Dell™ PowerConnect™ 34XX システム ユーザーズガイド

メモ、注意、警告

メモ： コンピュータを使いやすくする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やデータの損失の可能性を示し、その危険を回避するための方法を説明してい ます。

警告： 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。

2005 年 3 月

メモ、注意および警告

はじめに

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

PowerConnect 3424/3448 と PowerConnect 3424P/3448P は、スタック可能な新型のマルチレイヤーデバイスです。PowerConnect の各ユニットは、スタンドアロン、マルチレイヤー、スイッチングデバイス、またはスタック可能デバイス（スタッキングメンバーは最大 6 台）のいずれとしても使用できます。

本『ユーザーズガイド』には、PowerConnect の設置、設定、メンテナンスに必要な情報が記載されています。

システムの説明

PowerConnect 3424/3448 と PowerConnect 3424P/3448P は、汎用性と管理のしやすさを兼ね備えたデバイスです。PowerConnect 3424 と 3448 のシリーズには、以下のタイプがあります。

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

PowerConnect 3424

PowerConnect 3424 には、24 個の 10/100Mbps ポートと 2 つの SFP ポート、2 つの銅線ポートが装備されています。これらのポートは、スタンドアロンデバイス内でのトラフィックの転送に使用できるほか、デバイスをスタックする場合はスタッキングポートとして使用できます。デバイスには RS-232 コンソールポートも 1 つ装備されています。PowerConnect 3424 はスタック可能デバイスですが、スタンドアロンデバイスとしても動作します。

PowerConnect 3424P

PowerConnect 3424P には、24 個の 10/100Mbps ポートと 2 つの SFP ポート、2 つの銅線ポートが装備されています。これらのポートは、スタンドアロンデバイス内でのトラフィックの転送に使用できるほか、デバイスをスタックする場合はスタッキングポートとして使用できます。デバイスには RS-232 コンソールポートも 1 つ装備されています。PowerConnect 3424P はスタック可能デバイスですが、スタンドアロンデバイスとしても動作します。The PowerConnect 3424P は PoE（パワーオーバーイーサネット）も提供します。

図**1-1 PowerConnect 3424** と **PowerConnect 3424P**

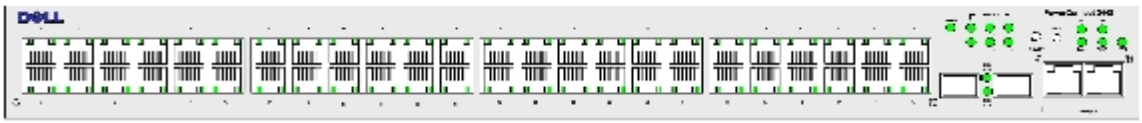
PowerConnect 3448

PowerConnect 3448 には、48 個の 10/100Mbps ポートと 2 つの SFP ポート、2 つの銅線ポートが装備されています。これらのポートは、スタンドアロンデバイス内でのトラフィックの転送に使用できるほか、デバイスをスタックする場合はスタッキングポートとして使用できます。デバイスには RS-232 コンソールポートも 1 つ装備されています。PowerConnect 3448 はスタック可能デバイスですが、スタンドアロンデバイスとしても機能します。

PowerConnect 3448P

PowerConnect 3448P には、48 個の 10/100Mbps ポートと 2 つの SFP ポート、2 つの銅線ポートが装備されています。これらのポートは、デバイスがスタンドアロンモードの場合にトラフィックの転送に使用できるほか、デバイスがスタックの一部である場合はスタッキングポートとして使用できます。デバイスには RS-232 コンソールポートも 1 つ装備されています。また、PowerConnect 3448P には PoE も提供します。

図**1-2 PowerConnect 3448** と **PowerConnect 3448P**



スタッキングの概要

PowerConnect 3424/P と PowerConnect 3448/P のスタッキングは、すべてのスタックメンバーが単一のユニットであるかのように、一ヶ所から複数のスイッチを管理することができます。すべてのスタックメンバーは 1 つの IP アドレスでアクセスでき、この IP アドレスでスタックが管理されます。スタックの管理は以下の場所から行うことができます。

- ウェブベースのインタフェース
- SNMP 管理ステーション
- コマンドラインインタフェース（CLI）

PowerConnect 3424/P デバイスと PowerConnect 3448/P デバイスは、1 つのスタックで最大 6 台のユニットのスタッキングをサポートしているほか、スタンドアロンユニットとしても使用できます。

スタッキングのセットアップ中に 1 つのスイッチがスタックマスターとして選択されます。そして、別のスタッキングメンバーをバックアップマスターとして選択することができます。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、固有のユニット ID が割り当てられます。

スイッチソフトウェアは、各スタックメンバーに個別にダウンロードされます。ただし、スタック内のすべてのユニットが同一のソフトウェアバージョンを実行している必要があります。

スイッチのスタッキングと設定は、スタックマスターに保持されています。以下の場合には、スタックマスターがポートの検出と再設定を行い、影響を最小限にとどめます。

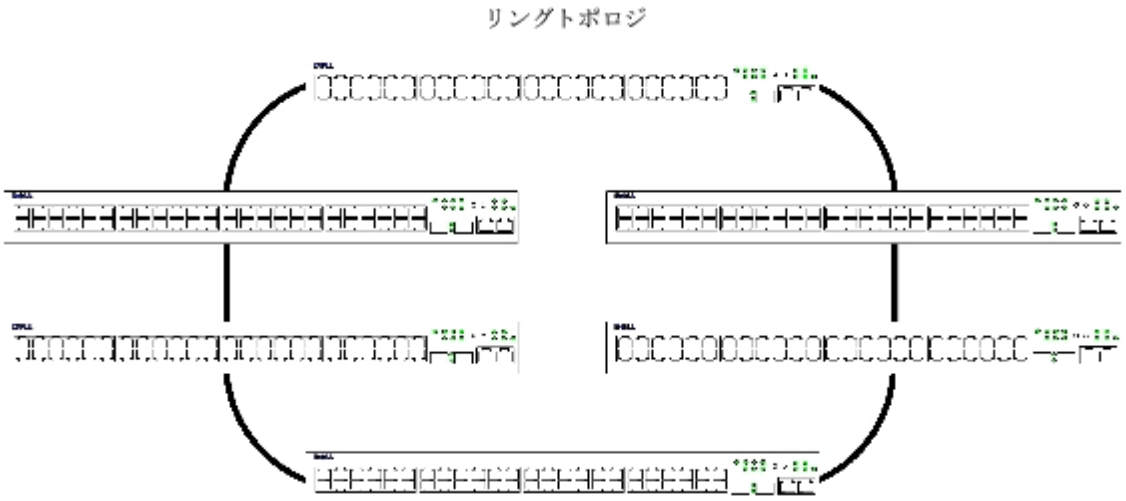
- ユニット障害
- ユニット間のスタッキングリンクの障害
- ユニットの挿入

- スタッキングユニットの取り外し

スタックトポロジについて

PowerConnect 3400 シリーズは、リングトポロジで動作します。スタックされたリングトポロジでは、スタック内のすべてのデバイスが円状に相互接続されています。スタック内の各デバイスはデータを受け入れ、接続されているデバイスに送信します。パケットは送信先に届くまでスタック内で転送されます。システムはトラフィックを送信する最適なパスを検出します。

図**1-3** リングトポロジのスタッキング



リングトポロジにおけるほとんどの問題は、リング内のデバイスが機能しなくなるか、リンクが切断された場合に発生します。**PowerConnect 3424/P** と **PowerConnect 3448/P** のスタックを使用していれば、システムは自動的にスタッキングフェイルオーバートポロジに切り替わり、ダウンタイムは発生しません。**SNMP** メッセージが自動的に生成されますが、スタック管理アクションは不要です。ただし、スタッキングの整合性を確保するために、スタッキングリンクまたはスタッキングメンバーを修復する必要があります。

スタッキングの問題が解決したら、デバイスをスタックに再接続できます。中断は発生せず、リングトポロジが回復します。

スタッキングフェイルオーバートポロジ

スタッキングトポロジで障害が発生すると、スタックはスタッキングフェイルオーバートポロジに戻ります。スタッキングフェイルオーバートポロジでは、デバイスはチェーン構成で動作します。スタックマスターはパケットの送信先を決定します。各ユニットは、最上部と最下部のユニットを除き、隣接する **2** つのデバイスに接続されます。

スタッキングメンバーとユニット **ID**

スタッキングユニット **ID** は、スタッキング構成には不可欠なものです。スタッキングの動作は、起動プロセス中に決定されます。動作モードは、初期化処理中に選択したユニット **ID** によって決定されます。たとえば、ユーザーがスタンドアロンモードを選択した場合、デバイスは起動プロセス中にスタンドアロンデバイスとして起動します。

デバイスユニットは、スタンドアロンユニットのデフォルトユニット **ID** が設定された状態で出荷されています。デバイスがスタンドアロンユニットとして動作している場合、スタッキング **LED** はすべて消灯しています。

ユーザーがいったん別のユニット **ID** を選択すると、そのユニット **ID** は消去されず、ユニットをリセットしても有効です。

ユニット ID 1 とユニット ID 2 は、マスター有効ユニット用に予約されています。3～6 のユニット ID は、スタックメンバー用に定義できます。

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もしくは削除する際に、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。

メモ： 同じユニット ID を持つメンバーが 2 台検出された場合でも、スタックは動作を続けま す。ただし、後から接続されたユニットのみがスタックに参加します。1 台のユニットがス タックに参加できなかったことを通知するメッセージがユーザーに送信されます。

スタッキングメンバーの取り外しと取り付け

ユニット 1 とユニット 2 はマスター有効ユニットです。ユニット 1 とユニット 2 は、マスターユニットまたはバックアップマスターユニットのどちらかに指定されています。スタックマスターの割り当ては、設定プロセス中に行われます。1 台のマスター有効スタックメンバーがマスターとして選択され、もう 1 台のマスター有効スタックメンバーがバックアップマスターとして選択されます。選択は以下の決定プロセスに基づいて行われます。

- スタックマスター有効ユニットが 1 台しかない場合、それがマスターとして選択されます。
- マスター有効スタッキングメンバーが 2 台あり、そのうちの 1 台がスタックマスターとして手動で設定されている場合、手動で設定されたメンバーがスタックマスターとして選択されます。
- マスター有効ユニットが 2 台あり、どちらもマスターとして手動で設定されていない場合、アップタイムが長い方がスタックマスターとして選択されます。
- マスター有効ユニットが 2 台あり、両方がマスターとして手動で設定されている場合、アップタイムが長い方がスタックマスターとして選択されます。
- 2 台のマスター有効スタッキングメンバーのアップタイムが同一の場合は、ユニット 1 がスタックマスターとして選択されます。

メモ： 挿入された時間差が 10 分以内である場合、2 台のスタッキングメンバーはアップ タイムが等しいと見なされます。

たとえば、10 分サイクルの最初の 1 分間にユニット 2 が挿入され、ユニット 1 が同一サイクルの 5 分目に挿入された場合、この 2 台のユニットはアップタイムが等しいと見なされます。アップタイムの等しいマスター有効スタックメンバーが 2 台ある場合は、ユニット 1 がマスターとして選択されます。

スタックマスターとバックアップマスターはウォームスタンバイを維持します。ウォームスタンバイにより、フェイルオーバー発生時に、バックアップマスターがスタックマスターを確実に引き継ぐことができます。これにより、スタックの正常な動作の継続が保証されます。

ウォームスタンバイ中、マスターとバックアップマスターは静的設定の場合のみに同期化されます。スタッキングマスターが設定される際に、スタックマスターはスタッキングバックアップマスターと同期化する必要があります。たとえば、動的設定は保存されず、動的に学習された MAC アドレスも保存されません。

スタックの各ポートには、特定のユニット ID、ポートタイプ、およびポート番号があります。これらは設定コマンドと設定ファイルの両方の一部をなしています。設定ファイルは、デバイススタックマスターからのみ管理できます。管理の内容は以下のとおりです。

- フラッシュへの保存
- 外部の TFTP サーバーへの設定ファイルのアップロード
- 外部の TFTP サーバーからの設定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。

再起動が行われた場合は必ず、トポロジの検出が行われ、マスターはスタック内のすべてのユニットを学習します。ユニット ID はユニット内に保存され、トポロジの検出を通じて学習されます。選択されたマスターがない状態で、あるユニットが起動を試み、そのユニットがスタンドアロンモードで動作していない場合、ユニットは起動しません。

設定ファイルは、ユーザーが設定を変更した場合にのみ変更されます。設定ファイルは、以下の場合に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
- ユニットにユニット 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の間で交互に切り替わる場合

システムが再起動するたびに、マスターユニット内の Startup Configuration ファイルが使用されて、スタックの設定が行われます。

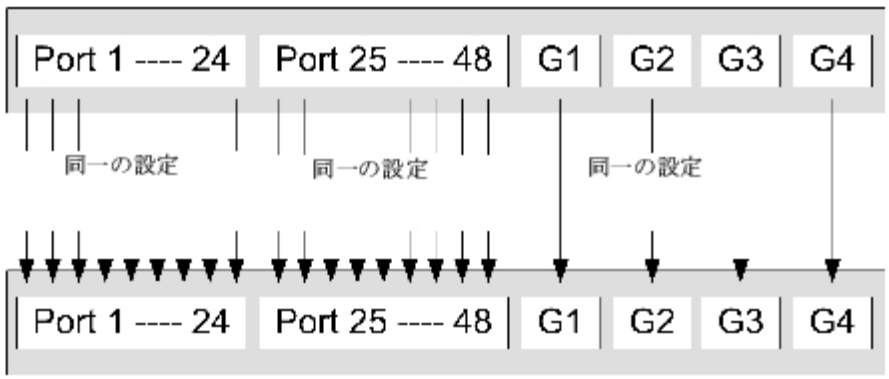
あるスタックメンバーがスタックから削除されて、同じユニット ID を持つユニットで置き換えられた場合、そのスタックメンバーは元のデバイス設定を使用して設定されます。物理的に存在するポートのみが PowerConnect OpenManage Switch Administrator のホームページに表示され、ウェブ管理システムから設定できます。存在しないポートは CLI または SNMP インタフェースから設定します。

スタックメンバーの交換

既存のスタックメンバーを同じユニット ID を持つスタックメンバーに交換する場合、挿入されたスタックメンバーにはそれまでのデバイス設定が適用されます。新しく挿入されたデバイスのポート数が以前のデバイスと比べて多いかまたは少ない場合、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。たとえば、以下のようになります。

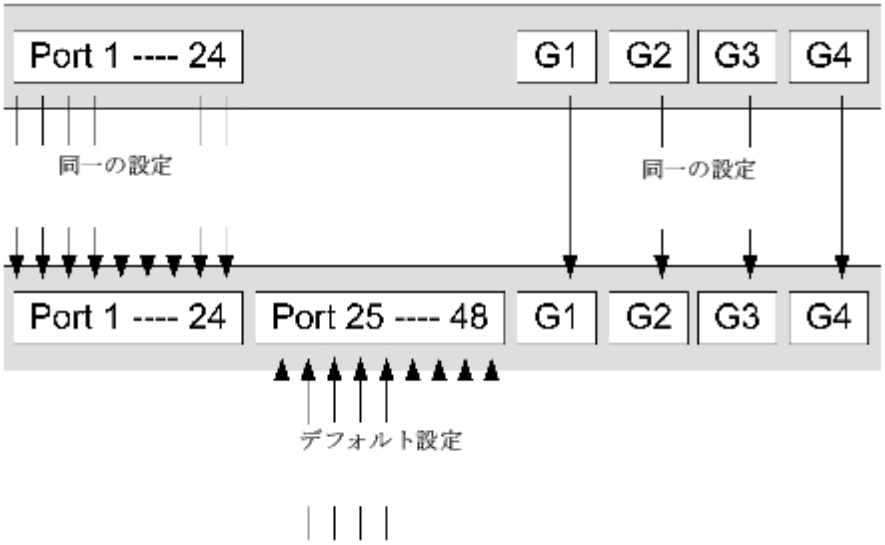
- PowerConnect 3424/P を PowerConnect 3424/P に交換する場合、ポート設定はすべて同じままです。
- PowerConnect 3448/P を PowerConnect 3448/P に交換する場合、ポート設定はすべて同じままです。

図**1-4 PowerConnect 3448/P** を **PowerConnect 3448/P** に交換する場合



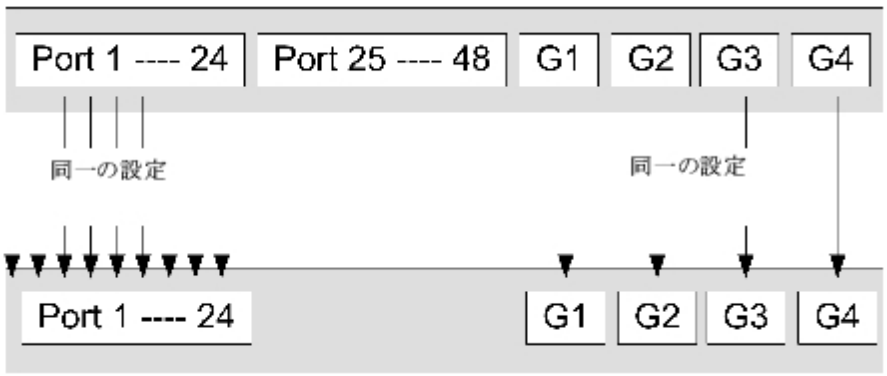
- PowerConnect 3424/P を PowerConnect 3448/P に交換する場合、3448/P の最初の 24 個の FE ポートは 3424/P の 24 個の FE ポートの設定を受け取ります。GE ポートの設定は同じままです。残りのポートはデフォルトのポート設定を受け取ります。

図**1-5 PowerConnect 3448/P** ポートを **PowerConect 3424/P** ポートに交換する場合



- PowerConnect 3448/P を PowerConnect 3424/P に交換する場合、PowerConnect 3424/P の 24 個の FE ポートは PowerConnect 3448/P の最初の 24 個の FE ポートの設定を受け取ります。GE ポートの設定は同じままです。

図**1-6 PowerConect 3424/P** ポートを **PowerConnect 3448/P** ポートに交換する場合



スタックマスターからバックアップスタックマスターへの切り替え

以下のいずれかのイベントが発生すると、スタックマスターからバックアップマスターに切り替わります。

- スタックマスターに障害が発生したか、スタックから取り外された。
- スタックマスターからスタッキングメンバーへのリンクに障害が発生した。
- ウェブインタフェースまたは CLI を介して、ソフト切り替えが行われた。

スタックマスターとバックアップマスターの間で切り替えを行うと、限定的なサービス停止が発生します。障害が発生すると、動的テーブルはすべて再学習されます。実行中の設定ファイルはスタックマスターとバックアップマスターの間で同期化され、バックアップマスター上で引き続き実行されます。

機能の概要

本項では、デバイスの機能について説明します。アップデートされたデバイスの全機能の詳細なリストについては、最新のソフトウェアバージョンの『リリースノート』を参照してください。

パワーオーバーイーサネット

パワーオーバーイーサネット（PoE）は、ネットワークインフラストラクチャのアップデートや修正を必要とせずに、既存の LAN ケーブルを介してデバイスに電力を供給する機能です。PoE により、ネットワークデバイスを電源の近くに設置する必要がなくなります。PoE には以下のような用途があります。

- IP 電話
- ワイヤレスアクセスポイント
- IP ゲートウェイ
- PDA
- オーディオとビデオのリモート監視

PoE の詳細については、「Power over Ethernetの管理」を参照してください。

ヘッドオブラインブロッキング

ヘッドオブライン（HOL）ブロッキングによって、同一の出口ポートリソースでのトラフィック競合を原因とするトラフィック遅延とフレーム消失が生じます。HOL ブロッキングはパケットをキューイングし、キュー先頭にあるパケットはキュー末尾のパケットより先に転送されます。

フロー制御のサポート（IEEE 802.3X）

フロー制御は、高速なデバイスにパケットの送信を抑制させることで、低速なデバイスと高速なデバイスとの通信を可能にします。バッファーオーバーフローを防ぐために、送信は一時的に中断されます。

ポートまたは LAG に対するフロー制御の設定情報については、「ポート設定の定義」または「LAG パラメータの定義」を参照してください。

バックプレッシャーサポート

半二重リンクにおいて、受信ポートはリンクを占有してそれ以後のトラフィックに対して利用不能にすることで、バッファオーバーフローを防止します。

ポートまたは LAG に対するフロー制御の設定情報については、「ポート設定の定義」または「LAG パラメータの定義」を参照してください。

仮想ケーブルテスト（VCT）

VCT は、ケーブル断線やケーブル短絡など、銅線リンクでのケーブル障害を検出し、報告します。ケーブルテストの詳細については、「ケーブル診断の実行」を参照してください。

MDI/MDIX のサポート

自動ネゴシエーションを有効に設定していると、RJ-45 ポートに接続されているケーブルがクロスかストレートかをデバイスが自動的に識別します。

エンドステーションの標準配線は **Media-Dependent Interface**（MDI）で、ハブとスイッチに使用する標準配線は **Media-Dependent Interface with Crossover**（MDIX）として知られています。

ポートまたは LAG に対する MDI/MDIX の設定情報については、「ポート設定の定義」または「LAG パラメータの定義」を参照してください。

自動ネゴシエーション

自動ネゴシエーションによって、デバイスは動作モードを通知することができます。自動ネゴシエーション機能によってポイントツーポイントリンクセグメントを共有する 2 台のデバイス間には情報を交換する手段が与えられ、両方のデバイスはそれぞれの伝送能力のメリットを最大限に生かすように自動的に設定されます。

PowerConnect 3400 シリーズは、ポート通知機能によって自動ネゴシエーション機能を向上させます。ポート通知によって、システム管理者は通知されたポートスピードを設定できます。

自動ネゴシエーションの詳細については、「ポート設定の定義」または「LAG パラメータの定義」を参照してください。

MAC アドレス対応機能

MAC アドレスキャパシティサポート

デバイスは最大 8 K の MAC アドレスをサポートしています。また、システム用に特定の MAC アドレスを予約しています。

静的 MAC エントリ

受信フレームから学習する代わりに、MAC エントリをブリッジテーブルに手動で入力することもできます。ユーザー定義のこれらのエントリは、エージングの影響を受けず、リセットや再起動の後も保存されます。

詳細については、「静的アドレスの定義」を参照してください。

MAC アドレスの自己学習

デバイスは、受信パケットに基づいて MAC アドレスを自動的に学習します。MAC アドレスはブリッジテーブルに格納されます。

MAC アドレスの自動エージング

指定された時間にわたってそこからのトラフィックが受信されない MAC アドレスは、エージアウト（削除）されます。これはブリッジテーブルのオーバーフローを防止するためです。

MAC アドレスのエージアウトタイムを設定する手順の詳細については、「動的アドレスの表示」を参照してください。

VLAN 対応 MAC ベーススイッチング

デバイスは常に VLAN に対応したブリッジ処理を実行します。送信先 MAC アドレスのみに基づいてフレームを転送する旧来のブリッジ処理（IEEE 802.1D）は実行されません。ただし、タグなしフレームに対して同様の機能を設定することは可能です。どのポートにも関連付けられていない、送信先の MAC アドレス向けフレームは、関連する VLAN のすべてのポートにフラッドされます。

MAC マルチキャストサポート

マルチキャストサービスは限定的なブロードキャストサービスであり、情報配信用に 1 対多、および多対多の接続を可能にします。レイヤー 2 マルチキャストサービスでは、シングルフレームが特定のマルチキャストアドレスに送られます。そこから、フレームのコピーが関連ポートに送信されます。

詳細については、「マルチキャストすべて転送パラメータの割り当て」を参照してください。

レイヤー 2 の機能

IGMP スヌーピング

IGMP スヌーピングは IGMP フレームの内容をデバイスがワークステーションからアップストリームマルチキャストルーターに転送する時に、その内容を検査します。フレームから、デバイスはマルチキャストセッション向けに設定されたワークステーションを識別します。そのマルチキャストセッションは、マルチキャストルーターがマルチキャストフレームに送信するものです。

詳細については、「IGMP スヌープ」を参照してください。

ポートミラーリング

ポートミラーリングは、監視対象のポートから監視する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リングを行います。指定されたソースポートを通過する全トラフィックのコピーを受け取るターゲットポートを指定することが可能です。

詳細については、「ポートミラーリングセッションの定義」を参照してください。

ブロードキャストストーム制御

ストーム制御は、デバイスが受け取り転送するマルチキャストフレームとブロードキャストフレームの量を制限します。

レイヤー 2 のフレームが転送される場合、ブロードキャストフレームとマルチキャストフレームは、関連する VLAN 上のすべてのポートにフラッドされます。これは帯域幅を占有し、接続されている全ノードをすべてのポートにロードします。

詳細については、「ストーム制御の有効化」を参照してください。

VLAN 対応機能

VLAN のサポート

VLAN は単一ブロードキャストドメインを構成するスイッチングポートの集合です。パケットは、VLAN タグに基づいて、または入口ポートとパケットコンテンツとの組合せに基づいて、VLAN に属するものとして分類されます。共通の属性を持つパケットは、同一の VLAN 内にグループ化できます。

詳細については、「VLAN の設定」を参照してください。

ポートベースの仮想 LAN（VLAN）

ポートベースの VLAN は入口ポートに基づいて受信パケットを VLAN に分類します。

詳細については、「VLAN ポート設定の定義」を参照してください。

Full 802.1Q VLAN のタギング準拠

IEEE 802.1Q には、仮想ブリッジ接続された LAN のアーキテクチャ、VLAN で提供されるサービス、およびそれらのサービスの供給に関係するプロトコルとアルゴリズムが定義されています。

GVRP のサポート

GARP VLAN 登録プロトコル （GVRP: GARP VLAN Registration Protocol）は、IEEE 802.1Q 準拠 VLAN のプルーニング、および802.1Q トランクポートでのダイナミック VLAN の作成を可能にします。GVRP が有効に設定されていると、デバイスは、基礎をなすアクティブな スパニングツリープロトコルの機能 トポロジの一部であるすべてのポート上の VLAN メンバーシップを登録し、伝搬します。

詳細については、「GVRP パラメータの設定」を参照してください。

プライベート VLAN

プライベート VLAN ポート、レイヤー 2 のセキュリティ機能は、同一のブロードキャストドメイン内のポート間を分離します。

プライベート VLAN の詳細については、「プライベート VLAN の設定」を参照してください。

スパニングツリープロトコルの機能

スパニングツリープロトコル（STP）

802.1d スパニングツリーは標準のレイヤー 2 スイッチの要件で、これにより、ブリッジは L2 転送ループを自動的に回避し、解決することができます。スイッチは、専用フォーマットのフレームを使用して設定メッセージを交換し、ポート上の転送を選択的に有効および無効にすることができます。

詳細については、「スパニングツリープロトコルの設定」を参照してください。

Fast Link（高速リンク）

STP の収束には、最長で 30～60 秒かかることがあります。この間、STP は可能なループを検出することで、ステータスの変化が伝搬し、関連するデバイスが応答する時間を与えます。30～60 秒という応答時間は、多くのアプリケーションで長すぎると考えられます。Fast Link（高速リンク）オプションではこの遅延が回避されており、転送ループが発生しないネットワークトポロジで使用できます。

ポートと LAG 用に Fast Link（高速リンク）を有効化する手順の詳細については、「STP ポート設定の定義」または「静的アドレスの定義」を参照してください。

IEEE 802.1w 高速スパニングツリー

スパニングツリーでは、各ホストがそのポートがアクティブにトラフィックを転送しているかどうかを判断するために、30～60 秒かかることがあります。高速スパニングツリー（RST: Rapid Spanning Tree）は、転送ループを作成することなく、収束の時間短縮を可能にするネットワークトポロジの使用を検出します。

詳細については、「高速スパニングツリーの設定」を参照してください。

IEEE 802.1s 多重スパニングツリー

多重スパニングツリー（MST）の動作により、VLAN が STP インスタンスにマップされます。MSTP は異なる負荷分散シナリオを提供します。さまざまな VLAN に割り当てられたパケットが、MSTP 領域（MST 領域）内の異なるパスで送信されます。領域は、フレームを転送できる 1 つまたは複数の MSTP ブリッジです。標準により、管理者は VLAN トラフィックを固有のパスに割り当てることができます。

詳細については、スパニングツリープロトコルの設定 を参照してください。

リンク集約

リンク集約

最大 8 つの集約リンクを定義して、それぞれに最大 8 つのメンバーポートを与えて、単一のリンク集約グループ（LAG: Link Aggregated Group）を形成することが可能です。これにより、以下のことが可能になります。

- リンクの物理的な障害に対するフォールトトレランス保護
- 広帯域接続
- 帯域粒度の改善
- 広帯域サーバー接続

LAG は全二重方式動作に設定されている同じ速度のポートで構成します。

詳細については、「LAG パラメータの定義」を参照してください。

リンク集約と LACP

LACP はリンク全体にピアエクスチェンジを使用して、さまざまなリンクの集約能力を継続的に判断し、所定のデバイスペアの間で達成可能な集約能力の最大レベルを継続的に示します。LACP は、システム内のポートバインディングの判断、設定、バインド、監視を自動的に行います。

詳細については、「ポートの集約」を参照してください。

BootP と DHCP クライアント

DHCP を使用すると、システムの起動時に、ネットワークサーバーから追加設定パラメータを受信できるようになります。DHCP サービスは継続的なプロセスです。DHCP はBootP の拡張版です。

DHCP の詳細については、「DHCP IP インタフェースパラメータの定義」を参照してください。

クオリティオブサービスの機能

Class of Service（クラスオブサービス）802.1p のサポート

IEEE 802.1p 信号方式はOSI のレイヤー 2 標準の 1 つで、データリンク / MAC サブレイヤーでネットワークトラフィックのマーキングと優先順付けを行います。802.1p トラフィックは分類分けされ、送信先に送信されます。いかなる帯域予約や制限も規定または強制されません。802.1p は 802.1Q（VLAN）標準の派生機能です。802.1p は IP Precedence（IP 優先度）IP ヘッダのビットフィールドと同様、8 レベルの優先順位を確立します。

詳細については、「サービス品質の設定」を参照してください。

デバイス管理機能

SNMP アラームとトラップログ

システムは、重大度コードとタイムスタンプ付きでイベントを記録します。イベントは、Trap Recipient List（トラップ受信者リスト）に SNMP トラップとして送信されます。

SNMP アラームとトラップの詳細については、「SNMP パラメータの定義」を参照してください。

SNMP バージョン 1、2 および 3

SNMP（Simple Network Management Protocol）は UDP/IP プロトコルを越えてシステムへのアクセスを制御し、コミュニティエントリの一覧が定義されます。各エントリはコミュニティストリングとそのアクセス権で構成されます。SNMP セキュリティには、読み取り専用、読み書き、スーパーの 3 レベルがあります。コミュニティテーブルにアクセスできるのは、スーパーユーザーのみです。

詳細については、「SNMP パラメータの定義」を参照してください。

Web ベースの管理

Web ベースの管理により、システムは任意の Web ブラウザから管理できます。システムには、システムのモニタと設定が可能な HTML ページを出力する埋め込み Web サーバー（EWS）が内蔵されています。システムは Web ベースの入力を、設定コマンド、MIB 変数設定、およびその他の管理関係の設定に内部で変換します。

設定ファイルのダウンロードとアップロード

デバイスの設定は設定ファイルに保存されます。設定ファイルには、システム全体とポート固有のデバイス設定が含まれています。システムは、設定ファイルを CLI コマンドの集まりの形で表示することができます。CLI コマンドは、テキストファイルとして保存され、操作されます。

詳細については、「ファイルの管理」を参照してください。

TFTP（Trivial File Transfer Protocol）

デバイスは、TFTP を介した、ブートイメージ、ソフトウェア、および設定のアップロードとダウンロードをサポートします。

リモート監視

リモート監視 （RMON）は SNMP の拡張版で、包括的なネットワークトラフィック 監視機能を提供します（ネットワークデバイスの管理と監視を可能にする SNMP の逆）。RMON は現在と過去の MAC レイヤー統計情報と制御オブジェクトを定義し、ネットワーク全体でリアルタイムな情報キャプチャを可能にする標準 MIB です。

詳細については、「統計の表示」を参照してください。

コマンドラインインタフェース

コマンドラインインタフェース（CLI）のシンタックスとセマンティクスは、業界の一般慣行にできるだけ準拠しています。CLI は強制的要素とオプション的要素で構成されています。CLI インタープリタは、ユーザーを支援し、入力を短縮するためのコマンドコンプリーションとキーワードコンプリーションを提供します。

Syslog

Syslog は、イベント通知を一連のリモートサーバーに送ることを可能にするプロトコルです。イベント通知は、リモートサーバーで保存、検討し、対策を実行することができます。システムは重要なイベントの通知をリアルタイムで送信し、それらのイベントの記録を事後に使用するためにとっておきます。

Syslog の詳細については、「ログの管理」を参照してください。

SNTP

SNTP（Simple Network Time Protocol）は、ネットワーク Ethernet スイッチクロックタイム同期化の精度をミリ秒まで保証します。時刻の同期化は、ネットワークの SNTP サーバーによって実行されます。タイムソースは層によって定められています。層は、リファレンスクロックからの距離を定義します。層が高いほど（ゼロが最高）、クロックの精度は高くなります。

詳細については、「SNTP の設定」を参照してください。

ドメインネームシステム

ドメインネームシステム（DNS）は、ユーザー定義のドメインネームを IP アドレスに変換します。ドメインネームが割り当てられるたびに、DNS サービスは名前を数字の IP アドレスに変換します。たとえば、www.ipexample.com は 192.87.56.2 に変換されます。DNS サーバーはドメインネームのデータベースと対応する IP アドレスを保持します。

詳細については、"ドメインネームシステムの設定" を参照してください。

トレースルート

トレースルートは、転送プロセス中にパケットの転送に使われた IP ルートを検出します。CLI トレースルートユーティリティは、user-exec モードまたは特権モードのどちらからでも実行できます。

セキュリティ機能

SSL

セキュアソケットレイヤー（SSL）は、プライバシー、認証、およびデータの整合性を保護しながらデータの安全なトランザクションを可能にするアプリケーションレベルのプロトコルです。このプロトコルは、証明書、パブリックキー、およびプライベートキーを頼りにセキュリティを確保します。

ポートベースの認証（802.1x）

ポートベースの認証により、外付けサーバーを介して、ポート単位でシステムユーザーを認証することができます。認証済みの認可されたシステムユーザーのみがデータを送受信できます。ポートは、EAP（Extensible Authentication Protocol）を使用して、RADIUS（Remote Authentication Dial In User Service）サーバーを介して認証されます。

詳細については、「ポートベース認証の設定」を参照してください。

Locked Port のサポート

Locked Port（ポートロック）は、特定ポートへのアクセスを特定の MAC アドレスを持つユーザーのみに制限することで、ネットワークセキュリティを高めます。これらのアドレスは手動で定義されるか、そのポートで学習されます。ロックされたポート上にフレームが見られ、フレームソースの MAC アドレスがそのポートに関連付けられていない場合に、プロテクションメカニズムが起動します。

詳細については、「ポートセキュリティの設定」を参照してください。

RADIUS Client

RADIUS はクライアント / サーバーベースのプロトコルです。RADIUS サーバーはユーザーデータベースを保持します。このデータベースには、ユーザー名、パスワード、およびアカウント情報などのユーザー単位の認証情報が含まれています。

詳細については、「RADIUS の設定」を参照してください。

SSH

SSH（Secure Shell）は、デバイスへの安全なリモート接続を提供するプロトコルです。SSH バージョン 2 は、現在サポートされています。SSH サーバーの機能により、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。この接続は、着信 telnet 接続に似た機能を提供します。SSH は、デバイスの接続と認証に RSA および DSA Public Key 暗号法を使用します。

TACACS+

TACACS+ は、デバイスにアクセスするユーザーの検証に集中的なセキュリティを提供します。TACACS+ は集中的なユーザー管理システムを提供する一方で、RADIUS およびその他の認証プロセスとの一貫性も保持します。

詳細については、「TACACS+ 設定の定義」を参照してください。

パスワード管理

パスワード管理により、ネットワークセキュリティとパスワード制御が向上します。SSH、Telnet、HTTP、HTTPS、および SNMP アクセスのパスワードには、セキュリティ機能が割り当てられています。パスワード管理の詳細については、「パスワードの管理」を参照してください。

CLI のその他のマニュアル

『Documentation CD』に収録されている『CLI Reference Guide』（CLI リファレンスガイド）では、デバイスの設定に使用する CLI コマンドについて説明しています。同書では、コマンドの記述、シンタックス、デフォルト値、ガイドラインについて、例を挙げて説明しています。

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™ 34XX システム ユーザーズガイド

ポートについて

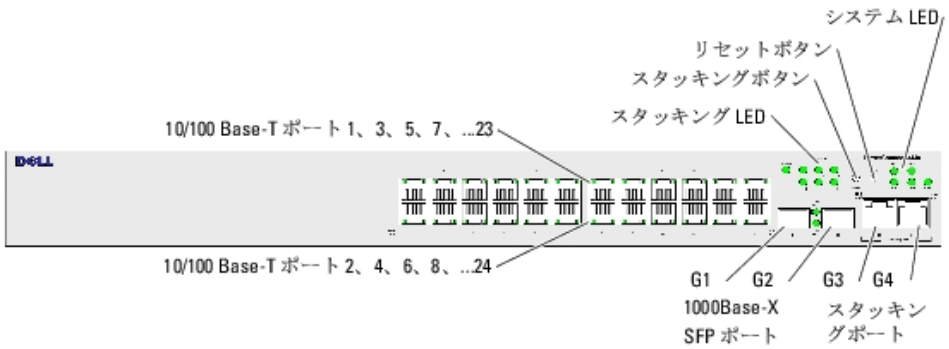
PowerConnect 3424 のポートについて

PowerConnect 3424 デバイスには、以下のポートが装備されています。

- **24** 個の **Fast Ethernet** ポート — 10/100Base-T ポートに指定された RJ-45 ポート
- **2** つのファイバーポート — 1000Base-X SFP ポートに指定
- **2** つの **Gigabit** ポート — 1000Base-T ポートに指定
- コンソールポート — RS-232 ベースのポート

PowerConnect 3424 の正面パネルを以下の図に示します。

図 **2-1 PowerConnect 3424** の正面パネル



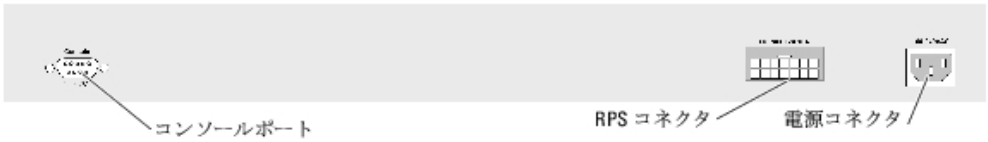
正面パネルには、番号 1～24 の RJ-45 ポート 24 個が装備されています。上段のポートには 1～23 の奇数番号が、下段のポートには 2～24 の奇数番号が記されています。また、正面パネルにはファイバーポート（G1～G2）と銅線ポート（G3～G4）もあります。ポート G3～G4 は、スタッキングポートとしても、または、スタンドアロンデバイス内のネットワークトラフィックを転送するためにも使用できます。

正面パネルには 2 つのボタンがあります。スタック ID ボタンは、ユニット番号を選択するために使用します。2 番目のボタンはリセットボタンで、デバイスを手動でリセットするために使用します。リセットボタンは、誤って押してしまうことがないように、デバイスの正面パネルの表面から突き出ない構造になっています。すべてのデバイス LED が正面パネルにあります。

次の図は PowerConnect 3424 の背面図です。

図**2-2 PowerConnect 3424** 背面パネル

背面パネルには、RPS コネクタ、コンソールポート、電源コネクタが装備されています。



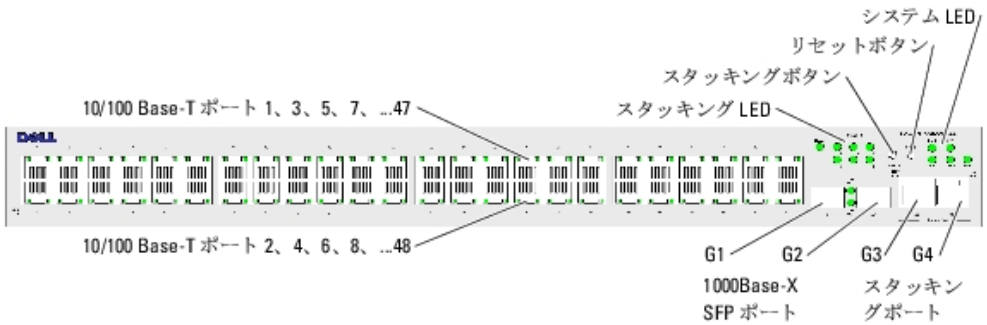
PowerConnect 3448 のポートについて

PowerConnect 3448 デバイスには、以下のポートが装備されています。

- **48** 個の **FE** ポート — 10/100Base-T ポートに指定されている RJ-45 ポート
- **2** つの **Fiber** ポート — 1000Base-X SFP ポートに指定
- **2** つの **Gigabit** ポート — 1000Base-T ポートに指定
- コンソールポート — RS-232 コンソールベースのポート

PowerConnect 3448 の正面パネルを以下の図に示します。

図**2-3 PowerConnect 3448** の正面パネル



正面パネルには、番号 1～48 の RJ-45 ポート 48 個が装備されています。上段のポートには 1～47 の奇数番号が、下段のポートには 2～48 の奇数番号が記されています。また、正面パネルにはファイバーポート（G1～G2）と銅線ポート（G3～G4）もあります。ポート G3～G4 は、スタッキングポートとしても、または、スタンドアロンデバイス内のネットワークトラフィックを転送するためにも使用できます。

正面パネルには 2 つのボタンがあります。スタック ID ボタンは、ユニット番号を選択するために使用します。2 番目のボタンはリセットボタンで、デバイスを手動でリセットするために使用します。リセットボタンは、誤って押してしまうことがないように、デバイスの正面パネルの表面から突き出ない構造になっています。すべてのデバイス LED が正面パネルにあります。

次の図は PowerConnect 3448 の背面パネルを示したものです。

図**2-4 PowerEdge 3448** 背面パネル

背面パネルには、RPS コネクタ、コンソールポート、電源コネクタが装備されています。

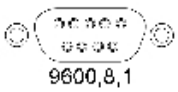
SFP ポート

SFP（Small Form Factor Pluggable）ポートは、1000Base-SX または LX に指定されている CPLD（Complex Programmable Logic Device）を介した通信用の TWSI（Two-Wire Serial Interface）です。

RS-232 コンソールポート

ターミナル接続用の DB-9 コネクタの 1 つは、デバッグ、ソフトウェアのダウンロードなどに使用されます。デフォルトのボーレートは 9,600 bps です。ボーレートは、2400 bps から最大 115,200 bps まで設定可能です。

図2-5 コンソールポート



寸法

PowerConnect 3424/P デバイスと PowerConnect 3448/P デバイスの寸法は次のとおりです。

PoE モデル:

- 幅 — 440 mm
- 奥行 — 387 mm
- 高さ — 43.2 mm

非 PoE デバイス:

- 幅 — 440 mm
- 奥行 — 257 mm
- 高さ — 43.2 mm

LED の定義

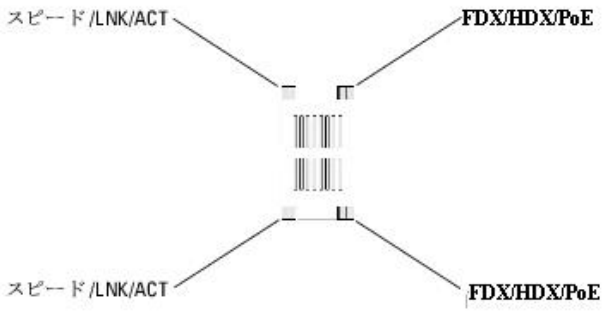
正面パネルには、リンク、電源、ファン、システム診断プログラムのそれぞれの状態を示す LED（発光ダイオード）が装備されています。

ポート LED

10/100/1000 Base-T の各ポートおよび 10/100 Base-T ポートには、それぞれ 2 つの LED がついています。スピード LED はポートの左側、 リンク / デュプレックス / アクティビティ LED は右側にあります。

次の図は、PowerConnect 3424 /P スイッチおよび PowerConnect 3448/P スイッチの 10/100 Base-T ポート LED を示したものです。

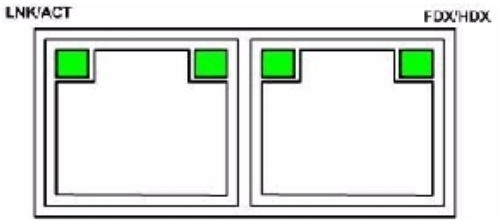
図2-6 RJ-45 銅ベース 10/100 BaseT LED



PowerConnect 3424 /P および PowerConnect 3448/P の RJ-45 100 Base-T ポートには、LNK/ACT とマークされた LED が 2 つあります。

次の図は、100 Base-T LED を示したものです。

図**2-7 RJ-45 1000 BaseT LED**



PowerConnect 3424 と PowerConnect 3448 における RJ-45 LED 表示の意味は、次のとおりです。

表**2-1 PowerConnect 3424** と **PowerConnect 3448 RJ-45 100BaseT LED** 表示

LED	色	説明
LNK/ACT/スピード	緑色点灯	ポートは 100 Mbs で動作している。
	緑色点滅	ポートは 100 Mbps でデータを送信または受信している。
	黄色点灯	ポートは 10 Mbs で動作している。
	黄色点滅	ポートは 10 Mbps でデータを送信または受信している。
	消灯	ポートは現在動作していない。
FDX	緑色点灯	ポートは現在、全二重モードで動作している。
	消灯	ポートは現在、半二重モードで動作している。

PowerConnect 3424P と PowerConnect 3448P における RJ-45 LED 表示の意味は、次のとおりです。

表**2-2 PowerConnect 3424P** と **PowerConnect 3448P RJ-45** 銅ベース **100BaseT LED** 表示

LED	色	説明
スピード/LNK/ACT	緑色点灯	ポートは現在、100 Mbps でリンクしている。
	緑色点滅	ポートは現在、100 Mbps で動作している。
	消灯	ポートは現在、10 Mbps で動作しているか、またはリンクされていない。
PoE	緑色点灯	PD（Powered Device）が検出され、常用負荷で動作している。PD の詳細については、「Power over Ethernetの管理」を参照してください。
	橙色点灯	PD に過負荷またはショートが発生した。PoE 障害の詳細については、「Power over Ethernetの管理」を参照してください。

	橙点滅	PD のパワーコンセプションが既定の電力割当を超えている。PoE の電力割当の詳細については、「Power over Ethernetの管理」を参照してください。
	消灯	PD が検出されていない。

Gigabit ポートの LED

次の表では、Gigabit（スタッキングポート）の LED について説明します。

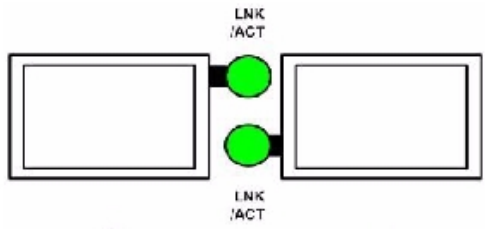
表**2-3 PowerConnect 3424** と **PowerConnect 3448 RJ-45** の銅ベース **100BaseT LED** 表示

LED	色	説明
LNK/ACT/スピード	緑色点灯	ポートは 1000 Mbs で動作している。
	緑色点滅	ポートは 1000 Mbps でデータを送信または受信している。
	黄色点灯	ポートは 10 または 100 Mbs で動作している。
	黄色点滅	ポートは 10 Mbps または 100 Mbps でデータを送信または受信している。
	消灯	ポートは現在動作していない。
FDX	緑色点灯	ポートは現在、全二重モードで動作している。
	消灯	ポートは現在、半二重モードで動作している。

SFP LED

各SFP ポートには、LNK/ACT とマークされた LED が 1 つずつあります。PowerConnect 3424/P デバイスと PowerConnect 3448/P デバイスでは、LED はポートの間にあり、丸い形をしています。次の図は、各デバイスの LED を示したものです。

図**2-8 SFP** ポートの **LED**



SFP ポート の LED 表示の意味は次のとおりです。

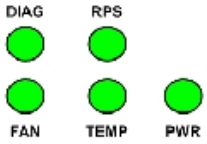
表**2-4 SFP** ポートの **LED** 表示

LED	色	説明
LNK/ACT	緑色点灯	リンクが確立されている。
	緑色点滅	ポートは現在、データを送信または受信している。
	消灯	ポートは現在リンクしていない。

システム LED

PowerConnect 3424 /P デバイスと PowerConnect 3448/P デバイスのシステム LED は、電源、ファン、温度状態、診断プログラムに関する情報を提供します。次の図は、システム LED を示したものです。

図**2-9** システム **LED**



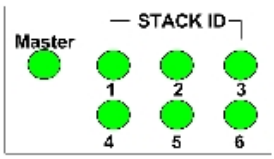
システム LED の表示の意味は次のとおりです。

表**2-5** システム **LED** のインジケータ

LED	色	説明
電源装置（PWR）	緑色点灯	スイッチは電源オンになっている。
	消灯	スイッチは電源オンになっていない。
冗長電源装置（RPS） （モデル：3424 および 3448）	緑色点灯	RPS は現在、動作している。
	赤色点灯	RPS が不良。
	消灯	冗長電源装置が接続されていない。
冗長電源装置（RPS） （モデル：3424P および 3448P）	緑色点灯	RPS は現在、動作している。
	消灯	冗長電源装置が故障したか、または接続されていない。
診断プログラム（DIAG）	緑色点滅	システム診断テストが現在実行中。
	緑色点灯	システム診断テストが成功した。
	赤色点灯	システム診断テストが失敗した。
	消灯	システムは正常に動作している。
温度（TEMP）	赤色点灯	デバイスの温度が許容範囲を超えた。
	消灯	デバイスは許容温度範囲内で動作している。
ファン（FAN）	緑色点灯	すべてのデバイスのファンが正常に動作している。
	赤色点灯	1 つまたは複数のデバイスのファンが動作していない。

スタッキング LED は、スタック内のデバイスの位置を示します。次の図は、正面パネルの LED を示したものです。

図**2-10** スタッキング **LED**



スタッキング LED には、1～6 の番号が割り当てられています。各スタッキングユニットは、スタッキング LED のうち 1 つを点灯することで、ユニット ID 番号を示します。スタッキング LED 1 または 2 のどちらかが点灯している場合、そのデバイスがスタックマスターまたはバックアップマスターのどちらかであることを示しています。

表**2-6** スタッキング **LED** の表示

LED	色	説明
すべてのスタッキング LED	消灯	スイッチは現在、スタンドアロンデバイスです。
スタッキング LED 1～6（S1～S6）	緑色点灯	デバイスはスタッキングユニット N に指定されています。
	消灯	デバイスはスタッキングユニット N に指定されていません。
スタックマスター LED	緑色点灯	デバイスはスタックマスターです。
	消灯	デバイスはスタックマスターです。

電源装置

デバイスには内蔵電源ユニット（AC ユニット）とコネクタが搭載されています。コネクタは、PowerConnect 3424/P デバイスと PowerConnect 3448/P デバイスを PowerConnect EPS-470 ユニットに、または PowerConnect 3424 デバイスと PowerConnect 3448 デバイスを PowerConnect RPS-600 ユニットに接続します。PowerConnect 3424/P デバイスと PowerConnect 3448/P デバイスには、内蔵電源（12 V）が搭載されています。

両方の電源ユニットを使用する動作は、負荷分散によって調整されます。電源 LED は、電源装置の状態を示します。

PowerConnect 3424/P デバイス と PowerConnect 3448/P デバイスには 470 W（12 V/-48 V）の内蔵電源が搭載されており、24 ポート PoE デバイスに合計 370 W を提供します。

AC 電源ユニット

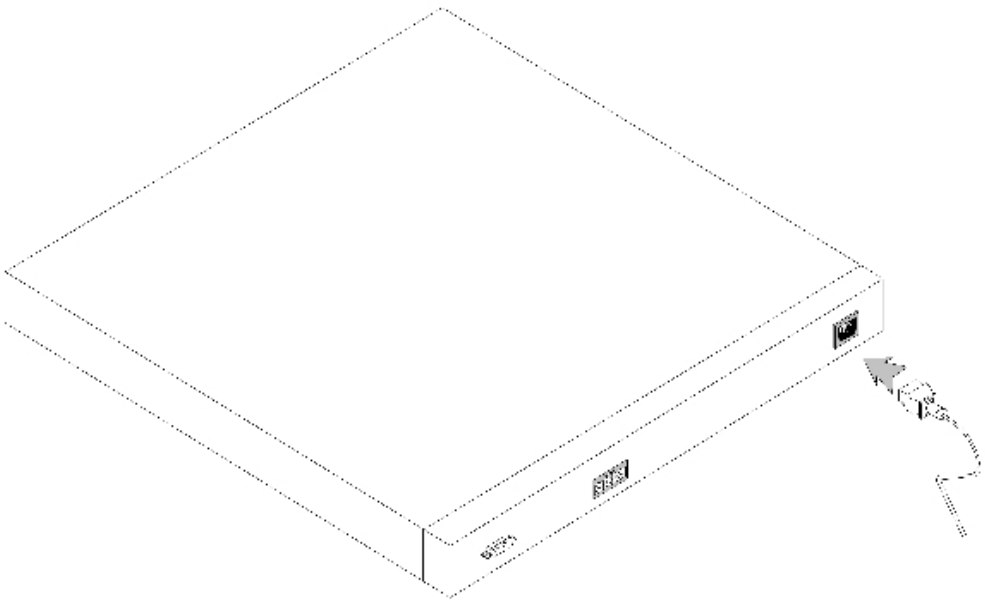
AC 電源ユニットは AC 90～264 V、47～63 Hz で動作します。AC 電源ユニットでは、標準コネクタを使用します。LED インジケータは正面パネルにあり、AC ユニットが接続されているかどうかを示します。

DC 電源ユニット

PowerConnect 3424 スイッチと PowerConnect 3448 スイッチは、外付けの RPS-600 ユニットに接続して冗長電源オプションを利用することができます。設定は不要です。正面パネルの "RPS" LED は、外付けの RPS-600 が接続されているかどうかを示します。RPS LED の定義については、表 2-5 を参照してください。

PowerConnect 3424/P スイッチと PowerConnect 3448/P スイッチは、外付けの EPS-470 ユニットに接続して冗長電源オプションを利用することができます。設定は不要です。正面パネルの "RPS" LED は、外付けの EPS-470 が接続されているかどうかを示します。RPS LED の定義については、表 2-5 を参照してください。

図2-11 電源の接続



デバイスが別の電源に接続されている場合、停電による障害の確率は低下します。

スタック ID ボタン

デバイスの正面パネルにはスタック ID ボタンがあります。このボタンはスタックマスターとメンバーのユニット ID を手動で選択するために使用します。

スタックマスターとメンバーは、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。15 秒以内にスタックマスターを選択しないと、デバイスはスタンドアロンモードで起動します。デバイスのユニット ID を選択するには、デバイスを再起動します。

スタックマスターは、1 または 2 のユニット ID を受け取ります。ユニット 1 とユニット 2 の両方が存在する場合、選択されていないユニットはバックアップマスターとして機能します。スタックマスターは別のユニット ID（3～6）を受け取ります。たとえば、スタック内に 4 台のユニットがある場合、マスターユニットは 1 または 2 のいずれか、バックアップマスターは 1 または 2 のいずれか（マスターユニットのユニット ID がどちらになるかで決まります）、3 つ目のメンバーは 3、4 つ目のスタックメンバーは 4 となります。

メモ： デバイスはスタンドアロンユニットを自動的に検出しません。ユニット ID の 1 つが選 択済みの場合は、点灯するスタッキング LED がなくなるまでスタック ID ボタンを数回押して ください。

リセットボタン

PowerConnect 3424/P スイッチと PowerConnect 3448/P スイッチには、正面パネルにリセットボタンがあります。このボタンは、デバイスを手動でリセットする際に使用します。マスターデバイスをリセットすると、スタック全体がリセットされます。1 台のメンバーユニットのみをリセットした場合、残りのスタッキングメンバーはリセットされません。

スイッチのシングルリセット回路は、パワーアップまたは低電圧状態でアクティブになります。

放熱システム

PoE 機能を備えた PowerConnect 3424/P スイッチと PowerConnect 3448/P スイッチには、内蔵ファンが 5 つ装備されています。非 PoE PowerConnect 3424 デバイスと PowerConnect 3448 デバイスには、内蔵ファンが 2 つ装備されています。動作は LED で確認できます。1 つまたは複数のファンに障害が発生すると、LED が障害を知らせます。

メモ、注意および警告

メモ、注意および警告

PowerConnect 3424/P と PowerConnect 3448/P の設置

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

設置場所の準備

PowerConnect 3424 /P デバイスと PowerConnect 3448/P デバイスは、テーブルの上または壁に設置した標準の 48.26 cm ラックに設置することができます。ユニットを設置する前に、設置場所が以下の要件を満たしていることを確認します。

- 電源 — ユニットの電源ケーブルが届く範囲内に AC 100～240 V、50/60 Hz のコンセントがあること。
- 全般 — 冗長電源が正しく取り付けられていること（正面パネルの LED の点灯を点検）。
- **PoE** モデル — RPS は現在、正面パネルの PoE LED が点灯することを確認して取り付けられています。
- スペース — オペレータの適切な作業に必要な空間を確保してください。ケーブル配線、電源接続、および放熱用の空間を確保してください。
- ケーブル配線 — 無線機、通信用の増幅器、電力線、蛍光灯取り付け器具などの電気的ノイズの発生源を避けて、ケーブルが配線されていること。
- 環境要件 — 動作時の周囲温度の範囲は 0～50℃、相対湿度は 95% 以下で結露しないこと。

開梱

パッケージの内容

デバイスの梱包を解き以下の同梱品が揃っていることを確認します。

- デバイス / スイッチ
- AC 電源ケーブル
- RS-232 クロスケーブル
- 粘着ゴムパッド
- ラック取り付けキット（ラック取り付け用）または壁取り付けキット
- マニュアル CD
-

製品情報ガイド

デバイスの開梱

メモ： 開梱する前に包装を調べて、損傷がある場合は、すぐにご連絡ください。

□□□ 箱をきれいで平らな面に置きます。

□□□ 箱を開けるか、箱の上部を取り外します。

□□□ デバイス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。

□□□ すべての梱包材を取り除きます。

□□□ デバイスとアクセサリに損傷がないか点検します。損傷がある場合は、すぐにご連絡 ください。

デバイスの設置

PowerConnect 3424/P デバイスと PowerConnect 3448/P デバイスは、以下に説明する手順で設置します。コンソールポートは背面パネルにあります。電源コネクタは背面パネルにあります。RPS（冗長電源装置）はオプションですが、取り付けることをお勧めします。RPS コネクタはデバイスの背面パネルにあります。

ラックへの設置

警告： スイッチに接続されている、またはスイッチをサポートするデバイスの安全情報については、『製品情報ガイド』に記載されている安全に関する注意をお読みください。

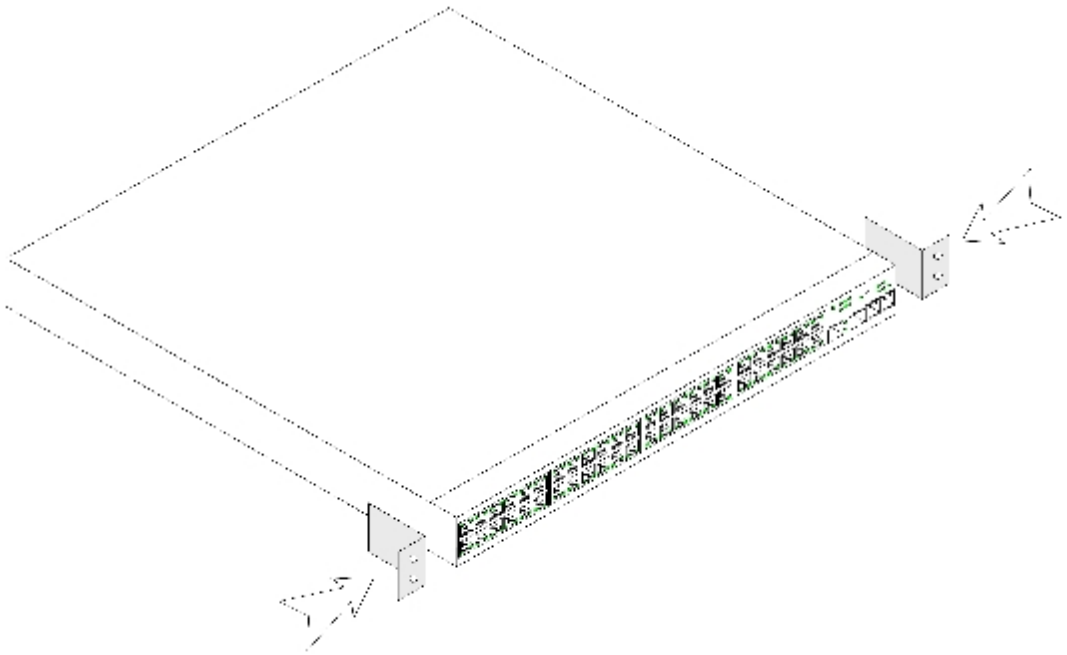
警告： デバイスをラックまたはキャビネットに設置する前に、デバイス本体からすべてのケーブルを取り外してください。

警告： 複数のデバイスはラックの下から上の順に搭載します。

□□□ デバイスとラック取り付けブラケットの両方の取り付け穴を合わせ、付属のラック取 り付けブラケットをデバイスの片側に取り付けます。

ブラケットの取り付け位置は以下の図を参照してください。

図 **3-1** ラック取り付けのためのブラケットの取り付け



□□□ 付属のネジをラックの取り付け穴に挿入してドライバで締め付けます。

□□□ この手順を繰り返して、ラック取り付けブラケットをデバイスのもう一方の側面にも 取り付けます。

□□□ デバイスのラック取り付け穴とラックの取り付け穴の位置を揃えて、デバイスを 48.26 cm のラックに挿入します。

□□□ ラック用のネジを使用して（デバイスには同梱されていません）デバイスをラックに 固定します。ブラケットの下側のネジを上側よりも先に締め付けます。通気孔がふさ がれていないことを確認します。

平らな場所への設置

ラックを使用しない場合、このデバイスは水平面に設置してください。設置する面は、デバイスとケーブルの重量に耐えることができる必要があります。

□□□ シャーシ底面の印が付いているそれぞれの場所に、粘着ゴムパッドを貼り付けます。

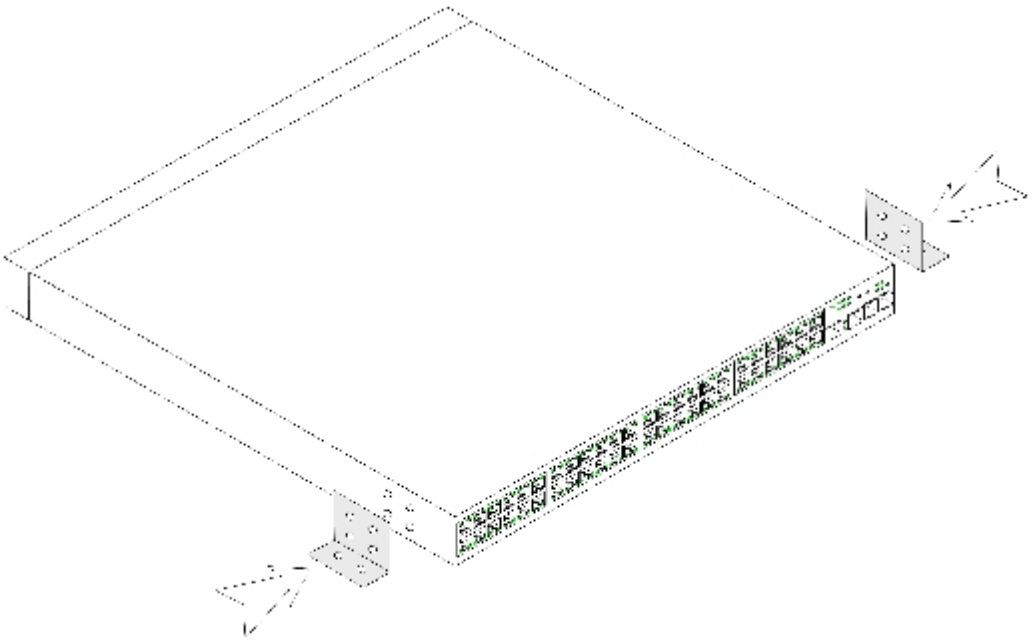
□□□ 両側に約 5 cm ずつ、背面に約 13 cm の隙間を確保してデバイスを水平面に置きます。

□□□ デバイスが適切に放熱されることを確認します。

壁面への取り付け

□□□ 壁用取り付けブラケットを、デバイスのネジ穴と壁取り付けブラケットの取り付け穴 の位置を揃えて、デバイスの一方の側面に取り付けます。ブラケットの取り付け位置 は以下の図を参照してください。

図**3 - 2** 壁面設置用ブラケットの取り付け



□□□ 付属のネジをラックの取り付け穴に挿入してドライバで締め付けます。

□□□ この手順を繰り返して、壁取り付けブラケットをデバイスのもう一方の側面にも取り 付けます。

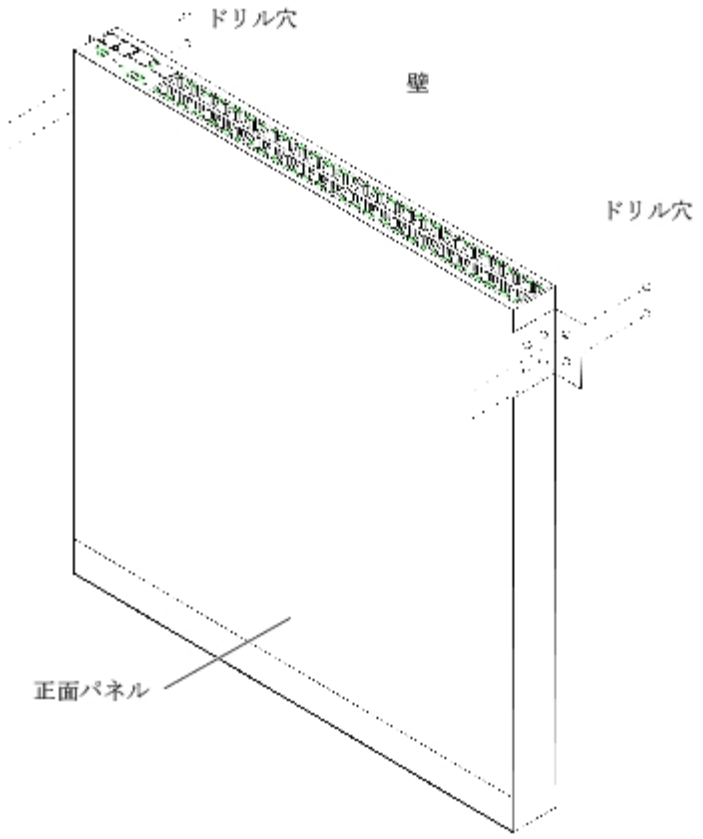
□□□ デバイスを取り付ける壁面の位置にデバイスを合わせます。

□□□ 壁面のデバイスを固定するネジ穴を設ける位置に印を付けます。

□□□ 印を付けた位置をドリルで穴開けし、コンクリート用プラグ（デバイスには同梱され ていません）をすべて穴に打ち込みます。

□□□ ネジ（デバイスには同梱されていません）を使用してデバイスを壁面に固定します。 通気孔がふさがれていないことを確認します。

図**3 - 3** 壁面への取り付け



ターミナルへの接続

□□□ RS-232 クロスケーブルを ASCII ターミナルに、またはターミナルエミュレーションソ フトウェアを実行しているデスクトップコンピュータのシリアルコネクタに接続しま す。

□□□ ケーブルのもう一方の側には DB-9 メスコネクタを取り付けて、デバイスのシリアル ポートコネクタに接続します。

デバイスの電源への接続

付属の AC 電源ケーブルを背面パネルの AC 電源コネクタに接続します。

メモ： この段階では、AC 電源ケーブルはまだ電源コンセントに接続しないでください。デ バイスの起動と設定で説明する手順で、デバイスを電源に接続します。

図3-4 背面パネルの電源コネクタ

PowerConnect 3424/3448 の背面図

PowerConnect 3424P/3448P の背面図

デバイスに AC 電源を接続したら、正面パネルの LED の点灯を確認することで、デバイスへの電源接続とデバイスの正常な動作を確認します。

スタックの設置

概要

各デバイスは、スタンドアロンデバイスとして、またはスタック内のメンバーとして使用できます。1 つのスタックで最大 6 台のデバイス、192 個のポートがサポートできます。

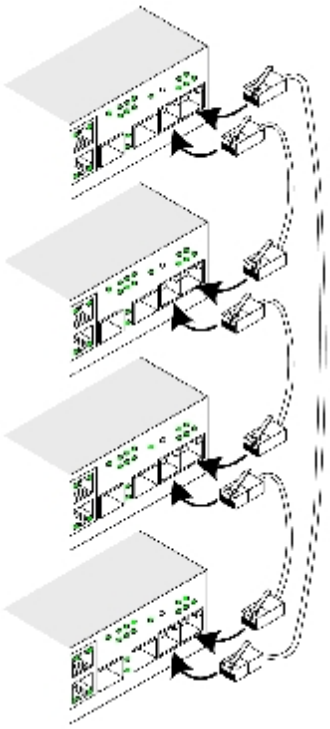
すべてのスタックには 1 台のマスターユニットが必要で、マスターバックアップユニットを加えることもできます。残りはメンバーとしてスタックに接続します。

PowerConnect 3400 シリーズスイッチのスタッキング

PowerConnect 3400 シリーズの各スタックに組み込まれるユニットは、1 台がマスターユニットで、マスターバックアップユニットを加えることもできます。残りのスタックのユニットはスタックメンバーとみなされます。

PowerConnect 3400 シリーズスイッチでは、スタッキングに RJ-45 Gigabit Ethernet ポート（G3 および G4）を使用します。これにより、デバイスアクセサリを追加せずにスタッキング機能を追加することができます。スタッキングを行うには、スタック最上部のデバイスのポート G3 と、そのすぐ下のデバイスのポート G4 に、標準のカテゴリ 5 ケーブルを挿入します。すべてのデバイスが接続されるまで、この手順を繰り返します。スタック最下部のデバイスのポート G3 を、スタック最上部のデバイスのポート G4 に接続します。

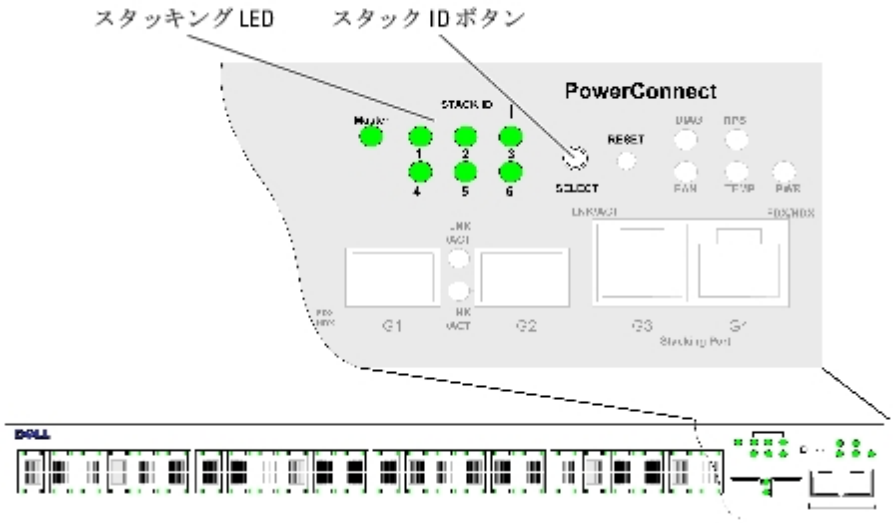
図**3-5** スタックケーブルの配線図



メモ： スタッキングモードでは、G3 と G4 に指定されているポートは EWS に表示されません が、これはデバイスには影響ありません。これはポートがスタッキング用の別のインデック スを受け取るためです。

スタックユニットの識別は、デバイスの正面パネルのスタック ID ボタンで行います。

図**3-6** スタックの構成と識別用パネル



各スタックデバイスには、スタック内でのそのデバイスの位置と機能を定義する固有の識別用ユニット ID があります。デバイスがスタンドアロンユニットの場合、スタック LED は点灯しません。デフォルト設定はスタンドアロンです。

ユニット ID は、スタック ID ボタンを使用して手動で設定します。設定したユニット ID はスタック ID LED に表示されます。ユニット ID 1 と 2 は、マスターとバックアップマスターユニット用に予約されています。ユニット ID 3～6 はメンバーユニット用です。

ユニット ID の選択手順

ユニット ID の選択手順は以下のとおりです。

□□□ スタンドアロンまたはマスターデバイスのコンソールポートが RS-232 クロスケーブ ルを介して VT100 ターミナルデバイスまたは VT100 ターミナルエミュレータに接続 されていることを確認します。

□□□ AC 電源ソケットの位置を確認します。

□□□ AC 電源ソケットの電源を切ります。

□□□ デバイスを AC 電源ソケットに接続します。

□□□ AC 電源ソケットの電源を入れます。

起動中に、設定済みの LED 番号（前回保存したユニット ID に対応）が点滅を開始します。LED は 15 秒間点滅します。この間に、希望のスタック ID LED が点灯するまでスタック ID ボタンを押すことで、特定のスタック ID を選択します。

□□□ 選択手順 ― スタック ID ボタンを押し続けると、スタック ID LED が順番に点灯します。 LED 6 の点滅中にスタック ID ボタンを押すと、デバイスはスタンドアロンとして設定さ れます。もう一度スタック ID ボタンを押すと、スタック ID は 1 に戻ります。ユニット 1 とユニット 2 はマスター有効ユニットです。マスターの選択手順については、スタッキ ングの概要 を参照してください。

□□□ 選択手順の終了 ― ユニット ID の選択手順は、15 秒間の点滅が終了するまでに完了し てください。LED の点滅終了時に選択されていたユニット IDが設定されると、スタッ ク ID ボタンは操作に応答しなくなります。

メモ： このスタック ID の選択手順は、一度にユニット 1 台ずつ実行して、順にすべてのス タックメンバーの電源を入れるようにします。一回にユニット 1 台ずつ実行することによっ て、時間に余裕をもって各ユニットにスタック ID を割り当てることができます。ただし、デ バイスに電源を入れる前にスタックケーブルの配線図に従ってスタック全体のケーブル接 続を行っておく必要があります。

デバイスの起動と設定

すべての外部接続の完了後、ターミナルをこのデバイスに接続してデバイスの設定を行います。詳細な機能の実行については、詳細設定で説明しています。

メモ： 以下の手順を実行する前に本製品のリリースノートをお読みください。リリースノー トは、デルサポートサイト **support.dell.com** からダウンロードできます。

メモ： ユーザー関連のマニュアルは、デルサポートサイト **support.dell.com** から最新版を入手 されるようお勧めします。

デバイスの接続

デバイスを設定するには、コンソールに接続しておく必要があります。ただし、デバイスがスタックの一部である場合は、スタック内のマスターユニットと呼ばれる 1 台のデバイスだけをターミナルに接続しておいてください。スタック全体が 1 つのデバイスとして動作するので、設定が必要なのはマスターユニットだけです。

ターミナルとデバイスの接続

このデバイスには、ターミナルデバイスとしてデバイスの監視と設定を行うためのターミナルエミュレーションソフトウェアを実行するデスクトップシステムに接続するためのコンソールポートが装備されています。コンソールポートコネクタは、データ端末デバイス（DTE）への接続を行うための DB-9 オスコネクタです。

コンソールポートを利用するには、次のハードウェアが必要です。

- VT100 互換のターミナル、または VT100 ターミナルエミュレーションソフトウェアを実行している、シリアルポートが装備されたデスクトップまたはポータブルコンピュータ
- コンソールポートとターミナルの適切なコネクタとを接続する DB-9 メスコネクタ付きの RS-232 クロスケーブル

ターミナルをデバイスのコンソールポートに接続するには、次の手順を実行します。

□□□ 付属の RS-232 クロスケーブルを VT100 ターミナルエミュレーションソフトウェアを 実行しているターミナルに接続します。

□□□ コンソールに接続する適切なシリアルポートを選択します（シリアルポート 1 または シリアルポート 2）。

□□□ データ速度を 9600 ボーに設定します。

□□□ データ形式を、データビット 8、ストップビット 1、パリティなしに設定します。

□□□ フロー制御を none に設定します。

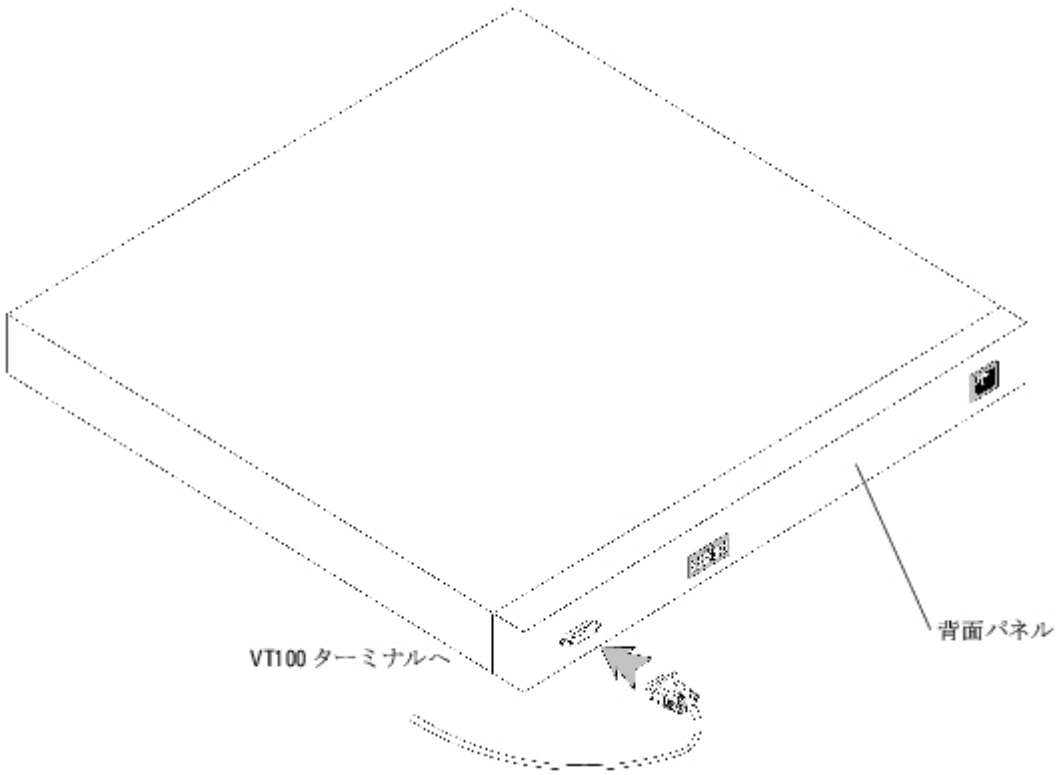
□□□ Properties（プロパティ）で VT100 for Emulation モードを選択します。

□□□ Function, Arrow, and Ctrl keys（ファンクション、矢印、および Ctrl キー）に Terminal keys（ターミナルキー）を設定します。設定が Windows keys（Windows キー）ではなく Terminal keys（ターミナルキー）であることを確認します。

注意： Microsoft® Windows® 2000 で HyperTerminal を使用する場合は、Windows 2000 Service Pack 2 以降をインストールしていることを確認してください。Windows 2000 Service Pack 2 を使用 すると、HyperTerminal の VT100 エミュレーションで矢印キーが正しく機能します。Windows 2000 のサービスパックの詳細については、www.microsoft.com を参照してください。

□□□ マスターユニットまたはスタンドアロンデバイスのコンソールポートに RS-232 クロ スケーブルのメスのコネクタを直接接続し、拘束ネジを締めます。PowerConnect 3400 シリーズのコンソールポートは背面パネルにあります。

図**3-7 PowerConnect 3400** シリーズのコンソールポートへの接続



メモ： コンソールはスタック内のどのコンソールポートにも接続可能ですが、スタック管理 はユニット ID 1 または 2 のスタックマスターユニットでのみ実行されます。

メモ、注意および警告

メモ、注意および警告

PowerConnect 3424/P と 3448/P の設定

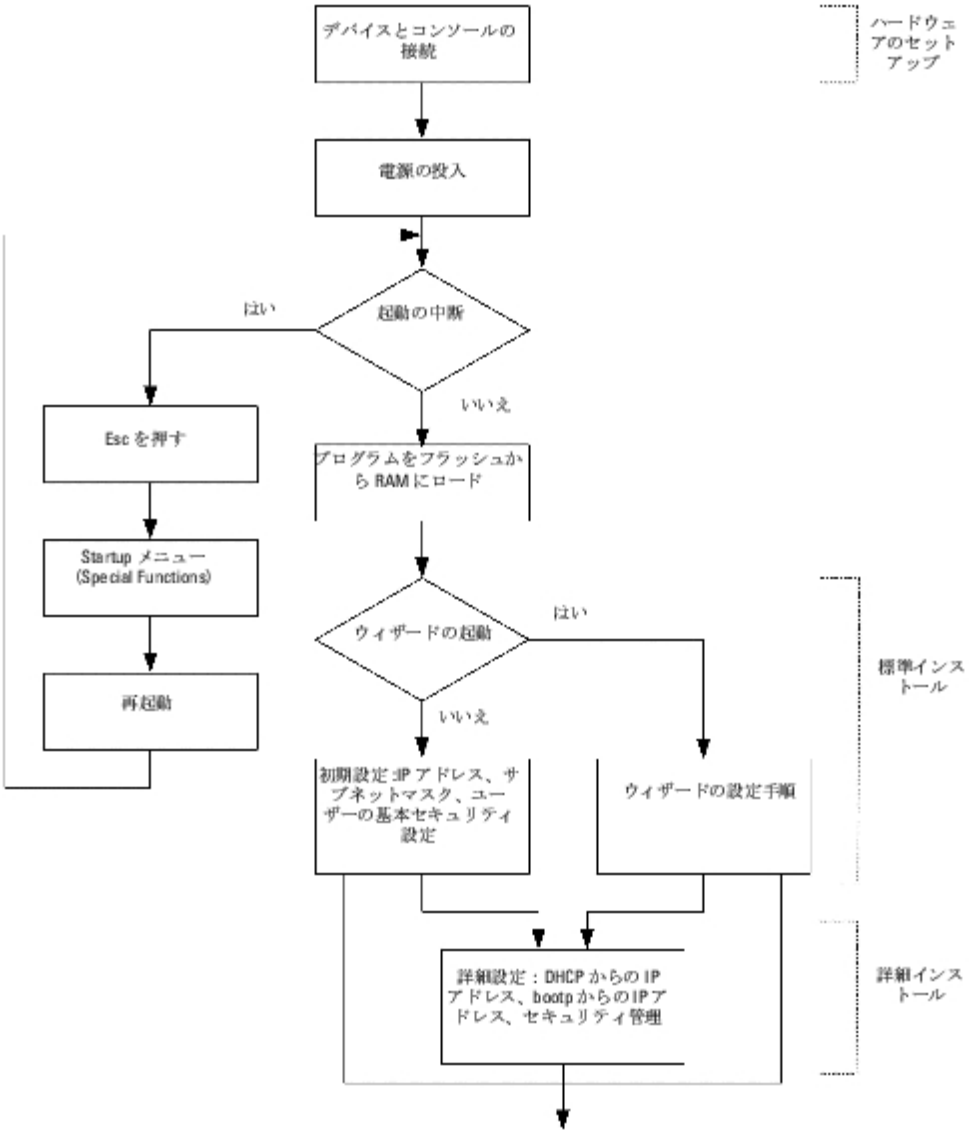
Dell™ PowerConnect™ 34XX システム ユーザーズガイド

設定の手順

すべてのデバイスの外部接続が完了したら、ターミナルをデバイスに接続して、起動その他の手順を監視します。取り付けと設定の手順の順序は、次の図に示すとおりです。

メモ： 以下の手順を実行する前に本製品のリリースノートをお読みください。リリースノー トは **support.dell.com** からダウンロードできます。

図 **4-1** 取り付けと設定の作業の流れ



スイッチの起動

ローカルターミナルを接続した状態で電源を入れると、スイッチは電源投入時の自己診断（POST）を実行します。POST はデバイスの初期化のたびに実行され、完全に起動する前にハードウェアコンポーネントをテストして、デバイスが正常に動作することを確認します。重大な問題が検出されると POST プログラムは中断します。POST が正常に完了すると、RAM に有効な実行可能イメージがロードされます。テストが正常に完了したか失敗したかを知らせる POST メッセージがターミナルに表示されます。

起動処理は約 30 秒で完了します。

初期設定

メモ： 以下の手順を実行する前に本製品のリリースノートをお読みください。リリースノー トは、デルサポートサイト **support.dell.com** からダウンロードできます。

メモ： 初期設定は、次のことを前提に実行されます。

- PowerConnect デバイスがこれまで設定されたことがなく、工場出荷時の状態のままであること。
- PowerConnect デバイスが正常に起動していること。

- コンソールへの接続が済んでいて、コンソールプロンプトが VT100 ターミナルデバイスの画面に表示されること。

デバイスの初期設定はコンソールポートを介して行います。初期設定が完了すれば、すでに接続されているコンソールポートまたは初期設定時に定義したインタフェースを介してデバイスを管理することができます。

デバイスを今回初めて起動する場合、またはデバイスが設定されていなかったために設定ファイルが空である場合は、セットアップウィザードの使用を促すメッセージが表示されます。セットアップウィザードの指示に従ってデバイスの初期設定を行えば、デバイスをすぐに動作可能な状態にすることができます。

メモ： デバイスを設定する前に、ネットワーク管理者から以下の情報を入手してください。

- 管理対象デバイスの VLAN 1 インタフェースに割り当てる IP アドレス（デフォルトでは、すべてのポートは VLAN 1 のメンバーです）。
- ネットワークの IP サブネットマスク。
- デフォルトルートを設定するデフォルトゲートウェイ（ネクストホップルーター）の IP アドレス。
- SNMP コミュニティストリングおよび SNMP 管理システムの IP アドレス（オプション）。
- ユーザー名とパスワード。

セットアップウィザードの指示に従ってスイッチの初期設定を行えば、システムをすぐに動作可能な状態にすることができます。セットアップウィザードを省略して、デバイスの CLI モードでデバイスを手動で設定することも可能です。

セットアップウィザードにより、以下のフィールドが設定されます。

- SNMP コミュニティストリングおよび SNMP 管理システムの IP アドレス（オプション）
- ユーザー名とパスワード
- デバイスの IP アドレス
- デフォルトゲートウェイの IP アドレス

以下のメッセージが表示されます。

```
Welcome to Dell Easy Setup Wizard


The Setup Wizard guides you through the initial switch configuration, and gets you up and running as
quickly as possible.You can skip the setup wizard, and enter CLI mode to manually configure the
switch.
The system will prompt you with a default answer; by pressing enter, you accept the default.
You must respond to the next question to run the setup wizard within 60 seconds, otherwise the
system will continue with normal operation using the default system configuration.


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

N を押すと、セットアップウィザードは終了します。60 秒以内に応答しなかった場合、セットアップウィザードは自動的に終了し、CLI コンソールプロンプトが表示されます。

Y を押すと、セットアップウィザードの指示に従ってデバイスの初期設定を行うことができます。

メモ： 60 秒以内に応答がなく、ネットワークに BootP サーバーが存在する場合は、アドレス が BootP サーバーから読み出されます。

メモ： セットアップウィザードは Ctrl+Z を押せばいつでも終了できます。

ウィザード手順 1

以下のメッセージが表示されます。

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

   • Setup the initial SNMP version 2 account now.

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


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

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

省略して手順 2 に進むには、N を押します。

セットアップウィザードを続行するには、Y を押します。以下のメッセージが表示されます。

```
To setup the SNMP management account you must specify the management system IP address and the
"community string" or password that the particular management system uses to access the switch.The
wizard automatically assigns the highest access level [Privilege Level 15] to this account.
You can use Dell Network Manager or CLI to change this setting, and to add additional management
systems.For more information on adding management systems, see the user documentation.
To add a management station:
Please enter the SNMP community string to be used:[Dell_Network_Manager]
Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from
any Management Station: [0.0.0.0]
```

以下を入力します。

- SNMP コミュニティストリング。たとえば、Dell_Network_Manager。
- いずれかの管理ステーションから管理する場合は、管理システムの IP アドレス（A.B.C.D）またはワイルドカード（0.0.0.0）。

メモ： 先頭が 0 の IP アドレスとマスクは使用できません。

Enter を押します。

ウィザード手順 2

以下のメッセージが表示されます。

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

以下を入力します。

- ユーザー名は、たとえば「admin」と入力します。
- パスワードを入力し、パスワードの確認を行います。

メモ： 1 回目と 2 回目に入力したパスワードが一致しない場合は、一致するまで再入力を促 されます。

Enter を押します。

ウィザード手順 **3**

以下のメッセージが表示されます。

```
Next, an IP address is setup.

The IP address is defined on the default VLAN (VLAN #1), of which all ports are members.This is the
IP address you use to access the CLI, Web interface, or SNMP interface for the switch.To setup an IP
address:

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

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

IP アドレスと IP サブネットマスクを入力します。たとえば、1.1.1.1 を IP アドレス、255.255.255.0 を IP サブネットマスクとして入力します。

Enter を押します。

ウィザード手順 **4**

以下のメッセージが表示されます。

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

デフォルトゲートウェイを入力します。

Enter を押します。以下のメッセージが表示されます（例として使われているパラメータによる）。

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

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


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


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

ウィザード手順 **5**

以下のメッセージが表示されます。

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up
configuration file. If the information is incorrect, select (N) to discard configuration and restart
```

```
the wizard:(Y/N)[Y]Y
```

省略してウィザードを再起動するには、N を押します。

セットアップウィザードを完了するには、Y を押します。以下のメッセージが表示されます。

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

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

ウィザード手順 **6**

CLI プロンプトが表示されます。

詳細設定

本項では、IP アドレスのダイナミックアロケーション、および AAA（認証、承認、アカウンティング）方式に基づくセキュリティ管理について説明します。本項で取り扱うトピックは以下のとおりです。

- DHCP を介した IP アドレスの設定
- BOOTP を介した IP アドレスの設定
- セキュリティ管理とパスワードの設定

DHCP と BOOTP を介して IP アドレスの設定や受信を行う際に、これらのサーバーから受信する設定には IP アドレスが含まれています。また、サブネットマスクとデフォルトゲートウェイを含む場合もあります。

DHCP サーバーからの **IP** アドレスの読み出し

DHCP プロトコルを使用して IP アドレスを読み出す場合、デバイスは DHCP クライアントとして動作します。デバイスがリセットされると、DHCP コマンドは設定ファイルに保存されますが、IP アドレスは保存されません。DHCP サーバーから IP アドレスを読み出すには、次の手順を実行します。

□□□ IP アドレスを読み出すために、任意のポートを選択し、DHCP サーバーまたは DHCP サーバーを持つサブネットに接続します。

□□□ 以下のコマンドを入力して、選択したポートを IP アドレスの受信に使用します。以下 の例では、コマンドは設定に使用されるポートタイプに基づいています。

- 動的 IP アドレスの割り当ての場合は、以下のとおりです。

```
console# configure

console(config)# interface ethernet 1/e1

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

console(config-if)# exit
```

```
console(config)#
```

- 動的 IP アドレスの割り当て（VLAN 上）の場合は、以下のとおりです。

```
console# configure

console(config)# interface ethernet vlan 1

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

console(config-if)# exit

console(config)#
```

インタフェースは IP アドレスを自動的に受け取ります。

□□□ IP アドレスを確認するには、次の例に示すように、システムプロンプトで **show ip interface** コマンドを入力します。

```
console# show ip interface

IP Address I/F Type


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

100.1.1.1/24 vlan 1 dynamic
```

メモ： DHCPサーバー用の IP アドレスを読み出すために、デバイス設定を削除する必要はあ りません。

メモ： 設定ファイルをコピーする際に、同一の DHCP サーバーまたは同一の設定を持つ DHCP サーバーに接続するインタフェース上で DHCP を有効にする命令が含まれている設定 ファイルの使用は避けてください。この例では、デバイスは新しい設定ファイルを読み出し、 そこから起動します。デバイスは次に、新しい設定ファイルの指示どおりに DHCP を有効に し、DHCP は同じファイルを再ロードするようにデバイスに指示します。

メモ： DHCP IP アドレスを設定すると、このアドレスは動的に読み出され、`ip address dhcp` コマンドは設定ファイルに保存されます。マスターに障害が発生した場合に、バック アップは DHCP アドレスの読み出しを再び試みます。その結果として発生する可能性がある イベントは、以下のとおりです。

- 同じ IP アドレスが割り当てられる場合があります。
- 異なる IP アドレスが割り当てられる場合があり、その結果、管理ステーションへの接続が失われる可能性があります。
- DHCP サーバーがダウンする場合があり、その結果、IP アドレスの読み出しにエラーが発生し、管理ステーションへの接続が失われる可能性があります。

BOOTP サーバーからの IP アドレスの取得

標準の BOOTP プロトコルはサポートされており、これによってデバイスは、ネットワーク内の任意の標準 BOOTP サーバーから IP ホストの設定を自動的にダウンロードできます。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。

□□□ 任意のポートを選択し、BOOTP サーバーまたは同サーバーを含むサブネットに接続し て、IP アドレスを読み出します。

□□□ システムプロンプトで **delete startup configuration** コマンドを入力して、フラッ シュから Startup Configuration を削除します。

デバイスは設定なしで再起動し、60 秒で BOOTP 要求の送信を開始します。デバイスは IP アドレスを自動的に取得します。

メモ： デバイスの再起動開始時に ASCII ターミナルまたはキーボードで任意のキーを押すと、 BOOTP の処理は完了前に自動的に取り消され、デバイスは BOOTP サーバーから IP アドレス を受信しません。

このプロセスを次の例で示します。

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

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

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

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

/* the device reboots
```

IP アドレスを確認するには、**show ip interface** コマンドを入力します。

デバイスには現在、IP アドレスが設定されています。

セキュリティ管理とパスワードの設定

システムセキュリティは、AAA（認証、承認、アカウンティング）方式によって処理されます。AAA 方式によって、ユーザーアクセス権、権限、管理方法が管理されます。AAA では、ローカルとリモートの両方のユーザーデータベースが使用されます。データの暗号化は、SSH 方式によって処理されます。

システムは出荷時にデフォルトのパスワードを設定していません。パスワードはすべてユーザーが定義します。ユーザー定義のパスワードを紛失した場合は、**Startup** メニューからパスワードリカバリ手順を呼び出すことができます。この手順はローカルターミナルでのみ使用できます。パスワードを入力していないローカルターミナルから 1 回限りのアクセスが可能です。

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以下のサービスについて設定できます。

- Terminal
- 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に、デフォルトの優先度は「1」です。この場合、アクセス は許可されますが、設定の権限はありません。アクセス権とデバイスを設定する権限を有効 にするには、優先度「15」を設定する必要があります。ユーザー名にパスワードの設定なし で権限レベル「15」を設定することも可能ですが、必ずパスワードを設定するようお勧めし ます。パスワードが指定されていない場合、権限を持つユーザーはパスワードなしで Web イ ンタフェースにアクセスできます。

メモ： パスワードは、パスワード管理コマンドを使用してパスワードのエージアウトや有効 期限を強制して、安全を確保することができます。詳細については、セキュリティ管理とパ スワードの設定 を参照してください。

初期 **Terminal** パスワードの設定

初期 Terminal 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(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line console

console(config-line)# login authentication default

console(config-line)# enable authentication default

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

- ターミナルセッションを介してデバイスに初めてログオンする場合は、パスワードプロンプトで george と入力します。
- デバイスのモードを有効に変更する場合は、パスワードプロンプトで george 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(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line telnet

console(config-line)# login authentication default

console(config-line)# enable authentication default

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

- Telnet セッションを介してデバイスに初めてログオンする場合は、パスワードプロンプトで bob と入力します。
- デバイスのモードを有効に変更する場合は、bob 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(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line ssh

console(config-line)# login authentication default

console(config-line)# enable authentication default

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

- SSH セッションを介してデバイスに初めてログオンする場合は、パスワードプロンプトで jones と入力します。
- デバイスのモードを有効に変更する場合は、jones 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(config)# ip http authentication local

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

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(config)# ip https authentication local

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

HTTPS セッションを使用するには、ターミナル、Telnet、または SSH セッションを使用する設定を行う際に、以下のコマンドを 1 回だけ入力します。

メモ： ページコンテンツを表示するには、Web ブラウザで SSL 2.0 以上を有効にします。

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

console(config)# ip https server
```

初めて http または https セッションを有効にする場合は、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 のサービスはレベル「15」のアクセスを必要とし、設定レベルのア クセスに直接接続する必要があります。

Startup 手順

Startup メニューの手順

Startup メニューから呼び出される手順には、ソフトウェアのダウンロード、フラッシュの処理、およびパスワードリカバリが含まれています。診断手順はテクニカルサポート担当者専用であり、マニュアルに公開されていません。

デバイスの起動時に Startup メニューに入ることができます。ユーザー入力は POST 直後に行います。

Startup メニューに入るには、以下の手順を実行します。

□□□ 電源を入れ、auto-boot メッセージを待ちます。

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

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

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

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

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

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

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

Carrier board, based on PPC8247

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

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

□□□ auto-boot メッセージが表示されたら、<Enter> を押して Startup メニューを表示し ます。Startup メニューの手順は、ASCII ターミナルまたは Windows HyperTerminal を使用して実行できます。

```
[1] Download Software

[2] Erase Flash File

[3] Password Recovery Procedure

[4] Enter Diagnostic Mode

[5] Set Terminal Baud-Rate

[6] Back
```

以下の各項で、利用可能な Startup メニューのオプションを説明します。

メモ： Startup メニューでオプションを選択する際には、タイムアウトを考慮してください。 35 秒（デフォルト）以内に選択が行われないと、デバイスはタイムアウトします。このデ フォルト値は CLI を通じて変更できます。

メモ： Diagnostics モード（ オプション[4]）の操作はテクニカルサポート担当者にのみ許可 されています。この理由で、Enter Diagnostics Mode については本書では説明してありません。

Download Software（ソフトウェアのダウンロード）**—** オプション **[1]**

ソフトウェアダウンロード手順は、破損したファイルの交換やシステムソフトウェアのアップデートまたはアップグレードのために新しいバージョンのダウンロードが必要な場合に実行します。Startup メニューからソフトウェアをダウンロードするには、以下の手順を実行します。

□□□ Startup メニューで [1] を押します。次のプロンプトが表示されます。

```
Downloading code using XMODEM

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

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

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

HW version is

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

Dram size is :128M bytes

Dram first block size is :36864K bytes

Dram first PTR is :0x1C00000

Flash size is:16M

Loading running configuration.

Number of configuration items loaded: 5

Loading startup configuration.

Number of configuration items loaded: 5

Device configuration:

Slot 1 - PowerConnect 3424 HW Rev. 0.0

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

-- Unit Number 1 Standalone --

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

BOXP_high_appl_init:dpssIpcInitStandAlone

Tapi Version:v1.3.1.6P_01_03

Core Version:v1.3.1.6P_01_02

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

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

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

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

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

□□□ HyperTerminal を使用している場合は、HyperTerminal のメニューバーで Transfer （転送）をクリックします。

□□□ Filename フィールドに、ダウンロードするファイルのファイルパスを入力します。

□□□ Protocol フィールドで Xmodem プロトコルが選択されていることを確認します。

□□□ Send を押します。ソフトウェアがダウンロードされます。

メモ： ソフトウェアがダウンロードされると、デバイスは自動的に再起動します。

Erase FLASH File（フラッシュファイルの消去）ー オプション [2]

場合によってはデバイス設定の消去が必要です。設定を消去すると、CLI、EWS、または SNMP を通じて設定したパラメータはすべて再設定が必要になります。

デバイス設定を消去するには、次の手順を実行します。

□□□ Startup メニューで 2 秒以内に [2] を押して、フラッシュファイルを消去します。次 のメッセージが表示されます。

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

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

□□□ Y を押します。次のメッセージが表示されます。

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

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

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

□□□ フラッシュファイルの名前として、config と入力します。設定は消去されデバイス は再起動します。

□□□ デバイスの初期設定を繰り返します。

Password Recovery（パスワードのリカバリ）ー オプション [3]

パスワードを紛失した場合は、Startup メニューから Password Recovery（パスワードのリカバリ）手順を呼び出すことができます。この手順により、パスワードの入力なしで 1 回だけデバイスにエントリできます。

紛失したパスワードのリカバリを行うには、以下の手順を実行します（ローカルターミナルのみで実行可能）。

□□□ Startup メニューで [3] と入力し、<Enter> を押します。パスワードが削除されま す。

希望の選択内容を入力するか、ESC を押して終了します。

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

メモ： デバイスのセキュリティを確実なものとするには、該当する管理方法のパスワードを 再設定します。

Enter Diagnostic Mode（診断モードの実行）― オプション [4]

テクニカルサポート専用です。

Set Terminal Baud-Rate（ターミナルボーレートのパスワード）― オプション [5]

ターミナルボーレートを設定するには、[5] を入力して <Enter> を押します。

希望の選択内容を入力するか、ESC を押して終了します。

Set new device baud-rate: 38,400

TFTP サーバーを通じてのソフトウェアのダウンロード

本項では、TFTP サーバーを通じてデバイスソフトウェア（システムイメージと起動イメージ）をダウンロードする手順について説明します。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。

システムイメージのダウンロード

デバイスは、システムイメージのコピーが保存されているフラッシュメモリ領域からシステムイメージを解凍する時に起動し、動作します。新しいイメージをダウンロードすると、もう一方のシステムイメージのコピー用に割り当てられているもう一方の領域に保存されます。

特に別の指定がなければ、次の起動時にはデバイスが現在アクティブなシステムイメージを解凍し、実行します。

TFTP サーバーを通じてシステムイメージをダウンロードするには、以下の手順を実行します。

□□□ IP アドレスがデバイスのポートの 1 つに設定されていて、TFTP サーバーに ping を送 信できることを確認します。

□□□ ダウンロードするファイルが TFTP サーバーに保存されていることを確認します（arc ファイル）。

□□□ **show version** コマンドを入力して、現在どのソフトウェアバージョンがデバイス上 で実行されているかを確認します。以下に、表示される情報の例を示します。

```
console# show version

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

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

HW version
```

□□□ **show bootvar** コマンドを入力し、現在どのシステムイメージがアクティブかを確認 します。以下に、表示される情報の例を示します。

```
console# show bootvar
```

```
Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

□□□ **copy tftp:**//{tftp アドレス}/{ファイル名} **image** コマンドを入力して、新しい システムイメージをデバイスにコピーします。新しいイメージをダウンロードすると、 システムイメージのもう一方のコピーに割り当てられている領域に保存されます（例 では **image-2**）。以下に、表示される情報の例を示します。

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

Accessing file `file1' on 176.215.31.3Ö

Loading file1 from 176.215.31.3:

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

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

感嘆符（**!**）は、コピー作業が進行中であることを示します。感嘆符 **1** つが正常に転送された **512** バイトに相当します。ピリオドは、コピー作業がタイムアウトしたことを示します。連続する多数のピリオドは、コピー作業が失敗したことを示します。

□□□ boot system コマンドを入力すると、次回の起動時のイメージが選択できます。この コマンドの後で、**show bootvar** コマンドを入力して、**boot system** コマンド内で パラメータとして示されているコピーが次回の起動時のイメージに選択されているこ とを確認します。

以下に、表示される情報の例を示します。

```
console# boot system image-2

console# show bootvar

Images currently available on the Flash

Image-1 active

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

起動システムコマンドを入力して次回の起動時のイメージを選択する手順を実行しなかった場合、システムは現在アクティブなイメージから起動します。

□□□ **reload** コマンドを入力します。次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]?
```

□□□ **y** を入力します。デバイスが再起動します。

起動イメージのダウンロード

新しい起動イメージを TFTP サーバーからロードし、起動イメージをプログラミングしてフラッシュを作成すると、起動イメージがアップデートされます。起動イメージは、デバイスの電源を入れるとロードされます。ユーザーは起動イメージのコピーを制御できません。TFTP サーバーを通じて起動イメージをダウンロードするには、以下の手順を実行します。

□□□ IP アドレスがデバイスのポートの 1 つに設定されていて、TFTP サーバーに ping を送 信できることを確認します。

□□□ ダウンロードするファイルが TFTP サーバーに保存されていることを確認します（rfb ファイル）。

□□□ show version コマンドを入力して、現在どのソフトウェアバージョンがデバイス上で 実行されているかを確認します。以下に、表示される情報の例を示します。

```
console# show version

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

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

HW version
```

□□□ **copy tftp://**{tftp アドレス}**/**{ファイル名}** boot** コマンドを入力して、起動イ メージをデバイスにコピーします。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.rfb boot

Erasing file..done.

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

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

□□□ **reload** コマンドを入力します。次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]?
```

□□□ y を入力します。デバイスが再起動します。

ポートのデフォルト設定

デバイスのポートを設定するための一般的情報には、オートネゴシエイションメカニズム、およびスイッチポートのデフォルト設定に関する簡単な説明が含まれます。

オートネゴシエイション

オートネゴシエイションにより、すべての 10/100/1000BaseT スイッチングポートの速度、二重モード、およびフロー制御の自動検出が可能になります。オートネゴシエイションは、デフォルトでポートごとに有効に設定されています。

オートネゴシエイションは、ポートがそれぞれのパートナーに送信速度、二重モード、およびフロー制御能力（フロー制御はデフォルトで無効）を通知できるように 2 つのリンクパートナー間に確立されたメカニズムです。2 つのポートは、各機能がそれぞれ低い方に合わせて動作します。

オートネゴシエイションに対応していない、またはオートネゴシエイションが設定されていない NIC を接続する場合は、デバイスのスイッチングポートと NIC の両方を手動で同じ速度および二重モードに設定する必要があります。

リンクの片方の端のステーションが全二重モードに設定されているデバイスの 100BaseT ポートとオートネゴシエイションを試みる場合、そのステーションのオートネゴシエイションは半二重モードになります。

MDI/MDIX

デバイスは、すべてのスイッチング 10/100/1000BaseT ポートでストレートケーブルとクロスケーブルの自動検出をサポートしています。この機能はオートネゴシエイションの一部であり、オートネゴシエイションが有効に設定されているときに有効となります。

MDI/MDIX（Media Dependent Interface with Crossover）が有効に設定されている場合は、ケーブル選択エラーの自動修正が可能です。そのため、ストレートケーブルとクロスオーバーケーブルの区別は無用となります。エンドステーションの標準配線はMDI（Media Dependent Interface）、ハブとスイッチに使用する標準配線は MDIX として知られています。

フロー制御

デバイスは、全二重モードに設定されているポートに対して 802.3x フロー制御をサポートしています。この機能はデフォルトでは無効に設定されていますが、ポートごとに有効に設定できます。フロー制御メカニズムにより、受信側は送信側に対し、バッファオーバーフローの防止のために転送を一時停止するよう信号を送ることができます。

バックプレッシャー

デバイスは、半二重モードで設定されたポートに対してバックプレッシャーをサポートしています。この機能はデフォルトでは無効に設定されていますが、ポートごとに有効に設定できます。バックプレッシャーメカニズムは、送信側による一時的な追加のトラフィックの送信を防止します。追加のトラフィックがリンクを利用できないように、受信側がリンクをふさぐことができます。

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。

表**4-7** 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	10/100BaseT 銅線: オートネゴシエイション 100 Mbps 全二重
	10/100/1000BaseT 銅線 / SFP: オートネゴシエイション 1000 Mbps 全二重
ポートの転送状態	有効
ポートのタグ付け	タグなし
フロー制御	オフ（入口で無効に設定）
バックプレッシャー	オフ（入口で無効に設定）

メモ、注意および警告

メモ、注意および警告

DellOpenManage Switch Administrator の使い方

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

本項では、Dell OpenManage Switch Administrator のユーザーインタフェースの概要について説明します。

アプリケーションの起動

メモ： アプリケーションを起動する前に、IP アドレスを定義する必要があります。詳細につ いては、初期設定 を参照してください。

□□□ Web ブラウザを開きます。

□□□ デバイスの IP アドレスをアドレスバーに入力して、<Enter> を押します。

□□□ **Log In**（ログイン）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。

メモ： 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。

□□□ **OK** をクリックします。

Dell OpenManage™ Switch Administrator のホームページが開きます。

インタフェースの概要

ホームページには以下の内容が表示されています。

- ツリービュー ― 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。
- デバイスビュー ― ホームページの右側に表示され、デバイスの図、情報または表、および設定手順を示します。

図 **5-1 Switch Administrator** のコンポーネント

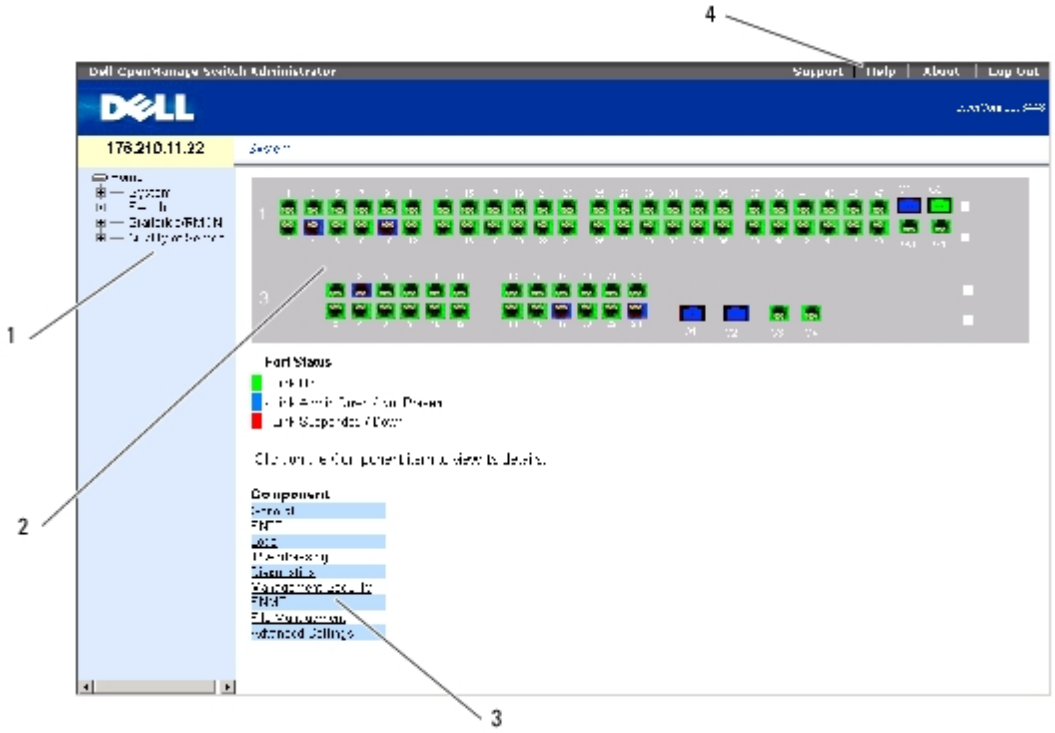


表 5-1 には、インタフェースコンポーネントと対応する番号をまとめています。

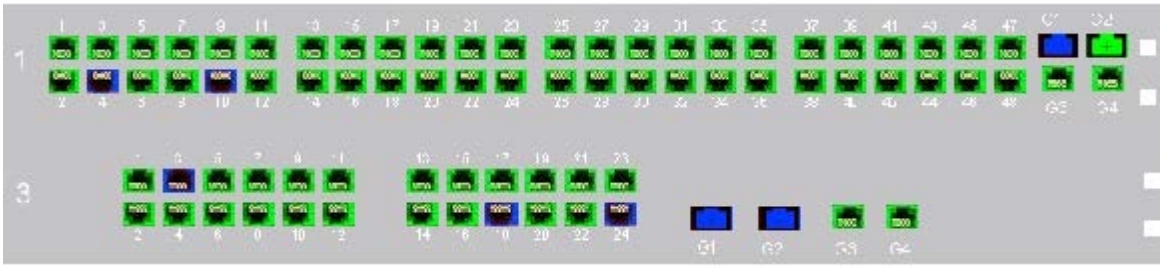
表**5-1** インタフェースコンポーネント

コンポーネント	説明
1	ツリービューにはデバイスの各機能がツリー状に表示されます。ツリービューの各枝は、展開して特定の機能の下にすべてのコンポーネントを表示したり、閉じて機能のコンポーネントを非表示にしたりできます。垂直のバーを右側にドラッグすると、ツリー領域を展開してコンポーネントの正式名称を表示することができます。
2	デバイスビューには、デバイスのポート、現在の設定と状態、表の情報、機能コンポーネントなどに関する情報が表示されます。 選択したオプションによって、デバイスのビューの下側に、デバイスの他の情報や、パラメータ設定に使用するダイアログが表示されます。
3	コンポーネントリストには、機能コンポーネントの一覧が含まれています。コンポーネントは、ツリービュー内の機能を展開しても表示できます。
4	デバイスに関する情報とデルサポートへのアクセスを提供する情報ボタンです。詳細については、「情報ボタン」を参照してください。

デバイスのグラフィック表示

ホームページには、デバイスの正面パネルのグラフィック表示があります。

図**5-2 PowerConnect** デバイスのポートインジケータ



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。ポートの色は以下のいずれかになります。

表**5-2 PowerConnect** のポートとスタッキングのインジケータ

コンポーネント	説明
ポートインジケータ	
緑色	ポートは現在有効に設定されています。
赤色	ポートにエラーが発生しました。
青色	ポートは現在無効に設定されています。
赤色	デバイスは現在スタックにリンクされていません。

メモ： ポート LED は、OpenManage Switch Administrator の PowerConnect 正面パネルに反映さ れません。LED の状態は、実際のデバイスを見ることでのみ確認できます。ただし、スタッ キング LED はスタッキングポートの状態を反映します。LED の詳細については、LED の定義を 参照してください。

Switch Administrator ボタンの使い方

本項では、OpenManage Switch Administrator のインタフェースに表示されるボタンについて説明します。インタフェースボタンは、以下のカテゴリに分類されます。

情報ボタン

情報ボタンはオンラインサポートおよびオンラインヘルプへのアクセスを提供し、併せて OpenManage Switch Administrator インタフェースに関する情報も提供します。

表**5-3** 情報ボタン

ボタン	説明
Support（サポート）	デルサポートページ **support.dell.com** を開きます。
Help（ヘルプ）	オンラインヘルプは、デバイスの設定と管理に役立つ情報を提供します。オンラインヘルプのページは状況対応型です。たとえば、**IP Addressing**（IP アドレッシング）ページを開いている状態で Help をクリックすると、IP アドレッシングに関するヘルプページが開きます。
About（このソフトウェアについて）	バージョンとビルド番号、およびデルの著作権情報が表示されます。
Log Out（ログアウト）	Log Out（ログアウト）ウィンドウが開きます。

デバイス管理ボタン

デバイス管理ボタンは、デバイスの情報を簡単に設定する手段です。デバイス管理ボタンには以下の種類があります。

表**5-4** デバイス管理ボタン

ボタン	説明
Apply Changes（変更の適用）	デバイスに設定の変更を適用します。
Add（追加）	表またはダイアログに情報を追加します。
Telnet	Telnet セッションを開始します。
Query（クエリ）	表を照会します。
Show All（すべてを表示）	デバイスの表を表示します。
Left arrow/Right Arrows（左右矢印キー）	リスト間で情報を移動します。
Refresh（表示の更新）	デバイスの情報を更新します。
Reset All Counters（すべてのカウンタをリセット）	統計カウンタをクリアします。
Print（印刷）	**Network Management System** ページや表の情報を印刷します。
Draw（描画）	統計チャートをオンザフライで作成します。

フィールド定義

OpenManage Switch Administrator のウェブページに特に記載がない限り、ユーザー定義のフィールドには 1～159 文字の入力が可能です。以下を除くすべての文字が使用できます。

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

デバイスへの **CLI** によるアクセス

ターミナルポートへの直接接続、または Telnet 接続により、デバイスを管理できます。Telnet 接続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 コマンドの使用を開始する前に、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ことを確認します。

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。

メモ： CLI を使用してデバイスにリモートでアクセスする前に、ソフトウェアがデバイスに ダウンロードされていることを確認してください。

ターミナル接続

□□□ デバイスの電源を入れ、起動が完了するまで待ちます。

□□□ Console> プロンプトが表示されたら、enable と入力し、<Enter> を押します。

□□□ デバイスを設定し、タスクを完了するのに必要なコマンドを入力します。

□□□ 入力が終わったら、特権 EXEC モードを **exit** します。

セッションが終了します。

メモ： 特権 EXEC コマンドモードのシステムに別のユーザーがログインすると、現在ログイ ンしているユーザーはログオフされます。

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。RS-232 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。

デバイスの管理に、最大 4 つの Telnet セッションを同時に実行することができます。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。

□□□ Start → Run と選択します。

Run ウィンドウが開きます。

□□□ **Run** ウィンドウで、**Open** フィールドに Telnet <IP アドレス> と入力します。

□□□ **OK** をクリックします。

Telnet セッションが開始します。

CLI の使い方

本項では、CLI の使い方について説明します。

コマンドモードの概要

CLI は複数の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。ターミナルプロンプトで疑問符を入力

すると、その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。

CLI セッション初期化中は、CLI モードは ユーザー EXEC モードです。ユーザー EXEC モードでは、コマンドの限られたサブセットしか利用できません。このレベルは、ターミナル設定を変更しないタスク用に予約されており、CLI などの設定サブシステムへのアクセスに使用されます。次のレベルである特権 EXEC モードを起動するには、パスワードが必要です（パスワードを必要とするように設定してある場合）。

特権 EXEC モードは、デバイスのグローバル設定へのアクセスを提供します。デバイス内の特定のグローバル設定には、次のレベル、グローバル設定モードを起動してください。パスワードは不要です。

グローバル設定モードは、デバイスの設定をグローバルレベルで管理します。

インタフェース設定モードは、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。サブコマンドを必要とするインタフェースコマンドには、サブインタフェース設定モードと呼ばれる別のレベルがあります。パスワードは不要です。

ユーザー **EXEC** モード

デバイスにログオンすると、EXEC コマンドモードが有効になります。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。たとえば、次のとおりです。

```
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。

ユーザー EXEC コマンドにより、リモートデバイスへの接続、ターミナル設定の一時的な変更、基本的なテストの実行、システム情報の一覧表示が許可されます。

ユーザー EXEC コマンドを一覧表示するには、コマンドプロンプトで疑問符を入力します。

特権 **EXEC** モード

不正なアクセスを防止し、動作パラメータを確保するために、特権アクセスを保護することができます。パスワードは画面に表示され、大文字と小文字が区別されます。

特権 EXEC モード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。

□□□ プロンプトで`enable` と入力し、<Enter> を押します。

□□□ パスワード入力のプロンプトが表示されたら、パスワードを入力し、<Enter> を押しま す。

特権 EXEC モードのプロンプトが、デバイスのホスト名の末尾に # を加えて表示されます。たとえば、次のような表示になります。

```
console#
```

特権 EXEC コマンドを一覧表示するには、コマンドプロンプトで疑問符を入力します。

特権 EXEC モードから ユーザー EXEC モードに戻るには、`disable` と入力し、<Enter> を押します。

次の例では、特権 EXEC モードにアクセスした後にユーザーEXEC モードに戻る方法を示します。

```
console> enable

Enter Password: ******

console#

console# disable

console>
```

前のモードに戻るには、**exit** コマンドを使用します。たとえば、インタフェース設定モードからグローバル設定モードに、グローバル設定モードから特権 EXEC モードに戻ることができます。

グローバル設定モード

グローバル設定コマンドは、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。

グローバル設定モードにアクセスするには、特権 EXEC モードのプロンプトで **configure** コマンド を入力し、<Enter> を押します。グローバル設定モードが、デバイスのホスト名の末尾に (config) と # を加えて表示されます。

```
console(config)#
```

グローバル設定コマンドを一覧表示するには、コマンドプロンプトで疑問符を入力します。

グローバル設定モードから 特権 EXEC モードに戻るには、 **exit** コマンドを入力するか、または<Ctrl> + <Z> のキーの組み合わせを使用します。

次の例では、グローバル設定モードにアクセスして 特権 EXEC モードに戻る方法を示します。

```
console#

console# configure

console(config)# exit

console#
```

CLI モードの詳細な一覧については、『Dell™ PowerConnect™3424/P and PowerConnect 3448/P CLI Guide』（Dell™ PowerConnect™3424/P & PowerConnect 3448/P CLI ガイド）を参照してください。

メモ、注意および警告

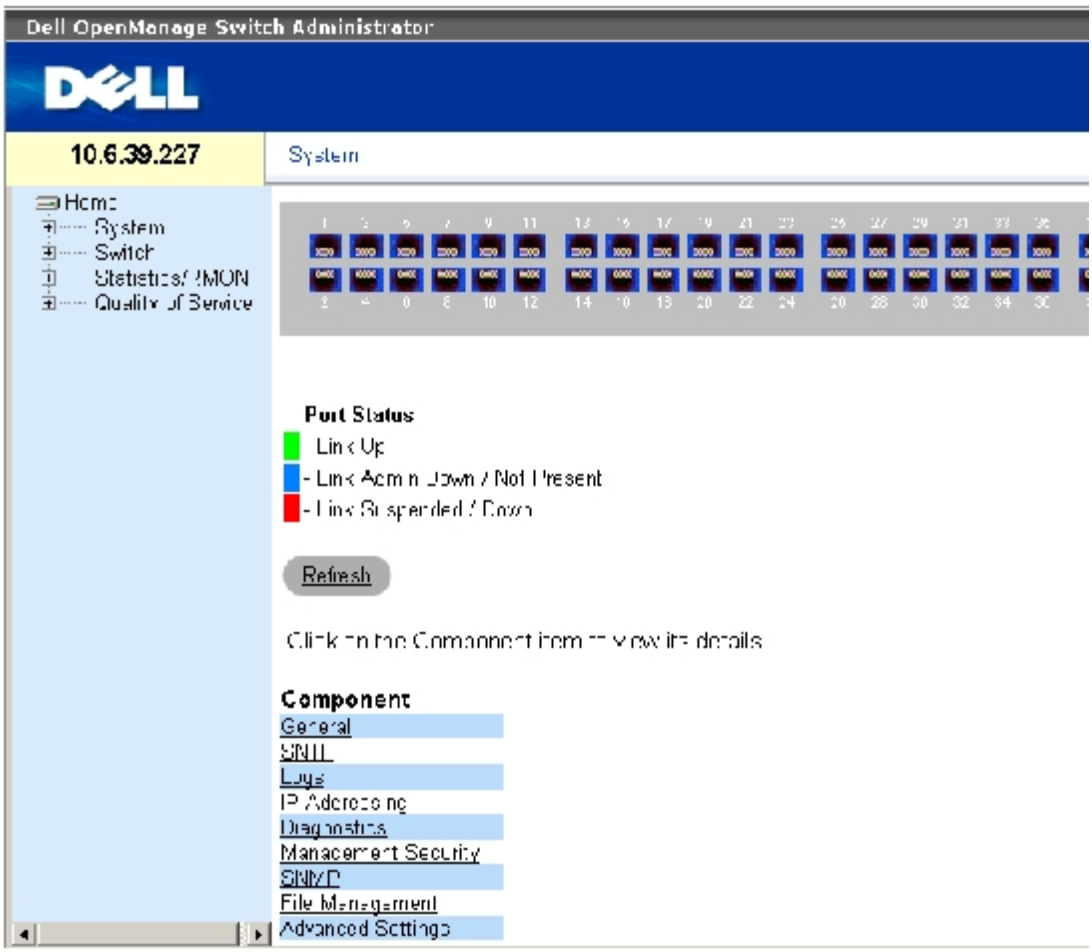
メモ、注意および警告

システム情報の設定

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

本項では、セキュリティ機能、スイッチソフトウェアのダウンロード、スイッチのリセットなど、システムパラメータの定義方法について説明します。システムページを開くにはツリービューから **System** （システム）をクリックします。

図 **6-1** システム



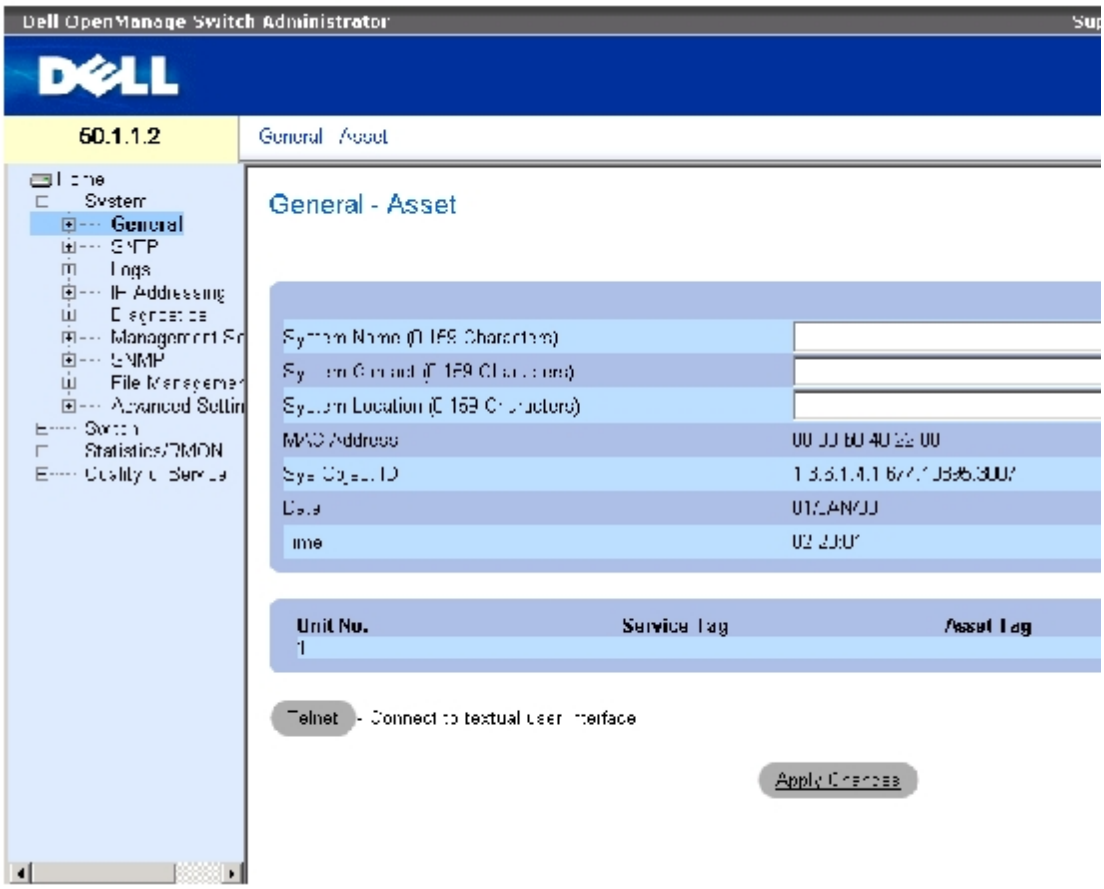
一般スイッチ情報の定義

一般ページには、ネットワーク管理者がスイッチパラメータを構成するために必要な、各ページへのリンクがまとめられています。

スイッチ資産情報の表示

資産ページは、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 ID、日付、時間、システムの稼働時間など、デバイスの一般情報の設定および閲覧パラメータで構成されています。資産ページを開くには、ツリービューから System（システム）→ General（一般）→ Asset（資産）をクリックします。

図**6-2** 資産



資産ページは、以下のフィールドで構成されます。

System Name （半角 0～159 文字）（システム名称）— ユーザー定義のデバイス名称を定義します。

System Contact （半角 0～159 文字）（システム問い合わせ先）— 問い合わせ担当者の名前を定義します。

System Location （半角 0～159 文字）（システムの場所情報）— システムを設置している場所を定義します。

MAC Address（MAC アドレス）— スイッチの MAC アドレスを示します。

Sys Object ID（システムオブジェクト ID）— エンティティに含まれるネットワーク管理サブシステムが持つ、ベンダーの authoritative な ID です。

Date (MM/DD/YY) — 現在の日付です。形式は、日、月、年の順で、たとえば 10 / OCT / 03 は 2003 年 10 月 10 日を表します。

Time (HH:MM:SS) — 時刻を表します。形式は、時、分、秒の順で、たとえば **20:12:21** は、午後 **8** 時 **12** 分 **21** 秒です。

Unit No.（ユニット番号）— デバイス資産情報を表示しているユニット番号を示します。

Service Tag（サービスタグ）— 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です。

Asset Tag （半角 0～16 文字）（資産タグ）— ユーザー定義のデバイス参照情報を示します。

Serial No.（シリアル番号）— デバイスのシリアル番号です。

システム情報の定義

□□□ 資産ページを開きます。

□□□ 関連フィールドを定義します。

□□□ **Apply Changes**（変更の適用）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 セッションの開始

□□□ 資産ページを開きます。

□□□ **Telnet**（Telnet）をクリックします。

Telnet セッションが始まります。

CLI コマンドを使用したデバイス情報の設定

資産ページ内のフィールド設定操作と等価な処理を実行する **CLI** コマンドを以下の表に示します。

表**6-1 Asset CLI** コマンド

CLI コマンド	説明
hostname name	デバイスホスト名を表示または変更します。
snmp-server contact text	システム担当者名を設定します。
snmp-server location text	デバイスの場所情報を入力します。
clock set hh:mm:ss day month year	システムクロックと日付を手動で設定します。
show clock [detail]	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。
asset-tag text	デバイスの資産タグを設定します。
show stack <1-6>	システムのスタッキング情報を表示します。

show system [unit *unit*]	システム情報を表示します。
show system id [unit *unit*]	システム識別情報を表示します。

デバイスホスト名、システム担当者名、デバイス設置場所、さらにシステムクロックの時刻と日付を CLI コマンドを使用して定義する例を以下に示します。

```
console(config)# hostname dell

dell (config)# snmp-server contact Dell_Tech_Supp

dell (config)# snmp-server location New_York

dell (config)# exit

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

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

Console# show clock

15:29:03 Jun 17 2002
```

スタンドアロンデバイスのシステム情報を CLI コマンドを使って表示させる例を以下に示します。

console# **show system id**	
Service tag :	
Serial number : 51	
Asset tag :	
console# **show system**	
System Description:	Ethernet Switch
System Up Time (days,hour:min:sec):	0,00:00:57
System Contact:	
System Name:	CARRIER-1
System Location:	
System MAC Address:	00:00:00:08:12:51
System Object ID:	1.3.6.1.4.1.674.10895.3006
Type:	PowerConnect 3424

Main Power Supply Status:	OK
Fan 1 Status:	NOT OPERATIONAL
Fan 2 Status:	NOT OPERATIONAL
Temperature (Celsius):	30
Temperature Sensor Status:	OK

スタッキングデバイスのシステム情報を CLI コマンドを使って表示させる例を以下に示します。

```
console# show system id

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

console# show system

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

Unit  Main Power Supply  Redundant Power Supply
----  -----------------  ----------------------
1     OK
```

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

システム時刻設定の定義

時刻同期ページは、ローカルハードウェアクロックと、外部 SNTP クロックの両者のシステム時刻パラメータを定義するフィールドで構成されています。外部 SNTP クロックを使用してシステム時刻が維持されている場合、外部 SNTP クロックに障害が発生すると、システム時刻はローカルハードウェアクロックに戻ります。デバイス側でサマータイムを有効にすることが可能です。以下に、各国におけるサマータイムの開始時期と終了時期を示します。

- Albania（アルバニア）— 3 月の最後の週末から 10 月の最後の週末まで
- Australia（オーストラリア）— 10 月末から 3 月末まで
- Australia - Tasmania （オーストラリア—タスマニア）— 10 月のはじめから 3 月末まで

- Armenia（アルメニア）— 3 月の最後の週末から 10 月の最後の週末まで
- Austria（オーストリア）— 3 月の最後の週末から 10 月の最後の週末まで
- Bahamas（バハマ）— 米国の夏時間に連動して 4 月から 10 月まで
- Belarus（ベラルーシ）— 3 月の最後の週末から 10 月の最後の週末まで
- Belgium（ベルギー）— 3 月の最後の週末から 10 月の最後の週末まで
- Brazil（ブラジル）— 10 月の第 3 日曜日から 3 月の第 3 土曜日まで。サマータイム期間中、ブラジル南東部のほとんどでブラジル時間が 1 時間進められます。
- Chile（チリ）—イースター島 3 月 9 日から 10 月 12 日まで。3 月の第 1 日曜日または 3 月 9 日以降。
- China（中国）— 中国ではサマータイムは実施されていません。
- Canada（カナダ）— 4 月の第 1 日曜日から 10 月の最後の日曜日まで。夏時間は、通常、州政府または準州政府によって管理されます。一部の自治体が例外となる場合があります。
- Cuba（キューバ）— 3 月の最後の日曜日から 10 月の最後の日曜日まで
- Cyprus（キプロス）— 3 月の最後の週末から 10 月の最後の週末まで
- Denmark（デンマーク）— 3 月の最後の週末から 10 月の最後の週末まで
- Egypt（エジプト）— 4 月の最後の金曜日から 9 月の最後の木曜日まで
- Estonia（エストニア）— 3 月の最後の週末から 10 月の最後の週末まで
- Finland（フィンランド）— 3 月の最後の週末から 10 月の最後の週末まで
- France（フランス）— 3 月の最後の週末から 10 月の最後の週末まで
- Germany（ドイツ）— 3 月の最後の週末から 10 月の最後の週末まで
- Greece（ギリシャ）— 3 月の最後の週末から 10 月の最後の週末まで
- Hungary（ハンガリー）— 3 月の最後の週末から 10 月の最後の週末まで
- India（インド）— インドではサマータイムは実施されていません。
- Iran（イラン）— 3月 21 日から 9 月 23 日まで
- Iraq（イラク）— 4 月 1 日から 10 月 1 日まで
- Ireland（アイルランド）— 3 月の最後の週末から 10 月の最後の週末まで
- Israel（イスラエル）— 年によって変わります。
- Italy（イタリア）— 3 月の最後の週末から 10 月の最後の週末まで
- Japan（日本）— 日本ではサマータイムは実施されていません。
- Jordan（ヨルダン）— 3 月の最後の週末から 10 月の最後の週末まで
- Latvia（ラトビア）— 3 月の最後の週末から 10 月の最後の週末まで
- Lebanon（レバノン）— 3 月の最後の週末から 10 月の最後の週末まで
- Lithuania（リトアニア）— 3 月の最後の週末から 10 月の最後の週末まで
- Luxembourg（ルクセンブルク）— 3 月の最後の週末から 10 月の最後の週末まで
- Macedonia（マケドニア）— 3 月の最後の週末から 10 月の最後の週末まで
- Mexico — 4 1 2:00 10 2:00

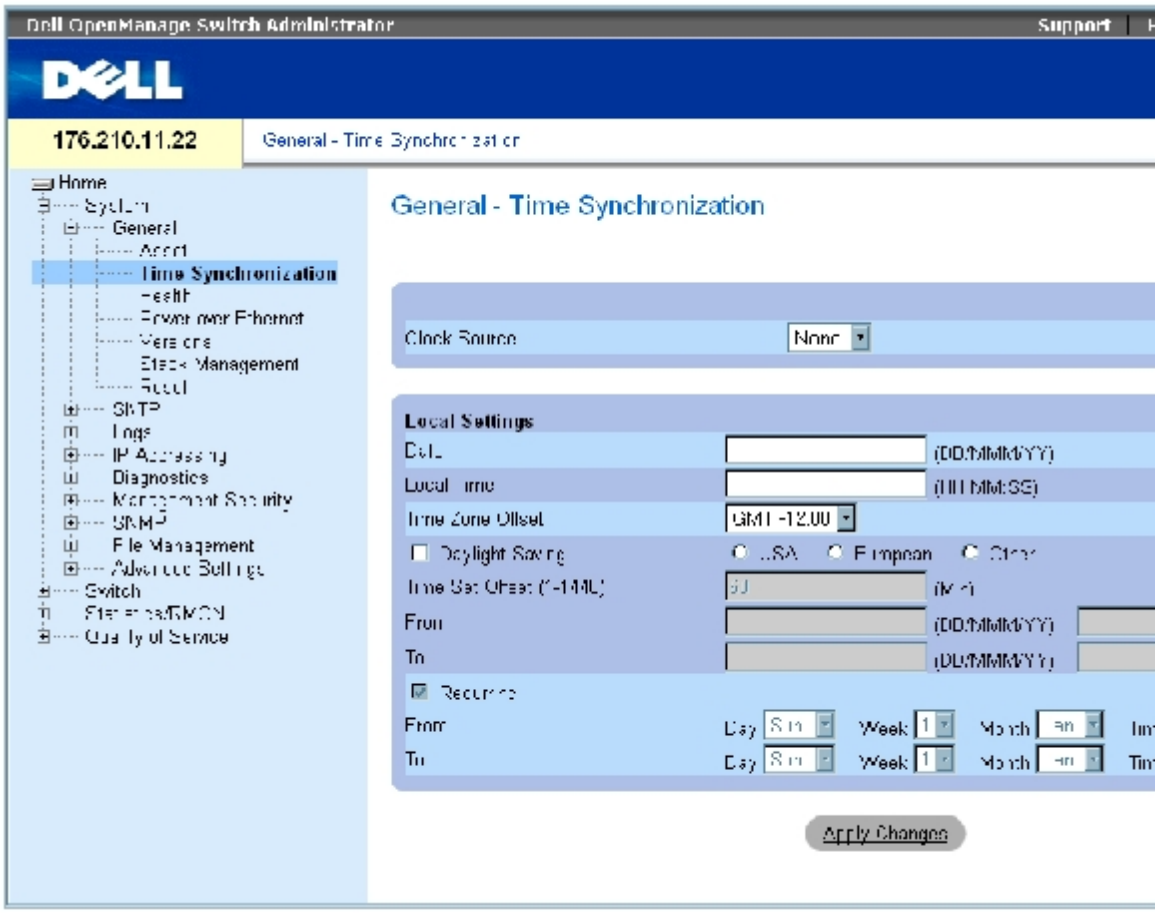
（メキシコ）　月の最　日曜日の　時から　月の最後の日曜日の　まで

- Moldova（モルドバ）— 3 月の最後の週末から 10 月の最後の週末まで
- Montenegro（モンテネグロ）— 3 月の最後の週末から 10 月の最後の週末まで
- Netherlands（オランダ）— 3 月の最後の週末から 10 月の最後の週末まで
- New Zealand（ニュージーランド）— 10 月の第 1 日曜日から 3 月 15 日以降の最初の日曜日まで
- Norway（ノルウェイ）— 3 月の最後の週末から 10 月の最後の週末まで
- Paraguay（パラグアイ）— 4 月 6 日から 9 月 7 日まで
- Poland（ポーランド）— 3 月の最後の週末から 10 月の最後の週末まで
- Portugal（ポルトガル）— 3 月の最後の週末から 10 月の最後の週末まで
- Romania（ルーマニア）— 3 月の最後の週末から 10 月の最後の週末まで
- Russia（ロシア）— 3 月の最後の週末から 10 月の最後の週末まで
- Serbia（セルビア）— 3 月の最後の週末から 10 月の最後の週末まで
- SlovakRepublic（スロバキア共和国）— 3 月の最後の週末から 10 月の最後の週末まで
- South Africa（南アフリカ）—南アフリカではサマータイムは実施されていません。
- Spain（スペイン）— 3 月の最後の週末から 10 月の最後の週末まで
- Sweden（スウェーデン）— 3 月の最後の週末から 10 月の最後の週末まで
- Switzerland（スイス）— 3 月の最後の週末から 10 月の最後の週末まで
- Syria（シリア）— 3 月 31 日から 10 月 30 日まで
- Taiwan（台湾）— 台湾ではサマータイムは実施されていません。
- Turkey（トルコ）— 3 月の最後の週末から 10 月の最後の週末まで
- United Kingdom（英国）— 3 月の最後の週末から 10 月の最後の週末まで
- United States of America（アメリカ合衆国）— 4 月の最 1 日曜日の 2:00 時から 10 月の最後の日曜日の 2:00 まで

SNTP の詳細は、「**SNTP** の設定」を参照してください。

時刻同期ページを開くには、ツリービューから **System**（システム）→ **General**（一般）→ **Time Synchronization**（時刻同期）をクリックします。

図**6-3** 時刻同期



時刻同期ページは以下のフィールドで構成されます。

クロック源

Clock Source（クロック源）— システムクロックの設定に使用するクロック源です。設定可能なフィールド値は以下のとおりです。

SNTP（SNTP）— システム時刻を SNTP サーバーを用いて設定します。詳細は「**SNTP** の設定 」を参照してください。

None（なし）— システム時刻の設定に外部クロック源を使用しません。

ローカル設定

Date（日付）— システムの日付を定義します。フィールドのフォーマットは DD / MMM / YY で、たとえば 04 / May / 50です。

Local Time（ローカル時間）— システムの時刻を定義します。フィールドのフォーマットは HH / MM / SS で、たとえば 21/15/03 です。

Time Zone Offset（タイムゾーンオフセット）— グリニッジ標準時刻（GMT）とローカル時間との時差です。たとえば、パリのタイムゾーンオフセットは GMT +1:00 で、ニューヨークのローカル時刻は GMT -5:00 です。

サマータイムの設定には、特定の年の特定の日付による設定方法と、年に関係なく繰返しによって設定する方法の 2 種類があります。特定の年の特定の日付による設定では **Daylight Savings**（サマータイム）フィールドを設定し、年に関係ない繰返しによる設定では **Recurring**（繰り返し）フィールドを設定します。

Daylight Savings（サマータイム）— デバイスの設置場所にもとづいて、デバイスのサマータイムを有効にします。設定可能なフィールド値は以下のとおりです。

USA（アメリカ合衆国）— デバイスは、4 月の第 1 日曜日の午前 2:0 0にサマータイムに切り替わり、10 月の最終日曜日の午前 2:00 に標準時間に戻ります。

European（欧州）— デバイスは、3 月の最終日曜日の午前 1:00 にサマータイムに切り替わり、10 月の最終日曜日の午前 1:00 に標準時間に戻ります。European（欧州）オプションは、EU 諸国と、EU 標準を適用している他の欧州諸国に適用します。

Other（その他）— サマータイム定義はデバイスの設置場所にもとづいてユーザーが定義します。Other（その他）を選択した場合は、**From**（から）と**To**（まで）フィールドを定義しなければなりません。

Time Set Offset（1～1440）（時刻設定オフセット）— 国がアメリカ合衆国か欧州以外の場合に、サマータイムで早める時刻を、分を単位として設定します。デフォルト時間は 60 分です。

From（から）— アメリカ合衆国か欧州以外の国でサマータイムが始まる日時を、1 つのフィールドには DD / MMM / YY の形式で、もう 1 つのフィールドには時刻の形式で、それぞれ定義します。たとえばサマータイムが 2007 年 10 月 25 日の午前 5:00 から始まる場合、2 つのフィールド定義は 25 / Oct / 07 と 05:00 になります。設定可能な値は次のとおりです。

Date（日）— サマータイムが開始される日です。可能なフィールド値の範囲は 1～31 です。

Month（月）— サマータイムが開始される月です。入力可能なフィールド値は Jan（1月）～Dec（12月）です。

Year（年）— 設定したサマータイムが始まる年です。

Time（時刻）— サマータイムが始まる時刻です。フィールドの形式は、時:分で、たとえば 05:30 です。

To（まで）— アメリカ合衆国か欧州以外の国でサマータイムが終わる日時を、1 つのフィールドには DD / MMM / YY の形式で、もう 1 つのフィールドには時刻の形式で、それぞれ定義します。たとえばサマータイムが 2008 年 3 月 23 日の 午前 12:00 に終了する場合、2 つのフィールド定義は 23 / Mar / 08 と 12:00 になります。設定可能な値は次のとおりです。

Date（日）— サマータイムが終わる日です。可能なフィールド値の範囲は 1～31 です。

Month（月）— サマータイムが終わる月です。入力可能なフィールド値は Jan（1月）～Dec（12月）です。

Year（年）— 設定したサマータイムが終わる年です。

Time（時刻）— サマータイムが終わる時刻です。フィールドの形式は、時:分で、たとえば 05:30 です。

Recurring（繰り返し）— アメリカ合衆国か欧州以外の国でサマータイムが毎年定期的に繰り返される場合に、サマータイムの始まる日時を設定します。設定可能なフィールド値は以下のとおりです。

From（から）— 例年サマータイムが始まる日時を設定します。たとえば、サマータイムが 4 月第 2 日曜日の午前 5:00 に毎年始まる場合などです。設定可能なフィールド値は次のとおりです。

Day（曜日）— 例年サマータイムが始まる曜日です。入力可能なフィールド値は Sunday（日）～Saturday（土）です。

Week（週）— 例年サマータイムが始まる月の週次です。可能なフィールド値の範囲は 1～5 です。

Month（月）— 例年サマータイムが始まる月です。入力可能なフィールド値は Jan（1月）～Dec（12月）です。

Time（時刻）— 例年サマータイムが始まる時刻です。フィールドの形式は、時:分で、たとえば 02:10 です。

To（まで）— 例年サマータイムが終わる日時を設定します。たとえば、サマータイムが 4 月第 4 金曜日の午前 5:00 に毎年終わる場合などです。設定可能なフィールド値は次のとおりです。

Day（曜日）— 例年サマータイムが終わる曜日です。入力可能なフィールド値は Sunday（日曜）～Saturday（土曜）です。

Week（週）—例年サマータイムが終わる月の週次です。可能なフィールド値の範囲は 1～5 です。

Month（月）— 例年サマータイムが終わる月です。入力可能なフィールド値は Jan（1月）～Dec（12月）です。

Time（時刻）— 例年サマータイムが終わる時刻です。フィールドの形式は、時:分で、たとえば 05:30 です。

クロック源の選択

□□□ 時刻同期ページを開きます。

□□□ **Clock Source**（クロック源）フィールドを定義します。

□□□ Apply Changes（変更の適用）をクリックします。

クロック源が選択され、デバイスがアップデートされます。

ローカルクロック設定の定義

□□□ 時刻同期ページを開きます。

□□□ 各フィールドを定義します。

□□□ Apply Changes（変更の適用）をクリックします。

ローカルクロック設定が適用されます。

CLI コマンドを使用したクロック設定の定義

時刻同期ページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

メモ： サマータイムを設定する場合は以下の手順に従ってください。

□□□ サマータイムを設定します。

□□□ タイムゾーンを定義します。

□□□ クロックを設定します。

たとえば。

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

表**6-2** クロック設定 **CLI** コマンド

CLI	説明
clock source sntp	システムクロックに外部時刻源を設定します。
clock time zone *hours-offset* [**minutes** *minutes-offset*][**zone** *acronym*]	表示を目的としてタイムゾーンを設定します。
clock summer-time	サマータイム（夏時間）へ自動的に切り替わるようシステムを設定します。
clock summer-time recurring {**usa** | **eu** | *week day month hh:mm week day month hh:mm}* [**offset** *offset*] [**zone** *acronym*]	アメリカ合衆国と欧州基準にもとづいて、サマータイム（夏時間）へ自動的に切り替わるようシステムを設定します。
clock summer-time date *date month year hh:mm date month year hh:mm* **[offset** *offset***] [zone** *acronym***]**	指定した期間（日 / 月 / 年の形式）にわたって、サマータイム（夏時間）へ自動的に切り替わるようシステムを設定します。

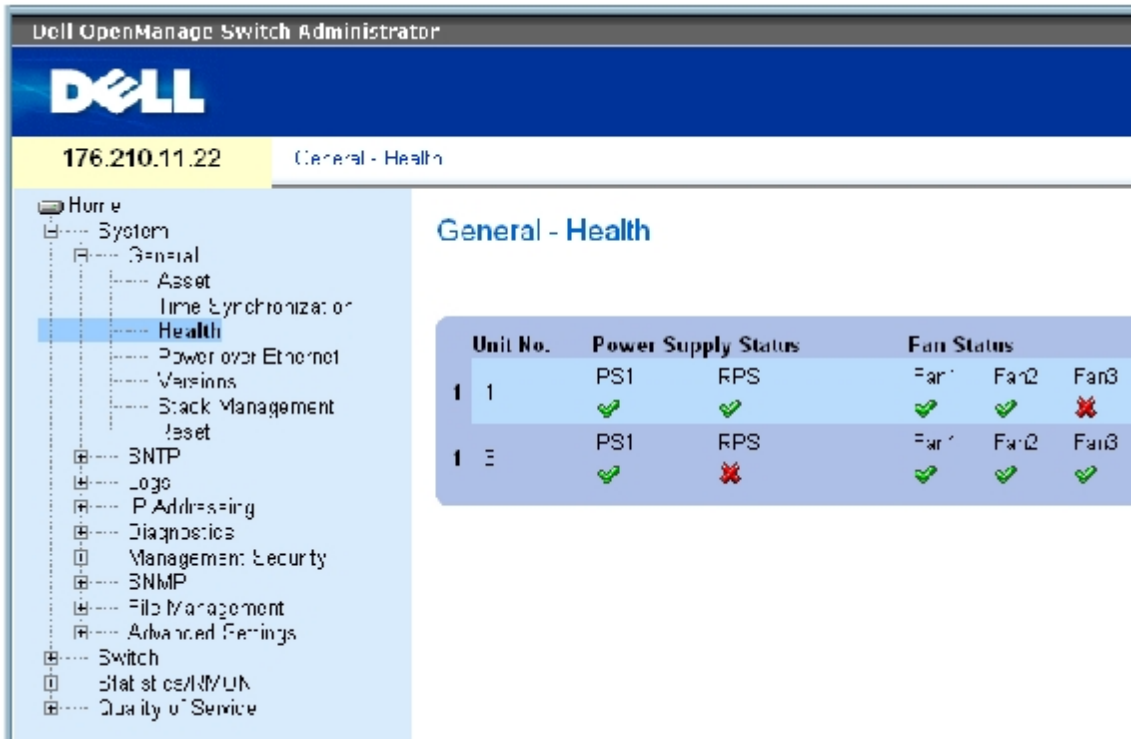
以下に CLI コマンドの例を示します。

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


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


console(config)# clock
source sntp


console(config)# interface
ethernet e14


console(config-if)# sntp
client enable


console(config-if)# exit


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

システムヘルス情報の表示

システムヘルスページは、デバイスの電源や換気に関する情報を含む、デバイスの物理的情報を表示します。システムヘルスページを開くにはツリービューから**System**（システム）→ **General**（一般）→ **Health**（ヘルス）をクリックします。

図**6-4** システムヘルス



システムヘルスページは以下のフィールドで構成されます。

Unit No.（ユニット番号）— デバイス資産情報を表示しているユニット番号を示します。

Power Supply Status（電源装置ステータス）— デバイスは 2 個の電源装置を内蔵しています。電源装置 1 は PS1 と表示され、冗長電源装置は RP Sと表示されます。表示されるフィールド値は以下のとおりです。

— 電源装置の動作は正常です。

— 電源装置の動作は正常ではありません。

Not Present（存在しない）— 電源装置は存在しません。

Fan Status（ファンステータス）— 非 PoE デバイスは 2 個のファンを内蔵し、PoE デバイスは 5 個のファンを内蔵しています。それぞれのファンは、ファンの末尾にファン番号が付記されて画面上に表示されます。表示されるフィールド値は以下のとおりです。

— ファンの動作は正常です。

— ファンの動作は正常ではありません。

Not Present（存在しない）— ファンが存在しません。

Temperature（温度）— デバイスが動作している場所の温度です。デバイス温度は摂氏を単位として表示されます。デバイス温度のしきい値は 0～40 ℃です。次の表は摂氏から華氏への換算表（5 ℃単位）です。

表**6-3** 摂氏から華氏への変換表

摂氏	華氏

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

CLI コマンドを使用したシステムヘルス情報の表示

システムヘルスページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-4** システムヘルス **CLI** コマンド

CLI コマンド	説明
show system [**unit** *unit*]	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 switch

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

System Contact:

System Name: RS1

System location:

System MAC Address: 00.10.B5.F4.00.01

Sys Object ID: 1.3.6.1.4.1.674.10895.3004

Type: PowerConnect 3424

Temperature Sensors:

Unit   Sensor   Temperature (Celsius)   Status
----   ------   ---------------------   ------
1      1                41              OK
1      2                41              OK
2      1                42              OK
```

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

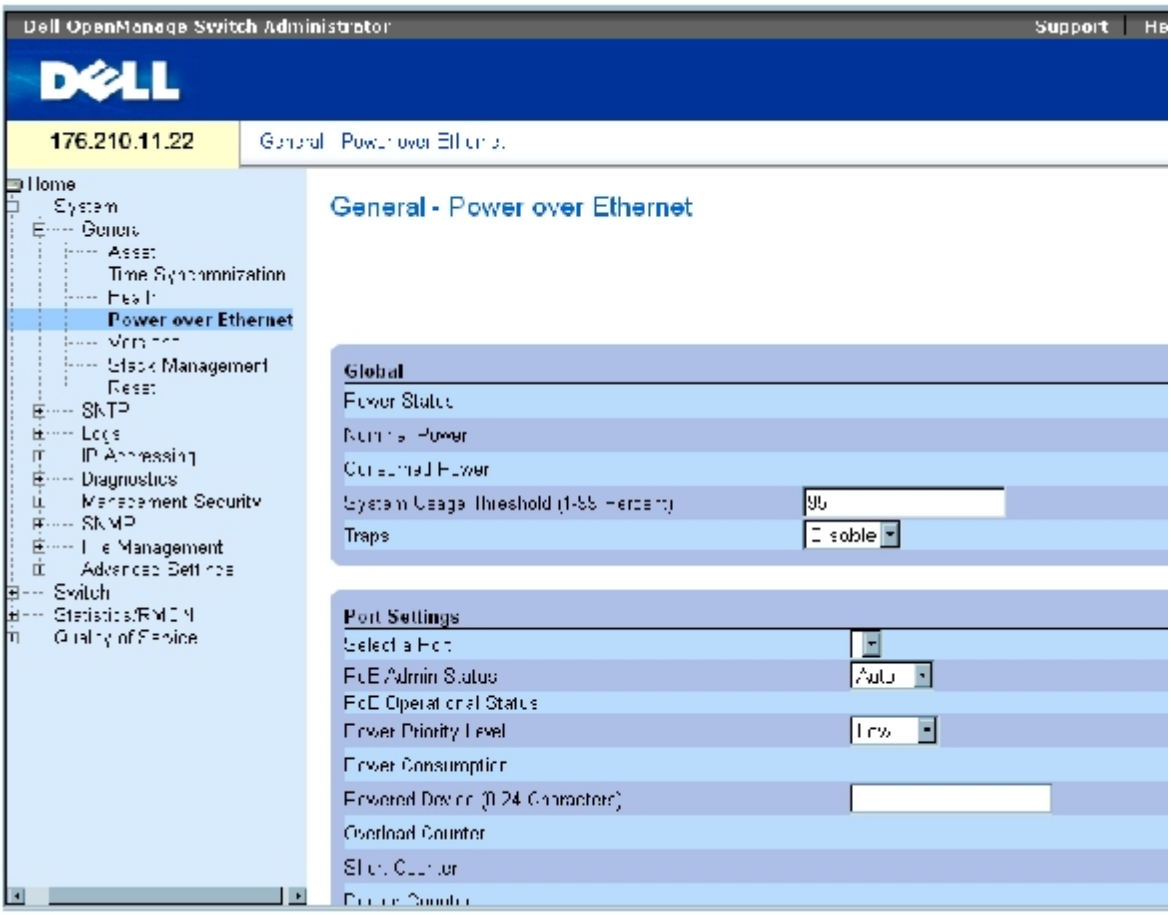
Power over Ethernetの管理

Power over Ethernet（PoE）は、ネットワーク基盤の更新や変更を必要とすることなく、既設の LAN ケーブルを使用して、デバイスに電源を供給する方式です。Power over Ethernet を用いれば、商用電源に近接させてネットワークデバイスを設置する必要はありません。

パワードデバイスとは、PowerConnect の電源装置から電源を受電するデバイスで、たとえば IP フォンが該当します。パワードデバイスは Ethernet ポートを介して PowerConnect デバイスと接続されます。パワードデバイスは、PowerConnect 3424P の FE 24 ポートか、PowerConnect 3448P の FE 48 ポートのいずれかを介して接続します。

Power over Ethernetページを開くには、ツリービューから、**System**（システム）→ **General**（一般）→ **Power over Ethernet**（Power over Ethernet）をクリックします。

図**6-5 Power over Ethernet**



Power over Ethernetページは以下のセクションで構成されます。

- Global（グローバル）
- Port Settings（ポート設定）

Global（グローバル）

Power over Ethernet の Global（グローバル）設定は以下のフィールドで構成されます。

Power Status（電源ステータス）— インライン電源ステータスを表示します。

On（オン）— 電源ユニットが機能していることを示します。

Off（オフ）— 電源ユニットが機能していないことを示します。

Faulty（故障）— 電源ユニットは機能しているもののエラーが発生していることを示します。たとえば、電源が過負荷になっているか、短絡状態になっている場合です。

Nominal Power（公称電力）— スイッチデバイスが供給できる実際の電力量を示します。フィールド値の単位はW（ワット）です。

Consumed Power （消費電力）— パワードデバイスによって使用されている電力量を示します。フィールド値の単位は W（ワット）です。

System Usage Threshold（**1**～**99 %**）（システム利用しきい値）— 消費電力が達したときにアラームを生成させるしきい値をパーセントで示します。フィールド値は 1～99 パーセントです。デフォルトは 95 パーセントです。

Traps（トラップ）— PoE デバイストラップの受信を有効または無効にします。デフォルトの設定は無効です。

Port Settings（ポート設定）

Select a Port（ポートの選択）— 選択したポートに接続されているパワードインタフェースに、PoE パラメータを定義して割り当てるインタフェースを示します。

PoE Admin Status（PoE 管理ステータス）— デバイス PoE モードを示します。表示されるフィールド値は以下のとおりです。

Auto（自動）— デバイス発見プロトコルを有効にし、 PoE モジュールを使用して電力をデバイスに供給します。デバイス発見プロトコルは、デバイスのインタフェースに接続されたパワードデバイスを発見し、そのクラス分けを学習します。これはデフォルト設定です。

Never（拒絶）— デバイス発見プロトコルを無効にし、PoE モジュールを使用したデバイスに対する電力供給を停止します。

PoE Operational Status（PoE 動作ステータス）— ポートの PoE 動作が有効か表示します。表示されるフィールド値は以下のとおりです。

On（オン）— デバイスはインタフェースに電力を供給中です。

Off（オフ）— デバイスはインタフェースに電力を供給していません。

Test Fail（テスト失敗）— パワードデバイスのテストに失敗したことを示します。たとえば、ポートの設定が有効ではなかったため、パワードデバイスへの電力供給にそのポートを使用できない場合が該当します。

Testing（テスト実行）— パワードデバイスのテスト中であることを示します。たとえば、パワードデバイスをテストして、電源から電力を受電できるかどうか確認する場合が該当します。

Searching（検索中）— PowerConnect デバイスがパワードデバイスを検索中であることを示します。Searching（検索中）は PoE 動作ステータスのデフォルトです。

Fault（故障）— PowerConnect デバイスがパワードデバイスで故障を検出したことを示します。あとえば、パワードデバイスのメモリを読み取ることができない場合が該当します。

Power Priority Level（電力優先レベル）— 電源供給が低下した場合のポート優先度を決定します。ポート電力優先度は電源の供給が低下した場合に使用されます。このフィールドのデフォルトは Low（低）です。たとえば、電源が使用率 99% で動作中の場合に、ポート 1 が優先度 High（高）として割り当てられ、一方ポート 3 は優先度 Low（低）として割り当てられていると、ポート 1 への電力供給が優先され、ポート 3 への電力供給は拒絶される可能性があります。

Critical（クリティカル）— 最高の電力優先レベルを割り当てます。

High（高）— 2 番目に高い電力優先レベルを割り当てます。

Low（低）— 最も低いの電力優先レベルを割り当てます。

Power Consumption（消費電力）— 指定インタフェースに接続されるパワードデバイスに割り当てられた電力量を示します。デバイスはパワードデバイスによってクラス分けされ、PowerConnect デバイスはクラス情報を使用します。フィールド値の単位は W（ワット）です。表示されるフィールド値は以下のとおりです。

0.44 ～12.95 — ポートに 0.44W～12.95W の電力消費レベルが割り当てられていることを示します。

0.44～3.8 — ポートに 0.44W～3.8W の電力消費レベルが割り当てられていることを示します。

3.84～6.49 — ポートに 3.84W～6.49W の電力消費レベルが割り当てられていることを示します。

6.49～12.95 — ポートに 6.49W～12.95W の電力消費レベルが割り当てられていることを示します。

Power Device（**0**～**24** 文字）（パワードデバイス）**—** ユーザー定義のパワードデバイスの説明を与えます。フィールドの長さは最大 24 文字です。

Overload Counter（過負荷カウンタ）**—** 電力過負荷の発生回数を示します。

Short Counter（電力不足カウンタ）**—** 電力不足の発生回数を示します。

Denied Counter（拒絶カウンタ）**—** パワードデバイスへの電力供給が拒絶された回数を示します。

Absent Counter（不在カウンタ）**—** パワードデバイスが検出されず、パワードデバイスへの電力供給を停止した回数を示します。

Invalid Signature Counter（無効シグネチャカウンタ）**—** 無効なシグネチャを受信した回数を示します。シグネチャはパワードデバイスが PSE に対して自分自身を識別させる手段です。シグネチャは、パワードデバイスの検出、クラス分け、またはメンテナンス中に生成されます。

PoE 設定の定義

□□□ Power over Ethernetページを開きます。

□□□ 各フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

PoE 設定が定義され、デバイスがアップデートされます。

CLI を使用した PoE の管理

Power over Ethernetページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-5 POE** 設定 **CLI** コマンド

CLI コマンド	説明
power inline {auto | never}	インタフェース上のインラインパワーの管理モードを設定します。
power inline powered-device *pd-type*	パワードデバイスタイプの説明を追加します。
power inline priority {critical | high | low}	インラインパワー管理の観点からインタフェースの優先度を設定します。
power inline usage-threshold	アラームをトリガーするしきい値を設定します。
power inline traps enable	PoE デバイストラップを有効にします。

show power inline [ethernet interface]	PoE 設定情報を表示します。

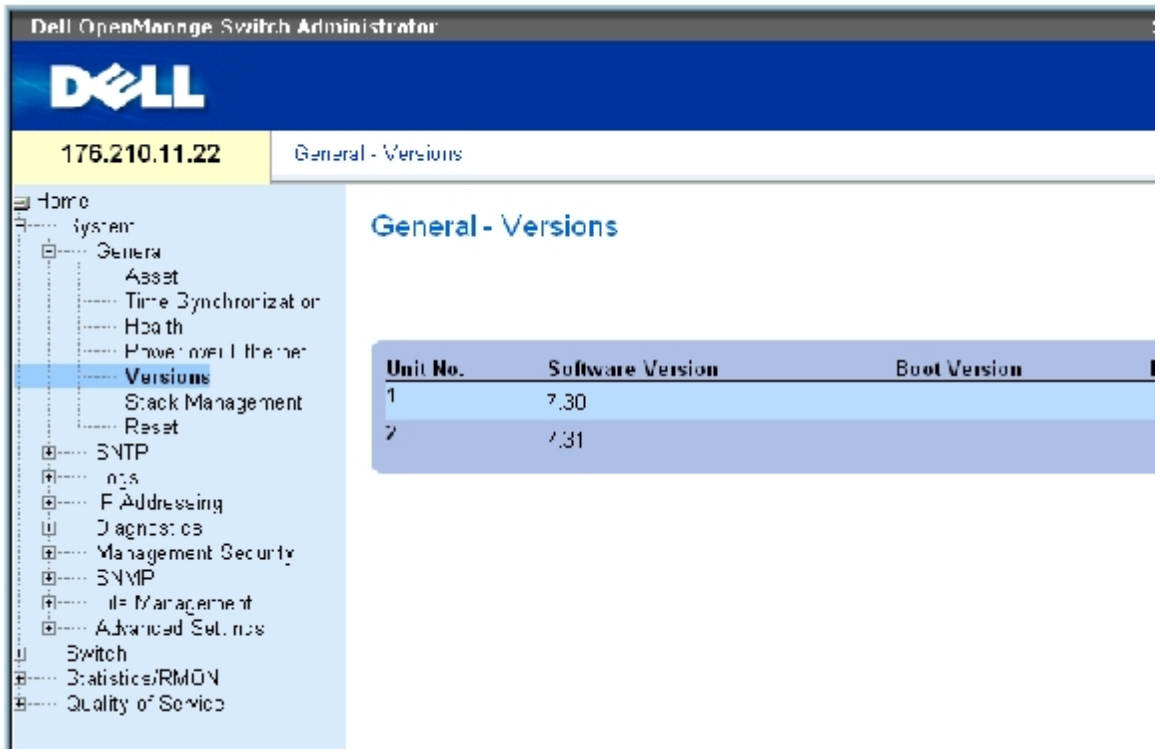
以下に CLI コマンドの例を示します。

```
Console# show power inline

Power: On

Nominal Power: 150 Watts

Consumed Power: 120 Watts (80%)

Usage Threshold: 95%

Traps: Enabled

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


Console# show power inline ethernet 1/e1

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

Overload Counter: 1

Short Counter: 0

Denied Counter: 0

Absent Counter: 0

Invalid Signature Counter: 0
```

バージョン情報の表示

バージョンページには、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関する情報が表示されます。バージョンページを開くにはツリービューから System（システム）→ General（一般）→ Versions（バージョン）をクリックします。

図**6-6** バージョン



バージョンページは以下のフィールドで構成されます。

Unit No.（ユニット番号）— デバイス資産情報が表示されているユニット番号を示します。

Software Version（ソフトウェアバージョン）— デバイス上で動作しているソフトウェアのバージョンです。

Boot Version（ブートバージョン）— デバイス上で動作しているブートバージョンです。

Hardware Version（ハードウェアバージョン）— デバイスのハードウェアバージョンです。

CLI を使用したデバイスバージョンの表示

バージョンページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-6** バージョン **CLI** コマンド

CLI コマンド	説明
show version	システムバージョン情報を表示します。

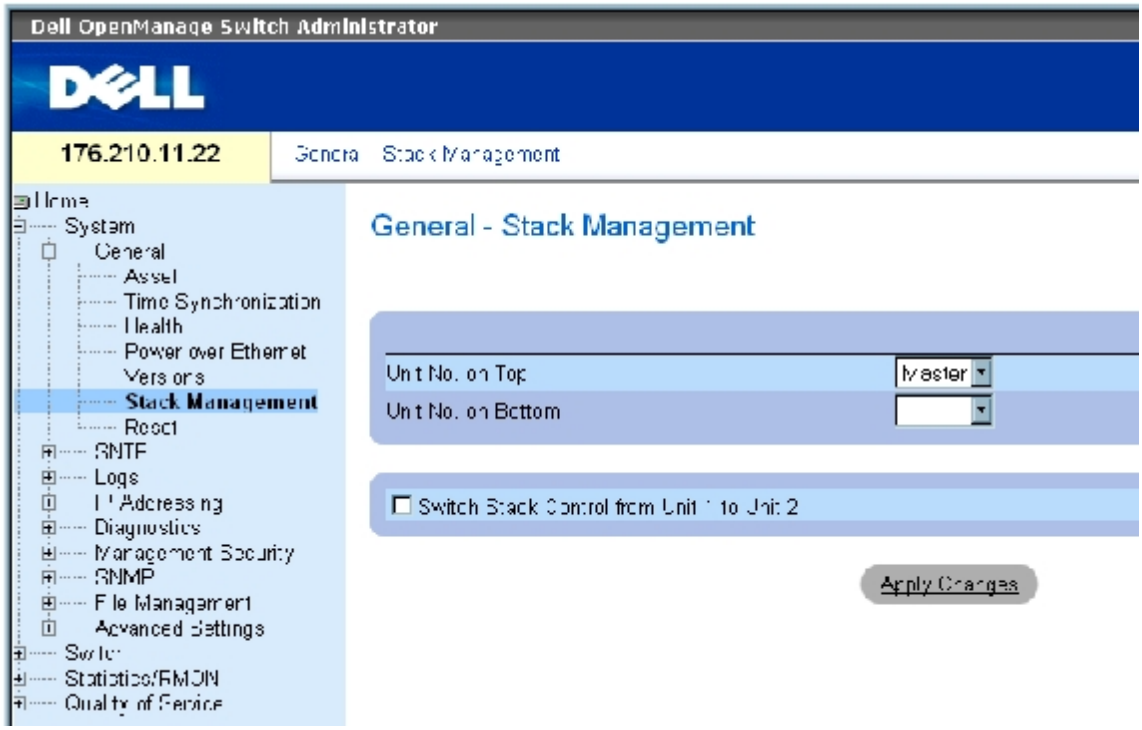
以下に CLI コマンドの例を示します。

```
console> show version

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

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

HW version 1.0.0
```

スタッキングメンバーの管理

スタッキング管理ページから、ネットワーク管理者は、スタッキング全体または特定のデバイスのいずれかのリセットが可能です。スタッキング管理ページを開くには、ツリービューから **System**（システム）→ **General**（一般）→ **Stack Management**（スタッキング管理）をクリックします。

図**6-7** スタッキング管理



メモ： デバイスをリセットする前に、動作中設定ファイルにすべての変更を保存してくださ い。現在のデバイス設定が失われることを防止するためです。設定ファイルの保存方法につ いては、「ファイルの管理」を参照してください。

Unit No. on Top（上部のユニット番号）— 最初のスタッキングメンバーの番号です。設定可能な値は、Master（マスター）および 1～6です。

Unit No. on Bottom（下部のユニット番号）— 第2のスタッキングメンバーの番号です。設定可能な値は、Master（マスター）および 1～6です。

Switch Stack Control from Unit 1 to Unit 2（スタッキング制御をユニット 1 からユニット 2 へ切り替える）— 現在のスタックマスターユニットからバックアップマスターユニットへの切り替えを有効にします。

メモ： マスターユニットをリセットするとスタッキング全体がリセットされます。

スタッキングマスターの切り替え

□□□ スタッキング管理ページを開きます。

□□□ Switch Stack Control from Unit 1 to Unit 2（スタッキング制御をユニット 1 からユニッ ト 2 へ切り替える）チェックボックスにチェックを入れます。

□□□ Apply Changes（変更の適用）をクリックします。

確認メッセージが表示されます。

□□□ 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の入力を求められます。

スタッキング表示順の設定

□□□ スタッキング管理ページを開きます。

□□□ 上部ユニットと下部ユニットを定義することで、スタッキングのトポロジを定義しま す。これら両ユニットは隣接していなければなりません。

□□□ **Apply Changes**（変更の適用）をクリックします。

システムページの表示順が再構成されます。

CLIコマンドを使用したスタッキング管理

スタッキング管理ページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-7** スタック管理 **CLI** コマンド

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。
stack reload	スタッキングメンバーをリロードします。
stack master	選択対象をスタッキングマスターに設定します。

以下に CLI コマンドの例を示します。

```
console# reload

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

デバイスのリセット

リセットページから、デバイスをリモートでリセットすることが可能です。リセットページを開くには、ツリービューから、System（システム）→ General（一般）→ Reset（リセット）をクリックします。

Reset（リセット）は以下のフィールドで構成されます。

Reset Unit No.（ユニット番号のリセット）— 指定したスタッキングメンバーをリセットします。

メモ： デバイスをリセットする前に、スタートアップ設定ファイルにすべての変更を保存し てください。現在のデバイス設定が失われることを防止するためです。設定ファイルの保存 方法については、「"ファイルの管理"」を参照してください。

デバイスのリセット

□□□ リセット ページを開きます。

□□□ **Reset Unit Number**（ユニット番号のリセット）フィールドからユニットを 1 つ選択し ます。

□□□ **Apply Changes**（変更の適用）をクリックします。

確認メッセージが表示されます。

□□□ **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の入力を求められます。

□□□ ユーザー名とパスワードを入力し、Web インタフェースに再接続してください。

CLI を使用したデバイスのリセット

CLI を介してデバイスのリセットと等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-8** リセット **CLI** コマンド

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] ?
```

SNTP の設定

本スイッチは Simple Network Time Protocol（SNTP）をサポートしています。SNTP は、ネットワークデバイスのクロック時刻に、ミリ秒単位での正確な同期を保証します。時刻同期はネットワーク SNTP サーバーによって処理されます。デバイスは SNTP クライアントとして動作するのみであり、他のシステムへ時刻サービスを提供することはできません。

スイッチは以下のサーバータイプのサーバー時刻をポーリングします。

- ユニキャスト
- エニキャスト
- ブロードキャスト

時刻ソースは stratum（階層）によって確立されます。stratum は基準クロックの精度を決定します。高次（ゼロが最高）の startum ほどクロックの精度は高くなります。スイッチは stratum-1 以上から時刻を受信します。以下に stratum の例を示します。

- **Stratum 0 —** たとえば GPS システムなどの外部時計をクロック源として直接参照していることを示します。
- **Stratum 1** —stratum-0 の時計を直接参照するサーバーが使用されていることを示します。stratum-1 タイムサーバーはプライマリネットワークの時刻標準となります。
- **Stratum 2** —ネットワーク経路を介して stratum-1 サーバーよりもクロック源が離れていることを示します。たとえば straturm-2 サーバーは、stratum-1 サーバーから NTP を使用して、ネットワークリンクを介して時刻を受信しているサーバーです。

SNTP サーバーから受信した情報は、時刻レベルとサーバータイプに基づき評価されます。SNTP 時刻定義は以下の時刻レベルによって評価および定義されます。

- **T1** —クライアントが最初の要求を送信した時刻。
- **T2**— サーバーが最初の要求を受信した時刻。
- **T3** —サーバーがクライアントに応答を送信した時刻。
- **T4**—クライアントがサーバーから応答を受信した時刻。

デバイスは以下のサーバータイプのサーバー時刻をポーリングします。ユニキャスト、エニキャスト、ブロードキャスト。

ユニキャスト情報のポーリング処理は、IP アドレスが判明しているサーバーのポーリングに使用されます。本デバイスに設定した SNTP サーバーが、同期情報をポーリングする唯一の対象になります。サーバー時刻を決定するために T1～T4 を使用します。デバイスの時刻をもっとも確実に同期させる推奨の方法です。この方法が選択された場合、**SNTP** サーバー ページでデバイス内に定義された SNTP サーバーから送られてくる SNTP 情報のみをデバイスは受け付けます。

エニキャストのポーリング処理は、サーバーの IP アドレスが未知の場合に使用されます。この方法が選択された場合、ネットワーク上のすべての SNTP サーバーが同期情報を送信します。デバイスは同期情報を主体的に要求したときのみ同期を行います。デバイスが発した同期情報の要求に対して、最初に応答した 3 つの SNTP サーバーから得られたうちの最善の応答（低次の stratum）が、時刻値の設定に使用されます。時刻レベル T3 と T4 を使ってサーバー時刻を決定します。

デバイスの時刻同期に必要な時刻情報の取得は、ブロードキャストポーリングよりも、エニキャストポーリングのほうが好まれます。ただしこの方法は、デバイスに指定されていない SNTP サーバーから発せられた SNTP パケットも受け付けてしまうことから、ユニキャストポーリングよりも確実性が低下します。

サーバーの IP アドレスが未知の場合にブロードキャスト情報を使用します。SNTP サーバーからブロードキャストメッセージが送信されると、SNTP クライアントはメッセージをリスンします。ブロードキャストポーリングが有効の場合、デバイスが要求していなくとも、同期情報は受け取られます。もっとも確実性が低い方法です。

デバイスは、主体的に情報を要求したときか各ポーリング間隔のいずれかに、同期情報を取得します。ユニキャスト、エニキャスト、またはブロードキャストポーリングが有効の場合、情報は次の順番で取得されます。

- デバイス内に設定されているサーバーからの情報が好まれます。ユニキャストポーリングが有効ではない場合、またはデバイスにサーバーが定義されていない場合、デバイスは応答したいかなる SNTP サーバーからの時刻情報も受理します。
- 2 つ以上のユニキャストデバイスが応答した場合、より低次の stratum デバイスから発せられた同期情報が適します。
- サーバーが同一の stratum を持つ場合、最初に応答した SNTP サーバーからの同期情報が受理されます。

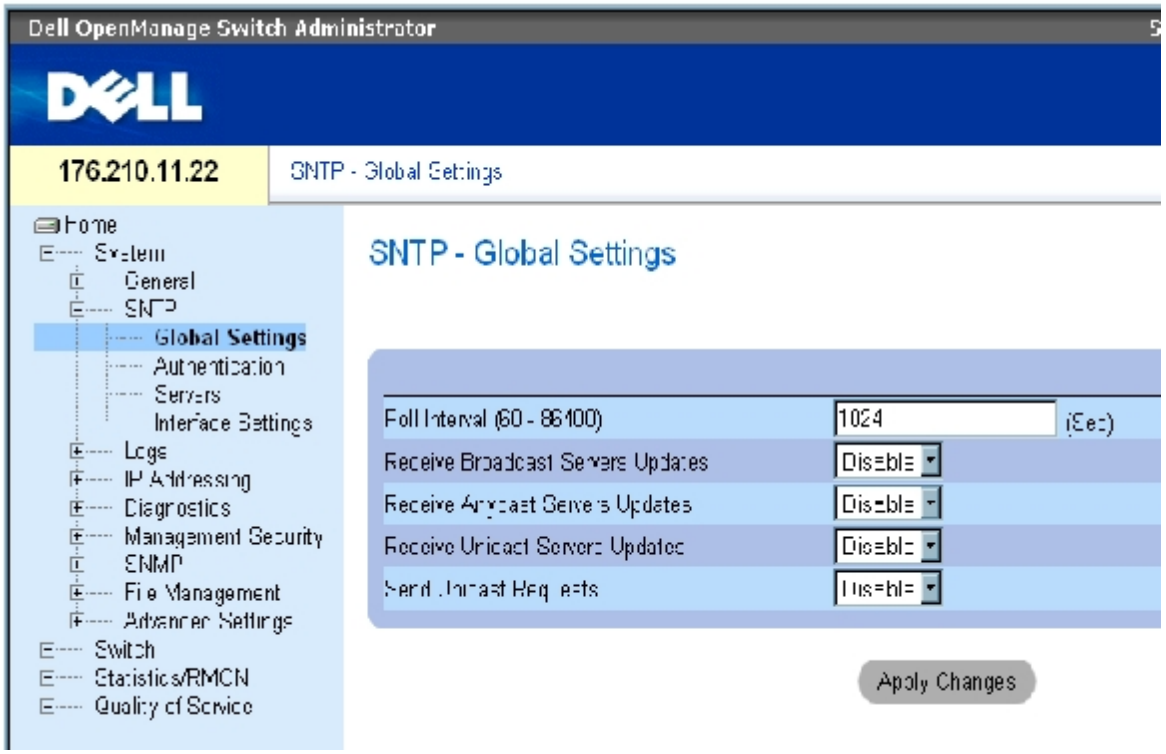
MD5（Message Digest 5）認証が SNTP サーバーへのデバイス同期経路を保護します。MD5 は 128 ビットハッシュを生成するアルゴリズムの 1 つです。MD5 は MD4 の変種の 1 つで、MD4 よりも高いセキュリティを有します。MD5 は通信の完全性を確認し、通信の起点を認証します。

SNTP ページを開くには、ツリービューから**System**（システム）→ **SNTP**（SNTP）をクリックします。

SNTP グローバルパラメータの定義

SNTP グローバル設定ページには、SNTP パラメータのグローバル定義に関する情報がまとめられています。**SNTP** グローバル設定ページを開くには、ツリービューから **System**（システム）→ **SNTP**（SNTP）→ **Global Settings**（グローバル設定）をクリックします。

図**6-8 SNTP** グローバル設定



SNTP グローバル設定ページは、以下のフィールドで構成されます。

Poll Interval（**60**～**86400**）（ポーリング間隔）— SNTP サーバーに対してユニキャスト情報をポーリングする間隔（秒）を定義します。デフォルトのポーリング間隔は 1024 秒です。

Receive Broadcast Servers Updates（ブロードキャストサーバー更新の受信）— 有効に設定されている場合に、ブロードキャストサーバー時刻情報を得るために、選択したインタフェース上の SNTP サーバーをリスンします。

Receive Anycast Servers Updates（エニキャストサーバー更新の受信）— 有効に設定されている場合に、エニキャストサーバー時刻情報を得るために SNTP サーバーをポーリングします。 **Receive Anycast Servers Update**（エニキャストサーバー更新の受信）と**Receive Broadcast Servers Update**（ブロードキャストサーバー更新の受信）の両方のフィールドが有効の場合、システム時刻はエニキャストサーバー時刻情報に従って設定されます。

Receive Unicast Servers Updates（ユニキャストサーバー更新の受信）— 有効に設定されている場合に、ユニキャストサーバー時刻情報を得るために SNTP サーバーをポーリングします。**Receive Broadcast Servers Update**（ブロードキャストサーバー更新の受信）、**Receive Anycast Servers Update**（エニキャストサーバー更新の受信）、さらには**Receive Unicast Servers Updates**（ユニキャストサーバー更新の受信）の各フィールドがすべて有効の場合、システム時刻はユニキャストサーバー時刻情報に従って設定されます。

Send Unicast Requests（ユニキャスト要求の送信）— 有効に設定されている場合に、SNTP サーバーに対して SNTP ユニキャストサーバー時刻情報要求を送信します。

クロック源の選択

□□□ 時刻同期ページを開きます。

□□□ **Clock Source**（クロック源）フィールドを定義します。

□□□ Apply Changes（変更の適用）をクリックします。

クロック源が選択され、デバイスがアップデートされます。

ローカルクロック設定の定義

□□□ 時刻同期ページを開きます。

□□□ 各フィールドを定義します。

□□□ Apply Changes（変更の適用）をクリックします。

ローカルクロック設定が適用されます。

CLI コマンドを使用した SNTP グローバルパラメータの定義

SNTP グローバル設定ページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-9 SNTP** グローバルパラメータ **CLI** コマンド

CLI コマンド	説明
sntp broadcast client enable	SNTP ブロードキャストクライアントを有効にします。
sntp anycast client enable	SNTP エニキャストクライアントを有効にします。
sntp unicast client enable	SNTP 設定済みユニキャストクライアントを有効にします。

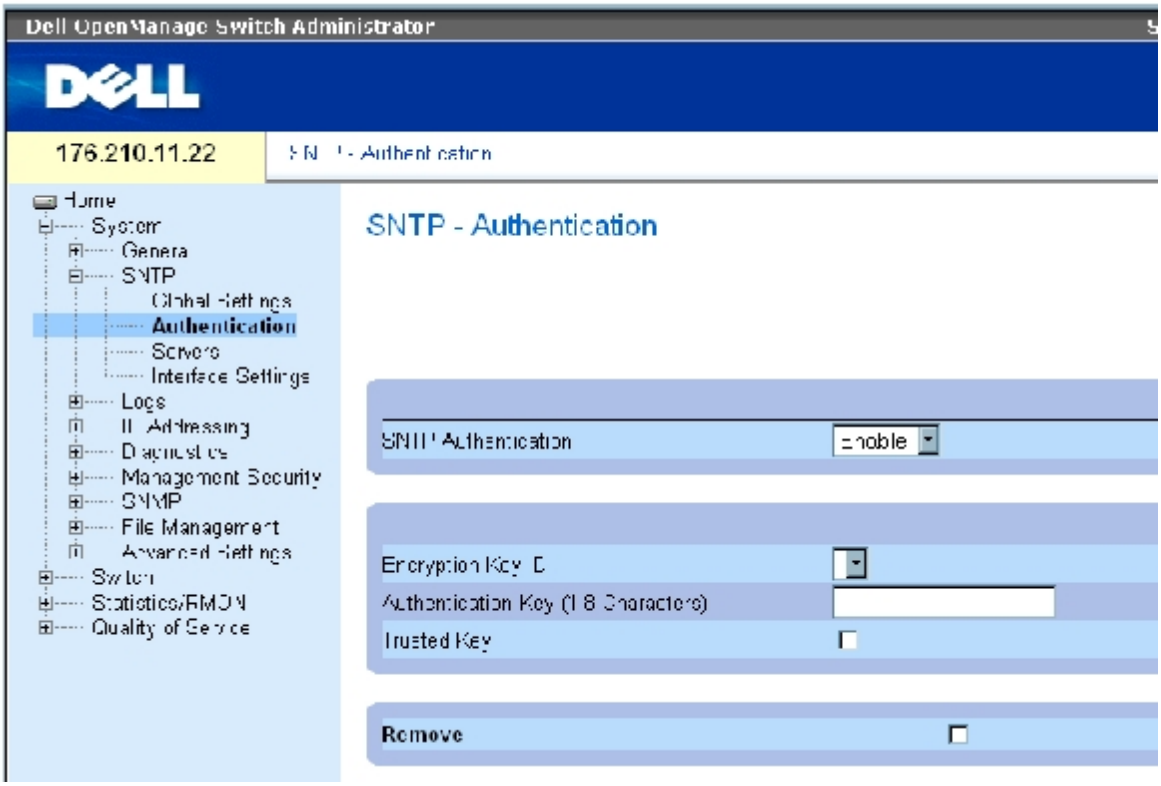
以下に CLI コマンドの例を示します。

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

SNTP 認証方法の定義

SNTP 認証ページから、デバイスと SNTP サーバー間の SNTP 認証を有効にします。SNTP サーバーを認証する手段もSNTP 認証ページから選択します。SNTP 認証ページを開くには、ツリービューから、**System**（システム）→ **SNTP**（SNTP）→ **Authentication**（認証）をクリックします。

図**6-9 SNTP** 認証



SNTP 認証ページは以下のフィールドで構成されています。

SNTP Authentication（SNTP 認証）— SNTP セッションが有効に設定されているとき、デバイスと SNTP サーバー間の SNTP セッションの認証を有効にします。

Encryption Key ID（暗号キー ID）— SNTP サーバーとデバイスの認証に使用するキーIDを定義します。フィールド値は最大で **4294967295** です。

Authentication Key（**1**～**8** 文字）（認証キー）— 認証に使用するキーです。

Trusted Key（信用できるキー）— SNTP サーバーの認証に使用される暗号キー（ユニキャスト）を示します。

Remove（削除）— チェックすることで、選択した認証キーを削除します。

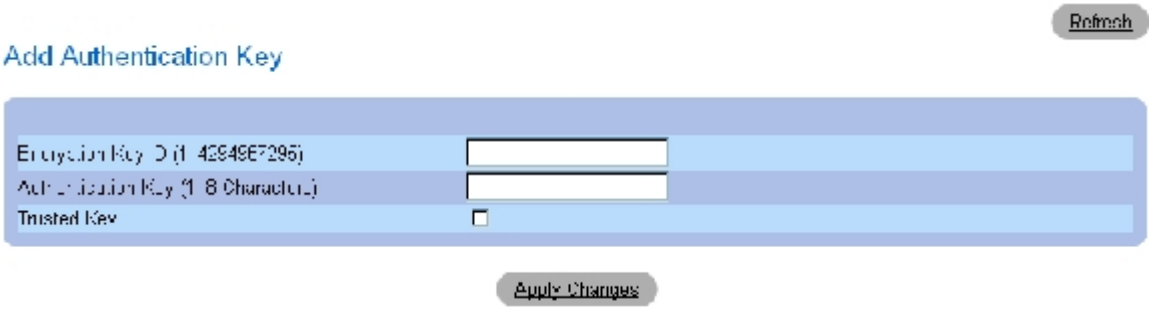
SNTP 認証キーの追加

□□□ **SNTP** 認証ページを開きます。

□□□ **Add**（追加）をクリックします。

ページが開きます。

図**6-10** 認証キーの追加



□□□ 各フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

SNMP 認証キーが追加され、デバイスがアップデートされます。

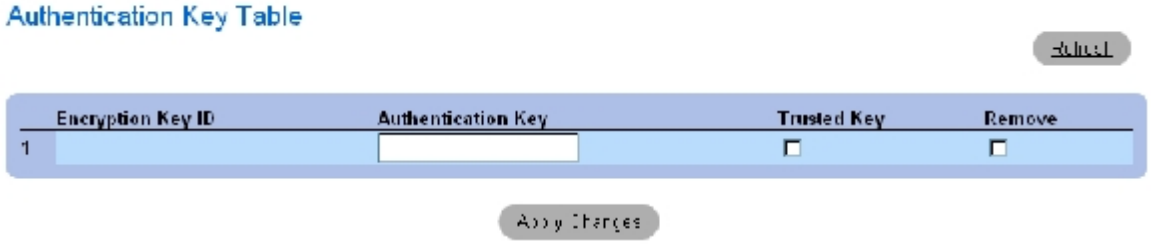
認証キー表の表示

□□□ **SNTP** 認証ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

認証キー表が開きます。

図**6-11** 認証キー表



認証キーの削除

□□□ **SNTP** 認証ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

認証キー表が開きます。

□□□ **Authentication Key Table**（認証キー表）のエントリを 1 つ選択します。

□□□ **Remove**（削除）チェックボックスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択した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 SNTP 認証設定の定義

SNTP 認証ページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-10 SNTP** 認証 **CLI** コマンド

CLI コマンド	説明
sntp authenticate	サーバーから受信した Simple Network Time Protocol（SNTP）トラフィックに対する認証を定義します。
sntp trusted key	SNTP が同期を行うシステムの識別性を認証します。
sntp authentication-key *number* **md5** *value*	SNTP 用認証キーを定義します。

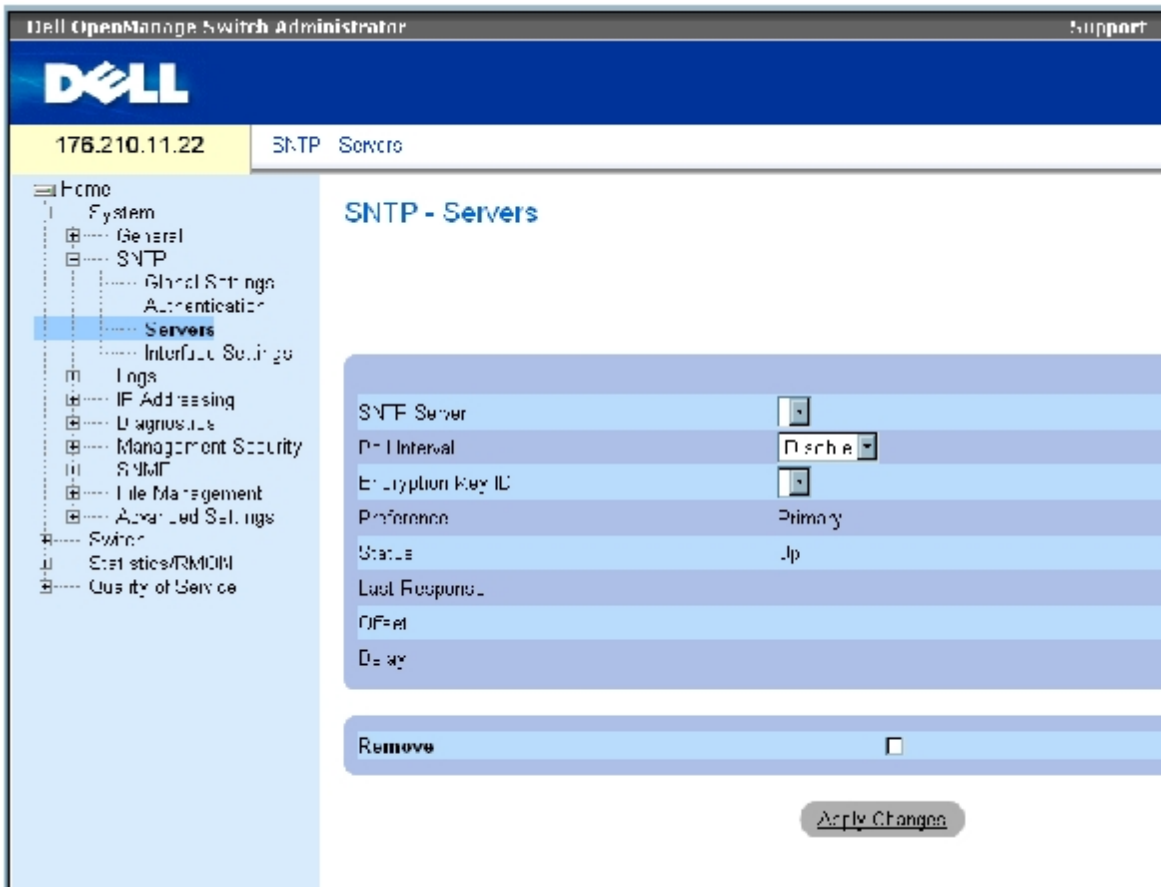
以下に CLI コマンドの例を示します。

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

console(config)# sntp
trusted-key 8

Console(config)# sntp
authenticate
```

SNTP サーバーの定義

SNTP サーバーの有効化や新規SNTPサーバーの追加は、**SNTP サーバー**ページから行います。**SNTP サーバー**ページを開くには、ツリービューから、**System**（システム）→ **SNTP**（SNTP）→ **Servers**（サーバー）をクリックします。

図**6-12 SNTP** サーバー



SNTP サーバーページは以下のフィールドで構成されています。

SNTP Server（SNTP サーバー）— ユーザー定義の SNTP サーバー IP アドレスを選択します。最大で 8 台の SNTP サーバーを定義することが可能です。

Poll Interval（ポーリング間隔）— 指定した SNTP サーバーが有効な場合に、システム時刻情報のポーリングを有効にします。

Encryption Key ID（暗号キー ID）— SNTP サーバーとデバイスの通信に使用するキー ID を定義します。値の範囲は 1～4294967295 です。

Preference（優先）— SNTP システム時刻情報を提供する SNTP サーバーです。フィールド値は以下のとおりです。

Primary（プライマリ）— プライマリサーバーが SNTP 情報を提供します。

Secondary（セカンダリ）— バックアップサーバーが SNTP 情報を提供します。

Status（ステータス）— 動作中の SNTP サーバーステータス。表示されるフィールド値は以下のとおりです。

Up（稼動中）— SNTP サーバーは正常に動作しています。

Down（停止中）— SNTP サーバーは現在利用できません。たとえば、その時点で接続されていない SNTP サーバー、または停止中のサーバーが該当します。

In progress（処理中）— SNTP サーバーは SNTP 情報を送信中または受信中です。

Unknown（不明）— 現在送信されている SNTP 情報の処理の進み度合いは不明です。たとえば、デバイスがインタフェースを探している場合が該当します。

Last Response（最終の応答）— SNTP サーバーから応答を最後に受信した時刻です。

Offset（偏差）— デバイスローカル時刻と SNTP サーバーから取得した時刻のタイムスタンプの差。

Delay（遅延）— SNTP サーバーに到達するまでに要した時間量。

Remove（削除）— 選択することで、特定の SNTP サーバーを**SNTP Servers**（SNTP サーバー）リストから削除します。

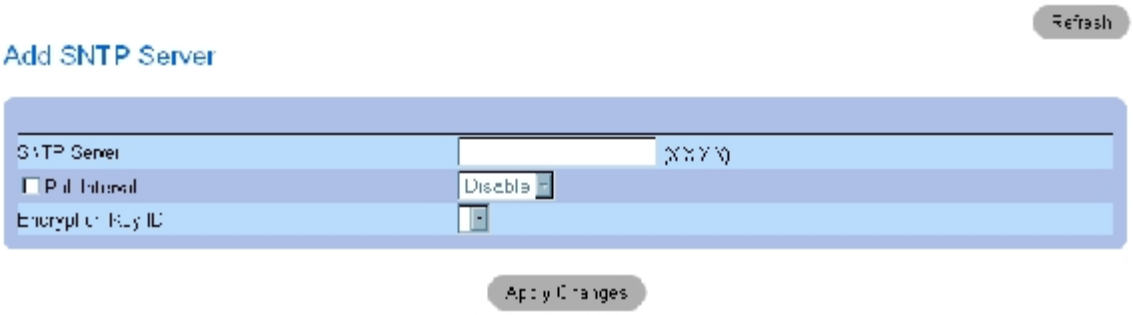
SNTP サーバーの追加

□□□ **SNTP** サーバーページを開きます。

□□□ Add（追加）をクリックします。

SNTP サーバーの追加ページが開きます。

図**6-13 SNTP** サーバーの追加



□□□ 各フィールドを定義します。

□□□ Apply Changes（変更の適用）をクリックします。

SNTP サーバーが追加され、デバイスがアップデートされます。

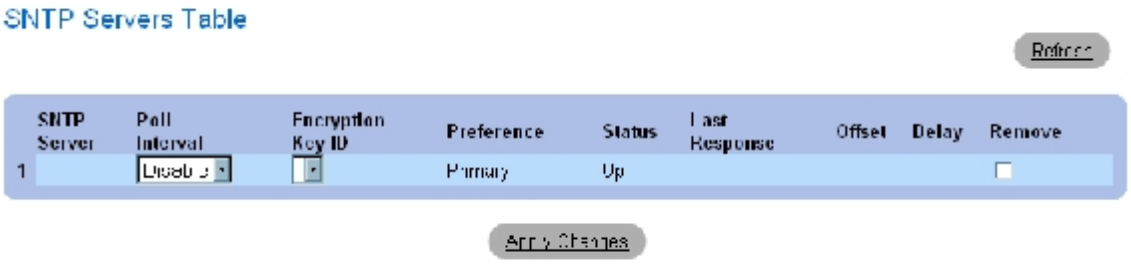
SNTP サーバー表の表示

□□□ **SNTP** サーバーページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

SNTP サーバー表が開きます。

図**6-14 SNTP** サーバー表



SNTP サーバーの変更

□□□ **SNTP** サーバーページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

SNTP サーバー表が開きます。

□□□ SNTP サーバーエントリを 1 つ選択します。

□□□ 各関連フィールドを変更します。

□□□ Apply Changes（変更の適用）をクリックします。

SNTP サーバー情報が更新されます。

SNTP サーバーの削除

□□□ **SNTP** サーバーページを開きます。

□□□ Show All（すべてを表示）をクリックします。

SNTP サーバー表が開きます。

□□□ **SNTP Server**（SNTP サーバー）エントリを 1 つ選択します。

□□□ **Remove**（削除）チェックボックスを選択します。

□□□ Apply Changes（変更の適用）をクリックします。

指定した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 SNTP サーバー設定の定義

SNTP サーバーページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-11 SNTP** サーバー **CLI** コマンド

CLI コマンド	説明

sntp server ip-address|hostname [poll] [key keyid]	SNTP を使用した要求の送信とサーバーからの SNTP トラフィックの受信を行うように、デバイスを設定します。

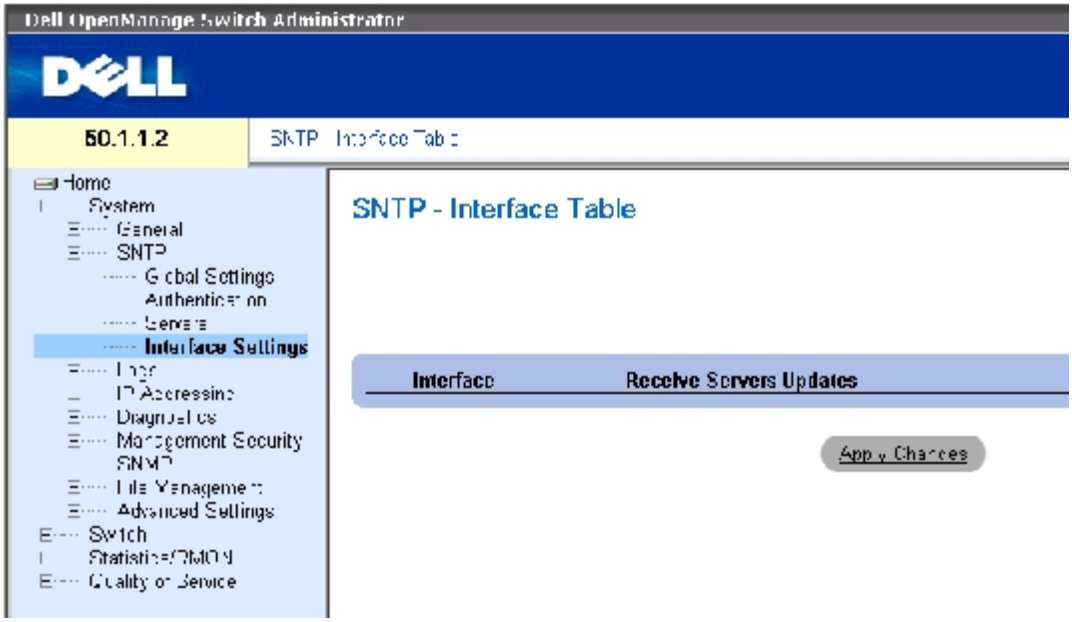
以下に CLI コマンドの例を示します。

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

SNTP インタフェースの定義

SNTP インタフェースの設定ページは SNTP インタフェース情報で構成されています。SNTP インタフェースの設定ページを開くには、System（システム）→ SNTP（SNTP）→ Interface Settings（インタフェースの設定）をクリックします。

図6-15 SNTP インタフェースの設定



SNTP インタフェースの設定ページは以下のフィールドで構成されます。

Unit No.（ユニット番号）— SNTP インタフェースが有効になっているスタッキングメンバーを示します。

Interface（インタフェース）— SNTP を有効にすることができるインタフェースのリストで構成されています。

Receive Servers Updates（サーバー更新の受信）— 特定インタフェースの SNTP を有効または無効にします。

Remove（削除）— 選択によって、SNTP を特定インタフェースから削除します。

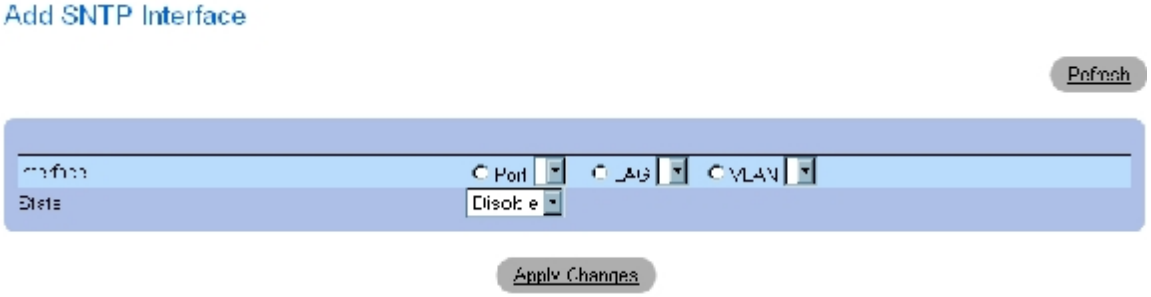
SNTP インタフェースの追加

□□□ SNTP インタフェースの設定ページを開きます。

□□□ Add（追加）をクリックします。

SNTP インタフェースの追加ページが開きます。

図**6-16 SNTP** インタフェースの追加



□□□ 各関連フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

SNTP 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。

CLI コマンドを使用した **SNTP** インタフェース設定の定義

SNTP インタフェースの設定ページ内のフィールド設定操作と等価な処理を実行する **CLI** コマンドを以下の表に示します。

メモ： 対象インタフェースをエニキャストインタフェースまたはブロードキャストインタ フェースとして設定を行うには、インタフェースに IP アドレスが定義されていなければなり ません。

表**6-12 SNTP** インタフェース設定 **CLI** コマンド

CLI コマンド	説明
sntp client enable	インタフェース上の Simple Network Time Protocol（SNTP）クライアントを有効にします。
show sntp configuration	Simple Network Time Protocol（SNTP）の設定を表示します。

以下に SNTP インタフェースを表示する CLI コマンドの例を示します。

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

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

Unicast Clients Polling: Enabled.
Server                          Polling     Encryption Key
------------                    --------    ---------------
```

176.1.1.8	Enabled	9
176.1.8.179	Disabled	Disabled
Broadcast Clients: Enabled		
Broadcast Clients Poll: Enabled		
Broadcast Interfaces:1/e1, 1/e3		

ログの管理

ログページには、各ログページへのリンクが張られています。ログページを開くには、ツリービューからSystem（システム）→ Logs（ログ）をクリックします。

グローバルログパラメータの定義

システムログは、デバイスイベントをリアルタイムで表示するとともに、後日の参照に備えてイベントを記録します。システムログは、イベントを記録および管理し、あわせて、エラーまたは情報メッセージを報告します。

すべてのエラー報告に対する System Logs プロトコル推奨メッセージフォーマットに従って、イベントメッセージには独自のフォーマットが割り当てられています。たとえば、syslog とローカルデバイスリポートメッセージには重要度コードが割り当てられており、また、メッセージを生成したソースアプリケーションを特定するメッセージニーモニックが含まれています。メッセージは、その重要性または関連性にもとづいてフィルタリングすることが可能です。ロギングバッファ、ロギングファイル、または syslog サーバーのようなさまざまな対象に対するロギングメッセージの分布は、syslog 設定パラメータで制御されます。ユーザーは最大で 8 つの syslog サーバーを定義することができます。

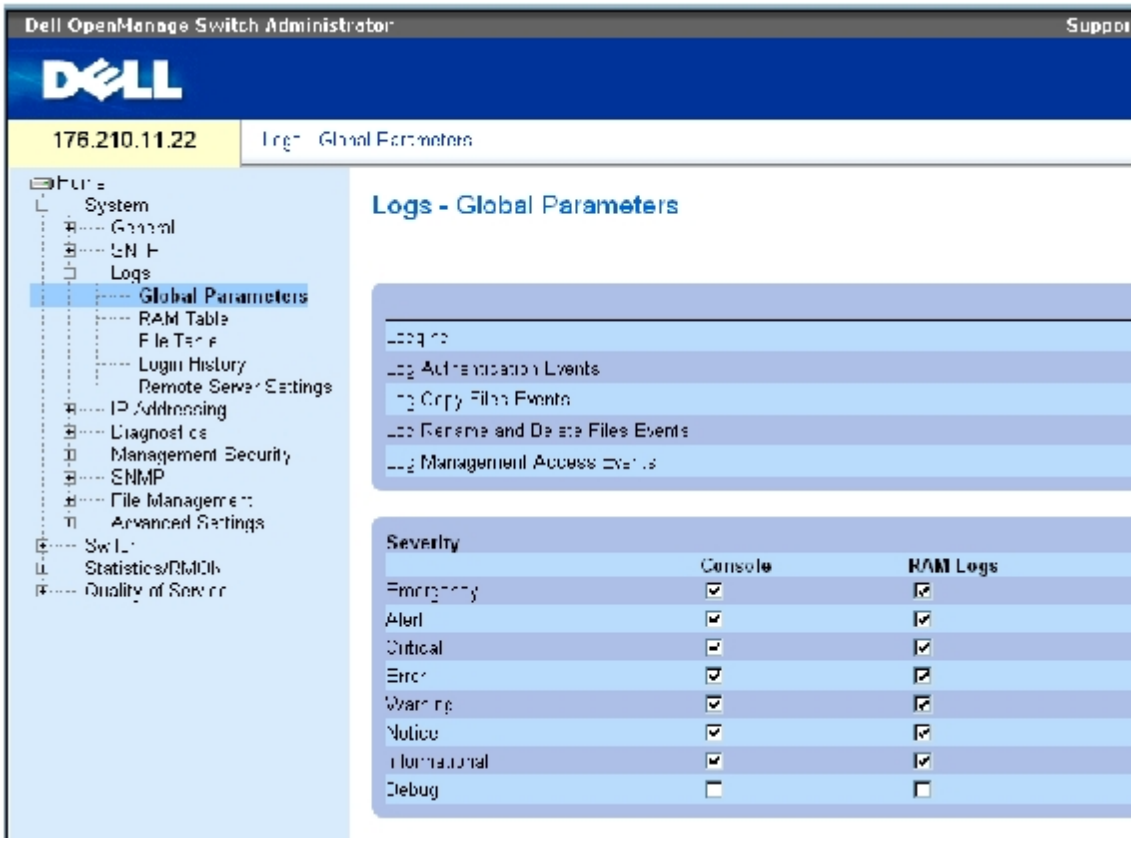
以下の表にログの重要度レベルを示します。

表**6-13** 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ません。
Alert	1	システムは速やかな対処を必要としています。
Critical	2	システムが危機的な状態になっています。
Error	3	システムエラーが発生しています。
Warning	4	システム警告が発生しています。
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。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連絡してください。

グローバルログパラメータページは、記録するイベントと記録先のログを定義するフィールドで構成されています。ログをグローバルに有効にするフィールドと、ログパラメータ定義のフィールドも、このページの中にあります。重要度ログメッセージは最も高い重要度から最も低い重要度の順に並んでいます。グローバルログパラメータページを開くには、ツリービューから System（システム）→ Logs（ログ）→ Global Parameters（グローバルパラメータ）をクリックします。

図**6-17** グローバルログパラメータ



グローバルログパラメータページは以下のフィールドで構成されています。

Logging（ロギング）— **Cache**（キャッシュ）、**File**（ファイル）、および **Server Log**（サーバーログ）のデバイスグローバルログを有効にします。コンソールログはデフォルトで有効です。

Log Authentication Events（認証イベントのログ）—ユーザーが認証されたときにログの生成を有効にします。

Log Copy Files Events（ファイルコピーイベントのログ）—ファイルがコピーされたときにログの生成を有効にします。

Log Rename and Delete Files Events（ファイルの名称変更と削除イベントのログ）—バックアップ構成ファイルの名前が変更されたとき、または削除されたときに、ログの生成を有効にします。

Log Management Access Events（管理アクセスイベントのログ）—管理方法によってデバイスがアクセスされたときに、ログの生成を有効にします。たとえば、SSHを使ってデバイスがアクセスされるごとに、デバイスはログを生成します。

Severity（重要度）— ログの重要度は以下のとおりです。

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、指定されたロギング場所に **emergency** ログメッセージが保存されます。

Alert — 2 番目に高い警告レベルを示します。重大なデバイス異常が存在する場合、たとえば、存在しない構成ファイルのダウンロードを試みた場合、**alert** ログが保存されます。

Critical — 3 番目に高い警告レベルを示します。重大なデバイス異常が存在する場合、たとえば、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、**critical** ログが保存されます。

Error — たとえばコピー操作に失敗した場合などのデバイスエラーが発生しています。

Warning — 最も低いデバイス警告レベルを示します。たとえば、デバイスは動作しているものの、ポートリンクがダウンしている場合が該当します。

Notice — 重要な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。たとえば、あるポートが現在動作中などです。

Debug — デバッグ用メッセージを提供します。

メモ： ある重要度レベルを選択すると、選択した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。

グローバルログパラメータページには、別ロギングシステムに対応するチェックボックスも存在します。

Console（コンソール）— ログをコンソールに送る最低の重要度レベルを示します。

RAM Logs（RAM ログ）— RAM（キャッシュ）に保存されているログファイルにログを送る最低の重要度レベルを示します。

Log File（ログファイル）— フラッシュメモリに保存されているログファイルにログを送る最低の重要度レベルを示します。

ログの有効化

□□□ グローバルログパラメータページを開きます。

□□□ **Logging**（ロギング）ドロップダウンリストから **Enable**（有効）を選びます。

□□□ **Global Log Parameters**（グローバルログパラメータ）の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。

□□□ **Apply Changes**（変更の適用）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

以下の表に、 グローバルログパラメータページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-14** グローバルログパラメータ **CLI** コマンド

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 | hostname} [port port] [severity level] [facility facility] [description text]	syslog サーバーにメッセージをロギングします。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	コンソールにロギングされるメッセージを重要度に基づいて制限します。
logging buffered level	内部バッファ（RAM）から出力表示される syslog メッセージを重要度に基づいて制限します。
logging file level	ロギングファイルへ送信する syslog メッセージを重要度に基づいて制限します。
clear logging	ログをクリアします。

clear logging file	ロギングファイルからメッセージをクリアします。

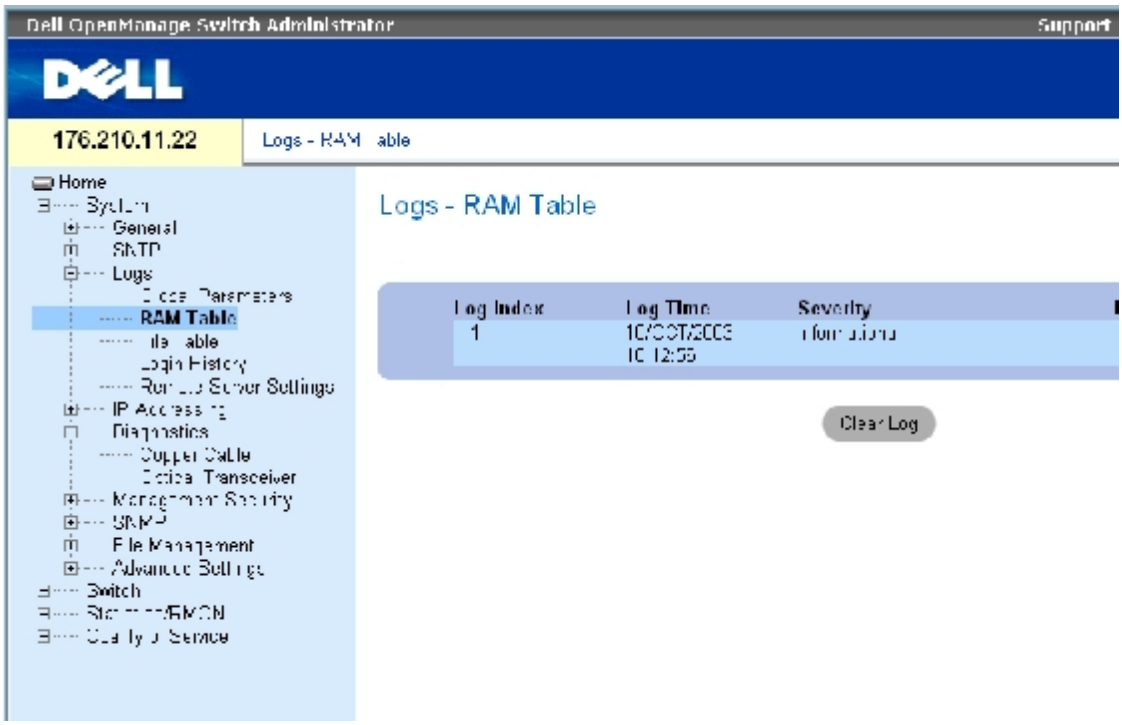
以下に CLI コマンドの例を示します。

```
console(config)# logging
on

console(config)# logging
console errors

console(config)# logging
buffered debugging

console(config)# logging
file alerts

console(config)# end

console# clear logging
file

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

RAM ログ表の表示

RAM ログ表 は、ログが記録された時刻、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関する情報で構成されています。RAM ログ表ページを開くには、ツリービューから System（システム）→ Logs（ログ）→ RAM Table（RAM 表）をクリックします。

図**6-18 RAM** ログ表



RAM ログ表ページは以下のフィールドで構成されています。

Log Index（ログインデックス） — **RAM Log Table**（RAM ログ表）内のログ番号を示します。

Log Time（ログ時刻） — **RAM Log Table**（RAM ログ表）にログが記録された時刻を示します。

Severity（重要度）— ログの重要度を示します。

Description（説明）— ログエントリの説明です。

ログ情報の削除

□□□ **RAM** ログ表を開きます。

□□□ **Clear Log**（ログのクリア）をクリックします。

ログ情報が **RAM Log Table**（RAM ログ表）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 ログ表の表示とクリア

RAM ログ表ページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-15 RAM** ログ表 **CLI** コマンド

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 syslog 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。

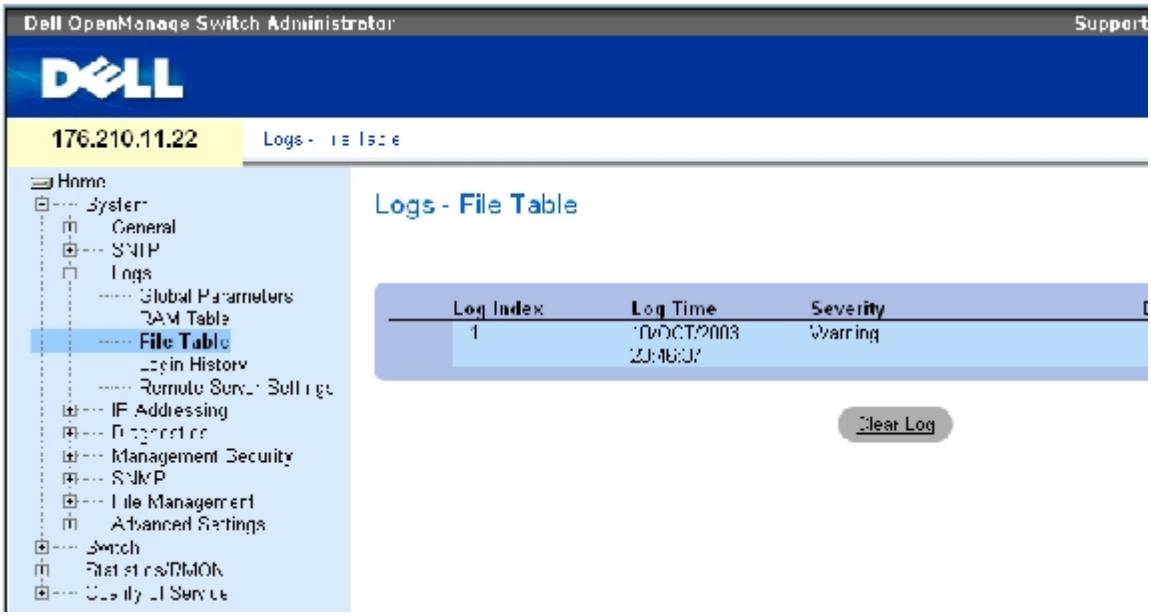
```
console# show logging

Logging is enabled.

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

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

File Logging: Level
error. File Messages: 157
Logged, 26 Dropped.

1 messages were not
logged

01-Jan-2000 01:03:42
:%INIT-I-Startup: Cold
Startup

01-Jan-2000 01:01:36
:%LINK-W-Down: 1/e14
```

```
01-Jan-2000 01:01:36
:%LINK-W-Down: 1/e13


01-Jan-2000 01:01:36
:%LINK-W-Down: 1/e12


01-Jan-2000 01:01:36
:%LINK-W-Down: 1/e15


01-Jan-2000 01:01:32
:%INIT-I-InitCompleted:
Initialization task is
completed



console# clear logging


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

ログファイル表の表示

ログファイル表には、ログが記録された時刻、ログの重要度、およびログメッセージの説明など、FLASH メモリ内のログファイルに保存されているログエントリについての情報が表示されます。ログファイル表ページを開くには、ツリービューから System（システム）→ Logs（ログ）→ File Table（ファイル表）をクリックします。

図**6-19** ログファイル表



ログファイル表ページは以下のフィールドで構成されています。

Log Index （ログインデックス） — Log File Table （ログファイル表）内のログ番号を示します。

Log Time （ログ時刻） — Log File Table （ログファイル表）にログが記録された時刻を示します。

Severity （重要度）— ログの重要度を示します。

Description （説明）— 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表の表示

ログファイル表ページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表6-16 ログファイル表 CLI コマンド

CLI コマンド	説明
show logging file	ロギングの状態とロギングファイルに保存されている syslog メッセージを表示します。
clear logging **file**	ロギングファイルからメッセージをクリアします。

以下に CLI コマンドの例を示します。

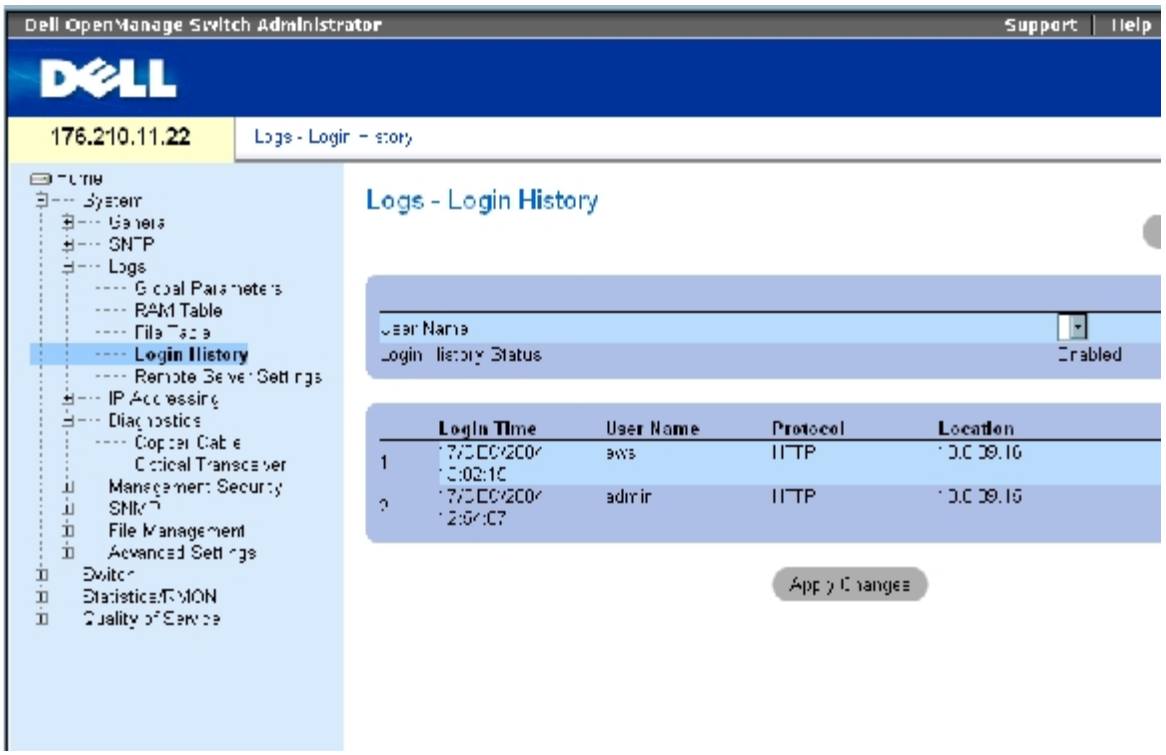
```
console# show
logging file


Logging is enabled.


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


Buffer Logging:
Level info. Buffer
Messages: 62 Logged,
62 Displayed, 200
Max.


File Logging: Level
debug. File
Messages: 11 Logged,
51 Dropped.


SysLog server
12.1.1.2 Logging:
warning. Messages:
14 Dropped.


SysLog server
1.1.1.1 Logging:
info. Messages: 0
Dropped.


01-Jan-2000 01:12:01
:%COPY-W-TRAP: The
copy operation was
completed
successfully


01-Jan-2000 01:11:49
:%LINK-I-Up: 1/e11


01-Jan-2000 01:11:46
:%LINK-I-Up: 1/e12


01-Jan-2000 01:11:42
:%LINK-W-Down:
1/e13


01-Jan-2000 01:11:35
:%LINK-I-Up: 1/e14
```

デバイスへのログイン履歴の表示

ログイン履歴 ページには、ユーザーのログイン時刻やデバイスへのログオンに使用したプロトコルを含む、デバイス利用状況の表示と監視に関する情報が表示されます。

ログイン履歴 ページを開くには、ツリービューから **System** （システム）→ **Logs** （ログ）→ **Login History** （ログイン履歴）をクリックします。

図**6-20** ログイン履歴



ログイン履歴 ページは以下のフィールドで構成されます。

User Name （ユーザー名）— ユーザー定義のデバイスユーザー名リストです。

Login History Status （ログイン履歴ステータス）— パスワード履歴ログがデバイス上で有効になっているかを示します。

Login Time （ログイン時刻）— 指定ユーザーがデバイスにログオンした時刻を示します。

User Name （ユーザー名）— デバイスにログオンしたユーザーを示します。

Protocol （プロトコル）— ユーザーがデバイスにログオンした手段を示します。

Location （場所）— デバイスをアクセスしたステーションの **IP** アドレスを示します。

ログイン履歴の表示

□□□ ログイン履歴 ページを開きます。

□□□ **User Name** （ユーザー名）フィールドでユーザーを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

指定ユーザーのログイン情報が表示されます。

CLI コマンドを使用したデバイスログ履歴の表示

ログイン履歴 ページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-17** デバイスログイン履歴 **CLI** コマンド

CLI コマンド	説明
show users login-history	パスワード管理履歴情報を表示します。

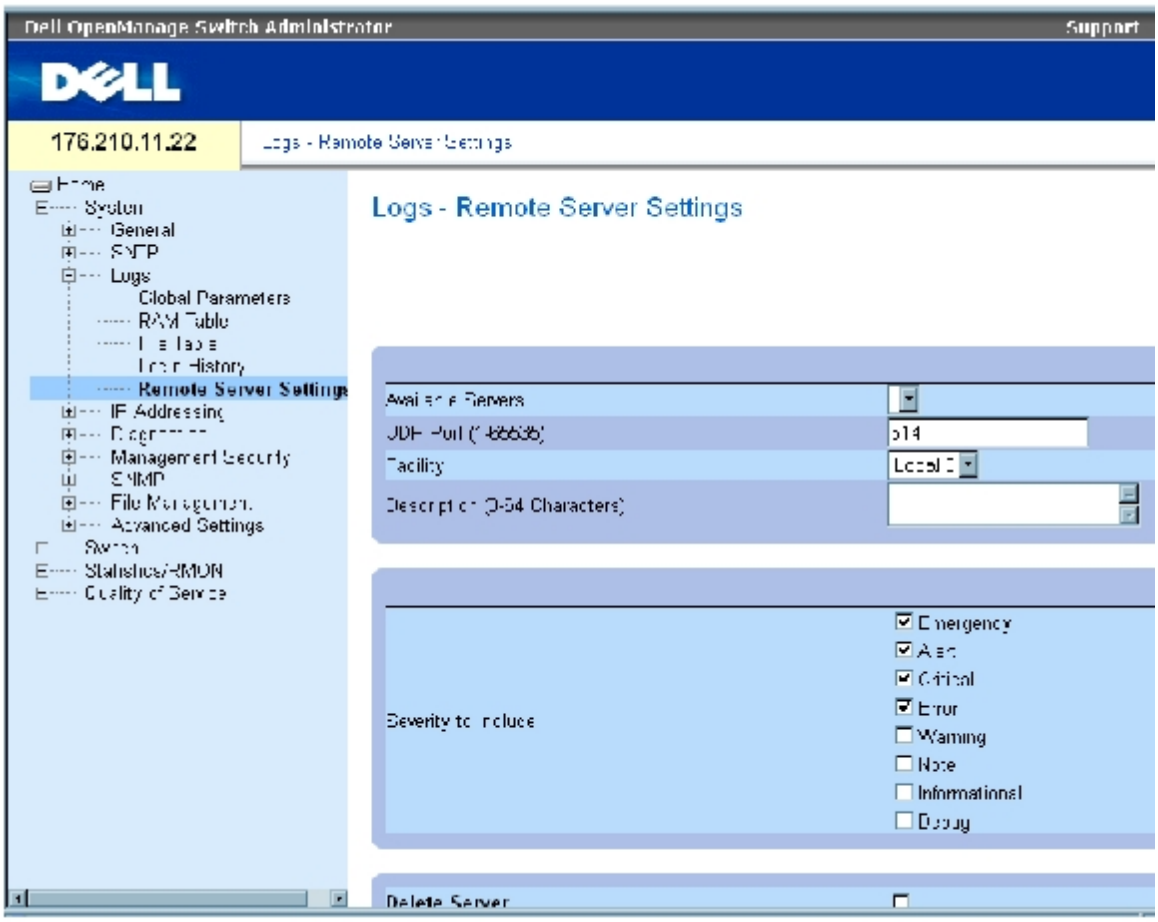
以下に CLI コマンドの例を示します。

```
console# show users login-history

Login Time          Username    Protocol    Location
-----------         --------    --------    ----------
Jan 1. 2005 23:58:17    Anna        HTTP        172.16.1.8
Jan 1. 2005 07:59:23    Errol       HTTP        172.16.0.8
Jan 1. 2005 08:23:48    Amy         Serial
Jan 1. 2005 08:29:29    Alan        SSH         172.16.0.8
Jan 1. 2005 08:42:31    Bob         HTTP        172.16.0.1
Jan 1. 2005 08:49:52    Cindy       Telnet      172.16.1.7
```

リモートログサーバー定義の変更

リモートログサーバー設定 ページには、利用可能なログサーバーの表示と設定を行うフィールドが表示されます。また、新しいログサーバーの定義と、各サーバーへログ重要度の送信を行います。リモートログサーバー設定 ページを開くには、ツリービューから **System**（システム）→ **Logs**（ログ）→ **Remote Server Settings**（リモートサーバー設定）をクリックします。

図**6-21** リモートログサーバー設定



リモートログサーバー設定 ページは以下のフィールドで構成されています。

Available Servers（利用可能サーバー）— ログが送信されるサーバーのリストが表示されます。

UDP Port（**1**～**65535**）（**UDP** ポート）— 選択されたサーバーにログを送信する **UDP** ポートを示します。可能な範囲は **1**～**65535** で、デフォルト値は **514** です。

Facility （ファシリティ）— システムログをリモートサーバーに送信するユーザー定義アプリケーションを定義します。**1** つのサーバーには単一のファシリティのみを割り当てることが可能です。第 **2** のファシリティレベルが割り当てられると、第**1**のファシリティレベルは無効になります。デバイスに定義されるすべてのアプリケーションは、サーバー上で同じファシリティを使用します。フィールドのデフォルト値は **Local 7** です。可能なフィールド値は次のとおりです。

Local 0～**Local 7**。

Description （**0**～**64** 文字）（説明）— ユーザー定義のサーバーの説明です。

Delete Server （サーバーの削除）— **Available Servers**（利用可能サーバー） リストから、現在選択されているサーバーを削除します。

リモートログサーバー設定ページには重要度リストも表示されます。重要度の定義は、グローバルログパラメータページ記載の重要度定義と同じです。

サーバーへのログ送信

□□□ リモートログサーバー設定 ページを開きます。

□□□ **Available Servers** （利用可能サーバー）のドロップダウンリストからサーバーを 1 つ 選択します。

□□□ 各フィールドを定義します。

□□□ **Severity to Include** （対象とする重要度）チェックボックスでログ重要度を選択しま す。

□□□ **Apply Changes** （変更の適用）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。

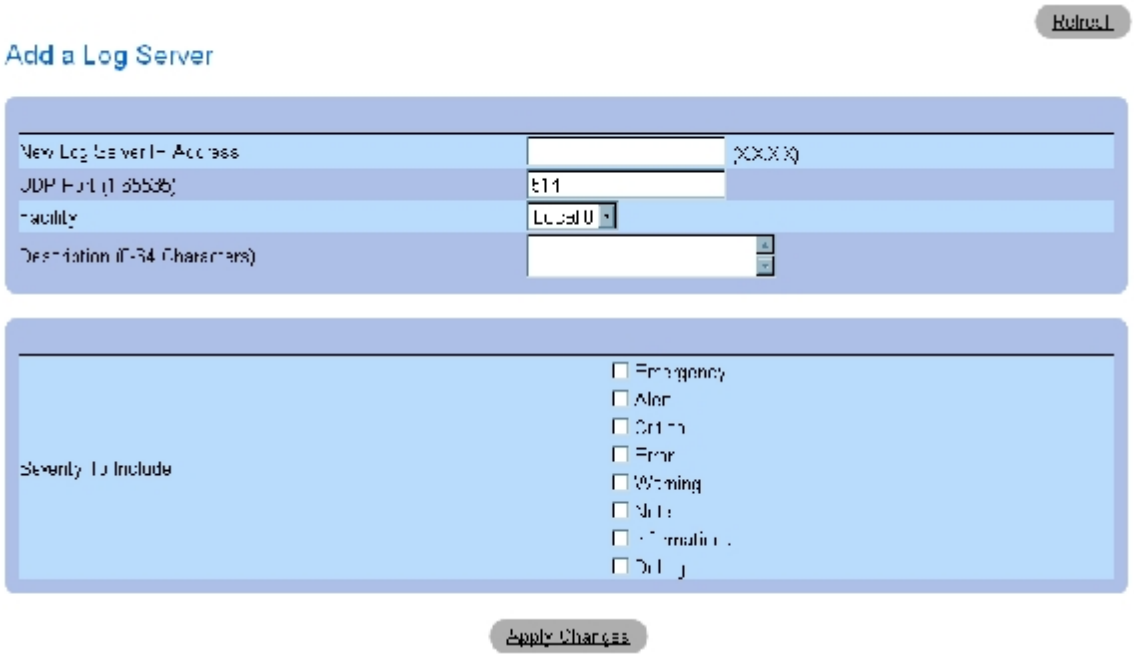
新規サーバーの定義

□□□ リモートログサーバー設定 ページを開きます。

□□□ **Add**（追加）をクリックします。

ログサーバーの追加ページが開きます。

図**6-22** ログサーバーの追加



ログサーバーの追加 ページは以下のフィールドで構成されます。

New Log Server IP Address（新ログサーバーの IP アドレス）— 新規ログサーバーの IP アドレスを定義します。

□□□ 各フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

サーバーが定義され、**Available Servers** （利用可能サーバー）リストに追加されます。

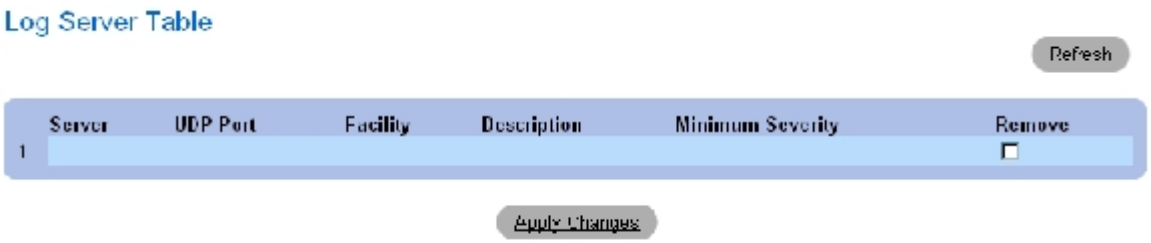
リモート ログサーバー表の表示

□□□ リモートログサーバー設定 ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

ログサーバー表ページが開きます。

図**6-23** ログサーバー表



ログサーバー表ページからログサーバーの削除

□□□ リモートログサーバー設定 ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

ログサーバー表ページが開きます。

□□□ ログサーバー表エントリを選択します。

□□□ **Remove** （削除）チェックボックスにチェックマークを付けます。

□□□ **Apply Changes** （変更の適用）をクリックします。

ログサーバー表の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リモートサーバーログの操作

リモートログサーバーの操作と等価な処理を実行する **CLI** コマンドを以下の表に示します。

表**6-18** リモートログサーバー **CLI** コマンド

CLI コマンド	説明
logging *{ip-address | hostname}* [port *port*] [severity *level*] [facility *facility*] [description *text*]	リモートサーバーにメッセージをロギングします。
no logging	syslog サーバーを削除します。
show logging	ロギングの状態と syslog メッセージを表示します。

以下に **CLI** コマンドの例を示します。

```
console> enable
```

```
console# configure

console(config) # logging
10.1.1.1 severity critical

console(config)# end

console# show logging

Logging is enabled.

Console Logging: Level
debug. Console Messages:
5 Dropped.

Buffer Logging: Level
debug. Buffer Messages:
16 Logged, 16 Displayed,
200 Max.

File Logging: Level
error. File Messages: 0
Logged, 209 Dropped.

SysLog server 31.1.1.2
Logging: error. Messages:
22 Dropped.

SysLog server 5.2.2.2
Logging: info. Messages:
0 Dropped.

SysLog server 10.2.2.2
Logging: critical.
Messages: 21 Dropped.

SysLog server 10.1.1.1
Logging: critical.
Messages: 0 Dropped.

1 messages were not
logged

03-Mar-2004 12:02:03
:%LINK-I-Up: 1/e11

03-Mar-2004 12:02:01
:%LINK-W-Down: 1/e12

03-Mar-2004 12:02:01
:%LINK-I-Up: 1/e13
```

IP アドレッシングの定義

IP アドレッシングページには、インタフェースの割り当て、デフォルトゲートウェイ IP アドレスの割り当て、インタフェースに対する ARP と DHCP パラメータの定義に関する各リンクが表示されます。IP アドレッシングページを開くには、ツリービューから System （システム）→ IP Addressing （IP アドレッシング）をクリックします。

デフォルトゲートウェイの定義

デフォルトゲートウェイページは、デバイスにゲートウェイを割り当てるフィールドで構成されています。パケットがリモートネットワークに送信されると、パケットはデフォルト 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 つと同じ IP アドレスサブネットに属している必要があります。 デフォルトゲートウェイページを開くには、ツリービューから、System （システム）→ IP Addressing （IP アドレッシング）→ Default Gateway （デフォルトゲートウェイ）をクリックします。

デフォルトゲートウェイページは以下のフィールドで構成されています。

User Defined \（ユーザー定義）— デバイスのゲートウェイ IP アドレスです。

Active （アクティブ）— ゲートウェイが有効であることを示します。

Remove User Defined （ユーザー定義の削除）— 選択によって、**Default Gateway** （デフォルトゲートウェイ）ドロップダウンリストから、デバイスのゲートウェイを削除します。

デバイスのゲートウェイの選択

□□□ デフォルトゲートウェイページを開きます。

□□□ **Default Gateway** （デフォルトゲートウェイ）ドロップダウンリストにある IP アドレ スを 1 つ選びます。

□□□ Active （アクティブ）チェックボックスを選択します。

□□□ **Apply Changes** （変更の適用）をクリックします。

デバイスのデフォルトゲートウェイが選択され、デバイスがアップデートされます。

デバイスのデフォルトゲートウェイデバイスの削除

□□□ デフォルトゲートウェイページを開きます。

□□□ デフォルトゲートウェイを削除するために**Remove** （削除）チェックボックスを選択 します。

□□□ **Apply Changes** （変更の適用）をクリックします。

デフォルトゲートウェイ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のゲートウェイの定義

デフォルトゲートウェイページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-19** デフォルトゲートウェイ **CLI** コマンド

CLI コマンド	説明
ip default-gateway ip-address	デフォルトゲートウェイを定義します。
no ip default-gateway	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。

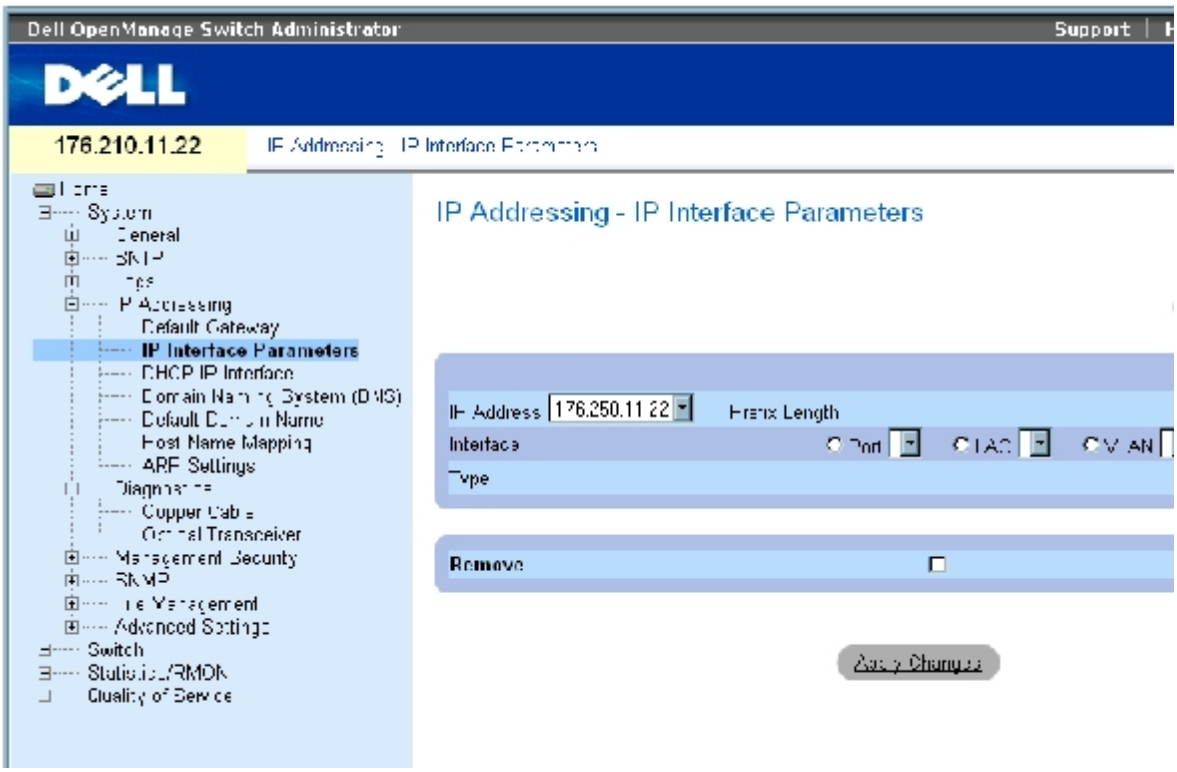
```
console(config)# ip
default-gateway
```

```
196.210.10.1


console(config)# no ip
default-gateway
```

IP インタフェースの定義

IP インタフェースパラメータ ページには、IP パラメータをインタフェースに割り当てるフィールドが表示されます。IP インタフェースパラメータ ページを開くには、ツリービューから **System** （システム）→ **IP Addressing** （IP アドレッシング）→ **IP Interface Parameters** （IP インタフェースパラメータ）をクリックします。

図**6-24 IP** インタフェースパラメータ



IP インタフェースパラメータページは以下のフィールドで構成されています。

IP Address （IP アドレス）— インタフェースの IP アドレスです。

Prefix Length （プレフィックス長）— ソース IP アドレスプレフィックスのビット数、またはソース IP アドレスのネットワークマスクを構成するビット数です。

Source Interface（ソースインタフェース）— IP アドレスを定義するインタフェースのタイプです。**Port** （ポート）、**LAG** （LAG）、または**VLAN** （VLAN）を選択します。

Type （タイプ）— IP アドレスが静的に設定されたか表示します。

Remove （削除）— 選択によって、**IP Address** （IP アドレス）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。

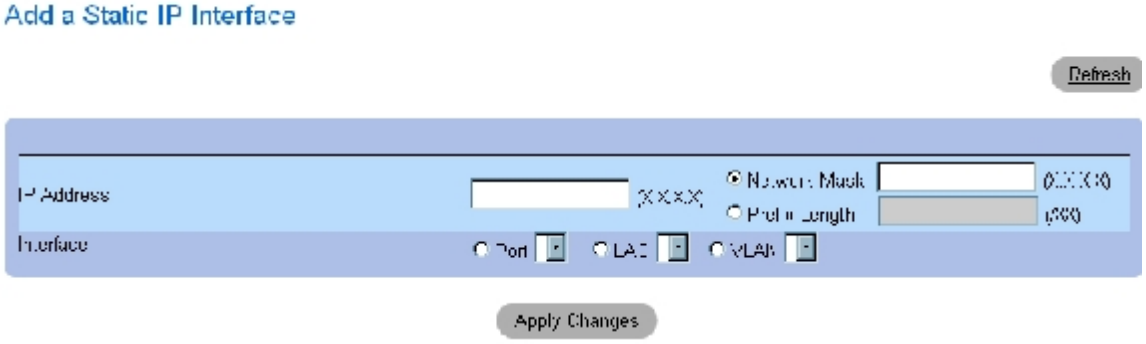
IP インタフェースの追加

□□□ IP インタフェースパラメータ ページを開きます。

□□□ **Add** （追加）をクリックします。

スタティック **IP** インタフェースの追加ページが開きます。

図**6-25** スタティック **IP** インタフェースの追加



Network Mask （ネットワークマスク）— ソース IP アドレスのサブネットワークマスクを示します。

□□□ ページ内の各フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

インタフェースに新しいスタティック IP アドレスが追加され、デバイスがアップデートされます。

IP アドレスパラメータの変更

□□□ IP インタフェースパラメータ ページを開きます。

□□□ **IP Address**（IP アドレス）ドロップダウンリストから IP アドレスを選びます。

□□□ インタフェースタイプを変更します。

□□□ **Apply Changes** （変更の適用）をクリックします。

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。

IP アドレスの削除

□□□ IP インタフェースパラメータ ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

IP インタフェース表ページが開きます。

図**6-26 IP** インタフェースパラメータ表

□□□ IP アドレスを 1 つ選択し、**Remove** （削除）チェックボックスを選択します。

□□□ **Apply Changes** （変更の適用）をクリックします。

選択した 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

IP インタフェースパラメータページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-20 IP** インタフェースパラメータ**CLI**コマンド

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 に対して設定されているインタフェースの使用状況を表示します。

以下に、CLI コマンドの例を示します。

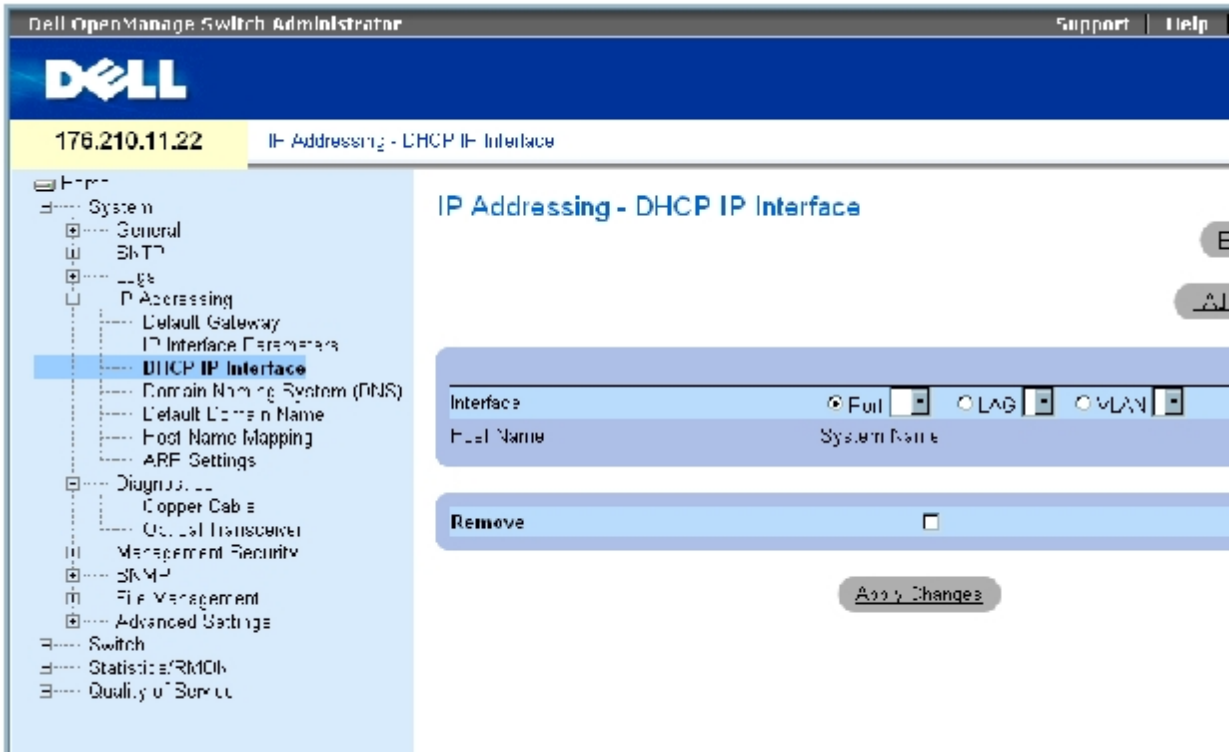
```
console(config)# interface
vlan 1

console(config-if)# ip
address 92.168.1.123
255.255.255.0

console(config-if)# no ip
address 92.168.1.123

console(config-if)# end

console# show ip interface
vlan 1

Gateway IP Address
Activity status

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

192.168.1.1 Active

IP address Interface Type
```

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

192.168.1.123/24 VLAN 1
Static
```

DHCP IP インタフェースパラメータの定義

DHCP IP インタフェース ページ には、デバイスに接続された DHCP クライアントの定義に関するパラメータが表示されます。 DHCP IP インタフェースページを開くには、ツリービューから、System （システム）→ IP Addressing （IP アドレッシング）→ DHCP IP Interface （DHCP IP インタフェース）をクリックします。

図**6-27 DHCP IP** インタフェース



DHCP IP インタフェース ページは以下のフィールドで構成されています。

Interface （インタフェース）— デバイスに接続されている特定のインタフェースです。**Port** （ポート）、**LAG** （LAG）、または**VLAN** （VLAN）の横にあるオプションボタンをクリックし、デバイスに接続されているインタフェースを選択します。

Host Name （ホスト名）— ホスト名です。

Remove （削除）— 選択によって DHCP クライアントを削除します。

DHCP クライアントの追加

□□□ DHCP IP インタフェースページを開きます。

□□□ **Add** （追加）をクリックします。

DHCP IP インタフェースの追加ページが開きます。

□□□ ページ内の各フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

DHCP 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。

DHCP IP インタフェースの変更

□□□ DHCP IP インタフェースページを開きます。

□□□ 各関連フィールドを変更します。

□□□ **Apply Changes**（変更の適用）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 インタフェースの削除

□□□ DHCP IP インタフェース ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

DHCP Client Table（DHCP クライアント表）が開きます。

□□□ DHCP クライアントエントリを 1 つ選択します。

□□□ **Remove**（削除）チェックボックスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択した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 IP インタフェースの定義

DHCP クライアントの定義操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-21 DHCP IP** インタフェース **CLI** コマンド

CLI コマンド	説明
ip address dhcp [**hostname** *host-name*]	Ethernet インタフェースの IP アドレスを Dynamic Host Configuration Protocol（DHCP）から取得します。

以下に、CLI コマンドの例を示します。

```
console(config)# interface
ethernet 1/e11
```

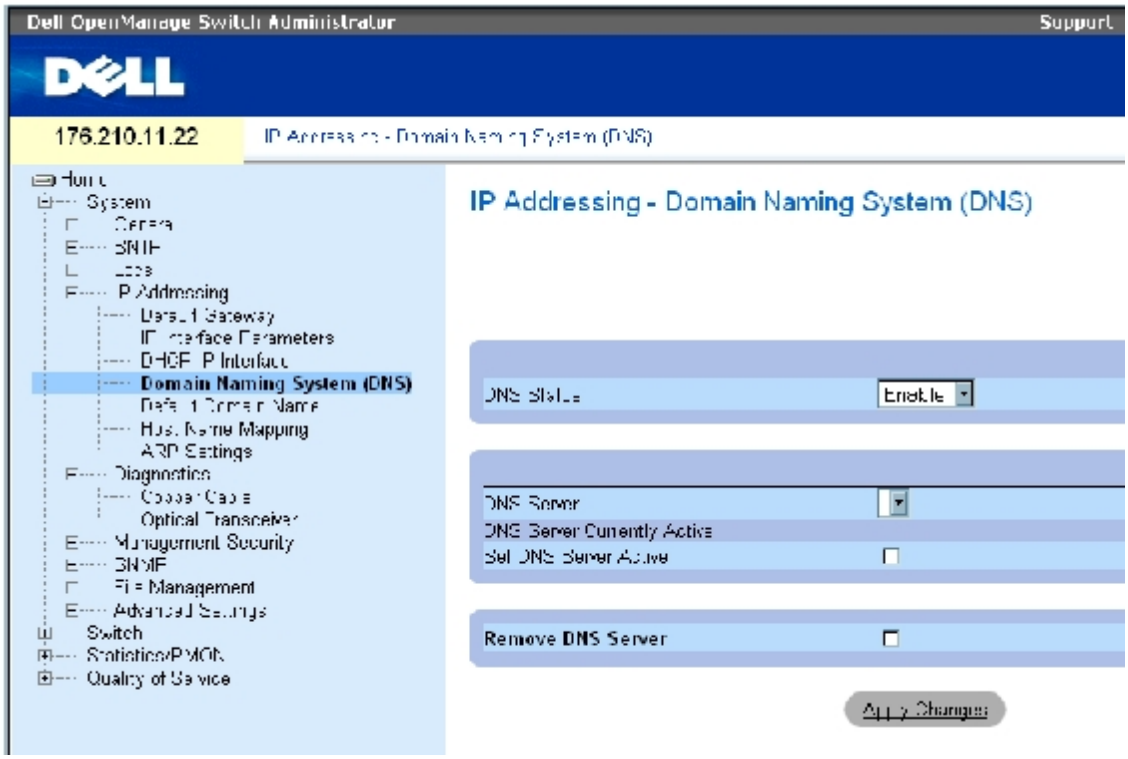
```
console(config-if)# ip
address dhcp
```

ドメインネームシステムの設定

ドメインネームシステム（DNS）は、ユーザー定義のドメイン名を IP アドレスに変換する仕組みです。ドメイン名が割り当てられるたびに、DNS サービスはそのドメイン名を数字の IP アドレスに変換します。たとえば、www.ipexample.com は 192.87.56.2 に変換されます。DNS サーバーはドメインネームデータベースおよび対応する IP アドレスの関係を維持します。

ドメインネームシステム **(DNS)**ページには、特定の DNS サーバーを有効およびアクティブにするフィールドが表示されます。ドメインネームシステム **(DNS)**ページを開くには、ツリービューから **System** （システム）→ **IP Addressing** （IP アドレッシング）→ **Domain Naming System**（**DNS**）（ドメインネームシステム）をクリックします。

図**6-28** ドメインネームシステム **(DNS)**



ドメインネームシステム (DNS)ページは以下のフィールドで構成されています。

DNS Status （DNS ステータス）— DNS ネームから IP アドレスへの変換を有効または無効にします。

DNS Server （DNS サーバー）— DNS サーバーのリストが表示されます。DNS サーバーの追加は **DNS** サーバーの追加ページで行います。

DNS Server Currently Active （現在アクティブな DNS サーバー）— 現時点でアクティブな DNS サーバーです。

Set DNS Server Active （DNS サーバーをアクティブに設定）— 選択した DNS サーバーをアクティブにします。

Remove DNS Server （DNS サーバーの削除）— 選択によって、指定した DNS サーバーを削除します。

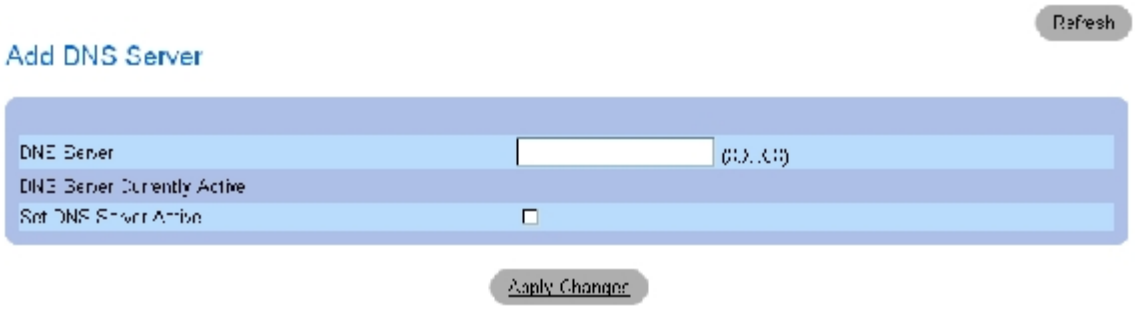
DNS サーバーの追加

□□□ ドメインネームシステム (DNS)ページを開きます。

□□□ **Add** （追加）をクリックします。

DNS サーバーの追加ページが開きます。

図**6-29 DNS** サーバーの追加



DNS Server （DNS サーバー）— DNS サーバーの IP アドレスです。

□□□ 各関連フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

新しい DNS サーバーが定義され、デバイスがアップデートされます。

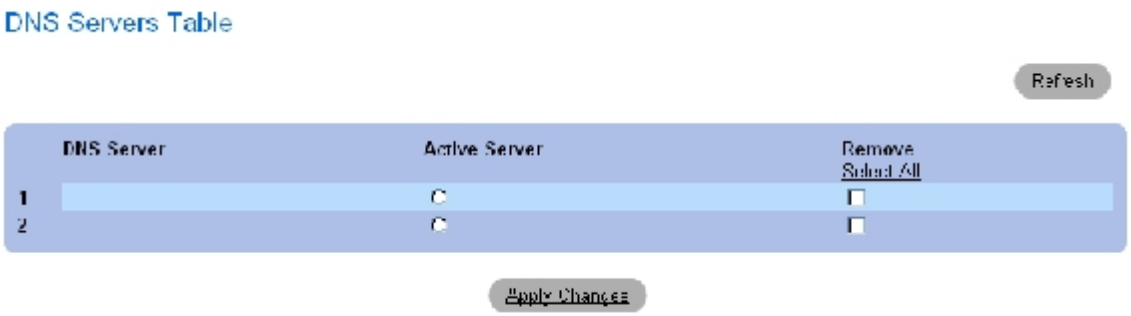
DNS サーバー表の表示

□□□ ドメインネームシステム (DNS)ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

DNS Server Table （DNS サーバー表）が開きます。

図**6-30 DNS**サーバー表



DNS サーバーの削除

□□□ ドメインネームシステム (DNS)ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

DNS Server Table（DNS サーバー表）が開きます。

□□□ **DNS Server Table** （DNS サーバー表）のエントリを 1 つ選びます。

□□□ **Remove** （削除）チェックボックスを選択します。

□□□ **Apply Changes** （変更の適用）をクリックします。

選択した DNS サーバーが削除され、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デバイス情報の設定

DNS サーバーを設定する CLI コマンドを以下の表に示します。

表**6-22 DNS** サーバー **CLI** コマンド

CLI コマンド	説明
ip name-server *server-address*	利用可能なネームサーバーを設定します。最大で 8 台のネームサーバーを定義することが可能です。
no ip name-server *server-address*	ネームサーバーを削除します。
ip domain-name *name*	資格のないホスト名を完全にするためにソフトウェアが使用するデフォルトドメイン名を定義します。
clear host {name | *}	ホスト名からアドレスへ変換するキャッシュエントリを削除します。
show hosts [*name*]	デフォルトドメイン名、ネームサーバーホストのリスト、ホスト名とアドレスのキャッシュされたスタティックなリストを表示します。
ip domain-lookup	ホスト名から IP アドレスへの変換を行う DNS システムを有効にします。

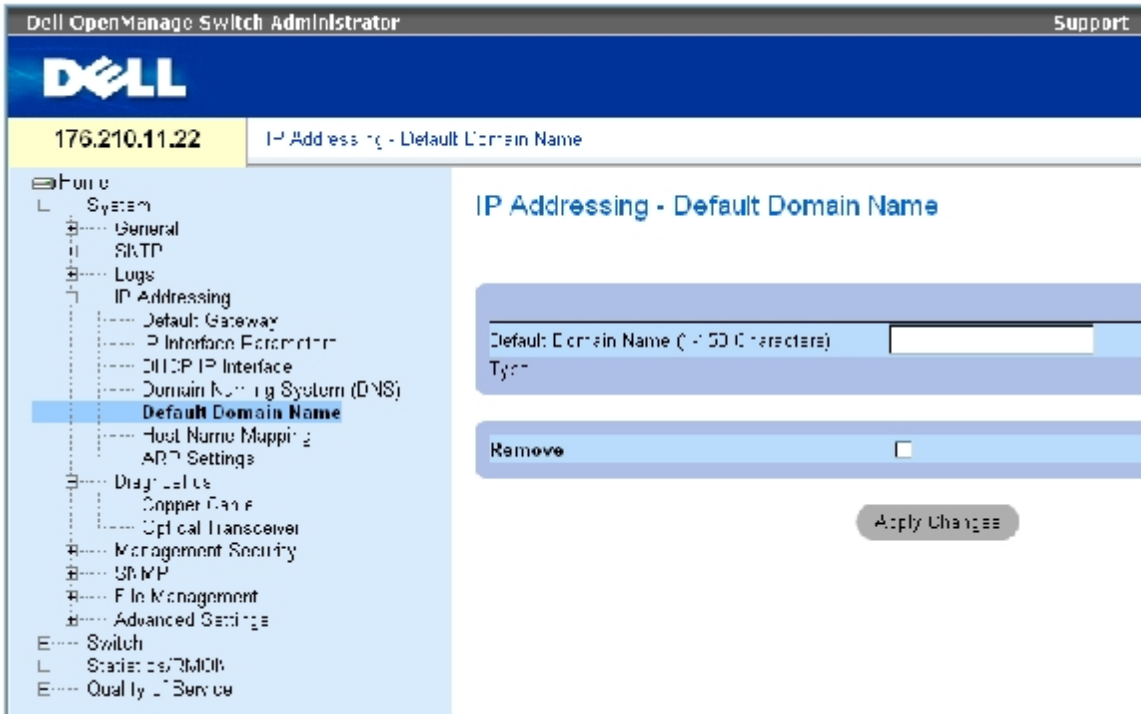
以下に、CLI コマンドの例を示します。

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

デフォルトドメインの定義

デフォルトドメイン名 ページには、デフォルト DNS ドメイン名の定義情報が表示されます。デフォルトドメイン名 ページを開くには、**System** （システム）→ **IP Addressing** （IP アドレッシング）→ **Default Domain Name** （デフォルトドメイン名）をクリックします。

図**6-31** デフォルトドメイン名



デフォルトドメイン名 ページは以下のフィールドで構成されています。

Default Domain Name（**1**～**158** 文字）（デフォルトドメイン名）— ユーザー定義のデフォルトドメイン名が表示されます。定義されている場合、すべての資格なしホスト名に対してデフォルトドメイン名が適用されます。

Type （タイプ）— IP アドレスタイプです。可能なフィールド値は、以下のとおりです。

Dynamic （ダイナミック）— IP アドレスは動的に生成されます。

Static （スタティック）— IP アドレスはスタティック IP アドレスです。

Remove （削除）— チェックによってデフォルトドメイン名を削除します。

CLI コマンドを使用した DNS ドメイン名の定義

DNS ドメイン名を設定する CLI コマンドを以下の表に示します。

表**6-23 DNS** ドメイン名 **CLI** コマンド

CLI コマンド	説明
ip domain-name name	資格のないホスト名を完全にするためにソフトウェアが使用するデフォルトドメインネームを定義します。
no ip domain-name	ドメインネームシステム（DNS）の使用を無効にします。
show hosts [*name*]	デフォルトドメイン名、ネームサーバーホストのリスト、ホスト名とアドレスのキャッシュされたスタティックなリストを表示します。

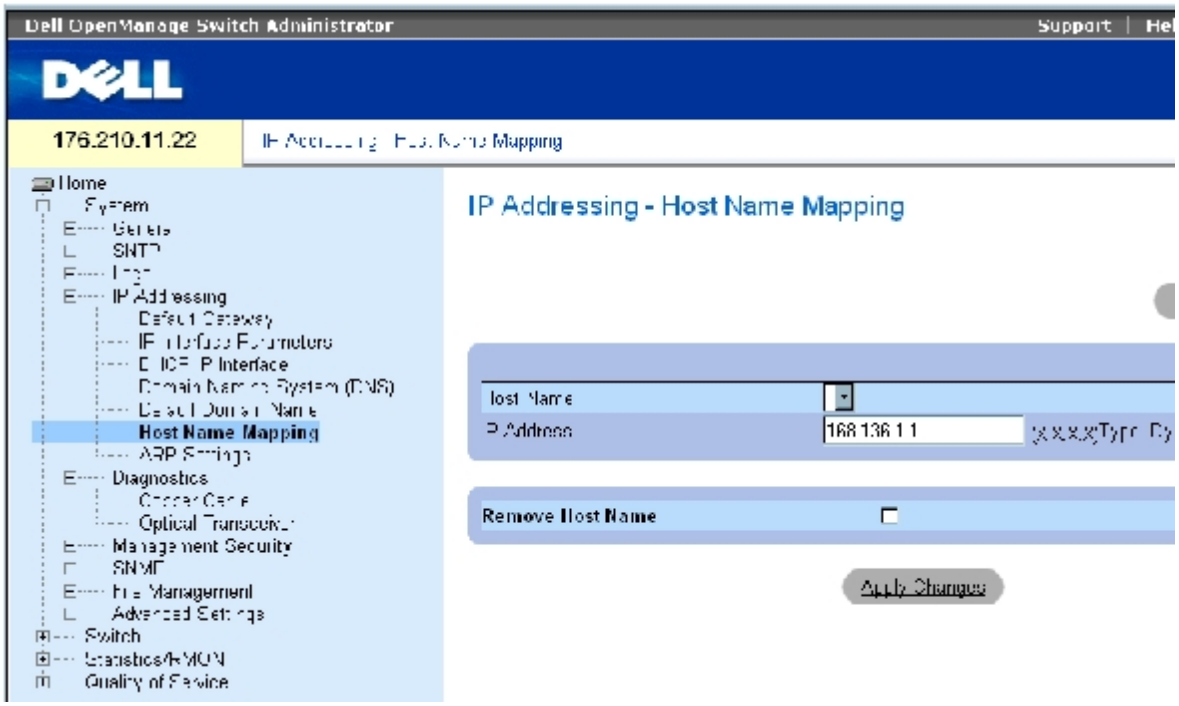
以下に、CLI コマンドの例を示します。

```
console(config)# ip
domain-name dell.com
```

ドメインホストのマッピング

ホスト名のマッピングページには、IP アドレスをスタティックホスト名に割り当てるパラメータが表示されます。このページで、ホストあたり 1 つの IP アドレスを割り当てます。ホスト名マッピングページを開くには、ツリービューから、**System** （システム）→**IP Addressing** （IP アドレッシング）→ **Host Name Mapping** （ホスト名マッピング）をクリックします。

図**6-32** ホスト名のマッピング



ホスト名のマッピングページは以下のフィールドで構成されています。

Host Name （ホスト名）— ホスト名のリストが表示されます。ホスト名はホスト名マッピングの追加ページで定義します。各ホストは単一の IP アドレスを提供します。

IP Address（**X.X.X.X**）（IP アドレス）— 特定のホスト名に割り当てられる IP アドレスを示します。

Type （タイプ）— IP アドレスタイプです。可能なフィールド値は以下のとおりです。

Dynamic （ダイナミック）— IP アドレスは動的に生成されます。

Static （スタティック）— IP アドレスはスタティック IP アドレスです。

Remove Host Name （ホスト名の削除）— チェックを入れることで DNS ホストマッピングを削除します。

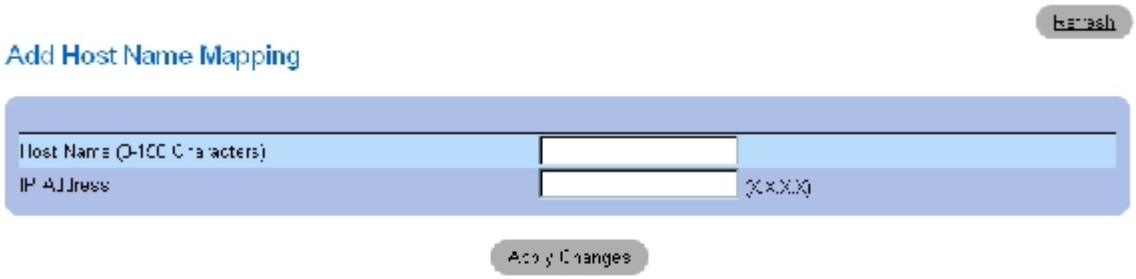
ホストドメイン名の追加

□□□ ホスト名のマッピングページを開きます。

□□□ **Add** （追加）をクリックします。

ホスト名マッピングの追加ページが開きます。

図**6-33** ホスト名マッピングの追加



□□□ 各関連フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

IP アドレスがホスト名にマッピングされ、デバイスは更新されます。

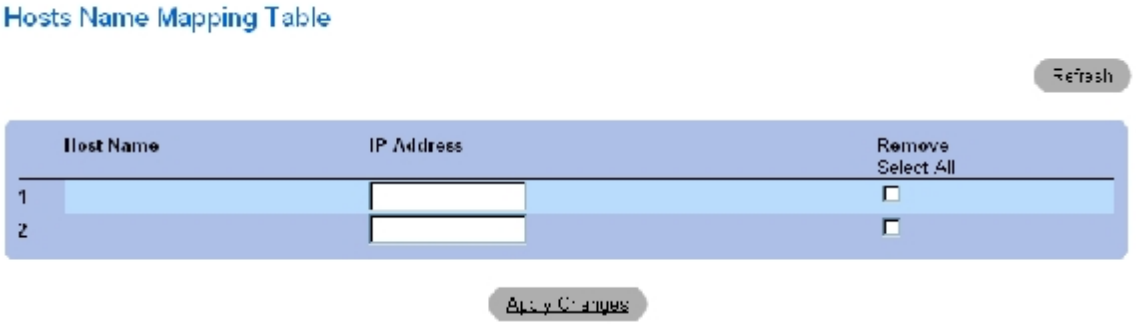
ホスト名マッピング表の表示

□□□ ホスト名のマッピングページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ホスト名マッピング表ページが開きます。

図**6-34** ホスト名マッピング表



IP アドレスマッピングからホスト名の削除

□□□ ホスト名のマッピングページを開きます。.

□□□ **Show All** （すべてを表示）をクリックします。

□□□ ホスト名マッピング表ページが開きます。

□□□ **Host Name Mapping Table** （ホスト名マッピング表）からエントリを 1 つ選択します。

□□□ **Remove** （削除）チェックボックスをチェックします。

□□□ **Apply Changes** （変更の適用）をクリックします。

Host Name Mapping Table （ホスト名マッピング表）から指定した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 IP アドレスのドメインホスト名へのマッピング

ドメインホスト名を IP アドレスにマッピングする設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-24** ドメインホスト名 **CLI** コマンド

CLI コマンド	説明
ip host *name address*	スタティックなホスト名とアドレスとのマッピングをホストキャッシュに定義します。
no ip host name	ホスト名とアドレスとのマッピングを削除します。
clear host {name | *}	ホスト名からアドレスへ変換するキャッシュエントリを削除します。
show hosts [name]	デフォルトドメイン名、ネームサーバーホストのリスト、ホスト名とアドレスのキャッシュされたスタティックなリストを表示します。

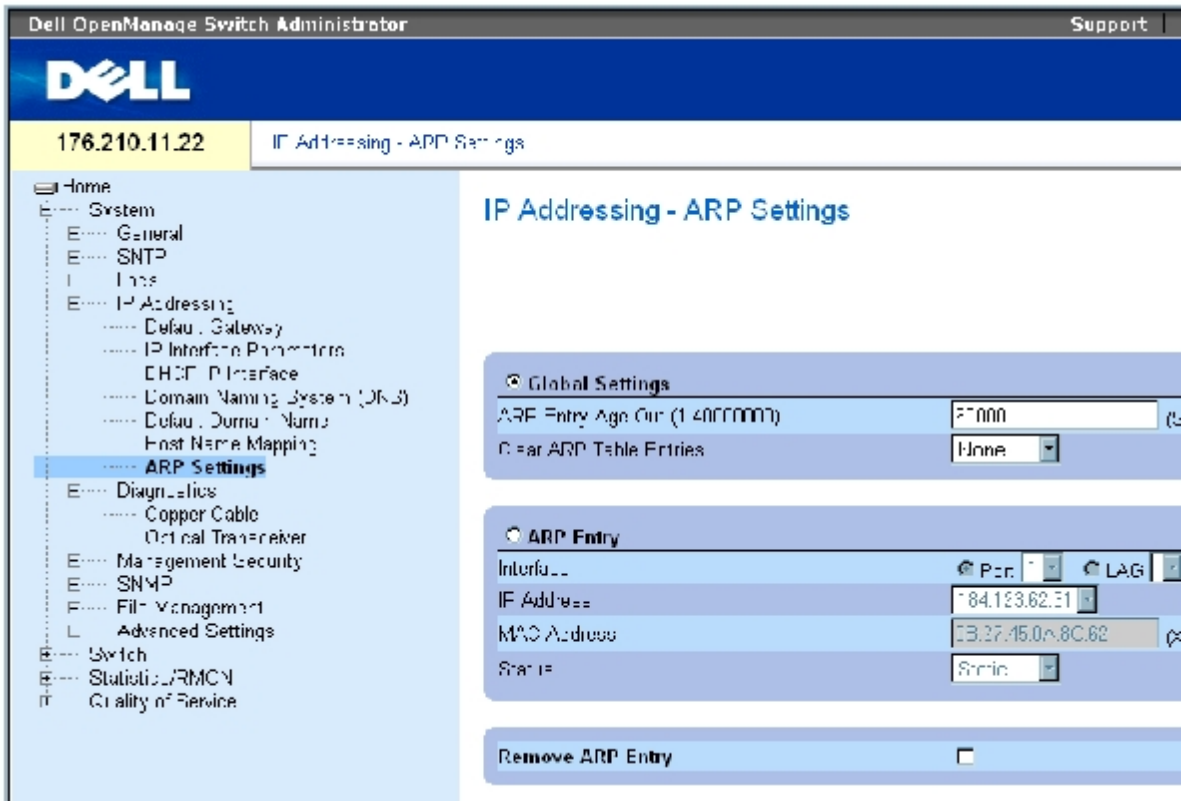
以下に CLI コマンドの例を示します。

```
console(config)# ip host
accounting.abc.com
176.10.23.1
```

ARP 設定の定義

Address Resolution Protocol（ARP）（アドレス解決プロトコル）は、IP アドレスを物理アドレスに変換し、IP アドレスを MAC アドレスにマッピングします。ARP は、近くのホストの IP アドレスが既知のときに限り、ホストと他のホストとの通信を許可します。**ARP** 設定ページを開くには、ツリービューから System （システム）→ IP Addressing （IP アドレッシング）→ ARP （ARP）をクリックします。

図**6-35 ARP** 設定



ARP 設定 ページは以下のフィールドで構成されます。

Global Settings（グローバル設定）— このオプションは、ARP グローバル設定に関するフィールドを有効にします。

ARP Entry Age Out（**1**～**40000000**）（ARP エントリの寿命）— すべてのデバイスに対して、ある ARP 表エントリに対する ARP 要求間の経過時間量（秒）です。この時間が経過すると、エントリは表から削除されます。値の範囲は 1～40000000 です。デフォルト値は 60000 秒です。

Clear ARP Table Entries （ARP 表エントリのクリア）— すべてのデバイス上でクリアする ARP エントリのタイプを示します。可能な値は以下のとおりです。

None （なし）— ARP エントリはクリアされません。

All （すべて）— すべての ARP エントリがクリアされます。

Dynamic（ダイナミック）— ダイナミック ARP エントリのみがクリアされます。

Static （スタティック）— スタティック ARP エントリのみがクリアされます。

ARP Entry （ARP エントリ）— このオプションを選択すると、単一 Ethernet デバイス上で、ARP 設定に必要なフィールドを有効にします。

Interface （インタフェース）— デバイスに設定されているポート、LAG、または VLAN のインタフェース番号を指定します。

IP Address （IP アドレス）— ステーション IP アドレスです。次に入力する MAC アドレスに対応します。

MAC Address （MAC アドレス）— ステーション MAC アドレスです。ARP 表で IP アドレスと関連付けされます。

Status （ステータス）— ARP 表エントリのステータスです。可能なフィールド値は以下のとおりです。

Dynamic （ダイナミック）— ARP エントリは動的に学習されます。

Static — ARP エントリはスタティックエントリです。

Remove ARP Entry （ARP エントリの削除）— 選択によって ARP エントリを削除します。

スタティック **ARP** 表エントリの追加

□□□ **ARP** 設定ページを開きます。

□□□ **Add** （追加）をクリックします。

ARP エントリの追加ページが開きます。

□□□ インタフェースタイプを選びます。

□□□ フィールドを定義します。

□□□ Apply Changes （変更の適用）をクリックします。

ARP Table （ARP 表）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 表の表示

□□□ **ARP** 設定ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

ARP 表ページが開きます。

ARP 表エントリの削除

□□□ **ARP** 設定 ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

ARP 表ページが開きます。

□□□ 表エントリを選びます。

□□□ **Remove** （削除）チェックボックスを選択します。

□□□ Apply Changes （変更の適用）をクリックします。

選択した**ARP Table** （ARP 表）エントリは削除され、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

ARP 設定ページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-25 ARP** 設定 **CLI** コマンド

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 ARP キャッシュで保持される時間を設定します。
clear arp-cache	ARP キャッシュからすべてのダイナミックエントリを削除します。
show arp	ARP 表にあるエントリを表示します。
no arp	ARP 表から ARP エントリの 1 つを削除します。

以下に CLI コマンドの例を示します。

```
console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

console(config)# arp timeout 12000

console(config)# exit

console# show arp

ARP timeout: 12000 Seconds
```

Interface	IP address	HW address	Status
---------	----------	----------	------
1/e11	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
1/e12	10.7.1.135	00:50:22:00:2A:A4	Static

ケーブル診断の実行

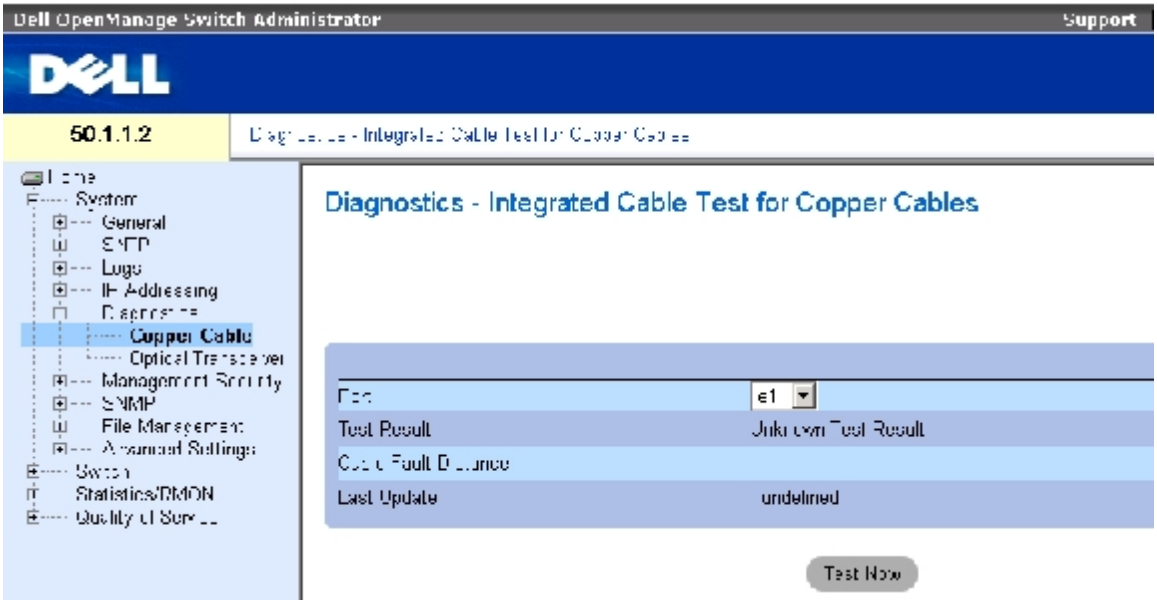
診断ページには、銅ケーブルの仮想ケーブルテストの実行ページへのリンクが掲載されています。診断ページを開くには、ツリービューから **System** （システム）→ **Diagnostics** （診断）をクリックします。

銅ケーブル診断の表示

銅ケーブル用ケーブルテストページは、銅ケーブルのテストを実行するフィールドで構成されています。ケーブルテストを行うと、エラーが発生したケーブル位置、ケーブルテストを最後に実行した時刻、発生したケーブルエラーの種類に関する情報が表示されます。テストは時間領域反射率測定法（TDR）テクノロジを使用して、ポートに接続されている銅ケーブルの品質と特性を検査します。長さ 120 m までのケーブルのテストが可能です。ケーブルテストは、**Approximate Cable Length**（概略ケーブル長）テストを除いて、ポートが動作していない状態で行われます。

銅ケーブル用ケーブルテストページを開くには、ツリービューから **System** （システム）→ **Diagnostics** （診断）→ **Copper Cable** （銅ケーブル）をクリックします。

図**6-36** 銅ケーブル用ケーブルテスト



銅ケーブル用ケーブルテストページは以下のフィールドで構成されます。

Port （ポート）— 測定対象のケーブルが接続されているポートを指定します。

Test Result （テスト結果）— ケーブルのテスト結果が表示されます。可能なフィールド値は以下のとおりです。

No Cable （ケーブルなし）— ポートにケーブルが接続されていません。

Open Cable （ケーブル開放）— ケーブルの他端が接続されていません。

Short Cable （ケーブル短絡）— ケーブルで短絡が発生しています。

OK （OK）— ケーブルテストは正常に終了しました。

Cable Fault Distance （ケーブル障害距離）— ケーブルエラーが発生した位置をポートからの距離で示します。

Last Update （最終更新）— ポートを最後にテストした日時を示します。

Approximate Cable Length （概略ケーブル長）— ケーブルのおよその長さを表示します。このテストは、ポートが動作状態にあって、かつ、1 Gbps で動作している場合にのみ実行されます。

ケーブルテストの実行

□□□ 銅ケーブルの両端がデバイスに接続されていることを確認します。

□□□ 銅ケーブル用ケーブルテストページを開きます。

□□□ テストを行うインタフェースを選択します。

□□□ **Test Now**（テスト実行）をクリックします。

銅ケーブルテストが実行され、結果は銅ケーブル用ケーブルテストページに表示されます。

仮想ケーブルテスト結果表の表示

□□□ 銅ケーブル用ケーブルテストページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

ケーブルテスト結果表ページが開きます。

メモ： この画面には以前実行したテストの結果が表示されます。すべてのポートに対して今 テストを実行するわけではありません。

銅ケーブル用ケーブルテストページの各フィールドに加えて、**Integrated Cable Test Results Table** （ケーブルテスト結果表）には次のフィールドがあります。

Unit No. （ユニット番号） — 表示されているケーブルのユニット番号です。

CLI コマンドを使用した銅ケーブルテストの実行

銅ケーブルテストの実行を指示する CLI コマンドを以下の表に示します。

表**6-26** 銅ケーブルテスト **CLI** コマンド

CLI コマンド	説明
test copper-port tdr *interface*	仮想ケーブルテストを実行します。
show copper-port tdr *interface*	ポートに対して最後に行った仮想ケーブルテストの結果を表示します。
show copper-port cable-length *interface*	ポートに接続されている銅ケーブルの推定長さを表示します。

以下に CLI コマンドの例を示します。

```
console> enable

Console# test copper-port tdr 1/e3

Cable is open at 100 meters.

Console# show copper-port cable-length

Port    Length (meters)
----    ---------------
1/e3    110-140
1/e4    Fiber
```

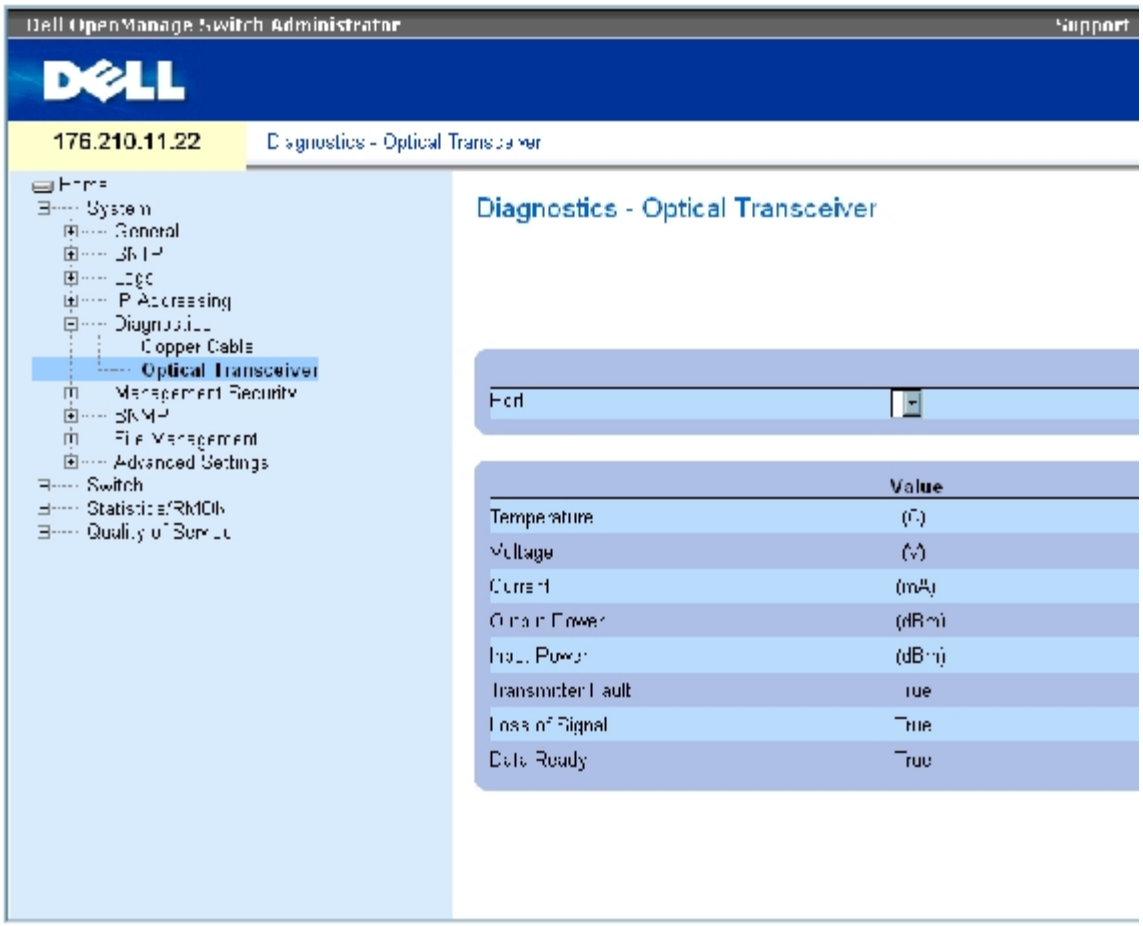
メモ： ケーブルテスター（ICT）が返すケーブル長は、50 m 未満、50 m～80 m、80 m～110 m、110 m～120 m、120 m 超のいずれかで、それぞれ概算値です。誤差は最大で 20 m で、ま た、ケーブル長測定は 10 Mbps リンクでは動作しません。

オプティカルトランシーバ診断の表示

オプティカルトランシーバはファイバケーブルのテストを実行するページです。オプティカルトランシーバページを開くには、ツリービューから **System** （システム）→ **Diagnostics** （診断）→ **Optical Transceiver** （オプティカルトランシーバ）をクリックします。

メモ： オプティカルトランシーバ診断は、リンクが存在するときのみ実行可能です。

図**6-37** オプティカルトランシーバ



オプティカルトランシーバ ページは以下のフィールドで構成されます。

Port（ポート）— 測定対象のケーブルのポート IP アドレスです。

Temperature （温度）— ケーブルが動作している温度（摂氏）です。

Voltage （電圧）— ケーブルが動作している電圧です。

Current （電流）— ケーブルが動作している電流です。

Output Power （出力パワー）— 出力パワーの送信レートです。

Input Power （入力パワー） — 入力パワーの送信レートです。

Transmitter Fault （トランスミッタ故障） — 送信中に故障が発生したことを示します。

Loss of Signal （信号損失） — ケーブルで信号損失が発生していることを示します。

Data Ready （データレディ） — オプティカルトランシーバが電源オンの状態にあり、データ転送の準備が整っていることを示します。

オプティカルトランシーバ診断テスト結果表の表示

□□□ オプティカルトランシーバページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

テストが実行され、オプティカルトランシーバ診断表ページが開きます。

オプティカルトランシーバページの各フィールドに加えて、**Optical Transceiver Diagnostics Table** （オプティカルトランシーバ診断表）には次のフィールドがあります。

Unit No（ユニット番号） — 表示されているケーブルのユニット番号です。

- **N/A** — 利用不可、N/S — 未サポート、W — 警告、E — エラー

メモ： Finisar 製トランシーバはトランスミッタの故障診断テストをサポートしていません。

メモ： ファイバー解析機能は、デジタル診断スタンダードSFF-872 をサポートする SFP のみ で動作します。

CLI コマンドを使用したファイバーケーブルテストの実行

ファイバーケーブルテストの実行を指示する CLI コマンドを以下の表に示します。

表**6-27** ファイバーケーブルテスト **CLI** コマンド

CLI コマンド	説明
show fiber-ports optical- transceiver [*interface*] [*detailed*]	オプティカルトランシーバ診断を表示します。

以下に CLI コマンドの例を示します。

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

Port	Temp [C]	Voltage	Current [Volt]	Output [mA]	Input [mWatt]	POWER TX [mWatt]	LOS Fault
----	----	------	-----	------	------	------	-----
1/e1	48	5.15	50	1.789	1.789	No	No
1/e2	43	5.15	10	1.789	1.789	No	No

スイッチセキュリティの管理

セキュリティ管理ページでは、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に関する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。セキュリティ管理ページを開くには、ツリービューから **System** （システム）→ **Management Security** （セキュリティ管理）をクリックします。

アクセスプロファイルの定義

アクセスプロファイルページは、デバイスをアクセスするプロファイルおよびルールを定義するフィールドで構成されています。管理機能へのアクセスは、**ingress** インタフェースおよびソース **IP** アドレスかソース **IP** サブネットによって定義されるユーザーグループに限定することが可能です。

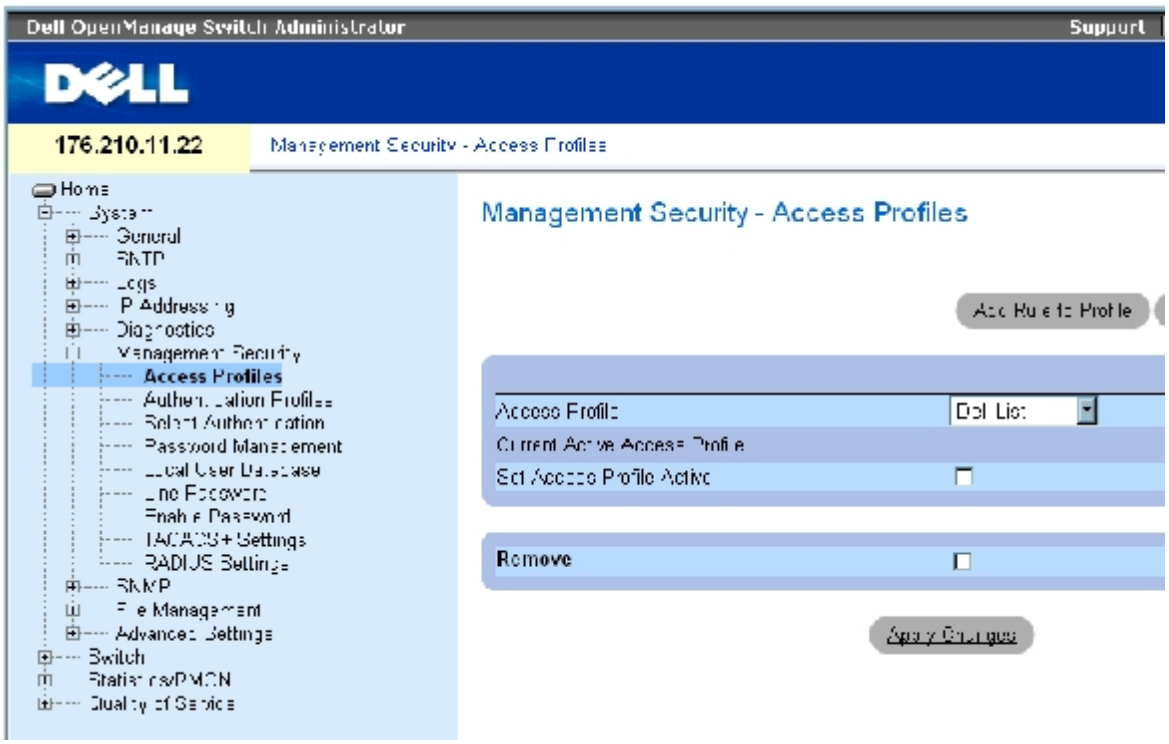
管理アクセスは、**Web**（**HTTP**）、セキュア **Web**（**HTTPS**）、**Telnet**、セキュア **Telnet** など、管理アクセス方法の各タイプごとに、個別に定義することが可能です。

異なる管理方法へのアクセスは、ユーザーグループ間で異なる場合があります。たとえば、ユーザーグループ **1** は **HTTPS** セッションのみを介してデバイスにアクセスすることができ、一方のユーザーグループ **2** は **HTTPS** と **Telnet** セッションの両方を介してデバイスにアクセスすることができる、といった場合です。

管理アクセスリストは、デバイスを管理できるユーザーとその方法を決定する、最大 **256**のルールで構成されます。また、デバイスへのアクセスに対してユーザーを遮断することが可能です。

アクセスプロファイルページには、管理リストの設定と特定インタフェースにリストを適用するフィールドが表示されます。アクセスプロファイルページを開くには、ツリービューから **System** （システム）→**Management Security** （管理セキュリティ）→**Access Profiles** （アクセスプロファイル）をクリックします。

図**6-38** アクセスプロファイル



アクセスプロファイルページは以下のフィールドで構成されています。

Access Profile （アクセスプロファイル）— ユーザー定義のアクセスプロファイルリストです。アクセスプロファイルは**Console Only**（コンソールのみ）がデフォルト値として書き込まれています。このアクセスプロファイルを選択すると、デバイスの有効な管理は、コンソール接続のみを使用して実行されます。

Current Active Access Profile （現在のアクティブなアクセスプロファイル） — 現在アクティブなアクセスプロファイルを示します。

Set Access Profile Active （アクセスプロファイルのアクティブ化） — アクセスプロファイルをアクティブにします。

Remove （削除）— 選択によって、アクセスプロファイルを**Access Profile Name** （アクセスプロファイル名）リストから削除します。

プロファイルの有効化

□□□ アクセスプロファイルページを開きます。

□□□ **Access Profile** （アクセスプロファイル）フィールドにあるアクセスプロファイルを 1 つ選択します。

□□□ **Set Access Profile Active** （アクセスプロファイルのアクティブ化）チェックボックス を選択します。

□□□ **Apply Changes** （変更の適用）をクリックします。

アクセスプロファイルがアクティブになります。

アクセスプロファイルの追加

ルールは、ルール優先度の決定、デバイスの管理方法、インタフェースタイプ、ソース 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の遮断と許可が可能です。ルール優先度は、実装されるルールの順番を設定します。

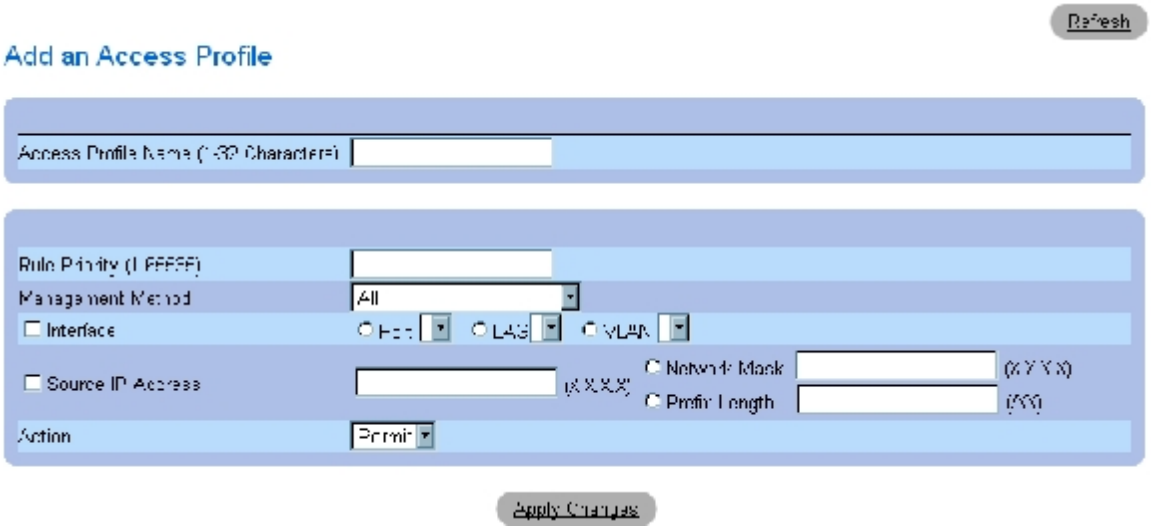
アクセスプロファイル用ルールの定義

□□□ アクセスプロファイルページを開きます。

□□□ **Add Profile** （プロファイルの追加）をクリックします。

アクセスプロファイルの追加ページが開きます。

図**6-39** アクセスプロファイルの追加



アクセスプロファイルの追加 ページは以下のフィールドで構成されます。

Access Profile Name（**1**～**32** 文字）（アクセスプロファイル名）— アクセスプロファイルのユーザー定義名です。アクセスプロファイル名は最大 32 文字です。

Rule Priority（**1**～**65535**）（ルールの優先度）— ルールの優先度を示します。パケットがルールに一致した場合、ユーザーグループはデバイス管理へのアクセスを許可されるか、もしくはアクセスを拒絶されます。このフィールドを使用してルール優先度を定義することにより、ルールの順序が決まります。パケットは先に適合するものから一致比較されるため、ルール番号はパケットをルールに一致比較させる操作に不可欠です。ルール優先度は **Profile Rules Table**（プロファイルルール表）に表示されます。

Management Method（管理方法）— アクセスプロファイルを定義する管理方法です。このアクセスプロファイルを有するユーザーは、指定した管理方法（ライン）によって、デバイスへのアクセスを拒絶または許可されます。

Interface（インタフェース）— 規則を適用するインタフェースタイプです。このフィールドはオプションです。このルールは、チェックボックスを選択し、次に対応するオプションボタンとインタフェースを選択することで、選択したポート、LAG、または VLAN に適用することが可能です。

メモ： アクセスプロファイルをインタフェースに割り当てると、他のインタフェースを介し たアクセスは拒絶されます。アクセスプロファイルがいかなるインタフェースにも割り当て られていない場合、デバイスはすべてのインタフェースからアクセスが可能です。

Source IP Address（X.X.X.X）（ソース IP アドレス）— ルールを適用するインタフェースのソース IP アドレスです。このフィールドはオプションで、ルールがサブネットワークに対して有効であることを示します。

Network Mask（X.X.X.X）（ネットワークマスク）— IP サブネットワークマスクです。

Prefix Length（**/XX**）（プレフィックス長）— ソース IP アドレスプレフィックスのビット数、またはソース IP アドレスのネットワークマスクのビット数です。

Action（アクション）— 定義したインタフェースに対して、管理アクセスの許可または拒否を定義します。

□□□ **Access Profile Name**（アクセスプロファイル名）フィールドを定義します。

□□□ 各関連フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

新しいアクセスプロファイルが追加され、デバイスがアップデートされます。

アクセスプロファイルへのルールの追加

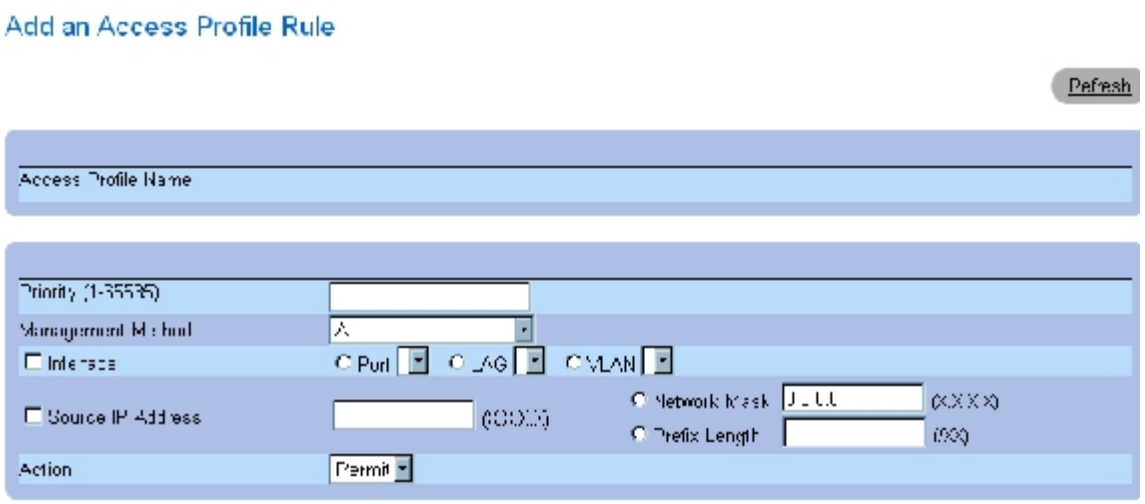
メモ： アクセスプロファイルへのトラフィックの一致比較を開始するには、最初のルールを 定義する必要があります。

□□□ アクセスプロファイルページを開きます。

□□□ **Add Rule to Profile** （プロファイルへのルール追加）をクリックします。

アクセスプロファイルルールの追加ページが開きます。

図**6-40** アクセスプロファイルルールの追加



□□□ 各フィールドを入力します。

□□□ **Apply Changes** （変更の適用）をクリックします。

ルールがアクセスプロファイルに追加され、デバイスがアップデートされます。

プロファイルルール表の表示

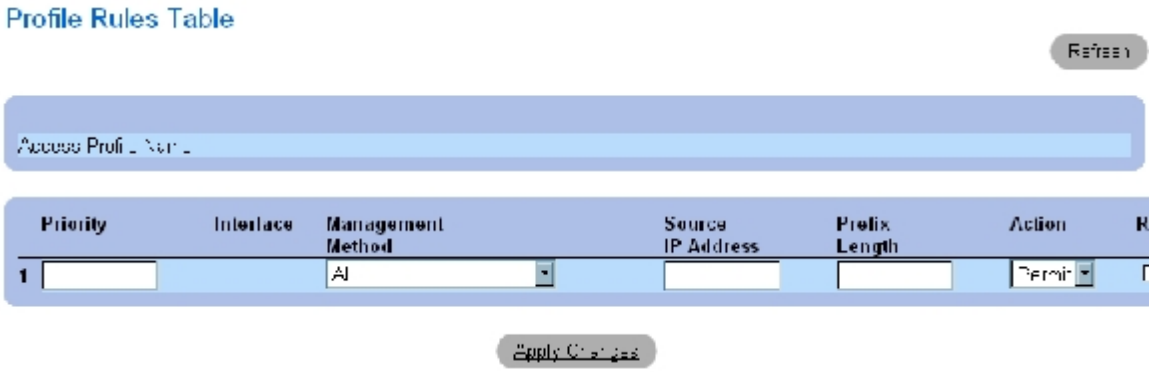
メモ： **Profile Rules Table** （プロファイルルール表）に表示されるルール順は重要です。パ ケットは、ルール条件を満たす最初のルールと一致比較されます。

□□□ アクセスプロファイル ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

Profile Rules Table （プロファイルルール表） ページ が開きます。

図**6-41** プロファイルルール表ページ



ルールの削除

□□□ アクセスプロファイル ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

プロファイルルール表ページが開きます。

□□□ ルールを選択します。

□□□ **Remove** （削除）チェックボックスを選択します。

□□□ **Apply Changes** （変更の適用）をクリックします。

選択したルールは削除され、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

アクセスプロファイルページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-28** アクセスプロファイル **CLI** コマンド

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入力します。
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拒否条件と、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拒否条件と、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)#
management access-list
mlist


console(config-macl)#
permit ethernet 1/e1


console(config-macl)#
permit ethernet 1/e2


console(config-macl)#
deny ethernet 1/e3


console(config-macl)#
deny ethernet 1/e4


console(config-macl)#
exit


console(config)#
management access-class
mlist


console(config)# exit


console# show management
access-list


mlist


-----


permit ethernet 1/e1


permit ethernet 1/e2


deny ethernet 1/e3


deny ethernet 1/e4


! (Note: all other access
implicitly denied)


Console# show management
access-class


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

認証プロファイルの定義

認証プロファイルページには、デバイス上でのユーザー認証方法を指定するフィールドが表示されます。ユーザー認証は以下のように行われます。

- ローカルに

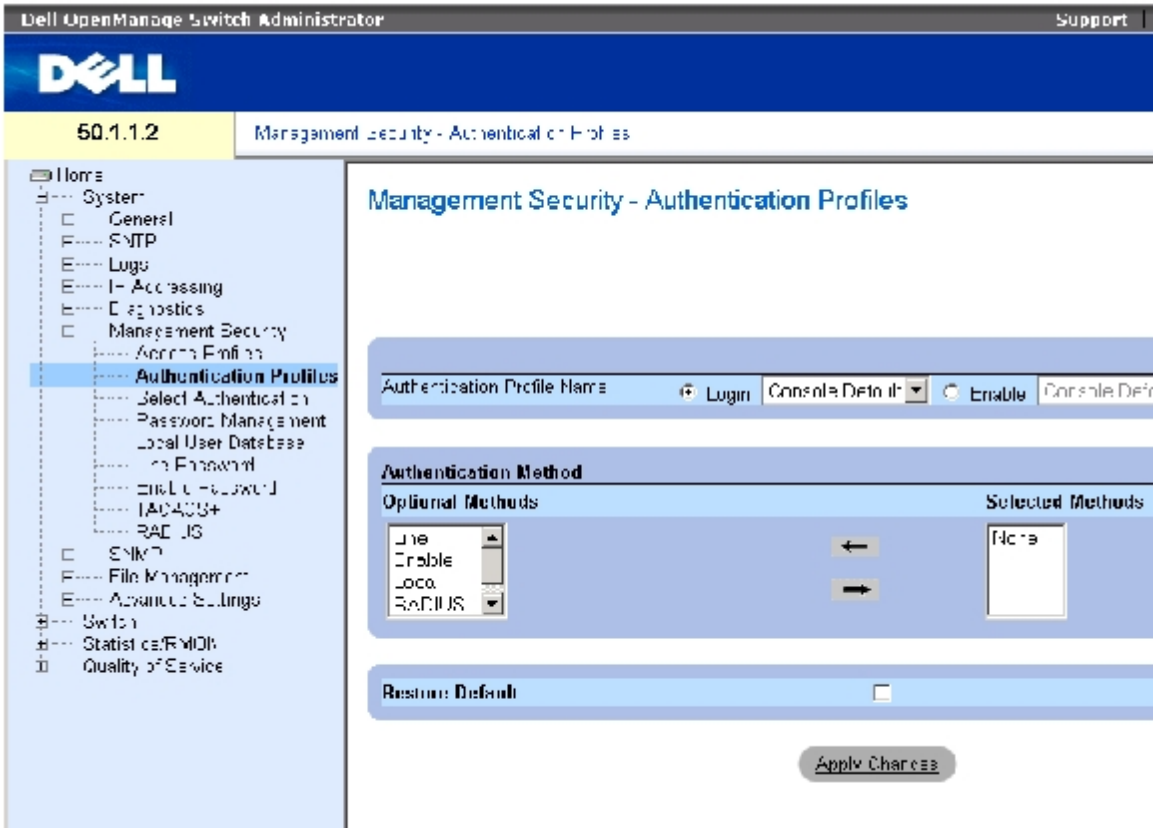
- 外部サーバーを経由して

ユーザー認証は、**None** （なし）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行われます。たとえば、**Local**（ローカル）オプションと **RADIUS** （**RADIUS**）オプションの両方が選択されている場合、ユーザーの認証は先にローカルで行われます。ローカルユーザーデータベースが空の場合、次にユーザー認証は **RADIUS** サーバーを介して行われます。第 **1** の方法を使用して認証に失敗した場合、認証プロセスは終了します。

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。認証プロファイル ページを開くには、ツリービューから **System** （システム）→ **Management Security** （セキュリティ管理）→ **Authentication Profiles** （アクセスプロファイル）をクリックします。

図**6-42** 認証プロファイル



認証プロファイルページは以下のフィールドで構成されています。

Authentication Profile Name （認証プロファイル名）— ユーザー定義の認証プロファイルが追加される、ユーザー定義の認証プロファイルリストです。デフォルトは**Network Default**（ネットワークデフォルト）と**Console Default**（コンソールデフォルト）です。

- **Login** （ログイン）— ログインパスワードに使用するユーザー定義認証プロファイルリストを指定します。
- **Enable** （有効）— パスワードの有効化に使用するユーザー定義認証プロファイルリストを指定します。

Optional Methods （オプション方法） — ユーザー認証方法です。可能なオプションは以下のとおりです。

None （なし）— ユーザー認証は行われません。

Local （ローカル）— ユーザー認証はデバイスレベルで行われます。デバイスは、ユーザー名とパスワードを確認して認証を行います。

RADIUS （RADIUS）— ユーザー認証は RADIUS サーバーで行われます。詳細については、「RADIUS の設定」を参照してください。

Line （ライン）— ユーザー認証にラインパスワードが使用されます。

Enable（有効化）— 認証に有効化パスワードが使用されます。

TACACS+ （TACACS+）— ユーザー認証は TACACS+ サーバーで行われます。

Restore Default （デフォルトに戻す）— デバイス上でのユーザー認証をデフォルトに戻します。デフォルトプロファイルのみで利用可能です。

Remove （削除）— チェックすることで、選択したプロファイルを削除します。アクティブプロファイルは削除できません。ユーザー定義プロファイルのみで利用可能です。

認証プロファイルの選択

□□□ 認証プロファイル ページを開きます。

□□□ **Authentication Profile Name** （認証プロファイル）フィールドでプロファイルを 1 つ選 びます。

□□□ ナビゲーションアイコンを使用して認証方法を選びます。リストに認証方法が並んで いる順で認証が行われます。

□□□ Apply Changes （変更の適用）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。

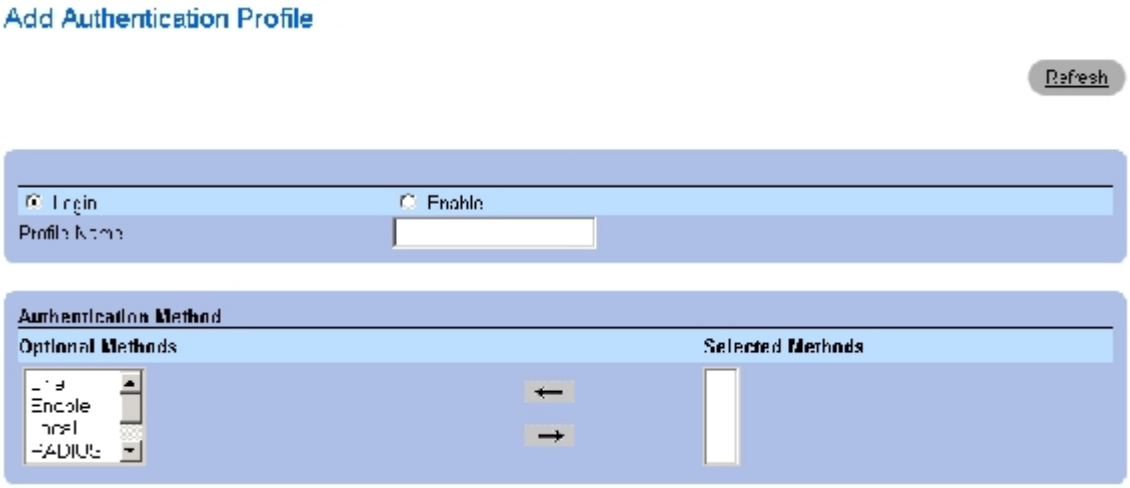
認証プロファイルの追加

□□□ 認証プロファイル ページを開きます。

□□□ Add （追加）をクリックします。

認証プロファイルの追加ページが開きます。

図**6-43** 認証プロファイルの追加



□□□ プロファイルを設定します。

メモ： 新規プロファイルの名称にスペース文字を使用してはなりません。

□□□ Apply Changes （変更の適用）をクリックします。

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。

認証プロファイル表の示

□□□ 認証プロファイル ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

認証プロファイルページが開きます。

認証プロファイルの削除

□□□ 認証プロファイル ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

認証プロファイル表ページが開きます。

□□□ 認証プロファイルを 1 つ選びます。

□□□ **Remove** （削除）チェックボックスを選択します。

□□□ **Apply Changes** （変更の適用）をクリックします。

選択された認証プロファイルが削除されます。

CLI コマンドを使用した認証プロファイルの設定

認証プロファイル ページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-29** 認証プロファイル**CLI**コマンド

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。

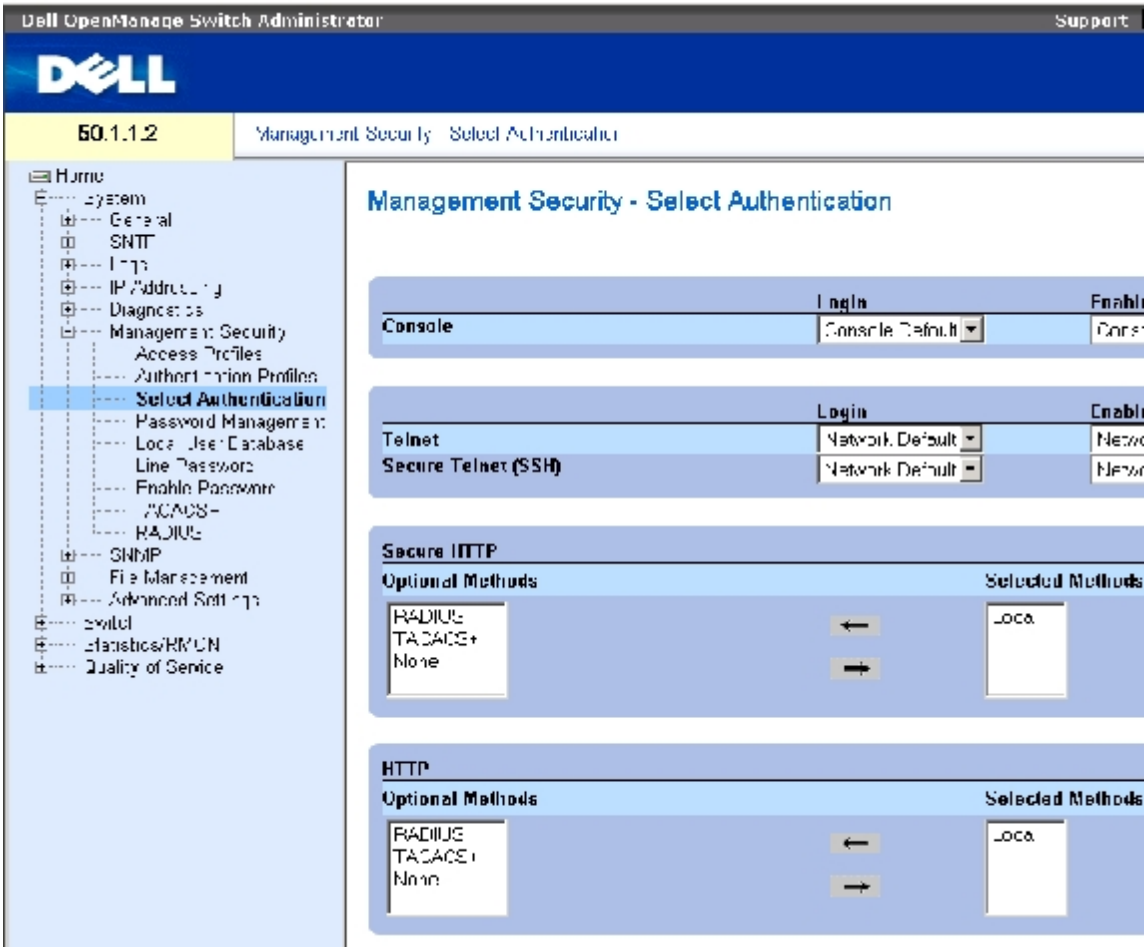
以下に CLI コマンドの例を示します。

```
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選択

認証プロファイルの定義後は、認証プロファイルを管理アクセス方法に適用することが可能です。たとえば、コンソールユーザーは認証方法リスト 1 で認証が行われ、一方の Telnet ユーザーは認証方法リスト 2 で認証が行われます。認証の選択ページを開くには、ツリービューから、System （システム）→ Management Security （セキュリティ管理）→ Select Authentication （認証の選択）をクリックします。

図**6-44** 認証の選択



認証の選択ページは以下のフィールドで構成されています。

Console （コンソール）— コンソールユーザーの認証に使用する認証プロファイルです。

Login （ログイン）— コンソールインタフェースにログインするユーザーに対して使用する認証プロファイルを指定します。

Enable （有効）— コンソールインタフェースから特権 EXEC モードを有効にするユーザーに対して使用する認証プロファイルを指定します。

Telnet （Telnet）— Telnet ユーザーの認証に使用する認証プロファイルです。

Secure Telnet（**SSH**）（セキュア Telnet）— SSH ユーザーの認証に使用する認証プロファイルです。SS Hは、デバイスに対するセキュアで暗号化されたリモート接続を、クライアントに提供します。

HTTP （HTTP）および **Secure HTTP** （セキュア HTTP）— HTTP およびセキュア HTTP アクセスに使用する、それぞれの認証方法です。可能なフィールド値は以下のとおりです。

None （なし）— アクセスには認証方法を使用しません。

Local （ローカル）— 認証はローカルに行われます。

RADIUS （RADIUS）— 認証は RADIUS サーバーで行われます。

TACACS+ （TACACS+）— 認証は TACACS+ サーバーで行われます。

認証リストのコンソールセッションへの適用

□□□ 認証の選択ページを開きます。

□□□ **Console** （コンソール）フィールドから認証プロファイルを選びます。

□□□ **Apply Changes** （変更の適用）をクリックします。

コンソールセッションが認証リストに割り当てられます。

認証リストの**Telnet**セッションへの適用

□□□ 認証の選択ページを開きます。

□□□ **Telnet** （Telnet）フィールドから認証プロファイルを選びます。

□□□ **Apply Changes** （変更の適用）をクリックします。

Telnet セッションが認証リストに割り当てられます。

認証リストのセキュア **Telnet**（**SSH**）セッションへの適用

□□□ 認証の選択ページを開きます。

□□□ **Secure Telnet**（**SSH**） （セキュア Telnet）フィールドから認証プロファイルを選びます。

□□□ **Apply Changes** （変更の適用）をクリックします。

SSH（Secure Telnet）セッションが認証プロファイルに割り当てられます。

HTTP セッションの認証シーケンスへの適用

□□□ 認証の選択ページを開きます。

□□□ **HTTP** （HTTP）フィールドから認証シーケンスを選びます。

□□□ **Apply Changes** （変更の適用）をクリックします。

HTTP セッションが認証シーケンスに割り当てられます。

セキュア**HTTP** セッションの認証シーケンスへの適用

□□□ 認証の選択ページを開きます。

□□□ **Secure HTTP** （セキュア HTTP）フィールドから認証シーケンス を選びます。

□□□ **Apply Changes** （変更の適用）をクリックします。

セキュア HTTP セッションが認証シーケンス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認証シーケンスの割り当て

認証の選択ページ内の各フィールド設定操作と等価な処理を実行するCLI コマンドを以下の表に示します。

表6-30 認証選択 CLI コマンド

CLI コマンド	説明
enable authentication [default | list-name]	リモート Telnet、コンソール、または SSH から、より高次の権限レベルにアクセスする際の認証方法のリストを示します。
login authentication [default | list-name]	リモート Telnet、コンソール、または SSH 用のログイン認証方法のリストを示します。
ip http authentication method1 [method2.]	HTTP サーバー用の認証方法を示します。
ip https authentication method1 [method2.]	HTTPS サーバー用の認証方法を示します。
show authentication methods	認証方法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-line)# enable
authentication default

console(config-line)# login
authentication default

console(config-line)# exit

console(config)# ip http
authentication radius local

console(config)# ip https
authentication radius local

console(config)# exit

console# show authentication methods

Login Authentication Method Lists

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

Console_Default  : None

Network_Default  : Local

Enable Authentication Method Lists

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

Console_Default  :
Enable   None
```

Network_Default	: Enable	
Line	Login Method List	Enable Method List
----	---------- ------	------ ------ ------
Console	Default	Default
Telnet	Default	Default
SSH	Default	Default
http	: Local	
https	: Local	
dot1x	:	

パスワードの管理

パスワード管理により、ネットワークセキュリティとパスワード制御が向上します。SSH、Telnet、HTTP、HTTPS、および SNMP アクセスのパスワードには、次のようなセキュリティ機能が割り当てられています。

- パスワード長の最小長さの定義
- パスワードの有効期限
- 頻度高いパスワード再利用の防止
- 不正ログイン試行後のユーザーのロックアウト

パスワード管理が有効な場合、パスワードの経時処理がすぐに始まります。パスワードは、ユーザー定義の時間/日数失効定義にもとづいて、有効期限が失効します。パスワードが失効する 10 日前に、デバイスはパスワードの失効を警告するメッセージを表示します。

パスワードが失効したあとも、ユーザーは 3 回までログインが可能です。残りの 3 回のログイン時に、パスワードを速やかに変更するように、ユーザーに対して別の警告メッセージが表示されます。パスワードが変更されないと、ユーザーはシステムからロックアウトされ、コンソールを使用してのみログインが可能になります。パスワード警告は syslog ファイルにロギングされます。

特権レベルを再定義した場合、そのユーザーも再定義が必要です。ただし、最初のユーザー定義からのパスワードの経時期間は失効となります。

パスワード管理ページを開くには、ツリービューから System （システム）→ Management Security （セキュリティ管理）→ Password Management （パスワード管理）をクリックします。

図**6-45** パスワード管理

パスワード管理 ページは以下のフィールドで構成されます。

Password Minimum Length（**8**～**64**）（パスワード最小長さ）— チェックを入れたときに、パスワードの最小長さを適用します。たとえば管理者は、すべてのパスワードが短くとも **10** 文字以上でなければならないと定義することが可能です。

Consecutive Passwords Before Re-use（再利用前の連続パスワード）— パスワードを変更するまでに、パスワードを再使用できる期間を示します。設定可能な値の範囲は **1** から **10** です。

メモ： パスワードの有効期限が失効し、変更を必要とする前に、ユーザーには注意が表示さ れます。ただし、この注意は **Web** ユーザーには表示されません。

Enable Login Attempts（ログイン試行の有効）— チェックを入れたとき、ユーザー定義回数を超えて誤ったパスワードが使用されたときに、デバイスに対するユーザーのロックアウトを有効にします。たとえば、このフィールドにチェックを入れ、設定値が **5** で、ユーザーが不正パスワードで **5** 回のログインを試行した場合、**6** 回目の試行でデバイスはユーザーをロックアウトします。設定可能な値の範囲は **1** から **5** です。

パスワード管理の定義

□□□ パスワード管理 ページを開きます。

□□□ 各フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

新しいパスワード管理が定義され、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パスワード管理

パスワード管理ページ内のフィールド設定操作と等価な処理を実行する **CLI** コマンドを以下の表に示します。

表**6-31 CLI** コマンドを使用したパスワード管理

CLI コマンド	説明
password min-length *length*	最小パスワード長を定義します。
password history number	パスワードを変更するまでに、パスワードを再使用可能できる回数を定義します。
password lock-out *number*	ユーザーをデバイスからロックアウトする、不正パスワードの入力回数を定義します。
show password configuration	パスワード管理情報を表示します。

以下に CLI コマンドの例を示します。

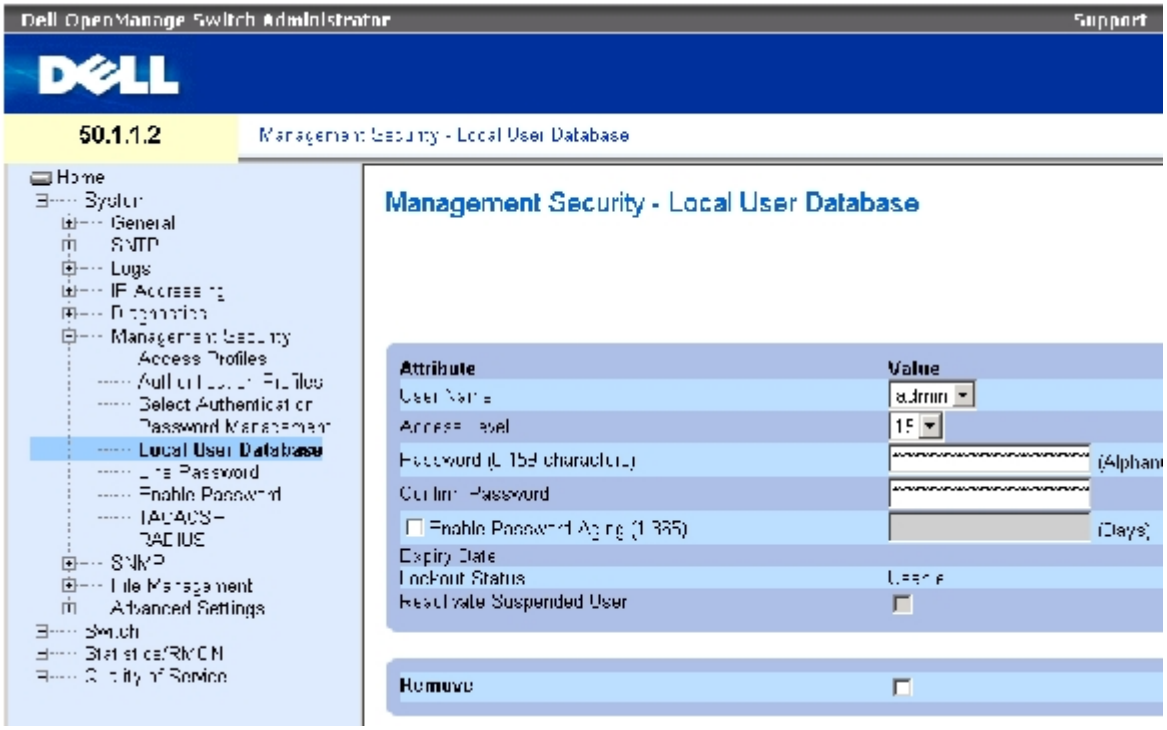
```
console # show passwords configuration

Minimal length: 0

History: Disabled

History hold time: no limit

Lockout control: disabled


Enable Passwords

Level   Password Aging  Password Expiry date  Lockout
-----   --------        ----------            -------
1       -               -                     -
15      -               -                     -


Line Passwords

Line    Password Aging  Password Expiry date  Lockout
-------  --------       ----------            -------
Telnet  -               -                     -
SSH     -               -                     -
Console -               -                     -

console # show users accounts
```

Username	Privilege	Password Aging	Password Expiry Date	Lockout
--------	--------	--------	--------	------
nim	15	39	18-Feb-2005	

ローカルユーザーデータベースの定義

ローカルユーザーデータベース ページには、ユーザー、パスワード、アクセスレベルを定義するフィールドが表示されます。ローカルユーザーデータベース ページを開くには、ツリービューから **System** （システム）→ **Management Security** （セキュリティ管理）→ **Local User Database** （ローカルユーザーデータベース）をクリックします。

図**6-46** ローカルユーザーデータベース



ローカルユーザーデータベース ページは以下のフィールドで構成されます。

User Name （ユーザー名）— ユーザーのリストです。

Access Level （アクセスレベル）— ユーザーアクセスレベルです。最低のユーザーアクセスレベルは **1** で、最高のユーザーアクセスレベルは **15** です。アクセスレベル **15** のユーザーは特権ユーザーです。このユーザーのみ、**OpenManage Switch Administrator** のアクセスと使用が可能です。

Password（**0**～**159** 文字）（パスワード）— ユーザー定義パスワードです。

Confirm Password （パスワードの確認）— ユーザー定義パスワードを確認します。

Enable Password Aging（**1**～**365**）（パスワード有効期限の有効化）— 選択したとき、パスワードの有効期限が満了となるまでに経過できる時間を単位を日数として示します。

Expiry Date （期限満了日）— ユーザー定義パスワードの期限満了日を示します。

Lockout Status （ロックアウト状態）— パスワード管理ページで**Enable Login Attempts** （ログイン試行の有効）チェックボックスが選択されている場合、ユーザーの正常な最終ログイン以降の不正認証試行回数を指定します。ユーザーアカウントがロックされているとき、**LOCKOUT** （ロックアウト）を指定します。

Reactivate Suspended User （保留中ユーザーの再アクティブ化）— 選択したとき、指定したユーザーのアクセス権を再度アクティブにします。不正ログイン試行後にアクセス権は保留状態になります。

Remove （削除）— 選択したとき、**User Name** （ユーザー名）リストからユーザーを削除します。

ユーザーへのアクセス権の割り当て

□□□ ローカルユーザーデータベース ページを開きます。

□□□ **User Name**（ユーザー名）フィールドでユーザーを 1 件選択します。

□□□ 各フィールドを定義します。

□□□ **Apply Changes** （変更の適用）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。

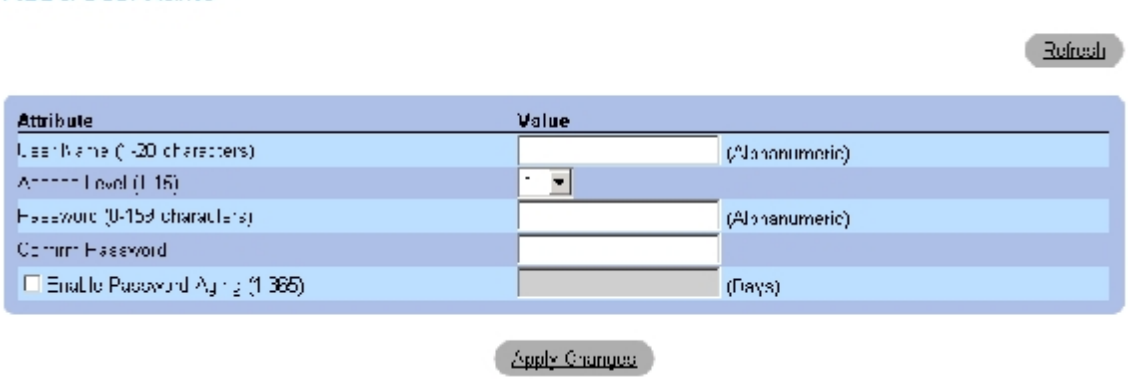
新規ユーザーの定義

□□□ ローカルユーザーデータベース ページを開きます。

□□□ **Add** （追加）をクリックします。

ユーザー追加ページが開きます。

図**6-47** ユーザー追加



□□□ 各フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

新規ユーザーが定義され、デバイスがアップデートされます。

ローカルユーザー表の表示:

□□□ ローカルユーザーデータベース ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

ローカルユーザー表が開きます。

図**6-48** ローカルユーザー表

保留中ユーザーの再アクティブ化

□□□ ローカルユーザーデータベース ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

ローカルユーザー表が開きます。

□□□ **User Name** （ユーザー名）エントリを 1 つ選択します。

□□□ **Reactivate Suspended User** （保留中ユーザーの再アクティブ化）チェックボックスを 選択します。

□□□ **Apply Changes** （変更の適用）をクリックします。

ユーザーアクセス権は再度アクティブとなり、デバイスがアップデートされます。

ユーザーの削除

□□□ ローカルユーザーデータベース ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ローカルユーザー表が開きます。

□□□ **User Name** （ユーザー名）を 1 件選択します。

□□□ **Remove** （削除）チェックボックスを選択します。

□□□ **Apply Changes** （変更の適用）をクリックします。

選択したユーザーは削除され、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

ローカルユーザーデータベース ページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-32** ローカルユーザーインタフェース **CLI** コマンド

CLI コマンド	説明
username name [password password] [level level] [encrypted]	ユーザー名に基づいた認証システムを確立します。
set username name active	保留中ユーザーのアクセス権を再度アクティブにします。

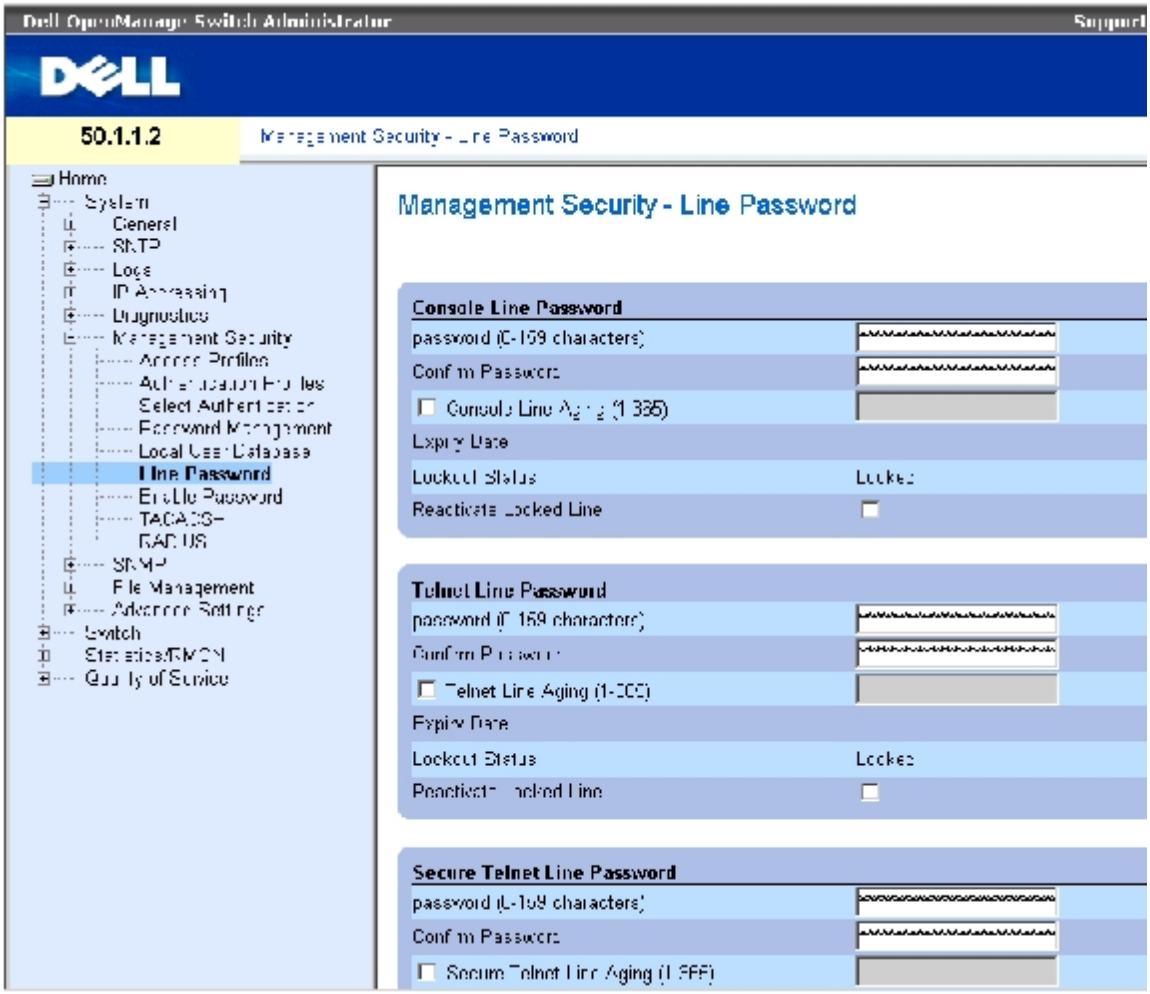
以下に CLI コマンドの例を示します。

```
console(config)# username
bob password lee level 15


console# set username bob
active
```

ラインパスワードの定義

ラインパスワード ページには、各管理方法に対するラインパスワードの定義フィールドが表示されます。ラインパスワードページを開くには、ツリービューから System （システム）→ Management Security （セキュリティ管理）→ Line Passwords （ラインパスワード）をクリックします。

図**6-49** ラインパスワード



ラインパスワードページは以下のフィールドで構成されています。

Line Password for Console / Telnet / Secure Telnet （コンソール / Telnet / セキュア Telnet用ラインパスワード）— コンソール、Telnet、またはセキュア Telnet セッションを介してデバイスをアクセスするラインパスワードです。

Confirm Password for Console / Telnet / Secure Telnet （コンソール / Telnet / セキュア Telnet 用パスワードの確認）— 新しいラインパスワードを確認します。パスワードは ***** のような形式で表示されます。

Line Aging（1～365）for Console / Telnet / Secure Telnet （コンソール / Telnet / セキュア Telnet 用ラインエージング）— 選択したとき、ラインパスワードの有効期限を満了にする経過時間を、単位を日数として示します。

Expiry Date for Console / Telnet / Secure Telnet （コンソール / Telnet / セキュア Telnet 用有効期限日）— ラインパスワードの有効期限日を示します。

Lockout Status for Console / Telnet / Secure Telnet （コンソール / Telnet / セキュア Telnet 用ロックアウト状態）— パスワード管理ページで**Enable Login Attempts** （ログイン試行の有効）チェックボックスが選択されている場合、ユーザーの正常な最終ログイン以後の不正認証試行回数を指定します。ユーザーアカウントがロックされているとき、**LOCKOUT** （ロックアウト）を表示します。

Reactivate Locked Line for Console / Telnet / Secure Telnet （コンソール / Telnet / セキュア Telnet 用ロックアウトラインの再アクティブ化）— 選択したときに、コンソール / Telnet / セキュア Telnet セッションのラインパスワードを再びアクティブにします。成功しなかったログイン試行後にアクセス権は保留状態になります。

コンソールセッション用ラインパスワードの定義

□□□ ラインパスワード ページを開きます。

□□□ **Console Line Password** （コンソールラインパスワード）フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

コンソールセッション用ライン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。

Telnetセッション用ラインパスワードの定義

□□□ ラインパスワード ページを開きます。

□□□ Telnet Line Password （Telnet ラインパスワード）フィールドを定義します。

□□□ Apply Change s（変更の適用）をクリックします。

Telnet セッション用ライン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。

セキュア **Telnet** セッション用ラインパスワードの定義

□□□ ラインパスワード ページを開きます。

□□□ **Secure Telnet Line Password** （セキュア Telnet ラインパスワード）フィールドを定義 します。

□□□ Apply Changes （変更の適用）をクリックします。

セキュア Telnet セッション用ライン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ラインパスワードの割り当て

ラインパスワード ページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-33** ラインパスワード **CLI** コマンド

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。

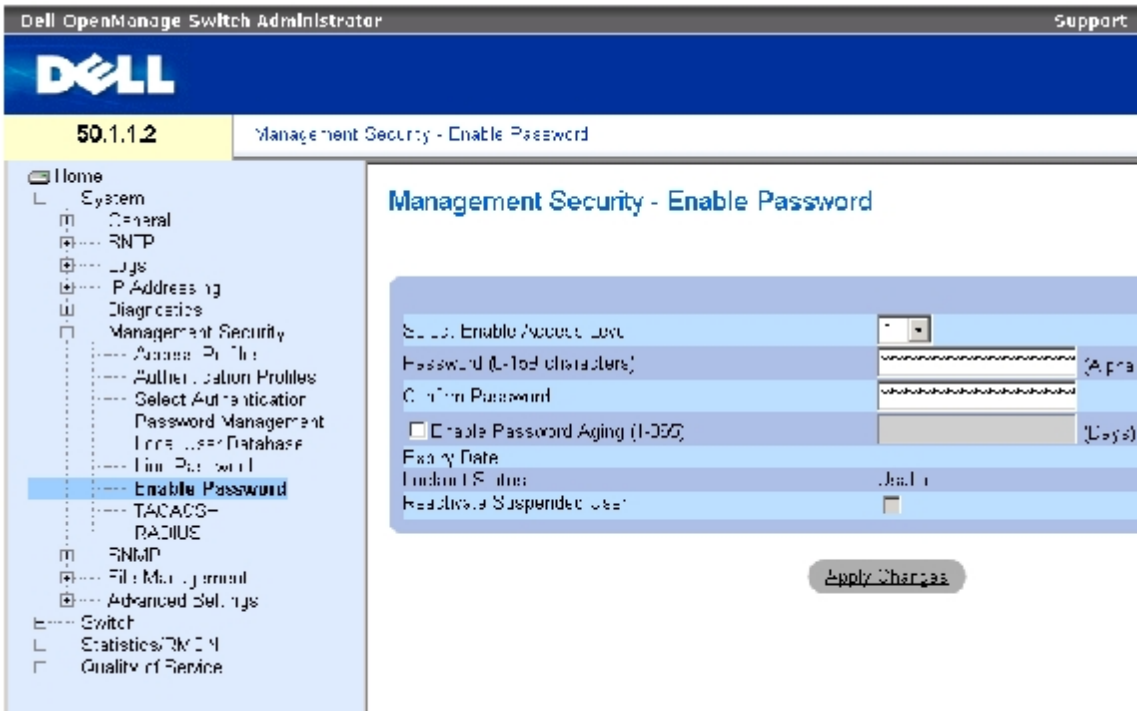
以下に CLI コマンドの例を示します。

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

有効パスワードの定義

有効パスワード ページでは、通常レベル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。有効パスワード ページを開くには、ツリービューから System （システム）→ Management Security （セキュリティ管理）→ Enable Passwords （有効パスワード）をクリックします。

図**6-50** 有効パスワード



有効パスワード ページは以下のフィールドで構成されます。

Select Enable Access Level（有効アクセスレベルの選択）— 有効パスワードに関連するアクセスレベルです。設定可能な値の範囲は 1 から 15 です。

Password（**0**～**159 characters**）（パスワード）— 現在の有効パスワードです。

Confirm Password （パスワードの確認）— 新しい有効パスワードを確認します。パスワードは ***** のような形式で表示されます。

Enable Password Aging（**1**～**365**）（パスワードの有効期限化）— 選択したとき、パスワードの有効期限が満了になる前に経過する時間を単位を日数として示します。

Expiry Date （期限満了日）— 有効パスワードの期限満了日を示します。

Lockout Status （ロックアウト状態）— パスワード管理ページで**Enable Login Attempts** （ログイン試行の有効）チェックボックスが選択されている場合、ユーザーの正常な最終ログイン以後の不正認証試行回数を指定します。ユーザーアカウントがロックされているとき、**LOCKOUT** （ロックアウト）を表示します。

Reactivate Suspended User （保留中ユーザーの再アクティブ化）— 選択したとき、指定したユーザーのアクセス権をもう一度アクティブにします。成功しなかったログイン試行後にアクセス権は保留状態になります。

新規有効パスワードの定義

□□□ 有効パスワード ページを開きます。

□□□ 各フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

新しい有効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パスワードの割り当て

有効パスワード ページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-34** 有効パスワード変更 **CLI** コマンド

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。

以下に CLI コマンドの例を示します。

```
console(config)# enable
password level 15 secret
```

TACACS+ 設定の定義

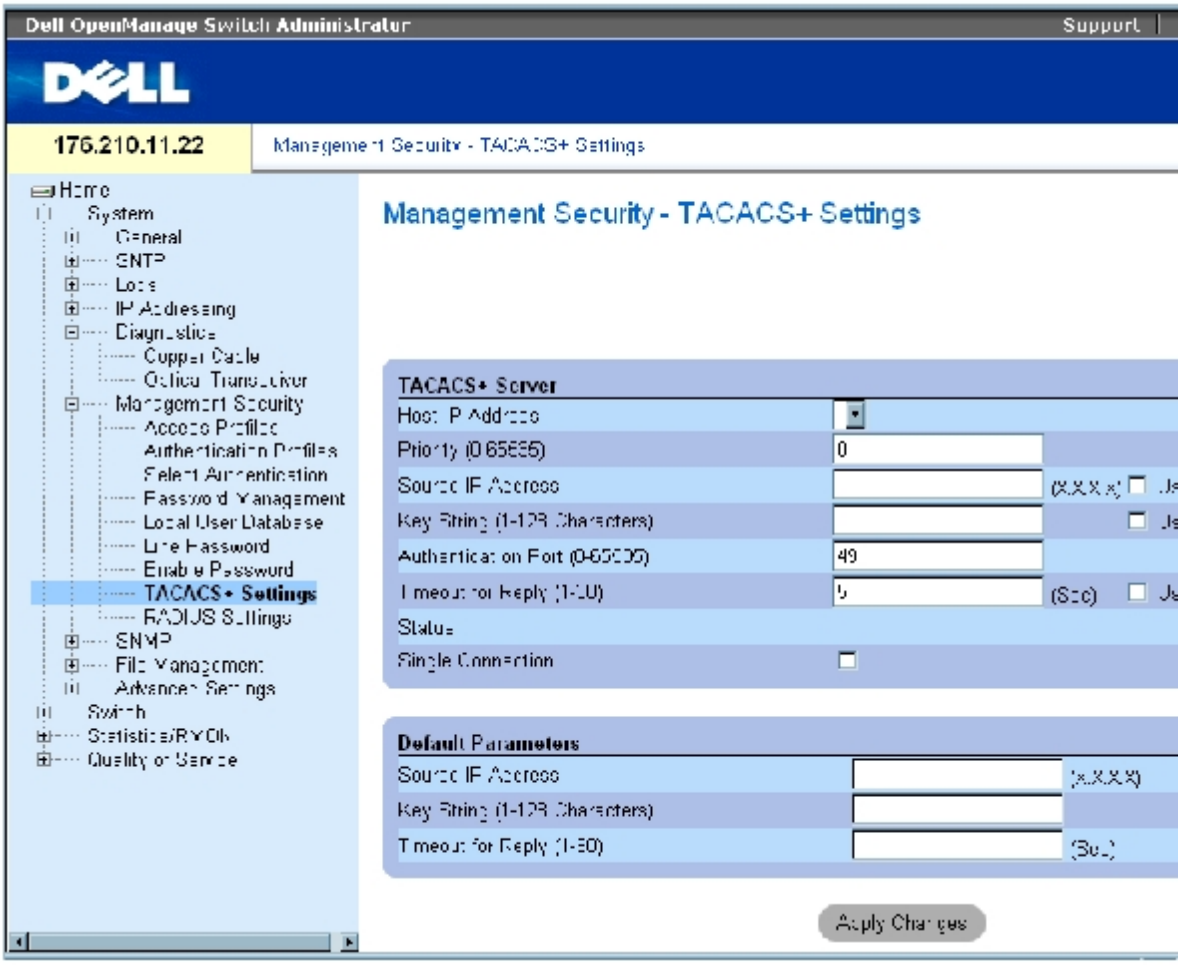
本デバイスは、Terminal Access Controller Access Control System （TACACS+）クライアントサポートを提供しています。TACACS+ は、デバイスにアクセスするユーザーの確認に関して、セキュリティの中央集約化を実現します。

TACACS+ は中央集約化したユーザー管理システムを提供する一方で、RADIUS や他の認証プロセスとの一貫性も維持します。TACACS+ は以下のサービスを提供します。

- Authentication （認証）— ログイン中、ユーザー名とユーザー定義パスワードを介して、認証を提供します。
- Authorization （認可）— ログイン時に実行されます。認証セッションが完了すると、認証が与えられたユーザー名を使用しながら認可セッションが始まります。TACACS+ サーバーはユーザー特権を確認します。

TACACS+ プロトコルは、デバイスと TACACS+ サーバー間とで交換される暗号化プロトコルを通じて、ネットワークの完全性を保証します。**TACACS+** の設定 ページを開くには、ツリービューから **System** （システム）→ **Management Security** （セキュリティ管理）→ **TACACS+** （TACACS+）をクリックします。

図**6-51 TACACS+** の設定



TACACS+ の設定 ページは以下のフィールドで構成されます。

Host IP Address （ホスト IP アドレス）— TACACS+ サーバーの IP アドレスを示します。

Priority（0～65535）（優先度）— 使用する TACACS+ サーバーの順番を示します。デフォルトは 0 です。

Source IP Address （ソース IP アドレス）— デバイスと TACACS+ サーバー間の TACACS+ セッションに使用されるデバイスソース IP アドレスです。

Key String（0～128 文字）（キーストリング）—デバイスと TACACS+ サーバー間の TACACS+ 通信用の認証キーと暗号化キーを定義します。キーは TACACS+ サーバーで使用される暗号化キーと一致しなければなりません。このキーは暗号化されます。

Authentication Port（0～65535）（認証ポート）— TACACS+ セッションが発生するポート番号です。デフォルトはポート 49 です。

Timeout for Reply（1～30）（応答のタイムアウト）— デバイスと TACACS+ サーバー間の接続がタイムアウトする前に経過する時間量です。フィールドに設定可能な値の範囲は 1～30 秒です。

Status （ステータス）— デバイスと TACACS+ サーバー間の接続ステータスです。可能なフィールド値は以下のとおりです。

Connected （接続）— デバイスと TACACS+ サーバー間に接続が存在します。

Not Connected （接続なし）— デバイスと TACACS+ サーバー間に接続が存在しません。

Single Connection （単一接続）— 選択されている場合、デバイスとTACACS+サーバー間に単一の接続を維持します。

TACACS+ デフォルトパラメータはユーザー定義デフォルトです。デフォルト設定は新規に定義される TACACS+ サーバーに適用されます。デフォルト値が定義されていない場合、システムデフォルトが新規 TACACS+ サーバーに適用されます。

TACACS+ デフォルトは以下のとおりです。

Source IP Address （ソース IP アドレス）— デバイスと TACACS+ サーバー間の TACACS+ セッションに使用されるデフォルトデバイスソース IP アドレスです。デフォルトソース IP アドレスは 0.0.0.0 です。

Key String（0～128 文字） （キーストリング）— デバイスと TACACS+ サーバー間のすべての通信の認証と暗号化に使用されるデフォルトキーストリングです。このキーは暗号化されます。

Timeout for Reply （1～30）（応答のタイムアウト）— デバイスと TACACS+ サーバー間の接続がタイムアウトする前に経過するデフォルトの時間量です。デフォルト値は 5 秒です。

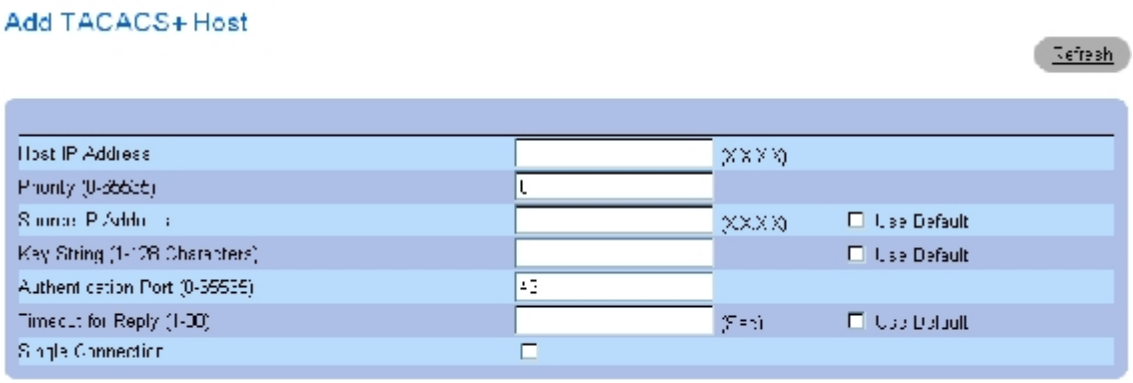
TACACS+ サーバーの追加

□□□ **TACACS+ の設定** ページを開きます。

□□□ Add（追加）をクリックします。

TACACS+ ホストの追加ページが開きます。

図**6-52 TACACS+** ホストの追加



□□□ 各フィールドを定義します。

□□□ Apply Changes （変更の適用）をクリックします。

TACACS+ サーバーが追加され、デバイスがアップデートされます。

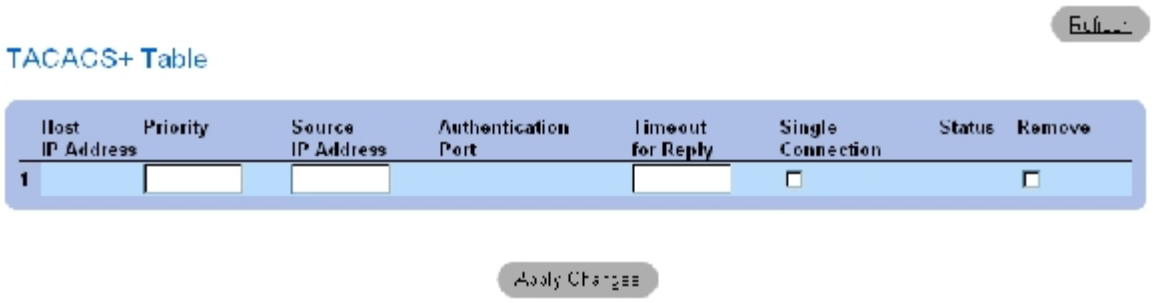
TACACS+表の表示

□□□ **TACACS+ の設定** ページを開きます。

□□□ Show All （すべてを表示）をクリックします。

TACACS+表が開きます。

図**6-53 TACACS+**表



TACACS+ サーバーの削除

□□□ **TACACS+**表 ページを開きます。

□□□ Show All （すべてを表示）をクリックします。

TACACS+表が開きます。

□□□ **TACACS+**表のエントリを 1 つ選択します。

□□□ **Remove** （削除）チェックボックスを選択します。

□□□ Apply Changes （変更の適用）をクリックします。

指定した TACACS+ サーバーが削除され、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 **TACACS+** 設定の定義

TACACS+ の設定 ページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-35 TACACS+ CLI** コマンド

CLI コマンド	説明
tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**port** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**source** *source*] [**priority** *priority*]	TACACS+ ホストを示します。
tacacs-server key key-string	デバイスと TACACS+ サーバー間のすべての TACACS+ 通信に用いる認証と暗号化キーを示します。キーは TACACS+ デーモンで使用される暗号化キーと一致しなければなりません。（範囲：0～128 文字）
tacacs-server timeout timeout	タイムアウト時間を単位を秒として示します。（範囲： 1～30）
tacacs-server source-ip source	ソース IP アドレスを示します。（範囲：有効な IP アドレス）
show tacacs [*ip-address*]	TACACS+ サーバーの設定と統計を示します。

以下に CLI コマンドの例を示します。

```
console# show tacacs
```

Device Configuration						
IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
----------	---------	----	----------	-------	--------	--------
12.1.1.2	Not Connected	49	Yes	1	12.1.1.1	1
Global values						

TimeOut : 5						
Device Configuration ----------						
Source IP : 0.0.0.0						
console#						

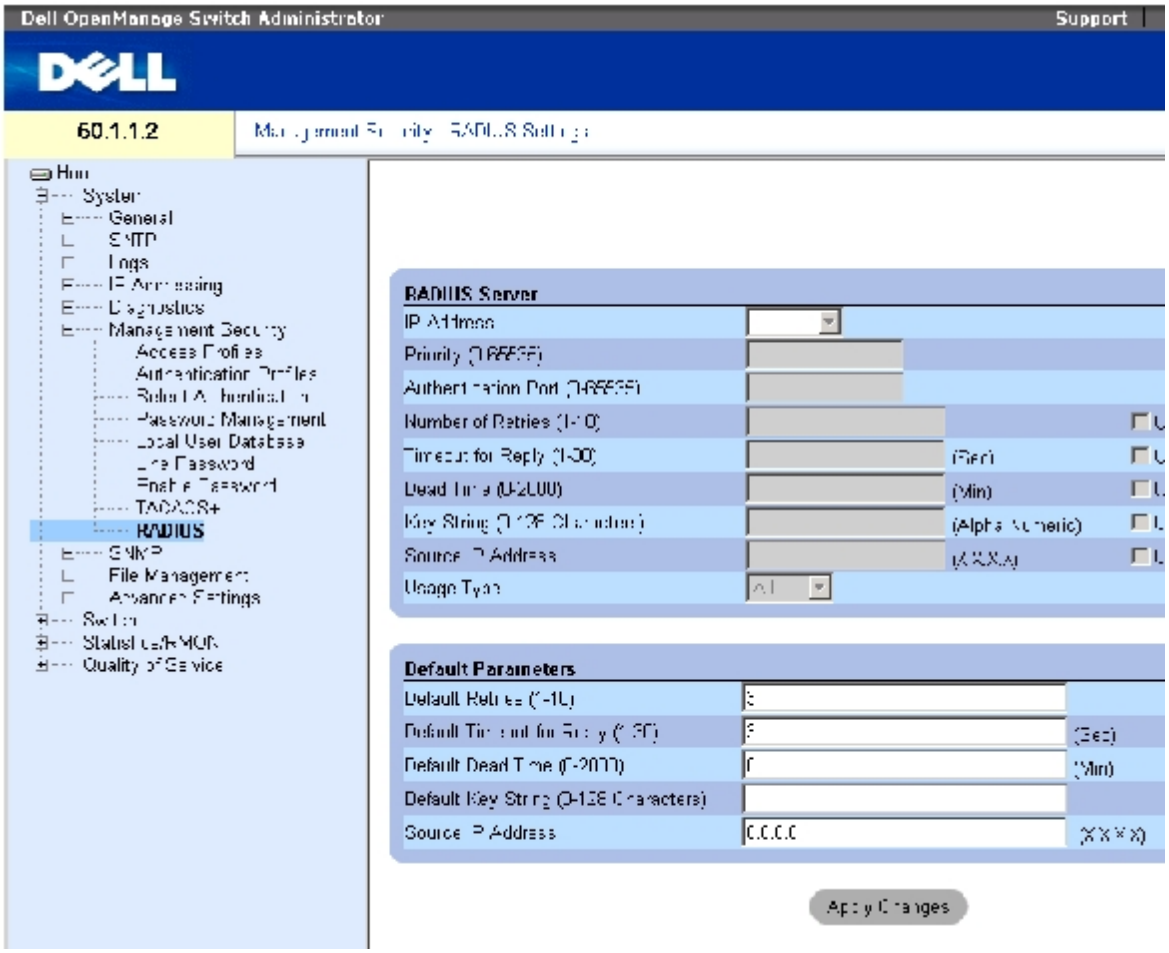
RADIUS の設定

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。最大で 4 台の RADIUS サーバーを定義することが可能です。RADIUS サーバーは以下のアクセスに対して中央集権化された認証方法を提供します。

- Telnet アクセス
- セキュア Shell アクセス
- Web アクセス
- Console アクセス

RADIUS の設定 ページを開くには、ツリービューから System （システム）→ Management Security （セキュリティ管理）→ RADIUS （RADIUS）をクリックします。

図**6-54 RADIUS** の設定



RADIUS の設定ページは以下のフィールドで構成されています。

IP Address （IP アドレス）— 認証サーバーの IP アドレスリストです。

Priority（0～65535）（優先度）— サーバーの優先度を示します。可能な値は 0～65535 で、0 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されます。

Authentication Port （認証ポート）— 認証ポートを示します。認証ポートは、RADIUS サーバー認証の確認に使用されます。

Number of Retries (1～10) （リトライ回数）— 失敗が発生するまでに RADIUS サーバーに送信される要求回数を指定します。設定可能な値の範囲は 1 から 10 です。

Timeout for Reply（1～30）（応答のタイムアウト）— デバイスが照会の再試行を行う前、または次のサーバーに切り替える前に RADIUS サーバーからの答を待つ時間を秒を単位として示します。設定可能な値の範囲は 1 から 30 です。

Dead Time（0～2000）（デッドタイム）— 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単位を分として示します。値の範囲は 0～2000 です。

Key String（1～128 文字） — デバイスと RADIUS サーバー間の全 RADIUS 通信の認証と暗号化に使用されるキーストリングです。このキーは暗号化されます。

Source IP Address （ソース IP アドレス）— RADIUS サーバーとの通信に使用されるソース IP アドレスを示します。

Usage Type （利用タイプ）— サーバーの利用タイプを示します。以下のうちのいずれかの値をとります。login（ログイン）、802.1、または all（すべて）。規定されない場合は all（すべて）がデフォルトになります。

以下のフィールドで RADIUS のデフォルト値を設定します。

メモ： ホスト固有のタイムアウト、リトライ、またはデッドタイム値が規定されていな い場合、グローバル値（デフォルト）が各ホストに適用されます。

Default Retries（1～10）（リトライのデフォルト）— 失敗するまでに RADIUS サーバーに送信される要求のデフォルト回数を示します。

Default Timeout for Reply（1～30）（応答のタイムアウトのデフォルト）— 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示します。デフォルト値は 5 秒です。

Default Dead Time（0～2000）（デッドタイムのデフォルト）— 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。値の範囲は 0～2000 です。

Default Key String（1～128 文字）（キーストリングのデフォルト）— デバイスと RADIUS サーバー間の全 RADIUS 通信の認証と暗号化に使用されるデフォルトのキーストリングです。このキーは暗号化されます。

Source IP Address （ソース IP アドレス）— RADIUS サーバーとの通信に使用されるデフォルトソース IP アドレスを示します。デフォルトソース IP アドレスは 0.0.0.0 です。

RADIUS パラメータの定義

□□□ RADIUS の設定 ページを開きます。

□□□ フィールドを定義します。

□□□ **Apply Changes** （変更の適用）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。

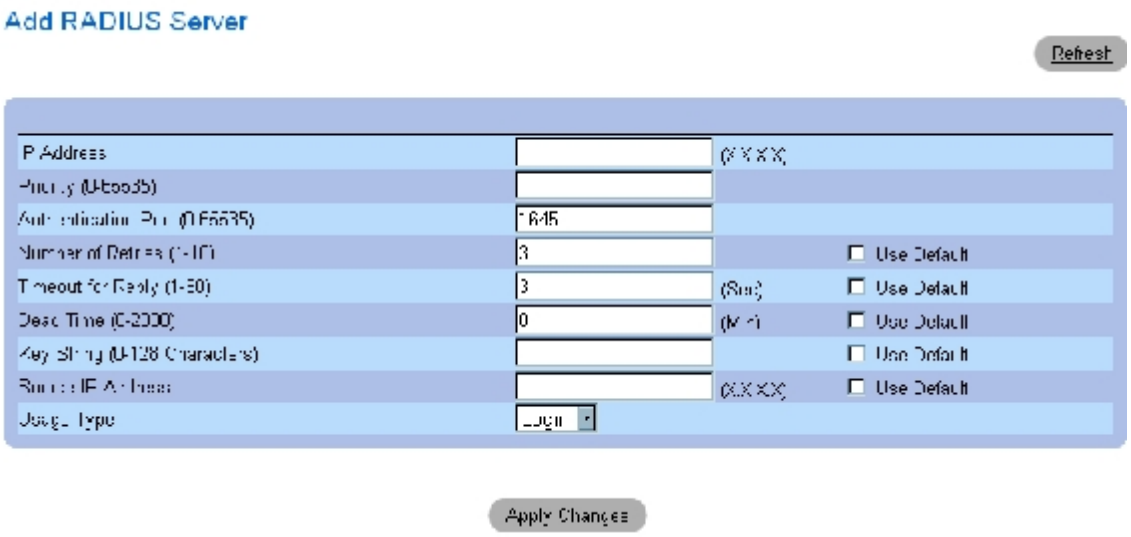
RADIUS サーバーの追加

□□□ RADIUS の設定 ページを開きます。

□□□ **Add** （追加）をクリックします。

RADIUS サーバーの追加ページが開きます。

図**6-55 RADIUS** サーバーの追加ページ



□□□ 各フィールドを定義します。

□□□ **Apply Changes** （変更の適用）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。

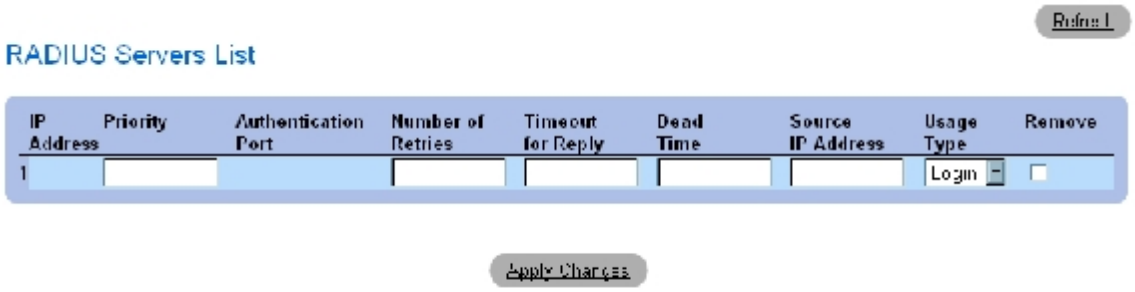
RADIUS サーバーリストの表示

□□□ RADIUS の設定 ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

RADIUS サーバーリスト が開きます。

図**6-56 RADIUS** サーバーリスト



RADIUS サーバーの削除

□□□ RADIUS の設定 ページを開きます。

□□□ Show All （すべてを表示）をクリックします。

RADIUS サーバーリストが開きます。

□□□ RADIUS サーバーリストのエントリを 1 つ選択します。

□□□ Remove （削除）チェックボックスを選択します。

□□□ Apply Changes （変更の適用）をクリックします。

指定した RADIUS サーバーが削除され、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 RADIUS サーバーの定義

RADIUS の設定ページに表示される各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表6-36 RADIUS サーバー CLI コマンド

CLI コマンド	説明
radius-server timeout *timeout*	ルーターがサーバーホストからの応答を待つ間隔を設定します。
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*	ルーターと RADIUS 環境間のすべての RADIUS 通信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 127 timeout 20

Console# show radius-
servers
```

```
IP address Auth Acct
TimeOut Retransmit
Deadtime Source IP
Priority


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


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

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方法を提供します。スイッチがサポートする SNMP バージョンは次のとおりです。

- SNMPv1（バージョン 1）
- SNMPv2（バージョン 2）
- SNMPv3（バージョン 3）

SNMP v1 と v2

SNMP エージェントは、スイッチ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）内で定義されます。MIB はエージェントによって管理される変数を提示します。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によって制御されます。

SNMPv1 と v2 はデフォルトで有効に設定されています。

SNMP v3

SNMP v3 もまた、SNMPv1 と SNMPv2 PDU に対して、アクセスコントロールおよび新しいトラップメカニズムを適用します。さらに、以下を含む、SNMPv3 のUser Security Model（USM）（ユーザーセキュリティモデル）が定義されます。

- **Authentication** （認証）— データの完全性とデータ起源認証を提供します。
- **Privacy** （プライバシー）— メッセージ内容の開示を保護します。暗号化には Cipher Block-Chaining （CBC）が使用されます。SNMP メッセージに対する認証が有効となるか、または SNMP メッセージ認証とプライバシーの両方が有効となります。ただし、認証なしでプライバシーを有効にすることはできません。
- **Timeliness** （適時性）— メッセージ遅延またはメッセージ冗長から保護します。SNM エージェントは入力メッセージをメッセージ時刻情報と比較します。
- **Key Management** （キー管理）— キー生成、キー更新、およびキー使用を定義します。

スイッチは、Object IDs（OID）（オブジェクト ID）に基づく SNMP 通知フィルタをサポートしています。OID はシステム機能を管理する目的でシステムによって使用されます。SNMP v3 は次の機能をサポートしています。

- セキュリティ
- 機能アクセスコントロール

- トラップ

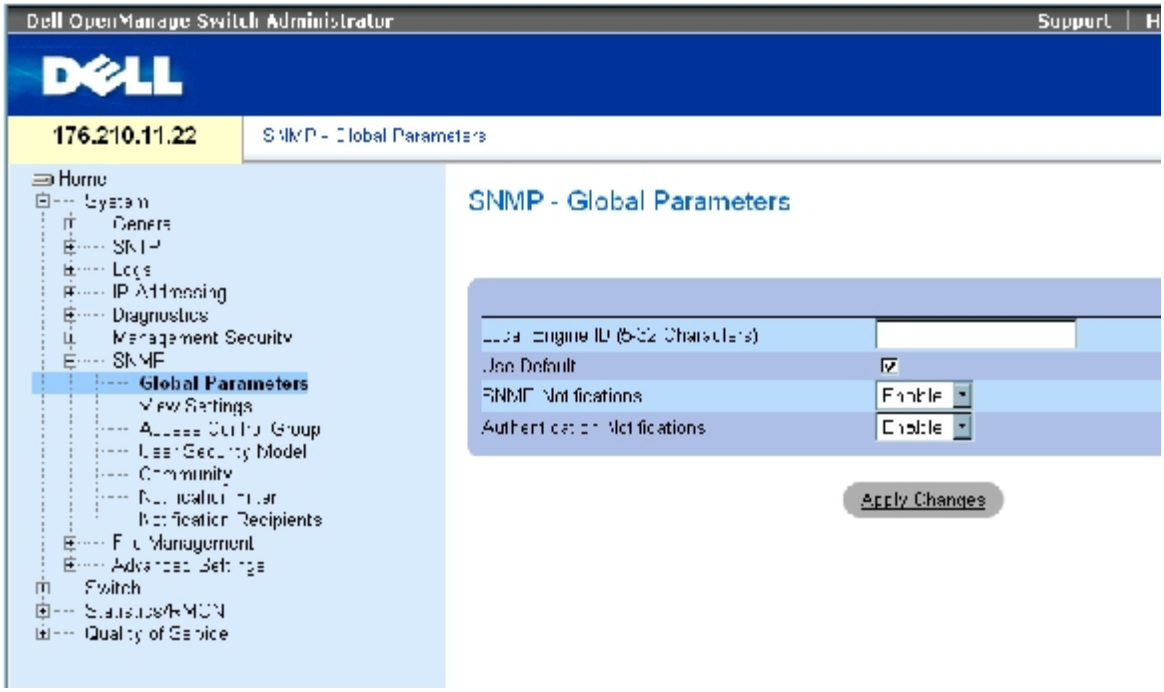
認証またはプライバシーキーは、User Security Model（USM）（ユーザーセキュリティモデル）内で変更されます。

ローカルエンジン ID が有効な場合に、SNMPv3 を有効にすることが可能です。

SNTP グローバルパラメータの定義

SNMP グローバルパラメータページは SNMP と認証通知の両方の有効化を許可します。**SNMP** グローバルパラメータページを開くには、ツリービューから、, click System （システム）→ SNMP （SNMP）→ Global Parameters （グローバルパラメータ）をクリックします。

図**6-57 SNMP** グローバルパラメータ



SNMP グローバルパラメータページは以下のフィールドで構成されています。

Local Engine ID （ローカルエンジンID）— ローカルデバイスエンジン ID を示します。フィールド値は 16 進ストリングです。16 進文字ストリング内の各バイトは 16 進 2 桁です。各バイトはピリオドまたはコロンで区切ることが可能です。SNMPv3 を有効に定義する前に、エンジン ID を定義しなければなりません。

スタンドアロンデバイスの場合、エンタープライズ番号とデフォルト MAC アドレスで構成される、デフォルトエンジン ID を選択します。

スタッキングク可能なシステムの場合、エンジン ID を設定し、そのエンジン ID が管理対象ドメインにユニークであることを確認します。同一のエンジン ID を持つ 2 つのデバイスがネットワークに存在することを防ぎます。

Use Defaults （デフォルトの使用）— デバイスが生成したエンジン ID を使用します。デフォルトエンジンIDは、デバイス MAC アドレスに基づいて、以下のようにスタンダードに従って定義されます。

First 4 octets （先頭の 4 オクテット）— 最初のビット =1、残りは IANA エンタープライズ番号 = 674。

Fifth octet （5 番目のオクテット）— MAC アドレスが次に続くことを示すために3に設定。

Last 6 octets （末尾の 6 オクテット）— デバイスの MAC アドレス。

SNMP Notifications （SNMP 通知）— ルーターの SNMP 通知送信を有効または無効にします。

Authentication Notifications （認証通知）— 認証が失敗したときに、ルーターの SNMP トラップ送信を有効または無効にします。

SNMP 通知の有効化

□□□ SNMP グローバルパラメータ ページを開きます。

□□□ **SNMP Notifications** （SNMP 通知）フィールド内の Enable （有効）を選択します。

□□□ Apply Changes （変更の適用）をクリックします。

SNMP 通知が有効になり、デバイスがアップデートされます。

認証通知の有効化

□□□ **SNMP** グローバルパラメータページを開きます。

□□□ **Authentication Notifications** （認証通知）フィールド内の Enable （有効）を選択しま す。

□□□ **Apply Changes** （変更の適用）をクリックします。

CLI コマンドを使用した SNMP 通知の有効化

SNMP グローバルパラメータページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-37 SNMP** 通知コマンド

CLI コマンド	説明
snmp-server enable traps	ルーターの Simple Network Management Protocol トラップ送信を有効にします。
snmp-server trap authentication	認証が失敗したときに、ルーターの Simple Network Management Protocol トラップ送信を有効にします。
show snmp	SNMP 通信ステータスをチェックします。
snmp-server engine ID local {*engineid-string* | **default**}	ローカルデバイスエンジンIDを示します。フィールド値は 16 進ストリングです。16 進文字ストリングの各バイトは 16 進 2 桁です。各バイトはピリオドまたはコロンで区切りることが可能です。SNMPv3 を有効に定義する前に、エンジン ID を定義しなければなりません。

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# show snmp

Community-String        Community-Access        View name       IP address
----------------        ----------------        ---------       ----------
public                  read only               view-1          All

Community-String        Group name              IP address      Type
----------------        ----------              ----------      ----

Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications

Target Address  Type  Community  Version  Udp Port  Filter name  To Sec  Retries
-------------  ----  ---------  -------  --------  -----------  ------  -------

Version 3 notifications

Target Address  Type  Username  Security Level  Udp Port  Filter name  To Sec  Retries
--------------  ----  --------  --------------  --------  -----------  ------  -------

System Contact: Robert
System Location: Marketing
```

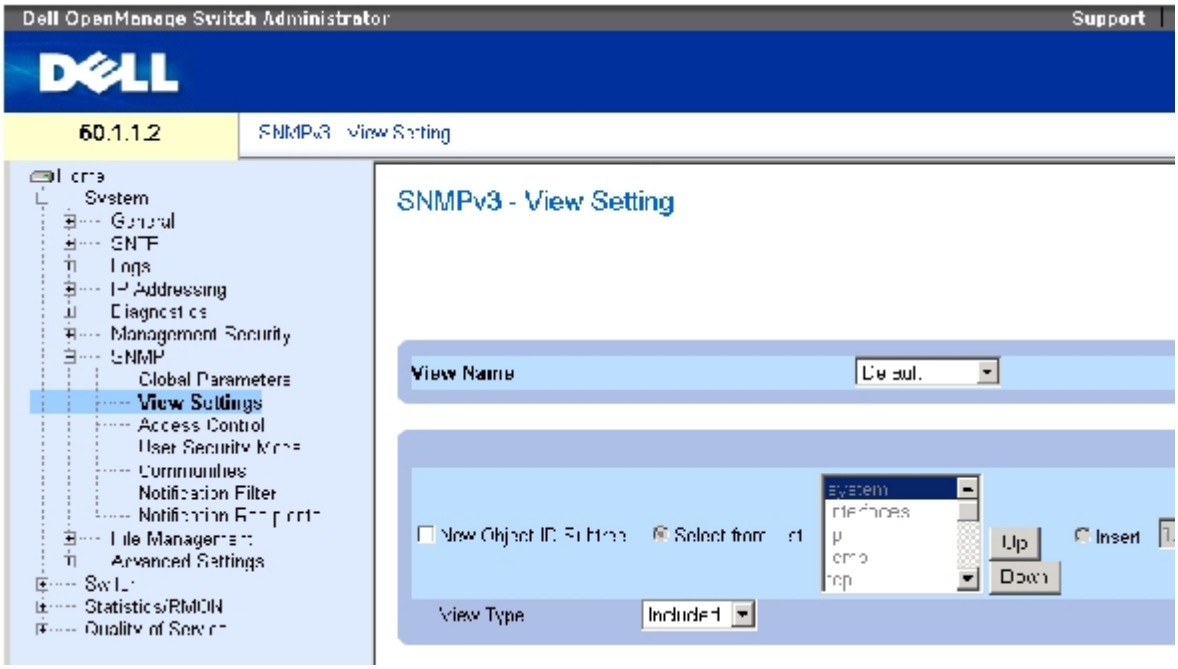
SNMP ビュー設定の定義

SNMP ビューは、デバイス機能または機能アスペクトに対して、アクセスまたはアクセス遮断を提供します。たとえば、SNMP グループ A がマルチキャストグループに対してリードオンリー（R / O）アクセスを持ち、一方で SNMP グループ B がマルチキャストグループに対してリードライト（R / W）アクセスを持つようなビューの定義が可能です。機能アクセスは、MIB 名称、または MIB オブジェクト ID を介して承認されます。

上矢印と下矢印を使って、MIB ツリーおよび MIB ブランチをわたるナビゲーションが可能です。

SNMPv3 ビューの設定 ページを開くには、ツリービューから、**System** （システム）→ **SNMP** （SNMP）→ **View Settings** （ビューの設定）をクリックします。

図**6-58 SNMPv3** ビューの設定



SNMPv3 ビューの設定 ページは以下のフィールドで構成されます。

View Name （ビュー名称）— ユーザー定義のビューで構成されます。ビュー名称は最大で英数字 30 文字です。

New Object ID Subtree （新規オブジェクト ID サブツリー）— 選択した SNMP ビューにデバイス機能 OID が含まれるか含まれないかを示します。

Selected from List （リストから選択）— デバイス機能 OID を、全デバイス OID のリストから **Up** （上）と **Down** （下）ボタンを使用して選択します。

Insert （挿入）— デバイス機能 OID を指定します。

View Type （ビュータイプ）— 定義した OID ブランチが選択した SNMP ビューに含まれる予定か除外される予定か指定します。

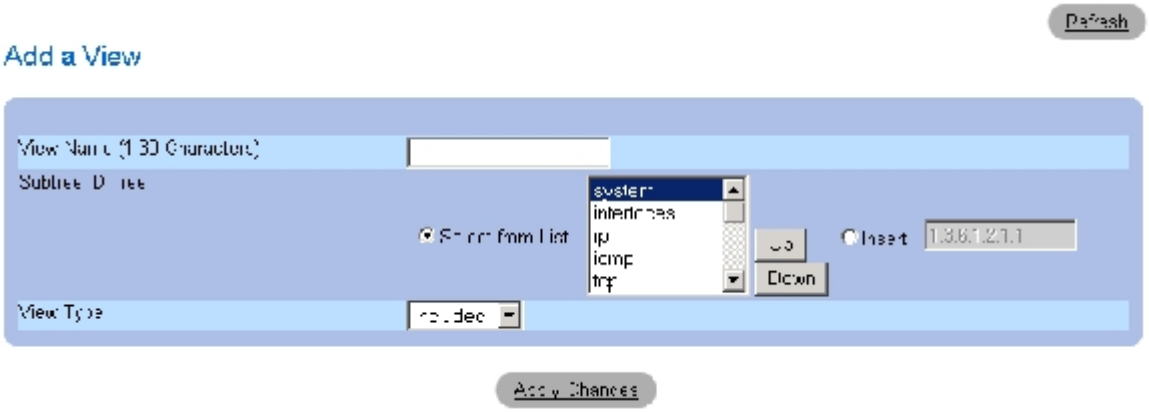
ビューの追加

□□□ **SNMPv3** ビューの設定 ページを開きます。

□□□ **Add** （追加）をクリックします。

ビューの追加 ページが開きます。

図**6-59** ビューの追加



□□□ 各フィールドを定義します。

□□□ Apply Changes （変更の適用）をクリックします。

SNTP ビューが追加され、デバイスがアップデートされます。

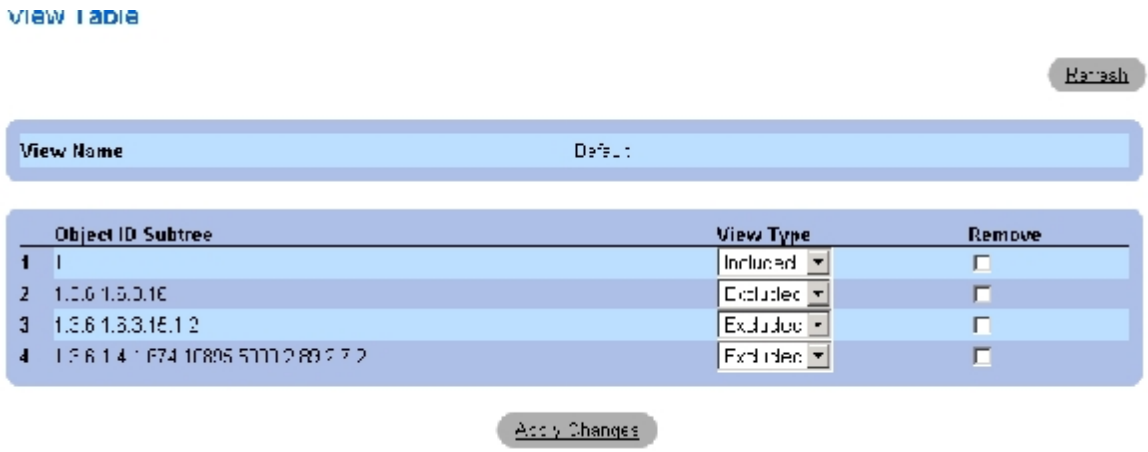
ビュー表の表示

□□□ **SNMPv3** ビューの設定 ページを開きます。

□□□ Show All （すべてを表示）をクリックします。

ビュー表ページが開きます。

図**6-60** ビュー表



CLI コマンドを使用した **SNMPv3** ビューの定義

SNMPv3 ビューの設定ページ内の各フィールド設定操作と等価な処理を実行する **CLI** コマンドを以下の表に示します。

表**6-38 SNMP** ビュー **CLI** コマンド

CLI	

コマンド	説明
snmp-server view *view-name oid-tree* {**included** | **excluded**}	ビューエントリの生成または更新を行います。
show snmp views [*viewname*]	ビュー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)# snmp-server view user1
1 included

Console(config)# end

Console# show snmp views
```

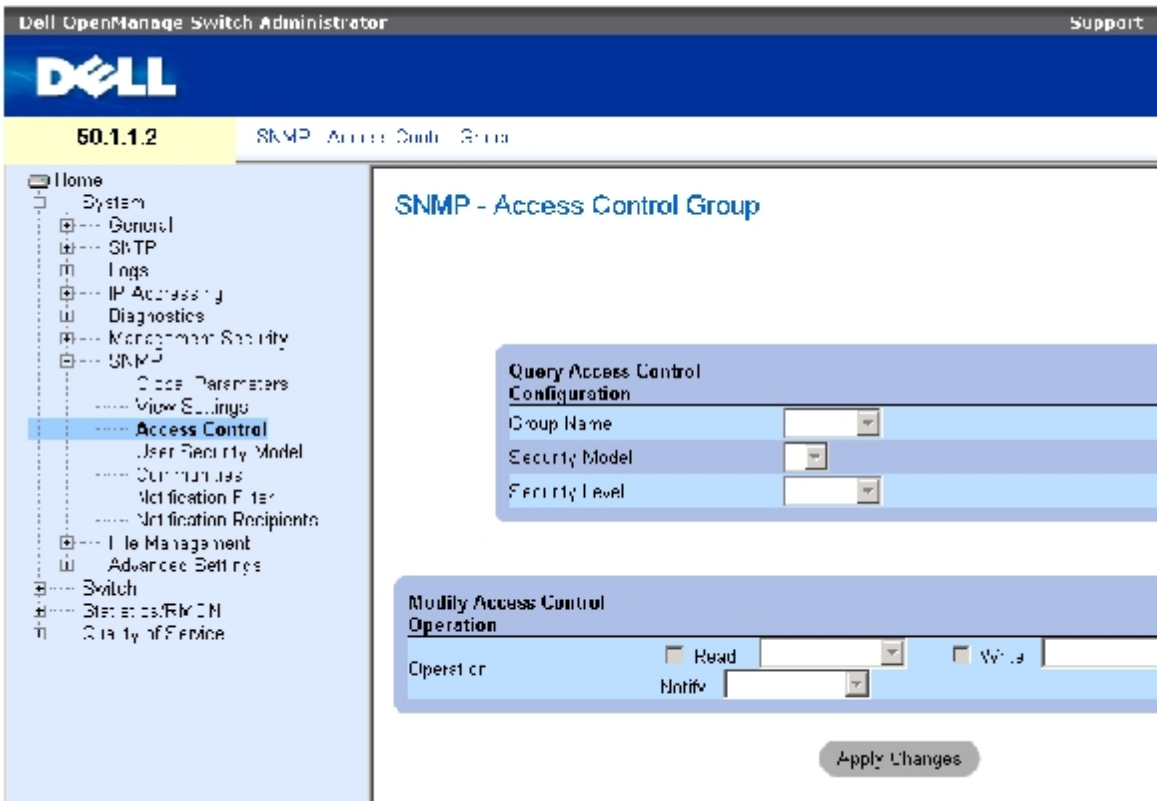
Name	OID Tree	Type
----------	----------	-------
user1	iso	included
Default	iso	included
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

SNMP アクセスコントロールの定義

アクセスコントロールページには、SNMP グループの生成や、SNMP グループへの SNMP アクセスコントロールの割り当てに必要な情報が表示されます。グループによってネットワーク管理者は、特定のデバイス機能、または機能アスペクトにアクセス権を割り当てることが可能です。

アクセスコントロールグループページを開くには、ツリービューからSystem （システム）→ SNMP （SNMP）→ Access Control （アクセスコントロール）をクリックします。

図**6-61** アクセスコントロールグループ



アクセスコントロールグループページは以下のフィールドで構成されています。

Group Name （グループ名）— アクセスコントロールルールが適用されるユーザー定義グループです。フィールド値は最大で 30 文字です。

SNMP Version （SNMP バージョン）— グループに付属するSNMPバージョンを定義します。可能なフィールド値は以下のとおりです。

SNMPv1 （SNMPv1）— グループに SNMPv1 が定義されます。

SNMPv2 （SNMPv2）— グループに SNMPv2 が定義されます。

SNMPv3 （SNMPv3）— グループに SNMPv3 が定義されます。

Security Level （セキュリティレベル）— グループに付属するセキュリティレベルです。セキュリティレベルは SNMPv3 にのみ適用されます。可能なフィールド値は以下のとおりです。

No Authentication （認証なし）— グループには認証もプライバシーセキュリティレベルも割り当てられていません。

Authentication （認証）— SNMP メッセージを認証し、また、SNMP メッセージの発信源が認証されていることを保証します。

Privacy （プライバシー）— SNMP メッセージを暗号化します。

Operation （動作）— グループアクセス権を定義します。可能なフィールド値は以下のとおりです。

Read （リード） — 管理アクセスはリードオンリーに制限され、割り当てられている SNMP ビューを変更することはできません。

Write （ライト） — 管理アクセスはリードライトが可能で、割り当てられている SNMP ビューを変更することが可能です。

Notify （通知）— 割り当てられている SNMP ビューにトラップを送信します。

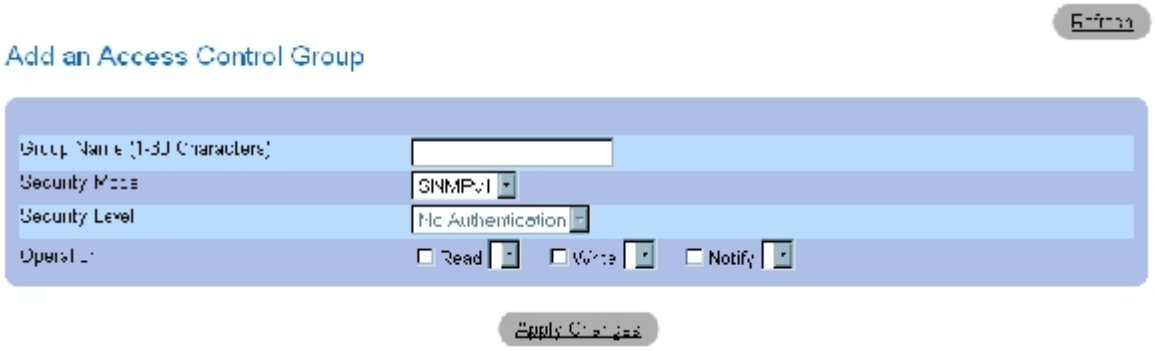
SNMP グループの定義

□□□ アクセスコントロールグループページを開きます。

□□□ **Add** （追加）をクリックします。

アクセスプロファイルの追加ページが開きます。

図**6-62** アクセスコントロールグループの追加



□□□ アクセスコントロールグループの追加ページ内の各フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

グループが追加され、デバイスがアップデートされます。

アクセス表の表示

□□□ アクセスコントロールグループページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

アクセス表が開きます。

図**6-63** アクセス表

SNMP グループの削除

□□□ アクセスコントロールグループページを開きます。

□□□ Show All （すべてを表示）をクリックします。

アクセス表が開きます。

□□□ SNMP グループを 1 つ選択します。

□□□ Remove （削除）チェックボックスをチェックします。

□□□ Apply Changes （変更の適用）をクリックします。

SNMP 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 SNMP アクセスコントロールの定義

アクセスコントロールグループページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-39 SNMP** アクセスコントロール **CLI** コマンド

CLI コマンド	説明
snmp-server group *groupname* **{v1 | v2 | v3 {noauth | auth | priv}} [read** *readview***] [write** *writeview***] [notify** *notifyview* **]**	新しい Simple Network Management Protocol（SNMP）グループの設定か、SNMP ユーザーを SNMP ビューにマッピングする表を設定します。
show snmp groups [*groupname*]	グループの設定を表示します。

以下に CLI コマンドの例を示します。

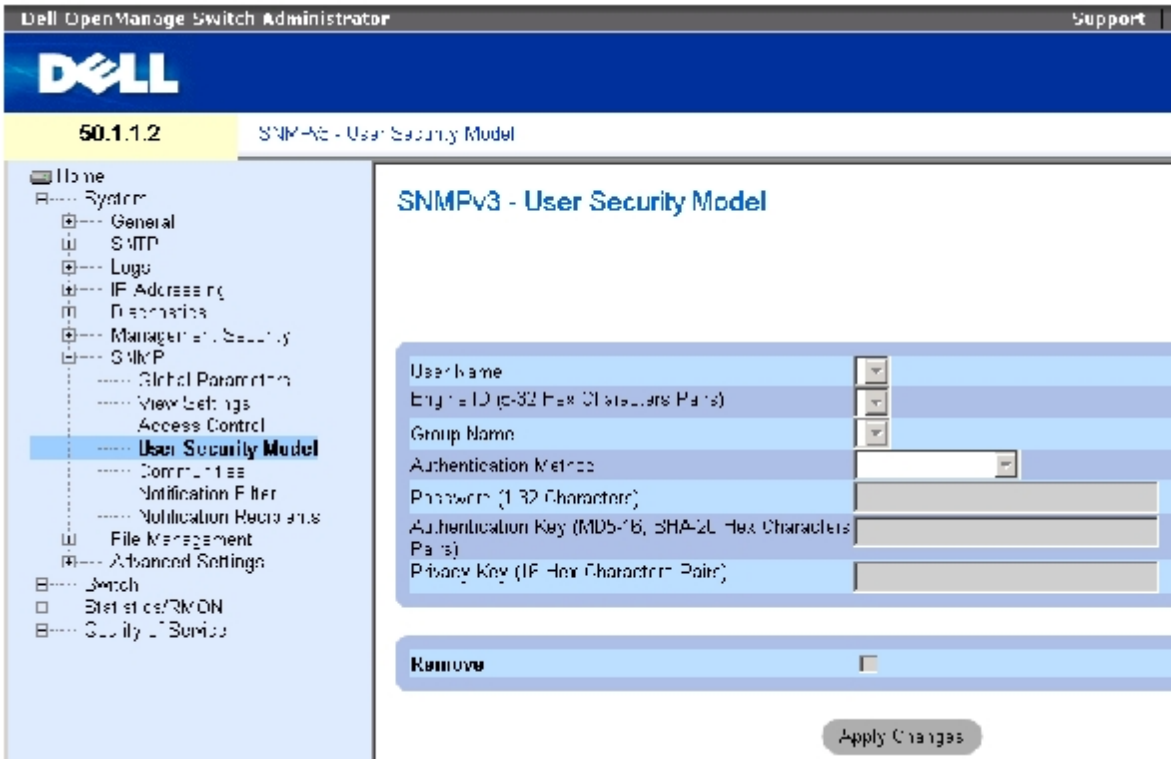
```
console (config)# snmp-
server group user-group
v3 priv read user- view
```

SNMP ユーザーセキュリティの割り当て

SNMPv3ユーザーセキュリティモデル（**USM**）ページから、システムユーザーの SNMP グループへの割り当てと、ユーザー認証方法が可能です。

SNMPv3ユーザーセキュリティモデル（**USM**）ページを開くには、ツリービューから、**System** （システム）→ **SNMP** （SNMP）→ **User Security Model** （ユーザーセキュリティモデル）をクリックします。

図**6-64 SNMPv3**ユーザーセキュリティモデル（**USM**）



SNMPv3ユーザーセキュリティモデル（**USM**） ページは以下のフィールドで構成されます。

User Name （ユーザー名称） — ユーザー定義のユーザー名リストで構成されます。フィールド値は最大で英数字 30 文字です。

Engine ID （エンジン ID）— ユーザーが接続している相手がローカルかリモートの SNMP エンティティであることを示します。ローカル SNMP エンジン ID の変更または削除を行うと、SNMPv3 ユーザーデータベースが削除されます。

Local （ローカル）— ユーザーがローカル SNMP エンティティに接続されていることを示します。

Remote （リモート）— ユーザーがリモート SNMP エンティティに接続されていることを示します。エンジン ID を定義すると、リモートデバイスは通知メッセージを受信します。

Group Name （グループ名称） — ユーザー定義の SNMP グループリストで構成されます。SNMP グループはアクセスコントロールグループページ内で定義されます。

Authentication Method （認証方法）— 認証ユーザーに使用される認証方法です。可能なフィールド値は以下のとおりです。

MD5 （MD5）キー— ユーザーは HMAC-MD5 アルゴリズムを使用して認証されます。

SHA （SHA）キー— ユーザーは HMAC-SHA-96 認証レベルを使用して認証されます。

MD5Password （MD5 パスワード）— HMAC-MD5-96 パスワードが認証に使用されることを示します。ユーザーはパスワード入力が必要です。

SHA Password （SHA パスワード）キー— ユーザーは HMAC-SHA-96 認証レベルを使用して認証されます。ユーザーはパスワード入力が必要です。

None （なし）— ユーザー認証は使用されません。

Password （0～32 文字）（パスワード）— グループ用のユーザー定義パスワードを変更します。パスワードは最大英数 32 文字です。

Authentication Key（**MD5-16; SHA-20 16** 進文字）（認証キー）— HMAC-MD5-96 または HMAC-SHA-96 認証レベルを定義します。認証キーを定義するために、認証とプライバシーキーを入力します。認証のみが必要な場合、MD5 には 16 バイトが定義されます。プライバシーと認証の両方が必要な場合、MD5 には 32 バイトが定義されます。16 進文字ストリングの各バイトは 16 進 2 桁です。各バイトはピリオドまたはコロンで区切ることが可能です。

Privacy Key（**16** 進文字 **x16**）（プライバシーキー）— 認証のみが必要な場合は 20 バイトを定義します。プライバシーと認証の両方が必要な場合は 16 バイトを定義します。16 進文字ストリングの各バイトは 16 進 2 桁です。各バイトはピリオドまたはコロンで区切ることが可能です。

Remove （削除）— チェックを入れることで、指定グループからユーザーを削除します。

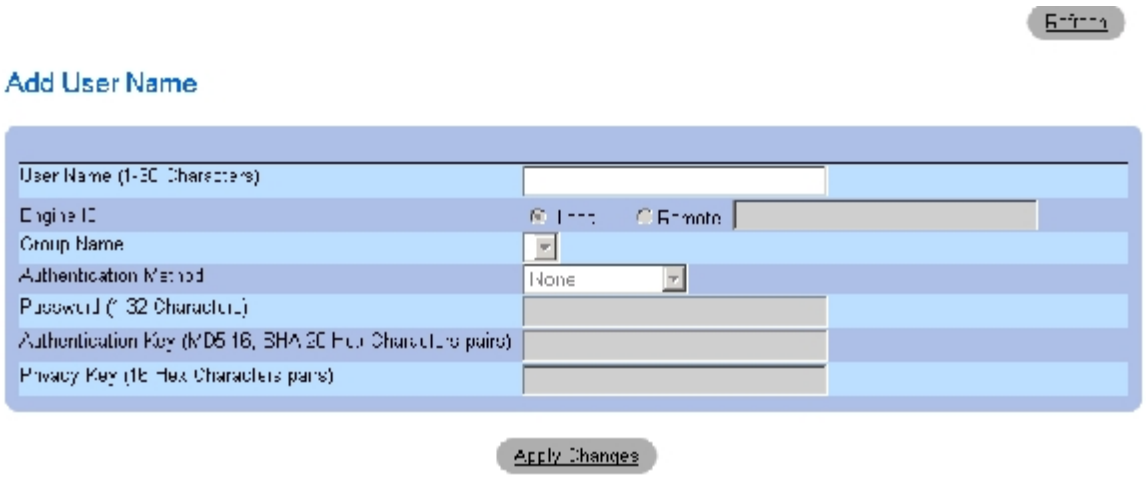
グループへのユーザー追加

□□□ SNMPv3ユーザーセキュリティモデル（USM） ページを開きます。

□□□ Add （追加）をクリックします。

SNMPv3 ユーザー名の追加 ページが開きます。

図**6-65 SNMPv3** ユーザー名の追加



□□□ 各関連フィールドを定義します。

□□□ Apply Changes （変更の適用）をクリックします。

ユーザーがグループに追加され、デバイスがアップデートされます。

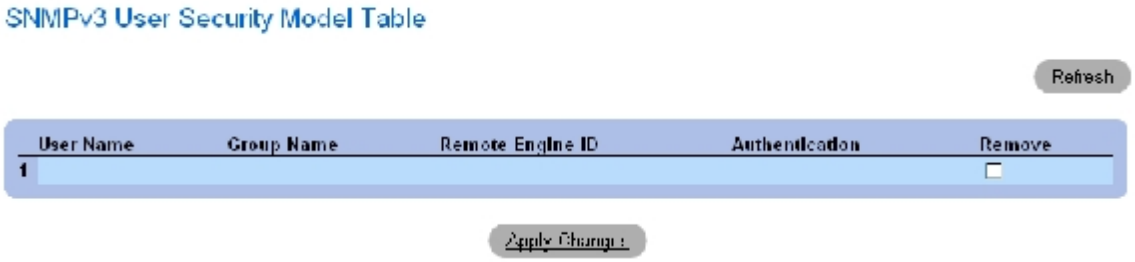
ユーザーセキュリティモデル表の表示

□□□ **SNMPv3**ユーザーセキュリティモデル（**USM**） ページを開きます。

□□□ Show All （すべてを表示）をクリックします。

ユーザーセキュリティモデル表が開きます。

図**6-66** ユーザーセキュリティモデル表



ユーザーセキュリティモデル表エントリの削除

□□□ **SNMPv3**ユーザーセキュリティモデル（**USM**）ページを開きます。

□□□ Show All （すべてを表示）をクリックします。

ユーザーセキュリティモデル表が開きます。

□□□ ユーザーセキュリティモデル表のエントリを 1 つ選択します。

□□□ **Remove** （削除）チェックボックスをチェックします。

□□□ Apply Changes （変更の適用）をクリックします。

選択したユーザーセキュリティモデル表の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 SNMPv3 ユーザーの定義

SNMPv3ユーザーセキュリティモデル（**USM**）ページ内の各フィールド設定操作と等価な処理を実行するCLI コマンドを以下の表に示します。

表**6-40 SNMPv3** ユーザー **CLI** コマンド

CLI コマンド	説明
snmp-server user *username groupname* [**remote** engineid- string][**auth-md5** password | **auth-sha password** | **auth- md5-key** *md5-des-key* | **auth- sha-key** *sha-des-key*]	新規 SNMP V3 ユーザーを設定します。
show snmp users [*username*]	ユーザーの設定を表示します。

以下に CLI コマンドの例を示します。

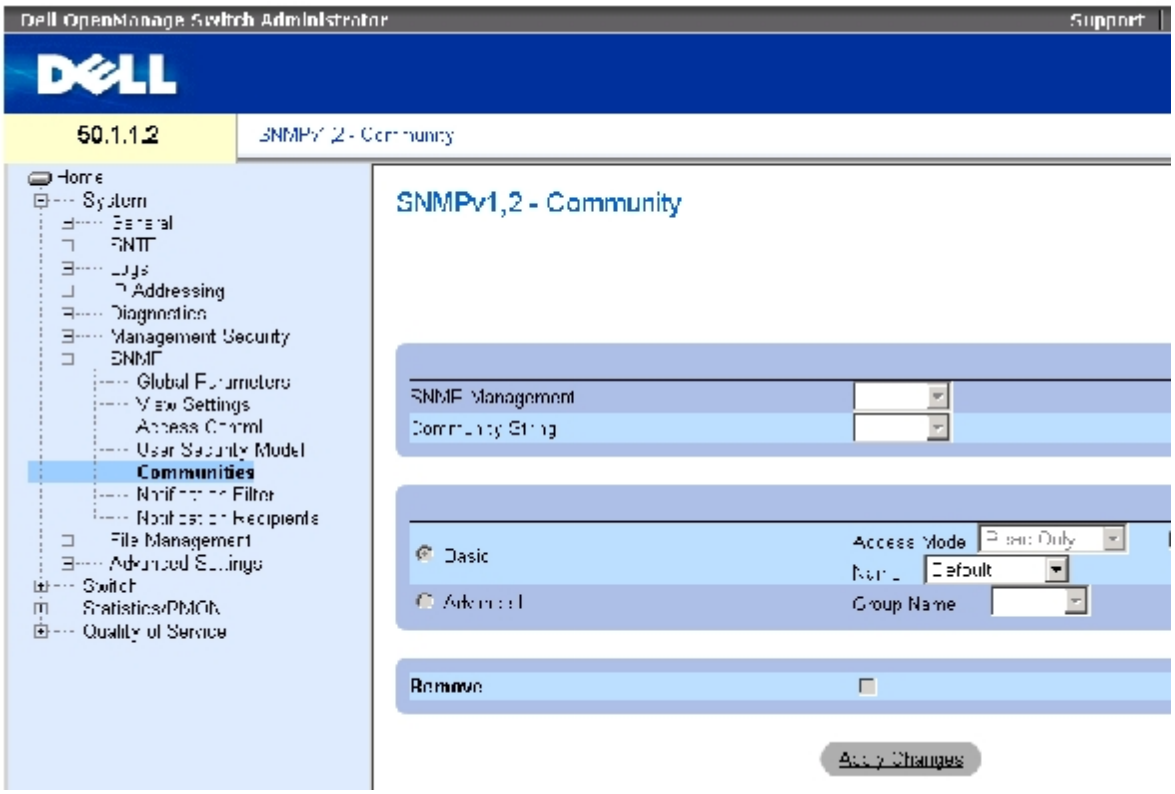
```
console (config)# snmp-server user John user-group auth-md5 1234

console (config)# end

console# show snmp users
```

Name	Group Name	Auth Method	Remote
John	user-group	md5	

SNMP コミュニティの定義

SNMPv1,2 コミュニティページ上でコミュニティを定義することでアクセス権を管理します。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 コミュニティは SNMPv1 と SNMPv2 のみ定義されます。**SNMPv1,2 コミュニティ**ページを開くには、ツリービューから **System** （システム）→ **SNMP** （SNMP）→ **Communities** （コミュニティ）をクリックします。

図**6-67 SNMPv1,2** コミュニティ



SNMPv1,2 コミュニティページは以下のフィールドで構成されます。

SNMP Management Station（SNMP 管理ステーション）— SNMP コミュニティを定義する管理ステーションの IP アドレスです。

Community String （コミュニティストリング）— パスワードとして機能し、管理ステーションをデバイスに対して認証するために使用します。

Basic （ベーシック）— 選択したコミュニティの SNMP ベーシックモードを有効にします。可能なフィールド値は以下のとおりです。

Access Mode （アクセスモード）— 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は以下のとおりです。

Read Only （リードオンリー）— 管理アクセスはリードオンリーに制限され、コミュニティを変更することはできません。

Read Write （リードライト） — 管理アクセス権はリードライトで、デバイス設定の変更は可能ですが、コミュニティの変更はできません。

SNMP Admin （SNMP 管理者） — 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を持ち、また、コミュニティ変更が許されています。

View Name （ビュー名称） — ユーザー定義の SNMP ビューリストで構成されます。

Name （名称） — SNMPv1, v2で使用するコミュニティ名を指定します。

Advanced （アドバンスト） — ユーザー定義のグループリストで構成されます。SNMP アドバンストモードを選択すると、選択したコミュニティに対して、グループを構成する SNMP アクセスコントロールルールが有効になります。また、アドバンストモードは、特定の SNMP コミュニティの SNMP グループを有効にします。SNMP アドバンストモードは SNMPv3 のみで定義します。設定可能なフィールド値は次のとおりです。

Group Name （グループ名） — SNMP アドバンストモードで動作する際のグループ名を指定します。

Remove （削除） — 選択によって、コミュニティを削除します。

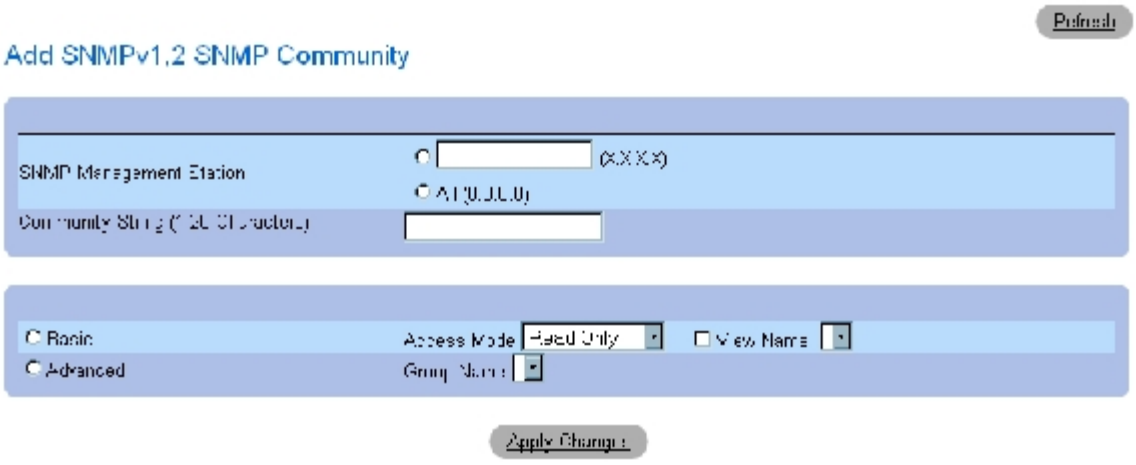
新規コミュニティの定義

□□□ SNMPv1,2 コミュニティページを開きます。

□□□ **Add** （追加）をクリックします。

SNMP コミュニティの追加 ページが開きます。

図**6-68 SNMP** コミュニティの追加



□□□ 各関連フィールドを定義します。

□□□ **Apply Changes** （変更の適用）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。

コミュニティの削除

□□□ **SNMPv1,2** コミュニティページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

コミュニティ表ページが開きます。

□□□ コミュニティの 1 つを選択し、**Remove** （削除）チェックボックスにチェックを入れ ます。

□□□ **Apply Changes** （変更の適用）をクリックします。

指定した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

SNMPv1,2 コミュニティページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-41 SNMP** コミュニティ **CLI** コマンド

CLI コマンド	説明
snmp-server community *community* [**ro** | **rw** | **su**] [*ip-address*][**view** *view-name*]	コミュニティアクセスストリングを設定して SNMP プロトコルへのアクセスを許可します。
snmp-server community-group *community group-name* [*ip-address*]	コミュニティアクセスストリングを設定して、グループアクセス権に基づいて、SNMP プロトコルへ限定アクセスを許可します。
show snmp	現在の SNMP デバイス設定を表示します。

以下に CLI コマンドの例を示します。

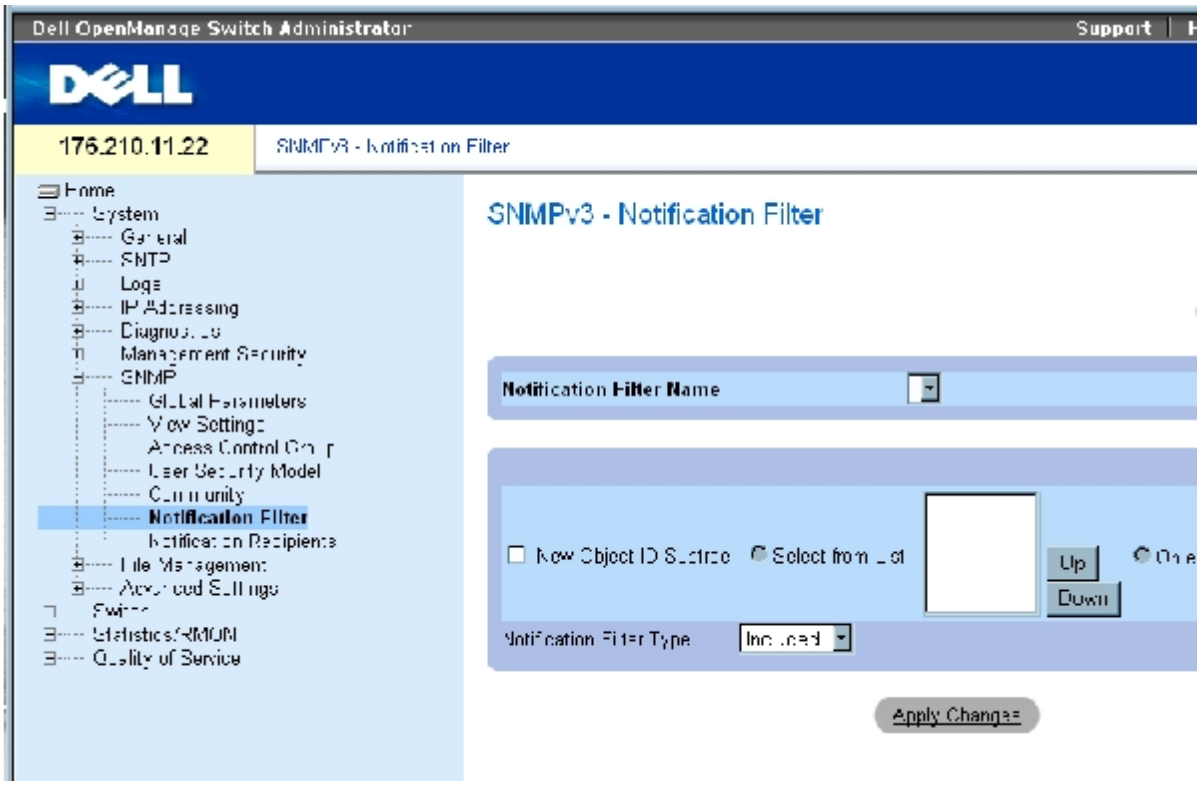
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

SNMP 通知フィルタの定義

通知フィルタページで、OID に基づくフィルタトラップが可能です。各OID は、デバイス機能または機能アスペクトにリンクされています。また、通知フィルタページは、ネットワーク管理者にフィルタ通知を許可します。

通知フィルタページを開くには、ツリービューから、**System** （システム）→ **SNMP** （SNMP）→ **Notification Filters** （通知フィルタ）をクリックします。

図**6-69** 通知フィルタ



通知フィルタページは以下のフィールドで構成されています。

Notification Filter Name （通知フィルタ名）— ユーザー定義の通知フィルタです。

New Object Identifier Tree （新規オブジェクト識別子ツリー）— 通知が送信または遮断される OID です。フィルタが OID に付属しているとき、トラップまたは通知が生成されてトラップ受領者に送信されます。オブジェクト ID は、*Select from List* （選択リスト）または *Object ID List* （オブジェクト ID リスト）のいずれかから選択します。

Notification Filter Type （通知フィルタタイプ）—トラップ受領者に対して、OID に関し通知またはトラップを送信するかどうかを示します。

Excluded （除外）— OID トラップまたは通知の送信を制限します。

Included （包含）— OID トラップまたは通知を送信します。

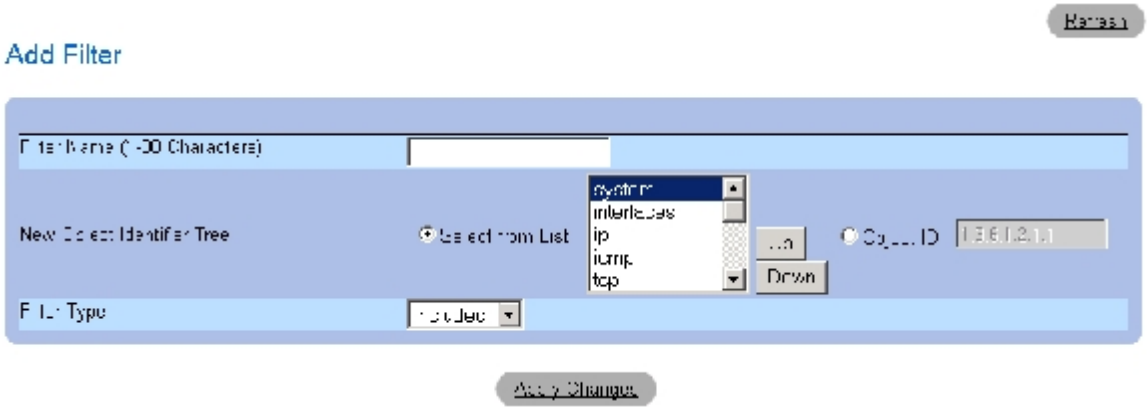
SNMP フィルタの追加

□□□ 通知フィルタページを開きます。

□□□ **Add** （追加）をクリックします。

フィルタの追加ページが開きます。

図**6-70** フィルタの追加



□□□ 各関連フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

新しいフィルタが追加され、デバイスがアップデートされます。

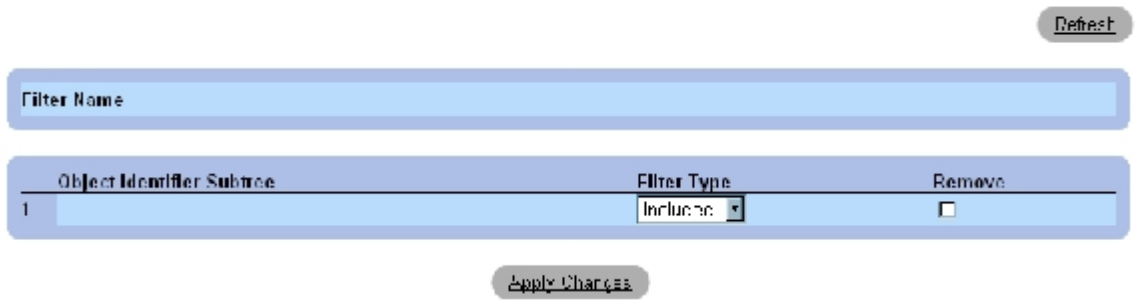
フィルタ表の表示

□□□ 通知フィルタページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

フィルタ表が開きます。

図**6-71** フィルタ表



フィルタの削除

□□□ 通知フィルタページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

フィルタ表が開きます。

□□□ フィルタ表のエントリを **1** つ選択します。

□□□ **Remove**（削除）チェックボックスをチェックします。

選択したフィルタ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通知フィルタの設定

通知フィルタページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-42 SNMP** 通知フィルタ **CLI** コマンド

CLI コマンド	説明
snmp-server filter filter-name oid-tree {**included** | **excluded**}	SNMP 通知フィルタを作成または更新します。
show snmp filters [filtername]	SNMP 通知フィルタ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)# snmp-server filter user1 iso included

Console(config)# end

Console # show snmp filters

Name            OID Tree          Type
-----------     -------------     --------
user1           iso               Included
```

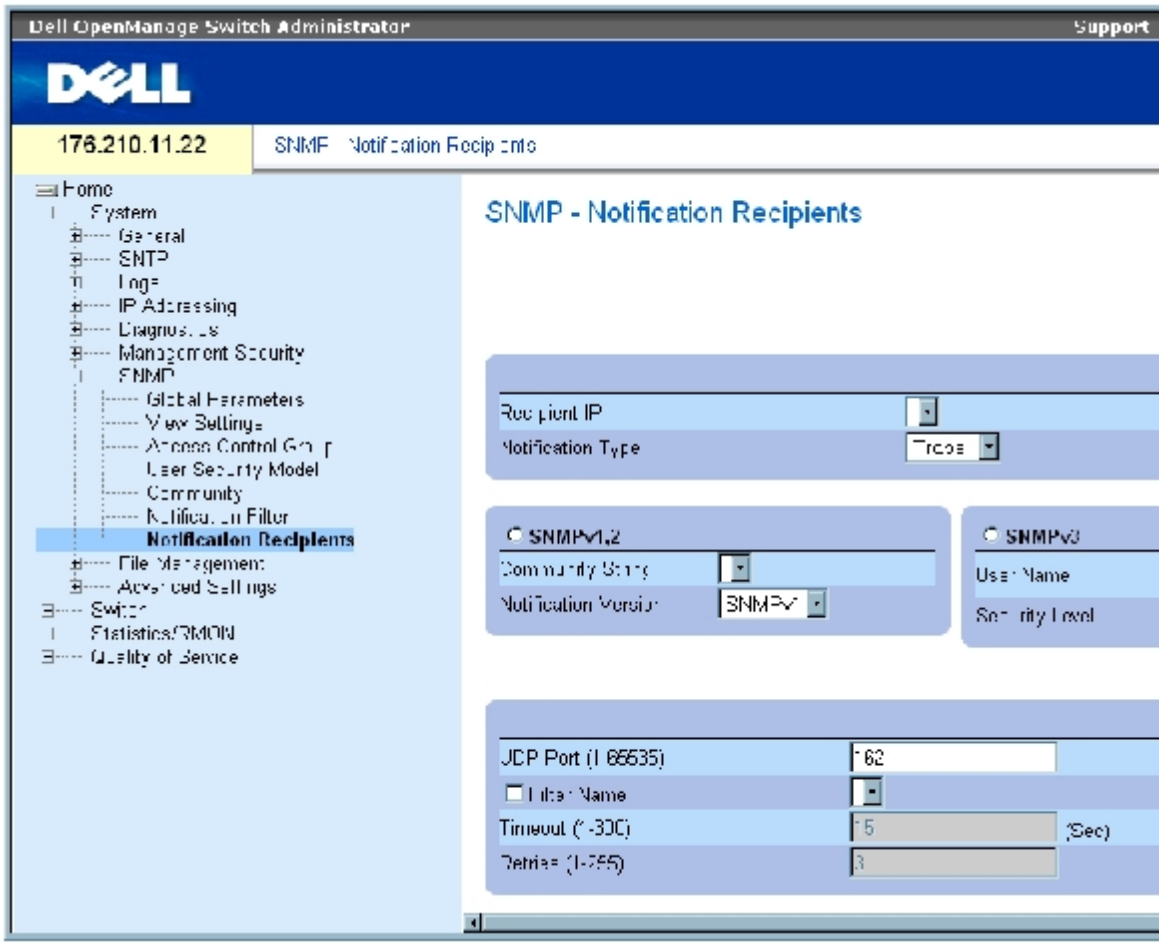
SNMP 通知受領者の定義

通知受領者 ページには、トラップとトラップタイプを特定ユーザーに送信するかどうかを決めるフィルタの定義情報が表示されます。SNMP 通知フィルタは次のサービスを提供します。

- 管理トラップターゲットの特定
- トラップのフィルタ
- トラップ生成パラメータの選択
- アクセスコントロールチェックの提供

通知受領者ページを開くには、ツリービューから**System** （システム）→ **SNMP** （SNMP）→ **Notification Recipient** （通知受領者）をクリックします。

図**6-72** 通知受領者



通知受領者 ページは以下のフィールドで構成されています。

Recipient IP （受領者 IP） — トラップ送信先の IP アドレスを示します。

Notification Type （通知タイプ） — 送信される通知です。可能なフィールド値は以下のとおりです。

Trap （トラップ） — トラップが送信されます。

Inform （通知） — 通知が送信されます。

SNMPv1,2 （SNMPv1,2） — 選択した受領者の SNMP バージョン 1 と 2 を有効にします。SNMPv1 と SNMPv2 の以下のフィールドを定義してください。

Community String（**1**～**20** 文字）（コミュニティストリング） — 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。

Notification Version （通知バージョン） — トラップタイプを決定します。可能なフィールド値は以下のとおりです。

SNMP V1 （SNMP V1） — SNMP Version 1 トラップが送信されます。

SNMP V2 （SNMP V2） — SNMP Version 2 トラップが送信されます。

SNMPv3 （SNMPv3） — SNMPv3 はトラップの送受信に使用されます。SNMPv3 の以下のフィールドを定義してください。

User Name （ユーザー名） — SNMP 通知が送信されるユーザーです。

Security Level （セキュリティレベル）— パケットを認証する手段を定義します。可能なフィールド値は以下のとおりです。

No Authentication （認証なし）Å\ パケットは認証も暗号化もされません。

Authentication （認証）— パケットは認証されます。

Privacy （プライバシー）— パケットは認証および暗号化されます。

UDP Port（1～65535）（UDP ポート）— 通知送信に使用されるUDPポートです。デフォルトは 162 です。

Filter Name （フィルタ名）— SNMP フィルタを包含または除外します。

Timeout（1～300） （タイムアウト）— 通知を再送信する前にデバイスが待つ時間（秒）です。デフォルトは 15 秒です。

Retries（1～255） （リトライ）— 通知要求をデバイスが再送信する回数です。デフォルトは 3 です。

Remove Notification Recipient （通知受領者の削除）— チェックを入れることで、選択した通知受領者を削除します。

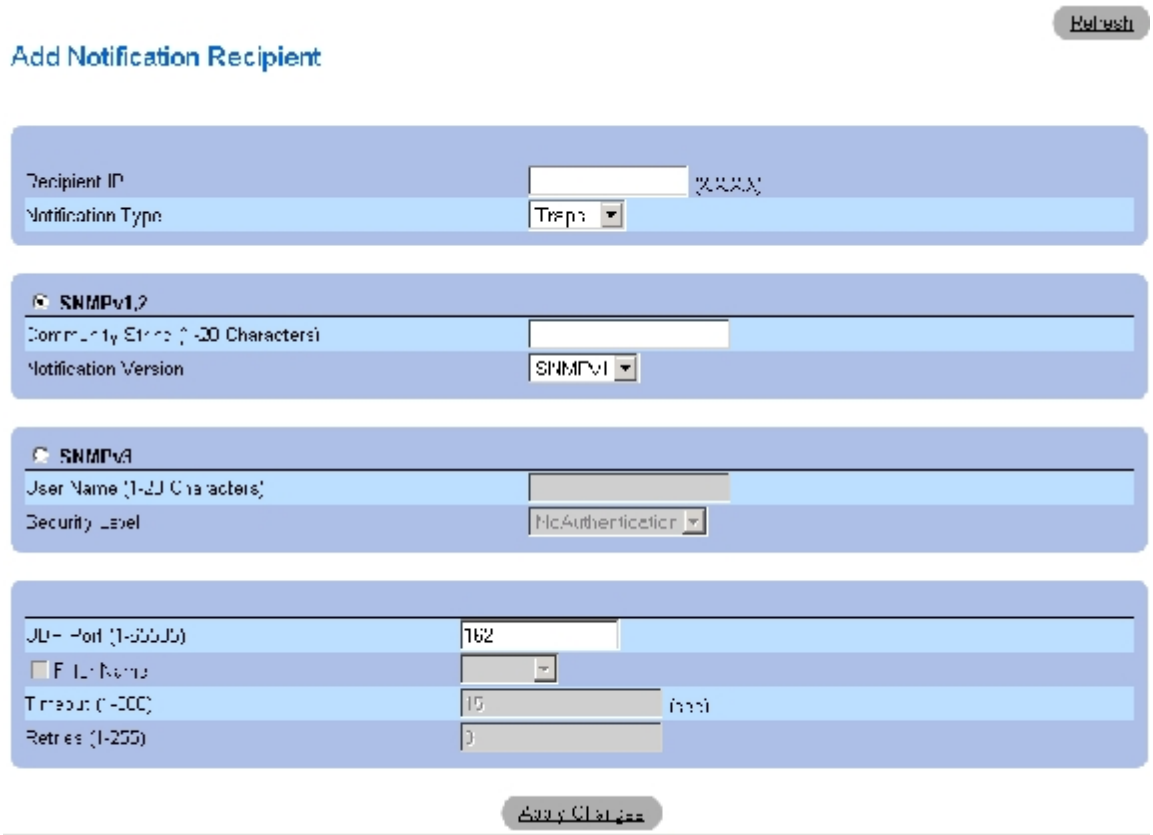
新規トラップ受領者の追加

□□□ 通知受領者 ページを開きます。

□□□ Add （追加）をクリックします。

通知受領者の追加ページが開きます。

図**6-73** 通知受領者の追加



□□□ 各関連フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

通知受領者が追加され、デバイスがアップデートされます。

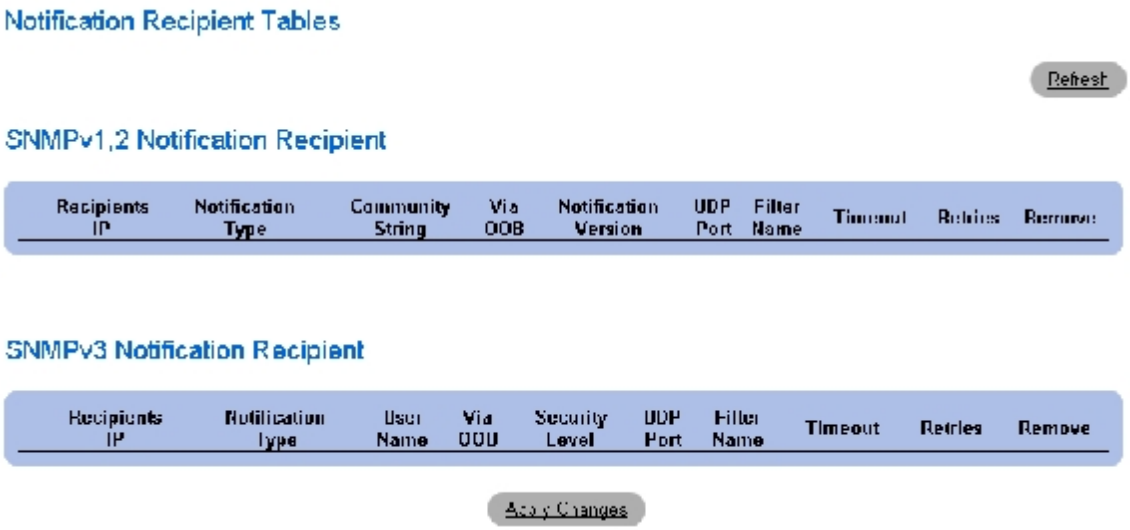
通知受領者表の表示

□□□ 通知受領者 ページを開きます。

□□□ **Show All** （すべてを表示）をクリックします。

通知受領者表 ページが開きます。

図**6-74** 通知受領者表



通知受領者の削除

□□□ 通知受領者 ページを開きます。

□□□ Show All （すべてを表示）をクリックします。

通知受領者表ページが開きます。

□□□ 通知受領者を、**SNMPV1,2 Notification Recipient** （SNMPv1,2 の通知受領者）か **SNMPv3 Notification Recipient Tables** （SNMPv3 の通知受領者表）のいずれかから選択 します。

□□□ **Remove** （削除）チェックボックスをチェックします。

□□□ Apply Changes （変更の適用）をクリックします。

選択した受領者が削除され、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 SNMP 通知受領者の設定

通知受領者ページ内の各フィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-43 SNMP** コミュニティ **CLI** コマンド

CLI コマンド	説明
snmp-server host {ipaddress | hostname} *community-string* [**traps** | **informs**] [**1** | **2**] [**udp-port** port] [**filter** filtername] [**timeout** seconds] [**retries** retries]	SNMP バージョン 1 または 2 で通知を受信する通知受領者の作成または更新を行います。
snmp-server v3-host {ip-address | hostname} *username* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *port*] [**filter** filtername] [**timeout** seconds] [**retries** retries]	SNMP バージョン 3 で通知を受信する通知受領者の作成または更新を行います。
show snmp	現在の SNMP 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)# snmp-server host 172.16.1.1 private

console(config)# end

console# show snmp
```

Community-String	Community-Access	View name	IP address
public	read only	user-view	All
private	read write	default	172.16.1.1
private	su	DefaultSuper	172.17.1.1

ファイルの管理

ファイルの管理 ページで、デバイスソフトウェア、イメージファイル、および設定ファイルの管理を行います。ファイルは TFTP サーバーとの間でダウンロードまたはアップロードが可能です。

ファイル管理の概要

管理ファイル構造は以下のファイルで構成されています。

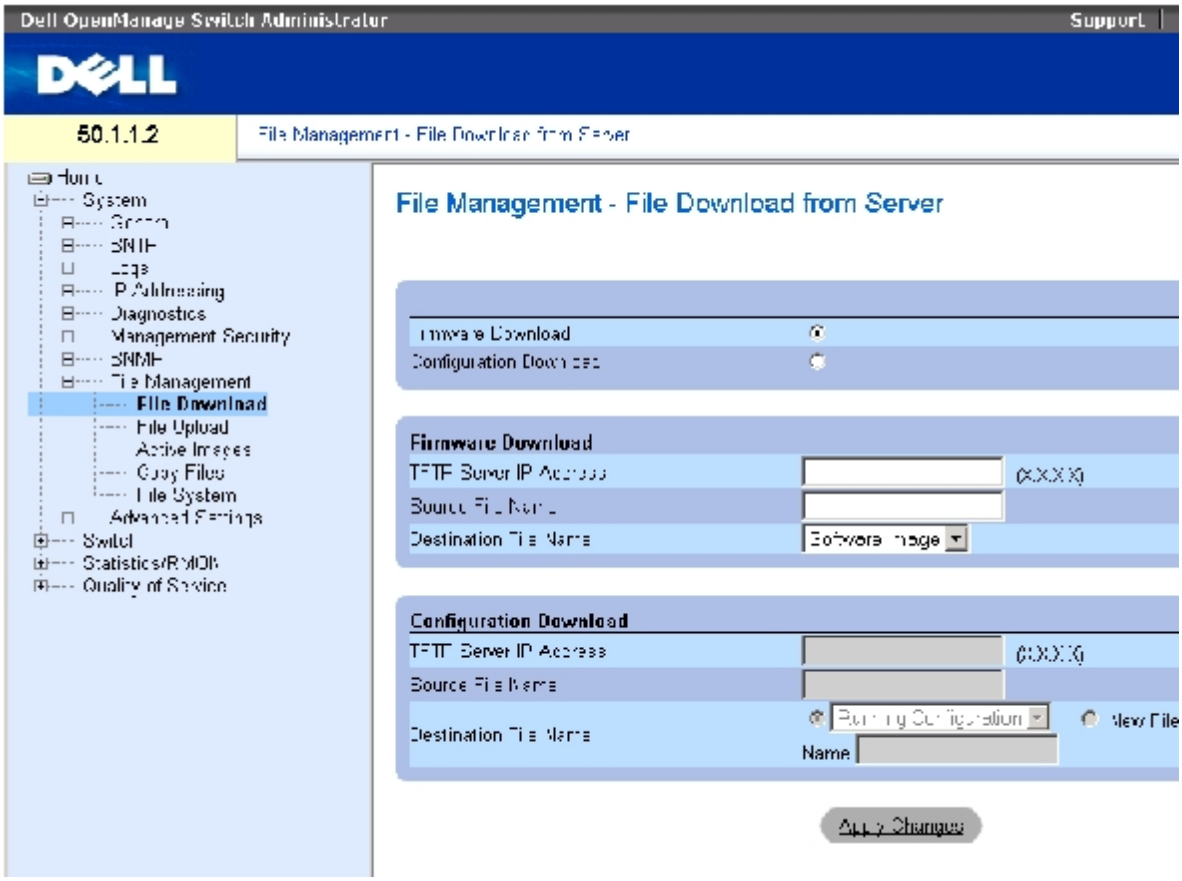
- Startup Configuration File （スタートアップ設定ファイル） — 起動時または再起動後にデバイスの設定に必要なコマンドで構成されています。スタートアップ設定ファイルは、動作中設定ファイルまたはバックアップ設定ファイルから、設定コマンドをスタートアップ設定ファイルにコピーして作成します。
- Running Configuration File（動作中設定ファイル） — すべてのスタートアップ設定ファイルコマンド、および現在のセッション中に入力されたコマンドをすべて含みます。デバイスの電源を切断した場合、あるいはデバイスを再起動した場合、動作中設定ファイルに保存されていたすべてのコマンドは失われます。スタートアップ処理中に、スタートアップ設定ファイル内のすべてのコマンド動作中設定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動作中設定ファイルの既存コマンドに追加されます。スタートアップ設定ファイルを更新するには、デバイスの電源を切る前に、動作中設定ファイルをスタートアップ設定ファイルにコピーする必要があります。
- Backup Configuration File（バックアップ設定ファイル） — デバイス設定のバックアップコピーが含まれています。ユーザー設定名を使用して、デバイスに最大で 5 件のバックアップ設定ファイルを保存することが可能です。これらバックアップファイルは、ユーザーが動作中設定ファイルかスタートアップ設定ファイルをユーザー名ファイルにコピーしたときに生成されます。バックアップ設定ファイルの内容は、動作中設定ファイル、またはスタートアップ設定ファイルのいずれかにコピーできます。
- Image Files （イメージファイル） — システムファイルイメージは、Image 1 と Image 2 として、2つの Flash ファイルに保存されます。アクティブイメージはアクティブコピーに保存され、他方のイメージは第 2 コピーに保存されます。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、システムは自動的に非アクティブイメージから起動します。以上はソフトウェアのアップグレード処理中に発生する障害に備えた安全機能です。

ファイルの管理ページを開くには、ツリービューから System （システム）→ File Management （ファイルの管理）をクリックします。

ファイルのダウンロード

サーバーからのファイルダウンロードページは、システムイメージや設定ファイルを TFTP サーバーからデバイスへダウンロードするフィールドで構成されています。サーバーからのファイルダウンロードページを開くには、ツリービューから System （システム）→ File Management （ファイルの管理）→ File Download （ファイルのダウンロード）をクリックします。

図**6-75** サーバーからのファイルダウンロード



サーバーからのファイルダウンロードページは以下のフィールドで構成されています。

Firmware Download（ファームウェアのダウンロード）— ファームウェアファイルをダウンロードします。**Firmware Download** （ファームウェアのダウンロード）が選択された場合、**Configuration Download** （設定のダウンロード）フィールドは薄いグレー表示になります。

Configuration Download （設定のダウンロード）— 設定ファイルをダウンロードします。**Configuration Download** （設定のダウンロード）を選択した場合、**Firmware Download** （ファームウェアのダウンロード）フィールドは薄いグレー表示になります。

ファームウェアのダウンロード

TFTP Server IP Address（TFTP サーバーの IP アドレス）— ファームウェアファイルをダウンロードする TFTP サーバーの IP アドレスです。

Source File Name （ソースファイル名）— ダウンロードするファイル名を示します。

Destination File （保存先ファイル）— ダウンロード後のファイルタイプを指定します。可能なフィールド値は以下のとおりです。

Software Image （ソフトウェアイメージ）— イメージファイルをダウンロードします。

Boot Code （ブートコード）— ブートファイルをダウンロードします。

設定のダウンロード

TFTP Server IP Address （TFTP サーバーの IP アドレス）— 設定ファイルをダウンロードする TFTP サーバーの IP アドレスです。

Source File Name （ソースファイル名）— ダウンロードする設定ファイル名を示します。

Destination File （保存先ファイル）— 設定ファイルをダウンロードした後の保存先ファイルです。可能なフィールド値は以下のとおりです。

Running Configuration （動作中設定）— 動作中設定ファイルにコマンドをダウンロードします。

Startup Configuration （スタートアップ設定）— スタートアップ設定ファイルをダウンロードして、上書きします。

User Defined Backup Configuration （ユーザー定義バックアップ設定）— ユーザー定義のバックアップ設定ファイルをダウンロードして、上書きします。

New File Name （新規ファイル名）— 新しいバックアップ設定ファイルを保存先ファイルとして指定しダウンロードします。

メモ： イメージファイルは非アクティブイメージを上書きします。リセット後に非アクティ ブイメージをアクティブファイルとなるように指定し、ダウンロードに続いてデバイスをリ セットすることを推奨します。

イメージファイルのダウンロード中は、ダウンロードの進行状況を表示するダイアログが開きます.ダウンロードが完了するとウインドウは自動的に閉じます。

ファイルのダウンロード

□□□ サーバーからのファイルダウンロードページを開きます。

□□□ ダウンロードするファイルタイプを定義します。

□□□ フィールドを定義します。

□□□ **Apply Changes** （変更の適用）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： 選択したイメージ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 バイスのリセット方法は、「スタッキングマスターの切り替え」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

サーバーからのファイルダウンロードページ内の各フィールド設定操作と等価な処理を実行するCLI コマンドを以下の表に示します。

表**6-44** ファイルダウンロード **CLI** コマンド

CLI コマンド	説明
copy source-url destination-url	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。

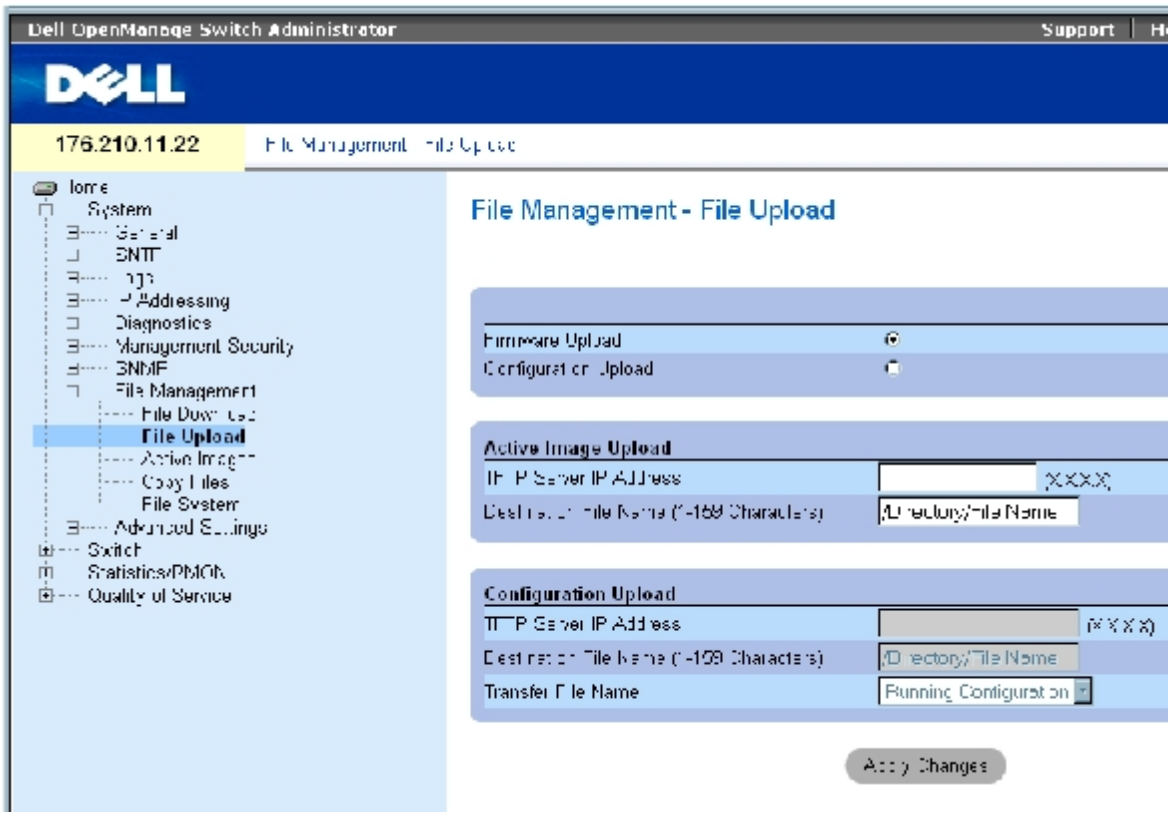
```
console# copy
tftp://10.6.6.64/pp.txt
startup-config


....!


Copy: 575 bytes copied in
00:00:06 [hh:mm:ss]


01-Jan-2000 06:41:55
%COPY-W-TRAP: The copy
operation was completed
successfully
```

メモ： 各 ! マークは、10 個のパケットが正常に転送されたことを示します。

ファイルのアップロード

サーバーへのファイルアップロードページには、デバイスからTFTP サーバーへソフトウェアをアップロードするフィールドが表示されます。また、イメージファイルのアップロードも、サーバーへのファイルアップロードページから行えます。サーバーへのファイルアップロードページを開くには、ツリービューから System （システム）→ File Management （ファイルの管理）→ File Upload （ファイルのアップロード）をクリックします。

図**6-76** サーバーへのファイルアップロード



サーバーへのファイルアップロードページは以下のフィールドで構成されています。

Firmware Upload （ファームウェアのアップロード）— ファームウェアファイルがアップロードされます。**Firmware Upload** （ファームウェアのアップロード）を選択した場合、**Configuration Upload** （設定のアップロード）フィールドは薄いグレー表示に変わります。

Configuration Upload （設定のアップロード）— 設定ファイルがアップロードされます。 **Configuration Upload** （設定のアップロード）を選択した場合、 **Active Image Upload** （アクティブイメージのアップロード）フィールドは利用できません。

アクティブイメージのアップロード

TFTP Server IP Address（TFTP サーバーの IP アドレス）— ソフトウェアイメージがアップロードされる TFTP サーバーの IP アドレスです。

Destination File Name（1～159 文字）（相手先ファイル名）— ファイルがアップロードされるソフトウェアイメージのファイルパスを示します。

設定のアップロード

TFTP Server IP Address（TFTP サーバーの IP アドレス）— 設定ファイルがアップロードされる TFTP サーバーの IP アドレスです。

Destination File Name（1～159 文字）（相手先ファイル名）— ファイルがアップロードされる設定ファイルのパスを示します。

Transfer File Name （転送ファイル名）— 設定がアップロードされるソフトウェアファイルです。可能なフィールド値は以下のとおりです。

Running Configuration （動作中設定）— 動作中設定ファイルをアップロードします。

Startup Configuration （スタートアップ設定）— スタートアップ設定ファイルをアップロードします。

List of User Defined Configuration Files （ユーザー定義ファイルのリスト）— ユーザー定義設定ファイルをアップロードします。

メモ： ユーザー定義設定ファイルのリストは、ユーザーがあらかじめバックアップ設定ファ イルを作成してある場合にのみ、メニューが現れます。たとえば、ユーザーが動作中設定 ファイルを BACKUP-SITE-1 という名称のユーザー定義設定ファイルにコピーした場合、この リストはサーバーへのファイルアップロードページに現れ、BACKUP-SITE-1 がリスト中に表 示されます。

ファイルのアップロード

□□□ サーバーへのファイルアップロードページを開きます。

□□□ アップロードするファイルタイプを定義します。

□□□ 各フィールドを定義します。

□□□ **Apply Changes** （変更の適用）をクリックします。

ソフトウェアが TFTP サーバー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

サーバーへのファイルアップロードページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-45** ファイルアップロード **CLI** コマンド

CLI コマンド	説明

copy source-url destination-url	コピー元からコピー先へファイルをコピーします。

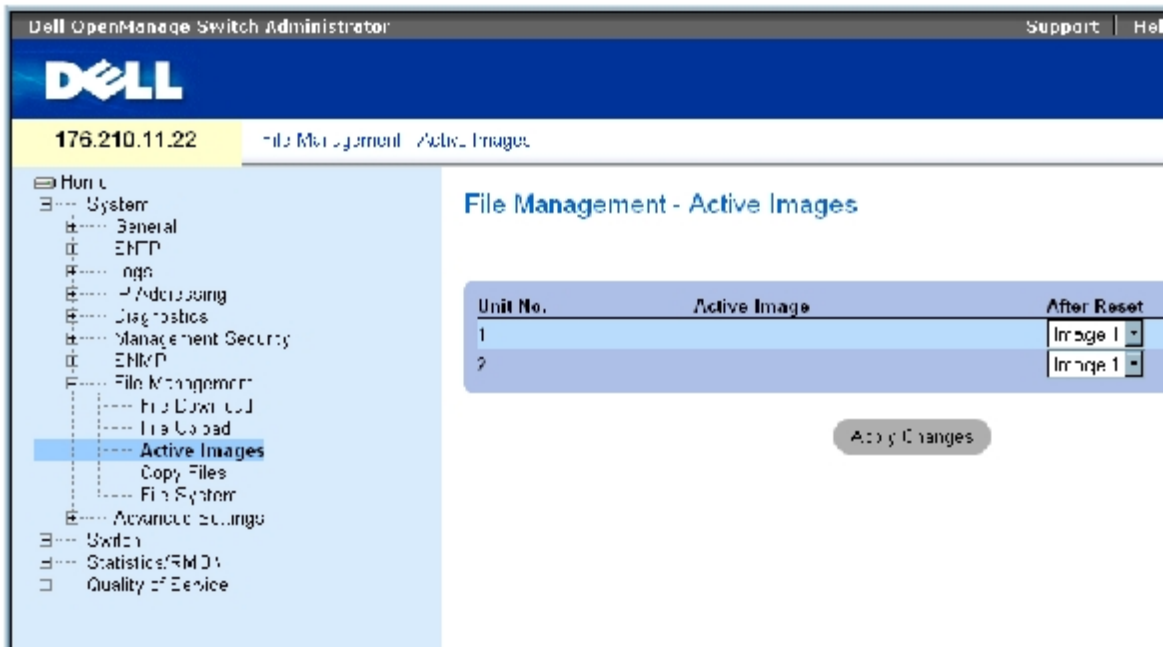
以下に CLI コマンドの例を示します。

```
console# copy image tftp://10.6.6.64/uploaded.ros

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

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

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

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

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

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

Copy: 4234656 bytes copied in 00:00:33 [hh:mm:ss]

01-Jan-2000 07:30:42 %COPY-W-TRAP: The copy operation was
completed successfully
```

イメージファイルのアクティブ化

アクティブイメージ ページでは、イメージファイルの選択とリセットを行います。スタッキング構成内の各ユニットのアクティブイメージファイルは、別々に選ぶことができます。アクティブイメージページを開くには、ツリービューから **System** （システム）→ **File Management** （ファイルの管理）→ **Active Images** （アクティブイメージ）をクリックします。

図**6-77** アクティブイメージ



アクティブイメージ ページは以下のフィールドで構成されています。

Unit No. （ユニット番号）— イメージファイルが選択されているユニット番号です。

Active Image （アクティブイメージ）— ユニット上で現在アクティブなイメージファイルです。

After Reset （リセット後）— デバイスのリセット後にユニット上でアクティブとなるイメージファイルを示します。可能なフィールド値は以下のとおりです。

Image 1 （イメージ 1）— イメージファイル 1 をデバイスのリセット後にアクティブにします。

Image 2 （イメージ 2）— イメージファイル 2 をデバイスのリセット後にアクティブにします。

イメージファイルの選択

□□□ アクティブイメージ ページを開きます。.

□□□ **After Reset**（リセット後）フィールドで、特定のユニットのイメージファイルを選 びます。

□□□ **Apply Changes**（変更の適用）をクリックします。

イメージファイルが選択されます。次回のリセット後にのみ、指定したイメージファイルが再ロードされます。現在選択されているイメージファイルは、次のデバイスリセットまで動作を続けます。

CLI コマンドを使用したアクティブイメージファイルの操作

アクティブイメージページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-46** ファイルアップロード **CLI** コマンド

CLI コマンド	説明
boot system [**unit** | *unit*] {**image-1** | **image-2**}	デバイスがスタートアップ時にロードするシステムイメージを示します。
show version [**unit** *unit*]	システムのバージョン情報を表示します。

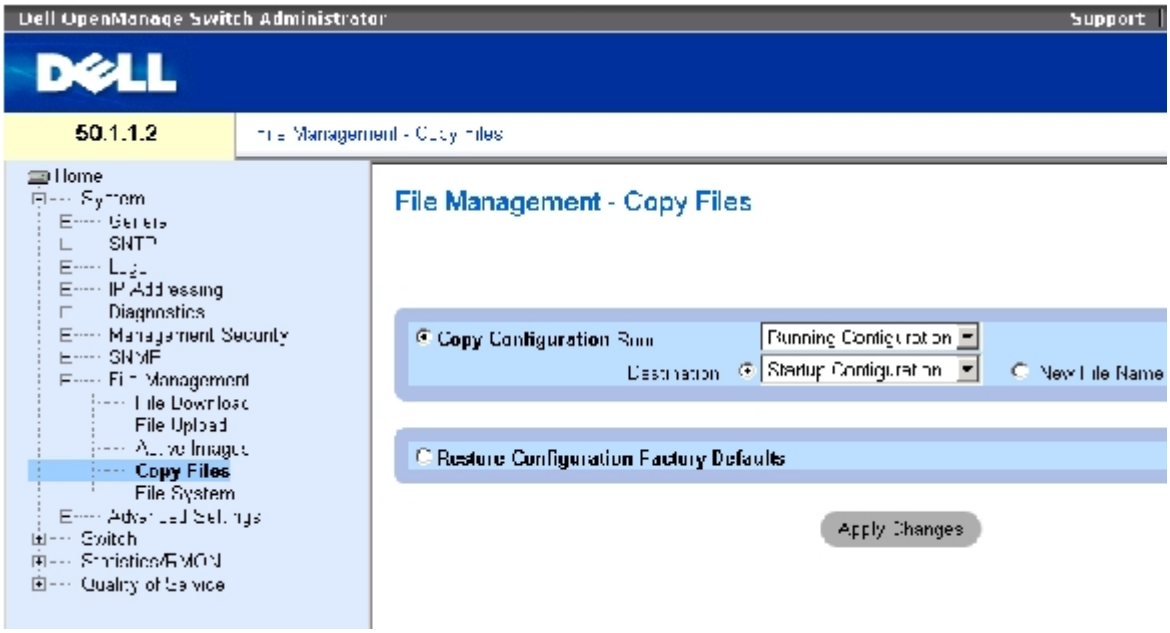
以下に CLI コマンドの例を示します。

```
Console# boot system
image-1
```

ファイルのコピー

ファイルのコピーページから、ファイルのコピーと削除が行えます。ファイルのコピーページを開くには、ツリービューから **System** （システム）→ **File Management** （ファイルの管理）→ **Copy Files** （ファイルのコピー）をクリックします。

図**6-78** ファイルのコピー



ファイルのコピーページは以下のフィールドで構成されています。

Copy Configuration （設定のコピー）— 選択することで、動作中ファイル、スタートアップファイル、またはバックアップのいずれかのマスターファイルを相手先ファイルにコピーします。

Source （ソース）— 相手先ファイルにコピーするファイルのタイプを示します。動作中設定ファイル、スタートアップ設定ファイル、またはユーザー定義のバックアップ設定ファイルの 1 つのいずれかを選択します。

Destination （相手先）— ソースファイルをコピーする相手先設定ファイルを示します。ファイルはバックアップマスターのバックアップファイルにはコピーできません。バックアップファイルが定義されている場合にのみ、**Destination Unit** （相手先ユニット）フィールド内にバックアップファイルが表示されます。New File Name （新規ファイル名）チェックボックスを選択し、ソースファイルをコピーする新しいバックアップ設定ファイルのファイル名を示します。

New File Name （新規ファイル名）— 新たに作成されるバックアップ設定ファイルの名前を示します。

Restore Configuration Factory Defaults （設定を工場デフォルトに戻す）— 選択によって、現在の構成設定は工場デフォルト設定に置き換えられます。クリアは現在の構成設定が維持されることを示します。

ファイルのコピー

□□□ ファイルのコピーページを開きます。

□□□ **Source**（コピー元）と**Destination** （コピー先）を定義します。

□□□ **Apply Changes** （変更の適用）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への復元

□□□ ファイルのコピーページを開きます。

□□□ **Restore Configuration Factory Defaults**（設定を工場デフォルトに戻す）にチェックを 入れます。

□□□ **Apply Changes** （変更の適用）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

ファイルのコピーページ内のフィールド設定操作と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-47** ファイルコピー **CLI** コマンド

CLI コマンド	説明
copy *source-url destination-url*	コピー元からコピー先へファイルをコピーします。
delete startup-config	Startup-Config ファイルを削除します。

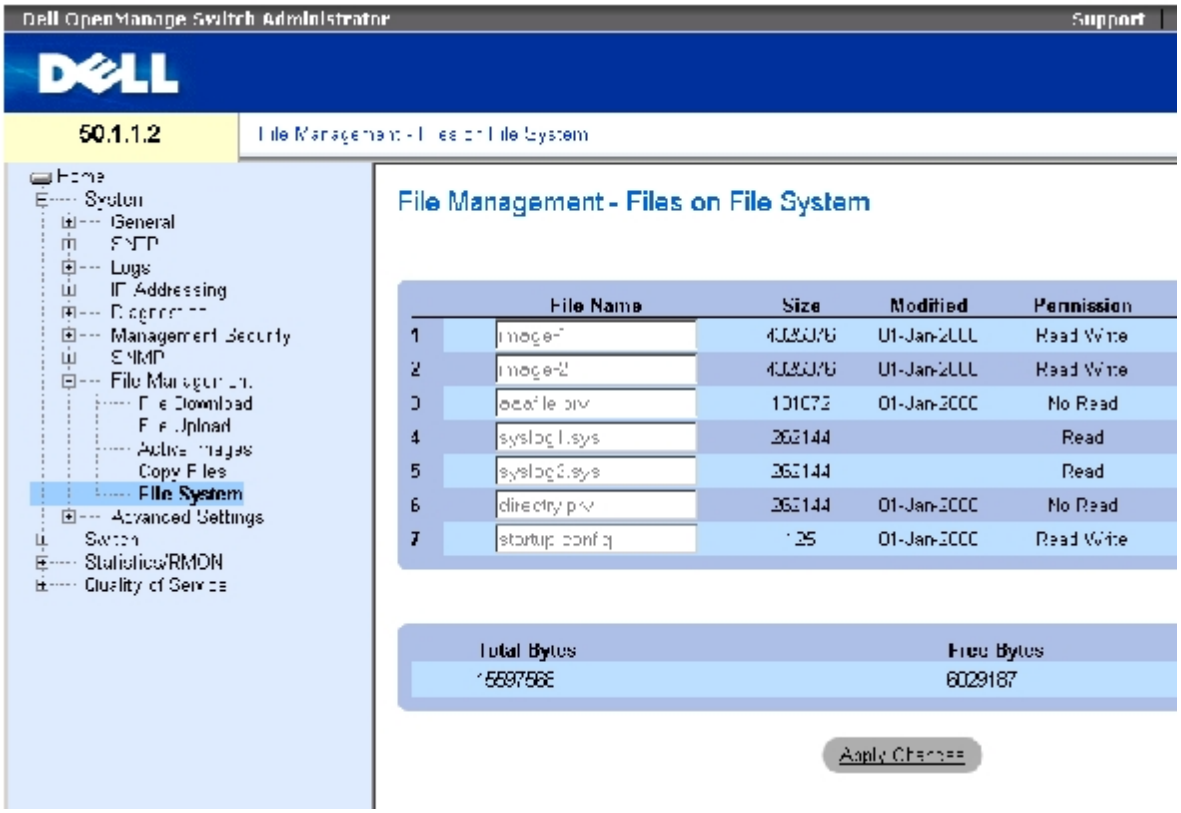
以下に CLI コマンドの例を示します。

```
console# delete startup-
config


Startup file was deleted


console#


console# copy running-
config startup-config


01-Jan-2000 06:55:32
%COPY-W-TRAP: The copy
operation was completed
successfully


Copy succeeded


console#
```

デバイスファイルの管理

ファイルシステム上のファイルページには、システム上に現在保存されているファイルに関するファイル名、サイズ、ファイル変更日、ファイルパーミッションなどの情報が表示されます。ファイルシステムは、最大 5 ファイル、合計 3 MB のファイルサイズの管理を許しています。ファイルシステム上のファイルページを開くには、ツリービューから **System** （システム）→ **File Management** （ファイルの管理）→ **File System** （ファイルシステム）をクリックします。

図**6-79** ファイルシステム上のファイル



ファイルシステム上のファイルページは以下のフィールドで構成されています。

File Name （ファイル名）— ファイル管理システムに現在保存されているファイル名を示します。

Size （サイズ）— ファイルサイズを示します。

Modified （変更日）— ファイルが最後に変更された日付を示します。

Permission （パーミッション）— ファイルに割り当てられているパーミッションタイプを示します。可能なフィールド値は以下のとおりです。

Read Only （リードオンリー）— リードオンリーファイルであることを示します。

Read Write （リードライト）— リードライトファイルであることを示します。

Remove （削除）— チェックによって、ファイルを削除します。

Rename （ファイル名変更）— ファイル名の変更を許可します。ファイル名は**File Name** （ファイル名）フィールドで変更します。

Total Bytes （総バイト数）— 現在使用している容量の合計を示します。

Free Bytes （空きバイト数）— 現在空いている残り容量の合計を示します。

CLI コマンドを使用したファイルの管理

システムファイル管理と等価な処理を実行する CLI コマンドを以下の表に示します。

表**6-48** ファイルコピー **CLI** コマンド

CLI コマンド	説明
dir	Display list of files on a flash file system

The following is an example of the CLI commands:

```
console# dir

Directory of flash:

File Name        Permis-  Flash    Data     Modified
                 sion     Size     Size
---------------  ------   ------   ------   ---------------
3.txt            rw       524288   523776   22-Feb-2005
                                              18:49:27
setup            rw       524288   95       22-Feb-2005
                                              15:58:19
setup2           rw       524288   95       22-Feb-2005
                                              15:58:35
image-1          rw       4325376  4325376  06-Feb-2005
                                              17:55:32
image-2          rw       4325376  4325376  06-Feb-2005
                                              17:55:31
test.txt         rw       524288   95       22-Feb-2005
                                              12:16:44
aaafile.prv      --       131072   --       06-Feb-2005
                                              19:09:02
syslog1.sys      r-       262144   --       22-Feb-2005
                                              18:49:27
syslog2.sys      r-       262144   --       22-Feb-2005
                                              18:49:27
directory.prv    --       262144   --       06-Feb-2005
                                              17:55:31
startup-         rw       524288   347      22-Feb-2005
config                                        11:56:03

Total size of flash: 16646144 bytes

Free size of flash: 4456448 bytes
```

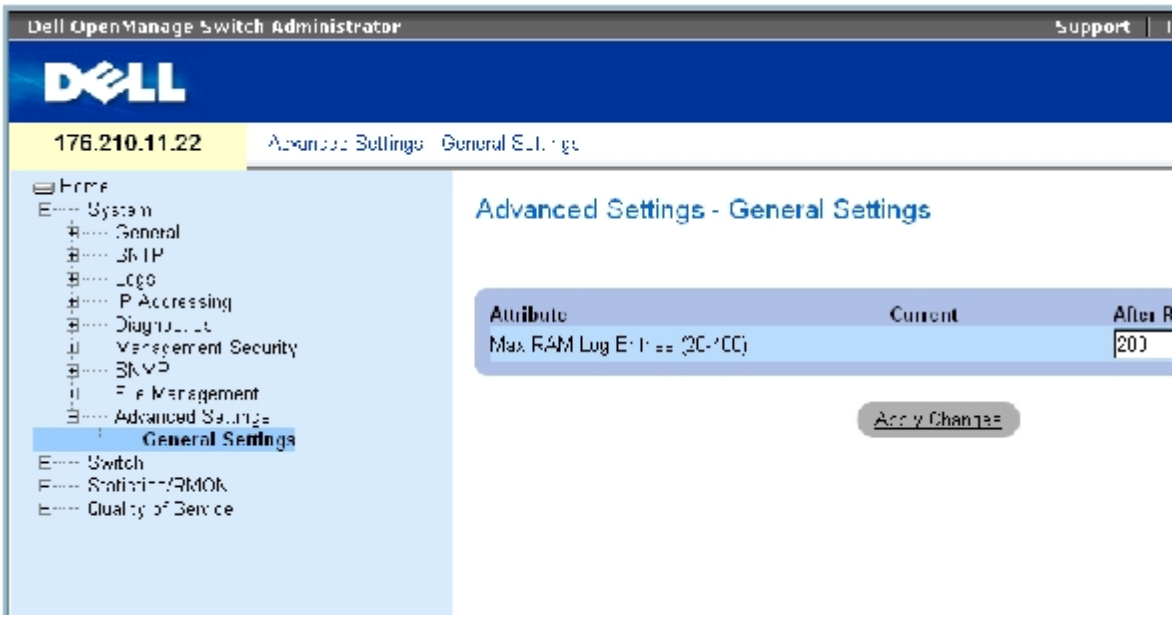
一般設定

スイッチのそのほかのグローバル属性を設定するには **Advanced**（アドバンスト）設定を使用します。ここで変更した属性は、スイッチをリセットしたあとで適用されます。詳細設定ページを開くには、ツリービューから、**System** （システム）→**Advanced Settings** （詳細設定）をクリックします。

詳細設定ページには一般設定用のリンクが表示されます。

一般設定ページには、一般デバイスパラメータの定義に関する情報が表示されます。一般設定ページを開くにはツリービューから **System** （システム）→ **Advanced Settings** （詳細設定）→ **General Settings** （一般設定）をクリックします。

図**6-80** 一般設定



一般設定ページは以下のフィールドで構成されています。

Attribute （属性）— 一般的な設定属性です。

Current （現在）— 現在の設定値です。

After Reset（リセット後）— 将来の（リセット後）の値です。**After Reset**（リセット後）フィールドに値を入力することにより、メモリがフィールド表に割り当てられます。

Max RAM Log Entries（20～400） （最大 **RAM** ログエントリ）— **RAM** ログエントリの最大数を示します。ログエントリが一杯になると、ログはクリアされログファイルが再起動します。

CLI コマンドを使用した RAM ログエントリカウンタの表示

一般設定ページ内のフィールド設定操作と等価な処理を実行する **CLI** コマンドを以下の表に示します。

表**6-49** 一般設定 **CLI** コマンド

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 syslog メッセージの数を設定します。

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

スイッチ情報の設定

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

本項では、ネットワークセキュリティ、ポート、アドレス表、GARP、VLAN、スパニングツリー、ポート集合、およびマルチキャストサポートの設定に関するシステムの運用および全般的な情報を提供します。

ネットワークセキュリティの設定

Network Security ページを使用して、アクセス制御リストとポートロックの両方を通じて、ネットワークセキュリティを設定します。ネットワークセキュリティページを開くには、**Switch** （スイッチ）→ **Network Security**（ネットワークセキュリティ）の順に選択します。

ポートベース認証

ポートベース認証により、外部サーバーを介して、ポート単位でシステムユーザーを認証することができます。認証済みの認可されたシステムユーザーのみがデータを送受信できます。ポートは、EAP（Extensible Authentication Protocol）を使用して、RADIUS サーバーを介して認証されます。ポートの認証には、次の 3 つが含まれます。

- **Authenticators**（認証符号）— システムへのアクセスを許可する前に、認証されるデバイスポートを指定します。
- **Supplicants**（サプリカント）— システムサービスへのアクセスを要求する認証済みポートに接続されるホストを指定します。
- **Authentication Server**（認証サーバー）— 外部サーバーを指定します。たとえば、認証符号に代わって認証を実行し、サプリカントがシステムサービスへの許可を受けているかどうかを示す RADIUS サーバーです。

ポートベース認証により、2 つのアクセス状況ができます。

- **Controlled Access**（制御アクセス）— サプリカントが認証されている場合、サプリカントとシステムの間の通信を許可します。
- **Uncontrolled Access**（無制御アクセス）— ポートの状態に関係なく、無制御の通信を許可します。

デバイスは現在、RADIUS サーバーを介してポートベース認証をサポートしています。

拡張ポートベース認証

Advanced Port Based Authentication（拡張ポートベース認証）には、以下の特徴があります。

- 単一ポートに複数のホストを接続することを可能にします。
- 1 つのホストを認証するだけで、すべてのホストにシステムアクセスを与えることができます。ポートが認証されていない場合、接続されているすべてのホストはネットワークへのアクセスを拒否されます。
- ユーザーベース認証を可能にします。**VLAN** に接続された特定のポートが認証されていない場合でも、デバイス内の特定の **VLAN** は常に利用可能です。
    - たとえば、**VoIP**（**Voice over IP**）は認証を必要としませんが、データトラフィックは認証を必要とします。認証が要求されない **VLAN** を定義することができます。**VLAN** に接続されているポートが認証済みとして定義されていても、ユーザーは非認証 **VLAN** を利用することができます。

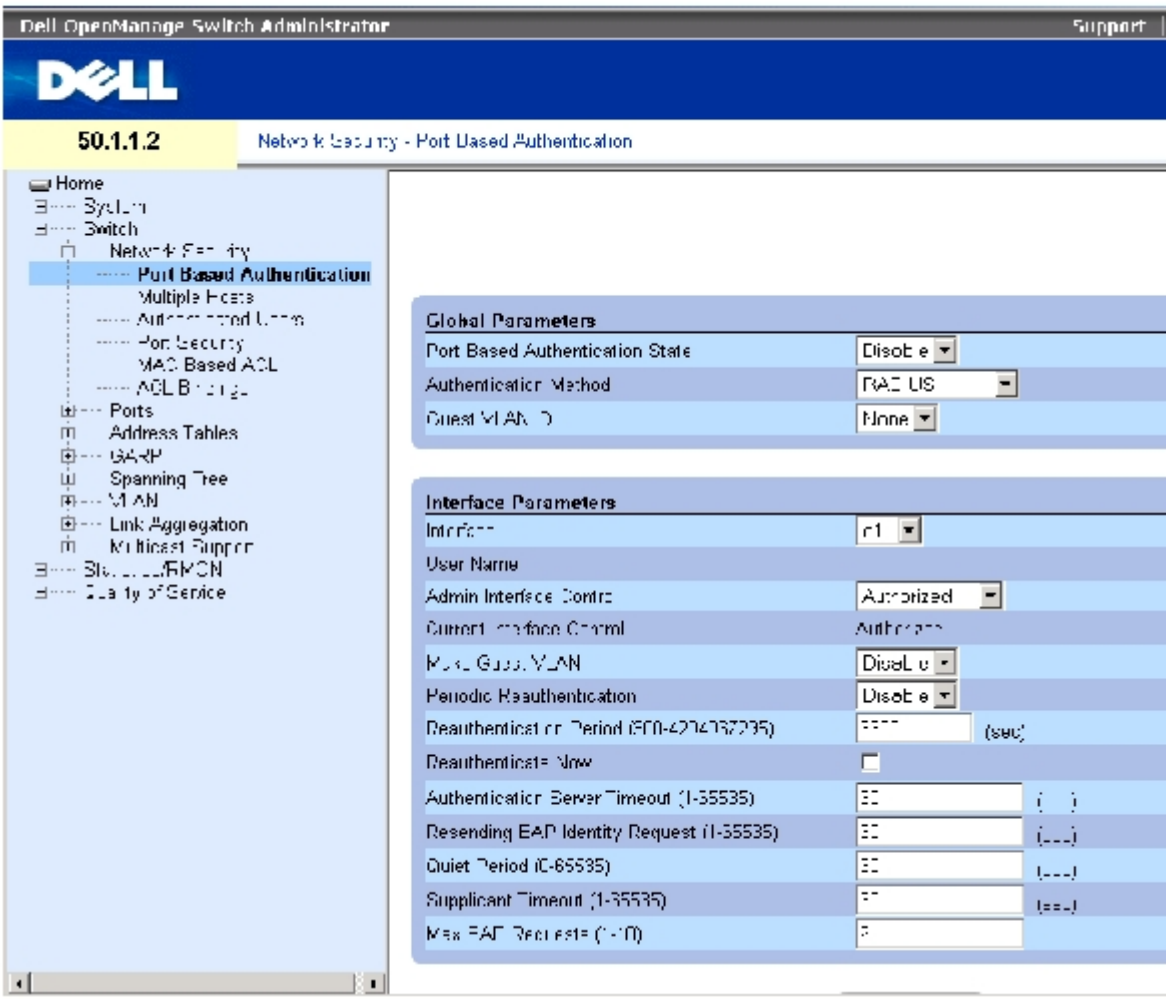
Advanced Port Based Authentication（拡張ポートベース認証）は、以下のモードに実装されています。

- **Single Host Mode**（単一ホストモード）— 認証を受けたホストのみがポートにアクセスできます。
- **Multiple Host Mode**（マルチホストモード）— 単一ポートに複数のホストを接続することができます。すべてのホストがネットワークにアクセスするには、認証を受けるホストは 1 台のみに限定する必要があります。ホストの認証が失敗するか、または **EAPOL** ログオフメッセージを受信した場合、接続されているすべてのクライアントはネットワークへのアクセスを拒否されます。
- **Guest VLANs**（ゲスト **VLAN**）— ポートに対し、限定されたネットワークアクセスの認証を与えます。ポートベース認証ではネットワークアクセスを拒否されたポートで、**Guest VLAN** が有効に設定されている場合、そのポートは限定されたネットワークアクセスを得ることになります。たとえば、ネットワーク管理者は、認証を受けていないユーザーに対して、**Guest VLAN** を使用してポートベース認証によるネットワークアクセスを拒否しながらも、インターネットアクセスを許可することができます。

ポートベース認証の設定

ポートベース認証 ページは、ネットワーク管理者にポートベース認証の設定を許可します。 ポートベース認証 ページを開くには、**Switch**（スイッチ）→ **Network Security**（ネットワークセキュリティ）→ **Port Based Authentication**（ポートベース認証）の順にクリックします。

図 **7-1** ポートベース認証



ポートベース認証 ページには、以下のフィールドがあります。

Port Based Authentication State（ポートベース認証の状態）— デバイスにポートベース認証を許可します。可能なフィールド値は、以下のとおりです。

Enable— デバイスに対するポートベース認証を有効に設定します。

Disable — デバイスに対するポートベース認証を無効に設定します。

Authentication Method（認証方法）— 使用されている認証方法を示します。可能なフィールド値には、以下のものがあります。

None（なし）— ポートの認証にどんな認証方法も使用されていないことを示します。

RADIUS — ポート認証が RADIUS サーバーを介して実行されていることを示します。

RADIUS, None（RADIUS、なし）— ポート認証が最初に RADIUS サーバーを介して行われていることを示します。ポートが認証されていない場合、どんな認証方法も使用されず、セッションは許可されます。

Guest VLAN （ゲスト VLAN）— 認証されていないポートに対するゲスト VLAN の使用を有効に設定します。Guest VLAN が有効に設定されている場合、認証されていないポートは **VLAN List** フィールドで選択されている VLAN に自動的に参加します。フィールドはデフォルトで無効に設定されています。

Interface（インタフェース）— ポートベース認証が有効に設定されているインタフェースの一覧が含まれています。

User Name（ユーザー名）—サプリカントのユーザー名を示します。

Admin Interface Control（管理インタフェース制御）— ポート認証の状態を定義します。可能なフィールド値には、以下のものがあります。

Auto（自動）— デバイスに対するポートベース認証を有効に設定します。。インタフェースは、デバイスとクライアントの間の認証の交換に基づいて、認証状態と非認証状態の間を行き来します。

Authorized（認証済み）— 認証を受けないままでインタフェースを認証状態にします。インタフェースは、クライアントポートベース認証なしで通常のトラフィックを再送信し、受信します。

Unauthorized（非認証）— インタフェースを非認証状態とすることで、選択されたインタフェースシステムのアクセスを拒否します。デバイスは、インタフェースを通じてクライアントに認証サービスを提供することができません。

Current Interface Control（現在のインタフェース制御）— 現在のポート認証状態。

Make Guest VLAN（ゲスト VLAN にする）— 有効に設定されていると、このインタフェースに接続されている認証されていないユーザーが Guest VLAN にアクセスできることを示します。

Periodic Reauthentication（定期的再認証）— 即時のポート再認証を許可します。

Reauthentication Period (300-4294967295)（再認証期間）— 選択されているポートが再認証を受けるタイムスパンを示します。フィールド値は秒単位で、フィールドのデフォルト値は 3600 秒です。

Reauthenticate Now（今すぐに再認証）— チェックを受けた時に、即座にポート再認証を許可します。

Authentication Server Timeout（認証サーバーのタイムアウト）（1～65535）— デバイスが認証サーバーに要求を再送信するまで待機する時間を定義します。フィールド値は秒単位で指定され、フィールドのデフォルト値は 30 秒です。

Resending EAP Identity Request（EAP アイデンティティ要求の再送信）（1～65535）— EAP 要求が再送信されるまでの待ち時間を定義します。フィールドのデフォルト値は 30 秒です。

Quiet Period（静止期間）（0～65535）—認証交換に失敗した後でデバイスが静止状態を続ける秒数を示します。可能なフィールド値の範囲は、0～65535 です。フィールドのデフォルト値は 60 秒です。

Supplicant Timeout（サプリカントのタイムアウト）（1～65535）— EAP 要求がサプリカントに再送信されるまでの待ち時間を示します。フィールド値は秒単位で、フィールドのデフォルト値は 30 秒です。

Max EAP Requests（最大 EAP 要求）（1～10）— 送信される EAP 要求の合計数を示します。定義された時間内に応答がなかった場合、認証処理は再試行されます。デフォルトの試行回数は 2 回です。

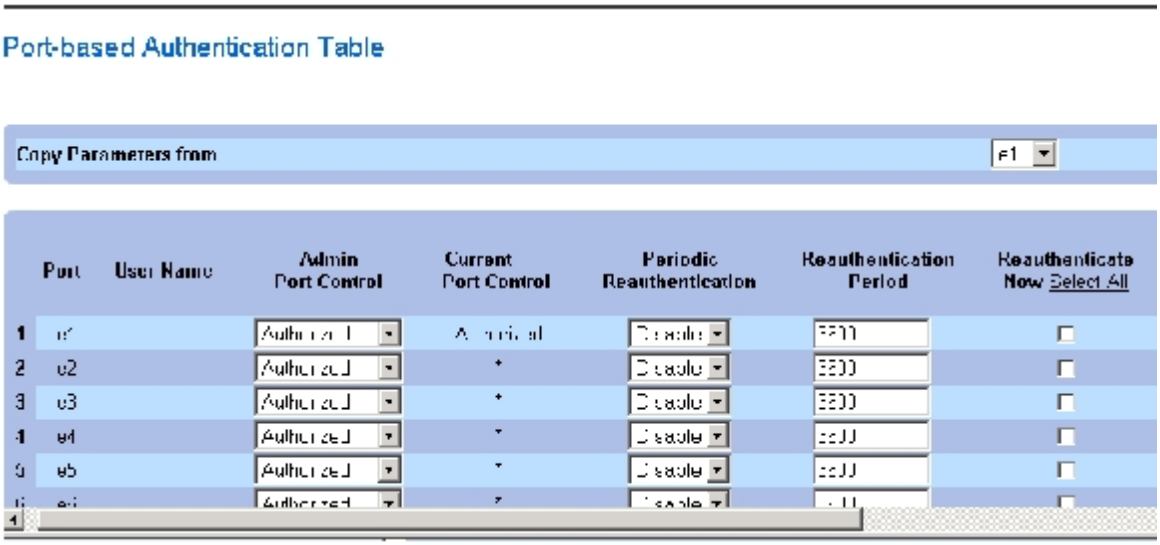
ポートベース認証表の表示

□□□ ポートベース認証 ページを開きます。

□□□ Show All（すべてを表示）をクリックします。

Port Based Authentication Table （ポートベース認証表）が開きます。

図**7-2** ポートベース認証表



ポートベース認証 ページ内のフィールドのほかに、ポートベース認証表には以下のフィールドも表示されます。

Unit No.（ユニット番号）— スタッキングメンバーを選択します。

Copy Parameters from Port No.（パラメータのコピー元のポート番号）— 選択したポートでパラメータをコピーします。

ポートベース認証表のパラメータのコピー

□□□ ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ポートベース認証表が開きます。

□□□ **Copy Parameters from Port No.**（パラメータのコピー元のポート番号）フィールドから インタフェースを選択します。

□□□ ポートベース認証表からインタフェースを選択します。

□□□ **Copy to**（コピー先）チェックボックスを選択して、ポートベース認証のパラメータ をコピーするインタフェースを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

CLI コマンドを使用したポートベース認証の有効化

次の表は、ポートベース認証 表に表示されているように、ポートベース認証を有効にする場合の等価な **CLI** コマンドをまとめたものです。

表**7-1** ポート認証に関連する **CLI** コマンド

CLI コマンド	説明
aaa authentication dot1x default *method1* [*method2*.]	IEEE 802.1X を実行するインタフェースで使用する 1 つまたは複数の AAA（認証、許可、アカウンティング）方式を指定します。
dot1x max-req *count*	認証処理を再試行するまでにデバイスからクライアントに EAP を送信する最大試行回数を設定します。
dot1x re-	すべての 802.1X 対応ポートまたは指定の 802.1X 対応ポートの再認証を手動で開始します。

authenticate [**ethernet** *interface*]	
dot1x re-authentication	クライアントの定期的な再認証を有効に設定します。
dot1x timeout quiet-period seconds	認証交換に失敗した後でデバイスが静止状態を続ける秒数を設定します。
dot1x timeout re-authperiod *seconds*	再認証の試行間隔を秒数で設定します。
dot1x timeout server-timeout *seconds*	認証サーバーへのパケットの再送信時間を設定します。
dot1x timeout supp-timeout *seconds*	クライアントへの EAP 要求フレームの再送信時間を設定します。
dot1x timeout tx-period *seconds*	EAP 要求 / アイデンティティフレームに対するクライアントからの応答を待つ秒数を設定します。この秒数を過ぎると、要求は再送信されます。
show dot1x [ethernet *interface*]	デバイスまたは指定のインタフェースに関する 802.1X の状態を表示します。
show dot1x users [username username]	デバイスの 802.1X ユーザーを表示します。
dot1x guest-vlan enable	認証されていないポートに対するゲスト VLAN の使用を有効に設定します。Guest VLAN が有効に設定されている場合、認証されていないポートは **VLAN List** フィールドで選択されている VLAN に自動的に参加します。フィールドはデフォルトで無効に設定されています。
dot1x guest-vlan	VLAN の一覧が含まれています。ゲスト VLAN は **VLAN List** から選択されます。

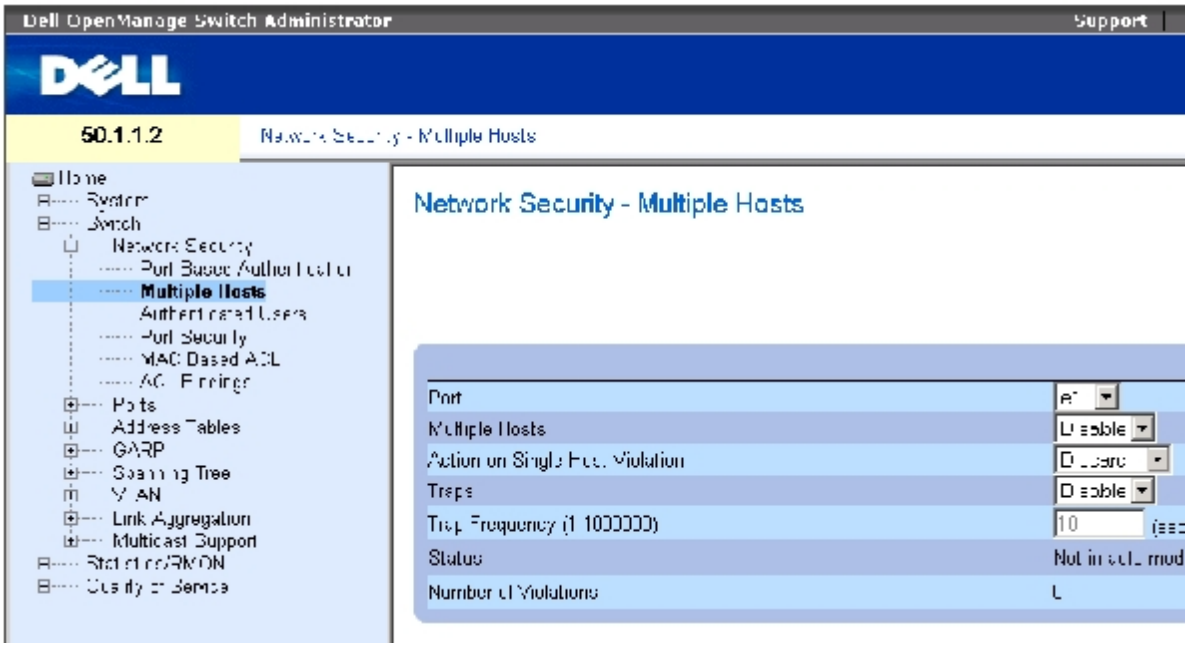
以下に、CLI コマンドの例を示します。

```
Console# show dot1x

Interface  Admin Mode  Oper Mode     Reauth Control  Reauth Period  Username
---------  ----------  ------------  --------------  -------------  --------
1/e1       Auto        Authorized    Ena             3600           Bob
1/e2       Auto        Authorized    Ena             3600           John
1/e3       Auto        Unauthorized  Ena             3600           Clark
1/e4       Force-auth  Authorized    Dis             3600           n/a
```

拡張ポートベース認証の設定

複数のホスト ページには、特定のポートと VLAN に対する拡張ポートベース認証の設定を定義するための情報があります。拡張ポートベース認証の詳細については、拡張ポートベース認証を参照してください。複数のホストを開くには、Switch（スイッチ）→Network Security（ネットワークセキュリティ）→ Multiple Hosts（複数のホスト）の順にクリックします。

図**7-3** 複数のホスト



複数のホストページには、以下のフィールドがあります。

Port（ポート）— 拡張ポートベース認証を有効にするポート番号です。

Multiple Hosts（複数のホスト）— 単一のホストから複数のホストにシステムへのアクセスを許可するオプションを有効または無効にします。選択したポートで入口フィルタを無効にするか、ポートロックセキュリティを使用するには、この設定を有効にする必要があります。

Action on Single Host Violation（単一ホスト違反に対する処置）— 所有する MAC アドレスがクライアント（サプリカント）の MAC アドレスではないホストから、単一ホストモードで到達したパケットに適用する処置を定義します。可能なフィールド値は、以下のとおりです。

Forward（転送）— 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（破棄）— 学習されていない送信元からのパケットを破棄します。これがデフォルト値です。

Shutdown（シャットダウン）— 学習されていない送信元からのパケットを破棄し、ポートをシャットダウンします。ポートをアクティブにするか、デバイスをリセットするまで、ポートはシャットダウンされたままです。

Traps（トラップ）— 違反が発生した場合に、ホストへのトラップの送信を有効または無効にします。

Trap Frequency（トラップの頻度）（1～1000000秒）— トラップがホストに送信される間隔を決めます。このフィールドは、**Multiple Hosts**（複数のホスト）フィールドが無効に設定されている場合にのみ定義できます。デフォルト値は 10 秒です。

Status（ステータス）— ホストのステータスです。可能なフィールド値は、以下のとおりです。

Unauthorized （権限なし）— ポート制御が ***Force Unauthorized***（強制権限なし）で、ポートリンクはダウンしているか、ポート制御が **Auto** に設定されているものの、クライアントはポートを介して認証されていることを示します。

Not in Auto Mode （自動モード以外）— ポート制御が ***Forced Authorized***（強制認証済み）で、クライアントがフルポートアクセス権を持つことを示します。

Single-host Lock（単一ホストロック）— ポート制御が ***Auto***（自動）に設定されていて、単一クライアントがポートを介して認証されていることを示します。

No Single Host — Multiple Host

（単一ホスト以外）　　（複数のホスト）が有効になります。

Number of Violations（違反の数）— 所有する **MAC** アドレスがクライアント（サプリカント）の **MAC** アドレスではないホストから、単一ホストモードでインタフェースに到達したパケットの数。

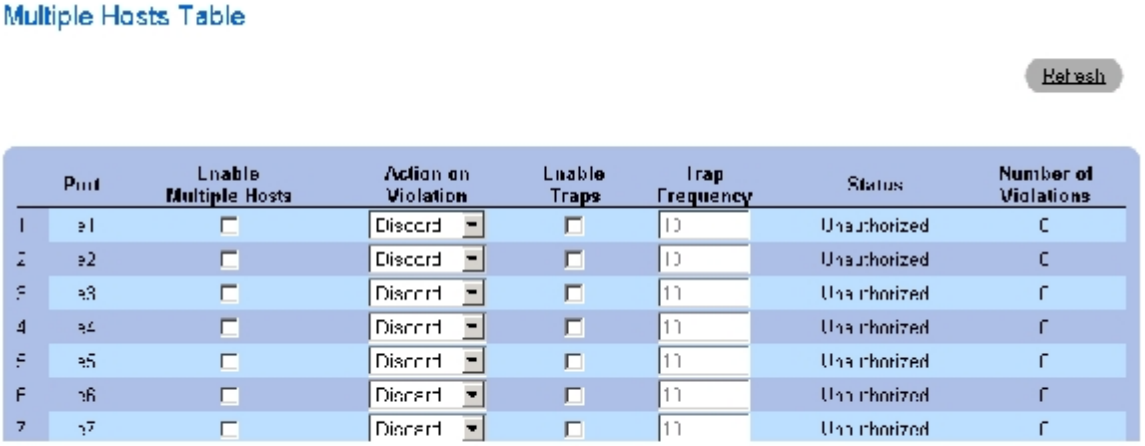
複数のホストの表の表示

□□□ 複数のホスト ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

複数のホストの表が開きます。

図**7-4** 複数のホストの表



CLI コマンドを使用した複数のホストの有効化

次の表は、複数のホスト ページに表示されているように、拡張ポートベース認証を有効にする場合の等価な **CLI** コマンドをまとめたものです。

表**7-2** 複数のホストに関連する **CLI** コマンド

CLI コマンド	説明
dot1x multiple-hosts	dot1x port-control インタフェース設定コマンドが auto に設定されている 802.1X 許可ポートに複数のホスト（クライアント）を許可します。
dot1x single-host-violation {forward |discard |discard-shutdown}[trap seconds]	所有する MAC アドレスがクライアント（サプリカント）の MAC アドレスではないステーションが、インタフェースへのアクセスを試みたときの対応処置を設定します。

以下に、**CLI** コマンドの例を示します。

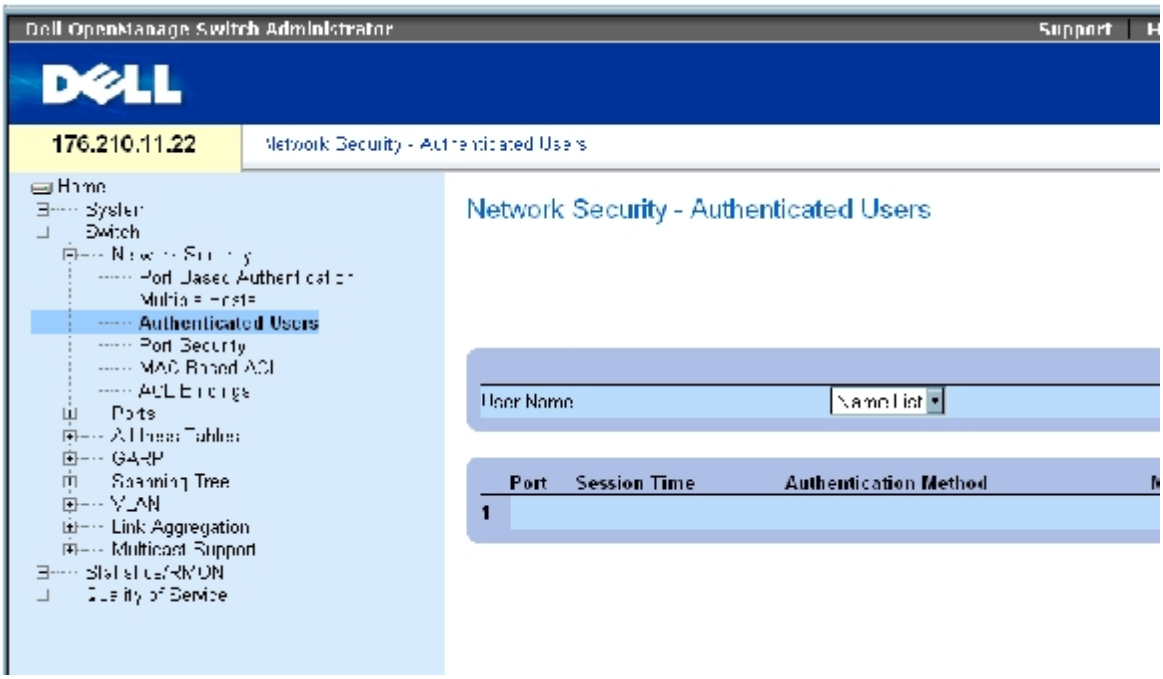
```
Console(config)# interface
ethernet 1/e1
```

```
Console(config-if)# dot1x
multiple-hosts
```

ユーザーの認証

認証ユーザー ページ には、ユーザーのポートアクセスリストが表示されます。ユーザーアクセスリストは、ユーザー名の追加ページで定義します。認証ユーザーページを開くには、 **Switch** （スイッチ）→ **Network Security** （ネットワークセキュリティ）→ **Authenticated Users**（認証ユーザー）の順にクリックします。

図**7-5** 認証ユーザー



認証ユーザーページには、以下のフィールドがあります。

User Name（ユーザー名）— RADIUS サーバーを介して権限が付与されたユーザーの一覧です。

Port（ポート）— ユーザー名別に認証に使用するポート番号です。

Session Time（セッション時間）— ユーザーがデバイスにログオンしていた時間です。フィールドの書式は、**Day:Hour:Minute:Seconds**（日数:時間数:分数:秒数）で、たとえば、**3 days: 2 hours: 4 minutes: 39 seconds**（3日:2時間:4分:39秒）となります。

Authentication Method（認証方法）— 最後のセッションが認証された方法です。可能なフィールド値は、以下のとおりです。

Remote（リモート）— ユーザーは、リモートサーバーから認証されました。

None（なし）— ユーザーは認証されていません。

MAC Address（MAC アドレス）— サプリカントの MAC アドレスです。

認証ユーザー表の表示

□□□ 認証ユーザー ページを開きます。

□□□ Show All（すべてを表示）をクリックします。

認証ユーザー表が開きます。

図**7-6** 認証ユーザー表

CLI コマンドを使用したユーザーの認証

次の表は、 認証ユーザー ページに表示されているように、ユーザーを認証する場合の等価な CLI コマンドをまとめたものです。

表**7-3** ユーザー名の追加に関連する **CLI** コマンド

CLI コマンド	説明
show dot1x users [username username]	デバイスの 802.1X ユーザーを表示します。

以下に、CLI コマンドの例を示します。

```
console# show dot1x users

Port Username Session Time Auth Method MAC Address

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

1/e11 gili 00:09:27 Remote 00:80:c8:b9:dc:1d
```

ポートセキュリティの設定

ネットワークセキュリティを高めるには、特定の MAC アドレスを持つユーザーのみに特定ポートへのアクセスを制限します。MAC アドレスは、制限する時点までに動的に学習されたものか、静的に設定したものになります。ポートロックセキュリティは、特定のポートで受信される受信パケットおよび学習パケットを監視します。ロックされたポートへのアクセスは、特定の MAC アドレスを持つユーザーに制限されます。これらのアドレスは、ポートに対して手動で定義したものか、ポートがロックされた時点までにそのポートで学習されたものになります。ロックされたポートでパケットを受信したときに、そのパケットの送信元 MAC アドレスがそのポートに関連付けられていない（別のポートで学習されたか、システムにとって未知である）場合、プロテクションメカニズムが起動し、各種のオプションが実行されます。権限のないパケットが、ロックされたポートに到達すると、次のいずれかの処置が取られます。

- 転送される
- トラップなしで破棄される
- トラップ付きで破棄される

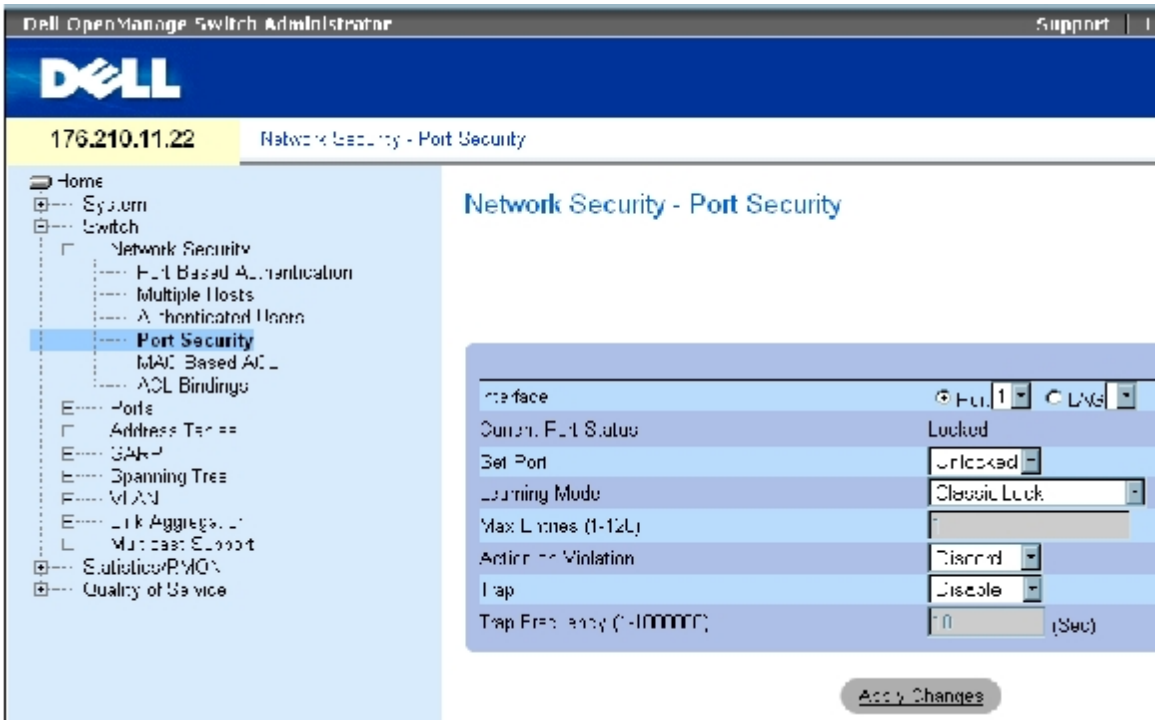
- ポートがシャットダウンされる

また、ポートロックセキュリティでは、MAC アドレスの一覧を設定ファイルに保存することもできます。MAC アドレスの一覧は、デバイスをリセットした後で復元できます。

メモ： ポートセキュリティを有効にするには、必要とされるポートで複数のホスト機能 を有効に設定します。

無効になっているポートは、ポートセキュリティページからアクティブにできます。ポートページには、ストームコントロールやポートミラーリングなどの拡張機能を含むポート機能を設定したり、仮想ポートテストを実行するためのリンクがあります。ポートセキュリティ ページを開くには、**Switch**（スイッチ）→ **Network Security**（ネットワークセキュリティ）→ **Port Security**（ポートセキュリティ）の順にクリックします。

図**7-7** ポートセキュリティ



ポートセキュリティ ページには、以下のフィールドがあります。

Interface（インタフェース）— ポートロックが有効に設定されている、選択されたインタフェースタイプ。

Port（ポート）— 選択されているインタフェースタイプはポートです。

LAG（LAG）— 選択されているインタフェースタイプは LAG です。

Current Port Status（現在のポートステータス）— 現在設定されているポートのステータスです。

Set Port（ポートの設定）— ポートをロックまたはロック解除します。可能なフィールド値は、以下のとおりです。

Unlocked（ロック解除）— ポートをロック解除します。これがデフォルト値です。

Locked（ロック）— ポートをロックします。

Learning Mode（学習モード）— ポートロックのタイプを定義します。**Learning Mode**（学習モード）フィールドは、**Set Port**（ポート

の設定）フィールドで **Locked**（ロック）が選択されている場合にのみ有効に設定されます。可能なフィールド値は、以下のとおりです。

Classic Lock（クラシックロック）— クラシックロックメカニズムを使用してポートをロックします。学習済みのアドレスの数に関係なく、ポートは即座にロックされます。

Limited Dynamic Lock（限定動的ロック）— ポートに関連付けられている現在の動的 MAC アドレスを削除することで、ポートをロックします。ポートは、そのポートに許可されている最大アドレス数まで学習します。再学習 MAC アドレスとエージング MAC アドレスの両方が有効です。

Max Entries（最大エントリ数）— ポートで学習できる MAC アドレスの数を指定します。**Max Entries**（最大エントリ数）フィールドは、**Set Port**（ポートの設定）フィールドで **Locked**（ロック）が選択されている場合にのみ有効になります。また、Limited Dynamic Lock（限定動的ロック）モードも選択されています。デフォルトは 1 です。

Action on Violation（違反に対する処置）— ロックされたポートに到達したパケットに適用する処置です。可能なフィールド値は、以下のとおりです。

Forward（転送）— 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（破棄）— 学習されていない送信元からのパケットを破棄します。これがデフォルト値です。

Shutdown（シャットダウン）— 学習されていない送信元からのパケットを破棄し、ポートをシャットダウンします。ポートを再度アクティブにするか、デバイスをリセットするまで、ポートはシャットダウンされたままです。

Trap（トラップ）— ロックされたポートでパケットを受信した時点でトラップが送信されるようにします。

Trap Frequency (1-1000000)（トラップの頻度）（1～1000000）— トラップの間隔を示す時間（秒単位）です。デフォルト値は 10 秒です。

ポートロックの定義

□□□ ポートセキュリティ ページを開きます。

□□□ インタフェースタイプと番号を選択します。

□□□ フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

ロックされたポートがポートセキュリティ表に追加され、デバイスがアップデートされます。

ポートセキュリティ表の表示

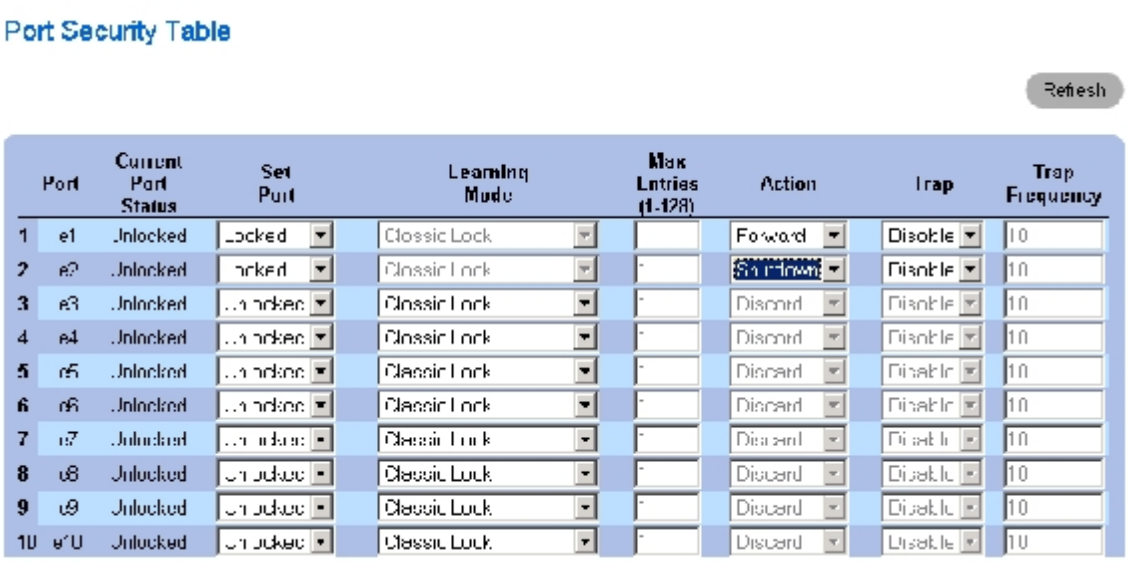
□□□ ポートセキュリティ ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ポートセキュリティ表が開きます。

メモ： ポートロックはポートセキュリティ表で定義できます。

図**7-8** ポートセキュリティ表



ポートセキュリティ表には、以下の追加のフィールドが含まれています。

Unit No.（ユニット番号）— ポートロック情報が表示されるスタッキングユニットを指定します。

Copy Parameters from（パラメータのコピー元）— 選択したユニット番号にパラメータをコピーします。

CLI コマンドを使用したポートロックセキュリティの設定

次の表は、ポートセキュリティページに表示されているように、ポートロックセキュリティを設定する場合の等価な CLI コマンドをまとめたものです。

表**7-4** ポートセキュリティに関連する **CLI** コマンド

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}	ポートセキュリティ上の理由でシャットダウンされたインタフェースを再びアクティブに戻します。
port security learning {disabled | dynamic}	ポートロックのタイプを定義します。
port security max max-addr	ポートで学習できる MAC アドレスの数を指定します。
port security [forward | discard | discard-shutdown] [trap seconds]	インタフェースに対して新規アドレスの学習をロックします。
show ports security {ethernet interface | port-channel port-channel-number}	ポートロック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 # show ports security

Port    Status    Action    Trap    Frequency    Counter
---     -------   -------   ------  ---------    ------
```

--			-	-	--
1/e1	locked	Discard	Enable	100	88
1/e2	locked	Discard, Shutdown	Disable		
1/e3	Unlocked	-	-	-	-

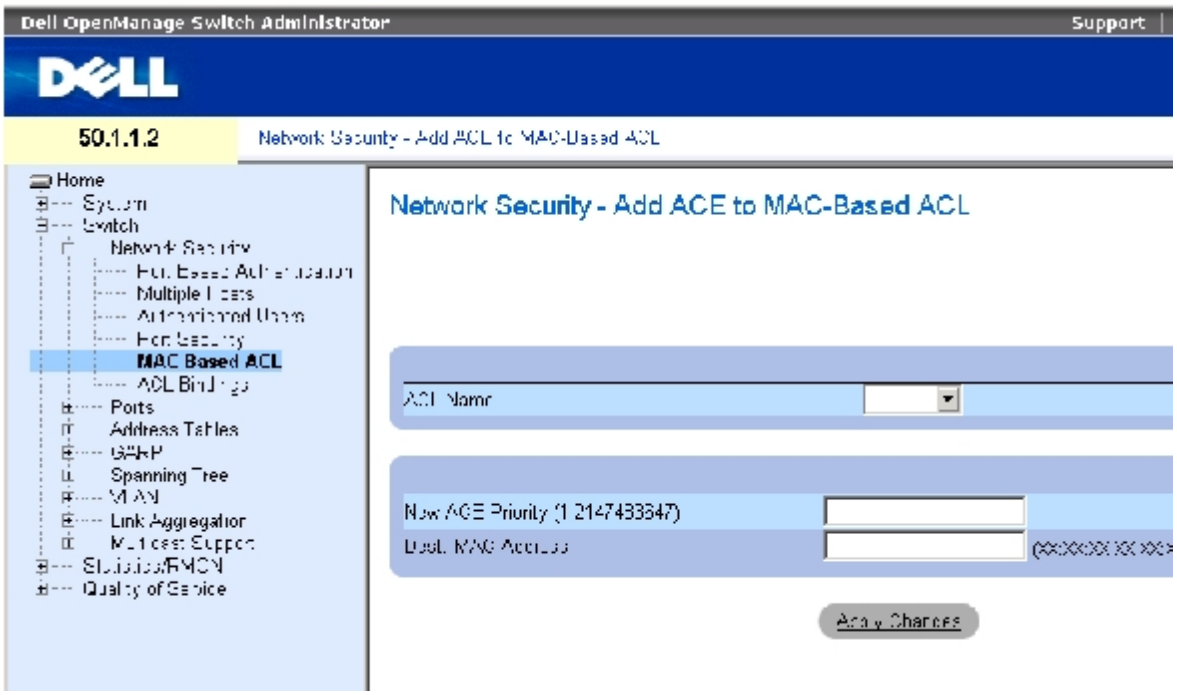
MAC ベースの ACL の定義

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入口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。各分類ルールとアクションは、ACE（Access Control Element）と呼ばれています。ACE は、トラフィックをフィルタして分類を決定します。MAC ベースの ACL は、非 IP を含むすべてのパケットに適用されます。分類フィールドは、L2 フィールドにのみ基づきます。

MAC ベースの ACLページにより、MAC ベースの ACL を定義することができます。ACL の説明については、「MAC ベースの ACL の定義」を参照してください。

MAC ベースの ACLページを開くには、**Switch**（スイッチ）→ **Network Security**（ネットワークセキュリティ）→ **MAC based ACL**（MAC ベースの ACL）の順に選択します。

図**7-9 MAC** ベースの **ACL**



MAC ベースの ACLページには、以下のフィールドがあります。

ACL Name（ACL 名）— ユーザー定義の ACL。

New ACE Priority (1-2147483647)（新規 ACE 優先度）（1～2147483647）— ACL フィールド内の ACE ルールのインデックス。

Destination MAC Address（送信先 MAC アドレス）— パケットの送信先の MAC アドレスを ACE と一致させます。

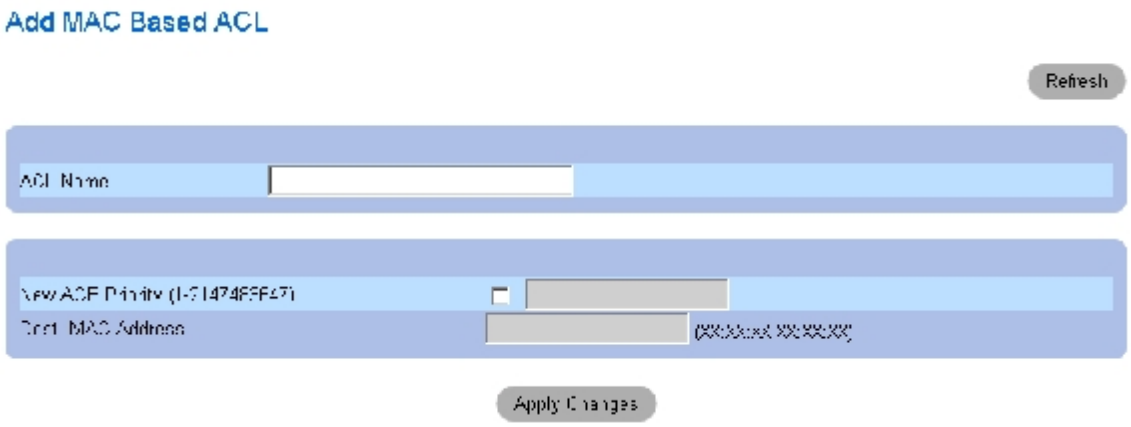
MAC ベースの ACL を追加するには、次の手順を実行します。

□□□ MAC ベースの ACLページを開きます。

□□□ **Add**（追加）をクリックします。

MAC ベースの ACL の追加ページが開きます。

図**7-10 MAC** ベースの **ACL** の追加



□□□ フィールドを定義します。

□□□ **Apply Changes**（変更の適用）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。

ACL 固有の ACE の表示

□□□ MAC ベースの ACLページを開きます。

□□□ ACL を選択します。

□□□ **Show All**（すべてを表示）をクリックします。

MAC ACL と関連する **ACE** ページが開きます。

ACL の削除

□□□ MAC ベースの ACLページを開きます。

メモ： ACL は、インタフェースにバインドされていない場合にのみ削除できます。

□□□ ACL を選択します。

□□□ **Show All**（すべてを表示）をクリックします。

MAC ACL と関連する **ACE** ページが開きます。

□□□ **Remove ACL** （ACL の削除）チェックボックスにチェックマークを付けます。

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

次の表は、MAC ベースの ACLページに表示されているように、MAC ベースの ACE を ACL に割り当てる場合の等価な CLI コマンドをまとめたものです。

表**7-5 MAC** ベースの **ACE CLI** コマンド

CLI コマンド	説明
`mac access-list name`	レイヤー 2 MAC ACL を作成し、MAC アクセスリスト設定モードに入ります。
`deny destination`	MAC ベースの ACL 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。
`show access-lists [name]`	デバイスに対して設定された ACL（アクセス制御リスト）を表示します。

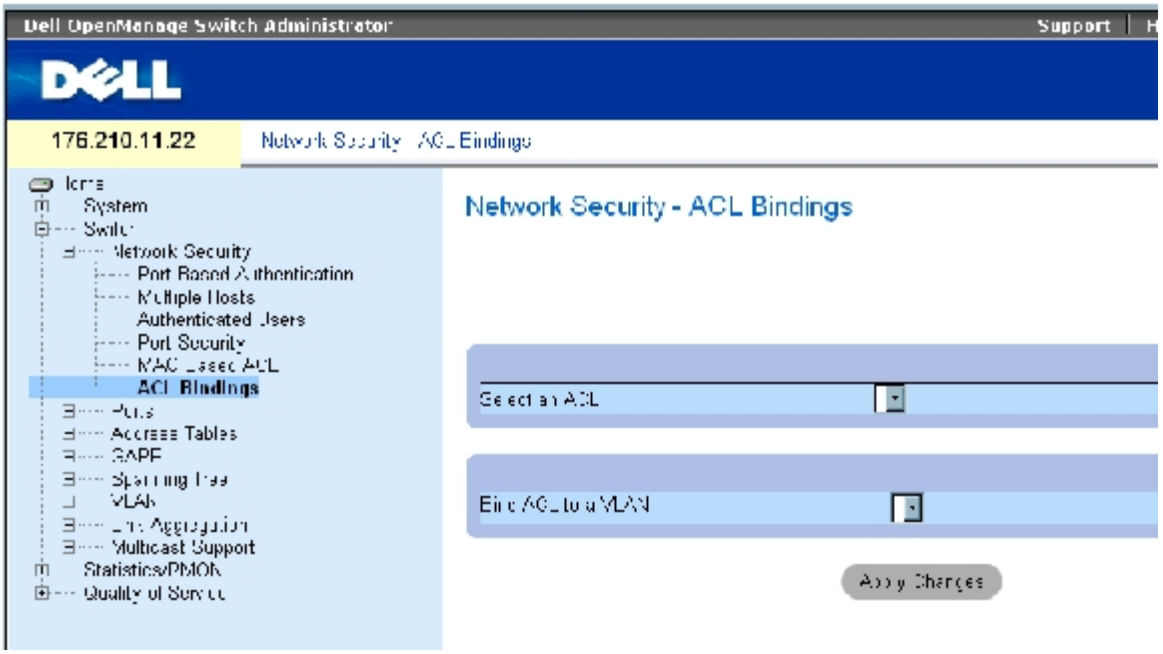
以下に、CLI コマンドの例を示します。

```
console (config)# mac access-list dell

console (config-mac-al)# deny 00-10-B5-F4-00-01
```

ACL バインドの設定

ACL がインタフェースにバインドされている場合、ACL は選択したインタフェースに適用されます。ACL バインドページを使用して、ACL リストを分類方法とインタフェースに割り当てます。ACL バインドページを開くには、**Switch**（スイッチ）→ **Network Security**（ネットワークセキュリティ）→ **ACL Binding**（ACL バインド）の順に選択します。

図**7-11 ACL** バインド



ACL バインドページには、以下のフィールドがあります。

Select an ACL （ACL の選択） — 受信パケットが一致する ACL タイプ。

Bind ACL to VLAN（ACL を VLAN にバインド） — ACL が割り当てられている VLAN。

インタフェースへの **ACL** の割り当て

□□□ ACL バインドページを開きます。

□□□ **Select an ACL** （ACL の選択）フィールドで、ACL タイプを選択します。

□□□ **Bind ACL to an VLAN** （ACL を VLAN にバインドする）フィールドで、ACL が割り 当てられている VLAN を選択します。

□□□ **Apply Changes**（変更の適用）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。

ACL バインド表からのエントリの削除

□□□ ACL バインドページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ACL バインド表 が開きます。

□□□ 削除する必要があるエントリの **Remove** （削除）チェックボックスにチェックマーク を付けます。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択したエントリが表から削除され、デバイスがアップデートされます。

ACL バインド表の表示

□□□ ACL バインドページを開きます。

□□□ **Show All**（すべてを表示）をクリックして、**ACL** バインド表 を開きます。

ACL バインド表 のフィールドは、**ACL** バインド ページのフィールドと同じです。

ACL バインド表のパラメータのコピー

□□□ ACL バインドページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ACL バインド表 が開きます。

□□□ **Copy Parameters from**（パラメータのコピー元）フィールドでインタフェースを選択 します。

□□□ **VLAN** ドロップダウンメニューから VLAN を選択します。

このインタフェースの定義が、選択したターゲットポート / トランクにコピーされます。

□□□ 編集するするエントリの **Copy to**（コピー先）チェックボックスにチェックマークを付 けるか、または利用可能なすべてのポート / トランクに定義をコピーします。

□□□ **Select All**（すべてを選択）をクリックします。

□□□ **Apply Changes**（変更の適用）をクリックします。

パラメータが *ACL* バインド表のターゲットポート / トランクにコピーされ、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 メンバーシップの割り当て

次の表は、**ACL** バインド ページに表示されているように、ACL メンバーシップを割り当てる場合の等価な CLI コマンドをまとめたものです。

表**7-6 ACL** バインドに関連する **CLI** コマンド

CLI コマンド	説明
service-acl {input *acl-name***}**	アクセスリストをインタフェース入力に適用します。

以下に、CLI コマンドの例を示します。

```
console(config)# interface vlan 123

console(config-if)# service-acl input dell
```

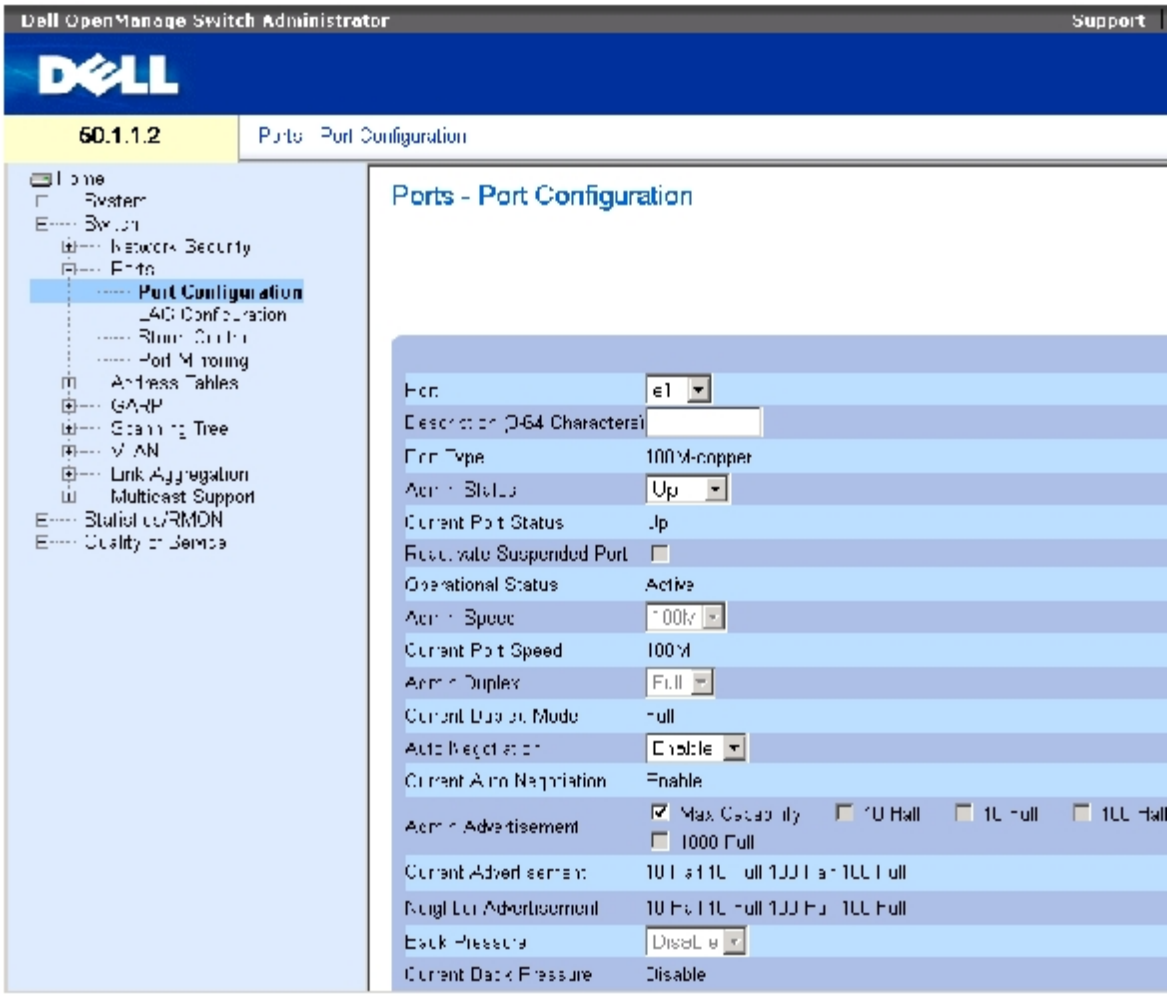
ポートの設定

ポートページには、ストームコントロールやポートミラーリングなどの拡張機能を含むポート機能を設定したり、仮想ポートテストを実行するためのリンクがあります。ポート ページを開くには、**Switch**（スイッチ）→ **Ports**（ポート）の順に選択します。

ポート設定の定義

ポートの設定ページを使用してポートパラメータを定義します。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。ポートの設定ページを開くには、ツリービューで、**Switch**（スイッチ）→ **Ports**（ポート）→ **Port Configuration** （ポートの設定）の順にクリックします。

図**7-12** ポートの設定



ポートの設定ページには、以下のフィールドがあります。

Port（ポート）— ポートパラメータを定義するポートの番号です。

Description (0 - 64 Characters)（説明）（0～64 文字）— Ethernet など、インタフェースの簡単な説明です。

Port Type（ポートタイプ）— ポートのタイプです。

Admin Status（管理ステータス）— 当該のポートを介したトラフィック転送を有効または無効にします。

Current Port Status（現在のポートステータス）— ポートが現在動作可能かどうかを示します。

Reactivate Suspended Port（サスペンドされたポートの再アクティブ化）— ポートロックセキュリティのオプションによってポートが無効になっている場合に、そのポートを再び有効にします。

Operational Status（動作ステータス）— ポートの動作ステータスを示します。可能なフィールド値は以下のとおりです。

Suspended（サスペンド）— ポートは現在アクティブですが、トラフィックの送受信は行っていません。

Active（アクティブ）— ポートは現在アクティブで、トラフィックの送受信を行っています。

Disable（無効）— ポートは現在無効であり、トラフィックの送受信も行っていません。

Admin Speed（管理スピード）— ポートに対して設定されている転送レートです。ポートタイプによって利用可能なスピード設定オプションが異なります。Admin speed（管理スピード）を指定できるのは、ポートが無効になっている場合のみです。

Current Port Speed（現在のポートスピード）— 同期化されている実際のポートスピード（bps）です。The actual synchronized port speed (bps).

Admin Duplex（管理二重モード）— ポートの二重モード（bps）です。**Full**（全二重）は、インタフェースがデバイスとクライアントの間の両方向の同時送信をサポートしていることを示します。**Half**（半二重）は、インタフェースがデバイスとクライアントの間で一度に一方向からの送信のみをサポートしていることを示します。

Current Duplex Mode（現在の二重モード）— 同期化されているポートの二重モードです。

Auto Negotiation（オートネゴシエイション）— ポートに対してオートネゴシエイションを有効にします。オートネゴシエイションは、2つのリンクのパートナー間のプロトコルであり、一方のポートから、その転送レート、二重モード、およびフロー制御の機能を他方に伝えられるようにします。

Current Auto Negotiation（現在のオートネゴシエイション）— 現在のオートネゴシエイションの設定です。

Admin Advertisement（管理アドバタイズメント）— ポートが他方に伝えるオートネゴシエイション設定を定義します。可能なフィールド値は、以下のとおりです。

Max Capability（最大能力）— すべてのポートスピードと二重モードの設定が受け入れられていることを示します。

10 Half（10 mbps 半二重）— ポートが 10 mbps のスピードのポートと半二重モードの設定を他方に伝えることを示します。

10 Full（10 mbps 全二重）— ポートが 10 mbps のスピードのポートと全二重モードの設定を他方に伝えることを示します。

100 Half（100 mbps 半二重）— ポートが 100 mbps のスピードのポートと半二重モードの設定を他方に伝えることを示します。

100 Full（100 mbps 全二重）— ポートが 100 mbps のスピードのポートと全二重モードの設定を他方に伝えることを示します。

1000 Full（1000 mbps 全二重）— ポートが 1000 mbps のスピードのポートと全二重モードの設定を他方に伝えることを示します。

Current Advertisement（現在のアドバタイズメント）— ポートは、ネゴシエイションプロセスを開始するために、隣接ポートにそのスピードを伝えます。可能なフィールド値は、Admin Advertisement（管理アドバタイズメント）フィールドに指定されている値です。

Neighbor Advertisement（近隣アドバタイズメント）— 近隣ポートのアドバタイズメント設定を示します。フィールド値は **Admin Advertisement**（管理アドバタイズメント）フィールドの値と同一です。

Back Pressure（バックプレッシャー）— ポートに対してバックプレッシャーモードを有効にします。バックプレッシャーモードは、半二重モードと併用し、ポートでメッセージを受信できないようにします。バックプレッシャーは OOB ポートではサポートされていません。

Current Back Pressure（現在のバックプレッシャー）— 現在のバックプレッシャーの設定です。

Flow Control（フロー制御）— フロー制御を有効または無効にするか、ポートに対してフロー制御のオートネゴシエイションを有効にします。

Current Flow Control（現在のフロー制御）— 現在のフロー制御の設定です。

MDI/MDIX — デバイスがクロスケーブルとストレートケーブルを判別できるようにします。ハブとスイッチの配線は、故意にエンドステーションの配線と逆にすることで、ハブまたはスイッチをエンドステーションに接続する場合に、ストレートスルー Ethernet ケーブルを使用で

き、ケーブルのペアを適切に組み合わせることができます。2 台のハブまたはスイッチが互いに接続しているか、2 台のエンドステーションが互いに接続している場合、適切なペアが接続されるようにクロスケーブルを使用します。オートネゴシエイションが無効な場合、Auto MDIX は FE ポートで動作しません。可能なフィールド値は、以下のとおりです。

Auto （自動） — ケーブルタイプを自動的に検知するために使用します。

MDIX（Media Dependent Interface with Crossover） — ハブおよびスイッチに使用します。

MDI（Media Dependent Interface） — エンドステーションに使用します。

Current MDI/MDIX（現在の MDI/MDIX） — デバイスの現在の MDIX 設定を示します。可能なフィールド値は、以下のとおりです。

MDI — 現在の MDI 設定は MDI です。

MDIX — 現在の MDI 設定は MDIX です。

LAG — ポートが LAG に属しているかどうかを示します。

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。

ポートパラメータの定義

□□□ ポートの設定ページを開きます。

□□□ **Port**（ポート）フィールドでポートを選択します。

□□□ ダイアログで利用可能なフィールドを定義します。

□□□ **Apply Changes**（変更の適用）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。

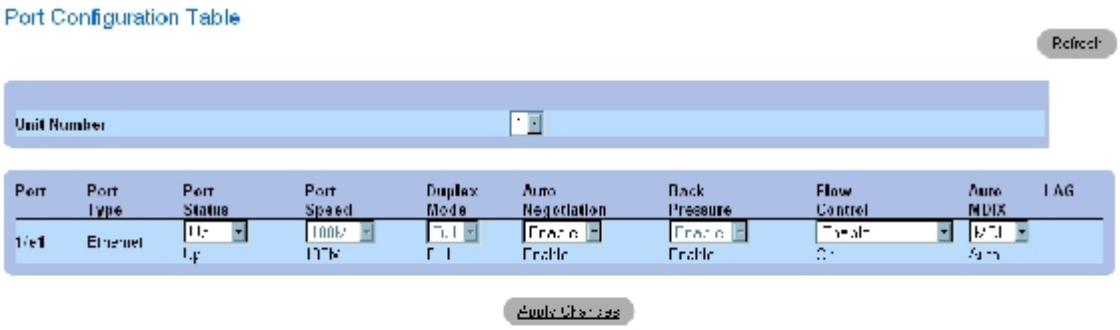
ポート設定表の表示

□□□ ポートの設定ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ポート設定表が開きます。

図**7-13** ポート設定表



CLI コマンドを使用したポート設定

次の表は、 ポートの設定ページに表示されているように、ポートを設定する場合の等価な CLI コマンドをまとめたものです。

表**7-7** ポート設定に関連する **CLI** コマンド

CLI コマンド	説明
interface ethernet *interface*	インタフェース設定モードに入り、Ethernet タイプのインタフェースを設定します。
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内のインタフェースを無効にします。
set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}	セキュリティ上の理由でシャットダウンされたインタフェースを再びアクティブに戻します。
speed *Mbps*	オートネゴシエイションを使用しない場合に、所定の Ethernet インタフェースのスピードを設定します。
duplex {half | full}	オートネゴシエイションを使用しない場合に、所定の Ethernet インタフェースの全二重または半二重動作を設定します。
negotiation [capability1 [capability2...capability5]	所定のインタフェースの speed および duplex パラメータに対してオートネゴシエイション動作を有効にします。
back-pressure	所定のインタフェースに対してバックプレッシャーを有効にします。
flowcontrol {auto | on | off}	所定のインタフェースに対してフロー制御を設定します。
mdix {on | auto}	所定のインタフェースまたはポートチャネルに対して自動クロスオーバーを有効にします。
show interfaces configuration [**ethernet** *interface* | **port-channel** *port-channel-number*]	設定済みのすべてのインタフェースに関する設定を表示します。
show interface advertise	インタフェースのネゴシエイション通知設定を表示します。
show interfaces status [**ethernet** *interface* | **port-channel** *port-channel-number*]	設定済みのすべてのインタフェースに関するステータスを表示します。
show interfaces description [**ethernet** *interface* | **port-channel** *port-channel-number*]	設定済みのすべてのインタフェースに関する説明を表示します。

以下に、CLI コマンドの例を示します。

```
console(config)# interface ethernet 1/e3

console(config-if)# description "RD SW#3"
```

```
console(config-if)# shutdown

console(config-if)# no shutdown

console(config-if)# speed 100

console(config-if)# duplex full

console(config-if)# negotiation

console(config-if)# back-pressure

console(config-if)# flowcontrol on

console(config-if)# mdix auto

console(config-if)# end

console# show interfaces configuration ethernet 1/e3
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
---	---	---	---	---	---	---	---	---
1/e3	100	Full	100	Enabled	On	Up	Enable	Auto

Console# **show interfaces status**

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
---	---	---	---	---	---	---	---	---
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On

Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	---	---	---	---	---	---	---	
1	1000	Full	1000	Off	Off	Disable	Up	

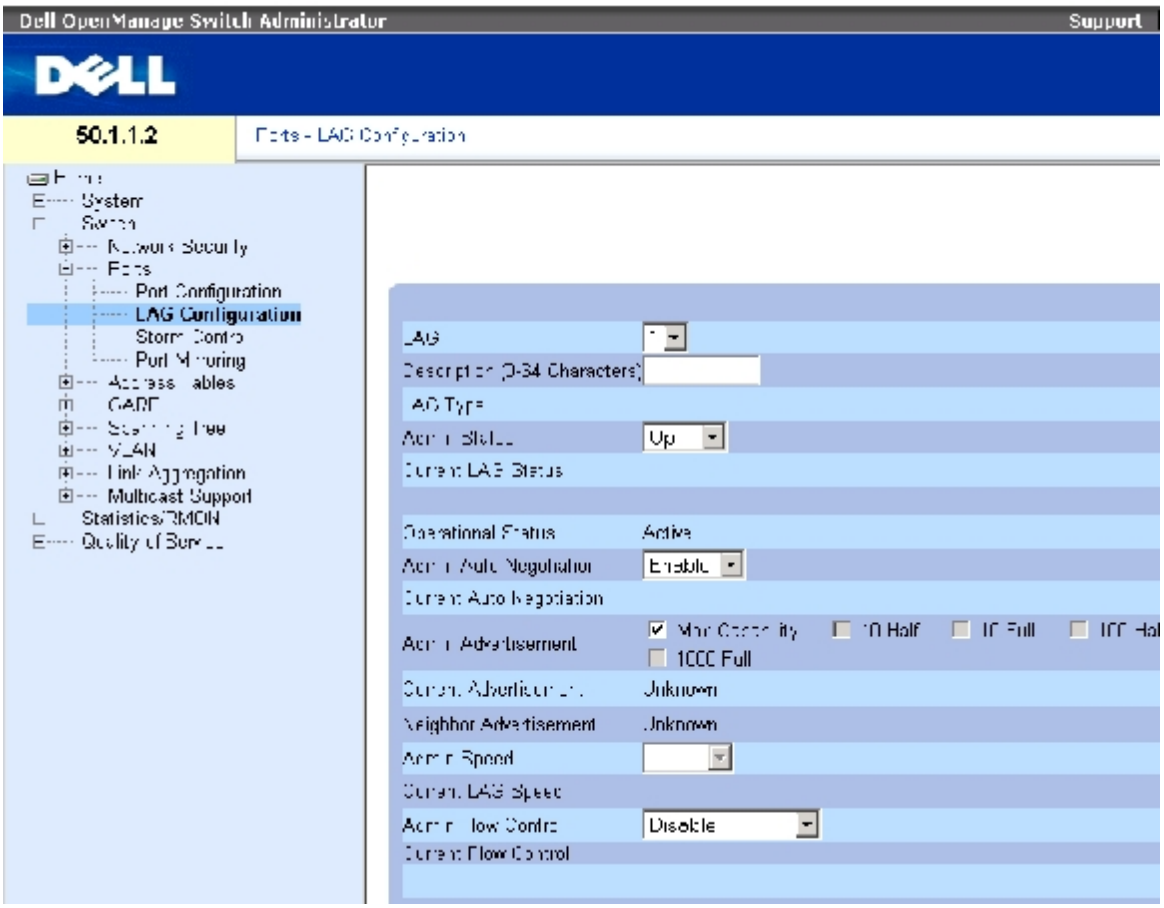
LAG パラメータの定義

LAG の設定ページには、設定済みの LAG に関するパラメータを設定するためのフィールドがあります。デバイスでは、LAG ごとに最大 8 つ

のポートと、システムごとに 8 つの LAG をサポートしています。リンク集約グループ（LAG: Link Aggregated Groups）および、LAG へのポートの割り当てに関しては、ポートの集約を参照してください。

ポートの設定ページを開くには、ツリービューで、Switch（スイッチ）→Ports（ポート）→ LAG Configuration（LAG の設定）の順にクリックします。

図**7-14 LAG** の設定



LAG の設定ページには、以下のフィールドがあります。

LAG — LAG の番号です。

Description (0 - 64 Characters)（説明）（0～64 文字）— 設定済みの LAG に関するユーザー定義の説明を示します。

LAG Type（LAG タイプ）— LAG を構成するポートのタイプです。

Admin Status（管理ステータス）— 選択した LAG を有効または無効にします。

Current LAG Status（現在の LAG ステータス）— LAG が現在動作しているかどうかを示します。

Operational Status（動作ステータス）— 選択した LAG を介したトラフィック転送を有効または無効にします。

Admin Auto Negotiation（管理オートネゴシエイション）— LAG に対してオートネゴシエイションを有効または無効にします。オートネゴシエイションは、リンクのパートナー間のプロトコルであり、一方の LAG からその転送レート、二重モード、およびフロー制御（デフォルトではフロー制御は無効になります）の機能を他方に伝えられるようにします。

Current Auto Negotiation（現在のオートネゴシエイション）— 現在の自動ネゴシエーションの設定です。

Admin Advertisement（管理アドバタイズメント）— LAG が伝えるオートネゴシエイションの設定を定義します。可能なフィールド値は、以下のとおりです。

Max Capability（最大能力）— すべての LAG のスピードと二重モードの設定が受け入れられていることを示します。

10 Half（10 mbps 半二重）— LAG が 10 mbps のスピードのポートと半二重モードの設定を他方に伝えることを示します。

10 Full（10 mbps 全二重）— LAG が 10 mbps のスピードの LAG と全二重モードの設定を他方に伝えることを示します。

100 Half（10 mbps 半二重）— LAG が 100 mbps のスピードのポートと半二重モードの設定を他方に伝えることを示します。

100 Full（10 mbps 全二重）— LAG が 100 mbps のスピードの LAG と全二重モードの設定を他方に伝えることを示します。

1000 Full（10 mbps 全二重）— LAG が 1000 mbps のスピードの LAG と全二重モードの設定を他方に伝えることを示します。

Current Advertisement（現在のアドバタイズメント）— LAG は、ネゴシエイションプロセスを開始するために、隣接 LAG にそのスピードを伝えます。可能なフィールド値は、Admin Advertisement（管理アドバタイズメント）フィールドに指定されている値です。

Neighbor Advertisement（近隣アドバタイズメント）— 近隣 LAG のアドバタイズメント設定を示します。フィールド値は Admin Advertisement（管理アドバタイズメント）フィールドの値と同一です。

Admin Speed — LAG の動作スピードです。

Current LAG Speed（現在の LAG スピード）— 現在設定されている LAG の動作スピードです。

Admin Flow Control（管理フロー制御）— フロー制御を有効または無効にするか、LAG に対してフロー制御のオートネゴシエイションを有効にします。フロー制御モードは、LAG の中で全二重モードで動作するポートに効果があります。

Current Flow Control（現在のフロー制御）— ユーザー指定のフロー制御の設定です。

LAG パラメータの定義

□□□ **LAG** の設定ページを開きます。

□□□ **LAG** フィールドで LAG を選択します。

□□□ フィールドを定義します。

□□□ **Apply Changes**（変更の適用）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 パラメータの変更

□□□ **LAG** の設定ページを開きます。

□□□ **LAG** フィールドで LAG を選択します。

□□□ フィールドを変更します。

□□□ **Apply Changes**（変更の適用）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。

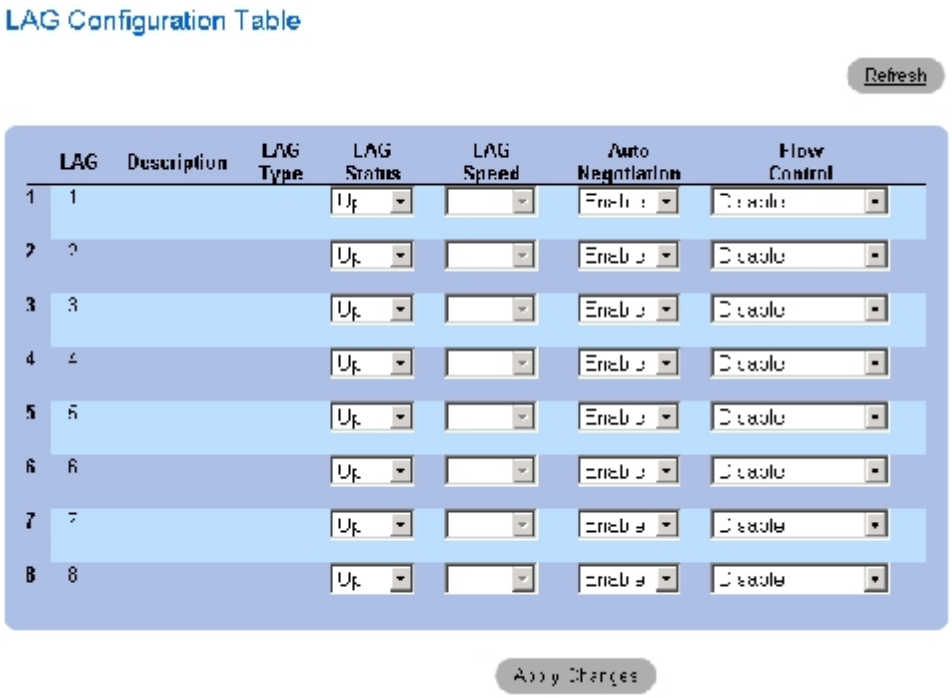
LAG の設定表を表示するには、次の手順を実行します。

□□□ **LAG の設定**ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

LAG の設定表が開きます。

図**7-15 LAG** の設定表



CLI コマンドを使用した LAG 設定

次の表は、 **LAG の設定**ページに表示されているように、LAG を設定する場合の等価な CLI コマンドをまとめたものです。

表**7-8 LAG** の設定に関連する **CLI** コマンド

CLI コマンド	説明
interface port-channel *port-channel-number*	特定のポートチャネルのインタフェース設定モードに入ります。
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内のインタフェースを無効にします。
speed *bps*	オートネゴシエイションを使用しない場合に、所定の Ethernet インタフェースのスピードを設定します。
negotiation [capability1 [capability2...capability5]	インタフェースのオートネゴシエイション動作を有効にします。

back-pressure	所定のインタフェースに対してバックプレッシャーを有効にします。
flowcontrol {auto | on | off }	所定のインタフェースに対してフロー制御を設定します。
show interfaces configuration [**ethernet** *interface*| **port-channel** *port-channel-number*]	設定済みのすべてのインタフェースに関する設定を表示します。
show interfaces status [**ethernet** *interface* | **port-channel** *port-channel-number*]	設定済みのすべてのインタフェースに関するステータスを表示します。
show interfaces description [**ethernet** *interface* | **port-channel** *port-channel-number*]	設定済みのすべてのインタフェースに関する説明を表示します。
show interfaces port-channel [*port-channel-number*]	ポートチャネル情報（どのポートが当該のポートチャネルのメンバーであるか、また、それらのポートが現在アクティブかどうか）を表示します。

以下に、CLI コマンドの例を示します。

```
console(config)# interface port-channel 2

console(config-if)# no negotiation

console(config-if)# speed 100

console(config-if)# flowcontrol on

console(config-if)# exit

console(config)# interface port-channel 3

console(config-if)# shutdown

console(config-if)# exit

console(config)# interface port-channel 4

console(config-if)# back-pressure

console(config-if)# description p4

console(config-if)# end

console# show interfaces port-channel
```

Channel	Ports
---------	---------
ch1	Inactive:1/e(11-13)
ch2	Active:1/e14

ストーム制御の有効化

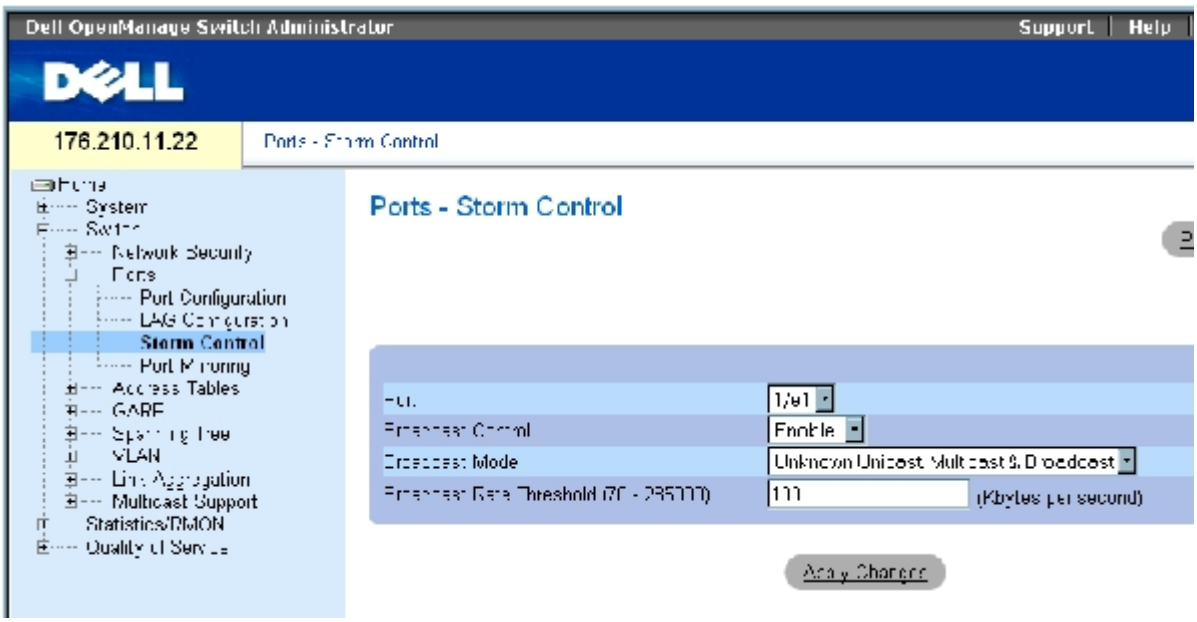
ブロードキャストストームは、単一のポートからネットワーク上に過剰な量のブロードキャストメッセージが同時に送信された場合に発生します。送信されたメッセージの応答がネットワークに蓄積され、ネットワークリソースの不足やネットワークのタイムアウトが発生します。

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、ポートごとに有効になります。

システムでは、ポートごとに着信したブロードキャスト、ユニキャスト、およびマルチキャストのフレームレートを個別に測定し、そのレートがユーザー定義のレートを超えた場合にフレームを破棄します。

ストーム制御ページには、ストーム制御を有効にして設定するためのフィールドがあります。ストーム制御ページを開くには、ツリービューでSwitch（スイッチ）→ Ports（ポート） Storm Control （ストーム制御）の順にクリックします。

図**7-16** ストーム制御



ストーム制御ページには、以下のフィールドがあります。

Port（ポート）— ストーム制御を有効にするポートです。

Broadcast Control（ブロードキャスト制御）— 特定のインタフェースに対してブロードキャストパケットタイプの転送を有効または無効にします。

Broadcast Mode（ブロードキャストモード）— デバイスまたはスタック上で現在有効になっているブロードキャストモードを示します。可能なフィールド値は、以下のとおりです。

Unknown Unicast, Multicast & Broadcast（未知のユニキャスト、マルチキャスト、およびブロードキャスト）— ユニキャスト、マルチキャスト、ブロードキャストのトラフィックを計数します。

Multicast & Broadcast（マルチキャストおよびブロードキャスト）— ブロードキャストおよびマルチキャストのトラフィックを一緒に計数します。

Broadcast Only（ブロードキャストのみ）— ブロードキャストトラフィックのみを計数します。

Broadcast Rate Threshold (70-285000)（ブロードキャストレートのしきい値）（70～285000）— 未知のパケットが転送される最大速度（1 秒あたりのキロバイト数）です。フィールド値の範囲は、70～285000 kBps です。

ストーム制御の有効化

□□□ ストーム制御ページを開きます。

□□□ ストーム制御を実装するインタフェースを選択します。

□□□ フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

ストーム制御が有効になります。

ストーム制御ポートパラメータの変更

□□□ ストーム制御ページを開きます。

□□□ フィールドを変更します。

□□□ **Apply Changes**（変更の適用）をクリックします。

ストーム制御ポートパラメータがデバイスに保存されます。

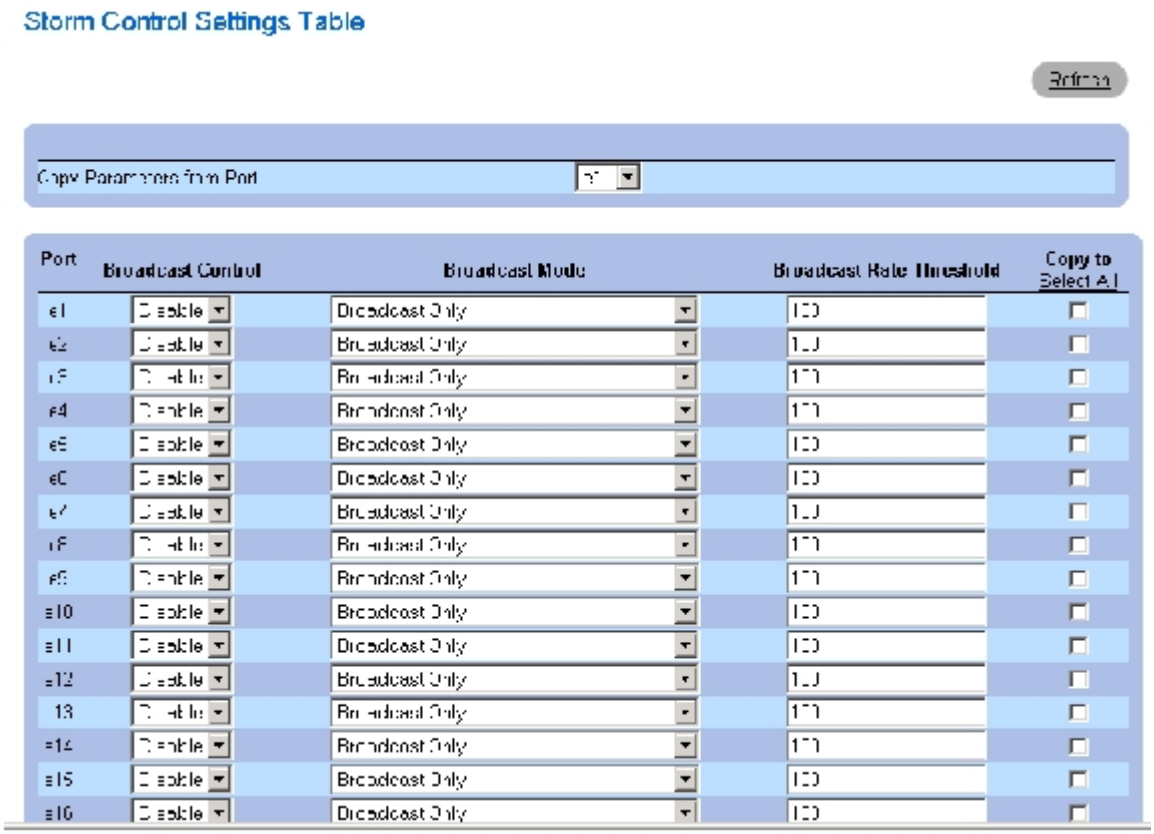
ポートパラメータ表の表示

□□□ ストーム制御ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ストーム制御の設定表が開きます。

図**7-17** ストーム制御の設定表



ストーム制御ページ内のフィールドのほかに、ストーム制御の設定表には以下の追加フィールドが含まれています。

Copy Parameters from Port（パラメータのコピー元のポート）— ストーム制御パラメータのコピー元である特定のポートを示します。

ストーム制御の設定表のパラメータのコピー

□□□ ストーム制御ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ストーム制御の設定表が開きます。

□□□ **Copy Parameters from Port** （パラメータのコピー元のポート）フィールドから、設定 をコピーするポートを選択します。

□□□ **Copy to**（コピー先）チェックボックスにチェックマークを付けて、ストーム制御の定 義のコピー先となるインタフェースを定義するか、**Select All**（すべてを選択）をク リックして、すべてのポートに定義をコピーします。

□□□ **Apply Changes**（変更の適用）をクリックします。

パラメータがストーム制御の設定表の選択したポートにコピーされ、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ストーム制御の設定

次の表は、 ストーム制御ページに表示されているように、ストーム制御を設定する場合の等価な CLI コマンドをまとめたものです。

表**7-9** ストーム制御に関連する **CLI** コマンド

CLI コマンド	説明
`port storm-control include-multicast`	デバイスが、マルチキャスト、ユニキャスト、およびブロードキャストのパケットを一緒に計数できるようにします。
`port storm-control broadcast enable`	ブロードキャストストーム制御を有効にします。
`port storm-control broadcast rate`	最大のブロードキャストレートを設定します。
`show ports storm-control` *port*	ストーム制御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)# port storm-control include-multicast

console(config)# interface ethernet 1/e1

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

console(config-if)# port storm-control broadcast rate 100000

console(config-if)# end

console# show ports storm-control
```

Port	Broadcast Storm control [kbyes/sec]
1/e1	8000
2/e1	Disabled
3/e2	Disabled

ポートミラーリングセッションの定義

ポートミラーリング

- ある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することによって、ネットワークトラフィックの監視とミラーリングを行います。
- 診断ツールやデバッグ機能として使用できます。

デバイスのパフォーマンスと監視を有効にします。

ポートミラーリングを設定するには、すべてのパケットをコピーする特定のポートと、パケットのコピー元となる別のポートを選択します。

ポートミラーリングを設定する前に、次の点に注意してください。

- ポートミラーリングは、監視対象のポートから監視する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リングを行います。
- 監視対象のポートは、監視す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。

宛先ポートとして設定されているポートには、次の制限が適用されます。

- ポートを送信元ポートとして設定できません。
- ポートは LAG メンバーにはなれません。
- ポートに対して IP インタフェースは設定されません。
- ポートに対して GVRP は無効になります。
- ポートは VLAN のメンバーにはなれません。
- 1 つの宛先ポートだけしか定義できません。

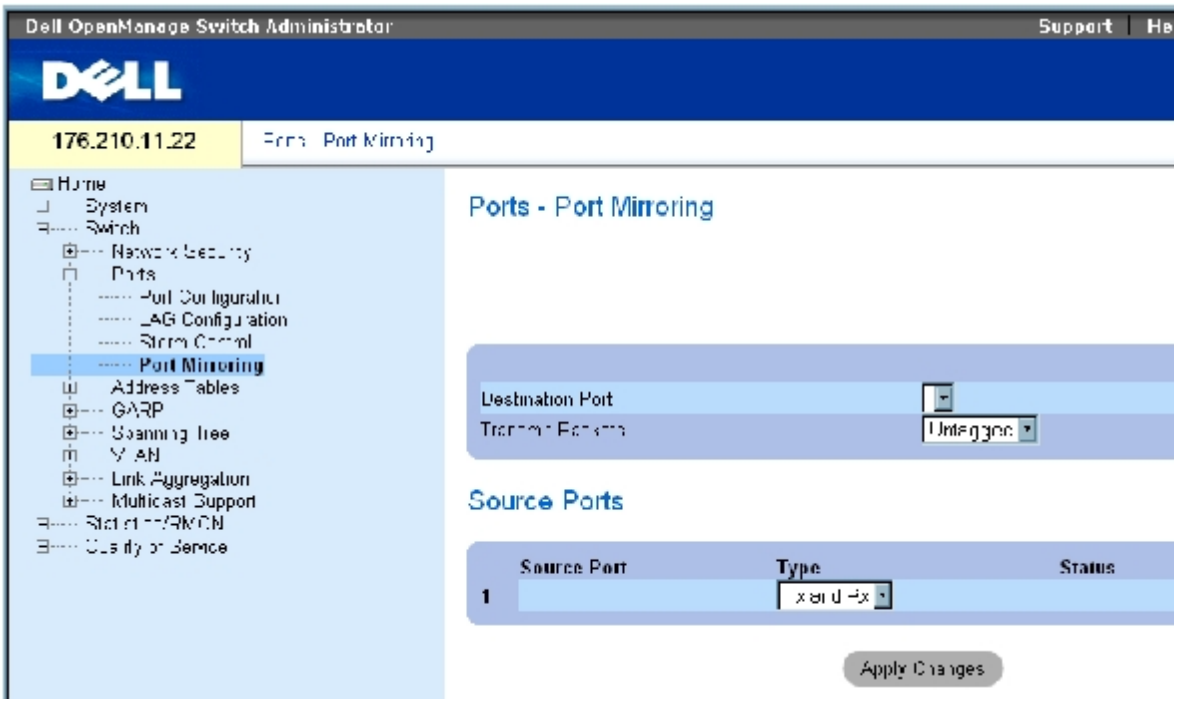
送信元ポートとして設定されているポートには、以下の制限が適用されます。

- 送信元ポートは LAG のメンバーにはなれません。
- ポートを宛先ポートとして設定できません。
- 送信元ポートの数は 8 つまでサポートされています。

ポートミラーリングページを開くには、ツリービューで **Switch**（スイッチ）→ **Ports**（ポート）→ **Port Mirroring**（ポートミラーリング）の順にクリックします。

メモ： ポートをポートミラーリングセッションのターゲットポートとして設定すると、 そのポートに関するすべての通常動作がサスペンドされます。この動作には、スパニングツ リーおよび LACP も含まれます。

図**7-18** ポートミラーリング



ポートミラーリングページには、以下のフィールドがあります。

Destination Port（宛先ポート）— ポートトラフィックのコピー先となるポートの番号です。

Transmit Packets （送信パケット）— パケットをミラーリングする方法を定義します。可能なフィールド値は、以下のとおりです。

Untagged（タグなし）— パケットをタグなしの vlan パケットとしてミラーリングします。これがデフォルト値です。

Tagged （タグ付き）— パケットをタグ付きの vlan パケットとしてミラーリングします。

Type（タイプ）— ミラーリングされたパケットが、RX、TX、または RX と TX の両方のいずれであるかを示します。

Status（ステータス）— ポートが現在監視されているか（アクティブ）、監視されていないか（監視可能）を示します。

Remove（削除）— この項目を選択すると、ポートミラーリングセッションが削除されます。

ポートミラーリングセッションの追加

□□□ ポートミラーリング ページを開きます。

□□□ **Add**（追加）をクリックします。

送信元ポートの追加ページが開きます。

□□□ **Source Port**（送信元ポート）と **Type**（タイプ）フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

□□□ **Destination Port** （宛先ポート）ドロップダウンメニューから宛先ポートを選択しま す。

□□□ **Refresh**（表示の更新）ボタンのポートミラーリング ページをクリックします。

□□□ **Tagged Packets**（タグ付きパケット）フィールドを定義します。

□□□ **Type**（タイプ）フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

新規の送信元ポートが定義され、デバイスがアップデートされます。

ポートミラーリングセッションからのコピーポート削除

□□□ ポートミラーリングページを開きます。

□□□ **Remove**（削除）チェックボックスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択したポートミラー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ーリングセッションの設定

次の表は、ポートミラーリングページに表示されているように、ポートミラーリングセッションを設定する場合の等価な CLI コマンドをまとめたものです。

表**7-10** ポートミラーリングに関連する **CLI** コマンド

CLI コマンド	説明
port monitor *src*-interface [**rx** | **tx**]	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/e2

console (config-if)# end

console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
----------	----------	----------	----------	----------
1/e2	1/e1	RX, TX	Active	No

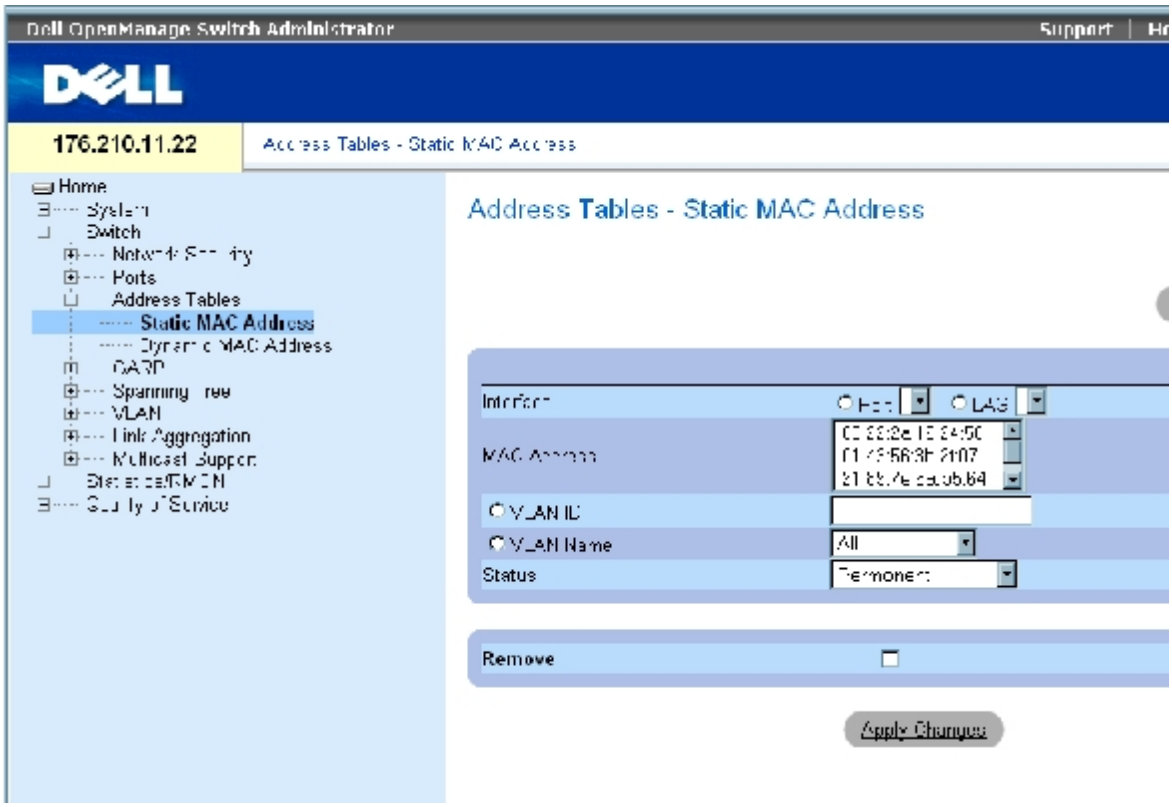
アドレス表の設定

MAC アドレスは、静的アドレスまたは動的アドレスデータベースに保存されます。いずれかのデータベースに保存されている宛先に指定されたパケットは、ただちにその宛先ポートに転送されます。動的アドレス表は、インタフェース、VLAN、および MAC アドレスによってソートできます。MAC アドレスは、パケットが送信元からデバイスに到達した時点で動的に学習されます。フレームの送信元アドレスからポートを学習することによって、アドレスがポートに関連付けられます。いずれのポートにも関連付けられていない MAC アドレスが宛先に指定されているフレームは、関連する VLAN のすべてのポートに送信されます。静的アドレスは手動で設定します。ブリッジ表が満杯にならないようにするため、一定の期間にトラフィックが送信されなかった動的 MAC アドレスは消去されます。アドレス表ページを開くには、ツリービューで **Switch**（スイッチ）→**Address Tables**（アドレス表）の順にクリックします。

静的アドレスの定義

静的 MAC アドレス表ページには、静的 MAC アドレスの一覧があります。静的 MAC アドレス表ページでは静的アドレスの追加と削除を行うことができます。また、複数の MAC アドレスを単一のポートに定義することもできます。静的 MAC アドレス表ページを開くには、ツリービューで **Switch** （スイッチ）→**Address Tables**（アドレス表）→**Static Address Table**（静的アドレス表）の順にクリックします。

図**7-19** 静的 **MAC** アドレス表



静的 MAC アドレス表ページには、以下のフィールドがあります。

Interface（インタフェース）— 静的 MAC アドレスが適用される特定のポートまたは LAG です。

MAC Address（MAC アドレス）— 現在の静的アドレスの一覧に登録されている MAC アドレスです。

VLAN ID — MAC に割り当てられている VLAN ID です。

VLAN Name（VLAN 名）— ユーザー定義の VLAN 名です。

Status（ステータス）— MAC アドレスのステータスです。可能な値は以下のとおりです。

Secure（保護）— ロックされているポートの静的 MAC アドレスの定義に使用します。

Permanent（永続的）— 当該の MAC アドレスは永続的です。

Delete on Reset（リセット時に削除）— MAC アドレスは、デバイスをリセットすると削除されます。

Delete on Timeout（タイムアウト時に削除）— MAC アドレスは、タイムアウトが発生すると削除されます。

メモ： Ethernet デバイスのリセット時に静的 MAC アドレスが削除されることを防ぐに は、MAC アドレスに接続されているポートがロックされていることを確認してくださ い。

Remove（削除）— この項目を選択すると、選択した MAC アドレスが MAC アドレス表から削除されます。

静的 **MAC** アドレスの追加

□□□ 静的 MAC アドレス表ページを開きます。

□□□ **Add**（追加）をクリックします。

静的 **MAC** アドレスの追加ページが開きます。

□□□ フィールドを完了します。

□□□ **Apply Changes**（変更の適用）をクリックします。

新規の静的アドレスが静的 **MAC** アドレス表に追加され、デバイスがアップデートされます。

静的 **MAC** アドレス表にある静的アドレス設定の変更

□□□ 静的 MAC アドレス表ページを開きます。

□□□ インタフェースを選択します。

□□□ フィールドを変更します。

□□□ **Apply Changes**（変更の適用）をクリックします。

静的 MAC アドレスが変更され、デバイスがアップデートされます。

静的アドレス表にある静的アドレスの削除

□□□ 静的 MAC アドレス表ページを開きます。

□□□ インタフェースを選択します。

□□□ **Show All**（すべてを表示）をクリックします。

静的 **MAC** アドレス表 が開きます。

□□□ 表のエントリを選択します。

□□□ **Remove**（削除）チェックボックスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択した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

次の表は、 静的 MAC アドレス表 ページに表示されているように、静的アドレスパラメータを設定する場合の等価な CLI コマンドをまとめたものです。

表**7-11** 静的アドレスに関連する **CLI** コマンド

CLI コマンド	説明
bridge address *mac-address* [permanent | delete-on-reset | delete-on-timeout | secure] {ethernet interface | port-channel *port-channel-number*}	静的 MAC 層の送信元ステーションアドレスをブリッジ表に追加します。
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のエントリを表示します。

以下に、CLI コマンドの例を示します。

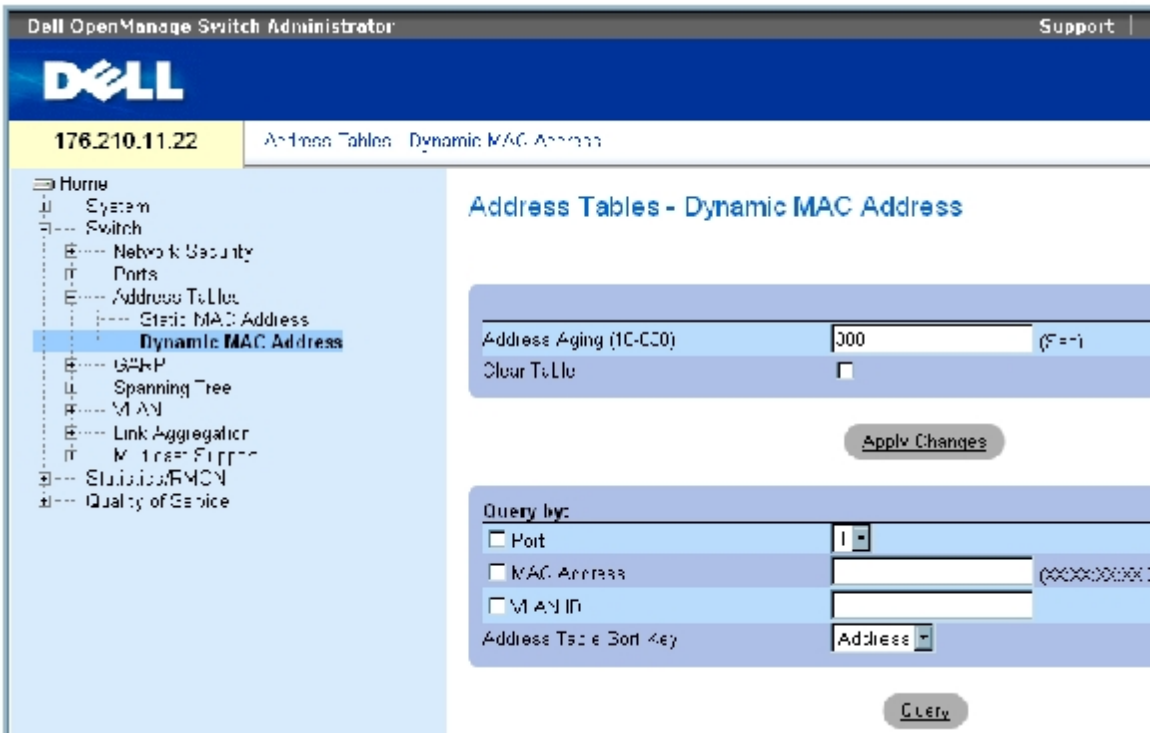
```
console(config-if)#bridge address 00:60:70:4C:73:FF permanent ethernet g8

console# show bridge address-table

Aging time is 300 sec

vlan    mac address          port    type
----    -----------          ----    --------
1       00:60:70:4C:73:FF    1/e8    dynamic
1       00:60:70:8C:73:FF    1/e8    dynamic
200     00:10:0D:48:37:FF    1/e9    static
```

動的アドレスの表示

動的 **MAC** アドレスには、インタフェースタイプ、MAC アドレス、VLAN、および表のソートなど、動的アドレス表内の情報をクエリするための情報があります。アドレス表に保存されているアドレスが指定されたパケットは、そのアドレスのポートに直接転送されます。 動的 **MAC** アドレスページには、動的 MAC アドレスが消去されるまでのエージング時間の情報と、動的アドレスの一覧をクエリおよび表示するためのパラメータがあります。現在のアドレス表には、パケットが直接ポートに転送されるように指示する動的アドレスパラメータがあります。

動的 **MAC** アドレスページを開くには、ツリービューで **Switch**（スイッチ）→**Address Tables**（アドレス表）→**Dynamic MAC Address**（動的 MAC アドレス）の順にクリックします。

図**7-20** 動的 **MAC** アドレス



動的 MAC アドレスページには、以下のフィールドがあります。

Address Aging (10-630)（アドレスエージング）（10～630）— MAC アドレスが動的 MAC アドレスに留まる時間を指定します。この時間を過ぎても、その送信元からのトラフィックが検知されない場合、その MAC アドレスはタイムアウトになります。デフォルト値は 300 秒です。

Clear Table（表のクリア）— これがチェックされると、動的アドレス表がクリアされます。

Port（ポート）— 表にクエリするインタフェースを指定します。2 つのインタフェースタイプから選択します。

MAC Address（MAC アドレス）— 表にクエリする MAC アドレスを指定します。

VLAN ID — 表にクエリする VLAN ID です。

Address Table Sort Key（アドレス表ソートキー）— 動的アドレス表をソートする方法を指定します。アドレス表は、アドレス、VLAN、またはインタフェースでソートできます。

エージング時間の再定義

□□□ 動的 MAC アドレスを開きます。

□□□ **Aging Time**（エージング時間）フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

エージング時間が変更され、デバイスがアップデートされます。

動的アドレス表へのクエリ

□□□ MAC

動的　　アドレスを開きます。

□□□ **Dynamic Address Table**（動的アドレス表）にクエリするパラメータを定義します。

エントリは、ポート、**MAC** アドレス、または **VLAN ID** を基準としてクエリできます。

□□□ **Query**（クエリ）をクリックします。

動的 MAC アドレスがクエリされます。

動的アドレス表のソート

□□□ 動的 **MAC** アドレスを開きます。

□□□ **Address Table Sort Key**（アドレス表ソートキー）ドロップダウンメニューで、アドレ スのソート基準をアドレス、VLAN ID、インタフェースから選択します。

□□□ **Query**（クエリ）をクリックします。

動的 MAC アドレスがソートされます。

CLI コマンドを使用した動的アドレスのクエリとソート

次の表は、動的 MAC アドレスに表示されているように、動的アドレスのエージング、クエリ、ソートを行う場合の等価な CLI コマンドをまとめたものです。

表**7-12** クエリおよびソートに関連する **CLI** コマンド

CLI コマンド	説明
bridge aging-time *seconds*	アドレス表のエージング時間を設定します。
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内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)# end

console# show bridge address-table

Aging time is 250 sec

vlan  mac address        port  type
----  -----------        ----  ----
1     00:60:70:4C:73:FF  1/e8  dynamic
```

1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e8	static

GARP の設定

GARP（Generic Attribute Registration Protocol）は、ネットワーク接続またはメンバーシップスタイルの情報を登録する一般用のプロトコルです。GARP は、VLAN やマルチキャストアドレスなど、所定のネットワーク属性に関係する一組のデバイスを定義します。

GARP を設定する際には、次の点を確認してください。

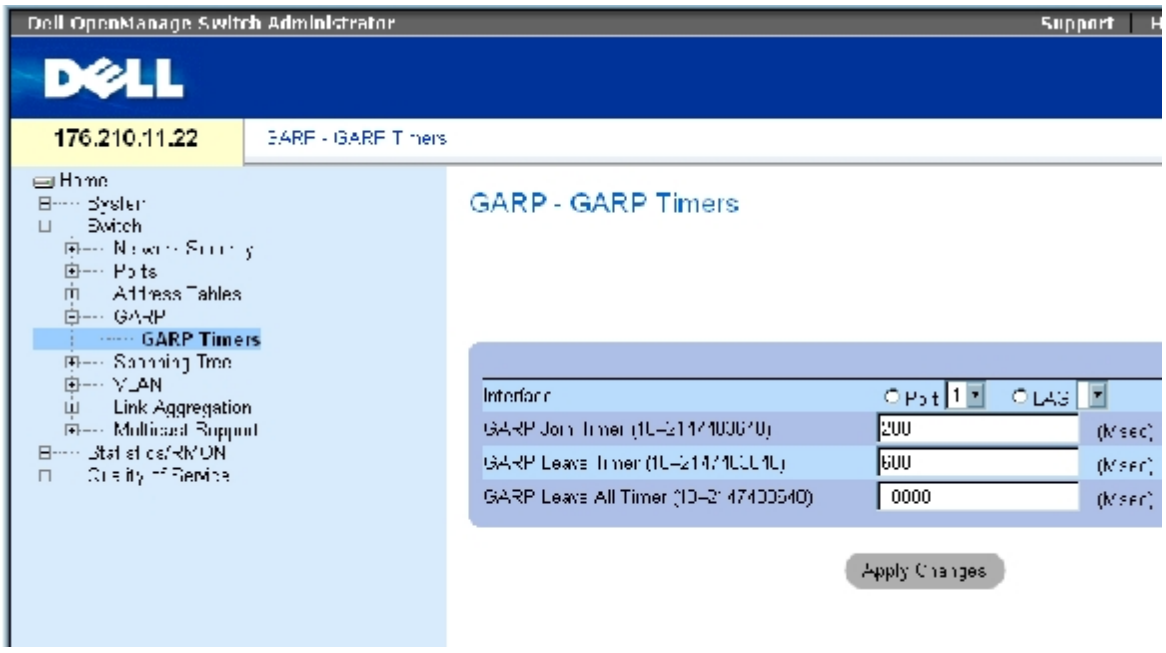
- Leave 時間は、Join 時間の 3 倍以上にする必要があります。
- Leave All 時間は Leave 時間より長くする必要があります。
- すべてのレイヤー 2 接続デバイスに対して同一の GARP タイマー値を設定してください。レイヤー 2 接続デバイスにそれぞれ異なる GARP タイマーを設定すると、GARP アプリケーションが正常に動作しません。

GARP ページを開くには、ツリービューで **Switch**（スイッチ）→ **GARP** の順にクリックします。

GARP タイマーの定義

GARP タイマーページには、デバイスに対して GARP を有効にするためのフィールドがあります。GARP タイマーページを開くには、ツリービューで **Switch**（スイッチ）→ **GARP** → **GARP Timers**（GARP タイマー）の順にクリックします。

図**7-21 GARP** タイマー



GARP タイマーページには、以下のフィールドがあります。

Interface （インタフェース）— GARP タイマーの編集用にポートまたは LAG を選択します。

GARP Join Timer (10 - 2147483640)(Msec)（GARP Join タイマー）（10～2147483640）— PDU が転送される時間（ミリ秒単位）です。デフォルト値は 200 ミリ秒です。

GARP Leave Timer (10 - 2147483640) (Msec)（GARP Leave タイマー）（10～2147483640）— デバイスが GARP 状態から離れるまでに待機する時間（ミリ秒単位）です。Leave 時間は、Leave All Time メッセージの送受信によってアクティブになり、Join メッセージの受信によって取り消されます。Leave 時間は、Join 時間の 3 倍以上にする必要があります。デフォルト値は 600 ミリ秒です。

GARP Leave All Timer (10 - 2147483640)(Msec)（GARP Leave All タイマー）（10～2147483640）— すべてのデバイスが GARP 状態を離れるまでに待機する時間（ミリ秒単位）です。Leave All 時間は Leave 時間より長くする必要があります。デフォルト値は 10000 ミリ秒です。

GARP タイマーの定義

□□□ GARP タイマーページを開きます。

□□□ インタフェースを選択します。

□□□ フィールドを完了します。

□□□ **Apply Changes**（変更の適用）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 タイマー表へのパラメータのコピー

□□□ GARP タイマーページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

GARP タイマー表が開きます。

□□□ **Copy Parameters from** （パラメータのコピー元）フィールドでインタフェースタイプ を選択します。

□□□ **Port**（ポート）または **LAG** ドロップダウンメニューからインターフェイスを選択しま す。

このインタフェースに対する定義が、選択したインタフェースにコピーされます。手順 6 を参照してください。

□□□ **Copy to**（コピー先）チェックボックスをオンにして、GARP タイマーの定義をコピー するインタフェースを定義するか、**Select All**（すべて選択）をクリックして、すべて のポートまたは LAG に定義をコピーします。

□□□ **Apply Changes**（変更の適用）をクリックします。

パラメータが **GARP** タイマー表で選択したポートまたは LAG にコピーされ、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 GARP タイマーの定義

次の表は、GARP タイマーページに表示されているように、GARP タイマーを定義する場合の等価な CLI コマンドをまとめたものです。

表**7-13 GARP** タイマーに関連する **CLI** コマンド

CLI コマンド	説明
garp timer {join | leave | leaveall} *timer_value*	GARP タイマーにおける GARP アプリケーションの Join、Leave、および Leaveall 値を調整します。

以下に、CLI コマンドの例を示します。

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

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet 1/e11


GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port(s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
1/e11	Disabled	Normal	Enabled	200	900	10000

スパニングツリープロトコルの設定

スパニングツリープロトコル（STP）は、ブリッジの配置に関係なくツリー構造を提供します。また、ネットワーク上のエンドステーション間に 1 つのパスを提供し、ループを排除します。

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。拡張ネットワークにループが発生すると、ブリッジはトラフィックを無制限に転送するため、トラフィックが増加し、ネットワークの効率が低下します。

デバイスでは、次のスパニングツリーバージョンをサポートしています。

- 標準 STP— エンドステーション間に 1 つのパスを提供し、ループを回避および排除します。標準 STP の設定の詳細については、**STP グローバル設定の定義**を参照してください。
- 高速 STP— 転送ループを作成せずに、スパニングツリーをより迅速に収束できるネットワークトポロジを検知して使用します。デバイスに対して RSTP が有効になっていても、近隣のデバイスの STP が有効になっている場合、ローカルデバイスは STP を使用します。

  高速 STP の設定の詳細については、高速スパニングツリーの設定を参照してください。
- 多重 STP— 任意の VLAN に割り当てたパケットに対し、完全な接続を提供します。多重 STP は RSTP に基づいています。また、多重 STP は異なる MST 領域を通じて、異なる VLAN に割り当てたパケットを送信します。デバイスに対して MSTP が有効になっている場

合、MST 領域は単一のブリッジとして動作します。ただし、近隣のデバイスに対して RSTP が有効になっており、ローカルデバイスが STP、RSTP、および MSTP を使用する場合は、両方のデバイスが同時に使用できます。

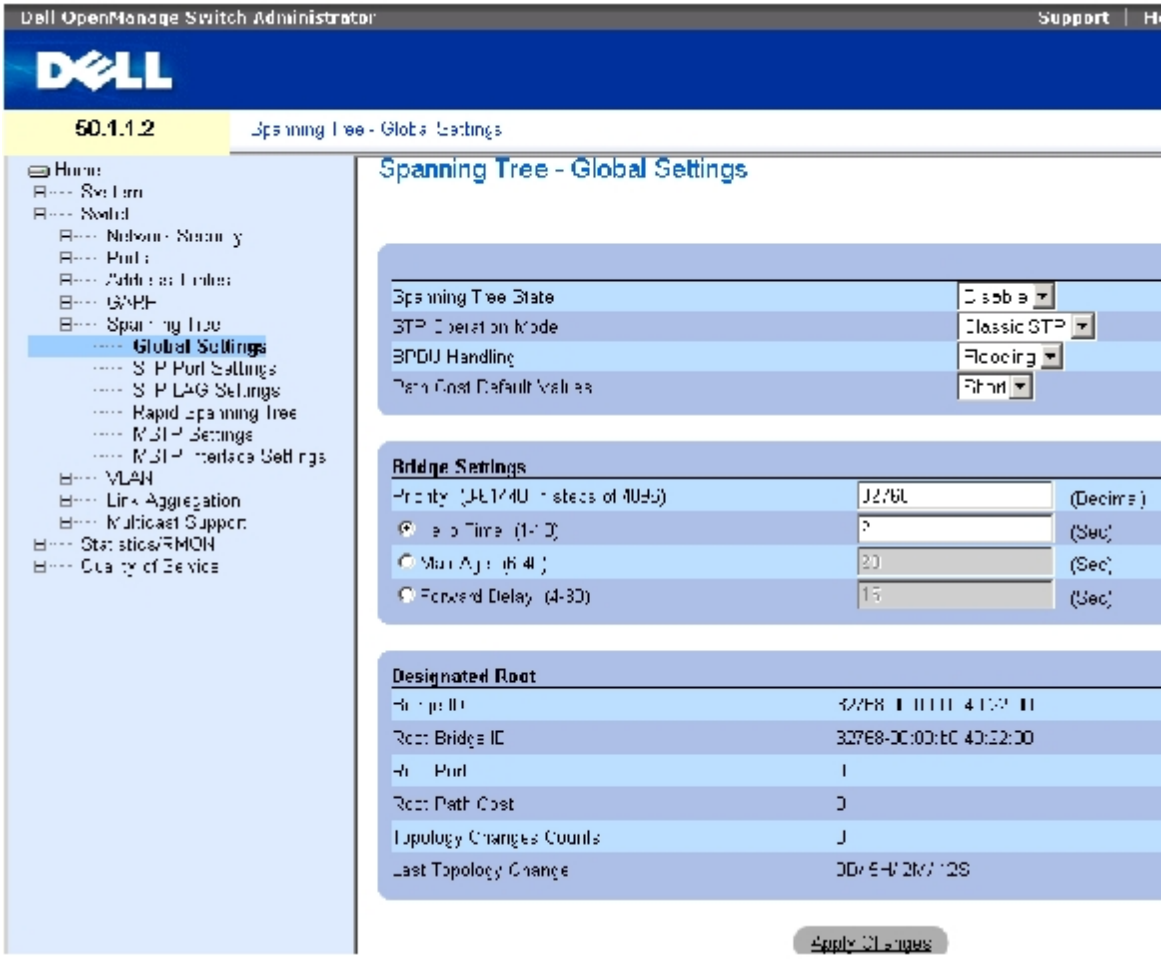
多重 STP の設定の詳細については、多重スパニングツリーを参照してください。

スパニングツリーページを開くには、ツリービューで **Switch**（スイッチ）→ **Spanning Tree** （スパニングツリー）の順にクリックします。

STP グローバル設定の定義

スパニングツリーのグローバル設定ページには、デバイスに対して STP を有効に設定するためのパラメータがあります。スパニングツリーのグローバル設定 ページを開くには、ツリービューで **Switch**（スイッチ）→ **Spanning Tree**（スパニングツリー）→ **Global Settings**（グローバル設定）の順にクリックします。

図**7-22** スパニングツリーのグローバル設定



スパニングツリーのグローバル設定ページには、以下のフィールドがあります。

Spanning Tree State（スパニングツリーの状態）— デバイスに対して STP、高速 STP、または MSTP を有効または無効にします。

STP Operation Mode（STP 動作モード）— デバイスに対して有効にする STP のモードです。可能なフィールド値は、以下のとおりです。

Classic STP（標準 STP）— デバイスに対して標準 STP を有効にします。これがデフォルト値です。

Rapid STP（高速 STP）— デバイスに対して高速 STP を有効にします。

Multiple STP（多重 STP）— デバイスに対して多重 STP を有効にします。

BPDU Handling（BPDU 処理）— ポートまたはデバイスに対して STP が無効である場合に、BPDU パケットを管理する方法を決定します。BPDU は、スパニングツリー情報の送信に使用します。可能なフィールド値は、以下のとおりです。

Filtering（フィルタリング）— インタフェースに対してスパニングツリーが無効である場合に、BPDU パケットをフィルタにかけます。これがデフォルト値です。

Flooding（フラッディング）— インタフェースに対してスパニングツリーが無効である場合に、BPDU パケットをフラッディングします。

Path Cost Default Values（パスコストのデフォルト値）— STP ポートにデフォルトパスコストを割り当てるために使用する方法を指定します。可能なフィールド値は、以下のとおりです。

Short（ショート）— ポートのパスコストに 1～65,535 の範囲を指定します。これがデフォルト値です。

Long（ロング）— ポートのパスコストに 1～200,000,000 の範囲を指定します。

インタフェースに割り当てるデフォルトパスコストは、選択する方法によって異なります。

インタフェース	ロング	ショート
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

Priority (0-65535)（優先度）（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 を実行している場合は、それぞれに優先度が割り当てられます。BPDU を交換した後、優先度の最も低いスイッチがルートブリッジになります。デフォルト値は 32768 です。ポート優先度値は、4096、8192、12288 などのように 4096 の倍数で指定します。

Hello Time (1-10)（ハロー時間）（1～10）— デバイスのハロー時間を指定します。ハロー時間は、設定メッセージ間でルートブリッジが待機する秒単位の時間です。デフォルト値は 2 秒です。

Max Age (6-40)（最大エージ）（6～40）— デバイスの最大エージ時間を指定します。最大エージ時間は、設定メッセージ間を送信するまでにブリッジが待機する秒単位の時間です。デフォルトの最大エージは 20 秒です。

Forward Delay (4-30)（転送遅延）（4～30）— デバイスの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、リスニング状態と学習状態でいる秒単位の時間です。デフォルト値は 10 秒です。

Bridge ID（ブリッジ ID）— ブリッジ優先度と MAC アドレスを識別します。

Root Bridge ID（ルートブリッジ ID）— ルートブリッジ優先度と MAC アドレスを識別します。

Root Port（ルートポート）— このブリッジからルートブリッジに最低コストのパスを提供するポート番号です。この設定は、ブリッジがルートでない場合に重要です。

Root Path Cost（ルートパスコスト）— このブリッジからルートへのパスコストです。

Topology Changes Counts（トポロジ変更カウント）— 発生した STP 状態の変化の合計を示します。

Last Topology Change（前回のトポロジ変更）— ブリッジが初期化またはリセットされ、最後にトポロジ変更が発生してからの経過時間です。この時間は、2D/5H/10M/4S のように日 / 時間 / 分 / 秒の書式で表示されます。

STP グローバルパラメータの定義

□□□ ページを開きます。

□□□ **Spanning Tree State**（スパニングツリーの状態）フィールドで**Enable**（有効）を選択し ます。

□□□ **STP Operation Mode**（STP 動作モード）フィールドで **STP** モードを選択し、ブリッジ の設定を定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

デバイスに対して STP が有効になります。

STP グローバルパラメータの変更

□□□ ページを開きます。

□□□ ダイアログ内のフィールドを定義します。

□□□ **Apply Changes**（変更の適用）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

次の表は、 スパニングツリーのグローバル設定ページに表示されているように、STP グローバルパラメータを定義する場合の等価な CLI コマンドをまとめたものです。

表**7-14 STP** グローバルパラメータに関連する **CLI** コマンド

CLI コマンド	説明
spanning-tree	スパニングツリー機能を有効にします。
spanning-tree mode {**stp** | **rstp** | **mstp**}	スパニングツリープロトコルのモードを設定します。
spanning-tree priority priority	スパニングツリー優先度を設定します。
spanning-tree hello-time *seconds*	スパニングツリーブリッジのハロー時間を設定します。ハロー時間は、デバイスが他のデバイスにハローメッセージをブロードキャストする頻度です。
spanning-tree max-age *seconds*	スパニングツリーブリッジの最大エージを設定します。
spanning-tree forward- time seconds	スパニングツリーブリッジの転送遅延時間を設定します。転送遅延時間は、ポートが転送状態に入るまでにリスニング状態および学習状態でいる時間です。
show spanning-tree [**ethernet** *interface* | **port-**	スパニングツリーの設定を表示します。

channel *port- channel-number*] [**instance** *instance-id*]	
show spanning-tree [**detail**] [**active** | **blockedports**] [**instance** *instance-id*]	アクティブポートまたはブロックポートに関する詳細なスパニングツリー情報を表示します。
show spanning-tree mst- configuration	スパニングツリー MST 設定の識別子を表示します。

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 12

console(config)# spanning-tree forward-time 25

console(config)# exit

console# show spanning-tree
```

Spanning tree enabled mode MSTP							
Default port cost method:short							
Gathering information							
###### MST 0 Vlans Mapped:			16-4094				
CST Root ID Priority 20480							
	Address		00:30:ab:00:00:08				
	Path Cost		4				
	Root Port		ch2				
	This switch is the IST master						
	Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec						
Bridge ID Priority			32768				
	Address		00:00:00:16:00:64				
	Max hops		20				
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-----	-------	----	---	----	-------	----
1/e2	enabled	128.2	100	DSBL	Dsbl	No	P2p Intr

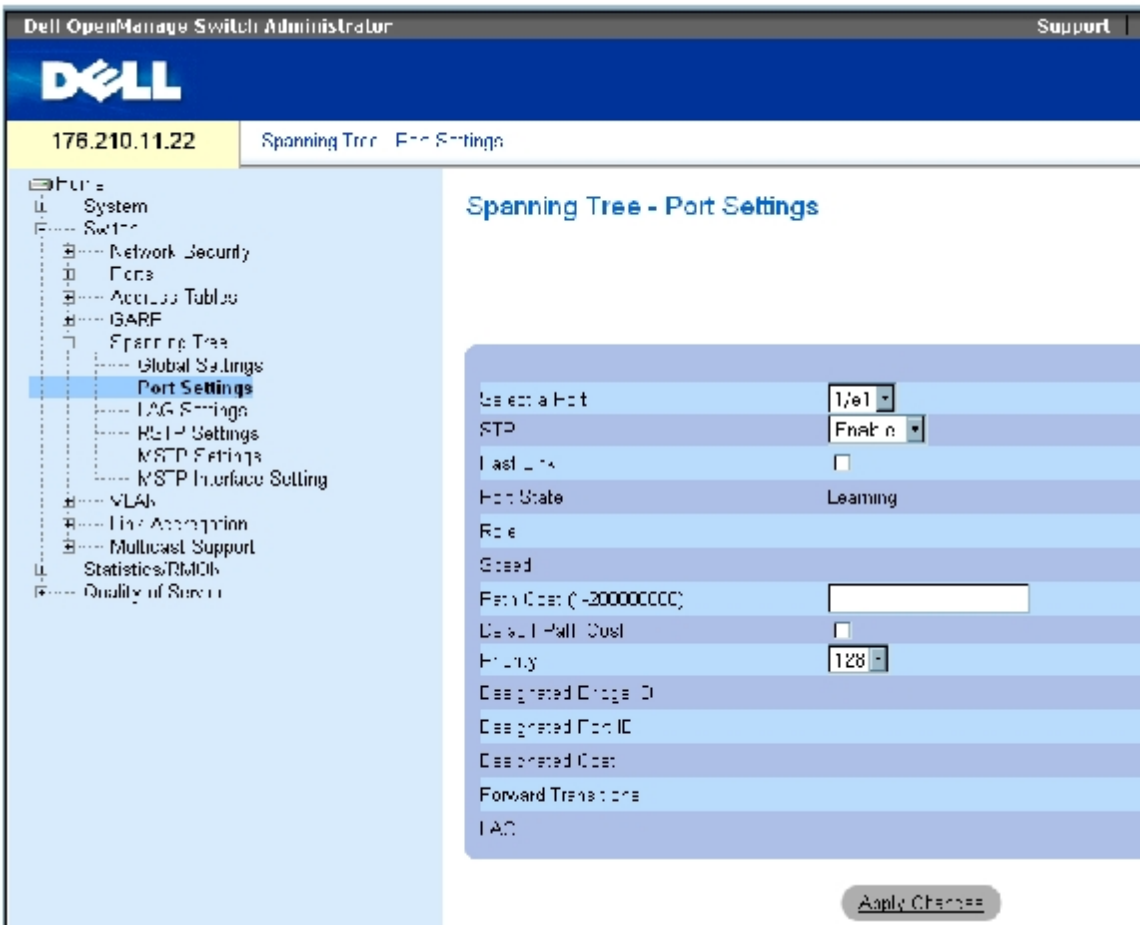
1/e3	enabled	128.3	100	DSBL	Dsbl	No	P2p Intr
1/e4	enabled	128.4	100	DSBL	Dsbl	No	P2p Intr
1/e5	enabled	128.5	19	FRW	Desg	Yes	P2p Intr
1/e6	enabled	128.6	100	DSBL	Dsbl	No	P2p Intr
1/e7	enabled	128.7	100	DSBL	Dsbl	No	P2p Intr
1/e8	enabled	128.8	100	DSBL	Dsbl	No	P2p Intr
1/e9	enabled	128.9	100	DSBL	Dsbl	No	P2p Intr
1/e10	enabled	128.10	100	DSBL	Dsbl	No	P2p Intr
1/e11	enabled	128.11	19	DSBL	Desg	Yes	P2p Intr
console# show spanning-tree active							
Spanning tree enabled mode MSTP							
Default port cost method:short							
Gathering information							
###### MST 0 Vlans Mapped: 16-4094							
CST Root ID Priority 20480							
	Address		00:30:ab:00:00:08				
	Path Cost		4				
	Root Port		ch2				
	This switch is the IST master						
	Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec						
Bridge ID Priority			32768				
	Address		00:00:00:16:00:64				
	Max hops		20				
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-----	-------	----	---	----	-------	----
1/e5	enabled	128.2	19	FRW	Desg	Yes	P2p Intr
1/e7	enabled	128.7	19	DSCR	Altn	No	P2p Bound (STP)
1/e11	enabled	128.11	19	FRW	Desg	Yes	P2p Intr
1/e15	enabled	128.15	19	FRW	Desg	No	P2p Intr

1/e22	enabled	128.22	19	FRW	Desg	Yes	P2p Intr

STP ポート設定の定義

スパニングツリーポート設定ページを使用して、STP プロパティを個々のポートに割り当てます。スパニングツリーポート設定ページを開くには、ツリービューで **Switch**（スイッチ）→ **Spanning Tree**（スパニングツリー）→ **Port Settings**（ポート設定）の順にクリックします。

図**7-23** スパニングツリーポートの設定



スパニングツリーポート設定ページには、以下のフィールドがあります。

Select a Port （ポートの選択）— STP 設定を修正するポート番号を指定します。

STP — ポートに対して STP を有効または無効にします。

Fast Link （高速リンク）— この項目をチェックすると、ポートに対して高速リンクモードが有効になります。ポートに対して高速リンクモードを有効にすると、ポートリンクが動作している場合、ポート状態が自動的に転送状態になります。高速リンクモードは、STP プロトコルによる収束の所要時間を最適化します。STP の収束には、大規模なネットワークでは 30～60 秒かかる場合があります。

Port State（ポート状態）— 現在のポートの STP 状態を示します。この項目を有効にすると、ポート状態によって、トラフィックに対する転送処置が決まります。可能なポート状態は以下のとおりです。

Disabled（無効）— STP は現在ポートに対して無効になっています。ポートは MAC アドレスを学習しながらトラフィックを転送し

ます。

Blocking（ブロッキング）— ポートは現在ブロックされていて、トラフィックの転送や MAC アドレスの学習に使用することができません。ブロッキングは、標準 STP が有効である場合に表示されます。

Listening（リスニング）— ポートは現在リスニングモードに入っていて、トラフィックを転送することも、MAC アドレスを学習することもできません。

Learning（学習）— ポートは現在学習モードに入っていて、トラフィックを転送することはできませんが、新規の MAC アドレスを学習することはできます。

Forwarding（転送）— ポートは現在転送モードに入っていて、トラフィックを転送することも、新規の MAC アドレスを学習することもできます。

Role（役割）— STP パスを提供するために STP アルゴリズムによって割り当てられるポートの役割を示します。可能なフィールド値は、以下のとおりです。

Root（ルート）— パケットをルートスイッチに転送する最低コストのパスを提供します。

Designated（指定）— 指定されているスイッチから LAN への接続に使用されているポートを示します。

Alternate（代替）— ルートインタフェースからルートスイッチへの代替パスを提供します。

Backup（バックアップ）— スパニングツリーリーフへの指定ポートパスに対するバックアップパスを提供します。バックアップポートは、2 つのポートがポイントツーポイントリンクでループ接続している場合にのみ提供されます。また、LAN で 2 つ以上のポートが共有セグメントに接続している場合にも、バックアップポートが提供されます。

Disabled（無効）— ポートがスパニングツリーに参加していないことを示します。

Speed（スピード）— ポートの動作スピードです。

Path Cost (1-200000000)（パスコスト）（1～200000000）— ルートパスコストに対するポートのコントリビューションです。パスコストの値を大きく、または小さくして、パスのルートが再指定されたときにトラフィックの転送に使用されるようにします。

Default Path Cost（デフォルトのパスコスト）— デフォルトのパスコスト。ロングパスコストのデフォルト値は、以下のとおりです。

Ethernet - 2,000,000

Fast Ethernet - 200,000

Gigabit Ethernet - 20,000

ショートパスコストのデフォルト値は、以下のとおりです。

Ethernet -100

Fast Ethernet -19

Gigabit Ethernet -4

Priority (0-240, in steps of 16)（優先度）（0～240、16 刻み）— ポートの優先度値です。ループ接続された 2 つのポートがブリッジに存在する場合、優先度値がポートの選択に影響します。優先度値の範囲は 0～240 で、16 刻みで指定します。

Designated Bridge ID（指定ブリッジ ID）— 指定ブリッジのブリッジ優先度および MAC アドレスです。

Designated Port ID（指定ポート ID）— 指定されているポートの優先度およびインタフェースです。

Designated Cost（指定コスト）— STP トポロジに参加するポートのコストです。コストの低いポートほど、STP でループが検知された場合にブロックされにくくなります。

Forward Transmission（転送への推移）— ポートが転送状態からブロック状態に変化した回数です。

LAG — ポートが属している LAG です。

ポートに対する **STP** の有効化

□□□ スパニングツリーポートの設定ページを開きます。

□□□ ポートを選択します。

□□□ **STP** フィールドで **Enabled**（有効）を選択します。

□□□ **Fast Link**（高速リンク）、**Path Cost**（パスコスト）、および **Priority**（優先度）フィー ルドを定義します。

□□□ **Apply Changes**（変更の適用）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の変更

□□□ スパニングツリーポートの設定ページを開きます。

□□□ ポートを選択します。

□□□ 関連するフィールドを変更します。

□□□ **Apply Changes**（変更の適用）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 ポート表の表示

□□□ スパニングツリーポートの設定ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

STP ポート表が開きます。

CLI コマンドを使用した**STP** ポート設定の定義

次の表は、 **STP** ポートの設定ページに表示されているように、STP ポートパラメータを定義する場合の等価な CLI コマンドをまとめたもの

です。

表**7-15 STP** ポートの設定に関連する **CLI** コマンド

CLI コマンド	説明
`spanning-tree disable`	特定のポートに対してスパニングツリーを無効にします。
`spanning-tree cost cost`	ポートのスパニングツリーコストのコントリビューションを設定します。
`spanning-tree port-priority priority`	ポートの優先度を設定します。
`show spanning-tree [ethernet interface | port-channel port-channel- number][instance` *`instance- id`*`]`	スパニングツリーの設定を表示します。
`spanning-tree portfast`	PortFast モードを有効にします。
`show spanning-tree [detail] [active | blockedports] [instance` *`instance-id`*`]`	アクティブポートまたはブロックポートに関する詳細なスパニングツリー情報を表示します。
`show spanning-tree mst- configuration`	スパニングツリー MST 設定の識別子を表示します。

以下に、CLI コマンドの例を示します。

```
console> enable

console# configure

Console(config)# interface ethernet 1/e1

Console(config-if)# spanning-tree disable

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

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

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree ethernet 1/e15
```

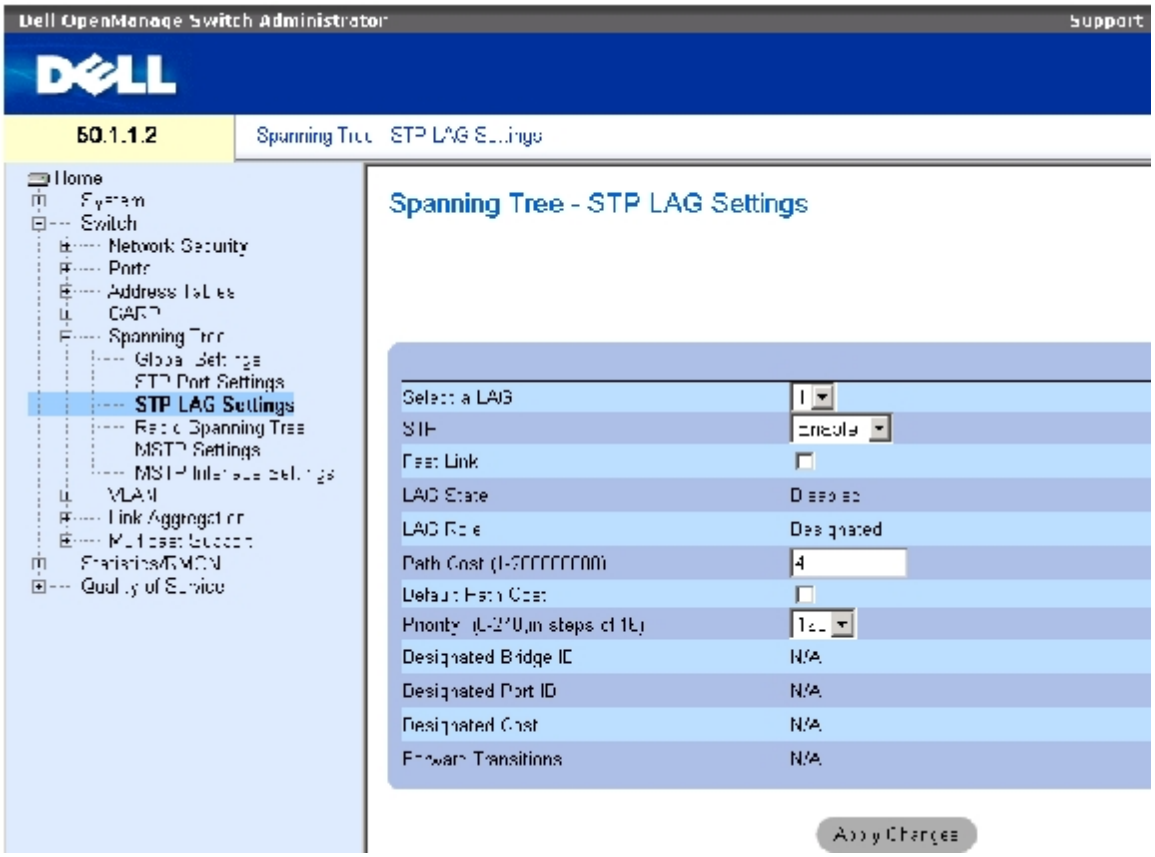
Port 1/e15 enabled					
State:forwarding			Role:designated		
Port id: 128.15			Port cost: 19		
Type:P2p (configured: Auto) Internal Port Fast: No (configured: No)					
Designated bridge Priority : 32768			Address: 00:00:00:16:00:64		
Designated port id: 128.15			Designated path cost: 4		

Guard root:Disabled						
Number of transitions to forwarding state: 2						
BPDU:sent 483, received 1037						
console# **show spanning-tree ethernet** 1/e15 **instance** 12						
Port 1/e15 enabled						
State:discarding				Role:alternate		
Port id: 128.15				Port cost: 19		
Type:P2p (configured:Auto) Internal Port Fast:No (configured:No)						
Designated bridge Priority : 32768				Address:00:00:b0:07:07:49		
Designated port id: 128.11				Designated path cost: 0		
Guard root:Disabled						
Number of transitions to forwarding state: 3						
BPDU:sent 482, received 1035						

STP LAG 設定の定義

スパニングツリー LAG の設定ページを使用して、STP ポート集約パラメータを割り当てます。スパニングツリー LAG の設定ページを開くには、ツリービューで **Switch**（スイッチ）→ **Spanning Tree**（スパニングツリー）→ **LAG Settings**（LAG の設定）の順にクリックします。

図**7-24** スパニングツリー **LAG** の設定



スパニングツリー LAG の設定ページには、以下のフィールドがあります。

Select a LAG（LAG の選択）— STP 設定を変更する LAG 番号です。

STP — LAG に対して STP を有効または無効にします。

Fast Link（高速リンク）— LAG に対して高速リンクモードが有効になります。LAG に対して高速リンクモードを有効にすると、LAG が動作している場合、**LAG State**（LAG 状態）が自動的に転送状態になります。高速リンクモードは、STP プロトコルによる収束の所要時間を最適化します。STP の収束には、大規模なネットワークでは 30～60 秒かかる場合があります。

LAG State（LAG 状態）— LAG の現在の STP 状態です。この項目を有効にすると、LAG 状態によって、トラフィックに対する転送処理が決まります。正常に機能しない LAG がブリッジで検出されると、その LAG は故障状態になります。可能な LAG 状態は以下のとおりです。

Disabled（無効）— STP は現在 LAG に対して無効になっています。LAG は MAC アドレスを学習しながらトラフィックを転送します。

Blocking（ブロッキング）— LAG は現在ブロックされていて、トラフィックの転送や MAC アドレスの学習に使用することができません。

RSTP Discarding State（RSTP 廃棄状態）— この状態では、ポートは MAC アドレスを学習せず、フレームの転送も行いません。

この状態は、STP（802.1.D）に導入されているブロック状態とリスニング状態を組み合わせたものです。

Listening（リスニング）— LAG はリスニングモードに入っていて、トラフィックを転送することも、MAC アドレスを学習することもできません。

Learning（学習）— LAG は学習モードに入っていて、トラフィックを転送することはできませんが、新規の MAC アドレスを学習することはできます。

Forwarding（転送）— LAG は現在転送モードに入っていて、トラフィックを転送することも、新規の MAC アドレスを学習することもできます。

Broken（故障）— LAG は現在誤動作しており、トラフィックの転送に使用できません。

LAG Role（LAG の役割）— STP パスを提供する STP アルゴリズムによって割り当てられた LAG の役割を示します。可能なフィールド値は、以下のとおりです。

Root（ルート）— パケットをルートスイッチに転送する最低コストのパスを提供します。

Designated（指定）— LAN に接続している指定スイッチが経由する LAG を示します。

Alternate（代替）— ルートインタフェースからルートスイッチへの代替 LAG を提供します。

Backup（バックアップ）— スパニングツリーのリーフへの指定ポートパスに対するバックアップパスを提供します。バックアップポートは、2 つのポートがポイントツーポイントリンクでループ接続している場合にのみ提供されます。また、LAN で 2 つ以上のポートが共有セグメントに接続している場合にも、バックアップポートが提供されます。

Disabled（無効）— LAG がスパニングツリーに参加していないことを示します。

Path Cost (1-200000000)（パスコスト）（1～200000000）— ルートパスコストに対する LAG のコントリビューションの量です。パスコストの値を大きく、または小さくして、パスのルートが再指定されたときにトラフィックの転送に使用されるようにします。パスコストには、1～200000000 の値があります。

Default Path Cost（デフォルトのパスコスト）—デフォルトのパスコストが使用されているかどうかを示します。LAG パスコストの可能なデフォルト値は、次のとおりです。

LAG 用のロング方式 — **20,000**

LAG 用のショート方式 — 4

Priority (0-240, in steps of 16)（優先度）（0～240、16 刻み） — LAG の優先度値です。ループ接続されたポートがブリッジに存在する場合、優先度値は LAG の選択に影響します。優先度値は 0～240 の間で、16 刻みです。

Designated Bridge ID（指定ブリッジ ID）— 指定ブリッジの優先度および MAC アドレスです。

Designated Port ID（指定ポート ID）— 選択したインタフェースの ID です。

Designated Cost（指定コスト）— STP トポロジに参加するポートのコストです。コストの低いポートほど、STP でループが検知された場合にブロックされにくくなります。

Forward Transitions（転送への推移）— **LAG** 状態が転送状態からブロック状態に変化した回数です。

LAG STP パラメータの変更

□□□ スパニングツリー **LAG** の設定 ページを開きます。

□□□ **Select a LAG**（LAG の選択）ドロップダウンメニューから LAG を選択します。

□□□ 必要に応じてフィールドを変更します。

□□□ **Apply Changes**（変更の適用）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。

CLI コマンドを使用した STP LAG 設定の定義

次の表は、STP LAG 設定を定義する CLI コマンドをまとめたものです。

表**7-16 STP LAG** の設定に関連する **CLI** コマンド

CLI コマンド	説明
`spanning-tree`	スパニングツリーを有効にします。
`spanning-tree disable`	特定の LAG に対してスパニングツリーを無効にします。
`spanning-tree cost` *`cost`*	スパニングツリーコストに対する LAG のコントリビューションを設定します。
`spanning-tree port-priority` *`priority`*	ポートの優先度を設定します。
`show spanning-tree [`**`ethernet`** `interface |` **`port-channel`** *`port-channel- number`*`][`**`instance`** *`instance- id`*`]`	スパニングツリーの設定を表示します。
`show spanning-tree [detail] [active | blockedports] [`**`instance`** *`instance-id`*`]`	アクティブポートまたはブロックポートに関する詳細なスパニングツリー情報を表示します。

以下に、CLI コマンドの例を示します。

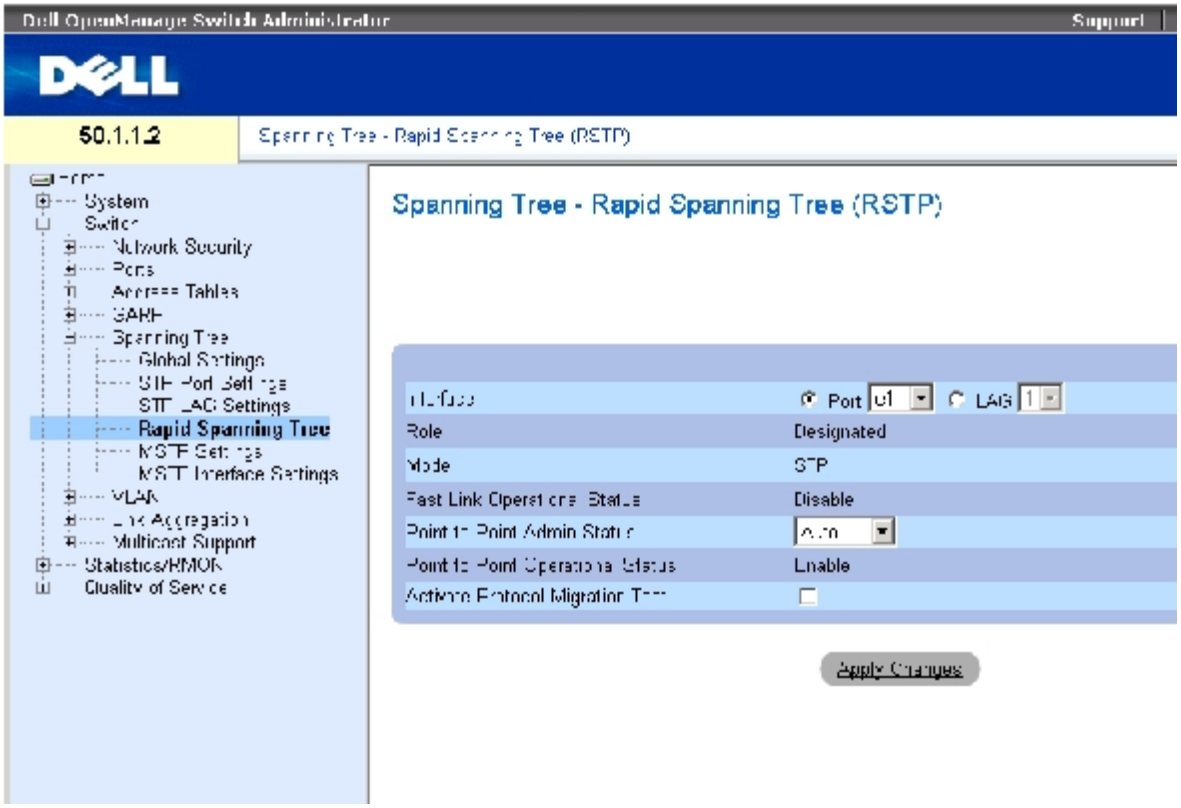
```
console(config)# interface
port-channel 1

console(config-if)#
spanning-tree disable

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

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

console(config-if)#
spanning-tree portfast
```

高速スパニングツリーの設定

標準スパニングツリーでは、一般的なネットワークトポロジにおけるレイヤー 2 転送ループが防止されますが、収束に最大 30～60 秒かかる場合があります。この収束時間に、ループがあれば検出し、ステータスの変更を伝えることができます。

高速スパニングツリープロトコル（RSTP: Rapid Spanning Tree Protocol）は、転送ループを作成せずに、スパニングツリーをより迅速に収束できるネットワークトポロジを検知して使用します。高速スパニングツリー（RSTP）設定ページを開くには、ツリービューで **Switch**（スイッチ）→ **Spanning Tree**（スパニングツリー）→**Rapid Spanning Tree** （高速スパニングツリー）の順にクリックします。

図**7-25** 高速スパニングツリー（**RSTP**）の設定



スパニングツリー RSTP ページには、以下のフィールドがあります。

Interface （インタフェース）— RSTP 設定を表示して編集できるポートまたは LAGです。

State （状態）— 選択したインタフェースの RSTP 状態を無効にします。

Role（役割）— STP パスを提供するために STP アルゴリズムによって割り当てられるポートの役割を示します。可能なフィールド値は、以下のとおりです。

Root（ルート）— パケットをルートスイッチに転送する最低コストのパスを提供します。

Designated（指定）— 指定されているスイッチから LAN への接続に使用されているポートまたは LAG を示します。

Alternate（代替）— ルートインタフェースからルートスイッチへの代替パスを提供します。

Backup（バックアップ）— スパニングツリーのリーフへの指定ポートパスに対するバックアップパスを提供します。バックアップポートは、2 つのポートがポイントツーポイントリンクでループ接続している場合にのみ提供されます。また、LAN で 2 つ以上のポートが共有セグメントに接続している場合にも、バックアップポートが提供されます。

Disabled（無効）— ポートがスパニングツリーに参加していないことを示します。

Mode（モード）— 現在のスパニングツリーモードを示します。スパニングツリーモードは、スパニングツリーのグローバル設定ページで選択します。可能なフィールド値は、以下のとおりです。

Classic STP（標準 STP）— デバイスに対して標準STP が有効であることを示します。

Rapid STP（高速 STP）— デバイスに対して高速 STP が有効であることを示します。

Multiple STP（多重 STP）— デバイスに対して多重 STP が有効であることを示します。

Fast Link Operational Status（高速リンクの動作状態）— ポートまたは LAG に対して高速リンクが有効か無効かを示します。インタフェースに対して高速リンクが有効である場合、インタフェースは自動的に転送状態になります。

Point-to-Point Admin Status（ポイントツーポイント管理ステータス）— デバイスによるポイントツーポイントリンクの確立を有効または無効にするか、デバイスがポイントツーポイントリンクを自動的に確立するように指定します。

ポイントツーポイントリンクを介した通信を確立するには、送信元の PPP がまず Link Control Protocol（LCP）パケットを送信してデータリンクを設定およびテストします。リンクが確立され、必要に応じて LCP によるオプション機能のネゴシエーションが行われると、送信元の PPP は、1 つまたは複数のネットワーク層プロトコルを選択して設定するために Network Control Protocol（NCP）パケットを送信します。選択された各ネットワーク層プロトコルが設定されると、各ネットワーク層プロトコルからのパケットはリンクを介して送信可能になります。明示的な LCP または NCP パケットがリンクを閉じるか、何らかの外部イベントが発生するまで、リンクは通信用に設定されたままになります。このリンクが、実際のスイッチポートリンクタイプになります。このリンクの状態は、管理状態とは異なる場合があります。

Point-to-Point Operational Status（ポイントツーポイントの動作ステータス）— ポイントツーポイントの動作状態です。

Activate Protocol Migrational（アクティブプロトコルのマイグレーションテスト）— この項目を選択すると、PPP が Link Control Protocol（LCP）パケットを送信してデータリンクの設定およびテストを可能にします。

RSTP パラメータの定義

□□□ スパニングツリー RSTP の設定ページを開きます。

□□□ インタフェースを選択します。

□□□ フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

RSTP 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。

高速スパニングツリー（RSTP）表の表示

□□□ 高速スパニングツリー（RSTP）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

高速スパニングツリー（**RSTP**）表が開きます。

CLI コマンドを使用した高速 STP パラメータの定義

次の表は、高速スパニングツリー（RSTP）に表示されているように、高速 STP パラメータを定義する場合の等価な CLI コマンドをまとめたものです。

表**7-17 RSTP** の設定に関連する **CLI** コマンド

CLI コマンド	説明
	デフォルトのリンクタイプ設定を置き換え

`spanning-tree link-type {point-to-point | shared}`	ます。
`spanning tree mode {stp | rstp | mstp}`	現在実行中のスパニングツリープロトコルを設定します。
`clear spanning-tree detected-protocols [ethernet interface | port-channel port- channel-number]`	プロトコル移行処理を再開します。
`show spanning-tree [ethernet interface | port-channel port- channel-number]`	スパニングツリーの設定を表示します。

以下に、CLI コマンドの例を示します。

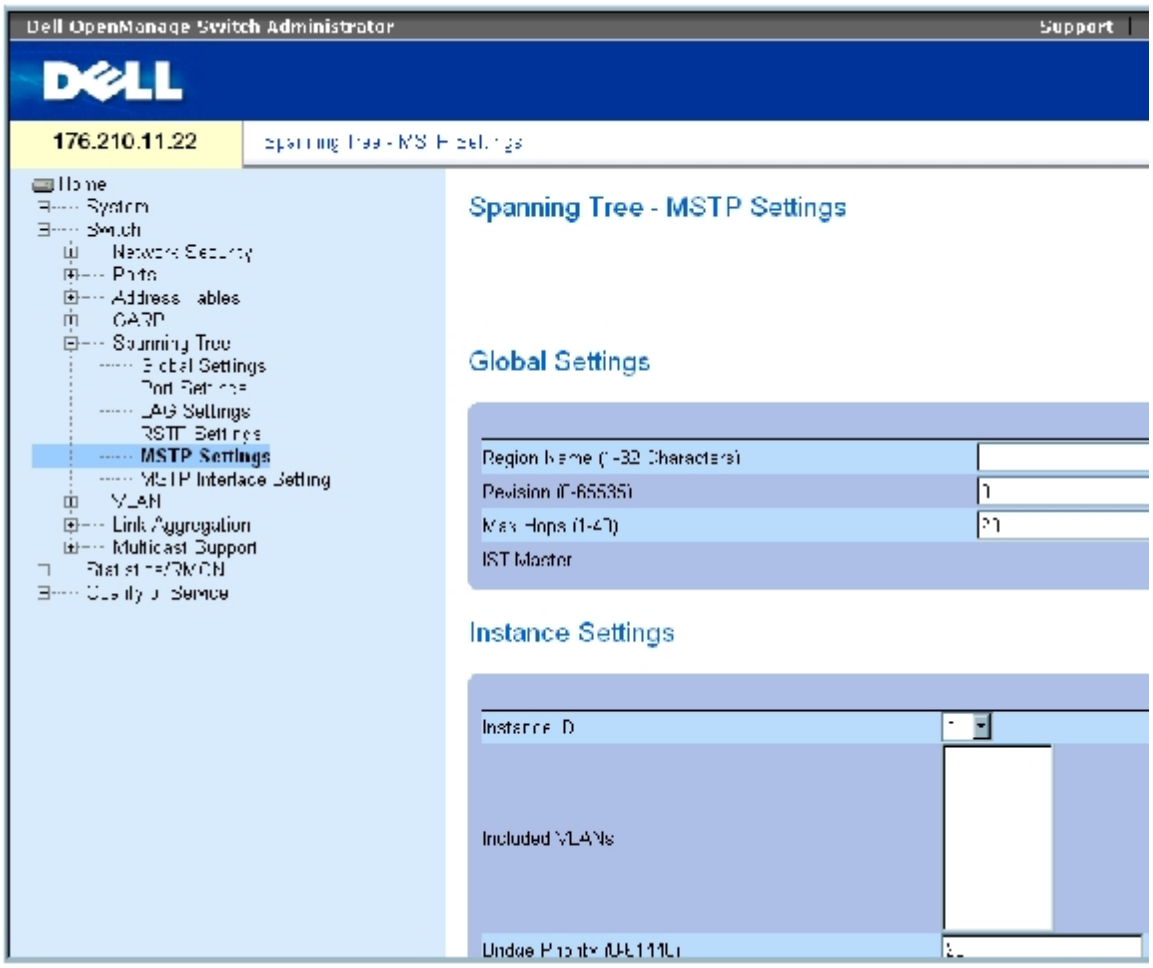
```
console(config)# interface ethernet 1/e5

console(config-if)# spanning-tree link-type shared

console(config-if)# spanning tree mode rstp
```

多重スパニングツリー

MST の動作により、VLAN が STP インスタンスにマッピングされます。多重スパニングツリーは異なる負荷分散シナリオを提供します。たとえば、ポート A が 1 つの STP インスタンスでブロックされている一方で、同一のポートを別の STP インスタンス内の転送状態に置くことができます。

また、さまざまな VLAN に割り当てられたパケットが、多重スパニングツリー領域（MST 領域）内の異なるパスで送信されます。領域は、フレームを転送できる 1 つまたは複数の多重スパニングツリーブリッジです。MSTP 設定ページを開くには、ツリービューで Switch（スイッチ）→ Spanning Tree（スパニングツリー）→MSTP Settings （MSTP 設定）の順にクリックします。

図**7-26 MSTP** 設定



MSTP 設定ページには、以下のフィールドがあります。

Region Name (1-32 Characters)（領域名）（1～32 文字）— ユーザー定義の MSTP 領域名を示します。

Revision (0-65535)（改訂）（0～65535）— 現在の MST 設定の改訂を識別する、署名なしの 16 ビット番号を定義します。改訂番号は、MST 設定の一部として要求されます。可能なフィールドの範囲は、0～65535 です。

Max Hops (1-40)（最大ホップ）（1～40）— BPDU が破棄されるまでに特定の領域で発生するホップの総数を定義します。BPDU が破棄されると、ポート情報はエージアウト（削除）されます。可能なフィールド値の範囲は、1～40 です。フィールドのデフォルト値は 20 ホップです。

IST Master（IST マスター）— 内部スパニングツリーのマスター ID を示します。IST マスターは、インスタンス 0 ルートです。

Instance ID（インスタンス ID）— MSTP インスタンスを定義します。フィールド値の範囲は、1～15 です。

Included VLANs（含まれている VLAN）— 選択したインスタンスにマッピングされている VLAN を表示します。各 VLAN が 1 つのインスタンスに属します。

Bridge Priority (0-61440)（ブリッジ優先度）（0～61440）— 選択したスパニングツリーのインスタンスにデバイス優先度を設定します。フィールド値の範囲は 0～61440 で、4096 刻みです。

Designated Root Bridge ID（指定ルートブリッジ ID）— 選択したインスタンスのルートであるブリッジの ID を示します。

Root Port（ルートポート）— 選択したインスタンスのルートポートを示します。

Root Path Cost（ルートパスコスト）— 選択したインスタンスのパスコストを示します。

Bridge ID （ブリッジ ID）— 選択したインスタンスのブリッジ ID を示します。

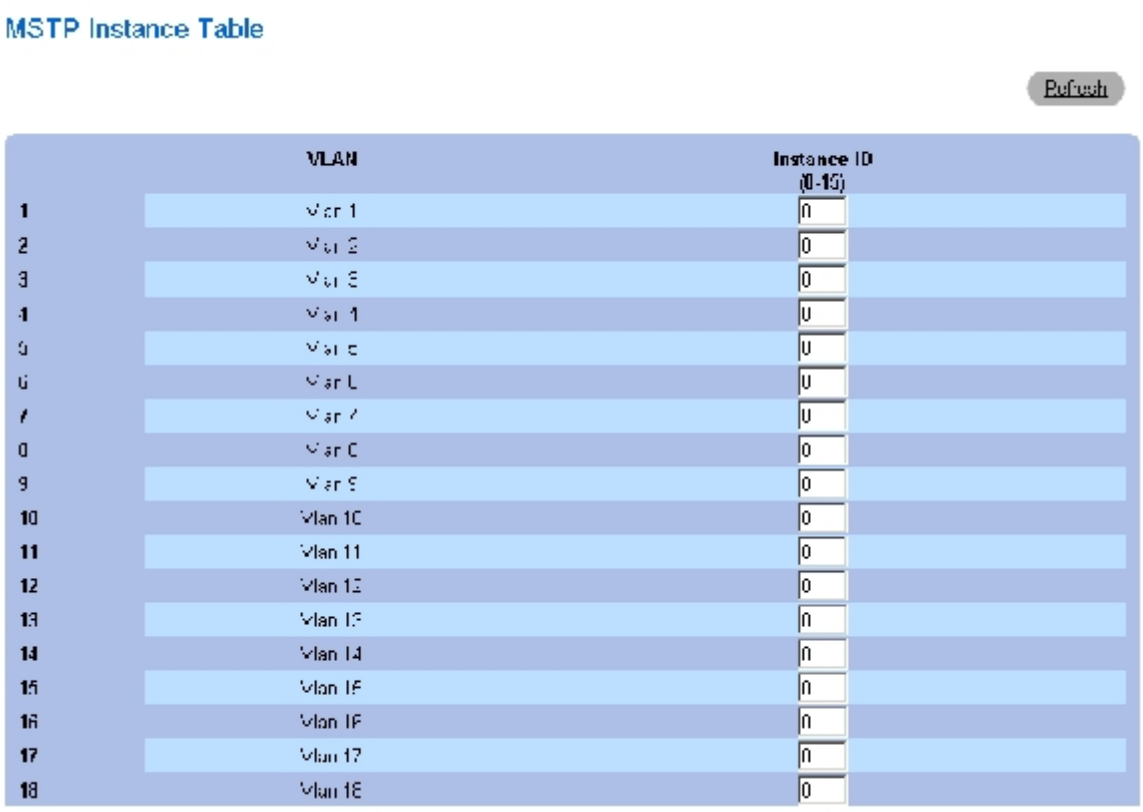
Remaining Hops （残りのホップ）— 次の送信先に対して残っているホップの数を示します。

MSTP インスタンス表の表示

□□□ スパニングツリーMSTP 設定ページを開きます。

□□□ **Show All**（すべてを表示）をクリックして、MSTP インスタンス表を開きます。

図**7-27 MSTP** インスタンス表



CLI コマンドを使用したMST インスタンスの定義

次の表は、スパニングツリーMSTP 設定ページに表示されているように、MST インスタンスグループを定義する場合の等価な CLI コマンドをまとめたものです。

表**7-18 MSTP** インスタンスに関連する **CLI** コマンド

CLI コマンド	説明
`spanning-tree mst configuration`	MST 設定モードに入ります。
`instance instance-id {add | remove} vlan`	VLAN を MST インスタンスにマッピングします。

vlan-range	
name string	設定名をセットします。
revision value	設定の改訂番号をセットします。
spanning-tree **mst** instance-id port-priority priority	ポートの優先度を設定します。
spanning-tree mst instance-id priority priority	指定したスパニングツリーのインスタンスにデバイス優先度を設定します。
spanning-tree mst max- hops hop-count	BPDU が破棄され、ポート情報がエージアウト（削除）されるまでの、MST 領域内のホップの数を設定します。
spanning-tree mst instance-id **cost** cost	MST 計算のためのポートのパスコストを設定します。
exit	MST 領域設定モードを終了し、設定の変更を適用します。
abort	設定の変更を適用せずに MST 領域設定モードを終了します。
show {current | pending}	現在の、または保留状態の MST 領域設定を表示します。

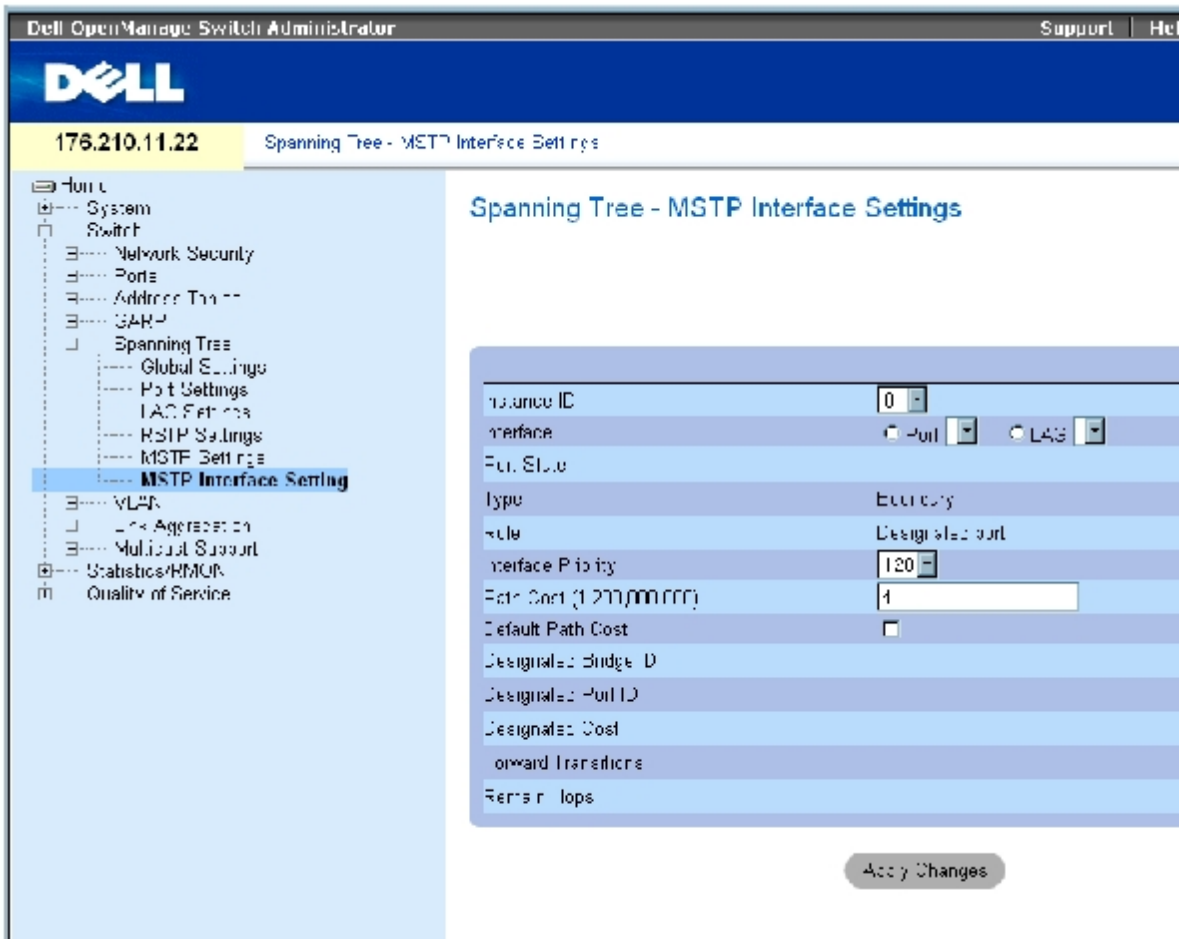
以下に、CLI コマンドの例を示します。

```
console(config)# spanning-tree mst configuration

console(config-mst)# instance 1 add vlan 10-20

console(config-mst)# name region1

console(config-mst)# revision 1

console(config)# spanning-tree mst configuration

console(config-mst)# instance 2 add vlan 21-30

console(config-mst)# name region1

console(config-mst)# revision 1

console(config-mst)# show pending

Pending MST configuration

Name:Region1

Revision: 1

Instance Vlans Mapped

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

0 1-9,31-4094

1 10-20

2 21-30
```

MSTP インタフェースの設定の定義

MSTP インタフェースの設定ページには、MSTP 設定を特定のインタフェースに割り当てるパラメータがあります。MSTP インタフェースの設定ページを開くには、ツリービューで Switch（スイッチ）→ Spanning Tree （スパニングツリー）→ MSTP Interface Settings（MSTP インタフェースの設定）の順にクリックします。

図**7-28 MSTP** インタフェースの設定



MSTP インタフェースの設定ページには、以下のフィールドがあります。

Instance ID（インスタンス ID）— デバイスに対して設定した MSTP インスタンスの一覧を表示します。可能なフィールド値の範囲は、1～15 です。

Interface （インタフェース）— ポートまたは LAG のいずれかを、選択した MSTP インスタンスに割り当てます。

Port State（ポート状態）— 特定のインスタンスでポートが有効か無効かを示します。

Type（タイプ）— MSTP がポートをポイントツーポイントのポートまたはハブに接続されているポートのどちらとして扱うか、ポートが MST 領域内にあるのか、または境界ポートなのかを表示します。マスターポートは、MSTP 領域から範囲外にある CIST ルートへの接続を提供します。境界ポートは MST ブリッジを範囲外の領域にある LAN に接続します。ポートが境界ポートである場合は、リンクの反対側にあるデバイスが RSTP または STP のどちらのモードで動作しているかをも示します。

Role（役割）— STP パスを提供するために STP アルゴリズムによって割り当てられるポートの役割を示します。可能なフィールド値は、以下のとおりです。

Root（ルート）— パケットをルートデバイスに転送する最低コストのパスを提供します。

Designated（指定）— 指定されているデバイスから LAN への接続に使用されているポートまたは LAG を示します。

Alternate（代替）— ルートインタフェースからルートデバイスへの代替パスを提供します。

Backup（バックアップ）— スパニングツリーリーフへの指定ポートパスに対するバックアップパスを提供します。バックアップポートは、2 つのポートがポイントツーポイントリンクでループ接続している場合にのみ提供されます。また、LAN で 2 つ以上のポートが共有セグメントに接続している場合にも、バックアップポートが提供されます。

Disabled（無効）— ポートがスパニングツリーに参加していないことを示します。

Interface Priority (0-240,in steps of 16)（インタフェース優先度）（0～240、16 刻み）— 指定したインスタンスのインタフェース優先度を定義します。デフォルト値は 128 です。

Path Cost（パスコスト）— スパニングツリーのインスタンスに対するポートのコントリビューションを示します。常に 1～200,000,000 の範囲でなければなりません。

Default Path Cost（デフォルトのパスコスト）— デフォルトのパスコストがスパニングツリーのグローバル設定ページで選択した方法に従って割り当てられていることを示します。

Designated Bridge ID（指定ブリッジ ID）— リンクまたは共有 LAN をルートに接続するブリッジ ID 番号です。

Designated Port ID（指定ポート ID）— リンクまたは共有 LAN をルートに接続する指定ブリッジのポート ID 番号です。

Designated Cost （指定コスト）— リンクまたは共有 LAN からルートへのパスのコストです。

Forward Transitions（転送への推移）— ポートが 転送状態に変化した回数です。

Remain Hops （残りのホップ）— 次の送信先に対して残っているホップの数を示します。

MSTP インタフェースの設定の定義

□□□ MSTP インタフェースの設定ページを開きます。

□□□ インタフェースを選択します。

□□□ フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

MSTP 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。

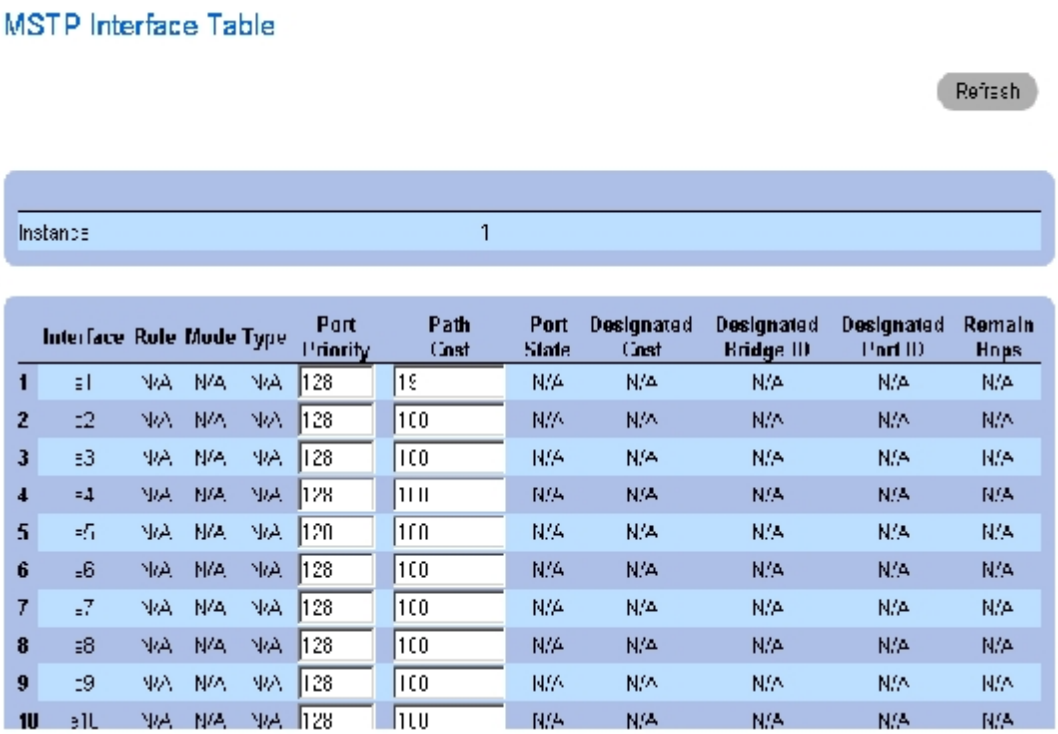
MSTP インタフェース表の表示

□□□ MSTP インタフェースの設定ページを開きます。

□□□ Show All（すべてを表示）をクリックします。

MSTP インタフェース表ページが開きます。

図**7-29 MSTP** インタフェース表



CLI コマンドを使用した **MSTP** インタフェースの定義

次の表は、スパニングツリーMSTP インタフェースの設定ページに表示されているように、MSTP インタフェースを定義する場合の等価な CLI コマンドをまとめたものです。

表**7-19 MSTP** インタフェースに関連する **CLI** コマンド

CLI コマンド	説明
`spanning-tree mst instance-id cost cost`	MST 計算のためのポートのパスコストを設定します。
`spanning-tree mst instance-id priority priority`	指定した ST（スパニングツリー）のインスタンスにデバイス優先度を設定します。
`show spanning-tree mst- configuration`	MST 設定を表示します。

以下に、CLI コマンドの例を示します。

```
console# show spanning-tree mst-configuration
Gathering information ..........
Current MST configuration
Name:Gili
Revision: 65000
Instance        Vlans Mapped            State
                ------------------------ -----------
```

0	16-4094	enabled
1	1	enabled
2	2	enabled
3	3	enabled
4	4	enabled
5	5	enabled
6	6	enabled
7	7	enabled
8	8	enabled
9	9	enabled
10	10	enabled
11	11	enabled
12	12	enabled
13	13	enabled
14	14	enabled
15	15	enabled

VLAN の設定

VLAN は、ハードウェアによるソリューションを定義するのではなく、ソフトウェアによって作成された LAN を使用した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 つのユニットに統合します。VLAN を使用することで、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、ネットワークの変化、追加、移動が導入される時間を短縮します。

VLAN には最小ポート数がなく、ユニット、デバイス、スタック、またはその他の任意の論理接続の組み合わせごとに作成できます。VLAN はソフトウェアベースであり、物理属性で定義されていないからです。

VLAN は、レイヤー 2 レベルで動作します。VLAN は VLAN 内でトラフィックを分離するので、VLAN 間でトラフィックが流れるように レイヤー 3 のプロトコルレベルで動作しているルーターが必要です。レイヤー 3 ルーターはセグメントを識別し、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 タギングは、VLAN グループ間で VLAN 情報をやり取りする方法です。VLAN タギングは、パケットヘッダーに 4 バイトのタグを付けます。VLAN タグは、どの VLAN にパケットが属しているかを示します。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いずれかで VLAN に添付されます。また、VLAN タグには、VLAN ネットワーク優先度情報も含まれています。

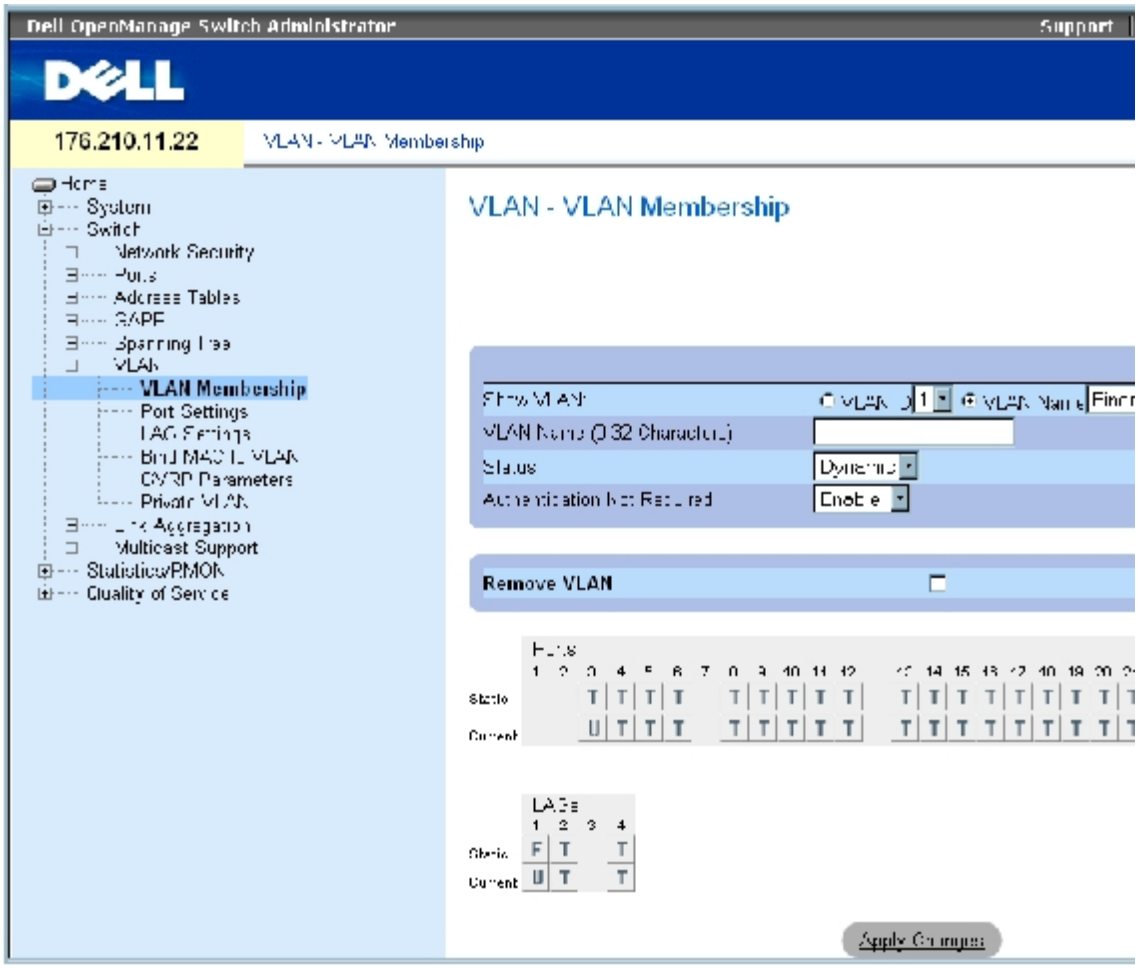
VLAN と GVRP を組み合わせることで、ネットワーク管理者はネットワークノードをブロードキャストドメイン内に定義することができます。ブロードキャストおよびマルチキャストトラフィックは、発信元のグループに限定されます。

VLANページを開くには、ツリービューで **Switch**（スイッチ）→**VLAN** の順にクリックします。

VLAN メンバーシップの定義

VLAN メンバーシップページには、VLAN グループを定義するためのフィールドがあります。デバイスでは、4094 個の VLAN ID から 256 個の VLAN へのマッピングをサポートしています。すべてのポートに、定義済みの PVID が必要です。特に値が設定されていなければ、デフォルトの VLAN PVID が使用されます。VLAN ID #1 はデフォルトの VLAN であり、システムから削除できません。**VLAN** メンバーシップページを開くには、ツリービューで **Switch**（スイッチ）→ **VLAN**→ **VLAN Membership**（VLAN メンバーシップ）の順にクリックします。

図**7-30 VLAN** メンバーシップ



VLAN メンバーシップ ページには、以下のフィールドがあります。

Show VLAN（VLAN の表示）— VLAN ID または VLAN 名に応じて特定の VLAN 情報を一覧表示します。

VLAN Name (0-32 Characters)（VLAN 名）（0～32 文字）— ユーザー定義の VLAN 名です。

Status （ステータス）— VLAN のタイプです。可能な値は以下のとおりです。

Dynamic（動的）— GVRP を通じて動的に作成された VLAN です。

Static（静的）— ユーザー定義の VLAN です。

Default（デフォルト）— この VLAN はデフォルトの VLAN です。

Authentication Not Required（認証不要）— 認証を受けていないユーザーによる VLAN へのアクセスを有効または無効にします。

Remove VLAN（VLAN の削除）— この項目を選択すると、VLAN メンバーシップ表から VLAN が削除されます。

VLAN の新規追加

□□□ **VLAN** メンバーシップページを開きます。

□□□ **Add**（追加）をクリックします。

VLAN の新規作成ページが開きます。

□□□ VLAN の ID と名前を入力します。

□□□ **Apply Changes**（変更の適用）をクリックします。

新規の VLAN が追加され、デバイスがアップデートされます。

VLAN メンバーシップグループの変更

□□□ **VLAN** メンバーシップページを開きます。

□□□ **Show VLAN**（VLAN の表示）ドロップダウンメニューから VLAN を選択します。

□□□ 必要に応じてフィールドを変更します。

□□□ **Apply Changes**（変更の適用）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 の削除

□□□ **VLAN** メンバーシップページを開きます。

□□□ **Show VLAN**（VLAN の表示）フィールドで VLAN を選択します。

□□□ **Remove VLAN**（VLAN の削除）チェックボックスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択した 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

次の表は、 VLAN メンバーシップページに表示されているように、VLAN メンバーシップグループを定義する場合の等価な CLI コマンドをまとめたものです。

表**7-20 VLAN** メンバーシップグループに関連する **CLI** コマンド

CLI コマンド	説明
vlan database	VLAN 設定モードに入ります。
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(config)# vlan
database

console(config-vlan)#
vlan 1972

console(config-vlan)# end

console(config)# interface
vlan 1972

console(config-if)# name
Marketing

console(config-if)# end
```

VLAN ポートメンバーシップ表

VLAN ポートメンバーシップ表には、VLAN にポートを割り当てるためのポート表が定義されています。VLAN へのポートの割り当ては、ポートのコントロール設定を通じて切り替えます。ポートには、次の値を設定できます。

表**7-21 VLAN** ポートメンバーシップ表

ポートのコントロール	定義
T	当該のインタフェースは VLAN のメンバーです。このインタフェースによって転送されるすべてのパケットには、タグが付きます。パケットには VLAN 情報が含まれています。
U	当該のインタフェースは VLAN のメンバーです。このインタフェースによって転送されるパケットには、タグは付きません。
F	当該のインタフェースは、VLAN へのメンバー登録を拒否されています。
	当該のインタフェースは VLAN のメンバーではありません。このインタフェースに関連付けられたパケットは転送されません。

VLAN ポートメンバーシップ表には、ポートとポート状態のほか、LAG も表示されます。

VLAN グループへのポートの割り当て

□□□ VLAN メンバーシップページを開きます。

□□□ **VLAN ID** または **VLAN Name**（VLAN 名）オプションボタンをクリックし、ドロップ ダウンメニューから VLAN を選択します。

□□□ ポートメンバーシップ表からポートを選択し、そのポートに値を割り当てます。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択したポートが 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 の削除

□□□ VLAN メンバーシップページを開きます。

□□□ **VLAN ID** または **VLAN Name**（VLAN 名）オプションボタンをクリックし、ドロップ ダウンメニューから VLAN を選択します。

□□□ **Remove VLAN**（VLAN の削除）チェックボックスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択した 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 グループへのポートの割り当て

次の表は、VLAN グループにポートを割り当てる場合の等価な CLI コマンドをまとめたものです。

表**7-22 VLAN** グループへのポートの割り当てに関連する **CLI** コマンド

CLI コマンド	説明
switchport general acceptable-frame-types tagged-only	タグなしのフレームを入口で破棄します。
switchport forbidden vlan {add *vlan-list* | remove *vlan-list*}	ポートに対する特定の VLAN の追加を禁止します。
switchport mode {access | trunk | general}	ポートの VLAN メンバーシップモードを設定します。
switchport access vlan vlan-id	インタフェースがアクセスモードである場合に、VLAN ID を設定します。
switchport trunk allowed vlan {add vlan-list | remove vlan-list}	VLAN をトランクポートに追加するか、トランクポートから削除します。
switchport trunk native vlan vlan-id	ポートを指定の VLAN のメンバーとして定義し、VLAN ID をポートのデフォルト VLAN ID（PVID）として定義します。
switchport general allowed vlan add vlan-list [tagged | untagged]	VLAN を一般用モードのポートに追加するか、一般用モードのポートから削除します。
switchport general pvid vlan-id	インタフェースが一般用モードである場合に、PVID を設定します。

以下に、CLI コマンドの例を示します。

```
console(config)# vlan
database

console(config-vlan)#
vlan 23-25

console(config-vlan)# end
```

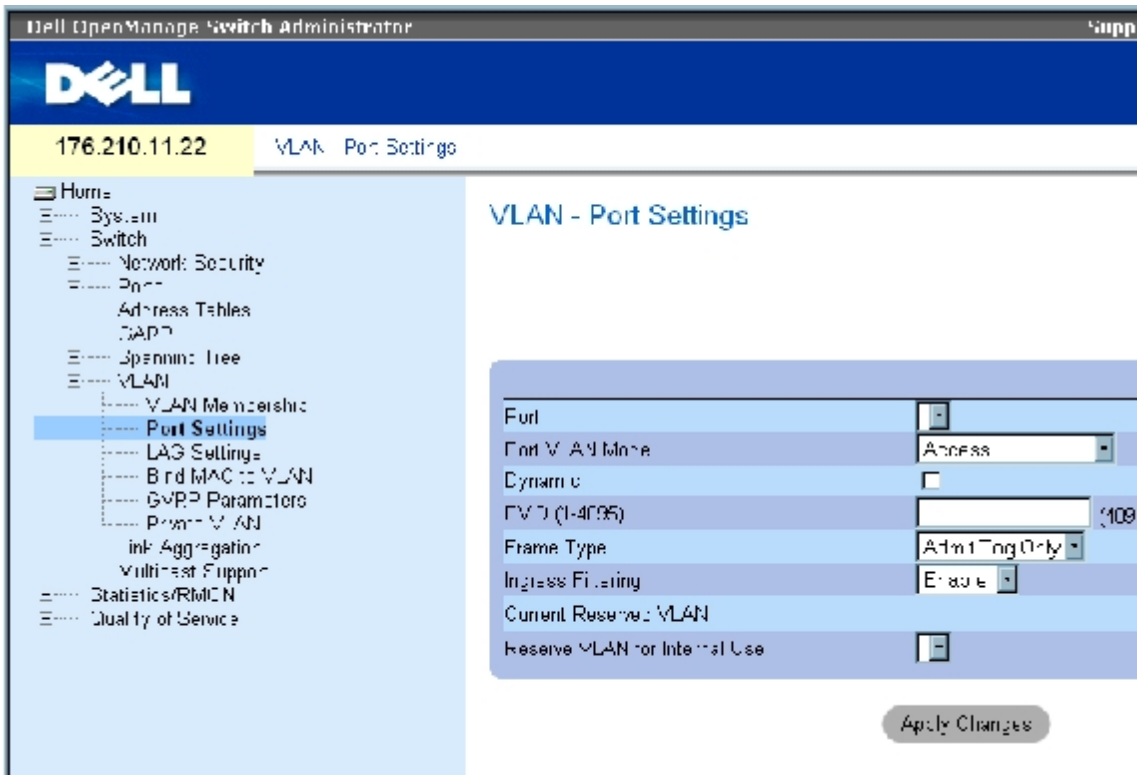
```
console(config)# interface
vlan 23


console(config-if)# name
Marketing


console(config-if)# end


console(config)# interface
ethernet 1/e8


console(config-if)#
switchport mode access


console(config-if)#
switchport access vlan 23


console(config-if)# end


console(config)# interface
ethernet 1/e9


console(config-if)#
switchport mode trunk


console(config-if)#
switchport mode trunk
allowed vlan add 23-25


console(config-if)# end


console(config)# interface
ethernet 1/e11


console(config-if)#
switchport mode general


console(config-if)#
switchport general
allowed vlan add 23,25
tagged


console(config-if)#
switchport general pvid
25
```

VLAN ポート設定の定義

VLAN ポートの設定 ページには、VLANの一部であるポートを管理するためのフィールドがあります。ポートのデフォルト VLAN ID（PVID）は、VLAN ポートの設定 ページで設定します。デバイスに到達したすべてのタグなしのパケットは、ポートの PVID によってタグが付けられます。

VLAN ポートの設定ページを開くには、ツリービューで **Switch**（スイッチ）→**VLAN**→**Port Settings**（ポート設定）の順にクリックします。

図**7-31 VLAN** ポートの設定



VLAN ポートの設定 ページには、以下のフィールドがあります。

Port（ポート）— VLAN に属するポートの番号です。

Port VLAN Mode（ポートの VLAN モード）— ポートのモードです。可能な値は以下のとおりです。

General（一般用）— 当該のポートは VLAN に属します。また、各 VLAN は、ユーザーによりタグ付きまたはタグなし（フル 802.1Q モード）として定義されます。

Access（アクセス）— 当該のポートは、単一のタグなし VLAN に属します。ポートがアクセスモードに入ると、ポートで許可するパケットタイプを指定できません。アクセスポートでは、入口フィルタリングの有効と無効を指定できません。

Trunk（トランク）— 当該のポートはすべてのポートにタグが付く VLAN に属します（タグなしが可能な 1 つのポートを除きます）。

PVE Promiscuous（PVE 無差別）— 当該のポートは、PVE 無差別 VLAN の一部です。

PVE Community（PVE コミュニティ）— 当該のポートは、PVE コミュニティ VLAN の一部です。

PVE Isolated（PVE 隔離）— 当該のポートは、PVE 隔離 VLAN の一部です。

Dynamic（動的）— ポートに接続されているホストソースの **MAC** アドレスに基づく **VLAN** にポートを割り当てます。

PVID— タグなしのパケットに VLAN ID を割り当てます。可能な値は、1～4095 です。VLAN 4095 は、業界標準により破棄 VLAN として定義されています。破棄 VLAN に分類されたパケットは削除されます。

Frame Type（フレームタイプ）— ポートで受け入れられるパケットのタイプです。可能な値は以下のとおりです。

Admit Tag Only（タグ付きのみ許可）— タグ付きのパケットのみをポートで受け入れます。

Admit All — タグ付き、タグなしの両方のパケットをポートで受け入れます。

Ingress Filtering（入口フィルタリング）— 当該のポートに対して入口フィルタリングを有効または無効にします。入口フィルタリングによって、特定のポートがメンバーになっていない VLAN を宛先とするパケットを破棄できます。

Current Reserved VLAN（現在の予約 VLAN）— 現在システムで予約 VLAN として指定されている VLAN です。

Reserve VLAN for Internal Use（内部用の予約 VLAN）— システムで使用されていない場合に、ユーザーが選択した VLAN を予約 VLAN とします。

ポートの設定の割り当て

□□□ VLAN ポートの設定ページを開きます。

□□□ **Port**（ポート）ドロップダウンメニューから、設定を割り当てる必要があるポートを 選択します。

□□□ ページ上の残りのフィールドを完了します。

□□□ **Apply Changes**（変更の適用）をクリックします。

VLAN ポートの設定が定義され、デバイスがアップデートされます。

VLAN ポート表の表示

□□□ VLAN ポートの設定ページを開きます。

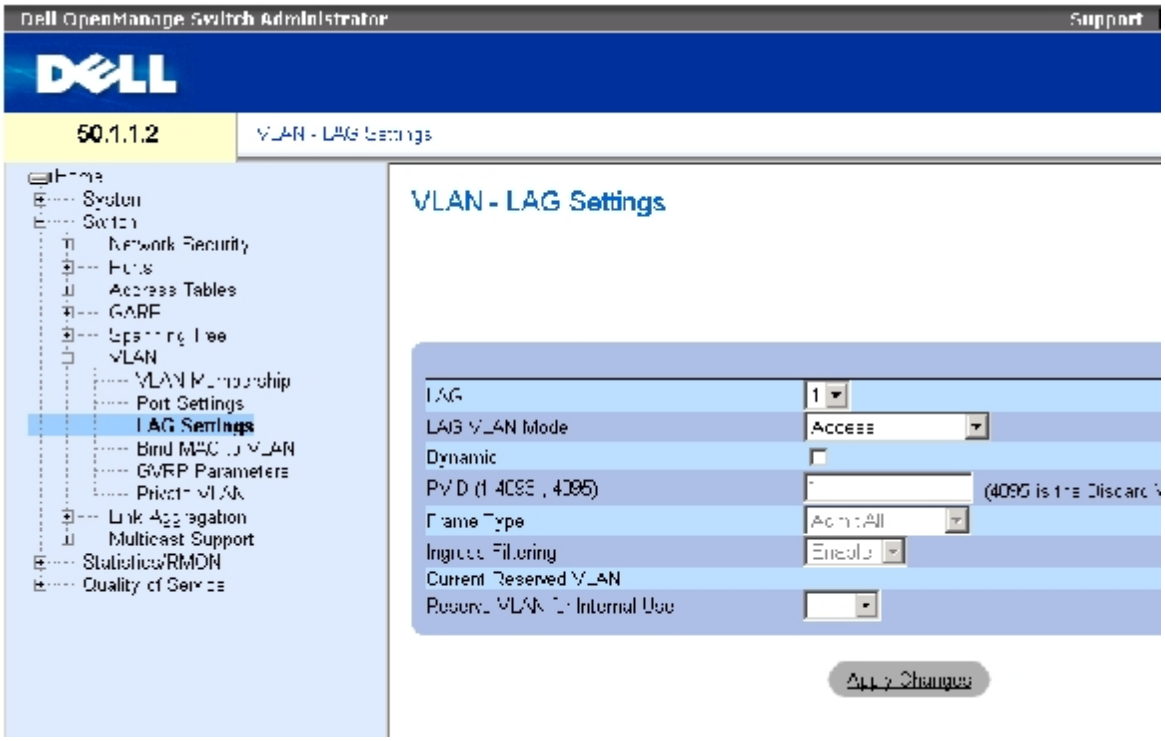
□□□ **Show All**（すべてを表示）をクリックします。

VLAN ポート表ページが開きます。

VLAN LAG 設定の定義

VLAN LAG 設定ページには、VLAN の一部である LAG を管理するためのパラメータがあります。VLAN は、個々のポートまたは LAG で構成できます。デバイスに入るタグなしのパケットは、PVID によって指定された LAG ID によってタグが付けられます。VLAN LAG 設定ページを開くには、ツリービューで **Switch**（スイッチ）→ **VLAN**→ **LAG Settings**（LAG の設定）の順にクリックします。

図**7-32 VLAN LAG** 設定



VLAN LAG 設定ページには、以下のフィールドがあります。

LAG — VLAN に含まれている LAG 番号を示します。

LAG VLAN Mode（LAG VLAN モード）— LAG VLAN のモードです。可能な値は以下のとおりです。

General（一般用）— 当該の LAG は VLAN に属します。また、各 VLAN は、ユーザーによりタグ付きまたはタグなし（フル 802.1Q モード）として定義されます。

Access（アクセス）— 当該の LAG は、単一のタグなし VLAN に属します。

Trunk（トランク）— 当該の LAG はすべてのポートにタグが付く VLAN に属します（タグなしが可能な 1 つのポートを除きます）。

PVE Promiscuous（PVE 無差別）— 当該の LAG は、PVE 無差別 VLAN の一部です。

PVE Community（PVE コミュニティ）— 当該の LAG は、PVE コミュニティ VLAN の一部です。

PVE Isolated（PVE 隔離）— 当該の LAG は、PVE 隔離 VLAN の一部です。

Dynamic（動的）— LAG に接続されているホストソースの MAC アドレスに基づく VLAN に LAG を割り当てます。

PVID (1-4093 , 4095)（PVID）（1～4093、4095）— VLAN ID をタグなしのパケットに割り当てます。可能なフィールド値は 1～4095 です。VLAN 4095 は、業界標準により破棄 VLAN として定義されています。この VLAN に分類されたパケットは削除されます。

Frame Type（フレームタイプ）— LAG で受け入れられるパケットのタイプです。可能な値は以下のとおりです。

Admit Tag Only（タグ付きのみ許可）— タグ付きのパケットのみを LAG で受け入れます。

Admit All（すべて許可）— タグ付き、タグなしの両方のパケットを LAG で受け入れます。

Ingress Filtering（入口フィルタリング）— 当該の LAG に対して入口フィルタリングを有効または無効にします。入口フィルタリングによって、特定の LAG がメンバーになっていない VLAN を宛先とするパケットを破棄できます。

Current Reserve VLAN（現在の予約 VLAN）— 現在予約 VLAN として指定されている VLAN です。

Reserve VLAN for Internal Use（内部用の予約 VLAN）— デバイスをリセットした後に予約 VLAN として指定された VLAN です。

VLAN LAG の設定の割り当て

□□□ VLAN LAG 設定ページを開きます。

□□□ **LAG** ドロップダウンメニューから LAG を選択し、ページ上のフィールドを完了しま す。

□□□ **Apply Changes**（変更の適用）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 表の表示

□□□ VLAN LAG 設定ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

VLAN LAG 表が開きます。

CLI コマンドを使用した LAG の VLAN グループへの割り当て

次の表は、VLAN LAG 設定ページに表示されているように、VLAN グループに LAG を割り当てる場合の等価な CLI コマンドをまとめたものです。

表**7-23 LAG VLAN** の割り当てに関連する **CLI** コマンド

CLI コマンド	説明
switchport mode {access | trunk | general}	LAG VLAN メンバーシップモードを設定します。
switchport trunk native vlan *vlan-id*	ポートを指定の VLAN のメンバーとして定義し、VLAN ID をポートの LAG のデフォルト 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、LAG VLAN ID（PVID）を設定します。
switchport general allowed vlan add *vlan-list* **[tagged | untagged]**	VLAN を一般用 LAG に追加するか、一般用 LAG から削除します。
switchport general acceptable-frame-type tagged-only	タグなしのパケットを入口で破棄します。
switchport access vlan dynamic	MAC アドレスを VLAN にバインドします。
switchport general ingress-filtering disable	入口フィルタリングを無効にします。

以下に、CLI コマンドの例を示します。

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


console(config-if)#
switchport mode access


console(config-if)#
switchport access vlan 2


console(config-if)# exit


console(config)# interface
port-channel 2


console(config-if)#
switchport mode general


console(config-if)#
switchport general
allowed vlan add 2-3
tagged


console(config-if)#
switchport general pvid 2


console(config-if)#
switchport general
acceptable-frame-type
tagged-only


console(config-if)#
switchport general
ingress-filtering disable


console(config-if)# exit


console(config)# interface
port-channel 3


console(config-if)#
switchport mode trunk


console(config-if)#
switchport trunk native
vlan 3


console(config-if)#
switchport trunk allowed
vlan add 2
```

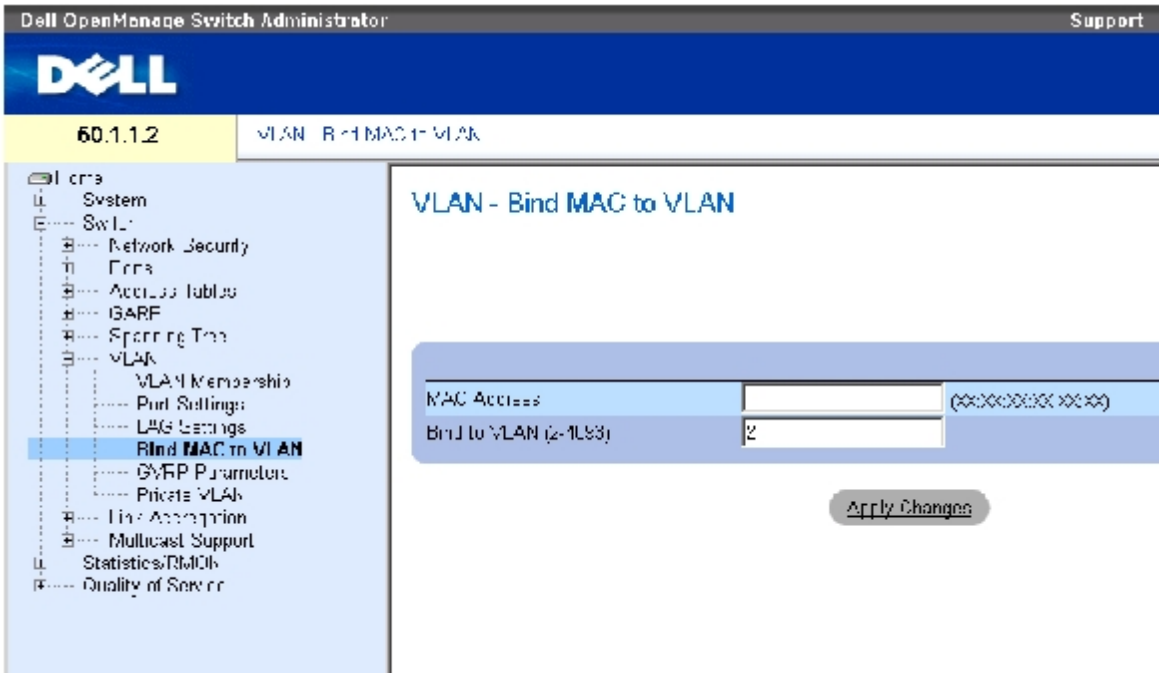
MAC アドレスの VLAN へのバインド

MAC アドレスを VLAN にバインドすると、MAC アドレスに基づいてポートに VLAN を割り当てることができます。VLAN に MAC アドレスを割り当て、ポートで MAC アドレスが学習されると、ポートはバインドされた VLAN に参加します。MAC アドレスがエージアウトすると、ポートは VLAN を離れます。MAC アドレスにバインドできるのは、動的 VLAN のみです。

MAC アドレスを VLAN にバインドするには、VLAN ポートが動的に追加されていて、静的 VLAN ポートではないことを確認してください。

MAC の VLAN へのバインドページを開くには、**Switch**（スイッチ）→ **VLAN**→ **Bind MAC to VLAN**（MAC を VLAN にバインドする）の順にクリックします。

図**7-33 MAC** の **VLAN** へのバインド



MAC の VLAN へのバインドページには、以下のフィールドがあります。

MAC Address（MAC アドレス）— VLAN にバインドされている MAC アドレスを示します。

Bind to VLAN (2-4093)（VLAN へのバインド）（2～4093）— MAC アドレスがバインドされている VLAN を示します。

MAC の VLAN 表への表示

□□□ MAC の VLAN へのバインド ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

MAC から **VLAN**の 表が開きます。

CLI コマンドを使用した MAC アドレスの VLAN へのバインド

次の表は、MAC アドレスを VLAN にバインドする場合の等価な CLI コマンドをまとめたものです。

表**7-24 MAC** アドレスの **VLAN CLI** コマンドへのバインド

CLI コマンド	説明
`mac-to-vlan mac-address vlan-id`	MAC アドレスを VLAN にバインドします。
`switchport access vlan dynamic`	プライベート VLAN を設定します。
`show mac-to-vlan`	MAC を VLAN データベースに表示します。
`no mac-to-vlan mac-address`	MAC アドレスを VLAN からバインド解除します。

以下に、CLI コマンドの例を示します。

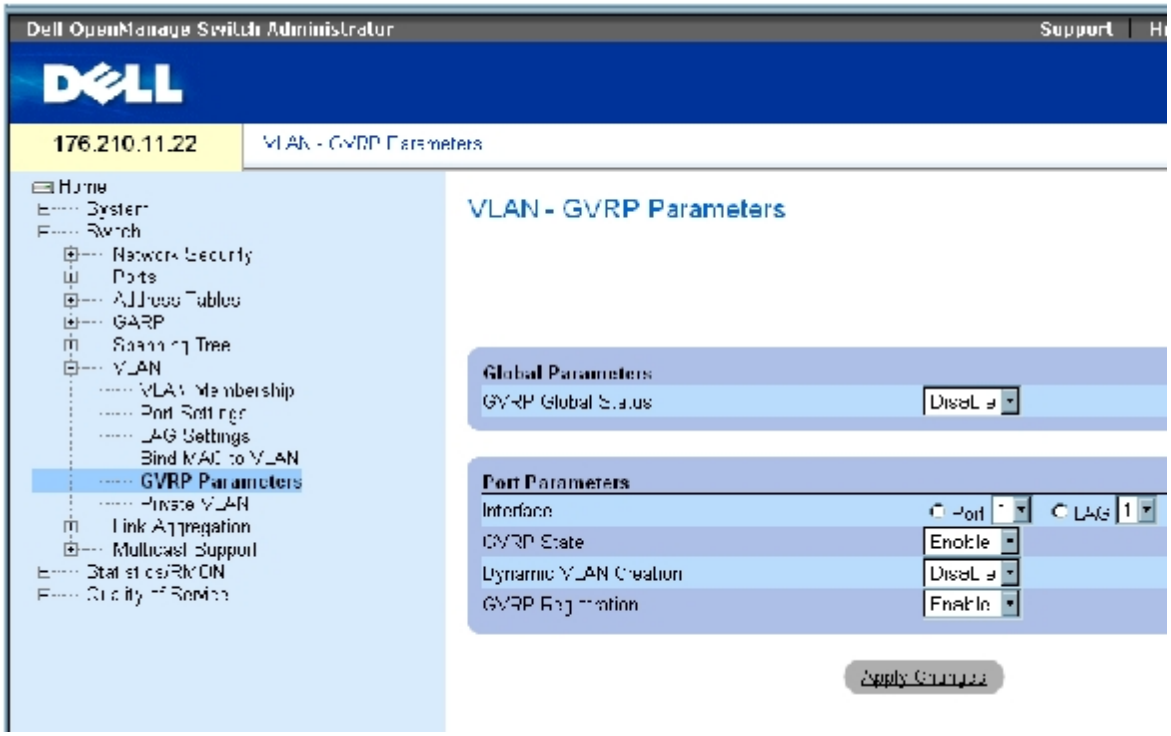
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123

console(config-vlan)# exit

console(config)# exit

console# show vlan mac-to-vlan

MAC Address VLAN

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

0060.704c.73ff 123
```

GVRP パラメータの設定

GARP VLAN Registration Protocol（GVRP）は、特に、VLAN 認識ブリッジに VLAN メンバーシップ情報を自動配布することを目的としています。GVRP は、VLAN 認識ブリッジが、VLAN とブリッジポートのマッピングを自動的に学習することを可能にするプロトコルで、各ブリッジを個別に設定して VLAN メンバーシップを登録する手間を省きます。

GVRP パラメータページは GVRP をグローバルに有効にします。GVRP は、インタフェースごとに有効にすることも可能です。GVRP パラメータページを開くには、ツリービューで **Switch**（スイッチ）→ **VLAN**→**GVRP Parameters**（GVRP パラメータ）の順にクリックします。

図**7-34 GVRP** パラメータ



GVRP パラメータページには、以下のフィールドがあります。

GVRP Global Status（GVRP グローバルステータス）— デバイスに対して GVRP を有効または無効にします。GVRP はデフォルトで無効です。

Interface（インタフェース）— GVRP の設定を編集するためのポートまたは LAG を指定します。

GVRP State（GVRP 状態）— インタフェースに対して GVRP を有効または無効にします。

Dynamic VLAN Creation（動的 VLAN の作成）— インタフェースに対して GVRP による VLAN の作成を有効または無効にします。

GVRP Registration（GVRP の登録）— インタフェースに対して GVRP による VLAN の登録を有効または無効にします。

デバイスに対する GVRP の有効化

□□□ GVRP グローバルパラメータページを開きます。

□□□ **GVRP Global Status**（GVRP グローバルステータス）フィールドで**Enable**（有効）を 選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

デバイスに対して GVRP が有効になります。

GVRP を介した VLAN 登録の有効化

□□□ GVRP グローバルパラメータページを開きます。

□□□ **GVRP Global Status**（GVRP グローバルステータス）で**Enable**（有効）を選択します。

□□□ 必要なインタフェースの GVRP 状態フィールドで、**Enable**（有効）を選択します。

□□□ **GVRP Registration**（GVRP の登録）フィールドで **Enable**（有効）を選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

GVRP VLAN の登録がポートに対して有効になり、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 GVRP の設定

次の表は、GVRP グローバルパラメータ ページで表示されているように、GVRP を設定する場合の等価な CLI コマンドをまとめたものです。

表**7-25 GVRP** グローバルパラメータに関連する **CLI** コマンド

CLI コマンド	説明
gvrp enable (global**)**	GVRP をグローバルに有効にします。
gvrp enable (interface)	インタフェースに対して GVRP を有効にします。
gvrp vlan-creation-forbid	動的 VLAN の作成を有効または無効にします。
gvrp registration-forbid	すべての動的 VLAN の登録を解除し、当該のポートに対する動的 VLAN の登録を防止します。
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、およびどのポートで GVRP が実行されているか、などの GVRP の設定情報を表示します。
show gvrp error-statistics [**ethernet** *interface*| **port-channel** *port-channel-number*]	GVRP エラー の統計を表示します。

show gvrp statistics [**ethernet** *interface*| **port-channel** *port-channel-number*]	GVRP の統計を表示します。
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。

以下に、CLI コマンドの例を示します。

```
console(config)# gvrp enable

console(config)# interface ethernet 1/e1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration

GVRP Feature is currently Enabled on the device

Maximum VLANs: 223
```

Port(s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
------	------	----------	-------	------------	-----	-----
1/e11	Enabled	Forbidden	Disabled	200	900	10000
1/e12	Disabled	Normal	Enabled	200	600	10000

プライベート **VLAN** の設定

プライベート VLAN（PVLAN）は、VLAN 内のポート間通信を制限することでネットワークセキュリティを高めます。プライベート VLAN は、レイヤー 2 レベルでのネットワークトラフィックを制限します。ネットワーク管理者がプライマリ VLAN を定義します。プライマリ VLAN 内に、隔離 VLAN とコミュニティ VLAN があります。プライベート VLAN ポートには、次の状態を設定できます。

- **Promiscuous**（無差別）— 無差別ポートは、PVLAN 内のすべてのポートと通信できます。すべての無差別パケットは、隔離 VLAN とコミュニティ VLAN の両方に自動的に割り当てられます。
- **Isolated**（隔離）— 隔離ポートは、同じ PVLAN 内の他のポートから完全に隔離されています。ただし、隔離ポートは無差別ポートと通信することができます。また、VLAN を持つ隔離ポートとの間で送受信されるすべてのトラフィックは、無差別ポートからのトラフィックを除いてブロックされます。すべての隔離ポートは、隔離 VLAN に自動的に割り当てられます。
- **Community**（コミュニティ）— コミュニティポートは他のコミュニティポートおよび無差別ポートと通信します。コミュニティポートは、他のコミュニティ内のすべての他のインタフェース、または同じ PVLAN 内の隔離ポートから分離されています。すべてのコミュニティポートは、コミュニティ VLAN とプライベート VLAN に自動的に割り当てられます。

メモ： ポートが既存の VLAN のメンバーである場合は、無差別ポートと隔離ポートのど ちらにも定義できません。

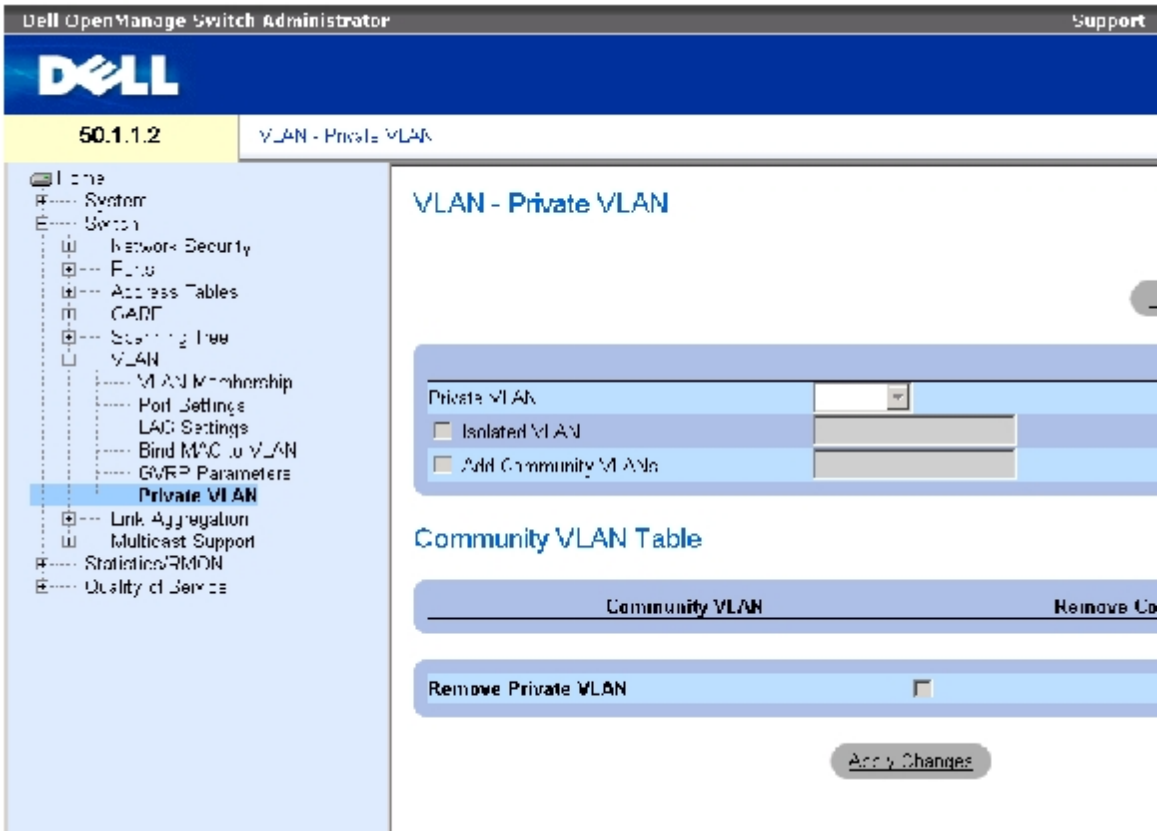
メモ： 以前に作成した VLAN は、隔離 VLAN とコミュニティ VLAN のどちらにも設定でき ません。

メモ： 隔離 VLAN とコミュニティ VLAN は、VLAN の総計に含まれます。

プライマリ VLAN が削除されると、隔離 VLAN とコミュニティ VLAN の両方が削除されます。また、隔離 VLAN とコミュニティ VLAN は、タグなしのトラフィックのみを転送します。

プライベート VLANページを開くには、ツリービューで **Switch**（スイッチ）→ **VLAN**→ **Private VLAN** （プライベート VLAN）の順にクリックします。

図**7-35** プライベート **VLAN**



プライベート VLANページには、以下のフィールドがあります。

Private VLAN（プライベート VLAN）— ユーザー定義のプライベート VLAN の一覧があります。プライベート VLAN は、プライベート **VLAN** の追加ページに定義されています。

Isolated VLAN （隔離 VLAN）— どの VLAN がどの隔離ポートに割り当てられているかを示します。

Add Community VLANs（コミュニティ VLAN の追加）— コミュニティポートが割り当てられているコミュニティ VLAN を追加します。

Community VLAN（コミュニティ VLAN）— コミュニティ VLAN の一覧を表示します。

Remove Community（コミュニティの削除）— この項目をチェックすると、コミュニティ VLAN が削除されます。

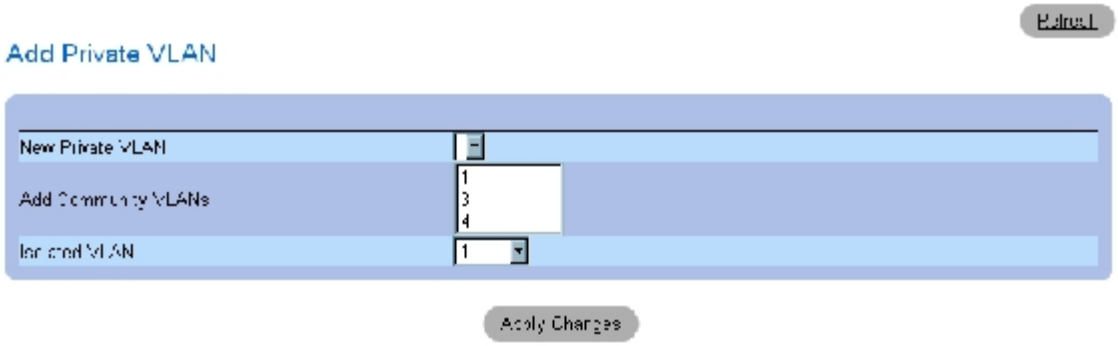
Remove Private VLAN （プライベート VLAN の削除）— この項目をチェックすると、プライベート VLAN が削除されます。

プライベート **VLAN** の追加

□□□ プライベート VLANページを開きます。

□□□ **Add**（追加）をクリックします。プライベート **VLAN** の追加ページが開きます。

図**7-36** プライベート **VLAN** の追加



プライベート VLAN の追加ページには、以下の追加フィールドがあります。

New Private VLAN（新規プライベート VLAN）— プライベート VLANの一覧が含まれています。コミュニティ VLAN がプライベート VLAN に追加されます。

Add Community VLANs（コミュニティ VLAN の追加）— コミュニティ VLAN をプライベート VLAN に追加します。

Isolated VLAN（隔離 VLAN）— 隔離 VLAN をプライベート VLAN に追加します。

□□□ フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

プライベート VLAN が定義され、デバイスがアップデートされます。

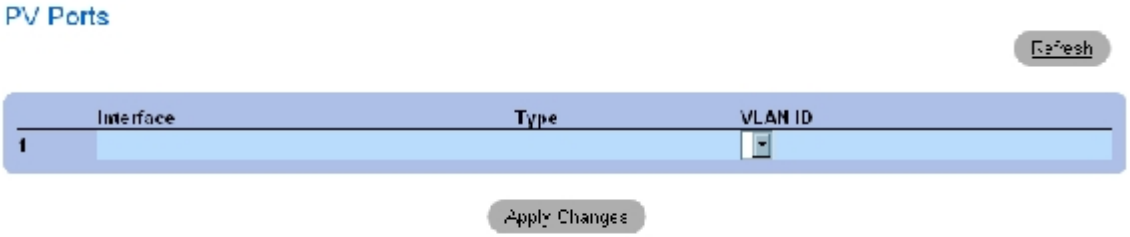
PV ポート表の表示

□□□ プライベート VLANページを開きます。

□□□ **Show PV Ports**（PV ポートを表示）をクリックします。

PV ポート表が開きます。

図**7-37 PV** ポート表



CLI コマンドを使用した PVLAN の設定

次の表は、プライベート VLANページに表示されているように、PVLAN を設定する場合の等価な CLI コマンドをまとめたものです。

表7-26 プライベート VLAN に関連する CLI コマンド

CLI コマンド	説明
switchport mode private vlan promiscuous	無差別 **VLAN** に無差別ポートを追加します。
switchport mode private vlan community	コミュニティ **VLAN** にコミュニティポートを追加します。
switchport mode private vlan isolated	隔離 **VLAN** に隔離ポートを追加します。
private-vlan primary	プライマリ VLAN を定義します。
private-vlan community {add community-vlan-list | remove community-vlan-list }	プライマリ VLAN のコミュニティ VLAN を定義または削除します。
private-vlan isolated	プライマリ VLAN の隔離 VLAN を定義します。
switchport private-vlan *pvlan* **[community** *cvlan***]**	プライベート VLAN ポートを定義します。
show vlan private-vlan [primary vlan-id]	プライベートプライマリ VLAN を表示します。

以下に、CLI コマンドの例を示します。

```
console(config)# vlan
database

console(config-vlan)#vlan
2

console(config-vlan)#exit

console(config)#interface
vlan 2

console(config-if)#
private-vlan primary

console(config)#interface
vlan 2

console(config-if)#
private-vlan isolated 10

console(config-if)#
private-vlan community
add 20

console# show vlan
private-vlan

console(config-if)# end
```

ポートの集約

ポートの集約は、ポートのグループを関連付けて 1 つのリンク集約グループ（LAG）を形成することにより、ポートの使用を最適化します。ポートの集約によって、デバイス間の帯域幅が倍増し、ポートの柔軟性が高まり、リンクに冗長性が備わります。

デバイスでは、静的 LAG と Link Aggregation Control Protocol（LACP）LAG の両方をサポートしています。LACP LAG は、別のデバイスに存在する他の LACP ポートとポート集約リンクのネゴシエイションを行います。他のデバイスポートも LACP ポートである場合には、両者間に LAG が確立されます。

ポートの集約を行う際は、以下のガイドラインに従ってください。

- LAG 内のすべてのポートが同じメディアタイプであること。
- VLAN がポートに対して設定されていないこと。
- ポートが別の LAG に割り当てられていないこと。
- オートネゴシエイションモードがポートに対して設定されていないこと。
- ポートが全二重モードになっていること。
- LAG 内のすべてのポートが同じ入口フィルタリングモードとタグ付きモードを持っていること。
- LAG 内のすべてのポートが同じバックプレッシャーモードとフロー制御モードを持っていることを
- LAG 内のすべてのポートが同じ優先度を持っていること。
- LAG 内のすべてのポートが同じトランシーバタイプを持っていること。
- デバイスが最大 8 つの LAG、および各 LAG 内で 8 つのポートをサポートしていること。
- ポートは、以前に設定した LAG に属していない場合にのみ、LACP ポートとして設定できます。

LAG に追加されたポートは、個々のポート設定を失います。LAG からポートを削除すると、そのポートは元のポート設定に戻ります。

デバイスでは、どの集約リンクメンバーにどのパケットを転送するかを決定するために、ハッシュ機能を使用します。ハッシュ機能は、集約リンクメンバーの負荷分散を統計的に行います。デバイスは、集約リンクを単一の論理ポートと見なします。

LACP パラメータの定義

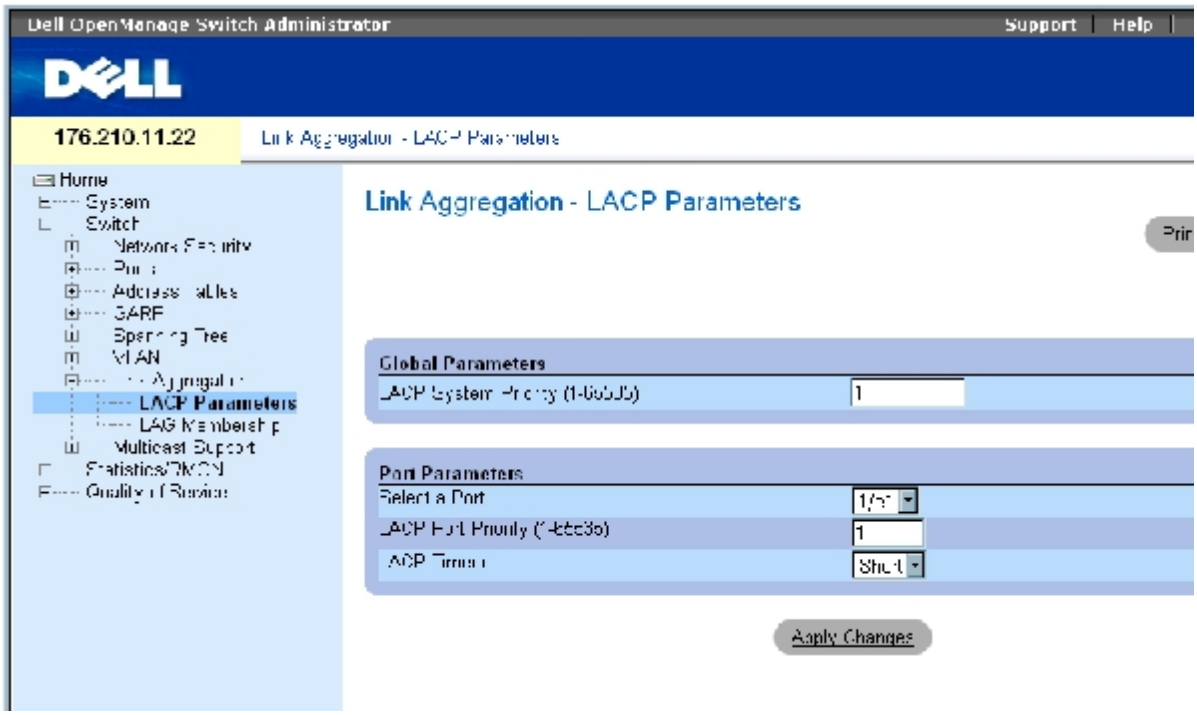
集約するポートは、集約リンクのポートグループに関連付けることができます。各グループは、全二重動作に設定された同スピードのポートで構成されます。

ポートが同スピードで動作している場合、リンク集約グループ（LAG）内のポートは異なるメディアタイプを含むことができます。集約リンクを手動または自動で設定するには、関連リンクに対して Link Aggregation Control Protocol（LACP）を有効にします。

LACP パラメータの定義

LACP パラメータページには、LACP LAG を設定するためのフィールドがあります。集約するポートは、集約リンクのポートグループに関連付けることができます。各グループは、同スピードのポートで構成されます。集約リンクを手動でセットアップするか、自動で確立するには、関連リンクに対して Link Aggregation Control Protocol（LACP）を有効にします。LACP パラメータページを開くには、ツリービューで **Switch**（スイッチ）→ **Link Aggregation**（リンク集約）→ **LACP Parameters**（LACP パラメータ）の順にクリックします。

図**7-38 LACP** パラメータ



LACP パラメータページには、以下のフィールドがあります。

LACP System Priority (1-65535)（LACP システム優先度）（1～65535）— グローバル設定用の LACP 優先度値です。可能な値の範囲は 1～65535 です。デフォルト値は 1 です。

Select a Port（ポートの選択）— タイムアウト値と優先度値を割り当てるポートの番号です。

LACP Port Priority (1-65535)（LACP ポートの優先度）（1～65535）— 当該ポートの LACP 優先度値です。

LACP Timeout（LACP タイムアウト）— 管理用の LACP タイムアウトです。可能なフィールド値は、以下のとおりです。

Short（ショート）— ショートタイムアウト値を指定します。

Long（ロング）— ロングタイムアウト値を指定します。

リンク集約グローバルパラメータの定義

□□□ LACP パラメータページを開きます。

□□□ **LACP System Priority**（LACP システム優先度）フィールドを完了します。

□□□ **Apply Changes**（変更の適用）をクリックします。

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。

リンク集約ポートパラメータの定義

□□□ LACP パラメータページを開きます。

□□□ **Port Parameters**（ポートパラメータ）エリアのフィールドを完了します。

□□□ **Apply Changes**（変更の適用）をクリックします。

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。

LACP パラメータ表の表示

□□□ LACP パラメータページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

LACP パラメータ表が開きます。

CLI コマンドを使用した **LACP** パラメータの設定

次の表は、LACP パラメータページに表示されているように、LACP パラメータを設定する場合の等価な CLI コマンドをまとめたものです。

表**7-27 LACP** パラメータに関連する **CLI** コマンド

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 ポートに関する 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/e11

Console (config-if)# lacp
port-priority 247

Console (config-if)# lacp
timeout long

Console (config-if)# end

Console# show lacp
ethernet 1/e11 statistics

Port 1/e11 LACP
Statistics:

LACP PDUs sent:2

LACP PDUs received:2
```

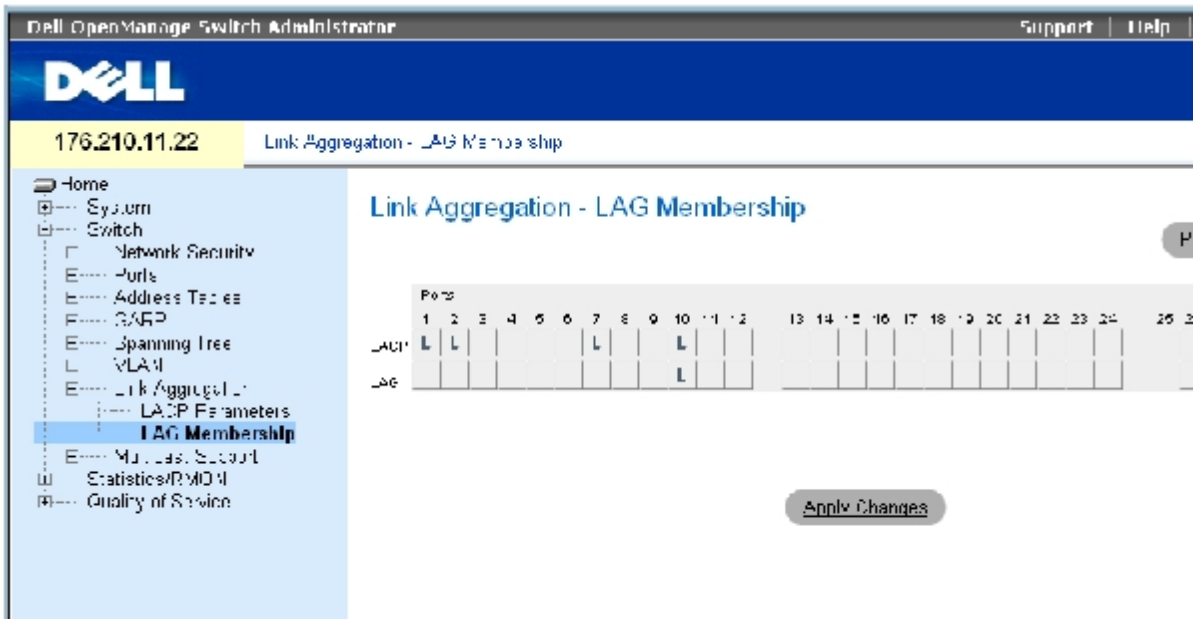
LAG メンバーシップの定義

デバイスは、スタンドアロンかスタックかに関係なく、システムごとに 8 つの LAG 、および LAG ごとに 8 ポートをサポートします。

ポートを LAG に追加すると、そのポートは LAG のプロパティを取得します。ポートが LAG のプロパティで設定できない場合には、LAG に追加されず、エラーメッセージが表示されます。ただし、LAG に参加する最初のポートが LAG 設定によって設定できない場合には、ポートは、ポートのデフォルト設定を使用して LAG に追加され、エラーメッセージが表示されます。ただし、これが LAG 内の唯一のポートであるため、LAG 全体が LAG の定義された設定ではなく、ポートの設定で動作します。

LAG メンバーシップページを使用してポートを LAG に割り当てます。**LAG メンバーシップ**ページを開くには、ツリービューで **Switch**（スイッチ）→ **Link Aggregation**（リンク集約）→ **LAG Membership**（LAG メンバーシップ）の順にクリックします。

図**7-39 LAG** メンバーシップ



LAG メンバーシップページには、以下のフィールドがあります。

LACP — LACP を使用して、LAG にポートを集約します。

LAG— LAG にポートを追加し、ポートが属している特定の LAG を示します。

LAG または LACP に対するポートの設定

□□□ **LAG メンバーシップ** ページを開きます。

□□□ LAG 列（2 列目）で特定の番号のボタンを切り替えて、その番号の LAG にポートを集 約するか、その番号の LAG からポートを削除します。

□□□ LACP 列（1 列目）でポート番号の下のボタンを切り替えて、LACP または静的 LAG のいずれかを割り当てます。

□□□ **Apply Changes**（変更の適用）をクリックします。

ポートが LAG または LACP 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 への追加

次の表は、**LAG** メンバーシップ に表示されているように、ポートを LAG に割り当てる場合の等価な CLI コマンドをまとめたものです。

表**7-28 LAG** メンバーシップに関連する **CLI** コマンド

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関連付けます。インタフェースからチャネルグループの設定を削除するには、このコマンドの no form を使用してください。
show interfaces port-channel [*port-channel-number*]	ポートチャネ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
ethernet 1/e11

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

マルチキャスト転送のサポート

マルチキャスト転送では、単一のパケットを複数の宛先に転送できます。レイヤー 2 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先指定された単一のパケットを受信するレイヤー 2 デバイスに基づきます。マルチキャスト転送によって、パケットのコピーが作成され、それらのパケットが関連ポートに送信されます。

Registered Multicast traffic（登録済みマルチキャストトラフィック）— 登録済みのマルチキャストグループを宛先とするトラフィックが送信された場合、トラフィックはマルチキャストフィルタリングデータベース内のエントリによって処理され、登録済みのポートにのみ転送されます。

Unregistered Multicast traffic（未登録マルチキャストトラフィック）— 未登録のマルチキャストグループを宛先とするトラフィックが送信された場合、トラフィックはマルチキャストフィルタリングデータベース内の特別なエントリによって処理されます。その種のトラフィックをすべてフラッディングする設定がデフォルトです（未登録のマルチキャストグループ内のトラフィック）。

デバイスは以下をサポートしています。

- **Forwarding L2 Multicast Packets**（L2 マルチキャストパケットの転送）— レイヤー 2 のマルチキャストパケットを転送します。レイヤー 2 マルチキャストフィルタリングがデフォルトで有効になっており、ユーザー設定は不可です。

メモ： システムは、256 のマルチキャストグループに対するマルチキャストフィルタリ ングをサポートしています。

- **Filtering L2 Multicast Packets**（L2 マルチキャストパケットのフィルタリング）— レイヤー 2 のパケットをインタフェースに転送します。マルチキャストフィルタリングが無効の場合、マルチキャストパケットは関連するすべてのポートにフラッディングされます。

マルチキャストサポートページを開くには、ツリービューで **Switch**（スイッチ）→ **Multicast Support**（マルチキャストサポート）の順にクリックします。

マルチキャストグローバルパラメータの定義

レイヤー 2 のスイッチングでは、デフォルトでマルチキャストパケットはすべての関連 VLAN ポートに転送され、パケットは単一のマルチキャスト送信として処理されます。マルチキャストトラフィック転送は効果的ではあるものの、無関係なポートもマルチキャストパケットを受信するため、無駄な動作になる可能性があります。過剰なパケットが原因でネットワークトラフィックが増加します。マルチキャスト転送フィルタを使用すると、レイヤー 2 のパケットをポートのサブセットに転送することができます。

IGMP スヌープをグローバルに有効にすると、すべての IGMP パケットが CPU に転送されます。CPU では着信パケットを分析し、以下の判断を下します。

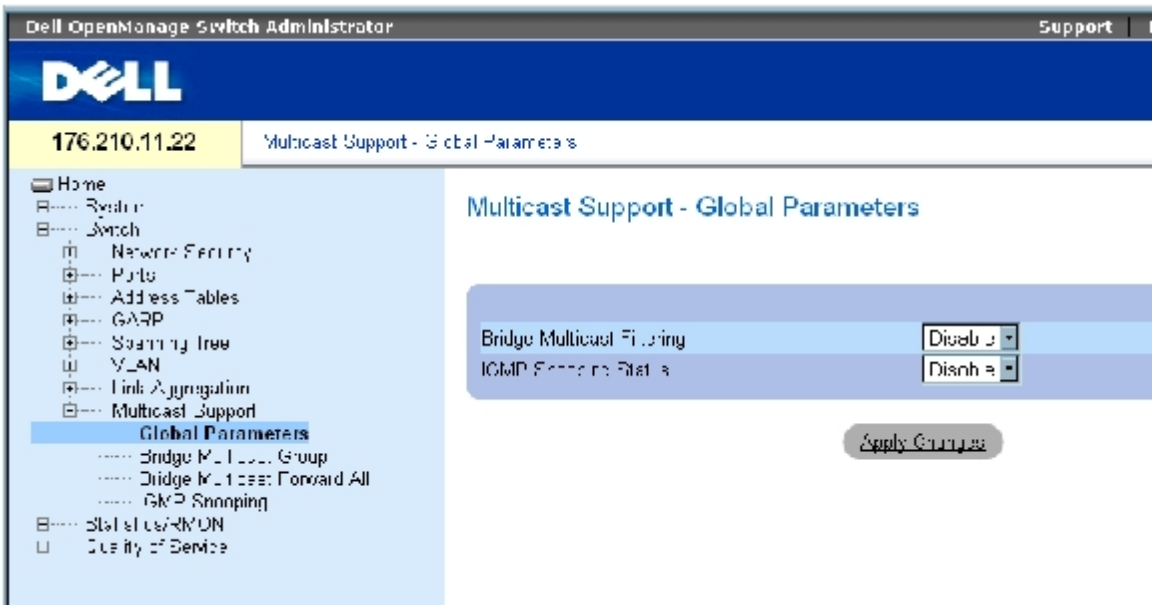
- どのポートがどのマルチキャストグループに参加しようとしているか。
- どのポートが IGMP クエリを生成するマルチキャストルーターを持っているか。
- どのルーティングプロトコルでパケットとマルチキャストトラフィックが転送されているか。

特定のマルチキャストグループへの参加を要求するポートは、そのマルチキャストグループがメンバーを受け入れることを示す IGMP レポートを発行します。この結果、マルチキャストフィルタリングデータベースが作成されます。

マルチキャストサポートページを開くには、ツリービューで **Switch**（スイッチ）→ **Multicast Support**（マルチキャストサポート）の順にクリックします。

グローバルパラメータページには、デバイスに対して IGMP スヌープを有効にするためのフィールドがあります。グローバルパラメータページを開くには、ツリービューで **Switch**（スイッチ）→ **Multicast Support**（マルチキャストサポート）→ **Global Parameters**（グローバルパラメータ）の順にクリックします。

図**7-40** グローバルパラメータ



グローバルパラメータページには、以下のフィールドがあります。

Bridge Multicast Filtering（ブリッジのマルチキャストフィルタリング）— ブリッジでのマルチキャストフィルタリングを有効または無効にします。無効がデフォルト値です。

IGMP Snooping Status（IGMP スヌープステータス）— デバイスに対して IGMP スヌープを有効または無効にします。無効がデフォルト値です。IGMP スヌープは、グローバルパラメータが有効の場合に限り有効にできます。

デバイスのブリッジマルチキャストフィルタリングの有効化

□□□ グローバルパラメータページを開きます。

□□□ **Bridge Multicast Filtering**（ブリッジマルチキャストフィルタリング）フィールドで **Enable**（有効）を選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

デバイスに対してブリッジマルチキャスト フィルタリングが有効になります。

デバイスの IGMP スヌープの有効化

□□□ グローバルパラメータページを開きます。

□□□ **IGMP Snooping Status**（IGMP スヌープステータス）フィールドで **Enable**（有効）を 選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

デバイスに対して IGMP スヌープが有効になります。

CLI コマンドを使用したマルチキャストフィルタリングおよび IGMP スヌープの有効化

次の表は、グローバルパラメータページに表示されているように、マルチキャストフィル タリングと IGMP スヌープを有効にする場合の等価な CLI コマンドをまとめたものです。

表**7-29** マルチキャストフィルタリングおよびスヌープに関連する **CLI** コマンド

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）スヌープを有効にします。

以下に、CLI コマンドの例を示します。

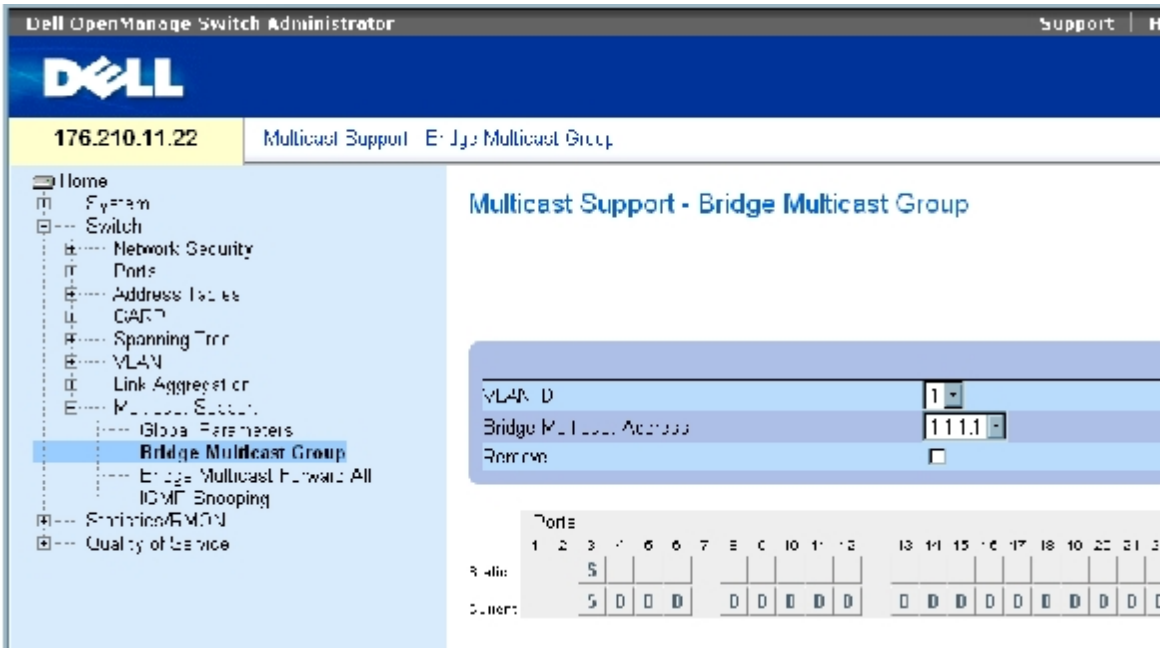
```
console(config)# bridge
multicast filtering

console(config)# ip igmp
snooping
```

ブリッジマルチキャストアドレスメンバーの追加

ブリッジマルチキャストグループページのポート表および **LAG** 表には、マルチキャストサービスグループに加わっているポートおよび LAG が表示されます。ポート 表および LAG 表には、マルチキャストグループに対するポートまたは LAG の加わり方も反映されます。ポートは、既存のグループまたは新規のマルチキャストサービスグループに追加できます。ブリッジマルチキャストグループ ページでは、新規のマルチキャストサービスグループを作成することができます。 ブリッジマルチキャストグループページでは、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ます。

ブリッジマルチキャストグループ ページを開くには、ツリービューで **Switch**（スイッチ）→ **Multicast Support**（マルチキャストサポート）→ **Bridge Multicast Group**（ブリッジマルチキャストグループ）の順にクリックします。

図**7-41** ブリッジマルチキャストグループ



ブリッジマルチキャストグループページには、以下のフィールドがあります。

VLAN ID — VLAN を識別し、マルチキャストグループアドレスに関する情報を示します。

Bridge Multicast Address（ブリッジマルチキャストアドレス）— マルチキャストグループの MAC アドレスまたは IP アドレスを識別します。

Remove（削除）— この項目を選択すると、ブリッジマルチキャストアドレスが削除されます。

Ports（ポート）— マルチキャストサービスに追加できるポートです。

LAG — マルチキャストサービスに追加できる LAG です。

次の表は、IGMP ポートおよび LAG メンバー管理の設定を示したものです。

表**7-30 IGMP**ポート **/LAG** メンバー表のコントロール設定

ポートのコントロール	定義
D	現在列でポートまたは LAG が、マルチキャストグループに動的に加わっています。
S	静的列でポートが、マルチキャストグループに静的メンバーとして加わります。 現在列でポートまたは LAG が、マルチキャストグループに静的に加わっています。
F	禁止されています。
空白	ポートは、マルチキャストグループに加わっていません。

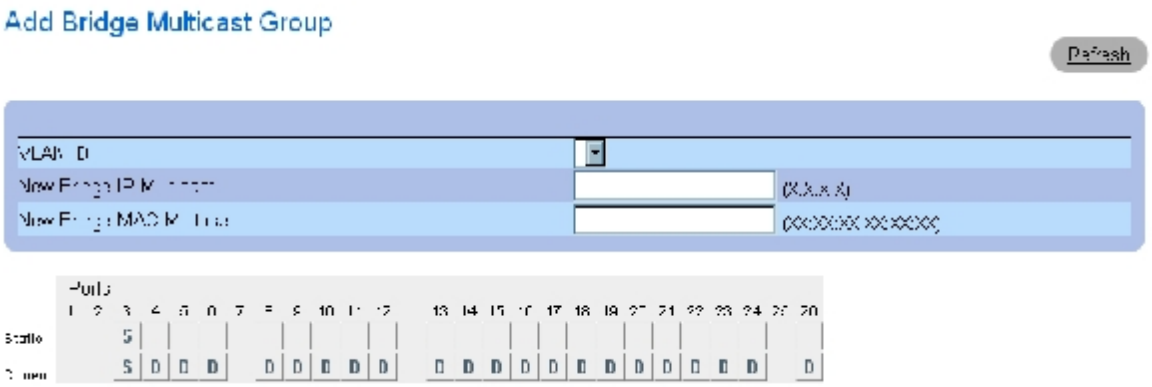
ブリッジマルチキャストアドレスの追加

□□□ ブリッジマルチキャストグループ ページを開きます。

□□□ **Add**（追加）をクリックします。

ブリッジマルチキャストグループの追加ページが開きます。

図**7-42** ブリッジマルチキャストグループの追加



□□□ **VLAN ID** フィールドと **New Bridge Multicast Address**（新規のブリッジマルチキャスト アドレス）フィールドを定義します。

□□□ ポートを **S** に切り替えて、選択したマルチキャストグループに追加します。

□□□ ポートを **F** に切り替えて、特定のマルチキャストアドレスを特定のポートに追加する ことを禁止します。

□□□ **Apply Changes**（変更の適用）をクリックします。

ブリッジマルチキャストアドレス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受信のためのポートの定義

□□□ ブリッジマルチキャストグループ ページを開きます。

□□□ **VLAN ID** フィールドと **Bridge Multicast Address**（ブリッジマルチキャストアドレス） フィールドを定義します。

□□□ ポートを **S** に切り替えて、選択したマルチキャストグループに追加します。

□□□ ポートを **F** に切り替えて、特定のマルチキャストアドレスを特定のポートに追加する ことを禁止します。

□□□ **Apply Changes**（変更の適用）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受信のための **LAG** の割り当て

□□□ ブリッジマルチキャストグループ ページを開きます。

□□□ **VLAN ID** フィールドと **Bridge Multicast Address**（ブリッジマルチキャストアドレス） フィールドを定義します。

□□□ LAG を **S** に切り替えて、選択したマルチキャストグループに追加します。

□□□ LAG を **F** に切り替えて、特定のマルチキャストアドレスを特定の LAG に追加するこ とを禁止します。

□□□ **Apply Changes**（変更の適用）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

次の表は、 ブリッジマルチキャストグループページに表示されているように、マルチキャストサービスメンバーを管理する場合の等価な CLI コマンドをまとめたものです。

表**7-31** マルチキャストサービスメンバーに関連する **CLI** コマンド

CLI コマンド	説明
bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}	MAC 層のマルチキャストアドレスをブリッジ表に登録し、静的ポートをグループに追加します。
bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*}[**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}	特定のマルチキャストアドレスを特定のポートに追加することを禁止します。デフォルトに戻すには、このコマンドの no form を使用してください。
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 アドレス表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-if)# bridge multicast address 0100.5e02.0203

add ethernet 1/e11,1/e12

console(config-if)# end

console # show bridge multicast address-table
```

Vlan	MAC Address	Type	Ports
----	-----------	-----	----------
1	0100.5e02.0203	static	1/e11, 1/e12
19	0100.5e02.0208	static	1/e11-16
19	0100.5e02.0208	dynamic	1/e11-12

```
Forbidden ports for multicast addresses:
```

Vlan	MAC Address	Ports	
----	-----------	----------	
1	0100.5e02.0203	1/e8	
19	0100.5e02.0208	1/e8	

```
console # show bridge multicast address-table format ip
```

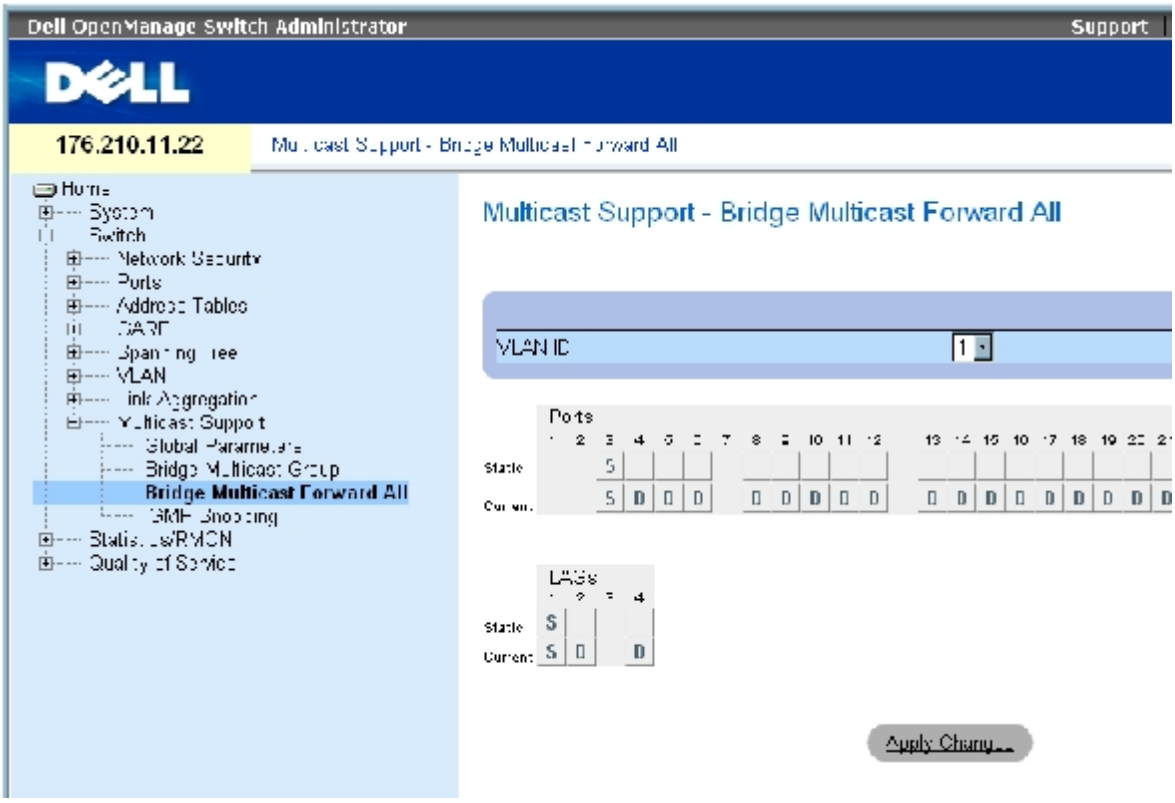
Vlan	IP Address	Type	Ports
----	----------	-----	----------
1	224-239.130|2.2.3	static	1/e11, 1/e12
19	224-239.130|2.2.8	static	1/e11-16
19	224-239.130|2.2.8	dynamic	1/e11-12
Forbidden ports for multicast addresses:			
Vlan	IP Address	Ports	
----	----------	----------	
1	224-239.130|2.2.3	1/e8	
19	224-239.130|2.2.8	1/e8	

マルチキャストすべて転送パラメータの割り当て

ブリッジマルチキャストすべて転送ページには、近隣のマルチキャストルーターまたはスイッチに接続するデバイスに、ポートまたは LAG を割り当てるためのフィールドがあります。IGMP スヌープを有効にすると、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。

ブリッジマルチキャストすべて転送ページを開くには、ツリービューで **Switch**（スイッチ）→ **Multicast Support**（マルチキャストサポート）→ブリッジマルチキャストすべて転送ページの順にクリックします。

図**7-43** ブリッジマルチキャストすべて転送



ブリッジマルチキャストすべて転送ページには、以下のフィールドがあります。

VLAN ID — VLAN を識別します。

Ports（ポート）— マルチキャストサービスに追加できるポートです。

LAG — マルチキャストサービスに追加できる LAG です。

ブリッジマルチキャストすべて転送に対応するスイッチまたはポートのコントロール設定表には、ルーターおよびポートの設定を管理するための設定があります。

ブリッジマルチキャストすべて転送を管理するスイッチまたはポートのコントロール設定表

次の表では、ポートの設定を管理するために使用するコントロールを示します。

表**7-32** ブリッジマルチキャストすべて転送に対応するスイッチまたはポートのコントロール設定表

ポートのコントロール	定義
D	当該のポートをマルチキャストルーターまたはスイッチに動的ポートとして接続します。
S	当該のポートをマルチキャストルーターまたはスイッチに静的ポートとして接続します。
F	禁止されています。
空白	当該のポートは、マルチキャストルーターまたはスイッチに接続されていません。

ポートのマルチキャストルーターまたはスイッチへの接続

□□□ ブリッジマルチキャストすべて転送ページを開きます。

□□□ **VLAN ID** フィールドを定義します。

□□□ ポート 表からポートを選択し、そのポートに値を割り当てます。

□□□ **Apply Changes**（変更の適用）をクリックします。

当該のポートがマルチキャストルーターまたはスイッチに接続されます。

LAG のマルチキャストルーターまたはスイッチへの接続

□□□ ブリッジマルチキャストすべて転送ページを開きます。

□□□ **VLAN ID** フィールドを定義します。

□□□ **LAG** 表からポートを選択し、その LAG に値を割り当てます。

□□□ **Apply Changes**（変更の適用）をクリックします。

当該の LAG がマルチキャストルーターまたはスイッチに接続されます。

CLI コマンドを使用したマルチキャストルーターに接続する LAG およびポートの管理

次の表は、 ブリッジマルチキャストすべて転送ページに表示されているように、マルチキャストルーターに接続された LAG およびポートを管理する場合の等価な CLI コマンドをまとめたものです。

表**7-33** マルチキャストルーターに接続された **LAG** およびポートを管理するための **CLI** コマンド

CLI コマンド	説明
show bridge multicast filtering *vlan-id*	マルチキャストフィルタリングの設定を表示します。
bridge multicast forward-all {add | remove} {ethernet *interface-list* **| port-channel** *port-channel-number-list*}	ポートに対してすべてのマルチキャストパケットの転送を有効にします。デフォルトに戻すには、このコマンドの no form を使用してください。

以下に、CLI コマンドの例を示します。

```
Console(config)# interface vlan 1

Console(config-if)# bridge multicast forward-all add ethernet 1/e3

Console(config-if)# end

Console# show bridge multicast filtering 1
```

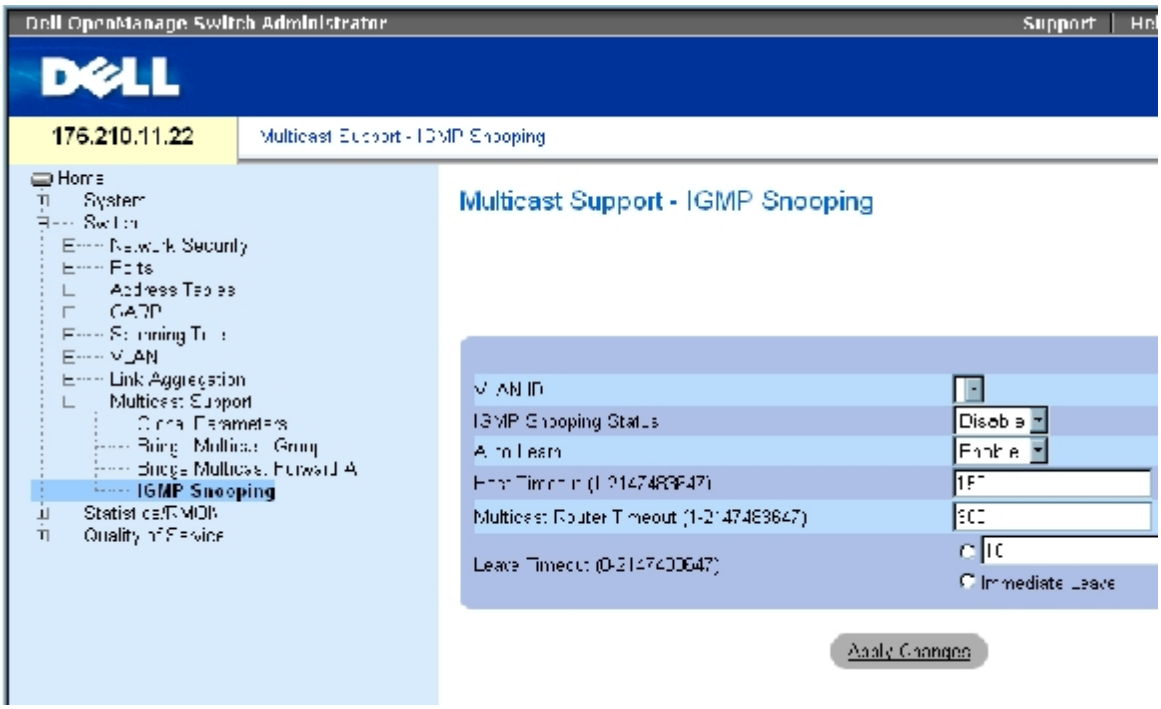
Filtering:Enabled		
VLAN:	Forward-All	
Port	Static	Status

| ------- | ---------- | ---------- |
1/e11	Forbidden	Filter
1/e12	Forward	Forward(s)
1/e13	-	Forward(d)

IGMP スヌープ

IGMP スヌープページには、VLAN ごとに IGMP スヌープを有効にし、パケットのエージング時間を定義するためのフィールドがあります。**IGMP** スヌープページを開くには、ツリービューで **Switch**（スイッチ）→ **Multicast Support**（マルチキャストサポート）→ **IGMP Snooping**（IGMP スヌープ）の順にクリックします。

図**7-44 IGMP** スヌープ



VLAN ID — VLAN ID を指定します。

IGMP Snooping Status（IGMP スヌープステータス）— VLAN に対して IGMP スヌープを有効または無効にします。

Auto Learn（自動学習）— Ethernet デバイスに対して自動学習を有効または無効にします。

Host Timeout (1-2147483647)（ホストのタイムアウト）（1～2147483647）— IGMP スヌープのエントリがエージアウトするまでの時間です。デフォルトの時間は 260 秒です。

Multicast Router Timeout (1-2147483647)（マルチキャストルーターのタイムアウト）（1～2147483647）— マルチキャストルーターのエントリがエージアウトするまでの時間です。デフォルト値は 300 秒です。

Leave Timeout (0-2147483647)（Leave のタイムアウト）（0～2147483647）— ポート Leave メッセージが受信された後、エントリがエージアウトするまでの時間（秒単位）です。デフォルトのタイムアウト時間は 10 秒です。

デバイスの IGMP スヌープの有効化

□□□ IGMP スヌープページを開きます。

□□□ IGMP スヌープを有効にする必要があるデバイスの VLAN ID を選択します。

□□□ **IGMP Snooping Status**（IGMP スヌープステータス）フィールドで **Enable**（有効）を 選択します。

□□□ ページ上のフィールドを完了します。

□□□ **Apply Changes**（変更の適用）をクリックします。

IGMP スヌープがデバイスで有効になります。

IGMP スヌープ表の表示

□□□ IGMP スヌープを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

IGMP スヌープ表が開きます。

CLI コマンドを使用した IGMP スヌープの設定

次の表は、デバイスに対してIGMP スヌープを設定する場合の等価な CLI コマンドをまとめたものです。

表**7-34 IGMP** スヌープに関連する **CLI** コマンド

CLI コマンド	説明
ip igmp snooping	IGMP（Internet Group Management Protocol）スヌープを有効にします。
ip igmp snooping mrouter learn-pim-dvmrp	特定の VLAN のコンテキストでマルチキャストルーターポートの自動学習を有効にします。
ip igmp snooping host-time-out time-out	ホストのタイムアウト（host-time-out）を設定します。
ip igmp snooping mrouter-time-out *time-out*	エムルーターのタイムアウト（mrouter-time-out）を設定します。
ip igmp snooping leave-time-out {*time-out* | **immediate-leave**}	Leave のタイムアウト（leave-time-out）を設定します。
show ip igmp snooping groups [**vlan** *vlan-id*] [**address** *ip-multicast-address*]	IGMP スヌープによって学習されたマルチキャストグループを表示します。
show ip igmp snooping interface *vlan-id*	IGMP スヌープの設定を表示します。
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ー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> enable

console# config
```

```
console(config)# ip igmp snooping

console(config)# interface vlan 1

console(config-if)# ip igmp
snooping mrouter learn-pim-dvmrp

console(config-if)# ip igmp
snooping host-time-out 300

Console(config-if)# ip igmp
snooping mrouter-time-out 200

console(config-if)# ip igmp
snooping leave-time-out 60

console(config-if)# end

console# show ip igmp snooping
groups
```

Vlan	IP Address	Querier	Ports
1	224-239.130|2.2.3	Yes	1/e11, 1/e12
19	224-239.130|2.2.8	Yes	1/e11-13

```
console# show ip igmp snooping
interface 1/e1

IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1

IGMP host timeout is 300 sec

IGMP Immediate leave is
disabled.IGMP leave timeout is 60
sec

IGMP mrouter timeout is 200 sec

Automatic learning of multicast
router ports is enabled

console# show ip igmp snooping
mrouter
```

VLAN	Ports		
1	1/e11		

メモ、注意および警告

メモ、注意および警告

統計の表示

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

統計ページには、インタフェース、GVRP、Etherlike、RMON、およびデバイスの利用率に関するデバイス情報があります。統計ページを開くには、ツリービューで **Statistics**（統計）をクリックします。

メモ： すべての統計ページに CLI コマンドを使用できるわけではありません。

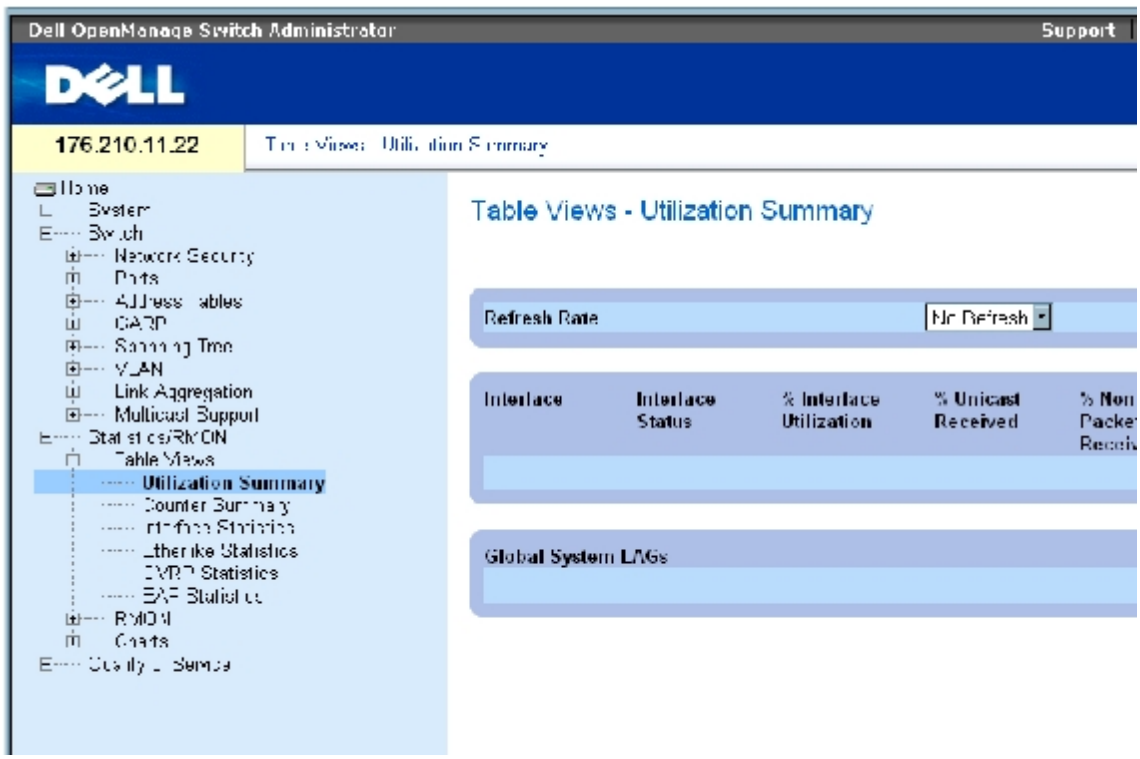
表の表示

表の表示ページには、統計を表形式で表示するためのリンクがあります。表の表示ページを開くには、ツリービューで **Statistics**（統計）→ **Table**（表）の順にクリックします。

利用率の要約の表示

利用率の要約ページには、インタフェースの利用率に関する統計があります。利用率の要約ページを開くには、**Statistics**（統計）→ **Table Views**（表の表示）→ **Utilization Summary**（利用率の要約）の順にクリックします。

図 **8-1** 利用率の要約



メモ： この画面は、メモリ容量の小さいコンピュータに対する影響を最小限に抑えるため に、定期的に更新されます。その間に表示が中断する場合があります。

利用率の要約ページには、以下のフィールドがあります。

Refresh Rate（リフレッシュレート）— インタフェース統計が更新される間隔を示します。

Interface（インタフェース）— インタフェースの番号です。

Interface Status （インタフェースステータス）— インタフェースの状態です。

% Interface Utilization （% インタフェース利用率）— インタフェースの二重モードに基づいたネットワークインタフェース利用率のパーセンテージです。この読み取り範囲は 0～200% です。全二重接続の最大読み取り値の 200% は、入力接続および出力接続の帯域幅がインタフェースを通過するトラフィックによって 100% 使用されていることを示します。半二重接続の最大読み取り値は 100% です。

% Unicast Received（受信されたユニキャストの %）— インタフェースで受信されたユニキャストパケットのパーセンテージです。

% Non Unicast Packets Received（受信された非ユニキャストパケットの %）— インタフェースで受信された非ユニキャストパケットのパーセンテージです。

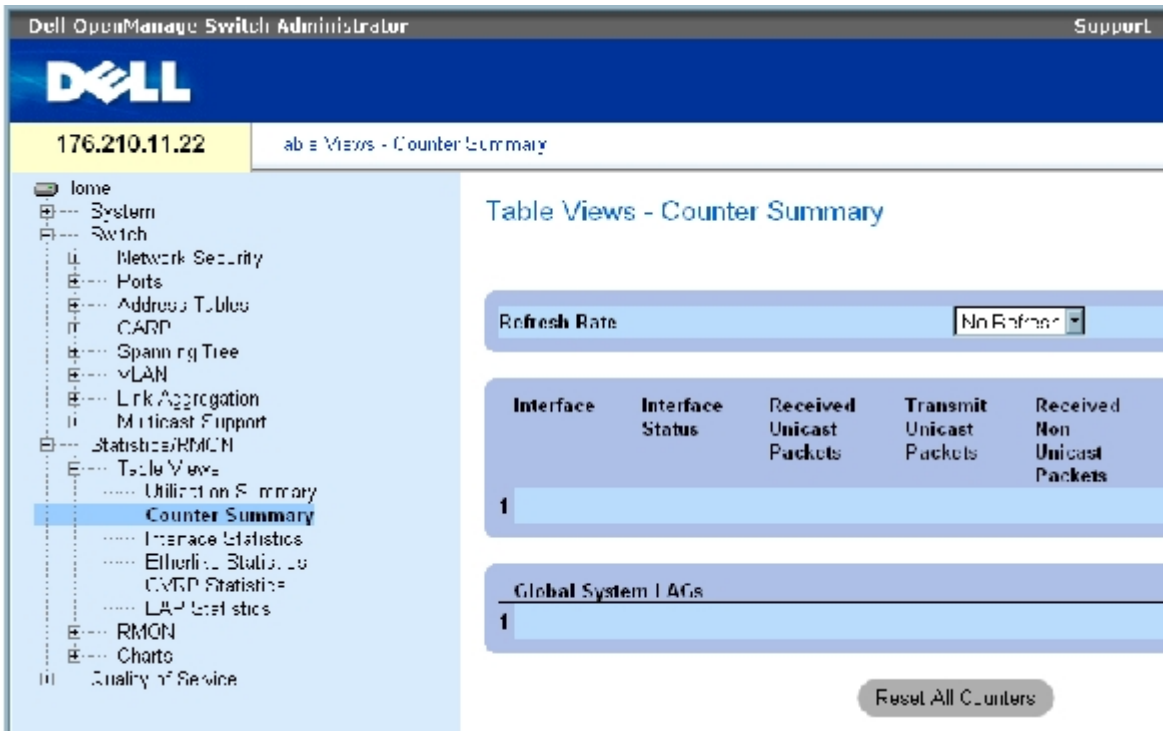
% Error Packets Received（受信されたエラーパケットの %）— インタフェースで受信されたエラーのあるパケットのパーセンテージです。

Global System LAGs（グローバルシステム LAG）— 現在のグローバル LAG の利用率を示します。

カウンタの要約の表示

カウンタの要約ページには、ポート利用率をパーセンテージではなく数値の合計で表示する統計があります。カウンタの要約ページを開くには、ツリービューで **Statistics/RMON**（統計 /RMON）→ **Table Views**（表の表示）→ **Counter Summary**（カウンタの要約）の順にクリックします。

図**8-2** カウンタの要約



カウンタの要約ページには、以下のフィールドがあります。

Refresh Rate（リフレッシュレート）— インタフェース統計が更新される間隔を示します。

Interface（インタフェース）— インタフェースの番号です。

Interface Status（インタフェースステータス）— インタフェースの状態です。

Received Unicast Packets（受信されたユニキャストパケット）— インタフェースで受信されたユニキャストパケットの数です。

Transmit Unicast Packets（送信されたユニキャストパケット）— 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数です。

Received Non Unicast Packets（受信された非ユニキャストパケット）— インタフェースで受信された非ユニキャストパケットの数です。

Transmit Non Unicast Packets（送信された非ユニキャストパケット）— インタフェースから送信された非ユニキャストパケットの数です。

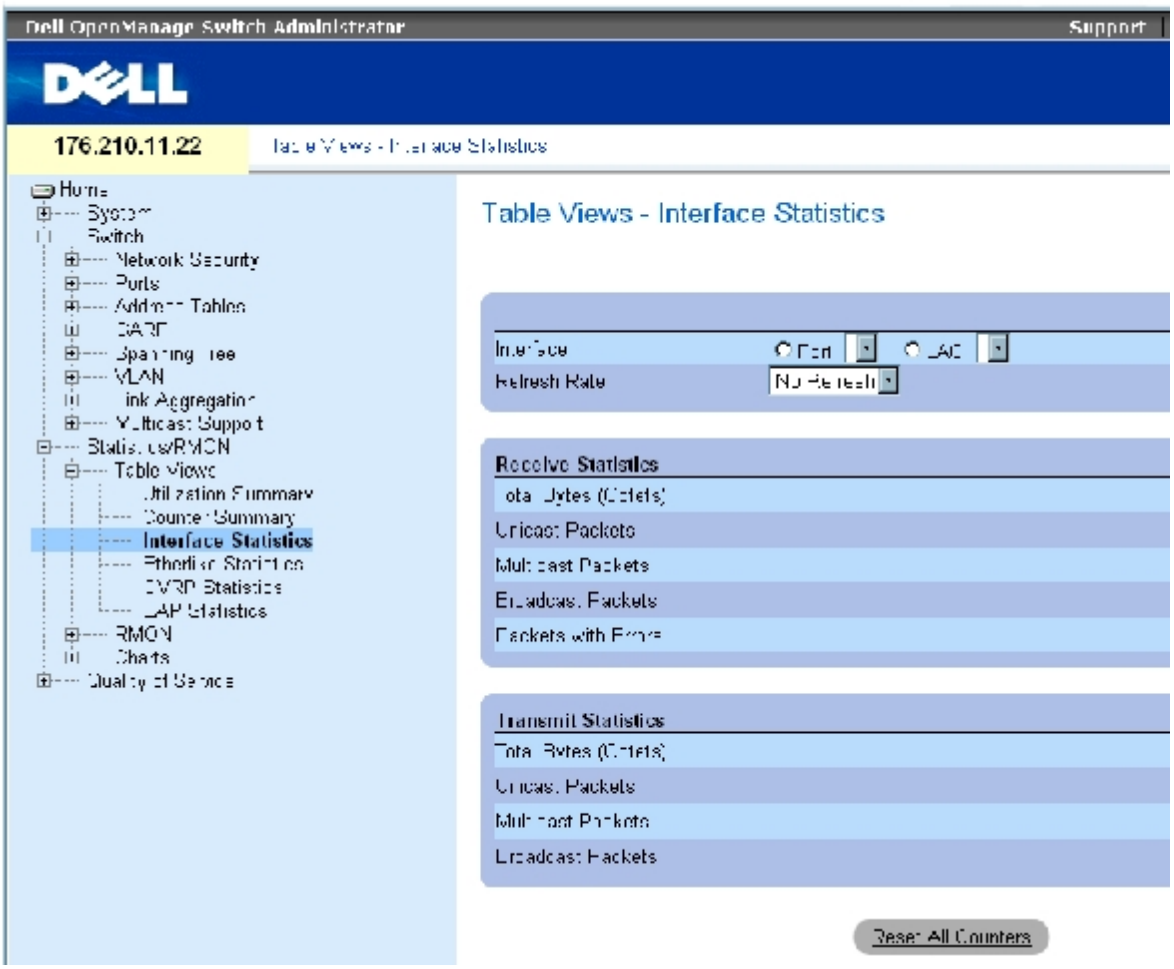
Received Errors（受信されたエラー）— インタフェースで受信されたエラーパケットの数です。

Global System LAGs（グローバルシステム LAG）— グローバルシステム LAG のカウンタの要約を示します。

インタフェース統計の表示

インタフェース統計ページには、受信されたパケットと送信されたパケットの両方に関する統計があります。受信されたパケットと送信されたパケットのフィールドは同じです。インタフェース統計ページを開くには、ツリービューで **Statistics/RMON**（統計 /RMON）→ **Table Views**（表の表示）→ **Interface Statistics**（インタフェース統計）の順にクリックします。

図**8-3** インタフェース統計



インタフェース統計 ページには、以下のフィールドがあります。

Interface（インタフェース）— 表示される統計がポートについてか LAG についてかを指定します。

Refresh Rate（リフレッシュレート）— インタフェース統計がリフレッシュされるまでに経過する時間です。

統計の受信

Total Bytes (Octets)（総バイト数）（オクテット）— 選択したインタフェースで受信されたオクテットの数です。

Unicast Packets（ユニキャストパケット）— 選択し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数です。

Multicast Packets（マルチキャストパケット）— 選択し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数です。

Broadcast Packets（ブロードキャストパケット）— 選択し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数です。

統計の送信

Total Bytes (Octets)（総バイト数）（オクテット）— 選択したインタフェースから送信されたオクテットの数です。

Unicast Packets（ユニキャストパケット）— 選択し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数です。

Multicast Packets（マルチキャストパケット）— 選択し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数です。

Broadcast Packets（ブロードキャストパケット）— 選択し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数です。

インタフェース統計の表示

□□□ インタフェース統計 ページを開きます。

□□□ **Interface**（インタフェース）フィールドでインタフェースを選択します。

選択したインタフェースのインタフェース統計が表示されます。

インタフェース統計カウンタのリセット

□□□ インタフェース統計 ページを開きます。

□□□ **Reset All Counters**（すべてのカウンタのリセット）をクリックします。

インタフェース統計カウンタがリセットされます。

CLI コマンドを使用したインタフェース統計の表示

次の表は、インタフェース統計を表示する場合の CLI コマンドを示したものです。

表**8-1** インタフェース統計に関連する **CLI** コマンド

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。

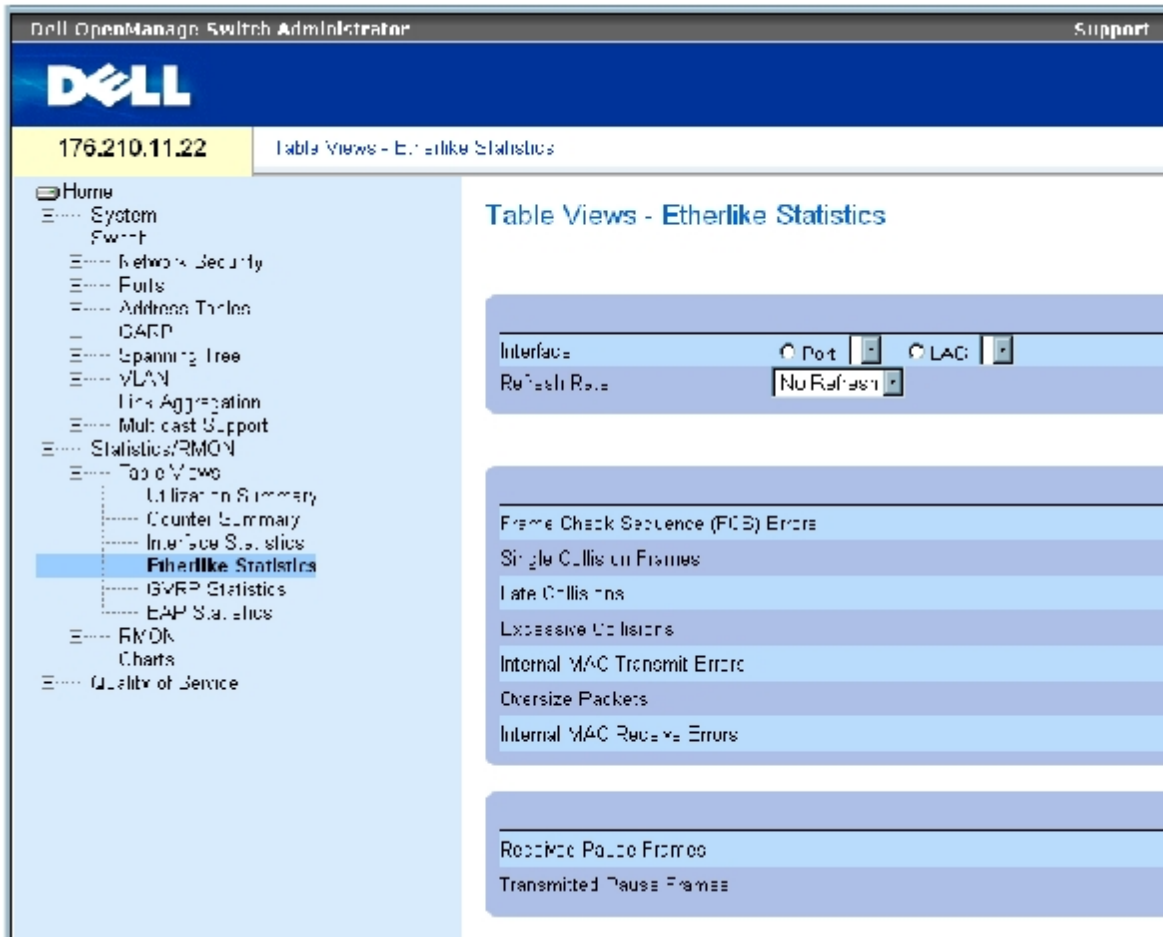
```
console> enable

console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

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

1/e1 0 0 0 0

1/e2 0 0 0 0

1/e3 0 0 0 0
```

```
1/e4 0 0 0 0

1/e5 0 0 0 0

1/ e6 0 0 0 0

1/e7 0 0 0 0

1/e8 0 0 0 0

1/e9 0 0 0 0

1/e10 0 0 0 0
```

Etherlike 統計の表示

Etherlike 統計ページには、インタフェースエラー統計があります。**Etherlike** 統計ページを開くには、ツリービューで **Statistics/RMON**（統計 /RMON）→ **Table Views**（表の表示）→ **Etherlike Statistics**（Etherlike 統計）の順にクリックします。

図**8-4 Etherlike** 統計



Etherlike 統計 ページには、以下のフィールドがあります。

Interface（インタフェース）— 表示される統計がポートについてか LAG についてかを指定します。

Refresh Rate（リフレッシュレート）— インタフェース統計がリフレッシュされるまでに経過する時間です。

Frame Check Sequence (FCS) Errors（フレームチェックシーケンス（FCS）エラー）— 選択したインタフェースで受信された FCS エラーの数です。

Single Collision Frames（シングル衝突フレーム）— 選択したインタフェースで受信されたシングル衝突フレームエラーの数です。

Late Collisions（遅い衝突）— 選択したインタフェースで受信された遅い衝突の数です。

Oversize Packets（オーバーサイズパケット）— 選択したインタフェースにおけるオーバーサイズパケットの数です。

Internal MAC Transmit Errors（内蔵 MAC 送信エラー）— 選択したインタフェースにおける内蔵 MAC 送信エラーの数です。

Received Pause Frames（ポーズフレームの受信）— 選択したインタフェースにおける受信されたポーズフレームの数です。

Transmitted Pause Frames（送信されたポーズフレーム）— 選択したインタフェースから送信されたポーズフレームの数です。

インタフェースの **Etherlike** 統計の表示

□□□ **Etherlike** 統計 ページを開きます。

□□□ **Interface**（インタフェース）フィールドでインタフェースを選択します。

Etherlike 統計のリセット

□□□ **Etherlike** 統計 ページを開きます。

□□□ **Reset All Counters**（すべてのカウンタのリセット）をクリックします。

Etherlike 統計カウンタがリセットされます。

CLI コマンドを使用した **Etherlike** 統計の表示

次の表は、Etherlike 統計を表示する場合の CLI コマンドを示したものです。

表**8-2 Etherlike** 統計に関連する **CLI** コマンド

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。

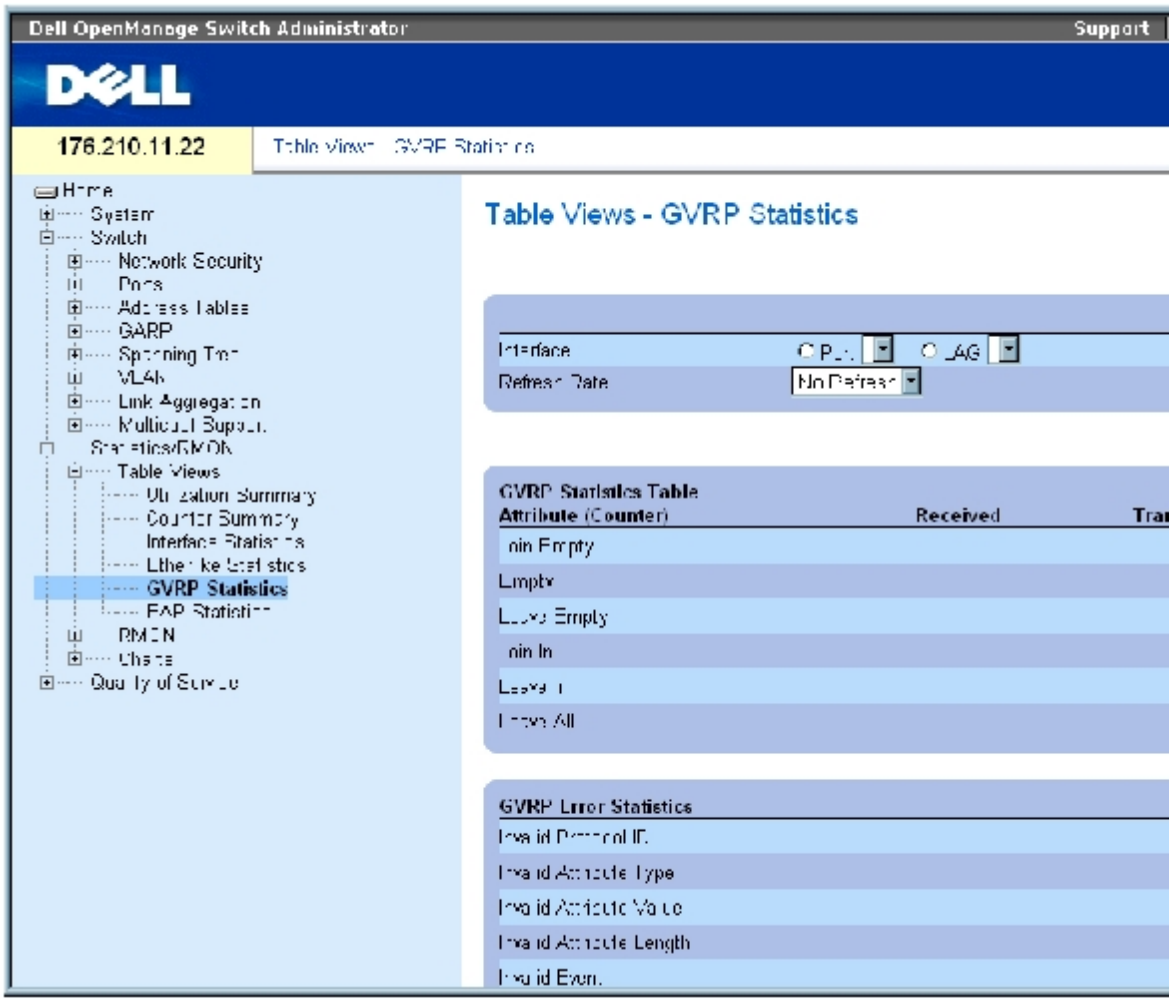
```
Console# show interfaces counters ethernet 1/1
```

Port	IN Octets	InUcastPkts	InMcastPkts	InBcastPkts
1/e1	183892	1289	987	8
Port	OUT Octets	OutUcastPkts	OutMcastPkts	OutBcastPkts
1/e1	9188	9	8	0
FCS Errors: 8				
Single Collision Frames: 0				
Multiple Collision Frames: 0				
SQE Test Errors: 0				
Deferred Transmissions: 0				
Late Collisions: 0				
Excessive Collisions: 0				
Internal MAC Tx Errors: 0				
Carrier Sense Errors: 0				
Oversize Packets: 0				
Internal MAC Rx Errors: 0				
Received Pause Frames: 0				
Transmitted Pause Frames: 0				

GVRP 統計の表示

GVRP 統計ページには、GVRP のデバイス統計が含まれます。GVRP 統計ページを開くには、ツリービューで **Statistics/RMON**（統計/RMON）→ **Table Views**（表の表示）→ **GVRP Statistics**（GVRP 統計）の順にクリックします。

図**8-5 GVRP** 統計



GVRP 統計 ページには、以下のフィールドがあります。

Interface（インタフェース）— 表示される統計がポートについてか LAG についてかを指定します。

Refresh Rate（リフレッシュレート）— インタフェース統計がリフレッシュされるまでに経過する時間です。

Join Empty（空への参加）— デバイス GVRP の空への参加統計です。

Leave Empty（空で残す）— デバイス GVRP の空で残す統計です。

Empty（空）— GVRP 空統計の数を示します。

Join In（参加）— デバイス GVRP 参加統計です。

Leave In（残留）— デバイス GVRP 残留統計です。

Leave All（すべてを残す）— デバイス GVRP のすべてを残す統計です。

Invalid Protocol ID（無効なプロトコル ID）— デバイス GVRP 無効プロトコル ID の統計です。

Invalid Attribute Type（無効な属性タイプ）— デバイス GVRP 無効属性 ID の統計です。

Invalid Attribute Value（無効な属性値）— デバイス GVRP 無効属性値の統計です。

Invalid Attribute Length（無効な属性の長さ）— デバイス GVRP 無効属性の長さの統計です。

Invalid Event（無効なイベント）— デバイス GVRP 無効イベントの統計です。

ポートの GVRP 統計の表示

□□□ GVRP 統計ページを開きます。

□□□ **Interface**（インタフェース）フィールドでインタフェースを選択します。

選択したインタフェースの GVRP 統計が表示されます。

GVRP 統計のリセット

□□□ GVRP 統計ページを開きます。

□□□ **Reset All Counters**（すべてのカウンタのリセット）をクリックします。

GVRP 統計カウンタがリセットされます。

CLI コマンドを使用した GVRP 統計の表示

次の表は、GVRP 統計を表示する場合の CLI コマンドを示したものです。

表**8-3 GVRP** 統計に関連する **CLI** コマンド

CLI コマンド	説明
show gvrp statistics [**ethernet** *interface* | **port-channel** *port- channel-number*]	GVRP の統計を表示します。
show gvrp error- statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	GVRP エラー 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 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 00 0
```

```
Console# show gvrp error-statistics

GVRP error statistics:

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

Legend:

INVPROT :Invalid Protocol Id

INVPLEN :Invalid PDU Length

INVATYP :Invalid Attribute Type

INVALEN :Invalid Attribute Length

INVAVAL :Invalid Attribute Value

INVEVENT :Invalid Event

Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

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

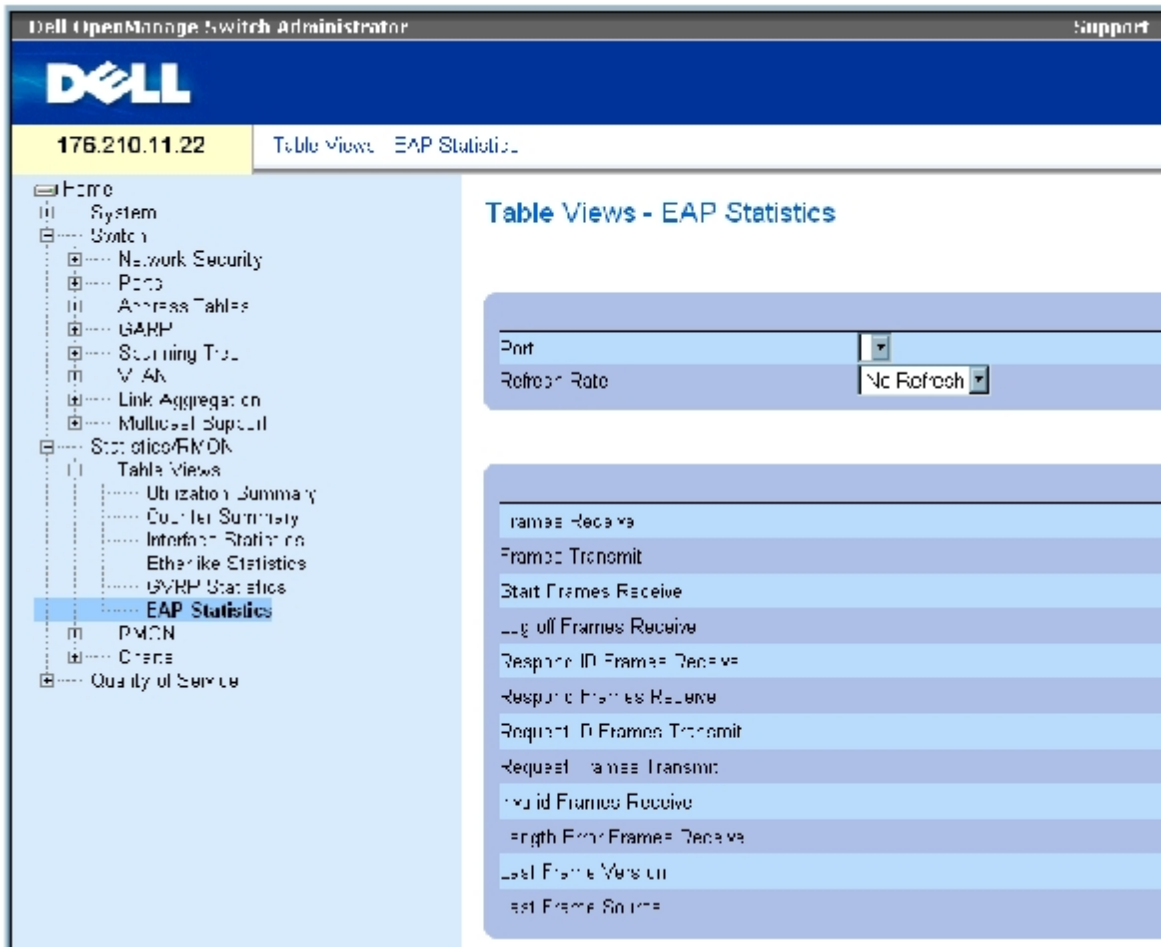
```
1/e1 0 0 0 0 0 0

1/e2 0 0 0 0 0 0

1/e3 0 0 0 0 0 0

1/e4 0 0 0 0 0 0
```

```
sLE :Leave Empty Sent

sLA :Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn
sLE sLA

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

1/e1 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0 0 0 0 0 0

1/e5 0 0 0 0 0 0 0 0 0 0 0 0

1/e6 0 0 0 0 0 0 0 0 0 0 0 0

1/e7 0 0 0 0 0 0 0 0 0 0 0 0

1/e8 0 0 0 0 0 0 0 0 0 0 0 0
```

EAP 統計の表示

EAP 統計ページには、特定のポートで受信された EAP パケットに関する情報があります。EAP の詳細については、「ポートベース認証の設定」を参照してください。**EAP** 統計ページを開くには、ツリービューで Statistics/RMON（統計 /RMON）→ Table Views（表の表示）→EAP Statistics（EAP 統計）の順にクリックします。

図**8-6 EAP** 統計



EAP 統計ページには、以下のフィールドがあります。

Port（ポート）— 統計を得るためにポーリングされるポートを示します。

Refresh Rate（リフレッシュレート）— インタフェース統計がリフレッシュされるまでに経過する時間です。

Frames Receive（フレーム受信）— ポートで受信された有効な EAPOL フレームの数を示します。

Frames Transmit（フレーム送信）— ポートを介して送信された EAPOL フレームの数です。

Start Frames Receive（スタートフレーム受信）— ポートで受信された EAPOL スタートフレームの数を示します。

Log off Frames Receive（ログオフフレーム受信）— ポートで受信された EAPOL ログオフフレームの数を示します。

Respond ID Frames Receive（応答 ID フレーム受信）— ポートで受信された EAP Resp/Id フレームの数を示します。

Respond Frames Receive（応答フレーム受信）— ポートで受信された有効な EAP 応答フレームの数を示します。

Request ID Frames Transmit（要求 IDフレーム送信）— ポートを介して送信された EAP 要求 ID フレームの数を示します。

Request Frames Transmit（要求フレーム送信）— ポートを介して送信された EAP 要求フレームの数を示します。

Invalid Frames Receive（無効なフレーム受信）— このポートで受信された未認識 EAPOL フレームの数を示します。

Length Error Frames Receive（長さエラーフレーム受信）— このポートで受信された無効なパケットボディの長さを有する EAPOL フレームの数を示します。

Last Frame Version（最後のフレームバージョン）— 最後に受信された EAPOL フレームに付されたプロトコルバージョンの番号を示します。

Last Frame Source（最後のフレームソース）— 最後に受信された EAPOL フレームに付されたソース MAC アドレスを示します。

ポートの **EAP** 統計の表示

□□□ **EAP** 統計ページを開きます。

□□□ **Interface**（インタフェース）フィールドでインタフェースを選択します。

インタフェース EAP 統計が表示されます。

EAP 統計のリセット

□□□ **EAP** 統計ページを開きます。

□□□ **Reset All Counters**（すべてのカウンタのリセット）をクリックします。

EAP 統計カウンタがリセットされます。

CLI コマンドを使用した **EAP** 統計の表示

次の表は、EAP 統計を表示する場合の CLI コマンドをまとめたものです。

表**8-4 EAP** 統計に関連する **CLI** コマンド

CLI コマンド	説明
show dot1x statistics	指定したインタフェースの 802.1X 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 dot1x statistics ethernet 1/e1

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3
```

```
EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource:0008.3b79.8787
```

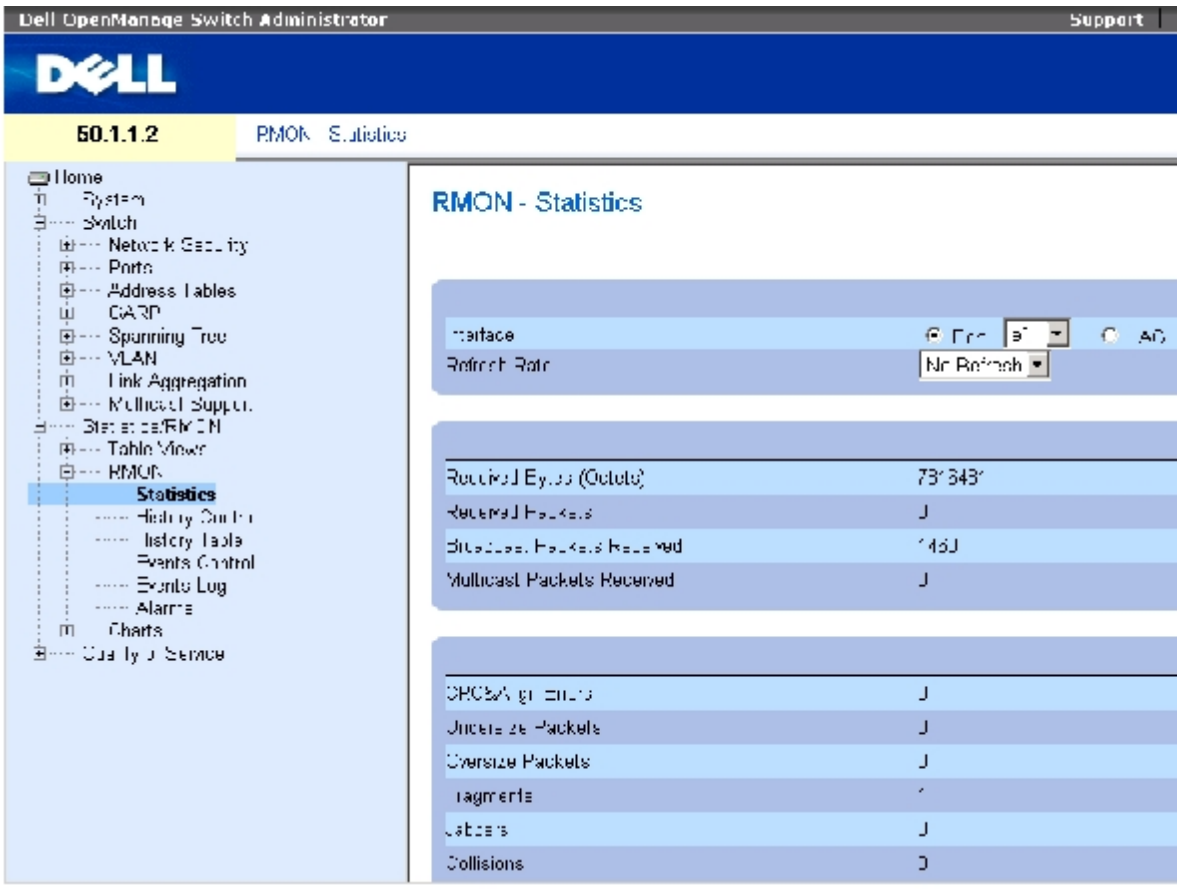
RMON 統計の表示

リモートモニタリング（RMON）では、ネットワーク管理者がリモートロケーションからのネットワーク情報を表示することができます。**RMON** ページを開くには、ツリービューで **Statistics / RMON**（統計 /RMON）→ **RMON** の順にクリックします。

RMON 統計グループの表示

デバイスの利用率およびデバイスに発生したエラーに関する RMON 統計ページ表示情報を使用します。RMON 統計ページを開くには、ツリービューで **Statistics / RMON**（統計 /RMON）→ **RMON**→ **Statistics**（統計）の順にクリックします。

図**8-7 RMON** 統計



RMON 統計ページには、以下のフィールドがあります。

Interface（インタフェース）— 統計が表示されるポートまたは LAG を指定します。

Refresh Rate（リフレッシュレート）— 統計がリフレッシュされるまでに経過する時間です。

Received Bytes (Octets)（受信されたバイト）（オクテット）— 選択したインタフェースで受信されたバイト数です。

Received Packets（受信されたパケット）— 選択したインタフェースで受信されたパケットの数です。

Broadcast Packets Received（受信されたブロードキャストパケット）— デバイスが最後にリフレッシュされてからインタフェースで受信された優良なブロードキャストパケットの数です。この数にはマルチキャストパケットは含まれません。

Multicast Packets Received（受信されたマルチキャストパケット）— システムが最後にリフレッシュされてからインタフェースで受信された優良なマルチキャストパケットの数です。

CRC & Align Errors（CRC および調整エラー）— デバイスが最後にリフレッシュされてからインタフェースで発生した CRC エラーおよび調整エラーの数です。

Undersize Packets（アンダーサイズパケット）— システムが最後にリフレッシュされてからインタフェースで受信されたアンダーサイズパケット（64 オクテット未満）のパケットの数です。

Oversize Packets（オーバーサイズパケット）— デバイスが最後にリフレッシュされてからインタフェースで受信されたオーバーサイズパケット（1518 オクテット超）のパケット数です。

Fragments（フラグメント）— デバイスが最後にリフレッシュされてからインタフェースが受信したフラグメント（フレーミングビットは含まないが FCS オクテットを含む、64 オクテット未満のパケット）の数です。

Jabbers（ジャバー）— デバイスが最後にリフレッシュされてからインタフェースで受信されたジャバー（1518 オクテットより長いパケット）の数です。

Collisions（衝突）— デバイスが最後にリフレッシュされてからインタフェースで受信された衝突の数です。

Frames of *xx* Bytes（バイトのフレーム）— デバイスが最後にリフレッシュされてからインタフェースで受信された *xx* バイトのフレームの数です。

インタフェース統計の表示

□□□ RMON 統計 ページを開きます。

□□□ **Interface**（インタフェース）フィールドでインタフェースのタイプと番号を選択しま す。

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 RMON 統計の表示

次の表は、RMON 統計を表示する場合の CLI コマンドを示したものです。

表**8-5 RMON** 統計に関連する **CLI** コマンド

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。

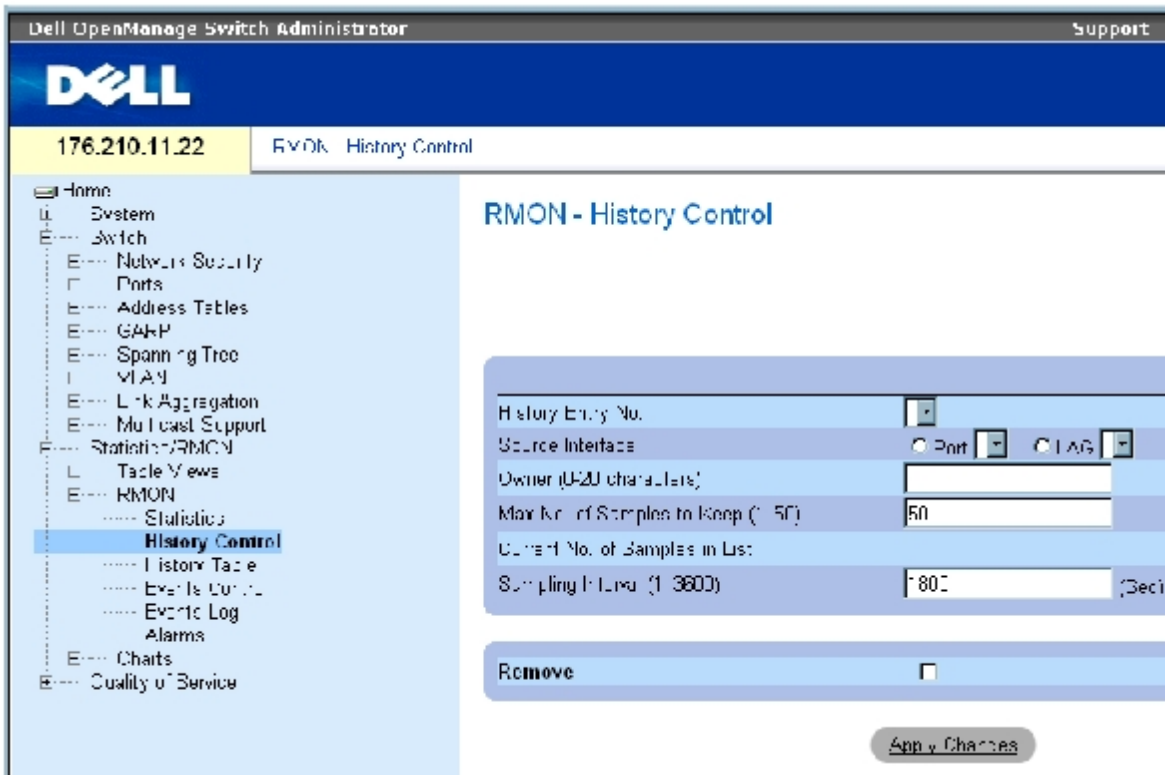
以下に、CLI コマンドの例を示します。

```
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
```

RMON ヒストリ制御統計の表示

RMON ヒストリ制御には、ポートから取ったデータのサンプルに関する情報があります。たとえば、サンプルにはインタフェース定義またはポーリング期間が含まれることがあります。**RMON** ヒストリ制御 ページを開くには、ツリービューで **Statistics / RMON**（統計 /RMON）→**RMON**→ **History Control**（ヒストリ制御）の順にクリックします。

図**8-8 RMON** ヒストリ制御



RMON ヒストリ制御ページには、以下のフィールドがあります。

History Entry No.（ヒストリエントリの番号）— ヒストリ制御ページのエントリの番号です。

Source Interface（ソースインタフェース）— ヒストリサンプルが取られたポートまたは LAG です。

Owner (0-20 characters)（オーナー）（0～20 文字）— RMON 情報を要求した RMON ステーションまたはユーザーです。

Max No. of Samples to Keep (1-50)（保存するサンプルの最大の番号）（1～50）— 保存されるサンプルの数です。デフォルト値は 50 です。

Current No. of Samples in List（リストにあるサンプルの現在の番号）— 得られたサンプルの現在の番号を示します。

Sampling Interval (1-3600)（サンプルの間隔）（1～3600）— サンプルがポートから得られる間隔を秒で示します。可能な値は、1～3600 秒です。デフォルトは 1800 秒（30 分）です。

Remove（削除）— このオプションを選択すると、ヒストリ制御表エントリが削除されます。

ヒストリ制御エントリの追加

□□□ **RMON** ヒストリ制御 ページを開きます。

□□□ **Add**（追加）をクリックします。

ヒストリエントリの追加ページが開きます。

□□□ ダイアログ内のフィールドを完成させます。

□□□ **Apply Changes**（変更の適用）をクリックします。

エントリがヒストリ制御表に追加されます。

ヒストリ制御表エントリの変更

□□□ **RMON** ヒストリ制御 ページを開きます。

□□□ **History Entry No.**（ヒストリエントリの番号）フィールドでエントリを選択します。

□□□ 必要に応じてフィールドを変更します。

□□□ **Apply Changes**（変更の適用）をクリックします。

表エントリが変更され、デバイスがアップデートされます。

ヒストリ制御表エントリの削除

□□□ **RMON** ヒストリ制御 ページを開きます。

□□□ **History Entry No.**（ヒストリエントリの番号）フィールドでエントリを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

表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 RMON ヒストリ制御の表示

次の表は、RMON ヒストリ制御を表示する CLI コマンドを示したものです。

表**8-6 RMON** ヒストリに関連する **CLI** コマンド

CLI コマンド	説明
rmon collection history index [**owner** *ownername* | **buckets** *bucket-number*] [**interval** *seconds*]	インタフェースに対して RMON を有効にし、設定します。
show rmon collection history [**ethernet** *interface* | **port-channel** *port-channel-number*]	RMON 収集ヒストリ統計を表示します。

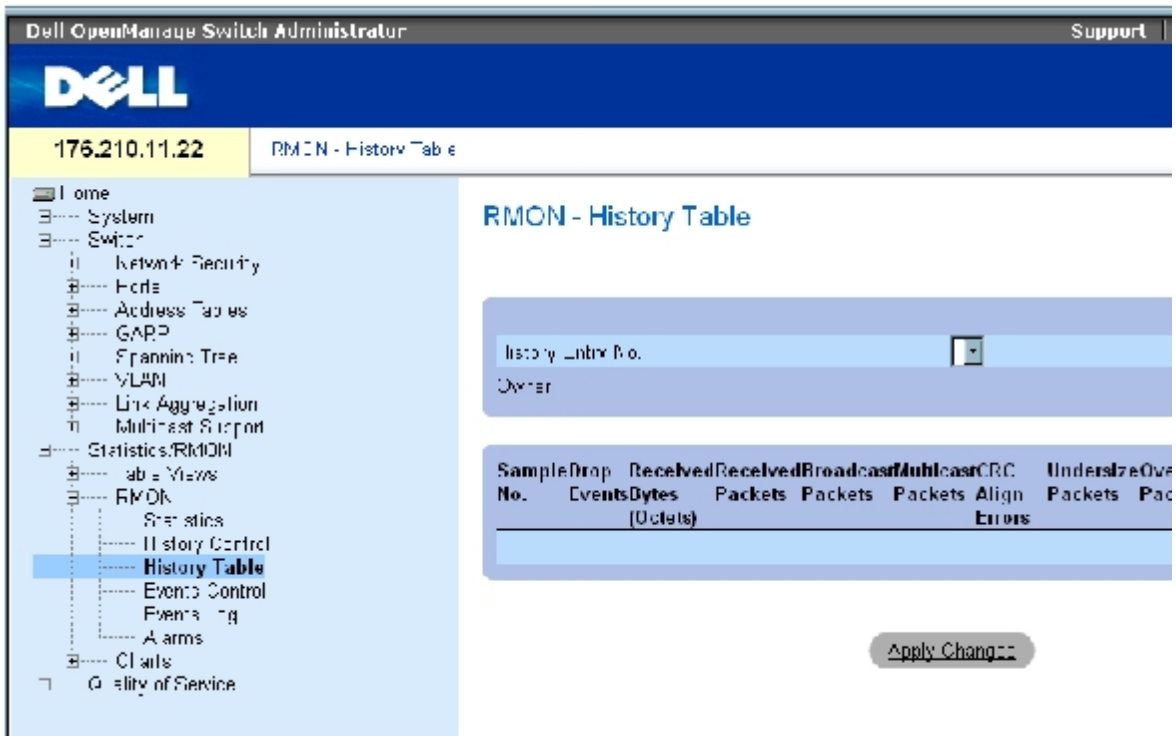
以下に、CLI コマンドの例を示します。

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

console(config-if)# rmon collection history 1
interval 2400
```

RMON ヒストリ表の表示

RMON ヒストリ表には、インタフェースに固有の統計ネットワークサンプルがあります。各表エントリは、1 回のサンプル収集中に編集されたすべてのカウンタ値を表します。**RMON** ヒストリ表を開くには、ツリービューで **Statistics / RMON**（統計 **/ RMON**）→ **RMON**→ **History Table**（ヒストリ表）の順にクリックします。

図**8-9 RMON** ヒストリ表



RMON ヒストリ表 ページには、以下のフィールドがあります。

メモ： すべてのフィールドが RMON ヒストリ表で表示されるわけではありません。

History Entry No.（ヒストリエントリの番号）— ヒストリ制御ページのエントリの番号を指定します。

Owner（オーナー）— 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。

Sample No.（サンプル番号）— 表の情報が反映される特定のサンプルの数を示します。

Drop Events（イベントの破棄）— 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すことがあります。

Received Bytes (Octets)（受信されたバイト）（オクテット）— 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オクテット数です。

Received Packets（受信されたパケット）— サンプルが収集される間に受信されたパケットの数です。

Broadcast Packets（ブロードキャストパケット）— サンプルが収集される間に受信された優良なブロードキャストパケットの数です。

Multicast Packets（マルチキャストパケット）— サンプルが収集される間に受信された優良なマルチキャストパケットの数です。

CRC Align Errors（CRC 調整エラー）— サンプルセッション中に受信された 64～1518 オクテットの長さのパケットの数です。ただし、不良なフレームチェックシーケンス（FCS）を持ち、整数のオクテットまたは非整数の不良な FCS を持つパケットです。

Undersize Packets（アンダーサイズパケット）— サンプルセッション中に受信された 64 オクテット未満の長さのパケットの数です。

Oversize Packets（オーバーサイズパケット）— サンプルセッション中に受信された 1,518 オクテットを超える長さのパケットの数です。

Fragments（フラグメント）— サンプルセッション中に受信された 64 オクテット未満の長さで FCS のあるパケットの数です。

Jabbers（ジャバー）— サンプルセッション中に受信された 1,518 オクテットを超える長さで FCS のあるパケットの数です。

Collisions（衝突）— サンプルセッション中に起きたパケット衝突の全体数の概算です。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リピーターポートが検出した際に検出されます。

Utilization（利用率）— サンプルセッション中のインタフェースのメイン物理層ネットワークの使用を概算します。値は小数点以下 2 桁までのパーセントで反映されます。

特定のヒストリエントリの統計の表示

□□□ **RMON** ヒストリ表を開きます。

□□□ **History Entry No.**（ヒストリエントリの番号）フィールドでエントリを選択します。

エントリの統計が RMON ヒストリ表に表示されます。

CLI コマンドを使用した **RMON** ヒストリ制御の表示

次の表は、RMON ヒストリを表示する場合の CLI コマンドを示したものです。

表**8-7 RMON** ヒストリ制御に関連する **CLI** コマンド

CLI コマンド	説明
show rmon history index {throughput | errors | other} [period seconds]	RMON Ethernet 統計ヒストリを表示します。

以下に、インデックス 1のスループットの RMON Ethernet 統計を表示するための CLI コマンドの例を示します。

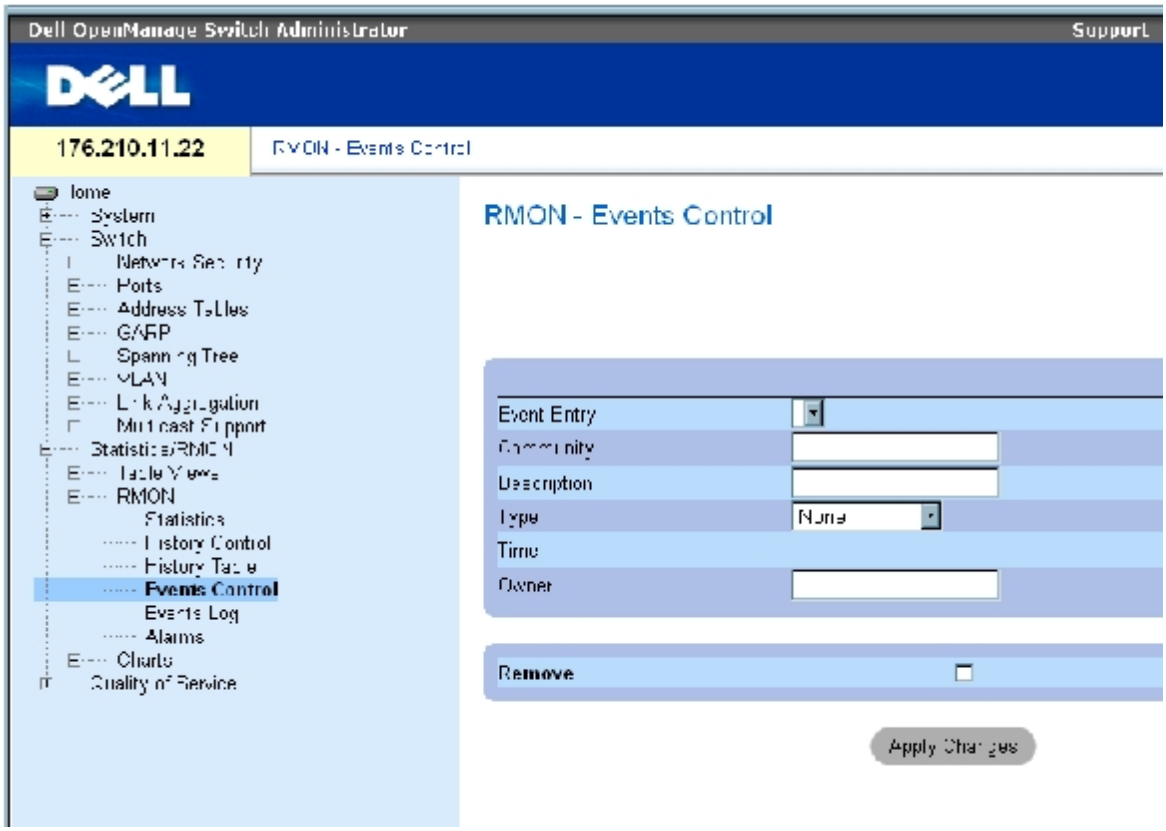
```
console> enable

console# show rmon history 1 throughput

Sample Set:5 Owner:cli

Interface:24 interval: 10

Requested samples:50 Granted samples: 50

Maximum table size: 270

Time Octets Packets Broadcast Multicast %

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

```
09-Mar-2003 18:29:32 0 0 0 0 0

09-Mar-2003 18:29:42 0 0 0 0 0

09-Mar-2003 18:29:52 0 0 0 0 0

09-Mar-2003 18:30:02 0 0 0 0 0

09-Mar-2003 18:30:12 0 0 0 0 0

09-Mar-2003 18:30:22 0 0 0 0 0
```

デバイス **RMON** イベントの定義

RMON イベント制御ページを使用して、RMON イベントを定義します。**RMON** イベント制御 ページを開くには、ツリービューで **Statistics / RMON**（統計 **/ RMON**）→ **RMON**→ **Events Control**（イベント制御）の順にクリックします。

図**8-10 RMON** イベント制御



RMON イベント制御 ページには、以下のフィールドがあります。

Event Entry（イベントエントリ）— イベントを示します。

Community（コミュニティ）— イベントが属するコミュニティです。

Description（説明）— ユーザー定義のイベントの説明です。

Type（タイプ）— イベントタイプの説明です。可能な値は以下のとおりです。

Log（ログ）— イベントタイプはログエントリです。

Trap（トラップ）— イベントタイプはトラップです。

Log and Trap（ログおよびトラップ）— イベントタイプはログエントリとトラップの両方です。

None（なし）— イベントはありません。

Time（時刻）— イベントが起きた時刻です。

Owner — イベントを定義したデバイスまたはユーザーです。

Remove（削除）— このオプションを選択すると、RMON イベント表からイベントが削除されます。

RMON イベントの追加

□□□ **RMON** イベント制御 ページを開きます。

□□□ **Add**（追加）をクリックします。

イベントエントリの追加ページが開きます。

□□□ ダイアログの情報を完成させて **Apply Changes**（変更の適用）をクリックします。

イベント表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 イベントの変更

□□□ **RMON** イベント制御 ページを開きます。

□□□ イベント表でエントリを選択します。

□□□ ダイアログのフィールドを変更して **Apply Changes**（変更の適用）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 イベントエントリの削除

□□□ **RMON** イベント制御 ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

RMON イベント制御ページが開きます。

□□□ 削除の必要があるイベントで **Remove**（削除）チェックボックスを選択してから、 **Apply Changes**（変更の適用）をクリックします。

選択した表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： **RMON** イベント制御ページで **Remove**（削除）チェックボックスを選択すると、その ページから単一のイベントエントリを削除できます。

CLI コマンドを使用したデバイスイベントの定義

次の表は、デバイスイベントを定義する場合の CLI コマンドを示したものです。

表**8-8** デバイスイベント定義の **CLI** コマンド

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 イベント表を表示します。

以下に、CLI コマンドの例を示します。

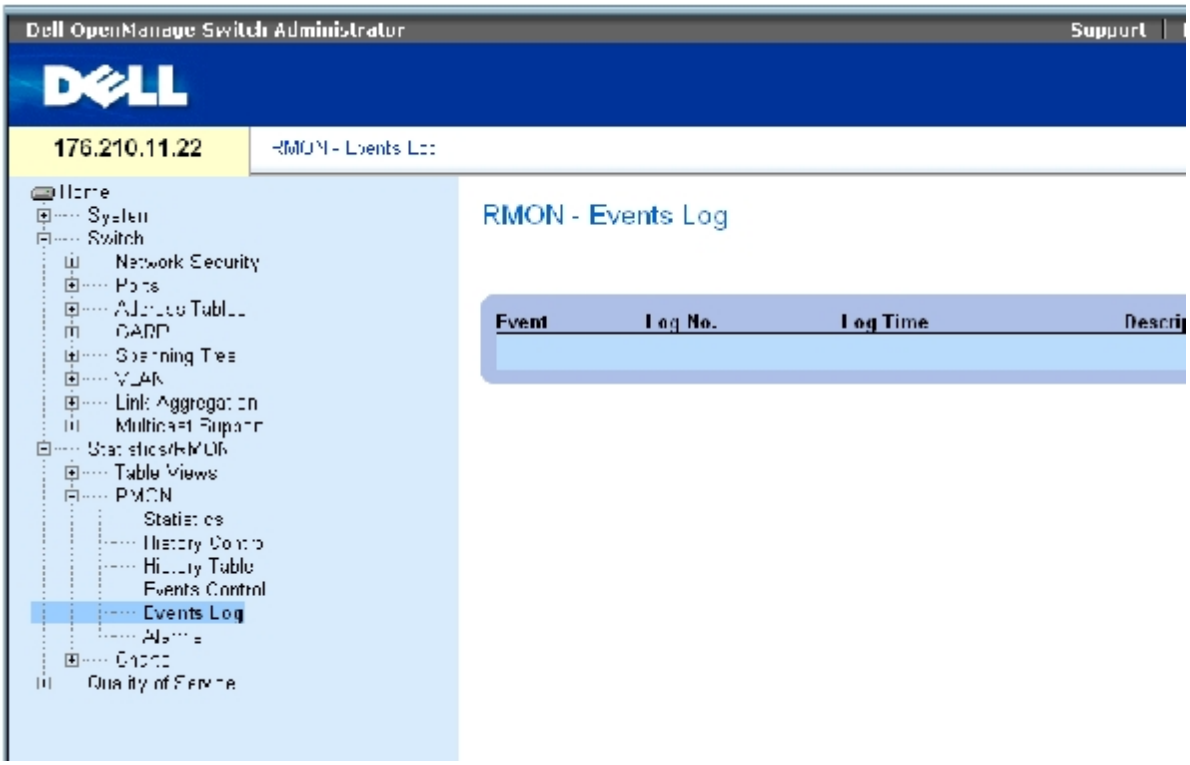
```
console(config)# rmon event 1 log
console(config)# exit
console# show rmon events
```

Index	Description	Type	Community	Owner	Last Time Sent
1	Errors	Log		CLI	Jan 18 2002 23:58:17
2	High Broadcast	Log-Trap	router	Manager	Jan 18 2002 23:59:48

RMON イベントログの表示

RMON イベントログページには、RMON イベントの一覧があります。**RMON** イベントログページを開くには、ツリービューで **Statistics/RMON**（統計 **/RMON**）→ **RMON**→ **Events Log**（イベントログ）の順にクリックします。

図**8-11 RMON** イベントログ



RMON イベントログ ページには、以下のフィールドがあります。

Event（イベント）— RMON イベントログエントリの番号です。

Log No.（ログ番号）— ログ番号です。

Log Time（ログタイム）— ログエントリが入力された時刻です。

Description（説明）— ログエントリの説明です。

CLI コマンドを使用したデバイスイベントの定義

次の表は、デバイスイベントを定義する場合の CLI コマンドを示したものです。

表**8-9** デバイスイベント定義の **CLI** コマンド

CLI コマンド	説明
show rmon log [*event*]	RMON ロギング表を表示します。

以下に、CLI コマンドの例を示します。

```
console(config)# rmon event 1 log

Console> show rmon log

Maximum table size: 500
```

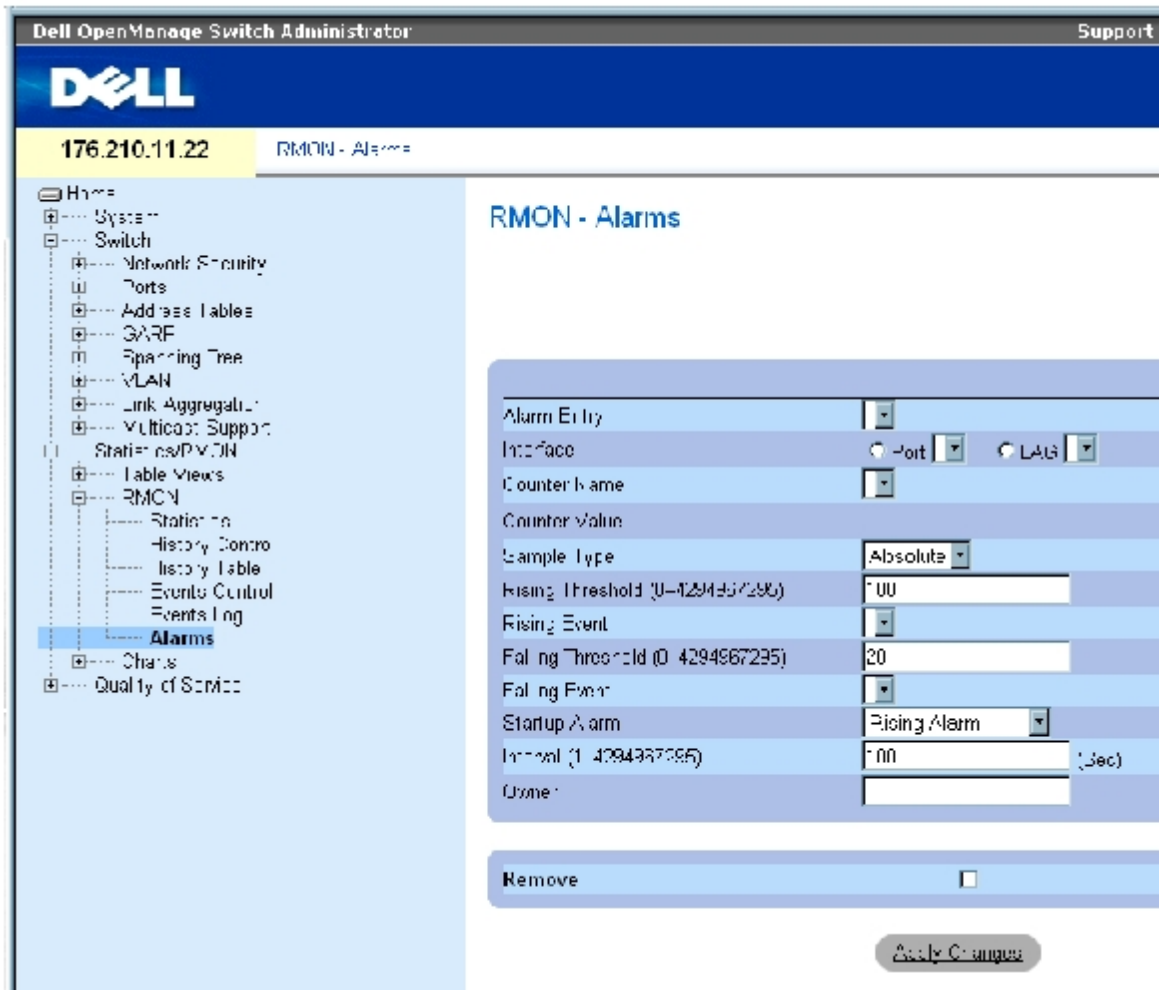
```
Event Description Time

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

1 Errors Jan 18 2002 23:58:17

2 High Broadcast Jan 18 2002 23:59:48
```

RMON デバイスアラームの定義

RMON アラームページを使用してネットワークアラームを設定します。ネットワークアラームは、ネットワークで問題またはイベントが検出されたときに起きます。しきい値を上げたり下げたりするとイベントが発生します。イベントの詳細については、「RMON イベントログの表示」を参照してください。

RMON アラームページを開くには、ツリービューで **Statistics / RMON**（統計 **/ RMON**）→ **RMON**→ **Alarms**（アラーム）の順にクリックします。

図**8-12 RMON** アラーム



RMON アラーム ページには、以下のフィールドがあります。

Alarm Entry（アラームエントリ）— 特定のアラームを示します。

Interface（インタフェース）— RMON 統計が表示されるインタフェースを示します。

Counter Name（カウンタ名）— 選択した MIB 変数を示します。

Counter Value（カウンタ値）— 選択した MIB 変数の値です。

Sample Type（サンプルタイプ）— 選択した変数のサンプルの収集方法を指定し、値をしきい値と比較します。可能なフィールド値は、以下のとおりです。

Delta（デルタ）— 現在の値から最後にサンプル収集された値を引きます。この値の差としきい値を比較します。

Absolute（絶対値）— サンプル収集の終りに値をしきい値と直接比較します。

Rising Threshold (0-4294967295)（上昇しきい値）（0～4294967295）— 上昇しきい値アラームを誘発する上昇カウンタ値です。上昇しきい値は、グラフバーの上に示されます。それぞれの監視される変数には指定された色があります。フィールドのデフォルト値は 100 秒です。

Rising Event（上昇イベント）— アラームが報告される機構です。ログ、トラップ、またはその両方の組み合わせがあります。ログを選択した場合、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ログ表に残ります。トラップを選択した場合、SNMP トラップが生成され、トラップの機構を介して報告されます。トラップは同じ機構を使用して保存できます。

Falling Threshold (0-4294967295)（下降しきい値）（0～4294967295）— 下降しきい値アラームを誘発する下降カウンタ値です。下降しきい値は、グラフバーの上にグラフで表示されます。それぞれの監視される変数には指定された色があります。フィールドのデフォルト値は 20 です。

Startup Alarm（スタートアップアラーム）— アラームの生成を有効にするトリガーです。上昇は、低しきい値から高しきい値までのしきい値を越えることで定義されています。

Interval (1-4294967295) **(sec)**（間隔）（1～4294967295）— アラームの間隔です。フィールドのデフォルト値は 100 秒です。

Owner（オーナー）— アラームを定義したデバイスまたはユーザーです。

Remove（削除）— このオプションを選択すると、RMON アラームが削除されます。

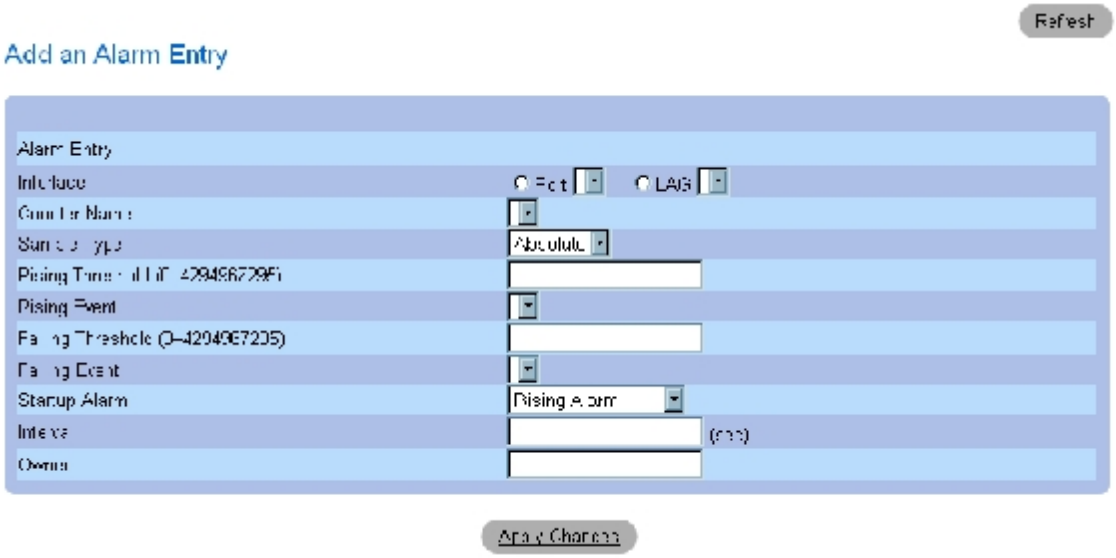
アラーム表エントリの追加

□□□ **RMON** アラーム ページを開きます。

□□□ **Add**（追加）をクリックします。

アラームエントリの追加ページが開きます。

図**8-13** アラームエントリの追加ページ



□□□ インタフェースを選択します。

□□□ フィールドを完了します。

□□□ **Apply Changes**（変更の適用）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。

アラーム表エントリの変更

□□□ **RMON** アラーム ページを開きます。

□□□ **Alarm Entry**（アラームエントリ）ドロップダウンメニューでエントリを選択します。

□□□ フィールドを変更します。

□□□ **Apply Changes**（変更の適用）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。

アラーム表の表示

□□□ **RMON** アラーム ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

アラーム表が開きます。

アラーム表エントリの削除

□□□ **RMON** アラーム ページを開きます。

□□□ **Alarm Entry**（アラームエントリ）ドロップダウンメニューでエントリを選択します。

□□□ **Remove**（削除）チェックボックスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

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

次の表は、デバイスアラームを定義する場合の CLI コマンドを示したものです。

表**8-10** デバイスアラームに関連する **CLI** コマンド

CLI コマンド	説明
rmon alarm *index MIB_Object_ID interval rthreshold fthreshold revent fevent* [**type** *type*] [**startup** *direction*] [**owner** *name*]	RMON アラーム条件を設定します。
show rmon alarm-table	アラーム表の要約を表示します。
show rmon alarm	RMON 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 1000
1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20

Console# show rmon alarm-table

Index OID Owner

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

1 1.3.6.1.2.1.2.2.1.10.1 CLI

2 1.3.6.1.2.1.2.2.1.10.1 Manager

3 1.3.6.1.2.1.2.2.1.10.9 CLI
```

チャートの表示

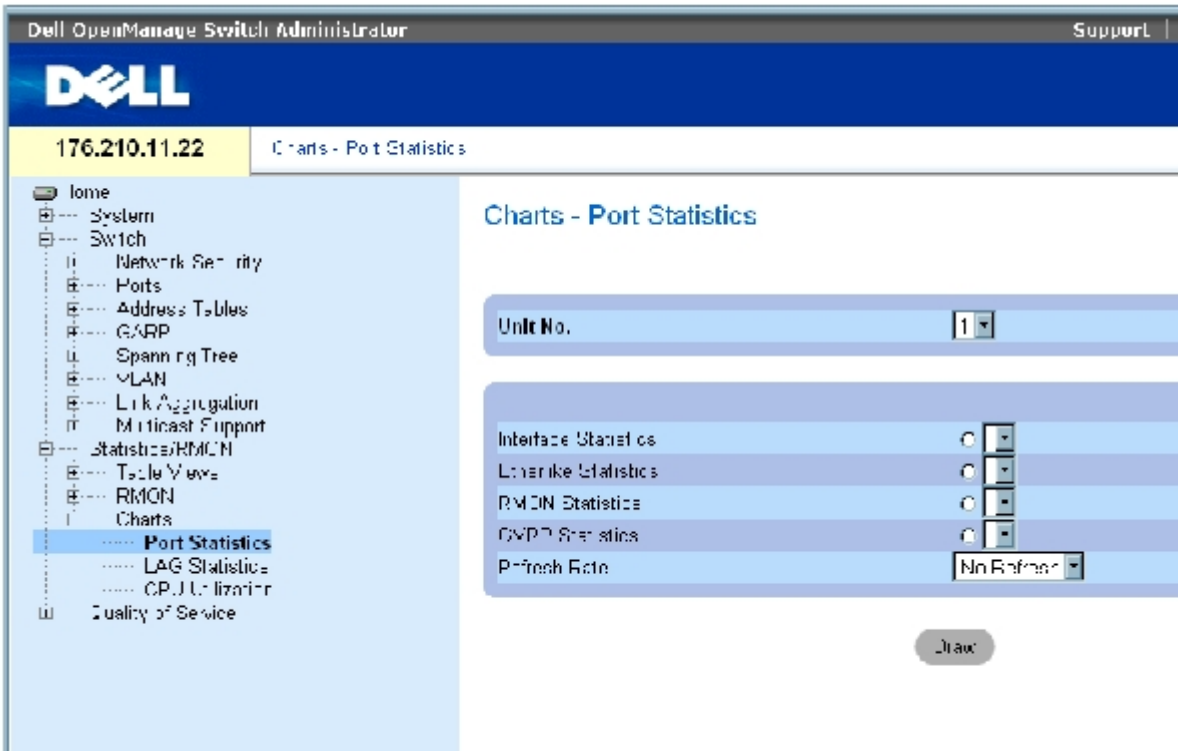
チャート ページには、統計をチャート形式で表示するためのリンクがあります。チャートページを開くには、ツリービューで **Statistics**（統計）→ **Charts**（表）の順にクリックします。

ポート統計の表示

ポート統計ページを使用して、ポート要素の統計をチャート形式で開きます。ポート統計ページを開くには、ツリービューで

Statistics/RMON（統計 /RMON）→ **Charts**（チャート）→ **Port Statistics**（ポート統計）の順にクリックします。

図**8-14** ポート統計



ポート統計ページには、以下のフィールドがあります。

Unit No.（ユニット番号）— 統計が表示されるスタッキングユニットを示します。

Interface Statistics（インタフェース統計）— 表示するインタフェース統計を選択します。

Etherlike Statistics（Etherlike 統計）— 表示する Etherlike 統計を選択します。

RMON Statistics（RMON 統計）— 表示する RMON 統計を選択します。

GVRP Statistics（GVRP 統計）— 表示する GVRP 統計のタイプを選択します。

Refresh Rate（リフレッシュレート）— 統計がリフレッシュされるまでに経過する時間です。

ポート統計の表示

□□□ ポート統計 ページを開きます。

□□□ 開く統計のタイプを選択します。

□□□ **Refresh Rate**（リフレッシュレート）ドロップダウンメニューから希望のリフレッシュ レートを選択します。

□□□ **Draw**（描画）をクリックします。

選択した統計のグラフが表示されます。

CLI コマンドを使用したポート統計の表示

次の表は、ポート統計を表示する場合の CLI コマンドを示したものです。

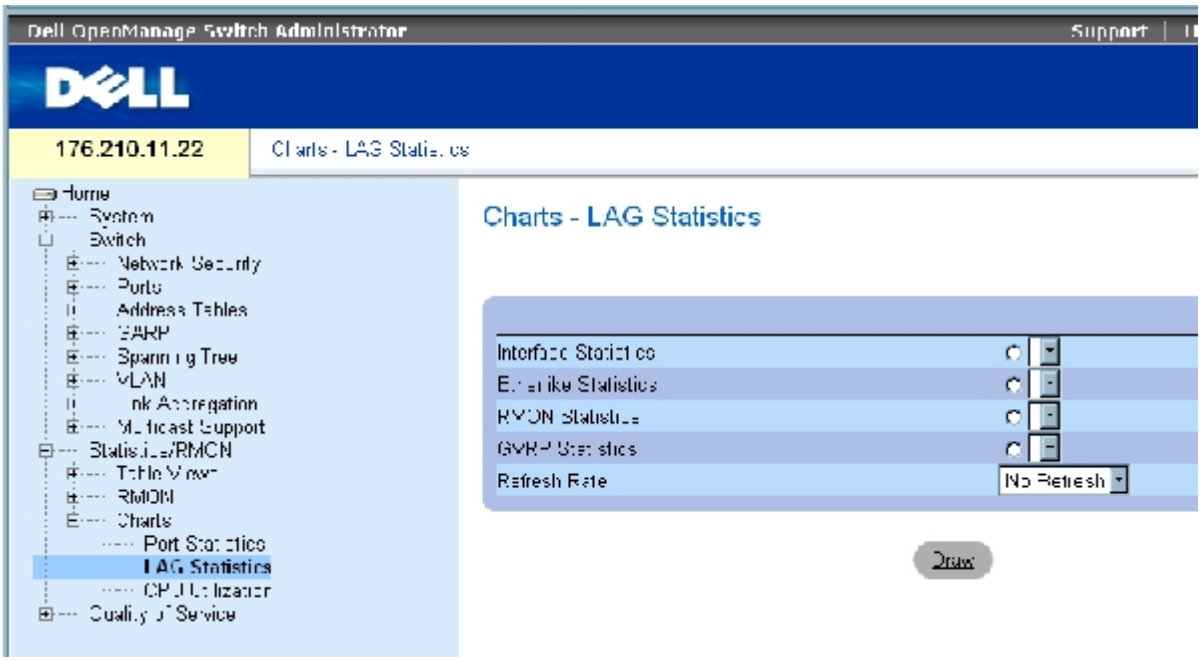
表**8-11** ポート統計に関連する **CLI** コマンド

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。
show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	RMON Ethernet 統計を表示します。
show gvrp statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	GVRP の統計を表示します。
show gvrp-error statistics {**ethernet** *interface* | **port- channel** *port-channel-number*}	GVRP エラー の統計を表示します。

LAG 統計の表示

LAG 統計ページを使用して、LAG の統計をチャート形式で開きます。LAG 統計ページを開くには、ツリービューで **Statistics / RMON**（統計 /RMON）→ **Charts**（チャート）→ **LAG Statistics**（LAG 統計）の順にクリックします。

図**8-15 LAG** 統計



LAG 統計ページには、以下のフィールドがあります。

Interface Statistics（インタフェース統計）— 表示するインタフェース統計を選択します。

Etherlike Statistics（Etherlike 統計）— 表示する Etherlike 統計を選択します。

RMON Statistics（RMON 統計）— 表示する RMON 統計を選択します。

GVRP Statistics（GVRP 統計）— 表示する GVRP 統計のタイプを選択します。

Refresh Rate（リフレッシュレート）— 統計がリフレッシュされるまでに経過する時間です。

LAG 統計の表示

□□□ **LAG** 統計ページを開きます。

□□□ 開く統計のタイプを選択します。

□□□ **Refresh Rate**（リフレッシュレート）ドロップダウンメニューから希望のリフレッシュ レートを選択します。

□□□ **Draw**（描画）をクリックします。

選択した統計のグラフが表示されます。

CLI コマンドを使用した LAG 統計の表示

次の表は、LAG 統計を表示する場合の CLI コマンドを示したものです。

表**8-12 LAG** の統計に関連する **CLI** コマンド

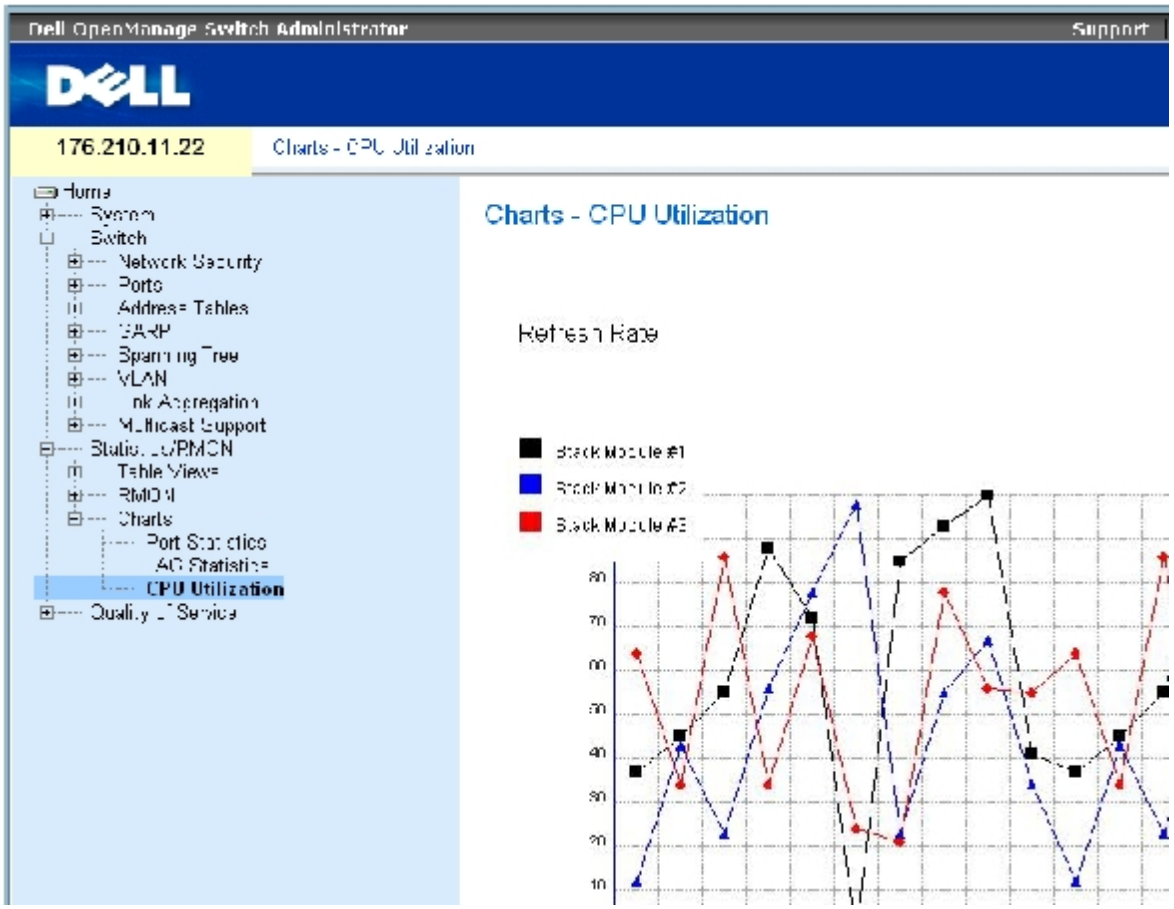
CLI コマンド	説明
show interfaces counters [ethernet *interface* **| port- channel** *port-channel-number*]	物理的なインタフェースで検出されたトラフィックを表示します。
show rmon statistics {ethernet *interface* **| port-channel** *port-channel-number*}	RMON Ethernet 統計を表示します。
show gvrp statistics {ethernet *interface* **| port-channel** *port-channel-number*}	GVRP の統計を表示します。
show gvrp-error statistics {ethernet *interface* **| port- channel** *port-channel-number*}	GVRP エラー の統計を表示します。

CPU 利用率の表示

CPU の利用率ページには、システムの CPU 利用率および各スタッキングメンバーによって使用されている CPU リソースのパーセンテージに関する情報があります。各スタッキングメンバーには、グラフの色が割り当てられます。

CPU の利用率ページを開くには、ツリービューで **Statistics/RMON**（統計 /RMON）→ **Charts**（チャート）→ **CPU Utilization**（CPU の利用率）の順にクリックします。

図**8-16 CPU** の利用率



CPU の利用率ページには、以下の情報があります。

Refresh Rate（リフレッシュレート）— 統計がリフレッシュされるまでに経過する時間です。

メモ、注意および警告

メモ、注意および警告

サービス品質の設定

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

本項では、サービス品質（QoS）パラメーターの定義および設定について説明します。サービス品質ページを開くには、ツリービューで Quality of Service（サービス品質）をクリックします。

サービス品質（QoS）の概要

サービス品質（QoS: Quality of Service）は、ネットワーク内に QoS と優先度キューを導入する機能を提供します。

QoS を必要とする導入例として、音声、ビデオ、およびリアルタイムトラフィックなど、高い優先度キューが割り当てられ、それ以外のトラフィックには低い先度キューが割り当てられる、特定のタイプのトラフィックがあります。結果として、需要の高いトラフィックのフローが改善されます。

QoS は、次の項目によって定義されます。

- Classification（分類）— どのパケットフィールドを特定の値と一致させるかを指定します。ユーザー定義の仕様に一致するすべてのパケットは同類として分類されます。
- Action（処置）— パケット情報や VLAN 優先度タグ（VPT）および DSCP（DiffServ Code Point）などのパケットフィールド値に基づいて転送されるパケットのトラフィック管理を定義します。

VPT の分類情報

VLAN 優先度タグを使用して、出力キューのいずれかにパケットをマッピングすることで、パケットを分類します。キューの割り当てに対する VLAN 優先度タグは、ユーザー定義が可能です。次の表は、キューに対する VPTのデフォルト設定を示します。

表**9-1 CoS** からキューへのマッピング表のデフォルト値

CoS 値	転送キューの値
0	q1（最低優先度）
1	q1（最低優先度）
2	q1（最低優先度）
3	q1（最低優先度）
4	q2
5	q2
6	q3
7	q3

メモ： スタッキング構成では、キュー 4 はスタッキングトラフィックの転送に使用され ます。そのため、キュー 4 にトラ

フィックを追加すると、トラフィックの転送が干渉を 受ける可能性があります。

タグなしで到着するパケットには、ポートごとに設定されるデフォルトの VPT 値が割り当てられます。割り当てられた VPT は、パケットを出力キューにマッピングするために使用されます。

DSCP 値は優先度キューにマッピングできます。次の表は、出力キューの値にマッピングするデフォルトの DSCP を示したものです。

表**9-2 DSCP** からキューへのマッピング表のデフォルト値

DSCP 値	転送キューの値
0-15	q1（最低優先度）
16-39	q2
40-63	q3

DSCP マッピングは、システムごとに有効になります。

CoS サービス

特定の出力キューにパケットを割り当てた後で、キューに CoS サービスを割り当てることができます。出力キューには、以下のいずれかの方法でスケジュール方式を設定します。

- Strict Priority（厳密優先度）— 時間的な影響を受けるアプリケーションが、常に迅速なパスで転送されるようにします。厳密優先度（SP）を使用すると、時間的にあまり影響を受けないアプリケーションよりも、ミッションクリティカルで時間的な影響を受けるトラフィックを優先させることができます。
  たとえば、厳密優先度を設定すると、IP トラフィック上の音声が優先され、FTP トラフィックや電子メール（SMTP）トラフィックよりも先に転送されます。

- Weighted Round Robin（加重ラウンドロビン）— 単一のアプリケーションによってデバイスの転送機能が独占されないようにします。加重ラウンドロビン（WRR）を設定すると、ラウンドロビンの順にキュー全体が転送されます。SP キューを除き、すべてのキューが WRR に参加できます。
  SP キューは WRR キューよりも前に処理されます。トラフィックのフローが非常に少なく、SP キューがポートに割り当てられた帯域幅全体を占めない場合、WRR キューは SP キューと帯域幅を共有できます。残りの帯域幅が加重率に従って配分されるようにします。WRR を選択している場合は、1、2、4、8 のウエートがキューに割り当てられます。

QoS グローバルパラメータの定義

QoS パラメータページには、QoS グローバルパラメータの設定を可能にするページへのリンクがあります。

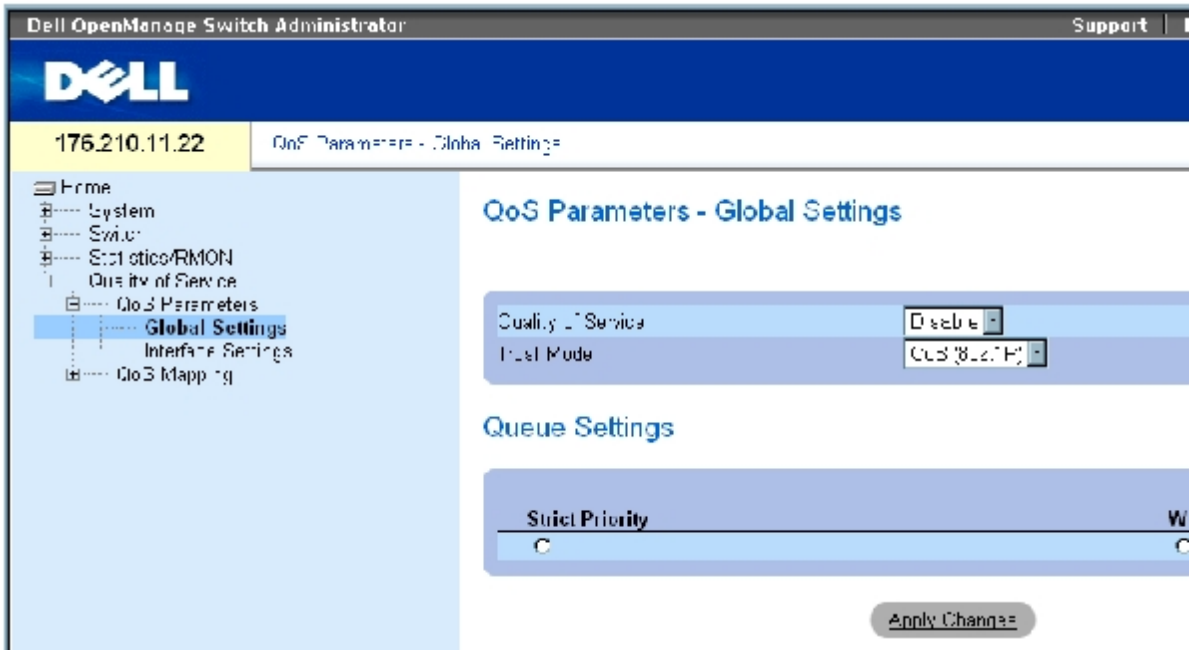
QoS のグローバル設定

グローバル設定ページには、QoS を有効または無効にするフィールドがあります。Trust（信頼）モードを選択するフィールドもあります。Trus（信頼）モードは、パケット内の定義済みフィールドに基づいて出力キューを判断します。

また、グローバル設定 ページにより、キューを厳密優先度（SP）または加重ラウンドロビン（WRR）のどちらかに定義することができます。

グローバル設定ページを開くには、ツリービューで Quality of Service（サービス品質）→ QoS Parameters （QoS パラメータ）→ Global Settings（グローバル設定）の順にクリックします。

図 **9-1** グローバル設定



グローバル設定 ページには、以下の項があります。

- QoS の設定
- キューの設定

QoS の設定

Quality of Service（サービス品質）— Quality of Service（サービス品質）を使用してネットワークトラフィックの管理を有効または無効にします。

Trust Mode（信頼モード）— デバイスに入るパケットの分類にどのパケットフィールドが使用されるかを決定します。いかなるルールも定義されていない場合、定義済みの Cos または DSCP パケットフィールドを含むトラフィックは、選択した信頼モードに従ってマッピングされます。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キュー（q2）にマッピングされます。Trust Mode（信頼モード）のフィールド値は以下のとおりです。

CoS (802.1p)— 割り当てられる出力キューは、IEEE802.1p VLAN 優先度タグ（VPT）またはポートに割り当てられたデフォルト VPT によって決まります。デバイスのデフォルトは IEEE802.1p です。

DSCP— DSCP フィールドによって出力キュー割り当てが決定されます。

メモ： インタフェースの Trust（信頼）設定は、グローバル Trust（信頼）設定よりも優先さ れます。

キューの設定

Strict Priority（厳密優先度）— この項目が選択されていると、システムキューが SP キューであることを示します。

WRR— この項目が選択されていると、システムキューが WRR キューであることが示されます。

サービス品質の有効化

□□□ グローバル設定ページを開きます。

□□□ **Quality of Service**（サービス品質）フィールドで**Enable**（有効）を選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

デバイスに対して Class of Service（クラスオブサービス）が有効になります。

Trust（信頼）モードの有効化

□□□ グローバル設定ページを開きます。

□□□ **Trust Mode**（信頼モード）フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

デバイスに対して Trust（信頼）モードが有効になります。

CLI コマンドを使用した Trust（信頼）の有効化

次の表は、 グローバル設定ページのフィールドを設定するための等価な CLI コマンドをまとめたものです。

表**9-3 QoS** の設定に関連する **CLI** コマンド

CLI コマンド	説明
qos trust [**cos** | **dscp**]	システムを信頼モードに設定します。
no qos trust	非信頼状態に戻します。

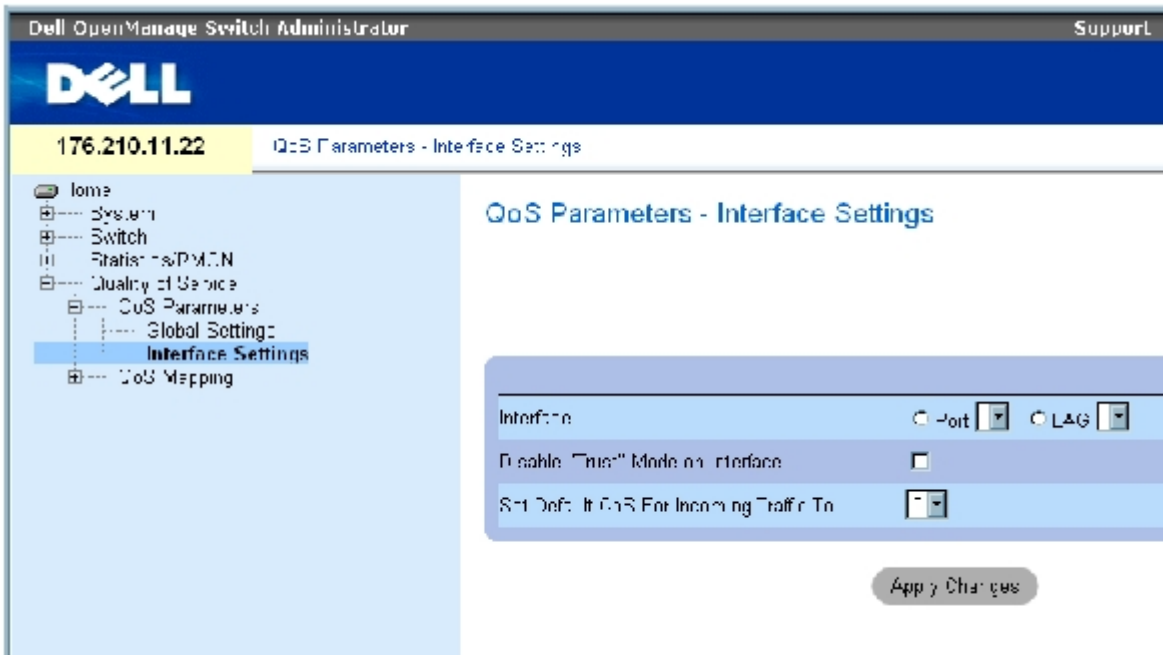
以下に、CLI コマンドの例を示します。

```
console(config)# qos trust
dscp
```

QoS インタフェース設定の定義

インタフェース設定ページには、Trust（信頼）モードを解除し、タグなしの受信パケットに対するデフォルト CoS 値を設定するフィールドがあります。インタフェース設定ページを開くには、ツリービューで Quality of Service（サービス品質）→ QoS Parameters （QoS パラメータ）→ Interface Settings（インタフェース設定）の順にクリックします。

図**9-2** インタフェース設定



インタフェース設定 ページには、以下のフィールドがあります。

Interface（インタフェース）— 設定を行う特定のポートまたは **LAG** です。

Disable "Trust" Mode on Interface（インタフェースの信頼モードの無効化）— 指定したインタフェースの **Trust**（信頼）モードを無効にします。この設定は、デバイス全体に設定された **Trust**（信頼）モードをオーバーライドします。

Set Default CoS For Incoming Traffic To（受信トラフィックに対するデフォルト **CoS** の設定）— タグなしパケットにデフォルトの **CoS** タグ値を設定します。**CoS** タグ値の範囲は、**0**～**7** です。 デフォルト値は **0** です。

インタフェースへの **QoS** 設定の割り当て

□□□ インタフェース設定ページを開きます。

□□□ **Interface**（インタフェース）フィールドでインタフェースを選択します。

□□□ フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

CoS 設定がインタフェースに割り当てられます。

QoS/CoS 設定の表示

□□□ インタフェース設定ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

インタフェース表が表示されます。

CLI コマンドを使用した **QoS** インタフェースの割り当て

次の表は、インタフェース設定ページのフィールドを設定するための等価な CLI コマンドをまとめたものです。

表**9-4 QoS** インタフェースに関連する **CLI** コマンド

CLI コマンド	説明
qos trust	信頼モードを有効にします。
no qos trust	各ポートに対して Trust（信頼）状態を無効にします。

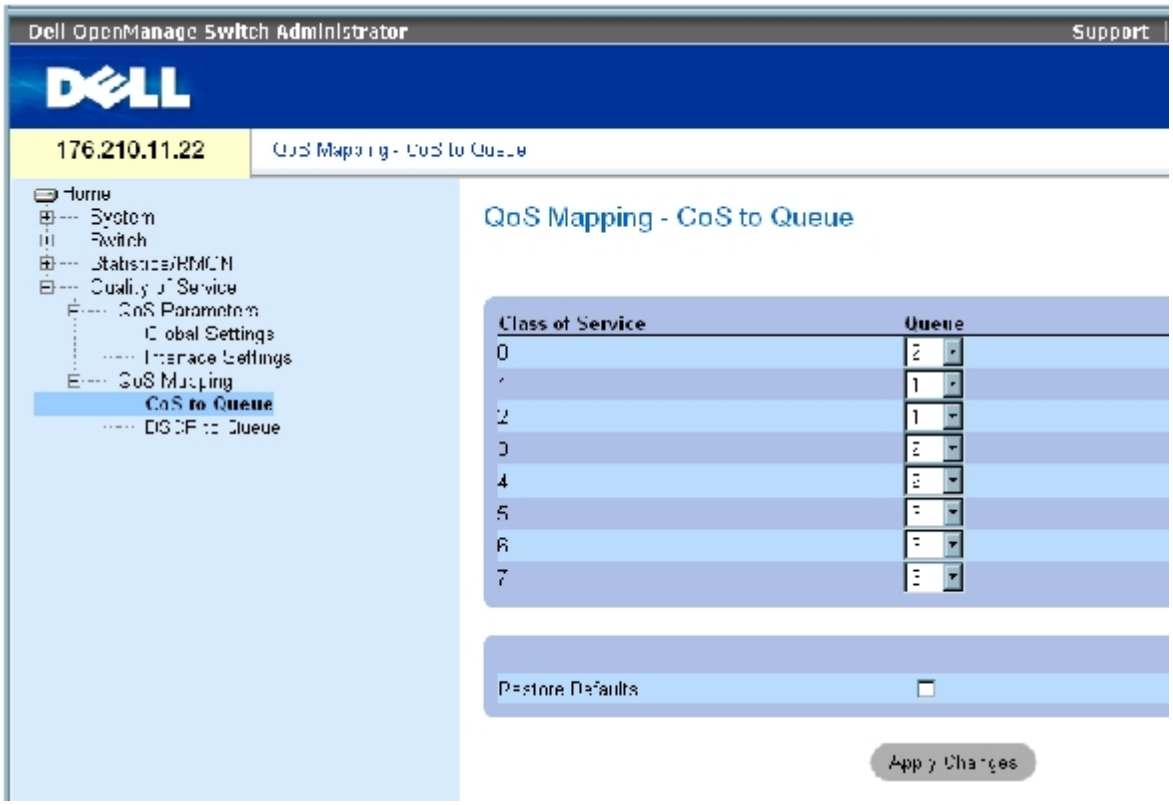
以下に、CLI コマンドの例を示します。

```
console(config)# interface
ethernet 1/e15


console(config-if)# qos
trust
```

CoS 値のキューへのマッピング

キューへの **CoS**ページには、CoS 設定をトラフィックキューに割り当てるためのフィールドがあります。キューへの **CoS**ページを開くには、ツリービューで Quality of Service（サービス品質）→**QoS Mapping**（QoS マッピング）→ CoS to Queue（キューへの QoS）の順にクリックします。

図**9-3** キューへの **CoS**



キューへの **CoS**ページには、以下のフィールドがあります。

Class of Service（クラスオブサービス）— 0 を最低、7 を最高とする、CoS 優先度タグ値を指定します。

Queue（キュー）— CoS 優先度をマッピングするキューです。4 つのトラフィック優先度キューがサポートされています。

Restore Defaults（デフォルトの復元）— CoS 値を出力キューにマッピングするためにデバイスの工場出荷時のデフォルトを復元します。

CoS 値のキューへのマッピング

□□□ キューへの **CoS**ページを開きます。

□□□ CoS エントリを選択します。

□□□ **Queue**（キュー）フィールドでキュー番号を定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

CoS 値が出力キューにマッピングされ、デバイスが更新されます。

CLI コマンドを使用した CoS 値のキューへの割り当て

次の表は、キューへの **CoS**ページのフィールドを設定するための等価な CLI コマンドをまとめたものです。

表**9-5** キューへの **CoS** 設定に関連する **CLI** コマンド

CLI コマンド	説明
wrr-queue cos-map queue-id cos0.cos7	割り当てられた CoS 値を出力キューにマッピングします。

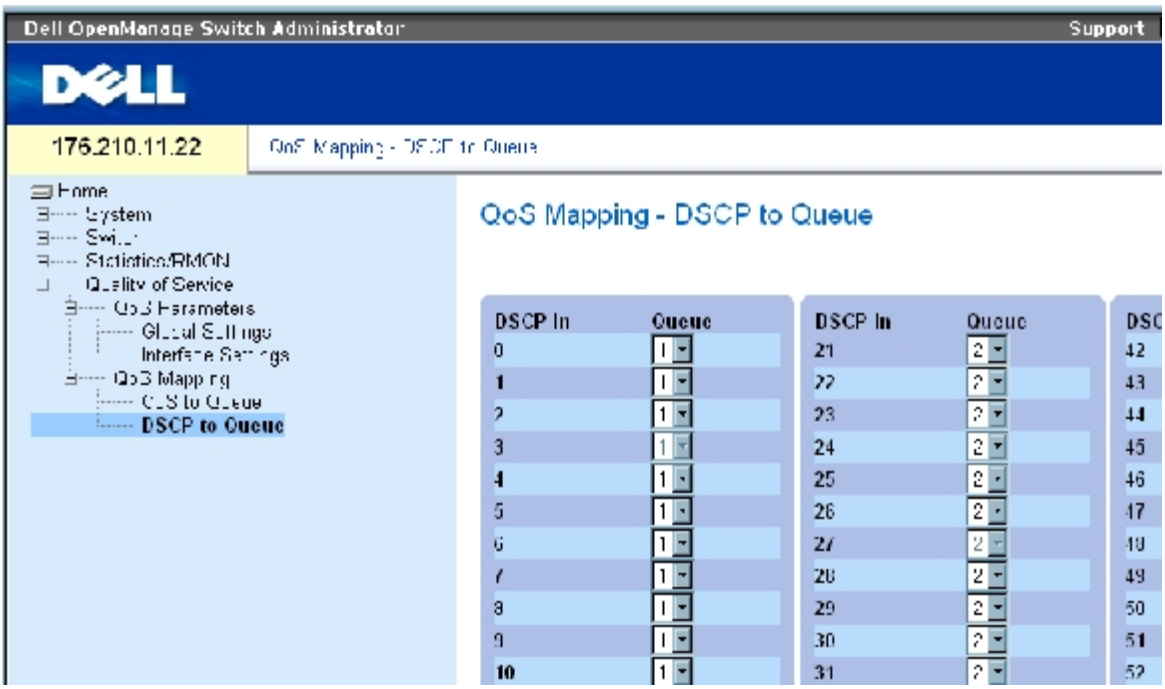
以下に、CLI コマンドの例を示します。

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

DSCP 値のキューへのマッピング

キューへの **DSCP**ページには、特定の DSCP フィールドに対する出力キューを定義するためのフィールドがあります。キューへの **DSCP**ページを開くには、ツリービューで Quality of Service（サービス品質）→**QoS** Mapping（QoS マッピング）→ DSCP to Queue（キューへの DSCP）の順にクリックします。

図**9-4** キューへの **DSCP**



キューへの **DSCP**ページには、以下のフィールドがあります。

DSCP In（DSCP 受信）— 受信パケット内の **DSCP** フィールドの値です。

Queue（キュー）— 特定の **DSCP** 値を持つパケットを割り当てるキューです。値は **1**～**4** で、最小値が **1**、最大値が **4** です。

DSCP 値のマッピングと優先度キューの割り当て

□□□ キューへの **DSCP**ページを開きます。

□□□ **DSCP In**（DSCP 受信）列の値を選択します。

□□□ **Queue**（キュー）フィールドを定義します。

□□□ **Apply Changes**（変更の適用）をクリックします。

DSCP が上書きされ、値が出力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

次の表は、キューへの **DSCP**ページのフィールドを設定するための等価な **CLI** コマンドをまとめたものです。

表**9-6** キューへの **DSCP** 値に関連する **CLI** コマンド

CLI コマンド	説明
qos map dscp-queue dscp-list **to** queue-id	キューへの DSCP のマッピングを変更します。

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
```

メモ、注意および警告

メモ、注意および警告

デバイスの機能競合について

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

以下の表に、機能競合に関する情報を示します。

機能	機能に関する注意点
802.1x 非認証 VLAN	以下の VLAN との間で機能に制限があります。 • 802.1X ゲスト VLAN • プライベート VLAN • 隔離 VLAN • コミュニティー VLAN • 特殊な VLAN
802.1x 非認証 VLAN ポート	以下との間で機能に制限があります。 • 独立ポート • コミュニティーポート • 無差別ポート • MAC ベースの VLAN ポート • イングレスフィルタリング
ACL	以下との間で機能に制限があります。 • MAC ベースの ACL • 特殊な VLAN
自動ネゴシエーション	機能競合による制限はありません。
バックプレッシャーサポート	
ブリッジマルチキャストフィルタリング	機能競合による制限はありません。
ケーブルテスト	機能競合による制限はありません。
コミュニティーポート	ロックポート（Locked Port）との間で機能に制限があります。
コミュニティー VLAN	以下との間で機能に制限があります。 • 静的 MAC アドレス • ACL • GVRP • IGMP スヌーピング • 特殊な VLAN
DNS	制限はありません。
デュプレックスモード	
フロー制御	機能競合による制限はありません。
GARP	機能競合による制限はありません。
ゲスト VLAN	以下の VLAN と一緒に使用できません。 • VLAN

	プライベート • 隔離 VLAN • コミュニティー VLAN • MAC ベースの VLAN • 特殊な VLAN
GVRP	機能競合による制限はありません。
IGMP スヌーピング	機能競合による制限はありません。
イングレスフィルタリング	機能競合による制限はありません。
独立ポート	以下と一緒に使用できません。 • コミュニティーポート • 無差別ポート • ポートロック • GVRP • MAC ベースの ACL • イングレスフィルタリング
隔離 VLAN	以下と一緒に使用できません。 • コミュニティー VLAN • 静的 MAC アドレス • ACL • GVRP • IGMP スヌーピング • 特殊な VLAN
LAG 統計	機能競合による制限はありません。
リンク集約	機能競合による制限はありません。ただし、この機能にはリンク集約を設定するためのガイドラインがいくつかあります。機能ガイドラインのすべてについては、「LAG パラメータの定義」を参照してください。
ロックポート	以下との間で機能に制限があります。 • MAC ベースの ACL • イングレスフィルタリング
ロギング	機能競合による制限はありません。
MAC アドレスサポート	機能競合による制限はありません。
MDI/MDIX 検出	機能競合による制限はありません。
マルチキャストフィルタリング	機能競合による制限はありません。
マルチホスト	802.1X 標準規格（マルチホスト）は、以下のポートと一緒に使用できません。 • 独立ポート • MAC ベースの VLAN ポート
多重スパニングツリー	以下と一緒に使用できません。 • 独立ポート • イングレスフィルタリング
ポートベースの認証	以下との間で機能に制限があります。 • 802.1 シングル • 独立ポート • ロックポート

	• MAC ベースの VLAN • イングレスポート
ポートミラーリング	機能競合による制限はありません。ただし、この機能にはストーム制御を設定するためのガイドラインがいくつかあります。機能ガイドラインのすべてについては、「ポートミラーリングセッションの定義」を参照してください。
ポート統計	機能競合による制限はありません。
プライベート VLAN	以下と一緒に使用できません。 • 独立ポート • コミュニティーポート • GVRP • IGMP スヌーピング • 特殊な VLAN
プライベート VLAN	以下との間で機能に制限があります。 • 隔離 VLAN • GVRP • IGMP スヌーピング • 特殊な VLAN
無差別ポート	以下と一緒に使用できません。 • ロックポート • GVRP • MAC ベースの VLAN ポート
クオリティオブサービス	機能競合による制限はありません。
RMON 統計	機能競合による制限はありません。
SNMP 認証通知	機能競合による制限はありません。
SNMP 通知	機能競合による制限はありません。
SNTP 認証	機能競合による制限はありません。
スパニングツリー	機能競合による制限はありません。
特殊な VLAN	機能競合による制限はありません。
静的 MAC	機能競合による制限はありません。
ストーム制御	機能競合による制限はありません。
システムログ	機能競合による制限はありません。
システム時刻の同期化	機能競合による制限はありません。
非認証 VLAN ポート	以下との間で機能に制限があります。 • 独立ポート • コミュニティーポート • 無差別ポート • GVRP • MAC ベースの VLAN ポート • イングレスフィルタリング

メモ、注意および警告

メモ、注意および警告

用語集

Dell™ PowerConnect™ 34XX システム ユーザーズガイド

この用語集に関連する技術用語をまとめています。

A | B | C | D | E | F | G | H | I | J | L | M | N | O | P | Q | R | S | T | U | V | W

A

Access Mode（アクセスモード）

システムへのユーザーアクセスを許可する方法を指定します。

Access Profiles（アクセスプロファイル）

ネットワーク管理者はこれを使用して、スイッチモジュールへのアクセスに関するプロファイルと規則を定義することができます。管理機能に対するアクセスをユーザーグループに限定できます。ユーザーグループは以下の基準によって定義されます。

- 入口インタフェース
- ソース IP アドレスまたはソース IP サブネット

Aggregated VLAN（集約 VLAN）

複数の VLAN を 1 つの集約 VLAN にまとめます。VLAN を集約することで、同じスーパー VLAN に属する別々のサブ VLAN にあるノードに送られる ARP 要求にルーターが応答できるようになります。ルーターは MAC アドレスを使用して応答します。

ARP

Address Resolution Protocol の略。IP アドレスを物理アドレスに変換するプロトコルです。

ASIC

Application Specific Integrated Circuit の略。特定用途向けに設計されたカスタムチップです。

Asset Tag（資産タグ）

ユーザー定義のスイッチモジュールリファレンスを指定します。

Authentication Profiles（認証プロファイル）

ユーザーおよびアプリケーションの認証とログインを有効にする一連の規則です。

Auto-negotiation（オートネゴシエイション）

10 / 100 Mbpsまたは 10 / 100 / 1000 Mbps Ethernet ポートを次の機能向けに確立できます。

- 全二重または半二重モード
- フロー制御
- スピード

B

Back Pressure（バックプレッシャー）

ポートにメッセージを受信させないようにする、半二重モードのメカニズムです。

Backplane（バックプレーン）

スイッチモジュール内で情報を伝えるメインバスです。

Backup Configuration Files（バックアップ設定ファイル）

スイッチモジュール設定のバックアップコピーが保存されます。実行設定ファイルまたはスタートアップ設定ファイルをバックアップファイルにコピーすると、バックアップファイルは変更されます。

Bandwidth（帯域幅）

一定の時間内に転送できるデータ量を指定します。デジタルスイッチモジュールの場合、帯域幅は 1 秒あたりのビット数（bps）または 1 秒あたりのバイト数で定義されます。

Bandwidth Assignments（帯域幅の割り当て）

特定のアプリケーション、ユーザー、またはインタフェースに割り当てられる帯域幅の量です。

Baud（ボー）

1秒間に送信される信号要素の数です。

Best Effort（ベストエフォート）

トラフィックが優先度の最も低いキューに割り当てられ、パケットの受け渡しは保証されません。

Boot Version（ブートバージョン）

起動イメージのバージョンです。

BootP

Bootstrap Protocol の略。ワークステーションで、その IP アドレス、ネットワーク上の BootP サーバーの IP アドレス、またはスイッチモジュールの起動イメージにロードされている設定ファイルを検出することが可能になります。

BPDU

Bridge Protocol Data Unit の略。ブリッジ情報をメッセージ形式で提供します。BPDU は、スパニングツリー設定においてスイッチモジュール情報の全体にわたって送信されます。BPDU パケットには、ポート、アドレス、優先度、および転送の各コストに関する情報が含まれます。

Bridge（ブリッジ）

2 つのネットワークを接続するデバイスです。ブリッジはハードウェアごとに異なりますが、プロトコルには依存しません。また、レイヤー 1 およびレイヤー 2 のレベルで動作します。

Broadcast Domain（ブロードキャストドメイン）

指定されたセットのどのデバイスからのブロードキャストフレームも受信するデバイスセットです。ルーターはブロードキャストフレームを転送しないため、ブロードキャストドメインをバインドします。

Broadcasting（ブロードキャスト）

ネットワーク上のすべてのポートにパケットを送信する方法です。

Broadcast Storm（ブロードキャストストーム）

過剰な量のブロードキャストメッセージが、単一のポートからネットワークに同時に送信された状態です。送信されたメッセージの応答がネットワークに蓄積され、ネットワークリソースのオーバーロードやネットワークのタイムアウトの原因となります。

ブロードキャストストームの詳細については、"LAG パラメータの定義" を参照してください。

C

CDB

Configuration Data Base の略。デバイスの設定情報が記録されているファイルです。

Class of Service（クラスオブサービス）

クラスオブサービス（CoS）。CoS は 802.1p 優先度付け方式で、パケットに優先度情報のタグを付けます。CoS 値 0～7 は、パケットのレイヤー 2 のヘッダーに追加されます。0 は優先度が最も低く、7 は優先度が最も高くなります。

複数のパケットの送信が重なり、衝突が発生している状態です。送信されたデータは使用できず、セッションは再スタートされます。

CLI

Command Line Interface の略。システムの設定に使用する行コマンドの集合。CLI の使用法の詳細については、「Using the CLI（CLI の使い方）」を参照してください。

Communities（コミュニティ）

同一のシステムアクセス権を保持するユーザーグループを指定します。

CPU

Central Processing Unit の略。コンピュータの中で情報を処理する部分。CPU は制御装置と ALU で構成されています。

D

DHCP Client（DHCP クライアント）

DHCP を使用してネットワークアドレスなどの設定パラメータを取得するデバイスです。

DSCP

DiffServe Code Point の略。DSCP は、IP パケットに QoS 優先度情報のタグを付ける方法です。

Domain（ドメイン）

ネットワークにおいて共通の規則と手順で管理されるコンピュータとデバイスのグループです。

DRAC/MC

デルのモジュラーサーバーシステムのコンポーネントに単一の管理点（ポイントオブコントロール）を提供します。

Duplex Mode（二重モード）

データの同時送受信を許可します。二重モードには、次の 2 つのタイプがあります。

- 全二重モードー 電話などの双方向同期通信を許可します。両側から同時に情報を送信できます。
- 半二重モードー トランシーバなどの非同期通信を許可します。一度に片方からのみ情報を送信できます。

E

Egress Ports（出口ポート）

ネットワークトラフィックを送信するポートです。

End System（エンドシステム）

ネットワーク上のエンドユーザーデバイスです。

Ethernet（イーサネット）

Ethernet は、IEEE 802.3 によって標準化されています。最も広く使われている LAN の標準です。データ転送レート Mbps をサポートし、10、100、または 1000 Mbps に対応します。

EWS

Embedded Web Server の略。標準の Web ブラウザを介してデバイス管理を行います。EWS は、CLI または NMS に加えて、またはそれらの代わりに使用されます。

F

FFT

Fast Forward Table の略。送信ルートの情報を示します。デバイスに到達したパケットのルートが登録されている場合、そのパケットは FFT にあるルートで送信されます。ルートが登録されていない場合、CPU はパケットを送信して、FFT をアップデートします。

FIFO

First In First Out の略。キューの最初のパケットが、最初に送信されるキューイングプロセスです。

Flapping（フラッピング）

インタフェースの状態が常に変化している場合はフラッピングが発生します。たとえば、STP ポートは、リスニング状態からラーニング状態、転送状態へと常に変化します。これによって、トラフィックの損失が発生することがあります。

Flow Control（フロー制御）

低速デバイスが高速デバイスと通信できるようにします。つまり、高速デバイスからのパケットの送信を止めます。

Fragment（フラグメント）

576 ビットよりも小さい Ethernet パケットです。

Frame（フレーム）

物理メディアに必要なヘッダー情報および後書き情報を含むパケットです。

G

GARP

General Attributes Registration Protocol の略。クライアントステーションをマルチキャストドメインに登録します。

Gigabit Ethernet（ギガビットイーサネット）

ギガビット Ethernet の伝送速度は 1000 Mbps です。既存の 10 / 100 Mbps Ethernet 標準との互換性があります。

GVRP

GARP VLAN Registration Protocol の略。クライアントステーションをマルチキャストドメインに登録します。

H

HOL

Head of Line の略。パケットはキューに入ります。キューの先頭にあるパケットは、行末のパケットより先に転送されます。

Host（ホスト）

他のコンピュータに対する情報またはサービスの発信元となるコンピュータです。

HTTP

Hypertext Transfer Protocol の略。インターネットを介して、サーバーとクライアントの間で HTML 文書を送信します。

I

IC

Integrated Circuit の略。IC は、半導体物質からなる小さい電子デバイスです。

ICMP

Internet Control Message Protocol の略。処理エラーを報告する場合などに、ゲートウェイまたは宛先のホストからソースホストに通信できるようにします。

IEEE

Institute of Electrical and Electronics Engineers の略。通信およびネットワークの標準を開発するエンジニアリング組織です。

IEEE 802.1d

スパニングツリープロトコルで使用される IEEE 802.1d では、ネットワークループを回避するために MAC ブリッジをサポートしています。

IEEE 802.1p

データリンク層または MAC 副層でネットワークトラフィックに優先度を付けます。

IEEE 802.1Q

ブリッジ接続された LAN インフラストラクチャ内の VLAN の定義、運用、および管理を可能にする VLAN Bridge の動作を定義します。

Image File

（イメージファイル）

システムイメージは、イメージ 1 およびイメージ 2 と呼ばれる 2 つのフラッシュセクターに保存されます。アクティブなイメージにはアクティブなコピーが保存され、もう 1 つのイメージには 2 番目のコピーが保存されます。

Ingress Port（入口ポート）

ネットワークトラフィックを受信するポートです。

IP

Internet Protocol の略。パケットのフォーマットとアドレス設定方法を指定します。IP はパケットをアドレス指定し、適切なポートに転送します。

IP Address（IP アドレス）

Internet Protocol アドレス。2 つ以上の LAN または WAN を相互接続しているネットワークデバイスに割り当てられた固有のアドレスです。

J

Jumbo Frames（ジャンボフレーム）

同一のデータを少数のフレームで送信できるようにします。ジャンボフレームによって、オーバーヘッド、処理時間、および割り込みが減少します。

L

LAG

Link Aggregated Group の略。ポートまたは VLAN を単一の仮想ポートまたは VLAN に集約します。

LAG の詳細については、「**LAG** メンバーシップの定義」を参照してください。

LAN

Local Area Networks の略。1 つの部屋、建物、キャンパスなど、地理的に限られたエリアに内包されるネットワークです。

Layer 2（レイヤー 2）

データリンク層または MAC 層です。クライアントまたはサーバーステーションの物理アドレスが含まれます。レイヤー 2 には処理する情報が少ないため、レイヤー 3 より迅速に処理されます。

Layer 4（レイヤー 4）

接続を確立し、すべてのデータがそれぞれの宛先に確実に到達するようにします。レイヤー 4 レベルで検査されたパケットは、各アプリケーションに基づいて分析され、送信決定が行われます。

Load Balancing（負荷分散）

データや処理パケットが、使用可能なネットワークリソース全体に均等に分配されるようにします。たとえば、負荷分散によって、着信パケットをすべてのサーバーに均等に分配したり、そのパケットを使用可能な次のサーバーにリダイレクトすることができます。

M

MAC Address（MAC アドレス）

Media Access Control アドレス。MAC アドレスは、各ネットワークノードを識別するハードウェア固有のアドレスです。

MAC Address Learning（MAC アドレス学習）

MAC アドレス学習はパケットの送信元 MAC アドレスが記録される学習ブリッジの特性です。記録されているアドレスに宛先指定されたパケットは、そのアドレスが存在するブリッジインタフェースにのみ送信されます。記録されていないアドレスに宛先指定されたパケットは、すべてのブリッジインタフェースに送信されます。MAC アドレス学習によって、接続されている LAN 上のトラフィックを最小限に抑えることができます。

MAC Layer（MAC 層）

データリンク制御（DTL）層の副層です。

Mask（マスク）

IP アドレスの一部など、特定の値を包含または除外するフィルターです。

たとえば、ユニット 2 が 10 分サイクルの最初の 1 分目に挿入され、ユニット 1 が同じサイクルの 5 分目に挿入された場合、いずれのユニットも挿入時間は同一と見なされます。

MD5

Message Digest 5 の略。128 ビットハッシュを作成するアルゴリズムです。MD5 は、MD4 の変形で、MD4 よりもセキュリティが向上しています。MD5 は、通信の完全性を検証し、通信の発信元を認証します。

MDI

Media Dependent Interface の略。エンドステーションに使用するケーブルです。

MDIX

Media Dependent Interface with Crossover の略。ハブとスイッチに使用するケーブルです。

MIB

Management Information Base の略。MIB には、ネットワークコンポーネントの特定の側面を示す情報が保存されています。

Multicast（マルチキャスト）

1 つのパケットのコピーを複数のポートに送信します。

N

NMS

Network Management System の略。システムを管理する方法を提供するインタフェースです。

Node（ノード）

ネットワーク接続のエンドポイント、または、複数のネットワークラインに共通する接点です。ノードには、次のものが含まれます。

- プロセッサ
- コントローラ

- ワークステーション

O

OID

Object Identifier の略。管理対象オブジェクトを識別するために SNMP が使用します。SNMP マネージャとエージェントのネットワーク管理パラダイムでは、管理対象オブジェクトごとに識別用の OID が必要です。

P

Packets（パケット）

パケット交換システムでやり取りされる情報のブロックです。

PDU

Protocol Data Unit の略。プロトコル制御情報と層のユーザーデータからなる、層プロトコルで指定されたデータユニットです。

PING

Packet Internet Groper の略。特定の IP アドレスが使用可能かどうかを確認します。パケットが別の IP アドレスに送信されて、応答を待ちます。

Port（ポート）

物理ポートは、マイクロプロセッサと周辺機器との通信を可能にする接続コンポーネントです。

Port Mirroring（ポートミラリング）

送受信パケットのコピーをあるポートから監視ポートへ転送することによって、ネットワークトラフィックの監視とミラーリングを行います。

ポートミラーリングの詳細については、「ポートミラーリングセッションの定義」を参照してください。

Port Speed（ポートスピード）

ポートのスピードを示します。ポートスピードには、次のものがあります。

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

Protocol（プロトコル）

デバイスがネットワーク全体で情報を交換する方法を規定した一連のルールです。

Q

QoS

Quality of Service の略。ネットワーク管理者は、QoS を使用することで、優先度、アプリケーションタイプ、および送信元と受信先のアドレスに従って、どのネットワークトラフィックをどのように送信するかを決定できます。

Query（クエリ）

データベースから情報を抽出し、使用する情報を表示します。

R

RADIUS

Remote Authentication Dial-In User Service の略。システムユーザーを認証し、接続時間を追跡する方法です。

RMON

Remote Monitoring の略。単一のワークステーションからネットワーク情報の収集が可能になります。

Router（ルーター）

独立した複数のネットワークに接続する 1 台のデバイスです。2 つ以上のネットワーク間でパケットを転送します。ルーターは、レイヤー 3 レベルで動作します。

RSTP

Rapid Spanning Tree Protocol の略。転送ループを作成せずに、スパニングツリーをより迅速に収束できるネットワークトポロジを検知して使用します。

Running Configuration File（実行設定ファイル）

起動設定ファイルのすべてのコマンドと、現在のセッション中に入力されたすべてのコマンドが保存されます。スイッチモジュールの電源を切ったり、再起動すると、実行設定ファイルに保存されたコマンドはすべて失われます。

S

Segmentation（セグメント化）

ブリッジングを行うために、LAN を別個の LAN セグメントに分割します。セグメント化によって、LAN 帯域幅の制限がなくなります。

Server（サーバー）

ネットワーク上の他のコンピュータにサービスを提供する中心的なコンピュータです。サービスには、ファイルの格納やアプリケーションへのアクセスなどがあります。

SNMP

Simple Network Management Protocol の略。LAN を管理します。SNMP ベースのソフトウェアは、SNMP エージェントが組み込まれたネットワークデバイスと交信します。SNMP エージェントは、ネットワークの活動とデバイスの状態に関する情報を集め、その情報をワークステーションに返信します。

SNTP

Simple Network Time Protocol の略。SNTP は、ネットワークスイッチのクロック時間についてミリ秒まで正確な同期を保証します。

SoC

System on a Chip の略。システム全体を包含する ASIC です。たとえば、電気通信の SoC アプリケーションには、マイクロプロセッサ、デジタル信号プロセッサ、RAM、および ROM を包含できます。

Spanning Tree Protocol（スパニングツリープロトコル）

ネットワークトラフィック内のループを防止します。スパニングツリープロトコル（STP）は、ブリッジの配置に関係なくツリー構造を提供します。また、ネットワーク上のエンドステーション間に 1 つのパスを提供し、ループを排除します。

SSH

Secure Shell の略。ネットワークを介して別のコンピュータにログインし、リモートコンピュータに対してコマンドを実行し、別のコンピュータにファイルを転送することを許可します。SSH により、セキュリティで保護されていないチャネルを介して強力な認証と安全な通信を行う方法が提供されます。

Startup Configuration（スタートアップ設定）

スイッチモジュールが停止または再起動されたときに、正確なスイッチモジュール設定を保持します。

Subnet（サブネット）

サブネットワーク。サブネットは、ネットワークの中で共通のアドレスコンポーネントを共有する部分です。TCP/IP ネットワークでは、プレフィックスを共有するデバイスが同一のサブネットに属します。たとえば、プレフィックス 157.100.100.100 を持つすべてのデバイスは、同一のサブネットに属します。

Subnet Mask（サブネットマスク）

サブネットアドレスに使用されている IP アドレスの全部または一部のマスキングに使用します。

Switch（スイッチ）

LAN セグメント間でパケットをフィルターにかけて転送します。スイッチは、すべてのパケットプロトコルタイプをサポートします。

T

TCP / IP

Transmissions Control Protocol の略。2 台のホストが接続し、データストリームを交換できるようにします。TCP はパケットの配信を保証します。また、パケットが送信された順序で受信されることを保証します。

Telnet

Terminal Emulation Protocol。システムユーザーは、Telnet を使用することで、リモートネットワーク上のリソースにログインし、使用することができます。

TFTP

Trivial File Transfer Protocol の略。ファイルの転送にセキュリティ機能のない User Data Protocol（UDP）を使用します。

Trap（トラップ）

システムイベントが発生したことを示す、SNMP によって送信されるメッセージです。

Trunking（トランキング）

リンク集約。ポートのグループを関連付けて 1 つのトランク（集約グループ）を形成することにより、ポートの使用を最適化します。

U

UDP

User Data Protocol の略。パケットは送信しますが、配信は保証しません。

Unicast（ユニキャスト）

あるパケットを特定のユーザーに送信する経路指定の形式です。

V

VLAN

Virtual Local Area Networks の略。ハードウェアソリューションの定義ではなく、ソフトウェアを介して作成されたローカルエリアネットワーク（LAN）を持つ論理的なサブグループです。

W

WAN

Wide Area Networks の略。地理的に広いエリアにまたがるネットワークです。

Wildcard Mask（ワイルドカードマスク）

どの IP アドレスビットを使用し、どのビットを無視するかを指定します。ワイルドスイッチモジュールマスク 255.255.255.255 は、重要なビットがないことを示します。ワイルドカード 0.0.0.0 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、宛先 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 アドレスの先頭 2 ビットが使用され、末尾の 2 ビットは無視されます。

メモ、注意および警告