Dell™ PowerConnect™ 5324 システム ユーザーガイド

メモ、注意、警告

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示します。

2007 年 5 月

目次に戻る

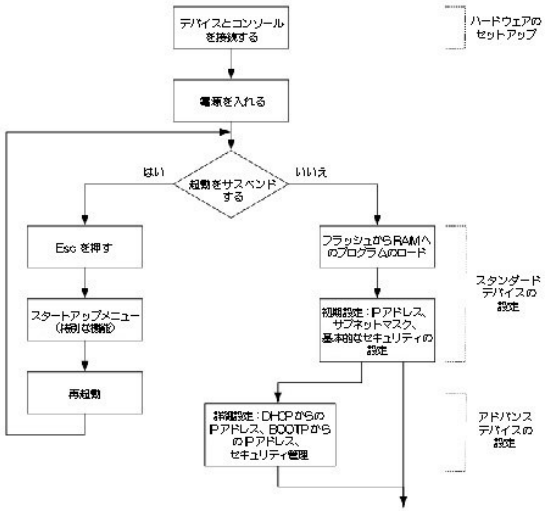
デバイスの起動および設定

Dell™ PowerConnect™ 5324 システムユーザーズガイド

外付けの接続がすべて終了したら、デバイスの設定や他の手順を実行するためにターミナルをデバイスに接続します。初期設定の場合は、標準のデバイス設定が実行されます。

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、**www.support.jp.dell.com** からダウンロードできます。

図 4-12. インストールと設定の流れ



ターミナルの設定

デバイスを設定するには、ターミナルでターミナルエミュレーションソフトウェアが実行されている必要があります。

ターミナルエミュレーションソフトウェアを次のように設定します。

1. 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。
2. データ速度を 9600 ボーに設定します。
3. データフォーマットをデータビットが 8、ストップビットが 1、パリティなしに設定します。

4. フロー制御を **none(なし)** に設定します。
5. **Properties(プロパティ)** で、**VT100 for Emulation(エミュレーション VT100)** モードを選びます。
6. **Function(ファンクション)**、**Arrow(矢印)**、**および Ctrl keys(Ctrl キー)**で、**Terminal keys(ターミナルキー)**を選びます。設定が **Terminal keys(ターミナルキー)**であることを確認してください(**Windows keys(Windows キー)**ではありません)。

注意: Microsoft® Windows 2000 を搭載したハイパーターミナルを使用している場合は、Windows® 2000 Service Pack 2 またはそれ以降のリリースがインストールされていることを確認してください。Windows 2000 Service Pack 2 がインストールされていると、ハイパーターミナルの VT100 エミュレーションで矢印キーが適切に機能します。Windows 2000 の Service Pack に関しては、www.microsoft.com/japan を参照してください。

デバイスの起動

メモ: 前提となる起動情報は次のとおりです。

- デバイスは、デフォルト設定された状態で出荷されています。
- デバイスは、デフォルトのユーザー名とパスワードで設定されていません。

デバイスを起動するには、次の手順に従います。

1. デバイスのシリアルポートが、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接続されていることを確認します。
2. AC 電源ソケットの位置を確認します。
3. AC 電源ソケットのスイッチを切ります。
4. デバイスを AC 電源ソケットに接続します。「デバイスと電源ユニットの接続」を参照してください。
5. AC 電源ソケットのスイッチを入れます。

ローカルターミナルが接続されている状態で電源を入れた場合、デバイスでは 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 が問題なく終了すると、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。

1. ASCII ケーブルがターミナルに接続されていること、およびソフトウェアエミュレーションのパラメーターが正しく設定されていることを確認します。
2. 電源ユニットをデバイスに接続します。
3. デバイスの電源を入れます。
4. デバイスを起動すると、起動テストによって使用可能なデバイスメモリがカウントされてから、起動が続行されます。次の画面は、POST の表示の例を示しています。

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


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


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


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


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


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



BOOT Software Version 1.0.0.20 Built 22-Jan-2004 15:09:28


Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.
```

```
I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.



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


Preparing to decompress...
```

起動プロセスの実行には、約 90 秒かかります。

POST の終わりに自動起動メッセージ（最後の行を参照）が表示された場合は、起動中に問題が発生しなかったことを示します。

起動時に **スタートアップ** メニューを使って、特別な手順を実行できます。**スタートアップ** メニューに入るには、自動起動メッセージが表示されてから 2 秒以内に <Esc> または <Enter> を押します。

<Esc> または <Enter> を押してもシステム起動処理が中断されない場合は、引き続きコードが解凍されて、RAM にロードされます。RAM からコードの実行が始まり、番号付きのシステムポートとその状態（有効または無効）を示すリストが表示されます。

次の画面は、設定の例を示しています。アドレス、バージョン、および日付などの項目は、デバイスごとに異なる場合があります。

```
Decompressing SW from image-2


78c000


OK


Running from RAM...



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


*** Running SW Ver. 1.0.0.15 Date 03-Mar-2004 Time 10:41:14 ***


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



HW version is 00.01.07


Base Mac address is: 00:00:07:77:77:77


Dram size is : 64M bytes


Dram first block size is : 40960K bytes
```

```
Dram first PTR is : 0x1800000

Flash size is: 16M

Device configuration:

Prestera based system

Slot 1 - Neyland24 HW Rev. 0.1

Tapi Version: v1.2.9

Core Version: v1.2.9

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

01-Jan-2000 01:01:36 %LINK-W-Down: ch1
```

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


01-Jan-2000 01:01:36 %TRUNK-I-PORTADDED: Port g24 added to ch1


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


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


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


01-Jan-2000 01:01:36 %LINK-I-Up: ch1


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


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



console>
```

デバイスが正常に起動すると、システムプロンプトが表示されます（console>）。このプロンプトを使って、デバイスを設定します。ただし、デバイスを設定する前に、最新のソフトウェアバージョンがデバイスにインストールされていることを確認してください。インストールされているソフトウェアが最新バージョンでない場合は、最新バージョンをダウンロードしてインストールしてください。最新バージョンのダウンロードの詳細に関しては、「ソフトウェアのダウンロード」を参照してください。

設定の概要

デバイスに静的 IP アドレスを割り当てる前に、次の情報を取得する必要があります。

- デバイスの設定用に割り当てられた特定の IP アドレス
- デフォルトのルート
- 当該ネットワークのネットワークマスク

設定のタイプには、次の 2 つがあります。

- **Initial Configuration（初期設定）** — 基本的なセキュリティが考慮された設定機能で構成されています。
- **Advanced Configuration（詳細設定）** — ダイナミックな IP 設定と、より詳細なセキュリティが考慮された設定機能で構成されています。

メモ: 設定に何らかの変更を加えた後は、再起動する前に新しい設定を保存する必要があります。設定を保存するには、次のように入力します。

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

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.jp.dell.com** からダウンロードできます。

メモ: 単純な初期設定は次の想定で実施されます。

- 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す。
- PowerConnect デバイスの起動が正常に終了しました。
- シリア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ます（<Enter> キーを数回押して、プロンプトが正しく表示されることを確認してください）。
- デバイスは、デフォルトのユーザー名とパスワードで設定されていません。

デバイスの初期設定は、シリアルポート経由で行われます。初期設定が終了した後、デバイスを接続済みのシリアルポートから管理するか、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。

初期設定の内容は次のとおりです。

- ユーザー名「admin」、パスワード「dell」、および最高特権レベル 15 を設定します。
- 静的 IP アドレスとデフォルトゲートウェイを設定します。
- SNMP 読み取り / 書き込みコミュニティストリングを設定します。
- DHCP サーバーによって割り当てられた IP アドレスを設定します。

PowerConnect デバイスで初期設定手順を行う前に、次の情報をネットワーク管理者に確認しておく必要があります。

- デバイス管理用の VLAN に割り当てる IP アドレス
- このネットワーク用の IP サブネットマスク
- デフォルトのゲートウェイ IP アドレス
- SNMP コミュニティ

静的 IP アドレスとサブネットマスク

IP アドレスは、VLAN、LAG、および物理ポートなどの任意のインタフェースに設定できます。設定コマンドを入力した後は、**show ip interface** コマンドを入力して、ポートに IP アドレスが設定されているかどうかを確認することをお勧めします。

重要: IP アドレスを LAG または物理ポート（g10 など）に設定すると、そのインタフェースは VLAN 1 から削除されます。

静的ルートの設定

リモートネットワークからデバイスを管理するには、静的ルートを設定する必要があります。静的ルートは、デバイス表にエントリが見つからない場合にパケットの送信先となる IP アドレスです。設定する IP アドレスは、デバイスの IP インタフェースのいずれかと同じサブネットに属している必要があります。

静的ルートを設定するには、次の設定例のとおりにシステムプロンプトにコマンドを入力します。このコマンドで 100.1.1.1（マスク 24）は特定の管理ステーション、100.1.1.10 はデフォルトゲートウェイとして機能する静的ルートです。

インバンドインタフェースに対する静的 IP アドレスの割り当て

メモ: この例では次のことを前提としています。

- PowerConnect VLAN インタフェースに割り当てられる IP アドレスは、192.168.1.123 です。
- ネットワークの IP サブネットマスクは、255.255.255.0 です。
- デフォルトルートの IP アドレスは、192.168.1.1 です。
- SNMP 読み取り / 書き込みコミュニティストリングは、"private" です。

```
console> enable
```

```
console# configure

console(config)# username admin password dell level 15

console(config)# interface VLAN 1

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

console (config-if) # exit

Console(config)# ip default-gateway 192.168.1.1

console (config) # snmp-server community private rw

console(config)# exit

console#
```

IP アドレスおよびデフォルトゲートウェイアドレスの確認

次のコマンドを実行し、その表示を調べることで、IP アドレスおよびデフォルトゲートウェイが正しく割り当てられていることを確認します。

コマンド

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

表示

Gateway IP Address	Activity status	
----------	----------	
192.168.1.1	Active	
IPアドレス	インタフェース	タイプ
----------	----------	----------
192.168.1.123 /24	VLAN 1	Static

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することをお勧めします。

ユーザー名

SSH、Telnet、ウェブインタフェースなどを通じてデバイスをリモートで管理するには、ユーザー名を設定する必要があります。デバイスを管理する完全な制御権を得るには、最高特権レベル(15)を指定します。

メモ: 最高特権レベル(15)を持つシステム管理者(スーパーユーザー)だけが、ウェブブラウザインタフェースを介してデバイスを管理できます。

特権レベルの詳細に関しては、『CLI リファレンスガイド』を参照してください。

設定するユーザー名は、リモート管理セッションのログイン名として入力します。ユーザー名と特権レベルを設定するには、次の設定例のとおりにシステムプロンプトにコマンドを入力します。

```
console> enable

console# configure

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

SNMP コミュニティストリング

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

デバイスは SNMP に準拠し、一連の標準およびプライベート MIB 変数をサポートする SNMP エージェントを搭載しています。管理ステーションを開発する際は、正確な MIB ツリー構造が必要です。プライベート MIB の全情報を取得してから、MIB の管理が可能になります。

SNMP 管理ステーションの IP アドレス、コミュニティ名、およびアクセス権を除く、すべてのパラメーターは、任意の SNMP 管理プラットフォームから管理できます。コミュニティストリングがない場合、デバイスへの SNMP 管理アクセスは無効になります。

メモ: デバイスの出荷時には、コミュニティストリングは設定されていません。デバイスでは、SNMPv1 および SNMPv2 がサポートされます。本項では、SNMPv1/v2 の設定パラメーターについて説明します。

次の画面はデフォルトのデバイス設定を示しています。

Console# **show snmp**

Community- String	Community-Access	IP address
---------------	----------------	------------------------------

Traps are enabled.
Authentication trap is enabled.

Trap-Rec- Address	Trap-Rec- Community	Version
System Contact:		
System Location:		

初期設定の手順の中で、ローカルターミナルを介してコミュニティストリング、コミュニティアクセス、および IP アドレスを設定できます。

SNMP の設定オプションは次のとおりです。

- コミュニティストリング。
  - **Read Only（読み取り専用）** — コミュニティメンバーは設定情報の閲覧ができ、変更はできないことを示します。
  - **Read/Write（読み取り / 書き込み）** — コミュニティメンバーは設定情報の閲覧も変更もできることを示します。
  - **Super（スーパー）** — コミュニティメンバーには管理アクセス権があることを示します。
- 設定可能な IP アドレス。IP アドレスを設定しないと、同じコミュニティ名を持つすべてのコミュニティメンバーに同じアクセス権が付与されます。

一般には、デバイスに 2 つのコミュニティストリングを使用します。一方は、読み取り専用アクセス権を持つ public（パブリック）コミュニティとし、もう一方は、読み書きアクセス権を持つ private（プライベート）コミュニティとします。権限のある管理ステーションに public ストリングが設定されている場合は、MIB オブジェクトを検索することができ、private ストリングが設定されている場合は、MIB オブジェクトを検索および変更することができます。

初期設定の際に、SNMP ベースの管理ステーションの使用に基づき、ネットワーク管理要件に応じてデバイスを設定することをお勧めします。

SNMP の設定

一般用のデバイスルーター表に SNMP ステーションの IP アドレスとコミュニティストリングを設定するには、次の手順を実行します。

1. コンソールプロンプトで、コマンド **Enable** を入力します。コンソールプロンプトは、**#** として表示されます。
2. コマンド **configure** を入力し、<Enter> を押します。
3. 次の例のとおりに、設定モードでコミュニティ名（private:プライベート）、コミュニティアクセス権（rw:読み書き）および IP アドレスを含むパラメーターを指定して、SNMP 設定コマンドを入力します。

```
console# configure

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

SNMP コミュニティ表の表示

SNMP ステーションの IP アドレスとコミュニティの表を表示するには、次の手順を実行します。

1. コンソールプロンプトで、コマンド **exit** を入力します。コンソールプロンプトは、**#** として表示されます。
2. 次の例のとおりに、Privileged Exec モードで show コマンドを入力します。

パラメーターの設定によって、遠隔地から詳細なデバイス設定が可能になります。

Console# **show snmp**		

Community- String	Community-Access	IP address
---	---	---
private	read write	11.1.1.2
Traps are enabled.		
Authentication trap is enabled.		
Trap-Rec- Address	Trap-Rec- Community	Version
System Contact:		
System Location:		

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 アドレスのダイナミック割り当てとセキュリティ管理について説明します。本項には、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
- セキュリティ管理とパスワードの設定

DHCP および BOOTP を介して IP アドレスを設定または受信する場合、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 アドレスの回復

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 アドレスを回復するには、次の手順を実行します。

1. 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。
2. 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 g1
```

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

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)#
```

3. 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**		
Gateway IP Address	Activity status	
----------	----------	
10.7.1.1	Active	
IP アドレス	インタフェース	タイプ
----------	----------	----------
10.7.1.192/24	VLAN 1	Static
10.7.2.192/24	VLAN 2	DHCP

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。

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 アドレスを回復するには、次の手順を実行します。

1. IP アドレスを回復するには、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。
2. 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. Do you want to continue (y/n) [n]?

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

/* the switch 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。

セキュリティ管理とパスワード設定

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。

システムは、デフォルトのパスワードが設定されていない状態で出荷されます。すべてのパスワードは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。

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 authenticationlocal

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。

スタートアップの手順

スタートアップメニューの手順

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。

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。

1. 電源を入れて、自動起動メッセージを待ちます。

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

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

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

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

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

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

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

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

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

BOOT Software Version 1.0.0.20 Built 22-Jan-2004 15:09:28

Processor: FireFox 88E6218 ARM946E-S , 64 MByte SDRAM.

I-Cache 8 KB. D-Cache 8 KB. Cache Enabled.

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

Preparing to decompress...
```

2. 自動起動メッセージが表示されたら、<Enter> を押して スタートアップメニューに入ります。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


Enter your choice or press 'ESC' to exit
```

次の項では、使用可能な 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する必要があります。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。

ソフトウェアのダウンロード

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。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、次の手順を実行します。

1. 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
```

2. 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。
3. **Filename（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。
4. **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。
5. **Send（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。

メモ: ダウンロードの所用時間は、使用するツールによって異なります。

フラッシュファイルの消去

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。

デバイス設定の消去

1. 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.


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

2. Y を押します。次のメッセージが表示されます。

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


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


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

3. 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。
4. 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

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に対してのみパスワードをリカバリするには、次の手順を実行します。

1. 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。

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。

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。ソフトウェアのダウンロードを始めるには、TFTP サーバーを設定する必要があります。

システムイメージのダウンロード

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。

1. 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。
2. 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（ros ファイル）。
3. 現在実行中のデバイスのソフトウェアバージョンを確認するには、show version を入力します。表示される情報の例を次に示します。

   ```
   console# show version

   SW version 1.0.0.42 (date 22-Jul-2004 time 13:42:41)

   Boot version 1.0.0.18 (date 01-Jun-2004 time 15:12:20)

   HW version
   ```

4. 現在アクティブなシステムイメージを確認するには、show bootvar を入力します。表示される情報の例を次に示します。

   ```
   console# sh bootvar

   Images currently available on the Flash

   Image-1 active (selected for next boot)

   Image-2 not active
   ```

console#

5. デバイスに新規のシステムイメージをコピーするには、copy tftp://{TFTP アドレス}/{ファイル名} image を入力します。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。

6. 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。この後、boot system コマンドのパラメーターとして指示したコピーが次の起動用に選択されていることを確認するには、show bootvar を入力します。

画面に表示される情報の例を次に示します。

console# boot system image-2

console# sh boot

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。

7. reload コマンドを入力します。次のメッセージが表示されます。

console# reload

This command will reset the whole system and disconnect your current

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

8. y を入力してください。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。

1. 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。
2. 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)。
3. 現在実行中のデバイスのソフトウェアバージョンを確認するには、show version を入力します。表示される情報の例を次に示します。

console# sh ver

SW version 1.0.0.42 (date 22-Jul-2004 time 13:42:41)

Boot version 1.0.0.18 (date 01-Jun-2004 time 15:12:20)

HW version 00.00.01 (date 01-May-2004 time 12:12:20)

4. デバイスに起動イメージをコピーするには、copy tftp://{TFTP アドレス}/{ファイル名} boot を入力します。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]

5. reload コマンドを入力します。次のメッセージが表示されます。

```
console# reload

This command will reset the whole system and disconnect your current

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

6. y を入力してください。

デバイスが再起動します。

目次に戻る

目次に戻る

用語集

Dell™ PowerConnect™ 5324 システムユーザーガイド

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

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

ARP

Address Resolution Protocol の略。IP アドレスを物理アドレスに変換する TCP/IP 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）

ユーザー定義のデバイス参照を指定します。

B

BootP

Bootstrap Protocol の略。このプロトコルによって、ワークステーションで、その IP アドレス、ネットワーク上の BootP サーバーの IP アドレス、またはデバイスの起動イメージにロードされる設定ファイルを検出することが可能になります。

BPDU

Bridge Protocol Data Unit の略。ブリッジ情報をメッセージ形式で提供します。BPDU は、スパニングツリー設定においてデバイス情報全体にわたって送信されます。BPDU パケットには、ポート、アドレス、優先度、および転送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。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。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を取得するインターネットホストです。

DSCP

DiffServe Code Point の略。DSCP は、IP パケットに QoS 優先度情報のタグを付ける方法です。

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。送信ルートの情報を示します。デバイスに到達したパケットのルートが登録されている場合、そのパケットは FFT にあるルートで送信されます。ルートが登録されていない場合、CPU はパケットを送信して、FFT をアップデートします。

FIFO

First In First Out の略。キューの最初のパケットが、最初に送信されるキューイングプロセスです。

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

Institute of Electrical and Electronics Engineers の略。通信およびネットワークの標準を開発するエンジニアリング組織です。

IEEE 802.1d

スパニングツリープロトコルで使用される IEEE 802.1d では、ネットワークループを回避するために MAC ブリッジをサポートしています。

IEEE 802.1p

データリンク層または MAC 副層でネットワークトラフィックに優先度を付けます。

IEEE 802.1Q

ブリッジ接続された LAN インフラストラクチャ内の VLAN の定義、運用、および管理を可能にする VLAN Bridge の動作を定義します。

IP

Internet Protocol の略。パケットのフォーマットとアドレス設定方法を指定します。IP はパケットをアドレス指定し、適切なポートに転送します。

IP アドレス

Internet Protocol アドレス。2 つ以上の LAN または WAN を相互接続しているネットワークデバイスに割り当てられた固有のアドレスです。

IPX

Internetwork Packet Exchange の略。無接続通信を行います。

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、「**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。

M

MAC アドレス

Media Access Control アドレス。MAC アドレスは、各ネットワークノードを識別するハードウェア固有のアドレスです。

MAC 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 の変形で、MD4 よりセキュリティが向上しています。MD5 は、通信の完全性を検証し、通信の発信元を認証します。

MDI

Media Dependent Interface の略。エンドステーションに使用するケーブルです。

MDIX

Media Dependent Interface with Crossover の略。ハブ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

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。

O

OID

Object Identifier の略。管理対象オブジェクトを識別するために SNMP が使用します。SNMP マネージャとエージェントのネットワーク管理パラダイムでは、管理対象オブジェクトごとに識別用の OID が必要です。

P

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。

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。

R

RADIUS

Remote Authentication Dial-In User Service の略。システムユーザーを認証し、接続時間を追跡する方法です。

RMON

Remote Monitoring の略。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。

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。ネットワークを介してリモートコンピュータにログインし、コマンドを実行し、あるコンピュータから別のコンピュータにファイルを転送します。

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。

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。

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することにより、デバイスにアクセスするためのプロファイルと規則を定義できます。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。

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。

- 入口インタフェース
- ソース IP アドレスおよびソース IP サブネット、またはそのいずれか

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 Ethernet ポートを次の機能向けに確立できます。

- 全二重または半二重動作モード
- フロー制御
- スピード

か

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。

クエリ

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。

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。

コンボポート

RJ45 接続や SFP 接続などの 2 つの物理接続を持つ 1 つの論理ポートです。

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。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

スタートアップファイルのすべてのコマンドと、現在のセッション中に入力されたすべてのコマンドが保存されます。デバイスを停止したり、再起動すると、実行設定ファイルに保存されたコマンドはすべて失われます。

ジャンボフレーム

同一のデータを少数のフレームで送信できるようにします。ジャンボフレームによって、オーバーヘッド、処理時間、および割り込みが減少します。

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。

スタートアップ設定

デバイスが停止または再起動されたときに正確なデバイス設定を保持します。

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

ブリッジングおよび経路指定を行うために、LAN を別個の LAN セグメントに分割します。セグメント化によって、LAN 帯域幅の制限が排除されます。

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。デジタルデバイスの場合、帯域幅は 1 秒あたりのビット数(bps)または 1 秒あたりのバイト数で定義されます。

帯域幅の割り当て

特定のアプリケーション、ユーザー、およびインタフェースまたはいずれかに割り当てられる帯域幅の量です。

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。

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。

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。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。

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

デバイス設定のバックアップコピーが保存されます。実行設定ファイルまたはスタートアップファイルをバックアップファイルにコピーすると、バックアップファイルが変更されます。

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。

バックプレーン

デバイスに情報を伝えるメインバスです。

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

データや処理パケットが、使用可能なネットワークリソース全体に均等に分配されるようにします。たとえば、負荷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分配したり、そのパケットを使用可能な次のサーバーにリダイレクトすることができます。

ブートバージョン

起動イメージのバージョンです。

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。

ブリッジ

2 つのネットワークを接続するデバイスです。ブリッジはハードウェア固有ですが、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。

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です。ルーターはブロードキャストフレームを転送しないため、ブロードキャストドメインをバインドします。

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 パラメータの定義」を参照してください。

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。

ボー

1 秒間に送信される信号要素の数です。

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。

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

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ー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。

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。

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。

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。ワイルドカードマスク 255.255.255.255 は、重要なビットがないことを示します。ワイルドカード 0.0.0.0 は、すべてのビットが重要であることを示します。

たとえば、宛先 IP アドレスが 149.36.184.198 で、ワイルドカードマスクが 255.36.184.00 の場合、IP アドレスの先頭 2 ビットが使用され、末尾の 2 ビットは無視されます。

目次に戻る

目次に戻る

ハードウェアの説明

Dell™ PowerConnect™ 5324 システムユーザーガイド

デバイスポートの設定

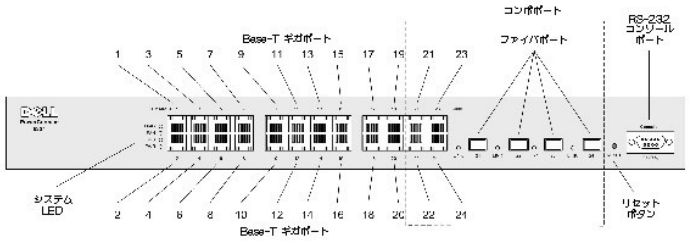
PowerConnect 5324 正面パネルのポートの説明

PowerConnect 5324 デバイスは、次のポートで構成されています。

- **銅ポート x 24** — 10/100/1000 BaseT ギガビットイーサネットポートとして指定された RJ45 ポート
- **ファイバポート x 4** — ギガビットポートとして指定されたポート
- ターミナル**ポート** — RS-232 コンソールベースポート

次の図は、PowerConnect 5324 の正面パネルを示しています。

図 2-3. PowerConnect 5324 の正面パネル



正面パネルに搭載されたポート 1 ～ 24 は、銅ベースの RJ45 ポートで、10/100/1000 Mbps として指定されており、半二重と全二重の両モードをサポートしています。また、コンボポート 21 ～ 24 として指定されている 4 つの SFP ファイバポートがあります。コンボポートは、2 つの物理接続を持つ単一の論理ポートです。1 度にアクティブにできる物理接続は 1 つだけなので、銅ポートまたは同等のファイバポート 21 ～ 24 のいずれかをアクティブにすることができますが、それらを同時にアクティブにすることはできません。上段のポートには、1 ～ 23 の奇数番号が付いており、下段のポートには 2 ～ 24 の偶数番号が付いています。

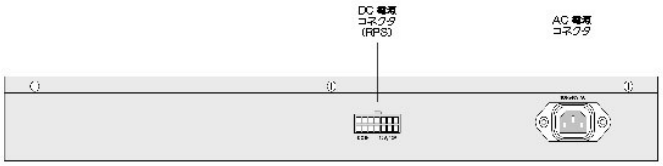
正面パネルには、RS-232 コンソールポート、すべてのデバイス LED、および、デバイスを手動でリセットするためのリセットボタンがあります。

デバイスは、RJ45 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、いずれかの方法で機能します。

PowerConnect 背面パネルのポートの説明

図 2-4 のように、デバイスの背面パネルには、電源用のコネクタがあります。

図 2-4. デバイスの背面パネル



デバイスの背面パネルには 2 つの電源コネクタがあり、一般用として、110 V または 220 V 電源ユニットに接続可能な AC 電源コネクタがあります。

DC 電源コネクタは、AC 電源ユニットの機能が停止した場合に自動的にアクティブになる冗長電源ユニット(RPS)に接続します。

デバイスポート

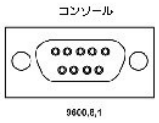
SFP ポート

スモールフォームファクタープラグ対応(SFP)ポートは、高速化とコンパクト化を実現するホットスワップ可能な光モジュールトランシーバで、1000 Base-SX または LX として指定されています。

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シリアルターミナル接続用の DB-9 コネクタ。デフォルトのボーレートは 9600 bps です。ボーレートは、2400 ～ 38400 bps の範囲で設定できます。

図 2-5. コンソールポート



コンボポート

コンボポートは、次の 2 つの物理接続を持つ 1 つの論理ポートです。

- RJ45 接続(ツイストペア銅ケーブル用)
- SFP 接続(各種のファイバベースモジュール用)

コンボポートの 2 つの物理接続のうち、1 度に 1 つの接続だけを使用できます。ポートの機能と使用可能なポートコントロールは、使用する物理接続によって決まります。

システムは、コンボポートで使用するメディアを自動的に検知し、すべての動作とコントロールインタフェースでその情報を利用します。

RJ45 と SFP の両方が存在する場合に、コネクタを SFP ポートに挿入すると、同じ番号の Base-T ポートの銅コネクタが挿入されてリンクが確立されていない限り、SFP ポートがアクティブになります。

RJ45 から SFP(またはその逆)に切り替える際に、システムの再起動やリセットは必要ありません。

寸法

デバイスの寸法は次のとおりです。

- 高さ — 44 mm
- 幅 — 440 mm
- 奥行き — 255 mm

LED の定義

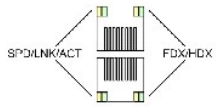
正面パネルには、リンク、電源ユニット、ファン、およびシステム診断のステータスを示す LED(Light Emitting Diode)が搭載されています。

ポート LED

10/100/1000 Base-T ポート LED

10/100/1000 Base-T ポートごとに 2 つの LED があります。左側の LED はスピード、リンク、活動を示し、右側の LED は二重モードを示します。

図 2-6. RJ45 銅ベースの 10/100/1000 BaseT LED



RJ45 LED の意味については次の表に示してあります。

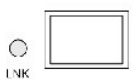
表 2-1. RJ45 銅ベースの 10/100/1000 BaseT LED の意味

LED	色	説明
左側の LED	緑色の点灯	ポートは、1000 Mbps でリンクされています。
	緑色の点滅	ポートは、1000 Mbps でデータを送信または受信しています。
	橙色の点灯	ポートは、10 または 100 Mbps でリンクされています。
	橙色の点滅	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。
	消灯	ポートは、半二重モードで動作しています。

SFP LED

SFP ポートごとに、LNK というマークの付いた LED が 1 つ存在します。

図 2-7.



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 2-2. SFP ポート LED の意味

LED	色	説明
SFP	緑色の点灯	ポートは現在開いています。
	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。
	消灯	ポートは現在閉じています。

SFP ポートを接続すると、対応する銅コンボポートの二重 LED が緑色になります。

システム LED

正面パネルの左側にあるシステム LED は、電源ユニット、ファン、温度、および診断に関する情報を示します。図 2-8 は、システム LED を示しています。

図 2-8. 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 2-3. システム LED の意味

LED	色	説明
DIAG（診断）	緑色の点滅	システムは現在診断テストを実行中です。
	緑色の点灯	システムは、診断テストに合格しました。
	赤色の点灯	システムは、診断テストに合格しませんでした。
FAN（ファン）	緑色の点灯	デバイスファンは、正常に動作しています。
	赤色の点灯	1 つまたは複数のファンが動作していません。
RPS（冗長電源ユニット）	緑色の点灯	冗長電源ユニットは正常に動作しています。
	赤色の点灯	冗長電源ユニットは動作していません。
	消灯	冗長電源ユニットは現在動作していません。
PWR（主電源ユニット）	緑色の点灯	主電源ユニットは現在正常に動作しています。
	消灯	主電源ユニットは現在動作していません。
	赤色	主電源ユニットが故障しています。

ハードウェアコンポーネント

電源

デバイスには、内蔵の電源ユニット（AC ユニット）と、デバイスを外付けの電源ユニット（DC ユニット）に接続するコネクタが付いています。外付けのユニットは RPS ユニットと呼ばれ、冗長性をもたらします。デバイスの電源投入には、電源ユニットが 1 台のみ必要です。両方の電源ユニットを使用した動作は、負荷共有によって調整されます。

負荷共有では、デバイス電源要件が 2 個の電源ユニットに分割されます。1 個の電源ユニットの機能が停止すると、2 個目の電源ユニットが自動的にデバイス全体への電力供給を続けます。

電源ユニット LED は、電源ユニットのステータスを示します。LED の詳細に関しては、「LED の定義」を参照してください。

AC 電源ユニット

AC 電源ユニットは、標準の 220/110 V AC 50/60 Hz を 5 A で 5 V DC、3 A で 12 V DC に変換します。このユニットは、使用可能な定格電圧（110 または 220 V）を自動的に検知するので、設定は必要ありません。

AC 電源ユニットでは、標準の AC 220/110 V コネクタを使用します。正面パネルにある LED インジケータから、AC ユニットが接続されているかどうかを判断できます。

DC 電源ユニット

外付けの DC 電源ユニットは、冗長電源ユニットとして使用します。動作は、このユニットのみから提供される電力によって可能になります。使用するコネクタタイプは RPS600 です。設定は必要ありません。正面パネルにある LED インジケータから、DC ユニットが接続されているかどうかを判断できます。

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。

リセットボタン

正面パネルにあるリセットボタンは、デバイスを手動でリセットする際に使用します。

換気装置

デバイスでは、冷却用にファン装置を使用します。ファンの動作ステータスを確認するには、欠陥ファンがないかどうかを示す LED を確認します。詳細に関しては、「LED の定義」を参照してください。

目次に戻る

目次ページに戻る

PowerConnect デバイスの取り付け

Dell™ PowerConnect™ 5324 システムユーザーガイド

本項では、デバイスの開梱、取り付け場所、取り付け手順、およびケーブルの接続について説明します。

取り付け前の注意事項

注意 以下の手順を実行する前に、デルマニュアルの中の『システム情報ガイド』を読み、その安全手順に従ってください。

注意 本項の手順を開始する前に、以下の点を確認してください。

- デバイスのぐらつきや落下を防ぐため、デバイスを設置するラックまたはキャビネットがしっかり固定されていることを確認します。
- 電源回路が適切にアースされていることを確認します。
- サービスマークに注意して、その指示に従います。システムマニュアルに記載されている以外の部品には触れないでください。稲妻の絵の三角形の記号が付いたカバーを開閉しないでください。感電の危険性があります。トレーニングを受けたサービス技術者以外の方は、これらの部品には触れないでください。
- 電源ケーブル、拡張ケーブル、またはプラグに損傷がないことを確認します。
- デバイスが水に濡れていないことを確認します。
- デバイスの近くに放熱器や熱源器がないことを確認します。
- 冷却用の通気孔が塞がれていないことを確認します。
- デバイスの中に異物を入れないでください。火事や感電の危険性があります。
- デバイスは必ずデル認定機器とともに使用してください。
- カバーを外したり、内部の部品に触れるときは、デバイスが充分冷えるまでお待ちください。
- デバイスが、電源回路、配線、および過電流保護に負荷をかけ過ぎていないことを確認します。電源回路に負荷がかかり過ぎているかどうかを判断するには、デバイスと同じ回路に取り付けたすべてのスイッチの定格電流を足し算します。この合計値と回路の定格制限値を比較します。
- 動作時の周囲温度が 40 ºC を超える可能性のある環境には、デバイスを取り付けないでください。
- デバイスの正面、側面、および背面の周りに通気を妨げるものがないことを確認します。

取り付け場所の要件

デバイスは、標準の 19 インチラックに取り付けるか、卓上に置くことができます。デバイスを取り付ける前に、取り付け場所が次の要件を満たしていることを確認します。

- 一般 — 電源ユニットが適切に取り付けられていることを確認します。
- 電源 — デバイスは、容易に手の届く AC 220/110 V 、50/60 Hz のアースされたコンセントから 1.5 m 以内に取り付けます。
- 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。ケーブリング、電源接続、および換気用のスペースを確保します。
- ケーブリング — ケーブルは、無線機、通信用の増幅器、電線、および蛍光灯のような電気的なノイズを避けて配線します。
- **環境要件** — 動作時の周囲温度の許容範囲は、結露のない相対湿度 10 ～ 90 % の環境で 0 ～ 40 ºC です。水や湿気がユニットケースに入らないことを確認してください。

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
- 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取り付けキット
- マニュアル CD

デバイスの開梱

デバイスを開梱するには、次の手順に従います。

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。

メモ: ESD(静電気防止用)ストラップは提供されていませんが、次の手順を行う際に装着することをお勧めします。

1. デバイスの入っている箱を整頓された平らな面に置き、箱を固定しているすべてのストラップを切ります。
2. 箱を開けるか、箱の上部を取り外します。
3. デバイスを箱から慎重に取り出し、安全で整頓された場所に置きます。
4. すべての梱包材を取り外します。
5. デバイスに損傷がないか調べます。損傷がある場合は、すぐにご連絡ください。

デバイスの取り付け

概要

デバイスの電源コネクタは、背面パネルにあります。DC 冗長電源ユニット(UPS)の接続はオプションですが、接続することをお勧めします。UPS DC コネクタは、デバイスの背面パネルにあります。

システムの取り付け

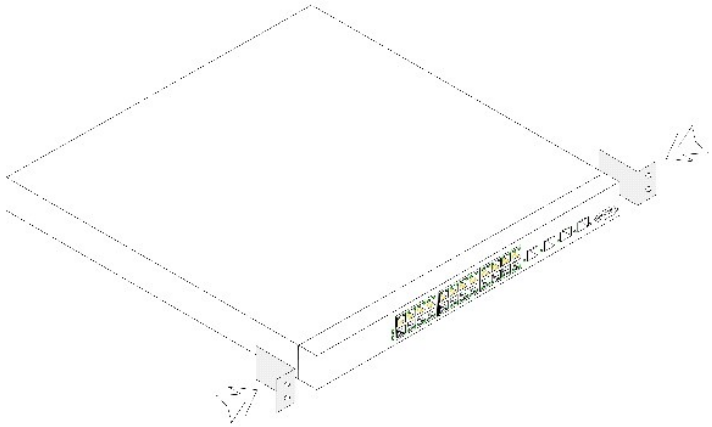
デバイスラックの取り付け

警告: 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。

警告: 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。

1. 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。図 3-9 は、ブラケットの取り付け位置を示します。

図 3-9. 接合用ラック取り付けブラケット



2. 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。
3. 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。
4. デバイスを 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。
5. 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。それによって、デバイスの重量が取り付け時に均等に配分されます。通気孔が塞がれていないことを確認します。

ラックを使用しないデバイスの取り付け

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。

1. デバイスに付属のラバーフィートを取り付けます。
2. 左右の側面に約 5 cm、背面に約 13 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。
3. デバイスの通気孔が塞がれていないことを確認します。

デバイスの接続

デバイスを設定するには、デバイスをターミナルに接続する必要があります。

デバイスとターミナルの接続

デバイスのコンソールポートは、デバイスをモニターおよび設定するためのターミナルエミュレーションソフトウェアを実行しているターミナルデスクトップシステムに接続できます。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。

1. 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、RS-232 クロスケーブルを接続します。
2. ターミナルエミュレーションソフトウェアを次のように設定します。
    a. 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。
    b. データ速度を 9600 ボーに設定します。
    c. データフォーマットをデータビットが 8、ストップビットが 1、パリティなしに設定します。
    d. フロー制御を none(なし) に設定します。

e. **Properties(プロパティ)** で、**VT100 for Emulation(エミュレーション VT100)** モードを選びます。

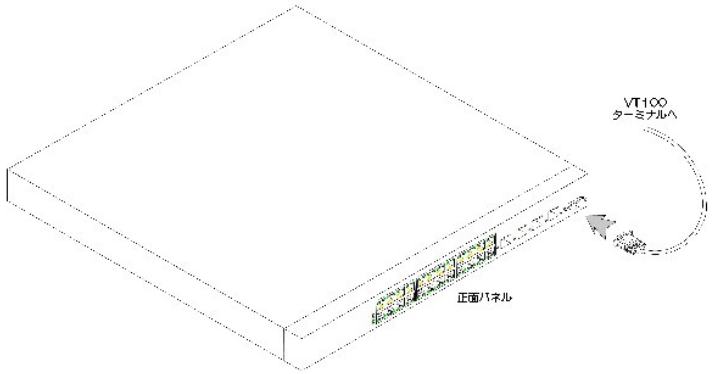
f. **Function(ファンクション)**、**Arrow(矢印)**、**および Carl keys(Ctrl キー)**で、**Terminal keys(ターミナルキー)**を選びます。設定が(**Windows keys(Windows キー)** ではなく)**Terminal keys(ターミナルキー)** であることを確認してください。

注意: Microsoft® Windows 2000 でハイパーターミナルを使用する場合は、Windows® 2000 Service Pack 2 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。

3. RS-232 クロスケーブルのメスコネクタをデバイスコンソールポートに直接接続し、固定ボルトを締めます。

デバイスのコンソールポートは、正面パネルにあります。

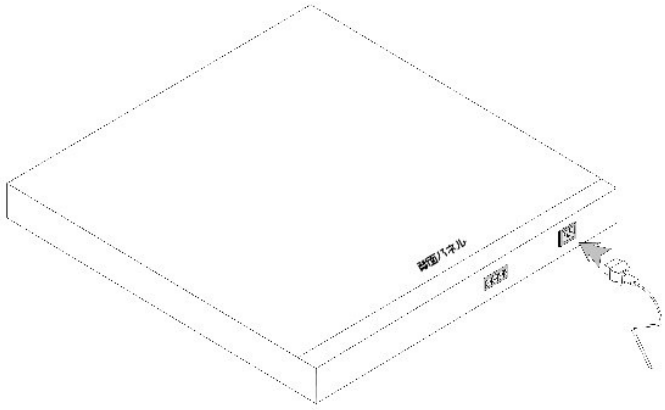
図 3-10. PowerConnect 5324 コンソールポートへの接続



デバイスと電源ユニットの接続

1. 安全にアース接続された 1.5 m の標準電源ケーブルを使って、背面パネルにある AC コネクタに電源ケーブルを接続します。
2. 電源ケーブルをアースされている電源コンセントに接続します。

図 3-11. デバイス電源コネクタへの接続



正面パネルの LED をチェックして、デバイスが接続され、正常に動作することを確認します。

ポート接続、ケーブル、およびピンアウト情報

本項では、デバイスの物理インタフェースとポート接続について説明します。コネクタタイプ、ポート、およびケーブルについては、「ポート、コネクタ、およびケーブル」の項に要約があります。銅ケーブルおよび光トランシーバ診断がサポートされています。

10/100/1000 BaseT ポート用の RJ45 接続

10/100/1000 BaseT ポートは、銅ツイストペアポートです。

ツイストペアポートのリンクを確立するには、一方のケーブル先端の Tx ペアを他方のケーブル先端の Rx ペアに接続(あるいはその逆)する必要があります。一方のケーブル先端の Tx を他方のケーブル先端の Tx に接続し、Rx を Rx に接続するように配線すると、リンクは確立されません。

デバイスポートをネットワークピアに接続するケーブルを選択する際に、デバイスをステーションに接続する場合はストレートケーブルを、転送デバイス(スイッチまたはハブ)から別の転送デバイスに接続するにはクロスケーブルを使用する必要があります。ストレートケーブルとクロスケーブルはいずれもカテゴリ 5 の部類に入ります。

ポートが接続された後は、リンク表示 LED が点灯します。

表 3-4.

コネクタ	ポート / インタフェース	ケーブル
RJ45	10/100/1000 BaseT ポート	カテゴリ 5

ポート、コネクタ、およびケーブル

次の表は、10/100/1000 BaseT ポート用の RJ45 ピン番号割り当てを示します。

表 3-5. 10/100/1000 BaseT イーサネットポート用の RJ45 ピン番号割り当て

ピン番号	機能
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

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、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で確立されるメカニズムで、一方のポートからその転送レート、二重モード、およびフロー制御(デフォルトではフロー制御は無効になります)の機能をパートナーに伝えることができます。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 10/100/1000 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、無関係な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）。

フロー制御

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おり、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。

バックプレッシャー

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おり、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に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 3-6. 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	10/100/1000 BaseT 銅ポート:オートネゴシエイション、100 Mbps、全二重
ポート転送状態	Enabled
ポートのタグ付け	タグなし
フロー制御	OFF（入口で無効）
バックプレッシャー	OFF（入口で無効）

目次ページに戻る

目次ページに戻る

はじめに

Dell™ PowerConnect™ 5324 システムユーザーガイド

注意： 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、www.support.jp.dell.com からダウンロードできます。

このユーザーガイドには、PowerConnect 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。

PowerConnect 5324

PowerConnect 5324 には、24 個のギガビットイーサネットポートが搭載されています。また、イーサネットポート 21 ～ 24 に代わるコンボポートとして指定されている、4 つの SFP ファイバポートがあります。コンボポートは、2 つの物理接続を持つ単一ポートです。一方が接続している場合、他方は無効になります。

図 1-1 および図 1-2 は、PowerConnect 5324 の正面パネルと背面パネルを示しています。

図 1-1. PowerConnect 5324 の正面パネル

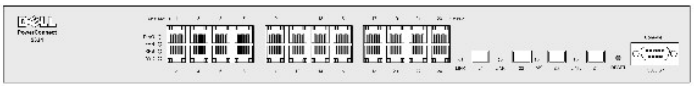


図 1-2. PowerConnect 5324 の背面パネル

機能

本項では、デバイスのユーザー設定機能について説明します。アップデートされた全デバイス機能の一覧については、ソフトウェアの最新バージョンのリリースノートを参照してください。

一般的な機能

ヘッドオブラインブロッキング

ヘッドオブライン（HOL）ブロッキングは、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 ブロッキングではパケットがキューに入り、キューの先頭のパケットがキューの最後のパケットより先に転送されます。

仮想ケーブルテスト（VCT：Virtual Cable Testing）

VCT は、銅リンクケーブリングの存在を検知して、空きケーブルやケーブル不足などを報告します。

ジャンボフレームのサポート

ジャンボフレームを使用することで、少数のフレームで同一のデータを転送できます。オーバーヘッド、処理時間および割り込みの減少を確実にします。

ジャンボフレームの有効化の詳細に関しては、「一般的なデバイス情報の定義」を参照してください。

MDI/MDIX のサポート

デバイスでは、クロスケーブルとストレートケーブルの間の自動検知をサポートしています。

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。

ポートまたはリンク集約グループ(LAG:Link Aggregate Groups)の詳細に関しては、「ポートパラメーターの定義」または「LAG パラメーターの定義」を参照してください。

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設定に関しては、「ポートパラメーターの定義」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 に対するバックプレッシャーの設定に関しては、「ポートパラメーターの定義」または「LAG パラメーターの定義」を参照してください。

MAC アドレスサポート機能

MAC アドレス容量のサポート

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

MAC アドレスの自動学習

デバイスは、着信パケットからの MAC アドレスの自動学習を可能にします。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 アドレスを削除します。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設定に関しては、「アドレス表の設定」を参照してください。

静的な MAC エントリ

ユーザー定義の静的な MAC エントリは、**ブリッジ表**に保存されます。

詳細に関しては、「アドレス表の設定」を参照してください。

VLAN 認識の MAC ベーススイッチング

記録されていない送信元アドレスから到達したパケットはマイクロプロセッサに送信されます。そこでその送信元アドレスはハードウェア表に追加されます。このアドレスとやり取りされるパケットは、ハードウェア表を使ってより効率的に転送されます。

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。

詳細に関しては、「マルチキャスト転送のサポート」を参照してください。

レイヤ 2 の機能

IGMP スヌープ

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。

詳細に関しては、「IGMP スヌープ」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、モニター対象のポートからモニター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。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コントロール

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、「ストームコントロールの有効化」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、または入口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口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。

IEEE802.1V プロトコルベースの仮想 LAN（VLAN）

VLAN 分類規則は、データリンク層（レイヤ 2）プロトコル識別子に対して定義されています。プロトコルベースの VLAN では、レイヤ 3 プロトコルと区別するためにレイヤ 2 トラフィックを隔離します。

詳細に関しては、「VLAN プロトコルグループの定義」を参照してください。

全 802.1Q VLAN タギングへの準拠

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。この標準に含まれる重要な要件として、望ましいサービスクラス（CoS）のタグ値（0 ～ 7）をフレームに付ける機能があります。

GVRP のサポート

GARP VLAN 登録プロトコル（GVRP：GARP VLAN Registration Protocol）は、IEEE 802.1Q 準拠の 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 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：Spanning Tree Protocol）

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設定」を参照してください。

リンク集約

詳細に関しては、「ポートの集約」を参照してください。

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：Link Aggregated Group）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、「LAG メンバーシップの定義」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、所定の対のシステム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、システム内の集約リンクのポートバインドに関して自動的に判断、設定、バインド、およびモニターを行います。

詳細に関しては、「LACP パラメーターの定義」を参照してください。

レイヤ 3 の機能

アドレス解決プロトコル（ARP：Address Resolution Protocol）

ARP は、IP アドレスを物理アドレスに変換する TCP/IP プロトコルです。ARP は、直接接続されているエンドシステムも含め、システムのデバイス次回ホップ MAC アドレスを自動的に判断します。ユーザーは、追加の ARP 表エントリを定義することで、この次回ホップ MAC アドレスをオーバーライドし、補足することができます。

詳細に関しては、「ドメインホストのマッピング」を参照してください。

TCP

転送制御プロトコル（TCP：Transport Control Protocol）接続は、最初の同期交換によって 2 ポート間に定義されます。TCP ポートは、IP アドレスと 16 ビットのポート番号によって識別されます。オクテットストリームは、それぞれにシーケンス番号を持つ TCP パケットに分割されます。

BootP および DHCP クライアント

ダイナミックホスト設定プロトコル（DHCP：Dynamic Host Configuration Protocol）は、システムの起動時に追加のセットアップパラメーターをネットワークサーバーから受信できるようにします。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 IP 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、簡易ネットワーク管理プロトコル（SNMP：Simple Network Management Protocol）トラップとして受信トラップリストに送信されます。

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 およびバージョン 2

UDP/IP 上 SNMP プロトコル。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。

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ー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

PowerConnect 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。

トリビアルファイル転送プロトコル（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。

リモートモニター

リモートモニター（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ーを可能にする 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ー機能を提供します。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、「RMON 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：Command Line Interface）の構文および解釈は、業界に共通する構文および解釈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。

シスログ

シスログは、イベント通知が一組のリモートサーバーに送信されるようにするプロトコルです。リモートサーバーでは、受信したイベント通知を保存し、検証し、対処することができます。重要なイベントの通知をリアルタイムで送信し、それらのイベントの記録を事後使用に備えて保存するために複数のメカニズムが実装されています。

Syslog の詳細に関しては、「ログの管理」を参照してください。

SNTP

簡易ネットワークタイムプロトコル (SNTP：Simple Network Time Protocol）は、ミリ秒以下の正確なネットワークデバイスクロック時間の同期を保証します。時間の同期は、ネットワーク SNTP サーバーによって実行されます。時間のソースは、Stratum によって設定されます。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。

トレースート

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 経路を検出できます。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。

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、パブリックおよびプライベートキーに依存します。

ポートベースによる認証(802.1x)

ポートベースによる認証では、外部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:Extensible Authentication Protocol)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:Remote Authentication Dial In User Service)サーバー経由で行われます。

詳細に関しては、「ポートベース認証の設定」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 グローバルパラメーターの設定」を参照してください。

SSH

セキュアシェル(SSH:Secure Shell)は、デバイスへの安全なリモート接続を実現します。SSH バージョン 1 が現在使用可能です。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 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確認するための集中化したセキュリティを可能にします。TACACS+ は、RADIUS およびその他の認証プロセスとの一貫性を保ちながら、集中化した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。

その他の 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。この情報には、CLI の説明、構文、デフォルト値、ガイドライン、および例が含まれます。

目次ページに戻る

目次に戻る

サービス品質の設定

Dell™ PowerConnect™ 5324 システムユーザーガイド

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。QoS を開くには、ツリービューでサービス品質をクリックします。

サービス品質(QoS)の概要

サービス品質(QoS:Quality of Service)は、ネットワーク内に QoS と優先度キューを実装する能力を提供します。QoS により、ポリシー、フレームカウンタ、およびコンテキストに基づいたネットワークトラフィックフローが改善されます。

QoS を必要とする実装例として、音声、ビデオ、およびリアルタイムトラフィックなど、高い優先度キューが割り当てられ、それ以外のトラフィックには低い先度キューが割り当てられる、特定のタイプのトラフィックがあります。それによって、需要の高いトラフィックのフローが改善されます。

QoS は、次の項目によって定義されます。

- 分類 — 特定の値に一致してい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。
- 処置 — パケット情報や VLAN 優先度(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 タグの分類情報

VLAN 優先度タグ(VPT:VLAN Priority Tag)を使って、出力キューのいずれかにパケットをマッピングさせることにより、パケットを分類します。キューの割り当てに対する VPT は、ユーザーが定義することもできます。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。

表 9-92. CoS に対するキューのマッピング表デフォルト値

CoS 値	転送キューの値
0	q2
1	q1(最低優先度 = ベストエフォート)
2	q1(最低優先度 = ベストエフォート)
3	q2
4	q3
5	q3
6	q4(最高優先度)
7	q4(最高優先度)

タグがない状態で到達したパケットには、ポートごとに設定されるデフォルトの VPT が割り当てられます。割り当てられた VPT を出口 VPT として使用して、パケットを出力キューにマッピングします。

DSCP 値は、優先度キューにマッピングできます。次の表は、転送キューの値にマッピングするデフォルトの DSCP を示します。

表 9-93. DSCP に対するキューのマッピング表デフォルト値

DSCP 値	転送キューの値
0 ～ 7	q2(最低優先度)
8 ～ 15	q1

16 ～ 23	q1
24 ～ 31	q2
32 ～ 39	q3
40 ～ 47	q3
48 ～ 55	q4
55 ～ 63	q4(最高優先度)

DSCP マッピングは、システムごとに有効になります。

CoS サービス

パケットを特定のキューに割り当てた後は、CoS サービスをキューに割り当てることができます。出力キューには、次のいずれかの方法でスケジュール方式を設定します。

- 厳密優先度 — 時間的な影響を受けるアプリケーションが、常に高速なパスで転送されるようにします。厳密優先度を使用すると、時間にあまり敏感でないアプリケーションよりも、重要な使命を持ち時間に敏感なトラフィックを優先させることができます。
  たとえば、厳密優先度を設定すると、IP 上の音声トラフィックが FTP トラフィックや電子メール(SMTP)トラフィックより先に転送されます。
  厳密優先度キューが空になると、残りのキューのトラフィックが転送されます。

- 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:Weighted Round Robin)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。キューの優先度は、キューの長さによって定義されます。キューが長いほど、キューの転送優先度が高くなります。
  たとえば、4 つのキューの重みが 1、2、3、および 4 である場合、転送優先度の最も高いパケットはキュー 4 に割り当てられ、転送優先度の最も低いパケットはキュー 1 に割り当てられます。WRR では、最高の転送優先度を長さ 4 のキューに割り当てることによって、優先度の高いトラフィックから処理し、優先度の低いトラフィックも順調に転送することができます。

  スケジュール方式は、システム規模で有効になります。厳密優先度ポリシーに割り当てられたキューは、優先度の最も高いキューに自動的に割り当てられます。デフォルトでは、すべての値が厳密優先度として設定されます。WRR モードに変更する場合、デフォルトの重み値は 1 になります。キューの重みの値は、WRR を使って任意の順番で割り当てることができます。WRR の値は、システム規模で割り当てることができます。ベストエフォートのトラフィックは常に、最初のキューに割り当てられます。キュー 1 にベストエフォートが保持されるように、WRR 値を割り当てる必要があります。

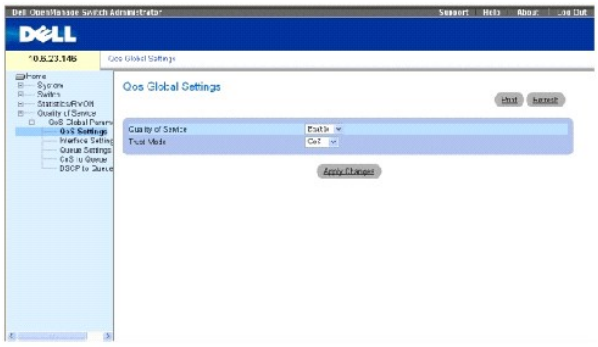
CoS グローバルパラメーターの定義

サービスクラス(CoS:Class of Service)グローバルパラメーターは、[**CoS グローバルパラメーター**] ページで設定します。

QoS のグローバル設定

[QoS のグローバル設定] ページには、QoS を有効または無効にするフィールドがあります。Trust(信頼)モードを選択することもできます。Trust(信頼)モードは、出力キューを判断するためにパケット内に事前に定義されたフィールドに依存します。[**QoS の設定**] ページを開くには、ツリービューでサービス品質→CoS グローバルパラメーター→CoS の設定の順にクリックします。

図 9-130. QoS の設定



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(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。規則が定義されていない場合、事前に定義されたパケットフィールド(CoS または DSCP)を含むトラフィックは、関連するTrust(信頼)モード表に従ってマッピングされます。事前に定義された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 — 出力キュー割り当ては、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。

DSCP — 出力キュー割り当ては、DSCP フィールドによって確定します。

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)設定をオーバーライドします。

サービス品質を有効にするには次の手順を実行します。

1. **QoS の設定** ページを開きます。
2. **CoS モード** フィールドで **Enable(有効にする)** を選択します。
3. 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。

Trust(信頼)を有効にするには次の手順を実行します。

1. **QoS の設定** ページを開きます。
2. **Trust(信頼)モード** フィールドで **Trust(信頼)** を選択します。
3. Apply Changes(変更の適用)をクリックします。

Trust(信頼)は、デバイスごとに有効になります。

CLI コマンドを使用した Trust(信頼)の有効化

次の表は、**QoS の設定** ページでフィールドを設定する場合と同等の CLI コマンドをまとめたものです。

表 9-94. CoS 設定用 CLI コマンド

CLI コマンド	説明
qos trust [**cos** | **dscp**]	システムを基本モードおよび "trust" 状態に設定します。
no cos trust	non-trusted 状態を返します。

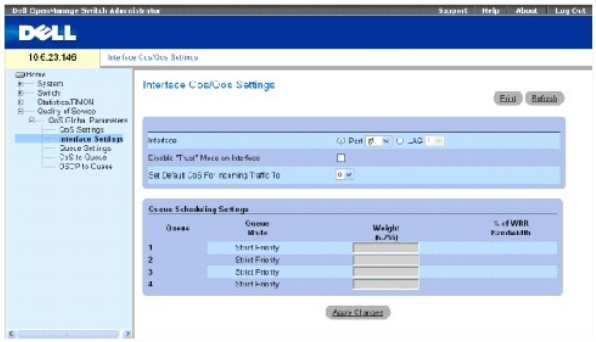
CLI コマンドの例は次のようになります。

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

QoS インタフェース設定の定義

インタフェースの CoS/QoS 設定 ページには、選択されている Trust(信頼)モードがアクティブになるかどうかを、インタフェースごとに定義するためのフィールドがあります。タグのない着信パケットに対するデフォルトの優先度も、**インタフェースの CoS/QoS 設定** ページで選択します。このページを開くには、ツリービューでサービス品質→CoS グローバルパラメーター→インタフェースの設定)の順にクリックします。

図 9-131. インタフェースの CoS/QoS 設定



インタフェース — 特定のポートまたは LAG を次のように設定します。

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に対して 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。

着信トラフィックにデフォルトの CoS を設定する — タグのないパケットにデフォルトの CoS タグ値を設定します。CoS タグ値の範囲は 0 ～ 7 です。デフォルト値は 0 です。

キュー — キュー番号。

キューモード — キューが [Strict Priority(厳密優先度)](SP)か [WRR] かを示します。このモードは、**Queue Settings(キューの設定)** 画面で定義します。

- SP は、1 ～ 4 のすべてのキューに設定できます。
- WRR は、1 ～ 4 のすべてのキューに設定できます。
- SP モードをキュー 1、2 に設定し、WRR をキュー 3、4 に設定できます。
- WRR モードをキュー 1、2 に設定し、SP をキュー 3、4 に設定できます。

重み(6 ～ 255) — WRR の重みをキューに割り当てます。このフィールドは、WRR キューモードのキューにのみ有効です。

WRR 帯域幅の割合 — **重み(6 ～ 255)** フィールドに定義された重みを割合で示した値。

インタフェースに QoS/CoS 設定を割り当てる

1. **インタフェースの CoS/QoS 設定** ページを開きます。
2. **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。
3. フィールドを定義します。
4. **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。

CLI コマンドを使用したインタフェースへの CoS 割り当て

次の表は、**インタフェースの CoS/QoS 設定** ページでフィールドを設定する場合と同等の CLI コマンドをまとめたものです。

表 9-95. インタフェースの CoS 設定用 CLI コマンド

CLI コマンド	説明
qos trust	ポートごとに trust 状態を有効にします。
qos cos default-cos	デフォルトのポート CoS 値を設定します。
no qos trust	ポートごとに trust 状態を無効にします。

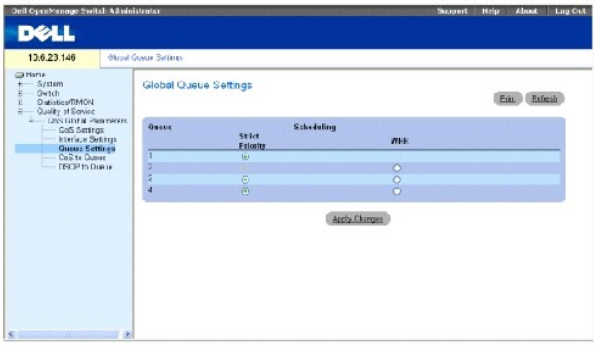
CLI コマンドの例は次のようになります。

```
Console (config)#
interface ethernet g5


Console (config-if)# qos
trust


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

キューの設定の定義

キューのグローバル設定 ページには、キューを保持するスケジュール方式を設定するためのフィールドがあります。**キューのグローバル設定** ページを開くには、ツリービューで サービス品質→ **CoS** グローバルパラメーターキューの設定を順にクリックします。

図 9-132. キューのグローバル設定



キュー — キュー番号。

厳密優先度 — トラフィックのスケジュールがキューの優先度に厳密に基づくかどうかを指定します。デフォルトでは有効になります。

WRR — トラフィックのスケジュールが出口キューへの Weighted Round Robin（WRR：重み付きラウンドロビン）の重みに基づくかどうかを指定します。

キューの設定の定義

1. **キューのグローバル設定** ページを開きます。
2. フィールドを定義します。
3. **Apply Changes（変更の適用）** をクリックします。

キューの設定が定義され、デバイスが更新されます。

CLI コマンドを使用したキュー設定の割り当て

次の表は、**キューのグローバル設定** ページでフィールドを設定する場合と同等の CLI コマンドをまとめたものです。

表 9-96. キューの設定用 CLI コマンド

CLI コマンド	説明
wrr-queue bandwidth weight1 weight2 . weight_n	WWR の重みを出口キューに割り当てます。
show qos interface [**ethernet** *インタフェース番号*] [queuing]	インタフェースの QoS データを表示します。

CLI コマンドの例は次のようになります。

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



Console(config)# exit



Console # exit



Console> show qos
interface ethernet g1
queueing



Ethernet g1



wrr bandwidth weights and
EF priority:
```

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



Console(config)# exit



Console # exit



Console> show qos
interface ethernet g1
queueing



Ethernet g1
```

wrr bandwidth weights and EF priority:

qid	weights	Ef	Priority
1	125	無効	適用なし
2	125	無効	適用なし
3	125	無効	適用なし
4	125	無効	適用なし

Cos queue map:

Cos	qid
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

CoS 値とキューのマッピング

CoS とキューのマッピング表 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 とキューのマッピング表 ページを開くには、ツリービューでサービス品質 →**CoS** グローバルパラメーター → CoS 対キューを順にクリックします。

図 9-133. CoS とキューのマッピング表

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。

キュー — CoS 優先度をマッピングする対象のトラフィック転送キュー。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。

デフォルトの復元 — CoS 値を転送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 値をキューにマッピングする

1. CoS とキューのマッピング表 ページを開きます。
2. CoS エントリを選択します。
3. **キュー** フィールドでキュー番号を定義します。
4. **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 キューへの CoS 値割り当て

次の表は、CoS とキューのマッピング表 ページでフィールドを設定する場合と同等の CLI コマンドをまとめたものです。

表 9-97. CoS とキューのマッピング用 CLI コマンド

CLI コマンド	説明
wrr-queue cos-map queue-id cos1..cos8	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。

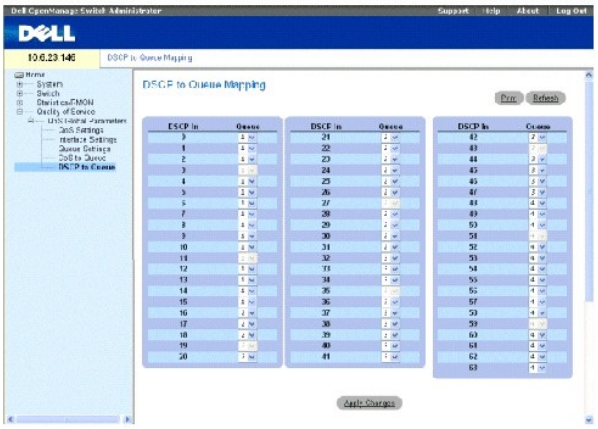
```
Console (config)# wrr-queue
cos-map 4 7
```

DSCP 値とキューのマッピング

DSCP マッピング ページには、特定の DSCP フィールドに出力キューを定義するためのフィールドがあります。DSCP マッピング ページを開くには、ツリービューでサービス品質→**CoS** グローバルパラメーター→DSCP マッピングを順にクリックします。

メモ: DSCP デフォルト設定のリストに関しては、「DSCP に対するキューのマッピング表デフォルト値」を参照してください。

図 9-134. DSCP マッピング



DSCP In(着信 DSCP)— 着信パケット内の DSCP フィールドの値。

キュー — 特定の DSCP 値を持つパケットに割り当てるキュー。値は 1 ～ 4 です。最小値は 1、最大値は 4 です。

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

1. **DSCP マッピング** ページを開きます。
2. **DSCP In(着信 DSCP)** 列の値を選択します。
3. **キュー** フィールドを定義します。
4. **Apply Changes(変更の適用)** をクリックします。

DSCP が上書きされ、値が転送キューに割り当てられます。

CLI コマンドを使用した DSCP 値の割り当て

次の表は、**DSCP マッピング** ページでフィールドを設定する場合と同等の CLI コマンドをまとめたものです。

表 9-98. DSCP 値とキューのマッピング用 CLI コマンド

CLI コマンド	説明
qos map dscp-queue dscp-list **to** queue-id	DSCP と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

デバイスの仕様

Dell™ PowerConnect™ 5324 システムユーザーガイド

この付録では、デバイスの実行に必要な情報を示します。

ポートおよびケーブルの仕様

本項では、ポートの仕様について説明します。

ポートの仕様

次の表は、デバイスポートのタイプと各ポートタイプの説明を示したものです。

表 10-99.

デバイス	仕様
PowerConnect 5324	• GE ポート x 24 • SFP ポート x 4 • RS-232 コンソールポート
ポートタイプ	
RJ45	• 10 Base-T • 100 Base-T • 1000 Base-T
SFP	標準のスモールフォームファクターをサポート ギガビットプラグトランシーバ
ポートの設定	
	• スピード、二重モード、およびフロー制御に対するオートネゴシエイション • バックプレッシャー • ヘッドオブラインブロッキング • 自動 MDI/MDIX • ポートミラーリング • ブロードキャストストームコントロール

ポートの仕様

動作条件

本項では、動作時の温度や湿度などの動作条件を示します。

表 10-100.

機能	仕様
動作温度	0 ～ 40 ℃
動作湿度	10～90 %（結露しないこと）

動作条件

デバイス本体の仕様

本項では、動作時の温度や湿度などの動作条件を示します。

表 10-101.

機能	仕様
ユニットサイズ	l 幅 48.26 cm l 高さ 1 U
換気装置	各ユニットにファン 2 個

デバイス本体の仕様

デバイスメモリの仕様

本項では、デバイスのメモリ仕様を示します。

表 10-102.

メモリのタイプ	メモリ量
CPU DRAM	64 MB
フラッシュメモリ	16 MB
パケットバッファメモリ	2 Mb

デバイスのメモリ仕様

機能の仕様

VLAN

- IEEE 802.1Q に従ったタギングおよびポートベースの VLAN サポート
- 最大 4094 の VLAN をサポート
- 内蔵システム用の予約 VLAN
- GVRP サポート付ダイナミック VLAN
- プロトコルベースの VLAN

サービス品質

- レイヤ 2 Trust(信頼)モード(IEEE 802.1p タギング)
- レイヤ 3 Trust(信頼)モード(DSCP)
- 調節可能な Weighted Round Robin(WRR:重み付きラウンドロビン)
- 調節可能な厳密キュースケジュール

レイヤ 2 マルチキャスト

- ダイナミックマルチキャストサポート - IGMP スヌープまたは静的マルチキャストで最大 256 のマルチキャストグループをサポート

デバイスセキュリティ

- スイッチへのアクセスパスワード保護
- ポートベースの MAC アドレス警告とロックダウン
- スイッチ管理アクセスの RADIUS リモート認証
- TACACS+
- 管理アクセスプロファイルを介した管理アクセスのフィルタリング

- SSH/SSL 暗号化管理

その他のスイッチング機能

- デバイスごとに最大 8 つの集約リンクと、集約リンクごとに最大 8 つのポートをサポートするリンク集約（IEEE 802.3ad）
- LACP サポート
- 最大 10 K のジャンボフレームをサポート
- ブロードキャストストームコントロール
- Port Mirroring（ポートのミラーリング）

デバイスの管理

- ウェブベースのマネジメントインタフェース
- Telnet を介した CLI アクセス
- SNMPv1 および SNMP v2 をサポート
- 4 つの RMON グループをサポート
- ファームウェアおよび設定ファイルの TFTP 転送
- 2 つのファームウェアイメージを搭載
- 複数の設定ファイルのアップロードおよびダウンロードをサポート
- エラーモニターの統計とパフォーマンスの最適化
- BootP/DHCP IP アドレス管理をサポート
- Syslog リモートログイン機能
- SNTP サポート
- レイヤ 3 トレースルート
- Telnet クライアント
- DNS クライアント

目次に戻る

目次に戻る

デバイス情報の設定

Dell™ PowerConnect™ 5324 システムユーザーガイド

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

デバイスでは、アクセス制御リストおよびポートロックによるネットワークセキュリティが可能です。**Network Security（ネットワークセキュリティー）** 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）を選択します。

ネットワークセキュリティの概要

本項では、ネットワークセキュリティの機能について説明します。

ポートベース認証（802.1x）

ポートベース認証では、外部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する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、そのユーザーに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 サーバーなどの外部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）— ユーザーに権限がある場合に、ユーザー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。

拡張ポートベース認証

拡張ポートベース認証によって、複数のホストを単一のポートに接続することができます。拡張ポートベース認証では、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。ポートに権限がない場合、すべての接続ホストはネットワークへのアクセスを拒否されます。

また、拡張ポートベース認証では、ユーザーベースの認証も可能です。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（IP 上音声通信）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、ユーザーはその認可なし VLAN を使用することができます。

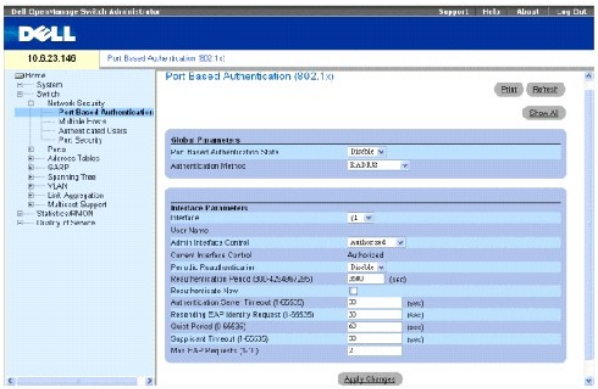
拡張ポートベース認証は、次のモードで実行します。

- **Single Host Mode（単一ホストモード）** — 権限のあるホストだけがポートにアクセスできるようにします。
- **Multiple Host Mode（複数ホストモード）** — 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。

ポートベース認証の設定

ポートベース認証 ページには、ポートベース認証を設定するためのフィールドがあります。**ポートベース認証** ページを開くには、スイッチ → Network Security（ネットワークセキュリティー）→ Port Based Authentication（ポートベース認証）をクリックします。

図 7-80. ポートベース認証



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以下のとおりです。

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です。可能なフィールド値は以下のとおりです。

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（RADIUS) — ポート認証は、RADIUS サーバーを使って行われます。

RADIUS, None（RADIUS、なし） — ポート認証は、最初に RADIUS サーバーを使って行われます。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。

インタフェース — インタフェースリストを示します。

ユーザー名 — RADIUS サーバーに設定されているとおりのユーザー名です。

Admin Interface Control（管理インタフェースコントロール） — ポートの認証状態を定義します。可能なフィールド値は以下のとおりです。

Authorized（権限あり） — インタフェースの状態を authorized（権限あり）（トラフィックを許可）に設定します。

Unauthorized（権限なし） — インタフェースの状態を unauthorized（権限なし）（トラフィックを拒否）に設定します。

Auto（自動） — 権限の状態は授権方法によって設定されます。

Current Interface Control（現在のインタフェースコントロール） — 現在設定されているポートの権限状態。

Periodic Reauthentication（断続的な再認証） — このオプションを有効にすると、選択したポートが断続的に再認証されます。再認証の時期は、**Reauthentication Period（再認証の時期）（300 ～ 4294967295）** フィールドで定義します。

Reauthentication Period（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） — このオプションを選択すると、ポートの再認証をただちに行うことができます。

Authentication Server Timeout（認証サーバーのタイムアウト）（1 ～ 65535） — このフィールドで定義した時間を経過すると、デバイスから認証サーバーに要求が再送信されます。フィールド値は秒単位です。デフォルト値は 30 秒です。

Resending EAP Identity Request（EAP アイデンティティ要求の再送信）（1 ～ 65535） — このフィールドに定義した時間を経過すると、EAP 要求が再送信されます。デフォルト値は 30 秒です。

Quiet Period（静止期間）（0 ～ 65535） — 認証交換に失敗した後でデバイスが静止状態になる秒数です。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（サプリカントのタイムアウト）（1 ～ 65535） — このフィールドに定義した時間を経過すると、EAP 要求がユーザーに再送信されます。フィールド値は秒単位です。デフォルト値は 30 秒です。

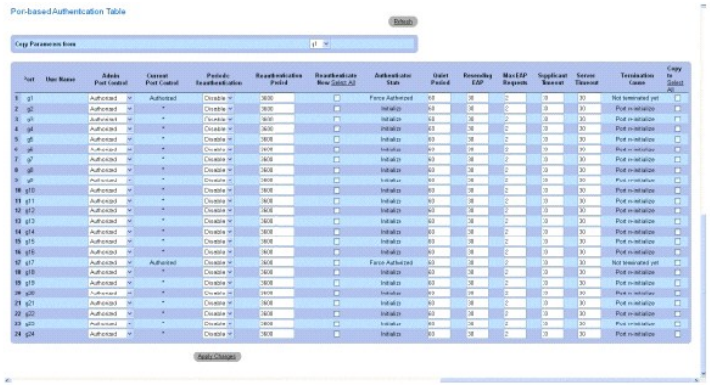
Max EAP Requests（最大 EAP 要求）（1 ～ 10） — 送信される EAP 要求の合計数です。定義された時間内に応答がなかった場合は、認証処理が再スタートされます。デフォルトの試行回数は 2 回です。

ポートベース認証表を表示する

1. **ポートベース認証** ページを表示します。
2. Show All（すべて表示）をクリックします。

次のような **ポートベース認証表** が開きます。

図 7-81. ポートベース認証表



Termination Cause（終了理由）— ポート認証が終了した理由です。

Copy To Checkbox（コピー先チェックボックス）— あるポートのポートパラメーターを、選択したポートにコピーします。

Select All（すべて選択）— **ポートベース認証表** 内のすべてのポートを選択します。

ポートベース認証表のパラメーターのコピー

1. **ポートベース認証** ページを開きます。
2. Show All（すべて表示）をクリックします。

   ポートベース認証表 が開きます。
3. **Copy Parameters from（パラメーターのコピー元）** フィールドからインタフェースを選択します。
4. **ポートベース認証表** からインタフェースを選択します。
5. **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。
6. Apply Changes（変更の適用）をクリックします。

   パラメーターが、**ポートベース認証表** 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ポートベース認証の有効化

次の表は**ポートベース認証** ページ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ための等価 CLI コマンドを、まとめたものです。

表 7-49. ポート認証に関連する CLI コマンド

CLI コマンド	説明
aaa authentication dot1x default *method1* [*method2*.]	IEEE 802.1X を実行するインタフェースで使用する、1 つまたは複数の AAA（認証、許可、アカウンティング）方式を指定します。
dot1x max-req *count*	認証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。
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 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。

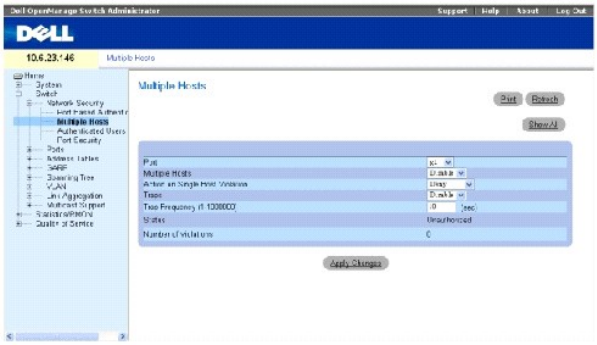
```
console> enable

Console# show dot1x

```

Interface	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
---------	----------	----------	--------	------	--------
g1	Auto	Authorized	Ena	3600	Bob
g2	Auto	Authorized	Ena	3600	John
g3	Auto	Unauthorized	Ena	3600	Clark
g4	Force-auth	Authorized	Dis	3600	n/a

拡張ポートベース認証の設定

複数のホスト ページには、特定のポート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。**複数のホスト** を開くには、Switch（スイッチ） → Network Security（ネットワークセキュリティー） → Multiple Hosts（複数のホスト）をクリックします。

図 7-82. 複数のホスト



Ｐｏｒｔ（ポート） — 拡張ポートベース認証を有効にするポート番号です。

Multiple Hosts（複数のホスト） — 単一のホストから複数のホストにシステムへのアクセスを許可するオプションを有効または無効にします。選択したポートで入口フィルタを無効にするか、ポートロックセキュリティを使用するには、この設定を有効にする必要があります。

Action on Single Host Violation（単一ホスト違反に対する処置） — 所有する MAC アドレスがクライアント（サプリカント）の MAC アドレスではないホストから、単一ホストモードで到達

したパケットに適用する処置を定義します。**Action on Single Host Violation（単一ホスト違反に対する処置）** フィールドを定義できるのは、**複数のホスト** 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。可能なフィールド値は以下のとおりです。

Permit（許可） — 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。

Deny（拒否） — 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、ポートをロックします。ポートをアクティブにするか、デバイスをリセットするまで、ポートはロックされたままです。

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。

トラップの頻度（1 ～ 1000000）（秒） — トラップをホストに送信する時間を定義します。**トラップの頻度（1－1000000）** フィールドを定義できるのは、**複数のホスト** 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以下のとおりです。

Unauthorized（権限なし） — クライアント（サプリカント）には、完全なポートアクセス権が付与されます。

Authorized（権限あり） — クライアント（サプリカント）には、制限付きのポートアクセス権が付与されます。

No single-host（単一ホスト以外） — **Multiple Hosts（複数のホスト）** が有効になります。

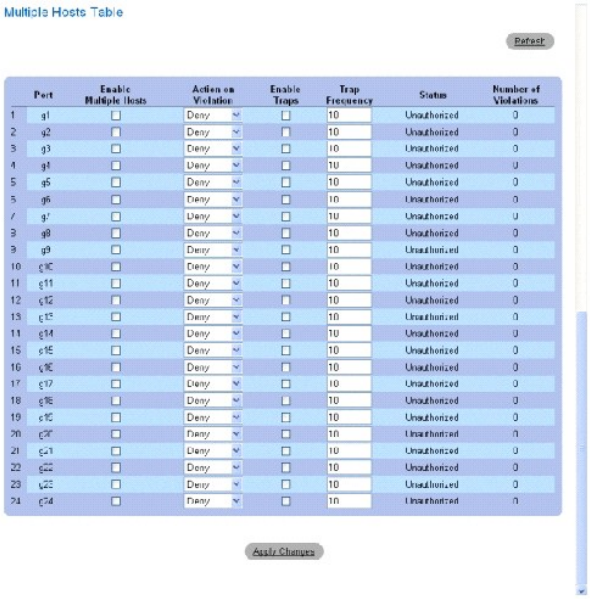
Number of Violations（違反の数） — 所有する MAC アドレスがクライアント（サプリカント）の MAC アドレスではないホストから、単一ホストモードでインタフェースに到達したパケットの数。

複数のホスト表 を表示する

1. **複数のホスト** ページを開きます。
2. Show All（すべて表示）をクリックします。

次のような **複数のホスト表** が開きます。

図 7-83. 複数のホスト表



CLI コマンドを使用した複数のホストの有効化

次の表は**複数のホスト** ページに表示されているように拡張ポートベース認証を有効にするための等価 CLI コマンドを、まとめたものです。

表 7-50. 複数のホストに関連する CLI コマンド

CLI コマンド	説明
dot1x multiple-hosts	dot1x port-control インタフェース設定コマンドが auto に設定されている 802.1X 許可ポートに複数のホスト（クライアント）を許可します。
dot1x single-host-violation {forward |discard |discard-shutdown}[trap seconds]	所有する MAC アドレスがクライアント（サプリカント）の MAC アドレスではないステーションが、インタフェースへのアクセスを試みたときの対応処置を設定します。

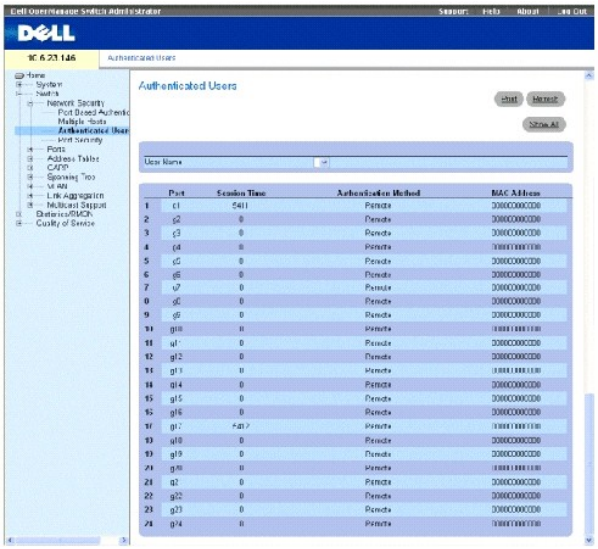
CLI コマンドの例は次のようになります。

```
Neyland# configure

Neyland(config)# interface
ethernet g1

Neyland(config-if)# dot1x
multiple-hosts
```

ユーザーの認証

認証ユーザーページには、ユーザーのポートアクセスリストが表示されます。ユーザーアクセスリストは、ユーザー名の追加ページで定義します。認証ユーザーページを開くには、 Switch(スイッチ) → Network Security（ネットワークセキュリティー） → Authenticated Users（認証ユーザー）をクリックします。

図 7-84. 認証ユーザー



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す。フィールドの書式は **Day:Hour:Minute:Seconds(日数:時間数:分数:秒数)**で、たとえば、3 days: 2 hours: 4 minutes: 39 seconds（3 日: 2 時間: 4 分: 39 秒）となります。

Last Authentication(前回の認証) — ユーザーが最後に認証されてから経過した時間です。フィールドの書式は **日数:時間数:分数:秒数**で、たとえば、3 days: 2 hours:4 minutes: 39 seconds（3 日: 2 時間: 4 分: 39 秒）となります。

Authentication Method（認証方法） — 最後のセッションが認証された方法です。可能なフィールド値は以下のとおりです。

Remote（リモート） — ユーザーは、リモートサーバーから認証されました。

None（なし） — ユーザーは認証されていません。

MAC Address（MAC アドレス） — クライアント（サプリカント）の MAC アドレスです。

認証ユーザー表の表示

1. ユーザー名の追加ページを開きます。
2. Show All（すべて表示）をクリックします。

次のような **認証ユーザー表** が開きます。

図 7-85. 認証ユーザー表

CLI コマンドを使用したユーザーの認証

次の表はユーザー名の追加ページに表示されている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。

表 7-51. ユーザー名の追加に関連する CLI コマンド

CLI コマンド	説明
show dot1x users [username username]	デバイスの 802.1X ユーザーを表示します。

CLI コマンドの例は次のようになります。

```
console# show dot1x users

Username  Session Time  Last Auth  Auth Method  MAC Address        Interface
--------  ------------  ---------  -----------  -----------------  ---------
Bob       1d3h          58m        Remoteg      00:08:3b:79:87:87  g1
John      8h19m         2m         None         00:08:3b:89:31:27  g2
```

ポートセキュリティの設定

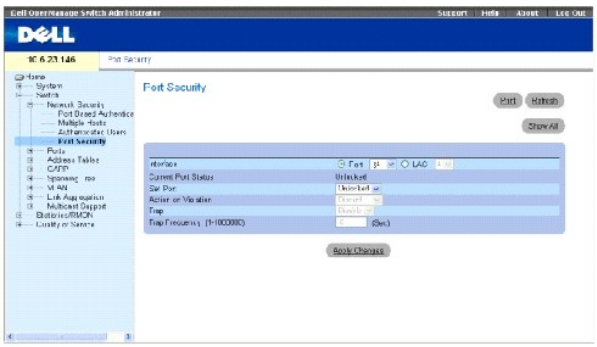
ネットワークセキュリティを高めるには、特定の MAC アドレスを持つユーザーのみに特定のポートへのアクセスを制限します。MAC アドレスは、制限する時点まで動的に学習されたものか、静的に設定したものになります。ポートロックセキュリティは、特定のポートで受信される受信パケットおよび学習パケットをモニターします。ロックされたポートへのアクセスは、特定の MAC アドレスを持つユーザーに制限されます。これらのアドレスは、ポートに対して手動で定義したものか、ポートがロックされた時点までそのポートで学習されたものになります。ロックされたポートでパケットを受信したときに、そのパケットの送信元 MAC アド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実行されます。権限のないパケットが、ロックされたポートに到達すると、次のいずれかの処置が取られます。

- 転送される
- トラップなしで破棄される
- トラップ付きで破棄される
- 入口ポートが無効になる

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。

無効になっているポートは、**ポートパラメーター** ページからアクティブにできます。「ポートパラメーターの定義」を参照してください。**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ー） → Port Security（ポートセキュリティ）をクリックします。

図 7-86. ポートセキュリティ



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（LAG） — 選択されているインタフェースタイプは LAG です。

Current Port Status（現在のポートステータス） — 現在設定されているポートのステータスです。

Set Port（ポートの設定） — ポートをロックまたはロック解除します。可能なフィールド値は以下のとおりです。

Unlocked（ロック解除） — ポートをロック解除します。これがデフォルト値になります。

Locked（ロック） — ポートをロックします。

Action on Violation（違反に対する処置） — ロックされたポートに到達したパケットに適用する処置です。可能なフィールド値は以下のとおりです。

Forward（転送） — 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） — 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ります。

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、ポートをロックします。ポートをアクティブにするか、デバイスをリセットするまで、ポートはロックされたままです。

Trap（トラップ） — ロックされたポートでパケットを受信した時点でトラップが送信されるようにします。

Trap Frequency (1-1000000)（トラップの頻度（1 ～ 1000000）） — トラップの間隔を示す時間（秒単位）です。このフィールドは、ロックされたポートにのみ適用されます。デフォルト値は 10 秒です。

ポートロックを定義する

1. **ポートセキュリティ** ページを開きます。
2. インタフェースのタイプと番号を選択します。
3. フィールドを定義します。
4. **Apply Changes（変更の適用）** をクリックします。

ロックされたポートが **ポートセキュリティ表** に追加され、デバイスがアップデートされます。

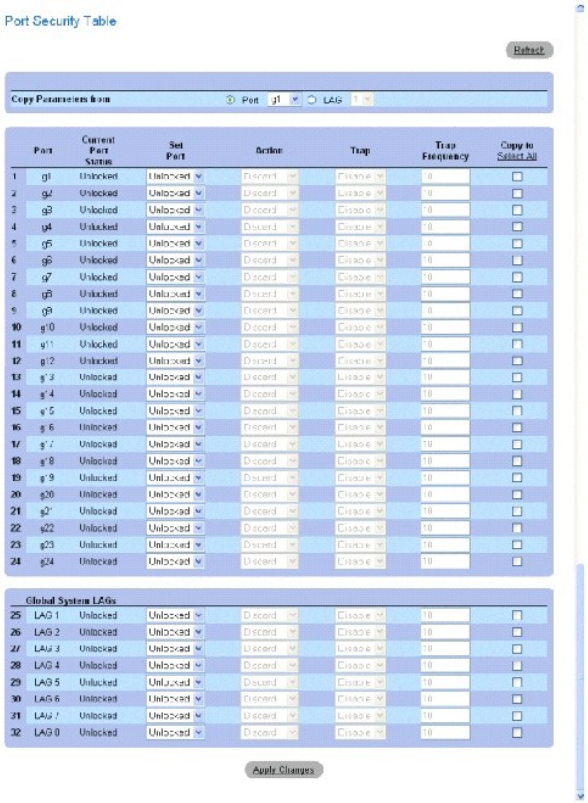
ポートロック表を表示する

1. **ポートセキュリティ** ページを開きます。
2. **Show All（すべて表示）** をクリックします。

次のような **ポートセキュリティ表** が開きます。

ポートロックは、**ポートロック表** でも、**ポートセキュリティ** ページでも定義できます。

図 7-87. ポートセキュリティ表



CLI コマンドを使用したポートロックセキュリティの設定

次の表は **ポートセキュリティ** ページに表示されているように、ポートロックセキュリティを設定するための等価 CLI コマンドをまとめたものです。

表 7-52. ポートセキュリティに関連する CLI コマンド

CLI コマンド	説明
shutdown	インタフェースを無効にします。
set interface active {ethernet interface | port-channel port-channel-number}	ポートセキュリティ上の理由でシャットダウンされたインタフェースを再びアクティブにします。
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
----	-------	-------	-------	---------	-------
g7	Unlocked	Discard	Enable	100	88
g8	Unlocked	Discard, Shutdown	Disable		
g3	Unlocked	-	-	-	-

ポートの設定

ポート ページには、ストームコントロールやポートミラーリングなどの拡張機能を含むポート機能ページへのリンクがあります。**ポート** ページを開くには、 Switch(スイッチ) → Ｐｏｒｔ（ポート）をクリックします。

ポートパラメーターの定義

ポートの設定 ページには、ポートパラメーターを定義するためのフィールドがあります。**ポートの設定** ページを開くには、ツリービューで Switch(スイッチ) → Port（ポート） → Port Configuration（ポートの設定）をクリックします。

図 7-88. ポートの設定

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） — 当該のポートを介したトラフィック転送を有効または無効にします。新規のポートステータスは、**現在のポートステータス** フィールドに表示されます。

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。

Re-Activate Port（ポートの再アクティブ化） — ポートロックセキュリティのオプションによってポートが無効になっている場合に、そのポートを再び有効にします。

Operational Status（動作ステータス） — ポートの動作ステータスです。可能なフィールド値は以下のとおりです。

Suspended（サスペンド） — ポートは現在アクティブですが、トラフィックの送受信は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） — ポートは現在無効であり、トラフィックの送受信も行っていません。

Admin Speed（管理スピード） — ポートに対して設定されている転送レートです。ポートタイプによって、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、設定対象のポートでオートネゴシエイションが無効になっている場合のみです。

Current Port Speed（現在のポートスピード） — 現在設定されている実際のポートスピード（bps）です。

Admin Duplex（管理二重モード） — ポートの二重モードは、**全二重** または **半二重** のいずれかになります。**全二重** は、デバイスとそのリンクパートナー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。**半二重** は、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） — 現在設定されているポートの二重モードです。

Auto Negotiation（オートネゴシエイション） — ポートに対してオートネゴシエイションを有効にします。オートネゴシエイションは、リンクのパートナー間のプロトコルであり、一方のポートから、その転送レート、二重モード、およびフロー制御の機能を他方に伝えられるようにします。

Current Auto Negotiation（現在のオートネゴシエイション） — 現在のオートネゴシエイションの設定です。

Back Pressure（バックプレッシャー） — ポートに対してバックプレッシャーモードを有効にします。バックプレッシャーモードは、半二重モードと併用し、ポートでメッセージを受信できないようにします。

Current Back Pressure（現在のバックプレッシャー） — 現在のバックプレッシャーの設定です。

Flow Control（フロー制御） — フロー制御を有効または無効にするか、ポートに対してフロー制御のオートネゴシエイションを有効にします。ポートが全二重モードのときに機能します。

Current Flow Control（現在のフロー制御） — 現在のフロー制御の設定です。

MDI/MDIX — デバイスがクロスケーブルとストレートケーブルを判別できるようにします。

ハブとスイッチの配線は、故意にエンドステーションの配線と逆にすることで、ハブまたはスイッチをエンドステーションに接続する場合に、ストレートスルー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。可能なフィールド値は以下のとおりです。

Auto（自動） — ケーブルタイプを自動的に検知するために使用します。

MDI（Media Dependent Interface） — エンドステーションに使用します。

MDIX（Media Dependent Interface with Crossover） — ハブおよびスイッチに使用します。

Current MDI/MDIX（現在の MDI/MDIX） — デバイスの現在の MDI/MDIX 設定です。

LAG — ポートが LAG に属しているかどうかを示します。

ポートパラメーターを定義する

1. **ポートの設定** ページを開きます。
2. **Port（ポート）** フィールドでポートを選択します。
3. 残りのフィールドを定義します。
4. **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。

ポートパラメーターの変更

1. **ポートの設定** ページを開きます。
2. **Port（ポート）** フィールドでポートを選択します。
3. 残りのフィールドを変更します。
4. **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。

ポート設定表の表示：

1. **ポートの設定** ページを開きます。
2. **Show All（すべて表示）** をクリックします。

次のような **ポートの設定表** が開きます。

図 7-89. ポートの設定表

CLI コマンドを使用したポートの設定

次の表はポートの設定表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 7-53. ポートの設定に関連する 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内のインタフェースを無効にします。
set interface active {**ethernet** *interface* | **port-channel** *port-channel-number*}	セキュリティ上の理由でシャットダウンされたインタフェースを再びアクティブにします。
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。
autobaud	ボーレートを自動検知するための行を設定します。
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	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 | rx | tx}	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 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 g5


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

```
Console (config-if)# shutdown

Console (config-if)# no shutdown

Console (config-if)# speed 100

Console (config-if)# duplex full

Console (config-if)# negotiation

Console (config-if)# back-pressure

Console (config-if)# flowcontrol on

Console (config-if)# mdix auto

Console(config-if)# exit

Console(config)# exit

Console# show interfaces configuration ethernet g5
```

Port	Typev	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Modeh
----	-----	------	-----	----	------	-----	------	----
g5	1G	Full	100	Enabled	On	Up	Enable	Auto

```
console#

console# show interfaces status ethernet g5
```

Port	Typev	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Modeh
----	-----	------	-----	----	------	-----	------	----
g5	1G	Full	100	Enabled	On	Up	Disabled	on

```
console#
```

```
Console# show interfaces status
```

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Modeh
----	-----	------	-----	----	------	-----	------	----
g1	1G	Full	100	Auto	On	Up	Enable	On
g1	100	Full	100	Offt	Off	Down	Disable	Off
g2	100	Full	1000	Off	Off	Up	Disable	On
Ch	Typev	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	-----	---	----	-------	-------	------	
1	1000	Full	1000	Offt	Off	Disable	Up	

LAG パラメーターの定義

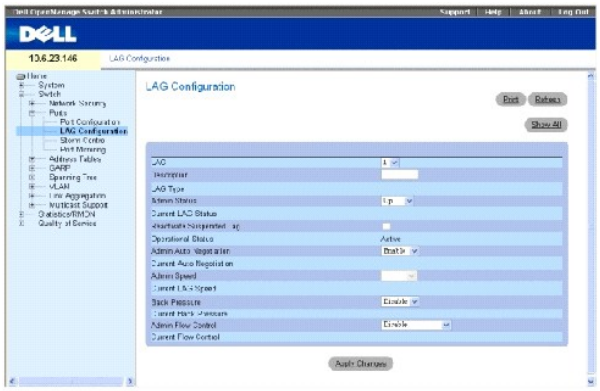
LAG の設定 ページには、設定済みの LAG に関するパラメーターを設定するためのフィールドがあります。デバイスでは、LAG ごとに最大 8 つのポートと、システムごとに 8 つの LAG をサポートしています。

リンク集約グループ（LAG：Link Aggregated Groups）および、LAG へのポートの割り当てに関しては、**ポートの集約** を参照してください。

LAG の設定 ページを開くには、ツリービューで Switch(スイッチ) → Ｐｏｒｔ（ポート） → LAG Configuration（LAG の設定）をクリックします。

メモ: 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。

図 7-90. LAG の設定



LAG — LAG の番号です。

Description (0-64 Characters)（説明（0 ～ 64 文字）） — 設定済みの LAG に関するユーザー定義の説明を示します。

LAG Type（LAG タイプ） — LAG を構成するポートのタイプです。

Admin Status（管理ステータス） — 選択した LAG を介したトラフィック転送を有効または無効にします。

Current LAG Status（現在の LAG ステータス） — LAG が現在動作しているかどうかを示します。

Re-Activate Suspended LAG（サスペンド中の LAG の再アクティブ化） — サスペンド中の LAG を再びアクティブにします。

Operational Status（動作ステータス） — LAG の動作ステータスです。

Admin Auto Negotiation（管理オートネゴシエイション） — LAG に対してオートネゴシエイションを有効または無効にします。オートネゴシエイションは、リンクのパートナー間のプロトコルであり、一方の LAG からその転送レート、二重モード、およびフロー制御（デフォルトではフロー制御は無効になります）の機能を他方に伝えられるようにします。

Current Auto Negotiation（現在のオートネゴシエイション） — 現在のオートネゴシエイションの設定です。

Admin Speed（管理スピード） — LAG の動作スピードです。

Current LAG Speed（現在の LAG スピード） — 現在設定されている LAG の動作スピードです。

Admin Back Pressure（管理バックプレッシャー） — LAG に対してバックプレッシャーモードを有効または無効にします。バックプレッシャーモードは、LAG の中で半二重モードで動作するポートに効果があります。

Current Back Pressure（現在のバックプレッシャー） — 現在のバックプレッシャーの設定です。

Current Flow Control（管理フロー制御） — フロー制御を有効または無効にするか、ポートに対してフロー制御のオートネゴシエイションを有効にします。フロー制御モードは、LAG の中で全二重モードで動作するポートに効果があります。

現在のフロー制御 — ユーザー指定のフロー制御の設定です。

LAG パラメーターの定義

1. **LAG の設定** ページを開きます。
2. **LAG** フィールドで LAG を選択します。
3. フィールドを定義します。
4. **Apply Changes（適用の変更）** 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

1. **LAG の設定** ページを開きます。
2. **LAG** フィールドで LAG を選択します。
3. フィールドを変更します。
4. **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 の設定表の表示：

1. **LAG の設定** ページを開きます。
2. **Show All（すべて表示）** をクリックします。

次のような **LAG の設定表** が開きます。

図 7-91. LAG の設定表

CLI コマンドを使用した LAG の設定

次の表は **LAG の設定** ページに表示されているように、LAG を設定するための等価 CLI コマンドをまとめたものです。

表 7-54. 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内のインタフェースを無効にします。
speed *bps*	オートネゴシエイションを使用しない場合に、所定のイーサネットインタフェースのスピードを設定します。

autobaud	ボーレートを自動検知するための行を設定します。
negotiation	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 | rx | tx}	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-if)# channel-group 1 mode on

console(config-if)# exit

console(config)# interface range e g21-24

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

console(config-if)# ex

console(config)# interface ethernet g5

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

console(config-if)# exit

console(config)# exit
```

```
console# show interfaces port-channel
```

Channel	Ports
---------	---------
ch1	Inactive: g(21-24)
ch2	Active: g5
ch3	

ch4	
ch5	
ch6	
ch7	
ch8	
console#	

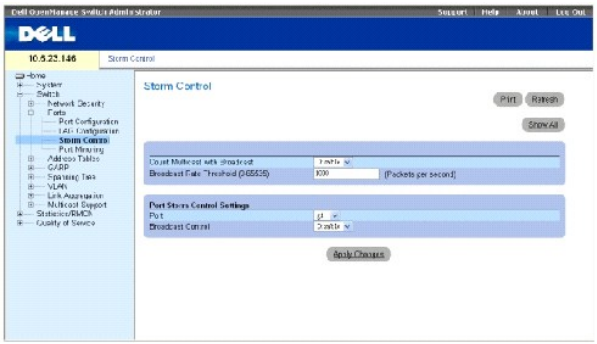
ストームコントロールの有効化

ブロードキャストストームは、単一のポートからネットワーク上に過剰な量のブロードキャストメッセージが同時に送信された場合に発生します。送信されたメッセージの応答がネットワークに蓄積され、ネットワークリソースの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。

システムでは、ポートごとに着信したブロードキャストおよびマルチキャストのフレームレートを個別に測定し、そのレートがユーザー定義のレートを超えた場合にフレームを破棄します。

ストームコントロール ページには、ストームコントロールを有効にして設定するためのフィールドがあります。ストームコントロール 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（ストームコントロール）をクリックします。

図 7-92. ストームコントロール



Count Multicast with Broadcast（マルチキャストとブロードキャストのカウント） — 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カウントします。可能なフィールド値は以下のとおりです。

- **Enable（有効）** — 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カウントします。
- **Disable（無効）** — ブロードキャストトラフィックのみをカウントします。

ブロードキャストレートしきい値（1 ～ 1000000） — 未知のパケットが転送される最大レート（1 秒あたりのパケット数）です。範囲は 0 ～ 1000000 です。デフォルト値は 0 です。すべての値は、最も近い 64 Kbps に繰り上げられます。フィールド値が 64 Kbps に満たない場合、値 0 以外は 64 Kbps に繰り上げられます。

Port（ポート） — ストームコントロールを有効にするポートです。

Broadcast Control（ブロードキャストコントロール） — デバイスに対してブロードキャストパケットタイプの転送を有効または無効にします。

デバイスのストームコントロール有効化

1. ストームコントロール ページを開きます。
2. ストームコントロールを実装するインタフェースを選択します。
3. フィールドを定義します。
4. **Show All（すべて表示）** をクリックします。

ストームコントロールがデバイスに対して有効になります。

ストームコントロールポートパラメーターの変更

1. ストームコントロール ページを開きます。
2. フィールドを変更します。
3. **Show All（すべて表示）** をクリックします。

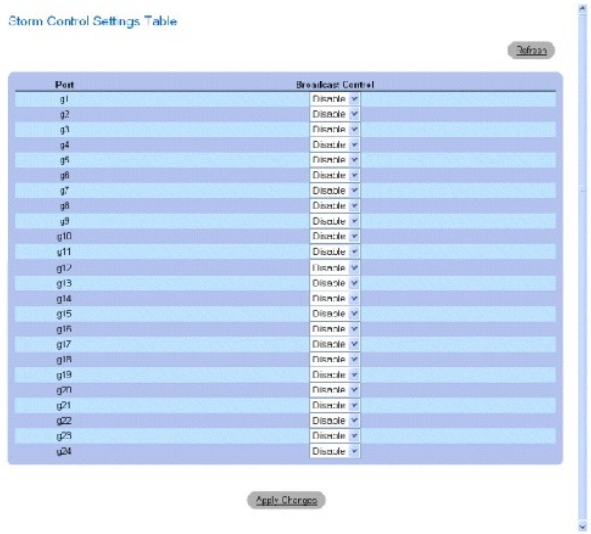
ストームコントロールのポートパラメーターがデバイスに保存されます。

ポートパラメーター表の表示

1. ストームコントロール ページを開きます。
2. **Show All（すべて表示）** をクリックします。

次のような ストームコントロールの設定表 が開きます。

図 7-93. ストームコントロールの設定表



CLI コマンドを使用したストームコントロールの設定

次の表はストームコントロールページの表示に表示されているように、ストームコントロール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 7-55. ストームコントロールに関連する 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と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 *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 [**ethernet** *interface*]	ストームコントロール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> enable

console#configure

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

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

Console(config)# interface ethernet g1

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

Console(config-if)# end

Console# show ports storm-control

Port    Broadcast Storm control [Packets/sec]
----    --------------------------------------
g1      8000
g2      Disabled
g4      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、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ー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。

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。

- モニター対象のポートは、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 パケットがモニターされます。

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。

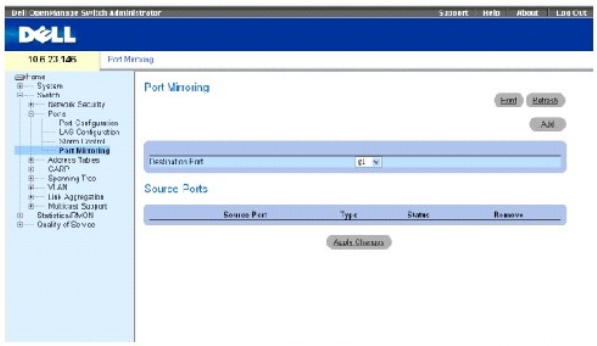
送信元ポートとして設定されているポートには、次の制限が適用されます。

- 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。
- すべてのパケットは、宛先ポートからタグ付きで送信されます。
- 同一ポートへのすべての RX/TX パケットがモニターされます。

ポートミラーリング ページを開くには、ツリービューで **Switch(スイッチ)** → **Ports（ポート）** → **Port Mirroring（ポートミラーリング）** をクリックします。

メモ: ポートをポートミラーリングセッションのターゲットポートとして設定すると、そのポートに関するすべての通常動作がサスペンドされます。この動作には、スパニングツリーおよび LACP も含まれます。

図 7-94. ポートミラーリング



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。

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） — 送信元ポートが RX か TX、または RX と TX の両方であることを示します。

Status（ステータス） — ポートが現在モニターされているか（**アクティブ**）、モニターされていないか（**モニター可能**）を示します。

Remove（削除） — この項目を選択すると、ポートミラーリングセッションが削除されます。

ポートミラーリングセッションの追加

1. ポートミラーリングページを開きます。
2. **Add（追加）** をクリックします。

送信元ポートの追加 ページが開きます。

3. **Destination Port（宛先ポート）**ドロップダウンメニューから宛先ポートを選択します。
4. **Source Port（送信元ポート）**ドロップダウンメニューから送信元ポートを選択します。
5. **Type（タイプ）**フィールドを定義します。
6. **Apply Changes（変更の適用）**をクリックします。

新規の送信元ポートが定義され、デバイスがアップデートされます。

ポートミラーリングセッションからのコピーポート削除

1. ポートミラーリングページを開きます。
2. **Remove（削除）** チェックボックスを選択します。
3. **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

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 7-56. 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 g1

Console(config-if)# port monitor g8

Console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
----------	---------------	----------	-------	----------
g8	g1	RX, TX	Active	No
g2	g8	RX, TX	Active	No

g18	g8	Rx	Active	No

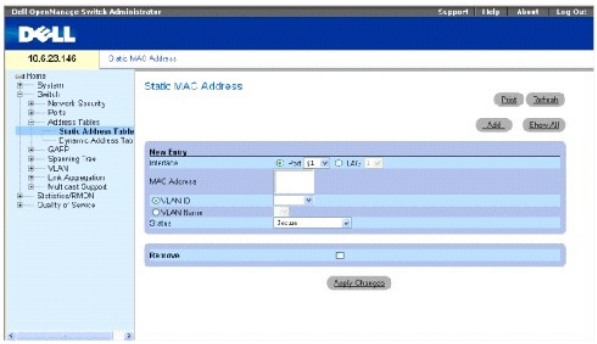
アドレス表の設定

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。静的アドレス表および動的アドレス表には、インタフェース、VLAN、およびインタフェースタイプを保存できます。MAC アドレスは、パケットが送信元からデバイスに到達した時点で動的に学習されます。フレームの送信元アドレスからポートを学習することによって、アドレスがポートに関連付けられます。いずれのポートにも関連付けられていない MAC アドレスが宛先に指定されているフレームは、関連する VLAN のすべてのポートに送信されます。静的アドレスは手動で設定します。ブリッジ表が満杯にならないようにするため、一定の期間にトラフィックが送信されなかった動的 MAC アドレスは消去されます。**アドレス表** ページを開くには、ツリービューで **Switch(スイッチ)** → **Address Table（アドレス表）** をクリックします。

静的アドレスを定義する

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。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。静的 MAC アドレスページを開くには、ツリービューで **Switch(スイッチ)** → **Address Table（アドレス表）** → **Static Address（静的アドレス）** をクリックします。

図 7-95. 静的 MAC アドレス



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。可能な値は以下のとおりです。

Secure（保護） — ロックされているポートの MAC アドレスは削除されないことを保証します。

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。

Remove（削除） — この項目を選択すると、対象の MAC アドレスが MAC アドレス表から削除されます。

静的 MAC アドレスの追加

1. 静的 MAC アドレスページを開きます。
2. **Add（追加）** をクリックします。

   静的 MAC アドレスの追加 ページが開きます。
3. フィールドを完了します。
4. **Apply Changes（変更の適用）** をクリックします。

   新規の静的アドレスが **静的 MAC アドレス表** に追加され、デバイスがアップデートされます。

静的 MAC アドレス表にある静的アドレスの変更

1. 静的 MAC アドレスページを開きます。
2. フィールドを変更します。
3. **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

1. 静的 MAC アドレスページを開きます。
2. **Show All（すべて表示）** をクリックします。

   静的 MAC アドレス表 が開きます。
3. 表のエントリを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. **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

次の表は静的 MAC アドレスページの表示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 7-57. 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* {**ethernet** *interface* | **port-channel** *port-channel-number*} [**permanent** | **delete-on-reset** | **delete-on-timeout** | **secure**]]	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# show bridge address-table

Aging time is 300 sec

```

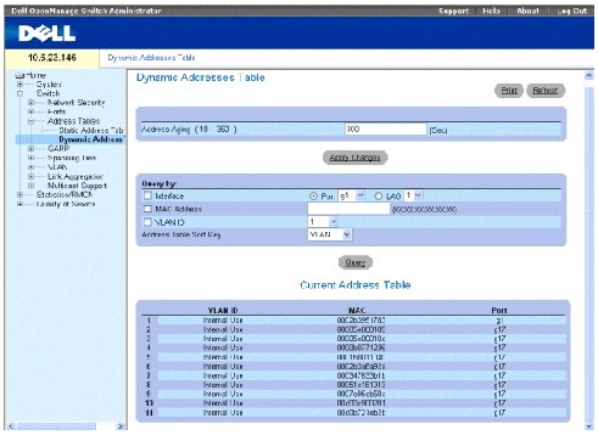
vlan	mac address	port	type
----	------------	----	--------
1	00:60:70:4C:73:FF	g8	dynamic
1	00:60:70:8C:73:FF	g8	dynamic
200	00:10:0D:48:37:FF	g9	static
g8	00:10:0D:98:37:88	g8	dynamic

動的アドレスの表示

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情報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。また、動的アドレス表には、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指示する動的アドレスパラメーターが定義されています。

動的アドレス表を開くには、ツリービューで **Switch(スイッチ)** → **Address Table（アドレス表）** → **Dynamic Addresses Table（動的アドレス表）** をクリックします。

図 7-96. 動的アドレス表



Address Aging (10-360)（アドレスエージング（10 ～ 360）） — MAC アドレスが動的アドレス表に留まる時間を指定します。この時間を過ぎても、その MAC アドレスを送信元としたトラフィックが検知されない場合、その MAC アドレスはタイムアウトになります。デフォルト値は 300 秒です。

Interface（インタフェース） — 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。

Port（ポート） — 表にクエリするポート番号を指定します。

LAG — 表にクエリする LAG を指定します。

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。

エージング時間の再定義

1. 動的アドレス表を開きます。
2. **Aging Time（エージング時間）** フィールドを定義します。
3. 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

1. 動的アドレス表を開きます。
2. **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、**ポート**、**MAC アドレス**、または **VLAN ID** を基準としてクエリできます。

3. **Query（クエリ）** をクリックします。

動的アドレス表がクエリされます。

動的アドレス表のソート

1. 動的アドレス表を開きます。
2. **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。
3. **Query（クエリ）** をクリックします。

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、動的アドレスをクエリおよびソートしたための CLI コマンドをまとめたものです。

表 7-58. 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)# exit
```

```
Console# show bridge address-table

Aging time is 250 sec

vlan  mac address        port  type
----  -----------        ----  ----
1     00:60:70:4C:73:FF  g8    dynamic
1     00:60:70:8C:73:FF  g8    dynamic
200   00:10:0D:48:37:FF  g8    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一組のデバイスを定義します。

GARP を設定する際には、次の点を確認してください。

- Leave 時間は、Join 時間の 3 倍以上にする必要があります。
- Leave All 時間は Leave 時間より長くする必要があります。

すべてのレイヤ 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** をクリックします。

GARP タイマーの定義

GARP タイマーページには、デバイスに対して GARP を有効にするためのフィールドがあります。GARP タイマーページを開くには、ツリービューで **Switch(スイッチ)** → **GARP** → **GARP Timers（GARP タイマー）** をクリックします。

図 7-97. GARP タイマー

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 Join タイマー（10 ー 2147483640）） ― PDU が転送される時間（ミリ秒単位）です。可能なフィールド値は 10 ～ 2147483640 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。可能なフィールド値は 0 ～ 2147483640 です。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。可能なフィールド値は 0 ～ 2147483640 です。デフォルト値は 10000 ミリ秒です。

GARP タイマーの定義

1. GARP タイマーページを開きます。
2. フィールドを完了します。
3. **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

1. GARP タイマーページを開きます。
2. **Show All（すべて表示）** をクリックします。

GARP タイマー表 が開きます。

3. **Copy Parameters from（パラメーターのコピー元）** フィールドでインタフェースタイプを選択します。
4. **Port（ポート）** または **LAG** ドロップダウンメニューからインタフェースを選択します。
5. このインタフェースに対する定義が、選択したインタフェースにコピーされます。手順 6 を参照してください。
6. **Copy to（コピー先）** チェックボックスをオンにして、GARP タイマーの定義をコピーするインタフェースを定義するか、**Select AI（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。
7. **Apply Changes（変更の適用）** をクリックします。

パラメーターが、**GARP タイマー表** で選択したポートまたは LAG にコピーされ、デバイスがアップデートされます。

CLI コマンドを使用した GARP タイマーの定義

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 7-59. 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 g1
```

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

console(config-if)# end

console# show gvrp configuration ethernet g1


GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port(s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
g1	Disabled	Normal	Enabled	200	900	10000

```
console#
```

スパニングツリープロトコルの設定

スパニングツリープロトコル（STP）は、ブリッジの配置に関係なくツリー構造を提供します。また、ネットワーク上のエンドステーション間に 1 つのパスを提供し、ループを排除します。

ループは、ホスト間に代替パス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プロトコルをサポートしています。

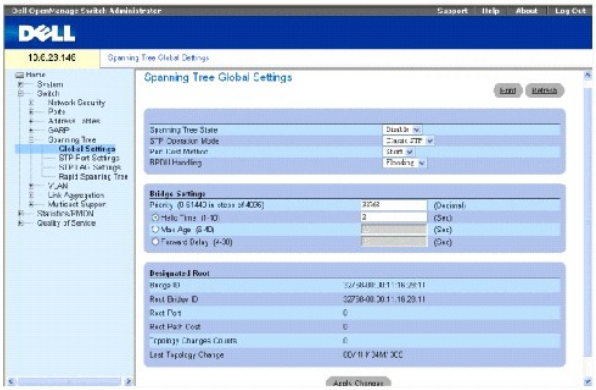
- 標準 STP— エンドステーション間に 1 つのパスを提供し、ループを回避および排除します。標準 STP の設定の詳細に関しては、「STP グローバル設定の定義」を参照してください。
- 高速 STP — 転送ループを作成せずに、スパニングツリーをより迅速に収束できるネットワークトポロジを検知して使用します。高速 STP の設定の詳細に関しては、「高速スパニングツリーの設定」を参照してください。

スパニングツリー ページを開くには、ツリービューで **Switch(スイッチ)** → **Spanning Tree（スパニングツリー）** をクリックします。

STP グローバル設定の定義

STP グローバル設定ページには、デバイスに対して STP 動作を有効にして設定するためのパラメーターがあります。STP グローバル設定ページを開くには、ツリービューでSwitch(スイッチ) → Spanning Tree（スパニングツリー） → Global Settings（グローバル設定）をクリックします。

図 7-98. STP グローバル設定



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以下のとおりです。

- **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 ModeSTP（動作モード） — デバイスに対して有効にする STP のモードです。可能なフィールド値は以下のとおりです。

Classic STP（標準 STP） — デバイスに対して標準 STP を有効にします。これがデフォルト値になります。

Rapid STP（高速 STP） — デバイスに対して高速 STP を有効にします。

Port Cost Method（ポートコスト方法） — スパニングツリーのデフォルトのパスコスト方法を決定します。可能なフィールド値は以下のとおりです。

Short（ショート） — ポートのパスコストに 1 ～ 65535 の範囲を指定します。これがデフォルト値になります。

Long（ロング） — ポートのパスコストに 1 ～ 200000000 の範囲を指定します。

BPDU Handling（BPDU 処理） — ポートまたはデバイスに対して STP が無効である場合に、BPDU パケットを管理する方法を決定します。BPDU は、スパニングツリー情報の送信に使用します。可能なフィールド値は以下のとおりです。

Filtering（フィルタリング） — インタフェースに対してスパニングツリーが無効である場合に、BPDU パケットをフィルタにかけます。

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。これがデフォルト値になります。

Priority (0-61440, in steps of 4096)（優先度（0 ～ 61440、4096 段階）） — ブリッジ優先度値を指定します。スイッチまたはブリッジが STP を実行している場合は、それぞれに優先度が割り当てられます。BPDU を交換した後、優先度の最も低いスイッチがルートブリッジになります。デフォルト値は 32768 です。ブリッジ優先度は、0、4096、8192 などのように、4096 単位（4K 増分）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。転送遅延時間は、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。

Bridge ID（ブリッジ ID） — ブリッジ優先度と MAC アドレスを識別します。

Root Bridge ID（ルートブリッジ ID） — ルートブリッジ優先度と MAC アドレスを識別します。

Root Port（ルートポート） — このブリッジからルートブリッジに最低コストのパスを提供するポート番号です。この設定は、ブリッジがルートでない場合に重要です。デフォルトは 0 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） — 前回の再起動以降に 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、0 日 1 時間 34 分 38 秒のように日,時間,分,秒の書式で表示されます。

STP グローバルパラメーターの定義

1. STP グローバル設定ページを開きます。
2. **Select a Port（ポートの選択）** ドロップダウンメニューから、有効にする必要があるポートを選択します。
3. **Spanning Tree State（スパニングツリーの状態）** フィールドで **Enable（有効）** を選択します。
4. **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。
5. **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

1. STP グローバル設定ページを開きます。
2. ダイアログ内のフィールドを定義します。
3. **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STP グローバル設定ページに表示されているように、STP グローバルパラメーターを定義するための CLI コマンドをまとめたものです。

表 7-60. 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}	スパニングツリープロトコルを設定します。

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、デバイスが他のスイッチにハローメッセージをブロードキャストする頻度です。
spanning-tree max-age *seconds*	スパニングツリーブリッジの最大エージを設定します。
spanning-tree forward-time *seconds*	スパニングツリーブリッジの転送遅延時間を設定します。転送遅延時間は、ポートが転送状態に入る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*]	スパニングツリー設定の識別子を表示します。
show spanning-tree [**detail**] [**active** | **blockedports**]	スパニングツリー設定情報、すなわち、アクティブポートまたはブロックポートに関する詳細情報を表示します。

CLI コマンドの例は次のようになります。

```
console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288

console(config)# spanning-tree hello-time 5

console(config)# spanning-tree max-age 15

console(config)# spanning-tree forward-time 25

console(config)# exit

console# show spanning-tree


Spanning tree enabled mode RSTP

Default port cost method: short

Root ID     Priority    12288
            Address     00:e8:00:b4:c0:00
            This switch is the root
            Hello Time 5 sec Max Age 15 sec Forward Delay 25 sec

Number of topology changes 5 last change occurred 00:05:28 ago
```

Times: hold 1, topology change 40, notification 5

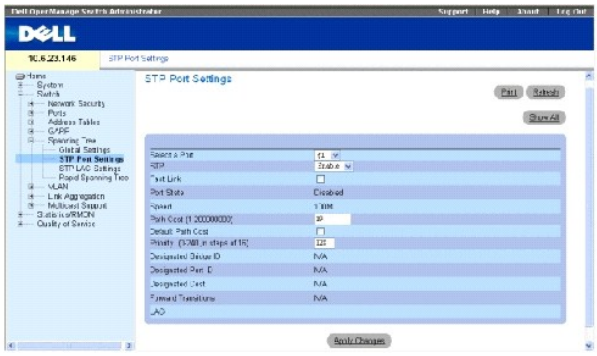
hello 5, max age 15, forward delay 25

Interfaces							
Name	Status	Prio. Nbr	Cost	Sts	Role	PortFast	Type
-----	------	-----	----	------	------	---------	------
g1	enabled	128.1	100	DSBL	Dsbl	No	P2p (STP)
g2	enabled	128.2	100	DSBL	Dsbl	No	P2p (STP)
g3	enabled	128.3	100	DSBL	Dsbl	No	P2p (STP)

STP ポートの設定の定義

STP ポートの設定 ページには、STP プロパティを個々のポートに割り当てるためのフィールドがあります。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）**をクリックします。

図 7-99. STP ポートの設定



Select a Port（ポートの選択） — STP を有効にするポートです。

STP — ポートに対して STP を有効または無効にします。

Fast Link（高速リンク） — この項目を選択すると、ポートに対して高速リンクモードが有効になります。ポートに対して高速リンクモードを有効にすると、ポートリンクが動作している場合 **ポート状態** が自動的に **転送** 状態になります。高速リンクモードは、STP プロトコルによる収束の所要時間を最適化します。STP の収束には、大規模なネットワークで 30 ～ 60 秒かかる場合があります。

Port State（ポート状態） — 現在のポートの STP 状態です。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） — ポートリンクは現在停止しています。

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。

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（デフォルトのパスコスト） — ポートのデフォルトのパスコストは、ポートスピードおよびデフォルトのパスコスト方法によって自動的に設定されます。

ロングパスコストのデフォルト値は、次のとおりです。

イーサネット - 2000000

ファーストイーサネット- 200000

ギガビットイーサネット- 20000

ショートパスコストのデフォルト値（ショートパスコストがデフォルトになります）は次のとおりです。

イーサネット - 100

ファーストイーサネット- 19

ギガビットイーサネット- 4

Priority (0-240, in steps of 16)（優先度（0 ～ 240、16 段階）） — 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） — 選択されているポートの優先度およびインタフェースです。

Designated Cost（指定コスト） — STP トポロジに関係するポートのコストです。コストの低いポートほど、STP でループが検知された場合にブロックされにくくなります。

Forward Transitions（転送への推移） — ポートが **ブロック** 状態から **転送状態** に変化した回数です。

LAG — ポートが属している LAG です。

ポートに対する STP の有効化

1. **STP ポートの設定** ページを開きます。
2. **STP Port StatusSTP（ポートのステータス）** フィールドで **Enabled（有効）** を選択します。
3. **Fast Link（高速リンク）**、**Path Cost（パスコスト）**、および **Priority（優先度）** フィールドを定義します。
4. **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

1. **STP ポートの設定** ページを開きます。
2. **Priority（優先度）**、**Fast Link（高速リンク）**および **Path Cost（パスコスト）**を変更します。
3. **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

1. **STP ポートの設定** ページを開きます。
2. **Show All（すべて表示）** をクリックします。

STP ポート表 が開きます。

CLI コマンドを使用した STP ポート設定の定義

次の表は**STP ポートの設定** ページに表示されているように、STP ポートパラメーターを定義するための CLI コマンドをまとめたものです。

表 7-61. 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。
spanning-tree portfast	PortFast モードを有効にします。
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 g5
```

```
console(config-if)# spanning-tree disable

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

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

console(config-if)# exit

console(config)# exit

console# show spanning-tree ethernet g5
```

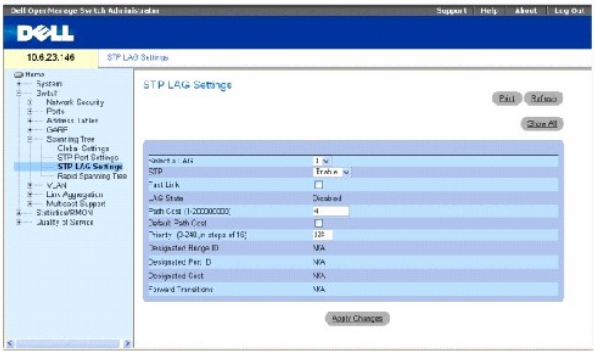
```
Port g5 disabled

State: disabled

Port id: 96.5

以下を入力します。P2p (configured: Auto)
STP

Designated bridge Priority : 32768

Designated port id: 96.5

Number of transitions to forwarding
state: 0

BPDU: sent 0, received 0

console#
```

```
Role: disabled

Port cost: 35000

Port Fast: No (configured: No)

Address:  00:e8:00:b4:c0:00

Designated path cost: 19
```

STP LAG の設定の定義

STP LAG の設定ページには、STP ポート集約パラメーターを割り当てるためのフィールドがあります。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 の設定）** をクリックします。

図 7-100. STP LAG の設定



Select a LAG（LAG の選択） — ユーザー定義の LAG です。詳細に関しては、「LAG メンバーシップの定義」を参照してください。

STP — LAG に対して STP を有効または無効にします。

Fast Link（高速リンク） — LAG に対して高速リンクモードが有効になります。LAG に対して高速リンクモードを有効にすると、LAG が動作している場合 **LAG State（LAG 状態）** が自動的に **転送** 状態になります。 高速リンクモードは、STP プロトコルによる収束の所要時間を最適化します。STP の収束には、大規模なネットワークで 30 ～ 60 秒かかる場合があります。

LAG State（LAG 状態） — LAG の現在の STP 状態です。この項目を有効にすると、LAG 状態によって、トラフィックに対する転送処置が確定します。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 リンクは現在停止しています。

Blocking（ブロッキング） — LAG は現在ブロックされていて、トラフィックの転送や MAC アドレスの学習に使用することができません。

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。

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。パスコストには、1 ～ 200000000 の値を設定します。パスコスト方法がショートである場合、LAG コストのデフォルト値は 4 になります。パスコスト方法がロングである場合、LAG コストのデフォルト値は 20000 になります。

Default Path Cost（デフォルトパスコスト） — この項目を選択すると、LAG のパスコストがデフォルト値に戻ります。

Priority (0-240, in steps of 16)（優先度（0 ～ 240、16 段階）） — LAG 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 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） — 指定ポートのポート優先度およびインタフェース番号です。

Designated Cost（指定コスト） — 指定ブリッジのコストです。

Forward Transitions（転送への推移） — **LAG 状態** が **ブロッキング** 状態から **転送** 状態に変化した回数です。

STP LAG パラメーターの変更

1. STP LAG の設定ページを開きます。
2. **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。
3. 必要に応じてフィールドを変更します。
4. **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。

CLI コマンドを使用した STP LAG の設定の定義

次の表は STP LAG の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 7-62. STP LAG の設定に関連する CLI コマンド

CLI コマンド	説明
spanning-tree	スパニングツリーを有効にします。
spanning-tree disable	特定の LAG に対してスパニングツリーを無効にします。
spanning-tree cost *cost*	スパニングツリーコストに対する LAG のコントリビューションを設定します。
spanning-tree port-priority *priority*	ポートの優先度を設定します。
show spanning-tree [**ethernet** *interface* | **port-channel** *port-channel-number*]	スパニングツリーの設定を表示します。
show spanning-tree [**detail**] [**active** | **blockedports**]	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 port-priority 16
```

高速スパニングツリーの設定

標準スパニングツリーでは、一般的なネットワークトポロジにおける L2 転送ループの防止が保証されますが、収束に最大 30 ～ 60 秒かかる場合があります。この収束時間は、多くのアプリケーションにとって長すぎると見なされます。ネットワークトポロジによっては、より迅速な収束が可能な場合もあります。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。

RSTP には、次のポート状態があります。

- Disabled（無効）
- Learning（ラーニング）
- Discarding（破棄）
- Forwarding（転送）

高速スパニングツリーは、**STP グローバル設定** ページで有効にします。高速スパニングツリーページを開くには、ツリービューで **Switch(スイッチ)** → **Spanning Tree（スパニングツリ**

ー） → **Rapid Spanning Tree（高速スパニングツリー）** をクリックします。

図 7-101. 高速スパニングツリー

Interface（インタフェース） — 高速 STP が有効に設定されているポートまたは LAG です。

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。可能なフィールド値は以下のとおりです。

Root（ルート） — パケットをルートデバイスに転送する最低コストのパスを示します。

Designated（指定） — LAN に接続されている指定デバイスを経由するポートまたは LAG です。

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、2 つのポートがループ接続している場合にのみ提供されます。また、LAN で 2 つ以上のポートが共有セグメントに接続している場合にも、バックアップポートが提供されます。

Disabled（無効） — ポートはスパニングツリーに関与していません（ポートのリンクが停止しています）。

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。ポートに対して高速リンクが有効である場合、ポートは自動的に転送状態になります。

Point-to-Point Admin Status（ポイントツーポイント管理ステータス） — デバイスによるポイントツーポイントリンクの確立を有効または無効にするか、デバイスがポイントツーポイントリンクを自動的に確立するように指定します。

ポイントツーポイントリンクを介した通信を確立するには、送信元の PPP がまず Link Control Protocol（LCP）パケットを送信してデータリンクを設定およびテストします。リンクが確立され、必要に応じて LCP によるオプション機能のネゴシエーションが行われると、送信元の PPP は、1 つまたは複数のネットワーク層プロトコルを選択して設定するために Network Control Protocol（NCP）パケットを送信します。選択された各ネットワーク層プロトコルが設定されると、各ネットワーク層プロトコルからのパケットはリンクを介して送信可能になります。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。このリンクが、実際のデバイスポートリンクタイプになります。このリンクの状態は、管理状態とは異なる場合があります。

Point-to-Point Operational Status（ポイントツーポイントの動作ステータス） — ポイントツーポイントの動作状態です。

Activate Protocol Migrational Test（アクティブプロトコルのマイグレーションテスト） — この項目を選択すると、PPP が LCP パケットを送信してデータリンクの設定およびテストを可能にします。

RSTP の有効化

1. 高速スパニングツリーページを開きます。
2. **Point-to-Point Admin（ポイントツーポイントの管理）**、**Point-to-Point Oper（ポイントツーポイントの動作）**、および **Activate Protocol Migration（アクティブプロトコルのマイグレーション）**フィールドを定義します。
3. **Apply Changes（変更の適用）** をクリックします。

高速 STP が有効になり、デバイスがアップデートされます。

CLI コマンドを使用した高速 STP パラメーターの定義

次の表は高速スパニングツリーページ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 CLI コマンドをまとめたものです。

表 7-63. 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**}	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 g5


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

VLAN の設定

VLAN は、ハードウェアソリューションの定義ではなく、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）からなる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、接続している物理的な LAN セグメントに関係なく 1 つのドメインに結集します。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。VLAN はソフトウェアを通じて管理されるので、ネットワークの変更にかかる時間を節約できます。

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、デバイス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。

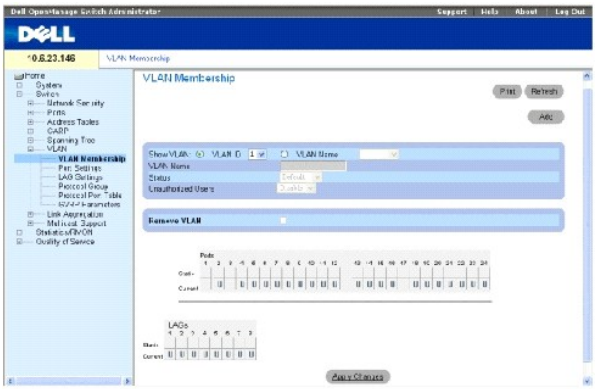
VLAN は、レイヤ 2 で機能します。トラフィックは VLAN 内で孤立化するため、VLAN 間のトラフィックフローを可能にするためには、レイヤ 3 のルーター機能が必要です。レイヤ 3 ルーターは、セグメントを識別し、VLAN と連係します。VLAN は、ブロードキャストおよびマルチキャストドメインです。ブロードキャストおよびマルチキャストトラフィックは、そのトラフィックが生成された VLAN 内のみで送信されます。

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 タギングでは、パケットヘッダーにタグを付けて、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パケットに添付されます。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。VLAN と GVRP を組み合わせることで、VLAN 情報を自動的に伝搬することが可能です。**VLAN** ページを開くには、ツリービューで **Switch(スイッチ)** → **VLAN** をクリックします。

VLAN メンバーの定義

VLAN メンバーシップページには、VLAN グループを定義するためのフィールドがあります。デバイスでは、4094 個の VLAN ID から 256 個の VLAN へのマッピングをサポートしています。すべてのポートに、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 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 メンバーシップページを開くには、ツリービューで **Switch(スイッチ)** → **VLAN** → **VLAN Membership（VLAN メンバーシップ）**をクリックします。

図 7-102. VLAN メンバーシップページ



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（VLAN 名） — ユーザー定義の VLAN 名です。

Status（ステータス） — VLAN のタイプです。可能な値は以下のとおりです。

Dynamic（動的） — GVRP を通じて動的に作成された VLAN です。

Static（静的） — ユーザー定義の VLAN です。

Default（デフォルト） — この VLAN はデフォルトの VLAN です。

Unauthorized Users（無許可のユーザー） — 無許可のユーザーによる VLAN へのアクセスを有効または無効にします。

Remove VLAN（VLAN の削除） — この項目を選択すると、VLAN メンバーシップ表から VLAN が削除されます。

VLAN の新規追加

1. VLAN メンバーシップページを開きます。
2. **Add（追加）** をクリックします。

   VLAN の新規作成 ページが開きます。
3. VLAN の ID と名前を入力します。
4. **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

1. VLAN メンバーシップページを開きます。
2. **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。

3. 必要に応じてフィールドを変更します。
4. **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 メンバーシップグループの削除

1. VLAN メンバーシップページを開きます。
2. **Show VLAN（VLAN の表示）** フィールドで VLAN を選択します。
3. **VLAN の削除（VLAN の削除）** チェックボックスを選択します。
4. **Apply Changes（変更の適用）** をクリックします。

選択した VLAN が削除され、デバイスがアップデートされます。

CLI コマンドを使用した VLAN メンバーシップグループの定義

次の表は VLAN メンバーシップページに表示されているように、VLAN メンバーシップを定義するための CLI コマンドをまとめたものです。

表 7-64. 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	インタフェース設定（VLAN）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)# exit

console(config)# interface vlan 1972

console(config-if)# name Marketing

console(config-if)# exit

console(config)#
```

VLAN ポートメンバーシップ表

VLAN ポートメンバーシップ表には、VLAN にポートを割り当てるためのポート表が定義されています。VLAN メンバーシップにポートを割り当てるには、ポートのコントロール設定を通じて切り替えます。ポートには、次の値を設定できます。

表 7-65. VLAN ポートメンバーシップ表

ポートのコントロール	定義
T	当該のインタフェースは VLAN のメンバーです。このインタフェースに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。
オフ	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。

メモ: LAG メンバーであるポートは、VLAN ポートメンバーシップ表に表示されません。

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

1. VLAN メンバーシップページを開きます。
2. **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。
3. **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。
4. **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

1. VLAN メンバーシップページを開きます。
2. **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。
3. **Remove VLAN（VLAN の削除）** チェックボックスを選択します。
4. **Apply Changes（変更の適用）** をクリックします。

選択した VLAN が削除され、デバイスがアップデートされます。

CLI コマンドを使用した VLAN グループへのポートの割り当て

次の表は VLAN グループにポートを割り当てる場合の等価 CLI コマンドをまとめたものです。

表 7-66. 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]	VLAN を一般用ポートに追加するか、一般用ポートから削除します。

switchport general pvid vlan-id	インタフェースが一般用モードである場合に、PVID を設定します。

CLI コマンドの例は次のようになります。

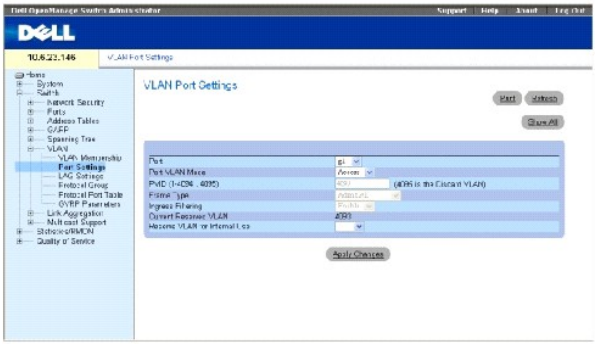
```
Console (config)# vlan database

Console (config-vlan)# vlan 23-25

Console (config-vlan)# exit

Console(config)# interface vlan 23

Console (config-if)# name Marketing

Console(config-if)# exit

Console (config)# interface ethernet g8

Console (config-if)# switchport mode access

Console (config-if)# switchport access vlan 23



Console(config-if)# exit

Console (config)# interface ethernet g9

Console (config-if)# switchport mode trunk

Console (config-if)# swithport mode trunk allowed vlan add 23-25



Console(config-if)# exit

Console (config)# interface ethernet g10

Console (config-if)# switchport mode general

Console (config-if)# switchport general allowed vlan add 23,25 tagged

Console (config-if)# switchport general pvid 25
```

VLAN ポートの設定の定義

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 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 ポートの設定ページを開くには、ツリービューで **Switch(スイッチ)** → **VLAN** → **Port Settings（ポートの設定）** をクリックします。

図 7-103. VLAN ポートの設定



Port（ポート） — VLAN に属するポートの番号です。

Port VLAN Mode（ポートの VLAN モード） — ポートのモードです。可能な値は以下のとおりです。

General（一般用） — 当該のポートは VLAN に属します。また、各 VLAN は、ユーザーによりタグ付きまたはタグなし（フル 802.1Q モード）として定義されます。

Access（アクセス） — 当該のポートは、単一のタグなし VLAN に属します。ポートがアクセスモードに入ると、ポートで許可するパケットタイプを指定できません。アクセスポートでは、入口フィルタリングの有効と無効を指定できません。

Trunk（トランク） — 当該のポートはすべてのポートにタグが付く VLAN に属します（タグなしが可能なポートを除きます）。

PVID — タグなしのパケットに VLAN ID を割り当てます。可能な値は、1 ～ 4094 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） — 当該のポートに対して入口フィルタリングを有効または無効にします。入口フィルタリングによって、特定の LAG がメンバーになっていない VLAN を宛先とするパケットを破棄できます。

Current Reserve VLAN（現在の予約 VLAN） — 予約 VLAN として現在システムで指定されている 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

1. VLAN ポートの設定ページを開きます。
2. **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。
3. ページ上の残りのフィールドを完了します。
4. **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 ポート表を表示する

1. VLAN ポートの設定ページを開きます。
2. **Show All（すべて表示）** をクリックします。

VLAN ポート表 が開きます。

CLI コマンドを使用した VLAN グループへのポートの割り当て

次の表は VLAN グループにポートを割り当てる場合の等価 CLI コマンドをまとめたものです。

表 7-67. VLAN ポートに関連する CLI コマンド

CLI コマンド	説明
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 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 pvid *vlan-id*	インタフェースが一般用モードである場合に、ポート VLAN ID（PVID）を設定します。
switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]	VLAN を一般用ポートに追加するか、一般用ポートから削除します。
switchport general acceptable-frame-types tagged-only	タグなしのパケットを入口で破棄します。
switchport general ingress-filtering disable	ポートの入口フィルタリングを無効にします。
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* }	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。

CLI コマンドの例は次のようになります。

```
Console (config)# interface range ethernet g18-20

Console (config-if)# switchport mode access

Console (config-if)# switchport general pvid 234

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

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

VLAN LAG の設定の定義

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 の設定ページを開くには、ツリービューで **Switch(スイッチ)** → **VLAN** → **LAG Settings（LAG の設定）** をクリックします。

図 7-104. VLAN LAG の設定

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。可能な値は以下のとおりです。

General（一般用） — 当該の LAG は VLAN に属します。また、各 VLAN は、ユーザーによりタグ付きまたはタグなし（フル 802.1Q モード）として定義されています。

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（オプションで選択する単一のネイティブ VLAN を除きます）。

PVID — タグなしのパケットに VLAN ID を割り当てます。可能なフィールド値は、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できます。

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 の設定の割り当てには次の手順を実行します。

1. VLAN LAG の設定ページを開きます。
2. **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。
3. **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

1. VLAN LAG の設定ページを開きます。
2. **Show All（すべて表示）** をクリックします。

VLAN LAG 表 が開きます。

CLI コマンドを使用した VLAN グループへの LAG の割り当て

次の表は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 を割り当てる場合と等価 CLI コマンドをまとめたものです。

表 7-68. 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}	ポートの VLAN メンバーシップモードを設定します。
switchport trunk native vlan *vlan-id*	ポートを指定の VLAN のメンバーとして定義し、VLAN ID をポートのデフォルト VLAN ID（PVID）とします。
switchport general pvid *vlan-id*	インタフェースが一般用モードである場合に、ポート VLAN ID（PVID）を設定します。
switchport general allowed vlan add *vlan-list* [**tagged** | **untagged**]	VLAN を一般用ポートに追加するか、一般用ポートから削除します。
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 general ingress-filtering disable	ポート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。

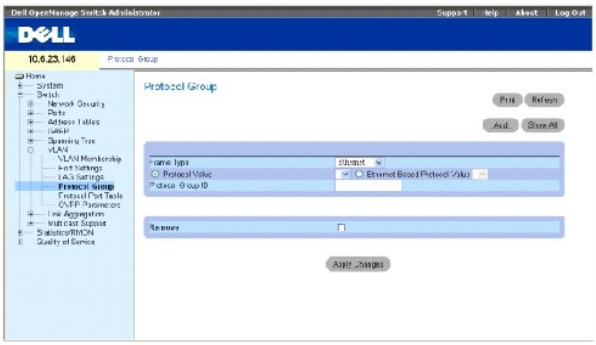
```
console(config)# interface port-channel 1

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


console(config-if)# exit
```

VLAN プロトコルグループの定義

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。プロトコルグループページを開くには、ツリービューで **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 7-105. プロトコルグループ



Frame Type（フレームタイプ） — パケットのタイプです。可能なフィールド値は、**Ethernet**、**RFC1042**、および **LLC 他** です。

Protocol Value（プロトコル値） — ユーザー定義のプロトコル名です。

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。可能なフィールド値は、IP、IPX、および **IPV6** です。

Protocol Group ID（プロトコルグループ ID） — VLAN グループ ID 番号です。

Remove（削除） — この項目が選択されている場合、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ます。

プロトコルグループの追加

1. プロトコルグループページを開きます。
2. **Add（追加）**をクリックします。

   グループへのプロトコルの追加 ページが開きます。
3. ページ上のフィールドを完了します。
4. **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

1. プロトコルグループページを開きます。
2. ページ上のフィールドを完了します。
3. **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

1. プロトコルグループページを開きます。
2. **Show All（すべて表示）** をクリックします。

   プロトコルグループ表 が開きます。
3. 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。
4. **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 7-69. 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。

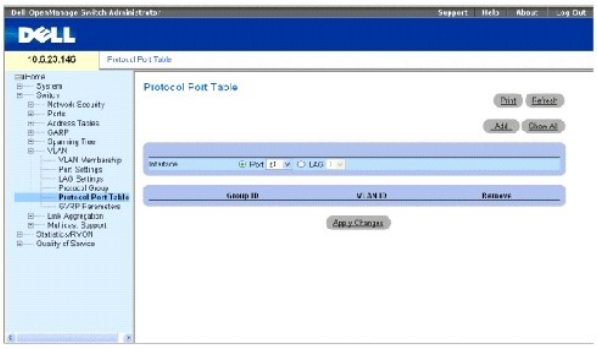
次の例は、ip-arp プロトコルをグループ "213" にマッピングする場合を示しています。

```
Console (config)# vlan
database

Console (config-vlan)#
map protocol ip-arp
protocols-group 213
```

プロトコルポートの追加

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。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）** をクリックします。

図 7-106. 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） — 当該の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 (1 ～ 4095) — 当該のインタフェースをユーザー定義の VLAN ID に割り当てます。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。

メモ: VLAN 4095 は、破棄 VLAN です。

プロトコルポートの新規追加

メモ: プロトコルポートは、**VLAN ポートの設定** ページで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。

1. プロトコルポートページを開きます。
2. **Add（追加）** をクリックします。

   プロトコルポートの追加 ページが開きます。
3. ダイアログ内のフィールドを完了します。
4. **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。

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 7-70. 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 の設定

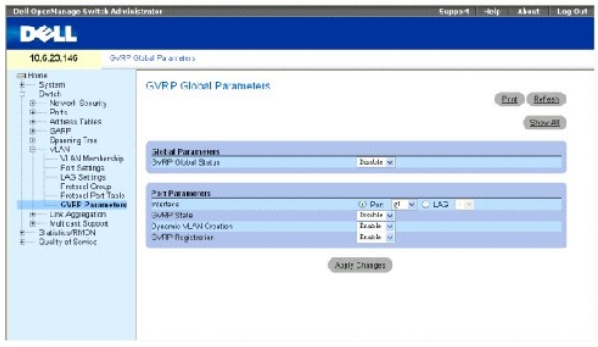
GARP VLAN Registration Protocol（GVRP）は、特に、VLAN 認識ブリッジに VLAN メンバーシップ情報を自動配布することを目的としています。GVRP は、VLAN 認識ブリッジが、VLAN とブリッジポートのマッピングを自動的に学習することを可能にするプロトコルで、各ブリッジを個別に設定して VLAN メンバーシップを登録する手間を省きます。

GVRP 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 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 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)** → **VLAN** → **GVRP Parameters（GVRP パラメーター）** をクリックします。

図 7-107. GVRP パラメーター



GVRP Global Status（GVRP グローバルステータス） — デバイスに対して GVRP を有効または無効にします。デフォルトでは、GVRP は無効になります。

Interface（インタフェース） — GVRP が有効なポートまたは LAG です。

GVRP State（GVRP 状態） — インタフェースに対して GVRP を有効または無効にします。

Dynamic VLAN Creation（動的 VLAN の作成） — GVRP による VLAN の作成を有効または無効にします。

GVRP Registration（GVRP の登録） — GVRP の登録ステータスです。

デバイスに対する GVRP の有効化

1. GVRP グローバルパラメーターページを開きます。
2. **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。
3. **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

1. GVRP グローバルパラメーターページを開きます。
2. 目的のインタフェースに対する **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。
3. **GVRP Registration（GVRP 登録）** フィールドで **Enable（有効）**を選択します。
4. **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。

CLI コマンドを使用した GVRP の設定

次の表は GVRP グローバルパラメータ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 7-71. 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 エラーの統計を表示します。
show gvrp statistics [**ethernet** *interface*| **port-channel** *port-channel-number*]	GVRP の統計を表示します。
clear gvrp statistics [**ethernet** *interface*| **port-channel** *port-channel-number*]	すべての GVRP 統計情報をクリアします。

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 g1
```

```
console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration



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
---	---	---	---	---	---	---
g1	Enabled	Forbidden	Disabled	200	900	10000
g2	Disabled	Normal	Enabled	200	600	10000

ポートの集約

ポートの集約は、ポートのグループを関連付けて 1 つのリンク集約グループ（LAG）を形成することにより、ポートの使用を最適化します。ポートの集約によって、デバイス間の帯域幅が倍増し、ポートの柔軟性が高まり、リンクに冗長性が備わります。デバイスでは、システムごとに最大 8 つの LAG をサポートし、LAG ごとにデバイスあたり最大 8 つのポートをサポートしています。

各 LAG 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。LAG に割り当てるポートは、動作スピードが同じである限り、メディアタイプ（UTP/Fiber、または異なるファイバタイプ）は違っていても構いません。

集約リンクを手動または自動で割り当てるには、関連リンクで Link Aggregation Control Protocol（LACP）を有効にします。デバイスには、送信元 MAC アドレスと宛先 MAC アドレスの両方に基づいた LAG 負荷バランシング機能が備わっています。

集約リンクは、単一の論理ポートとしてシステムで処理されます。すなわち、集約リンクは、オートネゴシエイション、スピード、二重設定など、非集約ポートと同様のポート属性を持ちます。

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 ポートとポート集約リンクのネゴシエイションを行います。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 LAG に追加する際は、次のガイドラインに従ってください。

- ポートにレイヤ 3 インタフェースが定義されていないこと。
- ポートがどの VLAN にも属していないこと。
- ポートがどの LAG にも属していないこと。
- ポートがミラーリング対象のポートでないこと。
- ポートの 802.1p 優先度が LAG の 802.1p 優先度と同じであること。
- ポートに対して QoS の Trust（信頼）モードが無効になっていること。
- GVRP が無効になっていること。

メモ: ポートは、以前に設定した LAG に属していない場合にのみ、LACP ポートとして設定できます。

デバイスでは、どの集約リンクメンバーにどのフレームを転送するかを決定するために、ハッシュ機能を使用します。ハッシュ機能は、集約リンクメンバーの負荷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。

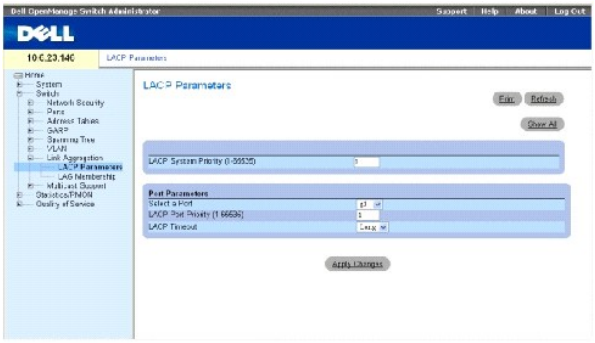
集約リンクにはそれぞれ、ギガビットイーサネットポートなどの集約リンクポートタイプがあります。ポートは、ポートタイプが同じ場合にのみ、集約リンクに追加できます。集約リンクからポートを削除すると、そのポートは元のポート設定に戻ります。**リンク集約** ページを開くには、ツリービューで **Switch(スイッチ)** → **Link Aggregation（リンク集約）**をクリックします。

LACP パラメーターの定義

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 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）**をクリックします。

図 7-108. LACP パラメーター



LACP System Priority (1-65535)（LACP システム優先度(1 ～ 65535)） — グローバル設定用の LACP 優先度値です。可能な値の範囲は 1 ～ 65535 です。デフォルト値は 1 です。

Select a Port（ポートの選択） — タイムアウト値と優先度値を割り当てるポートの番号です。

LACP Port Priority (1-65535)（LACP ポートの優先度(1 ～ 65535)） — 当該ポートの LACP 優先度値です。

LACP Timeout（LACP タイムアウト） — 管理用の LACP タイムアウトです。可能なフィールド値は以下のとおりです。

Short（ショート） — ショートタイムアウト値を指定します。

Long（ロング） — ロングタイムアウト値を指定します。

リンク集約グローバルパラメーターの定義

1. LACP パラメーターページを開きます。
2. **LACP System Priority（LACP システム優先度）**フィールドを完了します。
3. **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

1. LACP パラメーターページを開きます。
2. **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。
3. **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 を表示する

1. LACP パラメーターページを開きます。
2. **Show All（すべて表示）** をクリックします。

LACP パラメーター表 が開きます。

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 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 7-72. 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 g1

Console (config-if)# lacp port-priority 247
```

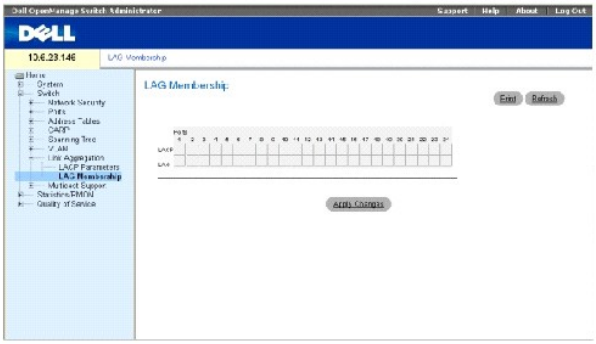
```
Console (config-if)# lacp timeout long


Console (config-if)# end


Console# show lacp ethernet g1 statistics


Port g1 LACP Statistics:


LACP PDUs sent:2


LACP PDUs received:2
```

LAG メンバーシップの定義

LAG メンバーシップ ページには、LAG にポートを割り当てるためのフィールドがあります。LAG には、8 ポートまで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には、トラップが生成され、ポートはそのデフォルト設定で動作します。

LAG メンバーシップ ページには、LAG にポートを割り当てるためのフィールドがあります。LAG メンバーシップ ページを開くには、ツリービューで **Switch(スイッチ)** → **Link Aggregation（リンク集約）** → **LAG Membership（LAG メンバーシップ）** をクリックします。

図 7-109. LAG メンバーシップ



LACP — LACP を使用して、LAG にポートを集約します。

LAG — LAG にポートを追加し、ポートが属している特定の LAG を示します。

LAG または LACP に対するポートの設定

1. LAG メンバーシップ ページを開きます。
2. 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。
3. 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。
4. **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 LAG にポートの割り当て

次の表は **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 7-73. 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
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。
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
console(config)# interface ethernet g1
console(config-if)# channel-group 1 mode on
console(config-if)# 01-Jan-2000 01:47:18 %LINK-W-Down: ch1



console(config-if)#
```

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。L2 マルチキャストサービスは、特定のマルチキャストアドレスに宛先指定された単一のパケットを受信する L2 スイッチに基づきます。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。

デバイスでは、次の機能をサポートしています。

- **L2 マルチキャストパケットの転送** — デフォルトで有効になりますが、設定はできません。

メモ: システムでは、63 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。

- **L2 マルチキャストパケットのフィルタリング** — インタフェースに対するレイヤ 2 パケットの転送を可能にします。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。

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）** をクリックします。

マルチキャストグローバルパラメーターの定義

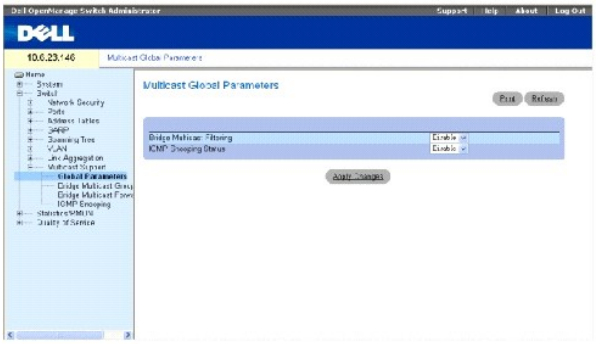
レイヤ 2 のスイッチングでは、デフォルトでマルチキャストパケットはすべての関連 VLAN ポートに転送され、パケットはマルチキャスト送信として処理されます。すべての関連ポートまたはノードがフレームのコピーを受信するという意味ではこの動作は機能的ですが、VLAN のポートのサブセットのみが必要とする無関係のフレームをポートまたはノードで受信する場合があるので、無駄な動作になる可能性があります。マルチキャスト転送フィルタを使用すると、マルチキャストフィルタデータベースに定義されたポートのサブセットにレイヤ 2 パケットを転送することができます。

IGMP スヌープをグローバルに有効にすると、スイッチング ASIC は、すべての IGMP パケットを CPU に転送するようにプログラムされます。CPU では、着信パケットを分析し、どのポートがどのマルチキャストグループに属するか、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、また、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を判断します。特定のマルチキャストグループへの加入を要求するポートは、そのマルチキャストグループを指定する IGMP レポートを発行します。この結果、マルチキャストフィルタリング

データベースが作成されます。

マルチキャスト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 スヌープを有効にするためのフィールドがあります。マルチキャスト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)** → **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）** をクリックします。

図 7-110. マルチキャストグローバルパラメーター



Bridge Multicast Filtering（ブリッジのマルチキャストフィルタリング） — ブリッジでのマルチキャストフィルタリングを有効または無効にします。無効がデフォルト設定になります。ブリッジのマルチキャストフィルタリングが有効になっている場合にのみ、IGMP スヌープを有効にすることができます。

IGMP Snooping Status（IGMP スヌープステータス） — デバイスに対して IGMP スヌープを有効または無効にします。無効がデフォルト設定になります。

デバイスのブリッジマルチキャストフィルタリングの有効化

1. マルチキャストグローバルパラメーターページを開きます。
2. **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。
3. **Apply Changes（変更の適用）** をクリックします。

ブリッジのマルチキャストがデバイスで有効になります。

デバイスの IGMP スヌープの有効化

1. マルチキャストグローバルパラメーターページを開きます。
2. **IGMP Snooping Status（IGMP スヌープステータス）** フィールドで **Enable（有効）** を選択します。
3. **Apply Changes（変更の適用）** をクリックします。

IGMP スヌープがデバイスで有効になります。

CLI コマンドを使用したマルチキャスト転送および IGMP スヌープの有効化

次の表は 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、マルチキャスト転送および IGMP スヌープ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 7-74. マルチキャスト転送および IGMP スヌープに関連する CLI コマンド

CLI コマンド	説明
bridge multicast filtering	マルチキャストアドレスのフィルタリングを有効にします。
ip igmp snooping	IGMP（Internet Group Membership Protocol）スヌープを有効にします。

CLI コマンドの例は次のようになります。

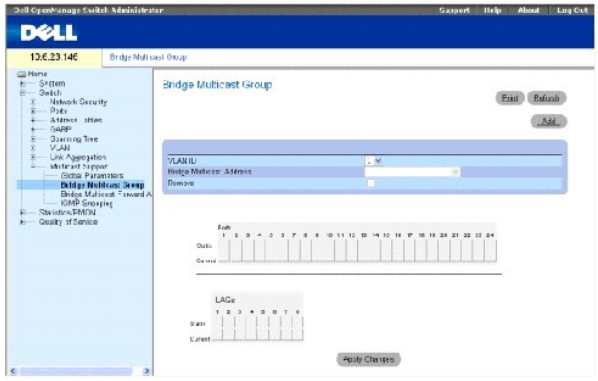
```
Console (config)# bridge
multicast filtering

Console (config)# ip igmp
snooping
```

ブリッジマルチキャストアドレスメンバーの追加

ブリッジマルチキャストグループ ページの **ポート** 表および **LAG** 表には、マルチキャストサービスグループに加わっているポートおよび LAG が表示されます。ポート 表および LAG 表には、マルチキャストグループに対するポートまたは LAG の加わり方も反映されます。ポートは、既存のグループまたは新規のマルチキャストサービスグループに追加できます。ブリッジマルチキャストグループ ページでは、新規のマルチキャストサービスグループを作成することができます。また、ブリッジマルチキャストグループ ページでは、特定のマルチキャストサービスアドレスグループにポートを割り当てます。

ブリッジマルチキャストグループ ページを開くには、ツリービューで **Switch(スイッチ)** → **Multicast Support（マルチキャストサポート）** → **Bridge Multicast Address（ブリッジマルチキャストアドレス）** をクリックします。

図 7-111. ブリッジマルチキャストグループ



VLAN ID — VLAN を識別し、マルチキャストグループアドレスに関する情報を示します。

Bridge Multicast Address（ブリッジマルチキャストアドレス） — マルチキャストグループの MAC アドレスまたは IP アドレスを識別します。

Remove（削除） — この項目を選択すると、ブリッジマルチキャストアドレスが削除されます。

Ports（ポート） — マルチキャストサービスに追加できるポートです。

LAG — マルチキャストサービスに追加できる LAG です。

次の表は、IGMP ポートおよび LAG メンバー管理の設定を示したものです。

表 7-75. IGMP ポート / LAG メンバー表のコントロール設定

ポートのコントロール	定義
D	現在列でポートまたは LAG が、マルチキャストグループに動的に加わっています。

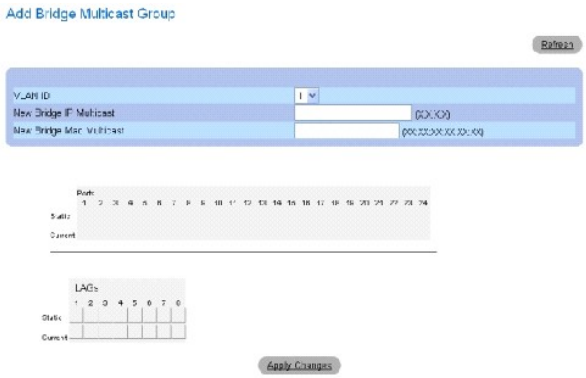
S	静的列でポートが、マルチキャストグループに静的メンバーとして加わります。 現在列でポートまたは LAG が、マルチキャストグループに静的に加わっています。
F	禁止されています。
オフ	ポートは、マルチキャストグループに加わっていません。

ブリッジマルチキャストアドレスの追加

1. ブリッジマルチキャストグループ ページを開きます。
2. **Add（追加）** をクリックします。

ブリッジマルチキャストグループの追加ページが開きます。

図 7-112. ブリッジマルチキャストグループの追加



3. **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。
4. 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。
5. 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。
6. **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

1. ブリッジマルチキャストグループ ページを開きます。
2. **VLAN ID** フィールドと **New 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。
3. 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。
4. 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。
5. **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

1. ブリッジマルチキャストグループ ページを開きます。
2. **VLAN ID** フィールドと **New 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。
3. 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。
4. 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。

5. **Apply Changes（変更の適用）** をクリックします。

LAG がマルチキャストグループに割り当てられ、デバイスがアップデートされます。

CLI コマンドを使用したマルチキャストサービスメンバーの管理

次の表は**ブリッジマルチキャストグループ** ページに表示されているように、マルチキャストサービスメンバーを管理にする場合の等価 CLI コマンドをまとめたものです。

表 7-76. マルチキャストサービスメンバーに関連する CLI コマンド

CLI コマンド	説明
bridge multicast address {*mac-multicast-address* | *ip-multicast-address*}	MAC 層のマルチキャストアドレスをブリッジ表に登録し、静的ポートをグループに追加します。
bridge multicast forbidden address {*mac-multicast-address* | *ip-multicast-address*} [**add** | **remove**] {**ethernet** *interface-list* | **port-channel** *port-channel-number-list*}	特定のマルチキャストアドレスを特定のポートに追加することを禁止します。デフォルトに戻すには、このコマンドの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> enable

Console# config

console(config)#vlan database

console(config-if)#vlan 8

console(config-if)# exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

console(config)# interface vlan 8

console(config-if)# exit

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1,g2

Console(config-if)# exit
```

```
Console(config)# exit
```

```
Console # show bridge multicast address-table
```

Vlan	MAC Address	Typev	Ports
----	-----------	-----	----------
1	0100.5e02.0203	static	g1, g2
19	0100.5e02.0208	static	g1-8
19	0100.5e02.0208	dynamic	g9-11

```
Forbidden ports for multicast addresses:
```

Vlan	MAC Address	Ports	
----	-----------	----------	
1	0100.5e02.0203	g8	
19	0100.5e02.0208	g8	

```
Console # show bridge multicast address-table format ip
```

Vlan	IP Address	Type	Ports
----	-----------	-----	----------
1	224-239.130|2.2.3	static	g1, g2
19	224-239.130|2.2.8	static	g1-8
19	224-239.130|2.2.8	dynamic	g9-11

```
Forbidden ports for multicast addresses:
```

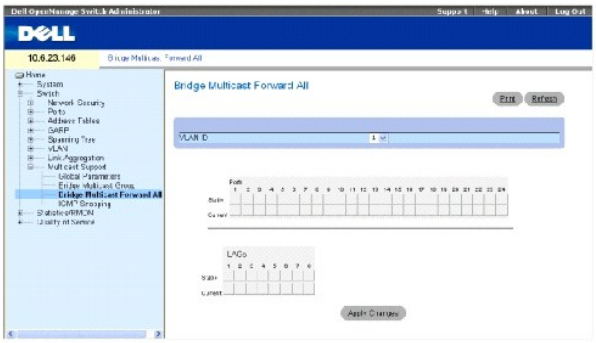
Vlan	IP Address	Ports	
----	----------	----------	
1	224-239.130|2.2.3	g8	
19	224-239.130|2.2.8	g8	

マルチキャストすべて転送パラメーターの割り当て

ブリッジマルチキャストすべて転送 ページには、近隣のマルチキャストルーターまたはスイッチに接続するデバイスに、ポートまたは LAG を割り当てるためのフィールドがあります。IGMP スヌープを有効にすると、マルチキャストパケットは適切なポートまたは VLAN に転送されます。

ブリッジマルチキャストすべて転送 ページを開くには、ツリービューで **Switch(スイッチ)** → **Multicast Support（マルチキャストサポート）** → **Bridge Multicast（ブリッジマルチキャスト）** → **Bridge Multicast Forward All（ブリッジマルチキャストすべて転送）** をクリックします。

図 7-113. ブリッジマルチキャストすべて転送



VLAN ID — VLAN を識別します。

Ports（ポート） — マルチキャストサービスに追加できるポートです。

LAG — マルチキャストサービスに追加できる LAGです。

ブリッジマルチキャストすべて転送に対応するルーターまたはポートのコントロール設定表には、ルーターおよびポートの設定を管理するための設定があります。

表 7-77. ブリッジマルチキャストすべて転送に対応するルーターまたはポートのコントロール設定表

ポートのコントロール	定義
D	当該のポートをマルチキャストルーターまたはスイッチに動的ポートとして割り当てます。
S	当該のポートをマルチキャストルーターまたはスイッチに静的ポートとして割り当てます。
F	禁止されています。
オフ	当該のポートは、マルチキャストルーターまたはスイッチに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

1. **ブリッジマルチキャストすべて転送** ページを開きます。
2. **VLAN ID** フィールドを定義します。
3. **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。
4. **Apply Changes（変更の適用）** をクリックします。

当該のポートがマルチキャストルーターまたはスイッチに割り当てられます。

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

1. **ブリッジマルチキャストすべて転送** ページを開きます。
2. **VLAN ID** フィールドを定義します。
3. **LAG** 表から LAG を選択し、その LAG に値を割り当てます。
4. **Apply Changes（変更の適用）** をクリックします。

当該の LAG がマルチキャストルーターまたはスイッチに割り当てられます。

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 **ブリッジですべてマルチキャスト転送** 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 7-78. 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。
no bridge multicast forbidden forward-all	ポートに対してマルチキャストパケットの転送を無効にします。
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)#vlan database

console(config-if)#vlan 8

console(config-vlan)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

Console(config-if)# exit
```

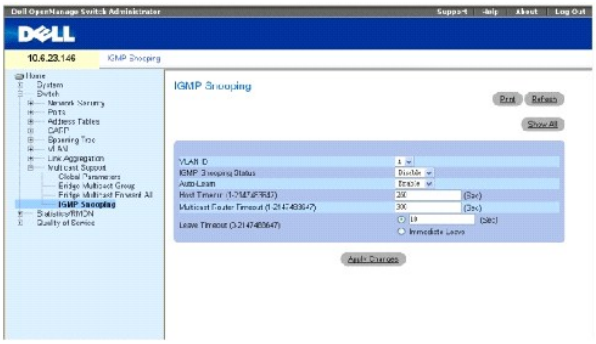
```
console(config)# interface vlan 8

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console(config-if)# exit

Console (config)# interface VLAN 1

Console (config-if)# bridge multicast forward-all add ethernet g8

Console(config-if)# end

Console # show bridge multicast filtering 1
```

```
Filtering: Enabled

VLAN:   Forward-All

Port    Static          Status
-------  -----------------  -----------
g1      Forbidden       Filter
g2      Forward         Forward(s)
g3      -               Forward(d)
```

IGMP スヌープ

IGMP スヌープ 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 スヌープ ページを開くには、ツリービューで **Switch(スイッチ)** → **Multicast Support（マルチキャストサポート）** → **IGMP Snooping（IGMP スヌープ）** をクリックします。

図 7-114. IGMP スヌープ



VLAN ID — VLAN ID を指定します。

IGMP Snooping Status（IGMP スヌープステータス） — VLAN に対して IGMP スヌープを有効または無効にします。

Auto Learn（自動学習） — デバイスに対して自動学習を有効または無効にします。

Host Timeout (1-2147483647)（ホストのタイムアウト（1 ～ 2147483647）） — IGMP スヌープのエントリが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タイム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、エントリがタイムアウトになるまでの時間（秒単位）です。**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 Leave）** 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 スヌープの有効化

1. **IGMP スヌープ** ページを開きます。
2. IGMP スヌープを有効にする必要があるデバイスの VLAN ID を選択します。
3. **IGMP Snooping Status（IGMP スヌープステータス）** フィールドで **Enable（有効）** を選択します。
4. ページ上のフィールドを完了します。
5. **Apply Changes（変更の適用）** をクリックします。

IGMP スヌープがデバイスで有効になります。

IGMP スヌープ表の表示

1. **IGMP スヌープ** ページを開きます。
2. **Show All（すべて表示）** をクリックします。

IGMP スヌープ表 が開きます。

CLI コマンドを使用した IGMP スヌープの設定

次の表はデバイスに対して IGMP スヌープを設定する場合の等価 CLI コマンドをまとめたものです。

表 7-79. IGMP スヌープに関連する CLI コマンド

CLI コマンド	説明
ip igmp snooping	Internet Group Membership Protocol（IGMP）スヌープを有効にします。
ip igmp snooping mrouter learn-pim-dvmrp	特定の VLAN のコンテキストでマルチキャストルーターポートの自動学習を有効にします。
ip igmp snooping host-time-out time-out	ホストのタイムアウト（host-time-out）を設定します。
ip igmp snooping mrouter-time-out *time-out*	エムルーターのタイムアウト（mrouter-time-out）を設定します。
ip igmp snooping leave-time-out {*time-out* | *immediate-leave*}	Leave のタイムアウト（leave-time-out）を設定します。
show ip igmp snooping groups [vlan *vlan-id*] [address *ip-multicast-address*]	IGMP スヌープによって学習されたマルチキャストグループを表示します。
show ip igmp snooping interface *vlan-id*	IGMP スヌープの設定を表示します。
show ip igmp snooping mrouter [**interface** *vlan-id*]	動的に学習されたマルチキャストルーターインタフェースの情報を表示します。

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

19 224-239.130|2.2.8 Yes g9-11



Console # show ip igmp snooping interface 1

IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1

IGMP host timeout is 300 sec

IGMP Immediate leave is disabled. IGMP leave timeout is 60 sec

IGMP mrouter timeout is 200 sec

Automatic learning of multicast router ports is enabled



Console # show ip igmp snooping mrouter
```

VLAN	Ports
----	------
1	g1

目次に戻る

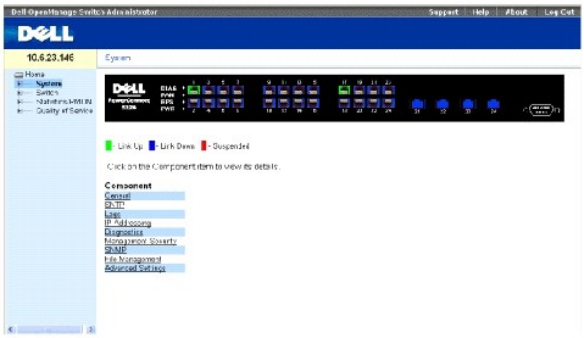
目次ページに戻る

システム設定の情報

Dell™ PowerConnect™ 5324 システムユーザーガイド

本項では、セキュリティの特徴をはじめ、デバイスソフトウェアのダウンロード、およびデバイスのリセットなど、システムパラメーターの定義に関する情報を提供します。システムページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム）をクリックします。

図 6-15. システム



一般的なデバイス情報の定義

一般 ページには、デバイスパラメーターの設定に関するページへのリンクがあります。

アセットページの表示

アセット ページには、システム名、場所、およびコンタクトを含む一般的なデバイス情報、システム MAC アドレス、システムオブジェクト ID、日、時間、およびシステムアップ時間を設定するためのパラメーターがあります。**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 6-16. アセット

System Name（システム名）**（0 ～ 160 文字）** — ユーザー定義のデバイス名を定義します。

System Contact **(0-160 Characters)**（システムコンタクト **（0 ～ 160 文字）**） — 担当者名を指定します。

System Location **(0-160 Characters)**（システムの場所 **（0 ～ 160 文字）**） — 現在システムが作動している場所を指定します。

MAC Address（MAC アドレス）— デバイスの MAC アドレスを指定します。

Sys Object 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のベンダーの認証 ID を指定します。

Service Tag（サービスタグ）— デバイスの保守をするときに使用する保守参照番号を指定します。

Asset Tag（アセットタグ）**（0 ～ 16 文字）** — ユーザー定義のデバイス参照を指定します。

Serial No.（シリアルナンバー）— デバイスのシリアルナンバーを指定します。

日付（DD/MM/YY）— 現在の日付を指定します。この形式は、月、日、年で、例えば、2002 年 11 月 10 日であれば 11/10/02 となります。

時間（HH:MM:SS）— 時間を指定します。この形式は、時、分、秒で、例えば、夜の 8 時 12 分 3 秒であれば、20:12:03 となります。

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。例えば、41 日、2 時、22 分、15 秒となります。

システム情報の定義：

1. **アセット ページ**を開きます。
2. 関連フィールドを定義します。
3. **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：

1. **アセット ページを開きます。**
2. **Telnet** をクリックします。

Telnet セッションが開始されます。

CLI コマンドを使用したデバイス情報の設定

次の表は、**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。

表 6-11. アセット CLI コマンド

CLI コマンド	説明
hostname name	デバイスのホストネームを指定または変更します。
snmp-server contact text	システムコンタクトをセットアップします。
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。
show clock [**detail**]	システムクロックからの時間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	デバイスのアセットタグを設定します。

CLI コマンドの例は次のとおりです。

```
Console (config)# hostname
dell

Console (config)# snmp-
server contact
Dell_Tech_Supp

Console (config)# snmp-
server location New_York

Console(config)# exit

Console # exit

Console (config)# asset-
tag 1qwepot

Console> clock set
13:32:00 7 Dec 2004

Console> show clock

13:32:00 (UTC+0) Dec 7
2004

No time source
```

DELL Switch# **show system**		
System Description:		Ethernet Routing Switch
System Up Time (days,hour:min:sec):		0,00:04:17
System Contact:		spk
System Name:		DELL Switch

System Location:		R&D
System MAC Address:		00:10:b5:f4:00:01
Sys Object ID:		1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324PowerConnect 5324		
Power Supply	Status	
------------	--------	
Main	OK	
Redundant	OK	
FAN	Status	
------------	--------	
1	OK	
2	OK	
DELL Switch#		

システムの時間設定の定義

時間同期 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間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。

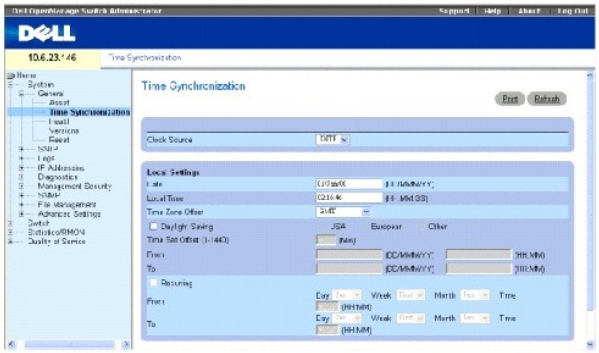
- アルバニア — 3 月の最後の週末から 10 月の最後の週末まで
- オーストラリア — 10 月の末日から 3 月の末日まで
- オーストラリア - タスマニア — 10 月の初めから 3 月の末日まで
- アルメニア — 3 月の週末から 10 月の最後の週末まで
- オーストリア — 3 月の最後の週末から 10 月の最後の週末まで
- バハマ — 米国の夏時間にともない、4 月から 10 月まで
- ベラルーシ — 3 月の最後の週末から 10 月の最後の週末まで
- ベルギー — 3 月の最後の週末から 10 月の最後の週末まで
- ブラジル — 10 月の第三週目の日曜日から 3 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 — 4 月の第一日曜日の 2:00 から 10 月の第一日曜日の 2:00 まで

SNTP の詳細に関しては、「SNTP の設定」を参照してください。

時間同期 ページを開くには、ツリー表示の **Ｓｙｓｔｅｍ（システム）** → **Ｇｅｎｅｒａｌ（一般）** → **Time Synchronization （時間同期）** をクリックします。

図 6-17. 時間同期



クロックソース

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。

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。詳細に関しては、「SNTP の設定」を参照してください。

None（なし） — システム時間が外付けのソースから設定されないことを指定します。

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、日：月：年で、例えば、04 May 2050（4 日 5 月 2050 年）です。

Local Time（ローカル時間）— システムの時間を定義します。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。例えば、パリのタイムゾーンオフセットは GMT +1 で、ニューヨークのタイムゾーンオフセットは GMT −5 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、**Daylight Savings （夏時間）** 領域を完成させ、繰返し設定の場合は、**Recurring （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以下のとおりです。

USA（米国） — デバイスを、4 月の第一日曜日の午前 2:00 に DST に切り換え、10 月の第一日曜日の午前 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。

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。

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。

Date（日付） — DST が始まる日です。可能なフィールドの範囲は 1 ～ 31 です。

Month（月） — 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。

Year（年） — 設定された DST が始まる年です。

Time（時間） — DST が始まる時間です。フィールドの形式は、時:分で、例えば、05:30 です。

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。

Date（日付） — DST が終る日です。可能なフィールドの範囲は 1 ～ 31 です。

Month（月） — 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。

Year（年） — 設定された DST が終る年です。

Time（時間） — 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。

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 が始まる時間を定義します。可能なフィールド値は以下のとおりです。

から（From）— 各年 DST が始まる時間を定義します。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以下のとおりです。

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 が終る繰返し時間を定義します。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以下のとおりです。

Day（日） — 毎年 DST が終る曜日。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。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。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。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

1. 時間同期 ページを開きます。
2. **Clock Source（クロックソース）**フィールドを定義します。
3. 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

1. 時間同期 ページを開きます。
2. **Recurring（繰り返し）** フィールドを定義します。
3. 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。

外付けの SNTP クロック設定の定義

1. 時間同期 ページを開きます。
2. フィールドを定義します。
3. Apply Changes（変更の適用）をクリックします。

外付けの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、 時間同期 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。

表 6-12. 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 timezone *オフセット - 時* [**minutes** *オフセット - 分*] [**zone** *頭文字*]	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** | {*週 日 月 hh:mm 週 日 月 hh:mm*}} [**offset** *オフセット*] [**zone** *頭文字*]	（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 *日付 月 年 hh:mm 日付 月 年 hh:mm* **[offset** *オフセット*] **[zone** *頭文字*]	特定の期間（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。

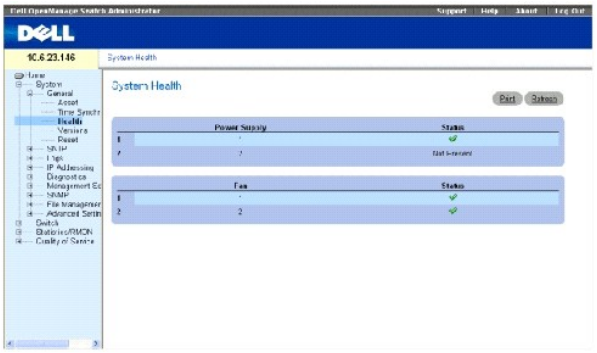
CLI コマンドの例は次のとおりです。

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



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

システムの健康情報の表示

システムの健康 ページは、物理的なデバイスのハードウェア情報を示しています。 システムの健康 ページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム）→ Ｇｅｎｅｒａｌ（一般）→ Ｈｅａｌｔｈ（健康）をクリックします。

図 6-18. システムの健康



Power Supply Status（電源ユニットの状態） — メインの電源ユニットの状態です。可能なフィールド値は以下のとおりです。

— メインの電源ユニットは特定の装置に関して正常に動作しています。

— メインの電源ユニットは特定の装置に関して正常に動作していません。

Not Present（存在しません）— 電源ユニットは特定の装置に関して存在していません。

Fan（ファン） — デバイスのファンの状態です。可能なフィールド値は以下のとおりです。

— ファンは特定の装置に関して正常に動作しています。

— ファンは特定の装置に関して正常に動作していません。

Not Present（存在しません）— ファンは特定の装置に関して存在していません。

CLI コマンドを使用したシステムの健康情報の表示

次の表は、システムの健康 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 6-13. システムの健康 CLI コマンド

CLI コマンド	説明
show system	システム情報を表示します。

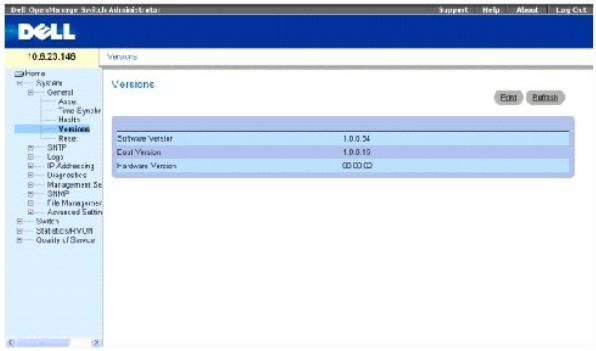
DELL Switch# **show system**	

System Description:		Ethernet Routing Switch
System Up Time (days,hour:min:sec):		0,00:04:17
System Contact:		spk
System Name		DELL Switch
System Location:		R&D
System MAC Address:		00:10:b5:f4:00:01
Sys Object ID:		1.3.6.1.4.1.674.10895.3000
Type: PowerConnect 5324PowerConnect 5324		
Power Supply	Status	
------------	--------	
Main	OK	
Redundant	OK	
FAN	Status	
------------	--------	
1	OK	
2	OK	
DELL Switch#		

バージョンページの表示

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。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 6-19. バージョン



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）— デバイスで実行している現在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、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 6-14. Versions（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。

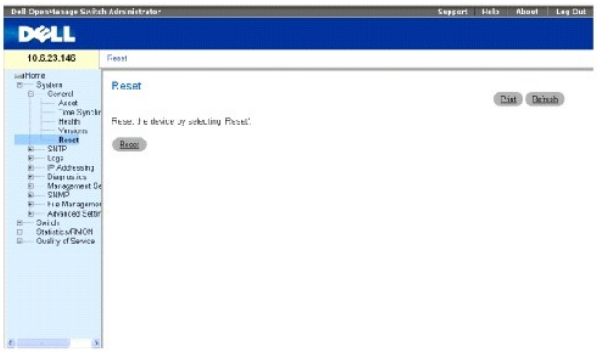
CLI コマンドの例は次のとおりです。

```
Console> show version

SW version x.xxx (date 23-Jul-xxxx time 17:34:19)

Boot version x.xxx (date 17-Jan-xxxx time 11:48:21)

HW version x.x.x
```

デバイスのリセット

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。 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 6-20. リセット



メモ: デバイスをリセットする前に、実行している設定ファイルに対する変更をすべて保存してください。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。設定ファイルの保存についての詳細に関しては、「ファイルの管理」を参照してください。

デバイスのリセット

1. リセットページを開きます。
2. Ｒｅｓｅｔ（リセット）をクリックします。

   確認のメッセージが表示されます。
3. **OK** をクリックします。

   デバイスがリセットされます。デバイスをリセットした後、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。
4. 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 6-15. リセット CLI コマンド

CLI コマンド	説明
reload	動作中のシステムをリロードします。

CLI コマンドの例は次のとおりです。

```
Console >reload


This command will reset
the whole system and
disconnect your current
session.


Do you want to continue
(y/n) n ?
```

SNTP の設定

デバイスは簡易ネットワークタイムプロトコル（SNTP）をサポートしています。SNTP は、ネットワークデバイスのミリ秒までの正確なクロックタイム同期を保証します。時間同期はネットワーク SNTP サーバーによって行います。デバイスは SNTP 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。

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
- 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。デバイスは階層 1 以上から時間を受信します。

階層の例を以下に示します。

- **階層 0** — 例えば、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を使用します。
- **階層 1** — 階層 0 タイムソースに直接リンクするサーバーを使用します。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。
- **階層 2** — タイムソースはネットワークパス上で階層 1 サーバーから隔たっています。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。

ユニキャストタイム情報のポーリング

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。スイッチタイムを同期にするための好ましい方法として T1 ～ T4 を使用し、サーバータイムを決定します。

エニキャストタイム情報のポーリング

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。最初のエニキャストサーバーが戻す応答は、タイム値を設定するために使用します。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。スイッチタイムを同期にするためには、ブロードキャストタイム情報を使用するよりもエニキャストタイム情報を使用することをお勧めします。

ブロードキャストタイム情報

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 クライアントは応答を聞きますが、SNTP クライアントは、タイム情報要求を送信することも、ブロードキャストサーバーからの応答を受信することもしません。

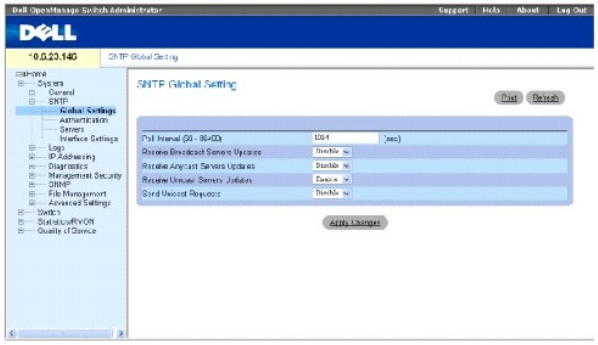
MD5（メッセージダイジェスト 5）認証は、SNTP サーバーへのスイッチ同期パスを保護します。MD5 は 128 ビットハッシュを生成するアルゴリズムです。MD5 は MD4 が変化したもので、MD4 のセキュリティを増加します。MD5 は、通信の保全性を検証し、通信の発信元の認証を行います。

ツリー表示の **Ｓｙｓｔｅｍ（システム）** → **SNTP** をクリックして、 **SNTP** ページを開きます。

SNTP グローバルパラメーターの定義

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 グローバル設定** ページを開くには、ツリー表示の **Ｓｙｓｔｅｍ（システム）** → **SNTP** → **SNTP Global Settings （SNTP グローバル設定）** をクリックします。

図 6-21. SNTP グローバル設定



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。

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） — 選択されたインタフェースについてのブロード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。

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 Servers（ユニキャストサーバーのポーリング） — 有効なとき、SNTP サーバーにユニキャスト転送情報を送信します。

CLI コマンドを使用した SNTP グローバルパラメーターの定義

次の表は、**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。

表 6-16. SNTP グローバルパラメーター CLI コマンド

CLI コマンド	説明
sntp broadcast client enable	SNTP ブロードキャストクライアントを有効にします。
sntp 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とおりです。

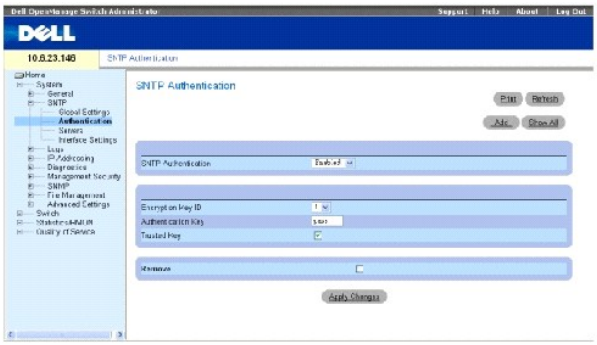
```
console> enable

console#configure
```

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

SNTP 認証方法の定義

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 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 認証** ページを開きます。

図 6-22. SNTP 認証



SNTP Authentication（SNTP 認証）— 有効なとき、デバイスと SNTP サーバー間の SNTP セッションの認証を有効にします。

Encryption Key ID（暗号化キー 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 4294967295 文字までです。

Authentication Key(**1-8** Characters)（認証キー（**1** ～ **8** 文字））— 認証に使用するためのキーを指定します。

Trusted Key（信用キー）— SNTP サーバーを認証するために使用される暗号化キーを指定します。

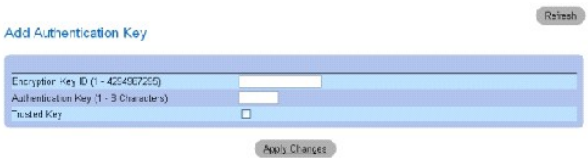
Remove（削除）— チェックがある場合、選択されたキーを削除します。

SNTP 認証キーの追加

1. **SNTP 認証** ページを開きます。
2. Add（追加）をクリックします。

   認証キーの追加ページを開きます。

図 6-23. 認証キーの追加



3. フィールドを定義します。
4. Apply Changes（変更の適用）をクリックします。

SNTP 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

1. **SNTP 認証** ページを開きます。
2. Show All（すべてを表示）をクリックします。

認証キー表 が開きます。

図 6-24. 認証キー表

認証キーの削除

1. **SNTP 認証** ページを開きます。
2. Show All（すべてを表示）をクリックします。

認証キー表 が開きます。

3. **Authentication Key Table（認証キー表）** エントリを選択します。
4. 削除チェックボックスを選択します。
5. 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 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。

表 6-17. SNTP 認証 CLI コマンド

CLI コマンド	説明
sntp authenticate	サーバーから受信したネットワークタイムプロトコルトラフィックの認証を定義します。
sntp authentication-key *番号* **md5** *可変値*	SNTP の認証キーを定義します。

CLI コマンドの例は次のとおりです。

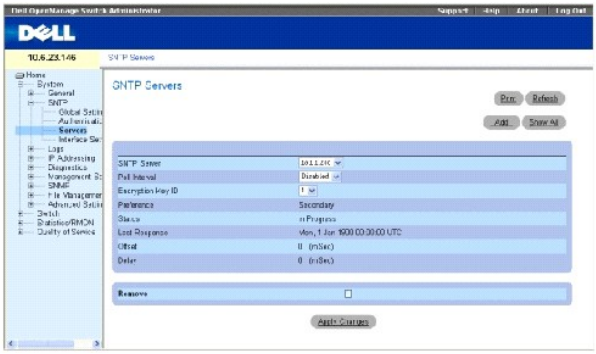
```
console> enable


console#configure


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

```
Console(config)# sntp
trusted-key 8


Console(config)# sntp
authenticate
```

SNTP サーバーの定義

SNTP サーバー ページには、SNTP サーバーを有効にするための情報、および新しい SNTP サーバーを追加するための情報があります。さらに、**SNTP サーバー** ページで、デバイスはサーバーに対して 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ことができます。**SNTP サーバー** ページを開くには、ツリー表示の **System（システム）** → **SNTP** → **SNTP Server（SNTP サーバー）** をクリックします。

図 6-25. SNTP サーバー



SNTP Server（SNTP サーバー） — ユーザー定義の SNTP サーバー IP アドレスまたはホストネームを入力します。最高 8 個までの SNTP サーバーを定義することができます。このフィールドには 1 ～ 158 文字を入力することができます。

Poll Interval（ポーリング間隔）— 有効なとき、選択された SNTP サーバーのシステムタイム情報に対してのポーリングを有効にします。

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 を指定します。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 Up（ステータスアップ） — 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以下のとおりです。

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 サーバーは現在正常に動作していません。

Unknown（不明） — SNTP サーバーステータスは現在不明です。

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（オフセット）— デバイスのローカル時間と SNTP サーバーから取得した時間との間のタイムスタンプの差です。

Delay（遅延）— SNTP サーバーに到達するまでに要した時間です。

Remove（削除） — 選択されているとき、**SNTP サーバー** リストから特定の SNTP サーバーを削除します。

SNTP サーバーの追加

1. **SNTP サーバー** ページを開きます。
2. Add（追加）をクリックします。

SNTP サーバーの追加 ページが開きます。

図 6-26. SNTP サーバーの追加

3. フィールドを定義します。
4. 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。

次の表は、 **SNTP サーバーの追加** 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。

表 6-18.

CLI コマンド	説明
sntp server ip-address|hostname poll key keyid	SNTP を使い、サーバーとして NTP トラフィックを要求したりトラフィックを受け取るようにデバイスを設定します。

SNTP サーバー CLI コマンド

CLI コマンドの例は次のとおりです。

```
console> enable


console#configure


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

SNTP サーバー表の表示

1. **SNTP サーバー** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

SNTP サーバー表 が開きます。

図 6-27. SNTP サーバー表

SNTP サーバーの変更

1. SNTP サーバー ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

   SNTP サーバー表 が開きます。
3. SNTP サーバーエントリを選択します。
4. 関連フィールドを変更します。
5. 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

1. SNTP サーバー ページを開きます。
2. Show All（すべてを表示）をクリックします。

   SNTP サーバー表 が開きます。
3. **SNTP Server （SNTP サーバー）** エントリを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. 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 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。

表 6-19. SNTP サーバー CLI コマンド

CLI コマンド	説明
sntp server *ip-address*|*hostname* **poll** *key keyid*	SNTP を使用し、サーバーとして NTP トラフィックを要求したり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とおりです。

```
console> enable
```

```
console#configure

Console(config)# sntp server 100.1.1.1 poll key 10

Console# show sntp status

Clock is synchronized, stratum 4, reference is 176.1.1.8

Reference time is AFE2525E.70597B34 (00:10:22.438 PDT Jul 5 1993)

Unicast servers:

Server          Preference      Status      Last response          Offset mSec    Delay mSec
---------       ----------      --------    ---------------        ------         ------
176.1.1.8       Primary         Up          AFE252C1.6DBDDFF2      7.33           117.79
176.1.8.179     Secondary       unknown     AFE21789.643287C9      8.98           189.19

Anycast server:

Server          Preference      Status      Last response          Offset         Delay
                                                                   mSec           mSec
-------         ----------      -------     --------------         -----          ------
VLAN 119        Secondary       Up          19:53:21.789 PDT Feb 19 2002  7.19    119.89

Broadcast:

Interface       IP address      Last response
-----------     -----------     ------------------------
176.1.1.8       Primary         AFE252C1.6DBDDFF2
176.1.8.179     Secondary       AFE21789.643287C9
```

SNTP インタフェースの定義

SNTP ブロードキャストインタフェース表 には、異なるインタフェースで SNTP を設定するためのフィールドがあります。**SNTP ブロードキャストインタフェース表** を開くには、Ｓｙｓｔｅｍ（システム）→ **SNTP** → Interfaces Settings（インタフェース設定）をクリックします。

SNTP ブロードキャストインタフェース表 には、以下のフィールドがあります。

Interface（インタフェース）— SNTP が有効化されるインタフェースリストがあります。

Receive Server Updates（サーバーアップデートの受信） — 指定のインタフェースを有効にする、または無効にします。

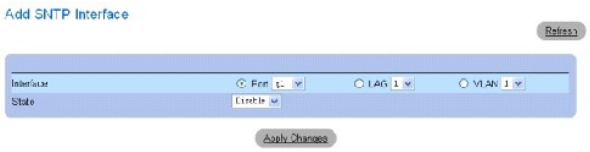
Remove（削除） — 選択されているとき、指定のインタフェースから SNTP を削除します。

SNTP インタフェースの追加

1. **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。
2. Add（追加）をクリックします。

SNTP インタフェースの追加 ページが開きます。

図 6-28. SNTP インタフェースの追加ページ



3. 関連フィールドの定義
4. **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。

表 6-20. SNTP ブロードキャスト CLI コマンド

CLI コマンド	説明
sntp client enable	インタフェースで簡易ネットワークタイムプロトコル（SNTP）クライアントを有効にします。
show sntp configuration	簡易ネットワークタイムプロトコル（SNTP）の設定を示します。

CLI コマンドの例は次のとおりです。

```
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: g1, g3		

ログの管理

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。**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。

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。

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。

SYSLOG RFC により、すべてのエラー報告に対してメッセージフォーマットが推奨されているため、イベントメッセージには固有のフォーマットがあります。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。それぞれのメッセージの重要度は、各イベントロギングにつき送信される一組のイベントロギングデバイスを決定します。

以下の表にはログ重要度レベルが記載されています。

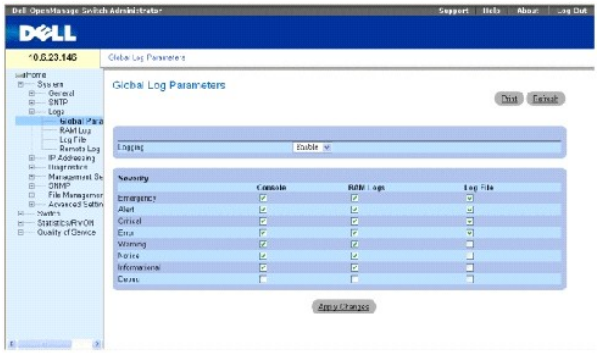
表 6-21. ログ重要度レベル

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、デルオンラインテクニカルポートへ連絡してください。

グローバルログパラメーター ページには、どのイベントがどのログに記録されたかを定義するための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パラメーターがあります。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。**グローバルログパラメーター** ページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム） → Ｌｏｇｓ（ログ） → Global Parameters （グローバルパラメーター）をクリックします。

図 6-29. グローバルログパラメーター



Logging（ロギング） — 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。

Severity（重要度） — 以下は使用可能な重要度レベルです。

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。

メモ: 重要度レベルが選択されているとき、その重要度レベルの上のすべてのレベルも自動的に選択されています。

また、**グローバルログパラメーターページ** には、独特のロギングシステムに対応するチェックボックスがあります。

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）にあるログファイルにログが送られる最低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低の重要度レベルです。

ログの有効化：

1. **グローバルログパラメーターページ** を開きます。
2. **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。
3. **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。
4. **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、**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。

表 6-22. グローバルログパラメーター CLI コマンド

CLI コマンド	説明
logging on	エラーメッセージのロギングを有効にします。
logging {ip-address | hostname} port port severity level facility facility description text	syslog サーバーにメッセージを記録します。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。

CLI コマンドの例は次のとおりです。

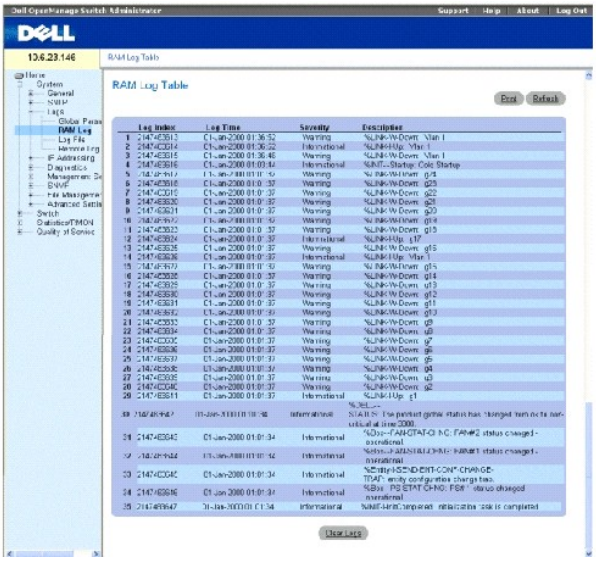
```
Console (config)# logging
on


Console (config)# logging
console errors


Console (config)# logging
buffered debugging


Console (config)# logging
file alerts


Console (config)# clear
```

```
logging


Console(config)# exit


Console# clear logging
file


Clear Logging File y/ny
```

RAM ログ表の表示

RAM ログ表 には、ログが入力された時間、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 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 6-30. RAM ログ表



Log Index（ログ索引）— RAM　ログ表 の中のログ番号です。

Log Time（ログタイム）— **RAM ログ表** に入力されたログの時間を指定します。

Severity（重要度）— ログの重要度を指定します。

Description（説明）— ユーザー定義のログの説明です。

ログ情報の削除：

1. RAM ログ表 を開きます。
2. Clear Log（ログのクリア）をクリックします。

ログ情報が **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 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。

表 6-23. RAM ログ表 CLI コマンド

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とおりです。

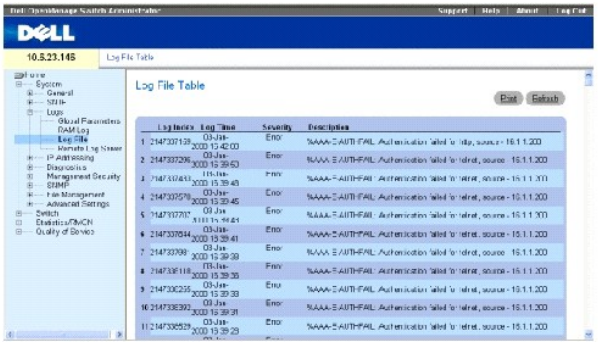
```
console# show logging

Logging is enabled.

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

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

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

1 messages were not logged

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

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

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

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

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

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

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



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



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



01-Jan-2000 01:01:36 :%
LINK-W-Down: g13



1-Jan-2000 01:01:36 :%
LINK-W-Down: g2



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




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




Console # clear logging



clear logging buffer y/n?



Console#
```

ログファイル表の表示

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。 ログファイル表を開くには、ツリー表示の Ｓｙｓｔｅｍ（システム） → Logs（ログ） → Log File （ログファイル）をクリックします。

図 6-31. ログファイル表



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

Log Time（ログタイム）— **ログファイル表** にログが入力された時間を指定します。

Severity（重要度）— ログの重要度を指定します。

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、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。

表 6-24. ログファイル表 CLI コマンド

CLI コマンド	説明
show logging file	ロギング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**	ロギングファイルからメッセージをクリアします。

CLI コマンドの例は次のとおりです。

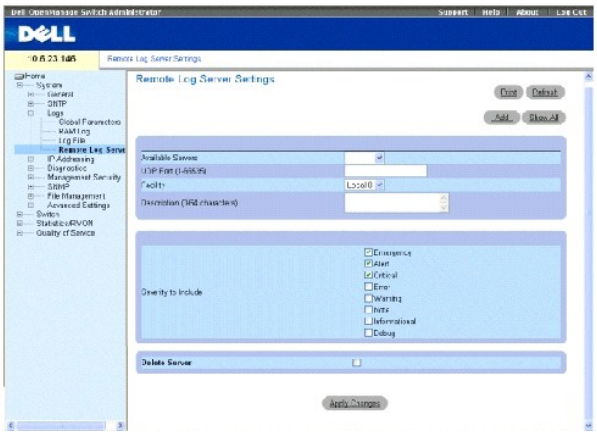
```
Console # show
logging file


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.


1 messages were not
logged


01-Jan-2000
01:12:01 :%COPY-W-
```

```
TRAP: The copy
operation was
completed
successfully



01-Jan-2000
01:11:49 :%LINK-I-Up:
g21



01-Jan-2000
01:11:49 :%2SWPHY-I-
CHNGCOMBOMEDIA: Media
changed from copper
media



to fiber media
(1000BASE-SX) on port
g21.



01-Jan-2000
01:11:48 :%2SWPHY-I-
CHNGCOMBOMEDIA: Media
changed from fiber
media to copper media
on port g21.



01-Jan-2000
01:11:48 :%LINK-W-
Down: g21



01-Jan-2000
01:11:46 :%LINK-I-Up:
g19



01-Jan-2000
01:11:42 :%LINK-W-
Down: g14



01-Jan-2000
01:11:41 :%LINK-I-Up:
g14



01-Jan-2000
01:11:36 :%LINK-W-
Down: g9



01-Jan-2000
01:11:35 :%LINK-I-Up:
g1



01-Jan-2000
01:11:34 :%LINK-W-
Down: g1



console#
```

リモートログサーバー設定ページの設定

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を定義することができ、ログの重要度が各サーバーに送られます。リモートログサーバーの設定 ページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム） → Logs（ログ） →Remote Log Server （リモートログサーバー）をクリックします。

図 6-32. リモートログサーバーの設定



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。可能なフィールド値は以下のとおりです。

Local 0 - Local 7（ローカル 0 ～ ローカル 7）

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

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。

また、リモートログサーバーの設定 ページには、重要度リストがあります。重要度の定義は、グローバルログパラメーターページの重要度の定義と同じです。

ログサーバーへの送信：

1. リモートログサーバーの設定 ページを開きます。
2. **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。
3. フィールドを定義します。
4. **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。
5. **Apply Changes（変更の適用）**をクリックします。

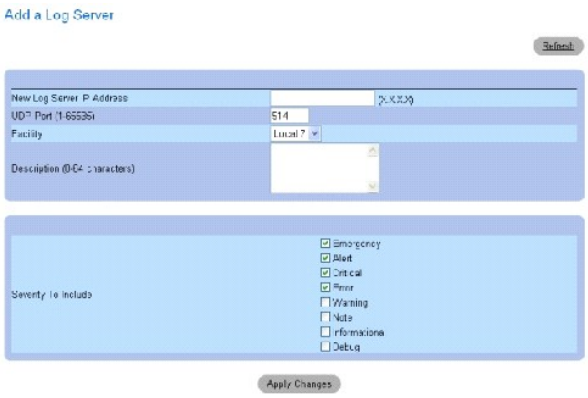
ログの設定が保存され、デバイスがアップデートされます。

新しいサーバーの定義：

1. リモートログサーバーの設定 ページを開きます。
2. **Add（追加）**をクリックします。

   ログサーバーの追加 ページが開きます。

図 6-33. ログサーバーの追加



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。

3. フィールドを定義します。
4. Apply Changes（変更の適用）をクリックします。

   サーバーが定義され、**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：

1. リモートログサーバーの設定 ページを開きます。
2. Show All（すべてを表示）をクリックします。

   リモートログサーバー表 ページが開きます。

図 6-34. リモートログサーバー表

ログサーバー表ページからのログサーバーの削除：

1. リモートログサーバーの設定 ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

   リモートログサーバー表 ページが開きます。

3. リモートログサーバー表 エントリを選択します。
4. **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。
5. **Apply Changes（変更の適用）**をクリックします。

リモートログサーバー表 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

次の表はリモートサーバーログを操作するための等価 CLI コマンドをまとめたものです。

表 6-25. リモートログサーバー CLI コマンド

CLI コマンド	説明
logging *(IP アドレス* **|** *ホスト名)* **port** *ポート* **severity** *レベル* **facility** *ファシリティ* **description** テキスト	リモートサーバーへ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とおりです。

```
console> enable


console# configure


console (config) # logging
10.1.1.1 severity critical




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: g1



03-Mar-2004 12:02:01 :%
LINK-W-Down: g2



03-Mar-2004 12:02:01 :%
LINK-I-Up: g3
```

デバイス IP アドレスの定義

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 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）をクリックしてください。

デフォルトゲートウェイの定義

デフォルトゲートウェイ ページには、ゲートウェイデバイスを割り当てるためのフィールドがあります。フレームがリモートネットワークに転送されると、パケットがデフォルト 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。**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） → Default Gateway （デフォルトゲートウェイ）をクリックします。

デフォルトゲートウェイ ページには以下のフィールドがあります。

Default Gateway （デフォルトゲートウェイ） — ゲートウェイデバイス IP アドレスです。

Remove（削除） — 選択されていると、**デフォルトゲートウェイ** ドロップダウンリストからゲートウェイデバイスを削除します。

ゲートウェイデバイスの選択：

1. **デフォルトゲートウェイ** ページを開きます。
2. **Default Gateway（デフォルトゲートウェイ）** ドロップダウンリストから IP アドレスを選択します。
3. チェックボックスの Active（アクティブ）を選択します。
4. **Apply Changes（変更の適用）** をクリックします。

   ゲートウェイデバイスが選択され、デバイスがアップデートされます。

デフォルトゲートウェイデバイスの削除：

1. **デフォルトゲートウェイ** ページを開きます。
2. **Remove（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。

3. **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ゲートウェイデバイスの定義

次の表は、**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。

表 6-26. デフォルトゲートウェイ CLI コマンド

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

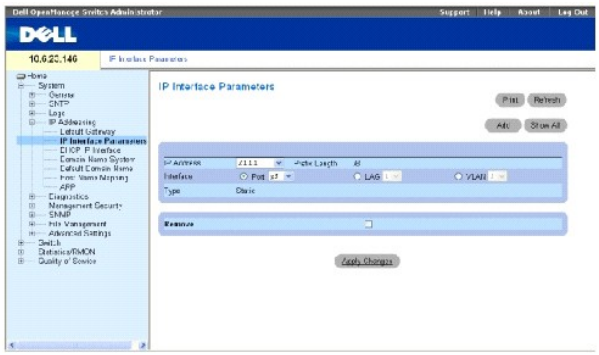
CLI コマンドの例は次のとおりです。

```
Console(config)# ip
default-gateway
196.210.10.1



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

IP インタフェースの定義

IP インタフェースパラメーターページには、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 インタフェースパラメーターページを開くには、ツリー表示の **System（システム）** → **IP Addressing（IP アドレス設定）** → **Interface Parameters（インタフェースパラメーター）** をクリックしてください。

図 6-35. IP インタフェースパラメーター



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

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

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。

詳細に関しては、「VLAN の設定」を参照してください。

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。

Forward Directed IP Broadcasts（指向された IP ブロードキャストの転送） — 指向されたブロードキャストの物理ブロードキャストへの移行を有効にします。無効にすると IP 指向ブロードキャストを撤回し、転送しません。

Broadcast Type（ブロードキャストタイプ） — インタフェースブロードキャストアドレスを定義します。

One Fill（ワンフィル） — インタフェースブロードキャストアドレスは ワンフィル（255.255.255.255）です。

Zero Fill（ゼロフィル） — インターフェースブロードキャストアドレスはゼロフィル（0.0.0.0）です。

Remove（削除） — 選択されていると、**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。

IP インタフェースの追加

1. IP インタフェースパラメーターページを開きます。
2. **Add（追加）**をクリックします。

静的インタフェースの追加 ページが開きます。

図 6-36. 静的インタフェースの追加

3. そのページにあるフィールドを完成させます。

Network Mask （ネットワークマスク） はソース IP アドレスのサブネットワークマスクを指定します。

4. **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。

IP アドレスパラメーターの変更

1. IP インタフェースパラメーターページを開きます。
2. **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。
3. 必要なフィールドを変更します。
4. **Apply Changes（変更の適用）**をクリックします。

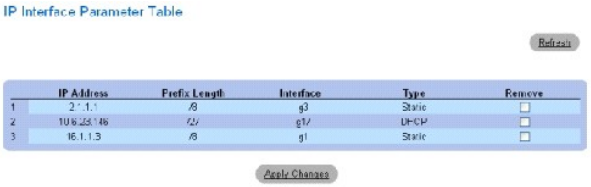
パラメーターが変更され、デバイスがアップデートされます。

IP アドレスの削除

1. IP インタフェースパラメーターページを開きます。
2. **Show All（すべてを表示）**をクリックします。

インタフェースパラメーター表 が開きます。

図 6-37. IP インタフェースパラメーター表



3. 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。
4. **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 IP インタフェースの削除

次の表は、IP 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。

表 6-27. IP インタフェースパラメーター CLI コマンド

CLI コマンド	説明
ip address ip-address {mask | prefix-length}	IP アドレスを設定します。
no ip address ip-address	IP アドレスを削除します。
show ip interface ethernet interface-number | vlan vlan-id | port-channel number	IP 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とおりです。

```
Console(config)#
interface vlan 1

Console(config-if)#
ip address
131.108.1.27
255.255.255.0

Console (config-if)#
no ip address
131.108.1.27

Console (config-if)#
exitconsole# show ip
interface vlan 1

Output

Gateway IP Address Activity
status
```

---------- ---------- --- 192.168.1.1 Active IP address Interface Type ---------- ---------- --------- 192.168.1.123 /24 VLAN 1 Static

DHCP IP インタフェースパラメーターの定義

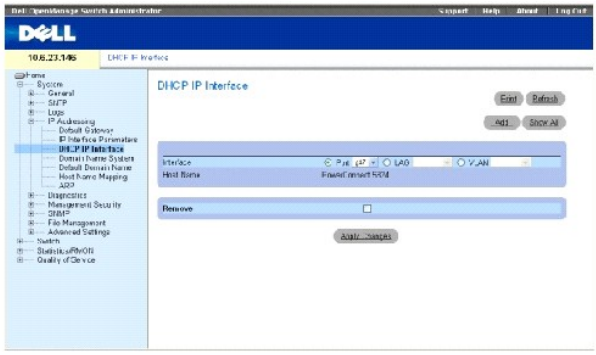
```
console# show ip interface vlan 1
```

Output

Gateway IP Address	Activity status	
----------	----------	
192.168.1.1	Active	
IP address	Interface	Type
----------	----------	----------
192.168.1.123 /24	VLAN 1	Static

DHCP IP インタフェース ページには、デバイスに接続されている DHCP クライアントを指定するためのフィールドがあります。ツリー表示の **System（システム）** → **IP Addressing（IP アドレス設定）** → **DHCP IP Interface （DHCP IP インタフェース）** をクリックします。 **DHCP IP インタフェース** ページが開きます。

図 6-38. DHCP IP インタフェース



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

Host Name （ホストネーム） — システムの名前です。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。

DHCP クライアントの追加

1. **DHCP IP インタフェース** ページを開きます。
2. **Add（追加）**をクリックします。

   DHCP IP インタフェースの追加 ページが開きます。
3. そのページにある情報を完成させます。
4. **Apply Changes（変更の適用）**をクリックします。

   DHCP インタフェースが追加され、デバイスがアップデートされます。

DHCP IP インタフェースの変更

1. **DHCP IP インタフェース** ページを開きます。
2. フィールドを変更します。
3. **Apply Changes（変更の適用）**をクリックします。

   エントリが変更され、デバイスがアップデートされます。

DHCP IP インタフェースの削除

1. **DHCP IP インタフェース** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

DHCP クライアント表 が開きます。

3. DHCP クライアントエントリを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. **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 IP 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。

表 6-28. DHCP IP インタフェース CLI コマンド

CLI コマンド	説明
ip address dhcp hostname *ホスト名*	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。

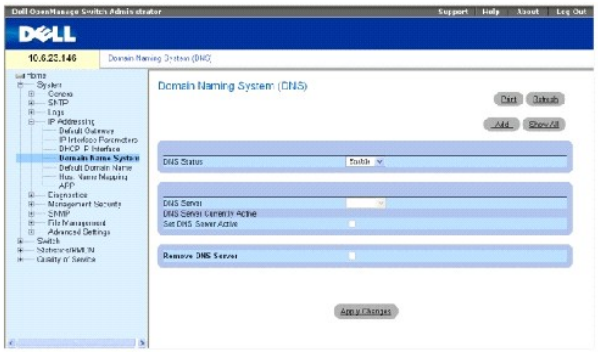
```
console> enable

console#config

console (config#)
interface ethernet g1

console (config-if)# ip
address dhcp 10.0.0.1 /8
```

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。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。

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。**ドメインネームシステム（DNS）** ページを開くには、ツリー表示の **System（システム）** → **IP Addressing（IP アドレス設定）** → **Domain Name System（ドメインネームシステム）** をクリックします。

図 6-39. ドメインネームシステム（DNS）



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 **DNS サーバーの追加** ページで追加されます。

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 サーバーとして設定されている DNS サーバーです。

Set DNS Server Active（DNS サーバーの有効化） — **DNS サーバー** フィールドで選択された DNS サーバーを有効にします。

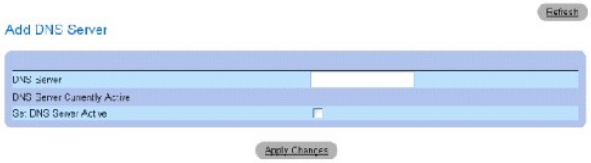
Remove DNS Server（DNS サーバーの削除） — 選択されていると、DNS サーバーを削除します。

DNS サーバーの追加

1. **ドメインネームシステム（DNS）** ページを開きます。
2. **Add（追加）** をクリックします。

   DNS サーバーの追加 ページが開きます。

図 6-40. DNS サーバーの追加



3. 関連フィールドを定義します。
4. **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

1. **ドメインネームシステム（DNS）** ページを開きます。
2. **Show All（すべてを表示）** をクリックします。

   DNS サーバー表 が開きます。

図 6-41. DNS サーバー表

DNS サーバーの削除

1. **ドメインネームシステム（DNS）** ページを開きます。
2. **Show All（すべてを表示）** をクリックします。
3. **DNS サーバー表** が開きます。
4. **DNS サーバー表** エントリを選択します。
5. **削除** チェックボックスを選択します。

6. **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。

.

表 6-29. DNS サーバー CLI コマンド

CLI コマンド	説明
ip name-server *サーバーアドレス*	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 *サーバーアドレス*	ネームサーバーを削除します。
ip domain-name *名前*	無資格のホストネームを完全にするためにソフトウェアが使用するデフォルトドメインネームを定義します。
clear host {名前 | *}	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 *名前*	デフォルトドメインネーム、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ネームおよびアドレスのリストを表示します。

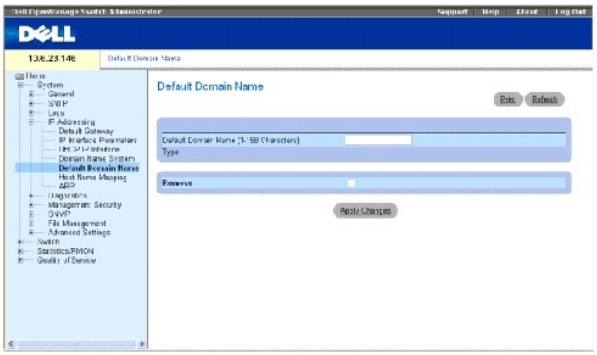
CLI コマンドの例は次のとおりです。

```
console> enable

Console#configure

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

デフォルトドメインの定義

デフォルトドメインネーム 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。**デフォルトドメインネーム** 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）** → **Default Domain Name（デフォルトドメインネーム）** をクリックします。

図 6-42. デフォルトドメインネーム



Default Domain Name（デフォルトドメインネーム）（1 ～ 158 文字） — ユーザー定義の DNS ドメインネームサーバーです。選択されていると、DNS ドメインネームがデフォルトドメインになります。

Type（タイプ） — ドメインが静的または動的に作成された場合のドメインタイプです。

Remove（削除） — 選択されていると、選択されたドメインを削除します。

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。

表 6-30. DNS ドメインネーム CLI コマンド

CLI コマンド	説明
ip domain-name name	無資格のホストネームを完全にするためにソフトウェアが使用するデフォルトドメインネームを定義します。
no ip domain-name	ドメインネームシステム（DNS）の使用を無効にします。
show hosts *名前*	デフォルトドメインネーム、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ネームおよびアドレスのリストを表示します。

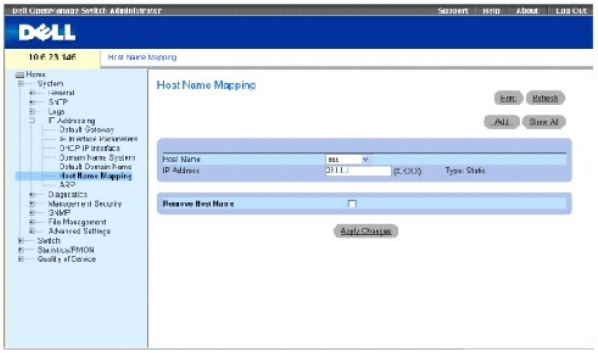
CLI コマンドの例は次のとおりです。

```
console> enable

console#configure

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

ドメインホストのマッピング

ホストネームのマッピング ページは、静的ホストネーム 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。**ホストネームのマッピング** ページは 、1 個のホストにつき IP アドレスを 8 個まで提供します。**ホストネームのマッピング** ページを開くには、 **Ｓｙｓｔｅｍ（システム）→IP Addressing（IP アドレス設定）→ Host Name Mapping（ホストネームのマッピング）をクリックします。**

図 6-43. ホストネームのマッピング



Host Name （ホストネーム） — ホストネームのリストです。ホストネームは **ホストネームのマッピングの追加** ページで定義されます。各ホストは IP アドレスを 8 個まで提供します。ホストネームフィールドのフィールド値は以下のとおりです。

IP Address（X.X.X.X） （IP アドレス（X.X.X.X）） — 指定のホストネームに割り当てられる IP アドレスを 8 個まで提供します。

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

Dynamic（動的） — IP アドレスは動的に作成されました。

Static（静的） — IP アドレスは静的な IP アドレスです。

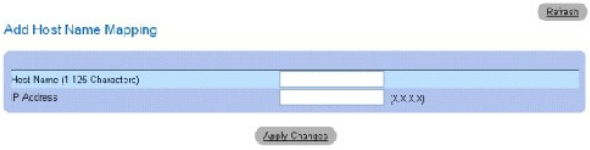
Remove Host Name Mapping（ホストネームのマッピングの削除）— チェックがあるとき、DNS ホストマッピングを削除します。

ホストドメインネームの追加

1. **ホストネームのマッピング** ページを開きます。
2. **Add（追加）**をクリックします。

ホストネームのマッピングの追加ページ が開きます。

図 6-44. ホストネームのマッピングの追加



3. 関連フィールドを定義します。
4. **Apply Changes（変更の適用）**をクリックします。

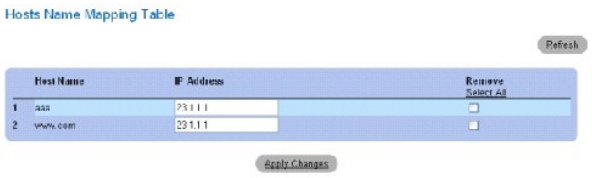
IP アドレスがホストネームにマップされ、デバイスがアップデートされます。

ホストネームのマッピング表の表示

1. **ホストネームのマッピング** ページを開きます。
2. **Show All（すべてを表示）** をクリックします。

ホストネームのマッピング表が開きます。

図 6-45. ホストネームのマッピング表



IP アドレスマッピングからのホストネームの削除

1. **ホストネームのマッピング** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。
3. **ホストマッピング表**が開きます。
4. **ホストマッピング表エントリを選択します。**
5. **Remove（削除）チェックボックスをクリックします。**
6. **Apply Changes（変更の適用）**をクリックします。

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ネームへのマッピング

次の表は、IP アドレスにドメインホストネーム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。

表 6-31. ドメインホストネーム CLI コマンド

CLI コマンド	説明
ip host name address1 address2 ... address8	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	ネームツーアドレス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ネーム、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ネームおよびアドレスのリストを表示します。

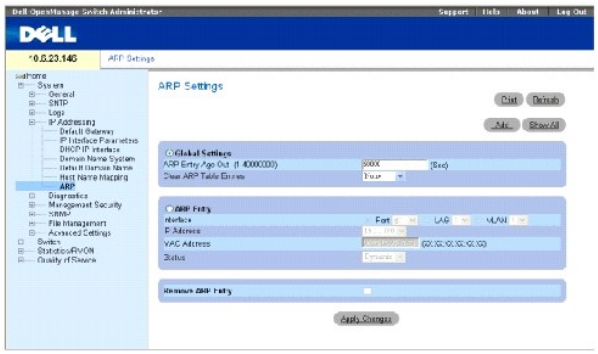
CLI コマンドの例は次のとおりです。

```
console# enable

console#configure

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

ARP の設定

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する TCP/IP プロトコルです。静的エントリは**ARP 表**で定義されます。静的エントリが定義されると、パーマネントエントリが入力され、IP アドレスを MAC アドレスに翻訳するために使用されます。**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 6-46. ARP の設定



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。この範囲は 1 ～ 4000000 で、ゼロはエントリがキャッシュから全くクリアされないことを示します。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 エントリ） — このオプションを選択し、1 つのデバイスでの ARP 設定のためのフィールドをアクティブにします。

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。

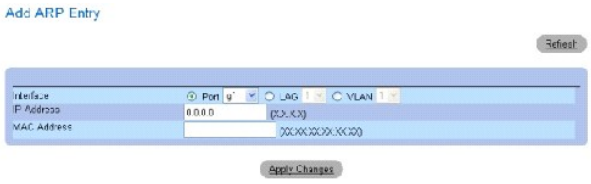
Remove ARP Entry（ARP エントリの削除） — 選択されていると、ARP エントリを削除します。

静的 ARP 表エントリの追加：

1. **ARP の設定 ページ**を開きます。
2. **Add（追加）** をクリックします。

ARP エントリの追加 ページが開きます。

図 6-47. ARP エントリの追加ページ



3. インタフェースを選択します。
4. フィールドを定義します。
5. Apply Changes（変更の適用）をクリックします。

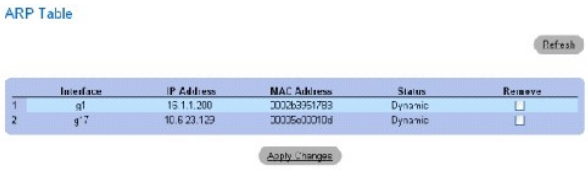
ARP 表 エントリが追加され、デバイスがアップデートされます。

ARP 表の表示

1. **ARP の設定ページ** を開きます。
2. **Show All（すべてを表示）**をクリックします。

ARP 表 が開きます。

図 6-48. ARP 表ページ



ARP 表エントリの削除

1. **ARP の設定ページ** を開きます。
2. **Show All（すべてを表示）**をクリックします。

ARP 表 ページが開きます。

3. 表エントリを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. Apply Changes（変更の適用）をクリックします。

選択された**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 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。

表 6-32. ARP の設定 CLI コマンド

CLI コマンド	説明
arp ip_addr hw_addr {ethernet interface-number | vlan vlan-id | port-channel number}	ARP キャッシュに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とおりです。

```
Console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

Console(config)# exit

Console# arp timeout 12000

Console# show arp

ARP timeout: 80000 Seconds
```

Interface	IP address	HW address	Status
---------	----------	----------	------
g1	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
g2	10.7.1.135	00:50:22:00:2A:A4	Static

ケーブル診断の実行

診断 ページには、銅ケーブル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。**診断** ページを開くには、ツリー表示の **Ｓｙｓｔｅｍ（システム）** → **Diagnostics （診断）** をクリックします。

銅ケーブル診断の表示

銅ケーブルの内蔵ケーブルテスト ページには、銅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。

銅ケーブルの内蔵ケーブルテスト 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 6-49. 銅ケーブルの内蔵ケーブルテスト

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。可能な値は以下のとおりです。

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。

Fiber Cable（ファイバーケーブル） — ファイバーケーブルがポートに接続されています。

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

1. 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。
2. **銅ケーブルの内蔵ケーブルテスト** ページを開きます。
3. **Test Now（テストの実行）** をクリックします。

銅ケーブルのテストが行われ、テストの結果が**銅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

1. **銅ケーブルの内蔵ケーブルテスト** ページを開きます。
2. **Show All（すべてを表示）** をクリックします。

仮想ケーブルテスト結果表 を開きます。

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等価 CLI コマンドをまとめたものです。

表 6-33. 銅ケーブルテスト CLI コマンド

CLI コマンド	説明
test copper-port tdr *インタフェース*	VCT テストを行います。
show copper-port tdr *インタフェース*	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 *インタフェース*	ポートに取り付けられた銅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とおりです。

```
console> enable

Console# test copper-port tdr g3

Cable is open at 100 meters.

Console> show copper-ports tdr
```

Port	Result	Length meters	Date
----	------	-------------	----
g1	OK		
g2	Short	50	13:32:00 15 January 2004

g3	Test has not been performed		
g4	Open	64	13:32:00 15 January 2004
g5	Fiber	-	-

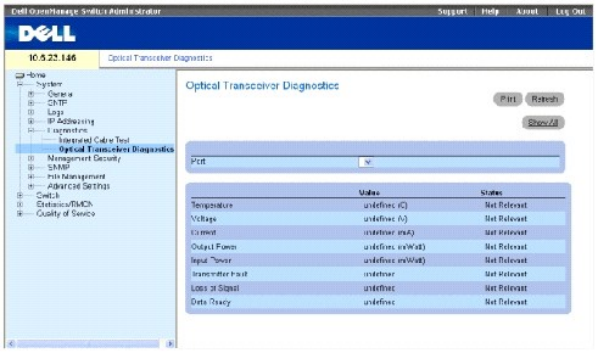
メモ: 結果として示されるケーブルの長さは、概算で 50m まで、50m ～ 80m、80m ～ 110m、110m ～ 120m、または 120m 以上の範囲です。偏差値は 20 メートルまでです。

光学送受信機診断の表示

光学送受信機診断ページには、光ファイバーケーブルのテストを行うためのフィールドがあります。 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。

メモ: 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。

図 6-50. 光学送受信機診断



Port（ポート） — ファイバーケーブルが接続されているポートです。

Temperature （温度） — ケーブルが動作している温度（セ氏）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。

光学送受信機診断テスト結果表の表示

1. 光学送受信機診断ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

テストが実行され、**仮想ケーブルテスト結果表** が開きます。

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等価 CLI コマンドをまとめたものです。

表 6-34. 光ファイバーケーブルテスト CLI コマンド

CLI コマンド	説明
show fiber-ports optical-transceiver *インタフェース* **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> enable

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

				Power			
Port	Temp (C)	Voltage (Volt)	Current (mA)	Output (mWatt)	Input (mWatt)	TX Fault	LOS
g1	W	OK	E	OK	OK	OK	OK
g2	OK	OK	OK	OK	OK	E	OK
g3	Copper						

```
Temp – Internally measured transceiver temperature.

Voltage - Internally measured supply voltage.

Current – Measured TX bias current.

Output Power – Measured TX output power.

Input Power – Measured RX received power.
```

```
Tx Fault – Transmitter fault


LOS – Loss of signal
```

光学送受信機診断表には、以下のコラムがあります。

- **Temp（温度）** — 内部的に測定された送受信機の温度です。
- **Voltage（電圧）** — 内部的に測定され電圧です。
- **Current（電流）** — 測定された TX バイアス電流です。
- **Output Power （出力電源）** — ミリワット単位で測定された TX 出力です。
- **Input Power （入力電源）** — ミリワット単位で測定された RX 受信電力です。
- **TX Fault（TX の故障）** — 送信機の故障です。

メモ: Finisair 送受信機では送信機故障診断テストをサポートしていません。

- **LOS** — 信号の損失（Loss of signal）です。
- **Data Ready（データの準備完了）** — 送受信機の電源が投入され、データの準備はできています。
- **N/A** — 利用不可、N/S - サポートなし、W - 警告、E - エラー。

メモ: 光ファイバー分析機能は、デジタル診断標準 SFF-4872 をサポートしている SFP でのみ動作します。

デバイスセキュリティの管理

管理セキュリティ ページでは、ポート、デバイス管理方法、ユーザー、およびサーバーセキュリティのセキュリティパラメーターを設定するためのフィールドを含む、セキュリティページへのアクセスを提供します。**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。

アクセスプロファイルの定義

アクセスプロファイル ページには、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ソース IP アドレス、および / またはソース IP サブネットによって定義されるユーザーグループだけに制限することができます。

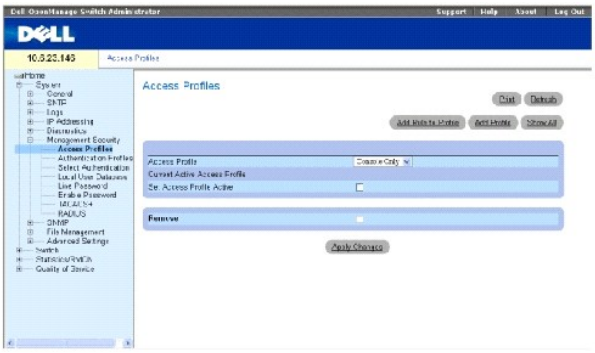
管理アクセスは、Web（HTTP）、Secure web（HTTPS）、Telnet、Secure Telnet および SNMP などの管理アクセス法のタイプごとに別個に定義することができます。

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、どのユーザーがどの方法でデバイスを管理できるかを決めるルールがあります。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。

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。**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 6-51. アクセスプロファイル



Access Profile（アクセスプロファイル） — ユーザー定義のアクセスプロファイルリストです。**アクセスプロファイル** リストには、ユーザー定義のアクセスプロファイルが追加される **コンソールリスト（Console List）** のデフォルト値があります。**アクセスプロフィアル** 名として **コンソールのみ** を選択するとセッションは切断され、デバイスにアクセスできるのはコンソールからのみとなります。

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） — 選択されていると、**アクセスプロファイル名** リストからアクセルプロファイルを削除します。

プロファイルの有効化

1. アクセスプロファイル ページを開きます。
2. **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。
3. **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。
4. **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。ルール優先度はプロファイルのルール適用の順序を設定します。

アクセスプロファイルのルールの定義：

1. **アクセスプロファイル** ページを開きます。
2. **Add an Access Profile（アクセスプロファイルの追加）** をクリックします。

アクセスプロファイルの追加 ページが開きます。

図 6-52. アクセスプロファイルの追加ページ

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。

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。ルール順序は、**プロファイルルール表** の中のルールナンバーを定義することによって設定されます。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 **プロファイルルール表** で割り当てられます。

Management Method （管理方法） — アクセスプロファイルを定義する管理方法です。このアクセスプロファイルを有するユーザーは、選択された管理方法を使用してデバイスにアクセスすることができます。

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。チェックボックスを選択し、適切なオプションボタンおよびインタフェースを選択することにより、このルールを指定されたポート、LAG、または VLAN に適用することができます。

メモ: アクセスプロファイルをインタフェースに割り当てると、他のインタフェースを介したアクセスを拒否します。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。

Source IP Address（ソース IP アドレス） — ルールが適用されるインタフェースソース 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（ネットワークマスク） — IP サブネットワークマスクです。

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

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か拒否するかを定義します。

3. **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。
4. 関連フィールドを定義します。
5. **Apply Changes（変更の適用）**をクリックします。

新しいアクセスプロファイルが追加され、デバイスがアップデートされます。

アクセスプロファイルへのルールの追加

メモ: 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。

1. **アクセスプロファイル** ページを開きます。
2. **Add Profile to Rule（プロファイルのルールへの追加）** をクリックします。

アクセスプロファイルへのルールの追加 ページが開きます。

図 6-53. アクセスプロファイルへのルールの追加

3. フィールドを完成させます。
4. **Apply Changes（変更の適用）**をクリックします。

ルールがアクセスプロファイルに追加され、デバイスがアップデートされます。

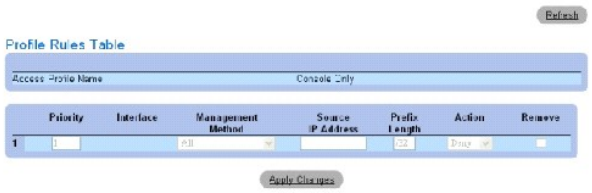
プロファイルルール表の表示：

メモ： 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、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。

1. **アクセスプロファイル** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

プロファイルルール表ページ が開きます。

図 6-54. プロファイルルール表ページ



ルールの削除

1. **アクセスプロファイル** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

プロファイルルール表 が開きます。

3. ルールを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. **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、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。

表 6-35. アクセスプロファイル CLI コマンド

CLI コマンド	説明
management access-list name	管理用のアクセスリストを定義し、設定用のアクセスリスト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 ip-address mask mask | prefix-length ethernet interface-number | vlan vlan-id | port-channel number service service	管理アクセスリストのためのポートの許可条件、および選択された管理方法を設定します。
deny ethernet interface-number | vlan vlan-id | port-channel number service service	管理アクセスリストのためのポートの拒否条件、および選択された管理方法を設定します。
deny ip-source ip-address mask mask | prefix-length ethernet interface-number | vlan vlan-id | port-channel number service service	管理アクセスリストのためのポートの拒否条件、および選択された管理方法を設定します。
management access-class {console-only | name}	どのアクセスリストがアクティブな管理接続として使用されるかを定義します。
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とおりです。

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



Console (config-macl)#
permit ethernet g1



Console (config-macl)#
permit ethernet g9



Console (config-macl)#
deny ethernet g2



Console (config-macl)#
deny ethernet g10



Console (config-macl)#
exit



Console (config)#
management access-class
mlist



Console(config)# exit



Console# show management
access-list



mlist



-----



permit ethernet g1



permit ethernet g9
```

```
! (Note: all other access
implicitly denied)



Console> show management
access-class



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

認証プロファイルの定義

認証プロファイル ページには、デバイス上で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。

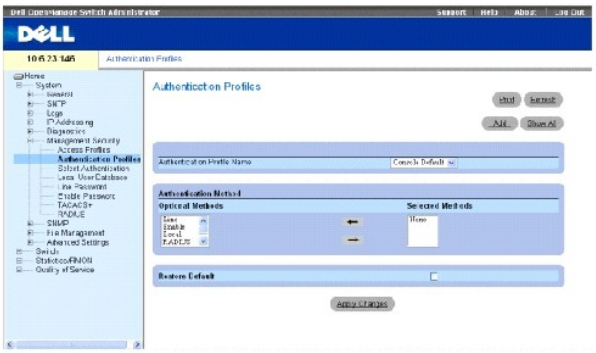
- ローカルで
- 外付けのサーバーを介して

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。

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。**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 6-55. 認証プロファイル



Authentication Profile Name（認証プロファイル名） — ユーザー定義の認証プロファイルが追加される、ユーザー定義の認証プロファイルリストです。デフォルトは **ネットワークデフォルト** および **コンソールデフォルト**です。

Optional Methods（任意の方法） — ユーザー認証方法です。可能なオプションは以下のとおりです。

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。詳細に関しては、「RADIUS グローバルパラメーター」を参照してください。

Line（ライン） — ユーザー認証にラインパスワードが使用されます。

Enable（有効） — 認証に有効パスワードが使用されます。

TACACS+ — ユーザー認証は TACACS+ サーバーで発生します。

Restore Default（デフォルトの復元） — デバイスのデフォルトユーザー認証方法を復元します。

認証プロファイルの選択：

1. **認証プロファイル** ページを開きます。
2. **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。
3. ナビゲーション矢印を使用して認証方法を選択します。
4. 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：

1. **認証プロファイル** ページを開きます。
2. Add（追加）をクリックします。

認証方法プロファイル名の追加 ページが開きます。

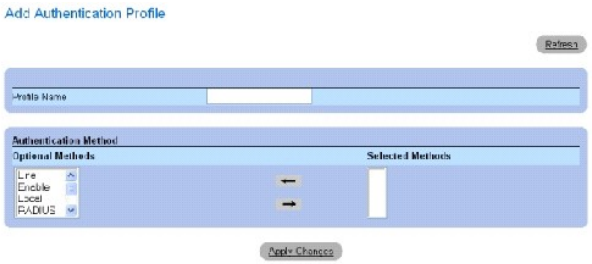


図 6-56. 認証プロファイルの追加ページ

3. プロファイルを設定します。
4. 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。

すべての認証プロファイルを表示するページの表示：

1. **認証プロファイル** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

認証プロファイル ページが開きます。

図 6-57. 認証プロファイル

認証プロファイルの削除：

1. **認証プロファイル** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

   認証プロファイル ページが開きます。
3. 認証プロファイルを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. **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、**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。

表 6-36. 認証プロファイル CLI コマンド

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

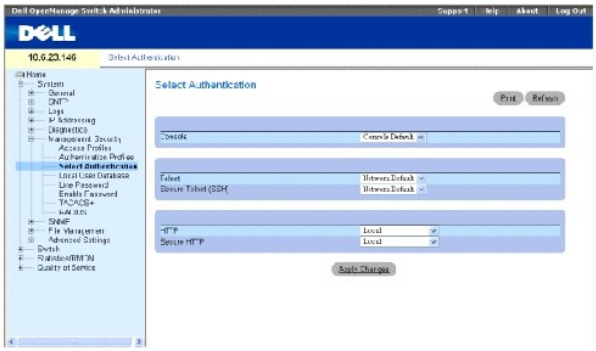
CLI コマンドの例は次のとおりです。

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



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

認証プロファイルの割り当て

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。例えば、コンソールユーザーは認証方法リスト 1 によって認証され、Telnet ユーザーは認証方法リスト 2 によって認証されます。 **認証の選択** 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） → Select Authentication （認証の選択） をクリックします。

図 6-58. 認証の選択



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。

HTTP および **Secure HTTP** — HTTP アクセスおよび Secure HTTP アクセスそれぞれのため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。

None（なし） — 認証方法はアクセスに使用されません。

Local（ローカル） — 認証はローカルで発生します。

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

1. **認証の選択** ページを開きます。
2. **コンソール** フィールドのプロファイルを選択します。
3. **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

1. **認証の選択** ページを開きます。
2. **Telnet** フィールドの認証プロファイルを選択します。
3. **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

1. **認証の選択** ページを開きます。
2. **Secure Telnet（SSH）** フィールドの認証プロファイルを選択します。
3. **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

1. **認証の選択** ページを開きます。
2. **HTTP** フィールドの認証シーケンスを選択します。
3. **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

1. **認証の選択** ページを開きます。
2. **Secure HTTP** フィールドの認証シーケンスを選択します。
3. **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、**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。

表 6-37. 認証の選択 CLI コマンド

CLI コマンド	説明
enable authentication default | list-name	リモート Telnet またはコンソールからより高いレベルの特権にアクセスするときに、認証方法リストを指定します。
login authentication default | list-name	リモート Telnet またはコンソールのための認証方法リストを指定します。
ip http authentication method1 method2.	HTTP サーバーのための認証方法を指定します。
ip https authentication method1 method2.	HTTPS サーバーのための認証方法を指定します。
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とおりです。

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


Console (config-line)
# login
authentication
default


Console (config-line)
# exit
```

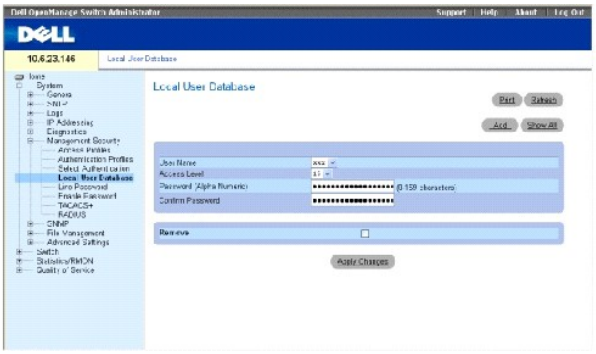
```
Console (config)# ip
http authentication
radius local


Console (config)# ip
https authentication
radius local


Console(config)# exit


Console# show
authentication
methods


Login Authentication
Method Lists


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


Default: Radius, Local,
Line


Console_Login: Line, None




Enable Authentication
Method Lists


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


Default: Radius, Enable


Console_Enable: Enable,
None







Line Login Method List
Enable Method List


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


Console Console_Login
Console_Enable


Telnet Default Default
```

```
SSH Default Default



HTTP: Radius, local


HTTPS: Radius, local


Dot1x: Radius
```

ローカルユーザーデータベースの定義

ローカルユーザーデータベース ページには、ユーザー、パスワード、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。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 6-59. ローカルユーザーデータベース



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。

パスワード（0 ～ 159 文字） — ユーザー定義のパスワードです。ローカルユーザーデータベースパスワードは最大 159 文字までです。

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。

Remove（削除） — 選択されていると、**ユーザー名** リストからユーザーを削除します。

アクセス権のユーザーへの割り当て：

1. ローカルユーザーデータベース ページを開きます。
2. **User Name（ユーザー名）** フィールドのユーザーを選択します。
3. フィールドを定義します。
4. **Apply Changes（変更の適用）**をクリックします。

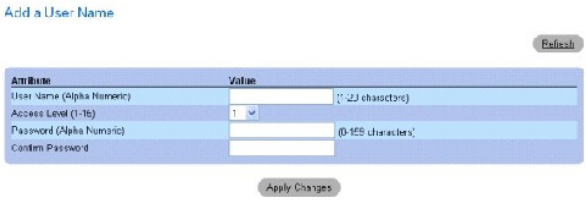
ユーザーアクセス権およびパスワードが定義され、デバイスがアップデートされます。

新しいユーザーの定義：

1. ローカルユーザーデータベース ページを開きます。
2. **Add（追加）**をクリックします。

ユーザーの追加 ページが開きます。

図 6-60. ユーザーの追加



3. フィールドを定義します。
4. **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：

1. ローカルユーザーデータベース ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

ローカルユーザー表が開きます。

図 6-61. ローカルユーザー表

ユーザーの削除：

1. ローカルユーザーデータベース ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

ローカルユーザーデータベース が開きます。

3. **ユーザー名** を選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. **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、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。

表 6-38. ローカルユーザーデータベース CLI コマンド

CLI コマンド	説明
username name password password level level encrypted	ユーザー名ベースの認証システムを確立します。

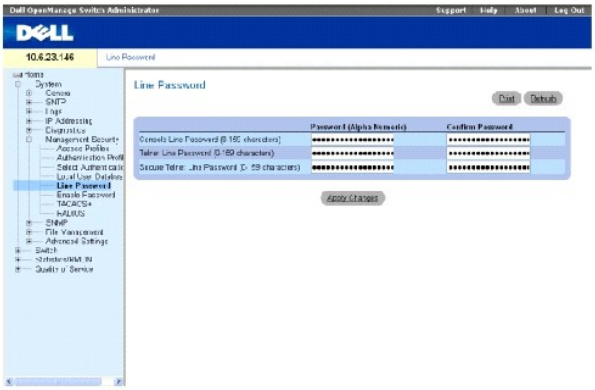
CLI コマンドの例は次のとおりです。

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

ラインパスワードの定義

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。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 6-62. ラインパスワード



Line Password for Console / Telnet / Secure Telnet (0-159 Characters)（コンソール / Telnet / Secure Telnet のためのラインパスワード（0 ～ 159 文字）） — コンソール、Telnet、または Secure Telnet セッションを介してデバイスにアクセスするためのラインパスワードです。パスワードは最大 159 文字入力することができます。

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。パスワードは ***** という形式で現われます。

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

1. ラインパスワード ページを開きます。
2. **Line Password for Console（コンソールのためのラインパスワード）** フィールドを定義します。
3. **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

1. ラインパスワード ページを開きます。

2. Telnet フィールドのためのラインパスワードを定義します。
3. 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

1. ラインパスワード ページを開きます。
2. **Line Password for Secure Telnet（Secure Telnet のためのラインパスワード）**フィールドを定義します。
3. 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、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。

表 6-39. ラインパスワード CLI コマンド

CLI コマンド	説明
password password encrypted	ラインでパスワードを指定します。

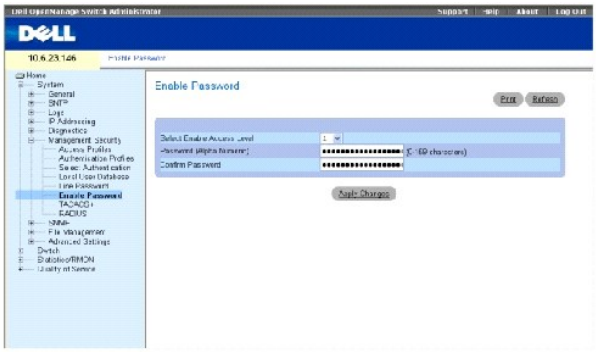
CLI コマンドの例は次のとおりです。

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

有効パスワードの定義

有効パスワードの変更 ページはアクセス制御を、通常、特権、およびグローバルの設定にするためのローカルパスワードを設定します。有効パスワードの変更 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 6-63. 有効パスワードの変更



Select Enable Access Level（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。可能なフィールド値は 1 ～ 15 です。

Password (0-159 Characters)（パスワード（0 ～ 159 文字）） — 現在設定されている有効パスワードです。有効パスワードは最大 159 文字入力することができます。

Confirm Password（パスワードの確認） — 新しい有効パスワードを確認します。パスワードは ***** 形式で現われます。

新しい有効パスワードの定義：

1. **有効パスワードの変更** ページを開きます。
2. 関連フィールドを定義します。
3. 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、**有効パスワードの変更** 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。

表 6-40. 有効パスワード変更 CLI コマンド

CLI コマンド	説明
enable password level level password encrypted	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。
show users accounts	ローカルユーザーデータベースについての情報を表示します。

CLI コマンドの例は次のとおりです。

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


Console# show users
accounts


Username Privilege


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


secret 15
```

TACACS+ 設定の定義

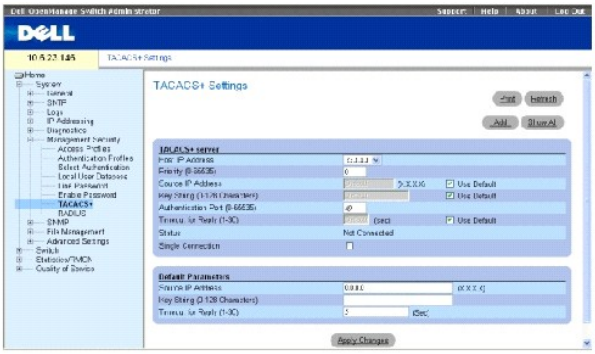
デバイスはタカックス（TACACS+：Terminal Access Controller Access Control System）クライアントサポートを提供します。TACACS+ は、デバイスにアクセスするユーザーを評価するための集中化セキュリティを提供します。

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 サーバーがユーザー特権をチェックします。

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+ の設定 ページ**を開き、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 6-64. TACACS+ の設定



Host IP Address（ホスト IP アドレス）— TACACS+ サーバー IP アドレスを指定します。

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 (0-128 Characters)（キーストリング（0 ～ 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と一致する必要があります。

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。

Reply Timeout (1-30) (Sec)（応答タイムアウト（1 ～ 30）（秒））— 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に経過する時間。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以下のとおりです。

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）— 選択されていると、デバイスと TACACS+ サーバー間に 1 個のオープン接続を維持しています。

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+ の新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。

Key String **(0-128 Characters)**（キーストリング**（0 ～ 128 文字）**）— デバイスと TACACS+ サーバー間の TACACS+ 通信のためのデフォルト認証および暗号化キーです。

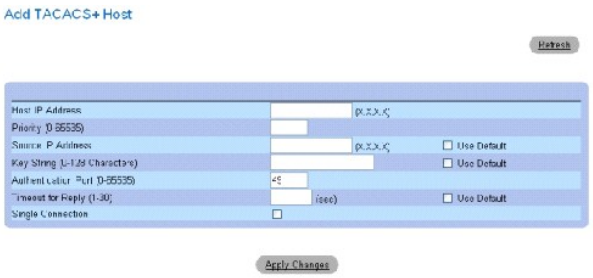
Timeout for Reply **(1-30)**（応答のタイムアウト**（1 ～ 30）**）— デバイスと TACACS+ 間の接続がタイムアウトするまでに経過する時間です。

TACACS+ サーバーの追加

1. **TACACS+ の設定ページ** を開きます。
2. Add（追加）をクリックします。

TACACS+ ホストの追加ページ が開きます。

図 6-65. TACACS+ ホストの追加



3. フィールドを定義します。
4. Apply Changes（変更の適用）をクリックします。

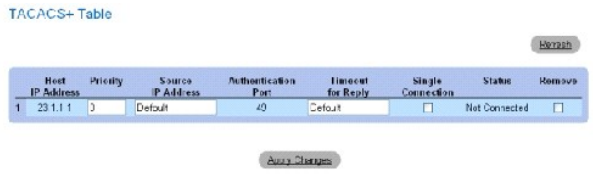
TACACS+ サーバーが追加され、デバイスがアップデートされます。

TACACS+ 表 の表示

1. **TACACS+ の設定ページ** を開きます。
2. Show All（すべてを表示）をクリックします。

TACACS+ 表 が開きます。

図 6-66. TACACS+ 表



TACACS+ サーバーの削除

1. **TACACS+ の設定ページ** を開きます。
2. Show All（すべてを表示）をクリックします。

TACACS+ 表 が開きます。

3. **TACACS+ 表** エントリを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. 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+ 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。

表 6-41. TACACS+ CLI コマンド

CLI コマンド	説明
TACACS-server host (*IP アドレス*|*ホスト名*) **single-connection port** *ポート番号* **timeout** *タイムアウト* **key** *キーストリング* **source** *ソース* **priority** *優先度*	TACACS+ ホストを指定します。
no TACACS-server host (*IP アドレス* | *ホスト名*)	TACACS+ ホストを削除します。
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指定します。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 タイムアウト	タイムアウト値を秒単位で指定します。（範囲： 1 ～ 30）
tacacs-server source-ip ソース	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 アドレス*	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とおりです。

```
Console# show tacacs

Router Configuration

----------  ---------  ----  ----------  ----------  ----------  ----------
IP address  Status     Port  Single      TimeOut     Source IP   Priority
                               Connection
----------  ---------  ----  ----------  ----------  ----------  ----------
12.1.1.2    Not        49    Yes         1           12.1.1.1    1
            Connected

Global values

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

TimeOut :
```

5						
Router Configuration ----------						
Source IP : 0.0.0.0						
console#						

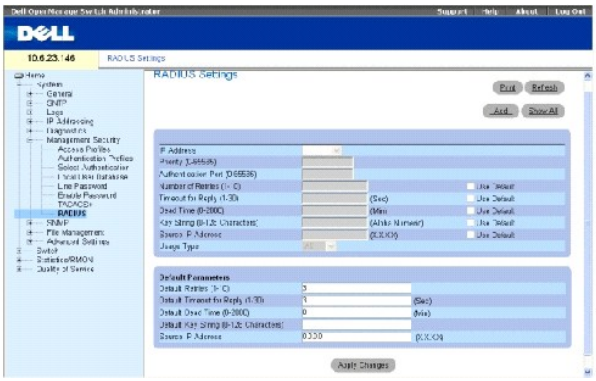
RADIUS グローバルパラメーターの設定

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。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
- ウェブアクセス
- デバイスへのコンソールアクセス

RADIUS 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） → RADIUS をクリックします。

図 6-67. RADIUS の設定



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 (1-65535)（優先度（1 ～ 65535））— サーバー優先度を指定します。可能な値は 1 ～ 65535 で、1 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（認証ポート）— 認証ポートを識別します。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)（再施行の数（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指定します。可能なフィールド値は 1 ～ 10 です、3 がデフォルト値です。

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指定します。可能なフィールド値は 1 ～ 30 で、デフォルトは 3 です。

Dead Time (0-2000)（無駄時間（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時間を（秒単位で）指定します。その範囲は 0 ～ 2000 です。

Key String (1-128 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を指定します。このキーは暗号化されます。

Source IP Address（ソース IP アドレス）— RADIUS サーバーとの通信のために使用されるソース IP アドレスを指定します。

以下のフィールドは RADIUS デフォルト値を設定します。

Default 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）指定します。

メモ: ホスト指定タイムアウト、再施行、または無駄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。

Default Retries (1-10)（デフォルトの再施行（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指定します。

Default Dead time (0-2000)（デフォルトの無駄時間（0 ～ 2000））— サービス要求に対して RADIUS サーバーがバイパスされるデフォルトの時間を（秒単位で）指定します。その範囲は 0 ～ 2000 です。

Default Key String (1-128 Characters)（デフォルトキーストリング（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デフォルトのキーストリングを指定します。このキーは暗号化されます。

Source IP Address（ソース IP アドレス）— RADIUS サーバーとの通信に使用されるソース IP アドレスを指定します。

Usage Type（使用タイプ）— サーバーの使用タイプを指定します。以下の値のうちのいずれか 1 つが可能です。ログイン、802.1x、または、すべて 指定しない場合はすべてがデフォルトになります。

RADIUS パラメーターの定義:

1. RADIUS の設定ページを開きます。
2. フィールドを定義します。
3. **Apply Changes（変更の適用）**をクリックします。

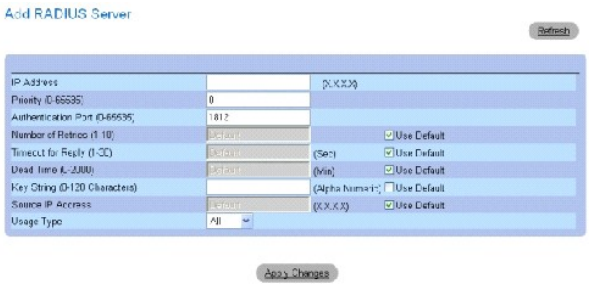
RADIUS の設定がデバイスにアップデートされます。

RADIUS サーバーの追加:

1. RADIUS の設定ページを開きます。
2. Add（追加）をクリックします。

RADIUS サーバーの追加 ページが開きます。

図 6-68. RADIUS サーバーの追加ページ



3. フィールドを定義します。
4. **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：

1. RADIUS の設定ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

すべての RADIUS サーバーの表示 ページが開きます。

図 6-69. すべての RADIUS サーバーの表示

RADIUS サーバー設定の変更：

1. RADIUS の設定ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

RADIUS サーバーリスト ページが開きます。

3. 関連フィールドを変更します。
4. Apply Changes（変更の適用）をクリックします。

RADIUS サーバーの設定が変更され、デバイスがアップデートされます。

RADIUS サーバーリストの RADIUS サーバーの削除：

1. RADIUS の設定ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

RADIUS サーバーリスト ページが開きます。

3. **RADIUS サーバーリスト** の RADIUS サーバーを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. Apply Changes（変更の適用）をクリックします。

RADIUS サーバーが **RADIUS サーバーリスト** から削除されます。

CLI コマンドを使用した RADIUS サーバーの定義

次の表は、RADIUS 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。

表 6-42. RADIUS の設定 CLI コマンド

CLI コマンド	説明
radius-server timeout timeout	デバイスがサーバーホストの応答を待つデフォルトの間隔を指定します。
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デフォルトの回数を指定します。
radius-server deadtime deadtime	使用不能なデフォルトのサーバーをスキップするように設定します。
radius-server key key-string	デバイスと RADIUS 環境間のすべての RADIUS 通信のためのデフォルトの認証および暗号化キーを設定します。
radius-server host {*IP アドレス* | *ホスト名*} **auth-port** *認証ポート番号* **timeout** *タイムアウト* **retransmit** *試行回数* **deadtime** *作業不能時間* **key** *キーストリング* **source** *ソース* **priority** *優先度* **usage** *タイプ*	RADIUS サーバーホストおよび非デフォルトの設定を指定します。
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 1645 timeout 20
```

```
Console# show radius-servers

                Port
IP address      Auth  Acct  TimeOut  Retransmit  Deadtime  Source IP  Priority  Usage
---------       ----  ----  -------  ----------  --------  ---------  --------  -----

33.1.1.1        1812  1813  6        4           10        0.0.0.0    0         All
```

172.16.1.2	1645	1646	11	8	Global	Global	2	All

Global values

TimeOut: 5

Retransmit: 5

Deadtime: 10

Source IP: 0.0.0.0

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。SNMP をサポートするデバイスはローカルソフトウェア（エージェント）を実行します。

SNMP エージェントはデバイス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りコントロールされる変数を含みます。SNMP プロトコルは MIB 仕様形式、およびネットワークを介して情報にアクセスするために使用される形式を定義します。

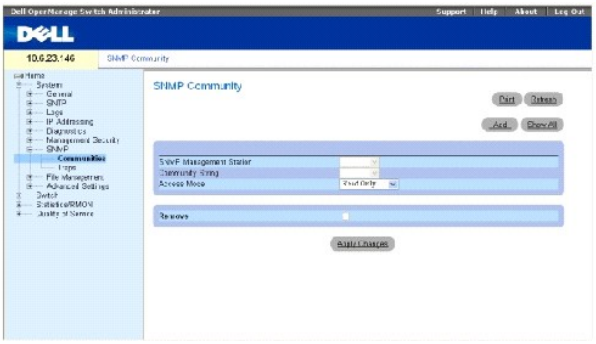
SNMP エージェントへのアクセス権はアクセスストリングによってコントロールされます。デバイスと通信を行うには、内蔵ウェブサーバーが有効なコミュニティストリングを送信して、認証を受ける必要があります。SNMP ページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム） → SNMP をクリックします。

本項には SNMP の設定を管理するための情報があります。

コミュニティの定義

コミュニティ表 の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** ページを開いてツリー表示の Ｓｙｓｔｅｍ（システム） → SNMP → Communities（コミュニティ）をクリックします。

図 6-70. SNMP コミュニティ



SNMP Management Station（SNMP 管理ステーション）— 管理ステーション IP アドレスのリストです。

Community String（コミュニティストリング）— デバイスに対して選択された管理ステーションを、認証するために使用されるパスワードとしての機能です。

Access Mode（アクセスモード）— コミュニティのアクセス権の定義可能なフィールド値は以下のとおりです。

Read Only（読み取り専用） — アクセスのないコミュニティ表を除くすべての MIB に対して、管理アクセスは読み取り専用に制限されます。

Read Write（読み書き） — アクセスのないコミュニティ表を除くすべての MIB に対して、管理アクセスは読み書きです。

SNMP Admin（SNMP 管理） — コミュニティ表を含むすべての MIB に対して、管理アクセスは読み書きです。

Remove（削除） — 選択されていると、コミュニティを削除します。

新しいコミュニティの定義

1. SNMP コミュニティ ページを開きます。
2. Add（追加）をクリックします。

   SNMP コミュニティの追加 ページが開きます。

図 6-71. SNMP コミュニティの追加

3. 次のうちのいずれか 1 つを選択します。

   Management Station（管理ステーション） — 特定の管理ステーションのための SNMP コミュニティを定義します。（値 0.0.0.0 はすべての管理ステーションを指定します。）

   All（すべて） — すべての管理ステーションのための SNMP コミュニティを定義します。
4. 残りのフィールドを定義します。
5. **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。

すべてのコミュニティの表示

1. **SNMP コミュニティ** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

コミュニティ表 が開きます。

図 6-72. コミュニティ表

コミュニティの削除

1. **SNMP コミュニティ** ページを開きます。
2. Show All（すべてを表示）をクリックします。

コミュニティ表 が開きます。

3. **コミュニティ表からコミュニティを選択します。**
4. **Remove（削除）** チェックボックスを選択します。
5. **Apply Changes（変更の適用）**をクリックします。

選択されたコミュニティエントリが削除され、デバイスがアップデートされます。

CLI コマンドを使用したコミュニティの設定

次の表は、**SNMP コミュニティ** 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。

表 6-43. SNMP コミュニティ CLI コマンド

CLI コマンド	説明
snmp-server community string ro | rw | su ip-address	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 host {ip-address | hostname} community-string 1 | **2**	選択された受け側へ送信されるトラップタイプを決定します。
show snmp	SNMP 通信状況をチェックします。

CLI コマンドの例は次のとおりです。

```
console(config)# snmp-server
community public_1 su 1.1.1.1
```

```
console(config)# snmp-server
community public_2 rw 2.2.2.2
```

```
console(config)# snmp-server
community public_3 ro 3.3.3.3
```

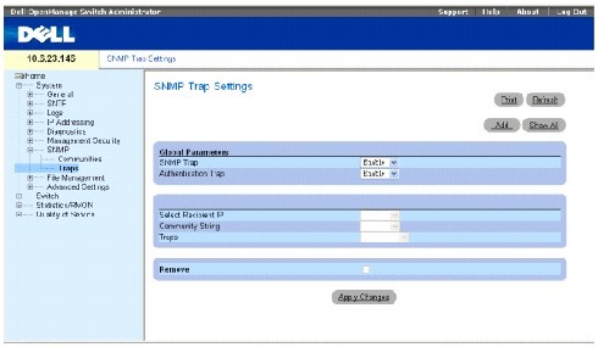
```
console(config)# snmp-server
```

```
host 1.1.1.1 public_1 1

console(config)# snmp-server
host 2.2.2.2 public_2 2

console(config)#

console#
show snmp

Community-
String      Community-
Access      IP
address
----------
----------
-------
public_1    super       1.1.1.1
public_2    readwrite   2.2.2.2
public_3    readonly    3.3.3.3

Traps are
enabled.

Authentication-failure trap is
enabled.

Trap-Rec-
Address     Trap-Rec-
Community   Version
----------
-------     ----------
---------   -------
                --
1.1.1.1     public_1    1
2.2.2.2     public_2    2

System Contact: 345
6789

System Location: 1234 5678

console#
```

トラップの定義

ユーザーは、**SNMP トラップの設定** ページから SNMP トラップまたは通知をデバイスに送信させる、または送信させないようにすることができます。 **SNMP トラップの設定** ページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム） → SNMP → Traps（トラップ）をクリックします。

図 6-73. SNMP トラップの設定



SNMP Trap（SNMP トラップ）— デバイスから定義されたトラップの受け側への SNMP トラップまたは SNMP 通知の送信を有効にします。

Authentication Trap（認証トラップ）— 認証が受け側の認証に失敗したときに、SNMP トラップの送信を有効にします。

Select Recipient IP（受け側 IP の選択）— トラップが送信される IP アドレスを指定します。

Community String（コミュニティストリング）— トラップマネージャのコミュニティストリングを識別します。

Traps（トラップ）— 選択された受け側へ送信されるトラップタイプを決定します。可能なフィールド値は以下のとおりです。

SNMP V1 — SNMP バージョン 1 トラップが送信されます

SNMP V2c — SNMP バージョン 2 トラップが送信されます

Remove（削除） — 選択されていると、**トラップマネージャ表** エントリを削除します。

デバイスでの SNMP トラップの有効化

1. **SNMP トラップの設定** ページを開きます。
2. **SNMP Trap（SNMP トラップ）**ドロップダウンリストの**Enable（有効）**を選択します。
3. フィールドを定義します。
4. Apply Changes（変更の適用）をクリックします。

SNMP トラップがデバイスで有効になります。

認証トラップのデバイスでの有効化

1. **SNMP トラップの設定** ページを開きます。
2. **Authentication Trap（認証トラップ）**ドロップダウンリストの**Enable（有効）**を選択します。
3. フィールドを定義します。
4. Apply Changes（変更の適用）をクリックします。

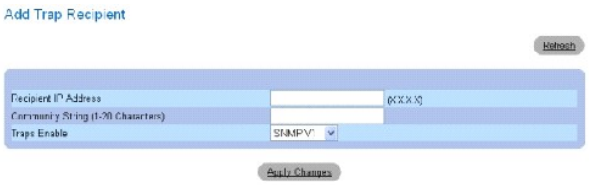
認証トラップがデバイスで有効になります。

新しいトラップ受け側の追加：

1. SNMP トラップの設定 ページを開きます。
2. **Add（追加）**をクリックします。

   トラップの受け側 / マネージャの追加 ページが開きます。

図 6-74. トラップの受け側 / マネージャの追加



3. フィールドを定義します。0.0.0.0 の設定は、「すべて」を意味し、トラップはブロードキャストされます。
4. **Apply Changes（変更の適用）**をクリックします。

   トラップの受け側 / マネージャが追加され、デバイスがアップデートされます。

トラップマネージャ表の表示

トラップマネージャ表 には、トラップのタイプを設定するフィールドがあります。

1. SNMP トラップの設定 ページを開きます。
2. Show All（すべてを表示）をクリックします。

   トラップマネージャ表 ページが開きます。

図 6-75. トラップマネージャ表

トラップマネージャ表エントリの削除

1. SNMP トラップの設定 ページを開きます。
2. Show All（すべてを表示）をクリックします。

   トラップマネージャ表 ページが開きます。

3. **トラップマネージャ表** エントリを選択します。
4. **Remove（削除）** チェックボックスを選択します。
5. **Apply Changes（変更の適用）**をクリックします。

   選択されたトラップマネージャが削除され、デバイスがアップデートされます。

CLI コマンドを使用したトラップの設定

次の表は、**SNMP トラップの設定** 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。

表 6-44. SNMP トラップの設定 CLI コマンド

CLI コマンド	説明
snmp-server enable traps	デバイスが SNMP トラップまたは SNMP 通知を送信できるようにします。
snmp-server trap authentication	認証が失敗したときにデバイスが SNMP トラップを送信できるようにします。
snmp-server host host-addr community-string **1** | **2**	選択された受け側へ送信されるトラップのタイプを決定します。
s**how snmp**	SNMP 通信状況を表示します。

CLI コマンドの例は次のとおりです。

```
console(config)# snmp-server
community public_1 su 1.1.1.1
```

```
console(config)# snmp-server
community public_2 rw 2.2.2.2
```

```
console(config)# snmp-server
community public_3 ro 3.3.3.3
```

```
console(config)# snmp-server
host 1.1.1.1 public_1 1
```

```
console(config)# snmp-server
host 2.2.2.2 public_2 2
```

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

```
console(config)# snmp-server
trap authentication
```

```
console(config)#
```

```
console# show snmp

Community-String  Community-Access  IP address
----------------  ----------------  ----------
public_1          super             1.1.1.1
public_2          readwrite         2.2.2.2
public_3          readonly          3.3.3.3
```

Traps are enabled.		
Authentication-failure trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
----------	----------	-------
1.1.1.1	public_1	1
2.2.2.2	public_2	2
System Contact: 345 6789		
System Location: 1234 5678		
console#		

ファイルの管理

ファイルの管理ページには、デバイスソフトウェア、イメージフィアル、および設定ファイルを管理するフィールドがあります。ファイルは TFTP サーバーからダウンロードすることができます。

ファイル管理の概要

設定ファイルの構造は、以下の設定ファイルから構成されます。

- スタートアップ設定ファイル — デバイスがパワーダウンまたは再起動したとき、デバイスを同じ設定に再構成することを要求するコマンドがあります。スタートアップファイルは、実行設定ファイルまたはバックアップ設定ファイルから設定コマンドをコピーすることにより作成されます。
- 実行設定ファイル — スタートアップファイルコマンド、および現在のセッション中に入力される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。セッション中に入力された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。コマンドは上書きされません。スタートアップ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。デバイスが次回再スタートするとき、コマンドはスタートアップ設定ファイルから実行設定ファイルにコピーし直されます。
- バックアップ設定ファイル — デバイス設定のバックアップコピーが含まれます。実行設定ファイルまたはスタートアップファイルがバックアップファイルにコピーされるとバックアップファイルが作成されます。ファイルにコピーされるコマンドは、バックアップファイルに保存されている既存のコマンドと交換されます。バックアップファイルの内容は実行設定ファイルまたはスタートアップ設定ファイルのいずれかにコピーされます。
- イメージファイル — システムファイルイメージは、イメージ（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保存し、その他のイメージは第 2 のコピーを保存します。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。

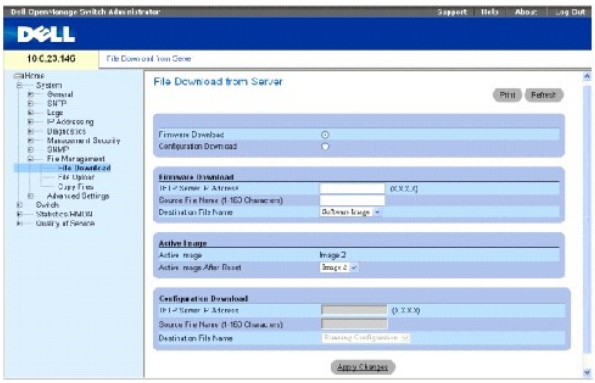
ファイルの管理ページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム） → File Management（ファイルの管理）をクリックします。ファイルの管理ページには以下のリンクがあります。

- ファイルのダウンロード
- ファイルのアップロード
- ファイルのコピー

ファイルのダウンロード

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。**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、ツリー表示の Ｓｙｓｔｅｍ（システム） → File Management（ファイルの管理） → File Download（ファイルのダウンロード）をクリックします。

表 6-76. サーバーからのファイルのダウンロード



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。**ファームウェアのダウンロード** が選択された場合、**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。**設定のダウンロード** が選択された場合、**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。

Firmware Download TFTP Server IP Address（ファームウェアのダウンロード TFTP サーバー IP アドレス） — ファイルがダウンロードされる TFTP サーバー IP アドレスです。

Firmware Download Source File Name（ファームウェアのダウンロードソースファイル名） — ダウンロードされるファイルを指定します。

Firmware Download Destination File（ファームウェアのダウンロード **宛先ファイル**） — ファイルがダウンロードされる宛先ファイルのタイプです。可能なフィールド値は以下のとおりです。

Software Image（ソフトウェアイメージ） — イメージファイルをダウンロードします。

Boot Code（ブートコード） — ブートファイルをダウンロードします。

Active Image（アクティブイメージ）— 現在アクティブなイメージファイルです。

Active Image After Reset（リセット後のアクティブイメージ）— デバイスがリセットされた後のイメージファイルです。

Configuration Download File TFTP Server IP Address（設定ダウンロードファイル TFTP サーバー 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 IP アドレスです。

Configuration Download File Source File Name（設定ダウンロードファイルソースファイル名）— ダウンロードされる設定ファイルを指定します。

Configuration Download File Destination（設定ダウンロードファイル宛先） — 設定ファイルがダウンロードされる宛先ファイルです。可能なフィールド値は以下のとおりです。

Running Configuration（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（スタートアップ設定）— — スタートアップ設定ファイルをダウンロードし、それに上書きします。

Backup Configuration（バックアップ設定） — バックアップ設定ファイルをダウンロードし、それに上書きします。

ファイルのダウンロード：

1. **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。
2. ダウンロードするファイルのタイプを定義します。
3. フィールドを定義します。
4. 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。

メモ： 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に関する詳細については、「**デバイスのリセット**」を参照してください。

CLI コマンドを使用したファイルのダウンロード

次の表は、**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。

表 6-45. ファイルのダウンロード CLI コマンド

CLI コマンド	説明
copy source-url destination-url snmp	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とおりです。

```
console# copy running-config tftp://11.1.1.2/pp.txt
```

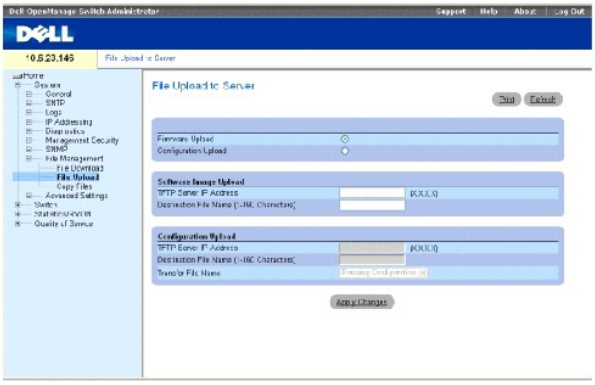
メモ： それぞれの "!" は、10 個のパケットの転送が成功したことを示しています。

```
Accessing file 'file1' on 172.16.101.101.

Loading file1 from 172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!
OK

Copy took 0:01:11 hh:mm:ss
```

ファイルのアップロード

サーバーへのファイルのアップロード ページには、TFTP サーバーからデバイスへソフトウェアをアップロードするためのフィールドがあります。また、イメージファイルも**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。**サーバーへのファイルのアップロード** 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 6-77. サーバーへのファイルのアップロード



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。**ファームウェアのアップロード** が選択された場合、**設定のアップロード** フィールドはグレーになります。

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。**設定のアップロード** が選択された場合、**ソフトウェアイメージのアップロード** フィールドはグレーになります。

Software Image Upload TFTP Server IP Address（ソフトウェアイメージのアップロード TFTP サーバー IP アドレス）— ソフトウェアイメージがアップロードされる TFTP サーバー IP アドレスです。

Software Image Upload Destination（ソフトウェアイメージのアップロード宛先）— ファイルがアップロードされるソフトウェアイメージファイルパスを指定します。

Configuration Upload TFTP Server IP Address（設定のアップロード TFTP IP アドレス）— 設定ファイルがアップロードされる TFTP サーバー IP アドレスです。

Configuration Upload Destination（設定のアップロード宛先）— ファイルがアップロードされる設定ファイルパスを指定します。

Configuration Upload Transfer file name（設定のアップロード転送ファイル名）— 設定がアップロードされるソフトウェアファイルです。可能なフィールド値は以下のとおりです。

Running Configuration（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

Backup Configuration（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

ファイルのアップロード

1. **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。
2. アップロードするファイルのタイプを定義します。
3. フィールドを定義します。
4. **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、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。

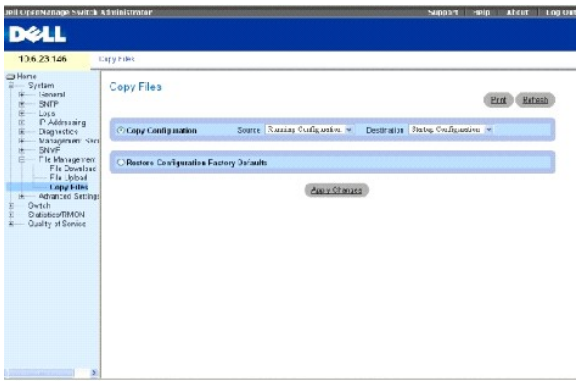
表 6-46. ファイルのアップロード CLI コマンド

CLI コマンド	説明
copy source-url destination-url snmp	ソースから宛先へファイルをコピーします。

ファイルのコピー

ファイルはファイルのコピー ページからコピーおよび削除することができます。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 6-78. ファイルのコピー



Copy Configuration（コピーの設定） — 選択されていると、実行設定ファイル、スタートアップ設定ファイル、またはバックアップ設定ファイルのいずれかをコピーします。可能なフィールド値は以下のとおりです。

Source（ソース） — 実行設定ファイル、スタートアップ設定ファイル、またはバックアップ設定ファイルのいずれかをコピーします。

Destination（宛先） — 実行設定ファイル、スタートアップ設定ファイル、またはバックアップ設定ファイルがコピーされる先のファイルです。

Restore Configuration Factory Defaults（工場出荷時デフォルト設定の復元） — 選択されていると、工場出荷時の設定デフォルトファイルがリセットされることを指定します。選択されていないと、現在の設定が維持されます。

ファイルのコピー

1. ファイルのコピー ページを開きます。
2. **Source（ソース）** および **Destination（宛先）** フィールドを定義します。
3. **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

1. ファイルのコピー ページを開きます。
2. **Restore Configuration Factory Defaults（工場出荷時のデフォルトの復元）** をクリックします。
3. 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、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。

表 6-47. ファイルのコピー CLI コマンド

CLI コマンド	説明
copy *source-url destination-url* **[snmp]**	ソースから宛先へ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。

CLI コマンドの例は次のとおりです。

```
Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101.

Loading file1 from
172.16.101.101: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

Copy took 0:01:11 [hh:mm:ss]

Console# delete startup-config



Console# copy running-config startup-config

01-Jan-2000 01:55:03 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded
```

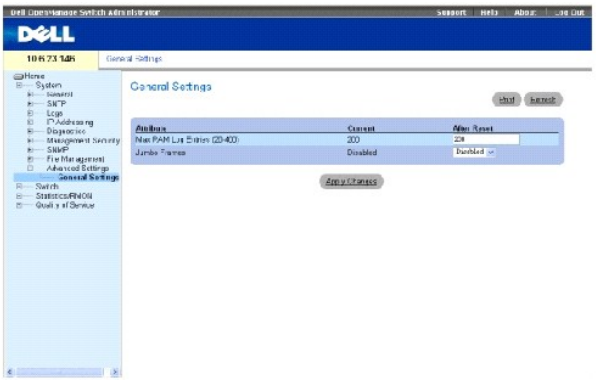
詳細設定の定義

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。詳細設定を使用してデバイスの様々なグローバル属性を設定します。これらの属性への変更は、デバイスがリセットされた後にのみ適用されます。**詳細設定** ページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム） → Advanced Settings（詳細設定）をクリックします。

一般的なデバイスのチューニングパラメーターの設定

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。一般的な設定 ページを開くには、ツリー表示の Ｓｙｓｔｅｍ（システム） → Advanced Settings（詳細設定） → General（一般）をクリックします。

図 6-79. 一般的な設定



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。

Jumbo Frames（ジャンボフレーム） — ジャンボフレーム機能を有効または無効にします。ジャンボフレームは、小数のフレームでの同一データの移動を可能にします。これにより、オーバーヘッドの減少、処理時間の短縮、割り込みの減少を確保します。

CLI コマンドを使用した RAM ログエントリカウンタの表示

以下の表は、一般的な設定 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。

表 6-48. 一般的な設定 CLI コマンド

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。
port jumbo-frame	デバイスのジャンボフレームを有効にします。

CLI コマンドの例は次のとおりです。

```
Console (config)# logging
buffered size 300
```

目次ページに戻る

目次ページに戻る

Dell™ PowerConnect™ 5324 システムユーザーガイド

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷またはデータの損失の可能性があることを示します。また、その問題を回避するための方法も記載されています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示します。

2004 年 4 月 Rev. A00

目次ページに戻る

目次に戻る

Dell OpenManage Switch Administrator の使い方

Dell™ PowerConnect™ 5324 システムユーザーガイド

本項では、ユーザーインタフェースの概要について説明します。

インタフェースについて

ホームページには以下の表示方法があります。

- 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 5-13. Switch Administrator コンポーネント

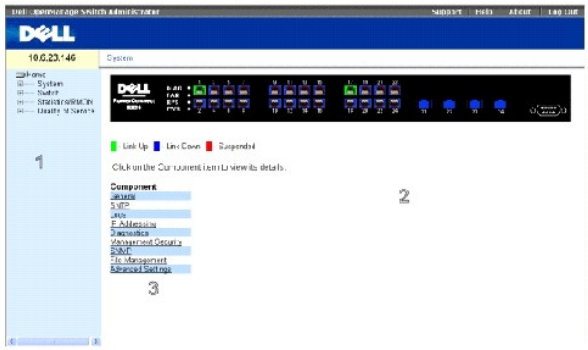


表 5-7 は、対応する番号の付いたインタフェースコンポーネントのリストです。

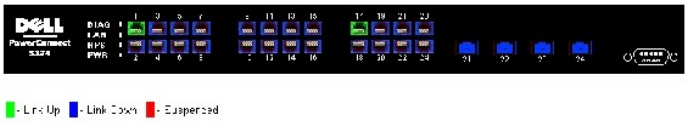
表 5-7. インタフェースコンポーネント

コンポーネント	名前
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

PowerConnect ホームページには、正面パネルのグラフィックデバイスの描写があります。

図 5-14. ポート LED 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。ポートには以下の色があります。

表 5-8. Led インジケータ

コンポーネント	名前
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。

メモ: ポート LED は、PowerConnect OpenManage Switch Administrator の PowerConnect フロント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。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説明します。

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 5-9. 情報ボタン

ボタン	説明
Support(サポート)	**support.jp.dell.com.** にアクセスしてデルサポートページを開きます。
Help(ヘルプ)	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現在開いているページに直接リンクしています。例えば、**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(バージョン情報)	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)	アプリケーションからログアウトしてブラウザウィンドウを閉じます。

デバイス管理ボタン

デバイス管理ボタンは、デバイス情報を設定する簡単な方法を提供します。このボタンには以下のものが含まれます。

表 5-10. デバイス管理ボタン

ボタン	説明
Apply Changes(変更の適用)	デバイスに変更を適用します。
Add(追加)	情報を表またはダイアログに追加します。
Telnet(Telnet)	Telnet セッションを開始します。
Query(クエリ)	表を問い合わせます。
Show All(すべてを表示)	デバイス表を表示します。

Left arrow/Right arrow(左矢印 / 右矢印)	リスト間で情報を移動します。
Refresh(リフレッシュ)	デバイス情報をリフレッシュします。
Reset All Counters(すべてのカウンタのリセット)	統計カウンタをクリアします。
Print(印刷)	**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。
Show Neighbors Info(隣接情報の表示)	**隣接表** ページから **隣接リスト** を表示します。
Draw(描画)	オンザフライで統計チャートを作成します。

アプリケーションの起動

1. ウェブブラウザを開きます。
2. (CLI で定義された)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。

   IP アドレスのデバイスへの割り当てについての情報に関しては、「静的 IP アドレスおよびサブネットマスク」を参照してください。
3. **Enter Network Password (ネットワークパスワードの入力)** ウィンドウが開いたら、ユーザー名とパスワードを入力します。

メモ: デバイスはデフォルトのパスワードでの設定がされていないので、パスワードを入力しなくても設定できます。紛失したパスワードの回復についての情報に関しては、「パスワードの回復」を参照してください。

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。

4. **OK** をクリックします。

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

CLI を使用したデバイスへのアクセス

デバイスは、コンソールポートへの直接接続により、または Telnet 接続によって管理することができます。CLI の使い方は、Linux システムでコマンドを入力することと類似しています。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、「静的 IP アドレスおよびサブネットマスク」を参照してください。

メモ: CLI を使用する前に、クライアントがロードされていることを確認します。

コンソール接続

1. 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。
2. Console> プロンプトが表示されたら、enable と入力し、<Enter> を押します。
3. 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。
4. 終了したら、quit または exit コマンドでセッションを終了します。

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。ASCII ターミナルは、TCP/IP プロトコルネットワークを介してローカルデバイスに仮想的に接続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、4 つまでの同時 Telnet セッションに対応できます。すべての CLI コマンドは、Telnet セッションで使用できます。

Telnet セッションを開始するには次の手順を実行します。

1. 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。

2. **Run(ファイル名を指定して実行)** ウィンドウの **Open(名前)** フィールドに、Telnet <IP アドレス> を入力します。
3. **OK** をクリックすると、Telnet セッションが開始します。

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。コンソールプロンプトで ?(疑問符)を入力すると、特定のコマンドモードで利用可能なコマンド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、コンソー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かぎり 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 ***** という形式で表示され、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。

1. プロンプトでenable と入力し、<Enter> を押します。
2. 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、<Enter> を押します。

特権 EXEC モードからユーザー EXEC モードに戻るには、次のいずれかのコマンドを使用します。disable, exit/end または <Ctrl><Z>

以下の例は、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 と入力し、<Enter> を押します。グローバル設定モードは、デバイスホスト名とそれに続く(config)およびポンド記号 # 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> コマンドを使用します。

以下の例は、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#
```

インタフェース設定モード

インタフェース設定コマンドは、ブリッジグループ、記述など特定の IP インタフェースの設定を変更します。

VLAN データベースモード

VLAN モードには、たとえば、VLAN を作成して IP アドレスを VLAN に適用するなどのように、VLAN 全体を作成したり設定するコマンドがあります。以下は VLAN モードプロンプトの例です。

```
Console # vlan database

Console (config-vlan)#
```

ポートチャネルモード

ポートチャネルモードには、リンクアグリゲーショングループ（LAG）を設定するためのコマンドがあります。以下はポートチャネルモードプロンプトの例です。

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

Console (config-if)#
```

インタフェースモード

インタフェースモードには、インタフェースを設定するコマンドがあります。グローバル設定モードコマンド `interface ethernet` を使用して、インタフェース設定モードに入ります。以下はインタフェースモードプロンプトの例です。

```
console> enable

console# configure

console(config)# interface ethernet g18

console(config-if)#
```

管理アクセスリスト

管理アクセスリストモードには、管理アクセスリストを定義するためのコマンドがあります。グローバル設定モードコマンド `management access-list` を使用して、管理アクセスリスト設定モードに入ります。

以下の例は、"mlist" と呼ばれるアクセスリストを作成し、2 つの管理インタフェースイーサネット `g1` および `g9` を設定し、アクセスリストをアクティブなリストにする方法を示したものです。

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

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

Console (config-macl)# exit

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

SSH パブリックキー

SSH パブリックキーモードには、他のデバイス SSH パブリックキーを手動で指定するためのコマンドがあります。

グローバル設定モードコマンド `crypto key pubkey-chain ssh` を使用して、SSH パブリックキーチェーン設定モードに入ります。

以下は SSH パブリックキーチェーン設定モードに入る例を示しています。

```
Console(config)# crypto key pubkey-chain ssh

Console(config-pubkey-chain)#
```

CLI の例

設定例としての CLI コマンドが提供されています。例を含む CLI コマンドの詳細に関しては、マニュアル CD に含まれる「CLI リファレンスガイド」を参照してください。

目次に戻る

目次に戻る

統計の表示

Dell™ PowerConnect™ 5324 システムユーザーガイド

統計 ページには、インタフェース、GVRP、Etherlike、RMON、およびデバイスの利用率に関するデバイス情報があります。**統計** ページを開くには、ツリー表示の **統計** をクリックします。

メモ: すべての統計ページに CLI コマンドを使用できるわけではありません。

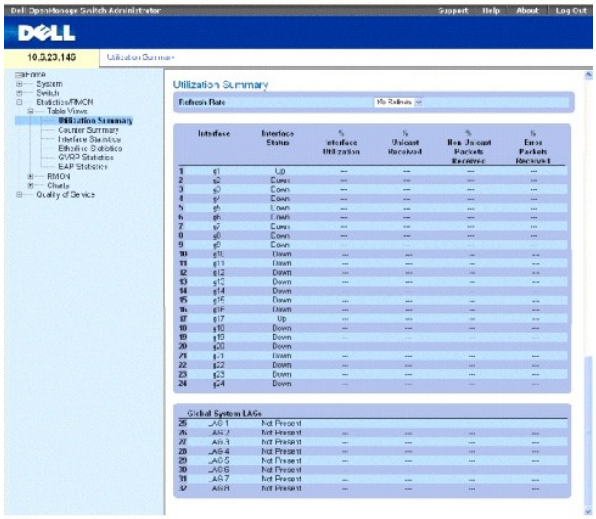
表の表示

表の表示 ページには、統計をチャート形式で表示するためのリンクがあります。**表の表示** ページを開くには、ツリー表示の **統計** → **表** をクリックします。

利用率の要約の表示

利用率の要約ページには、インタフェースの利用率に関する統計があります。利用率の要約 ページを開くには、ツリー表示の **統計** → **表の表示** → **利用率の要約** をクリックします。

図 8-115. 利用率の要約



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。

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。

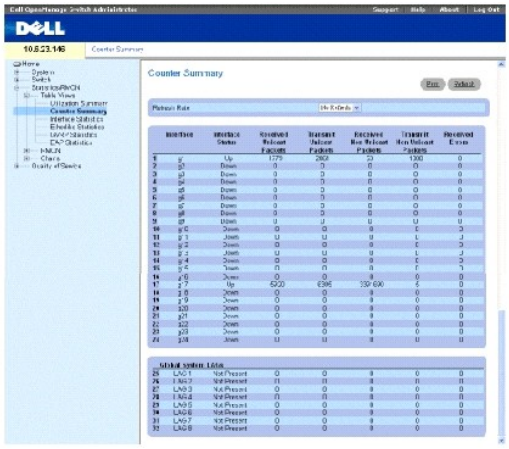
% Error Packets Received（受信されたエラーパケットの %） — インタフェースで受信されたエラーのあるパケットの数です。

Global System LAG（グローバルシステム LAG） — 現在の LAG/トランク性能です。

カウンタの要約の表示

カウンタの要約 ページには、ポート利用率をパーセンテージではなく数値の合計で表示する統計があります。**カウンタの要約** ページを開くには、ツリー表示の **統計 / RMON → 表の表示 → カウンタの要約** をクリックします。

図 8-116. カウンタの要約



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。

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。

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 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。

Transmit Non Unicast Packets（送信された非ユニキャストパケット） — インタフェースから送信された非ユニキャストパケットの数です。

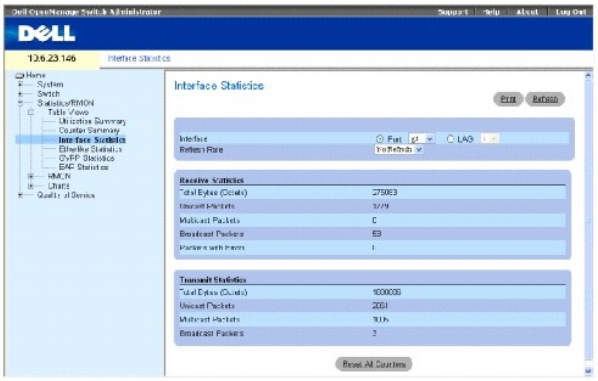
Received Errors（受信されたエラー） — インタフェースで受信されたエラーパケットの数です。

Global System LAG（グローバルシステム LAG） — 現在の LAG/トランク性能です。

インタフェース統計の表示

インタフェース統計 ページには、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。インタフェース統計 ページを開くには、ツリー表示の **統計 / RMON → 表の表示 → インタフェース統計** をクリックします。

図 8-117. インタフェース統計



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。

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。

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で送信されたエラーパケットの数です。

インタフェース統計の表示

1. **インタフェース統計** ページを開きます。
2. **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

1. **インタフェース統計** ページを開きます。
2. **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

以下の表は、インタフェース統計を表示するための等価 CLI コマンドをまとめたものです。

表 8-80. 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 *インタフェース* | **port-channel** *ポートチャネル番号*]	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。

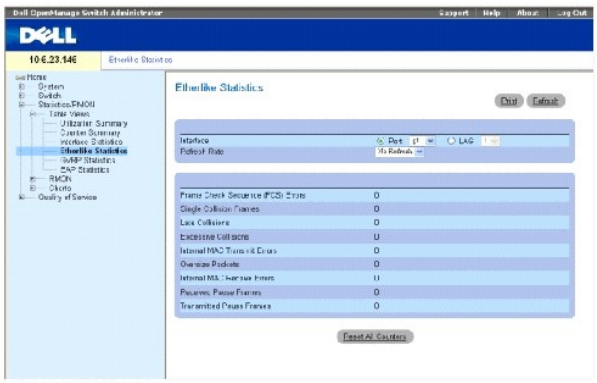
```
Console> enable

Console# show interfaces counters

Port    InOctets    InUcastPkts    InMcastPkts    InBcastPkts
------  ----------  -------------  -------------  ------------
g1      183892      1289           987            8
g2      0           0              0              0
```

g3	123899	1788	373	19
Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-------	----------	----------	----------	----------
g4	9188	9	8	0
g5	0	0	0	0
g6	8789	27	8	0
Ch	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
-------	----------	----------	----------	----------
1	27889	928	0	78
Ch	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-------	----------	----------	----------	----------
1	23739	882	0	122

Etherlike 統計の表示

Etherlike 統計 ページには、インタフェース統計が含まれます。Etherlike 統計 ページを開くには、ツリー表示の **統計 / RMON → 表の表示 → Etherlike 統計** をクリックします。

図 8-118. Etherlike 統計



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。

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の数です。

Multiple Collision Frames（マルチプ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マルチプルコリジョンフレームの数です。

Single Quality Error (SQE) Test Errors（シングル品質エラー（SQE）テストエラー） — 選択されたインタフェースで受信された SQE テストエラーの数です。

Deferred Transmissions（延期された送信） — 選択されたインタフェースにおける延期された送信の数です。

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。**Excessive Collisions（過度のコリジョン）** — 選択されたインタフェースで受信された過度のコリジョンの数です。

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。

Internal MAC Transmit Errors（キャリア検出エラー） — 選択されたインタフェースにおけるキャリア検出エラーの数です。

Oversize Packets（大型パケット） — 選択されたインタフェースにおける大型パケットのエラーの数です。

Internal MAC Receive Errors（内蔵 MAC 受信エラー） — 選択されたインタフェースにおける内蔵 MAC 受信エラーの数です。

Single Quality Errors (SQE) Test Errors（シングル品質エラー（SQE）テストエラー） — 選択されたインタフェースで受信された SQE テストエラーの数です。

Receive 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フレームの数です。

Transmitted Paused 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フレームの数です。

インタフェースの Etherlike 統計の表示

1. **Etherlike 統計** ページを開きます。
2. **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。

インタフェースの Etherlike 統計が表示されます。

Etherlike 統計のリセット

1. **Etherlike 統計** ページを開きます。
2. **Reset All Counters（すべてのカウンタのリセット）** をクリックします。

Ethernetlike 統計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

以下の表は、Etherlike 統計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 8-81. Etherlike 統計 CLI コマンド

CLI コマンド	説明
show interfaces counters [ethernet インタフェース | **port-channel** *ポートチャネル番号*]	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> enable

Console# show interfaces counters ethernet g1

Port    InOctets    InUcastPkts    InMcastPkts    InBcastPkts
------  ----------  -------------  -------------  ------------
g1      183892      1289           987            8

Port    OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
------  ----------  -------------  -------------  ------------
g1      9188        9              8              0

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0
```

```
Excessive Collisions: 0

Internal MAC Tx Errors: 0

Carrier Sense Errors: 0

Oversize Packets: 0

Internal MAC Rx Errors: 0

Received Pause Frames: 0

Transmitted Pause Frames: 0
```

GVRP 統計の表示

GVRP 統計 ページには、GVRP のデバイス統計が含まれます。**GVRP 統計** ページを開くには、ツリー表示の **統計 / RMON → 表の表示 → GVRP 統計** をクリックします。

図 8-119. GVRP 統計

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。

Join Empty（空への参加） — デバイス GVRP の空への参加統計です。

Empty（空） — デバイス GVRP 空統計です。

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。

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 Events（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

1. **GVRP 統計** ページを開きます。
2. **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。

インタフェースの GVRP 統計が表示されます。

GVRP 統計のリセット

1. **GVRP 統計** ページを開きます。
2. **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 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

以下の表は、GVRP 統計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 8-82. GVRP 統計 CLI コマンド

CLI コマンド	説明
show gvrp statistics [**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*]	GVRP 統計を表示します。
show gvrp error-statistics [**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*]	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:

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

rJE : Join Empty Received          rJIn : Join In Received
rEmp : Empty Received              rLIn : Leave In Received
rLE : Leave Empty Received         rLA : Leave All Received
sJE : Join Empty Sent              sJIn : Join In Sent
sEmp : Empty Sent                  sLIn : Leave In Sent
sLE : Leave Empty Sent             sLA : Leave All Sent

Port  rJE  rJIn  rEmp  rLIn  rLE  rLA  sJE  sJIn  sEmp  sLIn  sLE  sLA
----  ---  ----  ----  ----  ---  ---  ---  ----  ----  ----  ---  ---
g1    0    0     0     0     0    0    0    0     0     0     0    0
g2    0    0     0     0     0    0    0    0     0     0     0    0
g3    0    0     0     0     0    0    0    0     0     0     0    0
g4    0    0     0     0     0    0    0    0     0     0     0    0
g5    0    0     0     0     0    0    0    0     0     0     0    0
g6    0    0     0     0     0    0    0    0     0     0     0    0
g7    0    0     0     0     0    0    0    0     0     0     0    0
g8    0    0     0     0     0    0    0    0     0     0     0    0
```

```
Console# show gvrp error-statistics

GVRP error statistics:

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

Legend:

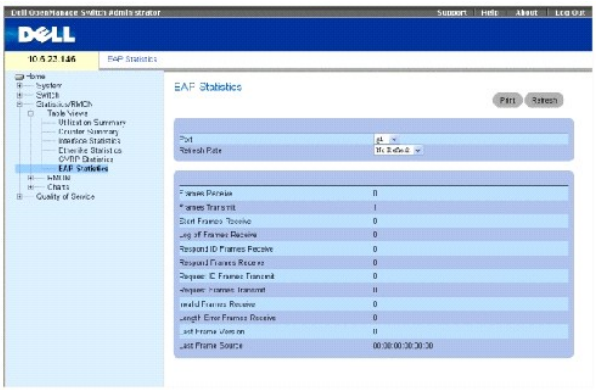
INVPROT : Invalid Protocol Id	INVPLEN : Invalid PDU Length
INVATYP : Invalid Attribute Type	INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value	INVEVENT : Invalid Event

Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
g1	0	0	0	0	0
g2	0	0	0	0	0
g3	0	0	0	0	0
g4	0	0	0	0	0
g5	0	0	0	0	0
g6	0	0	0	0	0
g7	0	0	0	0	0
g8	0	0	0	0	0

EAP 統計の表示

EAP 統計 ページには、特定のポートで受信された EAP パケットに関する情報があります。EAP の詳細に関しては、「ポートベース認証（802.1x）」を参照してください。**EAP 統計** ページを開くには、ツリー表示の統計/RMON > 表の表示 > EAP 統計をクリックします。

図 8-120. EAP 統計



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） — 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。

Frames Receive（フレーム受信） — ポートで受信された有効な EAPOL フレームの数です。

Frames Transmit（フレーム送信） — ポートを介して送信された EAPOL フレームの数です。

Start Frames Receive（スタートフレーム受） — ポ信ートで受信された EAPOL スタートフレームの数です。

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です。

Respond ID Frames Receive（応答 ID フレーム受信） — ポートで受信された EAP Resp/Id フレームの数です。

Respond Frames Receive（応答フレーム受信） — ポートで受信された有効な EAP 応答フレームの数です。

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 フレームの数です。

Request Frames Transmit（要求フレーム送信） — ポートを介して送信された EAP 要求フレームの数です。

Invalid Frames Receive（無効なフレーム受信） — このポートで受信された未認識 EAPOL フレームの数です。

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 フレームの数です。

Last Frame Version（最後のフレームバージョン） — 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です。

Last Frame Source（最後のフレームソース） — 最近受信された EAPOL フレームに付されたソース MAC アドレスです。

ポートの EAP 統計の表示

1. **EAP 統計** ページを開きます。
2. **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

1. **EAP 統計** ページを開きます。
2. Reset All Counters（すべてのカウンタのリセット）をクリックしてカウンタをリセットします。

EAP 統計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

以下の表は、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 8-83. GVRP 統計 CLI コマンド

CLI コマンド	説明
show dot1x statistics ethernet *インタフェース*	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。

```
Switch# show dot1x statistics ethernet g1

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 0008.3b79.8787
```

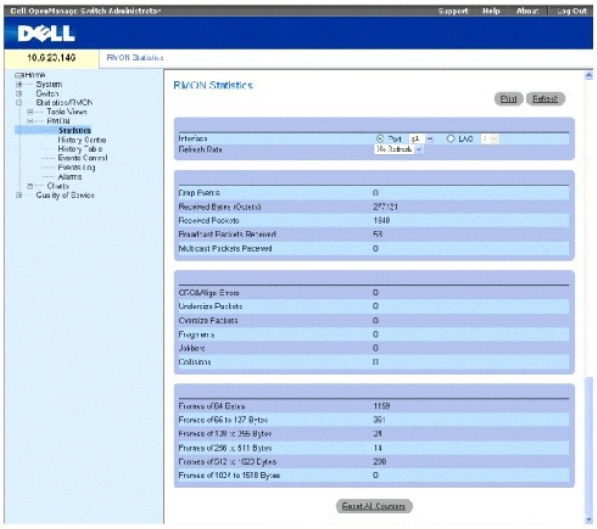
RMON 統計の表示

リモートモニタリング（RMON）には、リモートロケーションからのネットワーク情報を表示するためのリンクがあります。**RMON** ページを開くには、ツリー表示の **統計 / RMON → RMON** をクリックします。

RMON 統計グループの表示

RMON 統計ページには、デバイス利用率およびデバイスで発生するエラーに関する情報を表示するためのフィールドがあります。RMON 統計ページを開くには、ツリー表示の **統計 / RMON →** **RMON →統計** をクリックします。

図 8-121. RMON 統計



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。

Drop Events（イベントの破棄） — 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破棄されたイベントの数です。

Received Bytes (Octets)（受信されたバイト（オクテット）） — デバイスが最後にリフレッシュされてからインタフェースで受信されたオクテットの数です。この数には不良パケットおよび FCS オクテットは含まれますが、フレーミングビットは含まれません。

Received Packets（受信されたパケット） — 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、不良パケット、マルチキャストパケット、およびブロードキャストパケットなどのパケットの数です。

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（1518 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（1518 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（バイトのフレーム） — デバイスが最後にリフレッシュされてからインタフェースで受信された*xx* バイトのフレームの数です。

インタフェース統計の表示

1. RMON 統計ページを開きます。
2. **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

以下の表は、RMON 統計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 8-84. RMON 統計 CLI コマンド

CLI コマンド	説明
show rmon statistics {**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*}	RMON Ethernet 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> enable
```

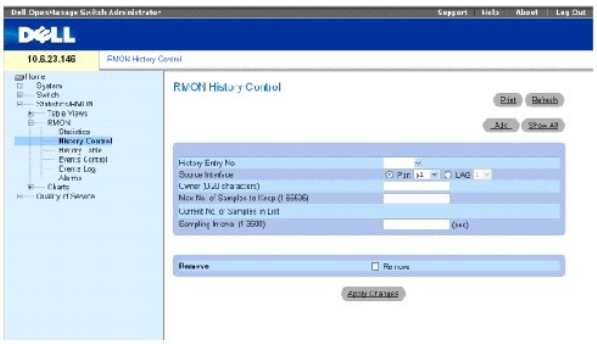
```
console> enable

Console# show rmon statistics ethernet g1

Port g1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0
```

```
Undersize Pkts: 0 Oversize Pkts: 0


Fragments: 0 Jabbers: 0


64 Octets: 98 65 to 127 Octets: 0


128 to 255 Octets: 0 256 to 511 Octets: 0


512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

RMON ヒストリ制御統計の表示

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ることがあります。
RMON ヒストリ制御 ページを開くには、ツリー表示の **統計 / RMON → ヒストリ制御** をクリックします。

図 8-122. RMON ヒストリ制御



History Entry No.（ヒストリエントリの番号） — **ヒストリ制御表** ページのエントリの番号です。

Source Interface（ソースインタフェース） — ヒストリサンプルが取られるポートまたは 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 (1-65535)（保存するサンプルの最大の番号（1 ～ 65535）） — 保存されるサンプルの数です。デフォルト値は 50 です。

Current No. of Samples in List（リストにあるサンプルの現在の番号） — 得られたサンプルの現在の番号です。

Sampling Interval (1-3600)（サンプルの間隔（1 ～ 3600）） — サンプルがポートから得られる時間を秒単位で表示します。可能な値は 1 ～ 3600 秒です。デフォルトは 1800 秒（30 分）です。

Remove（削除） — 選択されていると、**ヒストリ制御表** エントリを削除します。

ヒストリ制御エントリの追加

1. **RMON ヒストリ制御** ページを開きます。
2. **Add（追加）** をクリックします。

   ヒストリエントリの追加 ページが開きます。
3. ダイアログのフィールドを完成させます。
4. **Apply Changes（変更の適用）** をクリックします。

   エントリが **ヒストリ制御表** に追加されます。

ヒストリ制御表エントリの変更

1. **RMON ヒストリ制御** ページが開きます。
2. **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。
3. 要求されたフィールドを変更します。
4. **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

1. **RMON ヒストリ制御** ページを開きます。
2. **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。
3. **Remove（削除）**をクリックします。
4. **Apply Changes（変更の適用）** をクリックします。

   選択された表エントリが削除され、デバイスがアップデートされます。

CLI コマンドを使用した RMON ヒストリ制御の表示

以下の表は、GVRP 統計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 8-85. RMON ヒストリ CLI コマンド

CLI コマンド	説明
rmon collection history *index* **owner** [*オーナー名* | **buckets** *バケット番号*] [**インターバル** *秒*]	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** *インタフェース* | **port-channel** *ポートチャネル番号*]	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。

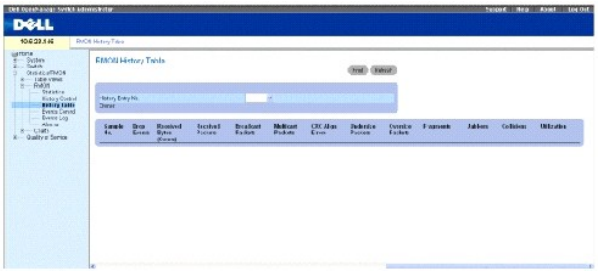
```
Console (config)#
interface ethernet g8



Console (config-if)# rmon
collection history 1
interval 2400



Console(config-if)# exit
```

```
Console(config)# exit
```

RMON ヒストリ表の表示

RMON ヒストリ表 には、インタフェースに固有の統計ネットワークサンプルが含まれます。各表エントリは、一回のサンプルを収集中に編集されたすべてのカウンタ値を表します。**RMON ヒストリテーブル** を開くには、ツリー表示の **統計 / RMON → RMON → ヒストリ表** をクリックします。

図 8-123. RMON ヒストリ表



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。

Drop Events（イベントの破棄） — サンプルが収集される間にネットワークリソースの不足によって破棄されたパケットの数を示します。これは破棄されたパケットの正確な数ではなく、破棄されたパケットが検出された回数を表わすことがあります。

Received Bytes (Octets)（受信されたバイト（オクテット）） — ネットワークで受信された不良パケットを含むデータのオクテット数を示します。

Received Packets（受信されたパケット） — サンプルが収集される間に受信されたパケットの数。

Broadcast Packets（ブロードキャストパケット） — サンプルが収集される間に受信された優良なブロードキャストパケットの数です。

Multicast Packets（マルチキャストパケット） — サンプルが収集される間に受信された優良なマルチキャストパケットの数です。

CRC Align Errors（CRC 調製エラー） — サンプルセッション中に受信された 64 ～ 1518 オクテットで、不良なフレームチェックシーケンス（FCS）を持つ、整数のオクテットまたは非整数による不良な FCS を持つパケットの数です。

Undersize Packets（小型パケット） — サンプルセッション中に受信された 64 オクテット未満のパケットの数です。

Oversize Packets（大型パケット） — サンプルセッション中に受信された 1518 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） — サンプル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 1518 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） — サンプルセッション中に発生したパケットコリジョンの全体数の概算です。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） — サンプルセッション中のインタフェースのメイン物理層ネットワークの使用を概算します。値は小数点以下 2 桁までのパーセントで反映されます。

特定のヒストリエントリの統計の表示

1. **RMON ヒストリ表** を開きます。
2. **ヒストリ表の番号** 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

以下の表は、RMON ヒストリ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 8-86. 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 Ethernet 統計ヒストリを表示します。

以下に、索引 1 のスループットの RMON Ethernet 統計を表示するための等価 CLI コマンドの例を示します。

```
console> enable

Console# show rmon history 1 throughput

Sample Set: 1                          Owner: CLI
Interface: g1                          Interval: 1800
Requested samples: 50                  Granted samples: 50

Maximum table size: 500

Time                 Octets      Packets  Broadcast  Multicast  %
-------------------  ----------  -------  ---------  ---------  -----
Jan 18 2004 21:57:00 303595962   357568   3289       7287       19.98%
Jan 18 2004 21:57:30 287696304   275686   2789       2789       20.17%
```

デバイス RMON イベントの定義

RMON イベント制御 ページには、RMON イベントを定義するためのフィールドがあります。RMON イベント制御 ページを開くには、ツリー表示の **統計 / RMON → RMON→ イベント制御** をクリックします。

図 8-124. RMON イベント制御

Event Entry（イベントエントリ） — イベントです。

Community（コミュニティ） — イベントが属するコミュニティです。

Description（説明） — ユーザー定義のイベントの説明です。

Type（タイプ） — イベントタイプの説明です。可能な値は以下のとおりです。

Log（ログ） — イベントタイプはログエントリです。

Trap（トラップ） — イベントタイプはトラップです。

Log and Trap（ログおよびトラップ） — イベントタイプはログエントリとトラップの両方です。

None（なし） — イベントはありません。

Time（時間） — イベントが起きた時間です。たとえば、2004 年 3 月 29 日午前 11:00 時は 29/03/2004 11:00:00と表示されます。

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を削除します。

RMON イベントの追加

1. RMON イベント制御 ページを開きます。
2. **Add（追加）** をクリックします。

イベントエントリの追加 ページが開きます。

3. 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。

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

1. **RMON イベント制御** ページを開きます。
2. **イベント表** でエントリを選択します。
3. 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。

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

1. **RMON イベント制御** ページを開きます。
2. **Show All（すべてを表示）**をクリックします。

イベント表 ページが開きます。

3. 削除の必要があるイベントで**Remove（削除）**を選択してから**Apply Changs（変更の適用）**をクリックします。

選択された表エントリが削除され、デバイスがアップデートされます。

メモ: **RMON イベント制御** ページで **Remove（削除）** チェックボックスを選択すると、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。

CLI コマンドを使用したデバイスイベントの定義

以下の表は、デバイスイベントを定義するための等価t CLI コマンドをまとめたものです。

表 8-87. 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 *インデックスタイプ* [**community** テキスト] [**description** テキスト] [**owner** *名前*]	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。

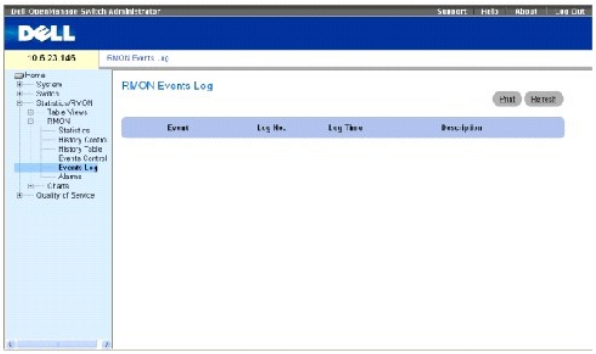
```
console> enable

console#config

console (config)# rmon event 1 log

console(config)# exit

Console# show rmon events
```

Index	Description	Type	Community	Owner	Last time sent
-----	----------	--------	---------	-------	-------------------
1	Errors	Log		CLI	Jan 18 2002 23:58:17
2	High Broadcast	Log-Trap	router	Manager	Jan 18 2002 23:59:48

RMON イベントログの表示

RMON イベントログ ページには、RMON イベントのリストがあります。RMON イベントログ ページを開くには、ツリー表示の **統計 / RMON → RMON → イベント**をクリックします。

図 8-125. RMON イベントログ



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

以下の表は、デバイスイベ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

表 8-88. 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 [イベント]	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> enable

console#config

console (config)# rmon event 1 log

console(config)# exit

Console# show rmon log
```

```
Maximum table size: 500
```

Event	Description	Time
1	Errors	Jan 18 2002 23:48:19
1	Errors	Jan 18 2002 23:58:17
2	High Broadcast	Jan 18 2002 23:59:48

```
Console# show rmon log
```

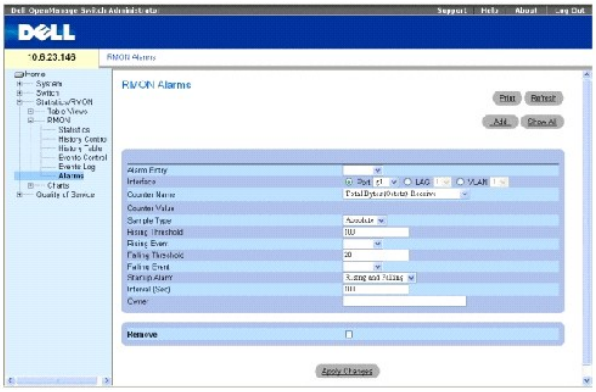
```
Maximum table size: 500 (800 after reset)
```

Event	Description	Time
1	Errors	Jan 18 2002 23:48:19
1	Errors	Jan 18 2002 23:58:17
2	High Broadcast	Jan 18 2002 23:59:48

RMON デバイスアラームの定義

RMON アラーム ページには、ネットワークアラームを設定するためのフィールドがあります。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ネットワークアラームが起きます。しきい値を上げたり下げたりするとイベントが発生します。 RMON アラーム ページを開くには、ツリー表示の **統計 / RMON → RMON→アラーム** をクリックします。

図 8-126. RMON アラーム



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 変数です。

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以下のとおりです。

Delta（デルタ） — 現在の値から最後にサンプル収集された値を引きます。この値の差としきい値を比較します。

Absolute（絶対値） — サンプル収集の終りに値をしきい値と直接比較します。

Rising Threshold（上昇しきい値） — 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。それぞれのモニターされた変数には指定され色があります。

Rising / Falling Event（上昇 / 下降イベント） — アラームが報告される機構です。ログ、トラップ、またはその両方の組合せがあります。ログを選択した場合、デバイスにも管理システムにも保存機構はありません。ただし、デバイスがリセットされていないと、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、トラップの一般的な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（下降しきい値） — 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、グラフバーの下にグラフで表示されます。それぞれのモニターされた変数には指定された色があります。

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 (sec)（間隔（秒）） — アラームの間隔です。

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） — 選択されていると、RMON アラームを削除します。

アラーム表エントリの追加

1. **RMON アラーム** ページを開きます。
2. **Add（追加）** をクリックします。

   アラームエントリの追加 ページが開きます。

図 8-127. アラームエントリの追加ページ

3. インタフェースを選択します。
4. ダイアログのフィールドを完成させます。
5. **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

1. **RMON アラーム** ページを開きます。
2. **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。
3. 要求されたダイアログのエントリを変更します。
4. **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

1. **RMON アラーム** ページを開きます。
2. **Show All（すべてを表示）** をクリックします。

   アラーム表 ページが開きます。

アラーム表エントリの削除

1. **RMON アラーム** ページを開きます。

2. **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。
3. **Remove（削除）** チェックボックスを選択します。
4. **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デバイスアラームの定義

以下の表は、デバイスアラーム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 8-89. デバイスアラーム CLI コマンド

CLI コマンド	説明
rmon alarm *index variable interval rthreshold fthreshold revent fevent* [**type** *タイプ*] [**startup** *ディレクション*] [**owner** *名前*]	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> enable

console#config

Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20

Console# show rmon alarm-table
```

Index	OID	Owner
------	-------------------	--------------
1	1.3.6.1.2.1.2.2.1.1 0.1	CLI
2	1.3.6.1.2.1.2.2.1.1 0.1	Manager
3	1.3.6.1.2.1.2.2.1.1 0.9	CLI

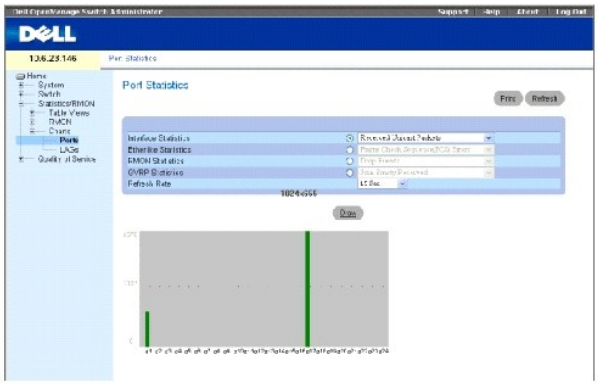
チャートの表示

チャート ページには、統計をチャート形式で表示するためのリンクがあります。**チャート** ページを開くには、ツリー表示の統計 → チャートをクリックします。

ポート統計の表示

ポート統計 ページには、ポート要素の統計をチャート形式で開くためのフィールドがあります。**ポート統計** ページを開くには、ツリー表示の**統計** → **チャート** → **ポート**をクリックします。

図 8-128. ポート統計



Interface Statistics（インタフェース統計） — インタフェース統計のタイプを選択して開きます。

Etherlike Statistics（Etherlike 統計） — Etherlike 統計のタイプを選択して開きます。

RMON Statistics（RMON 統計） — RMON 統計のタイプ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。

ポート統計の表示

1. **ポート統計** ページを開きます。
2. 統計タイプを選択して開きます。
3. **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。
4. **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

以下の表は、ポート統計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 8-90. ポート統計 CLI コマンド

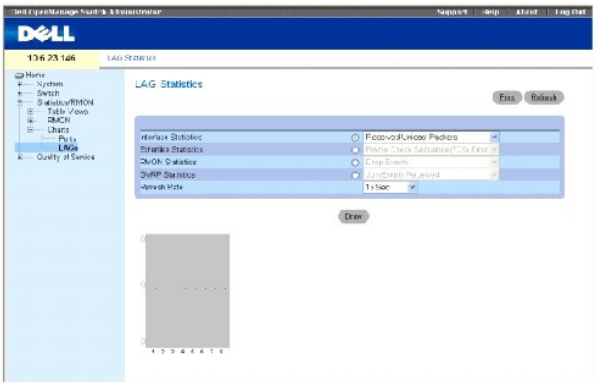
CLI コマンド	説明
show interfaces counters [**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*]	物理的なインタフェースで検出されたトラフィックを表示します。
show rmon statistics {**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*}	RMON Ethernet 統計を表示します。
show gvrp statistics {**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*}	GVRP 統計を表示します。
show gvrp error-statistics {**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*}	GVRP エラー統計を表示します。

Console# **show interfaces description ethernet g1**	
Port	Description
----	----------
g1	Management_port
g2	R&D_port
g3	Finance_port
Ch	Description
----	----------
1	Output

LAG 統計の表示

LAG 統計 ページには、LAG の統計をチャート形式で開くためのフィールドがあります。**LAG 統計** ページを開くには、ツリー表示の**統計** → **チャート** → **LAGs** をクリックします。

図 8-129. LAG 統計



Interface Statistics（インタフェース統計） — インタフェース統計のタイプを選択して開きます。

Etherlike Statistics（Etherlike 統計） — Etherlike 統計のタイプを選択して開きます。

RMON Statistics（RMON 統計） — RMON 統計のタイプ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

1. **LAG 統計** ページを開きます。
2. 統計タイプを選択して開きます。
3. **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。
4. **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

以下の表は、LAG 統計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 8-91. LAG 統計 CLI コマンド

CLI コマンド	説明
show interfaces counters [**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*]	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** *インタフェース* | **port-channel** *ポートチャネル番号*}	RMON Ethernet 統計を表示します。
show gvrp statistics {**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*}	GVRP 統計を表示します。
show gvrp error-statistics {**ethernet** *インタフェース* | **port-channel** *ポートチャネル番号*}	GVRP エラー統計を表示します。

```
Console# show gvrp statistics

GVRP statistics:

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

rJE : Join Empty Received          rJIn : Join In Received

rEmp : Empty Received              rLIn : Leave In Received

rLE : Leave Empty Received         rLA : Leave All Received

sJE : Join Empty Sent              sJIn : Join In Sent

sEmp : Empty Sent                  sLIn : Leave In Sent

sLE : Leave Empty Sent             sLA : Leave All Sent

Port  rJE  rJIn  rEmp  rLIn  rLE  rLA  sJE  sJIn  sEmp  sLIn  sLE  sLA

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

g1	0	0	0	0	0	0	0	0	0	0	0	0
g2	0	0	0	0	0	0	0	0	0	0	0	0
g3	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0

目次に戻る