **Error** — 単一のポートがオフラインになっている場合などのデバイスエラーが起こったことを示します。
- **Warning** — 最も低いデバイス警告レベルを示します。デバイスは機能していますが、動作上の問題が発生しました。
- **Notice** — ネットワーク管理者にデバイス情報を提供します。
- **Informational** — デバイス情報を提供します。
- **Debug** — ログについての詳細情報を提供します。Debug エラーが起こった場合、デルのオンラインテクニカルサポートにご連絡ください（**support.jp.dell.com**）。

メモ: 重要度レベルを選ぶと、そのレベル以上のすべての重要度レベルが自動的に選択されます。

Global Log Parameters ページには、特定のロギングシステムに対応するチェックボックスも含まれています。

- **Console** — ログがコンソールに送られる最低の重要度レベルを示します。
- **RAM Logs** — ログが RAM （キャッシュ） に保存されている Log File に送られる最低の重要度レベルを示します。
- **Log File** — ログがフラッシュメモリに保存されている Log File に送られる最低の重要度レベルを示します。

ログを有効にするには、次の手順を実行します。

1. **Global Log Parameters** ページを開きます。
2. **Logging** ドロップダウンリストから **Enable** を選びます。
3. **Global Log Parameters** チェックボックスで、ログタイプとログ重要度を選びます。
4. **Apply Changes** をクリックします。ログ設定が保存され、デバイスがアップデートされます。

CLI コマンドを使用したログの有効化

次の表に、**Global Log Parameters** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
logging on	エラーメッセージのロギングを有効にします。
logging ip-address [port port] [severity level] [facility facility] [description text]	シスログサーバーにメッセージを記録します。重要度レベルのリストについては、「ログ重要度レベル」を参照してください。
logging console level	重要度に基づいてコンソールに記録されるメッセージを制限します。
logging buffered level	重要度に基づいて内部バッファ （RAM） から表示されるシスログメッセージを制限します。
logging file level	重要度に基づいてログファイルへ送信されるシスログメッセージを制限します。
clear logging	ログをクリアします。

以下に、CLI コマンドの例を示します。

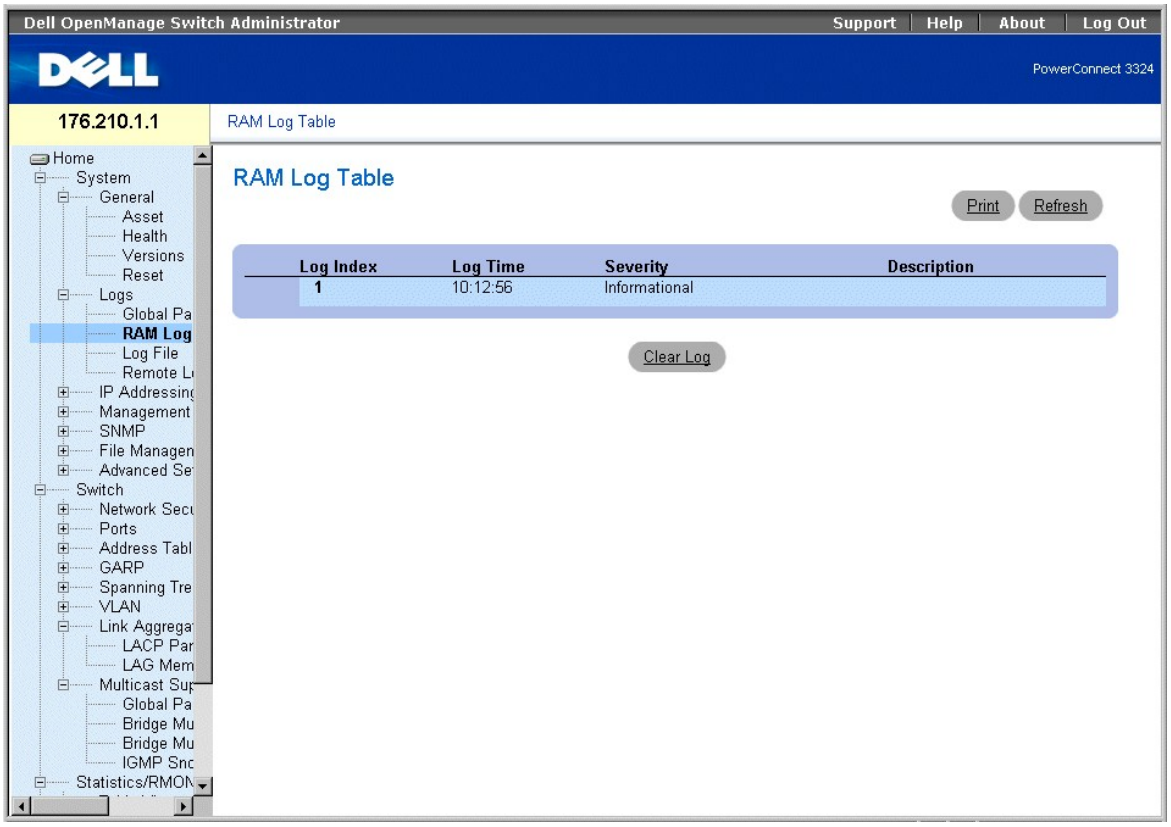
```
Console (config)# logging on

Console (config)# logging console errors
```

```
Console (config)# logging buffered debugging

Console (config)# logging file alerts

Console (config)# clear logging
```

RAM ログテーブルの表示

RAM Log Table には、ログが記録された時間、ログの重要度、およびログの説明など、RAM に保存されているログエントリについての情報が含まれています。**RAM Log Table** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Logs** → **RAM Log** とクリックします。
  RAM Log Table ページが開きます。



RAM Log Table ページ

RAM Log Table ページには、以下のフィールドが含まれています。

- **Log Index** — **RAM Log Table** 内のログ番号を示します。
- **Log Time** — **RAM Log Table** にログが記録された時間を示します。
- **Severity** — ログの重要度を示します。
- **Description** — ユーザー定義のログの説明を表示します。

ログ情報を削除するには、次の手順を実行します。

1. **RAM Log Table** ページを開きます。
2. **Clear Log** をクリックします。ログ情報が **RAM Log Table**/**Log File Table** から削除され、デバイスがアップデートされます。

CLI コマンドを使用した RAM ログテーブルの表示

次の表に、**RAM Log Table** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
show logging	ロギングの状態と内部バッファに保存されているシスログメッセージを表示します。
clear logging	ログをクリアします。

以下に、CLI コマンドの例を示します。

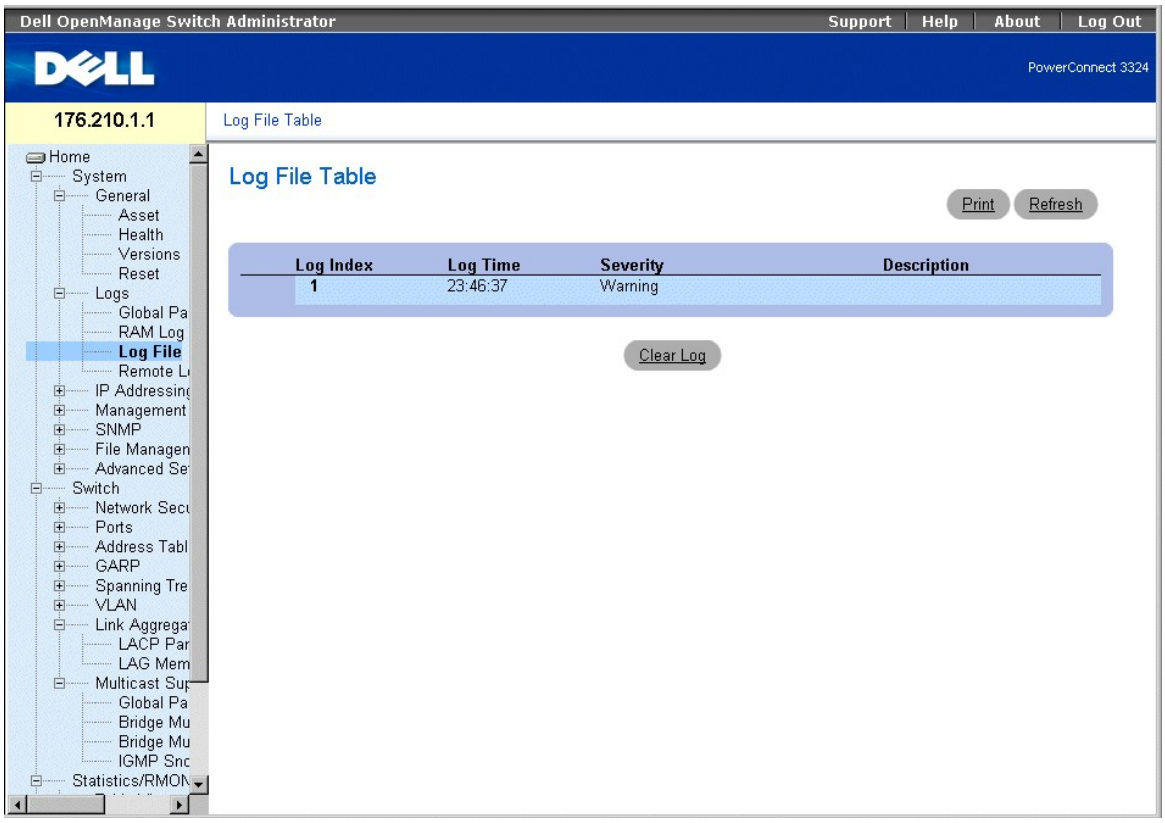
```
Console # show logging

Console logging:level debugging.Console Messages:0 Dropped (severity).

Buffer logging:level debugging.Buffer Messages:11 Logged, 200 Max.

File logging:level notifications.File Messages:0 Dropped (severity).

Syslog server 192.180.2.27 logging:errors.Messages:6 Dropped (severity).

Syslog server 192.180.2.28 logging:errors.Messages:6 Dropped (severity).

2 messages were not logged (resources)

Buffer log:

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface Ethernet1/e0, changed state to up

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface Ethernet1/e1, changed state to up

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface Ethernet1/e2, changed state to up
```

```
11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface Ethernet1/e3, changed state to up

11-Aug-2002 15:41:43:%SYS-5-CONFIG_I:Configured from memory by console

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1/e0, changed state to down

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1/e1, changed state to down

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1/e2, changed state to down

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1/e3, changed state to down

Console # clear logging

clear logging buffer [confirm]

Console#



Console # clear logging file

clear logging buffer [confirm]

Console#
```

ログファイルテーブルの表示

Log File Table には、ログが記録された時間、ログの重要度、およびログメッセージの説明など、フラッシュ内の Log File に保存されているログエントリについての情報が含まれています。**Log File Table** ページを開くには、次の手順を実行します。

1. Tree View で、**System** → **Logs** → **Log File** とクリックします。
   Log File Table ページが開きます。



Log File Table ページ

Log File Table ページには、以下のフィールドが含まれています。

- **Log Index** — **Log File Table** 内のログ番号を示します。
- **Log Time** — **Log File Table** にログが記録された時間を示します。
- **Severity** — ログの重要度を示します。
- **Description** — ログメッセージテキストを表示します。

CLI コマンドを使用したログファイルテーブルの表示

次の表に、**Log File Table** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
show logging file	ロギングの状態とログファイルに保存されているシスログメッセージを表示します。
clear logging	すべてのログファイルをクリアします。

以下に、CLI コマンドの例を示します。

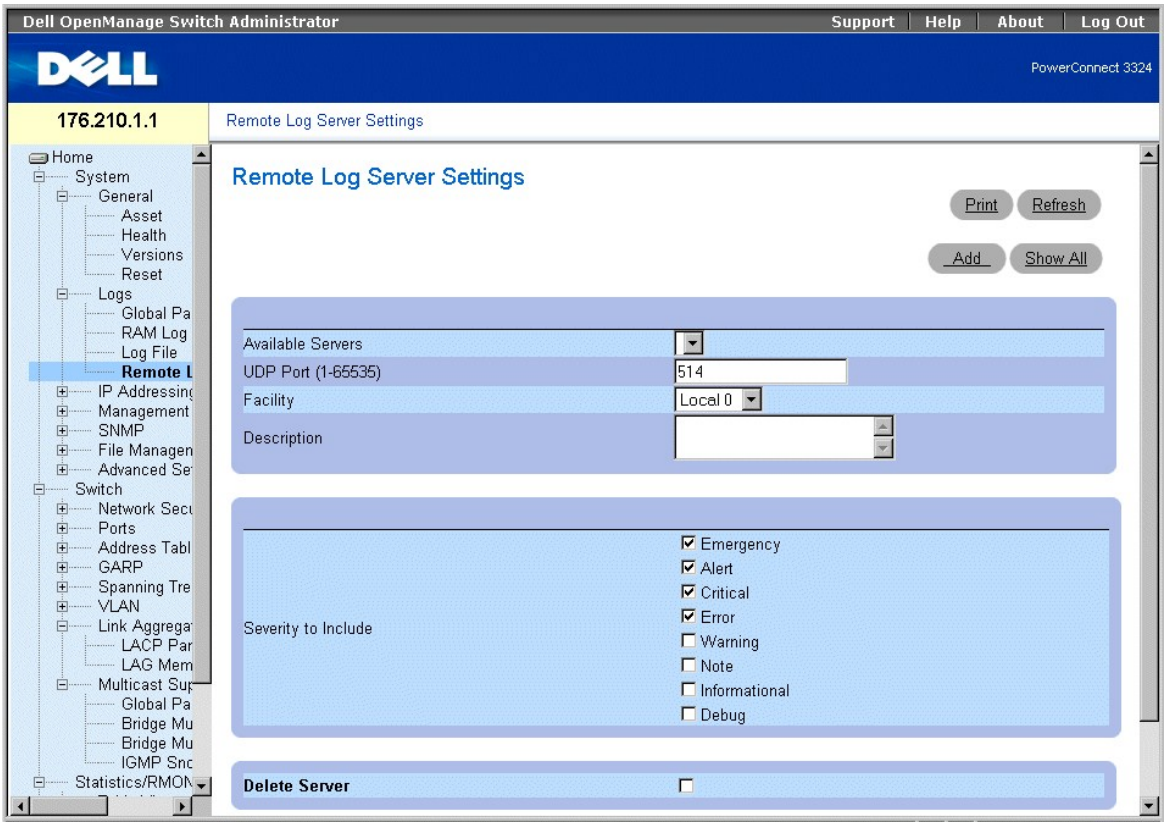
```
Console # show logging file
```

```
Console logging:level debugging.Console Messages:0 Dropped (severity).

Buffer logging:level debugging.Buffer Messages:11 Logged, 200 Max.

File logging:level notifications.File Messages:0 Dropped (severity).

Syslog server 192.180.2.27 logging:errors.Messages:6 Dropped (severity).

Syslog server 192.180.2.28 logging:errors.Messages:6 Dropped (severity).

2 messages were not logged (resources)

File log:

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface Ethernet1/e0, changed state to up

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface Ethernet1/e1, changed state to up

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface Ethernet1/e2, changed state to up

11-Aug-2002 15:41:43:%LINK-3-UPDOWN:Interface Ethernet1/e3, changed state to up

11-Aug-2002 15:41:43:%SYS-5-CONFIG_I:Configured from memory by console

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/0, changed state to up

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1/e0, changed state to down

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1/e1, changed state to down

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1/e2, changed state to down

11-Aug-2002 15:41:39:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1/e3, changed state to down
```

リモートログサーバーの設定ページの表示

Remote Log Server Settings ページには、利用可能な Logs Server を表示するためのフィールドが含まれています。また、新しいログサーバーと各サーバーに送信するログの重要度を定義できます。**Remote Log Server Settings** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Logs** → **Remote Log Server** とクリックします。**Remote og Server Settings** ページが開きます。



Remote Log Server Settings ページ

Remote Log Server Settings ページには、以下のフィールドが含まれています。

- **Available Servers** — ログを受信できるサーバーのリストがあります。
- **UDP Port (1-65535)** — 選択されたサーバーに対してログが送信される UDP ポートを示します。可能な範囲は 1 ～ 65,535 で、デフォルト値は 514 です。
- **Facility** — 選択されたサーバーのファシリティマッピングのレベルを示します。
  デフォルト値は Local 0 です。可能な値には、以下のものがあります。
  - **Local 0 - Local 7.**
  - **No Map.**
- **Description** — ユーザー定義のサーバーの説明を表示します。
- **Delete Server** — **Available Servers** リストから現在選択されているサーバーを削除します。可能なフィールド値には、以下のものがあります。
  - **Checked** — **Available Servers** リストからサーバーを削除します。
  - **Unchecked** — **Available Servers** リスト内のサーバーを保持します。

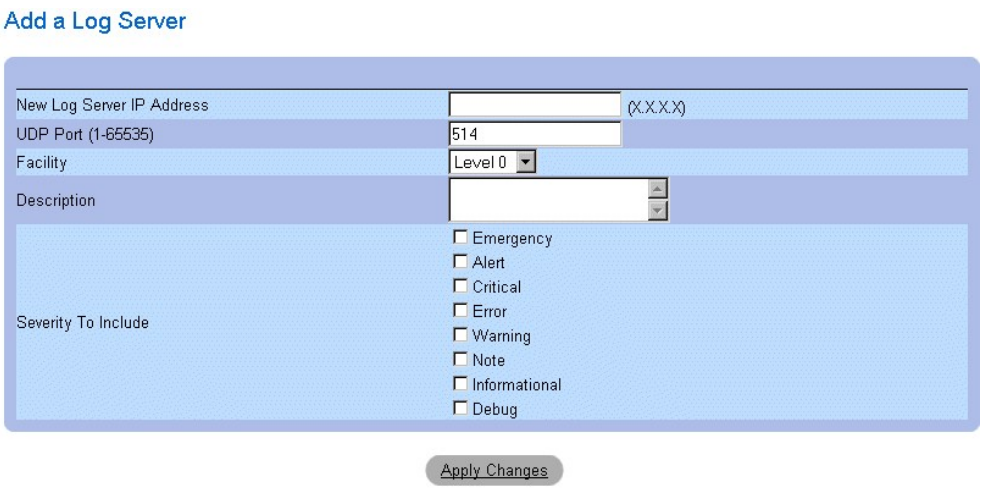
Remote Log Server Settings ページには、重要度リストも含まれています。重要度の定義は、「Global Log Parameters ページ」にある重要度定義と同じです。

ログをサーバーへ送信するには、次の手順を実行します。

1. **Remote Log Server Settings** ページを開きます。
2. **Available Servers** ドロップダウンリストからサーバーを選びます。
3. **UDP Port**、**Facility**、および **Description** フィールドを定義します。
4. **Severity to Include** チェックボックスでログ重要度を選びます。
5. **Apply Changes** をクリックします。ログ設定が保存され、デバイスがアップデートされます。

新しいサーバーを定義するには、次の手順を実行します。

1. **Remote Log Server Settings** ページを開きます。
2. **Add** （追加）をクリックします。**Add a Log Server** ページが開きます。



Add a Log Server ページ

Remote Log Server Settings ページのフィールドに加えて、**Add a Log Server** ページには以下のフィールドが含まれています。

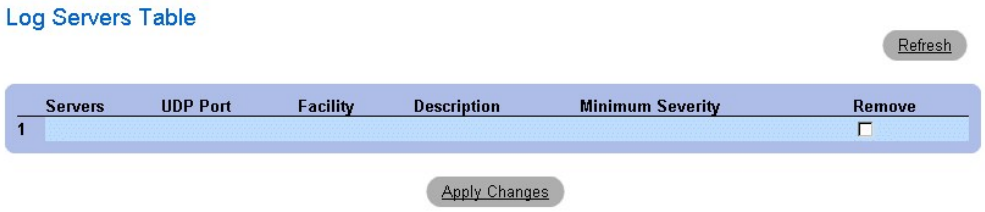
- **New Log Server IP Address** — 新しい Log Server の IP アドレスを指定します。

Log Server を追加するには、次の手順を実行します。

1. **New Log Server IP Address**、**UDP Port**、**Facility**、および **Description** フィールドを定義し、**Severity To Include** チェックボックスを選びます。
2. **Apply Changes** をクリックします。サーバーが定義され、 **Available Servers** リストに追加されます。

Log Servers Table を表示するには、次の手順を実行します。

1. **Remote Log Server Settings** ページを開きます。
2. **Show All** をクリックします。**Log Servers Table** ページが開きます。



Log Servers Table ページ

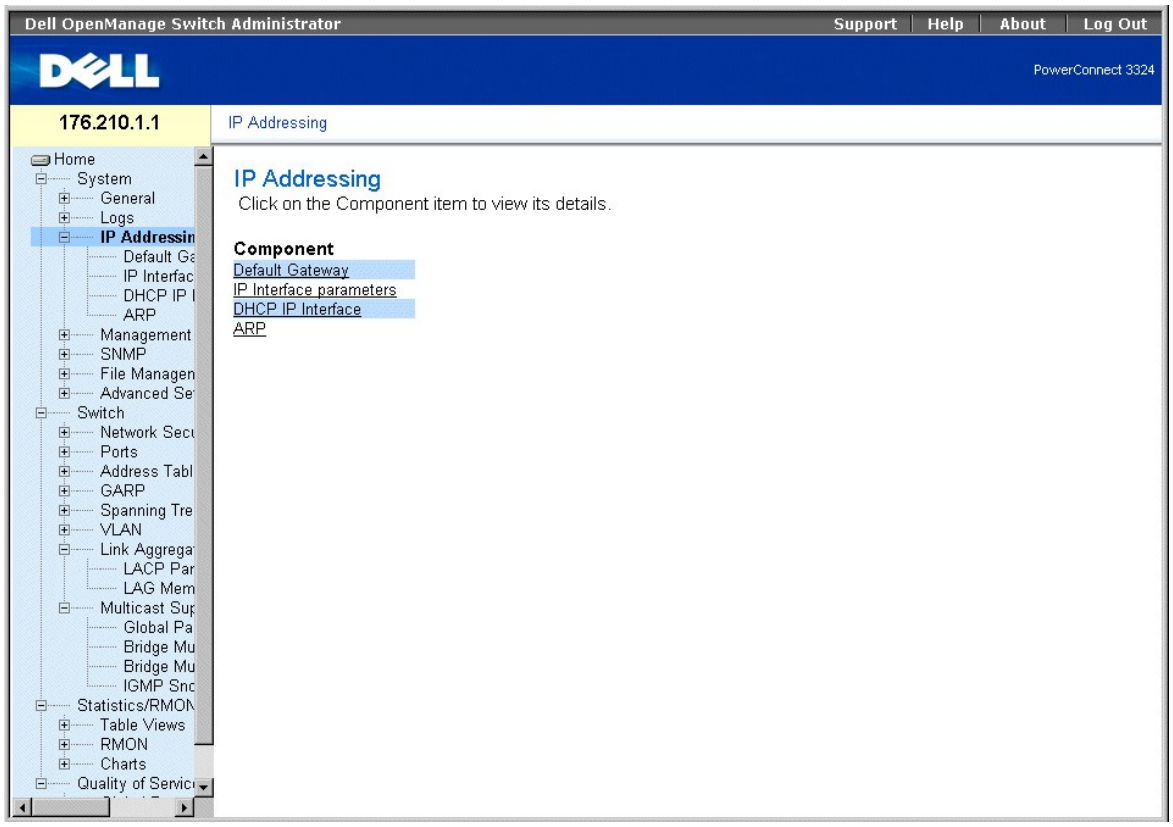
Log Servers Table ページから Log Server を削除するには、次の手順を実行します。

1. **Remote Log Server Settings** ページを開きます。
2. **Show All** をクリックします。**Log Servers Table** ページが開きます。
3. **Log Servers Table** エントリを選びます。
4. 削除するサーバーの **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。**Log Servers Table** エントリが削除され、デバイスがアップデートされます。

デバイスの IP アドレスの定義

IP Addressing ページには、インタフェースとデフォルトゲートウェイ IP アドレスの割り当て、およびインタフェース用の ARP と DHCP パラメータの定義用のリンクが含まれています。**IP Addressing** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **IP Addressing** とクリックします。
  IP Addressing ページが開きます。



IP Addressing ページ

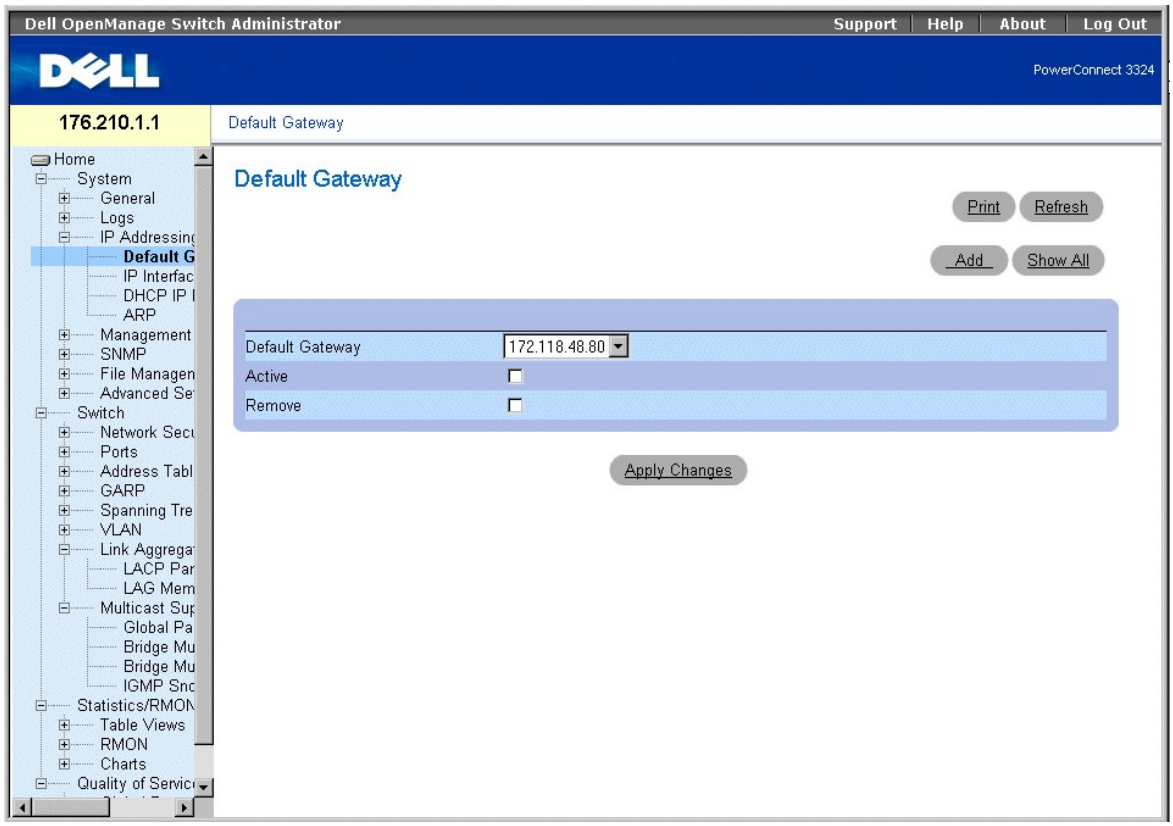
IP Addressing ページには、以下のページへのリンクがあります。

- デフォルトゲートウェイの設定
- IP インタフェースの定義
- DHCP IP インタフェースの定義
- ARP の設定

デフォルトゲートウェイの設定

Default Gateway ページを使用して、ネットワーク管理者は Gateway デバイスを割り当てることができます。フレームがリモートネットワークに送信される際に、パケットはデフォルトの IP に転送されます。設定された IP アドレスは、IP インタフェースのうちの 1 つの同じ IP アドレスサブネットに属している必要があります。**Default Gateway** ページを開くには、次の手順を実行します。

- Tree View で、**System → IP Addressing → Default Gateway** とクリックします。**Default Gateway** ページが開きます。



Default Gateway ページ

Default Gateway ページには、以下のフィールドが含まれています。

- **Default Gateway** — Gateway デバイスの IP アドレスを示します。
- **Active** — **Default Gateway** ドロップダウンリストで指定されている Default Gateway デバイスが現在アクティブかどうかを示します。可能なフィールド値には、以下のものがあります。
  - **Checked** — Gateway デバイスが現在アクティブであることを示します。
  - **Unchecked** — Gateway デバイスが現在アクティブでないことを示します。
- **Remove** — **Default Gateway** ドロップダウンリストから Gateway デバイスを削除します。
  - **Checked** — **Default Gateway** ドロップダウンリストから選択した Gateway デバイスを削除します。
  - **Unchecked** — **Default Gateway** ドロップダウンリストで Gateway デバイスを保持します。

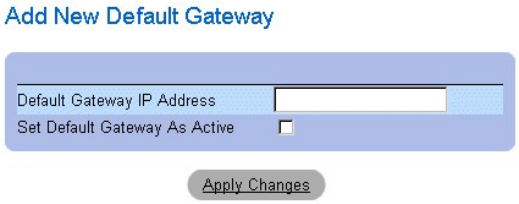
Gateway デバイスを選択するには、次の手順を実行します。

1. **Default Gateway** ページを開きます。
2. **Default Gateway** ドロップダウンリストで IP アドレスを選びます。
3. **Active** チェックボックスにチェックマークを付けます。
4. **Apply Changes** をクリックします。Gateway デバイスが選択され、 **Active**フィールドにステータスが表示されます。

Gateway デバイスを追加するには、次の手順を実行します。

1. **Default Gateway** ページを開きます。

2. **Add**（追加）をクリックします。**Add New Default Gateway** ページが開きます。



Add New Default Gateway ページ

3. **Default Gateway IP Address** フィールドを定義します。

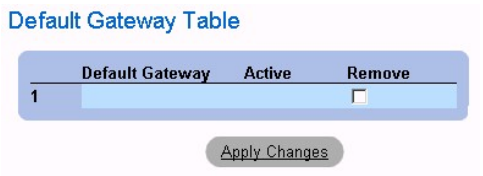
   または

   チェックボックスにチェックマークを付けて、新しいゲートウェイをアクティブに設定します。

4. **Apply Changes** をクリックします。新しい Default Gateway デバイスが定義され、デバイスがアップデートされます。

Default Gateway Table を表示するには、次の手順を実行します。

1. **Default Gateway** ページを開きます。
2. **Show All** をクリックします。**Default Gateway Table** ページが開きます。



Default Gateway Table ページ

Default Gateway デバイスを削除するには、次の手順を実行します。

1. **Default Gateway** ページを開きます。
2. **Show All** をクリックします。**Default Gateway Table** ページが開きます。
3. **Default Gateway Table** エントリを選びます。
4. 削除するデフォルトゲートウェイの **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。Default Gateway Table エントリが削除され、デバイスがアップデートされます。

CLI コマンドを使用したゲートウェイデバイスの定義

次の表に、**Default Gateway** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
ip default-gateway ip-address1 [ip-address2.]	デフォルトゲートウェイを定義します。
no ip default-gateway [ip-address]	デフォルトゲートウェイを削除します。

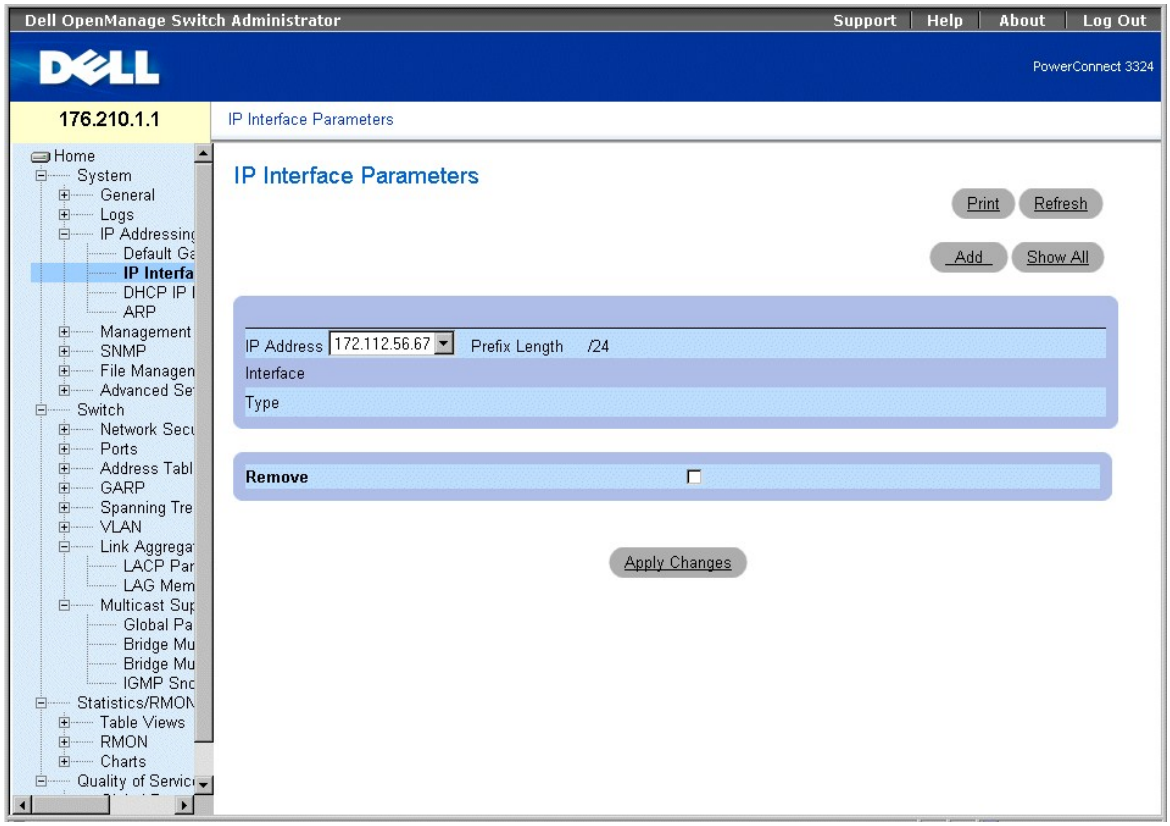
以下に、CLI コマンドの例を示します。

```
Console (config)# ip default-gateway 196.210.10.1

Console (config)# no ip default-gateway 196.210.10.1
```

IP インタフェースの定義

IP Interface Parameters ページには、インタフェースに IP アドレスを割り当てるためのパラメータが含まれています。**IP Interface Parameters** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **IP Addressing** → **IP Interface Parameters** とクリックします。**IP Interface Parameters** ページが開きます。



IP Interface Parameters ページ

IP Interface Parameters ページには、以下のフィールドが含まれています。

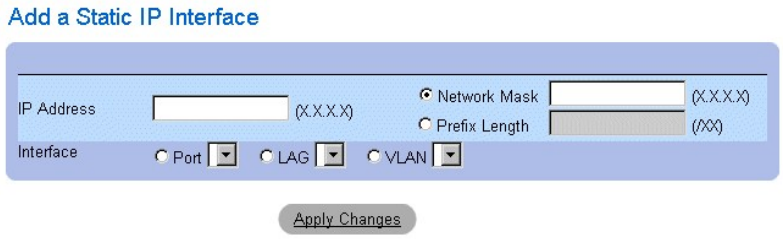
- **IP Address** — インタフェース IP アドレスのリストを示します。
- **Interface** — 選択された IP アドレスに対して定義されたインタフェースタイプを示します。可能なフィールド値には、以下のものがあります。
  - **Port** — IP アドレスがポートに割り当てられたことを示します。

- **LAG** — IP アドレスが LAG (Link Aggregated Group) に割り当てられたことを示します。
- **VLAN** — IP アドレスが VLAN に割り当てられたことを示します。

- **Type** — IP アドレスが静的 IP アドレスとして手動で定義されているか、DHCP を介して自動的に定義されているかを示します。
- **Remove** — **IP Address** ドロップダウンリストから選択したインタフェースを削除します。
  - **Checked** — **IP Address** ドロップダウンリストからインタフェースを削除します。
  - **Unchecked** — **IP Address** ドロップダウンリストでインタフェースを保持します。

IP インタフェースを追加するには、次の手順を実行します。

1. **IP Interface Parameters** ページを開きます。
2. **Add** （追加）をクリックします。**Add a Static IP Interface** ページが開きます。

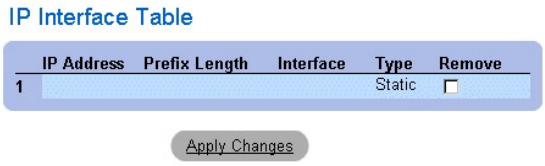


Add a Static IP Interface ページ

3. **IP Address**、**Interface**、**Network Mask**、または **Prefix Length** フィールドを定義します。
4. IP インタフェースを割り当てるインタフェースを選びます。
5. **Apply Changes** をクリックします。新しいインタフェースが追加され、デバイスがアップデートされます。

IP Interface Table を表示するには、次の手順を実行します。

1. **IP Interface Parameters** ページを開きます。
2. **Show All** をクリックします。**IP Interface Table** ページが開きます。 **IPInterface Table** ページには、「IP インタフェースの定義」 と同じフィールドが含まれています。



IP Interface Table ページ

IP アドレスを削除するには、次の手順を実行します。

1. **IP Interface** ページを開きます。
2. **Show All** をクリックします。**IP Interface Table** ページが開きます。
3. **IP Interface Table** でエントリを選びます。

4. 削除する IP アドレスの **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。IP アドレスが削除され、デバイスがアップデートされます。

CLI コマンドを使用した IP インタフェースの定義

次の表に、**IP Interface Parameters** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
ip address *ip-address {mask | prefix-length}*	IP アドレスを設定します。
no ip address [ip-address]	IP アドレスを削除します。
show ip interface [ethernet *interface-number* **| vlan** *vlan-id* **| port-channel** *number]*	IP に対して設定するインタフェースの使用可能ステータスを表示します。

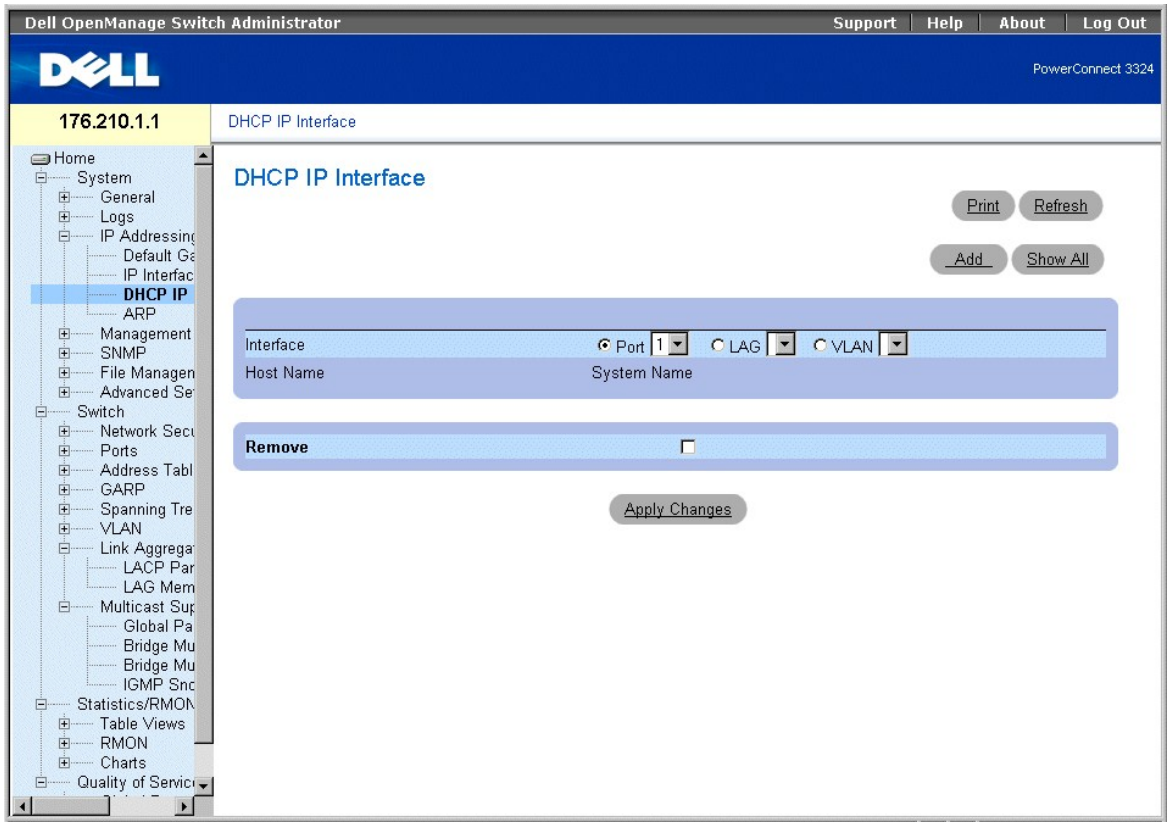
以下に、CLI コマンドの例を示します。

```
Console (config)# interface vlan 1

Console (config-if)# ip address 131.108.1.27 255.255.255.0

Console (config-if)# no ip address 131.108.1.27

Console (config-if)# exit

Console# show ip interface vlan 1

Internet address is 10.7.1.192/24

console# show ip interface vlan 204



IP Address Directed Broadcast

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

146.1.0.132/29 disable



console#
```

DHCP IP インタフェースの定義

DHCP IP Interface ページでは、インタフェースごとのデバイスの DHCP クライアント設定を指定します。

- Tree View で、**System** → **IP Addressing** → **DHCP IP Interface** とクリックします。**DHCP IP Interface** ページが開きます。



DHCP IP Interface ページ

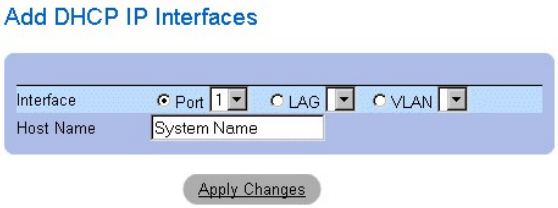
DHCP IP Interface ページには、以下のフィールドが含まれています。

- Interface — デバイスのインタフェースを選びます。
  - **Port** — インタフェースタイプがポートであることを示し、DHCP クライアント設定が表示されている特定のポート番号を示します。
  - **LAG** — インタフェースタイプが LAG であることを示し、DHCP クライアント設定が表示されている特定の LAG 番号を示します。
  - **VLAN** — インタフェースタイプが VLAN であることを示し、DHCP クライアント設定が表示されている特定の VLAN 番号を示します。
- **Host Name** — システム名を示します。
- **Remove** — **DHCP IP Interfaces Table** から選択されたインタフェースの DHCP クライアントインスタンスを削除します。
  - **Checked** — **DHCP IP Interfaces Table** からインタフェースを削除します。
  - **Unchecked** — **DHCP IP Interfaces Table** でインタフェースを保持します。

DHCP IP インタフェースを追加するには、次の手順を実行します。

1. **DHCP IP Interface** ページを開きます。

2. **Add** （追加）をクリックします。**Add DHCP IP Interfaces** ページが開きます。



Add DHCP IP Interfaces ページ

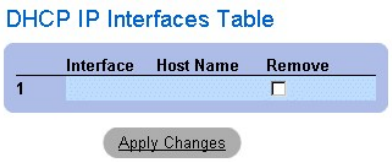
3. **Interface** を選び、**Host Name** を定義します。
4. **Apply Changes** をクリックします。新しい DHCP IP Interface が追加され、デバイスがアップデートされます。

DHCP IP Interface を変更するには、次の手順を実行します。

1. **DHCP IP Interface** ページを開きます。
2. **Interface** フィールドを変更します。
3. **Apply Changes** をクリックします。エントリが変更され、デバイスがアップデートされます。

DHCP IP Interfaces Table を表示するには、次の手順を実行します。

1. **DHCP IP Interface** ページを開きます。
2. **Show All** をクリックします。**DHCP IP Interfaces Table** ページが開きます。



DHCP IP Interfaces Table ページ

DHCP IP Interface を削除するには、次の手順を実行します。

1. **DHCP IP Interface** ページを開きます。
2. **Show All** をクリックします。**DHCP IP Interfaces Table** が開きます。
3. DHCP クライアントエントリを選びます。
4. **Remove** チェックボックスにチェックマークを付けて、DHCP クライアントエントリを削除します。
5. **Apply Changes** をクリックします。**DHCP IP Interfaces Table** エントリが削除され、デバイスがアップデートされます。

CLI コマンドを使用した DHCP クライアントの定義

次の表に、**DHCP IP Interface** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
ip address-dhcp [hostname *host-name*]	DHCP から Ethernet インタフェースの IP アドレスを取得します。

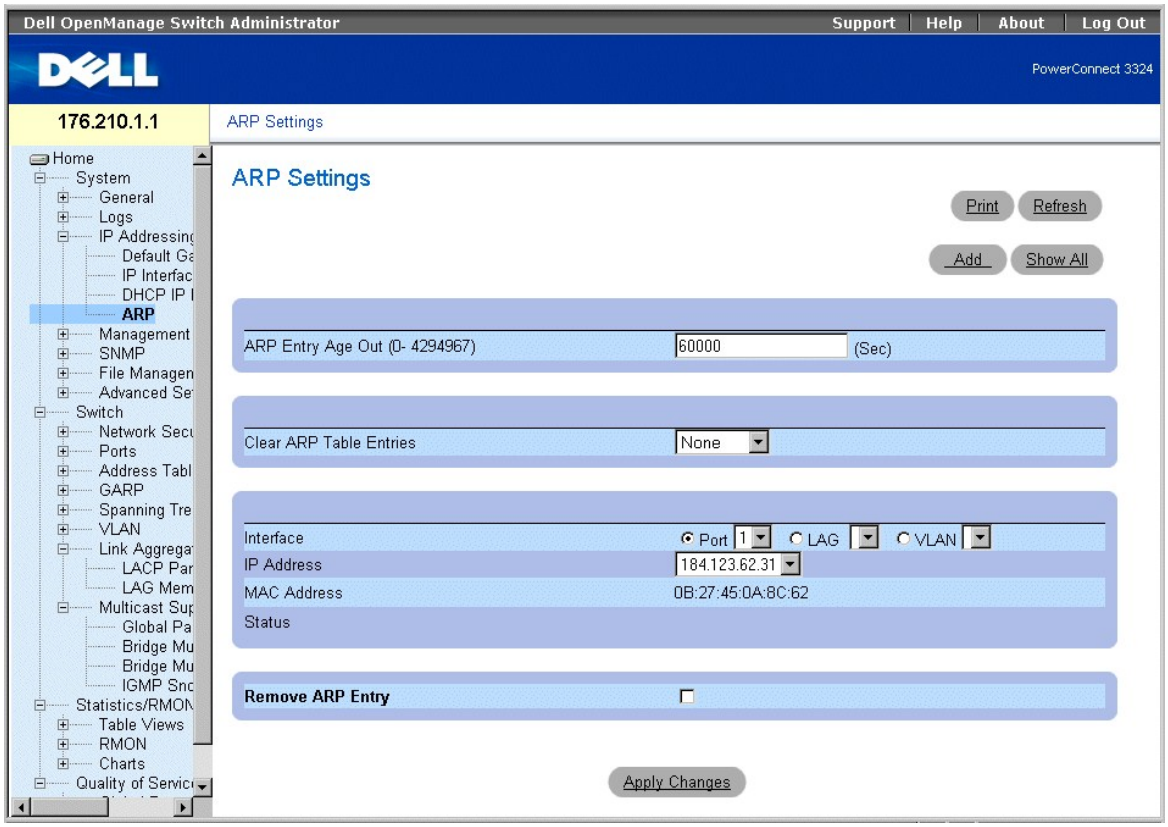
以下に、CLI コマンドの例を示します。

```
Console (config)# interface ethernet 1/e8

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

ARP の設定

ARP (**Address Resolution Protocol**) は、IP アドレスを物理的なアドレスに変換する TCP/IP プロトコルです。静的エントリを ARP Table で定義することができます。静的エントリを定義すると、恒久的なエントリが入力され、IP アドレスを MAC アドレスに変換するのに使用されます。**ARP Settings** ページを開くには、次の手順を実行します。

- Tree View で、**System → IP Addressing → ARP** とクリックします。**ARPSettings** ページが開きます。



ARP Settings ページ

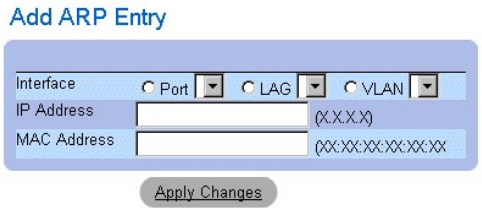
ARP Settings ページには、以下のフィールドが含まれています。

- **ARP Entry Age Out (0-4294967)** — ARP エントリがエージアウトするまでの時間を秒で示します。この時間が経過すると、エントリはテーブルから削除されます。デフォルト値は 60,000 秒です。

- **Clear ARP Table Entries** — クリアする ARP エントリのタイプを示します。
  可能なフィールド値には、以下のものがあります。
  - **None** — ARP エントリはクリアされないことを示します。
  - **All** — すべての ARP エントリがクリアされることを示します。
  - **Static** — 静的 ARP エントリのみがクリアされることを示します。
  - **Dynamic** — 動的 ARP エントリのみがクリアされることを示します。
- **Interface** — インタフェースタイプおよび特定のインタフェース番号を選びます。
  可能なフィールド値には、以下のものがあります。
  - **Port** — ARP を定義できるポートのリストが含まれています。
  - **LAG** — ARP を定義できる LAG のリストが含まれています。
  - **VLAN** — ARP を定義できる VLAN のリストが含まれています。
- **IP Address** — 指定されたインタフェースに関連する IP アドレスを選びます。
- **MAC Address** — 関連する MAC アドレスを示します。
- **Status** — **ARP Table** エントリのステータスを示します。可能なフィールド値には、以下のものがあります。
  - **Other** — ARP エントリが動的に学習されたものでも、静的エントリでもないことを示します。
  - **Invalid** — ARP エントリが無効であることを示します。
  - **Dynamic** — ARP エントリが動的に学習されたことを示します。
  - **Static** — ARP エントリが静的エントリであることを示します。
- Remove ARP Entry — **ARP Table** から ARP エントリを削除します。
  - **Checked** — 特定の ARP エントリを削除します。
  - **Unchecked** — ARP エントリを保持します。

静的 ARP Table エントリを追加するには、次の手順を実行します。

1. **ARP Settings** ページを開きます。
2. **Add** （追加）をクリックします。**Add ARP Entry** ページが開きます。

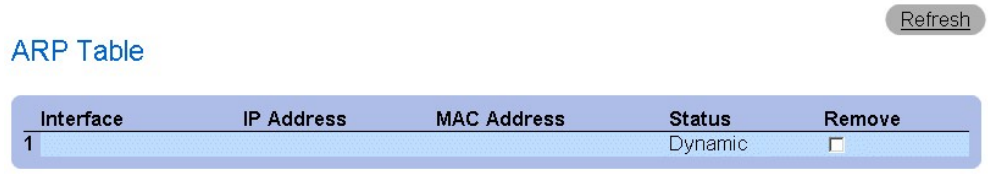


Add ARP Entry ページ

3. **Interface** を選び、**IP Address** および **MAC Address** フィールドを定義します。
4. **Apply Changes** をクリックします。**ARP Table** エントリが追加され、デバイスがアップデートされます。

ARP Table を表示するには、次の手順を実行します。

1. **ARP Settings** ページを開きます。
2. **Show All** をクリックします。**ARP Table** ページが開きます。



ARP Table ページ

ARP Table エントリを削除するには、次の手順を実行します。

1. **ARP Settings** ページを開きます。
2. **Show All** をクリックします。**ARP Table** ページが開きます。
3. テーブルエントリを選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。**ARP Table** エントリが削除され、デバイスがアップデートされます。

CLI コマンドを使用した ARP の設定

次の表に、**ARP Settings** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
arp *ip_addr hw_addr* **{ethernet** *interface-number* **| vlan** *vlan-id* **| port-channel** *number***}**	ARP キャッシュに恒久的なエントリを追加します。
arp timeout seconds	エントリがどのくらいの時間 ARP キャッシュに保存されるかを設定します。
show arp	ARP Table のエントリを表示します。
no arp	ARP Table から ARP エントリを削除します。

以下に、CLI コマンドの例を示します。

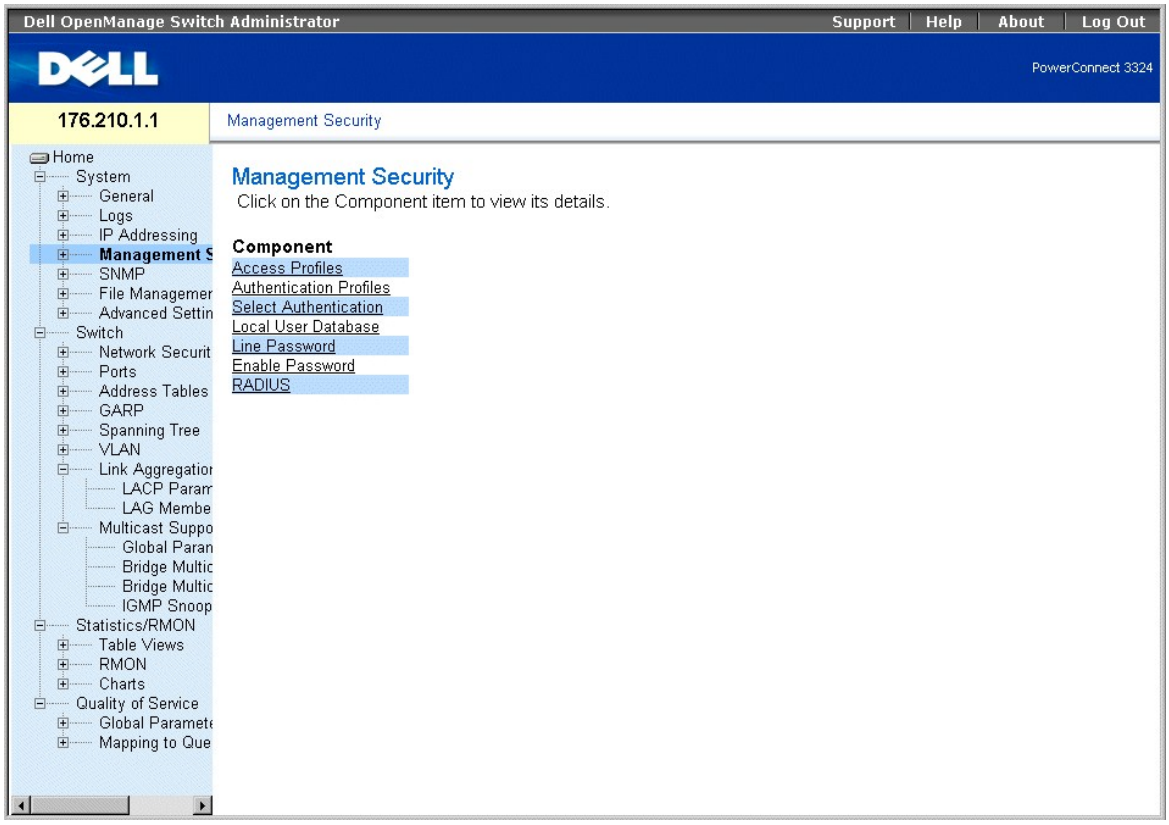
```
console(config)# arp 146.1.0.131 00-00-55-66-77-00 ethernet 1/e1

Console (config)# exit

Console# arp timeout 12000

Console# show arp

Interface IP address HW address Status

---- ---------- ----------------- -------
```

```
1/e1 10.7.1.102 00:10:B5:04:DB:4B Dynamic

2/e2 10.7.1.135 00:50:22:00:2A:A4 Static
```

デバイスのセキュリティ管理

Management Security ページでは、ネットワーク管理者がポート、デバイスの管理方法、ユーザー、およびサーバーセキュリティのセキュリティパラメータを設定できるセキュリティページへのアクセスを提供します。**Management Security** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Management Security** とクリックします。**Management Security** ページが開きます。



Management Security ページ

この項には以下のトピックがあります。

- アクセスプロファイルの定義
- 認証プロファイルの定義
- 認証プロファイルの割り当て
- ローカルユーザーデータベースの定義
- ラインパスワードの定義
- 有効化パスワードの定義
- RADIUS グローバルパラメータの設定

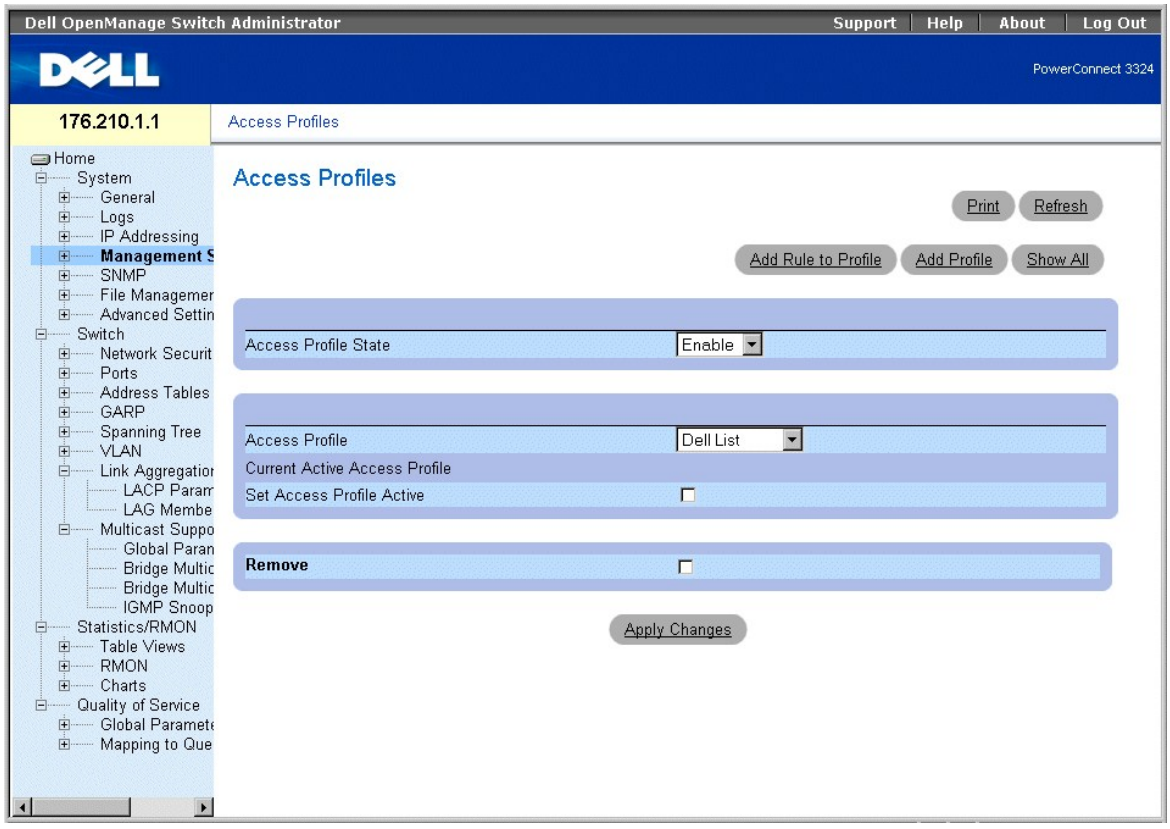
アクセスプロファイルの定義

Access Profiles ページを使用して、ネットワーク管理者はデバイスへのアクセスのプロファイルおよび規則を定義することができます。管理アクセス方法は、進入ポート、Source IP アドレス、およびサブネットマスクによって、特定のユーザーグループに限定することができます。管理アクセス方法は、以下のものに対して個別に定義することができます。

- Web Access (HTTP)
- Secure Web Access (HTTPS)
- Telnet
- SNMP
- 上記すべて

1 つの管理サービスにアクセスしているユーザーは、別の管理サービスを管理しているユーザーと異なる場合があります。Management Access List は、デバイスの管理方法およびデバイスの管理者を決定する規則で構成されています。**Access Profiles** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Management Security** → **Access Profiles** とクリックします。**Access Profiles** ページが開きます。



Access Profiles ページ

Access Profiles ページには、以下のフィールドが含まれています。

- **Access Profile State** — デバイスで Access Profiles を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — デバイスで Access Profile Security Management を有効にします。

- **Disable** — デバイスで Access Profile Security Management を無効にします。Access Profile Security Management が無効になっている場合、デバイスはすべてのステーションにアクセス可能です。

- **Access Profile** — ユーザー定義の **Access Profile Lists** のリストが含まれています。**Access Profile** リストには、以下のデフォルト値が含まれています。
  - **Console Only** — コンソールを介してのみアクセス可能です。Console Only を選択すると、HTTP および Telnet セッションが切断されます。これはデフォルト値で、削除できません。
- **Current Active Access Profile** — 現在アクティブな Access Profile を表示します。
- **Set Access Profile Active** — 選択した Access Profile をアクティブにします。
- **Remove** — **Access Profile Names** から選択した Access Profile を削除します。
  - **Checked** — Access Profile を削除します。
  - **Unchecked** — Access Profile を保持します。

メモ: アクティブなプロファイルは削除できません。

プロファイルをアクティブにするには、次の手順を実行します。

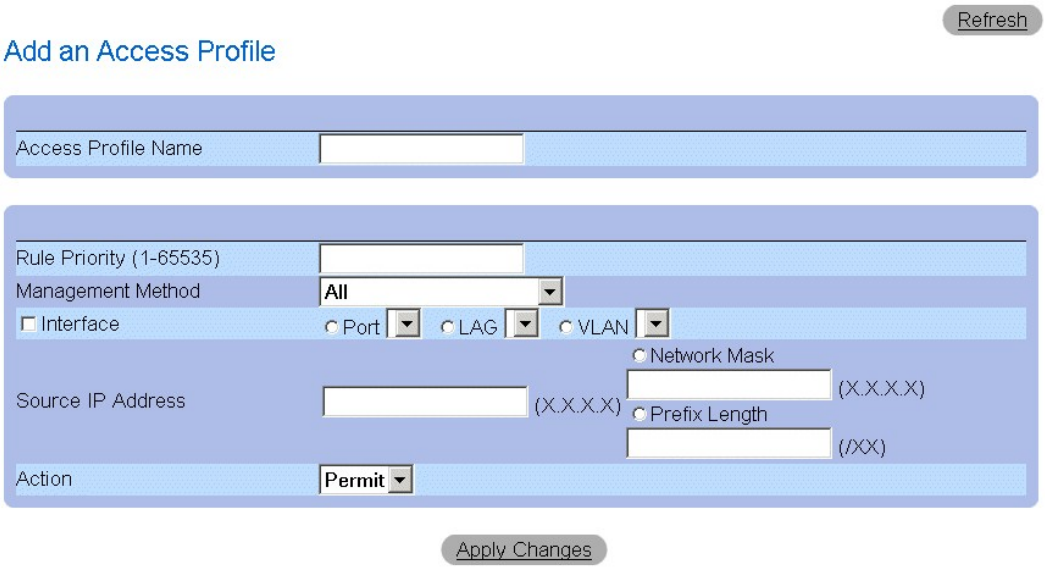
1. **Access Profiles** ページを開きます。
2. **Access Profile** フィールドで Access Profile を選びます。
3. **Set Access Profile Active** チェックボックスにチェックマークを付けます。
4. **Apply Changes** をクリックします。Access Profile がアクティブになります。

Access Profile を追加するには、次の手順を実行します。

規則は、規則優先度の決定、デバイスの管理方法、インタフェースタイプ、送信元の IP アドレスとネットワークマスク、およびデバイスの管理アクセスアクションを決定するためのフィルタとして機能します。ユーザーに対して管理アクセスをブロックしたり、許可したりできます。規則優先度は、プロファイルの規則適用順序を設定します。

Access Profile の規則を定義するには、次の手順を実行します。

1. **Access Profiles** ページを開きます。
2. **Add Profile** をクリックします。**Add an Access Profile** ページが開きます。



Add an Access Profile ページ

Add an Access Profile ページには、以下のフィールドが含まれています。

- **Access Profiles Name** — 規則が定義されている Access Profile を指定します。
- **Rule Priority (1-65535)** — 規則優先度を指定します（新しいプロファイルに含むオプションの最初の規則用に）。
- **Management Method** — Access Profile が定義されている管理方法を指定します。可能なフィールド値には、以下のものがあります。
  - **All** — すべての管理方法が Access Profile に割り当てられていることを示します。
  - **Telnet** — すべての Telnet セッションが Access Profile に割り当てられていることを示します。
  - **Telnet** — Secure Telnet セッションが Access Profile に割り当てられていることを示します。
  - **HTTP** — HTTP セッションが Access Profile に割り当てられていることを示します。
  - **Secure HTTP** — Secure HTTP セッションが Access Profile に割り当てられていることを示します。
  - **SNMP** — SNMP セッションが Access Profile に割り当てられていることを示します。
- **Interface** — 規則を適用するインタフェースを指定します。可能なフィールド値には、以下のものがあります。
  - **Port** — インタフェースがポートであり、Access Profile が定義されている特定のポートを示します。
  - **LAG** — インタフェースが LAG であり、Access Profile が定義されている特定の LAG を示します。
  - **VLAN** — インタフェースが VLAN であり、Access Profile が定義されている特定の VLAN を示します。
- **Source IP Address** — パケットが一致するインタフェースの Source IP Address を示します。
- **Network Mask** — パケットが一致するインタフェースネットワークマスクを示します。
- **Prefix Length** — パケットが一致するプレフィックスの長さを示します。
- **Action** — Management Security Rule の動作を定義します。可能なフィールド値には、以下のものがあります。
  - **Permit** — 定義されたインタフェースへの管理アクセスを許可します。
  - **Deny** — 定義されたインタフェースへの管理アクセスを許可しません。

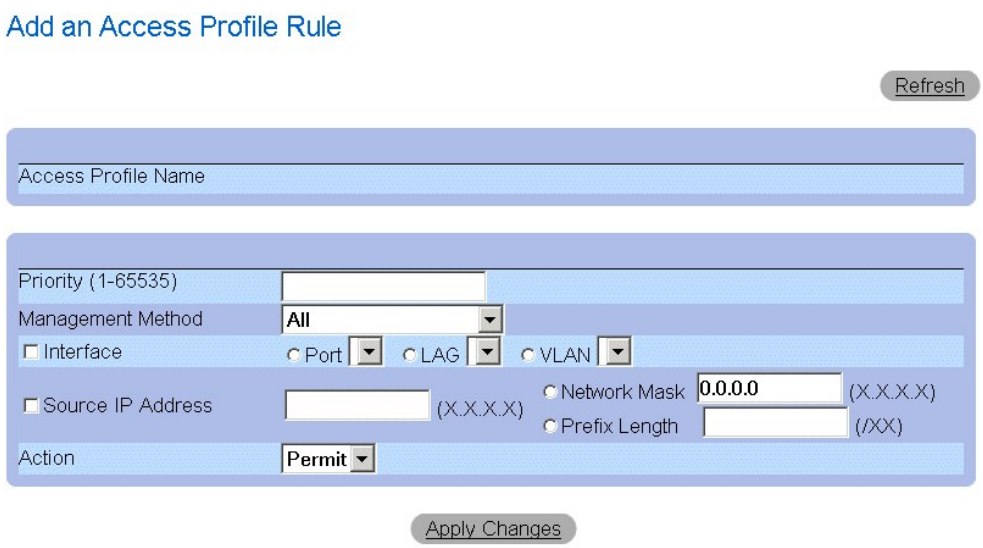
3. **Access Profile Name** フィールドを定義します。
4. **Priority**、**Management Method**、**Interface**、**Source IP Address**、 **Network Mask**、**Prefix Length**、および **Action** フィールドを定義します。

5. **Apply Changes** をクリックします。新しい Access Profile が追加され、デバイスがアップデートされます。

Access Profile へ規則を追加するには、次の手順を実行します。

メモ: アクセスプロファイルへのトラフィックの一致を開始するには、最初の規則を定義する必要があります。

1. **Access Profiles** ページを開きます。
2. **Add Rule to Profile** をクリックします。**Add an Access Profile Rule** ページが開きます。



Add an Access Profile Rule ページ

Add an Access Profile Rule ページには、以下のフィールドが含まれています。

- **Access Profile Name** — Access Profile の名前を示します。
- **Rule Priority (1-65535)** — 規則の優先度を示します。
- **Management Method** — Access Profile が定義されている管理方法を指定します。可能なフィールド値には、以下のものがあります。
  - **All** — すべての管理方法が Access Profile に割り当てられていることを示します。この Access Profile を持つユーザーは、すべての管理方法を使用しているデバイスにアクセスできます。
  - **Telnet** — すべての Telnet セッションが Access Profile に割り当てられていることを示します。この Access Profile を持つユーザーは、Telnet 管理方法を使用してデバイスにアクセスできます。
  - **Telnet** — Secure Telnet セッションが Access Profile に割り当てられていることを示します。この Access Profile を持つユーザーは、Secure Telnet 管理方法を使用してデバイスにアクセスできます。
  - **HTTP** — HTTP セッションが Access Profile に割り当てられていることを示します。この Access Profile を持つユーザーは、HTTP 管理方法を使用してデバイスにアクセスできます。
  - **Secure HTTP** — Secure HTTP セッションが Access Profile に割り当てられていることを示します。この Access Profile を持つユーザーは、Secure HTTP 管理方法を使用してデバイスにアクセスできます。
  - **SNMP** — SNMP セッションが Access Profile に割り当てられていることを示します。この Access Profile を持つユーザーは、SNMP 管理方法を使用してデバイスにアクセスできます。
- **Interface** — 規則を適用するインタフェースを指定します。可能なフィールド値には、以下のものがあります。
  - **Port** — インタフェースがポートであり、Access Profile が定義されている特定のポートを示します。

- **LAG** — インタフェースが LAG であり、Access Profile が定義されている特定の LAG を示します。
- **VLAN** — インタフェースが VLAN であり、Access Profile が定義されている特定の VLAN を示します。

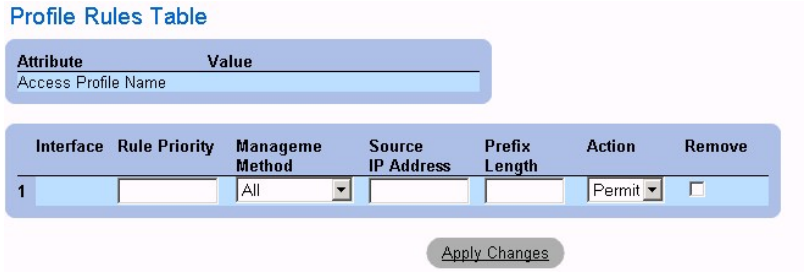
- **Source IP Address** — パケットが一致するインタフェースの Source IP Address を示します。
- **Network Mask** — パケットが一致するインタフェースネットワークマスク を示します。
- **Prefix Length** — パケットが一致するプレフィックスの長さを示します。
- **Action** — Management Security Rule の動作を定義します。可能なフィールド値には、以下のものがあります。
  - **Permit** — 定義されたインタフェースへの管理アクセスを許可します。
  - **Deny** — 定義されたインタフェースへの管理アクセスを許可しません。

3. **Access Profile Name** フィールドを定義します。
4. **Priority**、**Management Method**、**Interface**、**Source IP Address**、 **Network Mask**、**Prefix Length**、および **Action** フィールド を定義します。
5. **Apply Changes** をクリックします。規則が追加され、デバイスがアップデートされます。

Profile Rules Table を表示するには、次の手順を実行します。

メモ: **Profile Rules Table** に表示される規則の順序は重要です。パケットは、条件を満たす最初の規則に一致します。

1. **Access Profiles** ページを開きます。
2. **Show All** をクリックします。**Profile Rules Table** ページが開きます。



Profile Rules Table ページ

3. **Apply Changes** をクリックします。

規則を削除するには、次の手順を実行します。

メモ: 規則を削除すると、プロファイル名も削除されます。

1. **Access Profiles** ページを開きます。
2. **Show All** をクリックします。**Profile Rules Table** が開きます。
3. **Profile Rules Table** ページで規則を選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。規則が削除され、デバイスがアップデートされます。

CLI コマンドを使用したアクセスプロファイルの定義

次の表に、**Access Profiles** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
management access-list *name*	管理用のアクセスリストを定義し、設定用のアクセスリストコンテキストを起動します。
permit [ethernet *interface-number* **| vlan** *vlan-id* **| port-channel** *number***] [service** *service***]**	管理アクセスリストのポートの許可条件を設定します。
permit ip-source *ip-address* **[mask** *mask* **|** *prefix-length***] [ethernet** *interface-number* **| vlan** *vlan-id* **| port-channel** *number***] [service** *service***]**	管理アクセスリストのポートの許可条件と、選択した管理方法を設定します。
deny [ethernet *interface-number* **| vlan** *vlan-id* **| port-channel** *number***] [service** *service***]**	管理アクセスリストのポートの不許可条件と、選択した管理方法を設定します。
deny ip-source *ip-address* **[mask** *mask* **|** *prefix-length***] [ethernet** *interface-number* **| vlan** *vlan-id* **| port-channel** *number***] [service** *service***]**	管理アクセスリストのポートの不許可条件と、選択した管理方法を設定します。
management access-class {console-only | *name***}**	どのアクセスリストがアクティブな管理接続として使用されているかを定義します。
show management access-list [*name***]**	アクティブな管理アクセスリストを表示します。
show management access-class	管理アクセスクラスについての情報を表示します。

以下に、CLI コマンドの例を示します。

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

Console (config-macl)# permit ethernet 1/e1

Console (config-macl)# permit ethernet 2/e9

Console (config-macl)# deny ethernet 1/e2

Console (config-macl)# deny ethernet 2/e10

Console (config-macl)# exit

Console (config)# management access-class mlist

Console (config)# exit

Console# show management access-list

mlist

-----
```

```
permit ethernet 1/e1

permit ethernet 2/e9

! (Note:all other access implicitly denied)

Console> show management access-class

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

認証プロファイルの定義

Authentication Profiles ページを使用して、ネットワーク管理者はデバイスのユーザー認証方法を選ぶことができます。ユーザー認証は、以下の場合に必要です。

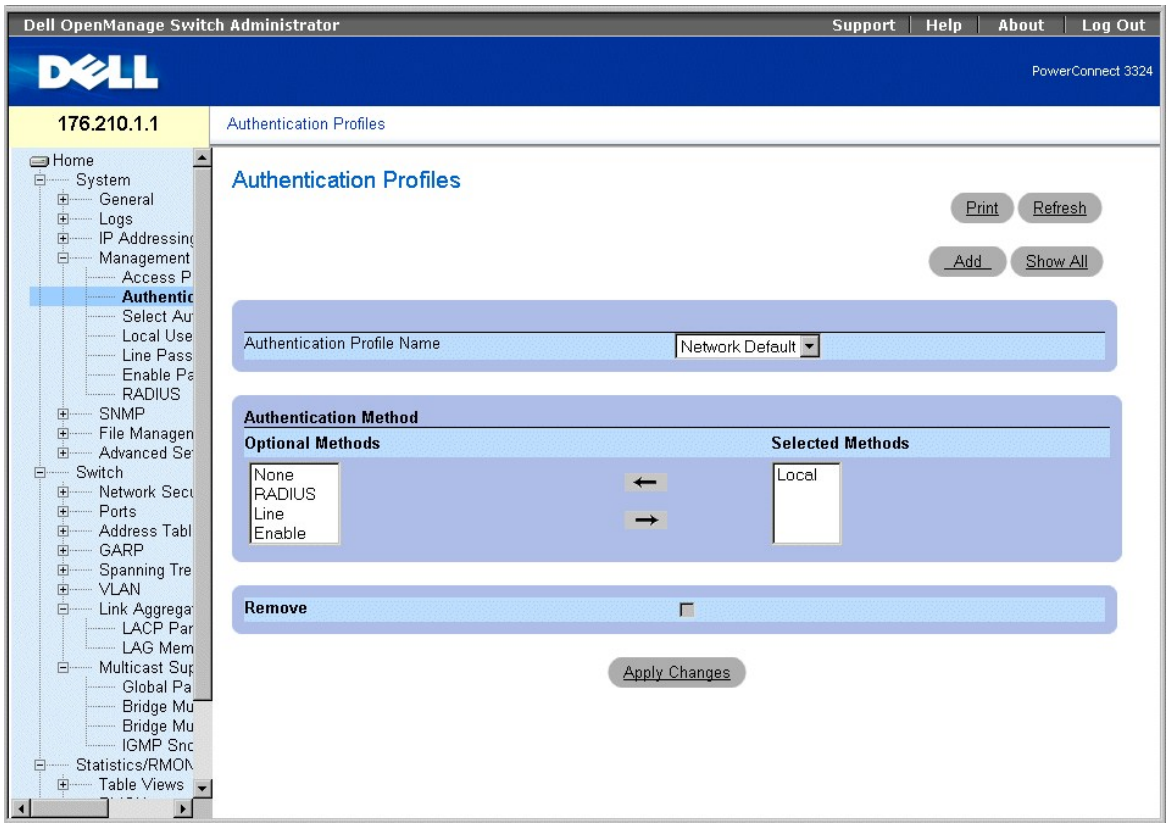
- ローカルで
- 外部サーバーを経由する場合

ユーザー認証は、**None** にも設定できます。

ユーザー認証は、方法が選択された順序で起こります。たとえば、**Local** オプションと **RADIUS** オプションの両方が選択されている場合、ユーザーの認証はローカルで先におこなわれます。ローカルユーザーデータベースが空の場合、ユーザーは次に RADIUS サーバーで認証されます。

認証中にエラーが発生した場合、次に選択されている方法が使われます。**Authentication Profiles** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Management Security** → **Authentication Profiles** とクリックします。**Authentication Profiles** ページが開きます。



Authentication Profiles ページ

Authentication Profiles ページには、以下のオプションリストが含まれています。

- **Authentication Profile Name** — ユーザー定義の認証方法リストが表示され、以下の値が含まれています。
  - **Network Default**
  - **Console Default**
- **Optional Methods** — ユーザー認証方法のリストを表示します。可能なオプションには、以下のものがあります。
  - **Local** — ローカルで認証がおこなわれることを示します。デバイスは、ユーザー名とパスワードを確認して認証をおこないます。
  - **None** — ユーザー認証はおこなわれないことを示します。
  - **RADIUS** — RADIUS サーバーでユーザー認証がおこなわれることを示します。
  - **Line** — ラインパスワードを使用して認証がおこなわれることを示します。
  - **Enable** — 認証に有効化パスワードが使用されることを示します。
- **Selected Methods** — 選択された認証方法とその順序を示します。
- **Remove** — **Authentication Profile Names** リストから選択した Authentication Profile を削除します。
  - **Checked** — Authentication Profile を削除します。
  - **Unchecked** — Authentication Profile を保持します。

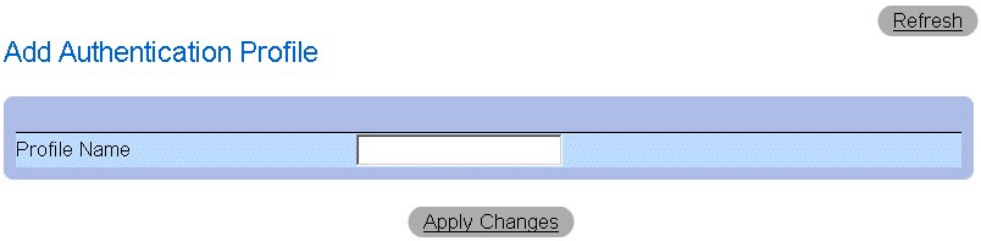
Authentication Profile を選択するには、次の手順を実行します。

1. **Authentication Profiles** ページを開きます。
2. **Authentication Profile Name** フィールドで、プロファイルを選びます。

3. 矢印アイコンを使用して認証方法を選びます。
4. **Apply Changes** をクリックします。ユーザー認証プロファイルがデバイスに対してアップデートされます。

Authentication Profile を追加するには、次の手順を実行します。

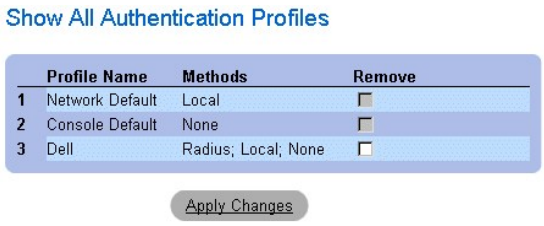
1. **Authentication Profiles** ページを開きます。
2. **Add** （追加）をクリックします。**Add Authentication Profile** ページが開きます。



Add Authentication Profile ページ

Show All Authentication Profiles ページを表示するには、次の手順を実行します。

1. **Authentication Profiles** ページを開きます。
2. **Show All** をクリックします。**Show All Authentication Profiles** ページが開きます。



Show All Authentication Profiles ページ

Authentication Profile を削除するには、次の手順を実行します。

1. **Authentication Profiles** ページを開きます。
2. **Show All** をクリックします。**Show All Authentication Profiles** ページが開きます。
3. Authentication Profile を選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。Authentication Profile が削除されます。

CLI コマンドを使用した認証プロファイルの設定

次の表に、**Authentication Profiles** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
aaa authentication login {default | *list-name***}** *method1* **[***method2.***]**	ログイン認証を設定します。
no aaa authentication login {default | *list-name*	ログイン認証プロファイルを削除します。

以下に、CLI コマンドの例を示します。

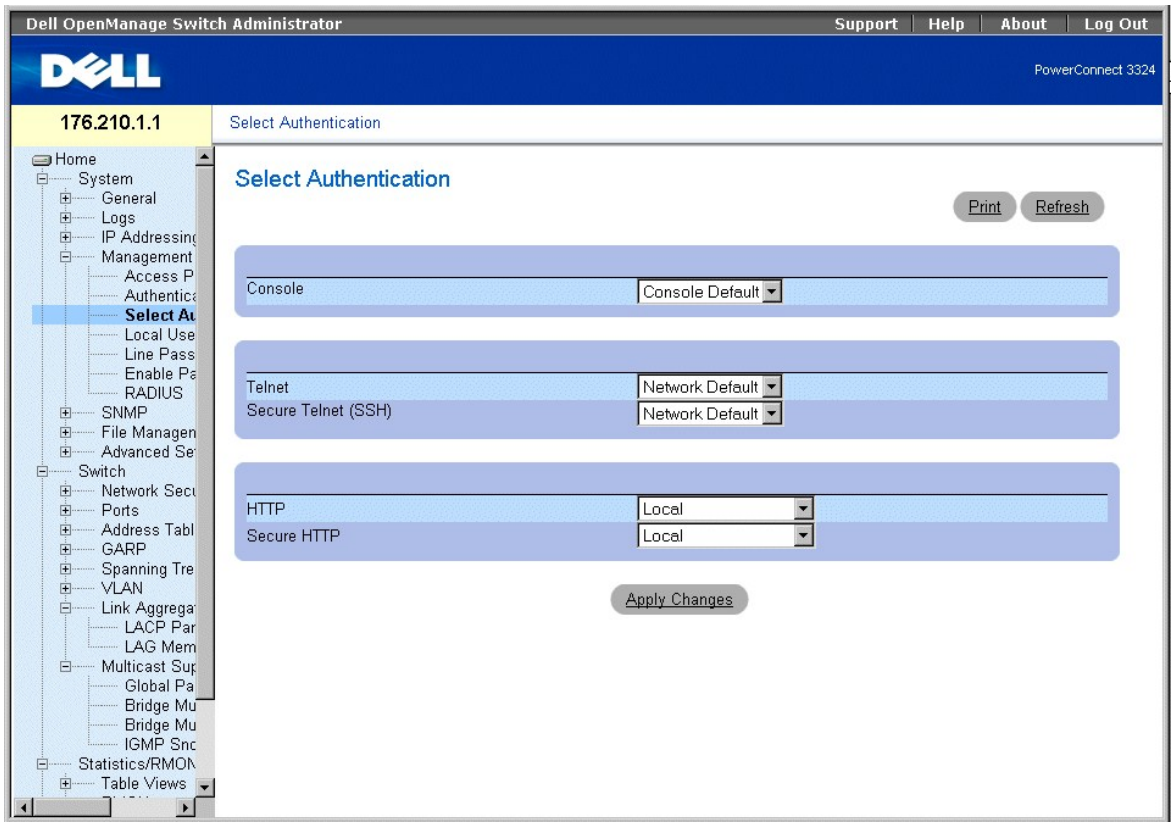
```
Console (config)# aaa authentication login default radius local enable none
```

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

認証プロファイルの割り当て

Authentication Profile を定義した後、Authentication Profile を Management Access 方法に適用できます。たとえば、Telnet ユーザーが Authentication Method List 2 で認証されている間に、コンソールユーザーを Authentication Method List 1 で認証することができます。 **Select Authentication** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Management Security** → **Select Authentication** とクリックします。**Select Authentication** ページが開きます。



Select Authentication ページ

Select Authentication ページには、以下のフィールドが含まれています。

- **Console** — コンソールユーザーの認証に使用する Authentication Profile を表示します。Authentication Profile は、「認証プロファイルの割り当て」 で割り当てられます。他の Authentication Profile を追加できる既定のフィールド値が 2 つあります。ただし、既定の値は削除できません。可能な既定値には、以下のものがあります。
  - **Network Default**
  - **Console Default**
- **Telnet** — Telnet ユーザーの認証に使用する Authentication Profile を表示します。Authentication Profile は、「認証プロファイルの割り当て」で割り当てられます。他の Authentication Profile を追加できる既定のフィールド値が 2 つあります。ただし、既定の値は削除できません。可能な既定値には、以下のものがあります。
  - **Network Default**
  - **Console Default**
- **Secure Telnet (SSH)** — SSH ユーザーの認証に使用する Authentication Profile を表示します。SSH (Secure Shell) は、デバイスへの安全なリモート接続を提供します。SSH を使用して、SSH クライアントは、デバイスとの暗号化された安全な接続を確立できます。Authentication Method リストは、「認証プロファイルの割り当て」で割り当てられます。
- **HTTP** — HTTP アクセスに使用される認証方法を表示します。可能なフィールド値には、以下のものがあります。
  - **None** — HTTP アクセスに Authentication Profile が使用されないことを示します。
  - **Local** — HTTP 認証がローカルでおこなわれることを示します。
  - **Radius** — HTTP 認証が RADIUS サーバーでおこなわれ、HTTP アクセスが許可されていることを示します。
  - **Local, None** — HTTP 認証がまずローカルでおこなわれることを示します。Authentication Method が使用されていない場合、ローカルユーザーデータベースは空で、HTTP アクセスは許可されます。
  - **Radius, None** — HTTP 認証がまず RADIUS サーバーでおこなわれることを示します。Authentication Method が使用されていない場合、RADIUS サーバーにはアクセスできません。
  - **Local, None** — HTTP 認証がまずローカルでおこなわれることを示します。RADIUS サーバーがユーザーを認証した場合、ローカルユーザーデータベースは空です。RADIUS サーバーが管理方法を認証できない場合、HTTP セッションはブロックされます。
  - **Radius, Local** — HTTP 認証がまず RADIUS サーバーでおこなわれることを示します。RADIUS サーバーにアクセスできない場合、HTTP セッションはローカルで認証されます。HTTP セッションをローカルで認証できない場合、HTTP セッションはブロックされます。
  - **Local, None** — HTTP 認証がまずローカルでおこなわれることを示します。
    ローカルデータベースが空の場合、RADIUS サーバーが管理方法を認証します。RADIUS サーバーにアクセスできない場合、HTTP セッションは許可されます。
  - **Radius, None** — HTTP 認証がまず RADIUS サーバーでおこなわれることを示します。RADIUS サーバーにアクセスできない場合、HTTP セッションはローカルで認証されます。ローカルデータベースが空の場合、HTTP セッションは許可されます。
- **Secure HTTP** — Secure HTTP アクセスに使用される Authentication Profile を指定します。可能なフィールド値には、以下のものがあります。
  - **None** — HTTP アクセスに Authentication Profile が使用されないことを示します。
  - **Local** — HTTP 認証がローカルでおこなわれることを示します。
  - **Radius** — Secure HTTP 認証が RADIUS サーバーでおこなわれることを示します。
  - **Local, None** — HTTP 認証がまずローカルでおこなわれることを示します。ローカルユーザーデータベースが空の場合、Authentication Method は使用されず、Secure HTTP アクセスは許可されます。
  - **Radius, None** — HTTP 認証がまず RADIUS サーバーでおこなわれることを示します。RADIUS サーバーにアクセスできない場合、Authentication Method は使用されず、Secure HTTP アクセスは許可されます。
  - **Local, None** — HTTP 認証がまずローカルでおこなわれることを示します。
    ローカルデータベースが空の場合、RADIUS サーバーがユーザーを認証します。RADIUS サーバーが管理方法を認証できない場合、Secure HTTP セッションはブロックされます。
  - **Radius, Local** — HTTP 認証がまず RADIUS サーバーでおこなわれることを示します。RADIUS サーバーにアクセスできない場合、Secure HTTP セッションはローカルで認証されます。Secure HTTP セッションをローカルで認証できない場合、Secure HTTP セッションはブロックされます。
  - **Local, None** — HTTP 認証がまずローカルでおこなわれることを示します。
    ローカルデータベースが空の場合、RADIUS サーバーが管理方法を認証します。RADIUS サーバーがデータベースにアクセスできない場合、Secure HTTP セッションは許可されます。
  - **Radius, None** — HTTP 認証がまず RADIUS サーバーでおこなわれることを示します。RADIUS サーバーにアクセスできない場合、Secure HTTP セッションはローカルで認証されます。ローカルデータベースが空の場合、Secure HTTP セッションは許可されます。

Authentication List をコンソールセッションに適用するには、次の手順を実行します。

1. **Select Authentication** ページを開きます。
2. **Console** フィールドで、Authentication Profile を選びます。
3. **Apply Changes** をクリックします。コンソールセッションが Authentication List に割り当てられます。

Authentication Profile を Telnet セッションに適用するには、次の手順を実行します。

1. **Select Authentication** ページを開きます。
2. **Telnet** フィールドで、Authentication Profile を選びます。
3. **Apply Changes** をクリックします。Telnet セッションが Authentication List に割り当てられます。

Authentication Profile を Secure Telnet (SSH) セッションに適用するには、次の手順を実行します。

1. **Select Authentication** ページを開きます。
2. **Secure Telnet (SSH)** フィールドで、Authentication Profile を選びます。
3. **Apply Changes** をクリックします。SSH (Secure Telnet) セッションが Authentication Profile に割り当てられます。

Authentication Sequence を HTTP セッションに割り当てるには、次の手順を実行します。

1. **Select Authentication** ページを開きます。
2. **HTTP** フィールドで、Authentication Sequence を選びます。
3. **Apply Changes** をクリックします。HTTP セッションが Authentication Sequence に割り当てられます。

Authentication Sequence を Secure HTTP セッションに割り当てるには、次の手順を実行します。

1. **Select Authentication** ページを開きます。
2. **Secure HTTP** フィールドにある Authentication Sequence を選びます。
3. **Apply Changes** をクリックします。Secure HTTP セッションが Authentication Sequence に割り当てられます。

CLI コマンドを使用したアクセス認証プロファイルまたは順序の割り当て

次の表に、**Select Authentication** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
enable authentication [default | *list-name*]	リモート Telnet またはコンソールからより高い権限レベルにアクセスする際の Authentication Method のリストを指定します。
login authentication [default | *list-name*]	リモート Telnet またはコンソール用のログイン Authentication Method のリストを指定します。
ip http authentication *method1* [*method2.*]	http サーバー用の Authentication Method を指定します。
ip https authentication *method1* [*method2.*]	https サーバー用の Authentication Method を指定します。
show authentication methods	Authentication Method についての情報を表示します。

以下に、CLI コマンドの例を示します。

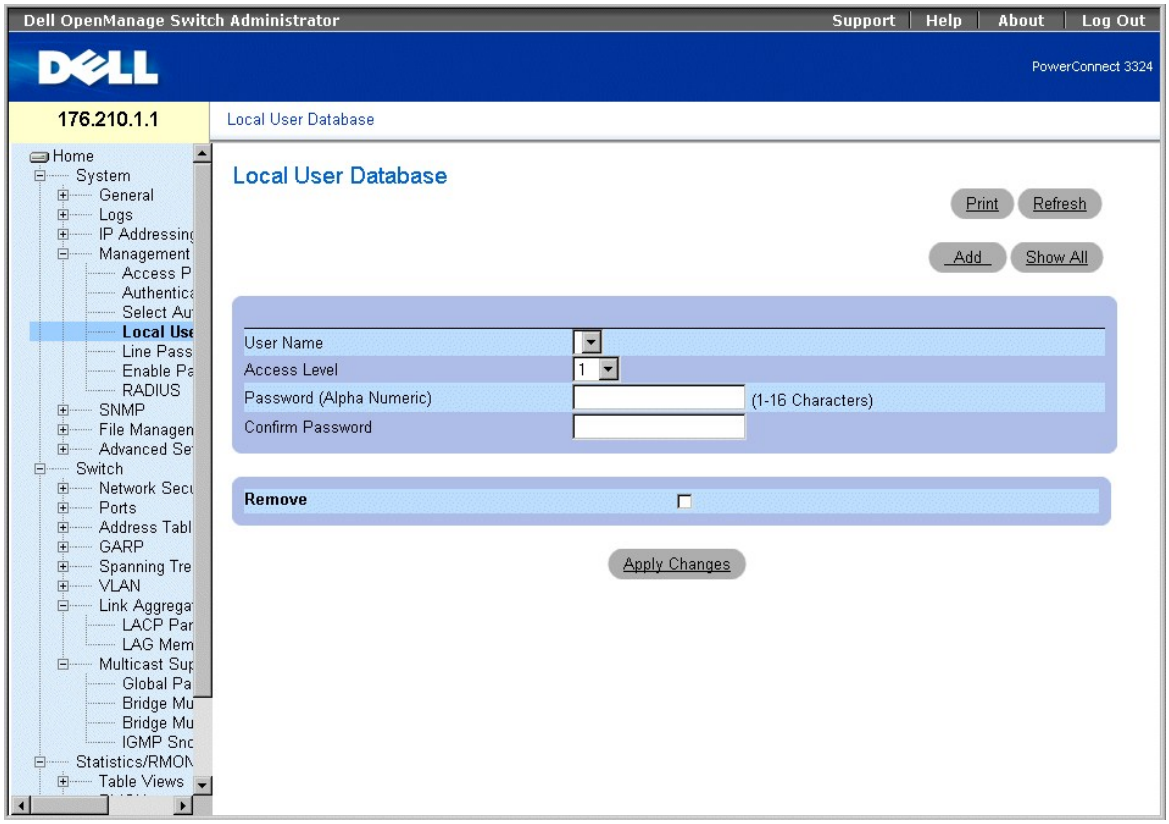
```
Console (config-line)# enable authentication default

Console (config-line)# login authentication default

Console (config-line)# exit

Console (config)# ip http authentication radius local

Console (config)# ip https authentication radius local

Console (config)# exit

Console# show authentication methods


Login Authentication Method Lists

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

Default:Radius, Local, Line

Console_Login:Line, None


Enable Authentication Method Lists

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

Default:Radius, Enable

console> enable:Enable, None


Line Login Method List Enable Method List
```

```
------- ---------------- ------------------

Console Console_Login Console_Enable

Telnet Default Default

SSH Default Default



HTTP:Radius, local

HTTPS:Radius, local
```

ローカルユーザーデータベースの定義

Local User Database ページを使用して、ネットワーク管理者はユーザー、パスワード、およびアクセスレベルを定義することができます。パスワードは、最大 16 文字までに制限されています。**Local User Database** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Management Security** → **Local User Database** とクリックします。**Local User Database** ページが開きます。



Local User Database ページ

Local User Database ページには、以下のフィールドが含まれています。

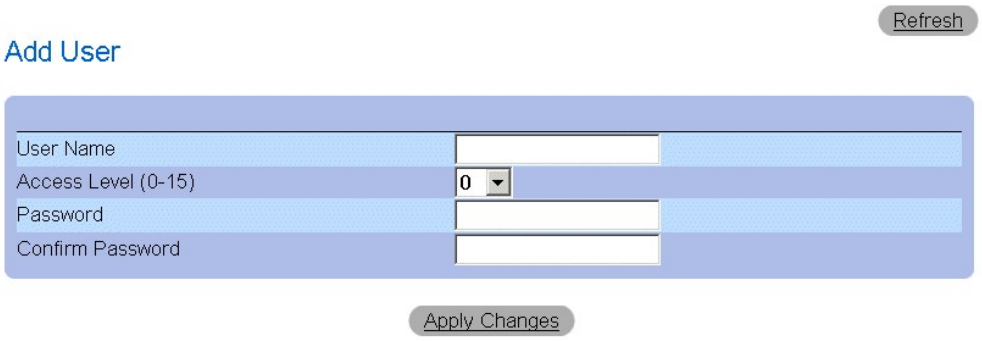
- **User Name** — ユーザーのリストが含まれています。
- **Access Level** — ユーザーのアクセスレベルを決定します。可能な値は以下のとおりです。
  - **1-15**— ユーザーのアクセスレベルを示します。**1** 1 は、最低のユーザーアクセスレベルを示します。
- **Password (Alpha Numeric)** — ユーザーパスワードを指定します。パスワードは ******* として表示されます。
- **Confirm Password** — ユーザー定義のパスワードを確認します。確認されたパスワードは ******* として表示されます。
- **Remove** — **User Name** リストからユーザーを削除します。
  - **Checked** — **Local User Database** から特定のユーザーを削除します。
  - **Unchecked** — **Local User Database** で、ユーザーを保持します。

アクセス権をユーザーに割り当てるには、次の手順を実行します。

1. **Local User Database** ページを開きます。
2. **User Name** フィールドで、ユーザーを選びます。
3. **Access Level** および **Password** フィールドを定義します。
4. **Apply Changes** をクリックします。ユーザーアクセス権とパスワードが定義され、デバイスがアップデートされます。

新しいユーザーを定義するには、次の手順を実行します。

1. **Local User Database** ページを開きます。
2. **Add** （追加）をクリックします。**Add User** ページが開きます。

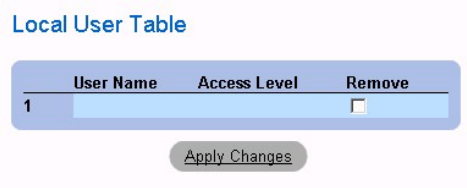


Add User ページ

3. **User Name**、**Access Level (0-15)**、**Password**、および **Confirm Password** フィールドで新しいユーザーを定義します。
4. **Apply Changes** をクリックします。新しいユーザーが定義され、デバイスがアップデートされます。

Local User Table を表示するには、次の手順を実行します。

1. **Local User Database** ページを開きます。
2. **Show All** をクリックします。**Local User Table** ページが開きます。



Local User Table ページ

ユーザーを削除するには、次の手順を実行します。

1. **Local User Database** ページを開きます。
2. **Show All** をクリックします。**Local User Table** ページが開きます。
3. **User Name** を選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。ユーザーが削除され、デバイスがアップデートされます。

CLI コマンドを使用したユーザーの割り当て

次の表に、**Local User Database** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
username *name* **[password** *password***] [privilege** *level***] [encrypted]**	ユーザー名ベースの認証システムを確立します。

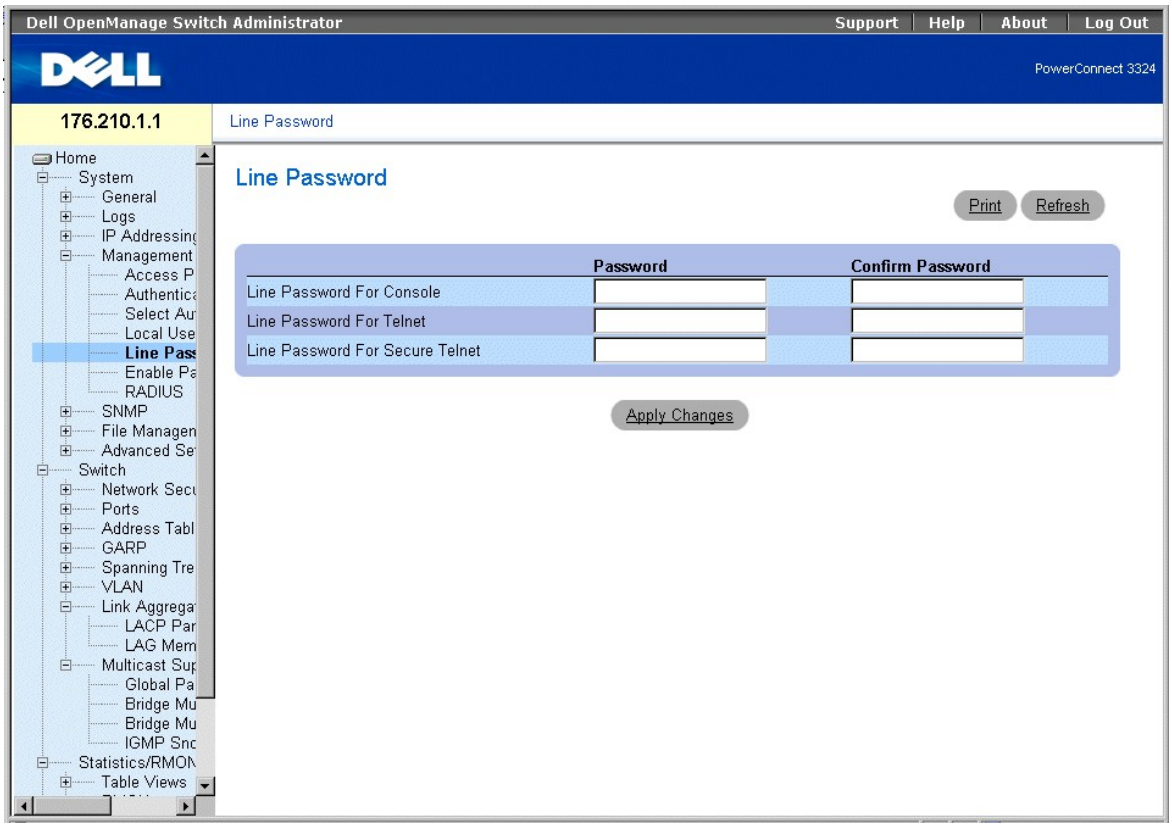
以下に、CLI コマンドの例を示します。

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

ラインパスワードの定義

Line Password ページを使用して、ネットワーク管理者は管理方法のラインパスワードを定義できます。パスワードは最大 16 文字までに制限されています。**Line Password** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Management Security** → **Line Passwords** とクリックします。**Line Password** ページが開きます。



Line Password ページ

Line Password ページには、以下のフィールドが含まれています。

- **Line Password For Console** — コンソールセッションを介してデバイスにアクセスするための Line Password を指定します。パスワードは ******* として表示されます。
- **Line Password For Telnet** — Telnet セッションを介してデバイスにアクセスするための Line Password を指定します。パスワードは ******* として表示されます。
- **Line Password For Secure Telnet** — Secure Telnet セッションを介してデバイスにアクセスするための Line Password を指定します。パスワードは ******* として表示されます。

コンソールセッションの Line Password を定義するには、次の手順を実行します。

1. **Line Password** ページを開きます。
2. **Line Password for Console** フィールドを定義します。
3. **Apply Changes** をクリックします。コンソールセッションの Line Password が定義され、デバイスがアップデートされます。

Telnet セッションの Line Password を定義するには、次の手順を実行します。

1. **Line Password** ページを開きます。
2. **Line Password for Telnet** フィールドを定義します。
3. **Apply Changes** をクリックします。Telnet セッションの Line Password が定義され、デバイスがアップデートされます。

Secure Telnet セッションの Line Password を定義するには、次の手順を実行します。

1. **Line Password** ページを開きます。
2. **Line Password for Secure Telnet** フィールドを定義します。
3. **Apply Changes** をクリックします。Secure Telnet セッションの Line Password が定義され、デバイスがアップデートされます。

CLI コマンドを使用したラインパスワードの割り当て

次の表に、**Line Password** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
password *password* **[encrypted]**	ライン上のパスワードを指定します。

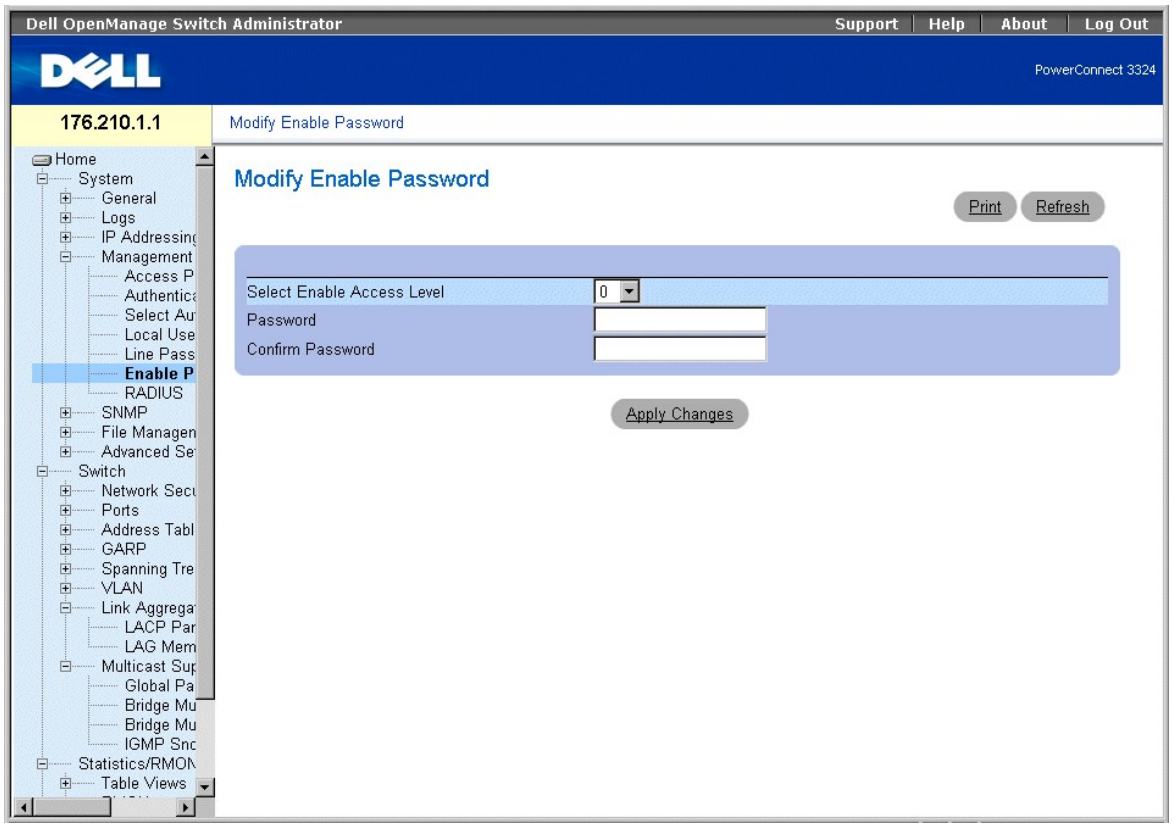
以下に、CLI コマンドの例を示します。

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

有効化パスワードの定義

Modify Enable Password ページで、Normal、Privilege、Global Configuration へのアクセスを制御するローカルパスワードを設定します。**Modify Enable Password** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Management Security** → **Enable Passwords** とクリックします。**Modify Enable Password** ページが開きます。



Modify Enable Password ページ

Modify Enable Password ページには、以下のフィールドが含まれています。

- **Select Enable Access Level** — Enable パスワードに関連するアクセスレベルを指定します。
- **Password** — Enable パスワードを示します。パスワードは ******* として表示されます。
- **Confirm Password** — 新しい Enable パスワードを確認します。確認されたパスワードは ******* として表示されます。

新しい Enable パスワードを定義するには、次の手順を実行します。

1. **Modify Enable Password** ページを開きます。
2. **Select Enable Access Level**、**Password**、および **Confirm Password** フィールドを定義します。
3. **Apply Changes** をクリックします。新しい Enable パスワードが定義され、デバイスがアップデートされます。

CLI コマンドを使用した有効化パスワードの割り当て

次の表に、**Modify Enable Password** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
enable password [level *level***]** *password* **[encrypted]**	ユーザーおよび特権レベルへのアクセスを制御するローカルパスワードを設定します。
show users accounts	ローカルユーザーデータベースに関する情報を表示します。

以下に、CLI コマンドの例を示します。

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

Console# show users accounts

Username Privilege

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

Bob 15

Robert 15
```

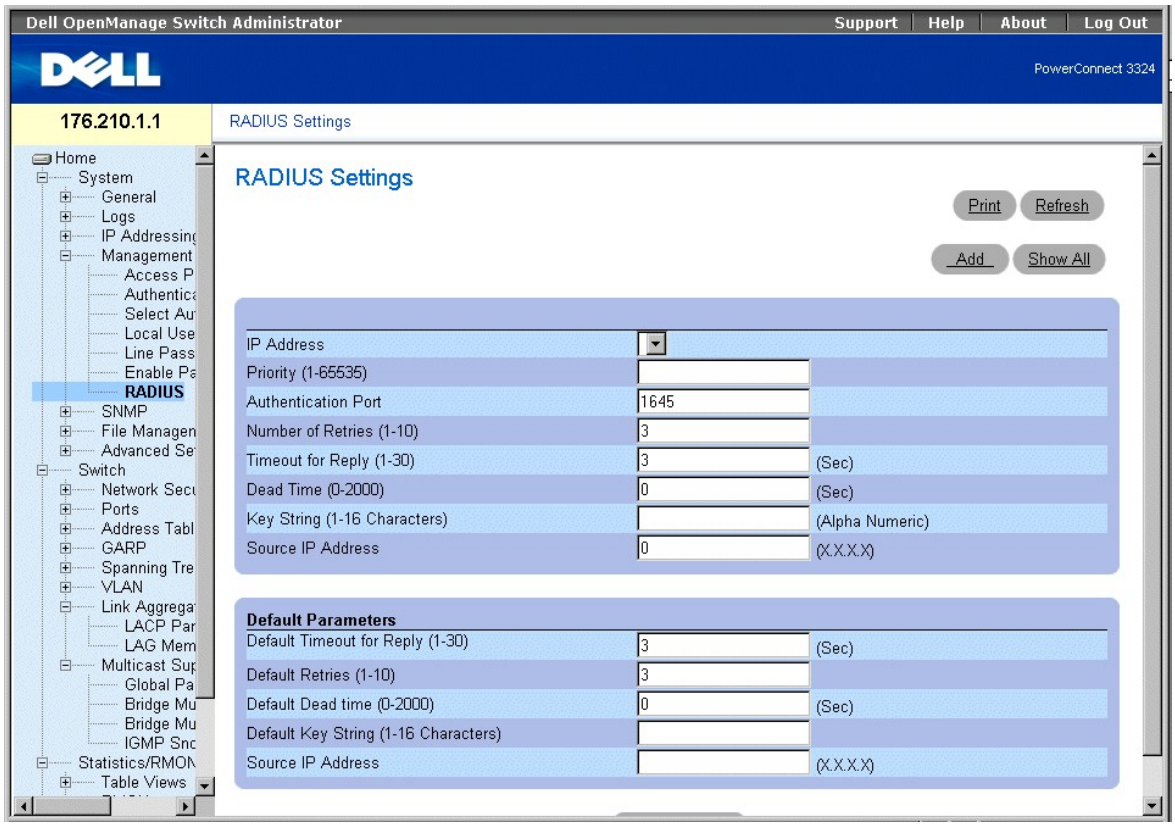
RADIUS グローバルパラメータの設定

RADIUS (Remote Authorization Dial-In User Service) サーバーは、より強化されたセキュリティをネットワークに提供します。RADIUS サーバーは、以下のものに中央化された認証方法を提供します。

- Telnet アクセス
- Web アクセス
- コンソールからスイッチへのアクセス

RADIUS Settings ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Management Security** → **RADIUS** とクリックします。**RADIUS Settings** ページが開きます。



RADIUS Settings ページ

RADIUS Settings ページには、以下のフィールドが含まれています。

- **IP Address** — 認証サーバーの IP アドレスの一覧を示します。
- **Priority (1-65535)** — サーバーの優先度を示します。可能な値は 1 ～ 65535 で、1 が 最高値です。これはサーバーが照会される順序の設定に使用します。
- **Authentication Port** — 認証ポートを示します。認証ポートは、RADIUS サーバー認証を確認するのに使用されます。
- **Number of Retries (1-10)** — 失敗するまでに RADIUS サーバーに送信される要求の数を指定します。可能なフィールド値は 1 ～ 10 で、デフォルト値は 3 です。
- **Timeout for Reply (1-30)** — デバイスが照会の再試行、または次のサーバーに移る前に RADIUS サーバーからの応答を待つ時間を秒で示します。可能なフィールド値は 1 ～ 30 で、デフォルト値は 3 です。
- **Dead Time (0-2000)** — サービスの要求に対して RADIUS サーバーがバイパスされる時間を秒で示します。範囲は、0 ～ 2000 です。
- **Key String (1-16 Characters)** — デバイスと RADIUS サーバー間の RADIUS 通信のすべての認証と暗号化に使用されるキーストリングを示します。このキーは暗号化されます。
- **Source IP Address** — デバイスが RADIUS サーバーへのアクセスに使用する IP アドレスを示します。

以下のフィールドで、RADIUS のデフォルト値を設定します。

- **Default Timeout for Reply (1-30)** — タイムアウトまでに RADIUS サーバーからの返答をデバイスが待つデフォルトの時間を秒で指定します。

メモ: **Host Specific Timeouts**、**Retransmit**、**Dead Time**、および **Deny** 値が指定されていない場合、Global 値が各ホストに適用されます。

- **Default Retries (1-10)** — 失敗するまでに RADIUS サーバーに送信される要求数のデフォルト値を指定します。
- **Default Dead Time (0-2000)** — サービス要求に対して RADIUS サーバーがバイパスされるデフォルトの時間を秒で示します。範囲は、0 ～

2000 です。

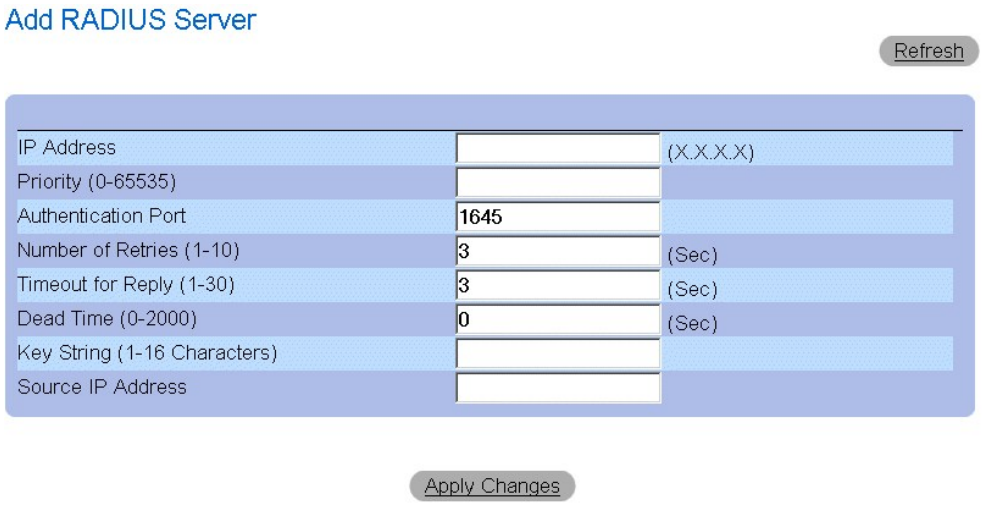
- **Default Key String (1-16 Characters)** — デバイスと RADIUS サーバー間の RADIUS 通信のすべての認証と暗号化に使用されるキーストリングのデフォルトを示します。このキーは暗号化されます。
- **Source IP Address** — デバイスが RADIUS サーバーへのアクセスに使用するデフォルトの IP アドレスを示します。

RADIUS パラメータを定義するには、次の手順を実行します。

1. **RADIUS Settings** ページを開きます。
2. **Default Timeout for Reply**、**Default Retries**、**Default Dead Time**、および **Default Key String** フィールドを定義します。
3. **Apply Changes** をクリックします。デバイスに対して RADIUS 設定がアップデートされます。

RADIUS サーバーを追加するには、次の手順を実行します。

1. **RADIUS Settings** ページを開きます。
2. **Add**（追加）をクリックします。**Add RADIUS Server** ページが開きます。



Add RADIUS Server ページ

3. **IP Address**、**Priority**、**Authentication Port**、**Number of Retries**、 **Timeout for Reply**、**Dead Time**、**Key String**、および **Source IP Address** フィールドを定義します。
4. **Apply Changes** をクリックします。新しい RADIUS サーバーが追加され、デバイスがアップデートされます。

RADIUS Servers List を表示するには、次の手順を実行します。

1. **RADIUS Settings** ページを開きます。
2. **Show All** をクリックします。**RADIUS Servers List** ページが開きます。

RADIUS Servers List ページ

RADIUS サーバー設定を変更するには、次の手順を実行します。

1. **RADIUS Settings** ページを開きます。
2. **Show All** をクリックします。**RADIUS Servers List** ページが開きます。
3. **Priority**、**Number of Retries**、**Timeout for Reply**、および **Dead Time** フィールドを変更します。
4. **Apply Changes** をクリックします。RADIUS サーバー設定が変更され、デバイスがアップデートされます。

RADIUS Servers List から RADIUS サーバーを削除するには、次の手順を実行します。

1. **RADIUS Settings** ページを開きます。
2. **Show All** をクリックします。**RADIUS Servers List** ページが開きます。
3. **RADIUS Servers List** で、RADIUS サーバーを選びます。
4. **Remove** チェックボックスにチェックマークを付けます。**RADIUS Servers List** から RADIUS サーバーが削除されます。

CLI コマンドを使用した RADIUS サーバーの定義

次の表に、**RADIUS Settings** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
radius-server timeout *timeout*	デバイスがサーバーホストの応答を待つデフォルトの間隔を設定します。
radius-server retransmit *retries*	RADIUS サーバーホストのリストをソフトウェアが検索するデフォルトの回数を指定します。
radius-server deadtime *deadtime*	利用できないデフォルトサーバーをスキップするよう設定します。
radius-server key *key-string*	デバイスと RADIUS 間の環境でのすべての RADIUS 通信用のデフォルトの認証および暗号化キーを設定します。
radius-server host *ip-address* **[auth-port** *auth-port-number***] [timeout** *timeout***] [retransmit** *retries***] [deadtime** *deadtime***] [key** *key-string***] [source** *source***] [priority** *priority***]**	RADIUS サーバーホストおよびデフォルト設定ではない設定を指定します。
show radius-servers	RADIUS サーバー設定を表示します。

以下に、CLI コマンドの例を示します。

```
Console (config)# radius-server timeout 5

Console (config)# radius-server retransmit 5

Console (config)# radius-server deadtime 10

Console (config)# radius-server key dell-server

Console (config)# radius-server host 196.210.100.1 auth-port 1645 timeout 20
```

```
Console# show radius-servers

Port

IP address Auth Acct TimeOut Retransmit deadtime Priority

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

172.16.1.1 1645 1646 3 3 0 1

172.16.1.2 1645 1646 11 8 0 2
```

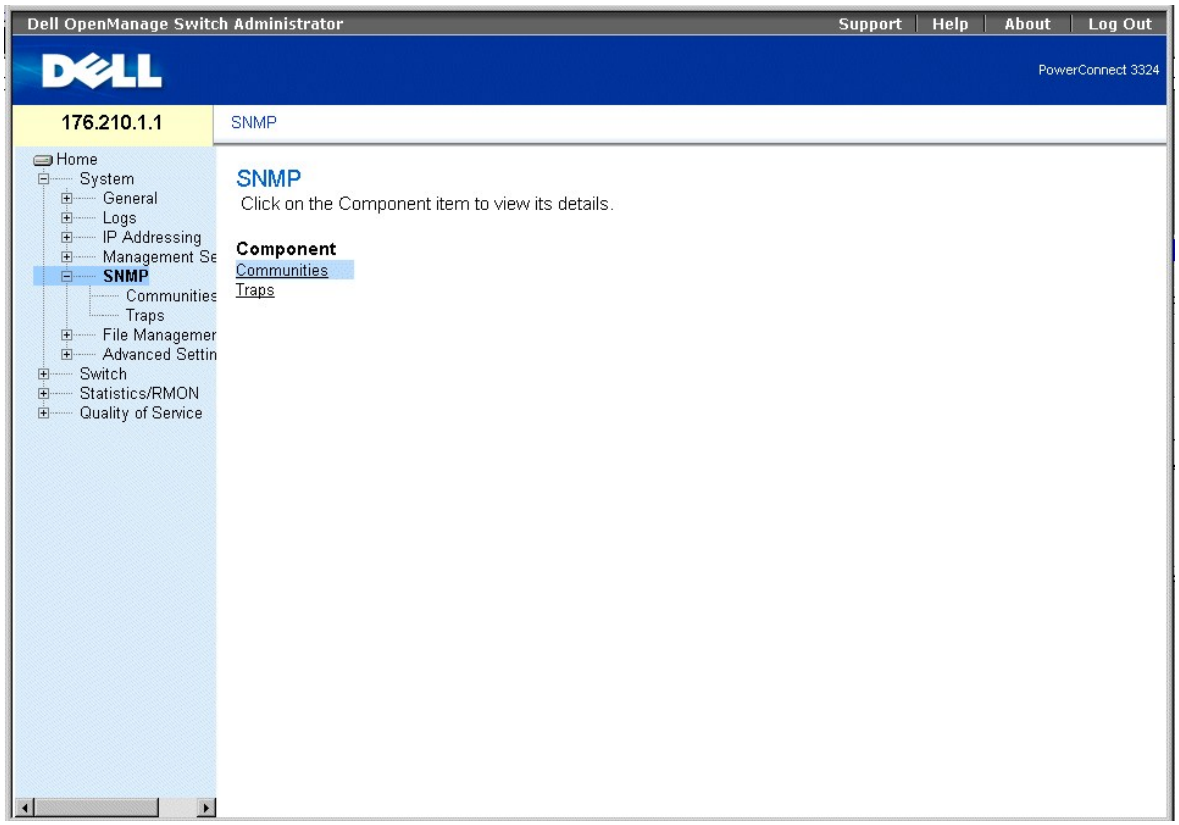
SNMP パラメータの定義

SNMP（Simple Network Management Protocol）はネットワークデバイスの管理メソッドを提供します。SNMP 対応デバイスは、ローカルソフトウェア（エージェント） を実行します。

SNMP エージェントは、デバイスの管理に使用される変数の一覧を保持します。変数は MIB（Management Information Base）で定義されます。MIB はエージェントによって管理される変数を表示します。SNMP プロトコルは、MIB 仕様フォーマットだけでなくネットワーク上で情報にアクセスするのに使用されるフォーマットも定義します。

SNMP エージェントへのアクセス権は、アクセスストリングによって制御されます。デバイスと通信を行うには、内蔵 Web サーバで有効なコミュニティストリングを送信して、認証を受ける必要があります。SNMP ページを開くには、次の手順を実行します。

- Tree View で、**System** → **SNMP** をクリックします。**SNMP** ページが開きます。



SNMP ページ

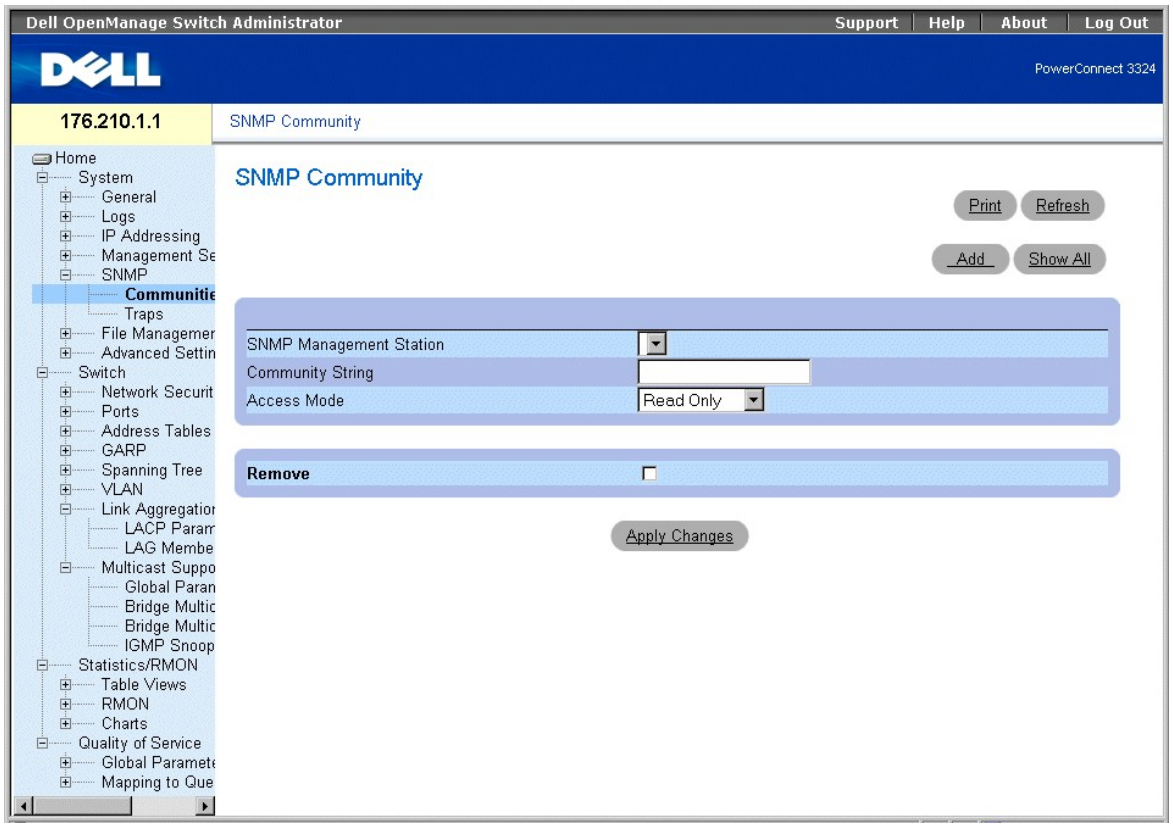
この項には、以下のトピックを含む SNMP 設定の管理についての情報が含まれています。

- コミュニティの定義
- トラップの定義

コミュニティの定義

システム管理者は、Community Table 内のコミュニティを定義して、アクセス権 （読み取りと書き込み、読み取り専用など） を管理します。コミュニティ名を変更した場合、アクセス権も変更されます。**SNMP Community** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **SNMP** → **Communities** をクリックします。
  SNMP Community ページが開きます。



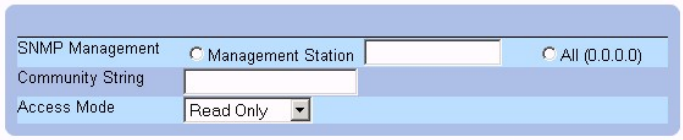
SNMP Community ページ

SNMP Community ページには、以下のフィールドが含まれています。

- **SNMP Management Station** — 管理ステーションの IP アドレスの一覧を示します。
- **Community String** — パスワードとして機能し、選択した管理ステーションのデバイスへの認証に使用します。
- **Access Mode** — コミュニティのアクセス権を定義します。可能なフィールド値には、以下のものがあります。
  - **Read Only** — 管理アクセスは読み取り専用に制限され、コミュニティに変更ができないことを示します。
  - **Read Write** — 管理アクセス権は読み取りおよび書き込みで、デバイス設定の変更は可能ですが、コミュニティへの変更はできないことを示します。
  - **SNMP Admin** — ユーザーはすべてのデバイス設定オプションへのアクセス権とコミュニティ変更のアクセス権を持っていることを示します。
- **Remove** — コミュニティを削除します。可能なフィールド値には、以下のものがあります。
  - **Checked** — コミュニティを削除します。
  - **Unchecked** — コミュニティを保持します。

新しいコミュニティを定義するには、次の手順を実行します。

1. **SNMP Community** ページを開きます。
2. **Add**（追加）をクリックします。**Add SNMP Community** ページが開きます。



Add SNMP Community ページ

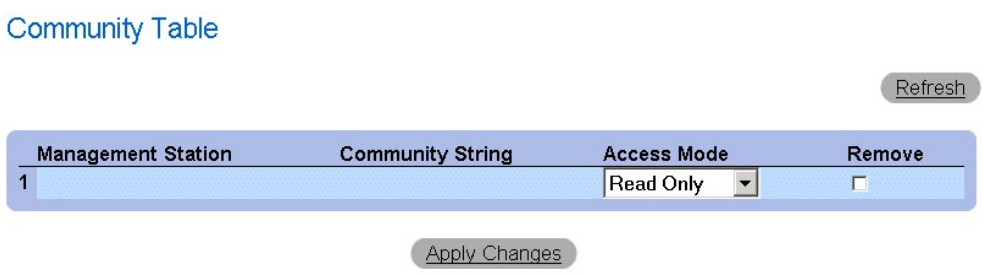
SNMP Community ページのフィールドに加えて、**Add SNMP Community** ページには、以下のフィールドが含まれています。

- **SNMP Management** — 特定の管理ステーション、またはすべての管理ステーションに対して SNMP コミュニティが定義されているかを示します。可能なフィールド値には、以下のものがあります。
  - **Management Station** — 管理ステーションの IP アドレスを示します。0.0.0.0 の値は、すべての管理ステーションを示します。
  - **All** — SNMP コミュニティがすべての管理ステーションに対して定義されていることを示します。

3. **SNMP Management**、**Management Station**、**Community String**、および **Access Mode** フィールドを定義します。
4. **Apply Changes** をクリックします。新しいコミュニティが保存され、デバイスがアップデートされます。

すべてのコミュニティを表示するには、次の手順を実行します。

1. **SNMP Community** ページを開きます。
2. **Show All** をクリックします。**Community Table** ページが開きます。



Community Table ページ

コミュニティを削除するには、次の手順を実行します。

1. **SNMP Community** ページを開きます。
2. **Show All** をクリックします。**Community Table** ページが開きます。
3. **Community Table** からコミュニティを選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。コミュニティエントリが削除され、デバイスがアップデートされます。

CLI コマンドを使用したコミュニティの設定

次の表に、**SNMP Community** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
snmp-server community *string* **[ro | rw | su] [***ip-address***]**	SNMP プロトコルへのアクセスを許可するコミュニティアクセスストリングを設定します。

show snmp	SNMP 通信のステータスをチェックします。

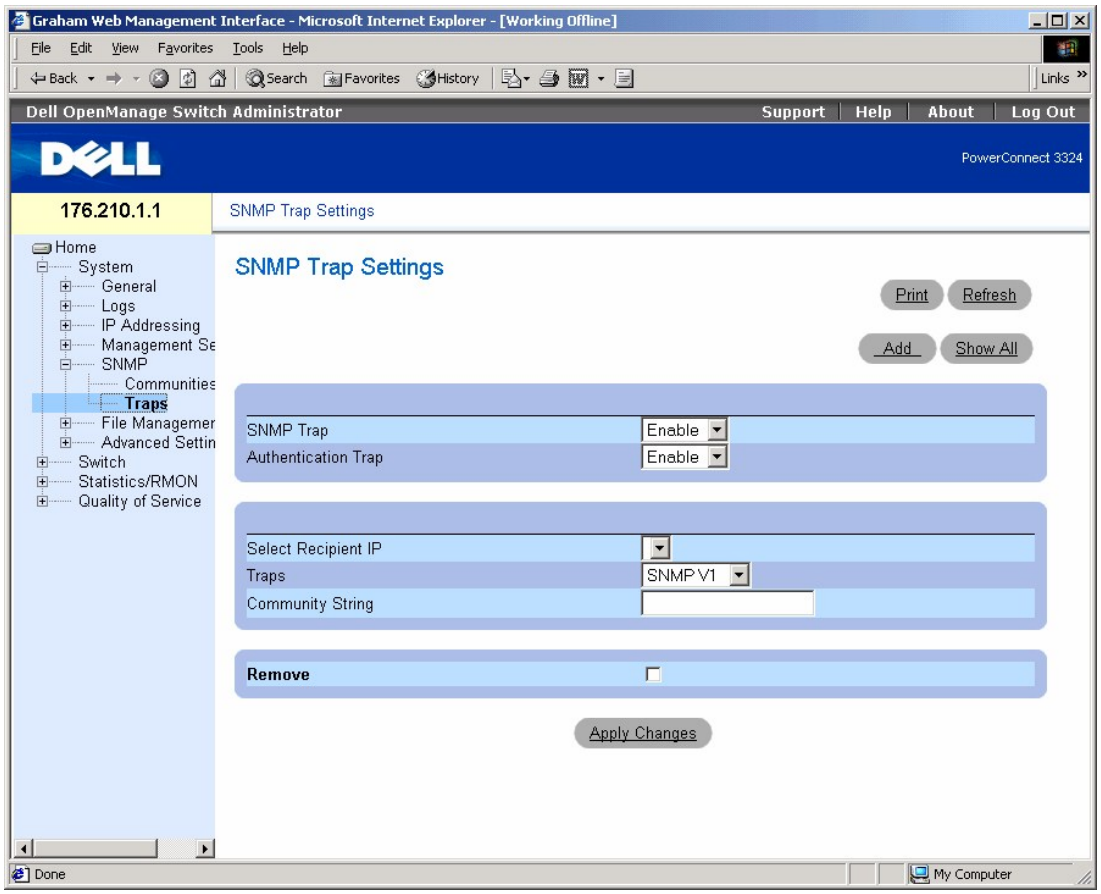
以下に、CLI コマンドの例を示します。

```
Console (config)# snmp-server community public su 0.0.0.0
```

トラップの定義

SNMP Trap Settings ページから、ユーザーはデバイスの SNMP トラップまたは通知の送信を有効または無効にすることができます。**SNMP Trap Settings** ページを開くには、次の手順を実行します。

1. Tree View で、**System** → **SNMP** → **Traps** をクリックします。
   SNMP Trap Settings ページが開きます。



SNMP Trap Settings ページ

SNMP Trap Settings ページには、以下のフィールドが含まれています。

- **SNMP Trap** — 定義済みのトラップ受信者へのスイッチからの SNMP トラップ、または SNMP 通知の送信を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — SNMP トラップまたは SNMP 通知の送信を有効にします。
  - **Disable** — すべての SNMP トラップの送信を停止します。

- **Authentication Trap** — 認証が失敗した際に、定義済みの受信者への SNMP トラップの送信を有効にします。可能なフィールド値には、以下のものがあります。
  - **Enable** — 認証が失敗した際に、SNMP トラップ送信を有効にします。
  - **Disable** — 認証が失敗した際に、SNMP トラップ送信を無効にします。
- **Select Recipient IP** — トラップの送信先の IP アドレスを指定します。
- **Traps** — 選択された受信者に送信されるトラップのタイプを決定します。
  可能なフィールド値には、以下のものがあります。
  - **SNMP V1** — SNMP Version 1 トラップが送信されることを示します。
  - **SNMP V2c** — SNMP Version 2 トラップが送信されることを示します。
  - **Disable** — 受信者へのトラップの送信を無効にします。
- **Community String** — トラップマネージャのコミュニティストリングを示します。
- **Remove** — **Trap Manager Table** エントリを削除します。
  - **Checked** — **Trap Manager Table** エントリを削除します。
  - **Unchecked** — **Trap Manager Table** エントリを保持します。

デバイスで SNMP トラップを有効にするには、次の手順を実行します。

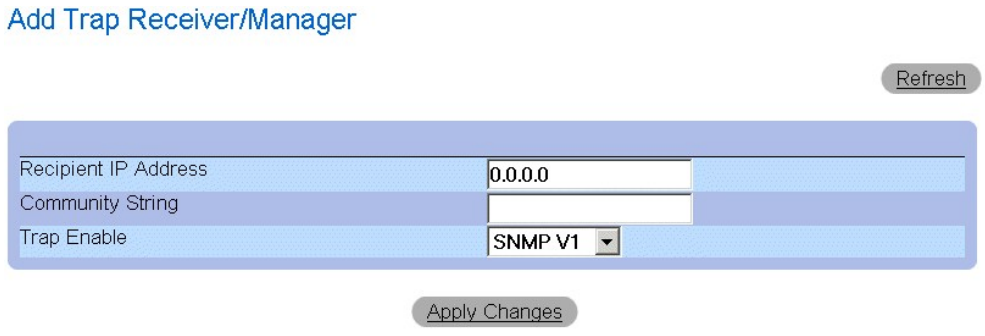
1. **SNMP Trap Settings** ページを開きます。
2. **SNMP Trap** ドロップダウンリストで **Enable** を選びます。
3. **Select Recipient IP**、**Traps**、および **Community String** フィールドを定義します。
4. **Apply Changes** をクリックします。SNMP トラップがデバイスで有効になります。

デバイスで認証トラップを有効にするには、次の手順を実行します。

1. **SNMP Trap Settings** ページを開きます。
2. **Authentication Trap** ドロップダウンリストで **Enable** を選びます。
3. **Select Recipient IP**、**Traps**、および **Community String** フィールドを定義します。
4. **Apply Changes** をクリックします。認証トラップがデバイスで有効になります。

新しいトラップの受信者を追加するには、次の手順を実行します。

1. **SNMP Trap Settings** ページを開きます。
2. **Add**（追加）をクリックします。**Add Trap Receiver / Manager** ページが開きます。



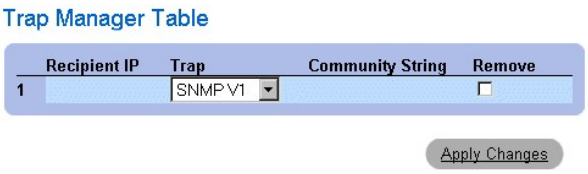
Add Trap Receiver / Manager ページ

3. **Recipient IP Address**、**Community String**、および **Trap Enable** フィールドを定義します。（0.0.0.0 は、「すべて」 を意味し、トラップはブロードキャストされます。
4. **Apply Changes** をクリックします。 Trap Receiver/Manager が追加され、デバイスがアップデートされます。

Trap Manager Table を表示するには、次の手順を実行します。

Trap Manager Table には、トラップタイプを設定するためのフィールドが含まれています。

1. **Traps** ページを開きます。
2. **Show All** をクリックします。**Trap Manager Table** ページが開きます。



Trap Manager Table ページ

Trap Manager Table エントリを削除するには、次の手順を実行します。

1. **SNMP Trap Settings** ページを開きます。
2. **Show All** をクリックします。**Trap Manager Table** ページが開きます。
3. **Trap Manager Table** エントリを選びます。
4. **Remove** チェックボックスにチェックマークを付けます。
5. **Apply Changes** をクリックします。Trap Manager が削除され、デバイスがアップデートされます。

CLI コマンドを使用したトラップの設定

次の表に、**SNMP Trap Settings** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
snmp-server enable traps	スイッチの SNMP トラップ、または SNMP 通知の送信を有効にします。
snmp-server trap authentication	認証が失敗した際に、スイッチの SNMP トラップの送信を有効にします。
snmp-server host host-addr community-string [1 | 2]	選択された受信者に送信されるトラップタイプを決定します。
show snmp	SNMP の通信状態を表示します。

以下に、CLI コマンドの例を示します。

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

```
Console (config)# snmp-server trap authentication

Console (config)# snmp-server host 10.1.1.1 trapRec 2

Console (config)# exit

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


Traps are enabled.

Authentication trap is enabled.


Trap-Rec-Address Trap-Rec-Community Version

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

192.122.173.42 public 2


System Contact:Robert

System Location:Marketing
```

ファイルの管理

File Management ページのデバイスを使用して、ネットワーク管理者はデバイスソフトウェア、Image ファイル、および Configuration ファイルを管理することができます。ファイルは、TFTP サーバーからダウンロードできます。

ファイルの管理の概要

設定ファイルは、以下のファイルで構成されています。

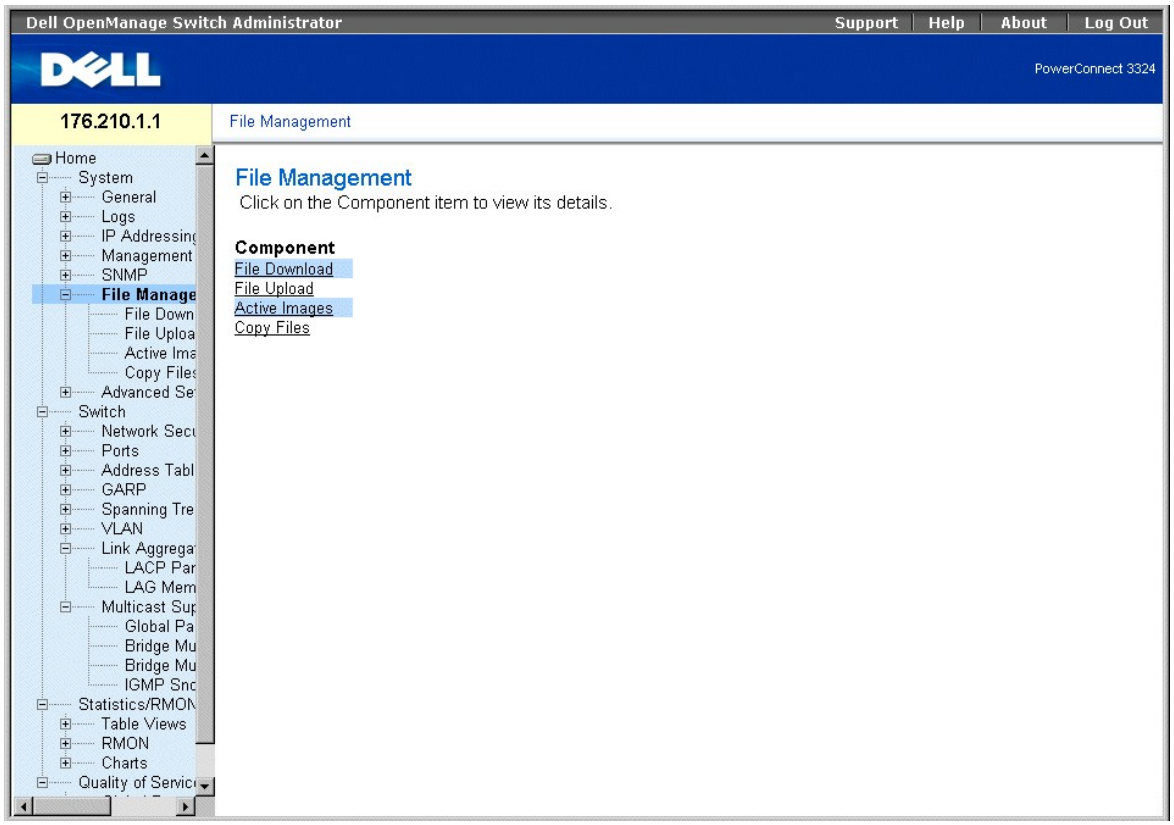
- Startup Configuration ファイル — デバイスの電源が切れたり、再起動された際に、正確なデバイス設定を保持します。Startup ファイルは設定コマンドを保持し、Running Configuration ファイルからの設定コマンドは Startup ファイルに保存することができます。
- Running Configuration ファイル — すべての Startup ファイルコマンド、および現在のセッション中に入力されたコマンドをすべて含みます。デバイスの電源が切れたり、再起動された場合、Running Configuration ファイルに保存されたすべてのコマンドは失われます。スタートアッププロセス中に、Startup ファイル内のすべてのコマンドは Running Configuration ファイルにコピーされ、デバイスに適用されます。セッション中は、新しく入力されたすべてのコマンドは Running Configuration ファイルにあるコマンドに追加されます。コマンドは上書きされません。Startup ファイルを更新するには、デバイスの電源を切る前に、Running Configuration ファイルを Startup Configuration ファイルにコピーする必要があります。次回にデバイスが再起動される際、コマンドは Startup Configuration ファイルから Running Configuration ファイルにコピーされます。

メモ: 設定コマンドは、Running Configuration ファイルに統合され、ただちにデバイスに適用されます。

- Backup Configuration ファイル — デバイス設定のバックアップコピーが含まれています。Running Configuration ファイルまたは Startup ファイルが Backup ファイルにコピーされると、Backup ファイルは変更されます。Backup ファイルにコピーされたコマンドは、保存されている既存のコマンドと置き換えられます。Backup ファイルの内容は、Running Configuration ファイル、または Startup Configuration ファイルのどちらにもコピーできます。
- Image ファイル — システムイメージは、イメージファイルと呼ばれる 2 つのフラッシュファイルに保存されます （Image 1 および Image 2）。アクティブイメージはアクティブコピーを保存し、もう 1 つのイメージは 2 つ目のコピーを保存します。デバイスはアクティブイメージから起動し、動作します。アクティブイメージが壊れている場合、システムは非アクティブイメージから自動的に起動します。これは不具合に対する安全機能で、ソフトウェアのアップグレード処理中におこなわれます。

File Management ページを開くには、次の手順を実行します。

- Tree View で、**System → File Management** とクリックします。**FileManagement** ページが開きます。



File Management ページ

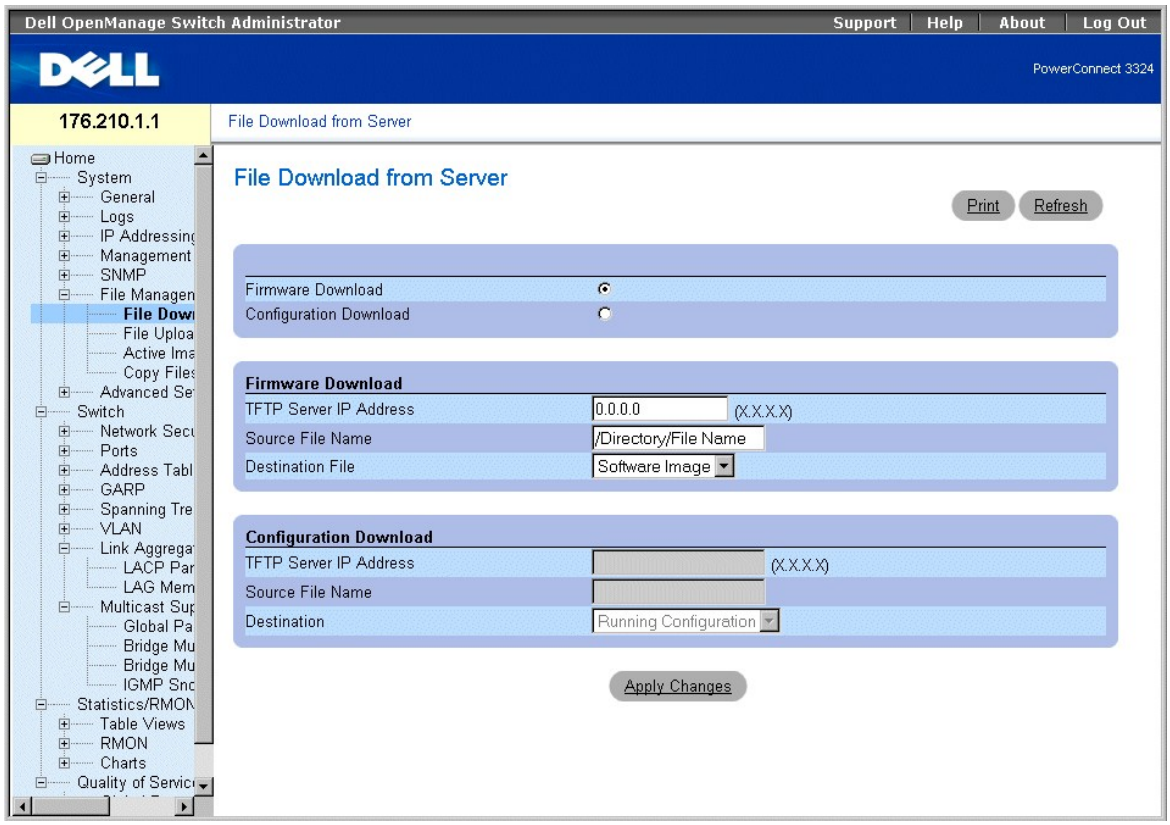
File Management ページには、以下のリンクがあります。

- ファイルのダウンロード
- ファイルのアップロード
- アクティブイメージのリセット
- ファイルのコピーと削除

ファイルのダウンロード

File Download from Server ページには、TFTP サーバーからデバイスへのイメージや Configuration ファイルのダウンロードのためのフィールドがあります。**File Download from Server** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **File Management** → **File Download** とクリックします。**File Download from Server** ページが開きます。



File Download from Server ページ

File Download from Server ページには、以下のフィールドが含まれています。

- **Firmware Download** — Firmware ファイルがダウンロードされることを示します。**Firmware Download** が選ばれている場合、**Configuration Download** フィールドは淡色表示されます。
- **Configuration Download** — Configuration ファイルがダウンロードされることを示します。**Configuration Download** が選ばれている場合、**Firmware Download** フィールドは淡色表示されます。
- **Firmware Download TFTP Server IP Address** — ファイルをダウンロードする TFTP Server の IP アドレスを示します。
- **Firmware Download Source File Name** — ダウンロードするファイルを指定します。
- **Firmware Download Destination File** — ファイルをダウンロードする先のファイルタイプを示します。可能なフィールド値には、以下のものがあります。
  - **Software Image** — Image ファイルをダウンロードします。
  - **Boot Code** — Boot ファイルをダウンロードします。
- **Configuration Download File TFTP Server IP Address** — Configuration ファイルをダウンロードする TFTP サーバーの IP アドレスを示します。
- **Configuration Download File Source File Name** — ダウンロードする Configuration ファイルを指定します。
- **Configuration Download File Destination** — Configuration ファイルのダウンロード先のファイルを示します。可能なフィールド値には、以下のものがあります。
  - **Running Configuration** — Running Configuration ファイルにコマンドをダウンロードします。
  - **Startup Configuration** — Startup Configuration ファイルをダウンロードして上書きします。
  - **Backup Configuration** — Backup Configuration ファイルをダウンロードして上書きします。

ファイルをダウンロードするには、次の手順を実行します。

1. **File Download from Server** ページを開きます。
2. ダウンロードするファイルタイプを定義します。
3. **TFTP Server IP Address**、**Source File Name**、および **Destination File** フィールドを定義します。
4. **Apply Changes** をクリックします。ソフトウェアがデバイスにダウンロードされます。

メモ： 選択した Image ファイルをアクティブにするには、デバイスをリセットします。デバイスのリセットについては、「デバイスのリセット」を参照してください。

CLI コマンドを使用したファイルのダウンロード

次の表に、**File Download from Server** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
copy *source-url destination-url* **[snmp]**	コピー元からコピー先へファイルをコピーします。

以下に、CLI コマンドの例を示します。

```
console# copy running-config tftp://11.1.1.2/pp.txt
```

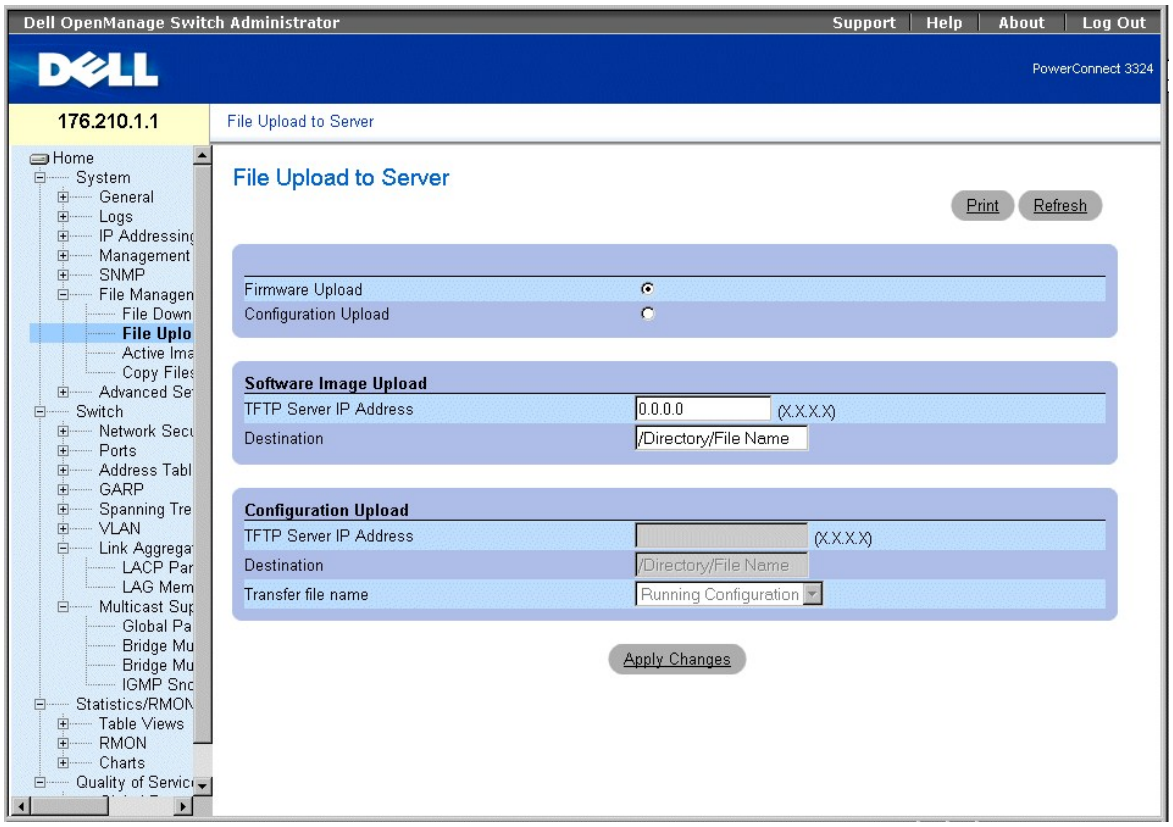
メモ： 各 ! は、10 個のパケットが正常に転送されたことを示します。

```
Accessing file 'file1' on 172.16.101.101.

Loading file1 from 172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

Copy took 0:01:11 [hh:mm:ss]
```

ファイルのアップロード

File Upload to Server ページには、TFTP サーバーからデバイスへソフトウェアをアップロードするためのフィールドがあります。Image ファイルも **File Upload to Server** ページからアップロードできます。**File Upload from Server** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **File Management** → **File Upload** とクリックします。**File Upload to Server** ページが開きます。



File Upload to Server ページ

File Upload to Server ページには、以下のフィールドが含まれています。

- Firmware Upload — Firmware ファイルがアップロードされることを示します。**Firmware Upload** が選ばれている場合、**Configuration Upload** フィールドは淡色表示されます。
- **Configuration Upload** — Configuration ファイルがアップロードされることを示します。**Configuration Upload** が選ばれている場合、**Software Image Upload** フィールドは淡色表示されます。
- **Software Image Upload TFTP Server IP Address** — Software Image のアップロード先の TFTP サーバーの IP アドレスを示します。
- **Software Image Upload Destination** — ファイルがアップロードされる Software Image ファイルパスを指定します。
- **Configuration Upload TFTP Server IP Address** — Configuration ファイルのアップロード先の TFTP サーバーの IP アドレスを示します。
- **Configuration Upload Destination** — ファイルがアップロードされる Configuration ファイルパスを指定します。
- **Configuration Upload Transfer file name** — 設定のアップロード先のソフトウェアファイルを示します。可能なフィールド値には、以下のものがあります。
  - **Running Configuration** — Running Configuration ファイルをアップロードします。
  - **Startup Configuration** — Startup Configuration ファイルをアップロードします。
  - **Backup Configuration** — Backup ファイルをアップロードします。

ファイルをアップロードするには、次の手順を実行します。

1. **File Upload to Server** ページを開きます。
2. アップロードするファイルタイプを定義します。
3. **TFTP Server IP Address**、**Destination**、および **Transfer file name** フィールドを定義します。
4. **Apply Changes** をクリックします。ソフトウェアがデバイスにアップロー

ドされます。

CLI コマンドを使用したファイルのアップロード

次の表に、**File Upload to Server** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
copy source-url destination-url [snmp]	コピー元からコピー先へファイルをコピーします。

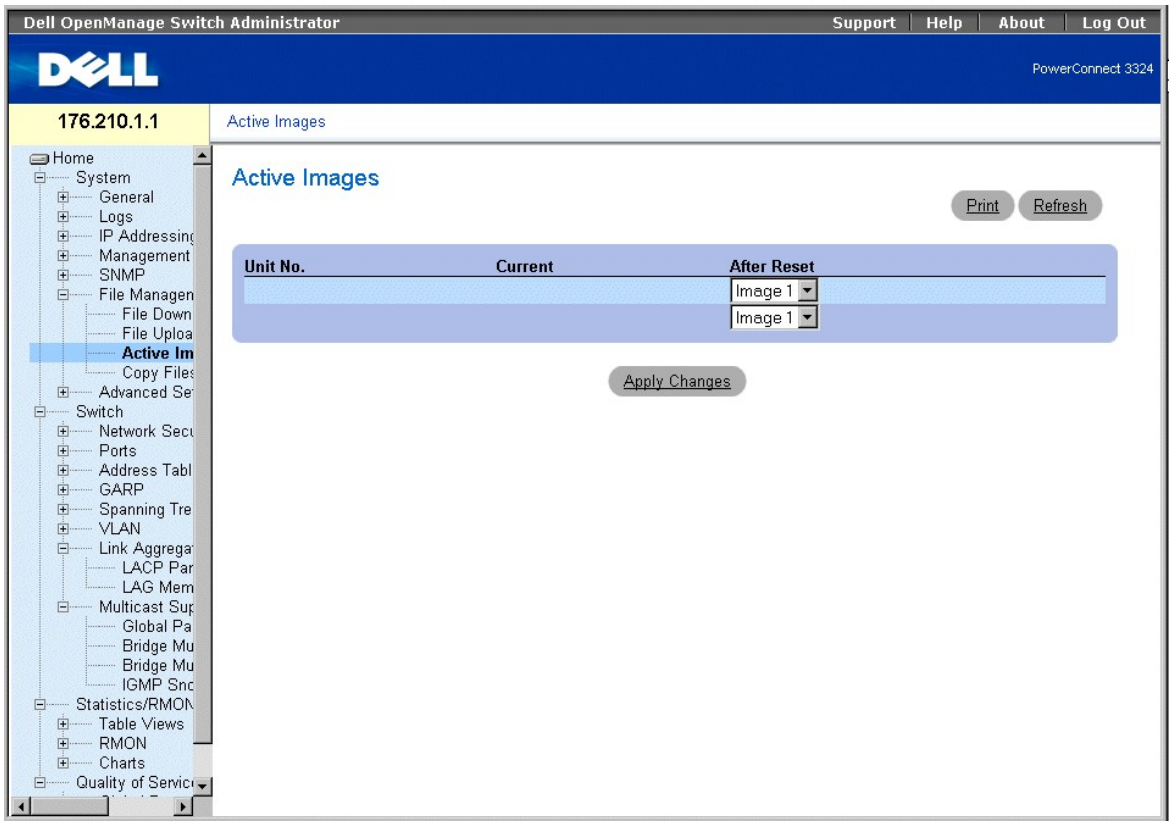
以下に、CLI コマンドの例を示します。

```
-----------------------------------------------------


console# copy tftp://16.1.1.200/file1 image


!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
2883576 bytes copied in 00:00:10 [hh:mm:ss]
```

アクティブイメージのリセット

Active Images ページを使用して、ネットワーク管理者は、Image ファイルの選択とリセットができます。スタッキング構成内の各ユニットの Active Image ファイルは、別々に選ぶことができます。**Active Images** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **File Management** → **Active Images** とクリックします。**Active Images** ページが開きます。



Active Images ページ

Active Images ページには、以下のフィールドが含まれています。

- **Unit No.** — Image ファイルが選択されているユニット番号を表示します。
- **Current** — ユニットで現在アクティブな Image ファイルを表示します。
- **After Reset** — デバイスのリセット後に、ユニットでアクティブな Image ファイルを示します。

イメージファイルを選択するには、次の手順を実行します。

1. **Active Images** ページを開きます。
2. **After Reset** フィールドで、特定のユニットの Image ファイルを選びます。
3. **Apply Changes** をクリックします。Image ファイルが選択されます。次回のリセット後にのみ、Image ファイルが再ロードされます。現在選択されている Image ファイルが、次のデバイスリセットまで実行し続けます。デバイスのリセットについては、「デバイスのリセット」を参照してください。

CLI コマンドを使用したアクティブイメージファイルの作業

次の表に、**Active Images** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
boot system [unit | unit] {image-1 | image-2}	スタートアップ時に、デバイスがロードするシステムイメージを指定します。

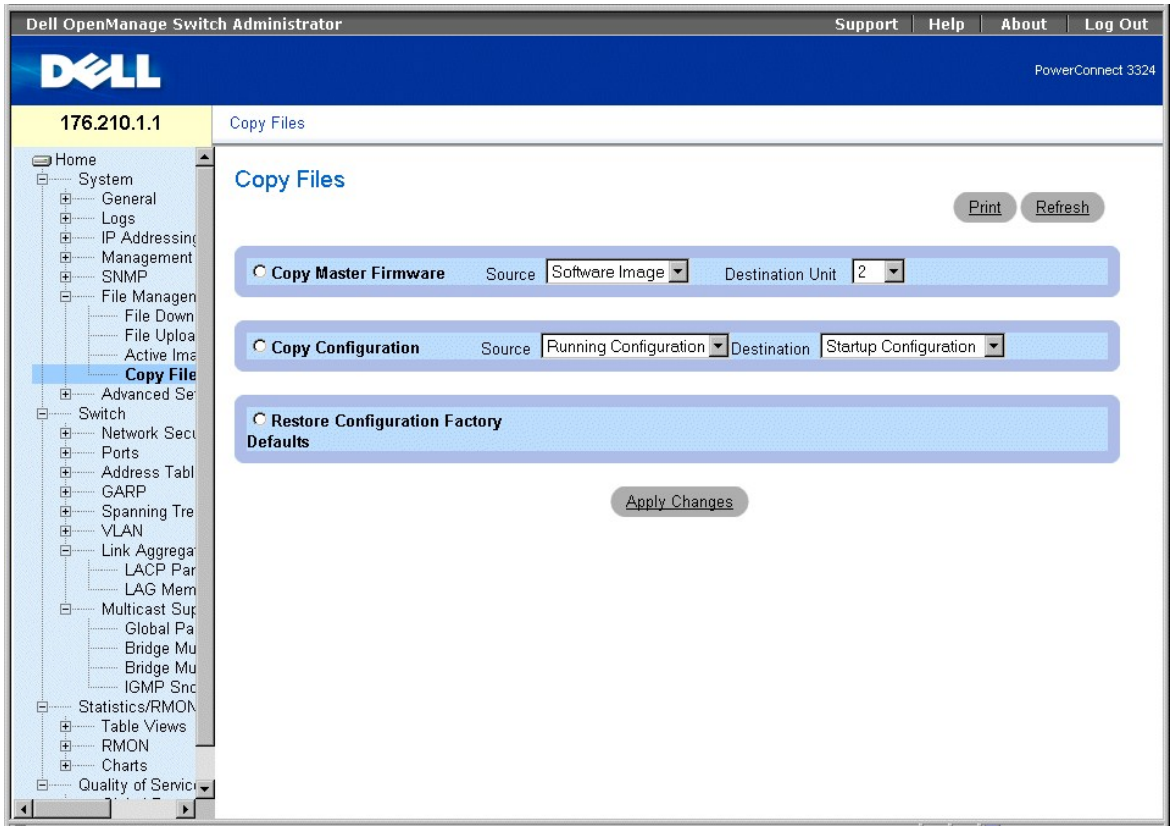
以下に、CLI コマンドの例を示します。

```
Console# boot system image-1
```

ファイルのコピーと削除

Copy Files ページから、ファイルのコピーと削除ができます。
Copy Files ページを開くには、次の手順を実行します。

- Tree View で、**System** → **File Management** → **Copy Files** とクリックします。**Copy Files** ページが開きます。



Copy Files ページ

Copy Files ページには、以下のフィールドが含まれています。

- **Copy Master Firmware** — マスターユニットから選択したスタッキングユニットに Software Image や Boot コードをコピーします。
  - **Source** — Software Image または Boot コードファイルを選択したスタッキングユニットにコピーします。
  - **Destination Unit** — Software Image または Boot コードのコピー先のスタッキングユニットを示します。
- **Copy Configuration** — Startup Configuration ファイルまたは Backup Configuration ファイルに、Running Configuration、Startup Configuration、または Backup Configuration ファイルをコピーします。
  - **Source** — 選択したスタッキングユニットにコピーする Running Configuration、Startup Configuration、または Backup Configuration ファイルを示します。

- **Destination** — 設定が Startup Configuration または Backup Configuration を上書きするかを示します。

- Restore Configuration Factory Defaults — Startup-Config ファイルを消去して、工場出荷時のデフォルトファイルを復元します。Backup-Config ファイルは消去されません。可能なフィールド値には、以下のものがあります。
  - **Checked** — 工場出荷時のデフォルトを復元します。
  - **Unchecked** — 現在の設定を保持します。

ファイルをコピーするには、次の手順を実行します。

1. **Copy Files** ページを開きます。
2. **Copy Configuration** または **Copy Master Firmware** フィールドを選びます。
3. ファイルの **Source** および **Destination** フィールドを定義します。
4. **Apply Changes** をクリックします。ファイルがコピーされ、デバイスがアップデートされます。

工場出荷時のデフォルト設定を復元するには、次の手順を実行します。

1. **Copy Files** ページを開きます。
2. **Restore Configuration Factory Defaults** フィールドを選びます。
3. **Apply Changes** をクリックします。工場出荷時のデフォルト設定が復元され、デバイスがアップデートされます。

CLI コマンドを使用したファイルのコピーと削除

次の表に、**Copy Files** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
delete *startup-config*	Startup-Config ファイルを削除します。
copy *source-url destination-url [snmp]*	コピー元からコピー先へファイルをコピーします。

以下に、CLI コマンドの例を示します。

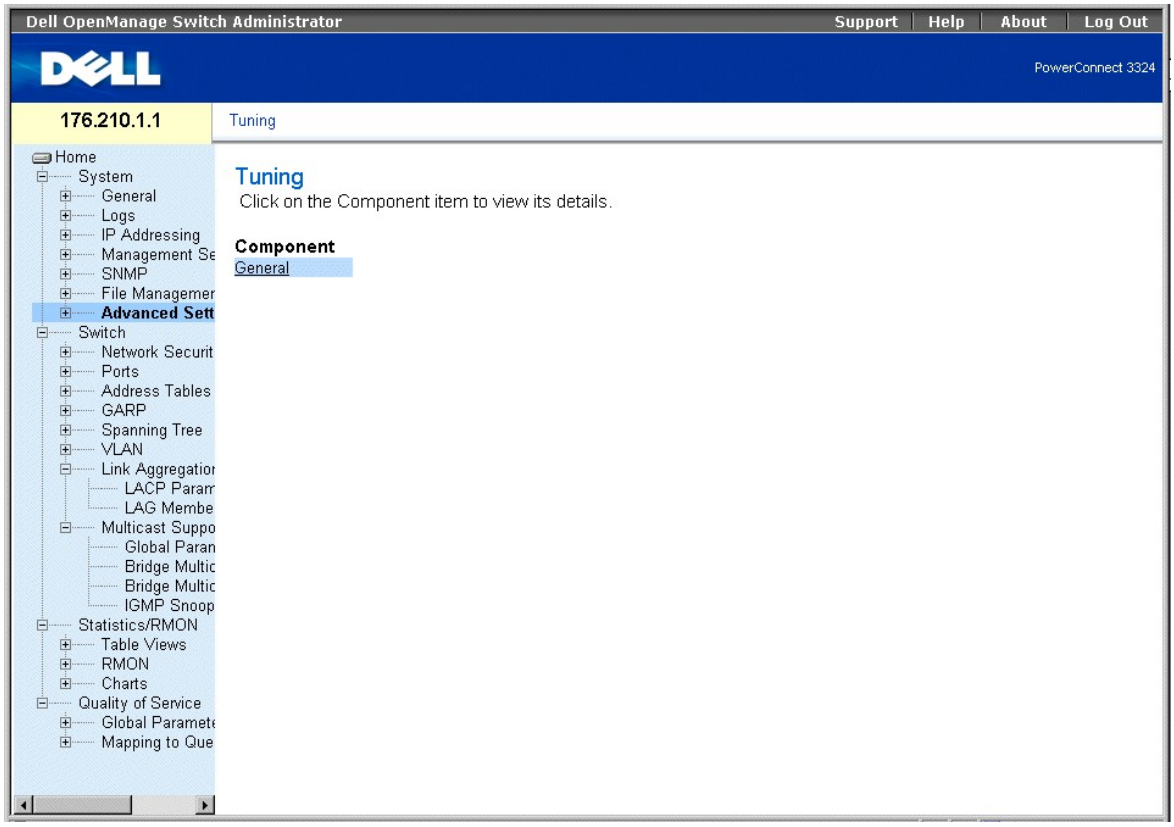
```
Console# delete startup-config

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

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]
```

詳細設定の定義

Device Tuning を使用して、一覧表示されている各種テーブルのエントリの最大数を決定します。デバイスがリセットされるまで、変更は適用されません。**Tuning** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Advanced Settings** とクリックします。
  Tuning ページが開きます。



Tuning ページ

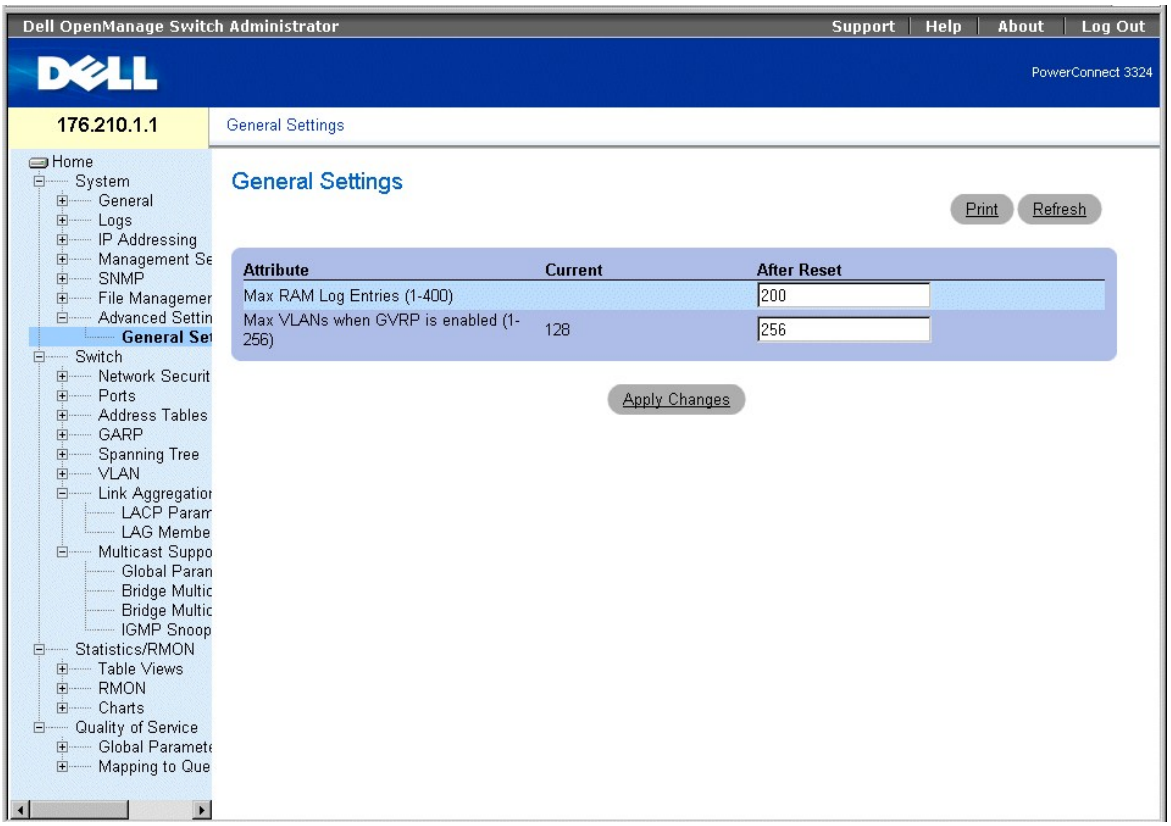
Tuning ページには、以下のリンクがあります。

- 一般的なデバイス調整パラメータの設定

一般的なデバイス調整パラメータの設定

General Settings ページを使用して、ネットワーク管理者は一般的なデバイスパラメータを定義することができます。**General Settings** ページを開くには、次の手順を実行します。

- Tree View で、**System** → **Advanced Settings** → **General** とクリックします。**General Settings** ページが開きます。



General Settings ページ

General Settings ページには、以下のコラムが含まれています。

- **Attribute** — 一般的な設定属性
- **Current** — 現在値
- **After Reset** — リセット後の値。**After Reset** コラムに値を入力することにより、メモリがフィールドテーブルに割り当てられます。

General Tuning ページには、以下のフィールドが含まれています。

- **Max RAM Log Entries (1-400)** — RAM Log エントリの最大数を示します。
  Log エントリが一杯になると、ログはクリアされ Log ファイルが再起動します。
- **Max VLANs when GVRP is enabled (1-256)** — GVRP が有効な場合、VLAN の全体的な数を定義します。

メモ: GVRP VLAN の最大数には、静的または動的 VLAN にかかわらず、GVRP 動作に参加しているすべての VLAN が含まれます。

CLI コマンドを使用した RAM ログエントリカウンタの表示

次の表に、**General Settings** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
logging buffered size *number*	内部バッファ （RAM） に保存されているシスログメッセージの数を設定します。
gvrp max vlan	GVRP が有効になっている際の VLAN の最大数を設定します。

以下に、CLI コマンドの例を示します。

```
Console (config)# logging buffered size 300
```

メモ、注意および警告

メモ、注意および警告

困ったときは

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

テクニカルサポート

技術的な問題について支援が必要な場合は、インストールとトラブルシューティングに関するヘルプが記載された、デルサポートウェブサイト（**support.jp.dell.com**）をご覧ください。

詳細については、「オンラインサービス」を参照してください。

これまでの手順で問題が解決されず、デルの技術者に問い合わせなければならないときは、デルのテクニカルサポートにお電話ください。

メモ: デルへお問い合わせになるときは、できればシステムの電源を入れて、システムの近くの電話から電話をかけてください。テクニカルサポート担当者がコンピュータの操作をお願いすることがあります。

メモ: デルのエクスプレスサービスコードシステムは、ご利用になれない国もあります。

デルのオートテレフォンシステムの指示に従って、エクスプレスサービスコード を入力すると、電話は適切なサポート担当者に転送されます。エクスプレスサービスコード（8 桁から 11 桁までの全桁数字のみの番号）は、コンピュータの前面、背面、または側面に貼られているシールに、サービスタグナンバー（5 桁もしくは 7 桁までの英数字混合の番号）と共に、記載されています（コンピュータ正面パネルに内に貼られている機種もあります）。

テクニカルサポートにお問い合わせの際は、「テクニカルサポートサービス」および「お問い合わせになる前に」をご覧ください。

メモ: 以下のサービスは、アメリカ以外ではご利用になれないこともあります。
サービスに関する情報は、最寄りのデルへお問い合わせください。

オンラインサービス

Dell Supportへは、**support.jp.dell.com**からアクセスできます。また、**support.jp.dell.com** のサイトで表示された地図上のお住まいの国をクリックすると、**サポートサイトへようこそ** ページが開きます。お使いのシステムの情報を入力し、サポートツールおよび情報にアクセスします。

インターネット上でのデルへのアクセスは、次のアドレスをご利用ください。

- World Wide Web http://www.dell.com/jp/（日本）

www.dell.com/（米国）

www.dell.com/ap/（アジア／太平洋諸国のみ）

www.euro.dell.com.（ヨーロッパのみ）

www.dell.com/la（ラテンアメリカ諸国）

www.dell.ca（カナダのみ）

- オンライン見積りサービス

sales@dell.com

apmarketing@dell.com（アジア／太平洋諸国のみ）

sales_canada@dell.com（カナダのみ）

- オンライン情報サービス

info@dell.co/jp/

ファックス情報サービス

オペレーティングシステムの再インストール情報など、技術的なサポート資料をお手持ちのFAXにお届けするサービスです。音声応答により、FAXBOX から必要な資料を注文することができます。

プッシュホン式の電話を使って、必要な資料を選択します。

ファックス情報サービスは、年中無休、毎日 24 時間いつでもご利用いただけます。資料は指定したファックス番号宛に送信されます。{DELETE !}このサービスの電話番号は「デルの連絡先」を参照してください。

24 時間納期案内電話サービス

注文したデル™製品の状況を確認するには、**www.dell.com/jp/** にアクセスするか、24 時間納期案内電話サービスにお問い合わせください。電話サービスでは、録音された指示に従って、ご注文の製品の納期を確認することができます。{DELETE !}このサービスの電話番号は「デルの連絡先」を参照してください。

テクニカルサポートサービス

デル製品に関するお問い合わせは、デルのテクニカルサポートをご利用ください。テクニカルサポートに電話をおかけになると、サポート担当者がお問い合わせの内容を確認するために、ご使用のシステムの詳細をお聞きすることがあります。サポート担当者はこの情報をもとに、正確な解答を迅速に提供します。

デルのテクニカルサポートにお問い合わせになる場合は、「お問い合わせになる前に」をお読みになってから、「デルの連絡先」を参照してください。

Dell 企業向けトレーニングおよび資格認証

Dell では、企業向けのトレーニングと資格認証を実施しております。詳細については、**http://www.dell.com/training** を参照してください。このサービスは、ご利用いただけない地域があります。

製品情報

Dellのその他の製品に関する情報や、ご注文に関しては、Dellのウェブサイトの**www.dell.com/jp/**をご覧ください。電話によるお問い合わせの場合は、「デルの連絡先」を参照してください。

お問い合わせになる前に

メモ: お電話の際には、エクスプレスサービスコードをご用意ください。エクスプレスサービスコードがあると、デルの電話自動サポートシステムによって、より迅速にサポートが受けられます。

デルのテクニカルサポートにお問い合わせの際には、できればコンピュータの電源を入れて、コンピュータの近くの電話から電話をかけてください。これは、キーボードからコマンドを入力したり、操作時に詳細情報を読んでいただいたり、問題のあるシステム自体でなければ実行できないトラブルシューティング手順を試されるように、サポート担当者がお願いする場合があるからです。また、システムのマニュアルもご用意ください。

警告: コンピュータ内部の作業を行う前に、「システム情報ガイド」を参照して、安全に関する注意事項について確認してください。

Dell の連絡先

インターネット上でのデルへのアクセスには、次のアドレスをご利用ください。

- **www.dell.com**
- **support.jp.dell.com**（テクニカルサポート）

デルへお問い合わせになる場合、次の表の電子アドレス、電話番号、およびコードをご利用ください。国際電話のかけ方については、国内または国際電話会社にお問い合わせください。

国（市） 国際電話アクセスコード 国番号 市外局番	部署名またはサービス内容、ウェブサイトおよび電子メールアドレス	市外局番 市内番号、または フリーダイヤル番号
日本（川崎） 国際電話アクセスコード: **001** 国番号: **81** 市外局番: **44**	ウェブサイト: **support.jp.dell.com**	
	テクニカルサポート（サーバー）	フリーダイヤル: 0120-198-498
	テクニカルサポート（海外から）（サーバー）	81-44-556-4162
	テクニカルサポート （Dimension™ および Inspiron™）	フリーダイヤル: 0120-198-226
	テクニカルサポート（海外から） （Dimension および Inspiron）	81-44-520-1435
	テクニカルサポート （Dell Precision™、OptiPlex™ Latitude™）	フリーダイヤル: 0120-198-433
	テクニカルサポート（海外から） （Dell Precision、OptiPlex、Latitude）	81-44-556-3894
	テクニカルサポート(Axim™)	フリーダイヤル: 0120-981-690
	テクニカルサポート（海外から）（Axim）	81-44-556-3468
	ファックス情報サービス	044-556-3490
	24時間納期案内サービス	044-556-3801
	カスタマーケア	044-556-4240

	ビジネスセールス本部 （従業員数 400 人未満の企業のお客様）	044-556-1465
	法人営業本部 （従業員数 400 人以上の企業のお客様）	044-556-3433
	エンタープライズ営業本部 （従業員数 3500 人以上の企業のお客様）	044-556-3430
	パブリック営業部 （官公庁/研究・教育機関/医療機関のお客様）	044-556-1469
	グローバル営業本部 （Global Segment Japan）	044-556-3469
	個人のお客様	044-556-1760
	代表電話番号	044-556-4300

メモ、注意および警告

メモ、注意および警告

はじめにお読みください

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

Switch Administrator の起動

Dell™ PowerConnect™ 3324/3348 Dell OpenManage™ Switch Administrator は、ウェブブラウザを搭載しているすべての PC からアクセスすることができます。Switch Administrator を起動するには、次の手順を実行します。

1. ウェブブラウザを起動します。
2. デバイスの IP アドレス/home.htm をアドレスバーに入力して、<Enter> を押します。ログインウィンドウが表示されます。

PowerConnect 3324/3348 Password ページ

3. ユーザー名とパスワードを入力します。

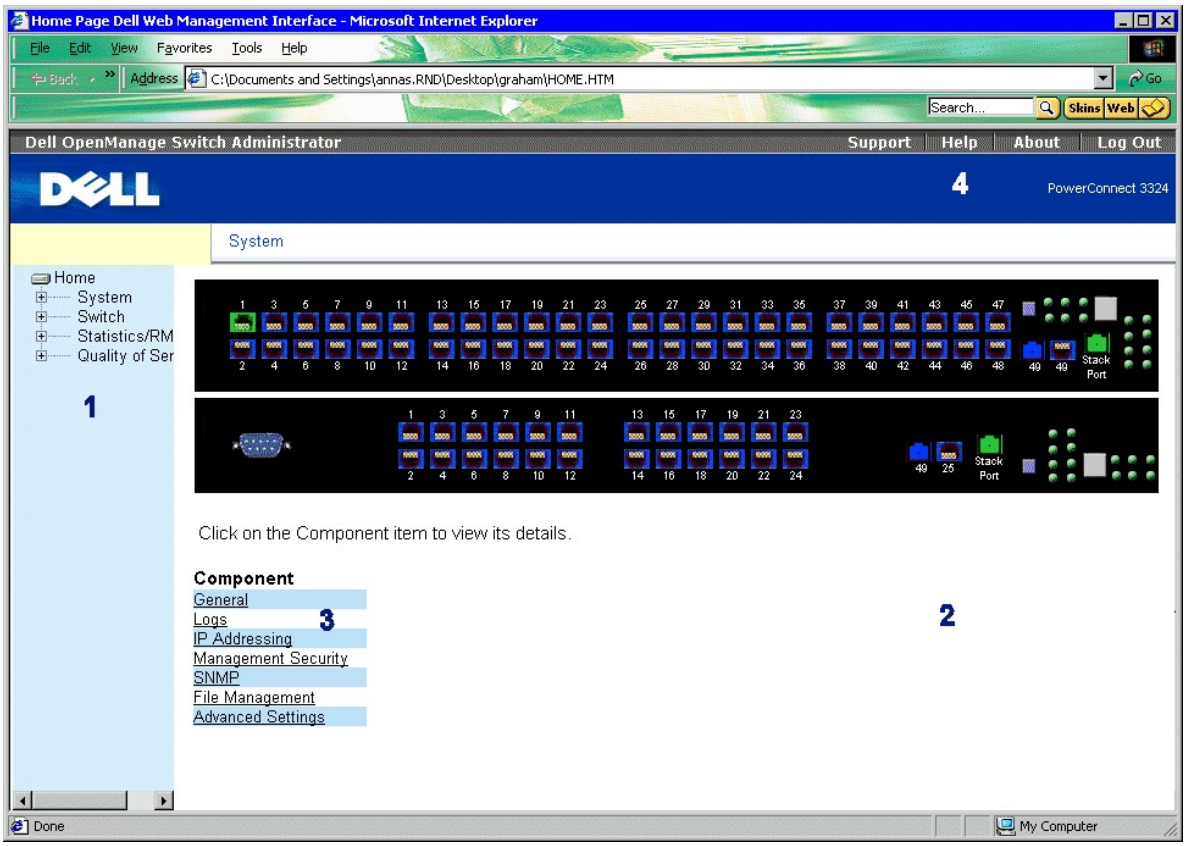
メモ: パスワードを入力しなくても、PowerConnect 3324/3348 の設定は可能です。
パスワードは、大文字と小文字が区別されます。英数文字で入力してください。

4. **OK**をクリックします。**Switch Administrator** のホームページが表示されます。

インタフェースの概要

Switch Administrator のホームページには、以下の表示部分があります。

- Tree View — **Switch Administrator** ホームページの左側に表示され、機能やコンポーネントを展開して表示できます（Component List）。
- Device View — **Switch Administrator** ホームページの右側に表示され、デバイス、情報または表の表示、および設定手順を表示します。



PowerConnect 3324/3348 ウェブ管理インタフェース

PowerConnect 3324/3348 Interface Components Table では、インタフェースコンポーネントとそれに対応する数字を一覧表示します。

PowerConnect 3324/3348 Interface Components Table

コンポーネント	名前
1	Tree View（ツリービュー）Tree View — Tree View には、デバイスの様々な機能の一覧が含まれています。Tree View の詳細については、「Tree View（ツリービュー）」を参照してください。
2	Device View（デバイスビュー）Device View は、デバイスポート、表、および搭載されているコンポーネントについての情報を提供します。Tree View の詳細については、「Device View（デバイスビュー）」を参照してください。
3	コンポーネントリストComponent List には、搭載されているコンポーネントの一覧が含まれています。Component List の使い方の詳細については、「コンポーネントリスト」を参照してください。
4	Information（情報）ボタンInformation ボタンは、PowerConnect デバイスの情報およびデルのサービスへのアクセスを提供します。Tree View の詳細については、「Switch Administrator ボタンの使い方」を参照してください。

Tree View（ツリービュー）

Tree View には、Switching 機能、ポート、Spanning Tree、VLAN、Class of Service、LAG（Link Aggregation）、Multicast Support、および Statistics を含む様々な機能の一覧が含まれています。

Tree View の各枝は、特定の機能ですべてのコンポーネントを表示するために展開したり、機能のコンポーネントを非表示するために閉じることができます。

Device View（デバイスビュー）

以下の項では、Device View の異なる機能を説明します。Device は、PowerConnect 3324/3348 スイッチの情報を提供します。Device View には、以下の機能が含まれています。

- コンポーネントリスト
- デバイスのグラフィック表示
- ワークデスク

コンポーネントリスト

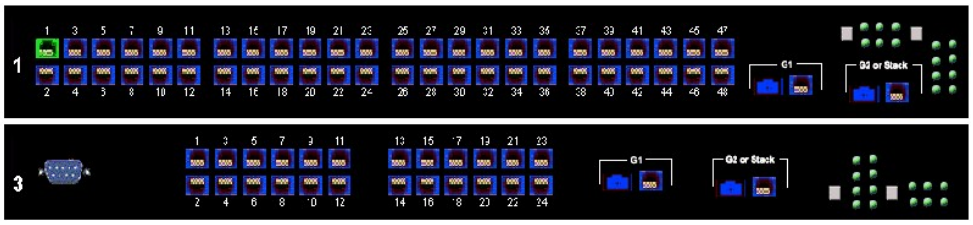
Switch Administrator ホームページで、機能メニューオプションを含む Component List を表示します。コンポーネントの機能を表示するには、次の手順を実行します。

- Component List アイテムをクリックします。特定のコンポーネントのページが開きます。たとえば、Tree View で、**Switch** をクリックすると、次のページが表示されます。

コンポーネントリスト

デバイスのグラフィック表示

Switch Administrator ホームページで、グラフィックを使用して PowerConnect 3324/3348 の正面パネルを表示します。



PowerConnect 3348

ポートの色は、特定のポートが現在アクティブかどうかを示します。ポートは以下の色で表示されます。

PowerConnect 3324/3348 ポートインジケータ

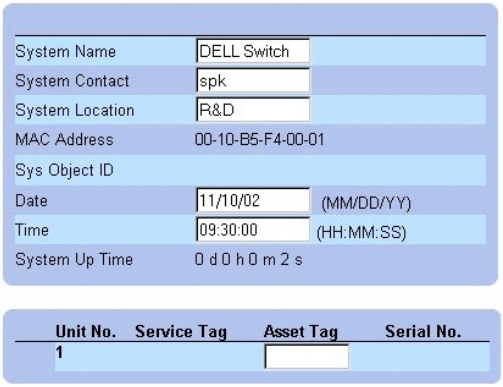
コンポーネント	名前
緑色	ポートは接続されています。
Blue	ポートはセキュリティ機能によってサスペンド状態です。
Red	ポートは接続されていません。

メモ: LED は、PowerConnect 3324/3348 の正面パネルの Switch Administrator には反映されません。LED のステータスは、実際のデバイスを見ることで確認できます。
LED の詳細については、「LED の定義」を参照してください。

ワークデスク

Device View のワークデスクは、デバイスの表、デバイスの全般情報、およびデバイスパラメータの設定を含む作業領域を提供します。以下の図に、表示されるワ

ークデスクの例を示します。



ワークデスク情報の例

Switch Administrator ボタンの使い方

この項では、インタフェースで提供される異なった OpenManage *Switch Administrator* ボタンについて説明します。Switch Administrator には、以下のボタンが含まれます。

- Information ボタン — テクニカルサポート、オンラインヘルプ、デバイスの情報、および *Switch Administrator* を含む情報サービスへのアクセスを提供します。
- Device Management ボタン — Add、Delete、Query、および Apply Changes ボタンを含む *Switch Administrator* 管理ボタンについて説明します。

Information（情報）ボタン

Switch Administrator ホームページには、以下の Information ボタンがあります。

Information（情報）ボタン

ボタン	説明
Support	デルサポートページを開きます。デルテクニカルサポートのアドレスは、**support.jp.dell.com** です。
Help	オンラインヘルプを開きます。
About	**About** ページを開きます。
Log Out	Switch Administrator からログアウトします。

Support（サポート）ボタン

Support ページには、デルテクニカルサポートページへのアクセスの情報が含まれています。

1. **Support** をクリックします。**Dell Technical Support** ページが開きます。

Dell Technical Support ページ

2. 必要なサポートを説明している領域を選びます。該当するページが表示されます。
3. ユーザー名とパスワードを入力します。
4. **Login** をクリックして、手順を完了します。

メモ: 必要とするテクニカルサポートによっては、ユーザー名とパスワードが必要な場合があります。

Help（ヘルプ）ボタン

Online Help ページには、スイッチの設定および管理に役立つ情報が含まれています。

1. **ヘルプ** をクリックします。**Online Help** ページが開きます。
2. Help トピックを選びます。選択した Help トピックのページが開きます。

メモ: 各画面には、簡単な Help ページが含まれています。Help にアクセスするには、Switch Administrator ページで **Help** をクリックします。

[バージョン情報] ボタン

The **バージョン情報**ボタンをクリックすると、**バージョン情報** ページが開きます。**About** ページには、デバイス名、ソフトウェアリリースナンバー、およびデルの著作権情報が含まれています。**About** ページにアクセスするには、次の手順を実行します。

- **About** をクリックします。**About** ページが開きます。

PageDevice Management ボタン

Switch Administrator 管理ボタンを使用して、ネットワーク管理者は、PowerConnect をリモートで簡単に設定することができます。Switch Administrator には、以下の管理ボタンが含まれています。

Device Management ボタン

ボタン	説明
Apply Changes	デバイスに設定の変更を適用します。
Add	表または情報ウィンドウに情報を追加します。
Telnet	Telnet セッションを開始します。
Reset All Counters	テーブルを照会します。
Show All	デバイスの表を表示します。
Transfer to Server	デバイスからサーバーにファームウェアを転送します。
← →	リスト間で情報を移動します。
Refresh	デバイス情報を更新します。
Show Log File	**Log File Table** ページを開きます。
Show Log RAM	**Log Ram Table** ページを開きます。

Restart DHCP	DHCP クライアント接続を再起動します。
Add ACE to ACL	ACE を ACL に追加します。
Add ACL	ACL を追加します。
Add List Name	新しいリストを追加します。
Attach to Interface	様々なリストをインタフェースに付加します。
Reset All Counters	統計カウンタをリセットします。
Print	**Network Management System** ページまたはテーブルの情報を印刷します。
Sort	テーブルの情報をソートします。
Show Neighbors List	**Neighbors Table** ページから、Neighbors List を表示します。
Restore Defaults	デバイスのデフォルト設定を復元します。
Draw	Statistics チャートをオンザフライで作成します。

CLI の使い方

この項には、CLI（コマンドラインインタフェース）の概要が含まれています。

Command Mode（コマンドモード）

CLI はコマンドモードに分かれます。各コマンドモードには、特定のコマンドセットがあります。システムプロンプト（コンソールプロンプト）で ?（疑問符）を入力すると、特定のコマンドモードで利用可能なコマンドが一覧表示されます。

各モードで、特定のコマンドを使用してコマンドモード間を移動できます。モードにアクセスするための以下の標準があります。

- User EXEC Mode（ユーザーアクセスモード）
- Privileged EXEC Mode（特権アクセスモード）
- Global Configuration Mode（グローバル設定モード）
- Interface Configuration Mode（インタフェース設定モード）

CLI セッション初期化中は、CLI モードは User EXEC Mode です。User EXEC Mode では、限られたコマンドのサブセットしか利用できません。このレベルは、デバイス設定を変更しないタスクや CLI などのサブシステム設定にアクセス用に確保されています。次のレベル Privileged EXEC Mode を起動するには、パスワードが必要です。

Privileged EXEC Mode は、デバイスの全般的な設定へのアクセスを提供します。デバイスでの特定のグローバル設定には、次のレベル Global Configuration Mode を起動する必要があります。パスワードは必要ありません。

Global Configuration Mode は、デバイスの設定をグローバルレベルで管理します。特定の設定には、次のレベル Interface Configuration Mode を起動する必要があります。パスワードは必要ありません。

Interface Configuration Mode は、デバイスを物理的なインタフェースレベルで設定します。サブコマンドが必要なインタフェースコマンドには、別のレベル Subinterface Configuration Mode があります。パスワードは必要ありません。

User EXEC Mode（ユーザーアクセスモード）

デバイスにログオンすると、User EXEC コマンドモードが有効になります。User EXEC コマンドを使用して、リモートデバイスの接続、ターミナル設定の一時的な変更、基本的なテストの実行、およびシステム情報の一覧表示をおこないます。

User EXEC コマンドを一覧表示するには、? コマンドを入力します。

ユーザーレベルのプロンプトは、ホスト名とそれに続くブラケット (>) で構成されます。

```
console>
```

メモ: デフォルトのホスト名は、初期設定で変更しないかぎり `console` です。

Privileged EXEC Mode（特権アクセスモード）

このモードを使用して、特権アクセスがパスワードによって無許可の使用から保護されているか確認します。パスワードは、画面で `*****` と表示され大文字と小文字が区別されます。

Privileged EXEC Mode コマンドにアクセスして一覧表示するには、次の手順を実行します。

1. プロンプトで、enable コマンドを入力して、<Enter> を押します。パスワードプロンプトが表示されます。
2. パスワードを入力して、<Enter> を押します。パスワードは * として表示されます。Privileged EXEC Mode プロンプトが表示されます。Privileged EXEC Mode プロンプトは、デバイスのホスト名とそれに続く # で構成されます。

```
console#
```

- Privileged EXEC コマンドを一覧表示するには、? コマンドを入力します。

Privileged EXEC Mode から User EXEC Mode に戻るには、以下のコマンドを使用します。

- `enable`
- `disable`
- `exit/end`
- Ctrl+Z

以下の例では、Privileged EXEC Mode にアクセスして、User EXEC Mode に戻る方法を示します。

```
console>enable
```

```
Enter Password: ******


console#


console#disable


console>
```

exit コマンドを使用して、たとえば、Interface Configuration Mode から Global Configuration Mode に、Global Configuration Mode から Privileged EXEC Mode のように、あるモードから前のモードに戻ります。

Global Configuration Mode（グローバル設定モード）

Global Configuration コマンドは、特定のプロトコルまたはインタフェースではなくシステム機能に適用されます。Privileged EXEC Mode コマンド configure を使用して、Global Configuration Mode を起動します。

Global Configuration Mode コマンドにアクセスして一覧表示するには、次の手順を実行します。

- Privileged EXEC Mode プロンプトで、configure と入力して、<Enter> を押します。Global Configuration Mode プロンプトが表示されます。Global Configuration Mode プロンプトは、デバイスのホスト名とそれに続く # および (config) で構成されます。

```
console(config)#
```

- Global Configuration コマンドを一覧表示するには、? コマンドを入力します。

Global Configuration Mode から Privileged EXEC Mode に戻るには、以下のコマンドのうちの 1 つを使用します。

- exit
- Ctrl+Z

以下の例では、Global Configuration Mode にアクセスして、Privileged EXEC Mode に戻る方法を示します。

```
console#


console#configure


console(config)#exit


console#
```

Interface Configuration Mode（インタフェース設定モード）

Interface Configuration コマンドを使用して、ブリッジ - グループ、および説明などの特定の IP インタフェースを変更します。Interface Configuration Mode には、以下のものがあります。

- VLAN — たとえば、VLAN を作成して IP アドレスをVLAN に適用するなどのように、VLAN 全体を作成したり設定するコマンドが含まれています。
- Port Channel — ポートを LAG に割り当てるなどの個別のポートを設定するコマンドが含まれています。
- Line Interface — 管理接続を設定するコマンドが含まれています。これらの設定には、回線速度およびタイムアウト設定が含まれています。
- IP Access-List — アクセス一覧を管理するコマンドが含まれています。このコマンドを使用して、一覧を作成したり管理します。
- Ethernet — ポートの設定を管理するコマンドが含まれています。
- Management Access List — 管理用のアクセス一覧を定義するコマンドが含まれています。アクセス一覧を使用して、アクセス権限およびユーザー認証を管理します。
- MAC List — MAC アドレスに基づくトラフィックを許可する条件を設定します。

CLI の起動

PowerConnect 3324/3348 は、コンソールポートへの直接接続または Telnet 接続を介して管理することができます。PowerConnect 3324/3348 は、コマンドプロンプトでコマンドキーワードおよびパラメータを入力して管理できます。CLI の使用は、UNIX システムでコマンドを入力するのに似ています。

Telnet コネクションを介したアクセスでは、デバイスに定義済みの IP アドレスがあり、CLI コマンドを使用する前に、デバイスにアクセスするワークステーションがデバイスに接続されているか確認します。

初期 IP アドレスの設定については、「初期設定」を参照してください。

コンソール接続

CLI を起動するには、次の手順を実行します。

1. デバイスを起動して、スタートアッププロンプト `Console>` が表示されるまで待ちます。
2. デバイスを設定して、タスクを完了するのに必要なコマンドを入力します。
3. 入力が終わったら、`quit` または `exit` と入力してセッションを終了します。

現在のユーザーをログオフして新しいユーザーでログオンするには、Privileged EXEC コマンドモードでログインコマンドを入力します。

メモ: Telnet セッションは、ユーザーが定義したアイドルタイムが切れると自動的に切断されます。

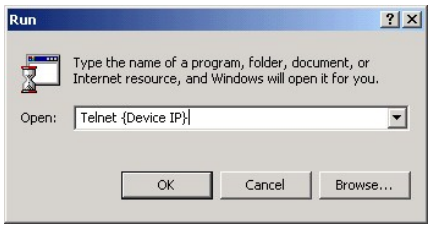
Telnet 接続

Telnet は、ターミナルエミュレーション TCP/IP プロトコルです。ASCII ターミナルは、TCP/IP プロトコルネットワークを介してローカルデバイスに仮想的に接続できます。Telnet は、リモートログインが必要なローカルログインターミナルに代わるものです。

PowerConnect 3324/3348 は、4 つまでの同時 Telnet セッションに対応しています。すべての CLI コマンドは、Telnet セッションで使用できます。

Telnet セッションを開始するには、次の手順を実行します。

1. **Start** → **Run** と選びます。**Run** ウィンドウが開きます。



Run ウィンドウ

2. `Telnet` と入力して、**Open** フィールドにデバイスの IP アドレスを入力します。
3. **OK**をクリックします。Telnet セッションが起動します。

Telnet ウィンドウ

メモ、注意および警告

メモ、注意および警告

ハードウェアについて

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

PowerConnect 3324/3348 について

PowerConnect 3324/3348 の寸法

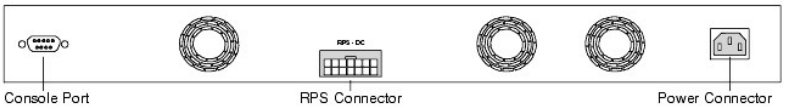
このデバイスの寸法は以下のとおりです。

- 幅 — 19″
- 高さ — 1U

PowerConnect 3324/3348 の背面パネル

Dell™ PowerConnect™ 3324/3348 の背面パネルを以下の図に示します。

PowerConnect 3324 の背面パネル



PowerConnect 3348 の背面パネル

PowerConnect 3324/3348 のコンポーネント

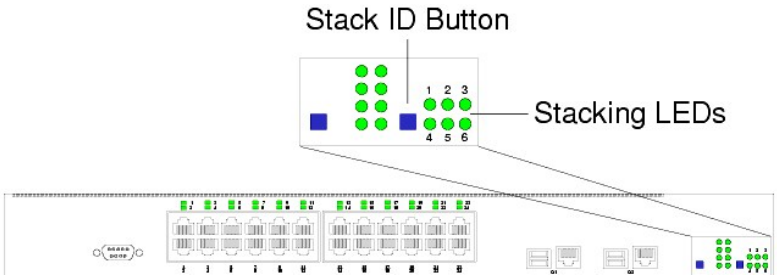
この項では、以下の項目を含む異なった PowerConnect 3324/3348 ハードウェアコンポーネントについて説明します。

- 一般的なデバイスコンポーネント
- モードボタン
- スタック ID ボタン

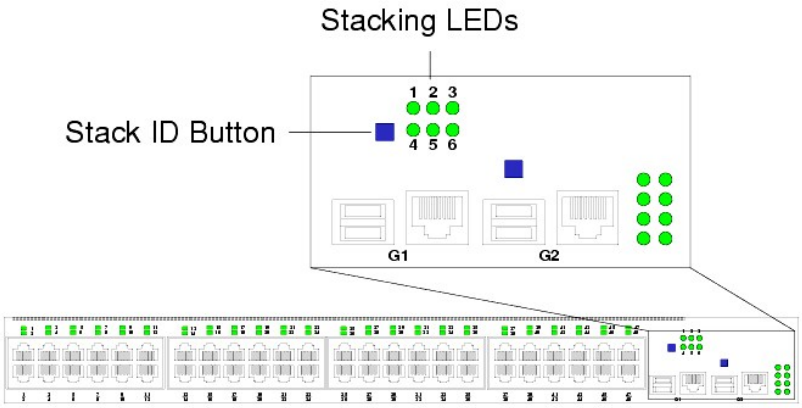
一般的なデバイスコンポーネント

PowerConnect 3324/3348 は、以下のハードウェアコンポーネントを含みます。

- CPU — モトローラ社製 MPC 8245 ベースの CPU
- フラッシュ — 8 MB のフラッシュメモリ
- SDRAM — 32 MB を搭載



PowerConnect 3324 の正面パネル



PowerConnect 3348 の正面パネル

モードボタン

Mode ボタンを使用して、ポートアクティビティおよびポートの二重方式設定を切り替えます。

スタック ID ボタン

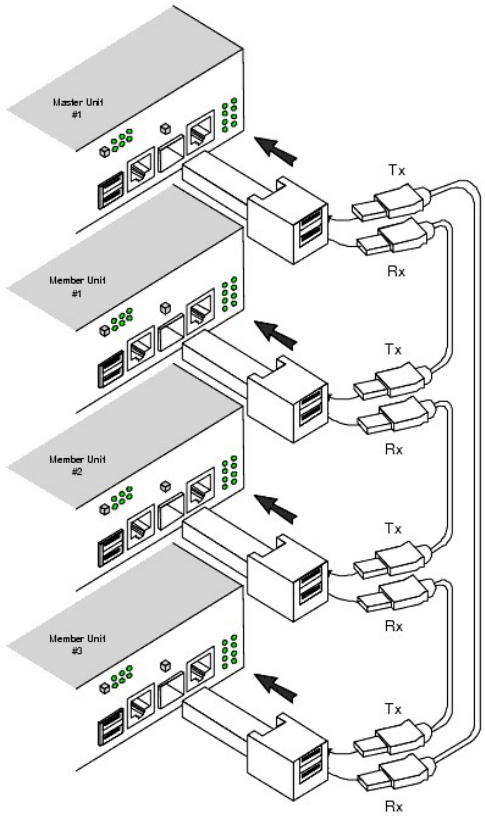
PowerConnect 3324/3348 の正面パネルには、ネットワーク管理者が手動で Stack Master およびスタックメンバーを選択できる **Stack ID** ボタンがあります。

メモ: Stack Master およびスタックメンバーはデバイスを起動してから 15 秒以内に選択する必要があります。スタックマスターが 15 秒以内に選択されなかった場合、デバイスは Unit ID を選択するようにリセットする必要があります。

スタックマスターが選択されると、残りのデバイスはスタックメンバーとして定義されます。マスターユニットは Unit ID 1 を受け取ります。スタックメンバーは別の Unit ID
（2 ～ 6）を受け取ります。たとえば、スタックに 4 つのユニットがある場合、マスターユニットは Unit ID 1、2 番目のスタックメンバーは Unit ID 2、3 番目のスタックメンバーは Unit ID 3、そして 4 番目のスタックメンバーは Unit ID 4 を受け取ることになります。

モジュールおよびコネクタのスタッキング

PowerConnect 3324/3348 スタッキングモジュールはポート G2 に接続されています。スタックモジュールは、RX および TX の 2 つのスタッキングコネクタを持つミニ GBIC モジュールです。RX は下部のコネクタポイントで、TX は上部のコネクタポイントです。モジュールは、スタッキングケーブル接続を使用して他のスタッキングユニットに接続されています。最上部の RX は下部ユニットの TX に接続されています。これでリングトポロジが完成します。スタッキング接続の図でリングトポロジを示します。



スタッキング接続

スタッキングケーブルの接続については、「スタッキングケーブルの接続」を参照してください。

ポートについて

Ethernet ポートについて

PowerConnect 3324 には、各ユニットに 24 個の FE 10BaseT/100BaseTX UTP 銅製 RJ45 ポートと 2 個のコンボポートがあります。PowerConnect 3348 には、各ユニットに 48 個の FE 10BaseT/100BaseTX UTP 銅製 RJ45 ポートと 2 個のコンボポートがあります。各コンボポートは、以下の 2 つの物理的なインタフェースを持つ単一の理論ポートです。

- 1000Base-T コネクタ
- ミニ GBIC（SFP）コネクタ

コンボポートで同時に使用できるのは、2 つの物理的な接続のうちの 1 つのみです。

自動 MDIX が有効な場合、PowerConnect 3324/3348 は、すべてのポートでクロスオーバケーブルとストレートケーブルの違いを自動的に検出して修正します。

PowerConnect 3324/3348 は、銅製ポートで 10/100 Mbps の半二重および全二重モードに対応しています。

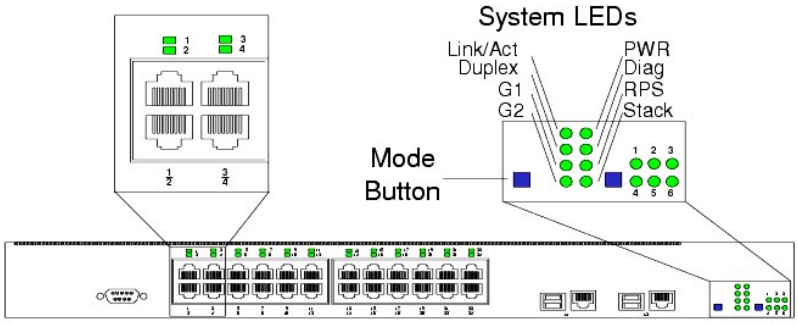
コンソールポートについて

コンソールポートインタフェースは、8 データビット、1 ストップビット、およびパリティなしの同期データに対応しています。モデムのサポート用（9 ピン）にすべての RS232 ピンに対応しています。

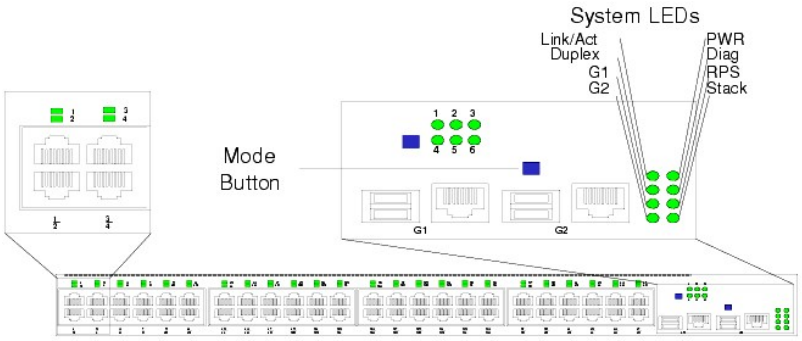
LED の定義

次の図に示す正面パネルの LED は、ポートリンクとモードの状態、電源装置の状態、スタッキングの状態、およびシステム診断を示します。以下の LED のタイプがあります。

- ポート LED
- システム LED
- スタッキング LED



正面パネルの LED: 24 ポート



正面パネルの LED: 48 ポート

ポート LED

各ポートには、ポートの上部に対応する LED があります。ポート LED は LED ディスプレイモードによって、リンクアクティビティまたは二重方式モードのどちらかを示します。LED ディスプレイモードの設定については、「システム LED」を参照してください。

色	動作	定義
緑色	点灯	ポートリンクが動作しています。 ポートは 100 Mbps で動作しています。
緑色	点滅	ポートリンクが動作中で、作業を実行しています。 ポートは 100 Mbps で動作しています。
赤色	点灯	ポートリンクが動作しています。 ポートは 10 Mbps で動作しています。
赤色	点滅	ポートリンクが動作中で、作業を実行しています。 ポートは 10 Mbps で動作しています。
消灯	消灯	ポートリンクがダウンしています。

ポートリンクの動作

色	動作	定義
緑色	点灯	ポートは全二重モードです。
消灯	消灯	ポートリンクはダウンしているか、半二重モードです。

ポートの二重方式モード

システム LED

8 つのシステム LED はデバイスの様々な面の状態を示します。

- この項の最初の正面パネルの図で示したように、左上の 2 つのシステム LED はリンクアクティビティおよび二重方式モードを示します。これらの LED は、ポート LED がリンクアクティビティ状態または二重方式モード状態のどちらを表示しているかを示します。
- 図の左下の 2 つの LED は、Giga ポート 1 および 2 のリンクアクティビティを以下のように示します。

色	動作	定義
緑色	点灯	ポートリンクが動作しています。 ポートは 1000 Mbps で動作しています。
緑色	点滅	ポートリンクが動作中で、作業を実行しています。 ポートは 1000 Mbps で動作しています。
赤色	点灯	ポートリンクが動作しています。 ポートは 10/100 Mbps で動作しています。
赤色	点滅	ポートリンクが動作中で、作業を実行しています。 ポートは 10/100 Mbps で動作しています。
消灯	消灯	ポートリンクがダウンしています。

Giga ポートリンクの動作状態

- システム LED の横にある **Mode** ボタンを使用して、2 つのディスプレイモードを切り替えます。各モードでのポート LED については、「ポート LED」を参照してください。

電源装置が故障した場合、エラーメッセージといくつかのトラップが生成されます。各電源装置の状態は、正面パネルの LED で示されます。

- 右側の 4 つの LED は電源装置の状態、診断モード、およびスタックモードを以下のように示します。

LED	色	動作	定義
PWR	緑色	点灯	電源装置は動作可能です。
	橙色	点灯	電源装置の故障です。
RPS	緑色	点灯	冗長電源装置は動作可能です。
	橙色	点灯	冗長電源装置は故障しています。
	消灯	消灯	冗長電源装置がありません。
Diag	緑色	点滅	システムは診断モードです。

Stack	緑色	点灯	スタッキングは正常に完了しました。
	消灯	消灯	スタンドアロンです。

電源 LED、診断 LED、およびスタック LED

スタッキング LED

スタッキング LED は、スタックでのユニットの位置を示します。この項の最初の正面パネルの図で示したように、スタッキング LED には 1 ～ 6 の数字が割り当てられています。スタック内の各ユニットは、スタッキング LED のうちの 1 つを点灯させ、スタック内での位置を示します。スタッキング LED 1 が点灯している場合、そのユニットはマスターユニットです。2 ～ 6 のスタッキング LED のうちの 1 つが点灯している場合、そのユニットは対応するスタッキングメンバーのユニットです。

メモ、注意および警告

メモ、注意および警告

PowerConnect 3324 / 3348 スイッチの設置

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

設置に関する注意事項

警告：スイッチのラックまたはキャビネットへの設置は、ラックやキャビネットが倒れたり不安定にならないようにしっかりとおこなってください。

警告：電源回路が適切にアースされているか確認してください。

警告：使用上の注意マークを守ってください。デルのシステムマニュアルに記載されている以外の製品には触れないでください。稲妻が描かれた三角形の記号の付いたカバーを開いたり取り外すと、感電の危険があります。これらのコンポーネントについては、訓練を受けたサービス技術者以外は修理をおこなうことができません。

警告：電源ケーブル、延長ケーブル、または電源プラグが破損していないか確認してください。

警告：製品が濡れていないか確認してください。

警告：異物をデバイスに押し込まないでください。 火事や感電の原因になることがあります。

警告：製品の温度が下がってから、カバーを取り外したり、内部装置に触れてください。

警告：スイッチが電源回路、配線、および過剰な電流からの保護を過負荷にしないか確認してください。供給回路の過負荷の可能性を調べるには、スイッチと同じ回路に取り付けられているすべてのスイッチのアンペアを加算します。この合計値を回路の定格限度と比較します。最大アンペア定格は、通常、AC 電源コネクタの近くのスイッチに印刷されています。

注意： デバイスが暖房器具や熱源の近くにないか確認してください。

注意： 冷却孔が塞がれていないか確認してください。

注意： 製品に接続して使用できるのは承認を受けた装置のみです。

注意： 動作時の周囲温度が 40 °C を超える環境ではスイッチを取り付けないでください。

注意： スイッチの前面、側面、および背面の空気の流れが妨げられないようにしてください。

設置要件

Dell™ PowerConnect™ 3324/3348 シリーズは、標準の 19 インチラックまたはテーブルの上に取り付けることができます。ユニットを設置する前に、設置する場所が以下の取り付け要件を満たしているか確認します。

- 一般要件 — 電源装置が正しく取り付けられているか確認します。
- 電源要件 — ユニットがアースされた簡単にアクセスできる 100 ～ 250 VAC、50 ～ 60Hz のコンセントから 1.5 m 以内にあるか確認します。たとえば、UPS とフェーズされた電源のように、2 つの個別の電源装置を使用することをお勧めします。
- クリアランス要件 — オペレーターが作業できるように正面に空間があるか確認します。ケーブル配線、電源接続、および換気用の空間を確保します。
- ケーブル配線要件 — ケーブルは、無線機、通信用の増幅器、電線、および蛍光灯取り付け器具のような電気的なノイズを避けて配線します。
- 環境要件 — 動作時の周囲温度の許容範囲は、結露のない相対湿度 95 % の環境で 0 ～ 40 °C です。ユニットのケースに水や水分が入らないようにし

ます。

開梱および設置

パッケージの内容

PowerConnect 3324/3348 を開梱しながら、以下の部品があるか確認します。

- PowerConnect 3324/3348 デバイス
- AC 電源ケーブル
- ヌルモデムケーブル
- 粘着ゴムパッド
- ラック設置用ラック取り付けキット
- マニュアル CD

開梱

メモ: PowerConnect 3324/3348 スイッチを開梱する前に梱包を調べて、損傷がある場合は、すぐにご連絡ください。

1. ESD リストストラップを身に付け、ESD クリップを金属面に取り付けて、身体から静電気を逃がします。
2. スイッチの入っている箱を整頓された平らな面に置き、箱をしっかり締めているすべてのストラップを切ります。
3. 箱を開けるか、箱の上部を取り外します。
4. ユニットを箱から慎重に取り出し、安全で整頓された場所に置きます。
5. すべての梱包材を取り外します。
6. 製品に損傷がないか調べます。損傷がある場合は、すぐにご連絡ください。
   デルへのお問い合わせ先については、「困ったときは」を参照してください。

デバイスのラックへの設置

警告: PowerConnect 3324/3348 スイッチをラックまたはキャビネットに設置する前に、すべてのケーブルをユニットから取り外してください。

PowerConnect 3324/3348 を設置するには、次の手順を実行します。

1. ESD リストストラップを身に付け、ESD クリップを金属面に取り付けて、身体から静電気を逃がします。
2. PowerConnect 3324/3348 スイッチを平らで安定した面に置きます。
3. 付属のラック取り付けブラケットを PowerConnect 3324/3348 の片方の側面に取り付けます。ラック取り付けブラケットの取り付け穴と PowerConnect 3324/3348 の取り付け穴が揃っているか確認します。
4. 付属のネジをラック取り付け穴に挿入して、プラスドライバでネジを締めます。
5. PowerConnect 3324/3348 のもう片方の側面で、ラック取り付けブラケットの取り付け手順を繰り返します。
6. ユニットを 19 インチラックに挿入して、ユニットをラックネジでラックに固定します（ラックネジは同梱されていません）。ラックに固定する際、先に下側のネジを締めてから上側のネジを締め、スイッチ本体の加重が均等にかかるようにします。通気孔がふさがれていないことを確認します。

ラックを使用しない場合のスイッチの設置

ラックに設置しない場合、PowerConnect 3324/3348 は平らな面に設置する必要があります。設置する面は、デバイスとデバイスケーブルの重量に耐えることが

できる必要があります。

1. 正面と側面に約 5 cm、背面に約 13 cm の空間をとって、PowerConnect 3324/3348 を平らな面に設置します。
2. デバイスに適切な換気があるか確認します。
3. デバイスが滑らないようにゴム製の脚をデバイスの底面に取り付けます。

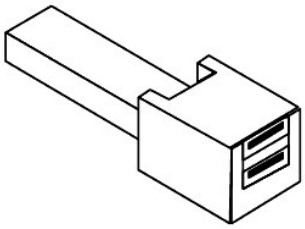
PowerConnect 3324/3348 のスタッキング

PowerConnect 3324/3348 は、最大 6 個までの PowerConnect 3324/3348 デバイスまたは 192 個までの Fast Ethernet ポートと 6 個の Giga ポートに対応しています。各 PowerConnect 3324/3348 スタックは、1 つのマスターユニットを含み、残りのすべてのユニットはスタックメンバーとしてみなされます。すべての管理はマスタユニットで行います。スタックには、24 ポートと 48 ポートの両方のデバイスを組み込むことができます。

スタッキングを有効にするには、ユニットを SFP スロットのポート G2 に接続されたスタックモジュールでスタックする必要があります。

スタッキングケーブルの接続

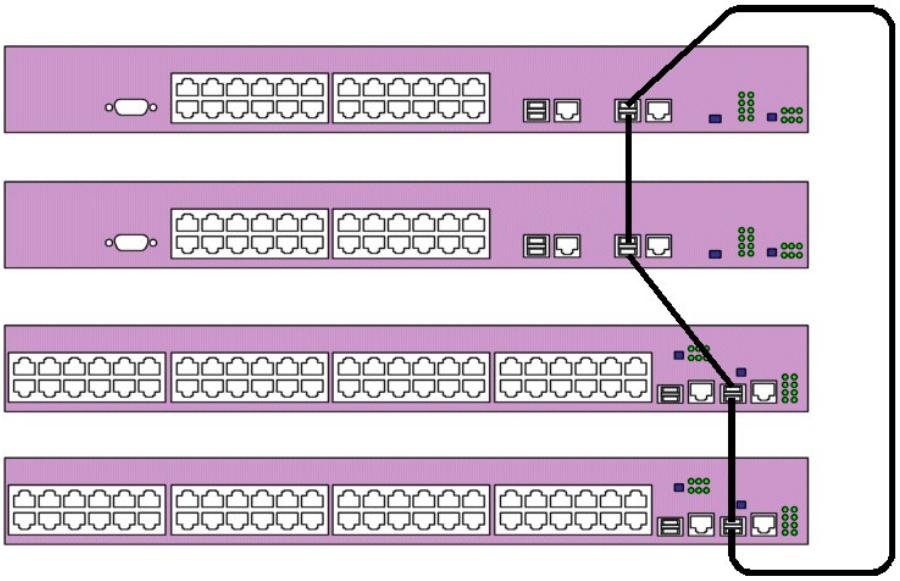
1. 各デバイスをラックまたは平らな面に設置します。
2. 各 G2 ポートにスタッキングコネクタを挿入します。



USB コネクタ

3. マスターユニットの下部の RX スタッキングコネクタを、選択したメンバーの上部の TX ポートに接続します。
4. 下部の RX コネクタから上部の TX コネクタにスタッキングケーブルを接続するスタッキングのリングトポロジでスタックを接続します。
5. 上部および下部のスタックメンバーがスタッキングケーブルで接続されているか確認します。下の図で正しく接続されたスタックを示します。

メモ: スタッキングのリングが完了していない場合、スタックは機能しません。



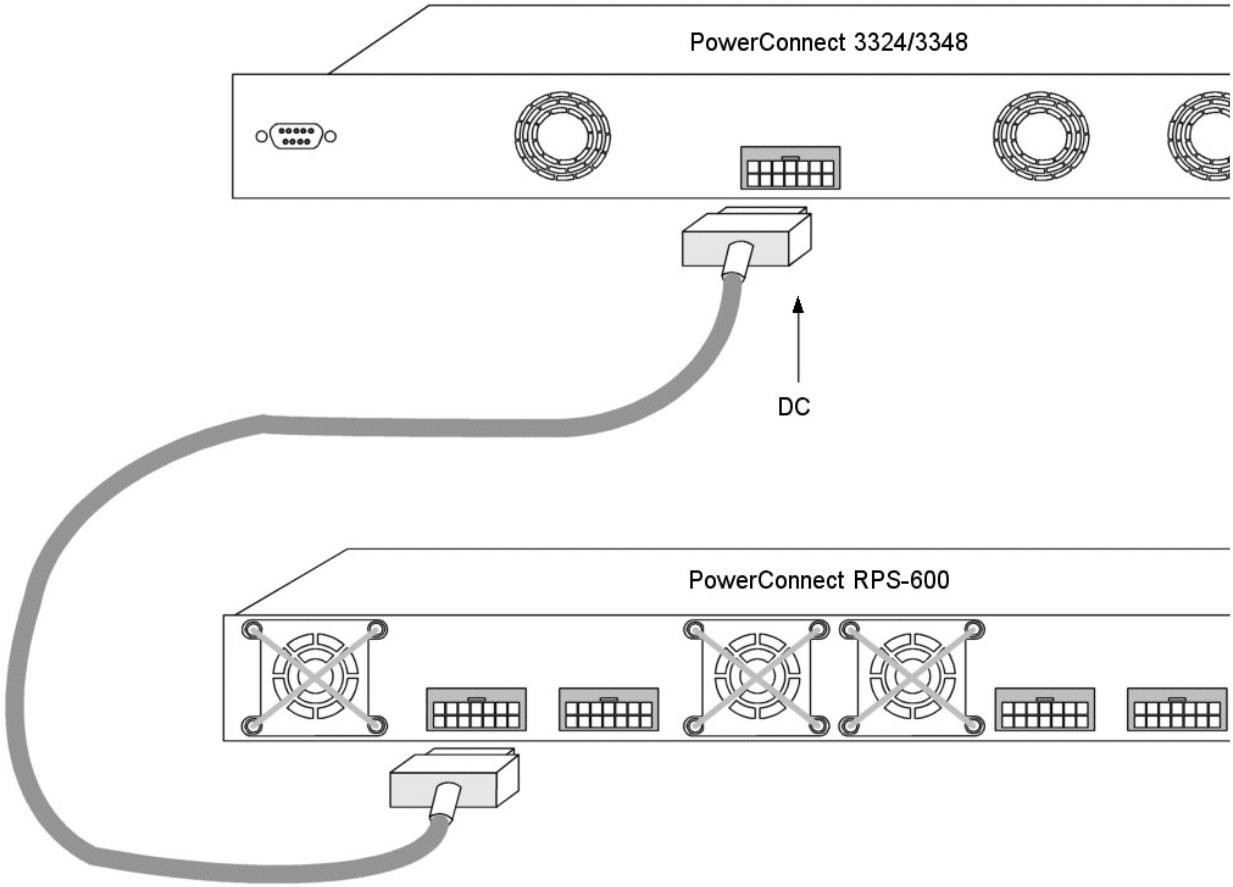
接続されたスタック

スタックの設定の詳細については、「 スタッキングの設定」を参照してください。

PowerConnect 3324/3348 の電源装置への接続

以下の項では、PowerConnect 3324/3348 の AC 電源への接続手順について説明します。PowerConnect 3324/3348 には、以下の電源から電力を供給することができます。

- AC 電源装置
- オプションの PowerConnect RPS-600 冗長電源装置
- AC および DC 電源



PowerConnect 3324/3348 の電源装置への接続

- PowerConnect 3324/3348 を前述した電源のうちの 1 つに接続します。

AC 電源接続

AC 電力は、安全にアースされた 1.5 m の標準ケーブルでユニットに供給します。

PowerConnect 3324/3348 を電源に接続するには、次の手順を実行します。

1. 電源ケーブルを背面パネルの AC メインソケットに接続します。冗長電源モジュールがある場合、冗長電源モジュールケーブルを別の電源装置に接続します。
2. 電源ケーブルをアースされている電源コンセントに接続します。
3. デバイスが接続され正しく動作するか正面パネルの LED を調べて確認します。
ドライバの詳細については、「LED の定義」を参照してください。

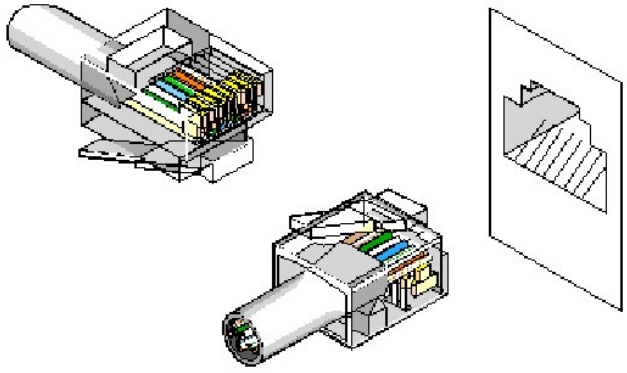
ケーブル、ポート、およびピンの割り当てについて

この項では、PowerConnect 3324/3348 の物理的なインタフェースについて説明し、ケーブル接続についての情報を提供します。ステーションは、正面パネルの物理的なインタフェースポートを介して PowerConnect 3324/3348 に接続されます。各ステーションで、適切なモード（半 / 全二重、オート）が設定されています。

ポート接続

ポートはすべて標準の RJ45 Ethernet ポートです。スイッチングポートは、ストレートケーブルを使用して、標準の RJ45 Ethernet ステーションモードでステーションに接続できます。送信デバイスは、クロスケーブルを使用してお互いに接続します。

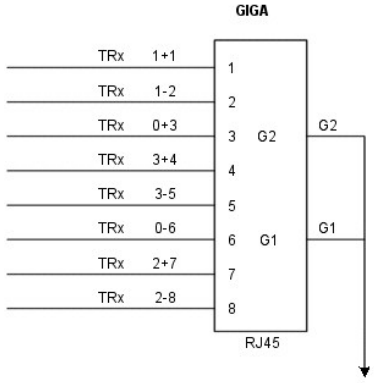
以下の図に、10/100M ポートの RJ45 ピン番号の割り当てを示します。



RJ45 ピン番号の割り当て

ピン	使用
1	RX +
2	RX -
3	TX +
4	
5	- -
6	TX -
7	-
8	-

以下の図に、Gigaport コネクタを示します。

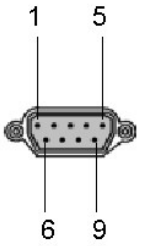


Gigaport コネクタ

PowerConnect 3324/3348 の初期設定では、シリアルケーブルを使用して PowerConnect 3324/3348 をターミナルに接続します。(ターミナルエミュレーションソ

フトウェアを使用している PC を使用することもできます。)シリアルケーブルは、両端がメスの DB-9 クロスオーバケーブルです。

以下の図に、DB-9 コネクタを示します。



DB-9 シリアルケーブル

ピン	使用
1	未使用
2	TXD
3	RXD
4	未使用
5	GND
6	未使用
7	CTS
8	RTS
9	未使用

DB-9 ピン番号の割り当て

ケーブル接続

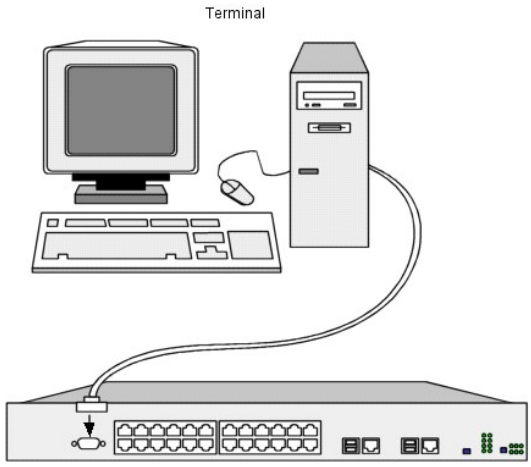
この項では、様々なケーブルを使用して PowerConnect 3324/3348 デバイスを接続する方法について説明します。

ASCII ターミナル（シリアル）接続

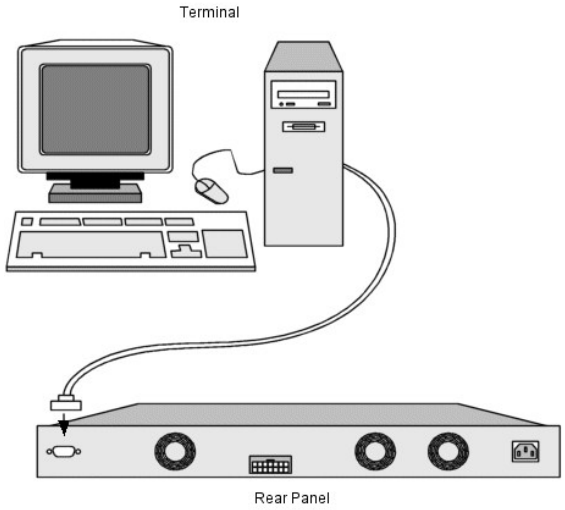
シリアルポートコネクタは、DB-9 型のコネクタです。付属のインタフェースケーブルはデバイスを接続するのに必要です。

デバイスを接続するには、次の手順を実行します。

1. インタフェースクロスケーブルをターミナル ASCII DTE RS-232 接続に接続します。
2. インタフェースクロスケーブルをデバイスのシリアル接続に接続します。



PowerConnect 3324 ターミナル接続



PowerConnect 3348 ターミナル接続

メモ、注意および警告

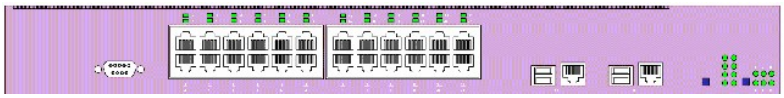
メモ、注意および警告

概要

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

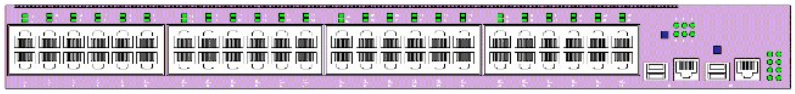
システムについて

Dell™ PowerConnect™ 3324 および 3348 デバイスは、スタンドアロンおよびスタック可能なアドバンス Layer 2 スイッチです。PowerConnect 3324 および PowerConnect 3348 は、スタンドアロンの Layer 2 スイッチシステムとしても機能します。PowerConnect 3324/3348 デバイスは、In-Band Management（ネットワークステーションを介してリモートで）またはコンソールを介して管理することができます。



PowerConnect 3324

スタックメンバーとして動作している場合、各 PowerConnect 3324 ユニットは、24 個の 10 BaseT/100BaseTX Fast Ethernet ポート、1 個の Gigabit Ethernet コンボポート（10/100/1000 BaseT またはミニ GBIC コネクタ）、および 1 個の Giga Ethernet スタッキングポートを提供します。



PowerConnect 3348

スタックメンバーとして動作している場合、各 PowerConnect 3348 ユニットは、48個の 10 BaseT/100BaseTX Fast Ethernet ポート、1 個の Gigabit Ethernet コンボポート（10/100/1000 BaseT またはミニ GBIC コネクタ）、および 1 個の Giga Ethernet スタッキングポートを提供します。

スタンドアロンユニットとして動作している場合、PowerConnect 3324/3348 スタッキングポートは、Giga Ethernet ポートとして使用できます。

PowerConnect 3324/3348 スタッキングの概要

PowerConnect 3324/3348 スタッキングは、複数のデバイス管理を提供して、すべてのスタックメンバーを単一のユニットのように一ヶ所から管理できます。すべてのメンバーには、SNMP 管理用の 1 つの IP アドレスおよびスタック全体を管理するコンソール / Telnet セッションを介してアクセスすることができます。

PowerConnect 3324/3348 は、各スタックで最大 6 個までのスタッキングまたは 192個の FE および 6 個の Gigabit Ethernet ポートに対応しています。PowerConnect 3324/3348 はスタンドアロンユニットとして動作することもできます。

スタッキングのセットアップ中に、1 つのデバイスがネットワーク管理者によってスタックマスターとして選択されると、残りのすべてのデバイスはスタックメンバーとして選択され、一意の Unit ID が割り当てられます。

PowerConnect 3324/3348 のスタックは、スタックにわたる以下の Layer 2 機能を提供します。

- Switching（スイッチング）
- Trunking（トランキング）
- Port Mirroring（ポートのミラリング）
- VLAN

たとえば、VLAN は異なるスタックメンバーに属するポートから設定することができ、2 つめのスタックメンバーから 3 つめのスタックメンバーにポートのミラリングを設定することもできます。スタッキング構成で動作しているアプリケーションは中央化されます。たとえば、スタック全体の Spanning Tree Protocol はマスターユニットで動作します。デバイスソフトウェアは、各スタックメンバーに個別にダウンロードされます。

PowerConnect 3324/3348 のスタッキングアーキテクチャは、スタッキングトポロジの動的学習を提供し、以下のイベントの際に影響を最小に抑えるため、ポートの検出および再設定を提供します。

- Unit Failure（ユニット障害）
- Inter-unit Link Loss（ユニット間のリンクの喪失）
- Unit Insertion（ユニットの挿入）
- Removal of a Stacking Unit（スタッキングユニットの削除）

スタックメンバーおよび Unit ID

スタッキングの動作モードは Boot プロセス中に決定されます。

PowerConnect 3324/3348 ユニットは、デフォルトの Unit ID 1 が設定されている状態で出荷されています。Unit ID はスタッキング構成には必要です。スタックメンバーがスタッキングモジュールなしで再起動すると、デバイスはデバイスがリセットされるまでスタンドアロンユニットとして動作します。PowerConnect 3324/3348 ユニットがスタンドアロンユニットとして動作している場合、すべてのスタッキング LED はオフになります。ユニットがスタックに再度接続されると、Unit ID は消去されず有効なまま残ります。

メモ: スタックが動作するには、スタッキングモジュールをポート G2 に挿入する必要があります。スタッキングモジュールがポート G1 に挿入されている場合、コンソールに警告メッセージが表示されます。

マスターユニットが起動する際、またはスタックメンバーを挿入または削除する際に、マスターユニットはスタッキング検出手順を開始します。2 つのメンバーが同じ Unit ID で検出された場合、またはマスターユニットが検出されなかった場合、スタック全体が機能しません。スタッキング LED は赤色のままです。

設定方法

PowerConnect 3324/3348 が動作可能なスタックでは、スタックはスタックマスターによって設定されます。各スタックメンバーには個別の Configuration ファイルがありません。スタックの各ポートは、Configuration コマンドおよび Configuration ファイルの一部である特定の Unit ID / ポートタイプおよびポート番号を持ちます。Configuration ファイルは、PowerConnect 3324/3348 のスタックマスターからのみ管理することができ、以下の項目を含みます。

- フラッシュへの保存
- 外部の TFTP サーバーへの Configuration ファイルのアップロード
- 外部の TFTP サーバーからの Configuration ファイルのダウンロード

メモ: スタックがリセットされた場合、またはあるポートが存在しなくなった場合でも、すべての設定されているポートのスタック設定は保存されます。

Configuration ファイルは、ユーザーが設定を変更した場合のみ変更されます。また、Configuration ファイルは以下の場合では、自動的に変更されません。

- ユニットが追加された場合
- ユニットが削除された場合

- ユニットに Unit ID を再割り当てした場合
- ユニットがスタッキングモードとスタンドアロンモードで交互に切り替わる場合

システムが再起動するたびに、保存されている設定は Startup Configuration ファイルに書き込まれます。

PowerConnect 3324/3348 スタックメンバーがスタックから削除されて、同じ Unit ID で置き換えられた場合、スタックメンバーは元のデバイス設定で設定されます。

物理的に存在するポートのみが Dell OpenManage™ Switch Administrator で表示され、ウェブ管理システムから設定できます。存在しないポートは CLI または SNMP インタフェースから設定します。

スタックの再構成

スタッキングの順番はスタックメンバーを削除するか、またはスタッキングケーブルを再接続することにより変更することができます。スタックメンバーの構成の順番は、スタックメンバーの物理的な順番ではなく Unit ID の割り当てにより確立されます。スタック構成は、スタックの順番が変更されてスタックがリセットされた後に、スタックマスターに保存されます。

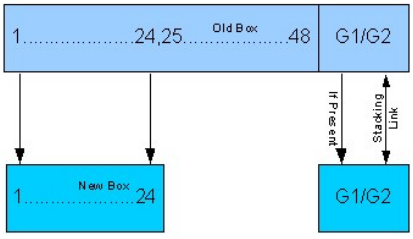
PowerConnect 3324/3348 ユニットがスタックから削除、またはスタックで交換された場合、以下のように接続を回復します。

- スタックが 2 分以上取り外された場合、スタック全体がネットワークトラフィックを転送しません。すべてのスタックメンバーが再起動し、スタックが再度接続されるまで待ちます。ユニットが交換されない場合、マスターユニットは常にスタックをポールします。
- 2 分以内にスタックが再度接続された場合、すべてのユニットはスタックされたままで、5 秒以内に他のユニットへの接続を回復します。新しいスタックメンバーはマスターユニットに接続されますが、マスターユニットの設定によって初期化されます。設定が保存されていない場合、デバイスはデフォルト設定で設定されます。

スタックメンバーの交換

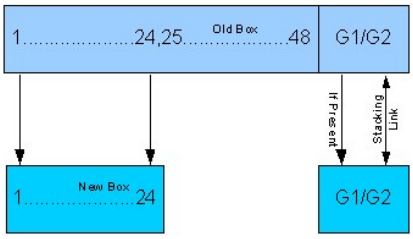
スタックメンバーを新しいデバイスと交換すると、要求されたデバイス ID が選択されます。また、以前のデバイス設定は挿入されたスタックメンバーに適用されます。新しく挿入されたデバイスが以前のデバイスより多くのまたは少ないポートを持っている場合、該当するポート設定が新しいスタックメンバーに適用されます。例えば、以下のように作成します。

- ある PowerConnect 3324 を別の PowerConnect 3324 と交換する場合、新しい 24 個の 10/100 BaseT ポートは、以前の 24 個の 10/100 BaseT ポート設定を受け取ります。ポート G1 および G2 は、以前のデバイスの G1 および G2 ポート設定を受け取ります。
- PowerConnect 3348 を PowerConnect 3324 と交換する場合、ポート 1 ～ 24 の 10/100 BaseT は以前のデバイスのポート 1 ～ 24 の設定を受け取ります。ポート G1 およびポート G2 は、以前のデバイスの G1 および G2 ポート設定を受け取ります。



PowerConnect 3348 を PowerConnect 3324 と交換する場合

- ある PowerConnect 3348 を別の PowerConnect 3348 と交換する場合、新しい 48 個の 10/100 BaseT ポートは、以前の 48 個の 10/100 BaseT ポート設定を受け取ります。ポート G1 および G2 は、以前のデバイスの G1 および G2 ポート設定を受け取ります。
- PowerConnect 3324 を PowerConnect 3348 と交換する場合、ポート 1 ～ 24 の 10/100 BaseT は、以前のデバイスのポート 1 ～ 24 の設定を受け取ります。
- ポート 25 ～ 48 は、デフォルトのポート設定を受け取ります。ポート G1 および G2 は、以前のデバイスの G1 および G2 ポート設定を受け取ります。



PowerConnect 3324 を PowerConnect 3348 と交換する場合

PowerConnect ユーザーガイドの概要

PowerConnect ユーザーガイドは、以下の 2 つのパートに分かれています。

- PowerConnect 3324/3348 スイッチの設置について
- OpenManage Switch Administrator の使い方

PowerConnect 3324/3348 スイッチの設置

この項には、PowerConnect 3324/3348 の開梱、設置、および設定についての以下の項目が含まれています。

- ハードウェアについて — ポートおよび LED タイプについての説明を含む、PowerConnect 3324/3348 ハードウェアの情報について説明しています。
- PowerConnect 3324/3348 スイッチの設置 — ラックまたは平らな面への PowerConnect 3324/3348 の設置手順について説明します。また、この項では設置に関する注意事項およびコネクタやケーブルについても説明しています。
- PowerConnect 3324/3348 スイッチの設定 — デバイスソフトウェアのダウンロードを含むデバイスの初期設定、デバイスの起動画面、およびオプションの設定機能について説明しています。

OpenManage Switch Administrator の使い方

この項には、ウェブ管理システムおよび CLI（コマンドラインインタフェース）デバイス管理システムを使用したデバイスの設定に関する以下の情報が含まれています。

- はじめにお読みください — 管理および情報アイコンの説明を含むウェブ管理システムインタフェースの始め方、Component List、および Device View と Tree View についての情報が含まれています。
- システム情報の設定 — システム情報の定義、デフォルト IP アドレスの設定、デバイスセキュリティおよび SNMP コミュニティの定義、デバイスソフトウェアのダウンロード、および詳細設定の定義についての情報が含まれています。
- スイッチ情報の設定 — ポートおよび VLAN の設定、静的および動的アドレステーブルの定義、GARP および GVRP の設定、Spanning Tree パラメータの定義、集合ポート、およびマルチキャスト転送サポートの設定についての情報が含まれています。
- Statistics（統計）の表示 — ポート、GVRP、Etherlike、RMON、およびインタフェース統計のテーブルおよびチャート統計表示についての情報が含まれています。
- Quality of Service（サービスのクオリティ）の設定 — デバイスの Class of Service（サービスのクラス）設定についての情報が含まれています。
- 困ったときは — テクニカルサポート、ご注文に関する問題、修理もしくは返品についてなど、デルへのお問い合わせについての情報が含まれています。

PowerConnect 3324/3348 CLI のマニュアル

『PowerConnect 3324/3348 ユーザーズガイド』に加えて、デルでは『PowerConnect 3324/3348 CLI リファレンスガイド』も提供しています。『PowerConnect 3324/3348 CLI リファレンスガイド』では、PowerConnect 3324/3348 の設定に使用する CLI コマンドについての情報を提供しています。

メモ、注意および警告

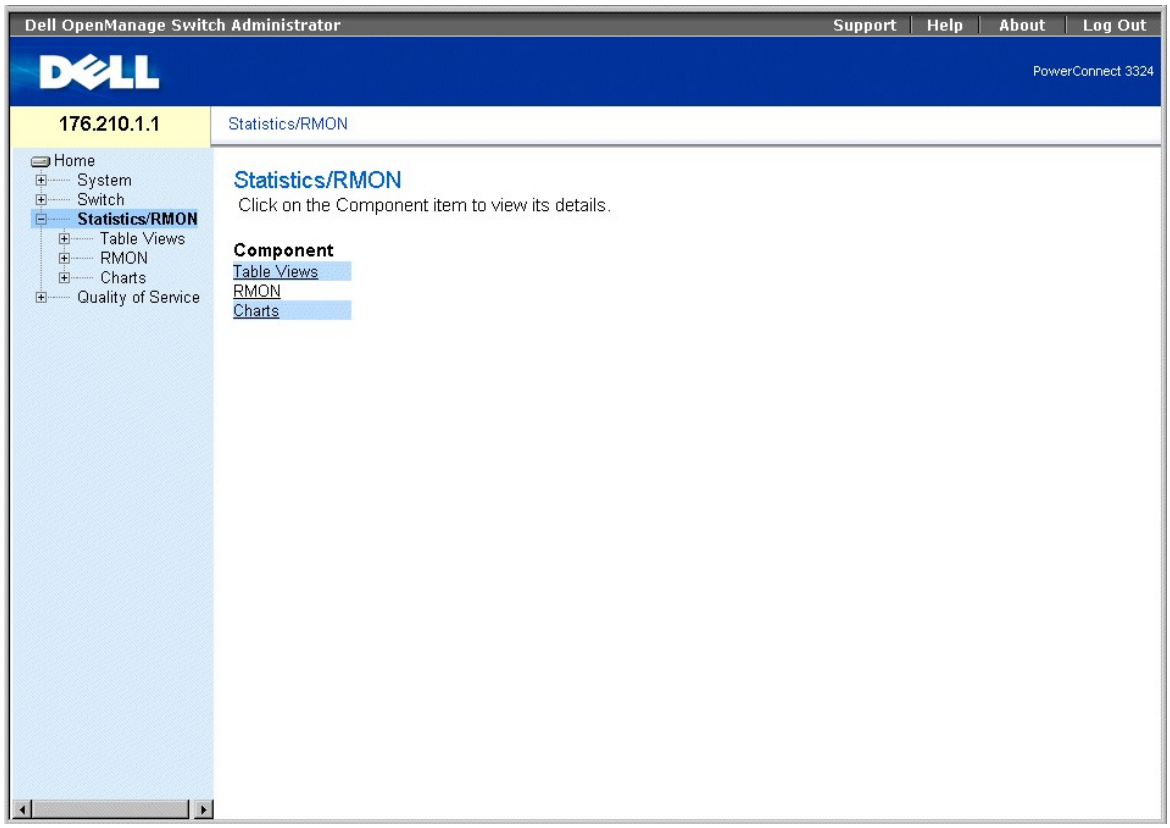
メモ、注意および警告

Statistics （統計） の表示

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

Statistic ページには、インタフェース、GVRP、Etherlike、RMON、およびデバイスの利用に関するデバイスの情報が含まれています。
Statistics / RMON ページを開くには、次の手順を実行します。

1. Tree View で、**Statistics / RMON** をクリックします。
   Statistics / RMON ページが開きます。



Statistics / RMON ページ

この項には、以下のトピックがあります。

- テーブルの表示
- RMON 情報の表示
- チャートの表示

テーブルの表示

Table Views ページには、表形式で統計を表示するためのリンクがあります。**TableViews** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON** → **Table Views** とクリックします。**TableViews** ページが開きます。

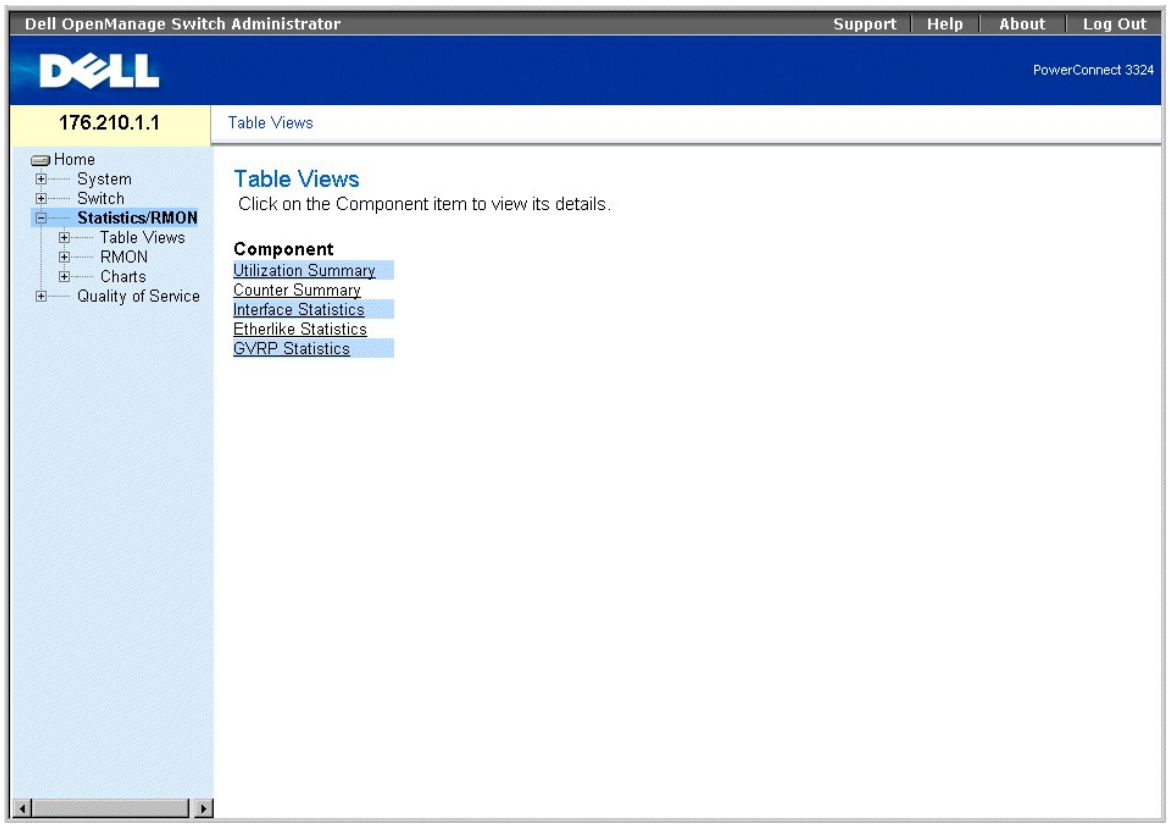


Table Views ページ

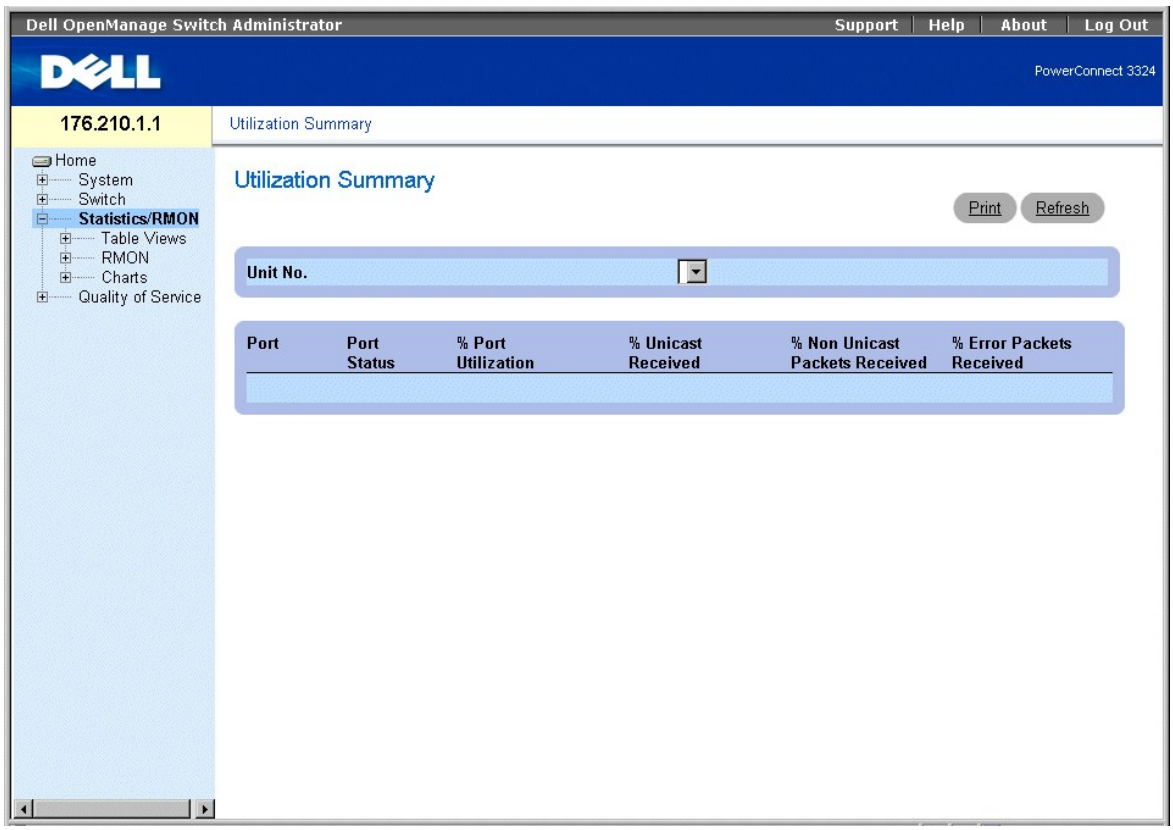
Table Views ページには、以下のリンクがあります。

- 利用率の要約の表示
- カウンタの要約の表示
- インタフェース統計の表示
- Etherlike 統計の表示
- GVRP 統計の表示

利用率の要約の表示

Utilization Summary ページには、ポートの利用率の統計が含まれています。**Utilization Summary** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON** → **Table Views** → **Utilization Summary** とクリックします。**Utilization Summary** ページが開きます。



Utilization Summary ページ

Utilization Summary ページには、以下のフィールドが含まれています。

- **Unit No.** — ポート統計が表示されるユニットの番号を示します。
- **Port** — ポート番号を指定します。
- **Port Status** — ポートの状態を示します。
- **% Port Utilization** — ポートの利用率を示します。
- **% Unicast Received** — ポートで受信されたユニキャストパケットの割合を示します。
- **% Non Unicast Packets** — ポートで受信された不良パケットの数を示します。
- **% Error Packets Received** — ポートで受信されたエラーのあるパケットの数を示します。

利用率の統計を表示するには、次の手順を実行します。

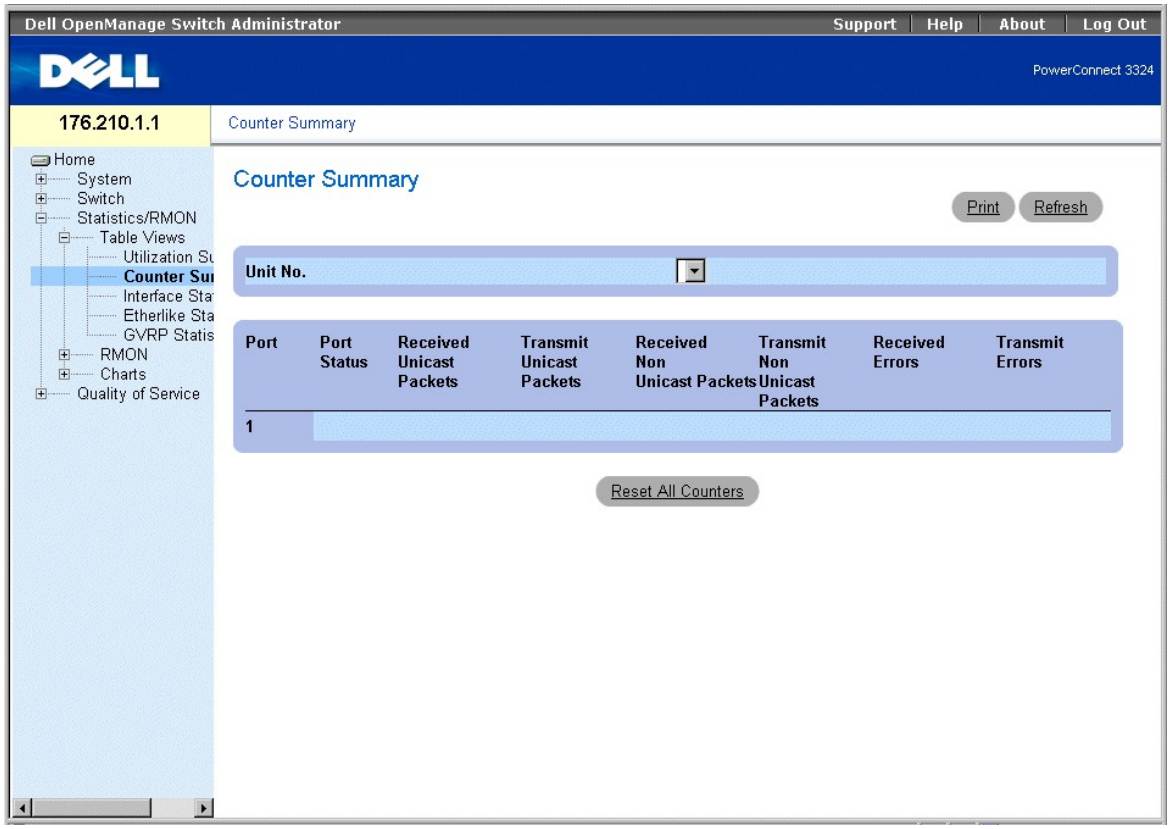
1. **Utilization Summary** ページを開きます。
2. **Unit** フィールドで、ユニットを選びます。利用率の統計は、選択されたユニットを表示します。

カウンタの要約の表示

Counter Summary ページには、ポートの利用率をパーセントではなく数値で表示する統計が含まれています。**Counter Summary** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON → Table Views → Counter Summary**

とクリックします。**Counter Summary** ページが開きます。



Counter Summary ページ

Counter Summary ページには、以下のフィールドが含まれています。

- **Unit No.** — ポート統計が表示されるユニットの番号を示します。
- **Port** — ポート番号を指定します。
- **Port Status** — ポートの状態を示します。
- **Received Unicast Packets** — ポートで受信されたユニキャストパケットの数を示します。
- **Transmit Unicast Packets** — ポートから送信されたユニキャストパケットの数を示します。
- **Received Non Unicast Packets** — ポートで受信された非ユニキャストパケットの数を示します。
- **Transmit Non Unicast Packets** — ポートから送信された非ユニキャストパケットの数を示します。
- **Received Errors** — ポートで受信されたエラーの数を示します。
- **Transmit Errors** — ポートから送信されたエラーの数を示します。

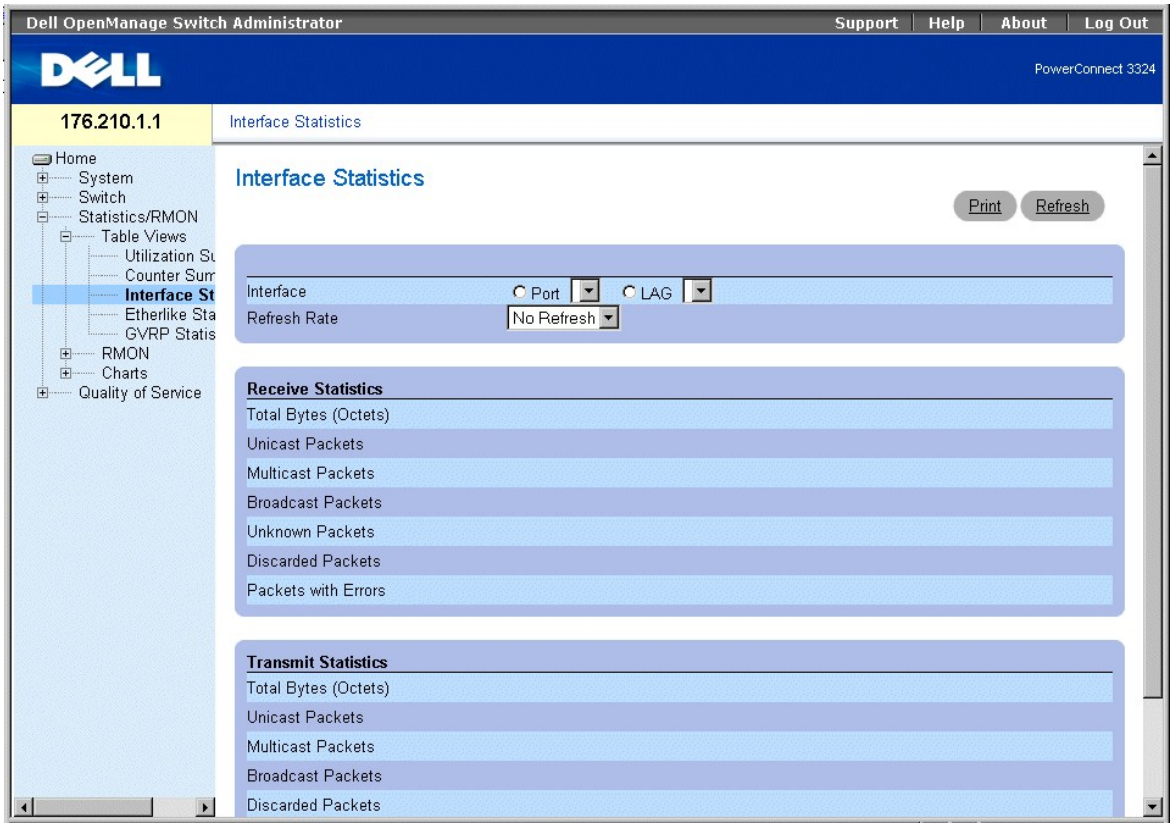
カウンタの要約の統計を表示するには、次の手順を実行します。

1. **Counter Summary** ページを開きます。
2. **Unit** フィールドで、ユニットを選びます。選択されたユニットのカウンタの要約の統計を表示します。

インタフェース統計の表示

Interface Statistics ページには、インタフェース統計が含まれています。 **Interface Statistics** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON** → **Table Views** → **Interface Statistics** とクリックします。 **Interface Statistics** ページが開きます。



Interface Statistics ページ

Interface Statistics ページには、以下のフィールドが含まれています。

- **Interface** — 統計が表示されるインタフェース （タイプおよび番号） を指定します。
  - **Port** — ポートの統計が表示されていることを示します。
  - **LAG** — LAG の統計が表示されていることを示します。
- **Refresh Rate** — インタフェース統計が更新される間隔を示します。可能なフィールド値には、以下のものがあります。
  - **15 Sec** — インタフェース統計が 15 秒毎に更新されることを示します。
  - **30 Sec** — インタフェース統計が 30 秒毎に更新されることを示します。
  - **60 Sec** — インタフェース統計が 60 秒毎に更新されることを示します。
  - **No Refresh** — インタフェース統計が自動的に更新されないことを示します。
- **Total Bytes (Octets) Received** — 選択されたインタフェースで受信されたバイトの量を表示します。
- **Received Unicast Packets** — 選択されたインタフェースで受信されたユニキャストパケットの量を表示します。
- **Received Multicast Packets** — 選択されたインタフェースで受信されたマルチキャストパケットの量を表示します。
- **Received Broadcast Packets** — 選択されたインタフェースで受信されたブロードキャストパケットの量を表示します。
- **Received Unknown Packets** — 選択されたインタフェースで受信された不明パケットの量を表示します。

- **Received Discarded Packets** — 選択されたインタフェースで受信中に破棄されたパケットの量を表示します。
- **Received Packets with Errors** — 選択されたインタフェースで受信されたエラーのあるパケットの量を表示します。
- **Total Bytes (Octets) Transmitted** — 選択されたインタフェースから送信されたバイト数を表示します。
- **Transmitted Unicast Packets** — 選択されたインタフェースから送信されたユニキャストパケットの量を表示します。
- **Transmitted Multicast Packets** — 選択されたインタフェースから送信されたマルチキャストパケットの量を表示します。
- **Transmitted Broadcast Packets** — 選択されたインタフェースから送信されたブロードキャストパケットの量を表示します。
- **Transmitted Unknown Packets** — 選択されたインタフェースから送信された不明パケットの量を表示します。
- **Transmitted Discarded Packets** — 選択されたインタフェースで送信中に破棄されたパケットの量を表示します。
- **Transmitted Packets with Errors** — 選択されたインタフェースから送信中にエラーがあると識別されたパケットの量を表示します。

ポートのインタフェース統計を表示するには、次の手順を実行します。

1. **Interface Statistics** ページを開きます。
2. **Interface** フィールドで、**Port** を選びます。
3. **Reset All Counters** をクリックします。ポートのインタフェース統計が表示されます。

LAG の Interface Statistics を表示するには、次の手順を実行します。

1. **Interface Statistics** ページを開きます。
2. **Interface** フィールドで、**LAG** を選びます。
3. **Reset All Counters** をクリックします。LAG のインタフェース統計が表示されます。

CLI コマンドを使用したインタフェース統計の表示

この項では、インタフェース統計を表示する CLI コマンドについて説明します。

CLI コマンド	説明
show interfaces counters [ethernet interface | port-channel port-channel-number]	物理的なインタフェースで検出されたトラフィックを表示します。

以下に、CLI コマンドの例を示します。

```
console# show interfaces counters ethernet 1/e1

Port InOctets InUcastPkts InMcastPkts InBcastPkts

---- ---------- ----------- ----------- -----------
```

1/e1 1717 0 326 26

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1/e1 21845 0 326 26

Alignment Errors: 0

FCS Errors: 0

Single Collision Frames: 0

Multiple Collision Frames: 0

Deferred Transmissions: 0

Late Collisions: 0

Excessive Collisions: 0

Internal MAC Tx Errors: 0

Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Symbol Errors: 0

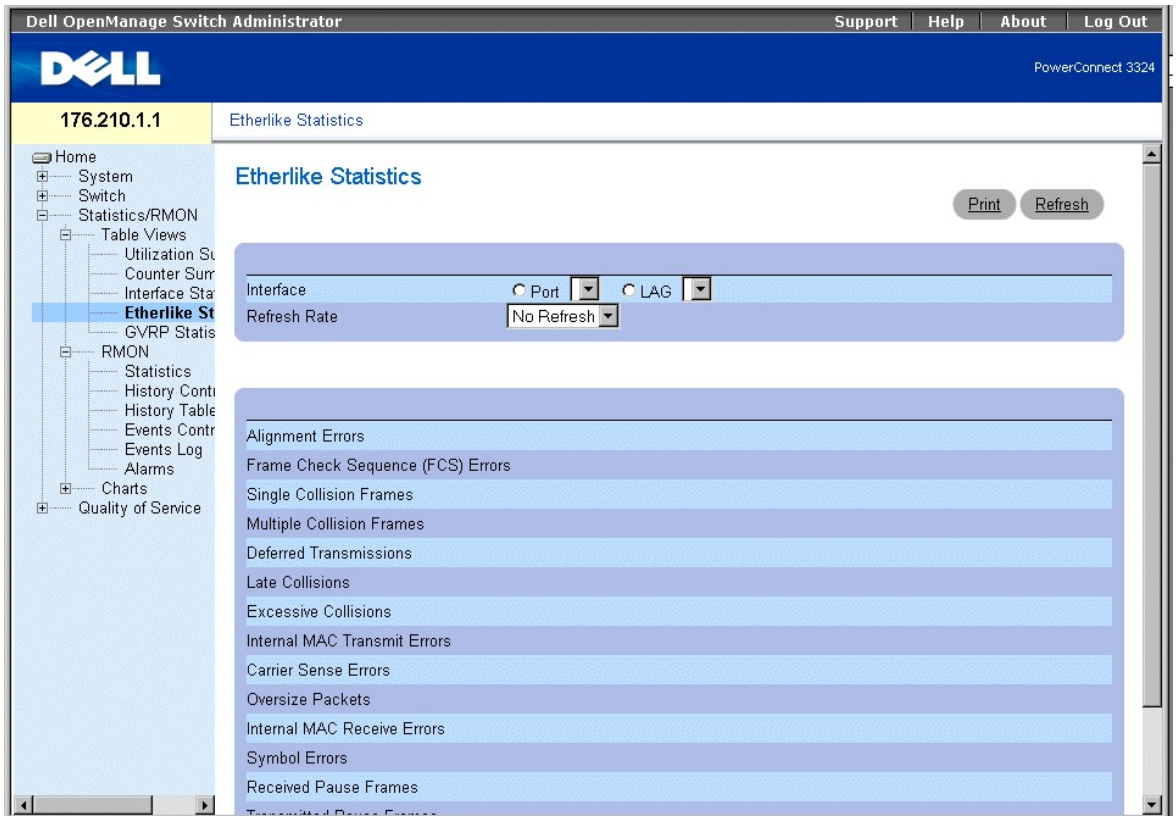
Received Pause Frames: 0

Transmitted Pause Frames: 0

Etherlike 統計の表示

Etherlike Statistics ページには、インタフェース統計が含まれています。**Etherlike Statistics** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON → Table Views → Etherlike Statistics** とクリックします。**Etherlike Statistics** ページが開きます。



Etherlike Statistics ページ

Etherlike Statistics ページには、以下のフィールドが含まれています。

- **Interface** — 統計を表示するインタフェースタイプを指定します。
  - **Port** — ポートの統計が表示されていることを示します。
  - **LAG** — LAG の統計が表示されていることを示します。
- **Refresh Rate** — インタフェース統計が更新される間隔を示します。可能なフィールド値には、以下のものがあります。
  - **15 Sec** — インタフェース統計が 15 秒毎に更新されることを示します。
  - **30 Sec** — インタフェース統計が 30 秒毎に更新されることを示します。
  - **60 Sec** — インタフェース統計が 60 秒毎に更新されることを示します。
  - **No Refresh** — インタフェース統計が自動的に更新されないことを示します。
- **Alignment Errors** — 選択されたインタフェースで受信された Alignment エラーの量を表示します。
- **Frame Check Sequence (FCS) Errors** — 選択されたインタフェースで受信された Frame Check Sequence エラーの量を表示します。
- **Single Collision Frames** — 選択されたインタフェースで受信された Single Collisions Frames エラーの量を表示します。

- **Multiple Collision Frames** — 選択されたインタフェースで受信された Multiple Collisions Frames エラーの量を表示します。
- **Deferred Transmissions** — 選択されたインタフェースで延期された送信の量を表示します。
- **Late Collisions** — 選択されたインタフェースで受信された Late Collisions の量を表示します。
- **Excessive Collisions** — 選択されたインタフェースで受信された Excessive Collisions の量を表示します。
- **Internal MAC Transmit Errors** — 選択されたインタフェースでの Internal MAC Transmit エラーの量を表示します。
- **Carrier Sense Errors** — 選択されたインタフェースでの Carrier Sense エラーの量を表示します。
- **Oversize Packets** — 選択されたインタフェースでの長すぎるフレームのエラーの量を表示します。
- **Internal MAC Receive Errors** — 選択されたインタフェースでの Internal MAC Received エラーの量を表示します。
- **Symbol Errors** — 選択されたインタフェースでの Symbol エラーの量を表示します。
- **Received Pause Frames** — 選択されたインタフェースでの Received Pause フレームの量を表示します （IEEE 802.3X）。
- **Transmitted Pause Frames** — 選択されたインタフェースでの Transmitted Pause フレームの量を表示します （IEEE 802.3X）。

ポートの Etherlike 統計を表示するには、次の手順を実行します。

1. **Etherlike Statistics** ページを開きます。
2. **Interface** フィールドで、**Port** を選びます。
3. **Query** をクリックします。ポートの Etherlike 統計が表示されます。

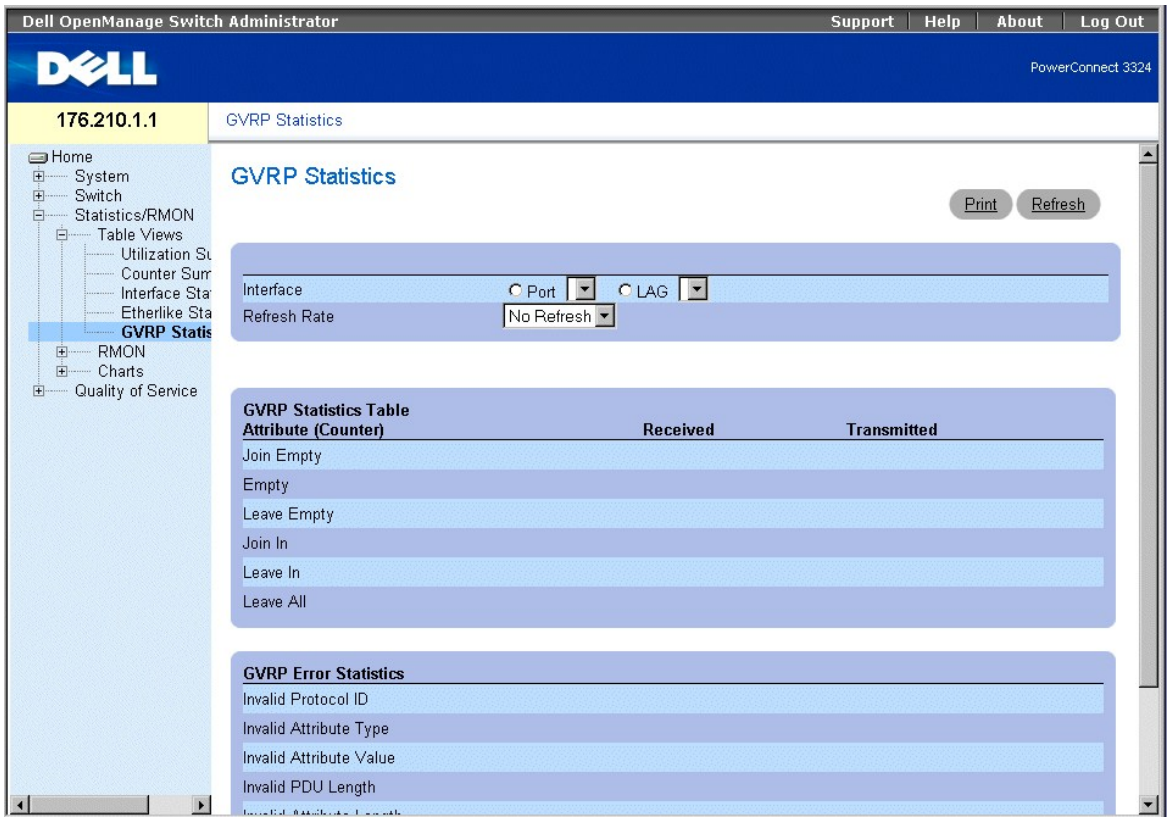
LAG の Etherlike 統計を表示するには、次の手順を実行します。

1. **Etherlike Statistics** ページを開きます。
2. **Interface** フィールドで、**LAG** を選びます。
3. **Query** をクリックします。LAG の Etherlike 統計が表示されます。

GVRP 統計の表示

GVRP Statistics ページには、GVRP 用のデバイスの統計が含まれています。**GVRPStatistics** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON → Table Views → GVRP Statistics** とクリックします。**GVRP Statistics** ページが開きます。



GVRP Statistics ページ

GVRP Statistics ページには、以下のフィールドが含まれています。

- **Interface** — 統計を表示するインタフェースタイプを指定します。
  - **Port** — ポートの統計が表示されていることを示します。
  - **LAG** — LAG の統計が表示されていることを示します。
- **Refresh Rate** — GVRP 統計が更新される間隔を示します。可能なフィールド値には、以下のものがあります。
  - **15 Sec** — GVRP 統計が 15 秒毎に更新されることを示します。
  - **30 Sec** — GVRP 統計が 30 秒毎に更新されることを示します。
  - **60 Sec** — GVRP 統計が 60 秒毎に更新されることを示します。
  - **No Refresh** — GVRP 統計が自動的に更新されないことを示します。
- **Join Empty** — デバイスの GVRP Join Empty 統計を表示します。
- **Empty** — デバイスの GVRP Empty 統計を表示します。
- **Leave Empty** — デバイスの GVRP Leave 統計を表示します。
- **Join In** — デバイスの GVRP Join In 統計を表示します。
- **Leave In** — デバイスの GVRP Leave in 統計を表示します。
- **Invalid Protocol ID** — デバイスの GVRP Invalid Protocol ID 統計を表示します。
- **Invalid Attribute Type** — デバイスの GVRP Invalid Attribute ID 統計を表示します。
- **Invalid Attribute Value** — デバイスの GVRP Invalid Attribute Value 統計を表示します。
- **Invalid PDU Length** — デバイスの GVRP Invalid PDU Length 統計を表示します。

- **Invalid Attribute Length** — デバイスの GVRP Invalid Attribute Length 統計を表示します。
- **Invalid Events** — デバイスの GVRP Invalid Events 統計を表示します。

ポートの GVRP 統計を表示するには、次の手順を実行します。

1. **GVRP Statistics** ページを開きます。
2. **Interface** フィールドで、**Port** を選びます。
3. **Query** をクリックします。ポートの GVRP 統計が表示されます。

LAG の GVRP 統計を表示するには、次の手順を実行します。

1. **GVRP Statistics** ページを開きます。
2. **Interface** フィールドで、**LAG** を選びます。
3. **Query** をクリックします。LAG の GVRP 統計が表示されます。

CLI コマンドを使用した GVRP 統計の表示

ポート毎の GVRP 手順の表示の詳細については、**Port Statistics** ページを参照してください。以下の表で、CLI コマンドについて説明します。

CLI コマンド	説明
show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel- number*]	GVRP 統計を表示します。
show gvrp error-statistics [**ethernet** *interface*| **port-channel** *port-channel-number*]	GVRP エラー 統計を表示します。

以下に、CLI コマンドの例を示します。

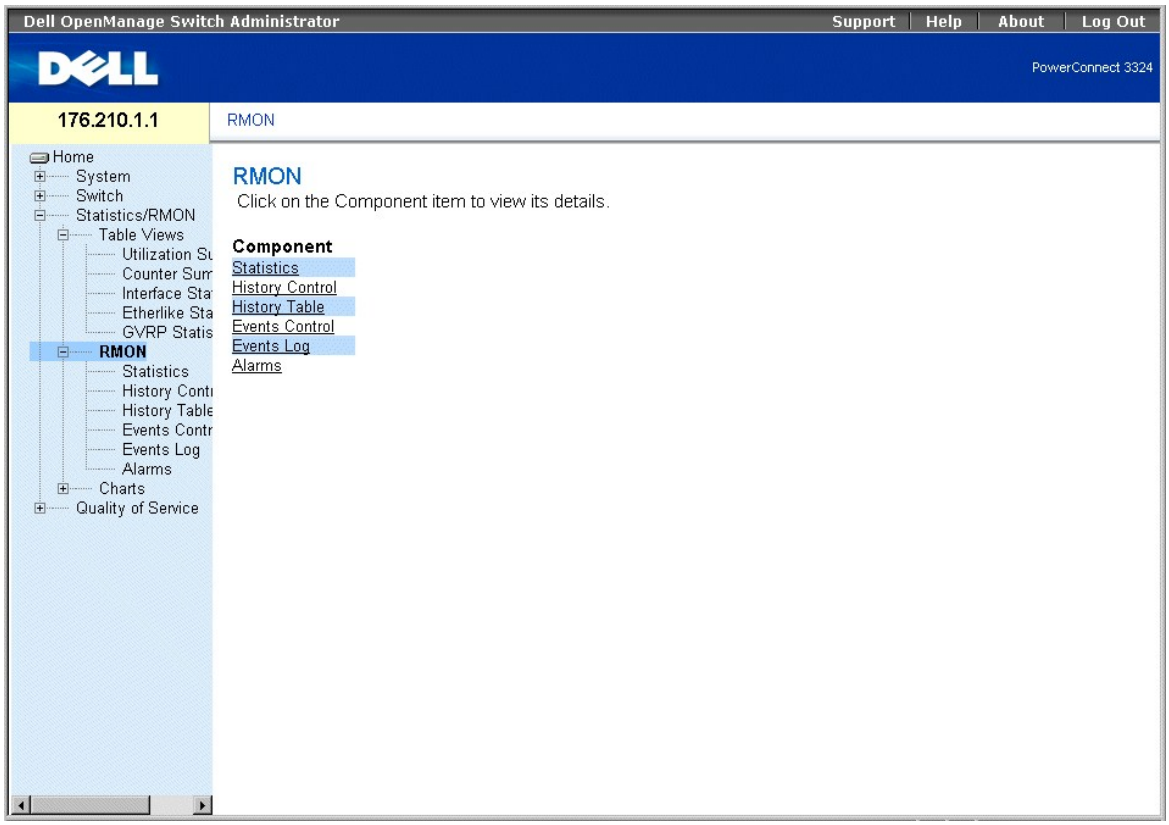
```
Console# show gvrp statistics


GVRP statistics:

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

Legend:

rJE :Join Empty Received .: Join In Received

rEmp :Empty Received rLIn :Leave In Received
```

```
rLE :Leave Empty Received rLA :Leave All Received

sJE :Join Empty Sent sJIn :Join In Sent

sEmp :Empty Sent sLIn :Leave In Sent

sLE :Leave Empty Sent sLA :Leave All Sent



Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA

---- --- ---- ---- ---- --- --- --- --- --- ---- 1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0

1/e5 0 0 0 0 0 0 0 0 0 0 0 0

1/e6 0 0 0 0 0 0 0 0 0 0 0 0

1/e7 0 0 0 0 0 0 0 0 0 0 0 0

1/e8 0 0 0 0 0 0 0 0 0 0 0 0
```

RMON 情報の表示

RMON （Remote Monitoring） を使用して、ネットワーク管理者は離れた場所からネットワークトラフィック情報を表示できます。**RMON** ページを開くには、次の手順を実行
します。

- Tree View で、**Statistics / RMON → RMON** とクリックします。**RMON** ページが開きます。



RMON ページ

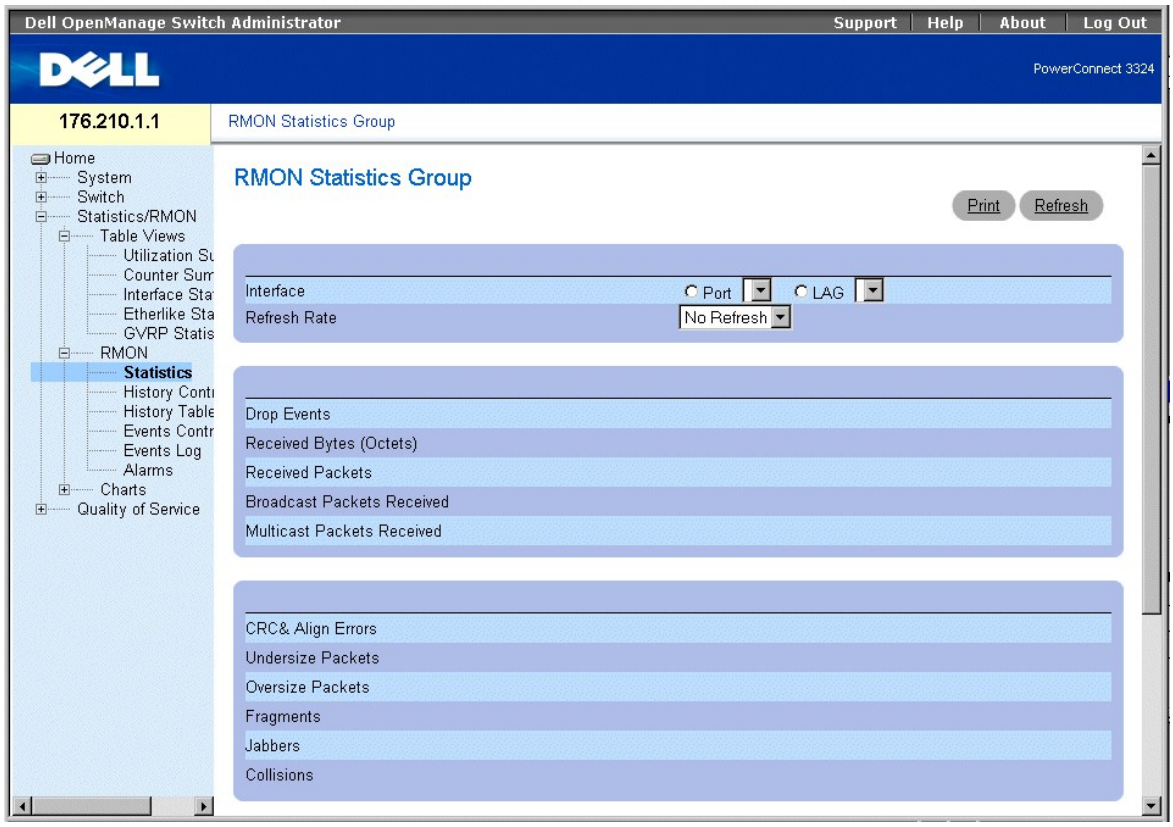
この項には、以下のトピックがあります。

- RMON 統計の表示
- History Control 統計の表示
- RMON History テーブルの表示
- デバイスイベントの定義
- イベントログの表示
- デバイスアラームの定義

RMON 統計の表示

RMON Statistics Group ページを使用して、ネットワーク管理者はインタフェースの RMON 統計を表示することができます。インタフェース統計は、デバイスの利用率、およびデバイスで起きたエラーについての情報を提供します。**RMON Statistics Group** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON → RMON → Statistics** とクリックします。**RMON Statistics Group** ページが開きます。



RMON Statistics Group ページ

RMON Statistics Group ページには、以下の情報が含まれています。

- **Interface** — 統計が表示されるインタフェースタイプと番号を示します。
  可能なフィールド値には、以下のものがあります。
  - **Port** — ポートに固有の統計が表示されていることを示します。
  - **LAG** — LAG に固有の統計が表示されていることを示します。
- **Refresh Rate** — RMON 統計が更新される間隔を示します。
  可能なフィールド値には、以下のものがあります。
  - **15 Sec** — RMON 統計が 15 秒毎に更新されることを示します。
  - **30 Sec** — RMON 統計が 30 秒毎に更新されることを示します。
  - **60 Sec** — RMON 統計が 60 秒毎に更新されることを示します。
  - **No Refresh** — RMON 統計が自動的に更新されないことを示します。
- **Drop Events** — カウンタが最後にクリアされてからインタフェースで起きた破棄されたイベントの量を示します。
- **Received Bytes (Octets)** — カウンタが最後にクリアされてからインタフェースで受信された Octet （バイト） の量を示します。
- **Received Packets** — カウンタが最後にクリアされてからインタフェースで受信されたパケット （バイト） の量を示します。
- **Broadcast Packets Received** — カウンタが最後にクリアされてからインタフェースで受信されたブロードキャストパケットの量を示します。
- **Multicast Packets Received** — カウンタが最後にクリアされてからインタフェースで受信されたマルチキャストパケットの量を示します。
- **CRC& Align Errors** — カウンタが最後にクリアされてからインタフェースで起きた CRC and Align エラーの量を示します。
- **Undersize Packets** — カウンタが最後にクリアされてからインタフェースで受信されたサイズの小さいパケット （バイト） の量を示します。
- **Oversize Packets** — カウンタが最後にクリアされてからインタフェースで受信されたサイズの大きいパケット （バイト） の量を示します。

- **Fragments** — カウンタが最後にクリアされてからインタフェースで受信された Fragment の量を示します。
- **Jabbers** — カウンタが最後にクリアされてからインタフェースで受信された Jabber の量を示します。
- **Collisions** — カウンタが最後にクリアされてからインタフェースで受信された Collision の量を示します。
- **Frames of 64 Bytes** — カウンタが最後にクリアされてからインタフェースで受信された 64 バイトのパケットの量を示します。
- **Frames of 65-127 Bytes** — カウンタが最後にクリアされてからインタフェースで受信された 65 ～ 127 バイトのパケットの量を示します。
- **Frames of 128-255 Bytes** — カウンタが最後にクリアされてからインタフェースで受信された 128 ～ 255 バイトのパケットの量を示します。
- **Frames of 256-511 Bytes** — カウンタが最後にクリアされてからインタフェースで受信された 256 ～ 511 バイトのパケットの量を示します。
- **Frames of 512-1023 Bytes** — カウンタが最後にクリアされてからインタフェースで受信された 512 ～ 1023 バイトのパケットの量を示します。
- **Frames of 1024-1518 Bytes** — カウンタが最後にクリアされてからインタフェースで受信された 1024 ～ 1518 バイトのパケットの量を示します。

インタフェース統計を表示するには、次の手順を実行します。

1. **RMON Statistics Group** ページを開きます。
2. **Interface** フィールドで、インタフェースタイプと番号を選びます。インタフェース統計が **RMON Statistics** に表示されます。

CLI コマンドを使用した RMON 統計の表示

次の表に、**RMON Statistics Group** ページでのフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
show rmon statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	RMON Ethernet 統計を表示します。

以下に、CLI コマンドの例を示します。

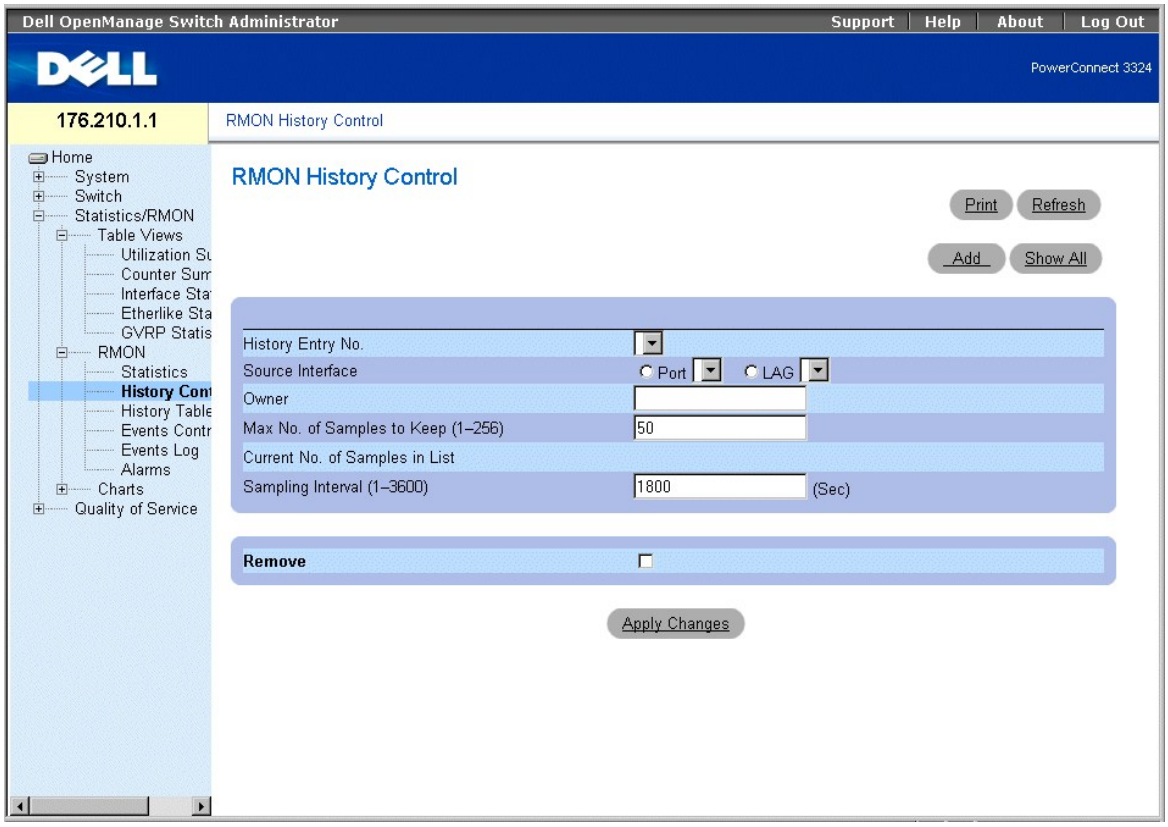
```
Console# show rmon statistics ethernet 1/e1

Port 1/e1

Dropped: 8

Octets:878128 Packets: 978

Broadcast:7 Multicast: 1

CRC Align Errors:0 Collisions: 0

Undersize Pkts:0 Oversize Pkts: 0
```

```
Fragments:0 Jabbers: 0

64 Octets:98 65 to 127 Octets: 0

128 to 255 Octets:0 256 to 511 Octets: 0

512 to 1023 Octets:491 1024 to 1518 Octets: 389
```

History Control 統計の表示

RMON History Control ページには、ポートから得られた RMON データのサンプルについての情報が含まれています。**RMON History Control** ページは、これらのサンプルの収集を制御します。

- Tree View で、**Statistics / RMON → RMON → History Control** とクリックします。**RMON History Control** ページが開きます。



RMON History Control ページ

RMON History Control ページには、以下の情報が含まれています。

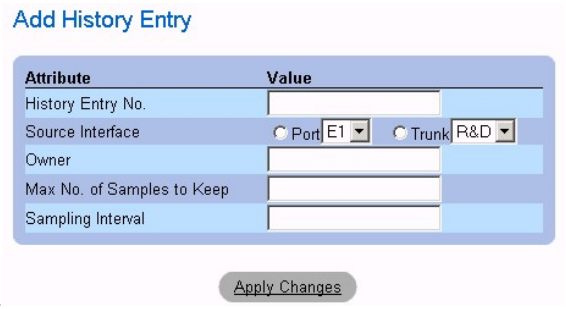
- **History Entry No.** — **History Control Table** エントリを指定します。
- **Source Interface** — History のサンプルが収集されるソースを示します。
  可能なフィールド値には、以下のものがあります。

- **Port** — History サンプルがポートから収集されることを示します。
- **LAG** — History サンプルが LAG から収集されることを示します。

- **Owner** — RMON 情報を要求したユーザーまたは RMON ステーションを示します。
- **Max No. of Samples to Keep (1-256)** — 保存するサンプルの数を示します。デフォルト値は **50** です。
- **Current No. of Samples in List** — 現在収集されたサンプルの数を示します。
- **Sampling Interval (1-3600)** — ポートからサンプルが収集される時間を秒で示します。可能な値は、1 ～ 3600 秒です。デフォルトは、**1800** 秒 （30 分） です。
- **Remove** — **History Control Table** エントリを削除します。
  - **Checked** — **History Control Table** エントリを削除します。
  - **Unchecked** — **History Control Table** エントリを保持します。

History Control エントリを追加するには、次の手順を実行します。

1. **RMON History Control** ページを開きます。
2. **Add** （追加）をクリックします。**Add History Entry** ページが開きます。



Add History エントリページ

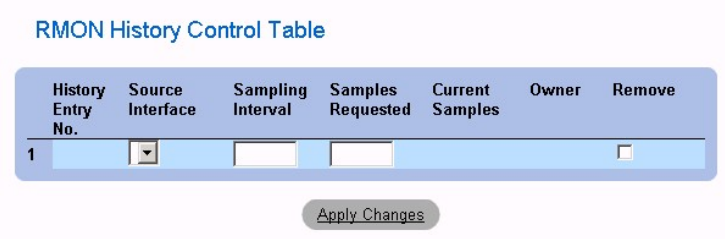
3. **History Entry No.**、**Source Interface**、**Owner**、**Max No. of Samples toKeep**、および **Sampling Interval** フィールドを定義します。
4. **Apply Changes** をクリックします。**History Control Entry** が追加されます。

History Control Table エントリを変更するには、次の手順を実行します。

1. **RMON History Control** ページを開きます。
2. **History Index** フィールドで、**RMON History Control Table** エントリを選びます。
3. **Source Interface**、**Owner**、**Max No. of Samples to Keep**、**No. of Current Samples**、または **Sampling Interval** フィールドを変更します。
4. **Apply Changes** をクリックします。**RMON History Control Table** エントリが変更され、デバイスがアップデートされます。

History Control Table を表示するには、次の手順を実行します。

1. **RMON History Control** ページを開きます。
2. **Show All** をクリックします。**History Control Table** が開きます。



History Control Table

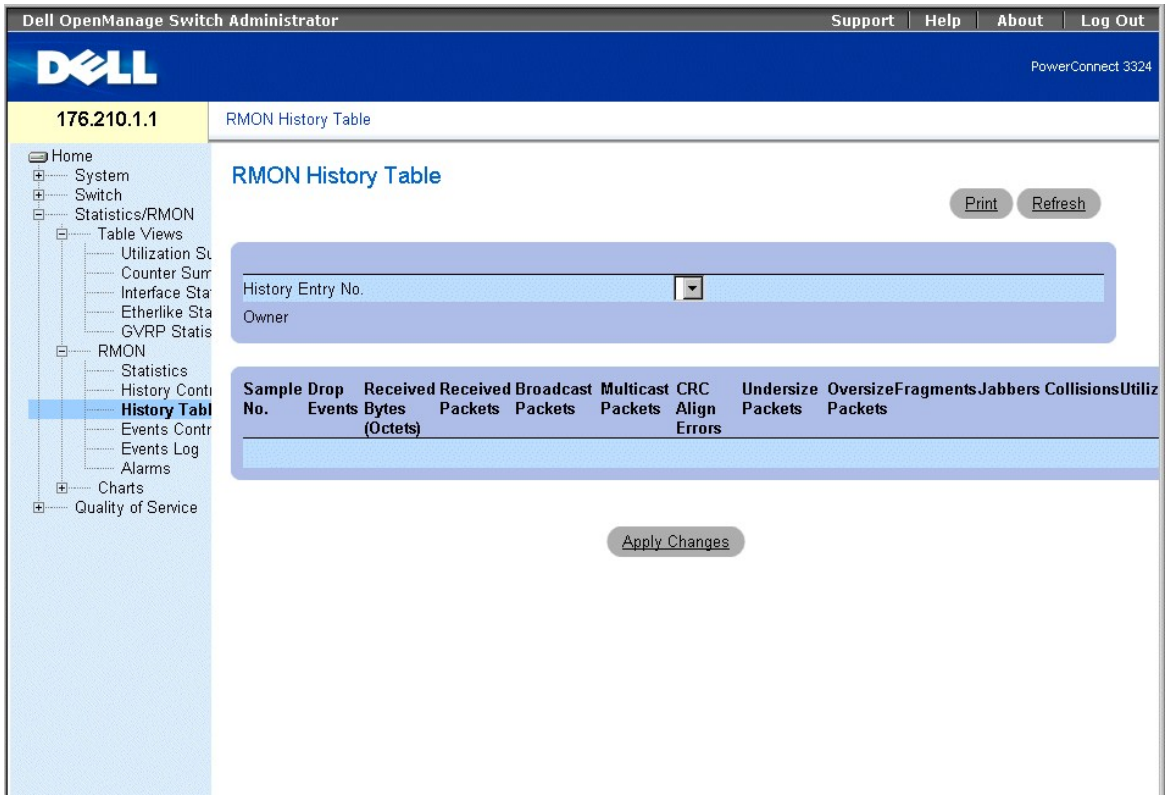
History Control Table エントリを削除するには、次の手順を実行します。

1. **RMON History Control** ページを開きます。
2. **History Index** フィールドで、**History Control Table** エントリを選びます。
3. **Remove** チェックボックスにチェックマークを付けます。
4. **Apply Changes** をクリックします。**RMON History Control Table** エントリが削除され、デバイスがアップデートされます。

RMON History テーブルの表示

RMON History Table には、インタフェースに固有の RMON 統計ネットワークサンプルが含まれています。各テーブルエントリは、サンプルを収集中に編集されたすべてのカウンタ値を表わします。**RMON History Table** を開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON → RMON → History Table** とクリックします。



RMON History Table

メモ: すべてのフィールドが RMON History Table で表示されるわけではありません。

RMON History Table には、以下のフィールドが含まれています。

- **Sample No.** — テーブルの情報に反映する特定のサンプルを示します。
- **Drop Events** — サンプルが収集される合間にネットワークリソースの不足によって破棄されたパケットの数を示します。これは破棄されたパケットの正確な数ではなく、破棄されたパケットが検出された回数を表わすことがあります。
- **Received Bytes (Octets)** — ネットワークで受信された不良パケットを含むデータのバイト数を示します。
- **Received Packets** — サンプル収集の合間に受信されたパケットの数を示します。
- **Broadcast Packets** — サンプル収集の合間に受信された優良なブロードキャストパケットの数を示します。
- **Multicast Packets** — サンプル収集の合間に受信された優良なマルチキャストパケットの数を示します。
- **CRC Align Errors** — サンプルセッション中に受信された整数または非整数バイトの不良な FCS （Frame Check Sequence） を持つ 64 ～ 1518 バイトのパケットの数を示します。
- **Undersized Packets** — サンプルセッション中に受信された 64 バイト以下のパケットの数を示します。
- **Undersized Packets** — サンプルセッション中に受信された 1518 バイト以上のパケットの数を示します。
- **Fragments** — サンプルセッション中に受信された 64 バイト以下で FCS のあるパケットの数を示します。
- **Jabbers** — サンプルセッション中に受信された 1518 バイト以上で FCS のあるパケットの数を示します。
- **Collisions** — サンプルセッション中に起きたパケット衝突の全体数を概算します。衝突は、2 つ以上のステーションが同時に送信しているのを repeater ポートが検出した際に検出されます。
- **Utilization** — サンプルセッション中の、インタフェース上のメイン物理的レイヤネットワーク Description を概算します。値は小数点以下 2 桁までのパーセントで反映されます。

特定の History エントリの統計を表示するには、次の手順を実行します。

1. **RMON History Table** ページを開きます。
2. **History Table No.** フィールドで、History エントリを選びます。エントリの統計が **RMON History Table** に表示されます。

CLI コマンドを使用した RMON History 統計の表示

以下の表では、RMON History 統計を表示する CLI コマンドについて説明します。

CLI コマンド	説明
rmon table-size history *entries*	History Table エントリの最大数を設定します。
rmon collection history *index* [owner *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	インタフェースで RMON MIB History 統計グループを有効にします。
show rmon history *index* {**throughput** | **errors** | **other**} [**period** *hh:mm:ss*]	RMON Ethernet Statistics History を表示します。

以下に、CLI コマンドの例を示します。

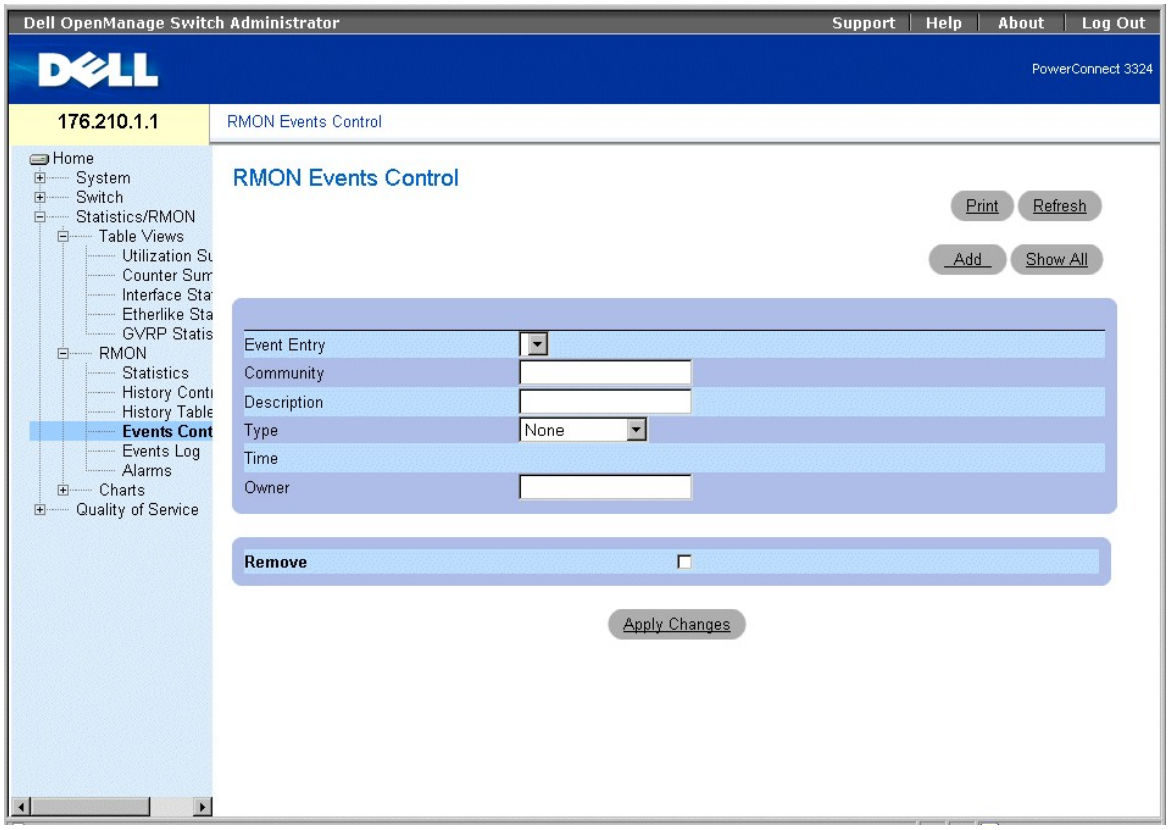
```
Console (config)# rmon table-size history 1000

Console (config)# interface ethernet 1/e8
```

```
Console (config-if)# rmon collection history 1 interval 2400

Console# show rmon history 1 throughput

Sample set:1 Owner:CLI

Interface:1/e1 Interval: 1800

Requested samples:50 Granted samples: 50


Maximum table size: 500


Day:Jan 18 2002

Time Octets Packets Broadcast Multicast Utilization

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

23:58:30 878128 878 7 1 20.87%

23:59:00 75898768 91892 932 1723 19.27%

23:59:30 171797536 193784 1817 3289 19.82%


Day:Jan 19 2002

Time Octets Packets Broadcast Multicast Utilization

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

00:00:00 287696304 275686 2789 5878 20.17%

00:00:30 303595962 357568 3289 7287 19.98%
```

デバイスイベントの定義

RMON Events Control ページを使用すると、ネットワーク管理者が RMON イベントを表示できます。**RMON Events** テーブルは、**RMON Events Control** テーブルから開くことができます。**RMON Events Control** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON → RMON → Events Log** とクリックします。**RMON Events Control** ページが開きます。



RMON Events Control ページ

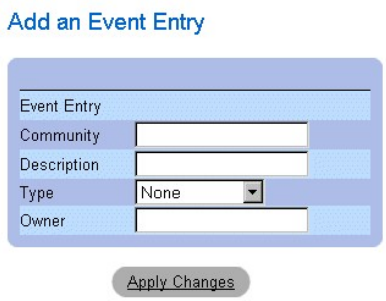
RMON Events Control ページには、以下のフィールドが含まれています。

- **Event Entry** — イベントを示します。
- **Community** — イベントが属する SNMP コミュニティを指定します。
- **Description** — ユーザー定義のイベントの説明を提供します。
- **Type** — イベントタイプを説明します。可能なフィールド値には、以下のものがあります。
  - **Log** — イベントタイプがログエントリであることを示します。
  - **Trap** — イベントタイプがトラップであることを示します。
  - **Log and Trap** — イベントタイプがログエントリとトラップの両方であることを示します。
- **Time** — イベントが起きた時間を示します。
- **Owner** — イベントを定義したデバイスまたはユーザーを示します。
- **Remove** — **Events Table** からイベントを削除します。
  - **Checked** — **Events Table** からイベントを削除します。

- **Unchecked** — **Events Table** からイベントを保持します。

RMON Event を追加するには、次の手順を実行します。

1. **RMON Events Control** ページを開きます。
2. **Add** （追加）をクリックします。**Add an Event Entry** ページが開きます。



Add an Event Entry ページ

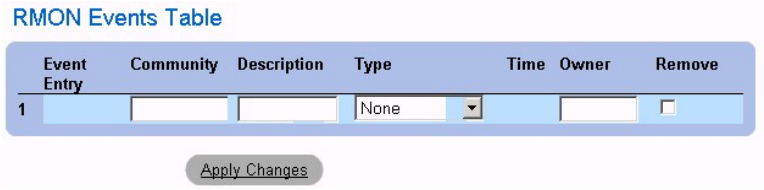
3. **New Event Index**、**Community**、**Description**、**Type**、および **Owner** フィールドを定義します。
4. **Apply Changes** をクリックします。**Event Table** エントリが追加されデバイスがアップデートされます。

RMON Event を変更するには、次の手順を実行します。

1. **RMON Events Control** ページを開きます。
2. **Event Entry** フィールドで、**Event Table** エントリを選びます。
3. **Community**、**Description**、**Type**、または **Owner** フィールドを変更します。
4. **Apply Changes** をクリックします。**Event Table** エントリが変更され、デバイスがアップデートされます。

RMON Event Table を表示するには、次の手順を実行します。

1. **RMON Events Control** ページを開きます。
2. **Show All** をクリックします。**RMON Events Table** が開きます。



RMON Events Table

複数の RMON Event エントリを削除するには、次の手順を実行します。

1. **RMON Events Control** ページを開きます。
2. **Event Index** フィールドで、**Event Table** エントリを選びます。
3. **Remove** チェックボックスにチェックマークを付けます。

4. **Apply Changes** をクリックします。**Event Table** エントリが削除され、デバイスがアップデートされます。

メモ: 単一の **Event** エントリは、**Remove** チェックボックスを使用して、**RMON Events** ページから削除することができます。

CLI コマンドを使用した RMON Events Control の定義および表示

次の表に、**RMON Events Control** ページでのフィールドの設定および表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
rmon event *index type* [**community** *text*] [**description** *text*] [*owner name*]	RMON イベントを設定します。
show rmon events	RMON イベントテーブルを表示します。

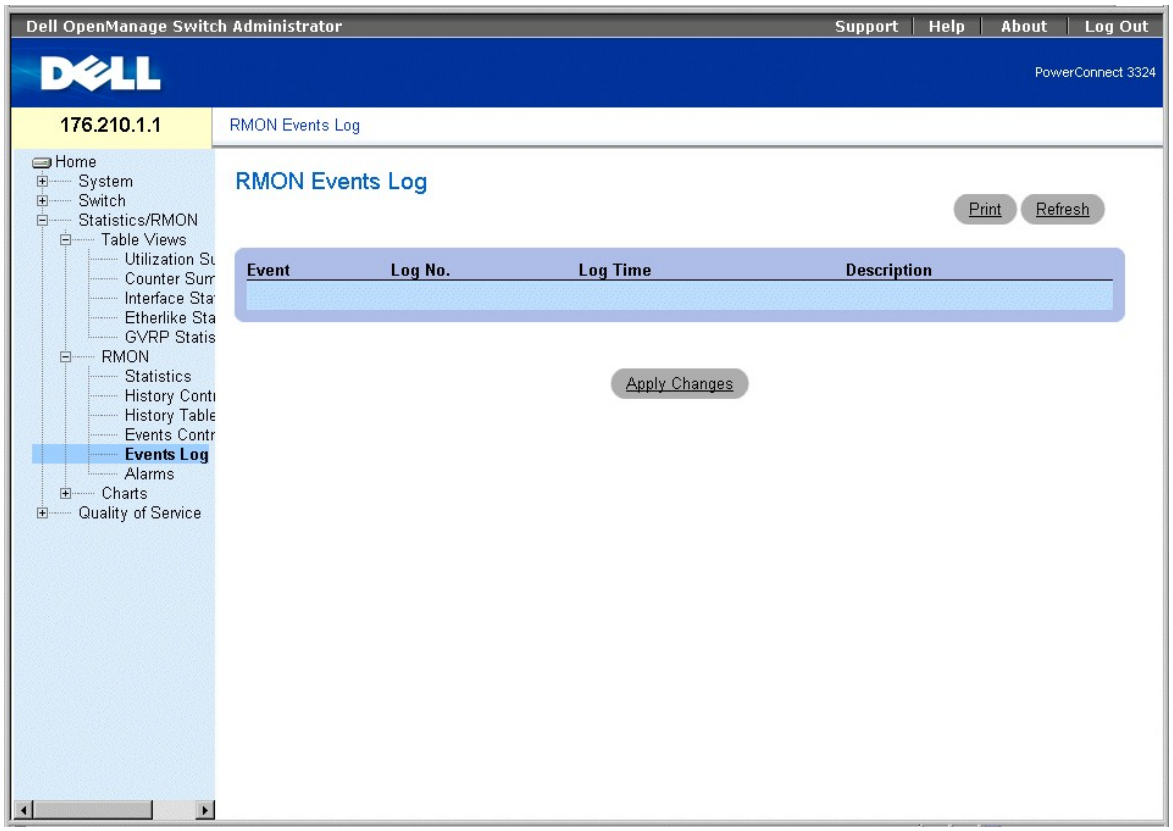
以下に、CLI コマンドの例を示します。

```
Console (config)# rmon event 10 log

Config (config)# exit

Console# show rmon events


Index Description Type Community Owner Last time sent

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

1 Errors Log CLI Jan 18 2002 23:58:17

2 High Broadcast Log-Trap device Manager Jan 18 2002 23:59:48
```

イベントログの表示

RMON Events Log ページには、RMON Events の一覧が含まれています。**RMONEvents Log** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON → RMON → Events Log** とクリックします。**RMON Events Log** ページが開きます。



RMON Events Log ページ

RMON Events Log ページには、以下のフィールドが含まれています。

- **Event** — **RMON Event Log** エントリ番号を識別します。
- **Log No.** — ログ番号を示します。
- **Log Time** — ログエントリが記述された時間を特定します。
- **Description** — ログエントリを説明します。

CLI コマンドを使用した RMON Events Log の表示

次の表に、**RMON Events Log** ページで表示されるフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
rmon table-size log *entries*	ログテーブルエントリの最大数を設定します。
show rmon log [*event*]	RMON ロギングテーブルを表示します。

以下に、CLI コマンドの例を示します。

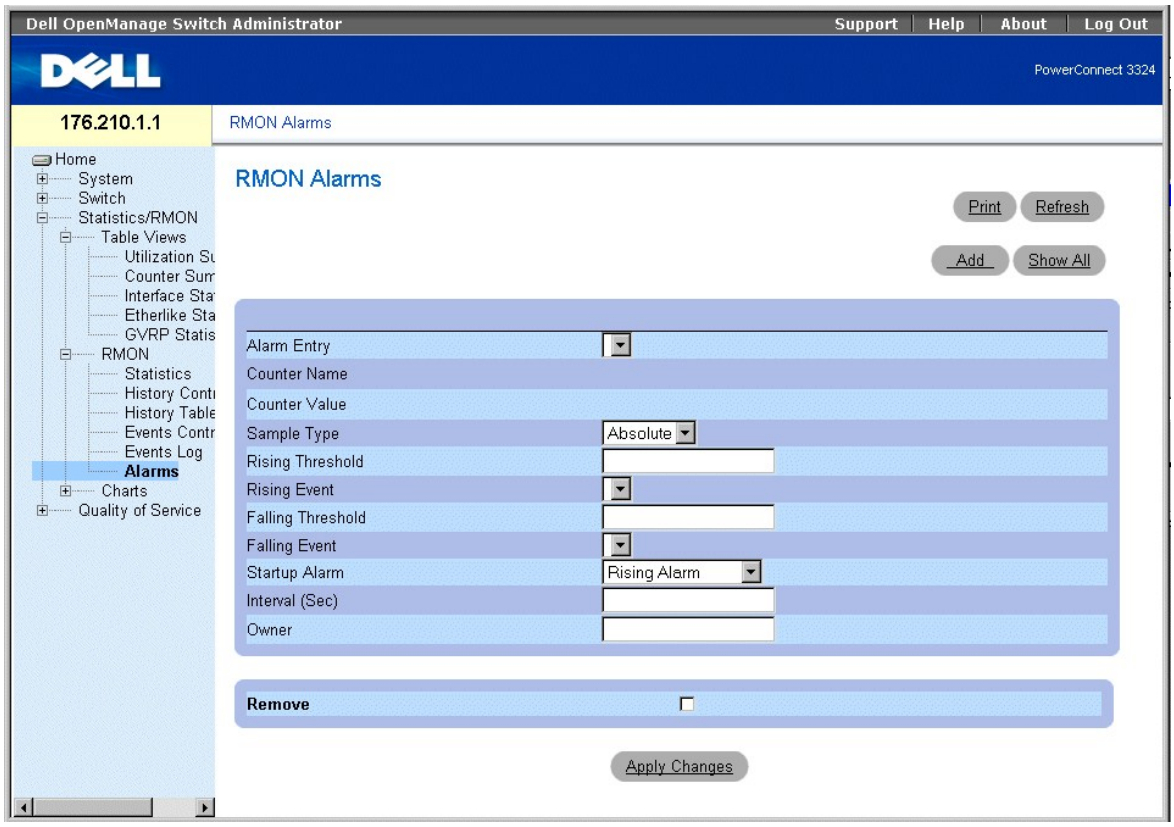
```
Console (config)# rmon table-size log 500
```

```
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



Console# show rmon log

Maximum table size:500 (800 after reset)

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
```

デバイスアラームの定義

RMON Alarm ページを使用して、ネットワーク管理者はネットワークアラームを設定することができます。ネットワークアラームは、ネットワークで問題が検出されたときに起きます。Rising 限界値および Falling 限界値で、アラームを生成します。**RMON Alarm** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON → RMON → Alarms** とクリックします。**RMON Alarm** ページが開きます。



RMON Alarm ページ

RMON Alarm ページには、以下のフィールドが含まれています。

- **Alarm Entry** — 特定のアラームを示します。
- **Counter Name** — 選択した RMON カウンタを示します。
- **Counter Value** — RMON カウンタの値を示します。
- **Sample Type** — 選択された変数のサンプルの収集方法を指定し、値を限界値と比較します。可能なフィールド値には、以下のものがあります。
  - **Delta** — 現在の値から最後のサンプル値を引きます。この値の差と限界値を比較します。
  - **Absolute** — サンプル収集間隔の最後で、値を限界値と比較します。
- **Rising Threshold** — Rising 限界値を生成する、上昇カウンタ値です。
- **Rising/Falling Event** — アラームを報告する機構です。LOGed または TRAPed、あるいはその両方があります。LOG を選んだ場合、デバイスにも管理システムにも保存機構はありません。ただし、デバイスがリセットされていない場合、デバイスはデバイス LOG テーブルに残ります。TRAP を選んだ場合、SNMP を介した TRAP が生成され、TRAP の一般的な機構を介して報告されます。TRAP は、同じ機構を使用して保存することができます。
- **Falling Threshold** — Falling 限界値を生成する、下降カウンタ値です。

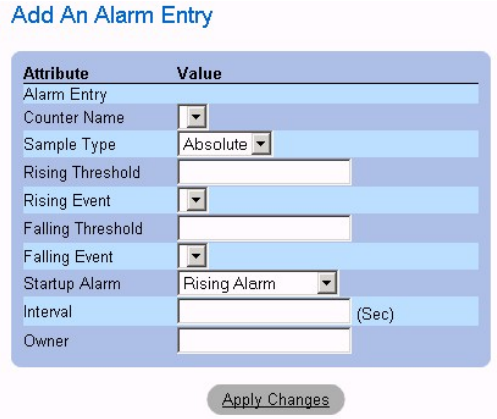
メモ: Rising および Falling 限界値は、グラフバーの上部にグラフィックで表示されます。監視されている各変数には、指定された色があります。

- **Startup Alarm** — アラームを起動するトリガです。Rising は、低限界値から高限界値を超えることで定義されています。可能なフィールド値には、以下のも
のがあります。
  - **Rising Alarm**
  - **Falling Alarm**
  - **Rising and Falling Alarm**

- **Interval** — アラームの間隔を示します。
- **Owner** — アラームを定義したデバイスまたはユーザーを示します。
- **Remove** — RMON Alarm を削除します。
  - **Checked** — **Alarm Table** エントリを削除します。
  - **Unchecked** — **Alarm Table** エントリを保持します。

Alarm Table エントリを追加するには、次の手順を実行します。

1. **RMON Alarm** ページを開きます。
2. **Add** （追加）をクリックします。**Add An Alarm Entry** ページが開きます。



Add An Alarm Entry ページ

3. ダイアログ内のフィールドを定義します。
4. **Apply Changes** をクリックします。RMON アラームが追加され、デバイスはアップデートされます。

Alarm Table エントリを変更するには、次の手順を実行します。

1. **RMON Alarm** ページを開きます。
2. **Alarm Entry** ドロップボックスで、**RMON Alarm Table** エントリを選びます。
3. ダイアログ内のフィールドを変更します。
4. **Apply Changes** をクリックします。**RMON Alarm Table** エントリが変更され、デバイスがアップデートされます。

Alarm Table を表示するには、次の手順を実行します。

1. **RMON Alarm Table** ページを開きます。
2. **Show All** をクリックします。**RMON Alarm Table** ページが開きます。

RMON Alarm Table

Alarm Table エントリを削除するには、次の手順を実行します。

1. **RMON Alarm** ページを開きます。
2. **Alarm Entry** ドロップダウンボックスで、**RMON Alarm** を選びます。
3. **Remove** チェックボックスにチェックマークを付けます。
4. **Apply Changes** をクリックします。**RMON Alarm Table** エントリが削除され、デバイスがアップデートされます。

CLI コマンドを使用したデバイスアラームの定義および表示

次の表に、**RMON Alarm** ページでのフィールドの設定および表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]	アラームの環境を設定します。
show rmon alarm-table	アラームの要約テーブルを表示します。
show rmon alarm *number*	アラームの設定を表示します。

以下に、CLI コマンドの例を示します。

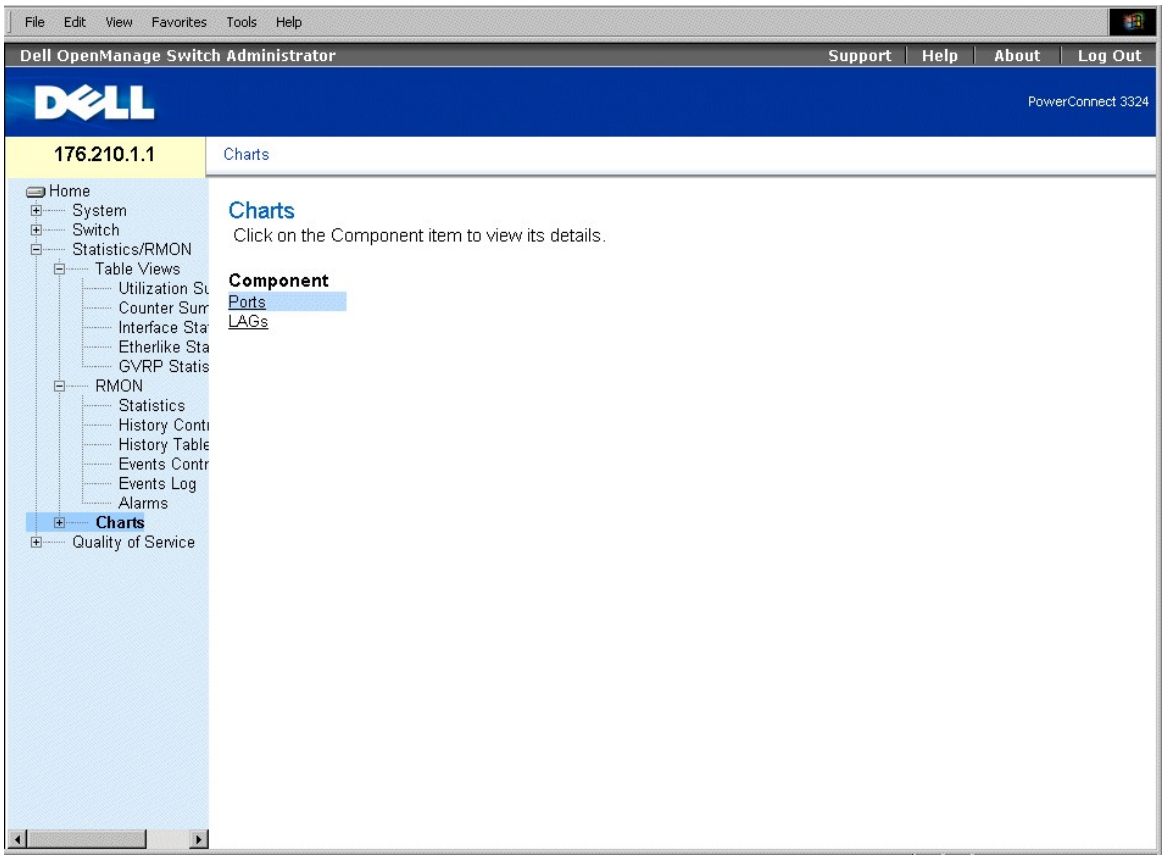
```
Console (config)# rmon alarm 1.3.6.1.2.1.2.2.1.10 1000000 10 20

Console (config)# exit

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

Console# show rmon alarm 1

Alarm 1
```

```
-------

OID: 1.3.6.1.2.1.2.2.1.10.1

Last sample Value: 878128

Interval: 30

Sample Type:delta

Startup Alarm:rising

Rising Threshold: 8700000

Falling Threshold: 78

Rising Event: 1

Falling Event: 1

Owner:CLI
```

チャートの表示

Charts ページには、チャート形式で統計を表示するためのリンクがあります。
Charts ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON** → **Charts** とクリックします。
  Charts ページが開きます。



Charts ページ

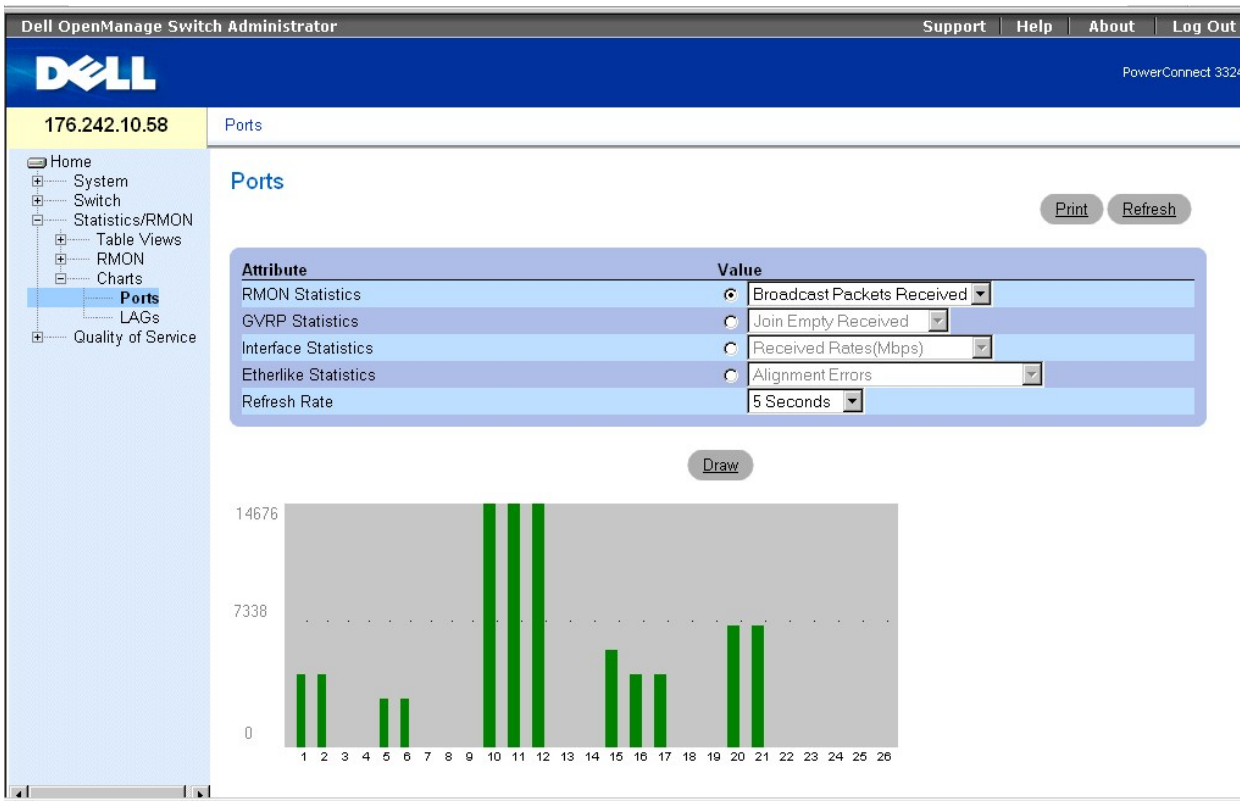
Charts ページには、以下のリンクがあります。

- ポートの統計の表示
- LAG の統計の表示

ポートの統計の表示

Ports ページでは、選択されたポートの統計をチャート形式で表示します。
Port Statistics ページを開くには、次の手順を実行します。

1. Tree View で、**Statistics / RMON** → **Charts** → **Ports** とクリックします。
   Port Statistics ページが開きます。



Ports ページ

Port Statistics ページには、以下のフィールドが含まれています。

- **RMON Statistics** — 選択されたユニットの RMON 統計を提供します。
- **Etherlink Statistics** — 選択されたユニットの Etherlink 統計を提供します。
- **Interface Statistics** — 選択されたユニットのインタフェース統計を提供します。
- **GVRP Statistics** — 選択されたユニットの GVRP 統計を提供します。
- **Refresh Rate** — デバイスが更新される間隔を示します。可能なフィールド値には、以下のものがあります。
  - **15 Sec** — ポート統計が 15 秒毎に更新されることを示します。
  - **30 Sec** — ポート統計が 30 秒毎に更新されることを示します。
  - **60 Sec** — ポート統計が 60 秒毎に更新されることを示します。
  - **No Refresh** — ポート統計が自動的に更新されないことを示します。

ポート固有の統計を表示するには、次の手順を実行します。

1. **Port Statistics** ページを開くには、次の手順を実行します。
2. 統計カテゴリおよびポートを選びます。
3. **Draw** をクリックします。選択されたインタフェースの統計が表示されます。

CLI コマンドを使用したポートの統計の表示

次の表に、**Port Statistics** ページでのフィールドの表示に対応する CLI コマンドをまとめます。

CLI コマンド	説明
clear counters [ethernet *interface* | **port-channel** *port-channel-number*]	インタフェースの統計をクリアにします。
show rmon statistics [ethernet *interface* | **port-channel** *port-channel-number*]	RMON Ethernet 統計を表示します。
clear gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	すべての GVRP 統計情報をクリアします。
show gvrp statistics [ethernet *interface* | **port-channel** *port-channel-number*]	GVRP 統計を表示します。
show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	GVRP エラー 統計を表示します。

以下に、CLI コマンドの例を示します。

```
Console# clear counters ethernet 1/e1

Console# show rmon statistics ethernet 1/e1

Port 1/e1

Dropped: 8

Octets:878128 Packets: 978

Broadcast:7 Multicast: 1

CRC Align Errors:0 Collisions: 0

Undersize Pkts:0 Oversize Pkts: 0

Fragments:0 Jabbers: 0

64 Octets:98 65 to 127 Octets: 0

128 to 255 Octets:0 256 to 511 Octets: 0

512 to 1023 Octets:491 1024 to 1518 Octets: 389

Console # configure

Console (config)# clear gvrp statistics ethernet 1/e8
```

```
Console (config)# exit

Console# show gvrp statistics

GVRP statistics:

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

Legend:

rJE :Join Empty Received rJIn :Join In Received

rEmp :Empty Received rLIn :Leave In Received

rLE :Leave Empty Received rLA :Leave All Received

sJE :Join Empty Sent sJIn :Join In Sent

sEmp :Empty Sent sLIn :Leave In Sent

sLE :Leave Empty Sent sLA :Leave All Sent


Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA

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

1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0

1/e5 0 0 0 0 0 0 0 0 0 0 0 0

1/e6 0 0 0 0 0 0 0 0 0 0 0 0
```

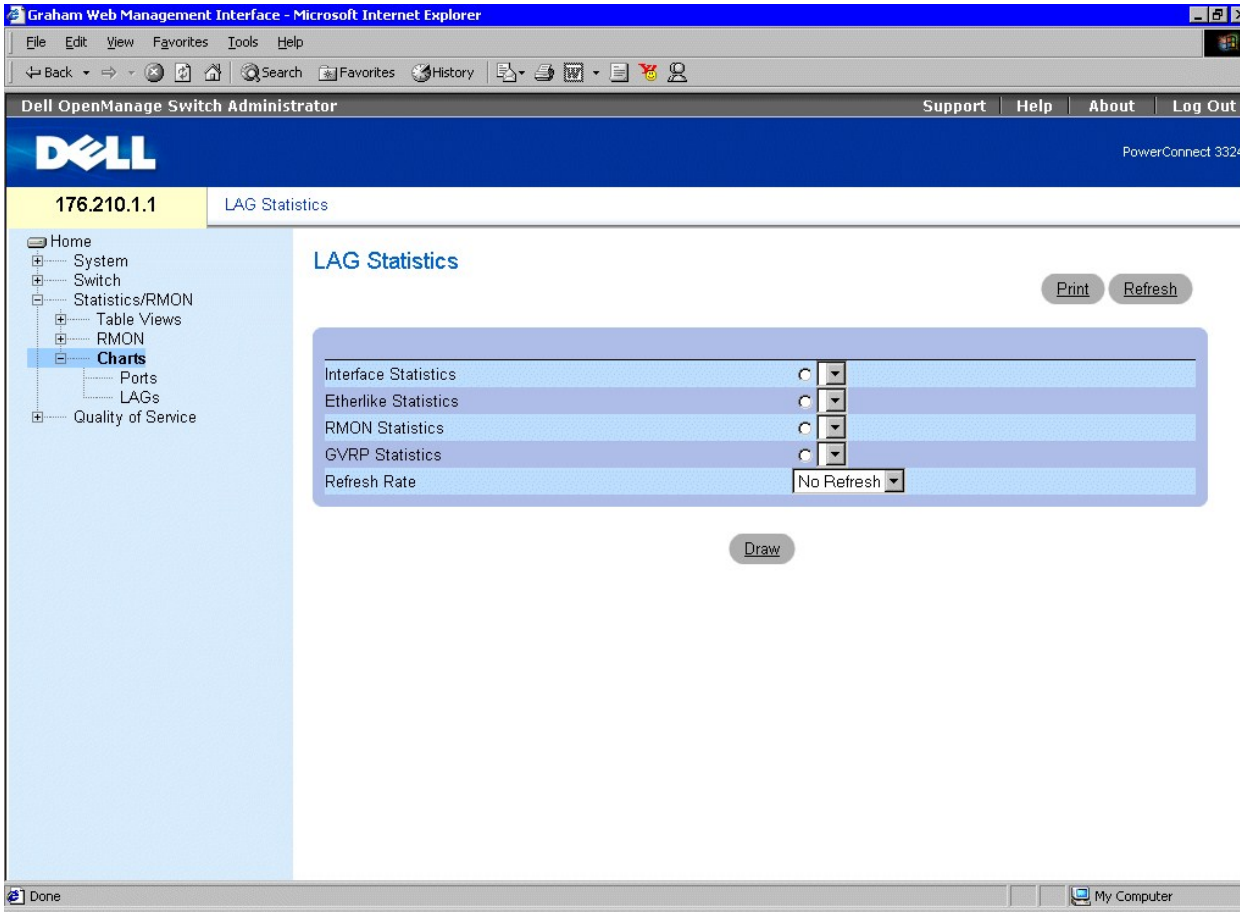
```
1/e7 0 0 0 0 0 0 0 0 0 0 0 0

1/e8 0 0 0 0 0 0 0 0 0 0 0 0


Console# show gvrp error-statistics

GVRP error statistics:

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

Legend:

INVPROT :Invalid Protocol Id INVPLEN :Invalid PDU Length

INVATYP :Invalid Attribute Type INVALEN :Invalid Attribute Length

INVAVAL :Invalid Attribute Value INVEVENT :Invalid Event


Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

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

1/e1 0 0 0 0 0 0

1/e2 0 0 0 0 0 0

1/e3 0 0 0 0 0 0

1/e4 0 0 0 0 0 0

1/e5 0 0 0 0 0 0

1/e6 0 0 0 0 0 0

1/e7 0 0 0 0 0 0
```

```
1/e8 0 0 0 0 0 0
```

LAG の統計の表示

LAG Statistics ページでは、ポートエレメントの統計をチャート形式で表示します。**LAG Statistics** ページを開くには、次の手順を実行します。

- Tree View で、**Statistics / RMON** → **Charts** とクリックします。
  LAG Statistics ページが開きます。



LAG Statistics ページ

LAG Statistics ページには、以下のフィールドが含まれています。

- **Interface Statistics** — トランクのインタフェース統計を提供します。
- **Etherlike Statistics** — トランクの Etherlike 統計を提供します。
- **RMON Statistics** — トランクの RMON 統計を提供します。
- **GVRP Statistics** — トランクの GVRP 統計を提供します。
- **Refresh Rate** — デバイスが更新される間隔を示します。可能なフィールド値には、以下のものがあります。
  - **15 Sec** — LAG 統計が 15 秒毎に更新されることを示します。
  - **30 Sec** — LAG 統計が 30 秒毎に更新されることを示します。

- **60 Sec** — LAG 統計が 60 秒毎に更新されることを示します。
- **No Refresh** — LAG 統計が更新されないことを示します。

ポート固有の統計を表示するには、次の手順を実行します。

1. **Port Statistics** ページを開くには、次の手順を実行します。
2. インタフェースタイプを選びます。
3. **Draw** をクリックします。選択されたインタフェースの統計が表示されます。

CLI コマンドを使用した LAG 統計の表示

次の表では、LAG 統計を表示する CLI コマンドについて説明します。

CLI コマンド	説明
show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]	物理的なインタフェースの統計を表示します。

以下に、CLI コマンドの例を示します。

```
Console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 183892 1289 987 8

2/e1 0 0 0 0

3/e1 123899 1788 373 19

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1/e1 9188 9 8 0

2/e1 0 0 0 0
```

3/e1 8789 27 8 0

Ch InOctets InUcastPkts InMcastPkts InBcastPkts

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

1 27889 928 0 78

Ch OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1 23739 882 0 122

Console# show interfaces counters ethernet 1/e1

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 183892 1289 987 8

Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts

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

1/e1 9188 9 8 0

Alignment Errors: 17

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

```
    Deferred Transmissions: 0

    Late Collisions: 0

    Excessive Collisions: 0

    Internal MAC Tx Errors: 0

    Carrier Sense Errors: 0

    Oversize Packets: 0

    Internal MAC Rx Errors: 0

    Symbol Errors: 0

    Received Pause Frames: 0

    Transmitted Pause Frames: 0

-------------------------------------------------------------------------------
```

メモ、注意および警告

Dell™ PowerConnect™ 3324/3348 ユーザーズガイド

- メモ、注意、および警告

Model PowerConnect 3324/3348

メモ、注意、および警告

メモ: メモは、デバイスをより有用に使うための重要な情報を説明しています。

注意: ハードウェアの損傷またはデータの損失の可能性を示唆し、問題を回避する方法を説明しています。

警告: **警告は、物的損害、けが、または死亡の原因となる可能性があることを示します。**

本書で使用されている商標について:Dell、DELL ロゴ、および *PowerConnect*, *Dell OpenManage*, *PowerEdge*, *Inspiron*, *Dell Precision*, *Dimension*, *OptiPlex*, *Axim*, *PowerVault*, *PowerApp*, *DellNet*, は *Latitude* は Dell Inc.の商標です。Microsoft および Windows は Microsoft Corporation の登録商標です。

本書では、必要に応じて上記記載以外の商標および会社名が使用されている場合がありますが、これらの商標や会社名は、一切 Dell Inc. に所属するものではありません。

2003 年 11 月 Rev. A01
