Dell™ PowerConnect™ 35xx 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：手順に従わなかった場合にハードウェアが損傷したり、データが損失したりする可能性を説明しています。

警告：物質的損害、けが、または死亡の原因となる可能性があることを示しています。

この文書の情報は、事前の通知なく変更されることがあります。
© 2007-2008 すべての著作権は **Dell Inc.** にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

この文書に使用されている商標について： Dell、DELL の logo、Dell OpenManage、および PowerConnect は Dell Inc. の商標です。Microsoft および Windows は、米国およびその他の国における Microsoft Corporation の商標または登録商標です。

この文書では、上記記載以外の商標や会社名が使用されている場合があります。これらの商標や会社名は、一切 Dell Inc. に帰属するものではありません。

2008 年 **11** 月　　**Rev. A01**

目次に戻る

はじめに

Dell™ PowerConnect™ 35xx システムユーザーズガイド

PowerConnect 3524/3548 および PowerConnect 3524P/3548P は、スタック可能な高性能マルチレイヤーデバイスです。PowerConnect のユニットは、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（最高 8 台のスタッキングメンバー）のいずれとしても機能します。

この 『ユーザーガイド』 には、本デバイスの取り付け、設定、および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 3524/3548 および PowerConnect 3524P/3548P は、最小限の管理に多用途性を備えています。PowerConnect 3524 および 3548 シリーズには、次のデバイスタイプがあります。

- PowerConnect 3524
- PowerConnect 3524P
- PowerConnect 3548
- PowerConnect 3548P

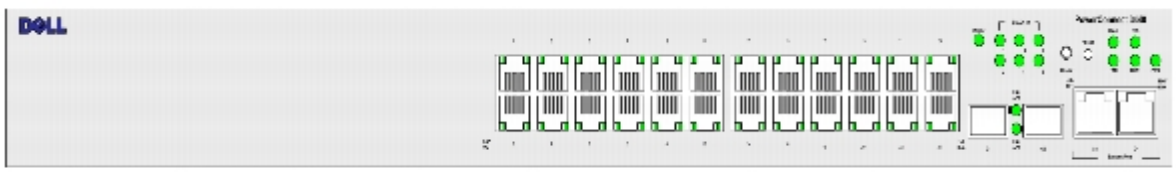
PowerConnect 3524

PowerConnect 3524 には、24 個の 10/100Mbps ポート、2 つの SFP ポート、および 2 つの銅線ポートが装備されており、スタンドアロンデバイスでのトラフィックの転送、またはデバイスがスタックされている場合はスタッキングポートとして使用できます。このデバイスには RS-232 コンソールポートも 1 つ装備されています。PowerConnect 3524 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 3524P

PowerConnect 3524P には、24 個の 10/100Mbps ポート、2 つの SFP ポート、および 2 つの銅線ポートが装備されており、スタンドアロンデバイスでのトラフィックの転送、またはデバイスがスタックされている場合はスタッキングポートとして使用できます。このデバイスには RS-232 コンソールポートも 1 つ装備されています。PowerConnect 3524P 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 3524P は パワーオーバーイーサネット（PoE）も装備されています。

図 **1-1 PowerConnect 3524** および **PowerConnect 3524P**



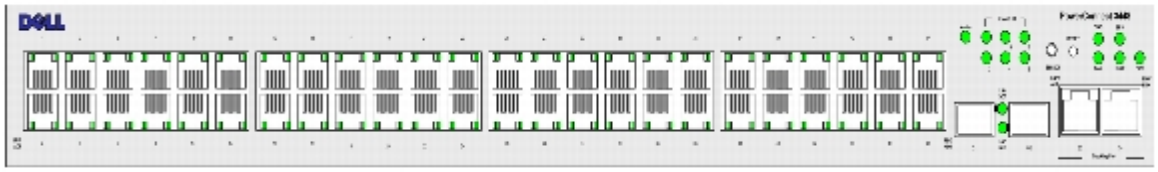
PowerConnect 3548

PowerConnect 3548 には、48 個の 10/100Mbps ポート、2 つの SFP ポート、および 2 つの 銅線ポートが装備されており、スタンドアロンデバイスでのトラフィックの転送、またはデバイスがスタックされている場合はスタッキングポートとして使用できます。このデバイスには RS-232 コンソールポートも 1 つ装備されています。PowerConnect 3548 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 3548P

The PowerConnect 3548P には、48 個の 10/100Mbps ポート、2 つの SFP ポート、および 2 つの 銅線ポートが装備されており、スタンドアロンデバイスでのトラフィックの転送、またはデバイスがスタックされている場合はスタッキングポートとして使用できます。このデバイスには RS-232 コンソールポートも 1 つ装備されています。さらに、PowerConnect 3548P には PoE も搭載されています。

図 **1-2 PowerConnect 3548** および **PowerConnect 3548P**



スタッキングの概要

PowerConnect 3524/P および PowerConnect 3548/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、一箇所からの複数のスイッチ管理を提供します。すべてのスタックメンバーは、スタックが管理される単一の IP アドレスを通じてアクセスされます。スタックは以下から管理されます。

- 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 3524/P および PowerConnect 3548/P デバイスはスタックごとに最高 8 台のユニットをサポートしますが、スタンドアロンユニットとしても動作します。

スタッキングをセットアップする際、1 つのスイッチをスタックマスターとして選択し、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。その他すべてのデバイスはスタックメンバーとして選択でき、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ごとに個別にダウンロードします。ただし、スタック内のすべてのユニットが同じソフトウェアバージョンを実行する必要があります。

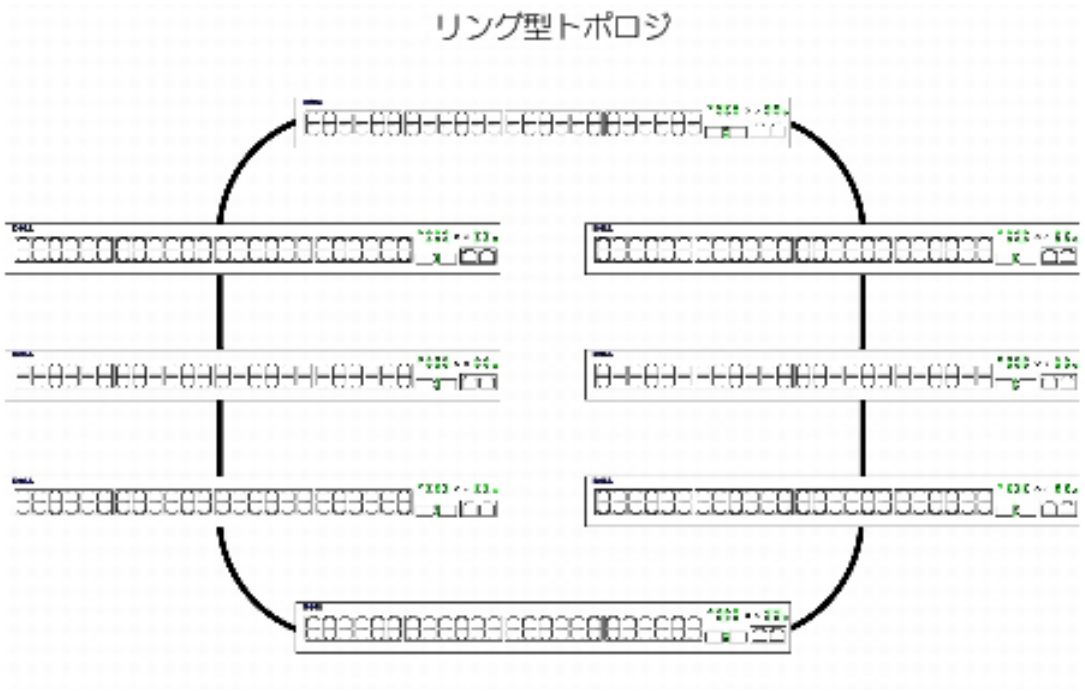
スイッチのスタッキングおよび設定はスタックマスターによって保持されます。次のイベントが発生した場合、スタックマスターは、操作上の影響を最小限にとどめながらポートを検出および再設定します。

- ユニット障害
- ユニット間のスタッキングリンク障害
- 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 35xx シリーズシステムはリング型トポロジで動作します。スタックされたリング型トポロジでは、スタック内のすべてのデバイスは円形に相互接続されています。スタック内の各デバイスは、データを受信し、それを接続されているデバイスに送信します。このパケットは送信先に届くまでスタック内で送信され続けます。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** リング型トポロジのスタッキング



リング型トポロジで発生する問題の多くは、リング内のデバイスが機能しなくなるか、リンクが切れた場合に起こります。PowerConnect 3524/P および PowerConnect 3548/P のスタックでは、システムはダウンタイムなしで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ます。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必要ありません。ただし、スタッキングの整合性を確実にするため、スタッキングリンクまたはスタッキングメンバーを修正する必要があります。

スタッキングの問題が解決した後、中断なしでデバイスをスタックに再接続でき、リング型トポロジが回復されます。

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不具合が発生すると、スタックはスタッキングフェイルオーバートポロジで復帰します。スタッキングフェイルオーバーでは、デバイスはチェーン型で動作します。スタックマスターはどこにパケットが送信されるかを決定します。各ユニットは、最上部および最下部のユニット以外、隣接する 2 つのデバイスに接続しています。

スタッキングメンバーおよびユニット ID

スタッキング構成にはスタッキングユニット ID が欠かせません。スタッキング動作は起動処理中に決定されます。動作モードは初期化処理中に選択されたユニット ID によって決定されます。例えば、ユーザーがスタンドアロンモードを選択した場合、デバイスは起動処理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、出荷時にスタンドアロンユニットのデフォルト ID が設定されています。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、すべてのスタッキング LED はオフになります。

ユーザーが別のユニット ID を選択すると、その ID は削除されず、ユニットがリセットされても引き続き有効となります。

ユニット ID 1 および Unit ID 2 はマスター対応ユニット用に予約されています。ユニット ID 3 から 8 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、またはスタックメンバーを挿入または取り外す際、マスターユニットはスタッキング検出処理を開始します。

メモ： 同じユニット ID を持つメンバーが 2 つ検出された場合、スタックは引き続き機能しますが、先にスタックに参加したユニットのみがスタックに参加できます。ユニットがスタックに参加できなかったことを伝え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および取り付け

ユニット 1 および ユニット 2 はマスター対応ユニットです。ユニット 1 および 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処理中に行われます。次の決定手順に沿って、マスター対応スタックメンバーのひとつがマスターとして選択され、もう一方のマスター対応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。

- スタックマスター対応ユニットが 1 台しかない場合、そのユニットがマスターとして選択されます。
- マスター対応スタッキングメンバーが 2 台あり、そのうちのひとつが手動でスタックマスターに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。
- マスター対応ユニットが 2 台あり、どちらもマスターとして手動設定されていない場合、アップタイムが長いユニットがスタックマスターとして選択されます。
- マスター対応ユニットが 2 台あり、両方がマスターとして手動設定されている場合、アップタイムが長いユニットがスタックマスターとして選択されます。
- 2 台のマスター対応スタッキングメンバーのアップタイムが同じである場合、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。

例えば、ユニット 2 が 10 分サイクルの最初の 1 分に挿入され、ユニット 1 が同じ 10 分サイクルの 5 分目に挿入された場合、これらのユニットのアップタイムは同じとみなされます。同じアップタイムのマスター対応スタックが 2 台ある場合、ユニット 1 がマスターとして選択されます。

スタックマスターおよび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。ウォームアップスタンバイは、フェイルオーバーが発生した場合に、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ようにします。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。

ウォームスタンドバイ中、マスターおよびバックアップマスターは静的設定でのみ同期化されます。スタッキングマスターが設定される際、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を同期化する必要があります。動的設定は保存されず、例えば、動的に学習された MAC アドレスは保存されません。

スタックの各ポートには固有のユニット ID、ポートタイプおよびポート番号があり、これらは設定コマンドおよび設定ファイル両方の一部です。設定ファイルはデバイススタックマスターによってのみ管理されます。管理には次が含まれます。

- フラッシュへの保存
- 外部 TFTP サーバー /HTTP クライアントへの設定ファイルのアップロード
- 外部 TFTP サーバー /HTTP クライアントからの設定ファイルのダウンロード

メモ： 設定済みポートすべてのスタック設定は、スタックがリセットされた、またはポートが存在しなくなった場合でも保存されます。

再起動が行われる時は常にトポロジの検出が実行され、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 はユニットに保存され、トポロジの検出によって学習されます。選択されたマスターがない状態で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。

設定ファイルは明確なユーザー設定を通じてのみ変更されます。次の場合には、設定ファイルの自動変更は行われません。

- ユニットが追加された
- ユニットが取り外された
- ユニットのユニット ID が再割り当てされた
- 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間で切り替えられた

システムが再起動される毎に、マスターユニット内のスタートアップ設定ファイルがスタックの設定に使用されます。

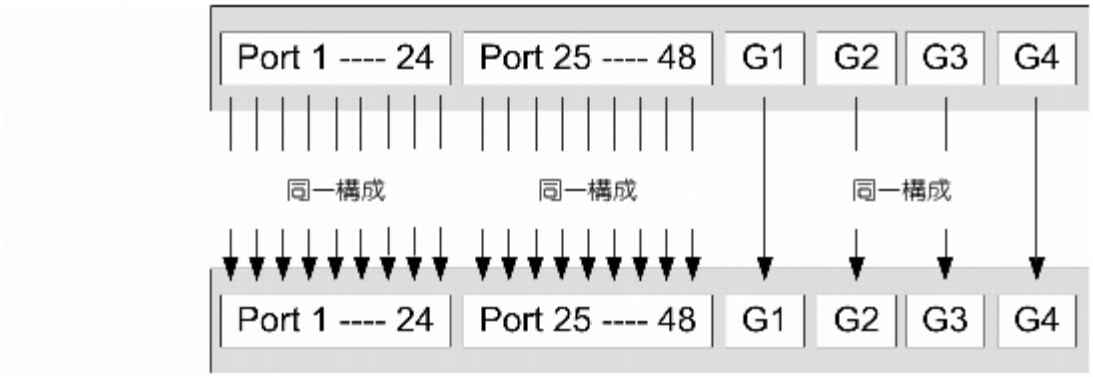
スタックからスタックメンバーが取り外され、同じユニット ID を持つユニットと交換された場合、スタックメンバーは元のデバイス設定によって設定されます。物理的に存在するポートのみが PowerConnect OpenManage Swhitch Administrator のホームページに表示され、ウェブ管理システムを使って設定できます。表示されないポートは CLI または SNMP インタフェースで設定します。

スタッキングメンバーの交換

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使用されていた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より多い、または少ない場合、適切なポート設定が新しいスタックメンバーに使用されます。例えば、次のように適用されます。

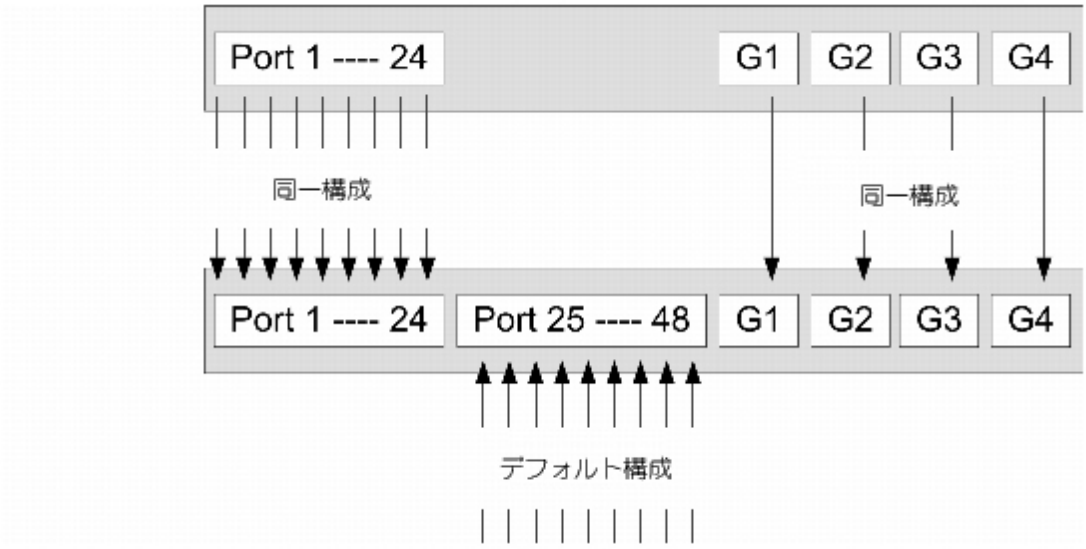
- PowerConnect 3524/P を PowerConnect 3524/P に交換する場合、すべてのポート設定はそのまま同じになります。
- PowerConnect 3548/P を PowerConnect 3548/P に交換する場合、すべてのポート設定はそのまま同じになります。

図 **1-4. PowerConnect 3548/P** を **PowerConnect 3548/P** に交換



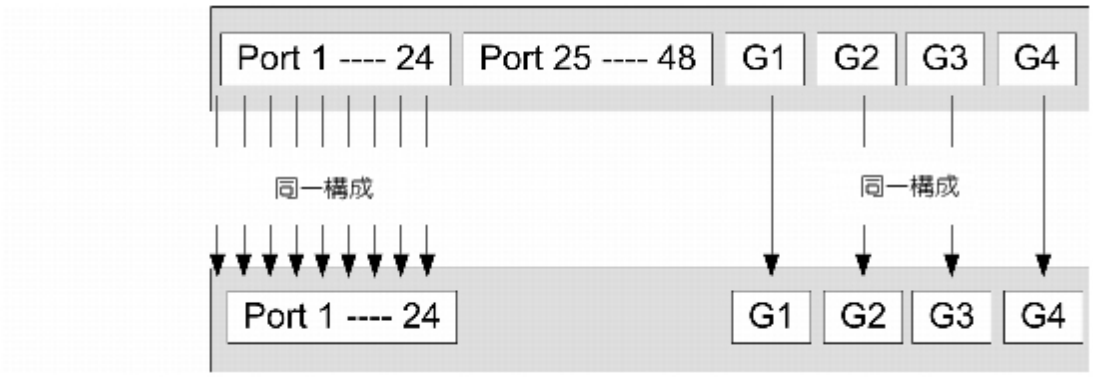
- PowerConnect 3524/P を PowerConnect 3548/P に交換する場合、最初の 3548/P 24 FE ポートが 3524/P 24 FE ポートの設定を受け取ります。GE ポート設定はそのまま同じになります。残りのポートはデフォルトのポート設定を受け取ります。

図 **1-5. PowerConnect 3548/P** ポートを **PowerConect 3524/P** ポートに交換



- PowerConnect 3548/P を PowerConnect 3524/P に交換する場合、PowerConnect 3524/P 24 FE ポートは最初の 24 FE PowerConnect 3548/P ポート設定を受け取ります。GE ポート設定はそのまま同じになります。

図 **1-6. PowerConect 3524/P** ポートを **PowerConnect 3548/P** ポートに交換



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

次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不具合が発生した、または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不具合が発生した
- 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間の切り替えは、限定的なサービスの損失を生じます。不具合が発生すると、動的テーブルのすべてが再学習されます。実行されている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機能の一覧は、最新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。

IP バージョン 6（IPv6）のサポート

このデバイスは、IPv6 対応ホストとしても、IPv4 ホストとしても機能します（デュアルスタックとも呼ばれます）。これは IPv6 のみのネットワーク、および IPv4 と IPv6 が組み合わされたネットワークにおいてもデバイスが動作することを可能にします。

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をアップデートまたは変更することなく、LAN ケーブルを通じてデバイスに電力を提供します。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 は次の用途に使用できます。

- IP 電話
- ワイヤレスアクセスポイント
- IP ゲートウェイ
- PDA
- オーディオおよびビデオリモート監視

パワーオーバーイーサネットに関する詳細は、「パワーオーバーイーサネットの管理」を参照してください。

ヘッドオブラインブロッキングの防止

ヘッドオブライン（HOL）ブロッキングは、トラフィックが同一の出口ポートリソースを求めて競合することから、トラフィックの遅延とフレームの損失が発生します。HOL がデバイスキューパケットをブロックすることを防止するため、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、パケットの送信を止めるように高速デバイスに要求することで、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。バッファのオーバーフローを防止するために、送信が一時的に停止されます。

ポートまたは LAG に対するフロー制御の詳細に関しては、「ポート設定の定義」または「LAG パラメーターの定義」を参照してください。

バックプレッシャーのサポート

半二重リンクにおいて、追加のトラフィックが使用できないように受信側のポートがリンクを占有することで、バッファの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詳細に関しては、「ポート設定の定義」または「LAG パラメーターの定義」を参照してください。

仮想ケーブルテスト（VCT：Virtual Cable Testing）

VCT は、銅線リンクケーブリングの存在を検知して、オープンケーブルやケーブルショートなどを報告します。ケーブルテストの詳細に関しては、「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

オートネゴシエーションが有効になっている場合、デバイスは RJ-45 ポートに接続されたケーブルがクロスケーブルかストレートケーブルかを自動的に検知します。

エンドステーション用の標準配線は メディア依存型インタフェース（MDI：Media-Dependent Interface）として知られ、ハブとスイッチ用の標準配線は メディア依存型インタフェースクロスオーバー（MDIX：Media-Dependent Interface with Crossover）として知られています。

ポートまたは LAG における MDI/MDIX 設定の詳細に関しては、「ポート設定の定義」またはLAG パラメーターの定義を参照してください。

オートネゴシエイション

オートネゴシエイションはデバイスが動作モードを公示することを可能にします。オートネゴシエイション機能は、ポイントツーポイントのリンクセグメントを共有する 2 つのデバイス間で情報交換するための手段を提供し、両方のデバイスの伝送能力を最大限に引き出すように自動設定します。

PowerConnect 35xx シリーズシステムは、ポート公示機能を提供することによりオートネゴシエーション機能を向上させます。ポート公示機能により、システム管理者は公示されるポートスピードを設定することが可能になります。

オートネゴシエイションの詳細に関しては、「ポート設定の定義」または「LAG パラメーターの定義」を参照してください。

音声 VLAN

ネットワーク管理者は音声 VLAN を利用して、特定の VLAN 上の IP 電話から IP 音声トラフィックを伝送するようにポートを設定することにより、VoIP サービスを拡張できます。VoIP トラフィックの送信元 MAC アドレスには、事前設定された OUI 識別コードが含まれています。ネットワーク管理者は、音声 IP トラフィックの転送元となる VLAN を設定できます。自動音声 VLAN セキュアモードでは、音声 VLAN からの VoIP 以外のトラフィックが破棄されます。また、音声 VLAN では VoIP に QoS が提供されるので、IP トラフィックの受信が不均衡の場合でも音声の品質が低下することはありません。

詳細に関しては、「音声 VLAN の設定」を参照してください。

ゲスト VLAN

ゲスト VLAN は、権限のないポートに制限付きのネットワークアクセス権を与えます。ポートがポートベース認証でネットワークアクセスを拒否された場合でも、ゲスト VLAN が有効であれば、そのポートは制限付きのネットワークアクセス権を得ることができます。

MAC アドレスサポート機能

MAC アドレス容量のサポート

デバイスは、最大 8,000 個の MAC アドレスをサポートします。特定の MAC アドレスがシステム用に予約されています。

静的な MAC エントリ

受信フレームから MAC エントリを学習する方法の代替として、ブリッジ表に MAC エントリを手動で入力することができます。このようにユーザーが定義したエントリは、エージングの対象にはならず、リセットおよび再起動を行った後も保持されます。

詳細に関しては、「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、受信するパケットからのコントロールされた MAC アドレスを学習します。MAC アドレスは、ブリッジ表に保存されます。

MAC アドレスの自動エージング

ある一定期間にトラフィックが送信されなかった MAC アドレスは削除されます。これによって、ブリッジ表のオーバーフローを防止できます。

MAC アドレスのエージングタイムの詳細に関しては、「動的アドレスの表示」を参照してください。

VLAN に対応した MAC ベースのスイッチング

デバイスは、常に VLAN 対応のブリッジングを実行します。宛先 MAC アドレスだけに基づいてフレームを転送する古典的なブリッジング（IEEE802.1D）は実行されません。ただし、タグなしのフレームに対して、同様の機能を設定することができます。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。

MAC マルチキャストのサポート

マルチキャストサービスは、制限付きのブロードキャストサービスで、1 対多および多対多の接続による情報配布を可能にします。レイヤ 2 マルチキャストサービスでは、単一のフレームが特定のマルチキャストアドレスに宛先指定され、そのアドレスからフレームのコピーが複数の関連ポートに送信されます。マルチキャストグループが静的に有効な場合、登録済みグループの宛先設定および未登録マルチキャストフレームの動作定義が可能です。

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

レイヤ 2 の機能

IGMP スヌーピング

インターネットグループメンバーシッププロトコル（IGMP：Internet Group Membership Protocol）スヌープ機能は、デバイスによってワークステーションからアップストリームのマルチキャストルータに転送される IGMP フレームの内容を検査します。デバイスは対象のフレームから、マルチキャストルータがマルチキャストフレームを送信する、マルチキャストセッションに設定されたワークステーションを識別します。IGMP クエリアは、マルチキャストルーターの動作をシミュレートすることから、マルチキャストルーターなしでも、レイヤ 2 マルチキャストドメインのスヌーピングが可能になります。

詳細に関しては、「IGMP スヌーピング」を参照してください。

ポートのミラーリング

ポートミラーリングは、着信パケットおよび発信パケットのコピーを、モニタ対象のポートからモニタ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モニタとミラーリングを行います。ユーザーは、指定のソースポートを通過するすべての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します。

詳細に関しては、「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

ストームコントロールによって、デバイスで受け入れ、転送するマルチキャストフレームおよびブロードキャストフレームの量を制限できます。

レイヤ 2 フレームが転送されると、関連する VLAN 上のすべてのポートに多数のブロードキャストフレームおよびマルチキャストフレームが送信されます。これによって帯域幅が占有され、すべてのポートに接続しているすべてのノードに負荷がかかります。

詳細に関しては、「ストーム制御の有効化」を参照してください。

VLAN サポート機能

VLAN のサポート

VLAN は、単一のブロードキャストドメインを構成するスイッチイングポートの集まりです。パケットは、VLAN タグ、または入力ポートとパケットの内容のコンビネーションに基づいて VLAN に属していると判断されます。属性を共有するパケットは、同じ VLAN にまとめることができます。

詳細に関しては、「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、VLAN への着信パケットを入力ポートに基づいて分類します。

詳細に関しては、「VLAN ポート設定の定義」を参照してください。

802.1Q VLAN タギングへの完全準拠

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）は、IEEE 802.1Q 準拠の VLAN のプルーニングと 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 が有効である場合、デバイスは、VLAN メンバーシップを、基礎をなすアクティブな「スパニングツリープロトコル機能」トポロジに属するすべてのポートに登録し伝搬します。

詳細に関しては、「GVRP パラメーターの設定」を参照してください。

プライベート VLAN エッジ

ポートはプライベート VLAN エッジ（PVE）グループに割り当てる事ができます。PVE として定義されたポートは、アップリンクによって保護されるので、同じ VLAN 内の他のポートから隔離されます。アップリンクは GE ポートである必要があります。

プライベート VLAN の詳細に関しては、「ポートの設定」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 2 スイッチ要件であり、ブリッジによってレイヤ 2 における転送ループを自動的に防止および解決することを可能にします。スイッチは、特別にフォーマット化されたフレームを使って設定メッセージを交換し、ポートに対して送信を有効にするか、無効にするかを選択します。

詳細に関しては、「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。

高速リンク

STP では、収束に最大 30～60 秒かかる場合があります。この時間で STP はループの存在を検知し、ステータス変更の伝搬と関連デバイスの応答を可能にします。30～60 秒は、多くのアプリケーションにとっては応答時間として長すぎると見なされます。高速リンクオプションはこの遅延を回避し、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。

ポートおよび LAG に対して高速リンクを有効にする場合の詳細に関しては、「STP ポート設定の定義」または「STP LAG 設定の定義」を参照してください。

IEEE 802.1w 高速スパニングツリー

スパニングツリーは、各ホストにつき 30～60 秒の間に、そのポートがアクティブにトラフィックを送信しているかどうかを判断できます。高速スパニングツリー（RSTP：Rapid Spanning Tree）は、ネットワークトポロジの使用を検知して、転送ループを作成しない迅速な収束を可能にします。

詳細に関しては、「高速スパニングツリーの定義」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（MSTP）動作は、VLAN を STP インスタンスにマップします。MSTP は異なる負荷バランシングシナリオを提供します。各種の VLAN に割り当てられたパケットは、多重スパニングツリーリージョン（MSTP リージョン）内の様々なパスに沿って送信されます。リージョンとは、フレームを送信できる 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。

詳細に関しては、「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 つの集約リンクまで定義でき、それぞれが 8 つまでのメンバーポートを持って単一の リンク集約グループ（LAG）を形成します。これによって、次のことが可能になります。

- 物理リンクの障害からのフォールトトレランス保護
- 広帯域幅による接続
- 帯域幅粒度の向上
- 広帯域幅によるサーバー接続

LAG は、スピードが同じで、全二重方式に設定された複数のポートで構成されます。

詳細に関しては、「Defining LAG パラメーターの定義」を参照してください。

リンク集約と **LACP**

LACP では、リンク上のピア交換を使って、絶えず、各種リンクの集約機能を判断し、所定の 2 つのデバイス間で実現可能な最大レベルの集約機能を継続的に提供します。LACP は、システム内でポートバインドを自動的に判断、設定、バインド、およびモニタします。

詳細に関しては、「ポートの集約」を参照してください。

BootP および **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のセットアップパラメーターを受け取ることができます。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 の詳細に関しては、「DHCP IPv4 インタフェースパラメーターの定義」を参照してください。

サービス品質の機能

サービスクラス **802.1p** のサポート

IEEE 802.1p 信号方式は、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マークを付け、優先度付けすることを目的とした、OSI レイヤ 2 の標準です。802.1p トラフィックは分類されて、宛先に送信されます。帯域幅の予約や制限は設定も強制もされていません。802.1p は、802.1Q（VLAN）標準の副次的な標準です。802.1p では、IP 優先権 IP ヘッダービットフィールドと同様に 8 つの優先度を設定しています。

詳細に関しては、「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 アラームおよびトラップのログ

システムは、重大度コードとタイムスタンプを付けてイベントをログに記録します。イベントは、SNMP トラップとしてトラップ宛先リストに送られます。

SNMP アラームおよびトラップの詳細に関しては、「SNMP パラメーターの定義」を参照してください。

SNMP バージョン 1、2 および 3

UDP/IP プロトコルを使用した Simple Network Management Protocol（SNMP）は、システムへのアクセスを制御します。システムへのアクセスを制御するために、コミュニティエントリのリストが定義されます。各リストは、コミュニティストリングとそのアクセス権限で構成されます。SNMP セキュリティには、読み取り専用、読み書き、およびスーパーの 3 つのレベルがあり、スーパーユーザーだけがコミュニティ表にアクセスできます。

詳細に関しては、「SNMP パラメーターの定義」を参照してください。

ウェブベースによる管理

ウェブベースによる管理では、任意のウェブブラウザからシステムを管理できます。システムには HTML ページを提供する組み込みウェブサーバー（EWS：Embedded Web Server）が存在し、このサーバーを通じてシステムのモニタおよび設定を行うことができます。システムは内部的に、ウェブベースの入力を設定コマンド、MIB 変数設定、および管理に関係するその他の設定に変換します。

設定ファイルのダウンロードとアップロード

デバイス設定は、設定ファイルに保存されます。この設定ファイルには、システム規模のデバイス設定とポート固有のデバイス設定の両方が含まれます。システムは、CLI コマンドの集合の形で設定ファイルを表示します。これらのファイルはテキストファイルとして保存され、処理されます。

詳細に関しては、「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 を介した起動イメージ、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ています。

Remote Monitoring（RMON）

リモートモニタ（RMON：Remote Monitoring）は、SNMP の拡張版です。ネットワークデバイスの管理とモニタを可能にする SNMP とは対照的に、総合的なネットワークトラフィックモニタ機能を提供します。_RMON は、現在および過去の MAC 層の統計とコントロールオブジェクトを定義する標準の MIB であり、ネットワーク全体でのリアルタイムな情報の取得を可能にします。

詳細に関しては、「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）の構文および解釈は、共通する業界の慣行にできるだけ従っています。_CLI は、必須の要素とオプションの要素で構成されます。CLI インタプリタは、コマンドおよびキーワードを完成させることで、ユーザーを援助し、タイピングを簡略化します。

Syslog

Syslog は、イベント通知を一連のリモートサーバーに送信する機能を提供するプロトコルです。リモートサーバーではイベントを保存および検査し、それに基づいたアクションを取ることができます。システムは、重要なイベントに関する通知をリアルタイムに送信し、事後の使用に

備えてこれらのイベントの記録を保存します。

Syslog の詳細に関しては、「ログの管理」を参照してください。

SNTP

Simple Network Time Protocol（SNTP）は、ネットワーク上のイーサネットスイッチのクロックが、ミリ秒単位まで正確に時刻同期されることを確実にします。時間同期はネットワーク SNTP サーバーによって行います。タイムソースは階層によって確立されます。Stratum は、参照クロックからの距離を定義します。Stratum の値が大きいほど（ゼロが最大）、クロックの正確さが増します。

詳細に関しては、「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 サービスはドメインネームを数字の IP アドレスに翻訳します。例えば、www.ipexample.com は 192.87.56.2 に翻訳されます。DNS サーバーはドメインネームデータベース、およびそれに対応する IP アドレスを維持します。

詳細に関しては、「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

トレースルートを使用することにより、転送処理でパケットが転送された IP 経路を検出します。CLI トレースルートユーティリティは、User EXEC または Privileged のいずれかのモードで実行できます。

802.1ab（LLDP-MED）

Link Layer Discovery Protocol（LLDP）は、マルチベンダ環境のネットワークトポロジを検出および保持することによって、ネットワーク管理者がトラブルシューティングとネットワーク管理の強化を実現できるようにします。LLDP では、ネットワークデバイスが他のシステムに公示する方法や、検出した情報を保存する方法を標準化することにより、近隣のネットワークを検出します。複数の公示セットは、パケットの **Type Length Value**（タイプ、長さ、値）（TLV）フィールドで送信されます。LLDP デバイスは、システム名、システム ID、システムの説明、およびシステムの機能の公示に加えて、シャーシおよびポート ID の公示をサポートしている必要があります。

LLDP Media Endpoint Discovery（LLDP-MED）は、異なる IP システムを単一ネットワークの LLDP に共存させることで、ネットワークの柔軟性を高めます。この機能により、詳細なネットワークトポロジ情報、IP電話のロケーション情報を介した緊急電話サービス、およびトラブルシューティング情報が得られます。

セキュリティ機能

SSL

セキュアソケットレイヤ（SSL：Secure Socket Layer）は、プライバシー、認証、およびデータの完全性によって、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。SSL は、証明書と、パブリックキーおよびプライベートキーに依存します。

ポートベース認証（802.1x）

ポートベースによる認証では、外付けのサーバーを介してポートごとにシステムユーザーを認証できます。認証および承認されたシステムユーザーだけが、データを送受信できます。ポートの認証は、拡張認証プロトコル（EAP）を使って リモート認証ダイヤルインユーザーサービス（RADIUS）サーバー経由で行われます。ダイナミック VLAN 割り当て（DVA）では、ネットワーク管理者が、RADIUS サーバーの認証中にユーザーを自動的に VLAN に割り当てることができます。

詳細に関しては、「ポートベース認証」を参照してください。

ポートロックのサポート

ポートロックを使用すると、特定の MAC アドレスを持つユーザーにのみ特定のポートへのアクセスを制限することで、ネットワークセキュリティが高まります。これらのアドレスは、そのポートに対して手動で定義するか、自動的に学習されます。ロックされているポートにフレームが到達したときに、フレームの送信元 MAC アドレスがそのポートに関連付けられていない場合は、プロテクションメカニズムが起動します。

詳細に関しては、「ポートセキュリティの設定」を参照してください。

RADIUS クライアント

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、ユーザー名、パスワード、およびアカウンティング情報など、ユーザーごとの認証情報が保存されたユーザーデータベースを保持します。

詳細に関しては、「RADIUS の設定」を参照してください。

SSH

セキュアシェル（SSH）は、デバイスへの安全なリモート接続を実現します。現在、SSH バージョン 2 がサポートされています。SSH サーバー機能によって、SSH クライアントはデバイスとの安全な暗号化接続を確立できます。この接続では、Telnet 着信接続と同様の機能を利用できます。SSH では、デバイスの接続および認証に RSA および DSA パブリックキー暗号解読法を使用します。

TACACS+

TACACS+ は、デバイスにアクセスするユーザーを評価するための集中化セキュリティを提供します。TACACS+ は RADIUS および他の認証プロセスとの整合性は保持したままで集中化ユーザー管理システムを提供します。

詳細に関しては、「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、ネットワークのセキュリティとパスワードの制御が強化されます。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関しては、「パスワードの管理」を参照してください。

アクセスコントロールリスト（ACL）

ネットワーク管理者はアクセスコントロールリスト（ACL）を利用することにより、特定の入力ポートの分類処理およびルールを定義できます。入力ポートに到達したパケットは、アクティブな ACL を使用して、エントリを許可または拒否されます。拒否されると、その入力ポートは無効になります。パケットのエントリが拒否された場合、ユーザーはそのポートを無効にできます。

詳細については、「ACL の概要」を参照してください。

DHCP スヌーピング

DHCP スヌーピングは、信頼できないインタフェースと DHCP サーバーの間にファイアウォールセキュリティを提供することによって、ネットワークのセキュリティを強化します。ネットワーク管理者は DHCP スヌーピングを有効にすることによって、エンドユーザーまたは DHCP サーバーに接続する信頼できるインタフェースと、ネットワークファイアウォールの向こう側にある信頼できないインタフェースを区別できます。

詳細に関しては、「DHCP スヌーピングの設定」を参照してください。

追加の **CLI** マニュアル

マニュアル **CD** に収録されている『**CLI** リファレンスガイド』には、デバイスの設定に使用する **CLI** コマンドの情報が記載されています。この文書では、コマンドの説明、シンタックス、デフォルト値、ガイドライン、および例が説明されています。

目次に戻る

目次に戻る

ハードウェアの説明

Dell™ PowerConnect™ 35xx システムユーザーズガイド

ポートの説明

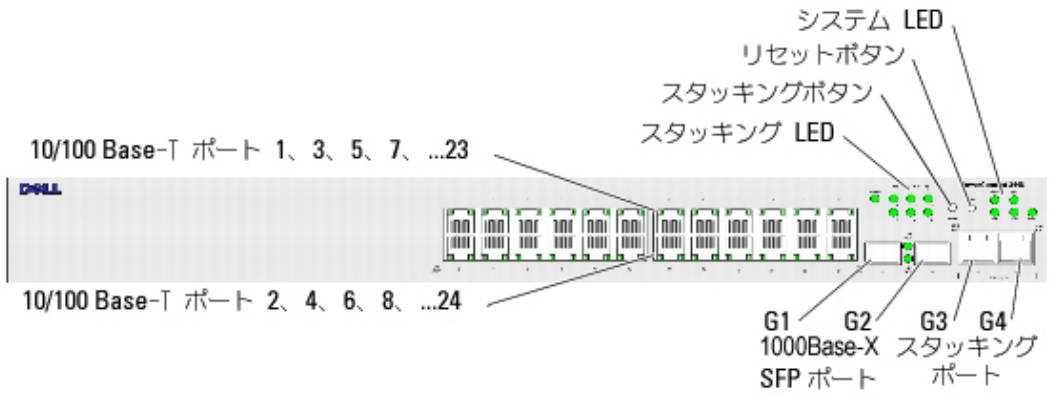
PowerConnect 3524 ポートの説明

PowerConnect 3524 デバイスは、次のポートで構成されています。

- ファーストイーサネットポート **×24** — 10/100Base-T ポートとして指定された RJ-45 ポート
- ファイバポート **×2** — 1000Base-X SFP ポートとして指定されたポート
- ギガビットポート **×2** — 1000Base-T ポートとして指定されたポート
- コンソールポート — RS-232 ベースのポート

次の図は、PowerConnect 3524 の前面パネルを示しています。

図 **2-1. PowerConnect 3524** の前面パネル

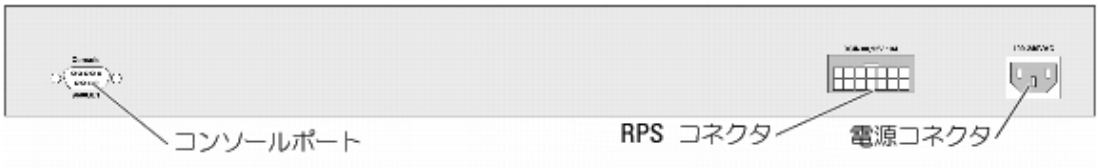


前面パネルには 24 個の RJ-45 ポート（1～24）が搭載されています。上の列にあるポートは 1 から 23 の奇数番号が付けられており、下の列にあるポートは 2 から 24 の偶数番号が付けられています。さらに、前面パネルにはファイバポートである ポート G1～G2 と、銅ポートであるポート G3～G4 もあります。ポート G3～G4 はスタッキングポートとして、またはスタンドアロンデバイスでのネットワークトラフィックの転送に使用できます。

前面パネルには 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の選択に使用され、2 番目のボタンであるリセットボタンは、デバイスを手動でリセットするために使用されます。リセットボタンは前面パネルの表面から突出していないので、誤ってボタンが押されることはありません。前面パネルの LED はすべてデバイス LED です。

次の図は、PowerConnect 3524 の背面を示しています。

図 **2-2. PowerConnect 3524** の背面パネル



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

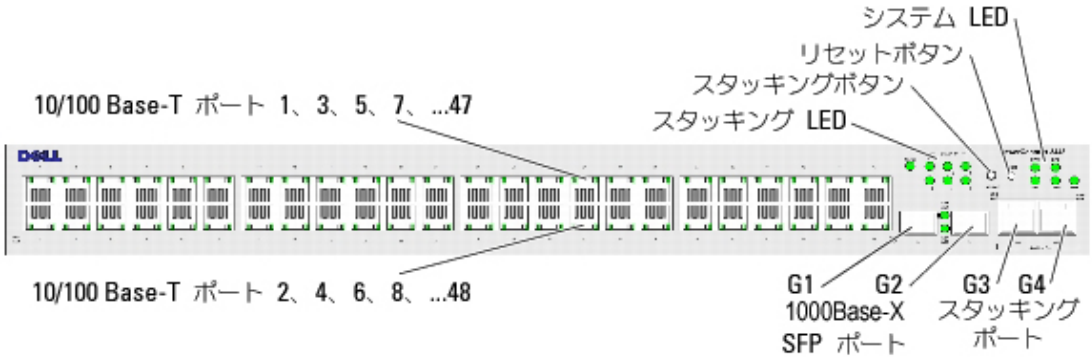
PowerConnect 3548 ポートの説明

PowerConnect 3548 デバイスは、次のポートで構成されています。

- **FE** ポート **×48** — 10/100Base-T として指定されている RJ-45 ポート
- ファイバポート **×2** — 1000Base-X SFP ポートとして指定されているポート
- ギガビットポート **×2** — 1000Base-T ポートとして指定されているポート
- コンソールポート — RS-232 コンソールベースのポート

次の図は、PowerConnect 3548 の前面パネルを示しています。

図 **2-3. PowerConnect 3548** の前面パネル

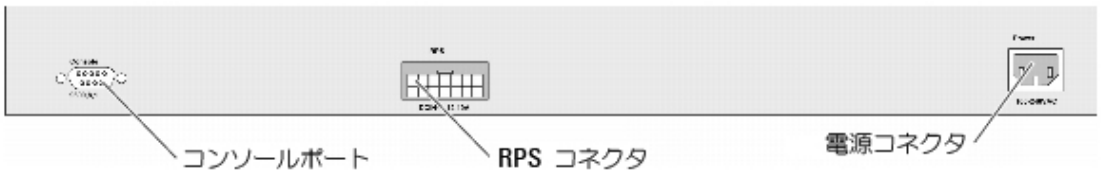


前面パネルには 48 個の RJ-45 ポート（1～48）が搭載されています。上の列にあるポートは 1 から 47 の奇数番号が付けられており、下の列にあるポートは 2 から 48 の偶数番号が付けられています。さらに、前面パネルいはファイバポートである ポート G1～G2 と、銅ポートであるポート G3～G4 があります。ポート G3～G4 はスタッキングポートとして、またはスタンドアロンデバイスでのネットワークトラフィックの転送に使用できます。

前面パネルには 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の選択に使用され、2 番目のボタンであるリセットボタンは、デバイスを手動でリセットするために使用されます。リセットボタンは前面パネルの表面から突出していないので、誤ってボタンが押されることはありません。前面パネルの LED はすべてデバイス LED です。

次の図は、PowerConnect 3548 の背面パネルを示しています。

図 **2-4. PowerConnect 3548** の背面パネル



背面パネルには RPS コネクタ、コンソールポートおよび電源コネクタが搭載されています。

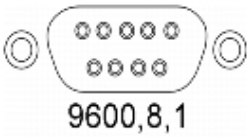
SFP ポート

スモールフォームファクタープラグ対応（SFP）ポートはファイバトランシーバで、10000 Base-SX または LX として指定されています。これには TWSI（2 線式シリアルインタフェース）および内蔵 EPROM が含まれています。

RS-232 コンソールポート

デバッグやソフトウェアのダウンロードなどに使用するターミナル接続用の DB-9 コネクタで、デフォルトのボーレートは 9,600 bps です。ボーレートは、2400～115,200 bps の範囲で設定できます。

図 **2-5.** コンソールポート



寸法

PowerConnect 3524/P および PowerConnect 3548/P デバイスの寸法は次の通りです。

PoE モデル：

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

非 PoE デバイス:

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

LED の定義

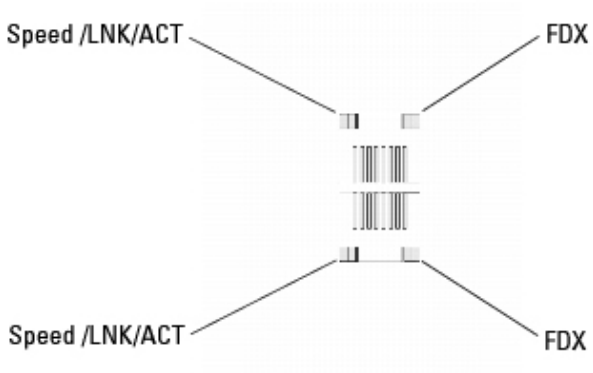
前面パネルには、リンク、電源装置、ファン、およびシステム診断のステータスを示す LED（Light Emitting Diode）が搭載されています。

ポート LED

10/100/1000 BaseT ポートおよび 10/100 BaseT ポートには、ポートごとに 2 つの LED があります。ポートの左側は スピード LED、右側はリンク / 二重 / アクティビティ LED です。

次の図は、PowerConnect 3524/P および PowerConnect 3548/P スイッチの 10/100 BaseT ポート LED を示しています。

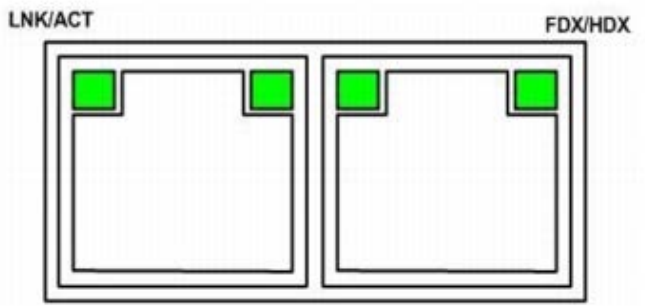
図 **2-6. RJ-45** 銅ベースの **10/100 BaseT LED**



PowerConnect 3524/P および PowerConnect 3548/P の RJ-45 100 Base-T ポートには LNK/ACT とマークが付いた 2 つの LED があります。

次の図は 100 Base-T LED を示しています。

図 **2-7 RJ-45 1000 Base-T LED**



次の表では、PowerConnect 3524 および PowerConnect 3548 用 RJ-45 LED の表示が説明されています。

表 **2-1 PowerConnect 3524** および **PowerConnect 3548** 用 **RJ-45 100 Base-T LED** の表示

LED	色	説明
リンク/アクティビティ/スピード	緑色の点灯	ポートは 100 Mbs で実行されています。
	緑色の点滅	ポートはデータを 100 Mbps で送信、または受信しています。
	橙色の点灯	ポートは 10 Mbs で実行されています。
	黄色の点滅	ポートは 10 Mbps でデータを送信または受信しています。
	オフ	ポートは現在動作していません。
FDX	緑色の点灯	ポートは現在全二重モードで動作しています。
	オフ	ポートは現在半二重モードで動作しています。

次の表では、PowerConnect 3524P および PowerConnect 3548P 用の RJ-45 LED の表示が説明されています。

表 **2-2 PowerConnect 3524P** および **PowerConnect 3548P** 用 **RJ-45** 銅ベース **100 Base-T LED** の表示

LED	色	説明
スピード/リンク/アクティビティ	緑色の点灯	ポートは現在 100 Mbps でリンクされています。
	緑色の点	ポートは現在 100 Mbps で動作しています。

	滅	
	オフ	ポートは現在 10 Mbps で動作しているか、リンクされていません。
FDX	緑色の点灯	パワードデバイス（PD）が検知され、通常のロードで動作しています。パワードデバイスの詳細に関しては、「パワーオーバーイーサネットの管理」を参照してください。
	緑色の点滅	ポートは移行モードで動作しています。PD を検知、または不具合が発生しています。 パワーオーバーイーサネットの詳細に関しては「パワーオーバーイーサネットの管理」を参照してください。
	橙色の点灯	パワードデバイスでオーバーロードが発生、またはショートしています。パワーオーバーイーサネットの障害の詳細に関しては、「パワーオーバーイーサネットの管理」を参照してください。
	橙色の点滅	パワードデバイスの消費電力が事前に定義された電力割り当てを超えています。パワーオーバーイーサネット電力割り当ての詳細に関しては、「パワーオーバーイーサネットの管理」を参照してください。
	オフ	パワードデバイスが検知されませんでした。

ギガビットポート **LED**

次の表では、ギガビット（スタッキングポート）LED について説明されています。

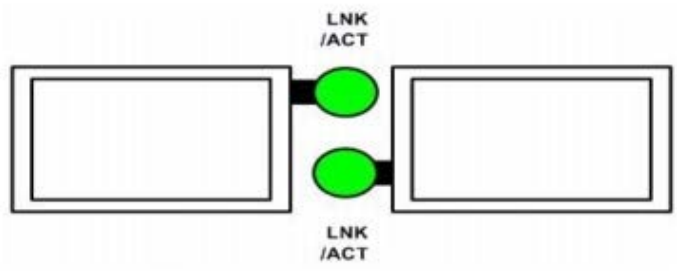
表 **2-3 PowerConnect 3524** および **PowerConnect 3548 RJ-45** 銅ベース **100 Base-T LED** の表示

LED	色	説明
リンク/アクティビティ/スピード	緑色の点灯	ポートは 1000 Mbs で実行されています。
	緑色の点滅	ポートはデータを 1000 Mbps で送信または受信しています。
	黄色の点灯	ポートは 10 または 100Mbs で実行されています。
	黄色の点滅	ポートは、10 または 100 Mbps でデータを送信または受信しています。
	オフ	ポートは現在動作していません。
FDX	緑色の点灯	ポートは現在全二重モードで動作しています。
	オフ	ポートは現在半二重モードで動作しています。

SFP LED

各 SFP ポートには、LNK/ACT と印が付いた LED が 1 つあります。PowerConnect 3524/P および PowerConnect 3548/P デバイスでは、LED はポート間にあり、丸い形になっています。次の図では、各デバイスの LED を示しています。

図 **2-8. SFP** ポート **LED**



SFP ポート LED の意味については次の表に示してあります。

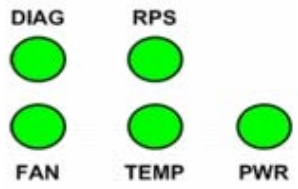
表 **2-4. SFP** ポート **LED** の意味

LED	色	説明
リンク/アクティビティ	緑色の点灯	リンクが確立されています。
	緑色の点滅	ポートは現在データを送信または受信しています。
	オフ	ポートは現在リンクされていません。

システム LED

PowerConnect 3524/P および PowerConnect 3548/P デバイスのシステム LED は、電源装置、ファン、温度状態および診断に関する情報を提供します。次の図は、システム LED を示しています。

図 2-9. システム LED



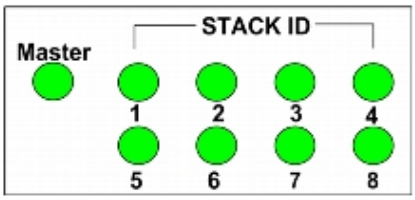
システム LED の意味については次の表に示してあります。

表 2-5. システム LED インジケータ

LED	色	説明
電源装置（PWR）	緑色の点灯	スイッチがオンになっています。
	オフ	スイッチがオフになっています。
冗長電源装置（RPS） （モデル：3524 および 3548）	緑色の点灯	RPS は現在動作中です。
	赤色の点灯	RPS に障害が発生しました。
	オフ	冗長電源装置は接続されていません。
冗長電源装置（RPS） （モデル：3524P および 3548P）	緑色の点灯	RPS は現在動作中です。
	オフ	冗長電源装置に障害が発生したか、接続されていません。
DIAG（診断）	緑色の点滅	現在システム診断テストを実行中です。
	緑色の点灯	システム診断テストは正常に終了しました。
	赤色の点灯	システム診断テストに失敗しました。
	オフ	システムは正常に動作しています。
TEMP（温度）	赤色の点灯	デバイスの温度が許容温度範囲を超えました。
	オフ	デバイスは許容温度範囲内で動作しています。
FAN（ファン）	緑色の点灯	すべてのデバイスファンは正常に動作しています。
	赤色の点灯	ひとつ、または複数のデバイスファンが動作していません。

スタッキング LED はスタック内のユニットの位置を示します。次の図は、前面パネルの LED を示しています。

図 2-10 スタッキング LED



スタッキング LED には 1～8 の番号が付いています。各スタッキングユニットにはそれぞれ LED ライトがひとつ点灯されており、ユニットの ID 番号を示しています。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	オフ	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 1～8（S1～S8）	緑色の点灯	デバイスはスタッキングユニット N として指定されています。
	オフ	デバイスはスタッキングユニット N として指定されていません。
スタッキングマスター LED	緑色の点灯	このデバイスはスタックマスターです。
	オフ	このデバイスはスタックマスターではありません。

電源

デバイスには内蔵電源装置ユニット（AC ユニット）、および PowerConnect 3524/P および PowerConnect 3548/P デバイスを PowerConnect EPS-470 ユニットに接続するコネクタ、または PowerConnect 3524 および PowerConnect 3548 デバイスを PowerConnect RPS-600 ユニットに接続するコネクタが搭載されています。PowerConnect 3524/P および PowerConnect 3548/P デバイスには内蔵電源装置（12 ボルト）が搭載されています。

両方の電源装置を使用した動作は、負荷共有によって調整されます。電源装置 LED は電源装置の状態を示します。

PowerConnect 3524/P および PowerConnect 3548/P デバイスは470 W（12 V/-48 V）の内蔵電源が搭載されており、24 ポート PoE デバイスでは合計 370 W を提供します

AC 電源装置

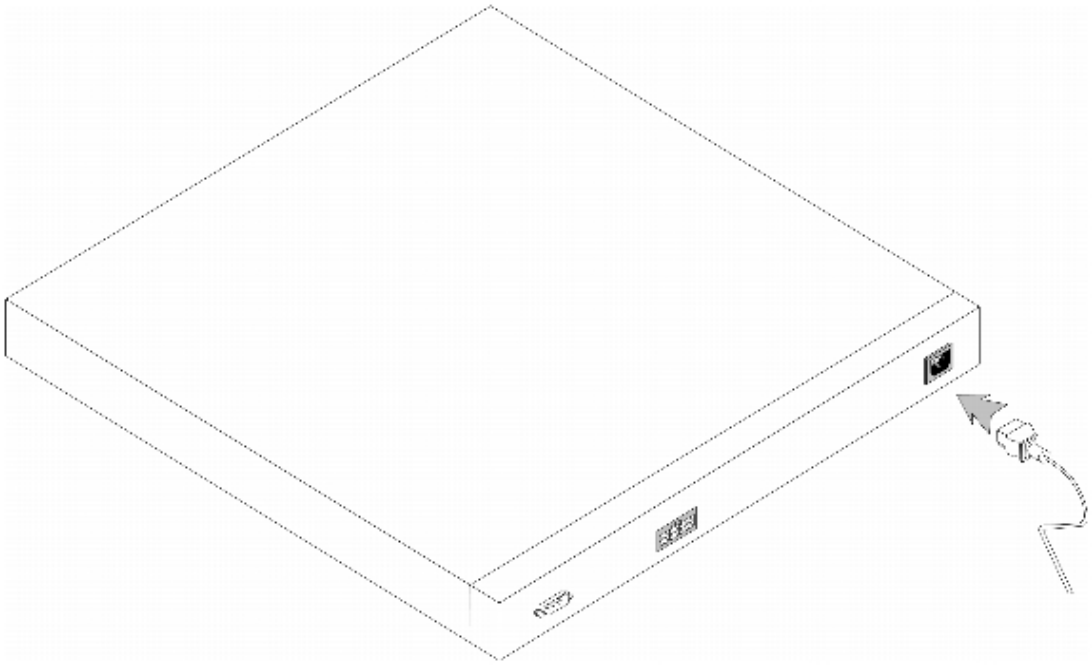
AC 電源装置は 90～264 VAC、47～63 Hz で動作します。AC 電源装置ユニットは標準コネクタを使用します。LED インジケータは前面パネルにあり、AC ユニットが接続されているかどうかを表示します。

DC 電源装置

PowerConnect 3524 および PowerConnect 3548 スイッチは外付けの RPS-600 ユニットに接続すると、冗長電源オプションを提供します。設定は必要ありません。前面パネル「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 の定義に関しては、表 2-5を参照してください。

PowerConnect 3524/P および PowerConnect 3548/P スイッチは外付けの EPS-470 ユニットに接続すると、冗長電源オプションを提供します。設定は必要ありません。前面パネル「RPS」LED は外付け EPS-470 が接続されているかどうかを表示します。RPS LED の定義に関しては、表 2-5を参照してください。

図 **2-11.** 電源の接続



デバイスを異なる電源に接続すると、電源異常による不具合が起こりにくくなります。

スタック **ID** ボタン

デバイスの前面パネルには、スタックマスターおよびメンバーのユニット ID を手動で選択するために使用するスタック ID ボタンがあります。

スタックマスターおよびメンバーは、デバイス起動後 15 秒以内に選択される必要があります。スタックマスターが 15 秒以内に選択されなかった場合、デバイスは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ユニット ID 1 または 2 を割り当てられます。ユニット 1 およびユニット 2 の両方が存在する場合、選択されていないユニットがバックアップマスターとして機能します。スタックメンバーには個別のユニット ID（3～8）が割り当てられます。例えば、スタック内に 4 つのユニットがある場合、マスターユニットは 1 または 2 になり、バックアップマスターはマスターユニットのユニット番号に応じて 1 か 2 のどちらかになります。3 番目のメンバーは 3、4 番目のスタックメンバーは 4 です。

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 がすでに選択されている場合、スタッキング LED が点灯しなくなるまでスタック ID ボタンを数回押します。

リセットボタン

PowerConnect 3524/P および PowerConnect 3548/P スイッチには前面パネルにリセットボタンがあり、デバイスを手動でリセットできます。マスターデバイスがリセットされると、全スタックがリセットされます。メンバーユニットのみがリセットされた場合は、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電源投入または低電圧状態でアクティブになります。

換気装置

PoE 機能付きの PowerConnect 3524/P および PowerConnect 3548/P スイッチには 5 つの内蔵ファンが搭載されています。非 PoE PowerConnect 3524 および PowerConnect 3548 デバイスには 2 つの内蔵ファンがあります。ひとつ、または複数のファンに不具合が発生している場合、LED を観察することで動作を確認できます。

目次に戻る

目次に戻る

PowerConnect 3524/P および PowerConnect 3548/P の取り付け

Dell™ PowerConnect™ 35xx システムユーザーズガイド

設置場所の準備

PowerConnect 3524/P および PowerConnect 3548/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。デバイスを設置する前に、設置場所が次の要件を満たしていることを確認します。

- 電源 — ユニットは容易にアクセスできる 100～240 VAC、50～60 Hz コンセントの近くに取り付けます。
- 一般 — 冗長電源装置（RPS）は、前面パネルの LED が点灯しているかをチェックして、正しく取り付けられているようにします。
- **PoE** モデル — 前面パネルの PoE LED が点灯していることをチェックして、RPS が取り付けられているようにします。
- スペース — オペレータが作業できるように正面に十分なスペースがあることを確認します。配線、電源接続、および換気用のスペースを確保します。
- ケーブル配線 — ケーブルは、無線送信機、ブロードキャスト増幅器、電線、および蛍光灯器具などの電気的雑音の原因となるものを避けて配線してください。
- 環境要件 — 動作時の周囲温度の許容範囲は、結露のない相対温度 10～90 % の環境で 0～45 ºC です。

開梱

パッケージの内容

デバイスを開梱し、次の部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
- ラック取り付け用のラックマウントキット、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： デバイスを開梱する前に、梱包を確認し、損傷がある場合はすぐにご連絡ください。

□□□ 平らで清潔な面に箱を置きます。

□□□ 箱を開けるか、箱のフタを取り外します。

□□□ デバイスを箱から慎重に取り出し、安全で清潔な場所に置きます。

□□□ すべての梱包材を取り外します。

□□□ デバイスとアクセサリに損傷がないかどうかを確認します。損傷がある場合は、すぐにご連絡ください。

デバイスの取り付け

以下の取り付け手順は、**PowerConnect 3524/P** および **PowerConnect 3548/P** デバイスに適用されます。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、背面パネルに配置されています。冗長電源装置（**RPS**）の接続はオプションですが、接続されることをお勧めします。**RPS** のコネクタは、デバイスの背面パネルにあります。

ラックへの取り付け

製品情報ガイドの安全情報および、スイッチに接続したりサポートする他のデバイスに関する安全情報を参照してください。

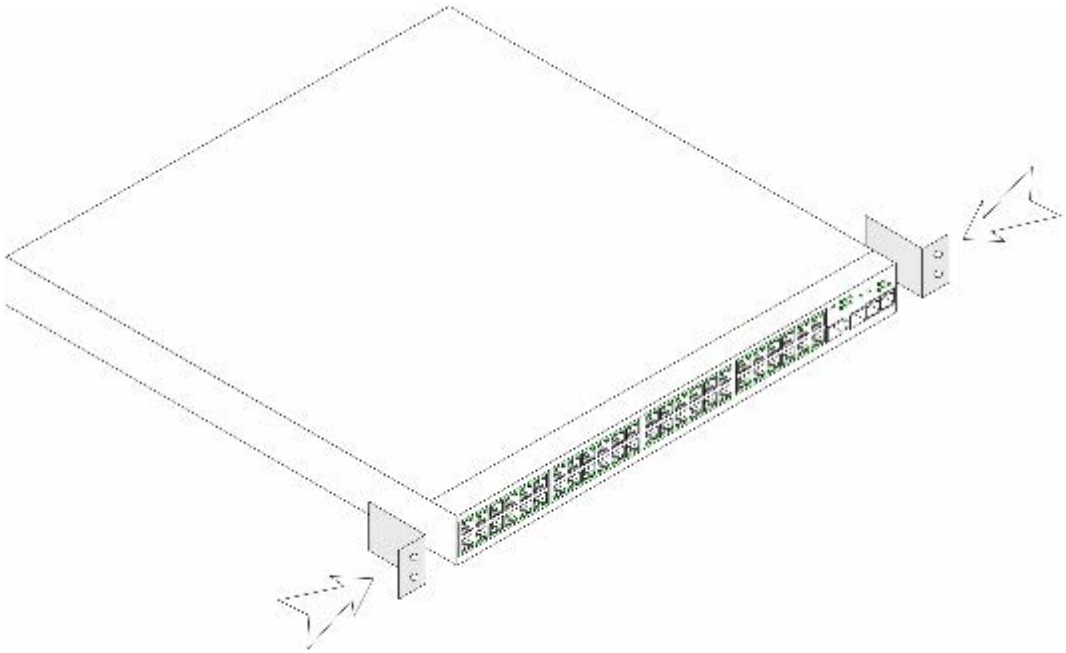
デバイスをラックまたはキャビネットに取り付ける前に、本体からすべてのケーブルを取り外してください。

ラックに複数のデバイスを取り付ける場合は、ラックの下から上へデバイスを順に取り付けてください。

□□□ 付属のラック取り付けブラケットを、デバイスの片方の側面に取り付けます。デバイスの取り付け穴がラック取り付けブラケットの取り付け穴と揃っていることを確認してください。

次の図は、ブラケットの取り付け位置を示しています。

図 **3-1.** ラックマウント用ブラケットの取り付け



□□□ 付属のネジをラック取り付け穴に挿入して、ドライバでネジを締めます。

□□□ 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片方の側面にも取り付けます。

□□□ デバイスを 48.26 cm（19 インチ）ラックに挿入します。デバイスのラック取り付け穴がラックの取り付け穴と揃っていることを確認してください。

□□□ デバイスをラックネジでラックに固定します（ラックネジは同梱されていません）。ラックに固定する際、先に下側のネジを締めてから上側のネジを締めます。通気孔が塞がれていないことを確認します。

水平面への設置

ラックに設置しない場合、デバイスは平らな面に設置する必要があります。設置する面は、デバイスとデバイスケーブルの重量に耐えられなければなりません。

□□□ シャーシ底面の印の付いた各位置に、粘着ゴムパッドを取り付けます。

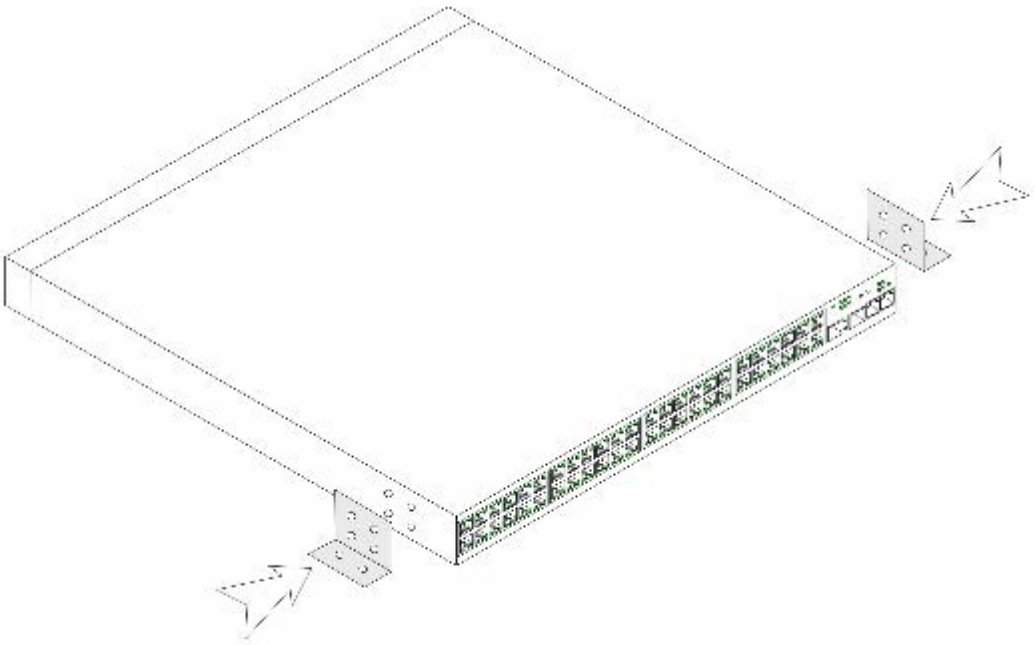
□□□ 左右の側面に 5.08 cm、背面に 12.7 cm のスペースをとって、デバイスを平らな面に設置します。

□□□ デバイスの通気孔がふさがれていないことを確認します。

デバイスの壁面への取り付け

□□□ 付属の壁面設置用ブラケットを、デバイスの片方の側面に取り付けます。デバイスの取り付け穴がラック取り付けブラケットの取り付け穴と揃っていることを確認してください。次の図は、ブラケットの取り付け位置を示しています。

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取り付け穴に挿入して、ドライバでネジを締めます。

□□□ この手順を繰り返して、壁面設置用ブラケットをデバイスのもう片方の側面にも取り付けます。

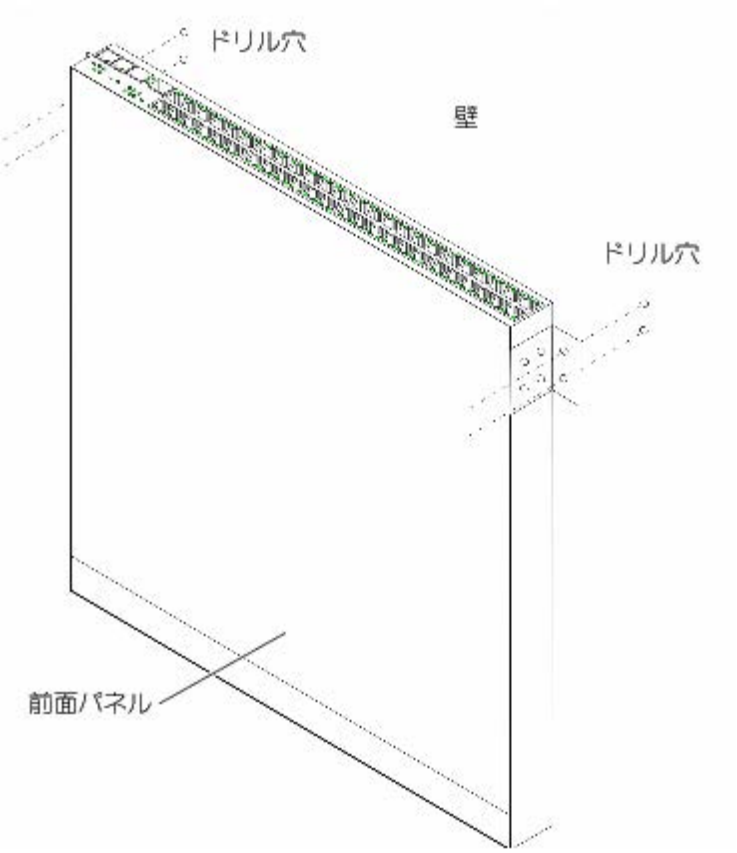
□□□ デバイスを取り付ける壁面の位置にデバイスを合わせます。

□□□ 壁面のデバイスを固定するネジ穴を設ける位置に印をつけます。

□□□ 印を付けた位置にドリルで穴を開け、すべての穴にプラグ（含まれていません）を差し込みます。

□□□ ユニットをネジ（含まれていません）で壁に固定します。通気孔が塞がれていないことを確認します。

図 **3-3.** 壁面へのデバイスの取り付け



ターミナルへの接続

□□□ ASCII ターミナル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システムのシリアルコネクタに、RS-232 クロスケーブルを接続します。

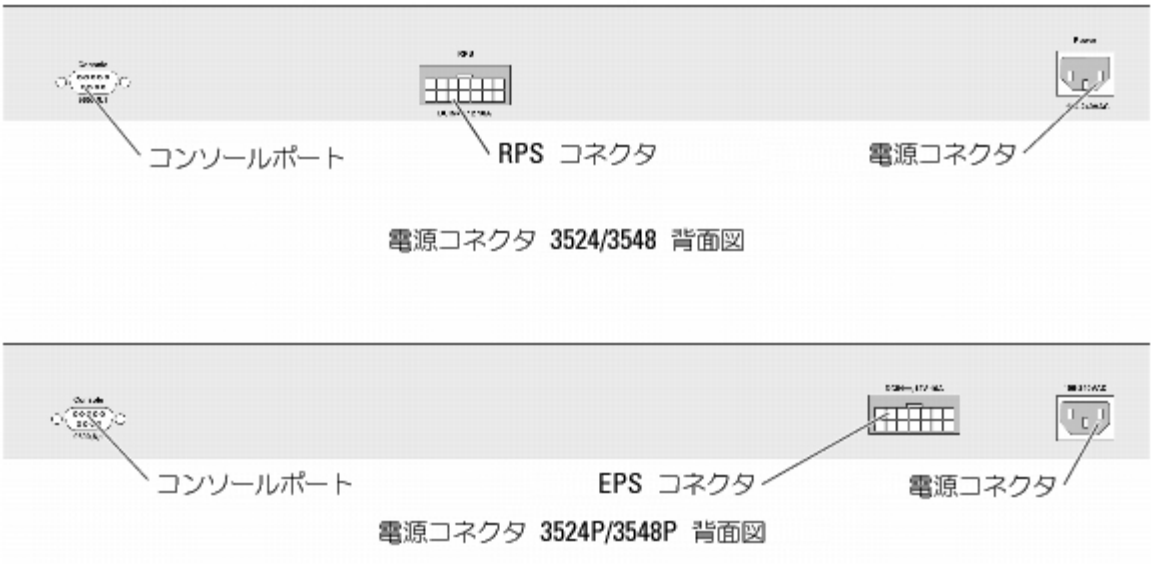
□□□ ケーブルのもう一方の端の DB-9 メスコネクタを、デバイスのシリアルポートコネクタに接続します。

デバイスと電源装置の接続

付属の AC 電源ケーブルは、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、電源ケーブルをアースされた AC コンセントに接続しないでください。デバイスの電源への接続は、デバイスの起動および設定の項で詳述する手順に従って行ってください。

図 **3-4.** 背面パネル電源コネクタ



デバイスを電源に接続したら、デバイスが正しく接続され、動作していることを前面パネルの LED で確認してください。

スタックの取り付け

概要

各デバイスはスタンドアロンデバイス、またはスタックのメンバーとして動作することができます。スタックごとに最高 8 台のデバイス、または最高 384 個のポートをサポートします。

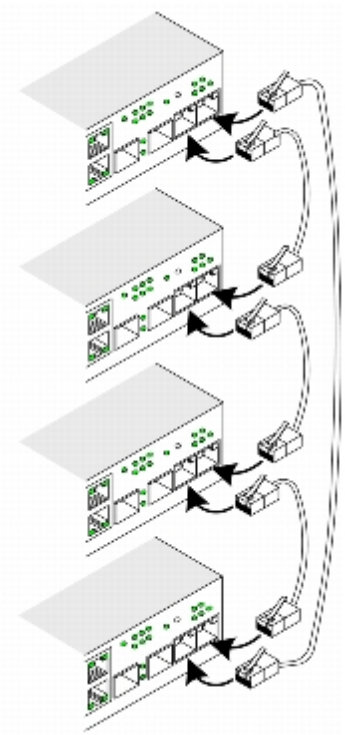
すべてのスタックにはマスターユニットが必要で、マスターバックアップユニットを加えることも出来ます。他のデバイスはメンバーとしてスタックに接続します。

PowerConnect 35xx シリーズシステムスイッチのスタッキング

各 PowerConnect 35xx シリーズシステムスタックには 1 台のマスターユニットがあり、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。残りのユニットはスタッキングメンバーとみなされます。

PowerConnect 35xx シリーズシステムスイッチは、スタッキングに RJ-45 ギガビットイーサネットポート（G3 および G4）を使用します。これは、デバイスにアクセサリを追加することなくスタッキングの追加機能を可能にします。デバイスをスタッキングするには、スタック最上部のデバイスのポート G3 、およびスタック内でそのすぐ下にあるデバイスのポート G4 に標準カテゴリ 5 ケーブルを差し込みます。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。

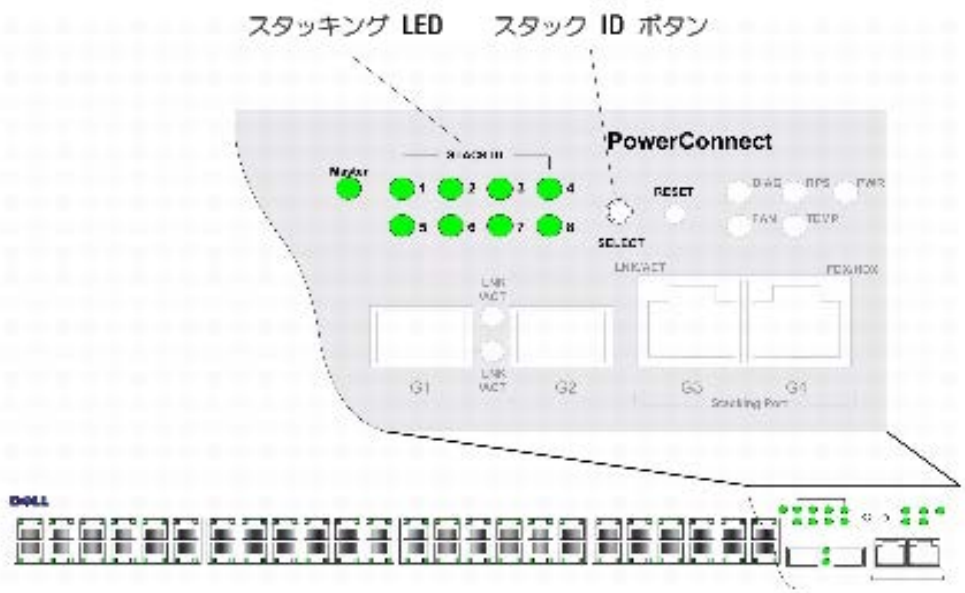
図 **3-5.** スタックのケーブル配線図



メモ： スタッキングモードでは、G3 および G4 として指定されたポートは EWS には表示されませんが、デバイスに影響はありません。これは、ポートがスタッキング用に異なるインデックスを受け取るからです。

スタックユニットの識別は、デバイス前面パネルのスタックID ボタンを使用して実行します。

図 **3-6.** スタッキング構成および識別パネル



各スタックデバイスには固有の識別用ユニット ID があり、デバイスのスタック内の位置および機能を定義します。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。デフォルトの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され、スタック ID は LED によって表示されます。ユニット ID 1 と 2 はマスターおよびバックアップマスターユニット用に予約され、ユニット ID 3 ～8 はメンバーユニット用に予約されます。

ユニット ID の選択過程

ユニット ID の選択過程は次の通りです。

□□□ スタンドアロン / マスターデバイスのコンソールポートと 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が、RS-232 クロスケーブルで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 電源ソケットを無効にします。

□□□ デバイスを AC 電源ソケットに接続します。

□□□ AC 電源ソケットを有効にします。

電源を投入すると、設定された LED 番号（保存されているユニット ID に対応）が点滅を始めます。LED は 15 秒間点滅します。この期間中、適切なスタック ID LED が点灯するまでスタック ID ボタンを押すことでスタック ID を選択します。

□□□ 選択過程 — スタッキング ID ボタンを押し続けると、LED 番号が進みます。 LED 8 が点滅している時にスタック 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。 スタック ID ボタンを再度押すとスタック ID が 1 に進みます。ユニット 1 および 2 はマスター設定可能のユニットです。スタッキングの概要のマスターの選択過程を参照してください。

□□□ 選択過程の終了 — ユニット ID の選択過程は 15 秒間の点滅時間が経過すると完了します。スタック ID ボタンが無反応になり、ユニット ID が過程最後の LED ID 点滅に設定されます。

メモ： これらの手順は、すべてのスタックメンバーに電源が投入され、スタック ID が選択されるまで、各ユニットごとに実行する必要があります。ひとつのユニットごとに手順を行うと、各ユニットに対するスタック ID を選択するための十分な時間を取る事が出来ます。ただし、デバイスに電源投入する前にスタック全体をスタックのケーブル配線図の通りに配線されている必要があります。

デバイスの起動および設定

外部接続がすべて完了したら、ターミナルをデバイスに接続し、デバイスの設定を行います。追加詳細機能の実行に関しては、詳細設定の項に説明されています。

メモ： 手順を開始する前に、この製品のリリースノートを読んでください。リリースノートは、デルサポートサイト **support.dell.com** からダウンロードしてください。

メモ： デルサポートサイト **support.jp.dell.com** からユーザーマニュアルをダウンロードされることをお勧めします。

デバイスへの接続

デバイスを設定するには、デバイスをコンソールに接続する必要があります。ただし、デバイスがスタックの一部である場合は、スタック中のマスターユニットと呼ばれるデバイスのみをターミナルに接続してください。スタックは単一のデバイスとして機能するため、マスターユニットのみが設定されます。

ターミナルとデバイスの接続

デバイスには、デバイスをモニタし設定するために、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デスクトップシステムに接続可能なコンソールポートが搭載されています。このコンソールポートコネクタは DB-9 オスコネクタで、DTE（Data Terminal Equipment）コネクタとして実装されています。

コンソールポートを使用するには、次のものが必要です。

- VT100 互換のターミナルまたはデスクトップ、もしくは 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搭載のノートブック
- コンソールポート用の DB-9 メスコネクタ、およびターミナル用の適切なコネクタが付いている RS-232 クロスケーブル

デバイスのコンソールポートにターミナルを接続するには、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（シリアルポート 1 またはシリアルポート 2）を選択します。

□□□ 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。

□□□ フロー制御をなしに設定します。

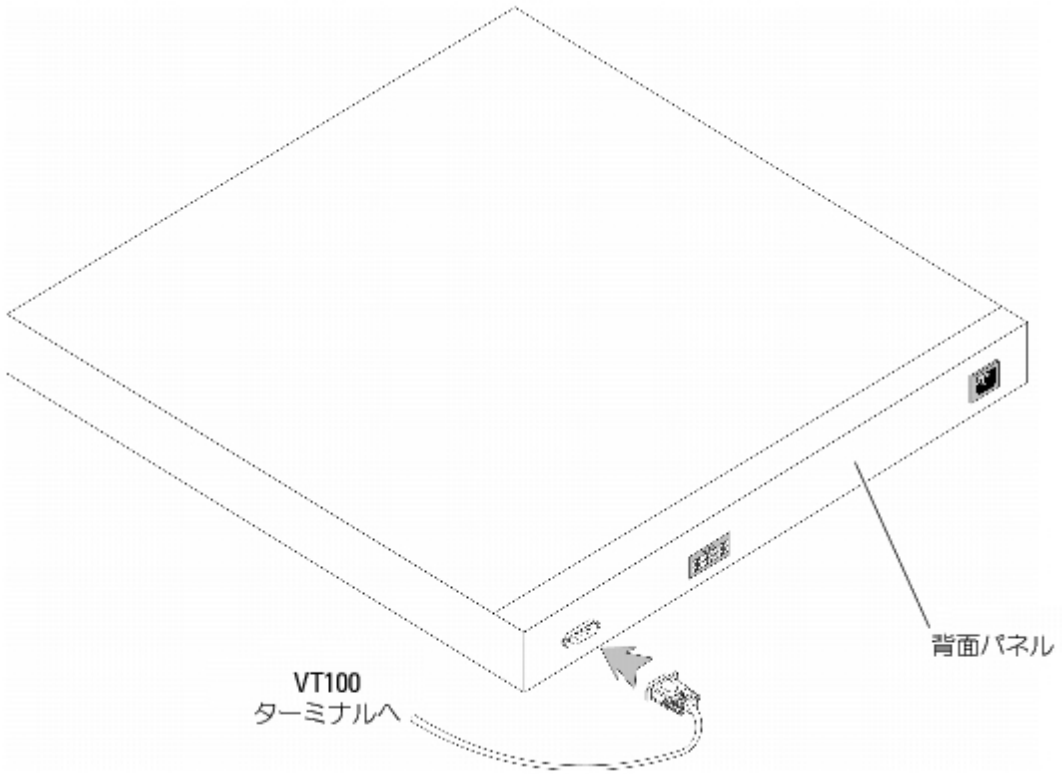
□□□ Properties（プロパティ）で、VT100 for Emulation（VT100 のエミュレーション）モードを選択します。

□□□ Function key（ファンクションキー）、Arrow key（矢印キー）、および Ctrl key（Ctrl キー）として使用する Terminal keys（ターミナルキー）を選択します。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てください。

△ 注意： **Microsoft® Windows® 2000** でハイパーターミナルを使用する場合、**Windows 2000 Service Pack 2** またはそれ以降がインストール済みであ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 **Service Pack** に関しては、**www.microsoft.com/japan** を参照してください。

□□□ RS-232 クロスケーブルのメスコネクタをマスターユニットまたは、スタンドアロンデバイスのデバイスコンソールポートに直接接続し、固定ねじを締めます。PowerConnect 35xx シリーズシステムコンソールポートは背面パネルにあります。

図 **3-7 PowerConnect 35xx** シリーズシステム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ユニットのコンソールポートすべてに接続できますが、スタック管理はスタックマスター（ユニット ID 1 または 2）からのみ実行可能です。

目次に戻る

目次に戻る

PowerConnect 3524/P および 3548/P の設定

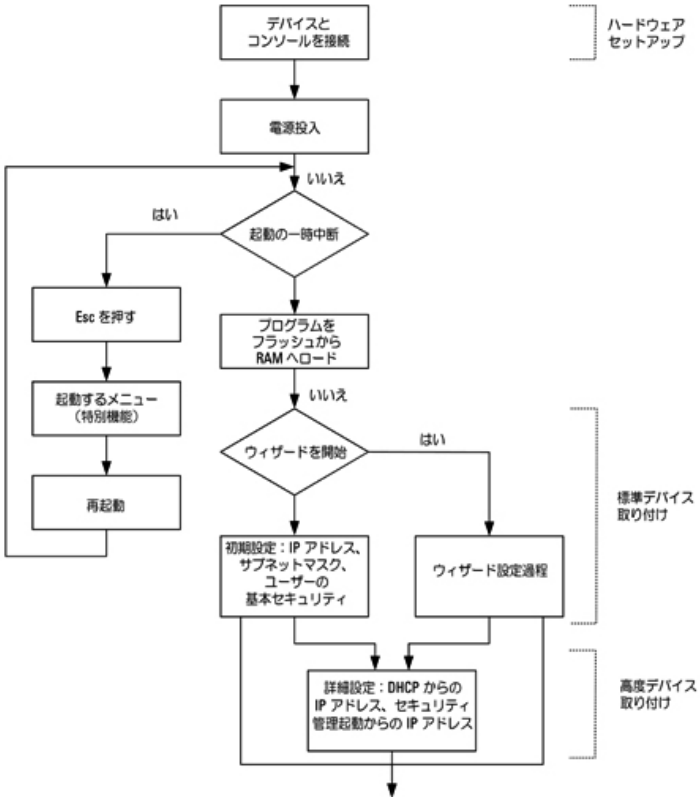
Dell™ PowerConnect™ 35xx システムユーザーズガイド

設定手順

すべてのデバイスの外付け接続が完了したら、起動やその他手順を監視するため、ターミナルをデバイスに接続します。取り付けおよび設定手順の順序は、次の図に示されています。

メモ： 手順を開始する前に、この製品のリリースノートを読んでください。**support.jp.dell.com** からリリースノートをダウンロードしてください。

図 **4-1.** インストールと設定の流れ



スイッチの起動

ローカルターミナルが接続された状態で電源をオンにした場合、スイッチでは POST（Power-On Self-Test）が実行されます。POST はデバイスを取り付けるたびに実行されます。POST ではハードウェアコンポーネントがチェックされ、起動が完了する前にデバイスが完全に動作可能な状態かどうかが確認されます。重大な問題が検出された場合は、プログラムフローの実行が停止します。POST が正常に終了した場合は、有効な実行可能イメージが RAM にロードされます。ターミナルに POST のメッセージが表示され、テストの成功または失敗を示します。

起動プロセスの実行には約 30 秒かかります。

初期設定

メモ： 手順を開始する前に、この製品のリリースノートを読んでください。リリースノートは、デルサポートサイト **support.dell.com** からダウンロードしてください。

メモ： 初期設定では、次のことを前提とします。

- PowerConnect デバイスが以前に一度も設定されたことがなく、出荷時と同じ状態である。

- PowerConnect デバイスの起動が正常に終了した。
- コンソール接続が確立されており、VT100 ターミナルデバイスの画面にコンソールプロンプトが表示されている。

デバイスの初期設定は、コンソールポート経由で行われます。初期設定が終了したら、デバイスは、接続済みのコンソールポートから管理するか、または初期設定中に指定したインタフェース経由でリモートから管理することができます。

デバイスを初めて起動した場合、またはデバイスが設定されていないために設定ファイルが空の場合、ユーザーはセットアップウィザードを使用するよう求められます。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うと、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： デバイスの設定を行う前に、ネットワーク管理者から次の情報を入手してください。

- デバイスの管理に使用する VLAN 1 インタフェースに割り当てられる IP アドレス（デフォルトでは、すべてのポートが VLAN 1 のメンバーです）
- このネットワーク用の IP サブネットマスク
- デフォルトルートを設定するための、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 コミュニティ文字列および SNMP 管理システムの IP アドレス（オプション）
- ユーザー名およびパスワード

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うと、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では、次のフィールドを設定します。

- SNMP コミュニティ文字列および SNMP 管理システムの IP アドレス（オプション）
- ユーザー名およびパスワード
- 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

次のメッセージが表示されます。

`Welcome to Dell Easy Setup Wizard`（`Dell` イージーセットアップウィザードへようこそ）

`The Setup Wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible.`（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うと、すぐに動作可能な状態にすることができます。）`You can skip the setup wizard, and enter CLI mode to manually configure the switch.`（セットアップウィザードを省略し、`CLI` モードでスイッチを手動で設定することも可能です。）
`The system will prompt you with a default answer; by pressing enter, you accept the default.`（システムはデフォルトの応答を表示します。`Enter` を押すとデフォルトを受け入れることになります。）
`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.`（セットアップウィザードを実行するには、次の質問に `60` 秒以内に応答する必要があります。そうしない場合、システムはデフォルトのシステム設定を使用して通常の操作を続行します。）

`Would you like to enter the Setup Wizard (you must answer this question within 60 seconds?`（セットアップウィザードを開始しますか。（`60` 秒以内にこの質問に応答する必要があります））（`Y/N`）`[Y]Y`
`You can exit the Setup Wizard at any time by entering [ctrl+Z].`（`[ctrl+Z]` を押すと、いつでもセットアップウィザードを終了できます。）

`[N]` を入力すると、セットアップウィザードは終了します。`60` 秒以内に何も入力しないと、セットアップウィザードは自動的に終了して、`CLI` コンソールプロンプトが表示されます。

`[Y]` を入力すると、セットアップウィザード によって、デバイスの初期設定が終了するまで対話型の案内が表示されます。

メモ： `60` 秒以内に何も入力せず、ネットワーク上に `BootP` サーバーが存在する場合は、`BootP` サーバーからアドレスを取得します。

メモ： `[ctrl+z]` を押すと、いつでもセットアップウィザードを終了できます。

ウィザード手順 1

次のメッセージが表示されます。

`The system is not setup for SNMP management by default.`（システムはデフォルトで `SNMP` 管理用に設定されていません。）
`To manage the switch using SNMP (required for Dell Network Manager) you can` (`SNMP` を使用してスイッチを管理するには（`Dell Network Manager` に必要）、次の方法があります。）

- `Setup the initial SNMP version 2 account now.`（初期 `SNMP` バージョン `2` を設定する。）
- `Return later and setup additional SNMP v1/v3 accounts.`（あとで追加の `SNMP v1/v3` アカウントを設定する。）

`For more information on setting up SNMP accounts, please see the user documentation.`（`SNMP` アカウントの設定の詳細に関しては、ユーザーマニュアルを参照してください。）

`Would you like to setup the SNMP management interface now?`（`SNMP` 管理インタフェースを設定しますか。）（`Y/N`）`[Y]Y`

省略して手順 2 に進む場合は、`[N]` を入力します。

セットアップウィザード を続行する場合は、`[Y]`を入力します。次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.`（`SNMP` 管理アカウントを設定するには、特定の管理システムがスイッチにアクセスす

るために使用する管理システムの IP アドレスと「コミュニティ文字列」またはパスワードを指定する必要があります。）The wizard automatically assigns the highest access level [Privilege Level 15] to this account.（ウィザードはこのアカウントに、最高のレベルである[権限レベル 15]を自動的に割り当てます。）
You can use Dell Network Manager or CLI to change this setting、and to add additional management systems.（Dell Network Manager または CLI を使用してこの設定を変更したり、管理システムを追加することもできます。）For more information on adding management systems、see the user documentation.（管理システムの追加に関する詳細はユーザーマニュアルを参照してください。）
To add a management station（管理ステーションを追加するには）:
Please enter the SNMP community string to be used:（使用する SNMP コミュニティ文字列を入力してください。）[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:（管理システムの IP アドレス（A.B.C.D）を入力してください。または、任意の管理ステーションから管理する場合はワイルドカード（0.0.0.0）を入力してください。）[0.0.0.0]

次の項目を入力します。

- SNMP コミュニティ文字列（Dell_Network_Manager など）
- 管理システムの IP アドレス（A.B.C.D）、または、任意の管理ステーションから管理する場合はワイルドカード（0.0.0.0）

メモ： ゼロで始まる IP アドレスおよび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

次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.（初期権限（レベル 15）のユーザーアカウントを設定する必要があります。）
This account is used to login to the CLI and Web interface.（このアカウントは、CLI およびウェブインタフェースのログインに使用されます。）
You may setup other accounts and change privilege levels later.（後で他のアカウントの設定および権限レベルの変更ができます。）
For more information on setting up user accounts and changing privilege levels、see the user documentation.（ユーザーアカウントの設定および権限レベルの変更に関する詳細はユーザーマニュアルを参照してください。）
To setup a user account（ユーザーアカウントを設定するには）:
Enter the user name（ユーザー名を入力してください）<1-20>:[admin]
Please enter the user password（ユーザーパスワードを入力してください）:*
Please reenter the user password（ユーザーパスワードを再入力してください）:*

次の項目を入力します。

- ユーザー名（「admin」など）
- パスワードおよびパスワードの確認

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

次のメッセージが表示されます。

Next、an IP address is setup.（次に IP アドレスを設定します。）

The IP address is defined on the default VLAN（VLAN #1）、of which all ports are members.（IP アドレスはデフォルトの VLAN（VLAN #1）上で定義されます。VLAN のすべてのポートがメンバーです。）This is the IP address you use to access the CLI、Web interface、or SNMP interface for the switch.To setup an IP address:（これは、スイッチの CLI、Web インタフェース、または SNMP インタフェースへのアクセスに使用する IP アドレスです。IP アドレスを設定するには、次の項目を入力します。）

Please enter the IP address of the device（A.B.C.D）（デバイスの IP アドレスを入力してください（A.B.C.D））:[1.1.1.1]

Please enter the IP subnet mask（A.B.C.D or nn）（IP サブネットマスクを入力してください（A.B.C.D または nn））: [255.255.255.0]

IP アドレスおよび IP サブネットマスクを入力します（例：IP アドレスとして 1.1.1.1、IP サブネットマスクとして 255.255.255.0）。

Enter を押します。

ウィザード手順 4

次のメッセージが表示されます。

Finally、setup the default gateway.（最後に、デフォルトゲートウェイを設定します。）
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）（このネットワークに到達できるゲートウェイの IP アドレスを入力してください（例：192.168.1.1）。デフォルトゲートウェイ（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。次のように表示されます（上記のパラメータ例を入力した場合）。

```
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

次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. (この情報が正しい場合は（Y）を選択して設定を保存し、起動設定ファイルにコピーします。) If the information is incorrect, select (N) to discard configuration and restart the wizard: (情報が正しくない場合は、（N）を選択して設定を破棄し、ウィザードを再スタートしてください。) (Y/N) [Y]Y
```

省略してセットアップウィザード を再スタートする場合は、[N] を入力します。

セットアップウィザード を完了する場合は、[Y]を入力します。次のメッセージが表示されます。

```
Configuring SNMP management interface (SNMP 管理インタフェースを設定しています)
Configuring user account (ユーザーアカウントを設定しています) ......
Configuring IP and subnet (IP およびサブネットを設定しています) ......

Thank you for using Dell Easy Setup Wizard. (Dell イージーセットアップウィザードをご利用いただきありがとうございました。) You will now enter CLI mode. (CLI モードに入ります。)
```

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、認証、権限、およびアカウンティング（AAA：Authentication、Authorization、Accounting）メカニズムに基づいた、IP アドレスの動的割り当てとセキュリティ管理について説明し、次のトピックが含まれます。

- 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
- セキュリティ管理およびパスワードの設定

DHCP および BOOTP を介して IP アドレスを設定または取得する場合、これらのサーバーから受信する設定値には IP アドレスと、場合によってはサブネットマスクおよびデフォルトゲートウェイが含まれます。

DHCP サーバーからの IP アドレスの取得

DHCP プロトコルを使って IP アドレスを回復する場合、デバイスは DHCP クライアントとして機能します。デバイスをリセットすると、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 アドレスを取得するには、次の手順を実行します。

□□□ IP アドレスを回復するには、任意のポートを選択し、DHCP サーバーまたは DHCP サーバーが属するサブネットに接続します。

□□□ 次のコマンドを入力し、選択したポートを使って IP アドレスを取得します。次の例のコマンドは、設定に使用したポートタイプに基づいています。

- ダイナミック IP アドレスの割り当て

  ```
  console# configure
  console(config)# interface ethernet 1/e1
  console(config-if)# ip address dhcp hostname powerconnect
  console (config-if) # exit
  console(config)#
  ```

- ダイナミック IP アドレスの割り当て（VLAN の場合）：

  ```
  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取得します。

□□□ IP アドレスを確認するには、次の例のとおりにシステムプロンプトに **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 サーバーから IP アドレスを回復するために、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場合は、同一の DHCP サーバーに接続するインタフェースで DHCP を有効にする命令コードを含む設定ファイル、または設定がまったく同一の設定ファイルは使用しないでください。そのような設定ファイルをコピーすると、デバイスは新規の設定ファイルを回復し、そこから起動するので、新規の設定ファイルの指示どおりに DHCP が有効になり、DHCP から同じファイルを再ロードするように指示されます。

メモ： DHCP IP アドレスを設定した場合、このアドレスは動的に回復され、**ip address dhcp** コマンドが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、バックアップが DHCP アドレスを回復しようと再度試みます。これは次の項目の原因となります。

- 同じ IP アドレスが割り当てられる。
- 異なる IP アドレス が割り当てられるが、管理ステーションとの接続を失う原因となる。
- DHCP サーバーがダウンし、IP アドレス回復の失敗、および管理ステーションとの接続を失う原因となる。

BootP サーバーからの IP アドレスの取得

標準の BootP プロトコルがサポートされており、デバイスでは、ネットワーク内の標準の BootP サーバーから IP ホスト設定ファイル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機能します。

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。

□□□ IP アドレスを取得するには、任意のポートを選択し、BootP サーバーまたは BootP サーバーが属するサブネットに接続します。

□□□ 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 起動設定を削除します。

デバイスは設定なしで再起動し、60 秒以内に BootP 要求の送信を始めます。デバイスは、IP アドレスを自動的に取得します。

メモ： デバイスの再起動が始まってから、ASCII ターミナルまたはキーボードで何らかの入力を行うと、BootP プロセスが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 アドレスを取得しません。

次の例はそのプロセスを示しています。

```
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. (このコマンドはシステム全体をリセットし、現在のセッションを終了します。) Do you want to continue (続行しますか) (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。

この時点で、デバイスに IP アドレスが設定されています。

セキュリティ管理およびパスワード設定

システムセキュリティは、ユーザーのアクセス権、特権、および管理方法を管理する AAA（Authentication、Authorization、Accounting）メカニズムによって処理されます。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を使用します。データ暗号化は、SSH メカニズムによって処理されます。

システムの出荷時には、デフォルトパスワードは設定されていません。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が分からなくなった場合は、スタートアップ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にのみ適用でき、ローカルターミナルからパスワードを入力せずに 1 度だけデバイスにアクセスできます。

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、次のサービスに対して設定できます。

- ターミナル
- Telnet
- SSH
- HTTP
- HTTPS

メモ： すべての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場合、デフォルトの優先度は **1** になります。この優先度にはアクセスは許可されますが、設定の権限はありません。デバイスに対するアクセス権と設定権を有効にするには、優先度 **15** を設定する必要があります。ユーザー名には、パスワードなしで特権レベル **15** を割り当てることもできますが、常にパスワードを割り当てることをお勧めします。パスワードが指定されていない場合、特権を持つユーザーは、任意のパスワードでウェブインタフェースにアクセスできます。

メモ： パスワードのエイジアウト、またはパスワードの期限切れを強制するパスワード管理コマンドを使用することによって、パスワードをセキュアすることができます。詳細に関しては、セキュリティ管理およびパスワード設定を参照してください。

初期ターミナルパスワードの設定

初期ターミナルパスワードを設定するには、次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通じてはじめてデバイスにログオンする際は、パスワードプロンプトに `george` と入力します。
- デバイスのモードを有効に変更する際は、パスワードプロンプトに `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、次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 セッションを通じてはじめてデバイスにログオンする際は、パスワードプロンプトに `bob` と入力します。
- デバイス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、次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 セッションを通じてはじめてデバイスにログオンする際は、パスワードプロンプトに `jones` と入力します。
- デバイス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、次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、次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 セッションを使用できるように設定する場合は、ターミナル、Telnet、または SSH セッションの設定をする時に、次のコマンドを 1 度入力します。

メモ： ウェブブラウザでページコンテンツを表示するには、SSL 2.0 またはそれ以上のバージョンを有効にしてください。

```
console(config)# crypto certificate generate key_generate
console(config)# ip https server
```

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

メモ： HTTP および HTTPS サービスではレベル 15 のアクセス権が要求され、設定レベルのアクセスに直接接続します。

ログインバナーの設定

次の 3 種類のログインバナーを定義できます。

- **Message-of-the-Day**（本日のメッセージ）バナー：ユーザーがログインする前にデバイスに接続すると表示されます。
- **Login**（ログイン）バナー：Message-of-the-Day（本日のメッセージ）バナーを表示してから、ユーザーがログインするまで表示されます。
- **Exec**（実行）バナー：すべての特権レベルおよびすべての認証方法で正常にログインすると表示されます。

ログインバナーの表示および設定を行うには、次のコマンドを入力します。

```
console# banner motd Welcome
console# show banner motd
console# banner login Please log in
console# show banner login
console# banner exec Successfully logged in
console# show banner exec
```

スタートアップの手順

スタートアップメニューの手順

Startup（スタートアップ）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、およびパスワードのリカバリがあります。診断手順はテクニカルサポート担当者専用のみであり、文書では公開されていません。

デバイスの起動時にスタートアップメニューに入ることができます。これには、POST テストの直後のユーザー入力が必要です。

Startup（スタートアップ）メニューに入るには、次の手順を実行します。

□□□ 電源を入れ、自動起動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-xxxx 14:46:49
Ryan board、based on PPC8247
128 MByte SDRAM. I-Cache 16 KB. D-Cache 16 KB. Cache Enabled.
Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

□□□ 自動起動メッセージが表示されたら、**<Enter>** を押して Startup（スタートアップ）メニューに入ります。Startup（スタートアップ）メニューの手順を実行するには、ASCII ターミナルまたは Windows ハイパーターミナルを使用します。

```
[1] Download Software
[2] Erase Flash File
```

```
[3] Password Recovery Procedure
[4] Enter Diagnostic Mode
[5] Set Terminal Baud-Rate
[6] Back
```

次の項では、使用可能な **Startup**（スタートアップ）メニューのオプションについて説明します。

メモ： スタートアップメニューの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。すなわち、**35** 秒（デフォルト）以内に選択しないと、デバイスがタイムアウトになります。このデフォルト値は **CLI** を介して変更できます。

メモ： **Diagnostics**（診断）モード（オプション**[4]**）を操作できるのはテクニカルサポート担当者だけです。このため、本書では **Diagnostics**（診断）モードの実施については説明していません。

ソフトウェアのダウンロード **-** オプション **[1]**

新規のバージョンをダウンロードして、破壊されたファイルを交換したり、システムソフトウェアをアップデートまたはアップグレードする必要がある場合に、ソフトウェアのダウンロード手順を実行します。**Startup**（スタートアップ）メニューからソフトウェアをダウンロードするには次を実行します。

□□□ **Startup**（スタートアップ）メニューで **[1]** を入力します。 次のプロンプトが表示されます。

```
Downloading code using XMODEM
****************************************************************
*** Running SW Ver. 21_08 Date 21-Aug-xxxx Time 17:22:25 ***
****************************************************************
HW version is 00.00.00
Base Mac address is: 00:14:47:78:89:96
Dram size is : 128M bytes
Dram first block size is : 102400K bytes
Dram first PTR is : 0x1800000
Dram second block size is : 4096K bytes
Dram second PTR is : 0x7C00000
Flash size is: 16M
01-Jan-xxxx 01:01:07 %CDB-I-LOADCONFIG: Loading running configuration.
01-Jan-xxxx 01:01:07 %CDB-I-LOADCONFIG: Loading startup configuration.
Device configuration:
CPLD revision: 1.01
Slot 1 - PowerConnect 35xx HW Rev. 1.1
-------------------------------------
-- Unit Standalone--
-------------------------------------
Tapi Version: v1.3.3.1
Core Version: v1.3.3.1
01-Jan-xxxx 01:01:19 %INIT-I-InitCompleted: Initialization task is completed
01-Jan-xxxx 01:01:19 %SNMP-I-CDBITEMSNUM: Number of running configuration items loaded: 0
01-Jan-xxxx 01:01:19 %SNMP-I-CDBITEMSNUM: Number of startup configuration items loaded: 0
01-Jan-xxxx 01:01:20 %Box-I-SFP-PRESENT-CHNG: unit_id 1 SFP 0 status is not present.
01-Jan-xxxx 01:01:20 %Box-I-SFP-PRESENT-CHNG: unit_id 1 SFP 1 status is not present.
```

□□□ ハイパーターミナルを使用する場合は、ハイパーターミナルのメニューバーで **Transfer**（転送）をクリックします。

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

□□□ **protocol**（プロトコル）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。

□□□ 送信を押します。ソフトウェアがダウンロードされます。

メモ： ソフトウェアのダウンロードが終了すると、デバイスが自動的に再起動します。

フラッシュファイルの消去 **-** オプション **[2]**

場合によっては、デバイス設定を消去する必要があります。設定を消去した場合には、**CLI**、**EWS**、または **SNMP** を介して設定したすべてのパラメーターを再設定する必要があります。

デバイス設定を消去するには次を実行します。

□□□ スタートアップ メニューで 2 秒以内に[2]を入力し、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.（警告! フラッシュファイルが削除されようとしています。）
Are you sure（よろしいですか）（Y/N）? y
```

□□□ 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.）（フラッシュファイル名（最高 8 文字。なしの場合は Enter。））:config
File config（if present）will be erased after system initialization （ファイル名 config（ある場合）はシステム初期化の後で削除されます）
======== Press Enter To Continue（Enter を押して続行します）========
```

□□□ フラッシュファイルの名前として config と入力します。設定が消去されて、デバイスが再起動します。

□□□ デバイスの初期設定を繰り返します。

パスワードのリカバリ - オプション [3]

パスワードが分からなくなった場合は、Startup（スタートアップ）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。この手順では、パスワードを使用せずに 1 度だけデバイスにログオンすることができます。

ローカルターミナルへ入る時にのみ、失ったパスワードをリカバリするには、次の手順を実行します。

□□□ Startup（スタートアップ）メニューで [3] を入力し、**<Enter>** を押します。パスワードが削除されます。

```
選択を入力するか、ESC を押して終了します。
現在のパスワードは無視されます。
```

メモ： デバイスのセキュリティを確保するため、適用可能な管理方法に対するパスワードを再設定してください。

Diagnostic（診断）モードの実行 - オプション [4]

テクニカルサポート限定。

ターミナルボーレートの設定 - 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、<Enter> を押します。

選択を入力するか「ESC」を押して終了します。

新規デバイスのボーレートを38,400 に設定します。

TFTP サーバーを介したソフトウェアのダウンロード

本項では、TFTP サーバーを介してデバイスソフトウェア（システムイメージおよび起動イメージ）をダウンロードする手順を説明します。ソフトウェアをダウンロードする前に、TFTP サーバーが設定されている必要があります。

システムイメージのダウンロード

システムイメージのコピーが格納されたフラッシュメモリのエリアからシステムイメージを解凍すると、デバイスが起動します。新しいイメージをダウンロードすると、そのイメージは、その他のシステムイメージのコピーに割り当てられた他のエリアに保存されます。

デバイスは次の起動時に、特に選択されていない限り、現在アクティブなシステムイメージを解凍して実行します。

TFTP サーバーを介してシステムイメージをダウンロードするには、次の手順を実行します。

□□□ いずれかのデバイスポートに IP アドレスが設定されており、Ping を TFTP サーバーに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、デバイスで現在実行されているソフトウェアのバージョンを確認します。 表示される情報の例を次に示します。

```
console# show version
SW version 1.0.0.30 (date 27-Jan-xxxx time 13:42:41)
Boot version 1.0.0.05 (date 27-Jan-xxxx time 15:12:20)
HW version
```

□□□ **show bootvar** コマンドを入力して、現在アクティブになっているシステムイメージを確認します。表示される情報の例を次に示します。

```
console# show bootvar
Images currently available on the Flash
Image-1 active（selected for next boot）
Image-2 not active
console#
```

□□□ **copy tftp:**//{tftp address}/{file name} **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。新規のイメージがダウンロードされると、そのイメージは、システムイメージのその他のコピー（例では image-2）に割り当てられたエリアに保存されます。表示される情報の例を次に示します。

```
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、コピー処理が実行中であることを示します。各感嘆符（!）は、正常に転送された 512 バイトに相当します。ピリオドは、コピー処理がタイムアウトになったことを示します。多数のピリオドが 1 列に並んでいる場合は、コピー処理が失敗したことを示します。

□□□ boot system コマンドを入力して、次の起動用のイメージを選択します。このコマンドの後、 **show bootvar** コマンドを入力して、**boot system** コマンドのパラメーターとして指定したコピーが次の起動用に選択されていることを確認します。

表示される情報の例を次に示します。

```
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）
```

boot system コマンドを入力して次の起動用のイメージを選択しないと、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.（このコマンドはシステム全体をリセットし、現在のセッションを終了します。）Do you want to continue（続行しますか）（y/n）[n]?

□□□ y と入力してください。デバイスが再起動します。

起動イメージのダウンロード

TFTP サーバーから新規の起動イメージをロードし、そのイメージをフラッシュにプログラミングすると、起動イメージがアップデートされます。デバイスの電源を入れると、起動イメージがロードされます。ユーザーには、起動イメージのコピーに対する制御権はありません。TFTP サーバーを介して起動イメージをダウンロードするには、次の手順を実行します。

□□□ いずれかのデバイスポートに IP アドレスが設定されており、Ping を TFTP サーバーに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、デバイスで現在実行されているソフトウェアのバージョンを確認します。 表示される情報の例を次に示します。

```
console# show version
SW version 1.0.0.30 (date 27-Jan-xxxx time 13:42:41)
Boot version 1.0.0.05 (date 27-Jan-xxxx time 15:12:20)
HW version
```

□□□ **copy tftp:**//{tftp address}/{file name} **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。表示される情報の例を次に示します。

```
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.（このコマンドはシステム全体をリセットし、現在のセッションを終了します。）Do you want to continue（続行しますか）（y/n）[n]?
```

□□□ y と入力してください。デバイスが再起動します。

ポートのデフォルト設定

デバイスポートの設定に関する一般情報には、オートネゴシエイションメカニズムの簡単な説明とスイッチングポートのデフォルト設定が含まれます。

オートネゴシエーション

オートネゴシエーションは、すべての 10/100/1000 BaseT ポートのスイッチングに関するスピード、二重モード、およびフロー制御の自動検出を可能にします。オートネゴシエイションはポートごとにデフォルトで有効に設定されています。

オートネゴシエイションは、2 つのリンクパートナー間に確立されるメカニズムであり、一方のポートからその転送速度、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）能力を他方に公示できるようにします。両ポートはその後、両ポートに共通する最大の機能で動作します。

オートネゴシエイションをサポートしていない、または、オートネゴシエイションが設定されていない NIC に接続する場合は、デバイススイッチングポートと NIC の両方を同じ速度および二重モードに手動で設定する必要があります。

リンクの相手側のステーションで、全二重に設定された 100 BaseT デバイスポートとのオートネゴシエイションが試みられた場合、結果として、そのステーションは半二重での動作を試みます。

MDI/MDIX

デバイスは、すべての 10/100/1000 BaseT スイッチングポートに対するストレートケーブルとクロスケーブルの自動検知をサポートしています。この自動検知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である場合に有効になります。

MDI/MDIX（メディア依存型インタフェースクロスオーバー）が有効である場合、関連性のないストレートケーブルとクロスケーブルを区別することで、ケーブル選択のエラーを自動修正することができます。エンドステーション用の標準配線は MDI（メディア依存型インタフェース）として知られ、ハブとスイッチ用の標準配線は MDIX として知られています。

Flow Control

デバイスでは、全二重モードに設定されたポートに対して 802.3x フロー制御をサポートしています。デフォルトでは、この機能は無効になっていて、ポートごとに有効にすることができます。フロー制御メカニズムによって、バッファのオーバーフローを防止するために送信を一時的に停止する必要があることを示す信号を、受信側から送信側に送ることができます。

Back Pressure

デバイスでは、半二重モードに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。デフォルトでは、この機能は無効になっていて、ポートごとに有効にすることができます。バックプレッシャーメカニズムは、一時的に送信側が追加のトラフィックを送信できないようにします。追加のトラフィックが使用できないように、受信側でリンクを占有することができます。

スイッチングポートのデフォルト設定

次の表は、ポートのデフォルト設定を示します。

表 **4-1.** ポートのデフォルト設定

機能	デフォルト設定
ポートスピードおよびモード	10/100 BaseT 銅：オートネゴシエイション、100 Mbps、全二重
	10/100/1000 BaseT 銅/SFP：オートネゴシエーション、1000 Mbps、全二重
ポート転送状態	Enabled
ポートのタグ付け	タグなし
フローコントロール	OFF（入口で無効）
バックプレッシャー	OFF（入口で無効）

目次に戻る

目次に戻る

Dell OpenManage Switch Administrator の使い方

Dell™ PowerConnect™ 35xx システムユーザーズガイド

本項では、Dell OpenManage Switch Administrator 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。詳細に関しては、初期設定を参照してください。

□□□ ウェブ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、**<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。英数字で入力してください。

□□□ **OK** をクリックします。

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

インタフェースについて

ホームページには次の表示があります。

- ツリー表示— ホームページの左側にあり、機能やそのコンポーネントを展開して表示します。
- デバイス表示 — ホームページの右側にあり、デバイス、情報またはテーブルの領域、および設定手順を表示します。

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

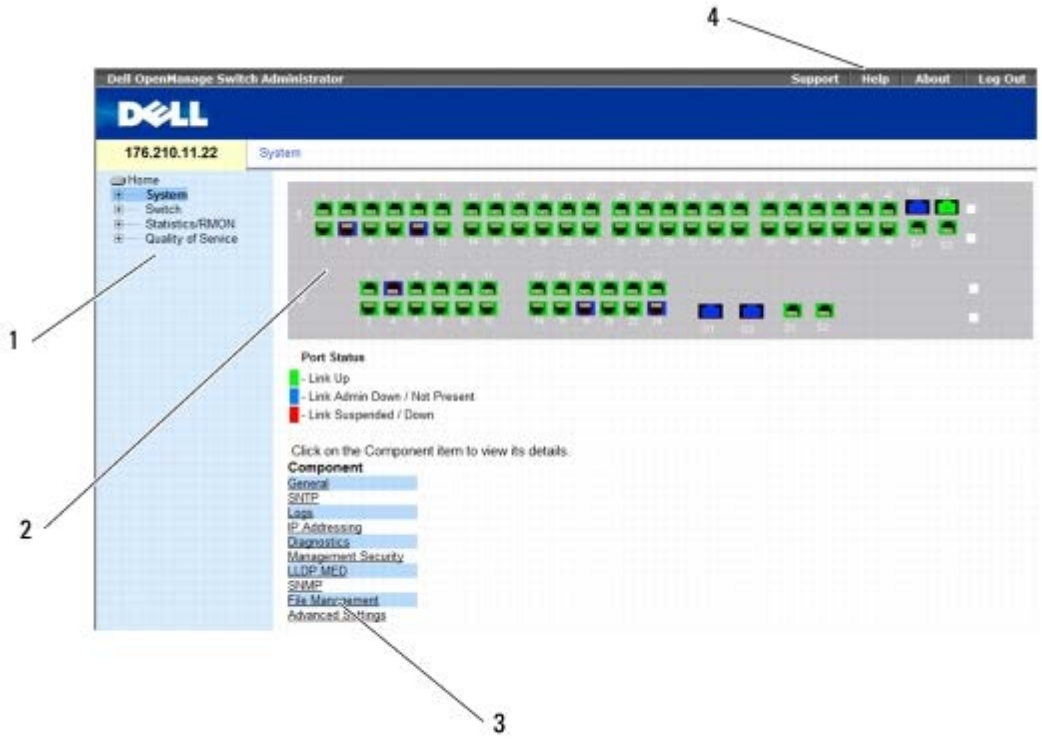


表 5-1 は、インタフェースコンポーネントと対応する番号を示します。

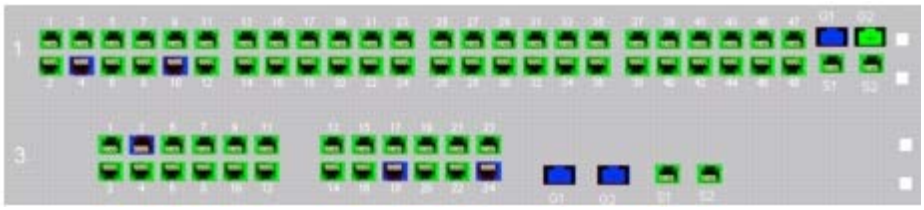
表 **5-1.** インタフェースコンポーネント

コンポーネント	説明
1	ツリー表示にはデバイスの異なる機能のリストがあります。ツリー表示の各枝は、特定の機能におけるすべてのコンポーネントを表示するために展開したり、機能のコンポーネントを非表示するために閉じることができます。縦の棒を右にドラッグすると、ツリー領域が展開し、コンポーネントの正式名を表示することができます。
2	デバイス表示は、デバイスポート、現在の設定および状態、表の情報、および機能コンポーネントについての情報を提供します。 選択されたオプションに応じて、デバイス表示の下部にある領域には、他のデバイス情報、および / またはパラメーターを設定するための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リストがあります。また、ツリー表示の機能を展開してコンポーネントを表示することができます。
4	情報ボタンは、デバイスに関する情報へのアクセス、および デルサポートへのアクセスを提供します。詳細に関しては、情報ボタンを参照してください。

デバイスの描写

ホームページには、デバイス前面パネルの画像があります。

図 **5-2. PowerConnect** デバイスポートインジケータ



ポートの色付けは、指定のポートが現在アクティブであるかどうかを示します。ポートには次の色があります。

表 **5-2. PowerConnect** ポートおよびスタッキングインジケータ

コンポーネント	説明
ポートインジケータ	
緑色	ポートは現在有効です。
赤色	ポートにエラーが発生しました。
青色	ポートは現在無効です。
赤色	このデバイスは現在スタック内でリンクされていません。

メモ： ポート LED は、OpenManage Switch Administrator の PowerConnect 前面パネルには反映されません。LED ステータスは、実際のデバイスを見ることによってのみ決定することができます。ただし、スタッキング LED はスタッキングポートのステータスを反映します。LED の詳細に関しては、**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 インタフェース上に見られるボタンについて記載します。インタフェースボタンは次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、並びに、OpenManage Switch Administrator インタフェースに関する情報を提供します。

表 **5-3.** 情報ボタン

ボタン	説明
Support	**support.jp.dell.com** のデルサポートページが開きます。
Help	オンラインヘルプには、デバイスの設定および管理を援助する情報があります。オンラインヘルプページはコンテキスト依存です。たとえば、**IP** アドレス指定 ページを開いていて ヘルプをクリック すると、そのページのヘルプトピックが開きます。
About	ここには、バージョン、ビルド番号、およびデルの著作権情報が含まれます。
Log Out	ログアウトウィンドウを開きます。

デバイス管理ボタン

デバイス管理ボタンは、以下を含む、デバイス情報を設定する簡単な方法を提供します。

表 **5-4.** デバイス管理ボタン

ボタン	説明
Apply Changes	デバイスの設定変更を適用します。
Add	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	表を問い合わせます。
Show All	デバイス表を表示します。
左矢印 **/** 右矢印	リスト間で情報を移動します。
Refresh	デバイス情報をリフレッシュします。
Reset All Counters	統計カウンタをクリアします。
Print	ネットワーク管理システムページ、および / または表の情報を印刷します。
Draw	オンザフライで統計チャートを作成します。
Details	現在のページに関連した詳細を表示します。
Back	前のページに戻ります。

フィールドの定義

OpenManage Switch Administrator のウェブページに特に指定のない限り、ユーザー定義のフィールドには 1～159 文字を含むことができます。次を除いたすべての文字および記号を使用できます。

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

CLI を使用したデバイスへのアクセス

デバイスは、ターミナルポートへの直接接続、または Telnet 接続によって管理することができます。Telnet 接続によるアクセスの場合は、デバイスに IP アドレスが定義されていること、および、CLI コマンドを使用する前にデバイスにアクセスするために使用され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の情報に関しては、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アクセスする前に、ソフトウェアが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、スタートアップ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、必要なコマンドを入力して要求されたタスクを完了させます。

□□□ 完了したら、**exit Privileged EXEC mode** コマンドを入力してください。

セッションが終了します。

メモ： 異なるユーザーが特権 EXEC コマンドモードでシステムにログインする場合、現在のユーザーはログオフされ、新しいユーザーがログインされます。

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することができます。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。

デバイスは、デバイス管理を行うため Telnet のセッションを最高 4 つ同時にサポートします。Telnet セッションでは、すべての CLI コマンドを使用できます。

Telnet セッションを開始するには次の手順を実行します。

□□□ **Start**（スタート）® **Run**（ファイル名を指定して実行）を選択します。

Run（ファイル名を指定して実行）ウィンドウが開きます。

□□□ **Run**（ファイル名を指定して実行ウィンドウ）の **Name**（名前）フィールドに、*`Telnet <IP address>`* を入力します。

□□□ **OK** をクリックします。

Telnet セッションが開始されます。

CLI の使い方

本項では、CLI コマンドの使い方の情報を記載します。

コマンドモードの概要

CLI はコマンドモードに分かれます。各コマンドモードには特定のコマンドセットがあります。ターミナルプロンプトで疑問符（?）を入力すると、特定のコマンドモードで利用可能なコマンドリストが表示されます。

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することができます。

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、限られたコマンドのサブセットしか利用できません。_このレベルは、ターミナル設定を変更しないタスク用に確保され、CLI などの設定サブシステムへアクセスするために使用されます。次のレベルの特権 EXEC モードに入るにはパスワードが必要です（設定している場合）。

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。 デバイスで特定のグローバル設定をするには、次のレベルのグローバル設定モードに入ります。パスワードは必要ありません。

グローバル設定モードは、グローバルレベルでデバイス設定を管理します。

インタフェース設定モードは、デバイスを物理的インタフェースレベルで設定します。サブコマンドを要求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。パスワードは必要ありません。

ユーザー **EXEC** モード

デバイスにログインすると、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。次はその例です。

```
console>
```

メモ： デフォルトのホスト名は、初期設定で変更しない限り **console** です。

ユーザー EXEC コマンドを使用して、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、およびシステム情報の一覧表示を行います。

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ぐため、および、動作パラメーターを確保するために、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 モードプロンプトは、デバイスホスト名とそれに続く **#** で表示します。次はその例です。

```
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** を入力してから **<Enter>** を押します。

次の例は、特権 EXEC モードにアクセスした後、ユーザー EXEC モードに戻る方法を示したものです。

```
console> enable
Enter Password: ******
console#
console# disable
console>
```

exit コマンドを使用して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、またはグローバル設定モードから特権 EXEC モードに、というように前のモードに戻ります。

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にではなく、システム機能に適用します。

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は、デバイスのホスト名の後ろに（**config**）と **#** が付いた形で表示されます。

```
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、**<Ctrl>+<Z>** キーの組み合わせを使います。

次の例は、グローバル設定モードにアクセスした後、特権 EXEC モードに戻る方法を示したものです。

```
console#
```

```
console# configure

console(config)# exit

console#
```

CLI モードの全一覧は、 **Dell™ PowerConnect™3524/P** および **PowerConnect 3548/P** コマンドラインインタフェースユーザーズガイド を参照してください。

目次に戻る

目次に戻る

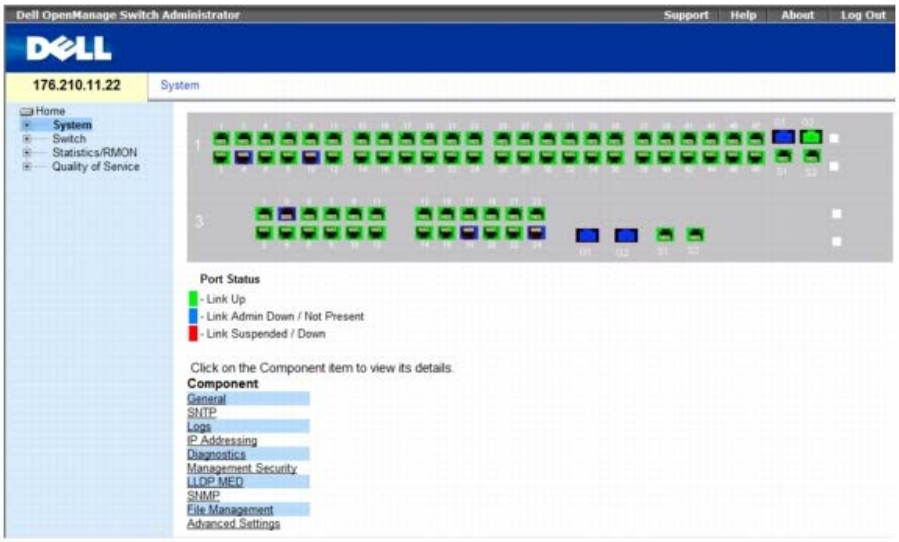
システム情報の設定

Dell™ PowerConnect™ 35xx システムユーザーズガイド

このページでは、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、およびスイッチのリセットを含むシステムパラメーターを定義するためのリンクを提供します。**System**（システム）ページを開くには、以下のリンクをクリックして、示されている画面のオンラインヘルプにアクセスします。

ツリー表示の **System**（システム）をクリックします。

図 **6-1.** システム



本項には、次のトピックがあります。

- スイッチの一般情報の定義
- SNTP の設定
- ログの管理
- IP アドレス設定の定義
- ケーブル診断の実行
- 管理セキュリティの管理
- LLDP および MED の設定
- SNMP パラメーターの定義
- ファイルの管理
- 詳細設定

スイッチの一般情報の定義

General（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設定するために必要な、各ページへのリンクを含んでいます。

本項には、次のトピックがあります。

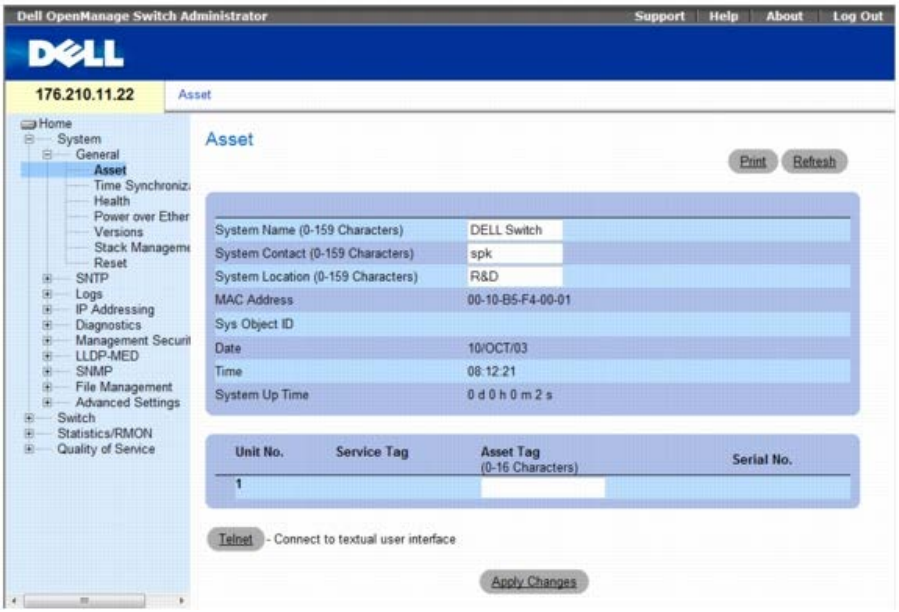
- スイッチアセット情報の表示
- アセット
- システムの時間設定の定義

スイッチアセット情報の表示

アセット

Asset（アセット）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、時刻、およびシステムの稼動時間など、デバイスの一般情報の設定および表示用パラメータで構成されています。**Asset**（アセット）ページを開くには、ツリー表示の **System**（システム）® **General**（一般）® **Asset**（アセット）をクリックします。

図 **6-2.** アセット



Asset（アセット）ページには、以下のフィールドがあります。

- **System Name** （**0-159 Characters**）（システム名（0～159 文字））— ユーザー定義のデバイス名を定義します。
- **System Contact** （**0-159 Characters**）（システム問い合わせ先（0～159 文字））— 問い合わせ担当者の名前を示します。
- **System Location** （**0-159 Characters**）（システムの場所情報（0～159 文字））— 現在システムが稼動している場所です。
- **MAC Address**（MAC アドレス）— デバイスの 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に関する、ベンダーの正式な ID です。
- **Date**（日付）— 現在の日付です。形式は、日、月、年の順で、たとえば 15/FEB/07 は 2007 年 2 月 15 日を表します。
- **Time**（時刻）— 時刻を示します。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。
- **System Up Time**（システムアップ時間）— 最後にデバイスをリセットしてからの時間を指定します。システムの時間は次の形式、つまり、日、時、分、秒で表示されます。つまり、日、時、分、秒で表示されます。例えば、41 日、2 時、22 分、15 秒となります。
- **Unit No.**（ユニット番号）— デバイスアセット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参照番号です。
- **Asset Tag** （**0-16 Characters**）（アセットタグ（0～16 文字））— ユーザー定義のデバイス参照情報を示します。
- **Serial No.**（シリアルナンバー）— デバイスのシリアルナンバーです。

システム情報の定義

□□□ **Asset page**（アセットページ）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ーが定義され、デバイスがアップデートされます。

Telnet セッションの開始

□□□ **Asset page**（アセットページ）を開きます。

□□□ **Telnet** をクリックします。

Telnet セッションが開始されます。

CLI コマンドを使用したデバイス情報の設定

次の表は、 **Asset page**（アセットページ）にあるフィールドを表示および設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
hostname *name*	デバイスのホスト名を指定または変更します。
snmp-server contact *text*	システムの担当者を設定します。
snmp-server location *text*	デバイスがある場所に関する情報を入力します。
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の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*	デバイスのアセットタグを設定します。
show stack <1-8>	システムのスタック情報を表示します。
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 ID 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:                        PowerConnect-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 5324	PowerConnect 3524
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	
7	893658978		mkt-7	89788984	
8	893658979		mkt-8	89788985	
console# **show system**					
Unit	Type				
----	----------				
1	PowerConnect 3524				
2	PowerConnect 3524				
3	PowerConnect 3524				
4	PowerConnect 3524P				
5	PowerConnect 3524P				
6	PowerConnect 3524P				
7	PowerConnect 3524P				
8	PowerConnect 3524P				
Unit	Main Power Supply		Redundant Power Supply		
----	----------		----------		
1	OK				
2	OK				
3	OK				
4	OK				
5	OK		OK		
6	OK		OK		
7	OK		OK		
8	OK		OK		
Unit	Fan1	Fan2	Fan3	Fan4	Fan5
----	----	----	----	----	----
1	OK	OK			
2	OK	OK			
3	OK	OK			
4	OK	OK			
5	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK
7	OK	OK	OK	OK	OK
8	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		
7	30		OK		
8	30		OK		

システムの時間設定の定義

Time Synchronization（時刻同期）ページには、ローカルなハードウェアクロックと外付けの SNTP クロック両方のシステム時刻パラメーターを定義するためのフィールドがあります。外付けの SNTP クロックを使用してシステム時間が計時され、外付けの SNTP クロックが故障した場合、システム時間はローカルなハードウェアクロックに戻ります。デバイスで夏時間を有効にすることができます。以下は指定国の夏時間の開始日および終了日のリストです。

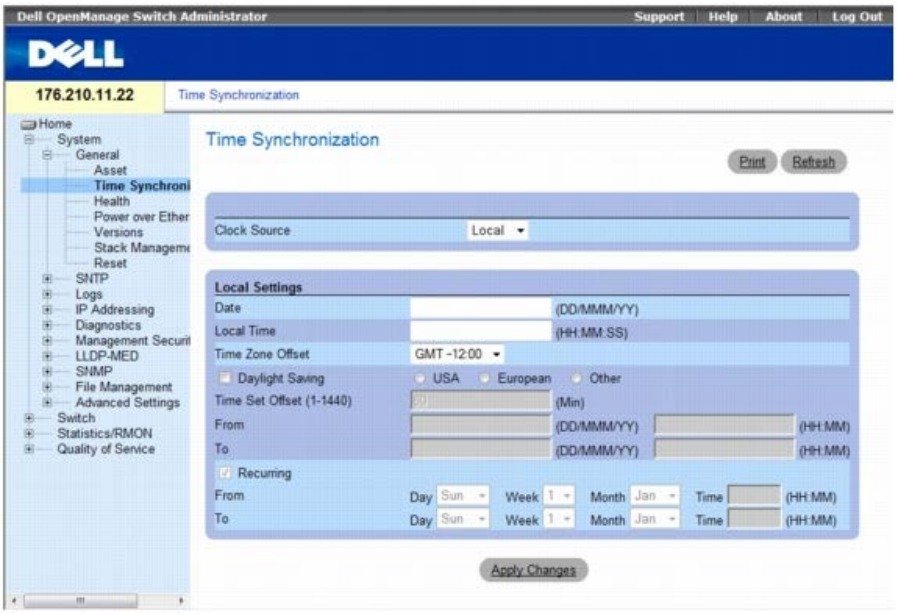
- アルバニア — 3 月の最後の週末から 10 月の最後の週末まで。
- オーストラリア — 10 月の末日から 3 月の末日まで。
- オーストラリア - タスマニア — 10 月の初めから 3 月の末日まで。
- アルメニア — 3 月の週末から 10 月の最後の週末まで。
- オーストリア — 3 月の最後の週末から 10 月の最後の週末まで。
- バハマ — 米国の夏時間にともない、4 月から 10 月まで。
- ベラルーシ — 3 月の最後の週末から 10 月の最後の週末まで。
- ベルギー — 3 月の最後の週末から 10 月の最後の週末まで。
- ブラジル — 10 月の第三週目の日曜日から 3 月の第三週目の土曜日まで。ブラジルの南東部のほとんどでは、夏時間の間、時計は 1 時間進みます。
- チリ — イースター島 3 月 9 日から 10 月 12 日まで。3 月の第一日曜日または 3 月 9 日以降。
- 中国 — 中国は夏時間を実施していません。
- カナダ — 4 月の第一日曜日から 10 月の最後の日曜日まで。夏時間は、通常、州政府および領土政府により管理され、特定の自治区では例外が存在する場合があります。
- 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。
- キプロス — 3 月の最後の週末から 10 月の最後の週末まで。
- 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。
- 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。
- 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。
- 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。
- フランス — 3 月の最後の週末から 10 月の最後の週末まで。
- ドイツ — 3 月の最後の週末から 10 月の最後の週末まで。
- ギリシャ — 3 月の最後の週末から 10 月の最後の週末まで。
- 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。
- インド — インドでは夏時間を実施していません。
- イラン — 3月 21 日から 9 月 23 日まで。
- イラク — 4 月 1 日から 10 月 1 日まで。
- 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。
- イスラエル — 年によって変わります。
- イタリア — 3 月の最後の週末から 10 月の最後の週末まで。
- 日本 — 日本では夏時間を実施していません。
- ヨルダン — 3 月の最後の週末から 10 月の最後の週末まで。
- ラトヴィア — 3 月の最後の週末から 10 月の最後の週末まで。
- レバノン — 3 月の最後の週末から 10 月の最後の週末まで。
- 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。
- 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。
- 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。
- メキシコ — 4 月の最初の日曜日の 2:00 時から 10 月の最後の日曜日の 2:00 まで。

- モルドヴァ — 3 月の最後の週末から 10 月の最後の週末まで。
- 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。
- オランダ — 3 月の最後の週末から 10 月の最後の週末まで。
- ニュージーランド — 10 月の第一日曜日から 3 月 15 日以降の最初の日曜日まで。
- ノルウェー — 3 月の最後の週末から 10 月の最後の週末まで。
- パラグアイ — 4 月 6 日から 9 月 7 日まで。
- 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。
- 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。
- 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。
- ロシア — 3 月 29 日から 10 月 25 日まで。
- セルビア — 3 月の最後の週末から 10 月の最後の週末まで。
- スロヴァキア共和国 — 3 月の最後の週末から 10 月の最後の週末まで。
- 南アフリカ — 南アフリカでは夏時間を実施していません。
- スペイン — 3 月の最後の週末から 10 月の最後の週末まで。
- 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。
- スイス — 3 月の最後の週末から 10 月の最後の週末まで。
- シリア — 3 月 31 日から 10 月 30 日まで。
- 台湾 — 台湾では夏時間を実施していません。
- トルコ — 3 月の最後の週末から 10 月の最後の週末まで。
- 英国 — 3 月の最後の週末から 10 月の最後の週末まで。
- アメリカ合衆国 — 3 月の第 2 日曜日の 2:00 から 11 月の第 1 日曜日の 2:00 まで。

SNTP の詳細については、SNTP の設定を参照してください。

Time Synchronization（時刻同期）ページを開くには、ツリー表示の **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



Time Synchronization（時刻同期）ページには、以下のフィールドがあります。

- **Clock Source**（クロックソース）— システムクロックを設定するためのソースです。可能なフィールド値は以下のとおりです。
  - **Local**（ローカル）— システム時刻の設定に外部クロック源を使用しないように指定します。
  - **SNTP** — システム時間が SNTP サーバーを介して設定されることを指定します。詳細については、SNTP の設定を参照してください。

ローカルな設定

- **Date**（日付）— システムの日付を定義します。フィールドの形式は、DD/MMM/YY（たとえば、04/May/07）です。
- **Local Time**（現地時間）— システム時刻を定義します。フィールドの形式は、時：分：秒で、例えば、21：15：03 です。
- **Time Zone Offset**（タイムゾーンオフセット）— グリニッジ標準時と現地時間との間の差です。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タイムは GMT –5:00 です。

夏時間の設定には 2 つのタイプがあり、特定の年の特定の日付による設定、または年に関係のない繰返し設定のいずれかです。特定の年の特定の設定の場合は、夏時間 領域を完成させ、繰返し設定の場合は、繰り返し 領域を完成させます。

- **Daylight Savings**（夏時間）— デバイスの場所に基づいて、デバイスの夏時間（DST）を有効にします。可能なフィールド値は次のとおりです。
  - **USA**（米国）— デバイスを、3 月の第 2 日曜日の午前 2:00 に DST に切り換え、11 月の第 1 日曜日の午前 2:00 に標準時刻に戻します。
  - **European**（欧州）— デバイスを、3 月の最後の日曜日の午前 1:00 に DST に切り換え、10 月の最後の日曜日の午前 1:00 に標準時刻に戻します。European（欧州）オプションは EU メンバーに適用し、その他の欧州各国は EU 標準を使用します。
  - **Other**（その他）— DST の定義はデバイスの場所に基づいてユーザーにより定義されます。その他 を選択する場合は、から（From）および まで（To）フィールドを定義する必要があります。
- **Time Set Offset**（**1-1440**）（時刻設定オフセット（1～1440））— 夏時間と現地標準時の時差を分単位で示します。デフォルトの時間は 60 分です。
- から（From）— 米国または欧州以外の各国で DST が始まる時間を、1 つのフィールドに日月年という形式で、もう 1 つのフィールドには時間を入力します。例えば、DST が 2007 年10 月 25 日の午前 5:00 に始まる場合は、2 つのフィールドは 25Oct07 および 5:00 となります。可能なフィールド値は以下のとおりです。
  - **DD/MMM/YY** — 夏時間が始まる日/月/年。
  - **HH/MM** — 夏時間が始まる時刻（時と分）。フィールドの形式は HH/MM で、たとえば 05:30 となります。
- まで（To）— 米国または欧州以外の各国で DST が終る時間を、1 つのフィールドに日月年という形式で、もう 1 つのフィールドには時間を入力します。例えば、DST が 2008 年 3 月 23 日の午前 12:00 に終る場合は、2 つのフィールドは、23Mar08 および 12:00 となります。可能なフィールド値は以下のとおりです。
  - **DD/MMM/YY** — 夏時間が終わる日/月/年。
  - **HH/MM** — 夏時間が終わる時刻（時と分）。フィールドの形式は HH/MM で、たとえば 05:30 となります。
- **Recurring**（繰り返し）— 毎年 DST が一定している米国または欧州以外の各国において、DST が始まる時刻を定義します。可能なフィールド値は次のとおりです。
- **From**（から）— 各年 DST が始まる時刻を定義します。例えば、DST は、4 月の第二日曜日の 午前 5:00 に地域毎に始まります。可能なフィールド値は次のとおりです。
  - **Day**（日）— 毎年 DST が始まる曜日です。可能なフィールドの範囲は日曜日～土曜日です。
  - **Week**（週）— 毎年 DST が始まる月の週です。可能なフィールドの範囲は 1～5 です。
  - **Month**（月）— 毎年 DST が始まる月です。可能なフィールドの範囲は1 月～12 月です。
  - **Time**（時間）— 毎年 DST が始まる時間です。フィールドの形式は、時:分で、例えば、02:10 です。
- **To**（まで）— 各年 DST が終わる繰返し時刻を定義します。例えば、DST は、4 月の第四金曜日の午前 5:00 に地域毎に終ります。可能なフィールド値は次のとおりです。
  - **Day**（日）— 毎年 DST が終わる曜日です。可能なフィールドの範囲は日曜日～土曜日です。
  - **Week**（週）— 毎年 DST が終る週です。可能なフィールドの範囲は 1～5 です。
  - **Month**（月）— 毎年 DST が終る月です。可能なフィールドの範囲は1 月～12 月です。
  - **Time**（時間）— 毎年 DST が終る時間です。フィールドの形式は、時:分で、例えば、05:30 です。

クロックソースの選択

□□□ **Time Synchronization**（時間同期）ページを開きます。

□□□ **Clock Source**（クロックソース）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。

クロックソースが選択され、デバイスがアップデートされます。

ローカルなクロック設定の定義

□□□ **Time Synchronization**（時間同期）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。

ローカルな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

次の表は、 **Time Synchronization**（時刻同期）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

クロックを夏時間に設定する前に、以下の手順を完了しなければなりません。

□□□ 夏時間の採用を設定する。

□□□ タイムゾーンを定義します。

□□□ 時間をセットする。

次はその例です。

```
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	システムクロックのための外付けのタイムソースを設定します。
clock time zone *hours-offset* [**minutes** *minutes-offset*][**zone** *acronym*]	表示目的のためにタイムゾーンを設定します。
clock summer-time	システムが自動的に夏時間（日照節約時間）に切り替わるように設定します。
clock summer-time recurring {**usa** | **eu** | *week day month hh:mm week day month hh:mm*} [**offset** *offset*] [**zone** *acronym*]	（米国の標準および欧州の標準に応じて）システムが自動的に夏時間に切り替わるように設定します。
clock summer-time date *date month year hh:mm date month year hh:mm* **[offset** *offset***] [zone** *acronym***]**	指定の期間（日、月、年の形式）について、システムが自動的に夏時間（日照節約時間）に切り替わるように設定します。

CLI コマンドの例は次のようになります。

```
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
```

システムの情報の表示

System Health（システムの状態）ページ には、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が表示されます。**System Health**（システムの状態）ページを開くには、ツリー表示の **System**（システム）® **General**（一般）® **Health**（状態）をクリックします。

図 **6-4.** システムの状態

System Health（システムの状態）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）— デバイスの状態情報が表示されているユニット番号を示します。

- **Power Supply Status**（電源ユニットステータス）— デバイスは 2 台の電源ユニットを内蔵しています。可能なフィールド値は次のとおりです。
  -  Checked（チェックマークあり）— 電源ユニットは正常に動作しています。
  -  Unchecked（チェックマークなし）— 電源ユニットは正常に動作していません。
  - **Not Present**（存在しない）— 電源ユニットは現在存在しません。
- **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インタフェース上に表示されます。可能なフィールド値は次のとおりです。
  -  Checked（チェックマークあり）— ファンは正常に動作しています。
  -  Unchecked（チェックマークなし）— ファンは正常に動作していません。
  - **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

Celsius（摂氏）	**Fahrenheit**（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の状態情報の表示

次の表は、**System Health**（システムの状態）ページにあるフィールドを表示するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
show system [unit ***unit*****]**	システム情報を表示します。

システムの状態を表示する CLI コマンドの例を以下に示します。

console#	**show system**			
Unit	**Type**			
1	PowerConnect 3524			
Unit	**Main Power Supply**	**Redundant Power Supply**		
1	OK			
Fan1	**Fan2**	**Fan3**	**Fan4**	**Fan5**
1	OK	OK	OK	OK
Unit	**Temperature (Celsius)**	**Temperature Sensor Status**		
1	27	OK		
Unit	**Up time**			
1	00,09:30:36			

パワーオーバーイーサネットの管理

Power over Ethernet（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 を使用すると、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 の電源ユニット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、イーサネットポートを介して PowerConnect デバイスと接続されます。パワードデバイスは、すべての PowerConnect 3524P の 24 FE ポートか、すべての PowerConnect 3548P の 48 FE 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、ツリー表示で、**System**（システム）® **General**（一般）® **Power over Ethernet** の順にクリックします。

図 6-5. Power Over Ethernet

Power Over Ethernet ページには、以下のセクションがあります。

- グローバル
- ポートの設定

グローバル

Power over Ethernet の Global Settings（グローバル設定）セクションには、以下のフィールドがあります。

- **Power Status**（電源ステータス）— インライン電源ステータスを示します。
  - **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、電源がオーバーロードになっているか、ショートしている場合です。
- **Nominal Power**（公称電力）— 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ワットです。
- **Consumed Power**（消費電力）— デバイスによって使用される電力量を示します。フィールド値の単位はワットです。
- **System Usage Threshold**（**1-99 Percent**）（システム利用しきい値（1～99 パーセント））— アラームが発せられるまでに達する消費電力の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。
  - **Enable**（有効）— デバイスで PoE トラップを有効にします。
  - **Disable**（無効）— デバイスで PoE トラップを無効にします。これがデフォルト値になっています。

ポートの設定

- **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定義され、割り当てられた PoE パラメータの特定の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。可能なフィールド値は次のとおりです。
  - **Auto**（自動）— デバイス検出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。デバイス検出プロトコルは、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検出し、その分類を学習します。これはデフォルト設定です。
  - **Never**（なし）— デバイス検出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 動作が有効かどうかを表示します。可能なフィールド値は次のとおりです。
  - **Disabled**（無効）—
  - **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。
  - **Delevering Power**（給電）— PowerConnect デバイスが給電中であることを示します。
  - **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。たとえば、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。
  - **Test**（テスト）— パワードデバイスが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、電源から電力が供給されているかどうか確認する場合が該当します
  - **Other Fault**（その他の故障）—
  - **Unknown**（不明）—
- **Power Priority Level**（電力優先度レベル）— 電力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力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、電源ユニットが使用率 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、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）— 最高の電力優先度レベルを割り当てます。
  - **High**（高）— 2 番目に高い電力優先度レベルを割り当てます。
  - **Low**（低）— 最も低い電力優先度レベルを割り当てます。
- **Power Classification**（電力の分類）— パワードデバイスが次のように分類されていることを示します。
  - **Class 0: 0.44 – 12.95** — ポートに 0.44～12.95 ワット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。
  - **Class 1: 0.44 – 3.8** — ポートに 0.44～3.8 ワット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。
  - **Class 2: 3.84 – 6.49** — ポートに 3.84～6.49 ワット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。
  - **Class 3: 6.49 – 12.95** — ポートに 6.49～12.95 ワット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
- **Powered Device**（**0-24 characters**）（パワードデバイス（0～24 文字））— ユーザー定義のパワードデバイスの説明を示します。フィールドの長さは最大 24 文字です。
- **Overload Counter**（オーバーロードカウンタ）— 電力オーバーロード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**（拒否カウンタ）— パワードデバイスへの電力供給が拒否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、分類、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。

□□□ 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 の設定が定義され、デバイスがアップデートされます。

すべてのポート用の **PoE** 設定の表示

□□□ **Power Over Ethernet** ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Power Over Ethernet Table（Power Over Ethernet 表）が開きます。

図 **6-6. Power Over Ethernet** 表

CLI コマンドを使用した PoE の管理

次の表は、**Power Over Ethernet** ページにあるフィールドを表示するための等価 CLI コマンドをまとめたものです。

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電力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}	インライン電力の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。

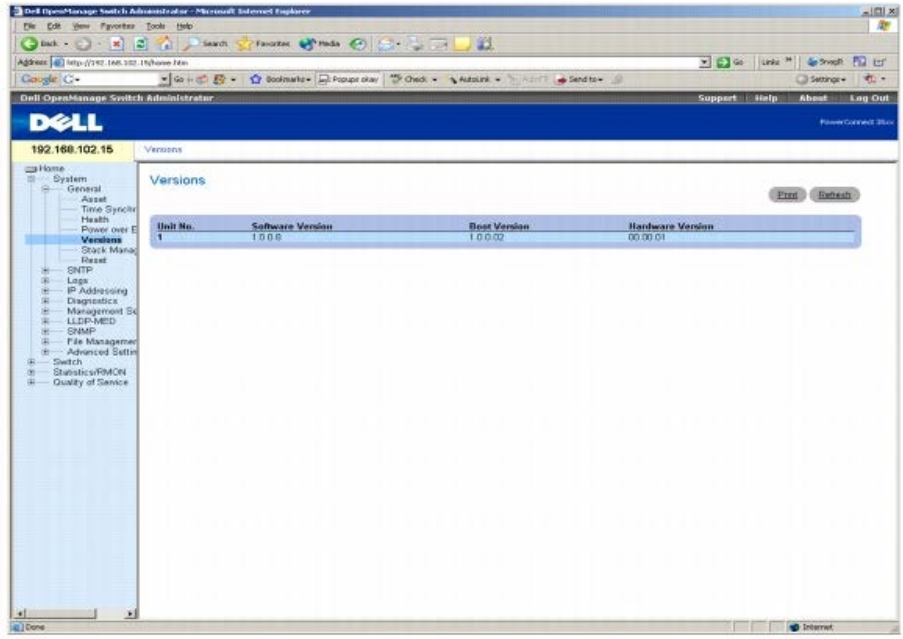
以下に、PoE CLI コマンドの例を示します。

```
Console> enable
Console# show power inline

Unit  Power  Nominal Power  Consumed Power  Usage  Threshold
1     On     370 Watts      0 Watts (0%)    95     Disable
2     Off    1 Watts        0 Watts (0%)    95     Disable
3     Off    1 Watts        0 Watts (0%)    95     Disable
4     Off    1 Watts        0 Watts (0%)    95     Disable
5     Off    1 Watts        0 Watts (0%)    95     Disable
6     Off    1 Watts        0 Watts (0%)    95     Disable
7     Off    1 Watts        0 Watts (0%)    95     Disable
8     Off    1 Watts        0 Watts (0%)    95     Disable

Port  Powered Device  Status  Status     Priority  Class
1/e1                  Auto    Searching  low       class0
1/e2                  Auto    Searching  low       class0
1/e3                  Auto    Searching  low       class0
1/e4                  Auto    Searching  low       class0
1/e5                  Auto    Searching  low       class0
1/e6                  Auto    Searching  low       class0
```

バージョン情報の表示

Versions（バージョン）ページには、現在実行しているハードウェアおよびソフトウェアのバージョンに関する情報があります。**Versions**（バージョン）ページを開くには、ツリー表示の **System**（システム）® **General**（一般）® **Versions**（バージョン）をクリックします。

図 **6-7.** バージョン



Versions（バージョン）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）— デバイスのバージョン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）— デバイスで実行している現在のソフトウェアバージョンです。
- **Boot Version**（ブートバージョン）— デバイスで実行している現在のブートバージョンです。
- **Hardware Version**（ハードウェアバージョン）— 現在の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のバージョンの表示

次の表は、**Versions**（バージョン）ページにあるフィールドを表示するための等価 CLI コマンドをまとめたものです。

表 **6-6.** バージョン **CLI** コマンド

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

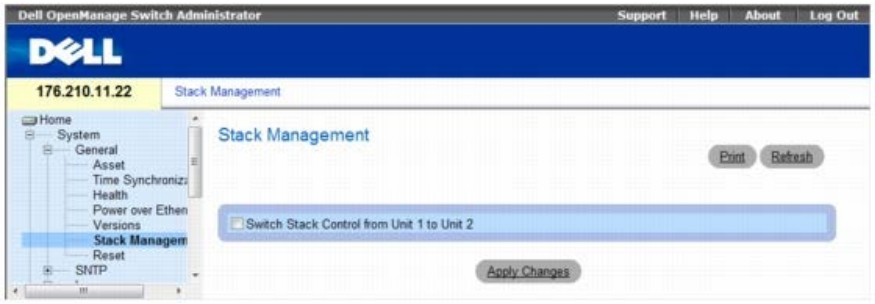
CLI コマンドの例は次のようになります。

```
console> show version

Unit SW version Boot version HW version

------------------- ------------------- ------------------- -
---- 1 1.0.0.8 1.0.0.02 00.00.01
```

スタッキングメンバーの管理

Stack Management（スタック管理）ページでは、ネットワーク管理者は、スタックのユニット 1 と ユニット 2 の間でスタックコントロールを切り替えることができます。**Stack Management**（スタック管理）ページを開くには、ツリー表示で、**System**（システム）® **General**（一般）® **Stack Management**（スタック管理）の順にクリックします。

図 **6-8.** スタック管理



- **Switch Stack Control from Unit 1 to Unit 2**（スタックコントロールをユニット 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。

スタックマスター間の切り替え

□□□ **Stack Management**（スタック管理）ページを開きます。

□□□ **Switch Stack Control from Unit 1 to Unit 2**（スタックコントロールをユニット 1 からユニット 2 へ切り替える）チェックボックスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

確認のメッセージが表示されます。

□□□ **OK**。

デバイスがリセットされます。デバイスをリセットした後、ユーザー名およびパスワードを促すプロンプトが表示されます。

CLI コマンドを使用したスタック管理

次の表は、 **Stack Management**（スタック管理）ページにあるフィールドを表示するための等価 CLI コマンドをまとめたものです。

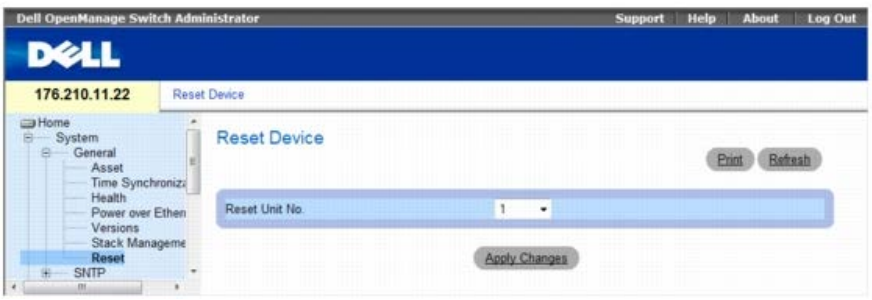
表 **6-7.** スタック管理に関連する **CLI** コマンド

CLI コマンド	説明
stack reload	スタックメンバをリロードします。
stack master	スタックマスター選択を強制します。

デバイスのリセット

Reset（リセット）ページでデバイスを遠隔地からリセットすることができます。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。これにより、現在のデバイスの設定が失われるのを防ぐことができます。設定ファイルの詳細については、ファイルのコピーを参照してください。**Reset**（リセット）ページを開くには、ツリー表示の **System**（システム）® **General**（一般）® **Reset**（リセット）をクリックします。

図 **6-9.** リセット



Reset（リセット）ページには、以下のフィールドがあります。

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

デバイスのリセット

□□□ **Reset**（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選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

確認の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で、ユーザー名とパスワードの入力を求められます。

□□□ ユーザー名およびパスワードを入力してウェブインタフェースに再接続します。

CLI を使用したデバイスのリセット

次の表は、CLI からデバイスのリセットを行う場合の等価 CLI コマンドをまとめたものです。

表 **6-8.** リセット **CLI** コマンド

CLI コマンド	説明
reload	デバイスをリロードします。

CLI コマンドの例は次のとおりです。

```
console# reload
You haven't saved your changes. Are you sure you want to continue? (Y/N)[N] Y
This command will reset the whole system and disconnect your current session.Do you want to continue ? (Y/N)[N] Y
```

SNTP の設定

スイッチは、Simple Network Time Protocol（SNTP）をサポートしています。SNTP は、ネットワークスイッチのクロック時間についてミリ秒以下の正確な同期を保証します。時間同期はネットワーク SNTP サーバーによって行います。SNTP は、クライアントとして動作するだけで、他のシステムへのタイムサービスを提供することはできません。

スイッチは、サーバータイムを要求するために、次のサーバータイプにポーリングできます。

- ユニキャスト
- エニキャスト
- ブロードキャスト

タイムソースは階層によって確立されます。階層は基準クロックの精度を定義します。階層（ゼロが最も高い）高くなるほどクロックはさらに正確になります。スイッチは、stratum 1 以上のサーバーから時刻を取得します。階層の例を以下に示します。

- **Stratum 0**（階層 0）— GPS システムのように、タイムソースとしてリアルタイムクロックが使用されることを示します。
- **Stratum 1**（階層 1）— 階層 0 のタイムソースに直接リンクされるサーバーが使用されることを示します。階層 1 タイムサーバーは、プライマリネットワークタイム標準を提供します。
- **Stratum 2**（階層 2）— ネットワークパスを介して階層 1 サーバーよりもタイムソースが離れていることを示します。例えば、階層 2 サーバーは ネットワークリンク上の NTP を介して階層 1 サーバーから時間を受信します。

SNTP サーバーから受信した情報はタイムレベルおよびサーバータイプに基づいて評価されます。SNTP タイム定義は以下のタイム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間。
- **T2** — サーバーが最初の要求を受信した時間。
- **T3** — サーバーがクライアントに応答を送信した時間。
- **T4** — クライアントがサーバーからの応答を受信した時間。

デバイスはサーバータイムに以下のサーバーのタイプをポーリングすることができます。ユニキャスト、エニキャスト、およびブロードキャスト。

ユニキャスト情報のポーリングは、IP アドレスが判明しているサーバーをポーリングするために使用します。デバイスに設定された 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。サーバータイムの決定には、T1～T4 が使用されます。これが最もセキュアなため、デバイスの時刻を同期させる推奨方法です。この方法が選択された場合、**SNTP Servers**（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。

サーバーの IP アドレスが不明なときにエニキャスト情報のポーリングを使用します。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できます。デバイスは同期情報を事前に要求したときに同期を行います。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（低次の層）が、時刻値の設定に使用されます。タイムレベル T3 および T4 は、サーバータイムを決定するために使用します。

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、デバイスで設定されていない SNTP サーバーから発せられた SNTP パケットも受け付けられることから、ユニキャストポーリングよりも安全性が低下します。

サーバーの IP アドレスが不明なときにブロードキャスト情報を使用します。ブロードキャストメッセージが SNTP サーバーから送信されると、SNTP クライアントはメッセージをリスニングします。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。これは、最も安全性が低い方法です。

デバイスは、アクティブ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優先されます。ユニキャストポーリングが有効でない場合、またはデバイスにサーバーが定義されていない場合、デバイスは応答する任意の SNTP サーバーからの時刻情報も受け入れます。
- 2 台以上のユニキャストデバイスが応答した場合は、最も低位の階層のデバイスからの同期情報が優先されます。
- サーバーが同一の階層を持つ場合、最初に応答した SNTP サーバーからの同期情報が受け入れられます。

MD5（メッセージダイジェスト 5）認証は、SNTP サーバーへのデバイス同期パスを保護します。MD5 は 128 ビットハッシュを生成するアルゴリズムです。MD5 は MD4 が変化したもので、MD4 のセキュリティを増加します。MD5 は、通信の保全性を検証し、通信の発信元の認証を行います。

SNTP ページを開くには、ツリー表示で、**System**（システム）® **SNTP** の順にクリックして、 **SNTP** ページを開きます。

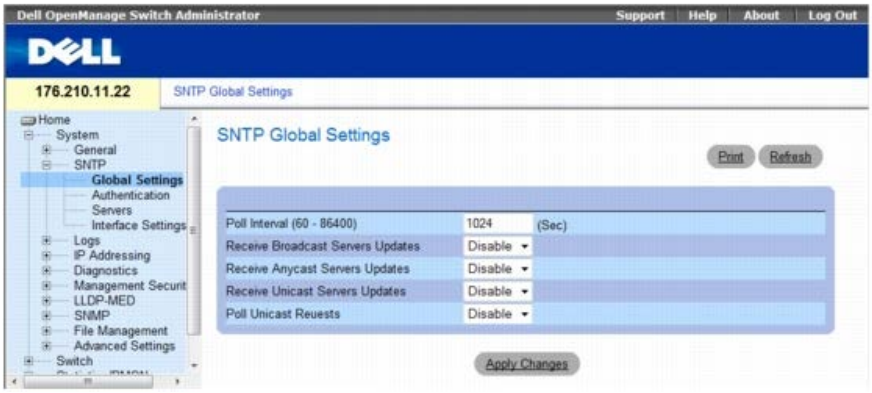
本項には、次のトピックがあります。

- SNTP グローバル設定の定義
- SNTP 認証方法の定義
- SNTP サーバーの定義
- SNTP インタフェースの定義

SNTP グローバル設定の定義

SNTP グローバル設定ページは、SNTP パラメーターをグローバルに定義するための情報を提供します。**SNTP Global Settings**（SNTP グローバル設定）ページを開くには、ツリー表示で、**System**（システム）® **SNTP** ® **Global Settings**（グローバル設定）の順にクリックします。

図 **6-10. SNTP** グローバル設定



SNTP Global Settings（SNTP 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。

- **Poll Interval**（**60-86400**）（ポーリング間隔（60～86400））— SNTP サーバーがユニキャスト情報のためにポーリングされる間隔（秒単位）を定義します。デフォルトでは、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アップデートの受信）— 有効にすると、選択したインタフェースに関するブロードキャストサーバーのタイム情報を得るために SNTP サーバーをリッスンします。
- **Receive Anycast Servers Updates**（エニキャストサーバーアップデートの受信）— 有効なとき、エニキャストサーバータイム情報により SNTP サーバーをポーリングします。エニキャストサーバーアップデートの受信およびブロードキャストサーバーアップデートの受信フィールドの両方が有効な場合、システムタイムはエニキャストサーバータイム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アップデートの受信）— 有効なとき、ユニキャストサーバータイム情報により SNTP サーバーをポーリングします。ブロードキャストサーバーアップデートの受信、 エニキャストサーバーアップデートの受信、およびユニキャストサーバーアップデートの受信フィールドのすべてが有効な場合、システムタイムはユニキャストサーバータイム情報に従って設定されます。
- **Poll Unicast Requests**（ユニキャスト要求のポーリング）— 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。

SNTP グローバル設定の定義

□□□ **SNTP Global Settings**（SNTP グローバル設定）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。

SNTP 設定の変更が適用されます。

CLI コマンドを使用した SNTP グローバル設定の定義

次の表は、**SNTP Global Settings**（SNTP グローバル設定）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

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 エニーキャストクライアントを有効にします。
sntp unicast client enable	SNTP 事前定義ユニキャストクライアントを有効にします。

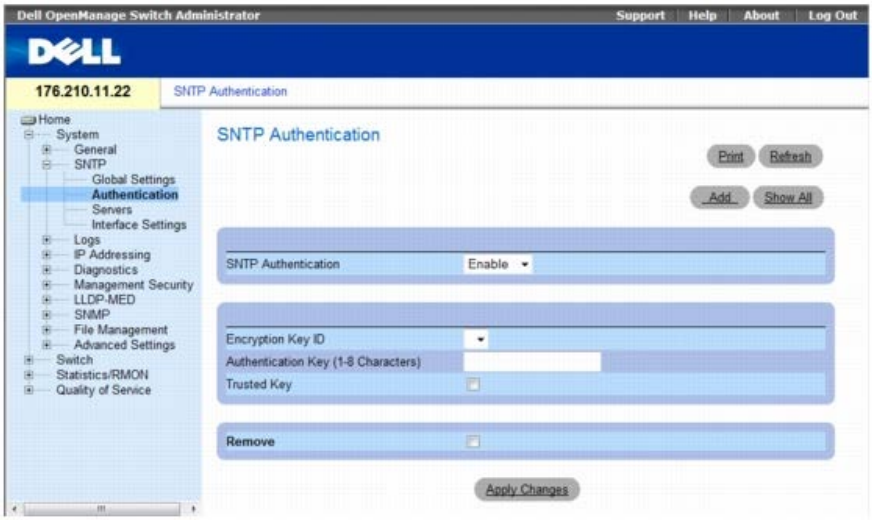
CLI コマンドの例は次のようになります。

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

SNTP 認証方法の定義

SNTP Authentication（SNTP 認証）ページはデバイスと SNTP サーバー間の SNTP 認証を有効にします。また、SNTP サーバーが認証される方法は **SNTP Authentication**（SNTP 認証）ページで選択されます。ツリー表示の **System**（システム）® **SNTP** ® **Authentication**（認証）をクリックして、**SNTP Authentication**（SNTP 認証）ページを開きます。

図 **6-11. SNTP** 認証



SNTP Authentication（SNTP 認証）ページには、以下のフィールドがあります。

- **SNTP Authentication**（SNTP 認証）— デバイスと SNTP サーバーの間の SNTP セッションの認証を有効または無効にします。
  - **Enable**（有効）— デバイスと SNTP サーバーの間の SNTP セッションが認証されます。
  - **Disable**（無効）— デバイスと SNTP サーバーの間の SNTP セッションの認証を無効にします。
- **Encryption Key ID**（暗号化キー ID）— SNTP サーバーとデバイスを認証するために使用されるキーの ID を定義します。フィールド値は最大 4,294,967,295 です。
- **Authentication Key**（**up to 8 Characters**）（認証キー（1～8 文字））— 認証に使用されるキーです。
- **Trusted Key**（トラストキー）— SNTP サーバーの認証に暗号キーが使用されている（ユニキャスト）かどうかを示します。
  - **Checked**（チェックマークあり）— 暗号化キーが使用されています。
  - **Unchecked**（チェックマークなし）— 暗号化キーは使用されていません。
- **Remove**（削除）— 選択した認証キーが削除されます。
  - **Checked**（チェックマークあり）— 選択された暗号化キー ID を削除します。
  - **Unchecked**（チェックマークなし）— 暗号化キー ID を保持します。これがデフォルト値になっています。

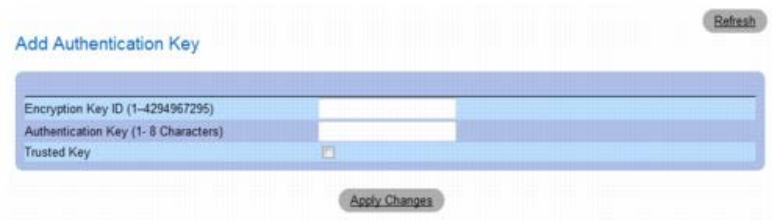
SNTP 認証キーの追加

□□□ **SNTP Authentication**（SNTP 認証）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add Authentication Key（認証キーの追加）ページが開きます。

図 **6-12.** 認証キーの追加



□□□ 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。

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 Authentication**（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。

Authentication Key Table（認証キー表）が開きます。

図 **6-13.** 認証キー表

認証キーの削除

□□□ **SNTP Authentication**（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。

Authentication Key Table（認証キー表）が開きます。

□□□ **Authentication Key Table**（認証キー表）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 SNTP 認証設定の定義

次の表は、 **SNTP Authentication**（SNTP 認証）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

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 ID を認証します。
sntp authentication-key *number* **md5** *value*	SNTP の認証キーを定義します。

CLI コマンドの例は次のようになります。

```
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 Servers**（SNTP サーバー）ページで実行できます。**SNTP Servers**（SNTP サーバー）ページを開くには、ツリー表示で、**System**（システム）® **SNTP** ® **Servers**（サーバー）の順にクリックします。

図 **6-14. SNTP** サーバー

SNTP Servers（SNTP サーバー）ページには、以下のフィールドがあります。

- **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 つの SNTP サーバーを定義できます。
- **Poll Interval**（ポーリング間隔）— 有効にすると、選択された SNTP サーバーのシステムタイム情報に対してポーリングを行います。
- **Encryption Key ID**（暗号化キー ID）— SNTP サーバーとデバイスとの間で通信するために使用されるキー ID を示します。その範囲は 1～4294967295 です。
- **Preference**（プリファランス）— SNTP システムタイム情報を提供する SNTP サーバーです。可能な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は 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は 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です。可能なフィールド値は次のとおりです。
  - **Up**（アップ）— SNTP サーバーは現在正常に動作しています。
  - **Down**（ダウン）— SNTP サーバーは現在使用できません。たとえば、SNTP サーバーは現在接続されていないか、ダウンしています。
  - **In progress**（処理中）— SNTP サーバーは現在、SNTP 情報を送信または受信中です。
  - **Unknown**（不明）— 現在送信中の SNTP 情報の進捗状況は不明です。たとえば、デバイスは現在、インタフェースを探しています。
- **Last Response**（最後の応答）— SNTP サーバーから受信した最後の応答です。
- **Offset**（**msec**）（オフセット（ミリ秒））— デバイスのローカルクロックと SNTP サーバーから取得した時刻のタイムスタンプの差です。
- **Delay**（**msec**）（ディレイ（ミリ秒））— SNTP サーバーに到達するまでの時間です。
- **Remove**（削除）— 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。
  - **Checked**（チェックマークあり）— 選択された SNTP サーバーを削除します。
  - **Unchecked**（チェックマークなし）— 構成の中に SNTP サーバーを保持します。これがデフォルト値になっています。

SNTP サーバーを追加する場合は、次のパラメーターを追加できます。

- **Supported IP Format**（サポートされている IP 形式）— SNTP サーバーでサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— サーバーで IPv6（前述のパラメーターを参照）がサポートされている場合、サポートされている静的アドレスのタイプを指

定します。可能な値は以下のとおりです。

- **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
- **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。

- **Link Local Interface**（リンクローカルインタフェース）— サーバーで IPv6 リンクローカルアドレス（前述のパラメーターを参照）がサポートされている場合、リンクローカルインタフェースを指定します。可能な値は以下のとおりです。
  - **VLAN1** — IPv6 インタフェースは、VLAN1 で設定されています。
  - **ISATAP** — IPv6 インタフェースは、ISATAP トンネルで設定されています。

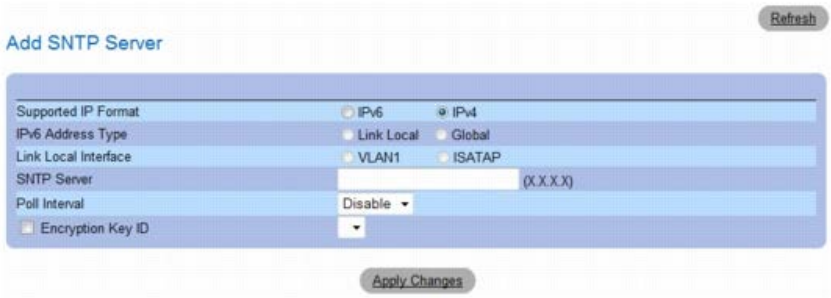
SNTP サーバーの追加

□□□ **SNTP Servers**（SNTP サーバー）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add SNTP Server（SNTP サーバーの追加）ページが開きます。

図 **6-15. SNTP** サーバーの追加



□□□ 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。

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。

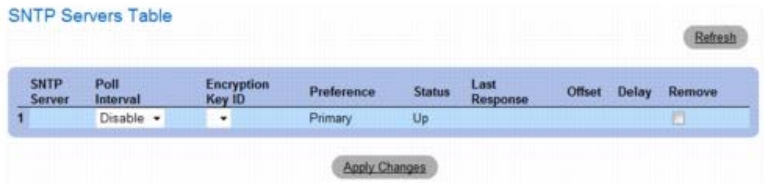
SNTP サーバー表の表示

□□□ **SNTP Servers**（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 Servers Table（SNTP サーバー表）が開きます。

図 **6-16. SNTP** サーバー表



SNTP サーバーの変更

□□□ **SNTP Servers**（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 Servers Table（SNTP サーバー表）が開きます。

□□□ SNTP サーバーエントリを選択します。

□□□ 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 サーバー情報がアップデートされます。

SNTP サーバーの削除

□□□ **SNTP Servers**（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 Servers Table（SNTP サーバー表）が開きます。

□□□ **SNTP Server**（SNTP サーバー）_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 SNTP サーバーの定義

次の表は、**SNTP Server**（SNTP サーバー）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
sntp server *pv4-address*|*ipv6-address*|*hostname* [**poll**] [**key** *keyid*]	SNTP を使用してサーバーに SNTP トラフィックを要求したり、サーバーから SNTP トラフィックを受け取るようにデバイスを設定します。

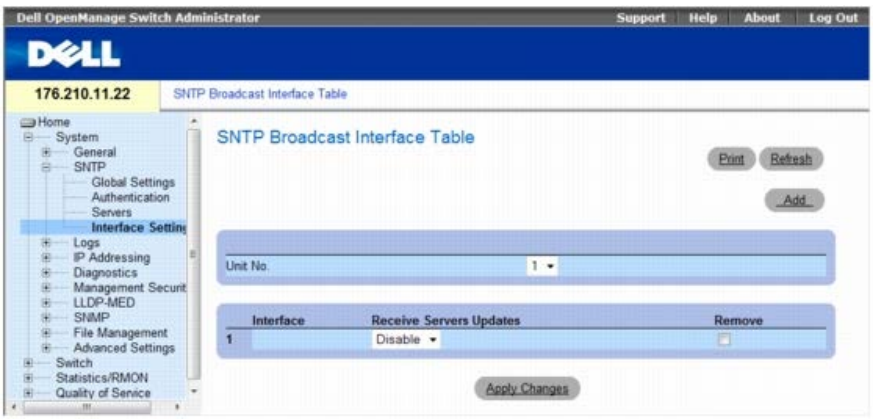
CLI コマンドの例は次のようになります。

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

SNTP インタフェースの定義

SNTP Broadcast Interface Table（SNTP ブロードキャストインタフェース表）ページには、SNTP インタフェース情報が表示されます。**SNTP Broadcast Interface Table**（SNTP ブロードキャストインタフェース表）ページを開くには、**System**（システム）® **SNTP** ® **Interface Settings**（インタフェース設定）の順にクリックします。

図 **6-17. SNTP** ブロードキャストインタフェース表



SNTP Broadcast Interface Table（**SNTP** ブロードキャストインタフェース表）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）— 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が含まれています。

- **Receive Servers Updates**（サーバーアップデートの受信）— 特定インタフェースの SNTP を有効または無効にします。
  - **Enable**（有効）— インタフェースによる SNTP トラフィックからのアップデート受信を有効にします。
  - **Disable**（無効）— インタフェースは SNTP トラフィックからアップデートを受信しません。
- **Remove**（削除）— 指定のインタフェースから SNTP を削除します。
  - **Checked**（チェックマークあり）— SNTP インタフェースエントリを削除します。
  - **Unchecked**（チェックマークなし）— SNTP インタフェースエントリを保持します。

SNTP インタフェースの追加

□□□ **SNTP Broadcast Interface Table**（SNTP ブロードキャストインタフェース表）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add SNTP Interface（SNTP インタフェースの追加）ページが開きます。

図 **6-18. SNTP** インタフェースの追加

□□□ 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

次の表は、**SNTP** ブロードキャストインタフェース表に表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
sntp client enable	インタフェースで 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）の設定を示します。

以下は、SNTP インタフェースを表示する CLI コマンドの例です。

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

Logs（ログ）ページには様々なログページへのリンクがあります。**Logs**（ログ）ページを開くには、ツリー表示の **System**（システム）® **Logs**（ログ）をクリックします。

本項には、次のトピックがあります。

- グローバルログパラメーターの定義
- RAM ログ表の表示
- ログファイル表の表示
- デバイスのログインヒストリの表示

- リモートログサーバー定義の変更

グローバルログパラメーターの定義

システムログは、デバイスのイベントをリアルタイムで表示し、後で使用するために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、エラーまたは情報メッセージを報告します。

イベントメッセージには、あらゆるエラー報告用のシステムログプロトコル推奨メッセージ形式のように、固有の形式があります。例えば、Syslog およびローカルデバイス報告メッセージには重要度コードが割り当てられ、メッセージを発しているソースアプリケーションを識別するメッセージ記憶コードが含まれます。それによりメッセージはその緊急性または関連性に基づいてフィルタリングされます。ログバッファー、ログファイル、またはシスログサーバーのようなさまざまな宛先へのログメッセージの配信は、シスログ設定のパラメーターによってコントロールされます。最大で 8 つの Syslog サーバーを定義できます。

以下の表にログの重要度レベルを示します。

- **Emergency**（緊急）— 最も高い警告レベルです。デバイスがダウンしているか、または適切に機能していない場合は、緊急ログメッセージが指定のロギングロケーションに保存されます。
- **Alert**（警戒）— 二番目に高い警告レベルです。例えば、すべてのデバイスの機能がダウンしているなど、デバイスの重大な誤動作がある場合は警告ログが保存されます。
- **Critical**（深刻）— 三番目に高い警告レベルです。例えば、2 つのデバイスポートが機能していないが残りのデバイスポートは機能しているなど、デバイスの深刻な誤動作がある場合は深刻ログが保存されます。
- **Error**（エラー）— 1 つのポートがオフラインの場合のような、デバイスエラーが発生しています。
- **Warning**（警告）— 最も低いレベルのデバイス警告です。デバイスは機能していますが、動作上の問題が発生しています。
- **Notice**（注意）— デバイス情報を提供します。
- **Informational**（情報提供）— デバイス情報を提供します。
- **Debug**（デバッグ）— デバッグメッセージを提供します。

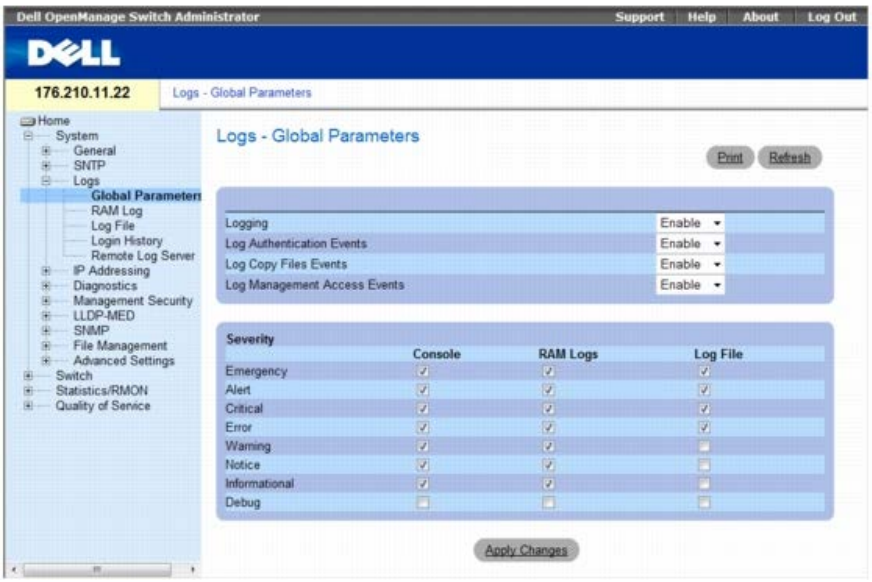
表 **6-13** ログ重要度レベル

重要度タイプ	重要度レベル	説明
Emergency（緊急）	0	システムは機能していません。
Alert（警告）	1	システムは速やかな対応を必要としています。
Critical（深刻）	2	システムは深刻な状態です。
Error（エラー）	3	システムエラーが発生しました。
Warning（警告）	4	システム警告が発生しました。
Notice（注意）	5	システムは適切に機能していますが、システム注意が発生しました。
Informational（情報提供）	6	デバイス情報を提供します。
Debug（デバッグ）	7	ログについての詳細情報を提供します。デバッグエラーが発生した場合、Dell オンラインテクニカルポートへ連絡してください。

Logs - Global Parameters（ログ - グローバルパラメーター）ページには、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があります。これにはログをグローバルに有効化するフィールド、およびログパラメーターを定義するフィールドがあります。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リストされています。

Logs - Global Parameters（ログ - グローバルパラメーター）ページを開くには、ツリー表示で、**System**（システム）® **Logs**（ログ）® **Global Parameters**（グローバルパラメーター）の順にクリックします。

図 **6-19.** ログ **-** グローバルパラメーター



Logs - Global Parameters（ログ - パラメーター）ページには、以下のパラメーターがあります。

- **Logging**（ログ）— キャッシュ、ファイル、およびサーバーのログのため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になります。
- **Log Authentication Events**（認証イベントのログ）— ユーザーが認証されるときのログ生成を有効または無効にします。
- **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るときのログ生成を有効または無効にします。
- **Log Management Access Events**（管理アクセスイベントのログ）— 管理方法を使用してデバイスがアクセスされたときのログ生成を有効または無効にします。たとえば、SSH を使ってデバイスがアクセスされるごとに、デバイスログが生成されます。
- **Severity**（重要度）— 重要度ログを表示します。以下に重要度ログレベルを示します。重要度レベルが選択されると、選択され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。
    - **Emergency**（緊急）— 最も高い警告レベルです。デバイスがダウンしているか、または適切に機能していない場合は、緊急ログメッセージが指定のロギングロケーションに保存されます。
    - **Alert**（警戒）— 二番目に高い警告レベルです。たとえば、存在しない設定ファイルのダウンロード試行など、重大なデバイスの誤動作が生じた場合、Alert（警告）ログが保存されます。
    - **Critical**（深刻）— 三番目に高い警告レベルです。例えば、2 つのデバイスポートが機能していないが残りのデバイスポートは機能しているなど、デバイスの深刻な誤動作がある場合は深刻ログが保存されます。
    - **Error**（エラー）— たとえば、コピー操作の失敗など、デバイスエラーが発生しました。
    - **Warning**（警告）— 最も低いレベルのデバイス警告です。たとえば、デバイスは機能しているが、ポートリンクが現在ダウンしている場合に生成されます。
    - **Notice**（注意）— 重要なデバイス情報を提供します。
    - **Informational**（情報提供）— デバイス情報を提供します。たとえば、ポートが現在動作中などです。
    - **Debug**（デバッグ）— デバッグメッセージを提供します。

Global Log Parameters（グローバルログパラメーター）ページには、個別のログシステムに対応するチェックボックスもあります。

- **Console**（コンソール）— コンソールにログが送られる最低の重要度レベルです。
- **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小の重要度レベルです。
- **Log File**（ログファイル）— フラッシュメモリにあるログファイルにログが送られる最小の重要度レベルです。

ログの有効化

□□□ **Global Log Parameters page**（グローバルログパラメーターページ）を開きます。

□□□ **Logging**（ロギング）ドロップダウンリストの **Enable**（有効化）を選択します。

□□□ **Global Log Parameters**（グローバルログパラメーター）チェックボックスのログタイプおよびログの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。

CLI コマンドを使用したログの有効化

次の表は、 **Global Log Parameters**（グローバルログパラメーター）ページに表示されているフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
logging on	エラーメッセージのロギングを有効にします。
logging {*ipv4-address* | *ipv6-address* | *hostname*} [**port** *port*] [**severity** *level*] [**facility** *facility*][**description** *text*]	syslog サーバーにメッセージを記録します。重要度レベルのリストについては、 ログ重要度レベルを参照してください。
logging console *level*	重要度に基づいて、コンソールに記録されるメッセージを制限します。
logging buffered *level*	重要度に基づいて、内蔵のバッファ（RAM）から表示される syslog メッセージを制限します。
logging file *level*	重要度レベルに基づいて、ログファイルに送られる syslog メッセージを制限します。
clear logging	ログをクリアします。
clear logging file	ログファイルからのメッセージをクリアします。
show syslog servers	シスログサーバーの設定を表示します。

CLI コマンドの例は次のようになります。

```
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

Console# show syslog-servers
デバイスの構成
------------------------------
IP
address     Port  facility  Severity  Description
----------     ----  --------  --------  ----
-------
  1.1.1.1       514 local7    info
fe80::11%vlan1  514 local7    info
  3211::22      514 local7    info
```

RAM ログ表の表示

RAM Log Table（RAM ログ表）には、ログが入力された時刻、重要度レベル、およびログの説明など、RAM に保存されているログエントリについての情報があります。**RAM Log Table**（RAM ログ表）を開くには、ツリー表示の **System**（システム）® **Logs**（ログ）® **RAM Log**（RAM ログ）をクリックします。

図 **6-20 RAM** ログ表

RAM Log Table（**RAM** ログ表）には、以下のフィールドがあります。

- **Log Index**（ログ索引）— **RAM Log Table**（RAM ログ表）の中のログ番号です。
- **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 Log Table**（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 ログ表の表示およびクリア

次の表は、**RAM Log Table**（RAM ログ表）にあるフィールドを表示およびクリアするための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
show logging	内蔵のバッファに保存されているロギングの状態および syslog メッセージを表示します。
clear logging	ログをクリアします。

CLI コマンドの例は次のようになります。

```
console# show logging
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 124 Logged, 124 Displayed, 200 Max.
File Logging: Level error. File Messages: 164 Logged, 126 Dropped.
3 messages were not logged
Application filtering control
Application Event Status
AAA Login Enabled
File system Copy Enabled
File system Delete-Rename Enabled
Management ACL Deny Enabled


01-Jan-2000 09:23:34 :%Box-I-PS-STAT-CHNG: PS# 1 status is - operational.
01-Jan-2000 09:23:29 :%Box-W-PS-STAT-CHNG: PS# 1 status is - not operational.
01-Jan-2000 09:22:44 :%Box-I-PS-STAT-CHNG: PS# 1 status is - operational.
01-Jan-2000 09:22:39 :%Box-W-PS-STAT-CHNG: PS# 1 status is - not operational.
01-Jan-2000 09:10:34 :%Box-I-PS-STAT-CHNG: PS# 1 status is - operational.
01-Jan-2000 09:10:29 :%Box-W-PS-STAT-CHNG: PS# 1 status is - not operational.
01-Jan-2000 09:09:16 :%AAA-I-CONNECT: New http connection for user admin, source 192.168.102.5
destination 192.168.102.15 ACCEPTED
01-Jan-2000 08:39:49 :%Box-I-PS-STAT-CHNG: PS# 1 status is - operational.
```

ログファイル表の表示

Log File Table（ログファイル表）には、ログが入力された時間、ログの重要度、およびログメッセージの説明など、フラッシュ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あります。**Log File Table**（ログファイル表）を開くには、ツリー表示で、**System**（システム）® **Logs**（ログ）® **Log File**（ログファイル）の順にクリックします。

図 **6-21** ログファイル表

Log File Table（ログファイル表）には、以下のフィールドがあります。

- **Log Index**（ログ索引）— ログファイル表の中のログ番号です。
- **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です。

CLI コマンドを使用したログファイル表の表示

次の表は、**Log File Table**（ログファイル表）にあるフィールドを、表示および設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
show logging file	ロギングファイルに保存されているロギング状態および syslog メッセージを表示します。
clear logging file	ログファイルからのメッセージをクリアします。

CLI コマンドの例は次のようになります。

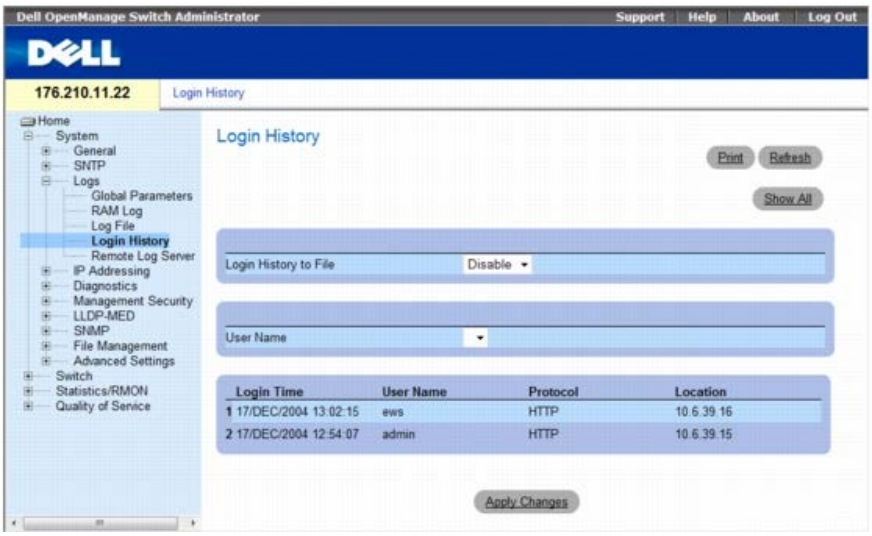
```
console# show logging file
Logging is enabled.
Console Logging: Level info. Console Messages: 0 Dropped.
Buffer Logging: Level info. Buffer Messages: 62 Logged, 62 Displayed, 200 Max.
File Logging: Level debug. File Messages: 11 Logged, 51 Dropped.
SysLog server 12.1.1.2 Logging: warning. Messages： 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
```

デバイスのログインヒストリの表示

Login History（ログインヒストリ）ページには、ユーザーがログインした時刻やデバイスへのログオンに使用されたプロトコルなど、デバイス利用率の表示およびモニタリングに必要な情報があります。

Login History（ログインヒストリ）ページを開くには、ツリー表示の **System**（システム）® **Logs**（ログ）® **Login History**（ログインヒストリ）をクリックします。

図 **6-22.** ログインヒストリ



Login History（ログインヒストリ）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）— ユーザー定義デバイスのユーザー名のリストがあります。
- **Login History**（ログインヒストリ）— ログインヒストリログが有効かどうかを示します。
- **Login Time**（ログイン時刻）— 選択された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へのログオンに使用した手段を示します。
- **Location**（場所）— デバイスにアクセスしたステーションの IP アドレスを示します。

ログインヒストリの表示

□□□ **Login History**（ログインヒストリ）ページを開きます。

□□□ **User Name**（ユーザー名）フィールドの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。

選択した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のログインヒストリの表示

次の表は、**Login History**（ログインヒストリ）ページに表示されるフィールドを表示および設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
show users login-history	パスワード管理のヒストリ情報を表示します。

CLI コマンドの例は次のようになります。

console# **show users login-history**			
Login Time	Username	Protocol	Location
-----------	--------	--------	----------
01-Jan-2005 23:58:17	Anna	HTTP	172.16.1.8
01-Jan-2005 07:59:23	Errol	HTTP	172.16.0.8
01-Jan-2005 08:23:48	Amy	Serial	
01-Jan-2005 08:29:29	Alan	SSH	172.16.0.8
01-Jan-2005 08:42:31	Bob	HTTP	172.16.0.1
01-Jan-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

Remote Log Server Settings（リモートログサーバーの設定）ページには、使用可能なログサーバーを表示および設定するためのフィールドがあります。さらに、新しいログ

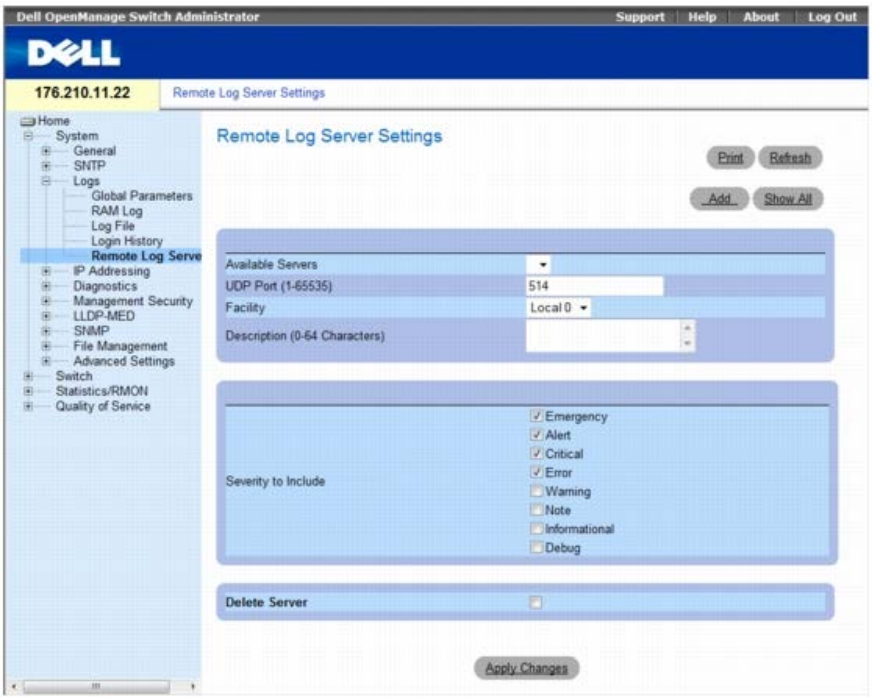
サーバーの定義、および各サーバーへのログ重要度の送信が可能です。

このページには、イベントの重要度レベルが最も高いものから最も低いものへと降順にリストされています。このログに重要度レベルが表示されるように選択すると、このレベル以上の重要度レベルのイベントはすべて、ログに表示されるように自動的に選択されます。セキュリティレベルが選択されていない場合、重要度の低いイベントはログ内に表示されません。

たとえば、Warning（警告）を選択すると、Warning（警告）以上の重要度レベルがすべてログに表示されます。また、セキュリティレベルが Warning（警告）よりも低いイベントはログに表示されません。

Remote Log Server Settings（リモートログサーバー設定）ページを開くには、ツリー表示で、**System**（システム）® **Logs**（ログ）® **Remote Server Settings**（リモートサーバー設定）の順にクリックします。

図 **6-23.** リモートログサーバーの設定



Remote Log Server Settings（リモートログサーバー設定）ページには、以下のフィールドがあります。

- **Available Servers**（使用可能なサーバー）— ログが送られるサーバーのリストがあります。
- **UDP Port**（**1-65535**）（UDP ポート（1-65535））— 選択されたサーバーのログが送られる UDP ポートです。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るユーザー定義のアプリケーションを定義します。ファシリティは 1 つのサーバーに 1 つだけ割り当てることができます。2 つ目のファシリティレベルを割り当てる場合は、最初のファシリティレベルはオーバーライドされます。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利用します。このフィールドのデフォルト値は Local 7（ローカル 7）です。可能なフィールド値を以下に示します。
  - **Local 0**（ローカル 0）～**Local 7**（ローカル 7）
- **Description**（**0-64 Characters**）（説明（0～64 文字））— ユーザー定義のサーバーの説明
- **Severity to Include**（含める重要度） — 使用可能な重要度レベルを以下に示します。
  - **Emergency**（緊急） —システムは機能していません。
  - **Alert**（警戒） —システムは速やかな対応を必要としています。
  - **Critical**（深刻） — システムは深刻な状態です。
  - **Error**（エラー） — システムエラーが発生しました。
  - **Warning**（警告） — システム警告が発生しました。
  - **Notice**（注意） — システムは適切に機能していますが、システム注意が発生しました。
  - **Informational**（情報提供）— デバイス情報を提供します。
  - **Debug**（デバッグ） — ログについての詳細情報を提供します。デバッグエラーが発生した場合は、カスタマ技術サポートに連絡してください。
- **Delete Server**（サーバーの削除）— 選択されていると、使用可能な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。

ログサーバーを追加する場合は、次のパラメーターを追加できます。

- **Supported IP Format**（サポートされている IP 形式）— サーバーでサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。

- **IPv4** — IP バージョン 4 がサポートされています。

- **IPv6 Address Type**（IPv6 アドレスタイプ）— サーバーで IPv6（前述のパラメーターを参照）がサポートされている場合、サポートされている静的アドレスのタイプを指定します。可能な値は以下のとおりです。
  - **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
  - **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。
- **Link Local Interface**（リンクローカルインタフェース）— サーバーで IPv6 リンクローカルアドレス（前述のパラメーターを参照）がサポートされている場合、リンクローカルインタフェースを指定します。可能な値は以下のとおりです。
  - **VLAN1** — IPv6 インタフェースは、VLAN1 で設定されています。
- **ISATAP** — IPv6 インタフェースは、ISATAP トンネルで設定されています。

ログのサーバーへの送信：

□□□ **Remote Log Server Settings**（リモートログサーバーの設定）ページを開きます。

□□□ **Available Servers**（使用可能なサーバー）ドロップダウンリストからサーバーを選択します。

□□□ フィールドを定義します。

□□□ **Severity to Include**（重要度）チェックボックスのログの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。

新しいサーバーの定義：

□□□ **Remote Log Server Settings**（リモートログサーバーの設定）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add a Log Server（ログサーバーの追加）ページが開きます。

図 **6-24.** ログサーバーの追加

Add a Log Server（ログサーバーの追加）ページには、次のような追加のフィールドがあります。

- **New Log Server IP Address**（新しいログサーバー IP アドレス）— 新しいログサーバーの IP アドレスを定義します。

- 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。

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

リモートログサーバー表の表示：

□□□ **Remote Log Server Settings**（リモートログサーバーの設定）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Log Servers Table（ログサーバー表）ページが開きます。

図 **6-25.** ログサーバー表

Log Servers Table（ログサーバー表）ページからのログサーバーの削除

□□□ **Remote Log Server Settings**（リモートログサーバーの設定）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Log Servers Table（ログサーバー表）ページが開きます。

□□□ **Log Servers Table**（ログサーバー表）エントリを選択します。

□□□ **Remove**（削除）チェックボックスを選択してサーバーを削除します。

□□□ **Apply Changes**（変更の適用）をクリックします。

Log Servers Table（ログサーバー表）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リモートサーバーログの操作

次の表は、リモートログサーバーの操作を行うための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
logging {*ipv4-address*|*ipv6-addres* **|** *hostname*} **[port** *port*] *[**severity** level] [**facility** facility] [**description** text]*	リモートサーバーにメッセージを記録します。
no logging	syslog サーバーを削除します。
show logging	ロギングの状態および syslog メッセージを表示します。

CLI コマンドの例は次のようになります。

```
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 アドレス設定の定義

IP Addressing（IP アドレス設定）ページには、インタフェースおよびデフォルトゲートウェイ IP アドレスを割り当てるためのリンク、およびインタフェースに ARP および DHCP パラメーターを定義するためのリンクがあります。**IP Addressing**（IP アドレス設定）ページを開くには、ツリー表示の **System**（システム）® **IP Addressing**（IP アドレス設定）をクリックします。

本項には、次のトピックがあります。

インターネットプロトコルバージョン 6（IPv6）の設定

このデバイスは、IPv6 対応ホストとしても、IPv4 ホストとしても機能します（デュアルスタックとも呼ばれます）。これにより、純粋な IPv6 ネットワークでも、IPv4/IPv6 統合ネットワークでもデバイス操作が可能です。

IPv4 と IPv6 での主な違いはネットワークアドレスの長さです。IPv4 アドレスの長さは 32 ビットであるのに対し、IPv6 アドレスは 128 ビット長であり、より拡大されたアドレス空間を持つことができます。

IPv6 構文

128 ビットの IPv6 アドレスは、4 桁の 16 進数を 8 グループに分けた形式です。連続するゼロを「ダブルコロン」（::）に置換することにより、省略することができます。IPv6 アドレスの表記は、先行ゼロ列を削除することでさらに簡素化することができます。

IPv6 アドレスはさまざまな形式で挿入することができます。ただし、システムでは、ゼロのグループを「ダブルコロン」に置換し、「先行ゼロ列」を削除する最も省略した形式でアドレスを表示します。

IPv6 プレフィックス

プレフィックス長で指定されたユニキャスト IPv6 アドレスが許可されてはいますが、実際のプレフィックス長は常に 64 ビットであるため、表記する必要はありません。64 ビット未満のプレフィックスは、IPv6 アドレス空間の一部を集約するルートまたはアドレス範囲です。

システムでは、IP アドレスをインタフェースに割り当てるたびに、重複アドレス検出（DAD）アルゴリズムを実行して、アドレスの一意性を確認します。

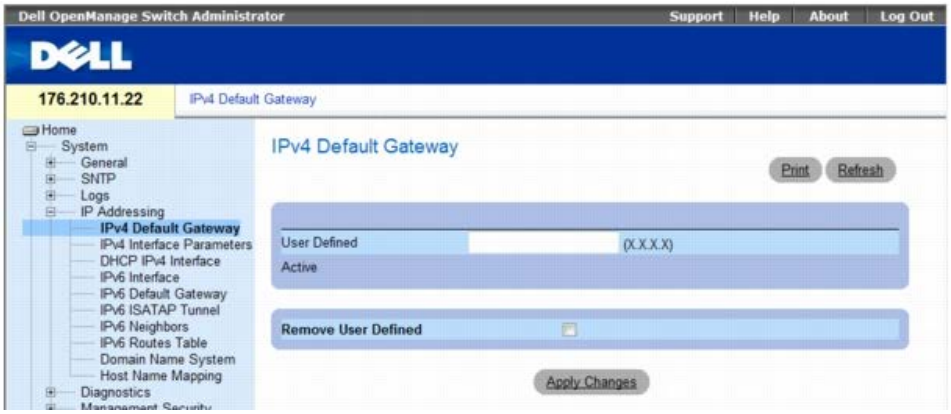
IPv4 環境で IPv6 ノードの通信を行うには、IPv6 専用ノードに中継移行メカニズムが必要となります。実装されているトンネリングメカニズムは、Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）です。このプロトコルは IPv4 ネットワークを IPv6 の仮想ローカルリンクとみなし、各 IPv4 アドレスを IPv6 リンクローカルアドレスへマップします。

IPv4 デフォルトゲートウェイの定義

IPv4 Default Gateway（IPv4 デフォルトゲートウェイ）ページには、ゲートウェイをデバイスに割り当てるためのフィールドがあります。パケットがリモートネットワークに転送されると、パケットはデフォルト IP に送られます。設定された IP アドレスは、IP インタフェースの 1 つの IP アドレスサブネットに属している必要があります。

IPv4 Default Gateway（IPv4 デフォルトゲートウェイ）ページを開くには、ツリー表示で、**System**（システム）® **IP Addressing**（IP アドレス設定）® **IPv4 Default Gateway**（IPv4 デフォルトゲートウェイ）の順にクリックします。

図 **6-26. IPv4** デフォルトゲートウェイ



IPv4 Default Gateway（IPv4 デフォルトゲートウェイ）ページには以下のフィールドがあります。

- **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）— ゲートウェイがアクティブかどうかを示します。
- **Remove User Defined**（ユーザー定義の削除）— デフォルトゲートウェイを削除します。可能なフィールド値は次のとおりです。
  - **Checked**（チェックマークあり）— 選択されたデフォルトゲートウェイを削除します。
  - **Unchecked**（チェックマークなし）— デフォルトゲートウェイを保持します。

デバイスの IPv4 ゲートウェイの選択

□□□ **IPv4 Default Gateway**（IPv4 デフォルトゲートウェイ）ページを開きます。

□□□ **User Defined**（ユーザー定義）フィールドに IP アドレスを入力します。

□□□ チェックボックスの **Active**（アクティブ）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 IPv4 デフォルトゲートウェイデバイスの削除

□□□ **IPv4 Default Gateway**（IPv4 デフォルトゲートウェイ）ページを開きます。

□□□ **Remove User Defined**（ユーザー定義の削除）チェックボックスを選択して、デフォルトゲートウェイを削除します。

□□□ **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 IPv4 ゲートウェイの定義

次の表は、 **Default Gateway**（デフォルトゲートウェイ）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

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。

CLI コマンドの例は次のようになります。

```
Console(config)# ip default-gateway 196.210.10.1
console(config)# no ip default-gateway
```

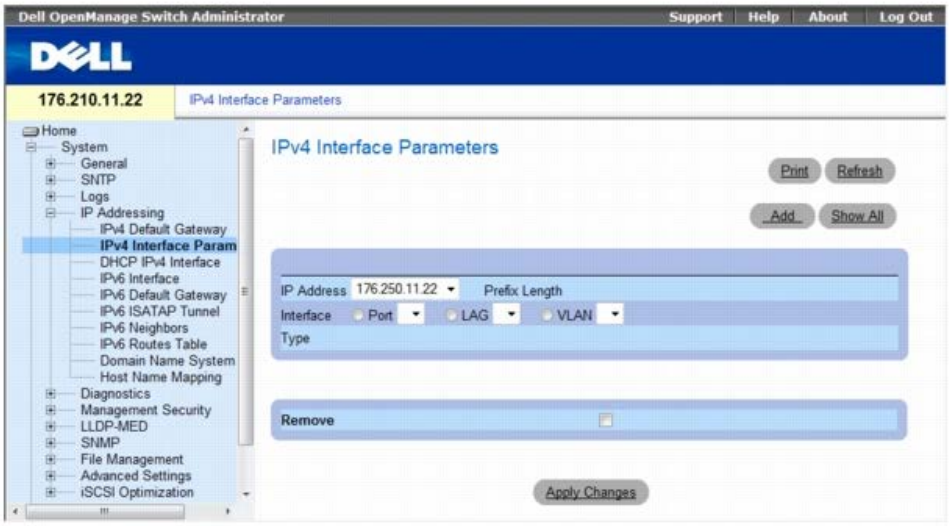
IPv4 インタフェースの定義

IPv4 Interface Parameters（IPv4 インタフェースパラメーター）ページには、IP パラメーターをインタフェースに割り当てるためのフィールドがあります。

IP Interface Parameters （IP インタフェースパラメーター）ページを開くには、ツリー表示で、**System**（システム）® **IP Addressing**（IP アドレス設定）® **IPv4**

Interface Parameters（IPv4 インタフェースパラメーター）の順にクリックします。

図 **6-27. IPv4** インタフェースパラメーター



IP Interface Parameters（IP インタフェースパラメーター）ページには、以下のパラメーターがあります。

- **IP Address**（IP アドレス）— インタフェース IP アドレスです。
- **Prefix Length**（プレフィックス長）— IP アドレスプレフィックスを構成するビット数です。
- **Interface**（インタフェース） — IP アドレスを定義するインタフェースタイプです。ポート、**LAG** または **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どうかを表示します。
- **Remove**（削除）— **IP Address**（IP アドレス）ドロップダウンメニューからインタフェースを削除します。
  - **Checked**（チェックマークあり）— 選択されたインタフェースを削除します。
  - **Unchecked**（チェックマークなし）— 選択されたインタフェースを保持します。

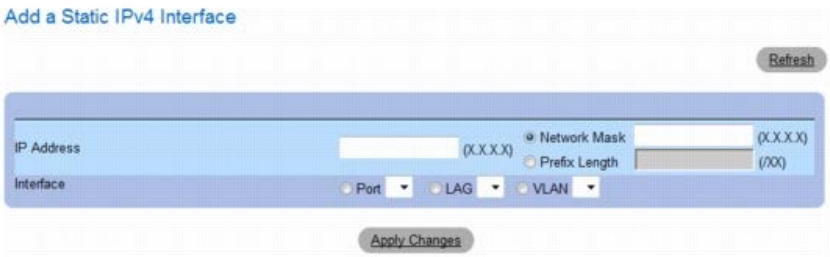
IPv4 IP インタフェースの追加

□□□ **IPv4 Interface Parameters**（IPv4 インタフェースパラメーター）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add a Static IPv4 Interface（静的 IPv4 インタフェースの追加）ページが開きます。

図 **6-28.** 静的 **IPv4** インタフェースの追加



IP Interface Parameters（IP インタフェースパラメーター）ページのパラメーターのほか、**Add a Static IP Interface**（静的 IP インタフェースの追加）ページには、以下のパラメーターがあります。

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

□□□ そのページにある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。

新しい IP アドレスがインタフェースに追加され、デバイスがアップデートされます。

IPv4 アドレスパラメーターの変更

□□□ **IPv4 Interface Parameters**（IPv4 インタフェースパラメーター）ページを開きます。

□□□ **IP Address**（IP アドレス）ドロップダウンメニューから IP アドレスを選択します。

□□□ インタフェースのタイプを変更します。

□□□ **Apply Changes**（変更の適用）をクリックします。

パラメーターが変更され、デバイスがアップデートされます。

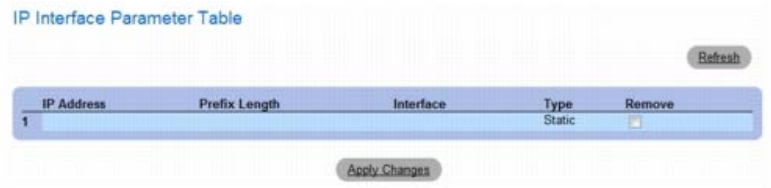
IPv4 アドレスの削除

□□□ **IPv4 Interface Parameters**（IPv4 インタフェースパラメーター）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Interface Parameters Table（インタフェースパラメーター表）ページが開きます。

図 **6-29. IPv4** インタフェースパラメーター表



□□□ IP アドレスを選択し、**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。

選択された 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 IPv4 インタフェースの定義

次の表は、**IPv4 Interfaces Parameters**（IPv4 インタフェースパラメーター）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ip address *ip-address* {*mask* | *prefix-length*}	IP アドレスを設定します。
no ip address [*ip-address*]	IP アドレスを削除します。
show ip interface [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]	IP 用に設定されたインタフェースの使用状況を表示します。

CLI コマンドの例は次のようになります。

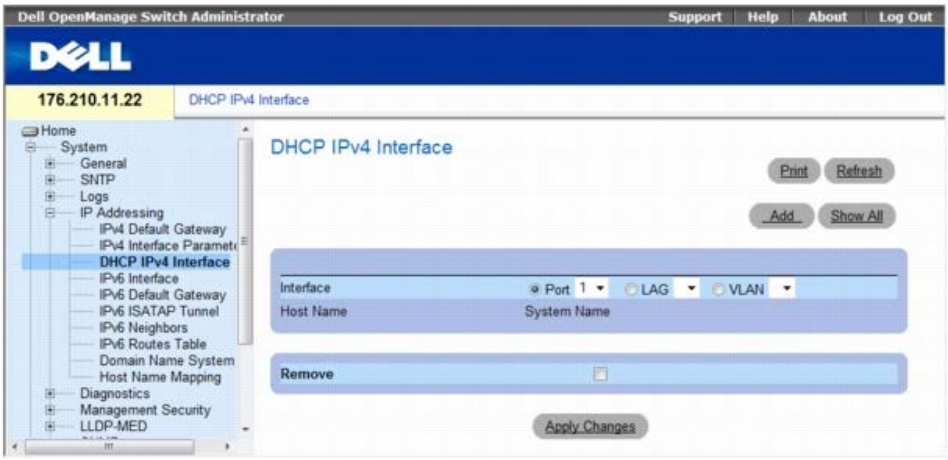
```
console(config)# interface vlan 1
console(config-if)# ip address 92.168.1.123 255.255.255.0
console(config-if)# no ip address 92.168.1.123
console(config-if)# end
console# show ip interface vlan 1
Gateway IP Address Activity status
---------------------- ------------------
192.168.1.1 Active
IP address Interface Type
------------------- ------------ ------------------
192.168.1.123/24 VLAN 1 Static
```

DHCP IPv4 インタフェースパラメーターの定義

DHCP IPv4 Interface（DHCP IPv4 インタフェース）ページには、デバイスインタフェースに DHCP クライアントを定義するためのパラメーターがあります。

DHCP IPv4 Interface（DHCP IPv4 インタフェース）ページを開くには、 ツリー表示で、**System**（システム）® **IP Addressing**（IP アドレス設定）® **DHCP IPv4 Interface**（DHCP IPv4 インタフェース）の順にクリックします。

図 **6-30. DHCP IPv4** インタフェース



DHCP IP Interface（DHCP IP インタフェース）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）— DHCP クライアントインタフェースです。**Port**（ポート）、**LAG**、**VLAN** の横にあるオプションボタンをクリックして、DHCP クライアントインタフェースを選択します。
- **Host Name**（ホスト名）— DHCP サーバーログに書き込まれるシステム名です。このフィールドには 20 文字まで入力できます。
- **Remove**（削除）— 選択されていると、DHCP クライアントを削除します。
  - **Checked**（チェックマークあり）— 選択された DHCP クライアントを削除します。
  - **Unchecked**（チェックマークなし）— 選択された DHCP クライアントを保持します。

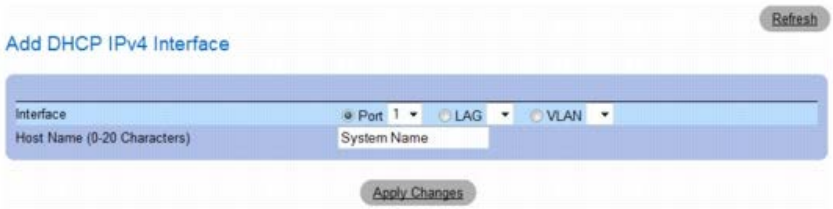
DHCP クライアントの追加

□□□ **DHCP IPv4 Interface**（DHCP IPv4 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。

Add DHCP IPv4 Interface（DHCP IPv4 インタフェースの追加）ページが開きます。

図 **6-31. DHCP IPv4** インタフェースの追加



□□□ そのページにある情報を完成させます。

□□□ **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 IPv4 インタフェースの変更

□□□ **DHCP IPv4 IP Interface**（DHCP IPv4 IP インタフェース）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。

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 IPv4 インタフェースの削除

□□□ **DHCP IPv4 Interface**（DHCP IPv4 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 IPv4 Interface Table（DHCP IPv4 インタフェース表）が開きます。

図 **6-32. DHCP IPv4** インタフェース表

□□□ DHCP クライアント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。

選択され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 IPv4 インタフェースの定義

次の表は DHCP クライアントを定義するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ip address dhcp [**hostname** *host-name*]	動的ホスト構成プロトコル（DHCP）からイーサネットインタフェース上の IP アドレスを取得します。

CLI コマンドの例は次のとおりです。

```
console(config)# interface ethernet 1/e11
console(config-if)# ip address dhcp
```

IPv6 インタフェースの定義

システムでは、IPv6 ホストをサポートしています。**IPv6 Interface**（IPv6 インタフェース）ページには、IPv6 インタフェースを定義するためのフィールドがあります。**IPv6 Interface**（IPv6 インタフェース）ページを開くには、ツリー表示で、**System**（システム）® **IP Addressing**（IP アドレス設定）® **IPv6 Interface**（IPv6 インタフェース）の順にクリックします。

図 **6-33. IPv6** インタフェース

- **Interface**（インタフェース）— 設定で指定されている IPv6 インタフェースです。
- **Remove**（削除）— 選択した場合、インタフェースの IPv6 属性が削除されます。
- **DAD Attempts**（DAD 試行回数）— インタフェース上のユニキャスト IPv6 アドレスで重複アドレス検出（DAD）が実行されている間にこのインタフェースで送信される近隣要請メッセージの連続数を定義します。重複アドレス検出が実行されている間は、新しいアドレスは仮の状態のまま保持されます。フィールド値が 0 の場合、指定インタフェースで処理される重複アドレス検出が無効化されます。フィールド値が 1 の場合、1 回のみの送信となり、再送信されません。範囲は 0～600 であり、デフォルトは 1 です。
- **Autoconfiguration**（自動設定）— インタフェースで IPv6 アドレスの割り当てを行う場合に、ステートレス自動設定を実行するかを指定します。有効にすると、ルーター要請 ND 手順が実行され、RA メッセージで受信したプレフィックスに基づいてインタフェースに IP アドレスを割り当てるためにルーターが検出されます。自動設定を無効にすると、IPv6 グローバルユニキャストアドレスの自動割り当ては実行されず、既存の自動的に割り当てられた IPv6 グローバルユニキャストアドレスがインタフェースから削除されます。デフォルトでは 有効化されています。
- **Send ICMP Unreachable**（ICMP 到達不能メッセージの送信）— ICMPv6 アドレスの到達不能メッセージを送信するかを指定します。有効にすると、TCP/UDP ポートが割り当てられてずにインタフェースに到達した全パケットに対し、到達不能メッセージが生成されます。デフォルトでは 有効化されています。
- **ICMP Error Rate Limit Interval**（ICMP エラーレート制限間隔）— ICMPv6 エラーメッセージにおけるレート制限間隔をミリ秒単位で指定します。このパラメーターの値とバケットサイズパラメーター（以下参照）により、特定の間隔で ICMP エラーメッセージが送信される数が決定します。例えば、レート制限間隔が 100 ミリ秒で、バケットサイズが 10 メッセージの場合は、1 秒ごとに 100 の ICMP エラーメッセージが送信されます。
- **ICMP Error Rate Limit Bucket Size**（ICMP エラーレート制限バケットサイズ）— ICMPv6 エラーメッセージのバケットサイズです。このパラメーターの値と間隔パラメーター（上記参照）により、特定の間隔で ICMP エラーメッセージが送信される数が決定します。例えば、レート制限間隔が 100 ミリ秒で、バケットサイズが 10 メッセージの場合は、1 秒ごとに 100 の ICMP エラーメッセージが送信されます。デフォルトでは、1 秒につき 100 の ICMP エラーメッセージが送信されます。これは、デフォルトの間隔である 100 ミリ秒にデフォルトのバケットサイズ 10 を乗じた数です。
- **IPv6 Address**（IPv6 アドレス）— インタフェースに割り当てられた IPv6 アドレスです。アドレスには、有効な IPv6 アドレス（16 ビットごとにコロンで区切られた 16 進数）を指定する必要があります。IPv6 アドレスは、2031:0:130F:0:0:9C0:876A:130D などの形式となり、これを 2031::0:9C0:876A:130D と圧縮することもできます。システムごとに最高 128 アドレスまでとし、最高 5 つまでの IPv6 アドレス（リンクローカルアドレスを含まない）をインタフェースごとに設定できます。
- **Prefix**（プレフィックス）— IPv6 プレフィックスの長さを指定します。長さとは、アドレスの上位連続ビットの何ビットがプレフィックス（アドレスのネットワーク部）を構成するかを指定する 10 進数値です。Prefix（プレフィックス）フィールドは、グローバル IPv6 アドレスとして定義される静的 IPv6 アドレスのみに適用されます。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— IP アドレスがインタフェースに追加された方法を指定します。可能なフィールド値は次のとおりです。
  - **Link Local**（リンクローカル） — IP アドレスは、リンクローカルであり、ルーティング不能で、同じネットワーク上の通信のみに使用できます。リンクローカルアドレスのプレフィックスは、「FE80」となります。
  - **Global Unicast**（グローバルユニキャスト）— IP アドレスは、異なるサブネットから検出および到達可能な、グローバルに一意の IPv6 ユニキャストアドレスです。
  - **Global Anycast**（グローバルエニキャスト）— IP アドレスは、異なるサブネットから検出および到達可能な、グローバルに一意の IPv6 エニキャストアドレスです。
  - **Multicast**（マルチキャスト）— IP アドレスはマルチキャストです。
- **IPv6 Address Origin Type** （IPv6 アドレスのオリジナルタイプ）— インタフェースに設定可能な静的 IPv6 アドレスのタイプを定義します。可能な値は以下のとおりです。
  - **Dyanmic**（動的） — IP アドレスは RA から受信されたことを示します。

- **Static**（静的）— IP アドレスはユーザーが設定したことを示します。
- **System**（システム）— IP アドレスはシステムで生成されたことを示します。

- **DAD Status**（DAD ステータス）— 挿入された IPv6 アドレスが固有のものであることを検証および確認する処理を行う重複アドレス検出（DAD）のステータスを表示します。これは、次のフィールド値を備えた読み取り専用パラメーターです。
  - **Tentative**（暫定的）— システムにおいて IPv6 重複アドレスの検出処理が実行中であるることを示します。
  - **Duplicate**（重複）— IPv6 アドレスが、ネットワーク上のほかのホストで使用されていることを示します。重複している IPv6 アドレスはサスペンドとなり、トラフィックの送信または受信に使用されません。
  - **Active**（有効）— IPv6 アドレスはアクティブとして設定されていることを示します。
- **Remove**（削除）— 選択した場合、アドレスを表から削除します。

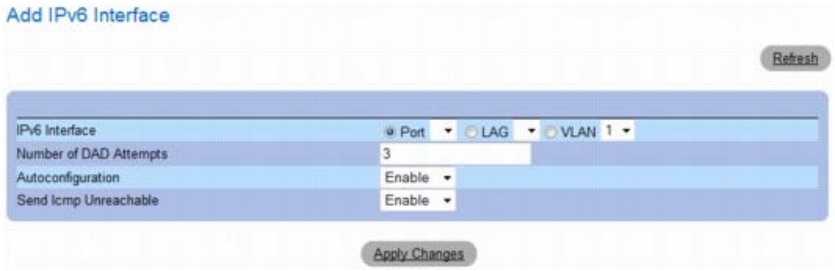
IPv6 インタフェースの追加

□□□ **IPv6 Interface**（IPv6 インタフェース）ページを開きます。

□□□ **Add IPv6 Interface**（IPv6 インタフェースの追加）をクリックします。

Add a Static IPv4 Interface（静的 IPv4 インタフェースの追加）ページが開きます。

図 **6-34. IPv6** インタフェースの追加



□□□ そのページにあるフィールドを完成させます。

IPv6 Interface（IPv6 インタフェース）では、インタフェースが特定のポート、LAG または VLAN であるかを指定します。

□□□ **Apply Changes**（変更の適用）をクリックします。

新しいインタフェースが追加され、デバイスがアップデートされます。

IPv6 アドレスを現在のインタフェースに追加

□□□ **IPv6 Interface**（IPv6 インタフェース）ページを開きます。

□□□ **Add IPv6 Address**（IPv6 アドレスの追加）をクリックします。

Add IPv6 Address（IPv6 アドレスの追加）ページが開きます。

図 **6-35. IPv6** アドレスの追加

□□□ そのページにある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。

新しいアドレスが追加され、デバイスがアップデートされます。

IPv6 インタフェースパラメーターの変更

□□□ **IPv6 Interface**（IPv6 インタフェース）ページを開きます。

□□□ **Interface**（インタフェース）ドロップダウンメニューでインタフェースを選択します。

□□□ 必要な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。

パラメーターが変更され、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 IPv6 インタフェースの定義

次の表は、**IPv6 Interface**（IPv6 インタフェース）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ipv6 enable [**no-autoconfig**]	インタフェースでの IPv6 処理を有効にします。
ipv6 address autoconfig	インタフェースでのステートレス自動設定を使用して、IPv6 アドレスの自動設定を有効にします。
ipv6 icmp error-interval *milliseconds* [*bucketsize*]	IPv6 インターネットコントロールメッセージプロトコル（ICMP）のエラーメッセージに対するレート制限間隔パラメーターおよびパケットサイズパラメーターを設定します。
show ipv6 icmp error-interval	IPv6 ICMP のエラー間隔を表示します。
ipv6 address *ipv6-address/prefix-length* [**eui-64**] [**anycast**]	インタフェースに IPv6 アドレスを設定します。
ipv6 address *ipv6-address* **link-local**	インタフェースに IPv6 リンクローカルアドレスを設定します。
ipv6 unreachables	特定のインタフェースに到達するパケットに対し、Internet Control Message Protocol for IPv6（ICMPv6）の到達不能メッセージが生成されます。
show ipv6 interface [ethernet *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]	IPv6 に設定されたインタフェースの有用性ステータスを表示します。
ipv6 nd dad attempts *attempts-number*	インタフェースのユニキャスト IPv6 アドレスで重複アドレス検出が実行される際にインタフェースに送信される近隣要請メッセージの連続数を設定します。
ipv6 host *name ipv6-address1 [ipv6-address2...ipv6-address4]*	ホスト名キャッシュで、静的なホストのネームツーアドレスマッピングを定義します。
ipv6 set mtu {**ethernet** *interface* | **port-channel** *port-channel-number*} { *bytes* | ***default***}	インタフェースで送信される IPv6 パケットの最大転送単位（MTU）サイズを設定します。
ping {*ipv4-address* | *hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]	IPv4 ICMP エコー要求パケットをネットワーク上のほかのノードに送信します。
ping ipv6 {*ipv6-address* | *hostname*} [**size** *packet_size*] [**count** *packet_count*] [**timeout** *time_out*]	IPv6 ICMP エコー要求パケットをネットワーク上のほかのノードに送信します。

CLI コマンドの例は次のようになります。

```
console# show ipv6 interface vlan 1

Number of ND DAD attempts: 1

MTU size: 1500

Stateless Address Autoconfiguration state: enabled

ICMP unreachable message state: enabled

MLD version: 2


IP addresses          Type      DAD State

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

fe80::232:87ff:fe08:1700 linklayer Active

ff02::1               linklayer N/A

ff02::1:ff08:1700      linklayer N/A


console(config)# ipv6 icmp

error-interval ICMP errors rate limiting

console(config)# ipv6 icmp error-interval

<0-2147483647> The time interval between tokens being placed in the bucket in milliseconds
```

```
console(config)# ipv6 icmp error-interval 100
<1-200>      The maximum number of tokens stored in the bucket
```

IPv6 デフォルトゲートウェイの定義

IPv6 Default Gateway（IPv6 デフォルトゲートウェイ）ページでは、すべてのオフリンクトラフィックのルーターを手動で設定できます。デフォルトのゲートウェイアドレスは、他のネットワークへのアクセスポイントとして機能するインタフェースです。IPv6 の場合、ホストがルーター公示処理でローカルネットワーク上のルーターの存在を自動的に学習できるため、デフォルトゲートウェイの設定は必須ではありません。

IPv4 とは異なり、IPv6 デフォルトゲートウェイでは、最大で単一のユーザー定義の静的アドレスおよびルーター要請メッセージから学習された複数の動的アドレスを含むことができる複数の IPv6 アドレスを設定できます。ユーザー定義のデフォルトゲートウェイは、自動的に公示されるルーターより優先されます。

- IP インタフェースを削除すると、そのデフォルトゲートウェイの IP アドレスはすべて削除されます。
- 動的 IP アドレスは削除することができません。
- 複数のユーザー定義アドレスを設定しようとすると、警告メッセージが表示されます。
- リンクローカル以外のアドレスを設定しようとすると、警告メッセージが表示されます。

IPv6 Default Gateway（IPv6 デフォルトゲートウェイ）ページを開くには、ツリー表示の **System**（システム）® **IP Addressing**（IP アドレス設定）® **IPv6 Default Gateway**（IPv6 デフォルトゲートウェイ）をクリックします。

図 **6-36. IPv6** デフォルトゲートウェイ

- **Default Gateway IP Address**（デフォルトゲートウェイ IP アドレス）— デフォルトゲートウェイのリンクローカル IPv6 アドレスを表示します。
- **Interface**（インタフェース）— デフォルトゲートウェイに到達できる出力インタフェースを指定します。インタフェースとは、ポート、LAG、VLAN および（または）トンネルを指します。
- **Type**（タイプ）— デフォルトゲートウェイが設定された方法を指定します。可能なフィールド値は次のとおりです。
  - **Static**（静的）— デフォルトゲートウェイはユーザー定義されています。
  - **Dynamic**（動的）— デフォルトゲートウェイは動的に設定されています。
- **State**（状態）— デフォルトゲートウェイステータスを表示します。可能なフィールド値は次のとおりです。
  - **Incomplete**（不完全）— アドレス解決が処理中であり、デフォルトゲートウェイのリンク層アドレスが未設定です。
  - **Reachable**（到達可能）— デフォルトゲートウェイが最近（十分の 1 秒以内）到達可能な状態になりました。
  - **Stale**（期限切れ）— デフォルトゲートウェイは到達不可能とされていますが、トラフィックがデフォルトゲートウェイに送信されるまで、その到達可能性の確認が行われません。
  - **Delay**（遅延）— デフォルトゲートウェイは到達不可能とされており、トラフィックがデフォルトゲートウェイに送信された直後です。デフォルトゲートウェイを即座にプローブするより、上位層プロトコルが到達可能性の確認を実行できるように、プローブの送信を短時間ディレイします。
  - **Probe**（プローブ）— デフォルトゲートウェイは到達不可能とされており、到達可能性の確認のためユニキャスト近隣要請プローブが送信されています。
  - **Unreachable**（到達不可）— 到達可能の確認が受信されなかったことを示します。
- **Remove**（削除）— 選択した場合、アドレスをリストから削除します。

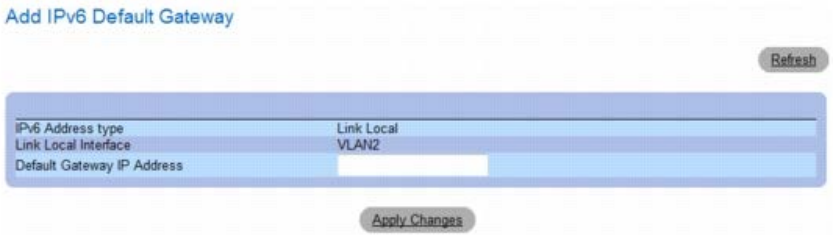
IPv6 デフォルトゲートウェイの追加

□□□ **IPv6 Default Gateway**（IPv6 デフォルトゲートウェイ）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add IPv6 Default Gateway（IPv6 デフォルトゲートウェイの追加）ページが開きます。

図 **6-37. IPv6** デフォルトゲートウェイの追加



□□□ そのページにある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。

新しいゲートウェイが追加され、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 IPv6 デフォルトゲートウェイパラメーターの定義

次の表は、**IPv6 Default Gateway**（IPv6 デフォルトゲートウェイ）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ipv6 default-gateway *ipv6-address*	IPv6 デフォルトゲートウェイを定義します。

IPv6 ISATAP トンネルの定義

IPv6 ISATAP Tunnel（IPv6 ISATAPトンネル）ページでは、IPv4 ネットワークでの伝達を行うために IPv4 パケットに IPv6 パケットをカプセル化するトンネリング処理をデバイスに定義します。

Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）とは、IPv6 インタフェースのトンネリングとして定義される IPv6 移行メカニズムです。IPv4 ネットワーク最上位のデュアルスタックノード間で IPv6 パケットを移行することを目的とします。

トンネリングインタフェースで ISATAP を有効にすると、明示的な IP アドレスはトンネルソース、または最下位の IPv4 アドレスが IP インタフェースに割り当てられている場所に存在する自動モードとして設定されます。このソース IPv4 は、ISATAP アドレス設定規則に準じたトンネルインタフェース識別子を設定するために利用されます。トンネルインタフェースで ISATAP が有効な場合、インタフェースをアクティブな状態にするため、トンネルソースをインタフェースに設定する必要があります。

ISATAP アドレスは、[64-bit prefix]:0:5EFE:w.x.y.z で指定されます。5EFE とは、ISATAP 識別子であり、w.x.y.z はパブリック IPv4 アドレスまたはプライベート IPv4 アドレスを示します。したがって、リンクローカルアドレスは FE80::5EFE:w.x.y.z となります。

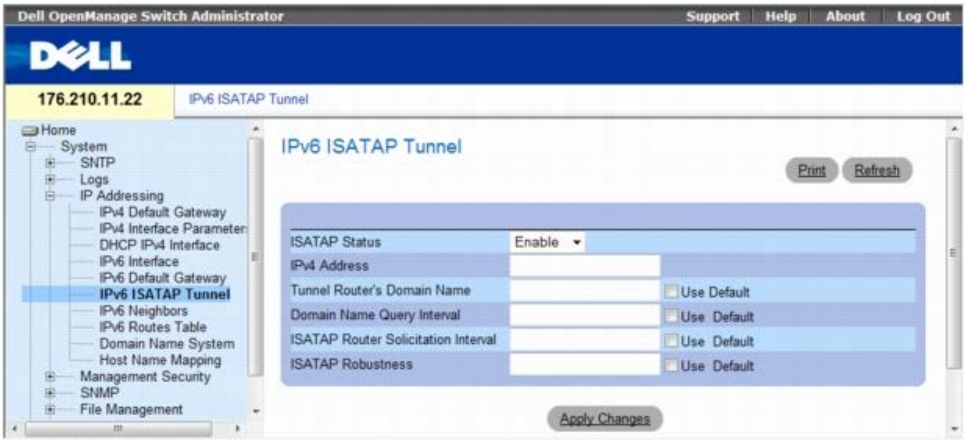
最後の IPv4 アドレスがインタフェースから削除されると、ISATAP IP インタフェースはアクティブではない状態となり、「Down（停止中）」と示されますが、管理状態はアクティブな状態のまま保持されます。

トンネリングを定義する場合は、以下にご注意ください。

- IPv6 リンクローカルアドレスは、ISATAP インタフェースに割り当てられます。最初の IP アドレスがインタフェースに割り当てられ、インタフェースの状態がアクティブになります。
- ISATAP インタフェースがアクティブな場合は、ISATAP 対 IPv4 のマッピングを使用することで、ISATAP ルーター IPv4 アドレスが DNS で解決されます。ISATAP DNS レコードが解決されない場合、ISATAP ホストネームツーアドレスマッピングがホスト名キャッシュで検索されます。
- ISATAP ルーター IPv4 アドレスが DNS プロセスで解決されない場合、ISATAP IP インタフェースのステータスは、Active（アクティブ）な状態で保持されます。システムでは、DNS 処理が解決されるまで ISATAP トラフィックのデフォルトゲートウェイが設定されません。
- ISATAP トンネルを IPv4 ネットワークで適切に動作させるには、ISATAP ルーターを設定する必要があります。

IPv6 ISATAP Tunnel（IPv6 ISATAP トンネル）ページを開くには、ツリー表示の **System**（システム）® **IP Addressing**（IP アドレス設定）® **IPv6 ISATAP Tunnel**（IPv6 ISATAP トンネル）をクリックします。

図 **6-38. IPv6 ISATAP** トンネル



- **ISATAP Status**（ISATAP ステータス）— デバイス上の ISATAP ステータスを指定します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— ISATAP はデバイス上で有効化されています。
  - **Disable**（無効）— ISATAP はデバイス上で無効化されています。これがデフォルト値になっています。
- **IPv4 Address**（IPv4 アドレス）— トンネルインタフェースのローカル（ソース）IPv4 アドレスを指定します。
- **Tunnel Router's Domain Name**（トンネルルーターのドメイン名）— 特定の自動トンネルルータードメイン名を示すグローバルストリングを指定します。デフォルト値は ISATAP です。
  - **Use Default**（デフォルトを使用する）— チェックボックスを選択すると、設定がデフォルトに戻ります。
- **Domain Name Query Interval**（ドメイン名クエリ間隔）— ISATAP ルーターの IP アドレスがわかる前に、自動トンネルルータードメイン名に対する DNS クエリの間隔を指定します。範囲は 10～3600 秒です。デフォルト値は 10 秒です。
  - **Use Default**（デフォルトを使用する）— チェックボックスを選択すると、設定がデフォルトに戻ります。
- **ISATAP Router Solicitation Interval**（ISATAP ルーター要請間隔）— アクティブなルーターがない場合に、ルーター要請メッセージの間隔を指定します。範囲は 10～3600 秒です。デフォルトは 10 です。
  - **Use Default**（デフォルトを使用する）— チェックボックスを選択すると、設定がデフォルトに戻ります。
- **ISATAP Robustness**（ISATAP 堅牢性）— デバイスが送信する DNS クエリまたはルーター要請リフレッシュメッセージの数を指定します。範囲は 1～20 秒です。デフォルトは 3 です。
  - **Use Default**（デフォルトを使用する）— チェックボックスを選択すると、設定がデフォルトに戻ります。

CLI コマンドを使用した IPv6 ISATAP トンネルパラメーターの定義

次の表は、**IPv6 ISATAP Tunnel**（IPv6 ISATAP トンネル）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
interface tunnel *number*	トンネルインタフェース設定モードに入ります。
tunnel mode ipv6ip {isatap}	IPv6 移行メカニズムグローバルサポートモードを設定します。
tunnel isatap router *router_name*	特定の自動トンネルのルータードメイン名を示すグローバルストリングを設定します。
tunnel source { auto | ip-address *ipv4-address* | *interface }*	トンネルインタフェースのローカル（ソース）IPv4 アドレスを設定します。
tunnel isatap query-interval *seconds*	ISATAP ルーターの IP アドレスが通知される前に、自動トンネルルータードメイン名に対する DNS クエリの間隔を設定します。
tunnel isatap solicitation-interval *seconds*	ISATAP ルーター要請メッセージの間隔を設定します（アクティブな ISATAP ルーターが存在しない場合）。
tunnel isatap robustness *number*	デバイスが送信する DNS クエリまたはルーター要請リフレッシュメッセージの数を設定します。
show ipv6 tunnel	ISATAP トンネルの情報を表示します。

CLI コマンドの例は次のようになります。

```
Console> show ipv6 tunnel

Router DNS name: ISATAP

Router IPv4 address: 172.16.1.1

DNS Query interval: 10 seconds
```

Min DNS Query interval: 0 seconds

Router Solicitation interval: 10 seconds

Min Router Solicitation interval: 0 seconds

Robustness: 3

IPv6 近隣の定義

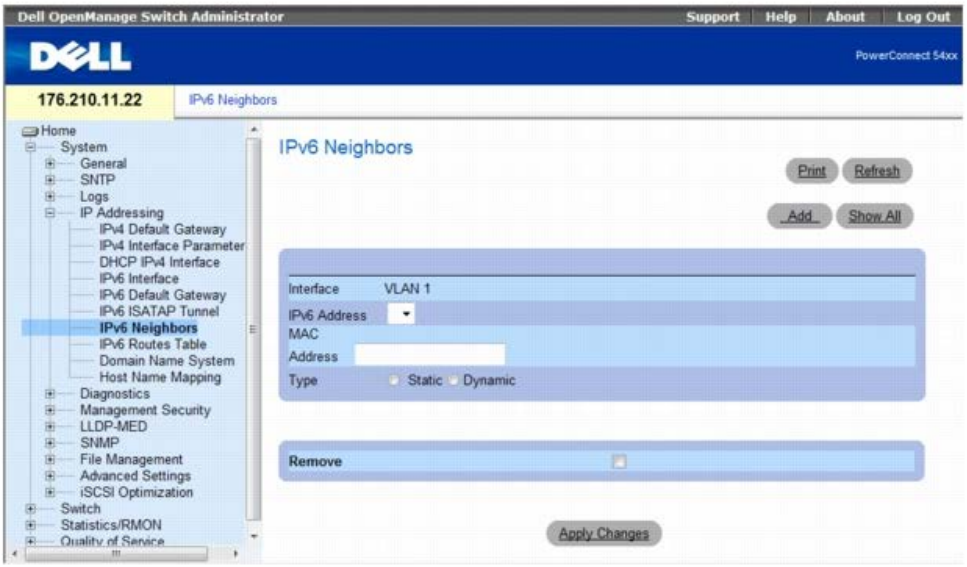
IPv6 Neighbors（IPv6 近隣）ページには、IPv4 アドレス解決プロトコル（ARP）の機能と類似した IPv6 近隣の定義に関する情報が含まれています。IPv6 近隣では、同じサブネット内のリンクローカルアドレスが検出され、アクティブな近隣パスについての到達可能性情報を保持するデータベースが含まれます。

デバイスでは、静的または動的に取得した近隣を最大で 256 までサポートします。

IPv6 インタフェースを削除すると、静的および動的に学習されたすべての近隣が削除されます。

IPv6 Neighbors（IPv6 近隣）ページを開くには、ツリー表示の **System**（システム）® **IP Addressing**（IP アドレス設定）® **IPv6 Neighbors**（IPv6 近隣）をクリックします。

図 **6-39. IPv6** 近隣



- **Interface**（インタフェース）— IPv6 インタフェースが定義されるインタフェースを表示します。インタフェースには、ポート、LAG、または VLAN が含まれます。
- **IPv6 Address**（IPv6 アドレス）— 現在設定されている近隣 IPv6 アドレスを定義します。
- **MAC Address**（MAC アドレス）— インタフェースに割り当てられている MAC アドレスを表示します。
- **Type**（タイプ）— 近隣検出キャッシュ情報のエントリタイプを表示します。可能なフィールド値は次のとおりです。
  - **Static**（静的）— 静的近隣検出キャッシュエントリを示します。指定された IPv6 アドレスのエントリが既に近隣検出キャッシュで存在する場合（IPv6 近隣検出プロセスで学習）、エントリを静的なエントリに変換できます。
  - **Dynamic**（動的）— 動的近隣検出キャッシュエントリを示します。
- **Remove**（削除）— 選択した場合、近隣をリストから削除します。

IPv6 近隣表には、次の追加パラメーターが示されています。

State（状態）— IPv6 近隣のステータスが表示されます。可能なフィールド値は以下のとおりです。

- **Incomplete**（不完全）— アドレス解決が処理中であり、近隣のリンク層アドレスが確定されていません。
- **Reachable**（到達可能）— 近隣が到達可能な状態になった直後です（数十秒以内）。
- **Stale**（期限切れ）— 近隣は到達不可能な状態とされていますが、トラフィックが近隣に送信されるまで、その到達可能性の確認が行われません。
- **Delay**（遅延）— 近隣は到達不可能な状態とされており、トラフィックが近隣に送信された直後です。近隣を即座にプローブするより、上位層プロトコルが到達可能性の確認を実行できるように、プローブの送信を短時間遅延します。
- **Probe**（プローブ）— 近隣は到達不可能な状態とされており、到達可能性の確認のためユニキャスト近隣要請プローブが送信されます。

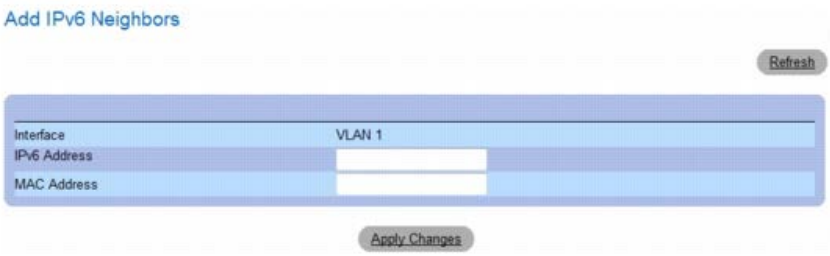
IPv6 近隣の追加

□□□ **IPv6 Neighbors**（IPv6 近隣）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add IPv6 Neighbors（IPv6 近隣の追加）ページが開きます。

図 **6-40. IPv6** 近隣の追加



□□□ そのページにある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。

新しい近隣が追加され、デバイスがアップデートされます。

近隣パラメーターの変更

□□□ **IPv6 Neighbors**（IPv6 近隣）ページを開きます。

□□□ **IPv6 Address**（IPv6 アドレス）ドロップダウンメニューで IP アドレスを選択します。

□□□ 必要な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。

パラメーターが変更され、デバイスがアップデートされます。

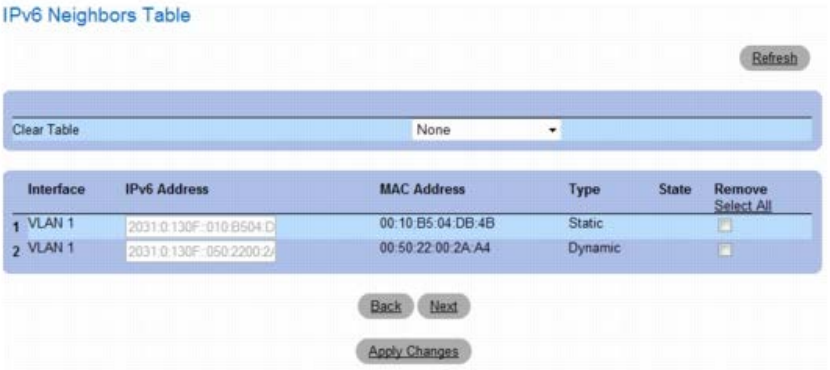
近隣の削除

□□□ **IPv6 Neighbors**（IPv6 近隣）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

IPv6 Neighbors Table（IPv6 近隣表）が開きます。

図 **6-41. IPv6** 近隣表



□□□ 目的のエントリで **Remove**（削除）チェックボックスを選択します。または、**Clear Table**（表のクリア）フィールドで目的の値を選択します。可能なフィールド値は以下のとおりです。

- Static Only（静的のみ）— IPv6 近隣表の静的エントリをクリアします。
- Dynamic Only（動的のみ）— IPv6 近隣表の動的エントリをクリアします。
- All Dynamic and Static（すべての動的および静的）— IPv6 近隣表の静的アドレスおよび動的アドレスのエントリをクリアします。
- None（なし）— エントリはクリアされません。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択された近隣が削除され、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 IPv6 近隣の定義

次の表は、**IPv6 Neighbors**（IPv6 近隣）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ipv6 neighbor *ipv6_addr hw_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number* }	IPv6 近隣検出キャッシュの静的エントリを設定します。
show ipv6 neighbors {static | dynamic}[**ipv6-address** *ipv6-address*] [**mac-address** *mac-address*] [**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*]	IPv6 近隣検出キャッシュの情報を表示します。
clear ipv6 neighbors	IPv6 近隣検出キャッシュのエントリをすべて削除します。

CLI コマンドの例は次のようになります。

```
Console# show ipv6 neighbors dynamic

Interface  IPv6 address            HW address       State

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

VLAN 1     2031:0:130F::010:B504:DBB4   00:10:B5:04:DB:4B  REACH

VLAN 1     2031:0:130F::050:2200:2AA4   00:50:22:00:2A:A4  REACH
```

IPv6 ルーティング表の表示

IPv6 Routes Table（IPv6 ルーティング表）には、IPv6 宛先プレフィックスについての情報と、その到達方法、および直接的または間接的であるかが示されています。このルーティング表は、転送に使用されるネクストホップアドレスおよびインタフェースの決定に使用されます。

また、各動的エントリでは、公示されなくなったエントリの削除に使用される関連の無効タイマー値（ルーター公示から抽出）を保持しています。

IPv6 Routes Table（IPv6 ルーティング表）ページを開くには、ツリー表示の **System**（システム）® **IP Addressing**（IP アドレス設定）® **IPv6 Routes Table**（IPv6 ルーティン表）をクリックします。

図 **6-42. IPv6** ルーティング表

- **IPv6 Address**（IPv6 アドレス）— 宛先 IPv6 アドレスを定義します。
- **Prefix Length**（プレフィックス長）— IPv6 プレフィックスの長さを指定します。Prefix（プレフィックス）フィールドは、IPv6 静的 IP アドレスがグローバル IPv6 アドレスとして定義される場合のみに適用可能です。その範囲は 5～128 です。
- **Interface**（インタフェース）— パケットの転送に使用されるインタフェースを表示します。インタフェースとは、ポート、LAG、VLAN を指します。
- **Next** Hop（ネクストホップ）— パケットが転送されるルート上のアドレスを宛先アドレス（通常は近隣ルーターのアドレス）に定義します。このアドレスは、リンクローカルまたはグローバル IPv6 アドレスのいずれかになります。
- **Metric**（メトリック）— IPv6 ルーティング表で同じ宛先を持つルートの比較に使用される値を示します。この値は、0～255 までの範囲の管理距離です。デフォルト値は 1 です。
- **Life-Time**（ライフタイム） — ルートのライフタイムを示します。
- **Route Type**（ルートタイプ）— 宛先が直接アタッチされているか、およびエントリが学習される方法を表示します。次の値を選択できます。
  - **Local**（ローカル）— 直接接続されているルートエントリです。

Static（静的）— ルートは ND プロセスで学習されます。エントリは自動的に静的エントリへ変換されます。

- **ICMP** — ルートは ICMP メッセージで学習されます。
- **ND** — ルートは RA メッセージで学習されます。

CLI コマンドを使用した IPv6 ルーティング表パラメーターの表示

次の表は、**IPv6 Routes Table**（IPv6 ルーティング表）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
traceroute {*ipv4-address* | *hostname*} [size *packet_size*] [*ttl max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]	IPv4 パケットが各宛先へ送信される際に実際に使用するルートを検出します。
traceroute ipv6 {*ipv6-address* | *hostname*} [**size** *packet_size*] [**ttl** *max-ttl*] [**count** *packet_count*] [**timeout** *time_out*] [**source** *ip-address*] [**tos** *tos*]	IPv6 パケットが各宛先に送信される際に実際に使用するルートを検出します。
show ipv6 route	IPv6 ルーティング表の現在のステータスを表示します。

CLI コマンドの例は次のようになります。

```
Console> show ipv6 route
Codes: L - Local, S - Static, I - ICMP, ND - Router Advertisment
The number in the brackets is the metric.
S ::/0 via fe80::77 [0] VLAN 1 Lifetime Infinite
ND ::/0 via fe80::200:cff:fe4a:dfa8 [0] VLAN 1 Lifetime 1784 sec
L 2001::/64 is directly connected, g2 Lifetime Infinite
L 2002:1:1:1::/64 is directly connected, VLAN 1 Lifetime 2147467 sec
L 3001::/64 is directly connected, VLAN 1 Lifetime Infinite
L 4004::/64 is directly connected, VLAN 1 Lifetime Infinite
L 6001::/64 is directly connected, g2 Lifetime Infinite
```

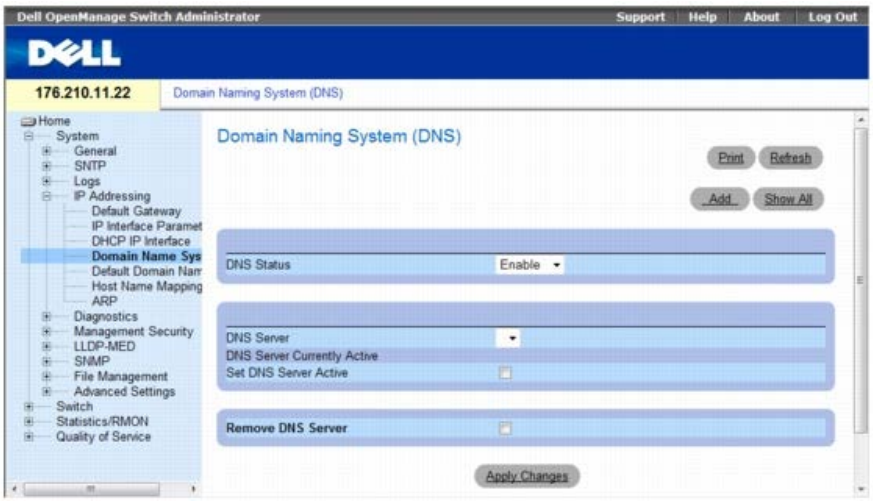
ドメインネームシステムの設定

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 サービスはドメインネームを数字の IP アドレスに翻訳します。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、およびそれに対応する IP アドレスを維持します。

Domain Naming System（**DNS**）（ドメインネームシステム（DNS））ページには、特定の DNS サーバーを有効化およびアクティブにするためのフィールドがあります。

Domain Naming System（DNS）（ドメインネームシステム（DNS））ページを開くには、ツリー表示で、System（システム）® IP Addressing（IP アドレス設定）® Domain Naming System（DNS）（ドメインネームシステム（DNS））の順にクリックします。

図 **6-43.** ドメインネームシステム（**DNS**）



Domain Naming System（**DNS**）（ドメインネームシステム（DNS））ページには、以下のフィールドがあります。

- **DNS Status**（DNS の状態）— DNS 名の IP アドレスへの翻訳を有効または無効にします。

- **DNS Server**（DNS サーバー）— DNS サーバーのリストです。DNS サーバーは **Add DNS Server**（DNS サーバーの追加）ページから追加されます。
- **DNS Server Currently Active**（現在アクティブな DNS サーバー）— 現在アクティブな DNS サーバーです。
- **Set DNS Server Active**（DNS サーバーの有効化）— 選択された DNS サーバーを有効にします。
- **Remove DNS Server**（DNS サーバーの削除）— 選択された DNS サーバーを削除します。
  - **Checked**（チェックマークあり）— 選択された DNS サーバーを削除します。
  - **Unchecked**（チェックマークなし）— 選択された DNS サーバーを保持します。

DNS サーバーを新しく定義する場合は、次のパラメーターを追加できます。

- **Supported IP Format**（サポートされている IP 形式）— サーバーでサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— サーバーで IPv6（前述のパラメーターを参照）がサポートされている場合、サポートされている静的アドレスのタイプを指定します。可能な値は以下のとおりです。
  - **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
  - **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。
- **Link Local Interface**（リンクローカルインタフェース）— サーバーで IPv6 リンクローカルアドレス（前述のパラメーターを参照）がサポートされている場合、リンクローカルインタフェースを指定します。可能な値は以下のとおりです。
  - **VLAN1** — IPv6 インタフェースは、VLAN1 で設定されています。
  - **ISATAP** — IPv6 インタフェースは、ISATAP トンネルで設定されています。

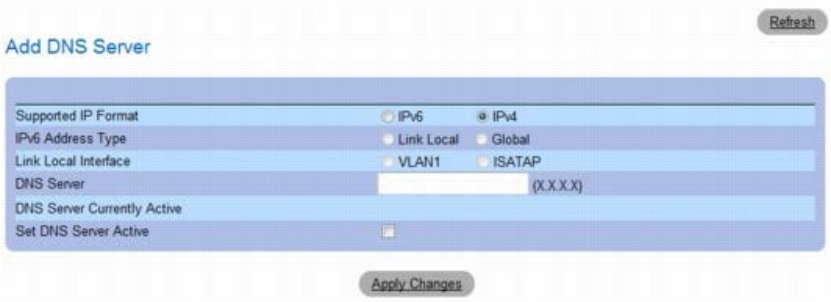
DNS サーバーの追加

□□□ **Domain Naming System**（**DNS**）（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。

Add DNS Server（DNS サーバーの追加）ページが開きます。

図 **6-44 DNS** サーバーの追加



Domain Naming System（**DNS**）（ドメインネームサーバー（DNS））ページのフィールドのほか、**Add DNS Server**（DNS サーバーの追加）ページには、以下のフィールドがあります。

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

□□□ 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。

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

□□□ **Domain Naming System**（**DNS**）（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 **6-45 DNS** サーバー表

DNS サーバーの削除

□□□ **Domain Naming System**（**DNS**）（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）ページが開きます。

□□□ **DNS Server Table**（DNS 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 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 DNS サーバーの設定

次の表は、デバイスシステム情報を設定するための CLI コマンドをまとめたものです。

CLI コマンド	説明
ip name-server *server-address*	使用可能なネームサーバーを設定します。8 個のネームサーバーを設定することができます。
no ip name-server *server-address*	ネームサーバーを削除します。
ip domain-name *name*	無資格の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* **| *}**	ホストのネームツーアドレスキャッシュから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、静的でキャッシュされたホスト名およびアドレスのリストを表示します。
ip domain-lookup	DNS システムに対してホスト名から IP アドレスへの変換を有効にします。

CLI コマンドの例は次のようになります。

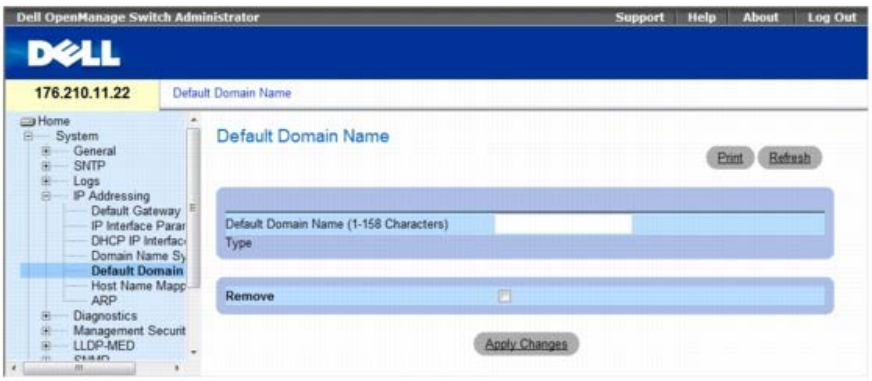
```
console(config)# ip name-server 176.16.1.18
```

デフォルトドメインの定義

Default Domain Name（デフォルトドメインネーム） ページは、デフォルト DNS ドメインネームを定義するための情報を提供します。

Default Domain Name（デフォルトドメインネーム）ページを開くには、**System**（システム）® **IP Addressing**（IP アドレス設定）® **Default Domain Name**（デフォルトドメインネーム）の順にクリックします。

図 **6-46.** デフォルトドメイン名



Default Domain Name（デフォルトドメインネーム）ページには、以下のフィールドがあります。

- **Default Domain Name**（**1-158 characters**）（デフォルトドメインネーム（1～158 文字））— ユーザー定義のデフォルトドメインネームが含まれます。定義されている場合、デフォルトドメインネームは、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ネームが適用されます。
- **Type**（タイプ） — IP アドレスタイプです。可能なフィールド値は次のとおりです。
  - **Dynamic**（動的）— IP アドレスが動的に作成されます。
  - **Static**（静的）— IP アドレスは静的な IP アドレスです。
  - **Remove**（削除）— デフォルトのドメインネームを削除します。
  - **Checked**（チェックマークあり）— 選択されたドメインネームを削除します。
  - **Unchecked**（チェックマークなし）— 選択されたドメインネームを保持します。

CLI コマンドを使用した DNS ドメインネームの定義

次の表は、DNS ドメインネームを設定するための CLI コマンドをまとめたものです。

CLI コマンド	説明
ip domain-name *name*	無資格の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。
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、静的でキャッシュされたホスト名およびアドレスのリストを表示します。

CLI コマンドの例は次のようになります。

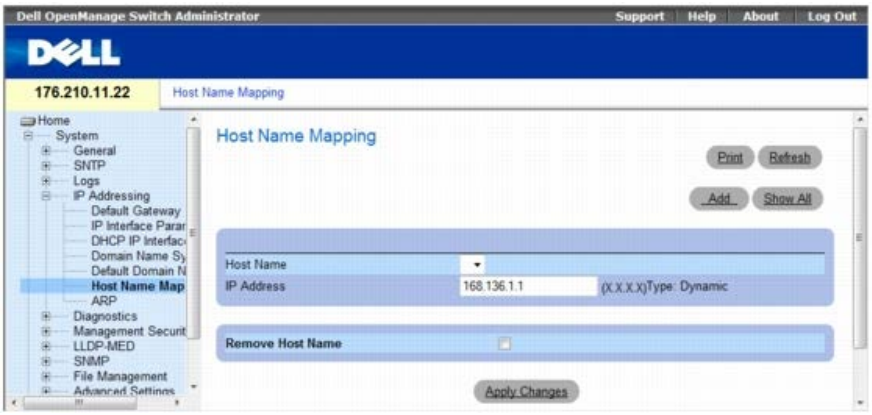
```
console(config)# ip domain-name dell.com
```

ドメインホストのマッピング

Host Name Mapping（ホスト名のマッピング）ページは、静的ホスト名に IP アドレスを割り当てるためのパラメーターを提供します。このページでは、ホストごとに 1 つの IP アドレスを割り当てることができます。

Host Name Mapping（ホスト名のマッピング）ページを開くには、ツリー表示で、**System**（システム）® **IP Addressing**（IP アドレス設定）® **Host Name Mapping**（ホスト名のマッピング）の順にクリックします。

図 **6-47.** ホスト名のマッピング



Host Name Mapping（ホスト名のマッピング）ページには、以下のフィールドがあります。

- **Host Name**（ホスト名）— ホスト名のリストです。ホスト名は **Add Host Name Mapping**（ホスト名のマッピングの追加）ページで定義されます。各ホスト 1 つの IP アドレスを提供します。
- **IP Address**（**X.X.X.X**）（IP アドレス（X.X.X.X））— 特定のホスト名に割り当てられた IP アドレスです。
- **Type**（タイプ） — IP アドレスタイプです。可能なフィールド値は次のとおりです。
  - **Dynamic**（動的）— IP アドレスが動的に作成されます。
  - **Static**（静的）— IP アドレスは静的な IP アドレスです。
- **Remove Host Name**（ホスト名の削除）— DNS ホストのマッピングを削除します。

Checked（チェックマークあり）— DNS ホストのマッピングを削除します。

- **Unchecked**（チェックマークなし）— DNS ホストのマッピングを保持します。

ホスト名のマッピングを新しく定義する場合は、次のパラメーターを追加できます。

- **Supported IP Format**（サポートされている IP 形式）— ホストでサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— ホストで IPv6 がサポートされている場合（前述のパラメーターを参照）、これによりサポートされている静的アドレスのタイプを指定します。可能な値は以下のとおりです。
  - **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
  - **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。
- **Link Local Interface**（リンクローカルインタフェース）— サーバーで IPv6 リンクローカルアドレス（前述のパラメーターを参照）がサポートされている場合、リンクローカルインタフェースを指定します。可能な値は以下のとおりです。
  - **VLAN1** — IPv6 インタフェースは、VLAN1 で設定されています。
  - **ISATAP** — IPv6 インタフェースは、ISATAP トンネルで設定されています。

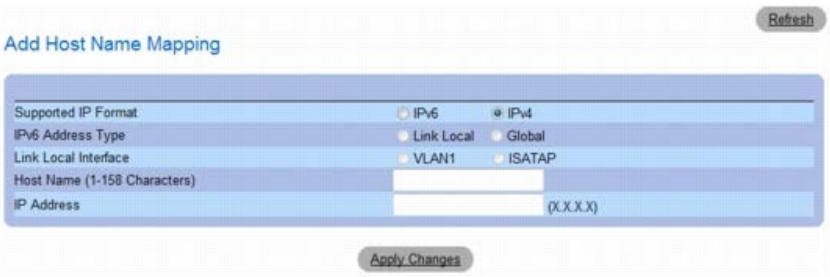
ホストドメイン名の追加

□□□ **Host Name Mapping**（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。

Add Host Name Mapping（ホスト名のマッピングの追加）ページ が開きます。

図 **6-48.** ホスト名のマッピングの追加



□□□ 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 アドレスがホストネームにマップされ、デバイスがアップデートされます。

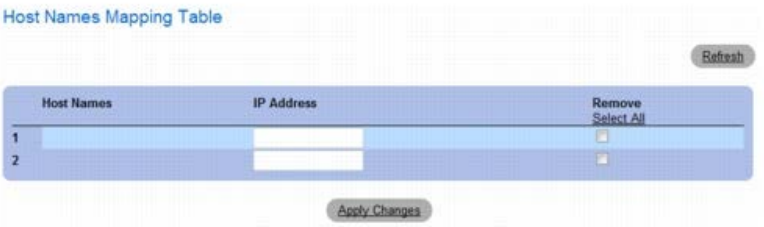
ホスト名のマッピング表の表示

□□□ **Host Name Mapping**（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。

Hosts Name Mapping Table（ホスト名のマッピング表）ページが開きます。

図 **6-49.** ホスト名のマッピング表



IP アドレスマッピングからのホスト名の削除

□□□ **Host Name Mapping**（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。

□□□ **Host Mapping Table**（ホストのマッピング表）ページが開きます。

□□□ **Host Name Mapping Table**（ホスト名マッピング表）のエントリを選択します。

□□□ **Remove**（削除）チェックボックスをクリックします。

□□□ **Apply Changes**（変更の適用）をクリックします。

Host Mapping Table（ホストマッピング表）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 IP アドレスのドメインホスト名へのマッピング

次の表は、IP アドレスにドメインホスト名をマップするための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ip host *name address*	ホストキャッシュで、静的なホストのネームツーアドレスマッピングを定義します。
no ip host ***name***	ホスト名からアドレスへのマッピングを削除します。
clear host {*name* **| *}**	ホストのネームツーアドレスキャッシュから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、静的でキャッシュされたホスト名およびアドレスのリストを表示します。

CLI コマンドの例は次のようになります。

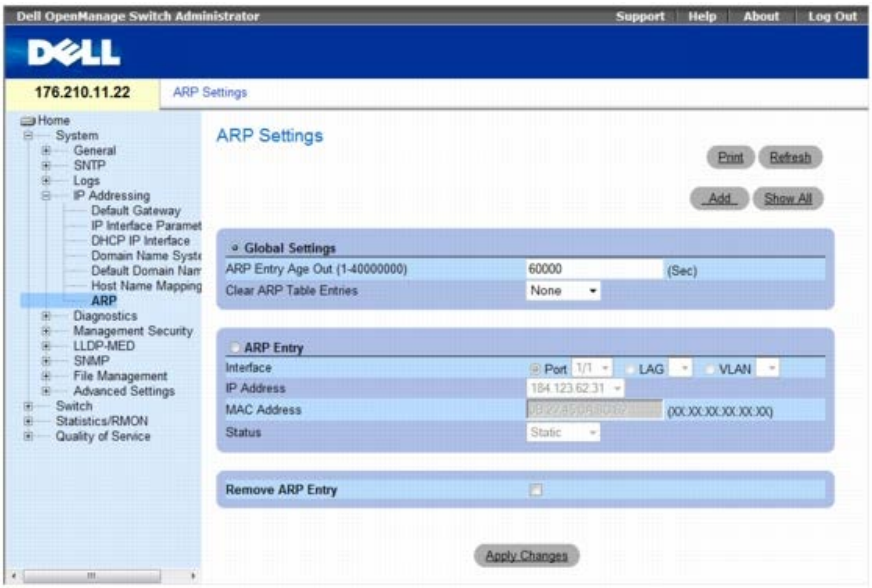
```
console(config)# ip host accounting.abc.com 176.10.23.1
```

ARP 設定の定義

アドレス解決プロトコル（ARP）は、IP アドレスを物理アドレスに変換し、IP アドレスから MAC アドレスへのマッピングを行います。ARP では、隣接ホストの IP アドレスが分かっている場合にのみ、そのホストが別のホストと通信できます。

ARP Settings（ARP の設定）ページを開くには、ツリー表示の **System**（システム）® **IP Addressing**（IP アドレス設定）® **ARP** をクリックします。

図 **6-50. ARP** の設定



ARP Settings（ARP 設定）ページには、次のフィールドがあります。

- **Global Settings**（グローバル設定）— このオプションを選択し、ARP のグローバル設定のためのフィールドをアクティブにします。
  - **ARP Entry Age Out**（**1-40000000**）（ARP エントリの寿命（1～40000000））— すべてのデバイスに関して、ARP 表エントリについての ARP 要求に費やせる時間（秒）です。 この期間の後、エントリは表から削除されます。範囲は **1**～**40000000** 秒です。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）— すべてのデバイスでクリアされる ARP エントリのタイプです。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 エントリはクリアされます。
- **Dynamic**（動的）— 動的 ARP エントリのみがクリアされます。
- **Static**（静的）— 静的 ARP エントリのみがクリアされます。

- **ARP Entry**（ARP 設定）— 1 つのイーサネットデバイスの ARP 設定用フィールドをアクティブにする場合は、このオプションを選択します。
  - **Interface**（インタフェース）— デバイスに接続されているポート、LAG、、または VLAN のインタフェースの番号です。
  - **IP Address**（IP アドレス）— 次に示される MAC アドレスと関連するステーション IP アドレスです。
  - **MAC Address**（MAC アドレス）— ARP 表で IP アドレスと関連するステーション MAC アドレスです。
  - **Status**（状態）— ARP 表エントリの状態 可能なフィールド値は以下のとおりです。
    - **Dynamic**（動的） — ARP エントリは動的に学習されます。
    - **Static**（静的） — ARP エントリは静的エントリです。
- **Remove ARP Entry**（ARP エントリの削除）— ARP エントリを削除します。
  - **Checked**（チェックマークあり）— ARP エントリを削除します。
  - **Unchecked**（チェックマークなし）— ARP エントリを保持します。

静的 **ARP** 表エントリの追加：

□□□ **ARP Settings page**（ARP の設定ページ）を開きます。

□□□ **Add**（追加）をクリックします。

Add ARP Entry（ARP エントリの追加）ページが開きます。

□□□ 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。

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 Settings page**（ARP 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。

ARP Table（ARP 表）ページが開きます。

ARP 表エントリの削除

□□□ **ARP Settings page**（ARP 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。

ARP Table（ARP 表）ページが開きます。

□□□ 表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。

選択された**ARP Table**（ARP 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 **ARP** の設定

次の表は、**ARP Settings**（ARP の設定ページ）に表示される、フィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明

arp *ip_addr hw_addr* {**ethernet** *interface-number* | **vlan** *vlan-id* | **port-channel** *number*}	ARP キャッシュにパーマネントエントリを追加します。
arp timeout *seconds*	エントリが ARP キャッシュに留まる時間を設定します。
clear arp-cache	ARP キャッシュからすべての動的エントリを削除します。
show arp	ARP 表のエントリを表示します。
no arp	ARP 表から ARP エントリを削除します。

CLI コマンドの例は次のようになります。

```
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

Diagnostics（診断）ページには、銅ケーブルおよび光ファイバーケーブルに行う仮想ケーブルテストのページへのリンクがあります。**Diagnostics**（診断）ページを開くには、ツリー表示で、**System**（システム）® **Diagnostics**（診断）の順にクリックします。

本項には、次のトピックがあります。

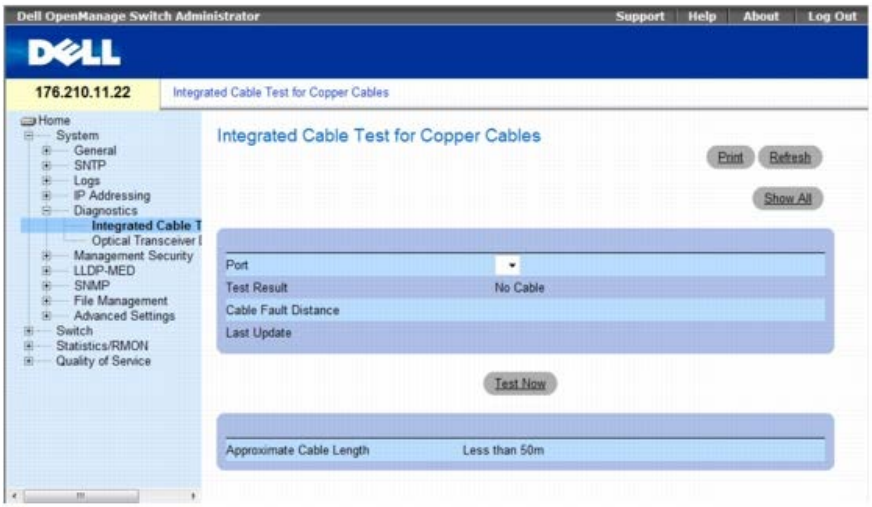
- 銅ケーブル診断の表示
- 光学送受信機診断の表示

銅ケーブル診断の表示

Integrated Cable Test for Copper Cables（銅線ケーブルの内蔵ケーブルテスト）ページには、銅線ケーブルのテストを行うためのフィールドがあります。ケーブルのテストを行うと、ケーブルのエラーが発生した場所、最後に行ったケーブルテスト、および発生したケーブルエラーのタイプについての情報が分かります。このテストでは、時間領域反射率測定法（TDR：Time Domain Reflectometry）を用いてポートに取り付けられた銅ケーブルの質および特徴をテストします。120 メートルまでのケーブルをテストすることができます。ケーブルのテストはポートがダウン状態のときに行い、概算ケーブル寸法テストは行いません。

Integrated Cable Test for Copper Cables（銅線ケーブルの内蔵ケーブルテスト）ページを開くには、ツリー表示の **System**（システム）® **Diagnostics**（診断）® **Integrated Cable Test**（内蔵ケーブルテスト）をクリックします。

図 **6-51.** 銅ケーブルの内蔵ケーブルテスト



Integrated Cable Test for Copper Cables（銅線ケーブルの内蔵ケーブルテスト）ページには、以下のフィールドがあります。

- **Port**（ポート）— ケーブルが接続されているポートです。
- **Test Result**（テスト結果）— ケーブルテストの結果です。可能なフィールド値は次のとおりです。

- **No Cable**（ケーブルなし）— ポートに接続されているケーブルはありません。
- **Open Cable**（オープンケーブル）— ケーブルは一方にのみ接続されています。
- **Short Cable**（ショートしたケーブル）— ケーブルにショートが起きました。
- **OK** — ケーブルはテストに合格しました。

- **Cable Fault Distance**（ケーブル故障距離）— ポートからケーブルエラーが発生した場所までの距離です。
- **Last Update**（最後のアップデート）— 最後にポートをテストした時間です。
- **Approximate Cable Length**（概算ケーブル寸法）— 概算ケーブル寸法です。このテストは、ポートが 1 Gbps で動作しているときにのみ実行することができます。

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。

□□□ **Integrated Cable Test for Copper Cables**（銅ケーブルの内蔵ケーブルテスト）ページを開きます。

□□□ テストするインタフェースを選択します。

□□□ **Test Now**（テストの実行）をクリックします。

銅線ケーブルのテストが行われ、テストの結果が**Integrated Cable Test for Copper Cables**（銅線ケーブルの内蔵ケーブルテスト）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

この画面には以前実行されたテストの結果が表示されます。ただし、現在、すべてのポートに対して実際にテストが実行されるわけではありません。内蔵ケーブルテスト（VCT）で結果として示されるケーブルの長さは、概算で 50 m まで、50 m～80 m、80 m～110 m、110 m～120 m、または 120 m 以上の範囲です。誤差は最大 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。

□□□ **Integrated Cable Test for Copper Cables**（銅ケーブルの内蔵ケーブルテスト）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Integrated Cable Test Results Table（内蔵ケーブルテスト結果表）ページが開きます。

図 **6-52.** 内蔵ケーブルテスト結果表

Integrated Cable Test for Copper Cables（銅線ケーブルの内蔵ケーブルテスト）ページのフィールドのほかに、**Integrated Cable Test Results Table**（内蔵ケーブルテスト結果表）には、以下のフィールドがあります。

- **Unit No.**（ユニット番号）— ケーブルが表示されるスタッキングメンバーユニットです。

CLI コマンドを使用した銅ケーブルテストの実行

次の表は、銅ケーブルのテストを行うための CLI コマンドをまとめたものです。

CLI コマンド	説明
test copper-port tdr interface	VCT テストを行います。
show copper-port tdr interface	最後にポートに対して行った VCT テストの結果を示します。
show copper-port cable-length interface	ポートに取り付けられた銅線ケーブルのおよその長さを表示します。

CLI コマンドの例は次のようになります。

```
console> enable
Console# test copper-port tdr 1/e3
Cable is open at 100 meters.

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

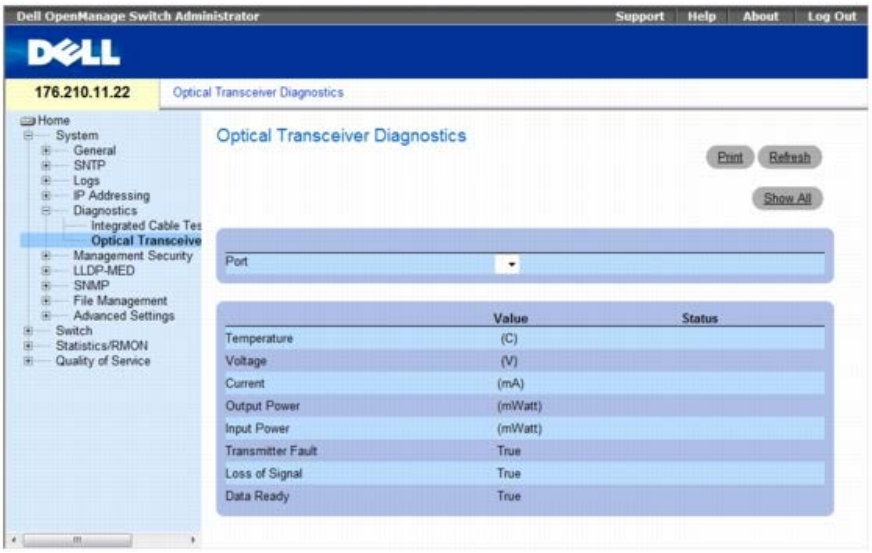
Port	Length (meters)
----	---------------
1/e3	110-140
1/e4	Fiber

光学送受信機診断の表示

Optical Transceiver Diagnostics（光学送受信機診断）ページを使用して、光ファイバーケーブルのテストを実行します。光学送受信機診断は、リンクが存在しているときにのみ行うことができます。Finisair 送受信機ではトランスミッタ故障診断テストをサポートしていません。光ファイバー分析機能は、デジタル診断標準 SFF--872 をサポートしている SFP でのみ動作します。

Optical Transceiver Diagnostics（光学送受信機診断）ページを開くには、ツリー表示の **System**（システム）® **Diagnostics**（診断）® **Optical Transceiver Diagnostics**（光学送受信機診断）をクリックします。

図 **6-53** 光学送受信機診断



Optical Transceiver Diagnostics（光学送受信機診断）ページには、以下のフィールドがあります。

- **Port**（ポート）— ケーブルがテストされるポート番号です。
- **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**（出力電源）— 出力電源が送られる速度です。
- **Input Power**（入力電源）— 入力電源が送られる速度です。
- **Transmitter Fault**（送信機の故障）— 送信中に故障が起きた場合に表示します。
- **Loss of Signal**（信号の損失）— ケーブルに信号損失が起きた場合に表示します。
- **Data Ready**（データ準備完了）— 送受信機は電源投入され、データの準備はできています。

Optical Transceiver Diagnostics Test Results Table（光学送受信機診断テスト結果表）の表示

□□□ **Optical Transceiver Diagnostics**（光学送受信機診断）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、**Optical Transceiver Diagnostics Table**（光学送受信機診断表）ページが開きます。

図 **6-54.** 光学送受信機診断表

Optical Transceiver Diagnostics（光学送受信機診断）ページのフィールドのほか、**Optical Transceiver Diagnostics Table**（光学送受信機診断表）には、以下のフィールドがあります。

- **Unit No.**（ユニット番号）— ケーブルが表示されるユニット番号です。
- **N/A** — 該当なし、N/S - サポートなし、W - 警告、E - エラー

CLI コマンドを使用した光ファイバーテストの実行

次の表は、光ファイバーテストを実行するための CLI コマンドをまとめたものです。

CLI コマンド	説明
show fiber-ports optical-transceiver [interface] [detailed]	光学送受信機診断を表示します。

CLI コマンドの例は次のとおりです。

Console# show fiber-ports optical-transceiver detailed

Port	Temp[C]	Voltage	Current [Volt]	Output[mA]	Input [mWatt]	POWER TX [mWatt]	LOS Fault
----	----	------	-----	------	------	------	-----
1/g1	48	5.15	50	1.789	1.789	No	No
1/g2	43	5.15	10	1.789	1.789	No	No

管理セキュリティの管理

Management Security（管理セキュリティ）ページを使用すると、デバイスの管理方法、ユーザー認証データベース、およびサーバーに関するセキュリティパラメータを設定するためのフィールドがある、各セキュリティページにアクセスできます。**Management Security**（管理セキュリティ）ページを開くには、ツリー表示の **System**（システム）®**Management Security**（管理セキュリティ）をクリックします。

本項には、次のトピックがあります。

- アクセスプロファイルの定義
- 認証プロファイルの定義
- 認証プロファイルの選択
- パスワードの管理
- アクティブユーザーの表示
- ローカルユーザーデータベースの定義
- ラインパスワードの定義
- 有効パスワードの定義
- TACACS+ 設定の定義
- RADIUS の設定

アクセスプロファイルの定義

Access Profiles（アクセスプロファイル）ページには、プロファイルを定義するためのフィールド、およびデバイスにアクセスするためのルールがあります。管理機能へのアクセスは、入口インタフェースおよび送信元 IP アドレスまたは送信元 IP サブネットによって定義されるユーザーグループに制限できます。

管理アクセスは、ウェブ（HTTP）、セキュアウェブ（HTTPS）、Telnet、および Secure Telnet といった管理アクセス方法の種類ごとに個別に定義できます。

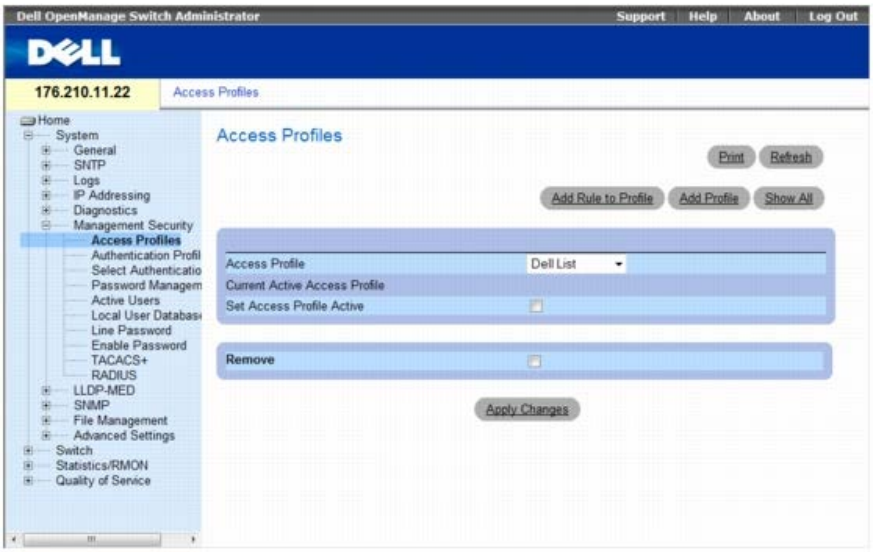
異なる管理方法へのアクセスは、ユーザーグループ間で異なる場合があります。例えば、ユーザーグループ 1 は HTTPS セッションのみを介してデバイスにアクセスしますが、ユーザーグループ 2 は HTTPS セッションと Telnet セッションの両方を介してデバイスにアクセスすることができるということです。

管理アクセスリストには、デバイスを管理できるユーザーおよびその方法を決定するルールを、最大 256 まで設定できます。また、ユーザーがデバイスにアクセスできないようにすることもできます。

Access Profiles（アクセスプロファイル）ページには、管理リストを設定するためのフィールド、およびこのリストを特定のインタフェースに適用するためのフィールドがあります。

Access Profiles（アクセスプロファイル）ページを開くには、ツリー表示の **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 **6-55** アクセスプロファイル



Access Profiles（アクセスプロファイル）ページには、以下のフィールドがあります。

- **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。Access Profile（アクセスプロファイル）リストには、デフォルト値の **Console Only**（コンソールのみ） が含まれます。このアクセスプロファイルを選択すると、デバイスのアクティブな管理は、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です。
- **Set Access Profile Active**（アクセスプロファイルをアクティブに設定）— アクセスプロファイルをアクティブにします。
- **Remove**（削除）— **Access Profile Name**（アクセスプロファイル名）リストからアクセスプロファイルを削除します。
  - **Checked**（チェックマークあり）— アクセスプロファイルを削除します。
  - **Unchecked**（チェックマークなし）— アクセスプロファイルを保持します。

プロファイルの有効化

□□□ **Access Profiles**（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）フィールドのアクセスプロファイルを選択します。

□□□ **Set Access Profile Active**（アクセスプロファイルをアクティブに設定）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、デバイス管理法、インタフェースのタイプ、ソース IP アドレスおよびネットワークマスク、およびデバイス管理アクセス処置を決めるためのフィルターとして機能します。ユーザーの管理アクセスを防御、または許可することができます。ルール優先度は、ルールを割り当てる順序を設定します。インタフェースにアクセスプロファイルを割り当てると、他のインタフェース経由のアクセスは拒否されます。アクセスプロファイルをどのインタフェースにも割り当てない場合は、すべてのインタフェースからデバイスにアクセスすることができます。

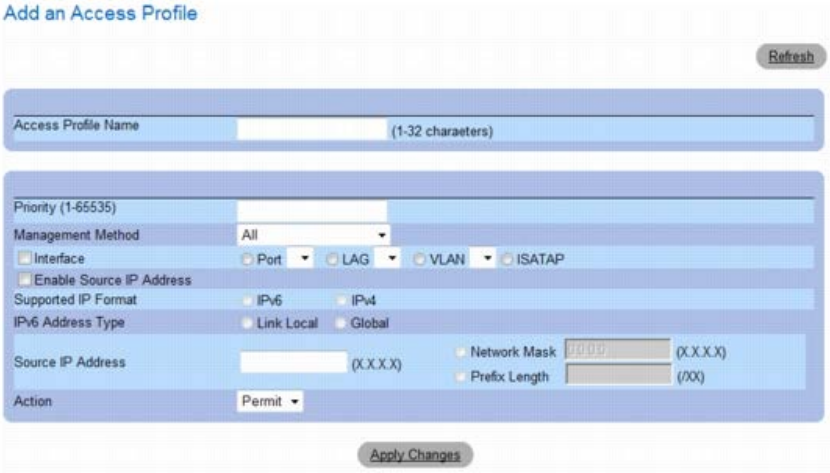
アクセスプロファイルのルールの定義：

□□□ **Access Profiles**（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。

Add an Access Profile（アクセスプロファイルの追加）ページが開きます。

図 **6-56.** アクセスプロファイルの追加



Add an Access Profile（アクセスプロファイルの追加）ページには、以下の追加フィールドがあります。

- **Access Profile Name**（**1-32 Characters**）（アクセスプロファイル名（1～32 文字））— ユーザー定義のアクセスプロファイルの名前です。アクセスプロファイル名は、最大 32 文字で使用できます。
- **Rule Priority**（**1-65535**）（ルール優先度（1～65535））— ルール優先度です。パケットがルールと適合すると、ユーザーはデバイス管理アクセスを許可されるか、または拒否されます。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。パケットは最初に合った順で適合するので、ルールナンバーはパケットをルールに適合するのに必須です。ルール優先度は、**Profile Rules Table**（プロファイルルール表）で表示できます。
- **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、選択された管理方法（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。可能なフィールド値は次のとおりです。
  - **All**（すべて）— すべての管理方法をルールに割り当てます。
  - **Telnet** — Telnet アクセスをルールに割り当てます。選択すると、アクセスプロファイル基準を満たし、Telnet を使用してデバイスにアクセスするユーザーのアクセスが、許可または拒否されます。
  - **Secure Telnet**（**SSH**）（セキュア Telnet（SSH））— SSH アクセスをルールに割り当てます。選択すると、アクセスプロファイル基準を満たし、Telnet を使用してデバイスにアクセスするユーザーのアクセスが、許可または拒否されます。
  - **HTTP** — HTTP アクセスをルールに割り当てます。選択すると、アクセスプロファイル基準を満たし、HTTP を使用してデバイスにアクセスするユーザーのアクセスが、許可または拒否されます。
  - **Secure HTTP**（**HTTPS**）（セキュア HTTP（HTTPS））— HTTPS アクセスをルールに割り当てます。選択すると、アクセスプロファイル基準を満たし、HTTPS を使用してデバイスにアクセスするユーザーのアクセスが、許可または拒否されます。
  - **SNMP** — SNMP アクセスをルールに割り当てます。選択すると、アクセスプロファイル基準を満たし、SNMP を使用してデバイスにアクセスするユーザーのアクセスが、許可または拒否されます。
- **Interface**（インタフェース）— 任意のフィールドで、ルールを適用するインタフェースのタイプです。これは、オプションフィールドです。チェックボックスを選択し、適切なオプションボタンとインタフェースを選択することによって、選択されたポート、LAG、または VLAN にこのルールを適用することができます。
- **Enable Source IP Address**（ソース IP アドレスの有効化）— このパラメーターをチェックすると、ソース IP アドレスに基づいて条件を制限します。チェックをしない場合は、設定される規則へソース IP アドレスを入力することができません。
- **Supported IP Format**（サポートされている IP 形式）— IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— IPv6 において（前述のパラメーターを参照）、サポートされている静的アドレスのタイプを指定します。可能な値は以下のとおりです。
  - **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
- **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。
- **Source IP Address**（X.X.X.X）（ソース IP アドレス（X.X.X.X））— 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。これは任意のフィールドで、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（X.X.X.X））— 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（/XX））— 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**（処置）— 定義されたインタフェースへの管理アクセスを許可する拒否するかを定義します。
  - **Permit**（許可）— デバイスへのアクセスを許可します。
  - **Deny**（拒否）— デバイスへのアクセスを拒否します。これがデフォルト設定になっています。

□□□ **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。

□□□ 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

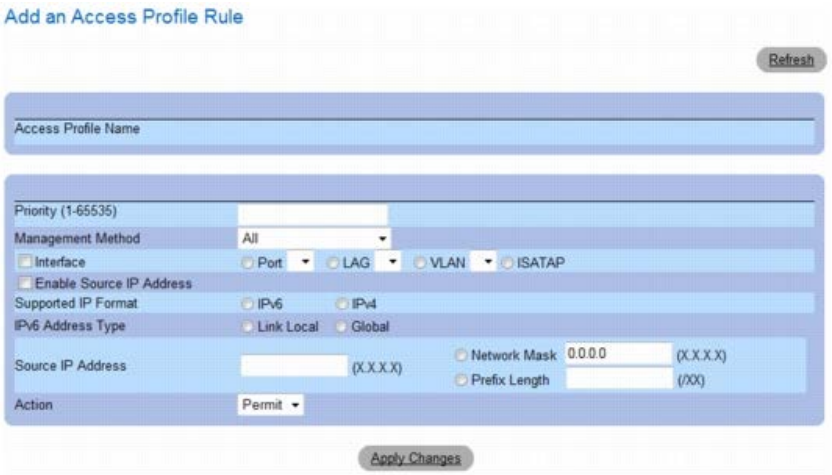
最初のルールはアクセスプロファイルに最初に適合するトラフィックに定義する必要があります。

□□□ **Access Profiles**（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。

Add an Access Profile Rule（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 **6-57.** アクセスプロファイルルールの追加



□□□ 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。

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。

Profile Rules Table（プロファイルルール表）の表示

パケットはルール基準に合う最初のルールに適合するので、**Profile Rules Table**（プロファイルルール表）にルールが現われる順序は重要です。パケットは、ルール条件を満たす最初のルールとマッチされます。

□□□ **Access Profile** （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 **6-58.** プロファイルルール表

ルールの削除

□□□ **Access Profiles**（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。

□□□ 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。

選択されたルールが削除され、デバイスがアップデートされます。

CLI コマンドを使用したアクセスプロファイルの削除

次の表は、**Access Profiles**（アクセスプロファイル）ページに表示されるフィールドを設定する等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
management access-list *name*	管理用のアクセスリストを定義し、設定用のアクセスリストの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ためのポートの許可条件を設定します。
permit ip-source {*ipv4-address* | *ipv6-address* / *prefix-length*} [**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ためのポートの許可条件、および選択された管理方法をを設定します。
deny [**ethernet** *interface-number* | **vlan** *vlan-id* **| port-channel** *number*] [**service** *service*]	管理アクセスリストのためのポートの拒否条件、および選択された管理方法をを設定します。
deny ip-source {*ipv4-address* | *ipv6-address* / *prefix-length*} [**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ためのポートの拒否条件、および選択された管理方法をを設定します。
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るかを定義します。
show management access-list [*name*]	アクティブな管理アクセスリストを表示します。
show management access-class	管理アクセスクラスについての情報を表示します。

CLI コマンドの例は次のようになります。

```
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

Authentication Profiles（認証プロファイル）ページには、デバイス上でユーザー認証方法を選択するフィールドがあります。ユーザー認証は以下のように発生します。

- ローカルで
- 外付けのサーバーを介して

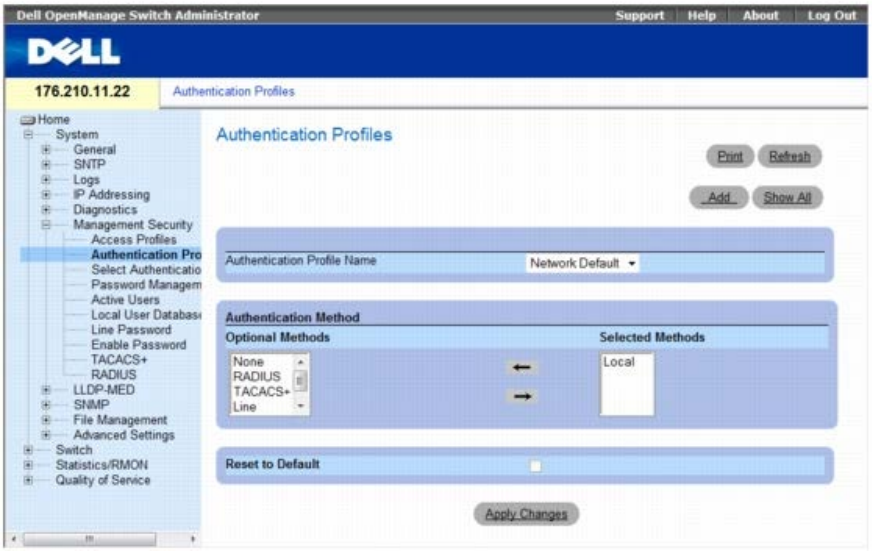
また、ユーザー認証を None（なし）に設定することもできます。

ユーザー認証は選択された方法の順序で発生します。例えば、Local オプションと RADIUS オプションが選択されている場合、ユーザーは最初にローカルで認証されます。ローカルのユーザーデータベースが空の場合は、ユーザーは RADIUS サーバーを介して認証されます。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は、次に選択された方法が使用されます。

Authentication Profiles（認証プロファイル）ページを開くには、ツリー表示の **System**（システム）® **Management Security**（管理セキュリティ）® **Authentication Profiles**（認証プロファイル）をクリックします。

図 **6-59.** 認証プロファイル



Authentication Profiles（認証プロファイル）ページには、以下のフィールドがあります。

- **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。オプションは **Network Default**（ネットワークデフォルト）および **Console Default**（コンソールデフォルト）です。プロファイル名に空スペースは使用できません。
- **Optional Methods**（任意の方法）— ユーザー認証方法です。可能なオプションには、以下のものがあります。
  - **None**（なし） — ユーザー認証は発生しません。
  - **Local**（ローカル） — ユーザー認証はデバイスレベルで発生します。デバイスは認証のために、ユーザー名およびパスワードをチェックします。
  - **RADIUS** — ユーザー認証は RADIUS サーバーで発生します。詳細については、 **RADIUS** の設定を参照してください。
  - **TACACS+** — ユーザー認証は TACACS+ サーバーで発生します。
  - **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） — 認証に有効パスワードが使用されます。
- **Reset to Default**（デフォルトにリセット）— デバイスのユーザー認証方法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。

認証プロファイルの選択：

□□□ **Authentication Profiles**（認証プロファイル）ページを開きます。

□□□ **Authentication Profile Name**（認証プロファイル名）フィールドのプロファイルを選択します。

□□□ ナビゲーション矢印を使用して認証方法を選択します。認証は、認証方法がリストされている順序で行われます。

□□□ **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アップデートされます。

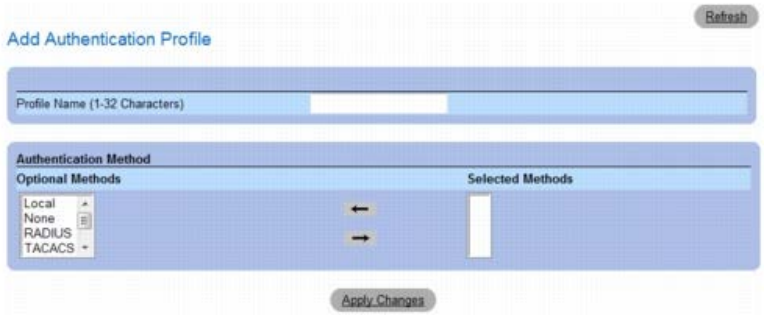
認証プロファイルの追加：

□□□ **Authentication Profiles**（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。

Add Authentication Profile（認証プロファイルの追加）ページが開きます。

図 **6-60.** 認証プロファイルの追加



□□□ プロファイルを設定します。

□□□ **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アップデートされます。

Authentication Profiles Table（認証プロファイル表）の表示

□□□ **Authentication Profiles**（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。

Authentication Profiles Table（認証プロファイル表）ページが開きます。

図 **6-61.** 認証プロファイル表

認証プロファイルの削除

□□□ **Authentication Profiles**（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。

Authentication Profiles Table（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

次の表は、 **Authentication Profiles**（認証プロファイル）ページに表示されるフィールドを設定するための等価 **CLI** コマンドをまとめたものです。

CLI コマンド	説明
aaa authentication login {**default** | *list-name*} *method1* [*method2*.]	ログイン認証を設定します。
no aaa authentication login {**default** | *list-name*}	ログイン認証プロファイルを削除します。

CLI コマンドの例は次のようになります。

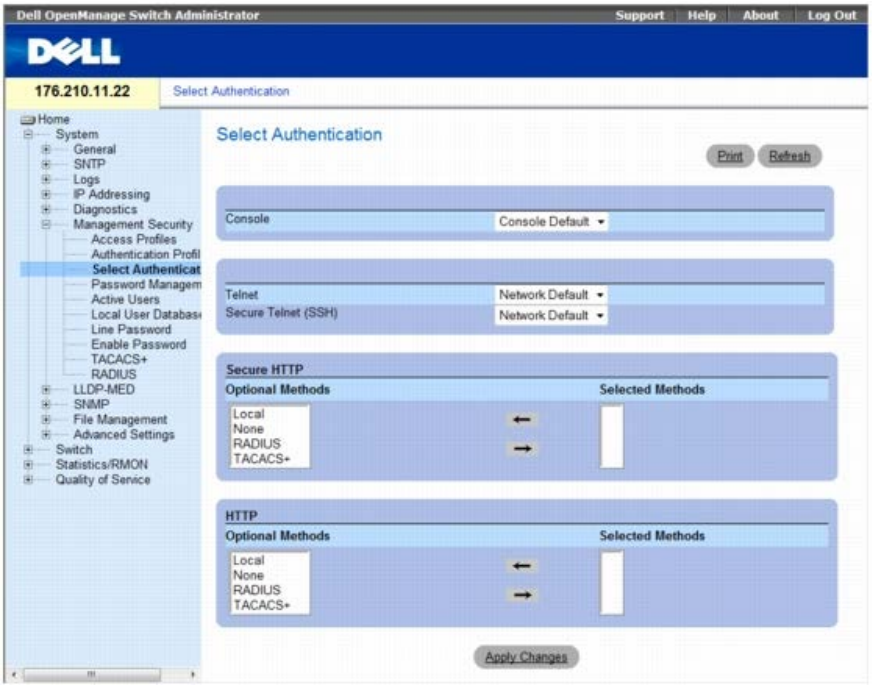
```
console(config)# aaa authentication login default radius local enable none
console(config)# no aaa authentication login default
```

認証プロファイルの選択

認証プロファイルが定義された後、認証プロファイルは管理アクセス法に適用することができます。たとえば、コンソールユーザーは Authentication Method List 1（認証方法リスト 1）、Telnet ユーザーは Authentication Method List 2（認証方法リスト 2）によって認証できます。

Select Authentication（認証の選択）ページを開くには、ツリー表で、**System**（システム）® **Management Security**（管理セキュリティ）® **Select Authentication**（認証の選択）の順にクリックします。

図 **6-62.** 認証の選択



Select Authentication（認証の選択）ページには、以下のフィールドがあります。

- **Console**（コンソール）— コンソールユーザーを認証するために使用される認証プロファイルです。
- **Telnet** — Telnet ユーザーを認証するために使用される認証プロファイルです。
- **Secure Telnet**（**SSH**）— Secure Shell（SSH）ユーザーを認証するために使用される認証プロファイルです。SSH は、クライアントに安全で暗号化されたデバイスへのリモート接続を提供します。
- **Secure HTTP**（セキュア HTTP）および **HTTP** — それぞれセキュア HTTP アクセスと HTTP アクセス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。
  - **Local**（ローカル） — 認証はローカルで発生します。
  - **None**（なし） — 認証方法はアクセスに使用されません。
  - **RADIUS** — 認証は RADIUS サーバーで発生します。
  - **TACACS+** — 認証は TACACS+ サーバーで発生します。

認証リストのコンソールセッションへの適用

□□□ **Select Authentication**（認証の選択）ページを開きます。

□□□ **Console**（コンソール）フィールドのプロファイルを選択します。

□□□ **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が認証リストに割り当てられます。

認証プロファイルの **Telnet** セッションへの適用

□□□ **Select Authentication**（認証の選択）ページを開きます。

□□□ **Telnet** フィールドの認証プロファイルを選択します。

□□□ **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。

認証プロファイルの Secure Telnet（SSH）セッションへの適用

□□□ **Select Authentication**（認証の選択）ページを開きます。

□□□ **Secure Telnet**（SSH）フィールドの認証プロファイルを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

Secure Telnet（SSH）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

□□□ **Select Authentication**（認証の選択）ページを開きます。

□□□ **HTTP** フィールドの認証シーケンスを選択します。

□□□ **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。

Secure HTTP セッションの認証シーケンスへの適用

□□□ **Select Authentication**（認証の選択）ページを開きます。

□□□ **Secure HTTP** フィールドの認証シーケンスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

Secure 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シーケンスの割り当て

次の表は、 **Select Authentication**（認証の選択）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

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、より高い権限レベルにアクセスする場合の認証方法リストを示します。
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リストを示します。
ip http authentication *method1* [*method2*.]	HTTP サーバーのための認証方法を示します。
ip https authentication *method1* [*method2*.]	HTTPS サーバーのための認証方法を示します。
show authentication methods	認証方法についての情報を表示します。

CLI コマンドの例は次のようになります。

```
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、ネットワークのセキュリティとパスワードの制御が強化されます。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設定されています。

- 最小パスワード長の定義
- パスワードの有効期限
- 頻繁なパスワード再使用の防止
- ログイン試行失敗後のユーザーのロックアウト

パスワード管理を有効にすると、パスワードのエージングが即時に開始されます。パスワードは、ユーザー定義の時間 / 日数定義に基づいて有効期限が切れます。パスワードが期限切れになる 10 日前に、パスワード期限切れの警告メッセージがデバイスに表示されます。

パスワードが失効した後も、ユーザーは数回ログインできます（この回数は設定可能）。残りのログイン時に、パスワードの変更が必要であることをユーザーに知らせる追加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場合、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なければログインできなくなります。パスワード警告は Syslog ファイルに記録されます。

特権レベルを再定義した場合は、ユーザーも再定義される必要があります。ただし、パスワードのエージ時間は、最初のユーザー定義に基づいて期限切れになります。

パスワードの期限が切れる前に、パスワードの変更が必要であることがユーザーに通知されます。ただし、この通知はウェブユーザーには表示されません。

Password Management（パスワード管理）ページを開くには、ツリー表示の **System**（システム）® **Management Security**（管理セキュリティ）® **Password Management**（パスワード管理）をクリックします。

図 **6-63.** パスワード管理

Password Management（パスワード管理）ページ には以下のフィールドがあります。

- **Password Minimum Length**（**8-64**）（最小パスワード長（8～64））— チェックを入れると、最小パスワード長が示されます。たとえば、管理者はすべてのパスワードの最小文字数を 10 文字と定義することができます。
- **Consecutive Passwords Before Re-use**（再使用前の連続パスワード）— パスワードが再使用できるようになる前に、パスワードが変更される回数を示します。設定可能なフィールド値は 1～10 です。
- **Enable Login Attempts**（**1-5**）（ログイン試行を有効にする（1～5））— 選択されている場合、ユーザー定義の回数を超えてパスワードが誤入力された場合にユーザーをデバイスからロックアウトする機能が有効になります。たとえば、このフィールドにチェックを入れ、値を 5 に設定した場合、ユーザーが間違ったパスワードで 5 回ログインを試行すると、6 回目の試行時にユーザーがデバイスからロックアウトされます。設定可能なィールド値は 1～5 です。

パスワード管理の定義

□□□ **Password Management**（パスワード管理）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。

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

次の表は、 **Password Management**（パスワード管理）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

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*	パスワードが再使用できるようになる前に、パスワードが変更される回数を定義します。
password lock-out *number*	ユーザーがデバイスからロックアウトされる前に、間違ったパスワードが入力される回数を定義します。
show password configuration	パスワード管理情報を表示します。
show users accounts	ユーザーアカウントを表示します。

CLI コマンドの例は次のようになります。

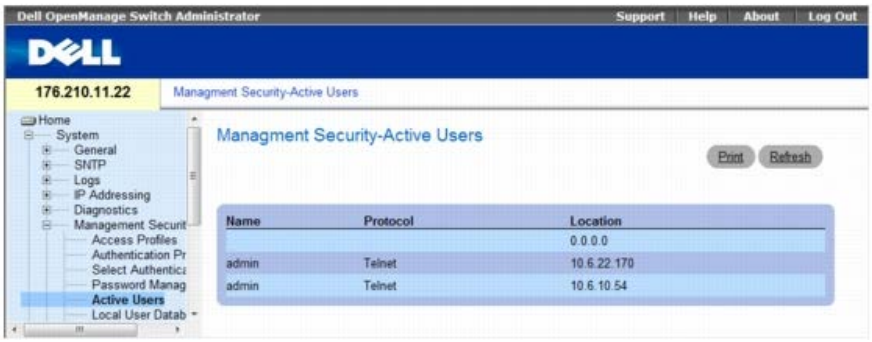
```
console # show passwords configuration

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
```

アクティブユーザーの表示

Active Users（アクティブユーザー）ページには、デバイスでアクティブなユーザーに関する情報が表示されます。

Active Users（アクティブユーザー）ページを開くには、ページ表示で、**System**（システム）® **Management Security**（管理セキュリティ）® **Active Users**（アクティブユーザー）の順にクリックします。

図 **6-64.** アクティブユーザー



Active Users（アクティブユーザー）ページには、以下のフィールドがあります。

- **Name**（名前）— デバイスにログインしているユーザー名のリストです。
- **Protocol**（プロトコル）— ユーザーがデバイスに接続するために使用している管理方法です。
- **Location**（場所）— ユーザーの IP アドレスです。

CLI Commands を使用したアクティブユーザーの表示

次の表は、デバイスに接続しているアクティブユーザーを表示する場合の等価 CLI コマンドをまとめたものです。

表 **6-37.** アクティブユーザーの表示に関する **CLI** コマンド

CLI コマンド	説明
show users	アクティブユーザーに関する情報を表示します。

この CLI コマンドの例を以下に示します。

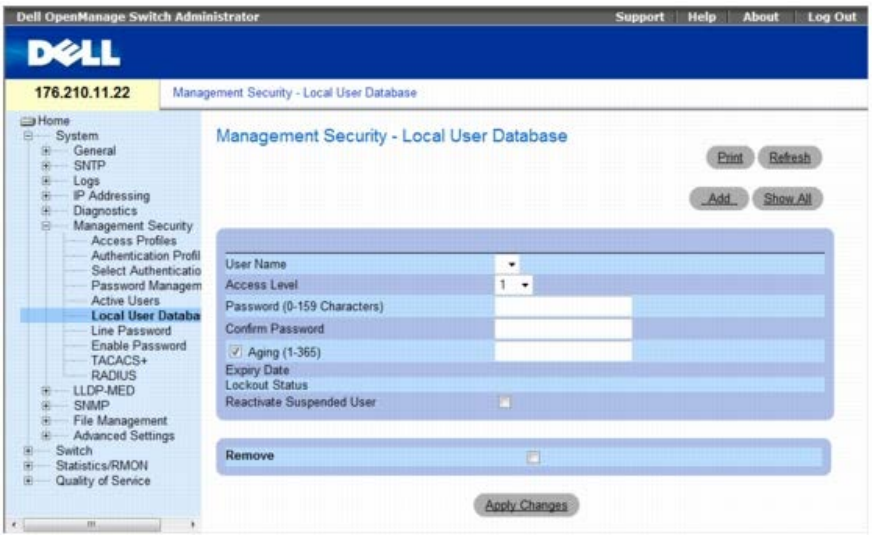
```
console> show users


Username        Protocol        Location
----------      ----------      -------
--
Bob             Serial
John            SSH             172.16.0.1
Robert          HTTP            172.16.0.8
Betty           Telnet          172.16.1.7
```

ローカルユーザーデータベースの定義

Local User Database （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、およびアクセスレベルを定義するフィールドがあります。

Local User Database（ローカルユーザーデータベース）ページを開くには、ツリー表示の **System**（システム）® **Management Security**（管理セキュリティ）® **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 **6-65.** ローカルユーザーデータベース



Local User Database（ローカルユーザーデータベース）には以下のフィールドがあります。

- **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。最も低いユーザーアクセスレベルは **1** で、最も高い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、このユーザーのみが OpenManage Switch Administrator にアクセスして使用できます。
- パスワード（0～159 文字） — ユーザー定義のパスワードです。
- **Confirm Password**（パスワードの確認）— ユーザー定義のパスワードを確認します。
- **Aging**（**1-365**）（エージング（1～365））— パスワードが期限切れになる前の経過日数が表示されます。
  - **Checked**（チェックマークあり）— 指定した日数が経過すると、パスワードが期限切れになります。
  - **Unchecked**（チェックマークなし）— パスワードには期限がありません。
- **Expiry Date**（有効期限）— ユーザー定義パスワードの有効期限を示します。
- **Lockout Status**（ロックアウトステータス）— ユーザーが現在アクセスできるか（Usable（使用可能）ステータス）、または、最後にログインに成功したあと、認証試行に何度も失敗したためにロックアウトされているか（Locked（ロック状態）ステータス）を示します。
- **Reactivate Suspended User**（サスペンドされたユーザーの再アクティブ化） — 指定されたユーザーのアクセス権が再アクティブ化されます。ログイン試行の失敗後、アクセス権をサスペンドすることができます。
  - **Checked**（チェックマークあり）— 指定されたユーザーのアクセス権が再アクティブ化されます。
  - **Unchecked**（チェックマークなし）— 指定されたユーザーのアクセス権をサスペンドしたままにします。
- **Remove**（削除）— **User Name**（ユーザー名）リストからユーザーを削除します。
  - **Checked**（チェックマークあり）— 選択されたユーザーを削除します。
  - **Unchecked**（チェックマークなし）— 選択されたユーザーを保持します。

アクセス権のユーザーへの割り当て：

□□□ **Local User Database**（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）フィールドのユーザーを選択します。

□□□ 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。

ユーザーアクセス権およびパスワードが定義され、デバイスがアップデートされます。

新しいユーザーの定義：

□□□ **Local User Database**（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。

Add User（ユーザーの追加）ページが開きます。

図 **6-66.** ユーザーの追加

□□□ 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。

新しいユーザーが定義され、デバイスがアップデートされます。

ローカルユーザー表の表示：

□□□ **Local User Database**（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。

Local User Table（ローカルユーザー表）が開きます。

図 **6-67.** ローカルユーザー表

サスペンドされたユーザーの再アクティブ化

□□□ **Local User Database**（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）のエントリを選択します。

□□□ **Reactivate Suspended User**（サスペンドされた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。

ユーザーのアクセス権が再アクティブ化され、デバイスがアップデートされます。サスペンドされたユーザーの再アクティブ化は、**Local User Table**（ローカルユーザー表）から実行することもできます。

ユーザーの削除：

□□□ **Local User Database**（ローカルユーザーデータベース）ページを開きます。

□□□ **User Nam**（ユーザー名）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。

選択されたユーザーが削除され、デバイスがアップデートされます。

CLI コマンドを使用したユーザーの割り当て

次の表は、 **Local User Database**（ローカルユーザーデータベース）ページに表示されるフィールドを設定するための等価 **CLI** コマンドをまとめたものです。

CLI コマンド	説明
username *name* [**password** *password*] [**level** *level*] [**encrypted**]	ユーザー名ベースの認証システムを確立します。
set username *name* **active**	サスペンドされたユーザーのアクセス権を再アクティブ化します。

CLI コマンドの例は次のようになります。

```
console(config)# username bob password lee level 15
console# set username bob active
```

ラインパスワードの定義

Line Password（ラインパスワード）ページには、管理方法のためのラインパスワードを定義するフィールドがあります。

Line Password（ラインパスワード）ページを開くには、ツリー表示の **System**（システム）® **Management Security**（管理セキュリティ）® **Line Passwords**（ラインパスワード）をクリックします。

図 **6-68.** ラインパスワード

Line Password（ラインパスワード）ページには以下のフィールドがあります。

- **Line Password / Telnet Line Password / Secure Telnet Line Password**（ラインパスワード /Telnet ラインパスワード / セキュア Telnet ラインパスワード）— コンソール、Telnet、またはセキュア Telnet セッション用の各パスワード設定です。
- **Password**（パスワード）— デバイスにアクセスするためのラインパスワードです。
- **Confirm Password**（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。セキュリティ上の理由で、パスワードは ***** のような形式で表示されます。
- **Console / Telnet / Secure Telnet Line Aging**（**1-365**）（コンソール/Telnet/Secure Telnet 用ラインパスワードのエージング（1～365））— ラインパスワードが期限切れになる前の経過日数が表示されます。
  - **Checked**（チェックマークあり）— 指定した日数が経過すると、パスワードが期限切れになります。
  - **Unchecked**（チェックマークなし）— パスワードには期限がありません。
- **Expiry Date**（有効期限） — ラインパスワードの有効期限を示します。
- **Lockout Status**（ロックアウトステータス）— ユーザーが現在アクセスできるか（Usable（使用可能）ステータス）、または、最後にログインに成功したあと、認証試行に何度も失敗したためにロックアウトされているか（Locked（ロック状態）ステータス）を示します。
- **Reactivate Locked Line**（ロックされたラインの再アクティブ化）— コンソール/Telnet/Secure Telnet セッション用のラインパスワードが再アクティブ化されます。ログイン試行の失敗後、アクセス権をサスペンドすることができます。
  - **Checked**（チェックマークあり）— ラインパスワードが再びアクティブ化されます。
  - **Unchecked**（チェックマークなし）— パスワードのロックを保持します。

コンソールセッションのためのラインパスワードの定義

□□□ **Line Password**（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のための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 セッションのためのラインパスワードの定義

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

Telnet セッションのための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。

Secure Telnet セッションのためのラインパスワードの定義

□□□ **Line Password**（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。

Secure Telnet セッションのための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

次の表は、 **Line Password**（ラインパスワード）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
password *password* [**encrypted**]	ラインパスワードを指定します。

CLI コマンドの例は次のようになります

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

有効パスワードの定義

Enable Password（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ためのローカルパスワードを設定します。

Enable Password（有効パスワード）ページを開くには、ツリー表示の **System**（システム）® **Management Security**（管理セキュリティ）® **Enable Passwords**（有効パスワード）をクリックします。

図 **6-69.** 有効パスワード

Enable Password（有効パスワード）ページには以下のフィールドがあります。

- 有効アクセスレベルの選択 — 有効パスワードと関連するアクセスレベルです。最も低いユーザーアクセスレベルは **1** で、最も高い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、このユーザーのみが OpenManage Switch Administrator にアクセスして使用できます。
- **Password**（**0-159 characters**）（パスワード（0～159 文字））— 有効にするパスワードです。

- **Confirm Password**（パスワードの確認）— パスワードを確認します。セキュリティ上の理由で、パスワードは ***** のような形式で表示されます。
- **Aging**（**1-365**）（エージング（1～365））— パスワードが期限切れになる前の経過日数が表示されます。
  - **Checked**（チェックマークあり）— 指定した日数が経過すると、パスワードが期限切れになります。
  - **Unchecked**（チェックマークなし）— パスワードには期限がありません。
- **Expiry Date**（有効期限） — 有効パスワードの有効期限を示します。
- **Lockout Status**（ロックアウトステータス） — **Password Management**（パスワード管理）ページで **Enable Login Attempts**（ログイン試行を有効にする）チェックボックスが選択されている場合、ユーザーが最後にログインに成功したあと、認証試行に失敗した回数を示します。ユーザーアカウントがロックされている場合は、**LOCKOUT**（ロックアウト）と表示されます。
- **Reactivate Suspended User**（サスペンドされたユーザーの再アクティブ化） — 指定されたユーザーのアクセス権が再アクティブ化されます。ログイン試行の失敗後、アクセス権をサスペンドすることができます。
  - **Checked**（チェックマークあり）— 指定されたユーザーのアクセス権が再アクティブ化されます。
  - **Unchecked**（チェックマークなし）— 指定されたユーザーのアクセス権をサスペンドしたままにします。

新しい有効パスワードの定義：

□□□ **Enable Password**（有効パスワード）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。

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

次の表は、 **Enable Password**（有効パスワード）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
enable password [**level** *level*] *password* [**encrypted**]	アクセスをユーザーレベルおよび特権レベルに制御するためのローカルパスワードを設定します。

CLI コマンドの例は次のようになります。

```
console(config)# enable password level 15 secret
```

TACACS+ 設定の定義

デバイスはタカックス（TACACS+：Terminal Access Controller Access Control System）クライアントサポートを提供します。TACACS+ は、デバイスにアクセスするユーザーを評価するための集中化セキュリティを提供します。

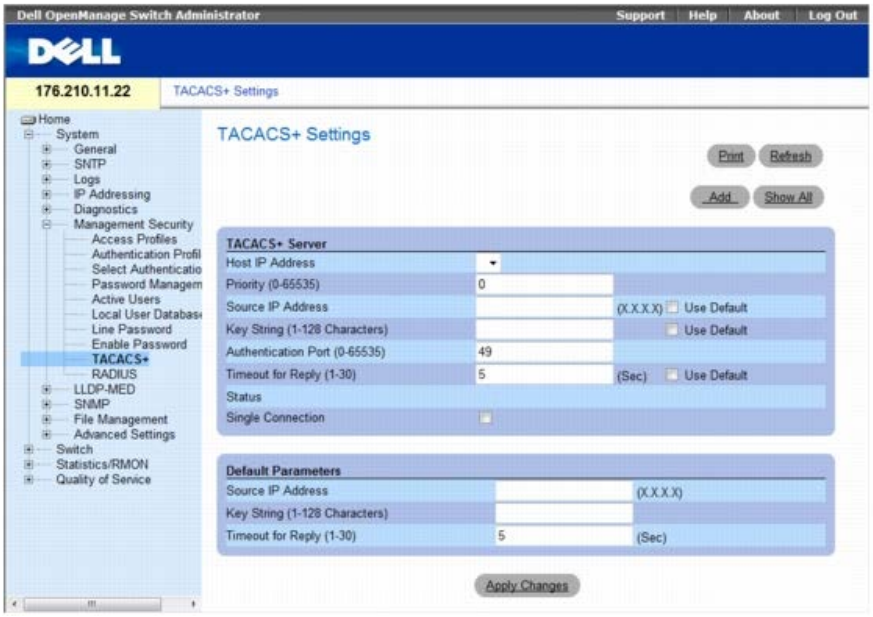
TACACS+ は RADIUS および他の認証プロセスとの整合性は保持したままで、集中化ユーザー管理システムを提供します。TACACS+ は以下のサービスを提供します。

- 認証 — ログインの際、ユーザ名およびユーザー定義のパスワードを介して認証を提供します。
- 認可 — ログインの際に行われます。認証セッションが完了すると、認証されたユーザー名を使用して認可セッションが開始します。TACACS+ サーバーは、ユーザー権限をチェックします。

TACACS+ プロトコルは、デバイスと TACACS+ サーバー間の暗号化プロトコルの交換によりネットワークの整合性を確保します。

TACACS+ Settings（TACACS+ の設定）ページを開くには、ツリー表示の **System**（システム）® **Management Security**（管理セキュリティ）® **TACACS+** をクリックします。

図 **6-70. TACACS+** の設定



TACACS+ Settings（TACACS+ 設定）ページには、以下のフィールドがあります。

- **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（0～65535））— TACACS+ サーバーが使用される順序を指定します。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**（**1-128 Characters**）（キーストリング（1～128 文字））— デバイスと TACACS+ サーバー間の TACACS+ 通信のための認証および暗号化キーを定義します。このキーは TACACS+ サーバー上で使用される暗号化キーと一致する必要があります。このキーは暗号化されます。
- **Authentication Port**（**0-65535**）（認証ポート（0～65535））— TACACS+ セッションが実行されるポートナンバーです。デフォルトはポート 49 です。
- **Timeout for Reply**（**1-30**）（応答タイムアウト（1～30））— デバイスと TACACS+ サーバー間の接続がタイムアウトになるまでの経過時間です。フィールドの範囲は 1～30 秒です。
- **Status**（状態）— デバイスと TACACS+ サーバー間の接続状態です。可能なフィールド値は次のとおりです。
  - **Connected**（接続）— デバイスと TACACS+ サーバーは現在接続されています。
  - **Not Connected**（接続なし）— デバイスと TACACS+ サーバーは現在接続されていません。
- **Single Connection**（単一接続）— 選択した場合、デバイスと TACACS+ サーバー間に 1 つのオープン接続が維持されます。
- **Use Default**（デフォルトの使用）— パラメーターにデフォルト値を使用します。

TACACS+ デフォルトパラメーターはユーザー定義のデフォルトです。デフォルト設定は新しく定義される 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は、システムデフォルトが新しい TACACS+ のサーバーに適用されます。

以下は TACACS+ デフォルトです。

- **Source IP Address**（ソース IP アドレス）— デバイスと TACACS+ サーバー間の TACACS+ セッションに使用するためのデフォルトデバイスソース IP アドレスです。デフォルトのソース IP アドレスは 0.0.0.0 です。
- **Key String**（**1-128 Characters**）（キーストリング（1～128））— 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（1～30））— デバイスと TACACS+ サーバー間の接続がタイムアウトになるまでのデフォルトの時間です。デフォルト値は 5 秒です。

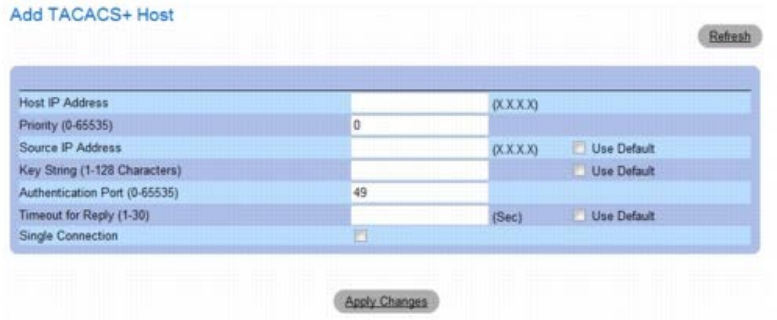
TACACS+ サーバーの追加

□□□ **TACACS+ Settings**（TACACS+ の設定）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add TACACS+ Host（TACACS+ ホストの追加）ページ が開きます。

図 **6-71. TACACS+** ホストの追加



□□□ 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。

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+ Table（TACACS+ 表）の表示

□□□ **TACACS+ Settings**（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+ Settings（TACACS+ 表）が開きます。

図 **6-72. TACACS+** 表

TACACS+ サーバーの削除

□□□ **TACACS+ Table**（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+ Settings（TACACS+ 表）が開きます。

□□□ **TACACS+ Table**（TACACS+ 表）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。

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

次の表は、**TACACS+ Settings**（TACACS+ の設定）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

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 TACACS+ 通信のための認証および暗号化キーを示します。このキーは、TACACS+ デーモン上で使用される暗号化と一致している必要があります。（範囲： 0～128 文字）
tacacs-server timeout *timeout*	タイムアウト値を秒単位で示します。（範囲： 1～30）
tacacs-server source-ip *source*	ソース IP アドレスを指定します。（範囲： 有効な IP アドレス）
show tacacs [*ip-address*]	TACACS+ サーバーの構成および統計を表示します。

CLI コマンドの例は次のようになります。

```
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#
```

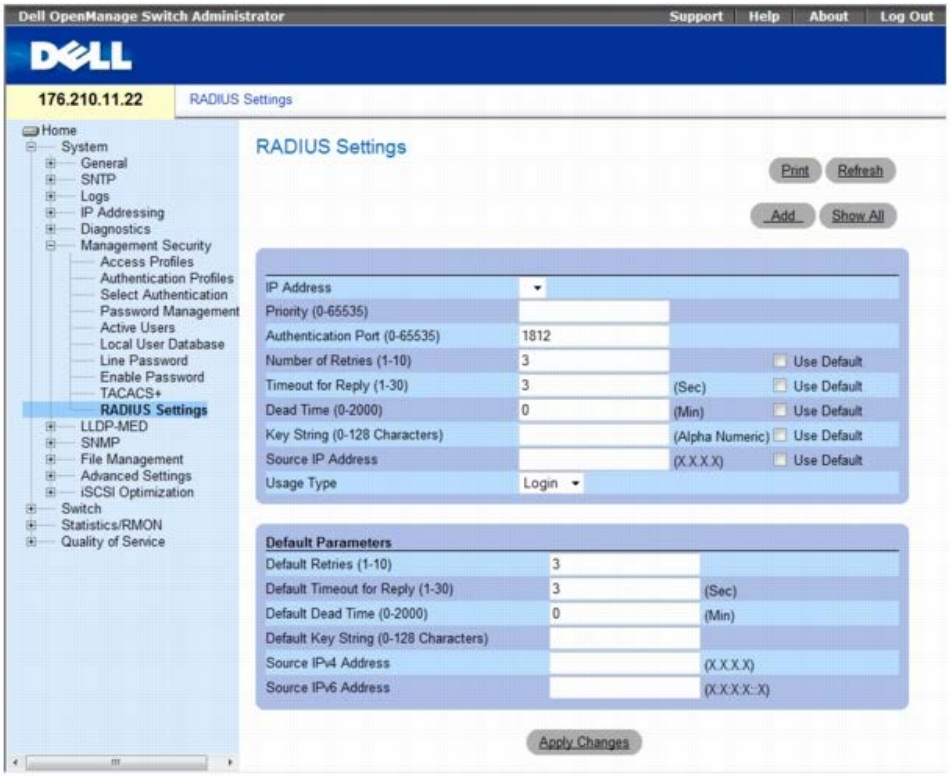
RADIUS の設定

リモート認証ダイヤルインユーザーサービス（RADIUS）サーバーは、ネットワークに対して追加のセキュリティを提供します。最高 4 つまでの RADIUS サーバーを定義することができます。RADIUS サーバーは以下に対して集中認証方法を提供します。

- Telnet アクセス
- Secure Shell アクセス
- ウェブアクセス
- Console アクセス

RADIUS Settings（RADIUS の設定）ページを開くには、ツリー表示で、**System**（システム）® **Management Security**（管理セキュリティ）® **RADIUS** の順にクリックします。

図 **6-73. RADIUS** の設定



RADIUS Settings（RADIUS の設定）ページには、以下のページがあります。

IP Address（IP アドレス） — 認証サーバー IP アドレスのリストです。

- **Priority**（**0-65535**）（優先度（0～65535））— サーバーの優先度です。可能な値は 0～65535 で、0 は最も高い値です。これはサーバーが問い合わせされる順序を設定するために使用されます。
- **Authentication Port**（**0-65535**）（認証ポート（0～65535））— 認証ポートを示します。認証ポートは RADIUS サーバー認証を確認するために使用されます。
- **Number of Retries**（**1-10**）（再試行回数（1～10））— 不具合が起こる前に RADIUS サーバーに送信される要求の数を示します。可能な値は 1～-10 です。
- **Timeout for Reply**（**1-30**）（応答のタイムアウト（1～30））— デバイスがクエリに応答する、または次のサーバーに切り替わる前に RADIUS からの応答を待つ時間を秒単位で示します。可能なフィールド値は 1～30 です。
- **Dead Time**（**0-2000**）（デッドタイム）— サービス要求に対して RADIUS サーバーがバイパスされる時間を（分単位で）示します。その範囲は 0～2000 です。
- **Key String**（**0-128 Characters**）（キーストリング（1～128 文字））— デバイスと RADIUS サーバー間のすべての RADIUS 通信を認証および暗号化するため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**Source IP Address（ソース IP アドレス）— RADIUS サーバーとの通信のために使用されるソース IP アドレスを示します。
- **Usage Type**（使用方法タイプ）—サーバーの使用方法タイプを示します。ログイン、**802.1x**、または、すべて の値のうちのいずれか 1 つが可能です。指定しない場合はすべてがデフォルトになります。
- **Use Default**（デフォルトの使用）— パラメーターにデフォルト値を使用します。

ホスト指定タイムアウト、再施行、または不動作時間値が指定されていない場合は、グローバル値（デフォルト）が各ホストに適用されます。以下のフィールドは RADIUS デフォルト値を設定します。

- **Default Retries**（**1-10**）（デフォルトの再試行回数（1～10））— 不具合が生じる前に RADIUS サーバーに送信されるデフォルトの要求数を示します。
- **Default Timeout for Reply**（**1-30**）（応答のデフォルトタイムアウト（1～30））— タイムアウトになる前に、デバイスが RADIUS サーバーからの返答を待つデフォルトの時間を（秒単位で）示します。デフォルト値は 5 秒です。
- **Default Dead time**（**0-2000**）（デフォルトのデッドタイム（0～2000））— サービス要求に対して RADIUS サーバーがバイパスされるデフォルトの時間を（分単位で）示します。その範囲は 0～2000 です。
- **Default Key String**（**0-128 Characters**）（デフォルトキーストリング（0～128 文字））— デバイスと RADIUS サーバー間のすべての RADIUS 通信を認証および暗号化するため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 IPv4 Address**（送信元 IPv4 アドレス）— RADIUS サーバーとの通信のために使用される送信元 IP バージョン 4 アドレスを指定します。
- **Source IPv6 Address**（送信元 IPv6 アドレス）— RADIUS サーバーとの通信のために使用される送信元 IP バージョン 6 アドレスを指定します。

RADIUS サーバーを新しく追加する場合は、次のパラメーターを追加できます。

- **Supported IP Format**（サポートされている IP 形式）— サーバーでサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** Global（IPv6 グローバル）— IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。

RADIUS パラメーターの定義：

□□□ **RADIUS Settings**（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。

RADIUS の設定がデバイスにアップデートされます。

RADIUS サーバーの追加：

□□□ **RADIUS Settings**（RADIUS の設定）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add RADIUS Server（RADIUS サーバーの追加）ページが開きます。

図 **6-74. RADIUS** サーバーの追加

□□□ 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。

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。

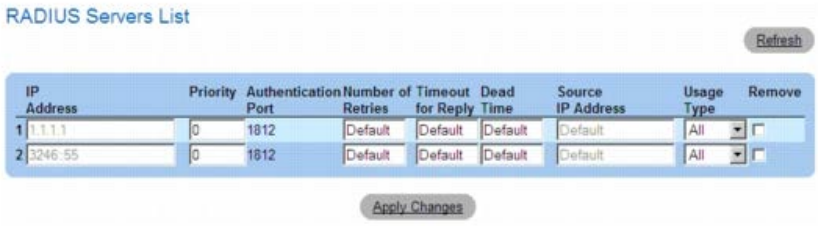
RADIUS サーバーリストの表示：

□□□ **RADIUS Settings**（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 Servers List（RADIUS サーバーリスト）が開きます。

図 **6-75. RADIUS** サーバーリスト



RADIUS サーバーの削除

□□□ **RADIUS Settings**（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 Servers List（RADIUS サーバーリスト）が開きます。

□□□ **RADIUS Servers List**（RADIUS サーバーリスト）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。

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

次の表は、**RADIUS Settings**（RADIUS の設定）ページに表示されるフィールドを定義するための等価 **CLI** コマンドをまとめたものです。

CLI コマンド	説明
radius-server timeout *timeout*	デバイスがサーバーホストの応答を待つ間隔を指定します。
radius-server source-ip source	RADIUS サーバーとの IPv4 通信のために使用される送信元 IPv4 アドレスを指定します。
radius-server source-ipv6 source	RADIUS サーバーとの IPv6 通信のために使用される送信元 IPv6 アドレスを指定します。
radius-server retransmit retries	ソフトウェアが RADIUS サーバーホストのリストを探す

	回数を指定します。
radius-server deadtime deadtime	使用不能なサーバーをスキップするように設定します。
radius-server key key-string	ルーターと RADIUS サーバー間のすべての RADIUS 通信のため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 サーバーの設定を表示します。

CLI コマンドの例は次のとおりです。

```
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
```

LLDP および MED の設定

Link Layer Discovery Protocol（LLDP）は、マルチベンダ環境のネットワークトポロジを検出および保持することによって、ネットワーク管理者がトラブルシューティングとネットワーク管理の強化を実現できるようにします。LLDP では、ネットワークデバイスが自身を他のシステムに公示し、検出された情報を保存する方法を標準化することによって、ネットワークの隣接デバイスを検出します。デバイス検出情報には以下が含まれます。

- デバイスの ID
- デバイスの機能
- デバイスの構成

公示を行うデバイスは、1 つの LAN パケットで複数の公示メッセージセットを送信します。複数の公示セットは、パケットの Type Length Value（タイプ-長さ-値）（TLV）フィールドで送信されます。LLDP デバイスは、システム名、システム ID、システムの説明、およびシステムの機能の公示に加えて、シャーシおよびポート ID の公示をサポートしている必要があります。

本項には以下のトピックがあります。

- グローバル LLDP プロパティの定義
- LLDP ポートの設定の定義
- MED ネットワークポリシーの定義
- LLDP MED ポートの設定の定義
- LLDP 隣接情報の表示

LLDP Media Endpoint Discovery（LLDP-MED）は、異なる IP システムを単一ネットワークの LLDP に共存させることで、ネットワークの柔軟性を高めます。

ネットワーク上に位置するデバイスや、デバイスが位置する場所などの詳細なネットワークトポロジ情報を提供します。たとえば、どの IP 電話がどのポートに接続されているか、どのソフトウェアがどのスイッチ上で実行されているか、どのポートがどの PC に接続されているかなどの情報が提供されます。以下に関するポリシーをネットワーク全体に自動的に展開します。

- QoS ポリシー
- 音声 VLAN

IP 電話の位置情報による緊急通報サービス（E-911）を提供します。

LLDP MED から以下に関する警告がネットワーク管理者に送信されることにより、トラブルシューティング情報が提供されます。

- ポートスピードおよび二重モードの拮抗
- QoS ポリシーの設定間違い

本項には、次のトピックがあります。

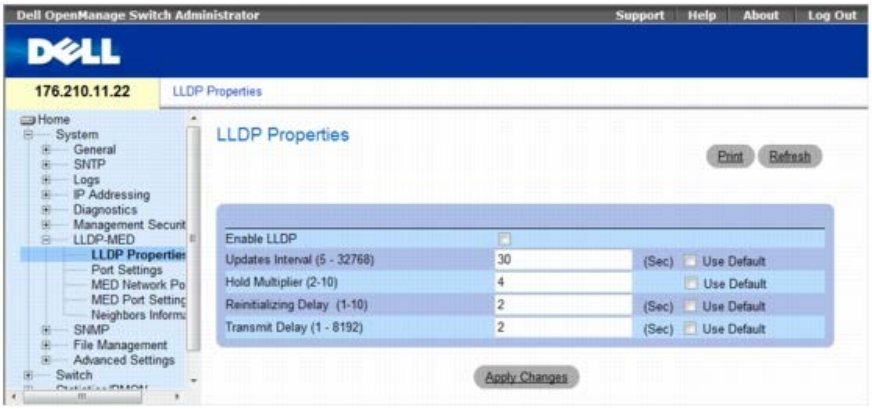
- LLDP プロパティの定義

LLDP プロパティの定義

LLDP Properties（LLDP プロパティ）ページには、LLDP を設定するためのフィールドがあります。

LLDP Properties（LLDP プロパティ）ページを開くには、ツリー表示の **System**（システム）® **LLDP-MED** ® **LLDP Properties**（LLDP プロパティ）をクリックします。

図 **6-76. LLDP** プロパティ



- **Enable LLDP**（LLDP を有効にする） — デバイス上で LLDP が有効になっているかどうかを示します。 可能なフィールド値は次のとおりです。
  - **Checked**（チェックあり）— デバイス上で LLDP が有効になっていることを示します。
  - **Unchecked**（チェックなし）— デバイス上で LLDP が無効になっていることを示します。これがデフォルト値になっています。
- **Updates Interval**（**5-32768**）（アップデート間隔（5～32768））— LLDP 公示のアップデートが送信されるペースを示します。可能なフィールドの範囲は 5～32768 秒です。デフォルト値は 30 秒です。
- **Hold Multiplier**（**2-10**）（ホールドマルチプライヤ（2～10））— LLDP アップデートで送信されるホールド時間をタイマー値の倍数として指定します。可能なフィールド値は 2～10です。フィールドのデフォルト値は 4 秒です。
- **Reinitializing Delay**（**1-10**）（再初期化ディレイ（1～10））— LLDP ポートが LLDP 転送の再初期化まで待機する最小時間を秒単位で指定します。可能なフィールドの範囲は 1～10 秒です。デフォルト値は 2 秒です。
- **Transmit Delay**（**1-8192**）（送信ディレイ（1～8192））— LLDP ローカルシステムの MIB の変更によって生じる連続した LLDP フレーム送信の経過時間を示します。可能なフィールド値は 1～8192 秒です。デフォルト値は 2 秒です。

CLI コマンドを使用した LLDP の設定

表 **6-43. LLDP** プロパティに関連する **CLI** コマンド

CLI コマンド	説明
`lldp enable (global)`	Link Layer Discovery Protocol を有効にします。
`lldp hold-multiplier` `number`	受信側のデバイスが Link Layer Discovery Protocol（LLDP）パケットを廃棄するまでのパケット保持時間を指定します。
`lldp reinit-delay` `Seconds`	LLDP ポートが初期化を行う前に待機する最小時間を指定します。
`lldp tx-delay Seconds`	連続した LLDP フレーム伝送のディレイを指定します。

CLI コマンドの例は次のようになります。

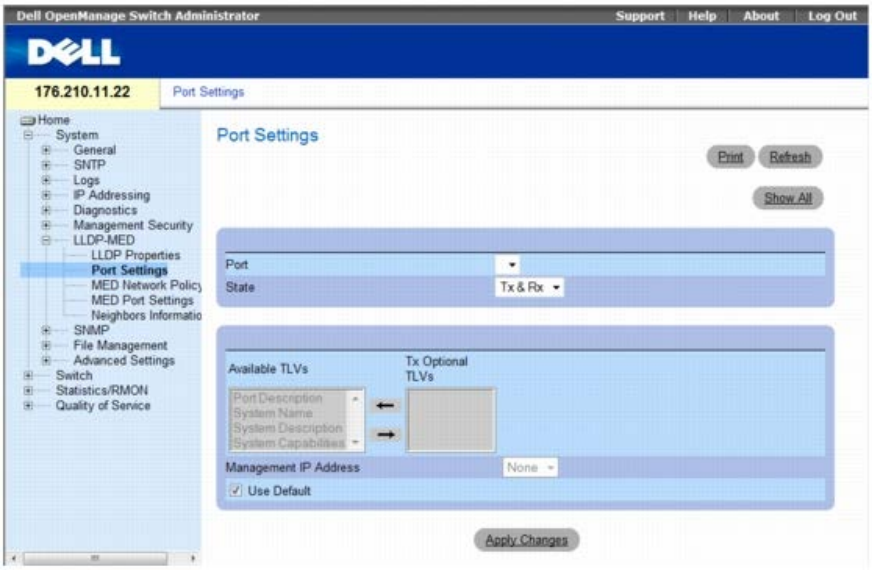
```
Console (config)# interface ethernet g1
Console (config-if) # lldp enable
```

LLDP ポートの設定の定義

LLDP の **Port Settings**（ポートの設定）ページを使用することにより、ネットワーク管理者は、ポート番号、LLDP ポート番号、公示されるポート情報のタイプを含む LLDP ポートの設定を定義できます。

Port Settings（ポートの設定）ページには、LLDP を設定するためのフィールドがあります。**Port Settings**（ポートの設定）ページを開くには、ツリー表示の **System**（システム）® **LLDP-MED** ® **Port Settings**（ポートの設定）をクリックします。

図 **6-77.** ポートの設定



- **Port**（ポート） — LLDP が有効になっているポートのリストです。
- **State**（状態） — LLDP が有効になっているポートのタイプを示します。可能なフィールド値は次のとおりです。
  - **Tx Only**（Tx のみ）— 送信 LLDP パケットのみを有効にします。
  - **Rx Only**（Rx のみ）— 受信 LLDP パケットのみを有効にします。
  - **Tx & Rx**（Tx および Rx）— 送信および受信 LLDP パケットを有効にします。これがデフォルト値になっています。
  - **Disable**（無効） — ポート上で LLDP が無効になっていることを示します。
- **Available TLVs**（利用可能 TLV）— ポートから公示できる利用可能 TLV のリストです。可能なフィールド値は次のとおりです。
  - **Port Description**（ポートの説明）— ポートの説明を公示します。
  - **System Name**（システム名） — システム名を公示します。
  - **System Description**（システムの説明） — システムの説明を公示します。
  - **System Capabilities**（システムの機能） — システムの機能を公示します。
- **Tx Optional TLVs**（Tx オプション TLV） — ポートから公示されるオプション TLV のリストです。完全なリストに関しては、**Available TLVs**（利用可能 TLV） フィールドを参照してください。
- **Management IP Address**（管理 IP アドレス）— インタフェースから公示される管理 IP アドレスを示します。
  - **Use Default**（デフォルトの使用）— TLV を含める方法を指定します。
  - **Checked**（チェックマークあり）— デフォルトでは、必須 TLV のみが使用されます。必須 TLV は、シャーシサブタイプ（MAC アドレス）、ポートサブタイプ（ポート番号）、および TTL（Leave 時間 120 秒）です。
  - **Unchecked**（チェックマークなし）— 上記の必須 TLV 3 つで構成されるユーザー定義の TLV に加えて、TLV の使用可能なセットからユーザーが移動したオプションの TLV です。

LLDP Port Table（LLDP ポート表）ページには、LLDP ポートの設定が表示されます。**LLDP Port Table**（LLDP ポート表）を開くには、ツリー表示の **Security**（セキュリティ）® **LLDP** ® **Port Settings**（ポートの設定）® **Show All**（すべてを表示）をクリックします。

図 **6-78. LLDP** ポート表

表 **6-44. LLDP** ポートの設定に関連する **CLI** コマンド

CLI コマンド	説明
clear lldp rx interface	LLDP RX 状態マシンを再スタートし、隣接表をクリアします。
lldp optional-tlv *tlv1 [tlv2 ... tlv5]*	基本セットからどのオプション TLV を送信するかを指定します。
lldp enable [rx | tx | both]	インタフェース上で Link Layer Discovery Protocol（LLDP）を有効にします。

CLI コマンドの例は次のようになります。

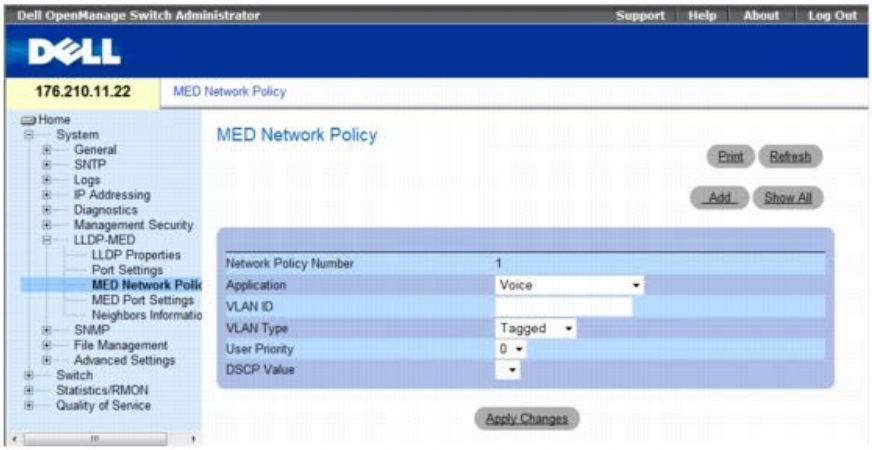
```
Console (config)# interface ethernet g1
Console（config-if）# lldp enable
```

LLDP MED ネットワークポリシーの定義

MED Network Policy（MED ネットワークポリシー）ページには、LLDP を設定するためのフィールドがあります。

MED Network Policy（MED ネットワークポリシー）ページを開くには、ツリー表示の **System**（システム）® **LLDP-MED** ® **MED Network Policy**（MED ネットワークポリシー）をクリックします。

図 **6-79. MED** ネットワークポリシー



MED Network Policy（**MED** ネットワークポリシー）ページには以下のフィールドがあります。

- **Network Policy Number**（ネットワークポリシー番号） — ネットワークポリシー番号を表示します。
- **Application**（アプリケーション） — ネットワークポリシーが定義されるアプリケーションを表示します。可能なフィールド値は次のとおりです。
  - **Voice**（音声） — 音声アプリケーション用にネットワークポリシーが定義されることを示します。
  - **Voice Signaling**（音声シグナリング） — 音声シグナリングアプリケーション用にネットワークポリシーが定義されることを示します。
  - **Guest Voice**（ゲスト音声）— ゲスト音声アプリケーション用にネットワークポリシーが定義されることを示します。
  - **Guest Voice Signaling**（ゲスト音声シグナリング）— ゲスト音声シグナリングアプリケーション用にネットワークポリシーが定義されることを示します。
  - **Softphone Voice**（ソフトフォン音声）— ソフトフォン音声アプリケーション用にネットワークポリシーが定義されることを示します。
  - **Video Conferencing**（テレビ会議）— テレビ会議アプリケーション用にネットワークポリシーが定義されることを示します。
  - **Streaming Video**（ストリーミングビデオ）— ストリーミングビデオアプリケーション用にネットワークポリシーが定義されることを示します。
  - **Video Signaling**（ビデオシグナリング）— ビデオシグナリングアプリケーション用にネットワークポリシーが定義されることを示します。
- **VLAN ID**— ネットワークポリシーが定義される VLAN の ID を表示します。

- **VLAN Type**（VLAN のタイプ）— ネットワークポリシーが定義される VLAN のタイプを示します。可能なフィールド値は次のとおりです。
  - **Tagged**（タグ付き）— タグ付き VLAN 用にネットワークポリシーが定義されることを示します。
  - **Untagged**（タグなし）— タグなし VLAN 用にネットワークポリシーが定義されることを示します。
- **User Priority**（ユーザー優先度）— ネットワークアプリケーションに割り当てられる優先度を定義します。範囲は、0～7 です。
- **DSCP Value**（DSCP 値）— ネットワークポリシーに割り当てられてる DSCP 値を定義します。範囲は、0～63 です。

MED ネットワークポリシーの追加

□□□ **MED Network Policy**（MED ネットワークポリシー）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add Network Policy（ネットワークポリシーの追加）ページが開きます。

図 **6-80.** ネットワークポリシーの追加

□□□ 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。

新しいネットワークポリシーが追加され、デバイスがアップデートされます。

MED ネットワークポリシー表の表示

□□□ **MED Network Policy**（MED ネットワークポリシー）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

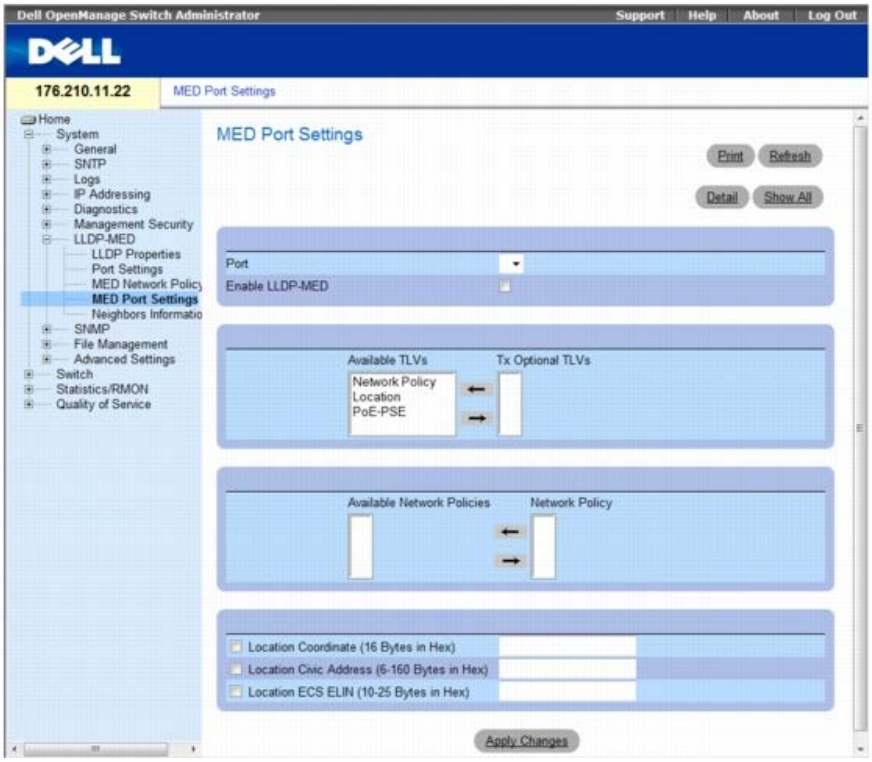
MED Network Policy Table（MED ネットワークポリシー表）が開きます。

図 **6-81. MED** ネットワークポリシー表

LLDP MED ポートの設定の定義

MED Port Settings（MED ポートの設定） には、特定のポートに LLDP ネットワークポリシーを割り当てるためのパラメーターがあります。**MED Port Settings**（MED ポートの設定） ページを開くには、ツリー表示の **System**（システム）® **LLDP-MED** ® **Port Settings**（ポートの設定） をクリックします。**MED Port Settings**（MED ポートの設定）が開きます。

図 **6-82. MED** ポートの設定



MED Port Settings（MED 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） — LLDP-MED が有効または無効になっているポートを表示します。
- **Enable LLDP-MED**（LLDP-MED を有効にする） — 選択されたポート上で LLDP-MED を有効にするかどうかを示します。可能なフィールド値は次のとおりです。
  - **Checked**（チェックあり）— ポート上で LLDP-MED を有効にします。
  - **Unchecked**（チェックなし） — ポート上で LLDP-MED を無効にします。これがデフォルト値になっています。
- **Tx Optional TLVs/Available TLVs**（Tx オプション TLV / 利用可能 TLV）— ポートから公示できる利用可能 TLV のリストです。可能なフィールド値は次のとおりです。
  - **Network Policy**（ネットワークポリシー）— ポートに設定されたネットワークポリシーを公示します。
  - **Location**（場所）— ポートの場所を公示します。
  - **PoE-PSE** — 接続されているメディアが PoE か PSE（給電装置）デバイスかを示します。
- **Network Policy/Available Network Policy**（ネットワークポリシー / 利用可能なネットワークポリシー）— ポートに割り当てることができるネットワークポリシーのリストです。
- **Location Coordinate**（**16 Bytes in Hex**）（位置座標（16 進数で 16 バイト））— デバイスの位置マップ座標（16 進数で 16 バイト）を表示します。
- **Location Civic Address**（**6-160 Bytes in Hex**）（位置 - 住所（16 進数で 6～160 バイト））— デバイスが設置されている位置 - 住所（たとえば、414 23rd Ave E）を表示します。可能なフィールド値の範囲は 16 進数で 6～160 バイトです。
- **Location ECS ELIN**（**10-25 Bytes in Hex**）（ECS ELIN の位置（16 進数で 10～25 バイト））— デバイスの ECS ELIN 位置を表示します。フィールドの範囲は、16 進数で 10～25 バイトです。

MED ポート設定の変更

□□□ **MED Port Settings**（MED ポートの設定）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。

パラメーターがデバイスに保存されます。

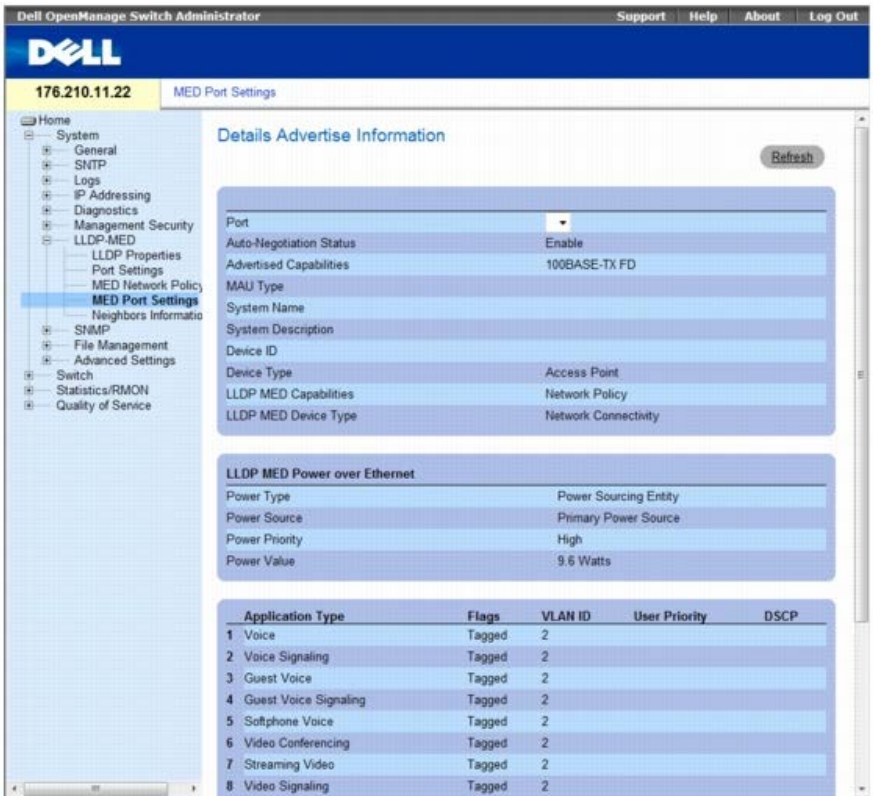
Advertise Information Details（公示情報の詳細）の表示

□□□ **MED Port Settings**（MED ポートの設定）ページを開きます。

□□□ **Details**（詳細）をクリックします。

Details Advertise Information（公示情報の詳細）ページが開きます。

図 **6-83.** 公示情報の詳細ページ



Details Advertise Information（公示情報の詳細）ページには以下のフィールドがあります。

- **Port**（ポート）— 詳細情報が表示されるポートです。
- **Auto-Negotiation Status**（オートネゴシエイションステータス） — ポートのオートネゴシエイションステータスです。可能なフィールド値は次のとおりです。
  - **Enabled**（有効）— ポート上でオートネゴシエイションが有効になっています。
  - **Disabled**（無効）— ポート上でオートネゴシエイションが無効になっています。
- **Advertised Capabilities**（公示される機能）—ポートに関して公示されるポートの機能です。
- **MAU Type**（MAU のタイプ） — メディアアタッチメントユニットのタイプを示します。
- **System Name**（システム名）— 公示されるシステム名です。
- **System Description**（システムの説明）— 公示されるシステムの説明です。
- **Device ID**（デバイス ID）— デバイスの MAC アドレスなどの公示されるデバイス ID です。
- **Device Type**（デバイスのタイプ）— デバイスのタイプです。
- **LLDP MED Capabilities**（LLDP MED の機能）— ポートによって公示される TLV です。
- **LLDP MED Device Type**（LLDP MED デバイスのタイプ）— 送信側がネットワーク接続デバイスかエンドポイントデバイスかを示します。
- **Power Type**（電源のタイプ）— ポートの電源のタイプです。
- **Power Source**（電源）— ポートの電源です。
- **Power Priority**（電源優先度）— ポートの電源優先度です。
- **Power Value**（電源値）— ポートの電源値（ワット）です。
- **LLDP MED Network Policy**（LLDP MED ネットワークポリシー）— 以下のアプリケーションタイプごとに設定されたポートの LLDP ネットワークポリシーです。
  - Voice（音声）
  - Voice Signaling（音声シグナリング）
  - Guest Voice（ゲスト音声）
  - Guest Voice Signaling（ゲスト音声シグナリング）
  - Softphone Voice（ソフトフォン音声）

- Video Conferencing（テレビ会議）
- Streaming Video（ストリーミングビデオ）
- Video Signaling（ビデオシグナリング）

- **Flags**（フラグ）— アプリケーションタイプの VLAN タグステータスを表示します。可能なフィールド値は次のとおりです。
  - **Tagged**（タグ付き）— パケットにタグが付いています。
  - **Untagged**（タグなし）— パケットにタグが付いていません。
- **VLAN ID** — アプリケーションタイプの VLAN 番号を表示します。
- **User Priority**（ユーザー優先度）— アプリケーションタイプの VLAN 番号を表示します。
- **DSCP Value**（DSCP 値）— ネットワークポリシーに割り当てられてる DSCP 値を定義します。可能なフィールド値は 1～64 です。
- **LLDP MED Location**（LLDP MED の場所）— 公示された LLDP ポートの場所です。
  - **Coordinates**（座標）— デバイスの場所のマップ座標を表示します。
  - **Civic Address**（住所） — デバイスの場所の住所またはストリートアドレスを表示します（例：414 23rd Ave E）。可能なフィールド値は 6～160 文字です。
  - **ECS ELIN** — デバイスの場所の ECS ELIN を表示します。フィールドの範囲は 10～25 です。

MED Port Settings Table（MED ポートの設定表）の表示

□□□ **MED Port Settings**（MED 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。

MED Port Settings Table（MED ポートの設定表）が開きます。

図 **6-84. MED** ポートの設定表

LLDP 隣接情報の表示

Neighbors Information（隣接情報）ページには、隣接デバイスの LLDP 公示によって受け取った情報があります。**Neighbor Information**（隣接情報）ページを開くには、ツリー表示の **System**（システム）® **LLDP-MED** ® **Neighbors Information**（隣接情報）をクリックします。

図 **6-85.** 隣接情報

- **Port**（ポート）— 隣接情報が表示されるポート番号を表示します。
- **Device ID**（デバイス ID）— 隣接デバイスの ID を表示します。
- **System Name**（システム名）— 隣接システムの名前を表示します。
- **Port ID**（ポート ID）— 隣接ポートの ID を表示します。
- **Capabilities**（機能）— 隣接デバイスの機能を表示します。

表からのポートの削除

□□□ **Neighbors Information**（隣接情報）ページを開きます。

□□□ 削除する各ポートの **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。ポートが削除されます。

表のクリア

□□□ **Neighbors Information**（隣接情報）ページを開きます。

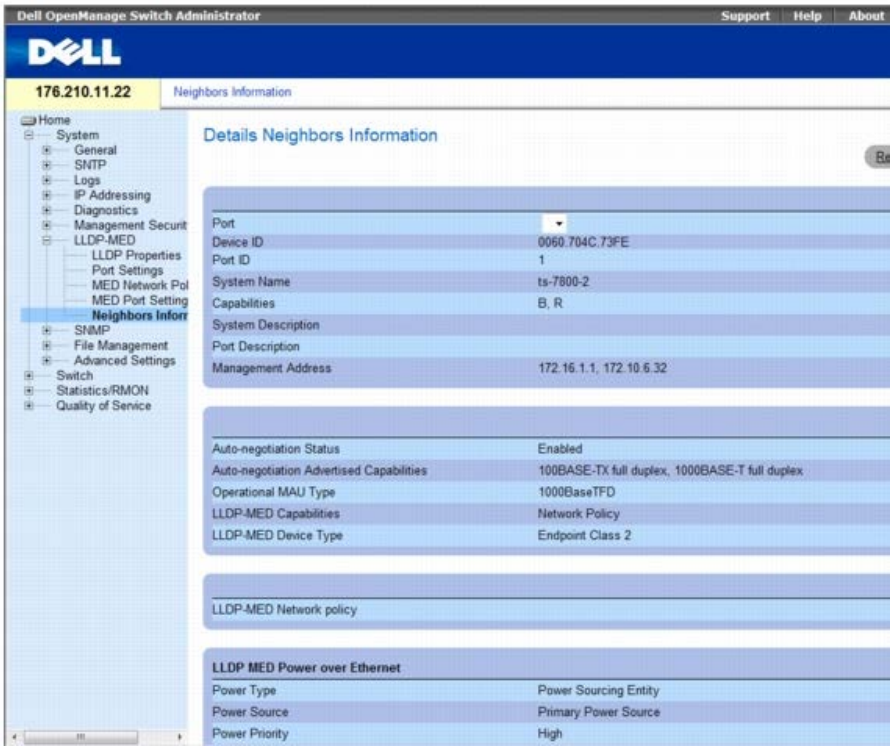
□□□ **Clear Neighbors Table**（隣接表のクリア）をクリックします。表がクリアされます。

隣接デバイスから公示された **LLDP MED** 情報の詳細の表示

□□□ **Neighbors Information**（隣接情報）ページを開きます。

□□□ 目的のエントリの **Details**（詳細）ボタンをクリックします。Details Neighbor Information（隣接情報の詳細）ページが表示されます。

図 **6-86.** 隣接情報の詳細



フィールドの詳細に関しては、上記の Details Advertise Information（公示情報の詳細）ページを参照してください。

表 **6-45. LLDP** 隣接情報に関連する **CLI** コマンド

CLI コマンド	説明
show lldp neighbors interface	Link Layer Discovery Protocol（LLDP）を使用して検出された隣接デバイスに関する情報を表示します。

CLI コマンドの例は次のようになります。

Port	Device ID	Port ID	System Name	Capabilities
3/e31	00:00:77:77:00:00	1/g3		0

SNMP パラメーターの定義

SNMP（Simple Network Management Protocol）はネットワークデバイスの管理メソッドを提供します。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 および v2

SNMP エージェントはスイッチを管理するために使用される変数のリストを維持します。変数は MIB（Management Information Base）で定義されます。MIB はエージェントによって管理される変数を表示します。SNMP エージェントは、MIB 指定フォーマットおよびネットワーク全体にわたる情報にアクセスするためのフォーマットを定義します。SNMP エージェントへのアクセス権はアクセスストリングによってコントロールされます。

デフォルトで SNMPv1 と v2 が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、アクセス制御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 のユーザーセキュリティモデル（USM）が定義されます。

- **Authentication**（認証）— データの完全性とデータ発信元認証を提供します。
- **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 メッセージに対する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）— メッセージディレイまたはメッセージ冗長が発生しないように保護します。SNMP エージェントは着信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、キーアップデート、およびキー使用を定義します。

スイッチは、Object ID（OID）（オブジェクト ID）に基づく SNMP 通知フィルター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
- 機能アクセス制御
- トラップ

認証またはプライバシーキーは、ユーザーセキュリティモデル（**USM**）内で変更できます。

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。

本項には、次のトピックがあります。

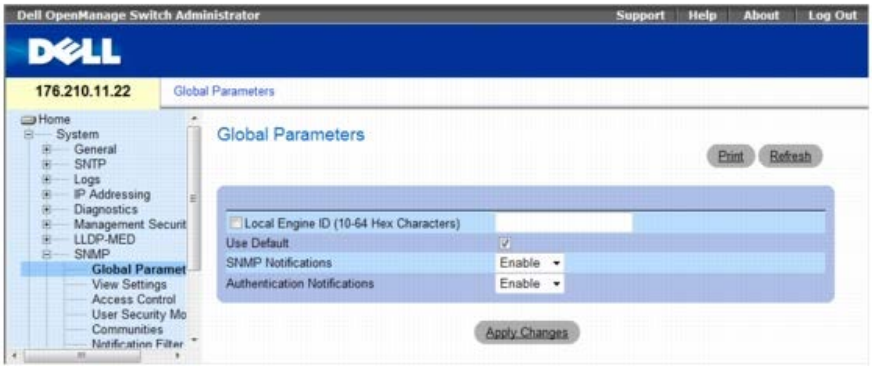
- SNMP グローバルパラメーターの定義
- SNMP ビューの設定の定義
- SNMP アクセス制御の定義
- SNMP ユーザーセキュリティの割り当て
- SNMP コミュニティの定義
- SNMP 通知フィルターの定義
- SNMP 通知受信者の定義

SNMP グローバルパラメーターの定義

SNMP Global Parameters（SNMP グローバルパラメーター）ページでは、SNMP 通知および認証通知を有効にすることができます。

SNMP Global Parameters（SNMP グローバルパラメーター）ページを開くには、ツリー表示の **System**（システム）® **SNMP** ® **Global Parameters**（グローバルパラメーター）をクリックします。

図 **6-87. SNMP** グローバルパラメーター



SNMP Global Parameters（SNMP グローバルパラメーター）ページには、以下のフィールドがあります。

- **Local Engine ID**（**10-64 Hex Characters**）（ローカルエンジン ID（16 進文字 10～64））— ローカルデバイスのエンジン ID を示します。フィールドの値は 16 進文字列です。16 進文字列内の各バイトは、2 桁の 16 進数です。各バイトはピリオドまたはコロンで区切ることができます。エンジン ID は、SNMPv3 を有効にする前に定義されている必要があります。
  - スタンドアロンデバイスの場合は、エンタープライズ番号とデフォルト MAC アドレスから成るデフォルトのエンジン ID を選択します。
  - スタッキング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とって一意であることを確認します。これにより、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止します。
- **Use Default**（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。デフォルトのエンジン ID は、デバイスの MAC アドレスに基づいており、次の標準に従って定義されます。
  - 最初の **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 です。
  - 第 **5** オクテット — 続く MAC アドレスを示す 3 に設定されます。
  - 最後の **6** オクテット — デバイスの MAC アドレスです。
- **SNMP Notifications**（SNMP 通知） — ルーターが送信する SNMP 通知を有効または無効にします。
- **Authentication Notifications**（認証通知）— 認証に失敗した場合にルーターが送信する SNMP トラップを有効または無効にします。

SNMP 通知を有効にする

□□□ SNMP Global Parameters（SNMP グローバルパラメーター）ページを開きます。

□□□ **SNMP Notifications**（SNMP 通知）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。

SNMP 通知が有効になり、デバイスがアップデートされます。

認証通知を有効にする

□□□ **SNMP Global Parameters**（SNMP グローバルパラメーター）ページを開きます。

□□□ **Authentication Notifications**（認証通知）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。

CLI コマンドを使用して SNMP 通知を有効にする

SNMP Global Parameters（SNMP グローバルログパラメーター）ページにあるフィールドを表示するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
snmp-server enable traps	ルーターが SNMP トラップを送信できるようにします。
snmp-server trap authentication	認証に失敗した場合にルーターが SNMP トラップを送信できるようにします。
show snmp	SNMP 通信のステータスをチェックします。
snmp-server engine ID local {*engineid-string* |	ローカルデバイスのエンジン ID を表示します。フィールドの値は 16 進文字列です。16 進文字列内の各バイトは、2 桁の 16 進数です。各バイトはピリオドまたはコロンで区切ることができます。エンジン ID は、SNMPv3 を有効にする前に定義されている必要があります。

default}	

CLI コマンドの例は次のようになります。

```
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
```

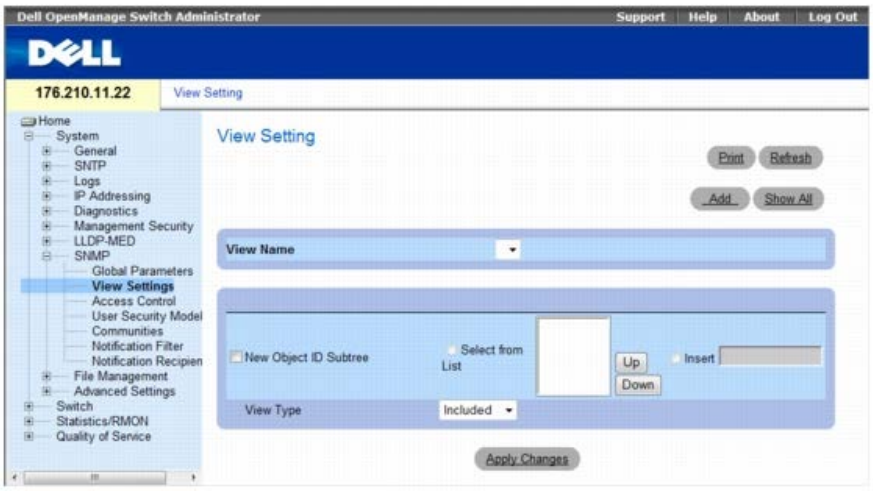
SNMP ビューの設定の定義

SNMP 表示では、デバイスの機能または機能の一部へのアクセスを許可またはブロックします。たとえば、あるビューで、SNMP グループ A にマルチキャストグループへの読み取り専用（R/O）アクセスを許可し、SNMP グループ B にマルチキャストグループへの読み書き（R/W）アクセスを許可する状態を定義することができます。機能へアクセスは、MIB 名または MIB オブジェクト ID によって付与されます。

上および下矢印を使用して、MIB ツリーおよび MIB ブランチ間を移動できます。

SNMPv3 View Settings（SNMPv3 ビューの設定）ページを開くには、ツリー表示の **System**（システム）® **SNMP** ® **View Settings**（ビューの設定）をクリックします。

図 **6-88. SNMPv3** ビューの設定



SNMPv3 View Settings（SNMPv3 表示の設定）ページには、以下のフィールドがあります。

- **View Name**（ビュー名） — ユーザー定義のビューのリストがあります。ビュー名の最大長は英数字 30 文字です。
- **New Object ID Subtree**（新規オブジェクト ID サブツリー） — 選択された SNMP ビューにデバイス機能 OID を含めるか除外するかを示します。

Selected from List（リストから選択） — 上および下ボタンで全デバイス OID のリストをスクロールして、デバイス機能 OID を選択します。

- **Inser**（挿入） — デバイス機能 OID を指定します。

- **View Type**（ビューのタイプ） — 定義された OID ブランチを選択された SNMP ビューに含めるか除外するかを示します。

ビューの追加

□□□ **SNMPv3 View Settings**（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。

Add A View（表示の追加）ページが開きます。

図 **6-89. Add A View**（表示の追加）

□□□ 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。

SNMP ビューが追加され、デバイスがアップデートされます。

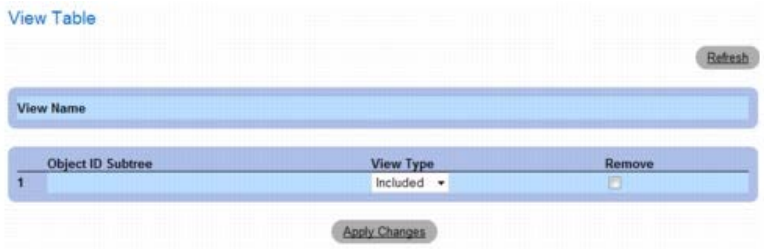
ビュー表の表示

□□□ **SNMPv3 View Settings**（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。

View Table（ビュー表）ページが開きます。

図 **6-90.** ビュー表



CLI コマンドを使用した SNMPv3 表示の定義

次の表は、 **SNMPv3 View Settings**（SNMPv3 ビューの設定）ページに表示されるフィールドを定義するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
snmp-server view *view-name* oid-tree {**included** | **excluded**}	ビューエントリを作成またはアップデートします。
show snmp views [*viewname*]	ビューの設定を表示します。

CLI コマンドの例は次のとおりです。

```
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

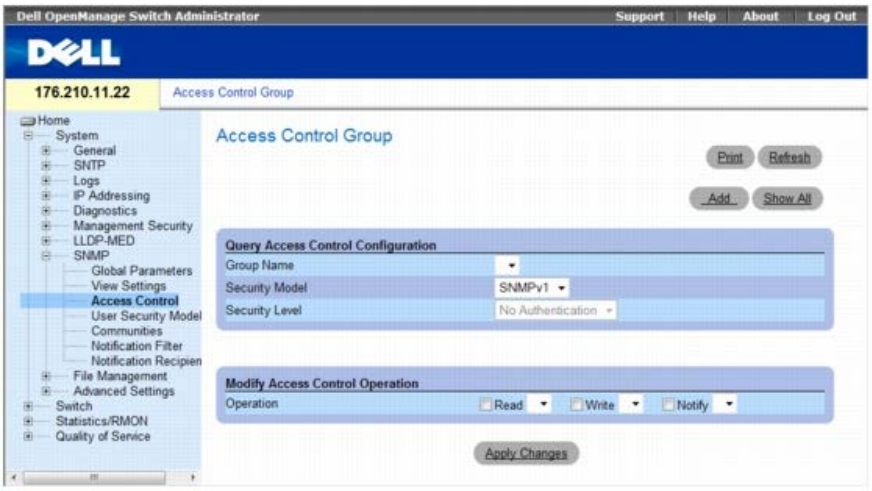
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

SNMP アクセス制御の定義

Access Control（アクセス制御）ページには、SNMP グループを作成し、SNMP アクセス制御特権を SNMP グループに割り当てるための情報が表示されます。ネットワーク管理者は、グループによって、特定のデバイスの機能または機能の一部に対するアクセス権を割り当てることができます。

Access Control Group（アクセス制御グループ）ページを開くには、ツリー表示の **System**（システム）® **SNMP**® **Access Control**（アクセス制御）をクリックします。

図 **6-91.** アクセス制御グループ



Access Control Group（アクセス制御グループ）には、以下のフィールドがあります。

- **Group Name**（グループ名）— アクセス制御のルールが適用されるユーザー定義のグループです。フィールドの範囲は最大 30 文字です。
- **Security Model**（セキュリティモデル）— 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次のとおりです。
  - **SNMPv1** — SNMPv1 がグループに定義されます。
  - **SNMPv2** — SNMPv2 がグループに定義されます。
  - **SNMPv3** — SNMPv3 がグループに定義されます。
- **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 のみに適用されます。可能なフィールド値は次のとおりです。
  - **No Authentication**（認証なし） — 認証もプライバシーセキュリティレベルもグループに割り当てられません。
  - **Authentication**（認証） — SNMP メッセージを認証し、SNMP メッセージの発信元が確実に認証されるようにします。
  - **Privacy**（プライバシー） — SNMP メッセージを暗号化します。
- **Operation**（動作） — グループのアクセス権を定義します。可能なフィールド値は次のとおりです。
  - **Read**（読み取り） — 管理アクセスは読み取り専用に制限され、割り当てられた SNMP ビューに対する変更はできません。
  - **Write**（書き込み） — 読み書きの管理アクセスが許可され、割り当てられた SNMP ビューへの変更が可能になります。
  - **Notify**（通知） — 割り当てられた SNMP ビューに関するトラップを送信します。

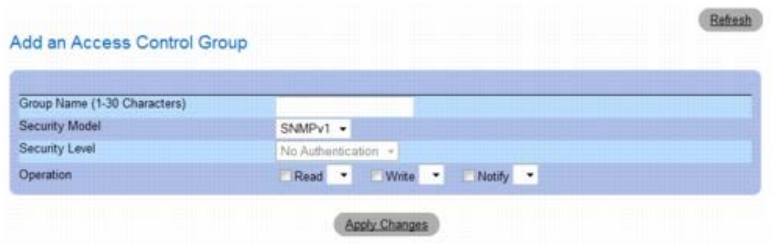
SNMP グループの定義

□□□ **Access Control Group**（アクセス制御グループ）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add an Access Control Group（アクセス制御グループの追加）ページが開きます。

図 **6-92.** アクセス制御グループの追加



□□□ **Add an Access Control Group**（アクセス制御グループの追加）ページ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。

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

□□□ **Access Control Group**（アクセス制御グループ）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Access Table（アクセス表）が開きます。

図 **6-93. Access Table**（アクセス表）

SNMP グループの削除

□□□ **Access Control Group**（アクセス制御グループ）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Access Table（アクセス表）が開きます。

□□□ SNMP グループを選択します。

□□□ **Remove**（削除）チェックボックスをクリックします。

□□□ **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 アクセス制御の定義

次の表は、 **Access Control Group**（アクセス制御グループ）ページに表示されるフィールドを定義するための等価 CLI コマンドをまとめたものです。

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、または 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。

CLI コマンドの例は次のようになります。

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

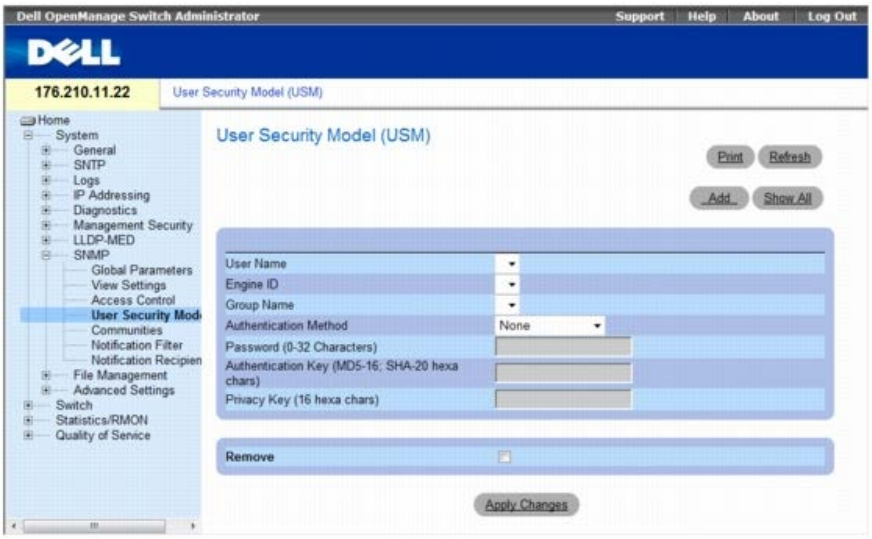
SNMP ユーザーセキュリティの割り当て

SNMPv3 User Security Model（**USM**）（SNMPv3 ユーザーセキュリティモード（USM））ページでは、システムのユーザーを SNMP グループに割り当て、ユーザー認証方法を定義できます。

SNMPv3 User Security Model（**USM**）（SNMPv3 ユーザーセキュリティモード（USM））ページを開くには、ツリー表示で **System**（システム）® **SNMP® User**

Security Model（ユーザーセキュリティモデル）の順にクリックします。

図 **6-94. SNMPv3** ユーザーセキュリティモデル（**USM**）



SNMPv3 User Security Model（**USM**）（SNMPv3 ユーザーセキュリティモデル（USM））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） — ユーザー定義のユーザー名のリストがあります。フィールドの範囲は最大で英数字 30 文字です。
- **Engine ID**（エンジン ID）— ユーザーが接続されるローカルまたはリモートの SNMP エンティティを示します。ローカルの SNMP エンジン ID を変更または削除すると、SNMPv3 ユーザーデータベースが削除されます。
- **Group Name**（グループ名） — ユーザ定義の SNMP グループのリストがあります。SNMP グループは、**Access Control Group**（アクセス制御グループ） ページで定義されます。
- **Authentication Method**（認証方法） — ユーザの認証に使用される方法です。可能なフィールド値は次のとおりです。
  - **None**（なし） — ユーザ認証は使用されません。
  - **MD5 Password**（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を入力する必要があります。
  - **SHA Password**（SHA パスワード） — 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を入力する必要があります。
  - **MD5** Key（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** Key（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。
- **Password**（**0-32 Characters**）（パスワード（0～32 文字））— グループ用のユーザー定義パスワードを変更します。 パスワードの最大長は英数字 32 文字です。
- **Authentication Key**（**MD5-16; SHA-20 hexa chars**）（認証キー（MD5-16、SHA-20 16 進文字））— HMAC-MD5-96 または HMAC-SHA-96 の認証レベルを定義します。認証キーとプライバシーキーを入力して認証キーを定義します。認証だけが必要な場合は、MD5 用に 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は、MD5 用に 32 バイトが定義されます。16 進数文字列内の各バイトは、2 桁の 16 進数です。各バイトはピリオドまたはコロンで区切ることができます。
- **Privacy Key**（**16 hexa characters**）（プライバシーキー（16 進文字））— 認証だけが必要な場合は、20 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は、16 バイトが定義されます。16 進文字列内の各バイトは、2 桁の 16 進数です。各バイトはピリオドまたはコロンで区切ることができます。
- **Remove**（削除） — チェックを入れると、指定されたグループからユーザーが削除されます。
  - **Checked**（チェックマークあり）— 指定したグループからユーザーを削除します。
  - **Unchecked**（チェックマークなし）— 指定したグループ内にユーザーを保持します。

ユーザーのグループへの追加

□□□ **SNMPv3 User Security Model**（**USM**）（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。

Add SNMPv3 User Name（SNMPv3 ユーザー名の追加）ページが開きます。

図 **6-95. SNMPv3** ユーザー名の追加

□□□ 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 User Security Model**（**USM**）（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。

User Security Model Table（ユーザーセキュリティモデル表）が開きます。

図 **6-96.** 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のエントリの削除

□□□ **SNMPv3 User Security Model**（**USM**）（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。

User Security Model Table（ユーザーセキュリティモデル表）が開きます。

□□□ **User Security Model Table**（ユーザーセキュリティモデル表）のエントリを選択します。

□□□ **Remove**（削除）チェックボックスをクリックします。

□□□ **Apply Changes**（変更の適用）をクリックします。

User Security Model Table（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

次の表は、**SNMPv3 User Security Model**（**USM**）（SNMPv3 ユーザーセキュリティモード（USM））ページに表示されるフィールドを定義するための等価 CLI コマンドをまとめたものです。

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*]	新しい 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。

CLI コマンドの例は次のようになります。

```
console(config)# snmp-server user John user-group auth-md5 1234
console(config)# end
console# show snmp users
```

Name	Group Name	Auth Method	Remoteg
-------	----------	----------	------

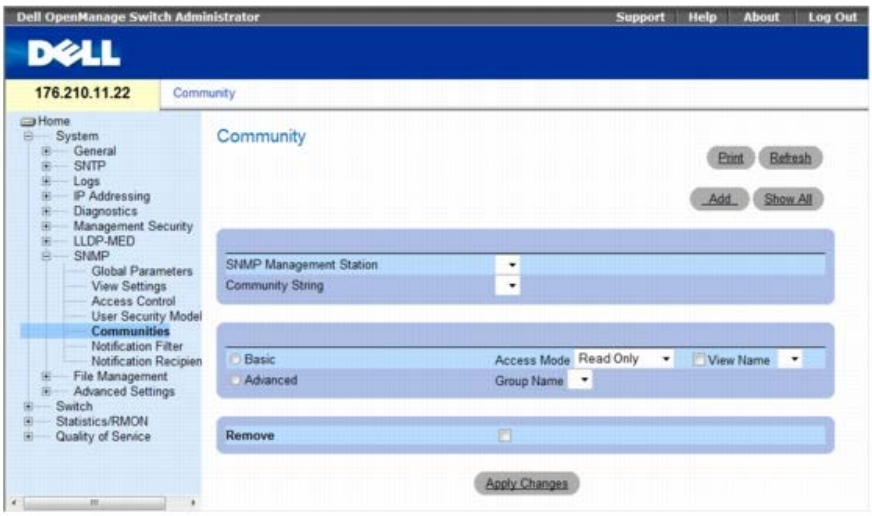
John	user-group	md5	

SNMP コミュニティの定義

SNMP Community（SNMP コミュニティ）ページでコミュニティを定義することによってアクセス権が管理されます。コミュニティの名前を変更するとアクセス権も変更されます。SNMP コミュニティは、SNMP v1 および SNMP v2 にのみ定義されます。

SNMP Community（SNMP コミュニティ）ページを開くには、ツリー表示で、**System**（システム）® **SNMP** ® **Communities**（コミュニティ）の順にクリックします。

図 **6-97. SNMP** コミュニティ



SNMP Community（**SNMP** コミュニティ）ページには、以下のフィールドがあります。

- **SNMP Management Station** — SNMP コミュニティが定義されている Management Station 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、Management Station 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）— 選択されたコミュニティの SNMP Basic（SNMP ベーシック）モードが有効になります。可能なフィールド値は次のとおりです。
  - **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次のとおりです。

    Read-Only（読み取り専用）— 管理アクセスは読み取り専用に制限され、コミュニティへの変更はできません。

    Read-Write（読み書き）— 管理アクセス権は読み書きで、デバイス設定の変更は可能ですが、コミュニティは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、コミュニティへの変更もできます。
  - **View Name**（表示名）— ユーザー定義の SNMP ビューのリストがあります。
- **Advanced**（詳細）— ユーザー定義のグループのリストがあります。SNMP Advanced（SNMP 詳細）モードを選択すると、選択したコミュニティに対して、グループを含む SNMP アクセス制御ルールが有効になります。また、Advanced（詳細）モードにより、特定の SNMP コミュニティの SNMP グループが有効になります。SNMP Advanced（SNMP 詳細）モードは SNMPv3 でのみ定義されます。可能なフィールド値は以下のとおりです。
  - **Group Name**（グループ名）— SNMP Advanced（SNMP 詳細）モードで動作するときのグループ名を指定します。

Remove（削除）— 指定したデバイスからコミュニティを削除します。

- **Checked**（チェックマークあり）— コミュニティを削除します。
- **Unchecked**（チェックマークなし）— 指定したデバイス内でコミュニティを保持します。

SNMP コミュニティを新しく定義する場合は、次のパラメーターを追加できます。

- **Supported IP Format**（サポートされている IP 形式）— コミュニティでサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— コミュニティで IPv6 がサポートされている場合（前述のパラメーターを参照）、これによりサポートされている静的アドレスのタイプを指定します。可能な値は以下のとおりです。
  - **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
  - **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。

- **Link Local Interface**（リンクローカルインタフェース）— サーバーで IPv6 リンクローカルアドレス（前述のパラメーターを参照）がサポートされている場合、リンクローカルインタフェースを指定します。可能な値は以下のとおりです。
  - **VLAN1** — IPv6 インタフェースは、VLAN1 で設定されています。
  - **ISATAP** — IPv6 インタフェースは、ISATAP トンネルで設定されています。

新しいコミュニティの定義

□□□ **SNMP Community**（SNMP 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。

Add SNMP Community（SNMP コミュニティの追加）ページが開きます。

図 **6-98. SNMP** コミュニティの追加

□□□ 関連フィールドすべてに入力します。

□□□ **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

□□□ **SNMP Community**（SNMP 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。

Community Table（コミュニティ表）ページが開きます。

図 **6-99.** コミュニティ表

□□□ コミュニティを選択して、**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。

コミュニティエントリが削除され、デバイスがアップデートされます。

CLI コマンドを使用したコミュニティの設定

次の表は、**SNMP Community**（SNMP コミュニティ）にあるフィールドを表示するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
snmp-server community *community* [**ro** | **rw** | **su**] [ipv4-address | ipv6-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* [ipv4-address | ipv6-address]	グループアクセス権に基づいて SNMP プロトコルへの限定アクセスを許可するコミュニティアクセスストリングを設定します。
show snmp	現在の SNMP デバイスの設定を表示します。

CLI コマンドの例は次のようになります。

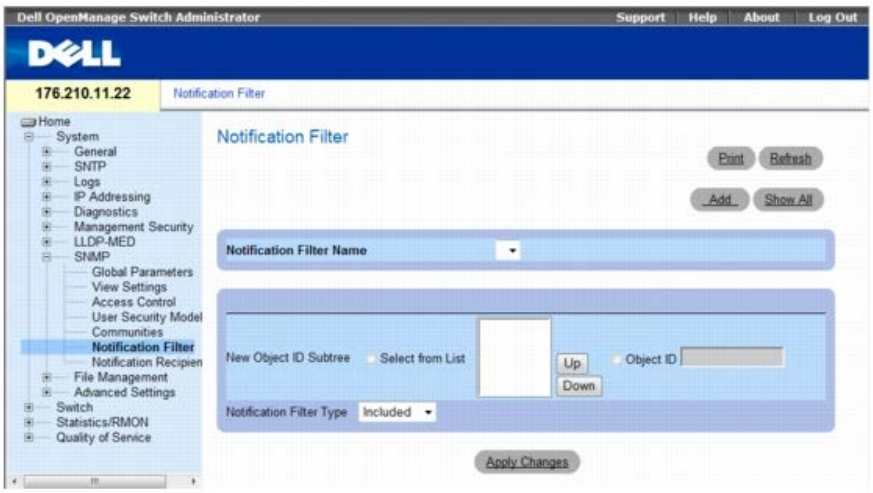
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

SNMP 通知フィルターの定義

Notification Filter（通知フィルタ）ページでは、OID に基づいてトラップをフィルタリングすることができます。各 OID は、デバイスの機能または機能の一部にリンクされています。**Notification Filter**（通知フィルタ）ページでは、ネットワーク管理者が通知をフィルタリングすることもできます。

Notification Filter（通知フィルター）ページを開くには、ツリー表示で、**System**（システム）® **SNMP** ® **Notification Filters**（通知フィルター）の順にクリックします。

図 **6-100.** 通知フィルター



Notification Filter（通知フィルター）ページには、以下のフィールドがあります。

- **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 ID Tree**（新規オブジェクト ID ツリー）— 通知が送信またはブロックされる OID です。フィルタが OID に関連付けられている場合は、トラップまたは通知が生成され、トラップの受信者に送信されます。オブジェクト ID は、**Select from List**（リストから選択）または **Object ID List**（オブジェクト ID リスト）のどちらかで選択します。
- **Notification Filter Type**（通知フィルターのタイプ）— OID に関する通知やトラップがトラップ受信者に送信され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が制限されます。
  - **Included**（含める） — Sends OID トラップまたは通知が送信されます。

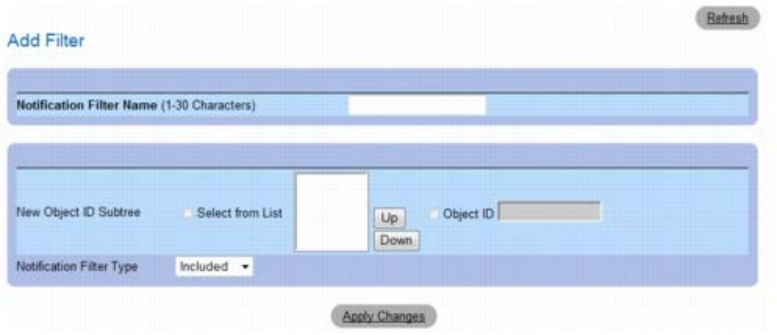
SNMP フィルタの追加

□□□ **Notification Filter**（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。

Add Filter（フィルタの追加）ページが開きます。

図 **6-101.** フィルタの追加



□□□ 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

□□□ **Notification Filter**（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。

Filter Table（フィルタ表）が開きます。

図 **6-102.** フィルタ表

フィルタの削除

□□□ **Notification Filter**（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。

Filter Table（フィルタ表）が開きます。

□□□ **Filter Table**（フィルタ表）のエントリを選択します。

□□□ **Remove**（削除）チェックボックスをクリックします。

フィルタ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通知フィルタの設定

次の表は、**Notification Filter**（通知フィルター）ページに表示されるフィールドを定義するための等価 CLI コマンドをまとめたものです。

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アップデートします。
show snmp filters [filtername]	SNMP 通知フィルターの設定を表示します。

CLI コマンドの例は次のとおりです。

```
Console(config)# snmp-server filter user1 iso included
Console(config)# end
Console # show snmp filters

Name                            OID Tree                        Type
```

| ---------- | ---------- | ---------- |
| user1 | iso | included |

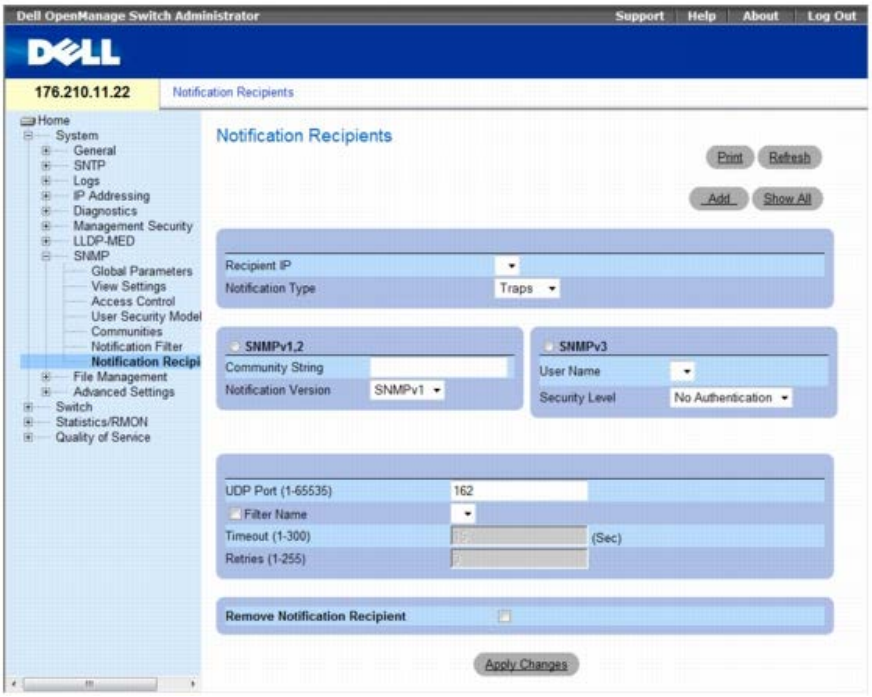
SNMP 通知受信者の定義

Notification Recipients（通知受信者）ページには、トラップが特定のユーザーに送信されるかどうか、および送信されるトラップのタイプを決めるフィルタを定義するための情報があります。_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識別
- トラップのフィルタリング
- トラップ生成パラメーターの選択
- アクセス制御チェックの提供

Notification Recipients（通知受信者）ページを開くには、ツリー表示で、**System**（システム）® **SNMP** ® **Notification Recipient**（通知受信者）の順にクリックします。

図 **6-103.** 通知受信者



Notification Recipients（通知受信者）ページには、以下のフィールドがあります。

- **Recipient IP**（受信者 IP） — トラップの送信先の 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次のとおりです。
  - **Trap**（トラップ）— トラップが送信されます。
  - **Inform**（案内）— 案内が送信されます。

SNMPv1,2

選択された受信者に対して、SNMP バージョン 1 および 2 が有効になります。SNMPv1 および SNMPv2 用に以下のフィールドを定義します。

- **Community String**（**1-20 Characters**）（コミュニティ文字列（1～20 文字））— トラップ管理者のコミュニティ文字列を識別します。
- **Notification Version**（通知バージョン） — トラップのタイプを決定します。可能なフィールド値は次のとおりです。
  - **SNMP V1** — SNMP バージョン 1 トラップが送信されます。
  - **SNMP V2** — SNMP バージョン 2 トラップが送信されます。

SNMPv3

トラップの送信および受信に SNMPv3 が使用されます。SNMPv3 用に以下のフィールドを定義します。

- **User Name**（ユーザー名） — SNMP 通知の送信先ユーザーです。
- **Security Level**（セキュリティレベル）— パケットが認証される手段を定義します。可能なフィールド値は次のとおりです。
  - **No Authentication**（認証なし） — 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（1～65535））— 通知の送信に使用される UDP ポートです。デフォルトは 162 です。
- **Filter Name**（フィルタ名） — SNMP フィルタを含めるか、除外します。
  - **Checked**（チェックマークあり）— SNMP フィルターを含めます。
  - **Unchecked**（チェックマークなし）— SNMP フィルターを除外します。
- **Timeout**（**1-300**）（タイムアウト（1～300））— 通知を再送信する前にデバイスが待つ時間（秒）です。デフォルト値は 15 秒です。
- **Retries**（**1-255**）（再試行（1～255））— 通知要求をデバイスが再送信する最大回数です。
  デフォルトは 3 です。
- **Remove Notification Recipient**（通知受信者の削除）— 選択された通知受信者が削除されます。
  - **Checked**（チェックマークあり）— 特定の通知受信者を削除します。
  - **Unchecked**（チェックマークなし）— 通知受信者を保持します。

通知受信者を追加する場合は、次のパラメーターを追加できます。

- **Supported IP Format**（サポートされている IP 形式）— 受信者でサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— 受信者で IPv6 がサポートされている場合（前述のパラメーターを参照）、これによりサポートされている静的アドレスのタイプを指定します。可能な値は以下のとおりです。
  - **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
  - **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。
- **Link Local Interface**（リンクローカルインタフェース）— サーバーで IPv6 リンクローカルアドレス（前述のパラメーターを参照）がサポートされている場合、リンクローカルインタフェースを指定します。可能な値は以下のとおりです。
  - **VLAN1** — IPv6 インタフェースは、VLAN1 で設定されています。
  - **ISATAP** — IPv6 インタフェースは、ISATAP トンネルで設定されています。

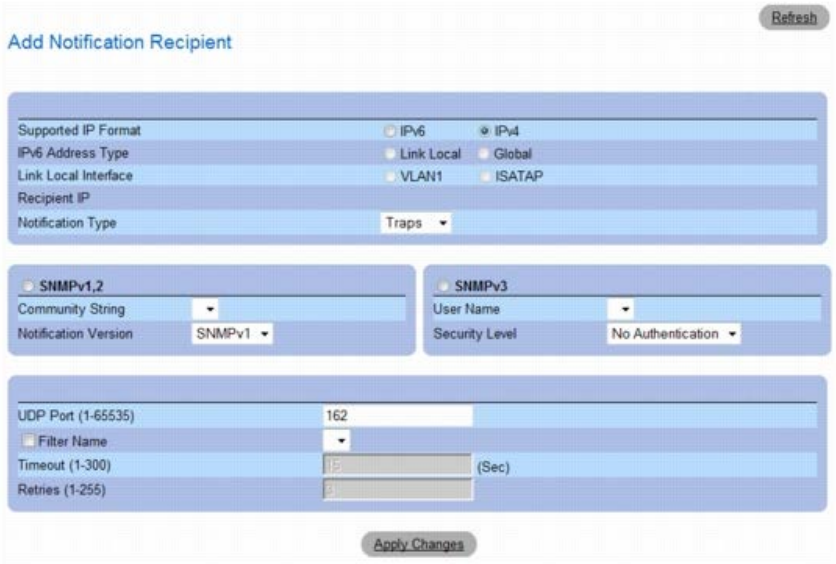
新しいトラップ受信者の追加

□□□ Notification Recipients（通知受信者）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add Notification Recipients（通知受信者の追加）ページが開きます。

図 **6-104.** 通知受信者の追加



□□□ 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。

通知受信者が追加され、デバイスがアップデートされます。

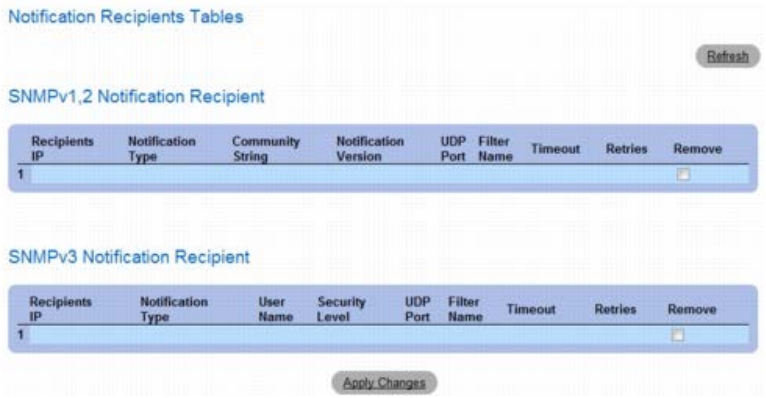
通知受信者表の表示

□□□ **Notification Recipients**（通知受信者）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Notification Recipients Tables（通知受信者表）ページが開きます。

図 **6-105.** 通知受信者表



通知受信者の削除

□□□ **Notification Recipients**（通知受信者）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Notification Recipients Tables（通知受信者表）ページが開きます。

□□□ **SNMPV1,2 Notification Recipient**（SNMPV1 および 2 通知受信者）または **SNMPv3 Notification Recipient Tables**（SNMPV3 通知受信者表）のどちらかで通知受信者を選択します。

□□□ **Remove**（削除）チェックボックスをクリックします。

□□□ **Apply Changes**（変更の適用）をクリックします。

受信者が削除され、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** 通知受信者の設定

次の表は、**Notification Recipients**（通知受信者）ページにあるフィールドを表示するための等価 CLI コマンドをまとめたものです。

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 の通知を受け取る通知受信者を作成またはアップデートします。
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 の通知を受け取る通知受信者を作成またはアップデートします。
show snmp	現在の SNMP 設定を表示します。

CLI コマンドの例は次のようになります。

```
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

File Management（ファイルの管理）ページを使用すると、デバイスソフトウェア、イメージファイル、設定ファイルを管理できます。ファイルは、TFTP サーバーを介してダウンロードまたはアップロードできます。管理ファイルは、次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を含みます。スタートアップ設定ファイルは、実行設定ファイルまたはイメージファイルから設定コマンドをコピーすることにより作成されます。
- **Running Configuration File**（実行設定ファイル） — すべての起動設定ファイルコマンド、および現行セッション中に入力されたすべてのコマンドが含まれます。デバイスがパワーダウンまたは再起動された後、実行設定ファイルに保存されているすべてのコマンドは失われます。スタートアップ処理中、スタートアップ設定ファイルにあるすべてのコマンドは実行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、すべての新しいコマンドは、実行設定ファイルの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アップデートするには、デバイスをパワーダウンする前に実行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。
- **Image Files**（イメージファイル）— システムのファイルイメージは、Image 1 および Image 2 という 2 つのフラッシュファイルに保存されます。アクティブなイメージはアクティブなコピーを格納し、他方のイメージは二次コピーを格納します。 デバイスは、アクティブなイメージから起動し実行します。 アクティブなイメージが破壊した場合は、システムは自動的に非アクティブなイメージから起動します。これはソフトウェアアップデート処理中に起こる不具合に対する安全機能です。

File Management（ファイルの管理）ページを開くには、ツリー表示の **System**（システム）® **File Management**（ファイルの管理）をクリックします。

本項には、次のトピックがあります。

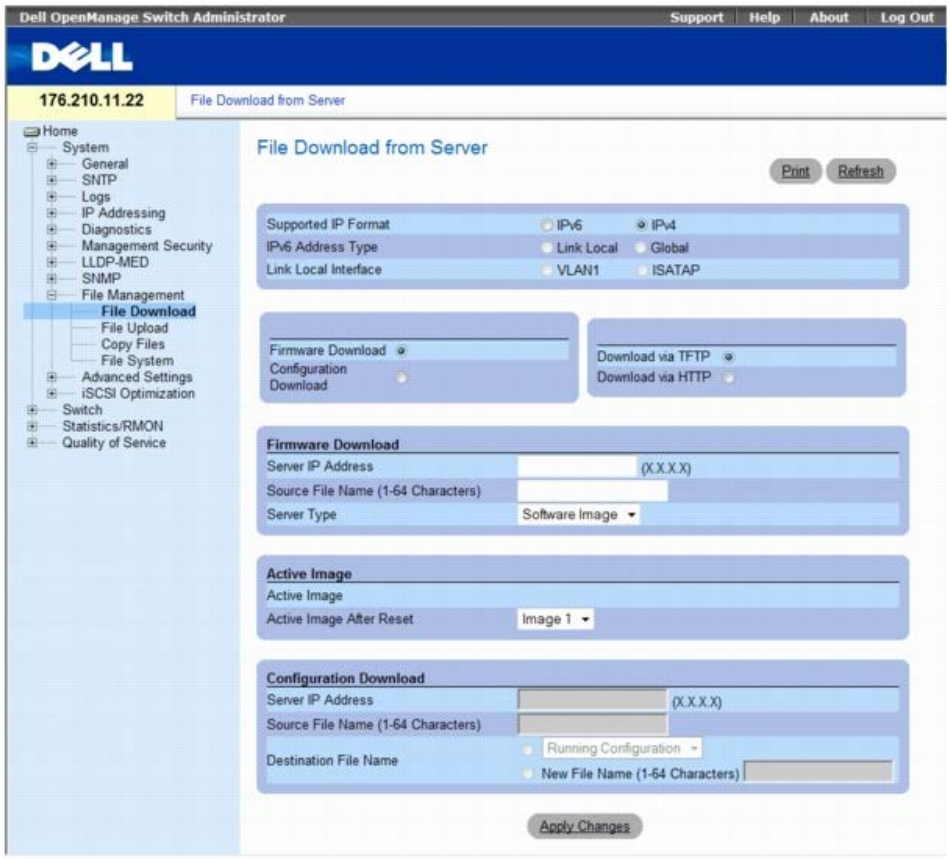
- ファイルのダウンロード
- ファイルのアップロード
- イメージファイルのアクティブ化
- ファイルのコピー
- デバイスファイルの管理

ファイルのダウンロード

File Download from Server（サーバーからのファイルのダウンロード）ページには、TFTP サーバーまたは HTTP クライアントからデバイスへ、システムイメージおよび設定ファイルをダウンロードするためのフィールドがあります。

File Download from Server（サーバーからのファイルのダウンロード）ページを開くには、ツリー表示で、**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）の順にクリックします。

図 **6-106.** サーバーからのファイルのダウンロード



File Download from Server（サーバーからのファイルのダウンロード）ページには、以下のフィールドがあります。

- **Supported IP Format**（サポートされている IP 形式）— サーバーでサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— サーバーで IPv6（前述のパラメーターを参照）がサポートされている場合、サポートされている静的アドレスのタイプを指定します。可能な値は以下のとおりです。
  - **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
  - **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。
- **Link Local Interface**（リンクローカルインタフェース）— サーバーで IPv6 リンクローカルアドレス（前述のパラメーターを参照）がサポートされている場合、リンクローカルインタフェースを指定します。可能な値は以下のとおりです。
  - **VLAN1** — IPv6 インタフェースは、VLAN1 で設定されています。
  - **ISATAP** — IPv6 インタフェースは、ISATAP トンネルで設定されています。
- **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がダウンロードされます。**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） フィールドはグレーになります。
- **Configuration Download**（設定のダウンロード）— 設定ファイルがダウンロードされます。**Configuration Download**（設定のダウンロード）が選択された場合、**Firmware Download**（ファームウェアのダウンロード）フィールドはグレーになります。
- **Download via TFTP**（TFTP 経由のダウンロード）— TFTP サーバー経由でのイメージのアップロード開始を有効にします。
- **Download via HTTP**（HTTP 経由のダウンロード） — HTTP サーバー経由でのイメージのアップロード開始を有効にします。

Firmware Download（ファームウェアのダウンロード）

- **Server IP Address**（サーバーの IP アドレス）— ファームウェアファイルがダウンロードされるサーバーの IP アドレスです。
- **Source File Name**（**1-64 characters**）（ソースファイル名（1～64 文字））— ダウンロードされるファイルを示します。
- **Destination File Name**（宛先ファイル名）— 設定ファイルのダウンロード先となるファイルのタイプです。可能なフィールド値は次のとおりです。
  - **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。イメージファイルは、アクティブでないイメージを上書きします。アクティブでないイメージがリセット後にアクティブイメージになるように指定してから、ダウンロードに続いてデバイスをリセットすることをお勧めします。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ボックスが開きます。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。

- **Boot Code**（起動コード）— 起動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）

- **Server IP Address**（サーバーの IP アドレス）— 設定ファイルがダウンロードされる TFTP サーバーの IP アドレスです。
- **Source File Name**（**1-64 characters**）（ソースファイル名（1～64 文字））— ダウンロードされる設定ファイルを示します。
- **Destination File**（宛先ファイル）— 設定ファイルのダウンロード先となるファイルです。可能なフィールド値は次のとおりです。
  - **Running Configuration**（実行設定）— 実行設定ファイルへのコマンドをダウンロードします。
  - **Startup Configuration**（起動設定）— 起動設定ファイルをダウンロードし、それに上書きします。
  - **<filename>**（ファイル名）— 設定バックアップファイルにコマンドをダウンロードします。ファイル名は、ダウンロード時にユーザーが指定します。

ファイルのダウンロード

□□□ **File Download from Server**（サーバーからのファイルのダウンロード）ページを開きます。

□□□ ダウンロードするファイルの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へダウンロードされます。選択され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の詳細については、「スタック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

次の表は、**File Download From Server**（サーバーからのファイルのダウンロード）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
copy source-url destination-url	ソースから宛先にファイルをコピーします。

CLI コマンドの例は次のようになります。

```
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
```

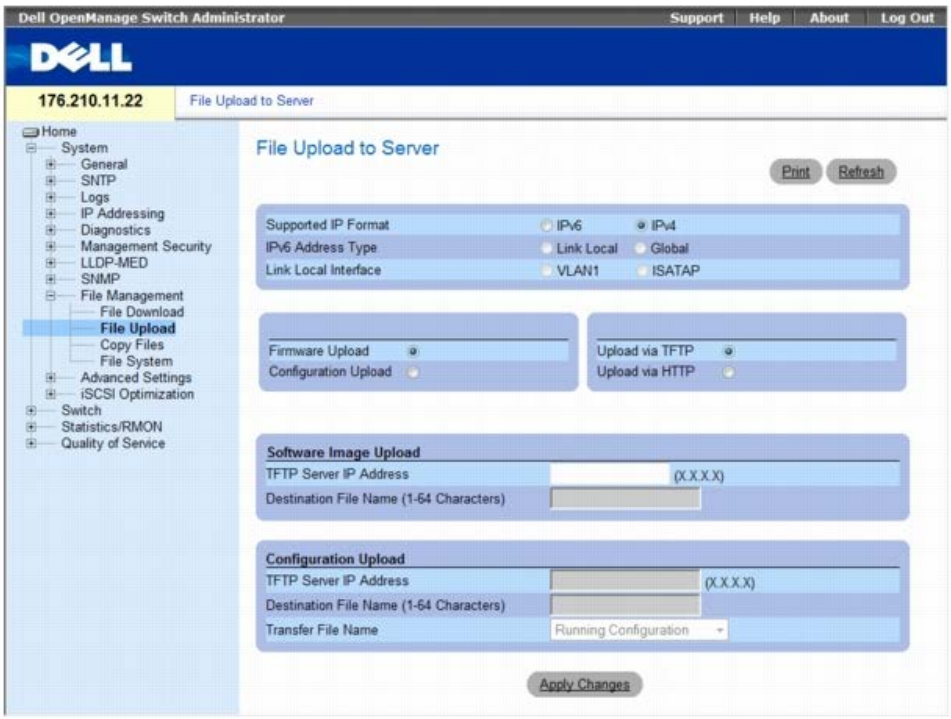
メモ： 感嘆符（!）は、それぞれ、10 のパケットが正常に転送されたことを示します。

ファイルのアップロード

File Upload to Server（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ためのフィールドがあります。また、イメージファイルも **File Upload to Server**（サーバーへのファイルのアップロード）ページからアップロードすることができます。

File Upload to Server（サーバーへのファイルアップロード）ページを開くには、ツリー表示の **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 **6-107.** サーバーへのファイルのアップロード



File Upload to Server（サーバーへのファイルアップロード）ページには、以下のフィールドがあります。

- **Supported IP Format**（サポートされている IP 形式）— サーバーでサポートされている IP 形式を指定します。可能な値は以下のとおりです。
  - **IPv6** — IP バージョン 6 がサポートされています。
  - **IPv4** — IP バージョン 4 がサポートされています。
- **IPv6 Address Type**（IPv6 アドレスタイプ）— サーバーで IPv6（前述のパラメーターを参照）がサポートされている場合、サポートされている静的アドレスのタイプを指定します。可能な値は以下のとおりです。
  - **Link Local**（リンクローカル）— ルーティング不能であり、同じネットワーク上の通信のみに使用するリンクローカルアドレスです。
  - **Global**（グローバル）— 異なるサブネットから検出および到達可能で、グローバルに一意な IPv6 アドレスです。
- **Link Local Interface**（リンクローカルインタフェース）— サーバーで IPv6 リンクローカルアドレス（前述のパラメーターを参照）がサポートされている場合、リンクローカルインタフェースを指定します。可能な値は以下のとおりです。
  - **VLAN1** — IPv6 インタフェースは、VLAN1 で設定されています。
  - **ISATAP** — IPv6 インタフェースは、ISATAP トンネルで設定されています。
- **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）が選択されている場合、**Configuration Upload**（設定のアップロード）フィールドは利用できなくなります。
- **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）が選択されている場合、**Software Image Upload**（ソフトウェアイメージのアップロード）フィールドは利用できなくなります。
- **Upload via TFTP**（TFTP 経由のアップロード） — TFTP サーバー経由でのイメージのアップロード開始が有効になります。
- **Upload via HTTP**（HTTP 経由のアップロード） — FTP サーバー経由でのイメージのアップロード開始が有効になります。

ソフトウェア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宛先の TFTP サーバーの IP アドレスです。
- **Destination File Name**（**1-64 Characters**）（宛先ファイル名（1～64 文字））— ファイルがアップロードされる宛先のソフトウェアイメージファイルのパスが示されます。

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宛先の TFTP サーバーの IP アドレスです。
- **Destination File Name**（**1-64 Characters**）（宛先ファイル名（1～64 文字））— ファイルがアップロードされる宛先の設定ファイルのパスが示されます。
- **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次のとおりです。

  - **Running Configuration**（実行設定）— 実行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。
  - **My Backup Configuration**（マイバックアップ設定）— バックアップ設定ファイルをアップロードします。このユーザー定義の設定ファイルのリストは、ユーザーがバックアップ設定ファイルを作成した場合にのみ表示されます。たとえば、ユーザーが実行設定ファイルを BACKUP-SITE-1 というユーザー定義の設定ファイルにコピーした場合は、このリストが File Upload to Server（サーバーへのファイルのアップロード）ページに表示され、設定ファイル BACKUP-SITE-1 がリストに表示されます。

ファイルのアップロード

□□□ **File Upload to Server**（サーバーへのファイルのアップロード）ページを開きます。

□□□ アップロードするファイルの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。

TFTP サーバーにソフトウェアがアップロードされます。

CLI コマンドを使用したファイルのアップロード

次の表は、 **File Upload to Server**（サーバーへのファイルのアップロード） ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
copy source-url destination-url	ソースから宛先にファイルをコピーします。

CLI コマンドの例は次のようになります。

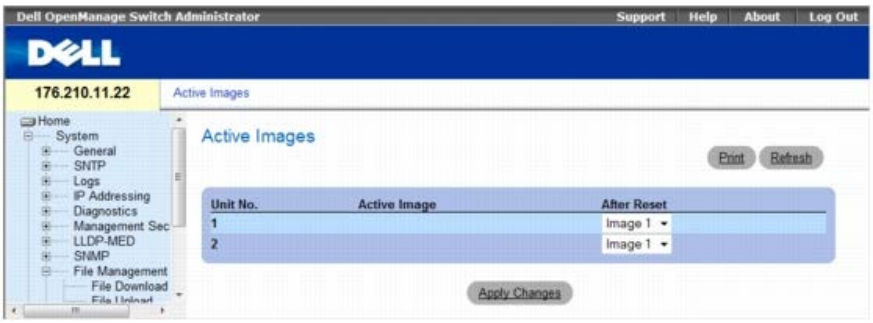
```
console# copy image tftp://10.6.6.64/uploaded.ros
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
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

Active Images（アクティブイメージ）ページを使用すると、ネットワーク管理者は、イメージファイルを選択およびリセットできます。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、別々に選択できます。

Active Images（アクティブイメージ）ページを開くには、ツリー表示で、**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）の順にクリックします。

図 **6-108.** アクティブイメージ



Unit No.	Active Image	After Reset
1		Image 1
2		Image 1

Active Images（アクティブイメージ）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）— 選択されるイメージファイルのユニット番号です。
- **Active Image** —

（アクティブイメージ）　ユニット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）— デバイスがリセットされた後にユニットでアクティブになるイメージファイルです。可能なフィールド値は次のとおりです。
  - **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

□□□ **Active Images**（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択します。

□□□ **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

次の表は、**Active Images**（アクティブイメージ）にあるフィールドを表示するための等価 CLI コマンドをまとめたものです。

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。

CLI コマンドの例は次のようになります。

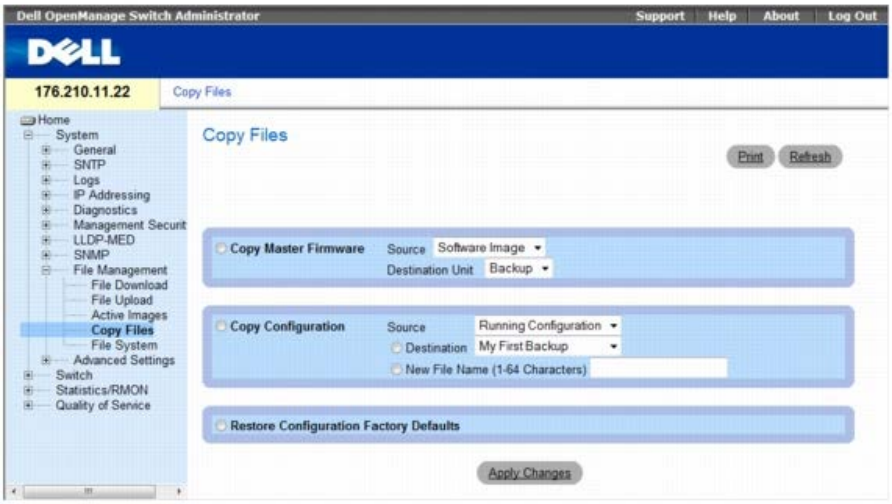
```
Console# boot system image-1
```

ファイルのコピー

ファイルは**Copy Files**（ファイルのコピー）ページからコピーおよび削除することができます。

Copy Files（ファイルのコピー）ページを開くには、ツリー表示の **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 **6-109.** ファイルのコピー



Copy Files（ファイルのコピー）ページには、以下のフィールドがあります。

- **Copy Master Firmware**（マスターファームウェアのコピー）— コピーするファームウェアファイルを示します。可能なフィールド値は次のとおりです。
  - **Source**（ソース）— 現在のスタッキングマスターのソフトウェアイメージファイルまたはブートコードファイルをコピーします。
  - **Destination Unit**（宛先ユニット）— ファイルのアップロード先となるスタッキングメンバーを指定します。
- **Copy Configuration**（設定）— 選択されている場合、マスターファイルの実効設定ファイル、スタートアップファイル、バックアップ設定ファイルのいずれかを宛先ファイルにコピーします。

- **Source**（ソース） — 宛先ファイルにコピーされるファイルのタイプを示します。**Running Configuration**（実行設定）または **Startup Configuration**（スタートアップ設定）のいずれかを選択します。
- **Destination**（宛先） — ソースファイルがコピーされる宛先の設定ファイルを示します。**My First Backup**（最初のマイバックアップ）または **Startup Configuration**（スタートアップ設定）を選択します。
- **New File Name**（**1-64 characters**）（新規ファイル名（1～64 文字））— 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**（設定を工場出荷時のデフォルトに戻す）— 選択されている場合、現在の構成設定が工場出荷時のデフォルト設定に置き換えられることを示します。選択されていない場合、現在の構成設定が保持されることを示します。

ファイルのコピー

□□□ **Copy Files**（ファイルのコピー）ページを開きます。

□□□ **Source**（ソース）および **Destination**（宛先）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。

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の復元

□□□ **Copy Files**（ファイルのコピー）ページを開きます。

□□□ **Restore Configuration Factory Defaults**（設定を工場出荷時のデフォルトに戻す）をクリックします。

□□□ **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および削除

以下の表は、**Copy Files**（ファイルのコピー）ページに表示されるフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
copy *source-url destination-url*	ソースから宛先にファイルをコピーします。
delete startup-config	スタートアップ構成ファイルを削除します。
delete *url*	フラッシュメモリデバイスからファイルを削除します。

CLI コマンドの例は次のようになります。

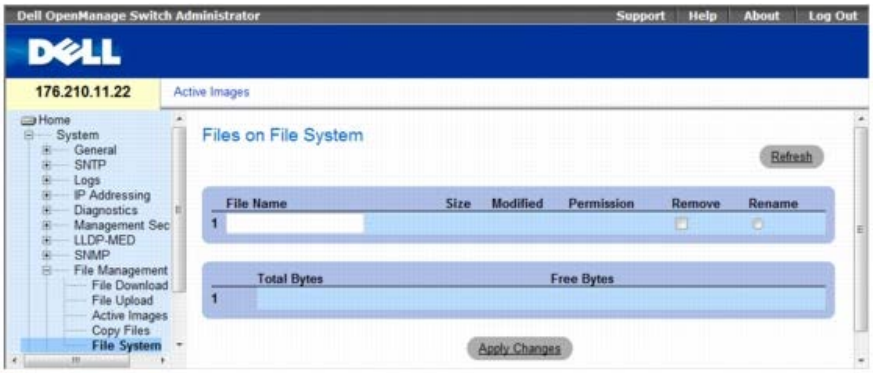
```
console# delete startup-config
Startup file was deleted
console#
console# copy running-config startup-config
01-Jan-2000 06:55:32 %COPY-W-TRAP: The copy operation was completed
successfully
Copy succeeded
console#
```

デバイスファイルの管理

Files on File System（ファイルシステム上のファイル）ページには、ファイル名、ファイルサイズ、ファイルの変更、ファイルのアクセス権など、システム上に現在保存されているファイルに関する情報が表示されます。ファイルシステムでは、最大 5 ファイル、1 ファイルあたり 0.5 MB までのサイズを管理できます。

Files on File System（ファイルシステム上のファイル）ページを開くには、ツリー表示の **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 **6-110.** ファイルシステム上のファイル



Files on File System（ファイルシステム上のファイル）ページには以下のフィールドがあります。

- **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を示します。
- **Size**（サイズ）— ファイルサイズを示します。
- **Modified**（変更）— ファイルの最終変更日を示します。
- **Permission**（アクセス権）— ファイルに割り当てられたアクセス権のタイプを示します。可能なフィールド値は次のとおりです。
  - **Read Only**（読み取り専用）— 読み取り専用ファイルを示します。
  - **Read Write**（読み書き）— 読み書きファイルを示します。
- **Remove**（削除）— ファイルを削除します。
  - **Checked**（チェックマークあり）— 指定されたファイルをファイル管理システムから削除します。
  - **Unchecked**（チェックマークなし）— 指定されたファイルをファイル管理システムに保持します。
- **Rename**（名前の変更）— ファイルの名前を変更できます。ファイル名は **File Name**（ファイル名）フィールドで変更されます。
- **Total Bytes**（合計バイト数）— 現在使用されている合計スペースを示します。
- **Free Bytes**（空きバイト数）— 現在の空きスペースの残り容量を示します。

CLI コマンドを使用したファイルの管理

下の表は、システムのファイルを管理するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
dir	フラッシュファイルシステム上のファイルのリストを表示します。

CLI コマンドの例は次のようになります。

```
console# dir
Directory of flash:

File Name       Permis-sion  Flash Size  Data Size  Modified
--------------  ------       ------      ------     --------------------
3.txt           rw           524288      523776     22-Feb-2005 18:49:27
setup           rw           524288      95         22-Feb-2005 15:58:19
setup2          rw           524288      95         22-Feb-2005 15:58:35
image-1         rw           4325376     4325376    06-Feb-2005 17:55:32
image-2         rw           4325376     4325376    06-Feb-2005 17:55:31
test.txt        rw           524288      95         22-Feb-2005 12:16:44
aaafile.prv     --           131072      --         06-Feb-2005 19:09:02
syslog1.sys     r-           262144      --         22-Feb-2005 18:49:27
syslog2.sys     r-           262144      --         22-Feb-2005 18:49:27
directory.prv   --           262144      --         06-Feb-2005 17:55:31
startup-config  rw           524288      347        22-Feb-2005 11:56:03

Total size of flash: 16646144 bytes
Free size of flash: 4456448 bytes
```

詳細設定

Advanced Settings（詳細設定）を使用すると、スイッチのその他のグローバル属性を設定できます。これらの属性変更は、スイッチのリセット後に適用されます。

次のリンクをクリックすると、指定されている画面のオンラインヘルプにアクセスできます。

ツリー表示で、**System**（システム）® **Advanced Settings**（詳細設定）をクリックして、**Advanced Settings**（詳細設定）ページを開きます。

Advanced Settings（詳細設定）ページには、一般的な設定のためのリンクがあります。

本項には、次のトピックがあります。

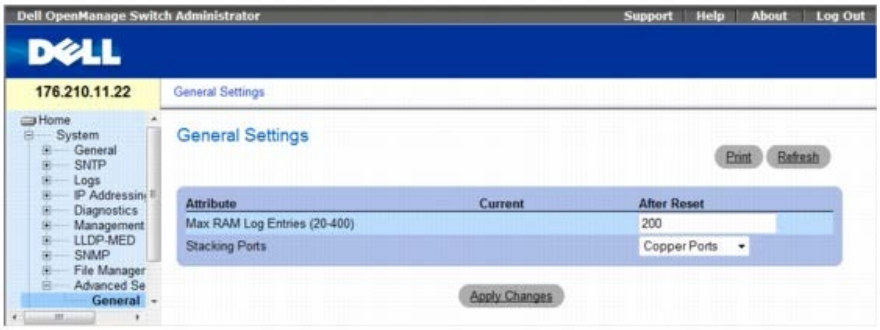
- 一般的な設定

一般的な設定

General Settings（一般的な設定）ページでは、一般的なデバイスパラメーターを定義するための情報を提供します。

General Settings（一般的な設定）ページを開くには、ツリー表示で、**System**（システム）® **Advanced Settings**（詳細設定）® **General Settings**（一般的な設定）の順にクリックします。

図 **6-111.** 一般的な設定



General Settings（一般的な設定）ページには、以下の情報が含まれています。

- **Attribute**（属性）— 一般的な設定属性です。
- **Current**（現在）— 現在設定されている値です。
- **After Reset**（リセット後）— 将来（リセット後）の値です。リセット後の行に値を入力することによって、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（20～400）— 最大数の RAM ログエントリです。ログエントリが一杯になると、ログがクリアされ、ログファイルが再スタートします。
- **Stacking Ports**（スタッキングポート）— スタッキングポートのタイプです。銅線ポートまたはファイバーポートです。

CLI コマンドを使用した RAM ログエントリカウンタの表示

以下の表は、 **General Settings**（一般設定）ページに表示されているフィールドを設定するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
logging buffered size *number*	内蔵バッファ（RAM）に保存される syslog メッセージの数を設定します。

CLI コマンドの例は次のようになります。

```
console(config)# logging buffered size 300
```

目次に戻る

目次に戻る

スイッチ情報の設定

Dell™ PowerConnect™ 35xx システムユーザーズガイド

本項には、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、ポートの集約、およびマルチキャストサポートの設定に関するすべてのシステム動作および一般情報が記載されています。

ネットワークセキュリティの設定

Network Security（ネットワークセキュリティ）ページを使用すると、アクセス制御リストとロックポートの両方を使用して、ネットワークセキュリティを設定できます。**Network Security**（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。

本項には、次のトピックがあります。

- ポートベース認証
- 拡張ポートベース認証の設定
- ユーザーの認証
- ポートセキュリティの設定

ポートベース認証

ポートベースによる認証では、外付けのサーバーを介してポートごとにシステムユーザーを認証できます。認証および承認されたシステムユーザーだけが、データを送受信できます。ポートの認証は、Extensible Authentication Protocol（EAP）を使って RADIUS サーバー経由で行われます。ポートの認証には、次の項目があります。

- **Authenticators**（オーセンティケータ）— 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）— 認証されたポートに接続し、システムサービスへのアクセスを要求するホストを指定します。
- **Authentication Server**（認証サーバー）— オーセンティケータの代わりに認証を行い、そのサプリカントがシステムサービスへのアクセス権があるかどうかを示す、RADIUS サーバーなどの外付けサーバーを指定します。

ポートベース認証によって、次の 2 つのアクセス状態が生じます。

- **Controlled Access**（制御アクセス）— サプリカントに権限がある場合に、サプリカントとシステムとの通信を許可します。
- **Uncontrolled Access**（非制御アクセス）— ポート状態に関係なく、制御なしで通信を許可します。

デバイスでは現在、RADIUS サーバーを介したポートベース認証をサポートしています。

MAC ベース認証

MAC ベース認証は 802.1x 認証の代わりに使用されます。この認証によって、プリンタ、IP 電話など 802.1X サプリカント機能を持たないデバイスへのネットワークアクセスが可能になります。MAC 認証は、接続デバイスの MAC アドレスを使用してネットワークアクセスを許可したり、拒否したりします。

拡張ポートベース認証

拡張ポートベース認証

- 複数のホストを単一のポートに接続できるようにします。
- 1 つのホストを許可するだけで、すべてのホストにシステムへのアクセス権を付与することができます。ポートが認証されていない場合、接続されたホストのすべて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 に接続している特定のポートに権限がない場合でも、デバイスでは特定の VLAN が常に使用可能になります。
    - たとえば、Voice over IP（VoIP）には認証は必要ありませんが、データトラフィックには認証が必要です。認証が必要でない VLAN を定義することができます。VLAN に接続しているポートが、認可されたと定義されている場合でも、ユーザーは認可なし VLAN を使用することができます。

拡張ポートベース認証は、次のモードで実行します。

- **Single Host Mode**（単一ホストモード）— 単一セッションでのポートへのアクセスで、権限のあるホストのみを有効にします。
- **Multiple Host Mode**（複数ホストモード）— 単一セッションでのアクセスで、複数のホストを単一ポートに接続できるようにします。1 つのホストを許可するだけですべてのホストがネットワークへアクセスすることができます。ホストの認証に失敗したり、EAPOL-logoff メッセージを受け取った場合には、すべての接続クライアントがネットワークへのアクセスを拒否されます。
- **Multiple Session Mode**（複数セッションモード）— 複数セッションでのポートへのアクセスで、権限のあるホストだけを有効にします。
- **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。ポートがポートベース認証でネットワークアクセスを拒否された場合でも、ゲスト VLAN が有効であれば、そのポートは制限付きのネットワークアクセス権を得ることができます。たとえば、ネットワーク管理者はゲスト VLAN を使用して、ポートベース認証によりネットワークアクセスを拒否しながら、権限のないユーザーにインターネットアクセス権を付与できます。

Port Based Authentication（ポートベース認証）ページを使用することで、ネットワーク管理者は、ポートベース認証を設定できます。

Port Based Authentication（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

Port Based Authentication（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）— デバイスに対してポートベース認証を許可します。可能なフィールド値は次のとおりです。

- **Enable**（有効）— デバイスに対してポートベース認証を有効にします。
- **Disable**（無効）— デバイスに対してポートベース認証を無効にします。

- **Authentication Method**（認証方法）— 使用される認証方法を示します。可能なフィールド値は次のとおりです。
  - **None**（なし）— ポートの認証に使用される認証方法はありません。
  - **RADIUS** — ポート認証が RADIUS サーバーによって実行されることを示します。
  - **RADIUS, None**（RADIUS、なし）— ポート認証が最初に RADIUS サーバーによって実行されることを示します。ポートが認証されない場合は、いずれの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）— デバイスでゲスト VLAN を有効にするかどうかを指定します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— 権限のないポートに対するゲスト VLAN の使用を有効にします。ゲスト VLAN を有効にすると、権限のないポートは自動的に、VLAN List（VLAN リスト）フィールドで選択された VLAN に接続します。
  - **Disable**（無効）— 権限のないポートに対するゲスト VLAN の使用を無効にします。これがデフォルト設定になっています。
- **VLAN List**（VLAN リスト）— VLAN のリストを示します。VLAN は、VLAN リストから選択されます。

インタフェースパラメーター

- **Interface**（インタフェース）— 有効にされているポートベース認証のインタフェースリストを示します。
- **User Name**（ユーザー名）— サプリカントのユーザー名です。
- **Admin Interface Control**（管理インタフェース制御）— ポートの認証状態を定義します。可能なフィールド値は次のとおりです。
  - **Auto**（自動） — デバイスのポートベース認証を有効にします。インタフェースの状態は、デバイスとクライアント間の認証交換に基づいて、許可または無許可のいずれかに変わります。
  - **Authorized**（許可）— インタフェースを認証なしで許可状態にします。この場合、インタフェースは、クライアントのポートベース認証を行うことなく通常のトラフィックを送受信します。
  - **Unauthorized**（無許可）— インタフェースを無許可状態に変更することによって、選択したインタフェースのシステムアクセスを拒否します。デバイスは、インタフェースを通してクライアントに認証サービスを提供することはできません。
- **Current Interface Control**（現在のインタフェース制御）— 現在のポートの認証状態です。
- **Authentication Type**（認証タイプ） — ポートの認証タイプを指定します。可能なフィールド値は次のとおりです。
  - **802.1x Only**（802.1x のみ）— 認証タイプを 802.1x ベース認証のみに設定します。
  - **MAC Only**（MAC のみ）— 認証タイプを MAC ベース認証のみに設定します。
  - **802.1x & MAC**（802.1x および MAC）— 認証タイプを 802.1x ベース認証および MAC ベース認証に設定します。
- **Dynamic VLAN Assignment**（動的 VLAN 割り当て）— ポートに対して動的 VLAN 割り当てが有効かどうかを示します。この機能を使用すると、ネットワーク管理者は、RADIUS サーバーの認証中にユーザーを自動的に VLAN に割り当てることができます。RADIUS サーバーでユーザーが認証されると、このユーザーは、RADIUS サーバーで設定されている VLAN に自動的に参加します。
  - DVA が有効の場合、ポートロックおよびポートモニタは無効です。
  - 動的 VLAN 割り当て（DVA）は、RADIUS サーバーが設定済みであり、ポート認証が有効で、802.1x multi-session mode（複数セッションモード）に設定されている場合のみ行われます。
  - Radius Accept Message にサプリカントの VLAN が含まれていない場合、そのサプリカントは拒否されます。
  - 認証されたポートは、タグ無しとしてサプリカント VLAN に追加されます。
  - 認証されたポートは、認証されていない VLAN およびゲスト VLAN メンバーのままになります。このポートには、静的 VLAN 設定は適用されません。
  - 認証されていない VLAN、GVRP で作成された動的 VLAN、音声 VLAN、デフォルトの VLAN、およびゲスト VLAN は DVA に参加できません。
  - ネットワーク管理者は、サプリカントがログイン状態の間にサプリカントの VLAN を削除できます。このサプリカントの VLAN が再作成されたり、RADIUS サーバーで新しい VLAN が設定された場合、このサプリカントは、次回再認証時に権限が付与されます。
- **Guest VLAN**（ゲスト VLAN）— 有効な場合、許可のないユーザーが、このインタフェースに接続した場合、ゲスト VLAN にアクセスできます。
  - **Enable**（有効）— 権限のないユーザーが、ゲスト VLAN にアクセスできるようにします。
  - **Disable**（無効）— 権限のないユーザーがゲスト VLAN にアクセスできないようにします。

- **Periodic Reauthentication**（断続的な再認証）— 選択したポートを断続的に再認証します。再認証の時期は、**Reauthentication Period**（**300**～**4294967295**）（再認証の時期（300～4294967295））フィールドで定義されます。
  - **Enable**（有効）— 断続的なポート再認証を有効にします。
  - **Disable**（無効）— 断続的なポート再認証を無効にします。
- **Reauthentication Period**（**300**～**4294967295**）（再認証の時期（300～4294967295））— 選択したポートを再認証するタイムスパンを指定します。フィールド値は秒単位です。デフォルト値は 3600 秒です。
- **Reauthenticate Now**（今すぐ再認証）— ポートの再認証を直ちに行うことができます。
  - **Checked**（チェックマークあり）— ポートの再認証を直ちに行うことができます。
  - **Disable**（無効）— ポートの再認証を直ちに行うことはできません。
- **Authentication Server Timeout**（**1**～**65535**）（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のにかかる時間を定義します。このフィールドの値は秒単位で指定します。デフォルト値は 30 秒です。
- **Resending EAP Identity Request**（**1**～**65535**）（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のにかかる時間を定義します。デフォルト値は 30 秒です。
- **Quiet Period**（**0-65535**）（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になる秒数を示します。可能なフィールド値の範囲は、0～65535 です。デフォルト値は 60 秒です。
- **Supplicant Timeout**（**1-65535**）（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のにかかる時間を示します。フィールド値は秒単位です。デフォルト値は 30 秒です。
- **Max EAP Requests**（**1-10**）（最大 EAP 要求（1～10））— 送信された 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は、認証処理が再スタートされます。デフォルトの試行回数は 2 回です。

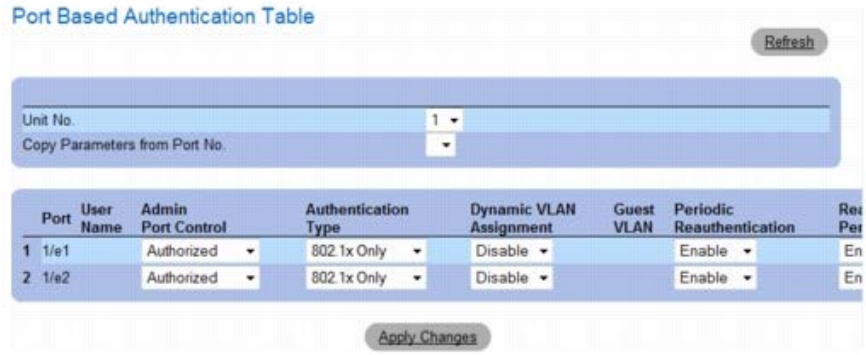
ポートベース認証表の表示

□□□ **Port Based Authentication**（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



これらのフィールドのほかに、**Port Based Authentication Table**（ポートベース認証表）には、次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.**（ポート番号からのパラメーターのコピー）— 選択したポートからパラメーターをコピーします。

Port Based Authentication Table（ポートベース認証表）のパラメーターのコピー

□□□ ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Port Based Authentication Table（ポートベース認証表）が開きます。

□□□ **Copy Parameters from Port No.**（ポート番号からのパラメーターのコピー）フィールドのインタフェースを選択します。

□□□ **Port Based Authentication Table**（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ー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、**Port Based Authentication Table**（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と等価 CLI コマンドをまとめたものです。

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 auth-not-req	権限のあるデバイスが VLAN にアクセスできるようにします。
dot1x guest-vlan	ゲスト VLAN を定義します。
dot1x guest vlan enable	インタフェース上で権限を付与されたユーザーがゲスト VLAN にアクセスできるようにします。
dot1x mac-authentication	ステーションの MAC アドレスに基づいた認証（MAC ベースの認証）を有効にします。
dot1x max-req *count*	認証プロセスを再スタートするまでに、デバイスからクライアントに EAP を送信する最大数を設定します。
dot1x re-authenticate [**ethernet** *interface*]	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。
dot1x re-authentication	クライアントの断続的な再認証を有効にします。
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にな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。
dot1x traps mac-authentication failure	MAC アドレスが認証（MAC ベースの認証）に失敗した場合、トラップの送信を有効にします。
dot1x radius-attribues vlan	ユーザーベースの VLAN 割り当てを有効にします。
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 ステータスを表示します。
show dot1x advanced	スイッチまたは指定インタフェースに関する 802.1X 拡張機能を表示します。
show dot1x users [**username** *username*]	デバイスに関する 802.1X ユーザーを表示します。
dot1x guest-vlan enable	権限のないポートに対するゲスト VLAN の使用を有効にします。Guest VLAN（ゲスト VLAN）を有効にすると、権限のないポートは自動的に **VLAN List**（VLAN リスト）フィールドで選択された VLAN に参加します。デフォルトでは、このフィールドは無効になっています。
dot1x guest-vlan	VLAN のリストを示します。ゲスト VLAN は、**VLAN List**（VLAN リスト）から選択されます。

CLI コマンドの例は次のようになります。

```
Console# show dot1x

Interface  Admin Mode  Oper Mode    Reauth Control  Reauth Period  Username
---------  ----------  -----------  --------------  -------------  --------
```

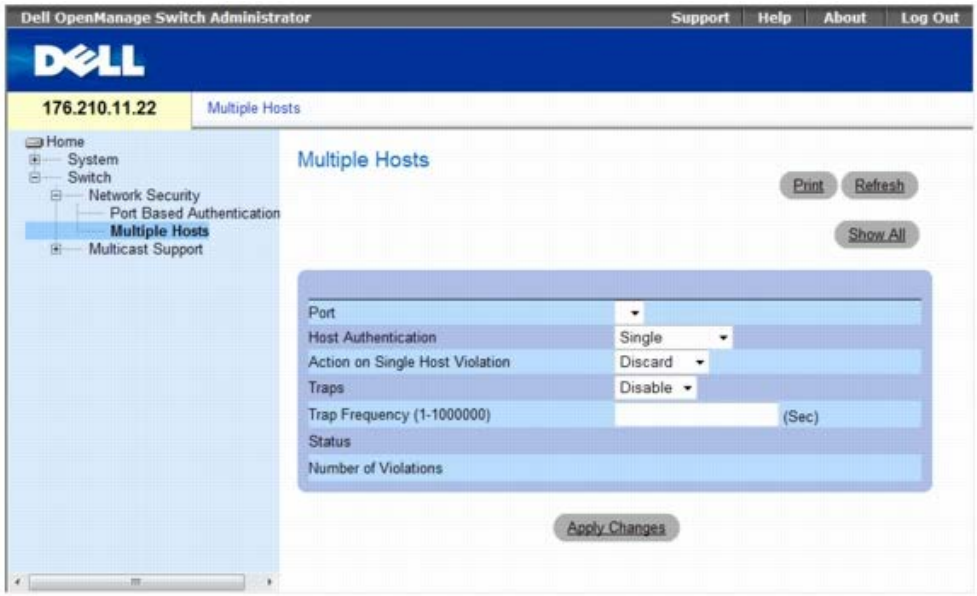
-	-----		--	-	-
1/e1	Auto	Authorized	Ena	3600	Bob
1/e2	Auto	Authorized	Ena	3600	John
1/e3	Auto	Unauthorized	Ena	3600	Clark
1/e4	Force-auth	Authorized	Dis	3600	n/a

拡張ポートベース認証の設定

Multiple Hosts（複数ホスト）ページには、特定のポート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。

Multiple Hosts（複数ホスト） 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**（複数ホスト）の順にクリックします。

図 **7-3.** 複数ホスト



Multiple Hosts（複数ホスト）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。
- **Host Authentication**（ホスト認証）— ホスト認証タイプを定義します。可能なフィールド値は次のとおりです。
  - **Single**（単一）— 単一セッションでのシステムへのアクセスで、単一の権限のあるホストのみを有効にします。
  - **Multiple Host**（複数ホスト）— 単一セッションでのシステムへのアクセスで、単一のホストが複数のホストを許可できるようにします。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。
  - **Multiple Session**（複数セッション）— 複数セッションでのシステムへのアクセスで、単一の権限のあるホストを有効にします。これがデフォルト値になっています。
- **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次のとおりです。
  - **Forward**（転送）— 未知の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）— いずれの未知の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になっています。
  - **Shutdown**（シャットダウン）— 未知の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。ポートがアクティブになるまで、またはスイッチがリセットされるまで、ポートはシャットダウン状態のままになります。
- **Traps**（トラップ）— 違反が発生した場合のホストへのトラップ送信を有効または無効にします。
  - **Enable**（有効）— トラップ送信を有効にします。
  - **Disable**（無効）— トラップ送信を無効にします。
- **Trap Frequency**（**1-1000000**）（トラップの頻度（1～1000000））— トラップをホストに送信する時間を秒単位で定義します。トラップの頻度（**1－1000000**）フィールドを定義できるのは、**Multiple Hosts**（複数ホスト）フィールドが **Disable**（無効）として定義されている場合のみです。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次のとおりです。
  - **Unauthorized**（無許可）— ポート制御が Force Unauthorized（強制無許可）で、ポートリンクがダウンしているかポート制御が Auto（自動）であるけれども、クライアントがポートを通して認証されていないことを示します。
  - **Not in Auto Mode**_（非自動モード）— ポート制御が Forced Authorized（強制無許可）で、クライアントがポートへのフルアクセス権を持っていることを示します。
  - **Single-host Lock**（単一ホストロック）— ポート制御が Auto（自動）で、単一のクライアントがポートを通して認証されていることを示します。
  - **No Single Host**（非単一ホスト）— Multiple Hosts（複数ホスト）が有効になっていることを示します。
- **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です。

Multiple Hosts Table（複数ホスト表）の表示

□□□ **Multiple Hosts**（複数ホスト）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

次のような **Multiple Hosts Table**（複数ホスト表）が開きます。

図 **7-4.** 複数ホスト表

Multiple Hosts Table（複数ホスト表）には、次の追加フィールドが表示されます。

- **Unit No.**（ユニット番号）— スタッキングメンバーを選択します。

CLI コマンドを使用した複数のホストの有効化

次の表は **Multiple Hosts**（複数ホスト）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 CLI コマンドをまとめたものです。

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るときの対応処置を設定します。

CLI コマンドの例は次のようになります。

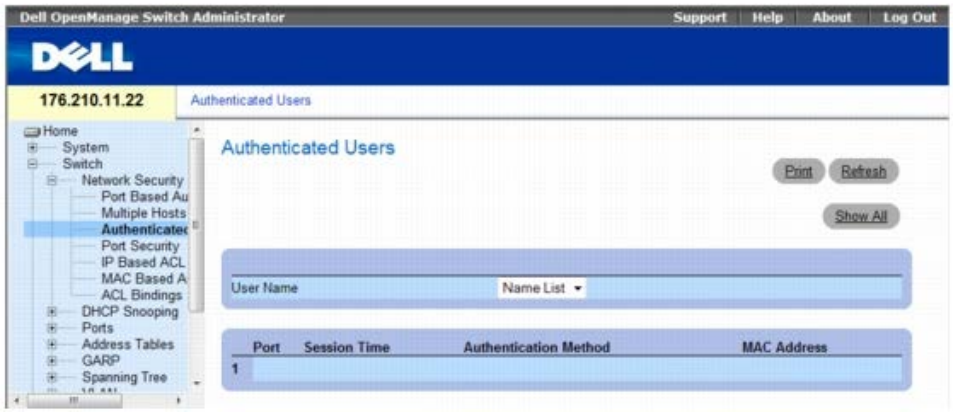
```
Console(config)# interface ethernet 1/e1
Console(config-if)# dot1x multiple-hosts
```

ユーザーの認証

Authenticated Users（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、_**Add User Name**（ユーザー名の追加）ページで定義します。

Authenticated Users（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



Authenticated Users（権限のあるユーザー）ページには、次のフィールドが含まれます。

- **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リストです。
- **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、フィールドの書式は **Day:Hour:Minute:Seconds**（日数:時間数:分数:秒数）です。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次のとおりです。
  - **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

□□□ **Authenticated Users**（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。

次のような **Authenticated Users Table**（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、**Authenticated Users**（認証ユーザー）ページに表示されたようにユーザーを認証するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
show dot1x users [**username** *username*]	デバイスに関する 802.1X ユーザーを表示します。

CLI コマンドの例は次のようになります。

```
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強化するには、特定の MAC アドレスを持つユーザーのみに特定の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モニタします。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ているか、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提供されます。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 アドレスのリストを設定ファイルに保存することもできます。MAC アドレスリストは、デバイスをリセットした後で復元できます。

ポートのセキュリティを有効にするためには、必要なポートで **Multiple Hosts**（複数ホスト）機能を有効にします。

無効にされたポートは、**Port Security**（ポートセキュリティ）ページからアクティブにできます。**Ports**（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のような高度な機能などのポート機能を設定したり、仮想ポートテスト実行したりできるリンクがあります。

Port Security（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

Port Security（ポートのセキュリティ）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）— ポートロックに選択されているインタフェースタイプは有効です。
  - **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** — 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）— ポートがロックまたはロック解除されます。可能なフィールド値は次のとおりです。
  - **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になっています。
  - **Locked**（ロック）— ポートをロックします。
- **Learning Mode**（ラーニングモード）— ロックされたポートタイプを定義します。**Learning Mode**（ラーニングモード）フィールドは、**Locked**（ロック）が **Set Port**（ポートの設定）フィールドで選択されている場合にのみ有効になります。可能なフィールド値は以下のとおりです。
  - **Classic Lock**（従来のロック）— 従来のロックメカニズムを使用してポートをロックします。すでに学習されているアドレス数に関係なく、ポートがただちにロックされます。

- **Limited Dynamic Lock**（制限動的ロック）— ポートに関連付けられた現在の動的 MAC アドレスを削除することで、ポートをロックします。ポートは許可されている最大アドレス数に達するまで学習します。MAC アドレスの再学習とエージングの両方が有効になります。

- **Max Entries**（**1-128**）（最大エントリ（1～128））— ポートで学習できる MAC アドレス数を指定します。**Max Entries**（最大エントリ）フィールドは、**Locked** が **Set Port**（ポートの設定）フィールドで選択にされている場合にのみ有効です。また、Limited Dynamic Lock（制限動的ロック）モードが選択されます。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次のとおりです。

  - **Forward**（転送）— 未知の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）— いずれの未知の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になっています。

  - **Shutdown**（シャットダウン）— 未知の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。ポートが再びアクティブになるまで、またはデバイスがリセットされるまで、ポートはシャットダウン状態のままになります。

- **Trap**（トラップ）— ロックされたポートでパケットを受信すると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

□□□ **Port Security**（ポートセキュリティ）ページを開きます。

□□□ インタフェースの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 **Port Security Table**（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

□□□ **Port Security**（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。

次のような **Port Security Table**（ポートセキュリティ表）が開きます。

Locked Ports（ロックされたポート）は、**Port Security Table**（ポートセキュリティ表）で定義されます。

図 **7-8.** ポートセキュリティ表

Port Security Table（ポートセキュリティ表）には、次の追加フィールドが含まれます。

- **Unit No.**（ユニット番号）— ロックされたポート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**（パラメーターのコピー元）— パラメーターがコピーされ、選択したユニット番号に割り当てられるポートです。

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 Port Security（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ための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
shutdown	インタフェースを無効にします。
set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}	ポート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します。
port security learning {disabled | dynamic}	ロックされるポート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。

CLI コマンドの例は次のようになります。

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	-	-	-	-

ACL の概要

ネットワーク管理者はアクセスコントロールリスト（ACL）を利用することにより、特定の入力ポートの分類処理およびルールを定義できます。入力ポートに到達したパケットは、アクティブな ACL を使用して、エントリを許可または拒否されます。拒否されると、その入力ポートは無効になります。パケットのエントリが拒否された場合、ユーザーはそのポートを無効にできます。

本項には、次のトピックがあります。

- IP ベース ACL の定義
- MAC ベースのアクセスコントロールリストの定義
- ACL のバインディングの定義

IP ベース ACL の定義

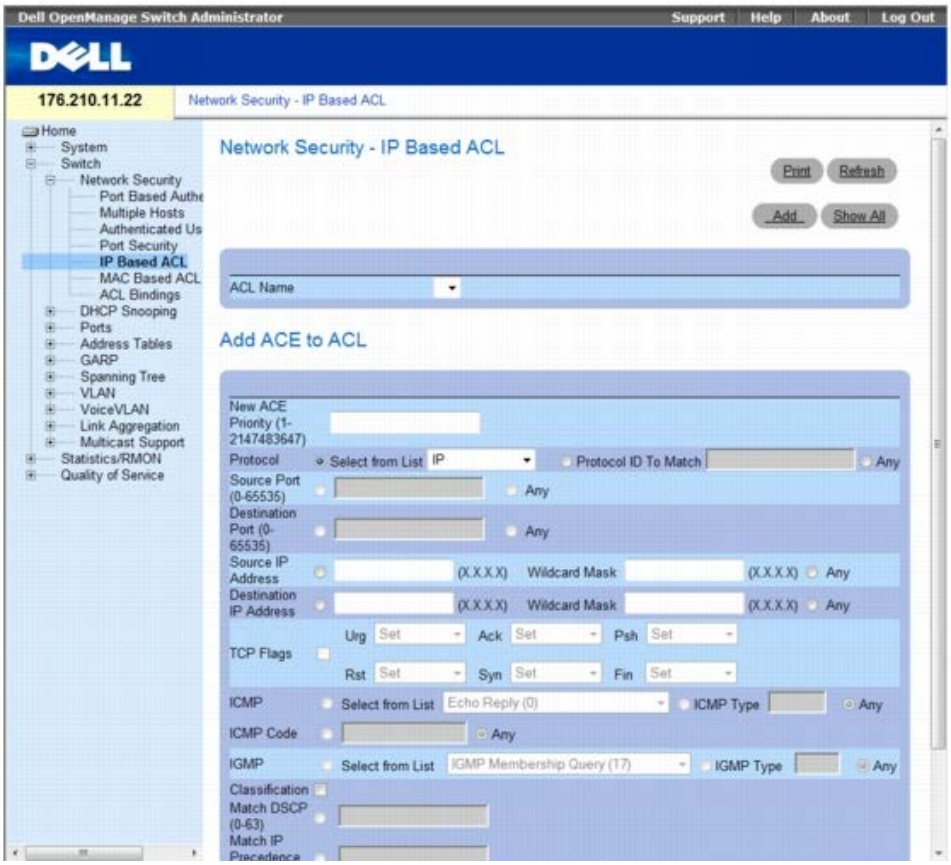
ネットワーク管理者は、アクセスコントロールエントリ（ACE）で構成されるアクセスコントロールリスト（ACL）を利用することにより、特定の入力ポートの分類処理およびルールを定義できます。入力ポートに到達したパケットは、アクティブな ACL を使用して、エントリを許可または拒否されます。拒否されると、その入力ポートは無効になります。パケットのエントリが拒否された場合、ユーザーはそのポートを無効にできます。

例えば、ネットワーク管理者は、ポート番号 20 では TCP パケットを受信できるが、UDP パケットを受信した場合は破棄されるように指示した ACL ルールを定義できます。

ACL は、トラフィックの分類を決定するフィルタからなるアクセスコントロールエントリ（ACE）で構成されます。各 ACE は 1 つのルールであり、使用可能なルールは 256 個あります。ただし、ルールはユーザー設定用だけでなく、DHCP スヌーピング、プロトコルグループ VLAN および PVE のような機能にも使用されるので、256 個すべてを ACE に使用できるわけではありません。少なくとも 124 のルールが使用可能になると予想されます。ルール数がより少ない場合、DHCP スヌーピングが原因の可能性があります。ACE ルールを解放するには、DHCP スヌーピング設定でエントリの数を減らしてください。

IP ベースの ACL を定義するには、**Switch**（スイッチ）® **Network Security**（ネットワークセキュリティ）® **IP Based ACL**（IP ベース ACL）の順にクリックします。

図 **7-9.** ネットワークセキュリティ **- IP** ベース **ACL**



- **ACL Name**（ACL 名）— ユーザー定義の ACL です。
- **New ACE Priority**（新規の ACE 優先度）— 最初のマッチに基づいて、どの ACE をパケットにマッチさせるかを決定する ACE 優先度です。
- **Protocol**（プロトコル）— 特定のプロトコルに基づいた ACE の作成を可能にします。可能なフィールド値は次のとおりです。
  - **IP** — インターネットプロトコル（IP）です。 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。
  - **ICMP** — インターネットコントロールメッセージプロトコル（ICMP）です。ICMP は、ゲートウェイまたは宛先ホストに、処理中エラーの報告など、送信元ホストとの通信を許可します。
  - **IGMP** — インターネットグループ管理プロトコル（IGMP）です。 ホストはローカルスイッチまたはルーターに対して、特定のマルチキャストグループに割り当てられた伝送を受信するように指示できます。
  - **TCP** — 伝送コントロールプロトコル（TCP）です。 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。
  - **EGP** — 外部ゲートウェイプロトコル（EGP）です。 自律的なシステムネットワーク内に隣接する 2 台のゲートウェイホスト間で、経路指定情報を交換できるようにします。
  - **IGP** — 内部ゲートウェイプロトコル（IGP）です。 自律的なネットワークのゲートウェイ間で経路指定情報を交換できるようにします。
  - **UDP** — ユーザーデータグラムプロトコル（UDP）です。 この通信プロトコルは、パケットを伝送しますが配信は保証しません。
  - **HMP** — ホストマッピングプロトコル（HMP）です。 各種のネットワークホストからネットワーク情報を収集します。HMP は、インターネット上に分散しているホスト、および単一ネットワーク内のホストをモニタします。
  - **RDP** — リモートデスクトッププロトコル（RDP）です。 クライアントとネットワーク上のターミナルサーバーとの通信を可能にします。
  - **IDPR** — パケットを IDPR プロトコルでマッチさせます。
  - **IPV6** — パケットを IPV6 プロトコルでマッチさせます。
  - **IPV6 ROUTE** — パケットを IPV6 ROUTE プロトコルでマッチさせます。
  - **IPV6 FRAG** — パケットを IPV6 FRAG プロトコルでマッチさせます。
  - **IDRP** — パケットをドメイン間ルーティングプロトコル（IDRP）でマッチさせます。
  - **RVSP** — パケットを ReSerVation プロトコル（RSVP）でマッチさせます。

AH — 認証ヘッダー（AH）です。送信元ホストの認証とデータ保全を実現します。

- **EIGRP** — 拡張内部ゲートウェイルーティングプロトコル（EIGRP）です。すばやい収束を実現し、可変長のサブネットマスクや複数のネットワーク層プロトコルをサポートします。
- **OSPF** — オープンショーテストパスファースト（OSPF）プロトコルは、ネットワークルーティングのレイヤ 2 トンネリングプロトコルに対応したリンクステート階層型の内部ゲートウェイプロトコル（IGP）であり、ISP による仮想プライベートネットワーク（VPN）の運用を可能にする PPP プロトコルの拡張版です。
- **IPIP** — IP over IP（IPIP）です。IP パケットをカプセル化して、2 つのルーター間にトンネルを作成します。これによって、IPIP トンネルは、複数の独立したインタフェースではなく、単一のインタフェースのように見えます。IPIP は、イントラネットのトンネル接続によるインターネットの構築を可能にするもので、ソースルーティングの代わりとなります。
- **PIM** — パケットをプロトコルインデペンデントマルチキャスト（PIM）でマッチさせます。
- **L2TP** — パケットをインターネットプロトコル（L2IP）でマッチさせます。
- **ISIS** — Intermediate System - Intermediate System（ISIS）です。IP ネットワーク内の単一の自律システム全体に IP 経路指定情報を配信します。
- **Protocol ID To Match**（マッチさせるプロトコル）— パケットを ACE にマッチさせる際のユーザー定義プロトコルを追加します。各プロトコルには、固有のプロトコル番号があります。可能なフィールド値は、0～255 です。
- **Any**（すべて）— プロトコルをすべてのプロトコルでマッチさせます。

- **Source Port**（送信元ポート）— TCP/UDP 送信元ポートです。すべてのポートを含めるには、**Any**（すべて）を選択します。
- **Destination Port**（宛先ポート）— TCP/UDP 宛先ポートです。すべてのポートを含めるには、**Any**（すべて）を選択します。
- **Source IP Address**（送信元 IP アドレス）— パケットに指定されている送信元ポートの IP アドレスと ACE のマッチングを行います。ワイルドカードマスクは、どのビットを使用し、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。
- **Destination IP Address**（宛先 IP アドレス）— パケットに指定されている宛先ポートの IP アドレスと ACE のマッチングを行います。ワイルドカードマスクは、どのビットを使用し、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。
- **TCP Flags**（TCP フラグ）— トリガ可能な指定された TCP フラグを設定します。TCP フラグを使用するには、**TCP Flag**（TCP フラグ）チェックボックスをオンにしてから、必要なフラグを設定します。
- **ICMP** — ICMP パケットをフィルタリングするための ICMP メッセージタイプを指定します。リストから選択するか、入力するか、またはすべての ICM メッセージタイプを含める場合は **Any**（すべて）を選択できます。このフィールドは、**Protocol**（プロトコル）フィールドで ICMP が選択されている場合のみ使用できます。
- **ICMP Code**（ICMP コード）— ICMP パケットをフィルタリングするための ICMP メッセージコードを指定します。ICMP パケットは、ICMP メッセージタイプまたは ICMP メッセージコードによってフィルタリングされ鑢す。このフィールドは、**Protocol**（プロトコル）フィールドで ICMP が選択されている場合のみ使用できます。
- **IGMP** — IGMP パケットは、IGMP メッセージタイプによってフィルタリングできます。リストから選択するか、入力するか、またはすべての IGMP メッセージタイプを含める場合は**Any**（すべて）を選択できます。このフィールドは、**Protocol**（プロトコル）フィールドで IGMP が選択されている場合のみ使用できます。
- **Classification Mach DSCP**（分類 DSCP のマッチ）— パケットの DSCP 値と ACL のマッチングを行います。パケットを ACL にマッチさせるには、DSCP 値または IP 優先権の値を使用します。可能なフィールド値は、0～63 です。
- **Match IP Precedence**（IP 優先権のマッチ）— ip-precedence とパケットの ip-precedence 値のマッチングを指示します。IP 優先権は、CIR しきい値を超えるフレームのマーキングを有効にします。混雑したネットワークでは、DP の小さいフレームよりも DP の大きいフレームの方が先に破棄されます。
- **Action**（処置）— ACL 転送処置を示します。可能なフィールド値は次のとおりです。
  - **Permit**（許可）— ACL の基準に一致するパケットを転送します。
  - **Deny**（拒否）— ACL の基準に一致するパケットを破棄します。
  - **Shutdown**（シャットダウン）— ACL の基準に一致するパケットを破棄し、パケットの宛先であるポートを無効にします。

IP ベース ACL への ACE の追加

□□□ **Network Security - IP Based ACL**（ネットワークセキュリティ - IP ベース ACL）ページを開きます。

□□□ ACL を選択します。

□□□ 関連するフィールドを編集します。

□□□ **Apply Changes**（変更の適用）をクリックします。

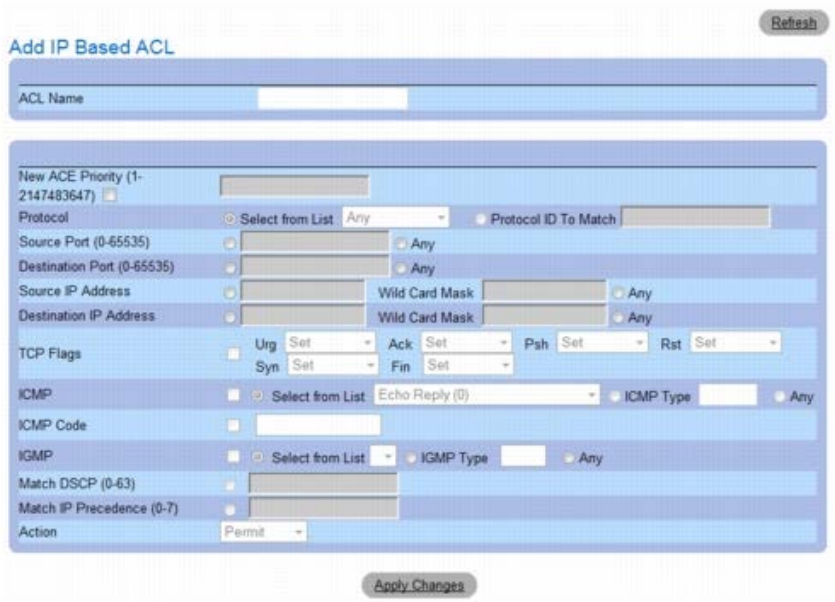
IP ベース ACL の追加

□□□ **IP Based ACL**（IP ベース ACL）ページを開きます。

□□□ **Add**（追加）をクリックします。

次のような **Network Security - IP Based ACL**（ネットワークセキュリティ - IP ベース ACL）ページが開きます。

図 **7-10. IP** ベース **ACL** の追加



□□□ 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 ベースプロトコルが定義され、デバイスがアップデートされます。

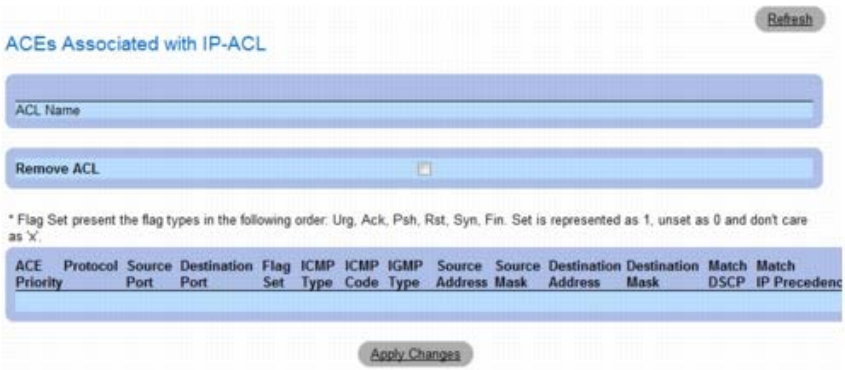
IP ベース ACL に関連付けられた ACE の表示

□□□ **Network Security - IP Based ACL**（ネットワークセキュリティ - IP ベース ACL）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

次のような ACEs Associated with IP-ACL（IP-ACL に関連付けられた ACE）が開きます。

図 **7-11. IP-ACL** に関連付けられた **ACE**



IP ベース ACL の削除

□□□ **Network Security - IP Based ACL**（ネットワークセキュリティ - IP ベース ACL）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。**ACEs Associated with IP-ACL Table**（IP-ACL に関連付けられた ACE 表）が開きます。

□□□ **Remove ACL**（ACL の削除）チェックボックスをオンにします。

□□□ **Apply Changes**（変更の適用）をクリックします。

IP ベース ACE の削除

□□□ **Network Security - IP Based ACL**（ネットワークセキュリティ - IP ベース ACL）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。**ACEs Associated with IP-ACL Table**（IP-ACL に関連付けられた ACE 表）が開きます。

□□□ ACE の横にある **Remove**（削除）チェックボックスをオンにします。

□□□ **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 IP ベース ACL の設定

次の表は、IP ベース ACL を設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ip access-list *access-list-name* **no ip access-list** *access-list-name*	IPv4 アクセスリストを定義し、デバイスを IPv4 アクセスリスト設定モードに設定するには、グローバル設定モードで ipv4 access-list コマンドを使用します。アクセスリストを削除するには、このコマンドの no 形式を使用します。
permit {any| *protocol*} {any|{*source source-wildcard*}} {any|{*destination destination-wildcard*}} [dscp *number* | ip-precedence *number*] [fragments] permit-icmp {any|{*source source-wildcard*}} {any|{*destination destination-wildcard*}} {any|*icmp-type*} {any|*icmp-code*} [dscp *number* | ip-precedence *number*] permit-igmp {any|{*source source-wildcard*}} {any|{*destination destination-wildcard*}} {any|*igmp-type*} [dscp *number* | ip-precedence *number*] permit-tcp {any|{ *source source-wildcard*}} {any|*source-port*} {any|{ *destination destination-wildcard*}} {any|*destination-port*} [dscp *number* | ip-precedence *number*] [flags *list-of-flags*] permit-udp {any|{ *source source-wildcard*}} {any| *source-port*} {any|{*destination destination-wildcard*}} {any|*destination-port*} [dscp *number* | ip-precedence *number*]	パケットが名前付き IP アクセスリストを渡すように条件を設定するには、アクセスリスト設定モードで permit コマンドを使用します。
deny [disable-port] {any| *protocol*} {any|{*source source-wildcard*}} {any|{*destination destination-wildcard*}} [dscp *number* | ip-precedence *number*] [fragments] deny-icmp [disable-port] {any|{*source source-wildcard*}} {any|{*destination destination-wildcard*}} {any|*icmp-type*} {any|*icmp-code*} [dscp *number* | ip-precedence *number*] deny-igmp [disable-port] {any|{*source source-wildcard*}} {any|{*destination destination-wildcard*}} {any|*igmp-type*} [dscp *number* | ip-precedence *number*] deny-tcp [disable-port] {any|{ *source source-wildcard*}} {any|*source-port*} {any|{ *destination destination-wildcard*}} {any|*destination-port*} [dscp *number* | ip-precedence *number*] [flags *list-of-flags*] deny-udp [disable-port] {any|{ *source source-wildcard*}} {any| *source-port*} {any|{*destination destination-wildcard*}} {any|*destination-port*} [dscp *number* | ip-precedence *number*]	パケットが名前付き IP アクセスリストを渡すように条件を設定するには、アクセスリスト設定モードで deny コマンドを使用します。

MAC ベースのアクセスコントロールリストの定義

MAC ベース ACL の定義は、**Network Security - MAC Based ACL**（ネットワークセキュリティ - MAC ベース ACL）ページで行います。ACE は、ACL がインタフェースにバインドされていない場合のみ追加できます。

MAC ベース ACL を定義するには、**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 ACL）をクリッ

クします。

- ネットワークセキュリティ - MAC ベース ACL

- **ACL Name**（ACL 名）— ユーザー定義の MAC ベース ACL を表示します。
- **New ACE Priority**（新規 ACE 優先度）— 最初のマッチに基づいて、どの ACE をパケットにマッチさせるかを決定する ACE 優先度です。可能なフィールド値は、1～2147483647 です。
- **Source Address**（送信元アドレス）— パケットの送信元である MAC アドレスと ACE のマッチングを行います。ワイルドカードマスクは、どのビットを使用し、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。
- **Destination Address**（宛先アドレス）— パケットの宛先である MAC アドレスと ACE のマッチングを行います。ワイルドカードマスクは、どのビットを使用し、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。
- **VLAN ID** — パケットの VLAN ID と ACE のマッチングを行います。可能なフィールド値は、1～4095 です。
- **CoS** — パケットのフィルタリングに使用する CoS 値を示します。
- **Cos Mask**（CoS マスク）— パケットのフィルタリングに使用する CoS マスクを示します。
- **Ethertype** — パケットのフィルタリングに使用する Ethertype パケットを示します。
- **Action**（処置）— ACL 転送処置を示します。可能なフィールド値は以下のとおりです。
  - **Permit**（許可）— ACL の基準に一致するパケットを転送します。
  - **Deny**（拒否）— ACL の基準に一致するパケットを破棄します。
  - **Shutdown**（シャットダウン）— ACL の基準に一致するパケットを破棄し、パケットの宛先であるポートを無効にします。

IP ベース ACL への ACE の追加

□□□ **Network Security - MAC Based ACL**（ネットワークセキュリティ - MAC ベース ACL）ページを開きます。

□□□ ACL を選択します。

□□□ 関連するフィールドを編集します。

□□□ **Apply Changes**（変更の適用）をクリックします。

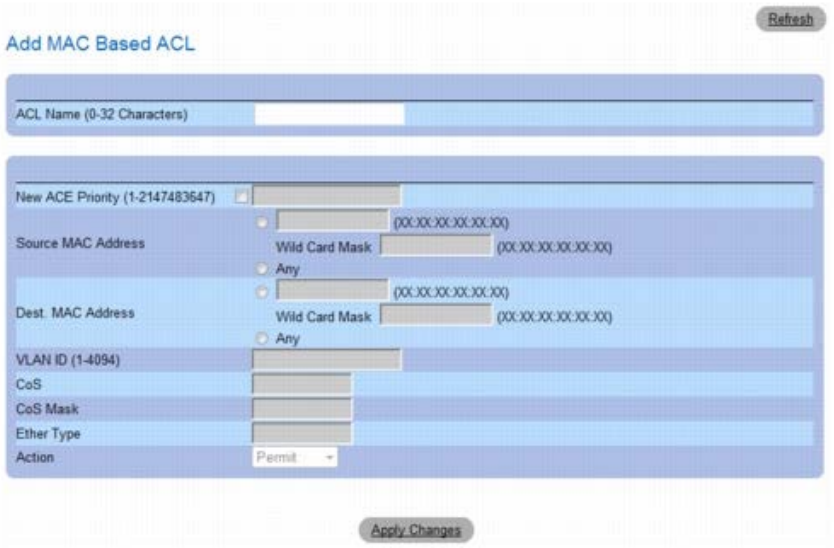
MAC ベース ACL の追加

□□□ **MAC Based ACL**（MAC ベース ACL）ページを開きます。

□□□ **Add**（追加）をクリックします。

次のような **Network Security - MAC Based ACL**（ネットワークセキュリティ - MAC ベース ACL）ページが開きます。

図 **7-12. MAC** ベース **ACL** の追加



□□□ 関連フィールドを定義します。

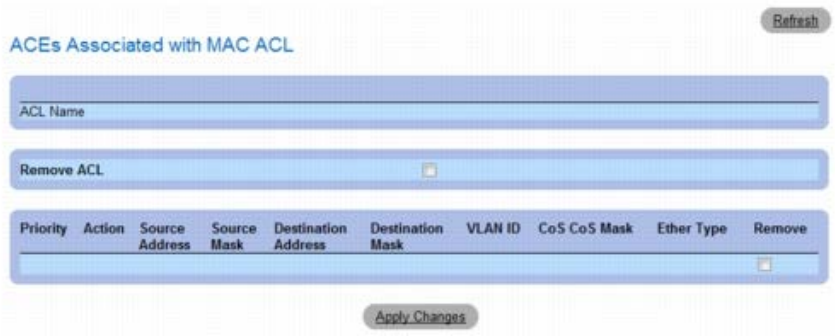
□□□ **Apply Changes**（変更の適用）をクリックします。MAC ベースプロトコルが定義され、デバイスがアップデートされます。

MAC ベース ACL に関連付けられた ACE の表示

□□□ **Network Security - MAC Based ACL**（ネットワークセキュリティ - MAC ベース ACL）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

次のような ACEs Associated with MAC Based ACL（MAC-ACL に関連付けられた ACE）が開きます。



MAC ベース ACL の削除

□□□ **Network Security - MAC Based ACL**（ネットワークセキュリティ - MAC ベース ACL）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。 **ACEs Associated with MAC-ACL Table**（MAC-ACL に関連付けられた ACE 表）が開きます。

□□□ **Remove ACL**（ACL の削除）チェックボックスをオンにします。

□□□ **Apply Changes**（変更の適用）をクリックします。

MAC ベース ACE の削除

□□□ **Network Security - MAC Based ACL**（ネットワークセキュリティ - MAC ベース ACL）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。 **ACEs Associated with MAC-ACL Table**（MAC-ACL に関連付けられた ACE 表）が開きます。

□□□ ACE の横にある **Remove**（削除）チェックボックスをオンにします。

□□□ **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 MAC ベース ACL の設定

次の表は、MAC ベース ACLを設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
mac access-list *access-list-name* **no mac access-list** *access-list-name*	レイヤ 2 アクセスリストを定義し、デバイスを MAC アクセスリスト設定モードに入れるには、グローバル設定モードで mac access-list コマンドを使用します。アクセスリストを削除するには、このコマンドの no 形式を使用します。
permit {any|{*source source- wildcard*} {any|{ *destination destination- wildcard*}} [vlan *vlan-id*] [cos *cos cos-wildcard*] [ethtype *eth-type*] [inner-vlan *vlan-id*]	MAC アクセスリストの許可条件を設定するには、MAC アクセスリスト設定モードで permit コマンドを使用します。
deny [disable-port] {any|{*source source- wildcard*} {any|{ *destination destination- wildcard*}} [vlan *vlan-id*] [cos *cos cos-wildcard*] [ethtype *eth-type*] [inner-vlan *vlan-id*]	MAC アクセスリストの拒否条件を設定するには、MAC アクセスリスト設定モードで deny コマンドを使用します。

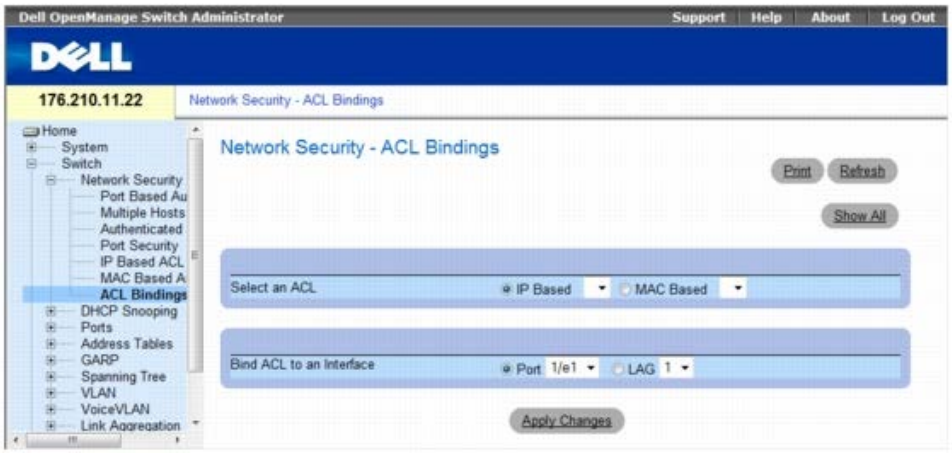
ACL のバインディングの定義

ACL をインタフェースにバインドすると、定義されているすべての ACE ルールが、選択したインタフェースに適用されます。ACL をポート、LAG または VLAN に割り当てると、その入力インタフェースのフローが ACL にマッチしない場合、Drop unmatched packets（マッチしないパケットを削除）というデフォルトルールが適用されます。

ACL をインタフェースにバインドするには、次の手順を実行します。

□□□ **Network Security - ACL Bindings**（ネットワークセキュリティ - ACL のバインディング）ページを開き、**Switch**（スイッチ）® **Network Security**（ネットワークセキュリティ）® **ACL Bindings**（ACL のバインディング）をクリックします。

図 **7-13.** ネットワークセキュリティ **- ACL** のバインディング



□□□ **Select an ACL**（ACL の選択）フィールドで、IP ベースまたは MAC ベースの ACL を選択します。

□□□ **Bind ACL to an Interface**（ACL をインタフェースにバインド）フィールドで、ポートまたは LAG を選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

ACL がインタフェースにバインドされます。

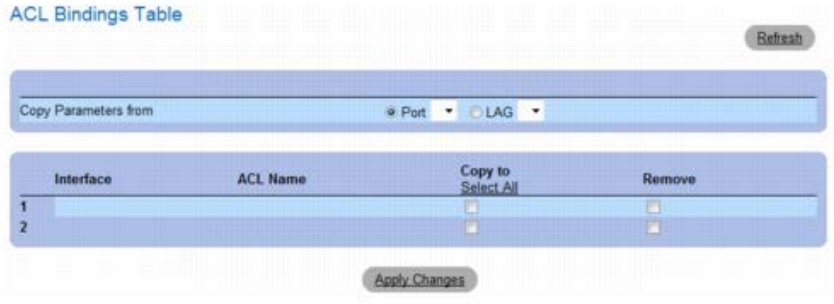
ACL のバインディング表を表示するには、次の手順を実行します。

□□□ **Network Security - ACL Binding**（ネットワークセキュリティ - ACL のバインディング）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

ACL Bindings Table（ACL のバインディング表）が開きます。

図 **7-14. ACL** のバインディング表



インタフェース間での ACL パラメーターのコピー

□□□ **Network Security - ACL Binding**（ネットワークセキュリティ - ACL のバインディング）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。**ACL Bindings Table**（ACL のバインディング表）が開きます。

□□□ **Copy Parameters from**（パラメーターのコピー元）フィールドで、ACL 設定のコピー元とするポートまたは LAG を選択します。

□□□ 表内で、設定のコピー先とする各エントリに対する **Copy to**（コピー先）チェックボックスをオンにします。

□□□ **Apply Changes**（変更の適用）をクリックします。

ACL のバインディングの削除

□□□ **Network Security - ACL Binding**（ネットワークセキュリティ - ACL のバインディング）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。**ACL Bindings Table**（ACL のバインディング表）が開きます。

□□□ 表内で、削除する各バインディングに対する **Remove**（削除）チェックボックスをオンにします。

□□□ **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 ACL のバインディングの設定

次の表は、ACL のバインディングを設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
service-acl input *acl-name* no service-acl input	インタフェースへのアクセスを制御するには、インタフェース設定モードで service-acl コマンドを使用します。アクセス制御を削除するには、このコマンドの no 形式を使用します。
show access-lists [*name*]	スイッチに設定されているアクセスコントロールリスト（ACL）を表示するには、show access-lists privileged EXEC コマンドを使用します。

次は、CLI コマンドの例です。

```
Switch# show access-lists
IP access list ACL1
permit 234 172.30.40.1 0.0.0.0 any
```

```
permit 234 172.30.8.8 0.0.0.0 any
```

DHCP スヌーピングの設定

DHCP スヌーピングは、信頼できないインタフェースと DHCP サーバーの間にファイアウォールセキュリティを提供することによって、ネットワークのセキュリティを強化します。ネットワーク管理者は DHCP スヌーピングを有効にすることによって、エンドユーザーまたは DHCP サーバーに接続する信頼できるインタフェースと、ネットワークファイアウォールの向こう側にある信頼できないインタフェースを区別できます。

DHCP スヌーピングは、信頼できないメッセージのフィルタを行います。DHCP スヌーピングにより、信頼できないパケットから受信した情報を示す DHCP スヌーピング表が作成され、保持されます。ネットワークの外側またはネットワークファイアウォールの向こう側のインタフェースからパケットを受信する場合、インタフェースは信頼できません。信頼できるインタフェースは、ネットワーク内またはネットワークファイアウォール内からのみパケットを受信します。

DHCP スヌーピング表には、信頼できないインタフェースの MAC アドレス、IP アドレス、リース時間、VLAN ID、およびインタフェース情報が含まれます。

DHCP の項には、次のトピックがあります。

- DHCP スヌーピングプロパティの定義
- VLAN における DHCP スヌーピングの定義
- 信頼できるインタフェースの定義
- DHCP スヌーピングデータベースへのインタフェースの追加

本項には、次のトピックがあります。

- DHCP スヌーピンググローバルパラメーターの定義
- VLAN における DHCP スヌーピングの定義
- 信頼できるインタフェースの定義
- DHCP スヌーピングデータベースへのインタフェースの追加

DHCP スヌーピンググローバルパラメーターの定義

DHCP Snooping Global Parameters（DHCP スヌーピンググローバルパラメーター）ページには、デバイスで DHCP スヌーピングを有効にして設定するためのパラメーターがあります。

DHCP グローバルパラメーターを定義するには、**Switch**（スイッチ）® **DHCP Snooping**（DHCP スヌーピング）® **Global Parameters**（グローバルパラメーター）の順にクリックします。

図 **7-15.** グローバルパラメーター

- **DHCP Snooping Status**（DHCP スヌーピングステータス）— DHCP スヌーピングがデバイスで有効であるかどうかを示します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— デバイスで DHCP スヌーピングを有効にします。
  - **Disable** — DHCP

（無効） デバイスで スヌーピングを無効にします。これがデフォルト値になっています。

- **Verify MAC Address**（MAC アドレスの検証）— MAC アドレスを検証するかどうかを示します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— 信頼できないポートの送信元 MAC アドレスがクライアントの MAC アドレスに一致するかどうかを検証します。
  - **Disable**（無効）— 信頼できないポートの送信元 MAC アドレスがクライアントの MAC アドレスに一致するかどうかを検証しません。これがデフォルト値になっています。
- **Save Binding Database to File**（バインディングデータベースをファイルに保存）— DHCP スヌーピングデータベースをファイルに保存するかどうかを示します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— データベースのファイルへの保存を有効にします。これがデフォルト値になっています。
  - **Disable**（無効）— データベースのファイルへの保存を無効にします。
- **Save Binding Database Internal**（バインディングデータベースの内部保存）— DHCP スヌーピングデータベースをアップデートする頻度を示します。可能なフィールド値は、600～86400 秒です。フィールドデフォルト値は 1200 秒です。

CLI コマンドを使用した DHCP スヌーピンググローバルパラメーターの設定

次の表は、DHCP スヌーピンググローバルパラメーターを設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ip dhcp snooping no ip dhcp snooping	DHCP スヌーピングをグローバルに有効にするには、ip dhcp snooping グローバル設定コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。
ip dhcp snooping verify no ip dhcp snooping verify	信頼できないポートで DHCP パケットの送信元 MAC アドレスがクライアントハードウェアアドレスに一致するかどうかを検証するように、スイッチを設定するには、ip dhcp snooping verify グローバル設定コマンドを使用します。スイッチが MAC アドレスを検証しないように設定するには、このコマンドの no 形式を使用します。
ip dhcp snooping database no ip dhcp snooping database	DHCP スヌーピングバインディングファイルを設定するには、ip dhcp snooping database グローバル設定コマンドを使用します。バインディングファイルを削除するには、このコマンドの no 形式を使用します。
ip dhcp snooping database update-freq *seconds* no ip dhcp snooping database update-freq	DHCP スヌーピングバインディングファイルのアップデート頻度を設定するには、ip dhcp snooping database update-freq グローバル設定コマンドを使用します。デフォルトに戻すには、このコマンドの形式を使用しません。
show ip dhcp snooping [ethernet *interface* | port-channel *port-channel-number*]	DHCP スヌーピング設定を表示するには、ip dhcp snooping EXEC コマンドを使用します。

次は、CLI コマンドの例です。

```
Console# show ip dhcp snooping


DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 2, 7-18
DHCP snooping database: enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled

   Interface    Trusted
   -----------  -----------
   1/1          yes
   1/2          yes
```

VLAN における DHCP スヌーピングの定義

ネットワーク管理者は**DHCP Snooping VLAN Settings**（DHCP スヌーピング VLAN 設定）ページを利用して、VLAN に DHCP スヌーピングを有効にできま

す。DHCP スヌーピングは、VLAN 内のポートを識別します。VLAN の DHCP スヌーピングを有効にするには、DHCP スヌーピングがデバイスで有効であることを確認してください。VLAN の DHCP スヌーピングを有効にするには、次の手順を実行します。

VLAN の DHCP スヌーピングを定義するには、**Switch**（スイッチ）® **DHCP Snooping**（DHCP スヌーピング）® **VLAN Settings**（VLAN 設定）をクリックします。

図 **7-16. VLAN** 設定

- **VLAN ID** — DHCP スヌーピングを有効にできる VLAN です。
- **Enabled VLANs**（有効な VLAN）— DHCP スヌーピングが有効である VLAN のリストを示します。

VLAN における DHCP スヌーピングの定義

□□□ DHCP Snooping VLAN Settings（DHCP スヌーピング VLAN 設定）ページを開きます。

□□□ Enabled VLAN（有効な VLAN）リストに対して VLAN ID を追加または削除するには、**Add**（追加）または **Remove**（削除）をクリックします。

□□□ **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 VLAN における DHCP スヌーピングの設定

次の表は、VLAN における DHCP スヌーピングを設定する場合の等価 CLI コマンドをまとめたものです。

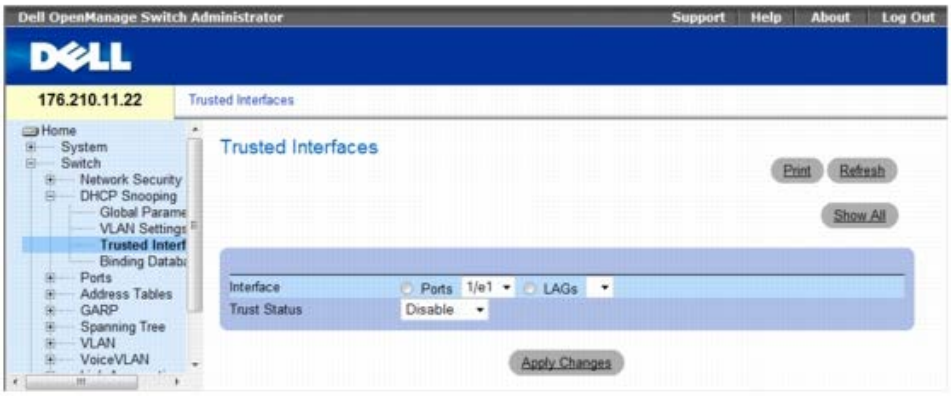
CLI コマンド	説明
ip dhcp snooping vlan *vlan-id* no ip dhcp snooping *vlan-id*	VLAN に対して DHCP スヌーピングを有効にするには、ip dhcp snooping vlan グローバル設定コマンドを使用します。VLAN に対して DHCP スヌーピングを無効にするには、このコマンドの no 形式を使用します。

信頼できるインタフェースの定義

ネットワーク管理者は **Trusted Interfaces**（信頼できるインタフェース）ページを利用して、信頼できるインタフェースを定義できます。ネットワークの外側またはネットワークファイアウォールの向こう側のインタフェースからパケットを受信する場合、インタフェースは信頼できません。信頼できるインタフェースは、ネットワーク内またはネットワークファイアウォール内からのみパケットを受信します。

信頼できるインタフェースを定義するには、**Switch**（スイッチ）® **DHCP Snooping**（DHCP スヌーピング）® **Trusted Interface**（信頼できるインタフェース）の順にクリックします。

図 **7-17.** 信頼できるインタフェース



- **Interface**（インタフェース）— DHCP スヌーピング信頼モードを有効にするポートまたは LAG を示します。
- **Trust Status**（信頼ステータス）— DHCP スヌーピング信頼モードがポートまたは LAG で有効であるかどうかを示します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— DHCP スヌーピング信頼モードがポートまたは LAG で有効であることを示します。
  - **Disable**（無効）— DHCP スヌーピング信頼モードがポートまたは LAG で無効であることを示します。

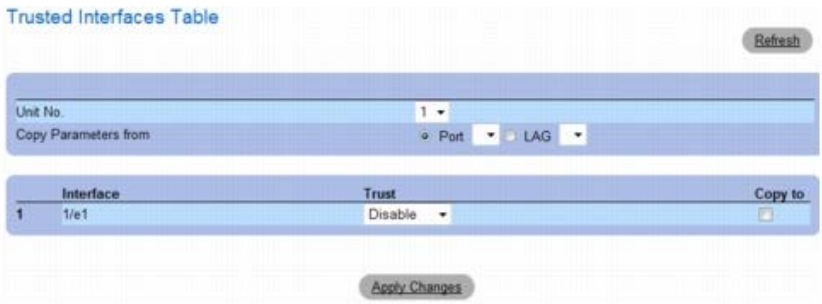
信頼できるインタフェース表を表示するには、次の手順を実行します。

□□□ **Trusted Interfaces**（信頼できるインタフェース）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Trusted Interfaces Table（信頼できるインタフェース表）が開きます。

図 **7-18.** 信頼できるインタフェース表



インタフェース間の信頼できるインタフェース設定のコピー

□□□ **Trusted Interfaces**（信頼できるインタフェース）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。**Trusted Interfaces Table**（信頼できるインタフェース表）が開きます。

□□□ **Unit**（ユニット）フィールドと **Copy from**（コピー元）フィールドで、設定のコピー元とするポートまたは LAG を選択します。

□□□ 表内で、設定のコピー先とする各エントリに対する **Copy to**（コピー先）チェックボックスをオンにします。

□□□ **Apply Changes**（変更の適用）をクリックします。

信頼できるインタフェースと信頼できないインタフェースの指定

□□□ **Trusted Interfaces**（信頼できるインタフェース）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。**Trusted Interfaces Table**（信頼できるインタフェース表）が開きます。

□□□ 表の **Trust**（信頼）列で、インタフェースの信頼を有効または無効にします。

□□□ **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 DHCP スヌーピングの信頼できるインタフェースの設定

次の表は、DHCP スヌーピングの信頼できるインタフェースを設定する場合の等価 CLI コマンドをまとめたものです。

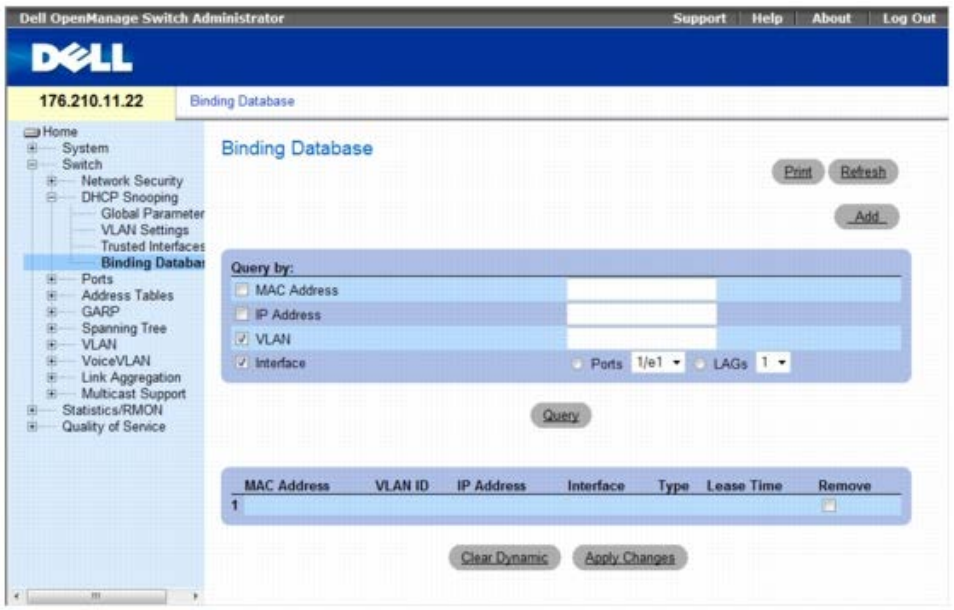
CLI コマンド	説明
ip dhcp snooping trust **no ip dhcp snooping trust**	DHCP スヌーピング用に信頼できるポートとして設定するには、ip dhcp snooping trust インタフェース設定コマンドを使用します。デフォルト設定に戻すには、このコマンドの no 形式を使用します。

DHCP スヌーピングデータベースへのインタフェースの追加

DHCP Snooping Binding Database（DHCP スヌーピングバインディングデータベース）ページには、DHCP スヌーピングデータベースに IP アドレスをクエリしたり、追加したりするパラメーターがあります。

Binding Database（バインディングデータベース）ページを開くには、**Switch**（スイッチ）® **DHCP Snooping**（DHCP スヌーピング）® **Binding Database**（バインディングデータベース）の順にクリックします。

図 **7-19.** バインディングデーターベース



データベースへのクエリ

□□□ **Binding Database**（バインディングデータベース）ページを開きます。

□□□ 次の分類項目を選択します。

- **MAC Address**（MAC アドレス）— DHCP スヌーピングデータベースに記録された MAC アドレスを示します。
- **IP Address**（IP アドレス）— DHCP スヌーピングデータベースに記録された IP アドレスを示します。
- **VLAN** — DHCP スヌーピングデータベースに記録された VLAN を示します。
- **Interface**（インタフェース）— DHCP スヌーピングデータベースに記録されたインタフェースのリストを示します。可能なフィールド値は次のとおりです。Port（ポート）および LAG です。

上記のフィールドのほか、クエリ結果表には次のフィールドが表示されます。

- **VLAN ID** — DHCP スヌーピングデータベースで IP アドレスを追加する VLAN ID を表示します。

- **Type**（タイプ）— IP アドレスバインディングタイプを表示します。可能なフィールド値は、IP アドレスが静的に設定されたことを示す **Static**（静的）と、IP アドレスが動的に設定されたことを示す **Dynamic**（動的）です。
- **Lease Time**（リース時間）— リース時間を表示します。リース時間は、DHCP データベース内でエントリがアクティブである時間を定義します。リース時間の期限が切れたエントリは、スイッチに無視されます。

□□□ **Query**（クエリ）をクリックします。

データベースエントリの削除

□□□ **Binding Database**（バインディングデータベース）ページを開きます。

□□□ 表の **Remove**（削除）列で、目的のエントリの横にあるチェックボックスをオンにします。

□□□ **Apply Changes**（変更の適用）をクリックします。

動的データベースのクリア

□□□ **Binding Database**（バインディングデータベース）ページを開きます。

□□□ **Clear Dynamic**（動的クリア）をクリックします。

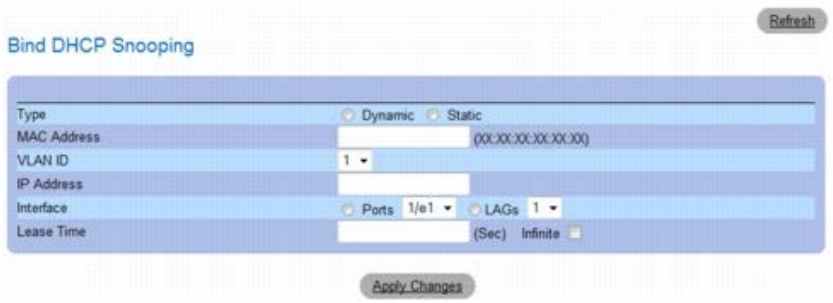
DHCP スヌーピングのバインディングデータベース

□□□ **Binding Database**（バインディングデータベース）ページを開きます。

□□□ **Add**（追加）をクリックします。

Bind DHCP Snooping（DHCP スヌーピングのバインド）ページが開きます。

図 **7-20. DHCP** スヌーピングのバインドページ



□□□ 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。

CLI コマンドを使用した **DHCP** スヌーピングバインディングデータベースの設定

次の表は、DHCP スヌーピングバインディングデータベースを設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
ip dhcp snooping binding *mac-address vlan-id ip-address* {ethernet *interface* | **port-channel** *port-channel-number*} expiry *seconds* **no ip dhcp snooping binding** *mac-address vlan-id*	DHCP スヌーピングバインディングデータベースを設定したり、バインディングエントリをデータベースに追加したりするには、**ip dhcp snooping binding** 特権 EXEC コマンドを使用します。バインディングデータベースからエントリを削除するには、このコマンドの no 形式を使用します。
clear ip dhcp snooping database	DHCP バインディングデータベースをクリアするには、**clear ip dhcp snooping database** 特権 EXEC コマンドを使用します。
show ip dhcp snooping binding [mac-address *mac-*	スイッチのすべてのインタフェースに関する、DHCP スヌーピングバインディングデータベースおよび

address] [ip-address *ip-address*] [vlan *vlan*] [ethernet *interface* | port-channel *port-channel-number*]	設定情報を表示するには、**show ip dhcp snooping binding** ユーザー EXEC コマンドを使用します。

次は、CLI コマンドの例です。

```
Console# show ip dhcp snooping binding

Update frequency: 1200

Total number of binding: 2
```

Mac Address	IP アドレス	Lease（sec）	Type	VLAN	Interface
----------	----------	----------	--------	--------	-------
0060.704C.73FF	10.1.8.1	7983	snooping	3	1/21
0060.704C.7BC1	10.1.8.2	92332	snooping	（s）3	1/22

ポートの設定

Ports（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のような高度な機能などのポート機能を設定したり、仮想ポートテスト実行したりできるリンクがあります。

Ports（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。

本項には、次のトピックがあります。

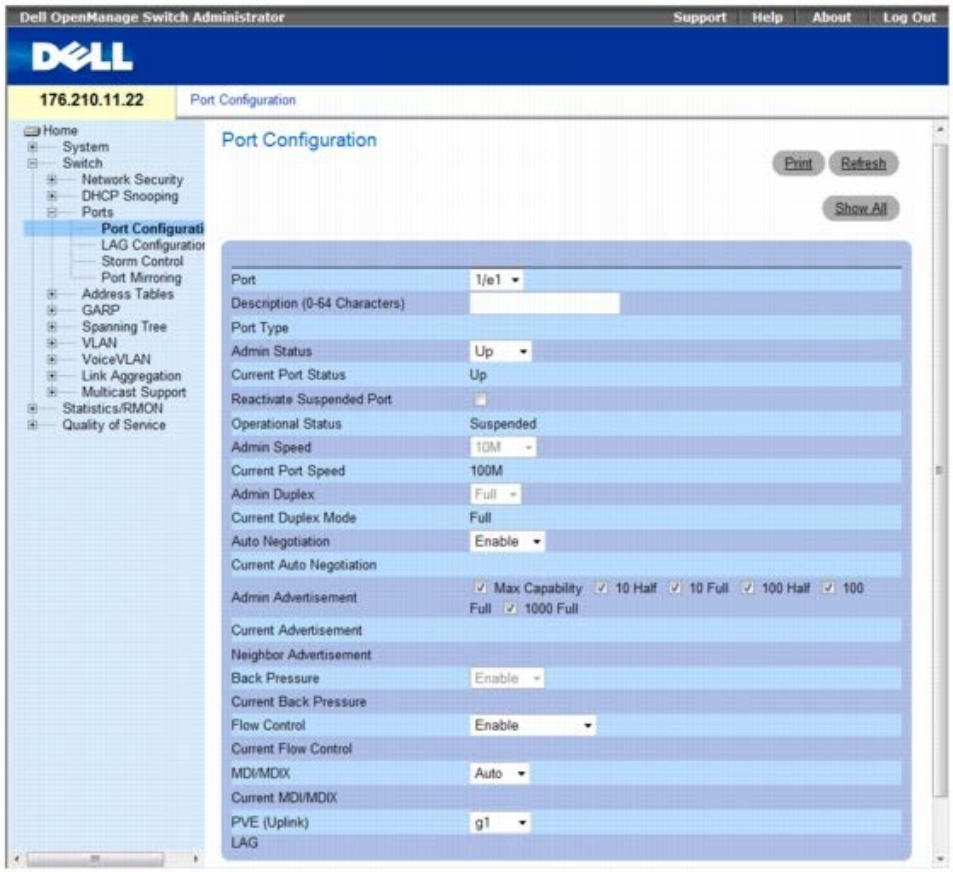
- ポートの設定の定義
- LAG パラメーターの定義
- ストーム制御の有効化
- ポートミラーリングセッションの定義

ポートの設定の定義

Port Configuration（ポートの設定）ページを使用すると、ポートパラメーターを定義できます。LAG メンバーであるポートの設定を変更した場合、その設定を有効にするには、ポートを LAG から削除する必要があります。

Port Configuration（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 **7-21.** ポートの設定



Port Configuration（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）— ポートパラメーターを定義するポートの番号です。
- **Description**（**0 - 64 Characters**） （説明（0～ 64 文字））— イーサネットなど、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）— 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。
  - **Up**（有効）— ポートを介したトラフィックを有効にします。
  - **Down**（ダウン）— ポートを介したトラフィックを無効にします。
- **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指定します。
- **Reactivate Suspended Port**（サスペンド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サスペンドになっている場合に、そのポートを再びアクティブにします。
  - **Checked**（チェックマークあり）— ポートを再びアクティブにします。
  - **Unchecked**（チェックマークなし）— ポートの動作ステータスを保持します。
- **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）— ポートはアクティブですが、トラフィックの送受信は現在行っていません。

  Active （アクティブ）— ポートは現在アクティブであり、トラフィックの送受信を行っています。

  Disable（無効）— ポートは無効であり、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速度です。ポートタイプによって、使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、ポーが無効になっている場合のみです。可能なフィールド値は次のとおりです。
  - **10M**— ポートが現在 10 Mbps で動作していることを示します。
  - **100M**— ポートが現在 100 Mbps で動作していることを示します。
  - **1000M**— ポートが現在 1000 Mbps で動作していることを示します。
- **Current Port Speed**（現在のポートスピード）— 実際に同期化されているポートスピード（bps）です。

- **Admin Duplex**（管理二重モード）— ポートの二重モードです（bps）。
  - **Full**（全二重）— デバイスとクライアントの両方向からの同時送信をインタフェースでサポートしていることを示します。
  - **Half**（半二重）— デバイスとクライアントの間で 1 度に一方向からの送信のみをインタフェースで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）— Auto Negotiation（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、一方のポートからその転送速度、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）の能力を他方に公示できるようにします。
  - **Enable**（有効）— ポートに対して Auto Negotiation（オートネゴシエイション）を有効にします。
  - **Disable**（無効）— ポートに対して Auto Negotiation（オートネゴシエイション）を無効にします。
- **Current Auto Negotiation**（現在のオートネゴシエイション）— 現在の Auto Negotiation（オートネゴシエイション）の設定です。
- **Admin Advertisement**（管理公示）— ポートが公示す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次のとおりです。
  - **Max Capability**（最大容量）— すべてのポートスピードおよび Duplex（二重）モードの設定が許可されます。
  - **10 Half**（10 Mbps 半二重）— ポートが 10 mbps のスピードポートと半二重モード設定を公示することを示します。
  - **10 Full**（10 Mbps 全二重）— ポートが 10 mbps のスピードポートと全二重モード設定を公示することを示します。
  - **100 Half**（100 Mbps 半二重）— ポートが 100 mbps のスピードポートと半二重モード設定を公示することを示します。
  - **100 Full**（100 Mbps 全二重）— ポートが 100 mbps のスピードポートと全二重モード設定を公示することを示します。
  - **1000 Full**（1000 Mbps 全二重）— ポートが 1000 mbps のスピードポートと全二重モード設定を公示することを示します。
- Current Advertisement（現在の公示）— ポートはネゴシエー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公示します。可能なフィールド値は、**Admin Advertisement**（管理公示）フィールドで指定した値です。
- Neighbor Advertisement（近隣公示）— 隣接ポートの公示設定を示します。フィールド値は、**Admin Advertisement**（管理公示）フィールド値と同じです。
- **Back Pressure**（バックプレッシャー）— Back Pressure（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。Back Pressure（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。
  - **Enable**（有効）— ポートに対して Back Pressure（バックプレッシャー）モードを有効にします。
  - **Disable**（無効効）— ポートに対して Back Pressure（バックプレッシャー）モードを無効にします。
- **Current Back Pressure**（現在のバックプレッシャー）— 現在の Back Pressure（バックプレッシャー）の設定です。
- **Flow Control**（フロー制御）— ポートのフロー制御ステータスを示します。
  - **Enable**（有効）— ポートに対してフロー制御を有効にします。
  - **Disable**（無効）— ポートに対してフロー制御を無効にします。
  - **Auto-negotiation**（オートネゴシエイション）— ポートの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 Flow Control（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、ストレートイーサネット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。Auto MDIX は、オートネゴシエイションが無効な場合、FE ポートでは機能しません。可能なフィールド値は以下のとおりです。
  - **Auto**（自動）— ケーブルのタイプを自動検出するために使用します。
  - **MDIX** — ハブおよびスイッチに使用します。
  - **MDI** — 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 設定です。可能なフィールド値は次のとおりです。
  - **MDI** — 現在の MDI 設定は MDI です。
  - **MDIX** — 現在の MDI 設定は MDIX です。
- **Private VLAN Edge**（**PVE**）（プライベート VLAN エッジ（PVE））— LAG が設定されるプライベート VLAN エッジ（PVE）グループです。PVE として定義されたポートは、アップリンクにより保護されるので、同じ VLAN 内の他のポートから隔離されます。アップリンクは GE ポートでなければなりません。
- **LAG** — ポートが LAG に属しているかどうかを示します。

LAG メンバーであるポートの設定を変更した場合、その設定を有効にするには、ポートを LAG から削除する必要があります。

ポートパラメーターの定義

□□□ **Port Configuration**（ポートの設定）ページを開きます。

□□□ **Ports**（ポート）フィールドでポートを選択します。

□□□ ダイアログで使用できる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。

ポートパラメーターがデバイスに保存されます。

複数のポート設定の表示および変更

□□□ **Port Configuration**（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。

Port Configuration Table（ポートの設定表）が開きます。

図 **7-22. Port Configuration Table**（ポートの設定表）

□□□ 関連するポートで使用できる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。

ポートパラメーターがデバイスに保存されます。

CLI コマンドを使用したポートの設定

次の表は、**Port Configuration**（ポートの設定）ページに表示されているように、ポートを設定するための等価 CLI コマンドをまとめたものです。

表 **7-12.** 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、イーサネットタイプのインタフェースを設定します。
description *string*	インタフェースの設定に説明を追加します。
shutdown	現在設定されているコンテキストの一部であるインタフェースを無効にします。
set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}	セキュリティ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、所定のイーサネット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、所定のイーサネット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 パラメーター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公示設定を表示します。
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。

CLI コマンドの例は次のようになります。

```
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	MdixMode
---	----	-----	-----	----	------	-----	------	----
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On

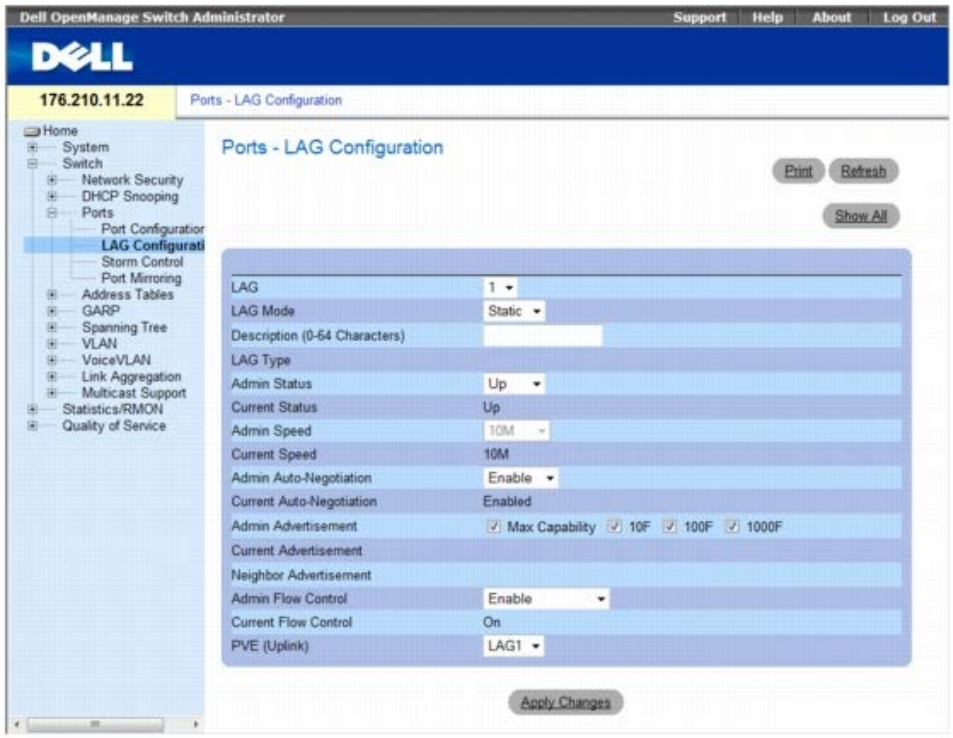
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	-----	-----	-----	-------	--------	------	
Ch1	1000	Full	1000	Off	Off	Disable	Up	

LAG パラメーターの定義

Ports - LAG Configuration（ポート - LAG の設定）ページには、設定済みの LAG に関するパラメーターを設定するためのフィールドがあります。デバイスは、システムごとに最大 15 の LAG をサポートします。リンクアグリゲーショングループ（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。

Ports - LAG Configuration（ポート - LAG の設定）ページを開くには、ツリー表示で、**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 **7-23.** ポート **- LAG** の設定



Ports - LAG Configuration（ポート - 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。
- **LAG Mode**（LAG モード）— LAG のタイプです。可能なフィールド値は次のとおりです。
  - **Static**（静的）— ポートは、ネットワーキングデバイス間における高速接続用の単一論理ポートで構成されます。
  - **LACP** — Link Aggregate Control Protocol です。LACP 対応 LAG は、他のリンクと情報を交換して、LAG の設定を自動的にアップデートおよび保守できます。
- **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。
  - **Up**（有効）— LAG を介したトラフィック転送を有効にします。
  - **Down**（無効）— LAG を介したトラフィック転送を無効にします。
- **Current Status**（現在のステータス）— LAG が現在動作しているかどうかを示します。
- **Admin Speed**（管理スピード）— LAG に対して設定された動作スピードです。可能なフィールド値は次のとおりです。
  - **10M**— LAG が現在 10 Mbps で動作していることを示します。
  - **100M**— LAG が現在 100 Mbps で動作していることを示します。
  - **1000M**— LAG が現在 1000 Mbps で動作していることを示します。
- **Current Speed**（現在のスピード）— LAG の現在の動作スピードです。
- **Admin Auto Negotiation**（管理オートネゴシエイション）— Auto Negotiation（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 からその転送速度、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）の能力を他方に公示できるようにします。
  - **Enable**（有効）— LAG に対して Auto Negotiation（オートネゴシエイション）を有効にします。
  - **Disable** —（無効）— LAG に対して Auto Negotiation（オートネゴシエイション）を無効にします。
- **Current Auto Negotiation**（現在のオートネゴシエイション）— 現在の Auto Negotiation（オートネゴシエイション）の設定です。
- **Admin Advertisement**（管理公示）— LAG が公示す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次のとおりです。
  - **Max Capability** —（最大容量）— すべての LAG スピードおよび Duplex（二重）モードの設定が許可されます。

- **10 Full**（10 Mbps 全二重）— LAG が 10 mbps のスピード LAG と全二重モード設定を公示することを示します。
- **100 Full**（100 Mbps 全二重）— LAG が 100 mbps のスピード LAG と全二重モード設定を公示することを示します。
- **1000 Full**（1000 Mbps 全二重）— LAG が 1000 mbps のスピード LAG と全二重モード設定を公示することを示します。

- **Current Advertisement**（現在の公示） — LAG はネゴシエーションプロセスを開始するために、隣接 LAG にそのスピードを公示します。可能なフィールド値は、**Admin Advertisement**（管理公示）フィールドで指定した値です。
- **Neighbor Advertisement**（近隣公示）— 隣接 LAG の公示設定を示します。フィールド値は、**Admin Advertisement**（管理公示）フィールド値と同じです。
- **Admin Flow Control**（管理フロー制御）— LAG のフロー制御ステータスを示します。フロー制御モードは、LAG において全二重モードで動作するポートで効果があります。
  - **Enable**（有効）— LAG に対してフロー制御を有効にします。
  - **Disable**（無効）— LAG に対してフロー制御を無効にします。
  - **Auto-negotiation**（オートネゴシエイション）— LAG の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 Flow Control（フロー制御）の設定です。
- **Private VLAN Edge**（**PVE**）（プライベート VLAN エッジ（PVE））— LAG が設定されているプライベート VLAN エッジ（PVE）グループです。PVE として定義されたポートは、アップリンクにより保護されるので、同じ VLAN 内の他のポートから隔離されます。アップリンクは、GE ポートまたは LAG でなければなりません。

LAG パラメーターの定義

□□□ **Ports - LAG Configuration**（ポート - 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 パラメーターがデバイスに保存されます。

LAG パラメーターの変更

□□□ **Ports - LAG Configuration**（ポート - 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 パラメーターがデバイスに保存されます。

複数の LAG 設定の表示および変更

□□□ **Ports - LAG Configuration**（ポート - 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。

次のような **LAG Configuration Table**（LAG 設定表）が開きます。

図 **7-24. LAG** 設定表

□□□ 関連する LAG で使用できる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 パラメーターがデバイスに保存されます。

CLI コマンドを使用した LAG の設定

次の表は、 **Ports - LAG Configuration**（ポート - LAG の設定）ページに表示されているように、LAG を設定するための等価 CLI コマンドをまとめたものです。

表 **7-13. 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*	インタフェースの設定に説明を追加します。
shutdown	現在設定されているコンテキストの一部であるインタフェースを無効にします。
speed *bps*	オートネゴシエイションを使用しない場合に、所定のイーサネットインタフェースのスピードを設定します。
negotiation [capability1 [capability2...capability5]	インタフェーススピード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。

CLI コマンドの例は次のようになります。

```
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、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ることによって発生します。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オーバーロードやネットワークのタイムアウトが発生します。

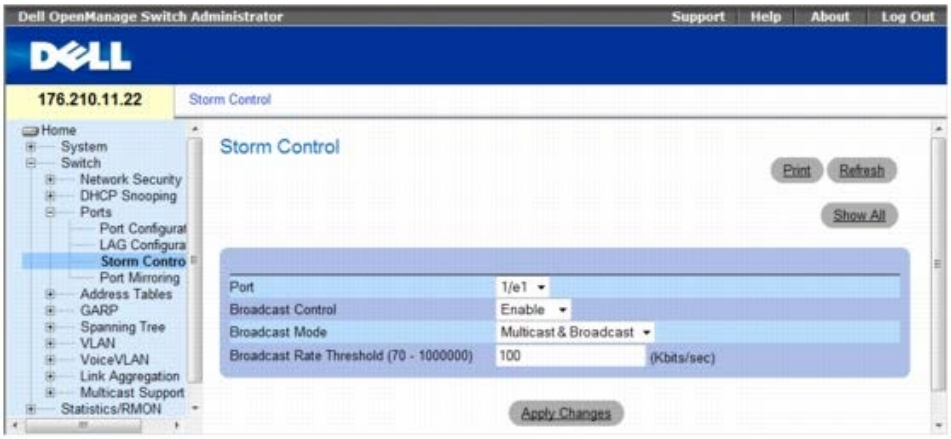
ストーム制御は、送信されるパケットのタイプおよび、パケットの転送速度を定義することによって、ポートごとに有効にできます。

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。

Storm Control（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。

Storm ControlStorm Control（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 **7-25.** ストーム制御



Storm Control（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でのブロードキャストパケットの転送を有効または無効にします。
  - **Enable**（有効）— ブロードキャストパケットタイプの転送を有効にします。
  - **Disable**（無効）— ブロードキャストパケットタイプの転送を無効にします。
- **Broadcast Mode**（ブロードキャストモード）— デバイスまたはスタックで現在有効にされているブロードキャストモードを指定します。可能なフィールド値は次のとおりです。
  - **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トラフィックを一緒にカウントします。
  - **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カウントします。
- **Broadcast Rate Threshold**（**70-1000000**）（ブロードキャストレートしきい値（70～1000000）— 未知のパケットが転送される最大レート（キロビット / 秒）です。このフィールドの範囲は、70～1,000,000 Kbps です。

ストーム制御の有効化

□□□ **Storm Control**（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ーの変更

□□□ **Storm Control**（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。

ストームコントロールのポートパラメーターがデバイスに保存されます。

ポートパラメーター表の表示

□□□ **Storm Control**（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。

Storm Control Settings Table（ストーム制御の設定表）が開きます。

図 **7-26.** ストーム制御の設定表

Storm Control（ストーム制御）ページのフィールドのほかに、**Storm Control Settings Table**（ストーム制御の設定表）には、次の追加フィールドがあります。

- **Unit No.**（ユニット番号）— ストーム制御情報が表示されるスタッキングメンバーを示します。
- **Copy Parameters from Port**（ポートからのパラメーターのコピー）— Storm Control（ストーム制御）パラメーターがコピーされる特定のポートを示します。
- **Copy To** （コピー先）— 選択されたポートに Storm Control（ストーム制御）パラメーターをコピーします。

ストーム制御の設定表のパラメーターのコピー

□□□ **Storm Control**（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。

Storm Control Settings Table（ストーム制御の設定表）が開きます。

□□□ **Copy Parameters from Port** （ポートからのパラメーターのコピー）フィールドから設定がコピーされるポートを選択します。

□□□ **Copy to**（コピー先）チェックボックスをオンにして、ストーム制御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。

パラメーターが、**Storm Control Settings Table**（ストーム制御の設定表）で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**Storm Control**（ストーム制御）ページの表示に表示されているように、ストーム制御を設定するための等価 CLI コマンドをまとめたものです。

表 **7-14.** 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、マルチキャストパケット、ユニキャストパケットおよびブロードキャストパケットを一緒にカウント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コントロールを有効にします。
`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。

CLI コマンドの例は次のようになります。

```
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は次のことを行います。

- 着信パケットおよび発信パケットのコピーをあるポートからモニタ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モニタとミラーリングを行います。
- 診断ツールおよび、デバッグ機能として使用できます。
- デバイスパフォーマンスおよびモニタリングを有効にします。

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各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、着信パケットおよび発信パケットのコピーを、モニタ対象のポートからモニタ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モニターとミラーリングを行います。
- モニタ対象のポートは、モニタリングポートよりも速く動作できません。
- 同一ポートへのすべての RX/TX パケットがモニタされます。

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 の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。

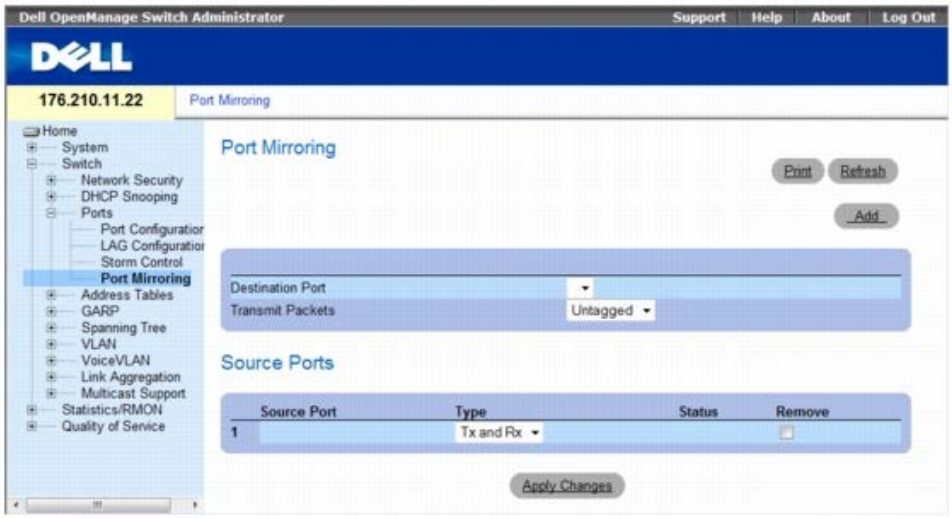
送信元ポートとして設定されるポートには、次の制限が適用されます。

- 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。
- このデバイスでミラーリングによりサポートされるポートは 4 つです。

Port Mirroring（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。

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 **7-27.** ポートミラーリング



Port Mirroring（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**（転送パケット）— パケットがどのようにミラーリングされるかを定義します。可能なフィールド値は次のとおりです。
  - **Untagged**（タグなし）— パケットをタグなし 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になっています。
  - **Tagged**（タグ付き）— パケットをタグ付き VLAN パケットとしてミラーリングします。

送信元ポート

- **Source Port**（送信元ポート）— ポートトラフィックをミラーリングするポートの番号を定義します。
- **Type**（タイプ）— ミラーリングするポートが RX か TX、または RX および TX の両方であるかを示します。可能なフィールド値は次のとおりです。
  - **RxOnly**（RX のみ）— 受信側ポートでポートミラーリングを定義します。これがデフォルト値になっています。
  - **TxOnly**（Tx のみ）— 転送側ポートでポートミラーリングを定義します。
  - **Tx and Rx**（Tx および Rx）— 受信側と送信側の両方のポートでポートミラーリングを定義します。
- **Status**（ステータス）— ポートが現在モニタされているか（**Active**（アクティブ））、モニタされていないか（**Ready**（モニタ可能））を示します。
- **Remove**（削除）— ポートミラーリングセッションを削除します。可能なフィールド値は次のとおりです。
  - **Checked**（チェックマークあり）— 選択されたポートミラーリングセッションを削除します。
  - **Unchecked**（チェックマークなし）— ポートミラーリングセッションを保持します。

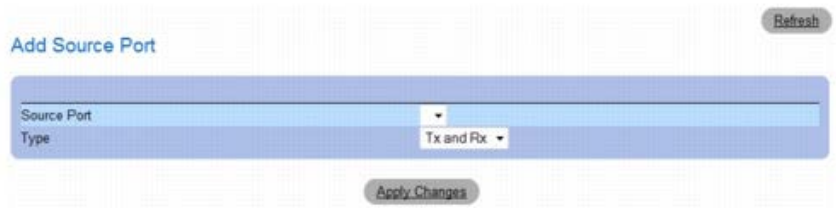
ポートミラーリングセッションの追加

□□□ **Port Mirroring**（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。

Add Source Port（送信元ポートの追加）ページが開きます。

図 **7-28. Add Source Port**（送信元ポートの追加）



□□□ **Source Port**（送信元ポート）および **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。

コピーしたポートをポートミラーリングセッションから削除する

□□□ **Port Mirroring**（ポートミラーリング）ページを開きます。

□□□ Source Ports table（送信元ポート表）で、ポートの **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

Port Mirroring（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ための等価 CLI コマンドをまとめたものです。

表 **7-15.** 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**]	ポートミラーリングセッションを開始します。

CLI コマンドの例は次のようになります。

```
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 アドレス別にソートできます。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。アドレスは、フレームの送信元アドレスから学習することによって、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。

Address Tables（アドレス表）ページを開くには、ツリー表示で、**Switch**（スイッチ）® **Address Tables**（アドレス表）の順に選択します。

本項には、次のトピックがあります。

静的アドレスの定義

Static MAC Address（静的 MAC アドレス）ページには、静的 MAC アドレスのリストがあります。**Static MAC Address**（静的 MAC アドレス）ページでは静的アドレスの追加や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。

Static MAC Address（静的 MAC アドレス）ページを開くには、ツリー表示で、**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 **7-29.** 静的 **MAC** アドレス

Static MAC Address（静的 MAC アドレス）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リストに登録されている MAC アドレスです。
- **VLAN ID** — MAC アドレス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。可能な値は次のとおりです。
  - **Secure**（送信元）— ロックされたポートに対する静的 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。

イーサネットデバイスのリセット時に静的 MAC アドレスが削除されるのを防ぐには、そのMAC アドレスに接続されているポートを必ずロックしてください。

- **Remove**（削除）— 選択された MAC アドレスを **Static MAC Address Table**（静的 MAC アドレス表）から削除します。可能なフィールド値は次のとおりです。
  - **Checked**（チェックマークあり）— 選択された MAC アドレスを削除します。
  - **Unchecked**（チェックマークなし）— 選択された MAC アドレスを保持します。

静的 **MAC** アドレスの追加

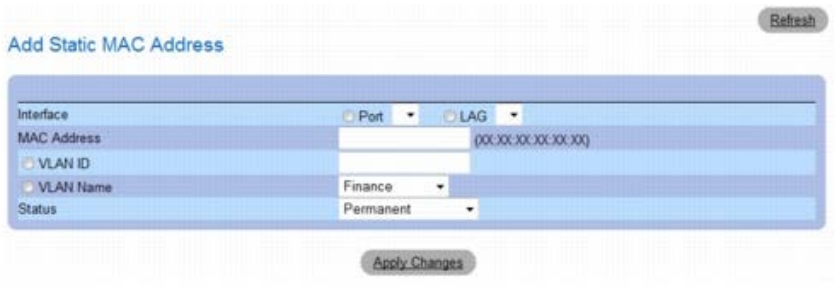
□□□ **Static MAC Address**（静的 MAC アドレス）ページを開きます。_

□□□ **Add**

（追加）をクリックします。

Add Static MAC Address（静的 MAC アドレスの追加）ページが開きます。

図 **7-30.** 静的 **MAC** アドレスの追加



□□□ 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。

新規の静的アドレスが **Static MAC Address**（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

□□□ **Static MAC Address**（静的 MAC アドレス）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 **MAC** アドレス表にある静的アドレスの削除

□□□ **Static MAC Address**（静的 MAC アドレス）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。

Static MAC Address Table（静的 MAC アドレス表）が開きます。

図 **7-31.** 静的 **MAC** アドレス表

□□□ 表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。

静的 MAC 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ーの設定

次の表は **Static MAC Address**（静的 MAC アドレス）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ーを設定するための等価 CLI コマンドをまとめたものです。

表 **7-16.** 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*}	MAC 層の静的な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内のエントリを表示します。

CLI コマンドの例は次のようになります。

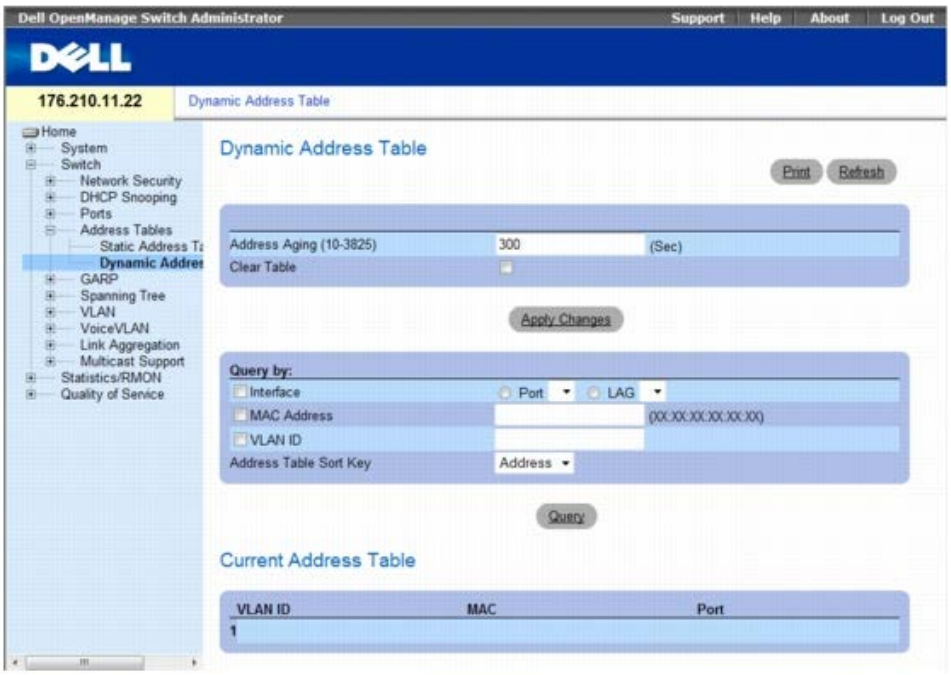
```
console(config-if)#bridge address 00:60:70:4C:73:FF permanent ethernet g8

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

Dynamic Address Table（動的アドレス表）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フィールドをクエリするためのフィールドがあります。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。**Dynamic Address Table**（動的アドレス表）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、動的アドレスリストをクエリおよび表示するためのパラメーターがあります。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する動的アドレスパラメーターが含まれています。

Dynamic Address Table（動的アドレス表）ページを開くには、ツリー表示で、**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 **7-32.** 動的アドレス表



Dynamic Address Table（動的アドレス表）ページには、以下のフィールドがあります。

- **Address Aging**（**10-3825**） （アドレスのエージング（10～3825））— 送信元からのトラフィックが検出されない場合にタイムアウトになるまでに、MAC アドレスが **Dynamic Address Table**（動的アドレス表）に保持される時間を指定します。デフォルト値は 300 秒です。
- **Clear Table**（表のクリア）— Dynamic Address table（動的アドレス表）をクリアします。
  - **Checked**（チェックマークあり）— Dynamic Address table（動的アドレス表）をクリアします。

- **Unchecked**（チェックマークなし）— Dynamic Address table（動的アドレス表）を保持します。

Query By（クエリ基準）

Query By（クエリ基準）セクションで、Dynamic Addresses Table（動的アドレス表）のソート基準オプションを選択します。

- **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 を指定します。
- **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、インタフェース別にソートできます。

エージング時間の再定義

□□□ **Dynamic Address Table**（動的アドレス表）を開きます。

□□□ **Address Aging**（アドレスのエージング）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

□□□ **Dynamic Address Table**（動的アドレス表）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ーを定義します。

エントリは、**Ports**（ポート）、**MAC Address**（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。

Dynamic Address Table（動的アドレス表）がクエリされ、結果が表示されます。

動的アドレス表のソート

□□□ **Dynamic Address Table**（動的アドレス表）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から、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。

Dynamic Address Table（動的アドレス表）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およびソート

次の表は、 **Dynamic Address Table**（動的アドレス表）に表示されているように、動的アドレスをエージング、クエリおよびソートする場合の等価 CLI コマンドをまとめたものです。

表 **7-17.** 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。

CLI コマンドの例は次のようになります。

```
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

Generic Attribute Registration Protocol（GARP）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 または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デバイスのセットを定義します。

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 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 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。

本項には、次のトピックがあります。

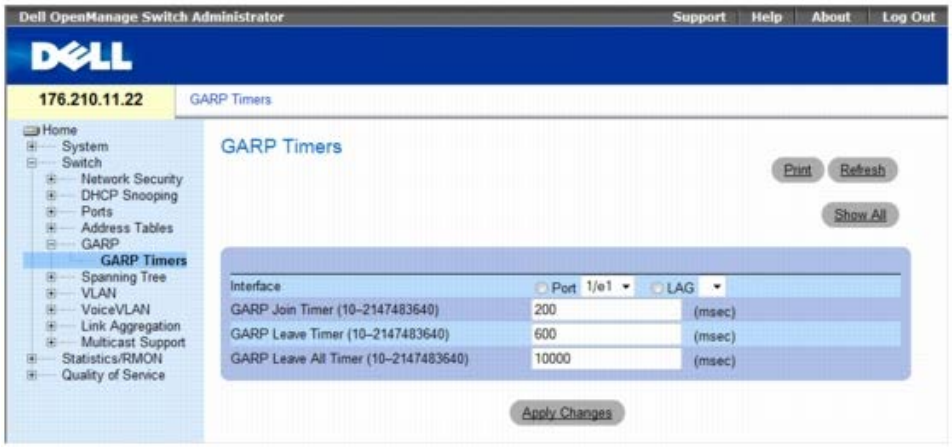
- GARP タイマーの定義

GARP タイマーの定義

GARP Timers（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 Timers（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 **7-33. GARP** タイマー



GARP Timers（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）— ポートに対して有効にするか、LAG に対して有効にするかを決定します。
- **GARP Join Timer**（**10 - 2147483640**） （GARP タイマー（10～2147483640））— Protocol Data Units（PDU）の転送時間（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**） （GARP Leave タイマー（10 ～ 2147483640））— デバイスが GARP 状態から離れる前に待機する時間

（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）**（GARP Leave All タイマー（10 ～ 2147483640））— すべてのデバイスが GARP 状態を離れる前に待機する時間（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 Timers**（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。

□□□ フィールドを完成させます。

□□□ **Apply Changes**（変更の適用）をクリックします。

GARP パラメーターがデバイスに保存されます。

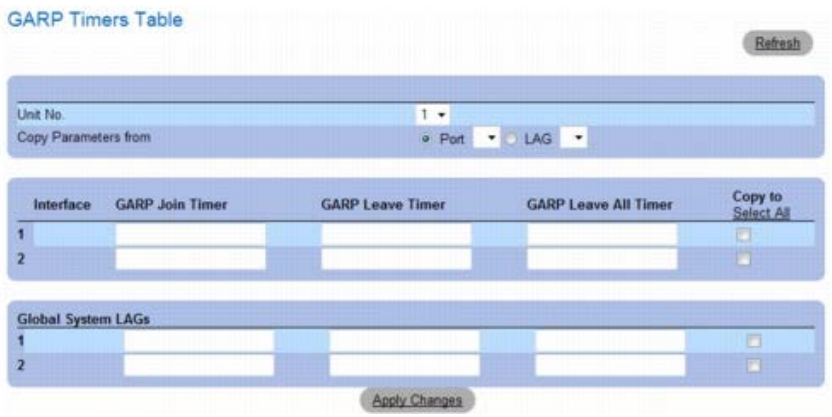
GARP タイマー表へのパラメーターのコピー

□□□ **GARP Timers**（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。

図 **7-34. GARP** タイマー表



□□□ **Copy Parameters from**（パラメーターのコピー元）フィールドのインタフェースを **Port**（ポート）または **LAG** のいずれかのドロップダウンメニューから選択します。

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 4 を参照してください。

□□□ **Copy to**（コピー先）チェックボックスを選択して、GARP タイマーの定義（**Copy Parameters from**（パラメーターのコピー元）フィールドからコピー）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。

パラメーターが、**GARP Timers Table**（GARP タイマー表）で選択されたポートまたは 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

GARP Timers（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ための等価 CLI コマンドをまとめたものです。

表 **7-18. 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 Leave All 値を調整します。

CLI コマンドの例は次のようになります。

```
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 Join	（milliseconds） 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、STP は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ます。

- **Classic STP**（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 の設定の詳細に関しては、**STP** グローバル設定の定義 を参照してください。
- **Rapid STP**（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。RSTP がデバイスで有効になっているが、隣接するデバイスでは STP が有効な場合、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定義 を参照してください。
- **Multiple STP**（多重 STP）— 任意の VLAN に割り当てられるパケットに対して完全な接続性を提供します。多重 STP は RSTP に基づいています。また、多重 STP は、異なる MST リージョンを介して異なる VLAN に割り当てられるパケットを転送します。MST は、MSTP がデバイスで有効にされている場合、単一ブリッジとして機能します。ただし、隣接するデバイスで RSTP が有効になっていて、ローカルデバイスが STP、RSTP および MSTP を使用している場合、これら両方のデバイスは、相互運用ができます。

  多重 STP の詳細については、多重スパニングツリーの設定 を参照してください。

Spanning Tree（スパニングツリー）ページを開くには、ツリー表示で、**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。

本項には、次のトピックがあります。

- STP グローバル設定の定義
- STP ポートの設定の定義
- STP LAG 設定の定義
- 高速スパニングツリーの定義
- 多重スパニングツリーの設定
- MSTP インタフェース設定の定義

STP グローバル設定の定義

Spanning Tree Global Settings（スパニングツリーグローバル設定）ページには、デバイスに対して STP を有効にするパラメーターが含まれています。

Spanning Tree Global Settings（スパニングツリーグローバル設定）ページを開くには、ツリー表示で、**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 **7-35.** スパニングツリーグローバル設定

Spanning Tree Global Settings（スパニングツリーグローバル設定）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）— デバイスに対してスパニングツリーを有効または無効にします。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— スパニングツリーを有効にします。
  - **Disable**（無効）— スパニングツリーを無効にします。
- **STP Operation Mode**（STP 動作モード）— デバイスに対して有効な STP のモードです。可能なフィールド値は次のとおりです。
  - **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になっています。
  - **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、Bridge Protocol Data Unit（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次のとおりです。
  - **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になっています。
  - **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**（パスコストデフォルト値）— デフォルトパスコストを STP ポートに割り当てるときに使用される方法を指定します。可能なフィールド値は次のとおりです。
  - **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になっています。
  - **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られるデフォルトパスコストは、選択された方法により異なります。

Interface	Long	Short
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19

10 Mbps	2,000,000	100

ブリッジの設定

- **Priority**（**0-61440 in steps of 4096**）（優先度（0～61440、増分 4096））— 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、優先度の最も低いデバイス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 のように 4096 単位で指定します。
- **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前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。転送ディレイ時間は、ブリッジがパケットを転送する前にリスニング状態およびラーニング状態でいる秒単位の時間です。デフォルト値は 15 秒です。

指定されたルート

- **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を示します。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ブリッジへのパスコストです。
- **Topology Changes Counts**（トポロジ変更カウント）— STP 状態が変化した合計回数を示します。
- **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、たとえば、2D/5H/10M/4S のように、D/H/M/S の書式で表示されます。

STP グローバルパラメーターの定義

□□□ 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）選択します。

□□□ **STP Operation Mode**（STP 動作モード）フィールドで **STP** 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。

STP がデバイスで有効になります。

STP グローバルパラメーターの変更

□□□ 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 パラメーターが変更され、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ーの定義

次の表は、Spanning Tree Global Settings（スピニングツリーグローバル設定）ページ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ーを定義するための CLI コマンドをまとめたものです。

表 **7-19. STP** グローバルパラメーターに関連する **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-ageseconds	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-timeseconds	スパニングツリーブリッジの転送時間を設定します。転送時間は、ポートが転送状態に入る前にリスニング状態およびラーニング状態でいる時間です。
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。
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。

CLI コマンドの例は次のようになります。

```
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 15 sec Forward Delay 20 sec

Bridge ID Priority                       32768
           Address                       00:00:00:16:00:64
           Max hops                      20
Name       Status     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
```

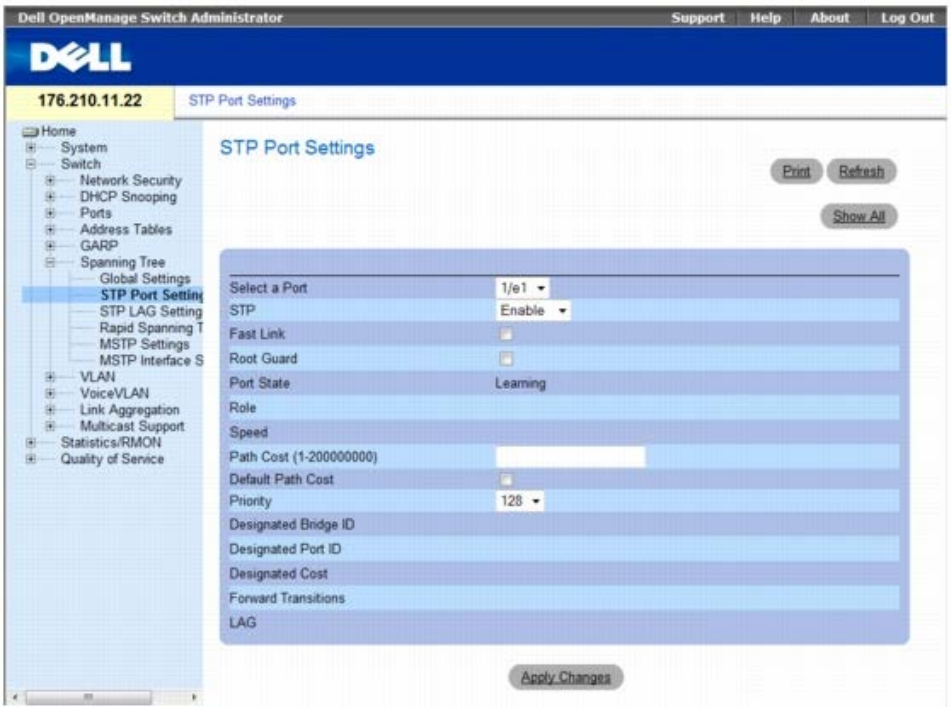
console# show spanning-tree active							
Spanning tree enabled mode MSTP							
Default port cost method: short							
Gathering information							
###### MST 0 Vlans Mapped: 16-4094							
CST Root ID Priority 20480							
	Address		00:30:ab:00:00:08				
	Path Cost		4				
	Root Port		ch2				
	This switch is the IST master						
	Hello Time 2 sec Max Age 15 sec Forward Delay 20 sec						
Bridge ID Priority				32768			
	Address		00:00:00:16:00:64				
	Max hops		20				
Name	Status	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 ポートの設定の定義

STP Port Settings（STP ポートの設定）ページを使用すると、STP プロパティを個々のポートに割り当てることができます。

STP Port Settings （STP 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）® **Spanning Tree**（スパニングツリー）® **Port Settings**（ポートの設定）の順にクリックします。

図 **7-36. STP** ポートの設定



STP Port Settings（STP ポートの設定）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 設定を変更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。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— ポート上で STP が有効になっていることを示します。
  - **Disable**（無効） — ポート上で STP が無効になっていることを示します。
- **Fast Link**（高速リンク）— 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 **Port State**（ポート状態）が自動的に **Forwarding**（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 30～60 秒かかる場合があります。可能な値は以下のとおりです。
  - **Checked**（チェックマークあり）— 高速リンクを有効にします。
  - **Unchecked**（チェックマークなし）— 高速リンクを無効にします。
- **Root Guard**（ルートガード）— ネットワークコアの外側にあるデバイスにスパニングツリールートを割り当てないようにします。
  - **Checked**（チェックマークあり）— ポートに対してルートガードを有効にします。
  - **Unchecked**（チェックマークなし）— ポートに対してルートガードを無効にします。
- **Port State**（ポートの状態）— ポート現在の 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確定します。可能なポート状態は次のとおりです。
  - **Disabled**（無効）— ポート上で STP が現在無効にされています。MAC アドレスを学習中に、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**（ラーニング）— ポートは現在ラーニングモードに入っていて、トラフィックを転送するはできませんが、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 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次のとおりです。
  - **Root**（ルート）— ルートスイッチにパケットを転送するための最低コストのパスを提供します。
  - **Designated**（指定）— 指定のスイッチが LAN に接続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示します。バックアップポートは、ポイントツーポイントリンクによってループ内で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関与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、パスがリルート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**（デフォルトパスコスト）— デバイスがデフォルトパスコストを使用するかどうかを示します。可能なフィールド値は次のとおりです。
  - **Checked**（チェックマークあり）— デバイスは、デフォルトパスコストを使用します。
  - **Unchecked**（チェックマークなし）— デバイスは、上記の Path Cost（パスコスト）フィールドで定義されたパスコストを使用します。
- **Priority**（優先度）— 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 増分で指定します。
- **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 トポロジに参加してい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**（転送の移行）— ポートの状態が **Forwarding**（転送）から **Blocking**（ブロッキング）に移行した回数です。
- **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

□□□ Spanning Tree **Port Settings**（スパニングツリーポート設定）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）、**Root Guard**（ルートガード）、**Path Cost**（パスコスト）、**Default Path Cost**（デフォルトパスコスト）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

□□□ Spanning Tree Port Settings（スパニングツリーポート設定）ページを開きます。

□□□ ポートを選択します。

□□□ 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。

STP ポートパラメーターが変更され、デバイスがアップデートされます。

STP ポート表の表示

□□□ Spanning Tree Port Settings（スパニングツリーポート設定）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 Port Table（STP ポート表）が開きます。

図 **7-37. STP** ポート表

CLI コマンドを使用した **STP** ポート設定の定義

次の表は、**STP Port Settings**（STP ポートの設定）ページに表示されているように、STP ポートパラメーターを定義するための等価 CLI コマンドをまとめたものです。

表 **7-20. 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	スパニングツリーコストに対するポー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	Fast Link（高速リンク）モードを有効にします。

spanning-tree guard root	インタフェースにおけるすべてのスパニングツリーインスタンスに対して、ルートガ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。

CLI コマンドの例は次のようになります。

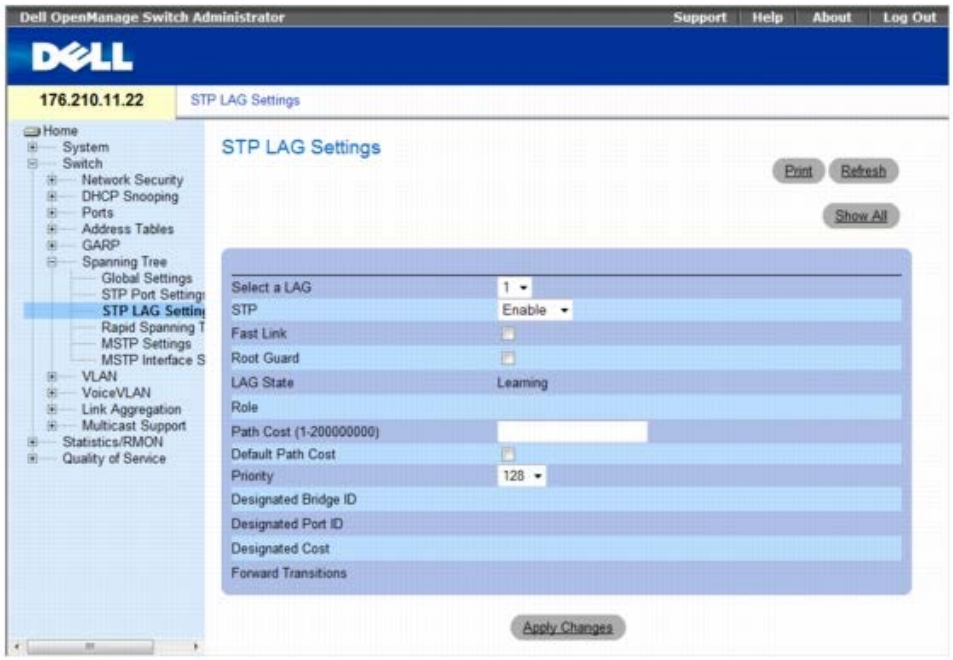
```
console> enable
console# configure
Console(config)# interface ethernet 1/e1
Console(config-if)# spanning-tree disable
Console(config-if)# spanning-tree cost 35000
Console(config-if)# spanning-tree port-priority 96
Console(config-if)# spanning-tree portfast
Console(config-if)# exit
Console(config)# exit
Console# show spanning-tree ethernet 1/e15
Port 1/e15 enabled                                  Role: designated
State: forwarding                                   Port cost: 19
Port id: 128.15
Type: PowerConnect 5324 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                                  Role: alternate
State: discarding                                   Port cost: 19
Port id: 128.15
Type: PowerConnect 5324 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

STP LAG Settings（STP LAG の設定）ページを使用すると、STP ポート集約パラメーターを割り当てることができます。

STP LAG Settings（STP 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 設定）の順にクリックします。

図 **7-38. STP STP LAG** の設定



Spanning Tree LAG Settings（スパニングツリー LAG 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。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— LAG 上で STP が有効になっていることを示します。
  - **Disable**（無効） — LAG 上で STP が無効になっていることを示します。
- **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 30～60 秒かかる場合があります。可能な値は以下のとおりです。
  - **Checked**（チェックマークあり）— 高速リンクを有効にします。
  - **Unchecked**（チェックマークなし）— 高速リンクを無効にします。
- **Root Guard**（ルールガード）— ネットワークコアの外側にあるデバイスにスパニングツリールートを割り当てないようにします。
  - **Checked**（チェックマークあり）— ポートに対してルートガードを有効にします。
  - **Unchecked**（チェックマークなし）— ポートに対してルートガードを無効にします。
- **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置が確定します。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 状態は次のとおりです。
  - **Disabled**（無効）— LAG 上で STP が現在無効にされています。MAC アドレスを学習中に、トラフィックを転送します。
  - **Blocking**（ブロッキング）— LAG は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 破棄ステータス）— この状態の場合、ポートは、MAC アドレスを学習せず、フレームを転送しません。
  - これは、STP（802.1.D）で導入された、Blocking（ブロッキング）と Listening（リスニング）状態を合わせた状態です。
  - **Listening**（リスニング）— LAG はリスニングモードにあり、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**（ラーニング）— LAG はラーニングモードにあり、トラフィックは転送できませんが、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あり、トラフィックの転送も新規の MAC アドレスの学習も可能です。
  - **Broken**（故障）— LAG は現在機能しておらず、トラフィックの転送に使用できません。
- **Role** （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る LAG の役割を示します。可能なフィールド値は次のとおりです。
  - **Root**（ルート）— ルートスイッチにパケットを転送するための最低コストのパスを提供します。
  - **Designated**（指定）— 指定のスイッチが LAN に接続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、ポイントツーポイントリンクによってループ内で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関与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です。パスコストの値を大きく、または小さくして、パスがリルートされるときにトラフィックの転送に使用されるようにします。パスコストの値は、1〜200000000 です。
- **Default Path Cost**（デフォルトパスコスト）— デバイスがデフォルトパスコストを使用するかどうかを示します。可能なフィールド値は次のとおりです。
  - **Checked**（チェックマークあり）— デバイスは、デフォルトパスコストを使用します。
  - **Unchecked**（チェックマークなし）— デバイスは、上記の Path Cost（パスコスト）フィールドで定義されたパスコストを使用します。
- **Priority**（優先度）— 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、優先度値が LAG の選択に影響します。優先度値の範囲は 0〜240 で、16 増分で指定します。
- **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）— 選択されたインタフェースの ID です。
- **Designated Cost**（指定コスト）— STP トポロジに参加してい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 State**（LAG 状態）が **Forwarding**（転送）状態から **Blocking**（ブロッキング）状態に変化した回数です。

STP LAG パラメーターの変更

□□□ **Spanning Tree LAG Settings**（スパニングツリー LAG 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 パラメーターが変更され、デバイスがアップデートされます。

STP LAG 表の表示

□□□ **STP LAG Settings**（STP 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。

STP LAG Table（STP LAG 表）が開きます。

図 **7-39. STP LAG** 表

CLI コマンドを使用した STP LAG 設定の定義

次の表は STP LAG の設定を定義する場合の CLI コマンドを示したものです。

表 **7-21. 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 guard root	インタフェースにおけるすべてのスパニングツリーインスタンスに対して、ルートガードを有効にします。
`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。

CLI コマンドの例は次のようになります。

```
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
```

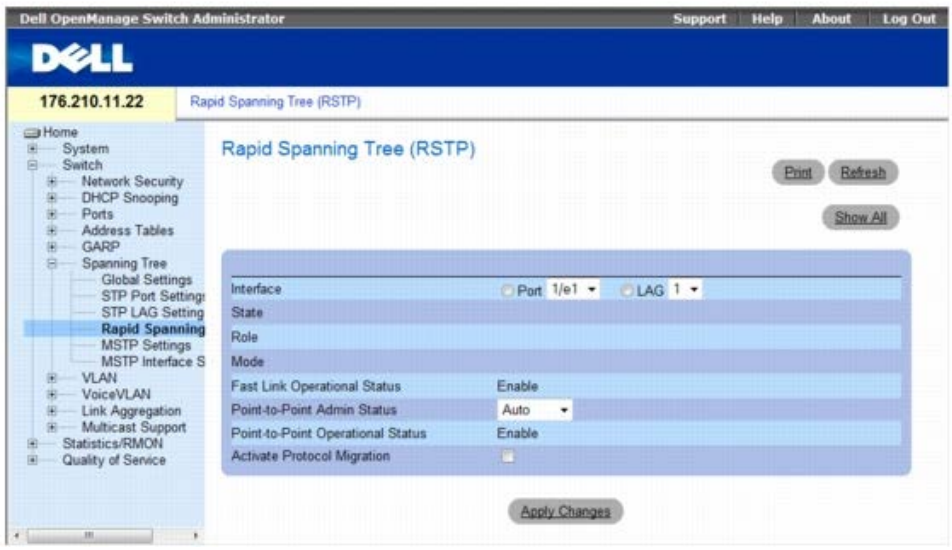
高速スパニングツリーの定義

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 2 転送ループが防止されますが、収束に 30～60 秒かかる場合があります。このディレイにより、ループの可能性を検出し、ステータスの変化を伝える時間が提供されます。

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。

Rapid Spanning Tree（RSTP）（高速スパニングツリー（RSTP））設定ページを開くには、ツリー表示で、**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 **7-40.** 高速スパニングツリー（**RSTP**）



Spanning Tree RSTP（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 設定を表示および編集できるポートまたは LAG です。
- **State**（状態）— 選択されたインタフェースの RSTP 状態を無効にします。
- **Role**（役割）— STP パスに提供するために 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次のとおりです。
  - **Root**（ルート）— ルートスイッチにパケットを転送するための最低コストのパスを提供します。
  - **Designated**（指定）— 指定のスイッチが LAN に接続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、ポイントツーポイントリンクによってループ内で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関与していないことを示します。

- **Mode**（モード）— 現在の Spanning Tree（スパニングツリー）モードを示します。Spanning Tree（スパニングツリー）モードは、**Spanning Tree Global Settings**（スパニングツリーグローバル設定）ページで選択されます。可能なフィールド値は次のとおりです。
  - **Classic STP**（標準 STP）— デバイスに対して標準 STP が有効になっていることを示します。
  - **Rapid STP**（高速 STP）— デバイスに対して高速 STP が有効になっていることを示します。
  - **Multiple STP**（多重 STP）— デバイスに対して多重 STP が有効になっていることを示します。
- **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。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— 高速リンクを有効にします。
  - **Disable**（無効）— 高速リンクを無効にします。
  - **Auto**（自動）— インタフェースがアクティブになった数秒後に、Fast Link（高速リンク）モードが有効になります。
- **Point-to-Point Admin Status**（ポイントツーポイント管理ステータス）— ポイントツーポイントリンクが確立されているかどうか、または、ポイントツーポイントリンクの確立をデバイスに対して許可します。可能なフィールド値は次のとおりです。
  - **Enable**（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。LCP または NCP パケットが明示的にリンクを閉じるか、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。これは、実際のスイッチポートのリンクタイプです。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。
  - **Disable**（無効）— ポイントツーポイントリンクを無効にします。
  - **Auto**（自動）— デバイスは、ポイントツーポイントリンクを自動的に確立します。
- **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）— データリンクの設定およびテストをするために、PPP が Link Control Protocol（LCP）パケットを送信できるようにします。可能なフィールド値は次のとおりです。
  - **Checked**（チェックマークあり）— プロトコルマイグレーションは有効です。
  - **Unchecked**（チェックマークなし）— プロトコルマイグレーションは無効です。

RSTP パラメーターの定義

□□□ Spanning Tree RSTP Settings（スパニングツリー RSTP 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 パラメーターが定義され、デバイスがアップデートされます。

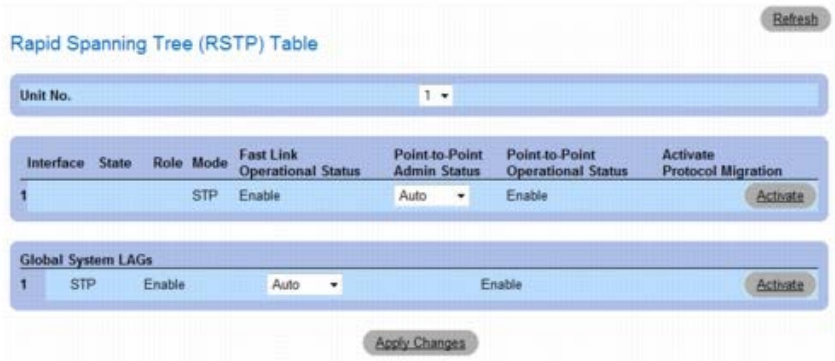
高速スパニングツリー（RSTP）表の表示

□□□ 高速スパニングツリー（RSTP：Rapid Spanning Tree）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Rapid Spanning Tree（**RSTP**） **Table**（高速スパニングツリー（RSTP）表）が開きます。

図 **7-41.** 高速スパニングツリー（**RSTP**）表



CLI コマンドを使用した高速 STP パラメーターの定義

次の表は、**Rapid Spanning Tree**（**RSTP**）（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 パラメーターを定義するための等価 CLI コマンドをまとめたものです。

表 **7-22. RSTP** の設定に関連する **CLI** コマンド

CLI コマンド	説明
spanning-tree link-type {point-to-point | shared}	デフォルトの link-type 設定をオーバーライドします。
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*]	プロトコルマイグレーション処理を再スタートします。
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。

CLI コマンドの例は次のようになります。

```
console(config)# interface ethernet 1/e5
console(config-if)# spanning-tree link-type shared
console(config-if)# spanning tree mode rstp
```

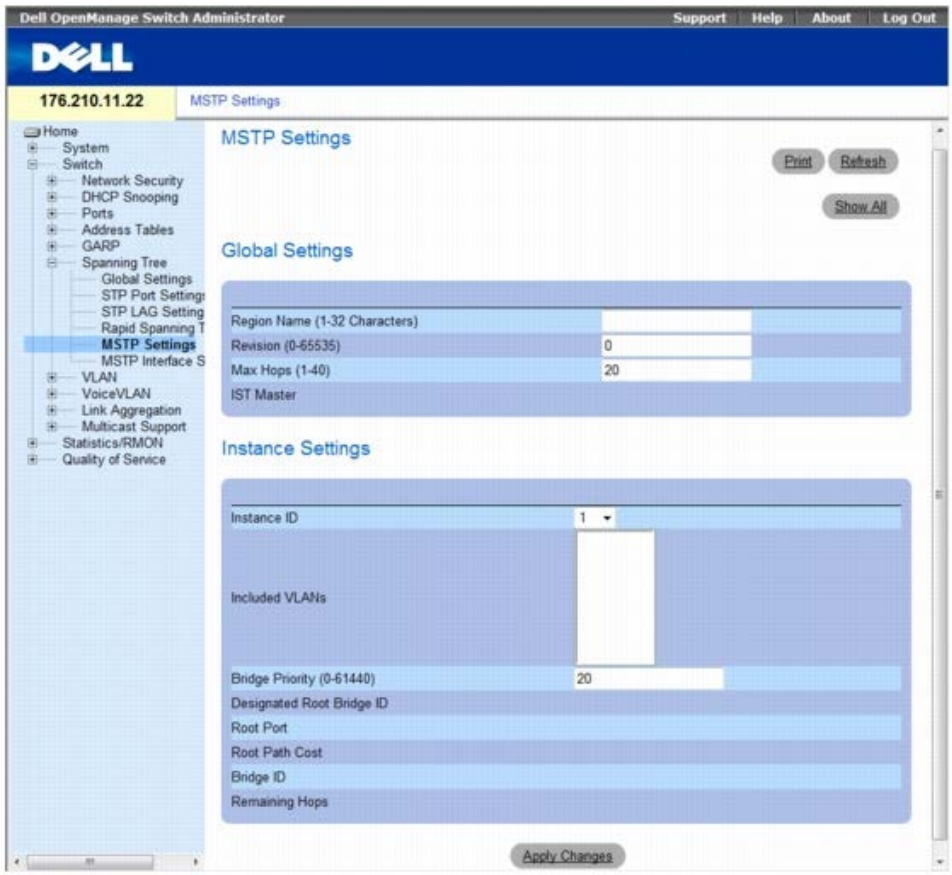
多重スパニングツリーの設定

MSTP の動作によって、VLAN は 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、様々な負荷バランシングシナリオを実現します。例えば、ある STP インスタンスではポート A がブロックされ、別の STP インスタンスでは同一ポートが *Forwarding State*（転送状態）に配置されます。

また、各種の VLAN に割り当てられたパケットは、多重スパニングツリーリージョン（MST リージョン）内の様々なパスに沿って送信されます。リージョンとは、フレームを送信できる 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 Settings（MSTP 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 Settings**（MSTP の設定）の順にクリックします。

図 **7-42. MSTP** の設定



MSTP Settings（MSTP 設定）ページには、以下のフィールドがあります。

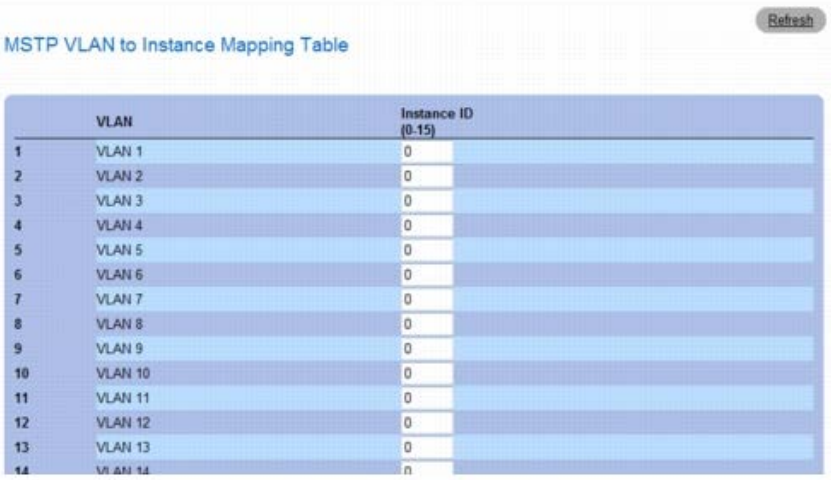
- **Region Name**（**1-32 Characters**）（リージョン名（1～32 文字））— ユーザー定義の MSTP リージョン名を示します。
- **Revision**（**0-65535**）（リビジョン（0～65535））— 現在の MST 設定リヴィジョンを識別する、署名のない 16 ビットの番号を定義します。リビジョン番号は、MST 設定の一部として必要です。可能なフィールド値は、0～65535 です。
- **Max Hops**（**1-40**）（最大ホップ数（1～40））— BPDU が破棄される前に特定のリージョンに存在する合計ホップ数を定義します。BPDU が破棄されると、ポート情報がエージアウトになります。可能なフィールド値は 1～40 です。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。フィールド範囲は、1～15 です。
- **Included VLANs**（包含する VLAN）— 選択されたインスタンスにマッピングされる VLAN を表示します。各 VLAN は、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））— 選択されたスパニングツリーインスタンスデバイスの優先度を指定します。フィールド範囲は 0～61440 で、4096 増分で指定します。
- **Designated Root Bridge ID**（指定のルートブリッジ ID）— 選択されたインスタンスのルーツであるブリッジの 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**（残りのホップ数）— 次の宛先までのホップ数を示します。

MSTP VLAN to Instance Mapping Table（MSTP VLAN とインスタンスのマッピング表）の表示

□□□ **Spanning Tree** **MSTP Settings**（スパニングツリー MSTP の設定）ページを開きます。

□□□ **Show All**（すべて表示）をクリックして、**MSTP VLAN to Instance Mapping Table**（MSTP VLAN とインスタンスのマッピング表）を開きます。

図 **7-43. MSTP VLAN** とインスタンスのマッピング表



CLI コマンドを使用した MST インスタンスの定義

Spanning Tree **MSTP Settings**（スパニングツリー MSTP の設定）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ための等価 CLI コマンドをまとめたものです。

表 **7-23. 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-range*	VLAN と MST インスタンスのマッチングを行います。
name *string*	設定名を設定します。
revision *value*	設定リビジョン番号を設定します。
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*	指定のスパニングツリーインスタンスに対して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、ポートに保持された情報がエージングされる前に、MST リージョンに存在するホップ数を設定します。
spanning-tree mst *instance-id* **cost** *cost*	MST 計算用にポートのパスコストを設定します。
Exit	MST リージョン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 リージョン設定モードを終了します。
show {**current** | **pending**}	現在または保留中の MST リージョンの設置を表示します。

CLI コマンドの例は次のようになります。

```
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
```

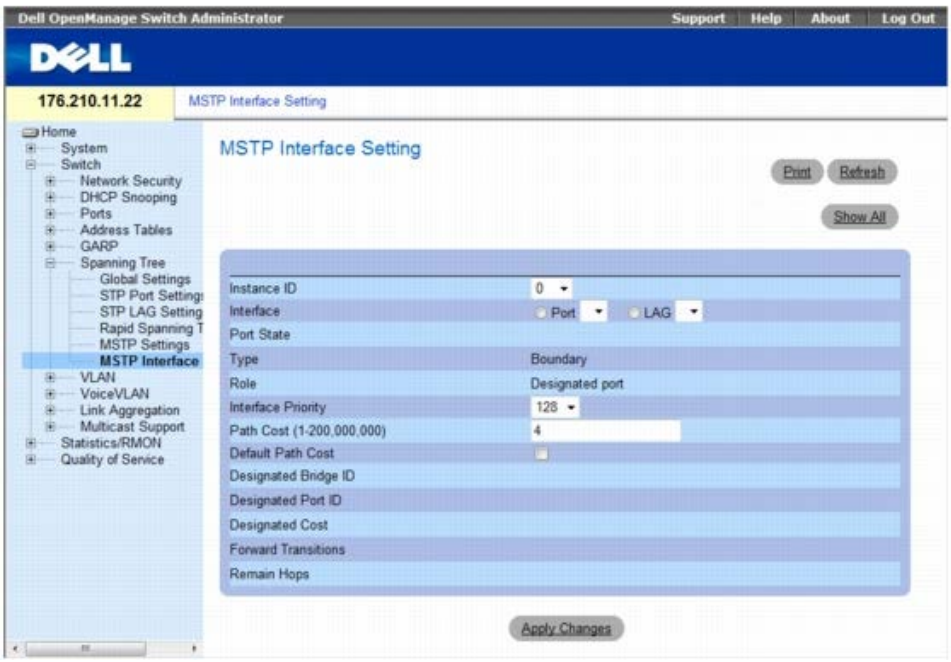
```
Instance Vlans Mapped
-------- ------------
0 1-9,31-4094
1 10-20
2 21-30
```

MSTP インタフェース設定の定義

MSTP Interface Settings（MSTP インタフェース設定）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ーがあります。

MSTP Interface Settings（MSTP インタフェース設定）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 インタフェース設定）の順にクリックします。

図 **7-44. MSTP** インタフェース設定



MSTP Interface Settings（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）— デバイスで設定されている MSTP インスタンスをリストします。可能なフィールド値は、0～15 です。
- **Interface**（インタフェース）— 選択した MSTP インスタンスにポートまたは LAG を割り当てます。
- **Port State**（ポートの状態）— 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ポートとして扱うか、またはハブに接続されたポートとして扱うかを示します。さらに、ポートが MST リージョンの内部であるか、境界ポートであるかを示します。マスターポートは、MSTP リージョンから外部 CIST ポートへの接続を提供します。境界ポートは、外部リージョンの LAN への MST ブリッジを接続します。また、ポートが境界ポートである場合は、リンクの他方のデバイスが RSTP モードで動作しているか、または STP モードで動作しているかを示します。
- **Role**（役割）— STP パスに提供するために 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次のとおりです。
  - **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示します。
  - **Designated**（指定）— 指定のデバイスを LAN に接続する際に経由するポートまたは 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示します。
  - **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示します。バックアップポートは、ポイントツーポイントリンクによってループ内で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関与していないことを示します。
- **Interface Priority**（インタフェース優先度）— 指定のインスタンスに対して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。可能な範囲は 1～200,000,000 です。

- **Default Path Cost**（デフォルトパスコスト）— デフォルトパスコストが使用されるかどうかを示します。可能な値は以下のとおりです。
  - **Checked**（チェックマークあり）— デフォルトパスコストが使用されます。
  - **Unchecked**（チェックマークなし）— パスコストはユーザー定義です。
- **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コストです。
- **Forward Transitions**（転送の移行）— ポートの状態が **forwarding**（転送）に移行した回数です。
- **Remain Hops**（残りのホップ数）— 次の宛先までのホップ数を示します。

MSTP インタフェース設定の定義

□□□ **MSTP Interface Settings**（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 パラメーターが定義され、デバイスがアップデートされます。

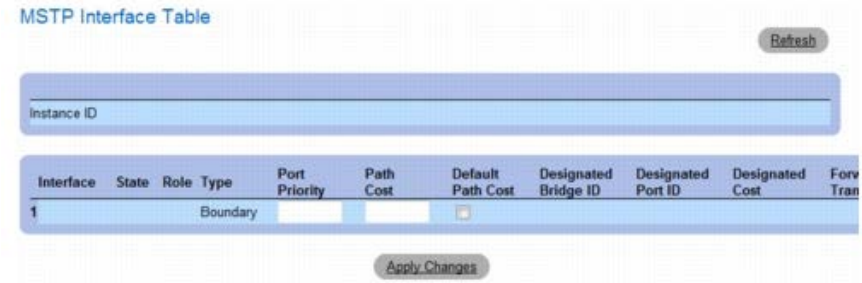
MSTP インタフェース表の表示

□□□ **MSTP Interface Settings**（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。

次のような **MSTP Interface Table**（MSTP インタフェース表）ページが開きます。

図 **7-45. 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

Spanning Tree MSTP Interface Settings（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ための等価 CLI コマンドをまとめたものです。

表 **7-24. MSTP** インス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 計算用にポートのパスコストを設定します。
spanning-tree mst *instance-id* **priority** *priority*	指定の ST インスタンスに対してデバイス優先度を設定します。
show spanning-tree mst-configuration	MST の設定を表示します。

CLI コマンドの例は次のようになります。

console# **show spanning-tree mst-configuration**		
Gathering information		
Current MST configuration		
Name: Gili		
Revision: 65000		
Instance	Vlans Mapped	Status
---	---	---
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 LAN を持つ論理的なサブグループです。VLAN は、ユーザーステーションとネットワークデバイスを、接続されている物理的な LAN セグメントに関係なく 1 つのユニットに結集します。VLAN によって、ネットワークトラフィックがサブグループ内で効率よく流れるようになります。ソフトウェアを通じて管理される VLAN は、ネットワークの変更、追加および移動にかかる時間を節約できます。

次のリンクをクリックすると、指定画面のオンラインヘルプにアクセスできます。

VLAN は、ソフトウェアベースであり、物理属性によって定義されないので、ポートの数に最小限度はなく、ユニット、デバイス、スタックやその他の論理接続コンビネーションごとに作成できます。

VLAN は、レイヤ 2 レベルで機能します。VLAN は その VLAN 内でトラフィックを隔離するので、VLAN 間のトラフィックフローを可能にするには、レイヤ 3 プロトコルレベルで機能するルーターが必要です。レイヤ 3 ルーターは、セグメントを識別し、VLAN と連係します。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、そのトラフィックが生成された VLAN 内のみで送信されます。

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、4 バイトタグをパケットヘッダーに付けて、そのパケットがどの VLAN に属しているかを示します。VLAN タグは、エンドステーションか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ます。

ネットワーク管理者は QinQ タギングを利用することにより、以前にタグを付けたパケットにタグを追加できます。カスタマ VLAN は、QinQ を使用して設定します。パケットにタグを追加することで、VLAN のスペースを増やすことができます。追加のタグで各カスタマに VLAN ID を付与し、それによってプライベートネットワークおよび隔離ネットワークのトラフィックを確保します。VLAN ID タグは、サービスプロバイダネットワークのカスタマポートに割り当てられます。指定されたポートでは、2 つのタグを持つパケットに追加のサービスが提供されます。システム管理者はこの機能を利用して、VLAN ユーザーにサービスを展開できます。

VLAN と GVRP を組み合わせることで、ネットワークマネージャは、ブロードキャストドメインのネットワークノードを定義できます。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、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。

本項には、次のトピックがあります。

- VLAN メンバーシップの定義
- VLAN ポートの設定の定義
- VLAN LAG の設定の定義
- MAC アドレスと VLAN のバインド

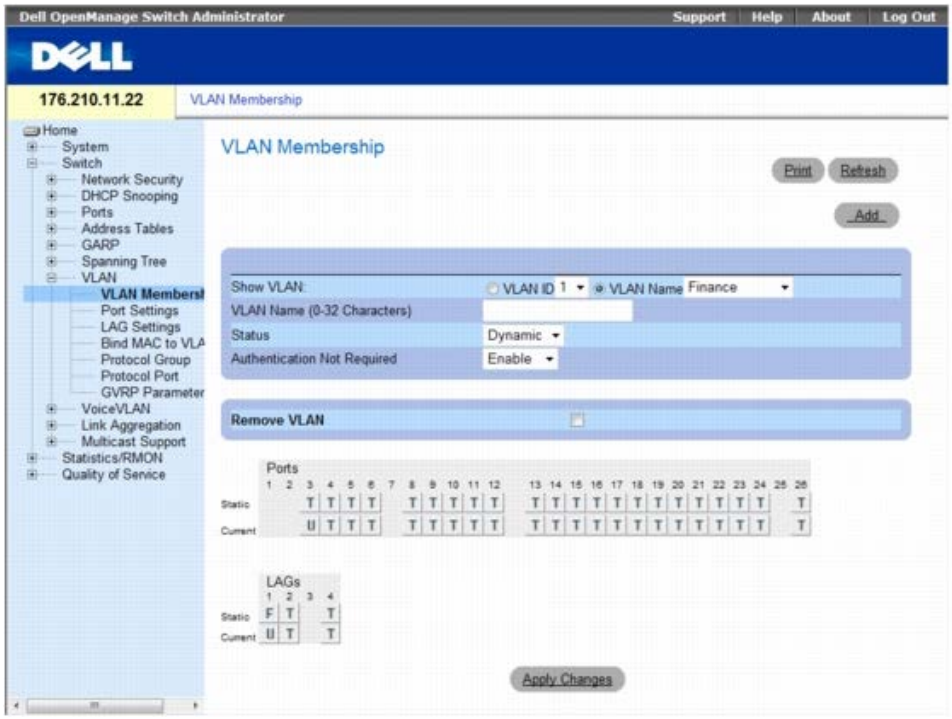
- VLAN プロトコルグループの定義
- インタフェースのプロトコルグループへの追加
- GVRP パラメーターの設定

VLAN メンバーシップの定義

VLAN Membership（VLAN のメンバーシップ）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、PVID が定義されている必要があります。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 番号 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 Membership（VLAN のメンバーシップ）ページを開くには、ツリービューで **Switch**（スイッチ）® **VLAN** ® **VLAN Membership**（VLAN のメンバーシップ）の順にクリックします。

図 **7-46. VLAN** のメンバーシップ



VLAN Membership（VLAN のメンバーシップ）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。可能な値は次のとおりです。
  - **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。
- **Authentication Not Required**（認証の必要なし）— 無許可のユーザーが VLAN にアクセスできるかどうかを示します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— 無許可のユーザーによる VLAN の使用を有効にします。
  - **Disable**（無効）— 無許可のユーザーによる VLAN の使用を無効にします。
- **Remove VLAN**（VLAN の削除）— VLAN Membership Table（VLAN メンバーシップ表）から VLAN を削除するかどうかを示します。
  - **Checked**（チェックマークあり）— VLAN を削除します。
  - **Unchecked**（チェックマークなし）— VLAN Membership Table（VLAN メンバーシップ表）の VLAN を保持します。

VLAN の新規追加

□□□ **VLAN Membership**（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。

Create New VLAN（VLAN の新規作成）ページが開きます。

図 **7-47. VLAN** の新規作成

□□□ 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 Membership**（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、デバイスが更新されます。

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。ポートを VLAN に割り当てるには、**Port Control**（ポートの制御）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 **7-25. VLAN** ポートメンバーシップ表

ポートの制御	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ました。
空白	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 の情報も表示されます。

VLAN グループへのポートの割り当て

□□□ **VLAN Membership**（VLAN のメンバーシップ）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。

□□□ **Port Membership Table**（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 Membership**（VLAN のメンバーシップ）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 メンバーシップグループの定義

次の表は **VLAN Membership**（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ための等価 CLI コマンドをまとめたものです。

表 **7-26. 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 に名前を追加します。

CLI コマンドの例は次のようになります。

```
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
```

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 CLI コマンドをまとめたものです。

表 **7-27. 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）とします。
switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]	ポートの一般モードで VLAN を追加または削除します。
switchport general pvid vlan-id	インタフェースが一般モードである場合に、PVID を設定します。

CLI コマンドの例は次のようになります。

```
console(config)# vlan database
console(config-vlan)# vlan 23-25
console(config-vlan)# end
console(config)# interface vlan23
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 ポートの設定の定義

VLAN Port Settings（VLAN ポートの設定）ページには、VLAN に属す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 Port Settings**（VLAN ポートの設定）ページで設定します。デバイスにタグなしで到達したすべてのパケットは、ポートの PVID を使ってタグが付けられます。

VLAN Port Settings（VLAN ポートの設定）ページを開くには、**Switch**（スイッチ）® **VLAN** ® **Port Settings**（ポート設定）の順にクリックします。

図 **7-48. VLAN** ポートの設定

VLAN Port Settings（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。可能な値は次のとおりです。
  - **Customer**（カスタマ）— ポートは VLAN に属します。ポートがカスタマモードであると、追加のタグによって各カスタマに VLAN ID が提供され、それによりプライベートで隔離されたネットワークのトラフィックが確保されます。

  - **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（タグなしが可能なポートを除きます）。
- **Dynamic**（動的）— ポートに接続されるホストソース **MAC** アドレスに基づいて、ポートを **VLAN** に割り当てます。
  - **Checked**（チェックマークあり）— ポートは、動的 VLAN に登録できます。
  - **Unchecked**（チェックマークなし）— ポートは、動的 VLAN に登録できません。
- **PVID**（**1-4095**）（PVID（1～4095））— VLAN ID をタグなしパケットに割り当てます。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撤回されます。
- **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。可能な値は次のとおりです。
  - **Admit Tag Only**（タグ付きのみ許可）— タグ付きのパケットのみポートで受け入れます。
  - **Admit All**（すべて許可）— タグ付き、タグなしの両方のパケットをポートで受け入れます。
- **Ingress Filtering**（入口フィルタリング）— 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 に関連付けられているパケットを破棄します。
  - **Enable**（有効）— ポートに対して入口フィルタリングが有効になります。
  - **Disable**（無効）— ポートに対して入口フィルタリングが無効になります。
- **Current Reserved VLAN**（現在の予約 **VLAN**）— 予約 VLAN として現在指定されている 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、ユーザーにより選択された VLAN を予約 VLAN とします。

ポートの設定の割り当て

□□□ **VLAN Port Settings**（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、デバイスが更新されます。

VLAN ポート表の表示

□□□ **VLAN Port Settings**（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 が開きます。

図 **7-49. VLAN** ポート表

VLAN LAG の設定の定義

VLAN LAG Settings（VLAN LAG の設定）ページには、VLAN に属する LAG を管理するためのパラメーターがあります。VLAN は、個々のポートと LAG のいずれかで構成できます。デバイスに到達したタグなしパケットには、PVID で指定される LAG ID のタグが付きます。

VLAN LAG Settings（VLAN LAG の設定）ページを開くには、ツリー表示で、**Switch**（スイッチ）® **VLAN** ® **LAG Settings**（LAG の設定）の順にクリックします。

図 **7-50. VLAN LAG** の設定

VLAN LAG Settings（VLAN LAG の設定）ページには、以下のフィールドがあります。

- **LAG** — VLAN に含まれる LAG の番号です。
- **LAG VLAN Mode**（LAG VLAN モード）— LAG VLAN モードです。可能な値は次のとおりです。
  - **Customer**（カスタマ）— LAG は VLAN に属します。LAG が Customer（カスタマ）モードであると、追加のタグによって各カスタマに VLAN ID が提供され、それによりプライベートで隔離されたネットワークのトラフィックが確保されます。
  - **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（タグなしが可能なポートを除きます）。
- **Dynamic**（動的）— LAG に接続されるホストソース MAC アドレスに基づいて、LAG を VLAN に割り当てます。可能な値は以下のとおりです。
  - **Checked**（チェックマークあり）— LAG は、動的 VLAN に登録できます。
  - **Unchecked**（チェックマークなし）— LAG は、動的 VLAN に登録できません。
- **PVID**（**1-4095**）（PVID（1～4095））— VLAN ID をタグなし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 LAG で受け入れられます。
  - **Admit All**（すべて許可）— タグ付き、タグなしの両方のパケットが LAG で受け入れられます。
- **Ingress Filtering**（入口フィルタリング）— LAG による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。可能な値は以下のとおりです。
  - **Enable**（有効）— LAG に対して入口フィルタリングが有効になります。
  - **Disable**（無効）— LAG に対して入口フィルタリングが無効になります。
- **Current Reserve VLAN**（現在の予約 VLAN）— 予約 VLAN として現在指定されている VLANです。
- **Reserve VLAN for Internal Use**（内部用の予約 VLAN）— デバイスのリセット後に予約 VLAN として指定する VLAN です。

VLAN LAG の設定の割り当て

□□□ **VLAN LAG Settings**（VLAN LAG の設定）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 パラメーターが定義され、デバイスがアップデートされます。

VLAN LAG 表の表示

□□□ **VLAN LAG Settings**（VLAN 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。

VLAN LAG Table（VLAN LAG 表）が開きます。

図 **7-51. VLAN LAG** 表

□□□ LAG の設定を変更するには、表の任意の LAG の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 LAG パラメーターが定義され、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 VLAN グループへの LAG の割り当て

次の表は、**VLAN LAG Settings**（VLAN LAG の設定）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 CLI コマンドをまとめたものです。

表 **7-28. VLAN** グループへの **LAG** 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 LAG のデフォルト VLAN ID（PVID）とします。
switchport general pvid *vlan-id*	インタフェースが一般モードである場合の LAG VLAN ID（PVID）を設定します。
switchport general allowed vlan add *vlan-list [***tagged | untagged***]*	VLAN を一般 LAG に追加するか、一般 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 アドレスと VLAN をバインドします。
switchport general ingress-filtering disable	LAG の入口フィルタリングを無効にします。

CLI コマンドの例は次のようになります。

```
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 アドレスと VLAN のバインド

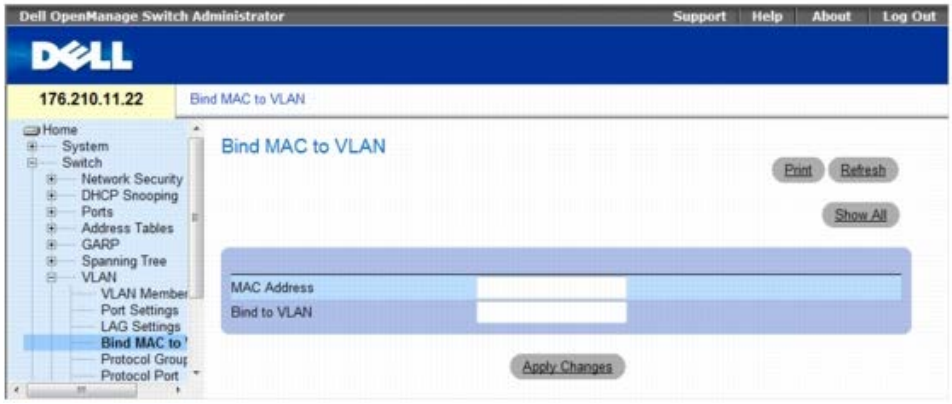
MAC アドレスを VLAN をバインドすると、MAC アドレスに基づいて、ポートが VLAN に割り当てられます。VLAN に MAC アドレスが割り当てられ、MAC アドレスがポートで学習されると、ポートは、バインドされた VLAN に参加します。MAC アドレスが期限切れになると、ポートは、VLAN から切り離されます。MAC アドレスには、動的 VLAN のみをバインドできます。

メモ： MAC と VLAN のバインド機能（MAC と VLAN の割り当て）は、動的 VLAN 割り当て機能（DVA）を含むバージョンには含まれません。DVA は、MAC と VLAN の割り当てと同じ機能を提供しますが、標準機能となります。

MAC アドレスを VLAN をバインドするには、VLAN ポートが動的に追加されており、静的 VLAN ポートでないことを確認してください。

Bind MAC to VLAN（MAC と VLAN のバインド）ページを開くには、**Switch**（スイッチ）® **VLAN** ® **Bind MAC to VLAN**（MAC と VLAN のバインド）の順に選択します。

図 **7-52. MAC** と **VLAN** のバインド



Bind MAC to VLAN（MAC と VLAN 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 にバインドされる MAC アドレスを示します。
- **Bind to VLAN**（VLNA にバインド）— MAC アドレスがバインドされる VLAN を示します。可能な値は、1～4094 です。

MAC to VLAN Table（MAC と VLAN のバインド表）の表示

□□□ **Bind MAC to VLAN**（MAC と VLAN 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 to VLAN Table（MAC と VLAN のバインド表）が開きます。

図 **7-53. MAC** と **VLAN** のバインド表

MAC と VLAN のバインドの削除

□□□ **Bind MAC to VLAN**（MAC と VLAN 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 to VLAN Table**（MAC と VLAN のバインド表）が開きます。

□□□ 目的の VLAN を選択するか、**All**（すべて）を選択してすべての VLAN のバインドを表示します。

□□□ 目的のバインドの横にある **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。

CLI コマンドを使用した MAC アドレス と VLAN のバインド

次の表は、MAC アドレスと VLAN をバインドする場合の等価 CLI コマンドをまとめたものです。

表 **7-29. MAC** アドレスと **VLAN** のバインドに関連する **CLI** コマンド

CLI コマンド	説明
mac-to-vlan mac-address vlan-id	MAC アドレスを VLAN をバインドします。
switchport access vlan dynamic	プライベート VLAN を設定します。
show mac-to-vlan	MAC と VLAN のバインドのデータベースを表示します。
no mac-to-vlan mac-address	MAC アドレスを VLAN のバインドから解除します。

CLI コマンドの例は次のようになります。

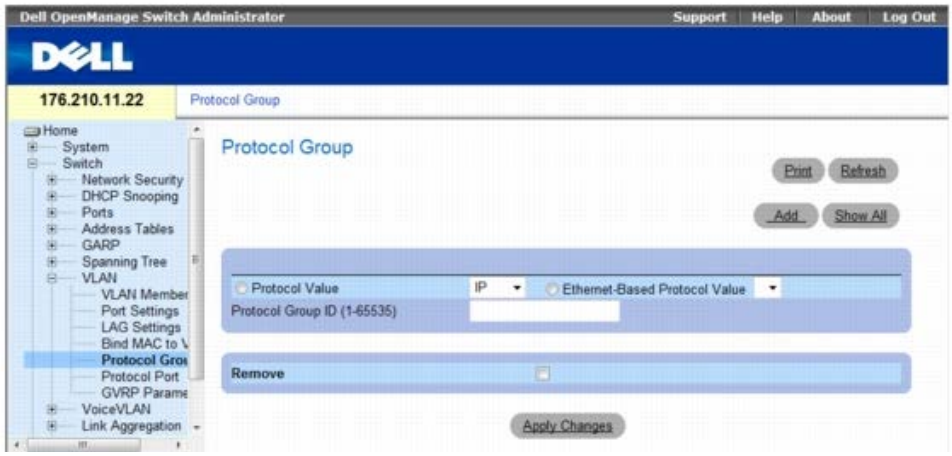
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123
console（config-vlan）# exit
console(config)# exit
console# show vlan mac-to-vlan
MAC Address VLAN
------------ ------
0060.704c.73ff 123
```

VLAN プロトコルグループの定義

Protocol Group（プロトコルグループ）ページには、フレームタイプを特定のプロトコルグループに設定するためのパラメーターがあります。

Protocol Group（プロトコルグループ）ページを開くには、ツリー表示で **Switch**（スイッチ）® **VLAN** ® **Protocol Group**（プロトコルグループ）をクリックします。

図 **7-54.** プロトコルグループ



- **Protocol Value**（プロトコル値）— ユーザー定義のプロトコル値を表示します。オプションを次に示します。
  - **Protocol Value**（プロトコル値）— ユーザー定義のプロトコル名です。可能なフィールド値は、**IP**、**IPX** および **ARP** です。
  - **Ethernet-Based Protocol Value**（イーサネットベースのプロトコル値）— イーサネットプロトコルグループのタイプです。
- **Protocol Group ID**（**1-65535**）（プロトコルグループ ID（1～65535））— VLAN グループ ID 番号です。
- **Remove**（削除）— 削除対象のプロトコルグループが当該のプロトコルポートに設定されていない場合、フレームとプロトコルグループのマッピングが削除されるかどうかを示します。
  - **Checked**（チェックマークあり）— プロトコルグループのマッピングを削除します。
  - **Unchecked**（チェックマークなし）— プロトコルグループのマッピングを保持します。

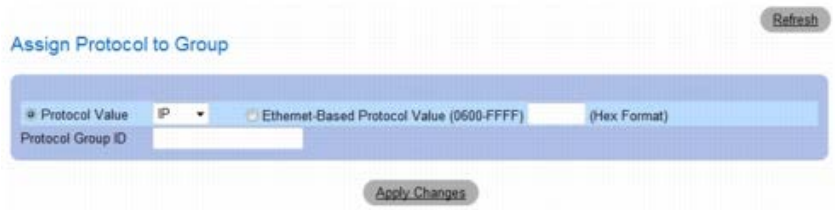
プロトコルのグループへの割り当て

□□□ **Protocol Group**（プロトコルグループ）ページを開きます。

□□□ **Add**（追加）をクリックします。

Assign Protocol To Group（プロトコルのグループへの割り当て）ページが開きます。

図 **7-55.** プロトコルのグループへの割り当て



□□□ そのページにある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。

プロトコルグループが割り当てられ、デバイスがアップデートされます。

VLAN プロトコルグループ設定の割り当て

□□□ **Protocol Group**（プロトコルグループ）ページを開きます。

□□□ そのページにある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。

VLAN プロトコルパラメーターが定義され、デバイスがアップデートされます。

プロトコルグループ表からのプロトコル削除

□□□ **Protocol Group**（プロトコルグループ）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Protocol Group Table（プロトコルグループ表）が開きます。

図 **7-56.** プロトコルグループ表

□□□ 削除する必要のあるプロトコルに対して、**Remove**（削除）を選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

プロトコルが削除され、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 プロトコルグループの定義

次の表はプロトコルグループを設定する場合の等価 CLI コマンドをまとめたものです。

表 **7-30. VLAN** プロトコルグループに関連する **CLI** コマンド

CLI コマンド	説明
map protocol *protocol [encapsulation]* **protocols-group** *group*	プロトコルとプロトコルグループをマッピングします。プロトコルグループは、プロトコルベースの VLAN 割り当てに使用されます。

次の例は、ip-arp プロトコルをグループ「213」にマッピングする場合を示しています。

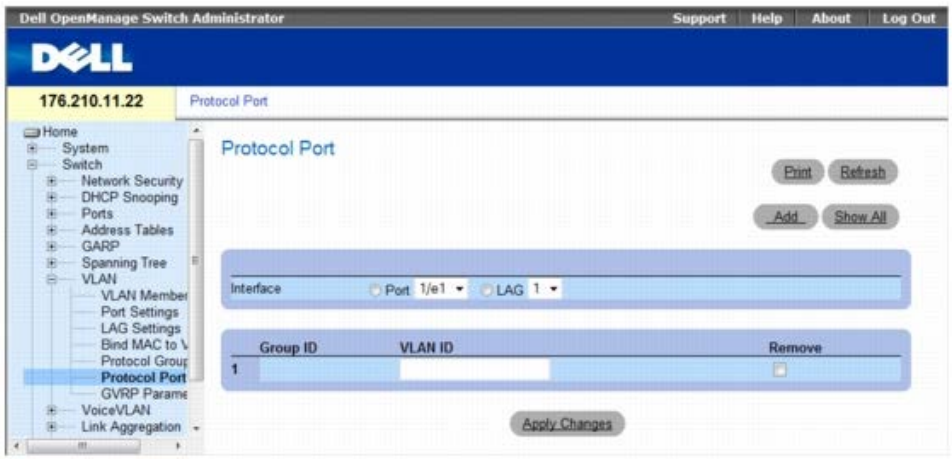
```
Console (config)# vlan database

Console (config-vlan)# map protocol ip-arp protocols-group 213
```

インタフェースのプロトコルグループへの追加

Protocol Port（プロトコルポート）ページでは、プロトコルグループにインタフェースを追加できます。

Protocol Port（プロトコルポート）ページを開くには、ツリービューで **Switch**（スイッチ）® **VLAN** ® **Protocol Port**（プロトコルポート）の順にクリックします。

図 **7-57.** プロトコルポート



- **Interface**（インタフェース）— プロトコルグループに追加するポートまたは LAG の番号です。
- **Group ID**（グループ ID）— インタフェースを追加するプロトコルグループの ID です。プロトコルグループ ID は、プロトコルグループ表に定義されていま

す。

- **VLAN ID** — インタフェースをユーザー定義の VLAN ID に結びつけます。VLAN ID は、**VLAN** の新規作成 ページで定義します。プロトコルポートは、VLAN ID と VLAN 名のいずれかに割り当てることができます。 可能な値は、1～4095 です。VLAN 4095 は、破棄 VLAN です。
- **Remove**（削除）— 選択されたインタフェースがそのプロトコルグループから削除されるかどうかを示します。
  - **Checked**（チェックマークあり）— 選択されたインタフェースを削除します。
  - **Unchecked**（チェックマークなし）— 選択されたインタフェースを保持します。

新しいプロトコルポートの **VLAN** への追加

プロトコルポートは、**VLAN Port Settings**（VLAN ポートの設定）ページで **General**（一般用）として定義したポートに対してのみ定義できます。

□□□ **Protocol Port**（プロトコルポート）ページを開きます。

□□□ **Add**（追加）をクリックします。

Assign Protocol Port To VLAN（プロトコルポートの VLAN への割り当て）ページが開きます。

図 **7-58.** プロトコルポートの **VLAN** への割り当て

□□□ ダイアログ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。

新規の VLAN プロトコルグループが プロトコルポート表 に追加され、デバイスがアップデートされます。

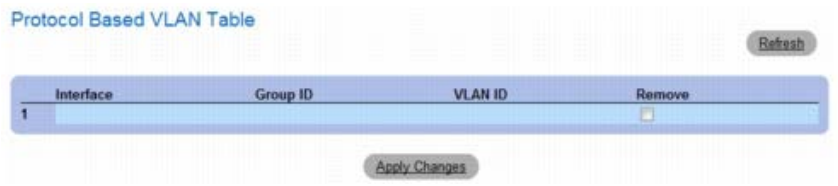
ポートに割り当てられたプロトコルの表示

□□□ **Protocol Port**（プロトコルポート）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Protocol Based VLAN Table（プロトコルベース VLAN 表）が開きます。

図 **7-59.** プロトコルベース **VLAN** 表



CLI コマンドを使用したプロトコルポートの定義

次の表はプロトコルポートを定義する場合の等価 CLI コマンドをまとめたものです。

表 **7-31.** プロトコルポートに関連する **CLI** コマンド

CLI コマンド	説明
switchport general map protocols-group *group* vlan *vlan-id*	プロトコルベースの分類ルールを設定します。

次の例は、プロトコルグループ 1 から VLAN 8 へのプロトコルベース分類ルールの設定を示しています。

```
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

GVRP パラメーターの設定

GARP VLAN Registration Protocol（GVRP）は、特に、VLAN 対応ブリッジに 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 対応ブリッジが、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 プロトコルを正常に動作させるには、GVRP VLAN の最大数が次の合計値を大幅に上回るように設定することをお勧めします。

- 現在設定されている静的 VLAN と、設定が予定されている静的 VLAN の総数。
- GVRP に関係する VLAN で、現在設定されている動的 VLAN（動的 GVRP VLAN の初期の数は 128 です）と、設定が予定されている動的 VLAN の総数。

GVRP Global Parameters（GVRP グローバルパラメーター）ページでは、GVRP をグローバルに有効にすることができます。また、GVRP は、インタフェースごとに有効にすることもできます。

GVRP Global Parameters（GVRP グローバルパラメーター）ページを開くには、ツリー表示で、**Switch**（スイッチ）® **VLAN** ® **GVRP Parameters**（GVRP パラメーター）の順にクリックします。

図 **7-60. GVRP** グローバルパラメーター

GVRP Global Parameters（GVRP グローバルパラメーター）ページには、以下のフィールドがあります。

グローバルパラメーター

- **GVRP Global Status**（GVRP グローバルステータス）— デバイスで GVRP が有効かどうかを示します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— 選択されたデバイスの GVRP を有効にします。
  - **Disable**（無効）— 選択されたデバイスの GVRP を無効にします。デフォルトでは、GVRP は無効になります。

ポートパラメーター

- **Interface**（インタフェース）— GVRP 設定を編集するポートまたは LAG を指定します。
- **GVRP State**（GVRP 状態）— GVRP がインタフェースで有効になっているかどうかを示します。可能なフィールド値は次のとおりです。
  - **Enabled**（有効）— 選択されたインタフェースの GVRP を有効にします。
  - **Disabled**（無効）— 選択されたインタフェースの GVRP を無効にします。
- **Dynamic VLAN Creation**（動的 VLAN 作成）— 動的 VLAN 作成がインタフェースで有効になっているかどうかを示します。可能なフィールド値は次のとおりです。

- **Enabled**（有効）— インタフェースで動的 VLAN 作成を有効にします。
- **Disabled**（無効）— インタフェースで動的 VLAN 作成を無効にします。

- **GVRP Registration**（GVRP 登録）— GVRP を介した VLAN 登録がインタフェースで有効かどうかを示します。可能なフィールド値は次のとおりです。
  - **Enabled**（有効）— インタフェースで GVRP 登録を有効にします。
  - **Disabled**（無効）— インタフェースで GVRP 登録を無効にします。

デバイスに対する **GVRP** の有効化

□□□ **GVRP Global Parameters**（GVRP グローバルパラメーター）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。

GVRP がデバイスで有効になります。

GVRP を介した **VLAN** 登録の有効化

□□□ **GVRP Global Parameters**（GVRP グローバルパラメーター）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。

□□□ 目的のインタフェースに対する GVRP State（GVRP 状態）フィールドで **Enable**（有効）を選択します。

□□□ **GVRP Registration**（GVRP 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。

選択したポートに対して GVRP VLAN 登録が有効になり、デバイスがアップデートされます。

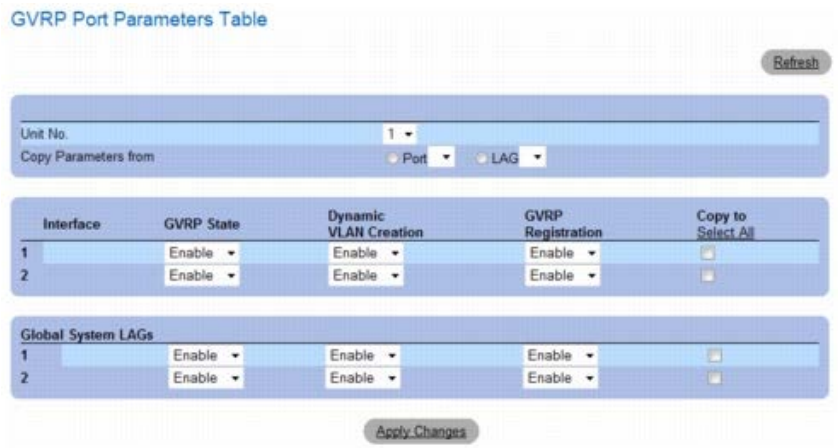
GVRP Port Parameters Table（**GVRP** ポートパラメーター表）の表示

□□□ **GVRP Global Parameters**（GVRP グローバルパラメーター）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

GVRP Port Parameters Table（GVRP ポートパラメーター表）が開きます。

図 **7-61. GVRP** ポートパラメーター表



GVRP Global Parameters（GVRP グローバルパラメーター）画面のほか、**GVRP Port Parameters Table**（GVRP ポートパラメーター表）には、以下のフィールドがあります。

Copy Parameters from（パラメーターのコピー元）— パラメーターがコピーされ、他のインタフェースに割り当てられるポートまたは LAG です。

CLI コマンドを使用した **GVRP** の設定

次の表は **GVRP Global Parameters**（GVRP グローバルパラメーター）ページに表示されているように、GVRP を設定する場合の等価 CLI コマンドをまとめたものです。

表 **7-32. GVRP** グローバルパラメーターに関連する **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 エラー統計を表示します。
show gvrp statistics [**ethernet** *interface*| **port-channel** *port-channel-number]*	GVRP 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。

CLI コマンドの例は次のようになります。

```
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

音声 **VLAN** の設定

ネットワーク管理者は音声 VLAN を利用して、特定の VLAN 上の IP 電話から IP 音声トラフィックを伝送するようにポートを設定することにより、VoIP サービスを拡張できます。VoIP トラフィックの送信元 MAC アドレスには、事前設定された OUI 識別コードが含まれています。ネットワーク管理者は、音声 IP トラフィックを転送する VLAN を設定できます。自動音声 VLAN セキュアモードでは、音声 VLAN からの VoIP 以外のトラフィックが破棄されます。また、音声 VLAN では VoIP に QoS が提供されるので、IP トラフィックの受信が不均衡の場合でも音声の品質が低下することはありません。システムは、1 つの音声 VLAN をサポートします。

IP 電話には、次の 2 つの動作モードがあります。

- IP 電話の VLAN モードを有効に設定すると、すべての通信にタグ付きパケットが使用されます。
- IP 電話の VLAN モードが無効の場合、電話にはタグなしパケットが使用されます。電話でタグなしパケットが使用されると、DHCP を介して初期 IP アドレスが取得されます。電話では最終的に音声 VLAN が使用され、タグ付きパケットの送信が開始されます。

本項には、次のトピックがあります。

- 音声 VLAN プロパティページの定義
- 音声 VLAN ポート設定の定義
- OUI の定義

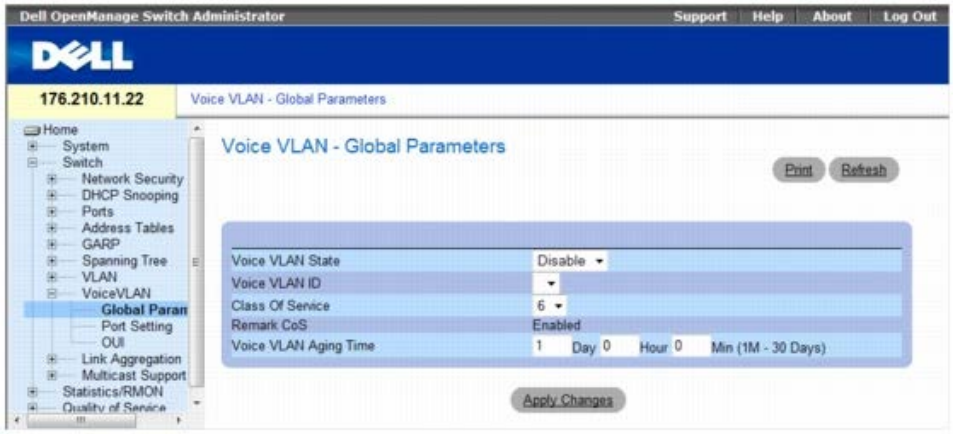
本項には、次のトピックがあります。

音声 **VLAN** グローバルパラメーターの定義

Voice VLAN Global Parameters（音声 VLAN グローバルパラメーター）ページには、デバイスのすべての音声 VLAN に適用されるパラメーターがあります。

Voice VLAN Global Parameters（音声 VLAN グローバルパラメーター）ページを開くには、ツリービューで **Switch**（スイッチ）® **Voice VLAN**（音声 VLAN）® **Global Parameters**（グローバルパラメーター）の順にクリックします。

図 **7-62.** 音声 **VLAN** グローバルパラメーター



- **Voice VLAN Status**（音声 VLAN ステータス）— 音声 VLAN がデバイスで有効であるかどうかを示します。可能なフィールド値は次のとおりです。
  - **Enable**（有効）— デバイスに対して音声 VLAN を有効にします。
  - **Disable**（無効）— デバイスに対して音声 VLAN を無効にします。これがデフォルト値になっています。
- **Voice VLAN ID**（音声 VLAN ID）— 音声 VLAN ID 番号を定義します。
- **Class of Service**（サービスクラス）— 音声 VLAN で受信したタグなしパケットに、CoS タグが追加されるようにします。可能なフィールド値は 0～7 です。0 は最低優先度を示し、7 は最高優先度を示します。
- **Remark CoS**（CoS の注釈）— Remark CoS（CoS の注釈）が常に有効になっていることを示します。
- **Voice VLAN Aging Time**（音声 VLAN エージングタイム）— 特定のポートについて、最後の IP 電話の OUI がエージアウトになるまでの時間を示します。ポートは、ブリッジおよび音声エージング時間後にエージアウトします。デフォルトの時間は 1 日です。フィールド形式は Day、Hour、Minute（日数、時間数、分数）です。エージングタイムは、MAC アドレスが動的 MAC アドレス表からエージアウトされた後から始まります。デフォルトタイムは 300 秒です。MAC アドレスのエージングタイムの定義に関しては、「エージングタイムの再定義」を参照してください。

音声 **VLAN** グローバルパラメーターを設定するには、次の手順を実行します。

□□□ **Voice VLAN Global Parameters**（音声 VLAN グローバルパラメーター）ページを開きます。

□□□ そのページにある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。

音声 VLAN グローバルパラメーターが定義され、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音声 **VLAN** グローバルパラメーターの定義

次の表は、音声 VLAN グローバルパラメーターを定義する場合の等価 CLI コマンドをまとめたものです。

表 **7-33.** 音声 **VLAN** グローバルパラメーターに関連する **CLI** コマンド

CLI コマンド	説明
voice vlan id *vlan-id* ***no voice vlan id***	音声 VLAN を有効にして、音声 VLAN ID を設定するには、グローバル設定モードで voice vlan id コマンドを使用します。音声 VLAN を無効にするには、このコマンドの no 形式を入力します。
voice vlan cos *cos* no voice vlan cos	音声 VLAN にサービスクラスを設定するには、グローバル設定モードで voice vlan cos コマンドを使用します。デフォルトに戻すには、このコマンドの no 形式を使用します。
voice vlan aging-timeout ***minutes*** no voice aging-timeout	音声 VLAN にエージングタイムアウトを設定するには、グローバル設定モードで voice vlan aging-timeout コマンドを使用します。デフォルトに戻すには、このコマンドの no 形式を使用します。
voice vlan enable	ポートに対して自動音声 VLAN 設定を有効にするには、voice vlan enable インタフェース設定コマンドを使用します。自動音声 VLAN 設定を無効にするには、このコマンドの no 形式を使用します。
show voice vlan [ethernet *interface* | port-channel *port-channel-number*]	音声 VLAN ステータスを表示するには、show voice vlan EXEC コマンドを使用します。

次は、CLI コマンドの例です。

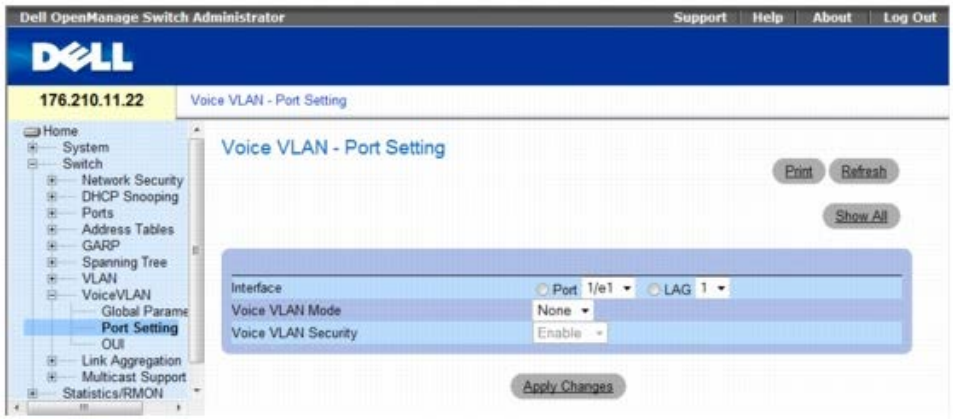
Switch# show voice vlan Aging timeout: 1440 minutes OUI table			
MAC Address - Prefix	Description		
00:E0:BB	3COM		
00:03:6B	Cisco		
00:E0:75	Veritel		
00:D0:1E	Pingtel		
00:01:E3	Siemens		
00:60:B9	NEC/Philips		
00:0F:E2	Huawei-3COM		
Voice VLAN VLAN ID: 8 CoS: 6 Remark: Yes			
Interface	Enabled	Secure	Activated
------	------	------	------
1/e1	Yes	Yes	Yes
1/e2	Yes	Yes	Yes
1/e3	Yes	Yes	Yes
1/e4	Yes	Yes	Yes
1/e5	No	No	-
1/e6	No	No	-
1/e7	No	No	-
1/e8	No	No	-
1/e9	No	No	-

音声 **VLAN** ポート設定の定義

Voice VLAN Port Settings（音声 VLAN ポート設定）ページには、音声 VLAN にポートまたは LAG を追加するためのフィールドがあります。

Voice VLAN Port Setting（音声 VLAN 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）® **Voice VLAN**（音声 VLAN）® **Port Setting**（ポート設定）の順にクリックします。

図 **7-63.** 音声 **VLAN** ポート設定



- **Interface**（インタフェース）— 音声 VLAN 設定を適用する特定のポートまたは LAG を示します。
- **Voice VLAN Mode**（音声 VLAN モード）— 音声 VLAN モードを定義します。可能なフィールド値は次のとおりです。
  - **None**（なし）— 音声 VLAN に対して選択したポートまたは LAG を無効にします。
  - **Static**（静的）— 現在の音声 VLAN ポートまたは LAG の設定を保持します。これがデフォルト値になっています。
  - **Auto**（自動）— IP 電話の MAC アドレスを持つトラフィックがポートまたは LAG に送信されると、そのポートまたは LAG は音声 VLAN に接続されることを示します。IP 電話の MAC アドレス（OUI 識別コード付き）がエージアウトされ、定義済みのエージングタイムを超えると、ポートまたは LAG は音声 VLAN からエージアウトされます。OUI 付きの IP 電話の MAC アドレスを音声 VLAN のポートまたは LAG に手動で追加した場合、そのユーザーは音声 VLAN に手動モードでポートまたは LAG を追加できますが、自動モードでは追加できません。
- **Voice VLAN Port/LAG Security**（音声 VLAN ポート /LAG のセキュリティ）— 音声 VLAN においてポートまたは LAG のセキュリティが有効であるかどうかを示します。ポートセキュリティによって、OUI が認識されない受信パケットは破棄されます。
  - **Enable**（有効）— 音声 VLAN に対してポートセキュリティを有効にします。
  - **Disable**（無効）— 音声 VLAN に対してポートセキュリティを無効にします。これがデフォルト値になっています。

ポートの設定

□□□ **Voice VLAN Port Settings**（音声 VLAN ポート設定）ページを開きます。

□□□ ポートまたは 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。

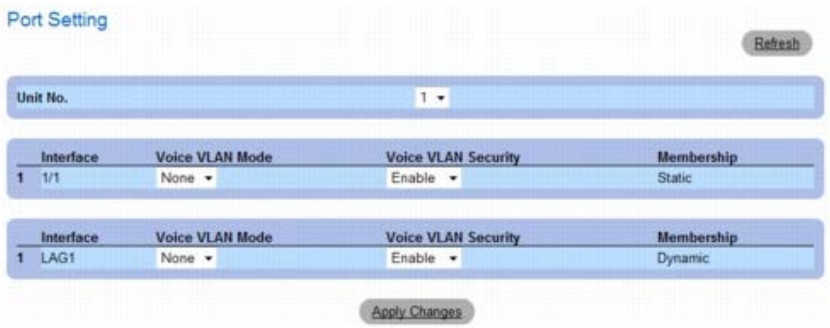
設定が変更され、デバイスがアップデートされます。

ポート設定表の表示

□□□ **Voice VLAN Port Settings**（音声 VLAN ポート設定）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。 **Port Setting Table**（ポート設定表）が開きます。

図 **7-64.** 音声 **VLAN** ポート設定表



音声 **VLAN** ポート設定表には、音声 VLAN メンバーが静的であるか、動的であるかを示す **Membership**（メンバーシップ）フィールドがあります。フィールド値 Dynamic（動的）は、VLAN メンバーシップが GARP を通じて動的に作成されたことを示します。フィールド値 Static（静的）は、VLAN メンバーシップがユーザー定義であることを示します。

□□□ ユニット番号を選択します。

□□□ 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。

CLI コマンドを使用した音声 VLAN ポート設定の定義

次の表は、音声 VLAN ポート設定を定義する場合の等価 CLI コマンドをまとめたものです。

表 **7-34.** 音声 **VLAN** ポート設定に関連する **CLI** コマンド

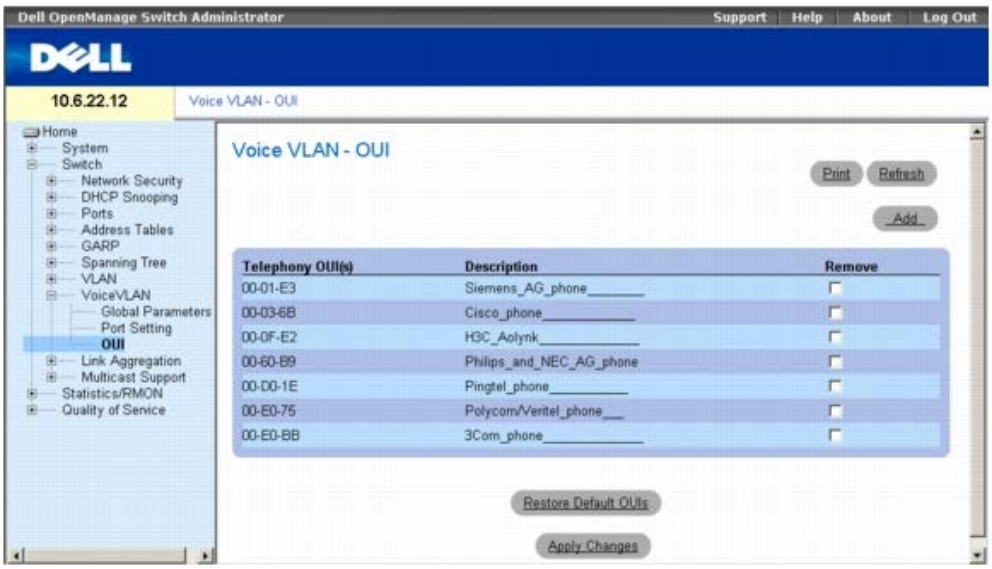
CLI コマンド	説明
voice vlan secure ***no voice vlan secure***	音声 VLAN に対してセキュアモードを設定するには、voice vlan secure インタフェース設定コマンドを使用します。セキュアモードを無効にするには、このコマンドの no 形式を使用します。

OUI の定義

Voice VLAN OUI（音声 VLAN OUI）ページには、音声 VLAN に関連付けられた Organizationally Unique Identifier（OUI）のリストが表示されます。MAC アドレスの最初の 3 バイトは、製造元の識別子を示します。一方、最後の 3 バイトは固有のステーション ID を示します。ネットワーク管理者は OUI を使用することで、特定の製造元の MAC アドレスを OUI 表に追加できます。OUI を追加すると、リストにある OUI を持つ特定の IP 電話から音声 VLAN ポートで受信したすべてのトラフィックは、音声 VLAN に転送されます。

Voice VLAN OUI（音声 VLAN OUI）ページを開くには、ツリービューで **Switch**（スイッチ）® **Voice VLAN**（音声 VLAN）® **OUI** の順にクリックします。

図 **7-65.** 音声 **VLAN OUI**



- **Telephony OUI**（**s**）（電話通信 OUI）— 音声 VLAN で現在有効な OUI のリストを表示します。デフォルトで次の OUI が有効になります。
  - 00-01-E3 — Siemens AG
  - 00-03-6B — Cisco
  - 00-0F-E2 — H3C Aolynk
  - 00-60-B9 — Philips/NEC AG
  - 00-D0-1E — Pingtel

- 00-E0-75 — Polycom/Veritel
- 00-E0-BB — 3COM

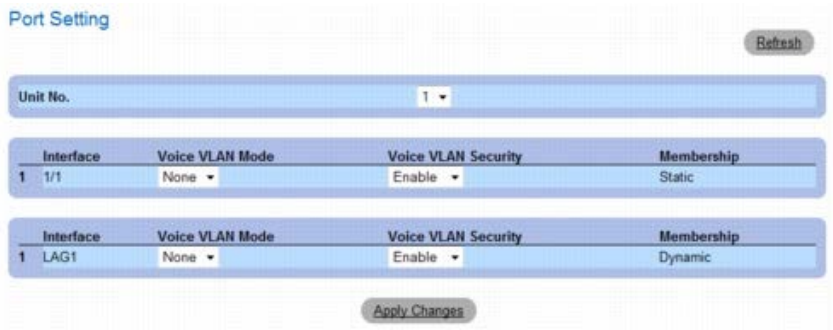
- **Description**（説明）— 最大 32 文字で OUI について説明します。
- **Remove**（削除）— 電話通信の OUI リストから OUI を削除します。可能なフィールド値は次のとおりです。
  - **Checked**（チェックマークあり）— 選択された OUI を削除します。
  - **Unchecked**（チェックマークなし） — 電話通信の OUI リストに現在存在する OUI を保持します。これがデフォルト値になっています。
- **Restore Default OUIs**（デフォルト OUI の復元）— OUI を工場出荷時のデフォルトに復元します。

OUI の追加

□□□ **Voice VLAN OUI**（音声 VLAN OUI）ページを開きます。

□□□ **Add**（追加）をクリックします。Add OUI（OUI の追加）ページが開きます。

図 **7-66.** 音声 **VLAN** の **OUI** の追加ページ



□□□ フィールドに入力します。

□□□ **Apply Changes**（変更の適用）をクリックします。

OUI が追加されます。

OUI の削除

□□□ **Voice VLAN OUI**（音声 VLAN OUI）ページを開きます。

□□□ 削除する OUI の横にある **Remove**（削除）チェックボックスをオンにします。

□□□ **Apply Changes**（変更の適用）をクリックします。

選択した OUI が削除されます。

デフォルト OUI の復元

□□□ **Voice VLAN OUI**（音声 VLAN OUI）ページを開きます。

□□□ **Restore Default OUIs**（デフォルト OUI の復元）をクリックします。

デフォルト OUI が復元されます。

CLI コマンドを使用した音声 VLAN OUI の定義

次の表は、音声 VLAN OUI を設定する場合の等価 CLI コマンドをまとめたものです。

表 **7-35.** 音声 **VLAN OUI** に関連した **CLI** コマンド

CLI コマンド	説明
voice vlan oui-table {add** mac-address-prefix **[description** text**] | remove** mac-address-prefix**} ***no voice vlan oui-table***	音声 VLAN OUI 表を設定するには、グローバル設定モードで voice vlan oui-table コマンドを使用します。デフォルトに戻すには、このコマンドの no 形式を使用します。

ポートの集約

リンクの集約は、ポートのグループを関連付けて 1 つの 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 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 ポートとポートリンクの集約をネゴシエイションします。他方のデバイスのポートも LACP ポートである場合には、両者間に LAG が確立されます。

ポートを集約する場合、次のことに注意してください。

- LAG 内のすべてのポートのメディアタイプが同じである
- VLAN がポートで設定されていない
- ポートが別の LAG に割り当てられていない
- オートネゴシエイションモードがポートで設定されていない
- ポートが全二重モードである
- LAG のすべてのポートの入口フィルタリングおよびタグモードが同じである
- LAG のすべてのポートのバックプレッシャーおよびフロー制御モードが同じである
- LAG のすべてのポートの優先度が同じである
- LAG のすべてのポートの同じトランシーバタイプが同じである
- デバイスでサポートされる LAG は 8つ で、各 LAG には最大 8 ポートを割り当てることができる
- 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る

LAG に追加されたポートは、その個々のポート設定が無効になります。ポートが LAG から削除されると、元のポート設定がそのポートに適用されます。

デバイスは、ハッシュ機能を使用して、どのパケットが、どの集約リンクメンバーを通過するか判別します。ハッシュ機能は、集約リンクメンバーの負荷バランシング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。

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、全二重方式に設定された同スピードの複数のポートで構成されます。

リンク集約グループ（LAG）のポートは、ポートの動作スピードが同じ場合、異なるメディアタイプを使用できます。集約リンクを手動または自動で設定するには、関連リンクで Link Aggregation Control Protocol（LACP）を有効にします。

本項には、次のトピックがあります。

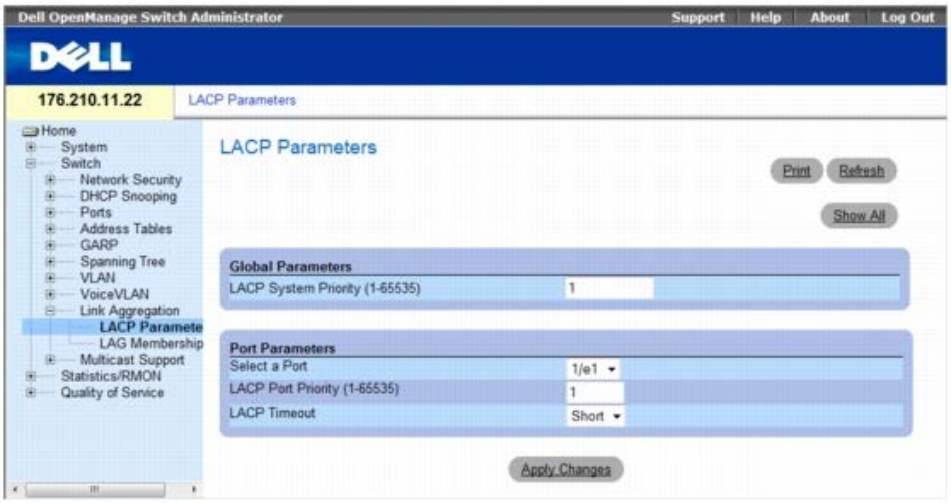
- LACP パラメーターの定義
- LAG メンバーシップの定義

LACP パラメーターの定義

LACP Parameters（LACP パラメーター）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 Parameters（LACP パラメーター）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 パラメーター）順にクリックします。

図 **7-67. LACP** パラメーター



LACP Parameters（LACP パラメーター）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次のとおりです。
  - **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ーの定義

□□□ **LACP Parameters**（LACP パラメーター）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。

パラメーターが定義され、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ーの定義

□□□ **LACP Parameters**（LACP パラメーター）ページを開きます。

□□□ **Port Parameters**（ポートパラメーター）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。

パラメーターが定義され、デバイスがアップデートされます。

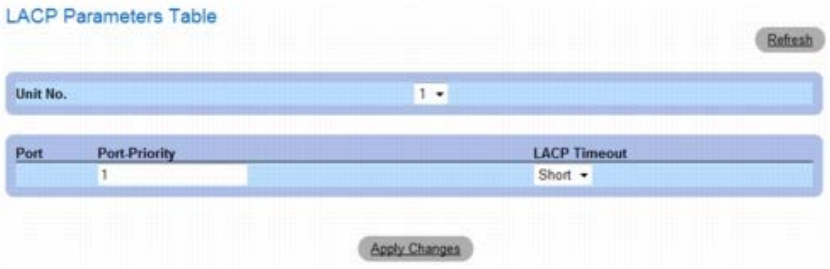
LACP パラメーター表の表示

□□□ **LACP Parameters**（LACP パラメーター）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

LACP Parameters Table（LACP パラメーター表）が開きます。

図 **7-68. LACP** パラメーター表



CLI コマンドを使用した LACP パラメーターの設定

次の表は **LACP Parameters**（LACP パラメーター）ページに表示されているように、LACP パラメーターを設定する場合の等価 CLI コマンドをまとめたものです。

表 **7-36. LACP** パラメーターに関連する **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**]	イーサネットポートに関する LACP 情報を表示します。

CLI コマンドの例は次のようになります。

```
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

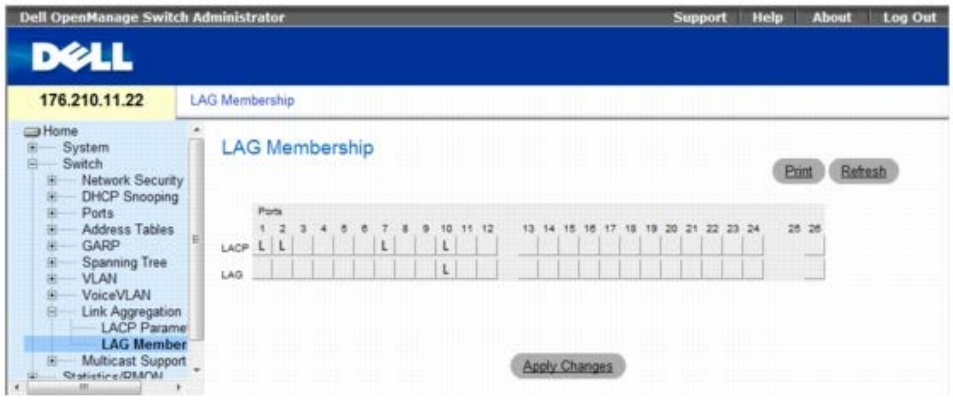
デバイスが、スタンドアロンデバイスまたはスタックのデバイスかどうかに関係なく、デバイスでサポートされる LAG はシステムあたり 15 つ です。また、LAG ごとに 8 ポート割り当てることができます。

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 プロパティで設定できない場合、ポートは LAG に追加されず、エラーメッセージが生成されます。ただし、LAG に参加する最初のポートが LAG で設定できない場合、ポートデフォルト設定を使用して、ポートが LAG に追加され、エラーメッセージが生成されます。また、これが、LAG の唯一のポートである場合、LAG 全体は、LAG で定義されている設定ではなく、ポートの設定を使用して動作します。

LAG Membership（LAG メンバーシップ）ページを使用すると、ポートを LAG に割り当てることができます。

LAG Membership（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 **7-69. LAG** メンバーシップ



LAG Membership（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。

ポートの **LAG** または **LACP** への追加

□□□ **LAG Membership**（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 Membership**（LAG メンバーシップ）ページに表示されているように、LAG にポートを割り当てる場合の等価 CLI コマンドをまとめたものです。

表 **7-37. 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、このコマンドの形式は使用しません。
show interfaces port-channel [*port-channel-number*]	ポートチャネル情報を表示します。

CLI コマンドの例は次のようになります。

```
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 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 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）— 登録済みマルチキャストグループにアドレスされるトラフィックがあった場合、これは、マルチキャストフィルタリングデータベースのエントリにより処理され、登録済み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）— 未登録マルチキャストグループにアドレスされるトラフィックがあった場合、これは、マルチキャストフィルタリングデータベースのエントリにより処理されます。デフォルトの設定では、このようなトラフィック（未登録マルチキャストグループのトラフィック）はすべてフラッドされます。

デバイスでは、次の機能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 2 マルチキャストパケットを転送します。レイヤ 2 マルチキャストフィルタリングは、デフォルトで有効になっていますが、ユーザーが設定することはできません。

システムでは、256 個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 2 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を無効にすると、マルチキャストパケットがすべての関連ポートに送信されます。

Multicast Support（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。

本項には、次のトピックがあります。

マルチキャストグローバルパラメーターの定義

レイヤ 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、パケットは単一マルチキャスト送信として管理されます。マルチキャストトラフィック転送は効果的ですが、関連しないポートもマルチキャストパケットを受信するので、最適ではありません。余分なパケットにより、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リングは、ポートサブセットへのレイヤ 2 パケットの転送を有効にします。

IGMP スヌーピングがグローバルで有効にされている場合、すべての IGMP パケットが、CPU に転送されます。CPU は、着信パケットを解析し、次のことを判断します。

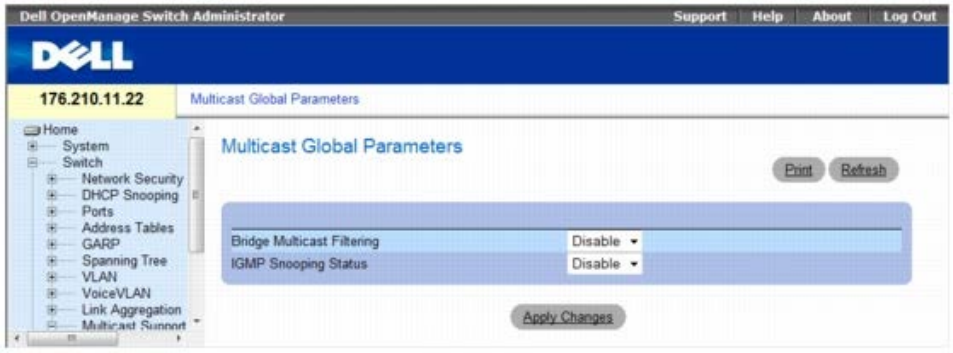
- どのポートがどのマルチキャストグループに参加するか
- どのポートが IGMP クエリを生成するマルチキャストルーターであるか
- どのルーティングプロトコルでパケットおよびマルチキャストトラフィックが転送されているか

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、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。

Global Parameters（グローバルパラメーター）ページには、デバイスに対して IGMP スヌーピングを有効にするためのフィールドがあります。

Global Parameters（グローバルパラメーター）ページを開くには、ツリー表示で、**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ー）の順にクリックします。

図 **7-70.** グローバルパラメーター



Global Parameters（グローバルパラメーター）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。無効がデフォルト設定になります。
  - **Enable**（有効）— デバイスでブリッジのマルチキャストフィルタリングを有効にします。
  - **Disable**（無効）— デバイスでブリッジのマルチキャストフィルタリングを無効にします。
- **IGMP Snooping Status**（IGMP スヌービングステータス）— デバイスに対して IGMP スヌービングを有効または無効にします。無効がデフォルト設定になります。IGMP スヌーピングを有効にできるのは、**Global Parameters**（グローバルパラメーター）が有効にされている場合のみです。

- Enable（有効）— デバイスで IGMP スヌーピングを有効にします。
- Disable（無効）— デバイスで IGMP スヌーピングを無効にします。

デバイスでのブリッジマルチキャストフィルタリングの有効化

□□□ **Global Parameters**（グローバルパラメーター）ページを開きます。

□□□ **Bridge Multicast Filtering**（ブリッジの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。

Bridge Multicast Filtering（ブリッジのマルチキャストフィルタリング）がデバイス有効になります。

デバイスでの **IGMP** スヌーピングの有効化

□□□ **Global Parameters**（グローバルパラメーター）ページを開きます。

□□□ **IGMP Snooping Status**（IGMP スヌーピングステータス）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。

IGMP スヌーピングがデバイスで有効になります。

CLI コマンドを使用したマルチキャストフィルタリングおよび **IGMP** スヌーピングの有効化

次の表は、**Global Parameters**（マルチキャストグローバルパラメーター）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および IGMP スヌーピングを有効にする場合の等価 CLI コマンドをまとめたものです。

表 **7-38.** マルチキャストフィルタリングおよびスヌーピングに関連する **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 Membership Protocol）スヌーピングを有効にします。

CLI コマンドの例は次のようになります。

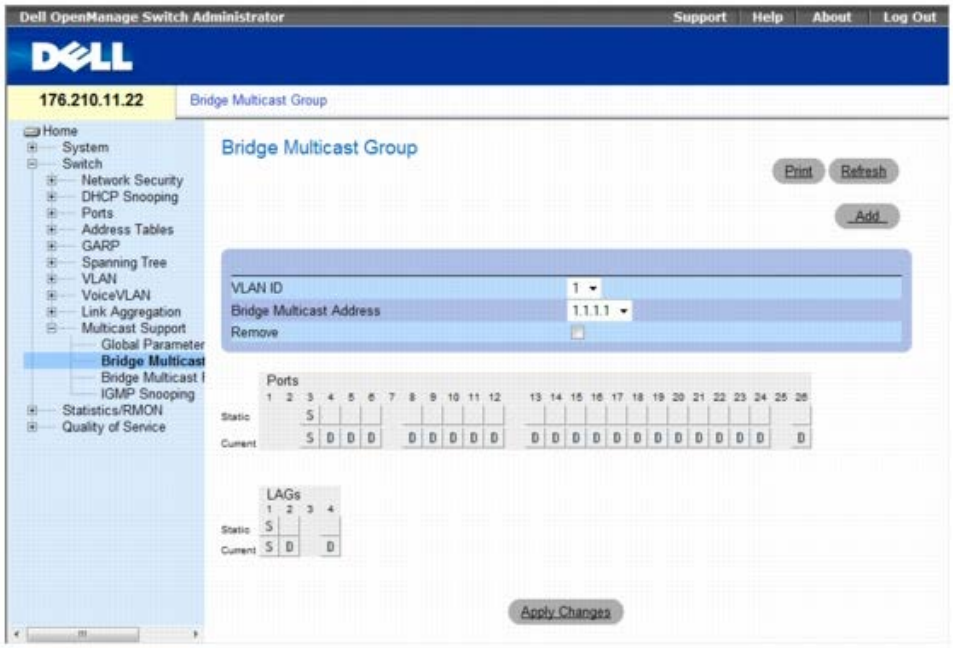
```
console(config)# bridge multicast filtering

console(config)# ip igmp snooping
```

ブリッジのマルチキャストアドレスメンバーの追加

Bridge Multicast Group（ブリッジマルチキャストグループ）ページで **Ports**（ポート）表および **LAG** 表の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。**Bridge Multicast Group**（ブリッジの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。また、**Bridge Multicast Group**（ブリッジの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。

Bridge Multicast Group（マルチキャストグループ）ページを開くには、ツリー表示で、**Switch**（スイッチ）® **Multicast Support**（マルチキャストサポート）® **Bridge Multicast Group**（ブリッジのマルチキャストグループ）の順にクリックします。

図 **7-71.** ブリッジのマルチキャストグループ



Bridge Multicast Group（ブリッジの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**（ブリッジの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）— ブリッジのマルチキャストアドレスを削除するかどうかを示します。
  - **Checked**（チェックマークあり）— 選択されたブリッジのマルチキャストアドレスを削除します。
  - **Unchecked**（チェックマークなし）— 選択されたブリッジのマルチキャストアドレスを保持します。
- **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。

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 **7-39. IGMP** ポート **/LAG** メンバー表の制御設定

ポートの制御	定義
D	Current（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	Static（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。 Current（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。

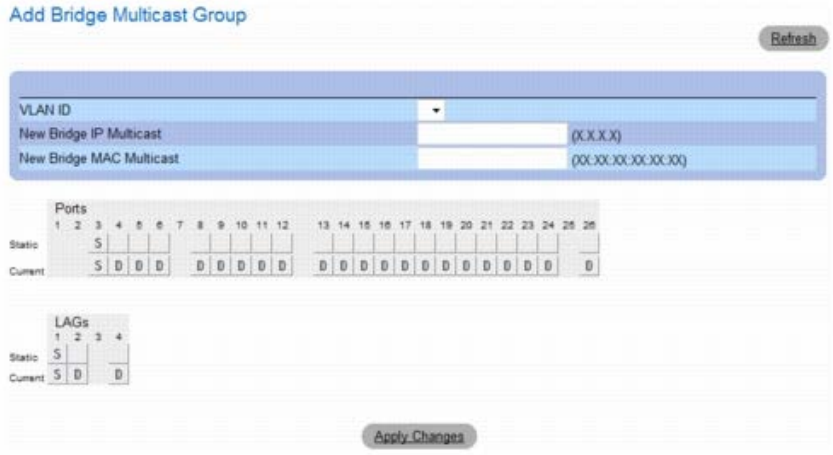
ブリッジのマルチキャストアドレスの追加

□□□ **Bridge Multicast Group**（ブリッジの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。

The **Add Bridge Multicast Group**（ブリッジのマルチキャストグループの追加）ページが開きます。

図 **7-72.** ブリッジの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。

ポートのマルチキャストサービス受信化の定義

□□□ **Bridge Multicast Group**（ブリッジの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。

LAG のマルチキャストサービス受信化の割り当て

□□□ **Bridge Multicast Group**（ブリッジの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 **Bridge Multicast Group**（ブリッジの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 CLI コマンドをまとめたものです。

表 **7-40.** 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-*	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

address}[**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}	止します。デフォルトに戻すには、このコマンドの形式を使用しません。
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。

CLI コマンドの例は次のようになります。

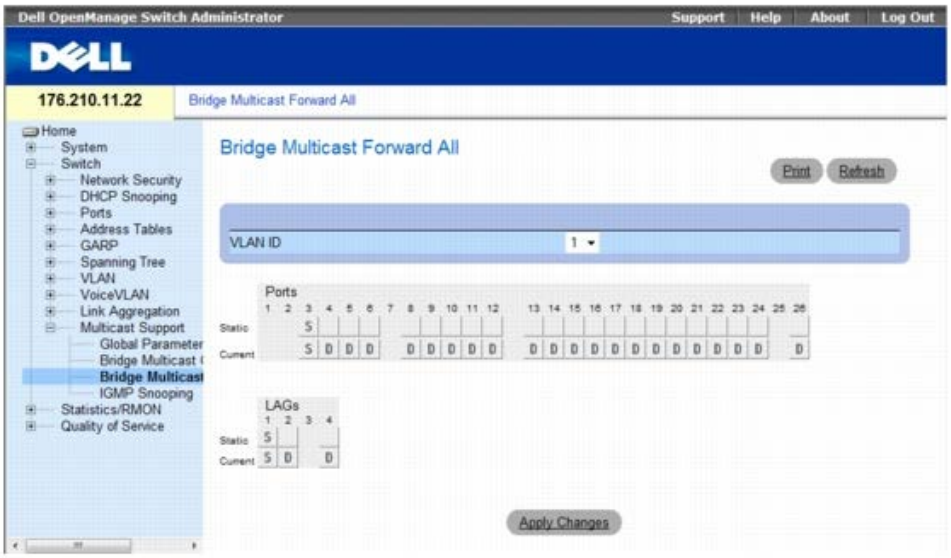
```
Console（config-if）# bridge multicast address 0100.5e02.0203
add ethernet 1/e11,1/e12
console(config-if)# end
console # show bridge multicast address-table

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ーの割り当て

Bridge Multicast Forward All（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 スヌーピングを有効にすると、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。

Bridge Multicast Forward All（ブリッジのマルチキャストすべて転送）ページを開くには、ツリー表示で、**Switch**（スイッチ）® **Multicast Support**（マルチキャストサポート）® **Bridge Multicast Forward All**（ブリッジのマルチキャストすべて転送）の順にクリックします。

図 **7-73.** ブリッジのマルチキャストすべて転送



Bridge Multicast Forward All（ブリッジの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。

Bridge Multicast Forward All Switch/Port Control Settings Table（ブリッジの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制御設定表）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。

ブリッジの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制御設定表の管理

次の表は、ポート制御設定に使用されるコントロールについて説明しています。

表 **7-41.** ブリッジの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制御設定表

Port Control（ポートの制御）	定義
D	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割り当てます。
S	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割り当てます。
F	禁止されています。
空白	ポートは、マルチキャストルーターまたはスイッチに割り当てられていません。

ポートのマルチキャストルーターまたはスイッチへの割り当て

□□□ **Bridge Multicast Forward All**（ブリッジの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。

□□□ **Ports**（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。

ポートがマルチキャストルーターまたはスイッチに割り当てられます。

LAG のマルチキャストルーターまたはスイッチへの割り当て

□□□ **Bridge Multicast Forward All**（ブリッジの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。

LAG がマルチキャストルーターまたはスイッチに割り当てられます。

CLI コマンドを使用したマルチキャストルーターに割り当てる LAG およびポートの管理

次の表は、**Bridge Multicast Forward All**（ブリッジの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割り当てられた LAG およびポートを管理する場合の等価 CLI コマンドをまとめたものです。

表 **7-42.** マルチキャストルーターに割り当てられた **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、このコマンドの形式を使用しません。

CLI コマンドの例は次のようになります。

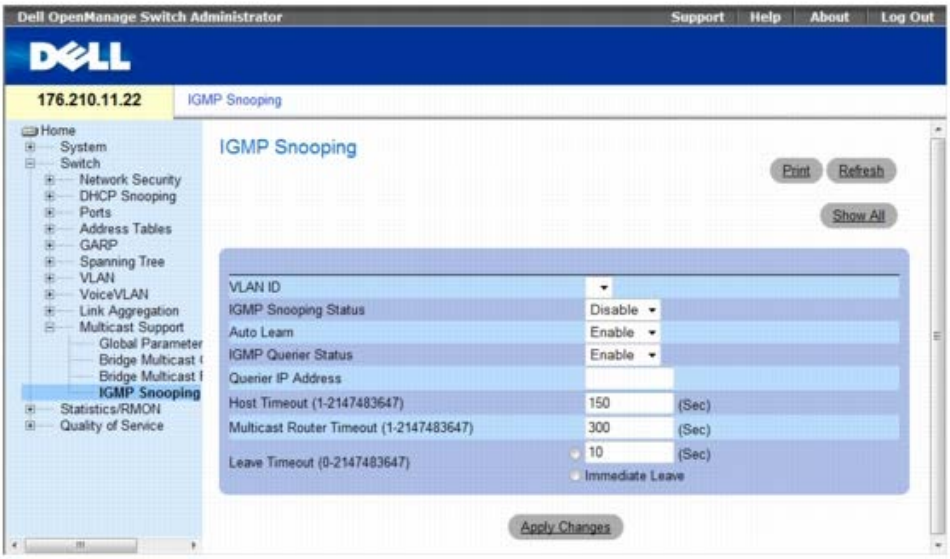
```
Console(config)# interface vlan 1
Console(config-if)# bridge multicast forward-all add ethernet 1/e3
Console(config-if)# end
Console# show bridge multicast filtering 1
```

Filtering: Enabled		
VLAN:	Forward-All	
Port	Static	Status
-------	----------	----------
1/e11	Forbidden	Filter^
1/e12	Forward	Forward（s）
1/e13	-	Forward（d）

IGMP スヌーピング

IGMP Snooping（IGMP スヌーピング）ページには、IGMP メンバーを追加するためのフィールドがあります。**IGMP Snooping**（IGMP スヌーピング）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 スヌーピング）の順にクリックします。

図 **7-74. IGMP** スヌーピング



- **VLAN ID** — VLAN ID を指定します。

- **IGMP Snooping Status**（IGMP スヌーピングステータス）— VLAN で IGMP スヌーピングを有効または無効にします。
- **Auto Learn**（自動学習）— デバイスに対して自動学習を有効または無効にします。
- **IGMP Querier Status**（IGMP クエリアステータス）— IGMP クエリアを有効または無効にします。IGMP クエリアは、マルチキャストルーターの動作をシミュレートし、マルチキャストルーターなしでも、レイヤ 2 マルチキャストドメインのスヌーピングを可能にします。
- **Querier IP Address**（クエリア IP アドレス）— IGMP クエリアの IP アドレスです。VLAN の IP インタフェースアドレスを使用するか、クエリアの送信元アドレスとして使用する固有の IP アドレスを定義します。
- **Host Timeout**（**1-2147483647**）（ホストのタイムアウト（1～2147483647））— IGMP スヌーピングのエントリがタイムアウトになるまでの時間です。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になるまでの時間です。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））— ポートが Leave メッセージを受け取ってから、エントリがエージアウトになるまでの時間（秒単位）です。**User-defined**（ユーザー定義）を指定すると、ユーザー定義のタイムアウト時間が有効になり、**Immediate Leave**（即時退去）では、即時のタイムアウト時間を指定できます。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 スヌーピングの有効化

□□□ **IGMP Snooping**（IGMP スヌーピング）ページを開きます。

□□□ IGMP スヌーピング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 スヌーピングステータス）フィールドで **Enable**（有効）を選択します。

□□□ そのページにある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。

IGMP スヌーピングがデバイスで有効になります。

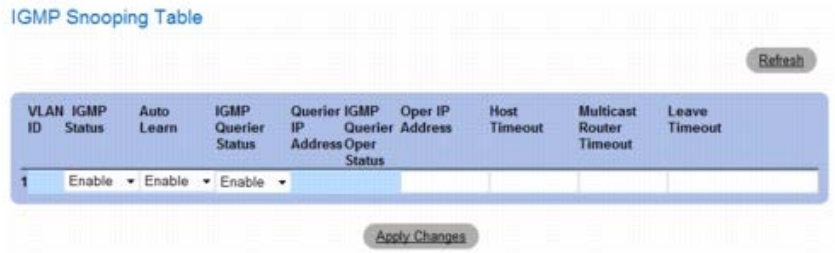
IGMP スヌーピング表の表示

□□□ **IGMP Snooping**（IGMP スヌーピング）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

IGMP Snooping Table（IGMP スヌーピング表）が開きます。

図 **7-75. IGMP** スヌーピング表



CLI コマンドを使用した IGMP スヌーピングの設定

次の表はデバイスに対して IGMP スヌーピングを設定する場合の等価 CLI コマンドをまとめたものです。

表 **7-43. IGMP** スヌーピングに関連する **CLI** コマンド

CLI コマンド	説明
ip igmp snooping	IGMP（Internet Group Membership Protocol）スヌーピングを有効にします。
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	host-time-out を設定します。

ip igmp snooping mrouter-time-out time-out	mrouter-time-out を設定します。
ip igmp snooping leave-time-out {time-out | *immediate-leave*}	leave-time-out を設定します。
ip igmp snooping querier enable no ip igmp snooping querier enable	特定の VLAN に対してインターネットグループ管理プロトコル（IGMP）クエリアを有効にします。無効にするには、このコマンドの no 形式を使用します。
ip igmp snooping querier address *ip-address* no ip igmp snooping querier address	IGMP スヌーピングクエリアを使用する送信元 IP アドレスを定義します。デフォルトに戻すには、このコマンドの形式を使用しません。
show ip igmp snooping groups [vlan *vlan-id*] [address *ip-multicast-address*]	IGMP スヌーピング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 スヌーピング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。

CLI コマンドの例は次のようになります。

```
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)# exit
Console (config)# interface vlan 1
Console (config-if)# ip igmp snooping leave-time-out 60
Console (config-if)# exit
Console (config)# exit
Console # show ip igmp snooping groups
Vlan IP Address Querier Ports
----- ------------------ -------- -----
1 224-239.130|2.2.3 Yes g1, g2

Console # show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
```

```
IGMP Snooping admin: Enabled
Hosts and routers IGMP version: 2
IGMP snooping oper mode: Enabled
IGMP snooping querier admin: Enabled
IGMP snooping querier oper: Enabled
IGMP snooping querier address admin:
IGMP snooping querier address oper: 172.16.1.1
IGMP snooping querier version admin: 3
IGMP snooping querier version oper: 2



IGMP host timeout is 300 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 300 sec
Automatic learning of multicast router ports is enabled
```

```
Console # show ip igmp snooping mrouter

VLAN    Ports
----    ------
1       g1
```

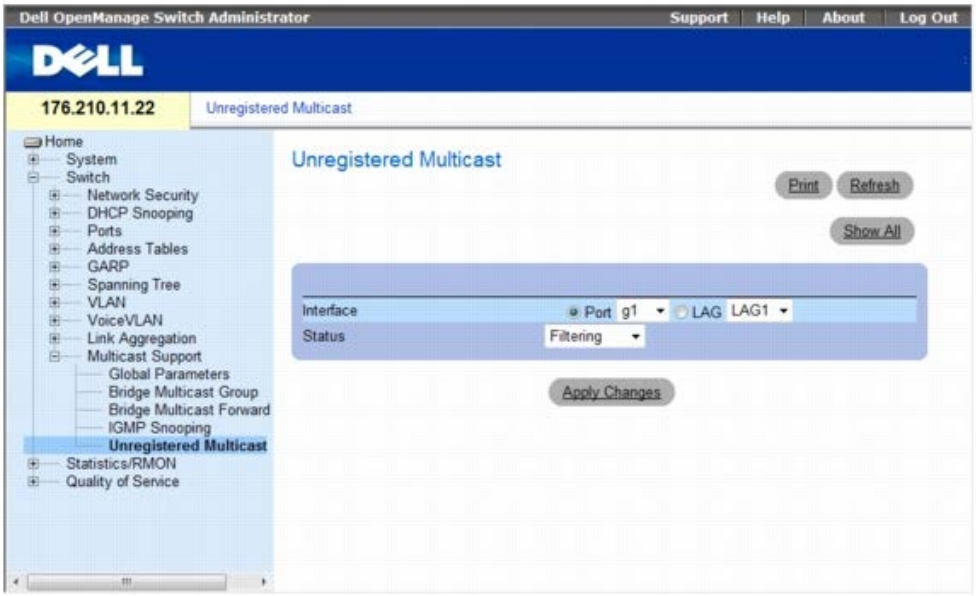
未登録マルチキャスト

マルチキャストフレームは、通常、VLAN 内のすべてのポートに転送されます。IGMP スヌーピングが有効な場合、デバイスはマルチキャストグループの存在を学習し、どのポートがどのマルチキャストグループに参加したかをモニタします。マルチキャストグループは、静的に有効にすることもできます。これにより、デバイスは登録済みマルチキャストグループからのマルチキャストフレームを、そのマルチキャストグループに登録されたポートにのみ転送することが可能になります。

Unregistered Multicast（未登録マルチキャスト）ページには、未登録マルチキャストグループに属するマルチキャストフレームを処理するフィールドがあります。未登録マルチキャストグループは、デバイスにとって未知のグループです。すべての未登録マルチキャストフレームは、依然として VLAN 上のすべてのポートに転送されます。ポートを Forwarding（転送）または Filtering（フィルタリング）に設定すると、このポートの設定はメンバーである（または今後メンバとなる）VLAN で有効になります。

Unregistered Multicast（未登録マルチキャスト）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）® **Unregistered Multicast** （未登録マルチキャスト）の順にクリックします。

図 **7-76.** 未登録マルチキャスト



- **Interface**（インタフェース） — ポートまたは LAG を選択します。
- **Status**（ステータス）— 選択したインタフェースの転送ステータスを示します。可能な値は以下のとおりです。
  - **Forwarding**（転送）— 選択したポートまたはポートチャネルの未登録マルチキャストフレームの転送を有効にします。これがデフォルト値になっています。
  - **Filtering**（フィルタリング）— 選択した **VLAN** インタフェースの未登録マルチキャストフレームのフィルタリングを有効にします。

インタフェースの未登録マルチキャストステータスの設定

□□□ **Unregistered Multicast**（未登録マルチキャスト）ページを開きます。

□□□ 設定する未登録マルチキャストのインタフェースを選択します。

□□□ **Status**（ステータス）フィールドでステータスを選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

未登録マルチキャストのステータスが設定されました。

未登録マルチキャスト表の表示

□□□ **Unregistered Multicast**（未登録マルチキャスト）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

Unregistered Multicast Table（未登録マルチキャスト表）が開きます。

図 **7-77.** 未登録マルチキャスト表

Unregistered Multicast Table（未登録マルチキャスト表）には、次の追加フィールドが表示されます。

- **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 from**（コピー元）— 選択されたアイテムからパラメーターをコピーします。

インタフェース間の未登録マルチキャスト設定のコピー

□□□ **Unregistered Multicast**（未登録マルチキャスト）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。**Unregistered Multicast Table**（未登録マルチキャスト表）が開きます。

□□□ **Copy Parameters from**（パラメーターのコピー元）フィールドでコピー元のインタフェースタイプを選択します。

□□□ パラメーターをコピーする各インタフェースに対して、**Copy to**（コピー先）フィールドのチェックボックスをオンにします。 または、**Select All**（すべて選択）をクリックしてすべてのインタフェースを自動的に選択します。

□□□ **Apply Changes**（変更の適用）をクリックします。

未登録マルチキャストのパラメーターがインタフェース間でコピーされます。

CLI コマンドを使用した未登録マルチキャストの設定

次の表はデバイスに対して 未登録マルチキャスト を設定する場合の等価 CLI コマンドをまとめたものです。

表 **7-44.** 未登録マルチキャストに関連する **CLI** コマンド

CLI コマンド	説明
bridge multicast unregistered	未登録マルチキャストアドレスの転送状態を設定します。
show bridge multicast unregistered	未登録マルチキャストフィルタリングの設定を表示します。

CLI コマンドの例は次のようになります。

```
Console # show bridge multicast unregistered

Port Unregistered
---- -------------
1/1   Forward
1/2   Filter
```

```
1/3   Filter
```

目次に戻る

目次に戻る

統計の表示

Dell™ PowerConnect™ 35xx システムユーザーズガイド

Statistic（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へのリンクがあります。統計 ページを開くには、ツリー表示の **Statistics**（統計）をクリックします。

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

The **Table Views**（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。ページを開くには、ツリー表示の **Statistics**（統計）® **Table**（表） をクリックします。

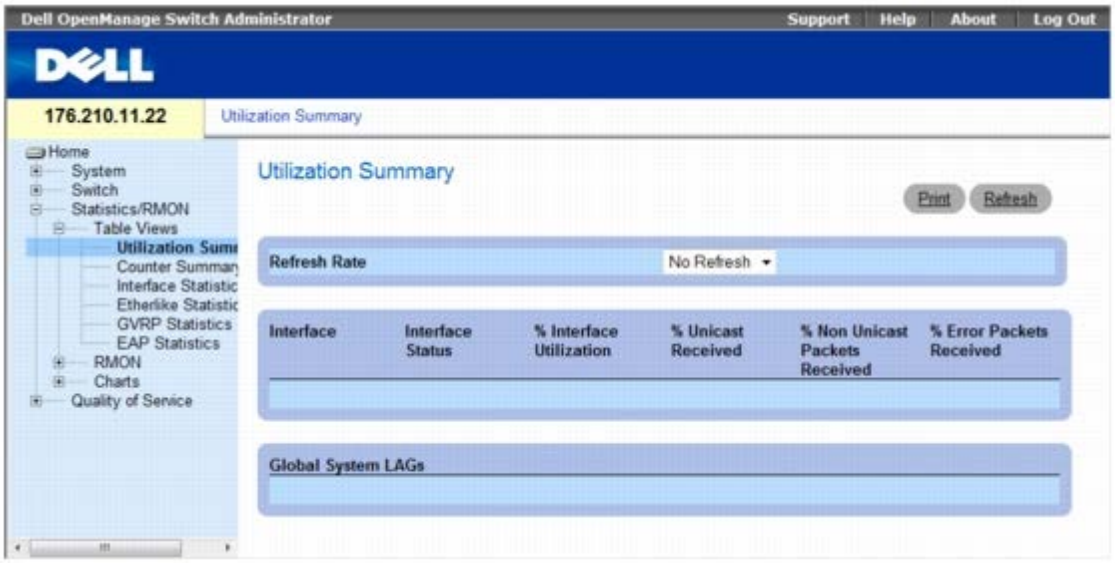
本項には、次のトピックがあります。

利用率の要約の表示

Utilization Summary（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。この画面は定期的に更新され、メモリの少ないコンピュータに対する影響を最小限にします。更新中には表示が中断することがあります。

ページを開くには、ツリー表示の **Statistics**（統計）® **Table Views**（表の表示）® **Utilization Summary**（利用率の要約）をクリックします。

図 **8-1.** 利用率の要約



Utilization Summary（利用率の要約）ページには、次のフィールドがあります。

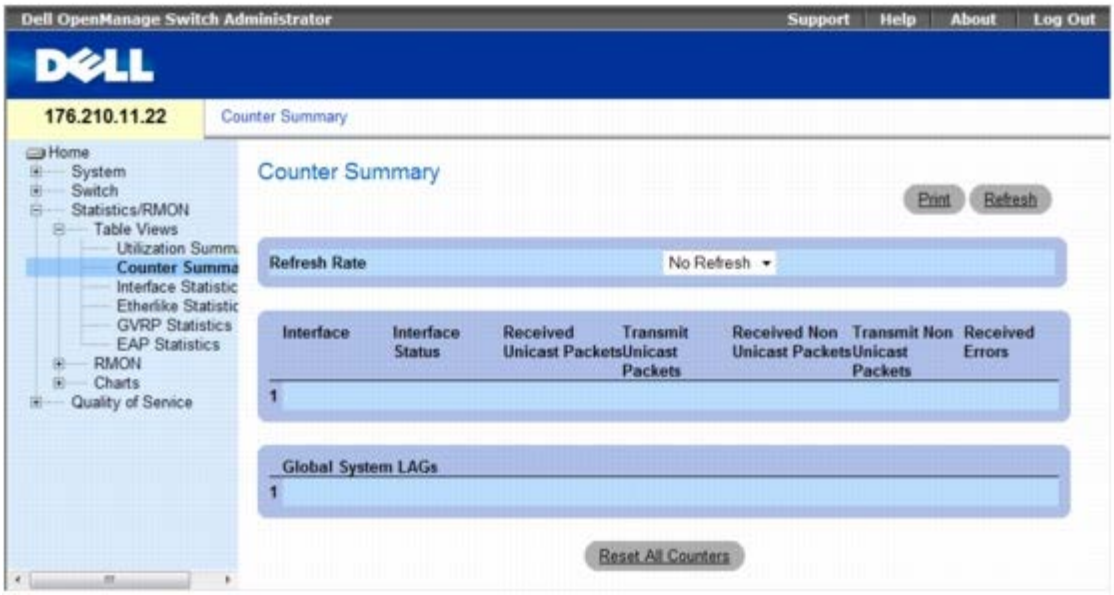
- **Refresh Rate**（リフレッシュレート）— インタフェース統計がリフレッシュされる前に経過する時間を示します。可能なフィールド値は次のとおりです。
  - **15 Sec**（15 秒）— インタフェース統計が 15 秒ごとにリフレッシュされることを示します。
  - **30 Sec**（30 秒）— インタフェース統計が 30 秒ごとにリフレッシュされることを示します。
  - **60 Sec**（60 秒）— インタフェース統計が 60 秒ごとにリフレッシュされることを示します。
  - **No Refresh**（リフレッシュなし）— インタフェース統計が自動的にリフレッシュされないことを示します。
- **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 から 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割合です。
- **Global System LAGs**（グローバルシステム LAG）— 現在のグローバル LAG 利用率を示しています。

カウンタの要約の表示

Counter Summary（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。

Counter Summary（カウンタの要約）ページを開くには、ツリー表示の **Statistics/RMON**（統計/RMON）® **Table Views**（表の表示）® **Counter Summary**（カウンタの要約）をクリックします。

図 **8-2.** カウンタの要約



Counter Summary（カウンタサマリ）ページには次のフィールドが含まれています。

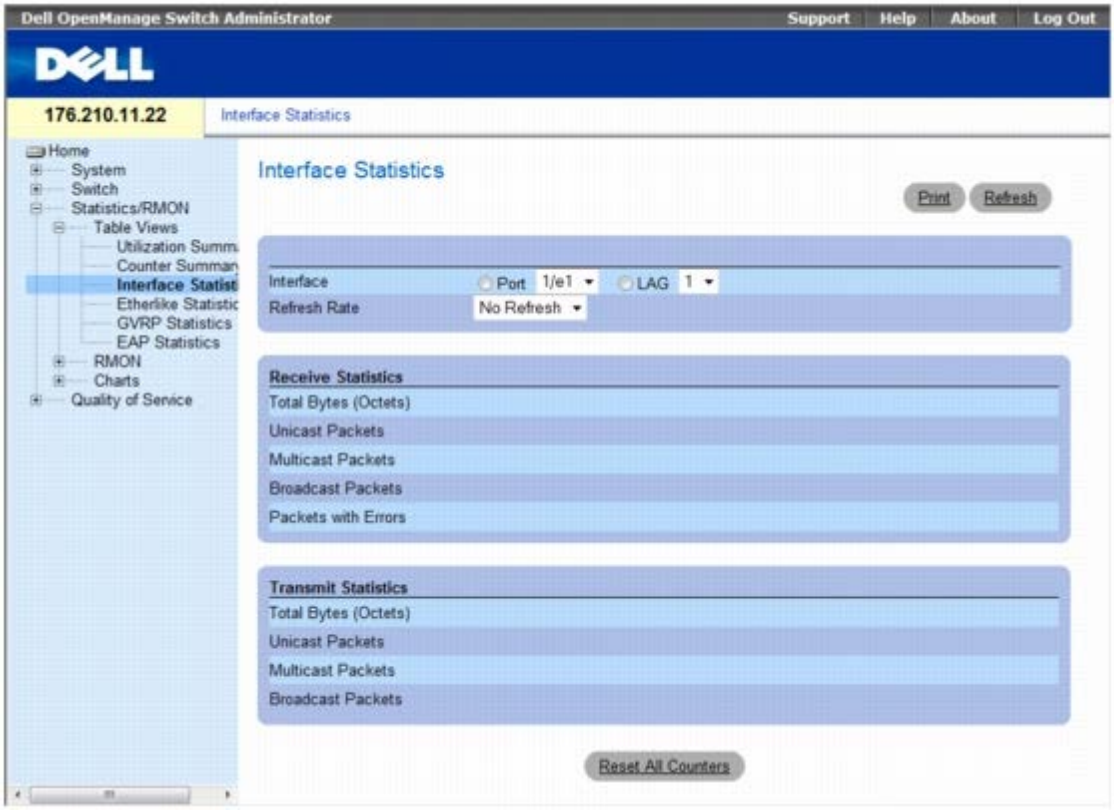
- **Refresh Rate**（リフレッシュレート）— インタフェース統計がリフレッシュされる前に経過する時間を示します。可能なフィールド値は次のとおりです。
  - **15 Sec**（15 秒）— インタフェース統計が 15 秒ごとにリフレッシュされることを示します。
  - **30 Sec**（30 秒）— インタフェース統計が 30 秒ごとにリフレッシュされることを示します。
  - **60 Sec**（60 秒）— インタフェース統計が 60 秒ごとにリフレッシュされることを示します。
  - **No Refresh**（リフレッシュなし）— インタフェース統計が自動的にリフレッシュされないことを示します。
- **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のあるパケットの数です。
- **Global System LAGs**（グローバルシステム LAG）— グローバルシステム LAG 用のカウンタサマリを提供します。

インタフェース統計の表示

Interface Statistics（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のパケット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。

Interface Statistics（インタフェース統計）ページを開くには、ツリー表示の **Statistics/RMON**（統計/RMON）® **Table Views**（表の表示）® **Interface Statistics**（インタフェース統計）をクリックします。

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次のフィールドが含まれています。

- **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前に経過する時間です。可能なフィールド値は次のとおりです。
  - **15 Sec**（15 秒）— インタフェース統計が 15 秒ごとにリフレッシュされることを示します。
  - **30 Sec**（30 秒）— インタフェース統計が 30 秒ごとにリフレッシュされることを示します。
  - **60 Sec**（60 秒）— インタフェース統計が 60 秒ごとにリフレッシュされることを示します。
  - **No Refresh**（リフレッシュなし）— インタフェース統計が自動的にリフレッシュされないことを示します。

統計の受信

- **Total Bytes**（**Octets**）（総バイト数（オクテット））— 選択され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）— 選択されたインタフェースで受信されたユニキャストパケットの数です。
- **Multicast Packets**（マルチキャストパケット）— 選択されたインタフェースで受信されたマルチキャストパケットの数です。
- **Broadcast Packets**（ブロードキャストパケット）— 選択されたインタフェースで受信されたブロードキャストパケットの数です。
- **Packets with Errors**（エラーのあるパケット）— 選択されたインタフェースから受信されたエラーパケットの数です。

統計の送信

- **Total Bytes**（**Octets**）（総バイト数（オクテット））— 選択されたインタフェースで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）— 選択されたインタフェースで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）— 選択されたインタフェースで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）— 選択されたインタフェースで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

□□□ **Interface Statistics**（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。

選択され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

□□□ **Interface Statistics**（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

次の表には、インタフェース統計を表示するための等価 CLI コマンドが説明されています。

表 **8-1** インタフェース統計 **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。

CLI コマンドの例は次のようになります。

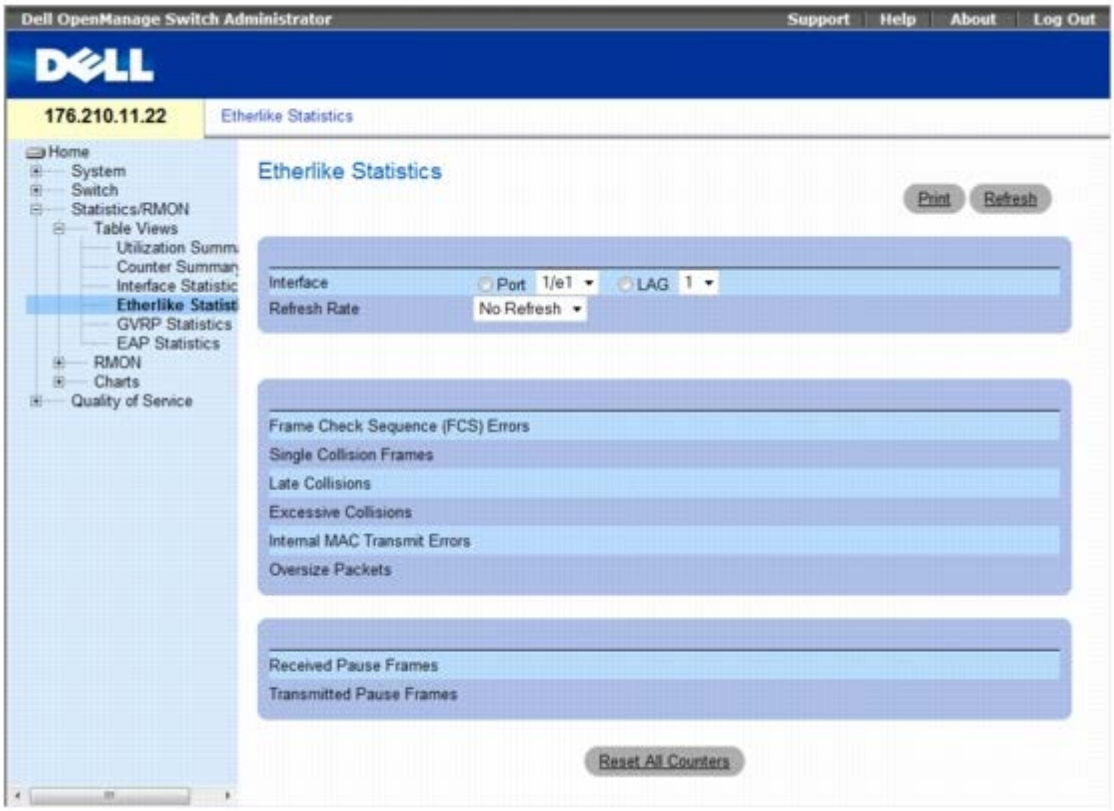
```
console> console enable
console# show interfaces counters
Port InOctets InUcastPkts InMcastPkts InBcastPkts
------ --------- ----------- ----------- -----------
1/e1 0 0 0 0
1/e2 0 0 0 0
1/e3 0 0 0 0
1/e4 0 0 0 0
1/e5 0 0 0 0
1/ e6 0 0 0 0
1/e7 0 0 0 0
1/e8 0 0 0 0
1/e9 0 0 0 0
1/e10 0 0 0 0
```

Etherlike 統計の表示

Etherlike Statistics （Etherlike 統計）ページにはインタフェースエラー統計が含まれます。

Etherlike Statistics（Etherlike 統計）ページを開くには、ツリー表示の **Statistics/RMON**（統計/RMON）® **Table Views**（表の表示）® **Etherlike Statistics**（Etherlike 統計）をクリックします。

図 **8-4. Etherlike** 統計



Etherlike Statistics （Etherlike 統計）ページには次のフィールドが含まれています。

- **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前に経過する時間です。可能なフィールド値は次のとおりです。
  - **15 Sec**（15 秒）— Etherlike 統計が 15 秒ごとにリフレッシュされることを示します。
  - **30 Sec**（30 秒）— Etherlike 統計が 30 秒ごとにリフレッシュされることを示します。
  - **60 Sec**（60 秒）— Etherlike 統計が 60 秒ごとにリフレッシュされることを示します。
  - リフレッシュなし — Etherlike 統計が自動的にリフレッシュされないことを示します。
- **Frame Check Sequence**（**FCS**）**Errors**（フレームチェックシーケンス（FCS）エラー）— 選択され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**（シングルコリジョンフレーム）— 選択されたインタフェースで受信されたシングルコリジョンフレームエラーの数です。
- **Late Collisions**（遅いコリジョン）— 選択されたインタフェースで受信された遅いコリジョンフレームの数です。

- **Internal MAC Transmit Errors**（内蔵 MAC 送信エラー）— 選択されたインタフェースにおける内蔵 MAC 送信エラーの数です。
- **Oversize Packets**（過大パケット）— 選択されたインタフェースにおける過大パケットの数です。
- **Received Pause Frames** （ポーズフレームの受信）— 選択されたインタフェースにおける受信されたポーズエラーの数です。
- **Transmitted Pause Frames**（送信されたポーズフレーム）— 選択されたインタフェースから送信されたポーズエラーの数です。

インタフェースの **Etherlike** 統計の表示

□□□ **Etherlike Statistics**（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 Statistics**（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

次の表には、Etherlike 統計を表示するための等価 CLI コマンドが説明されています。

表 **8-2. Etherlike** 統計 **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。

CLI コマンドの例は次のようになります。

```
Console# show interfaces counters ethernet 1/e1

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
```

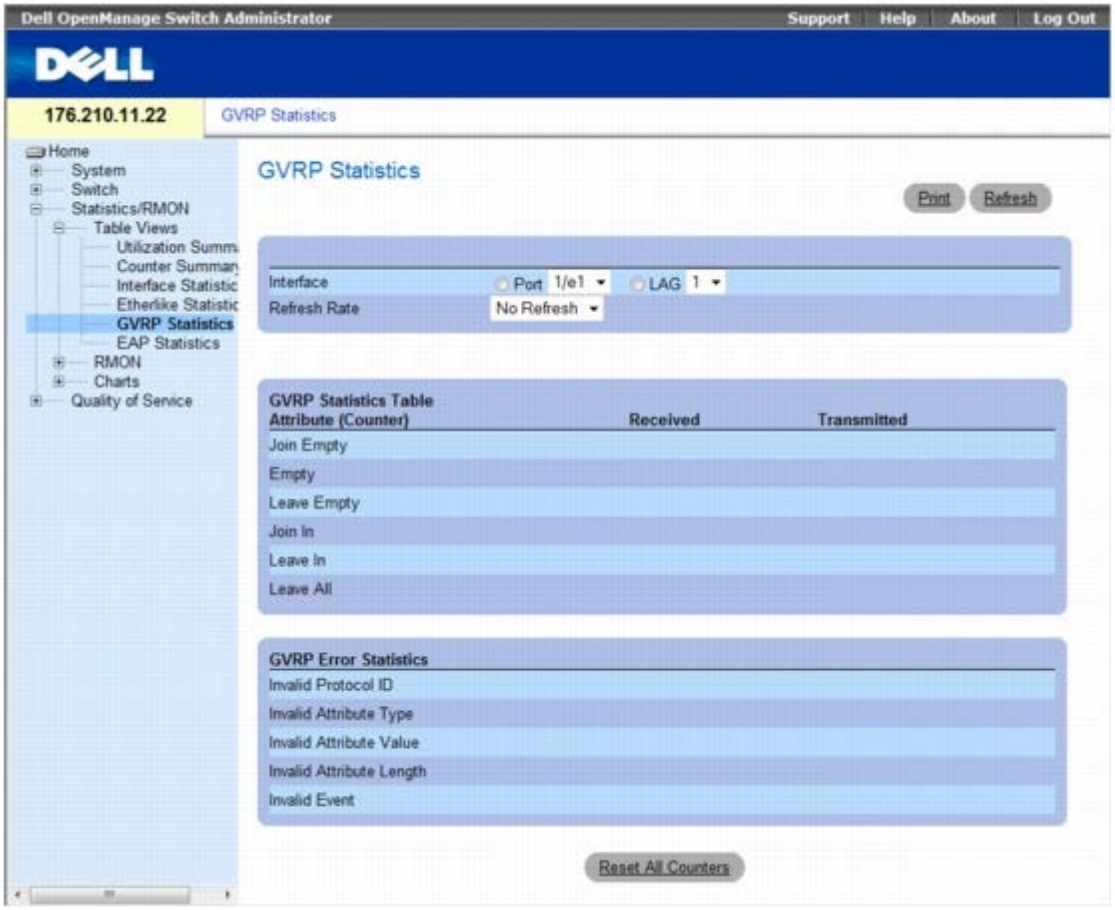
Late Collisions: 0	
Excessive Collisions: 0	
Internal MAC Tx Errors: 0	
Carrier Sense Errors: 0	
Oversize Packets: 0	
Internal MAC Rx Errors: 0	
Received Pause Frames: 0	
Transmitted Pause Frames: 0	

GVRP 統計の表示

GVRP Statistics（GVRP 統計）ページには、GVRP のデバイス統計が含まれます。

ページを開くには、ツリー表示の **Statistics/RMON**（統計/RMON）® **Table Views**（表の表示）® **GVRP Statistics**（GVRP 統計）をクリックします。

図 **8-5. GVRP** 統計



GVRP Statistics（GVRP 統計）ページには次のフィールドが含まれています。

- **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）— GVRP 統計がリフレッシュされる前に経過する時間です。可能なフィールド値は次のとおりです。
  - **15 Sec**（15 秒）— GVRP 統計が 30 秒ごとにリフレッシュされることを示します。
  - **30 Sec**（30 秒）— GVRP 統計が 30 秒ごとにリフレッシュされることを示します。

- **60 Sec**（60 秒）— GVRP 統計が 30 秒ごとにリフレッシュされることを示します。
- **No Refresh**（リフレッシュなし）— GVRP 統計が自動的にリフレッシュされないことを示します。

GVRP 統計表

- **Join Empty**（空への参加）— デバイス GVRP の空への参加統計です。
- **Empty** （空）— 空の GVRP 統計の数を示します。
- **Leave Empty**（空で残す）— デバイス GVRP の空で残す統計です。
- **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。

GVRP エラー統計

- **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 Statistics**（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。

選択され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 Statistics**（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

次の表には、GVRP 統計を表示するための等価 CLI コマンドが説明されています。

表 **8-3. GVRP** 統計 **CLI** コマンド

CLI コマンド	説明
show gvrp statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	GVRP 統計を表示します。
show gvrp error-statistics [**ethernet** *interface* | **port-channel** *port-channel-number*]	GVRP エラー統計を表示します。

CLI コマンドの例は次のようになります。

```
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
```

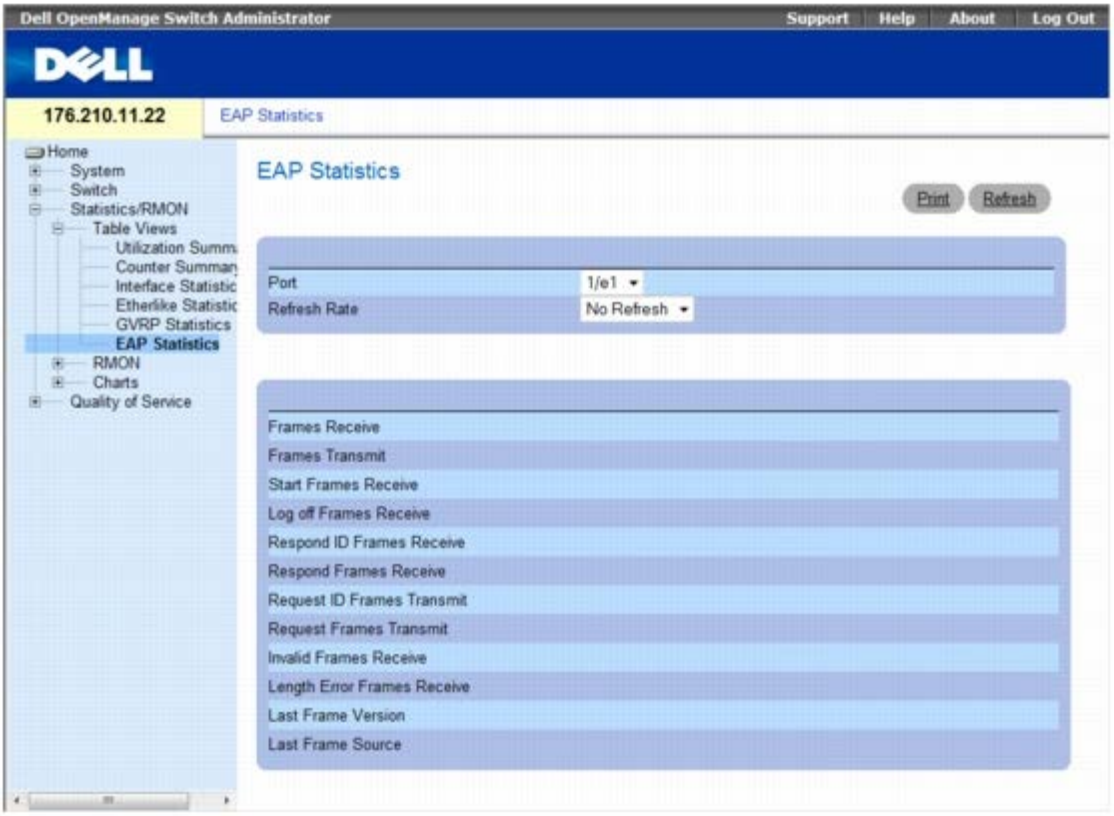
```
sLE : Leave Empty Sent
sLA : Leave All Sent
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA
---- --- ---- ---- ---- --- --- --- --- --- ---- --- ---
1/e1 0 0 0 0 0 0 0 0 0 0 0 0
1/e2 0 0 0 0 0 0 0 0 0 0 0 0
1/e3 0 0 0 0 0 0 0 0 0 0 0 0
1/e4 0 0 0 0 0 0 0 0 0 0 0 0
1/e5 0 0 0 0 0 0 0 0 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 Statistics（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 の詳細に関しては、ポートベース認証を参照してください。

EAP 統計ページを開くには、ツリー表示の **Statistics/RMON**（統計 /RMON）® **Table View**（表の表示）® **EAP Statistics**（EAP 統計）をクリックしてください。

図 **8-6. EAP** 統計



EAP 統計ページには次のフィールドが含まれています。

- **Port**（ポート）— 統計を得るためにポーリングされるポートです。
- **Refresh Rate**（リフレッシュレート）— EAP 統計がリフレッシュされる前に経過する時間です。可能なフィールド値は次のとおりです。

- **15 Sec**（15 秒）— EAP 統計が 15 秒ごとにリフレッシュされることを示します。
- **30 Sec**（30 秒）— EAP 統計が 30 秒ごとにリフレッシュされることを示します。
- **60 Sec**（60 秒）— EAP 統計が 60 秒ごとにリフレッシュされることを示します。
- **No Refresh**（リフレッシュなし）— EAP 統計が自動的にリフレッシュされないことを示します。

- **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 フレームの数を示します。
- **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 要求/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 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。
- **Invalid Frames Receive**（無効フレーム受信）— ポートで受信された認証されない 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**（最後のフレームのバージョン）— 最近受信された 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**（最後のフレームの送信元）— 最近受信された EAPOL フレームに付された送信元 MAC アドレスを示します。

ポートの **EAP** 統計の表示

□□□ **EAP Statistics**（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 Statistics**（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 統計の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 統計を表示するための CLI コマンドをまとめたものです。

表 **8-4. EAP** 統計 **CLI** コマンド

CLI コマンド	説明
show dot1x statistics	指定されたインタフェースの 802.1X 統計を表示します。

CLI コマンドの例は次のようになります。

```
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

Remote Monitoring（RMON）のページには、ネットワーク管理者がリモート環境からネットワーク情報を表示することができるリンクがあります。**RMON** ページを開くには、下記のリンクをクリックして、この画面に関するオンラインヘルプにアクセスしてください。

ツリー表示の **Statistics/RMON**（統計 /RMON）® **RMON** をクリックします。

この項には、次のトピックがあります。

- RMON 統計グループの表示
- RMON ヒストリ制御統計の表示
- RMON ヒストリ表の表示
- デバイス RMON イベントの定義
- RMON イベントログの表示
- RMON デバイスアラームの定義

RMON 統計グループの表示

RMON 統計ページで、デバイス利用率およびデバイスで発生したエラーに関する情報を表示します。**RMON** 統計ページを表示するには、ツリー表示の **Statistics/RMON**（統計 /RMON）® **RMON**® **Statistics**（統計）をクリックしてください。

図 **8-7 RMON** 統計

RMON 統計ページには次のフィールドが含まれています。

- **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前に経過する時間です。
- **Received Bytes**（**Octets**）（受信バイト数（オクテット））— 選択されたインタフェースで受信されたバイトの数です。
- **Received Packets**（受信パケット数）— 選択され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）— 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マルチキャストパケットの数です。
- **CRC & Align Errors**（調製エラー）— 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 および 調製エラーの数です。
- **Undersize Packets**（小型パケット）— 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（64 オクテット未満の）小型パケットの数です。
- **Oversize Packets**（大型パケット）— 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（1632 オクテット以上の）大型パケットの数です。
- **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で受信された、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）— 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（1632 オクテットより長いパケット）の数です。

- **Collisions**（コリジョン）— 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コリジョンの数です。
- **Frames of xx Bytes**（xx 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送信および受信された 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** 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

次の表には、EAP 統計を表示するための CLI コマンドが説明されています。

表 **8-5. RMON** 統計 **CLI** コマンド

CLI コマンド	説明
show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	RMON イーサネット統計を表示します。

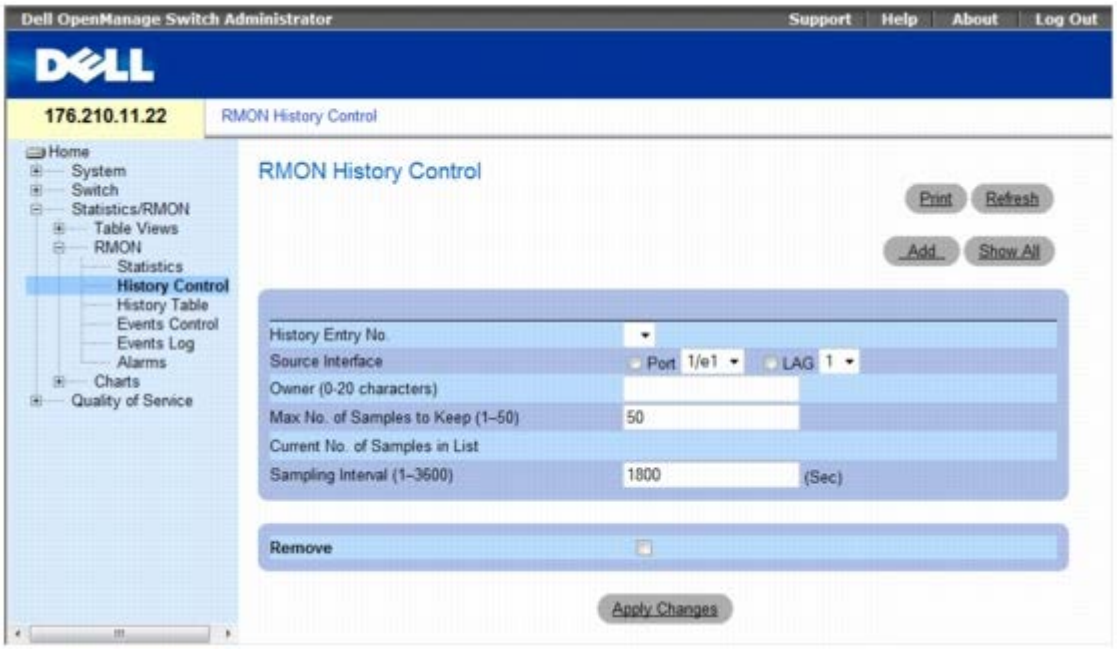
CLI コマンドの例は次のようになります。

```
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 1632 Octets: 389
```

RMON ヒストリ制御統計の表示

RMON History Control（RMON ヒストリ制御）ページには、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ます。**RMON History Control**（RMON ヒストリ制御）ページを開くには、ツリー表示の **Statistics/RMON**（統計 /RMON）® **RMON**® **History Control**（ヒストリ制御） をクリックします。

図 **8-8. RMON** ヒストリ制御



RMON ヒストリ制御ページには次のフィールドが含まれています。

- **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るポートまたは 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数（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** （リストにある現在のサンプル数）— 現在の取得サンプル数を示します。
- **Sampling Interval**（**1-3600**）（サンプリング間隔（1～3600））— ポートからサンプルを取る時間間隔を秒単位で示します。可能な値は 1～3600 秒です。デフォルトは 1800 秒（30 分）です。
- **Remove** — 選択されていると、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 History Control**（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。

Add History Entry（ヒストリエントリの追加）ページが開きます。

□□□ ダイアログ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 **History Control Table**（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 History Control**（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 History Control**（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

次の表には、RMON ヒストリ制御を表示するための等価 CLI コマンドが説明されています。

表 **8-6. RMON** ヒストリ **CLI** コマンド

CLI コマンド	説明
rmon collection history index [**owner** *ownername* | **buckets** *bucket-number*] [**interval** *seconds*]	インタフェースで RMON を有効化および設定します。
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。

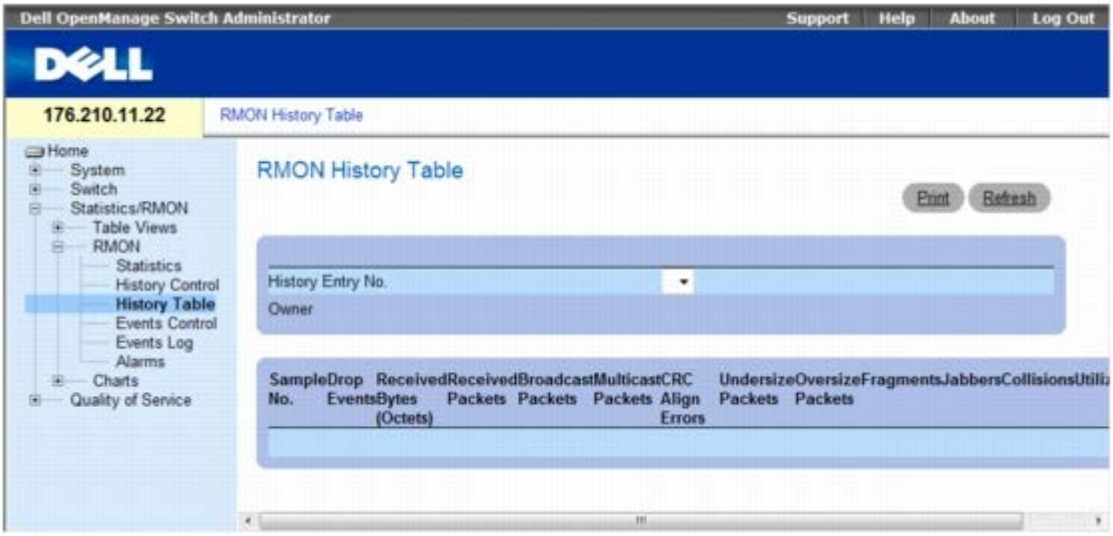
CLI コマンドの例は次のようになります。

```
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 History Table（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含まれます。各表のエントリは、一回のサンプル中に集計されたすべてのカウンタ値を表します。**RMON History Table**（RMON ヒストリ表）を開くには、ツリー表示の **Statistics/RMON**（統計/RMON）® **RMON® History Table**（ヒストリ表）をクリックします。

図 **8-9. RMON** ヒストリ表



RMON ヒストリ表ページには次のフィールドが含まれています。

RMON ヒストリ表の図 では RMON ヒストリ表のすべてのフィールドは表示されていません。

- **History Entry No.**（ヒストリエントリの番号）— ヒストリ制御 ページからエントリ番号を指定します。
- **Owner**（オーナー）— RMON 情報を要求した RMON ステーションまたはユーザーを示します。
- **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番号を示します。
- **Drop Events**（破棄イベント）— サンプリング間隔中にネットワークリソースの不足によって破棄されたパケットの数を示します。これは破棄されたパケットの正確な数ではなく、破棄されたパケットが検出された回数を表わすことがあります。
- **Received Bytes**（**Octets**）（受信バイト（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を示します。
- **Received Packets**（受信パケット）— サンプリング間隔中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）— サンプリング間隔中に受信された正常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）—サンプリングセッション中に受信された 64～1632 オクテット長のパケットの数です。ただし、パケットには整数のオクテットを持つ不良のフレームチェックシーケンス（FCS）、または非整数の不良 FCS があります。
- **Undersize Packets**（過小パケット）— サンプリングセッション中に受信された 64 オクテット未満のパケットの数です。
- **Oversize Packets**（過大パケット）— サンプリングセッション中に受信された 1632 オクテットより大きいパケットの数です。
- **Fragments**（フラグメント）— サンプリングセッション中に受信された 64 オクテット未満で FCS のあるパケットの数です。
- **Jabbers**（ジャバ）— サンプルセッション中に受信された 1632 オクテットより大きく、FCS のあるパケットの数です。
- **Collisions**（コリジョン）— サンプリングセッション中に発生したパケットコリジョンの合計数の概算です。コリジョンは、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ポートが検知した際に検出されます。
- **Utilization**（利用率）— サンプリング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 History Table**（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。

エントリ統計を RMON ヒストリ表で表示します。

CLI コマンドを使用した RMON ヒストリ制御の表示

次の表には、RMON ヒストリを表示するための等価 CLI コマンドが説明されています。

表 **8-7. RMON** ヒストリ制御 **CLI** コマンド

CLI コマンド	説明
show rmon history *index* {**throughput	errors	other**}_[**period** *seconds*]	RMON イーサネット統計ヒストリを表示します。

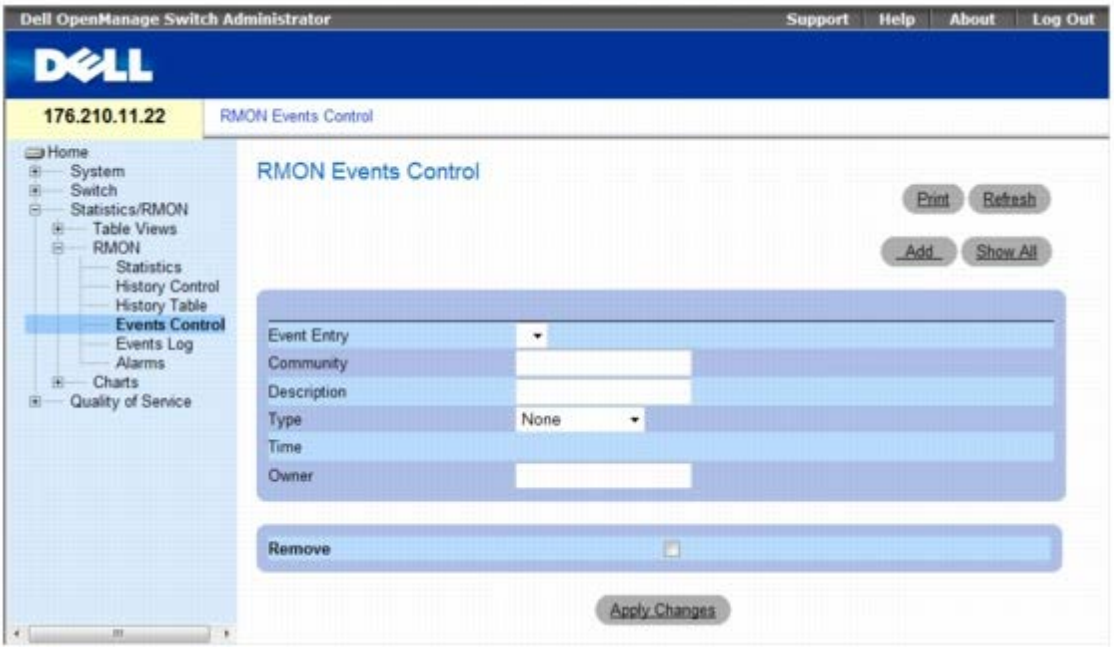
次に、索引 1 のスループットの RMON イーサネット統計を表示するための CLI コマンドの例を示します。

```
console> 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 Events Control（RMON イベント制御）ページを利用して、RMON イベントを定義します。**RMON Events Control**（RMON イベント制御）ページを開くには、ツリー表示の **Statistics/RMON**（統計/RMON）® **RMON® Events Control**（イベント制御）をクリックします。

図 **8-10. RMON** イベント制御



RMON Events Control（RMON イベント制御）ページには次のフィールドが含まれています。

- **Event Entry** （イベントエントリ）— イベントを表示します。
- **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。可能な値は次のとおりです。
  - **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**（時間）— イベントが発生した時間です。
- **Owner**（オーナー）— 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）—選択されていると、**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 Events Control**（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。

Add an Event Entry（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 Changs**（変更の適用）をクリックします。

Event Table（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 Events Control**（RMON イベント制御）ページを開きます。

□□□ **Event Table**（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 Changs**（変更の適用）をクリックします。

Event Table（イベント表）エントリが変更され、デバイスがアップデートされます。

RMON イベントエントリの削除

RMON Events Control>（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、このページから単一のイベントエントリを削除できます。

□□□ **RMON Events Control**（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 Events Table（RMON イベント表）ページが開きます。

□□□ 削除の必要があるイベントで **Remove**（削除）を選択してから **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デバイスイベントの定義

次の表には、デバイスイベントを定義するための等価 CLI コマンドが説明されています。

表 **8-8.** デバイスイベントの定義 **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。

CLI コマンドの例は次のようになります。

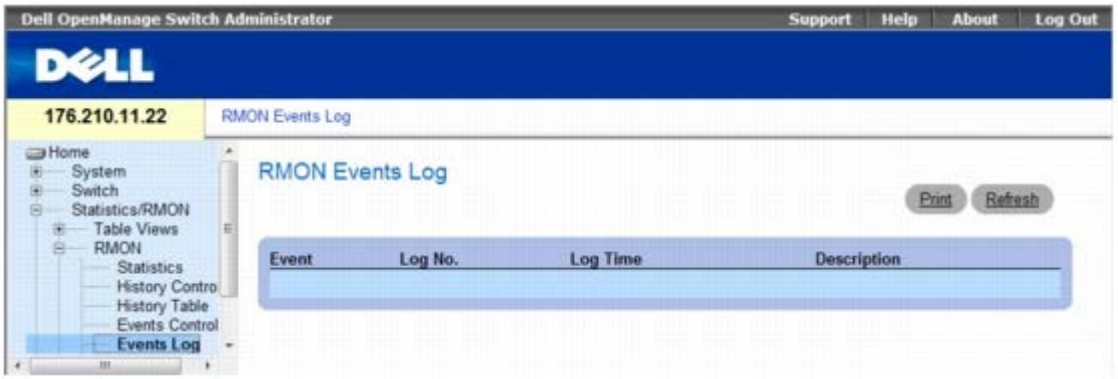
```
console(config)# rmon event 1 log
console(config)# exit
console# show rmon events
```

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 Events Log（RMON イベントログ）ページには、RMON イベントのリストがあります。**RMON Events Log**（RMON イベントログ）ページを開くには、ツリー表示の **Statistics/RMON**（統計 /RMON）® **RMON® Events Log**（イベントログ）をクリックします。

図 **8-11. RMON** イベントログ



RMON Events Log（RMON イベントログ）ページには次のフィールドが含まれています。

- **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間です。
- **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

次の表には、デバイスイベントを定義するための等価 CLI コマンドが説明されています。

表 **8-9.** デバイスイベントの定義 **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。

CLI コマンドの例は次のようになります。

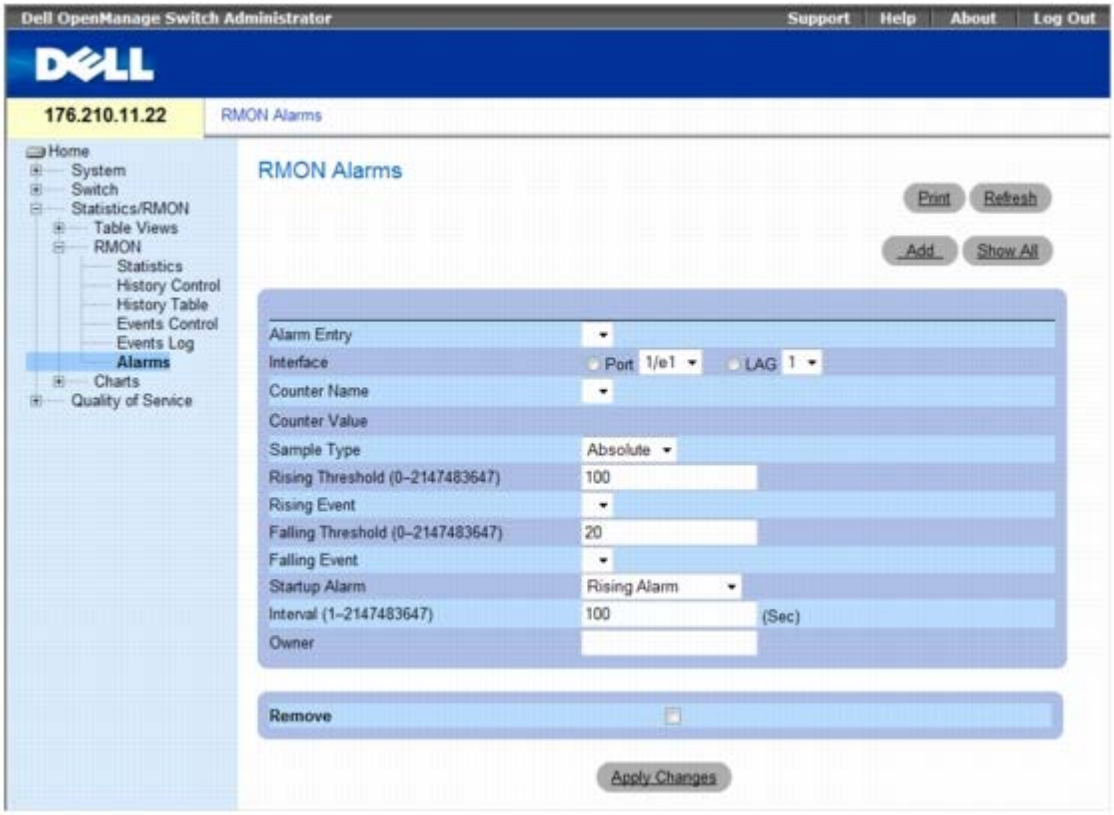
```
console(config)# rmon event 1 log
Console> show rmon log
Maximum table size: 500
Event Description Time
----- ---------- ----- --------------
1 Errors Jan 18 2002 23:58:17
2 High Broadcast Jan 18 2002 23:59:48
```

RMON デバイスアラームの定義

RMON Alarms（RMON アラーム）ページを利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、ネットワークの問題、または、イベントが検知されたときに生成されます。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。イベントの詳細に関しては、RMON イベントログの表示を参照してください。

RMON Alarms（RMON アラーム）ページを開くには、ツリー表示の **Statistics/RMON**（統計/RMON）® **RMON® Alarms**（アラーム）をクリックします。

図 **8-12. RMON** アラーム



The **RMON Alarms**（RMON アラーム）ページには次のフィールドが含まれています。

- **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です。
- **Counter Name** —（カウンタ名）— 選択された MIB 変数を示します。
- **Counter Value**（カウンタ値）— 選択された MIB 変数の値です。
- **Sample Type**（サンプルタイプ）— 選択され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次のとおりです。
  - **Delta**（デルタ）— 現在の値から最後にサンプリング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）— サンプリング間隔の最後に値をしきい値と直接比較します。
- **Rising Threshold**（**0**～**2147483647**）（上昇しきい値（0～2147483647））— 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。それぞれのモニタされた変数には指定された色があります。フィールドデフォルト値は 100 秒です。
- **Rising Event**（上昇イベント）— ログ、トラップ、またはその両方を含むアラームが報告される機構です。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と、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 トラップが生じ、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**～**2147483647**）（下降しきい値（0～2147483647））— 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。それぞれのモニタされた変数には指定された色があります。フィールドデフォルトは 20 です。
- **Startup Alarm**（スタートアップアラーム）— アラームの発生を有効化する引き金です。上昇は、低しきい値から高しきい値までのしきい値を超えることによって定義されます。
- **Interval**（**1**～**2147483647**）（**sec**）（間隔（1～2147483647）（秒））— アラームの時間間隔です。フィールドデフォルト値は 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）— 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 Alarms**（RMON アラーム）ページを開きます。

□□□ **Add**（追加）をクリックします。

Add an Alarm Entry（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。

□□□ フィールドを完成させます。

□□□ **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、デバイスがアップデートされます。

アラーム表エントリの変更

□□□ **RMON Alarms**（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 Alarms**（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。

Alarms Table（アラーム表）が開きます。

アラーム表エントリの削除

□□□ **RMON Alarms**（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）の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

次の表には、デバイスアラームを定義するための等価 CLI コマンドが説明されています。

表 **8-10.** デバイスアラーム **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 アラーム設定を表示します。

CLI コマンドの例は次のようになります。

```
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

Chart（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。ページを開くには、ツリー表示の **Statistics**（統計）® **Charts**（チャート）をクリックします。

本項には、次のトピックがあります。

ポート統計の表示

Port Statistics（ポート統計）ページを利用してポート要素の統計をチャート形式で開きます。**Port Statistics**（ポート統計）ページを開くには、ツリー表示で **Statistics/RMON**（統計 /RMON）® **Charts® Port Statistics**（ポート統計）をクリックします。

図 **8-14.** ポート統計

Port Statistics（ポート統計）ページには次のフィールドが含まれています。

- **Unit No.**（ユニット番号）— 表示されている統計の対象であるスタッキングユニットの番号を示します。
- **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 統計のタイプを選択します。
- **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前に経過する時間です。

ポート統計の表示

□□□ **Port Statistics**（ポート統計）ページを開きます。

□□□ 統計タイプを選択して開きます。

□□□ **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。

選択され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

次の表には、EAP 統計を表示するための CLI コマンドが説明されています。

表 **8-11.** ポート統計 **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 イーサネット統計を表示します。
show gvrp statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	GVRP 統計を表示します。
show gvrp-error statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	GVRP エラー統計を表示します。

LAG 統計の表示

LAG Statistics（LAG 統計）ページを利用して LAG の統計をチャート形式で開きます。**LAG Statistics**（LAG 統計）ページを開くには、ツリー表示の **Statistics/RMON**（統計 /RMON）® **Charts**（チャート）® **LAG Statistics**（LAG 統計）をクリックします。

図 **8-15. LAG** 統計

LAG Statistics（**LAG** 統計）ページには次のフィールドが含まれています。

- **Interface Statistics** （インタフェース統計）— インタフェース統計を選択して開きます。
- **Etherlike Statistics**（Etherlike 統計）— Etherlike 統計を選択して開きます。
- **RMON Statistics**（RMON 統計）— RMON 統計を選択して開きます。
- **GVRP Statistics** （GVRP 統計）— GVRP 統計のタイプを選択して開きます。
- **Refresh Rate**（リフレッシュレート）— 統計がリフレッシュされる前に経過する時間です。

LAG 統計の表示

□□□ **LAG Statistics**（LAG 統計）ページを開きます。

□□□ 統計タイプを選択して開きます。

□□□ **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。

選択され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

次の表には、EAP 統計を表示するための CLI コマンドが説明されています。

表 **8-12. LAG** 統計 **CLI** コマンド

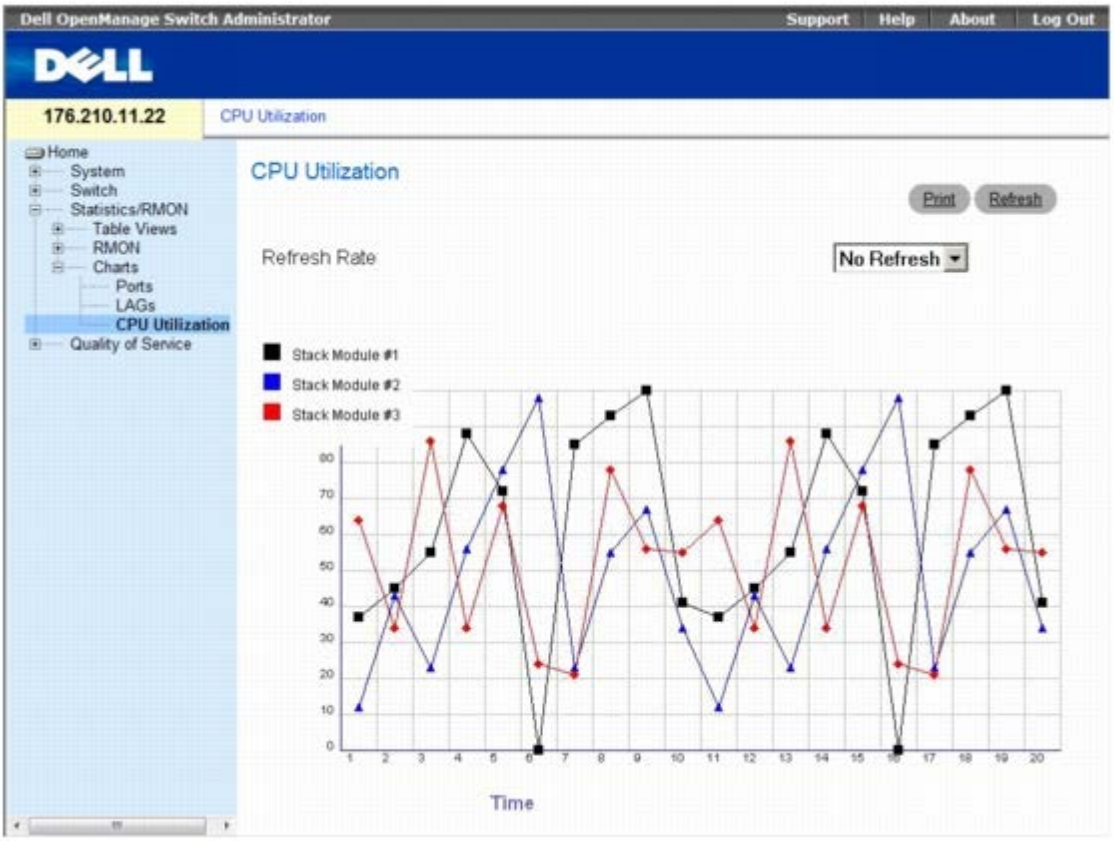
CLI コマンド	説明
show interfaces counters [**ethernet** *interface* | **port-channel** *port-channel-number*]	物理的なインタフェースで検出されたトラフィックを表示します。
show rmon statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	RMON イーサネット統計を表示します。
show gvrp statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	GVRP 統計を表示します。
show gvrp-error statistics {**ethernet** *interface* | **port-channel** *port-channel-number*}	GVRP エラー統計を表示します。

CPU 利用率の表示

CPU Utilization（CPU 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、グラフの色が設定されます。

CPU Utilization（CPU 利用率）ページを開くには、ツリー表示の **Statistics/RMON**（統計/RMON）® **Charts**（チャート）® **CPU Utilization**（CPU 利用率）をクリックします。

図 **8-16. CPU** 利用率



CPU Utilization（CPU 利用率）ページには、次の情報があります。

- **Refresh Rate**（リフレッシュレート）— 統計がリフレッシュされる前に経過する時間です。

CLI コマンドを使用した CPU 利用率の表示

次の表は、CPU 利用率を表示するための等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
`show cpu utilization`	CPU 利用率を表示します。

CLI コマンドの例は次のようになります。

```
Console# show cpu utilization
CPU utilization service is on.


CPU utilization
---------------------------
five seconds: 5%; one minute: 3%; five minutes: 3%
```

目次に戻る

目次に戻る

サービス品質の設定

Dell™ PowerConnect™ 35xx 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。**Quality of Service** （サービス品質）ページを開くには、ツリー表示の **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）は、ネットワーク内に QoS と優先度キューを実装する能力を提供します。

QoS を必要とする実装例には、音声、ビデオ、およびリアルタイムトラフィックといった種類のトラフィックがあります。これらのトラフィックに優先度の高いキューを割り当てる一方、他のトラフィックには優先度の低いキューを割り当てることができます。実装によって、要求度の高いトラフィックのフローが向上します。

QoS は、次の項目によって定義されます。

- **Classification**（分類）— 特定の値に一致しているパケットフィールドを指定します。ユーザー定義の仕様に一致するすべてのパケットは一緒に分類されます。
- **Action**（アクション）— 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（VPT）使って、パケットを出口キューの 1 つにマッピングすることによりパケットを分類します。VLAN 優先度タグによるキューの割り当ては、ユーザーが定義できます。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。

CoS 値	転送するキューの値
0	q2
1	q1（最低の優先度）
2	q1（最低の優先度）
3	q2
4	q3
5	q3
6	q4
7	q4

タグなしで到着するパケットには、デフォルトの VPT 値が割り当てられます。デフォルト値はポートごとに設定されます。割り当てられた VPT は、パケットを出口キューにマッピングする際に使用されます。

DSCP 値は、優先度キューにマッピングできます。次の表は、出口キュー値に対する DSCP マッピングのデフォルト設定を示します。

DSCP 値	転送するキューの値
0-15	q1（最低の優先度）

16-31	q2
32-47	q3
48-63	q4

DSCP マッピングは、システムごとに有効になります。

この項には、次のトピックがあります。

- CoS サービス

CoS サービス

パケットを特定の出口キューに割り当てた後、CoS サービスをキューに割り当てることができます。出口キューには、次の方法のいずれかによるスケジューリング方法を設定することができます。

- **Strict Priority**（厳密優先）— 時間に依存するアプリケーションは、常に転送されるようにします。厳密優先（SP）を使用すれば、時間に依存する基幹業務のトラフィックを、時間に依存しないアプリケーションに優先させることができます。
  たとえば、厳密優先を設定すると、IP 上の音声トラフィックが優先されるので、FTP トラフィックや E-メール（SMTP）トラフィックより先に転送されます。

- **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。すべてのキューは WRR または SP キューに設定できます。WRR を選択すると、1、2、4、8 の荷重がキューに割り当てられます。

QoS のグローバル設定

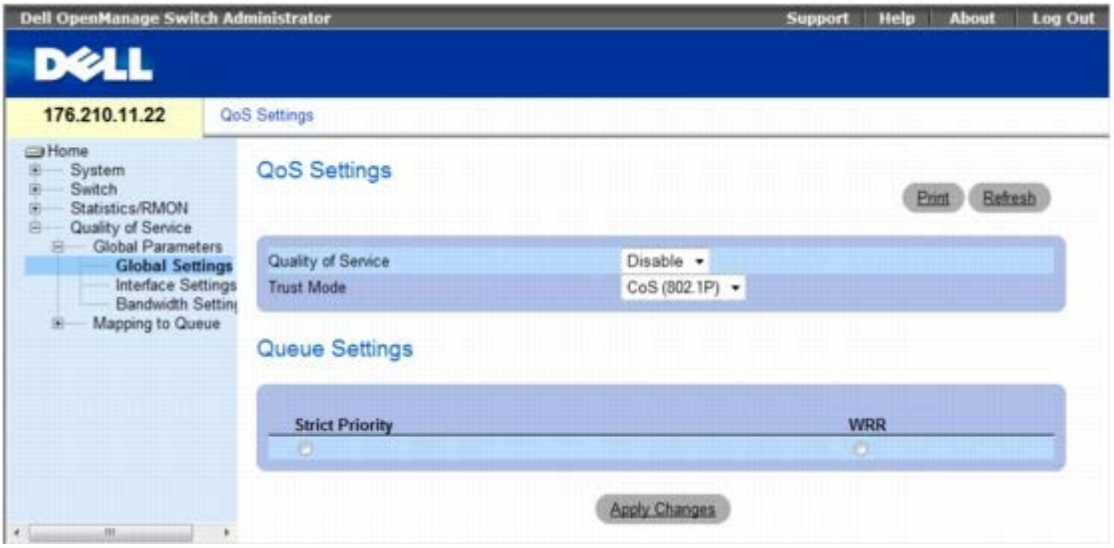
サービス品質（QoS）は、ネットワーク内に QoS と優先度キューを実装する能力を提供します。

Global Settings（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。また、信頼モードを選択するためのフィールドもあります。信頼モードでは、パケット内の事前定義フィールドに依存して出口キューが決定されます。

さらに、**Global Settings**（グローバル設定）ページでは、厳密優先（SP）または荷重ラウンドロビン（WRR）のいずれかにキューを定義することもできます。

Global Settings（グローバル設定）ページを開くには、ツリー表示で **Quality of Service**（サービス品質）® **QoS Parameters**（QoS パラメータ）® **Global Settings**（グローバル品質）とクリックします。

図 **9-1.** グローバル設定



The **Global Settings**（グローバル設定）ページには次の項が含まれています。

- QoS 設定
- キュー設定

QoS 設定

- **Quality of Service**（サービス品質）— QoS を使用した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使用するパケットフィールドを確定します。ルールが定義されていない場合、選択した信頼モードに応じて、事前定義の CoS または DSCP パケットフィールドを含むトラフィックがマッピングされます。事前定義のパケットフィールドを含まないトラフィックは、ベストエフォートのキュー（q2）にマッピングされます。可能な Trust（信頼）モードフィールドの値は次のとおりです。
  - **CoS**（802.1p）— 出口キュー割り当ては、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の VPT によって確定します。デバイスのデフォルトは IEEE802.1p です。
  - **DSCP** — 出口キューの割り当ては、DSCP フィールドによって決定されます。

メモ： インタフェースの Trust（信頼）設定はグローバルの Trust（信頼）設定に優先します。

キュー設定

- **Strict Priority** （厳密優先）— 選択されると、システムキューが SP キューであることを示します。
- **WRR**（荷重ラウンドロビン）— 選択されると、システムキューが WWR キューであることを示します。

サービス品質を有効にするには、次の手順を実行します

□□□ **Global Settings**（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。

CoS は、デバイスごとに有効になります。

信頼モードを有効にするには：

□□□ **Global Settings**（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。

デバイスで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 **Global Settings**（グローバル設定）ページでフィールドを設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
qos trust [cos | dscp]	システムを Trust（信頼）モードに設定します。
no qos trust	非 Trust（信頼）状態に戻します。

CLI コマンドの例は次のようになります。

```
console(config)# qos trust dscp
```

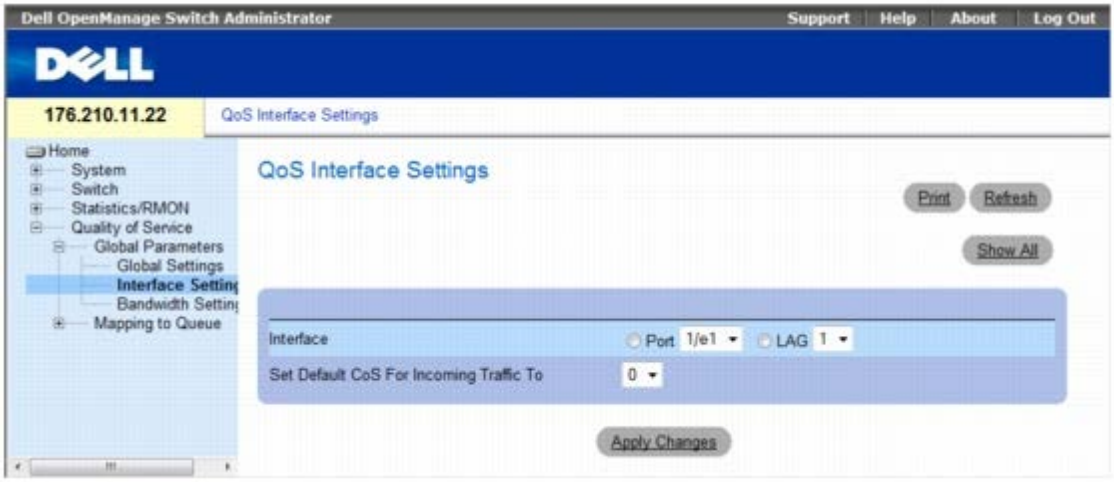
本項には、次のトピックが含まれています。

- QoS インタフェース設定の定義
- 帯域幅設定の定義
- CoS 値からキューへのマッピング
- DSCP 値のキューへのマッピング

QoS インタフェース設定の定義

Interface Settings（インタフェース設定）ページには、Trust（信頼）モードを非アクティブにするためのフィールド、およびタグなしの入力パケットにデフォルトの CoS 値を設定するためのフィールドがあります。**Interface Settings**（インタフェース設定）ページを開くには、ツリー表示の **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）をクリックします。

図 **9-2.** インタフェース設定



Interface Settings（インタフェース設定）ページには次のフィールドが含まれています。

- **Interface**（インタフェース）— 設定を行うポートまたは LAG です。
- **Disable 「Trust」 Mode on Interface**（インタフェースの「Trust」（信頼）モードを無効にする）— 指定のインタフェースの 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デフォルト Cos を設定）— タグなしパケットに対してデフォルトの 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。

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

□□□ **Interface Settings**（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 設定を表示するには、次の手順を実行します

□□□ **Interface Settings**（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インタフェースへの **QoS** 割り当て

次の表は、 **Interface Settings**（インタフェース設定）ページのフィールドを設定する場合の相当する CLI コマンドを示します。

CLI コマンド	説明
qos trust	Trust（信頼）モードを有効にします。
no qos trust	ポートごとに Trust（信頼）状態を無効にします。

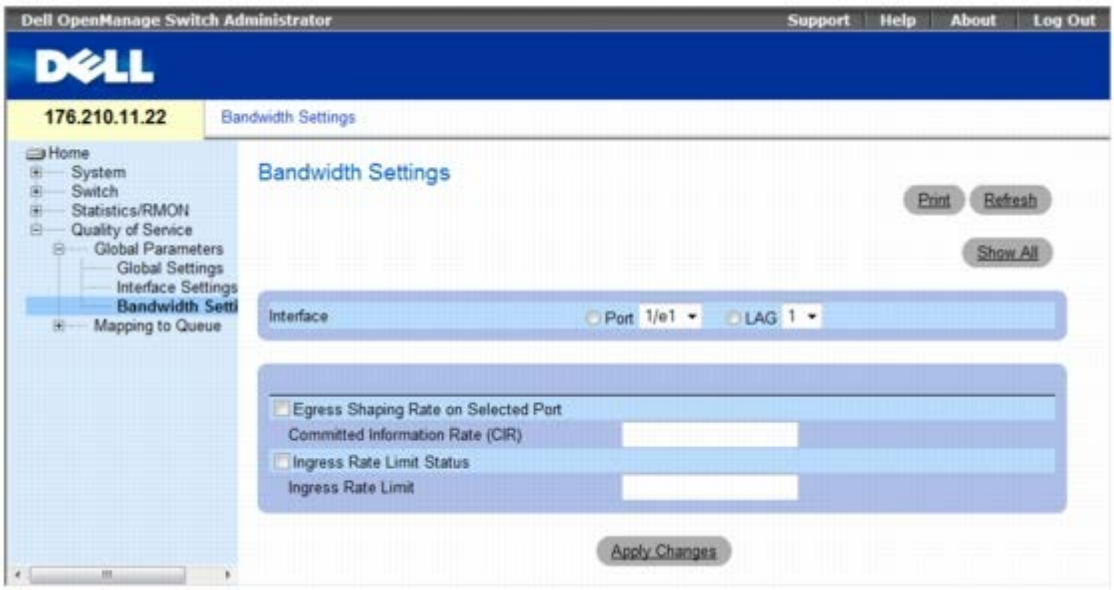
CLI コマンドの例は次のようになります。

```
console(config)# interface ethernet 1/e15

console(config-if)# qos trust
```

帯域幅設定の定義

Bandwidth Settings（帯域幅設定）ページには、特定の出力インタフェースに対する帯域幅設定を定義するためのフィールドがあります。キューのスケジューリングを変更すると、キュー設定全体に影響します。キューのシェイピングは、キューごとかインタフェースごと、あるいはその両方を基準に設定できます。シェイピングは、低い方の指定値によって決定します。キューのシェイピングタイプは、Bandwidth Settings（帯域幅設定）ページで選択します。このページを開くには、ツリー表示で **Quality of Service**（サービス品質）® **CoS Global Parameters**（CoS グローバルパラメータ）® **Bandwidth Settings**（帯域幅設定）をクリックします。

図 **9-3.** 帯域幅設定



- **Interface**（インタフェース）— 表示されるポートまたは LAG を示します。
- **Egress Shaping Rate on Selected Port**（選択したポートに対する出口レートシェイピングレート）— インタフェースに対する出力トラフィックの制限ステータスを示します。
  - Checked（チェックマークあり）— 出力トラフィック制限が有効です。
  - Not Checked（チェックマークなし）— 出力トラフィック制限が無効です。
- **Committed Information Rate**（**CIR**）（認定情報レート（CIR））— インタフェースに対する出力 CIR トラフィック制限を定義します。
- **Ingress Rate Limit Status**（受信レート上限値ステータス）— インタフェースに対する受信トラフィック制限ステータスを示します。
  - Checked（チェックマークあり）— 受信トラフィック制限が有効です。
  - Not Checked（チェックマークなし）— 受信トラフィック制限が無効です。
- **Ingress Rate Limit**（受信レート上限値）— インタフェースに対する受信トラフィック制限を定義します。

インタフェースに帯域幅設定を割り当てるには、次の手順を実行します

□□□ **Bandwidth Settings**（帯域幅設定）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。

帯域幅設定が、インタフェースに割り当てられます。

帯域幅設定表を表示するには、次の手順を実行します

□□□ **Bandwidth Settings**（帯域幅設定）ページを開きます。

□□□ **Show All**（すべてを表示）をクリックします。

帯域幅設定表が開きます。

図 **9-4.** 帯域幅設定表

CLI コマンドを使用した帯域幅設定の割り当て

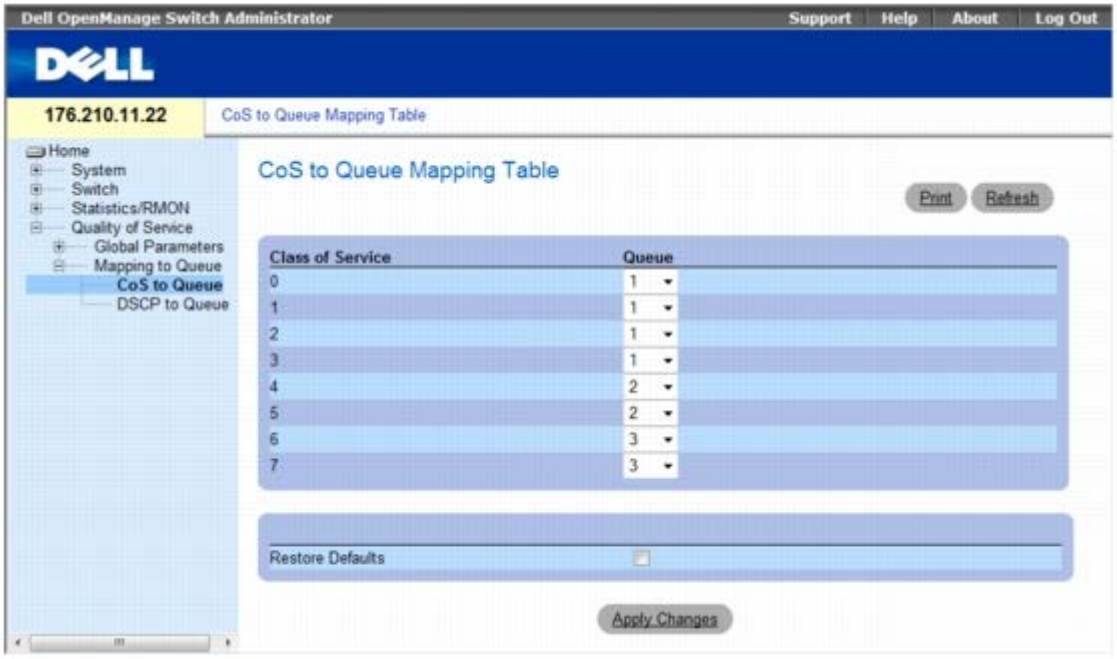
次の表は、 **Bandwidth Settings**（帯域幅設定）ページのフィールドを設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
traffic-shape *committed-rate* [*committed-burst*] no traffic-shape	出力ポートにシェイパを設定します。シェイパを無効にするには、no 形式を使用します。
rate-limit *rate* no rate-limit	受信トラフィックのレートを制限します。レート制限を無効にするには、**no** 形式を使用します。

CoS 値からキューへのマッピング

CoS to Queue（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分類するためのフィールドがあります。**CoS to Queue**（キューへの CoS）ページを開くには、ツリー表示の **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 CoS）をクリックします。

図 **9-5.** キューへの **CoS**



CoS to Queue（キューへの CoS）ページには次のフィールドが含まれています。

- **Class of Service**（サービスクラス）— CoS 優先度タグ値を指定します。最低は 0、最高は 7 です。
- **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 値を出口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

□□□ **CoS to Queue**（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、 **CoS to Queue**（キューへの CoS）ページのフィールドを設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
wrr-queue cos-map *queue-id cos0.cos7*	割り当てられた CoS 値を出口キューにマッピングします。

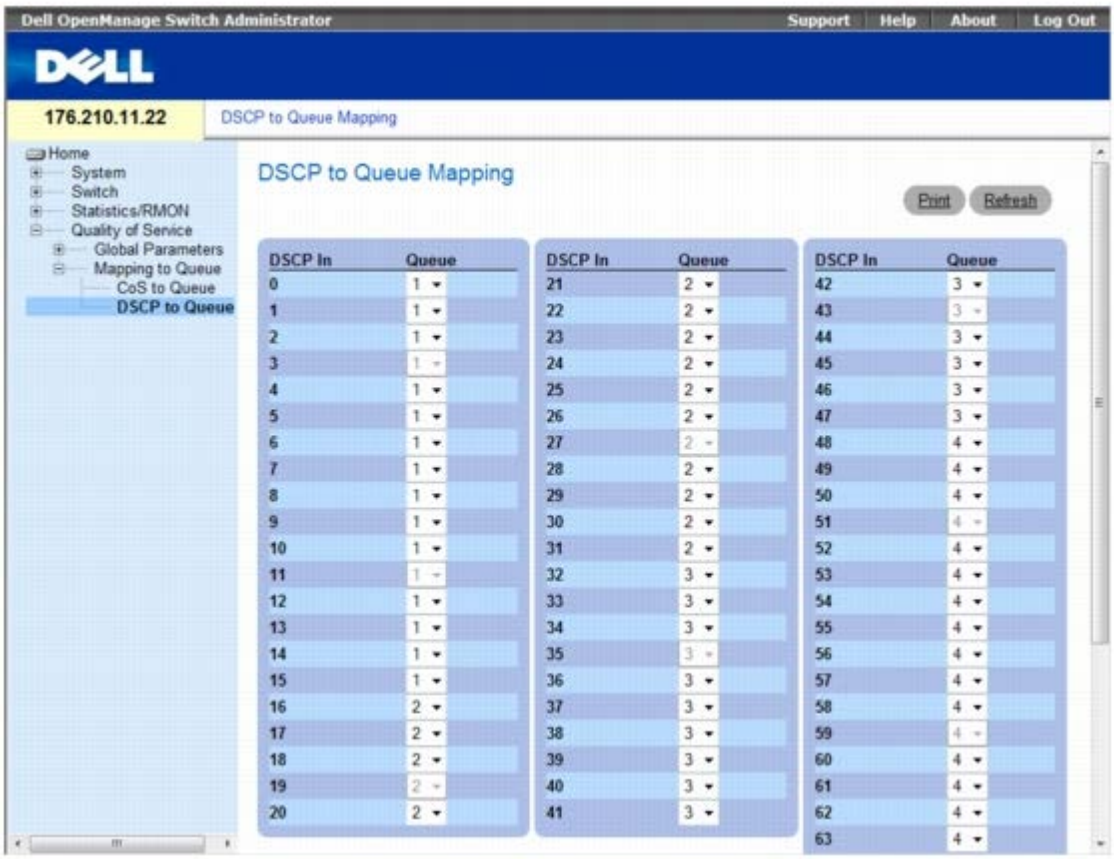
CLI コマンドの例は次のようになります。

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

DSCP 値のキューへのマッピング

DSCP to Queue（キューへの DSCP）ページでは、特定の DSCP フィールドに出口キューを定義するためのフィールドを提供します。**DSCP to Queue**（キューへの DSCP）ページを開くには、ツリー表示の **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）とクリックします。

図 **9-6. DSCP** に対するキュー



DSCP to Queue（キューへの DSCP）ページには次のフィールドが含まれています。

- **DSCP In**（着信 DSCP）— 着信パケット内の DSCP フィールドの値。
- **Queue**（キュー）— 特定の DSCP 値を持つパケットに割り当てられるキュー。可能な値は 1～4 です。最低値は 1、最高値は 4 です。
- **Restore Defaults**（デフォルトの復元）— CoS 値を出口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。

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

□□□ **DSCP to Queue**（DSCP に対するキュー）ページを開きます。

□□□ **DSCP In**（着信 DSCP）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、出口キューに値が割り当てられます。

CLI コマンドを使用した DSCP 値の割り当て

次の表は、 **DSCP to Queue**（DSCP に対するキュー）ページのフィールドを設定する場合の等価 CLI コマンドをまとめたものです。

CLI コマンド	説明
qos map dscp-queue *dscp-list* **to** *queue-id*	DSCP に対するキューのマッピングを変更します。

CLI コマンドの例は次のようになります。

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

目次に戻る

目次に戻る

用語集

Dell™ PowerConnect™ 35xx システムユーザーズガイド

この用語集では、対象となる主要な技術用語を解説します。

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W | あ | か | さ | た | な | は | ま | や | ら | わ

A

ACL

Access Control List の略。ネットワーク管理者は、特定の入口ポートに対する分類処置および規則を定義できます。

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（管理タグ）

スイッチモジュールに関するユーザー定義のリファレンスを指定します。

B

BootP

Bootstrap Protocol の略。 ワークステーションは、自分の 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ブートエリアにロードされた設定ファイルを検出できます。

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内でスイッチモジュールをまたがって送信されます。BPDU パケットには、ポート、アドレス、優先度、および転送コストの情報が含まれます。

C

CDB

Configuration Data Base の略。デバイスの設定情報が保存されたファイルです。

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です。CLI の使用法の詳細に関しては、「**Using the CLI**（CLI の使い方）」を参照してください。

CPU

Central Processing Unit の略。 コンピュータの中で情報を処理する部分です。CPU は、コントロールユニットと ALU で構成されています。

D

DHCP クライアント

DHCP を使ってネットワークアドレスなどの設定パラメーターを取得するデバイスです。

DHCP スヌーピング

DHCP スヌーピングは、信頼できないインタフェースと DHCP サーバーの間にファイアウォールセキュリティを提供することによって、ネットワークのセキュリティを強化します。

DRAC/MC

DRAC/MC。Dell モジュラーサーバーシステムコンポーネントに対する単一の制御ポイントを提供します。

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。

E

EWS

Embedded Web Server の略。 標準のウェブ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、または代わりとして使用されます。

F

FFT

Fast Forward Table の略。 転送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 はパケットを転送して、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。

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。

GVRP

GARP VLAN Registration Protocol の略。クライアントステーションを VLAN 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、行の終わりのパケットより先に転送されます。

HTTP

HyperText Transport 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 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。

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。

IGMP スヌーピング

IGMP スヌープ機能は、デバイスによってワークステーションからアップストリームのマルチキャストルータに転送される際に、IGMP フレームの内容を検査します。デバイスは対象のフレームから、マルチキャストルータがマルチキャストフレームを送信する、マルチキャストセッションに設定されたワークステーションを識別します。

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。

IP バージョン **6**（**IPv6**）

従来の IPv4 よりも長いアドレスを持つ IP バージョン。IPv4 アドレスの長さは 32 ビットでしたが、IPv6 アドレスは 128 ビットです。したがって、より拡大されたアドレス空間を持つことができます。

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。

ISATAP

Intra-Site Automatic Tunnel Addressing Protocol の略。
ISATAP は、基盤となる IPv4 ネットワークを IPv6 向けの非ブロードキャスト/マルチキャストアクセスリンクレイヤとして使用する、オーバーレイ自動トンネルメカニズムです。ISATAP は、ネイティブの IPv6 インフラストラクチャをまだ使用できないサイト内での IPv6 パケットの転送用に設計されています。

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 の詳細に関しては、「**Defining LAG Membership**（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。

LLDP-MED

Link Layer Discovery Protocol **-** Media Endpoint Discovery の略。LLDP は、ネットワーク管理者が、マルチベンダ環境のネットワークトポロジを検出および保持することによって、トラブルシューティングを行い、ネットワーク管理を強化できるようにします。MED は、1 つの LLDP ネットワーク上で異なる IP システムが共存できるようにすることで、ネットワークの柔軟性を向上させます。

M

MAC アドレス

Media Access Control アドレスの略。 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 アドレスラーニング

MAC アドレスラーニングは、パケットの送信元 MAC アドレスが記録されるラーニングブリッジの特性です。記録されているアドレスが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が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 アドレスラーニングによって、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 層

データリンク制御（DTL）層の副層です。

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 が変化したもので、MD4 のセキュリティを増加します。MD5 は、通信の保全性を検証し、通信の発信元の認証を行います。

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。 ハブおよび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。

N

NA

Neighbor Advertisement の略。

ND

Neighbor Discovery の略。

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。

NS

Neighbor Solicitation の略。

O

OID

Organizationally Unique Identifiers の略。音声 VLAN に関連付けられた識別子です。

OUI

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

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。パケットは、別の IP アドレスに送信されて、応答を待ちます。

PVE

Protocol VLAN Edge の略。ポートをアップリンクポートのプライベート VLAN エッジ（PVE）ポートとして定義できるので、同じ VLAN 内の他のポートから隔離できます。

Q

QoS

Quality of Service の略。ネットワーク責任者は、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

データベースから情報を解凍し、目的の情報を表示します。

R

RA

RADIUS Advertisement の略。

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。

RD

RADIUS Discovery の略。

RMON

Remote Monitoring の略。 ネットワーク情報を単一のワークステーションから収集します。

RS

Router Solicitation の略。

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。

S

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以下の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。

SSH

Secure Shell の略。 ネットワーク上で別のコンピュータにログインし、リモートマシン上でコマンドを実行したり、マシン間でファイルを移動することができます。Secure Shell は、セキュリティのないチャネル上で、強力な認証方法および安全な通信方法を提供します。

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 の略。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。

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。

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。

VoIP

Voice over IP の略。

W

WAN

Wide Area Network の略。 地理的に広いエリアにまたがるネットワークです。

あ

アクセスプロファイル

ネットワーク管理者は、アクセスプロファイルを使用して、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およびルールを定義できます。管理機能へのアクセスは、次の条件で定義されたユーザーグループに制限できます。

- 入口インタフェース

- 送信元 IP アドレスまたは送信元 IP サブネット

アクセスモード

システムに付与されているユーザーアクセス権に対する方法を指定します。

イーサネット

イーサネットは、IEEE 802.3 により標準化されています。最も一般的に実装されている LAN の標準です。データ転送レート Mpbs をサポートし、10、100、または 1000 Mpbs に対応します。

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。

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。

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。

オートネゴシエイション

10/100 Mpbs または 10/100/1000 Mbps イーサネットポートを次の機能向けに確立できます。

- 二重 / 半二重モード
- フロー制御
- スピード

か

起動設定

スイッチモジュールの電源が切れたとき、または再起動時に、正確なスイッチモジュールの構成を保存します。

ギガビットイーサネット

ギガビットイーサネットの伝送速度は 1000 Mbps です。既存の 10/100 Mbpsイーサネット標準との互換性があります。

コミュニティ

同じ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。

さ

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央コンピュータです。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。

サービスクラス

サービスクラス（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 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不可能になり、セッションが再スタートされます。

サブネット

サブネットワークです。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。

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。

実行設定ファイル

すべての起動設定ファイルコマンド、および現行セッション中に入力されたすべてのコマンドが含まれます。スイッチモジュールの電源がオフ、または再起動を行った場合、実行設定ファイルに保存されたコマンドはすべて消去されます。

集約型 **VLAN**

複数の VLAN を 1 つの集約型 VLAN にグループ化します。VLAN を集約すると、ルーターは、同一のスーパー VLAN に属する異なるサブ VLAN に存在するノードへの ARP 要求に応答できます。ルーターは、MAC アドレスを使って応答します。

スイッチ

LAN セグメント間でパケットをフィルタ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。

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する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。

セグメント化

LAN を個別の LAN セグメントに分割してブリッジングを行います。セグメント化によって、LAN 帯域幅の制限が排除されます。

た

帯域幅

決められた時間内に送信できるデータ量を指定します。デジタルのスイッチモジュールに対して、帯域幅はビット / 秒（bps）またはバイト / 秒で定義されます。

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。

ダイナミック **VLAN** 割り当て（**DVA**）

- RADIUS サーバーの認証中に、ユーザーを自動的に VLAN に割り当てることができます。RADIUS サーバーでユーザーが認証されると、このユーザーは、RADIUS サーバーで設定されている VLAN に自動的に参加します。

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。

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。

トランキング

リンク集約です。 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。

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 1 つのグループです。

な

二重通信モード

データの同時送受信を許可します。二重通信モードには、次の 2 つのタイプがあります。

- 全二重モード— 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— ウォーキートーキー（トランシーバ）などの非同期通信を許可します。1 度に 1 方向からのみ情報を送信できます。

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規則の集合です。

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

は

バックアップ設定ファイル

スイッチモジュールの設定のバックアップを保存したファイルです。実行設定ファイルまたは起動設定ファイルがバックアップファイルにコピーされた場合、バックアップファイルは変更されます。

バックプレーン

スイッチモジュール内で情報伝送を担うメインバスです。

バックプレッシャー

ポートがメッセージを受信しないようにする、半二重モードのメカニズムです。

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。

負荷バランシング

使用可能なネットワークリソース全体にわたって、均等なデータ配分またはパケット処理を可能にします。たとえば、負荷バランシングによって、着信パケットをすべてのサーバーに均等に配分したり、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。

フラグメント

576 ビットより小さいイーサネットパケットです。

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。

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。

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。

ブートバージョン

起動イメージのバージョンです。

ブリッジ

2 つのネットワークを接続するデバイス。ブリッジはハードウェア固有ですが、プロトコルに依存しません。また、レイヤ 1 および レイヤ 2 レベルで動作します。

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。

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が発生します。

ブロードキャストストームの詳細に関しては、LAG パラメーターの定義を参照してください。

ブロードキャストドメイン

指定されたセットのいずれかのデバイスから生成された、ブロードキャストフレームを受け取るデバイスセット。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。

プロトコル

デバイスがネットワーク上で情報を交換する方法を規定する一連の規則です。

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。

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。

ボー

1 秒間に送信される信号要素の数です。

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。

ポートのミラーリング

着信パケットおよび発信パケットのコピーをあるポートからモニタ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モニタ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関しては、「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、次のものが含まれます。

- イーサネット 10 Mbps
- ファーストイーサネット 100Mbps
- ギガビットイーサネット 1000 Mbps

ま

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。

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。

や

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。

ら

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の間でパケットを転送します。ルーターは、レイヤ 3 レベルで動作します。

レイヤ **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 2 には処理する情報が少ないため、レイヤ 3 より迅速に処理されます。

レイヤ **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 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。

わ

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。スイッチモジュールのワイルドカードマスク 255.255.255.255 は、どのビットも重要では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。

目次に戻る

目次に戻る

デバイス機能相互作用情報

Dell™ PowerConnect™ 35xx システムユーザーズガイド

次の表に、機能相互作用に関する情報を説明します。

機能	機能メモ
802.1x 非認証 VLAN	以下では、802.1x 非認証 VLAN の機能が制限されます。 • 802.1X ゲスト VLAN • 特殊な VLAN
802.1x 非認証 VLAN ポート	以下では、802.1X 非認証 VLAN ポートの機能が制限されます。 • MAC ベースの VLAN ポート • イングレスフィルタリング
ACL	以下では、ACL の機能が制限されます。 • IP ベースの ACL • MAC ベースの ACL • 特殊な VLAN
オートネゴシエイション	機能の相互作用に制約または制限はありません。
バックプレッシャーのサポート	
ブリッジマルチキャストフィルタリング	機能の相互作用に制約または制限はありません。
ケーブルテスト	機能の相互作用に制約または制限はありません。
コミュニティーポート	コミュニティーポートでは、ロックポートの機能に制限があります。
DHCP スヌーピング	制約または制限はありません。
DNS	制約または制限はありません。
二重モード	
Flow Control	機能相互作用に制約または制限はありません。
GARP	機能相互作用に制約または制限はありません。
ゲスト VLAN	ゲスト VLAN は、次の VLAN とは機能しません。 • MAC ベースの VLAN • 特殊な VLAN
GVRP	機能相互作用に制約または制限はありません。
IGMP スヌーピング	機能相互作用に制約または制限はありません。
イングレスフィルタリング	機能相互作用に制約または制限はありません。
LAG 統計	機能相互作用に制約または制限はありません。
リンク集約	機能相互作用に制約または制限はありません。ただし、この機能にはリンク集約設定の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。

LLDP-MED	機能相互作用に制約または制限はありません。
ロックポート	以下では、ロックポートの機能が制限されます。 • MAC ベースの ACL • イングレスフィルタリング
ロギング	機能相互作用に制約または制限はありません。
MAC アドレスサポート	機能相互作用に制約または制限はありません。
MDI/MDIX 検出	機能相互作用に制約または制限はありません。
マルチキャストフィルタリング	機能相互作用に制約または制限はありません。
マルチホスト	802.1X スタンダード（マルチホスト）は次のポートでは機能しません。 • MAC ベースの VLAN ポート
マルチスパニングツリー	マルチスパニングツリーは以下では機能しません。 • イングレスフィルタリング
ポートベース認証	ポートベース認証は、以下では機能が制限されます。 • 802.1 シングル • 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	機能相互作用に制約または制限はありません。ただし、この機能にはストーム制御設定の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詳細は、「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	機能相互作用に制約または制限はありません。
プライベート VLAN	プライベート VLAN は以下では機能しません。 • GVRP • IGMP スヌーピング • 特殊な VLAN
プライベート VLAN	プライベート VLAN は、以下では機能が制限または制約されます。 • GVRP • IGMP スヌーピング • 特殊な VLAN
サービス品質	機能相互作用に制約または制限はありません。
RMON 統計	機能相互作用に制約または制限はありません。
SNMP 認証通知	機能相互作用に制約または制限はありません。
SNMP 通知	機能相互作用に制約または制限はありません。
SNTP 認証	機能相互作用に制約または制限はありません。
スパニングツリー	機能相互作用に制約または制限はありません。
特殊な VLAN	機能相互作用に制約または制限はありません。
静的 MAC	機能相互作用に制約または制限はありません。
ストーム制御	機能相互作用に制約または制限はありません。
システムログ	機能相互作用に制約または制限はありません。

システム時刻の同期化	機能相互作用に制約または制限はありません。
音声 VLAN	音声 VLAN は、以下では機能が制限されます。 • GVRP

目次に戻る