D-Link DES-3200 シリーズ

Layer2+ 10/100Mbps Metro Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠危険	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
⚠警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、間違った使い方をすると、傷害または物損損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠危険

禁止 **分解・改造をしない**
火災、やけど、けが、感電などの原因となります。

禁止 **ぬれた手でさわらない**
感電の原因となります。

禁止 **水をかけたり、ぬらしたりしない**
内部に水が入ると、火災、感電、故障の原因となります。

禁止 **水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない**
火災、やけど、けが、感電、故障の原因となります。

禁止 **各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く**
火災、やけど、けが、感電、故障の原因となります。

禁止 **油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない**
火災、やけど、けが、感電、故障の原因となります。

禁止 **内部に金属物や燃えやすいものを入れない**
火災、感電、故障の原因となります。

禁止 **砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない**
火災、やけど、けが、感電、故障の原因となります。

禁止 **電子レンジ、IH 調理器などの加熱調理機、圧力釜など高圧容器に入れたり、近くに置いたりしない**
火災、やけど、けが、感電、故障の原因となります。

⚠警告

禁止 **落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない**
故障の原因となります。

禁止 **発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない**
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼ください。

禁止 **表示以外の電圧で使用しない**
火災、感電、または故障の原因となります。

禁止 **たこ足配線禁止**
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

❗ **設置、移動のときは電源プラグを抜く**
火災、感電、または故障の原因となります。

禁止 **雷鳴が聞こえたら、ケーブル / コード類にはさわらない**
感電の原因となります。

禁止 **ケーブル / コード類や端子を破損させない**
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障の原因となります。

❗ **本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する**
火災、感電、または故障の原因となります。

禁止 **各光源をのぞかない**
光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED をのぞきますと強力な光源により目を損傷するおそれがあります。

禁止 **各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほこりが内部に入ったりしないようにする**
火災、やけど、けが、感電または故障の原因となります。

禁止 **使用中に布団で覆ったり、包んだりしない**
火災、やけどまたは故障の原因となります。

❗ **ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る**
引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。

禁止 **カメラのレンズに直射日光などを長時間あてない**
素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の原因となります。

❗ **無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する**
電子機器や医療電気機器に悪影響を及ぼすおそれがあります。

禁止 **本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない**
火災、または故障の原因となります。

❗ **耳を本体から離してご使用ください**
大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。

❗ **無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する**
医療電気機器に悪影響を及ぼすおそれがあります。

❗ **高精度な制御や微弱な信号を取り扱う電子機器の近くでは使用しない**
電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。

❗ **ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する**
破損部や露出部に触れると、やけど、けが、感電の原因となります。

❗ **ペットなどが本機に噛みつかないように注意する**
火災、やけど、けがなどの原因となります。

禁止 **コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない**
火災、やけど、感電または故障の原因となります。

禁止 **AC アダプタや電源ケーブルに海外旅行用の変圧器等を使用しない**
発火、発熱、感電または故障の原因となります。

⚠警告

- ACアダプタもしくは電源プラグについたほこりは、拭き取る
  ほこりが付着した状態で使用すると、
  火災、やけど、感電または故障の原因となります。
- ACアダプタや電源ケーブルをコンセントに
  さしこむときは、確実に差し込む
  確実に差し込まないと、火災、やけど、
  感電もしくは故障の原因となります。
- 接続端子が曲がるなど変形した場合は、直ちに使用を中止する。
  また、変形をもとに戻しての使用も行わない
  端子のショートにより、火災、やけど、けが、
  感電または故障の原因となります。
- 各種接続端子を機器本体に接続する場合、斜めに差したり、
  差した状態で引っ張ったりしない
  火災、やけど、感電または故障の原因となります。
- 使用しない場合は、ACアダプタもしくは
  電源ケーブルをコンセントから抜く
  電源プラグを差したまま放置すると、火災、やけど、
  感電または故障の原因となります。
- お手入れの際は、ACアダプタもしくは
  電源ケーブルをコンセントから抜く
  抜かずに行うと、火災、やけど、感電または故障の原因となります。
- 禁止 SDやMicroSDカード、USBメモリの使用中は、
  カードやメモリを取り外したり、本製品の電源を切ったりしない
  データの消失、機器本体の故障の原因となります。
- 禁止 磁気カードや磁気を帯びたものを本製品に近づけない
  磁気カードのデータが消えてしまうおそれもしくは
  機器本体の誤作動の原因となります。
- ディーリンクジャパンが販売している無線機器は
  国内専用のため、海外で使用しない
  海外では国によって電波使用制限があるため、
  本製品を使用した場合、罰せられる場合があります。
  海外から持ち込んだディーリンク製品や並行輸入品を
  日本国内で使用する場合も同様に、罰せられる場合があります。

⚠注意

- 禁止 乳幼児の手の届く場所では使わない
  やけど、ケガまたは感電の原因となります。
- 静電気注意
  コネクタや電源プラグの金属端子に触れたり、
  帯電したものを近づけますと故障の原因となります。
- 禁止 コードを持って抜かない
  コードを無理に曲げたり、引っ張ると、
  コードや機器本体の破損の原因となります。
- 禁止 振動が発生する場所では使用しない
  故障の原因となります。
- 付属品の使用は取扱説明書に従う
  本製品の付属品は、取扱説明書に従い、
  他の製品に使用しないでください。機器の破損の原因となります。
- 禁止 破損したまま使用しない
  火災、やけどまたはけがの原因となります。
- 禁止 ぐらついた台の上や傾いた場所などの
  不安定な場所や高所には置かない
  落下して、けがなどの原因となります。
- 禁止 子供が使用する場合は、保護者が取扱いの方法を教え、
  誤った使い方をさせない
  けがや故障などの原因となります。
- 本製品を長時間連続使用する場合は、
  温度が高くなることがあるため、注意する。
  また、使用中に眠ってしまうなどして、
  意図せず長時間触れることがないようにする
  温度の高い部分に直接長時間触れると
  お客様の体質や体調によっては肌の赤みや
  かゆみ、かぶれ、低温やけどの原因となります。
- 禁止 コンセントにつないだ状態で、ACアダプタや
  電源コンセントに長時間触れない
  やけど、感電の原因となります。
- 一般の電話機やコードレス電話、テレビ、ラジオなどを
  お使いになっている近くで使用しない
  近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、
  なるべく離れた場所で使用してください。
- 禁止 D-Linkが指定したオプション品がある場合は、
  指定オプションを使用する
  不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。
この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を逃がしてください。
さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。
http://www.dlink-jp.com/support/product-assurance-provision

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。
http://www.dlink-jp.com/support

目次

はじめに

DES-3200 シリーズユーザマニュアルは、本スイッチのインストールおよび操作方法を例題と共に記述しています。

第 1 章 本製品のご使用にあたって
- 本スイッチの概要とその機能について説明します。また、前面、背面、側面の各パネルと LED 表示について説明します。

第 2 章 スイッチの設置
- システムの基本的な設置方法について説明します。また、本スイッチの電源接続の方法についても紹介します。

第 3 章 スイッチの接続
- スイッチをご使用のネットワークに接続する方法を説明します。

第 4 章 スイッチの管理
- パスワード設定、SNMP 設定、および各種デバイスからの本スイッチへの接続など基本的なスイッチの管理について説明します。

第 5 章 Web ベースのスイッチ設定
- Web ベースの管理機能への接続方法および使用方法について説明します。

第 6 章 System Configuration（スイッチの主な設定）
- デバイス情報、ポート設定、ユーザアカウント、システムログ設定、時刻設定、シリアルポートなどの基本機能の設定について説明します。

第 7 章 Management（スイッチの管理）
- IP インタフェース設定、ARP 設定、シングル IP マネジメント設定、SNMP 設定、Telnet 設定、Web 設定などの管理機能について説明します。

第 8 章 L2 Features（L2 機能の設定）
- VLAN、トランキング、スパニングツリー、フォワーディング、フィルタリング、ERPS、LLDP などのレイヤ 2 機能について説明します。

第 9 章 L3 Features（レイヤ 3 機能の設定）
- スタティック / デフォルトルート設定などのレイヤ 3 機能について説明します。

第 10 章 QoS（QoS 機能の設定）
- 帯域制御、QoS スケジューリング、802.1p プライオリティ設定、トラフィックコントロールなどの QoS 機能について説明します。

第 11 章 ACL（ACL 機能の設定）
- アクセスプロファイルテーブルや CPU インタフェースフィルタリングなどの ACL（アクセスコントロールリスト）機能、フローベースのコントロールについて説明します。

第 12 章 Security（セキュリティ機能の設定）
- 802.1X、トラストホスト、アクセス認証コントロール、ポートセキュリティ、トラフィックセグメンテーション、SSL、SSH、IP-MAC- ポートバインディング、MAC ベースアクセスコントロールおよびセーフガードエンジンなどのセキュリティ機能について説明します。

第 13 章 Network Application（ネットワークアプリケーション）
- DHCP 設定、SMTP 設定、SNTP などのネットワークアプリケーション機能について説明します。

第 14 章 OAM（Object Access Method : オブジェクトアクセス方式）
- CFM（接続性障害管理）、イーサネット OAM、ケーブル診断機能機能について説明します。

第 15 章 Monitoring（スイッチのモニタリング）
- CPU 使用率、パケット統計情報、ミラーリング、Ping、トレースルートなどのモニタ機能について説明します。

第 16 章 スイッチメンテナンス
- リセット、システムの再起動、変更の保存について説明します。

付録 A ケーブルとコネクタ
- RJ-45 コンセント / コネクタ、ストレート / クロスオーバケーブルの標準的なピンの配置について説明します。

付録 B ケーブル長
- ケーブルの種類と最大ケーブル長についての情報を示します。

付録 C ログエントリ
- スイッチのシステムログに表示される可能性のあるログエントリとそれらの意味について説明します。

付録 D トラップログ
- スイッチで検出されるのトラップログについて記載しています。

付録 E RADIUS 属性の割り当て
- Ingress/Egress 帯域、802.1p デフォルトプライオリティ、VLAN、および ACL の RADIUS 属性の割り当てについて説明します。

付録 F パスワードのリカバリ手順
- スイッチのパスワードのリセット方法について説明します。

付録 G 用語解説
- 本マニュアルに使用される用語の定義を示します。

本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "（13 ページ）をご参照ください。
`courier` フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
`courier` 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
`courier` 斜体	コマンドパラメータ（可変または固定）。	*`value`*
< >	可変パラメータ。< > にあたる箇所に値または文字を入力します。	<*`value`*>
[ ]	任意の固定パラメータ。	[*`value`*]
[< >]	任意の可変パラメータ。	[<*`value`*>]
{ }	{ } 内の選択肢から 1 つ選択して入力するパラメータ。	{*`choice1`* | *`choice2`*}
|（垂直線）	相互排他的なパラメータ。	*`choice1`* | *`choice2`*
[{ }]	任意のパラメータで、指定する場合はどちらかを選択します。	[{*`choice1`* | *`choice2`*}]

第 1 章　本製品のご利用にあたって

本スイッチについて

DES-3200 スイッチは D-Link スイッチファミリーの製品です。本シリーズは、高性能、フォルトトレランス、スケーラブルな柔軟性、強健なセキュリティ、標準規格に準拠した相互運用性、および非常に高い技術をサポートしており、将来的な部門ネットワークおよびエンタプライズネットワーク構築への移行も簡単に行うことができます。

本マニュアルでは、D-Link DES-3200 シリーズの設置、設定、およびメンテナンスの方法について記述しています。これらのスイッチの基本的なハードウェア構成は似ており、設定方法、操作性はほぼ共通です。また、本マニュアル内の記載事項の多くが本スイッチシリーズで共通です。Web 画面は、シリーズの中の一製品を例にとって説明していますが、ポート数を除き設定方法は同じです。本マニュアル中の説明では主として DES-3200-28P の画面と設定を例題として使用しています。

サポートする機能

- L2 機能
  - IGMP スヌーピング※1：v1/v2/v3、スヌーピンググループ数：1K、IGMP Fast Leave、VLAN 毎の IGMP、IGMP 認証、IGMP フィルタリング
  - MLD スヌーピング※1：v1/v2、スヌーピンググループ数：1K、VLAN 毎の MLD、MLD Fast Leave
  - スパニングツリー：IEEE 802.1D STP、IEEE 802.1w RSTP、IEEE 802.1s MSTP、BPDU フィルタリング、ルートガード
  - ループバック検知（STP 無し）
  - ポートトランキング：IEEE 802.3ad/IEEE 802.1ax/ スタティック
    DES-3200-10/T：5 グループ / デバイス、8 ポート / グループ
    DES-3200-18/T：9 グループ / デバイス、8 ポート / グループ
    DES-3200-26/T：13 グループ / デバイス、8 ポート / グループ
    DES-3200-28/T、28F：14 グループ / デバイス、8 ポート / グループ
    DES-3200-28P：14 グループ / デバイス、8 ポート / グループ
    DES-3200-52/T、52P：26 グループ / デバイス、8 ポート / グループ
  - ポートミラーリング：1 ポート対 1 ポート / 多対 1 ポート /ACL モード
  - L2 プロトコルトンネリング：GVRP/STP
  - E-RPS（ITU-T G.8032 イーサネットリング）
  - ジャンボフレーム：12KByte
- VLAN
  - IEEE802.1Q タグ VLAN、IEEE 802.1v プロトコルベース VLAN、ポートベース VLAN、MAC ベース VLAN：1K エントリ
  - VLAN グループ数：4094（スタティック）/255（ダイナミック VLAN）、VLAN ID レンジ：1-4094
  - GVRP、ダブル VLAN：Port-based Q in Q、Selective Q in Q
  - ISM VLAN、VLAN トランスレーション
- L3 機能
  - Gratuitous ARP
- QoS
  - 帯域制御
  - キューの数：8 レベル / ポート
  - キューのスケジューリング：WRR（重み付けラウンドロビン）、Strict、Strict+WRR、
  - CoS：IEEE802.1p プライオリティ、VLAN ID、MAC アドレス、Ether タイプ、IPv4/IPv6 アドレス、TOS、DSCP、プロトコルタイプ、TCP/UDP ポート、IPv6 トラフィッククラス、IPv6 フローラベル、ユーザ定義パケット、
  - QoS フローアクション：802.1p プライオリティリマーク、ToS/DSCP リマーク、帯域制御
  - CIR（trTCM、srTCM）、タイムベース QoS
- ACL（アクセスコントロールリスト）
  - 最大 4 プロファイル、256 ルール / プロファイル
  - ACL 定義パラメータ：VLAN ID、IEEE 802.1p プライオリティ、MAC アドレス、Ether タイプ、IPv4/v6 アドレス、DSCP、プロトコルタイプ、TCP/UDP ポート、ユーザ定義パケット、IPv6 トラフィッククラス、IPv6 フローラベル
  - タイムベース ACL、ACL 統計、
  - CPU インタフェースフィルタリング：5 プロファイル、100 ルール / プロファイル

- セキュリティ
  - SSHv2、SSLv3 管理アクセス認証用：ローカル /RADIUS/TACACS/XTACACS/TACACS+、ユーザ認証用：ローカル /RADIUS
  - RADIUS アカウンティング：管理アクセス /802.1X
  - IEEE 802.1X 認証：ポート / ホストベース認証、MAC アドレス認証、ゲスト / ダイナミック VLAN
  - Microsoft®NAP 検疫対応：NAP-802.1X 方式 /NAP-DHCP 方式
  - 認証 DB フェイルオーバ：802.1X/MAC、認証バイパス機能
  - ブロードキャスト / マルチキャストストームコントロール、トラフィックセグメンテーション
  - IP-MAC ポートバインディング：ARP モード /ACL モード /DHCP スヌーピングモード
  - ポートセキュリティ：3328MAC/ デバイス、BPDU アタック防止、ARP スプーフィング防止
  - NetBIOS/NetBEUI フィルタリング、DoS 攻撃防御、DHCP クライアントフィルタリング
  - DHCP サーバスクリーニング、D-Link セーフガードエンジン
- マネージメント
  - 4 レベルのユーザアカウント権限
  - LLDP、Web ベース GUI、CLI
  - ZMODEM、Telnet サーバ、Telnet クライアント
  - SNMPv1/v2c/v3、SNMP トラップ
  - RMONv1：4 グループ
  - RMONv2：プルーブコンフィググループ
  - PPPoE Circuit-ID、トラストホスト
  - DHCP 自動設定、DHCP/BOOTP クライアント
  - DHCP リレー：オプション 82
  - Syslog
  - TFTP クライアント、FTP クライアント、SNTP クライアント
  - show tech-support コマンド、SMTP クライアント
  - パスワードリカバリ、パスワードの暗号化、複数設定ファイル、複数イメージ、フラッシュファイルシステム
  - IPv6 Neighbor Discovery（ND）、ループバック診断、ケーブル診断、802.3ah、片方向リンク検知（DULD）
  - CFM（Connectivity Fault Management）
  - NLB：ユニキャスト / マルチキャストモード
  - CPU モニタリング、メモリモニタリング、ポートステータスモニタリング、デバイスステータスモニタリング、トラフィックモニタリング、スイッチパフォーマンスモニタリング、DDM
- 以下の MIB のサポート
  - MIB II（RFC1213）
  - MIB Traps Convention（RFC1215）
  - Bridge MIB（RFC4188）
  - SNMP MIB（RFC1157, 2571-2576）
  - SNMPv2 MIB（RFC1901-1908, 1442, 2578）
  - RMON MIB（RFC271, 1757, 2819）
  - RMONv2 MIB（RFC2021）
  - Ether-like MIB（RFC1398, 1643, 1650, 2358, 2665, 3635）
  - 802.3 MAU MIB（RFC2668）
  - 802.1p MIB（RFC2674, 4363）
  - IF MIB（RFC2233, 2863）
  - RADIUS 認証クライアント MIB（RFC2618）
  - RADIUS アカウンティングクライアント MIB（RFC2620）
  - TCP MIB（RFC4022）
  - UDP MIB（RFC4113）
  - Ping MIB（RFC2925）
  - Traceroute MIB（RFC2925）
  - Trap MIB、IPv6 MIB（RFC2465）
  - ICMPv6 MIB（RFC2466）
  - Entity MIB（RFC2737）
  - IPv6 SNMP Mgmt Interface MIB（RFC4293）
  - DDM MIB
  - Private MIB
  - DIFFSERV MIB（RFC3289）
  - D-Link Zone Defense MIB

※1 Source フィルタ未サポート

ポート

DES-3200 シリーズスイッチはそれぞれ以下のポートを搭載しています。

型番	DES-3200-10/T	DES-3200-18/T	DES-3200-26/T	DES-3200-28/T	DES-3200-28F
10BASE-T/100BASE-TX ポート	8	16	24	24	—
10BASE-T/100BASE-TX/1000BASE-T ポート	1	1	2	2	4 （SFP とのコンボ）
SFP スロット	1	1	—	2	4
SFP スロット（100BASE-X のみ）	—	—	—	—	24
SFP コンボスロット	1	1	2	2	—
RJ-45 コンソールポート	1	1	1	1	1

型番	DES-3200-52/T	DES-3200-28P	DES-3200-52P
10BASE-T/100BASE-TX ポート	48	24（PoE 給電）	48（PoE 給電）
10BASE-T/100BASE-TX/1000BASE-T ポート	2	4	4
SFP スロット	2	—	—
SFP コンボスロット	2	2	2
RJ-45 コンソールポート	1	1	1

DES-3200 シリーズの各ポートタイプの特長および使用可能なオプションは次の通りです。

10BASE-T/100BASE-TX	SFP コンボ	1000BASE-T
• IEEE 802.3 • IEEE 802.3u • 全二重通信 • 全二重モード時の IEEE 802.3x フローコントロール	• IEEE 802.3z 対応 SFP トランシーバ : • DEM-210（100BASE-FX） • DEM-211（100BASE-FX） • DEM-220T/R（100BASE-BX-D/U、WDM） • DEM-310GT※1（1000BASE-LX） • DEM-311GT※1（1000BASE-SX） • DEM-312GT2※1（1000BASE-SX2） • DEM-314GT※1（1000BASE-LH） • DEM-315GT※1（1000BASE-ZX） • DEM-330T/R※1（1000BASE-BX-D/U、WDM） • DEM-331T/R※1（1000BASE-BX-D/U、WDM） • DGS-712※2（1000BASE-T）	• IEEE 802.3 • IEEE 802.3u • IEEE 802.3ab • 全二重通信 • 全二重モード時の IEEE 802.3x フローコントロール

※ 1 ：DES-3200-28F の SFP スロット（100M）には対応していません。

※ 2 ：SFP コンボスロットと DES-3200-28F の SFP スロット（100M）とには対応していません。

注意 SFP コンボポートは、対応する 1000BASE-T ポートと同時に使用することはできません。同時に使用すると（例 : SFP のポート 25 と 1000BASE-T のポート 25）、SFP ポートが優先となり 1000BASE-T ポートは使用不可能となります。

前面パネル

前面パネルには、Power、Console、およびオプションモジュール用の SFP ポートを含む各ポートの Link/Act の状態を表示する LED を搭載しています。「LED 表示」の項で詳細の動作について説明します。

DES-3200-10/T

- 10BASE-T/100BASE-TX ポート x 8
- 10BASE-T/100BASE-TX/1000BASE-T ポート x 1
- SFP スロット x 1
- SFP コンボスロット x 1
- RJ45 コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

図 3-1　DES-3200-10/T の前面パネル

DES-3200-18/T

- 10BASE-T/100BASE-TX ポート x 16
- 10BASE-T/100BASE-TX/1000BASE-T ポート x 1
- SFP スロット x 1
- SFP コンボスロット x 1
- RJ45 コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

図 3-2　DES-3200-18/T の前面パネル

DES-3200-26/T

- 10BASE-T/100BASE-TX ポート x 24
- 10BASE-T/100BASE-TX/1000BASE-T ポート x 2
- SFP コンボスロット x 2
- RJ45 コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

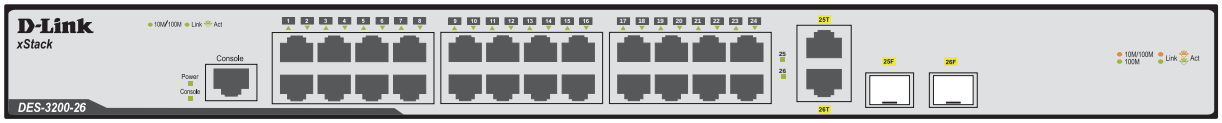


図 3-3　DES-3200-26/T の前面パネル

DES-3200-28/T

- 10BASE-T/100BASE-TX ポート x 24
- 10BASE-T/100BASE-TX/1000BASE-T ポート x 2
- SFP スロット x 2
- SFP コンボスロット x 2
- RJ45 コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

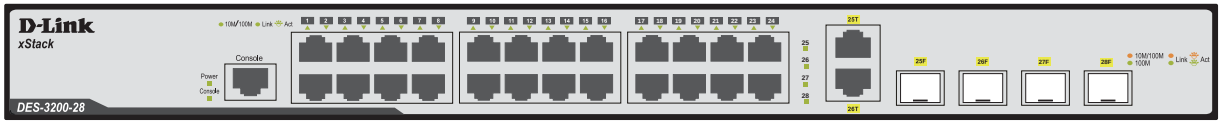


図 3-4　DES-3200-28/T の前面パネル

DES-3200-28F

- SFP スロット（100BASE-X のみ）x 24
- 10BASE-T/100BASE-TX/1000BASE-T コンボポート x 4
- SFP スロット x 4
- LED : Power、Console、Link/Act/Speed（各ポート）

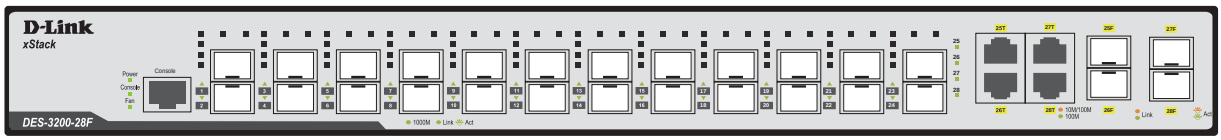


図 3-5　DES-3200-28F の前面パネル

DES-3200-28P

- 10BASE-T/100BASE-TX ポート x 24
- 10BASE-T/100BASE-TX/1000BASE-T ポート x 4
- SFP コンボスロット x 2
- RJ45 コンソールポート x 1
- LED : Power、Console、Fan、Link/PoE、Link/Act/Speed（各ポート）

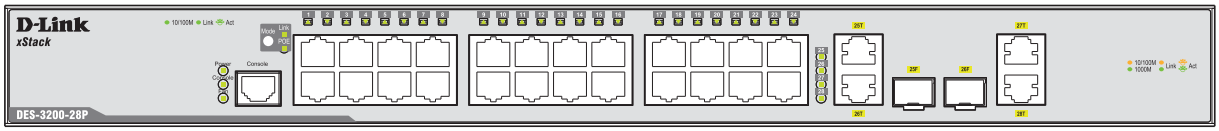


図 3-6　DES-3200-28P の前面パネル

DES-3200-52/T

- 10BASE-T/100BASE-TX ポート x 48
- 10BASE-T/100BASE-TX/1000BASE-T ポート x 2
- SFP スロット x 2
- SFP コンボスロット x 2
- RJ45 コンソールポート x 1
- LED : Power、Console、Fan、Link/Act/Speed（各ポート）

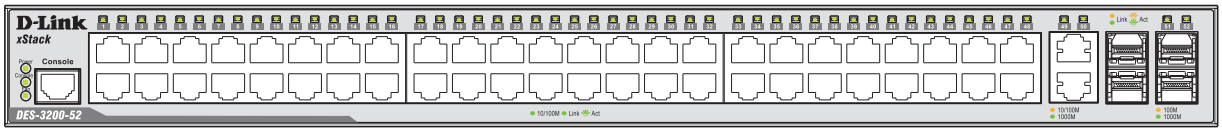


図 3-7　DES-3200-52/T の前面パネル

DES-3200-52P

- 10BASE-T/100BASE-TX ポート x 48
- 10BASE-T/100BASE-TX/1000BASE-T ポート x 4
- SFP コンボスロット x 2
- RJ45 コンソールポート x 1
- LED : Power、Console、Fan、Link/PoE、Link/Act/Speed（各ポート）

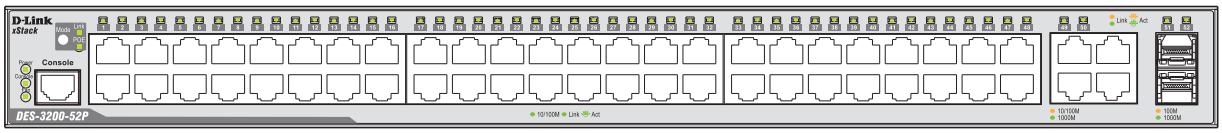


図 3-8　DES-3200-52P の前面パネル

LED 表示

DES-3200 シリーズスイッチは、Power、Console、および各ポートについて LED をサポートします。

DES-3200-10/T の LED

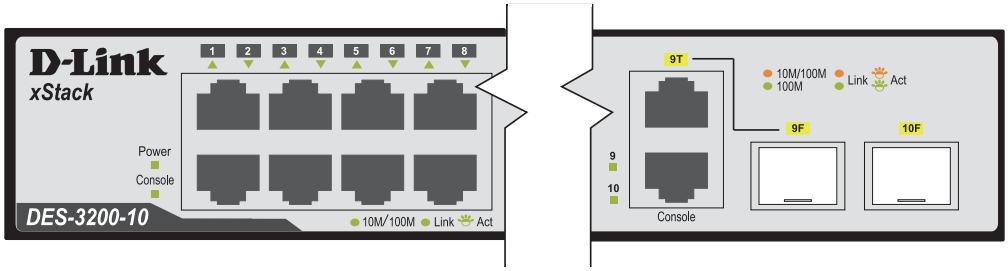


図 3-9　DES-3200-10/T の前面パネル LED 配置図

DES-3200-18/T の LED

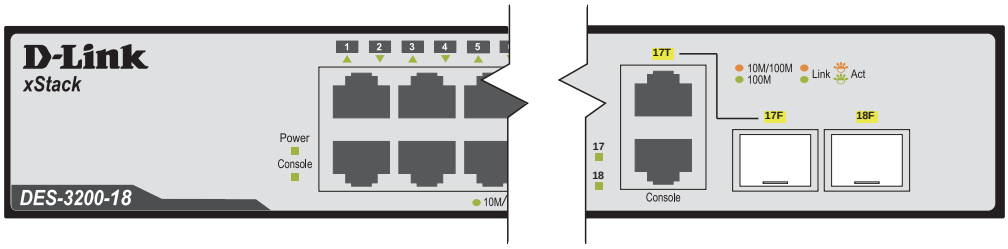


図 3-10　DES-3200-18/T の前面パネル LED 配置図

DES-3200-26/T の LED

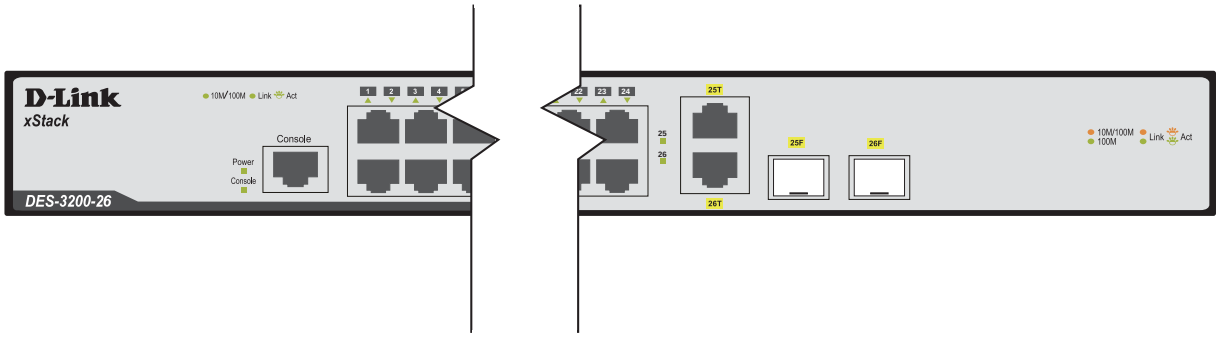


図 3-11　DES-3200-26/T の前面パネル LED 配置図

DES-3200-28/T の LED

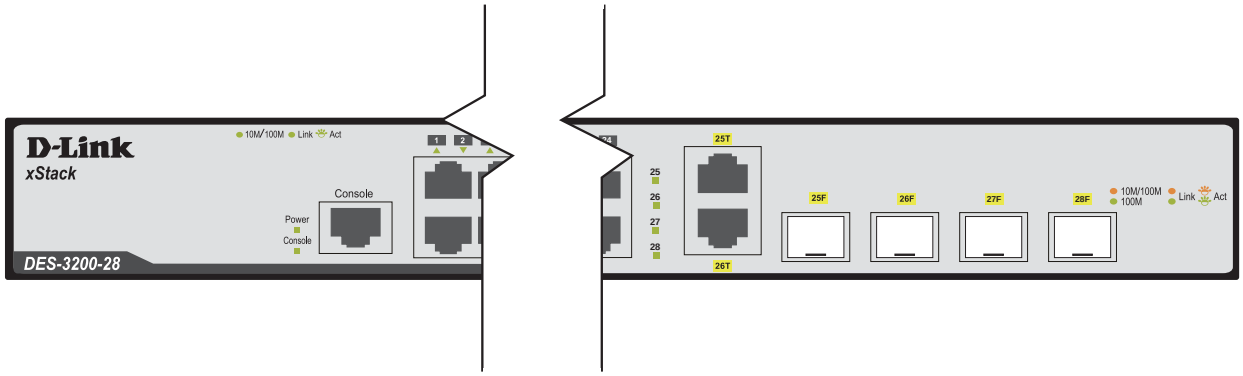


図 3-12　DES-3200-28/T の前面パネル LED 配置図

DES-3200-28F の LED

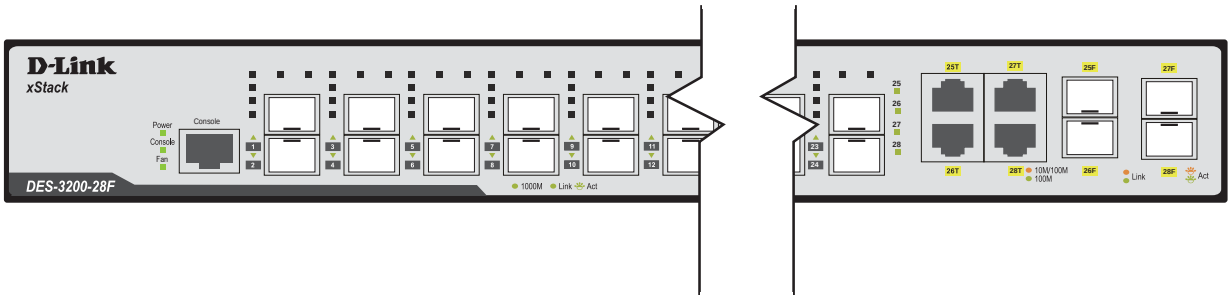


図 3-13　DES-3200-28F の前面パネル LED 配置図

DES-3200-28P の LED

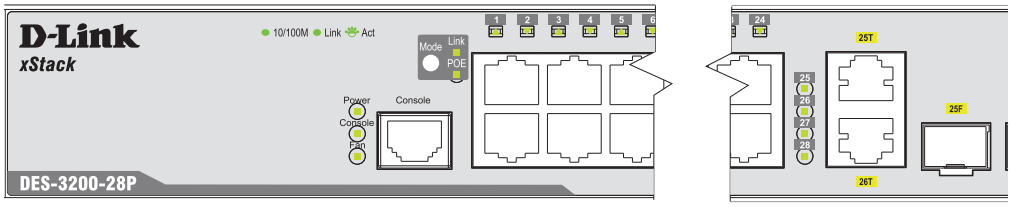


図 3-14　DES-3200-28P の前面パネル LED 配置図

DES-3200-52/T の LED

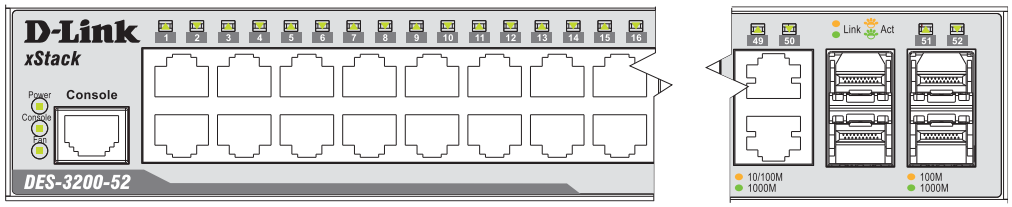


図 3-15　DES-3200-52/T の前面パネル LED 配置図

DES-3200-52P の LED

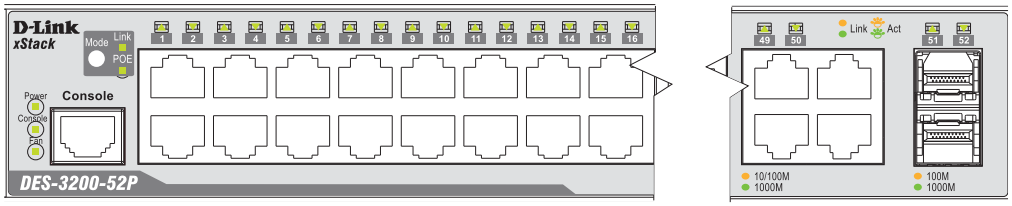


図 3-16　DES-3200-52P の前面パネル LED 配置図

DES-3200 スイッチシリーズに搭載している LED は以下の通りです。以下の表より、ご使用のスイッチに搭載の LED について確認ください。

LED	状態	色	状態説明
Power	点灯	緑	スイッチに電源が供給され正常に動作しています。
	消灯	ー	スイッチに電源が供給されていません。
Console	点滅	緑	電源投入後の Power ON Self Test（POST）中に点滅し、終了すると消灯します。
	点灯		コンソールポートのリンクが確立しています。
	消灯	ー	コンソールポートのリンクが確立していません。
Fan （DES-3200-28F/52T/28P/52P）	点滅	赤	ファンのいずれかが故障しています。
	消灯	ー	ファンは正常に動作しています。
Mode/Link (DES-3200-28P/52P)	点灯	緑	Link モードを選択中です。
Mode/PoE (DES-3200-28P/52P)	点灯	緑	PoE モードを選択中です。
10/100Mbps Copper ポート LED	ポート左上の LED は上段ポート、右上の LED は下段ポートの状態を表示します。		
	点灯	緑	10/100Mbps でリンクが確立しています。
	点滅		10/100Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。

LED	状態	色	状態説明
PoE モード 10/100Mbps ポート LED (DES-3200-28P/52P)	ポート左上の LED は上段ポート、右上の LED は下段ポートの状態を表示します。		
	点灯	緑	接続中の PoE 受電機器に給電中です。
	点滅		PoE ポートにエラーが発生しました。
	消灯	ー	給電をしていません。（受電機器が未検出または未接続）
SFP ポート LED	ポート左上の LED は上段ポート、右上の LED は下段ポートの状態を表示します。		
	点灯	緑	1000Mbps でリンクが確立しています。
	点滅		1000Mbps でデータを送受信しています。
	点灯	橙	100Mbps でリンクが確立しています。
	点滅		100Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。
10/100/1000Mbps Copper ポート LED	ポート左上の LED は上段ポート、右上の LED は下段ポートの状態を表示します。		
	点灯	緑	1000Mbps でリンクが確立しています。
	点滅		1000Mbps でデータを送受信しています。
	点灯	橙	10/100Mbps でリンクが確立しています。
	点滅		10/100Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。
100M SFP ポート LED (DES-3200-28F)	点灯	緑	100Mbps でリンクが確立しています。
	点滅		100Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。

背面パネル

DES-3200 シリーズの背面パネルは次の通りです。

DES-3200-10/T

電源コネクタおよびアース線用端子が配備されています。

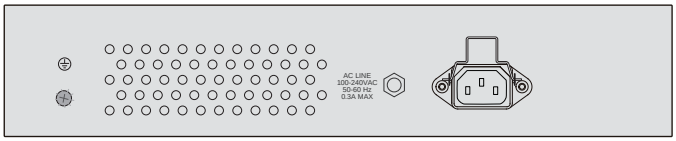


図 3-17　DES-3200-10/T の背面パネル図

DES-3200-18/T

電源コネクタ、セキュリティロックおよびアース線用端子が配備されています。

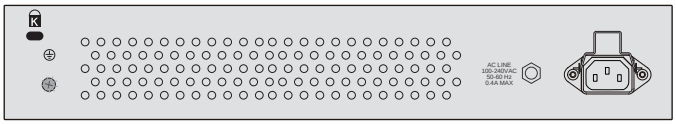


図 3-18　DES-3200-18/T の背面パネル図

DES-3200-26/T、DES-3200-28/T

電源コネクタおよびアース線用端子が配備されています。

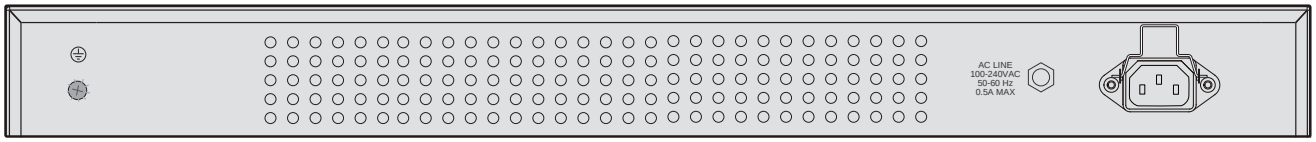


図 3-19　DES-3200-26/T、DES-3200-28/T の背面パネル図

DES-3200-28F

電源コネクタ、セキュリティロックおよびアース線用端子が配備されています。

図 3-20　DES-3200-28F の背面パネル図

DES-3200-28P

電源コネクタおよびアース線用端子が配備されています。

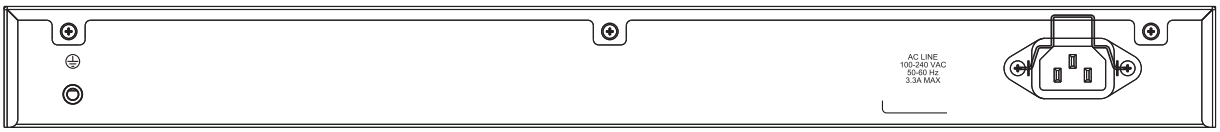


図 3-21　DES-3200-28P の背面パネル図

DES-3200-52/T

電源コネクタおよびアース線用端子が配備されています。

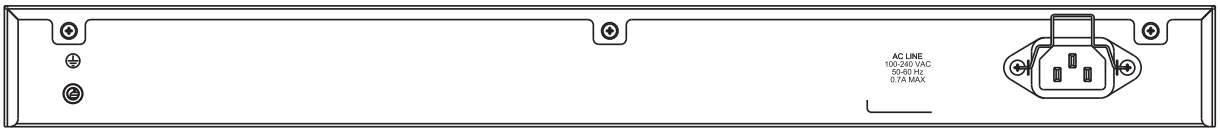


図 3-22　DES-3200-52/T の背面パネル図

DES-3200-52P

電源コネクタおよびアース線用端子が配備されています。

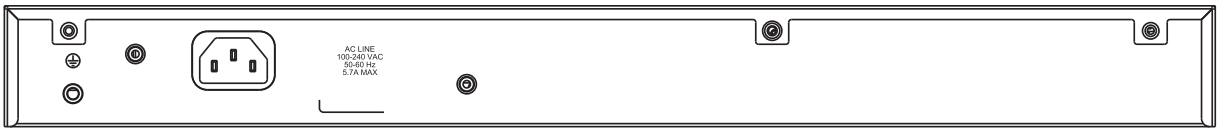


図 3-23　DES-3200-52P の背面パネル図

電源コネクタは標準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ～ 240VAC 内の電圧に調整されます。

側面パネル

システムのファンまたは通気口がスイッチの側面にあり内部の熱を放出します。これらをふさがないようにご注意ください。スイッチの適切な通気のためには、少なくとも 16cm 以上のスペースを確保してください。最適な熱放出、空気の循環をしないとシステム障害や部品の激しい損傷を引き起こす場合がありますのでご注意ください。

DES-3200-10/T、DES-3200-18/T

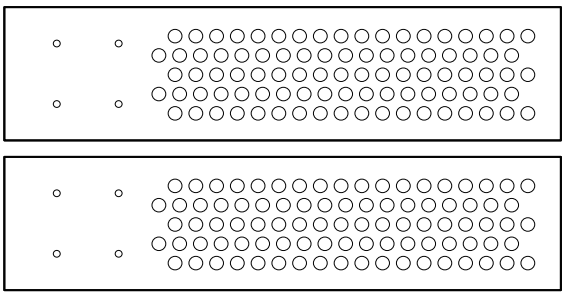


図 3-24　DES-3200-10/T、DES-3200-18/T の側面パネル図

DES-3200-26/T、DES-3200-28/T

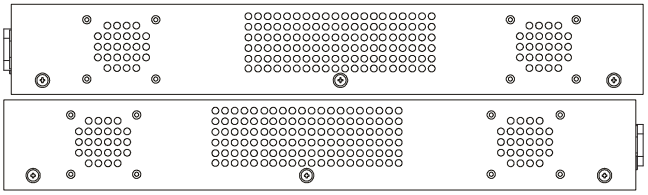


図 3-25　DES-3200-26/T、DES-3200-28/T の側面パネル図

DES-3200-28F

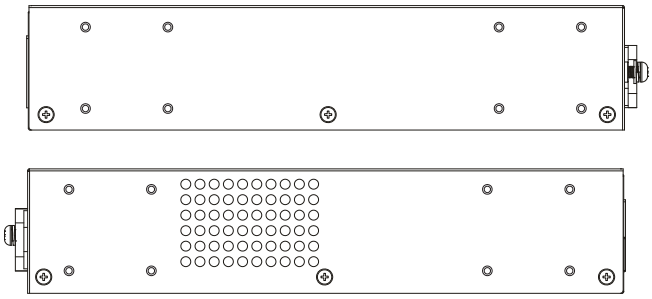


図 3-26　DES-3200-28F の側面パネル図

DES-3200-28P

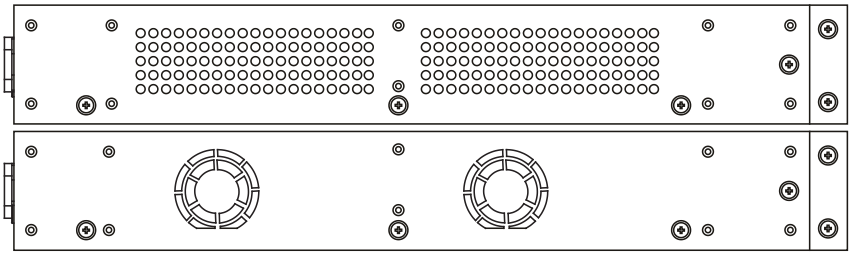


図 3-27　DES-3200-28P の側面パネル図

DES-3200-52/T

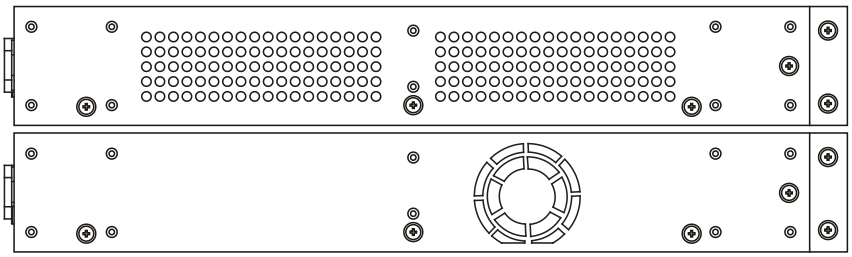


図 3-28　DES-3200-52/T の側面パネル図

DES-3200-52P

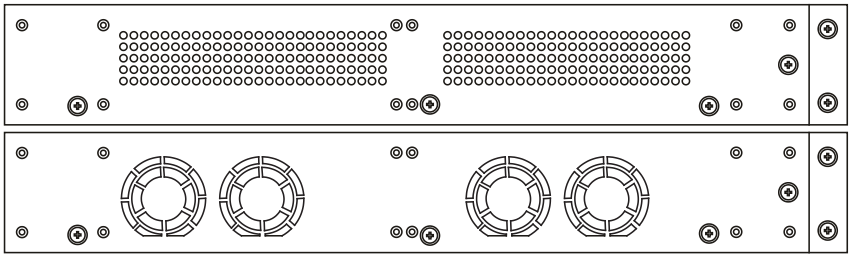


図 3-29　DES-3200-52P の側面パネル図

ギガビットコンボポート

DES-3200 シリーズスイッチは、スイッチの前面パネルに 1、2 または 4 つのギガビットイーサネットコンボポートを装備しています。これらのポートは 1000BASE-T ポートと SFP ポート（オプション）の兼用ポートです。また、DES-3200-28P/52P はそれぞれ 24、48 個の PoE 給電ポートも搭載しています。以下に、スイッチに SFP ポートモジュールを挿入した図を示します。

注意 これらの前面パネルモジュールは同時に使用できますが、コンボポートの SFP ポートモジュール挿入時は 1000BASE-T ポートとしての使用はできません。SFP ポートが優先されます。

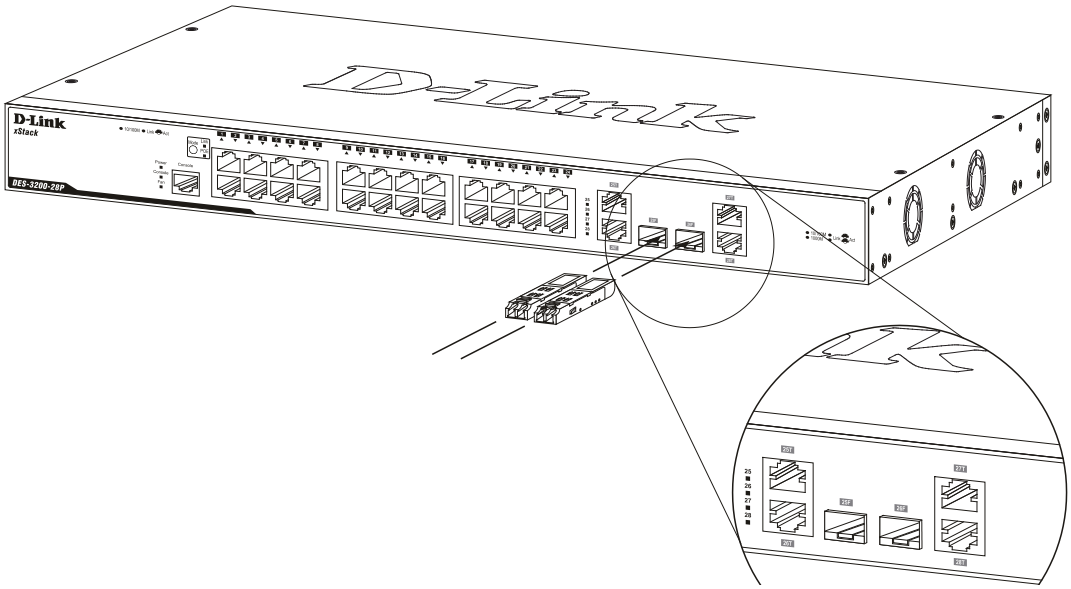


図 3-30　DES-3200 シリーズスイッチに光トランシーバを取り付ける

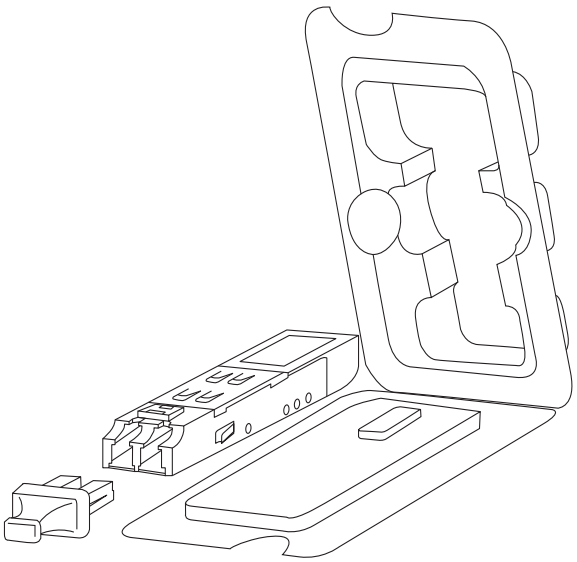


図 3-31　SFP モジュール図

第 2 章　スイッチの設置

パッケージの内容

ご購入いただいたスイッチの梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。

- 本体　x　1
- 電源ケーブル　x　1
- ラックマウントキット 1 式（ブラケット 2 枚、ネジ）
- 電源ケーブル抜け防止金具　x　1（DES-3200-52P を除く）
- ゴム足（貼り付けタイプ）　x　4
- CD-ROM
- RS-232C/RJ-45 コンソールケーブル
- クイックインストールガイド（英語版）
- 製品保証書
- シリアルラベル

万一、不足しているものや損傷を受けているものがありましたら、弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

ネットワーク接続前の準備

スイッチの設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

- スイッチは、しっかりとした水平面で耐荷重性のある場所に設置してください。
- スイッチの上に重いものを置かないでください。
- 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本スイッチの周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後 16cm 以上の空間を保つようにしてください。
- スイッチは動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- スイッチは強い電磁場が発生するような場所（モータの周囲など）や、振動、ほこり、および直射日光を避けて設置してください。
- スイッチを水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

ゴム足の取り付け（19 インチラックに設置しない場合）

机や棚の上に設置する場合は、まずスイッチに同梱されていたゴム製足をスイッチの裏面の四隅に取り付けます。スイッチの周囲に十分な通気を確保するようにしてください。

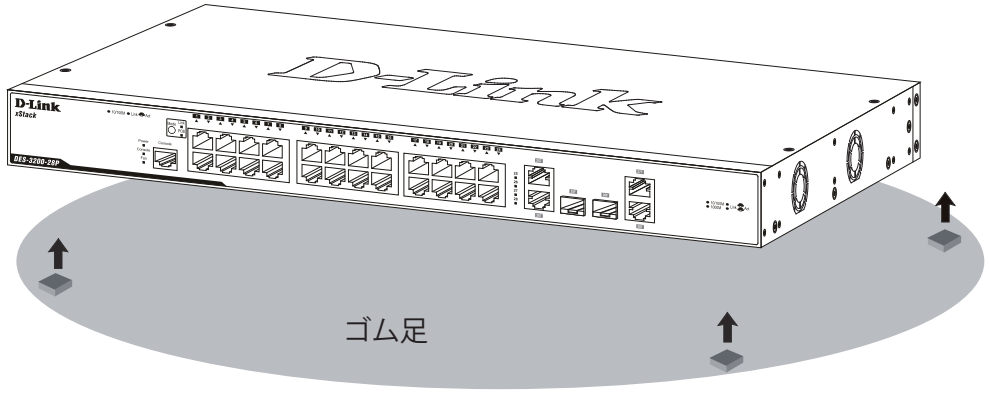


図 2-1　机や棚の上に設置する場合の準備図（DES-3200-28P）

19 インチラックへの取り付け

警告 前面、側面にスタビライザを取り付けないで製品を設置すると、ラックが転倒し、場合によっては人身事故を引き起こすことがあります。そのため、ラック内に製品を取り付ける前に必ずスタビライザを取り付けてください。ラックにシステム / コンポーネントを取り付けた後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つだけとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。

注意 スイッチをラックに固定するネジは付属品には含まれません。別途ご用意ください。

1. 電源ケーブルおよびケーブル類がシャーシ、拡張モジュールに接続していないことを確認します。
2. 付属のネジで、スイッチの両側側面にブラケットを取り付けます。

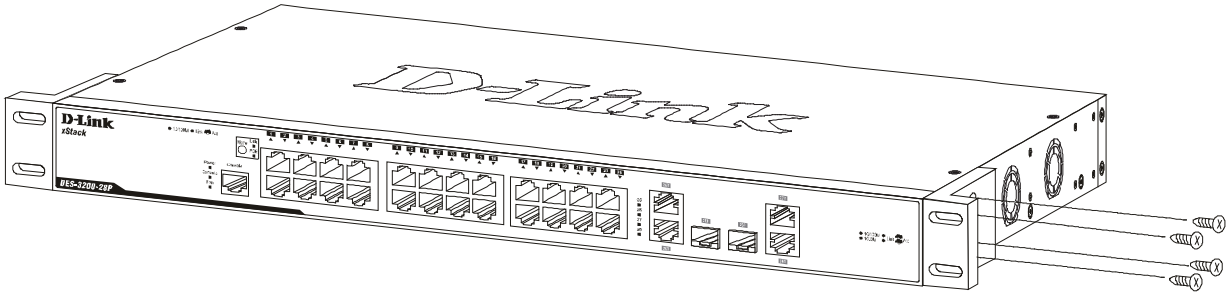


図 2-4　スイッチへのブラケットの取り付け図（DES-3200-28P）

3. 完全にブラケットが固定されていることを確認し、本スイッチを以下の通り標準の 19 インチラックに固定します。

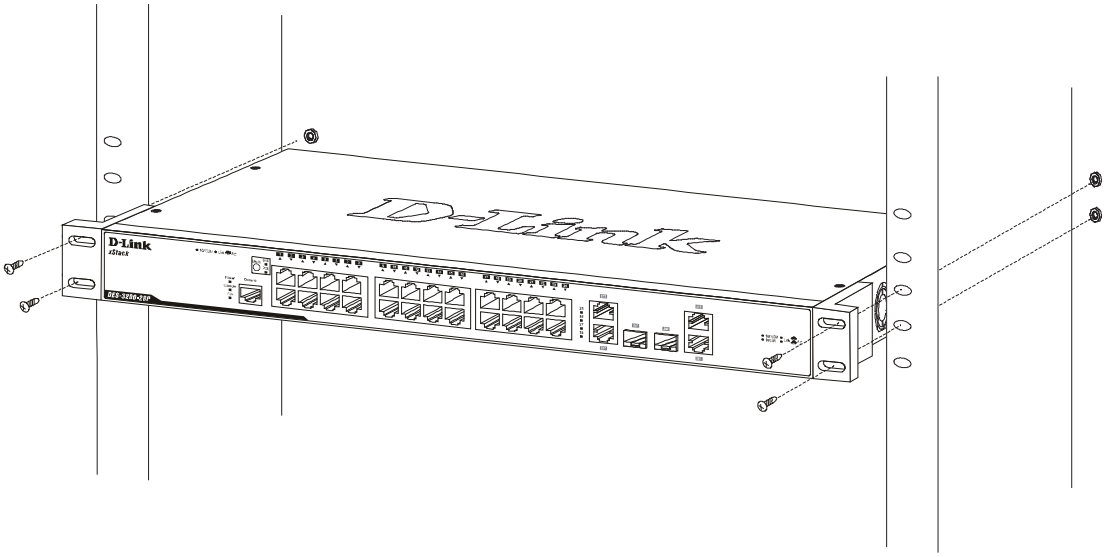


図 2-7　スイッチのラックへの設置図（DES-3200-28P）

電源の投入

1. 電源ケーブルを本スイッチの電源コネクタに接続し、電源ケーブルのプラグを電源コンセントに接続します。
2. 本スイッチに電源が供給されると、Power LED は点灯します。Console LED は点滅し、システムの設定が終了すると消灯します。

第 3 章　スイッチの接続

注意　すべてのポートは Auto MDI/MDI-X 接続をサポートしています。

エンドノードと接続する

本スイッチの 100BASE-TX または 1000BASE-T ポートとエンドノードをカテゴリ 3、4、5 の UTP ケーブルを使用して接続します。
エンドノードとは、RJ-45 コネクタ対応ネットワークインタフェースカードを装備した PC やルータを指しています。エンドノードとスイッチ間はカテゴリ 3、4、または 5 の UTP ケーブルで接続できます。エンドノードへの接続はスイッチ上のすべてのポートから行えます。

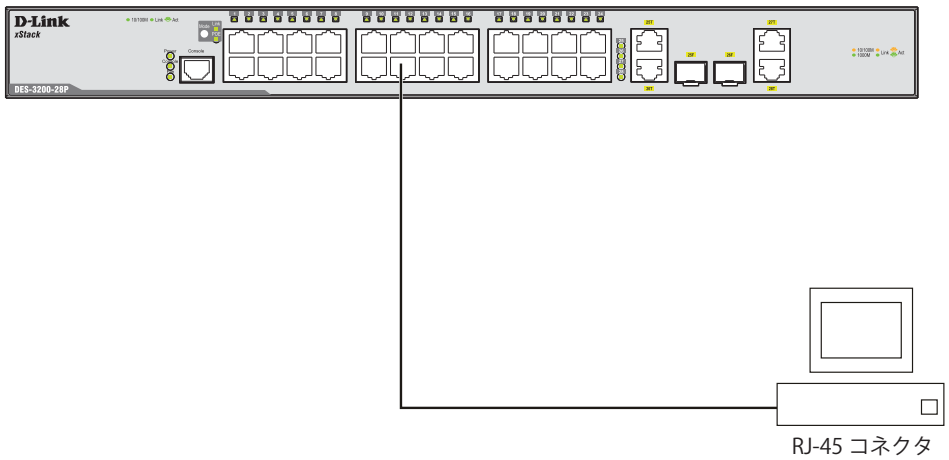


図 3-1　エンドノードと DES-3200-28P の接続図

エンドノードと正しくリンクが確立すると本スイッチの各ポートの LED は緑または橙に点灯します。データの送受信中は点滅します。

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- カテゴリ 3 以上の UTP ケーブル：10BASE-T ハブまたはスイッチと接続する。
- カテゴリ 5 以上の UTP ケーブル：100BASE-TX ハブまたはスイッチと接続する。
- エンハンスドカテゴリ 5 以上の UTP ケーブル：1000BASE-T スイッチと接続する。
- 光ファイバケーブル：SFP ポートを光ファイバネットワークに接続します。

ケーブル仕様については「付録 A ケーブルとコネクタ」（315 ページ）を参照してください。

スイッチとの接続例

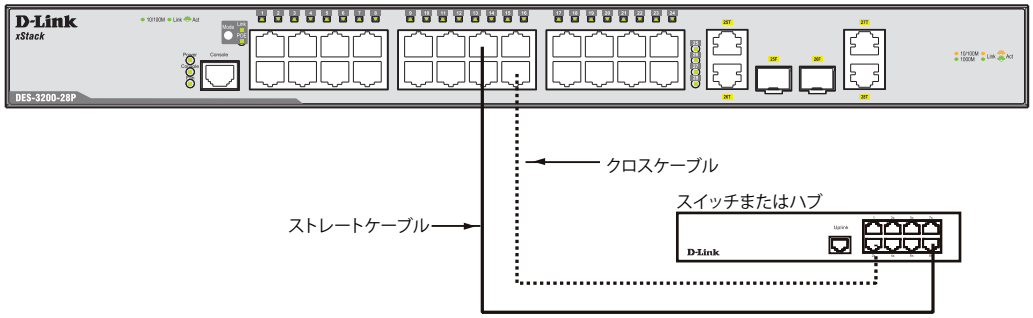


図 3-2　ストレート、クロスケーブルでスイッチ（DES-3200-28P）と接続する図

スイッチ構成例

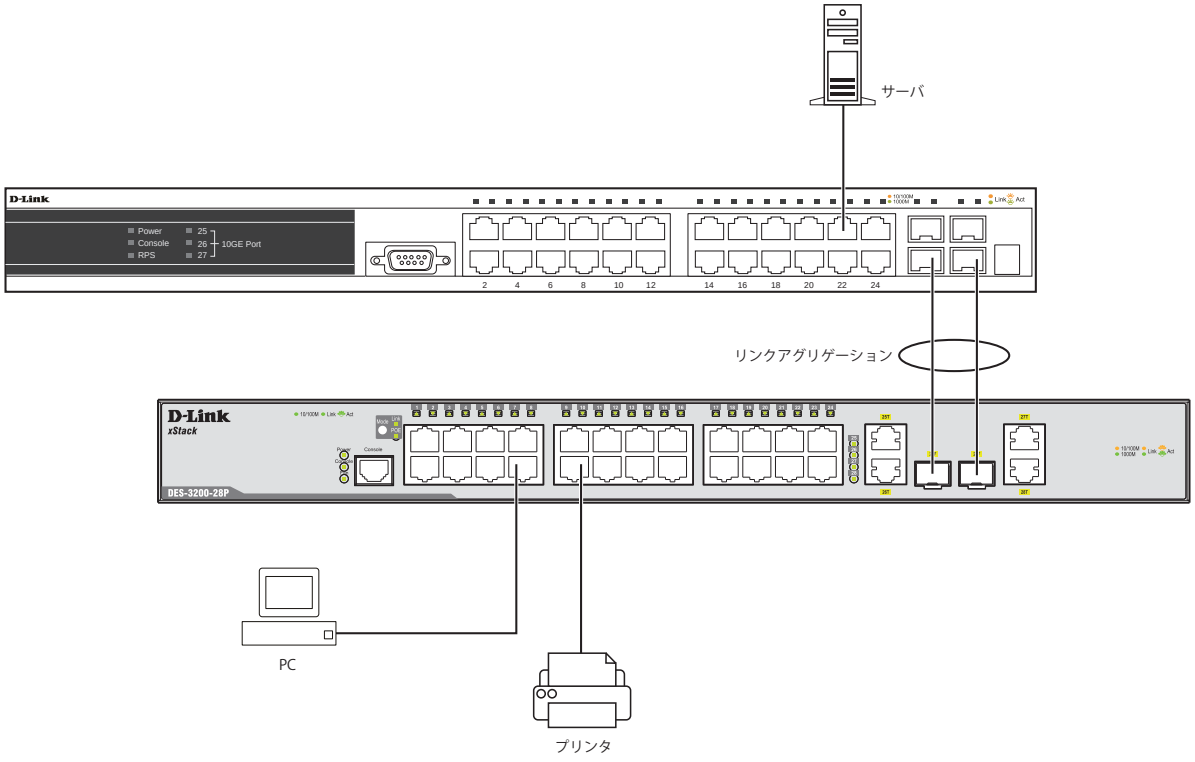


図 3-3　スイッチ構成例（DES-3200-28P）

注意　SFP トランシーバがリンクすると、対応するコンボ 10/100/1000BASE-T ポートは無効になります。

バックボーンまたはサーバと接続する

SFP ポートは、ネットワークバックボーンやサーバとのアップリンク接続に適しています。RJ-45 ポートは、全二重モード時において 10/100/1000Mbps の速度を提供し、SFP ポートは、全二重モード時において 1000Mbps の速度を提供します。
ギガビットイーサネットポートとの接続はポートのタイプによって光ファイバケーブルまたはエンハンスドカテゴリ 5 ケーブルを使用します。正しくリンクが確立すると Link LED が点灯します。

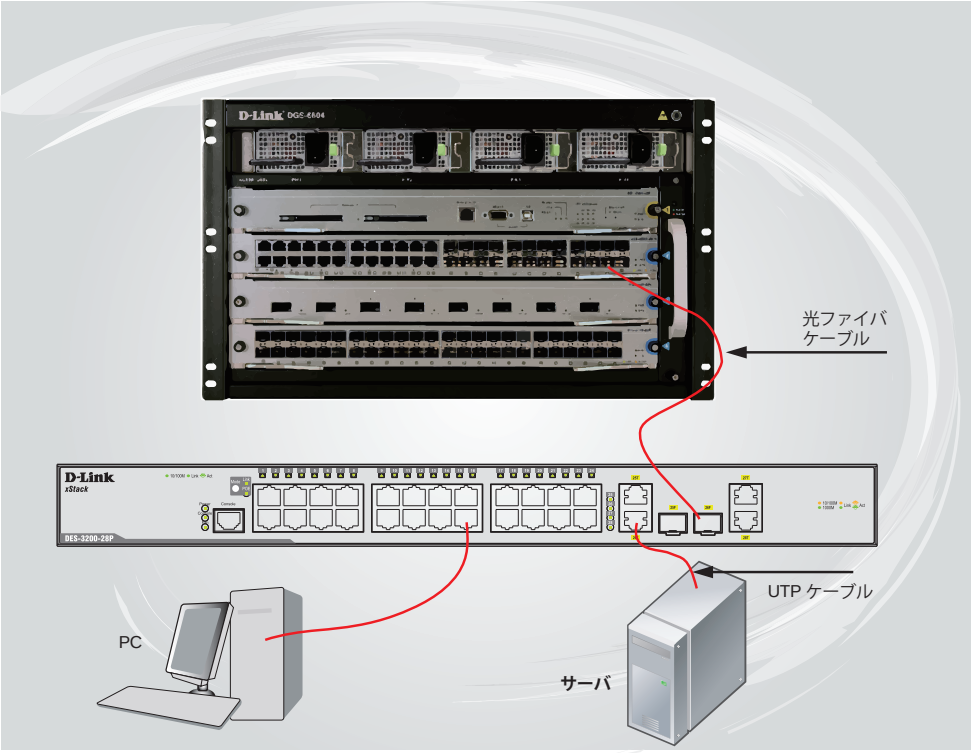


図 3-4　サーバ、PC、スイッチとのアップリンク接続図（DES-3200-28P）

第 4 章　スイッチ管理の導入

管理オプション

本システムはコンソールポートを経由した接続や Telnet を使用した接続を行い管理することができます。さらに Web ブラウザによっても管理することができます。

- Web ベースの管理インタフェース
  本スイッチの設置完了後、Firefox または Microsoft® Internet Explorer（バージョン 6.0 以降）などの Web ブラウザを使用してによって本スイッチの設定、LED のモニタ、および統計情報をグラフィカルに表示することができます。

- SNMP ベースの管理
  SNMP をサポートするコンソールプログラムでスイッチの管理をすることができます。本スイッチは SNMP v1、v2c、および v3 をサポートしています。SNMP エージェントは、受信した SNMP メッセージを復号化し、マネージャからの要求に対してデータベースに保存された MIB オブジェクトを参照して応答を返します。SNMP エージェントは MIB オブジェクトを更新し、統計情報およびカウンタ情報を生成します。

- シリアルポートまたはリモートの Telnet 経由によるコマンドラインインタフェース管理
  スイッチのモニタリングと設定のために RJ-45 シリアルポートを搭載しています。
  コンソールポートを使用するためには以下をご用意ください。

  - ターミナルソフトを操作するシリアルポート搭載の端末またはコンピュータ
  - 同梱のコンソールケーブル（D-Sub9 ピン オスコネクタ / RJ-45 コネクタ）を使用して接続します。

端末をコンソールポートに接続する

1. 本製品付属の RS-232C/RJ-45 コンソールケーブルの RJ-45 コネクタをスイッチの RJ-45 コンソールポートに接続します。
2. ケーブルのもう一方を端末またはターミナルソフトが動作するコンピュータのシリアルコネクタに接続します。以下の手順でターミナルソフトを設定します。
3. 「接続の設定」画面の「接続方法」で、適切なシリアルポート（COM ポート）を選択します。
4. 選択したポートの「プロパティ」画面で「115200」ビット / 秒にデータ速度を設定します。
5. 「データビット」は「8」、「ストップビット」は「1」、「パリティ」は「なし」に設定します。
6. 「フロー制御」は「なし」に設定します。
7. 「エミュレーションモード」を「VT100」に設定します。
8. 「ファンクションキー」、「方向キー」、「Ctrl キー」の使い方で「ターミナルキー」を選択します。「ターミナルキー」（Windows キーではない）の選択を確認します。

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 以降でないとハイパーターミナルの VT100 端末で矢印キーは使用できません。Windows 2000 Service Pack に関する情報はマイクロソフト社のホームページでご確認ください。

9. 端末設定の完了後、本スイッチに電源ケーブルを接続し、電源プラグをコンセントに接続します。端末でブートシーケンスが始まります。
10. ブートシーケンスが完了すると、コンソールのログイン画面が表示されます。
11. 購入後はじめてログインする場合は、ユーザ名（UserName）とパスワード（PassWord）プロンプトで Enter キーを押します。本スイッチには、ユーザ名（UserName）とパスワード（PassWord）の初期値はありません。はじめに、管理者によるユーザ名（UserName）とパスワード（PassWord）の作成が必要です。既にユーザアカウントを作成している場合は、ログインし、続けて本スイッチの設定をします。
12. コマンドを入力して設定を行います。コマンドの多くは管理者レベルのアクセス権が必要です。次のセクションでユーザアカウントの設定について説明します。CLI のすべてのコマンドリストおよび追加情報については、製品付属 CD-ROM に収録された「DES-3200 Series CLI Reference Guide」を参照してください。
13. 管理プログラムを終了する場合は、logout コマンド使用するか、ターミナルソフトを終了します。
14. 接続する端末または PC が以上の通り設定されたことを確認してください。

端末上で接続に問題が発生した場合は、ターミナルソフトの設定で「エミュレーション」が「VT-100」となっていることを確認してください。「エミュレーション」は「ハイパーターミナル」画面の「ファイル」メニューから「プロパティ」をクリックし、「設定」タブにて設定します。何も表示されない場合はスイッチの電源を切り再起動してください。

コンソールに接続すると、コンソール画面が表示されます。この画面上でコマンドを入力し、管理機能を実行します。ユーザ名とパスワードの入力プロンプトが表示されます。初回接続時はユーザ名とパスワードは設定されていないため、「Enter」キーを 2 度押して CLI に接続します。

スイッチへの初回接続

本スイッチは本スイッチへのアクセス権限のないユーザのアクセスや設定変更を防ぐセキュリティ機能をサポートしています。このセクションではコンソール接続で本スイッチにログインする方法を説明します。

注意 パスワードは大文字小文字を区別します。例えば、「S」と「s」は別の文字として認識されます。

スイッチに初めて接続すると、次のログイン画面が表示されます。

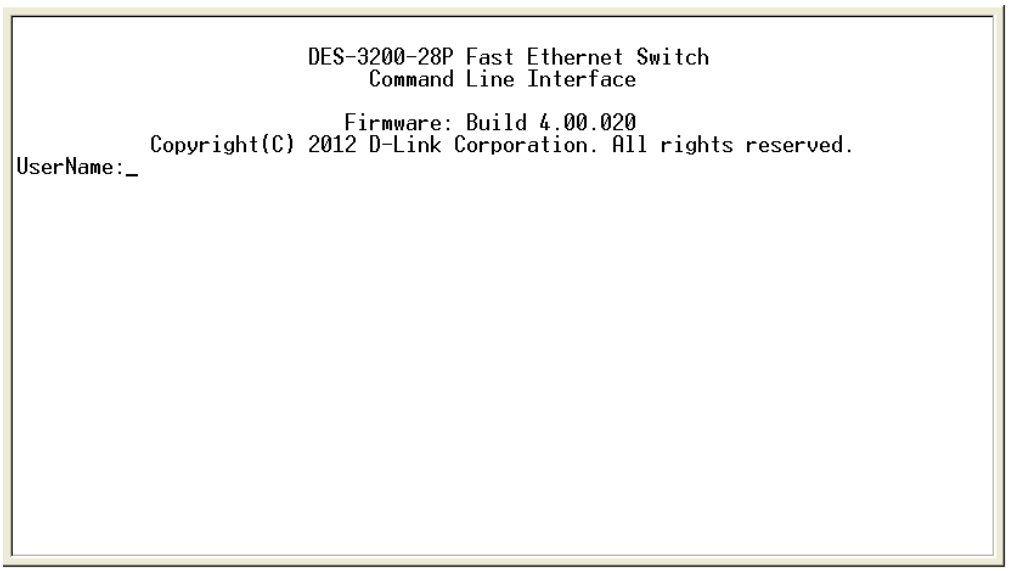


図 4-1　コマンドプロンプト

初回接続する場合、「UserName」または「PassWord」は登録されていません。「UserName」と「PassWord」には何も入力せず、「Enter」キーを押します。
既に設定されている場合は、「UserName」と「PassWord」の両方を入力します。
「DES-3200-xx:admin#」というコマンドプロンプトが表示されます。

注意 はじめにログインしたユーザが自動的に管理者権限を取得します。少なくとも一つは管理者レベルのユーザカウントを登録することをお勧めします。

パスワード設定

本スイッチは、初期値としてユーザ名およびパスワードの設定はありません。はじめにユーザアカウントの作成を行います。定義済みの管理者レベルのユーザ名でログインすることでスイッチ管理ソフトウェアに接続できます。
はじめてログインした際に本スイッチに対する不正アクセスを防ぐためにユーザ名に対して必ず新しいパスワードを定義してください。このパスワードは忘れないように記録しておいてください。
管理者レベルのアカウントを作成する手順は以下の通りです。

1. ログインプロンプトで「create account admin <user name>」を入力し、「Enter」キーを押下します。
2. パスワード入力プロンプトが表示されます。管理者アカウントに使用する <password> を入力し、「Enter」キーを押下します。
3. 確認のために再度同じ入力プロンプトが表示されます。同じパスワードを入力し、「Enter」キーを押下します。
4. 管理者アカウントが正しく登録されると、画面に「Success.」と表示されます。

注意 パスワードの大文字、小文字は区別されます。ユーザ名、パスワードのどちらも 15 文字以内の半角英数字を指定してください。

以下は新しい管理者レベルユーザに「newmanager」を指定する手順の例です。

```
DES-3200-28P:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:********
Enter the new password again for confirmation:********
Success.

DES-3200-28P:4#
```

注意 CLI 設定コマンドは動作中の設定だけが変更され、本スイッチを再起動するとその設定内容は消去されます。フラッシュメモリ（NV-RAM）にすべての変更内容を保存するためには「save」コマンドを投入して稼動中のコンフィグレーションファイルを、スタートアップ設定に格納する必要があります。

SNMP 設定

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルで、ネットワークデバイスの管理やモニタリングを行います。ネットワーク管理デバイスは、SNMP を利用してゲートウェイ、ルータ、そしてその他のネットワークデバイスの設定状態を確認または変更できます。SNMP を利用してスイッチやスイッチ群、またはネットワークに対し、正常な動作のためのシステム設定、パフォーマンスの監視、問題の検出を行います。

SNMP をサポートする管理デバイスは、デバイス上でローカルに動作する SNMP エージェントと呼ばれるソフトウェアを備えています。SNMP エージェントは管理オブジェクトの変数定義を保持し、デバイスの管理を行います。これら管理オブジェクトは MIB（Management Information Base）内に定義され、デバイスの SNMP エージェントにより管理される情報表示の基準を（管理側のデバイスに）伝えます。SNMP では、MIB（情報管理ベース）仕様形式およびネットワークを経由してこれらの情報にアクセスするために使用するプロトコルの両方を定義しています。

本スイッチは、SNMP のバージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）を実装しており、スイッチの監視と制御にどの SNMP バージョンを使用するかを指定します。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

SNMP バージョン 1 と 2 では、ユーザ認証において SNMP コミュニティ名をパスワードとして利用します。リモートユーザの SNMP アプリケーションとスイッチの SNMP は同じコミュニティ名を使用する必要があります。認証が行われていない SNMP パケットを受信した場合、そのパケットは無視（廃棄）されます。

SNMP バージョン 1 と 2 を使用するスイッチのデフォルトのコミュニティ名は、以下の 2 種類です。

- public -（ネットワークデバイス SNMP 管理ソフトに）MIB オブジェクトの読み取り権限が許可されているコミュニティ名です。
- private - MIB オブジェクトの読み取りと書き込みの権限を与えられているコミュニティ名です。

SNMP バージョン 3 では、2 つのパートで構成され、さらに高度な認証プロセスを採用しています。最初のパートは SNMP マネージャとして動作することができるユーザとその属性を掲載したリストを保持し、次のパートではリスト上のユーザの SNMP マネージャとしての権限を記載しています。

スイッチではユーザのグループをリストにまとめ、権限を設定できます。リスト上の SNMP マネージャのグループに対して、SNMP バージョン情報を登録可能です。そのため、SNMP マネージャを「SNMP バージョン 1 を使用して読み取り専用の情報とトラップの受信のみを可能にするグループ」や、「SNMP バージョン 3 を使用して高いセキュリティレベルを与え、読み書き可能にするグループ」など、グループごとに登録することができます。

個別のユーザや SNMP マネージャグループに SNMP バージョン 3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。そのような管理機能の可否は、各 MIB に関連付けられる OID（Object Identifier）を使用して定義します。SNMP バージョン 3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。スイッチでの SNMP バージョン 3 の設定方法については「System IP Address Settings（IP アドレス設定）」（63 ページ）をご参照ください。

トラップ

トラップとは、スイッチ上で発生したイベントを、ネットワーク管理者に警告するためのメッセージです。イベントには、再起動（誰かが誤ってスイッチの電源を切ってしまった）などの重大なものから、ポートの状態変化を知らせるものまで幅広い種類があります。スイッチはトラップを生成してトラップ受信者（またはネットワークマネージャ）に送信します。典型的なトラップには、認証の失敗、トポロジの変化、ブロードキャスト / マルチキャストストーム発生などがあります。

MIB

スイッチの MIB には管理情報およびカウンタ情報が格納されています。本スイッチは標準 MIB-II モジュールを使用し、MIB オブジェクトの値を SNMP ベースのネットワーク管理ソフトウェアにより取得します。本スイッチは、標準 MIB-II に加えて、拡張 MIB としてベンダ固有の MIB もサポートしています。MIB OID の指定によってもベンダ固有の MIB を取得することができます。MIB の値は読み取り専用、または読み書き可能なものがあります。

IP アドレスの割り当て

各スイッチに対して、SNMP ネットワークマネージャまたは他の TCP/IP アプリケーション（例 : BOOTP、TFTP）と通信するために IP アドレスを割り当てる必要があります。本スイッチの IP アドレスの初期値は 10.90.90.90 です。この IP アドレスはご使用のネットワークのアドレス計画に基づいて変更することができます。

また、本スイッチには、出荷時に固有の MAC アドレスが割り当てられており、この MAC アドレスは変更できません。MAC アドレスは、CLI で「show switch」コマンドを入力することにより、以下のように参照することができます。

```
DES-3200-28P:admin#show switch
Command: show switch

Device Type                : DES-3200-28P Fast Ethernet Switch
MAC Address                : 00-01-02-03-04-00
IP Address                 : 10.90.90.90 (Manual)
VLAN Name                  : default
Subnet Mask                : 255.0.0.0
Default Gateway            : 0.0.0.0
Boot PROM Version          : Build 4.00.001
Firmware Version           : Build 4.00.020
Hardware Version           : C1
System Name                :
System Location            :
System Uptime              : 0 days, 2 hours, 2 minutes, 28 seconds
System Contact             :
Spanning Tree              : Disabled
GVRP                       : Disabled
IGMP Snooping              : Disabled
MLD Snooping               : Disabled
VLAN Trunk                 : Disabled
Telnet                     : Enabled (TCP 23)
Web                        : Enabled (TCP 80)
SNMP                       : Enabled
SSL Status                 : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

図 4-2　show switch コマンドによる表示画面

本スイッチの MAC アドレスは、Web ベース管理インタフェースの「Device Information」および「System Information」画面にも表示されます。

本スイッチの IP アドレスは、Web ベース管理インタフェースの使用前に設定する必要があります。スイッチの IP アドレスは BOOTP または DHCP プロトコルを使用して自動的に取得することもできます。この場合は、スイッチに割り当てた本来のアドレスを知っておく必要があります。

IP アドレスはコンソールから CLI を使用して、以下のように設定することができます。

コマンドラインプロンプトの後に、以下のコマンドを入力します。

```
config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy
```

xxx.xxx.xxx.xxx は IP アドレスを示し、System と名づけた IP インタフェースに割り当てられます。**yyy.yyy.yyy.yyy** は対応するサブネットマスクを示しています。

または **config ipif System ipaddress xxx.xxx.xxx.xxx/z** と入力することもできます。**xxx.xxx.xxx.xxx** は IP インタフェースに割り当てられた IP アドレスを示し、**z** は CIDR 表記で対応するサブネット数を表します。

本スイッチ上の「System」という名前の IP インタフェースに IP アドレスとサブネットマスクを割り当てて、管理ステーションから本スイッチの Telnet または Web ベースの管理エージェントに接続します。

```
DES-3200-28P:admin#config ipif System ipaddress 10.90.90.91/255.0.0.0
Command: config ipif System ipaddress 10.90.90.91/8

Success.

DES-3200-28P:admin#
```

図 4-3　スイッチへの IP アドレス割り当て時の表示画面

上記例では、スイッチに IP アドレス「10.90.90.91」とサブネットマスク「255.0.0.0」を割り当てています。CIDR 表記（10.90.90.91/8）でのアドレス指定も可能です。「Success.」というメッセージにより、コマンドの実行が成功したことが確認できます。スイッチのアドレス設定が終了すると、Telnet での CLI、または Web ベースによる管理を開始することができます。

第 5 章　Web ベースのスイッチ管理

Web ベースの管理について

本スイッチのすべてのソフトウェア機能は、実装されている Web ベース (HTML) インタフェース経由で管理、設定およびモニタできます。標準的なブラウザを使用してネットワーク上のリモートステーションから本スイッチを管理できます。ブラウザが普遍的なアクセスツールの役割をし、HTTP プロトコルを使用してスイッチと直接通信することが可能です。

Web ベースの管理モジュールとコンソールプログラム（および Telnet）は、異なるインタフェースを経由して同じスイッチ内部のソフトウェアにアクセスし、その設定を行います。つまり、Web ベースでスイッチ管理を実行して行う設定は、コンソール接続によっても行うことができます。

Web マネージャへのログイン

スイッチの管理を行うには、はじめにコンピュータでブラウザを起動し、本スイッチに定義した IP アドレスを入力します。ブラウザのアドレスバーに以下のように URL を入力します。例 : http://10.90.90.90（10.90.90.90 はスイッチの IP アドレス。）

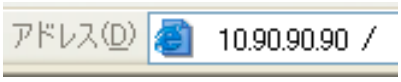


図 5-1　URL の入力

注意　工場出荷時設定では IP アドレス「10.90.90.90」、サブネットマスク「255.0.0.0」が設定されています。端末側の IP インタフェースを本スイッチにあわせるか、本スイッチを端末側の IP インタフェースにあわせてください。

以下のユーザ認証画面が表示されます。

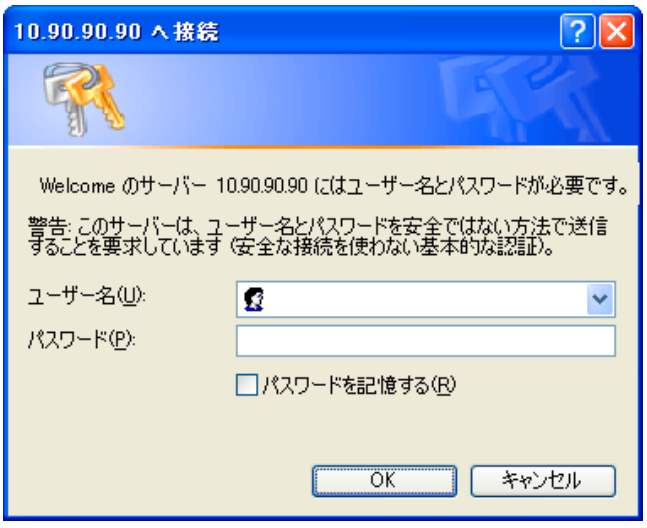


図 5-2　パスワード入力用画面

「ユーザー名」欄と「パスワード」欄を空白のまま「OK」をクリックし、Web ベースユーザインタフェースに接続します。Web ブラウザによって使用可能な機能を以下で説明します。
CLI でユーザ名、パスワードを既に設定している場合は、設定したパラメータを入力します。

Web マネージャの画面構成

Web マネージャによるスイッチの設定または管理画面にアクセス、およびパフォーマンス状況やシステム状態をグラフィック表示で参照できます。

Web マネージャのメイン画面について

Web マネージャのメイン画面は 3 つのエリアで構成されています。

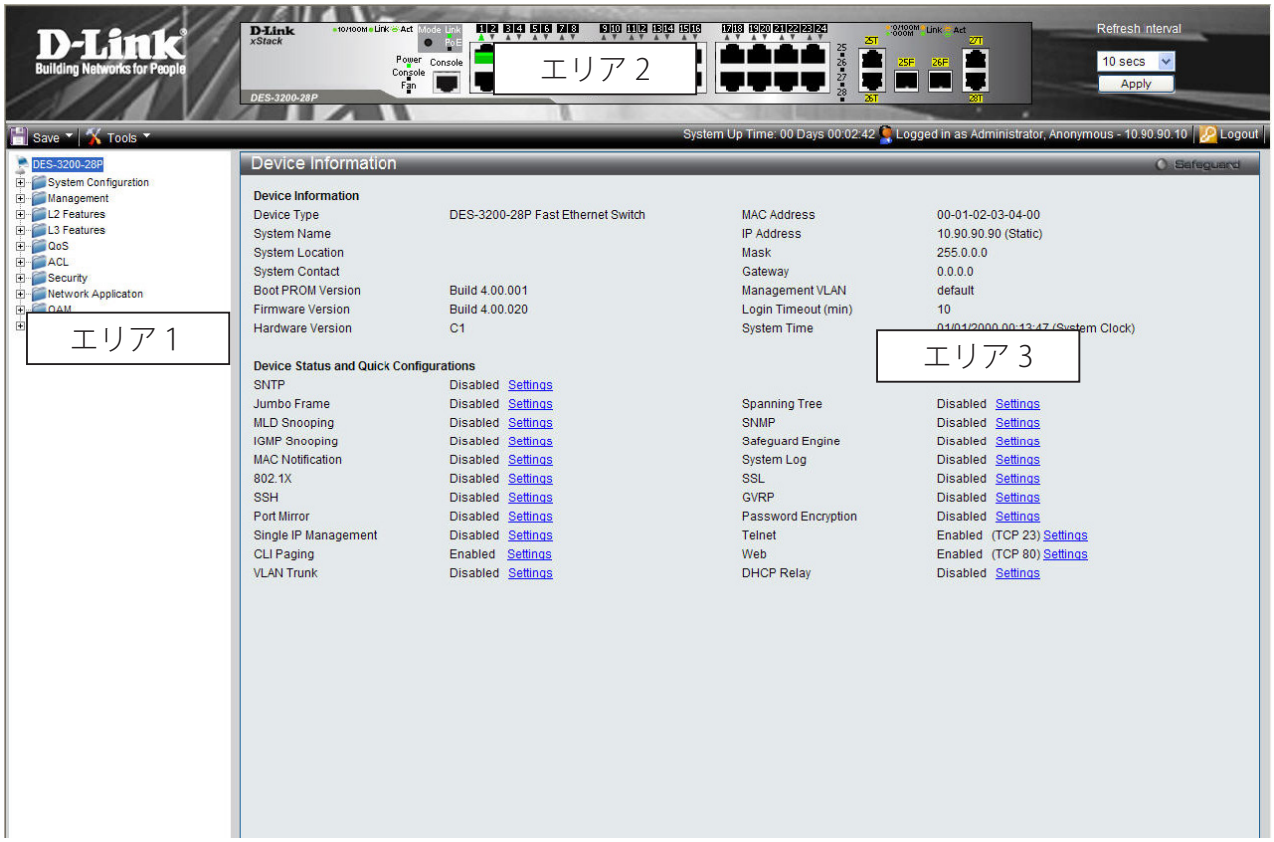


図 5-3　Web マネージャのメインページ

エリア	機能
エリア 1	表示するメニューまたは画面を選択します。フォルダアイコンを開き、ハイパーリンクしたメニューボタンの表示、および格納するサブフォルダの表示ができます。D-Link のロゴをクリックすると D-Link のホームページに接続します。
エリア 2	本スイッチの前面パネルをリアルタイムに近い画像で表示します。本エリアにはスイッチのポートや拡張モジュール、各ポートの状態、デュプレックスモード、フローコントロールの状態などが、指定したモードにより表示できます。
エリア 3	選択したスイッチ情報と設定データのエントリを表示します。

注意　現在のセッション中にスイッチのコンフィグレーションに行った変更は、「Save Configuration / Log」画面またはコマンドラインインタフェース (CLI) の「save」コマンドにて保存する必要があります。

Web マネージャのメニュー構成

Web マネージャで本スイッチに接続し、ログイン画面でユーザ名とパスワードを入力して本スイッチの管理モードにアクセスします。
Web マネージャで設定可能な機能を次に説明します。

メインメニュー	サブメニュー	説明	参照ページ
System Configuration	Device Information	スイッチの主な設定情報を表示します。	37
	System Information Settings	スイッチの基本情報を表示します。	39
	Port Configuration	ポート設定、ジャンボフレーム設定などを行います。: Port Settings、Port Description Settings、Port Error Disabled、Jumbo Frame	39
	PoE Configuration	PoE システムの設定を行います。: PoE System Settings、PoE Port Settings	43
	Serial Port Settings	ボーレートの値と自動ログアウト時間を調整します。	46
	Warning Temperature Settings	システムの警告温度パラメータを設定します。	46
	System Log Configuration	フラッシュメモリにスイッチのログを保存する方法、Syslog サーバの設定を行います。: System Log Settings、System Log Server Settings、System Log、System Log & Trap Settings、System Severity Settings	47
	Time Range Settings	アクセスプロファイル機能を実行する期間を決定します。	50
	Time Settings	スイッチに時刻を設定します。	50
	User Accounts Settings	ユーザおよびユーザの権限を設定します。	51
	Command Logging Settings	コマンドログ設定を有効または無効にします。	52
Management	ARP	スタティック ARP、ARP テーブルを設定します。: Static ARP Settings、ARP Table	54
	Gratuitous ARP	Gratuitous ARP の設定をします。: Gratuitous ARP Global Settings、Gratuitous ARP Settings	56
	IPv6 Neighbor Settings	IPv6 Neighbor の設定を行います。	58
	IP Interface	スイッチの IP インタフェース設定を行います。: System IP Address Settings、Interface Settings	59
	Management Settings	CLI ページング、DHCP 自動設定などの管理設定を行います。	63
	Session Table	スイッチが最後に起動してからの管理セッションを表示します。	63
	Single IP Management	シングル IP マネジメント機能を設定します。: Single IP Settings、Firmware Upgrade、Configuration File Backup/ Restore、Upload Log File	64
	SNMP Settings	SNMP 設定を行います。: SNMP Global Settings、SNMP Trap Settings、SNMP Link Change Traps Settings、SNMP View Table Settings、SNMP Community Table Settings、SNMP Group Table Settings、SNMP Engine ID Settings、SNMP User Table Settings、SNMP Host Table Settings、SNMP v6Host Table Settings、RMON Settings	73
	Telnet Settings	スイッチに Telnet 設定をします。	87
	Web Settings	スイッチに Web ステータスを設定します。	96
L2 Features	VLAN	802.1Q スタティック VLAN 設定を行います。: 802.1Q VLAN Settings、802.1v Protocol VLAN、GVRP、MAC-based VLAN Settings、PVID Auto Assign Settings、VLAN Trunk Settings、Browse VLAN、Show VLAN Ports	87
	QinQ	Q-in-Q 機能を有効または無効にします。: QinQ Settings、VLAN Translation Settings	96
	Layer 2 Protocol Tunneling Settings	レイヤ 2 プロトコルトンネリング機能を設定します。	99
	Spanning Tree	スパニングツリープロトコルの設定を行います。: STP Bridge Global Settings、STP Port Settings、MST Configuration Identification、STP Instance Settings、MSTP Port Information	100
	Link Aggregation	ポートトランキング設定を行います。: Port Trunking Settings 、LACP Port Settings	107
	FDB	スタティック FDB、MAC アドレスエージングタイム、MAC アドレステーブルなどを設定します。: Static FDB Settings、MAC Notification Settings、MAC Address Aging Time Settings、MAC Address Table、ARP & FDB Table	110
	L2 Multicast Control	IIGMP Snooping、MLD Snooping の設定を行います。: IGMP Snooping、MLD Snooping、IP Multicast VLAN Replication	115
	Multicast Filtering	マルチキャストフィルタリングの設定を行います。: IPv4 Multicast Filtering、IPv6 Multicast Filtering、Multicast Filtering Mode	133
	ERPS Settings	イーサネットリングプロテクション設定を有効にします。	145
	LLDP	LLDP 設定を行います。	144
	NLB FDB Settings	NLB 機能を設定します。	151

メインメニュー	サブメニュー	説明	参照ページ
L3 Features	IPv4 Static/Default Route Settings	IPv4 スタティック / デフォルトルートの設定を行います。	152
	IPv4 Route Table	IPv4 ルーティングテーブルの外部経路情報を参照します。	153
	IPv6 Static/Default Route Settings	IPv6 スタティック / デフォルトルートの設定を行います。	153
QoS	802.1p Settings	ポート単位にプライオリティを割り当てます。: 802.1p Default Priority Settings、802.1p User Priority Settings、802.1p Map Settings（802.1p マップ設定）	156
	Bandwidth Control	送信と受信のデータレートを制限します。: Bandwidth Control Settings、Queue Bandwidth Control Settings	158
	Traffic Control Settings	ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整します。	160
	DSCP	ポートの DSCP トラスト状態の設定および DSCP マッピング設定を行います。: DSCP Trust Settings、DSCP Map Settings	166
	Scheduling Settings	QoS スケジューリングを設定します。: QoS Scheduling、QoS Scheduling Mechanism	164
ACL	ACL Configuration Wizard	ウィザードを使用してアクセスプロファイルとルールを作成します。	166
	Access Profile List	パケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定するプロファイルを設定します。	168
	CPU Access Profile List	CPU インタフェースフィルタリング機能を設定します。	185
	ACL Finder	ACL エントリを検索します。	200
	ACL Flow Meter	フローごとの帯域幅制御設定を行います。	201
Security	802.1X	802.1X 認証を設定します。: 802.1X Global Settings、802.1X Port Settings、802.1X User Settings、Guest VLAN、Authenticator State、Authenticator Statistics、Authenticator Session Statistics、Authenticator Diagnostics、Initialize Port(s)、Reauthenticate Port(s)	206
	RADIUS	RADIUS サーバの設定を行います。: Authentication RADIUS Server Settings、RADIUS Accounting Setting、RADIUS Authentication、RADIUS Account Client	219
	IP-MAC-Port Binding	IP アドレス、MAC アドレスおよびポートを結合し、レイヤ間通信を行います。: IMPB Global Settings、IMPB Port Settings、IMPB Entry Settings、MAC Block List、DHCP Snooping	223
	MAC-based Access Control	MAC アドレス認証機能を設定します。: MAC-based Access Control Settings、MAC-based Access Control Local Settings、MAC-based Access Control Authentication State	228
	Compound Authentication	コンパウンド認証方式を設定します。	231
	Port Security	ダイナミックな MAC アドレス学習をロックします。: Port Security Settings、Port Security VLAN Settings、Port Security Entries	232
	ARP Spoofing Prevention Settings	パケットコンテンツ ACL を使用して、ARP スプーフィング攻撃を防止します。	235
	BPDU Attack Protection	ポートに BPDU 防止機能を設定します。	236
	Loopback Detection Settings	ループバック検知機能の設定を行います	237
	Traffic Segmentation Settings	ポートのトラフィックフローを制限します。	238
	NetBIOS Filtering Setting	NetBIOS フィルタ設定を行います。	239
	DHCP Server Screening	不正な DHCP サーバへのアクセスを拒否します。: DHCP Server Screening Port Settings、DHCP Offer Permit Entry Settings	240
	Access Authentication Control	TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。: Enable Admin、Authentication Policy Settings、Application Authentication Settings、Authentication Server Group Settings、Authentication Server Settings、Login Method Lists Settings、Enable Method Lists Settings、Local Enable Password Settings	242
	SSL Settings	証明書の設定、暗号スイートの設定を行います。	250
	SSH	SSH サーバ、SSH アルゴリズム、SSH ユーザ認証の設定を行います。: SSH Settings、SSH Authentication Method and Algorithm Settings、SSH User Authentication List	252
	Trusted Host Settings	リモートのスイッチ管理用トラストホストを設定します。	255
	Safeguard Engine Settings	セーフガードエンジンの設定を行います。	256
	DoS Attack Prevention Settings	各 DoS アタックに対して防御設定を行います。	258
	IGMP Access Control Settings	各ポートに IGMP 認証（IGMP アクセスコントロール）を設定します。	259

メインメニュー	サブメニュー	説明	参照ページ
Network Application	DHCP	DHCP リレーの設定を行います。: DHCP Relay、DHCP Local Relay Settings、DHCP Local Relay Option 82 Settings	260
	PPPoE Circuit ID Insertion Settings	PPPoE Circuit ID の挿入機能を設定します。	267
	SMTP Settings	問題が発生した場合に設定した E-mail アドレスに従ってスイッチのログファイルを送信する SMTP サーバを設定します。	267
	SNTP	スイッチに時刻とタイムゾーンの設定を行います。: SNTP Settings、Time Zone Settings	268
	Flash File System Settings	フラッシュファイルシステムを利用したファイル操作を行います。	268
OAM	CFM	CFM 機能を設定します。: CFM Settings、CFM Port Settings、CFM MIPCCM Table、CFM Loopback Settings、CFM Linktrace Settings、CFM Packet Counter、CFM Fault Table、CFM MP Table	272
	Ethernet OAM	ポートにイーサネット OAM モード、イベント、ログを設定します。: Ethernet OAM Settings、Ethernet OAM Configuration Settings、Ethernet OAM Event Log、Ethernet OAM Statistics	282
	DULD Settings	ポートにおいて単方向リンク検出の設定および表示を行います。	285
	Cable Diagnostics	ケーブル診断を行います。	286
Monitoring	Utilization	CPU 使用率、ポートの帯域使用率を表示します。: CPU Utilization、DRAM & Flash Utilization、Port Utilization	287
	Statistics	パケット統計情報とエラー統計情報を表示します。: Port Statistics	289
	Mirror	ポートミラーリングの設定を行います。: Port Mirror Settings	298
	Ping Test	IPv4 アドレスまたは IPv6 アドレスに Ping することができます。	299
	Trace Route	ネットワーク上のスイッチとホスト間の経路をトレースします。	300
	Peripheral	デバイス環境機能はスイッチの内部温度ステータスを表示します。: Device Environment	301

第 6 章　System Configuration（スイッチの主な設定）

以下は、System Configuration サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
Device Information（デバイス情報）	スイッチの主な設定情報を表示します。	37
System Information Settings（システム情報設定 ）	スイッチの基本情報を表示します。	39
Port Configuration（ポート設定）	ポート設定、ジャンボフレーム設定などを行います。以下のメニューがあります。 Port Settings（スイッチのポート設定）、Port Description Settings（ポート名設定）、Port Error Disabled（エラーによるポートの無効）、Jumbo Frame（ジャンボフレームの有効化）	39
PoE Configuration（PoE 設定）（DES-3200-28P/52P のみ）	PoE システムの設定を行います。以下のメニューがあります。 PoE System Settings（PoE システムの設定）、PoE Port Settings（PoE ポート設定）	43
Serial Port Settings（シリアルポート設定）	ボーレートの値と自動ログアウト時間を調整します。	46
Warning Temperature Settings（警告温度設定）	システムの警告温度パラメータを設定します。	46
System Log Configuration（システムログ構成）	フラッシュメモリにスイッチのログを保存する方法、Syslog サーバの設定を行います。以下のメニューがあります。 System Log Settings（システムログ設定）、System Log Server Settings（システムログサーバの設定）、System Log（Syslog ログ）、System Log & Trap Settings（Syslog とトラップ設定）、System Severity Settings（システムセベリティ設定）	47
Time Range Settings（タイムレンジ設定）	アクセスプロファイル機能を実行する期間を決定します。	50
Time Settings（時刻設定）	スイッチに時刻を設定します。	50
User Accounts Settings（ユーザアカウントの設定）	ユーザおよびユーザの権限を設定します。	51
Command Logging Settings（コマンドログ設定）	コマンドログ設定を有効または無効にします。	52

Device Information（デバイス情報）

本画面は、ログインを行うと自動的に表示される画面で、スイッチの主な設定情報を確認できます。本画面に戻るためには「DES-3200 シリーズ」フォルダをクリックします。

本画面には、スイッチの「MAC Address」（工場による設定のため変更不可）、「Boot PROM Version」と「Firmware Version」、「Hardware Version」などが表示されます。これらの情報は、PROM やファームウェアの更新状況の把握や他のネットワークデバイスのアドレステーブルにスイッチの MAC アドレスを登録する際の確認などに便利です。さらに、スイッチの各機能の状態を表示し、現在のグローバルステータスにアクセス可能です。いくつかの機能は、各設定画面にリンクしており、本画面から接続できます。

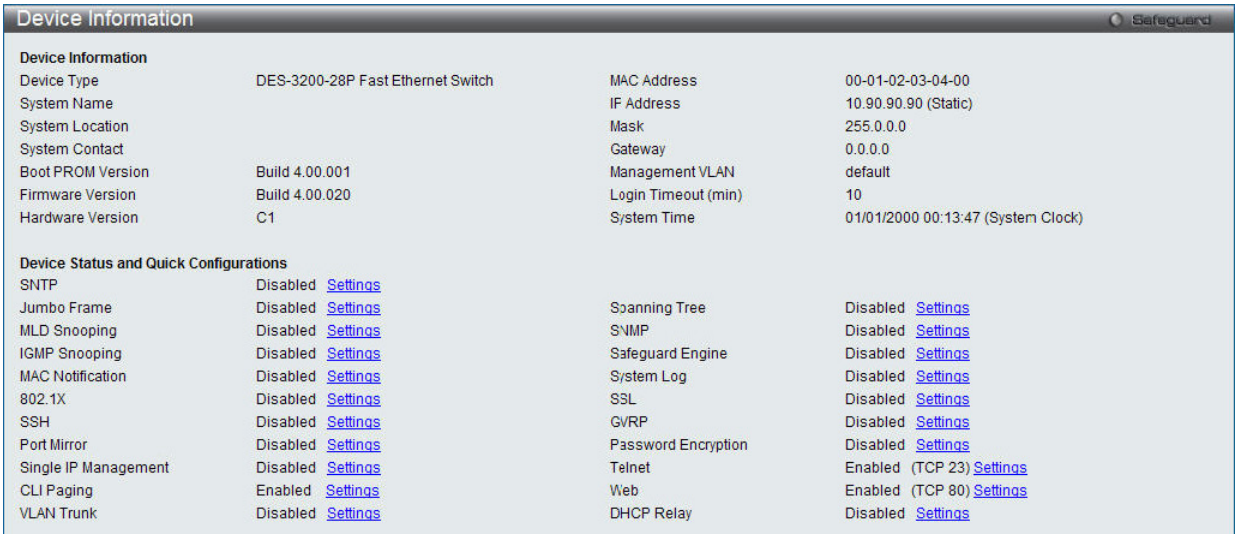


図 6-1　Device Information 画面

画面には以下の項目があります。

項目	説明
Device Information	
Device Type	工場にて定義した機種名と型式を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。（半角英数字 160 文字以内）
System Contact	担当者名を表示します。（半角英数字 31 文字以内）
Boot PROM Version	デバイスのブートバージョンを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
Hardware Version	デバイスのハードウェアバージョンを表示します。
MAC Address	デバイスに割り当てられた MAC アドレスを表示します。
IP Address	デバイスに割り当てられた IP アドレスを表示します。
Mask	デバイスに割り当てられたサブネットマスクを表示します。
Gateway	デバイスに割り当てられたデフォルトゲートウェイを表示します。
Management VLAN	デバイスに割り当てられた VLAN 名を表示します。
Login Timeout (min)	ユーザが何もしなかった場合にデバイスがタイムアウトするまでの時間を表示します。初期値は 10（分）です。
System Time	最後のデバイスリセットからの経過時間を表示します。日、時、分、秒の形式で表示します。 例 : 41days 2 hours 22 mins 5 seconds

項目	説明
Device Status and Quick Configurations	
SNTP	SNTP 機能の状態（有効 / 無効）を表示します。SNTP 設定にリンクします。
Jumbo Frame	Jumbo Frame 機能の状態（有効 / 無効）の表示と、Jumbo Frame の設定にリンクします。
MLD Snooping	MLD Snooping 機能の状態（有効 / 無効）の表示と、MLD の設定にリンクします。
IGMP Snooping	IGMP Snooping 機能の状態（有効 / 無効）の表示と、IGMP の設定にリンクします。
MAC Notification	MAC 通知機能の状態（有効 / 無効）を表示します。MAC 通知設定にリンクします。
802.1X	802.1X 機能の状態（有効 / 無効）の表示と、802.1X の設定にリンクします。
SSH	SSH（Secure Shell Protocol）機能の状態（有効 / 無効）の表示と、SSH の設定にリンクします。
Port Mirror	ポートミラーリング機能の状態（有効 / 無効）の表示と、ポートミラーリングの設定にリンクします。
Single IP Management	SIM 機能の状態（有効 / 無効）を表示します。SIM 設定にリンクします。
CLI Paging	CLI ページング機能を有効 / 無効にします。CLI ページングの設定にリンクします。
VLAN Trunk	VLAN トランク機能を有効 / 無効にします。VLAN トランクの設定にリンクします。
Spanning Tree	STP 機能の状態（有効 / 無効）を表示します。STP 設定にリンクします。
SNMP	SNMP 機能の状態（有効 / 無効）を表示します。SNMP 設定にリンクします。
Safeguard Engine	Safeguard エンジン機能の状態（有効 / 無効）の表示と、Safeguard エンジンの設定にリンクします。
System Log	Syslog 機能をグローバルに有効 / 無効にします。初期値は無効です。Syslog の設定にリンクします。
SSL	SSL（Secure Socket Layer）機能の状態（有効 / 無効）の表示と、SSL の設定にリンクします。
GVRP	GVRP（Group VLAN Registration Protocol）機能の状態（有効 / 無効）の表示と、GVRP の設定にリンクします。
Password Encryption	パスワードの暗号化機能を有効 / 無効にします。パスワードの設定にリンクします。
Telnet	Telnet 機能の状態（有効 / 無効）の表示と、Telnet 設定にリンクします。
Web	Web ベースの管理機能を有効 / 無効にします。Web ベースの管理は初期値で有効になっています。無効に設定し、システムに適用すると、Web インタフェースによるシステム設定は行えなくなります。Web ベースの設定にリンクします。
DHCP Relay	DHCP リレー機能を有効または無効にします。DHCP リレー機能の設定にリンクします。

デバイスの機能設定の参照手順

1. 「Device Status and Quick Configurations」セクションのデバイスの機能を選択します。

2. 機能名の後の Setting をクリックし、選択したデバイスの機能の設定画面を表示します。「Apply」ボタンをクリックし、設定を適用します。

System Information Settings（システム情報設定 ）

ここでは、スイッチの詳細情報を表示します。本画面には、「System Name」、「System Location」、「System Contact」などを入力し、スイッチの定義を行う際にも利用できます。また、スイッチの「MAC Address」（工場による設定のため変更不可）、「Firmware Version」、「Hardware Version」が表示されます。

System Configuration > System Information Settings の順にメニューをクリックして、以下の画面を表示します。

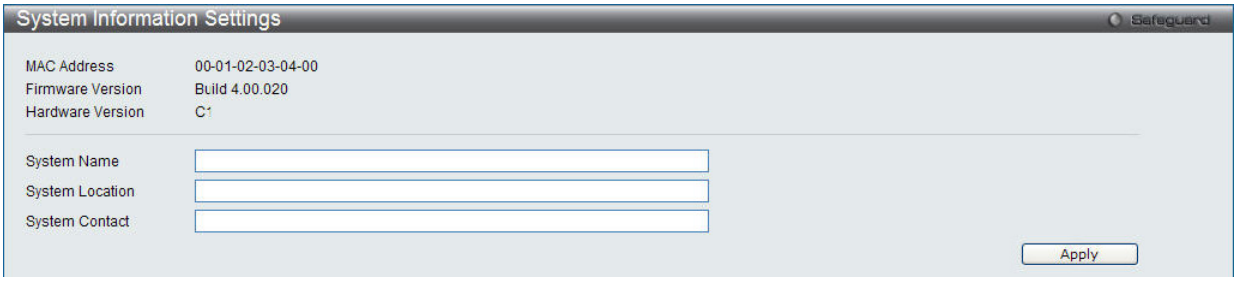


図 6-2　System Information Settings 画面

画面には次の項目があります。

項目	説明
MAC Address	デバイスに割り当てられた MAC アドレスを表示します。
Firmware Version	スイッチのファームウェアバージョンを表示します。
Hardware Version	スイッチのハードウェアバージョンを表示します。
System Name	ユーザが定義するシステム名を設定します。
System Location	システムが現在動作している場所を定義します。（半角英数字 160 文字以内）
System Contact	スイッチの管理者情報を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Port Configuration（ポート設定）

Port Settings（スイッチのポート設定）

スイッチポートの詳細を設定します。
「State」、「Speed/Duplex」、「Flow Control」、「Address Learning」、「Medium Type」、および「MDIX」を含むさまざまなポート設定をスイッチに行うことができます。

ポートの設定や情報の表示を行うには、**System Configuration > Port Configuration > Port Settings** の順にメニューを選択し、以下の画面を表示します。

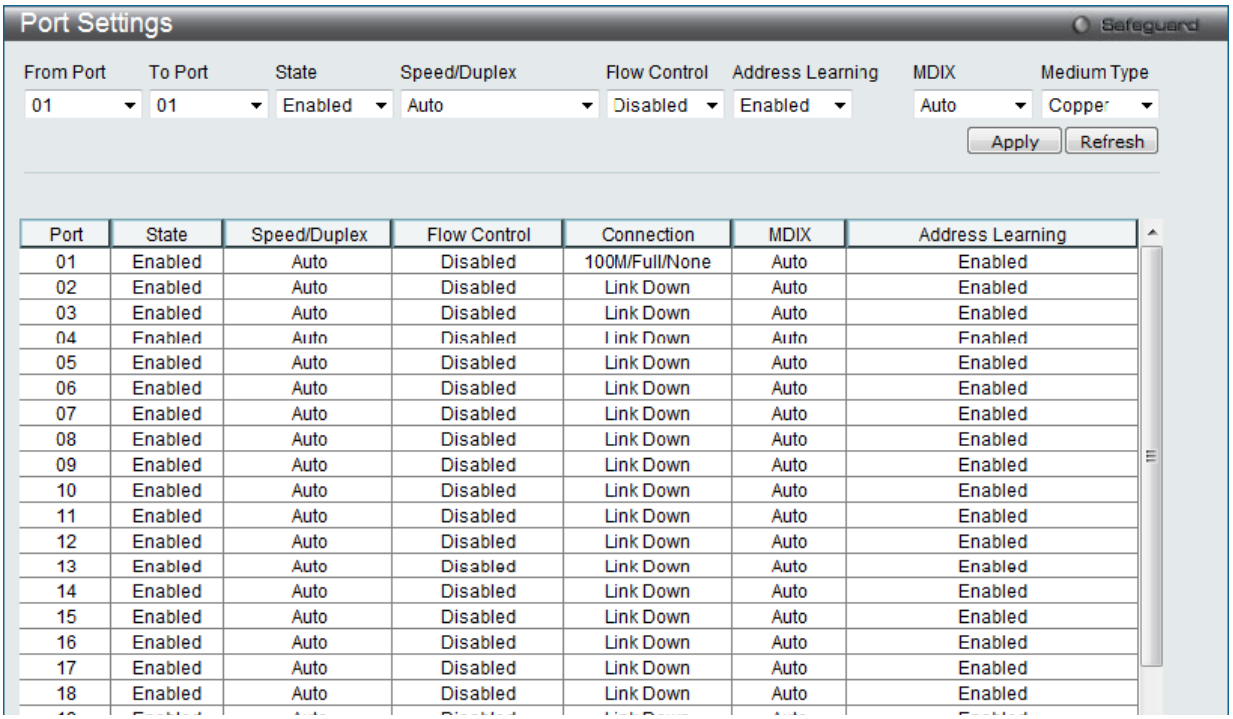


図 6-3　Port Settings 画面

「From Port」と「To Port」のプルダウンメニューからポートまたはポートの範囲を選択します。
残りのプルダウンメニューから以下に示す項目について設定を行います。

項目	説明
From Port/To Port	本設定に使用される適切なポート範囲を選択します。
State	指定したポートまたはポート範囲を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Speed/ Duplex	ポートの速度および全二重 / 半二重の指定を行います。「Auto」は、10/100Mbps のデバイス間（全二重または半二重モード時）のオートネゴシエーションを示します。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 オプションには「Auto」、「10M Half」、「10M Full」、「100M Half」、「100M Full」、「1000M Full_Master」、および「1000M Full_Slave」があります。Auto 以外のオプションのポート設定は固定となります。 スイッチは 1000M Full_Master および 1000M Full_Slave タイプのギガビット接続設定ができます。ギガビット接続はフルデュプレックス接続だけをサポートしており、他の選択肢とは異なる特徴を持っています。 1000M Full_Master（マスタ）および 1000M Full_Slave（スレーブ）項目は、ギガビット接続が可能なスイッチポートと他のデバイス間を 1000BASE-T で結ぶ接続を表示しています。マスタ設定（1000M Full_Master）によりポートはデュプレックス、速度および物理レイヤタイプに関連する情報を通知することができます。さらに 2 つの接続している物理レイヤ間のマスタおよびスレーブを決定します。この関係は 2 つの物理レイヤ間のタイミングコントロールを確立するために必要です。タイミングコントロールはローカルソースによってマスタ物理レイヤ上に設定されます。スレーブ設定（1000M Full_Slave）はループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わせます。一方の接続に 1000M Full_Master を設定するともう一方の接続は 1000M Full_Slave に設定する必要があります。その他の設定は両ポートのリンクダウンを引き起こします。
Flow Control	各ポートのフローコントロール設定を選択します。Full-Duplex では 802.3x フローコントロールを、Half-Duplex ではバックプレッシャーによる制御を自動で行います。「Enabled」（フロー制御あり）または「Disabled」（フロー制御なし）を選択します。初期値は「Disabled」（フロー制御なし）です。
Address Learning	選択ポートにおける MAC アドレスの学習の有無を設定します。 • Enabled - 終点と始点 MAC アドレスをフォワーディングテーブルに自動的にリストアップします。 • Disabled - MAC アドレスはフォワーディングテーブルに手動で登録します。セキュリティや効率上の理由で使用されることがあります。フォワーディングテーブルに MAC アドレスを登録する方法については、「FDB (FDB 設定)」(114 ページ)を参照してください。初期値は「Enabled」です。
MDIX	• Auto - 最適なケーブル配線タイプを自動的に感知します。 • Normal - 標準のケーブル配線となります。「normal」状態に設定すると、MDI モードになり、ストレートケーブルを通し PC の NIC に接続し、クロスケーブルを通して他のスイッチ上のポートに接続することができます。 • Cross - クロスケーブル接続のために選択します。ストレートケーブルを通して別のスイッチの上のポート (MDI モード) に接続することができます。
Medium Type	本設定はコンボポートだけに適用します。コンボポートを設定する場合、使用する変換メディアのタイプを選択します。SFP ポートの場合は「Fiber」、10/100/1000BASE-T の場合は「Copper」を設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Refresh」ボタンをクリックして、本画面を更新します。

Port Description Settings（ポート名設定）

本スイッチはポート説明機能をサポートしており、ユーザはスイッチ上のポートに名前をつけることができます。

System Configuration > Port Configuration > Port Description Settings の順にメニューをクリックし、以下の画面を表示します。

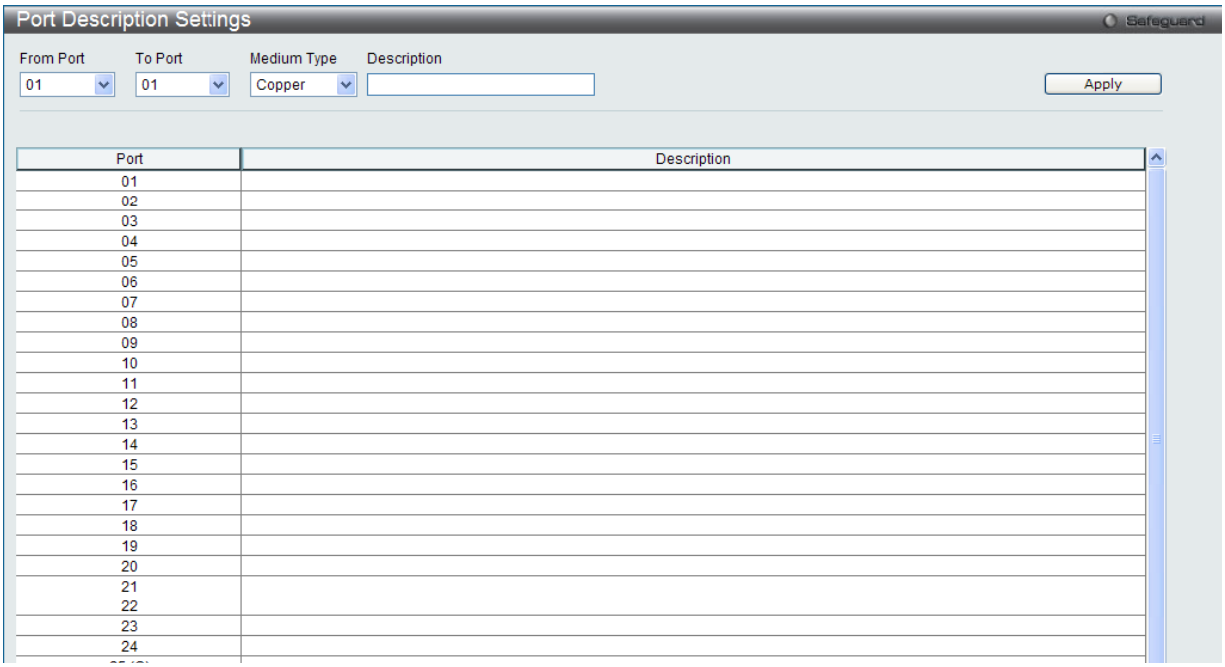


図 6-4　Port Description Settings 画面

ポート、またはポート範囲を「From」と「To」プルダウンメニューから選択し、それらのポートについての名前や説明を入力します。

以下の項目を使用して設定します。

項目	説明
From Port / To Port	本設定に使用される適切なポート範囲を選択します。
Medium Type	選択ポートのメディアタイプを指定します。コンボポートを設定する場合、使用している通信メディアのタイプを指定します。SFP ポートの場合は「Fiber」を指定し、10/100/1000BASE-T ポートの場合は「Copper」を指定します。
Description	選択ポートの説明を入力します。

「Apply」ボタンをクリックすると、「Port Description」テーブルに追加されます。

Port Error Disabled（エラーによるポートの無効）

パケットストームの発生やループバックの検出などの理由で、スイッチが切断したポートに関する情報を表示します。

System Configuration > Port Configuration > Port Error Disabled の順にメニューをクリックし、以下の画面を表示します。

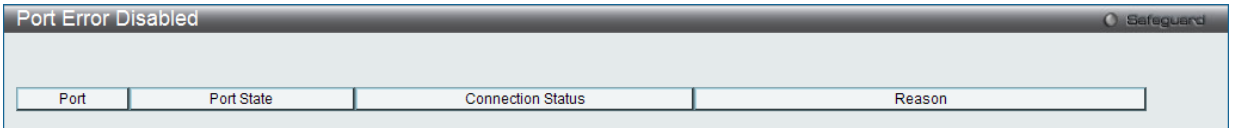


図 6-5　Port Error Disabled 画面

以下の項目が表示されます。

項目	説明
Port	エラーのために無効になっているポートを表示します。
Port State	現在のポートのステータス（「Enabled」または「Disabled」）を表示します。
Connection Status	各ポートのアップリンク状況（「Enabled」または「Disabled」）を表示します。
Reason	ストームコントロールによるポートのシャットダウンなどポートがエラーによって無効になった理由を表示します。

Jumbo Frame Settings（ジャンボフレームの有効化）

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。有効にすると、最大 12228 バイトを持つジャンボフレーム（1536 バイトの標準イーサネットフレームより大きいサイズのフレーム）の送信が可能になります。

ここでは、スイッチでジャンボフレームを扱うことを可能にします。これによりオーバヘッド、処理時間、割り込みを確実に減らすことができます。

System Configuration > Port Configuration > Jumbo Frame Settings の順にクリックし、以下の画面を表示します。

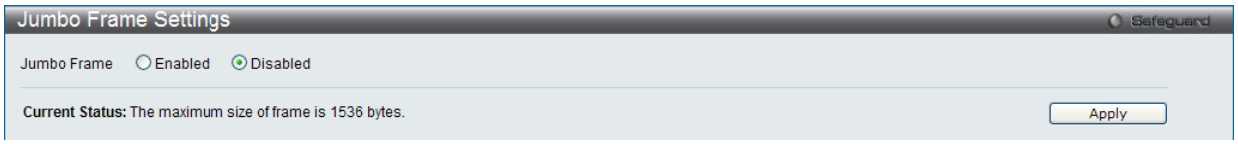


図 6-6　Jumbo Frame Settings 画面

本画面には次の項目があります。

項目	説明
Jumbo Frame Global Settings	
Jumbo Frame	ジャンボフレームを扱うかどうかを設定します。無効時の最大フレームサイズは 1536 バイトです。 • Enabled - デバイスでジャンボフレームを有効に設定します。最大フレームサイズは 12228 バイトです。 • Disabled - デバイスでジャンボフレームを無効に設定します。（初期値）

「Enabled」または「Disabled」を設定し、「Apply」ボタンをクリックします。

PoE Configuration（PoE 設定）（DES-3200-28P/52P のみ）

DES-3200-28P および DES-3200-52P は、IEEE 802.3af と 802.3at 規格で定義される PoE（Power over Ethernet）をサポートしています。DES-3200-28P は 1-24 ポート、DES-3200-52P は 1-48 ポートが PoE をサポートしています。

カテゴリ 5 またはカテゴリ 3 の UTP イーサネットケーブル経由で受電機器に 48VDC の電力を供給します。スイッチは標準の PSE（Power Source over Ethernet）のピン配列 Alternative A に従い、電源出力は 1、2、3 および 6 番ピンで行われます。スイッチは、弊社の IEEE 802.3af 準拠製品すべてに給電することができます。

RJ-45 ピン番号	信号名
1	Negative Vport
2	Negative Vport
3	Positive Vport
4	—
5	—
6	Positive Vport
7	—
8	—
9	—
10	—

スイッチは以下の PoE 給電機能を持ちます。
- 自動検出機能により、受電機器（PD : Power Device）の接続を認識し、自動的に電力を送信します。
- 自動無効化機能はポートの電流値が 350mA を超過するか、またはショートが起こった場合にアクティブにします。

802.3af が有効なデバイスでは、各クラスの PSE デバイスにおける最小出力電力レベルは以下の通りです。

クラス	利用	PSE デバイスの最小出力電力レベル
0	初期値	15.4W
1	オプション	4.0W
2	オプション	7.0W
3	オプション	15.4W
4	予約	クラス 0 として処理

LLDP 方式を使用した、グラニュラリティ 0.1W の電力割り当てを持つ 802.3at が有効なデバイスでは、各クラスの PSE デバイスにおける最小出力電力レベルは以下の通りです。

クラス	利用	PSE デバイスの最小出力電力レベル
0	初期値	15.4W
1	オプション	4.0W
2	オプション	7.0W
3	オプション	15.4W
4	オプション	15.4 または 30W

注意 クラス 4 デバイスは以下の式を使用します。

Ptype=Icable x V Port_PSE min
Type 1 = 15.4 W
Type 2 = 30 W

スイッチに PoE 機能を設定するためには、**System Configuration > PoE** の順にメニューを選択します。

PoE System Settings（PoE システムの設定）

電力制限値および全 PoE システムの給電停止方法について設定を行います。消費電力の合計が上限値を上回った時、PSE 内部の PoE コントローラが給電を停止してオーバロードを防ぎます。

PoE 機能の設定を行うためには、**System Configuration > PoE > PoE System Settings** の順にメニューを選択し、以下の画面を表示します。

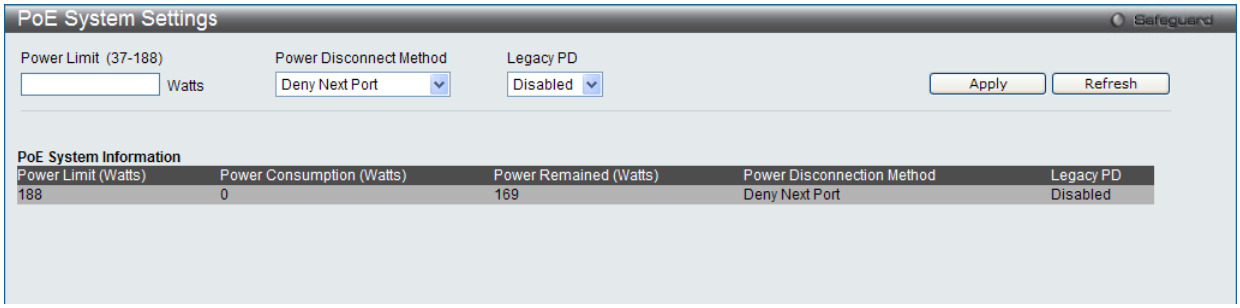


図 6-7　PoE System Settings 画面

以下の項目を使用します。

項目	説明
Power Limit	スイッチの給電機器から PoE ポート群に供給可能な電力の上限値。DES-3200-28P に 37-188W、DES-3200-52P に 37-370W の電力制限を設定できます。
Power Disconnect Method	PoE コントローラは、「Deny Next Port」または「Deny Low Priority Port」によって、供給可能な電力の上限値の超過を防ぎ、スイッチの給電レベルを一定内に保ちます。プルダウンメニューから電力の停止方法を選択します。 • Deny Next Port - スイッチが給電できる最大電力を到達した場合には、優先度に関わらず、新規に接続された PD に給電しません。未使用電力の最大は 19W です。（初期値） • Deny Low Priority Port - スイッチが給電できる最大電力に到達した場合に新規の PD が接続された場合は、ポート優先度の最も低いポートを切断し、高優先度でクリティカルなポートに給電します。
Legacy PD	プルダウンメニューを使用して、旧型の PD 信号の検知を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、設定内容を適用します。

PoE Port Settings（PoE ポート設定）

デバイスの各ポートに PoE 設定を行います。

System Configuration > PoE > PoE Port Settings の順にメニューをクリックし、以下の画面を表示します。

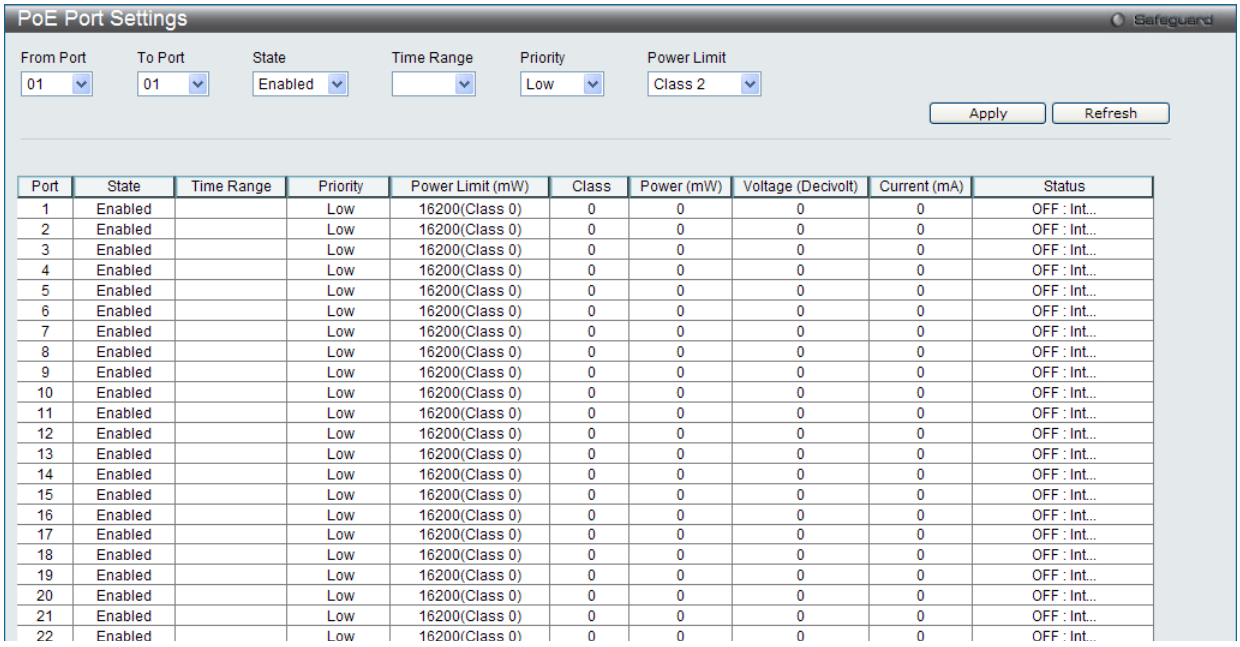


図 6-8　PoE Port Settings 画面

以下の項目を使用します。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>From Port / To Port</td><td>プルダウンメニューから PoE 機能を有効または無効にするポート範囲を選択します。</td></tr>
<tr><td>State</td><td>ポートの PoE 機能を「Enabled」（有効）/「Disabled」（無効）にします。</td></tr>
<tr><td>Time Range</td><td>設定した PoE ポートにタイムレンジを選択します。タイムレンジを設定すると、指定期間だけ電力が供給されます。</td></tr>
<tr><td>Priority</td><td>PoE ポートの優先度を指定します。ポート優先度はシステムがポートへの電力の供給を試みる優先度を決定します。ポート優先度には、高い順に「Critical」、「High」、「Low」の 3 つのレベルがあります。複数のポートに同じ優先レベルがたまたまある場合、ポート ID が優先度を決定するのに使用されます。低いポート ID ほど高い優先度を持ちます。優先度設定はポートに電力を供給する順番に影響します。「PoE System Settings」画面で停止方法に「Deny Low Priority Port」が設定されているかどうかにかかわらず、ポートへの電力供給を管理するためにシステムは各ポートの優先度を使用します。</td></tr>
<tr><td>Power Limit</td><td>1 ポートあたりの電力制限を設定します。ポートが電力制限を超過していると、シャットダウンされます。

802.3af が有効なデバイスでは、各クラスの PSE デバイスにおける最小出力電力レベルは以下の通りです。
<table>
<tr><th>クラス</th><th>利用</th><th>PSE デバイスの最小出力電力レベル</th></tr>
<tr><td>0</td><td>初期値</td><td>15.4W</td></tr>
<tr><td>1</td><td>オプション</td><td>4.0W</td></tr>
<tr><td>2</td><td>オプション</td><td>7.0W</td></tr>
<tr><td>3</td><td>オプション</td><td>15.4W</td></tr>
<tr><td>4</td><td>予約</td><td>クラス 0 として処理</td></tr>
</table>
LLDP 方式を使用してした、グラニュラリティ 0.1W の電力割り当てを持つ 802.3at が有効なデバイスでは、各クラスの PSE デバイスにおける最小出力電力レベルは以下の通りです。
<table>
<tr><th>クラス</th><th>利用</th><th>PSE デバイスの最小出力電力レベル</th></tr>
<tr><td>0</td><td>初期値</td><td>15.4W</td></tr>
<tr><td>1</td><td>オプション</td><td>4.0W</td></tr>
<tr><td>2</td><td>オプション</td><td>7.0W</td></tr>
<tr><td>3</td><td>オプション</td><td>15.4W</td></tr>
<tr><td>4</td><td>オプション</td><td>15.4 または 30W</td></tr>
</table>
これらの 5 つのクラスに対してポートに適用可能な電力の制限値は以下の通りです。各クラスの電力制限はそのクラスの電力範囲よりも若干大きくなっています。これはケーブル上の電力損失も考慮に入れているためです。そのため、標準値は以下のようになります。
<table>
<tr><th>クラス</th><th>PSE の最大出力電力</th></tr>
<tr><td>0</td><td>16200mW</td></tr>
<tr><td>1</td><td>4200mW</td></tr>
<tr><td>2</td><td>7400mW</td></tr>
<tr><td>3</td><td>16200mW</td></tr>
<tr><td>ユーザ定義</td><td>35000mW</td></tr>
</table>
</td></tr>
</table>

「Apply」ボタンをクリックし、設定内容を適用します。PoE 設定が行われたすべてのポートの状態は、上記画面下半分のテーブルに表示されます。

Serial Port Settings（シリアルポート設定）

ボーレートの値と自動ログアウト時間を調整します。また、シリアルポート設定に関する情報を表示します。

スイッチにシリアルポート設定をするためには、**System Configuration > Serial Port Settings** の順にメニューをクリックし、以下の画面を表示します。

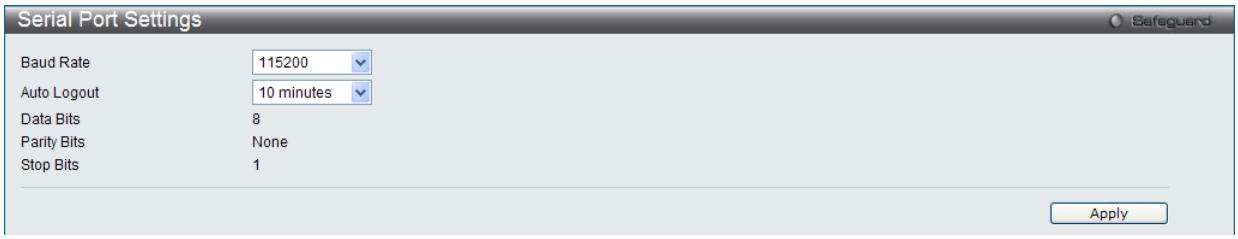


図 6-9　Serial Port Settings 画面

画面には次の項目があります。

項目	説明
Baud Rate	スイッチのシリアルポートのボーレートを指定します。9600、19200、38400、115200 から選択できます。 CLI インタフェースを使用したスイッチ接続には 115200（初期値）を指定します。
Auto Logout	コンソールインタフェースのログアウト時間を選択します。ここで設定した時間アイドル状態が続くと自動的にログアウトします。次のオプションから、選択します。2、5、10、15 minutes（分）または Never（自動ログアウトを行わない）から選択できます。初期値 :10 minutes（分）。
Data Bits	シリアルポート接続に使用されるデータビットを表示します。
Parity Bits	シリアルポート接続に使用されるパリティビットを表示します。
Stop Bits	シリアルポート接続に使用されるストップビットを表示します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意　シリアルポートのボーレートを設定すると、ボーレートは、直ちに適用され、保存されます。

Warning Temperature Settings（警告温度設定）

システムの警告温度パラメータを設定します。

System Configuration > Warning Temperature Settings の順にメニューをクリックし、以下の画面を表示します。

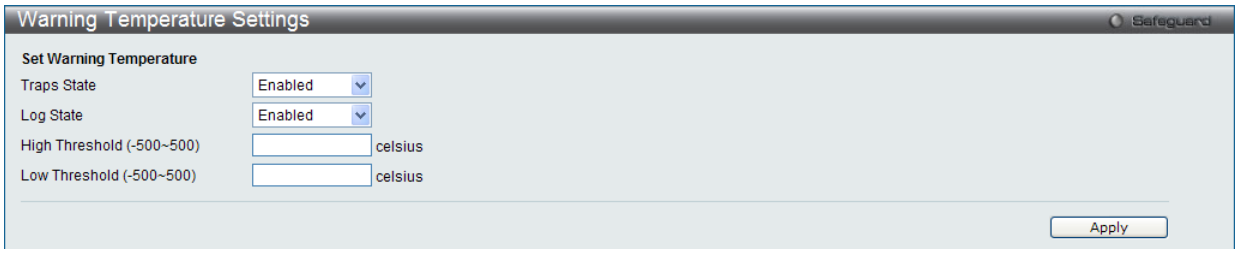


図 6-10　Warning Temperature Settings 画面

画面には次の項目があります。

項目	説明
Traps State	警告温度設定のトラップ状態を有効または無効にします。
Log State	警告温度設定のログ状態を有効または無効にします。
High Threshold (-500-500)	警告温度設定の上のしきい値を入力します。
Low Threshold (-500-500)	警告温度設定の下のしきい値を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

System Log Configuration（システムログ構成）

System Log Settings（システムログ設定）

システムログ機能を有効または無効にし、スイッチのフラッシュメモリにスイッチログを保存する方法を選択します。

System Configuration > System Log Configuration > System Log Settings の順にメニューをクリックし、以下の画面を表示します。

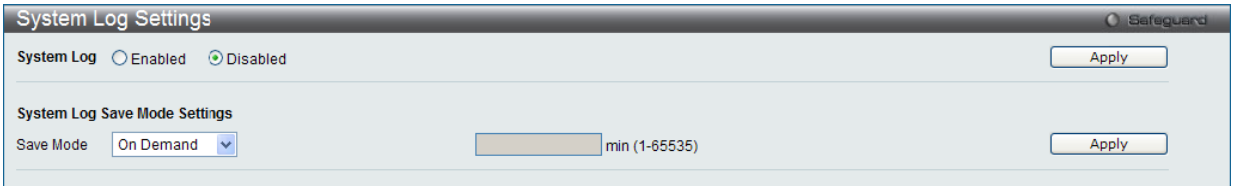


図 6-11　System Log Settings 画面

画面には次の項目があります。

項目	説明
System Log	システムログ機能を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Save Mode	プルダウンメニューよりフラッシュメモリにスイッチのログを保存する方法を指定します。３つのオプションがあります。 • Time Interval - 本項目横にある欄にログを保存する間隔（1-65535）（分）を設定します。 • On Demand - 手動でスイッチに、ログファイルを保存します。「Save」フォルダを使用して保存します。（初期値） • Log Trigger - スイッチにログイベントが発生すると、スイッチにログファイルを保存します。

1. 「System Log」を「Enabled」（有効）にし、「Apply」ボタンをクリックします。
2. プルダウンメニューよりフラッシュメモリにスイッチのログを保存する方法を指定します。「Time Interval」を選択した場合は、横にある欄にログを保存する間隔を入力します。
3. 設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

System Log Server Settings（システムログサーバの設定）

システムログはイベントの記録と管理、エラーと情報のメッセージをレポートします。イベントメッセージは、すべてのエラーレポートに Syslog プロトコルの推奨する固有のフォーマットを使用します。例えば、Syslog とローカルデバイスのレポートメッセージはその重要度や、メッセージを生成するアプリケーションを識別するためのメッセージ識別名を含みます。メッセージは緊急度かその関連する事項に基づいてフィルタされます。各メッセージの重要度によって、イベントメッセージの送信先となるイベントを記録するデバイスを決めることができます。

本スイッチは指定した 4 台までの Syslog サーバに Syslog メッセージを送信できます。

1. **System Configuration > System Log Configuration > System Log Server Settings** の順にクリックし、以下の画面を表示します。

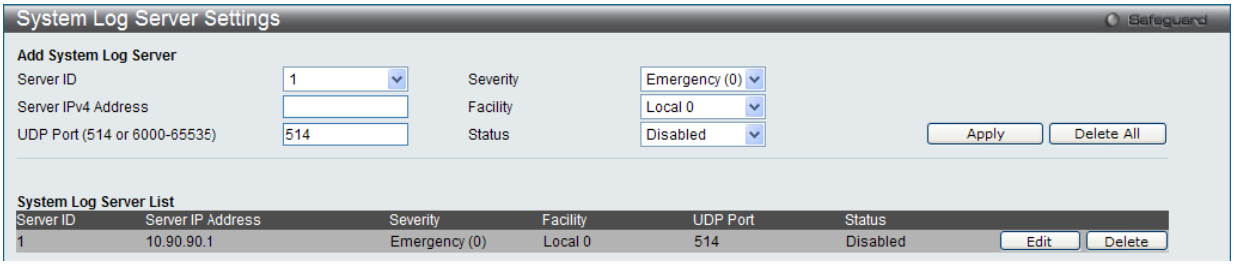


図 6-12　System Log Server Settings 画面

本画面には次の項目があります。

項目	説明
Server ID	Syslog サーバ設定のインデックス（1-4）を設定します。
Severity	送信されるメッセージレベルをプルダウンメニューから選択します。選択したレベル以上のメッセージをすべて送信します。オプションは Emergency (0)、Alert (1)、Critical (2)、Error (3)、Warning (4)、Notice (5)、Informational (6) および Debug (7) です。
Server IPv4 Address	ログを記録するサーバの IPv4 アドレスを設定します。
Facility	オペレーティングシステムデーモンおよびプロセスでファシリティ値を割り当てている場合に設定します。Local 0、Local 1、Local 2、Local 3、Local 4、Local 5、Local 6、または Local 7 を選択します。
UDP Port (514 or 6000-65535)	Syslog メッセージを送信するのに使用する UDP ポートを設定します。514 または 6000-65535 が設定できます。初期値は 514 です。
Status	「Enabled」（有効）または「Disabled」（無効）を選択します。

各項目を設定します。「Apply」ボタンをクリックし、システムログホスト設定をデバイスに適用します。

エントリの変更

1. 編集する場合は、該当エントリ横の「Edit」ボタンをクリックして、編集画面を表示します。

2. 項目を入力後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックし、デバイスのエントリを削除します。または、「Delete All」ボタンをクリックして、設定したすべてのサーバを削除します。

System Log（Syslog ログ）

スイッチの管理エージェントでまとめたローカルなヒストリログの表示および削除を行います。

System Configuration > System Log Configuration > System Log の順にメニューをクリックし、以下の画面を表示します。

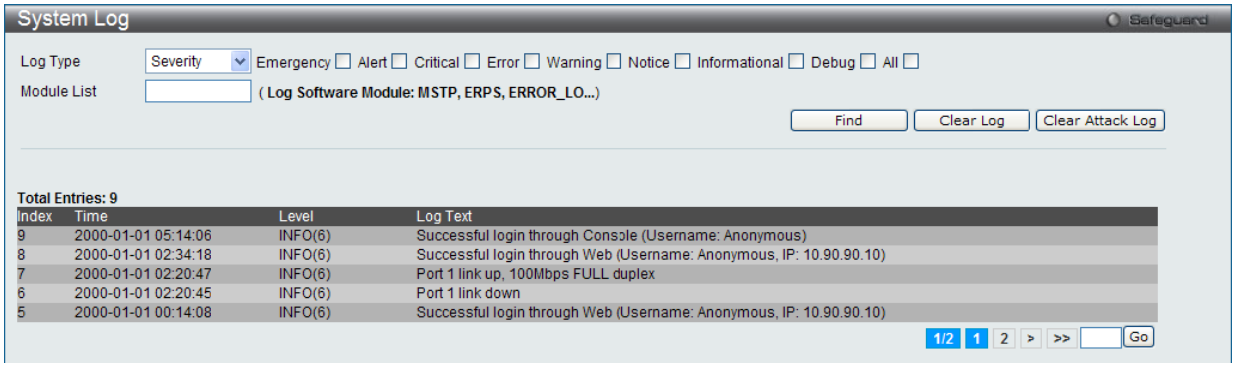


図 6-13　System Log 画面

スイッチは自身のログにイベント情報を記録できます。「Go」ボタンをクリックすると、「System Log」画面の次のページへ移動します。

画面には次の項目があります。

項目	説明
Log Type	プルダウンメニューで表示するログタイプを選択します。 • Severity - これを選択する場合、次のチェックも行う必要があります。次にチェックするのは Emergency、Alert、Critical、Error、Warning、Notice、Informational および Debug です。ログ内の全情報を単に参照するには、「All」オプションを選択します。特定のモジュールを検索するためには、モジュール名を入力します。 • Module List - これを選択する場合、手動でモジュール名を入力する必要があります。利用可能なモジュールは、MSTP、DHCPv6_CLIENT、DHCPv6_RELAY、ERPS、および ERROR_LOG です。 • Attack Log - すべての攻撃が表示されます。
Index	エントリが加わるごとに 1 増加します。新しいエントリ順に表示されます。
Time	スイッチの最後の再起動から経過した時間（日、時、分、秒）を表示します。
Level	ログエントリのレベルを表示します。
Log Text	イベントの内容を表示します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Find」ボタンをクリックして、選択に基づいて表示セクションにログを表示します。
「Clear Log」ボタンをクリックして、表示画面内のすべてのエントリをクリアします。
「Clear Attack Log」ボタンをクリックして、表示セクション内の攻撃ログからエントリをクリアします。

System Log & Trap Settings（Syslog とトラップ設定）

スイッチに Syslog の送信元 IP インタフェースアドレスを設定できます。

1. **System Configuration > System Log Configuration > System Log & Trap Settings** の順にクリックし、以下の画面を表示します。

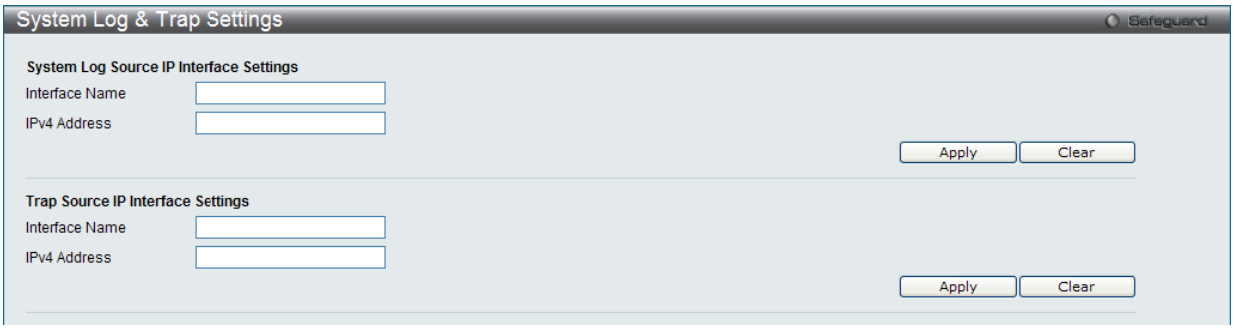


図 6-14　System Log & Trap Settings 画面

本画面には次の項目があります。

項目	説明
Interface Name	使用する IP インタフェース名を入力します。
IPv4 Address	使用する IPv4 アドレスを入力します。

各セクションで行った変更を適用するためには、必ず「Apply」ボタンをクリックします。

「Clear」ボタンをクリックして、欄内に入力されたすべての情報をクリアします。

System Severity Settings（システムセベリティ設定）

スイッチは、アラートが発生した場合、ログとして記録するか、または SNMP エージェントにトラップとして送信することができます。また、アラートの発生がログイベント、またはトラップメッセージをトリガにするレベルも指定することができます。ここではアラートの基準を設定します。「System Severity Table」セクションに現在の設定を表示します。

System Configuration > System Log Configuration > System Severity Settings の順にメニューを選択し、以下の設定画面を表示します。

注意　画面中に表示されるログイベントの詳細情報については、本マニュアル中の「付録 C ログイベント」（316 ページ）を参照してください。

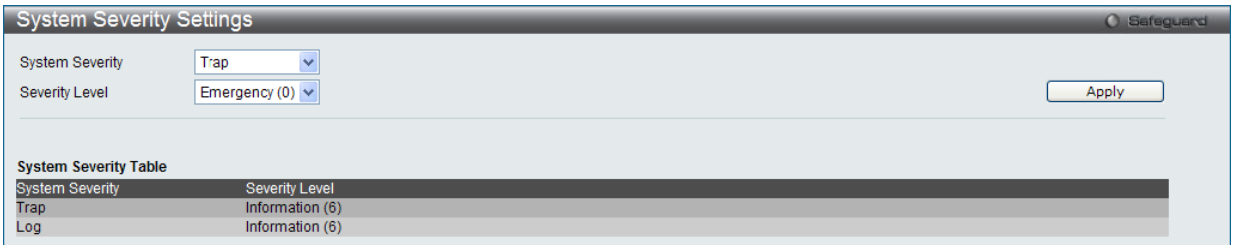


図 6-15　System Severity Settings 画面

プルダウンメニューを使用して、以下の項目の設定を行います。

項目	説明
System Severity	「Severity Type」で指定したレベルのアラートが発生した時に実行するアクションを選択します。 • Log - 分析のためにスイッチのログに設定した「Severity Level」のアラートを送信します。 • Trap - 分析のために SNMP エージェントに送信します。 • All - 分析のために SNMP エージェントとスイッチのログに選択したアラートタイプを送信します。
Severity Level	送信されるメッセージレベルをプルダウンメニューから選択します。オプションは Emergency (0)、Alert (1)、Critical (2)、Error (3)、Warning (4)、Notice (5)、Informational (6) および Debug (7) です。

「Apply」ボタンをクリックして、システムのログレベル設定を適用します。

Time Range Settings（タイムレンジ設定）

各機能（ACL など）が作用する期間（タイムレンジ）を設定します。スイッチのアクセスプロファイル設定が有効な場合、アクセスプロファイル機能を実行する期間（開始点と終了点）を一週間の特定の曜日によって決定します。

例えば、管理者は週土日にインターネットの閲覧を許可し、一方平日はインターネットの閲覧を拒否するようなタイムベース ACL を設定することができます。64 個のタイムレンジを入力することができます。

注意 タイムレンジ機能は、スイッチの時刻設定をベースにしています。Time と SNTP コマンドのセクションにあるコマンドを使用して適切にスイッチに時刻設定されていることをご確認ください。

System Configuration > Time Range Settings の順にメニューをクリックし、以下の画面を表示します。

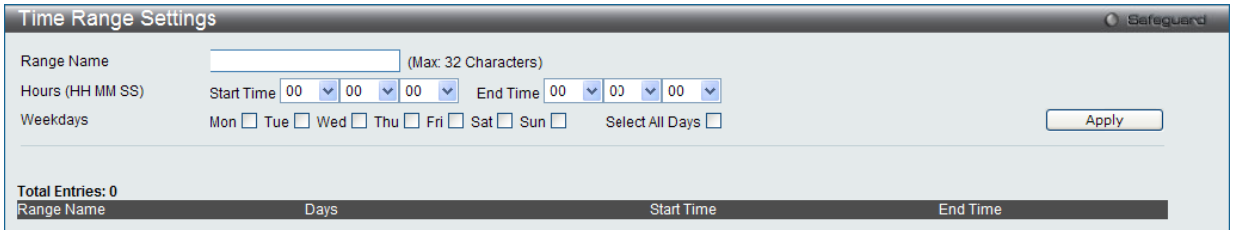


図 6-16　Time Range Settings 画面

以下の項目を設定することができます。

項目	説明
Range Name	タイムレンジを識別するために使用する名前を半角英数字 32 文字以内で入力します。このレンジ名は Access Profile テーブルで使用され、このタイムレンジで有効であるアクセスプロファイルと関連するルールを識別します。
Hours (HH MM SS)	プルダウンメニューを使用し、タイムレンジの時刻を以下の項目で設定します。 • Start Time - 開始時刻を時間、分、秒（24 時形式）で指定します。 • End Time - 終了時刻を時間、分、秒（24 時形式）で指定します。
Weekdays	チェックボックスを使用し、タイムレンジを有効にする曜日を選択します。「Select All Days」をチェックすると、すべての曜日を設定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。設定したエントリは上記画面下半分にあるテーブルに表示されます。

エントリの削除
削除するエントリ横の「Delete」ボタンをクリックします。

Time Settings（時刻設定）

スイッチに時刻を設定します。

System Configuration > Time Settings の順にクリックし、以下の画面を表示します。

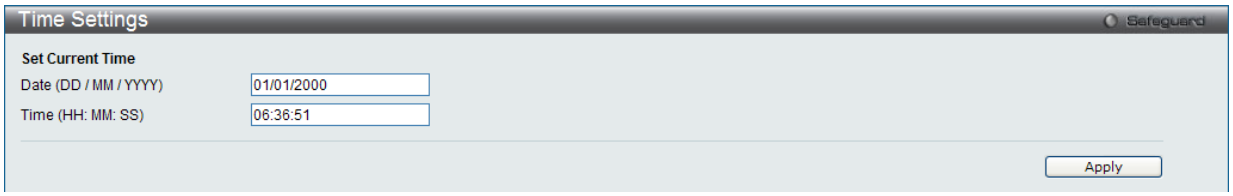


図 6-17　Time Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Date（DD/MM/YYYY）	システムクロックの更新を行うために現在の年月日を入力します。項目のフォーマットは日 / 月 / 年です。
Time（HH:MM:SS）	現在のシステム時刻を時 : 分 : 秒（24 時間制）で設定します。例えば午後 9 時であれば 21:00:00 と指定します。

「Apply」ボタンをクリックし、デバイスに時刻設定を適用します。

User Accounts Settings（ユーザアカウントの設定）

スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。以下の手順でユーザアカウント情報を設定します。

1. **System Configuration > User Accounts Settings** の順にクリックし、「User Accounts」画面を表示します。

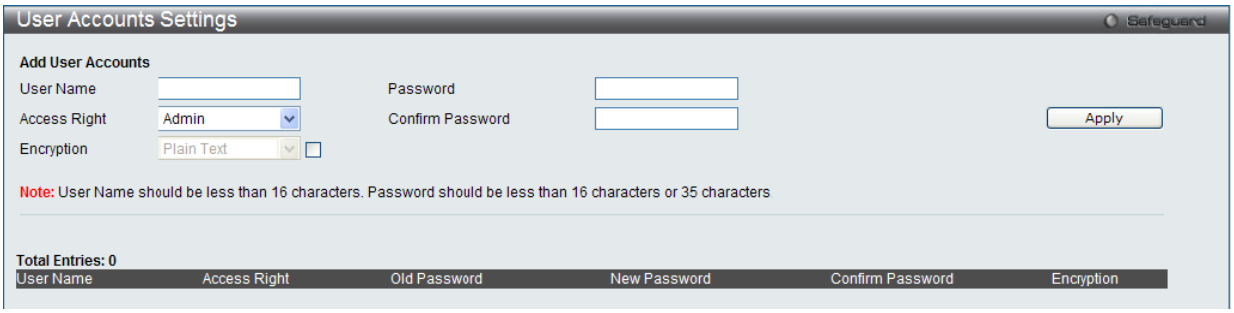


図 6-18　User Accounts Settings 画面

Admin レベル、Operator レベル、Power User および User レベルの権限は以下の通りです。

管理	Admin	Operator	Power User	User
コンフィグレーション設定	読み / 書き可	読み / 書き（一部）	読み / 書き（一部）	不可
ネットワークモニタリング	読み / 書き可	読み / 書き可	読み出しのみ	読み出しのみ
コミュニティ名とトラップステーション	読み / 書き可	読み出しのみ	読み出しのみ	読み出しのみ
ファームウェアとコンフィグレーションファイルの更新	読み / 書き可	読み / 書き可	不可	不可
システムユーティリティ	読み / 書き可	読み出しのみ	読み出しのみ	読み出しのみ
リセット（工場出荷状態へ）	読み / 書き可	不可	不可	不可
ユーザアカウント管理				
ユーザアカウントの登録、更新、変更	読み / 書き可	不可	不可	不可
ユーザアカウントの確認	読み / 書き可	不可	不可	不可

User Accounts 画面には次の項目があります。

項目	説明
User Name	ユーザ名を定義します。（半角英数字 15 文字以内）
Access Right	ユーザのアクセス権限（Admin、Operator、Power User および User）を指定します。
Encryption	本ボックスをチェックして、アカウントに適用する暗号化タイプ（Plain Text または SHA-1）を指定します。
Password	ユーザアカウントに対するパスワードを設定します。（半角英数字 16 文字以内）
Confirm Password	ユーザパスワードの確認のために再度入力をします。

2. 「User Name」を設定します。
3. アクセス権限を「Access Right」に設定します。
4. 新しいパスワードを「Password」に入力し、再度確認のために「Confirm Password」にも入力します。
5. 「Apply」ボタンをクリックし、新しいユーザアカウント、パスワード、アクセス権限をデバイスに適用します。

ユーザアカウントの編集

1. User List から編集するユーザ名の「Edit」ボタンをクリックし、編集画面を表示します。
2. 各項目を設定します。必要に応じ、「Encrypt」で暗号化タイプ（「Plain Text」または「SHA-1」）を選択します。
3. パスワードを変更する場合は、現在のパスワードを「Old Password」に、新しいパスワードを「New Password」に、確認のために再度新しいパスワードを「Confirm Password」に入力します。
4. 「Apply」ボタンをクリックし、新しいアクセス権限をデバイスに適用します。

注意　パスワードを忘れてしまった場合やパスワード不正の場合は、「付録 F パスワードリカバリ手順」（327 ページ）を参照してください。本問題を解決する手順が記載されています。

エントリの削除

該当エントリの「Delete」ボタンをクリックします。ユーザアカウントが削除され、デバイスが更新されます。

注意　ユーザ名とパスワードは 16 文字以内とします。

Command Logging Settings（コマンドログ設定）

コマンドログ設定を有効または無効にします。

System Configuration > Command Logging Settings の順にメニューをクリックし、以下の画面を表示します。

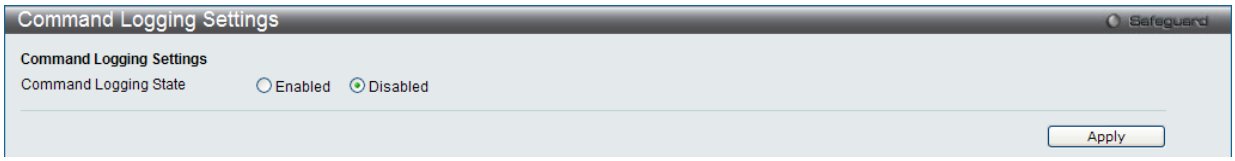


図 6-19　Command Logging Settings 画面

以下の項目を設定することができます。

項目	説明
Command Logging State	ラジオボタンを使用して機能を「Enabled」（有効）/「Disabled」（無効）にします。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意　スイッチの再起動中は、すべてのコンフィグレーションコマンドがログに出力されるというわけではありません。または、ユーザが AAA 認証を使用してログインした際、ユーザが権限を取り替えるために「enable admin」コマンドを使用した場合には、ユーザ名を変更するべきではありません。

第 7 章　Management（スイッチの管理）

以下は、Management サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
ARP（ARP 設定）	スタティック ARP、ARP テーブルを設定します。次のメニューがあります。 Static ARP Settings（スタティック ARP 設定）、ARP Table（ARP テーブルの参照）	54
Gratuitous ARP（Gratuitous ARP の設定）	Gratuitous ARP の設定をします。次のメニューがあります。 Gratuitous ARP Global Settings（Gratuitous ARP グローバル設定）、Gratuitous ARP Settings（Gratuitous ARP 設定）	56
IPv6 Neighbor Settings （IPv6 Neighbor 設定）	IPv6 Neighbor の設定を行います。	58
IP Interface（IP インタフェース設定）	スイッチの IP インタフェース設定を行います。次のメニューがあります。 System IP Address Settings（IP アドレス設定）、Interface Settings（インタフェース設定）	59
Management Settings（管理設定）	CLI ページング、DHCP 自動設定などの管理設定を行います。	63
Session Table（セッションテーブル）	スイッチが最後に起動してからの管理セッションを表示します。	63
Single IP Management （シングル IP マネジメント設定）	シングル IP マネジメント機能を設定します。次のメニューがあります。 Single IP Settings（シングル IP 設定）、Firmware Upgrade（ファームウェア更新）、Configuration File Backup/ Restore（コンフィグレーションファイルの更新）、Upload Log File（ログファイルのアップロード）	64
SNMP Settings（SNMP 設定）	SNMP 設定を行います。次のメニューがあります。 SNMP Global Settings（SNMP グローバル設定）、SNMP Trap Settings（SNMP トラップ設定）、SNMP Link Change Traps Settings（SNMP リンクチェンジトラップ設定）、SNMP View Table Settings（SNMP ビューテーブル）、SNMP Community Table Settings（SNMP コミュニティテーブル設定）、SNMP Group Table Settings（SNMP グループテーブル）、SNMP Engine ID Settings（SNMP エンジン ID 設定）、SNMP User Table Settings（SNMP ユーザテーブル設定）、SNMP Host Table Settings（SNMP ホストテーブル設定）、SNMP v6Host Table Settings（SNMP v6 ホストテーブル設定）、RMON Settings（RMON 設定）	73
Telnet Settings（Telnet 設定）	スイッチに Telnet 設定をします。	80
Web Settings（Web 設定）	スイッチに Web ステータスを設定します。	80

ARP（ARP 設定）

Static ARP Settings（スタティック ARP 設定）

ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換する TCP/IP プロトコルです。ここでは特定のデバイスに対する ARP 情報を参照、編集および削除することができます。
スタティックエントリを ARP テーブルに定義します。スタティックエントリを定義する場合、継続的なエントリを入力し、IP アドレスを MAC アドレスに変換するために使用します。以下の手順で ARP 情報を定義します。

1. **Management > ARP > Static ARP Settings** の順にクリックし、以下の画面を表示します。

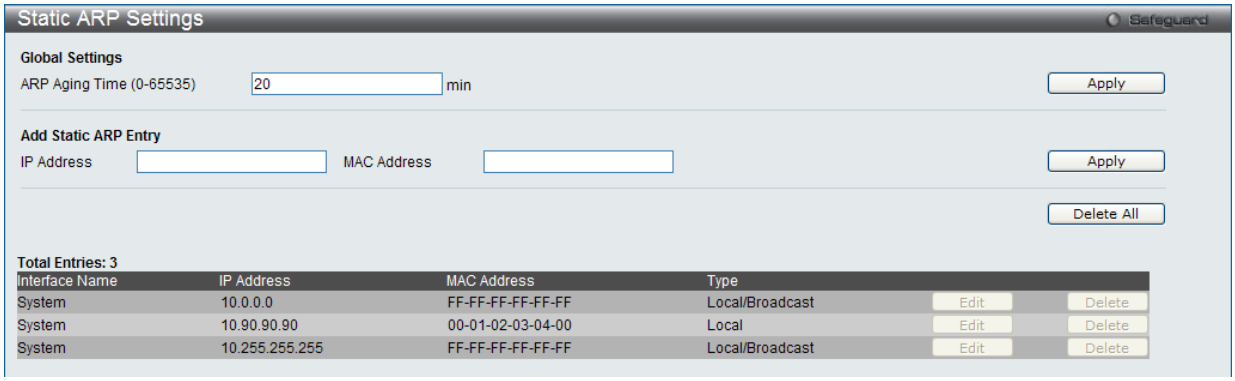


図 7-1　Static ARP Settings 画面

「Static ARP Settings」画面には次の項目があります。

項目	説明
Global Settings	
ARP Aging Time (0-65535)	ARP エントリのエージングタイム（分）。この時間が経過すると、エントリはテーブルから削除されます。範囲は 0-65535（分）です。初期値は 20（分）です。
Add Static ARP Entry	
IP Address	MAC アドレスとスタティックに結びつける IP アドレスを設定します。
MAC Address	ARP テーブルで IP アドレスとスタティックに結びつける MAC アドレスを設定します。
スタティック ARP リスト	
ユーザがスタティックに設定した IP アドレスと MAC アドレスの対応エントリを表示します。	

2. 「ARP Aging Time」を設定します。
3. 「Apply」ボタンをクリックし、ARP の全体的な設定を更新します。
4. 「IP Address」と「MAC Address」を設定します。
5. 「Apply」ボタンをクリックし、デバイスの ARP 設定を更新します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックし、編集画面を表示します。
2. 「MAC Address」を編集します。
3. 「Apply」ボタンをクリックします。

エントリの削除

1. 削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除する場合は、「Delete All」ボタンをクリックします。

ARP Table（ARP テーブルの参照）

スイッチ上の現在の ARP エントリを表示します。

Management > ARP > ARP Table メニューをクリックし、以下の画面を表示します。

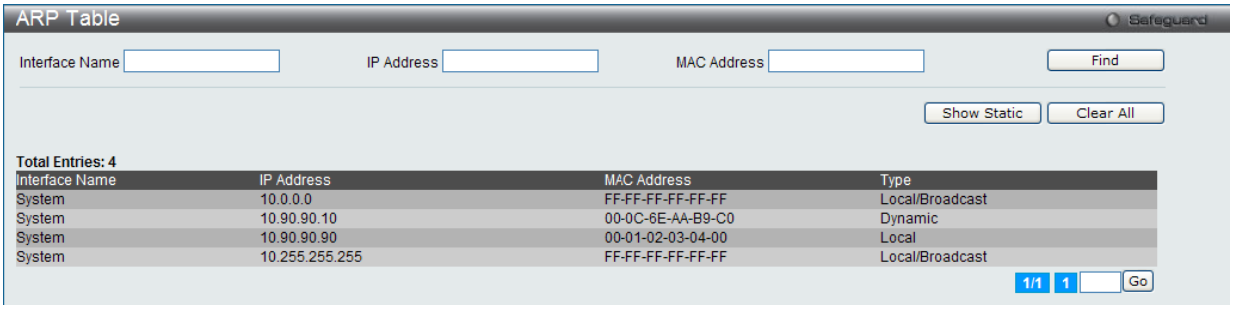


図 7-2　ARP Table 画面

設定対象となる項目は以下の通りです。

項目	説明
Interface Name	使用する IP インタフェース名を入力または参照します。
IP Address	使用する IP アドレスを入力または参照します。
MAC Address	使用する MAC アドレスを入力または参照します。

特定の ARP エントリを検索するためには、画面の上の「Interface Name」または「IP Address」を入力し、「Find」ボタンをクリックします。

スタティック ARP エントリを表示する場合は、「Show Static」ボタンをクリックします。
ARP テーブルをクリアする場合は、「Clear All」ボタンをクリックします。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Gratuitous ARP（Gratuitous ARP の設定）

Gratuitous ARP として知られている ARP 通知は、TAP と SPA が等しい場合、それを送信したホストに有効である SHA と SPA を含むパケット（通常 ARP リクエスト）です。このリクエストは、応答を求めることを意図されたものでなく、パケットを受信する他のホストの ARP キャッシュを更新しません。

本機能は、起動時に多くのオペレーティングシステムで一般的に行われています。これは、ネットワークカードの変更により、MAC アドレスに対する IP アドレスのマッピングが変更になっていても、他のホストがまだその ARP キャッシュに古いマップを持っているというような問題が発生した場合に、その問題を解決します。

Gratuitous ARP Global Settings（Gratuitous ARP グローバル設定）

Gratuitous ARP のグローバル設定を行います。

Management > Gratuitous ARP > Gratuitous ARP Global Settings の順にメニューをクリックし、以下の画面を表示します。

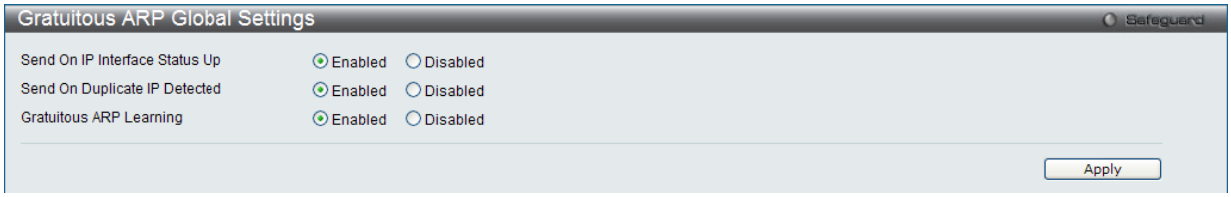


図 7-3　Gratuitous ARP Global Settings 画面

以下の項目を使用して、設定します。

項目	説明
Send On IP Interface Status Up	IP インタフェースの起動中に、Gratuitous ARP リクエストの送信を有効または無効にします。これは、自動的にインタフェースの IP アドレスを他のノードにアナウンスするために使用されます。初期値は有効で、単一の Gratuitous ARP パケットだけがブロードキャストされます。
Send On Duplicate IP Detected	重複した IP アドレスが検知された場合の Gratuitous ARP リクエストパケットの送信を有効または無効にします。初期値は有効です。検出された重複 IP アドレスは、システム自身の IP アドレスに一致する IP アドレスによって送信された ARP リクエストパケットをシステムが受信したことを意味します。この場合、システムは、誰かがシステムと重複する IP アドレスを使用していることがわかります。この IP アドレスのホストを正しくするために、システムはこの重複 IP アドレスに Gratuitous ARP リクエストパケットを送信することができます。
Gratuitous ARP Learning	システムは、通常、システムの IP アドレスに一致している MAC アドレスを求める ARP 応答パケットか正常な ARP リクエストパケットを学習するだけです。受信した Gratuitous ARP パケットに基づいて、ARP キャッシュの更新を有効または無効にします。Gratuitous ARP パケットはパケットがクエリである IP と同じ送信元 IP アドレスによって送信されます。初期値は有効です。

Gratuitous ARP 設定に変更を行った場合には、「Apply」ボタンをクリックします。

注意　Gratuitous ARP を学習すると、システムは新しいエントリを学習しません。また、受信した Gratuitous ARP パケットに基づいて ARP テーブルの更新のみ行います。

Gratuitous ARP Settings（Gratuitous ARP 設定）

IP インタフェースの Gratuitous ARP パラメータを設定します。

Management > Gratuitous ARP > Gratuitous ARP Settings の順にメニューをクリックし、以下の画面を表示します。

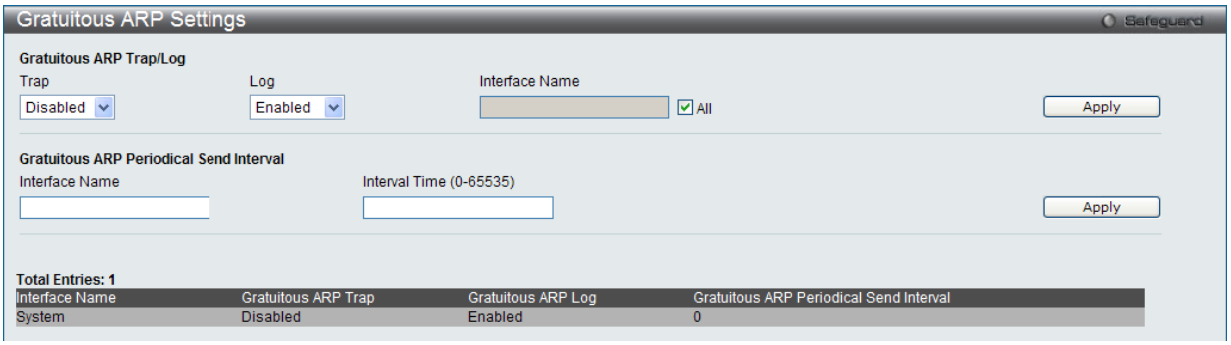


図 7-4　Gratuitous ARP Settings 画面

以下の項目を使用して設定します。

項目	説明
Gratuitous ARP Trap/Log	
Trap	スイッチは、IP の重複イベントをトラップし、管理者に通知します。初期値ではトラップは無効です。
Log	スイッチは、IP の重複イベントのログを取得し、管理者に通知します。初期値ではログは有効です。
Interface Name	レイヤ 3 インフェース名を入力します。「All」を選択して全インタフェース上の Gratuitous ARP トラップを有効または無効にします。
Gratuitous ARP Periodical Send Interval	
Interface Name	編集するインタフェース名を表示します。
Interval Time (0-65535)	定期的に Gratuitous ARP を送信する間隔（秒）を入力します。0 は Gratuitous ARP リクエストが定期的に送信されないことを意味します。初期値は 0（秒）です。

各セクションにある「Apply」ボタンをクリックして、行った変更を適用します。

IPv6 Neighbor Settings（IPv6 Neighbor 設定）

スイッチの IPv6 Neighbor 設定を行います。

Management > IPv6 Neighbor Settings の順にメニューをクリックし、以下の画面を表示します。

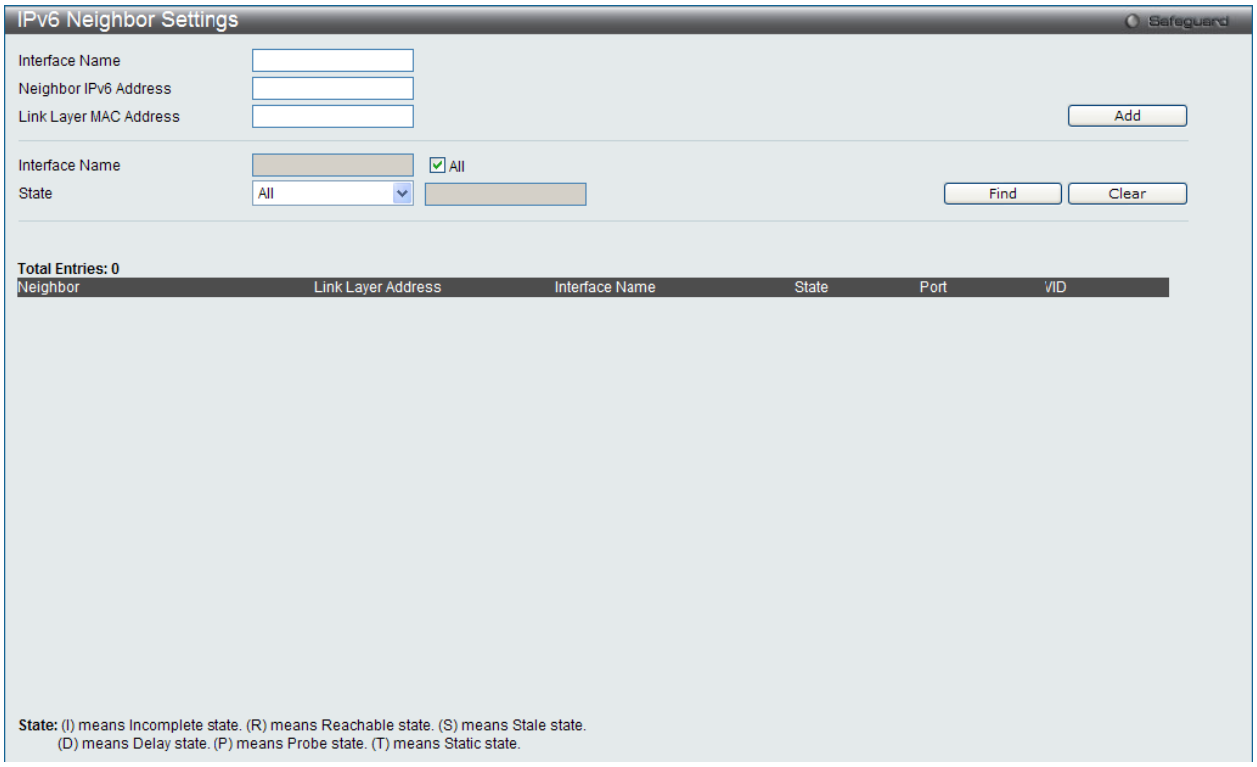


図 7-5　IPv6 Neighbor Settings 画面

スイッチの現在の IPv6 Neighbor 設定が下部に表示されます。

IPv6 Neighbor の新規登録

「Interface Name」、「Neighbor IPv6 Address」および「Link Layer MAC Address」を入力し、「Add」ボタンをクリックします。「State」には、「All」、「Address」、「Static」または「Dynamic」を設定します。

エントリの検索

「IPv6 Neighbor Settings」テーブルエントリを検索するには、「Interface Name」を入力し、画面中央の「State」を選択後、「Find」ボタンをクリックします。

エントリの削除

本画面の下部のテーブルに表示されているすべてのエントリを削除するには、「Clear」ボタンをクリックします。

以下の項目が表示、または設定変更に使用できます。

項目	説明
Interface Name	IPv6 Neighbor のインタフェース名を入力します。
Neighbor IPv6 Address	Neighbor の IPv6 アドレスを入力します。
Link Layer MAC Address	リンクレイヤの MAC アドレスを入力します。
Interface Name	IPv6 Neighbor 名を入力します。IPv6 Neighbor 名を入力します。「All」を選択すると、スイッチにおける現在の全インタフェースを参照します。
State	「All」、「Address」、「Static」または「Dynamic」を指定します。「Address」を選択すると、「State」オプション横にあるスペースに IP アドレスを入力できるようになります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

IP Interface（IP インタフェース設定）

IP 設定を変更します。

ネットワーク接続前に IP アドレスをコンソールより設定する必要があります。Web マネージャはスイッチの現在の IP 設定が表示します。

注意 工場出荷時は、IP アドレス「10.90.90.90」、サブネットマスク「255.0.0.0」、デフォルトゲートウェイに「0.0.0.0」が設定されています。

System IP Address Settings（IP アドレス設定）

スイッチの IP アドレス設定を変更します。

Management > IP Interface > System IP Address Settings の順にメニューをクリックし、以下の画面を表示します。

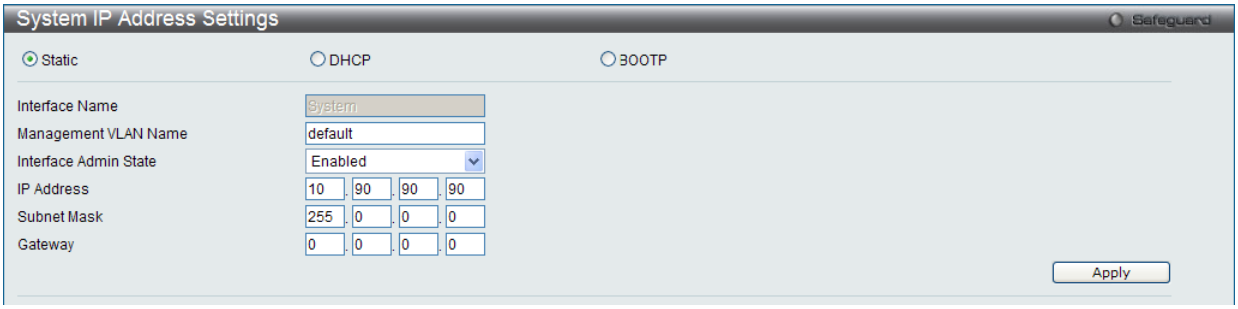


図 7-6　System IP Address Settings 画面

スイッチの現在の IP 設定が表示されます。

本スイッチの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを固定設定する方法を説明します。

1. 画面先頭のメニューから「Static」を選択します。

2. 適切な「IP Address」と「Subnet Mask」を入力します。

3. 異なるサブネットから本スイッチにアクセスする場合は、「Gateway」の IP アドレスを入力します。同じサブネットからスイッチを管理する場合は、この項目内は初期値（0.0.0.0）のままにします。

4. 本スイッチに VLAN 設定をしていない場合は、初期設定の「Management VLAN Name」を使用できます。本スイッチは、購入時に VLAN「default」が設定されていて、すべてのポートが所属しています。既に VLAN 設定をしている場合は、本スイッチにアクセスするためには、管理ステーションに接続しているポートが所属している VLAN の名称を入力します。

5. 設定が行われていない場合は、「Interface Admin State」プルダウンメニューから「Enabled」（有効）を選択します。

DHCP または BOOTP プロトコルを使用してスイッチに IP アドレス、サブネットマスクおよびデフォルトゲートウェイアドレスを割り当てるためには、画面先頭のメニューから「DHCP」または「BOOTP」を選択します。次回の再起動時に、ここで選択した方法により IP アドレスの割り当てが行われます。

プロトコルは以下の通りです。

項目	説明
Static	本スイッチの IPv4 アドレス、ネットマスク、およびデフォルトゲートウェイを固定設定します。アドレスはネットワーク管理者によって割り当てられる固有のアドレスを指定します。入力形式：xxx.xxx.xxx.xxx（x は 0 ～ 255 の数字）。本アドレスはネットワーク管理者により割り振られたネットワークに唯一のアドレスである必要があります。
DHCP	電源が投入されるとスイッチは DHCP ブロードキャストリクエストを送信します。DHCP プロトコルを使用して DHCP サーバが IP アドレス、ネットワークマスクおよびデフォルトゲートウェイを割り当てます。本オプションを選択すると、スイッチは初期設定や以前に登録された設定を使用する前に、DHCP サーバにアクセスし、これらの情報を取得します。
BOOTP	電源が投入されるとスイッチは BOOTP ブロードキャストリクエストを送信します。BOOTP プロトコルを使用して BOOTP サーバが IP アドレス、ネットワークマスクおよびデフォルトゲートウェイを割り当てます。本オプションが選択すると、スイッチは初期設定や以前に登録された設定を使用する前に、BOOTP サーバにアクセスし、これらの情報を取得します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

以下の表は「System」インタフェースに関する項目について説明します。

項目	説明
Interface Name	System インタフェース名が表示されます。
Management VLAN Name	管理ステーションが、TCP/IP（Web マネージャまたは Telnet）によるスイッチ管理を行う時に使用する VLAN 名を入力します。ここで登録した VLAN 以外に所属する管理ステーションからは、スイッチのインバンド管理を行うことができません。ただし、そのアドレスが「Trusted Host」（**Security > Trusted Host**）画面で登録されている場合は可能になります。 スイッチにまだ VLAN を登録していない場合は、スイッチ上のすべてのポートはデフォルト VLAN に所属しています。「Trusted Host」テーブルには初期状態でエントリはないため、管理 VLAN が指定されるまで、または管理ステーションの IP アドレスが登録されるまでは、接続可能な全管理ステーションがスイッチにアクセスできます。
Interface Admin State	「Enabled」（有効）/「Disabled」（無効）にします。IP アドレスを設定する場合は、「Enabled」を設定する必要があります。
IP Address	IP インタフェースに割り当てる IPv4 アドレスを入力します。本スイッチの IP アドレスの初期値は 10.90.90.90 です。
Subnet Mask	本スイッチのサブネットを指定します。入力形式：xxx.xxx.xxx.xxx（x は 0 ～ 255 の数字）。クラス A ネットワークには 255.0.0.0、クラス B ネットワークには 255.255.0.0、クラス C ネットワークには 255.255.255.0 を入力します。カスタムサブネットマスクも入力できます。
Gateway	所属するサブネット外の宛先アドレスを持つパケットの送信先。通常 IP ゲートウェイの役割をするルータやホストのアドレスを指定します。ご使用のネットワークがイントラネットの一部でない場合、またはローカルネットワーク外からのスイッチへのアクセスを許可しない場合は、本項目はそのままにします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Interface Settings（インタフェース設定）

スイッチの IP インタフェース設定を行います。

Management > IP Interface > Interface Settings の順にメニューをクリックし、以下の画面を表示します。

図 7-7　Interface Settings 画面

スイッチの現在の IP インタフェース設定が表示されます。

項目	説明
Interface Name	検索する IP インフェース名を入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。
「IPv4 Edit」ボタンをクリックして、指定エントリの IPv4 設定を編集します。
「IPv6 Edit」ボタンをクリックして、指定エントリの IPv6 設定を編集します。

注意　IPv6 にインタフェースを作成するために、IPv4 インタフェースを作成して、それを IPv6 用に編集する必要があります。

IP インタフェースの追加

1. 「Add」ボタンをクリックして以下の画面を表示します。

図 7-8　IPv4 Interface Settings 画面

2. 以下の項目を設定します。

項目	説明
Interface Name	作成するインフェース名を入力します。
IPv4 Address	使用する IPv4 アドレスを入力します。
Subnet Mask	使用する IPv4 サブネットを入力します。
VLAN Name	使用する VLAN 名を入力します。
Interface Admin State	インタフェースの管理を有効または無効にします。

画面上のセクションにある「Apply」ボタンをクリックし、設定内容を適用してください。
「<<Back」をボタンをクリックすると、変更は破棄されて前のページに戻ります。

IPv4 インタフェースの編集

1. 「Interface Settings」画面で編集するエントリの「IPv4 Edit」ボタンをクリックすると、以下の画面が表示されます。

図 7-9　IPv4 Interface Settings 画面 - Edit

2. 以下の項目を設定します。

項目	説明
Get IP From	このインタフェースが IP アドレスを取得するのに使用する方式（Static、DHCP、BOOTP）を指定します。
Interface Name	編集するインフェース名が表示されます。
IPv4 Address	使用する IPv4 アドレスを入力します。
Subnet Mask	使用する IPv4 サブネットを入力します。
VLAN Name	使用する VLAN 名を入力します。
IPv4 State	IPv4 の状態を有効または無効にします。
Interface Admin State	インタフェースの管理を有効または無効にします。
DHCP Option 12 State	DHCPDISCOVER および DHCPREQUEST メッセージへのオプション 12 の挿入を有効または無効にします。
DHCP Option 12 Host Name	DHCPDISCOVER および DHCPREQUEST メッセージに挿入するホスト名を入力します。

画面上のセクションにある「Apply」ボタンをクリックし、設定内容を適用してください。

「<<Back」をボタンをクリックすると、変更は破棄されて前のページに戻ります。

IPv6 インタフェースの編集

1. 「Interface Settings」画面で編集するエントリの「IPv6 Edit」ボタンをクリックすると、以下の画面が表示されます。

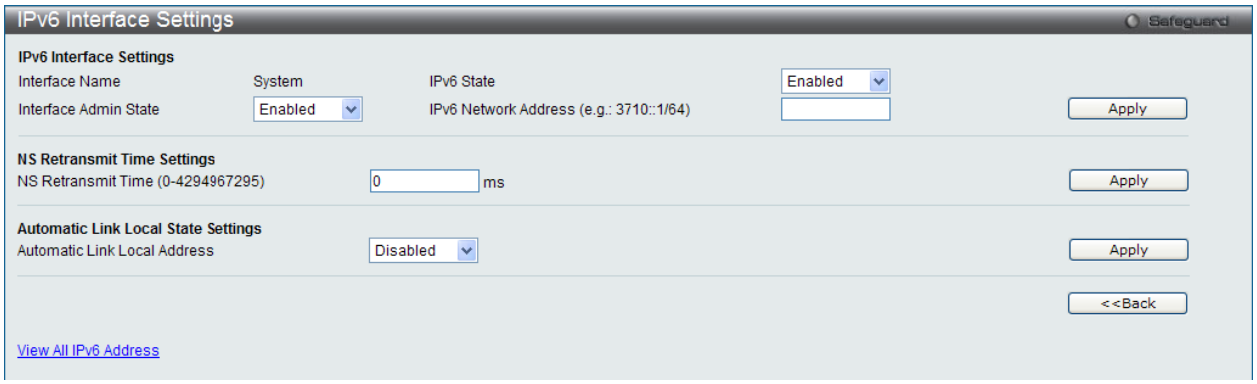


図 7-10　IPv6 Interface Settings 画面 - Edit

2. 以下の項目を設定します。

項目	説明
IPv6 Interface Settings	
Interface Name	IPv6 インタフェース名を表示します。
IPv6 State	IPv6 の状態を有効または無効にします。
Interface Admin State	インタフェースの管理を有効または無効にします。
IPv6 Network Address	Neighbor のグローバルまたはローカルリンクアドレスを入力します。
NS Retransmit Time Settings	
NS Retransmit Time (0-4294967295)	Neighbor Solicitation の再送タイマ（ミリ秒）を入力します。「config ipv6 nd ra」コマンドの設定における「ra retrans_time」と同じ値を持っています。本欄を設定する場合、「RA」欄への入力をコピーします。
Automatic Link Local State Settings	
Automatic Link Local Address	自動リンクローカルアドレスを有効または無効にします。

画面上のセクションにある「Apply」ボタンをクリックし、設定内容を適用してください。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。
「View All IPv6 Address」リンクをクリックして、現在の全 IPv6 アドレスを参照します。

IPv6 アドレスの参照

1. 「View All IPv6 Address」リンクをクリックすると、以下の画面が表示されます。

図 7-11　IPv6 Interface Settings 画面

「<<Back」をボタンをクリックして前のページに戻ります。

IPv6 インタフェースの削除

1. 「Interface Settings」画面で削除するエントリの「Delete」ボタンをクリックします。

Management Settings（管理設定）

本スイッチの管理設定を行います。

コマンドラインインタフェースを使用する場合、コンソールの制限を超えた複数ページのスクロールを停止することができます。また、本画面で本スイッチ DHCP 自動設定機能を有効にします。「Enabled」の時、本スイッチは TFTP サーバからコンフィグレーションファイルを受信して、起動時に自動的に DHCP クライアントになるように設定します。この方法を使用するためには、DHCP サーバは TFTP サーバに IP アドレスと DHCP リプライパケット内の設定ファイル名情報を渡すように設定する必要があります。TFTP サーバを起動し、スイッチからリクエストを受信する時、そのベースディレクトリ内に構成ファイルを保管しておく必要があります。クライアントが使用するための設定ファイルに関する詳しい情報は、DHCP サーバまたは TFTP サーバソフトウェアの手順を参照してください。さらに、本マニュアルの「Tools」セクションの「Upload Log File」画面に関する説明を参照ください。

本スイッチが DHCP 自動設定を完了できない場合は、スイッチのメモリ内にある以前に保存したコンフィグレーションが使用されます。また、本画面では、スイッチの内蔵電源を節電する機能を実装しています。省電力機能が「Enabled」（有効）である場合、リンクダウン状態のポートは電源をオフにしてスイッチへの電力を節約します。ポート状態がリンクアップになっても、これはポートの性能に影響しません。スイッチにパスワードの暗号化機能を設定することができます。

1. **Management > Management Settings** の順にメニューをクリックし、以下の画面を表示します。

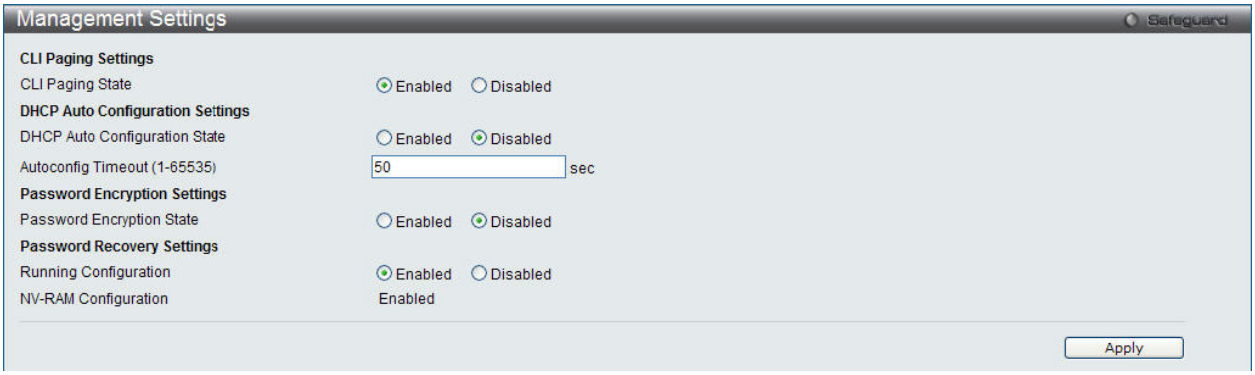


図 7-12　Management Settings 画面

2. 以下の項目を設定します。

項目	説明
CLI Paging State	コマンドラインインタフェースのページング機能はコンソールの終わりで各ページを停止します。これはコンソールの制限を超えた複数ページのスクロールを停止することができます。初期値では CLI ページング機能は有効です。無効にするためには「Disabled」ボタンをクリックします。
DHCP Auto Configuration State	スイッチの DHCP 自動設定機能を有効または無効にします。「Enabled」の時、本スイッチは TFTP サーバからコンフィグレーションファイルを受信して、起動時に自動的に DHCP クライアントになるように設定します。この方法を使用するためには、DHCP サーバは TFTP サーバに IP アドレスと DHCP リプライパケット内の設定ファイル名情報を渡すように設定する必要があります。TFTP サーバを起動し、スイッチからリクエストを受信する時、そのベースディレクトリ内に構成ファイルを保管しておく必要があります。
Autoconfig Timeout (1-65535)	自動コンフィグレーションのタイムアウト時間（1-65535）を入力します。
Password Encryption State	パスワードの暗号化はコンフィグレーションファイル内のパスワード設定を暗号化します。初期値ではパスワードの暗号化は「Disabled」(無効) になっています。パスワードの暗号化を有効にするためには「Enabled」ボタンをクリックします。
Running Configuration	「Password Recovery」オプションにおける動作中のコンフィグレーションを有効または無効にすることができます。有効にすると、動作中のコンフィグレーションのパスワードリカバリの実行を可能とします。

「Apply」ボタンをクリックして行った変更を適用します。

Session Table（セッションテーブル）

スイッチが最後に起動してからの管理セッションを表示します。

1. **Management > Session Table** の順にメニューをクリックし、以下の画面を表示します。

図 7-13　Session Table 画面

「Refresh」ボタンをクリックして、テーブルを更新し、新しいエントリを表示します。

Single IP Management（シングル IP マネジメント設定）

シングル IP マネジメント（SIM）の概要

D-Link シングル IP マネジメントとは、スタックポートまたはモジュールを使用する代わりにイーサネット経由でスイッチをスタックする方法です。シングル IP マネジメント機能を利用する利点を以下に示します。

1. ネットワークを拡大し、増大する帯域幅に対する要求に対処しながら、小規模のワークグループや、ワイヤリングクローゼット（ユーザ接続エリア）を簡単に管理できるようになります。
2. ネットワークに必要な IP アドレス数を減らします。
3. スタック接続のために特別なケーブル配線を必要とせず、他のスタック技術ではトポロジ上の問題になる距離的制限を取り除きます。

D-Link シングル IP マネジメント（以下 SIM と呼びます）機能を搭載するスイッチには、以下の基本的なルールがあります。
- SIM はスイッチのオプション機能であり、CLI または Web インタフェース経由で簡単に有効 / 無効にできます。また、SIM グループはご使用のネットワーク内でスイッチの操作に影響を与えることはありません。
- SIM には 3 つのクラスのスイッチがあります。Commander Switch（CS）はグループのマスタスイッチ、Member Switch（MS）は CS によって SIM グループのメンバとして認識されるスイッチ、Candidate Switch（CaS）は SIM グループに物理的にリンクはしているが、SIM グループのメンバとして認識されていないスイッチです。
- 1 つの SIM グループには、Commander Switch（CS）を 1 つだけ持つことができます。
- 特定の SIM グループ内のすべてのスイッチは、同じ IP サブネット（ブロードキャストドメイン）内にある必要があります。ルータを越えた位置にあるメンバの設定はできません。
- 1 つの SIM グループには、Commander Switch（番号：0）を含めずに、最大 32 台のスイッチ（番号：1-32）が所属できます。
- 同じ IP サブネット（ブロードキャストドメイン）内の SIM グループ数に制限はありませんが、各スイッチは、1 つの SIM グループにしか所属することができません。
- マルチプル VLAN が設定されていると、SIM グループはスイッチ上のデフォルト VLAN だけを使用します。
- SIM は SIM をサポートしていないデバイスを経由することができます。そのため CS から 1 ホップ以上はなれたスイッチを管理することができます。

SIM グループは 1 つのエンティティとして管理されるスイッチのグループです。SIM スイッチは 3 つの異なる役割を持っています。

1. Commander Switch（CS）- グループの管理用デバイスとして手動で設定されるスイッチで、以下の特長を持っています。
   - IP アドレスを 1 つ持つ。
   - 他のシングル IP グループの CS や MS ではない。
   - マネジメント VLAN 経由で MS に接続する。

2. Member Switch（MS）- シングル IP グループに所属するスイッチで、CS からアクセスが可能です。MS は以下の特徴を持ちます。
   - 他のシングル IP グループの CS や MS ではない。
   - CS マネジメント VLAN 経由で CS に接続する。

3. Candidate Switch（CaS）- SIM グループに参加する準備が整っているが、まだ MS ではないスイッチです。CaS を SIM グループ内の MS として、本スイッチの機能を使用して手動で登録することが可能です。CaS として登録されたスイッチは、SIM グループには所属せず、以下の特長を持っています。
   - 他のシングル IP グループの CS や MS ではない。
   - CS マネジメント VLAN 経由で CS に接続する。

上記の役割には、以下のルールを適用します。
- 各デバイスは、まず CS の状態から始まります。
- CS は、はじめに CaS に、その後 MS となり、SIM グループの MS へと遷移します。つまり CS から MS へ直接遷移することはできません。
- ユーザは、CS から CaS へ手動で遷移させることができます。
- 以下のような場合に MS から CaS に遷移します。
   - CS を介して CaS として設定される時。
   - CS から MS への Report パケットがタイムアウトになった時。
- ユーザが手動で CaS から CS に遷移するように設定できます。
- CS を介して CaS は MS に遷移するように設定されます。

SIM グループの CS として運用するスイッチを 1 台登録した後、スイッチを手動によりグループに追加して MS とします。CS はその後 MS へのアクセスのためにインバンドエントリポイントとして動作します。CS の IP アドレスがグループのすべての MS への経路になり、CS の管理パスワードや認証によって、SIM グループのすべての MS へのアクセスを制御します。

SIM 機能を有効にすると、CS 内のアプリケーションはパケットを処理する代わりに、リダイレクト（宛先変更）します。アプリケーションは管理者からのパケットを復号化し、データの一部を変更し、MS へ送信します。処理後、CS は MS から Response パケットを受け取り、これを符号化して管理者に返送します。

CS が MS に遷移すると、自動的に CS が所属する最初の SNMP コミュニティ（リード権 / ライト権、リード権だけを含む）のメンバになります。しかし、自身の IP アドレスを持つ MS は、グループ内の他のスイッチ（CS を含む）が所属していない SNMP コミュニティに加入することができます。

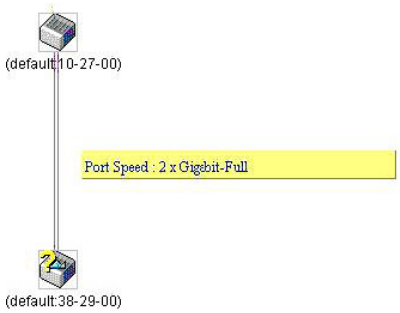
バージョン 1.61 へのアップグレード

SIM 管理機能強化の目的で、本スイッチは本リリースにおいて、バージョン 1.61 にアップグレードしています。本バージョンでは以下の改善点が加わりました。

1. CS は、再起動または Web での異常検出によって、SIM グループから抜けたメンバスイッチを自動的に再検出する機能が搭載しました。この機能は、以前設定された SIM メンバが再起動の後に発行する Discovery パケットと Maintain パケットを使用することにより実現されます。一度 MS の MAC アドレスとパスワードが CS のデータベースに記録され、MS が再起動を行うと、CS はこの MS の情報をデータベースに保存し、MS が再検出された場合、これを SIM ツリーに自動的に戻します。これらのスイッチを再検出するために設定を行う必要はありません。

一度保存を行った MS の再検出ができないという場合もあります。例えば、スイッチの電源がオンになっていない場合、他のグループのメンバとなっている場合、または CS スイッチとして設定された場合は再検出処理をすることができません。

2. トポロジマップには、ポートトランクグループのメンバの接続に関する新機能が加わりました。これはポートトランクグループを構成するイーサネット接続の速度と接続数を表示する機能です。



3. 本バージョンでは、以下のファームウェア、コンフィグレーションファイル、およびログファイルのアップロードやダウンロードを複数スイッチに対して行う機能が追加されました。

- ファームウェア : TFTP サーバから複数の MS に対するファームウェアダウンロードがサポートされました。
- コンフィグレーションファイル : TFTP サーバを使用した複数のコンフィグレーションのダウンロード / アップロード（コンフィグレーションの復元やバックアップ用）が可能になりました。
- ログ : 複数のログファイルを TFTP サーバにアップロード可能になりました。

4. より詳細に構成を確認しやすいようにトポロジ画面を拡大、縮小することができます。

Single IP Settings（シングル IP 設定）

スイッチは工場出荷時設定で Candidate Switch（CaS）として設定され、SIM は無効になっています。

1. Web インタフェースを使用してスイッチの SIM を有効にするためには **Management > Single IP Management > Single IP Settings** の順にメニューをクリックし、以下の画面を表示します。

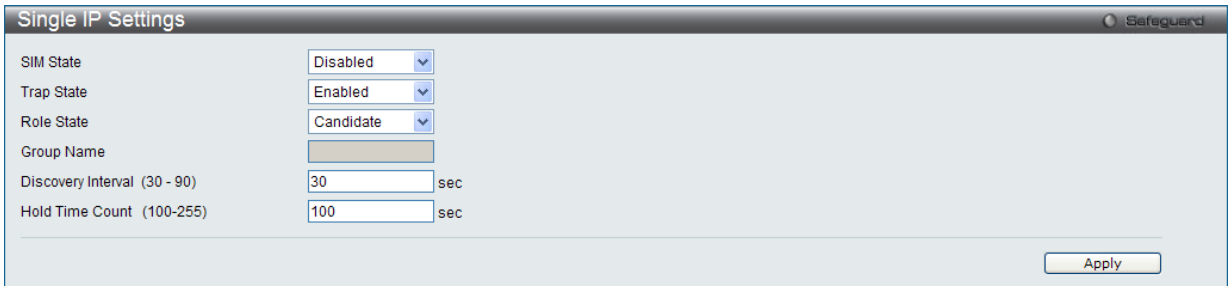


図 7-14　Single IP Settings 画面（CaS 無効状態）

2. プルダウンメニューを使用して、「SIM State」を「Enabled」（有効）、「Role State」を「Commander」に変更し、次に「Group Name」欄を指定します。

3. 「Apply」ボタンをクリックして、設定を有効にします。

以下の項目が使用できます。

項目	説明
SIM State	プルダウンメニューから「Enabled」（有効）または「Disabled」（無効）を選択します。「Disabled」を選択すると、スイッチのすべての SIM 機能が無効になります。初期値は「Disabled」です。
Trap State	プルダウンメニューからトラップの送信を「Enabled」（有効）または「Disabled」（無効）にします。
Role State	プルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。 • Candidate - Candidate Switch（CaS）は SIM グループメンバではありませんが、Commander スイッチに接続しています。本スイッチの SIM 機能の初期設定です。 • Commander - Commander Switch（CS）。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオプションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。
Group Name	SIM グループ名を入力します。これはオプションで、「SIM State」が「Enabled」（有効）、「Role State」が「Candidate」である場合にだけ利用できます。この名称は別の SIM グループにスイッチを区分するのに使用されます。
Discovery Interval (30-90)	スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔（秒）を設定します。CS スイッチに情報が送られてくると、接続する他のスイッチ（MS、CaS）の情報が CS に組み込まれます。値は 30-90（秒）の間から指定します。初期値は 30（秒）です。
Hold Time Count (100-255)	他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間（秒）を指定します。値は 100-255（秒）の間から指定します。初期値は 100（秒）です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

スイッチを CS として登録すると、「Single IP Management」フォルダには 4 つのリンクが追加され、Web を使用した SIM 設定が続けられるようになります。追加されるリンクは「Topology」、「Firmware Upgrade」、「Configuration Backup/Restore」、「Upload Log File」です。

Topology（トポロジ）

SIM グループ内のスイッチの設定および管理を行います。本画面は表示のためには、ご使用のコンピュータに Java スクリプトが必要です。インストール方法についてはサンマイクロシステムズ社のホームページをご確認ください。

Management > Single IP Management > Topology の順にメニューをクリックします。

サーバ上で Java Runtime Environment が起動し、以下の画面が表示されます。

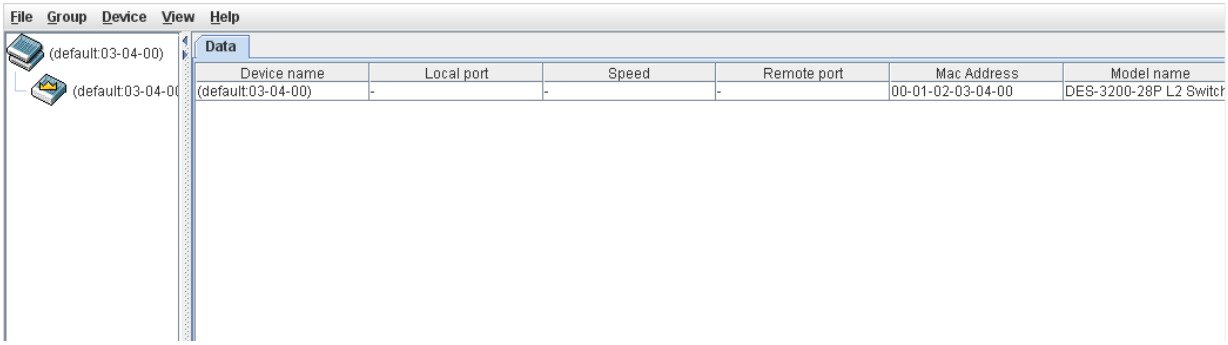


図 7-15　トポロジ画面

トポロジ画面の「Data」タブには以下の情報が表示されます。

項目	説明
Device Name	ユーザが設定した SIM グループ内のスイッチのデバイス名を表示します。デバイス名がない場合は、default が与えられ、識別のために MAC アドレスの終わり 6 桁が付加されます。
Local port	MS または CaS が接続している CS 上の物理ポート数を表示します。CS の場合は何も表示されません。
Speed	CS と MS、または CaS 間の接続速度を表示します。CS の場合は何も表示されません。
Remote port	CS が接続している MS または CaS 上の物理ポート数を表示します。CS の場合は何も表示されません。
Mac Address	対応するスイッチの MAC アドレスを表示します。
Model name	対応するスイッチのモデル名を表示します。

トポロジマップの表示

ツールバーの「View」メニューから「Topology」を選択し、以下の画面を表示します。トポロジビューは定期的に（初期値：20 秒）更新されます。

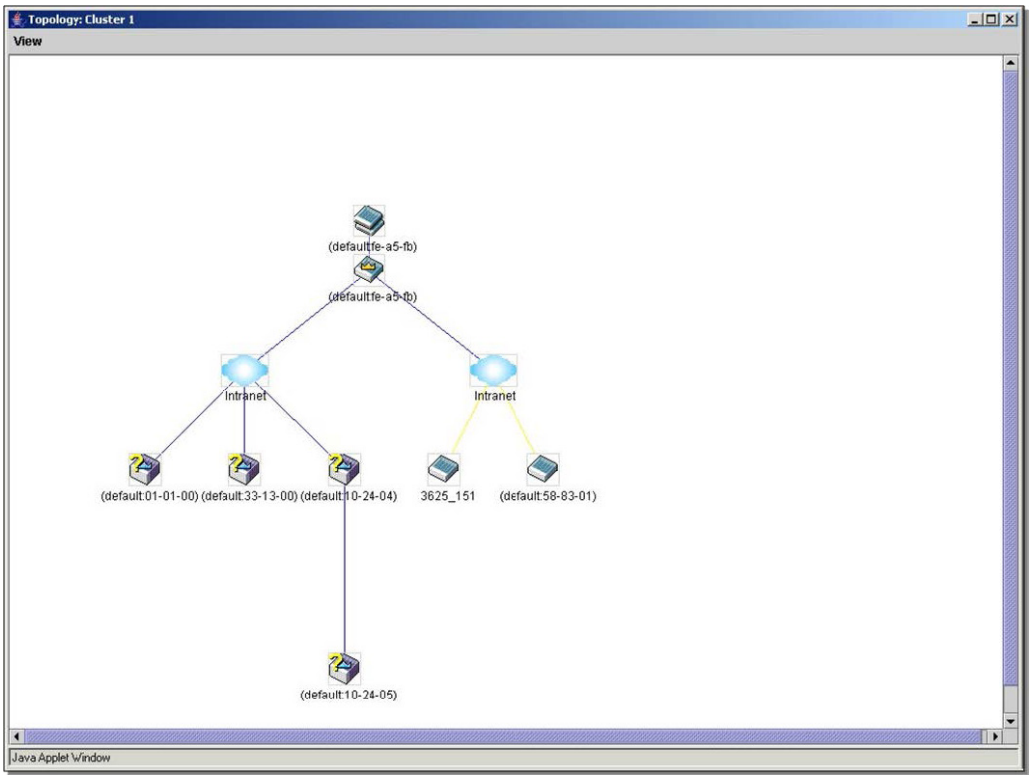
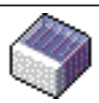


図 7-16　Topology 画面

本画面は、SIM グループ内のデバイスが他のグループやデバイスとどのように接続しているかを表示します。

本画面で表示されるアイコンは以下の通りです。

アイコン	説明
	グループ
	レイヤ 2 Commander スイッチ
	レイヤ 3 Commander スイッチ
	他のグループの Commander スイッチ
	レイヤ 2 Member スイッチ
	レイヤ 3 Member スイッチ
	他のグループの Member スイッチ
	レイヤ 2 Candidate スイッチ
	レイヤ 3 Candidate スイッチ
	不明なデバイス
	SIM 非対応のデバイス

ツールヒント

ツリービュー画面では、マウスはデバイス情報の確認と設定のために重要な役割を果たします。トポロジ画面の特定のデバイス上にマウスポインタを指定すると、ツリービューと同様にデバイス情報（ツールヒント）を表示します。以下にその例を示します。

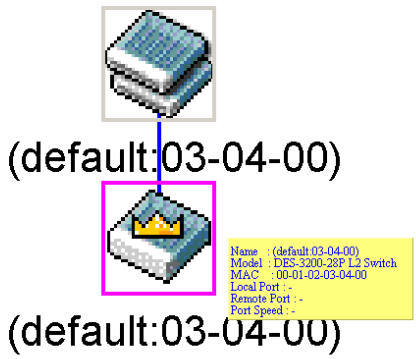


図 7-17　ツールヒントを利用したデバイス情報の表示

2 つのデバイスの間のライン上でマウスポインタを静止させると、以下の図のようにデバイス間の接続速度を表示します。

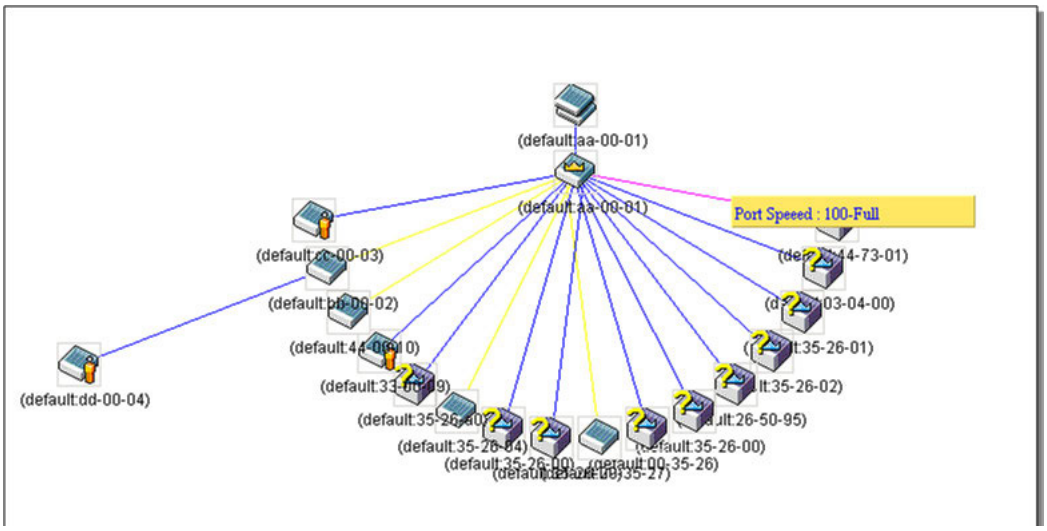


図 7-18　ツールヒントを利用したポート速度の表示

右クリックメニュー

デバイスのアイコン上で右クリックすると、SIM グループ内でのスイッチの役割や、関連付けられているアイコンの種類に応じた様々な機能を実行できます。

グループアイコン

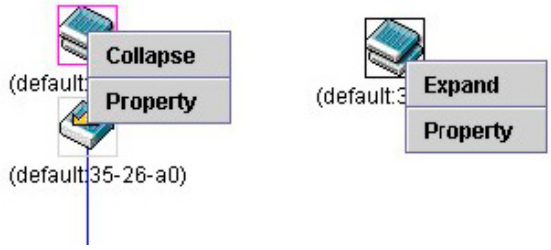


図 7-19　グループアイコン上での右クリック

以下のオプションが表示されます。

- Collapse – グループのアイコンを折りたたみ、1 つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Property – ポップアップ画面が開き、グループ情報を表示します。

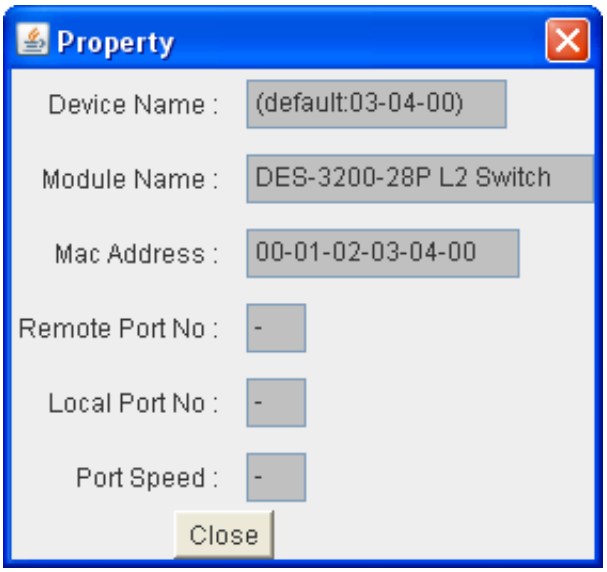


図 7-20　Property 画面

画面には以下の情報が表示されます。

項目	説明
Device Name	ユーザが設定した SIM グループ内のスイッチのデバイス名を表示します。デバイス名がない場合は、「default」が与えられ、識別のために MAC アドレスの終わり 6 桁が付加されます。
Module Name	右クリックされたスイッチのモジュール名を表示します。
Mac Address	対応するスイッチの MAC アドレスを表示します。
Remote Port No	CS が接続している MS または CaS の物理ポートの番号を表示します。CS の場合は何も表示されません。
Local Port No	MS または CaS が接続している CS の物理ポートの番号を表示します。CS の場合は何も表示されません。
Port Speed	CS と MS/CaS 間の接続スピードを表示します。

「Close」ボタンをクリックし、「Property」画面を閉じます。

Commander スイッチアイコン

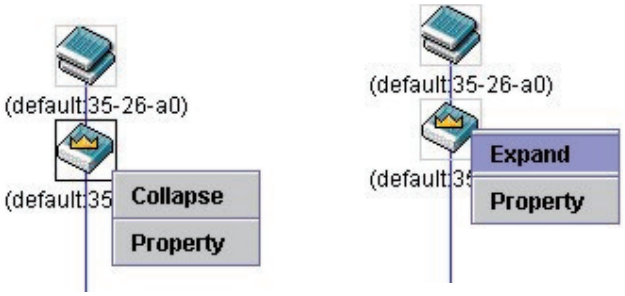


図 7-21　Commander スイッチアイコン上での右クリック

以下のオプションが表示されます。
- Collapse – グループのアイコンを折りたたみ、1 つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Property – ポップアップ画面が開き、グループの情報を表示します。

Member スイッチアイコン

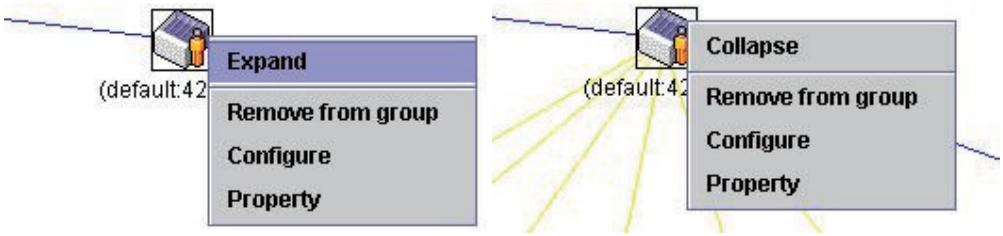


図 7-22　Member スイッチアイコン上での右クリック

以下のオプションが表示されます。
- Collapse – グループのアイコンを折りたたみ、1 つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Remove from group – メンバをグループから削除します。
- Configure - Web 管理機能を起動して、スイッチの設定を可能にします。
- Property – ポップアップ画面が開き、デバイスの情報を表示します。

Candidate スイッチアイコン

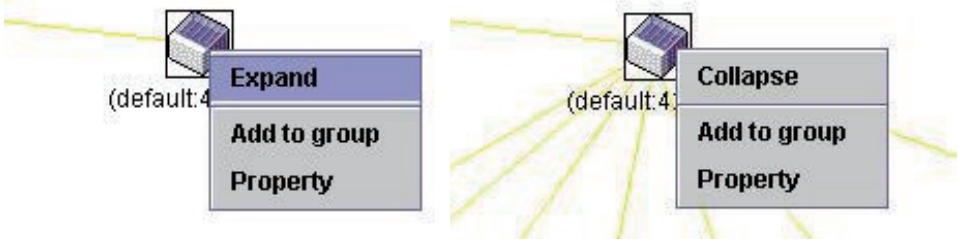


図 7-23　Candidate スイッチアイコン上での右クリック

以下のオプションが表示されます。
- Collapse – グループのアイコンを折りたたみ、1 つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Add to group – CaS をグループに追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS スイッチを SIM グループに追加するための認証を行います。パスワードを入力して「OK」ボタンをクリックするか、「Cancel」ボタンをクリックして画面を閉じます。

図 7-24　Input password ダイアログボックス

- Property – ポップアップ画面が開き、デバイスの情報を表示します。

メニューバー

「Single IP Management」画面には、デバイスの設定のために以下のようなメニューバーが配置されています。

図 7-25　トポロジビュー内のメニューバー

メニューバーには以下の 5 つのメニューが存在します。

「File」メニュー
- Print Setup – 印刷イメージを表示します。
- Print Topology – トポロジマップを印刷します。
- Preference – ポーリング間隔、SIM 起動時にオープンするビューなどの表示プロパティを設定します。

「Group」メニュー
- Add to Group – グループに CaS を追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS を SIM グループに追加するための認証を行います。パスワードを入力して「OK」ボタンをクリックするか、「Cancel」ボタンをクリックして画面を閉じます。

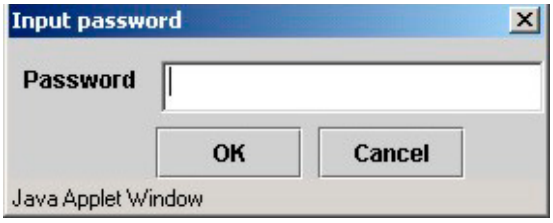


図 7-26　Input password ダイアログボックス

- Remove from Group – MS をグループから削除します。

「Device」メニュー
- Configure – 指定したデバイスの Web マネージャを開きます。

「View」メニュー
- Refresh – ビューを最新の状態に更新します。
- Topology – トポロジビューを表示します。

「Help」メニュー
- About – 現在の SIM バージョンなどの SIM 情報を表示します。

図 7-27　About ダイアログボックス

Firmware Upgrade（ファームウェア更新）

CS から MS へのファームウェアの更新を行います。

Management > Single IP Management > Firmware Upgrade の順にメニューをクリックし、以下の画面を表示します。

図 7-28　Firmware Upgrade 画面

MS は、「ID」、「Port」（MS に接続する CS 上のポート）、「MAC Address」、「Model Name」、「Firmware Version」の情報と共にリスト表示されます。ダウンロード対象のスイッチは、「Port」欄の下のチェックボックスで選択します。ファームウェアを格納する「Server IP Address」を入力して、ファームウェアの「Path\Filename」を指定します。「Download」ボタンをクリックすると、ファイル転送が開始されます。

Configuration File Backup/ Restore（コンフィグレーションファイルの更新）

TFTP サーバを使用して CS から MS にコンフィグレーションファイルのダウンロード / アップロードを行います。

Management > Single IP Management > Configuration File Backup/Restore の順にメニューをクリックし、以下の画面を表示します。

図 7-29　Configuration File Backup/Restore 画面

MS は、「ID」、「Port」（MS に接続する CS 上のポート）、「MAC Address」、「Model Name」、「Firmware Version」の情報と共にリスト表示されます。コンフィグレーションファイルのダウンロード / アップロードために、ファイルをおく「Server IP Address」を入力して、コンフィグレーションファイルの「Path/Filename」を指定します。

「Restore」ボタンをクリックすると、TFTP サーバからのファイル転送が開始されます。
「Backup」ボタンをクリックすると、TFTP サーバへファイル転送が開始されます。

Upload Log File（ログファイルのアップロード）

MS から、指定した PC にログファイルのアップロードを行います。

Management > Single IP Management > Upload Log File の順にメニューをクリックし、以下の画面を表示します。

図 7-30　Upload Log File 画面

ログファイルをアップロードするためには、SIM メンバスイッチの IP アドレスと、ログファイルを保存する PC のパスを入力し、「Upload」ボタンをクリックするとファイル転送が開始されます。

SNMP Settings（SNMP 設定）

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルで、ネットワークデバイスの管理や監視を行います。ネットワーク管理デバイスは、SNMP を利用してゲートウェイ、ルータ、およびその他のネットワークデバイスの設定状態を確認または変更します。また、SNMP を利用してスイッチやスイッチ群、またはネットワークに対し、正常な動作を行うためのシステム設定、パフォーマンスの監視、問題の検出を行います。

SNMP をサポートする管理デバイスは、スイッチ上で動作する SNMP エージェントと呼ばれるソフトウェアを実装しています。SNMP エージェントが管理する定義された変数（管理オブジェクト）により、デバイスの管理を行います。これらのオブジェクトは MIB（Management Information Base）内に定義され、デバイス上の SNMP エージェントにより管理される情報表示の基準を（管理側のデバイスに）伝えます。SNMP では、MIB の仕様と、ネットワークを経由してこれらの情報にアクセスするために使用するプロトコルのフォーマットを定義しています。

本スイッチシリーズは、SNMP バージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）をサポートしています。スイッチの監視と制御に使用する SNMP バージョンを選択することができます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

SNMP バージョン 1 と 2 では、ユーザ認証はパスワードに良く似た「コミュニティ名」を使用して行われます。リモートユーザの SNMP アプリケーションとスイッチの SNMP は同じコミュニティ名を使用する必要があります。認証が行われていない SNMP パケットを受信した場合、そのパケットは廃棄されます。

SNMP バージョン 1 と 2 を使用するスイッチのコミュニティ名の初期値は次の通りです。

- public -（ネットワークデバイス SNMP 管理ソフトに）MIB オブジェクトの読み取り権限が許可されているコミュニティ名です。
- private - MIB オブジェクトの読み取りと書き込みの権限を与えられているコミュニティ名です。

SNMP バージョン 3 では、さらに高度な認証プロセスを採用し、そのプロセスは 2 つのパートに分かれます。最初のパートは SNMP マネージャとして動作することのできるユーザとその属性を掲載したリストを保持し、次のパートではリスト上のユーザの SNMP マネージャとしての権限を記載しています。

スイッチではユーザグループをリストにまとめ、権限を設定します。SNMP のバージョンは SNMP マネージャのグループごとに設定可能です。そのため、SNMP マネージャを “SNMP バージョン 1 を使用して読み取り専用の情報とトラップの受信のみを可能にするグループ” や、“SNMP バージョン 3 を使用して高いセキュリティレベルを与え、読み書き可能にするグループ” など、グループごとに登録することができます。

個別のユーザや SNMP マネージャグループに SNMP バージョン 3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。そのような管理機能の許可または制限は、各 MIB に関連付けられる OID（Object Identifier）を使用して定義します。SNMP バージョン 3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。スイッチでの SNMP バージョン 3 の設定方法については次のセクションを参照してください。

トラップ

トラップとは、スイッチ上で発生したイベントを、ネットワーク管理者に警告するためのメッセージです。イベントには、再起動（誰かが誤ってスイッチの電源を切ってしまった）などの重大なものから、ポートの状態変化を知らせる軽微なものまで幅広い種類があります。スイッチはトラップを生成してトラップ受信者（またはネットワークマネージャ）に送信します。典型的なトラップには、認証の失敗、トポロジの変化、ブロードキャスト / マルチキャストストーム発生などがあります。

MIB

スイッチの MIB には管理情報およびカウンタ情報が格納されています。本スイッチは標準 MIB-II モジュールを使用し、MIB オブジェクトの値は SNMP ベースのネットワーク管理ソフトウェアから読み出されます。標準 MIB-II に加えて、拡張 MIB としてベンダ固有の MIB もサポートします。MIB OID の指定によってもベンダ固有の MIB を取得することができます。MIB の値は読み取り専用、または読み書き可です。

本スイッチシリーズは、スイッチの環境に合わせた柔軟性のある SNMP 管理機能を採用しています。SNMP 管理機能は、ネットワークの要求やネットワーク管理者の好みに合わせてカスタマイズすることができます。SNMP バージョンの選択は、「SNMP V3」メニューから行うことができます。

本スイッチシリーズは、SNMP バージョン 1、2c、および 3 をサポートします。管理者は、スイッチの監視と制御にどの SNMP バージョンを使用するかを指定できます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

SNMP 設定は、Web マネージャの「SNMP Settings」フォルダ下のメニューから行います。SNMP 権限を持ちスイッチへのアクセスを許されたワークステーションに制限を設けることも可能です。

SNMP Global Settings（SNMP グローバル設定）

SNMP グローバルステート設定を有効または無効にします。

1. **Management > SNMP Settings > SNMP Global Settings** の順にメニューをクリックし、以下の画面を表示します。

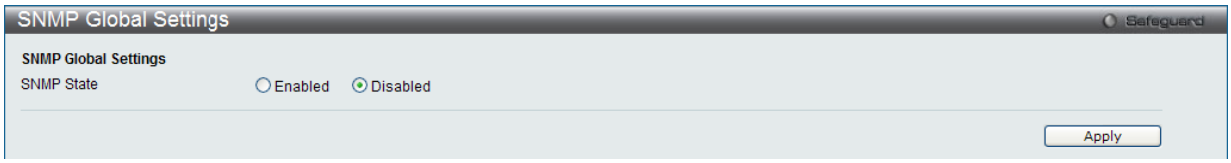


図 7-31　SNMP Global Settings 画面

2. 以下の項目を設定します。

項目	説明
SNMP State	SNMP 機能を使用するためには本オプションを有効にします。

「Apply」ボタンをクリックして行った変更を適用します。

SNMP Trap Settings（SNMP トラップ設定）

スイッチの SNMP 機能のトラップ設定を有効または無効にします。

1. **Management > SNMP Settings > SNMP Trap Settings** の順にメニューをクリックし、以下の画面を表示します。

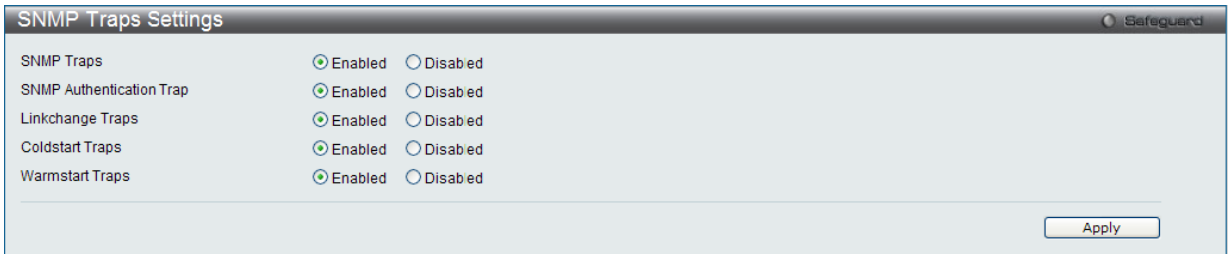


図 7-32　SNMP Traps Settings 画面

2. 以下の項目を設定します。

項目	説明
SNMP Traps	SNMP トラップ機能を使用するためには本オプションを有効にします。
SNMP Authentication Trap	SNMP 認証トラップ機能を使用するためには本オプションを有効にします。
Linkchange Traps	SNMP リンクチェンジトラップ機能を使用するためには本オプションを有効にします。
Coldstart Traps	SNMP コールドスタートトラップ機能を使用するためには本オプションを有効にします。
Warmstart Traps	SNMP ウォームスタートトラップ機能を使用するためには本オプションを有効にします。

「Apply」ボタンをクリックして行った変更を適用します。

SNMP Linkchange Traps Settings（SNMP リンクチェンジトラップ設定）

SNMP リンクチェンジトラップを設定します。

1. **Management > SNMP Settings > SNMP Linkchange Traps Settings** の順にメニューをクリックし、以下の画面を表示します。

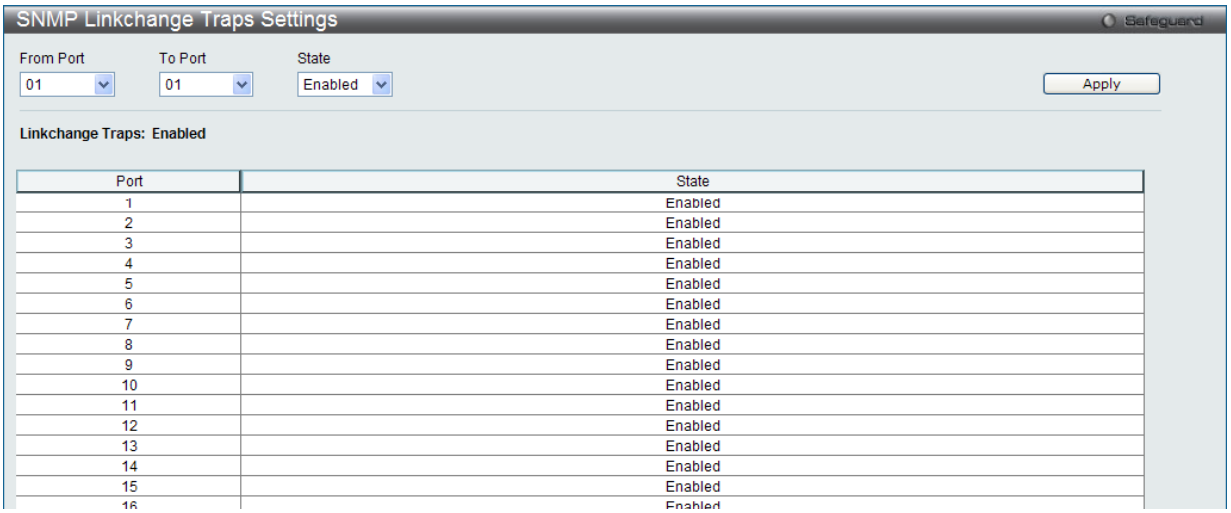


図 7-33　SNMP Linkchange Traps Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port / To Port	使用する開始 / 終了ポートを選択します。
State	SNMP リンクチェンジトラップを有効または無効にします。

「Apply」ボタンをクリックして行った変更を適用します。

SNMP View Table Settings（SNMP ビューテーブル）

コミュニティ名に対しビュー（アクセスできる MIB オブジェクトの集合）を割り当て、リモート SNMP マネージャがどの MIB オブジェクトにアクセスするかを定義するために使用します。

Management > SNMP Settings > SNMP View Table Settings の順にメニューをクリックし、以下の画面を表示します。

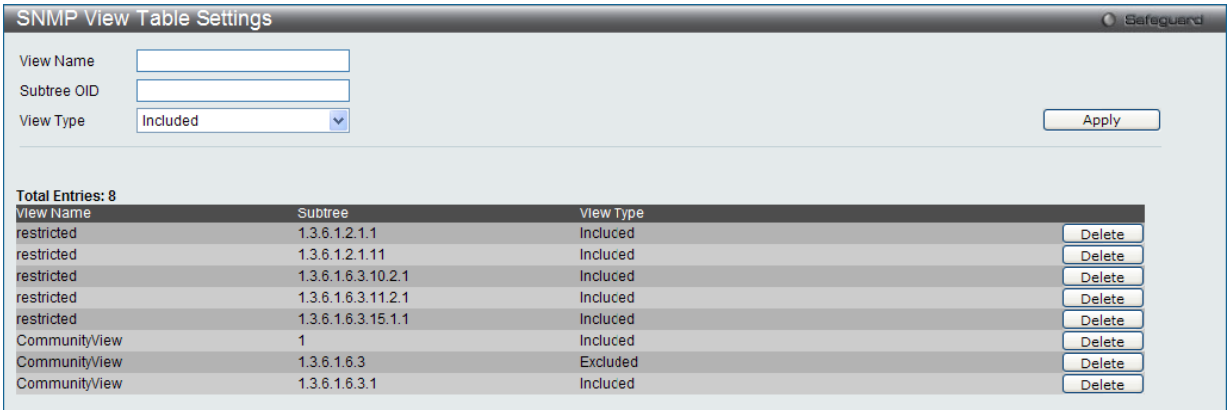


図 7-34　SNMP View Table Settings 画面

エントリの削除

「SNMP View Table Settings」画面のエントリを削除するためには、エントリの行の「Delete」ボタンをクリックします。

エントリの新規作成
新しいエントリを作成するためには、上記テーブルに情報を入力し、「Apply」ボタンをクリックします。

SNMP ユーザ（「SNMP User Table」で設定）と本画面で登録するビューは、「SNMP Group Table」によって作成する SNMP グループによって関連付けます。

以下の項目が使用されます。

項目	説明
View Name	32 文字までの半角英数字を入力します。新しい SNMP ビューを登録し、識別する際に使用します。
Subtree OID	ビューの OID（Object Identifier）サブツリーを入力します。OID は、オブジェクトツリー（MIB ツリー）が SNMP マネージャによってアクセス可能な範囲かどうかを識別します。
View Type	「Subtree OID」で指定した OID が、SNMP マネージャがアクセス可能な範囲であるかを指定します。 • Included - アクセス可能になります。 • Excluded - アクセス不可になります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SNMP Community Table Settings（SNMP コミュニティテーブル設定）

定義済みの SNMP コミュニティテーブルの参照、および、SNMP マネージャとエージェントの関係を定義する SNMP コミュニティ名を登録します。コミュニティ名は、スイッチのエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。

- コミュニティ名を使用して、スイッチの SNMP エージェントにアクセスを行う SNMP マネージャの IP アドレスが掲載されるアクセスリスト。
- MIB オブジェクトのすべてのサブセットを定義する MIB ビューは SNMP コミュニティにアクセス可能である。
- SNMP コミュニティにアクセス可能な MIB オブジェクトが Read/Write または Read-only レベルである。

エントリの設定
「SNMP Community Table」画面でコミュニティエントリを設定します。

Management > SNMP Settings > SNMP Community Table Settings の順にクリックし、以下の画面を表示します。

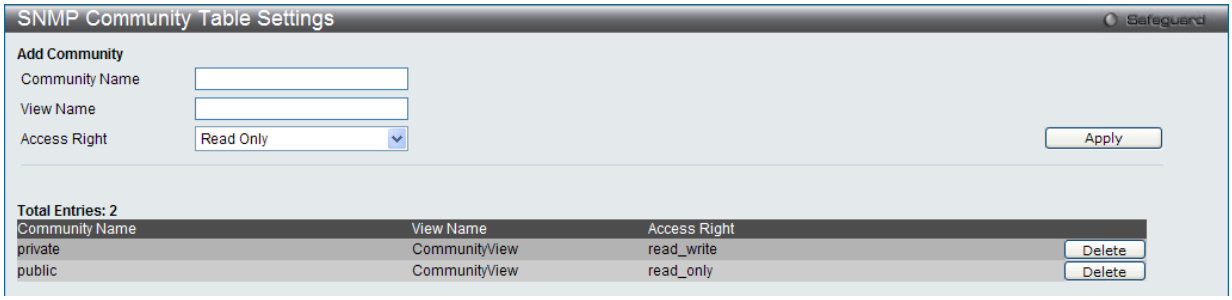


図 7-35　SNMP Community Table Settings 画面

以下の項目が使用されます。

項目	説明
Community Name	32 文字までの半角英数字を入力し、SNMP コミュニティメンバを識別します。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
View Name	32 文字までの半角英数字を入力します。本値は、リモート SNMP マネージャがアクセスすることのできる MIB グループの定義に使用します。View Name は「SNMP View Table」に存在する必要があります。
Access Right	• Read Only - 指定した「Community Name」を使用する SNMP コミュニティメンバは、スイッチの MIB の内容について読み出しのみ可能となります。 • Read Write - 指定した「Community Name」を使用する SNMP コミュニティメンバは、スイッチの MIB の内容について読み出し、および書き込みが可能です。

「Apply」ボタンをクリックし、新しい SNMP コミュニティテーブル設定を適用します。

エントリの削除
削除するエントリ横の「Delete」ボタンをクリックし、エントリを削除します。

SNMP Group Table Settings（SNMP グループテーブル）

SNMP グループを登録します。本グループは、SNMP ユーザ（「SNMP User Table」で設定）と「SNMP View Table」で設定するビューを関連付けるものです。

Management > SNMP Settings > SNMP Group Table Settings の順にメニューをクリックし、以下の画面を表示します。

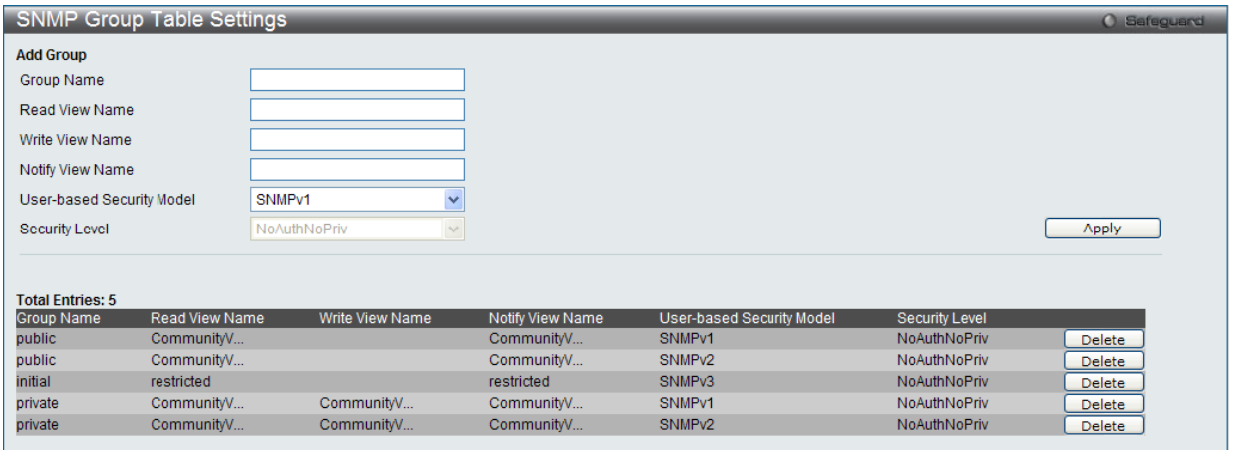


図 7-36　SNMP Group Table Settings 画面

エントリの削除

削除するエントリの行の「Delete」ボタンをクリックします。

エントリの新規登録

新規エントリを追加するためには、上記画面に情報を入力し、「Apply」ボタンをクリックします。

以下の項目が使用されます。

項目	説明
Group Name	32 文字までの半角英数字を入力します。SNMP ユーザのグループの識別に使用します。
Read View Name	SNMP メッセージを要求する SNMP グループ名を入力します。
Write View Name	スイッチの SNMP エージェントに書き込み権限を与える SNMP グループ名を入力します。
Notify View Name	スイッチの SNMP エージェントによるトラップメッセージを送信する SNMP グループ名を入力します。
User-based Security Model	• SNMPv1 - SNMP バージョン 1 が使用されます。 • SNMPv2 - SNMP バージョン 2c が使用されます。SNMP バージョン 2 は集中型、分散型どちらのネットワーク管理にも対応します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。 • SNMPv3 - SNMP バージョン 3 が使用されます。ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。
Security Level	セキュリティレベル設定は SNMP バージョン 3 にのみ適用されます。 • NoAuthNoPriv - 認証なし。スイッチとリモート SNMP マネージャ間の暗号化パケットの送信もないことを示します。 • AuthNoPriv - 認証あり。スイッチとリモート SNMP マネージャ間の暗号化パケットの送信がないことを示します。 • AuthPriv - 認証あり。スイッチとリモート SNMP マネージャ間のパケットも暗号化されて送信されることを示します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SNMP Engine ID Settings（SNMP エンジン ID 設定）

エンジン ID は、SNMP バージョン 3 で使用される場合に定義される固有の識別名です。識別名は半角英数字の文字列で表記され、スイッチ上の SNMP エンジン（エージェント）を識別するために使用します。

Management > SNMP Settings > SNMP Engine ID Settings の順にメニューをクリックし、以下の画面でスイッチの SNMP エンジン ID を表示します。

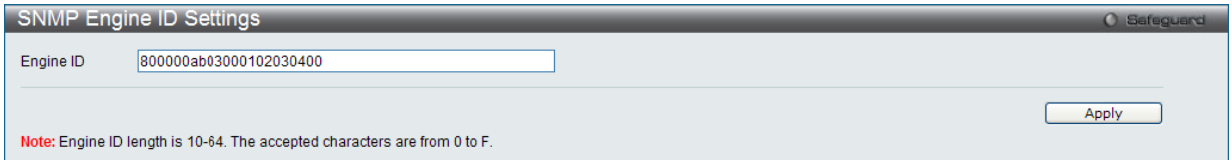


図 7-37　SNMP Engine ID Settings 画面

以下の項目を使用します。

項目	説明
Engine ID	スイッチの SNMP エンジンの識別子を表示します。初期値は RFC2271 にて提示されています。 一番最初のビットは 1 で、最初の 4 つのオクテットには、IANA が割り当てるエージェントの SNMP マネジメントのプライベートエンタープライズ番号 (D-Link は 171) に相当する 2 進数が設定されます。5 番目のオクテットは 03 で、残りがこのデバイスの MAC アドレスであることを示しています。6 ～ 11 番目のオクテットは MAC アドレスです。

エンジン ID を変更するためには、新しいエンジン ID を入力し、「Apply」ボタンをクリックします。

注意　エンジン ID 長は 10-64 で、0 ～ F の文字が許可されます。

SNMP User Table Settings（SNMP ユーザテーブル設定）

SNMP ユーザを登録します。また、スイッチに現在設定されているすべての SNMP ユーザを表示します。

Management > SNMP Settings > SNMP User Table Settings の順にメニューをクリックし、以下の画面を表示します。

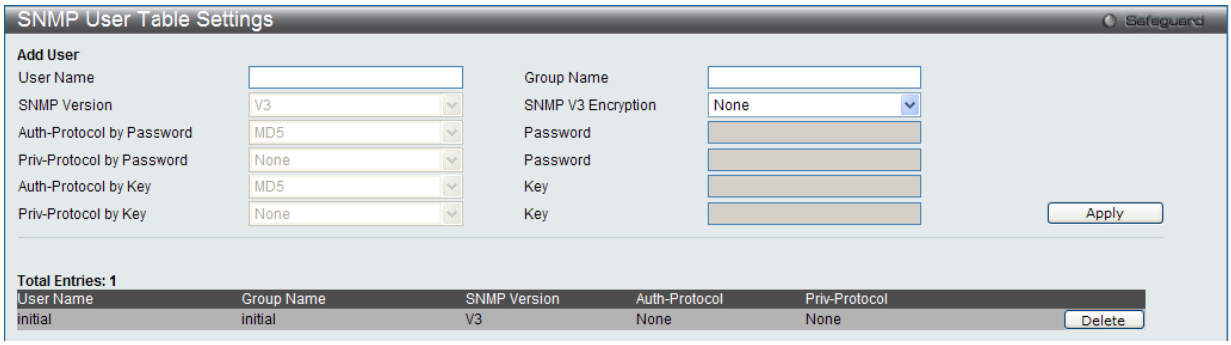


図 7-38　SNMP User Table Settings 画面

エントリの削除

「SNMP User Table」からエントリを削除するためには、エントリの行の「Delete」ボタンをクリックします。

エントリの新規登録

新規エントリを追加するためには、上記画面に情報を入力し、「Apply」ボタンをクリックします。

以下の項目があります。

項目	説明
User Name	32 文字までの半角英数字。SNMP ユーザを識別します。
Group Name	作成した SNMP グループが SNMP メッセージを要求するために使用される名前です。
SNMP Version	• V1 - SNMP バージョン 1 が使用されています。 • V2 - SNMP バージョン 2 が使用されています。 • V3 - SNMP バージョン 3 が使用されています。
SNMP V3 Encryption	SNMP V3 に対して暗号化を有効にします。本項目は「SNMP Version」で「V3」を選択した場合に有効になります。 • None - ユーザ認証は使用しません。 • Key - HMAC-MD5 アルゴリズムまたは HMAC-SHA-96 アルゴリズムレベルのユーザ認証を行います。 • Password - HMAC-SHA-96 アルゴリズムレベルのパスワードか HMAC-MD5-96 パスワードによる認証を行います。
Auth-Protocol by Password/Key	本項目は「SNMP Version」で「V3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。本項目を選択後、「Password」/「Key」にパスワードを入力します。 • MD5 - HMAC-MD5-96 認証レベルが使用されます。 • SHA - HMAC-SHA 認証プロトコルが使用されます。
Priv-Protocol by Password/Key	本項目は「SNMP Version」で「V3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 • None - 認証プロトコルは使用されていません。 • DES - CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されています。本項目を選択後、「Password」/「Key」にパスワード（半角英数字 8-16 文字）を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SNMP Host Table Settings（SNMP ホストテーブル設定）

IPv4 用の SNMP トラップの送信先を設定します。

Management > SNMP Settings > SNMP Host Table Settings の順にメニューをクリックし、以下の画面を表示します。

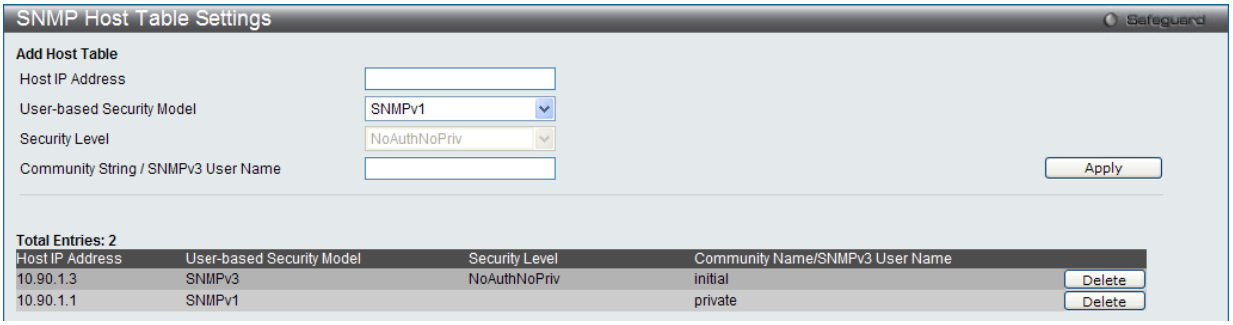


図 7-39　SNMP Host Table Settings 画面

エントリの新規登録

スイッチの SNMP ホストテーブルに新しいエントリを追加するためには、上記画面に情報を入力し、「Apply」ボタンをクリックします。

以下の項目を設定します。

項目	説明
Host IP Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IP アドレスを入力します。
User-based Security Model	• SNMPv1 - SNMP バージョン 1 が使用されます。 • SNMPv2c - SNMP バージョン 2c が使用されます。 • SNMPv3 - SNMP バージョン 3 が使用されます。
Security Level	• NoAuthNoPriv - NoAuth-NoPriv セキュリティレベルが使用されます。 • AuthNoPriv - Auth-NoPriv セキュリティレベルが使用されます。 • AuthPriv - Auth-Priv セキュリティレベルが使用されます。
Community String/ SNMPv3 User Name	コミュニティ名または SNMP V3 ユーザ名を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

エントリの削除

エントリを削除するためには、該当するエントリの行の「Delete」ボタンをクリックします。

RMON Settings（RMON 設定）

スイッチにおける SNMP 機能の上昇 / 下降アラームトラップに対するリモートモニタリング (RMON) を有効または無効にします。

Management > SNMP Settings > RMON Settings の順にメニューをクリックし、以下の画面を表示します。

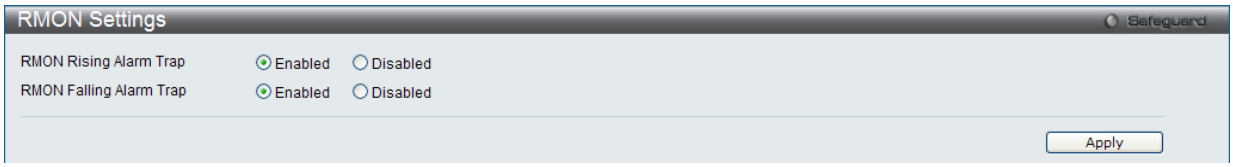


図 7-40　RMON Settings 画面

以下の項目を設定します。

項目	説明
RMON Rising Alarm Trap	RMON 上昇アラームトラップ機能を使用するためには本オプションを有効にします。
RMON Falling Alarm Trap	RMON 下降アラームトラップ機能を使用するためには本オプションを有効にします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Telnet Settings（Telnet 設定）

スイッチに Telnet 設定をします。

Management > Telnet Settings の順にメニューをクリックし、以下の画面を表示します。

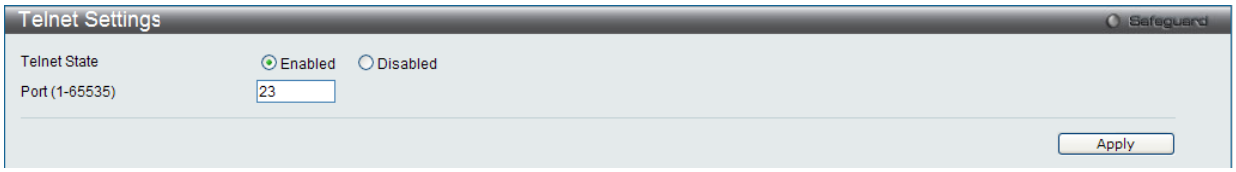


図 7-41　Telnet Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Telnet State	Telnet 設定は初期値で「Enabled」（有効）です。Telnet 経由のシステム設定を許可しない場合は、「Disabled」（無効）を選択します。
Port (1-65535)	スイッチの Telnet 管理に使用される TCP ポート番号。Telnet プロトコルに通常使用される TCP ポートは 23 です。

「Apply」ボタンをクリックし、Telnet 設定を適用します。

Web Settings（Web 設定）

スイッチに Web ステータスを設定します。

Management > Web Settings の順にクリックし、以下の画面を表示します。

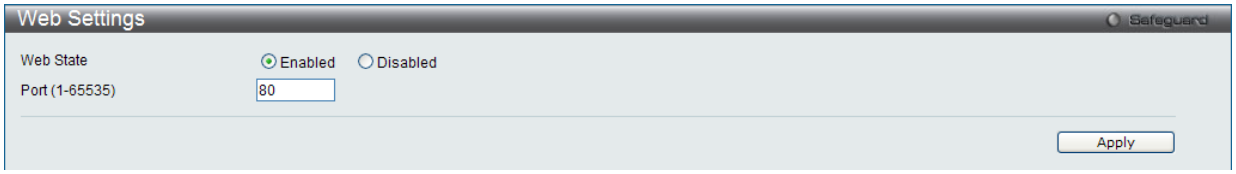


図 7-42　Web Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Web State	Web ベースマネジメントは初期値で「Enabled」（有効）です。「Disabled」を選択してステータスを無効にすると、設定はすぐに適用され、Web インタフェースを使用したシステムの設定はできなくなります。
Port (1-65535)	スイッチの Web ベースマネジメントに使用される TCP ポート番号。Web プロトコルに通常使用される TCP ポートは 80 です。

「Apply」ボタンをクリックし、Web 設定を適用します。

第 8 章　L2 Features（L2 機能の設定）

L2 Features メニューを使用し、本スイッチにレイヤ 2 機能を設定することができます。

以下は L2 Features サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
VLAN（VLAN 設定）	802.1Q スタティック VLAN 設定を行います。以下のメニューがあります。 802.1Q VLAN Settings（802.1Q VLAN 設定）、802.1v Protocol VLAN（802.1v プロトコル VLAN）、GVRP（GVRP の設定）、MAC-based VLAN Settings（MAC ベース VLAN 設定）、PVID Auto Assign Settings（PVID 自動割り当て設定）、VLAN Trunk Settings（VLAN トランク設定）、Browse VLAN（VLAN の参照）、Show VLAN Ports（VLAN ポートの参照）	87
QinQ（QinQ 設定）	Q-in-Q 機能を有効または無効にします。次のメニューがあります。 QinQ Settings（QinQ 設定）、VLAN Translation Settings（VLAN 変換機能の設定）	96
Layer 2 Protocol Tunneling Settings（レイヤ 2 プロトコルトンネリング設定）	レイヤ 2 プロトコルトンネリング機能を設定します。	99
Spanning Tree（スパニングツリーの設定）	スパニングツリープロトコルの設定を行います。以下のメニューがあります。 STP Bridge Global Settings（STP ブリッジグローバル設定）、STP Port Settings（STP ポートの設定）、MST Configuration Identification（MST の設定）、STP Instance Settings（STP インタンス設定）、MSTP Port Information（MSTP ポート情報）	100
Link Aggregation（ポートトランキングの設定）	ポートトランキング設定を行います。以下のメニューがあります。 Port Trunking Settings（ポートトランキング設定）、LACP Port Settings（LACP ポートの設定）	107
FDB（FDB 設定）	スタティック FDB、MAC アドレスエージングタイム、MAC アドレステーブルなどを設定します。以下のメニューがあります。 Static FDB Settings（スタティック FDB の設定）、MAC Notification Settings（MAC 通知設定）、MAC Address Aging Time Settings（MAC アドレスエージングタイムの設定）、MAC Address Table（MAC アドレステーブル）、ARP & FDB Table（ARP と FDB テーブル）	110
L2 Multicast Control（L2 マルチキャストコントロール）	IIGMP Snooping、MLD Snooping の設定を行います。以下のメニューがあります。 IGMP Snooping（IGMP Snooping の設定）、MLD Snooping（MLD Snooping 設定）、IP Multicast VLAN Replication（IP マルチキャスト VLAN レプリケーション）	115
Multicast Filtering（マルチキャストフィルタリング）	マルチキャストフィルタリングの設定を行います。以下のメニューがあります。 IPv4 Multicast Filtering（IPv4 マルチキャストフィルタリング）、IPv6 Multicast Filtering（IPv6 マルチキャストフィルタリング）、Multicast Filtering Mode（マルチキャストフィルタリングモード）	133
ERPS Settings（イーサネットリングプロテクション設定）	イーサネットリングプロテクション設定を有効にします。	145
LLDP（LLDP 設定）	LLDP 設定を行います。	144
NLB FDB Settings（NLB FDB 設定）	NLB 機能を設定します。	151

VLAN について

IEEE 802.1p プライオリティについて

IEEE 802.1p 標準規格において定義され何種類ものデータが同時に送受信されるようなネットワーク内で、トラフィックを管理するための方法です。本機能は混雑したネットワーク上でのタイムクリティカルなデータの伝送時に発生する問題を解決するために開発されました。例えばビデオ会議のような、タイムクリティカルなデータに依存するタイプのアプリケーションの品質は、ほんの少しの伝送遅延にも多大な影響を受けてしまいます。

IEEE 802.1p 標準規格に準拠するネットワークデバイスは、データパケットのプライオリティレベル（優先度）を認識することができます。また、これらのデバイスはパケットに対してプライオリティレベルやタグを割り当てることができ、パケットからタグを取り外すことも可能です。このプライオリティタグ（優先タグ）は、パケットの緊急度を決定し、またそのパケットがどのキューに割り当てられるかを決定します。

プライオリティタグは、0 から 7 までの値で示され、0 が最も低い優先度、7 が最も高い優先度を表します。一般的に、7 番のプライオリティタグは、少しの遅延にも影響されやすい音声や映像に関わるデータに対して、またはデータ転送速度が保証されているような特別なユーザに対して使用されます。

本スイッチでは、プライオリティタグ付きのパケットをご使用のネットワークでどのように扱うかを細かく調整することができます。プライオリティタグ付きのデータをキューの使用によって管理することにより、ご使用のネットワークのニーズに合わせて優先度を設定できます。1 つのキューに複数の異なるタグを使用したパケットを関連付ける方が効果のある場合もありますが、一般的には最高の優先度のキュー（キュー 7）には、プライオリティレベル 7 のパケットに割り当てることをお勧めします。プライオリティを与えられないパケットはキュー 0 に割り当てられ、最も低い送信優先度となります。

スイッチは Strict モードと WRR（重み付けラウンドロビン）機能をサポートし、それによりキューからパケットを送信する速度を決定します。速度の対比は 4 : 1 と設定されています。これは、最高のプライオリティのキュー（キュー 7）が 4 つのパケットを送信する間に、キュー 0 では 1 つのパケットを送信することを意味しています。

プライオリティキューの設定はスイッチ上のすべてのポートに対して行われるため、スイッチに接続されるすべてのデバイスがその影響を受けることに注意してください。このプライオリティキューイングシステムは、ご使用のネットワークがプライオリティタグ割り当て機能をサポートする場合、この機能は特にその効果を発揮します。

VLAN とは

VLAN（Virtual Local Area Network : 仮想 LAN）とは、物理的なレイアウトではなく、論理的なスキームに従って構成されるネットワークトポロジです。VLAN は LAN セグメントの集まりを自律的なユーザグループへと結合させて、1 つの LAN のように見せるために使用します。また、VLAN は VLAN 内のポート間にのみパケットが送信されるように、ネットワークを異なるブロードキャストドメインに論理的に分割します。一般的には 1 つの VLAN は 1 つのサブネットと関連付けられます。

VLAN では、帯域を浪費しないでことによりパフォーマンスを強化し、トラフィックを特定のドメイン内に制限することにより、セキュリティを増強します。

VLAN はエンドノードを物理的位置ではなく、論理的に束ねた集合体です。頻繁に通信を行うエンドノード同士は、それらのネットワーク上の物理的位置に関わらず、同じ VLAN を割り当てます。論理的には、VLAN とブロードキャストドメインは等しいと言えます。これは、ブロードキャストパケットはブロードキャストが行われた VLAN 内のメンバにのみ送信されるためです。

本スイッチシリーズにおける VLAN について

どんな方法でエンドノードの識別を行い、エンドノードに VLAN メンバシップを割り当てたとしても、VLAN 間にルーティング機能を持つネットワークデバイスが存在しない限り、パケットは VLAN に所属しないポートに送信されることはありません。

本スイッチシリーズは IEEE 802.1Q 標準で規定する VLAN とポートベース VLAN をサポートします。ポートタグ取り機能は、パケットヘッダから 802.1Q タグを取り外すことにより、タグを理解しないデバイスとの互換性を保ちます。

スイッチの初期状態では、すべてのポートに「default」と名付けられた 802.1Q VLAN が割り当てられています。
「default」VLAN の VID は 1 です。

IEEE 802.1Q VLAN

用語の説明

- タグ付け - パケットのヘッダに 802.1Q VLAN 情報を挿入すること。
- タグ取り - パケットのヘッダから 802.1Q VLAN 情報を削除すること。
- イングレスポート - スイッチ上のパケットを受信するポート。VLAN の照合が行われます。
- イーグレスポート - スイッチ上のパケットを送信するポート。タグ付けの決定が行われます。

本スイッチ上では、IEEE 802.1Q（タグ付き）VLAN が実装されています。ネットワーク上のすべてのスイッチが IEEE 802.1Q 準拠である場合、ネットワーク全体に 802.1Q VLAN が有効となります。

VLANは、ネットワークを分割し、ブロードキャストドメインのサイズを縮小します。あるVLANに到着するすべてのパケットは、（IEEE 802.1Qをサポートするスイッチを通して）そのVLANのメンバであるステーションに送信されます。これには、送信元の不明なブロードキャスト、マルチキャスト、ユニキャストパケットも含まれます。
さらに、ネットワークでのセキュリティ機能を提供します。IEEE 802.1Q VLANは、VLANメンバであるステーションにのみパケットを送信します。

すべてのポートは、タグ付け / タグなしに設定されます。IEEE 802.1Q VLANのタグ取り機能は、パケットヘッダ中のVLANタグを認識しない旧式のスイッチとの連携に使用されます。タグ付け機能により、複数の802.1Q準拠のスイッチを1つの物理コネクションで結びつけ、すべてのポート上でスパニングツリーを有効にします。

IEEE 802.1Q標準では、受信ポートが所属するVLANへのタグなしパケットの送信を禁じています。

IEEE 802.1Q標準規格の主な機能は以下の通りです。
- フィルタリングによりパケットをVLANに割り当てます。
- 全体で1つのスパニングツリーが構成されていると仮定します。
- 1レベルのタグ付けによるタグ付けを行います。
- 802.1Q VLANのパケット転送
- パケットの転送は以下の3つの種類のルールに基づいて決定されます。:
  - イングレスルール - 受け取ったパケットがどのVLANに所属するかの分類に関するルール。
  - ポート間のフォワーディングルール - 転送するかしないかを決定します。
  - イーグレスルール - パケットが送信される時にタグ付きかタグなしかを決定します。

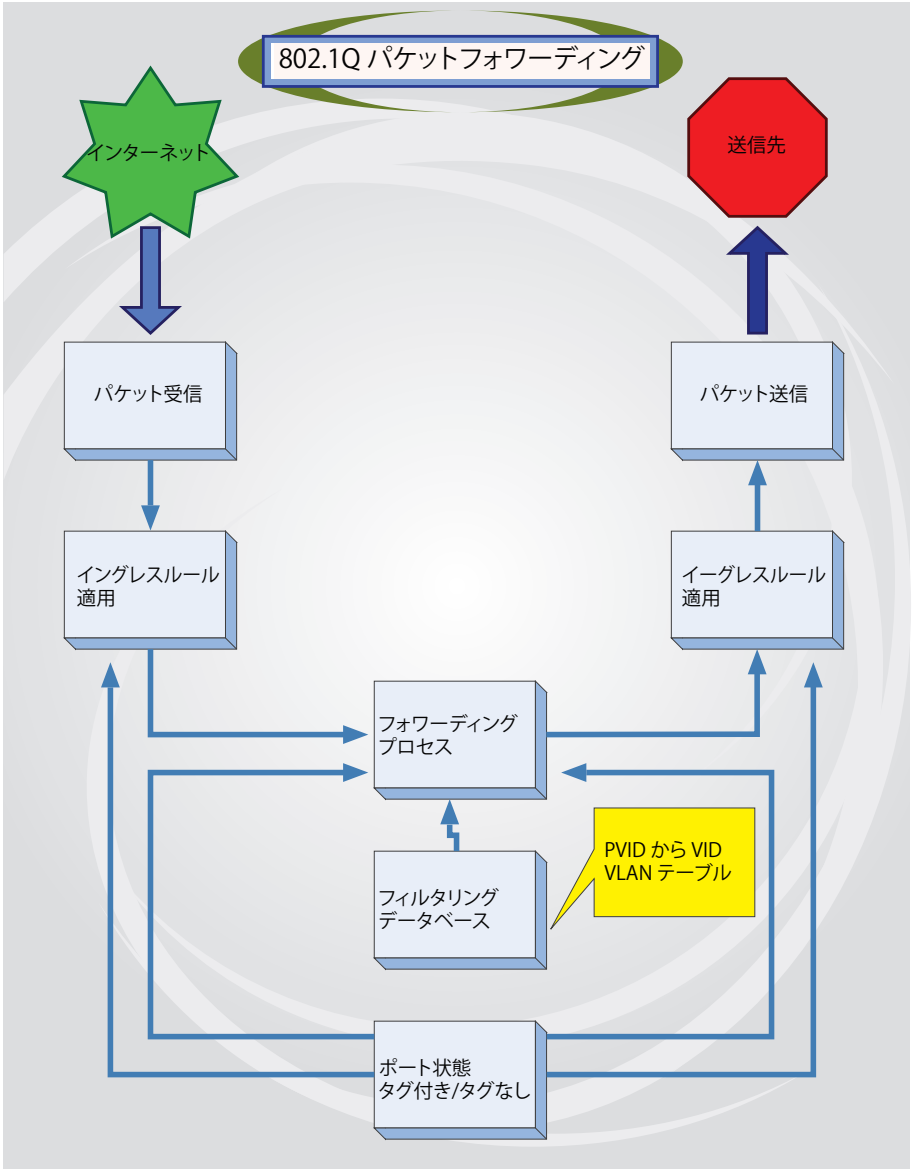


図 8-1　IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

次の図は 802.1Q VLAN のタグについて表示しています。ソース MAC アドレスの後に 4 オクテットのフィールドが挿入されています。それらが存在する場合、EtherType フィールドの値は 0x8100 になります。つまり、パケットの EtherType フィールドが 0x8100 と等しい時に、パケットには IEEE 802.1Q/802.1p タグが含まれています。タグは以下の 2 オクテットに含まれていてユーザプライオリティの 3 ビット、CFI(Canonical Format Identifier: トークンリングパケットをカプセル化してイーサネットバックボーンをはさんで転送するためのもの) の 1 ビット、および VID(VLAN ID) の 12 ビットから成ります。ユーザプライオリティの 3 ビットは 802.1p によって使用されます。VID は VLAN を識別するためのもので 802.1Q 標準によって使用されます。VID は長さ 12 ビットなので 4094 のユニークな VLAN を構成することができます。
タグはパケットヘッダに埋め込まれ、パケット全体は 4 オクテット分長くなります。そして、元々のパケットに含まれていた情報のすべてが保持されます。

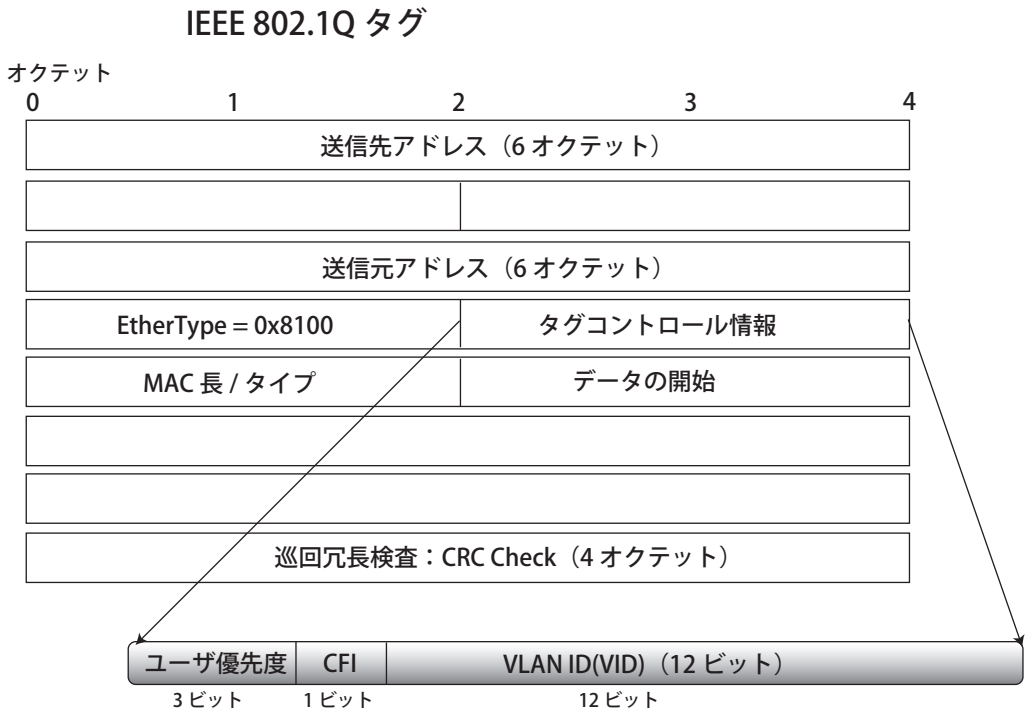


図 8-2　IEEE 802.1Q タグ

EtherType と VLAN ID はソース MAC アドレスと元の Length/EtherType か Logical Link Control の間に挿入されます。パケットは元のものよりも少し長くなるので、CRC は再計算されます。

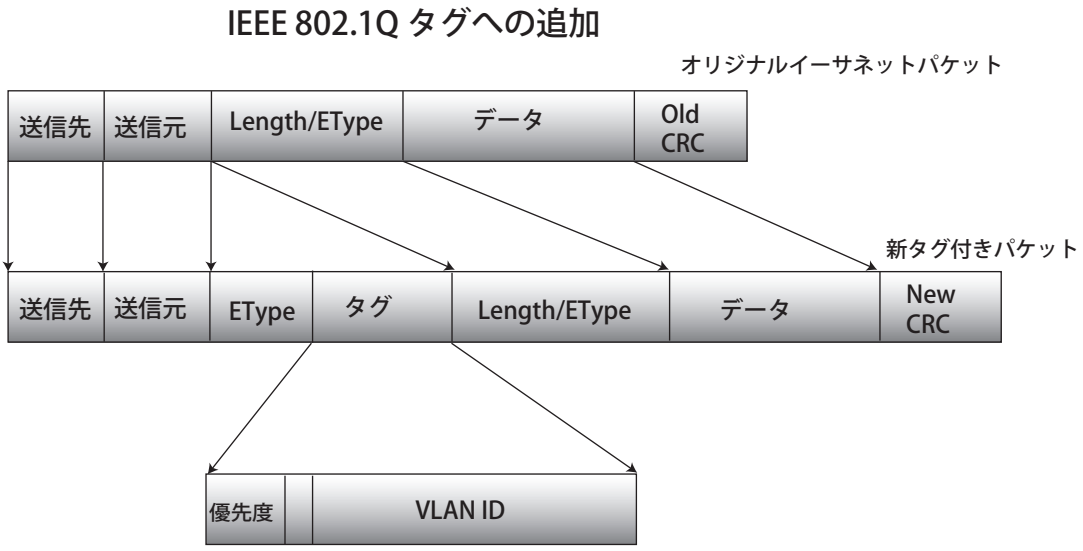


図 8-3　IEEE 802.1Q タグの挿入

ポート VLAN ID

802.1Q VID 情報を持ったタグを付けられたパケットは 802.1Q に対応したネットワークデバイスから他のデバイスまでは完全な VLAN 情報を保持したまま転送することができます。これにより、すべてのネットワークデバイスが 802.1Q に準拠していればネットワーク全体をまるごと 802.1Q VLAN で結ぶことができます。

残念ながら、すべてのネットワークデバイスが 802.1Q に準拠しているわけではありません。これらの 802.1Q 非準拠のデバイスを tag-unaware（タグ認識不可）、802.1Q 準拠のデバイスを tag-aware（タグ認識可能）と呼ぶことにします。

802.1Q VLAN が採用される以前は、ポートベースや MAC ベースの VLAN が主流でした。これらの VLAN でのパケット送信はポート VLAN ID（PVID）を元に行われます。あるポートで受信したパケットには、そのポートの PVID を割り当てて、パケットの宛先アドレス（スイッチのフォワーディングテーブルで参照）へと送信されます。もしパケットを受信したポートの PVID がパケットの宛先のポートの PVID と異なる場合は、スイッチはそのパケットを廃棄します。

スイッチ内では、異なる PVID とは異なる VLAN を意味しています。（2 つの VLAN は外部ルータなしでは通信ができません。）そのため PVID をベースにした VLAN の識別はスイッチ外へ広がる（またはスイッチスタックの）VLAN を実現することができません。

スイッチのすべての物理ポートは PVID を持っています。802.1Q にも PVID が割り当てられ、スイッチ内で使用されます。スイッチ上に VLAN が定義されていなければ、すべてのポートはデフォルト VLAN と PVID 1 が割り当てられます。タグなしのパケットはそれらを受信したポートの PVID を割り当てられます。フォワーディングはこの PVID を元に決定されます。タグ付きのパケットはタグ中に含まれる VID に従って送信されます。タグ付きのパケットにも PVID が割り当てられますが、パケットフォワーディングを決定するのは PVID ではなく VID です。

tag-aware（タグ認識可能）のスイッチはスイッチ内の PVID とネットワークの VID を関係付けるテーブルを保持しなければなりません。スイッチは送信されるパケットの VID と、パケット送信を行うポートの VID を比較します。この 2 つが一致しない場合、スイッチはこのパケットを廃棄します。タグなしパケット用に PVID が存在し、またタグ付きパケット用に VID が存在するので、タグを認識するネットワークデバイスも認識しないデバイスも、同じネットワーク内に共存が可能になります。

PVID は 1 ポートに 1 つしか持てませんが、VID はスイッチの VLAN テーブルメモリが可能なだけ持つことができます。

ネットワーク上にはタグを認識しないデバイスが存在するため、送信するパケットにタグを付けるかどうかの判断は、タグを認識できるデバイスの各ポートで行わなければなりません。送信するポートがタグを認識しないデバイスと接続していれば、タグなしのパケットを送信し、逆にタグを認識するデバイスと接続していれば、タグ付きのパケットを送信します。

タグ付きとタグなし

802.1Q に対応するスイッチのすべてのポートは、タグ付きかタグなしに設定できます。
タグ付きのポートは受信、送信するすべてのパケットのヘッダに、VID、プライオリティ、そしてそのほかの VLAN 情報を埋め込みます。パケットが既にタグ付けされていたなら、VLAN 情報を完全に保つためにポートはパケットを変更しません。ネットワーク上の他の 802.1Q 対応デバイスも、タグの VLAN 情報を使用してパケットの転送を決定します。
タグなしのポートは、受信、送信するすべてのパケットから 802.1Q タグを削除します。パケットに 802.1Q VLAN タグがなければ、ポートはパケットを変更しません。つまり、タグなしのポートが受信して、転送したすべてのパケットは 802.1Q VLAN 情報をまったく持ちません。PVID はスイッチの内部で使用されるだけです。タグなしはパケットを 802.1Q 対応のデバイスから、非対応のデバイスにパケットを送信するのに使用します。

イングレスフィルタリング

スイッチ上のポートの内、スイッチへのパケットの入り口となり、VLAN を照合するポートをイングレスポートと呼びます。イングレスフィルタリングがポート上で有効に設定されていれば、スイッチはパケットヘッダ内の VLAN 情報を参照し、パケットの送信を行うかどうかを決定します。

パケットに VLAN 情報のタグが付加されていれば、イングレスポートはまず、自分自身がそのタグ VLAN のメンバであるかどうかを確認します。メンバでない場合、そのパケットは廃棄されます。イングレスポートが 802.1Q VLAN のメンバであれば、スイッチは送信先ポートが 802.1Q VLAN のメンバであるかどうかを確認します。802.1Q VLAN メンバでない場合は、そのパケットは廃棄されます。送信先ポートが 802.1Q VLAN のメンバであれば、そのパケットは送信され、送信先ポートはそのパケットを接続するネットワークセグメントに転送します。

パケットに VLAN 情報のタグが付加されていない場合は、イングレスポートはそのパケットに VID として自分の PVID を付加します（ポートがタグ付きポートである場合）。するとスイッチは、送信先ポートはイングレスポートと同じ VLAN のメンバであるか（同じ VID を持っているか）を確認します。同じ VLAN メンバでない場合、パケットは廃棄されます。同じ VLAN メンバである場合、パケットは送信され、送信先ポートはそのパケットを接続するネットワークセグメントに転送します。

本プロセスは、イングレスフィルタリングと呼ばれ、同じイングレスポートと同じ VLAN 上のものではないパケットを受信時に廃棄することにより、スイッチ内での帯域を有効利用するために使用されます。これにより送信先ポートに届いてから廃棄されるだけとなるパケットを事前に処理することができるようになります。

デフォルト VLAN

スイッチでは、最初に「default」という名で VID が 1 の VLAN が設定されています。本製品の初期設定ではスイッチ上のすべてのポートが「default」に割り当てられています。新しい VLAN がポートベースモードで設定される時、そのポートは自動的に「default」VLAN から削除されます。

パケットは VLAN 間をまたぐことはできません。ある VLAN のメンバが他の VLAN と接続を行うためには、そのリンクは外部ルータを経由する必要があります。

注意 スイッチ上に 1 つも VLAN が設定されていない場合、すべてのパケットがすべての送信先ポートへと転送されます。宛先アドレスが不明なパケットはすべてのポートに送信されます。ブロードキャストパケットやマルチキャストパケットも、すべてのポートに大量に送信されます。

VLAN の設定例を以下に示します。

VLAN 名	VID	ポート番号
System (default)	1	5、6、7
Engineering	2	9、10
Sales	5	1、2、3、4

ポートベース VLAN

ポートベース VLAN は、スイッチで送受信するトラフィックを制限します。あるポートに接続するすべてのデバイスは、スイッチにコンピュータが 1 台のみ直接接続されている場合でも、ある部署全体が接続されている場合でも、そのポートが所属する VLAN のメンバである必要があります。

ポートベース VLAN では、NIC はパケットヘッダ内の 802.1Q タグを識別できる必要はありません。NIC は通常のイーサネットパケットを送受信します。もしパケットの送信先が同じセグメント上にあれば、通信は通常のイーサネットプロトコルを使用して行われます。通常このように処理が行われますが、パケットの送信先が他のスイッチのポートである場合、スイッチがパケットを廃棄するか、転送を行うかは VLAN の照会を行い決定します。

VLAN セグメンテーション

あるデバイスの VLAN 2 に所属するポート 1 から送信されるパケットを例に説明します。もし、宛先があるポートである場合（通常のフォワーディングテーブル検索により発見）、スイッチはそのポート（ポート 10）は VLAN 2 に所属しているか（つまり VLAN 2 パケットを受け取れるか）どうかを確認します。ポート 10 が VLAN 2 のメンバでない場合は、スイッチはそのパケットを廃棄します。メンバである場合、パケットは送信されます。このように VLAN 基準にそった送信選択機能により VLAN セグメントネットワークが成り立っています。重要なのは、ポート 1 は VLAN 2 にのみ送信を行うということです。

VLAN（VLAN 設定）

802.1Q VLAN Settings（802.1Q VLAN 設定）

802.1Q VLAN を設定します。

L2 Features > VLAN > 802.1Q VLAN Settings の順にメニューをクリックして、以下の画面を表示します。

VLAN リストの表示

「VLAN List」タブでは、既に設定されている VLAN の VLAN ID と VLAN 名が表示されます。

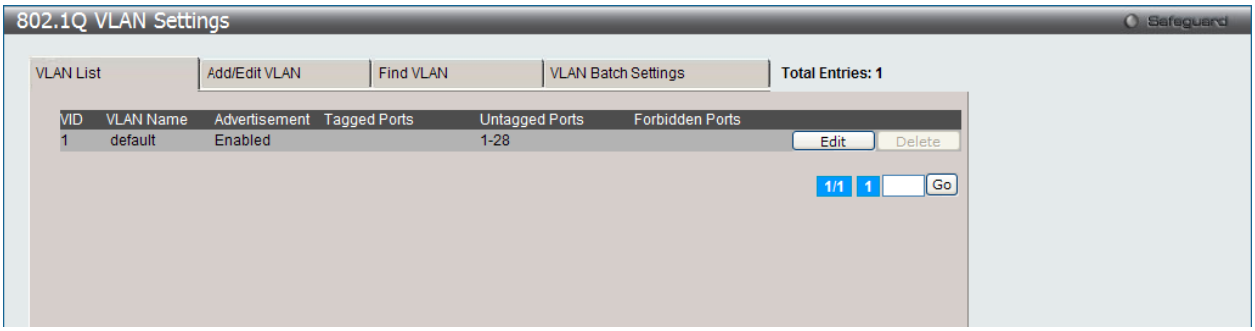


図 8-4　802.1Q VLAN Settings - VLAN List タブ画面

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

新規 / 既存の 802.1Q VLAN の登録

「Add/Edit VLAN」タブをクリックします。新しいタブが以下の通り表示され、ポートの設定、および新しい VLAN の固有名と番号を割り当てることができます。

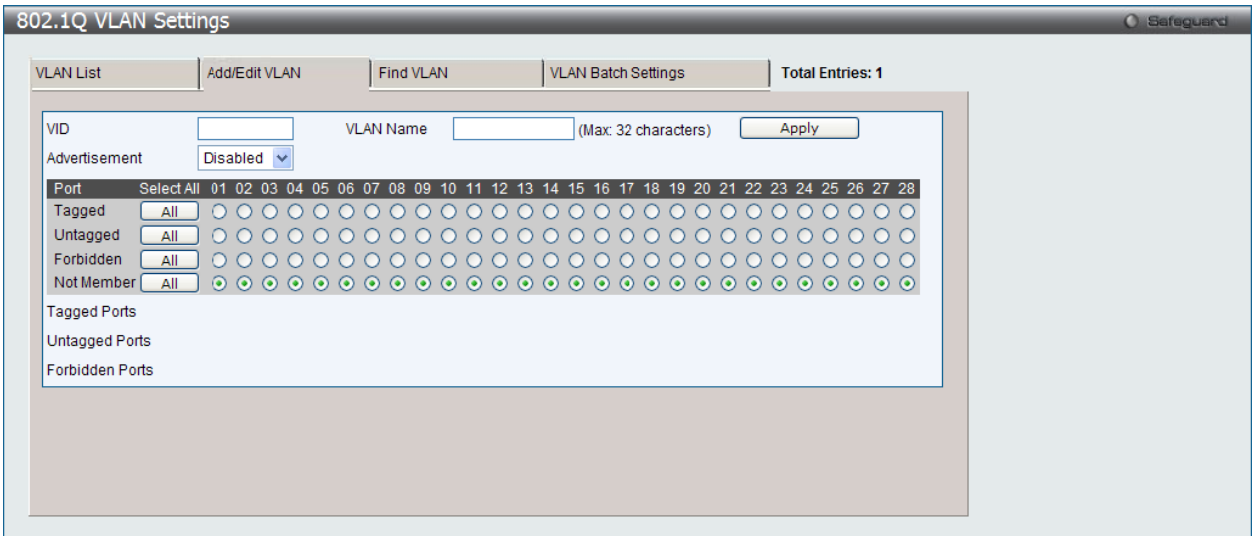


図 8-5　802.1Q VLAN Settings - Add/Edit VLAN タブ画面（Add）

802.1Q VLAN の編集

設定済みの 802.1Q VLAN エントリを変更するためには、「VLAN List」タブで変更する VLAN エントリの横にある「Edit」ボタンをクリックします。

「Add/Edit VLAN」タブには以下の項目が含まれます。

項目	内容
VID	VLAN ID の定義、または定義済みの VLAN の VLAN ID を表示します。VLAN は VID または VLAN 名で識別されます。
VLAN Name	VLAN 名の定義、または VLAN 名の編集をします。ユーザ定義の VLAN 名を定義します。（半角英数字 32 文字以内）
Advertisement	「Enabled」（有効）にすると、外部ソースに GVRP パケットを送信し、既存の VLAN に加わる可能性があることを通知します。
Port	各ポートを以下の通り VLAN のメンバとして定義します。 • Tagged - ポートを 802.1Q タグ付きとして定義します。タグ付きとするポートのボックスをチェックします。 • Untagged - ポートを 802.1Q タグなしとして定義します。タグなしとするポートのボックスをチェックします。 • Forbidden - ポートを VLAN のメンバとならないことを定義し、ダイナミックにポートが VLAN のメンバになることを禁止します。 • Not Member - 各ポートが VLAN メンバでないことを定義します。 • Select All -「All」ボタンをクリックし、すべてのポートを選択します。

「Apply」ボタンをクリックし、デバイスに VLAN 設定を適用します。

VLAN の検索

1. 「Find VLAN」タブをクリックします。以下の画面が表示されます。

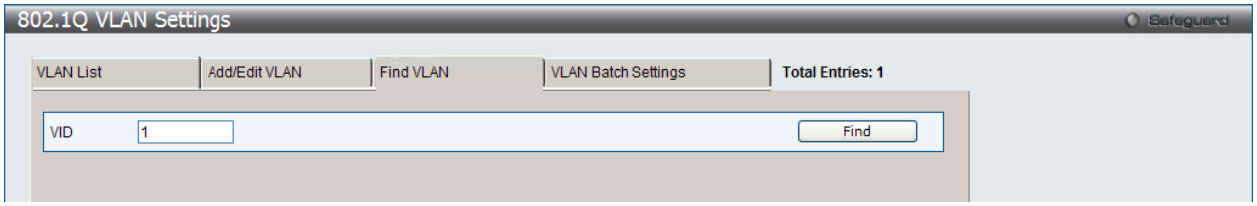


図 8-6　802.1Q VLAN Settings - Find VLAN タブ画面

2. 「VID」を入力し、「Find」ボタンをクリックします。「VLAN List」タブに結果が表示されます。

802.1Q VLAN バッチの作成

「VLAN Batch Settings」タブをクリックし、以下の画面を表示します。

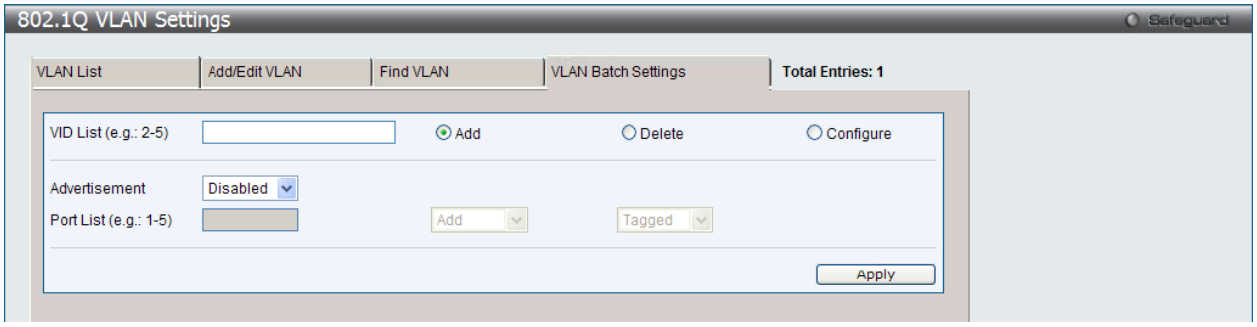


図 8-7　802.1Q VLAN Settings - VLAN Batch Settings タブ画面

以下の項目を使用して設定します。

項目	説明
VID List (e.g. : 2-5)	VID の範囲（1-4094）を指定します。続いて、「Add」、「Delete」または「Config」をボタンをクリックし、指定した VID List を追加、削除または編集します。
Advertisement	本機能を「Enabled」（有効）にすると、スイッチは GVRP パケットを送信し、VLAN に参加できることを通知します。
Port List (e.g. : 1:1-1:5)	VLAN のメンバとして追加または削除するポートまたはポート範囲を指定します。 指定ポートに行う操作を指定します。 • Add - VLAN のメンバとして追加します。 • Delete - VLAN のメンバとして削除します。 • config - 指定ポートに以下の設定を行います。 　- Tagged - ポートを 802.1Q タグ付きとして定義します。 　- Untagged - ポートを 802.1Q タグなしとして定義します。 　- Forbidden - ポートを VLAN のメンバではないポートとして定義します。動的に VLAN メンバになることが禁じられます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意　本スイッチは、最大 4K スタティック VLAN の設定をサポートしています。

802.1v Protocol VLAN（802.1v プロトコル VLAN）

802.1v Protocol VLAN フォルダには次の 2 つの画面があります。:「Protocol VLAN Group Settings」および「802.1v Protocol VLAN Settings」

802.1v Protocol Group Settings（802.1v プロトコルグループ設定）

本テーブルで、プロトコル VLAN グループを作成し、そのグループにプロトコルを追加します。802.1v プロトコル VLAN グループ設定は、各プロトコルのためにマルチプル VLAN をサポートし、同じ物理ポートに異なるプロトコルを持つタグなしポートの設定が可能です。例えば、同じ物理ポートに 802.1Q と 802.1v タグなしポートを設定できます。

注意 SNAP フレームの OUI が 0x080007 のフレームはサポートしておりません。

L2 Features > VLAN > 802.1v Protocol VLAN > 802.1v Protocol Group Settings の順にメニューをクリックし、以下の画面を表示します。

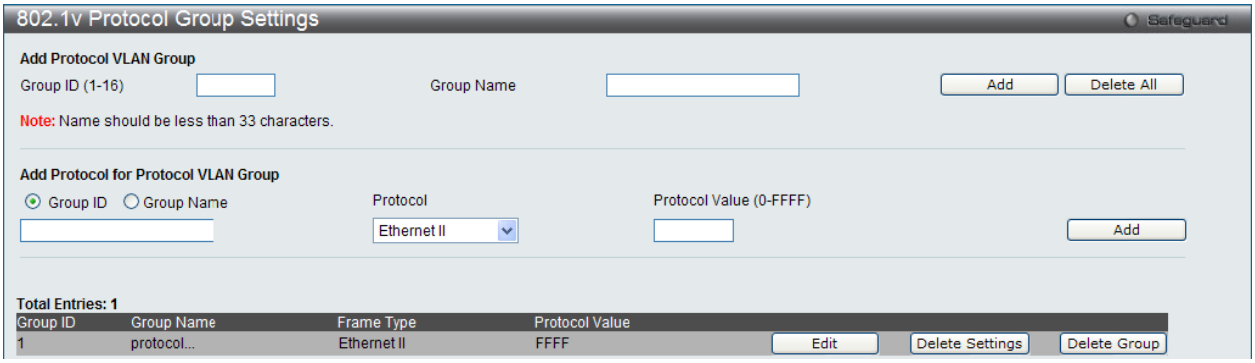


図 8-8　802.1v Protocol Group Settings 画面

テーブルの下半分は定義済みのすべてのグループを表示します。

以下の項目を使用して、設定します。

項目	説明
Add Protocol VLAN Group	
Group ID (1-16)	グループの ID 番号を 1-16 の範囲から指定します。
Group Name	新しいプロトコル VLAN グループの識別に使用します。32 文字までの半角英数字を入力します。
Add Protocol for Protocol VLAN Group	
Group ID	グループの ID 番号を 1-8 の範囲から指定します。
Group Name	新しいプロトコル VLAN グループの識別に使用します。32 文字までの半角英数字を入力します。
Protocol	本機能は、関連するプロトコルのタイプを検出するためにパケットヘッダのタイプオクテットを検証することで、パケットをプロトコルで定義された VLAN にマップします。 プルダウンメニューを使用して、Ethernet II、IEEE802.3 LLC および IEEE802.3 SNAP から選択します。
Protocol Value (0-FFFF)	グループに対してプロトコル値を入力します。これは、指定されたフレームタイプのプロトコルを識別するために使用されます。入力形式は 0x0 から 0xffff です。オクテット文字列は、フレームタイプによって、以下に示す値の 1 つを持っています。 • ethernet II - 16 ビット (2 オクテット) の 16 進数です。例えば、IPv4 は 800、IPv6 は 86dd、ARP は 806 などです。 • IEEE802.3 SNAP - 16 ビット (2 オクテット) の 16 進数です。 • IEEE802.3 LLC - 2 オクテットの IEEE 802.2 Link Service Access Point(LSAP) ペアです。はじめのオクテットは、Destination Service Access Point (DSAP) のための値であり、2 番目のオクテットは送信元のための値です。

注意 SNAP フレームの OUI が 0x080007 のフレームはサポートしておりません。

プロトコル VLAN グループの新規追加

「Add Protocol VLAN Group」セクション内の項目を入力し、「Add」ボタンをクリックします。

プロトコル VLAN グループの編集

1. テーブル内のエントリの「Edit」ボタンをクリックし、編集画面を表示します。
2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

プロトコル VLAN グループの削除

画面下半分に表示されたテーブル内のエントリの「Delete Group」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

プロトコル VLAN グループのプロトコル設定

「Add Protocol for Protocol VLAN Group」セクションの各項目を入力し、「Add」ボタンをクリックします。

プロトコル VLAN グループのプロトコルの削除

画面下半分に表示されたテーブル内のエントリの「Delete Settings」ボタンをクリックします。

802.1v Protocol VLAN Settings（802.1v プロトコル VLAN 設定）

プロトコル VLAN ポートの設定を行います。テーブルの下半分は定義済みのすべての設定を表示します。

L2 Features > VLAN > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings の順にメニューをクリックし、以下の画面を表示します。

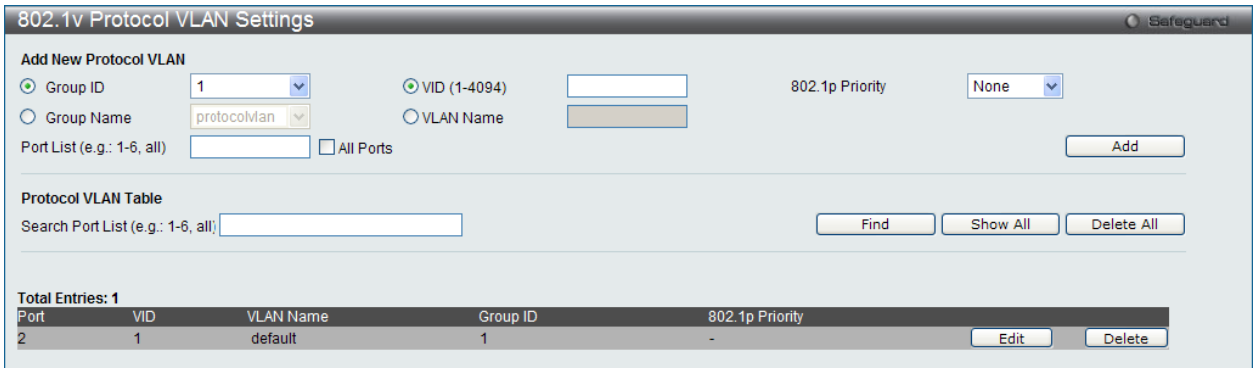


図 8-9　802.1v Protocol VLAN Settings 画面

以下の項目を使用して、設定します。

項目	説明
Add New Protocol VLAN	
Group ID	対応するボタンをチェックし、プルダウンメニューから定義済みの Group ID を選択します。
Group Name	対応するボタンをチェックし、プルダウンメニューから定義済みの Group Name を選択します。
VID (1-4094)	対応するボタンをチェックし、VID を入力します。これは、VLAN 名と共に、ユーザが作成する VLAN を識別するために使用する ID です。
VLAN Name	対応するボタンをチェックし、VLAN Name を入力します。これは、VLAN ID と共に、ユーザが作成する VLAN を識別するために使用する VLAN 名です。
802.1p Priority	スイッチに設定済みの 802.1p デフォルトプライオリティ（パケットが送られる CoS キューを決定するために使用）の設定を書き換える場合に使用します。本項目を選択すると、スイッチが受信したパケット内の本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。 本画面で設定した基準に一致するパケットが、指定された CoS キューに送られる前に、パケットの 802.1p デフォルトプライオリティを、「Priority（0-7）」に指定した値に書き換える場合に対応するボックスをクリックします。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。 プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの参照してください。「802.1p Settings（802.1p 設定）」（160 ページ）
Port List (e.g.: 1-6)	本項目にポート番号を入力することで特定のポートを選択するか、または「All Ports」をチェックします。
Protocol VLAN Table	
Search Port List	定義済みの全ポートリスト設定を検索し、テーブルの下半分に結果を表示します。

プロトコル VLAN ポートの新規設定

「Add New Protocol VLAN」セクションの各項目を入力し、「Add」ボタンをクリックします。

プロトコル VLAN ポートの設定編集

1. 編集するポートの「Edit」ボタンをクリックし、編集画面を表示します。
2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

プロトコル VLAN ポートの削除

画面下半分に表示されたポートリストで削除するポートの「Delete」ボタンをクリックします。

ポートリストの検索

ポートリストを検索するために、「Search Port List」に参照するポート番号を入力し、「Find」ボタンをクリックします。

定義済み全ポートリストの表示

「Show All」ボタンをクリックします。

すべての設定リストのクリア

「Delete All」ボタンをクリックします。

GVRP（GVRP の設定）

GVRP Global Settings（GVRP グローバル設定）

GVRP（GARP VLAN Registration Protocol）が有効なスイッチ同士で VLAN 構成情報を共有するかどうかを指定することができます。さらに、Ingress を「Enabled」（有効）にすることで、PVID がポートの PVID と一致しない入力パケットをフィルタしてトラフィックを制限します。
設定内容は、設定画面下部のテーブルで参照することができます。

L2 Features > VLAN > GVRP Settings > GVRP Global Settings の順にクリックし、以下の画面を表示します。

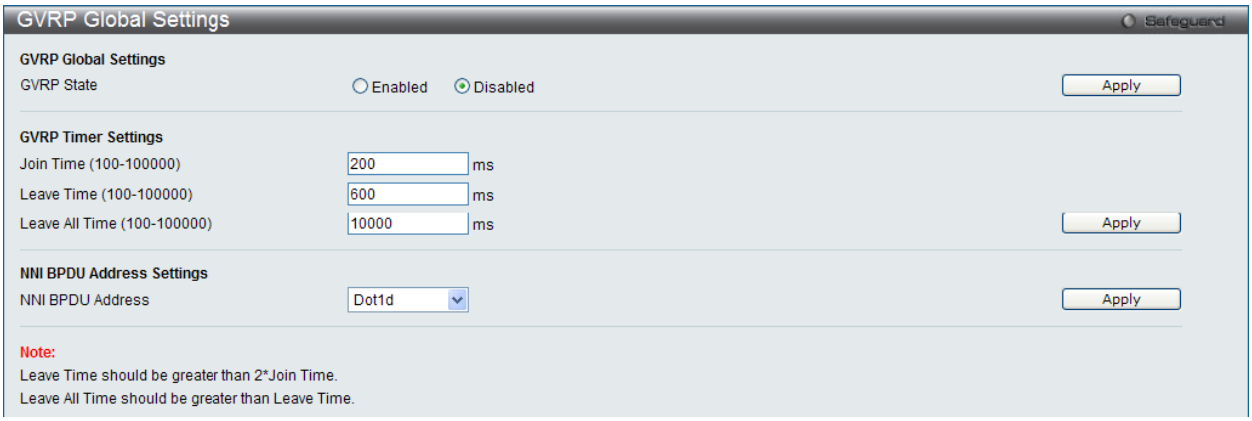


図 8-10　GVRP Global Settings 画面

本画面には次の項目があります。

項目	説明
GVRP Global Settings	
GVRP State	GVRP 状態を有効または無効にして「Apply」ボタンをクリックします。 • Enabled - デバイスで GVRP を有効に設定します。 • Disabled - デバイスで GVRP を無効に設定します。（初期値）
GVRP Timer Settings	
Join Time	Join Time（ミリ秒）を入力します。
Leave Time	Leave Time（ミリ秒）を入力します。
Leave All Time	Leave All Time（ミリ秒）を入力します。
NNI BPDU Address Settings	
NNI BPDU Address	サービス提供サイトにおける GVRP の BPDU プロトコルアドレスを決定します。802.1d GVRP アドレス、または 802.1ad サービスプロバイダの GVRP アドレスを使用します

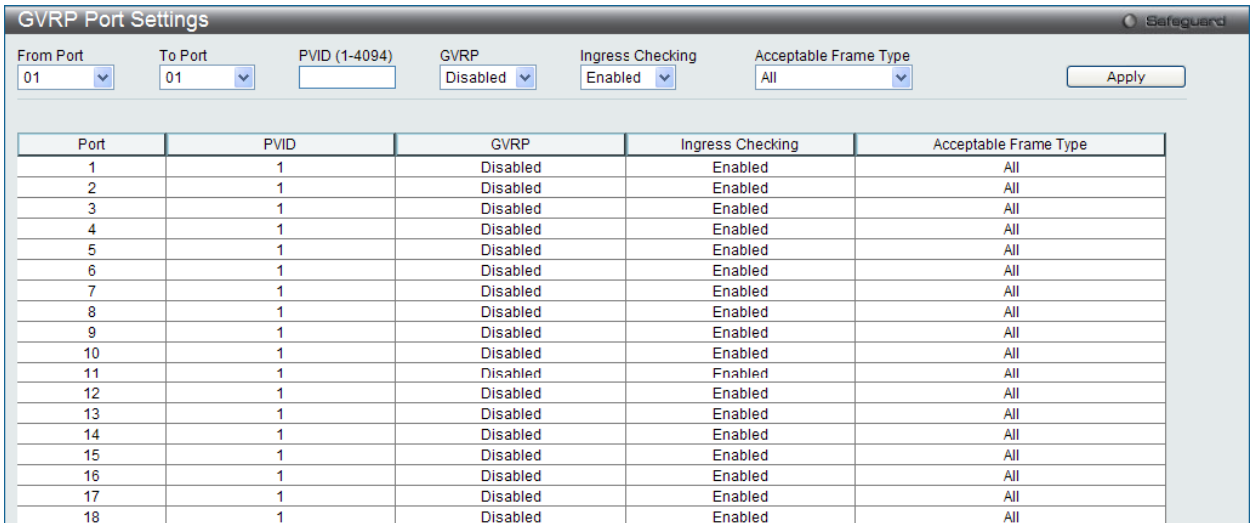
「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

注意　「Leave time」は「Join time」の 2 倍以上である必要があります。「Leave All Time」は「Leave Time」より大きくする必要があります。

GVRP Port Settings（GVRP ポート設定）

GVRP ポートパラメータを設定します。

L2 Features > VLAN > GVRP Settings > GVRP Port Settings の順にクリックし、以下の画面を表示します。



Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Disabled	Enabled	All
2	1	Disabled	Enabled	All
3	1	Disabled	Enabled	All
4	1	Disabled	Enabled	All
5	1	Disabled	Enabled	All
6	1	Disabled	Enabled	All
7	1	Disabled	Enabled	All
8	1	Disabled	Enabled	All
9	1	Disabled	Enabled	All
10	1	Disabled	Enabled	All
11	1	Disabled	Enabled	All
12	1	Disabled	Enabled	All
13	1	Disabled	Enabled	All
14	1	Disabled	Enabled	All
15	1	Disabled	Enabled	All
16	1	Disabled	Enabled	All
17	1	Disabled	Enabled	All
18	1	Disabled	Enabled	All

図 8-11　GVRP Port Settings 画面

本画面には次の項目があります。

項目	説明
From Port / To Port	ポートベース VLAN に含まれるポートの範囲を指定します。
PVID (1-4094)	PVID を VLAN に手動で割り当てます。スイッチには初期状態ですべてのポートが default VLAN（VID=1）に割り当てられています。PVID はポートが送信時にタグなしパケットにタグ付けをしたり、受信時にフィルタリングをするためのものです。 もし、ポートがタグ付きのフレームのみ受け付けるよう指定されていて（Tagging 指定）、タグなしのパケットがそのポートに送信されてきたら、ポートは PVID を使用してタグ内に VID を書き込み、802.1Q タグを追加します。 パケットが宛先に届いた時、受信するデバイスは PVID を VLAN に送出するか否かを決定するために使用します。パケットを受信するポートの Ingress フィルタリングが有効である場合、ポートは到着したパケットの VID と自分の PVID を比較します。2 つが一致しないと、ポートはパケットを廃棄します。2 つが一致すると、ポートはパケットを受信します。
GVRP	GVRP が各ポートをダイナミックに VLAN メンバにするかどうかを設定します。 • Enabled - 選択したポートで GVRP を有効に設定します。 • Disabled - 選択したポートで GVRP を無効に設定します。（初期値）
Ingress Checking	プルダウンメニューでポートを有効にすると、VLAN メンバシップを持つ入力パケット内の VID タグを比較します。イングレスチェックが有効であり、受信ポートがフレームの VLAN のメンバポートでないと、フレームは破棄されます。
Acceptable FrameType	ポートが受け入れるフレームの種類を設定します。 • Tagged Only - タグ付きフレームのみポートは受け入れます。 • All - タグ付き、タグなし両方のフレームをポートは受け入れます。（初期値）

「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

MAC-based VLAN Settings（MAC ベース VLAN 設定）

新しく MAC ベース VLAN エントリを作成し、設定済みのエントリを検索 / 編集 / 削除します。

エントリがポートに作成されると、ポートは自動的に指定した VLAN のタグなしメンバポートになります。スタティック MAC ベース VLAN のエントリがユーザに作成されると、このユーザからのトラフィックは指定 VLAN の下で送信されます。

L2 Features > VLAN > MAC-based VLAN Settings の順にメニューをクリックし、以下の画面を表示します。

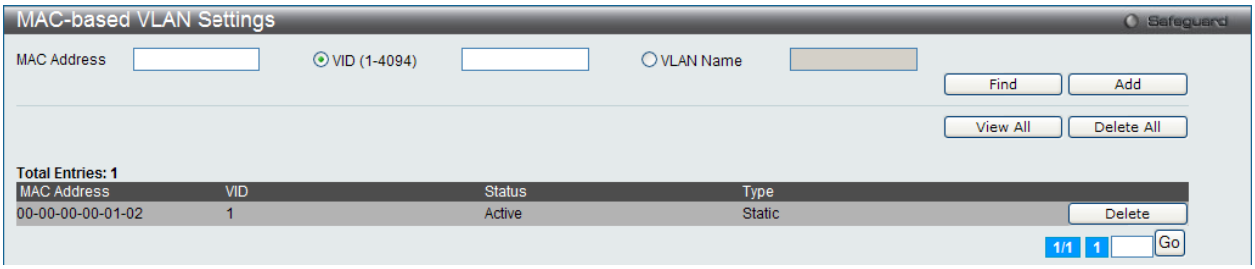


図 8-12　MAC-based VLAN Settings 画面

以下の項目を使用して設定します。

項目	説明
MAC Address	ユニキャスト MAC アドレスを指定します。
VID	VLAN ID を入力します。
VLAN Name	作成済みの VLAN の VLAN 名を指定します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

エントリの新規登録

MAC ベース VLAN に登録する MAC アドレスを「MAC Address」に入力し、関連付ける「VLAN Name」を指定後、「Add」ボタンをクリックします。

エントリの検索

「MAC Address」または「VLAN Name」を入力し、「Find」ボタンをクリックします。結果は画面下のテーブルに表示されます。

エントリの削除

テーブル内の削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの参照

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

PVID Auto Assign Settings（PVID 自動割り当て設定）

PVID 自動割り当て設定を有効または無効にすることができます。

L2 Features > VLAN > PVID Auto Assign Settings の順にメニューをクリックし、以下の画面を表示します。

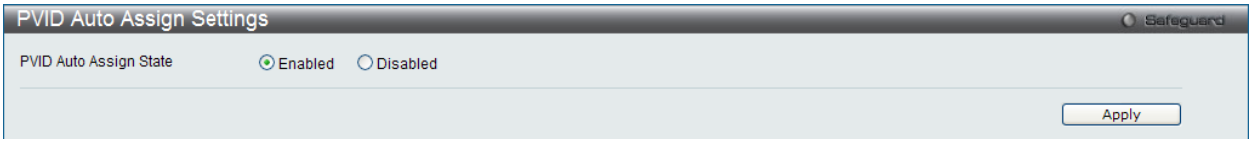


図 8-13　PVID Auto Assign Settings 画面

以下の項目を使用して設定します。

項目	説明
PVID Auto Assign State	PVID 自動割り当て設定を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Enabled」（有効）です。

「Apply」ボタンをクリックし、デバイスに設定を適用します。

VLAN Trunk Settings（VLAN トランク設定）

ポートの VLAN を有効にすることで、未知の VLAN グループに所属するフレームがそのポートを通過することができるようになります。これは、中継するデバイスに同じ VLAN グループを設定しないで、末端のデバイスに VLAN グループを設定する場合に便利です。

スイッチ A と B に VLAN グループ 1 と 2（V1 と V2）を作成するものとします。VLAN トランクを使用しない場合、はじめにすべての中継スイッチ C、D、E のすべてに VLAN グループ 1、2 を設定します。そうでない場合、未知の VLAN グループのタグを持つフレームを廃棄します。しかし、各中継スイッチのポートで VLAN トランクを有効にすれば、末端のデバイスに VLAN グループを作成するだけとなります。C、D、および E は、それらのスイッチにとって未知の VLAN グループのタグ 1 および 2 を持つフレームを自動的にそれらの VLAN トランキングポートから通過させます。

以下の図例を参照してください。

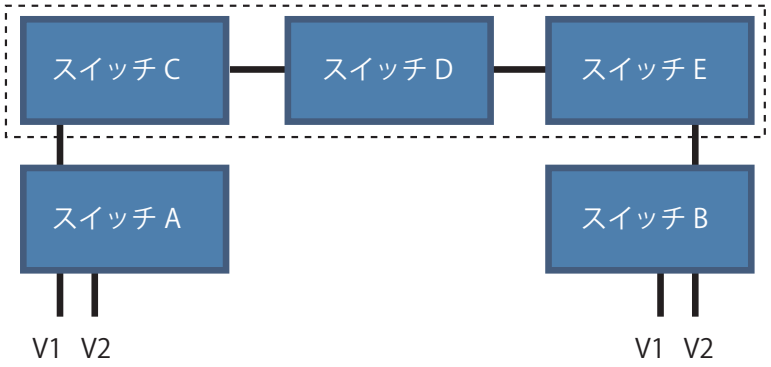


図 8-14　VLAN トランクの例題

本画面では、多くの VLAN ポートを集約して VLAN トランクを作成します。

L2 Features > VLAN > VLAN Trunk Settings の順にメニューをクリックし、以下の画面を表示します。

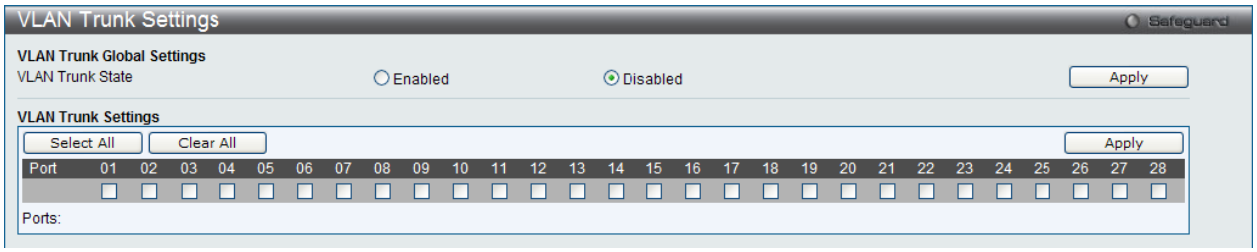


図 8-15　VLAN Trunk Settings 画面

本画面には次の項目があります。

項目	説明
VLAN Trunk State	VLAN トランキングのグローバルな状態を有効または無効にします。
Port Settings	設定するポートを指定します。

スイッチに VLAN トランクポートを設定するためには、設定するポートを指定し、ステータスを「Enabled」に変更して「Apply」ボタンをクリックします。

「Select All」ボタンをクリックすると、全ポートが設定に使用されます。
「Clear All」ボタンをクリックすると、全ポートの設定がクリアされます。

Browse VLAN（VLAN の参照）

本画面では、スイッチの各ポートの VLAN ステータスを VLAN ごとに表示します。

L2 Features > VLAN > Browse VLAN メニューをクリックし、以下の画面を表示します。

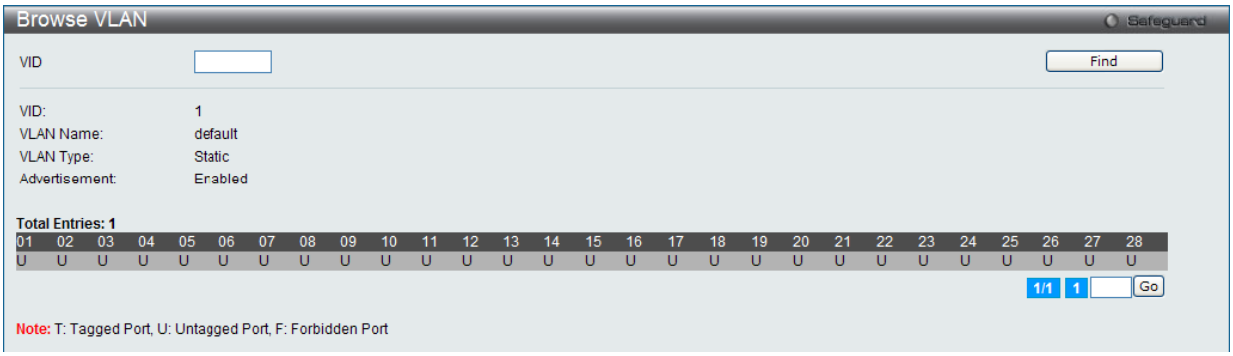


図 8-16　Browse VLAN 画面

画面上の「VID」に VLAN ID を入力し、「Find」ボタンをクリックします。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

注意　本ページで使用される略記は、Tagged Port(T)、Untagged Port(U)、および Forbidden Port(F) です。

Show VLAN Ports（VLAN ポートの参照）

スイッチの VLAN ポートを VID ごとに表示します。

L2 Features > VLAN > Show VLAN Ports メニューをクリックし、以下の画面を表示します。

図 8-17　Show VLAN Ports 画面

画面の上にある「Port List」欄にポートまたはポート範囲を入力して、「Find」ボタンをクリックします。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

QinQ（QinQ 設定）

QinQ VLAN または Q-in-Q VLAN と呼ばれる技術を利用することにより、ネットワークプロバイダは規模の大きい包括的な VLAN の中に、顧客用の VLAN を設置し、VLAN 構成に新しい階層を導入することにより、その規模を拡張することができます。基本的には大規模な ISP のネットワーク内に、レイヤ 2 の VPN（Virtual Private Network）および、顧客用の透過型 LAN を配置することにより、クライアント側の構造を複雑にすることなく、複数の顧客の LAN を接続します。構造の複雑化が回避できるだけでなく、4000 以上の VLAN を定義できるようになるため、VLAN ネットワークを大幅に拡張し、複数の VLAN を使用する顧客数を増やすことができます。

QinQ VLAN とは、基本的には既存の IEEE 802.1Q VLAN タグ中に挿入する VLAN タグのことで、SPVID（Service Provider VLAN ID）と呼ばれます。これらの VLAN タグは TPID（Tagged Protocol ID）でマークされ、16 進数形式で設定され、パケットの VLAN タグの内部にカプセル化されます。パケットは 2 つタグ付けされ、ネットワーク上の他の VLAN とは区別されます。このように 1 つのパケットの中に VLAN の階層を与えています。

以下に QinQ VLAN タグ付きパケットの例を示します。

宛先アドレス	送信元アドレス	SPVLAN (TPID+ サービスプロバイダ VLAN タグ)	802.1Q CEVLAN タグ (TPID+ 顧客 VLAN タグ)	イーサタイプ	ペイロード

以下に QinQ VLAN を使用した ISP ネットワークの例を示します。

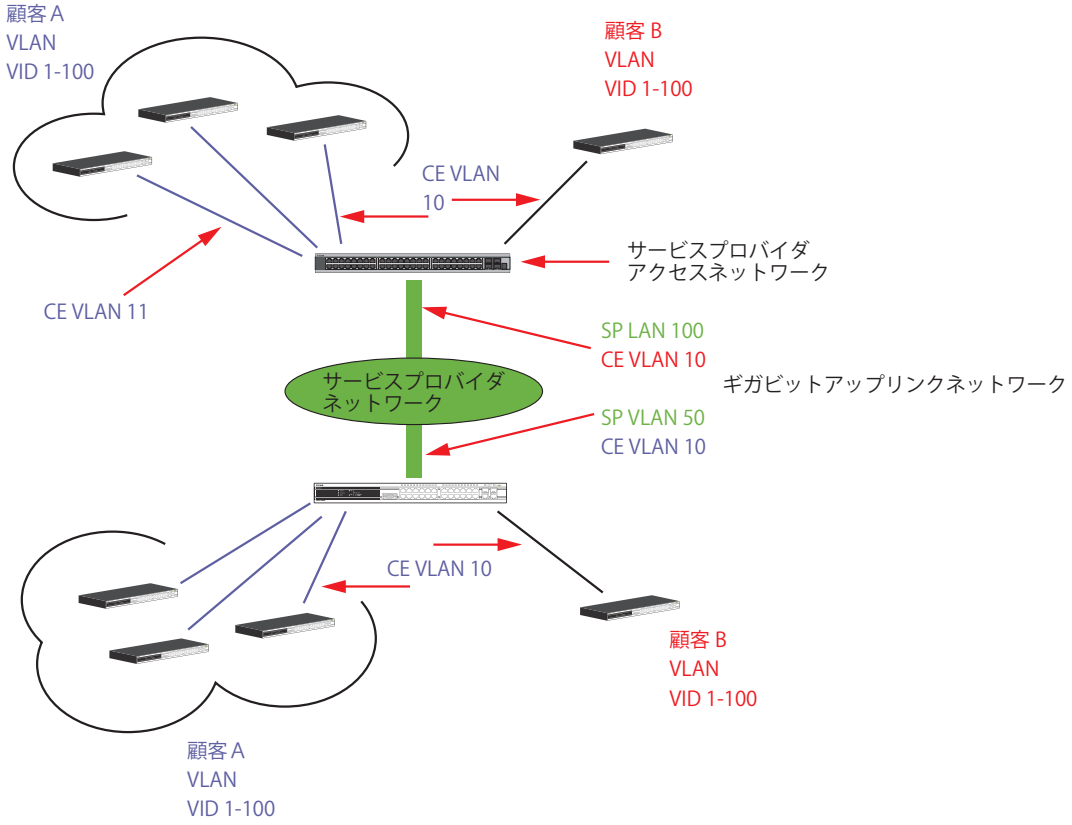


図 8-18　QinQ VLAN を使用したネットワーク例

上の図例では、サービスプロバイダ・アクセスネットワーク・スイッチ (プロバイダのエッジスイッチ) は顧客 A と顧客 B という特定の顧客に対して異なる SPVID を持つ QinQ VLAN を設定しているデバイスです。CEVLAN（Customer VLAN）10 は、サービスプロバイダ・アクセスネットワーク上で顧客 A には SPVID 100 を、顧客 B には SPVID 200 をタグ付けされるので、サービスプロバイダのネットワーク上では 2 つの VLAN に属していることになります。
このように、顧客は通常の VLAN を保持しながら、サービスプロバイダは、複数の顧客の VLAN を 1 つの SP VLAN によって分割することができ、サービスプロバイダのスイッチ上でのトラフィックとルーティングのプロセスを調整します。これらの情報はサービスプロバイダのメインのネットワークに送られ、1 セットのプロトコルと 1 つのルーティング動作を持つ 1 つの VLAN として認識されます。

ダブル VLAN 使用時のルール

ダブル VLAN を使用するために、以下のルールがあります。

1. すべてのポートに対して SPVID と関連するサービスプロバイダのエッジスイッチ上の TPID の設定が必要です。
2. すべてのポートはアクセスポートまたはアップリンクポートとして設定される必要があります。アクセスポートはイーサネットポート、アップリンクポートはギガビットポートである必要があります。
3. プロバイダのエッジスイッチには SPVID タグが追加されるため、1522 バイト以上のフレームに対応する必要があります。
4. アクセスポートはサービスプロバイダ VLAN のタグなしポートである必要があります。アップリンクポートはサービスプロバイダ VLAN のタグ付きポートである必要があります。
5. スイッチ上にはダブル VLAN と通常の VLAN が混在できません。一度 VLAN を変更すると、すべてのアクセスコントロールリストがクリアになり、再設定が要求されます。
6. ダブル VLAN を有効にすると GVRP は無効になります。
7. CPU からアクセスポートに送信されたすべてのパケットはタグなしになります。
8. スイッチがダブル VLAN モードにある時、以下の機能は使用できなくなります。:
   - ゲスト VLAN
   - Web ベースのアクセス制御
   - IP マルチキャストルーティング
   - GVRP
   - 通常の 802.1Q VLAN 機能

QinQ Settings（QinQ 設定）

QinQ のパラメータを設定します。

L2 Features > QinQ > QinQ Settings の順にメニューをクリックし、以下の画面を表示します。

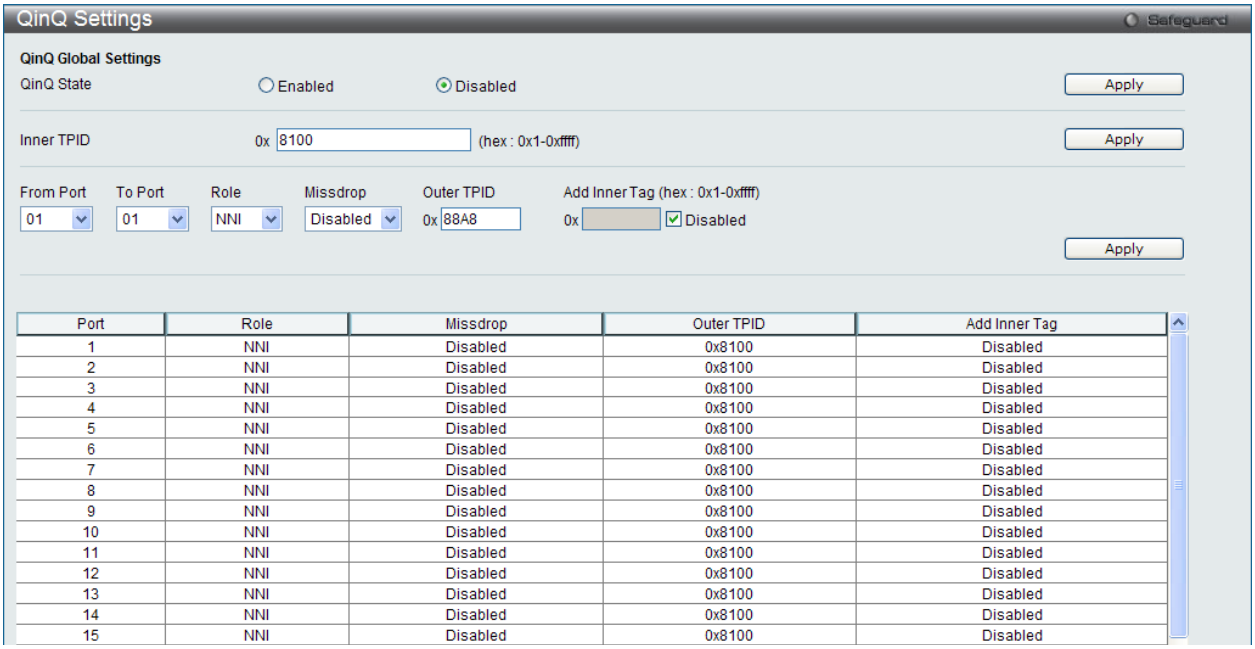


図 8-19　QinQ Settings 画面

以下の項目を使用して設定します。

項目	説明
QinQ State	QinQ 機能をグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
Inner TPID	SP-VLAN タグに Inner TPID を入力します。
From Port/To Port	設定に使用するポート範囲を選択します。
Role	役割（UNI または NNI）を選択します。 • UNI - UNI（user-network interface）を選択すると、指定ユーザと指定ネットワーク間の通信が行われることを示します。 • NNI - NNI（network-to-network interface）を選択すると、指定した 2 つのネットワーク間で通信が行われることを示します。
Missdrop	このオプションは、C-VLAN ベースの SP-VLAN 割り当ての Missdrop を有効または無効にします。 • Enabled - QinQ プロファイルにおけるどんな指定ルールにも一致しないパケットは廃棄されます。 • Disabled - パケットは転送され、受信ポートの PVID に割り当てられます。
Outer TPID	SP-VLAN タグに Outer TPID を入力します。
Add Inner Tag	「Disabled」のチェックを外して、「Inner Tag」が追加されるエントリを入力します。初期値では無効です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

VLAN Translation Settings（VLAN 変換機能の設定）

C-VLAN と SP-VLAN 間の変換関係を追加します。

UNI ポートのイングレスでは、C-VLAN タグ付きパケットは、定義済みルールに従って追加または交換することで SP-VLAN のタグ付きパケットに変換されます。このポートのイーグレスでは、SP-VLAN タグは、C-VLAN タグに復元されるか、またはタグ取りされます。Inner 優先度フラグが受信ポートに対して無効になると、優先度は SP-VLAN タグの優先度となります。

L2 Features > QinQ > VLAN Translation Settings の順にメニューをクリックし、以下の画面を表示します。

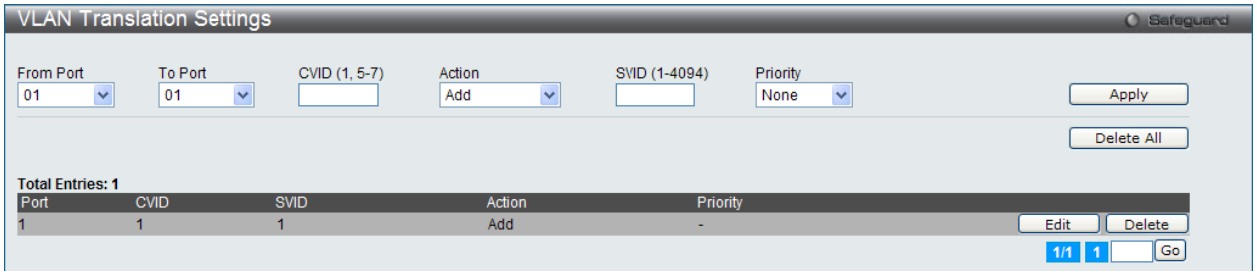


図 8-20　VLAN Translation Settings 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
From Port / To Port	設定に使用するポート範囲を選択します。
CVID (1, 5-7)	照合する C-VLAN ID を指定します。
Action	• Add - C- タグの前に S- タグを追加します。 • Replace - オリジナルの C- タグを S- タグに置き換えます。
SVID (1-4094)	SP-VLAN ID を入力します。
Priority	S- タグの優先度を選択します。

「Apply」ボタンをクリックし、新しいエントリを追加します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックし、編集画面を表示します。
2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

Layer 2 Protocol Tunneling Settings（レイヤ 2 プロトコルトンネリング設定）

レイヤ 2 プロトコルトンネリングポートを設定します。

L2 Features > Layer 2 Protocol Tunneling Settings の順にメニューをクリックし、以下の画面を表示します。

図 8-21　Layer 2 Protocol Tunneling Settings 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Layer 2 Protocol Tunneling State	レイヤ 2 プロトコルトンネリング状態を有効または無効にします。
From Port / To Port	設定に使用するポート範囲を選択します。
Type	ポートタイプを指定します。UNI、NNI、および None（なし）が選択可能です。初期値は「None」です。
Tunneled Protocol	「Type」で「UNI」を選択した場合、このプルダウンメニューでは以下のオプションを表示します。 • STP - これらの UNI で受信した BPDU をトンネルします。 • GVRP - これらの UNI で受信した GVRP PDU をトンネルします。 • Protocol MAC - これらの UNI ポートでトンネルする L2 プロトコルパケットの送信先 MAC アドレスを指定します。現時点では、MAC アドレスは、01-00-0C-CC-CC-CC または 01-00-0C-CC-CC-CD です。 • All - すべてをサポートします。
Threshold (0-65535)	この UNI ポートで受け入れるパケット / 秒の破棄しきい値を入力します。プロトコルのしきい値を超過すると、ポートは PDU を破棄します。値の範囲は 0-65535（パケット / 秒）です。値 0 は無制限であることを意味します。初期値は 0 です。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

Spanning Tree（スパニングツリーの設定）

本スイッチは 3 つのバージョンのスパニングツリープロトコル（8802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。ネットワーキング管理者間では 802.1D-1998 STP が最も一般的なプロトコルとして認識されていると思います。しかし、D-Link のマネジメントスイッチにも 802.1D-2004 RSTP と 802.1Q-2005 MSTP は導入されており、それらの技術について、以下に簡単に紹介します。また、802.1D-1998 STP、802.1D-2004 RSTP および 802.1Q-2005 MSTP の設定方法についても記述します。

802.1Q-2005 MSTP

MSTP（Multiple Spanning Tree Protocol）は IEEE 委員会により定義された標準規格で、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングし、ネットワーク中に複数の経路を提供します。また、ロードバランシングを可能にし、1 つのインスタンスに障害が発生した場合でも、広い範囲で影響を与えないようにすることができます。障害発生時には障害が発生したインスタンスに代わって新しいトポロジを素早く収束します。これら VLAN 用のフレームは、これらの 3 つのスパニングツリープロトコル（STP、RSTP、MSTP）のいずれかを使用して、素早く適切に相互接続されたブリッジを通して処理されます。

本プロトコルでは、BPDU（Bridge Protocol Data Unit）パケットにタグ付けを行い、受信するデバイスが、スパニングツリーインスタンス、スパニングツリーリージョン、またはそれらに関連付けられた VLAN を区別できるようにしています。MSTI ID（MST インスタンス ID）はこれらのインスタンスをクラス分けします。MSTP では、複数のスパニングツリーを CIST（Common and Internal Spanning Tree）で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を決定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジのように見せかけます。そのため、異なる VLAN を割り当てられたフレームは、定義した VLAN や各スパニングツリー内の管理エラーに関係なく、フレームの単純で完全な処理を続けながら、ネットワーク上の管理用に設定されたリージョン中の異なるデータ経路を通ります。

ネットワーク上の MSTP を使用しているスイッチは、以下の 3 つの属性で 1 つの MSTP が構成されています。

1. 32 文字までの半角英数字で定義された「Configuration 名」。「MST Configuration Identification」画面中の「Configuration Name」で設定します。
2. 「Configuration Revision 番号」（「MST Configuration Identification」画面内の「Revision Level」）。
3. 4094 エレメントテーブル（「MST Configuration Identification」画面内の「VID List」）。スイッチがサポートする 4094 件までの VLAN とインスタンスとの関連付けです。

スイッチ上で MSTP 機能を利用するためには、以下の手順を実行してください。

1. スイッチに MSTP 設定を行います。（「STP Bridge Global Settings」画面の「STP Version」で設定）
2. MSTP インスタンスに適切なスパニングツリープライオリティを設定します。（「STP Instance Settings」画面の「Priority」で設定）
3. 共有する VLAN を MSTP Instance ID に追加します。（「MST Configuration Identification」画面の「VID List」で設定）

802.1D-2004 Rapid Spanning Tree

本スイッチには、IEEE 802.1Q-2005 に定義される MSTP（Multiple Spanning Tree Protocol）、IEEE 802.1D-2004 に定義される RSTP（Rapid Spanning Tree Protocol）、および 802.1D-1998 で定義される STP（Spanning Tree Protocol）の 3 つのプロトコルを実装しています。RSTP は IEEE 802.1D-1998 をサポートするレガシー機器との併用が可能ですが、その場合 RSTP を使用する利点は失われます。

RSTP は 802.1D-1998 STP 標準の進化型です。RSTP は、STP を使用する上での制限を克服する目的で開発されました。制限とは、特に今日イーサネットスイッチに取り入れられているレイヤ 3 の諸機能を妨害するものを指しています。RSTP の基本的な機能や用語の多くは STP と同じであると言えます。STP 用の設定項目の多くも RSTP で同じように使用されます。本項では、スパニングツリーの新しいコンセプトと、これらの 2 つのプロトコル間の主な違いについて記述します。

ポートの状態遷移

3 つのプロトコル間の根本的な相違は、ポートがフォワーディング状態に遷移する方法と、この遷移とトポロジの中でのポートの役割（Forwarding/Not Forwarding）の関連性にあります。MSTP と RSTP では、802.1D-1998 で使用されていた 3 つの状態、「Disabled」、「Blocking」、「Listening」が、「Discarding」という 1 つの状態に統合されました。どちらのケースにおいてもポートはパケットの送信を行わない状態です。STP の「Disabled」、「Blocking」、「Listening」であっても RSTP/MSTP の「Discarding」であっても、ネットワークトポロジ中では「アクティブではない状態」であり、機能の差はありません。表にポートの状態遷移における 3 つのプロトコルの差を示しています。

トポロジの計算については 3 つのすべてのプロトコルにおいて同様に行われます。各セグメントにはルートブリッジへの 1 つのパスがあります。すべてのブリッジは BPDU パケットをリッスンします。しかし、BPDU パケットは、さらに Hello パケット送信ごと送信されます。
BPDU パケットは、受信されないことがあっても送信されます。そのため、ブリッジ間のリンクはリンクの状態に反応します。結果として、この違いがリンク断の素早い検出とトポロジの調整に繋がるのです。802.1D-1998 の欠点は隣接するブリッジからの即時のフィードバックがないことです。

ポート状態の比較

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	不可能	不可能
Discarding	Discarding	Blocking	不可能	不可能
Discarding	Discarding	Listening	不可能	不可能
Learning	Learning	Learning	不可能	可能
Forwarding	Forwarding	Forwarding	可能	可能

RSTP では、タイマの設定への依存をやめ、フォワーディング状態への急速な遷移が可能になりました。RSTP 準拠のブリッジは他の RSTP に準拠するブリッジリンクのフィードバックに反応するようになりました。ポートは、フォワーディング状態の遷移の間トポロジが安定するまで待つ必要がなくなりました。この急速な遷移を実現するために、RSTP プロトコルでは以下の 2 つの新しい変数（Edge Port と P2P Port）が使用されます。

Edge Port

エッジポートは、ループを作成できないセグメントに直接接続しているポートに指定するものです。例えば、1 台のワークステーションに接続しているポートがこれに該当します。エッジポートとして指定されたポートは、直接 forwarding に遷移し、listening および learning の段階は飛ばしてしまいます。エッジポートは BPDU パケットを受け取った時点で、通常のスパニングツリーポートに変わります。

P2P Port

P2P ポートでも急速な遷移が可能になっています。P2P ポートは他のブリッジとの接続に使用されます。RSTP と MSTP では、全二重モードで動作しているすべてのポートは、特に設定を変えられていない限り、P2P ポートと見なされます。

802.1D-1998/802.1D-2004/802.1Q-2005 の互換性

RSTP や MSTP はレガシー機器と相互運用が可能で、必要に応じて BPDU パケットを 802.1D-1998 形式に自動的に変換することができます。しかし、802.1D-1998 STP を使用しているセグメントでは、MSTP や RSTP の利点である迅速な遷移やトポロジ変更の検出を享受することはできません。それらのプロトコルは、セグメント上でレガシー機器が RSTP や MSTP を使用するためにアップデートを行う場合などの、マイグレーションに使用する変数を用意しています。

2 つのレベルで動作するスパニングツリープロトコル

1. スイッチレベルでは、設定はグローバルに実行されます。
2. ポートレベルでは、設定はポートベースのユーザ定義のグループに対して実行されます。

STP Bridge Global Settings（STP ブリッジグローバル設定）

STP ブリッジグローバルパラメータを設定します。

L2 Features > Spanning Tree > STP Bridge Global Settings の順にメニューをクリックし、以下に示す画面を表示します。
「STP State」でデバイスの STP をグローバルに有効または無効にします。また、「STP Version」で STP の方式を選択します。

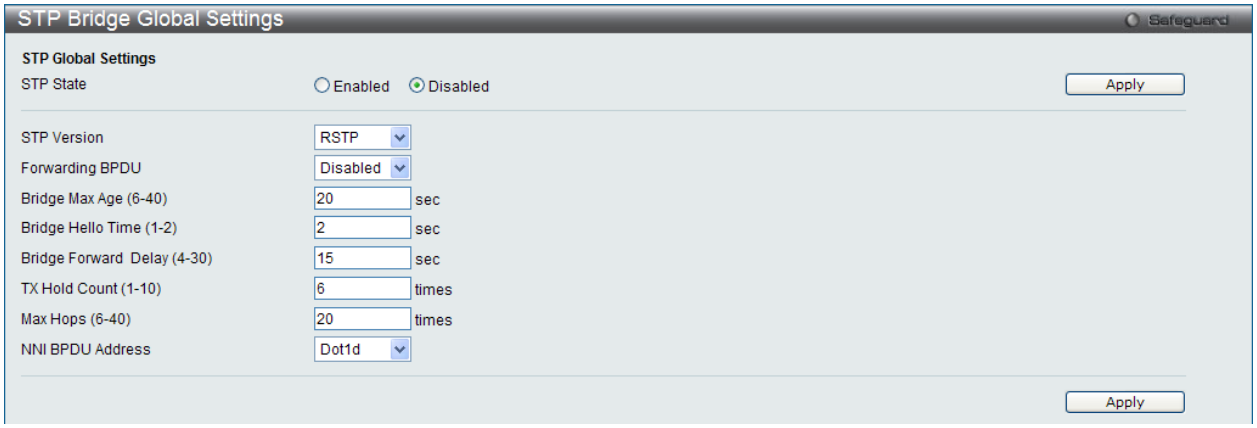


図 8-22　STP Bridge Global Settings 画面 : RSTP（初期値）

STP バージョンと対応する設定オプションの説明は、以下の表で参照してください。
設定には以下の項目が使用されます。

項目	説明
STP State	STP をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
STP Version	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。 • MSTP - スイッチ上で MSTP がグローバルに使用されます。
Forwarding BPDU	「Enabled」（有効）または「Disabled」（無効）にします。「Enabled」にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は「Disabled」です。
Bridge Max Age (6-40)	本項目は、古い情報がネットワーク内の冗長パスを永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40（秒）の範囲から値を指定します。初期値は 20（秒）です。
Bridge Hello Time (1-2)	ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために BPDU パケットを 2 回送信します。本値は、1 回目の送信と 2 回目の送信の間隔です。STP または RSTP が「STP Version」で選択された場合にだけ本項目は表示されます。MSTP に対して、Hello Time はポートごとに設定される必要があります。詳しくは「STP ポート設定」セクションを参照してください。1-2 秒で指定します。初期値は 2（秒）です。
Bridge Forward Delay (4-30)	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間に本値で指定した時間 Listening 状態を保ちます。4-30（秒）の範囲から指定します。初期値は 15（秒）です。
Tx Hold Count (1-10)	Hello パケットの最大送信回数を指定します。1-10 の範囲から指定します。初期値は 6 です。
Max Hops (6-40)	スイッチが送信した BPDU パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BPDU パケットを破棄し、ポートに保持していた情報を解放します。ホップカウントは 6-40 で指定します。初期値は 20 です。
NNI BPDU Address	サービス提供サイトにおける STP の BPDU プロトコルアドレスを決定します。802.1D STP アドレス、または 802.1ad サービスプロバイダの STP アドレスを使用します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意　Bridge Hello Time は Max. Age より長い時間を指定すると、コンフィグレーションエラーの原因となります。Hello Time と Max. Age の設定には以下の式に従って行ってください。

Bridge Max Age <= 2 x（Bridge Forward Delay - 1 秒）
Bridge Max Age <= 2 x（Bridge Hello Time + 1 秒）

STP Port Settings（STP ポートの設定）

STP をポートごとに設定します。

L2 Features > Spanning Tree > STP Port Settings の順にクリックし、以下の画面を表示します。

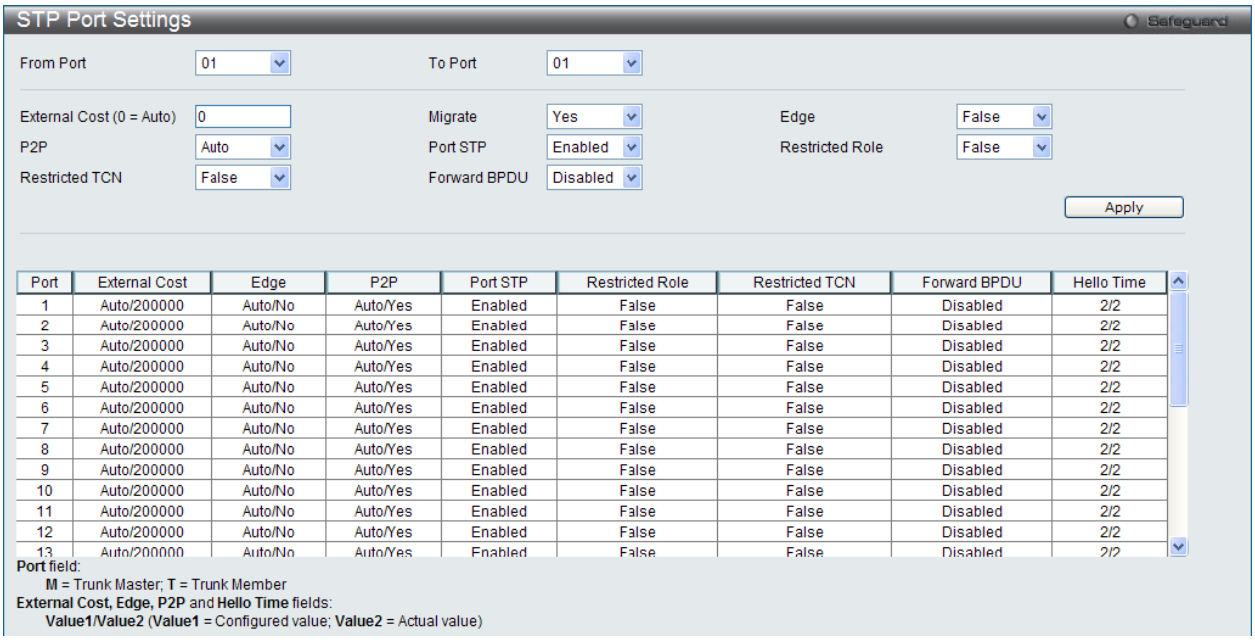


図 8-23　STP Port Settings 画面

参照　STP グループと VLAN グループを関連付けて定義することをお勧めします。

設定には以下の項目が使用されます。

項目	説明
From/ To Port	設定対象のポート範囲を指定します。
External Cost (0=Auto)	設定対象のポートに対し、パケット送信のためのコストを表すメトリックを定義します。ポートコストは、自動設定、あるいは手動でメトリック値を指定できます。初期値は 0（自動）です。 • 0 - 0 を指定すると、指定したポートに対して、最適なパケット送信スピードを自動的に設定します。デフォルトポートコスト：100Mbps ポートの場合は 200000、ギガビットポートの場合は 20000。 • 1-200000000 の範囲から指定 - 小さい数字を指定すると、パケット送出ポートとして選出される確率が上がります。
Migrate	RSTP モードで動作中に、「Yes」を選択すると、選択されたポートは RSTP BPDU を送信します。
Edge	• True - 選択されたポートはエッジポートとして指定されます。エッジポートはループを発生しません。しかし、トポロジの変更によってループ発生の可能性が生じると、エッジポートはエッジポートとしての資格を失います。エッジポートは通常 BPDU パケットを受け取りません。しかし、BPDU パケットが受信されると、そのポートはエッジポートの資格を失います。 • False - そのポートにエッジポートの資格がないことを示しています。 •「Auto」オプションが利用可能です。
P2P	• True - 選択されたポートは P2P ポートとして指定されます。P2P ポートはエッジポートと似ていますが、全二重モードでのみ稼動する点で異なります。RSTP の特長として、エッジポート同様、P2P ポートは迅速に Forwarding 状態に遷移します。 • False - そのポートに P2P ポートの資格がないことを示しています。 • Auto - ポートはいつでも可能な時に（True を指定した時と同様に）P2P ポートとして稼動します。ポートの資格を失う時（例えば、半二重モードを指定された時など）、自動的に False を指定した時と同様になります。（初期値）
Port STP	ポートの STP を「Enabled」(有効)/「Disabled」(無効) にします。初期値は「Enabled」です。
Restricted Role	「True」と「False」を切り替えます。True に設定すると、ポートはルートポートになるように選択されることはありません。初期値は「False」です。
Restricted TCN	TCN（Topology Change Notification）は、ブリッジがトポロジ変更を合図するためにルートポートに送出する簡単な BPDU です。Restricted TCN は「True」と「False」間で切り変わります。「True」に設定すると、受信した TCN とトポロジ変更を他のポートへ伝搬することを停止します。初期値は「False」です。
Forward BPDU	プルダウンメニューから STP が無効の場合の BPDU パケットのフラッドを「Enabled」(有効)、「Disabled」(無効) にします。「Enabled」を選択すると、選択されたポートは他のネットワークデバイスから来る BPDU パケットの転送を行うようになります。

「Apply」ボタンをクリックし、設定を有効にします。

注意　BPDU の送出をポートベースで有効とする場合は、はじめに以下の設定を行ってください。

1. STP をグローバルに無効とする。
2. BPDU の送出をグローバルに有効とする。

これらの設定は、前述の「STP Bridge Global Settings」メニューで行います。

MST Configuration Identification（MST の設定）

スイッチ上で MST インスタンスの設定を行います。本設定は MSTI（マルチプルスパニングツリーインスタンス）を識別するためのものです。スイッチは初期状態で 1 つの CIST（Common Internal Spanning Tree）を持ちます。ユーザはその項目を変更できますが、MSTI ID の変更や削除は行うことができません。

L2 Features > Spanning Tree > MST Configuration Identification の順にメニューをクリックし、以下の画面を表示します。

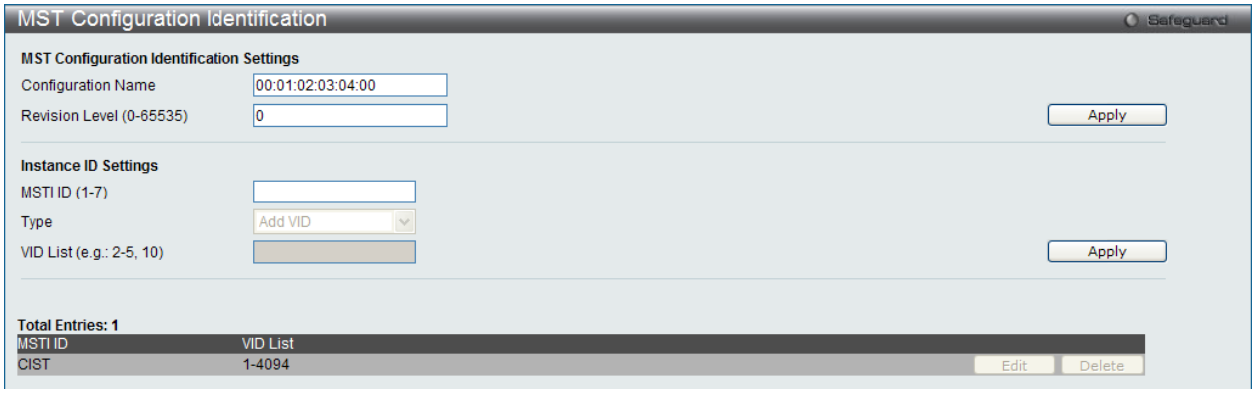


図 8-24　MST Configuration Identification 画面

上記画面には以下の項目が含まれます。

項目	説明
Configuration Name	各 MSTI（Multiple Spanning Tree Instance）を識別するためにスイッチに名前を設定します。名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level (0-65535)	スイッチ上に設定された MSTP リージョンの値を設定します。Configuration Name に同期しています。0 から 65535 の範囲で設定します。初期値は 0 です。
MSTI ID (1-7)	新規の MSTI ID を 1-7 の範囲から指定します。
Type	MSTI 設定の変更方法を指定します。2 つのタイプから選択します。 • Add VID - MSTI ID に「VID List」で指定する VID を追加します。 • Remove VID - MSTI ID から「VID List」で指定する VID を削除します。
VID List	スイッチに登録済みの VLAN の中から VID の範囲を指定します。指定できる VID の範囲は 1 から 4094 までです。

「Apply」ボタンをクリックし、デバイスに MST 設定を適用します。

エントリの編集

1. 編集するエントリ横の「Edit」ボタンをクリックし、編集画面を表示します。
2. 「MST Configuration Identification Settings」セクションに現在の設定が表示されます。設定変更後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックします。

STP Instance Settings（STP インスタンス設定）

スイッチの MSTI に関する現在の設定を表示し、MSTI のプライオリティを変更できます。

L2 Features > Spanning Tree > STP Instance Settings をクリックし、以下の画面を表示します。

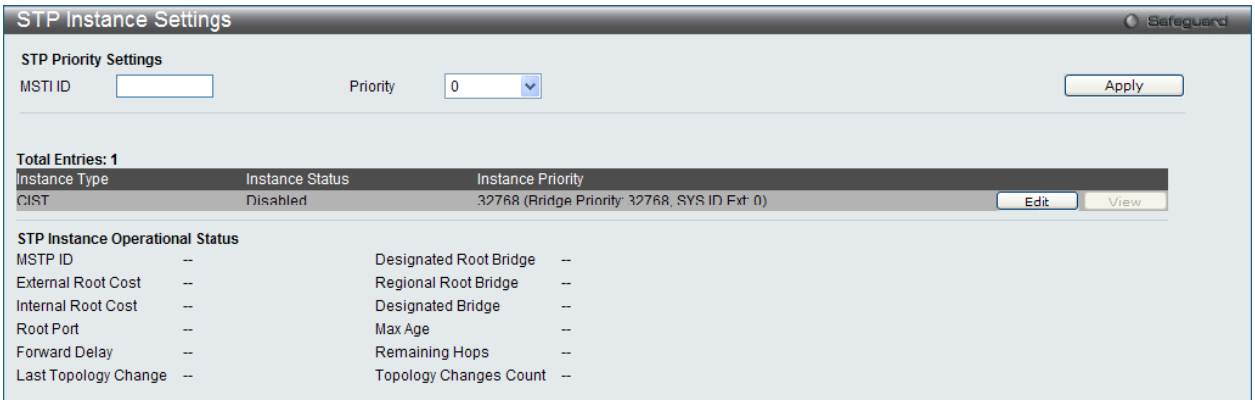


図 8-25　STP Instance Settings 画面

本画面には以下の情報があります。

項目	説明
MSTI ID	デバイスで設定した MSTP ID を設定します。0 は CIST（デフォルト MSTI）を表します。
Priority	指定したインスタンスのためのプライオリティ（0-61440）を設定します。

「Apply」ボタンをクリックし、新しいプライオリティ設定を適用します。

エントリの編集

1. 編集するエントリ横の「Edit」ボタンをクリックし、編集画面を表示します。
2. 「STP Priority Settings」セクションに現在の設定が表示されます。設定変更後、「Apply」ボタンをクリックし、設定を適用します。

エントリの詳細情報の参照

参照するエントリ横の「View」ボタンをクリックすると、STP インスタンスの状態が表示されます。

MSTP Port Information（MSTP ポート情報）

本画面では現在の MSTP ポート情報が表示され、MSTI ID 単位でポート構成の更新を行います。ループが発生した場合に MSTP 機能はポートプライオリティを使用して、Forwarding 状態に遷移させるインタフェースを選択します。最初に選択したいインタフェースには高いプライオリティ（小さい数値）を与え、最後に選択したいインタフェースには低いプライオリティ（大きい数値）を与えます。インタフェースに同じプライオリティ値が与えられている場合、MSTP は MAC アドレスの値が最小のインタフェースを Forwarding 状態にし、他のインタフェースをブロックします。低いプライオリティ値ほど転送パケットに対して高いプライオリティを意味することにご注意ください。

各ポートに MSTP の設定を行うには、**L2 Features > Spanning Tree > MSTP Port Information** の順にメニューをクリックし、以下の画面を表示します。

図 8-26　MSTP Port Information 画面

指定ポートの MSTP 設定の参照

特定ポートの MSTP 設定を参照するためには、プルダウンメニューでポート番号を選択し、「Find」ボタンをクリックします。

指定ポートの MSTI インスタンス設定の編集

1. 特定の MSTI インスタンス設定を編集する場合は、対象とする MSTI の「Edit」ボタンをクリックし、編集画面を表示します。
2. 「MSTP Port Settings」セクションに現在の設定が表示されます。「Internal Path Cost」に値を入力し、「Priority」のプルダウンメニューでプライオリティを選択し、「Apply」ボタンをクリックします。

以下の項目を設定または参照できます。

項目	説明
Port	適用するポートを選択します。
Instance ID	設定済みインスタンスの MSTI ID（0-15）。0 は CIST を意味します（初期値は MSTI）。
Internal Path Cost (1-200000000)	インタフェースを STP インスタンスで選択する場合、指定ポートにパケットを転送する相対的なコストを設定します。 • 0（Auto）- インタフェースに自動的で最適な最速のルートを設定します。（初期値） • 値 1-200000000 - ループが発生した場合、この範囲で指定した値を使用した最短のルートを設定します。コストが小さいほど高速で伝送されます。
Priority	ポートインタフェースのプライオリティ（0-240）までの値を指定します。高いプライオリティほど、パケットの転送は優先されます。値が低いほどプライオリティは高くなります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Link Aggregation（ポートトランキングの設定）

ポートトランクグループについて

ポートトランクグループは、多くのポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。本スイッチは各グループ 2 個から 8 個のポートを束ねた最大 26 個のポートトランクグループをサポートしています。800Mbps のビットレートを実現する可能性があります。

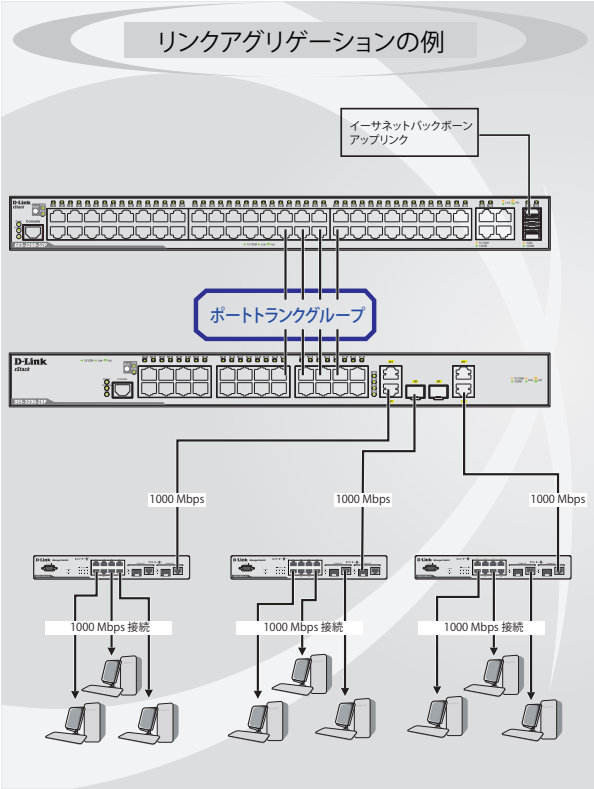


図 8-27　ポートトランクグループの例

設定可能なポートトランクグループ数（DES-3200）

DES-3200-10/T：5 グループ / デバイス、8 ポート / グループ
DES-3200-18/T：9 グループ / デバイス、8 ポート / グループ
DES-3200-26/T：13 グループ / デバイス、8 ポート / グループ
DES-3200-28/T、28F、28P：14 グループ / デバイス、8 ポート / グループ
DES-3200-52/T、52P：26 グループ / デバイス、8 ポート / グループ

スイッチはトランクグループ内のすべてのポートを 1 つのポートと見なします。あるホスト（宛先アドレス）へのデータ転送は、トランクグループ内のいつも同じポートから行われます。これにより、データが送信された順に受け取られるようになります。

リンクアグリゲーション機能により、 1 つのグループとして束ねられたポートは、1 つのリンクの働きをします。この時、 1 つのリンクの帯域は、束ねられたポート分拡張されます。

リンクアグリゲーションは、サーバやバックボーンなど、広帯域を必要とするネットワークデバイスにおいて広く利用されています。

本スイッチでは、2 から 8 のリンク（ポート）で構成する最大 26 個のリンクアグリゲーショングループをサポートします。オプションのギガビットポートは 1 つのリンクアグリゲーショングループにだけ所属できます。

1 つのグループ内の全ポートは同じ VLAN に属し、それぞれのスパニングツリープロトコル（STP）ステータス、スタティックマルチキャスト、トラフィックコントロール、トラフィックセグメンテーション、および 802.1p デフォルトプライオリティの設定は同じである必要があります。また、ポートブロッキング、ポートミラーリング、および 802.1X は有効化されていてはなりません。さらに、集約するリンクはすべて同じ速度で、全二重モードで設定されている必要があります。

グループのマスタポートの設定はユーザにより行われます。また、マスタポートに適用される VLAN 設定を含むすべての設定オプションは、グループ内全体に適用されます。

グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断によって発生するネットワークトラフィックは、グループ内の他のリンクに振り分けられます。

スパニングツリープロトコル（STP）は、スイッチレベルにおいて、リンクアグリゲーショングループを 1 つのリンクとしてとらえます。ポートレベルでは STP はマスタポートのポートパラメータを使用してポートコストを計算し、リンクアグリゲーショングループの状態を決定します。スイッチ上に 2 つのリンクアグリゲーショングループが冗長して設定された場合、STP は冗長リンクを持つポートのブロックを行うのと同様に、 1 つのグループをブロックします。

注意　トランクグループ内のあるポートが接続不可になると、そのポートが処理するパケットは他のリンクアグリゲーション（集約）グループ内の他のポート間でロードシェアされます。

Port Trunking Settings（ポートトランキング設定）

スイッチにポートトランクを設定します。

L2 Features > Link Aggregation > Port Trunking Settings の順にクリックし、以下の画面を表示します。

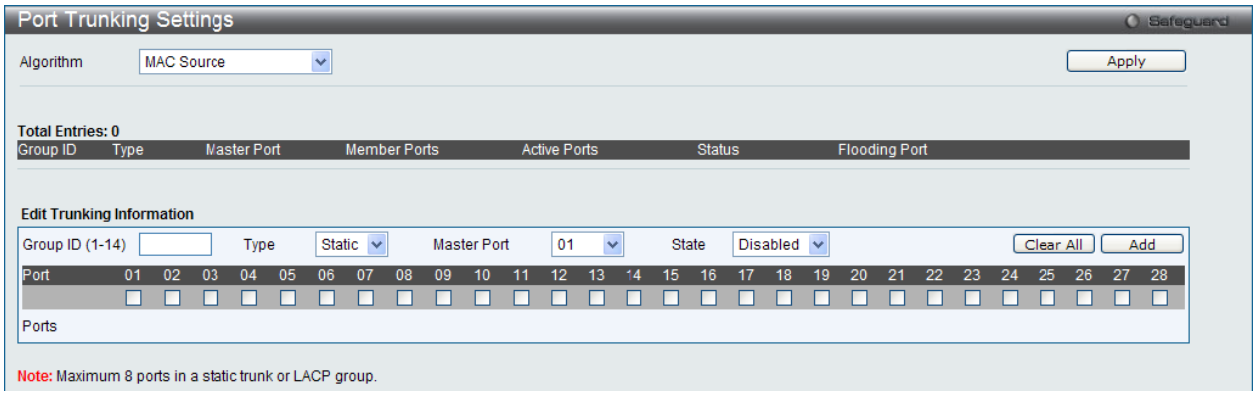


図 8-28　Port Trunking Settings 画面

本画面には次の項目があります。

項目	説明
Algorithm	ポートトランクグループを構成するポートのロードバランスに使用するアルゴリズムを選択します。「MAC Source」、「MAC Destination」、「MAC Source Destination」、「IP Source」、「IP Destination」、「IP Source Dest」、「L4 Port Source」、「L4 Port Destination」、「L4 Source Dest」から指定してください。
Edit Trunking Information	
Group ID (1-14)	グループの ID 番号を 1-14 の範囲から指定します。（DES-3200-28P の場合）
Type	トランキンググループの種類を設定します。「Static」または「LACP」から選択します。LACP（Link Aggregation Control Protocol）を選択すると、ポートトランキンググループ内でのリンクの自動検出を行います。
Master Port	トランキンググループのマスタポートを選択します。
State	ポートトランキンググループを「Enabled」（有効）または「Disabled」（無効）にします。これは、診断、迅速に帯域が集中するネットワークデバイスの迅速な分離する場合、または自動制御下にない独立したバックアップアグリゲーショングループを持つ場合に有益です。
Member Ports	トランキンググループのメンバポートを選択します。各グループに 8 ポートまで割り当てることができます。
Active Ports	現在パケットの送出を行っているポートが表示されます。
Flooding Ports	本ポートは、トランクグループ内の CPU から送信されるフラッディングブロードキャスト、マルチキャスト、および DLF (unicast Destination Lookup Fail) パケットのために設計されています。また、ソフトウェアによって定義されており、ハードウェアには存在しません。

ポートトランキンググループの設定

各項目を入力後、「Add」ボタンをクリックし、ポートトランキンググループを設定します。

ポートトランクグループの編集

1. 画面上部で編集するグループの「Edit」ボタンをクリックし、編集画面を表示します。
2. 項目を編集後「Apply」ボタンをクリックします。

ポートトランキンググループの削除

編集するポートトランキンググループを削除するためには、削除するグループの「Delete」ボタンをクリックします。「Clear All」ボタンをクリック

注意　ひとつのスタティックもしくは LACP グループに設定可能な最大ポート数は 8 です。

LACP Port Settings（LACP ポートの設定）

スイッチにポートトランキンググループを作成します。LACP 制御フレームの処理と送出を行う際、どのポートが「Active」または「Passive」の役割を担うかを指定します。

L2 Features > Link Aggregation > LACP Port Settings の順にメニュークリックし、以下の画面を表示します。

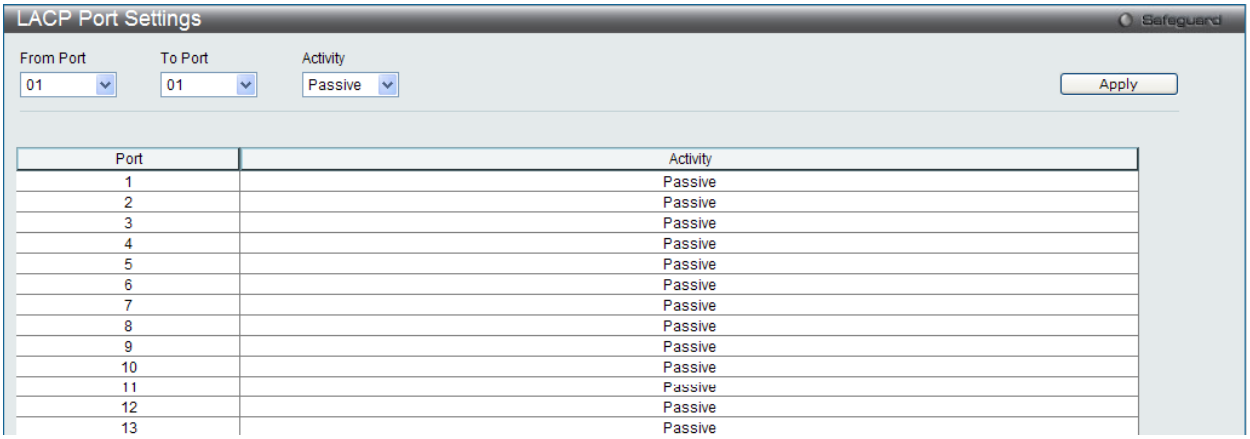


図 8-29　LACP Port Settings 画面

以下の項目を使用して設定を行います。

項目	説明
From Port / To Port	設定対象のポート範囲を指定します。
Activity	• Active - Active ポートは LACP 制御フレームの処理と送信を行います。これにより LACP 準拠のデバイス同士はネゴシエーションとリンクの集約を行い、グループは必要に応じて動的に変更されます。グループへのポート追加、または削除などのグループの変更を行うためには、少なくともどちらかのデバイスで LACP ポートを「Active」に設定する必要があります。また、両方のデバイスは LACP をサポートしている必要があります。 • Passive - Passive ポートは自分から LACP 制御フレームの送信を行いません。リンクするポートグループがネゴシエーションを行い、動的にグループの変更を行うためには、接続のどちらか一端が Active な LACP ポートである必要があります。（初期値）

「Apply」ボタンをクリックし、デバイスに LACP 設定を適用します。

FDB（FDB 設定）

Static FDB Settings（スタティック FDB の設定）

Unicast Static FDB Settings（ユニキャストスタティック FDB の設定）

スイッチにスタティックなユニキャストフォワーディングを設定します。

L2 Features > FDB > Static FDB Settings > Unicast Static FDB Settings の順にメニュークリックし、以下の画面を表示します。

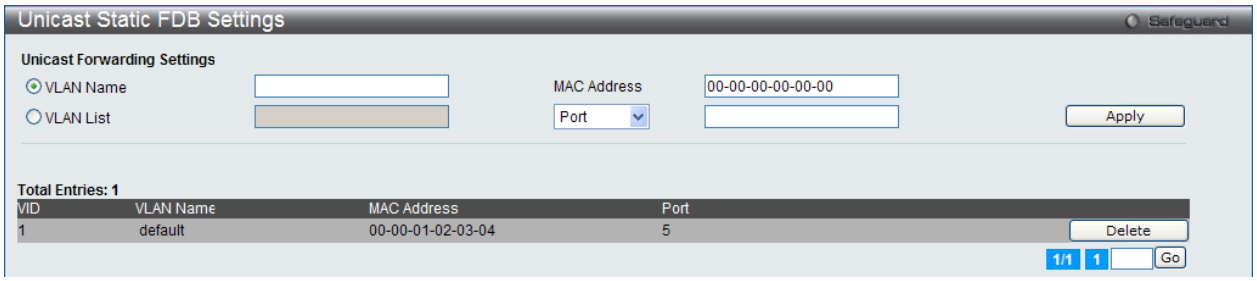


図 8-30　Unicast Static FDB Settings 画面

以下の項目を使用して設定を行います。

項目	説明
VLAN Name	ラジオボタンをクリックし、関連するユニキャスト MAC アドレスが存在する VLAN 名を入力します。
VLAN List	ラジオボタンをクリックし、関連するユニキャスト MAC アドレスが存在する VLAN リストを入力します。
MAC Address	パケットがスタティックに送信される宛先の MAC アドレス。ユニキャスト MAC アドレスを指定します。
Port/Drop	上記 MAC アドレスのあるポート番号を指定します。また、ユニキャストのスタティックな FDB から MAC アドレスを破棄します。 • Port - 上記 MAC アドレスのあるポート番号を指定します。 • drop - ユニキャストのスタティックな FDB から MAC アドレスを破棄します。

「Apply」ボタンをクリックして設定を適用します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

Multicast Static FDB Settings（マルチキャストスタティック FDB の設定）

スイッチにスタティックなマルチキャストフォワーディングを設定します。

L2 Features > FDB > Static FDB Settings > Unicast Static FDB Settings の順にメニュークリックし、以下の画面を表示します。

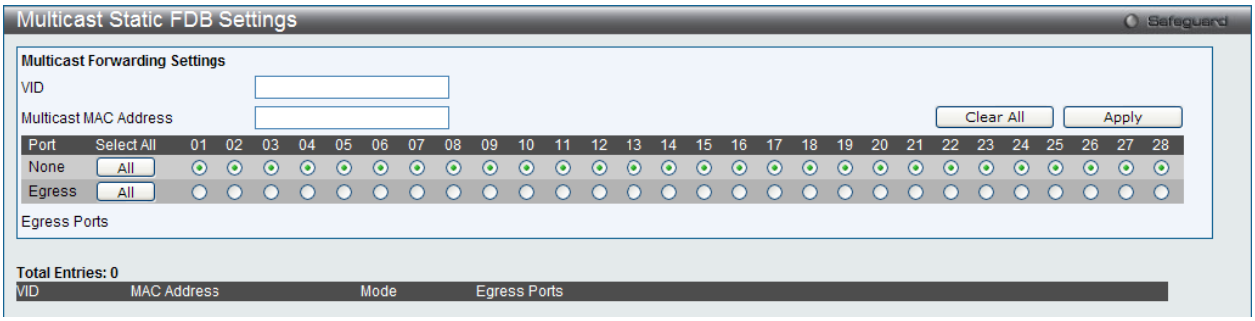


図 8-31　Multicast Static FDB Setting 画面

以下の項目を使用して設定を行います。

項目	説明
VID	指定の Multicast MAC アドレスが属する VLAN の VLAN ID。
Multicast MAC Address	マルチキャストパケットの送信先 MAC アドレス。マルチキャスト MAC アドレスを指定します。
Port	スタティックマルチキャストグループのメンバとなるポート、および GMRP によってダイナミックにグループに参加させるポート、参加させないポートを選択します。オプションは以下の通りです。 • None - ダイナミックにマルチキャスト参加を行います。指定すると、ポートはスタティックマルチキャストグループのメンバにはなりません。「All」ボタンをクリックするとすべてのポートを選択します。 • Egress - ポートはマルチキャストグループのスタティックメンバとなります。「All」ボタンをクリックするとすべてのポートを選択します。

「Apply」ボタンをクリックして設定を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 項目を編集後「Apply」ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。「Clear All」ボタンをクリックして、すべての情報エントリをクリアします。

MAC Notification Settings（MAC 通知設定）

MAC Notification（通知）は、学習によりフォワーディングデータベースに記録された MAC アドレスの監視を行うために使用します。スイッチの MAC 通知をグローバルに設定します。また、スイッチの各ポートに MAC 通知を設定します。

注意 本機能をご使用になる場合、NMS 側で、MAC Notification トラップを受信できる環境が必要になります。E-mail や Syslog における通知には対応しておりません。

L2 Features > FDB > MAC Notification Settings の順にメニューをクリックし、以下の画面を表示します。

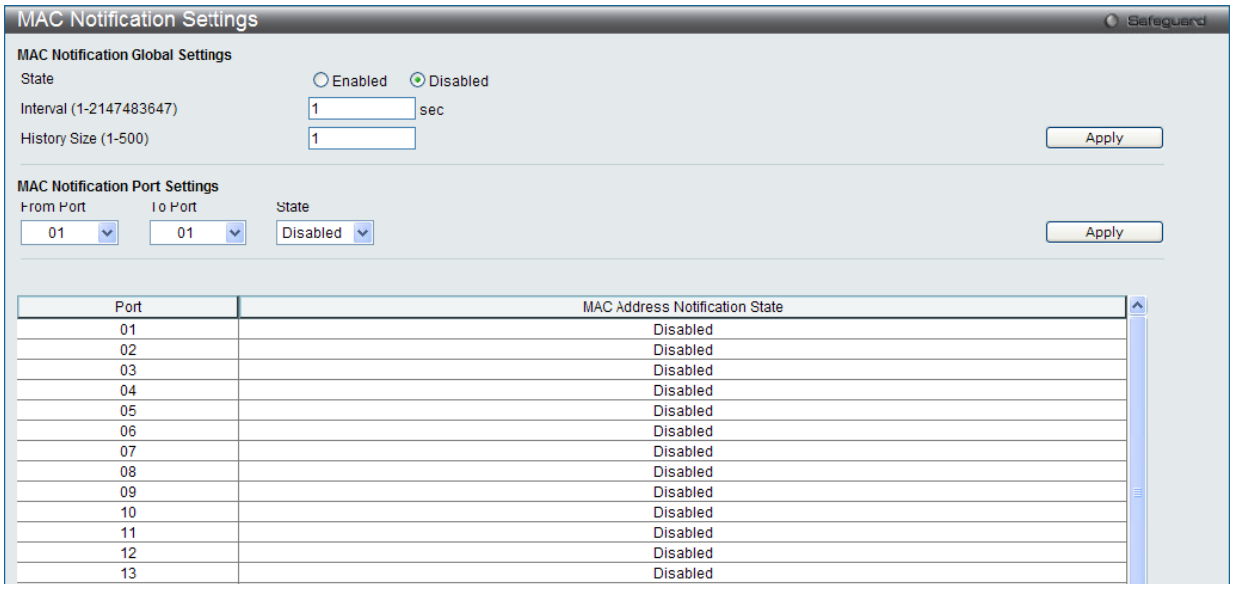


図 8-32　MAC Notification Settings 画面

以下の項目を使用して設定を行います。

項目	説明
MAC Notification Global Settings	
State	スイッチ上の MAC 通知をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Interval (1-2147483647)	通知を行う間隔（秒）。初期値 : 1（秒）
History Size (1-500)	通知に使用するヒストリログの最大エントリ数（最大 500 エントリ）。初期値 : 1
MAC Notification Port Settings	
From Port / To Port	プルダウンメニューを使用して MAC 通知を有効にするポート範囲を指定します。
State	指定したポートの MAC 通知設定を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。

各セクションの「Apply」ボタンをクリックして行った変更を適用します。

MAC Address Aging Time Settings（MAC アドレスエージングタイムの設定）

スイッチに MAC アドレスエージングタイムを設定します。

L2 Features > FDB > MAC Address Aging Time の順にクリックし、以下の画面を表示します。

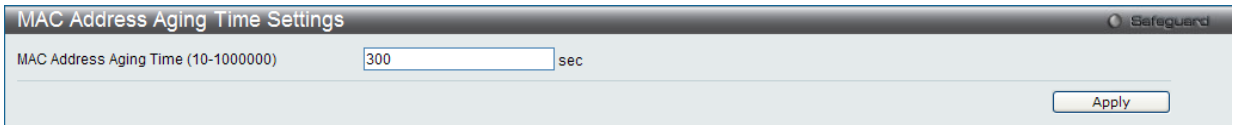


図 8-33　MAC Address Aging Time Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
MAC Address Aging Time (10-1000000)	学習した MAC アドレスがアクセスされないままフォワーディングテーブルに保存される時間（学習した MAC アドレスがアイドル状態でいる時間）。 この値を変更するためには、MAC アドレスエージングタイム（秒）を示す別の値を入力します。10-1000000（秒）の範囲で値を入力します。初期値は 300（秒）です。

「Apply」ボタンをクリックし、MAC アドレスエージングタイム設定を適用します。

MAC Address Table（MAC アドレステーブル）

スイッチの MAC アドレスフォワーディングテーブルを参照します。スイッチが MAC アドレス、VLAN、およびポート番号間の関連性を学習するとテーブルに記載します。それらのエントリは、スイッチ経由でパケットを送信するのに使用されます。

L2 Features > FDB > MAC Address Table の順にメニューをクリックし、以下の画面を表示します。

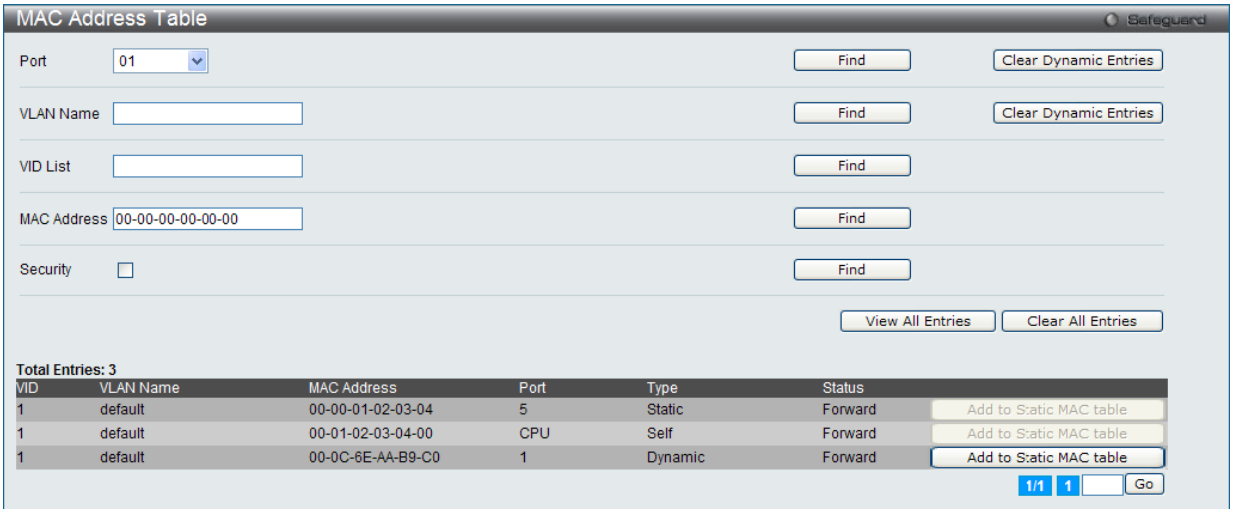


図 8-34　MAC Address Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	以下の MAC アドレスと関連付けられるポート。
VLAN Name	参照するフォワーディングテーブルの VLAN 名を入力します。
VID List	参照するフォワーディングテーブルの VLAN ID リストを入力します。
MAC Address	参照するフォワーディングテーブルの MAC アドレスを入力します。
Security	チェックすると、セキュリティモジュールによって作成される FDB エントリを表示します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

エントリの検索

「Find」ボタンをクリックして、指定したポート、VLAN または MAC アドレスをキーとして検索します。

ダイナミックエントリの削除

「Clear Dynamic Entries」ボタンをクリックして、アドレステーブルのすべてのダイナミックエントリを削除します。

エントリの表示

「View All Entries」ボタンをクリックして、アドレステーブルのすべてのエントリを表示します。

全エントリの削除

「Clear All Entries」ボタンをクリックして、アドレステーブルのすべてのエントリを表示します。

エントリの追加

「Add to Static MAC table」ボタンをクリックして、スタティックテーブルに指定エントリを追加します。

ARP & FDB Table（ARP と FDB テーブル）

ARP と FDB テーブルのパラメータを検索します。

L2 Features > FDB > ARP & FDB の順にメニューをクリックし、以下の画面を表示します。

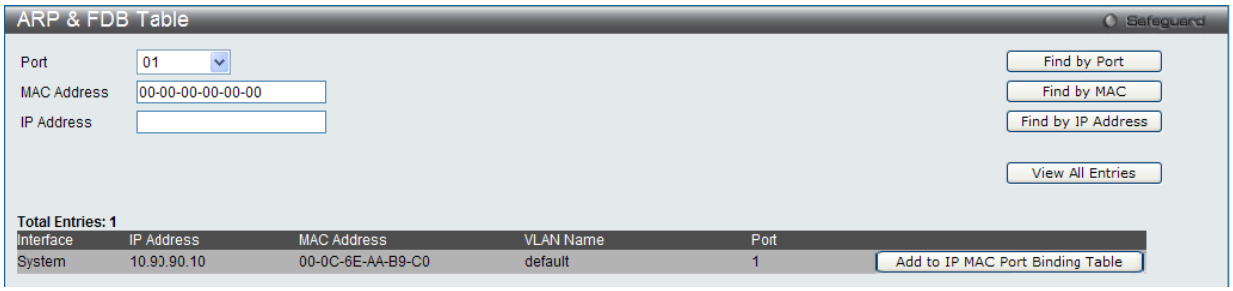


図 8-35　ARP & FDB Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	この設定に使用するポート番号を選択します。
MAC Address	本設定に使用する MAC アドレスを指定します。
IP Address	本設定に使用する IP アドレスを入力します。

エントリの検索（ポートベース）

「Find by Port」ボタンをクリックして、選択したポート番号に基づく特定のエントリを検出します。

エントリの検索（MAC ベース）

「Find by MAC」ボタンをクリックして、入力した MAC アドレスに基づく特定のエントリを検出します。

エントリの検索（IP アドレスベース）

「Find by IP Address」ボタンをクリックして、入力した IP アドレスに基づく特定のエントリを検出します。

エントリの表示

「View All Entries」ボタンをクリックして、すべてのエントリを表示します。

エントリの追加

「Add to IP MAC Port Binding Table」ボタンをクリックして、IP MAC ポートバインディングテーブルに指定エントリを追加します。

L2 Multicast Control（L2 マルチキャストコントロール）

IGMP Snooping（IGMP Snooping の設定）

IGMP（Internet Group Management Protocol）Snooping 機能を利用すると、スイッチはネットワークステーションまたはデバイスと IGMP ホスト間で送信される IGMP クエリと IGMP レポートを認識するようになります。また、スイッチを通過する IGMP メッセージの情報に基づいて、指定したデバイスに接続するポートをオープン / クローズできるようになります。

IGMP Snooping Settings（IGMP Snooping 設定）

IGMP Snooping 設定をグローバルに有効または無効にします。

IGMP Snooping 機能を利用するためには、まず、画面上にある「IGMP Snooping Global Settings」でスイッチ全体を有効にする必要があります。その後、対応する「Edit」ボタンをクリックして、各 VLAN に詳細な設定を行います。

IGMP Snooping を有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバに接続するポートをオープンまたはクローズできるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストがもう存在していないと判断すれば、マルチキャストパケットの送信を停止します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings の順にクリックし、以下の画面を表示します。

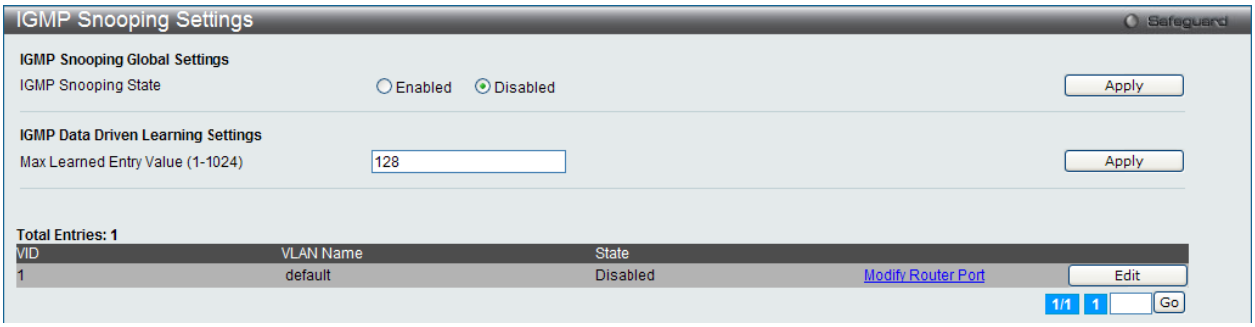


図 8-36　IGMP Snooping Settings 画面

画面には以下の項目があります。

項目	説明
IGMP Snooping Global Settings	
IGMP Snooping State	IGMP Snooping 状態を有効または無効にします。 • Enabled - デバイスで IGMP Snooping を有効にします。 • Disabled - デバイスで IGMP Snooping を無効に設定します。（初期値）
Max Learned Entry Value (1-1024)	学習するグループの最大エントリ数を指定します。

IGMP Snooping 機能の利用

画面上部の「IGMP Snooping Global Settings」セクションでスイッチ全体に機能を有効にします。

1. 「IGMP Snooping State」の「Enabled」ボタンをクリックします。
2. 「Apply」ボタンをクリックして、IGMP Snooping 設定を適用します。

IGMP Snooping 機能の詳細設定

関連する VLAN エントリの「Edit」ボタンをクリックし、以下の画面を表示して各 VLAN に対して詳細な設定を行います。

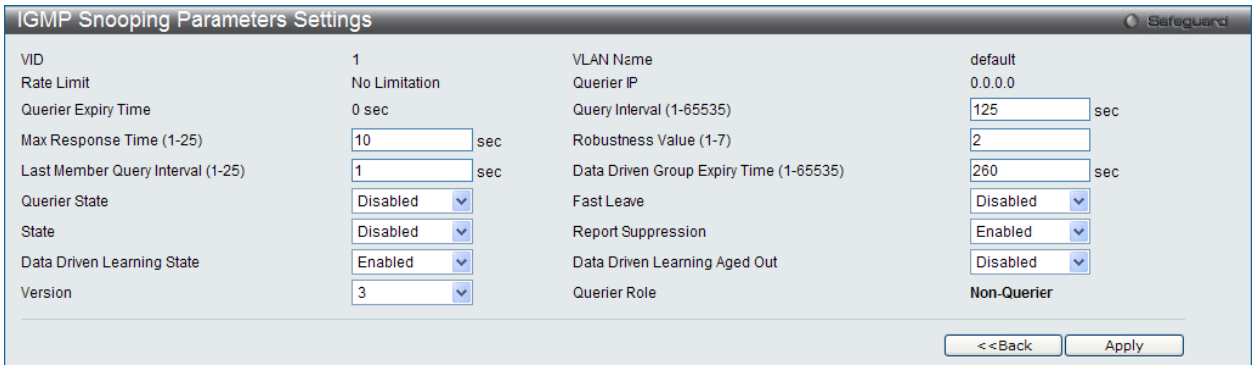


図 8-37　IGMP Snooping Parameters Settings 画面

以下の項目を参照または編集することができます。

項目	説明
VID	VLAN ID を表示します。VLAN 名と共に、IGMP Snooping 設定の対象となる VLAN を識別するために使用します。
VLAN Name	IGMP Snooping クエリアを設定する VLAN 名を表示します。VLAN ID と共に、IGMP Snooping 設定を行う対象の VLAN を識別します。
Rate Limit	スイッチが特定のポート /VLAN で処理できる IGMP 制御パケットのレートを表示します。レートはパケット / 毎秒で指定されます。制限レートを超過したパケットは破棄されます。
Querier IP	ネットワークに IGMP クエリを送信するデバイスの IP アドレスを表示します。
Querier Expiry Time	クエリアの有効時間を表示します。
Query Interval (1-65535)	一般的な IGMP クエリア送信間隔（秒）を指定します。初期値は 125（秒）です。
Max Response Time (1-25)	メンバからのレポートを待つ最大時間を 1-25（秒）で設定します。初期値は 10（秒）です。
Robustness Value (1-7)	予想されるサブネット上のパケットの損失に応じてこの変数を調整します。Robustness Variable は以下の IGMP メッセージ間隔の計算に使用されます。1-7 の範囲から指定します。初期値は 2 です。
Last Member Query Interval (1-25)	Group-Specific Query メッセージ（Leave Group メッセージに応じて送信されるものも含む）の最大送信間隔を指定します。この間隔はルータがグループのラストメンバの損失を検出するためにかかる時間をより減少するように低くします。初期値は 1 です。
Data Driven Group Expiry Time (1-65535)	使用する Data Driven グループの生存時間を指定します。
Querier State	クエリア状態を有効または無効にします。 • Enabled - スイッチが IGMP クエリパケットを送信する IGMP クエリアとして選択されます。 • Disabled - スイッチが IGMP クエリアとしての役目を果たしません。
Fast Leave	IGMP Snooping の Fast Leave 機能を有効または無効にします。有効にすると、システムが IGMP Leave メッセージを受信するとメンバはすぐにグループから削除されます。
State	指定した VLAN への IGMP Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。有効の場合、スイッチが IGMP クエリパケットを送信する IGMP クエリアとして選択され、無効の場合、スイッチが IGMP クエリアとしての役目を果たしません。 **注意** スイッチに接続するレイヤ 3 ルータが IGMP プロキシ機能だけを提供し、マルチキャストルーティング機能を提供しない場合、この状態は無効に設定されます。そうでない場合、レイヤ 3 ルータをクエリアとして選択しないと、IGMP クエリパケットを送信しません。また、マルチキャストルーティングプロトコルパケットを送信しないため、ポートはルータポートとしてタイムアウトになります。
Report Suppression	有効にすると、特定の (S、G) に対する複数の IGMP レポートまたはリーブがルータポートに送信される前に 1 つのレポートに統合されます。
Data Driven Learning State	Data Driven Learning 状態を有効または無効にします。
Data Drive Learning Aged Out	Data Driven Learning のエージングアウトオプションを有効または無効にします。
Version	スイッチが送信する IGMP general クエリのバージョンを指定します。
Querier Role	Query パケット送信についてのスイッチの動作を表示します。 • Querier - スイッチが MLD Query パケットの送信を行います。 • Non-Querier - スイッチが MLD Query パケットの送信を行いません。 本項目は「Querier State」と「State」で「Enabled」指定時には「Querier」と表示されます。

上記項目設定後、「Apply」ボタンをクリックして変更を有効にします。

前の画面に戻るためには、「<< Back」ボタンをクリックします。

IGMP Snooping ルータポート設定の変更

対応する「Modify Router Port」リンクをクリックし、以下の画面を表示します。

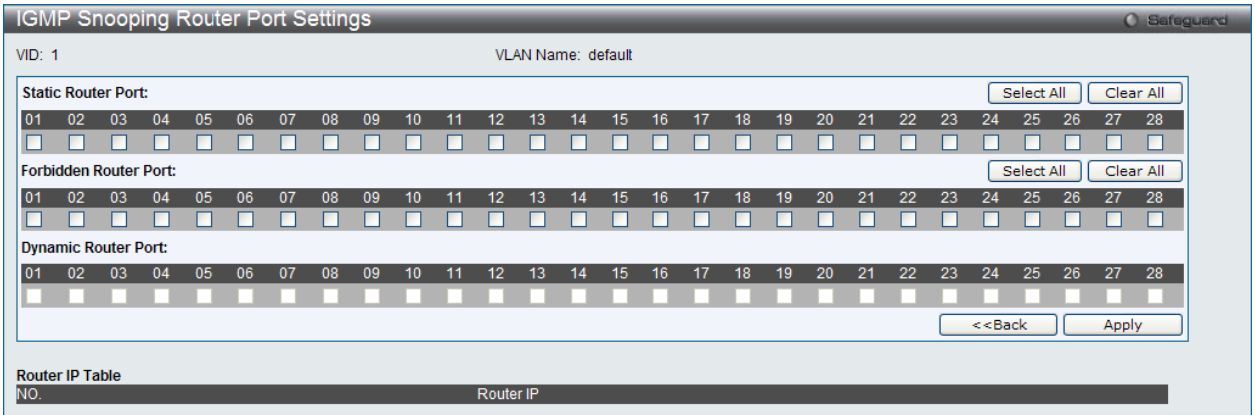


図 8-38　IGMP Snooping Router Ports Settings 画面

以下の項目を設定または表示します。

項目	説明
Static Router Port	マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先としてルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストが有効なルータに到達するように設定します。
Forbidden Router Port	マルチキャストが有効なルータに接続しないポート範囲を指定します。これは、禁止ポートがルーティングパケットを送信しないように設定します。
Dynamic Router Port	ダイナミックに設定されたルータポートを表示します。

メンバにするポートのチェックボックスを選択して「Apply」ボタンをクリックします。

「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。
「IGMP Snooping Settings」画面に戻るためには、「<<Back」ボタンをクリックします。

IGMP Snooping Rate Limit Settings（IGMP Snooping レート制限設定）

IGMP Snooping レート制限パラメータを設定します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Rate Limit Settings の順にクリックし、以下の画面を表示します。

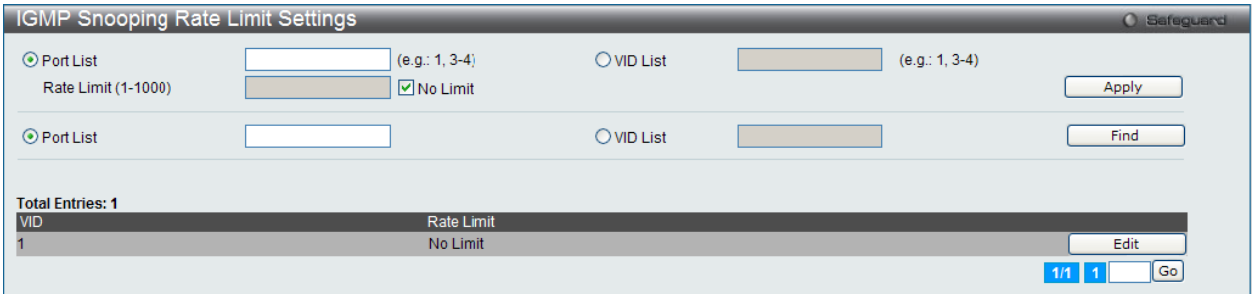


図 8-39　IGMP Snooping Rate Limit Settings 画面

以下の項目があります。

項目	説明
Port List	本設定に使用するポートリストを指定します。
VID List	本設定に使用する VID リストを指定します。
Rate Limit (1-1000)	使用する IGMP Snooping レート制限を入力します。「No Limit」を選択すると、入力ポートのレート制限は無視されます。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IGMP Snooping Static Group Settings（IGMP Snooping スタティックグループ設定）

スイッチの IGMP Snooping スタティックグループテーブルを参照します。IGMP Snooping 機能では、スイッチを通過する IGMP パケットからマルチキャストグループ IP アドレスと対応する MAC アドレスを読み取ることができます。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Static Group Settings の順にクリックし、以下の画面を表示します。

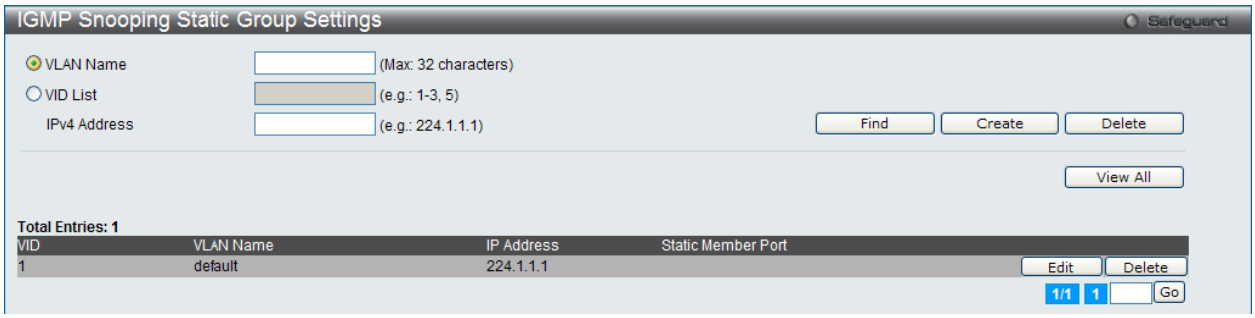


図 8-40　IGMP Snooping Static Group Settings 画面

以下の項目を設定または表示します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名を入力します。
VID List	マルチキャストグループの VID リストを入力します。
IPv4 Address	IPv4 アドレスを指定します。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

エントリの登録

「VLAN Name」または「VID List」、および「IPv4 Address」入力後、「Create」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

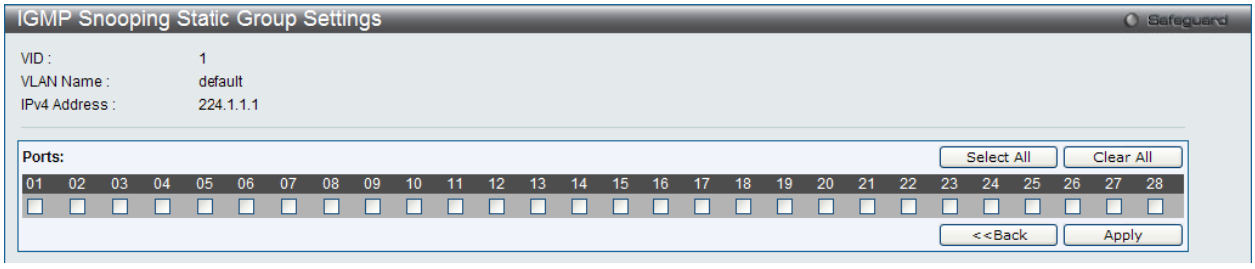


図 8-41　IGMP Snooping Static Group Settings 画面

2. 以下の項目を設定または表示します。

項目	説明
Ports	個別に適切なポートを選択して、IGMP Snooping スタティックグループ設定に含めます。

「Apply」ボタンをクリックして行った変更を適用します。

「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

IGMP Router Port（ルータポート参照）

スイッチが現在ルータポートとして設定しているポートを表示します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Router Port メニューをクリックして、以下の画面を表示します。

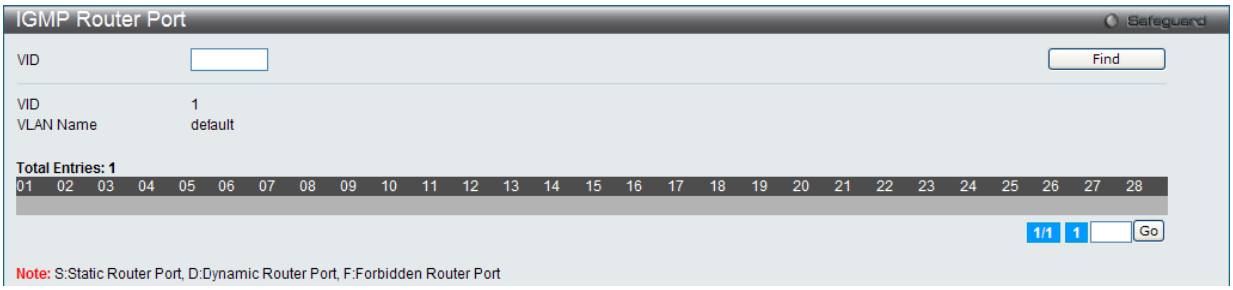


図 8-42　IGMP Router Port 画面

1. 画面上の VID(VLAN ID) を入力します。

2. 「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

コンソールまたは Web ベースの管理インタフェースで設定されたルータポートはスタティックルータポートとして「S」で表示されます。スイッチにダイナミックに設定されたルータポートは「D」と表示され、Forbidden ポートは「F」と表示されます。

IGMP Snooping Group（IGMP Snooping グループ）

スイッチの IGMP Snooping グループテーブルを参照します。IGMP Snooping 機能では、スイッチを通過する IGMP パケットからマルチキャストグループの IP アドレスと送信元の IP アドレスを読み取ることができます。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Group の順にメニューをクリックし、以下の画面を表示します。

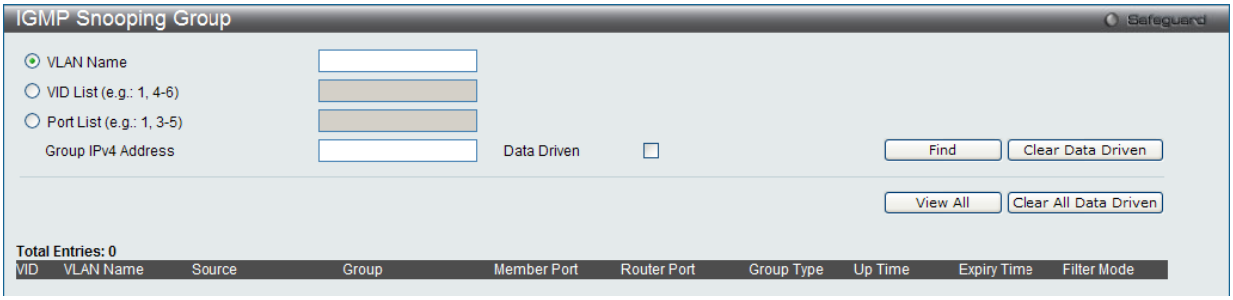


図 8-43　IGMP Snooping Group 画面

以下の項目があります。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List	マルチキャストグループの VLAN ID リスト。
Port List	マルチキャストグループを検索するのに使用されるポート番号を指定します。
Group IPv4 Address	IPv4 アドレスを指定します。
Data Driven	選択すると、Data Driven グループだけを表示します。

エントリの参照

画面左上の「VLAN Name」または「VID」を入力して「Find」ボタンをクリックすることにより、IGMP Snooping グループテーブルを検索することができます。「View All」ボタンをクリックして、すべての定義済みエントリを表示します。検索されたエントリは「IGMP Snooping Group Table」に表示されます。

Data Driven 情報のクリア

「Clear Data Driven」ボタンをクリックして、指定 VLAN の Data Driven 機能が学習した IGMP Snooping グループをクリアします。「Clear All Data Driven」ボタンをクリックして、すべての Data Driven 情報をクリアします。

IGMP Snooping Forwarding Table（IGMP Snooping フォワーディングテーブル）

スイッチ上の現在の IGMP Snooping フォワーディングテーブルのエントリを表示します。

マルチキャストグループを送出するポートリストと転送される特定の送信元をチェックする簡単な方法を提供します。送信元 VLAN からのパケットをフォワーディング VLAN に転送します。さらに、IGMP Snooping はフォワーディングポートを制限します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Forwarding Table の順にメニューをクリックし、以下の画面を表示します。

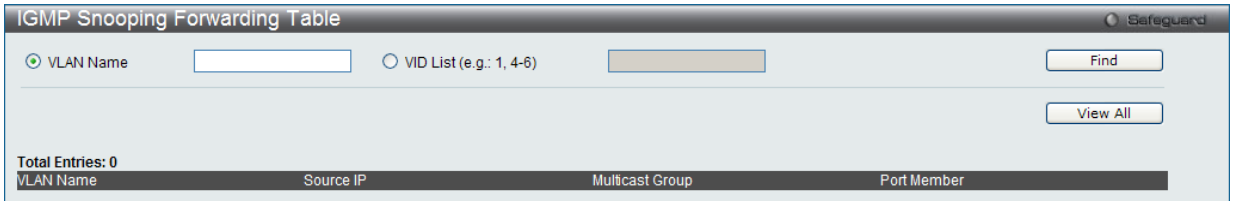


図 8-44　IGMP Snooping Forwarding Table 画面

以下の項目が表示されます。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List	マルチキャストグループの VLAN ID リスト。

エントリの参照

画面左上の「VLAN Name」欄に VLAN 名を入力して「Find」ボタンをクリックすることにより、テーブル内を検索することができます。
「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

カウンタテーブルの参照

「Packet Statistics」リンクをクリックして、IGMP Snooping カウンタテーブルを参照します。

IGMP Snooping Counter（IGMP Snooping カウンタ）

スイッチの IGMP Snooping カウンタテーブルを参照します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Counter の順にメニューをクリックし、以下の画面を表示します。

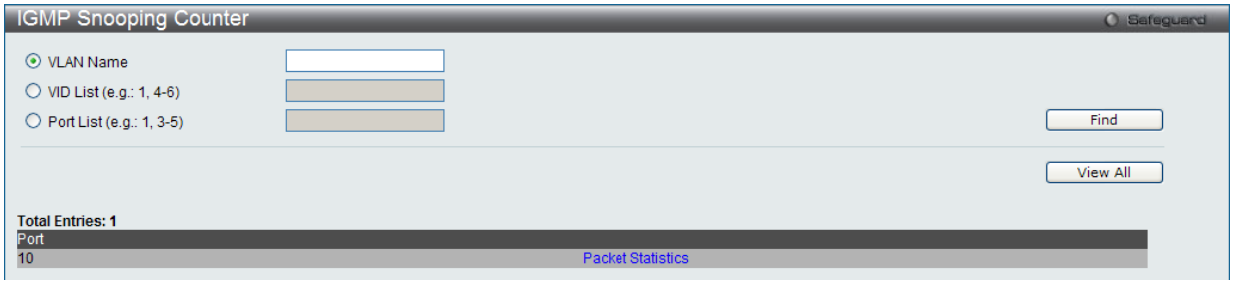


図 8-45　IGMP Snooping Counter 画面

以下の項目が表示されます。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List	マルチキャストグループの VLAN ID リスト。
Port List	マルチキャストグループのポートリスト。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

IGMP Snooping カウンタテーブルの参照

「Packet Statistics」リンクをクリックすると、以下の画面が表示されます。

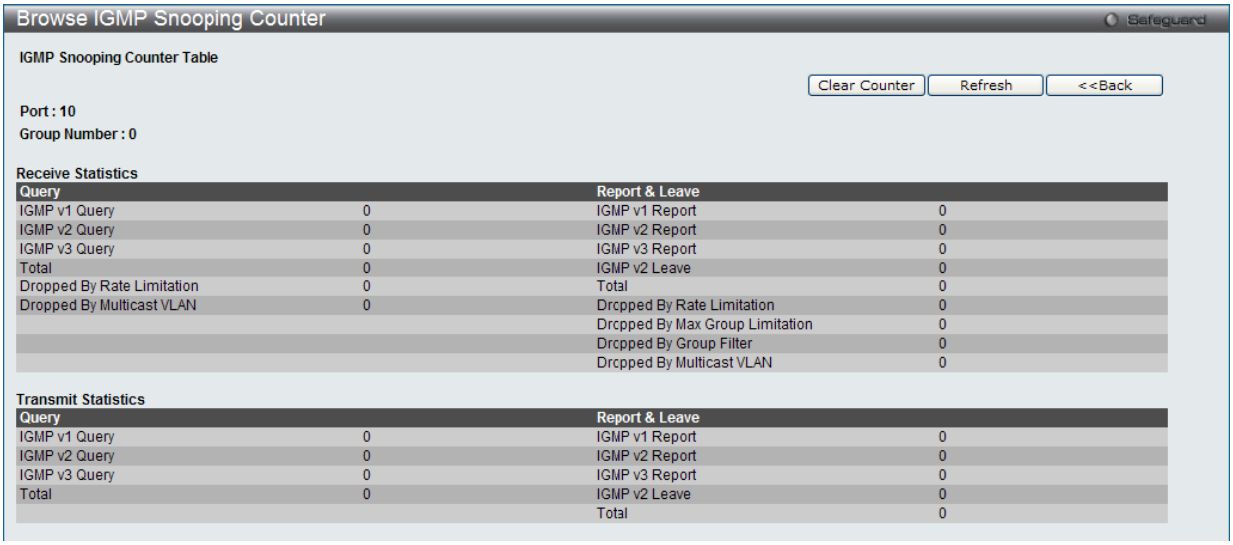


図 8-46　Browse IGMP Snooping Counter 画面

「Clear Counter」ボタンをクリックして、本欄に表示したすべてのエントリをクリアします。
「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。
「<<Back」をボタンをクリックして前のページに戻ります。

CPU Filter L3 Control Packet Settings（CPU フィルタ L3 コントロールパケット設定）

指定ポートから CPU に送信される L3 コントロールパケットを破棄および表示します。

L2 Features > L2 Multicast Control > IGMP Snooping > CPU Filter L3 control Packet Settings の順にメニューをクリックし、以下の画面を表示します。:

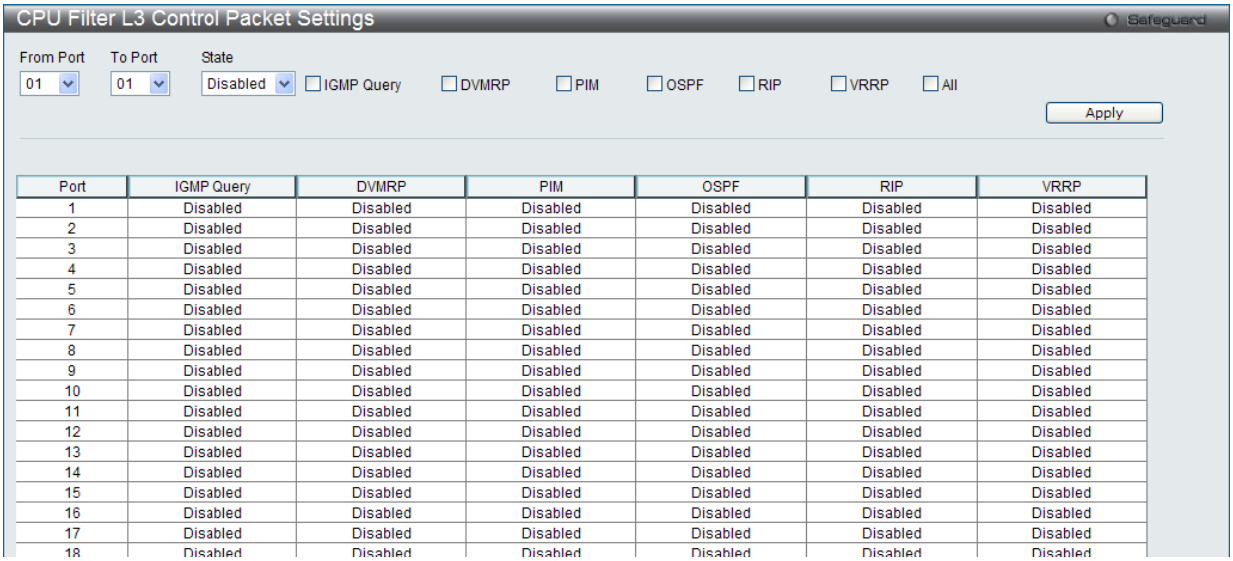


図 8-47　CPU Filter L3 Control Packet Settings 画面

以下の項目が表示されます。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
State	フィルタリング機能を「Enabled」（有効）/「Disabled」（無効）にします。チェックしたプロトコルをフィルタリングします。 • IGMP Query - IGMP Query プロトコルパケットのフィルタリングを有効または無効にします。 • DVMRP - DVMRP プロトコルパケットのフィルタリングを有効または無効にします。 • PIM - PIM プロトコルパケットのフィルタリングを有効または無効にします。 • OSPF - OSPF プロトコルパケットのフィルタリングを有効または無効にします。 • RIP - RIP プロトコルパケットのフィルタリングを有効または無効にします。 • VRRP - VRRP プロトコルパケットのフィルタリングを有効または無効にします。 • All - すべてのレイヤ 3 コントロールパケットのフィルタリングを有効または無効にします。

「Apply」ボタンをクリックして行った変更を適用します。

MLD Snooping（MLD Snooping 設定）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じように使用される IPv6 機能です。マルチキャストデータを要求する VLAN に接続しているポートを検出するために使用されます。選択した VLAN 上のすべてのポートにマルチキャストトラフィックが流れる代わりに、MLD Snooping は、リクエストポートとマルチキャストの送信元によって生成する MLD クエリと MLD レポートを使用してデータを受信したいポートにのみマルチキャストデータを転送します。

MLD Snooping は、エンドノードと MLD ルータ間で交換される MLD コントロールパケットのレイヤ 3 部分を調査することで実行されます。ルータがマルチキャストトラフィックをリクエストしていることをスイッチが検出すると、該当ポートを IPv6 マルチキャストテーブルに直接追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のこのエントリは該当ポート、その VLAN ID、および関連する IPv6 マルチキャストグループアドレスを記録し、このポートをアクティブな Listening ポートと見なします。アクティブな Listening ポートはマルチキャストグループデータの受信だけをします。

MLD コントロールメッセージ

MLD Snooping バージョン 1 の実行には、デバイス間で 3 つのタイプのメッセージが送信されます。これらのメッセージは、130、131、132 および 143 にラベル付けされた ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query
IPv4 の IGMPv2 Host Membership Query（HMQ）と類似のものです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query は全マルチキャストアドレスに Listening ポートすべてにマルチキャストデータを送信する準備が整ったことを通知するために使用します。また、Multicast Specific query は特定のマルチキャストアドレスに送信準備が整ったことを通知するために使用します。 2 つのメッセージタイプは IPv6 ヘッダ内のマルチキャスト終点アドレス、および Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別します。

2. Multicast Listener Report Version1
IGMPv2 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMP パケットヘッダ内に 131 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

3. Multicast Listener Done
IGMPv2 の Leave Group Message と類似のものです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからマルチキャストデータを受信せず、このアドレスからのマルチキャストデータとともに" done"（完了）した旨を伝えます。スイッチは本メッセージを受信すると、この Listening ポートには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しません。

4. Multicast Listener Report、Version 2
IGMPv3 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMP パケットヘッダ内に 143 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

Data Driven Learning

MLD Snooping グループのために Data Driven Learning を実行できます。Dynamic IP Multicast Learning として知られる Data Driven Learning が VLAN に対して有効な場合、またはスイッチがこの VLAN で IP マルチキャストトラフィックを受信する場合、MLD Snooping グループが作成されます。エントリの学習は MLD メンバシップ登録ではなく、トラフィックによりアクティブになります。通常の MLD Snooping エントリのために、MLD プロトコルはエントリのエージングアウトを認めます。Data Driven エントリのために、エントリは、エージングアウトしないように指定されるか、またはタイマによってエージングアウトするように指定されます。

Data Driven Learning を有効にすると、すべてのポートのマルチキャストフィルタリングモードは無視されます。これは、マルチキャストパケットがフォワーディングテーブルとしてフラッドされることを意味します。

注意 Data Driven グループが作成され、MLD メンバポートが後で学習されると、エントリは、通常の MLD Snooping エントリになります。つまり、エージングアウトメカニズムは、通常、MLD Snooping エントリの状態に追従します。

Data Driven Learning は IP マルチキャストデータを記録して、送信するレイヤ 2 スイッチにビデオカメラが接続しているネットワークにおいて有益です。スイッチは、パケットを破棄せずに、またはパケットをフラッドせずにデータセンタに IP データを送信する必要があります。ビデオカメラには MLD プロトコルを実行する機能がないため、IP マルチキャストデータは通常の MLD Snooping 機能で破棄されます。

MLD Snooping Settings（MLD Snooping 設定）

スイッチの MLD Snooping を有効にして、MLD Snooping の設定を行います。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings の順にメニューをクリックし、以下の画面を表示します。

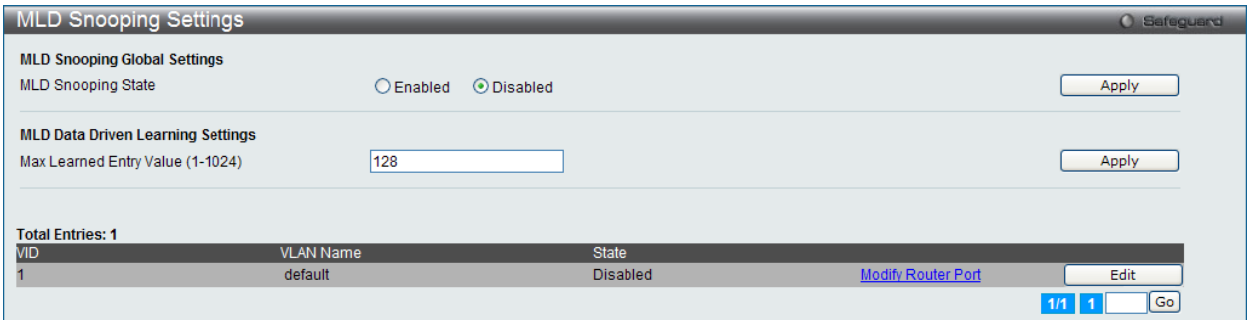


図 8-48　MLD Snooping Settings 画面

VLAN よって定義されているスイッチの現在の MLD Snooping 設定を表示します。

画面には以下の項目があります。

項目	説明
MLD Snooping State	MLD Snooping 状態を「Enabled」（有効）/「Disabled」（無効）にします。
Max Learned Entry Value (1-1024)	学習する最大エントリ数を指定します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

MLD Snooping のグローバル設定

画面上部の「MLD Snooping Global Settings」セクションでスイッチ全体に機能を有効にします。

1. 「MLD Snooping State」の「Enabled」ボタンをクリックします。
2. 「Apply」ボタンをクリックして、MLD Snooping 設定を適用します。

MLD Snooping 機能の詳細設定

関連する VLAN エントリの「Edit」ボタンをクリックして以下の画面を表示します。

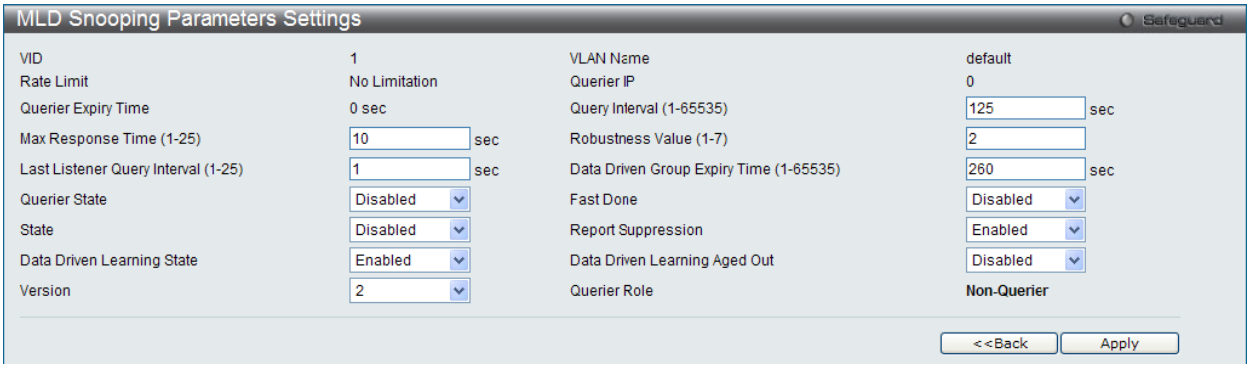


図 8-49　MLD Snooping Parameters Settings 画面

以下の項目を参照または編集することができます。

項目	説明
VID	VLAN 名と共に MLD Snooping 設定の編集を行う VLAN を識別するために使用する ID です。
VLAN Name	VLAN ID と共に MLD Snooping 設定の編集を行う VLAN を識別するために使用する名称です。
Rate Limit	スイッチが特定のポート /VLAN で処理できる MLD 制御パケットのレートを表示します。レートはパケット / 秒で指定されます。制限レートを超過したパケットは破棄されます。
Querier IP	ネットワークに MLD クエリを送信するデバイスの IP アドレスを表示します。
Querier Expiry Time	クエリアの有効時間を表示します。
Query Interval (1-65535)	一般的なクエリア送信間隔（秒）を指定します。初期値は 125（秒）です。
Max Response Time (1-25)	リスナーからのからのレポートを待つ最大時間を 1-25（秒）で設定します。初期値は 10（秒）です。

項目	説明
Robustness Value (1-7)	予想されるサブネット上のパケットの損失に応じてこの変数を調整します。Robustness Variable は以下の MLD メッセージ間隔の計算に使用されます。1-7 の範囲から指定します。初期値は 2 です。 • Group Listener Interval - マルチキャストルータがネットワーク上のグループにリスナーがいないと判断するまでの時間。 • Other Querier Present Interval- マルチキャストルータがクエリアである他のマルチキャストルータがないと判断するまでの時間。 • Last Listener Query Count- ルータがグループにローカルリスナーがいないと見なす前に送信された Group-Specific Query 数。初期値は Robustness Variable の値です。 サブネットが失われたと予想する場合には、この値を増やすことができます。
Last Listener Query Interval (1-25)	Group-Specific Query メッセージ（Leave Group メッセージに応じて送信されるものも含む）の最大送信間隔を指定します。この間隔はルータがグループのラストメンバの損失を検出するためにかかる時間をより減少するように低くします。
Data Driven Group Expiry Time (1-65535)	使用する Data Driven グループの生存時間を指定します。
Querier State	有効または無効にして、スイッチを（MLD クエリパケットを送信する）MLD Querier または（MLD クエリパケットを送信しない）Non-Querier として指定します。初期値は無効です。
Fast Done	MLD Snooping の Fast Done 機能を有効または無効にします。有効にすると、システムが MLD Leave メッセージを受信するとメンバはすぐにグループから削除されます。
State	指定した VLAN への MLD Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。 • Enabled - スイッチが MLD クエリパケットを送信する MLD クエリアとして選択されます。 • Disabled - スイッチは MLD クエリアとしての役目を果たしません。
Report Suppression	レポート抑制機能を有効または無効にします。
Data Driven Learning State	MLD Snooping グループの Data Driven Learning を有効または無効にします。
Data Driven Learning Aged Out	Data Driven エントリのエージングアウト機能を有効または無効にします。
Version	スイッチが送信する MLD general クエリのバージョンを指定します。
Querier Role	Query パケット送信についてのスイッチの動作を表示します。 • Querier - スイッチが MLD Query パケットの送信を行います。 • Non-Querier - スイッチが MLD Query パケットの送信を行いません。 本項目は「Querier State」と「State」で「Enabled」指定時には「Querier」と表示されます。

上記項目設定後、「Apply」ボタンをクリックして変更を有効にします。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。
「Modify Router Port」リンクをクリックすると、エントリの編集をすることができます。

MLD Snooping ルータポートの設定

MLD Snooping ルータポート設定を編集する場合は、対応する「Modify Router Port」リンクをクリックし、以下の画面を表示します。

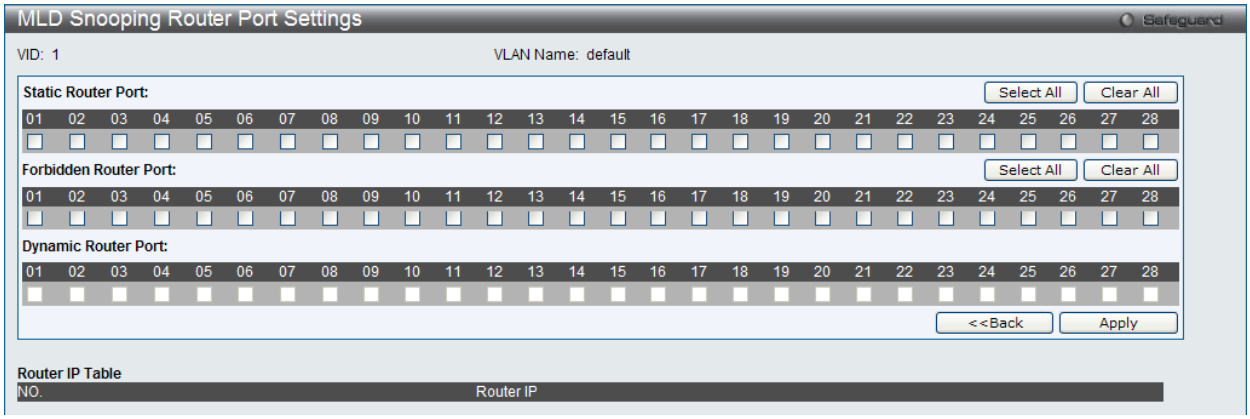


図 8-50　MLD Snooping Router Port Settings 画面

以下の項目を指定します。

項目	説明
Static Router Port	マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先としてルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストが有効なルータに到達するように設定します。
Forbidden Router Port	マルチキャストが有効なルータに接続しないポート範囲を指定します。これは、禁止ポートがルーティングパケットを送信しないように設定します。
Dynamic Router Port	ダイナミックに設定されたルータポートを表示します。
Ports	個別に適切なポートを選択して、ルータポート設定に含めます。 • 「Select All」ボタンをクリックするとすべてのポートを選択します。 • 「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

「Apply」ボタンをクリックして行った変更を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

MLD Snooping Rate Limit Settings（MLD Snooping レート制限設定）

スイッチが特定のポート /VLAN で処理できる MLD 制御パケットのレート制限を設定します。この設定は、ポートまたは VLAN 内の最大パケット数 / 秒を制限するのに使用されます。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Rate Limit Settings の順にクリックし、以下の画面を表示します。

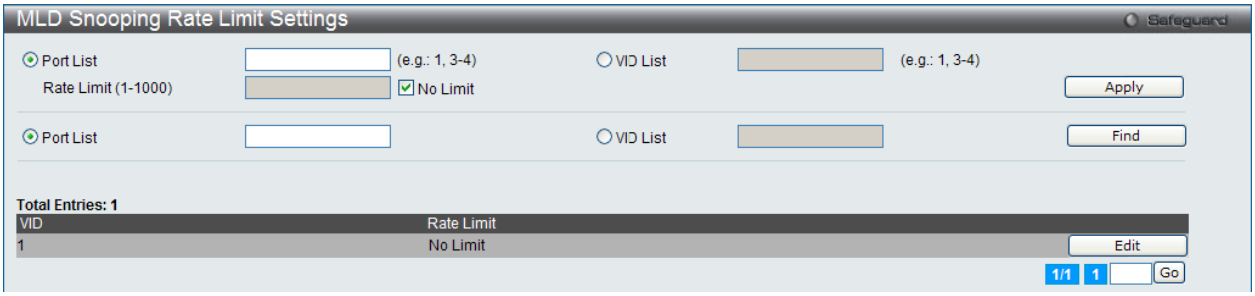


図 8-51　MLD Snooping Rate Limit Settings 画面

以下の項目があります。

項目	説明
Port List	本設定に使用するポートリストを指定します。
VID List	本設定に使用する VID リストを指定します。
Rate Limit	スイッチが特定のポート /VLAN で処理できる MLD 制御パケットのレート制限を設定します。レートはパケット / 秒で指定されます。制限を超過したパケットは破棄されます。「No Limit」オプションを選択すると、レート制限の要求は解除されます。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

MLD Snooping Static Group Settings（MLD Snooping スタティックグループ設定）

MLD Snooping マルチキャストグループのスタティックメンバポートを設定します。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Static Group Settings の順にクリックし、以下の画面を表示します。

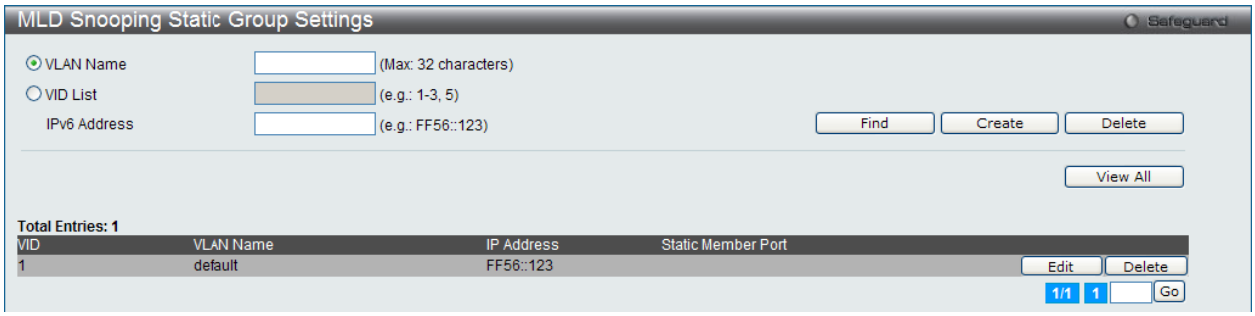


図 8-52　MLD Snooping Static Group Settings 画面

以下の項目を設定または表示します。

項目	説明
VLAN Name	スタティックグループのある VLAN 名。
VID List	スタティックグループのある VID リスト。
IPv6 Address	マルチキャストグループの IPv6 アドレスを指定します。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

エントリの登録

「VLAN Name」または「VID List」、および「IPv6 Address」入力後、「Create」ボタンをクリックします。

エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

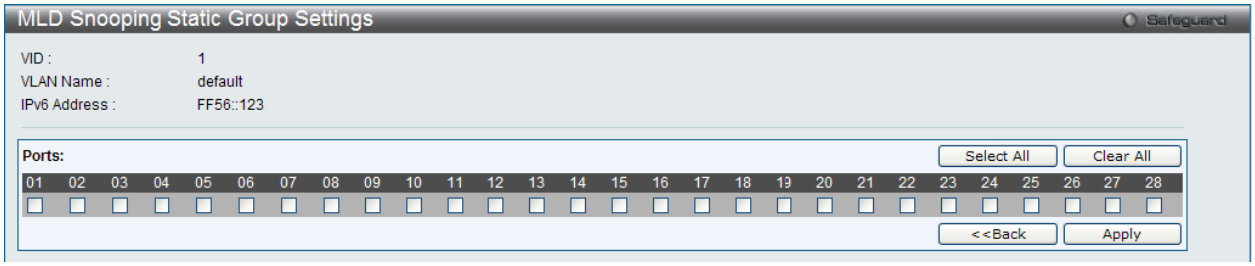


図 8-53　MLD Snooping Static Group Settings 画面

以下の項目を設定または表示します。

項目	説明
Ports	ボックスをチェックして、設定するポートを選択します。

「Apply」ボタンをクリックして行った変更を適用します。

「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

MLD Router Port（ルータポート参照）

スイッチの現在 IPv6 におけるルータポートとして設定されているポートを表示します。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Router Port メニューをクリックし、以下の画面を表示します。

図 8-54　MLD Router Port 画面

1. 画面上の VID(VLAN ID) を入力します。

2. 「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

注意 コンソールまたは Web ベースの管理インタフェースで設定されたルータポートはスタティックルータポートとして「S」で表示されます。スイッチにダイナミックに設定されたルータポートは「D」と表示され、Forbidden ポートは「F」と表示されます。

MLD Snooping Group（MLD Snooping グループ）

スイッチの MLD Snooping グループテーブルを参照します。MLD Snooping 機能では、スイッチを通過する MLD パケットからマルチキャストグループの IP アドレスと送信元の IP アドレスを読み取ることができます。MLD Snooping は、IPv4 の IGMP Snooping に相当する IPv6 の機能です。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Group の順にメニューをクリックし、以下の画面を表示します。

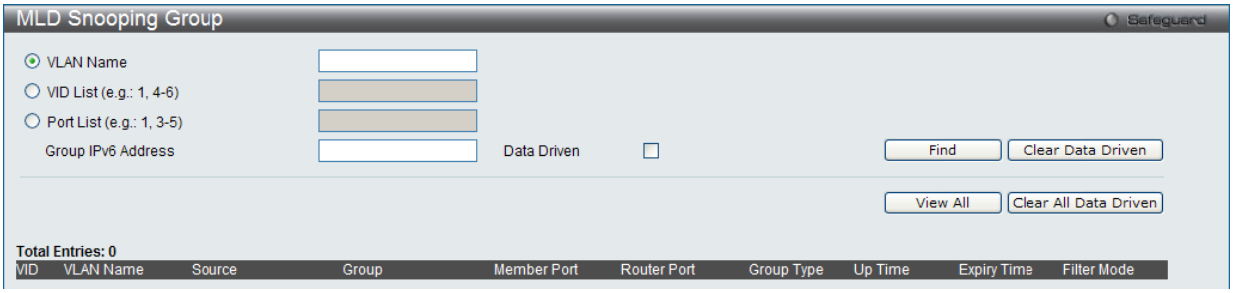


図 8-55　MLD Snooping Group 画面

MLD Snooping グループテーブルの参照

以下の項目を使用して、検索します。

項目	説明
VLAN Name	ラジオボタンをクリックして、マルチキャストグループの VLAN 名を入力します。
VID List	ラジオボタンをクリックして、マルチキャストグループの VLAN リストを入力します。
Port List	マルチキャストグループを検索するのに使用されるポート番号を指定します。
Group IPv6 Address	使用するグループ IPv6 アドレスを入力します。
Data Driven	Data Driven を有効または無効にします。有効にすると、Date Driven グループのみ表示されます。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。検索されたエントリは「MLD Snooping Group Table」に表示されます。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの削除

「Clear Data Driven」ボタンをクリックすると、指定 VLAN の Data Driven 機能が学習した MLD Snooping グループを削除します。

「Clear All Data Driven」ボタンをクリックすると、指定 VLAN の Data Driven 機能が学習した MLD Snooping グループをすべて削除します。

MLD Snooping Forwarding Table（MLD Snooping フォワーディングテーブル）

スイッチ上の現在の MLD Snooping フォワーディングテーブルのエントリを表示します。

マルチキャストグループを送出するポートリストと転送される特定の送信元をチェックする簡単な方法を提供します。送信元VLANのパケットをフォワーディング VLAN に転送します。さらに、MLD Snooping はフォワーディングポートを制限します。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Forwarding Table の順にメニューをクリックし、以下の画面を表示します。

図 8-56　MLD Snooping Forwarding Table 画面

以下の項目を使用して検索します。

項目	説明
VLAN Name	MLD Snooping フォワーディングテーブル情報を参照する VLAN 名。
VID List	MLD Snooping フォワーディングテーブル情報を参照するマルチキャストグループの VLAN ID リスト。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

MLD Snooping Counter（MLD Snooping カウンタ）

MLD Snooping の有効後に、スイッチが受信した MLD プロトコルパケットの統計情報カウンタを表示します。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Counter の順にメニューをクリックし、以下の画面を表示します。

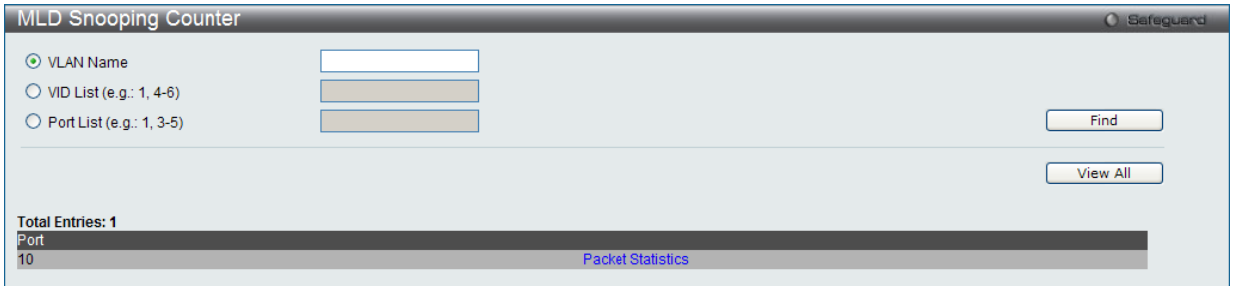


図 8-57　MLD Snooping Counter 画面

以下の項目が表示されます。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List	マルチキャストグループの VLAN ID リスト。
Port List	マルチキャストグループのポートリスト。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

MLD Snooping カウンタテーブルの参照

「Packet Statistics」リンクをクリックすると、以下の画面が表示されます。

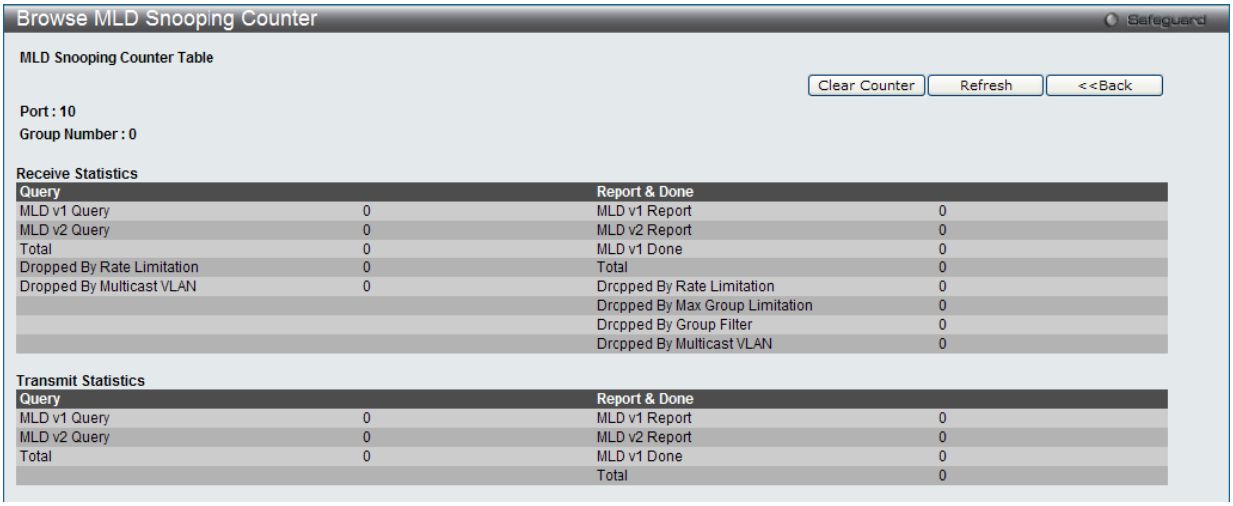


図 8-58　Browse MLD Snooping Counter 画面

「Clear Counter」ボタンをクリックして、本欄に表示したすべてのエントリをクリアします。
「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。
「<<Back」をボタンをクリックして前のページに戻ります。

Multicast VLAN（マルチキャスト VLAN）

スイッチング環境には、マルチプル VLAN が存在する可能性があります。マルチキャストクエリがスイッチを通過する度に、スイッチはシステム上の各 VLAN にそれぞれ異なるデータのコピーを送信する必要があります。これは順々にデータトラフィックを増加していき、トラフィックのパスを塞いでしまう可能性があります。トラフィックの負荷を軽減するために、マルチキャスト VLAN を組み込むことができます。これらのマルチキャスト VLAN は、複数のコピーの代わりにこのマルチキャストトラフィックを 1 つのコピーとしてマルチキャスト VLAN の受信者に送信します。

スイッチに組み込まれている他の一般的な VLAN に関係なく、マルチキャストトラフィックを送信したいマルチプル VLAN に対してどんなポートも追加することができます。マルチキャストトラフィックをスイッチに送信するソースポートを設定した後、そのマルチキャストトラフィックを送信するべきポートを設定します。ソースポートは受信ポートとなることはできないため、指定すると、スイッチはエラーメッセージを表示します。一度適切に設定されると、マルチキャストデータの流れはタイムリーで信頼できる方式で受信ポートに中継されます。

本スイッチのマルチキャスト VLAN 機能には、以下のような制限があります。

制限と条件 :

1. マルチキャスト VLAN はエッジおよびエッジでないスイッチで実行することができます。

2. メンバポートとソースポートはマルチプル ISM VLAN で使用できます。しかし、特定の ISM VLAN では、メンバポートとソースポートを同じポートにはできませんのでご注意ください。

3. マルチキャスト VLAN はノーマルな 802.1Q VLAN とは排他的です。これは、802.1Q VLAN と ISM VLAN の VLAN ID(VID) と VLAN 名は同じにはできないことを意味します。VID または VLAN 名がどんな VLAN でも一度選択されると、別の VLAN に使用することはできません。

4. 設定された VLAN の通常の表示は設定されたマルチキャスト VLAN を表示しません。

5. 一度、ISM VLAN が有効になると、この VLAN に対応する IGMP Snooping 状態も有効になります。有効になったマルチキャスト VLAN の IGMP 機能を無効にすることはできません。

6. 1 つの IP マルチキャストアドレスを複数の ISM VLAN に追加することはできませんが、1 つの ISM VLAN に複数の範囲を追加することはできます。

IGMP Multicast Group Profile Settings（IGMP マルチキャストグループプロファイル設定）

プロファイルを追加し、指定したスイッチポートに受信するマルチキャストアドレスレポートを設定します。本機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。
特定のスイッチポートに到着するレポートを受信する（Permit）またはレポートを拒否する（Deny）IP アドレス /IP アドレス範囲を設定することができます。

L2 Features > L2 Multicast Control > Multicast VLAN > IGMP Multicast Profile Settings の順にメニューをクリックし、以下の画面を表示します。

図 8-59　IGMP Multicast Group Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile Name	IP マルチキャストプロファイル名を入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの追加
「Profile Name」を入力して「Add」ボタンをクリックして新しいエントリを追加します。

エントリの削除
削除するエントリの「Delete」ボタンをクリックします。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

エントリの変更
1. 「Multicast Address List」欄の対応する「Group List」リンクをクリックし、以下の画面を表示します。

図 8-60　Multicast Group Profile Multicast Address Settings 画面

以下の項目が表示されます。

項目	説明
Multicast Address List	マルチキャストアドレスリストの値を入力します。

2. 「Multicast Address List」でアドレス範囲を入力し、「Add」ボタンをクリックします。

エントリの削除
該当するエントリの「Delete」ボタンをクリックします。

「<<Back」をボタンをクリックし、前のページに戻ります。

IGMP Snooping Multicast VLAN Settings（IGMP Snooping マルチキャスト VLAN 設定）

IGMP Snooping マルチキャスト VLAN の作成と設定を行います。

L2 Features > L2 Multicast Control >Multicast VLAN > IGMP Snooping Multicast Group VLAN Settings の順にメニューをクリックし、以下の画面を表示します。

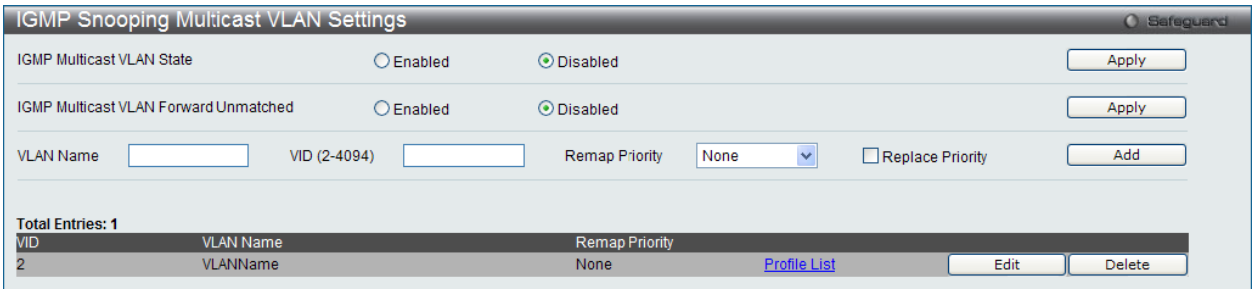


図 8-61　IGMP Snooping Multicast VLAN Settings 画面

以下の項目を使用して設定します。

項目	説明
IGMP Multicast VLAN State	IGMP マルチキャスト VLAN 状態を有効または無効にします。
IGMP Multicast VLAN Forward Unmatched	IGMP マルチキャスト VLAN フォワーディングの状態を有効または無効にします。
VLAN Name	使用する VLAN 名を入力します。
VID (2-4094)	使用する VID を指定します。
Remap Priority	• 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 • None - パケットの元の優先度が使用されます。（初期値）
Replace Priority	スイッチはパケットの優先度をリマップ優先度に基づいて変更します。リマップ優先度が設定される場合だけ、このフラグは有効になります。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

マルチキャスト VLAN の登録

1. 「IGMP Multicast VLAN State」を「Enabled」（有効）を選択し、「Apply」ボタンをクリックします。

2. 各項目を入力後、「Add」ボタンをクリックしてエントリを追加します。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

マルチキャスト VLAN の変更

1. 変更するエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

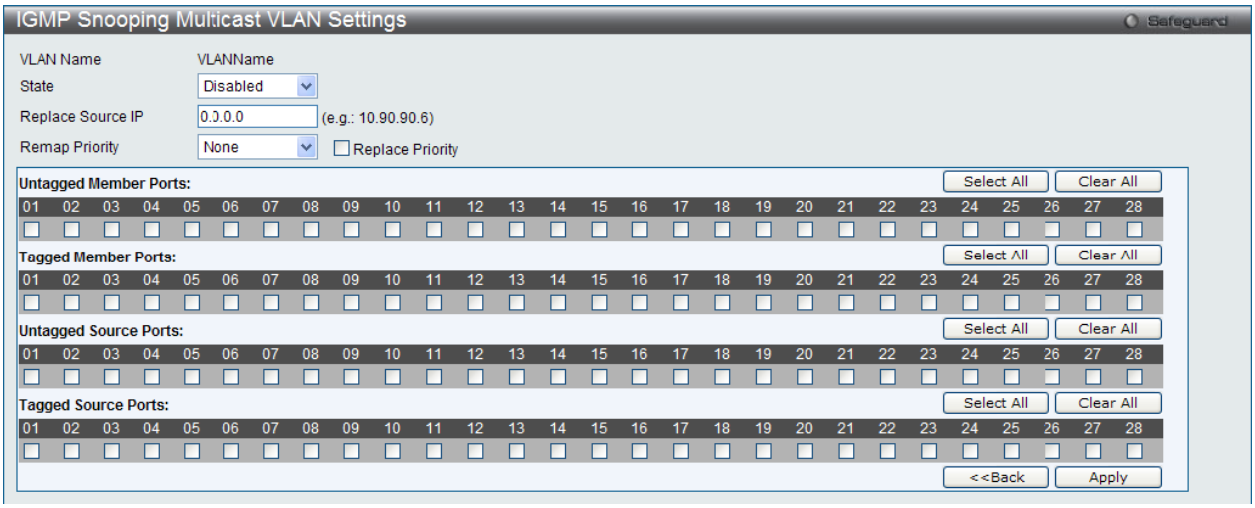


図 8-62　IGMP Snooping Multicast VLAN Settings 画面 - Edit

以下の項目を使用して設定します。

項目	説明
VLAN Name	定義済みのマルチキャスト VLAN 名を表示します。
State	選択した VLAN のマルチキャスト VLAN を「Enabled」（有効）または「Disabled」（無効）にします。
Replace Source IP	IGMP Snooping 機能を使用すると、ホストが送信した IGMP レポートパケットは送信元ポートに転送されます。パケットの転送の前に、Join パケット内の送信元 IP アドレスはこの IP アドレスに変更されます。「0.0.0.0」を指定すると、送信元 IP アドレスは変更されません。
Remap Priority	リマップの優先順位は、マルチキャスト VLAN に送信されるデータトラフィックに対応しています。 • 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 • None - パケットの元の優先度が使用されます。（初期値）
Replace Priority	スイッチがリマップ優先順位に基づいてパケットの元の優先順位を変更します。本オプションは、リマップ優先順位を設定している場合にのみ有効です。
Untagged Member Ports	マルチキャスト VLAN のタグなしメンバポートを指定します。
Tagged Member Ports	マルチキャスト VLAN のタグ付きメンバポートを指定します。
Untagged Source Ports	マルチキャストトラフィックがスイッチに入力しているタグなしソースポートまたはポート範囲を指定します。タグなしソースポートの PVID は、自動的にマルチキャスト VLAN に対して変更されます。ソースポートは 1 つのマルチキャスト VLAN に対してタグ付けまたはタグなしのいずれかとなり、つまり、両方のタイプは同じマルチキャスト VLAN のメンバとなることができません。
Tagged Source Ports	マルチキャスト VLAN のタグ付きメンバとしてソースポートまたはソースポート範囲を指定します。

「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。
「Apply」ボタンをクリックして行った変更を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

2. 画面上部に表示される定義済みの項目を変更し、「Apply」ボタンをクリックします。

マルチキャスト VLAN グループリストの設定

1. 既に作成したプロファイルにマルチキャスト VLAN を追加する場合は、追加するグループリストの「Profile List」のリンクをクリックし、以下の画面を表示します。

図 8-63　IGMP Snooping Multicast VLAN Group List Settings 画面

以下の項目を使用して設定します。

項目	説明
VID	VLAN ID が表示されます。
VLAN Name	VLAN 名が表示されます。
Profile Name	IGMP Snooping マルチキャスト VLAN グループプロファイル名を選択します。

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

2. プロファイル名を入力し、「Add」ボタンをクリックしてエントリを追加します。

マルチキャスト VLAN グループリストの削除

1. マルチキャスト VLAN グループリストを削除する場合は、該当する行の「Delete」ボタンをクリックします。

「IGMP Snooping VLAN Settings」画面に戻るためには、「Show IGMP Snooping Multicast VLAN Entries」リンクをクリックします。

Multicast Filtering（マルチキャストフィルタリング）

IPv4 Multicast Filtering（IPv4 マルチキャストフィルタリング）

IPv4 Multicast Profile Settings（IPv4 マルチキャストプロファイル設定）

指定したスイッチポートにマルチキャストアドレスレポートを受信するプロファイルを追加します。本機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。特定のスイッチポートに到着するレポートを受信する (Permit) またはレポートを拒否する (Deny)IPv4 アドレス /IPv4 アドレス範囲を設定することができます。

L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Multicast Profile Settings の順にメニューをクリックし、以下の画面を表示します。

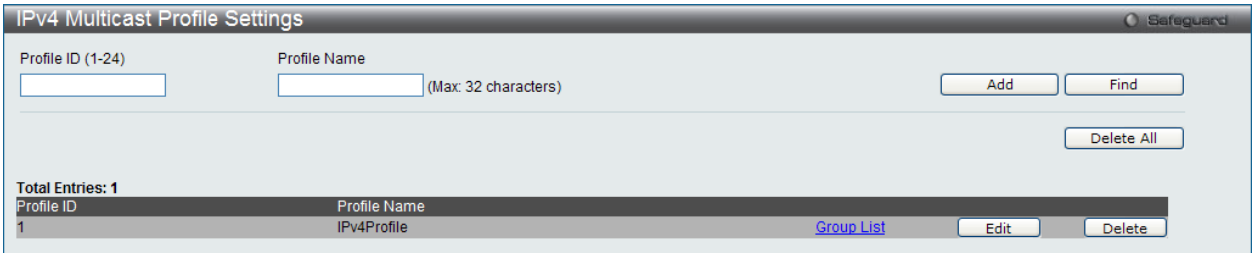


図 8-64　IPv4 Multicast Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile ID (1-24)	プロファイル ID を入力します。
Profile Name	IP マルチキャストプロファイル名を入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

エントリの登録
各項目を入力後、「Add」ボタンをクリックしてエントリを追加します。

エントリの編集
1. 「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリ名を編集し、「Apply」ボタンをクリックします。

エントリの削除
「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

マルチキャストグループリストの設定
「Group List」リンクをクリックして、以下の画面を表示します。

図 8-65　Multicast Address Group List Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile ID	プロファイル ID が表示されます。
Profile Name	プロファイル名が表示されます。
Multicast Address List	マルチキャストアドレスリストを入力します。

エントリの登録
各項目を入力後、「Add」ボタンをクリックしてエントリを追加します。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

エントリの編集

1. 「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

IPv4 Limited Multicast Range Settings（IPv4 マルチキャスト範囲の限定設定）

IPv4 マルチキャスト範囲の制限設定を適用するスイッチのポートまたはVLAN を設定します。送信元ポートごとに受信ポートに送信可能なマルチキャストアドレスの範囲を設定します。

L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Limited Multicast Range Settings の順にメニューをクリックし、以下の画面を表示します。

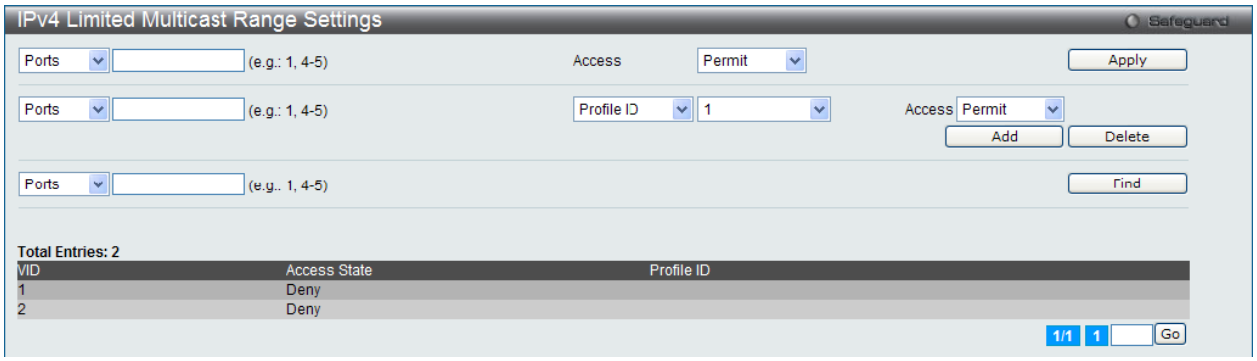


図 8-66　IPv4 Limited Multicast Range Settings 画面

制限する IP マルチキャストの範囲に含まれるスイッチポートを設定します。

以下の項目を指定してポートにマルチキャストアドレスフィルタリング機能を設定します。

項目	説明
Ports/VID List	マルチキャストアドレスフィルタ機能を追加または削除するポート範囲または VLAN ID を指定します。
Access	以下のオプションの一つを選択します。 • Permit - 指定したポートまたは VID に一致するパケットを許可することを指定します。 • Deny - 指定したポートまたは VID に一致するパケットを破棄することを指定します。

「Apply」ボタンをクリックし、設定を適用します。

画面中央にある項目を設定し、指定のプロファイルのポートにマルチキャストアドレスフィルタリング機能を設定します。

項目	説明
Ports	マルチキャストアドレスフィルタ機能を追加または削除するポート範囲を指定します。
Profile ID / Profile Name	プルダウンメニューを使用して、指定したポート範囲に (から) 追加または削除するプロファイル ID またはプロファイル名を選択します。
Access	プルダウンメニューを使用して、以下のオプションの一つを選択します • Permit - プロファイル内に指定されているアドレスに一致するパケットを許可します。 • Deny - プロファイル内に指定されているアドレスに一致するパケットを破棄します。

新しいマルチキャストアドレス範囲の追加

適切な情報を入力し、「Add」ボタンをクリックします。

マルチキャストアドレス範囲の削除

情報を入力し、「Delete」ボタンをクリックします。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IPv4 Max Multicast Group Settings（IPv4 マルチキャストグループの最大数の設定）

学習されるマルチキャストグループの最大数をスイッチのポートに設定します。

L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Max Multicast Group Settings の順にメニューをクリックし、以下の画面を表示します。

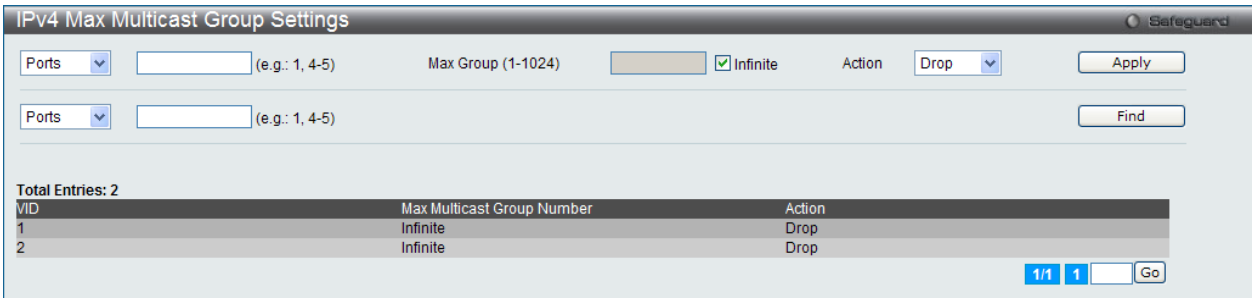


図 8-67　IPv4 Max Multicast Group Settings 画面

以下の項目を使用して、設定します。

項目	説明
Ports / VID List	本設定に使用される適切なポートまたは VLAN ID を選択します。
Max Group (1-1024)	マルチキャストグループの最大数を指定します。範囲は 1-1024 です。「Infinite」ボックスをチェックしない場合、ここに最大グループ数を入力します。
Infinite	「Infinite」（制限なし）を有効または無効にします。
Action	ルールに適切な操作を選択します。 • Drop - 破棄の動作を行います。 • Replace - 交換の動作を行います。

エントリの追加

適切な情報を入力し「Apply」ボタンをクリックします。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IPv6 Multicast Filtering（IPv6 マルチキャストフィルタリング）

指定したスイッチポートにマルチキャストアドレスレポートを受信するプロファイルを追加します。本機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。特定のスイッチポートに到着するレポートを受信する (Permit) またはレポートを拒否する (Deny)IPv6 アドレス /IPv6 アドレス範囲を設定することができます。

IPv6 Multicast Profile Settings（IPv6 マルチキャストプロファイル設定）

IPv6 マルチキャストプロファイルの追加、削除、または設定を行います。

L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Multicast Filtering Profile Settings の順にメニューをクリックし、以下の画面を表示します。

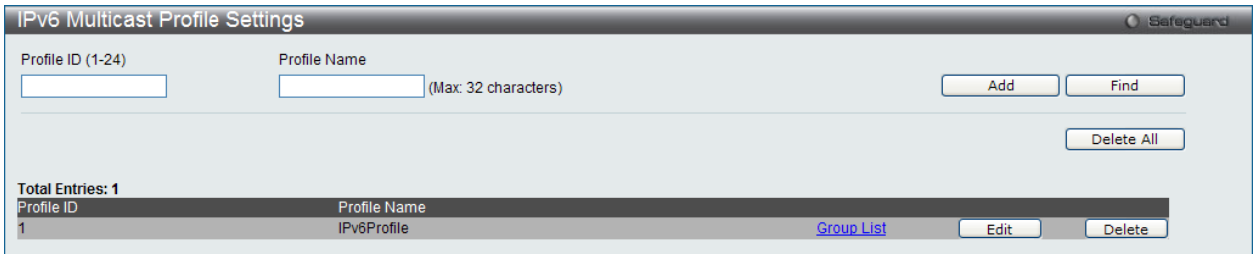


図 8-68　IPv6 Multicast Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile ID (1-24)	プロファイル ID を入力します。
Profile Name	IP マルチキャストプロファイル名を入力します。

エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

エントリの編集

1. 「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

マルチキャストグループリストの設定

「Group List」リンクをクリックすると、以下の画面が表示されます。

図 8-69　Multicast Address Group List Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile ID	プロファイル ID が表示されます。
Profile Name	プロファイル名が表示されます。
Multicast Address List	マルチキャストアドレスリストを入力します。

エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

エントリの編集

1. 「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

IPv6 Limited Multicast Range Settings（IPv6 マルチキャスト範囲の限定設定）

IPv6 マルチキャスト範囲の制限設定を適用するスイッチのポートまたはVLAN を設定します。送信元ポートごとに受信ポートに送信可能なマルチキャストアドレスの範囲を設定します。

L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Limited Multicast Range Settings の順にメニューをクリックし、以下の画面を表示します。

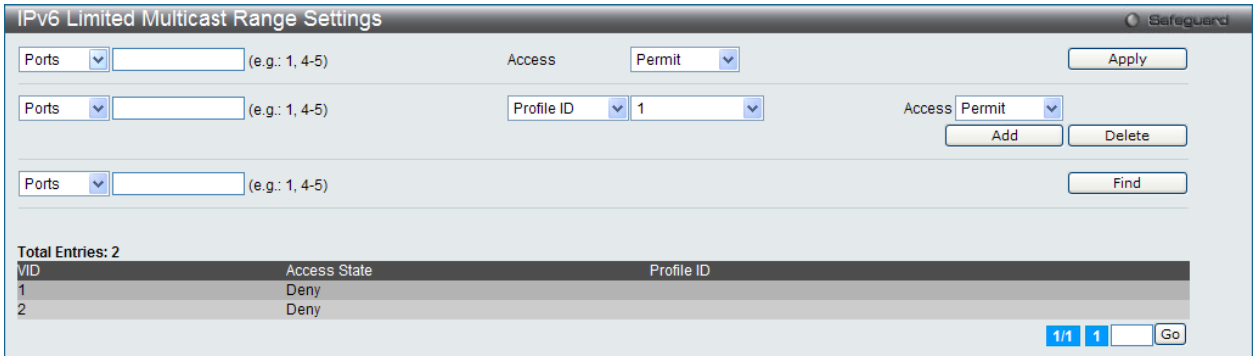


図 8-70　IPv6 Limited Multicast Range Settings 画面

制限する IP マルチキャストの範囲に含まれるスイッチポートを設定します。

以下の項目を指定してポートにマルチキャストアドレスフィルタリング機能を設定します。

項目	説明
Ports/VID List	マルチキャストアドレスフィルタ機能を追加または削除するポート範囲または VID を指定します。
Access	プルダウンメニューを使用して、以下のオプションの一つを選択します。 • Permit - 指定したポートまたは VID に一致するパケットを許可することを指定します。 • Deny - 指定したポートまたは VID に一致するパケットを破棄することを指定します。

「Apply」ボタンをクリックし、設定を適用します。

画面中央にある項目を設定し、指定のプロファイルのポートにマルチキャストアドレスフィルタリング機能を設定します。

項目	説明
Ports / VID List	マルチキャストアドレスフィルタ機能を追加または削除するポート範囲または VID を指定します。
Profile ID	プルダウンメニューを使用して、指定したポート範囲に（から）追加または削除するプロファイル ID を選択します。
Access	プルダウンメニューを使用して、以下のオプションの一つを選択します • Permit - プロファイル内に指定されているアドレスに一致するパケットを許可します。 • Deny - プロファイル内に指定されているアドレスに一致するパケットを破棄します。

新しいマルチキャストアドレス範囲の追加
適切な情報を入力し、「Add」ボタンをクリックします。

マルチキャストアドレス範囲の削除
情報を入力し、「Delete」ボタンをクリックします。

エントリの検索
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IPv6 Max Multicast Group Settings（IPv6 マルチキャストグループの最大数の設定）

ここでは、学習されるマルチキャストグループの最大数をスイッチのポートに設定します。

L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Max Multicast Group Settings の順にメニューをクリックし、以下の画面を表示します。

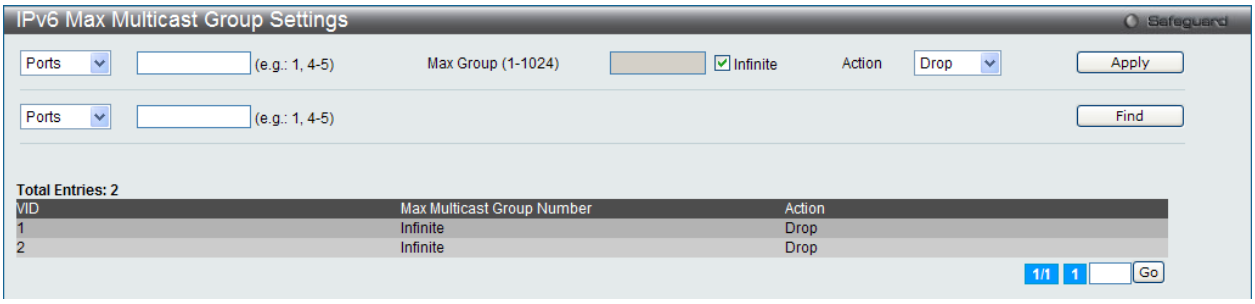


図 8-71　IPv6 Max Multicast Group Settings 画面

以下の項目を使用して設定します。

項目	説明
Ports / VID List	本設定に使用される適切なポート範囲または VID を選択します。
Max Group (1-1024)	マルチキャストグループの最大数を指定します。範囲は 1-1024 です。「Infinite」ボックスをチェックしない場合、ここに最大グループ数を入力します。
Infinite	「Infinite」（制限なし）を有効または無効にします。
Action	ルールに適切な操作を選択します。「Drop」を選択すると破棄の動作を行い、「Replace」を選択すると交換の動作を行います。

エントリの登録

適切な情報を入力し「Apply」ボタンをクリックします。

エントリの検索

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Multicast Filtering Mode（マルチキャストフィルタリングモード）

マルチキャストフィルタリングモードを設定します。

L2 Features > Multicast Filtering > Multicast Filtering Mode の順にメニューをクリックし、以下の画面を表示します。

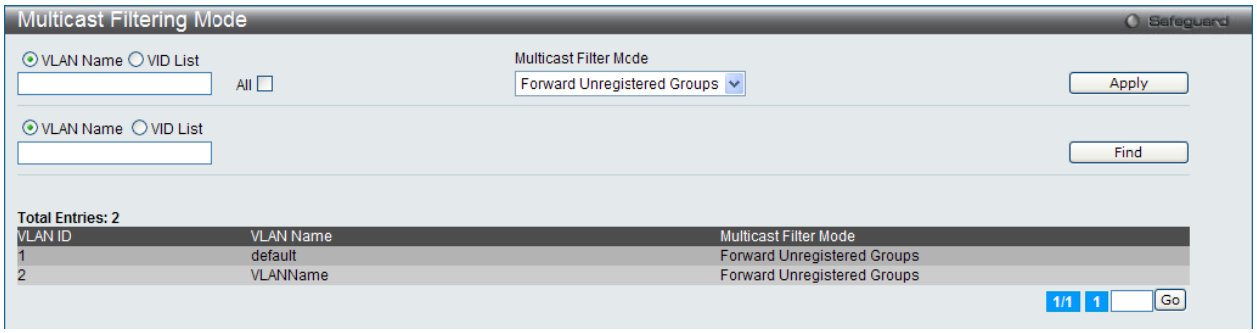


図 8-72　Multicast Filtering Mode 画面

以下の項目を使用して設定します。

項目	説明
VLAN Name/VID List	フィルタリングが適用される VLAN を指定します。「All」をチェックするとすべての VLAN にフィルタリングが適用されます。
Multicast Filter Mode	指定した VLAN ポートに転送されるマルチキャストパケットを受信した時の動作を指定します。 • Forward All Groups - 指定ポート VLAN にすべてのマルチキャストパケットを転送します。 • Forward Unregistered Groups - 宛先が未登録のマルチキャストグループであるマルチキャストパケットは、上記指定ポート範囲に転送されます。 • Filter Unregistered Groups - 宛先が登録済みのマルチキャストグループであるマルチキャストパケットは、上記指定ポート範囲に転送されます。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの検索

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ERPS Settings（イーサネットリングプロテクション設定）

ERPS（Ethernet Ring Protection Switching）はイーサネットリング保護スイッチングの業界標準（ITU-T G.8032）です。これは、イーサネットリングネットワークに対して十分に考慮されたイーサネット操作、管理、およびメンテナンス機能と簡単な APS（automatic protection switching）プロトコルを統合することによって実行されます。ERPS はリングトポロジ内のイーサネットトラフィックに sub-50ms 保護を提供します。これはイーサネットレイヤにループが全く形成されないこと保証します。

リング内の 1 つのリンクが、ループ（RPL : Ring Protection Link）を回避するためにブロックされます。障害が発生すると、保護スイッチングは障害のあるリンクをブロックして RPL のブロックを解除します。障害が解決すると、保護スイッチングは再度 RPL をブロックして、障害が解決したリンクのブロックを解除します。

G.8032 の用語と概念

用語	説明
RPL (Ring Protection Link)	ブリッジされたリングでループを防ぐためにアイドル状態でブロックされるメカニズムによって指定されるリンク。
RPL Owner	アイドル状態で RPL 上のトラフィックをブロックし、保護状態でブロックを解除する RPL に接続するノード。
R-APS (Ring - Automatic Protection Switching)	RAPS VLAN（R-APS チャンネル）経由でリング上の保護操作を調整するために使用する Y.1731 および G.8032 に定義されているプロトコルメッセージ。
RAPS VLAN (R-APS Channel)	R-APS メッセージ送信用の個別のリング範囲における VLAN。
Protected VLAN	通常のネットワークトラフィックの送信用サービストラフィック VLAN。

スイッチの ERPS 機能を有効にします。

注意 ERPS を有効にする前に、STP と LBD をリングポートで無効にする必要があります。R-APS VLAN の作成前およびリングポート、RPL ポート、RPL オーナの設定前に ERPS を有効にすることはできません。ERPS が有効になると、これらの項目を変更することはできません。

L2 Features > ERPS Settings の順にメニューをクリックし、以下の画面を表示します。

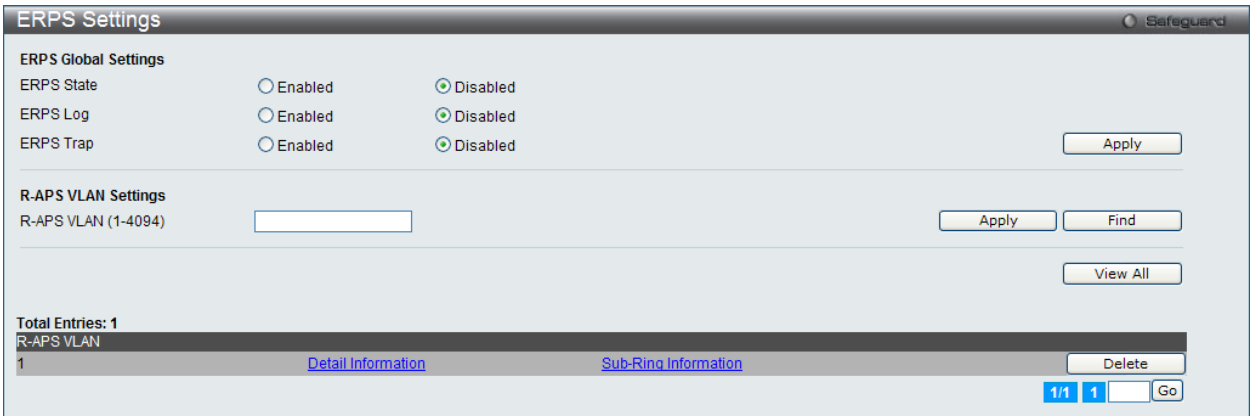


図 8-73　ERPS Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
ERPS Global Settings	
ERPS State	ERPS 状態を有効または無効にします。
ERPS Log	ERPS ログを有効または無効にします。
ERPS Trap	ERPS トラップを有効または無効にします。
R-APS VLAN Settings	
R-APS VLAN (1-4094)	R-APS VLAN とする VLAN を指定します。

エントリの追加

新しい R-APS VLAN を作成するためには、メニューで必要な項目の設定を行い、「Apply」ボタンをクリックします。

詳細情報の参照

「Detail Information」リンクをクリックすると、以下の画面が表示されます。

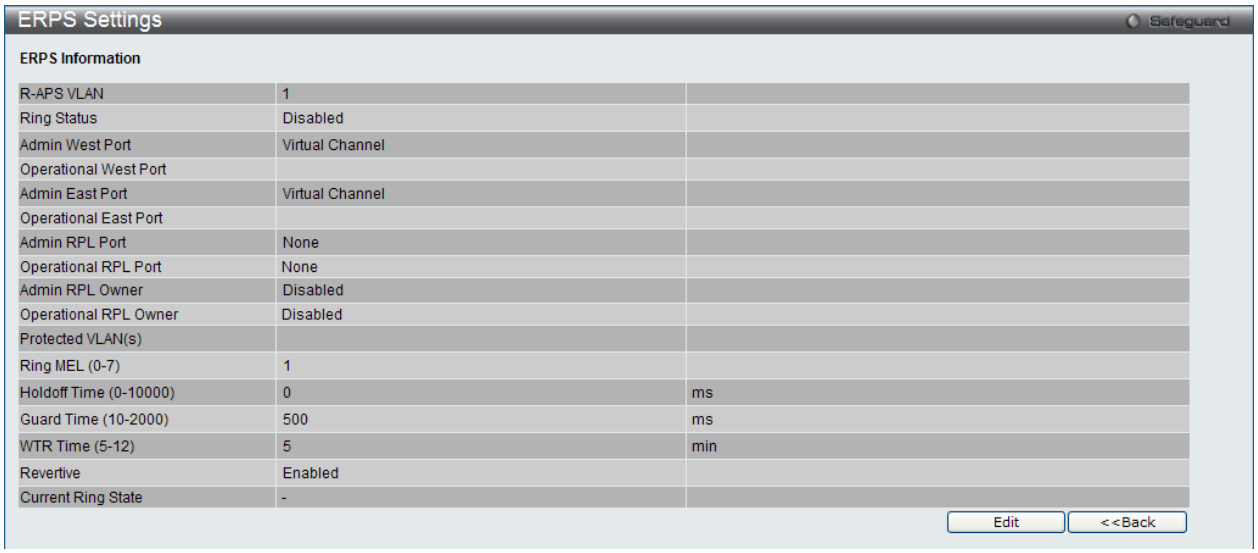


図 8-74　ERPS Settings 画面 - ERPS Information

エントリの編集

1. 「Edit」ボタンをクリックすると、画面上部に現在の設定が表示されます。

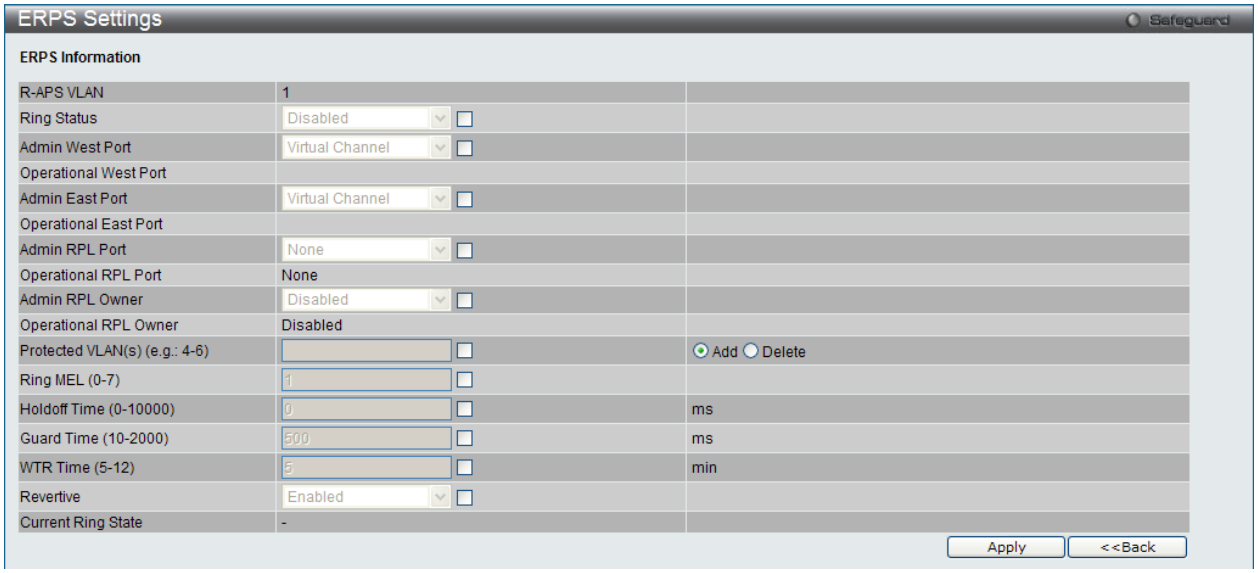


図 8-75　ERPS Settings 画面 - Edit

設定対象となる項目は以下の通りです。

項目	説明
R-APS VLAN	R-APS VLAN ID を表示します。
Ring Status	チェックし、プルダウンメニューを使用して、指定リングを「Enabled」(有効)/「Disabled」(無効) にします。
Admin West Port	チェックし、West リングポートとしてポートを指定します。また、使用する仮想ポートチャンネルも指定します。
Operational West Port	操作可能な West ポート値が表示されます。
Admin East Port	チェックし、East リングポートとしてポートを指定します。また、使用する仮想ポートチャンネルも指定します。
Operational East Port	操作可能な East ポート値が表示されます。
Admin RPL Port	チェックし、使用する RPL ポートを指定します。オプションを West Port、East Port、および None から選択します。
Operational RPL Port	操作可能な RPL ポートを表示します。
Admin RPL Owner	チェックを行い、プルダウンメニューを使用して、RPL オーナノードを「Enabled」(有効)/「Disabled」(無効) にします。
Operational RPL Owner	操作可能な RPL オーナを表示します。
Protected VLAN(s)	チェックを行い、「Add」または「Delete」を指定して、防御する VLAN グループを入力します。
Ring MEL (0-7)	チェックを行い、R-APS 機能のリングの MEL を入力します。リングの MEL の初期値は 1 です。
Holdoff Time (0-10000)	チェックを行い、R-APS 機能のホールドオフタイムを入力します。初期値は 0(ミリ秒) です。
Guard Time (10-2000)	チェックを行い、R-APS 機能のガードタイムを入力します。初期値は 500(ミリ秒) です。
WTR Time (5-12)	チェックを行い、R-APS 機能の WTR タイムを入力します。
Revertive	チェックを行い、プルダウンメニューを使用して、R-APS 復帰オプションを「Enabled」(有効)/「Disabled」(無効) にします。
Current Ring State	現在のリング状態を表示します。

2. 項目設定後、「Apply」ボタンをクリックして、ERPS、ERPS ログ、および ERPS トラップ設定への有効 / 無効状態の変更を適用します。

「<<Back」をボタンをクリックして前のページに戻ります。

サブリング情報の参照

1. 「Sub-Ring Information」リンクをクリックすると、以下の画面が表示されます。

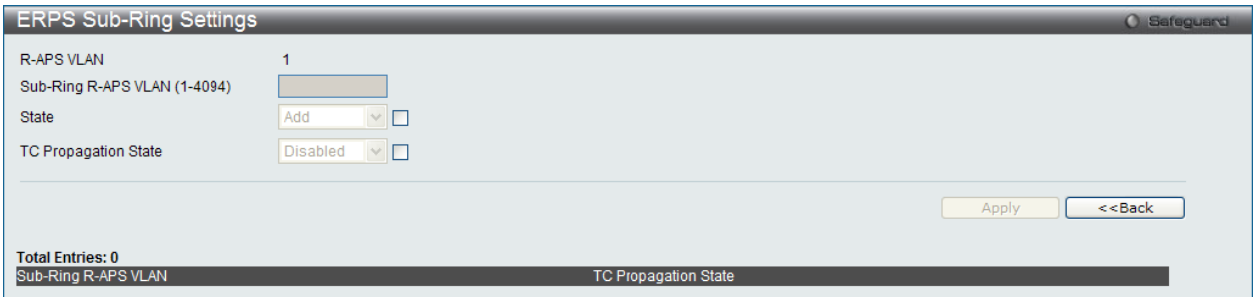


図 8-76　ERPS Sub-Ring Settings 画面

2. 以下の項目を使用して設定します。

項目	説明
Sub-Ring R-APS VLAN (1-4094)	使用するサブリングの R-APS VLAN ID を入力します。
State	ERPS Sub-Ring の状態を指定します。「Add」（追加）または「Delete」（削除）を選択します。
TC Propagation State	TC Propagation の状態を指定します。「Enabled」（有効）または「Disabled」（無効）を選択します。

3. 「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」をボタンをクリックして前のページに戻ります。

エントリの削除

テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。
「Clear All」ボタンをクリックすると、本画面のすべての設定がクリアされます。

LLDP（LLDP 設定）

LLDP（Link Layer Discovery Protocol）は、IEEE 802 ネットワークに接続しているステーションから同じ IEEE 802 ネットワークに接続している他のステーションに通知を出します。本システムが提供する主な機能は、ステーションまたは本機能の管理を提供するエンティティの管理アドレスと、管理エンティティが要求する IEEE 802 ネットワークに接続するステーションの接続点の識別子を組み合わせることです。

本プロトコルによって送信される情報は、受信先によって標準の管理情報ベース（MIB）に格納されるため、SNMP（Simple Network Management Protocol）などの管理プロトコルを使用したネットワーク管理システム（NMS）からその情報にアクセスできるようになります。

LLDP（LLDP 設定）

LLDP Global Settings（LLDP グローバル設定）

LLDP グローバルパラメータを設定します。

L2 Features > LLDP > LLDP > LLDP Global Settings の順にメニューをクリックし、以下の画面を表示します。

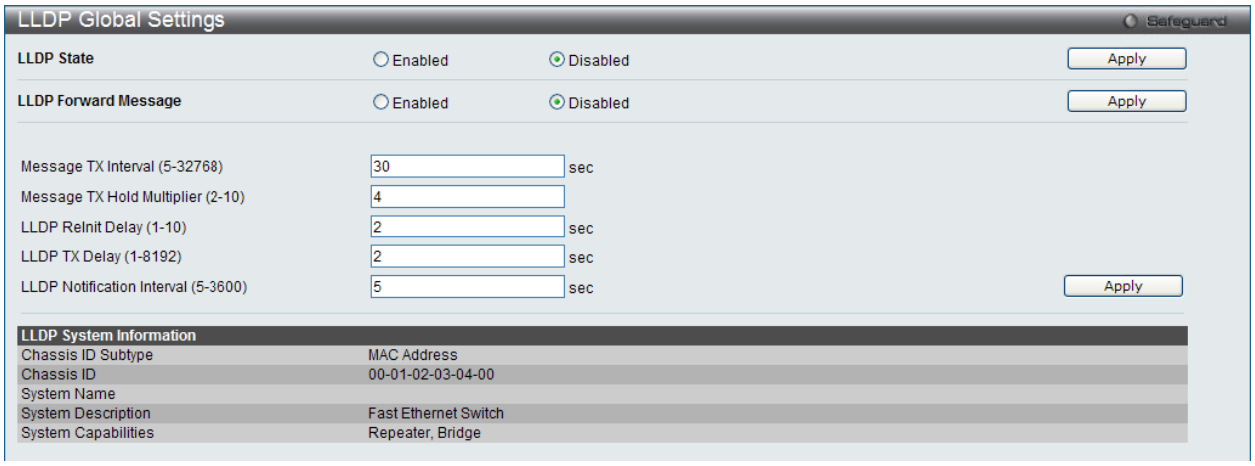


図 8-77　LLDP Global Settings 画面

以下の項目を設定できます。

項目	説明
LLDP State	スイッチにおける LLDP 機能を「Enabled」（有効）または「Disabled」（無効）にします。
LLDP Forward Message	同じ IEEE 802 ネットワークに割り当てられた他のステーションに通知するために LLDP 機能のメッセージ転送を「Enabled」（有効）または「Disabled」（無効）にします。 • Enabled - 同一のポート VLAN を持つすべてのポートに LLDP パケットをフラッドして、同じ IEEE 802 LAN に接続している他のコンピュータに通知します。 • Disabled - 本機能が各ポートにおいて LLDP パケットのメッセージ転送を制御します。
Message TX Interval (5-32768)	アクティブなポートが通知を再送する方法を制御します。パケット伝送間隔を変更するために、5-32768（秒）の範囲で値を入力します。
Message TX Hold Multiplier (2-10)	LLDP スイッチに使用される乗数を変更することで LLDP Neighbor に LLDP 通知を作成して送信する有効期間（TTL：Time-to-Live）を計算します。指定通知の TTL（time-to-Live）の期限が来ると、通知データは Neighbor スイッチの MIB から削除されます。
LLDP Reinit Delay (1-10)	LLDP ポートが LLDP 無効にするコマンドを受け取った後、再初期化を行う前に待機する時間です。1-10（秒）から値を入力します。
LLDP TX Delay (1-8192)	LLDP MIB コンテンツの変更のために、LLDP ポートが連続した LLDP 通知の送信を遅らせる最短時間（遅延間隔）を変更します。LLDP TX Delay を変更するために、1-8192（秒）から値を入力します。
LLDP Notification Interval (5-3600)	LLDP データ変更が LLDP Neighbor からポートに受信した通知の中に検出される場合、定義済みの SNMP トラップレシーバに変更通知を送信する時に使用されます。5-3600（秒）から値を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

LLDP Port Settings（LLDP ポート設定）

LLDP ポートパラメータを設定します。

L2 Features > LLDP > LLDP > LLDP Port Settings の順にメニューをクリックし、以下の画面を表示します。

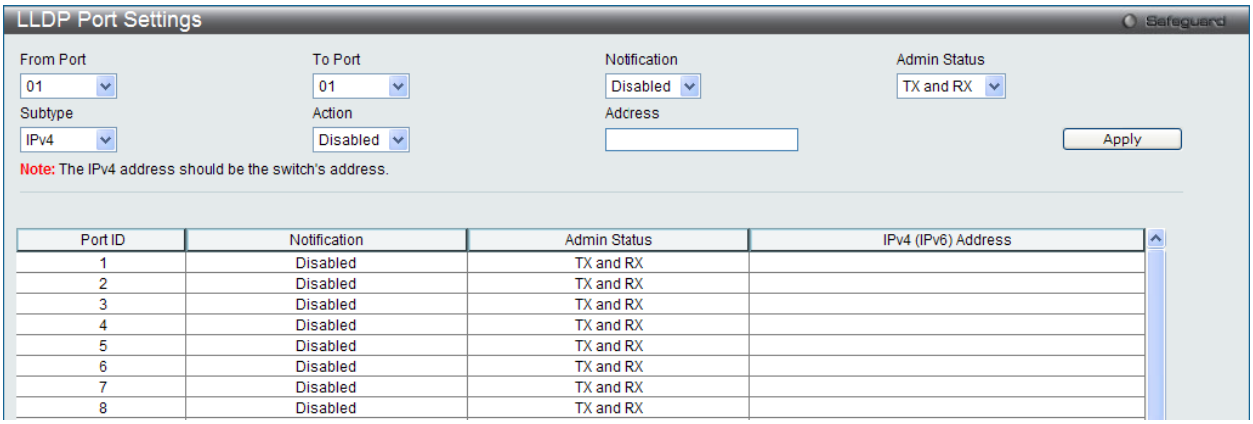


図 8-78　LLDP Port Settings 画面

以下の項目を設定できます。

項目	説明
From Port/To Port	プルダウンメニューを使用して、この設定に使用するポート範囲を指定します。
Notification	プルダウンメニューを使用して、LLDP 通知を「Enabled」（有効）または「Disabled」（無効）にします。本機能は SNMP トラップを制御し、無効にするとトラップを実行しません。
Admin Status	本機能はローカル LLDP エージェントを制御し、ポートで LLDP フレームの送受信を行うことができるようになります。通知のステータスを選択します。 • TX - ローカル LLDP エージェントは LLDP フレームを送信します。 • RX - ローカル LLDP エージェントは LLDP フレームを受信します。 • TX and RX - ローカル LLDP エージェントは LLDP フレームの送受信両方を行います。（初期値） • Disabled - ローカル LLDP エージェントは、LLDP フレームの送受信を行いません。
Subtype	送信される IP アドレス情報（IPv4 / IPv6）のタイプを選択します。
Action	ポートベースの管理アドレス機能を「Enabled」（有効）または「Disabled」（無効）にします。
Address	通知するエンティティの管理アドレスを入力します。

「Apply」ボタンをクリックし、変更を有効にします。

注意　ここに入力する IPv4 または IPv6 アドレスを既存の LLDP 管理 IP アドレスとする必要があります。

LLDP Management Address List（LLDP 管理アドレスリスト）

LLDP 管理アドレスを参照します。

L2 Features> LLDP > LLDP > LLDP Management Address List の順にメニューをクリックし、以下の画面を表示します。

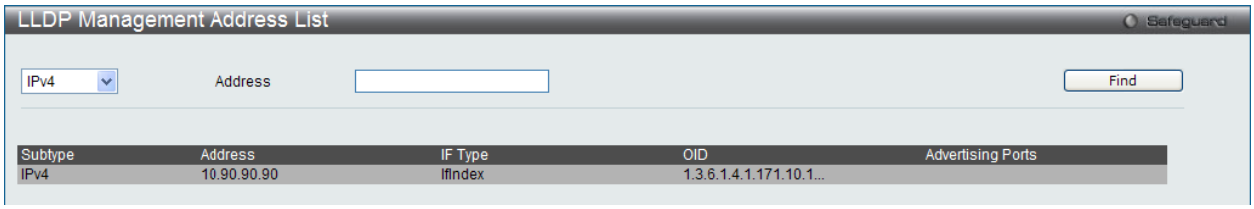


図 8-79　LLDP Management Address List 画面

以下の項目を設定できます。

項目	説明
IPv4/IPv6	「IPv4」または「IPv6」を選択します。
Address	通知するエンティティの管理 IP アドレスを入力します。IPv4 アドレスは管理 IP アドレスであるため、IP 情報がフレームと共に送信されます。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）

TLV（Type-length-value）は、LLDP パケット内の TLV エレメントとして特定の送信情報を許可します。本スイッチにおけるベーシック TLV 設定を有効にします。

スイッチのアクティブな LLDP ポートは、通常その外向き通知にいつも必須データを含んでいます。外向き LLDP 通知からこれらのデータタイプの 1 個以上を除外するために、個別のポートまたはポートグループに設定できる 4 つのオプションデータがあり、必須データタイプには、4 つの基本的な情報タイプ（end f LLDPDU TLV、chassis ID TLV、port ID TLV および Time to Live TLV）があります。必須データタイプは無効にすることができません。さらに、オプションで選択可能な 4 つのデータタイプ（Port Description、System Name、System Description および System Capability）があります。

本スイッチにおけるベーシック TLV 設定を有効にします。

L2 Features> LLDP > LLDP > LLDP Basic TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

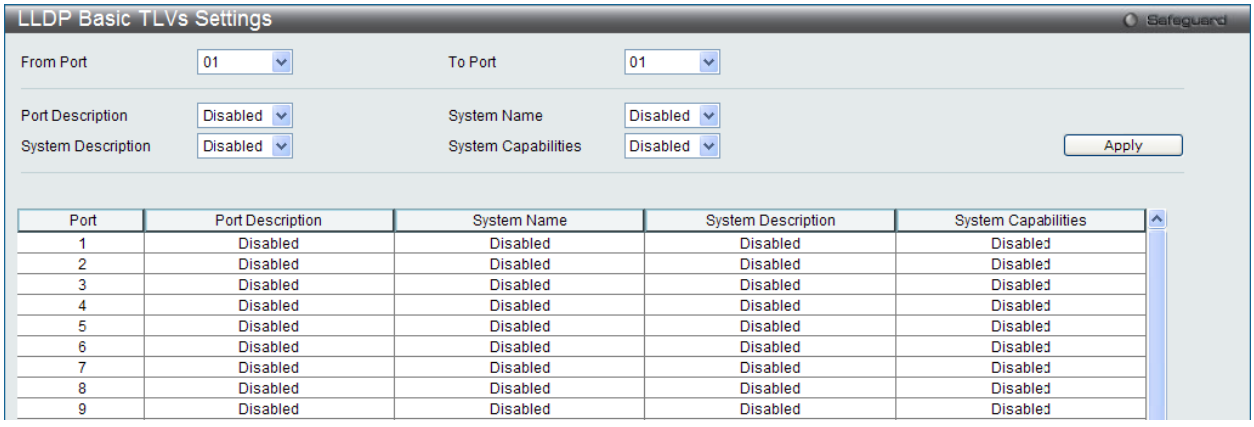


図 8-80　LLDP Basic TLVs Settings 画面

プルダウンメニューを使用してベーシック TLV 設定を「Enabled」（有効）/「Disabled」（無効）にします。

以下の項目を設定できます。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
Port Description	ポート説明を「Enabled」（有効）/「Disabled」（無効）にします。
System Name	システム名を「Enabled」（有効）/「Disabled」（無効）にします。
System Description	システム説明を「Enabled」（有効）/「Disabled」（無効）にします。
System Capabilities	システムケーパビリティを「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

LLDP Dot1 TLV は、IEEE 802.1 によって組織的に定義されている TLV で、送信する LLDP 通知から IEEE 802.1 規定のポート VLAN ID の TLV データタイプを除外するようにポートやポートグループを設定する時に使用します。

L2 Features> LLDP > LLDP > LLDP Dot1 TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

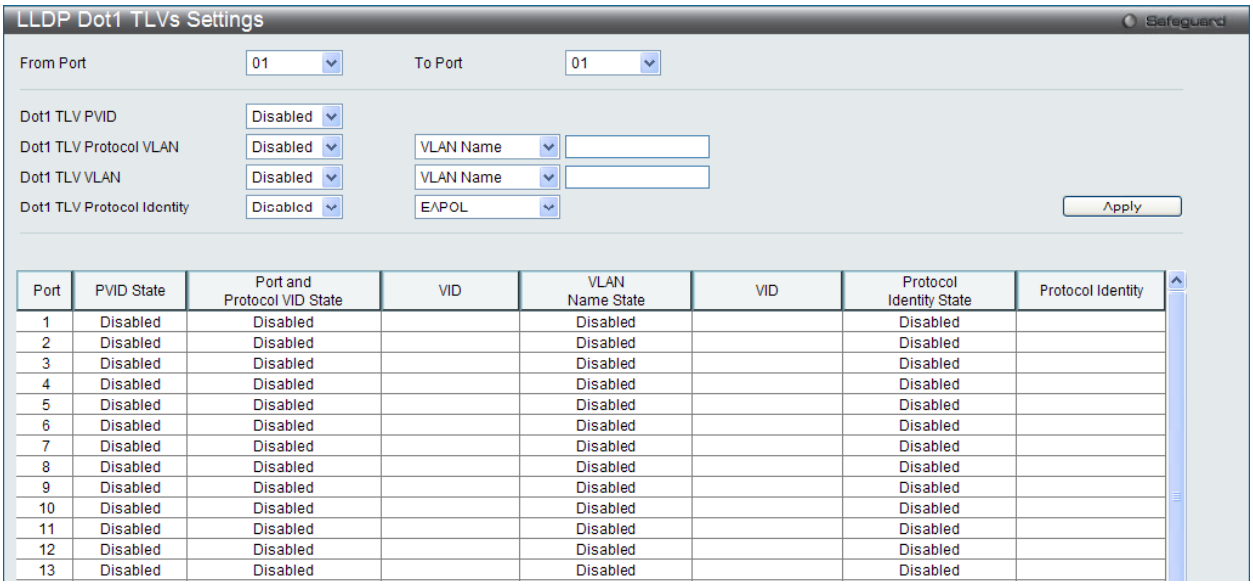


図 8-81　LLDP Dot1 TLVs Settings 画面

以下の項目が使用できます。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
Dot1 TLV PVID	Dot1 TLV PVID の通知を「Enabled」（有効）/「Disabled」（無効）にします。
Dot1 TLV Protocol VLAN	プロトコル VLAN ID の通知を「Enabled」（有効）/「Disabled」（無効）にします。本オプションの有効後、次のプルダウンメニューで「VLAN Name」、「VID List」または「All」を選択することができます。これを選択後に、対象となるプロトコル VLAN を右の欄で指定します。 • VLAN Name - VLAN 名を指定します。 • VLAN ID - VLAN ID を指定します。 • All - すべてを対象とします。
Dot1 TLV VLAN	Dot1 TLV VLAN の有効 / 無効、および設定を行います。本オプションの有効後、次のプルダウンメニューで「VLAN Name」、「VID List」または「All」を選択することができます。これを選択後に、対象となるプロトコル VLAN を右の欄で指定します。 • VLAN Name - VLAN 名を指定します。 • VLAN ID - VLAN ID を指定します。 • All - すべてを対象とします。
Dot1 TLV Protocol Identity	プロトコル識別子の通知を「Enabled」（有効）/「Disabled」（無効）にします。次に対象とするプロトコルを「EAPOL」、「LACP」、「GVRP」、「STP」または「All」から選択します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

個別のポートやポートグループが送信する LLDP 通知から IEEE 802.3 規定のポート VLAN ID TLV データタイプを除外するように設定します。

L2 Features> LLDP > LLDP > LLDP Dot3 TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

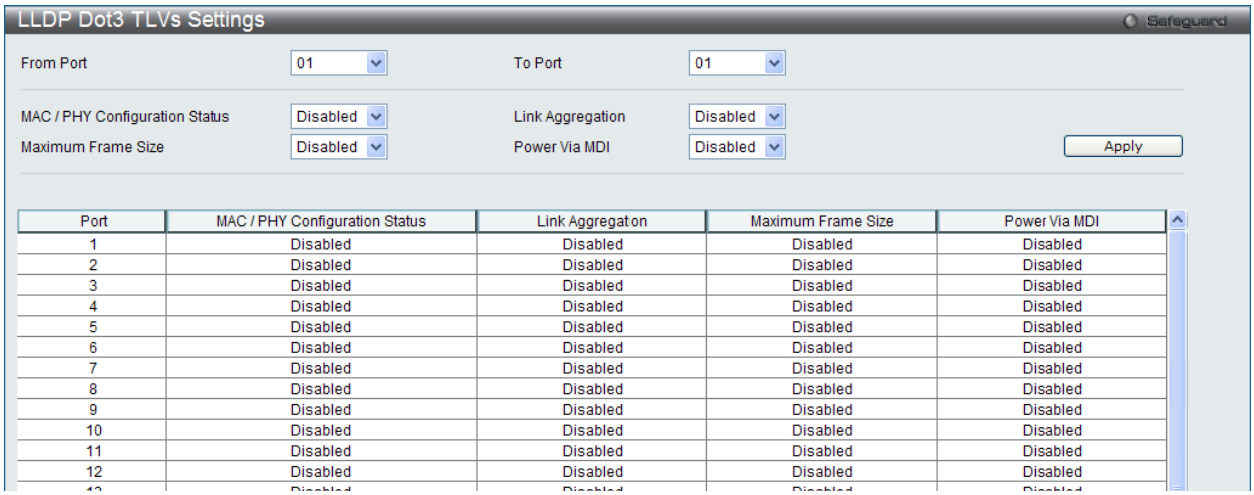


図 8-82　LLDP Dot3 TLVs Settings 画面

以下の項目を設定できます。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
MAC/PHY Configuration Status	スイッチの MAC または PHY 状態の通知を「Enabled」（有効）/「Disabled」（無効）にします。 本 TLV のオプションデータタイプは、LLDP エージェントが「MAC/PHY configuration/status TLV」を送信する必要があることを示します。このタイプは、IEEE 802.3 リンクの 2 つの終端が異なる速度設定で、何らかの限定的な接続性を確立することが可能であることを示しています。情報には、ポートがオートネゴシエーション機能をサポートしているかどうか、機能が有効であるかどうか、自動通知機能、および操作可能な MAU タイプが含まれます。初期値は無効です。
Link Aggregation	スイッチのリンクアグリゲーション状態の通知を「Enabled」（有効）/「Disabled」（無効）にします。 これは、LLDP エージェントが「Link Aggregation TLV」を送信する必要があることを示します。このタイプは IEEE 802.3 MAC における現在のリンクアグリゲーションステータスを示します。情報には、ポートがリンクアグリゲーションができるかどうか、ポートが集約した 1 つのリンクにまとめられるかどうか、および束ねられたポートの ID が含まれる必要があります。初期値は無効です。
Maximum Frame Size	最大フレームサイズの通知を「Enabled」（有効）/「Disabled」（無効）にします。LLDP エージェントが「Maximum-frame-size TLV」を送信する必要があることを示します。初期値は無効です。
Power Via MDI	プルダウンメニューを使用して、MDI 経由の電力供給機能を「Enable」（有効）/「Disable」（無効）にします。MDI TLV 経由の電力供給により、ネットワーク管理が通知を行い、送信する IEEE 802.3 LAN ステーション MDI 電力のサポート機能を検出します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Statistics System（LLDP 統計情報システム）

スイッチの各ポートにおける Neighbor 検出アクティビティ、LLDP 統計情報および設定の概要を表示します。

L2 Features > LLDP > LLDP > LLDP Statistics System の順にメニューをクリックし、以下の画面を表示します。

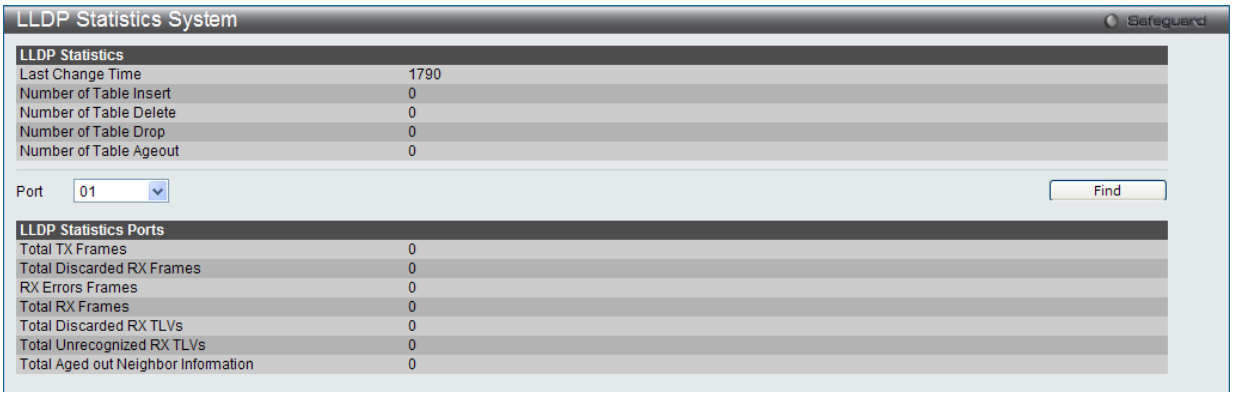


図 8-83　LLDP Statistics System 画面

ポート番号を選択し、「Find」ボタンをクリックして、特定ポートの統計情報を参照します。

LLDP Local Port Information（LLDP ローカルポート情報）

ローカルポートの要約テーブルに外向きの LLDP 通知を入力するために現在有効なポートベースの情報を表示します。

ポートごとに LLDP ローカルポート情報を参照するには、「Show Normal」ボタンをクリックします。
ポートごとに LLDP Local Port 情報の概要を参照するためには、「Show Brief」ボタンをクリックします。

L2 Features > LLDP > LLDP > LLDP Local Port Information の順にメニューをクリックし、以下の画面を表示します :

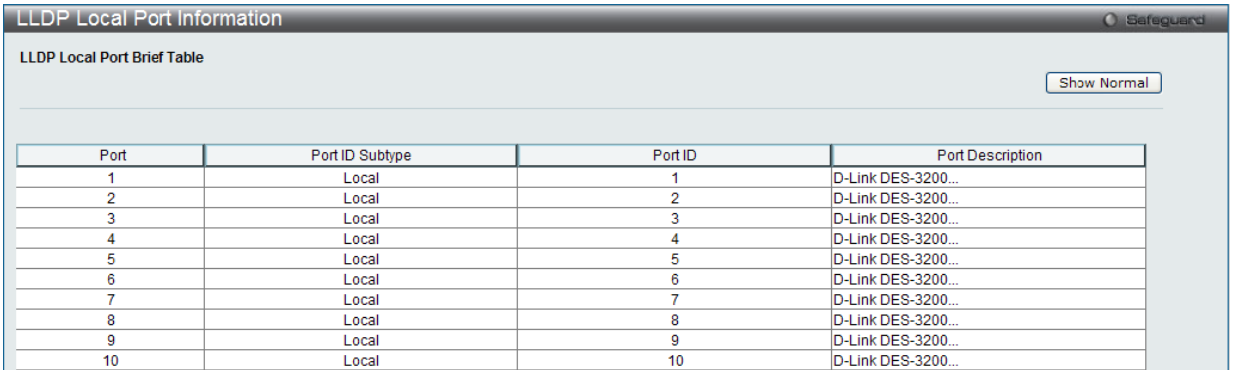


図 8-84　LLDP Local Port Information 画面 - Brief

「Show Detail」リンクをクリックすると、以下の画面を表示されます。

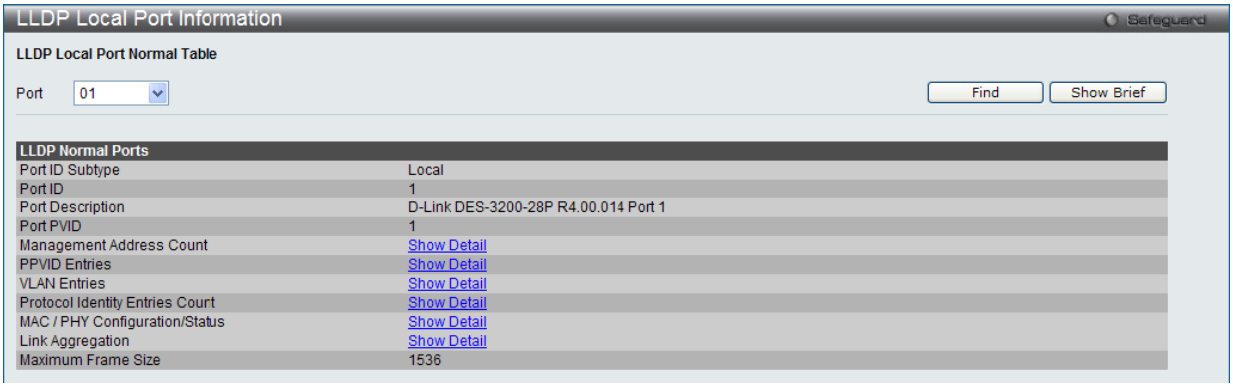


図 8-85　LLDP Local Port Information 画面 - Normal

以下の項目を設定できます。

項目	説明
Port	プルダウンメニューを使用してポートを指定します。

ポート番号を選択し、「Find」ボタンをクリックして指定エントリを表示します。

例えば、管理アドレスカウントに関してさらに詳細を参照するためには、「Management Address Count」の「Show Detail」リンクをクリックします。

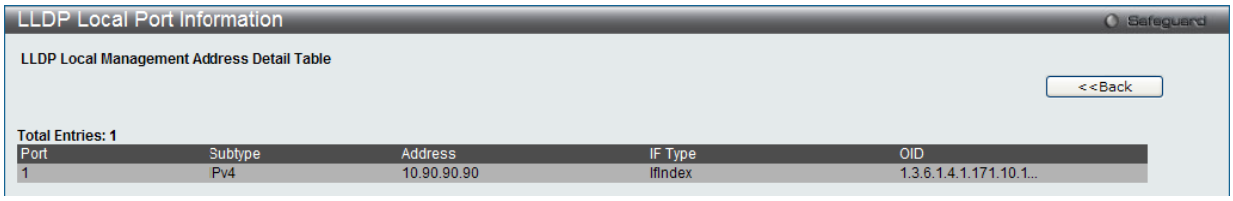


図 8-86　LLDP Local Port Information 画面 - Detail

「<<Back」をボタンをクリックして前のページに戻ります。

LLDP Remote Port Information（LLDP リモートポート情報）

Neighbor から学習したポート情報を表示します。スイッチは、リモートステーションからのパケットを受信しますが、ローカルとして情報を保存することができます。

L2 Features > LLDP > LLDP > LLDP Remote Port Information の順にメニューをクリックし、以下の画面を表示します。

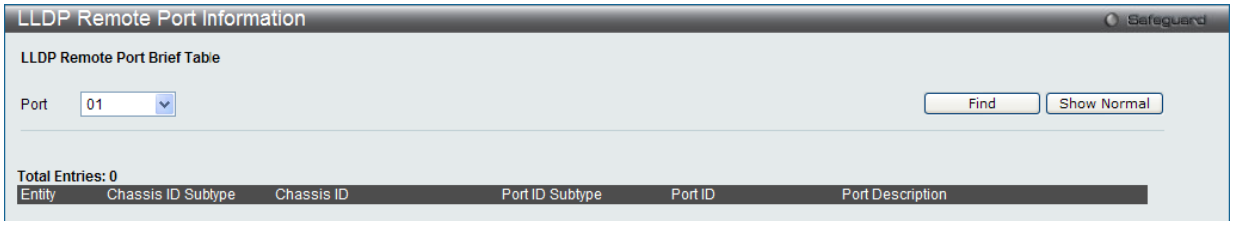


図 8-87　LLDP Remote Port Information 画面 - Brief

以下の項目を設定できます。

項目	説明
Port	プルダウンメニューを使用してポートを指定します。

ポート番号を選択し、「Find」ボタンをクリックして指定ポートの統計情報を表示します。

ポートごとに LLDP リモートポート情報を参照するには、「Show Normal」ボタンをクリックします。

図 8-88　LLDP Remote Port Information 画面 - Normal

「<<Back」をボタンをクリックして前のページに戻ります。

NLB FDB Settings（NLB FDB 設定）

本スイッチは、NLB（ネットワークロードバランシング）をサポートしています。これは、複数のサーバが同じ IP アドレスと MAC アドレスを共有できるマイクロソフト社のサーバロードバランシングアプリケーションをサポートするための MAC フォワーディングコントロールです。クライアントからのリクエストをすべてのサーバに送信しますが、それらの 1 つだけが処理します。マルチキャストモードでは、クライアントはサーバに到達するようにマルチキャスト MAC を宛先 MAC として使用します。モードに関係なく、宛先 MAC は共有 MAC です。サーバは応答パケットの送信元 MAC アドレスとして (共有 MAC よりむしろ) 自身の MAC アドレスを使用します。NLB マルチキャスト FDB エントリは L2 マルチキャストエントリと相互に排他的になっています。

L2 Features > NLB FDB Settings の順にメニューをクリックし、以下の画面を表示します。

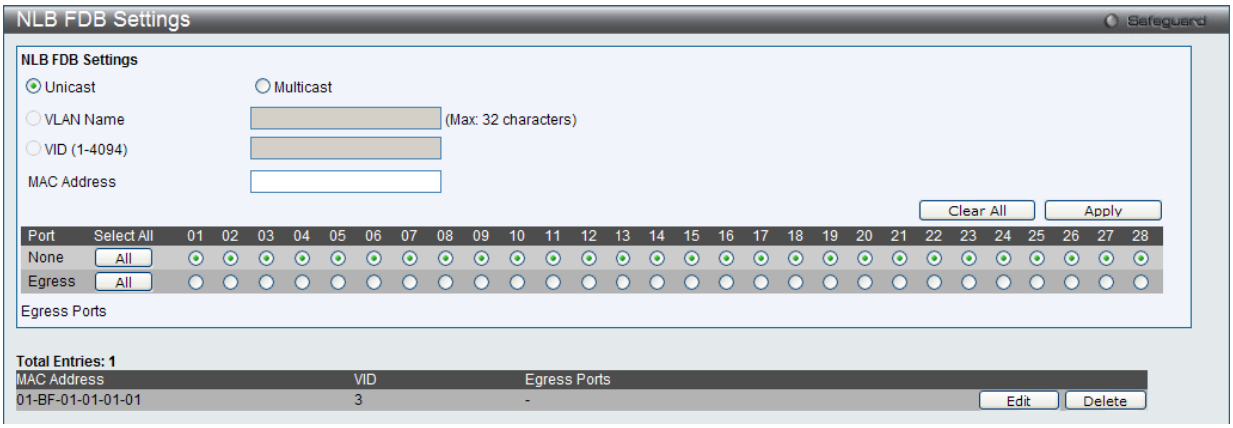


図 8-89　NLB FDB Settings 画面

以下の項目が設定可能です。

項目	説明
Unicast	ラジオボタンをクリックして、NLB ユニキャスト FDB エントリを作成します。
Multicast	ラジオボタンをクリックして、NLB マルチキャスト FDB エントリを作成します。
VLAN Name	ラジオボタンをクリックして、作成される NLB マルチキャスト FDB エントリの VLAN 名を入力します。
VID (1-4094)	ラジオボタンをクリックして、VLAN ID を入力します。
MAC Address	作成される NLB マルチキャスト FDB エントリの MAC アドレスを入力します。
Port	指定した NLB マルチキャスト FDB エントリに使用するフォワーディングポートを選択します。 • None - ポートはフォワーディングポートではありません。「All」ボタンをクリックするとすべてのポートを選択します。 • Egress - ポートはフォワーディングポートです。「All」ボタンをクリックするとすべてのポートを選択します。

「Apply」ボタンをクリックして行った変更を適用します。
「Clear All」ボタンをクリックして、すべての情報エントリをクリアします。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 画面上の「NLB FDB Settings」セクションの値を編集し、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

第 9 章　L3 Features（レイヤ 3 機能の設定）

L3 Features メニューを使用し、本スイッチにレイヤ 3 機能を設定することができます。

以下は L3 Features サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
IPv4 Static/Default Route Settings（IPv4 スタティック / デフォルトルート設定）	IPv4 スタティック / デフォルトルートの設定を行います。	152
IPv4 Route Table（IPv4 ルートテーブル）	IPv4 ルーティングテーブルの外部経路情報を参照します。	153
IPv6 Static/Default Route Settings（IPv6 スタティック / デフォルトルート設定）	IPv6 スタティック / デフォルトルートの設定を行います。	153

IPv4 Static/Default Route Settings（IPv4 スタティック / デフォルトルート設定）

本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。IPv4 には最大 256 個のスタティックルートエントリを作成することできます。

IPv4 スタティックルートのために、スタティックルートが一度設定されると、スイッチは設定されたネクストホップルータに ARP リクエストパケットを送信します。ARP の応答をネクストホップからスイッチが取得すると、ルートは有効になりますが、ARP エントリが既に存在している場合には、ARP 要求は送信されません。

L3 Features > IPv4 Static/Default Route Settings の順にメニューをクリックし、以下の画面を表示します。

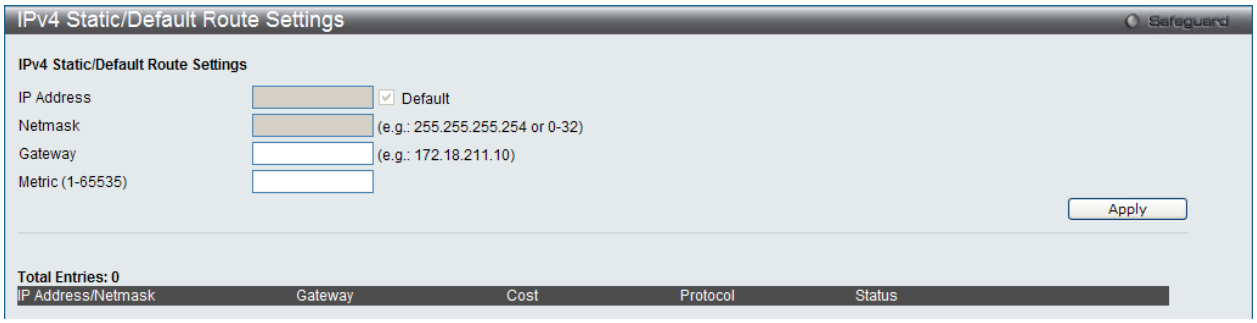


図 9-1　IPv4 Static/Default Route Settings 画面

画面には以下の項目が表示されます。

項目	説明
IP Address	スタティックルートに割り当てる IPv4 アドレスを入力します。「Default」をチェックすると、デフォルトルートに割り当てられます。
Netmask	対応するサブネットマスクを入力します。
Gateway	対応するゲートウェイ IP アドレスを入力します。
Metric	テーブルに入力した IP インタフェースのメトリック値を示します。1-65535 の範囲の値です。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの削除
対象のエントリの行の「Delete」ボタンをクリックします。

IPv4 Route Table（IPv4 ルートテーブル）

IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。

L3 Features > IPv4 Route Table の順にメニューをクリックし、以下の画面を表示します。

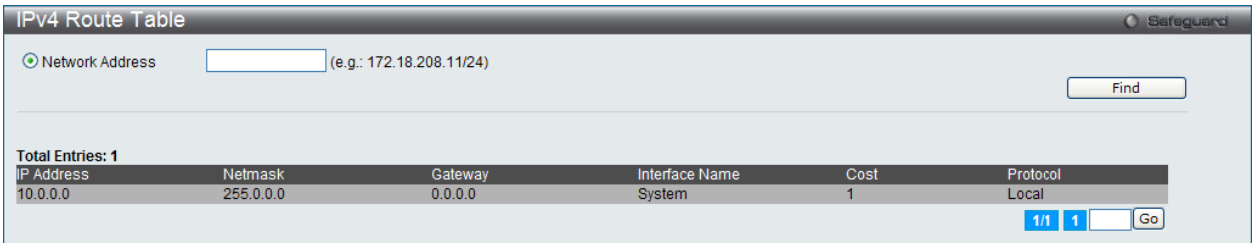


図 9-2　IPv4 Route Table 画面

画面には以下の項目が表示されます。

項目	説明
Network Address	表示するルートの宛先ネットワークアドレスを指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IPv6 Static/Default Route Settings（IPv6 スタティック / デフォルトルート設定）

IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。

L3 Features > IPv6 Static/Default Route Settings の順にメニューをクリックし、以下の画面を表示します。

図 9-3　IPv6 Static/Default Route Settings 画面

画面には以下の項目が表示されます。

項目	説明
IPv6 Address/Prefix Length	スタティックルートに割り当てる IPv6 アドレスを入力します。「Default」をチェックするとデフォルトルートに割り当てられます。
Interface Name	スタティック IPv6 ルートが作成される IP インタフェース名を指定します。
Nexthop Address	IPv6 形式におけるネクストホップゲートウェイアドレスに対応する IPv6 アドレスを指定します。
Metric (1-65535)	IPv6 インタフェースのメトリック値を指定します。スイッチと上記 IPv6 アドレス間のルータの数を表します。範囲は 1-65535 です。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの削除

テーブル内の削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

第 10 章　QoS（QoS 機能の設定）

以下は QoS サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
802.1p Settings（802.1p 設定）	ポート単位にプライオリティを割り当てます。以下のメニューがあります。 802.1p Default Priority Settings（ポートへのパケットプライオリティの割り当て）、802.1p User Priority Settings（802.1p ユーザプライオリティ）、802.1p Map Settings（802.1p マップ設定）	156
Bandwidth Control（帯域幅の設定）	送信と受信のデータレートを制限します。以下のメニューがあります。 Bandwidth Control Settings（帯域幅の設定）、Queue Bandwidth Control Settings（キュー帯域幅制御の設定）	158
Traffic Control Settings（トラフィックコントロールの設定）	ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整します。	160
DSCP（DSCP 設定）	ポートの DSCP トラスト状態の設定および DSCP マッピング設定を行います。以下のメニューがあります。 DSCP Trust Settings（DSCP トラスト設定）、DSCP Map Settings（DSCP マップ設定）	166
Scheduling Settings（スケジュールの設定）	QoS スケジューリングを設定します。以下のメニューがあります。 QoS Scheduling（QoS スケジュール作成）、QoS Scheduling Mechanism（QoS スケジュールメカニズム設定）	164

本スイッチシリーズは、802.1p プライオリティキューイング QoS(Quality of Service) をサポートしています。以下の項では QoS の機能と、802.1 プライオリティキューイングを利用するメリットについて説明します。

QoS の長所

QoS は IEEE 802.1p 標準で規定される技術で、ネットワーク管理者に、VoIP（Voice-over Internet Protocol）、Web 閲覧用アプリケーション、ファイルサーバアプリケーション、またはビデオ会議などの広帯域を必要とする、または高い優先順位を持つ重要なサービスのために、帯域を予約する方法を提供します。より大きい帯域を作成可能なだけではなく他の重要度の低いトラフィックを制限することで、ネットワークが必要以上の帯域を使用しないようにします。スイッチは各物理ポートで受信した様々なアプリケーションからのパケットをプライオリティに基づき独立したハードウェアキューに振り分けます。以下の図に、802.1p プライオリティキューイングがどのように本スイッチに実装されているかを示しています。

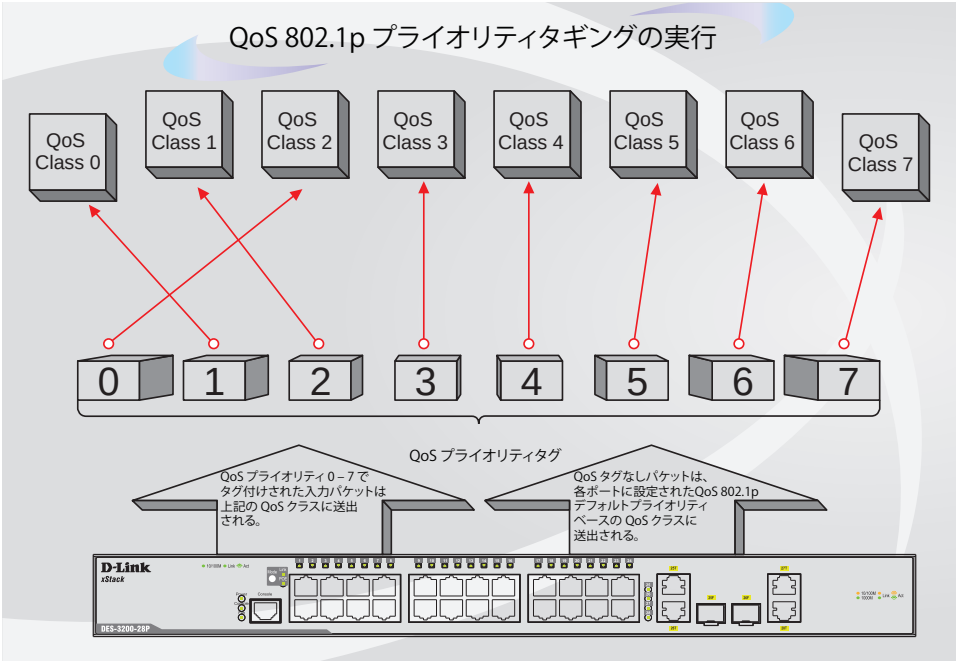


図 10-1　スイッチ上での QoS マッピングの例

上の図は本スイッチのプライオリティの初期設定です。クラス -7 は、スイッチ上における 7 つのプライオリティキューの中で、最も高い優先権を持っています。 QoS を実行するためには、ユーザはスイッチに対し、パケットのヘッダに適切な識別タグが含まれているかを確認するように指示する必要があります。そして、ユーザはそれらのタグ付きパケットをスイッチ上の指定されたキューに送り、優先順序に従って送出するようにします。

例えば、遠隔地に設置した 2 台のコンピュータ間でビデオ会議を行うとします。管理者は Access Profile コマンドを使用して、送信するビデオパケットにプライオリティタグを付加します。次に受信側ではスイッチにそのタグの確認するよう指示を行い、タグ付きパケットを受信したら、それをスイッチのクラスキューに関連付けを行うようにします。また、管理者はこのキューに優先順位を与え、他のパケットが送出されるよりも前に送信されるように設定を行います。この結果、このサービス用のパケットは、できるだけ早く送信され、キューが最優先されることにより、中断されることなくパケットを受け取ることができるため、このビデオ会議用に帯域を最適化することが可能になります。

QoS について

本スイッチには、4 つのプライオリティキューがあります。プライオリティキューには、最高レベルの 7 番（クラス 7）から最低レベルの 0 番（クラス 0）まであります。IEEE 802.1p に規定される 8 つのプライオリティタグはスイッチのプライオリティタグと以下のように関連付けされます。

- プライオリティ 0 は、スイッチの Q2 キューに割り当てられます。
- プライオリティ 1 は、スイッチの Q0 キューに割り当てられます。
- プライオリティ 2 は、スイッチの Q1 キューに割り当てられます。
- プライオリティ 3 は、スイッチの Q3 キューに割り当てられます。
- プライオリティ 4 は、スイッチの Q4 キューに割り当てられます。
- プライオリティ 5 は、スイッチの Q5 キューに割り当てられます。
- プライオリティ 6 は、スイッチの Q6 キューに割り当てられます。
- プライオリティ 7 は、スイッチの Q7 キューに割り当てられます。

Strict（絶対優先）のプライオリティベースのスケジューリングでは、優先度の高いキューに属するパケットから送信されます。優先度の高いキューが複数ある場合は、プライオリティタグに従って送信されます。高プライオリティのキューが空である時にだけプライオリティの低いパケットは送信されます。

重み付けラウンドロビンキューイングでは、各プライオリティキューから送信されるパケットの数は、指定された重み付けによって決定されます。A から H までの 8 つある CoS キューに、8 から 1 までの重み付けを設定したとすると、パケットは以下の順に送信されます。: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1。

重み付けラウンドロビンキューイングでは、各 QoS キューが同じ重み付けを持つならば、各 QoS キューのパケット送信の機会はラウンドロビンキューイングのように、全く同じになります。また、ある CoS の重み付けとして 0 を設定すると、その CoS から送信するパケットがなくなるまでパケットを処理します。0 以外の値を持つ他の CoS キューでは、重み付けラウンドロビンの規則により、重みに従って送信を行います。

注意 本スイッチは内部的にはポートに対して 8 つのサービスクラスを持っています。そのうち 1 つは最初からスイッチが使用するように予約されていて変更できません。以下のサービスクラスに関する説明はすべて管理者が使用および変更できる 8 つのサービスクラスについて行っています。

802.1p Settings（802.1p 設定）

802.1p Default Priority Settings（ポートへのパケットプライオリティの割り当て）

本スイッチは、各ポートにデフォルトの 802.1p プライオリティを割り当てることができます。

本画面では、スイッチのそれぞれのポートにデフォルトの 802.1p プライオリティを割り当てて、受信したタグなしパケットに 802.1p プライオリティタグを挿入します。プライオリティと有効なプライオリティタグは、最低の 0 から最高の 7 まで指定できます。有効なプライオリティは、RADIUS に割り当てられた実際のプライオリティを示しています。RADIUS が割り当てた値が指定した制限を超えると、値はデフォルトプライオリティに設定されます。例えば、RADIUS が制限値に 8、デフォルトプライオリティに 0 を割り当てている場合、有効なプラオリティは 0 になります。

QoS > 802.1p Settings > 802.1p Default Priority Settings の順にクリックし、以下の画面を表示します。

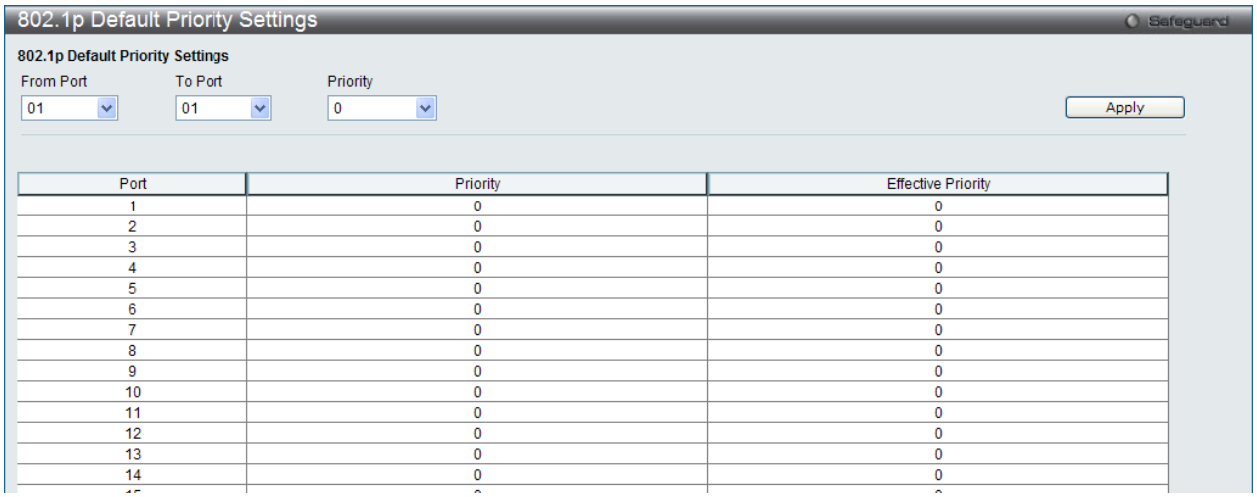


図 10-2　802.1p Default Priority Settings 画面

新しいデフォルトプライオリティを実行するためには、はじめに「From」、「To」プルダウンメニューでポート範囲を選択し、「Priority」プルダウンメニューで値 0 から 7 を選択します。「Apply」ボタンをクリックして行った変更を適用します。

本画面には以下の項目があります。

項目	説明
From Port / To Port	使用する開始 / 終了ポートを選択します。
Priority	プルダウンメニューを使用して、0-7 の値を選択します。

「Apply」ボタンをクリックして行った変更を適用します。

802.1p User Priority Settings（802.1p ユーザプライオリティ）

スイッチは各 802.1p プライオリティにユーザプライオリティを割り当てることができます。

QoS > 802.1p Settings > 802.1p User Priority Settings の順にクリックし、以下の画面を表示します。

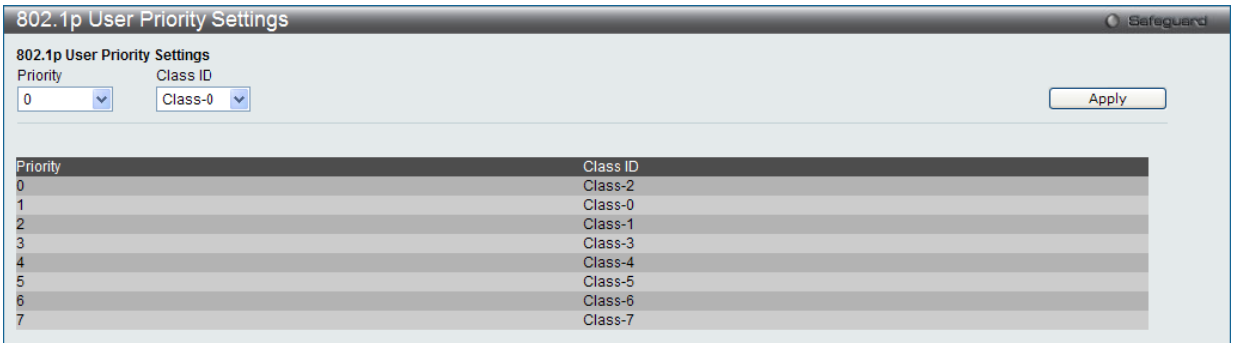


図 10-3　802.1P User Priority Settings 画面

スイッチのポートグループにプライオリティを割り当てると、本画面のプルダウンメニューを使用して 802.1p プライオリティの 8 レベルのそれぞれに対してクラスを設定することができます。ユーザプライオリティのマッピングは最後のページで設定したデフォルトプライオリティに対するだけではなく、802.1p タグを持つすべての入力パケットに対しても行われます。

本画面には以下の項目があります。

項目	説明
Priority	キューに割り当てられるプライオリティを表示します。
Class ID	プライオリティを割り当てるクラス（キュー）を設定します。「Class-0」（クラス 0）は最も低い優先度のキューで、「Class-3」（クラス 7）が最も高くなります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

802.1p Map Settings（802.1p マップ設定）

802.1p のパケットの初期カラーに対するマッピングを行います。

QoS > 802.1p Settings > 802.1p Map Settings の順にメニューをクリックし、以下の画面を表示します。:

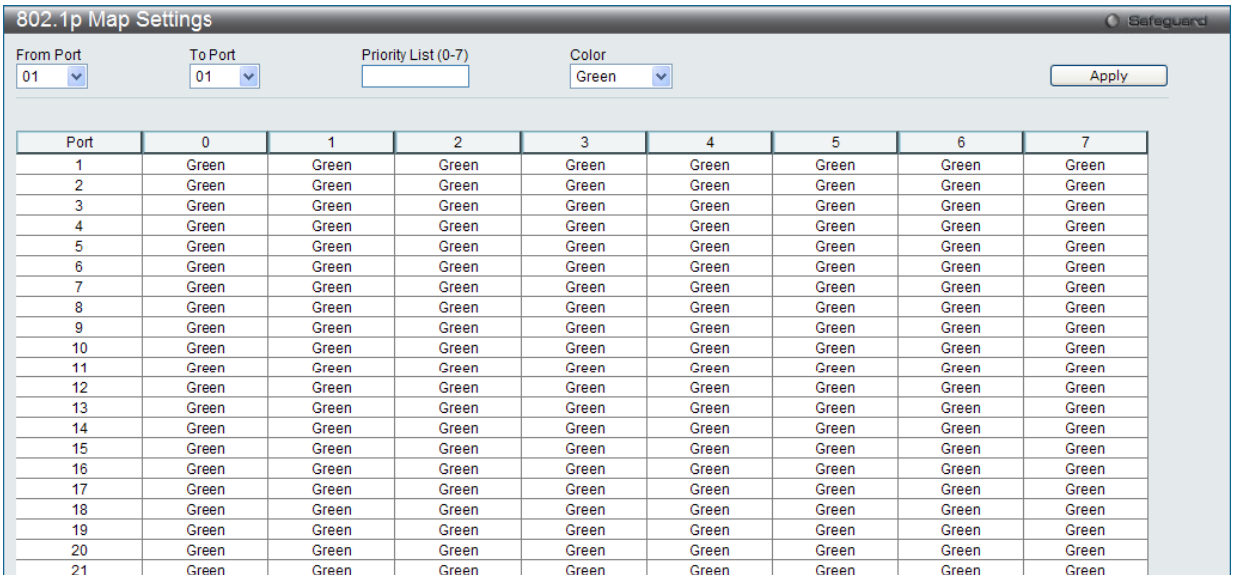


図 10-4　802.1p Map Settings 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	使用する開始 / 終了ポートを選択します。
Priority (0-7)	入力パケットに対する送信元優先度のリストを入力します。
Color	マップするパケットカラーを選択します。初期値は緑です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Bandwidth Control（帯域幅の設定）

帯域制御の設定を行うことにより、すべての選択ポートに対して、送信と受信のデータレートを制限することができます。

Bandwidth Control Settings（帯域幅の設定）

「Effective RX Rate」は設定した速度に一致しない場合にスイッチポートの実際の帯域幅を表示します。これは、通常 RADIUS サーバをなどの高優先度を持つリソースが割り当てた速度を表示します。

QoS > Bandwidth Control > Bandwidth Control Settings の順にメニューをクリックし、以下の画面を表示します。

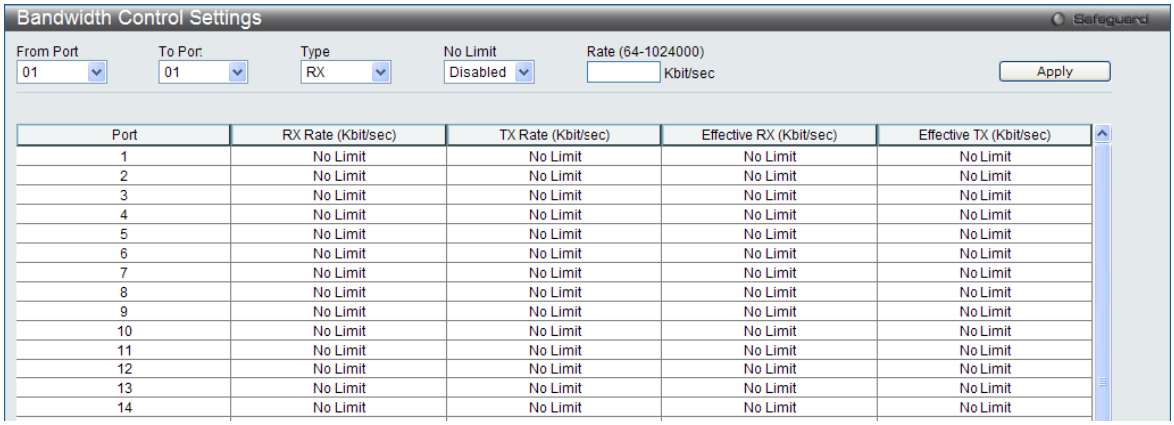


図 10-5　Bandwidth Control Settings 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	設定対象のポート範囲を指定します。
Type	RX（受信）、TX（送信）および Both（両方）から選択します。帯域上限を受信、送信、送受信の両方のいずれに適用するのかを設定します。
No Limit	選択ポートに対する帯域制限を設定します。 • Enabled - ポートで帯域制限を行いません。 • Disabled - ポートで帯域制限を行います。（初期値） **注意**　設定値がポート速度より大きいと、帯域幅制限の意味がなくなります。
Rate (64-1024000)	選択ポートのデータ速度の上限値（Kbit/ 秒）を指定します。値は 64 から 1024000 の間で速度を指定します。
Effective RX	RADIUS サーバが RX の帯域幅を割り当てると、それは有効な RX 帯域幅となります。RADIUS サーバを使用した認証は、ポートごとかユーザごとに行われます。ユーザごとの認証のために、指定ポートに複数ユーザが割り当てられていると、割り当てられる RX 帯域幅が複数あります。最終的な RX 帯域幅は、これら複数の RX 帯域幅の中で最も大きいものとなります。
Effective TX	RADIUS サーバが TX の帯域幅を割り当てると、それは有効な TX 帯域幅となります。RADIUS サーバを使用した認証は、ポートごとかユーザごとに行われます。ユーザごとの認証のために、指定ポートに複数ユーザが割り当てられていると、割り当てられる TX 帯域幅が複数あります。最終的な TX 帯域幅は、これら複数の TX 帯域幅の中で最も大きいものとなります。

「Apply」ボタンをクリックし、選択ポートの帯域制御を設定します。設定の結果は、画面下部の「Bandwidth Control Table」に表示されます。

Queue Bandwidth Control Settings（キュー帯域幅制御の設定）

キューの帯域幅を設定します。

QoS > Bandwidth Control > Queue Bandwidth Control Settings の順にメニューをクリックし、以下の画面を表示します。

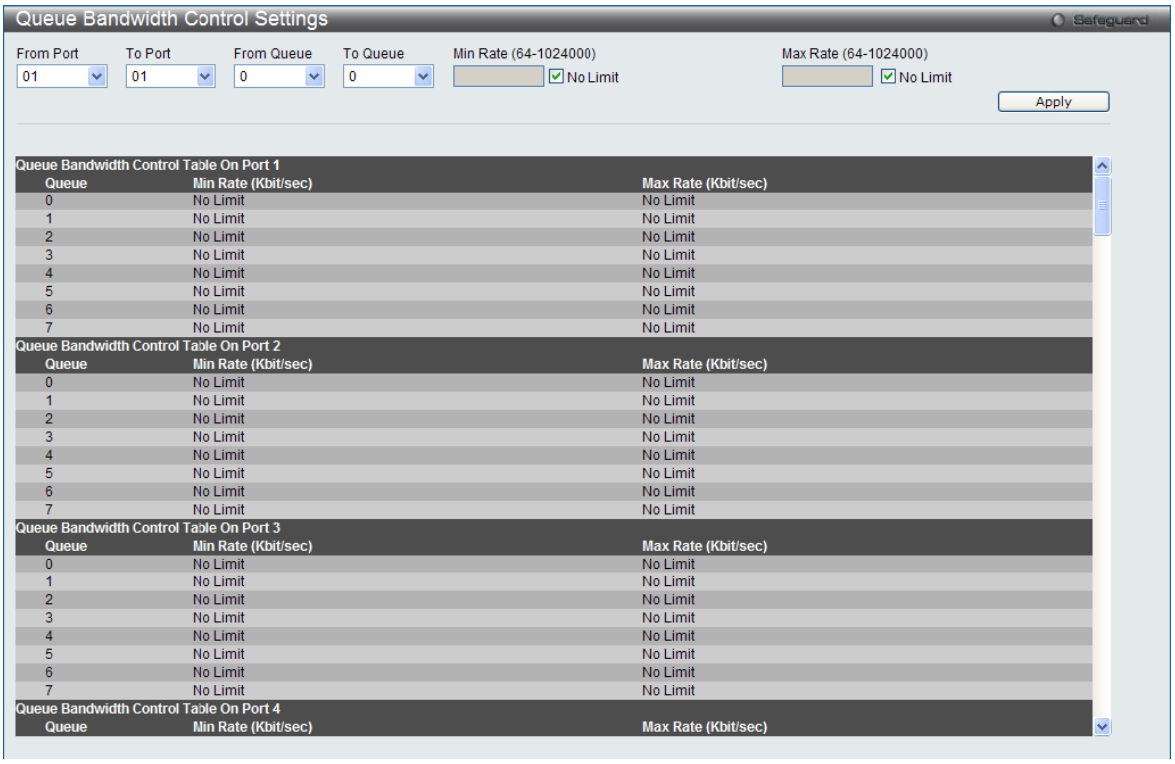


図 10-6　Queue Bandwidth Control Settings 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	この設定に使用するポート範囲を選択します。
From Queue / To Queue	この設定に使用するキュー範囲を選択します。
Min Rate (64-10240000)	ポートが受信できるパケット制限 (Kbps) を指定します。「No Limit」をチェックすると指定キューが受信するパケットにレート制限がなくなります。
Max Rate (64-10240000)	キューの最大レートを入力します。「No Limit」オプションを選択すると、レート制限はなくなります。

「Apply」ボタンをクリックして行った変更を適用します。

注意　キュー帯域幅制御の最小グラニュラリティは 64Kbps です。システムは自動的に 64 倍の数に調整します。

Traffic Control Settings（トラフィックコントロールの設定）

コンピュータネットワーク上にはマルチキャストパケットやブロードキャストパケットなどのパケットが正常な状態でも絶えずあふれています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどのように誤動作しているデバイスによって増加することもあります。 そのため、スイッチのスループットに関する問題が発生し、その結果、ネットワークの全体的なパフォーマンスにも影響する可能性があります。このパケットストームを調整するために、本スイッチは状況を監視し、制御します。

パケットストームを監視し、ユーザが指定したしきい値レベルを基に非常に多くのパケットがネットワークであふれているどうかを判断します。パケットストームが検出されると本スイッチはパケットストームが緩和されるまで受信したパケットを破棄します。この方法を使用するためには以下の画面の「Action」欄の「Drop」オプションを設定します。

トラフィックコントロールに設定したポートで本時間経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」(永久シャットダウン) モードに遷移し、トラップレシーバに送信する警告メッセージを生成します。一度「Shutdown Forever」モードに入ると、本ポートを回復する方法は、**System Configuration > Port Configuration > Port Settings** 画面で手動により有効状態に戻すか、または「Traffic Auto Recover Time」欄に設定した時間経過後自動的に回復します。無効なポートを選択して、「Status」を「Enabled」ステータスに戻します。このようなストームコントロール機能を利用するためには、次に示す画面の「Action」フィールドで「Shutdown」オプションを選択してください。この画面を使用して、ストームコントロールの有効 / 無効や、マルチキャストおよびブロードキャストのしきい値の調整を行います。

QoS > Traffic Control Settings の順にクリックし、以下の画面を表示します。

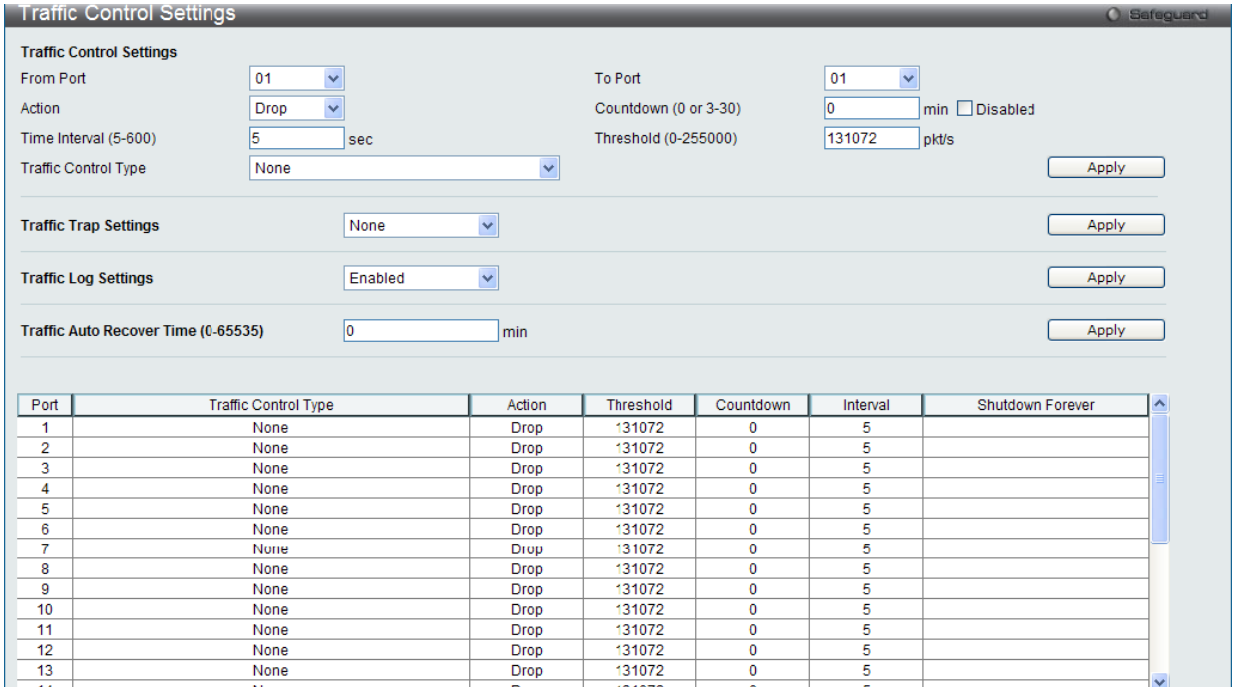


図 10-7　Traffic Control Settings 画面

本画面には次の項目があります。

項目	説明
Traffic Control Settings	
From Port / To Port	ストームコントロールを表示するポート範囲を設定します。
Action	トラフィックコントロールの方法をプルダウンメニューで指定します。以下の方法を指定できます。 • Drop – スイッチのハードウェアによるトラフィックコントロールを行います。選択すると、スイッチのハードウェアが指定したしきい値に基づくパケットストームの検知を行い、パケットストームが発生すると、状態が改善するまでパケットの廃棄を行います。 • Shutdown – スイッチのソフトウェアによるトラフィックコントロールにより、トラフィックストームの発生を検知します。ストームが検出されると、スイッチはスパニングツリーの保持に必要である STP BPDU パケットを除くすべてのトラフィックの入力に対して、ポートをシャットダウンします。カウントタイマ経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」(永久シャットダウン) モードに遷移し、5 分後自動的にポートが回復するまで操作できません。本ポートを通常の状態に戻すには、**System Configuration > Port Configuration> Port Settings** 画面で、無効になっているポートを手動で有効状態に戻します。本オプションを選択する際は、スイッチのチップからパケットカウントを受け取ってパケットストームの発生を検知するために必要な「Time Interval」の設定も必要となります。
Countdown (0 or 3-30)	本値はスイッチがトラフィックストームが発生中のポートをシャットダウンするまでに待機する時間 (分) を表します。本値は、「Action」で「Shutdown」を指定し、ハードウェアによるトラフィックコントロールを行わない場合に有効です。0、3-30（分）が指定できます。機能を「Disabled」にすると、オプションは無効になります。

項目	説明
Time Interval (5-600)	スイッチのチップからトラフィックコントロール機能に送信する、マルチキャストおよびブロードキャストパケットカウントの送信間隔を指定します。このパケットカウントにより、いつ入力パケットがしきい値を超過したかの検出が行われます。値の範囲は 5-600 で、初期値は 5（秒）です。
Threshold (0-255000)	トラフィックコントロール機能を起動させるトリガーとなる、1 秒あたりの最大パケット数。設定可能なしきい値の範囲は 0-255000 です。初期値は 131072 パケット / 秒です。
Traffic Control Type	検知の対象となるストームの種類を選択します。 Broadcast、Multicast、Unknown Unicast、Broadcast + Multicast、Broadcast + Unknown Unicast、Multicast + Unknown Unicast、Broadcast + Multicast + Unknown Unicast、または None
Traffic Trap Settings	トラフィックコントロール機能によるトラフィックストームの扱いを指定します。 • None - ストームトラップメッセージを送信しません。 • Storm Occurred - ストームトラップ発生時にストームトラップ警告メッセージを送信します。 • Storm Cleared - スイッチがストームトラップを消失させた時ストームトラップメッセージを送信します。 • Both - ストームトラップ発生時と消失時にストームトラップメッセージを送信します。 本機能は、ハードウェアモード中 (「Action」で「Drop」が選択された時) は実行できません。
Traffic Log Settings	プルダウンメニューを使用して、本機能を「Enabled」(有効)/「Disabled」(無効) にします。ログ状態が有効な場合、ストームが発生した場合やストームがクリアされた場合にトラフィックコントロール状態がログに出力されます。ログ状態が無効な場合、トラフィックコントロールイベントはログに出力されません。
Traffic Auto Recover Time (0-65535)	ポートがシャットダウンからの自動回復を許可する時間を入力します。初期値は 0 で、自動回復モードが無効で、永久にシャットダウンするということを意味します。ポートをフォワーディング状態に戻すためには、**System Configuration > Port Configuration > Port Settings** 画面で手動の設定が必要です。

注意 トラフィックコントロールは、リンクアグリケーション（ポートトランキング）が設定されたポートに対しては行うことができません。

注意 「Shutdown Forever」モードのポートは、スイッチの CPU に BPDU 送信を行いますが、「Spanning Tree」画面では「Discarding」状態として表示されます。

注意 「Shutdown Forever」モードのポートは、ユーザがポートの復旧を行うまでの間はリンクダウン状態として表示されます。

注意 各ポートの最小のストームコントロールの最小グラニュラリティは 1pps です。

DSCP（DSCP 設定）

DSCP Trust Settings（DSCP トラスト設定）

ポートの DSCP トラスト状態を設定します。ポートが DSCP トラストモードにある場合、スイッチは、デフォルトポートプライオリティの代わりに DSCP マップ設定を使用して、タグなしパケットにプライオリティタグを挿入します。

QoS > DSCP > DSCP Trust Settings の順にクリックし、以下の画面を表示します。

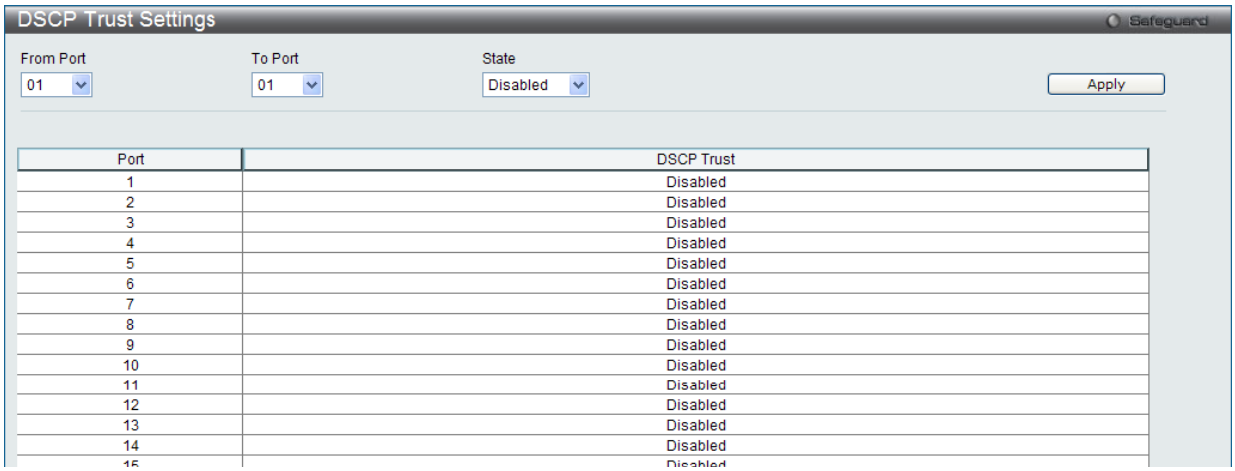


図 10-8　DSCP Trust Settings 画面

本画面には次の項目があります。

項目	説明
From Port / To Port	設定するポート範囲を選択します。
State	トラスト DSCP を有効または無効にします。初期値ではトラスト DSCP は無効です。

「Apply」ボタンをクリックして行った変更を適用します。

DSCP Map Settings（DSCP マップ設定）

キューに対する DSCP のマッピングは、ポートが DSCP トラスト状態にある場合、（次に、スケジューリングキューを決定するのに使用される）パケットのプライオリティを決定するために使用されます。パケットがポートへのイングレスである場合に、DSCP-to-DSCP マッピングはパケットの DSCP のスワップに使用されます。残りのパケットの処理は新しい DSCP に基づきます。初期値では、DSCP は同じ DSCP にマップされます。

QoS > DSCP > DSCP Map Settings の順にクリックし、以下の画面を表示します。

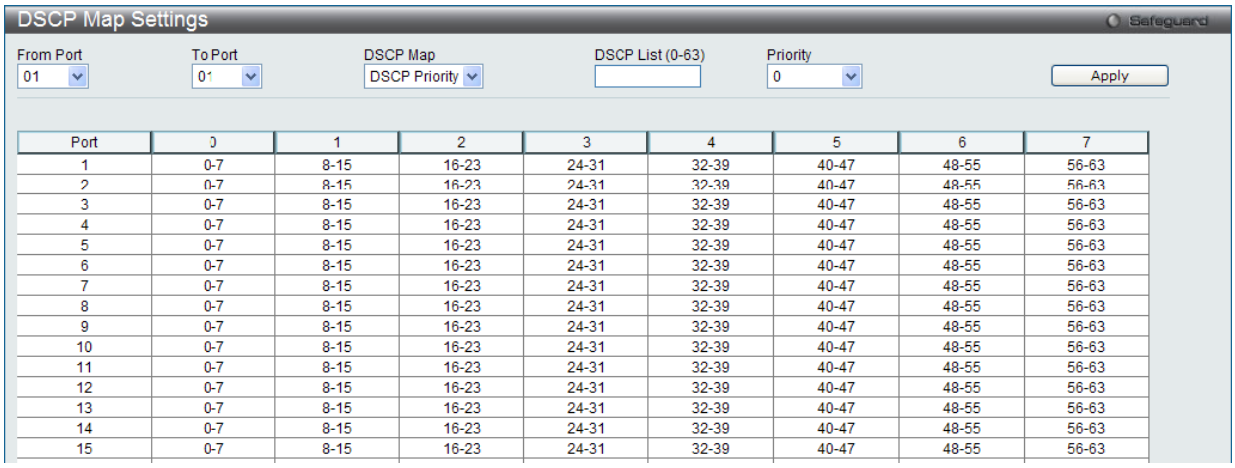


図 10-9　DSCP Map Settings - DSCP Priority 画面

QoS > DSCP > DSCP Map Settings の順にクリックし、「DSCP Map」メニューから「DSCP DSCP」を選択して以下の画面を表示します。

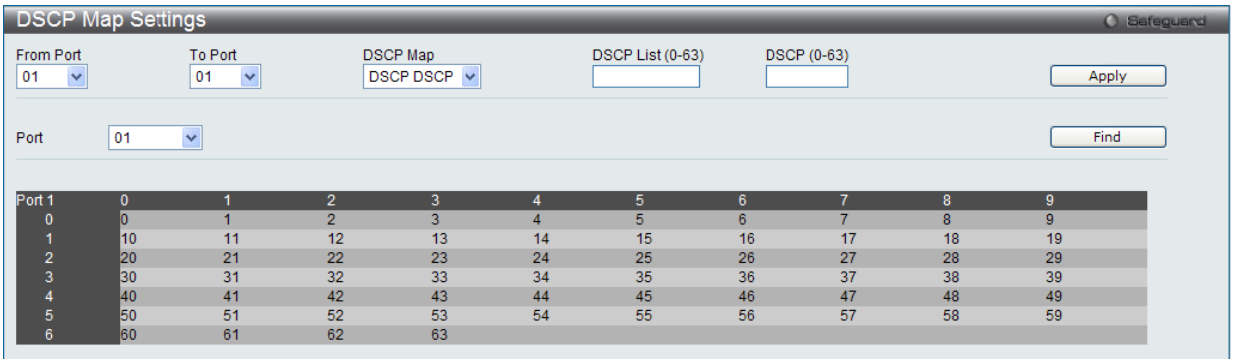


図 10-10　DSCP Map Settings - DSCP Priority 画面

QoS > DSCP > DSCP Map Settings の順にクリックし、「DSCP Map」メニューから「DSCP Color」を選択して以下の画面を表示します。

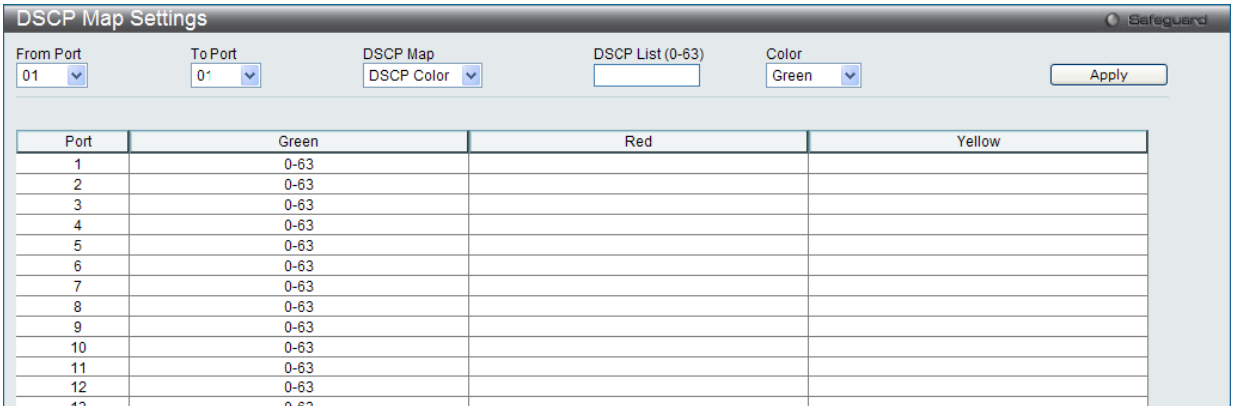


図 10-11　DSCP Map Settings - DSCP Color 画面

本画面には次の項目があります。

項目	説明
From Port / To Port	プルダウンメニューを設定するポート範囲を指定します。
DSCP Map	プルダウンメニューを使用して以下のオプションから 1 つを選択します。 • DSCP Priority - 指定プライオリティにマップする DSCP 値のリストを指定します。 • DSCP DSCP - 指定した DSCP にマップする DSCP 値のリストを指定します。 • DSCP Color - 指定カラーにマップする DSCP 値のリストを指定します。
DSCP List (0-63)	DSCP リストを入力します。
Priority	プライオリティ値を選択します。「DSCP Map」から「DSCP Priority」を選択すると、表示されます。
DSCP (0-63)	DSCP 値を入力します。「DSCP Map」プルダウンメニューで「DSCP DSCP」を選択すると表示されます。
Port	ポートを指定します。「DSCP Map」プルダウンメニューで「DSCP DSCP」を選択すると表示されます。
Color	マッピングの結果のカラーを選択します。「DSCP Map」から「DSCP Color」を選択すると表示されます。

「Apply」ボタンをクリックして行った変更を適用します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

Scheduling Settings（スケジュール設定）

QoS Scheduling（QoS スケジュール作成）

スイッチで利用可能な 8 個のハードウェアキューの 1 つに入力パケットの 802.1p ユーザプライオリティに基づいてポートごとに入力パケットを照合する方法を設定します。

QoS > Scheduling Settings > QoS Scheduling の順にメニューをクリックし、以下の画面を表示します。

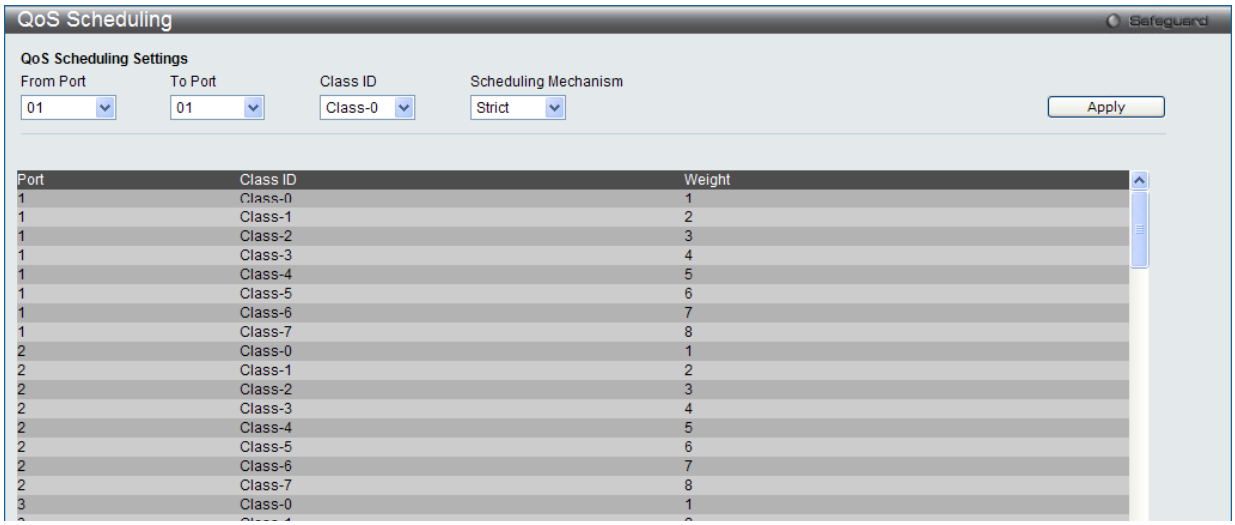


図 10-12　QoS Scheduling 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	設定対象のポート (範囲) を指定します。
Class ID	QoS パラメータに設定するクラス ID を 0 から 7 の範囲で指定します。
Scheduling Mechanism	• Strict - 上位の CoS キューからトラフィックを処理します。上位キューの送信が完了するまで下位キューからはパケットは送信されません。 • Weight - プライオリティのサービスクラスで配分されたパケットを重み付けされたラウンドロビン (WRR) アルゴリズムによって処理します。

「Apply」ボタンをクリックして行った変更を適用します。

QoS Scheduling Mechanism（QoS スケジュールメカニズム設定）

QoS のカスタマイズは、スイッチのハードウェアキューに使用する出力スケジュールを変更することにより実行できます。QoS 設定の変更は、どのような変更であっても気をつけて行う必要がありますが、特に優先度の低いキューでのネットワークトラフィックへの影響に注意が必要です。スケジュールの変更により、許容範囲外のパケットロスや重大な伝送遅延が発生することがあります。不適切な QoS 設定により急激なボトルネックが引き起こされる場合があるため、本設定をカスタマイズする際、特にトラフィックのピーク時には、ネットワークパフォーマンスをモニタしながら行うことが重要です。

QoS > Scheduling Settings > QoS Scheduling Mechanism の順にクリックし、以下の画面を表示します。

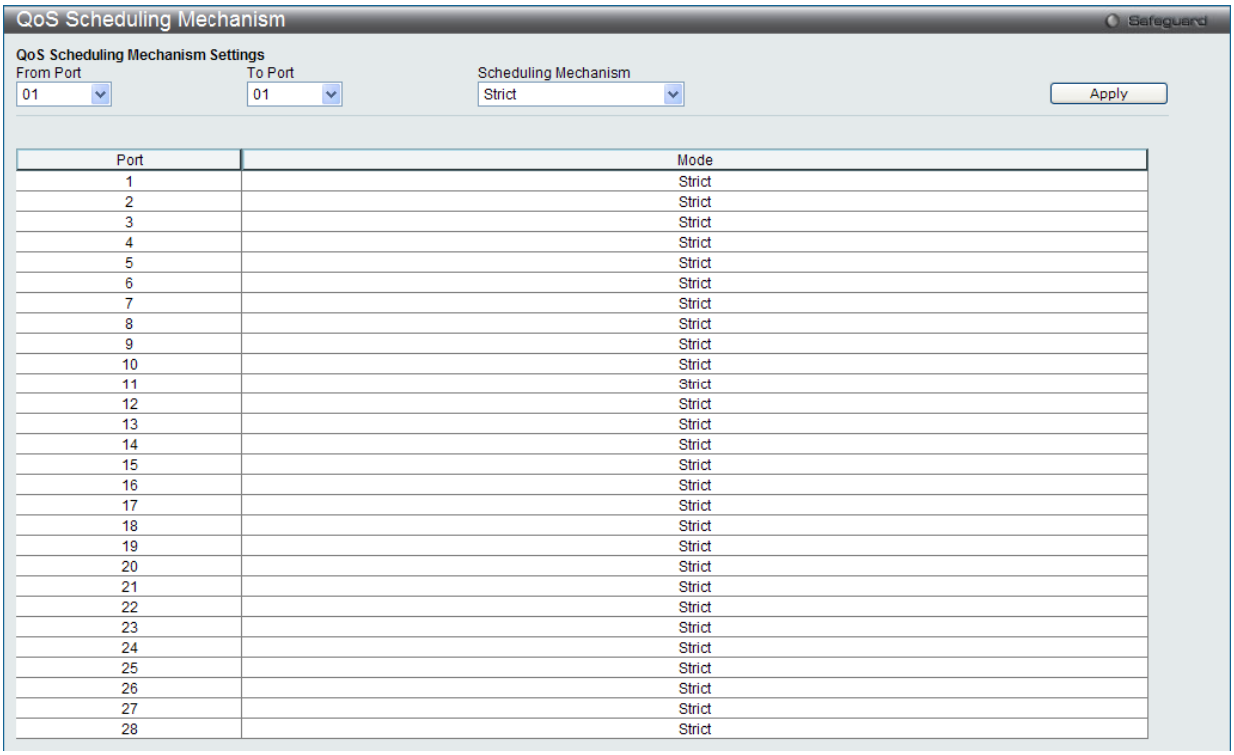


図 10-13　Scheduling Profile Settings 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	設定対象のポート (範囲) を指定します。
Scheduling Mechanism	2 つのスケジューリングメカニズムの 1 つを選択します。 • Strict - 上位の CoS キューからトラフィックを処理します。上位キューの送信が完了するまで下位キューからはパケットは送信されません。 • Weight Round Robin - プライオリティ CoS で配分されたパケットを重み付けされたラウンドロビン (WRR) アルゴリズムによって処理します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 キューに割り当てる 0 から 7 の番号は IEEE 802.1p プライオリティタグの番号を表しています。ポート番号の指定ではない点にご注意ください。

第 11 章　ACL（ACL 機能の設定）

ACL メニューを使用し、本スイッチにアクセスプロファイルおよびルールの設定を行うことができます。

以下は、ACL サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
ACL Configuration Wizard（ACL 設定ウィザード）	ウィザードを使用してアクセスプロファイルとルールを作成します。	166
Access Profile List（アクセスプロファイルリスト）	パケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定するプロファイルを設定します。	168
CPU Access Profile List（CPU アクセスプロファイルリスト）	CPU インタフェースフィルタリング機能を設定します。	185
ACL Finder（ACL 検索）	ACL エントリを検索します。	200
ACL Flow Meter（ACL フローメータ）	フローごとの帯域幅制御設定を行います。	201

ACL Configuration Wizard（ACL 設定ウィザード）

ACL 設定ウィザードは、必要なアドレスやサービスタイプおよび操作を簡単に入力することで自動的にアクセスプロファイルと ACL ルールを作成します。管理者の多くの時間を節約します。

ACL > ACL Configuration Wizard の順にメニューをクリックし、以下の画面を表示します。

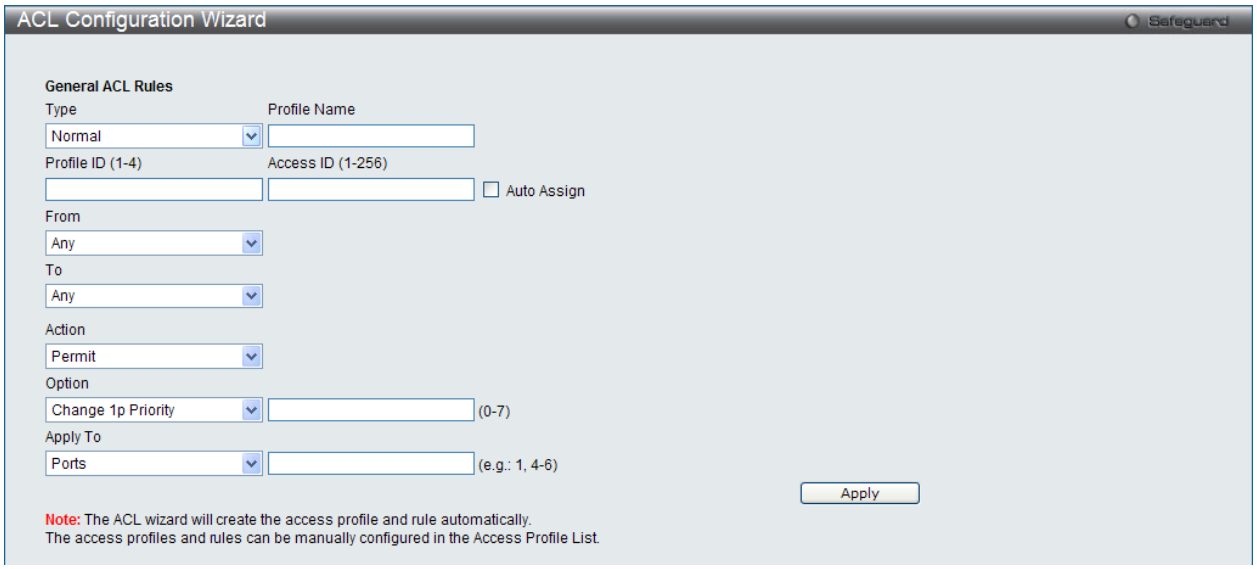


図 11-1　ACL Configuration Wizard 画面

1. ACL の種類（Normal または CPU）を選択します。「Normal」を選択すると、スイッチのインタフェースの 1 つに受信したパケットに適用される ACL ルールを作成します。「CPU」を選択すると、スイッチに送信されるパケットにだけ適用される ACL ルールを作成します。
2. Profile ID と Access ID を割り当てるか、またはこれを自動的に行うために「Auto Assign」欄をチェックします。
3. 範囲を From（Any、MAC Address、IPv4 Address または IPv6）と To（Any、MAC Address、IPv4 Address）から選択します。
4. 「Action」を「Permit」、「Deny」または「Mirror」から選択します。
5. 「Option」を「Change 1p Priority」、「Replace DSCP」または「Replace ToS Precedence」から選択し、隣接している欄に 0-7 の値を入力します。
6. 新しい ACL ルール用のポートを「Ports」横の欄に入力し、「Apply」ボタンをクリックして設定を適用します。

以下の項目を使用して、設定を行います。

項目	説明
Type	プルダウンメニューを使用して以下の ACL ルールタイプを選択します。 • Normal - ノーマル ACL ルールを作成します。 • CPU - CPU ACL ルールを作成します。 • Egress - Egress ACL ルールを作成します。
Profile Name	「Normal」タイプルールを選択後、新しいルールに対するプロファイル名を入力します。
Profile ID	新しいルールに対するプロファイル ID を入力します。「Type」プルダウンメニューから「Normal」を選択した場合のプロファイル ID の範囲は 1-4 です。「Type」プルダウンメニューから「CPU」を選択した場合のプロファイル ID の範囲は 1-5 です。
Access ID	新しいルールに対するアクセス ID を入力します。「Auto Assign」オプションを選択すると、このルールに対して自動的に未使用のアクセス ID を割り当てます。「Type」プルダウンメニューから「Normal」を選択した場合のアクセス ID の範囲は 1-256 です。「Type」プルダウンメニューから「CPU」を選択した場合のアクセス ID の範囲は 1-100 です。
From / To	以下の 4 つの異なるカテゴリに適用するためにこのルールを作成します。 • Any - あらゆる開始カテゴリをこのルールに含めます。 • MAC Address - このルールに MAC アドレス範囲を入力します。 • IPv4 Address - このルールに IPv4 アドレス範囲を入力します。 • IPv6 - このルールに IPv6 アドレス範囲を入力します。
Action	• Permit- スイッチはアクセスプロファイルに一致するパケットの送信を、以下のフィールドで設定する追加のルールに従って行います。 • Deny- スイッチはアクセスプロファイルに一致するパケットを送信せずにフィルタリングします。 • Mirror- スイッチはアクセスプロファイルに一致するパケットをミラーポートセクションで定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。
Option	「Permit」アクション選択後、以下のオプションの 1 つを選択します。 • Change 1p Priority - 802.1p プライオリティ値を入力します。 • Replace DSCP - DSCP 値を入力します。 • Replace ToS Precedence - ToS 優先度値を入力します。
Apply To	このルールに適用するオブジェクトの選択または入力を行います。 • Ports - ポート番号またはポート範囲を入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

「Apply」ボタンをクリックして行った変更を適用します。

注意 スイッチはユーザが 入力するすべての項目をカバーするために最小限のマスクを使用しますが、余分なビットまで同時にマスクする可能性があります。ACL プロファイルとルールを最適化するためには、手動設定を行ってください。

Access Profile List（アクセスプロファイルリスト）

アクセスプロファイルを使用することにより、それぞれのパケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定することができます。スイッチは、4 つのプロファイルタイプ（イーサネット ACL、IPv4 ACL、IPv6 ACL およびパケットコンテンツ ACL）をサポートしています。

アクセスプロファイルの作成は 2 段階に分かれます。はじめにフレームのどの部分を調べるのか、送信元 MAC アドレスか、受信先 IP アドレスか、などを決定します。次に、そのフレームに対してどのような処理を行うのかという基準になる値を入力します。詳しくは以下で説明します。

スイッチに現在定義済みのアクセスプロファイルを表示できます。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。

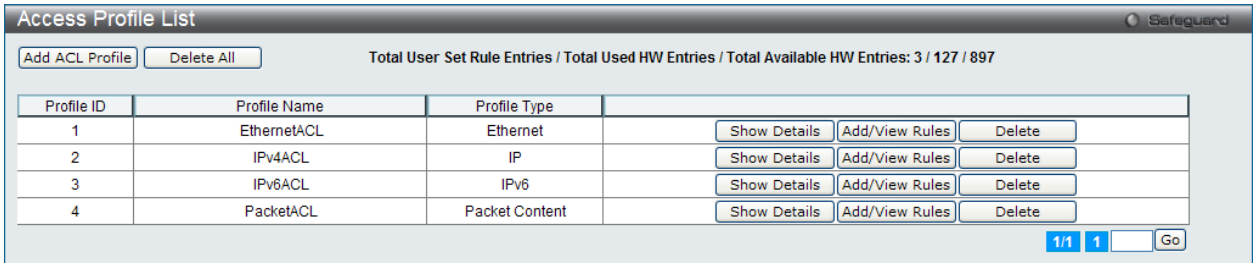


図 11-2　Access Profile List 画面

項目	説明
Add ACL Profile	アクセスプロファイルリストにエントリを追加します。
Delete All	テーブルからすべてのアクセスプロファイルを削除します。
Show Details	指定プロファイル ID エントリに関する情報を表示します。
Add/View Rules	指定プロファイル ID の ACL ルールの参照または追加を行います。
Delete	指定エントリを削除します。
Go	複数ページが存在する場合は、ページ番号を入力後、クリックして、特定のページへ移動します。

「Add Access Profile」画面には 4 種類あります。:

- イーサネット（MAC アドレスベース）プロファイル設定用
- IPv6 アドレスベースプロファイル設定用
- IPv4 アドレスベースプロファイル設定用
- パケットコンテンツマスクプロファイル設定用

アクセスプロファイルリストの作成（Ethernet）

イーサネット用のアクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。

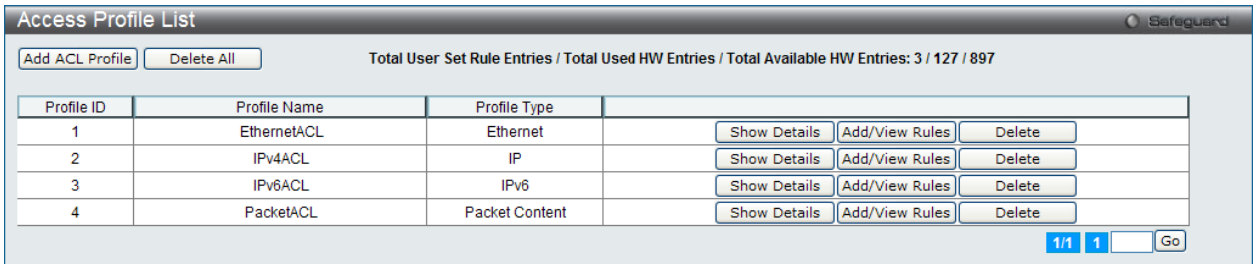


図 11-3　Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

イーサネットの「Add ACL Profile」画面

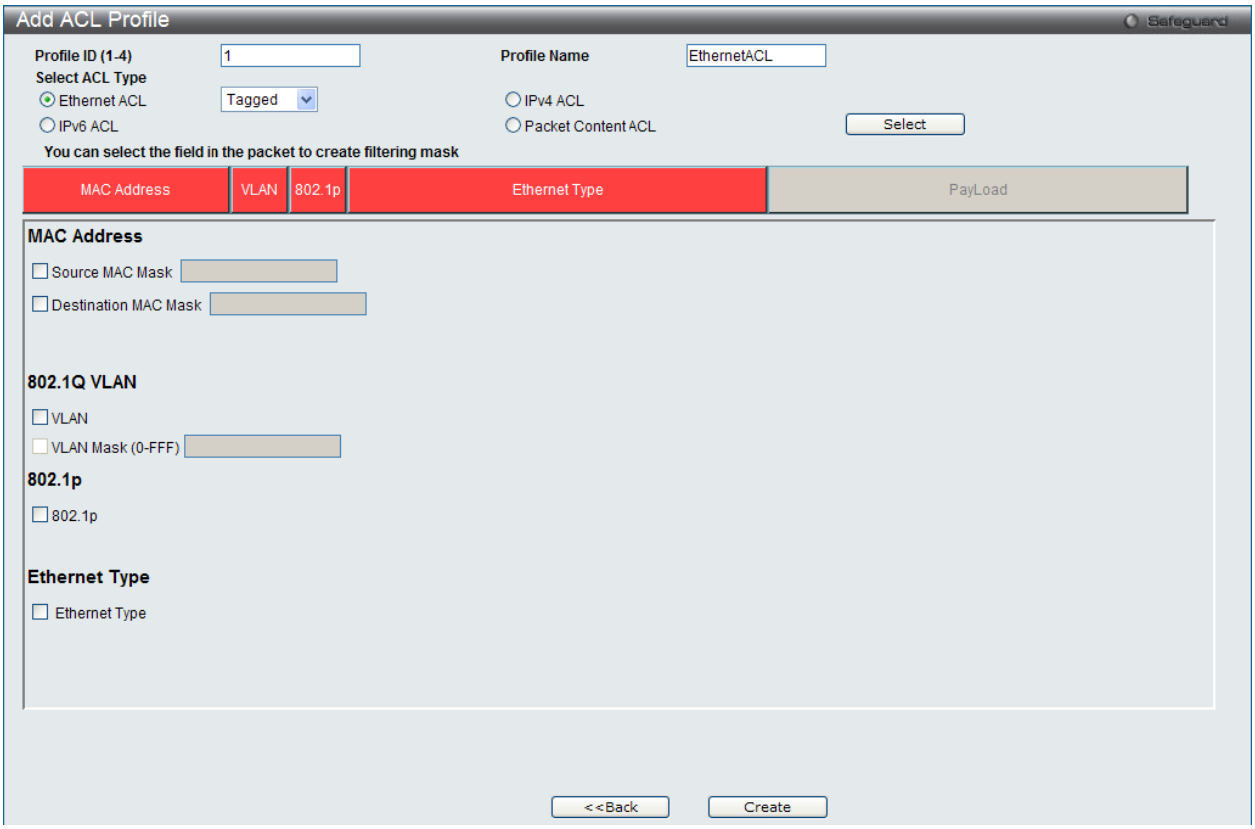


図 11-4　Add ACL Profile - Ethernet ACL 画面

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」で「Ethernet ACL」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を Ethernet ACL タイプに設定します。

項目	説明
Profile ID	プロファイル設定のための固有の識別番号を指定します。1 から 4 が指定できます。
Profile Name	作成したプロファイルにプロファイル名を入力します。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツからプロファイルのタイプを指定します。Type の変更に伴いメニューも変わります。ここでは、「Ethernet ACL」を選択します。 • Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
MAC Address	• Source MAC Mask - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。例 : FF-FF-FF-FF-FF-FF • Destination MAC Mask - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。例 : FF-FF-FF-FF-FF-FF
802.1Q VLAN	パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 • VLAN - VLAN マスクを指定します。 • VLAN Mask (0-FFF) - VLAN マスクを指定します。
802.1p	各パケットヘッダの 802.1p プライオリティを調べて、部分的または全体を転送基準として使用します。
Ethernet Type	フレームヘッダでイーサネットタイプの値を調べます。

「Create」ボタンをクリックし、プロファイルを作成します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

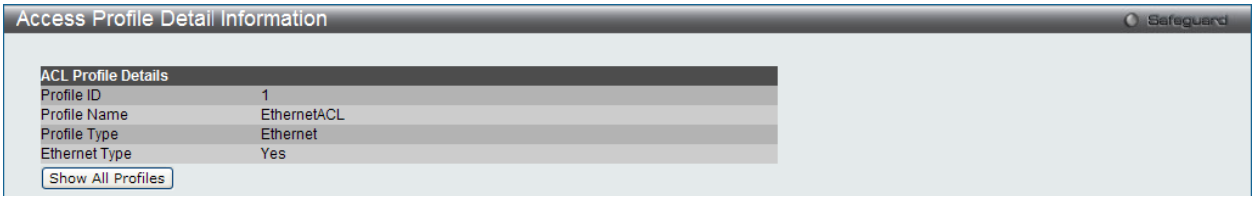


図 11-5　Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順（Ethernet）：

Ethernet アクセスルールの設定

1. 「Access Profile List」画面を表示します。

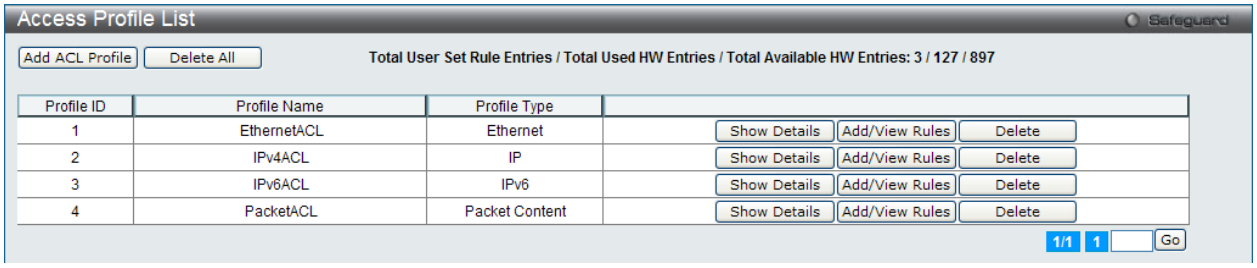


図 11-6　Access Profile List 画面

2. Ethernet エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

図 11-7　Access Rule List - Ethernet 画面

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。
「<<Back」をボタンをクリックし、前のページに戻ります。

作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

ルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

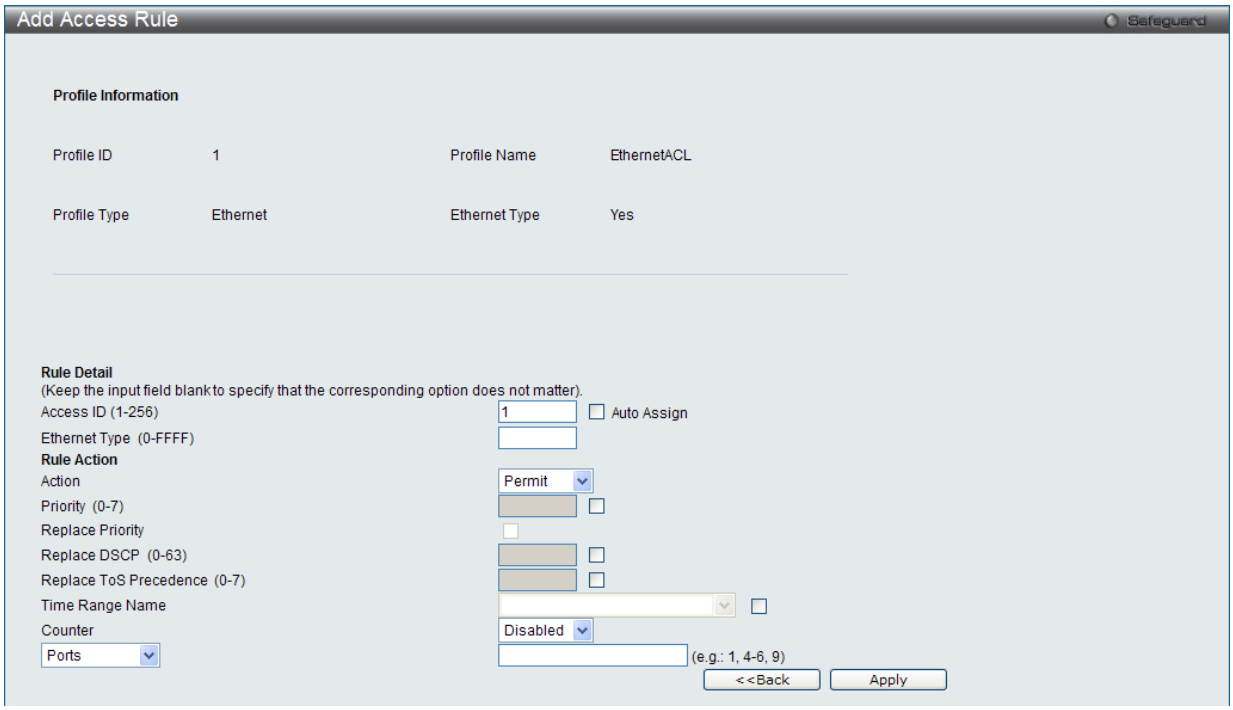


図 11-8　Add Access Rule - Ethernet 画面

Ethernet のアクセスルールを設定するためには以下の項目を設定して、「Apply」ボタンをクリックします。

項目	説明
Rule Detail	
Access ID (1-256)	プロファイル設定のための固有の識別番号を指定します。1 から 256 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
VLAN Name	設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準（または基準の一部）とします。
VLAN ID	VLAN ID 番号を指定します。
VLAN Mask	VLAN マスクを指定します。
Source MAC Address	送信元 MAC アドレスの MAC アドレスマスクを指定します。
Source MAC Address Mask	送信元 MAC アドレスの MAC アドレスマスクを 16 進数形式で指定します。
Destination MAC Address	送信先 MAC アドレスの MAC アドレスマスクを入力します。
Destination MAC Address Mask	送信先 MAC アドレスの MAC アドレスマスクを 16 進数形式で入力します。
802.1p (0-7)	802.1p プライオリティ値を 0-7 で入力します。アクセスプロファイルをこの値を持つパケットに適用します。
Ethernet Type (0-FFFF)	アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数（hex 0x0-0xffff）で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff（a-f の半角英文字、と 0-9999 の数字を使用します。）
Rule Action	
Action	• Permit - スイッチはアクセスプロファイルに一致するパケットの送信を、以下のフィールドで設定する追加のルールに従って行います。 • Deny - スイッチはアクセスプロファイルに一致するパケットを送信せずにフィルタリングします。 • Mirror - スイッチはアクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。
Priority (0-7)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの「第 10 章　QoS（QoS 機能の設定）」（158 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側のフィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Counter	「Counter」機能を「Enabled」（有効）/「Disabled」（無効）にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。
Ports / VLAN Name / VLAN ID	このルールに適用するオブジェクトの選択または入力を行います。 • Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

「Apply」ボタンをクリックして行った変更を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

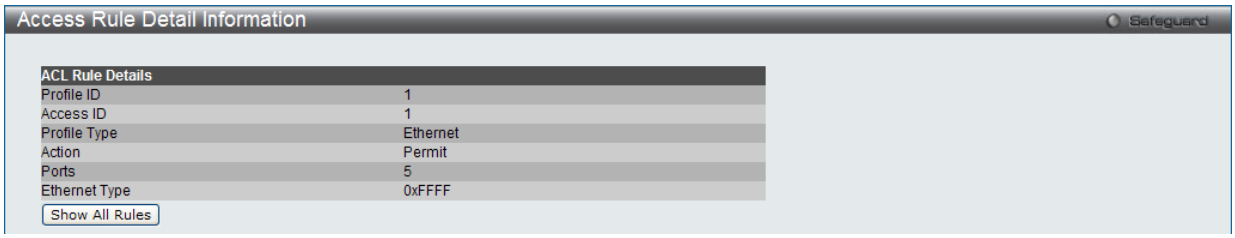


図 11-9　Access Rule Detail Information - Ethernet 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成（IPv4）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。1 つのアクセスプロファイルが説明のために作成されています。

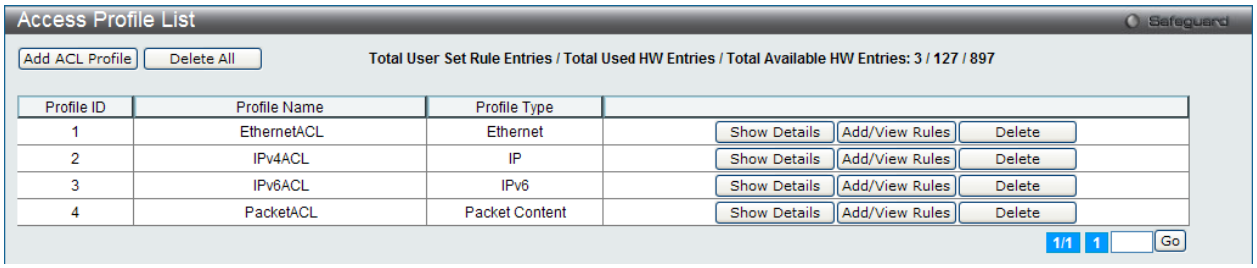


図 11-10　Access Profile List 画面

エントリの削除

エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv4 の「Add ACL Profile」画面

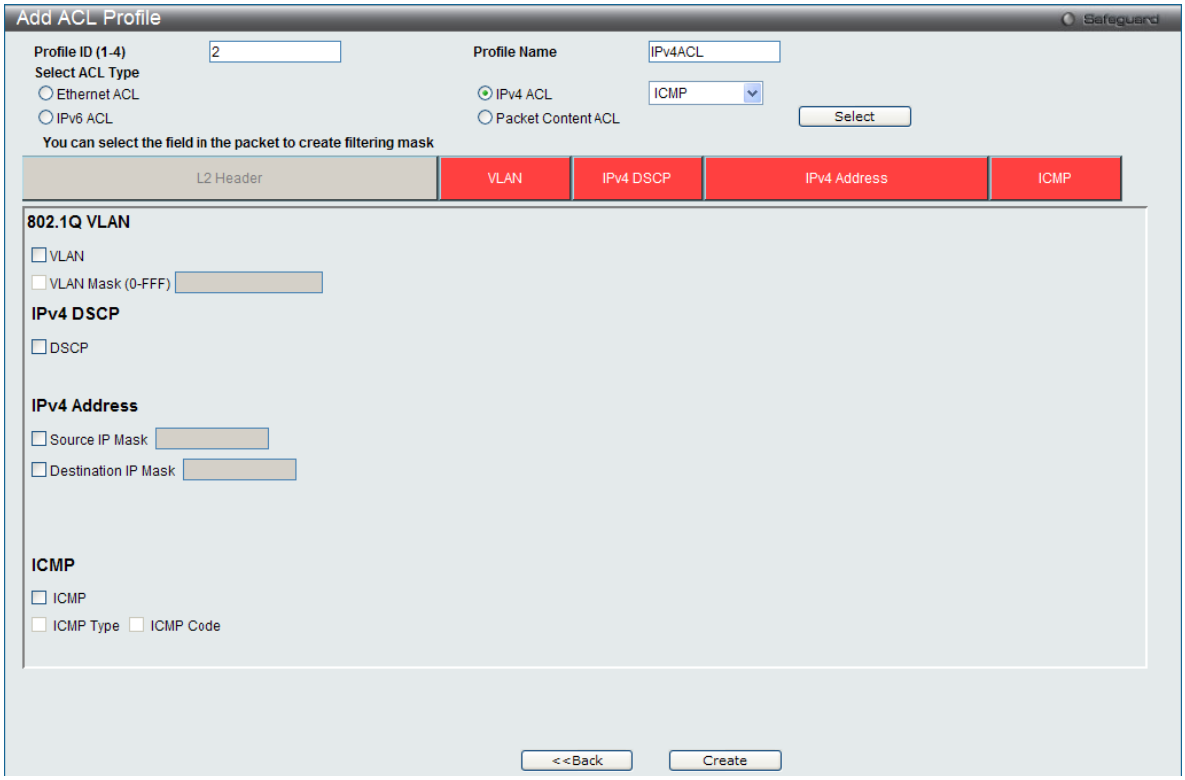


図 11-11　Add ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」で「IPv4 ACL」をチェック後、隣接する欄で設定するフレームヘッダ（ICMP、IGMP、TCP、UDP、Protocol ID）選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を IPv4 ACL タイプに設定します。

項目	説明
Profile ID	プロファイル設定のための固有の識別番号を指定します。1 から 4 が指定できます。
Profile Name	作成したプロファイルにプロファイル名を入力します。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4 ACL」を選択します。 • IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
802.1Q VLAN	パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 • VLAN - VLAN マスクを指定します。 • VLAN Mask (0-FFF) - VLAN マスクを指定します。
IPv4 DSCP	各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。
IPv4 Address	• Source IP Mask - 送信元 IP アドレスをマスクする IP アドレスを指定します。 • Destination IP Mask - 送信先 IP アドレスをマスクする IP アドレスを指定します。
ICMP	各パケットのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。 • ICMP Type - アクセスプロファイルを ICMP Type 値に適用します。 • ICMP Code - アクセスプロファイルを ICMP Code に適用します。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）または Check All（すべて）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク（source port mask）と（もしくは）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。例：255.255.255.255 - Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。例：255.255.255.255
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask（0-FF）を指定します。「User Define」マスクは 16 進数（0-FFFFFFFF）で指定します。

「Create」ボタンをクリックし、設定を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照するには、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

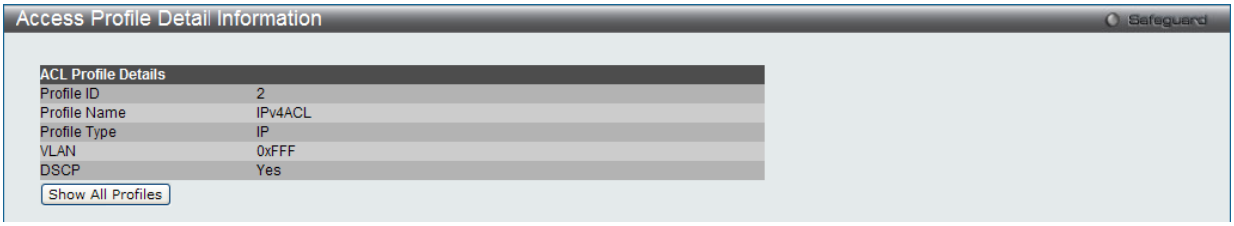


図 11-12　Access Profile Detail Information - IPv4 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順（IPv4）：

IPv4 アクセスルールの設定

1. 「Access Profile List」画面を表示します。

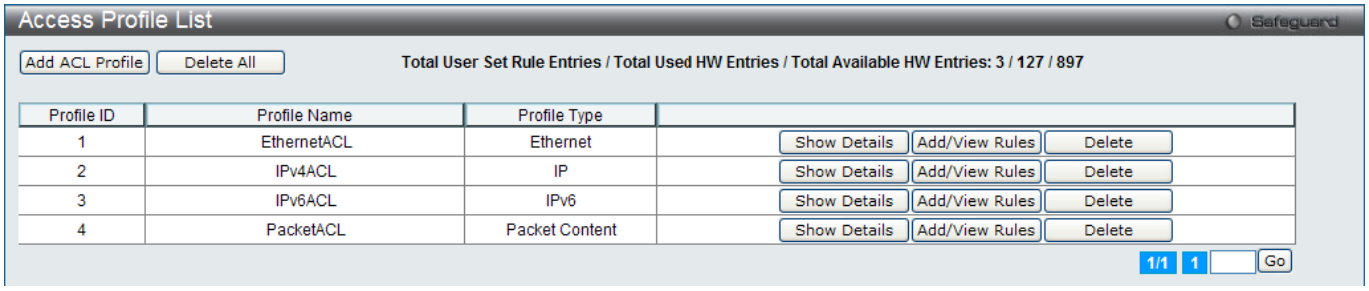


図 11-13　Access Profile List 画面

2. IPv4 エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

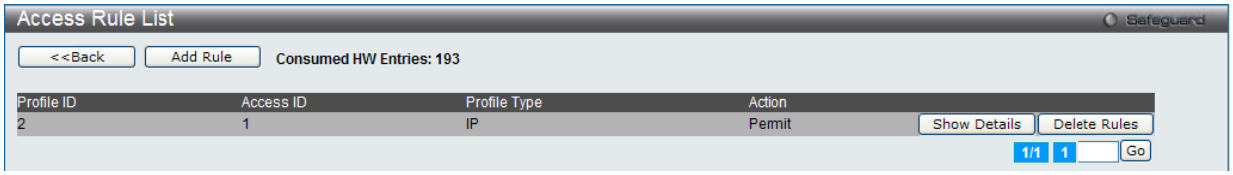


図 11-14　Access Rule List - IPv4 画面

「<<Back」をボタンをクリックして前のページに戻ります。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

新しいルールを作成するには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

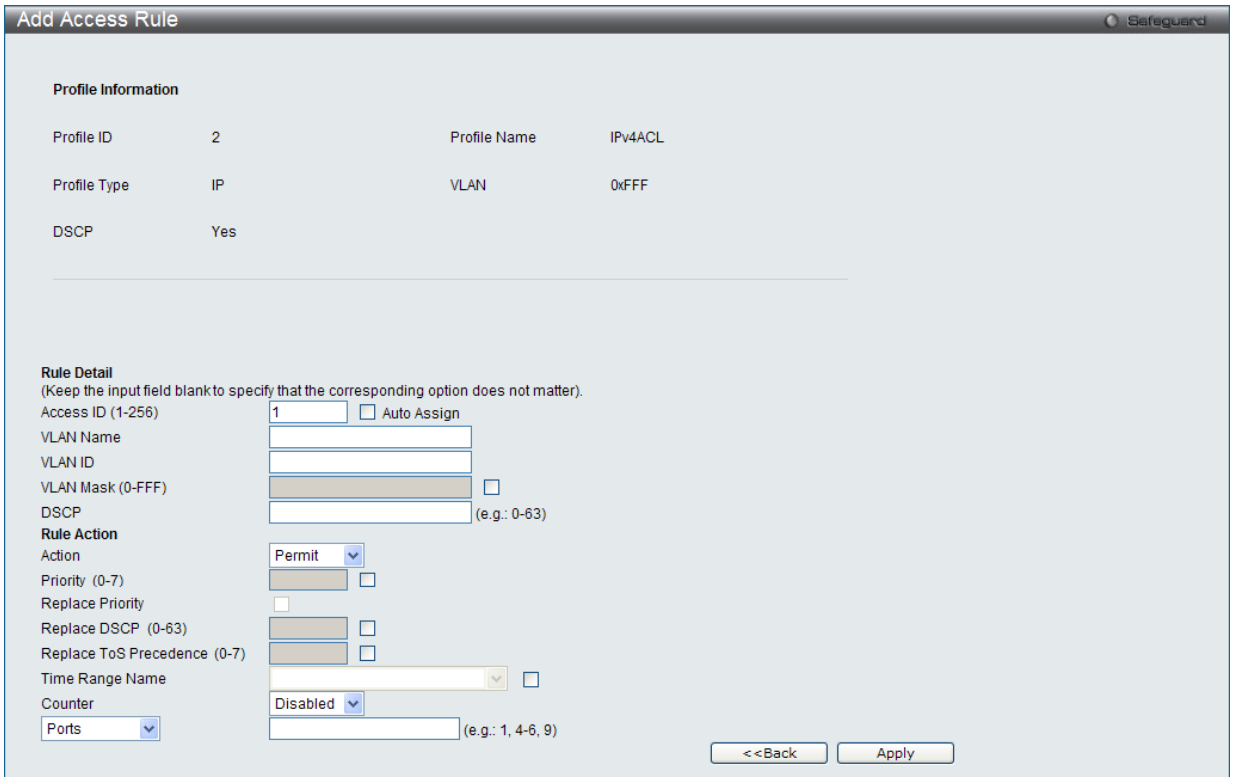


図 11-15　Add Access Rule - IPv4 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-256)	プロファイル設定のための固有の識別番号を指定します。1 から 256 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
VLAN Name	設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。
VLAN ID	VLAN ID を入力します。「Mask」（0-FFF）にマスク値を入力します。
VLAN Mask	VLAN マスクを指定します。
Source IP Address	送信元の IP アドレスの IP アドレスを入力します。
Source IP Address Mask	送信元の IP アドレスの IP アドレスマスクを入力します。
Destination IP Address	宛先 IP アドレスの IP アドレスを入力します。
Destination IP Address Mask	送信先 IP アドレスの IP アドレスマスクを入力します。
DSCP	DSCP 値（0-63）を指定すると各パケットヘッダの DiffServ コードを調べて、部分的または全体を転送基準として使用します。
ICMP	各パケットのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。 • Type - アクセスプロファイルを ICMP Type 値に適用します。 • Code - アクセスプロファイルを ICMP Code に適用します。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - TCP Source Port (0-65535) - フィルタリングしたい送信元ポートを指定します。 - TCP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 - TCP Destination Port (0-65535) - フィルタリングしたい送信先ポートを指定します。 - TCP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。 - Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - UDP Source Port (0-65535) - フィルタリングしたい送信元ポートを指定します。 - UDP Source Port Mask 0-FFFF) - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - UDP Destination Port (0-65535) - フィルタリングしたい送信先ポートを指定します。 - UDP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。0-255 の値を入力します。
User	マスクしたいパケットヘッダの Protocol ID Mask を 16 進数（0-FFFFFFFF）で指定します。
User Mask (0-FFFFFFFF)	マスクしたいパケットヘッダの Protocol ID Mask を 16 進数（0-FFFFFFFF）で指定します。
Rule Action	
Action	• Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。
Priority (0-7)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの「第 10 章　QoS（QoS 機能の設定）」（158 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	スイッチはここで指定した基準に一致するパケットの DSCP をボックスの右側の欄内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するのに追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方を変更するように設定している場合は、現在のプライオリティを変更します。

項目	説明
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Counter	「Counter」機能を「Enabled」（有効）/「Disabled」（無効）にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。
Ports / VLAN Name / VLAN ID	このルールに適用するオブジェクトの選択または入力を行います。 • Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

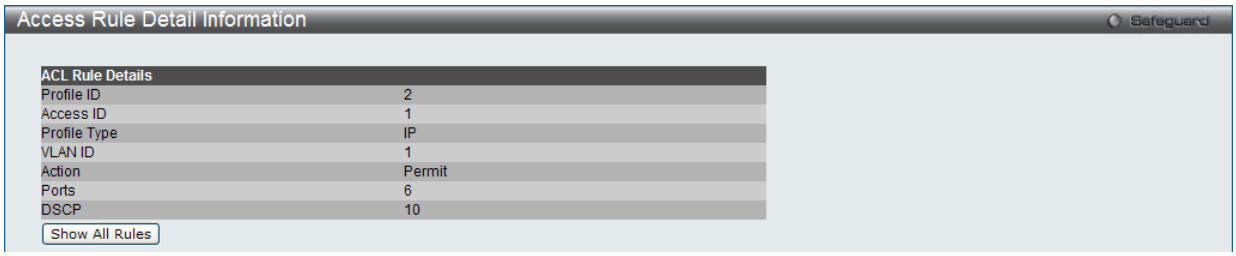


図 11-16　Access Rule Detail Information - IP 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成（IPv6）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。１つのアクセスプロファイルが説明のために作成されています。

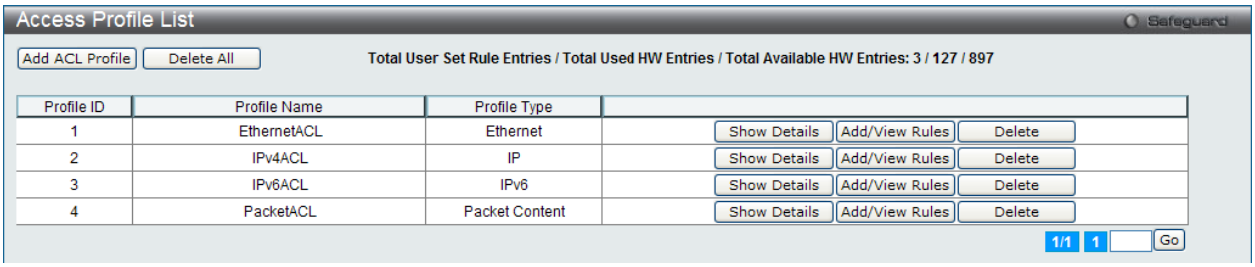


図 11-17　Access Profile List 画面

エントリの削除

エントリの削除は、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルの削除は、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」で「IPv6 ACL」ボタンをチェック後、隣接する欄で設定するフレームヘッダ（TCP または UDP）選択して「Select」ボタンをクリックします。

IPv6 の「Add ACL Profile」画面

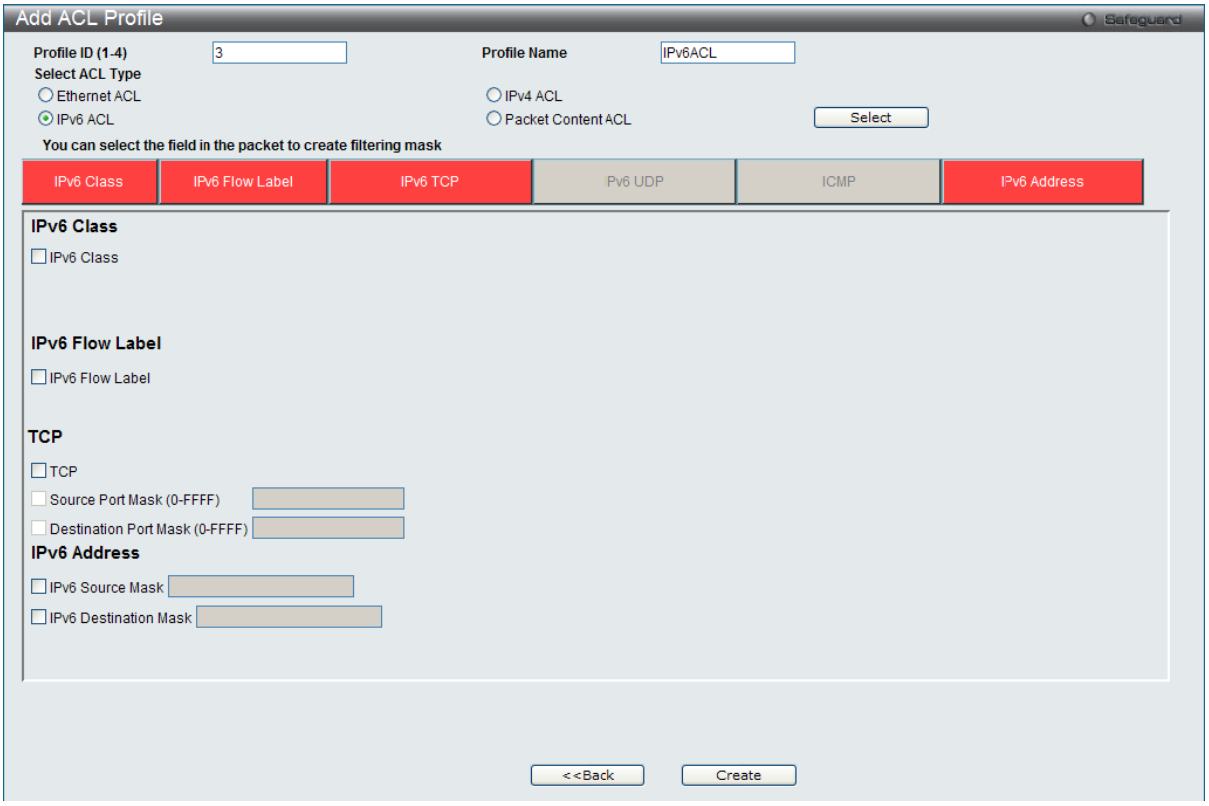


図 11-18　Add ACL Profile - IPv6 ACL 画面

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を IPv6 ACL タイプに設定します。

項目	説明
Profile ID	プロファイル設定のための固有の識別番号を指定します。1 から 4 を指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv6 ACL」を選択します。 • IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
IPv6 Class	この項目を選ぶと IPv6 ヘッダの「Class」を調べます。「Class」は IPv4 における「Type of Service」（ToS）、「Precedence bits」のようなパケットヘッダの一部です。
IPv6 Flow Label	この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 TCP	• TCP - TCP トラフィックに適用するルールを指定します。 • Source Port Mask (0-FFFF) - TCP 送信元ポートマスクを指定します。 • Destination Port Mask (0-FFFF) - TCP 宛先ポートマスクを指定します。
IPv6 UDP	UDP - ルールを UDP トラフィックに適用するように指定します。 • Source Port Mask (0-FFFF) - UDP 送信元ポートマスクを指定します。 • Destination Port Mask (0-FFFF) - UDP 宛先ポートマスクを指定します。
ICMP	各パケットのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。 • ICMP Type - アクセスプロファイルを ICMP Type 値に適用します。 • ICMP Code - アクセスプロファイルを ICMP Code に適用します。
IPv6 Address	• IPv6 Source Address - 対応するボックスをチェックして、送信元 IPv6 アドレスをマスクする IP アドレスを指定します。 • IPv6 Destination Address - 対応するボックスをチェックして、送信先 IPv6 アドレスをマスクする IP アドレスを指定します。

「Create」ボタンをクリックし、設定を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照する場合は、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

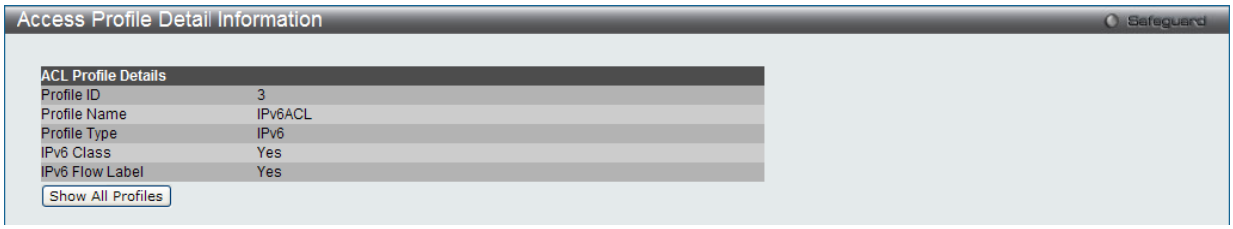


図 11-19 Access Profile Detail Information - IPv6 ACL 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順（IPv6）：

IPv6 アクセスルールの設定

1. 「Access Profile List」画面を表示します。

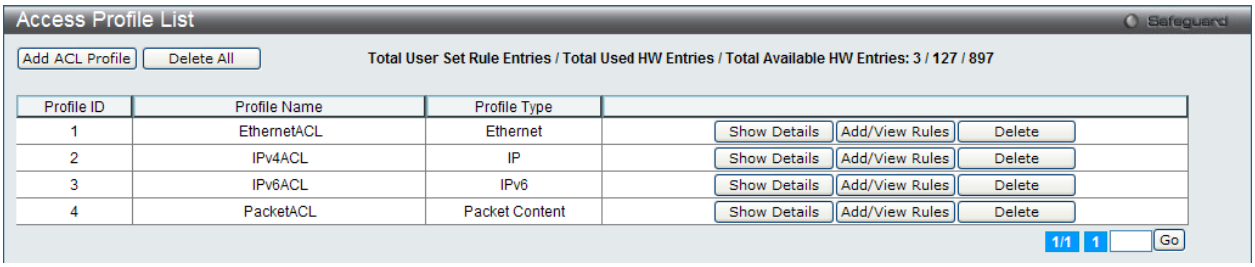


図 11-20　Access Profile List 画面

2. IPv6 エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

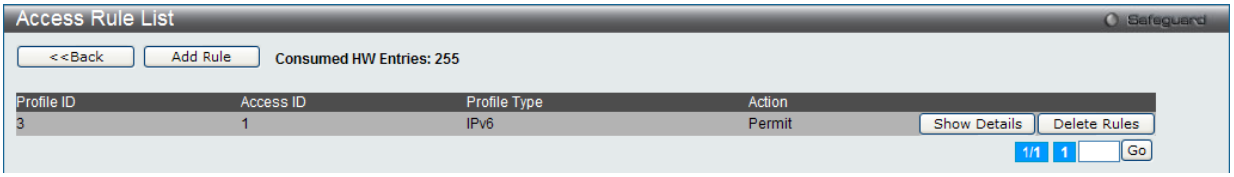


図 11-21　Access Rule List - IPv6 画面

「<<Back」をボタンをクリックして前のページに戻ります。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

作成済みのルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

新しいルールを作成するためには、「Add Rule」ボタンをクリックします。

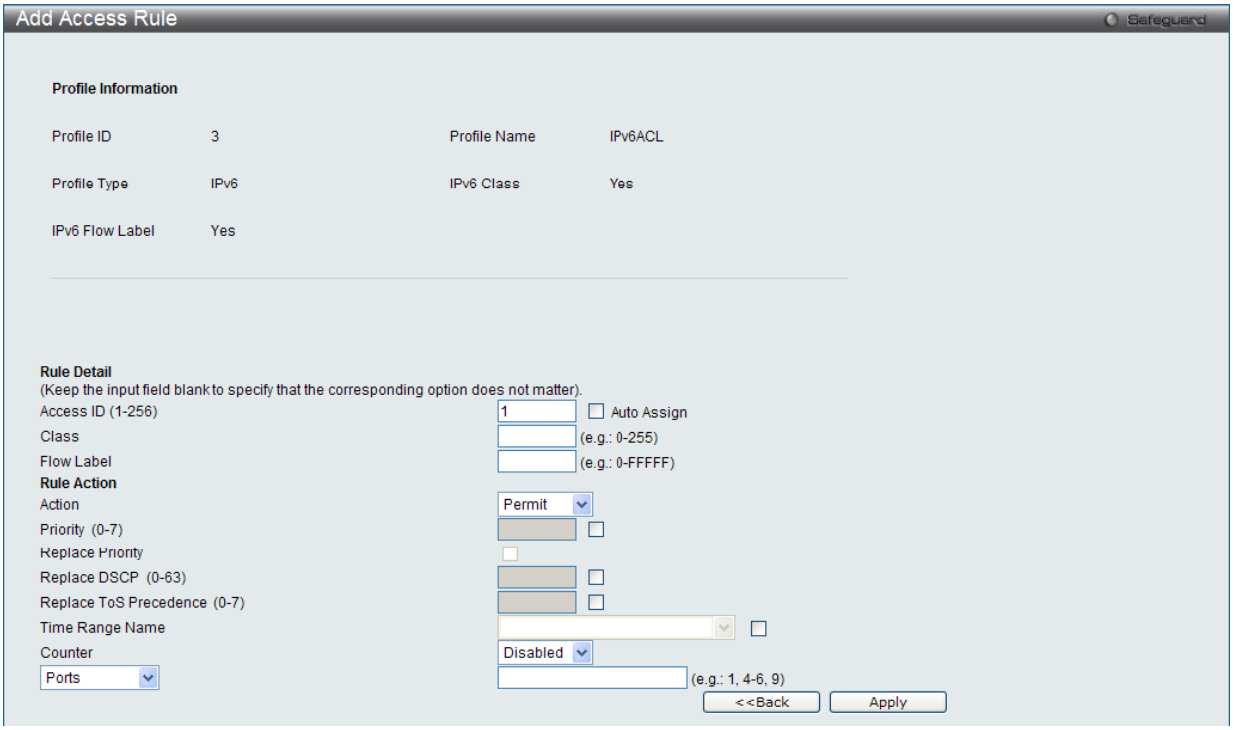


図 11-22　Add Access Rule - IPv6 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-256)	プロファイル設定のための固有の識別番号を指定します。1 から 256 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Class	IPv6 クラスのマスク値を入力します。
Flow Label	16 進数で指定して IPv6 ヘッダの「Flow Label」フィールドを調べます。本フィールドは送信元で順番につけられる QoS やリアルタイムサービスパケットのためのフィールドです。
IPv6 Source Address	IPv6 送信元アドレスの IPv6 アドレスを入力します。
IPv6 Source Address Mask	IPv6 送信元サブマスクを指定します。送信元 IPv6 アドレスの最後の 44 ビット (LSB) のフィルタリングのみを行います。
IPv6 Destination Address	送信先 IPv6 アドレスの IP アドレスを入力します。
IPv6 Destination Address Mask	送信先 IPv6 アドレスの IP アドレスマスクを入力します。
TCP	• TCP Source Port (0-65535) - IPv6 L4 TCP 送信元ポートサブマスクを指定します。 • TCP Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 • TCP Destination Port (0-65535) - IPv6 L4 TCP 送信先ポートサブマスクを指定します。 • TCP Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。
UDP	• UDP Source Port (0-65535) - IPv6 L4 UDP 送信元ポートサブマスクを指定します。 • UDP Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数で指定します。 • UDP Destination Port (0-65535) - IPv6 L4 UDP 送信先ポートサブマスクを指定します。 • UDP Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数で指定します。
ICMP	各パケットのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。 • Type - アクセスプロファイルを ICMP Type 値に適用します。 • Code - アクセスプロファイルを ICMP Code に適用します。
Rule Action	
Action	• Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。
Priority (0-7)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの「第 10 章　QoS（QoS 機能の設定）」（158 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側のフィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Counter	「Counter」機能を「Enabled」（有効）/「Disabled」（無効）にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。
Ports / VLAN Name / VLAN ID	このルールに適用するオブジェクトの選択または入力を行います。 • Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

IPv6 のアクセスルールを設定するためには、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

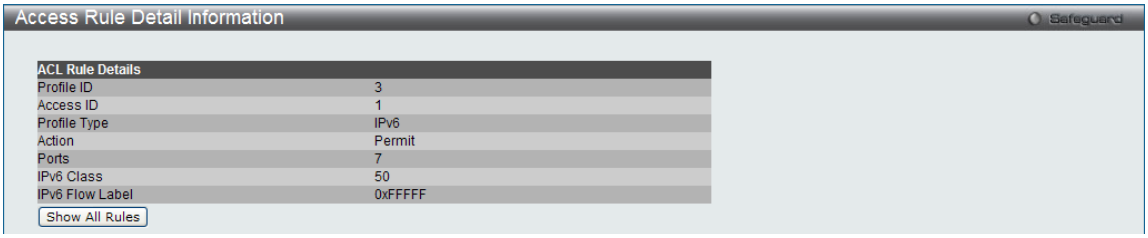


図 11-23　Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成（パケットコンテンツ）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。 1 つのアクセスプロファイルが説明のために作成されています。

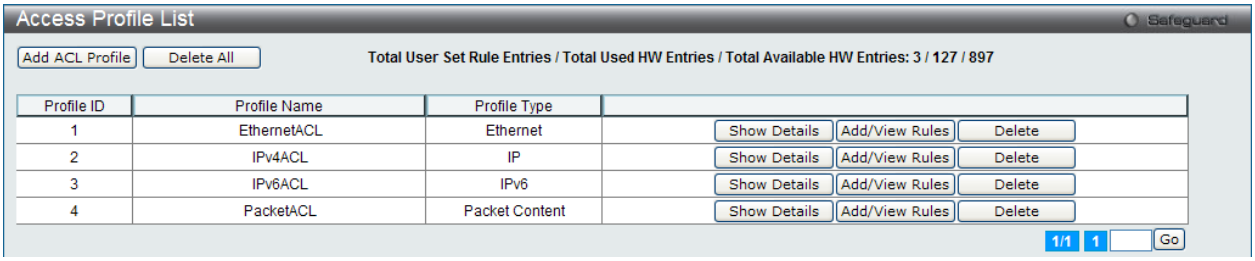


図 11-24　Access Profile List 画面

エントリの削除

エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

パケットコンテンツの「Add ACL Profile」画面

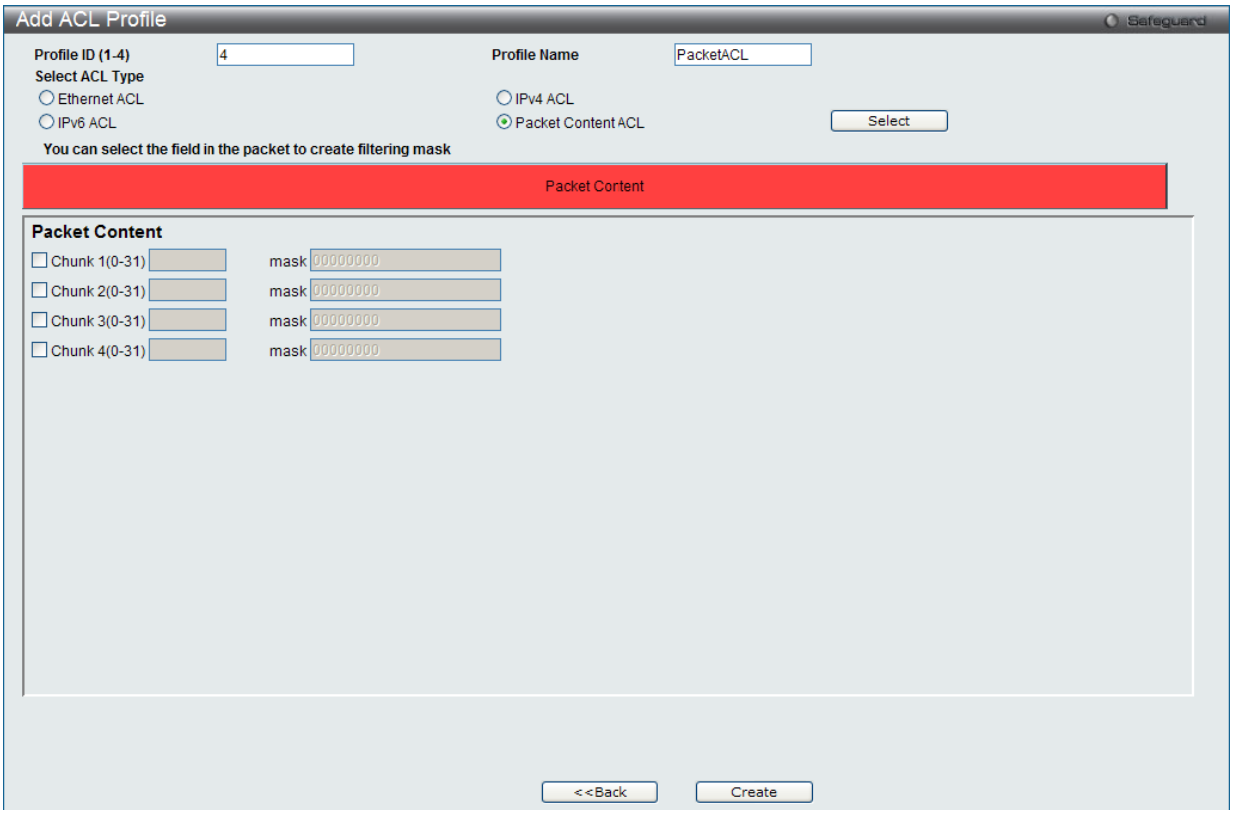


図 11-25　Add ACL Profile 画面 - パケットコンテンツ

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」で「Packet Content ACL」をチェック後、「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目をパケットコンテンツタイプに設定します。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>Profile ID</td><td>プロファイル設定のための固有の識別番号を指定します。1 から 4 を指定できます。</td></tr>
<tr><td>Select ACL Type</td><td>Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv6 ACL」を選択します。
• Packet Content - フレームヘッダのパケットコンテンツを検証します。</td></tr>
<tr><td>Packet Content</td><td>パケットコンテンツは、同時にパケット内の 4 個のオフセットチャンクと、そのフレームコンテンツとオフセットを検証できます。設定可能な 4 個のチャンクオフセットとマスクがあります。チャンクマスクは 4 バイトを示します。

以下で説明するように、32 個の定義済みオフセットチャンクから 4 つのオフセットチャンクを選択することができます。
offset_chunk_1、offset_chunk_2、offset_chunk_3、offset_chunk_4
<table>
<tr><td>chunk0</td><td>chunk1</td><td>chunk2</td><td>……</td><td>chunk29</td><td>chunk30</td><td>chunk31</td></tr>
<tr><td>B126, B127,
B0, B1</td><td>B2, B3,
B4, B5</td><td>B6, B7,
B8, B9</td><td>……</td><td>B114, B115,
B116, B117</td><td>B118, B119,
B120, B121</td><td>B122, B123,
B124, B125</td></tr>
</table>
例題：
offset_chunk_1 0 0xffffffff はパケットバイトオフセット 126,127,0,0,1 に一致します。
offset_chunk_1 0 0x0000ffff はパケットバイトオフセット 0,1 に一致します。

注意 一度に、1 個のパケットコンテンツマスクプロファイルしか作成できません。</td></tr>
</table>

「Select」ボタンをクリックし、ACL タイプを選択します。
「Create」ボタンをクリックし、プロファイルを追加します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

作成したプロファイル設定を参照するためには、「Access Profile List」画面の対応する「Show Details」ボタンをクリックし、以下の画面を表示します。

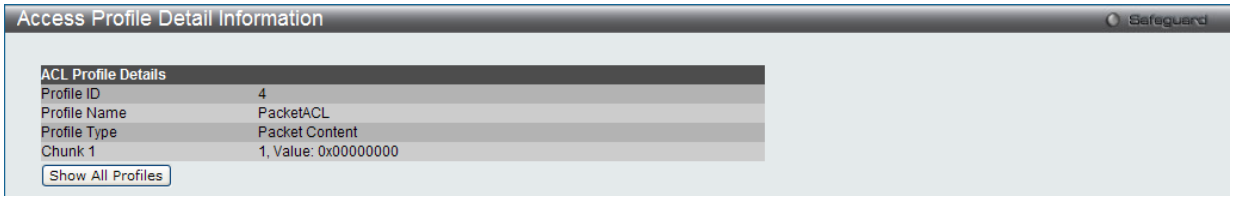


図 11-26 Access Profile Detail Information 画面 - パケットコンテンツ

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順（パケットコンテンツ）：

パケットコンテンツアクセスルールの設定

1. 「Access Profile List」画面を表示します。

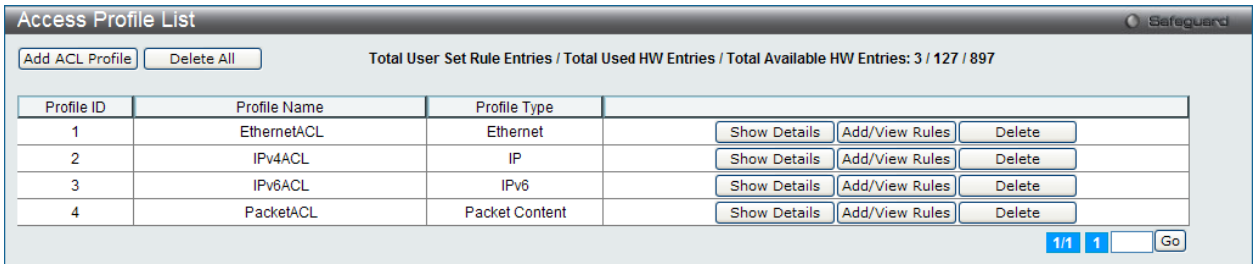


図 11-27 Access Profile List 画面

2. パケットコンテンツエントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

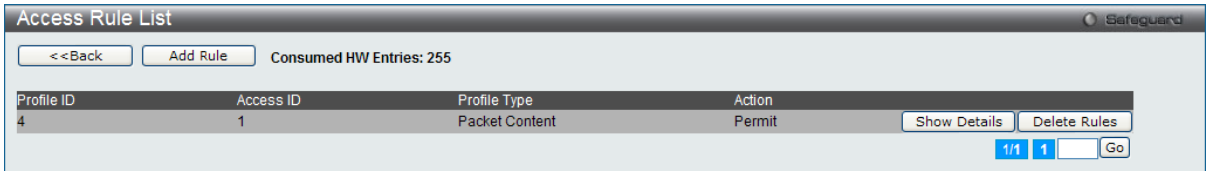


図 11-28 Access Rule List 画面 - パケットコンテンツ

「<<Back」をボタンをクリックして前のページに戻ります。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

既に作成したルールの削除
該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成
新しいルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

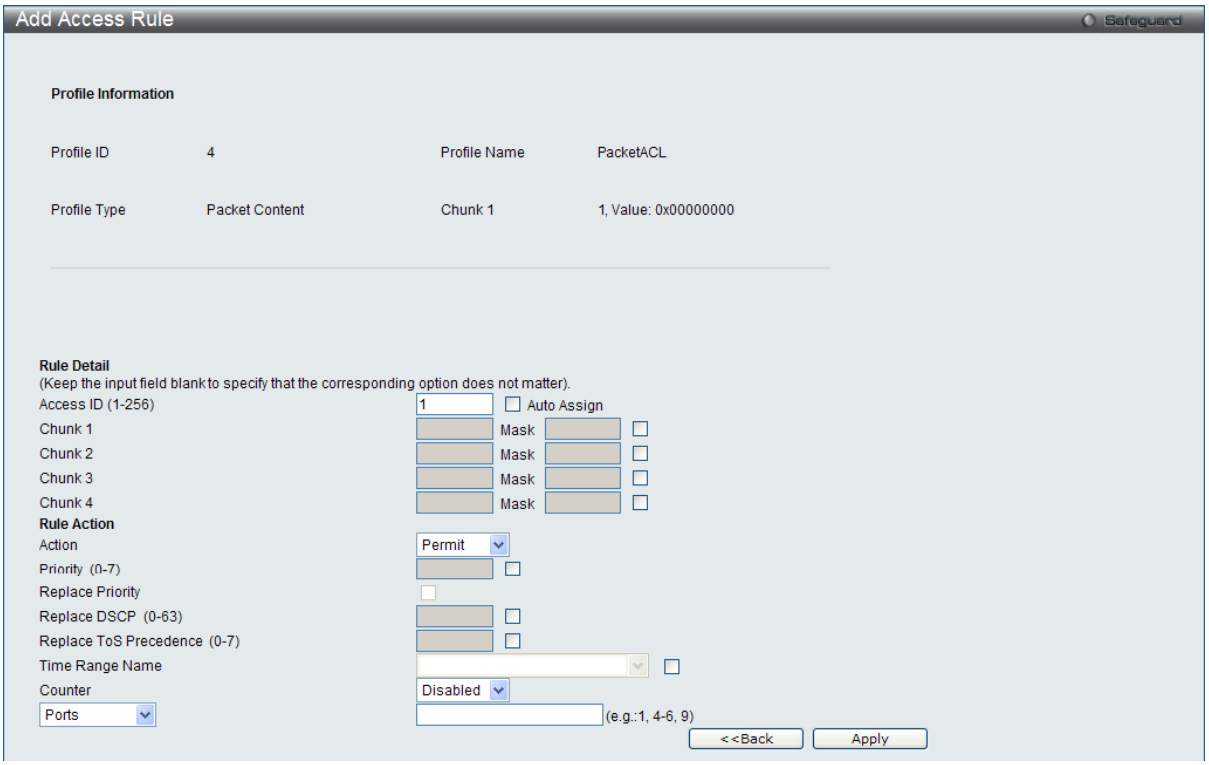


図 11-29 Add Access Rule 画面 - パケットコンテンツ

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-256)	プロファイル設定のための固有の識別番号を指定します。1 から 256 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Chunk (1-4)	プロファイルで定義された各 UDF データフィールドと照合するデータを入力します。 • Mask - 使用されるオフセットマスク値を入力します。
Rule Action	
Action	• Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。
Priority (0-7)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの「第 10 章　QoS（QoS 機能の設定）」（158 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側のフィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。

項目	説明
Counter	「Counter」機能を「Enabled」（有効）/「Disabled」（無効）にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。
Ports / VLAN Name / VLAN ID	このルールに適用するオブジェクトの選択または入力を行います。 • Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

パケットコンテンツマスクのアクセスルールを設定するためには、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

図 11-30　Access Rule Detail Information - パケットコンテンツ画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

CPU Access Profile List（CPU アクセスプロファイルリスト）

チップセットの制限やスイッチのセキュリティの必要性などから、本スイッチは、CPU インタフェースフィルタリング機能を持っています。この追加機能によって CPU インタフェース向けのパケットアクセスルールリストの作成が可能になり、動作時のセキュリティが高くなります。既に説明したアクセスプロファイル機能と似た方法で CPU インタフェースフィルタリングは CPU に到達するイーサネット、IPv4、IPv6 およびパケットコンテンツマスクのパケットヘッダを調べて、ユーザ設定に基づきそれらを転送もしくはフィルタリングします。そして CPU フィルタリングの追加機能として、CPU フィルタリングでは多彩なルールのリストをあらかじめ用意しておき、必要に応じてグローバルに有効 / 無効を設定することができます。

注意 CPU インタフェースフィルタリングは、プロトコル変換または管理アクセスなど直接スイッチへのトラフィックアクセスを制御するのに使用されます。CPU インタフェースフィルタリングルールは正常な L2/3 トラフィックの送信には影響ありません。しかし、不適当な CPU インタフェースフィルタリングルールによって、ネットワークは不安定になる可能性があります。

CPU 用のアクセスプロファイルの作成は 2 段階に分かれます。はじめにフレームのどの部分を調べるのか、送信元 MAC アドレスか、送信先 IP アドレスか、などを決定します。次に、そのフレームに対してどのような処理を行うのかという基準になる値を入力します。詳しくは以下で 2 つに分けて説明します。

動作状態を変更するためには、ラジオボタンを使用して、CPU インタフェースフィルタリング機能をグローバルに「Enabled」(有効) または「Disabled」(無効) にします。
「Enabled」を選択するとスイッチは CPU パケットを詳しく調べます。「Disabled」にするとこの動作は行われません。

ACL > CPU Access Profile List の順にメニューをクリックし、以下の画面を表示します。

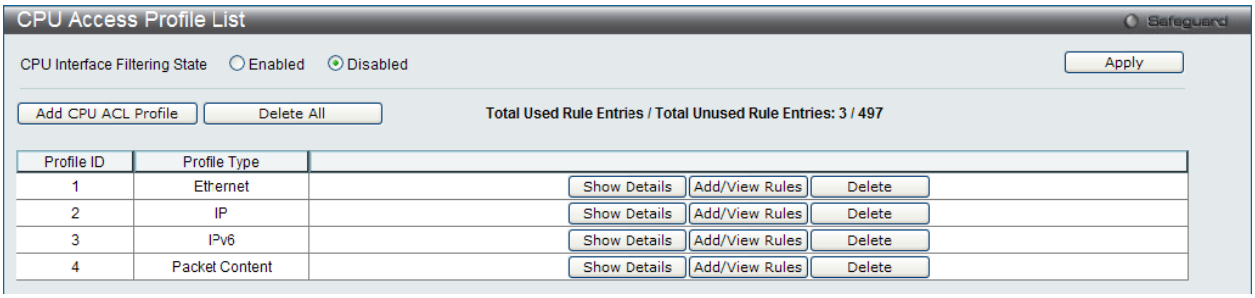


図 11-31　CPU Access Profile List 画面

項目	説明
CPU Interface Filtering State	CPU インタフェースフィルタリング状態を有効または無効にします。「Apply」ボタンをクリックして行った変更を適用します。
Add CPU ACL Profile	CPU ACL リストにエントリを追加します。
Delete All	テーブルからすべてのアクセスプロファイルを削除します。
Show Details	指定プロファイル ID エントリに関する情報を表示します。
Add/View Rules	指定プロファイル ID 内の CPU ACL ルールの参照または追加を行います。
Delete	指定エントリを削除します。

「Add CPU ACL Profile」画面には 4 種類あります。:

- イーサネット（MAC アドレスベース）プロファイル設定用
- IPv6 アドレスベースプロファイル設定用
- IPv4 アドレスベースプロファイル設定用
- パケットコンテンツマスクプロファイル設定用

CPU アクセスプロファイルの作成（Ethernet）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、「CPU Interface Filtering State」をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

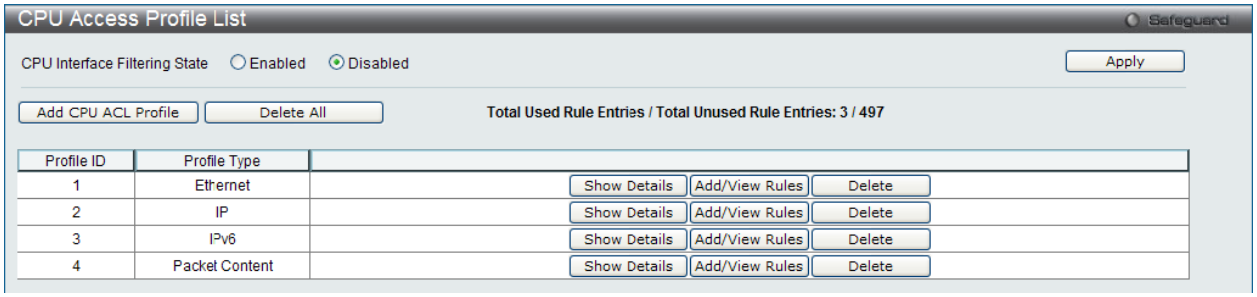


図 11-32 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。各タイプに 1 つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

イーサネットの「Add CPU ACL Profile」画面

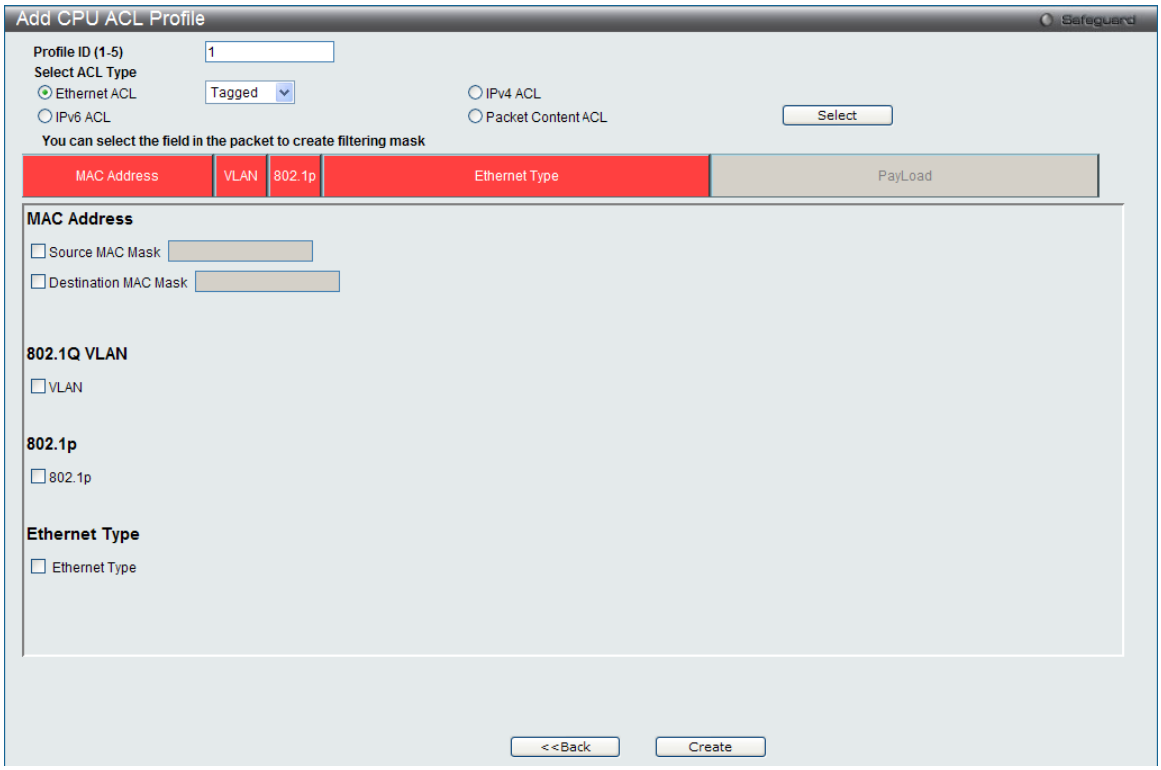


図 11-33 Add CPU ACL Profile - Ethernet 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「Ether ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を設定します。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Ethernet」を選択します。 • Ethernet - パケットヘッダのレイヤ 2 部分を対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
MAC Address	• Source MAC Mask - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。 • Destination MAC Mask - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。
802.1Q VLAN	パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 • VLAN Mask (0-FFF) - VLAN マスクを指定します。
802.1p	アクセスルールを設定する 802.1p プライオリティ値を指定できるようになります。
Ethernet Type	各フレームヘッダの Ethernet Type 値を調べます。

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

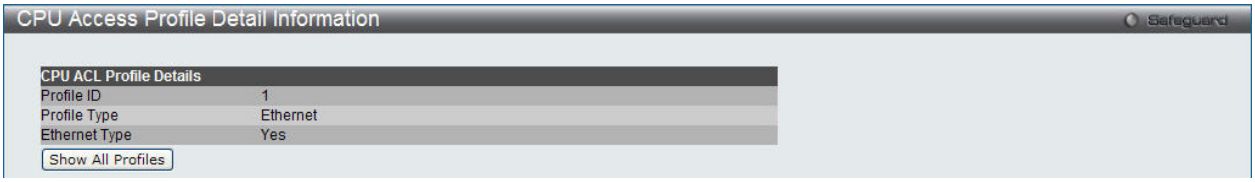


図 11-34 CPU Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（Ethernet）

Ethernet アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

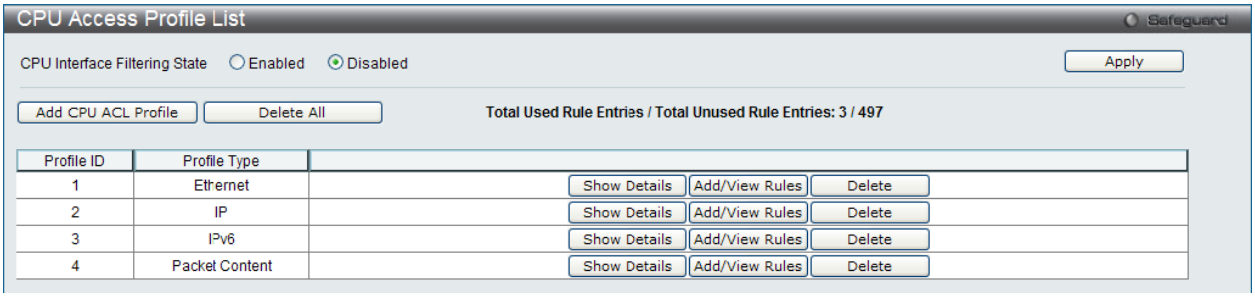


図 11-35 CPU Access Profile List 画面

2. イーサネットエントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

図 11-36 CPU Access Rule List - Ethernet 画面

「Show Details」ボタンをクリックし、作成した指定ルールに関する詳しい情報を表示します。
「Delete Rules」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

新しいルールの作成

「Add Rule」ボタンをクリックし、以下の画面を表示します。

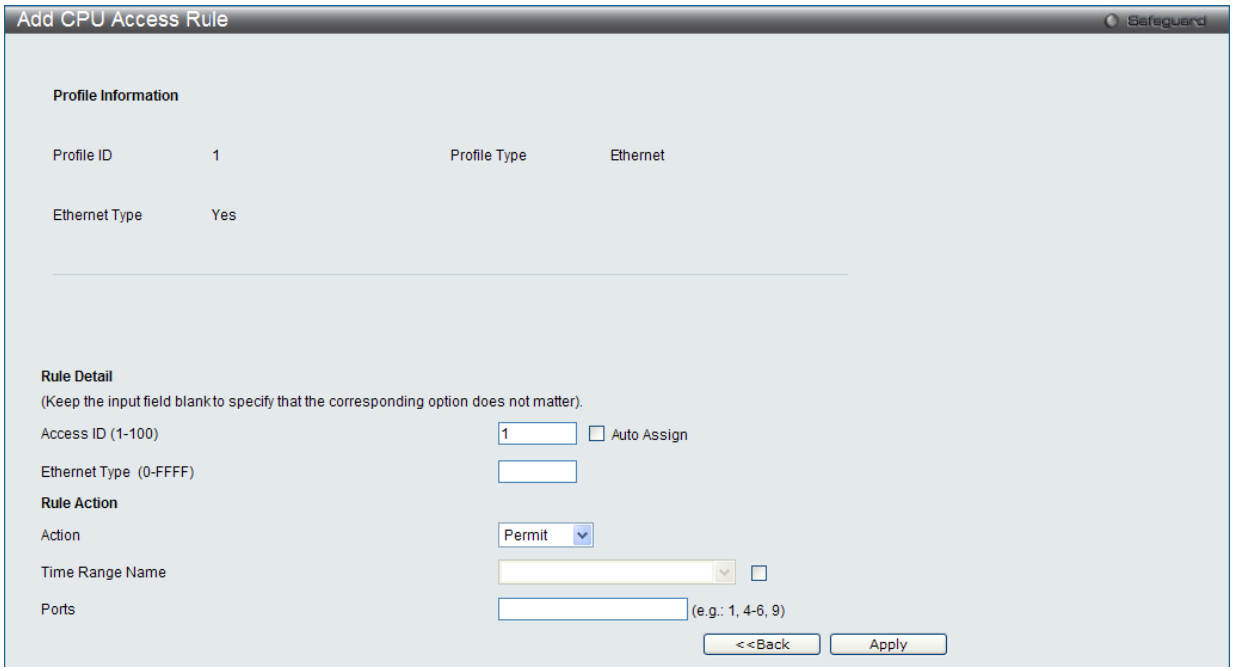


図 11-37 Add Access Rule - Ethernet 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。
VLAN Name	設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準（または基準の一部）とします。
VLAN ID	設定済みの VLAN ID を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準（または基準の一部）とします。
Source MAC Address	送信元 MAC アドレスの MAC アドレスマスクを指定します。
Destination MAC Address	送信先 MAC アドレスの MAC アドレスマスクを入力します。
802.1p (0-7)	アクセスプロファイルは、ここで指定する 802.1p プライオリティ値 (0-7) を持つパケットにのみ適用されます。
Ethernet Type (0-FFFF)	アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数（hex 0x0-0xffff）で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff（a-f の半角英文字、と 0-9999 の数字を使用します。）
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - Deny- スイッチはアクセスプロファイルに一致するパケットを送信せずにフィルタリングします。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Ports	設定するポート範囲を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

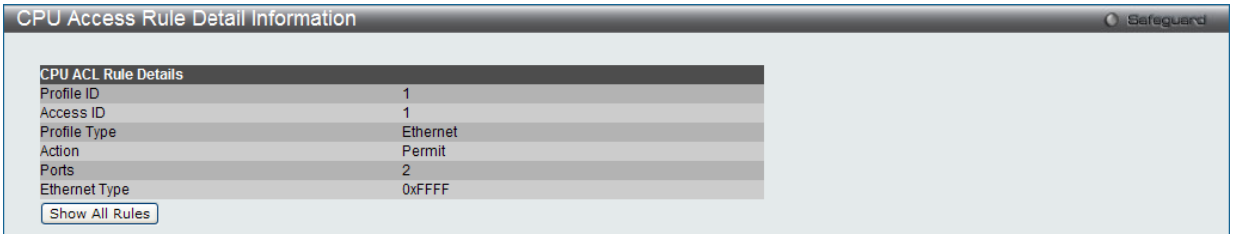


図 11-38 CPU Access Rule Detail Information - Ethernet 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセスプロファイルの作成（IPv4）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

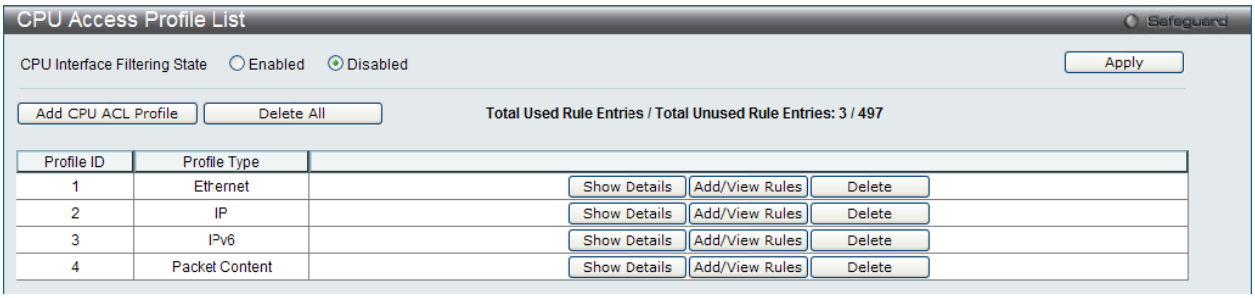


図 11-39 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。1 つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv4 の「Add CPU ACL Profile」画面

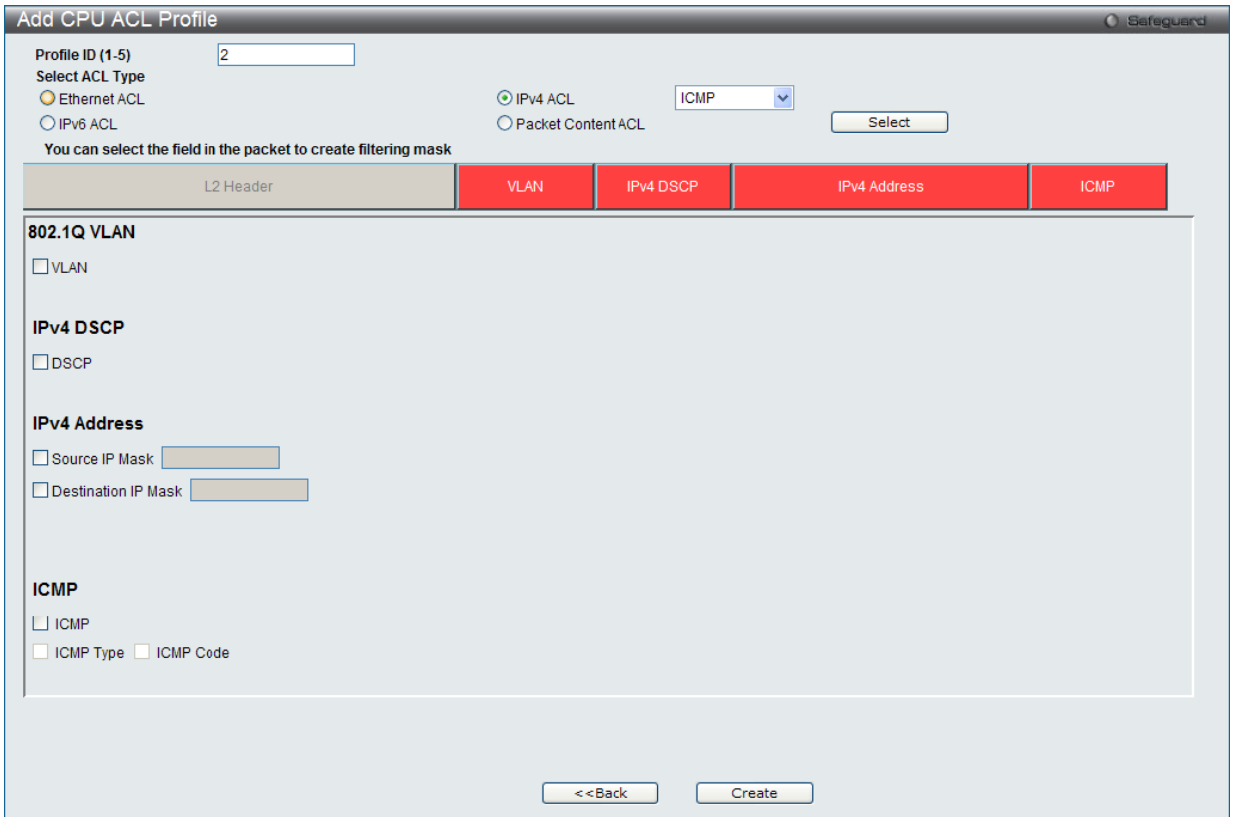


図 10-38　Add CPU ACL Profile - IPv4 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「IPv4 ACL」を選択します。さらに、隣接する欄で設定するフレームヘッダ（ICMP、IGMP、TCP、UDP、Protocol ID）を指定して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を IP（IPv4）フィルタに設定できます。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4」を選択します。 • IPv4 - フレームヘッダの IP アドレスを対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
802.1Q VLAN	パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 • VLAN - VLAN マスクを指定します。 • VLAN Mask (0-FFF) - VLAN マスクを指定します。
IPv4 DSCP	このオプションを指定すると各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。
IPv4 Address	転送決定の基準として使用されます。 • Source IP Mask - 送信元 IP アドレスをマスクする IP アドレスを指定します。例 : 255.255.255.255 • Destination IP Mask - 送信先 IP アドレスをマスクする IP アドレスを指定します。例 : 255.255.255.255
Protocol: 各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
ICMP	それぞれのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。

項目	説明
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（もしくは）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには TCP 項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）、または Check All（すべて）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスクと (または) 送信先ポートマスクを指定する必要があります。 • Source Port Mask (0-FFFF) - フィルタリングする送信元ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 • Destination Port Mask (0-FFFF) - フィルタリングする送信先ポートをマスクする TCP ポートを 16 進数 (hex 0x0-0xffff) で指定します。
Protocol ID	Protocol ID Mask をチェックし、マスクするパケットヘッダの protocol ID を定義する値を指定します。 • Protocol ID Mask (0-FF) - IP ヘッダの後のマスクオプションに定義する値を指定します。 • User Define (0-FFFFFFFF) - ユーザ定義のレイヤ 4 パートマスク値を指定します。

「Create」ボタンをクリックし、このエントリをスイッチに保存します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

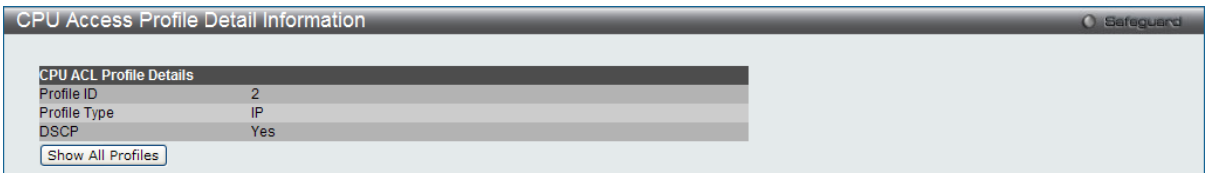


図 11-40 CPU Access Profile Detail Information - IP（IPv4）画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（IPv4）：

IP アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

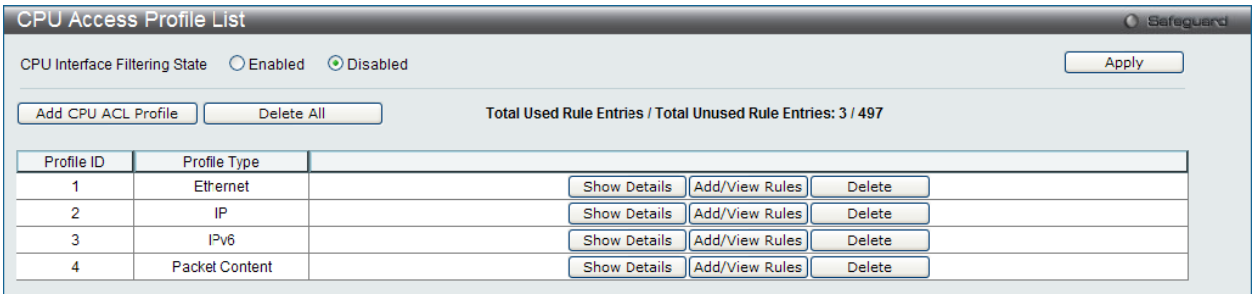


図 11-41 CPU Access Profile List 画面

2. IP エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

図 11-42 CPU Access Rule List - IP 画面

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」ボタンをクリックします。

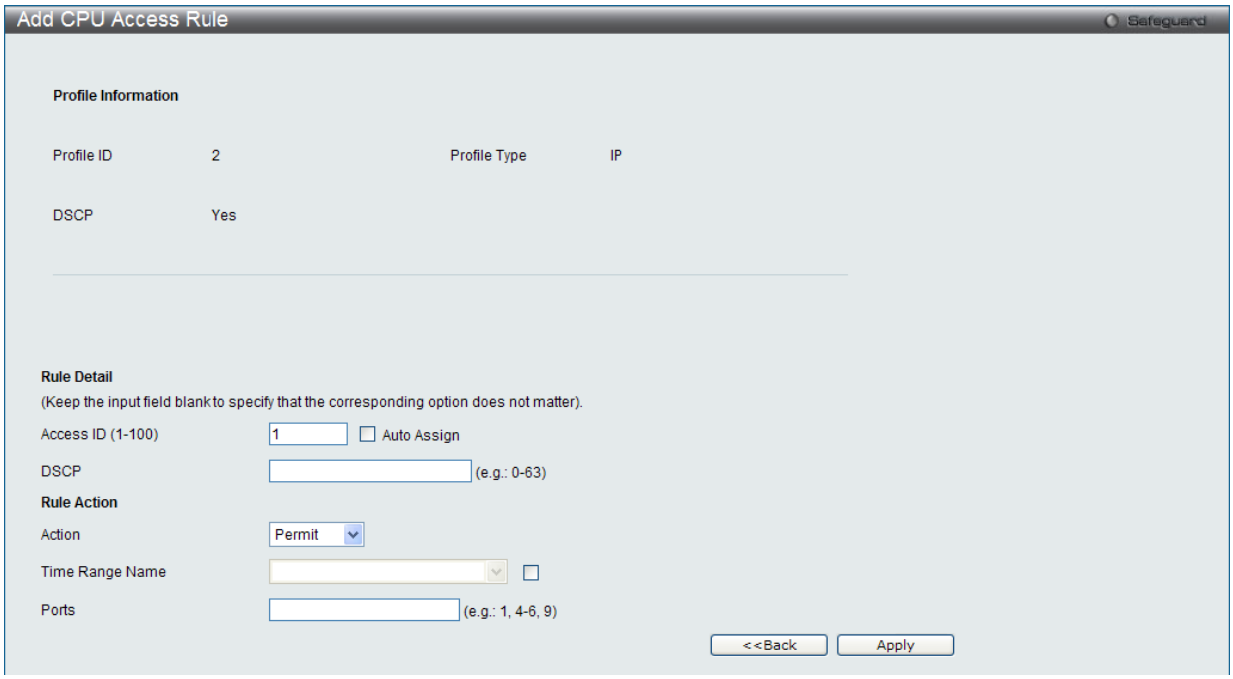


図 11-43　Add Access Rule - IP 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。
VLAN Name	設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。
VLAN ID	設定済みの VLAN ID を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。
Source IP Address	送信元の IP アドレスの IP アドレスを入力します。
Destination IP Address	宛先 IP アドレスの IP アドレスを入力します。
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - TCP Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 - TCP Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。 - Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - UDP Source Port Mask - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - UDP Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。0-255 の値を入力します。
User	マスクしたいパケットヘッダの Protocol ID Mask を 16 進数（0-FFFFFFFF）で指定します。
DSCP	各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。
ICMP	各フレームヘッダの Internet Control Message Protocol(ICMP) フィールドを調べます。

項目	説明
Rule Action	
Action	• Permit - アクセスプロファイルに一致したパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Ports	設定するポート範囲を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

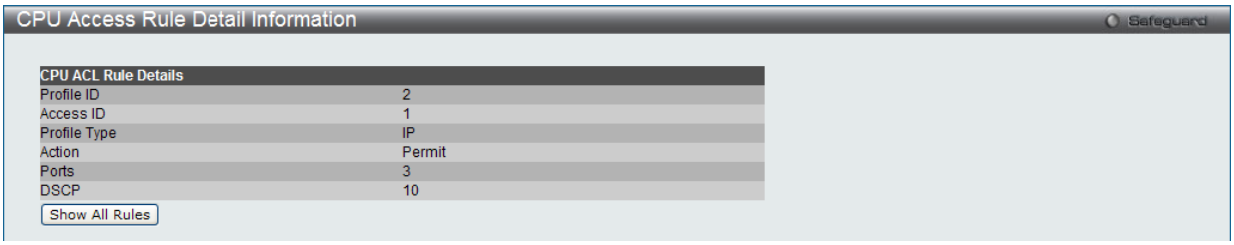


図 11-44 CPU Access Rule Detail Information - IP 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセスプロファイルの作成（IPv6）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

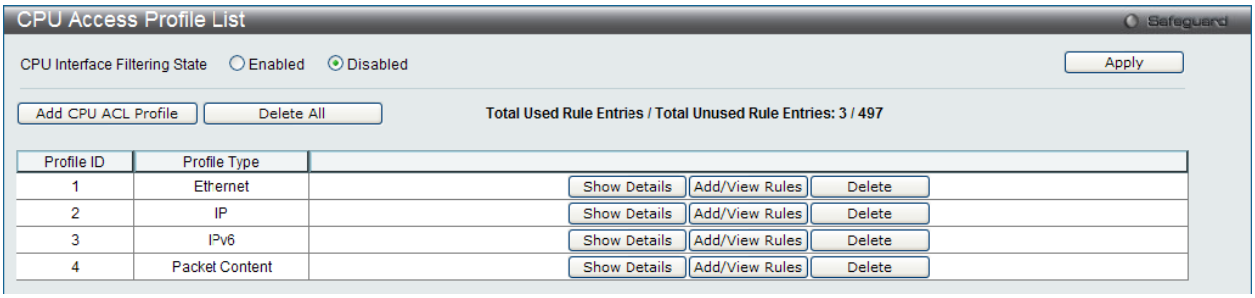


図 11-45 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。１つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv6 の「Add CPU ACL Profile」画面

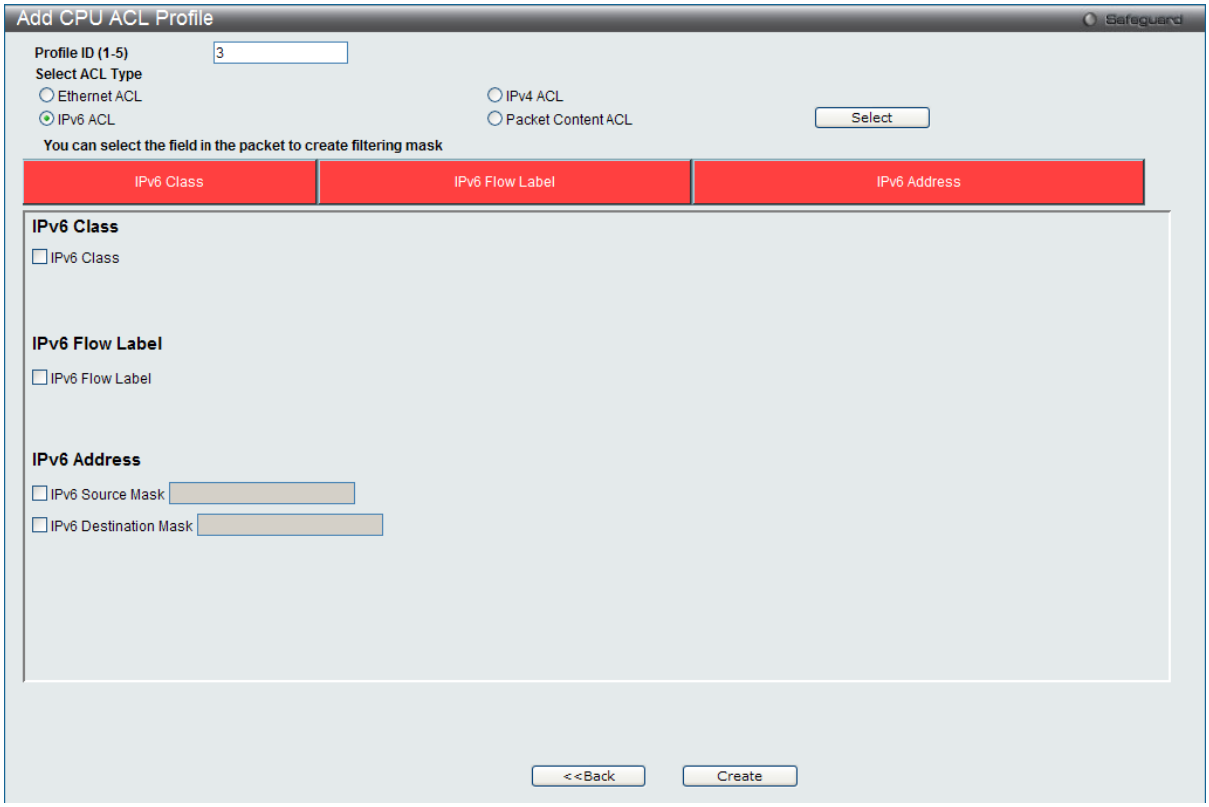


図 11-46　Add CPU ACL Profile - IPv6 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「IPv6 ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を IP（IPv6）フィルタに設定できます。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは、「IPv6」を選択します。 • IPv6 - フレームヘッダの IP アドレスを対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
IPv6 Class	この項目を選ぶと IPv6 ヘッダの「Class」項目を調べます。「Class」項目は IPv4 における Type of Service（ToS）、「Precedence bits」項目のようなパケットヘッダの一部です。
IPv6 Flow Label	この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 Address	• IPv6 Source Mask - 送信元アドレスとして使用する IPv6 アドレスを入力します。 • IPv6 Destination Mask - 宛先アドレスとして使用する IPv6 アドレスを入力します。

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

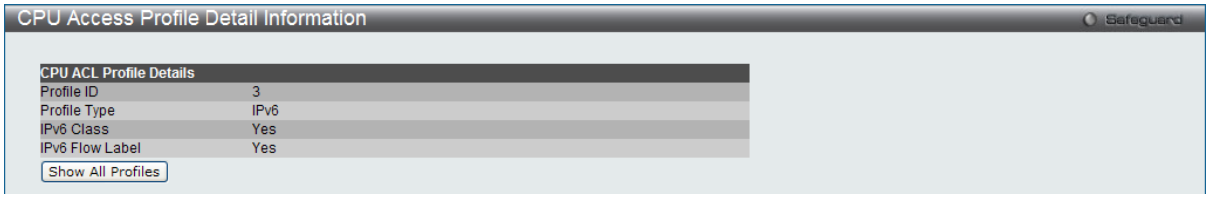


図 11-47　CPU Access Profile Detail Information - IPv6 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（IPv6）：

IPv6 アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

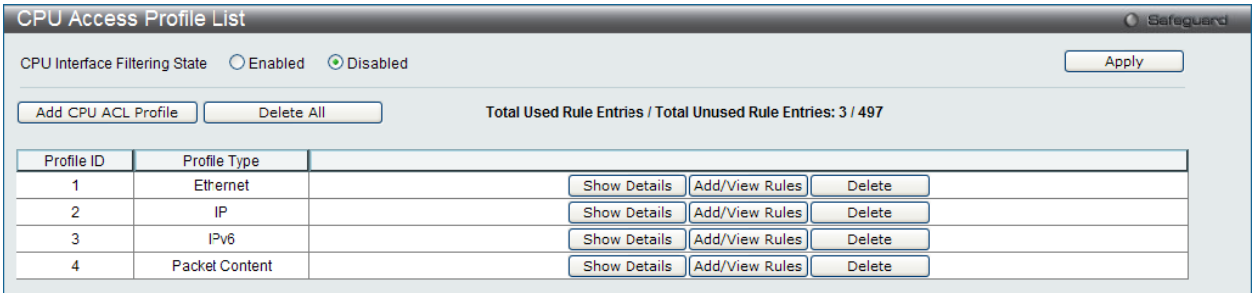


図 11-48 CPU Access Profile List 画面

2. IPv6 エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

図 11-49 CPU Access Rule List - IPv6 画面

既に作成したルールの削除

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」ボタンをクリックし、以下の画面を表示します。

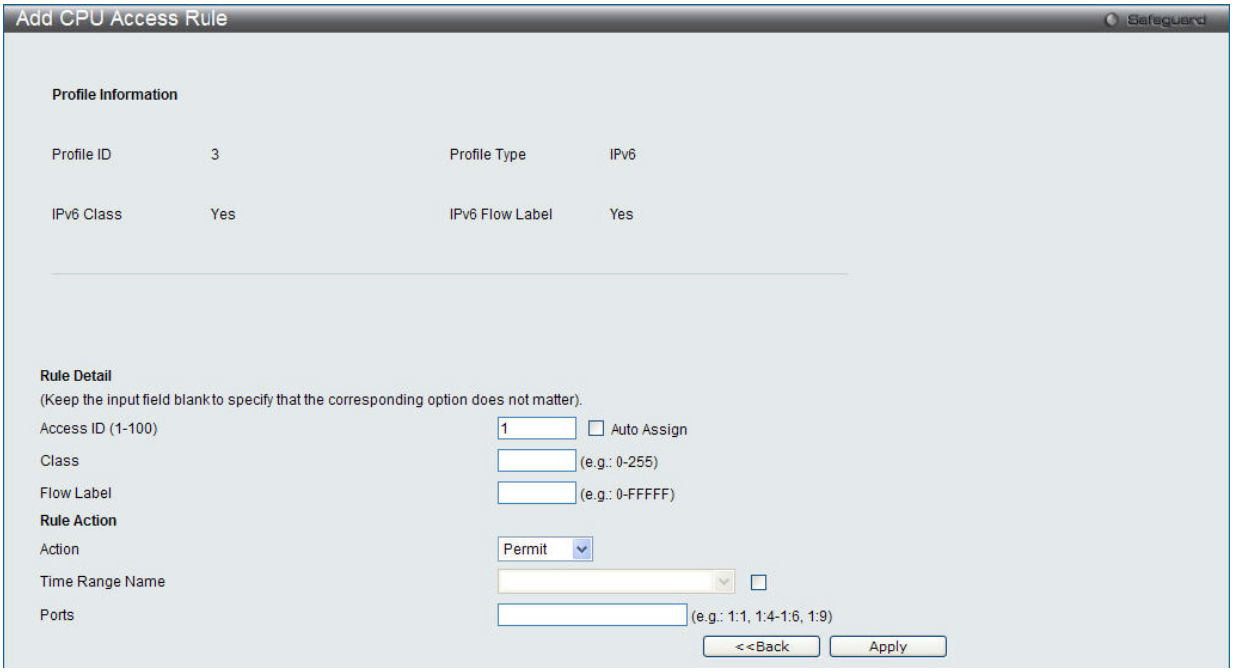


図 11-50 Add Access Rule - IPv6 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。
Class	クラスを入力し、IPv6 ヘッダの「Class」フィールドを調べます。本フィールドは IPv4 における「Type of Service(ToS)」、「Precedence bits」フィールドのようなパケットヘッダの一部です。
Flow Label	この項目を選ぶと IPv6 ヘッダの flow label 項目を調べます。flow label 項目は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 Source Address	IPv6 送信元アドレスの IPv6 アドレスを入力します。
IPv6 Destination Address	IPv6 送信先アドレスの IPv6 アドレスを入力します。
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Ports	設定するポート範囲を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

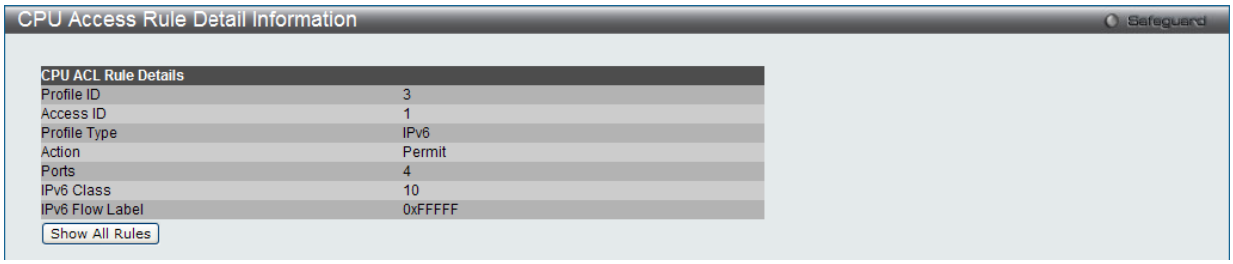


図 11-51　CPU Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセスプロファイルの作成（パケットコンテンツ）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、「CPU Interface Filtering State」をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

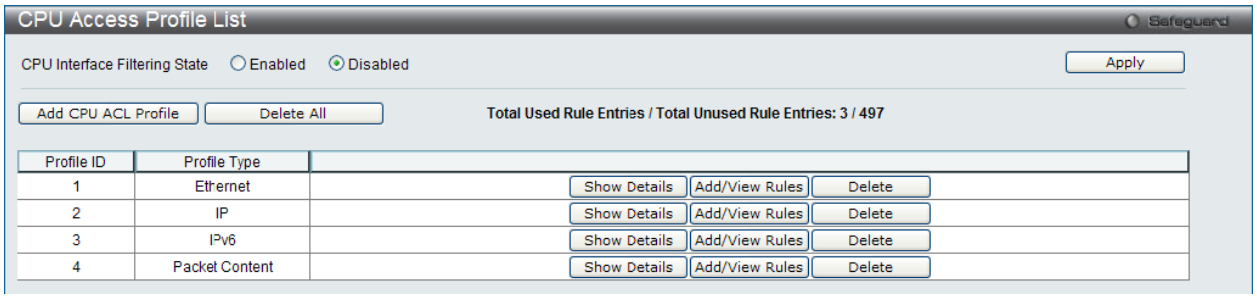


図 11-52　CPU Access Profile List 画面

本画面は、スイッチに作成した CPU アクセスプロファイルリストを表示します。各タイプに 1 つのアクセスプロファイルが説明のために作成されています。「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「CPU Interface Filtering State」に「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

パケットコンテンツの「Add CPU ACL Profile」画面

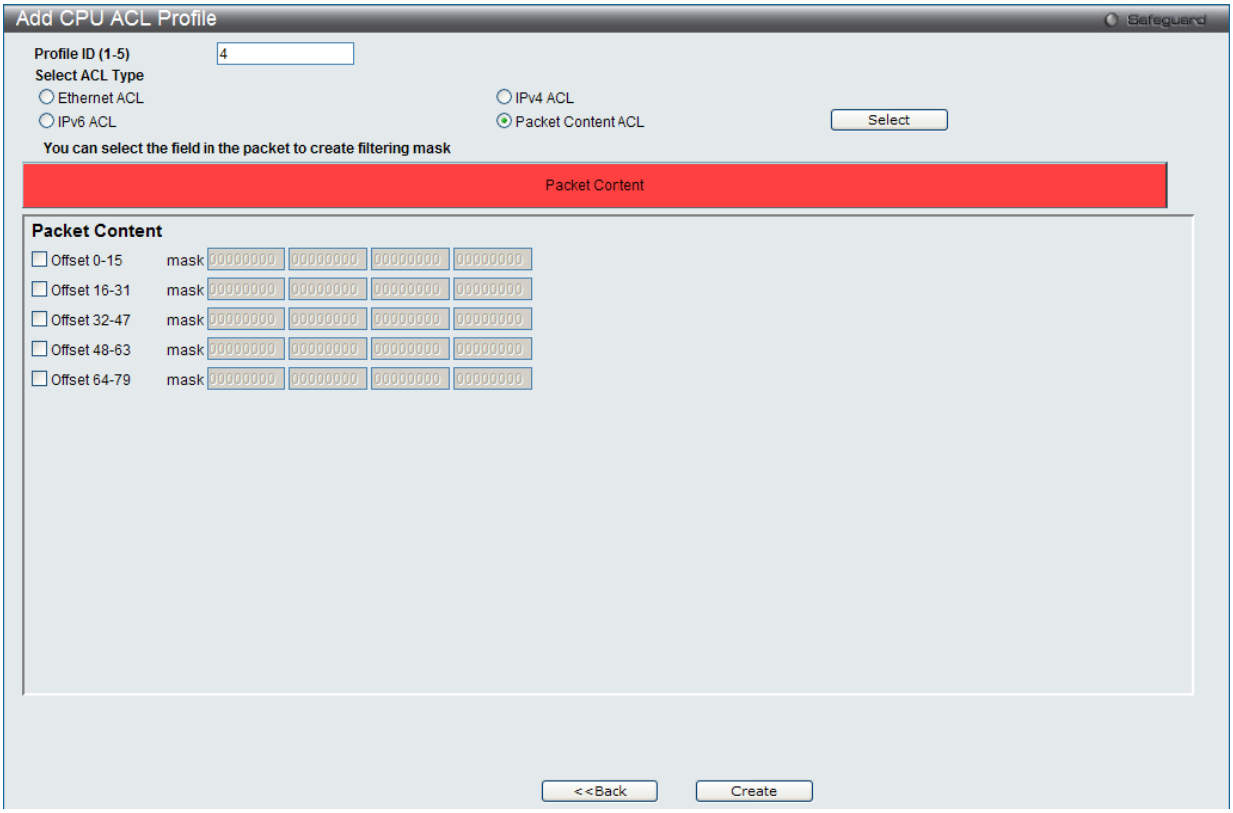


図 11-53　Add CPU ACL Profile - Packet Content 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「Packet Content ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を Packet Content フィルタに設定できます。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Packet Content」を選択します。 • Packet Content - パケットヘッダの内容をマスクして隠します。
Packet Content	1 個のパケット内で最大 5 個のパケットコンテンツオフセットチャンクを同時に検証し、そのフレームコンテンツオフセット、マスクおよびレイヤを規定することができます。5 個のパケットコンテンツチャンクオフセットが設定できます。パケットコンテンツチャンクマスクは 4 バイトを示します。最大 5 個までパケットコンテンツオフセットチャンクを選択することが可能です。パケットヘッダにマスクを開始するオフセットを指定します。 • Offset 0-15 - 16 進数でパケットの最初から 15 バイト目までのマスクを指定します。 • Offset 16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 • Offset 32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 • Offset 48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 • Offset 64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

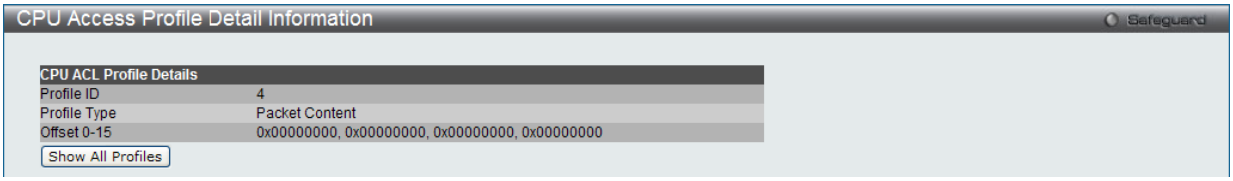


図 11-54　CPU Access Profile Detail Information - Packet Content 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（Packet Content）：

Packet Content アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

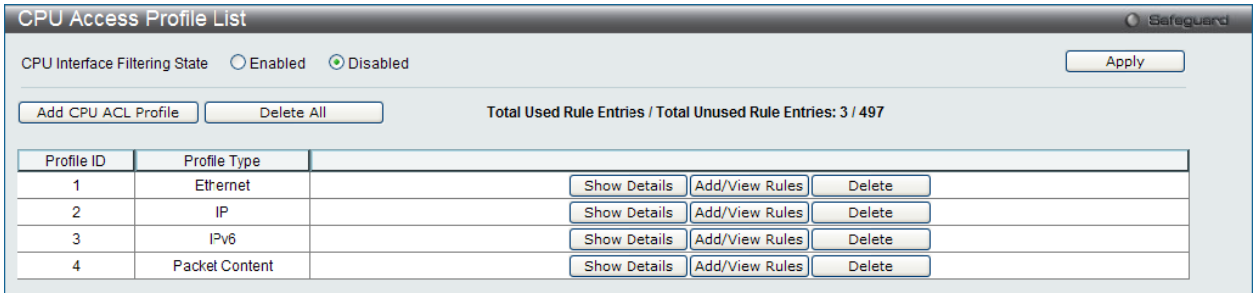


図 11-55　CPU Access Profile List 画面

2. Packet Content エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

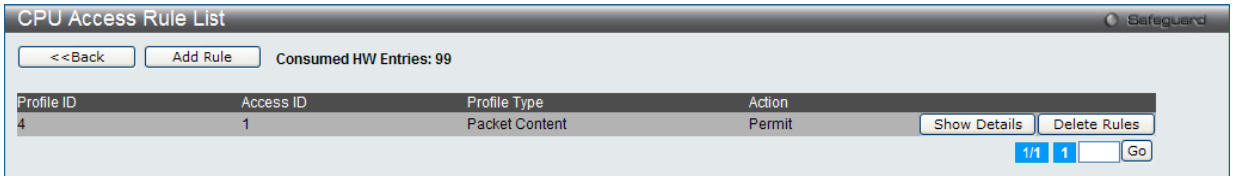


図 11-56　CPU Access Rule List - Packet Content 画面

作成済みのルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

「Add Rule」ボタンをクリックします。

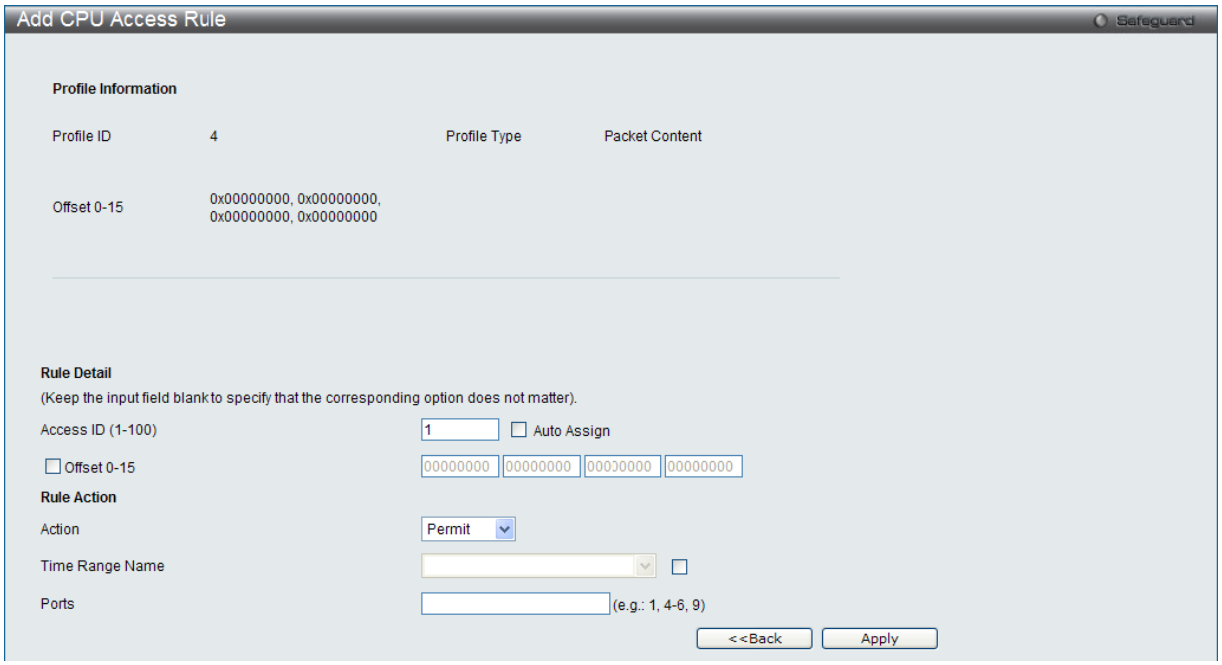


図 11-57　Add Access Rule - Packet Content 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。
Offset	パケットヘッダにマスクを開始するオフセットを指定します。 • Offset 0-15 - 16 進数でパケットの最初から 15 バイト目までのマスクを指定します。 • Offset 16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 • Offset 32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 • Offset 48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 • Offset 64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。
Time Range Name	チェックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Ports	設定するポート範囲を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

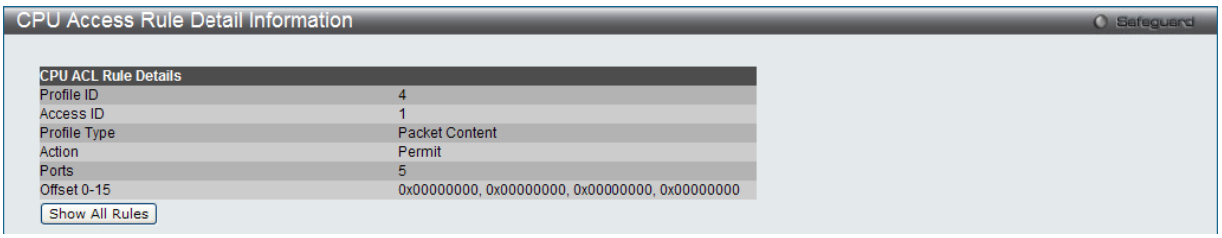


図 11-58 CPU Access Rule Detail Information - Packet Content 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

ACL Finder（ACL 検索）

ACL ルール検索を使用して、特定のポートに割り当てられたすべてのルールを確認し、すばやく既存のルールを編集します。

ACL > ACL Finder の順にメニューをクリックし、以下の画面を表示します。

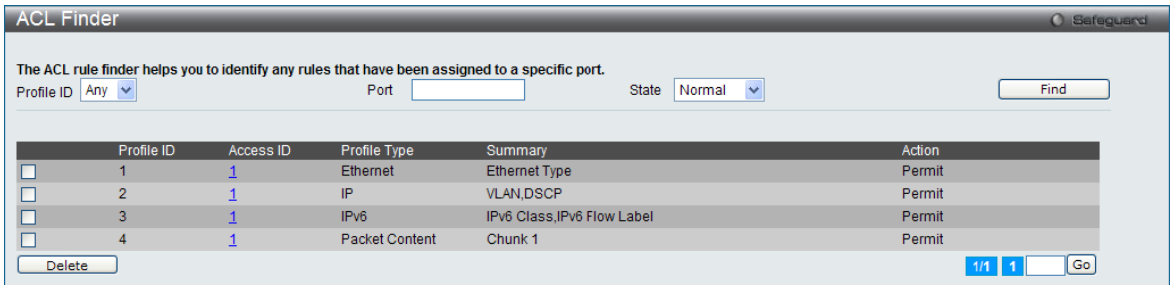


図 11-59　ACL Finder 画面

本画面には以下の項目があります。

項目	説明
Profile ID	ルールの特定のために ACL ルール検索でプロファイル ID を選択します。
Port	ルールの特定のために ACL ルール検索でポート番号を入力します。
State	プルダウンメニューを使用して状態を選択します。 • Normal - 通常の ACL ルールを検索します。 • CPU - CPU ACL ルールを検索します。 • Egress - Egress ACL ルールを検索します。

定義済みの ACL エントリの検索

エントリを検索するためには、「Profile ID」でプロファイル ID を、「Port」で参照するポートを指定し、さらに「State」を定義して、「Find」ボタンをクリックします。画面下半分のテーブルにエントリは表示されます。

エントリの削除

削除するエントリのラジオボタンをチェックし、「Delete」ボタンをクリックします。

プロファイルの参照

参照するエントリの「Access ID」のリンクをクリックします。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL Flow Meter（ACL フローメータ）

ACL フローメータを設定する前に、ユーザが知っておく必要がある頭文字語および項目のリストは次の通りです。

trTCM - Two Rate Three Color Marker。これは、srTCM と共にメータリングおよびパケットフローをマーキングするためにスイッチで可能な 2 つの方式です。trTCM が IP フローを計測し、2 つのレート（CIR および PIR）に基づいて、色でマークします。

CIR - Committed Information Rate。trTCM と srTCM の両方に共通で、CIR は IP パケットのバイト数を計測します。IP パケットのバイト数は、リンクする特定のヘッダではなく、IP ヘッダのサイズを取得することで計測します。trTCM に関しては、パケットフローは、CIR を超過していない場合に緑色でマークされ、CIR を超過している場合に黄色でマークされます。設定される CIR のレートは PIR のレートを超過してはなりません。また、CBS および PBS フィールドを使用して予期しないパケットバーストのために CIR を設定することができます。

- **CBS** - Committed Burst Size。バイト数を計測する場合、CBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、CBS を設定する必要があります。

PIR - Peak Information Rate。このレートは IP パケットのバイト数で計測されます。IP パケットのバイト数は、リンクする特定のヘッダではなく、IP ヘッダのサイズを取得することで計測します。パケットフローが PIR を超過すると、そのパケットフローは赤でマークされます。CIR のレートと同じかそれ以上になるように PIR を設定する必要があります。

- **PBS** - Peak Burst Size。バイト数を計測する場合、PBS は、PIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、PBS を設定する必要があります。

srTCM - Single Rate Three Color Marker。これは、trTCM と共にメータリングおよびパケットフローをマーキングするためにスイッチで可能な 2 つの方式です。srTCM は、設定された CBS と EBS に基づいて IP パケットフローをマークします。CBS に到達しないパケットフローは、緑色にマークされ、EBS ではなく CBS を超過している場合、黄色にマークされ、EBS を超過している場合、赤色にマークされます。

CBS - Committed Burst Size。バイト数を計測する場合、CBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、CBS を設定する必要があります。

EBS - Excess Burst Size。バイト数を計測する場合、EBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。EBS は、CBS と同じかさらに大きいレートに設定されます。

DSCP - Differentiated Services Code Point。色が追加されるパケットヘッダの部分。入力パケットの「DSCP」フィールドを変更することが可能です。ACL フローメータ機能により、入力パケットのレートに基づいて IP パケットフローにカラーコードを付加することができます。以前に説明した通り、２つのフローメータリングのタイプ（trTCM および srTCM）を選択することができます。パケットフローがカラーコードに置かれる時、その色分けされたレートを超過したパケットで何をするべきかを決めることができます。

緑 - IP フローが緑色のモードである時、設定可能なパラメータは、パケットがその「DSCP」フィールドを変更できる「Conform」フィールドにて設定されます。これは ACL フローメータ機能で許容できるフローレートです。

黄 - IP フローが黄色のモードである時、設定可能なパラメータは、「Exceed」フィールドにて設定されます。超過したパケットを「Permit」（許可）または「Drop」（廃棄）するかを選択します。パケットの「DSCP」フィールドを変更ために選択します。

赤 - IP フローが赤色のモードである時、設定可能なパラメータは、「Violate」フィールドにて設定されます。

超過したパケットを「Permit」（許可）または「Drop」（廃棄）するかを選択します。パケットの「DSCP」フィールドを変更ために選択します。
また、「Counter」を指定することによって超過パケットをカウントできるように選択することができます。
「Counter」を有効にすると、アクセスプロファイル内のカウンタ設定は無効になります。どんな指定時間においても 1 つのフローメータに対して 2 つのカウンタのみ有効になります。

ACL > ACL Flow Meter の順にメニューをクリックし、以下の画面を表示します。

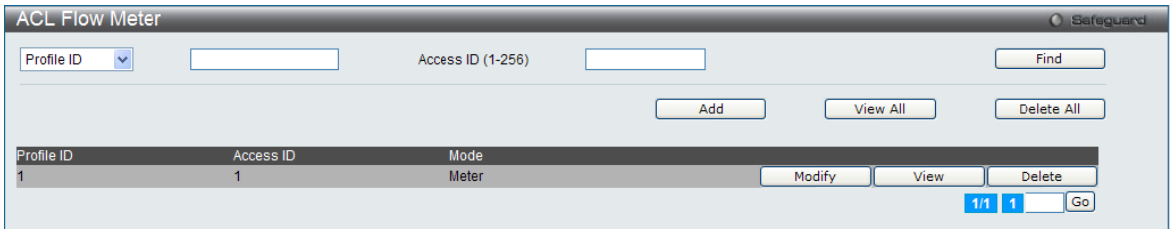


図 11-60　ACL Flow Meter 画面

以下の項目を使用して設定を行います。

項目	説明
Profile ID	フローメータの定義済みプロファイル ID を指定します。
Profile Name	フローメータの定義済みプロファイル名を指定します。
Access ID (1-256)	フローメータの定義済みアクセス ID を指定します。

入力後、「Find」ボタンをクリックします。情報が画面下半分に表示されます。

エントリの削除

対応する「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Add」ボタンをクリックし、以下の画面を表示します。

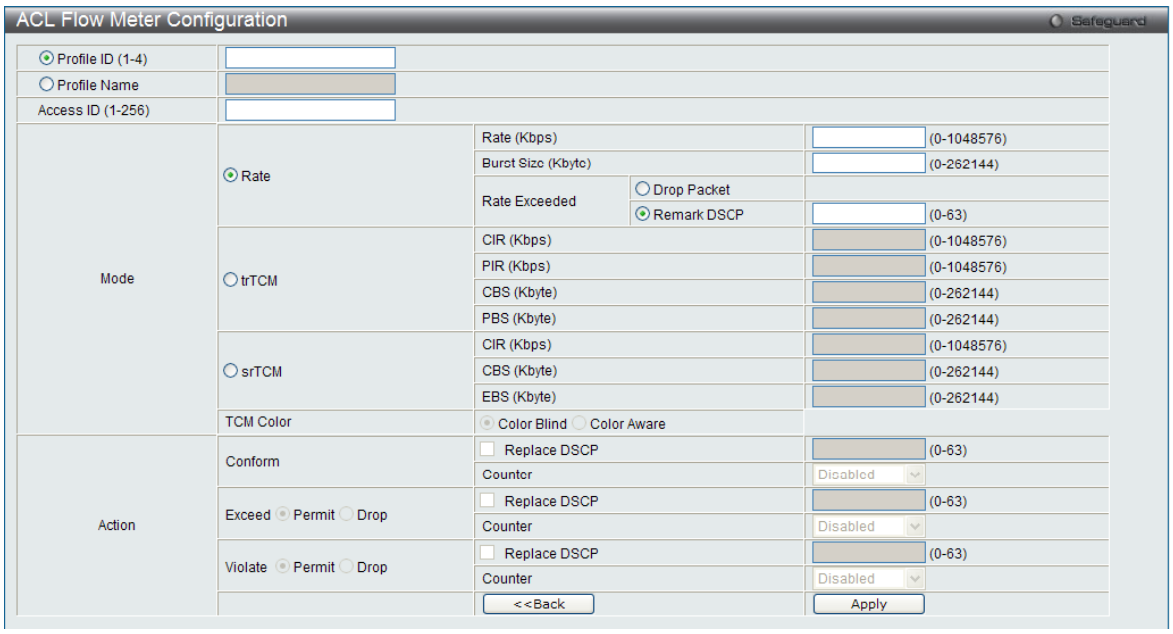


図 11-61　ACL Flow Meter Configuration 画面 - Add

以下の項目を使用して、設定を行います。

項目	説明
Profile ID (1-4)	プルダウンメニューから、フローメータリングを設定する定義済みのプロファイル ID を指定します。
Profile Name	フローメータに対するプロファイル名を入力します。
Access ID (1-256)	ACL フローメータリングを設定する定義済みアクセス ID を 1-256 の範囲で指定します。
Mode	Rate - シングルレート 2 カラーモードのレートを指定します。 • Rate - フローに規定する帯域幅を Kbps 単位で指定します。 • Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 • Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: - Drop Packet - パケットを直ちに破棄します。 - Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。 trTCM -「2 レート 3 カラーモード」を指定します。 • CIR - コミット情報レートの値を入力します。単位は Kbps です。CIR は PIR 以下である必要があります。 • PIR - ピーク情報レートを指定します。単位は Kbps です。PIR は CIR 以上である必要があります。 • CBS -「コミットバーストサイズ」の値を入力します。 • PBS - ピークバーストサイズの値を入力します。 srTCM -「シングルレート 3 カラーモード」を指定します。 • CIR - コミット情報レートの値を入力します。 • CBS -「コミットバーストサイズ」の値を入力します。 • EBS -「超過バーストサイズ」を指定します。
Action	Conform - 本フィールドは緑色のパケットフローを表します。緑色のパケットフローは、DSCP フィールドを本フィールドで指定された値に書き換える可能性があります。また、「Counter」パラメータを使用することで緑色のパケットをカウントするように選択することができます。 • Replace DSCP - 緑色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 • Counter - 緑色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。 Un-conform - 不適合 (黄色または赤) パケットの DSCP を変更します。 • Replace DSCP - 赤色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 Exceed - 本フィールドは黄色のパケットフローを表します。黄色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。 • Counter - 黄色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。 Violate - 本フィールドは赤色のパケットフローを表します。赤色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。 • Counter - 赤色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。

「Apply」ボタンをクリックして、設定を適用します。

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

エントリの変更

1. 対応する「Modify」ボタンをクリックし、編集画面を表示します。

2. 以下の項目を使用して、設定を行います。

項目	説明
Mode	Rate - シングルレート 2 カラーモードのレートを指定します。 • Rate - フローに規定する帯域幅を Kbps 単位で指定します。 • Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。 • Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: - Drop Packet - パケットを直ちに破棄します。 - Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。

「Apply」ボタンをクリックして、設定を適用します。

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

エントリの参照

すべてのエントリを参照するためには、「View All」ボタンをクリックします。

エントリを参照するためには、対応する「View」ボタンをクリックし、以下の画面を表示します。

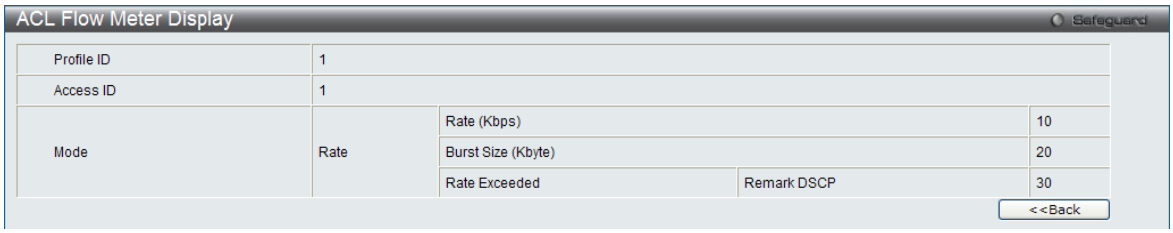


図 11-62 ACL Flow Meter Display 画面

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

第 12 章　Security（セキュリティ機能の設定）

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

以下は Security サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
802.1X（802.1X 設定）	802.1X 認証を設定します。以下のメニューがあります。 802.1X Global Settings（802.1X グローバル設定）、802.1X Port Settings（802.1X ポート設定）、802.1X User Settings（802.1X ユーザ設定）、Guest VLAN（ゲスト VLAN の設定）、Authenticator State（オーセンティケータの状態）、Authenticator Statistics（オーセンティケータ統計情報）、Authenticator Session Statistics（オーセンティケータセッション統計情報）、Authenticator Diagnostics（オーセンティケータ診断）、Initialize Port(s)（初期化ポート）、Reauthenticate Port(s)（再認証ポート）	206
RADIUS（RADIUS 設定）	RADIUS サーバの設定を行います。以下のメニューがあります。 Authentication RADIUS Server Settings（認証 RADIUS サーバ設定）、RADIUS Accounting Setting（RADIUS アカウンティング設定）、RADIUS Authentication（RADIUS 認証）、RADIUS Account Client（RADIUS アカウンティングクライアント）	219
IP-MAC-Port Binding（IMPB : IP-MAC- ポートバインディング）	IP アドレス、MAC アドレスおよびポートを結合し、レイヤ間通信を行います。以下のメニューがあります。: IMPB Global Settings（IMPB グローバル設定）、IMPB Port Settings（IMPB ポート設定）、IMPB Entry Settings（IMPB エントリ設定）、MAC Block List（MAC ブロックリスト）、DHCP Snooping（DHCP Snooping 設定）	223
MAC-based Access Control（MAC ベースアクセスコントロール）	MAC アドレス認証機能を設定します。以下のメニューがあります。 MAC-based Access Control Settings（MAC ベースアクセスコントロール設定）、MAC-based Access Control Local Settings（MAC ベースアクセスコントロール ローカル設定）、MAC-based Access Control Authentication State（MAC ベースアクセスコントロールの認証状態）	228
Compound Authentication（コンパウンド認証）	コンパウンド認証方式を設定します。	231
Port Security（ポートセキュリティ）	ダイナミックな MAC アドレス学習をロックします。以下のメニューがあります。 Port Security Settings（ポートセキュリティの設定）、Port Security VLAN Settings（ポートセキュリティ VLAN 設定）、Port Security Entries（ポートセキュリティエントリ）	232
ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）	パケットコンテンツ ACL を使用して、ARP スプーフィング攻撃を防止します。	235
BPDU Attack Protection（BPDU アタック防止設定）	ポートに BPDU 防止機能を設定します。	236
Loopback Detection Settings（ループバック検知設定）	ループバック検知機能の設定を行います。	237
Traffic Segmentation Settings（トラフィックセグメンテーション設定）	ポートのトラフィックフローを制限します。	238
NetBIOS Filtering Setting（NetBIOS フィルタリング設定）	NetBIOS フィルタ設定を行います。	239
DHCP Server Screening（DHCP サーバスクリーニング）	不正な DHCP サーバへのアクセスを拒否します。以下のメニューがあります。 DHCP Server Screening Port Settings（DHCP サーバスクリーニング設定）、DHCP Offer Permit Entry Settings（DHCP オファー許可エントリ設定）	240
Access Authentication Control（アクセス認証コントロール）	TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。以下のメニューがあります。 Enable Admin（管理者レベルの認証）、Authentication Policy Settings（認証ポリシー設定）、Application Authentication Settings（アプリケーションの認証設定）、Authentication Server Group Settings（認証サーバグループ設定）、Authentication Server Settings（認証サーバ設定）、Login Method Lists Settings（ログインメソッドリスト）、Enable Method Lists Settings（メソッドリストの有効化）、Local Enable Password Settings（ローカルユーザパスワード設定）	242
SSL Settings（Secure Socket Layer の設定）	証明書の設定、暗号スイートの設定を行います。	250
SSH（Security Shell の設定）	SSH サーバ、SSH アルゴリズム、SSH ユーザ認証の設定を行います。以下のメニューがあります。: SSH Settings（SSH サーバ設定）、SSH Authentication Method and Algorithm Settings（SSH 認証モードとアルゴリズム設定）、SSH User Authentication List（SSH ユーザ認証リスト）	252
Trusted Host Settings（トラストホスト）	リモートのスイッチ管理用トラストホストを設定します。	255
Safeguard Engine Settings（セーフガードエンジン）	セーフガードエンジンの設定を行います。	256
DoS Attack Prevention Settings（DoS アタック防止設定）	各 DoS アタックに対して防御設定を行います。	258
IGMP Access Control Settings（IGMP アクセスコントロール設定）	各ポートに IGMP 認証（IGMP アクセスコントロール）を設定します。	259

802.1X（802.1X 設定）

Port Access Entity（ポートアクセスエンティティ）

802.1X ポートベースおよび MAC ベースのアクセスコントロール

IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。本方式は、ネットワークへアクセスするユーザを認証するために RADIUS サーバを使用し、EAPOL（Extensible Authentication Protocol over LAN）と呼ばれるパケットをクライアント・サーバ間で中継することにより実現します。以下の図は基本的な EAPOL パケットの構成を示しています。

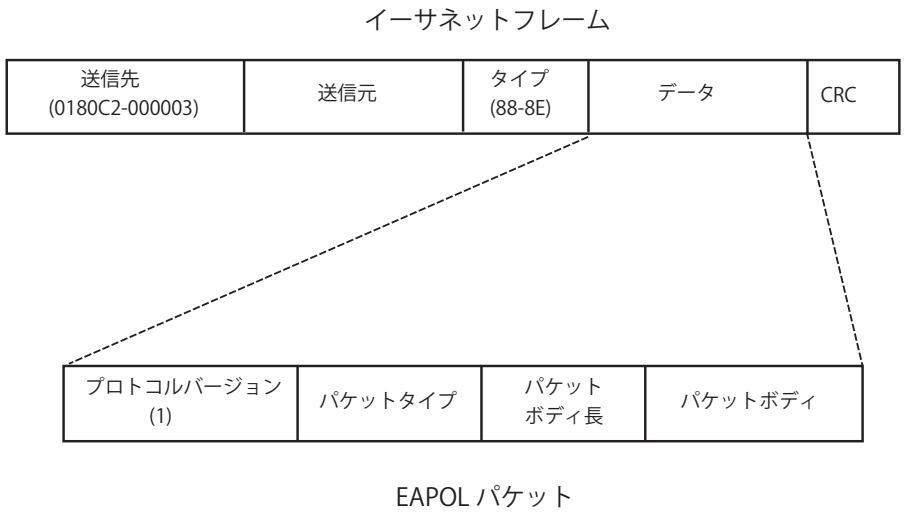


図 12-1　EAPOL パケット

本方法を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。EAPOL パケットは、承認が与えられるまでの間指定ポート経由で送受信される唯一のトラフィックです。802.1X アクセスコントロール方式は 3 つの役割を持っており、それぞれがアクセスコントロールセキュリティ方法の作成、状態の保持および動作のために必要不可欠です。

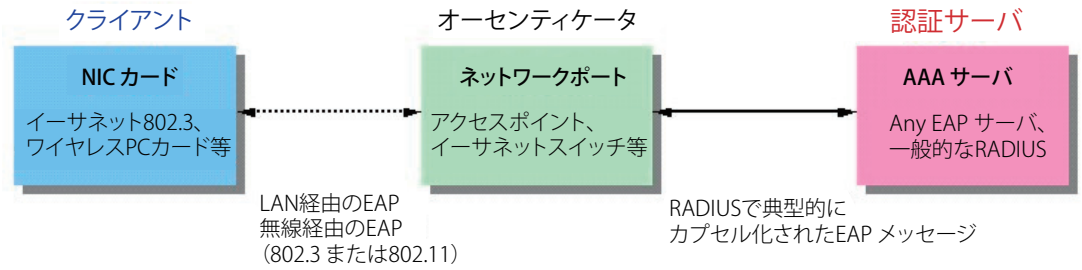


図 12-2　802.1X の 3 つの要素

以下の項では、クライアント、オーセンティケータ、および認証サーバのそれぞれの役割について詳しく説明します。

認証サーバ

認証サーバはクライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。認証サーバ上では RADIUS サーバプログラムを実行し、またそのサーバのデータがオーセンティケータ側（スイッチ）に正しく登録されている必要があります。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを受ける前に、認証サーバ（RADIUS）による認証を受ける必要があります。認証サーバは、RADIUS サーバとクライアントの間で EAPOL パケットを通じて信頼できる情報を交換し、そのクライアントの LAN やスイッチのサービスに対するアクセス許可の有無をスイッチに通知します。このように、認証サーバの役割は、ネットワークにアクセスを試みるクライアントの身元を保証することです。

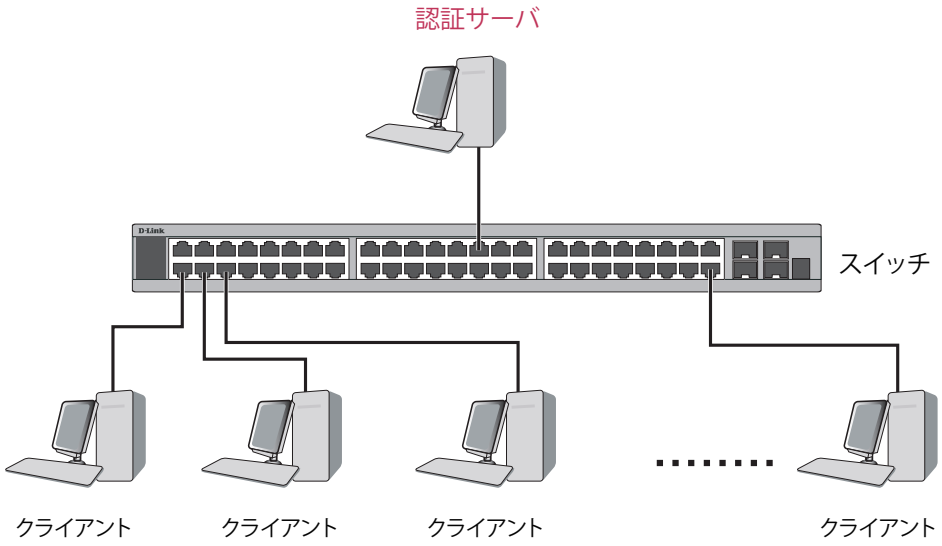


図 12-3　認証サーバ

オーセンティケータ

オーセンティケータ（スイッチ）は、認証サーバとクライアントの間を取り持つ、仲介の役割を果たします。802.1X を使用する場合、オーセンティケータサーバには 2 つの目的があります。 1 つ目の目的は、クライアントに EAPOL パケットを通して認証情報を提出するよう要求することです。EAPOL パケットはクライアントにアクセスが許可される前にオーセンティケータを通過することのできる唯一の情報です。2 つ目の目的はクライアントから収集した情報を、認証サーバに確認してもらい、その結果をクライアントに伝達することです。

スイッチをオーセンティケータとして正しく設定するためには、以下の 3 つの手順を実行する必要があります。

1. 802.1X 機能を有効にします。（**DES-3200 Web Management Tool**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Port Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > RADIUS > Authentication RADIUS Server Settings**）

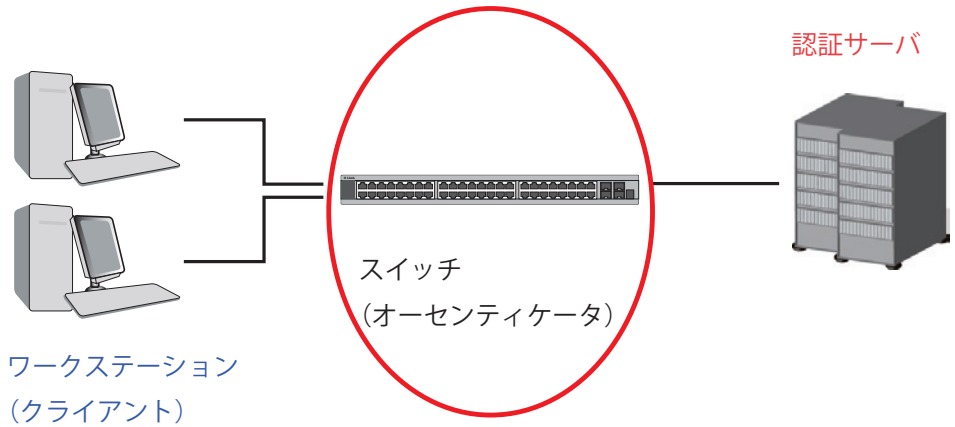


図 12-4　オーセンティケータ

クライアント

クライアントとは、簡単に言うと LAN やスイッチが提供するサービスへのアクセスを希望するワークステーションです。クライアントとなるワークステーションでは、802.1X プロトコルに準拠したソフトウェアが起動している必要があります。Windows XP 使用の場合には、OS 内に既にそのようなソフトウェアが組み込まれています。それ以外の場合には、802.1X クライアントソフトウェアを別途用意する必要があります。クライアントは EAPOL パケットを使用して LAN へのアクセスを要求し、またスイッチからの要求に対しても応答します。

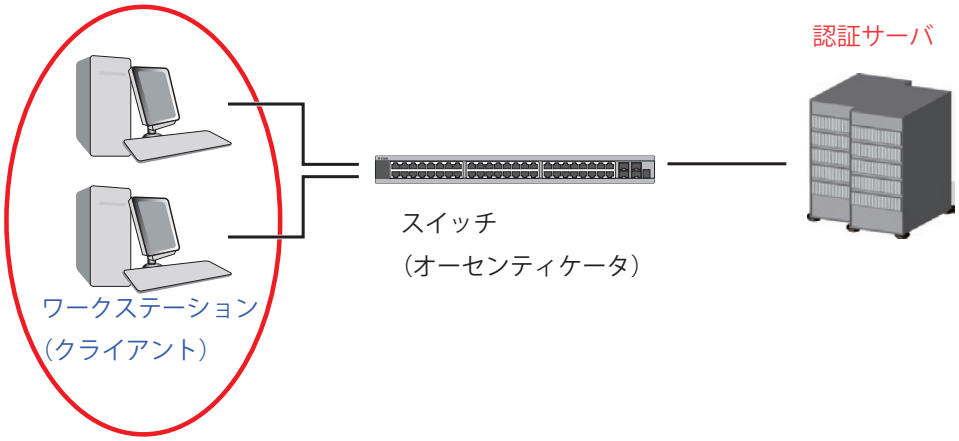


図 12-5　クライアント

認証プロセス

これらの 3 つの要素により、802.1X プロトコルはネットワークへのアクセスを試みるユーザの認証を安定的かつ安全に行います。認証に成功する前は、EAPOL トラフィックのみが特定ポートの通過を許可されます。このポートは、有効なユーザ名とパスワード（802.1X の設定で MAC アドレスも指定されている場合は MAC アドレスも）を持つクライアントがアクセス権を取得してポートのロックが解除されるまで、ロック状態を保ちます。ロックが解除されると、通常のトラフィックがポートを通過できるようになります。D-Link が実装する 802.1X では以下の 2 種類のアクセスコントロールが選択できます。

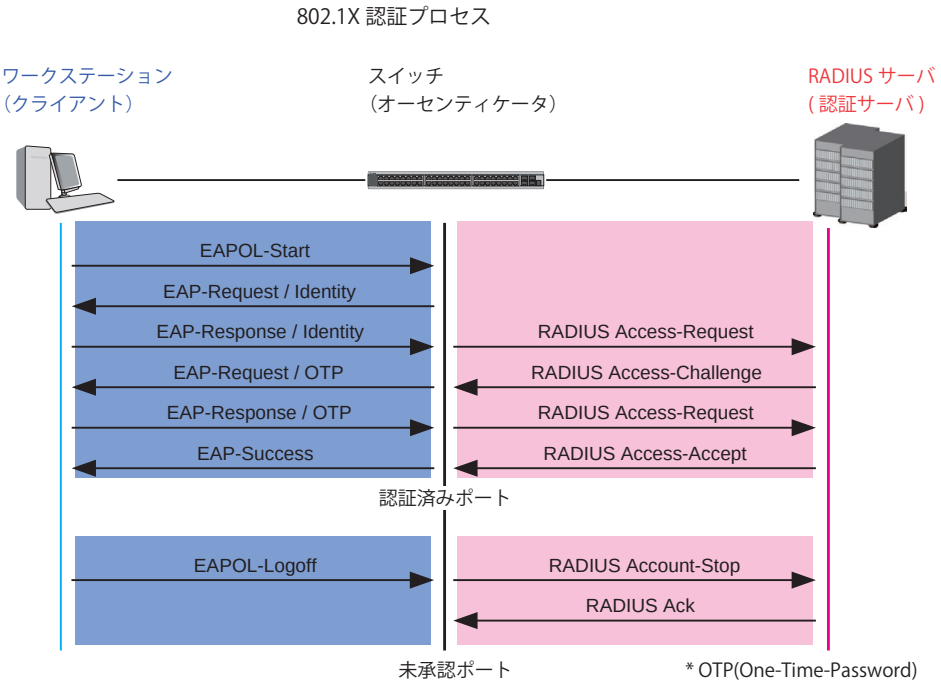


図 12-6　802.1X 認証プロセス

本スイッチの 802.1X 機能では、以下の 2 つのタイプのアクセスコントロールから選択することができます。

1. ポートベースのアクセスコントロール
   本方式では、 1 人のユーザがリモートの RADIUS サーバにポートごとの認証をリクエストし、残りのユーザも同じポートをアクセスできるようにします。
2. MAC ベースのアクセスコントロール
   本方式では、スイッチは自動的に各ポートに対して 448 件までの MAC アドレスを自動的に学習してリストに追加します。スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に各 MAC アドレスの認証を行います。

ポートベースのネットワークアクセスコントロール

802.1X 開発の本来の目的は、LAN 上で Point to Point プロトコルの機能を利用することでした。インフラストラクチャのように単一の LAN セグメントが 2 個以上のデバイスを持たない場合、どちらかがブリッジポートとなります。ブリッジポートは、リンクのリモートエンドにあるアクティブなデバイスの接続を示すイベントや、アクティブなデバイスが非アクティブ状態に遷移することを示すイベントの検知を行います。これらのイベントをポートの認証状態の制御に利用し、ポートでの認証が行わない場合に接続デバイスの認証プロセスを開始します。これをポートベースのアクセスコントロールと呼びます。

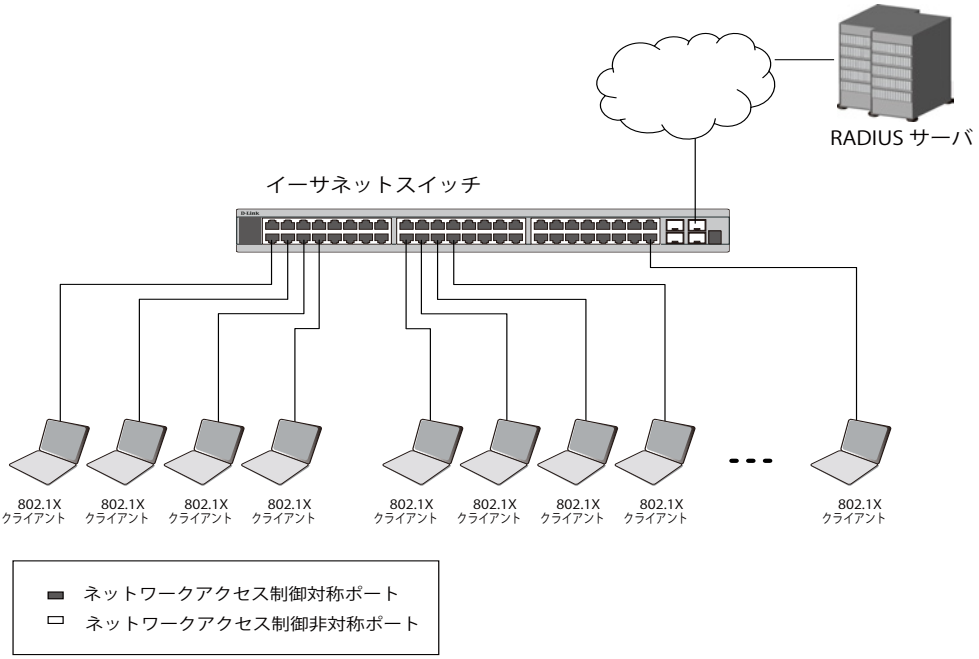


図 12-7　典型的なポートベースアクセスコントロールのネットワーク構成例

一度接続デバイスが認証に成功すると、ポートは Authorized（認証済み）状態になり、ポートが未認証になるようなイベントが発生するまでポート上のすべてのトラフィックはアクセスコントロール制限の対象となりません。そのため、ポートが 1 台以上のデバイスが所属する共有 LAN セグメントに接続される場合、接続デバイスの 1 つが認証に成功すると共有セグメント上のすべての LAN に対して事実上アクセスを許可することになります。このような状態のセキュリティは明らかに脆弱であると言えます。

MAC ベースのネットワークアクセスコントロール

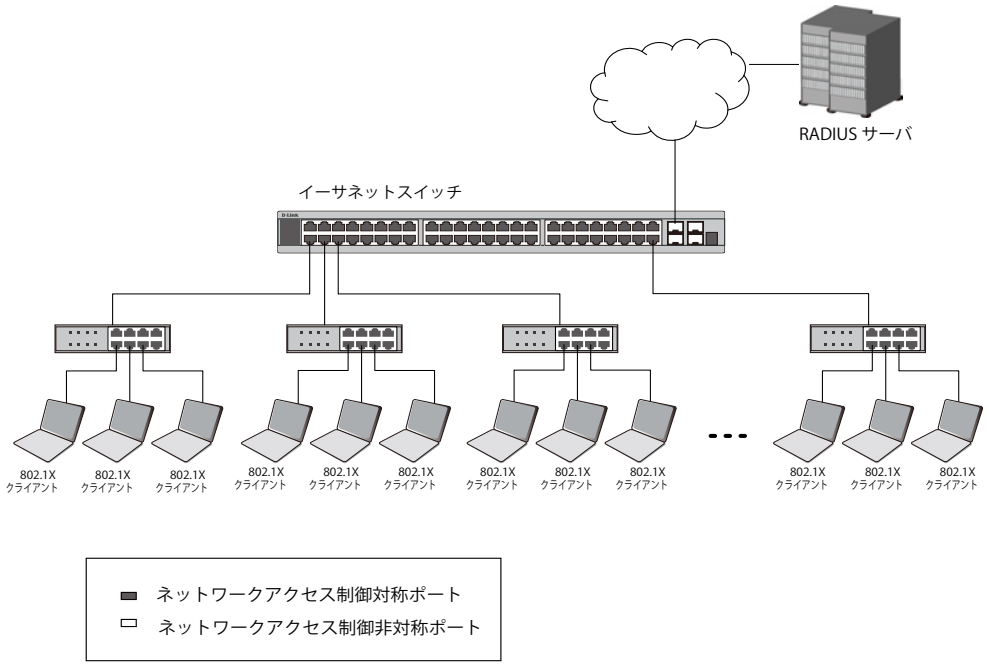


図 12-8　典型的な MAC ベースアクセスコントロールのネットワーク構成例

共有 LAN セグメント内で 802.1X を活用するためには、LAN へのアクセスを希望する各デバイスに「仮想」ポートを定義する必要があります。するとスイッチは共有 LAN セグメントに接続する 1 つの物理ポートを、異なる論理ポートの集まりであると認識し、それら仮想ポートを EAPOL の交換と認証状態に基づいて別々に制御します。スイッチは接続する各デバイスの MAC アドレスを学習し、それらのデバイスがスイッチ経由で LAN と通信するための仮想ポートを確立します。

802.1X Global Settings（802.1X グローバル設定）

802.1X グローバルパラメータを設定します。

Security > 802.1X > 802.1X Global Settings の順にメニューをクリックし、以下の画面を表示します。

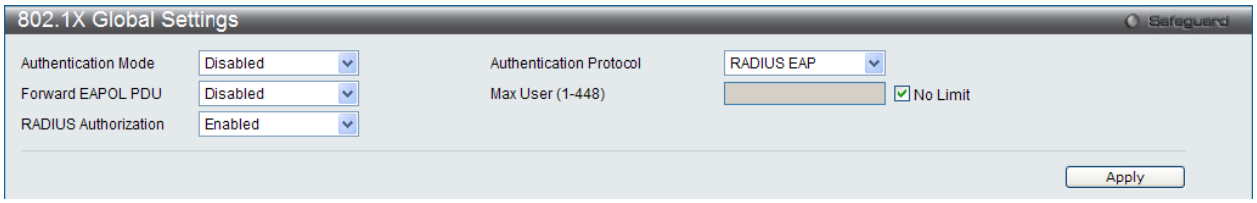


図 12-9　802.1X Global Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Authentication Mode	80.1X 機能を「Disabled」、「Port-based」または「MAC-based」から選択します。
Authentication Protocol	認証プロトコルを「Local」または「RADIUS EAP」から選択します。
Forward EAPOL PDU	これは、EAPOL PDU の転送を制御するグローバル設定です。802.1X 機能をグローバルまたはポートに無効とした場合に、802.1X forward PDU がグローバルおよびポートに有効にされると、ポートに受信した EAPOL パケットは同じ VLAN 内で（グローバルまたはそのポートに対して）802.1X forward PDU が有効で 802.1X が無効であるポートにフラッドします。初期値は無効です。
Max Users (1-448)	ユーザの最大数を指定します。最大ユーザ数は 448 です。「No Limit」をチェックすると、ユーザ制限はなくなります。
RADIUS Authorization	認可設定の受け入れを有効または無効にします。802.1X の RADIUS における許可を有効にする場合、グローバルな認可ネットワークが有効になると、RADUIS サーバに割り当てられる認可データが許可されます。

「Apply」ボタンをクリックして行った変更を適用します。

802.1X Port Settings（802.1X ポート設定）

802.1X のオーセンティケータ設定を行います。

Security > 802.1X > 802.1X Port Settings の順にメニューをクリックし、以下の画面を表示します。

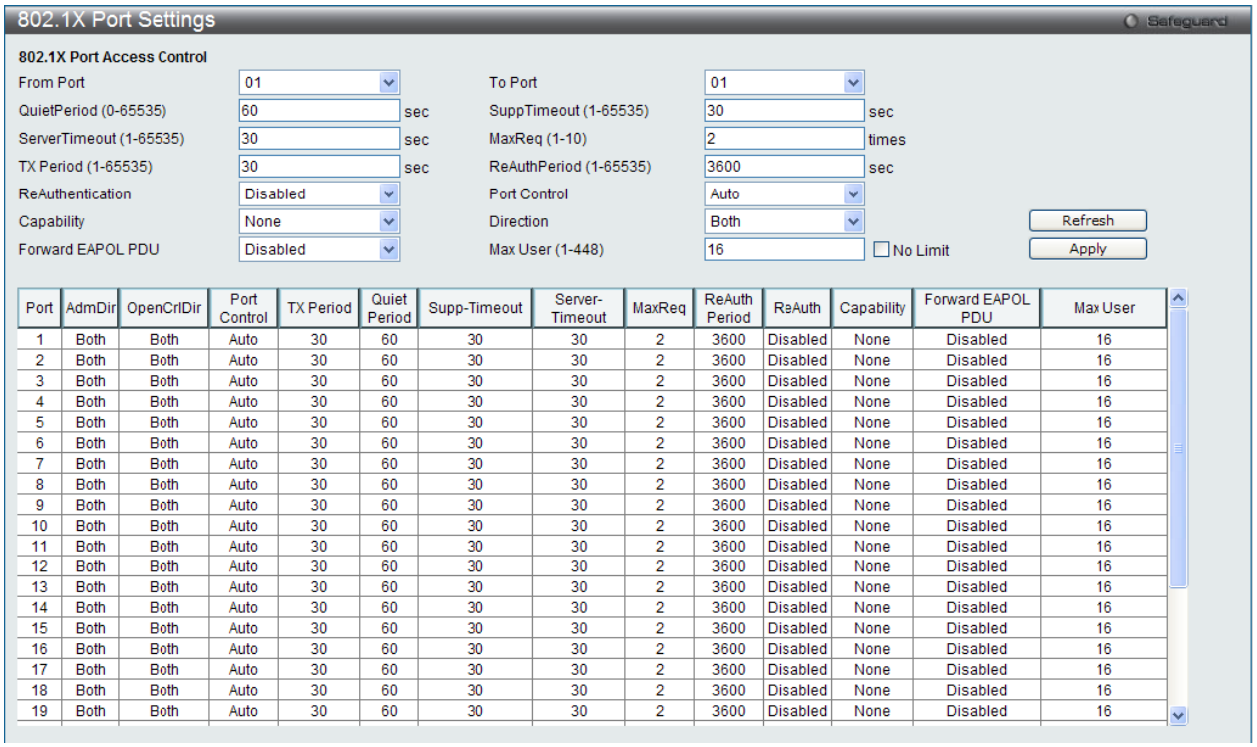


図 12-10　802.1X Port Settings 画面

以下の項目を使用して設定を行います。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
QuietPeriod (0-65535)	クライアントの認証交換に失敗した後、スイッチが静止状態のままクライアントとの通信を拒否する期間（秒）。初期値は 60（秒）です。
SuppTimeout (1-65535)	オーセンティケータとクライアント間の交換でクライアントに EAP-Request を送信した後、応答を待つ時間。初期値は 30（秒）です。IEEE-802.1X-2001 P47 の SuppTimeout で定義されています。サプリカントがタイムアウトになった際に aWhile タイマを初期化する値です。初期値は 30（秒）です。しかし、現在の認証交換に関連するチャレンジのタイプが異なるタイムアウト値を要求する場合（例えば、チャレンジがユーザ側の操作を必要とする場合）、タイムアウト値はそれに基づいて調整されます。1-65535（秒）の範囲の任意の値に設定することができます。
ServerTimeout (1-65535)	オーセンティケータが認証サーバ間の交換でオーセンティケータが Access-Request を送信した後、応答を待つ時間。初期値は 30（秒）です。
MaxReq (1-10)	認証セッションのタイムアウト前にスイッチからクライアントへの EAPOL-Request パケットの最大再送回数。初期値は 2 です。IEEE-802.1X-2001 P47 の MaxReq で定義されています。認証セッションのタイムアウト前にスイッチからクライアントへの EAPOL-Request パケットの最大再送回数。初期値は 2 です。1-10 までの範囲の任意の値を設定できます。
TxPeriod (1-65535)	オーセンティケータ PAE 状態マシンの TxPeriod の時間を指定します。本値がクライアントへの EAP Request/Identity パケットの送信間隔となります。初期値は 30（秒）です。
ReAuthPeriod (1-65535)	クライアントの再認証間隔を定義する 0（秒）以外の定数。初期値は 3600（秒）です。
ReAuthentication	このポート上で通常の再認証を行うかどうか指定します。初期値は「Disabled」です。
Port Control	ポートの認証状態を制御できます。 • ForceAuthorized - 802.1X を無効にし、認証情報の交換を要求せずにポートを Authorized 状態にします。この時ポートではクライアントの 802.1X ベースの認証を行うことなく、通常のトラフィックの送受信が可能になります。 • ForceUnauthorized - 対象ポートは Unauthorized 状態を貫き、すべてのクライアントからの認証要求を無視します。スイッチはインタフェースを通したクライアントの認証サービスを行いません。 • Auto - 802.1X を有効にし、Unauthorized 状態を開始し、ポートにおいて EAPOL フレームのみの送受信を許可します。認証プロセスは、ポートのリンク状態が Down から Up に遷移した時、または EAPOL-start フレームが受信された時に開始されます。スイッチはクライアントの ID を要求し、クライアントと認証サーバとの間で認証メッセージの中継を開始します。（初期値）
Capability	ポートに 802.1X オーセンティケータの設定を適用するために使用します。Authenticator が設定をポートに適用するのを選択してください。 • Authenticator - ユーザは認証プロセスを通過するとネットワークにアクセス可能になります。 • None - 指定ポートは 802.1X 認証機能によって制御されません。
Direction	管理制御するトラフィックの方向（Both または In）を指定します。 • Both - 指定したポートでの入力、出力トラフィックの両方が制御対象となります。 • In - 最初の欄に指定したポートへの入力トラフィックのみ制御対象となります。
Forward EAPOL PDU	EAPOL PDU の転送を制御するポートの設定です。802.1X 機能をグローバルまたはポートに無効とした場合に、802.1X forward PDU がグローバルおよびポートに有効にされると、ポートに受信した EAPOL パケットは同じ VLAN 内で（グローバルまたはそのポートに対して）802.1X forward PDU が有効で 802.1X が無効であるポートにフラッドします。初期値は無効です。
Max User (1-448)	ユーザの最大数を指定します。最大ユーザ数は 448 です。初期値は 16 です。「No Limit」をチェックすると、最大ユーザ数は 448 になります。

「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。
「Apply」ボタンをクリックして行った変更を適用します。

802.1X User Settings（802.1X ユーザ設定）

スイッチのローカルデータベースに様々な 802.1X ユーザを設定します。

Security > 802.1X > 802.1X User Settings の順にメニューをクリックし、以下の画面を表示します。

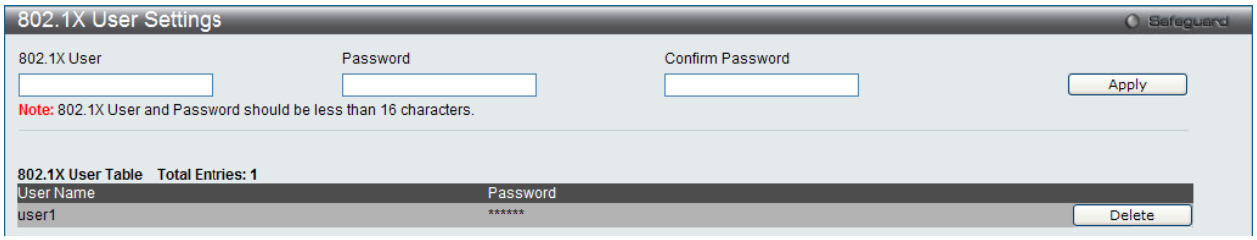


図 12-11 802.1X User Settings 画面

以下の項目を使用して設定を行います。

項目	説明
802.1X User	802.1X ユーザのユーザ名を入力します。
Password	802.1X ユーザのパスワードを入力します。
Confirm Password	802.1X ユーザのパスワードを再度入力します。

「Apply」ボタンをクリックして行った変更を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

注意 802.1X ユーザ名とパスワードは 16 文字以内とします。

Guest VLAN（ゲスト VLAN の設定）

802.1X セキュリティが有効であるネットワークでは、Windows 98 やそれより以前の OS が動作するコンピュータのように適切な 802.1X ソフトウェアの欠落や互換性のないデバイス、またはゲストが限定した権限でネットワークに接続するために 802.1X をサポートしていないデバイスにも限られた範囲でアクセスできる必要があります。本スイッチは、ゲスト 802.1X VLAN 機能を搭載しています。この VLAN には制限付きのアクセス権があり、他の VLAN とは分かれています。

ゲスト 802.1X VLAN を実行するためには、はじめにネットワークに制限付き 802.1X ゲスト VLAN を作成し、この VLAN を有効にします。スイッチへはじめてエントリする際には、スイッチにアクセスするクライアントは、リモート RADIUS サーバまたはフル操作が可能な VLAN 内に設置されているスイッチのローカル認証により認証される必要があります。

認証され、Authenticator が VLAN プレースメント情報を処理した場合、クライアントはフル操作が可能なターゲット VLAN にアクセスを許可され、通常のスイッチ機能がクライアントにサービスを開始します。Authenticator がターゲットの VLAN プレースメント情報を持たない場合、クライアントは元の VLAN に戻されます。クライアントが Authenticator によって認証を拒否されたら、制限付き権限を持つゲスト VLAN に置かれます。以下でゲスト VLAN プロセスについて説明します。

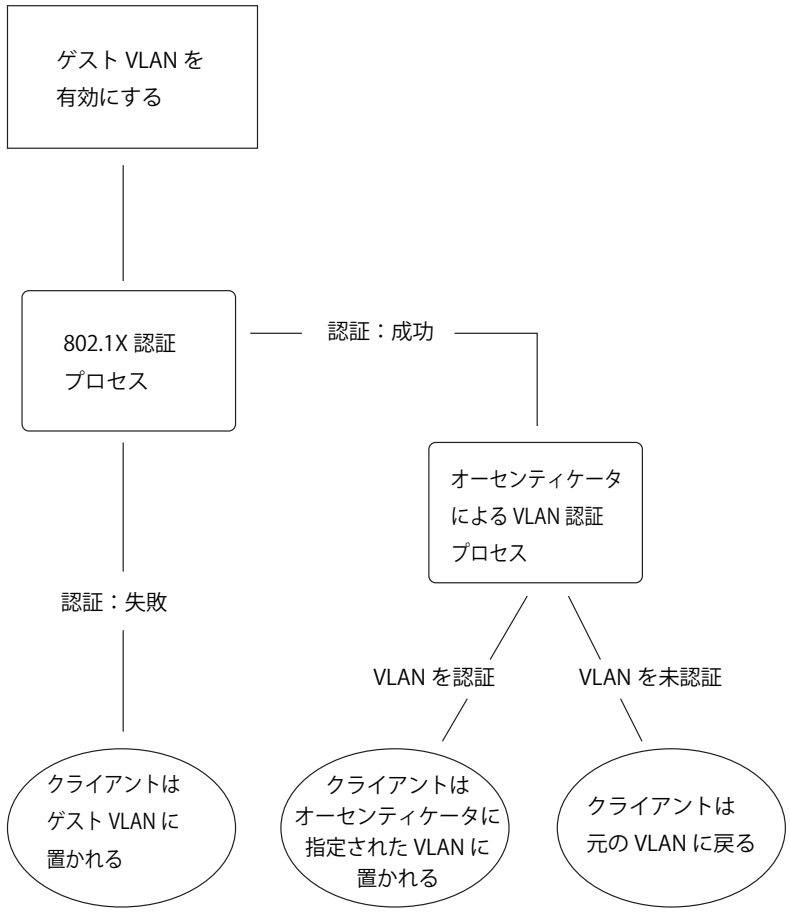


図 12-12　ゲスト VLAN 認証プロセス画面

ゲスト VLAN を使用する場合の制限事項

1. ゲスト VLAN はポートベースの VLAN にのみ対応しています。MAC ベースの VLAN では、本プロセスは行われません。
2. ゲスト VLAN をサポートするポートで GVRP を有効化することはできません。また、GVRP が有効であるポートでゲスト VLAN はサポートできません。
3. ポートはゲスト VLAN とスタティック VLAN の両方に所属することはできません。
4. クライアントがターゲット VLAN に所属を許可されると、ゲスト VLAN にはアクセスできなくなります。
5. ポートが複数の VLAN に所属している場合、ゲスト VLAN には所属できません。

ゲスト VLAN 設定

ゲスト VLAN を設定します。

注意 ゲスト VLAN を設定するためには、ここでゲスト VLAN ステータスを有効にできる VLAN をあらかじめ設定しておく必要があります。

Security > 802.1X > Guest VLAN の順にクリックし、以下の画面を表示します。

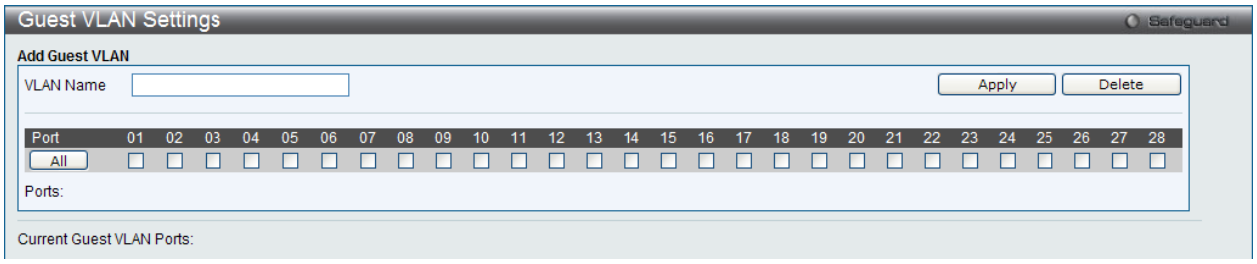


図 12-13 Guest VLAN Settings 画面

以下の項目によりゲスト VLAN を有効にすることができます。

項目	説明
VLAN Name	ゲスト 802.1X VLAN にする定義済みの VLAN 名を入力します。
Port List	ゲスト 802.1X VLAN を有効にするポートを設定します。「All」ボタンをクリックするとすべてのポートを選択します。

「Apply」ボタンをクリックし、設定を有効にします。正しく設定されるとゲスト VLAN 名と対象のポートが画面の下部に表示されます。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

Authenticator State（オーセンティケータの状態）

オーセンティケータの状態を表示します。

Security > 802.1X > Authenticator State の順にメニューをクリックし、以下の画面を表示します。

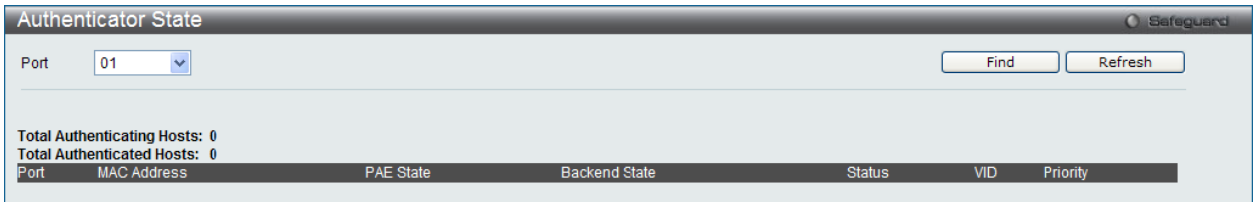


図 12-14 Authenticator State 画面

設定対象となる項目は以下の通りです。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

注意 ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Authenticator Statistics（オーセンティケータ統計情報）

オーセンティケータの統計情報を表示します。

Security > 802.1X > Authenticator Statistics の順にメニューをクリックし、以下の画面を表示します。

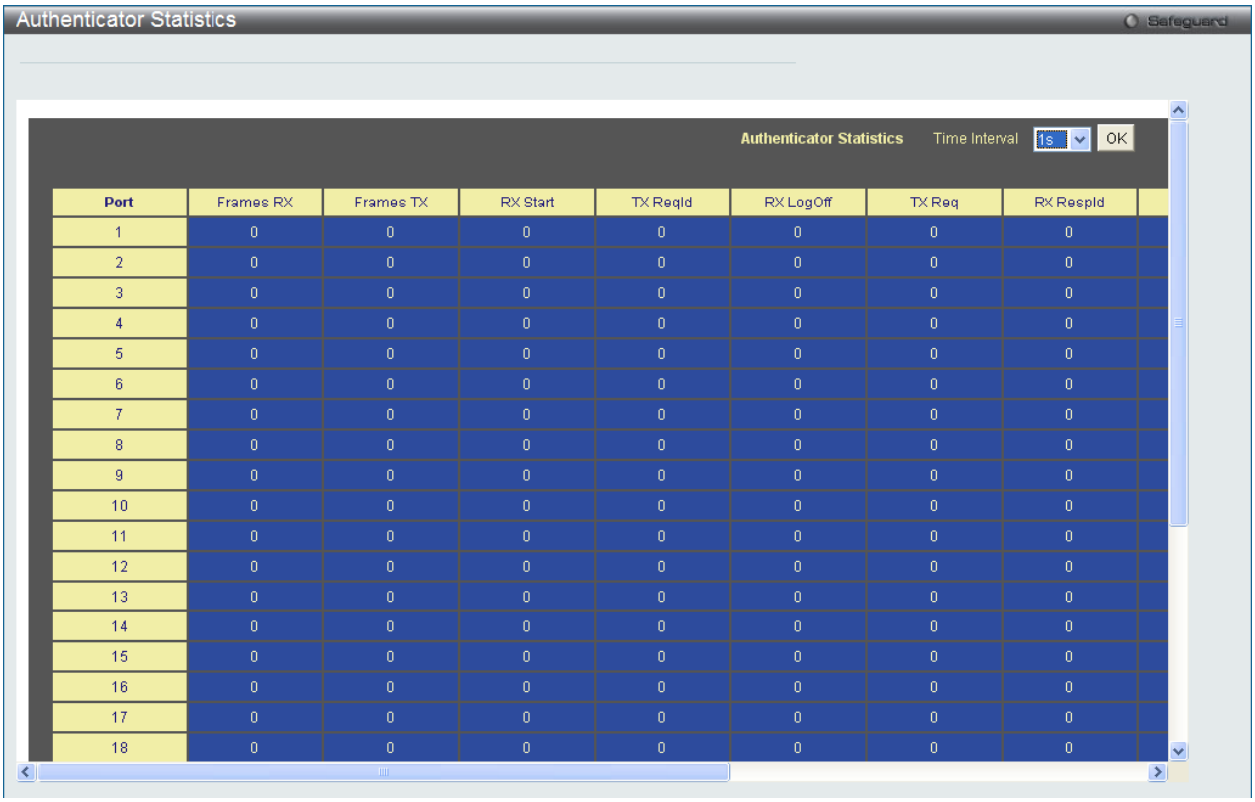


図 12-15　Authenticator Statics 画面

設定対象となる項目は以下の通りです。

項目	説明
Time Interval	プルダウンメニューを使用して、統計情報を更新する間隔を選択します。

「OK」ボタンをクリックして行った変更を適用します。

注意　ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Authenticator Session Statistics（オーセンティケータセッション統計情報）

オーセンティケータセッションの統計情報を表示します。

Security > 802.1X > Authenticator Session Statistics の順にメニューをクリックし、以下の画面を表示します。

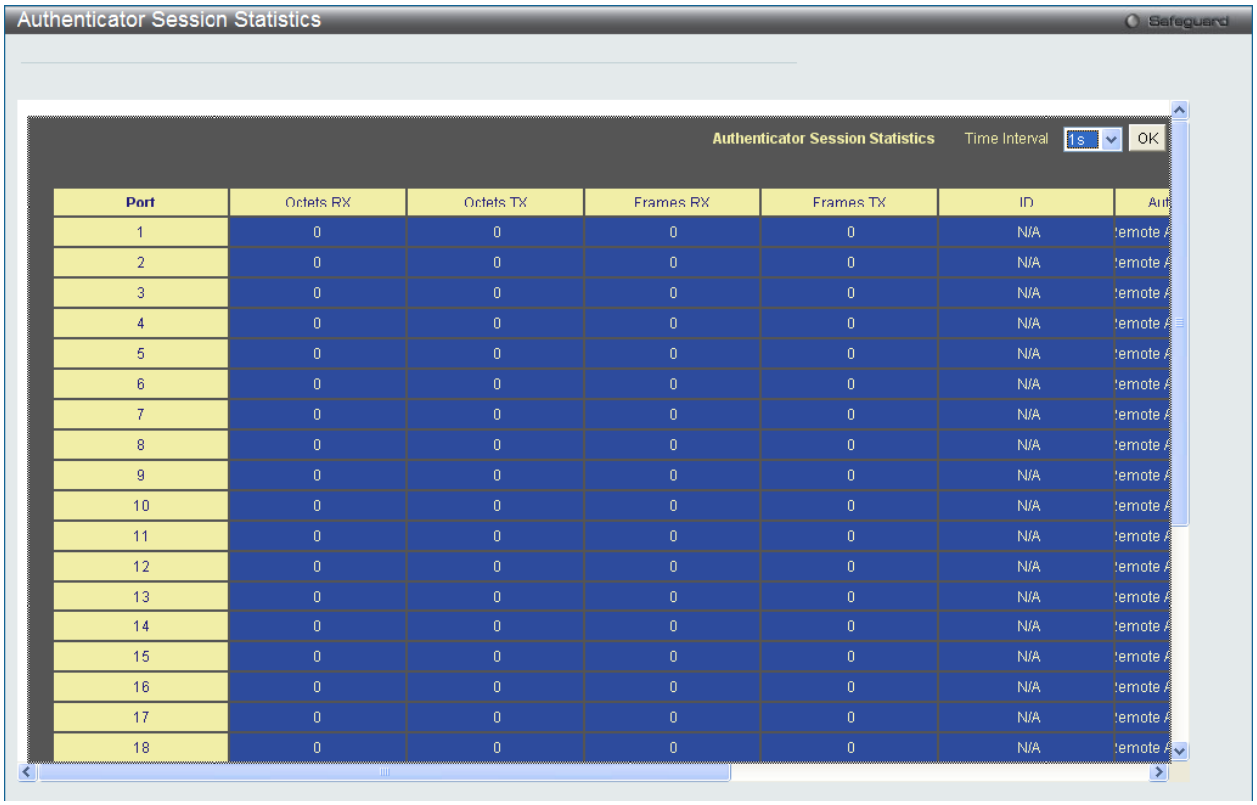


図 12-16　Authenticator Session Statistics 画面

設定対象となる項目は以下の通りです。

項目	説明
Time Interval	プルダウンメニューを使用して、統計情報を更新する間隔を選択します。

「OK」ボタンをクリックして行った変更を適用します。

注意　ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Authenticator Diagnostics（オーセンティケータ診断）

オーセンティケータ診断情報を表示します。

Security > 802.1X > Authenticator Diagnostics の順にメニューをクリックし、以下の画面を表示します。

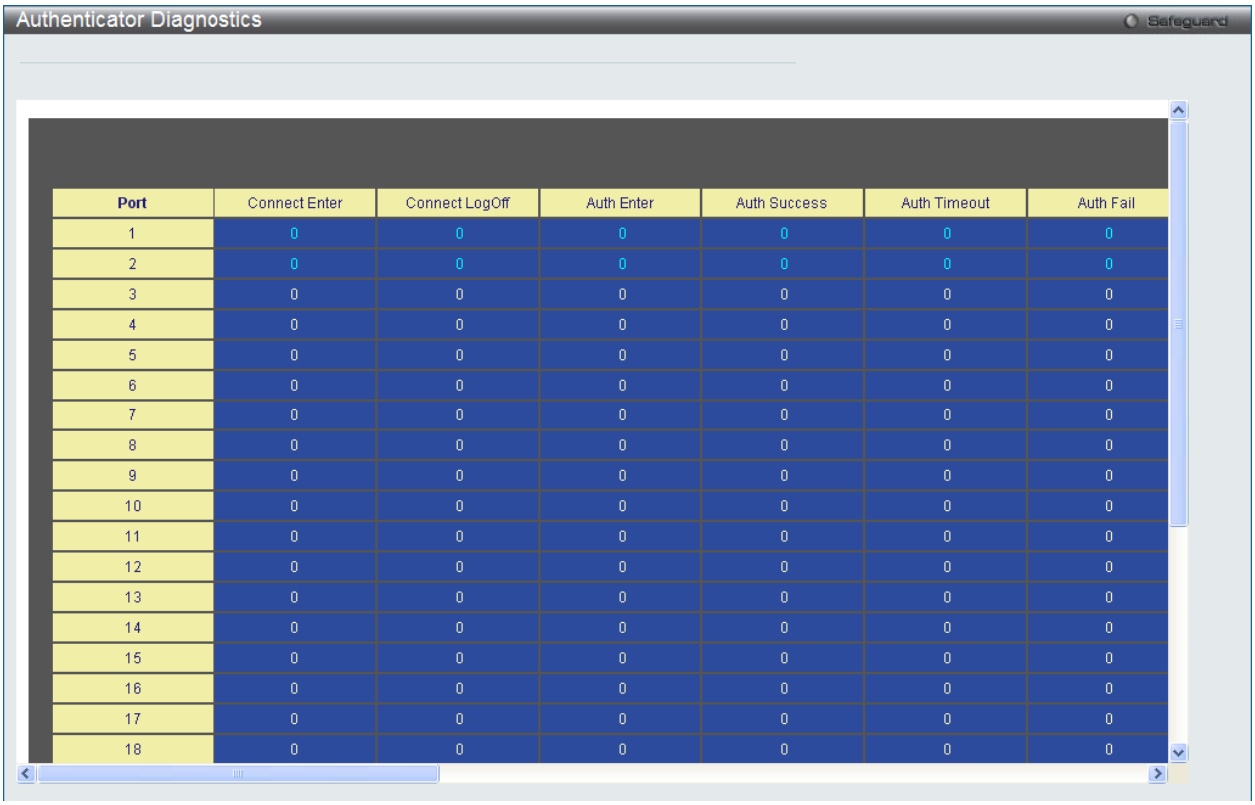


図 12-17　Authenticator Diagnostics 画面

設定対象となる項目は以下の通りです。

項目	説明
Time Interval	プルダウンメニューを使用して、統計情報を更新する間隔を選択します。

「OK」ボタンをクリックして行った変更を適用します。

注意　ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Initialize Port(s)（初期化ポート）

ポート説明文を初期化します。

Security > 802.1X > Initialize Port(s) の順にメニューをクリックします。

「802.1X Global Settings」画面で「Authentication Mode」に「Port-based」を選択していると、以下の画面が表示されます。

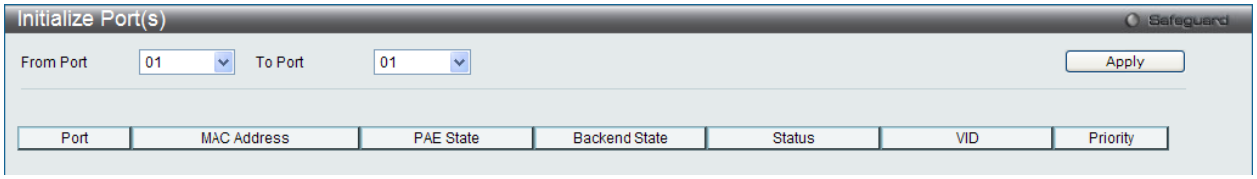


図 12-18 Initialize Port(s) - Port-based 画面

「802.1X Global Settings」画面で「Authentication Mode」に「MAC-based」を選択していると、以下の画面が表示されます。

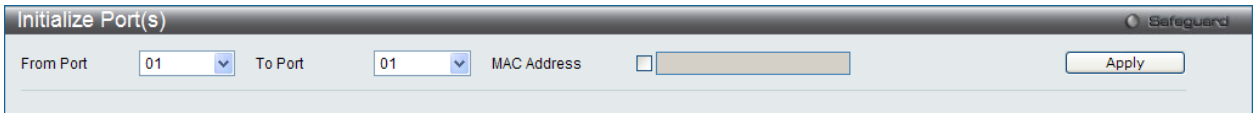


図 12-19 Initialize Port(s) - MAC-based 画面

設定対象となる項目は以下の通りです。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
MAC Address	ボックスをチェックして、対応するポートに接続するクライアントの認証する MAC アドレスを入力します。

「Apply」ボタンをクリックして行った変更を適用します。

注意 ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Reauthenticate Port(s)（再認証ポート）

現在の再認証ポート（ポートベース）を表示します。

Security > 802.1X > Reauthenticate Port-based Port(s) の順にメニューをクリックします。

「802.1X Global Settings」画面で「Authentication Mode」に「Port-based」を選択していると、以下の画面が表示されます。

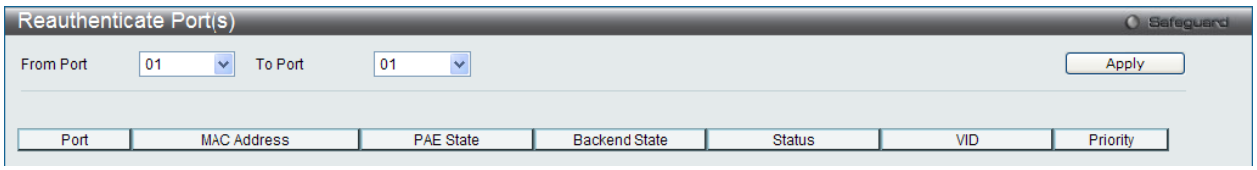


図 12-20 Reauthenticate Port(s) - Port-based 画面

「802.1X Global Settings」画面で「Authentication Mode」に「MAC-based」を選択していると、以下の画面が表示されます。

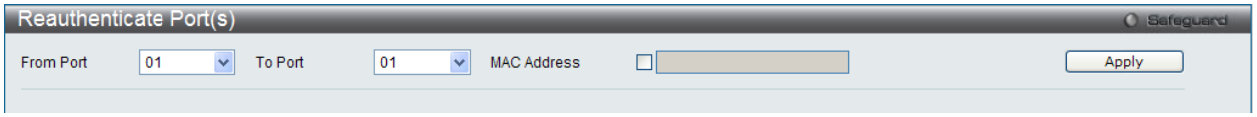


図 12-21 Reauthenticate Port(s) - MAC-based 画面

設定対象となる項目は以下の通りです。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
MAC Address	ボックスをチェックして、対応するポートに接続するクライアントの認証する MAC アドレスを入力します。

「Apply」ボタンをクリックして行った変更を適用します。

注意 ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

RADIUS（RADIUS 設定）

Authentication RADIUS Server Settings（認証 RADIUS サーバ設定）

スイッチの RADIUS 機能は中央集中型のユーザ管理を容易にし、またスニッフィングやハッカーからの攻撃から保護します。

Security > RADIUS > Authentication RADIUS Server の順にメニューをクリックし、以下の画面を表示します。

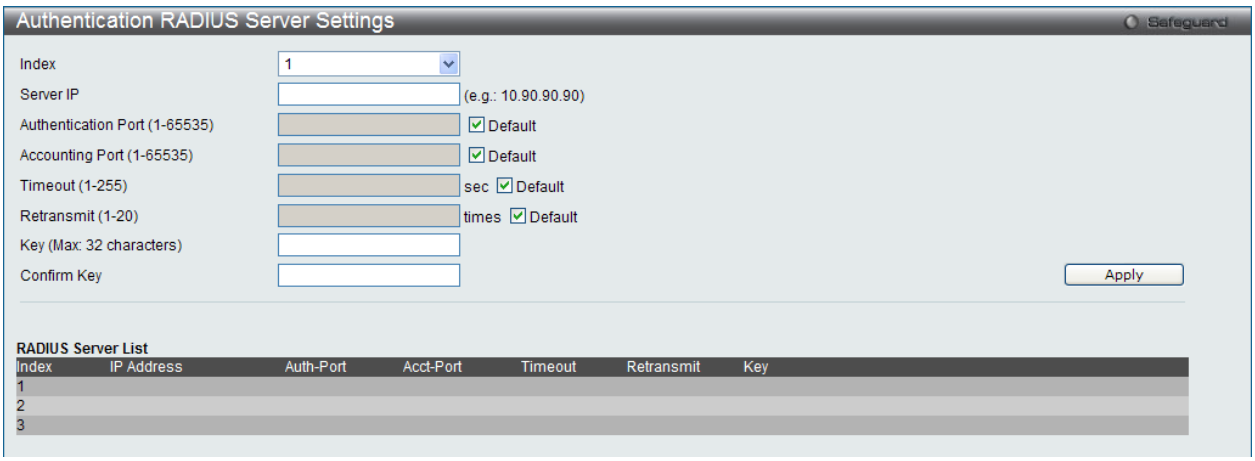


図 12-22　Authentic RADIUS Server Settings 画面

本画面は 2 つのメインセクションに分かれています。上のセクションでは、管理者が RADIUS サーバ設定を行い、下のセクションではシステムに現在設定されている RADIUS サーバの設定を表示します。
使用される項目の説明は以下の通りです。

項目	説明
Index	「1」、「2」、「3」から設定を行う RADIUS サーバを選択します。
Server IP	RADIUS サーバの IP アドレスを入力します。
Authentication Port (1-65535)	スイッチと RADIUS サーバ間で RADIUS 認証データを送信するために使用される RADIUS 認証サーバの UDP ポート番号を指定します。初期値は 1812 です。
Accounting Port (1-65535)	スイッチと RADIUS サーバ間で RADIUS アカウンティング統計情報を送信するために使用される RADIUS 認証サーバの UDP ポート番号を指定します。初期値は 1813 です。
Timeout (1-255)	RADIUS サーバのエージングタイム (秒) を設定します。
Retransmit (1-20)	RADIUS サーバの送信回数を設定します。
Key	RADIUS サーバと同じキーを入力します。
Confirm Key	RADIUS サーバと同じキーを確認のために再度入力します。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. エントリの編集後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

RADIUS Accounting Setting（RADIUS アカウンティング設定）

指定した RADIUS アカウンティングサービスの状態を設定します。

Security > RADIUS > Authentication RADIUS Server の順にメニューをクリックし、以下の画面を表示します。

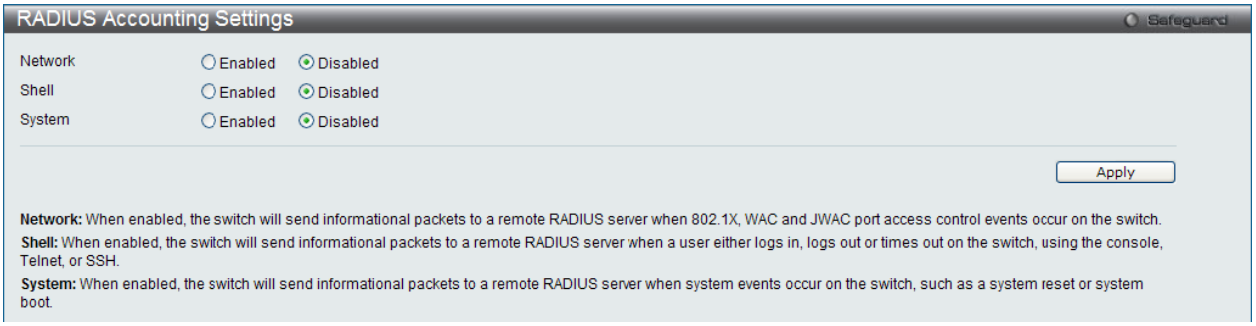


図 12-23　RADIUS Accounting Settings 画面

使用される項目の説明は以下の通りです。

項目	説明
Network	Network- 有効にすると、スイッチは、スイッチに 802.1X にポートアクセスコントロールイベントが発生した場合にリモート RADIUS サーバに情報パケットを送信します。
Shell	有効にすると、スイッチは、コンソール、Telnet、または SSH を使用してスイッチにログイン、ログアウトまたはタイムアウトの場合にリモート RADIUS サーバに情報パケットを送信します。
System	有効にすると、スイッチは、システムリセットやシステムリブートなどのシステムイベントがスイッチに発生した場合にリモート RADIUS サーバに情報パケットを送信します。

「Apply」ボタンをクリックして行った変更を適用します。

RADIUS Authentication（RADIUS 認証）

RADIUS 認証プロトコルでクライアント側の RADIUS 認証クライアントの動作に関連する情報を表示します。

Security > RADIUS > RADIUS Authentication をクリックし、以下の画面を表示します。

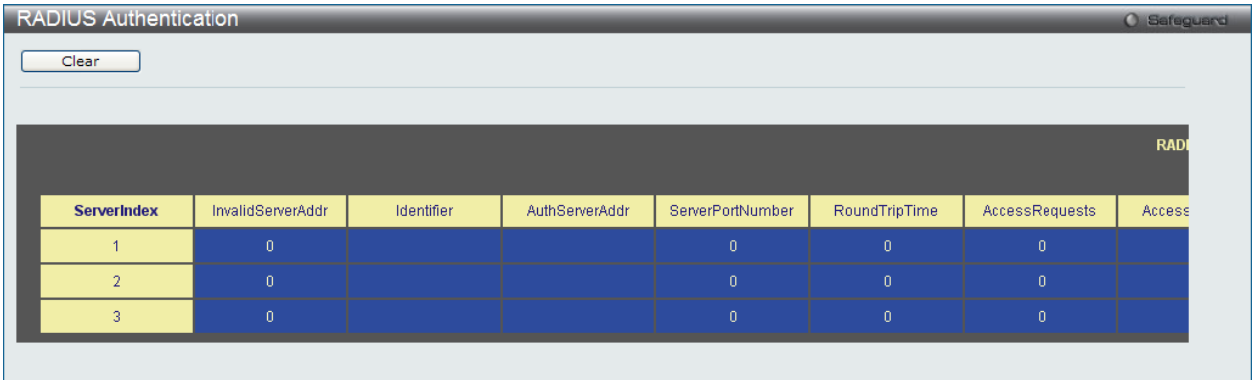


図 12-24 RADIUS Authentication 画面

統計情報の更新間隔を 1s から 60s（s：秒）で選択します。初期値は 1s（1 秒）です。現在の統計情報をクリアするためには左上角の「Clear」ボタンをクリックします。以下の情報が表示されます。

項目	説明
ServerIndex	クライアントが暗号鍵を共有している各 RADIUS 認証サーバに割り当てられた識別子の番号。
InvalidServerAddr	不明なアドレスから受信した RADIUS Access-Response パケット数。
Identifier	RADIUS 認証クライアントの NAS 識別子。（MIB II の sysName と同じである必要はありません。）
AuthServerAddr	クライアントが暗号鍵を共有している RADIUS 認証サーバを一覧にしているテーブル。
ServerPortNumber	クライアントがこのサーバにリクエストを送信するために使用する UDP ポート。
RoundTripTime	最も最近 RADIUS 認証サーバから送信された Access-Reply/Access-Challenge と Access-Request の間隔（1/100 秒単位）。
AccessRequests	サーバに送信された RADIUS Access-Request パケット数。再送信は含まれません。
AccessRetrans	本 RADIUS 認証サーバに再送信された RADIUS Access-Request パケット数。
AccessAccepts	本サーバから受信した RADIUS Access-Accept パケット数（有効 / 無効パケット）。
AccessRejects	本サーバより受信した RADIUS Access-Reject パケット数（有効 / 無効パケット）。
AccessChallenges	本サーバより受信した RADIUS Access-Challenge パケット数（有効 / 無効パケット）。
AccessResponses	本サーバより受信した不正な形式の RADIUS Access-Response パケット数。不正形式のパケットには不正な長さのパケットも含まれます。不正認証、署名属性、または不明なタイプは不正な Access Responses としては含まれません。
BadAuthenticators	本サーバより受信した不正認証や署名属性 RADIUS Access-Response パケット数。
PendingRequests	まだタイムアウトになっていない、またはレスポンスを受信していないこのサーバ行きの RADIUS Access-Request パケット数。この変数は Access-Request が送信されると 1 つ増加し、Access-Accept、Access-Reject または Access-Challenge の受信、タイムアウトまたは再転送時に 1 つ減少します。
Timeouts	本サーバへの認証タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Request としてカウントされます。
UnknownTypes	本サーバから認証ポートに受信した不明なタイプの RADIUS パケット数。
PacketsDropped	本サーバから認証ポートに受信し、何らかの理由で破棄した RADIUS パケット数。

RADIUS Account Client（RADIUS アカウンティングクライアント）

RADIUS Accounting クライアントを管理するために使用する管理オブジェクトとそれらに関連した現在の統計情報を表示します。

Security > RADIUS > RADIUS Accounting Client をクリックし、以下の画面を表示します。

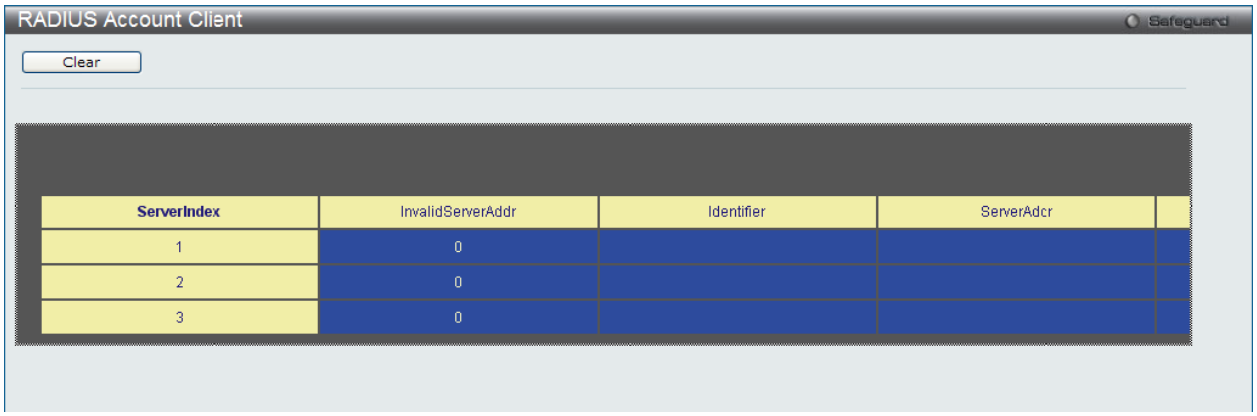


図 12-25　RADIUS Accounting Client 画面

統計情報を更新するためには更新間隔を 1s ～ 60s（s は秒）から指定します。初期値は 1（秒）です。現在の統計情報をクリアするためには左上の「Clear」ボタンをクリックします。以下の情報が表示されます。

項目	説明
ServerIndex	クライアントが暗号鍵を共有する RADIUS Accounting サーバの IP アドレス。
InvalidServerAddr	不明なアドレスから受信した RADIUS Accounting-Response パケット数。
Identifier	RADIUS アカウンティングクライアントの NAS 識別子。（MIB II の sysName と同じである必要はありません。）
ServerAddress	クライアントが暗号鍵を共有している RADIUS アカウンティングサーバを一覧にしているテーブル。
ServerPortNumber	クライアントがこのサーバにリクエストを送信するために使用する UDP ポート。
RoundTripTime	RADIUS アカウンティングサーバからクライアントに送信される最も新しい Accounting-Response と Accounting-Request の間隔。
Requests	送信された RADIUS Accounting-Request パケット数。これは再転送のパケット数は含まれていません。
Retransmissions	RADIUS アカウンティングサーバに再送された RADIUS Accounting-Request 数。再送には、同じものが残るような Identifier および Acct-Delay が更新されるというリトライも含まれます。
Responses	本サーバから Accounting ポートに受信した RADIUS パケット数。
MalformedResponses	このサーバから受信した不正な形式の RADIUS Accounting-Response パケット数。Malformed packets には不正な長さのパケットを含まれます。認証エラーや不明なタイプは不正な accounting responses としては含まれません。
BadAuthenticators	このサーバから受信した不正な認証を含む RADIUS Accounting-Response パケット数。
PendingRequests	まだタイムアウトになっていない、またはレスポンスを受信していないサーバ行きの RADIUS Accounting-Request パケット数。この変数は Accounting-Request が送信された時に 1 つ加算し、Accounting-Response の受信、タイムアウトまたは再転送時に 1 つ減少します。
Timeouts	このサーバへの Accounting タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Accounting-Request としてカウントされます。
UnknownTypes	このサーバから Accounting ポートに受信した不明なタイプの RADIUS パケット数。
PacketsDropped	このサーバから Accounting ポートに受信し、何らかの理由で破棄した RADIUS パケット数。

IP-MAC-Port Binding（IMPB : IP-MAC- ポートバインディング）

IP ネットワークレイヤ（IP レベル）では 4 バイトのアドレスを使用し、イーサネットリンクレイヤ（データリンクレベル）では 6 バイトの MAC アドレスを使用します。これらの 2 つのアドレスタイプを結合させることにより、レイヤ間のデータ転送を可能にします。IP-MAC- ポートバインディングの第一の目的は、スイッチにアクセスする認可ユーザ数を制限することです。IP/MAC アドレスのペアを、事前に設定したデータベースと比較を行うことで、認証クライアントはスイッチのポートアクセスできるようになります。また、DHCP Snooping を有効にすると、スイッチは、DHCP パケットを検索し、IMPB ホワイトリストにそれらを保存することで自動的に IP/MAC アドレスのペアを学習します。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。DES-3200 シリーズでは、アクティブ、インアクティブエントリは同じデータベースを使用します。作成できるエントリの最大数は 510 です。最大 255 エントリだけがその時々でアクティブとなります。認証クライアントのリストは、CLI または Web により手動で作成できます。本機能はポートベースであるため、ポートごとに本機能を有効 / 無効にすることができます。

IMPB Global Settings（IMPB グローバル設定）

スイッチのグローバルな IP-MAC- ポートバインディング設定（トラップログステータスおよび DHCP Snoop ステータス）を有効または無効にするのに使用します。「Trap/Log」欄では、IP-MAC- ポートバインディングのトラップログメッセージ送信を有効または無効にします。有効にすると、スイッチはスイッチに設定された IP-MAC バインディング - ポートに一致しない ARP パケットを受信した場合に、SNMP エージェントとスイッチログにトラップログメッセージを送信します。

Security > IP-MAC-Port Binding (IMPB) > IMPB Global Settings の順にメニュークリックして、以下の画面を表示します。

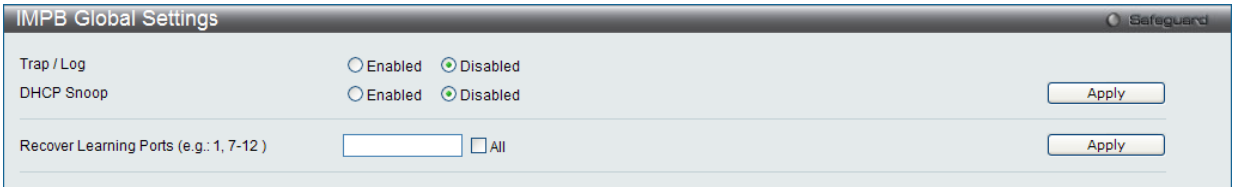


図 12-26　IMPB Global Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
Trap/Log	IP-MAC- ポートバインディングのトラップログメッセージ送信を有効または無効にします。有効にすると、スイッチはスイッチに設定された IP-MAC バインディングに一致しない ARP パケットを受信した場合に、SNMP エージェントとスイッチログにトラップログメッセージを送信します。初期値は「Disabled」です。
DHCP Snooping	IP-MAC- ポートバインディングの DHCP Snooping オプションを「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Recover Learning Ports	学習状態を回復するポート番号を選択します。「All」をチェックすると、すべての学習ポートのリカバリを行います。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

IMPB Port Settings（IMPB ポート設定）

ポートベースで IP-MAC- ポートバインディング設定を行います。

Security > IP-MAC-Port Binding (IMPB) > IMPB Port Settings の順にメニューをクリックし、以下の画面を表示します。

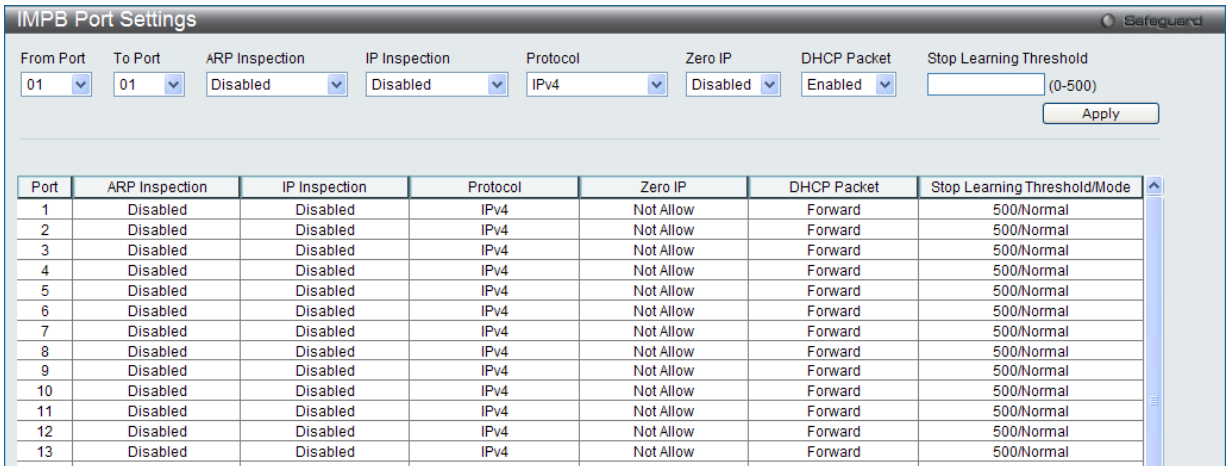


図 12-27　IMPB Port Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
From Port/To Port	IP-MAC- ポートバインディングを設定する対象のポートを指定します。
ARP Inspection	ARP 検証機能が有効な場合、正しい ARP パケットは転送され、一方不正なパケットは破棄されます。 • Disabled - ARP 検証機能を無効にします。 • Enabled (Strict) - 本モードはハードウェアによる MAC アドレスの学習を無効にします。本モードでは、正しい ARP または IP パケットが検出されるまで、すべてのパケットが初期値で破棄されます。本モードを有効にすると、スイッチはポートの破棄 FDB エントリの記載を停止します。正しいパケットを検出した場合は、スイッチは FDB エントリを記載する必要があります。 • Enabled (Loose) - 本モードでは、不正な ARP またはブロードキャスト IP パケットが検出されるまで、初期値ですべてのパケットを転送します。初期値は「Disabled」（無効）です。
IP Inspection	ARP と IP 検証の両方を有効にすると、すべての IP パケットがチェックされます。正しい IP パケットは転送され、一方不正なパケットは破棄されます。IP 検証が有効で、ARP 検証が無効である場合、IP でない全パケット（例 L2 パケット、または ARP）が初期値で送信されます。初期値は「Disabled」（無効）です。
Protocol	プルダウンメニューを使用してプロトコルを選択します。
Zero IP	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。「Allow zero IP」を設定すると、ステートが 0.0.0.0 送信元 IP の ARP パケットを許容します。
DHCP Packet	初期設定では、ブロードキャスト DA の DHCP パケットをフラッドします。無効にすると、指定ポートが受信したブロードキャスト DHCP パケットは、「strict」モードでは転送されません。本設定は、CPU がトラップした DHCP パケットをソフトウェアが転送する必要がある時、DHCP Snooping で有効である場合に効果があります。本設定はこの状況における転送の実行を制御します。
Stop Learning Threshold	ポートにおいてブロックされるエントリ数を表示します。初期値は 500 です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

IMPB Entry Settings（IMPB エントリ設定）

スイッチにスタティック IP-MAC- ポートバインディングエントリを作成します。

Security > IP-MAC-Port Binding (IMPB) > IMPB Entry Settings の順にメニューをクリックし、以下の画面を表示します。

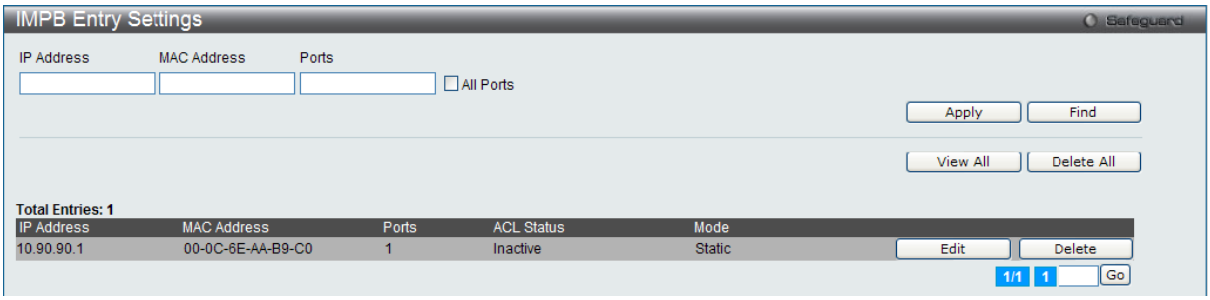


図 12-28　IMPB Entry Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
IP Address	チェックして MAC アドレスにバインドする IP アドレスを入力します。
MAC Address	IP アドレスとバインドする MAC アドレスを入力します。
Ports	本IP-MACバインディングエントリ(IPアドレス+MACアドレス)を設定する対象のポートを指定します。「All Ports」を選択すると、スイッチのすべてのポートに設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

エントリの追加

1. 「IP Address」、「MAC Address」および「Ports」にバインドする IP アドレス、MAC アドレスおよびポートを入力します。
2. 「Apply」ボタンをクリックします。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックし、編集画面を表示します。
2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

エントリの検索

検索する項目を入力し、「Find」ボタンをクリックします。

すべてのエントリの表示

「View All」ボタンをクリックします。

エントリの削除

エントリの「Delete」ボタンをクリックします。すべてのエントリを削除する場合は、「Delete All」ボタンをクリックします。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

MAC Block List（MAC ブロックリスト）

IP-MAC バインディング機能によりブロックされた未承認のデバイスを参照します。

Security > IP-MAC-Port Binding (IMPB) > MAC Block List の順にメニューをクリックして、以下の画面を表示します。

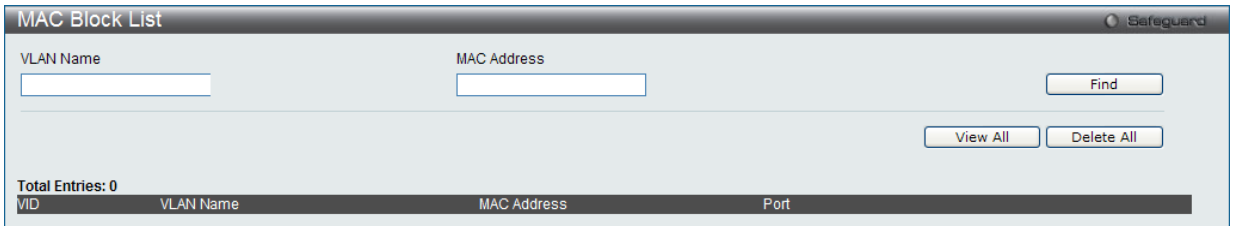


図 12-29 MAC Block List 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
VLAN Name	検出または削除する VLAN の VLAN 名を入力します。
MAC Address	検出または削除する MAC アドレスを入力します。

VIP-MAC バインディング機能によりブロックされた未承認デバイスの検索

「VLAN ID」と「MAC Address」を入力し、「Find」ボタンをクリックします。

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。テーブル内のすべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの表示

すべてのエントリを表示するためには、「View All」ボタンをクリックします。

DHCP Snooping（DHCP Snooping 設定）

DHCP Snooping Maximum Entry Settings（DHCP Snooping 最大エントリ設定）

DHCP Snooping の最大エントリをポートに設定します。

Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Maximum Entries の順にクリックして、以下の画面を表示します。

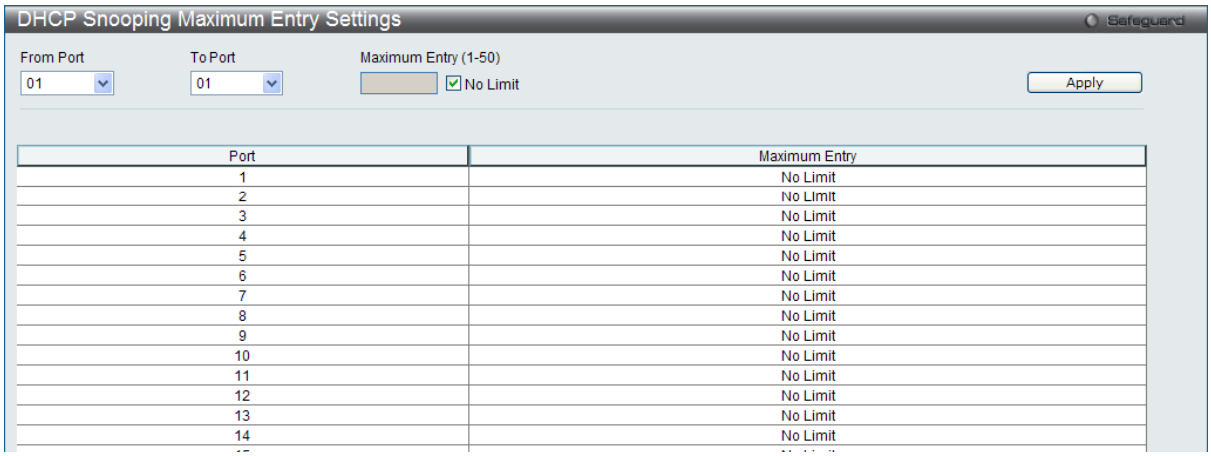


図 12-30 DHCP Snooping Maximum Entry Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
From Port / To Port	使用するポート範囲を選択します。
Maximum Entry (1-50)	最大エントリ数を入力します。「No Limit」をチェックすると学習するエントリの最大数になります。

「Apply」ボタンをクリックして行った変更を適用します。

DHCP Snooping Entry（DHCP Snooping エントリ）

特定ポートのダイナミックエントリを表示します。

Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Entry の順にクリックして、以下の画面を表示します。

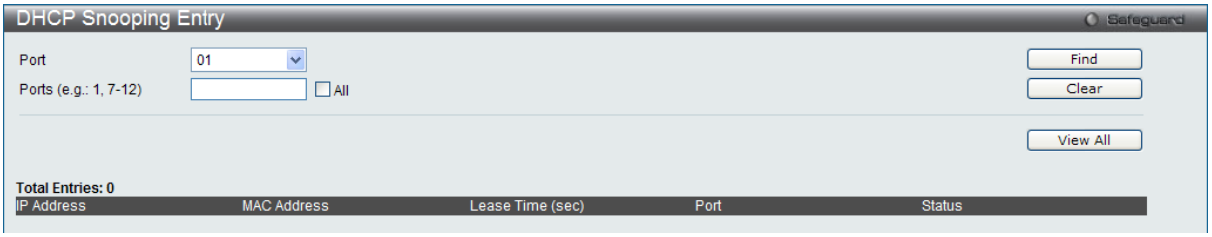


図 12-31 DHCP Snooping Entry 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
Port	プルダウンメニューで希望するポートを選択します。
Ports	DHCP Snooping エントリを表示するポートを指定します。 • All - すべてのポートの全エントリを選択します。

特定ポートの設定の表示
ポート番号を入力して「Find」ボタンをクリックします。

すべてのエントリの表示
「View All」ボタンをクリックします。

エントリの削除
「Clear」ボタンをクリックします。

MAC-based Access Control（MAC ベースアクセスコントロール）

MAC ベースアクセスコントロールは、ポートまたはホストを使用してアクセスを認証および認可する方式です。本方式では、ポートベースの MAC にはポートアクセス権を決定し、一方ホストベースの MAC には MAC アクセス権を決定します。ネットワークへのアクセスを許可する前に MAC ユーザが認証される必要があります。

本スイッチは、ローカル認証とリモート RADIUS サーバ認証の両方の方法をサポートしています。MAC ベースアクセスコントロールでは、ローカルデータベースまたは RADIUS サーバデータベース内の MAC ユーザ情報が認証のために検索されます。認証結果に基づいて、ユーザは異なるレベルの許可を取得します。

MAC ベースアクセスコントロールに関する注意

MAC ベースアクセスコントロールに関するいくつかの制限と規則があります。

1. 本機能がポートで有効になると、スイッチはそのポートの FDB をクリアします。
2. ポートが、ゲスト VLAN ではない VLAN で MAC アドレスをクリアする権利を認められている場合、そのポート上の他の MAC アドレスは、アクセスのために認証されている必要があり、そうでない場合、スイッチにブロックされます。
3. リンクアグリゲーション、およびポートセキュリティが有効なポートは、MAC ベースアクセスコントロールを有効にすることはできません。
4. GVRP 認証が有効なポートをゲスト VLAN で有効にすることはできません。

MAC-based Access Control Settings（MAC ベースアクセスコントロール設定）

スイッチの MAC ベースアクセスコントロール機能にパラメータを設定します。動作状態、認証方式、RADIUS パスワードの設定、およびスイッチの MAC ベースアクセスコントロール機能に関連するゲスト VLAN 設定の参照を行います。また、ポートの MAC ベースアクセスコントロール機能を有効または無効にします。以前に記述した他の機能で有効とされているポートは、MAC ベースアクセスコントロールを使用できないことにご注意ください。

Security > MAC-based Access Control (MAC) > MAC-based Access Control Settings の順にメニューをクリックし、以下の画面を表示します。

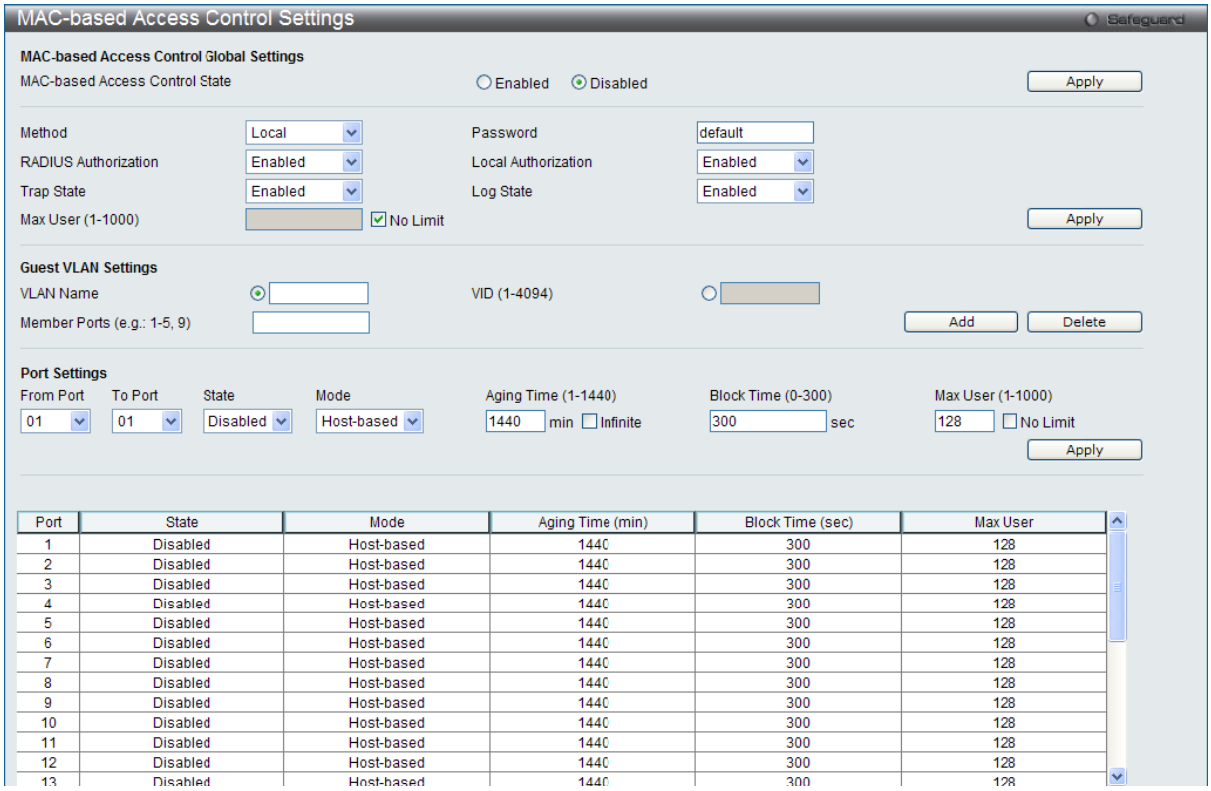


図 12-32　MAC-based Access Control Settings 画面

以下の項目を参照、または設定可能です。

項目	説明
MAC-based Access Control Global Settings	
MAC-based access control State	「Enabled」（有効）または「Disabled」（無効）を選択し、スイッチの MAC ベースアクセスコントロールをグローバルに設定します。
Method	認証 MAC アドレスがポートにある場合、認証タイプをプルダウンメニューで選択します。認証タイプは以下の通りです。 • Local - MAC ベースアクセスコントロールのオーセンティケータとしてローカルに設定された MAC アドレスデータベースを利用します。この MAC アドレスリストは、「MAC-Based Access Control Local Database Settings」画面で設定します。 • RADIUS - MAC ベースアクセスコントロールのオーセンティケータとしてリモート RADIUS サーバを利用します。
Password	認証リクエストのパケットを送信するために使用する RADIUS サーバのパスワードを入力します。初期値は「default」です。
RADIUS Authorization	RADIUS 認証を有効または無効にします。
Local Authorization	ローカル認証を有効または無効にします。
Trap State	トラップの状態を「Enabled」（有効）または「Disabled」（無効）にします。
Log State	ログの状態を「Enabled」（有効）/「Disabled」（無効）にします。
Max User (1-1000)	スイッチの最大ユーザ数を指定します。「No Limit」を選択すると、ユーザの最大数は 1000 になります。
Guest VLAN Settings	
VLAN Name	本機能に使用される設定済みのゲスト VLAN 名を入力します。
VID (1-4094)	先頭のラジオボタンをクリックしてゲスト VLAN ID を入力します。
Member Ports	ゲスト VLAN に設定するポートリストを入力します。
Port Settings	
From Port / To Port	MAC ベースアクセスコントロールに設定するポート範囲を指定します。
State	本画面の「Port Settings」セクションで選択したポートまたはポート範囲の MAC ベースアクセスコントロール有効または無効にします。
Mode	「Port-based」または「Host-based」を選択します。
Aging Time (1-1440)	1-1440（分）の範囲で指定します。初期値は 1440 です。エージングタイムを無効にするためには、「Infinite」オプションを選択します。
Block Time (0-300)	1-300（秒）の範囲で指定します。初期値は 300 です。
Max User (1-1000)	本設定に使用する最大ユーザ数を指定します。「No Limit」を選択すると、ユーザの最大数は 1000 になります。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

MAC-based Access Control Local Settings（MAC ベースアクセスコントロール ローカル設定）

スイッチに対して認証されるターゲット VLAN と MAC アドレスリストを設定します。MAC アドレスのクエリが本テーブルに一致すると、MAC アドレスは、関連する VLAN に置かれます。スイッチ管理者は、ここで設定された local 方式を使用して、認証する最大 128 個の MAC アドレスを入力することができます。

Security > MAC-based Access Control (MAC) > MAC-based Access Control Local Settings をクリックし、以下の画面を表示します。

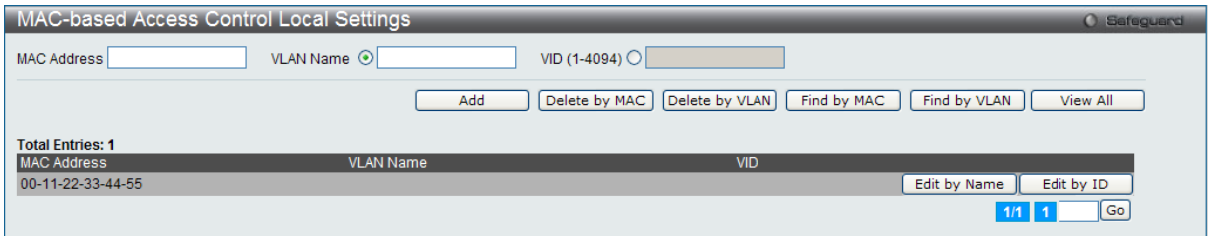


図 12-33　MAC-based Access Control Local Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
MAC Address	ローカル認証リストに追加する MAC アドレスを入力します。
VLAN Name	MAC アドレスに対応する VLAN 名を入力します。
VID (1-4094)	MAC アドレスに対応する VLAN ID を入力します。

MAC アドレスリストへの新規登録

MAC アドレスをローカル認証リストに追加するためには、「MAC Address」と「VLAN Name」/「VID」に MAC アドレスとターゲット VLAN 名 / VLAN ID をそれぞれ入力し、「Add」ボタンをクリックします。

MAC アドレスリストの検出

「Find by MAC」ボタンをクリックして、入力した MAC アドレスに基づく特定のエントリを検出します。また、「Find by VLAN」ボタンをクリックして、入力した VLAN 名または VLAN ID に基づく特定のエントリを検出します。

MAC アドレスリストの参照

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

MAC アドレスエントリの削除

「Delete by MAC」ボタンをクリックして、入力した MAC アドレスに基づいて指定エントリを削除します。または、「Delete by VLAN」ボタンをクリックして、入力した VLAN 名または VLAN ID に基づいて指定エントリを削除します。

MAC アドレスリストの変更

選択した MAC アドレスの VLAN 名を変更するためには、「Edit by Name」ボタンをクリックし、以下の画面を表示します。

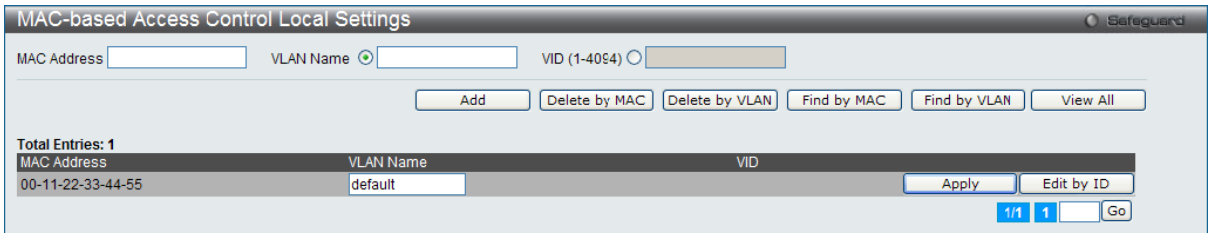


図 12-34　Edit by VLAN Name 画面

選択した MAC アドレスの VID 変更するためには、「Edit by ID」ボタンをクリックします。

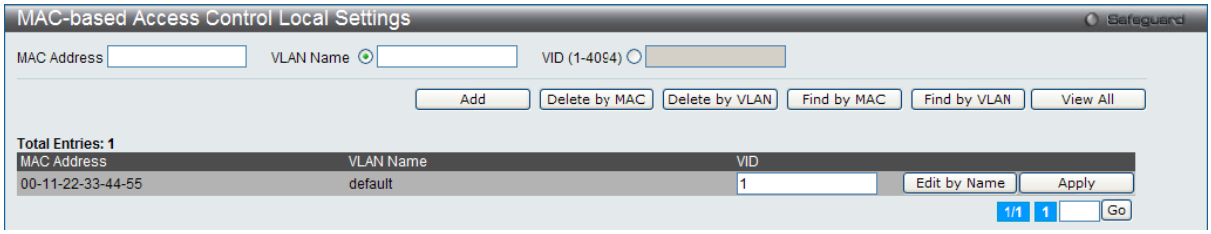


図 12-35　Edit by VID 画面

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

MAC-based Access Control Authentication State（MAC ベースアクセスコントロールの認証状態）

MAC ベースアクセスコントロールの認証情報を表示します。

Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State をクリックし、以下の画面を表示します。

図 12-36 MAC-based Access Control Authentication State

以下の項目を使用して、設定または編集を行います。

項目	説明
Port List	本設定に使用するポートリストを指定します。

MAC ベースアクセスコントロールの認証状態の情報を表示するためには、ポート番号を入力し、「Find」ボタンをクリックします。
「Clear by Port」ボタンをクリックして、入力したポートにリンクするすべての情報をクリアします。
「View All Hosts」ボタンをクリックして、すべての定義済みホストを表示します。
「Clear All Hosts」ボタンをクリックして、すべての定義済みホストをクリアします。

Compound Authentication（コンパウンド認証）

認証 DB フェールオーバとしてのコンパウンド認証を設定します。

Compound Authentication Settings（コンパウンド認証設定）

認証 DB フェールオーバとしてのコンパウンド認証方式の設定を行います。

Security > Compound Authentication > Compound Authentication Settings の順にメニューをクリックし、以下の画面を表示します。

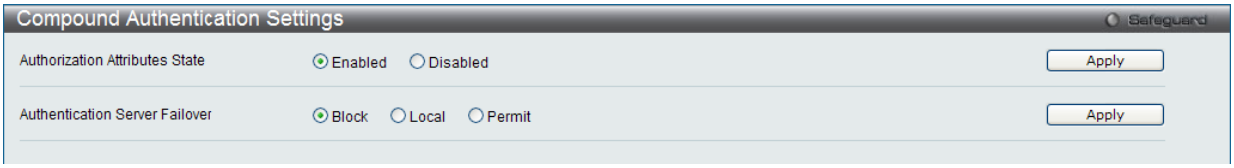


図 12-37 Compound Authentication Settings 画面

スイッチの各ポートにコンパウンド認証を設定するには、以下の項目を指定します。

項目	説明
Authorization Attributes State	認可ネットワーク状態を有効または無効にします。
Authentication Server Failover	認証サーバが応答しなかった場合のフェイルオーバ機能を設定します。 • Local - スイッチは、クライアントを認証するためにローカルデータベースを使用します。クライアントがローカル認証に失敗すると、クライアント未認証ユーザとみなされます。 • Permit - クライアントは、認証済みユーザとして扱われます。ゲスト VLAN が有効であると、クライアントはゲスト VLAN にとどまり、そうでない場合、オリジナルの VLAN にとどまります。 • Block - クライアントは未認証ユーザとして扱われます。(初期値)

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Port Security（ポートセキュリティ）

Port Security Settings（ポートセキュリティの設定）

ポートやポート範囲を指定して、ダイナミックなMACアドレス学習をロックすることにより、MACアドレスフォワーディングテーブルへ、新しいソース MAC アドレスが追加されないよう設定することができます。「Admin State」のプルダウンメニューで「Enabled」を選択し、「Apply」ボタンをクリックするとポートをロックできます。

ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

Security > Port Security > Port Security Settings の順にクリックし、以下の画面を表示します。

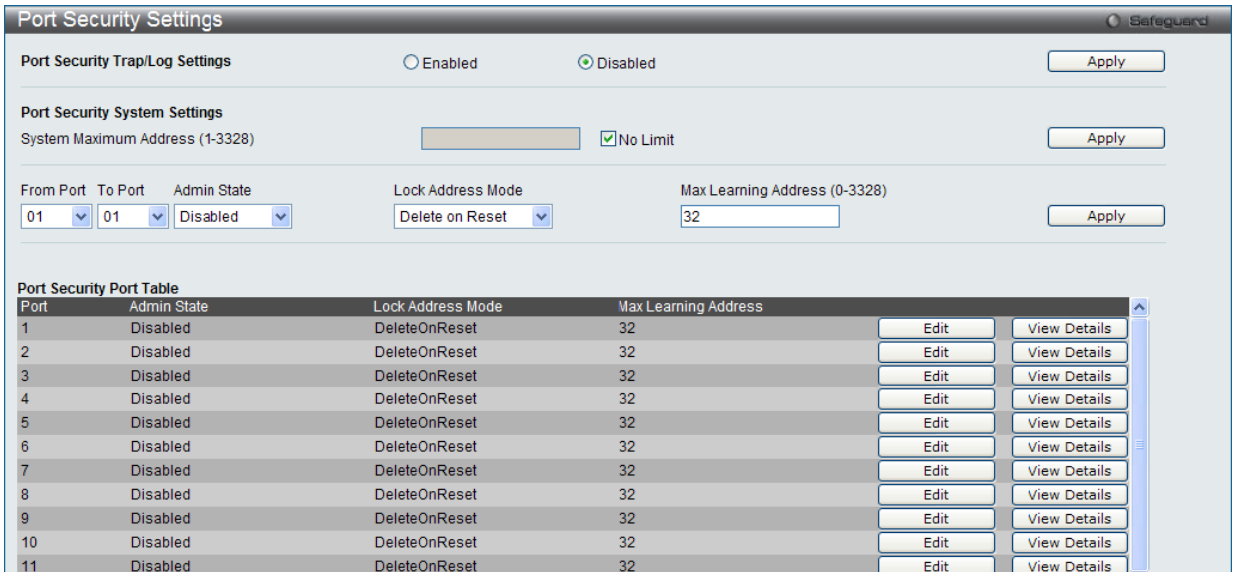


図 12-38　Port Security Settings 画面

本画面には次の項目があります。

項目	説明
Port Security Trap/Log Settings	スイッチのポートセキュリティトラップとログ設定を「Enabled」（有効）または「Disabled」（無効）にします。
System Maximum Address (1-3328)	システムの最大アドレス数を入力します。「No Limit」をチェックすると、無制限になります。
From Port / To Port	ポートセキュリティ項目を表示するポート範囲を選択します。
Admin State	ポートセキュリティの有効 / 無効をプルダウンメニューで指定します。「Enabled」にすると、該当ポートは MAC アドレステーブルがロックされます。
Lock Address Mode	プルダウンメニューでスイッチの選択ポートグループに対して MAC アドレステーブルのロック動作の詳細を指定します。オプションは以下の通りです。 • Permanent – ロックされたアドレスは、リセットされるまでエージアウトしません。 • Delete On Timeout – ロックされたアドレスは、エージングタイム経過後に削除されます。 • Delete On Reset – ロックされたアドレスはリセットか再起動されるまで削除されません。
Max Learning Address (0-3328)	本ポートが学習できるポートセキュリティエントリの最大数を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

指定エントリの参照

「View Detail」ボタンをクリックし、以下の画面を表示します。

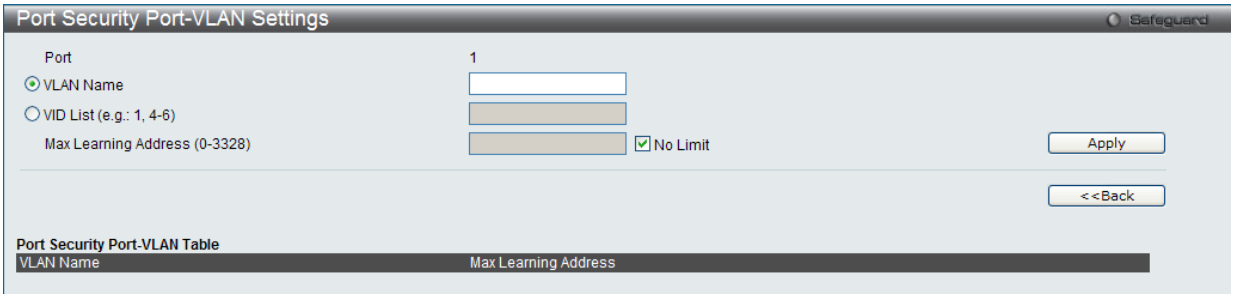


図 12-39 Port Security Port-VLAN Settings 画面

本画面には次の項目があります。

項目	説明
VLAN Name	ラジオボタンをクリックしてポートセキュリティ設定を表示する VLAN 名を入力します。
VID List	ラジオボタンをクリックしてポートセキュリティ設定を表示する VLAN ID リストを入力します。
Max Learning Address (0-3328)	VLAN が学習できるポートセキュリティエントリの最大数を指定します。「0」は、本 VLAN で MAC アドレスの学習が行われないことを意味します。設定が VLAN ポートで現在学習したエントリ数より小さいと、コマンドは拒否されます。「No Limit」をチェックすると、システムが学習できるポートセキュリティエントリの最大数を制限しません。初期値は「No Limit」です。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

Port Security VLAN Settings（ポートセキュリティ VLAN 設定）

指定 VLAN で学習されるポートセキュリティエントリの最大数を指定します。

Security > Port Security > Port Security VLAN Settings の順にクリックし、以下の画面を表示します。

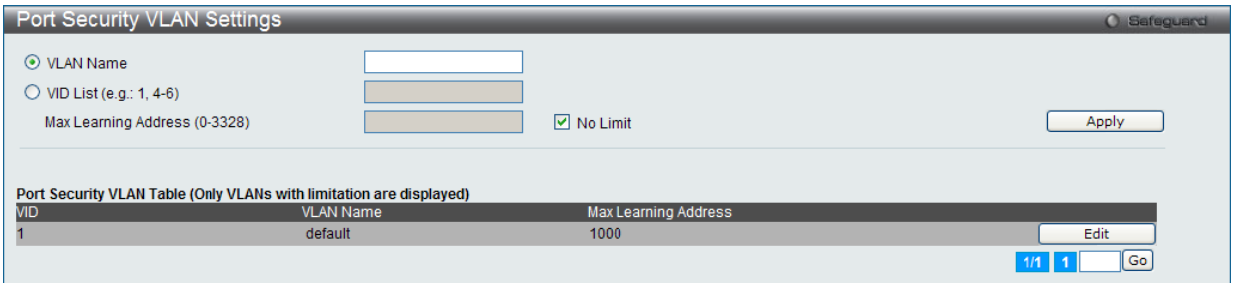


図 12-40 Port Security VLAN Settings 画面

本画面には次の項目があります。

項目	説明
VLAN Name	VLAN 名を入力します。
VID List	VLAN リストを指定します。
Max Learning Address (0-3328)	VLAN が学習できるポートセキュリティエントリの最大数を指定します。「No Limit」をチェックすると、VLAN が学習できるポートセキュリティエントリの最大数を制限しません。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

Port Security Entries（ポートセキュリティエントリ）

スイッチが学習して転送データベースに登録したポートセキュリティエントリからエントリを削除します。

Security > Port Security > Port Security Entries の順にメニューをクリックし、以下の画面を表示します。

図 12-41　Port Security Entries 画面

この画面では以下の情報を表示できます。

項目	説明
VLAN Name	スイッチの転送データベーステーブルに登録されているエントリの VLAN 名です。
VID List	スイッチの転送データベーステーブルに登録されているエントリの VLAN ID です。
Port List	ポートセキュリティエントリ検索に使用するポート番号（リスト）を入力します。「All」を選択すると、設定されているすべてのポートを表示します。
MAC Address	スイッチの転送データベーステーブルに登録されているエントリの MAC アドレスを表示します。
Lock Mode	転送データベーステーブルに登録されている MAC アドレスの種類を表示します。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリのクリア

「Clear」ボタンをクリックして、入力した情報に基づいてすべてのエントリを削除します。
「Clear All」ボタンをクリックして、表示されたすべてのエントリを削除します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）

保護されたゲートウェイに対する MAC のなりすましを防止するためにスプーフィング防止エントリを設定します。エントリが作成されると、送信側 IP がエントリのゲートウェイ IP に一致するが、送信側 MAC フィールドまたは送信元 MAC フィールドがエントリのゲートウェイ MAC に一致しない ARP パケットは、システムによって破棄されます。

Security > ARP Spoofing Prevention Settings の順にメニューをクリックし、以下の画面を表示します。

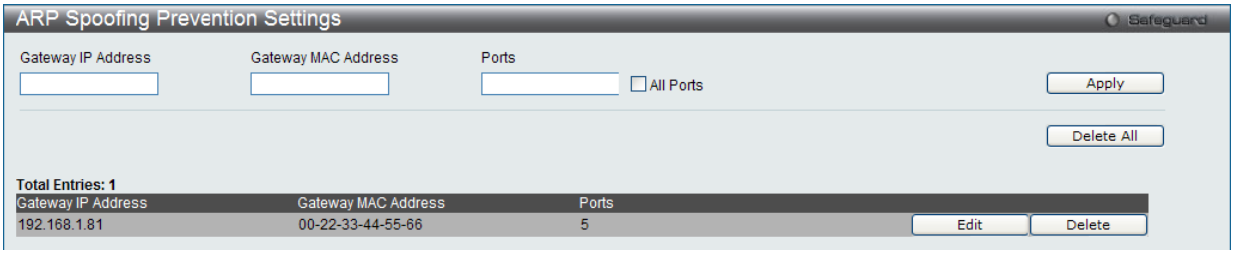


図 12-42　ARP Spoofing Prevention Settings 画面

この画面では以下の情報を表示できます。

項目	説明
Gateway IP Address	ARP Spoofing を防止するのに使用するゲートウェイ IP アドレスを入力します。
Gateway MAC Address	ARP Spoofing を防止するのに使用する MAC アドレスを指定します。
Ports	機能を適用するポート番号を選択します。また、「All Ports」を選択するとスイッチのすべてのポートに本機能が適用されます。

「Gateway IP」（ゲートウェイの IP アドレス）、「Gateway MAC」（ゲートウェイの MAC アドレス）および「Port List」を入力し、「Apply」ボタンをクリックします。

エントリの編集
編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除
「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

BPDU Attack Protection（BPDU アタック防止設定）

スイッチのポートに BPDU 防止機能を設定します。通常、BPDU 防止機能には 2 つの状態があります。1 つは正常な状態で、もう 1 つはアタック状態です。
アタック状態には、3 つのモード（破棄、ブロックおよびシャットダウン）があります。BPDU 防止が有効なポートは、STP BPDU パケットを受信するとアタック状態に入ります。そして、設定に基づいてアクションを行います。このように、BPDU 防止は STP が無効なポートにだけ有効にすることができます。

BPDU 防止では、「STP Port Settings」画面 (**L2 Features > Spanning Tree > STP Port Settings**) の「Forward BPDU」に設定したものより高い優先度を持っています。つまり、ポートが「STP Port Settings」画面の「Forward BPDU」に設定されており、BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

BPDU 防止では、BPDU の処理を決定するために設定したレイヤ 2 プロトコルトンネルポートより高い優先度を持っています。つまり、ポートが **L2 Features > Layer2 Protocol Tunneling Settings** 画面の「Tunnel STP Port(s)」にレイヤ 2 プロトコルトンネルポートとして設定されていると、ポートは STP BPDU を転送します。しかし、ポートで BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

Security > BPDU Attack Protection の順にメニューをクリックし、以下の画面を表示します。

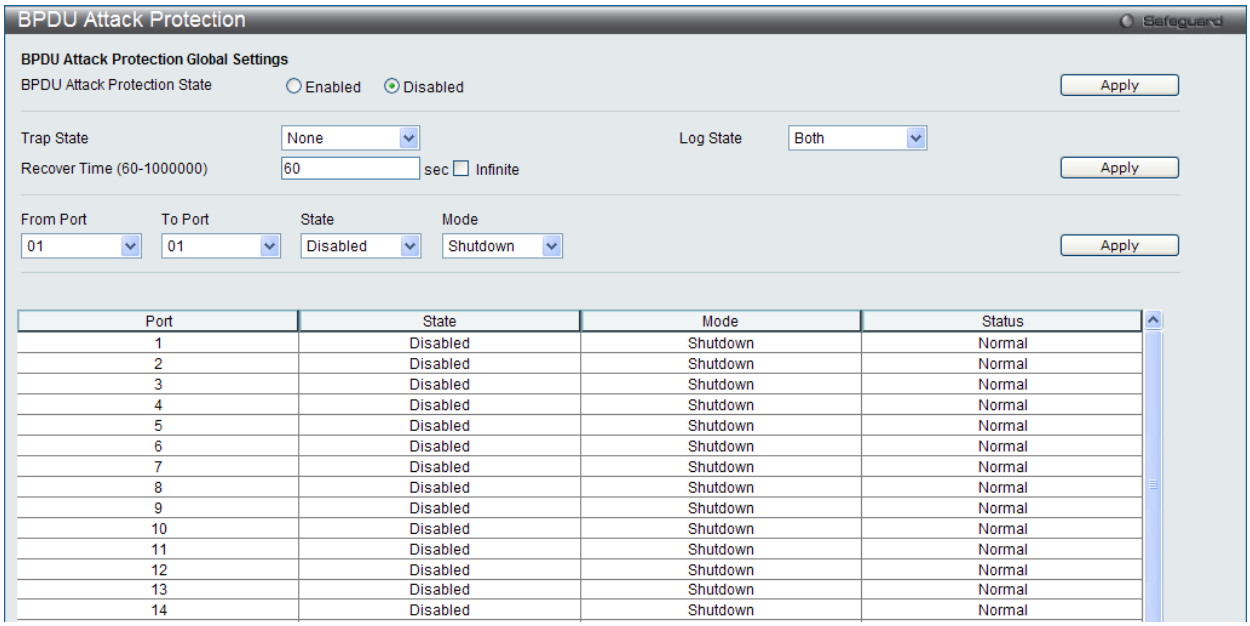


図 12-43　BPDU Attack Protection 画面

以下の項目を使用して、設定します。

項目	説明
BPDU Attack Protection State	BPDU アタック防止機能をグローバルに有効または無効にします。初期値は無効です。
Trap State	トラップをいつ送信するか指定します。「None」、「Attack Detected」、「Attack Cleared」、または「Both」を選択します。初期値は「None」（なし）です。
Log State	ログエントリをいつ送信するか指定します。「None」、「Attack Detected」、「Attack Cleared」、または「Both」を選択します。初期値は「Both」です。
Recover Time (60-1000000)	BPDU 防止の自動復帰タイマを指定します。復帰タイマの初期値は 60 です。
From Port / To Port	設定を使用するポート範囲を選択します。
State	指定ポートに対してモードを有効または無効にします。
Mode	BPDU 防止モードを指定します。 • Drop - ポートがアタック状態に入るとすべての受信 BPDU パケットを破棄します。 • Block - ポートがアタック状態に入るとすべてのパケット（BPDU と正常なパケットを含む）を破棄します。 • Shutdown - ポートがアタック状態に入るとポートをシャットダウンします。（初期値）

「Apply」ボタンをクリックし、変更を有効にします。

Loopback Detection Settings（ループバック検知設定）

ループバック検知（LBD）機能は、特定のポートに生成されるループを検出するために使用されます。本機能は、CTP(Configuration Testing Protocol) パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN から受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートは再起動 (Normal 状態へ遷移) を行います。ループバック検知機能はポート範囲に実行されます。

Security > Loopback Detection Settings の順にメニューをクリックし、以下の画面を表示します。

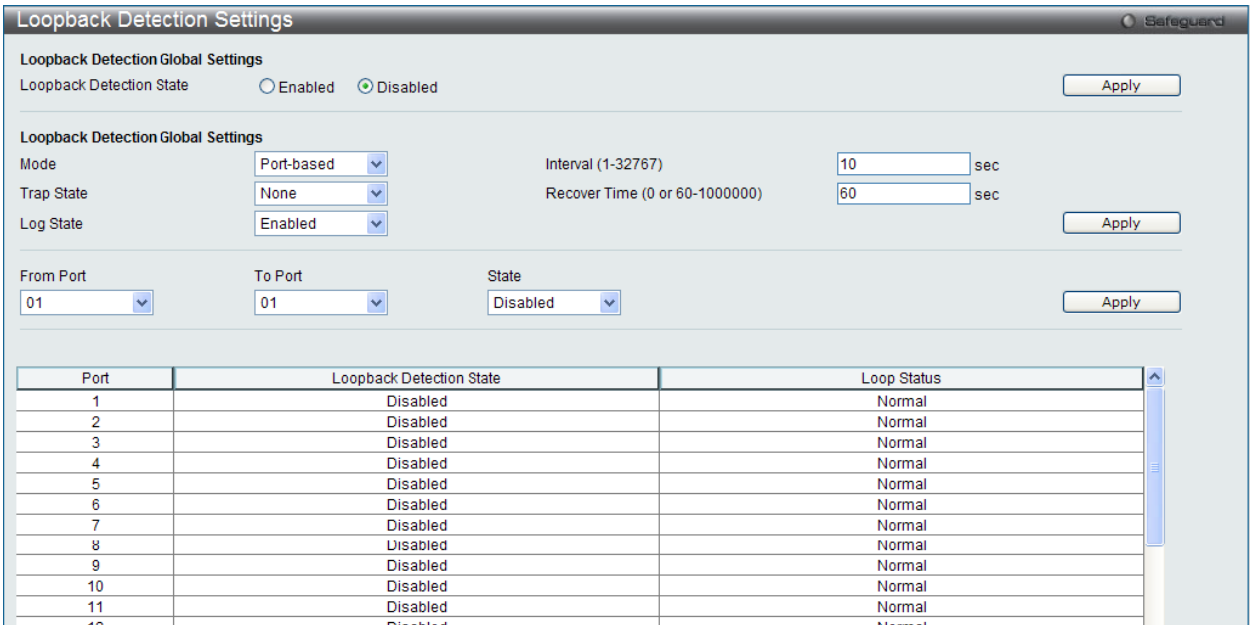


図 12-44　Loopback Detection Settings 画面

本画面には次の項目があります。

項目	説明
Loopback Detection State	ループバック検知機能を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Mode	プルダウンメニューを使用して、「Port-based」と「VLAN-based」を切り替えます。
Trap State	トラップを送信する状態を選択します。オプションは以下の通りです。 • Loop Detected - ループ状態を検知すると、トラップを送信します。 • Loop Cleared - ループ状態がクリアされると、トラップを送信します。 • None - ループバック検知のトラップを送信しません。(初期値)。 • Both - 検知およびクリアのトラップを両方送信します。
Log State	プルダウンメニューを使用して、ループバック検知のログ状態を「Enabled」(有効)/「Disabled」(無効) にします。
Interval (1-32767)	デバイスがループバックイベントを検出するためにすべての CTP(Configuration Test Protocol) パケットを送信する間隔（秒）。有効な範囲は 1-32767（秒）です。初期値 :10（秒）。
Recover Time (0 or 60-1000000)	ループが検知された場合にリカバリする時間（秒）を指定します。指定時間に到達すると、スイッチはループをチェックします。ループが検知されないと、ポートが再度有効になります。0 または 60-1000000（秒）に設定します。0 を指定すると、ループバックリカバリタイムは無効になります。初期値は 60（秒）です。
From Port / To Port	プルダウンメニューで適用するポート範囲を選択します。
State	プルダウンメニューで「Enabled」（有効）または「Disabled」（無効）を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意　「Untag（タグなし）」時でも「VID 0」は CTP に「Tag Field」を付与されます。規定上「VID 0」は「Untag（タグなし）」として扱われますが、古い一部のハードウェア製品（chipset 等）では破棄する場合があるのでご注意ください。

Traffic Segmentation Settings（トラフィックセグメンテーション設定）

トラフィックセグメンテーション機能は、（単一 / 複数）ポート間のトラフィックの流れを制限するために使用します。「トラフィックフローの分割」という方法は、「VLAN によるトラフィック制限」に似ていますが、さらに制限的です。本機能によりマスタスイッチ CPU のオーバヘッドを増加させないようにトラフィックを操作することが可能です。

Security > Traffic Segmentation Settings の順にメニューをクリックし、以下の画面を表示します。

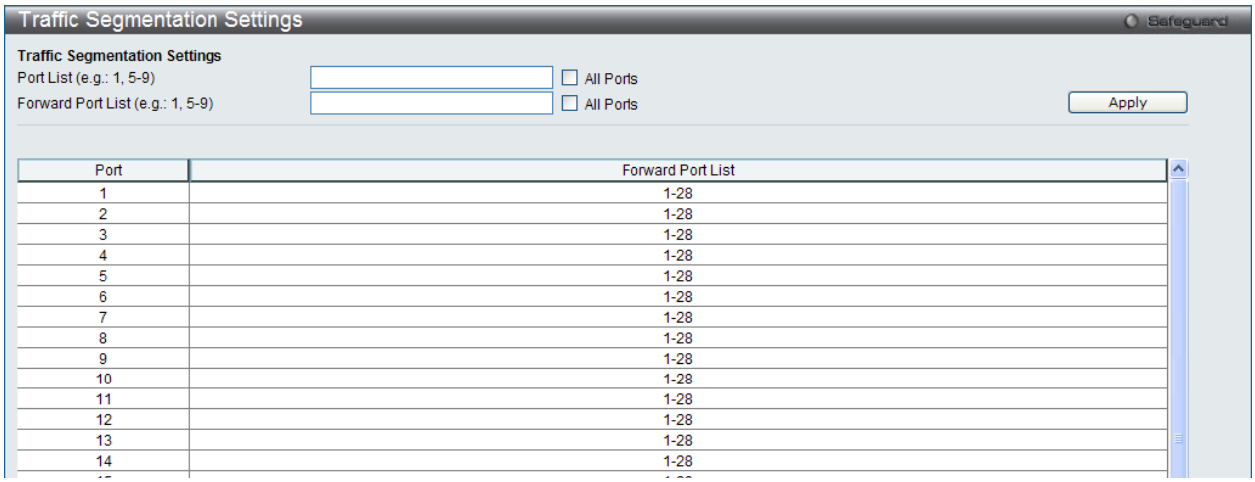


図 12-45　Traffic Segmentation Settings 画面

以下の項目を使用して設定します。

項目	説明
Port List	トラフィックセグメンテーションを設定するポートを入力します。「All Ports」ボタンをクリックすると設定用にすべてのポートを選択します。
Forward Port List	トラフィックセグメンテーション設定に含めるポートを入力します。「All Ports」ボタンをクリックすると設定用にすべてのポートを選択します。
Port	トラフィックセグメンテーション設定に含めたポートを表示します。

「Apply」ボタンをクリックすると、転送ポートの組み合わせが入力され、設定内容がテーブルに反映されます。

NetBIOS Filtering Setting（NetBIOS フィルタリング設定）

ネットワークをまたいで通信するために、NetBIOS はインタフェースをプログラミングするアプリケーションで、アプリケーションが使用する多くの機能を提供します。NetBEUI(NetBIOS Enhanced User Interface) は、NetBIOS のためのデータリンク層フレーム構造として作成されました。NetBIOS トラフィックを送信するためのシンプルなメカニズムである NetBEUI は小規模の MS-DOS や Windows ベースのワークグループのために選択するプロトコルです。NetBIOS は、厳密には NetBEUI プロトコル内には含まれません。マイクロソフトは、RFC1001 と RFC1002 に NetBIOS over TCP/IP(NBT) を記述した国際規格を作成するために取り組みました。

NetBUEI プロトコルを使用する 2 台以上のコンピュータのネットワーク通信をブロックする場合、これらの種類のパケットをフィルタするために NetBIOS フィルタリングを使用することができます。

NetBIOS フィルタを有効にすると、スイッチは自動的に 1 つのアクセスプロファイルと 3 つのアクセスルールを作成します。ユーザが広範囲に NetBIOS フィルタを有効にすると、スイッチはもう 1 つずつアクセスプロファイルとアクセスルールを作成します。

Security > NetBIOS Filtering Setting の順にメニューをクリックし、以下の画面を表示します。

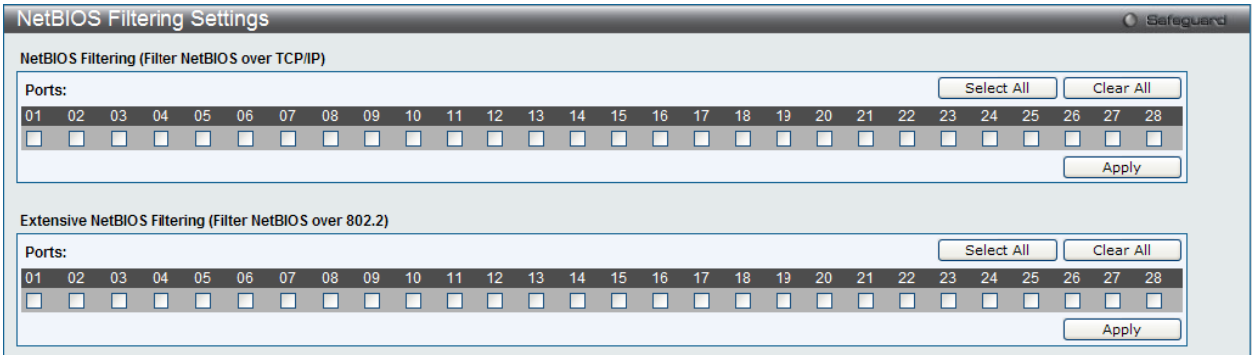


図 12-46　NetBIOS Filtering Settings 画面

以下の項目を使用して設定します。

項目	説明
NetBIOS Filtering	
NetBIOS フィルタリング設定に含める適切なポートを選択します。	
Ports	NetBIOS フィルタリング設定に含める適切なポートを簡単にチェックできます。
Extensive NetBIOS Filtering Ports	
Extensive NetBIOS フィルタリング設定に含める適切なポートを選択します。Extensive NetBIOS は 802.3（TCP/IP）における NetBIOS です。スイッチはこれが有効なポートでは 802.3 における NetBIOS フレームを拒否します。	
Ports	Extensive NetBIOS フィルタリング設定に含める適切なポートを簡単にチェックできます。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。
「Select All」ボタンをクリックすると設定用にすべてのポートを選択します。
「Clear All」ボタンをクリックして、すべてのポートを削除します。

DHCP Server Screening（DHCP サーバスクリーニング）

本機能では、ユーザはすべての DHCP サーバパケットを制限できるだけでなく、指定したどの DHCP クライアントからの DHCP サーバパケットも受信することが可能になります。この機能は 1 つ以上の DHCP サーバがネットワークに存在する場合に DHCP サービスを異なるクライアントグループと区別するのに役に立ちます。

初めて DHCP フィルタを有効にした時にアクセスプロファイルエントリとポートエントリごとのアクセスルールとその他のアクセスルールが作成されます。これらのルールは、すべての DHCP サーバパケットをブロックするのに使用します。さらに、DHCP エントリの許可のために、初めて DHCP クライアント MAC アドレスがクライアント MAC アドレスとして使用される時に、1 つのアクセスプロファイルと 1 つのアクセスルールエントリが作成されます。送信元 IP アドレスは DHCP サーバの IP アドレスと同じになります（UDP ポート番号は 67 です）。これらのルールは、ユーザが設定した特定のフィールドを持つ DHCP サーバパケットを許可するのに使用します。

DHCP サーバフィルタ機能が有効の場合、指定されたポートからのすべての DHCP サーバパケットはフィルタされます。

DHCP Server Screening Port Settings（DHCP サーバスクリーニング設定）

DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。この DHCP サーバフィルタ機能が有効になると指定ポートからのすべての DHCP サーバパケットはフィルタされます。

Security > DHCP Server Screening > DHCP Screening Port Settings の順にメニューをクリックして画面を表示します。

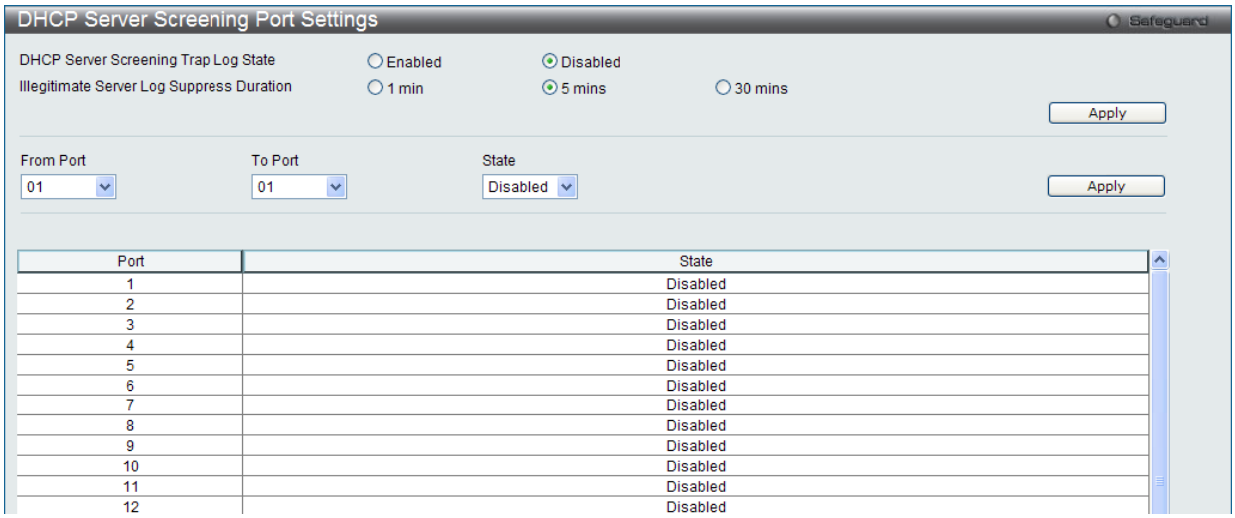


図 12-47　DHCP Screening Port Settings 画面

本画面には次の項目があります。

項目	説明
DHCP Server Screening Trap Log State	DHCP サーバのトラップログのフィルタを「Enabled」（有効）または「Disabled」（無効）にします。
Illegitimate Server Log Suppress Duration	不正なサーバログの抑制時間を 1、5、または 30 分から選択します。
From Port/To Port	設定の対象となるポートを指定します。
State	DHCP サーバスクリーニングを「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。

設定後、「Apply」ボタンをクリックして設定を有効にします。

DHCP Offer Permit Entry Settings（DHCP オファー許可エントリ設定）

許可エントリの追加または削除を行います。

Security > DHCP Server Screening > DHCP Offer Permit Entry Settings の順にクリックし、画面を表示します。

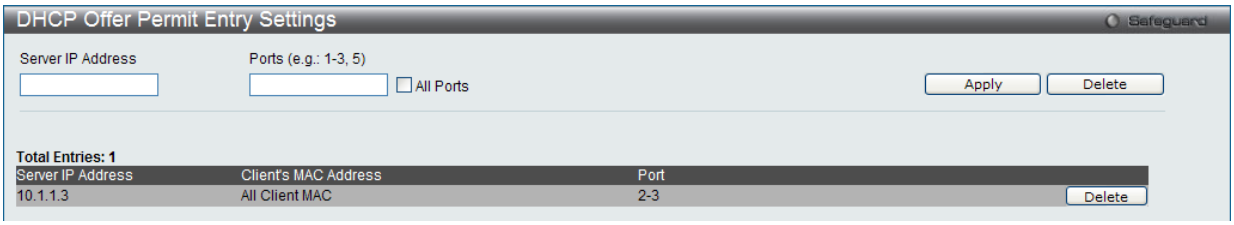


図 12-48　DHCP Offer Permit Entry Settings 画面

本画面には次の項目があります。

項目	説明
Server IP Address	フィルタを通過させる DHCP サーバを指定します。
Ports	フィルタする DHCP サーバのポート番号を入力します。スイッチのすべてのポートを使用する場合は「All Ports」をチェックします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

Access Authentication Control（アクセス認証コントロール）

TACACS/ XTACACS/ TACACS+/ RADIUS コマンドは、TACACS/ XTACACS/ TACACS+ /RADIUS プロトコルを使用してスイッチへの安全なアクセスを可能にします。ユーザがスイッチへのログインや、管理者レベルの特権へのアクセスを行おうとする時、パスワードの入力を求められます。TACACS/ XTACACS/ TACACS+/ RADIUS 認証がスイッチで有効になると、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバと連絡し、ユーザの確認をします。確認が行われたユーザは、スイッチへのアクセスを許可されます。

現在 TACACS セキュリティプロトコルには異なるエンティティを持つ 3 つのバージョンが存在します。本スイッチのソフトウェアは TACACS の以下のバージョンをサポートします。

•TACACS（Terminal Access Controller Access Control System）
　セキュリティのためのパスワードチェック、認証、およびユーザアクションの通知を、1 台またはそれ以上の集中型の TACACS サーバを使用して行います。パケットの送受信には UDP プロトコルを使用します。
• XTACACS（拡張型 TACACS）
　TACACS プロトコルの拡張版で、TACACS プロトコルより多種類の認証リクエストとレスポンスコードに対応します。パケットの送受信に UDP プロトコルを使用します。
• TACACS+（Terminal Access Controller Access Control System plus）
　ネットワークデバイスの認証のために詳細なアクセス制御を提供します。TACACS+ は、1 台またはそれ以上の集中型のサーバを経由して認証コマンドを使用することができます。TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間のすべてのトラフィックを暗号化します。また、TCP プロトコルを使用して信頼性の高い伝達を行います。

TACACS/ XTACACS/ TACACS+/ RADIUS のセキュリティ機能が正常に動作するためには、スイッチ以外の認証サーバホストと呼ばれるデバイス上で認証用のユーザ名とパスワードを含む TACACS/ XTACACS/ TACACS+/ RADIUS サーバの設定を行う必要があります。スイッチがユーザにユーザ名とパスワードの要求を行う時、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバにユーザ認証の問い合わせを行います。サーバは以下の 3 つのうちの 1 つの応答を返します。

• サーバは、ユーザ名とパスワードを認証し、ユーザにスイッチへの通常のアクセス権を与えます。
• サーバは、入力されたユーザ名とパスワードを受け付けず、スイッチへのアクセスを拒否します。
• サーバは、認証の問い合わせに応じません。この時点でスイッチはサーバからタイムアウトを受け取り、メソッドリスト中に設定された次の認証方法へと移行します。

本スイッチには TACACS、XTACACS、TACACS+、RADIUS の各プロトコル用に 4 つの認証サーバグループがあらかじめ組み込まれています。これらの認証サーバグループはスイッチにアクセスを試みるユーザの認証に使用されます。認証サーバグループ内に任意の順番で認証サーバホストを設定し、ユーザがスイッチへのアクセス権を取得する場合、1 番目の認証サーバホストに認証を依頼します。認証が行われなければ、リストの 2 番目のサーバホストに依頼し、以下同様の処理が続きます。実装されている認証サーバグループには、特定のプロトコルが動作するホストのみを登録できます。例えば TACACS 認証サーバグループは、TACACS 認証サーバホストのみを登録できます。

スイッチの管理者は、ユーザ定義のメソッドリストに 6 種類の異なる認証方法（TACACS/ XTACACS/ TACACS+/ RADIUS/ local/ none）を設定できます。これらの方法は、任意に並べ替えることが可能で、スイッチ上での通常のユーザ認証に使用されます。リストには最大 8 つの認証方法を登録できます。ユーザがスイッチにアクセスしようとすると、スイッチはリストの 1 番目の認証方法を選択して認証を行います。1 番目の方法で認証サーバホストを通過しても認証が返ってこなければ、スイッチはリストの次の方法を試みます。この手順は、認証が成功するか、拒否されるか、またはリストのすべての認証方法を試し終わるまで繰り返されます。

TACACS/XTACACS/TACACS+ または non（認証なし）のメソッド経由でユーザがデバイスへのログインに成功すると、「User」の権限のみが与えられます。ユーザが管理者レベルの権限に更新したい場合、「enable admin」コマンドを実行し、権限レベルを昇格させる必要があります。しかし、ユーザが RADIUS サーバまたはローカルな方法を経由してデバイスへのログインに成功すると、3 種類の権限レベルをユーザに割り当てることが可能であり、ユーザは「enable admin」コマンドを使用して、権限レベルを昇格させることはできません。

スイッチへのアクセス権を取得したユーザは、スイッチに通常ユーザのアクセス権を与えられています。理者特権レベルの権利を取得するためには、ユーザは「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

注意 TACACS、XTACACS、TACACS+、RADIUS は独立したエンティティであり、互換性はありません。スイッチとサーバ間は、同じプロトコルを使用した全く同じ設定を行う必要があります。（例えば、スイッチに TACACS 認証を設定した場合、ホストサーバにも同様の設定を行います。）

Enable Admin（管理者レベルの認証）

本画面は、通常のユーザレベルとしてスイッチにログインした後、管理者レベルに昇格したい場合に使用します。スイッチにログインした後のユーザにはユーザレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本画面を開き、認証用パスワードを入力します。本機能における認証方法は、TACACS/XTACACS/TACACS+/RADIUS、ユーザ定義のサーバグループ、local enable(スイッチ上のローカルアカウント) または、認証なし (none) から選択できます。XTACACS と TACACS は Enable の機能をサポートしていないため、ユーザはサーバホスト上に特別なアカウントを作成し、ユーザ名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「Disabled」(無効) である場合には実行できません。

Security > Access Authentication Control > Enable Admin の順にメニューをクリックし、以下の画面を表示します。

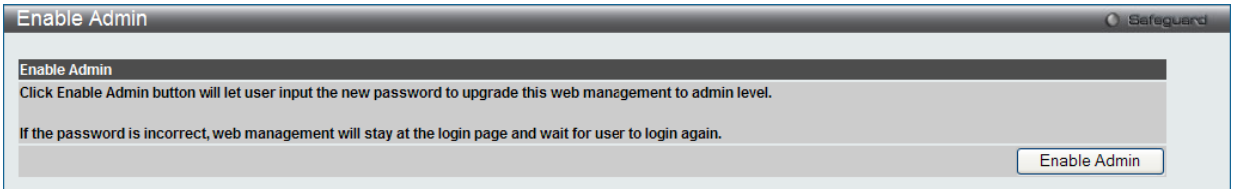


図 12-49　Enable Admin 画面

「Enable Admin」ボタンをクリックして以下のダイアログボックスを表示します。

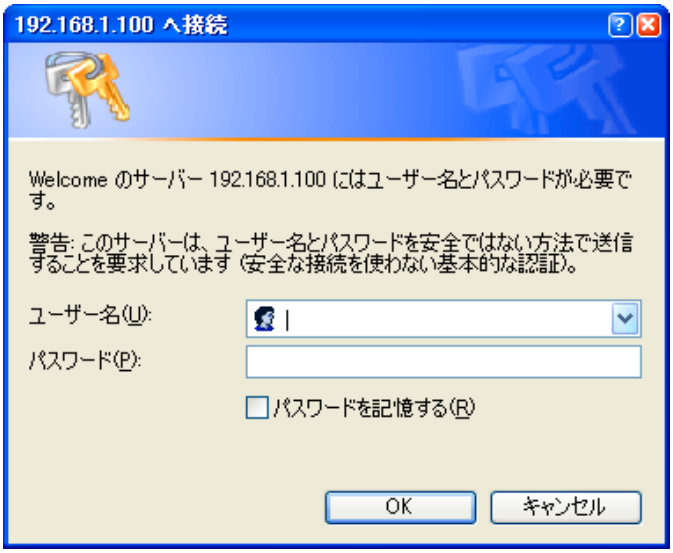


図 12-50　ユーザ名とパスワード入力ダイアログボックス

「ユーザー名」と「パスワード」を入力して「OK」ボタンをクリックします。「ユーザー名」と「パスワード」が承認されると、ユーザ権限は管理者特権レベルに変更されます。

Authentication Policy Settings（認証ポリシー設定）

スイッチにアクセスするユーザのために管理者が定義した認証ポリシーを有効にします。有効にすると、デバイスはログインメソッドリストをチェックし、ログイン時のユーザ認証に使用する認証方法を選択します。

Security > Access Authentication Control > Authentication Policy Settings の順にメニューをクリックし、以下の画面を表示します。

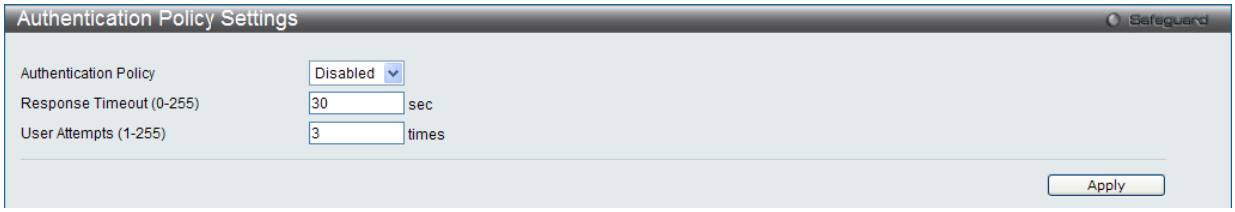


図 12-51　Authentication Policy Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Authentication Policy	プルダウンメニューからスイッチの認証ポリシーを「Enabled」（有効）または「Disabled」（無効）に設定します。
Response Timeout (0-255)	ユーザからの認証のレスポンスに対するスイッチの待ち時間を指定します。0-255（秒）の範囲から指定します。初期値は 30（秒）です。
User Attempts (1-255)	ユーザが認証を試みることができる最大回数。指定回数認証に失敗すると、そのユーザはスイッチへのアクセスを拒否され、さらに認証を試みることができなくなります。CLI ユーザは、再度認証を行う前に 60 秒待つ必要があります。Telnet および Web ユーザはスイッチから切断されます。1-255 の範囲で指定します。初期値は 3（回）です。

「Apply」ボタンをクリックし、設定を有効にします。

Application Authentication Settings（アプリケーションの認証設定）

作成済みのメソッドリストを使用して、ユーザレベルおよび管理者レベル（Enable Admin）でログインする際に使用するスイッチの設定用アプリケーション（Console、Telnet、SSH、HTTP）を設定します。

Security > Access Authentication Control > Application Authentication Settings の順にクリックし、以下の画面を表示します。

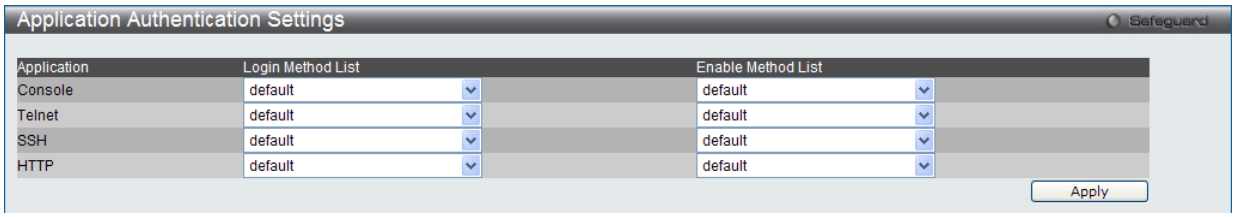


図 12-52　Application Authentication Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Application	スイッチ上の設定用アプリケーションをリスト表示しています。それぞれのアプリケーション（Console、Telnet、SSH、HTTP）を使用するユーザ認証用の「Login Method List」と「Enable Method List」を指定できます。
Login Method List	プルダウンメニューを使用し、登録済みのメソッドリストから、ユーザレベルの通常ログインを行うアプリケーションに適用するリストを選択します。初期設定のメソッドリスト、またはユーザ定義のメソッドリストを選択できます。詳細な情報は、後述の「Login Method Lists Settings」画面を参照してください。
Enable Method List	プルダウンメニューにより、登録済みのメソッドリストを使用してユーザレベルを管理者レベルに昇格させるアプリケーションを選択します。初期設定のメソッドリスト、またはユーザ定義のメソッドリストを選択できます。詳細な情報は、後述の「Enable Method Lists Settings」画面を参照してください。

「Apply」ボタンをクリックし、設定を有効にします。

Authentication Server Group Settings（認証サーバグループ設定）

本画面では、スイッチ上に認証サーバグループの設定を行います。サーバグループとは、TACACS/ XTACACS/ TACACS+/ RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。プロトコルによって、または定義済みのサーバグループに組み込むことによりグループ分けを行います。スイッチには 4 つの認証サーバグループがあらかじめ組み込まれています。これらは削除することができませんが、内容の変更は可能です。1 つのグループにつき最大 8 個までの認証サーバホストを登録できます。

Security > Access Authentication Control > Authentication Server Group Settings の順にメニューをクリックし、以下の画面を表示します。

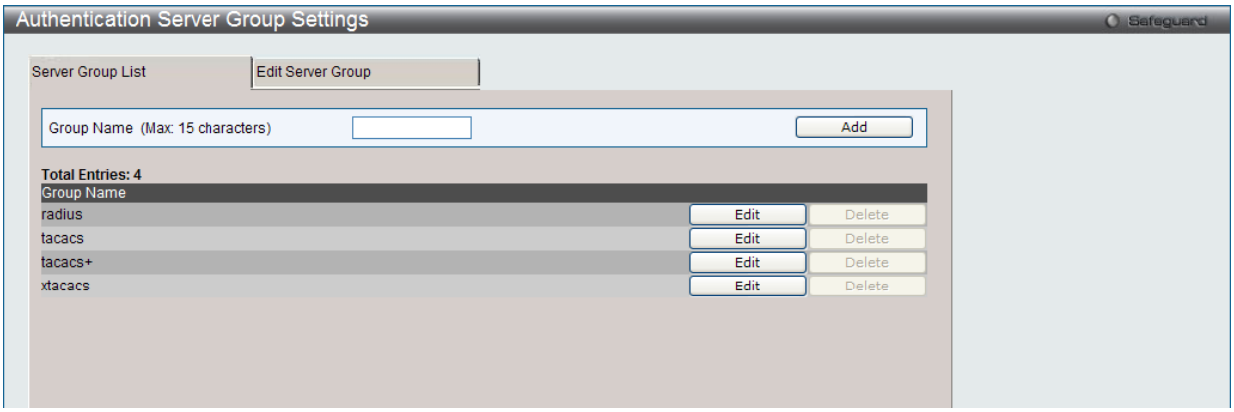


図 12-53　Authentication Server Group Settings 画面

スイッチの認証サーバグループを表示します。スイッチには 4 つの認証サーバグループが組み込まれています。これらは削除できませんが、内容の変更は可能です。

以下の項目を使用して、設定を行います。

項目	説明
Group Name	新規サーバグループ名を指定します。

新しいサーバグループを作成するためには、「Group Name」欄に名前を入力し、「Add」ボタンをクリックします。特定のグループを編集するためには、対応する「Edit」ボタンをクリックするか、またはこの画面の上の「Edit Server Group」タブをクリックし、以下の画面を表示します。

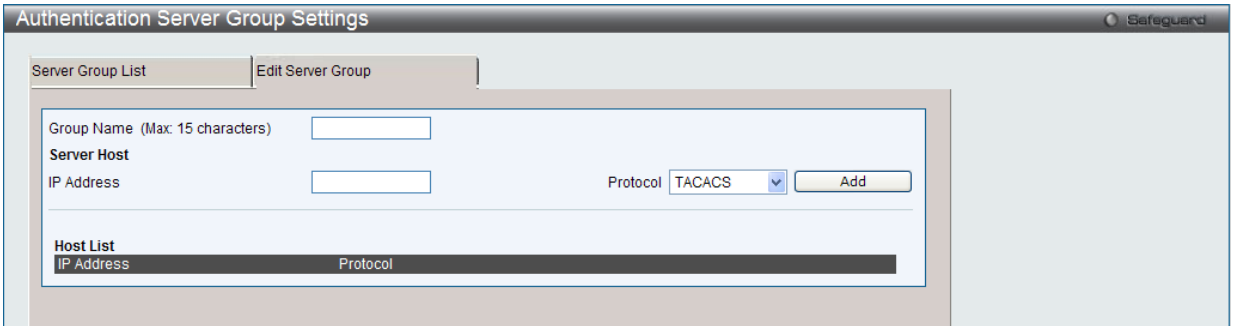


図 12-54　Authentication Server Group Settings (Edit) 画面

以下の項目を使用して、設定を行います。

項目	説明
Group Name	サーバグループ名を指定します。
IP Address	サーバホストの IP アドレスを入力します。
Protocol	プルダウンメニューを使用して、認証サーバホストの IP アドレスに割り当てるプロトコルを選択します。

リストに認証サーバホストを追加するためには、「Group Name」欄にホストの名称、「IP Address」フィールドにホストの IP アドレスを入力し、プルダウンメニューから認証サーバホストの IP アドレスに関連付けるプロトコルを指定します。その後「Add」ボタンをクリックすると、本認証サーバホストがグループに登録されます。エントリはこのタブの「Host List」に表示されます。

注意　認証サーバホストをリストに追加する前に、「Authentication Server Settings」画面にてホストの登録を行う必要があります。本機能を正しく動作させるためには、リモートの中央管理サーバ上でプロトコルを指定して認証サーバホストの設定を行う必要があります。

注意　あらかじめ組み込まれている 4 つのサーバグループには、同じ TACACS デーモンが起動されているサーバホストのみを入れることができます。TACACS/ XTACACS /TACACS+ プロトコルは別のエンティティで、互換性はありません。

Authentication Server Settings（認証サーバ設定）

本画面では、スイッチに TACACS/ XTACACS/ TACACS+/ RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを設定します。

ユーザが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストに認証パケットを送信します。すると TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/ XTACACS/ TACACS+/ RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

Security > Access Authentication Control > Authentication Server Settings の順にメニューをクリックし、以下の画面を表示します。

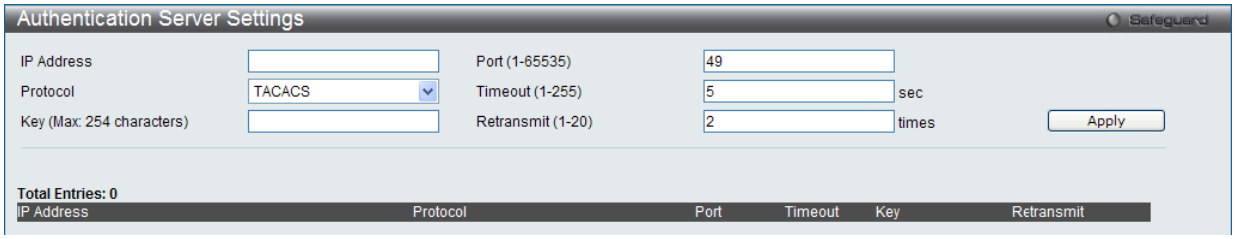


図 12-55　Authentication Server Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
IP Address	追加するリモートサーバホストの IP アドレス。
Port (1-65535)	サーバホスト上で認証プロトコルに使用する仮想ポート番号（1-65535）。ポート番号の初期値は、TACACS/ XTACACS/ TACACS+ サーバの場合は 49、RADIUS サーバの場合は 1812 です。独自の番号を設定してセキュリティを向上することも可能です。
Protocol	サーバホストが使用するプロトコル。以下から選択します。 • TACACS - ホストが TACACS プロトコルを使用している場合に選択します。 • XTACACS - ホストが XTACACS プロトコルを使用している場合に選択します。 • TACACS+ - ホストが TACACS+ プロトコルを使用している場合に選択します。 • RADIUS - ホストが RADIUS プロトコルを使用している場合に選択します。
Timeout (1-255)	スイッチが、サーバホストからの認証リクエストへの応答を待つ時間（秒）。初期値は 5（秒）です。
Key	TACACS+ と RADIUS サーバの場合に指定する共有キー。254 文字までの半角英数字を入力します。
Retransmit (1-20)	TACACS サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数を入力します。TACACS+ に設定すると、この値は効果はありません。初期値は 2 です。

「Apply」ボタンをクリックし、サーバホストを追加します。

注意　1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/ XTACACS/ TACACS+ は個別のエンティティであり、互換性を持たないことに注意が必要です。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

Login Method Lists Settings（ログインメソッドリスト）

本メニューでは、ユーザがスイッチにログインする際の認証方法を規定するユーザ定義または初期設定のログインメソッドリストを設定します。本メニューで設定した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS-XTACACS-Local の順番で認証方法を指定すると、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに認証リクエストを送信します。そのサーバホストから応答がない場合、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリストの次の方法（XTACACS）を試します。それでも認証が行われなければ、スイッチ内に設定したローカルアカウントデータベースを使用して認証を行います。Local メソッドが使用される時、ユーザの権限はスイッチに設定されたローカルアカウントの権限に依存します。

これらの認証方法によって、認証に成功したユーザには「User」の権限のみが与えられます。ユーザが管理者レベルの権限を必要とするのであれば、「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

Security > Access Authentication Control > Login Method Lists Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-56　Login Method Lists Settings 画面

スイッチには、あらかじめ削除できない Login Method List が登録されています。このリストの内容の変更は可能です。

Login Method List の新規登録

以下の項目を設定し、「Apply」ボタンをクリックします。

項目	説明
Method List Name	15 文字までの半角英数字でメソッドリスト名を入力します。
Priority 1, 2, 3, 4	本メソッドリストに追加する認証方法を最大 4 件まで指定します。 • tacacs – リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs – リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ – リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 • radius – リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 • server_group – スイッチ上に設定したユーザ定義のサーバグループを使用してユーザ認証を行います。 • local – スイッチ上のローカルユーザアカウントデータベースを使用してユーザ認証を行います。 • none – スイッチへアクセスするための認証を行います。

Login Method List の変更

1. 対応する「Edit」ボタンをクリックし、編集画面を表示します。
2. 項目を編集し、「Apply」ボタンをクリックします。

ユーザ定義の Login Method List の削除

1. 削除対象のエントリの行の「Delete」ボタンをクリックします。

Enable Method Lists Settings（メソッドリストの有効化）

スイッチ上で認証メソッドを使用して、ユーザの権限をユーザレベルから管理者（Admin）レベルに上げる際に利用するメソッドリストの設定を行います。通常のユーザレベルの権限を取得したユーザが管理者特権を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の Enable Method List が登録でき、そのうちの 1 つは default Enable メソッドリストになります。本 default Enable メソッドリストは内容の変更はできますが、削除はできません。

本メニューで定義した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS-XTACACS-Local の順番で認証方法を指定した場合、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに対して、認証リクエストを送信します。認証が確認できなければ、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリスト中の次の方法（XTACACS）を試します。それでも認証が行われなければ、スイッチ内に設定したローカル Enable パスワードを使用してユーザの認証を行います。

以上のいずれかの方法で認証されたユーザは、「Admin」（管理者）権限を取得することができます。

注意 ローカル Enable パスワードの設定については「Local Enable Password Settings（ローカルユーザパスワード設定）」（253 ページ）の項を参照してください。

Security > Access Authentication Control > Enable Method Lists Settings の順にメニューをクリックし、以下の画面を表示します。

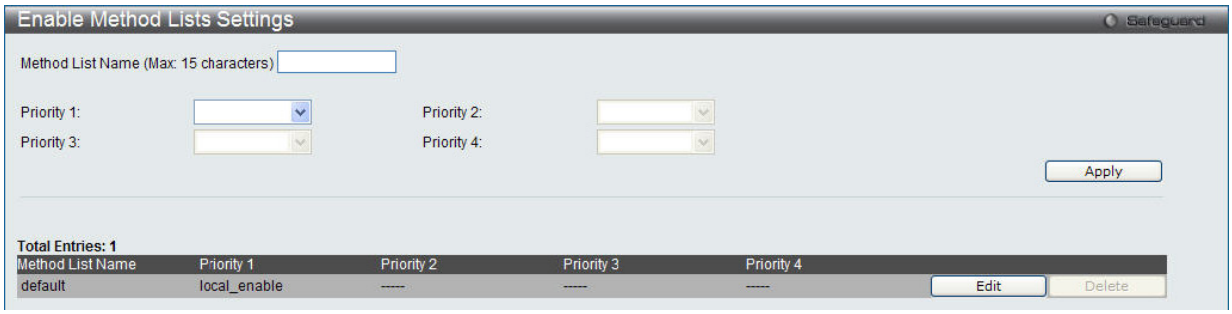


図 12-57 Enable Method Lists Settings 画面

以下の項目を使用して、Enable Method List の設定を行います。入力後、「Apply」ボタンをクリックします。

項目	説明
Method List Name	15 文字までの半角英数字でメソッドリスト名を入力します。
Priority 1, 2, 3, 4	本メソッドリストに追加する認証方法を最大 4 件まで指定します。 • local_enable – スイッチ上のローカル Enable パスワードデータベースを使用してユーザ認証を行います。Local enable password は次セクションの「Local Enable Password Settings（ローカルユーザパスワード設定）」（253 ページ）を参照し、設定してください。 • none – スイッチへアクセスするために必要とされる認証を行いません。 • radius – リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 • tacacs – リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs – リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ – リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 • server_group – スイッチ上に設定したユーザ定義のサーバグループを使用してユーザ認証を行います。

メソッドリストの作成

1. メソッドリスト名を「Method List Name」に入力し、認証方法を「Priority 1-4」に設定します。
2. 「Apply」ボタンをクリックして設定を適用します。

ユーザ定義の Enable メソッドリストの削除

対象の行で「Delete」ボタンをクリックします。

メソッドリストの変更

1. 対応するメソッドリスト名の「Edit」ボタンをクリックし、編集画面を表示します。
2. 項目を編集後、エントリの「Apply」ボタンをクリックします。

Local Enable Password Settings（ローカルユーザパスワード設定）

本画面では、「Enable Admin」コマンド用の Local Enable Password を設定します。ユーザがその権限をユーザレベルから管理者レベルに変更する際の認証方法に、「local_enable」を選択している場合、本画面でスイッチに登録したパスワードの入力が要求されます。

Security > Access Authentication Control > Local Enable Password Settings の順にメニューをクリックし、以下の画面を表示します。

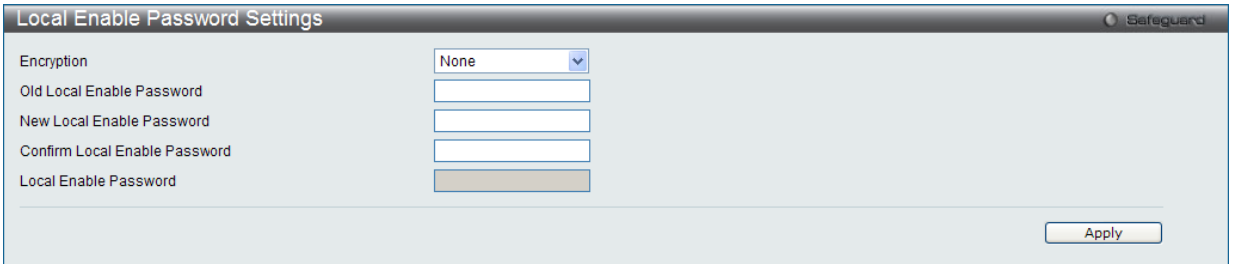


図 12-58 Local Enable Password Settings 画面

以下の項目を使用して、Local Enable Password を設定します。

項目	説明
Encryption	パスワードに使用する暗号化タイプを指定します。 • Plain Text - プレーンテキスト形式でパスワードを指定します。 • SHA1 - SHA-1 暗号化形式でパスワードを指定します。
Old Local Enable Password	登録済みのパスワードがある場合は、新しいパスワードに変更するために入力します。
New Local Enable Password	スイッチの管理者レベルでアクセスを試みるユーザの認証に使用する（新しい）パスワードを入力します。15 文字までの半角英数字を使用します。
Confirm Local Enable Password	確認のため、上記の新パスワードを再度入力します。先に入力したものと異なると、エラーメッセージが表示されます。
Local Enable Password	「Encryption」オプションの 1 つを選択後に、使用するローカルパスワードを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SSL Settings（Secure Socket Layer の設定）

Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、認証セッションに使用する厳密な暗号パラメータ、特定の暗号化アルゴリズムおよびキー長を決定する、暗号スイートと呼ばれるセキュリティ文字列により実現しています。SSL は、以下の 3 つの段階で構成されます。

1. 鍵交換
暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。

2. 暗号化
暗号スイートの次の段階は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
- ストリーム暗号 – スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとホスト間で一致させる必要があります。
- CRC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義する 3 DES EDE 暗号化コードをサポートし、暗号文を生成します。

3. ハッシュアルゴリズム
暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）の 2 種類のハッシュアルゴリズムをサポートします。

これら 3 つのパラメータは、スイッチ上での 4 つの選択肢として独自に組み合わされ、サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。本スイッチは、SSLv3 および TLSv1 をサポートしています。SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する場合があります。

証明書のダウンロード (Download Certificate)
本画面では、SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者の情報や認証のための鍵やデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバとクライアントが一致した証明書ファイルを持つ必要があります。スイッチは、拡張子 ".der" を持つ証明書のみをサポートします。スイッチは証明書が既にロードされている形で発送されますが、ユーザの環境によっては、さらにダウンロードが必要になる場合があります。

暗号スイート
「SSL Configuration Settings」画面では、ネットワークマネージャが SSL を有効にしてスイッチに暗号スイートを設定できます。暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

SSL 機能が有効になると、Web の使用はできなくなります。SSL 機能を使用しながら Web ベースの管理を行うためには、Web ブラウザが SSL 暗号化をサポートし、https:// で始まる URL を使用しなければなりません。（例 : https://10.90.90.90）これを守らないと、エラーが発生し、Web ベースの管理機能にアクセスできなくなります。

Security > SSL Settings の順にメニューをクリックし、以下の画面を表示します。

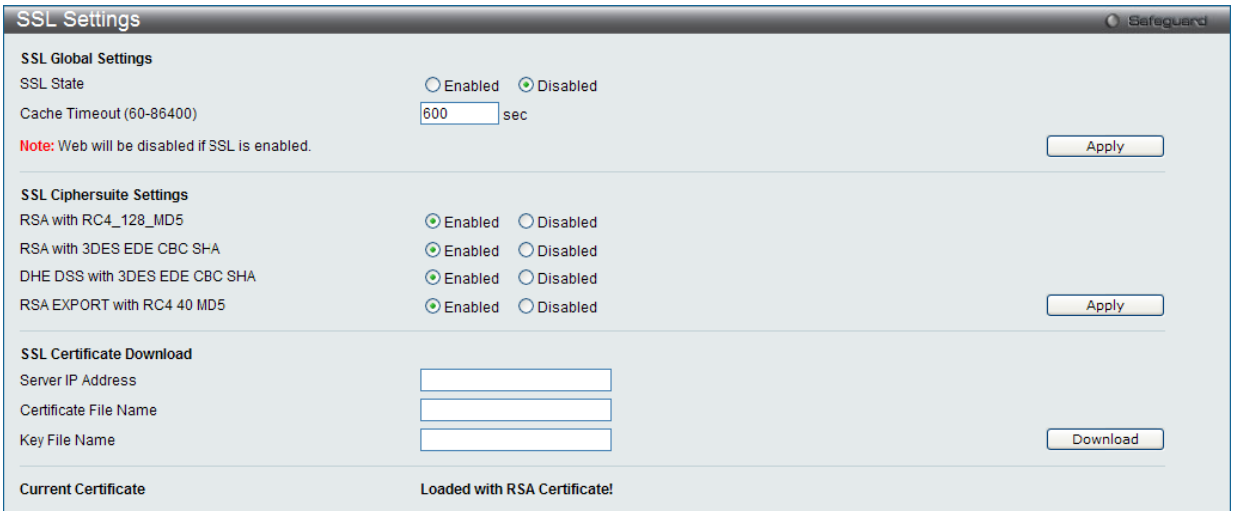


図 12-59　SSL Settings 画面

SSL 機能の設定

「SSL Global Settings」セクションの項目を設定し、「Apply」ボタンをクリックします。

SSL 暗号スイート機能の設定

「SSL Ciphersuite Settings」セクションの項目を設定し、「Apply」ボタンをクリックします。

SSL 証明書のダウンロード

「SSL Certificate Download」セクションの項目を設定し、「Download」ボタンをクリックします。

項目	説明
SSL Global Settings	
SSL State	スイッチの SSL の「Enabled」（有効）、「Disabled」（無効）を指定します。初期値は「Disabled」です。
Cache Timeout (60-86400)	クライアントとホストの間の SSL による新しい鍵交換の間隔を指定します。クライアントとホストが鍵交換をすると常に新しい SSL セッションが確立します。この値を長くすると SSL セッションによる特定のホストとの再接続には主鍵が再利用されます。それためネゴシエーション処理は速くなります。初期値は 600（秒）です。
SSL Ciphersuite Settings	
RSA with RC4_128_MD5	この暗号スイートは RSA key exchange、stream cipher C4（128-bit keys）、MD5 Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
RSA with 3DES EDE CBC SHA	この暗号スイートは RSA key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
DHE DSS with 3DES EDE CBC SHA	この暗号スイートは DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
RSA EXPORT with RC4 40 MD5	この暗号スイートは RSA Export key exchange、stream cipher RC4（40-bit keys）、MD5 Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
SSL Certificate Download	
Server IP Address	証明書のファイルがある TFTP サーバの IP アドレスを指定します。
Certificate File Name	ダウンロードする証明書のパスとファイル名を指定します。ファイルには拡張子 ".der" が必要です。（例 c:/cert.der）
Key File Name	ダウンロードする鍵ファイルのパスとファイル名を指定します。ファイルには拡張子 ".der" が必要です。（例 c:/pkey.der）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意　SSL の機能と構成に関するいくつかの機能は本スイッチの Web ベースマネジメントでは利用できません。

注意　SSL 機能が有効になると Web ベースマネジメントは無効になります。再度本スイッチにログオンするには URL の始まりを「https://」にする必要があります。それ以外のアドレスを Web ブラウザに指定してもエラーになり認証されません。

SSH（Secure Shell の設定）

SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。SSH は、リモートのホストコンピュータへの安全なログインや、リモートのエンドノードでの安全なコマンド実行メソッドを可能にし、信頼関係を結んでいないホスト間に暗号化と認証を利用した安全な通信を提供します。高度なセキュリティ機能を備えた SSH は、今日のネットワーク環境に必要不可欠なツールです。ネットワーク通信を脅かす数々のセキュリティハザードに対して、強力な監視者としての役割を担います。

リモート PC（SSH クライアント）とスイッチ（SSH サーバ）間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

1. **System Configuration > User Accounts** で管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
2. 「SSH User Authentication Lists」画面を使用して、ユーザアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「Host-based」、「Password」、「Public Key」の 3 つがあります。
3. 「SSH Authentication Method and Algorithm Settings」画面を使用して、SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。
4. 最後に「SSH Settings」画面で、SSH を有効にします。

これらの手順が完了後、安全な帯域内の接続でスイッチの管理を行うために、リモート PC 上の SSH クライアントの設定を行います。

SSH Settings（SSH サーバ設定）

本画面は SSH サーバの設定および設定内容の確認に使用します。

Security > SSH > SSH Settings の順にメニューをクリックします。

図 12-60　SSH Settings 画面

以下の項目を使用して、SSH サーバの設定を行います。

項目	説明
SSH Server State	スイッチ上で SSH 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Max Session (1-8)	同時にスイッチに接続できる数を 1 から 8 の数字を設定します。初期値は 8 です。
Connection Timeout (120-600)	接続のタイムアウト時間を指定します。120 から 600（秒）が指定できます。初期値は 120（秒）です。
Authfail Attempts (2-20)	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。指定した回数を超えるとスイッチは接続を切り、ユーザは再度スイッチに接続する必要があります。2 から 20 が指定できます。初期値は 2 です。
Rekey Timeout	スイッチが SSH 鍵の再交換を行う間隔をプルダウンメニューから選択します。「Never」、「10 min」、「30 min」、「60 min」です。初期値は「Never」（鍵再交換を行わない）です。
TCP Port Number (1-65535)	SSH に使用する TCP 番号を入力します。初期値は 22 です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SSH Authentication Method and Algorithm Settings（SSH 認証モードとアルゴリズム設定）

認証および暗号化に使用する SSH アルゴリズムの種類を設定します。アルゴリズムはカテゴリに分けてリスト表示され、各アルゴリズムは対応するチェックボックスを使用して有効、無効に設定できます。すべてのアルゴリズムは初期値で有効です。

Security > SSH > SSH Authentication mode and Algorithm Settings の順にメニューをクリックし、以下の画面を表示します。

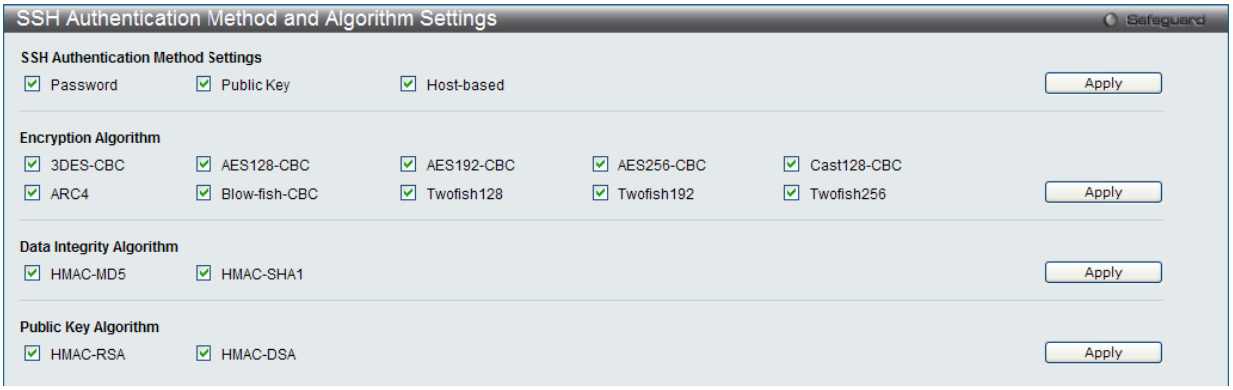


図 12-61　SSH Authentication Method and Algorithm Settings 画面

以下のアルゴリズムが設定できます。

項目	説明
SSH Authentication Mode Settings	
Password	スイッチにおける認証にローカルに設定したパスワードを使用する場合に「Enabled」（有効）にします。初期値は「Enabled」です。
Public Key	スイッチにおける認証に SSH サーバに設定した公開鍵を使用する場合に「Enabled」（有効）にします。初期値は「Enabled」です。
Host-based	認証にホストコンピュータを使用する場合に「Enabled」（有効）にします。本項目は SSH 認証機能を必要とする Linux ユーザ向けに設定されます。ホストコンピュータには SSH プログラムがインストールされ、Linux OS が起動している必要があります。初期値は「Enabled」です。
Encryption Algorithm	
3DES-CBC	CBC 方式で 3DES 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Blow-fish-CBC	CBC 方式で Blowfish 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES128-CBC	CBC 方式で AES128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES192-CBC	CBC 方式で AES192 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES256-CBC	CBC 方式で AES256 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
ARC4	ARC4 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Cast128-CBC	CBC 方式で Cast128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish128	Twofish128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish192	Twofish192 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish256	Twofish256 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Data Integrity Algorithm	
HMAC-SHA1	SHA1（セキュアハッシュ）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
HMAC-MD5	MD5（メッセージダイジェスト）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Public Key Algorithm	
HMAC-RSA	RSA 暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
HMAC-DSA	DSA（デジタル署名）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SSH User Authentication Lists（SSH ユーザ認証リスト）

SSH を使用してスイッチにアクセスを行うユーザの設定を行います。

Security > SSH > SSH User Authentication Lists の順にメニューをクリックし、以下の画面を表示します。

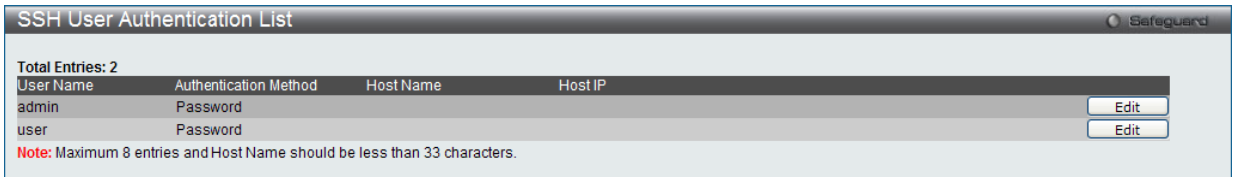


図 12-62 SSH User Authentication List 画面

上記画面例のユーザアカウントは **System Configuration > User Accounts** で既に設定されているものとします。SSH ユーザとしての項目を設定するためには、ユーザアカウントをあらかじめ登録しておく必要があります。

SSH ユーザの設定

1. SSH ユーザとしての項目を設定するためには、本画面で対応するエントリの「Edit」ボタンをクリックし、編集画面を表示します。

2. 以下の項目を使用して、参照または設定を行います。

項目	説明
User Name	SSH ユーザを識別するユーザ名を 15 文字までの半角英数字で指定します。本ユーザ名はスイッチにユーザアカウントとして登録済みである必要があります。
Authentication Method	スイッチにアクセスを試みるユーザの認証モードを以下から指定します。 • Host-Based - 認証用にリモート SSH サーバを使用する場合に選択します。本項目を選択すると、SSH ユーザ識別のために以下の情報を入力することが必要になります。 - Host Name - リモート SSH ユーザを識別する 31 文字までの半角英数字を入力します。 - Host IP - SSH ユーザの IP アドレスを入力します。 • Password - 管理者定義のパスワードを使用して認証を行う場合に選択します。本項目を選択すると、スイッチは管理者にパスワードの入力（確認のため 2 回）を促します。 • Public Key - SSH サーバ上の公開鍵を使用して認証を行う場合に選択します。
Host Name	リモート SSH ユーザを識別する 32 文字までの半角英数字を入力します。本項目は「Authentication Mode」で「Host-Based」を選択した場合のみ入力が必要です。
Host IP	SSH ユーザの IP アドレスを入力します。本項目は「Authentication Mode」で「Host-Based」を選択した場合のみ入力が必要です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 SSH User Authentication Mode の項目を設定するためには、事前にユーザアカウントを登録しておく必要があります。スイッチのローカルユーザアカウント設定に関する詳しい情報に関しては、本マニュアルの「User Accounts Settings（ユーザアカウントの設定）」（55 ページ）を参照してください。

Trusted Host Settings（トラストホスト）

最大 10 個までのトラストホストのセキュアな IP アドレスが、リモートのスイッチ管理のために設定され、使用できます。1 個以上のトラストホストが使用可能な状態にあると、スイッチは直ちに指定 IP アドレスからのリモートアクセスのみ許可することにご注意ください。この機能を有効にする場合、はじめに現在使用している IP アドレスを入力してください。

Security > Trusted Host Settings の順にクリックし、以下の画面を表示します。

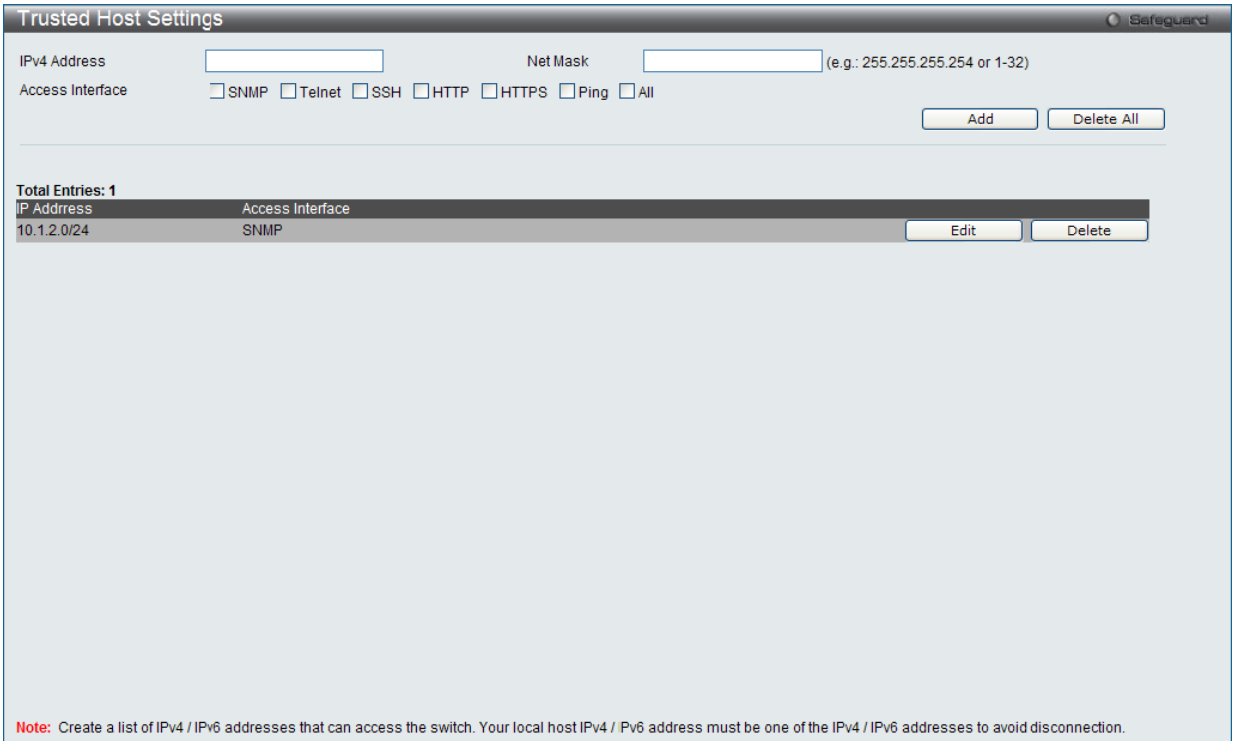


図 12-63　Trusted Host Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
IPv4 Address	IPv4 アドレスを入力してトラストホストリストに追加します。
Net Mask	ネットマスクを入力してトラストホストリストに追加します。
Access Interface	トラストホストに許可するサービスを選択します。

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの編集

1. 設定するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

Safeguard Engine Settings（セーフガードエンジン設定）

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃はスイッチに能力以上の負荷を加える可能性があります。このような問題を軽減するために、本スイッチのソフトウェアにセーフガードエンジン機能を付加しました。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。セーフガードエンジンには、Strict と Fuzzy の 2 つの操作モードがあります。

「Strict」モードでは、スイッチの CPU 使用率が設定した「Rising Threshold」を超えた場合に、「Exhausted」モードに遷移します。本モードでは、スイッチは算出された間隔で、信頼できない IP アドレスからのすべての IP ブロードキャストパケットを廃棄します。その後、5 秒毎に、スイッチの CPU 使用率をチェックします。しきい値を超過した場合、スイッチは、最初の 5 秒間で「Exhausted」モードに遷移します。その 5 秒後に、スイッチは再び CPU 利用率をチェックします。CPU 使用率が「Falling Threshold」より低いと、スイッチは再びすべてのパケットの受信を開始します。しかし、チェックにより、スイッチがビジー状態であることを示されると、前の停止間隔の 2 倍の期間「Exhausted」モードに遷移します。パケットの停止時間は、最大時間（320 秒）に達するまで倍増していき、それ以降は、通常の入力フローに戻るまで 320 秒で行われます。さらに理解するために、セーフガードエンジンについて以下に例示します。

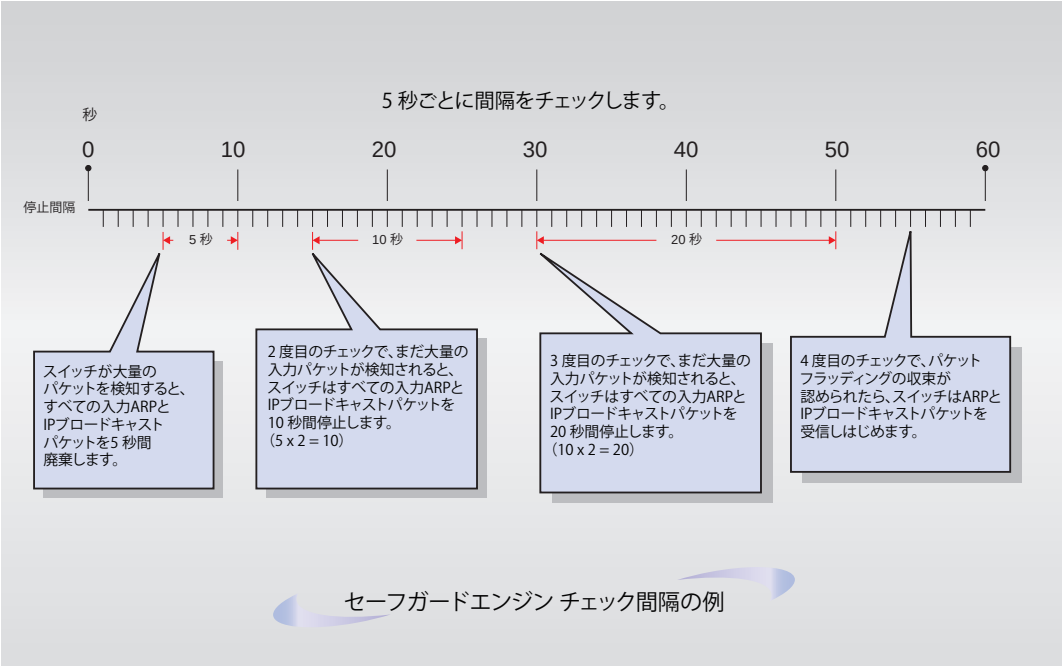


図 12-64　セーフガードエンジンの例

高い CPU 使用率の問題を明らかにするために継続したチェック間隔で、スイッチは特定のトラフィックをスイッチに対して制限するために「Exhausted」モードに入る時間を倍にします。上の例題では継続した高 CPU 利用率問題が 5 秒間隔で検出された場合に、「Exhausted」モードに入る時間を倍にしています。（最初の破棄 = 5 秒、2 回目の破棄 = 10 秒、3 回目の破棄 = 20 秒）一度、CPU 使用率が「Falling Threshold」を下回ると、「Exhausted」モードの待機期間は 5 秒に戻り、プロセスは再開します。

Fuzzy モードでは、一度セーフガードエンジンは Exhausted モードになると、スイッチに対するパケットフローは本モード開始時の半分のレベルまで減少させます。Normal モードに戻ると、パケットを 25%ずつ増加させます。スイッチは、その後間隔をチェックし、スイッチのオーバロードを避けるように動的に通常のパケットフローに戻します。

スイッチのセーフガードエンジン機能の有効化およびセーフガードエンジンの設定を行います。

Security > Safeguard Engine Settings の順にクリックし、以下の画面を表示します。

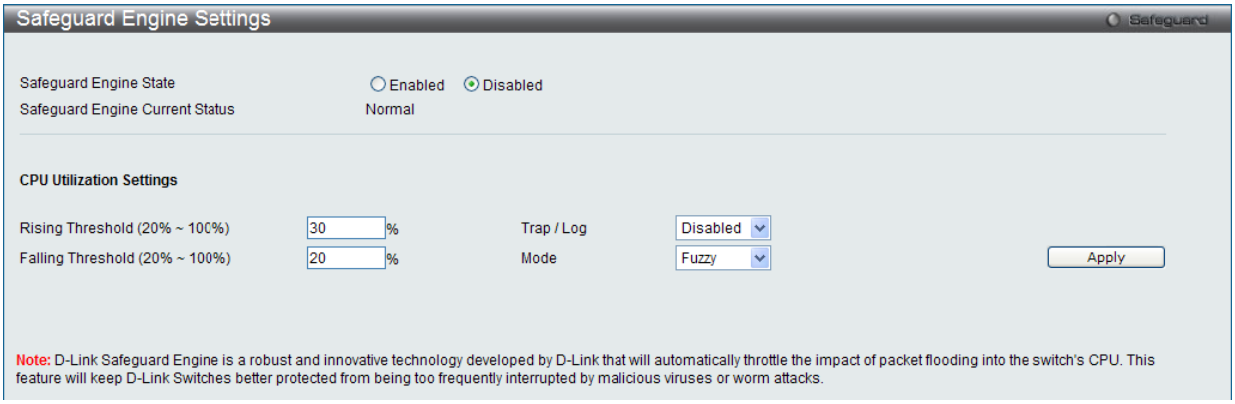


図 12-65　Safeguard Engine Settings 画面

セーフガードエンジンオプションの有効化

「Safeguard Engine State」を「Enabled」にします。

高度なセーフガードエンジン設定

以下の項目を設定します。

項目	説明
Safeguard Engine State	セーフガードエンジン機能を「Enabled」（有効）/「Disabled」（無効）にします。
Safeguard Engine Current Status	現在のセーフガードエンジンの状態を表示します。
Rising Threshold (20% ~ 100%)	Safeguard Engine を有効にする前に許容可能な CPU 使用率のレベルを設定します。CPU 使用率がこのしきい値に到達すると、ここで設定した項目に基づいて、Exhausted モードに入ります。
Falling Threshold (20% ~ 100%)	許容可能な CPU 使用率のレベルを設定します。スイッチは CPU 使用率がこのしきい値に到達すると Safeguard Engine 状態から Normal モードに戻ります。
Trap/Log	CPU 使用率が高くなりセーフガードエンジン機能が作動した際にデバイスの SNMP エージェントとスイッチのログにメッセージを送信する機能を「Enabled」（有効）/「Disabled」（無効）にします。
Mode	CPU 高使用率に到達した際に起動する Safeguard Engine のタイプを選択します。 • Fuzzy - スイッチは、適切なアルゴリズムに従ってダイナミックに帯域を調整します。（初期値） • Strict - スイッチは、信頼されていない IP アドレスから到着するすべての「IP ブロードキャスト」パケットの受信を停止し、「自分宛の ARP ではない」パケット（ARP パケットの宛先のプロトコルアドレスがスイッチ自身である）の帯域幅を減少させます。たとえどんな理由で CPU 高使用率に到達しても（ARP ストームが発生しないかもしれません）、スイッチは「Exhausted」モードで特定のパケットを処理することを意味します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

DoS Attack Prevention Settings（DoS アタック防止設定）

各 DoS（Denial-of-Service）攻撃に対して防御設定を行います。パケット照合はハードウェアで行われます。特定タイプの攻撃に対しては、パケットの内容を特定パターンと照合します。

Security > DoS Attack Prevention Settings の順にメニューをクリックし、以下の画面を表示します。

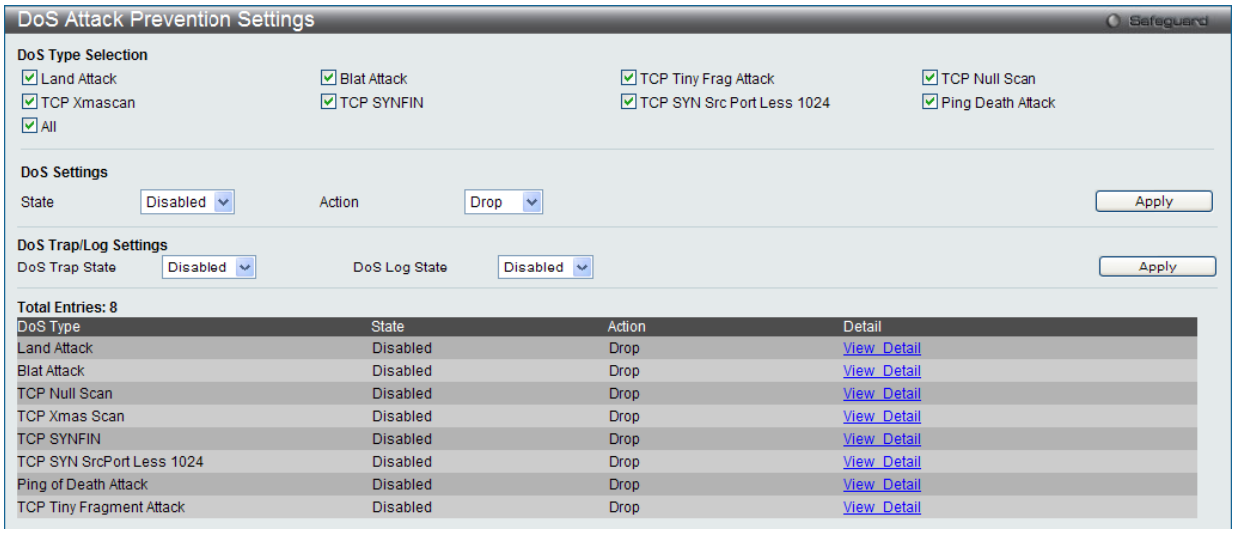


図 12-66 DoS Attack Prevention Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
DoS Type Selection	適切な DoS アタック防御のタイプを選択します。 • Land Attack - 送信元アドレスが受信した IP パケットの宛先アドレスと等しいかどうかをチェックします。 • Blat Attack - 送信元ポートが受信した TCP パケットの宛先ポートと等しいかどうかをチェックします。 • TCP Tiny Frag Attack - パケットが TCP Tiny フラグメントパケットであるかどうかをチェックします。 • TCP Null Scan - 受信した TCP パケットがシーケンス番号 0 を含むか、またはフラグを含まないかどうかをチェックします。 • TCP Xmascan - 受信した TCP パケットが URG、Push、および FIN フラグを含むかどうかをチェックします。 • TCP SYNFIN - 受信した TCP パケットが FIN と SYN フラグを含むかどうかをチェックします。 • TCP SYN Src Port Less 1024 - 受信した TCP パケットの送信元ポートが 1024 未満のパケットであるかどうかをチェックします。 • Ping Death Attack - 受信したパケットが断片化された ICMP パケットであるかどうかを検出します。 • All - すべての DoS アタックタイプを選択します。
DoS Settings	
State	DoS アタック防止を有効または無効にします。
Action	攻撃を検出した際に行うアクションを選択します。
DoS Trap/Log Settings	
DoS Trap State	DoS 防止トラップの状態を有効または無効に設定します。
DoS Log State	DoS 防止ログの状態を有効または無効に設定します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

詳細情報の表示

「DoS Type」の横に表示される「View Detail」リンクをクリックすると、以下の画面が表示されます。

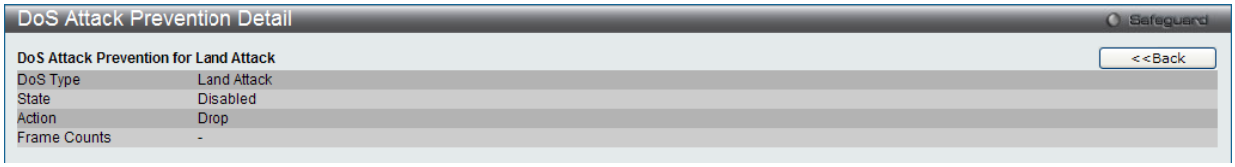


図 12-67 DoS Attack Prevention Detail 画面

「<<Back」をボタンをクリックして前のページに戻ります。

IGMP Access Control Settings（IGMP アクセスコントロール設定）

スイッチ上の各ポートに IGMP 認証（IGMP アクセスコントロール）を設定することができます。認証状態を有効にして、スイッチが IGMP JOIN リクエストを受信すると、スイッチは、認証を行うために RADIUS サーバにアクセスリクエストを送信します。

IGMP 認証では以下の手順で IGMP レポートを処理します。:
ホストが希望するマルチキャストグループに join メッセージを送信する場合、スイッチは、マルチキャストグループ / ポートを学習する前に、認証を行う必要があります。スイッチはホストの MAC アドレス、スイッチポート番号、スイッチの IP アドレス、およびマルチキャストグループの IP アドレスを含む情報のために認証サーバに Access-Request を送信します。Access-Accept が認証サーバから戻ってくると、スイッチはマルチキャストグループ / ポートについて学習します。Access-Reject が認証サーバから戻ってくると、スイッチはマルチキャストグループ / ポートを学習せず、パケットをそれ以上処理しません。エントリ（ホスト MAC、スイッチポート番号、およびマルチキャストグループ IP）は「認証失敗リスト」に置かれます。認証サーバからの応答が T1 期間後もない場合、スイッチはサーバに Access-Request を再度送信します。スイッチが N1 回後に応答を受信しないと、結果は拒否され、エントリ（ホスト MAC、スイッチポート番号、マルチキャストグループ IP）は「認証失敗リスト」に置かれます。通常、マルチキャストグループ / ポートがスイッチに既に学習されている場合、再度認証は行いません。規則通り、パケットを処理するだけです。

IGMP 認証では以下の手順で IGMP Leave を処理します。:
ホストが特定のマルチキャストグループに Leave メッセージを送信する場合、スイッチは、グループを離脱する標準的な手順に従って、AccountingRequest を通知としてアカウンティングサーバに送信します。認証サーバからの応答が T2 期間後もない場合、スイッチはサーバに Accounting-Request を再度送信します。最大リトライ回数は N2 です。

Security > IGMP Access Control Settings の順にメニューをクリックし、以下の画面を表示します。

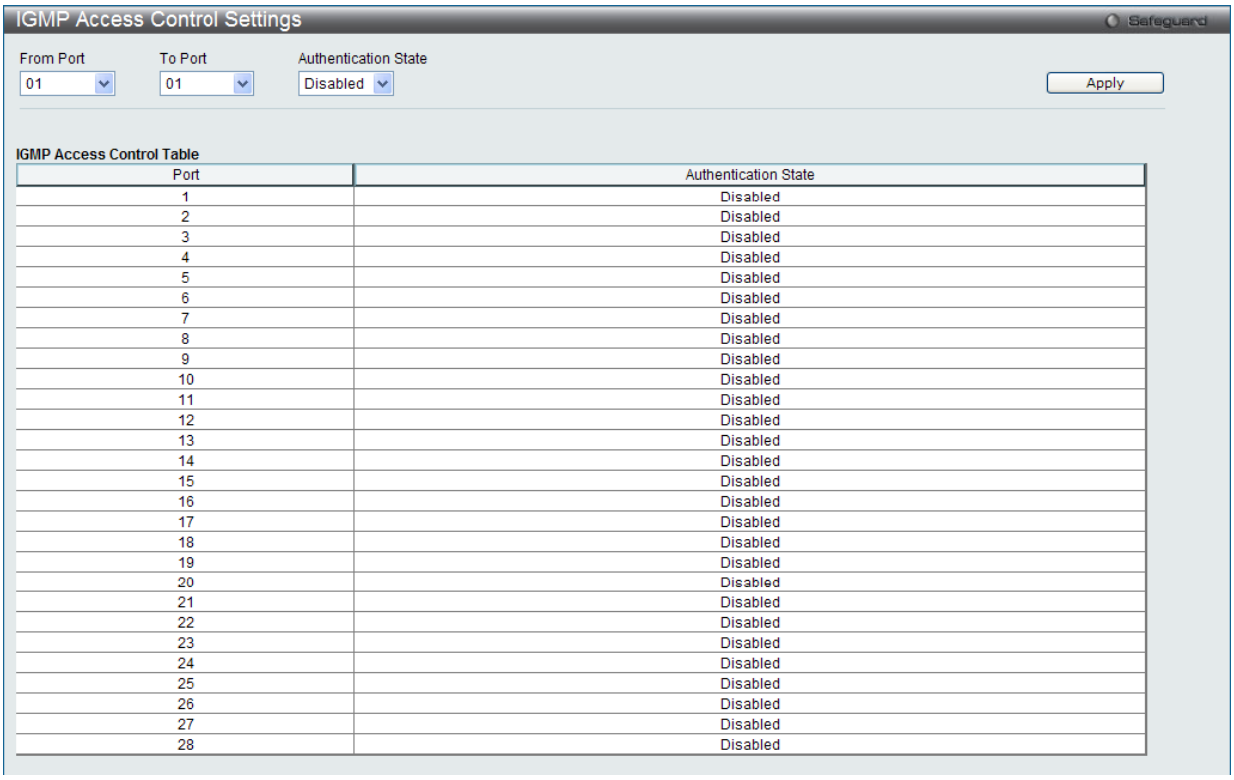


図 12-68 IGMP Access Control Settings 画面

以下の項目を設定します。

項目	説明
From Port / To Port	プルダウンメニューを使用して、コンパウンド認証ポートとして有効にするポート範囲を選択します。
Authentication State	プルダウンメニューを使用して、認証状態を有効または無効にします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

第 13 章　Network Application（ネットワークアプリケーション）

以下は Network Application サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
DHCP（DHCP 設定）	DHCP リレーの設定を行います。以下のメニューがあります。 DHCP Relay（DHCP リレー）、DHCP Local Relay Settings（DHCP ローカルリレー設定）、DHCP Local Relay Option 82 Settings（DHCP ローカルリレーオプション 82 設定）	260
PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入設定）	PPPoE Circuit ID の挿入機能を設定します。	267
SMTP Settings（SMTP 設定）	問題が発生した場合に設定した E-mail アドレスに従ってスイッチのログファイルを送信する SMTP サーバを設定します。	267
SNTP（SNTP 設定）	スイッチに時刻とタイムゾーンの設定を行います。以下のメニューがあります。 SNTP Settings（SNTP 設定）、Time Zone Settings（タイムゾーン設定）	268
Flash File System Settings（フラッシュファイルシステム設定）	フラッシュファイルシステムを利用したファイル操作を行います。	268

DHCP（DHCP 設定）

DHCP Relay（DHCP リレー）

DHCP Relay Global Settings（DHCP リレーグローバル設定）

DHCP リレーグローバル設定の有効化および設定を行うことができます。

DHCP メッセージが中継される最大のホップ（ルータの）数を「DHCP Relay Hops Count Limit」として、指定することができます。パケットのホップ数が、Hops Count Limit より多いと、そのパケットは廃棄されます。値の範囲は 1-16 で、初期値は 4 です。「Relay Time Threshold」はスイッチが DHCPREQUEST パケットを送出する前に待機する最小の時間（秒）です。パケットの「Seconds」の値が「DHCP Relay Time Threshold」の値より小さければ、そのパケットは廃棄されます。値の範囲は 0-65535 で初期値は 0（秒）です。

Network Application > DHCP > DHCP Relay > DHCP Relay Global Settings の順にメニューをクリックし、以下の画面を表示します。DHCP リレーのグローバル設定を有効にして、設定を行います。

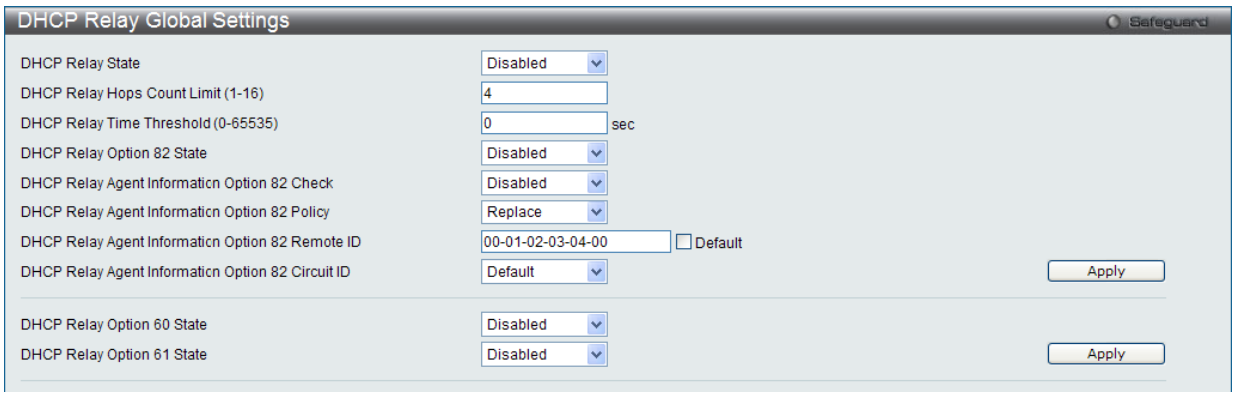


図 13-1　DHCP Relay Global Settings 画面

以下の項目が使用されます。

項目	説明
DHCP Relay State	スイッチ上で DHCP リレーサービスを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
DHCP Relay Hops Count Limit (1-16)	DHCP メッセージが中継されるルータホップの最大数（1-16）を定義します。初期値は 4 です。
DHCP Relay Time Threshold (0-65535)	DHCP パケットのルーティングを行うタイムリミットを 0-65535（秒）で定義します。0 を指定すると、スイッチは DHCP パケットの「Seconds」内の値の処理を行いません。0 以外の値を指定すると、スイッチはその値を使用し、ホップカウントと併用しながら DHCP パケットの送出を決定します。初期値は 0 です。
DHCP Relay Agent Option 82 State	スイッチ上で DHCP Agent Information Option 82 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。 • Enabled - リレーエージェントは DHCP サーバとクライアント間で交わすメッセージに DHCP Relay Information（「Option 82」欄）を挿入 / 削除します。リレーエージェントが DHCP リクエストを受信すると、Option 82 情報と（設定があれば）リレーエージェントの IP アドレスをパケットに付加します。Option 82 情報が付加されたパケットは DHCP サーバに送信されます。Option 82 をサポートする DHCP サーバがパケットを受信すると、そのサーバは remote ID、circuit ID、またはそれらの両方を使用して IP アドレスを割り当て、単一の remote ID または circuit ID に割り当て可能な IP アドレス制限などのポリシーを適用できます。また、DHCP サーバは「Option-82」欄の値を DHCP reply の中にそのまま残します。DHCP サーバはスイッチが DHCP request を中継していた場合には、ユニキャストで reply を返します。スイッチは remote ID や circuit ID 欄を調べて、本来の Option-82 情報が insert されていたかを確認します。スイッチは「Option-82」欄を削除してからそのパケットを DHCP クライアントに接続されているスイッチポートに転送します。 • Disabled - リレーエージェントは DHCP サーバとクライアント間で交換するメッセージへの DHCP Relay Information（「Option 82」欄）の挿入 / 削除を行いません。また、以下の Option 82 のチェックとポリシーの項目は無効になります。
DHCP Relay Agent Information Option 82 Check	スイッチのパケットの Option 82 項目の妥当性のチェックを行う機能を「Enabled」（有効）/「Disabled」（無効）にします。 • Enabled - リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行います。スイッチが DHCP クライアントから Option 82 項目を含むパケットを受信すると、スイッチはこれらのパケットは不正だとしてパケットを廃棄します。リレーエージェントは DHCP サーバから受信したパケットから不正なメッセージを削除します。 • Disabled - リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行いません。
DHCP Relay Agent Information Option 82 Policy	「DHCP Relay Agent Information Option82 Check」が「Disabled」の場合のパケットの処理ポリシー（Replace、Drop、または Keep）を設定します。初期値は「Replace」です。 • Replace - DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。 • Drop - DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。 • Keep - DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。
DHCP Relay Agent Information Option 82 Remote ID	Remote ID を入力します。「Default」に設定すると、Remote ID としてスイッチの MAC アドレスを使用します。
DHCP Relay Agent Information Option 82 Circuit ID	DHCP Relay Agent Information Option 82 Circuit ID を入力します。
DHCP Relay Option 60 State	DHCP Relay Option 60 State 機能を有効または無効にします。パケットが有効なオプション 60 を持たないと、リレーサーバをオプション 60 に基づいて決定できません。この場合、リレーサーバは、オプション 61 または IP インタフェースに従って設定したサーバに基づいて決定されます。リレーサーバをオプション 60 またはオプション 61 に基づいて決定すると、IP インタフェースに従って設定したサーバは無視されます。リレーサーバをオプション 60 またはオプション 61 で決定しないと、IP インタフェースに従って設定したサーバがリレーサーバを決定するのに使用されます。 • Enabled - 選択して、DHCP パケットをリレーするために、DHCP Relay Option 60 の状態を有効にします。 • Disabled - 選択して、DHCP Relay Option 60 の状態を無効にします。
DHCP Relay Option 61 State	DHCP Relay Option 61 State 機能を有効または無効にします。オプション 61 が有効な場合、パケットがオプション 61 を持たないと、リレーサーバをオプション 61 に基づいて決定できません。リレーサーバをオプション 60 またはオプション 61 に基づいて決定すると、IP インタフェースに従って設定したサーバは無視されます。リレーサーバをオプション 60 またはオプション 61 で決定しないと、IP インタフェースに従って設定したサーバは、リレーサーバを決定するのに使用されます。 • Enabled - 選択して、DHCP パケットをリレーするために、DHCP Relay Option 61 の状態を有効にします。 • Disabled - 選択して、DHCP Relay Option 61 の状態を無効にします。

「Apply」ボタンをクリックして設定内容を有効にします。

注意 スイッチが、DHCP クライアントから「Option-82」項目を含むパケットを受信し、チェック機能が「Enabled」（有効）になっている場合、スイッチはこのようなパケットは不正だとして、パケットを破棄します。しかし、場合によってはクライアント側で Option-82 情報が設定されることもあります。そのような状況では、チェック機能を無効にしてスイッチがパケットから Option-82 欄を破棄しないようにします。DHCP クライアントから受信したパケット内に既にリレー情報があった場合のスイッチの動作を「DHCP Agent Information Option 82 Policy」で指定します。

DHCP Relay Agent Information Option 82 の実装

config dhcp_relay option_82 コマンドは、スイッチの DHCP リレーエージェント Information Option 82 の設定を行う際に使用します。Circuit ID サブオプションおよび Remote ID サブオプションのフォーマットは以下の通りです。

注意 スタンドアロンスイッチの場合、サーキット ID のサブオプションのモジュールフィールドは常に 0 です。

サーキット ID のサブオプションフォーマット

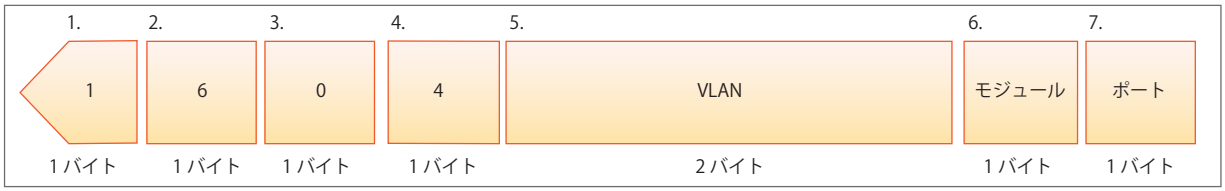


図 13-2　サーキット ID サブオプション形式

1. サブオプションタイプ
2. サブオプションタイプ長
3. Circuit ID タイプ
4. Circuit ID 長
5. VLAN : DHCP クライアントパケットを受信した VLAN
6. モジュール : スタンドアロンスイッチの場合は常に 0。スタッカブルスイッチの場合は Unit ID。
7. ポート : DHCP クライアントパケットを受信したポート番号。ポート番号は 1 から始まります。

リモート ID のサブオプションフォーマット（初期値）

図 13-3　リモート ID サブオプション形式

1. サブオプションタイプ
2. サブオプション長
3. Remote ID タイプ
4. Remote ID 長
5. MAC アドレス : スイッチのシステム MAC アドレス

DHCP Relay Interface Settings（DHCP リレーインタフェース設定）

DHCP 情報をスイッチに中継するために、IP アドレスでサーバを設定します。以下の画面を使用して、DHCP サーバに直接接続するスイッチ上に定義済みの IP インタフェースを入力します。正しく入力を行い「Apply」ボタンをクリックすると、以下の画面の下部に位置する「DHCP Relay Interface Table」にリスト表示されます。スイッチの 1 つの IP インタフェースに対して 4 件までのサーバ IP アドレスを登録できます。

Network Application > DHCP > DHCP Relay > DHCP Relay Interface Settings の順にメニューをクリックし、以下の画面を表示します。

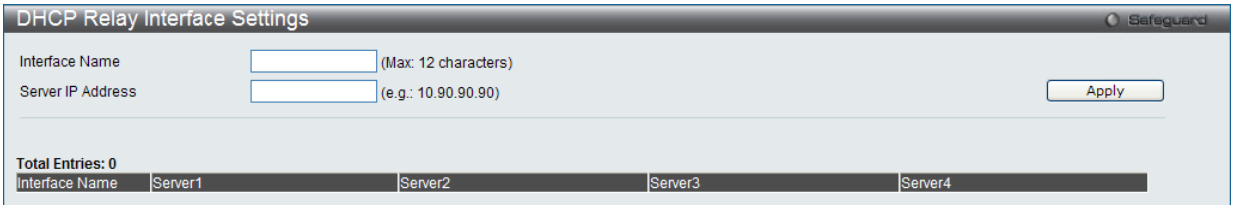


図 13-4　DHCP Relay Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface Name	DHCP サーバに直接接続するスイッチの IP インタフェース
Server IP Address	DHCP サーバの IP アドレス。1 つの IP インタフェースに対して 4 件までの入力が可能です。

「Apply」ボタンをクリックして設定内容を有効にします。

DHCP リレーインタフェース設定の削除
削除するエントリの「Delete」ボタンをクリックします。

DHCP Relay Option 60 Server Settings（DHCP リレーオプション 60 サーバ設定）

DHCP リレーオプション 60 サーバのパラメータを設定します。

DHCP オプション 60 はベンダクラス識別子です。本機能が有効である場合、スイッチは、DHCP クライアントからのオプション 60 をチェックして、それを送信すべき DHCP サーバを決定します。本スイッチに転送ルールを設定することができます。

Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Server Settings の順にメニューをクリックし、以下の画面を表示します。

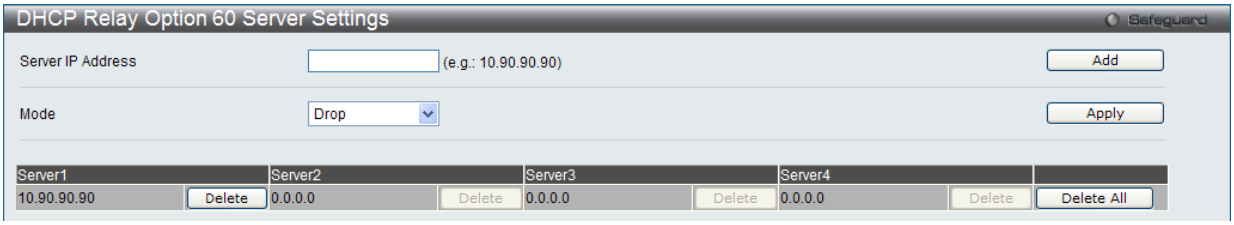


図 13-5　DHCP Relay Option 60 Server Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Server IP Address	DHCP リレーオプション 60 サーバのリレー IP アドレスを指定します。「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。
Mode	DHCP リレーオプション 60 サーバのモードを選択します。「Apply」ボタンをクリックして行った変更を適用します。

エントリの削除
「Delete」ボタンをクリックして、指定エントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

注意　オプション 60 に基づくパケットに一致しないサーバが発見された場合、リレーサーバはデフォルトリレーサーバによって判断されます。

DHCP Relay Option 60 Settings（DHCP リレーオプション 60 設定）

これは、DHCP リレーが DHCP オプション 60 を処理するかどうか決定します。

Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Settings の順にメニューをクリックし、以下の画面を表示します。

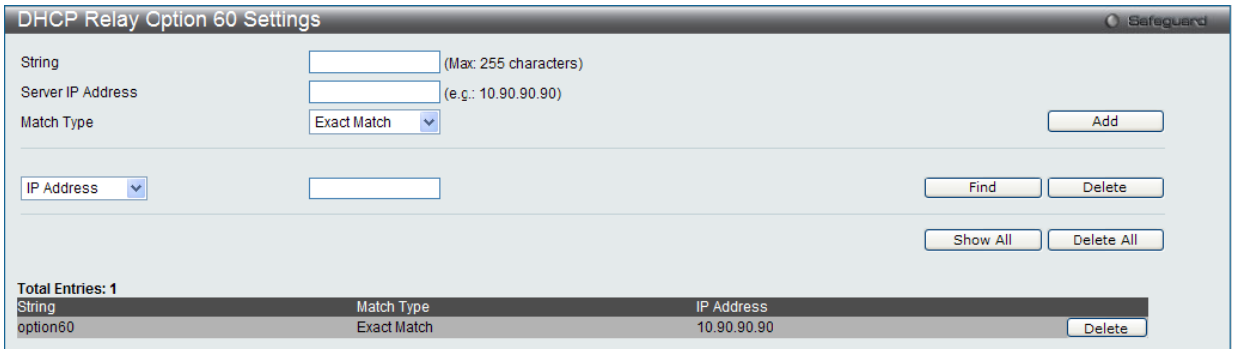


図 13-6　DHCP Relay Option 60 Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
String	DHCP リレーオプション 60 文字列を入力します。 同じリレーサーバに異なる文字列を指定でき、複数のリレーサーバに同じ文字列を指定できます。システムはすべてが一致しているサーバにパケットをリレーします。
Server IP	DHCP リレーオプション 60 サーバの IP アドレスを入力します。
Match Type	DHCP リレーオプション 60 サーバの一致タイプを入力します。 • Exact Match - パケットにおけるオプション 60 の文字列が指定した文字列に完全に一致する必要があります。 • Partial Match - パケットにおけるオプション 60 の文字列が指定した文字列に部分的にだけ一致する必要があります。
IP Address	DHCP リレーオプション 60 の IP アドレスを入力します。

エントリの追加
「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの参照
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの削除
「Delete」ボタンをクリックして、入力した情報に基づいて対応するエントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

DHCP Relay Option 61 Settings（DHCP リレーオプション 61 設定）

DHCP リレーオプション 61 のパラメータを追加および削除します。

Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Settings の順にメニューをクリックし、以下の画面を表示します。

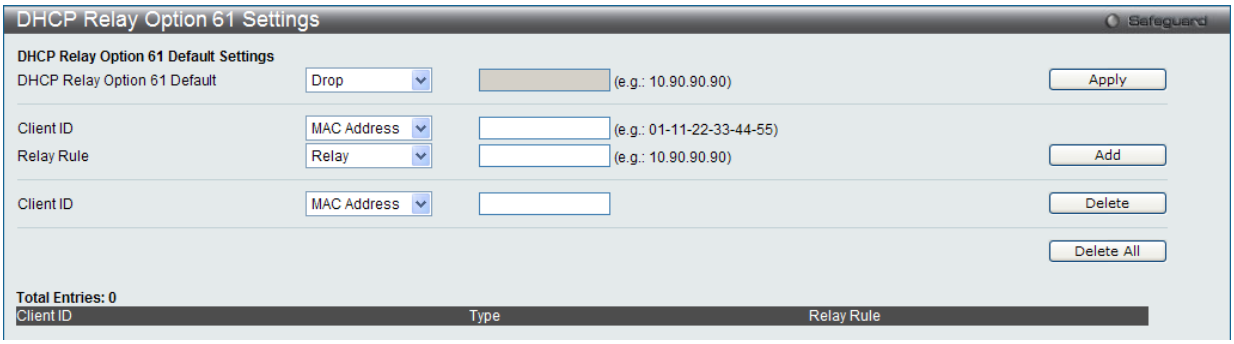


図 13-7　DHCP Relay Option 61 Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCP Relay Option 61 Default	DHCP リレーオプション 61 デフォルトオプションを選択します。 • Drop - パケットを破棄します。 • Relay - IP アドレスにパケットをリレーします。デフォルトリレーサーバの IP アドレスを入力します。オプション 61 に基づくパケットに一致しないサーバが発見された場合、リレーサーバはデフォルトリレーサーバ設定によって判断されます。
Client ID	• MAC Address - クライアントのハードウェアアドレスであるクライアント ID。 • String - 管理者によって指定されるクライアント ID。
Relay Rule	• Drop - パケットを破棄します。 • Relay - IP アドレスにパケットをリレーします。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの追加

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

DHCP Local Relay Settings（DHCP ローカルリレー設定）

DHCP クライアントが同じ VLAN から IP アドレスを取得する場合、DHCP ローカルリレー設定では、DHCP リクエストパケットにオプション 82 を追加できます。DHCP ローカルリレー設定をしないと、スイッチは VLAN にパケットをフラッドします。DHCP リクエストパケットにオプション 82 を追加するためには、DHCP ローカルリレー設定と Global VLAN の状態を有効にする必要があります。

Network Application > DHCP Server > DHCP Local Relay Settings の順にメニューをクリックし、以下の画面を表示します。

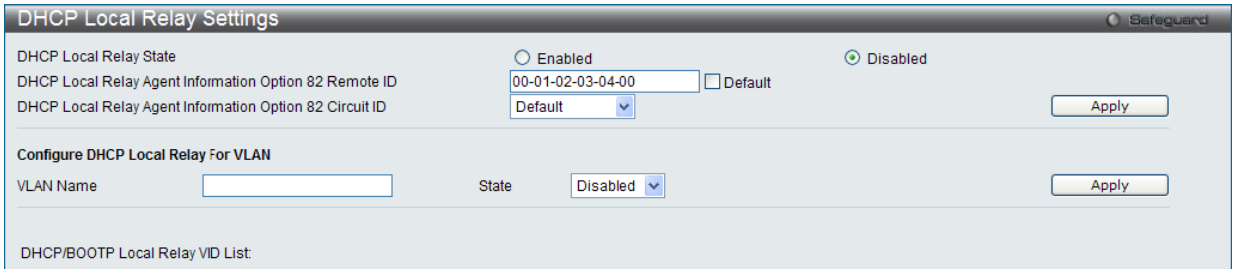


図 13-8　DHCP Local Relay Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCP Local Relay State	DHCP ローカルリレー設定を「Enabled」(有効) または「Disabled」(無効) にします。初期値は「Disabled」です。
DHCP Local Relay Agent Information Option 82 Remote ID	ユーザ定義の Remote ID を入力します。または、「Default」をチェックして、Remote ID としてスイッチの MAC アドレスを使用します。
DHCP Local Relay Agent Information Option 82 Circuit ID	DHCP Local Relay Agent Information Option 82 Circuit ID を入力します。
VLAN Name	DHCP ローカルリレー操作に適用する VLAN の識別に使用する VLAN 名です。
State	VLAN に対する DHCP ローカルリレー設定を「Enabled」(有効) または「Disabled」(無効) にします。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

DHCP Local Relay Option 82 Settings（DHCP ローカルリレーオプション 82 設定）

本画面は、オプション 82 ポリシーを処理する DHCP ローカルリレーの各ポートの設定に使用されます。

Network Application > DHCP > DHCP Local Relay Option 82 Settings の順にメニューをクリックし、以下の画面を表示します。

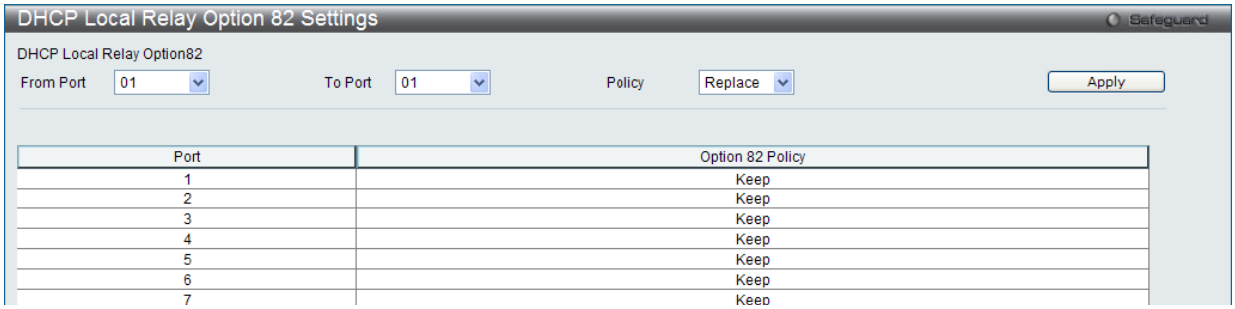


図 13-9　DHCP Local Relay Option 82 Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
From Port / To Port	プルダウンメニューを使用して使用するポート範囲を指定します。
Policy	オプション 82 フィールドを持つクライアント側から到着するパケットを処理する方法を選択します。 • Replace - パケット内の既存のオプション 82 フィールドを交換します。 • Drop - パケットにオプション 82 フィールドがある場合、破棄します。 • Keep - パケット内の既存のオプション 82 フィールドを保持します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入設定）

PPPoE Circuit ID の挿入機能を設定します。

Network Application > PPPoE Circuit ID Insertion Settings の順にメニューをクリックし、以下の画面を表示します。

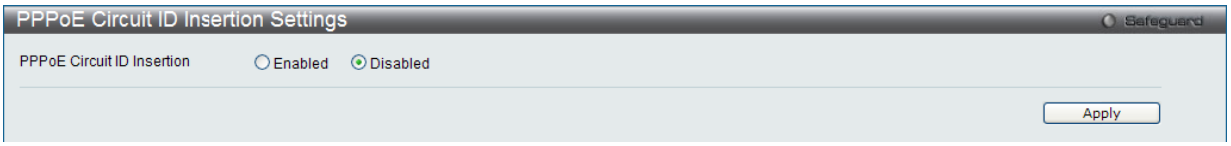


図 13-10　PPPoE Circuit ID Insertion Settings 画面

以下の項目を設定します。

項目	説明
PPPoE Circuit ID Insertion	スイッチの PPPoE Circuit ID の挿入を「Enabled」（有効）または「Disabled」（無効）にします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SMTP Settings（SMTP 設定）

SMTP（Simple Mail Transfer Protocol）は、以下の画面で入力するメール受信者にスイッチイベントを送信するスイッチの機能です。スイッチは SMTP のクライアントとして設定され、一方サーバはスイッチからメッセージを受信し、スイッチが設定した受信者に E-mail で適切な情報を送信します。これによって、小規模ワークグループや配線室の管理を簡素化、緊急のスイッチイベントの処理速度を向上、スイッチに起きた疑わしいイベントの記録によるセキュリティの強化など、スイッチ管理者の利便が図られます。

スイッチ用の SMTP サーバの設定と、問題がスイッチに発生した場合にスイッチのログファイルを送信する E-mail アドレスを設定します。

Network Application > SMTP Settings の順にメニューをクリックし、以下の画面を表示します。

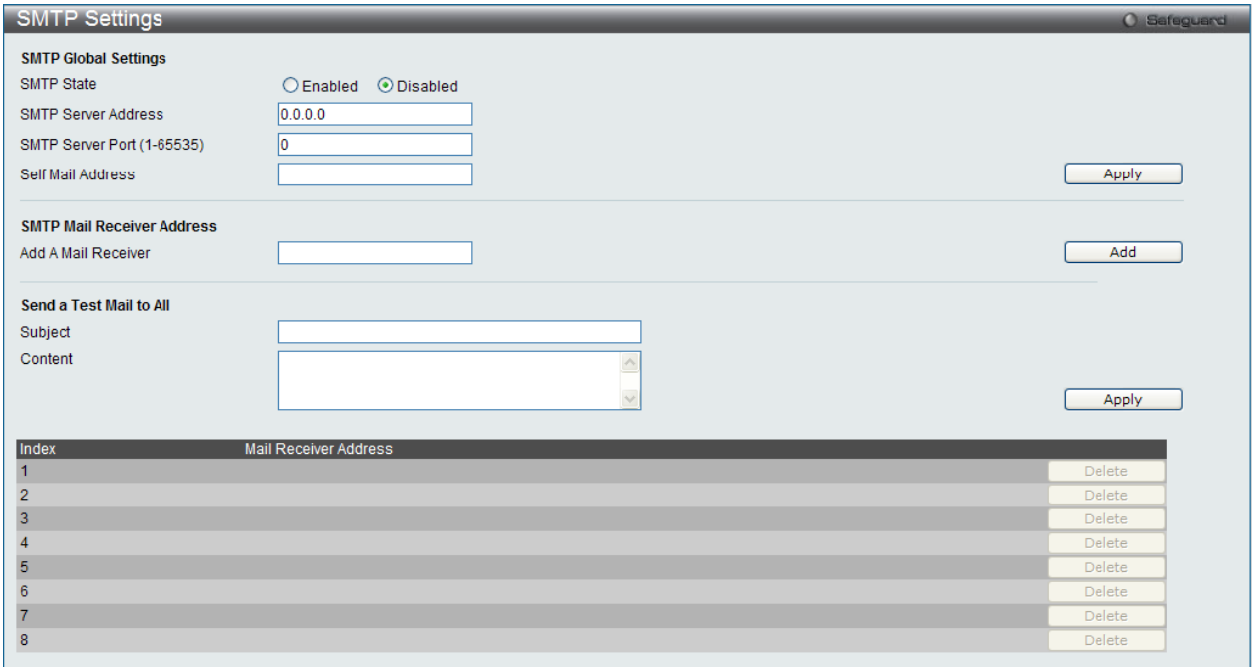


図 13-11　SMTP Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
SMTP Global Settings	
SMTP State	本デバイスの SMTP サービスを「Enabled」（有効）または「Disabled」（無効）にします。
SMTP Server Address	外部デバイスの SMTP サーバの IP アドレスを入力します。これはメールを送信するデバイスとなります。
SMTP Server Port (1-65535)	SMTP サーバに接続するスイッチの仮想ポート番号（1-65535）を入力します。SMTP の一般的なポート番号は 25 です。
Self Mail Address	メールメッセージの送信元 E-mail アドレスを入力します。このアドレスは受信者に送られる E-mail メッセージに送信元として記載されます。このスイッチに設定できるセルフメールアドレスは 1 つだけです。英数 64 文字以内で設定します。
SMTP Mail Receiver Address	
Add A Mail Receiver	E-mail アドレスを入力し、「Add」ボタンをクリックします。8 個までの E-mail アドレスを追加することができます。アドレスを削除する場合は、画面下部にある「Mail Receiver Address」テーブルで削除するエントリの「Delete」ボタンをクリックします。
Send a Test Mail to All	
Subject	テストメールの題名を入力します。
Content	テストメールの内容を入力します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。
「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。
「Delete」ボタンをクリックして、指定エントリを削除します。

SNTP（SNTP 設定）

SNTP（Simple Network Time Protocol ）はインターネット経由でコンピュータのクロックに同期するプロトコルです。標準時と周波数標準サービスへのアクセス、サーバとクライアントの SNTP サブネットの体系付け、および各関係者のシステムクロックの調整を行う包括的なメカニズムを提供します。

SNTP Settings（SNTP 設定）

スイッチに時刻を設定します。

Network Application > SNTP > SNTP Settings の順にクリックし、以下の画面を表示します。

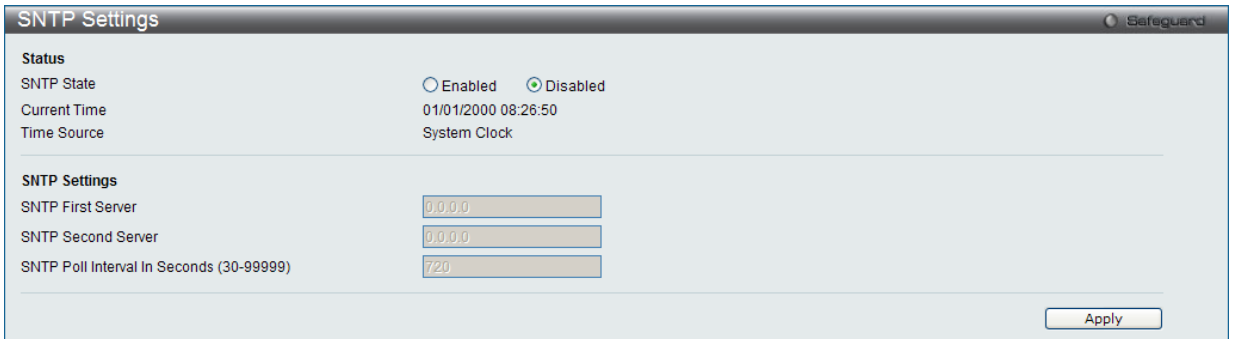


図 13-12 SNTP Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Status	
SNTP State	SNTP を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Current Time	現在の日付と時刻を表示します。
Time Source	システム時刻を設定するタイムソースを表示します。
SNTP Settings	
SNTP First Server	システム時刻を受け取るプライマリ SNTP サーバの IP アドレスを設定します。
SNTP Second Server	システム時刻を受け取るセカンダリ SNTP サーバの IP アドレスを設定します。
SNTP Poll Interval In Seconds (30-99999)	SNTP 情報の更新リクエストの送信間隔（秒）を設定します。

「Apply」ボタンをクリックし、デバイスに SNTP 設定を適用します。

Time Zone Settings（タイムゾーン設定）

以下の画面では、SNTP 用のタイムゾーンとサマータイム（Daylight Saving Time）の設定を行います。

Network Application > SNTP > Time Zone Settings の順にメニューをクリックし、以下の設定画面を表示します。

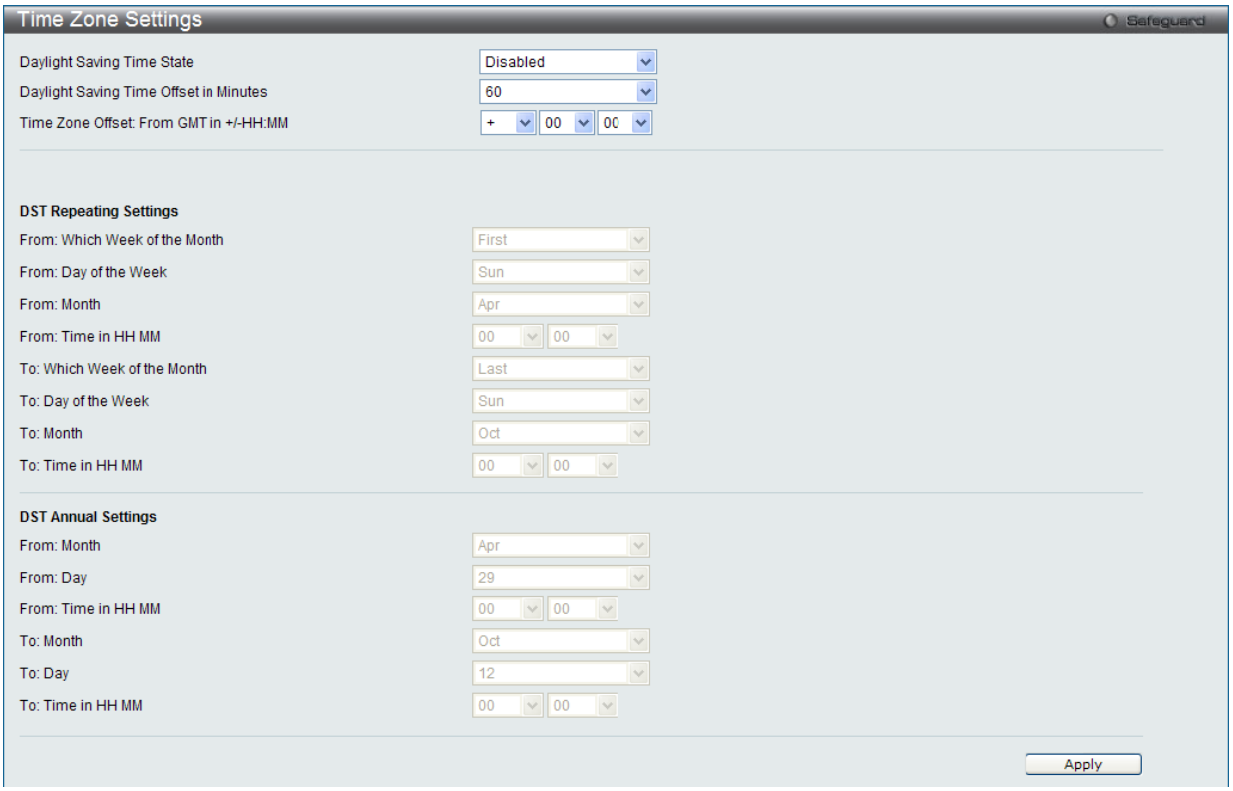


図 13-13　TimeZone Settings 画面

以下に、画面の各項目を示します。

項目	説明
Daylight Saving Time State	デバイスに設定するサマータイムの種類を設定します。 • Disabled - サマータイムを無効にします。（初期値） • Repeating - サマータイムを周期的に有効にします。このオプションでは開始と終了のタイミングを設定する必要があります。 • Annual - サマータイムを日付指定で有効にします。このオプションでは開始と終了の日付を設定する必要があります。
Daylight Saving Time Offset in Minutes	プルダウンメニューを使用して、サマータイムによる調整時間を 30、60、90、120 分から選択します。
Time Zone Offset: From GMT in +/ - HH:MM	プルダウンメニューを使用して、GMT（グリニッジ標準時）からのオフセット時間を選択します。
DST Repeating Settings	
Repeating モードを使用すると、DST（サマータイム）の設定を指定した期間で自動的に調整できるようになります。本モードでは、法則に従って指定される DST（サマータイム）の開始日と終了日が必要です。例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。	
From: Which Week of the Month	月の第何週から DST が始まるかを設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
From: Day of the Week	DST が開始する曜日を指定します。Sun、Mon、Tue、Web、Tues、Fri、Sat
From: Month	DST が開始する月を指定します。Jan、Feb、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec
From: Time In HH MM	DST が開始する時間を指定します。
To: Which Week of the Month	月の第何週で DST が終わるかを設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
To: Day of the Week	DST が終了する曜日を指定します。
To: Month	DST が終了する月を指定します。
To: Time in HH MM	DST が終了する時間を指定します。

項目	説明
DST Annual Settings	
Annual モードを使用すると、DST（サマータイム）設定を指定した詳細な期日で自動的に調整できるようになります。本モードを使用すると、DST（サマータイム）の開始日と終了日を簡潔に指定することが必要です。例：DST を 4 月 3 日から開始し、10 月 14 日を終了と設定します。	
From: Month	DST が開始する月を指定します。（毎年）
From: Day	DST が開始する日を指定します。（毎年）
From: Time in HH MM	DST が開始する時間を指定します。（毎年）
To: Month	DST が終了する月を指定します。（毎年）
To: Day	DST が終了する日を指定します。（毎年）
To: Time in HH MM	DST が終了する時間を指定します。（毎年）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Flash File System Settings（フラッシュファイルシステム設定）

フラッシュファイルシステムを使用する理由

古いスイッチシステムでは、ファームウェア、コンフィグレーション、およびログ情報は固定アドレスとサイズを持つフラッシュに保存されます。これは、最大のコンフィグレーションファイルが 2M バイトだけであり、現在のコンフィグレーションが 40K バイトにすぎなくても、フラッシュストレージスペースの 2M バイトを消費することを意味します。また、コンフィグレーションファイル番号とファームウェア番号は固定されています。コンフィグレーションファイルまたはファームウェアサイズが元々設計されたサイズを超えている場合、互換性の問題が発生します。

使用するシステムにおけるフラッシュファイルシステム

フラッシュファイルシステムは、フラッシュメモリにおける柔軟なファイル操作を提供します。すべてのファームウェア、コンフィグレーション情報、および Syslog ログ情報はフラッシュ内のファイルに保存されます。これは、すべてのファイルが取得したフラッシュスペースが固定されておらず、実ファイルサイズであることを意味します。フラッシュスペースが十分であれば、より多くのコンフィグレーションファイルまたはファームウェアファイルをダウンロードできます。また、フラッシュファイル情報の表示やファイル名の変更、および削除するコマンドを使用することができます。その上、必要に応じて、起動用のランタイムイメージや動作するコンフィグレーションファイルを設定できます。

ファイルシステムに不具合がある場合、Z- モデムを使用して直接システムにバックアップファイルをダウンロードすることができます。

Network Application > Flash File System Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-14　Flash File System Settings 画面

「Current Path」に現在のパスを入力し、「Go」ボタンをクリックすると入力したパスに遷移します。
「C:」リンクをクリックすると、「C:」ドライブに遷移します。

「C:」リンクをクリックすると、以下の画面が表示されます。

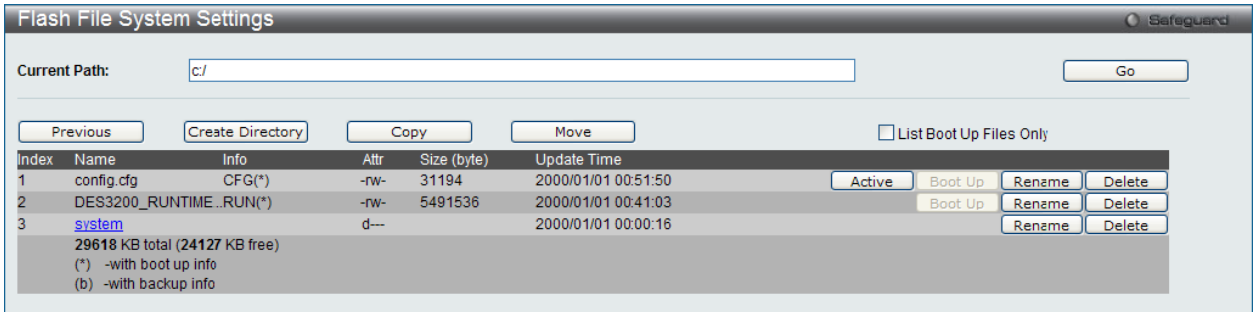


図 13-15　Flash File System Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Previous	前のページに戻ります。
Create Directory	スイッチのファイルシステムに新しいディレクトリを作成します。
Copy	指定ファイルをスイッチにコピーします。
Move	指定ファイルをスイッチに移動します。
List Boot Up Files Only	チェックすると起動ファイルだけを表示します。
Active	アクティブなランタイムコンフィグレーションとして指定したコンフィグファイルを設定します。
Boot Up	起動用のブートアップイメージとして指定したランタイムイメージを設定します。
Rename	指定ファイルを変更します。
Delete	ファイルシステムから指定ファイルを削除します。

ファイルのコピー

1. 「Copy」ボタンをクリックすると、以下の画面が表示されます。

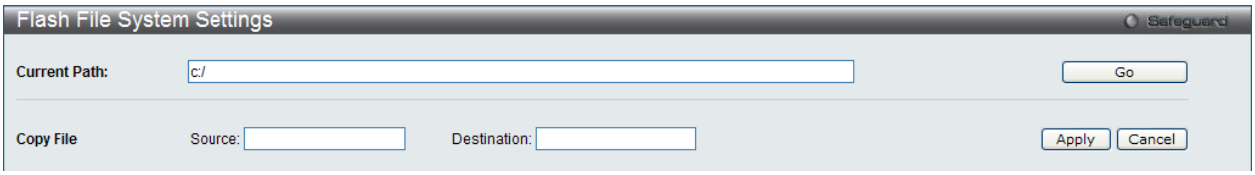


図 13-16 Flash File System Settings 画面 - Copy

2. このスイッチのファイルシステムにファイルをコピーする場合、送信元と送信先のパスを入力します。

3. 「Apply」ボタンをクリックして、コピーを開始します。「Cancel」ボタンをクリックすると処理は破棄されます。

ファイルの移動

「Move」ボタンをクリックすると、以下の画面が表示されます。

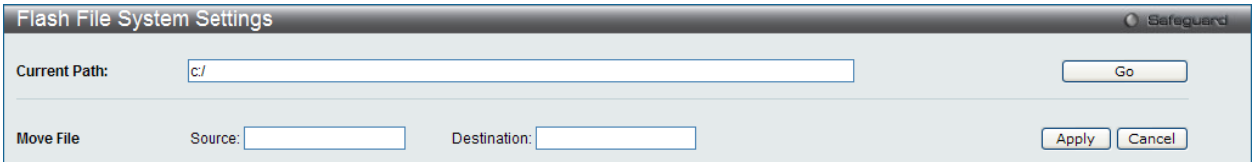


図 13-17 Flash File System Settings - Move 画面

ファイルを別の場所に移動する場合、「Source」（送信元）と「Destination」（送信先）のパスを入力する必要があります。
「Apply」ボタンをクリックして、コピーを開始します。
「Cancel」ボタンをクリックすると処理は破棄されます。

ファイル名の変更

1. 「Rename」ボタンをクリックすると、編集画面が表示されます。
2. ファイル名を変更して「Apply」ボタンをクリックします。

第 14 章　OAM（Operations、Administration、Maintenance：運用・管理・保守）

以下は OAM サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
CFM（Connectivity Fault Management : 接続性障害管理）	CFM 機能を設定します。以下のメニューがあります。CFM Settings（CFM 設定）、CFM Port Settings（CFM ポート設定）、CFM MIPCCM Table（CFM MIPCCM テーブル）、CFM Loopback Settings（CFM ループバック設定）、CFM Linktrace Settings（CFM リンクトレース設定）、CFM Packet Counter（CFM パケットカウンタ）、CFM Fault Table（CFM 障害テーブル）、CFM MP Table（CFM MP テーブル）	272
Ethernet OAM（イーサネット OAM）	ポートにイーサネット OAM モード、イベント、ログを設定します。以下のメニューがあります。Ethernet OAM Settings（イーサネット OAM 設定）、Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）、Ethernet OAM Event Log（イーサネット OAM イベントログ）、Ethernet OAM Statistics（イーサネット OAM 統計情報）	282
DULD Settings（単方向リンク検出設定）	ポートにおいて単方向リンク検出の設定および表示を行います。	285
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。	286

CFM（Connectivity Fault Management : 接続性障害管理）

CFM Settings（CFM 設定）

CFM 機能を設定します。

OAM > CFM > CFM Settings の順にメニューをクリックし、以下の画面を表示します。

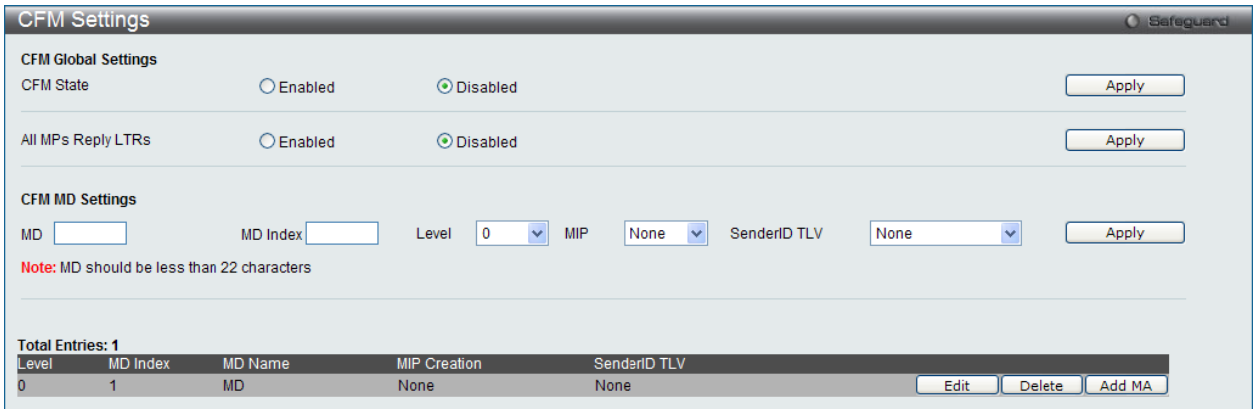


図 14-1　CFM Settings 画面

以下の項目を設定できます。

項目	説明
CFM Global Settings	
CFM State	CFM 機能を有効または無効にします。
All MPs Reply LTRs	Link Trace Reply（LTR）メッセージに応答するために、すべての MP（メンテナンスポイント）を有効または無効にします。
CFM MD Settings	
MD	メンテナンスドメインの名称を入力します。22 文字内で指定します。
MD Index	使用するメンテナンスドメインインデックスを入力します。
Level	メンテナンスドメインのレベルを選択します。レベルは、0-7 の範囲で設定します。0 が最も低く、7 が最も高いレベルです。
MIP	MIP の作成を制御します。 • None - MIP を作成しません。（初期値） • Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッチでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。 • Explicit - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。
SenderID TLV	SenderID TLV の転送を制御します。 • None - SenderID TLV を転送しません。（初期値） • Chassis - シャーシ ID 情報を持つ SenderID TLV を転送します。 • Manage - 管理アドレス情報を持つ SenderID TLV を転送します。 • Chassis Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、編集画面を表示します。
2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

注意 グループ名は 22 文字未満とします。

CFM メンテナンスアソシエーション（MA）設定

メンテナンスアソシエーションを設定します。

OAM > CFM > CFM Settings 画面で「Add MA」ボタンをクリックし、以下の画面を表示します。

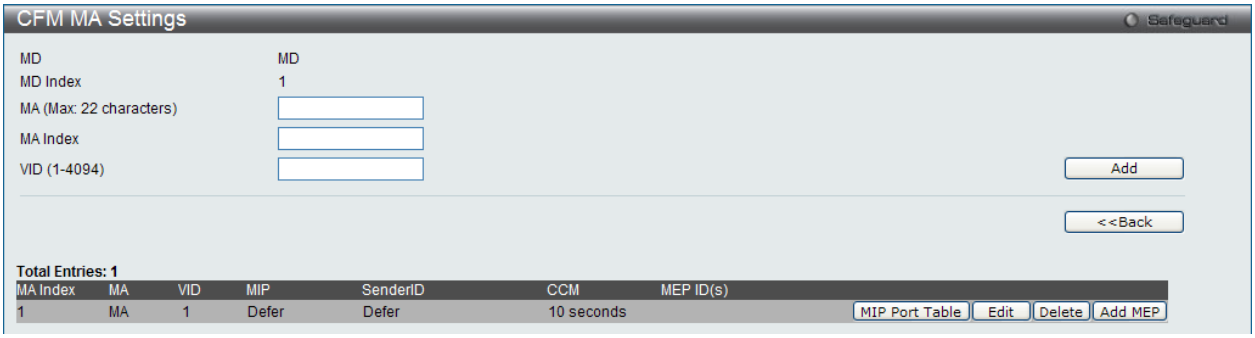


図 14-2　CFM MA Settings 画面

以下の項目が使用できます。

項目	説明
MA	メンテナンスアソシエーションの名称を入力します。
MA Index	メンテナンスアソシエーションのインデックスを入力します。
VID (1-4094)	VLAN 識別子。異なる MA は異なる VLAN に関連付ける必要があります。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。
「MIP Port Table」ボタンをクリックして、CFM MIP Table を参照します。
「Add MEP」ボタンをクリックして、MEP（Maintenance End Point）エントリを追加します。

エントリの削除

テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。

エントリの追加

項目入力後、「Add」ボタンをクリックします。

MIP ポートテーブルの参照

MIP ポートテーブルを参照します。

OAM > CFM > CFM Settings 画面で「MIP Port Table」ボタンをクリックします。

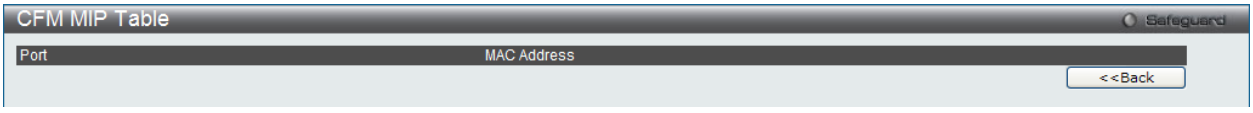


図 14-3　CFM MIP Table 画面

エントリの編集

エントリ横の「Edit」ボタンをクリックして、以下の画面を表示します。

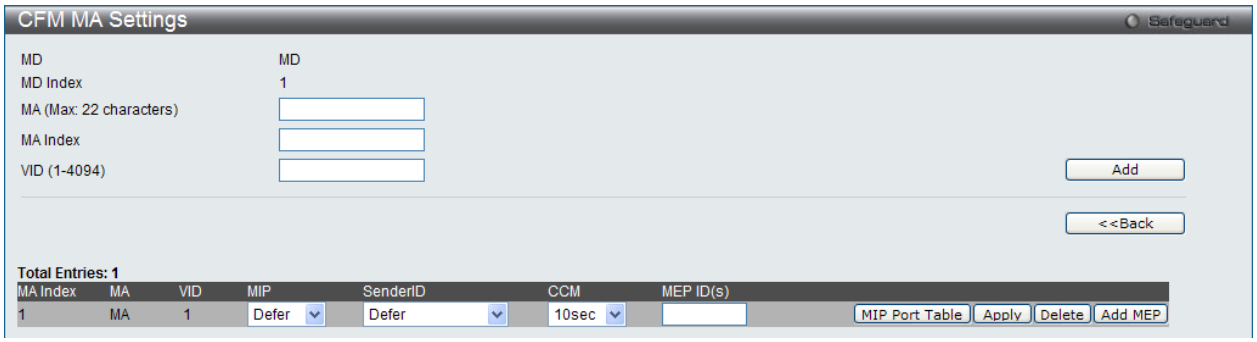


図 14-4　CFM MA Settings 画面 - Edit

以下の項目が使用できます。

項目	説明
MA	メンテナンスアソシエーションの名称を入力します。
MA Index	メンテナンスアソシエーションのインデックスを入力します。
VID	VLAN 識別子。異なる MA は異なる VLAN に関連付ける必要があります。
MIP	MIP の作成を制御します。 • None - MIP を作成しません。（ハードウェアモード : 初期値） • Defer - この MA が関連するメンテナンスドメインの設定を継承します。（ソフトウェアモード : 初期値） • Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッチでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。 • Explicit - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。 注意　CFM ハードウェアモードでは初期値は「None」です。
SenderID	これは、SenderID TLV の転送を制御します。 • None - SenderID TLV を転送しません。 • Chassis - シャーシ ID 情報を持つ SenderID TLV を転送します。 • Manage - 管理アドレス情報を持つ SenderID TLV を転送します。 • Chassis Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。 • Defer - この MA が関連するメンテナンスドメインの設定を継承します。（初期値）
CCM	これは CCM 送信間隔です。 • 10ms - 10（ミリ秒）。これは CFM ハードウェアモードでのみ動作します。（推奨されません。） • 100ms - 100（ミリ秒）。（推奨されません。） • 1sec - 1（秒） • 10sec - 10（秒）（初期値） • 1min - 1（分） • 10min - 10（分）
MEP ID(s)	メンテナンスアソシエーションに含まれる MEP ID を指定します。 初期値では、初めて作成されたメンテナンスアソシエーションには MEP ID はありません。MEP ID の範囲は、1-8191 です。

2.　項目設定後、「Apply」ボタンをクリックします。

CFM MEP 設定

MEP を追加します。

OAM > CFM > CFM Settings 画面で「Add MEP」ボタンをクリックし、以下の画面を表示します。

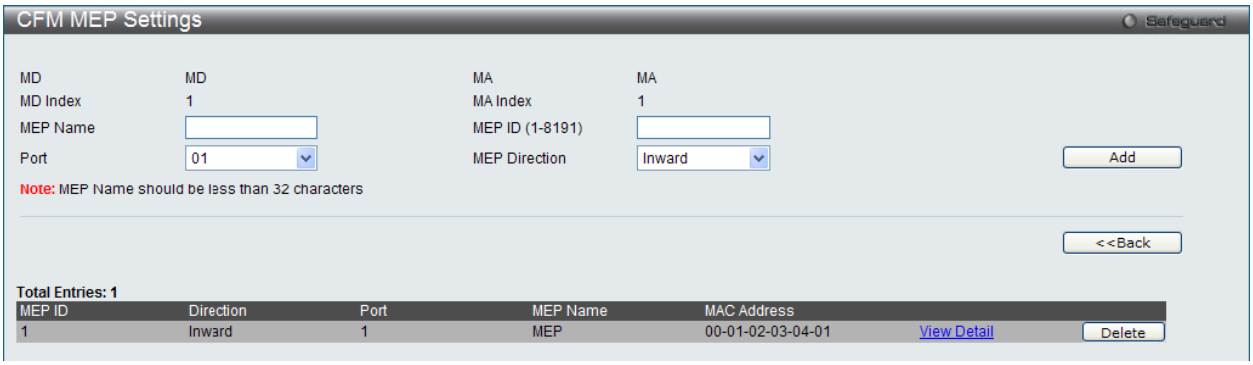


図 14-5　CFM MEP Settings 画面

以下の項目を設定できます。

項目	説明
MEP Name	MEP 名（32 文字以内）を入力します。デバイスに設定されたすべての MEP 内で固有です。
MEP ID (1-8191)	MA の MEP ID リストに設定される MEP ID を入力します。
Port	ポートを指定します。本ポートは MA の関連付けられている VLAN メンバである必要があります。CFM ハードウェアモードでは、本ポートは MA の関連付けられている VLAN のメンバである必要があります。
MEP Direction	MEP の方向を指定します。 • Inward - 内向き（アップ）MEP。内向きの MEP は、内側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。そして、フレームの送信元が内向きまたは外向きにかかわらず、より高いレベルにあるすべての CFM フレームを転送します。 • Outward - 外向き（ダウン）MEP。外向きのポートは、ブリッジリレー機能側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。それは、そのレベルにあるすべての CFM フレームを処理して、ブリッジポートからから受信する低いレベルの CFM フレームすべてを破棄します。外向きポートは、フレームの送信先の方向にかかわらず、より高いレベルにあるすべての CFM フレームを転送します。

項目設定後、「Add」ボタンをクリックします。

MEP エントリに関する詳細情報の参照

「View Detail」リンクをクリックし、以下の画面を表示します。

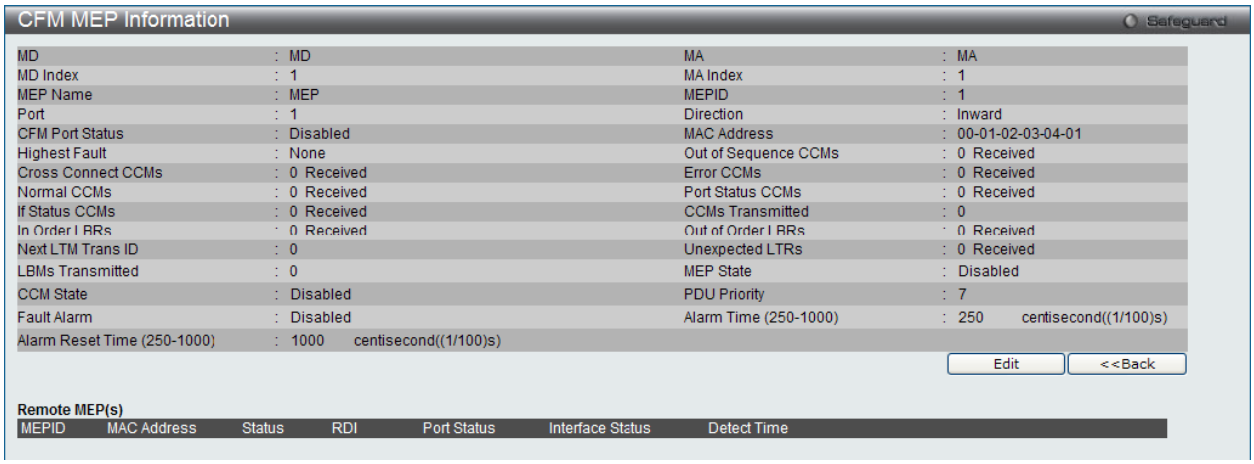


図 14-6　CFM MEP Information 画面

MEP の編集

「Edit」ボタンをクリックし、以下の画面を表示します。

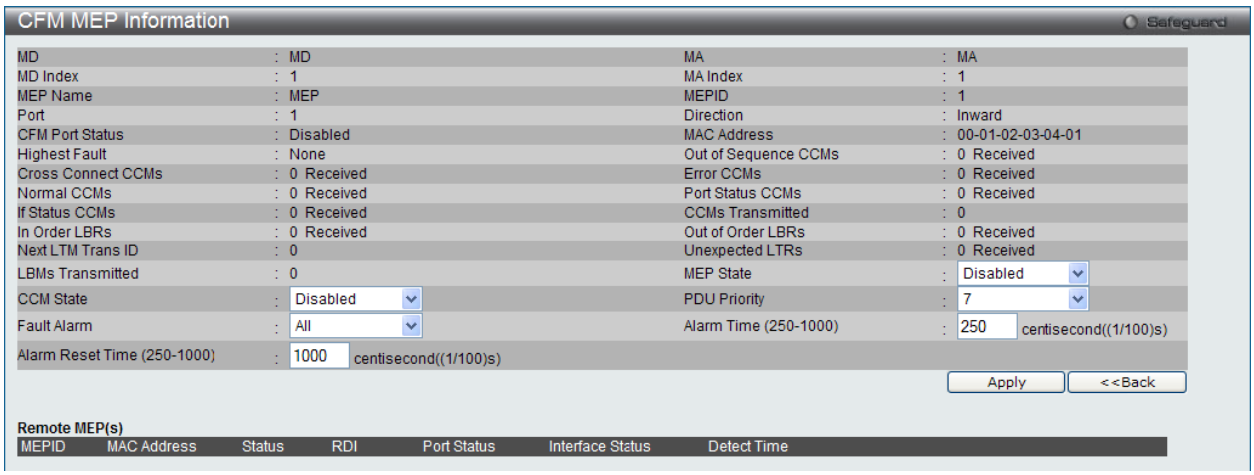


図 14-7　CFM MEP Information 画面 - Edit

以下の項目を設定または表示できます。

項目	説明
MEP State	MEP 管理状態を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
CCM State	CCM 送信状態を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
PDU Priority	802.1p 優先度は MEP によって送信された CCM および LTM メッセージに設定されます。初期値は 7 です。
Fault Alarm	これは、MEP によって送信される障害アラームの制御タイプです。 • All - すべての障害アラームのタイプが送信されます。 • Mac Status - 優先度が「Some Remote MEP MAC Status Error」（リモート MEP の MAC ステータスエラー）以上である障害アラームだけが送信されます。 • Remote CCM - 優先度が「Some Remote MEP Down」（リモート MEP のダウン）以上である障害アラームだけが送信されます。 • Error CCM - 優先度が「Error CCM Received」（エラー CCM の受信）以上である障害アラームだけが送信されます。 • Xcon CCM - 優先度が「Cross-connect CCM Received」（クロスコネクト CCM の受信）以上である障害アラームだけが送信されます。 • None - 障害アラームは送信されません。（初期値）
Alarm Time (250-1000)	これは、障害検出後に障害アラームが送信されるまでの経過時間です。範囲は 250-1000（センチ秒）です。初期値は 250（センチ秒）です。
Alarm Reset Time (250-1000)	これは、障害による再度アラーム送信前の検知が始動されるまでの待機時間です。範囲は 250-1000（センチ秒）です。初期値は 1000（センチ秒）です。

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

CFM Port Settings（CFM ポート設定）

ポートベースで CFM ポート状態を有効または無効にします。

OAM > CFM > CFM Port Settings の順にメニューをクリックし、以下の画面を表示します。

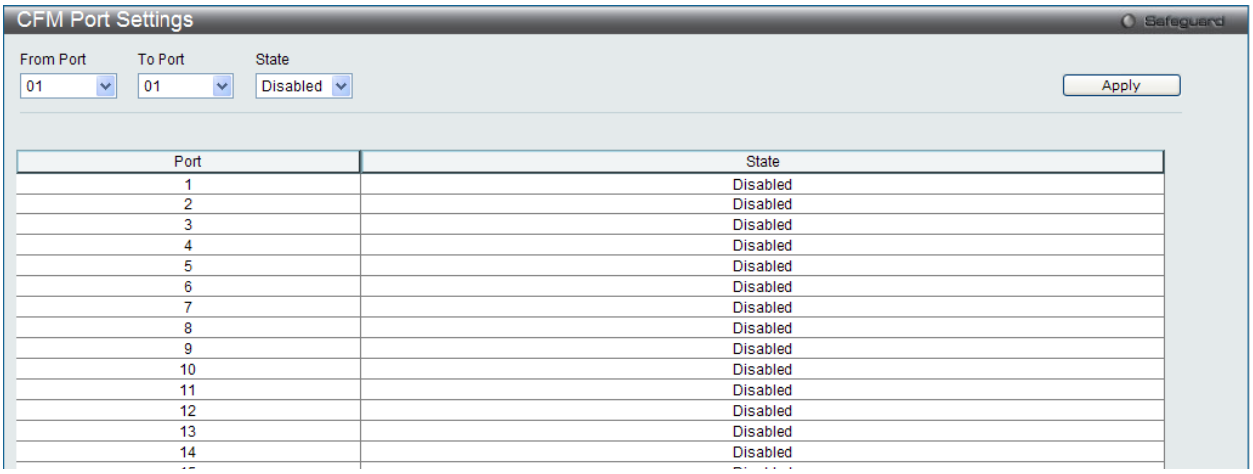


図 14-8　CFM Port Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
From Port/To Port	本設定に使用されるポート範囲を選択します。
State	特定ポートの CFM 設定を有効または無効にします。初期値は無効です。

「Apply」ボタンをクリックし、変更を有効にします。

CFM MIPCCM Table（CFM MIPCCM テーブル）

MIP CCM データベースのエントリを表示します。

OAM > CFM > CFM MIPCCM Table の順にメニューをクリックし、以下の画面を表示します。

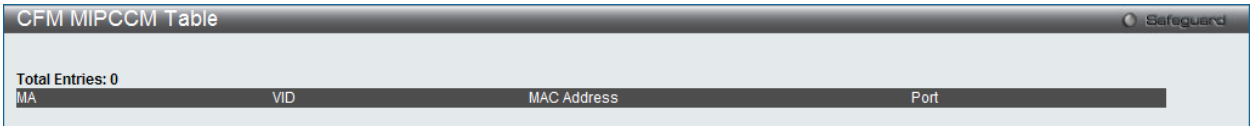


図 14-9　CFM MIPCCM Table 画面

CFM Loopback Settings（CFM ループバック設定）

CFM ループバックテストを設定します。

OAM > CFM > CFM Loopback Settings の順にメニューをクリックし、以下の画面を表示します。

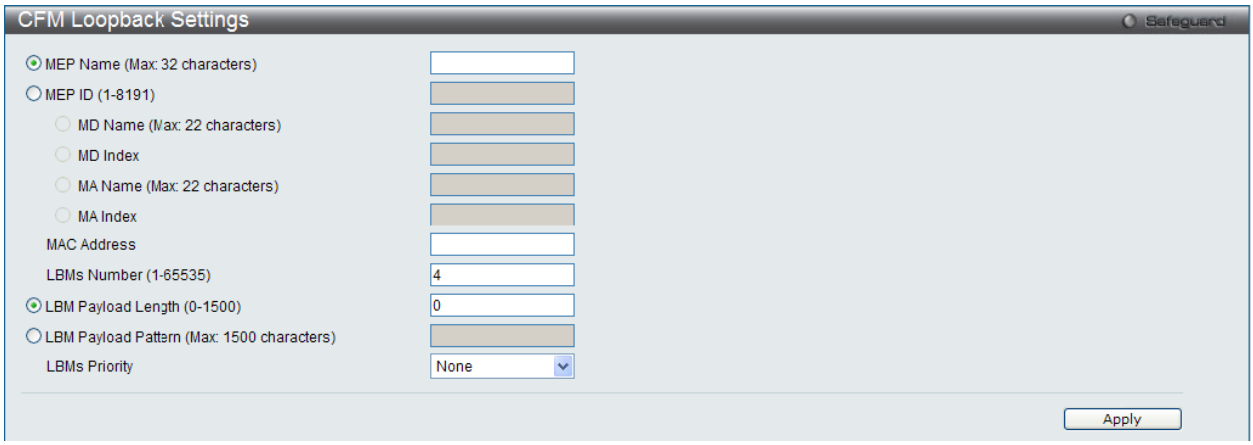


図 14-10　CFM Loopback Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
MEP Name (Max: 32 characters)	MEP 名を入力します。
MEP ID (1-8191)	MEP ID を入力します。
MD Name	使用するメンテナンスドメイン名を指定します。
MD Index	使用するメンテナンスドメインのインデックスを指定します。
MA Name	使用するメンテナンスアソシエーション名を指定します。
MA Index	使用するメンテナンスアソシエーションのインデックスを指定します。
MAC Address	宛先 MAC アドレスを入力します。
LBMs Number (1-65535)	送信する LBM 数。初期値は 4 です。1 ～ 65535 の範囲で指定します。
LBM Payload Length (0-1500)	送信される LBM のペイロード長。初期値は 0 です。
LBM Payload Pattern (Max: 1500 characters)	データ TLV が含まれるかどうかの指示に伴うデータ TLV に含める任意データの量。
LBMs Priority	送信される LBM に設定される 802.1p 優先度（0-7）。指定しない場合、MA が送信した CCM と LTM と同じ優先度を使用します。初期値は「None」（なし）です。

「Apply」ボタンをクリックし、変更を有効にします。

CFM Linktrace Settings（CFM リンクトレース設定）

CFM リンクトラックメッセージの発行、またはリンクトレース応答の表示、削除を行います。

OAM > CFM > CFM Linktrace Settings の順にメニューをクリックし、以下の画面を表示します。

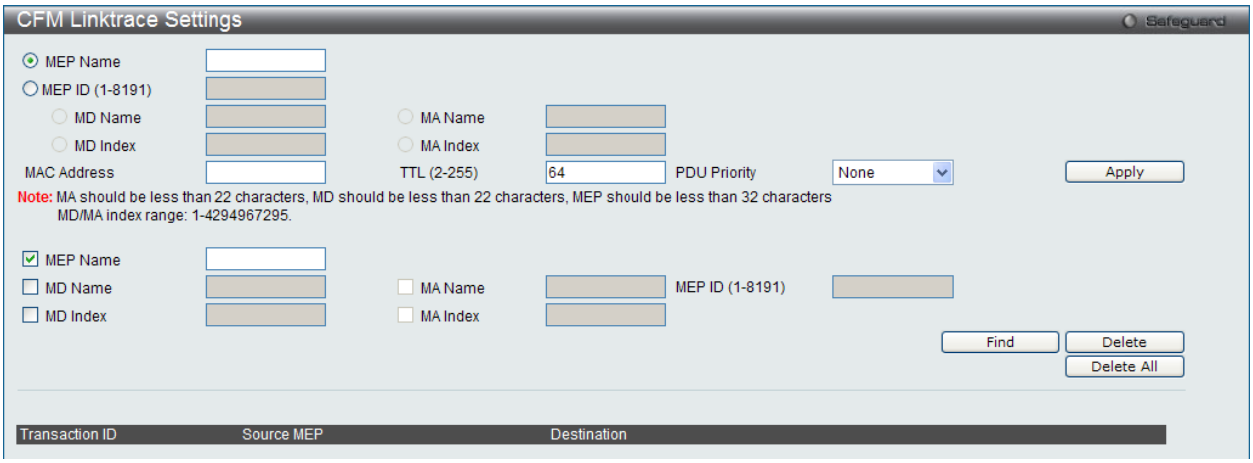


図 14-11　CFM Linktrace Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
MEP Name	使用するメンテナンスエンドポイントを指定します。
MEP ID (1-8191)	使用するエンドポイント ID を指定します。
MD Name	使用するメンテナンスドメイン名を指定します。
MD Index	使用するメンテナンスドメインのインデックスを指定します。
MA Name	使用するメンテナンスアソシエーション名を指定します。
MA Index	使用するメンテナンスアソシエーションのインデックスを指定します。
MAC Address	送信先 MAC アドレスを入力します。
TTL (2-255)	リンクトレースメッセージの TTL 値。初期値は 64 です。範囲は 2-255 です。
PDU Priority	送信される LTM に設定される 802.1p 優先度（0-7）。指定しない場合、MEP が送信した CCM と CCM と同じ優先度を使用します。

「Apply」ボタンをクリックし、変更を有効にします。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。検出後、「View Detail」リンクをクリックすると、CFM リンクトレースの詳細情報が表示されます。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

CFM Packet Counter（CFM パケットカウンタ）

CFM パケットの送受信カウンタ情報を表示します。

OAM > CFM > CFM Packet Counter の順にメニューをクリックし、以下の画面を表示します。

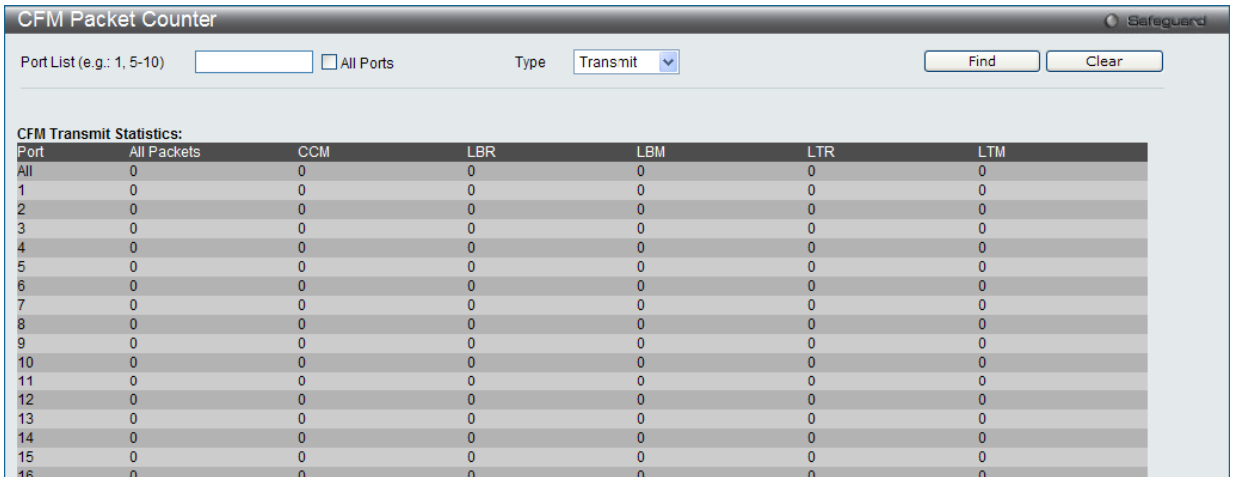


図 14-12　CFM Packet Counter 画面

画面には以下の項目があります。

項目	説明
Port List	参照するポートを選択します。「All Ports」を選択すると、すべてのポートを表示します。
Type	• Receive - 受信したすべての CFM パケットを表示します。 • Transmit - 送信したすべての CFM パケットを表示します。 • CCM - 送受信したすべての CCM パケットを表示します。

参照するポート番号を入力し、「Find」ボタンをクリックします。
「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。

CFM Fault Table（CFM 障害テーブル）

エラーとなった MEP を表示します。

OAM > CFM > CFM Fault Table の順にメニューをクリックし、以下の画面を表示します。

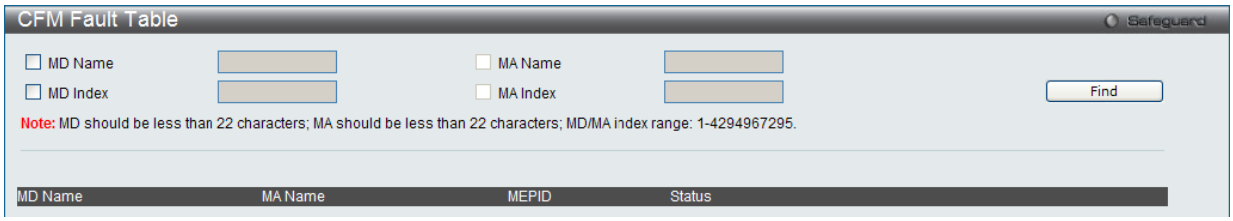


図 14-13　CFM Fault MEP 画面

画面には以下の項目があります。

項目	説明
MD Name	表示するメンテナンスドメイン名を指定します。
MD Index	表示するメンテナンスドメインのインデックスを指定します。
MA Name	表示するメンテナンスアソシエーション名を指定します。
MA Index	表示するメンテナンスアソシエーションのインデックスを指定します。

項目入力後、「Find」ボタンをクリックして、特定の MD および MA の接続障害を表示します。

CFM MP Table（CFM MP テーブル）

CFM MP 情報を表示します。

OAM > CFM > CFM MP Table の順にメニューをクリックし、以下の画面を表示します。

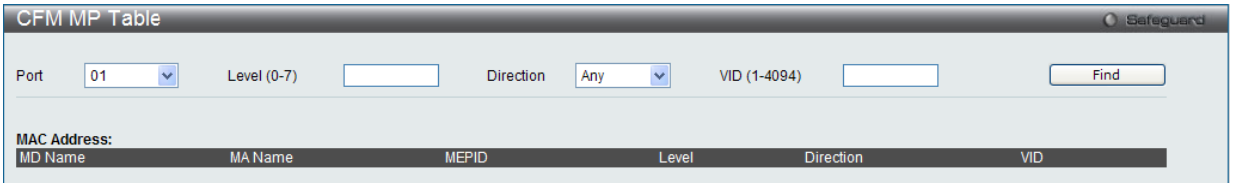


図 14-14 CFM MP Table 画面

画面には以下の項目があります。

項目	説明
Port	参照するポート番号を選択します。
Level (0-7)	参照するレベルを指定します。
Direction	プルダウンメニューを使用して参照する方向を選択します。 • Inward - 内向き MP を示します。 • Outward - 外向き MP を示します。
VID (1-4094)	参照するエントリの VID を指定します。

項目入力後、「Find」ボタンをクリックして、エントリをテーブルに表示します。

Ethernet OAM（イーサネット OAM）

Ethernet OAM Settings（イーサネット OAM 設定）

ポートにイーサネット OAM モードを設定します。

OAM > Ethernet OAM > Ethernet OAM Settings の順にメニューをクリックし、以下の画面を表示します。

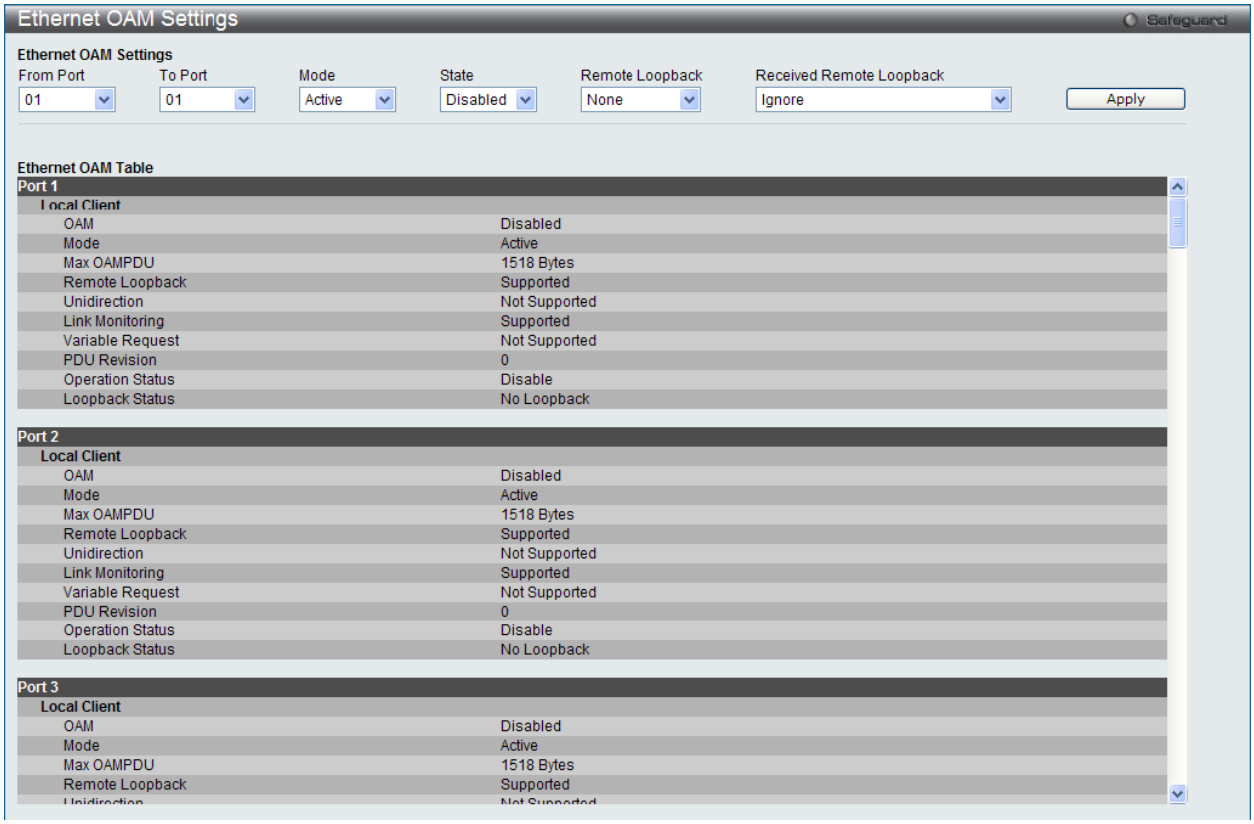


図 14-15　Ethernet OAM Settings 画面

以下の項目を設定できます。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Mode	動作するモード（「Active」または「Passive」）を指定します。初期モードは「Active」です。
State	OAM 機能を有効または無効にします。初期値は無効です。
Remote Loopback	• None - リモートループバックを行いません。（初期値） • Start - リモートループバックモードに変更するようにピアに要求します。 • Stop - 通常の操作モードに変更するようにピアに要求します。
Received Remote Loopback	クライアントが受信したイーサネット OAM リモートループバックコマンドの処理を指定します。 • Process - 受信したイーサネット OAM リモートループバックコマンドを処理します。 • Ignore - 受信したイーサネット OAM リモートループバックコマンドを無視します。（初期値）

「Apply」ボタンをクリックし、変更を有効にします。

Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）

ポートにイーサネット OAM のイベントを設定します。

OAM > Ethernet OAM > Ethernet OAM Configuration Settings の順にメニューをクリックし、以下の画面を表示します。

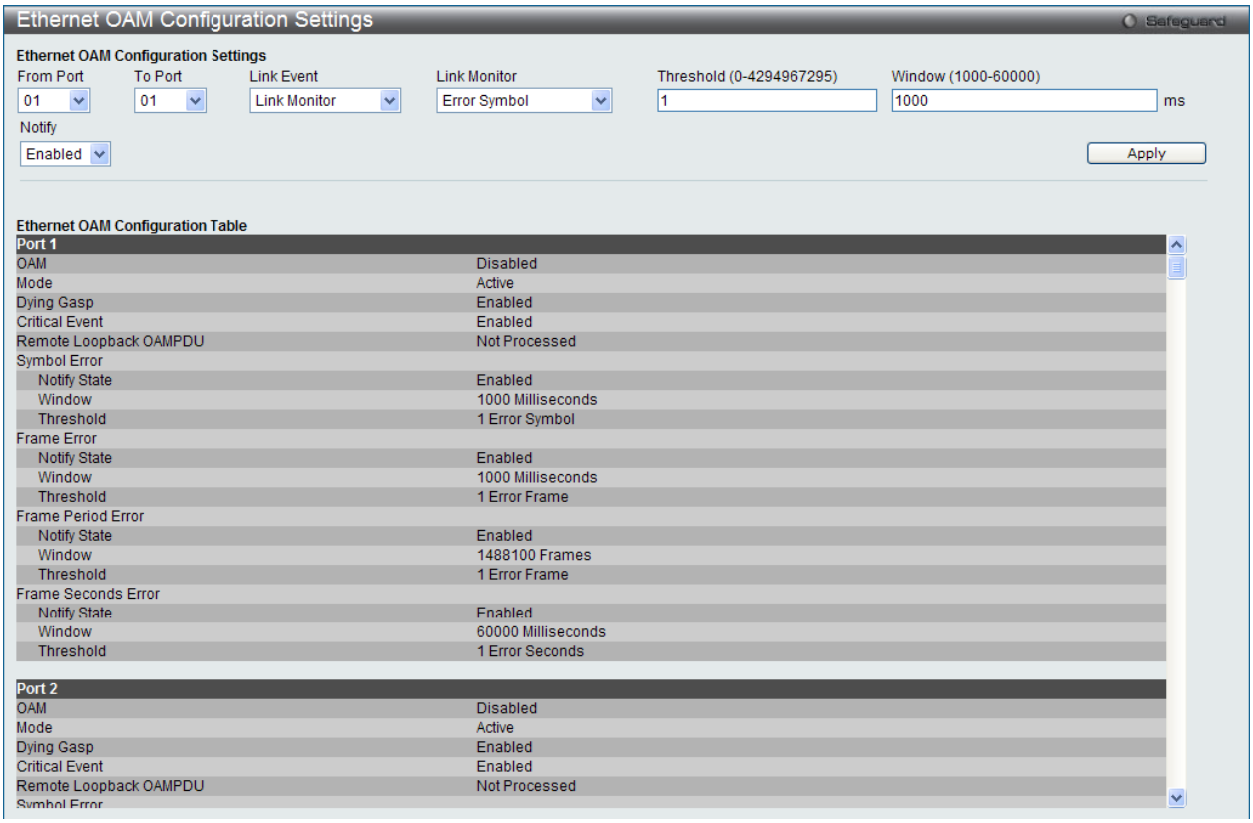


図 14-16　Ethernet OAM Configuration Settings 画面

以下の項目を設定できます。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Link Event	イーサネット OAM のクリティカルなリンクイベント機能（「Link Monitor」または「Critical Link Event」）を設定します。イベント機能を無効にすると、ポートは対応するクリティカルなリンクイベントを送信しません。
Link Monitor	ポートにイーサネット OAM リンクモニタリング (Error Symbol) を設定します。リンクモニタリング機能は、さまざまな条件のもとでリンク障害を検出して示すメカニズムを提供します。OAM はコード化されたシンボルのエラー数と共にフレームエラー数により統計情報をモニタリングします。シンボルエラー数が、期間内に定義したしきい値以上になる場合およびイベント通知状態 (Notify) が有効になる場合、リモート OAM ピアに通知するエラーシンボル期間のイベントを生成します。使用可能オプションは、Error Symbol、Error Frame、Error Frame Period、および Error Frame Second です。
Critical Link Event	イーサネット OAM のクリティカルなリンクイベント機能を設定します。イベント機能が無効になると、ポートは対応するクリティカルなリンクイベントを送信しません。 • Critical Event - 不特定のクリティカルなイベントを参照します。 • Dying Gasp - リモートデバイスの電源障害など回復不可能なイベントの発生の検出を指定します。
Threshold	イベント生成のためには、期間内に要求以上のにシンボルエラー数を指定します。しきい値の範囲は選択したリンクに基づいて変更できます。初期値は 1 です。
Window	エラーフレームまたはシンボルのサマリイベントの期間（ミリ秒）を入力します。
Notify	イベント通知を有効または無効にします。初期値は「Enabled」（有効）です。

「Apply」ボタンをクリックし、設定を有効にします。

Ethernet OAM Event Log（イーサネット OAM イベントログ）

ポートのイーサネット OAM イベントログ情報を表示します。

OAM > Ethernet OAM > Ethernet OAM Event Log の順にメニューをクリックし、以下の画面を表示します。

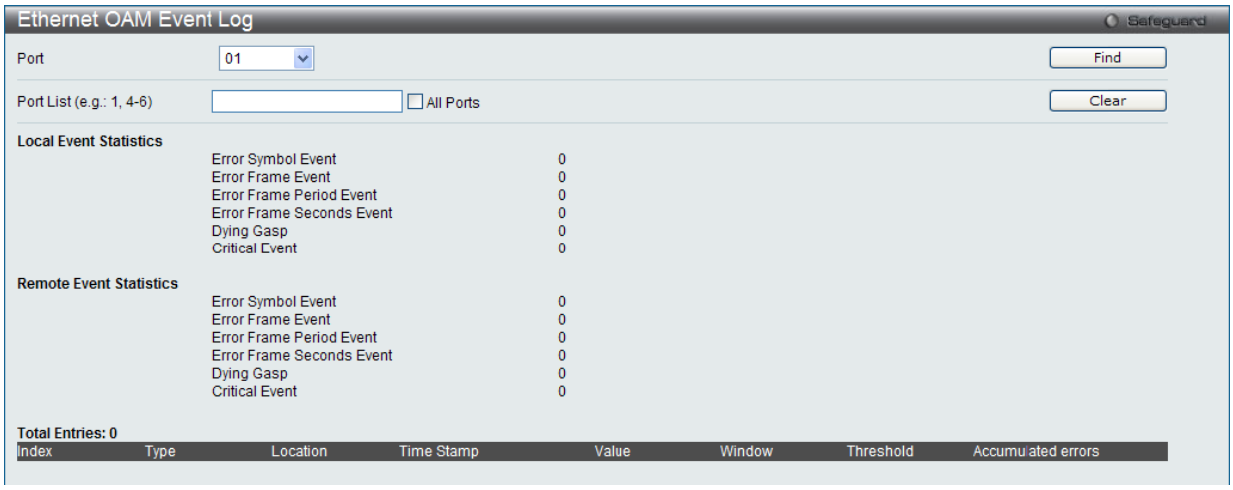


図 14-17　Ethernet OAM Event Log 画面

以下の項目を設定できます。

項目	説明
Port	参照するポート番号を選択します。
Port List	本設定に使用するポートリストを指定します。「All Ports」を選択すると、すべてのポートを選択します。

参照するポート番号またはポートリストを指定し、「Find」ボタンをクリックします。

エントリを削除するためには、適切な情報を入力して、「Clear」ボタンをクリックします。

Ethernet OAM Statistics（イーサネット OAM 統計情報）

スイッチの各ポートに関するイーサネット OAM 統計情報を表示します。

OAM > Ethernet OAM > Ethernet OAM Statistics の順にメニューをクリックし、以下の画面を表示します。

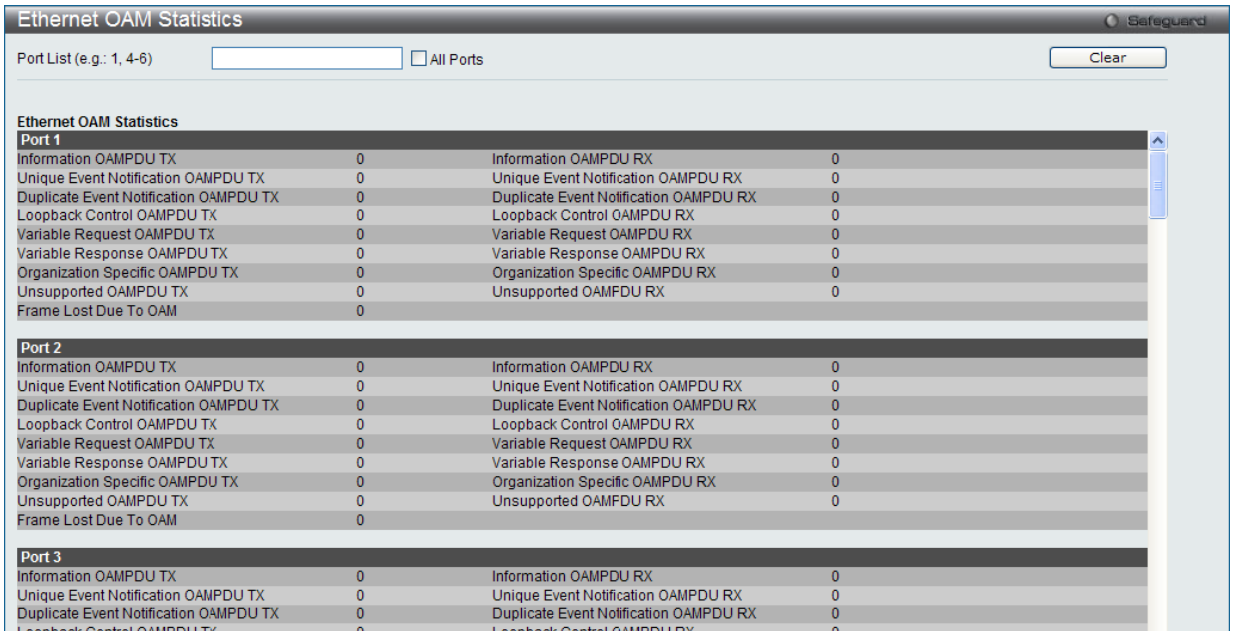


図 14-18　Ethernet OAM Statistics 画面

以下の項目を設定できます。

項目	説明
Port List	本設定に使用するポートリストを指定します。「All Ports」を選択すると、すべてのポートを選択します。

特定のポートまたはポートリストの情報をクリアするためには、ポートを入力し、「Clear」ボタンをクリックします。

DULD Settings（単方向リンク検出設定）

ポートにおいて単方向のリンク検出の設定および表示を行います。

OAM > DULD Settings の順にメニューをクリックし、以下の画面を表示します。

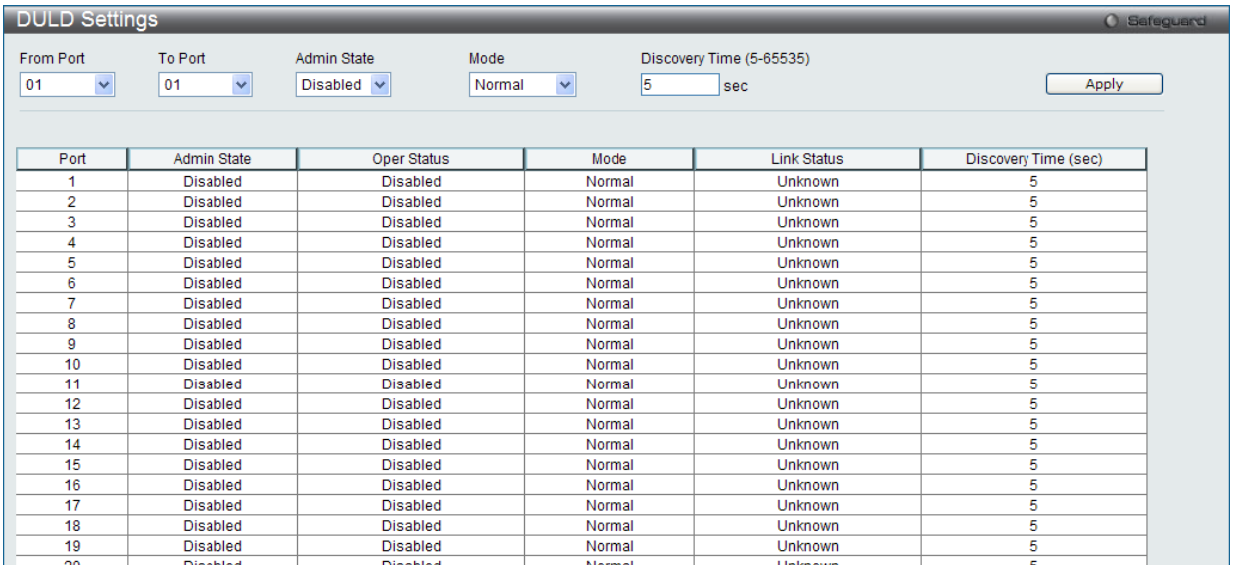


図 14-19 DULD Settings 画面

以下の項目を設定できます。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Admin State	プルダウンメニューか選択ポートの単方向リンク検出状態を「Enabled」(有効) または「Disabled」(無効) に設定します。
Mode	プルダウンメニューを使用してモード（「Shutdown」および「Normal」）を選択します。 • Shutdown - 単方向のリンクが検出されると、ポートを無効にしてイベントをログに出力します。 • Normal - 単方向のリンクが検出した場合にイベントを単にログに出力します。
Discovery Time (5-65535)	これらのポートの Neighbor 検出時間を入力します。検出がタイムアウトになると、単方向リンク検出が開始します。

「Apply」ボタンをクリックして、行った変更を適用します。

Cable Diagnostics（ケーブル診断機能）

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は主に管理者とカスタマサービス担当者が UTP ケーブルを検証するために設計されています。ケーブルの品質やエラーの種類を即座に診断します。

Monitoring > Cable Diagnostics の順にメニューをクリックし、以下の画面を表示します。

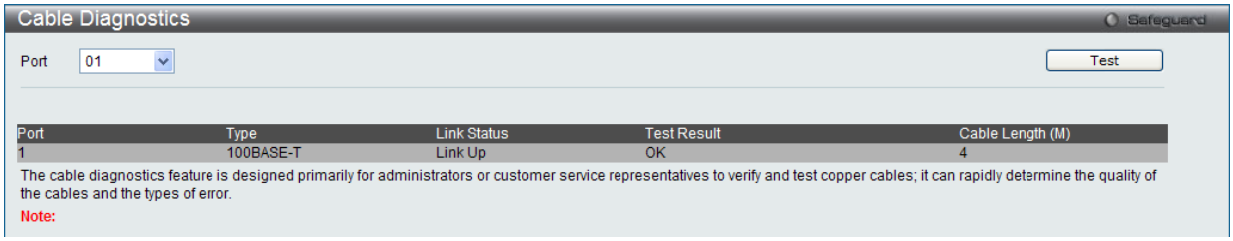


図 14-20　Cable Diagnostics 画面

特定のポートに対するケーブル診断を表示するためには、プルダウンメニューを使用してポートを選択し、「Test」ボタンをクリックします。情報が画面に表示されます。

テスト結果のメッセージは以下の通りです。

項目	説明
Open	エラーになっている 2 対のケーブルが特定された箇所で接続していません。
Short	エラーになっている 2 対のケーブルが特定された箇所でショートしています。
CrossTalk	エラーになっている 2 対のケーブルが特定された箇所でクロストークの問題があります。
Shutdown	リモートパートナーの電源がオフになっています。
Unknown	診断はケーブルステータスを取得しません。再試行してください。
No cable	ポートでは、ケーブルがリモートパートナーに接続していません。

注意　ケーブル診断機能の制限

ケーブル長検出はポートまたはリンクパートナーの電源がオフである場合にだけ GE ポート上にサポートされます。ポートは 1000M の速度でリンクおよび動作する必要があります。クロストークエラー検出は FE ポートではサポートされません。

第 15 章　Monitoring（スイッチのモニタリング）

Monitoring メニューを使用し、本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報を提供することができます。

以下は Monitoring サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
Utilization（CPU 使用率）	CPU 使用率、ポートの帯域使用率を表示します。次のメニューがあります。 CPU Utilization（CPU 使用率）、DRAM & Flash Utilization（DRAM とフラッシュ利用率）、Port Utilization（ポート使用率）	287
Statistics（統計情報）	パケット統計情報とエラー統計情報を表示します。次のメニューがあります。 Port Statistics（ポート統計情報情報）	289
Mirror（ポートミラーリング）	ポートミラーリングの設定を行います。次のメニューがあります。 Port Mirror Settings（ポートミラーリング設定）	298
Ping Test（Ping テスト）	IPv4 アドレスまたは IPv6 アドレスに Ping することができます。	299
Trace Route（トレースルート）	ネットワーク上のスイッチとホスト間の経路をトレースします。	300
Peripheral（周辺機器）	デバイス環境機能はスイッチの内部温度ステータスを表示します。次のメニューがあります。 Device Environment（デバイス環境の参照）	301

Utilization（使用率）

CPU Utilization（CPU 使用率）

現在の CPU 使用率をパーセント表示し、また指定した間隔で計算した平均値も表示します。

Monitoring > Utilization > CPU Utilization メニューをクリックし、以下の画面を表示します。

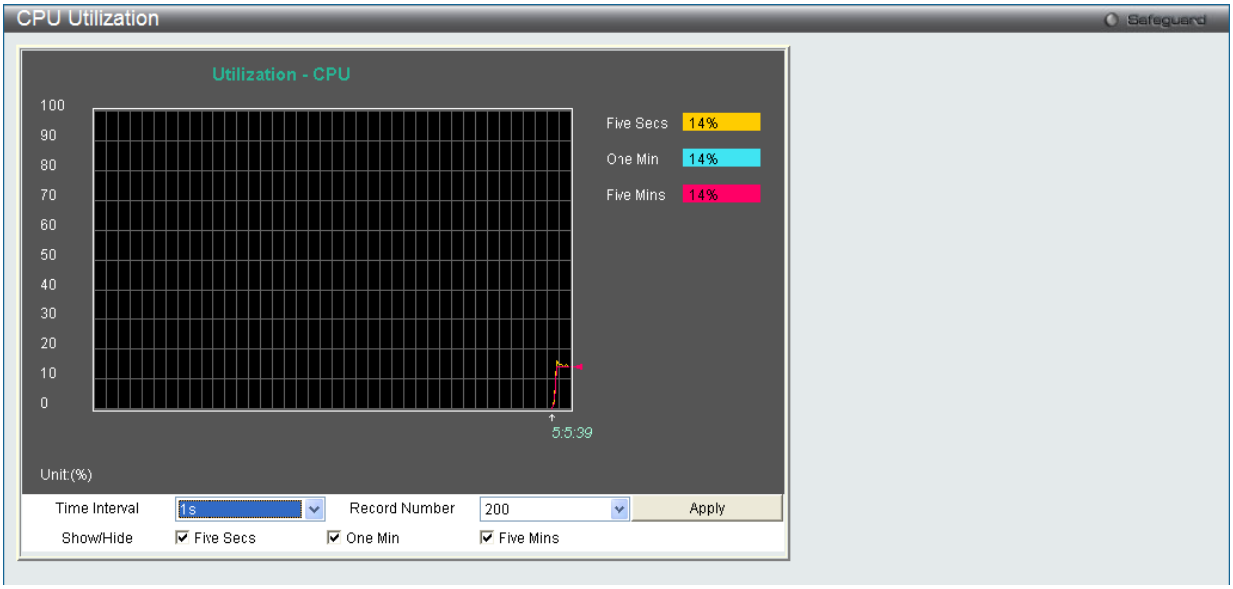


図 15-1　CPU Utilization 画面

以下の設定項目を使用して表示を変更します。

項目	説明
Timer Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Show/Hide	チェックボックスにて CPU 使用率を計算する時間経過を Five Secs、One Min および Five Mins から選択します。各時間経過は色分けされた線で表示されます。Five Secs は黄色、One Min は青、Five Mins はピンク色で表示されます。選択すると CPU 使用率を表示します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。

DRAM & Flash Utilization（DRAM とフラッシュ利用率）

DRAM とフラッシュ利用率に関する情報を参照します。

Monitoring > Utilization > DRAM & Flash Utilization メニューをクリックし、以下の画面を表示します。

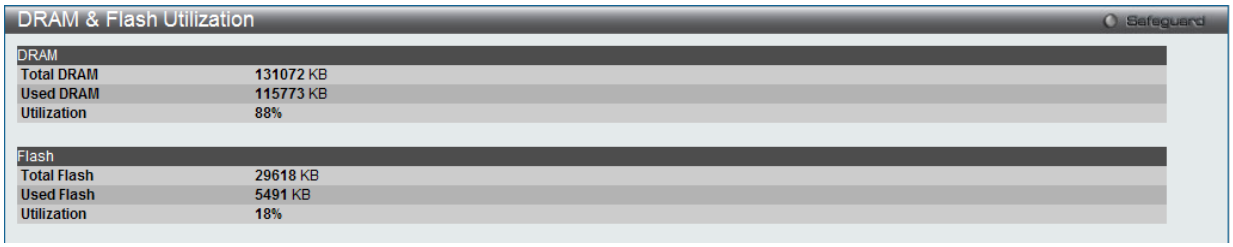


図 15-2　DRAM & Flash Utilization 画面

Port Utilization（ポート使用率）

本画面では、ポートの帯域使用率を表示します。

Monitoring > Utilization > Port Utilization の順にメニューをクリックし、以下の画面を表示します。

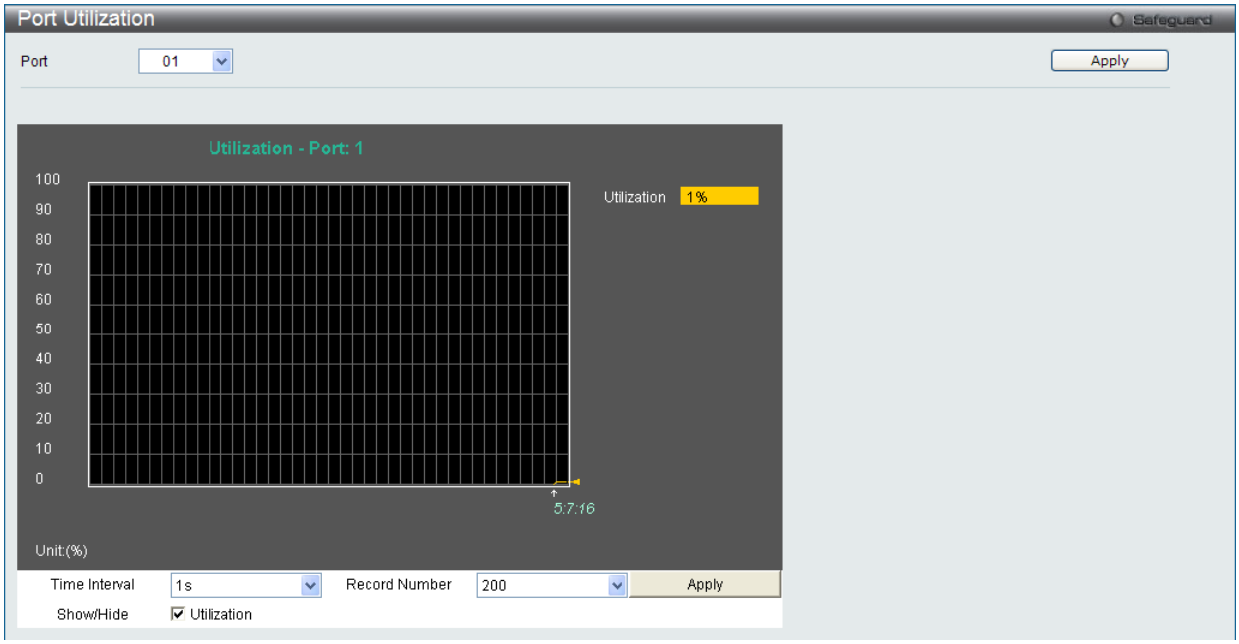


図 15-3　Port Utilization 画面

統計情報を参照するためには、プルダウンメニューでポート番号を選択します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

以下の設定項目が使用できます。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Show/ Hide	「Utilization」にチェックすると、使用率を表示します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Statistics（統計情報）

Port Statistics（ポート統計情報）

Packets（パケット統計情報）

Web マネージャは、パケットの統計情報を折れ線グラフまたは表の形式で表示します。6 個の画面が表示されます。

Received（RX）（受信パケット状態の参照）

スイッチが受信したパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packets > Received（RX）の順にメニューをクリックし、以下の画面を表示します。

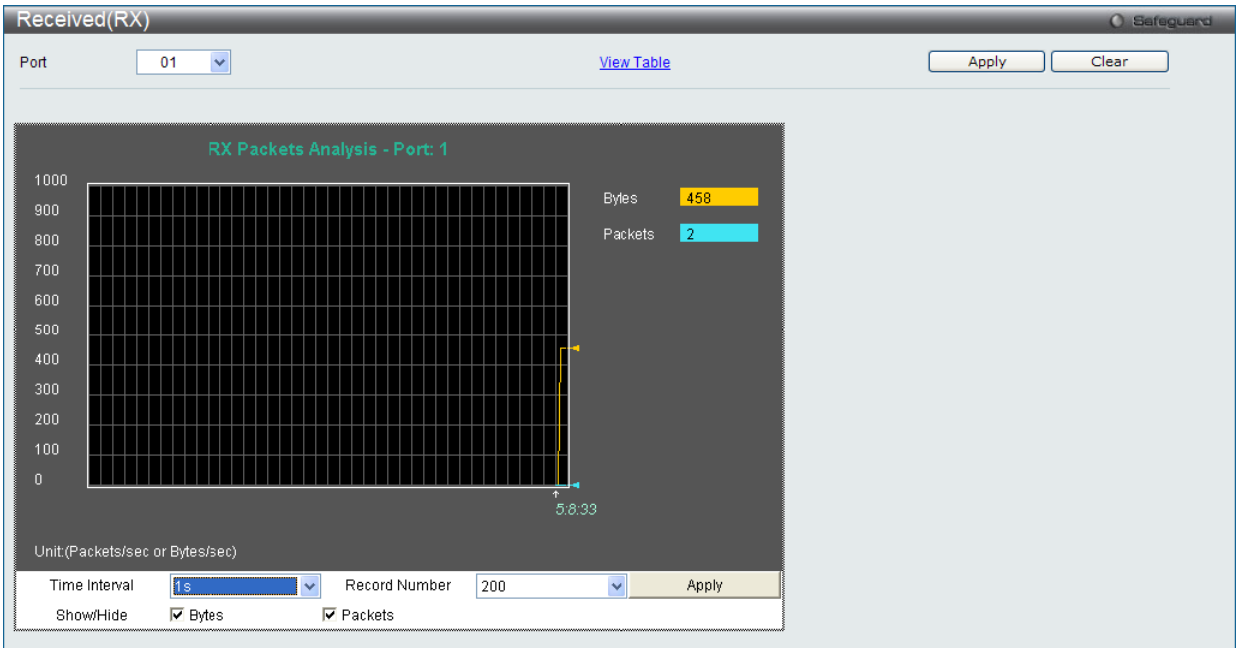


図 15-4　Received（RX）画面（バイトとパケットの折れ線グラフ）

「Received（RX）Table」を表示するには「View Table」リンクをクリックして、次の表を表示します。

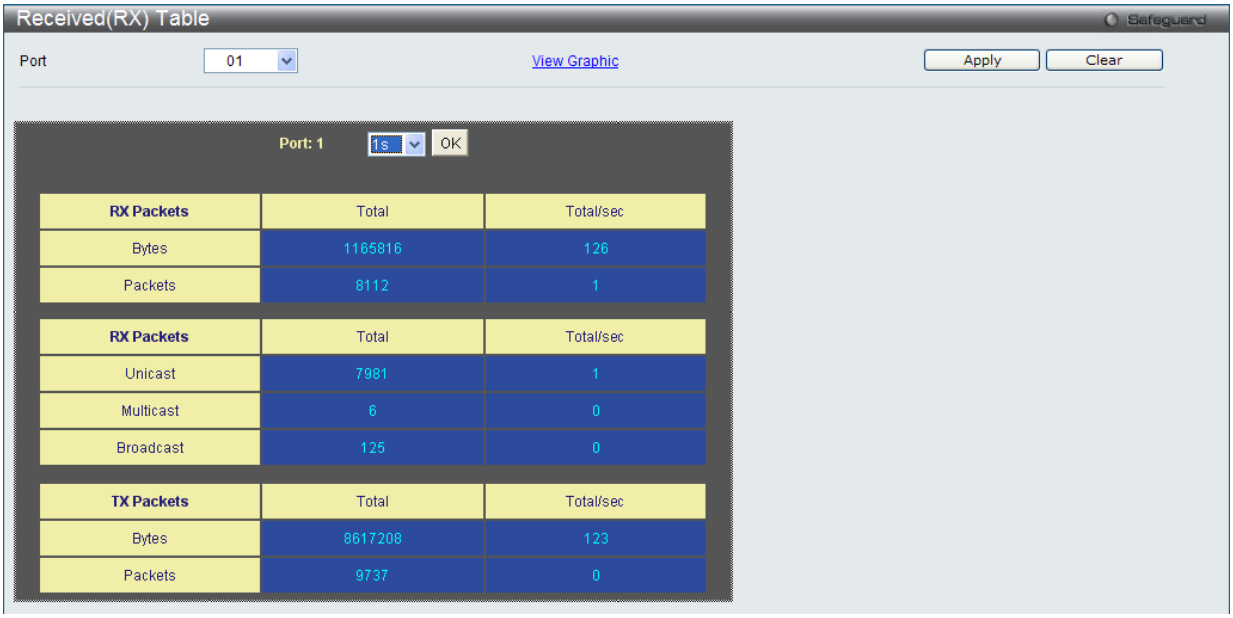


図 15-5　Received（RX）Table 画面（バイトとパケットの表）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Bytes	ポートに受信したパケット量（バイト）をカウントします。
Packets	ポートに受信したパケット数をカウントします。
Unicast	ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストキャストアドレスが受信した正常なパケットの合計数をカウントします。
Show/ Hide	Bytes と Packets を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

UMB_Cast (RX)（UMB Cast パケット統計情報の参照）

UMB（ユニキャスト、マルチキャスト、ブロードキャスト）に関する折れ線グラフを表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packets > UMB_Cast（RX）の順にメニューをクリックし、以下の画面を表示します。

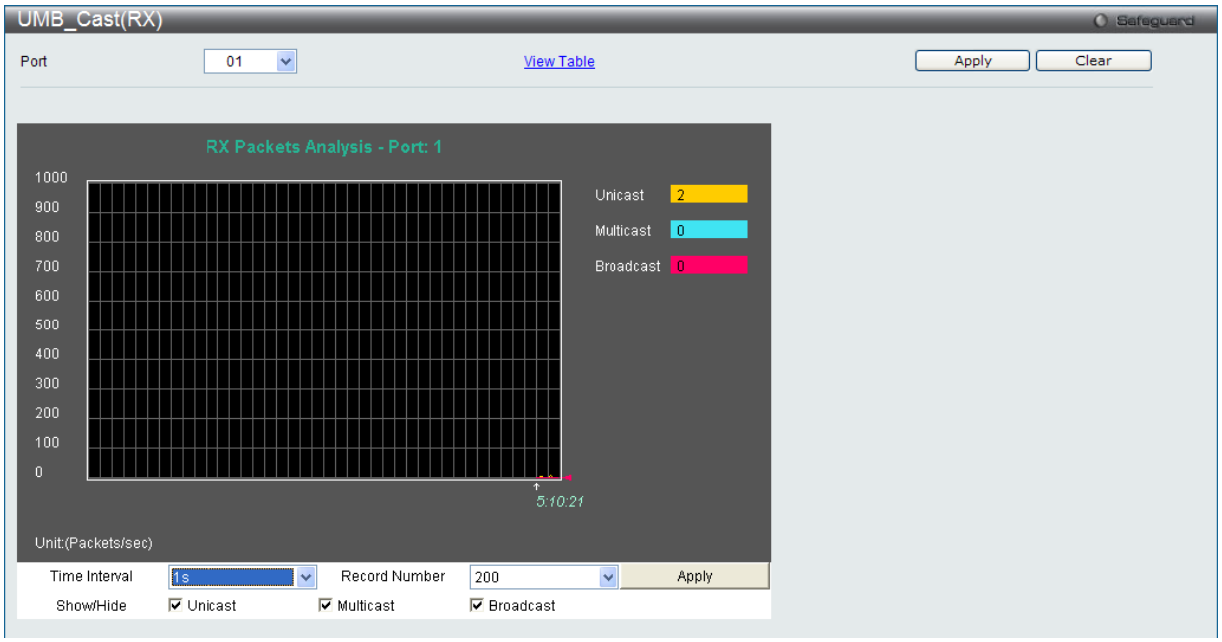


図 15-6　UMB_Cast（RX）画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の折れ線グラフ）

「UMB_Cast（RX）Table」画面の表示を行うためには、「View Table」リンクをクリックします。

図 15-7　UMB_Cast（RX）Table 画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の表形式表示）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Unicast	ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが受信した正常なパケットの合計数をカウントします。
Show/ Hide	Unicast、Multicast、Broadcast を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Transmitted（TX）（送信パケット統計情報）

スイッチから送信したパケットの情報をグラフ表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packets > Transmitted（TX）の順にメニューをクリックし、以下の画面を表示します。

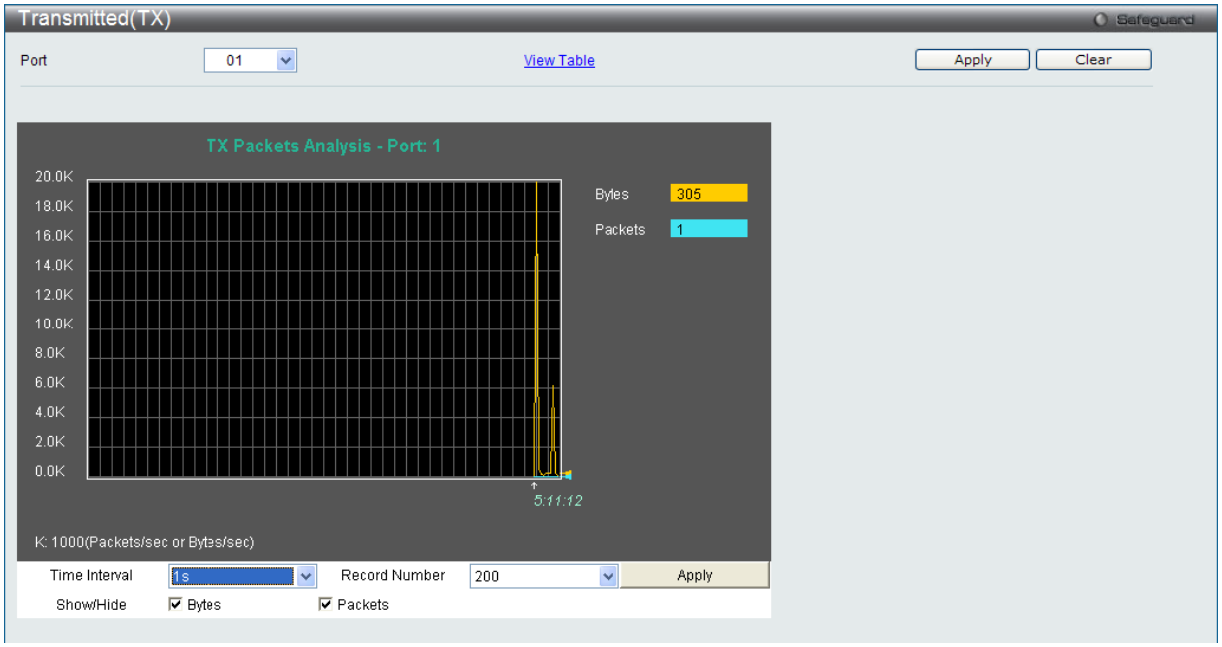


図 15-8　Transmitted（TX）画面（パケットサイズ、パケット数の折れ線グラフ表示）

送信パケットの情報を、表形式で表示するには、「View Table」リンクをクリックし、以下の画面を表示します。

図 15-9　Transmitted（TX）Table 画面（パケットサイズ、パケット数の表示）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Bytes	ポートから送信に成功したパケット量（バイト）。
Packets	ポートから送信に成功したパケット数。
Unicast	ユニキャストアドレスが送信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが送信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが送信した正常なパケットの合計数をカウントします。
Show/ Hide	Bytes と Packets を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Errors（パケットエラー）

Web マネージャは、スイッチの管理エージェントが集計したエラー統計情報を、折れ線グラフまたは表形式で表示します。以下の 4 つの画面で表示できます。

Received（RX）（受信エラーパケット統計情報の参照）

スイッチが受信したエラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Errors > Received（RX）の順にメニューをクリックし、以下の画面を表示します。

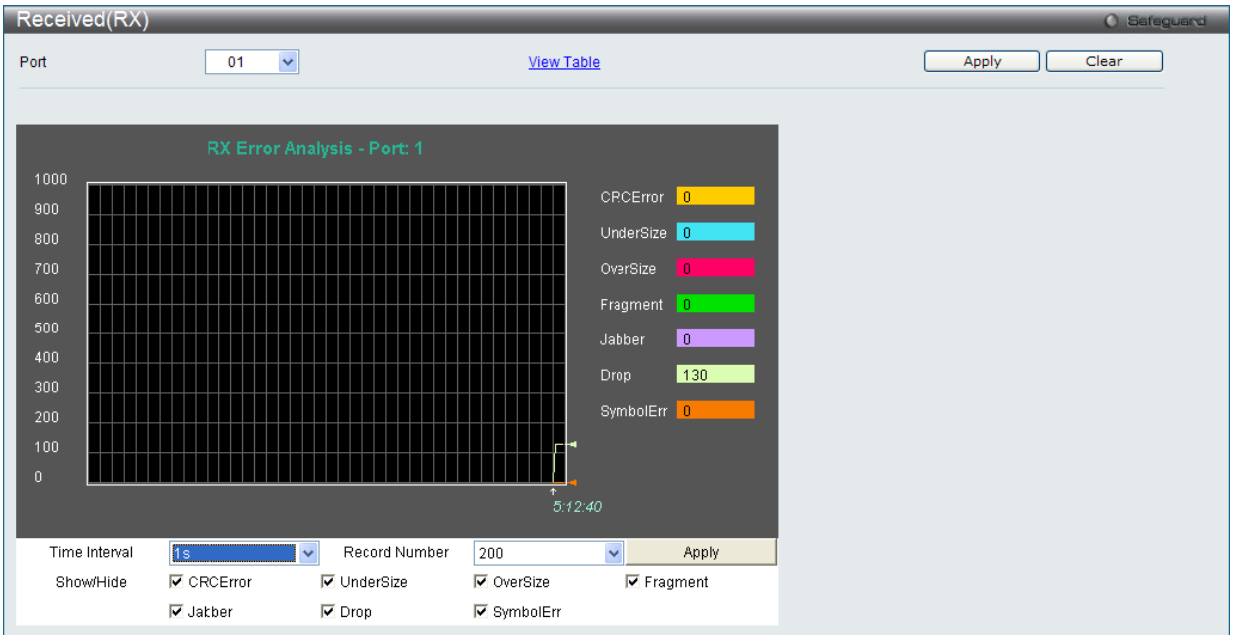


図 15-10　Received（RX）- Error 画面（折れ線グラフ形式）

表形式の「Received（RX）Table」画面を表示するためには、「View Table」リンクをクリックします。

図 15-11　Received（RX）Table - Error 画面（表形式）

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
CRCError	CRC エラーがある受信パケット数。パケットの許容値のバイト（オクテット）で終了しない正常なパケットの数。
UnderSize	パケットの最小許容値である 64 バイト以下で、CRC 値は正常なパケットの受信数。アンダーサイズパケットはコリジョンの発生を示しています。
OverSize	エラーパケットが 1518 オクテットより長く、さらに MAX_PKT_LEN より短い正常な受信パケットをカウントします。内部的には MAX_PKT_LEN は 1536 オクテットです。
Fragment	64 バイト以下でフレーミングエラーや無効な CRC を含むパケット受信数。これらのパケットはコリジョンの発生に起因します。
Jabber	エラーパケットが 1518 オクテットより長く、さらに CRC Error を持つ MAX_PKT_LEN より短い不正な受信パケットをカウントします。内部的には MAX_PKT_LEN は 1536 オクテットです。
Drop	前回の再起動からその時点までに廃棄したパケット数。
Symbol	物理的に配下にあるシンボル内に受信したエラーパケット数。
Show/ Hide	CRCError、UnderSize、OverSize、Fragment、Jabber、Drop および SymbolErr を表示するかどうかをチェックします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Transmitted（TX）（送信エラーパケット統計情報の参照）

スイッチでの送信エラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Error > Transmitted（TX）の順にメニューをクリックし、以下の画面を表示します。

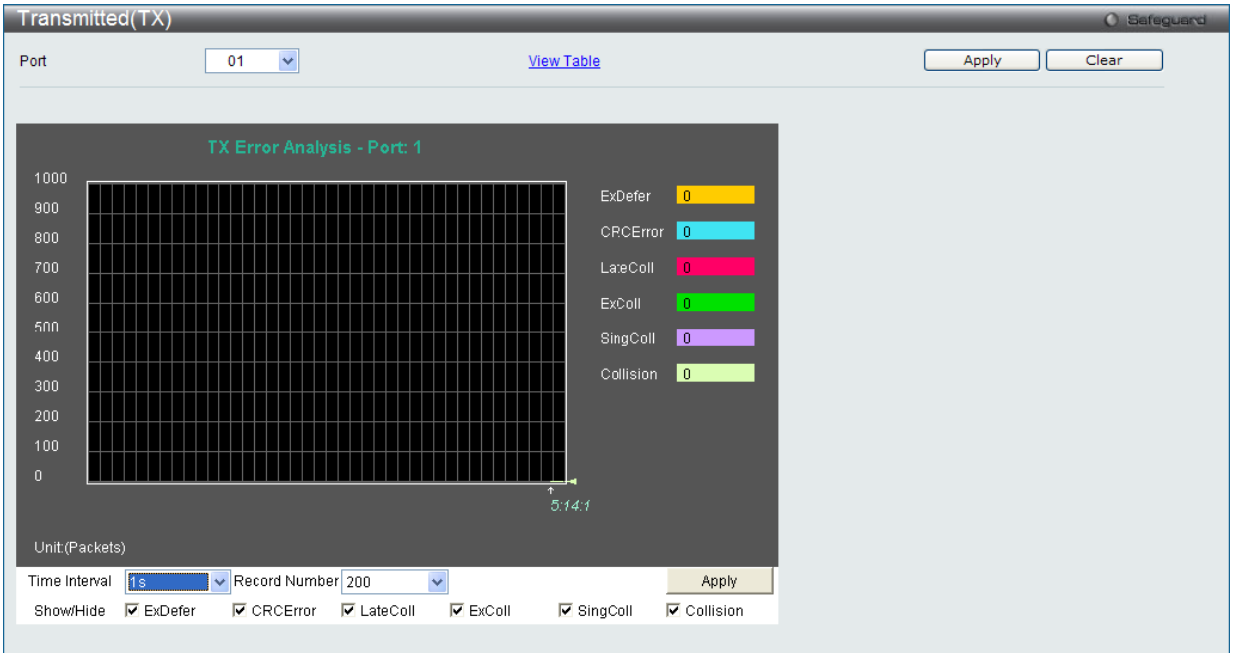


図 15-12　Transmitted（TX）- Error 画面（折れ線グラフ形式）

表形式の「Transmitted（TX）」画面を表示するためには、「View Table」リンクをクリックします。

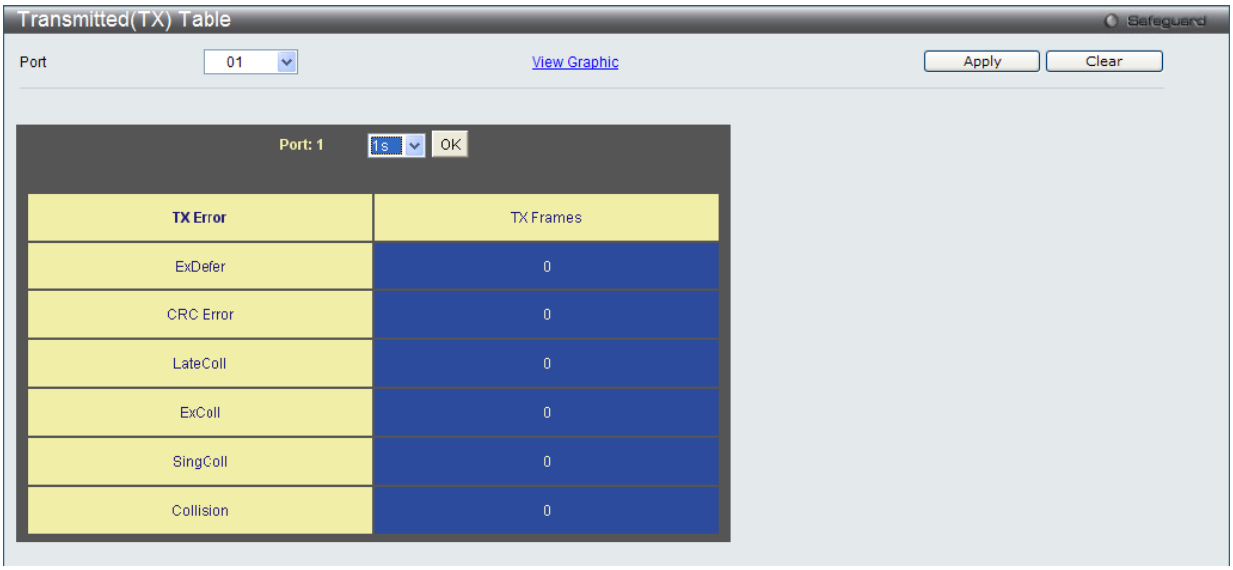


図 15-13　Transmitted（TX）Table - Error 画面（表形式）

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
ExDefer	特定のインタフェースに対する最初の送信が回線ビジーのために遅延したパケット数をカウントします。
CRC Error	CRC エラーがある受信パケット数。パケットの許容値のバイト（オクテット）で終了しない正常なパケットの数。
LateColl	パケットの送信に 512bit times より大きい往復遅延時間を検出されたコリジョンの回数をカウントします。
ExColl	過度のコリジョンのために送信エラーとなったパケット数。
SingColl	シングルコリジョンフレーム数。1 個以上のコリジョンにより送信されていなかったパケットで送信に成功した数。
Collision	ネットワークセグメントにおける推定総コリジョン数。
Show/ Hide	CRCError、UnderSize、OverSize、Fragment、Jabber、Drop および SymbolErr を表示するかどうかをチェックします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Packet Size（パケットサイズ）

Web マネージャはスイッチが受信したパケットを 6 個のグループに整理し、サイズによってクラス分けして折れ線グラフまたはテーブルにします。２つの画面が提供されます。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packet Size の順にメニューをクリックし、以下の画面を表示します。

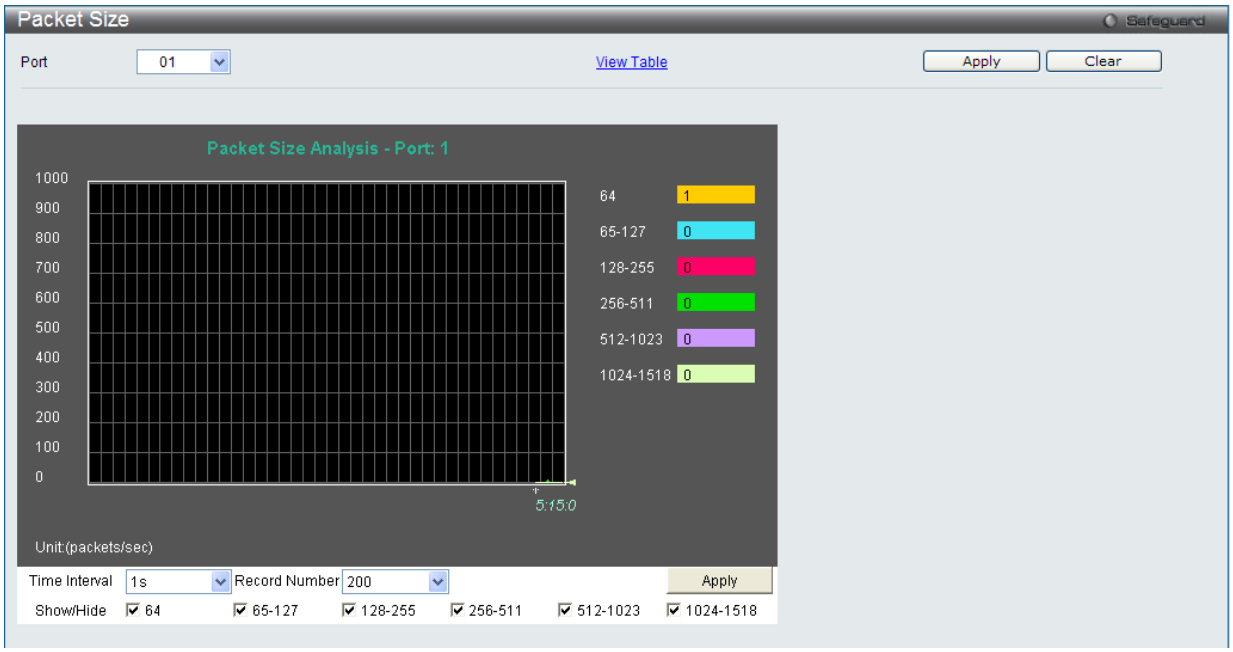


図 15-14　Packet Size 画面（折れ線グラフ）

「Packet Size Table」を表示するためには、「View Table」リンクをクリックします。

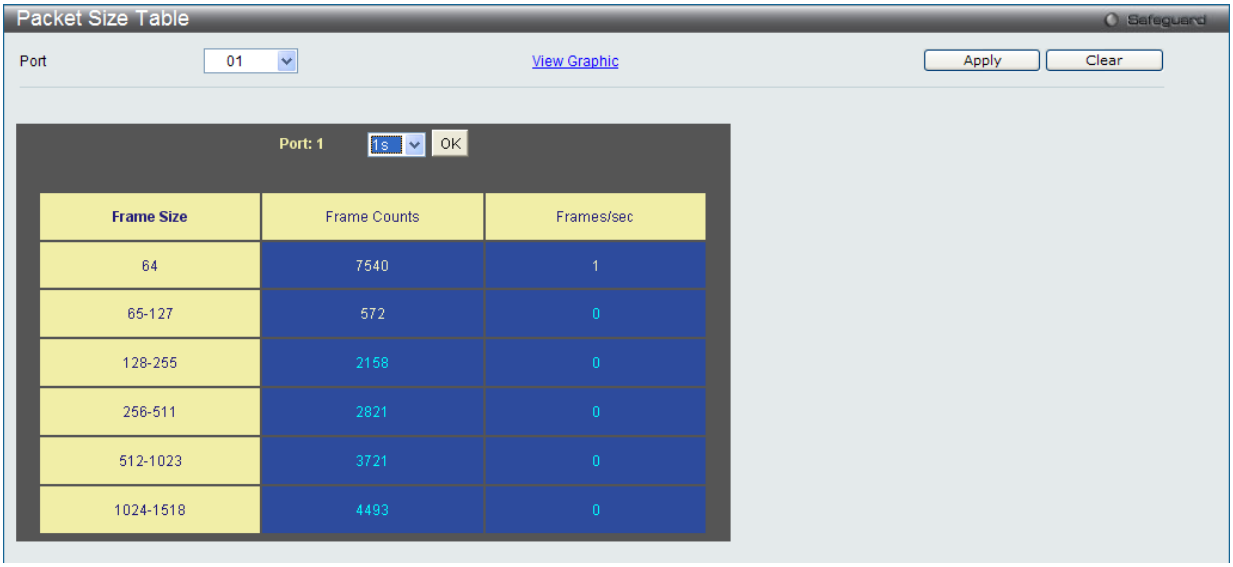


図 15-15　Packet Size Table 画面（表形式）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
64	サイズが 64 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
65-127	サイズが 65 から 127 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
128-255	サイズが 128 から 255 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
256-511	サイズが 256 から 511 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
512-1023	サイズが 512 から 1023 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
1024-1518	サイズが 1024 から 1518 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
1519-2047	サイズが 1519 から 2047 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
2048-4095	サイズが 2048 から 4095 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
4096-9216	サイズが 4096 から 9216 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
Show/ Hide	64、65-127、128-255、256-511、512-1023、1024-1518、1519-1552、1519-2047、2048-1095 および 4096-9216 の受信パケットを表示 / 非表示にします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Mirror（ポートミラーリング）

本スイッチはポート上で送受信したフレームをコピーし、別のポートに転送します。スニファーやRMON probeのようなモニタデバイスをミラーポートに接続し、最初のポートを通過するパケット情報を参照できます。ネットワーク監視とトラブルシューティングの目的で使用します。

Port Mirror Settings（ポートミラーリング設定）

ポートミラーリング機能を設定します。

Monitoring > Mirror > Port Mirror Settings の順にメニューをクリックし、以下の画面を表示します。

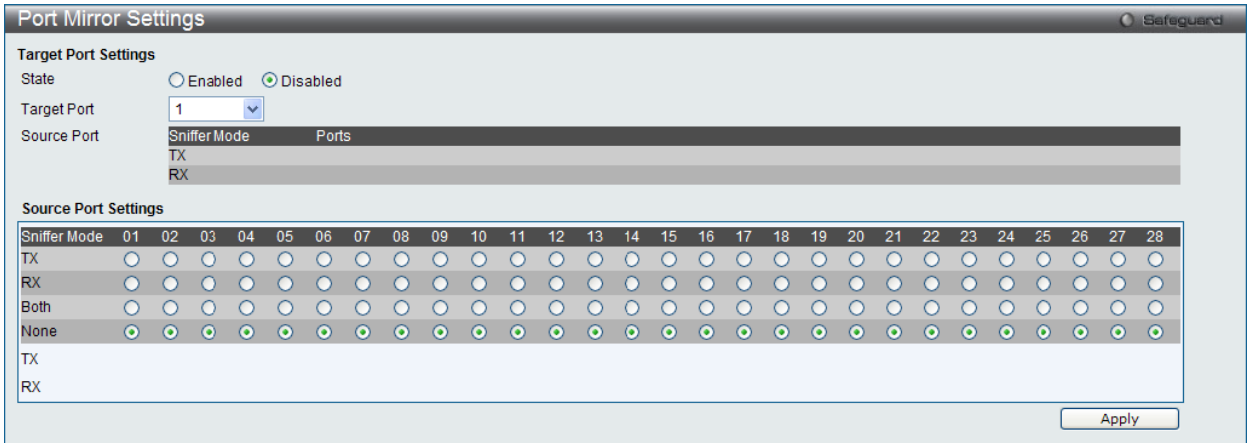


図 15-16　Port Mirror Settings 画面

ミラーポートの設定手順：

1. 「State」で「Enabled」（有効）を選択します。
2. ソースポートからフレームのコピーを受信する「Target Port」（ターゲット）を選択します。
3. フレームのコピーを行う対象の「Source port」（ソースポート）とコピーを行うフレームの方向（入力：TX、出力：RX、両方：Both、なし：None）を選択します。
4. 設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意　転送速度の速いポートを遅いポートにミラーリングはできません。例えば、100Mbps ポートからのトラフィックを 10Mbps ポートにミラーリングしようとすると、スループットの問題が起こります。ソースポートの速度はターゲットポートと同じかそれ以下としてください。また、ターゲットポートとソースポートを同じポートにはできませんのでご注意ください。

本画面には次の項目があります。

項目	説明
Target Port Setting	
State	ポートミラーリング機能を有効または無効にします。
Target Port	ターゲットポートを設定します。
Source Port	ソースデータの方向とソースポートを表示します。
Source Port Setting	
TX (Egress)	ポートが外向きトラフィックを含むかどうかを選択します。
RX (Ingress)	ポートが内向きトラフィックを含むかどうかを選択します。
Both	ポートが内向きおよび外向きの両方のトラフィックを含むかどうかを選択します。
None	ポートがどのトラフィックも含まないかどうかを選択します。

Ping Test（Ping テスト）

IPv4 アドレスまたは IPv6 アドレスに Ping することができます。

Ping とは、指定したアドレスに ICMP Echo パケットを送信する簡単なプログラムです。送信先のノードは、送信元のスイッチに応答を返すか、送信されたパケットをエコーバックします。本機能はスイッチとネットワーク上の他のノードとの接続性を確認するために使用します。

Monitoring > Ping Test の順にメニューをクリックし、以下の画面を表示します。

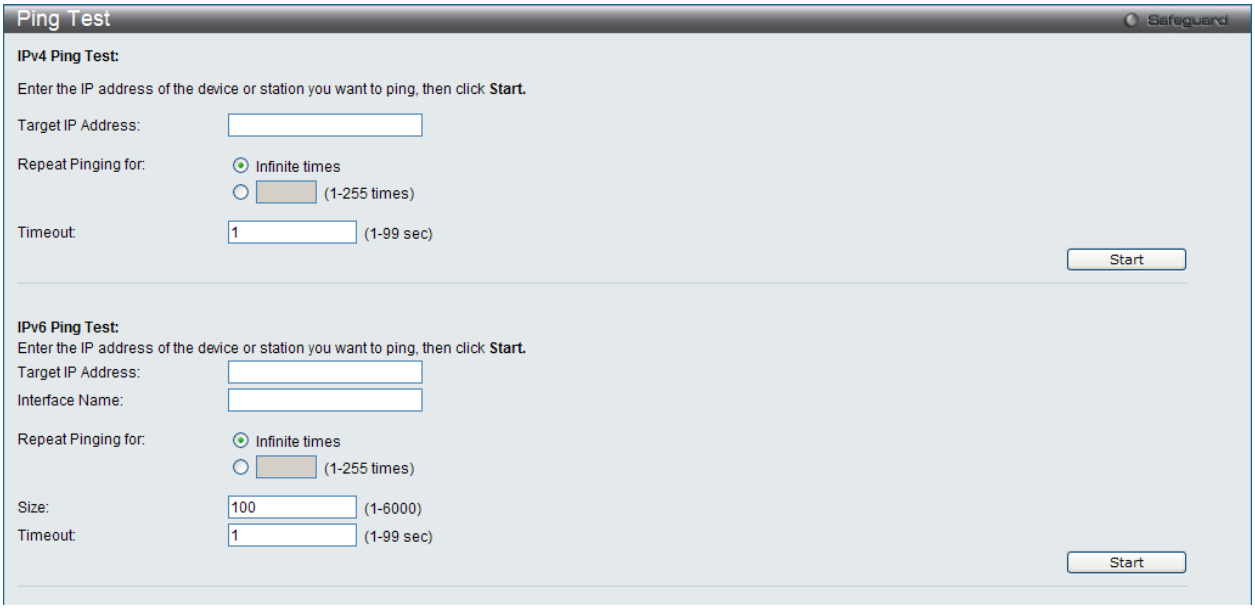


図 15-17　Ping Test 画面

「Repeat Pinging for」で「Infinite times」を選択すると、「Target IP Address」に指定した IP アドレス宛てに、ICMP Echo パケットをプログラムが停止するまで送信し続けます。または、「Repeat Pinging for」で 1-255 までの数字を指定して、送信回数を指定することもできます。

以下の項目を使用して設定、表示を行います。

項目	説明
Target IP Address	Ping する IP アドレスを入力します。
Repeat Pinging for	送信先 IPv4 アドレスまたは IPv6 アドレスに Ping する回数（1-255）を指定します。 「Infinite times」を選択すると、ICMP Echo パケットをプログラムが停止するまで送信し続けます。
Size	IPv6 の場合、1-6000 の値を入力します。初期値は 100 です。
Timeout	送信先への Ping メッセージの応答待ち時間 1-99（秒）で入力します。この時間内に応答パケットの検出に失敗すると、Ping パケットを破棄します。

「Start」ボタンをクリックし、Ping プログラムを開始します。

以下の結果画面が表示されます。

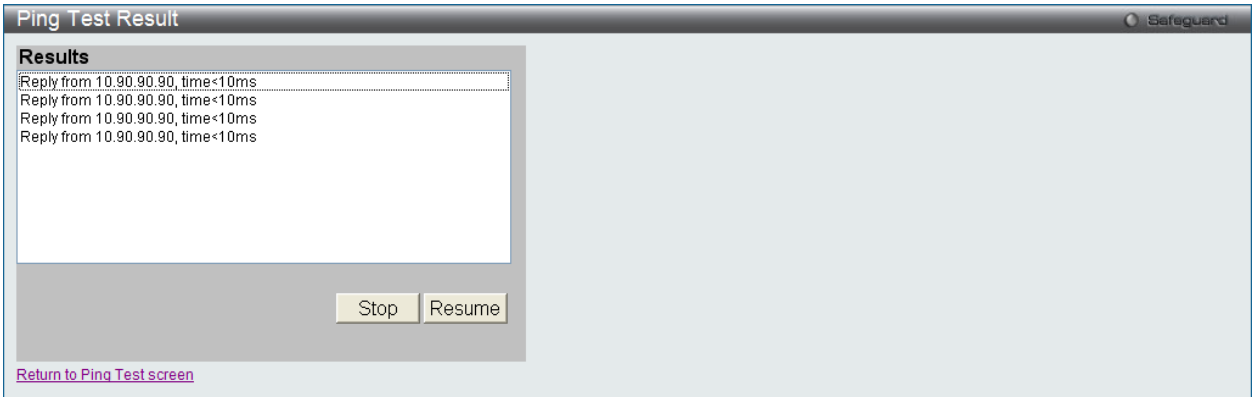


図 15-18　Ping Test (Result) 画面

「Stop」ボタンをクリックして、Ping テストを停止します。
「Resume」ボタンをクリックして、Ping テストを再開します。

Trace Route（トレースルート）

ネットワーク上のスイッチとホスト間の経路をトレースします。

Monitoring > Trace Route の順にメニューをクリックし、以下の画面を表示します。

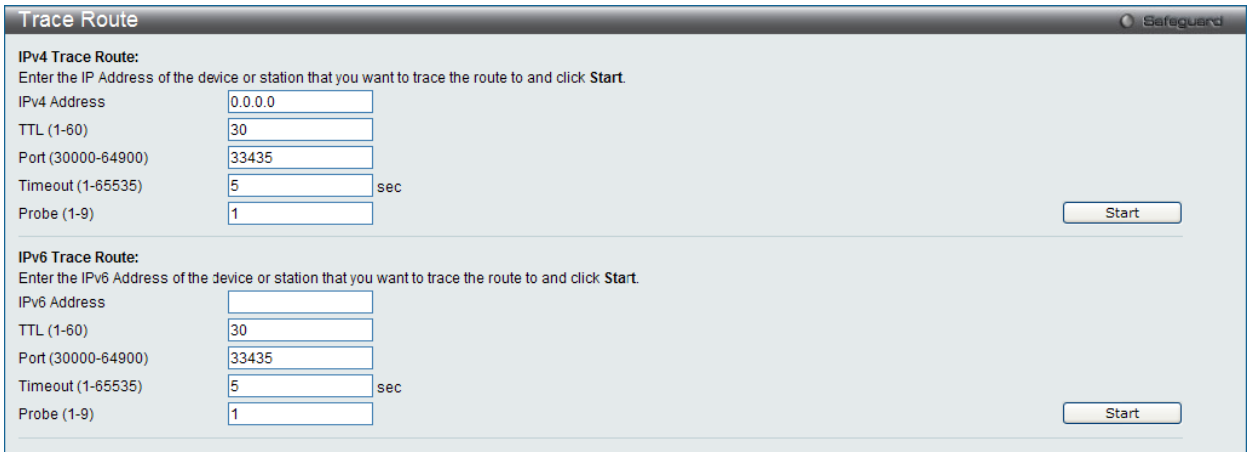


図 15-19 Trace Route 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IPv4 Address	宛先ステーションの IPv4 アドレス。
IPv6 Address	宛先ステーションの IPv6 アドレス。
TTL	トレースルートリクエストの有効時間。これは、トレースルートパケットが経由するルータの最大数です。トレースルートは、2 つのデバイス間のネットワーク経路を検索する間に経由します。TTL の範囲は、1-60 ホップです。
Port	ポート番号。値の範囲は、30000-64900 です。
Timeout	リモートデバイスからの応答を待つ時間を定義します。1-65535（秒）を指定します。初期値は 5（秒）です。
Probe	プローブ数。範囲は 1-9 です。指定しない場合、初期値は 1 です。

「Start」ボタンをクリックして、トレースルートを開始します。

以下の結果画面が表示されます。

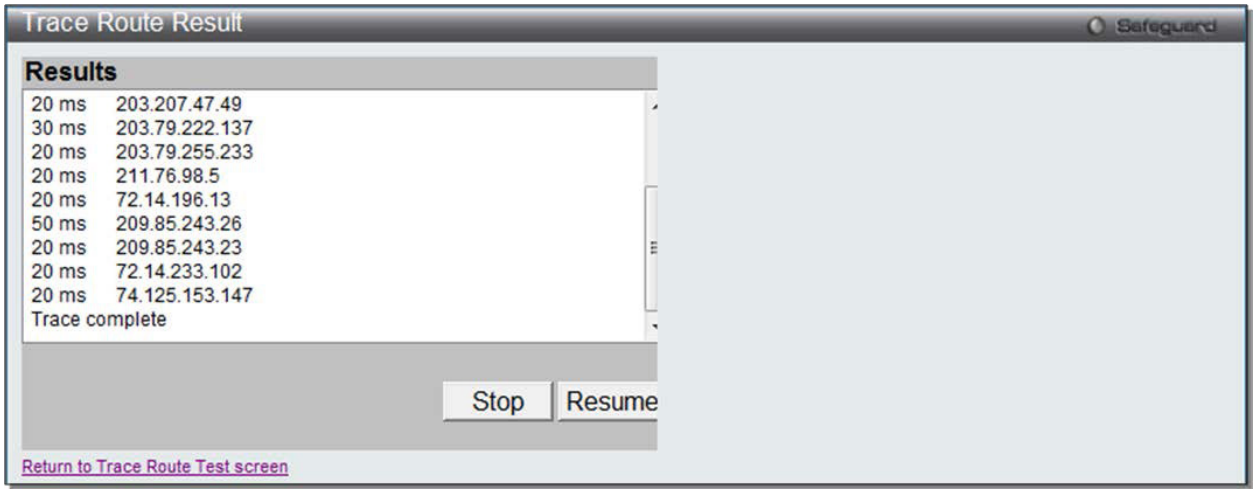


図 15-20 Trace Route (Result) 画面

「Stop」ボタンをクリックして、トレースルートを停止します。
「Resume」ボタンをクリックして、トレースルートを再開します。

Peripheral（周辺機器）

Device Environment（デバイス環境の参照）

デバイス環境機能はスイッチの内部温度ステータスを表示します。

Monitoring > Peripheral > Device Environment の順にメニューをクリックし、以下の画面を表示します。

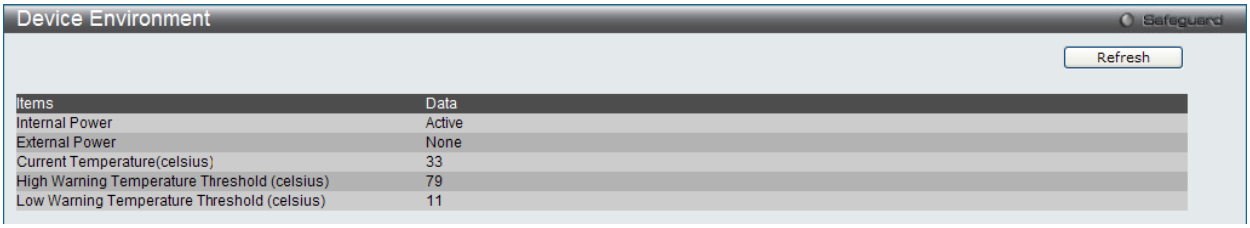


図 15-21　Device Environment 画面

「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

第 16 章　Maintenance（スイッチのメンテナンス）

メンテナンス用のメニューを使用し、本スイッチのリセットおよび再起動等を行うことができます。

以下はサブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
Save（コンフィグレーションとログの保存）		
Save Configuration / Log（コンフィグレーションとログの保存）	コンフィグレーションとログをスイッチに保存します。	302
Tools（ツールメニュー）		
Download Firmware（ファームウェアのダウンロード）	ファームウェアファイルをダウンロードします。	303
Upload Firmware（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をアップロードします。	304
Download Configuration（コンフィグレーションのダウンロード）	コンフィグレーションファイルをダウンロードします。	305
Upload Configuration（コンフィグレーションのアップロード）	コンフィグレーションファイルをアップロードします。	307
Upload Log File（ログファイルのアップロード）	ログファイルをアップロードします。	308
Reset（リセット）	工場出荷時設定に戻し、メモリに保存します。	310
Reboot System（システムの再起動）	スイッチの再起動を行います。	310

Save Configuration / Log（コンフィグレーションとログの保存）

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Type」プルダウンメニューの「Configuration」を選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。

Web マネージャ先頭の **Save > Save Configuration / Log** をクリックし、以下の画面を表示します。

コンフィグレーションの保存

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Type」プルダウンメニューの「Configuration」を選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。

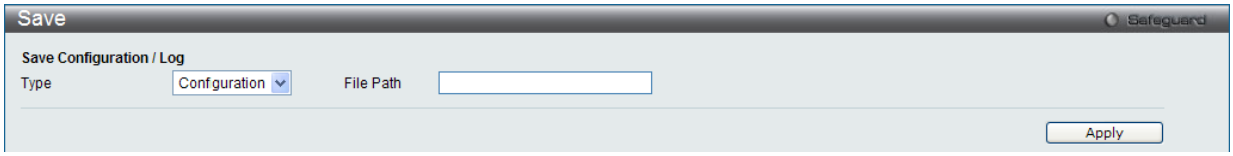


図 16-1　Save 画面 - Configuration

ログの保存

「Save Log」では現在のログをスイッチに保存します。「Type」プルダウンメニューの「Log」を選択し、「Apply」ボタンをクリックします。

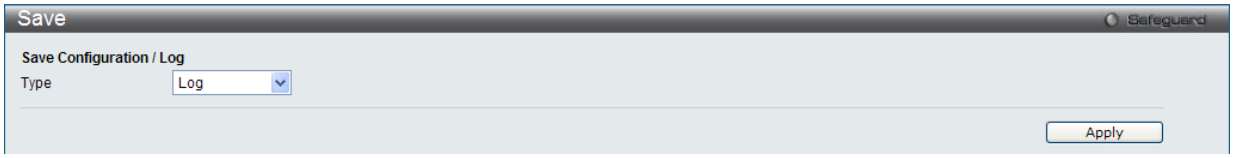


図 16-2　Save 画面 - Log

すべての保存

コンフィグレーションおよびログファイルに行った変更を永続的に保存します。本オプションを使用すると、スイッチの再起動後も変更は維持されます。「Type」欄から「All」を選択して、「Apply」ボタンをクリックします。

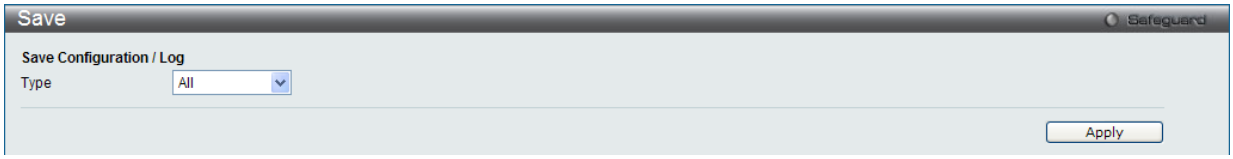


図 16-3　Save 画面 - All

Tools（ツールメニュー）

Web マネージャ先頭の **Tools** をクリックして、オプションを選択します。

Download Firmware（ファームウェアのダウンロード）

スイッチにファームウェアをダウンロードします。

Download Firmware From TFTP（TFTP からファームウェアをダウンロード）

TFTP サーバからスイッチにファームウェアをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Firmware** を選択し、「Download Firmware From TFTP」を選択して以下の画面を表示します。

図 16-4　Download Firmware From TFTP 画面

以下の項目があります。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - チェックします。
Source File	送信元ファイルの位置と名前を入力します。
Destination File	送信先ファイルの位置と名前を入力します。

「Download」ボタンをクリックすると、ダウンロードが開始されます。

Download Firmware From FTP（FTP からファームウェアをダウンロード）

FTP サーバからスイッチにファームウェアをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Firmware** を選択し、「Download Firmware From FTP」を選択して以下の画面を表示します。

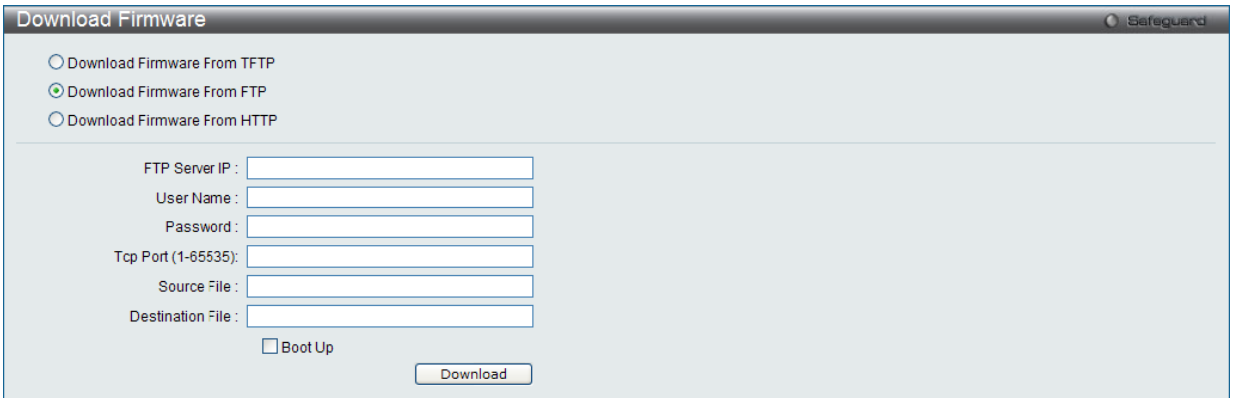


図 16-5　Download Firmware From FTP 画面

以下の項目があります。

項目	説明
FTP Server IP	使用する FTP サーバの IP アドレスを指定します。
User Name	使用する適切なユーザ名を指定します。
Password	使用する適切なパスワードを指定します。
TCP Port	使用する TCP ポート番号を入力します。
Source File	送信元ファイルの位置と名前を入力します。
Destination File	送信先ファイルの位置と名前を入力します。
Boot Up	本オプションを選択すると起動ファイルとしてこのファームウェアを使用します。

「Download」ボタンをクリックすると、ダウンロードが開始されます。

Download Firmware From HTTP（HTTP からファームウェアをダウンロード）

コンピュータからスイッチにファームウェアをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Firmware** を選択し、「Download Firmware From HTTP」を選択して以下の画面を表示します。

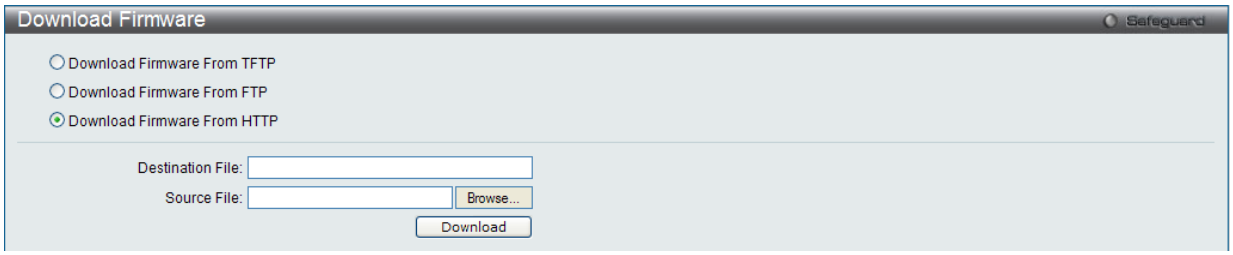


図 16-6　Download Firmware From HTTP 画面

以下の項目があります。

項目	説明
Destination File	送信先ファイルの位置を入力します。
Source File	送信元ファイルの位置を入力します。

「Browse」ボタンをクリックすると、ダウンロードのためのファームウェアファイルを参照することができます。
「Download」ボタンをクリックすると、ダウンロードが開始されます。

Upload Firmware（ファームウェアのアップロード）

スイッチにファームウェアをアップロードします。

Upload Firmware To TFTP（ファームウェアを TFTP にアップロードする）

スイッチから TFTP サーバにファームウェアをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Firmware** を選択し、「Upload Firmware To TFTP」を選択して以下の画面を表示します。

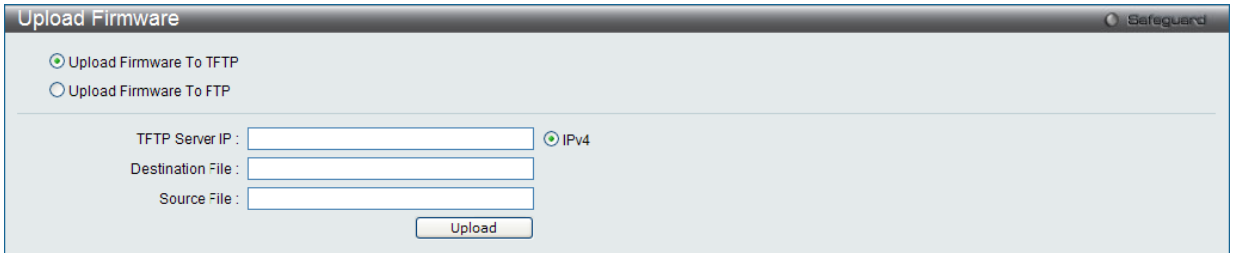


図 16-7　Upload Firmware To TFTP 画面

以下の項目があります。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - チェックします。
Destination File	送信先ファイルの位置と名前を入力します。
Source File	送信元ファイルの位置と名前を入力します。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Firmware To FTP（ファームウェアを FTP にアップロードする）

スイッチから FTP サーバにファームウェアをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Firmware** を選択し、「Upload Firmware To FTP」を選択して以下の画面を表示します。

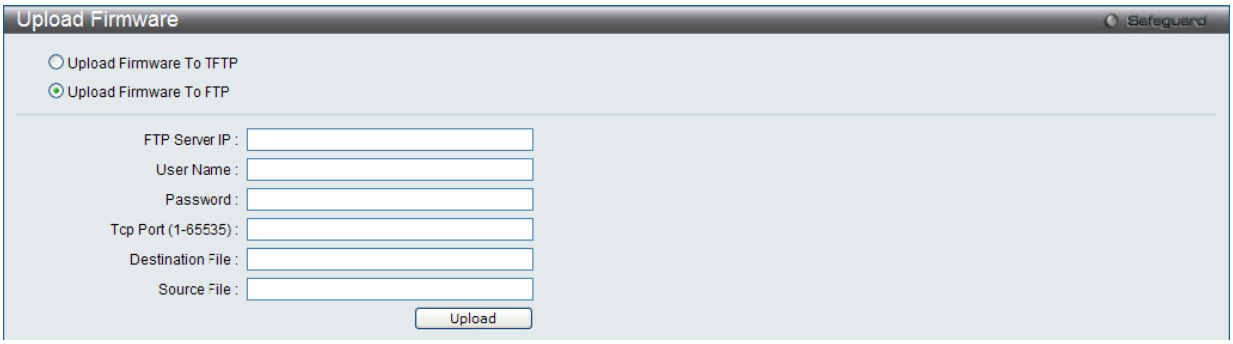


図 16-8　Upload Firmware To FTP 画面

以下の項目があります。

項目	説明
FTP Server IP	使用する FTP サーバの IP アドレスを指定します。
User Name	使用する適切なユーザ名を指定します。
Password	使用する適切なパスワードを指定します。
TCP Port	使用する TCP ポート番号を入力します。
Destination File	送信先ファイルの位置と名前を入力します。
Source File	送信元ファイルの位置と名前を入力します。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Download Configuration（コンフィグレーションのダウンロード）

スイッチにコンフィグレーションをダウンロードするために以下の画面を使用します。

Download Configuration From TFTP（TFTP サーバからコンフィグレーションファイルをダウンロードする）

TFTP サーバからスイッチにコンフィグレーションをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Configuration** を選択し、「Download Configuration From TFTP」を選択して以下の画面を表示します。

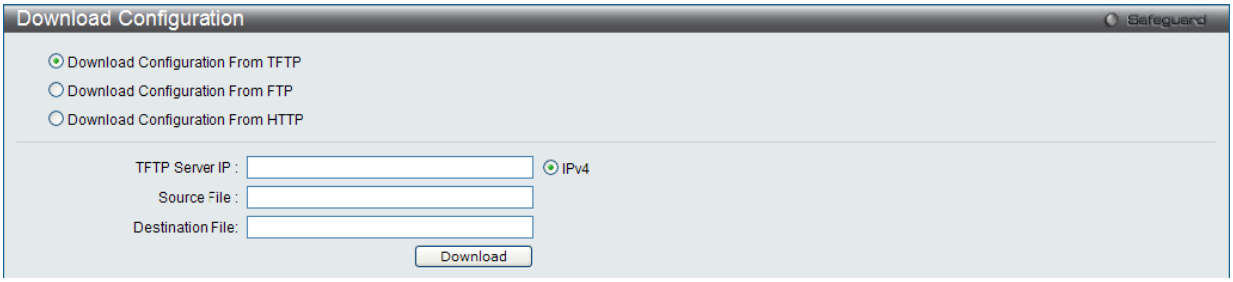


図 16-9　Download Configuration From TFTP 画面

以下の項目があります。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - チェックします。
Destination File	送信先ファイルの位置と名前を入力します。
Source File	送信元ファイルの位置と名前を入力します。

「Download」ボタンをクリックすると、ダウンロードが開始されます。

Download Configuration From FTP（FTP サーバからコンフィグレーションファイルをダウンロードする）

FTP サーバからスイッチにコンフィグレーションをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Configuration** を選択し、「Download Configuration From FTP」を選択して以下の画面を表示します。

図 16-10　Download Configuration From FTP 画面

以下の項目があります。

項目	説明
FTP Server IP	使用する FTP サーバの IP アドレスを指定します。
User Name	使用する適切なユーザ名を指定します。
Password	使用する適切なパスワードを指定します。
TCP Port	使用する TCP ポート番号を入力します。
Source File	送信元ファイルの位置と名前を入力します。
Destination File	送信先ファイルの位置と名前を入力します。

「Download」ボタンをクリックすると、ダウンロードが開始されます。

Download Configuration From HTTP（HTTP からコンフィグレーションファイルをダウンロードする）

コンピュータからスイッチにコンフィグレーションをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Configuration** を選択し、「Download Configuration From HTTP」を選択して以下の画面を表示します。

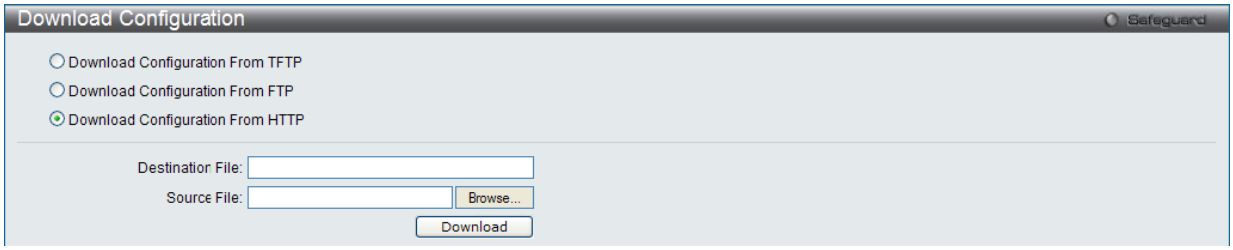


図 16-11　Download Configuration From HTTP 画面

以下の項目があります。

項目	説明
Destination File	送信先ファイルの位置と名前を入力します。
Source File	送信元ファイルの位置と名前を入力します。

「Browse」ボタンをクリックすると、ダウンロードのためのコンフィグレーションファイルを参照することができます。
「Download」ボタンをクリックすると、ダウンロードが開始されます。

Upload Configuration（コンフィグレーションファイルのアップロード）

スイッチからコンフィグレーションをアップロードするために以下の画面を使用します。

Upload Configuration To TFTP（TFTP サーバにコンフィグレーションをアップロードする）

スイッチから TFTP サーバにコンフィグレーションファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Configuration** を選択し、「Upload Configuration To TFTP」を選択して以下の画面を表示します。

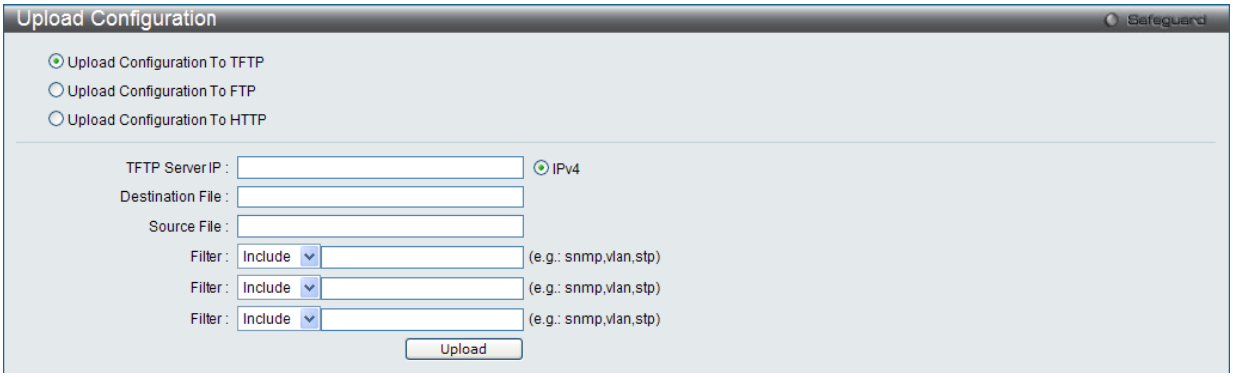


図 16-12　Upload Configuration To TFTP 画面

以下の項目があります。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - チェックします。
Destination File	送信先ファイルの位置と名前を入力します。
Source File	送信元ファイルの位置と名前を入力します。
Filter	ここでは、SNMP、VLAN または STP のようなフィルタを含む、開始する、または除外するように指定できます。適切な「Filter」アクションを選択し、提供されたスペースにファイル名を入力します。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Configuration To FTP（コンフィグレーションを FTP サーバにアップロードする）

このページでは、スイッチから FTP サーバにコンフィグレーションをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Configuration** を選択し、「Upload Configuration To FTP」を選択して以下の画面を表示します。

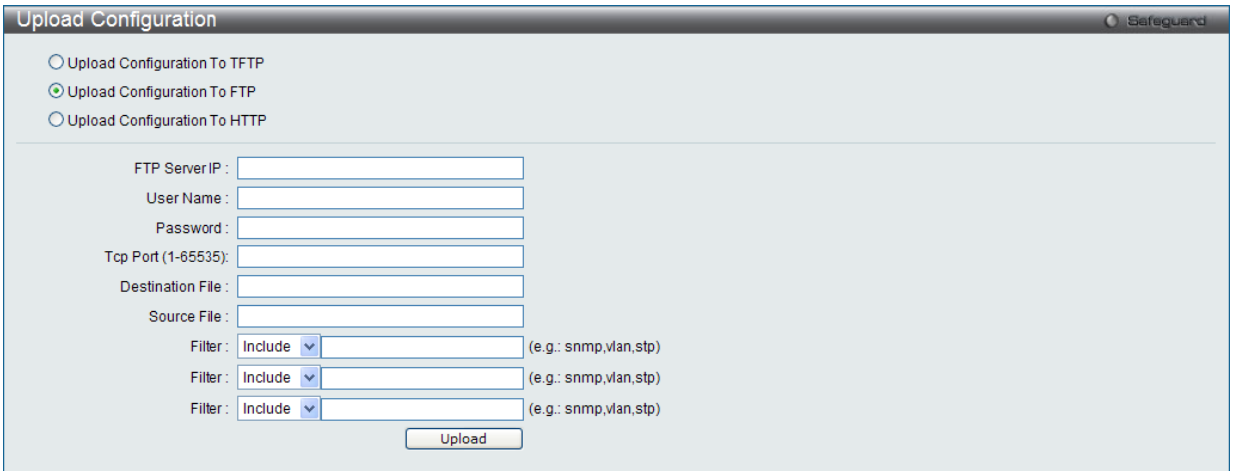


図 16-13　Upload Configuration To FTP 画面

以下の項目があります。

項目	説明
FTP Server IP	使用する FTP サーバの IP アドレスを指定します。
User Name	使用する適切なユーザ名を指定します。
Password	使用する適切なパスワードを指定します。
TCP Port	使用する TCP ポート番号を入力します。
Destination File	送信先ファイルの位置と名前を入力します。
Source File	送信元ファイルの位置と名前を入力します。
Filter	ここでは、SNMP、VLAN または STP のようなフィルタを含む（include）、開始する（begin）、または除外（exclude）するように指定できます。適切な「Filter」アクションを選択し、提供されたスペースにファイル名を入力します。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Configuration To HTTP（コンフィグレーションを HTTP にアップロードする）

スイッチからコンピュータにコンフィグレーションファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Configuration** を選択し、「Upload Configuration To HTTP」を選択して以下の画面を表示します。

図 16-14 Upload Configuration To HTTP 画面

以下の項目があります。

項目	説明
Source File	送信先ファイルの位置と名前を入力します。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Log File（ログファイルのアップロード）

スイッチのログファイルをアップロードします。

Upload Log To TFTP（TFTP サーバにログをアップロードする）

スイッチから TFTP サーバにログファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Log File** を選択し、「Upload Log To TFTP」を選択して以下の画面を表示します。

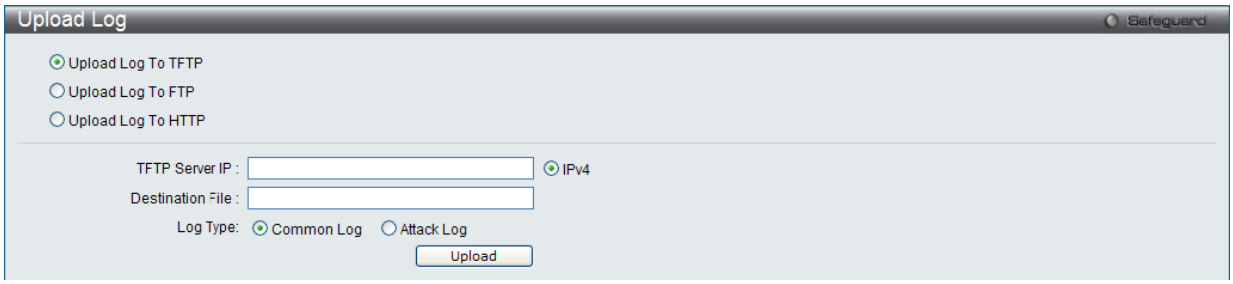


図 16-15 Upload Log To TFTP 画面

以下の項目があります。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。ユーザが、IPv4 アドレスを入力するためには「IPv4」、IPv6 を入力するためには「IPv6」を選択して提供されている欄に IP アドレスを入力します。
Destination File	送信先ファイルの位置と名前を入力します。
Log Type	転送されるログのタイプを選択します。 • Common Log - 一般的なログエントリをアップロードします。 • Attack Log - 攻撃に関するログをアップロードします。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Log To FTP（FTP サーバにログをアップロードする）

スイッチから FTP サーバにログファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Log File** を選択し、「Upload Log To FTP」を選択して以下の画面を表示します。

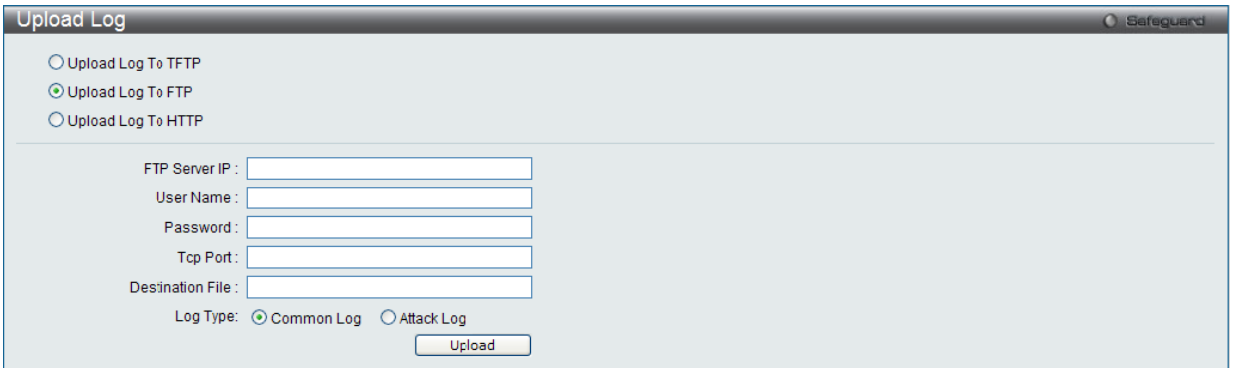


図 16-16 Upload Log To FTP 画面

以下の項目があります。

項目	説明
FTP Server IP	使用する FTP サーバの IP アドレスを指定します。
User Name	使用する適切なユーザ名を指定します。
Password	使用する適切なパスワードを指定します。
TCP Port	使用する TCP ポート番号を入力します。
Destination File	送信先ファイルの位置と名前を入力します。
Log Type	転送されるログのタイプを選択します。 • Common Log - 一般的なログエントリをアップロードします。 • Attack Log - 攻撃に関するログをアップロードします。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Log To HTTP（HTTP にログをアップロードする）

スイッチからコンピュータにログファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Log File** を選択し、「Upload Log To HTTP」を選択して以下の画面を表示します。

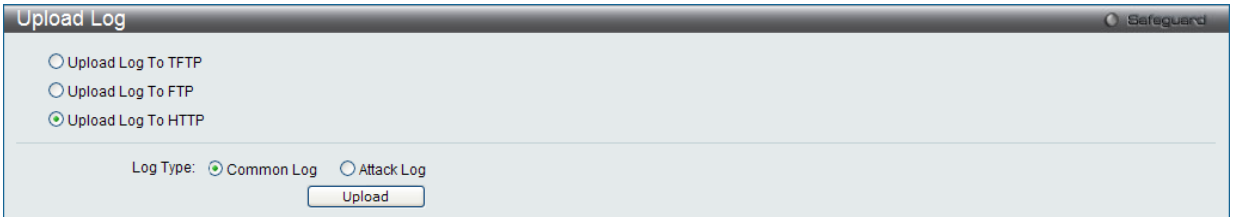


図 16-17 Upload Log To HTTP 画面

以下の項目があります。

項目	説明
Log Type	転送されるログのタイプを選択します。 • Common Log - 一般的なログエントリをアップロードします。 • Attack Log - 攻撃に関するログをアップロードします。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Reset（リセット）

スイッチのリセット機能にはいくつかのオプションが用意されています。いくつかのパラメータの設定内容を保持したままで、他のすべての設定内容を工場出荷時状態に戻すことが可能です。

注意 「Reset System」オプションだけは工場出荷時設定をスイッチの NV-RAM に書き込み、スイッチを再起動します。他のすべてのオプションは現在の設定を出荷時設定に戻しますが、この設定は保存されません。「Reset System」はスイッチのコンフィグレーションを工場出荷状態まで戻します。

「Reset」はスイッチの IP アドレス、ユーザアカウント、およびバナーを除いて他のすべての設定を工場出荷時の初期設定に戻します。スイッチは、本画面を使用してリセットされ、「Save」オプションが実行されないと、スイッチは再起動時に最後に保存されたコンフィグレーションに戻ります。

Web マネージャ先頭の **Tools > Reset** を選択し、以下の画面を表示します。

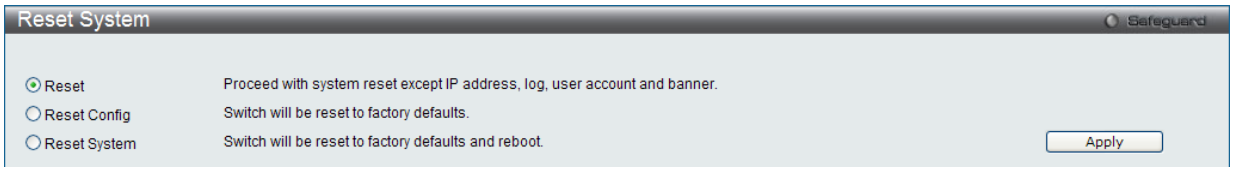


図 16-18　Reset System 画面

項目	説明
Reset	IP アドレス、ログ、ユーザアカウントおよびバナーを除いてスイッチを工場出荷時の初期設定に戻します。
Reset Config	スイッチを工場出荷時設定にリセットしますが、再起動は行いません。
Reset System	スイッチを工場出荷時設定にリセットして、再起動を実行します。

「Apply」ボタンをクリックして、リセット操作を開始します。

Reboot System（システムの再起動）

以下の画面を使用してスイッチの再起動を行います。

Tools > Reboot の順にクリックし、以下の画面を表示します。

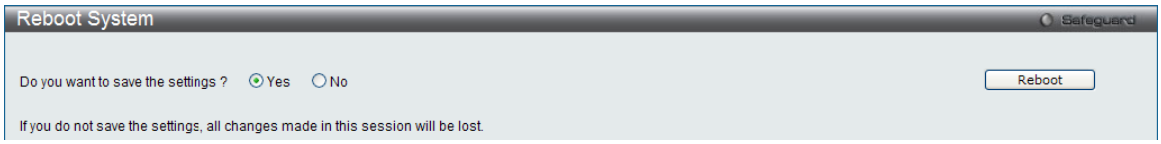


図 16-19　Reboot System 画面

項目	説明
Yes	スイッチは再起動する前に現在の設定を NV-RAM に保存します。
No	スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。
Reboot	スイッチは再起動します。

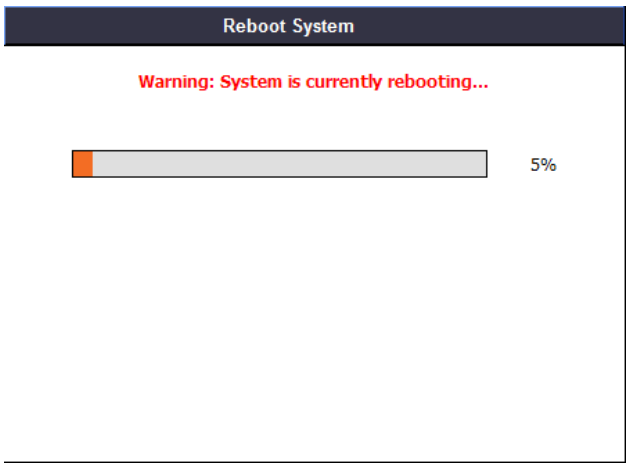


図 16-20　System Reboot 画面

付録 A ケーブルとコネクタ

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。
以下の図と表は標準の RJ-45 プラグ / コネクタとピンアサインです。

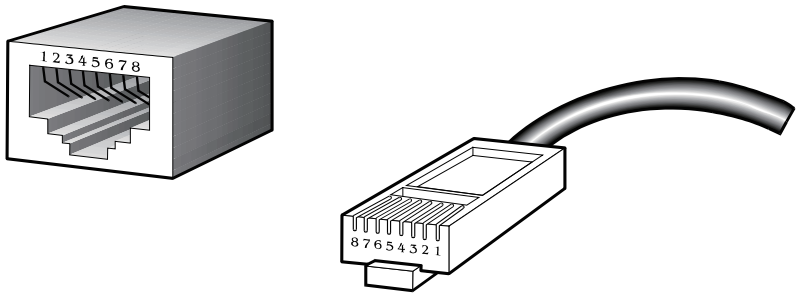


表 A-1　標準的な RJ-45 ピンアサイン

RJ-45 ピンアサイン		
コンタクト（ピン番号）	MDI-X 信号	MDI-II 信号
1	RD+（受信）	TD+（送信）
2	RD-（受信）	TD-（送信）
3	TD+（送信）	RD+（受信）
4	1000BASE-T	1000BASE-T
5	1000BASE-T	1000BASE-T
6	TD-（送信）	RD-（受信）
7	1000BASE-T	1000BASE-T
8	1000BASE-T	1000BASE-T

付録 B ケーブル長

以下の表は各規格に対応するケーブル長 (最大) です。

規格	メディアタイプ	最大伝送距離
Mini-GBIC	1000BASE-LX、シングルモードファイバモジュール 1000BASE-SX、マルチモードファイバモジュール 1000BASE-LH、シングルモードファイバモジュール 1000BASE-ZX、シングルモードファイバモジュール	10 km 550 m 40 km 80 km
1000BASE-T	エンハンスドカテゴリ 5 UTP ケーブル カテゴリ 5 UTP ケーブル（1000 Mbps）	100 m
100BASE-TX	カテゴリ 5 UTP ケーブル（100 Mbps）	100 m
10BASE-T	カテゴリ 3 UTP ケーブル（10 Mbps）	100 m

付録 C ログイベント

スイッチのシステムログに表示される可能性のあるログイベントとそれらの意味を以下に示します。

Critical（重大）、Warning（警告）、Informational（報告）

カテゴリ	ログの内容	緊急度	イベントの説明
システム	System started up	Critical	システムスタート
	System warm start	Critical	システムのウォームスタート
	System cold start	Critical	システムのコールドスタート
	Configuration saved to flash by console (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	コンソールでコンフィグレーションをフラッシュメモリに保存しました。
	System log saved to flash by console (Username: < ユーザ名 > IP: <IP アドレス >)	Informational	コンソールでシステムログをフラッシュメモリに保存しました。
	Configuration and log saved to flash by console(Username: < ユーザ名 > IP: <IP アドレス >)	Informational	コンソールでコンフィグレーションとシステムログをフラッシュメモリに保存しました。
	Internal Power failed	Critical	内部電源が故障しました。
	Internal Power is recovered	Critical	内部電源が故障から回復しました。
	Side Fan failed	Critical	側面のファンが故障しました。
	Side Fan recovered	Critical	側面のファンの故障から回復しました。
	Back Fan failed	Critical	背面のファンが故障しました。
	Back Fan recovered	Critical	背面のファンの故障から回復しました。
	Temperature sensor < センサ ID> enters alarm state (current temperature: < 温度 >)	Warning	温度センサがアラーム状態に入りました。
	Temperature sensor < センサ ID> recovers to normal state (current temperature: < 温度 >)	Informational	温度が正常に戻りました。
アップロード / ダウンロード	Firmware upgraded by console successfully (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	ファームウェアの更新成功。
	Firmware upgrade by console was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	ファームウェアの更新失敗。
	Configuration successfully downloaded by console (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	コンフィグレーションファイルのダウンロード成功。
	Configuration download by console was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	コンフィグレーションファイルのダウンロード失敗。
	Configuration successfully uploaded by console (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	コンフィグレーションファイルのアップロード成功。
	Configuration upload by console was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	コンフィグレーションファイルのアップロード失敗。
	Log message successfully uploaded by console (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	ログメッセージのアップロード成功。
	Log message upload by console was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	ログメッセージのアップロード失敗。
	Firmware successfully uploaded by console (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	ファームウェアのアップロード成功。
	Firmware upload by console was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	ファームウェアのアップロード失敗。
インタフェース	Port < ポート番号 > link up, < リンク状態 >	Informational	ポートリンクアップ
	Port < ポート番号 > link down	Informational	ポートリンクダウン
コンソール	Successful login through Console (Username: < ユーザ名 >)	Informational	コンソール経由のログイン成功
	Login failed through Console (Username: < ユーザ名 >)	Warning	コンソール経由のログイン失敗
	Logout through Console (Username: < ユーザ名 >)	Informational	コンソール経由でログアウト
	Console session timed out (Username: < ユーザ名 >)	Informational	コンソールセッション、タイムアウト

カテゴリ	ログの内容	緊急度	イベントの説明
Web	Successful login through Web (Username: <ユーザ名>, IP: <IPアドレス>)	Informational	Web 経由のログイン成功
	Login failed through Web (Username: <ユーザ名>, IP: <IPアドレス>)	Warning	Web 経由のログイン失敗
	Logout through Web (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Web 経由でログアウト
	Web session timed out (Username: < ユーザ名 >, IP:<IP アドレス >)	Informational	Web セッションタイムアウト
	Successful login through Web(SSL) (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Web(SSL) 経由のログイン成功
	Login failed through Web(SSL) (Username: <ユーザ名>, IP: <IPアドレス>)	Warning	Web(SSL) 経由のログイン失敗
	Logout through Web(SSL) (Username: <ユーザ名>, IP: <IPアドレス>)	Informational	Web(SSL) 経由でログアウト
	Web(SSL) session timed out (Username: <ユーザ名>, IP:<IPアドレス>)	Informational	Web(SSL) セッションタイムアウト
Telnet	Successful login through Telnet (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Telnet 経由のログイン成功
	Login failed through Telnet (Username: <ユーザ名>, IP: <IPアドレス>)	Warning	Telnet 経由のログイン失敗
	Logout through Telnet (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Telnet 経由でログアウト
	Telnet session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Telnet セッションタイムアウト
SNMP	SNMP request received from < IP アドレス > with invalid community string !	Informational	無効なコミュニティ名を含む SNMP request 受信
STP	Topology changed (Instance:< インスタンス ID> port< ポート番号 >)	notice	トポロジ変更
	Spanning Tree Protocol is enabled	Informational	スパニングツリープロトコル有効化
	Spanning Tree Protocol is disabled	Informational	スパニングツリープロトコル無効化
	CIST New Root bridge selected (<MAC アドレス > Priority :< 値 >)	Informational	新規ルートを選択
	CIST Region New Root bridge selected (<MACアドレス> Priority :<値>)	Informational	新規ルートを選択
	MSTI Region New Root bridge selected([Instance: < インスタンス ID>]MAC: <MAC アドレス > Priority :< 値 >)	Informational	新規ルートを選択
	New Root bridge selected (<MAC アドレス > Priority :< 値 >)	Informational	新規ルートを選択
	New root port selected (Instance:<インスタンス>, Port:<ポート番号>)	notice	新規ルートポートを選択
	Spanning Tree port status changed (Instance:< インスタンス >, Port:< ポート番号 >) <old_status> -> < 新しい状態 >	notice	スパニングツリーポート状態の変更
	Spanning Tree port role changed (Instance:< インスタンス >, Port:< ポート番号 >) <old_role> -> < 新規ロール >	Informational	スパニングツリーポートのロール変更
	Spanning Tree instance created (Instance:< インスタンス ID>)	Informational	スパニングツリーインスタンスの作成
	Spanning Tree instance deleted (Instance:< インスタンス ID>)	Informational	スパニングツリーインスタンスの削除
	Spanning Tree version changed (new version:< 新バージョン >)	Informational	スパニングツリーバージョンの変更
	Spanning Tree MST configuration ID name and revision level changed (name:< 名前 > ,revision level < リビジョンレベル >)	Informational	スパニングツリー MST コンフィグレーション ID 名とリビジョンレベルの変更
	Spanning Tree MST configuration ID VLAN mapping table changed (instance: < インスタンス ID> add vlan < 開始 VLANID> [- < 終了 VLANID>])	Informational	スパニングツリー MST コンフィグレーション ID が VLAN マッピングテーブルに追加
	Spanning Tree MST configuration ID VLAN mapping table changed (instance: < インスタンス ID> delete vlan < 開始 VLANID> [- < 終了 VLANID>])	Informational	スパニングツリー MST コンフィグレーション ID が VLAN マッピングテーブルから削除
DoS	Possible spoofing attack from (IP: <IP アドレス > MAC: <MAC アドレス > Port: < ポート番号 >)	Critical	スプーフィング攻撃 1. 送信元 IP は、送信元 MAC アドレスが異なるのにもかかわらず、スイッチのインタフェース IP と同じです。 2. 送信元 IP が ARP パケット内のスイッチの IP と同じです。 3. 自身の IP パケットが検出されました。
	<DoS 名 > is blocked from (IP: <IP アドレス > Port: < ポート番号 >)	Critical	DoS 攻撃がブロックされました。
SSH	Successful login through SSH (Username: <ユーザ名>, IP: <IPアドレス>)	Informational	SSH 経由のログイン成功
	Login failed through SSH (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	SSH 経由のログイン失敗
	Logout through SSH (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	SSH 経由のログアウト
	SSH session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	SSH セッションタイムアウト
	SSH server is enabled	Informational	SSH サーバ有効化
	SSH server is disabled	Informational	SSH サーバ無効化

カテゴリ	ログの内容	緊急度	イベントの説明
AAA	Authentication Policy is enabled (Module: AAA)	Informational	認証ポリシー有効化
	Authentication Policy is disabled (Module: AAA)	Informational	認証ポリシー無効化
	Successful login through Console authenticated by AAA local method（Username: < ユーザ名 >）	Informational	AAA ローカルメソッドによるコンソール経由のログイン認証成功
	Login failed through Console authenticated by AAA local method（Username: < ユーザ名 >）	Warning	AAA ローカルメソッドによるコンソール経由のログイン認証失敗
	Successful login through Web from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによる Web 経由のログイン認証成功
	Login failed through Web from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによる Web 経由のログイン認証失敗
	Successful login through Web(SSL) from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによる Web (SSL) 経由のログイン認証成功
	Login failed through Web(SSL) from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによる Web (SSL) 経由のログイン認証失敗
	Successful login through Telnet from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによる Telnet 経由のログイン認証成功
	Login failed through Telnet from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによる Telnet 経由のログイン認証失敗
	Successful login through SSH from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによる SSH 経由のログイン認証成功
	Login failed through SSH from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによる SSH 経由のログイン認証失敗
	Successful login through Console authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによるコンソール経由のログイン認証成功
	Successful login through Web from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Web 経由のログイン認証成功
	Successful login through Web(SSL) from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Web (SSL) 経由のログイン認証成功
	Successful login through Telnet from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Telnet 経由のログイン認証成功
	Successful login through SSH from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる SSH 経由のログイン認証成功
	Successful login through Console authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによるコンソール経由のログイン認証成功
	Login failed through Console authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによるコンソール経由のログイン認証失敗
	Login failed through Console due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による コンソール経由のログイン認証失敗
	Successful login through Web from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Web 経由のログイン認証成功
	Login failed through Web from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Web 経由のログイン認証失敗
	Login failed through Web from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Web 経由の Admin レベル遷移失敗
	Successful login through Web(SSL) from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Web (SSL) 経由のログイン認証成功
	Login failed through Web(SSL) from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Web (SSL) 経由のログイン認証失敗
	Login failed through Web(SSL) from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Web (SSL) 経由のログイン認証失敗
	Successful login through Telnet from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Telnet 経由のログイン認証成功
	Login failed through Telnet from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Telnet 経由のログイン認証失敗
	Login failed through Telnet from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Telnet 経由のログイン失敗

カテゴリ	ログの内容	緊急度	イベントの説明
AAA	Successful login through SSH from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる SSH 経由のログイン認証成功
	Login failed through SSH from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる SSH 経由のログイン認証失敗
	Login failed through SSH from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による SSH 経由のログイン失敗
	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによるコンソール経由の Admin レベル遷移成功
	Enable Admin failed through Console authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	AAA local_enable メソッドによるコンソール経由の Admin レベル遷移失敗
	Successful Enable Admin through Web from <ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによる Web 経由の Admin レベル遷移成功
	Enable Admin failed through Web from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	AAA local_enable メソッドによる Web 経由の Admin レベル遷移失敗
	Successful Enable Admin through Web(SSL) from < ユ ー ザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによる Web(SSL) 経由の Admin レベル遷移成功
	Enable Admin failed through Web(SSL) from < ユーザ IP> authenticated by AAA local_enable method (Username: <ユーザ名 >)	Warning	AAA local_enable メソッドによる Web(SSL) 経由の Admin レベル遷移失敗
	Successful Enable Admin through Telnet from <ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによる Telnet 経由の Admin レベル遷移成功
	Enable Admin failed through Telnet from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	AAA local_enable メソッドによる Telnet 経由の Admin レベル遷移失敗
	Successful Enable Admin through SSH from <ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによる SSH 経由の Admin レベル遷移成功
	Enable Admin failed through <Telnet、Web または SSH> from < ユーザ IP> authenticated by AAA local_enable method (Username: <ユーザ名 >)	Warning	AAA local_enable メソッドによる SSH 経由の Admin レベル遷移失敗
	Successful Enable Admin through Console authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによるコンソール経由の Admin レベル遷移成功
	Successful Enable Admin through Web from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Web 経由の Admin レベル遷移成功
	Successful Enable Admin through Web(SSL) from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Web(SSL) 経由の Admin レベル遷移成功
	Successful Enable Admin through Telnet from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Telnet 経由の Admin レベル遷移成功
	Successful Enable Admin through SSH from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる SSH 経由の Admin レベル遷移成功
	Successful Enable Admin through Console authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによるコンソール経由の Admin レベル遷移成功
	Enable Admin failed through Console authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによるコンソール経由の Admin レベル遷移失敗
	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定によるコンソール経由の Admin レベル遷移失敗
	Successful Enable Admin through Web from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Web 経由の Admin レベル遷移成功
	Enable Admin failed through Web from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Web 経由の Admin レベル遷移失敗
	Enable Admin failed through Web due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Web 経由の Admin レベル遷移失敗
	Successful Enable Admin through Web(SSL) from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Web(SSL) 経由の Admin レベル遷移成功
	Enable Admin failed through Web(SSL) from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Web(SSL) 経由の Admin レベル遷移失敗
	Enable Admin failed through Web(SSL) due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Web(SSL) 経由の Admin レベル遷移失敗

カテゴリ	ログの内容	緊急度	イベントの説明
AAA	Successful Enable Admin through Telnet from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Telnet 経由の Admin レベル遷移成功
	Enable Admin failed through Telnet from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Telnet 経由の Admin レベル遷移失敗
	Enable Admin failed through Telnet from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Telnet 経由の Admin レベル遷移失敗
	Successful Enable Admin through SSH from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる SSH 経由の Admin レベル遷移成功
	Enable Admin failed through SSH from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる SSH 経由の Admin レベル遷移失敗
	Enable Admin failed through SSH from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による SSH 経由の Admin レベル遷移失敗
	AAA server < サーバ IP> (Protocol: < プロトコル >) connection failed Warning		AAA サーバタイムアウト
	AAA server < サーバ IP> (Protocol: < プロトコル名 >) response is wrong	Warning	AAA サーバの応答が不正です。
	AAA doesn't support this functionality	Informational	AAA はこの機能を未サポートです。
ポートセキュリティ	Port security violation (MAC address:<MAC アドレス > on port:< ポート番号 >)	Warning	ポートセキュリティは最大学習サイズを超えたため、新しいアドレスを学習できません。
IP-MAC ポートバインディング	Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <IP アドレス >, MAC: <MAC アドレス >, Port < ポート番号 >)	Warning	IP-MAC ポートバインディング機能により、非認証の IP アドレスからのパケットを廃棄しました。
	Dynamic IMPB entry is conflicting with static ARP(IP: <IP アドレス >, MAC: <MAC アドレス >, Port: < ポート番号 >)	Informational	ダイナミック IMPB エントリが、スタティック ARP とコンフリクトしています。
	Dynamic IMPB entry is conflicting with static FDB(IP: <IP アドレス >, MAC: <MAC アドレス >, Port: < ポート番号 >)	Informational	ダイナミック FDB エントリが、スタティック ARP とコンフリクトしています。
	Dynamic IMPB entry is conflicting with static IMPB: IP: <IP アドレス >, MAC: <MAC アドレス >, Port: < ポート番号 >	Informational	ダイナミック IMPB エントリが、スタティック IMPB とコンフリクトしています。
	Creating IMPB entry failed due to no ACL rule available: IP: <IP アドレス >, MAC: <MAC アドレス >, Port: < ポート番号 >	Informational	有効な ACL ルールがないため、IMPB エントリの作成に失敗しました。
IP とパスワード変更	Management IP address was changed by (Username: < ユーザ名 >,IP:<IP アドレス >)	Informational	IP アドレスが変更されました。
	Password was changed by (Username: < ユーザ名 >,IP:<IP アドレス >)	Informational	パスワードが変更されました。
セーフガードエンジン	SafeGuard Engine enters NORMAL mode	Informational	セーフガードエンジン機能がノーマルモードに遷移しました。
	Safeguard Engine enters EXHAUSTED mode	Warning	セーフガードエンジン機能がフィルタリングパケットモードに遷移しました。
パケットストーム	Port < ポート番号 > Broadcast storm is occurring	Warning	ブロードキャストストーム発生中。
	Port < ポート番号 > Broadcast storm has cleared	Informational	ブロードキャストストーム停止。
	Port < ポート番号 > Multicast storm is occurring	Warning	マルチキャストストーム発生中。
	Port < ポート番号 > Multicast storm has cleared	Informational	マルチキャストストーム停止。
	Port < ポート番号 > is currently shut down due to a packet storm	Warning	パケットストームのためにポートはシャットダウン。
ループバック検知	Port < ポート番号 > LBD loop occurred. Port blocked	Critical	ポートにループが発生し、ポートはブロックされました。
	Port < ポート番号 > LBD port recovered. Loop detection restarted	Informational	インターバルタイム後に LBD ポートが回復し、ループ検知が再スタートしました。
	Port < ポート番号 > VID <VLAN ID> LBD loop occurred. Packet discard begun	Critical	VID を持つポートにループが発生しました。パケットの破棄が開始されました。
	Port < ポート番号 > VID <VLAN ID> LBD recovered. Loop detection restarted	Informational	VID を持つポートが回復し、ループ検知が再スタートしました。

カテゴリ	ログの内容	緊急度	イベントの説明
802.1X	Radius server < サーバ IP> assigned VID: <VLAN ID> to port < ポート番号 > (Account: < ユーザ名 >)	Informational	RADIUS サーバによる RADIUS クライアント認証の成功後に、RADIUS サーバから割り当てられる VID。この VID はポートに割り当てられ、このポートは VLAN タグなしポートのメンバになります。
	Radius server < サーバ IP> assigned ingress bandwidth:< イングレス帯域値 > to port< ポート番号 > (Account:< ユーザ名 >)	Informational	RADIUS サーバによる RADIUS クライアント認証の成功後に、RADIUS サーバから割り当てられるイングレス帯域。このイングレス帯域はポートに割り当てられます。
	Radius server < サーバ IP> assigned egress bandwidth:< イーグレス帯域値 > to port< ポート番号 > (Account:< ユーザ名 >)	Informational	RADIUS サーバによる RADIUS クライアント認証の成功後に、RADIUS サーバから割り当てられるイーグレス帯域。このイーグレス帯域はポートに割り当てられます。
	Radius server < サーバ IP> assigned 802.1p default priority: < プライオリティ > to port < ポート番号 > (Account:< ユーザ名 >)	Informational	RADIUS サーバによる RADIUS クライアント認証の成功後に、RADIUS サーバから割り当てられる 802.1p デフォルトプライオリティ。この 802.1p デフォルトプライオリティはポートに割り当てられます。
	802.1x Authentication failure from (Username: < ユーザ名 >, Port < ポート番号 >, MAC: <MAC アドレス >)	Warning	802.1X 認証失敗
	802.1x Authentication success from (Username: < ユーザ名 >, Port < ポート番号 >, MAC: <MAC アドレス >)	Informational	802.1X 認証成功
CFM	CFM cross-connect. VLAN:<VLAN ID>, Local (MD Level:<MD レベル >, Port < ポート番号 >, Direction: <MEP direction>) Remote (MEPID:<MEP ID>, MAC: <MAC アドレス >)	Critical	クロスコネクトの検出
	CFM error ccm. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local(Port < ポート番号 >, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<MAC アドレス >)	Warning	エラー CFM CCM パケットの検出
	CFM remote down. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP direction>)	Warning	リモート MEP の CCM パケットを受信できません。
	CFM remote MAC error. MD Level:<MD レベル l>, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP direction>)	Warning	リモート MEP の MAC はエラー状態を報告しています。
	CFM remote detects a defect. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP direction>)	Informational	リモート MEP は CFM 不良を検出しています。
ARP	Conflict IP was detected with this device (IP: <IP アドレス >, MAC: <MAC アドレス >, Port < ポート番号 >, Interface: <ip インタフェース名 >)	Informational	Gratuitous ARP は重複 IP アドレスを検出しました。
DHCP	Detected untrusted DHCP server(IP: <IP アドレス >, Port: < ポート番号 >)	Informational	信頼性の低い DHCP サーバの IP アドレスを検出。
コマンドログ出力	< ユーザ名 >: execute command "< 文字列 >"	Informational	コマンドをログに出力します。
MAC ベースアクセスコントロール	MAC-based Access Control host login successful (MAC: <MAC アドレス >, port: < ポート番号 >, VID: <VLAN ID>)	Information	ホストは認証に成功しました。
	MAC-based Access Control unauthenticated host (MAC: <MAC アドレス >, Port < ポート番号 >, VID: <VID>)	Information	ホストは認証通過に失敗しました。
	MAC-based Access Control host aged out (MAC: <MAC アドレス >, port: < ポート番号 >, VID: <VLAN ID>)	Information	ホストはエージングされました。
	Port < ポート番号 > enters MAC-based Access Control stop learning state	Warning	ポートにおける認可ユーザ数が最大ユーザの制限に到達しました。
	Port < ポート番号 > recovers from MAC-based Access Control stop learning state	Warning	ポートにおける認可ユーザ数が時間内の最大ユーザの制限に到達しました。(時間はプロジェクトに依存します。)
	MAC-based Access Control enters stop learning state	Warning	デバイス全体の認可ユーザ数が最大ユーザの制限に到達しました。
	MAC-based Access Control recovers from stop learning state	Warning	デバイス前端の認可ユーザ数が時間内の最大ユーザの制限に到達しました。(時間はプロジェクトに依存します。)

カテゴリ	ログの内容	緊急度	イベントの説明
BPDU 防御	Port < ポート番号 > enter BPDU under attacking state (mode: drop)	Informational	攻撃状態下でポートは BPDU 防御（破棄）に入りました。
	Port < ポート番号 > enter BPDU under attacking state (mode: block)	Informational	攻撃状態下でポートは BPDU 防御（ブロック）に入りました。
	Port < ポート番号 > enter BPDU under attacking state (mode: shutdown)	Informational	攻撃状態下でポートは BPDU 防御（シャットダウン）に入りました。
	Port < ポート番号 > recover from BPDU under attacking state automatically	Informational	ポートは BPDU 防御から自動的に回復しました。
	Port < ポート番号 > recover from BPDU under protection state manually	Informational	ポートは BPDU 防御から手動で回復しました。
	System re-start reason: system fatal error	Emergent	システム再起動の原因 : システムのファータルエラー
	System re-start reason: CPU exception	Emergent	システム再起動の原因 : CPU 例外エラー
診断	Diagnostic: Burn in start at %S	Informational	診断 : バーンイン開始
	Diagnostic: Burn in end at %S	Informational	診断 : バーンイン終了
	Diagnostic: Burn in result is %S	Informational	診断 : バーンイン結果
DULD	Port: < ポート番号 > is unidirectional		単方向リンクが本ポートで検出。
ERPS	Signal fail detected on node (MAC: <MAC アドレス >)	Informational	シグナルエラーの検出
	Signal fail cleared on node (MAC: <MAC アドレス >)	Informational	シグナルエラーのクリア
	RPL owner conflicted on the ring (MAC: <MAC アドレス >)	Warning	RPL オーナーの重複

付録 D トラップログ

トラップ名 /OID	変数バインド	形式	MIB 名
coldStart	None	V1/V2	SNMPv2-MIB
warmStart	None	V1/V2	SNMPv2-MIB
linkDown	ifIndex	V1/V2	IF-MIB
linkUp	ifIndex	V1/V2	IF-MIB
authenticationFailure	None	V1/V2	SNMPv2-MIB
newRoot	None	V1/V2	BRIDGE-MIB
topologyChange	None	V1/V2	BRIDGE-MIB
risingAlarm	alarmIndex alarmVariable alarmSampleType alarmValue alarmRisingThreshold	V1/V2	RMON-MIB
fallingAlarm	alarmIndex alarmVariable alarmSampleType alarmValue alarmFallingThreshold	V1/V2	RMON-MIB
lldpRemTablesChange	lldpStatsRemTablesInserts lldpStatsRemTablesDeletes lldpStatsRemTablesDrops lldpStatsRemTablesAgeouts	V1/V2	LLDP-MIB
swPowerStatusChg	swPowerUnitIndex swPowerID swPowerStatus	V2	Equipment.MIB
swPowerFailure	swPowerUnitIndex, swPowerID swPowerStatus	V2	Equipment.MIB
swPowerRecover	swPowerUnitIndex swPowerID swPowerStatus	V2	Equipment.MIB
swFanFailure	swFanUnitIndex swFanID	V2	Equipment.MIB
swFanRecover	swFanUnitIndex swFanID	V2	Equipment.MIB
swHighTemperature	swTemperatureUnitIndex swTemperatureCurrent	V2	Equipment.MIB
swHighTemperatureRecover	swTemperatureUnitIndex swTemperatureCurrent	V2	Equipment.MIB
swLowTemperature	swTemperatureUnitIndex swTemperatureCurrent	V2	Equipment.MIB
swLowTemperatureRecover	swTemperatureUnitIndex swTemperatureCurrent	V2	Equipment.MIB
swPktStormOccurred	swPktStormCtrlPortIndex	V2	PktStormCtrl.mib
swPktStormCleared	swPktStormCtrlPortIndex	V2	PktStormCtrl.mib
swPktStormDisablePort	swPktStormCtrlPortIndex	V2	PktStormCtrl.mib
swSafeGuardChgToExhausted	swSafeGuardCurrentStatus	V2	SafeGuard.mib
swSafeGuardChgToNormal	swSafeGuardCurrentStatus	V2	SafeGuard.mib
swIpMacBindingRecoverLearningTrap	swIpMacBindingPortIndex	V2	IPMacBind.mib
SwMacBasedAuthLoggedSuccess	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	mba.mib
swMacBasedAuthLoggedFail	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	mba.mib

トラップ名 /OID	変数バインド	形式	MIB 名
SwMacBasedAuthAgesOut	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	mba.mib
swFilterDetectedTrap	swFilterDetectedIP swFilterDetectedport	V2	Filter.MIB
swPortLoopOccurred	swLoopDetectPortIndex	V2	LBD.mib
swPortLoopRestart	swLoopDetectPortIndex	V2	LBD.mib
swVlanLoopOccurred	swLoopDetectPortIndex	V2	LBD.mib
swVlanLoopRestart	swLoopDetectPortIndex swVlanLoopDetectVID	V2	LBD.mib
swDdmAlarmTrap	swDdmPort swDdmThresholdType swDdmThresholdExceedType	V2	DDM.MIB
swDdmWarningTrap	swDdmPort swDdmThresholdType swDdmThresholdExceedType	V2	DDM.MIB
swBpduProtectionUnderAttackingTrap	swBpduProtectionPortIndex swBpduProtectionPortMode	V2	BPDUProtection.MIB
swBpduProtectionRecoveryTrap	swBpduProtectionPortIndex swBpduProtectionRecoveryMethod	V2	BPDUProtection.MIB
swL2macNotification	swL2macNotifyInfo	V2	L2MGMT-MIB
swL2PortSecurityViolationTrap	swPortSecPortIndex swL2PortSecurityViolationMac	V2	L2MGMT-MIB
swERPSSFDetectedTrap	swERPSNodeId	V2	ERPS.mib
swERPSSFClearedTrap	swERPSNodeId	V2	ERPS.mib
swERPSRPLOwnerConflictTrap	swERPSNodeId	V2	ERPS.mib
agentCfgOperCompleteTrap	unitID agentCfgOperate agentLoginUserName	V2	Genmgmt.mib
agentFirmwareUpgrade	swMultiImageVersion	V2	Genmgmt.mib
agentGratuitousARPTrap	agentGratuitousARPIpAddr agentGratuitousARPMacAddr agentGratuitousARPPortNumber agentGratuitousARPInterfaceName	V2	Genmgmt.MIB
swSingleIPMSLinkDown	swSingleIPMSID swSingleIPMSMacAddr ifIndex	V2	SingleIP.mib
swSingleIPMSLinkUp	swSingleIPMSID swSingleIPMSMacAddr ifIndex	V2	SingleIP.mib
swSingleIPMSAuthFail	swSingleIPMSID swSingleIPMSMacAddr	V2	SingleIP.mib
swSingleIPMSnewRoot	swSingleIPMSID swSingleIPMSMacAddr	V2	SingleIP.mib
swSingleIPMSTopologyChange	swSingleIPMSID swSingleIPMSMacAddr	V2	SingleIP.mib
swDoSAttackDetected	swDoSCtrlType swDoSNotifyVarIpAddr swDoSNotifyVarPortNumber	V1/V2	DOSPrev.mib

付録 E RADIUS 属性の割り当て指定

DES-3200 における RADIUS 属性の割り当ては、以下のモジュールで使用されます。
- 802.1X（ポートベースとホストベース）
- MAC ベースのアクセスコントロール

以下の記述では、続く RADIUS 属性の割り当てのを説明します。
- Ingress/Egress 帯域
- 802.1p デフォルトプライオリティ
- VLAN
- ACL

RADIUS サーバで Ingress/Egress の帯域幅を割り当てるためには、適切なパラメータを RADIUS サーバに設定する必要があります。以下の表では帯域幅のパラメータを示しています。

ベンダー指定の属性の項目は以下の通りです。

ベンダー指定の属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171（DLINK）	必須
ベンダータイプ	本属性の定義	2（イングレス帯域用） 3（イーグレス帯域用）	必須
属性指定フィールド	ポートの帯域を割り当てるために使用します。	単位（Kbits）	必須

RADIUS サーバの帯域幅属性（例 : イングレス帯域幅 1000Kbps）を設定し、802.1X 認証に成功すると、RADIUS サーバに従ってデバイスは正しい帯域幅をポートに割り当てます。しかし、帯域幅属性を設定せずに認証に成功しても、デバイスは帯域幅をポートに割り当てません。帯域幅属性に 0 またはポートの有効帯域幅（イーサネットポートでは 100Mbps またはギガビットポートでは 1Gbps）より大きい数値を設定する場合、no_limit を指定します。

RADIUS サーバで 802.1p デフォルトプライオリティを割り当てるためには、適切な項目を RADIUS サーバに設定する必要があります。

ベンダー指定の属性の項目は以下の通りです。

ベンダー指定の属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171（DLINK）	必須
ベンダータイプ	本属性の定義	4	必須
属性指定フィールド	ポートの 802.1p デフォルトプライオリティを割り当てるために使用します。	0-7	必須

RADIUS サーバの 802.1p プライオリティ属性（例 : プライオリティ 7）を設定し、802.1X または MAC ベース認証に成功すると、RADIUS サーバに従ってデバイスは 802.1p デフォルトプライオリティをポートに割り当てます。しかし、プライオリティ属性を設定せずに認証に成功しても、デバイスはプライオリティをポートに割り当てません。RADIUS サーバに設定されたプライオリティ属性が範囲外（7 より大きい）であると、そのデバイスには設定されません。

RADIUS サーバで VLAN を割り当てるためには、適切なパラメータを RADIUS サーバに設定する必要があります。VLAN の割り当てを使用するために、RFC3580 では RADIUS パケットに以下のトンネル属性を定義しています。

以下の表では VLAN の項目を示しています。

RADIUS トンネル属性	説明	値	摘要
トンネルタイプ	本属性はトンネルの開始に使用されるトンネリングプロトコルまたはトンネルの終了に使用されるトンネリングプロトコルを示します。	13 (VLAN)	必須
Tunnel-Medium-Type	本属性は使用されている伝送の媒体を示します。	6 (802)	必須
Tunnel-Private-Group-ID	本属性は特定のトンネルセッションのグループ ID を示します。	文字列（VID）	必須

RADIUS サーバの VLAN 属性 (例 : VID 3) を設定し、802.1X または MAC ベースアクセスコントロール認証に成功すると、ポートは VLAN 3 に追加されます。しかし、VLAN 属性を設定せずに認証に成功しても、ポートは元の VLAN に置かれます。RADIUS サーバに設定された VLAN 属性が存在しないと、ポートは要求された VLAN に割り当てられません。

RADIUS サーバが ACL を割り当てるためには、適切な項目を RADIUS サーバに設定する必要があります。以下の表では ACL の項目を示しています。

RADIUS ACL の割り当ては、MAC ベースアクセスコントロールにて使用されるだけです。

ベンダー指定の属性の項目は以下の通りです。

RADIUS トンネル属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171 (DLINK)	必須
ベンダータイプ	属性を定義します。	12（ACL プロファイル用） 13 (ACL ルール用)	必須

属性指定フィールド	ACL プロファイルまたはルールを割り当てるために使用されます。	ACL コマンド
		例 :
		ACL プロファイル :
		`create access_profile profile_id 1 profile_name profile1 ethernet vlan 0xFFF`
		ACL ルール :
		`config access_profile profile_id 1 add access_id auto_assign ethernet vlan_id 1 port all deny`
			必須

RADIUS サーバの ACL 属性（例 : ACL プロファイル :「`create access_profile profile_id 1 profile_name profile1 ethernet vlan 0xFFF`」、ACL ルール :「`config access_profile profile_id 1 add access_id auto_assign ethernet vlan_id 1 port all deny`」）を設定し、MAC ベースアクセスコントロール認証に成功すると、RADIUS サーバに従ってデバイスは ACL プロファイルとルールを割り当てます。ACL モジュールに関する詳しい情報については、「DES-3200 CLI Reference Manual」の「Access Control List (ACL) Commands」を参照してください。

付録 F パスワードリカバリ手順

ここでは、弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用するこうとです。時々パスワードが忘れられたり、壊れたりするため、ネットワーク管理者は、これらのパスワードをリセットする必要があります。ここでは、パスワードリカバリ機能は、そのような場合にネットワーク管理者を助けるものです。以下の手順で、容易にパスワードを回復するパスワードリカバリ機能の使用方法を説明します。

これらの手順を終了するとパスワードはリセットされます。

1. セキュリティの理由のため、パスワードリカバリ機能は物理的にデバイスにアクセスすることが必要です。そのため、デバイスのコンソールポートへの直接接続を行っている場合だけ、本機能を適用することが可能です。ユーザは端末エミュレーションソフトを使用して、スイッチのコンソールポートに端末または PC を接続する必要があります。
2. 電源をオンにします。runtime image が 100% までロードされた後に、「Password Recovery Mode」に入るために、2 秒以内に、ホットキー「 ^ 」（シフト +6）を押します。「Password Recovery Mode」に一度入ると、スイッチのすべてのポートが無効になります。

```
  Boot Procedure                                          V4.00.000
--------------------------------------------------------------------------------

  Power On Self Test ....................................  100%

  MAC Address   : 00-01-02-03-04-00
  H/W Version   : C1

  Please Wait, Loading V1.00.024 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
```

```
Password Recovery Mode
>
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
reset config	リセットし、全設定を工場出荷時設定に戻します。
reboot	「Password Recovery Mode」を終了し、スイッチを再起動します。現在の設定を保存するように確認メッセージが表示されます。
reset account	作成済みのアカウントのすべてを削除します。
reset password	指定ユーザのパスワードをリセットします。
{< ユーザ名 >}	ユーザ名を指定しないと、すべてのユーザのパスワードがリセットされます。
show account	設定済みのすべてのアカウントを表示します。

付録 G 用語解説

用語	説明
1000BASE-LX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。長い光波長で長距離伝送用に使用されます。伝送距離 (最大) はシングルモード光ファイバを使用した場合で 10km。
1000BASE-SX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。短い光波長でマルチモード光ファイバを使用した場合伝送距離 (最大) は 550km。
100BASE-FX	光ファイバを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
100BASE-TX	カテゴリ 5 以上の UTP ケーブルを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
10BASE-T	IEEE 802.3 準拠でカテゴリ 3 以上の UTP ケーブルを使用する最大伝送速度 10Mbps の Ethernet の規格のひとつ。
エージング	タイムアウトし、無効のスイッチのダイナミックデータベースを自動的に消去します。
ATM	非同期転送モード。セルと呼ばれる固定長のセル (パケット) ベースで転送するプロトコル。ATM は音声、データおよびビデオ信号を含むユーザトラフィックの完全な列を転送するために開発されたものです。
オートネゴシエーション	スピード、デュプレックスおよびフローコントロールを自動的に認識する機能。オートネゴシエーションをサポートする端末と接続すると、リンクは自動的に最適なリンク条件に設定されます。
バックボーンポート	デバイスのアドレスを学習せず不明なアドレスを持つすべてのフレームを受信するポート。バックボーンポートは通常ご使用のネットワークのバックボーンにスイッチを接続するために使用されるポートです。バックボーンポートは以前はダウンリンクポートとして知られていました。
バックボーン	ネットワークセグメント間でトラフィックが転送される場合に優先パスとして使用されるネットワークの一部分。
帯域	1 秒あたりのビット数で計算される 1 チャンネルが転送できる情報量。イーサネットの帯域は 10Mbps、ファーストイーサネットは 100Mbps。
ボーレート	ラインのスイッチングスピード。ネットワークセグメント間のラインスピードとして知られています。
BOOTP	BOOTP プロトコルはデバイスが起動するたびに IP アドレスを MAC アドレスに自動マッピングします。さらにデバイスにサブネットマスク、デフォルトゲートウェイを割り当てます。
ブリッジ	たとえ高いレベルのプロトコルが関連してもローカルまたはリモートネットワークを相互接続するデバイス。ブリッジはネットワーク管理を中央に集めて 1 個の論理ネットワークを形成します。
ブロードキャスト	ネットワーク上のすべての終点デバイスに送信されるメッセージ。
ブロードキャストストーム	が主として可能なネットワーク帯域を奪い、ネットワークエラーを引き起こす Multiple simultaneous ブロードキャスト。
コンソールポート	端末またはモデムコネクタと接続可能なスイッチ上のポート。コンピュータ内でパラレル配列のデータをデータ転送リンクで使用されるシリアル形式に変換します。このポートはほとんどの場合ローカル管理のために使用されます。
CSMA/CD	イーサネットと IEEE 802.3 標準によって使用されるチャンネルアクセス方法で検索したデータチャンネルが一定期間後クリアされた後にだけデバイスに転送します。2 つのデバイスが同時に転送する場合、コリジョンが発生し、コリジョンを発生したデバイスは任意の時間再転送を遅らせます。
データセンタースイッチング	スイッチがサーバファームへの高パフォーマンスアクセス、高速バックボーン接続、およびネットワーク管理とセキュリティのためのコントロールポイントを提供するコーポレートネットワーク内のアグリゲーションポイント
イーサネット	Xerox、Intel および DEC が共同で開発した LAN 仕様。イーサネットネットワークは CSMA/CD を使用して 10Mbps で処理を行います。
ファーストイーサネット	Ethernet/CD ネットワークアクセス方法をベースにした 100Mbps 技術。
フローコントロール	(IEEE 802.3z) 端末に接続した転送ポートへのパケットを抑止します。受信バッファがあふれそうになった場合にパケットロスを防ぎます。
フォワーディング	中間のネットワークデバイスによりパケットを到達点に向けて送信するプロセス。
フルデュプレックス	同時にパケットの送受信を可能とし、スループットを 2 倍にするシステム。
ハーフデュプレックス	パケットの送受信を行うが、同時には行えないシステム。
IP アドレス	Internet Protocol アドレス。TCP/IP を使用するネットワークに付属するデバイスの固有な識別子。IPv4 アドレスは 8 ビットずつピリオドで区切られ、ネットワークセクション、サブネットセクション、ホストセクションで構成されます。
IPX（Internetwork Packet Exchange）	ネットワーク通信で使用するプロトコル。
LAN – ローカルエリアネットワーク	通常フロアもしくはビルのような規模の小さいエリアで PC、プリンタ、サーバのようなコンピュータリソースを接続するネットワーク。高速で低エラー率が特長です。
レイテンシ	デバイスがパケットを受信する時間とパケットが到達点ポートに転送される時間の遅延。
ラインスピード	ボーレートを参照。
メインポート	通常の操作条件でデータトラフィックを送信する Resilient リンク内のポート。
MDI（Medium Dependent Interface）	1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。
MDI-X（Medium Dependent Interface Cross-over）	接続送受信のラインが交差しているイーサネットポート接続。
MIB（Management Information Base）	デバイスの管理特性と設定項目を保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。
マルチキャスト	シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。
プロトコル	ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。
Resilient link	他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。
RJ-45	10BASE-T や 100BASE-TX などで使用する標準 8 線コネクタ
RMON	リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。

用語	説明
RPS（リダンダント電源システム）	スイッチに接続されて、バックアップ電源を供給するデバイス。
サーバファーム	大量のユーザにサービスを提供する中央に位置するサーバグループ。
SLIP（Serial Line Internet Protocol）	IP がシリアルライン接続を経由して動作することが可能なプロトコル。
SNMP（Simple Network Management Protocol）	当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。
スパニングツリープロトコル (STP)	ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。
スタック	1 個の論理的なデバイスの形をとするために統合されたネットワークデバイスのグループ。
スタンバイポート	リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。
スイッチ	パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。
TCP/IP	Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。
telnet	仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。
TFTP（Trivial File Transfer Protocol）	スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する (ソフトウェアアップグレードなど) ことができます。
UDP（User Datagram Protocol）	インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。
VLAN（Virtual LAN）	物理的に接続した LAN のように通信する位置やトポロジが独立しているデバイスのグループ。
VLT（Virtual LAN Trunk）	各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。
VT100	ASCII コードを使用するターミナルタイプ。VT100 画面はテキストベースの表示をします。