D-Link DES-3810 シリーズ

Layer3 10/100Mbps Managed 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。

⚠警告	この表示を無視し、まちがった使いかたをすると、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、まちがった使いかたをすると、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。

⚠警告

分解・改造をしない
分解禁止
機器が故障したり、異物が混入すると、やけどや火災の原因となります。

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
禁止
故障の原因につながります。

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
禁止
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してください。

ぬれた手でさわらない
ぬれ手禁止
感電のおそれがあります。

水をかけたり、ぬらしたりしない
水ぬれ禁止
内部に水が入ると、火災、感電、または故障のおそれがあります。

油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない
禁止
火災、感電、または故障のおそれがあります。

内部に金属物や燃えやすいものを入れない
禁止
火災、感電、または故障のおそれがあります。

表示以外の電圧で使用しない
禁止
火災、感電、または故障のおそれがあります。

たこ足配線禁止
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
禁止
火災、感電、または故障のおそれがあります。

雷鳴が聞こえたら、ケーブル / コード類にはさわらない
禁止
感電のおそれがあります。

ケーブル / コード類や端子を破損させない
禁止
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、または故障につながります。

正しい電源ケーブル、コンセントを使用する
禁止
火災、感電、または故障の原因となります。

乳幼児の手の届く場所では使わない
禁止
やけど、ケガ、または感電の原因になります。

次のような場所では保管、使用をしない
禁止
・直射日光のあたる場所
・高温になる場所
・動作環境範囲外

光源をのぞかない
禁止
光ファイバケーブルの断面、コネクタ、および製品のコネクタ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。

⚠注意

静電気注意
❗
コネクタや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。

コードを持って抜かない
❗
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

振動が発生する場所では使用しない
❗
接触不良や動作不良の原因となります。

付属品の使用は取扱説明書にしたがう
禁止
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。

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。

- 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあけたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。
- 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
  - 電源ケーブル、延長ケーブル、またはプラグが破損した。
  - 製品の中に異物が入った。
  - 製品に水がかかった。
  - 製品が落下した、または損傷を受けた。
  - 操作方法に従って運用しているのに正しく動作しない。
- 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔をふさがないようにしてください。
- 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。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。
- 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。
- 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプがわからない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。
- システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
  - 東日本では 100V/50Hz、西日本では 100V/60Hz
- また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。
- 付属の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、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3 ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグが付いている 3 線式コードを使用してください。
- 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システムコンポーネントを保護するには、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。踏みつけられたりつまず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。
- 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。
- 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ください。
- 製品の移動は気をつけて行ってください。キャスタやスタビライザがしっかり装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

ラック搭載型製品に関する一般的な注意事項

ラックの安定性および安全性に関する以下の注意事項を遵守してください。また、システムおよびラックに付随する、ラック設置マニュアル中の注意事項や手順についてもよくお読みください。

- システムとは、ラックに搭載されるコンポーネントを指しています。コンポーネントはシステムや各種周辺デバイスや付属するハードウェアも含みます。

警告 前面および側面のスタビライザを装着せずに、システムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムを搭載する前には、必ずスタビライザを装着してください。

警告 接地用伝導体を壊したり、接地用伝導体を適切に取り付けないで装置を操作しないでください。適切な接地ができるかわからない場合、電気保安協会または電気工事士にお問い合わせください。

警告 システムのシャーシは、ラックキャビネットのフレームにしっかり接地される必要があります。接地ケーブルを接続してから、システムに電源を接続してください。電源および安全用接地配線が完了したら、資格を持つ電気検査技師が検査する必要があります。安全用接地ケーブルを配線しなかったり、接続されていない場合、エネルギーハザードが起こります。

- ラックにシステム / コンポーネントを搭載した後は、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 つのみとしてください。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。
- ラックに装置を搭載する前に、スタビライザがしっかりとラックに固定されているか、床面まで到達しているか、ラック全体の重量がすべて床にかかるようになっているかをよく確認してください。ラックに搭載する前に、シングルラックには前面および側面のスタビライザを、複数結合型のラックには前面用スタビライザを装着してください。
- ラックへの装置の搭載は、常に下から上へ、また最も重いものから行ってください。
- ラックからコンポーネントを引き出す際には、ラックが水平で、安定しているかどうか確認してから行ってください。
- コンポーネントレール解除ラッチを押して、ラックから、またはラックへコンポーネントをスライドさせる際は、指をスライドレールに挟まないよう、気をつけて行ってください。
- ラックに電源を供給する AC 電源分岐回路に過剰な負荷をかけないでください。ラックの合計負荷が、分岐回路の定格の 80 パーセントを超えないようにしてください。
- ラック内部のコンポーネントに適切な空気流があることを確認してください。
- ラック内の他のシステムを保守する際には、システムやコンポーネントを踏みつけたり、その上に立ったりしないでください。

注意 資格を持つ電気工事士が、DC 電源への接続と接地を行う必要があります。すべての電気配線が、お住まいの地域、および国の電気基準と規制に準拠していることを確認してください。

静電気障害を防止するために

静電気は、システム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、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

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. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネント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してください。
2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。
3. 静電気に敏感なコンポーネントの取り扱いは、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。

バッテリの取り扱いについて

警告 不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

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、および同梱されている製品保証書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。

- 本書および同梱されている製品保証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。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を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。
また、テクニカルサポートご提供のためにはユーザ登録が必要となります。
http://www.dlink-jp.com/

目次

はじめに

xStack DES-3810 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、IP アドレス割り当て、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、IP アドレス、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、TFTP サービス、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 VPN（VPN の設定）
- MPLS、LDP、VPWS などの VPN 機能について説明します。

第 9 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、LLDP などのレイヤ 2 機能について説明します。

第 10 章 L3 Features（レイヤ 3 機能の設定）
- MD5 キー設定、ルート再配送設定、スタティック / ダイナミックルート設定、ルート優先度設定、ポリシールート設定、RIP、OSPF、VRRP、IP マルチキャストルーティングプロトコルなどのレイヤ 3 機能について説明します。

第 11 章 QoS（QoS 機能の設定）
- QoS 機能について説明します。帯域制御、QoS スケジューリング、QoS 送信スケジューリング、802.1p デフォルトプライオリティ、802.1p ユーザプライオリティなどの機能を含みます。

第 12 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）機能について説明します。

第 13 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、IP マルチキャスト範囲の制限、Web 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 14 章 Network Application（ネットワークアプリケーション）
- DHCP サーバ設定、DNS 設定、SNTP、SMTP 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 15 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 16 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、エラー、パケットサイズ、ミラーリング、sFlow、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 17 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と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とその意味について説明します。

付録 E パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減

- ARP プロトコル、ARP スプーフィング攻撃、および D-Link スイッチが提供する ARP スプーフィング攻撃を防御する対策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　本製品のご使用にあたって

xStack DES-3810 シリーズについて

D-Link の DES-3810 シリーズは D-Link xStack® ファミリーの高性能なメンバです。10/100Mbps エッジスイッチからコアのギガビットスイッチまでの広範囲においてご使用いただけます。また、ネットワーク管理者向けに操作性のよい管理インタフェースと共にフォールトトレランス、柔軟性、ポート数、高セキュリティ、および高スループットを提供します。

本スイッチは、PC、ハブ、およびその他のスイッチを含むスイッチに各種ネットワークデバイスをアップリンクさせる 1000BASE-T ポートおよび SFP ポートの組み合わせを搭載し、フルデュプレックスモードのギガビットイーサネットを提供します。SFP（Small Form Factor Pluggable）コンボポートは、長距離伝送のためのギガビットリンクにアップリンクさせるために光ファイバトランシーバを装着することが可能です。

本スイッチにおけるアドバンスド ACL およびユーザ認証機能はコアからエッジまでネットワークセキュリティ適用範囲を拡張します。ユニークな D-Link セーフガードエンジンはワームとウィルスの脅威からスイッチを保護します。その結果、総合的な信頼度、実用性、および可用性を増強します。

本マニュアルでは、DES-3810 シリーズの設置、管理、および設定の方法について記述しています。

サポートする機能

- IEEE 802.3 10BASE-T、IEEE 802.3u 100BASE-TX、IEEE 802.3ab 1000BASE-T、IEEE 802.3z 1000BASE-X 準拠
- IEEE 802.3x Flow Control 準拠
- IEEE 802.3ad Link Aggregation
- IEEE 802.1Q VLAN Tagging、IEEE 802.1v Protocol Based VLAN
- IEEE 802.1D Spanning Tree（STP compatible）、IEEE 802.1w Rapid Spanning Tree、IEEE 802.1s Multiple Spanning Tree
- IEEE 802.1p Class of Service、IEEE 802.1X Port Based Network Access Control
- L2 機能（SI/EI）
  - IGMP スヌーピング：v1/v2/v3、スヌーピンググループ数：1024、スタティックマルチキャストグループ数：128、VLAN 毎の IGMP、IGMP Fast Leave
  - MLD スヌーピング：v1/v2、スヌーピンググループ数：1024、スタティックマルチキャストグループ数：128、VLAN 毎の MLD、MLD Fast Leave
  - スパニングツリー：IEEE 802.1d STP/IEEE 802.11w RSTP/IEEE 802.1s MSTP、ルートガード、BPDU フィルタリング
  - 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-3810-28：14 グループ / デバイス、8 ポート / グループ
    - DES-3810-52：26 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、RSPAN
  - 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）：最大 4 リング
  - ジャンボフレーム：10,240Bytes
- VLAN（SI/EI）
  - IEEE 802.1Q タグ VLAN、ポートベース VLAN、VLAN グループ数：4094（スタティック）/4094（ダイナミック）
  - VLAN ID レンジ：1-4094、IEEE 802.1v プロトコル VLAN、Subnet ベース VLAN
  - MAC ベース VLAN：512 エントリ、GVRP、ダブル VLAN：Port-base Q in Q/Selective Q in Q
  - VLAN トランキング、VLAN トランスレーション、ISM VLAN、Voice VLAN、Private VLAN
- L3 機能

  SI/EI
  - ダイナミックルーティングエントリ（IPv4/IPv6 共有）：最大 7286（IPv4：7286、IPv6：1821）
  - スタティックルーティングエントリ（IPv4/IPv6 共有）：最大 256（IPv4：256、IPv6：128）
  - L3 フォワーディングエントリ（IPv4/IPv6 共有）：最大 3575（IPv4：3575、IPv6：1821）
  - デフォルトルート（IPv4/IPv6）、2nd デフォルトルート、IP インターフェース数：256、VLAN 毎の IP インタフェース数：10
  - RIPv1/v2、OSPFv2、OSPF パッシブインタフェース、ECMP
  - ポリシーベースルーティング、Null インタフェース、ループバックインタフェース、VRRP、プロキシ ARP、Gratuitous ARP、IPv6 トンネリング

  EI のみ
  - RIPng
- マルチキャスト（SI/EI）
  - マルチキャストルーティングテーブル：1024（IPv4）、256（IPv6）
  - I P マルチキャストフィルタリング
  - IGMP：v1/v2/v3、IGMP/MLD Proxy、DVMRP、PIM SM、PIM DM、PIM SSM、PIM Sparse-Dense Mode、マルチキャストデュプリケーション

- MPLS（EI のみ）
  - LDP、VPWS
- QoS（SI/EI）
  - 帯域制御、キュー：8 レベル / ポート
  - キューのスケジューリング：Strict/WRR/Strict+WRR
  - CoS：VLAN ID、IEEE 802.1p プライオリティ、MAC アドレス、IPv4/IPv6 アドレス、DSCP、プロトコルタイプ、Ether 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
  - trTCM/srTCM
- ACL（アクセスコントロールリスト）（SI/EI）
  - Ingress ACL：最大 1024 プロファイル、1024 ルール / デバイス
  - Egress ACL：最大 500 プロファイル、500 ルール / デバイス
  - 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、ToS、DSCP、プロトコルタイプ、TCP/UDP ポート、TCP/UDP ペイロード、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
  - 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：最大 6 プロファイル 、100 ルール / デバイス
- セキュリティ（SI/EI）
  - SSHv2（IPv4/IPv6）、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、Web 認証 ※1 ※2（ 日本語カスタマイズ対応）、
  - Compound 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、
  - Web ベース検疫ソリューション：NOSiDE LAN 検疫 /ROUD Registgate ハードウェア認証 /QSM 認証 /QuOLA、
  - 認証 DB フェイルオーバ：802.1X/MAC/WAC/JWAC/Compound、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（IPv4/IPv6）/IPv6 ND スヌーピングモード
  - ポートセキュリティ：最大 16384MAC/ 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、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

  SI/EI
  - 3 レベルのユーザアカウント権限、LLDP、LLDP-MED、Web ベース GU（I IPv4/IPv6）、CLI、ZMODEM
  - Telnet サーバ（IPv4/IPv6）、Telnet クライアント（IPv4/IPv6）、RCP、SNMPv1/v2c/v3、SNMP over IPv6、
  - SNMP トラップ、PPPoE Circuit-ID、RMONv1：4 グループ、RMONv2：プルーブコンフィググループ、sflow
  - トラストホスト（IPv4/IPv6）、DHCP 自動設定、DHCP/BOOTP クライアント、DHCP リレー：オプション 82/60/61、
  - DHCPv6 リレー、DHCP サーバ、DNS リレー（IPv4/IPv6）、Syslog（IPv4/IPv6）、TFTP クライアント（IPv4/IPv6）、
  - FTP クライアント、SNTP クライアント、SMTP クライアント、フラッシュファイルシステム、
  - show tech-support コマンド、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、
  - 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）、ITU-T Y.1731、NLB：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

  EI
  - Switch Resource Management（SRM）：ルーティングモード /VPWS モード

- 以下の MIB のサポート（SI/EI）
  - MIBII（RFC1213）、Bridge MIB（RFC1493）、SNMP MIB（RFC1157, 2571-2576）、SNMPv2 MIB（RFC 1901-1908, 1442, 2578）
  - RMON MIB（RFC1757, 2819）、RMONv2 MIB（RFC2021）、Ether-like MIB（RFC1398, 1643, 1650, 2358, 2665）
  - IEEE 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）、Private MIB、Ping/Traceroute MIB（RFC2925）、VRRP MIB（RFC2787）、
  - RIPv2 MIB（RFC1724）、OSPF MIB（RFC1850）、IPv4 Multicast Routing MIB（RFC2932）、PIM MIB for IPv4（RFC2934）

※ DES-3810-52 は EI 版のみとなり、すべての機能に対応しています。
※ 1 WAC/JWAC を使う場合は、利用可能な ACL ルール数が減少します。
※ 2 WAC/JWAC を使う場合は、必ず SystemIPIF が有効になっている必要があります。

- スイッチ管理用 RS-232 /RJ-45 コンソールポート
- パラレルポート状態 LED 表示（リンク、アクション、スピード等）
- レート適応およびプロトコル変換に対応するための、非ブロック型ストアアンドフォワードスイッチング機能
- ワイヤスピードでのフォワーディング速度に対応するための自己学習機能およびアドレス認識メカニズム

ポート

DES-3810 シリーズは以下のポートを搭載しています。

型番	DES-3810-28	DES-3810-52
10BASE-T/100BASE-TX ポート	24	48
10BASE-T/100BASE-TX/1000BASE-T ポート	4	-
10BASE-T/100BASE-TX/1000BASE-T コンボポート	-	2
SFP コンボスロット	4	-
SFP スロット	-	4
RJ-45 コンソールポート	1	1
管理ポート	1	1
RPS スロット	1	1

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 スロット / コンボスロット	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）（SFP コンボのみ） • DEM-211（100BASE-FX）（SFP コンボのみ） • DEM-310GT（1000BASE-LX） • DEM-311GT（1000BASE-SX） • DEM-312GT2（1000BASE-SX2） • DEM-314GT（1000BASE-LH） • DEM-315GT（1000BASE-ZX） • DEM-330T/R（WDM） • DEM-331T/R（WDM）	• 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

注意 SFP コンボスロットは、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 のスロット 25 と 1000BASE-T のポート 25）、SFP スロットが優先となり 1000BASE-T ポートは使用不可能となります。

- すべてのスイッチは 1 つの RJ-45 コンソールポートを実装しています（スイッチを PC に接続するために DB9 インタフェースを持つ特別なコンソールケーブルを提供します）。

- すべてのスイッチはそれぞれ 1 つの管理ポートを搭載しています。このポートは管理用の目的で利用され、Telnet、WebUI、SNMP での管理に利用されます。

- すべてのスイッチはオプションの外部 RPS 用の Redundant Power Supply（RPS）アウトレットを 1 つ搭載しています。

前面パネル

DES-3810-28

前面パネルには、10BASE-T/100BASE-TX ポート、10BASE-T/100BASE-TX/1000BASE-T コンボポート、SFP コンボスロット、管理ポート、および RJ-45 コンソールポートが配置されています。また、電源、コンソール、RPS（冗長電源システム）、およびオプションモジュール用の SFP スロットを含む各ポートの Link/Act/Speed 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。

- 10BASE-T/100BASE-TX ポート x 24
- 1000BASE-T/SFP コンボスロット x 4
- RJ-45 コンソールポート x 1
- 管理ポート x 1
- LED : Power、Console、RPM、Link/Act/Speed（各ポート）
- スタックモジュール番号 LED

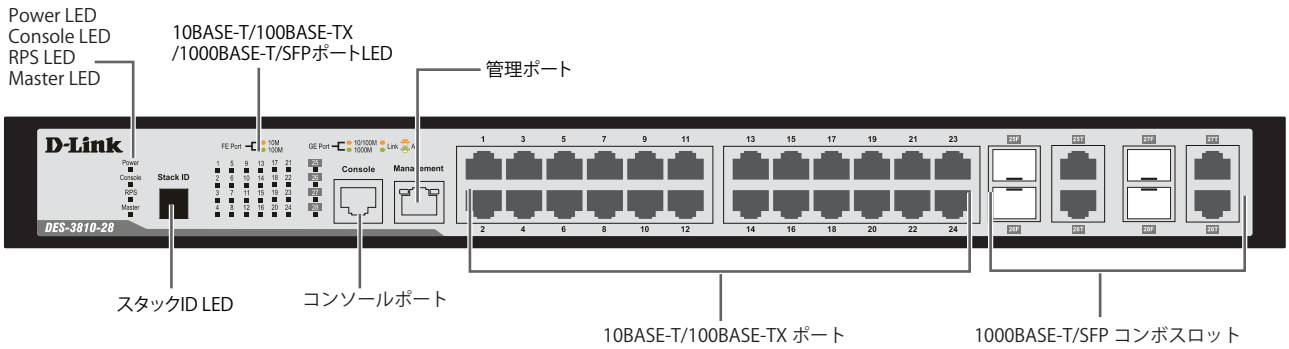


図 3-1　DES-3810-28 前面パネル

DES-3810-52

前面パネルには、10BASE-T/100BASE-TX ポート、および SFP スロットなどが配置されています。また、電源、コンソール、RPS（冗長電源システム）、およびオプションモジュール用の SFP スロットを含む各ポートの Link/Act/Speed 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。

- 10BASE-T/100BASE-TX ポート x 48
- 10BASE-T/100BASE-TX/1000BASE-T コンボスロット ×2
- SFP スロット× 4
- LED : Power、Console、RPM、Link/Act/Speed（各ポート）
- スタックモジュール番号 LED

注意　10BASE-T/100BASE-TX/1000BASE-T コンボポート、RJ-45 コンソールポート、管理ポートは背面に配置されています。

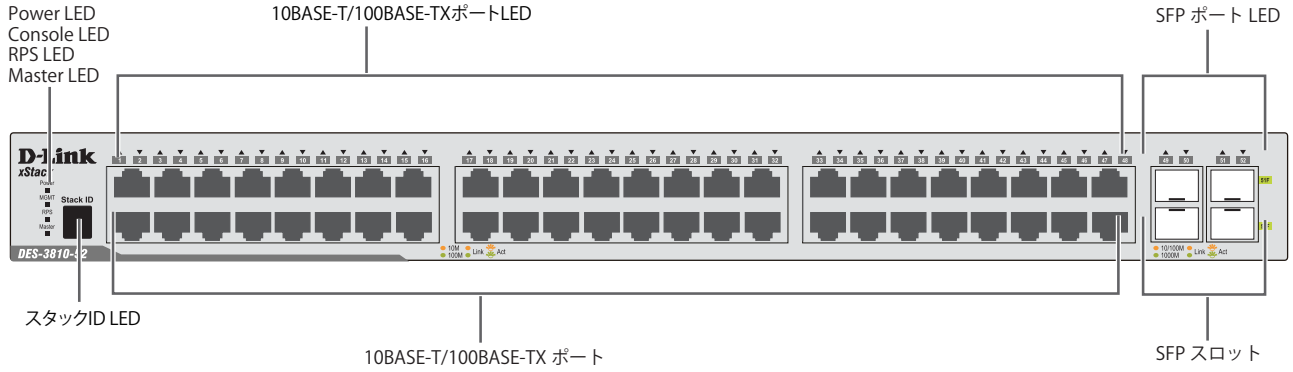


図 3-2　DES-3810-52 前面パネル

LED 表示

LED はスイッチとネットワークの状態を表示します。Power、Console、RPS、Master および各ポートについて LED をサポートします。以下に、スイッチ上の LED の配置と、各 LED の状態が表す意味を示します。

DES-3810-28

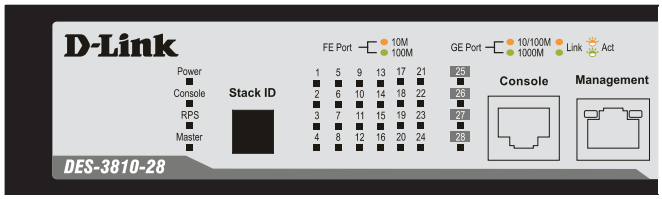


図 3-3　DES-3810-28 の前面パネル LED 配置図

DES-3810-52

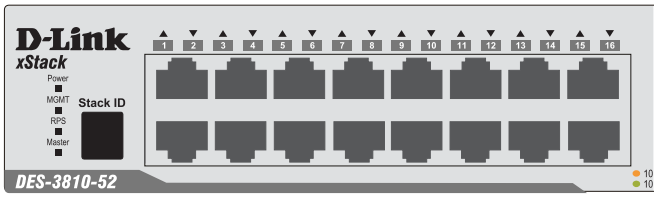


図 3-4　DES-3810-52 の前面パネル LED 配置図

以下の表に LED の状態が意味するスイッチの状態を示します。

LED	色	状態	状態説明
Power	緑	点灯	スイッチに電源が供給され正常に動作しています。
	ー	消灯	スイッチに電源が供給されていません。
Console	緑	点滅	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。
RPS	橙	点灯	電源投入後の Power ON Self Test（POST）中に点灯し、終了すると消灯します。 または、内蔵電源ユニットの異常により、拡張のリダンダント電源ユニットが動作しています。
	ー	消灯	リダンダント電源ユニットは動作していません。
Master ※スタックはサポートされていません	緑	点灯	スイッチはスタックマスタです。
	ー	消灯	スイッチはスタックマスタではありません。
スタック ID ※スタックはサポートされていません	緑	番号表示	スイッチスタックにおけるスイッチのボックス番号。スタンドアロンモードのスイッチでは、本フィールドは 1 です。スイッチがスイッチスタックのマスタである場合、スタック内のスイッチの番号が表示されます。「H」の文字はこの番号の代わりに点灯します。
FE ポート	緑	点灯	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。
	橙	点灯	10Mbps でリンクが確立しています。
		点滅	10Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
コンボポート	1000BASE-T/SFP ポートそれぞれに LED が配置されています。		
GE	緑	点灯	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。
	橙	点灯	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。
	ー	消灯	リンクが確立していません。
MGMT ポート	緑	左の LED 点灯	10/100Mbps でリンクが確立しています。
		右の LED 点滅	10/100Mbps でデータを送受信しています。
	ー	消灯	リンクまたはアクティビティがありません。

背面パネル

スイッチの背面パネルには、AC 電源コネクタ、オプションの外部リダンダント電源用のコネクタが配備されています。また、DES-3810-52 では 10BASE-T/100BASE-TX/1000BASE-T ポート、管理ポート、コンソールポートが配備されています。

DES-3810-28

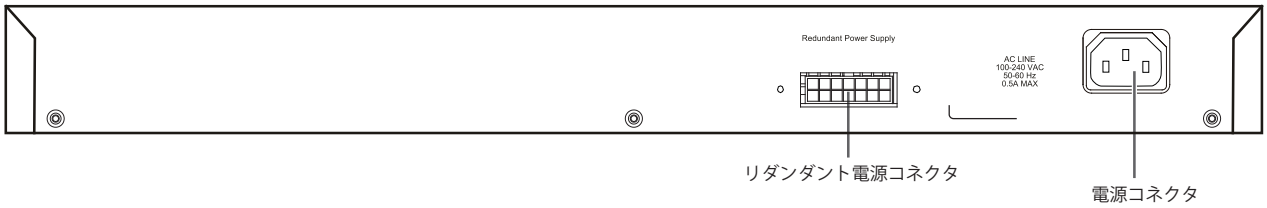


図 3-5　DES-3810-28 の背面パネル図

DES-3810-52

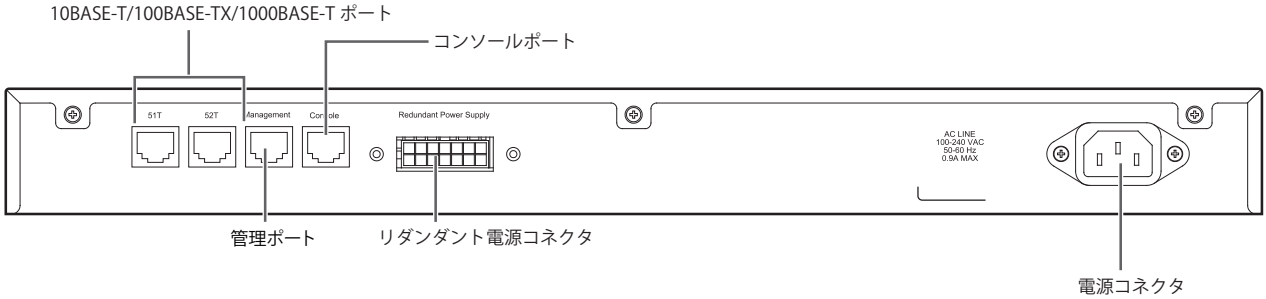


図 3-6　DES-3810-28 の背面パネル図

背面パネルにはオプションのリダンダント電源ユニット用のアウトレットがあります。内蔵電源ユニットに異常が発生した場合に外部リダンダント電源ユニット (オプション) が自動的にスイッチに電源を供給します。AC 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

システムのファンと通気口がスイッチ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-3810-28

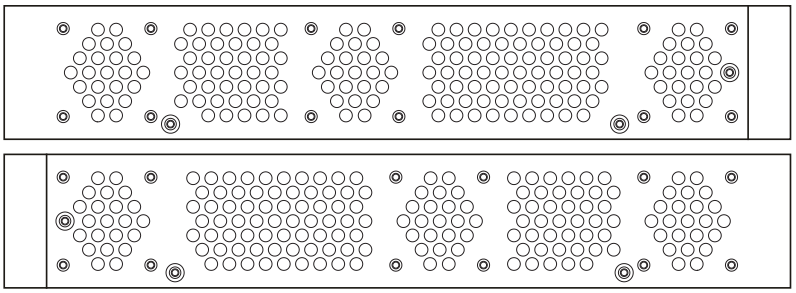


図 3-7　DES-3810-28 の側面パネル図

DES-3810-52

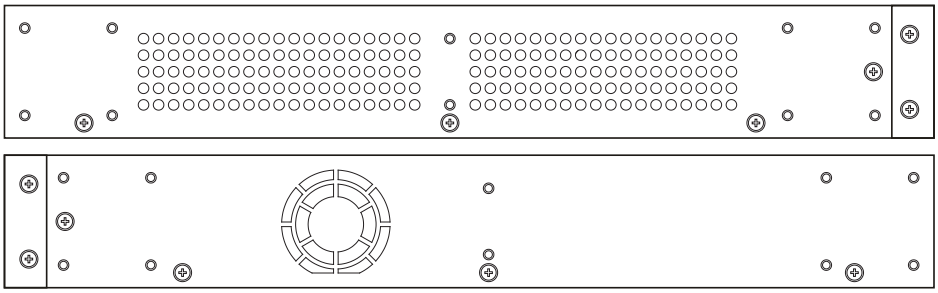


図 3-8　DES-3810-52 の側面パネル図

ギガビットコンボポート

スイッチは、スイッチの前面パネルに 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。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 2 つ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。

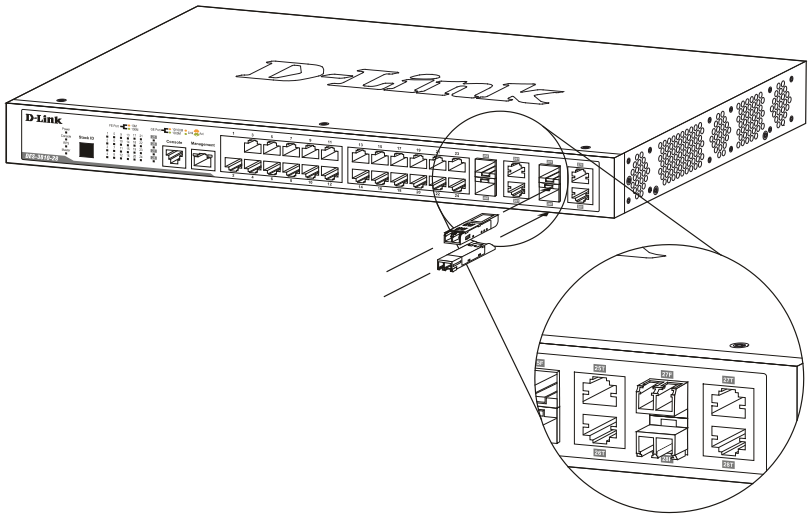


図 3-9　　前面パネルの SFP ポート

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
- AC 電源ケーブル　x　1
- RS-232C/RJ-45 コンソールケーブル　x　1
- 電源抜け防止金具（DES-3810-52 のみ）
- 19 インチラックマウントキット　x　1
- マニュアル　x　1
- シリアルラベル　x　1
- 製品保証書　x　1
- CD-ROM　x　1
- ゴム足 (貼り付けタイプ)　x　4
- CD-ROM

万一、不足しているもの損傷を受けているものがありましたら、交換のために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。また、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。

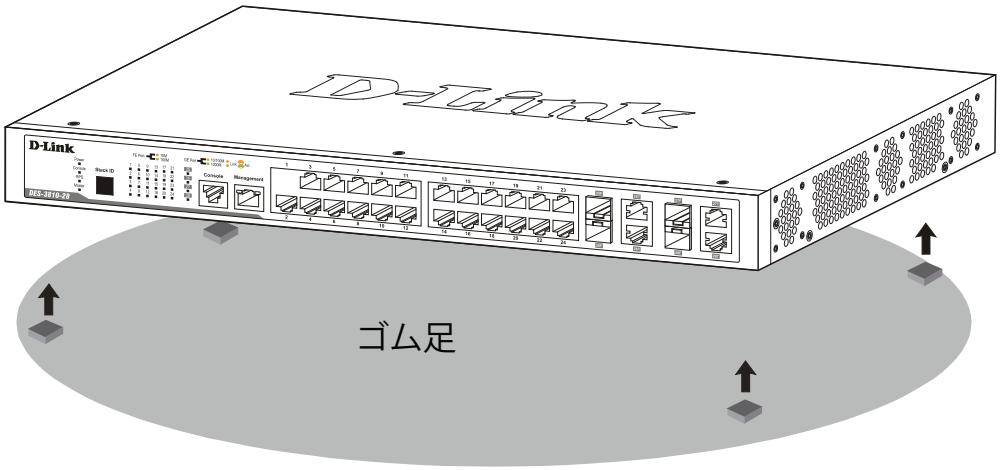


図 2-1　机や棚の上に設置する場合の準備

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。

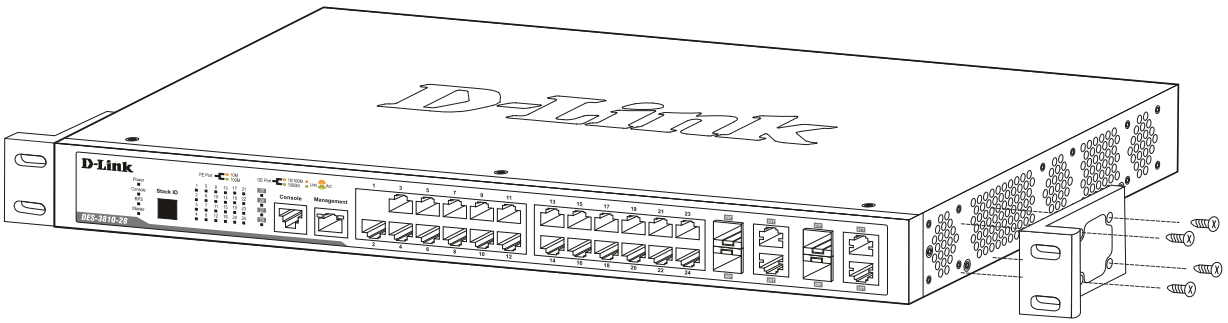


図 2-2　スイッチへのブラケットの取り付け図

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。

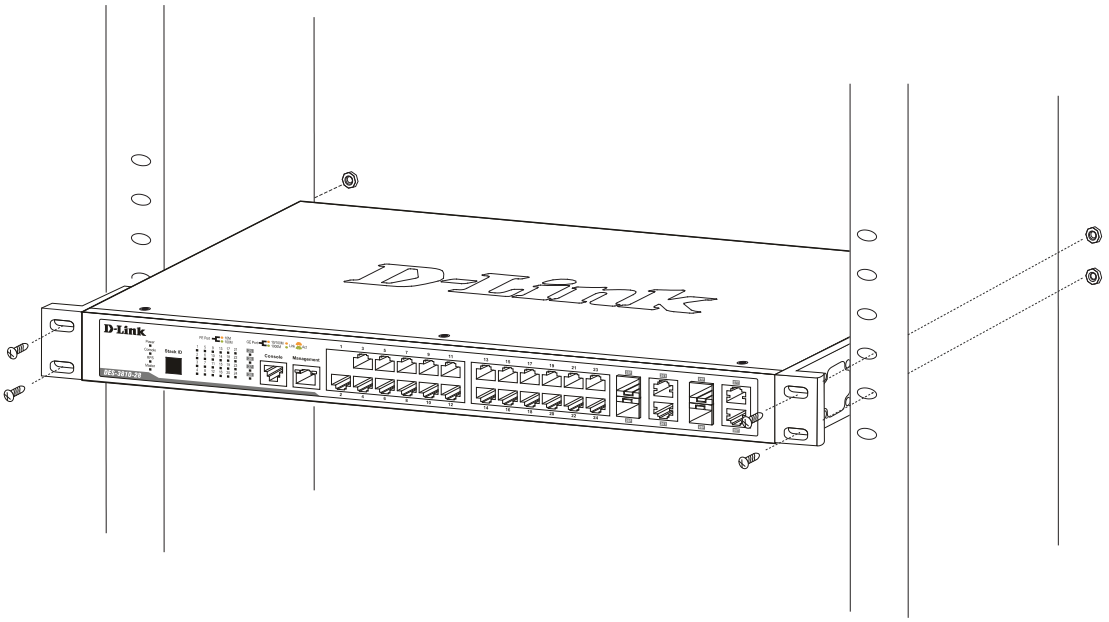


図 2-3　スイッチのラックへの設置図

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ます。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 が点灯します。システムのリセット中、LED は点滅します。

警告 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。

リダンダント電源システムの設置

リダンダント電源システムをスイッチに取り付けるためには、以下の手順を実行します。DPS-200 は、スイッチに必要な電力を供給するリダンダント電源ユニットです。DPS-200 は DPS-900 または DPS-800 に取り付けることができます。

警告 DPS-200 の設置を行う前に、スイッチの AC 電源ケーブルを抜いておいてください。

警告 フロントおよびサイドのスタビライザを装着せずにシステムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムの搭載を行う前には、必ずスタビライザを装着してください。ラックにシステム / コンポーネントを搭載した後は、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 つのみとしてください。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。

リダンダント電源システムの接続

DPS-200 のマスタスイッチへの接続は、14 ピンの DC 電源ケーブルを使用して行います。標準の三極の AC 電源ケーブルでリダンダント電源装置とメイン電源を接続します。

注意 さらに詳細な情報については DPS-200 のマニュアルをご参照ください。

警告 本スイッチを DPS-200 以外のリダンダント電源ユニット使用しないでください。

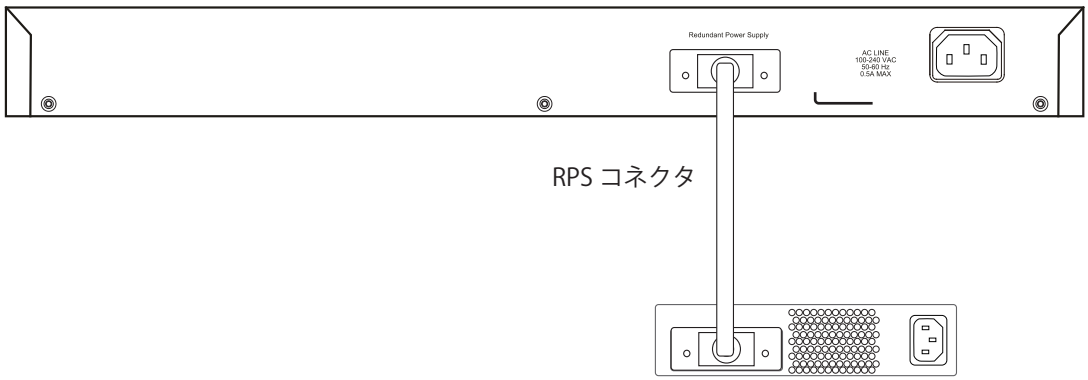


図 2-4　DES-3810-28 と DPS-200 RPS の接続

1. 14 ピン DC 電源ケーブルの一端をスイッチのソケットに挿入し、もう一端をリダンダント電源装置に挿入します。
2. 標準の AC 電源ケーブルでリダンダント電源装置とメインの AC 電源を接続します。DPS-200 の前面の緑の LED 点灯により、正しく接続が行われたことが確認できます。
3. スイッチを再び AC 電源に接続します。RPS LED が点灯してリダンダント電源が動作していることを確認できます。
4. 本手順の実行による設定変更は必要ありません。

外部リダンダント電源システムへの接続

DPS-900

DPS-900 は標準サイズのラックマウント（5U サイズ）です。8 台までの DPS-200 を収容できます。

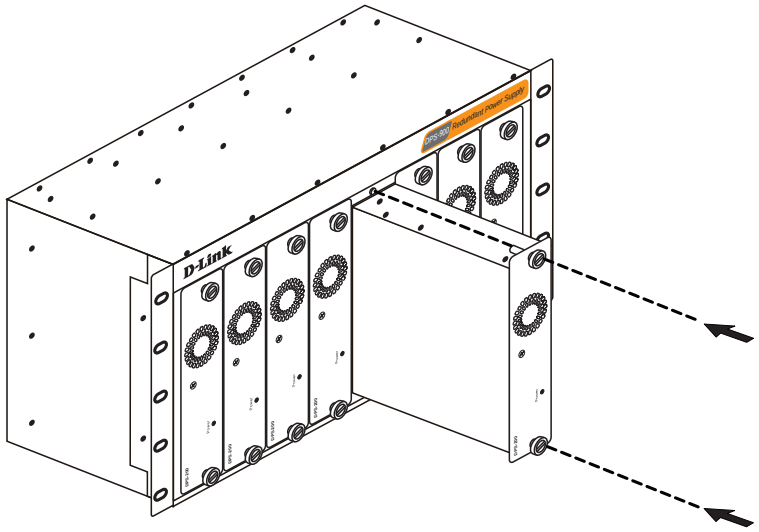


図 2-5　DPS-200 を DPS-900 に取り付ける

リダンダント電源は、標準 19 インチラックにも取り付けることができます。以下の図を参照してください。

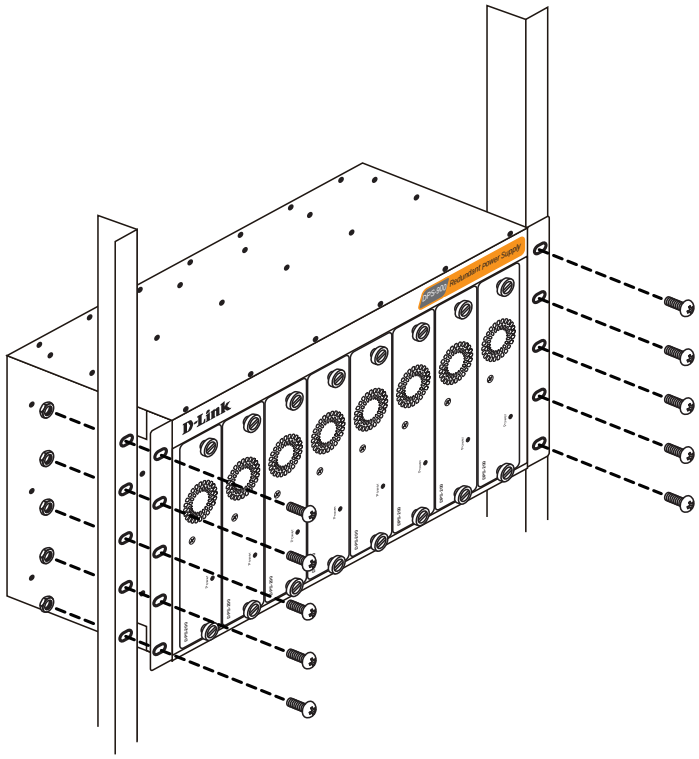


図 2-6　DPS-900 をラックに取り付ける

DPS-800

DPS-800 は標準サイズのラックマウント（1.5U サイズ）です。2 台までの DPS-200 を収容できます。

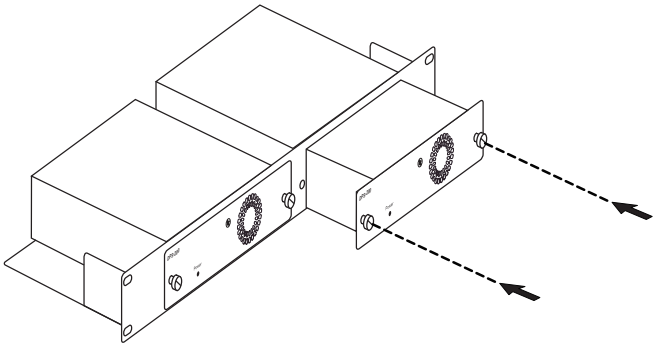


図 2-7　DPS-200 を DPS-800 に取り付ける

RPS は標準 19 インチラックにも取り付けることができます。以下の図を参照してください。

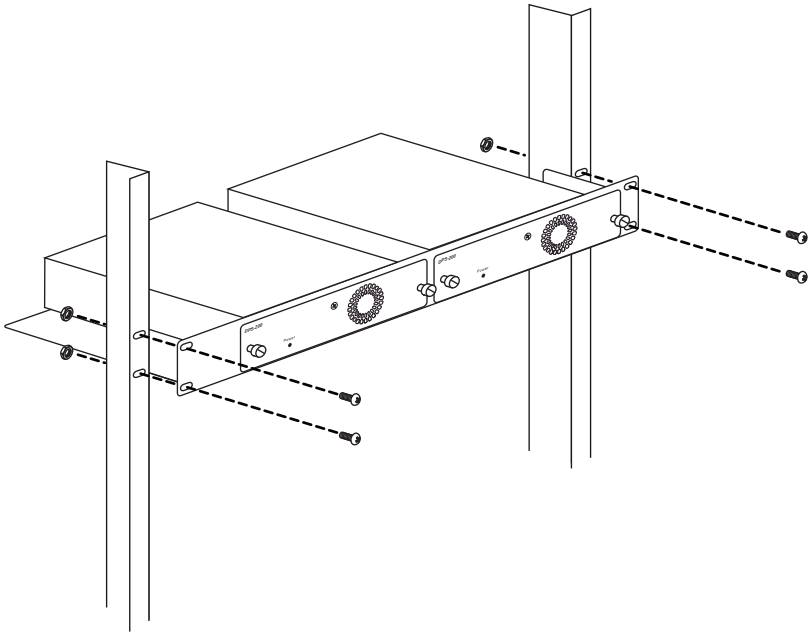


図 2-8　DPS-800 をラックに取り付ける

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 1000BASE-T ポートとエンドノードをカテゴリ 3、4、5 の UTP/STP 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 10/100/1000Mbps 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。

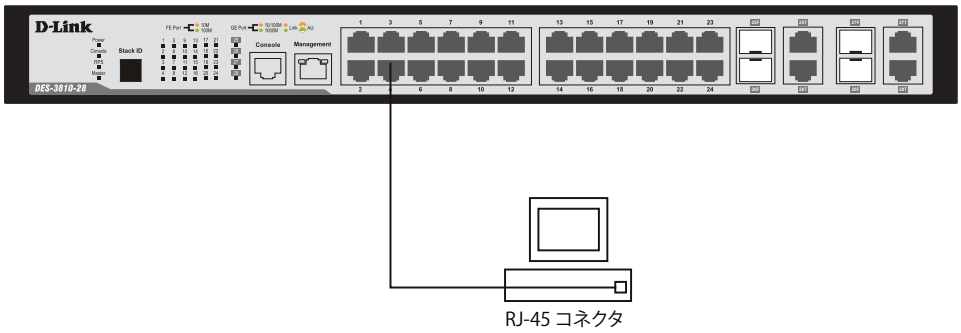


図 3-1　エンドノードと接続した図

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 Link/Act 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 : 本スイッチの SFP ポートと光ファイバアップリンクサポートのスイッチを接続する。

ケーブル仕様については「付録 A ケーブルとコネクタ」（476 ページ）を参照してください。

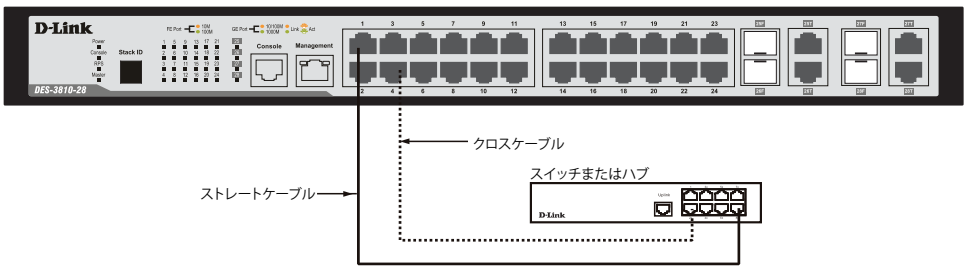


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

2 つの 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 100Mbps または 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。

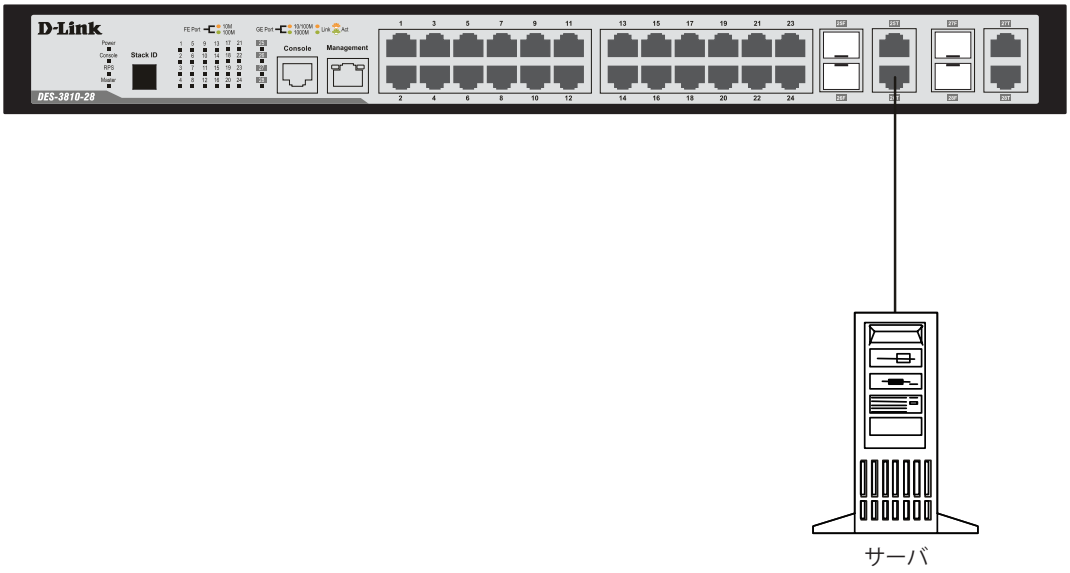


図 3-3　サーバ、PC、スイッチスタックとのアップリンク接続図

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、Microsoft® Internet Explorer（バージョン 6.0 以上）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 v1.0、v2.0、および v3.0 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。

- コンソールポートの接続（RS-232 DCE）
  スイッチのモニタリングと設定のために RS-232C シリアルポート（RJ-45 コネクタ）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 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-3810 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、以下のように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。

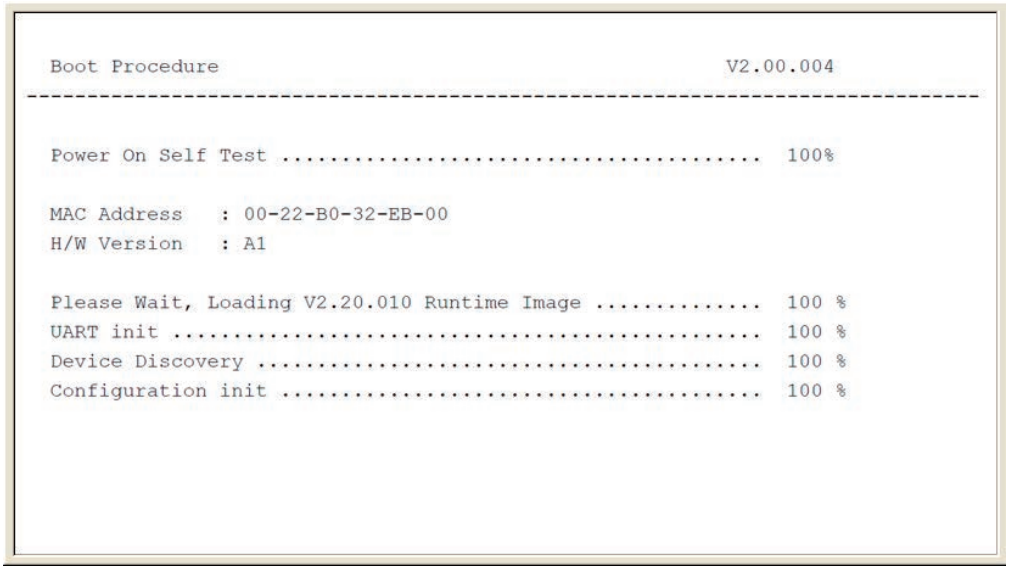


図 4-1　コンソールのブート画面

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。

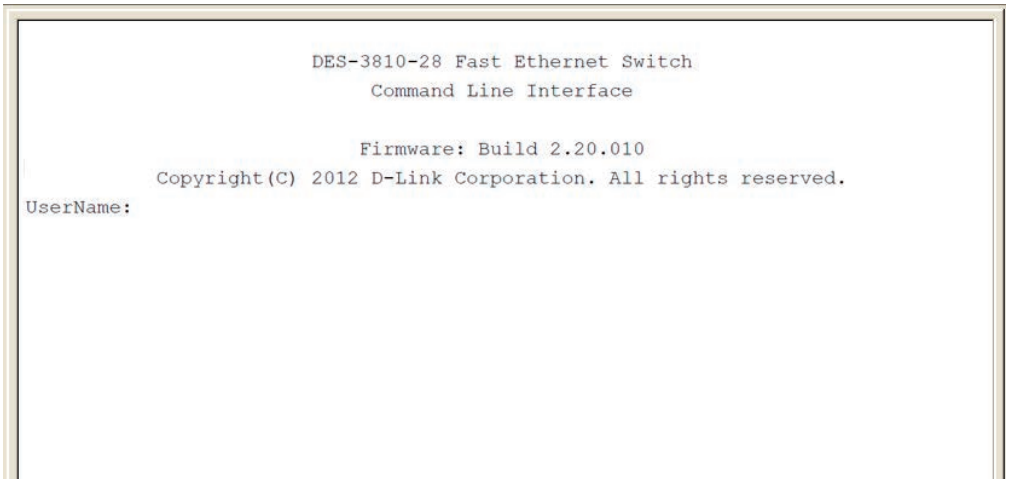


図 4-2　コマンドプロンプト

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-3810-28: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。

管理ポートへの接続

スイッチの前面パネルには Out-of-Band（帯域外）管理ポートがあります。ポートは、標準的なイーサネットケーブルを使用してノート PC に簡単に接続可能な RJ-45 ポートです。Web ブラウザまたは Telnet コマンドプロンプトインタフェースを使用して、Out-of-Band 管理を行うポートに接続します。管理ポートは初期値で有効であるため、初めてスイッチに接続するために使用することができます。

管理ポートを使用するためには、イーサネットケーブルを使用してスイッチ管理に使用するコンピュータのイーサネットインタフェースにポートを接続します。IP アドレスの初期値は 192.168.0.1 で、サブネットマスクは 255.255.255.0 です。スイッチ管理に使用するコンピュータが、192.168.0.x サブネットで重複しない IP アドレスを持っていることを確認してください。

コンソールポート、または Web ベースのスイッチ管理インタフェースを通じて IP 設定または管理ポートのステータスを変更することができます。管理ポートの設定を変更するためには、以下のコマンドを使用します。:

```
config out_band_ipif {ipaddress <network_address> | state [enable | disable] | gateway <ipaddr>}
```

IP 設定のステータスを参照するためには、以下のコマンドを使用します。

```
show out_band_ipif
```

Web インタフェースにおける Out-of-Band 管理ポートの設定を変更するためには、**Management > Out of Band Management Settings** メニューを使用します。

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-3810-28:admin#create account admin newmanager
Command: create account admin newmanager

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

DES-3810-28:admin#
```

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。

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-3810-28:admin#show switch
Command: show switch

Device Type        : DES-3810-28 Fast Ethernet Switch
MAC Address        : 34-08-04-4A-DC-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 2.00.004
Firmware Version   : Build 2.20.010
Hardware Version   : A1
Firmware Type      : SI
Serial Number      : PVN71B3000039
System Name        :
System Location    :
System Uptime      : 0 days, 1 hours, 9 minutes, 58 seconds
System Contact     :
Spanning Tree      : Disabled
GVRP               : Disabled
IGMP Snooping      : Disabled
MLD Snooping       : Disabled
RIP                : Disabled
DVMRP              : Disabled
PIM                : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

図 4-3　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-3810-28:admin#config ipif System ipaddress 10.24.22.100/255.0.0.0
Command: config ipif System ipaddress 10.24.22.100/8

Success.

DES-3810-28:admin#
```

図 4-4　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「10.24.22.100」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（10.24.22.100/8）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。

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 66 ページの「System IP Address Settings（システム IP アドレス設定）」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。

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://123.123.123.123（123.123.123.123 はスイッチの IP アドレス。）

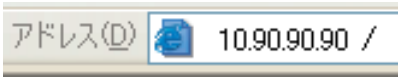


図 5-1　URL の入力

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。

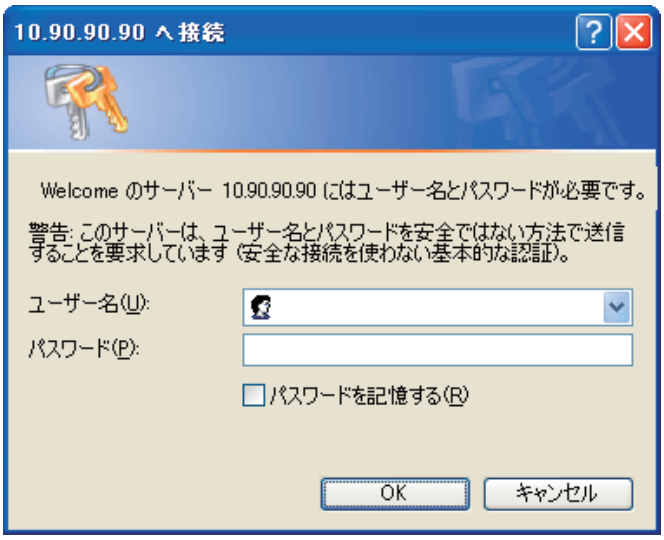


図 5-2　パスワード入力用画面

「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。

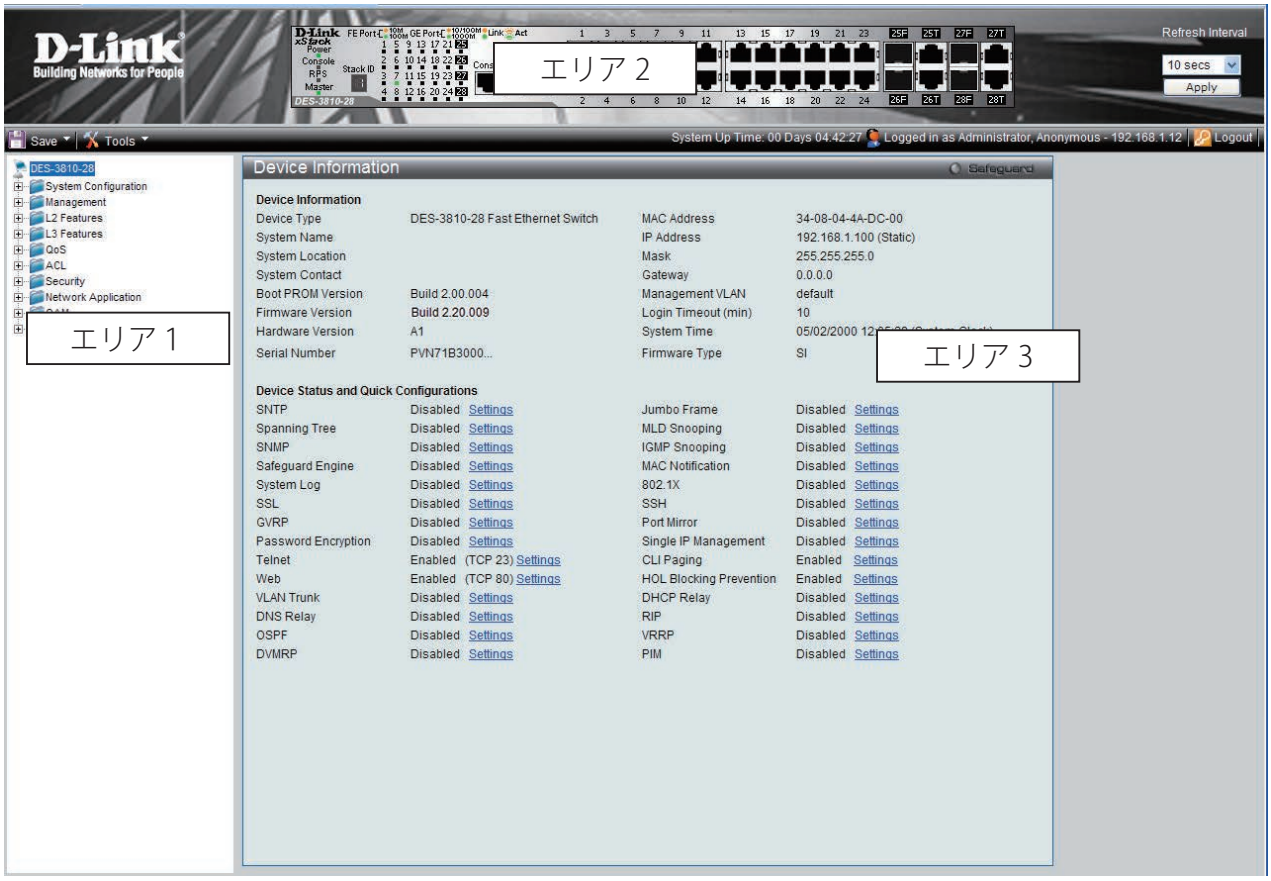


図 5-3　Web マネージャのメインページ

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の表示と設定データの入力を行えます。

注意　スイッチ設定を変更した場合、以下で説明する Web ブラウザの「Save」メニュー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
System Configuration	Device Information	スイッチの主な設定情報を表示します。
	System Information Settings	スイッチの基本情報を表示します。
	Port Configuration	ポート設定、ジャンボフレーム設定などを行います。次のメニューがあります。: DDM、Port Settings、Port Description Settings、Port Error Disabled、Jumbo Frame Settings
	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。
	Warning Temperature Settings	システムの警告温度パラメータを設定します。
	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。次のメニューがあります。: System Log Settings、System Log Server Settings、System Log、System Log & Trap Settings、System Severity Settings
	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。
	Time Settings	スイッチに時刻を設定します。
	User Accounts Settings	ユーザおよびユーザの権限を設定します。
	SRM	スイッチリソース管理モードを設定します。
Management	ARP	スタティック ARP、プロキシ 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、Proxy ARP Settings、ARP Table
	Gratuitous ARP	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 Settings
	IPv6 Neighbor Settings	IPv6 Neighbor の設定を行います。
	IP Interface	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、Interface Settings、Loopback Interface Settings
	Management Settings	CLI ページング、DHCP 自動設定、省電力モードなどの管理設定を行います。
	Out of Band Management Settings	RJ-45 のアウトバンド管理の詳細を設定します。
	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。
	Single IP Management	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、Topology、Firmware Upgrade、Configuration File Backup/ Restore、Upload Log File
	SNMP Settings	SNMP 設定を行います。次のメニューがあります。: SNMP Global Settings、SNMP Trap Settings、SNMP Linkchange 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
	Telnet Settings	スイッチに Telnet 設定をします。
	Web Settings	スイッチに Web ステータスを設定します。
	Power Saving	スイッチに省電力設定を行います。次のメニューがあります。: LED State Settings、Power Saving Settings、Power Saving LED Setting、Power Saving Port Settings
VPN	MPLS	マルチプロトコルスイッチングの設定を行います。次のメニューがあります。: LDP、MPLS Settings、MPLS Static LSP Settings、MPLS Dynamic LSP Table、MPLS FTN Table、MPLS Interface Settings、MPLS Class Map Settings、MPLS FEC EXP Settings
	VPWS	仮想専用線サービスの設定を行います。次のメニューがあります。: VPWS Settings
L2 Features	VLAN	VLAN 設定を行います。次のメニューがあります。: 802.1Q VLAN Settings、802.1v Protocol VLAN、GVRP、MAC-based VLAN Settings、Private VLAN Settings、PVID Auto Assign Settings、Subnet VLAN、VLAN Counter Settings、Voice VLAN、VLAN Trunk Settings、Browse VLAN、Show VLAN Ports
	QinQ	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、VLAN Translation Settings、Double Tagged VLAN Translation Settings、VLAN Translation Port Mapping Settings、VLAN Translation Profile List

メインメニュー	サブメニュー	説明
L2 Features	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。
	Spanning Tree	スパニングツリープロトコルの設定を行います。次のメニューがあります。: STP Bridge Global Settings、STP Port Settings、MST Configuration Identification、STP Instance Settings、MSTP Port Information
	Link Aggregation	ポートトランキング設定を行います。次のメニューがあります。: Port Trunking Settings 、LACP Port Settings
	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。次のメニューがあります。: Static FDB Settings、MAC Notification Settings、MAC Address Aging Time Settings、MAC Address Table、ARP & FDB Table
	L2 Multicast Control	IGMP プロキシ、MLD プロキシ、IGMP Snooping、MLD Snooping の設定を行います。次のメニューがあります。: IGMP Proxy、IGMP Snooping、MLD Proxy、MLD Snooping、Multicast VLAN、IP Multicast VLAN Replication
	Multicast Filtering	マルチキャストフィルタリングの設定を行います。次のメニューがあります。: IPv4 Multicast Filtering、IPv6 Multicast Filtering、Multicast Filtering Mode
	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。
	Local Loopback Port Settings	ローカルループバックポートのパラメータを設定します。
	LLDP	LLDP 設定を行います。次のメニューがあります。: LLDP、LLDP-MED
	NLB FDB Settings	NLB 機能を設定します。
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。
	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。
	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。
	IPv6 Route Table	IPv6 ルーティングテーブルの外部経路情報を参照します。
	Policy Route Settings	ポリシールート機能を設定します。
	IP Forwarding Table	直接接続するすべての IP 情報を参照します。
	IP Multicast Forwarding Table	直接接続するすべての IP マルチキャスト情報を参照します。
	IP Multicast Interface Table	直接接続するすべての IP マルチキャストインタフェース 情報を参照します。
	Route Preference Settings	ルート優先度の設定を行います。
	ECMP Algorithm Settings	ECMP OSPF の 状態を設定します。
	Route Redistribution Settings	OSPF または RIP が動作するネットワーク上のルータに OSPF と RIP 間のルーティング情報を再配送する設定を行います。
	IP Tunnel	IP トンネルを設定します。次のメニューがあります。: IP Tunnel Settings、IP Tunnel GRE Settings
	OSPF	OSFP の設定を行います。次のメニューがあります。: OSPFv2
	RIP	RIP の設定を行います。次のメニューがあります。 : RIP Settings、RIPng
	IP Multicast Routing Protocol	IP マルチキャスティング設定を行います。次のメニューがあります。: IGMP、DVMRP、PIM
	VRRP	VRRP リレーの設定を行います。次のメニューがあります。: VRRP Global Settings、VRRP Virtual Router Settings、VRRP Authentication Settings
	MD5 Key Settings	MD キーを登録します。
QoS	802.1p Settings	ポート単位にプライオリティを割り当てます。次のメニューがあります。: 802.1p Default Priority Settings、802.1p User Priority Settings
	Bandwidth Control	送信と受信のデータレートを制限します。次のメニューがあります。: Bandwidth Control Settings、Queue Bandwidth Control Settings
	Traffic Control	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。
	DSCP	DSCP を設定します。次のメニューがあります。: DSCP Trust Settings、DSCP Map Settings
	HOL Blocking Prevention	HOL ブロッキング防止機能を有効または無効にします。
	Scheduling Settings	QoS スケジューリングを設定します。次のメニューがあります。: Scheduling Profile Settings、Scheduling Group Settings

メインメニュー	サブメニュー	説明
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。
	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。
	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。
	ACL Finder	ACL エントリを検索します。
	ACL Flow Meter	フローごとの帯域幅制御設定を行います。
	Egress Access Profile List	フローごとのパケット処理を実行します
	Egress ACL Flow Meter	Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。
Security	802.1X	802.1X 認証を設定します。次のメニューがあります。: 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)
	RADIUS	RADIUS サーバの設定を行います。次のメニューがあります。: Authentication RADIUS Server Settings、RADIUS Accounting Setting、RADIUS Authentication、RADIUS Account Client
	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。次のメニューがあります。: IMPB Global Settings、IMPB Port Settings、IMPB Entry Settings、MAC Block List、DHCP Snooping、ND Snooping
	MAC Based Access Control	MAC アドレス認証機能を設定します。次のメニューがあります。: MAC-based Access Control Settings、MAC-based Access Control Local Settings、MAC-based Access Control Authentication State
	Web-based Access Control (WAC)	Web ベースアクセスコントロールを設定します。次のメニューがあります。: WAC Global Settings、WAC User Settings、WAC Port Settings、WAC Authentication State
	Japanese Web-based Access Control	JWAC の有効化および設定をします。次のメニューがあります。: JWAC Global Settings、JWAC Port Settings、JWAC User Settings、JWAC Authentication State、JWAC Customize Page Language、JWAC Customize Page
	Compound Authentication	コンパウンド認証方式を設定します。次のメニューがあります。: Compound Authentication Settings、Compound Authentication Guest VLAN Settings
	Port Security	ダイナミックな MAC アドレス学習をロックします。次のメニューがあります。: Port Security Settings、Port Security VLAN Settings、Port Security Entries
	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。
	BPDU Attack Protection	ポートに BPDU 防止機能を設定します。
	Loopback Detection Settings	ループバック検知機能の設定を行います。
	Traffic Segmentation Settings	ポートのトラフィックフローを制限します
	NetBIOS Filtering Setting	NetBIOS フィルタ設定を行います。
	DHCP Server Screening	不正な DHCP サーバへのアクセスを拒否します。次のメニューがあります。: DHCP Server Screening Port Settings、DHCP Offer Permit Entry Settings
	Access Authentication Control	TACACS/XTACACS/TACACS+/RADIUS 認証の設定を行います。次のメニューがあります。: 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
	SSL Settings	証明書の設定、暗号スイートの設定を行います。
	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。次のメニューがあります。: SSH Settings、SSH Authentication Method and Algorithm Settings、SSH User Authentication List
	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。
	Safeguard Engine Settings	セーフガードエンジンの設定を行います。

メインメニュー	サブメニュー	説明
Network Application	DHCP	DHCP の設定を行います。次のメニューがあります。: DHCP Relay、DHCP Server、DHCP Local Relay Settings、DHCPv6 Relay
	DNS	DNS リレーの設定を行います。次のメニューがあります。: DNS Relay
	PPPoE Circuit ID Insertion Settings	受信した PPPoE Discovery および Request パケットへの Circuit ID タグの挿入および削除を行います。
	RCP Server Settings	RCP サーバの設定を行います。
	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。
	SNTP Settings	本製品に時刻設定をします。次のメニューがあります。: SNTP Settings、Time Zone Settings
	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。
OAM	CFM	CFM 機能を設定します。次のメニューがあります。: CFM Settings、CFM Port Settings、CFM MIPCCM Table、CFM Loopback Settings、CFM Linktrace Settings、CFM Packet Counter、CFM Fault Table、CFM MP Table
	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。次のメニューがあります。: Ethernet OAM Settings、Ethernet OAM Configuration Settings、Ethernet OAM Event Log、Ethernet OAM Statistics
	DULD Settings	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。
	Cable Diagnostics	ケーブル診断を行います。
Monitoring	Utilization	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、DRAM & Flash Utilization、Port Utilization
	Statistics	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、Packet Size、VLAN Counter Statistics、Historical Counter & Utilization
	Mirror	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、RSPAN Settings
	sFlow	sFlow 機能の設定を行います。次のメニューがあります。: sFlow Global Settings、sFlow Analyzer Server Settings、sFlow Flow Sampler Settings、sFlow Counter Poller Settings
	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。
	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。
	Device Environment	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。

第 6 章　System Configuration（スイッチの主な設定）

以下は、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。	41
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。	43
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。 DDM（DDM 設定）、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 Settings（ジャンボフレームの有効化）	44
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。	51
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。	51
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）	52
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。	56
Time Settings（時刻設定）	スイッチに時刻を設定します。	56
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。	57
SRM（スイッチリソース管理設定）	スイッチリソース管理モードを設定します。	58

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-3810-xx」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（EI モード）

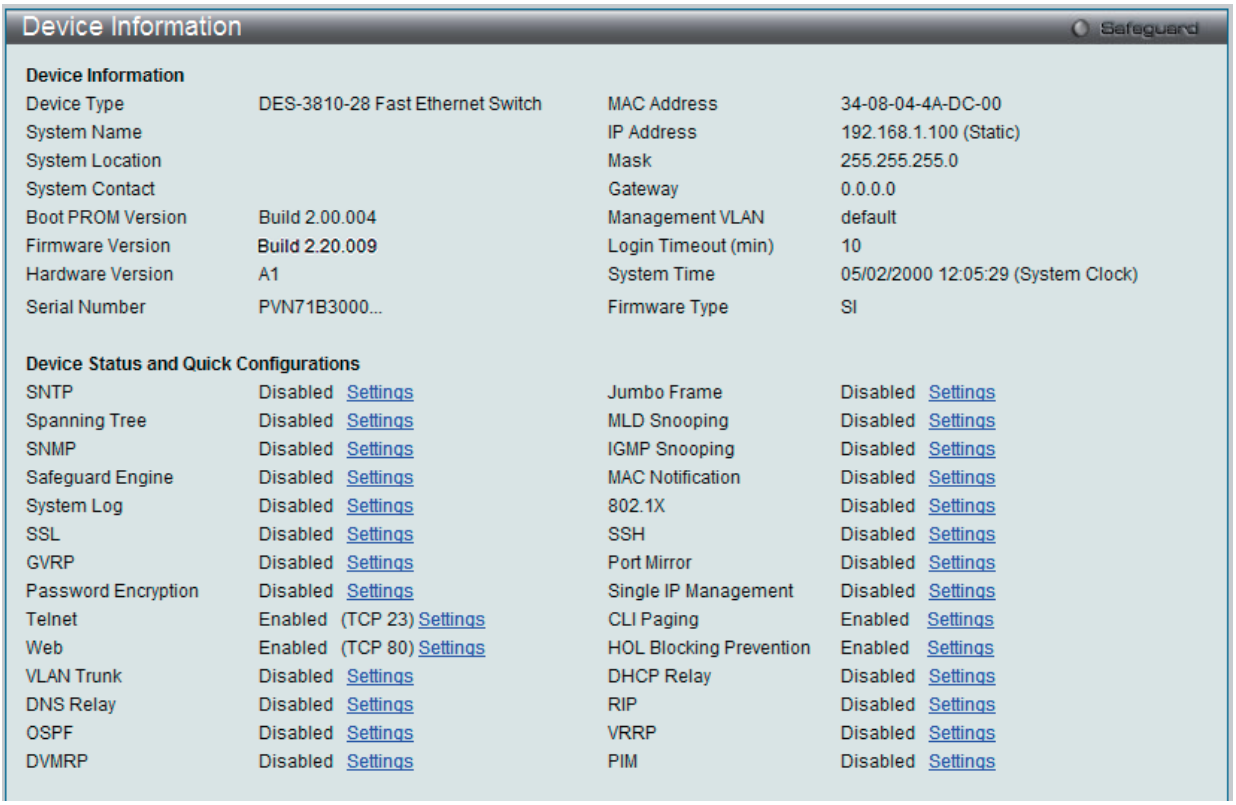


図 6-2　Device Information 画面（SI モード）

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。
Serial Number	デバイスのシリアル番号を表示します。
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 (Minutes)	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
Firmware Type	ファームウェアのタイプ（EI または SI）を表示します。
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。
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。

項目	説明
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。
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。
DNS Relay	DNS リレー機能を有効 / 無効にします。DNS リレーの設定にリンクします。
OSPF	OSPF 機能を有効 / 無効にします。OSPF の設定にリンクします。
DVMRP	DVMRP 機能を有効 / 無効にします。DVMRP の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。
HOL Blocking Prevention	HOL ブロッキング防止機能を有効または無効にします。HOL ブロッキング防止機能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。
RIP	RIP 機能を有効または無効にします。RIP 機能の設定にリンクします。
VRRP	VRRP 機能を有効または無効にします。VRRP 機能の設定にリンクします。
PIM	PIM 機能を有効 / 無効にします。PIM 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。

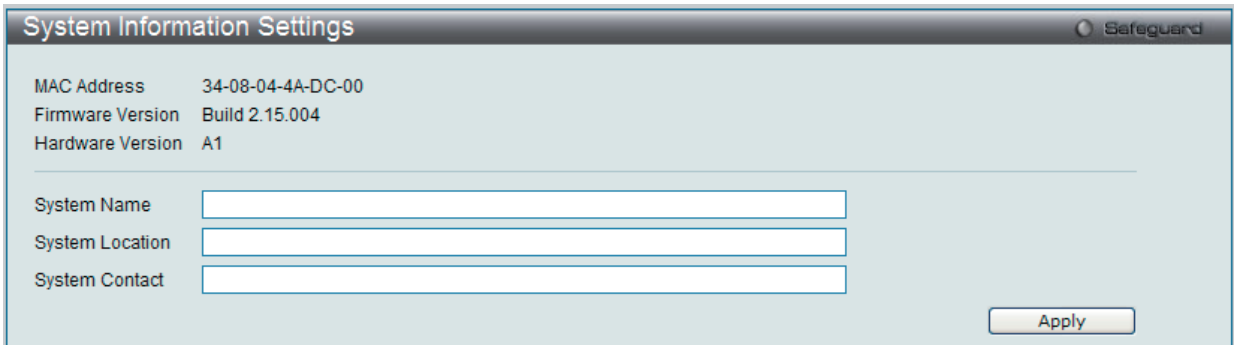


図 6-3　System Information 画面

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）

DDM（DDM 設定）

DDM Settings（DDM 設定）

SFP ポートの状態を設定します。

System Configuration > Port Configuration > DDM > DDM 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。

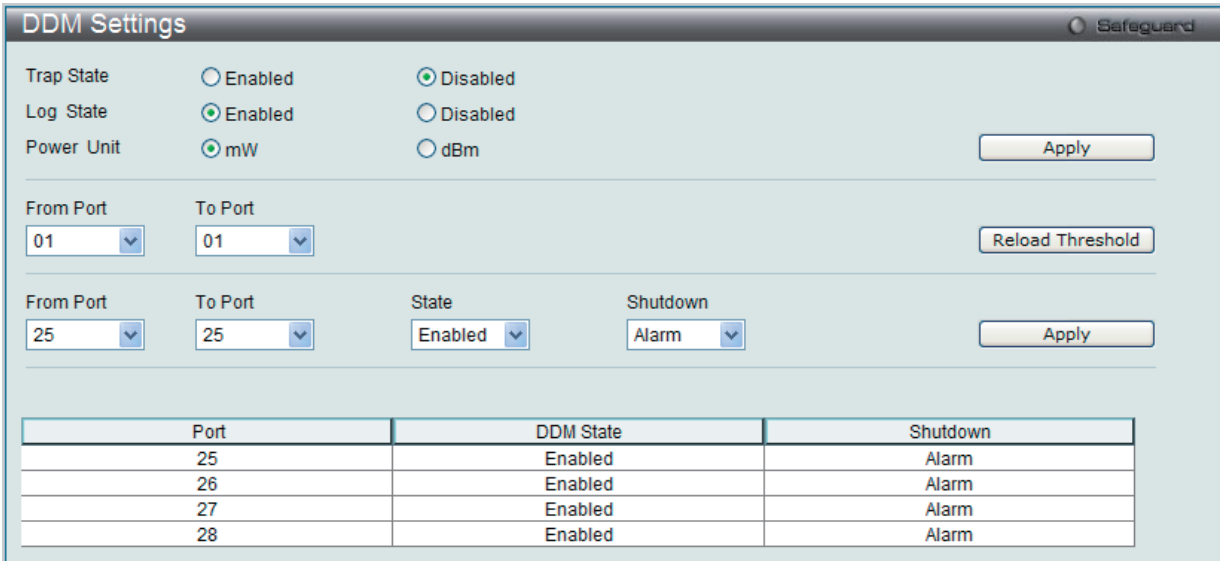


図 6-4　DDM Settings 画面

以下の項目を使用して設定します。

項目	説明
Trap State	SFP ポートにおけるトラップを「Enabled」（有効）/「Disabled」（無効）にします。
Log State	SFP ポートにおけるログ出力を「Enabled」（有効）/「Disabled」（無効）にします。
Power Unit	電力値の単位（mW または dBm）を選択します。
From / To Port	適用するポートまたはポート範囲を指定し、「Reload Threshold」ボタンをクリックして、しきい値をリロードします。
From / To Port	「State」および「Shutdown」パラメータを適用するポートまたはポート範囲を指定します。
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。
Shutdown	シャットダウンした場合の通知をアクション（Alarm、Warning、None）を選択します。

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。

DDM Temperature Threshold Settings（DDM 温度しきい値設定）

SFP ポートの温度しきい値を設定します。

System Configuration > Port Configuration > DDM > DDM Temperature Threshold 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。

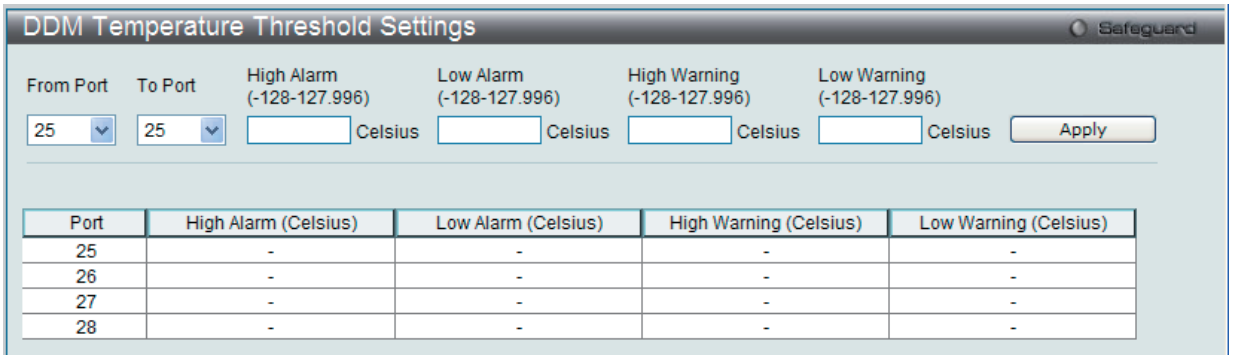


図 6-5　DDM Temperature Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm	注意温度の上限を指定します。
Low Alarm	注意温度の下限を指定します。
High Warning	警告温度の上限を指定します。
Low Warning	警告温度の下限を指定します。

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。

DDM Voltage Threshold Settings（DDM 電圧しきい値設定）

SFP ポートの電圧しきい値を設定します。

System Configuration > Port Configuration > DDM > DDM Voltage Threshold 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。

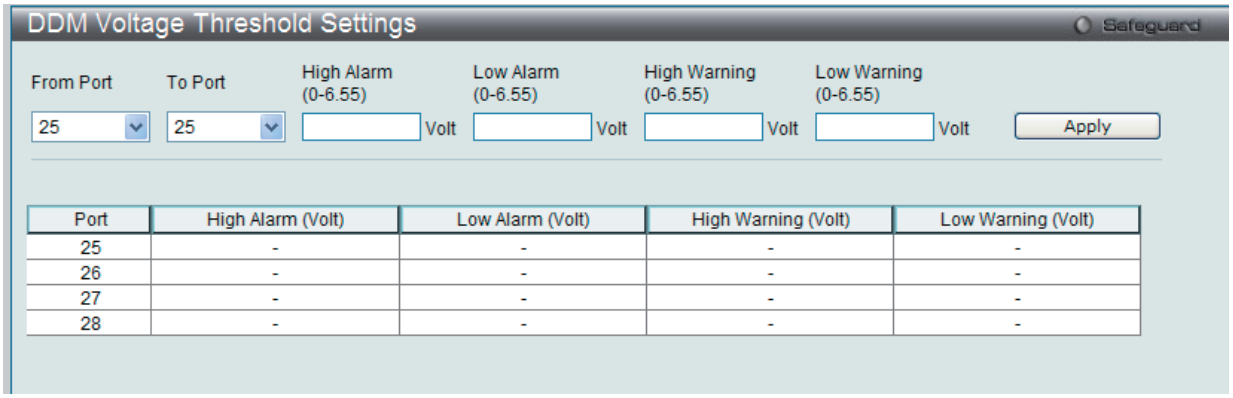


図 6-6　DDM Voltage Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm	注意電圧の上限を指定します。
Low Alarm	注意電圧の下限を指定します。
High Warning	警告電圧の上限を指定します。
Low Warning	警告電圧の下限を指定します。

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。

DDM Bias Current Threshold Settings（DDM バイアス電流しきい値設定）

SFP ポートのバイアス電流しきい値を設定します。

System Configuration > Port Configuration > DDM > DDM Bias Current Threshold 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。

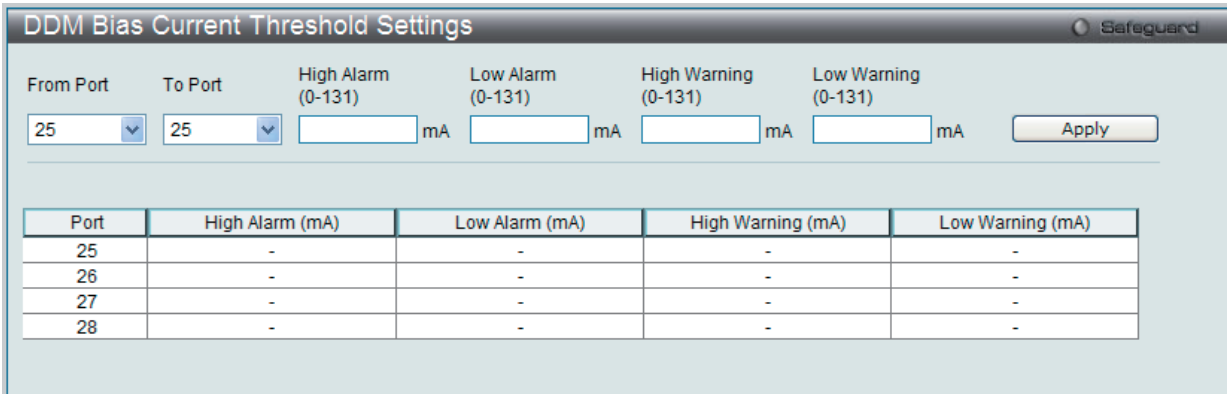


図 6-7　DDM Bias Current Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm	注意電流の上限を指定します。
Low Alarm	注意電流の下限を指定します。
High Warning	警告電流の上限を指定します。
Low Warning	警告電流の下限を指定します。

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。

DDM TX Power Threshold Settings（DDM 送信電力しきい値設定）

SFP ポートの送信電力しきい値を設定します。

System Configuration > Port Configuration > DDM > DDM TX Power Threshold 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。

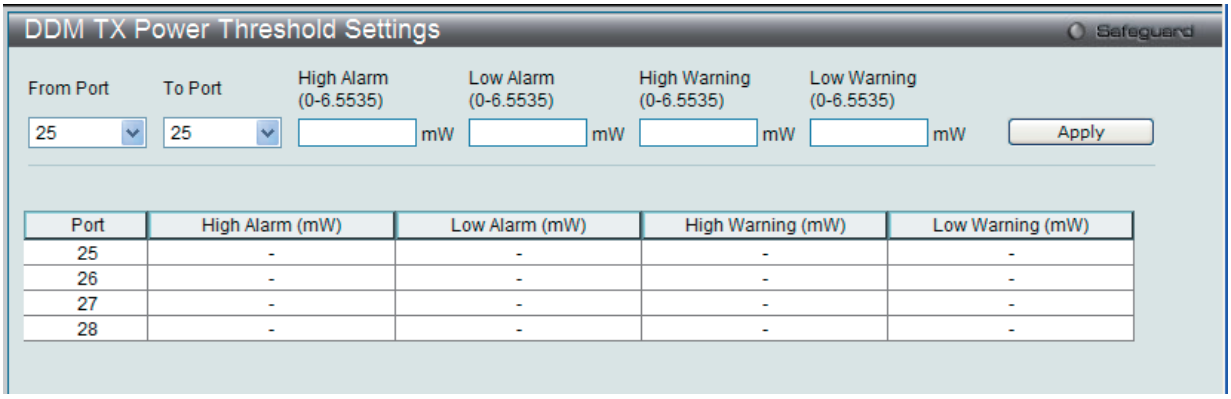


図 6-8　DDM TX Power Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm	注意送信電力の上限を指定します。
Low Alarm	注意送信電力の下限を指定します。
High Warning	警告送信電力の上限を指定します。
Low Warning	警告送信電力の下限を指定します。

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。

DDM RX Power Threshold Settings（DDM 受信電力しきい値設定）

SFP ポートの受信電力しきい値を設定します。

System Configuration > Port Configuration > DDM > DDM RX Power Threshold 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。

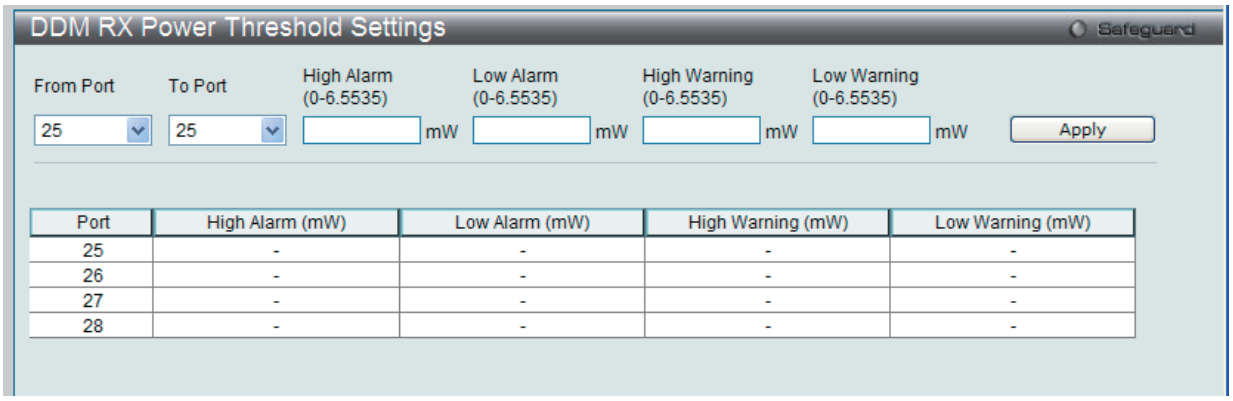


図 6-9　DDM RX Power Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm	注意受信電力の上限を指定します。
Low Alarm	注意受信電力の下限を指定します。
High Warning	警告受信電力の上限を指定します。
Low Warning	警告受信電力の下限を指定します。

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。

DDM Status Table（DDM ステータステーブル）

SFP ポートの状態を表示します。

System Configuration > Port Configuration > DDM > DDM Status 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。

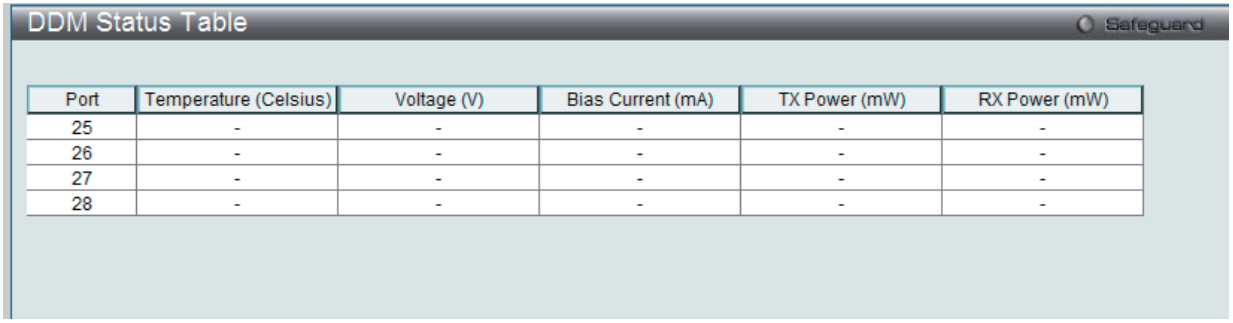


図 6-10　DDM Status Table 画面

以下の項目を使用して設定します。

項目	説明
Temperature	ポートの現在の温度を表示します。
Voltage	ポートの現在の電圧を表示します。
Bias Current	ポートの現在のバイアス電流を表示します。
TX Power	ポートの現在の送信電力を表示します。
RX Power	ポートの現在の受信電力を表示します。

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。

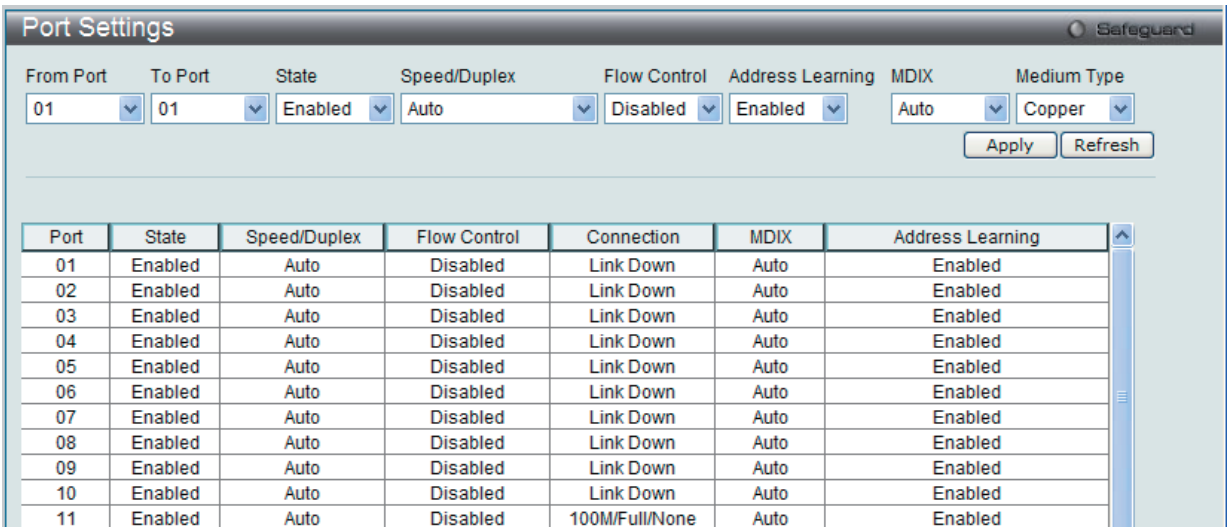


図 6-11　Port Settings 画面

「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
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」、「1000M Full_Slave」、および「1000M Full」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 3 つのタイプ (1000M Full_Master、1000M Full_Slave および 1000M Full) 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長を持っています。 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。それ以外の設定をすると両ポートともリンクダウンします。
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。
Connection	現在の接続スピードが表示されます。
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 - 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。
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、153 ページの「FDB (FDB 設定)」を参照してください。初期値は「Enabled」です。
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。

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。

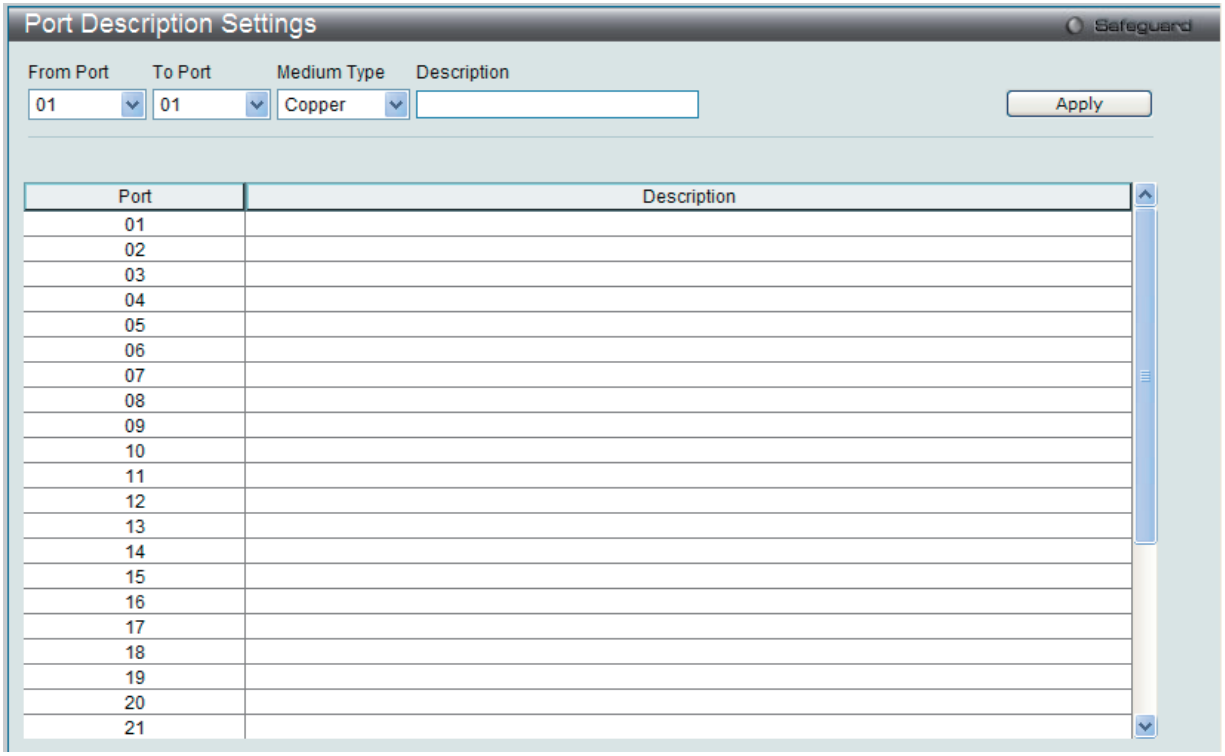


図 6-12　Port Description Settings 画面

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）

以下の画面では、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、接続状態が自動的にスイッチによって無効とされたポートに関する情報を表示します。

この画面を参照するためには、**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。

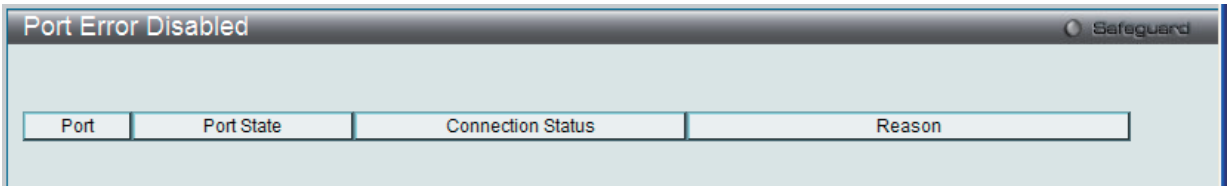


図 6-13　Port Error Disabled 画面

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 10240 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 > Jumbo Frame Settings の順にクリックし、以下の画面を表示します。

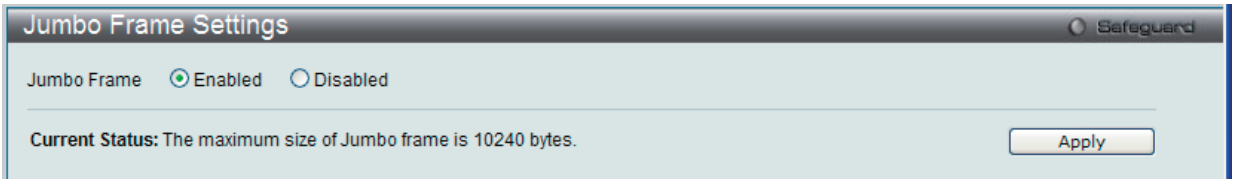


図 6-14　Jumbo Frame 画面

本画面には次の項目があります。

項目	説明
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。 • 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。

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。

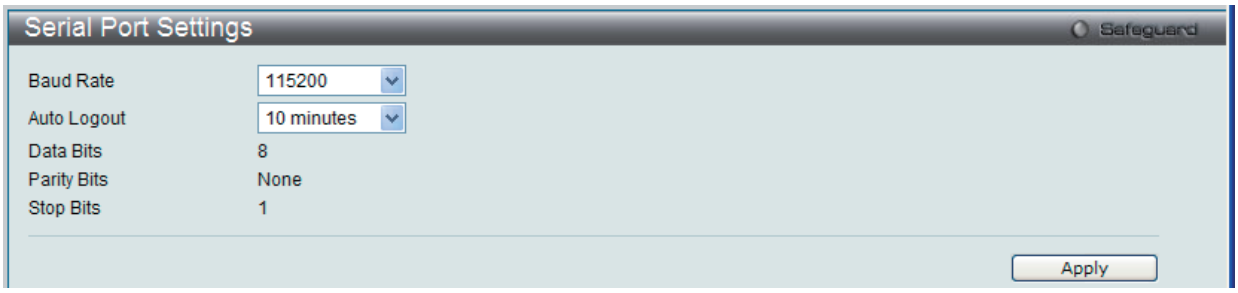


図 6-15　Serial Port Settings 画面

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。

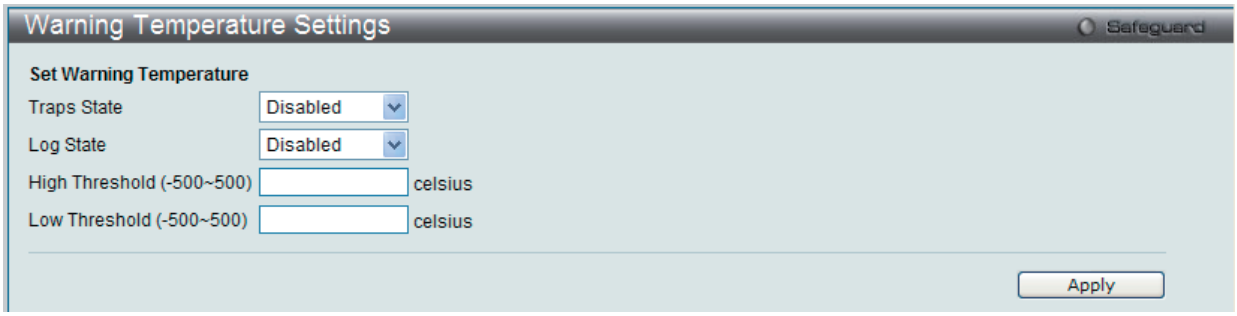


図 6-16　Warning Temperature Settings 画面

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。

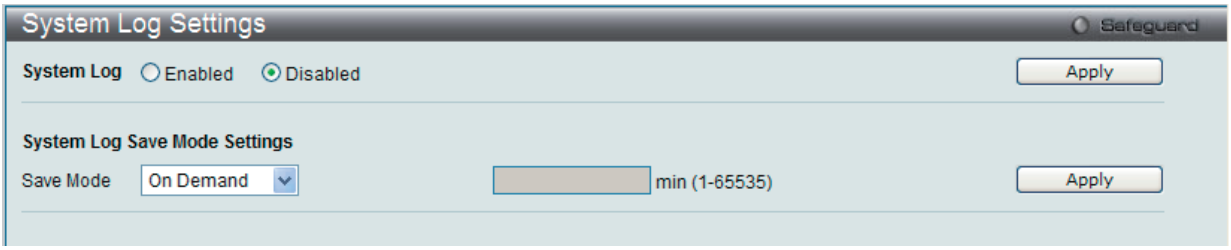


図 6-17　System Log Settings 画面

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 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。

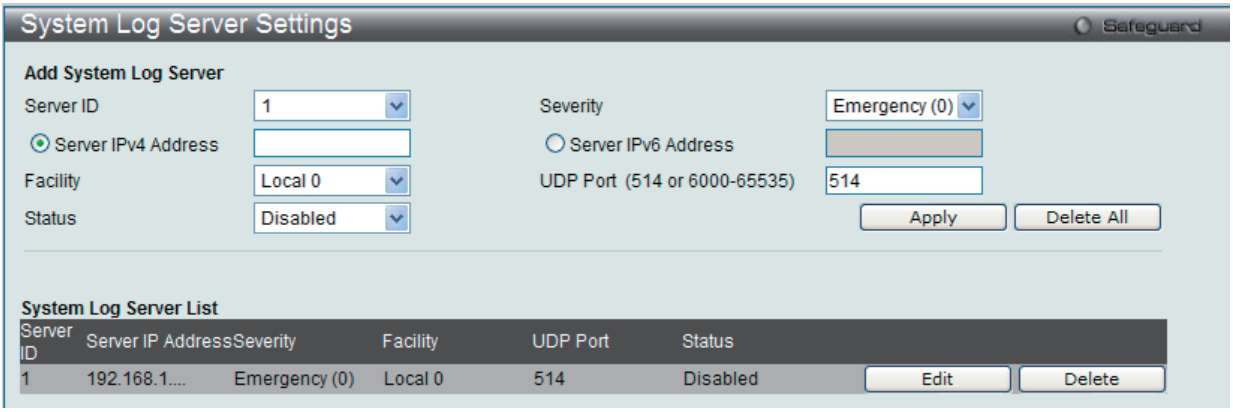


図 6-18　System Log Server Settings 画面

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、Alert、Critical、Error、Warning、Notice、Informational および Debug 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。
Server IPv6 Address	ログを記録するサーバの IPv6 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)	ログを送信するサーバの 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以下の画面を表示します。

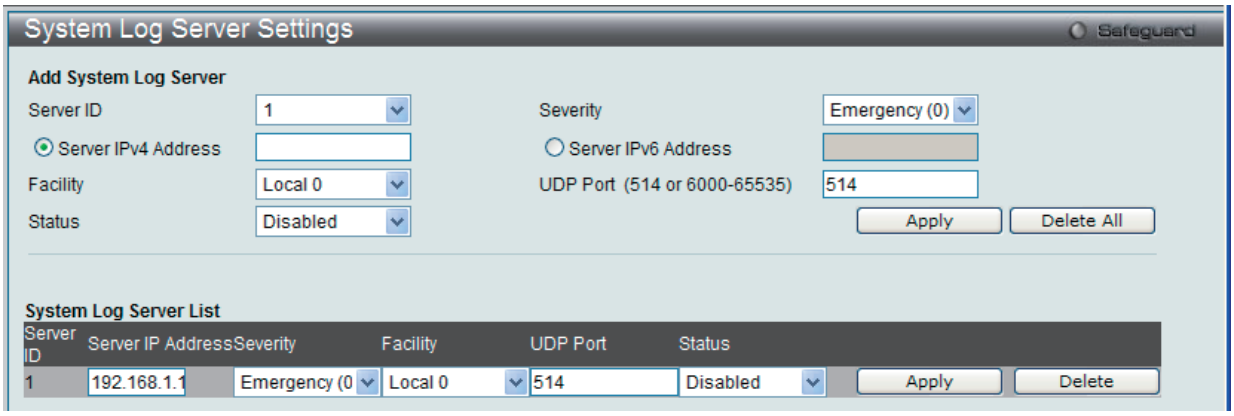


図 6-19　System Log Server Settings 画面 - Edit

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。

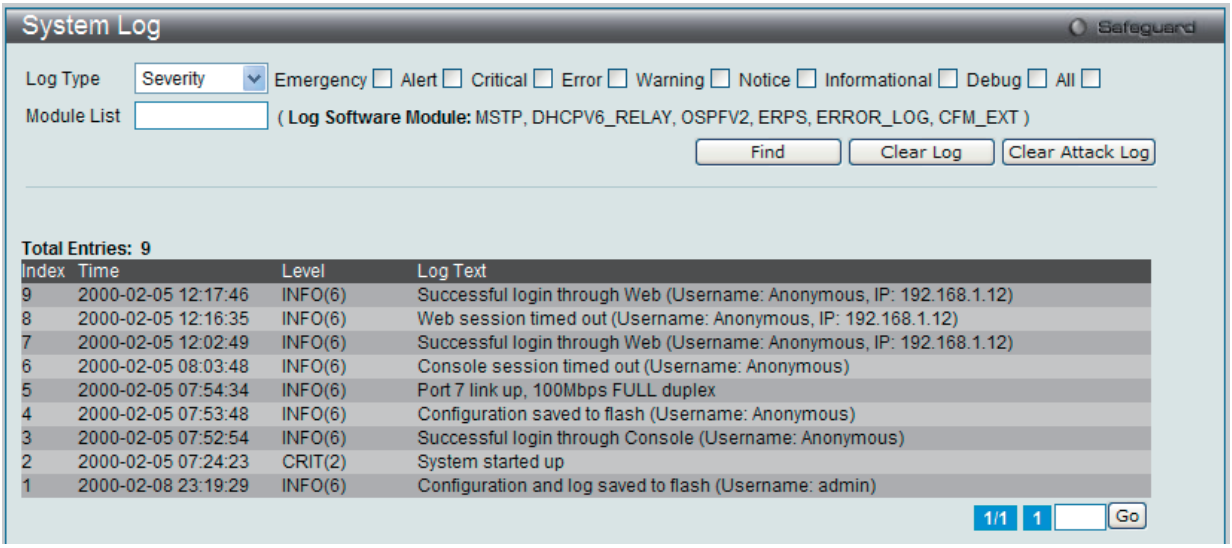


図 6-20　System Log 画面

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 -「Severity」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。 • Module List -「Module List」を選択する場合、MSTP または ERPS のように手動でモジュール名を入力する必要があります。 • Attack Log -「Attack Log」を選択する場合、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。

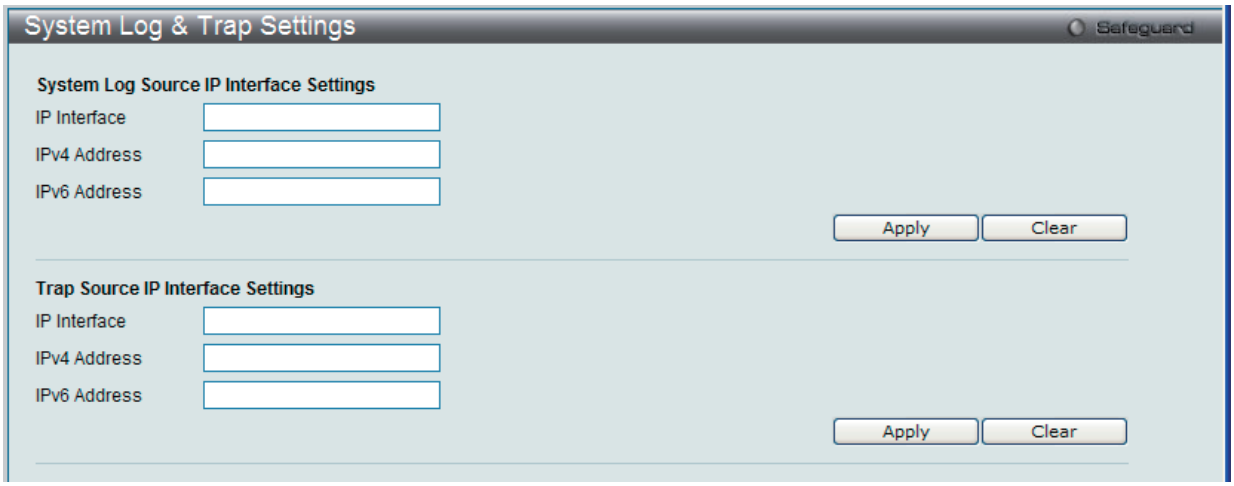


図 6-21　System Log & Trap Settings 画面

本画面には次の項目があります。

項目	説明
IP Interface	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。
IPv6 Address	使用する IPv6 アドレスを入力します。

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。

「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か、またはその両方を選択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 483 ページの「付録 C ログエントリ」を参照してください。

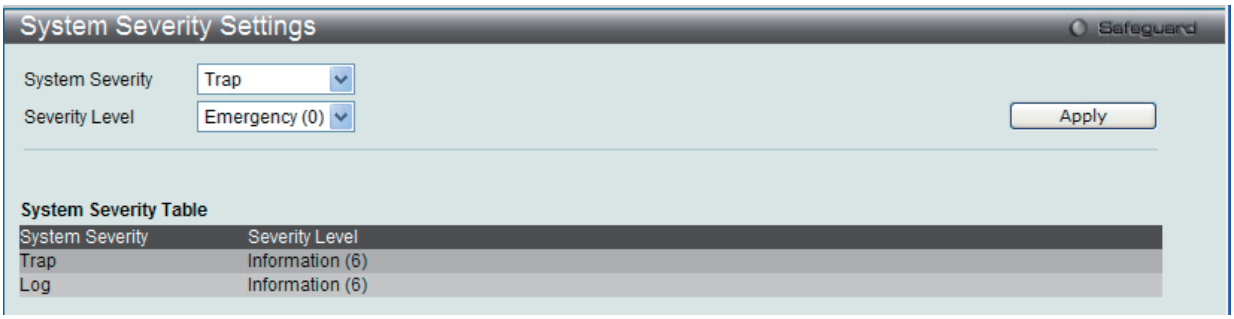


図 6-22　System Severity Settings 画面

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。

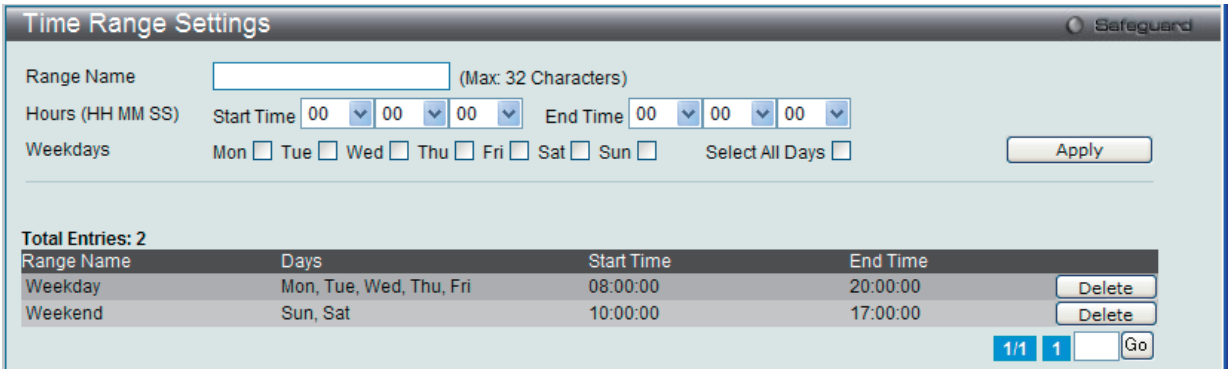


図 6-23　Time Range Settings 画面

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。

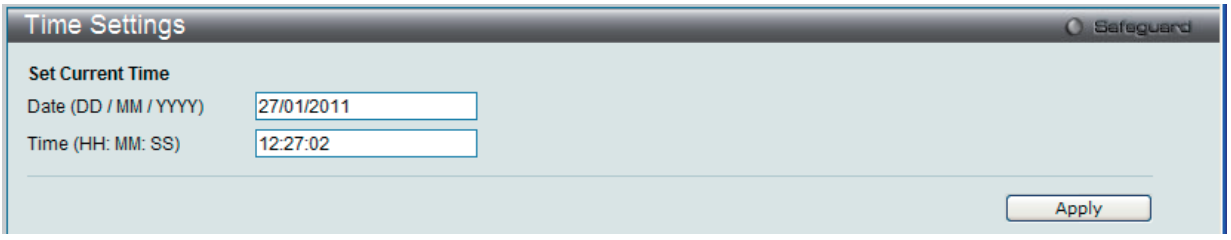


図 6-24　Time Settings 画面

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 SNTP 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。

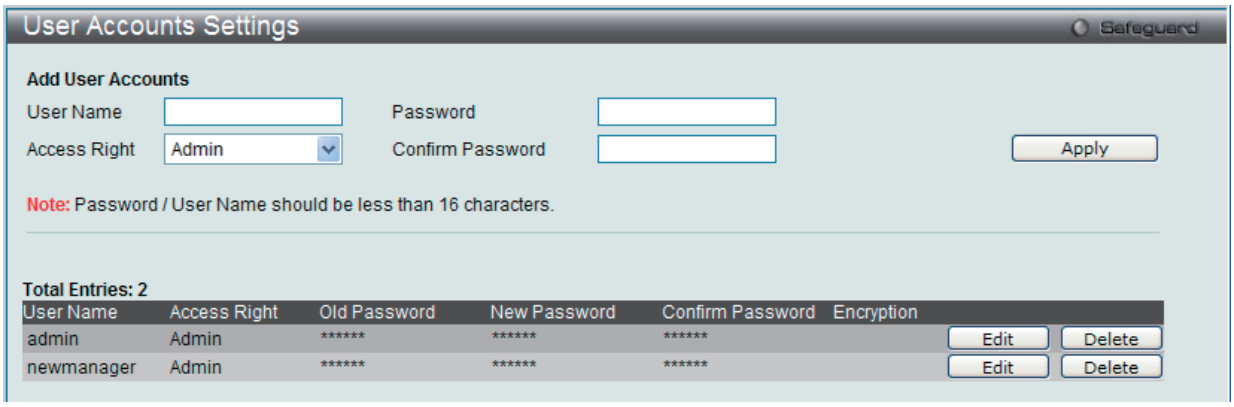


図 6-25　User Accounts Settings 画面

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には、「Admin」（管理者）、「Operator」（オペレータ）および「User」（一般ユーザ）の 3 つのレベルがあります。Admin 権限を持つユーザが使用できるメニューが、User または Operator 権限では使用できない場合があります。Operator レベル権限は、Admin 権限が行うセキュリティ機能に関わることを除き、スイッチにコンフィグレーション設定および参照が可能です。Operator ユーザは、後述のスイッチのローカルな認証方式またはアクセス認証制御機能を通じ、認証されます。ユーザが Operator レベルでスイッチにログインすると、特定のセキュリティ画面は参照または設定できなくなります。Admin レベルユーザだけが、これらの機能にアクセスすることができます。
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、以下の画面を表示します。

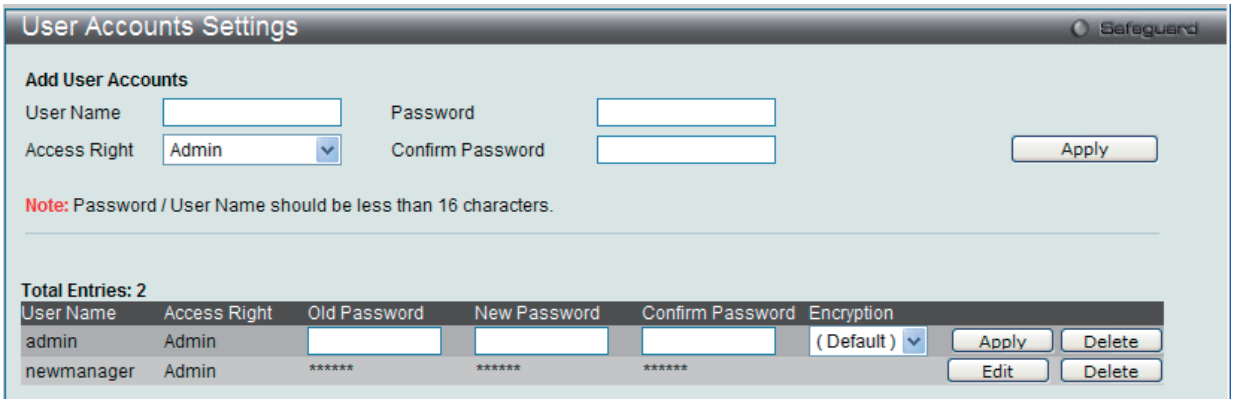


図 6-26　User Accounts Settings 画面 - 編集

2. 値を設定します。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、512 ページの「付録 F パスワードのリカバリ手順」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。

User Accounts 画面のエントリの削除
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。

Admin、Operator および User 権限
ユーザ権限には Admin、Operator および User の 3 つのレベルがあります。Admin 権限を持つユーザが利用可能なメニューのうちのいくつかは、Operator、または User 権限では利用できません。

以下の表に、Admin レベル、Operator レベルおよび User レベルの違いをまとめます。

表 6-1　Admin、Operator、User 特権

管理	Admin	Operator	User
コンフィグレーション設定	読み / 書き可	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
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
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	不可	不可
システムユーティリティ	読み / 書き可	不可	不可
リセット（工場出荷状態へ）	読み / 書き可	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
ユーザアカウントの確認	読み / 書き可	不可	不可

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、本マニュアル終わりにある 512 ページの「付録 F パスワードのリカバリ手順」を参照してください。これは、この問題を解決するように必要な手順を案内します。

注意　ユーザ名とパスワードは 16 文字以内とします。

SRM（スイッチリソース管理設定）（EI モードのみ）

SRM Settings（SRM 設定）

SRM（Switch Resource Management: スイッチリソース管理）構成モードを設定します。スイッチのリブート後にだけ、本コンフィグレーションは適用されます。

System Configuration > SRM > SRM 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。

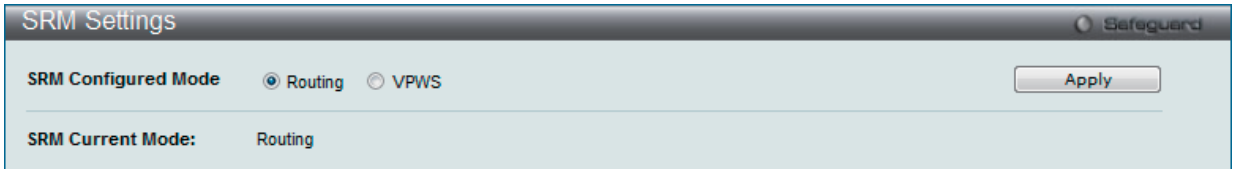


図 6-27　SRM Settings 画面

以下の項目を設定することができます。

項目	説明
SRM Configured Mode	• Routing - より多くのハードウェアリソースが L3 ルーティング機能に割り当てられるように指定します。 • VPWS - より多くのハードウェアリソースが MPLS 機能に割り当てられるように指定します。

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。

第 7 章　Management（スイッチの管理）

以下は、Management の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、プロキシ 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）、Proxy ARP Settings（プロキシ ARP 設定）、ARP Table（ARP テーブルの参照）	60
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）	63
IPv6 Neighbor Settings （IPv6 Neighbor 設定）	IPv6 Neighbor の設定を行います。	65
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（システム IP アドレス設定）、Interface Settings（インタフェース設定）、Loopback Interface Settings（ループバックインタフェース設定）	66
Management Settings（管理設定）	CLI ページング、DHCP 自動設定、省電力モードなどの管理設定を行います。	73
Out of Band Management Settings （アウトバンド管理設定）	RJ-45 のアウトバンド管理の詳細を設定します。	74
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。	74
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）、Topology（トポロジ）、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）	75
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 Linkchange 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）	84
Telnet Settings（Telnet 設定）	スイッチに Telnet 設定をします。	92
Web Settings（Web 設定）	スイッチに Web ステータスを設定します。	92
Power Saving（省電力設定）	スイッチに省電力設定を行います。次のメニューがあります。 LED State Settings（LED 状態設定）、Power Saving Settings（省電力設定）、Power Saving LED Setting（省電力 LED の設定）、Power Saving Port Settings（省電力ポート設定）	93

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。

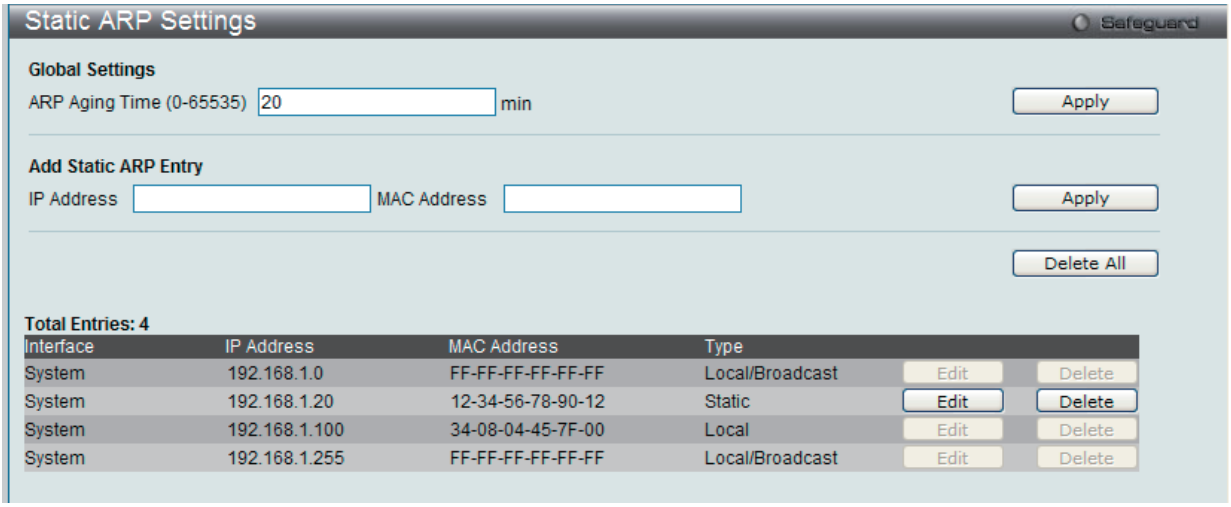


図 7-1　Static ARP Settings 画面

「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。

Static ARP List のエントリの編集

1. 編集するエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

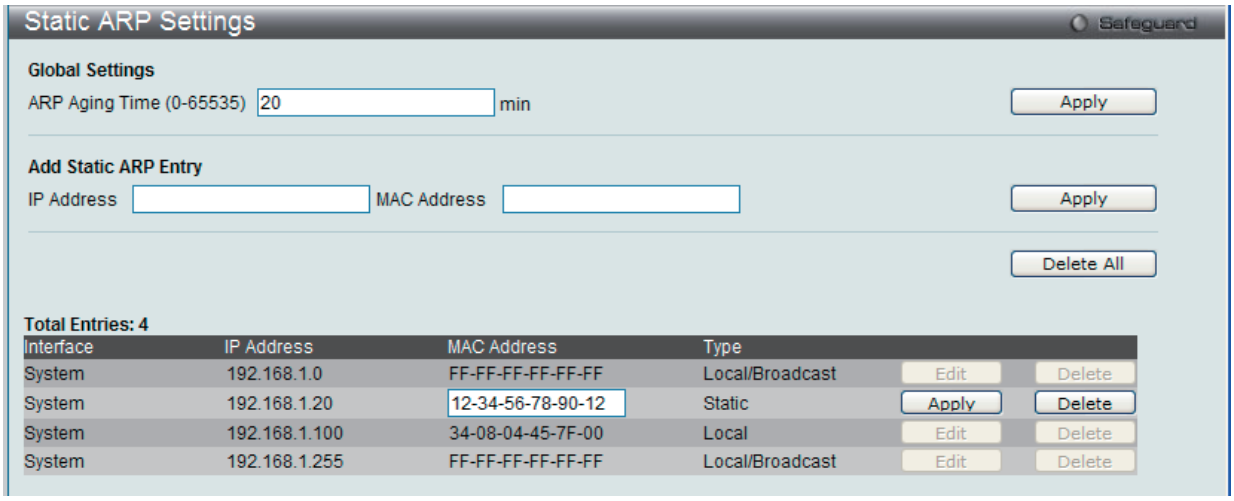


図 7-2　Static ARP Settings 画面

2. 「MAC Address」を編集します。

3. 「Apply」ボタンをクリックします。

Static ARP List のエントリの削除

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。

Proxy ARP Settings（プロキシ ARP 設定）

プロキシ ARP 機能に関する基本設定を参照および編集します。

スイッチのプロキシ ARP（Address Resolution Protocol）機能を使用して、スイッチはオリジナルの ARP 応答者のように識別子（IP および MAC アドレス）を見せかけることによって別のデバイス宛の ARP リクエストに応答することができます。そのため、スイッチは、スタティックルーティングまたはデフォルトゲートウェイを設定せずに、意図した宛先にパケットを送信することができます。

ホスト（通常レイヤ 3 スイッチ）は他のデバイス宛のパケットに応答します。例えば、ホスト A と B が異なる物理ネットワークにあると、B は A から ARP ブロードキャストリクエストを受信しないため応答できません。しかし、A の物理ネットワークがルータまたはレイヤ 3 スイッチを使用して B に接続していると、ルータまたはレイヤ 3 スイッチは A からの ARP リクエストを参照します。

送信元 IP と宛先 IP が同じインタフェースにあると、スイッチはこのローカルなプロキシ ARP 機能によりプロキシ ARP に応答することができます。

Management > ARP > Proxy 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。

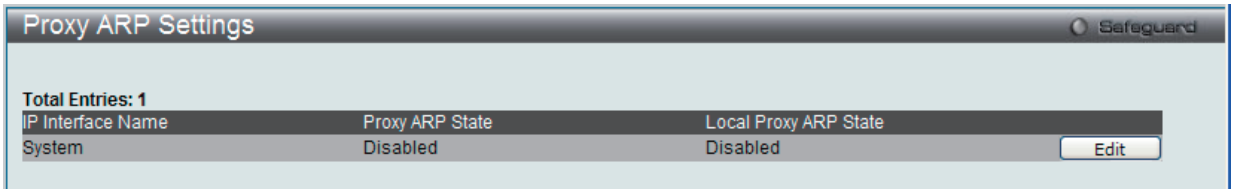


図 7-3　Proxy ARP Settings 画面

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、以下の画面を表示します。

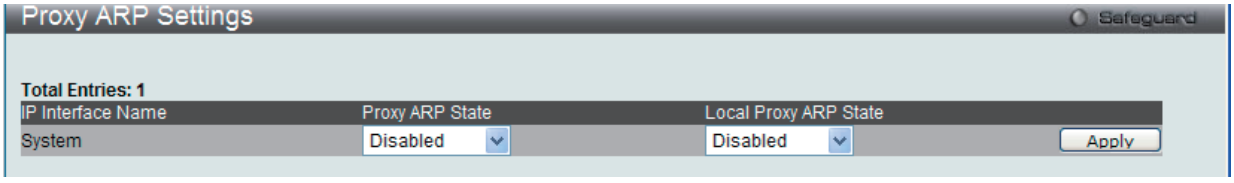


図 7-4　Static ARP Settings 画面

2. 指定エントリを編集して、IP インタフェースのプロキシ ARP の状態を選択します。

3. 「Apply」ボタンをクリックします。

初期値では、「Proxy ARP State」と「Local Proxy ARP State」の両方とも無効です。

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。

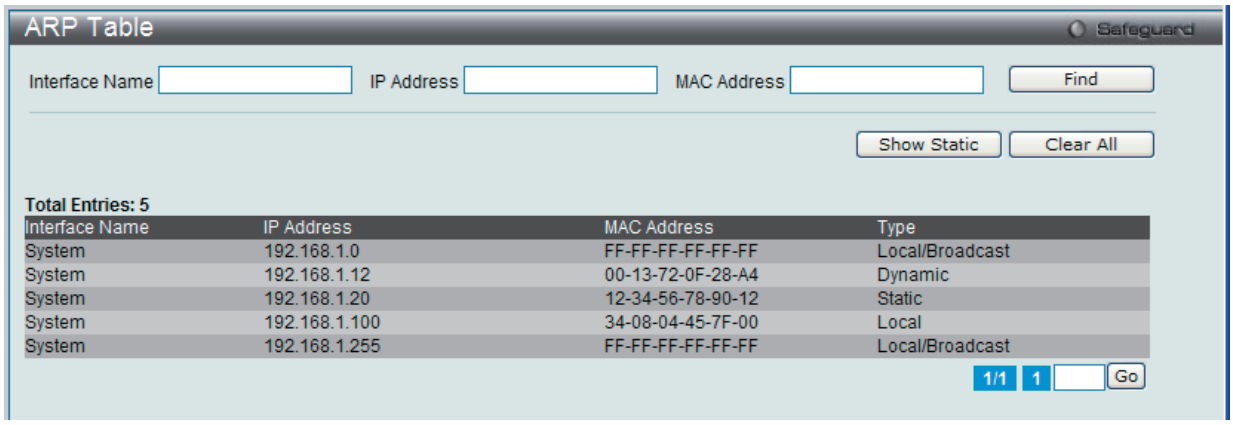


図 7-5　ARP Table 画面

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。

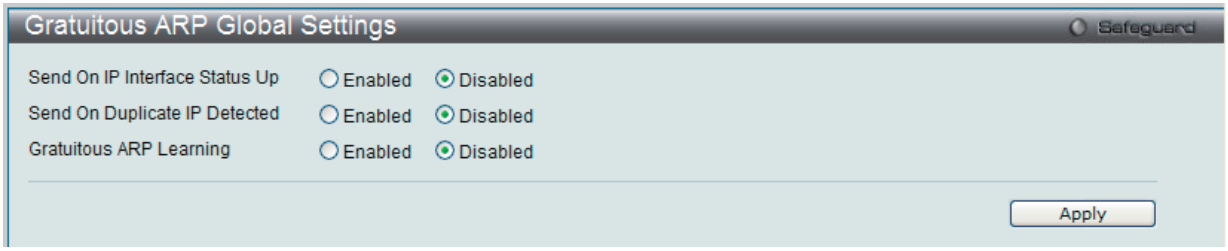


図 7-6　Gratuitous ARP Global Settings 画面

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。初期値は無効で、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。初期値は無効です。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。初期値は無効です。

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。

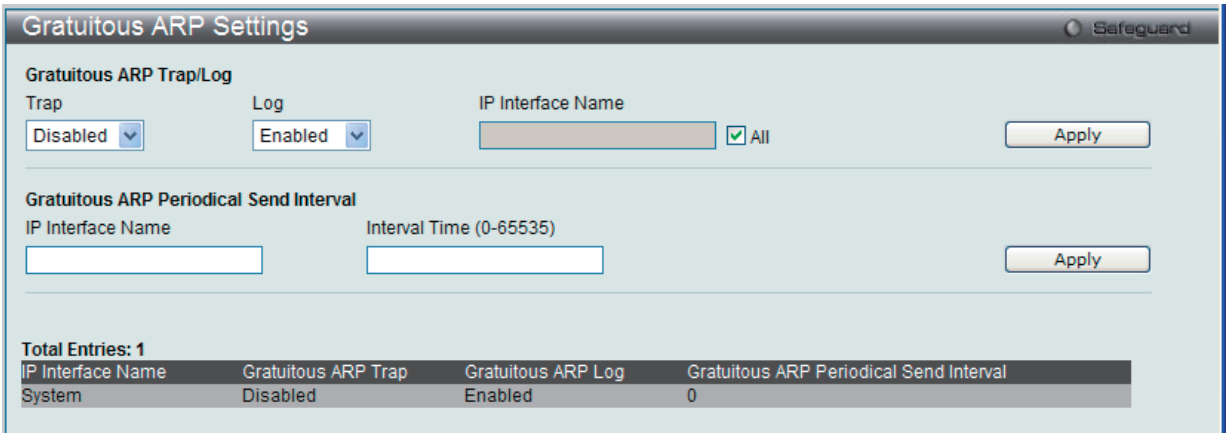


図 7-7　Gratuitous ARP Settings 画面

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。
IP 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	
IP 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。

「Gratuitous ARP Trap/Log」セクションにある「Apply」ボタンをクリックしてこのセクションで行った変更を適用します。
「Gratuitous ARP Periodical Send Interval」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。

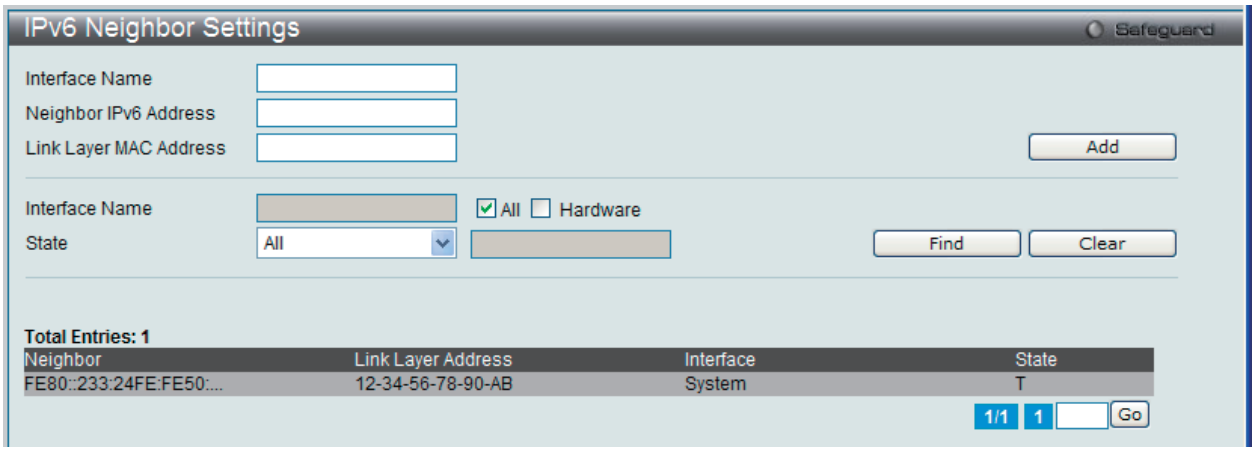


図 7-8　IPv6 Neighbor Settings 画面

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 名を入力します。スイッチにおける現在の全インタフェースに対して検索するには、画面の中央部分にある 2 個目の「Interface Name」欄で「All」を選択し、「Find」ボタンをクリックします。また、「Hardware」オプションを選択して、ハードウェアテーブルに書かれたすべての Neighbor キャッシュエントリを表示します。
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。
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（システム 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。

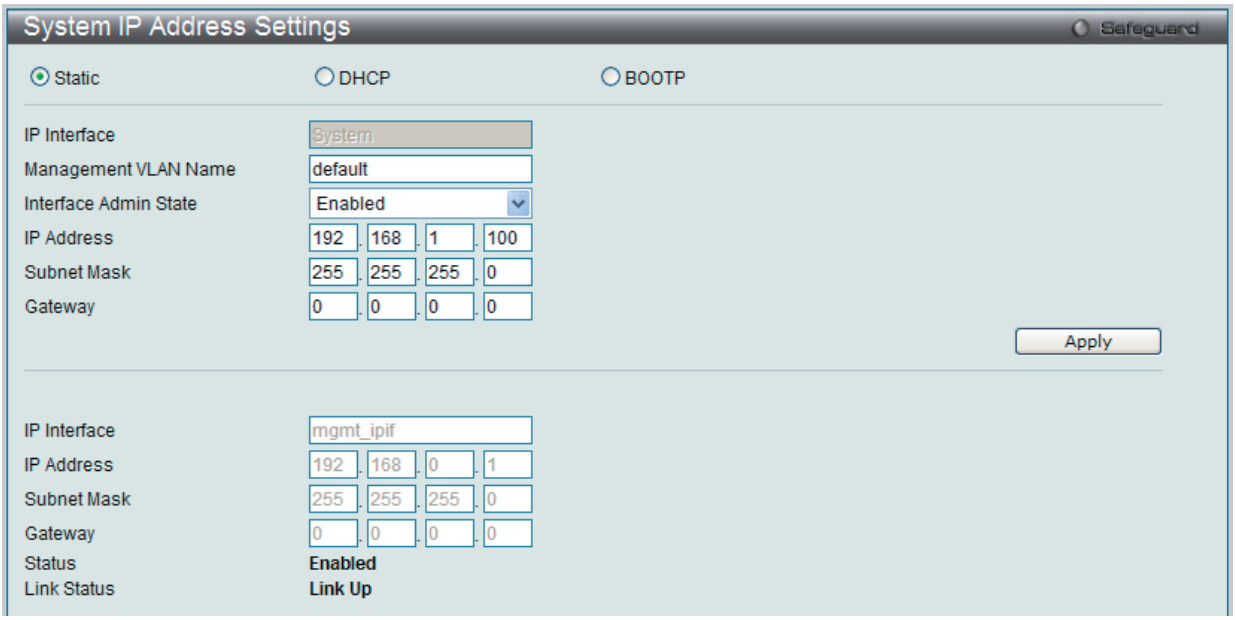


図 7-9　IP Address Settings 画面

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
IP Interface	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 経由）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。本項目で登録した VLAN 以外に所属する管理ステーションからは、帯域内管理を行うことができません。ただし、そのアドレスが402 ページの「Trusted Host Settings（トラストホスト設定）」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 が登録されていない場合は、スイッチ上のすべてのポートは default VLAN に所属しています。経由するインバンド「Trusted Host」テーブルにはエントリはないため、管理 VLAN が設定されるまで、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、スイッチに接続している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。

以下の表は「Management」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
IP Interface	管理インタフェース名が表示されます。
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。
Status	管理ポートを有効または無効にします。
Link Status	物理接続が管理ポートに行われているかどうかを示します。

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。

コンソールインタフェースを使用したスイッチの IP アドレス設定

各スイッチに IP アドレスを設定し、設定した IP アドレスを使用して SNMP ネットワークマネージャや TCP/IP アプリケーション（例えば BOOTP、TFTP など）との通信をします。本スイッチの IP アドレスの初期値は 10.90.90.90 です。初期値の IP アドレスはご使用のネットワークアドレス体系に合うように変更してください。

IP アドレスは、Web マネージャを使用する前に設定してください。本スイッチの 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設定することもできます。その場合は、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。コンソールポートから Command Line Interface（CLI）を使用する設定方法は以下の通りです。

・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: System という名前のインタフェースに割り当てる IP アドレス、yyy.yyy.yyy.yyy: 対応するサブネットマスク）

・**`config ipif System ipaddress xxx.xxx.xxx.xxx/z`** とコマンド入力することも可能です。
（xxx.xxx.xxx.xxx: System という名前のインタフェースに割り当てる IP アドレス、z: CIDR 表記によるサブネットマスク数）

スイッチ上の「System」と名付けた IP インタフェースには IP アドレスとサブネットマスクを割り当て、管理ステーションをスイッチの Telnet または Web ベース管理エージェントに接続するために使用します。

「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を確認できます。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。

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 > Interfaces 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。

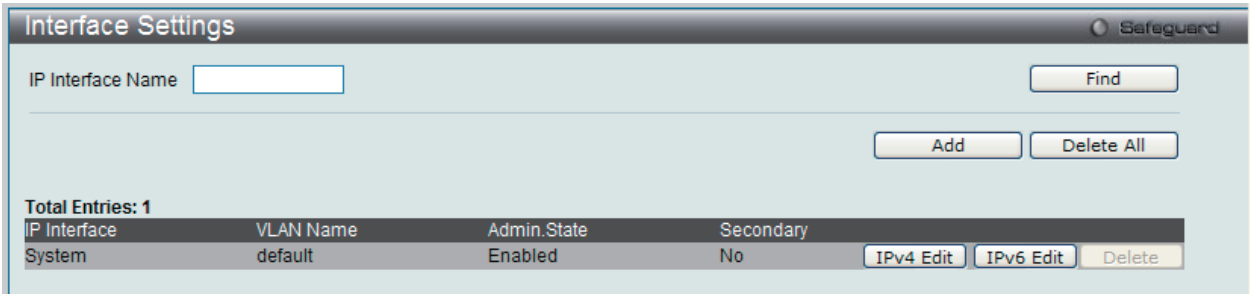


図 7-10　Interface Settings 画面

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
IP 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。

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 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 7-11　IPv4 Interface Settings 画面

2. 以下の項目を設定します。

項目	説明
IP 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。
Secondary Interface	このオプションを選択してセカンダリインタフェースとしてこのインタフェースを使用します。プライマリ IP が利用できない場合、VLAN はセカンダリインタフェースに切り替わります。プライマリ IP が回復すると、元に戻ります。

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 7-12　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を指定します。
IP 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。

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。

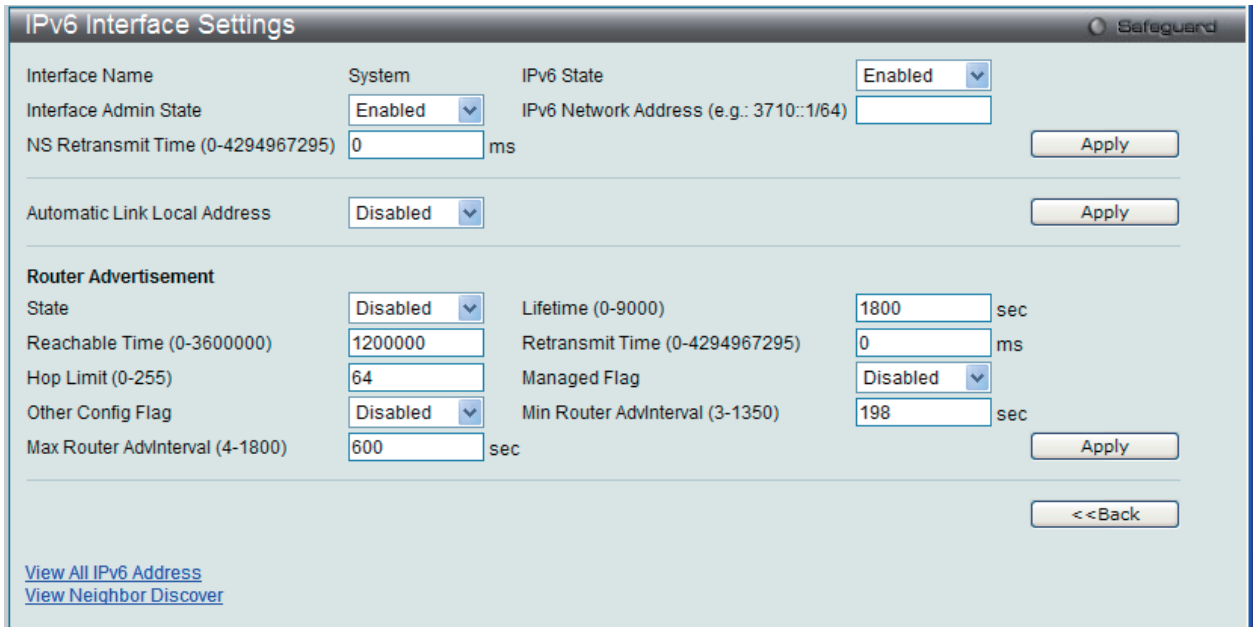


図 7-13　IPv6 Interface Settings 画面 - Edit

2. 以下の項目を設定します。

項目	説明
IP 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	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 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。
Router Advertisement	
State	ルータの通知状態を有効または無効にします。
Lifetime	デフォルトルータとしてのルータの寿命 (秒) を指定します。
Reachable Time	到達性の確認を受け取った後に、ノードが隣接しているノードを到達可能と見なす時間 (ミリ秒) を指定します。
Retransmit Time	ルータ通知メッセージの再送間隔 (ミリ秒) を指定します。ルータ通知パケットがホストにそれを渡します。
Hop Limit	この RA メッセージを受信するホストに送信されるパケットのために IPv6 ヘッダ内の「hop_limit」フィールドの初期値を指定します。
Managed Flag	有効に設定されると、この RA を受信するホストは、ステートレスアドレス設定から取得したアドレスに加え、ステートフルアドレス設定プロトコルを使用する必要があります。
Other Config Flag	有効に設定されると、この RA を受信するホストは、アドレス設定情報を取得するために、ステートフルアドレス設定プロトコルを使用する必要があります。
Min Router Advinterval	インタフェースから求められていないマルチキャスト通知が送信される最小時間 (秒)。本エントリは、3(秒) より大きくし、MaxRtrAdvInterval の 3/4 より大きくしないでください。初期値は 198（秒）です。
Max Router Advinterval	インタフェースから求められていないマルチキャスト通知が送信される最大時間 (秒)。4-1800(秒) で指定します。初期値は 600（秒）です。

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。
「View Neighbor Discover」リンクをクリックして、すべての Neighbor 検出情報エントリを参照します。

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 7-14　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。

Neighbor の参照

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

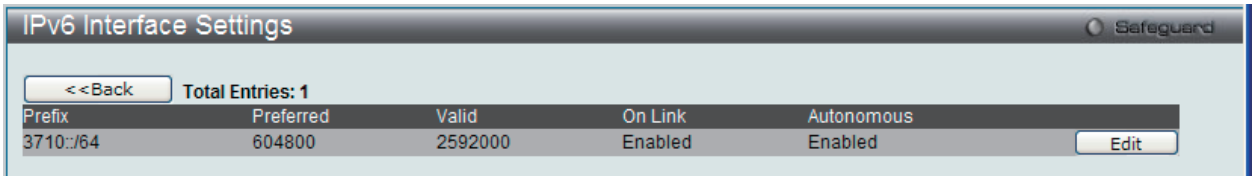


図 7-15　IPv6 Interface Settings 画面

Neighbor の編集

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

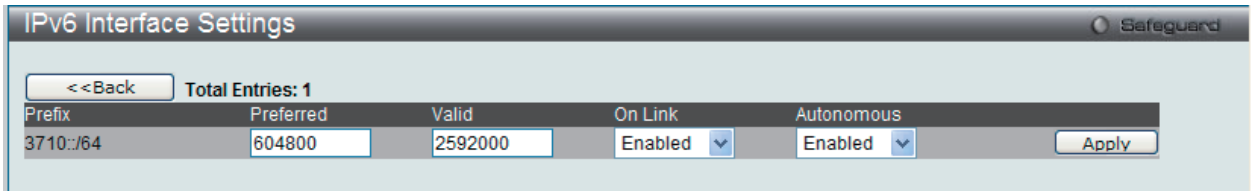


図 7-16　IPv6 Interface Settings 画面 - Edit

2. 設定変更後、「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックして前のページに戻ります。

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。

Loopback Interface Settings（ループバックインタフェース設定）

ループバックインタフェースを設定します。ループバックインタフェースは、それを無効または削除するまで通常アクティブな論理 IP インタフェースで、どんな物理インタフェースの状態からも独立しています。

Management > IP Interface > Loopback 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。

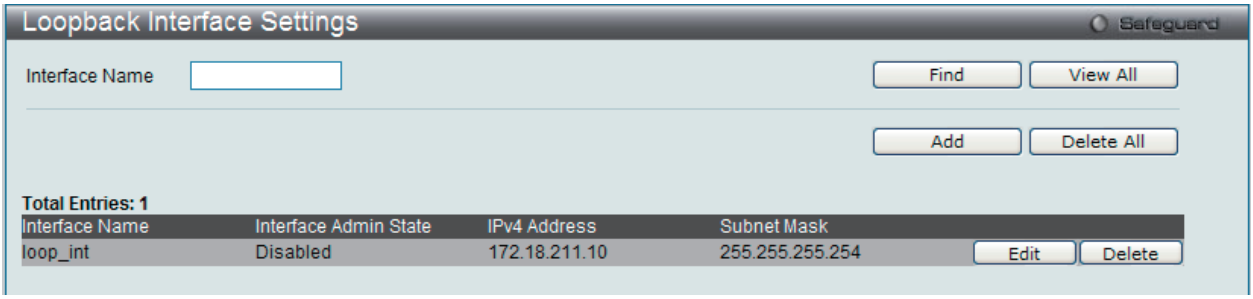


図 7-17　Loopback Interface Settings

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	インタフェース名を入力します。

インタフェースの検索

「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。「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。

ループバックインタフェースの追加、編集

1. 「Add」（追加）または「Edit」（編集）ボタンをクリックして、以下の画面を表示します。

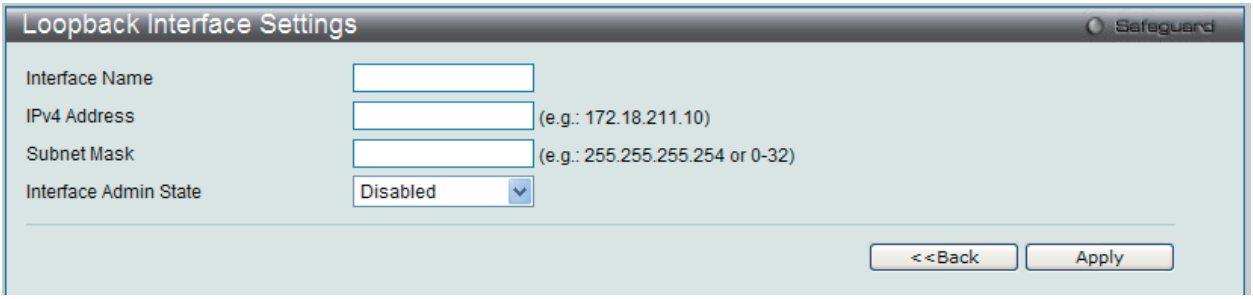


図 7-18　Loopback Interface Settings - Add/Edit 画面

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	ループバックインタフェース名。 注意 ループバック IP インタフェースは通常の IP インタフェースと共に同じネームドメイン空間を持つため、名前は通常の IP インタフェースと重複することはできません。
IPv4 Address	ループバックインタフェース用に 32 ビットの IPv4 アドレスを入力します。
Subnet Mask	ループバックインタフェースに割り当てるサブネットマスクを入力します。
Interface Admin State	プルダウンメニューを使用して、ループバックインタフェースを「Enabled」(有効)/「Disabled」(無効) にします。

2. 該当項目を入力後、「Apply」ボタンをクリックし、設定内容を適用します。

「<<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。

インタフェースの削除

「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、テーブルに表示されたすべてのエントリを削除します。

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手順を参照してください。本マニュアルの「Tools」セクションの「Upload Log File」画面の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、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 7-19　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。
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。

「Apply」ボタンをクリックして行った変更を適用します。

注意　D-Link グリーンテクノロジーに関する詳細については、http://green.dlink.com/ を参照してください。

Out of Band Management Settings（アウトバンド管理設定）

RJ-45 のアウトバンド管理の詳細を設定します。

1. **Management > Out of Band 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。

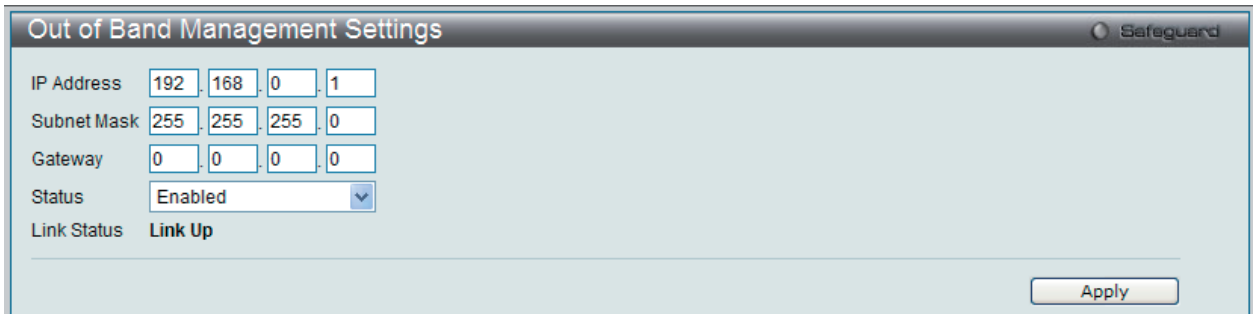


図 7-20　Out of Band Management Settings 画面

2. 以下の項目を設定します。

項目	説明
IP Address	使用する IP アドレスを入力します。
Subnet Mask	使用するサブネットを入力します。
Gateway	使用するゲートウェイ IP アドレスを入力します。
Status	アウトバンド管理の状態を有効または無効にします。
Link Status	リンクステータスを表示します。

「Apply」ボタンをクリックして行った変更を適用します。

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。

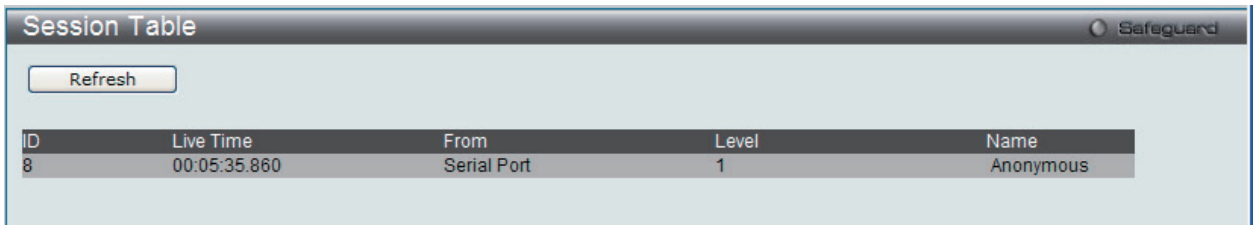


図 7-21　Session Table 画面

「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。
- 複数の 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。

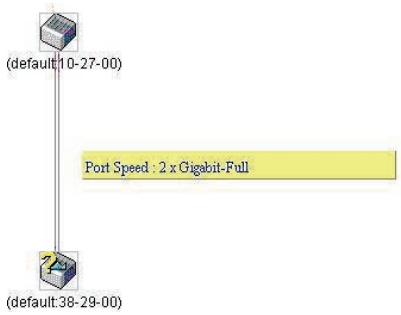
バージョン 1.61 へのアップグレード

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。

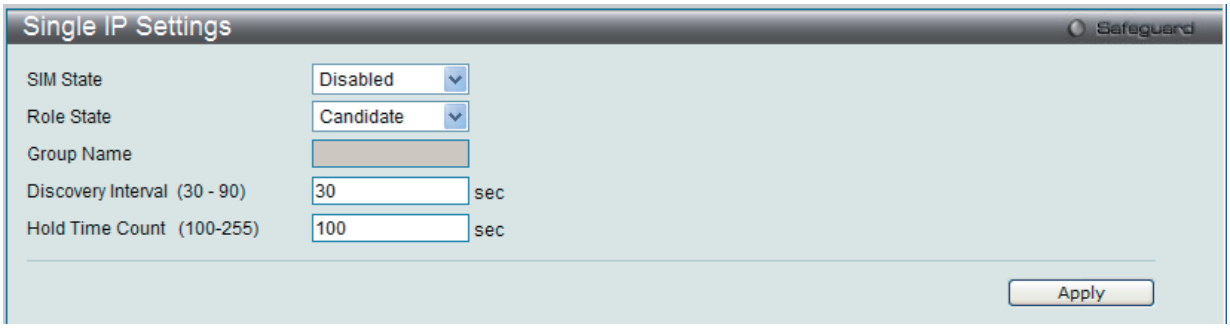


図 7-22　Single IP Settings 画面（CaS 無効状態）

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。

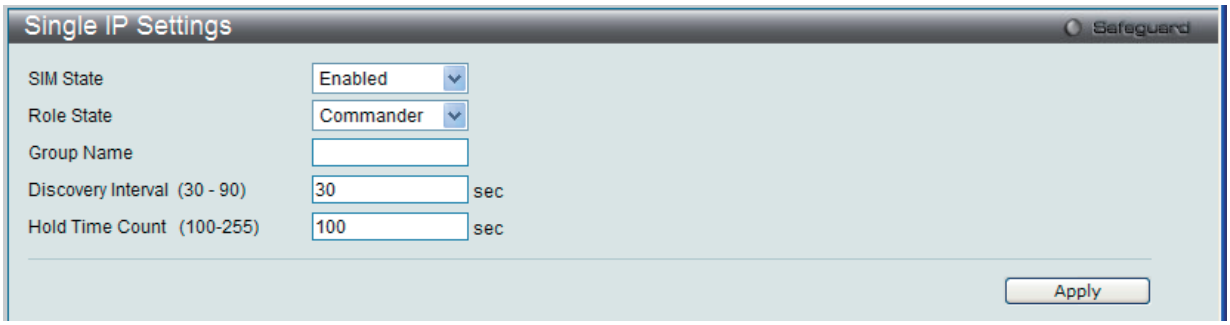


図 7-23　Single IP Settings 画面（CS 有効状態）

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。
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。
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。

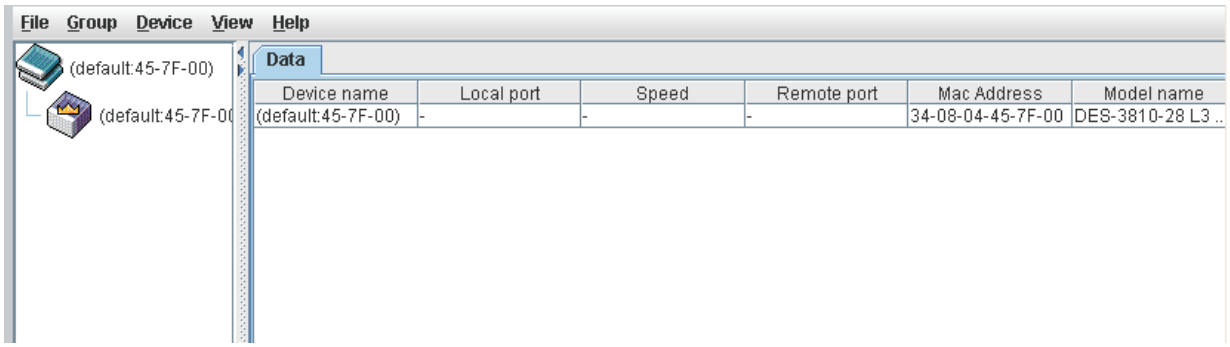


図 7-24　トポロジ画面

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。

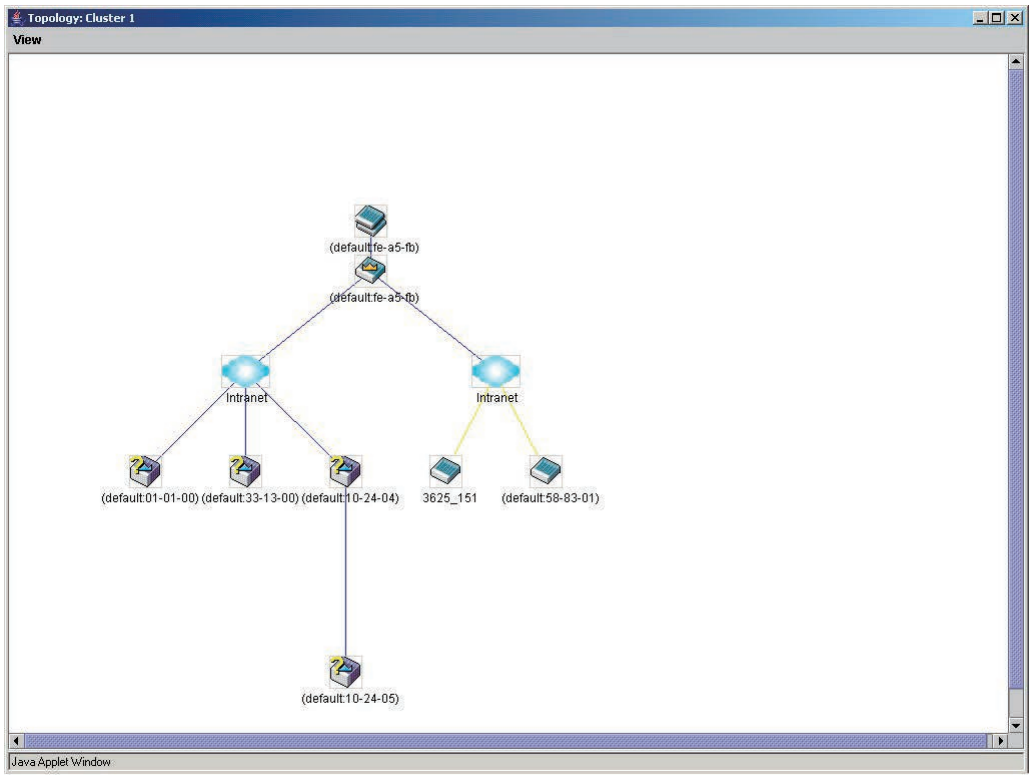


図 7-25　Topology 画面

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。

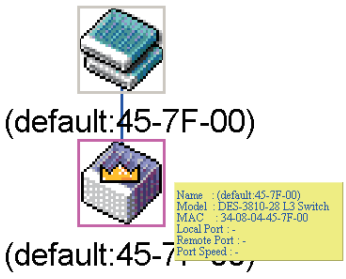


図 7-26　ツールヒントを利用したデバイス情報の表示

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。

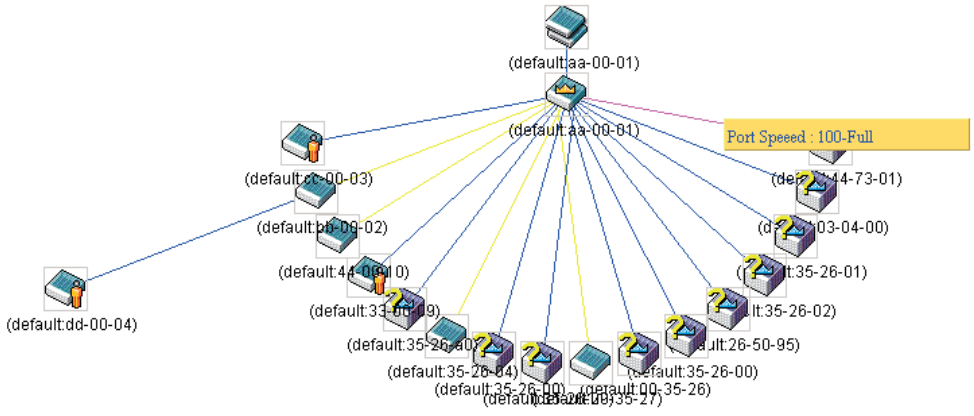


図 7-27　ツールヒントを利用したポート速度の表示

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

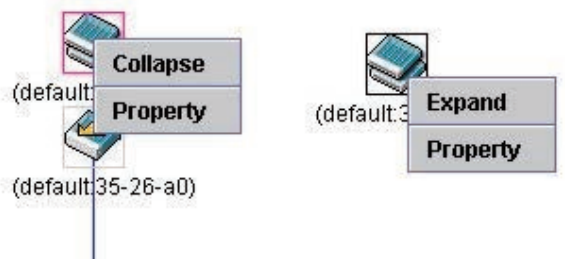


図 7-28　グループアイコン上での右クリック

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。

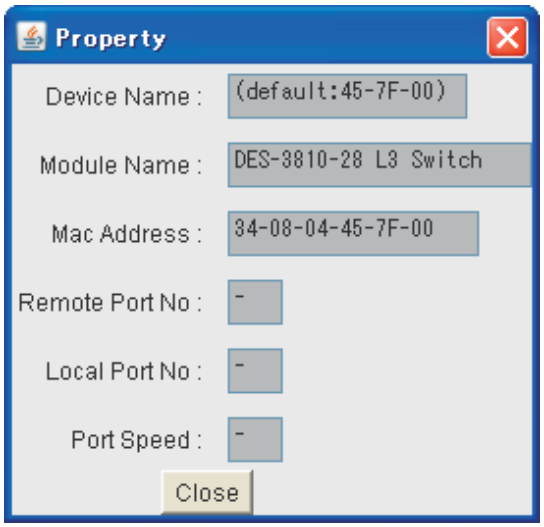


図 7-29　Property 画面

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

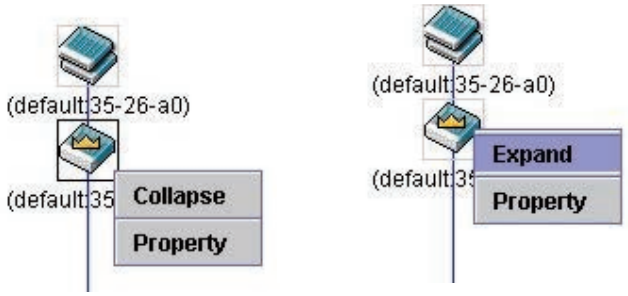


図 7-30　Commander スイッチアイコン上での右クリック

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

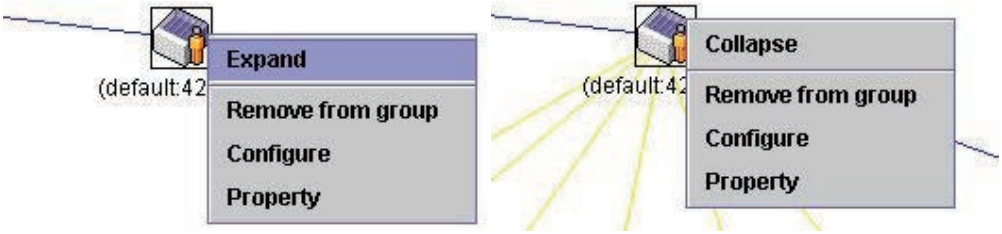


図 7-31　Member スイッチアイコン上での右クリック

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

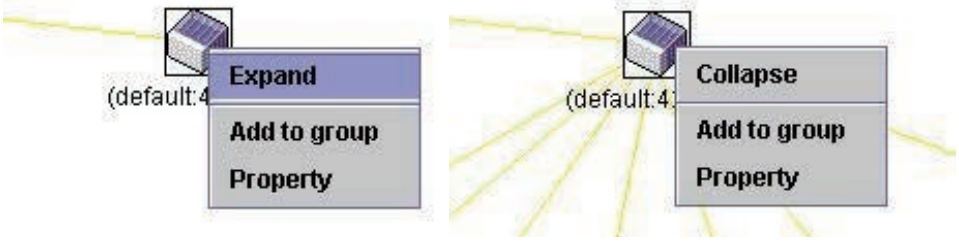


図 7-32　Candidate スイッチアイコン上での右クリック

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 7-33　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 7-34　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 7-35　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 7-36　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。

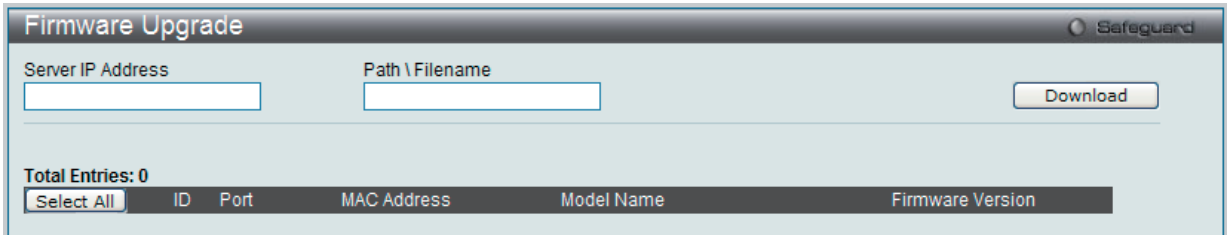


図 7-37　Firmware Upgrade 画面

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保存と復元）

CS から MS に対して TFTP サーバを使用してコンフィグレーションファイルのバックアップまたはリストアを行います。

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。

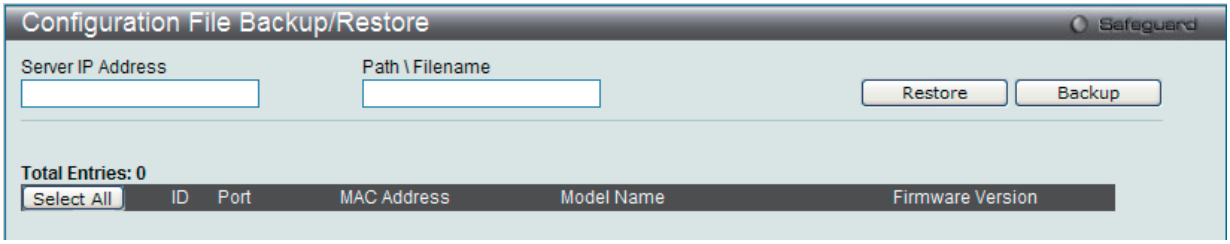


図 7-38　Configuration File Backup/Restore 画面

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アップデート対象のスイッチは、「Port」欄の下のラジオボタンで選択します。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。「Restore」ボタンをクリックすると、TFTP サーバから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 サーバにファイルがバックアップされます。

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。

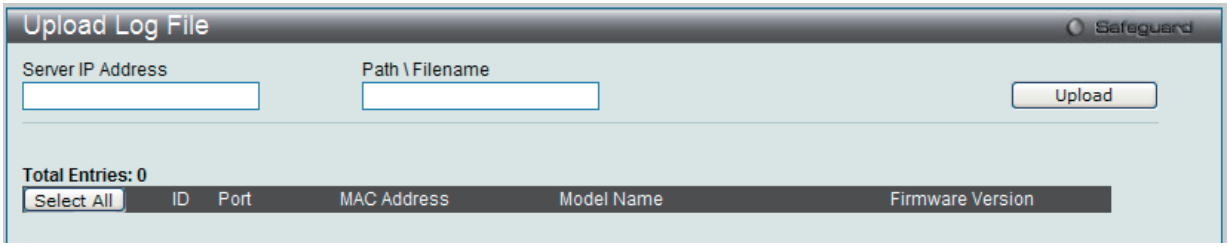


図 7-39　Upload Log File 画面

ログファイルをアップロードするためには、ログを保存する 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。

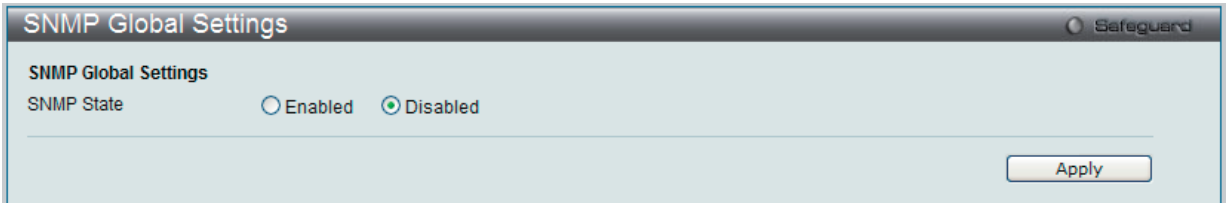


図 7-40　SNMP Global Settings 画面

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 7-41　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。

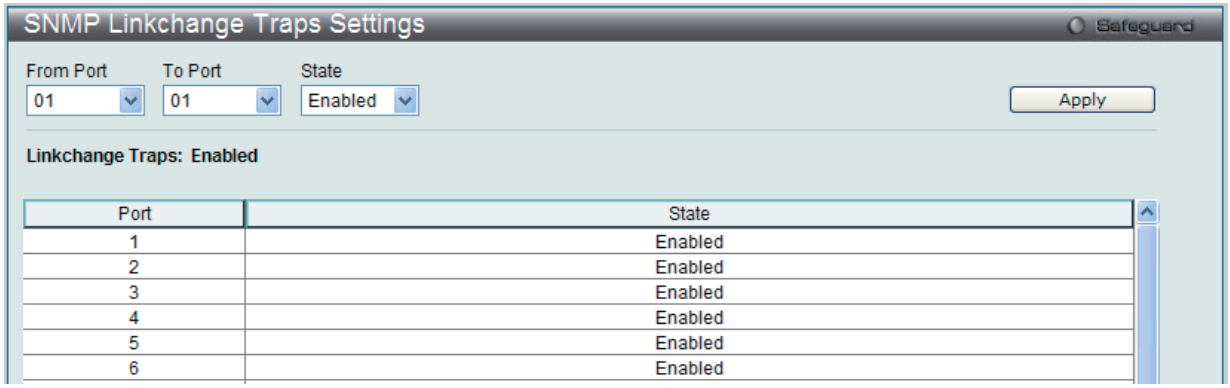


図 7-42　SNMP Link Change Traps Settings 画面

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。

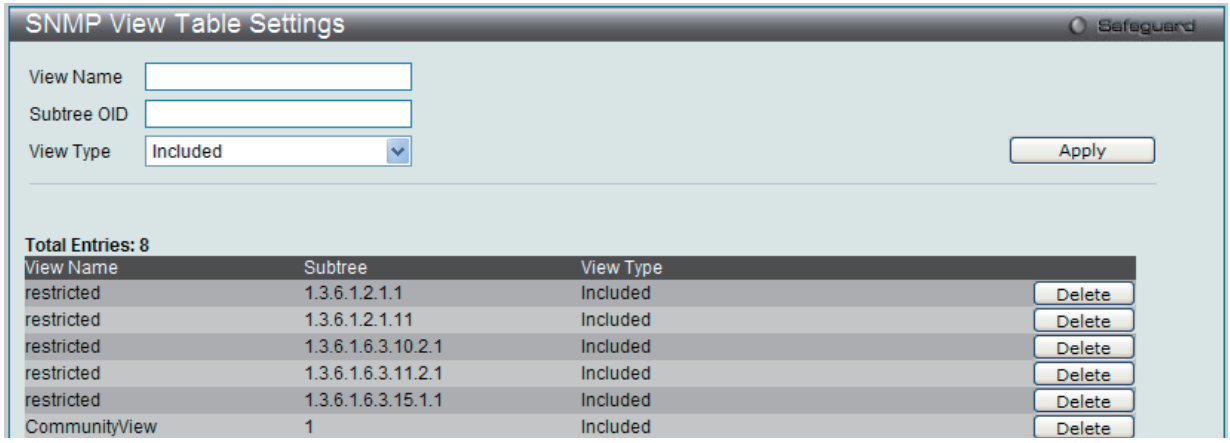


図 7-43　SNMP View Table Settings 画面

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 7-44　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。

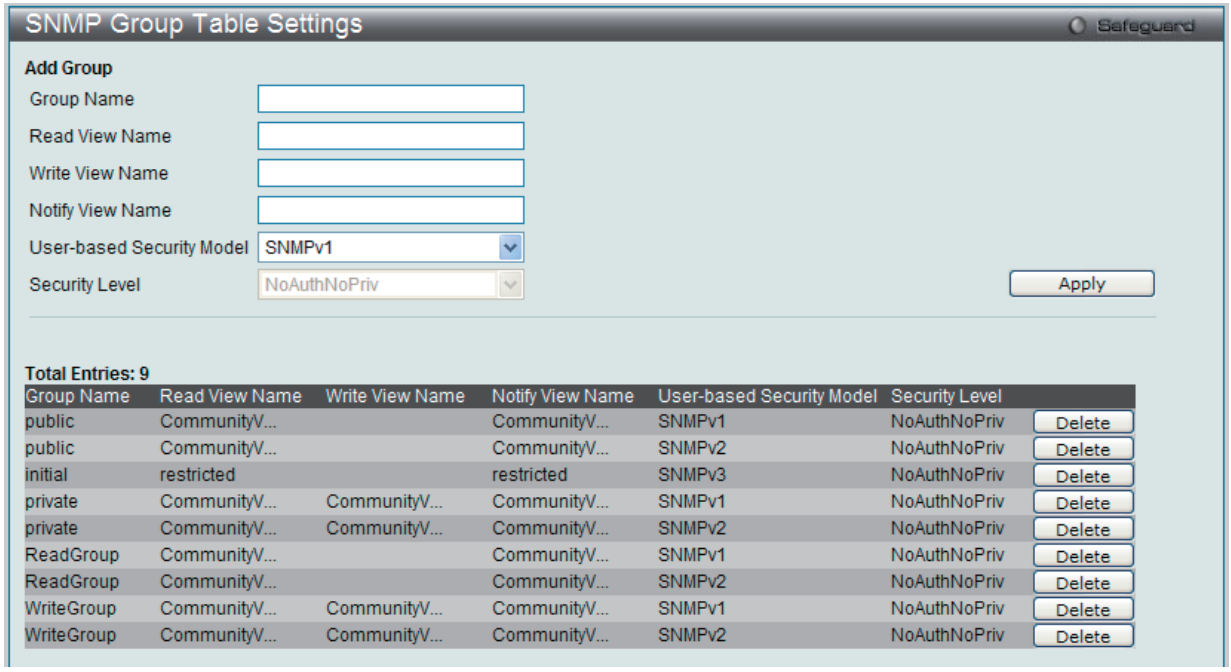


図 7-45　SNMP Group Table Settings 画面

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。

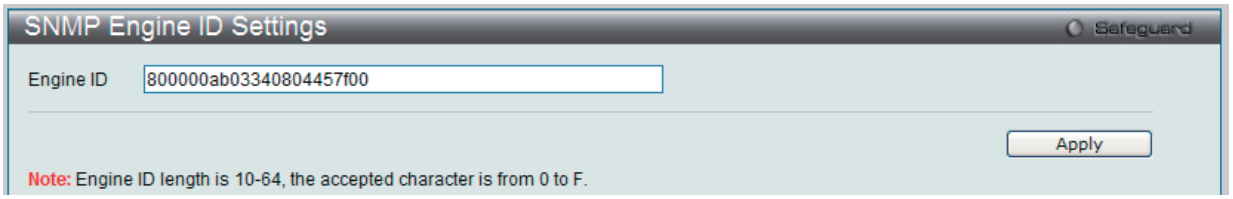


図 7-46　SNMP Engine ID Settings 画面

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。

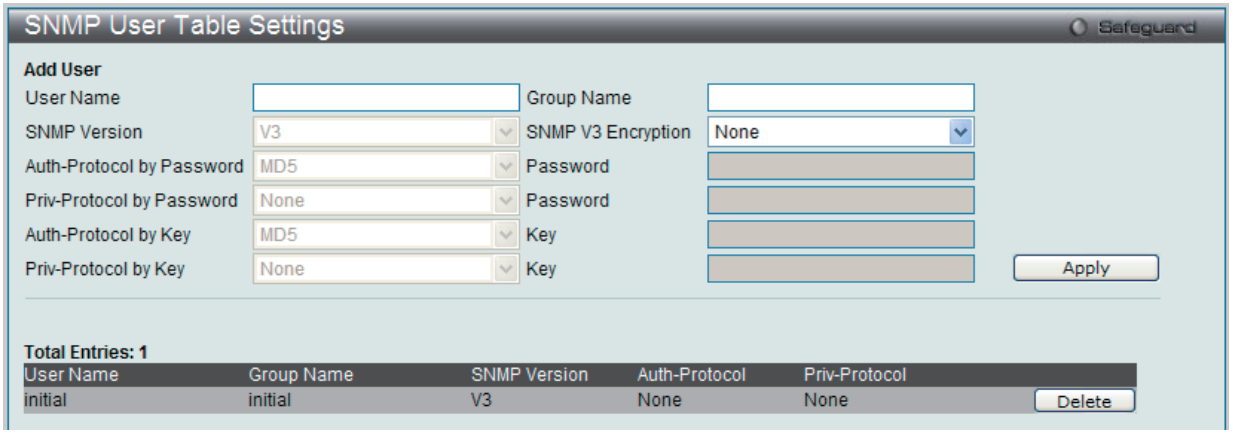


図 7-47　SNMP User Table Settings 画面

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。

上記画面中の項目を以下に示します。

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。

項目	説明
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。

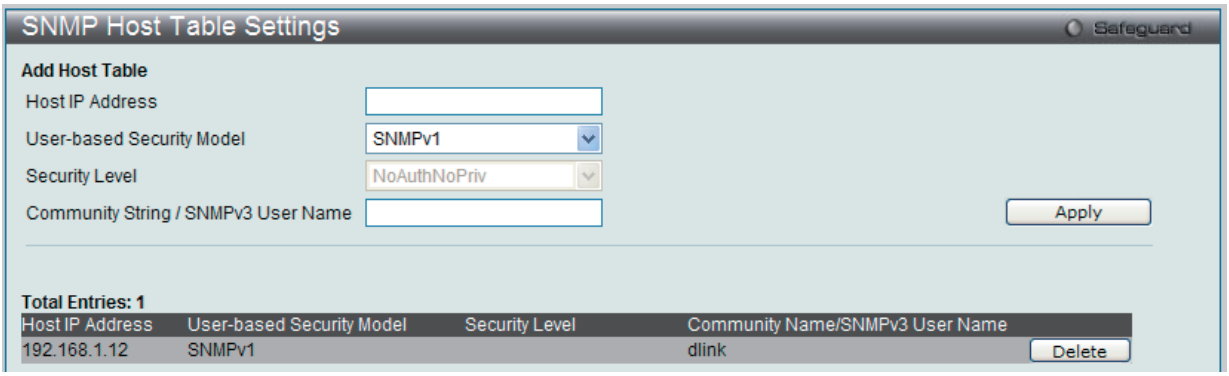


図 7-48　SNMP Host Table Settings 画面

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。

SNMP v6Host Table Settings（SNMP v6 ホストテーブル設定）

IPv6 用の SNMP トラップの送信先を設定します。

Management > SNMP Settings > SNMP v6Host 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。

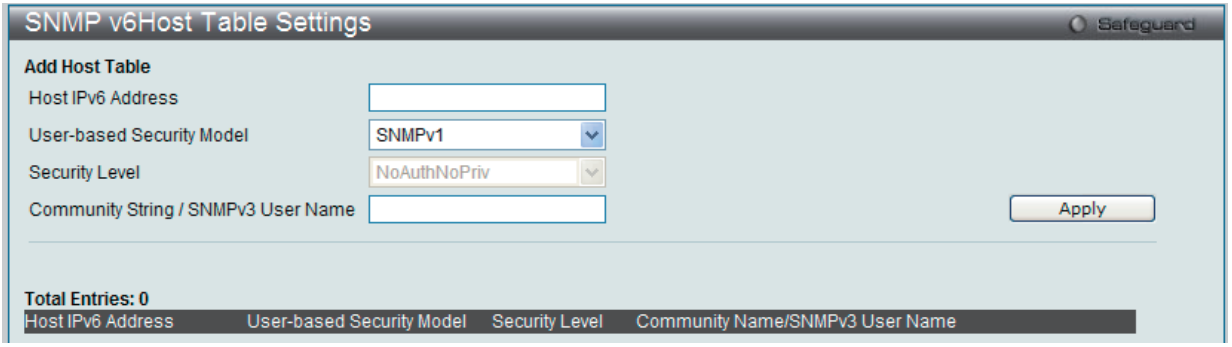


図 7-49　SNMP v6Host Table Settings 画面

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 IPv6 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 IPv6 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。

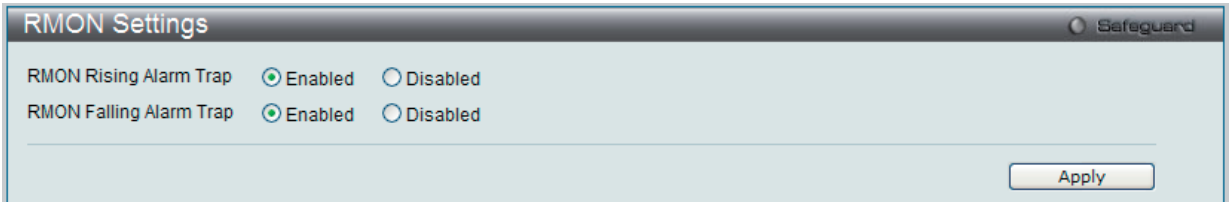


図 7-50　RMON Settings 画面

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。

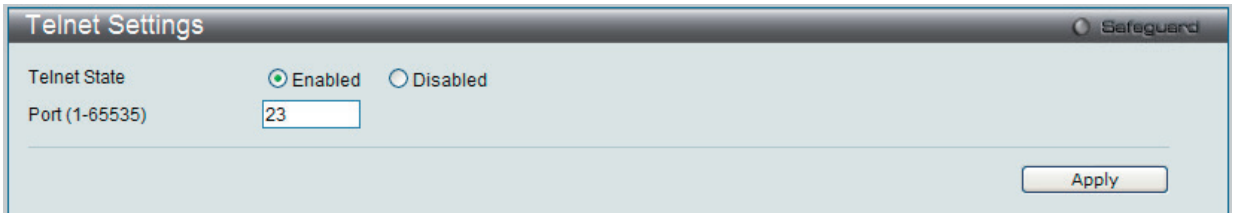


図 7-51　Telnet Settings 画面

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 マネジメントに使用される 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。

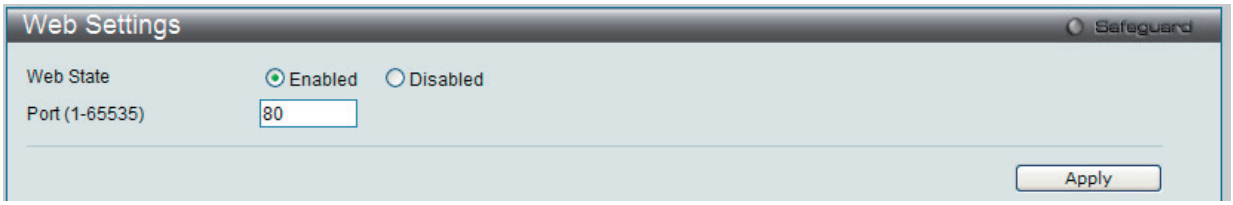


図 7-52　Web Settings 画面

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。

Power Saving（省電力設定）

LED State Settings（ポート LED 状態設定）

ポート LED の状態を設定します。

Management > Power Saving > LED State 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。

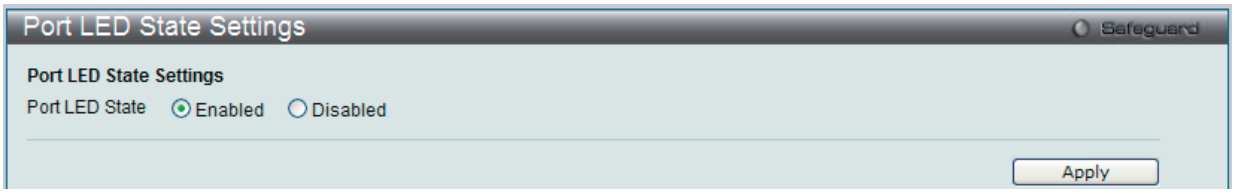


図 7-53　Port LED State Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Port LED State	本オプションを使用して、ポート LED の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。

Power Saving Settings（省電力設定）

スイッチの内蔵電源の節電機能、および本設定を実行するスケジュールを設定できます。

Management > Power Saving > Power Saving 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。

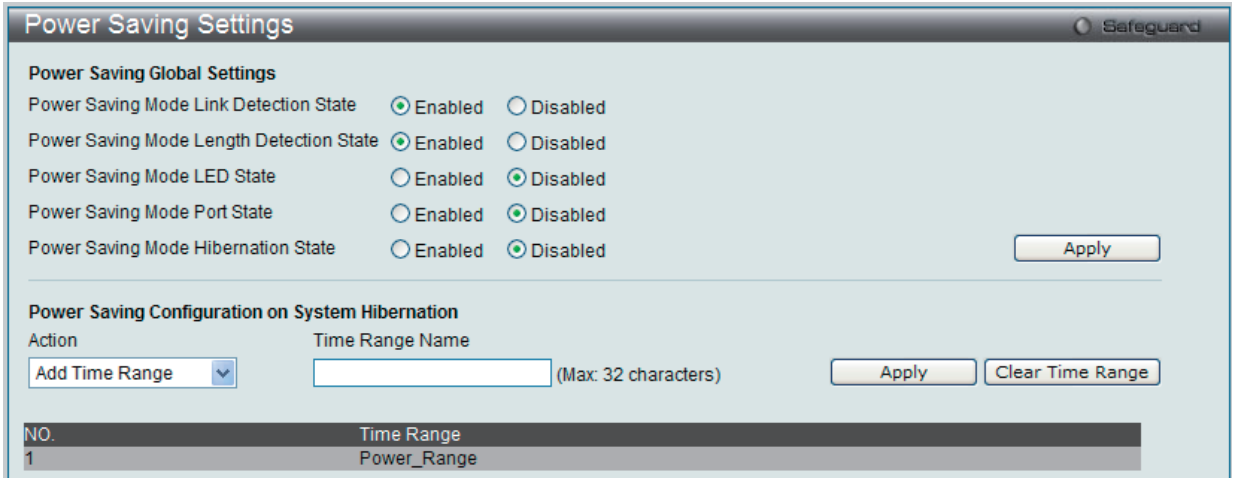


図 7-54　Power Saving Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Power Saving Global Settings	
Power Saving Mode Link Detection State	「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。
Power Saving Mode Length Length Detection State	「Enabled」（有効）である場合、スイッチは自動的にケーブルの長さを測定して電力フローを調整します。
Power Saving Mode Length LED State	「Enabled」（有効）である場合、ポートの LED 状態を設定した時間オフにします。
Power Saving Mode Length Port State	「Enabled」（有効）である場合、ポーを設定した時間シャットダウンします。
Power Saving Mode Length Hibernation State	「Enabled」（有効）である場合、スイッチは、低電力状態に入り、設定した時間アイドル状態になります。これは、すべてのポートをシャットダウンし、すべてのネットワーク機能（telnet、ping など）は動作しません。コンソール接続だけが RS232 ポートを通じて動作します。スイッチがエンドポイントタイプ PSE（Power Sourcing Equipment: 給電機器）である場合、ポートに電源を供給しません。
Power Saving Configuration on System Hiberation	
Action	スケジュールを追加（Add Time Range ）または削除（Delete Time Range）を削除します。
Time Range Name	スケジュール名を指定します。

「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。

「Clear Time Range」ボタンをクリックして、設定済みのすべてのタイムレンジを削除します。

Power Saving LED Settings（省電力 LED の設定）

すべてのポートの LED における省電力スケジュールを追加または削除します。

Management > Power Saving > Power Saving LED 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。

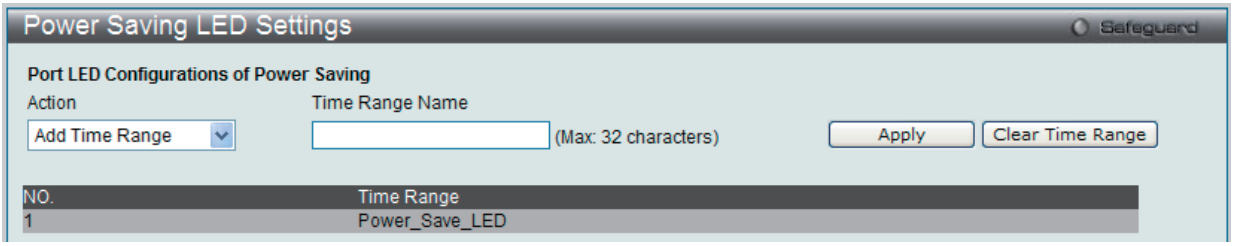


図 7-55　Power Saving LED Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Action	プルダウンメニューを使用して、スケジュールを追加または削除します。
Time Range Name	使用するスケジュール名を入力します。

「Apply」ボタンをクリックして行った変更を適用します。

「Clear Time Range」ボタンをクリックして、設定済みのすべてのタイムレンジを削除します。

Power Saving Port Settings（省電力ポート設定）

ポートにおける省電力スケジュールを追加または削除します。

Management > Power Saving > Power Saving 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。

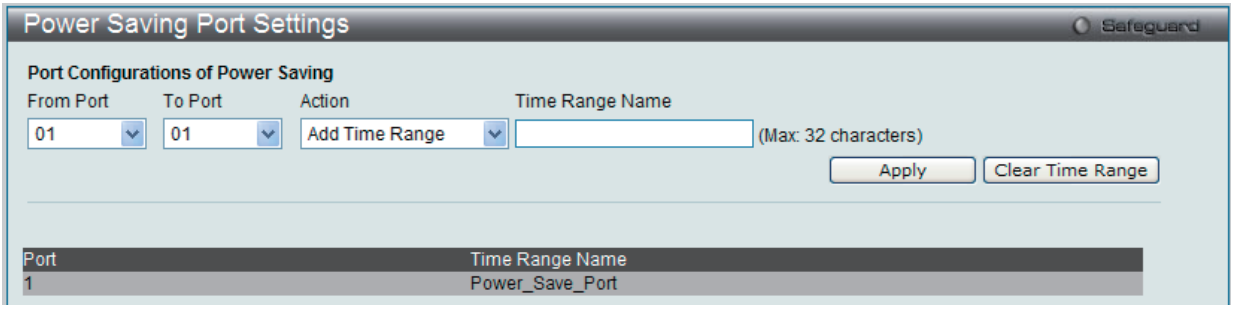


図 7-56　Power Saving Port Settings 画面

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	本設定に使用するポートリストを選択します。
Action	プルダウンメニューを使用して、スケジュールを追加または削除します。
Time Range Name	使用するスケジュール名を入力します。

「Apply」ボタンをクリックして行った変更を適用します。

「Clear Time Range」ボタンをクリックして、設定済みのすべてのタイムレンジを削除します。

第 8 章　VPN（VPN 設定）（EI モードのみ）

以下は、VPN の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
MPLS（マルチプロトコルスイッチング）	マルチプロトコルスイッチングの設定を行います。次のメニューがあります。 LDP（ラベル配布プロトコル設定）、MPLS Settings（MPLS 設定）、MPLS Static LSP Settings（MPLS スタティック LSP 設定）、MPLS Dynamic LSP Table（MPLS ダイナミック LSP テーブル）、MPLS FTN Table（MPLS FTN テーブル）、MPLS Interface Settings（MPLS インタフェース設定）、MPLS Class Map Settings（MPLS クラスマップ設定）、MPLS FEC EXP Settings（MPLS FEC EXP 設定）	95
VPWS（仮想専用線サービス設定）	仮想専用線サービスの設定を行います。次のメニューがあります。 VPWS Settings（VPWS 設定）	108

MPLS（マルチプロトコルラベルスイッチング）

Multiprotocol Label Switching (MPLS) は、TCP/IP プロトコルスタックのネットワーク層とデータリンク層間で動作し、従来の IP 転送をラベルスイッチングに置き換えるために使用されるプロトコルです。MPLS の最も強力な特徴は、データリンク層におけるどの特定プロトコルによっても制限されることはなく、すべてのレイヤ 2 メディアもパケットを転送できます。

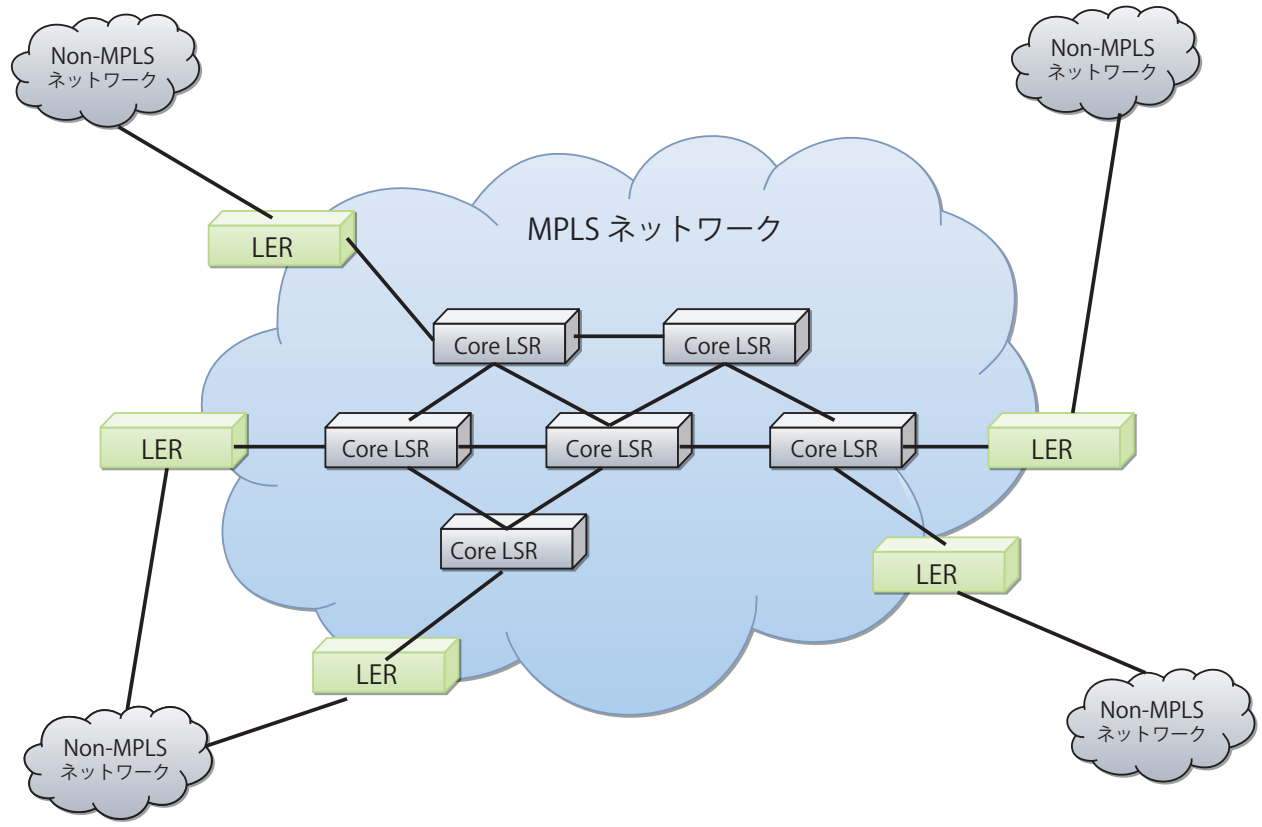


図 7-1　　MPLS ネットワーク構造

MPLS ネットワークでは、最も重要なノードを LSR（Label Switching Router: ラベルスイッチルータ）と呼びます。MPLS ドメインのエッジに位置している LSR は、LER（Label Edge Router: ラベルエッジルータ）として知られています。MPLS ドメイン内に位置している LSR は、Core LSR（コア LSR）と認識されます。LSR が別の LSR のパケットを受信する場合、送信側の LSR は上流の LSR と認識されます。受信側 LSR は送信側 LSR の下流の LSR として認識されます。

以下の例を参照ください。LSR B 経由で LSR A から LSR C にパケットを送信する場合、LSR A は LSR B の上流の LSR であり、LSR C は LSR B の下流の LSR となります。

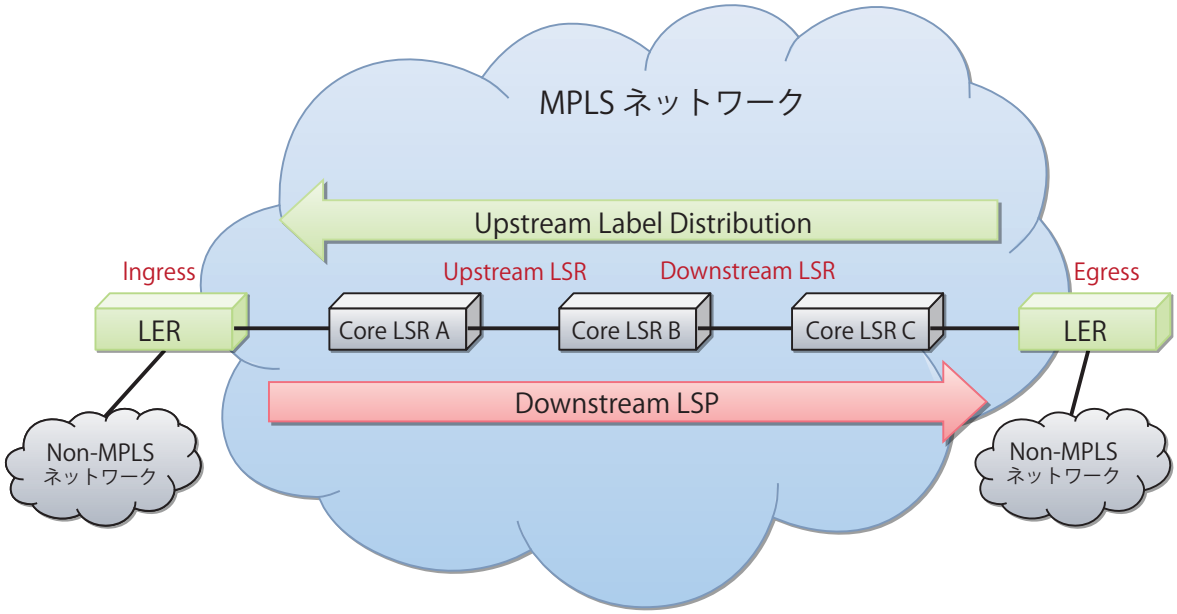


図 7-2　MPLS の説明図

パケットが MPLS ドメインに入る時、LER はパケットにラベルを追加する責任があります。また、パケットが MPLS ドメインから出る時、LER はラベルを削除する責任もあります。MPLS ドメイン内では、それらのラベルに基づいてパケットは転送されます。MPLS ドメインから入出力されるパケットのパスは、LSP（Label Switch Path: ラベルスイッチパス）として知られています。LSP は通常の環境下では単方向です。LSP における最初の LER は LSP のイングレスとして知られ、最後の LER は LSP のイーグレスとして知られています。LSP では 1 つのイングレスとイーグレスのみ存在可能です。

ラベルのないパケットがイングレスルータに入り、LSP に渡される必要があると、イングレス LER は最初に、パケットの FEC（Forwarding Equivalence Class: 等価転送クラス）を決定して、パケットの MPLS ヘッダに 1 つ以上のラベルを挿入します。その後、パケットは次の LSR に渡されます。ラベルは LDP（Label Distribution Protocol: ラベル配布プロトコル）を使用して LER と LSR 間で配布されます。

LDP は、MPLS ドメインを経由した特定な MPLS トンネルのイングレスとイーグレス LER 間に双方向の通信を定義します。LER は、LDP を使用し、MPLS ネットワークを通じてトラフィックを転送するのに使用される LSP データベースを構築して、維持します。そのため、2 つのピア LER は、効果的にトラフィックフローを制御するために絶えずこの情報を交換します。ラベルは LSP を通じて常にデータフローの逆方向に配布されます。つまり、ラベル配布は上流方向に行われます。LDP のメイン機能は FEC を分類して、ラベルを配布し、LSP を作成して維持することです。

- スタティック LSP
  上流 LSR ラベルの外向きラベルと下流 LSR の内向きなラベルを物理的に定義することによって、ユーザは手動で LSP を設定することができます。スタティック LSP は、LDP の必要はなく、管理パケットの交換なしで設定されます。本設定は、ほとんどデータオーバヘッドがなくて、ネットワークレイアウトが簡単で固定されている小規模ネットワークだけに適しています。

- ダイナミック LSP
  ユーザは LDP を使用して自動的に LSP を開始するように設定できます。さらに、MPLS ラベルを追加したルーティング機能を配布するために、Interior Gateway Protocol (IGP)、Border Gateway Protocol (BGP) および Resource Reservation Protocol (RSVP) を拡張できます。この設定は、大規模なネットワークに適しており、VPN サービスに使用されます。

MPLS パケットヘッダの構造：

図 7-3　MPLS パケットヘッダ

ラベルは以下のフィールドを含みます。

項目	説明
Label	これはラベルの値フィールドを示します。長さは 20 ビットです。
EXP	これは拡張に使用されるビットを示します。長さは 3 ビットです。通常、このフィールドは CoS（Class of Service）サービスに使用されます。
S	これはラベルスタック値の末尾を示します。長さは 1 ビットです。この値が設定される場合（つまり、「1」に設定）、これはこのエントリがラベルスタックの末尾にあることを意味します。
TTL	これは生存可能時間（TTL: Time-To-Live）の値を示します。長さは 8 ビットです。本フィールドは IP パケットの TTL と同様です。ラベルは常にデータリンク層とネットワーク層間でカプセル化されます。これは、カプセル化されたラベルがデータリンク層で利用可能なすべてのプロトコルをサポートすることを意味します。

LDP（ラベル配布プロトコル設定）

LDP Settings（LDP 設定）

スイッチに LDP 設定を行います。

VPN > MPLS > LDP > LDP 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。

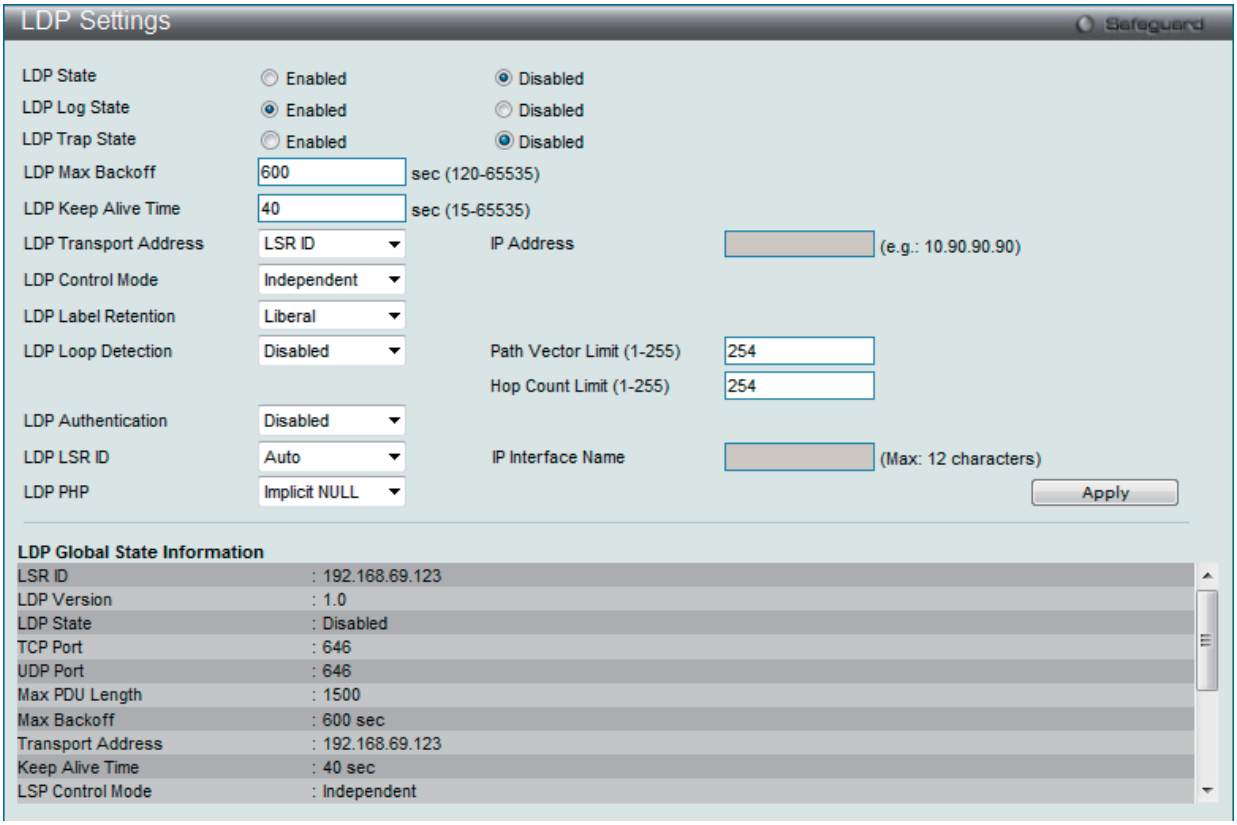


図 7-4　LDP Settings 画面

以下の項目を使用して、設定します。

項目	説明
LDP State	指定インタフェースの LDP の状態を指定します。MPLS が有効である必要があります。有効でないと LDP が無効になるということに注意してください。
LDP Log State	LDP ログの状態を有効または無効にします。
LDP Trap State	LDP トラップの状態を有効または無効にします。
LDP Max Backoff	最大のバックオフ時間を入力します。LDP バックオフメカニズムは、互換性なく設定された 2 つの LSR が、セッション確立失敗という無限のシーケンスに陥ることを防ぎます。セッション確立の試みが非互換性のために失敗するなら、アクティブな LSR は次の試みを遅らせて、セッション確立を再試行します。遅延は 15 秒で始まり、最大のバックオフ遅延に到達するまで、各連続する失敗に伴い指数関数的に増加します。セッションが確立されない場合に、トラップまたはログ状態が有効であると、LDP はセッション確立失敗を通知するために SNMP サーバにトラップまたはログを送信します。この値は 120-65535（秒）である必要があります。
LDP Keep Alive Time	LDP セッションキープアライブ時間を入力します。LDP は各ピアセッションのためにキープアライブタイマを保持します。キープアライブタイマがピアからの LDP PDU の受信なしで期限が切れると、LDP はピアが失敗したと結論づけて、LDP セッションを終えます。各 LSR は、セッションをアクティブに保つために一定の間隔を置いて LDP ピアにキープアライブメッセージを送信します。この値は 15-65535（秒）である必要があります。
LDP Transport Address	使用する LDP トランスポートアドレスモードを選択します。トランスポートアドレスは、LDP TCP 接続を確立するのに使用されます。初期値では、LSR ID はトランスポートアドレスとしてインタフェースのすべてに使用されます。特定の IP アドレスにトランスポートアドレスを選択すると、このアドレスがトランスポートアドレスとしてすべてのインタフェースに使用されます。インタフェースにトランスポートアドレスを設定すると、各インタフェースの IP アドレスがトランスポートアドレスとして使用されます。LSR ID を選択することで、LSR ID がトランスポートアドレスとして使用されるように指定します。
LDP Control Mode	LSP 制御モードを選択します。 • Independent LSP Control（独立 LSP 制御）- 各 LSR は独自にラベルを FEC に割り当てて、ラベル配布ピアにその割り当てを配布します。 • Ordered LSP Control（順次 LSP 制御）- その FEC のためのイーグレス LSR である場合、またはその FEC のネクストホップから FEC へのラベル割り当てを既に受信している場合にだけ、LSR はラベルを FEC に割り当てます。
LDP Label Retention	LDP ラベル保持モードを選択します。 • Conservative - ラベル配布方式が Downstream-Unsolicited（DU）で、ラベル保持モードが「Conservative」である場合、LSR が、（その FEC のネクストホップでない）LSR からラベル割り当てを一度受信すると、割り当てを破棄します。 • Liberal - ラベル保持モードが「Liberal」であると、その割り当てを維持します。これは、ネクストホップに変更があった場合に LSP の迅速なセットアップを補助します。
LDP Loop Detection	LDP ループ検知モードを有効または無効にします。LDP ループ検知メカニズムは、ループする LSP を検知するためにラベル要求とラベルマッピングメッセージによって運ばれた Path Vector および Hop Count TLV を利用します。
Path Vector Limit	使用するパスベクトルの制限値を入力します。この値は 1-255 である必要があります。
Hop Count Limit	使用するホップカウントの制限値を入力します。この値は 1-255 である必要があります。
LDP Authentication	LDP 認証オプションを有効または無効にします。認証が有効であると、LSR は MD5 アルゴリズムを適用して、ピアに送信される TCP セグメントのために MD5 ダイジェストを計算します。この計算は TCP セグメントと同様にピアパスワードを利用します。LSR が MD5 ダイジェストと共に TCP セグメントを受信すると、MD5 ダイジェストを算出し、自身の記録を使用して、ダイジェストを受信したダイジェストと比較することで、セグメントを有効にします。比較でエラーとなると、セグメントは送信側に応答せずに破棄されます。LSR はパスワードが設定されていない LSR からの LDP Hello メッセージをすべて無視します。
LDP LSR ID	使用する LDP LSR ID モードを選択します。LSR ID はインタフェースの IPv4 アドレスであり、MPLS ネットワークで LSR を特定するのに使用されます。LSR ID に推奨されるインタフェースはループバックインタフェースです。LSR ID を「Auto」に設定すると、この決定は以下のルールに基づきます。ループバックインタフェースが設定されると、LSR ID はループバックインタフェースの IP アドレスに設定されます。複数のループバックインタフェースが設定されると、最も高い IP アドレスを持つループバックが使用されます。ループバックインタフェースが設定されないと、LSR ID は物理インタフェースで最も高い IP アドレスに設定されます。IP インタフェースを選択および入力して、LSR ID として使用する IP インタフェースを指定します。
LDP PHP	PHP（LDP Penultimate Hop Popping）の動作を選択します。LSR を「egress」に、PHP を「Implicit NULL」（暗黙 NULL）に設定する場合、Implicit NULL ラベルを上流（Penultimate Hop: 最後から 2 番目のホップ）に配布します。その後、上流は PHP を行います。Penultimate Hop に配布されたラベルを「Explicit NULL」に設定すると、Penultimate Hop はそれをポップ（ラベル削除）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。

LDP Statistic Table（LDP 統計情報テーブル）

LDP 統計情報をクリアします。

VPN > MPLS > LDP > LDP Statistic 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。

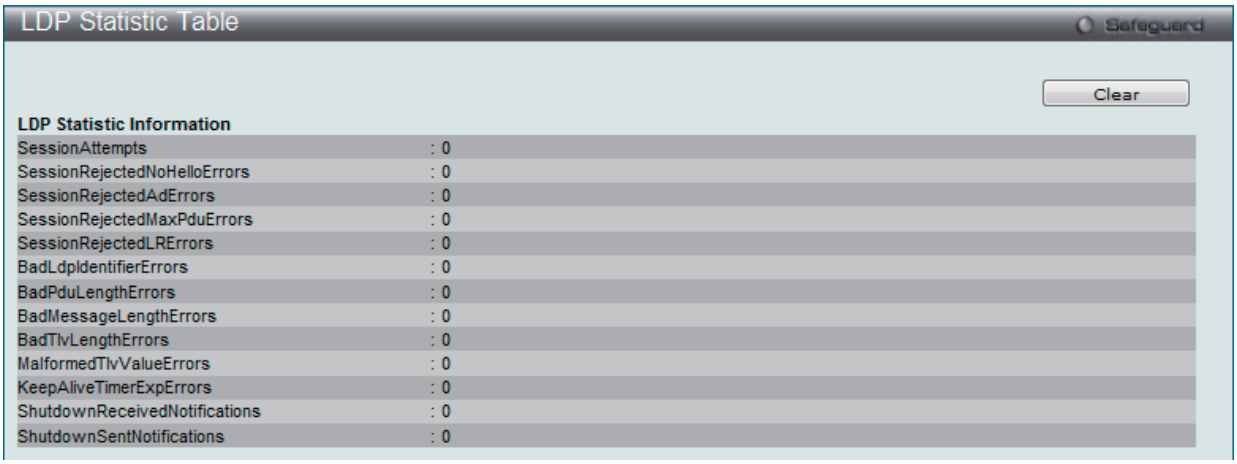


図 7-5　LDP Statistic Table 画面

「Clear」ボタンをクリックして、表示されたすべての情報をクリアします。

LDP IP Interface Settings（LDP IP インタフェース設定）

特定のインタフェースに LDP パラメータを設定します。

VPN > MPLS > LDP > LDP IP 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。

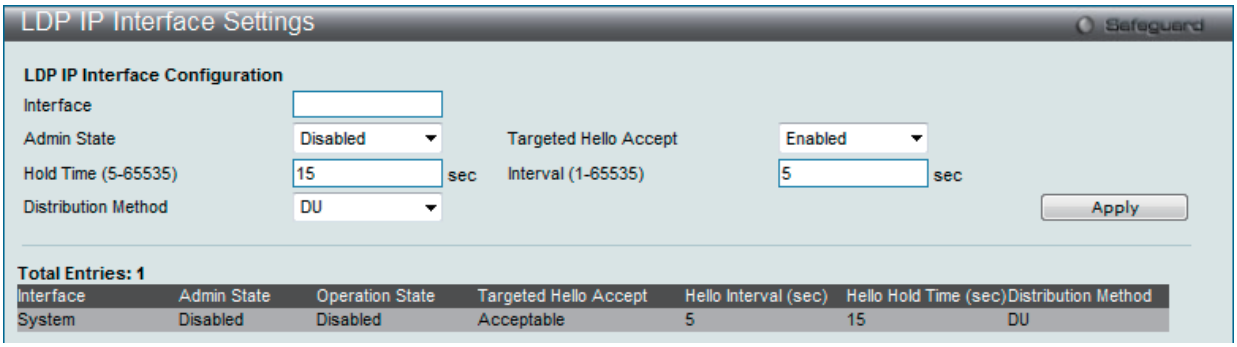


図 7-6　LDP IP Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface	使用する IP インタフェース名を入力します。12 文字以内で指定します。
Admin State	指定インタフェースの LDP の admin 状態を有効または無効にします。MPLS が有効である必要があります。有効でないと LDP が無効になるということに注意してください。
Target Hello Accept	Target Hello メッセージを許可または拒否します。Target Hello メッセージを許可すると、インタフェースは受信した Target Hello メッセージに応答します。許可しないと、受信した Target Hello メッセージを拒否します。
Hold Time	リンク保持時間を入力します。LDP は、直接接続する Neighbor を発見するために定期的に Link Hello メッセージを送信します。その後、LDP は各検出 Neighbor の保持タイマを維持します。タイマが Neighbor から Hello メッセージの受信なしで期限切れとなると、LDP は Neighbor がエラー状態であると見なします。この値は 5-65535(秒) である必要があります。
Interval	使用する間隔を入力します。この値は 1-65535 である必要があります。
Distribution Method	使用する LDP ラベル配布方式を選択します。 • DU - 配布モードを「Downstream-Unsolicited」に設定します。 • DoD - 配布モードを「Downstream-on-Demand」に設定します。

「Apply」ボタンをクリックして行った変更を適用します。

LDP Targeted Peer Settings（LDP ターゲットピアの設定）

LDP のターゲットとするピアを設定します。

VPN > MPLS > LDP > LDP Targeted Peer 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。

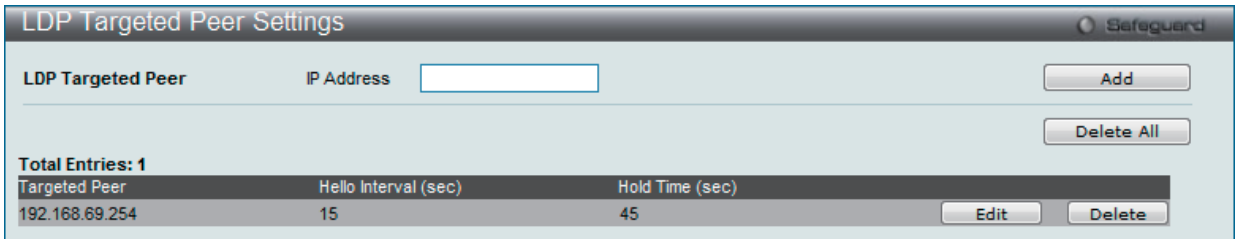


図 7-7　LDP Targeted Peer Settings 画面

エントリの新規登録

LDP のターゲットとするピアを追加するためには、上記画面に情報を入力し、「Add」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
IP Address	使用するターゲットピアの IP アドレスを入力します。ターゲットとするピアの LSR ID とします。
Hello Interval	「Edit」ボタンをクリックし、Target Hello メッセージを送信する間隔を入力します。この値は 5-65535(秒) である必要があります。
Hold Time	「Edit」ボタンをクリックし、Target Hello の保持時間を入力します。この値は 15-65535(秒) である必要があります。

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ます。
2. エントリを編集します。
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。

LDP Neighbor Table（LDP Neighbor テーブル）

LDP に発見されたすべての近接を表示します。

VPN > MPLS > LDP > LDP Neighbor 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。

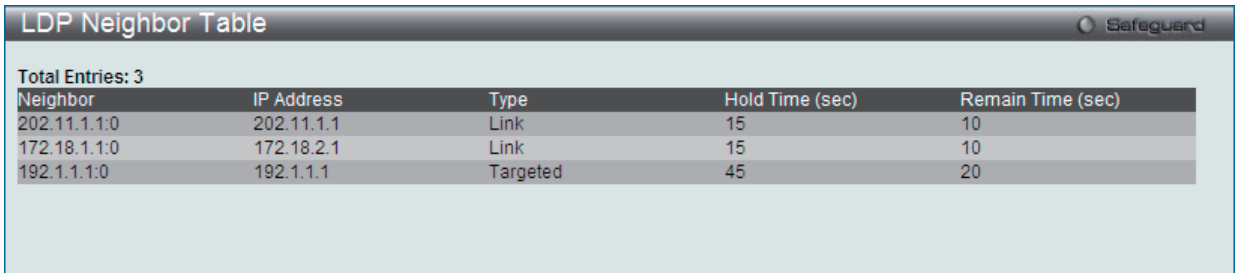


図 7-8　LDP Neighbor Table 画面

LDP Peer Table（LDP ピアテーブル）

LDP ピアの情報を表示します。

VPN > MPLS > LDP > LDP Peer 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。

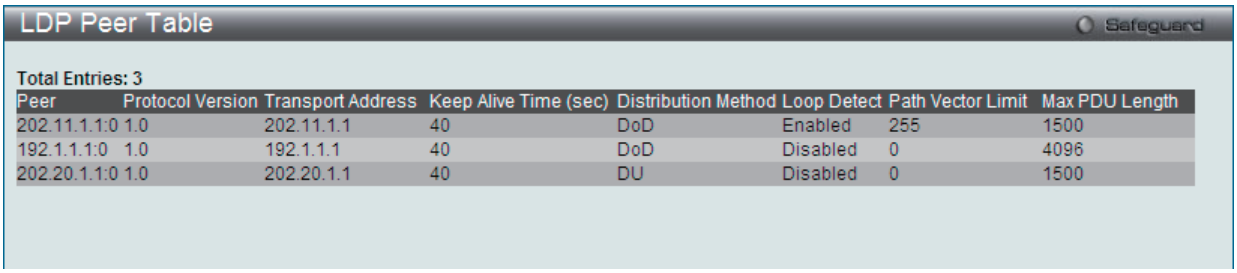


図 7-9　LDP Peer Table 画面

LDP Peer Password Settings（LDP ピアパスワード設定）

LDP ピアのパスワードを設定します。

VPN > MPLS > LDP > LDP Peer 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。

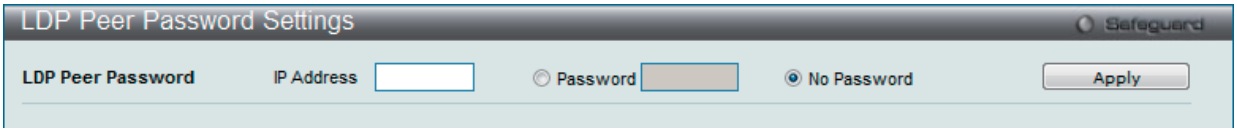


図 7-10　LDP Peer Password Settings 画面

以下の項目を設定します。

項目	説明
IP Address	使用するピアの IP アドレスを入力します。IP アドレスはピアの LSR ID とします。
Password	選択して、使用するピアのパスワードを入力します。このパスワードは 32 文字以内で指定します。
No Password	ピアパスワードにはパスワードを設定しません。

「Apply」ボタンをクリックして行った変更を適用します。

LDP Session Table（LDP セッションテーブル）

すべての LDP セッションを表示します。

VPN > MPLS > LDP > LDP 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。

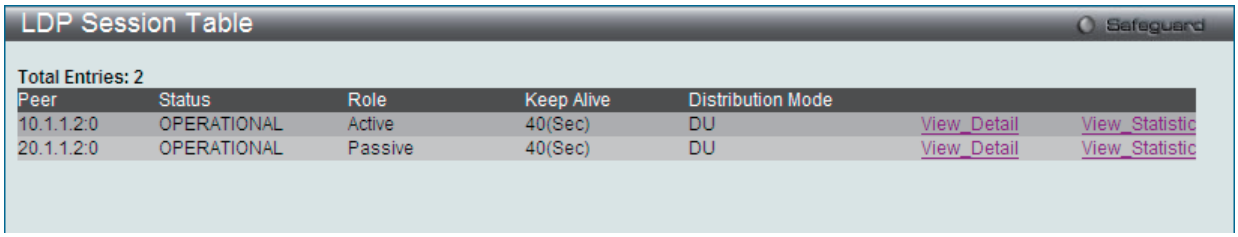


図 7-11　LDP Session Table 画面

エントリの詳細表示

エントリに関するより詳細な情報を表示します。

「View Detail」リンクをクリックして、以下の画面を表示します。

図 7-12　LDP Session Table 画面 - View Detail

エントリの統計情報表示

エントリに関するより詳細な統計情報を表示します。

「View Statistic」リンクをクリックして、以下の画面を表示します。

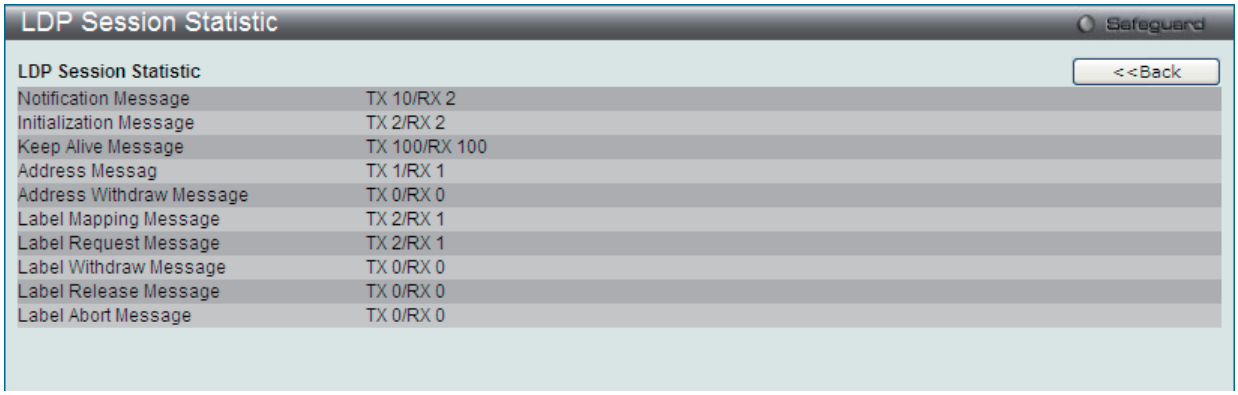


図 7-13　LDP Session Table 画面 - View Statistic

「<<Back」をボタンをクリックして前のページに戻ります。

LDP Binding Table（LDP バインディングテーブル）

すべての LDP ラベルバインディング情報を表示します。

VPN > MPLS > LDP > LDP Binding 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。

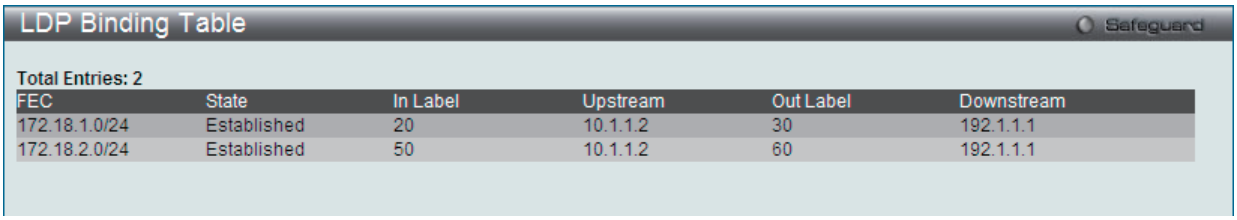


図 7-14　LDP Binding Table 画面

MPLS Settings（MPLS 設定）

MPLS 機能をグローバルに有効または無効にします。また、Trust EXP、MPLS Log、および MPLS Trap の状態を設定することができます。

VPN > MPLS > MPLS 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 7-15　MPLS Settings 画面

以下の項目を設定します。

項目	説明
MPLS State	MPLS 機能をグローバルに有効または無効にします。
Trust EXP	MPLS Trust EXP オプションを有効または無効にします。EXP が信頼されると、内向きなラベルの EXP 値は入力パケットの QoS として使用されます。EXP が信頼されないと、EXP 値は QoS に使用されません。
Log	MPLS ログの状態を有効または無効にします。
Trap	MPLS トラップの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。

MPLS Static LSP Settings（MPLS スタティック LSP 設定）

MPLS のスタティック LSP 設定を行います。

VPN > MPLS > MPLS Static LSP 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。

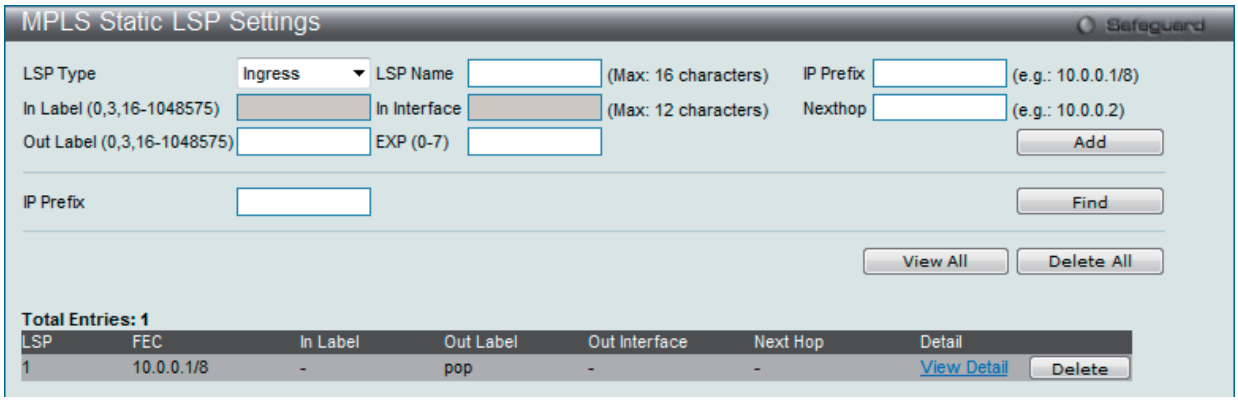


図 7-16　MPLS Static LSP Settings 画面

エントリの新規登録

MPLS のスタティック LSP 設定を追加するためには、上記画面に情報を入力し、「Add」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
LSP Type	スタティックな Egress LSP またはスタティックな Ingress LSP の確立を選択します。
LSP Name	使用する LSP 名を入力します。16 文字以内で指定します。
IP Prefix	LSP の IP プレフィックス FEC アドレスを入力します。特定の FEC を LSP にマップします。
In Label	使用する内向きラベルの値を入力します。
In Interface	使用する内向きインタフェースの名前を入力します。12 文字以内で指定します。
Nexthop	使用するネクストホップの IP アドレスを入力します。
Out Label	使用する外向きのラベル値を入力します。
EXP	使用する EXP 値を入力します。初期値では、EXP は入力パケットの QoS に従って設定されます。EXP が指定されると、指定値に従って、外向きラベルの EXP が設定されます。この値は 0-7 である必要があります。

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。「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

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。

エントリの詳細表示

エントリに関するより詳細な情報を表示します。

「View Detail」リンクをクリックして、以下の画面を表示します。

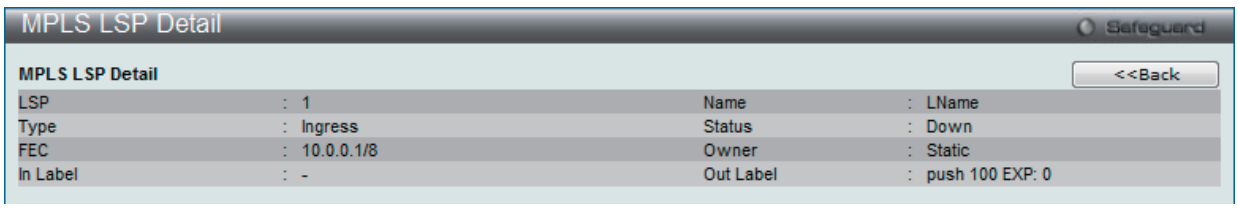


図 7-17　MPLS LSP Detail 画面

「<<Back」をボタンをクリックして前のページに戻ります。

MPLS Dynamic LSP Table（MPLS ダイナミック LSP テーブル）

ダイナミックな MPLS LSP エントリを検索して、表示します。

VPN > MPLS > MPLS Dynamic LSP 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。

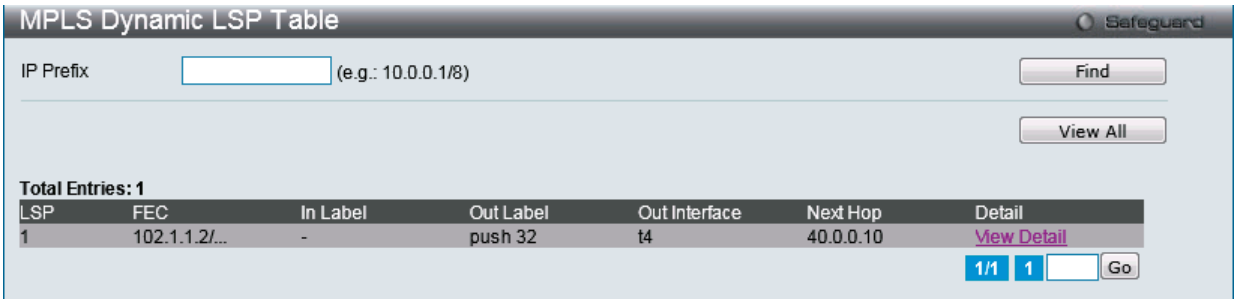


図 7-18　MPLS Dynamic LSP Table 画面

以下の項目があります。

項目	説明
IP Prefix	LSP の IP プレフィックス FEC アドレスを入力します。

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。「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。

エントリの詳細表示

エントリに関するより詳細な情報を表示します。

「View Detail」リンクをクリックして、以下の画面を表示します。

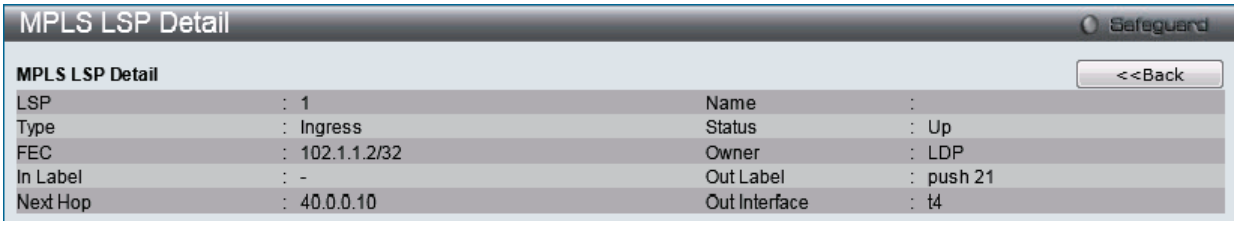


図 7-19　MPLS Dynamic LSP Table Detail 画面

「<<Back」をボタンをクリックして前のページに戻ります。

MPLS FTN Table（MPLS FTN テーブル）

Next-Hop Label Forwarding Entry（NHLFE）は、MPLS パケット転送を誘導するのに使用されます。
NHLFE は次の情報を含んでいます。：トンネル ID、外向きインタフェース、ネクストホップ、外向きラベル、およびラベル操作。

VPN > MPLS > MPLS FTN 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。

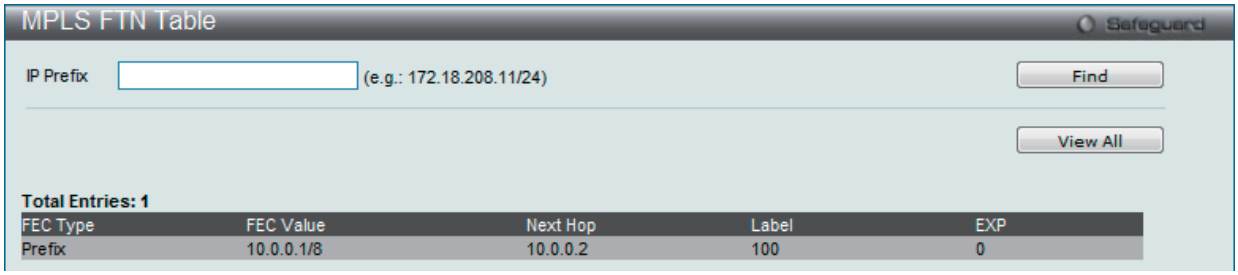


図 7-20　MPLS FTN Table 画面

以下の項目があります。

項目	説明
IP Prefix	LSP の IP プレフィックス FEC アドレスを入力します。

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。「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。

MPLS Interface Settings（MPLS インタフェース設定）

特定のインタフェースにおける MPLS を有効または無効にします。

VPN > MPLS > MPLS 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。

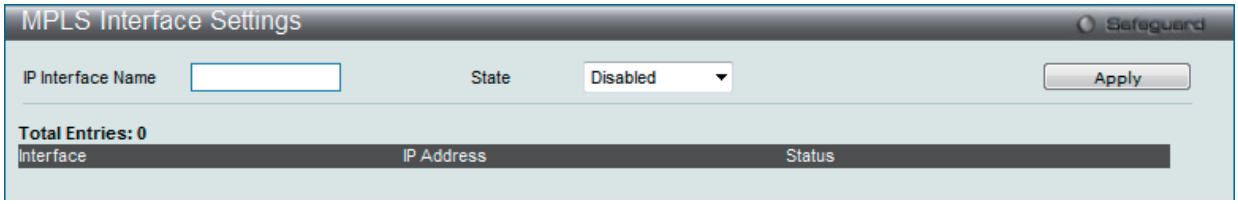


図 7-21　MPLS Interface Settings 画面

以下の項目を設定します。

項目	説明
IP Interface Name	使用する IP インタフェース名を入力します。12 文字以内で指定します。
State	MPLS IP インタフェースを有効または無効にします。初期値では、状態はすべてのインタフェースで無効です。

「Apply」ボタンをクリックして行った変更を適用します。

MPLS Class Map Settings（MPLS クラスマップ設定）

EXP と CoS 間のマッピングを設定します。CoS 7 はシステムのために予約されています。

以下の表は、EXP と CoS 間のマッピングの初期値を示しています。

EXP	0	1	2	3	4	5	6	7
CoS	2	0	1	3	4	5	6	6

VPN > MPLS > MPLS Class 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。

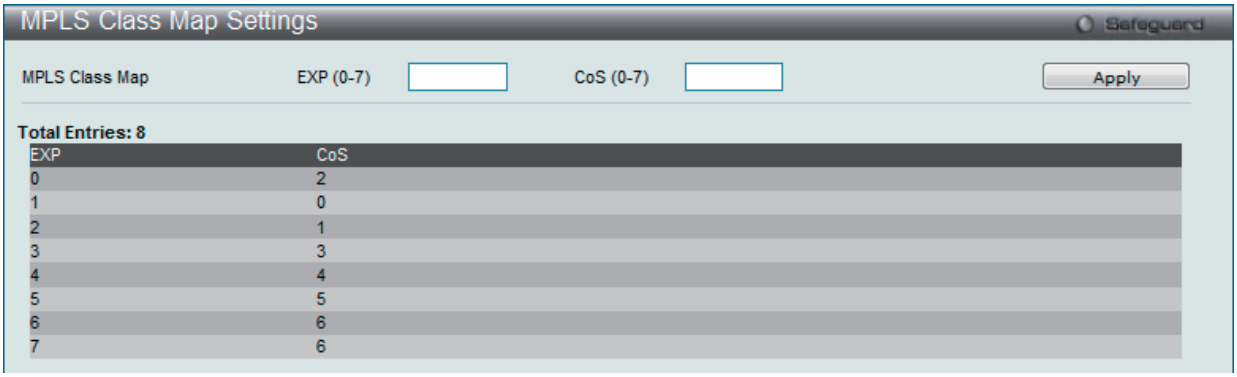


図 7-22　MPLS Class Map Settings 画面

以下の項目を設定します。

項目	説明
EXP	CoS にマップする EXP 値を入力します。この値は 0-7 である必要があります。
CoS	使用する CoS 値を入力します。この値は 0-7 である必要があります。

「Apply」ボタンをクリックして行った変更を適用します。

MPLS FEC EXP Settings（MPLS FEC EXP 設定）

FEC の EXP 割り当てを設定します。

EXP を LSP を作成することで明示的に割り当てないと、指定 FEC の外向き EXP は定義済み EXP 値に従って設定されます。初期値では、すべての FEC に対する外向きラベルの EXP 値は、入力パケットの QoS に従って設定されます。

VPN > MPLS > MPLS FEC EXP 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。

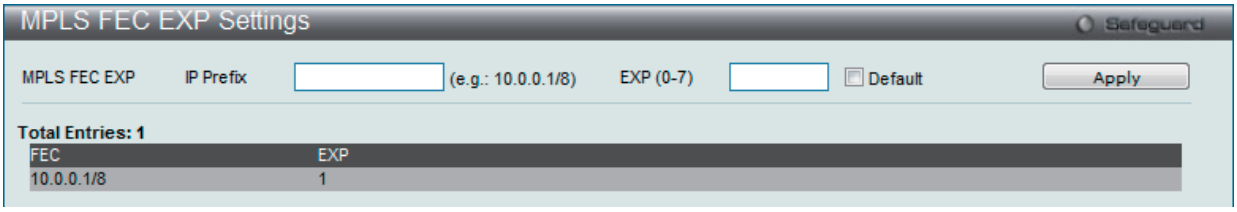


図 7-23　MPLS FEC EXP Settings 画面

以下の項目を設定します。

項目	説明
IP Prefix	使用する IP プレフィックスの FEC アドレスを入力します。
EXP	FEC に対する外向きラベルにおける EXP 値を入力します。この値は 0-7 である必要があります。「Default」を選択すると、入力パケットの QoS に従って EXP 値を設定します。そうでない場合、指定値に従って設定します。

「Apply」ボタンをクリックして行った変更を適用します。

VPWS（仮想専用線サービス設定）

Virtual Private Wire Service (VPWS) は、プロバイダネットワークにおけるカスタマサイト間にレイヤ 2 のポイントツーポイント仮想回線接続を提供する L2VPN ソリューションです。VPWS は IP と L2VPN 間のプロバイダのコアネットワーク基幹の共有を可能とし、プロバイダサービスの提供にかかるコストを削減します。VPWS のトンネリングメカニズムは、トランスポート層の MPLS のように、どんなトンネリングプロトコルも使用できます。

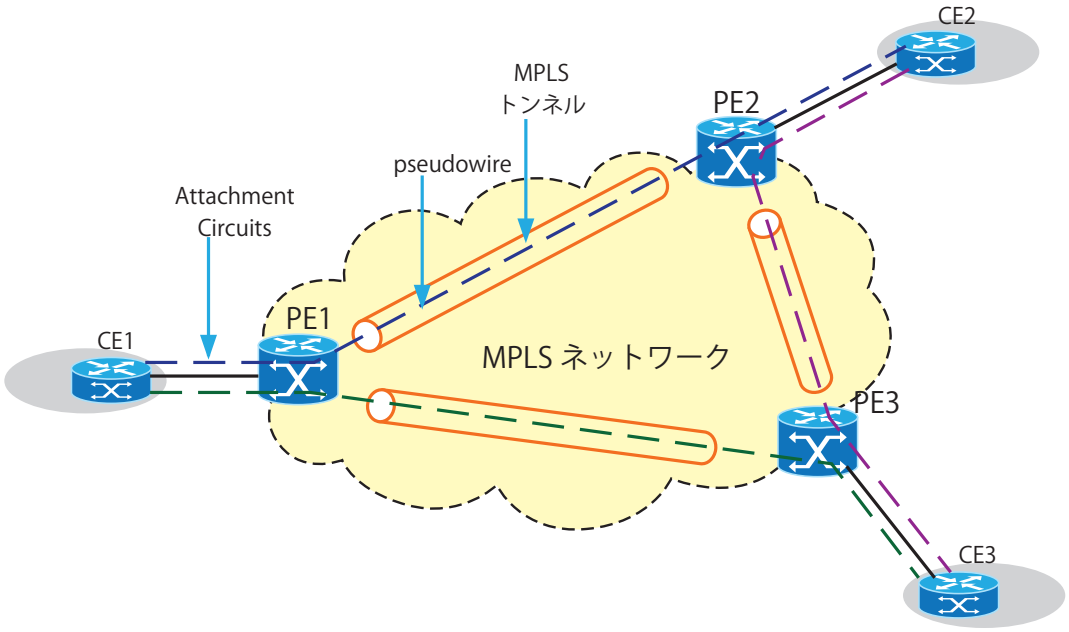


図 7-24　MPLS ベースの VPWS の図

上の図では、MPLS ネットワークはパケット交換網（PSN）です。各 CE（Customer Edge: カスタマエッジ）デバイスは AC（Attachment Circuit: 接続回線）を経由して PE（Provider Edge: プロバイダエッジ）に接続します。PE はローカル情報に基づいて PW（Pseudo-Wire: 疑似配線）と AC 間に 1 対 1 のマッピングを行います。PW はどのレイヤ 2 技術を持つ 2 つのノードの相互接続も許可するパケット交換網上にエミュレートされたポイントツーポイント接続です。

PW に必要とされる機能には、イングレスポートに到着して、IP パスまたは MPLS トンネルを通過して転送する Service-Specific ビットストリーム、セル、または PDU のカプセル化が含まれます。PW は、特有のサービスの動作と特性をエミュレートするために以下の機能を提供します。

- Service-Specific PDU または PE 行きのポートに到着する回線データ（論理的または物理的）のカプセル化。
- PSN トンネルを通過するカプセル化されたデータの送信。
- PSN トンネルエンドポイントによって使用される PW 識別子の交換、および / または、配布を含む PW の確立。
- PW の境界におけるサービスのシグナリング、タイミング、順序、または他のアスペクトを管理します。Service-Specific 状態とアラームの管理。

1 つ以上の PW が PE から別の PE まで MPLS トンネルにおいて運ばれます。どのフレームもイングレス AC、PW、イーグレス AC の順に移動します。この特定の組合せは 2 つの CE デバイス間に仮想回線を形成します。

Virtual Private Network (VPN)
VPN は、インターネットのようなパブリックネットワークを通過するリンクを包括するプライベートネットワークの拡張です。VPN は、ポイントツーポイントのプライベートリンクのプロパティをエミュレートする方法でパブリックネットワークを通過する 2 台のコンピュータ間のデータ送信を可能にします。

Virtual Private Wire Service (VPWS)
VPWS は、プロバイダネットワーク上のカスタマサイト間にレイヤ 2 のポイントツーポイント仮想回線接続を提供する VPN サービスです。

Packet Switched Network (PSN)
PSN は、VPN サービスをサポートするトンネルがセットアップされているネットワークです。このスイッチでは、PSN は MPLS ネットワークです。

Customer Edge Device (CE)
CE はカスタマネットワークにあり、プロバイダネットワークに直接する 1 つ以上のインタフェースを持っています。

Provider Edge (PE)
PE はサービスプロバイダネットワークにあり、1 つ以上の CE をネットワークに接続します。

Provider Router (PR)
PR はサービスプロバイダネットワークにあり、ファストパケットスイッチングを提供します。

Attachment Circuit (AC)
AC は CE を PE に接続する物理的または仮想的な回線です。AC を識別するために、イーサネットポート、VLAN または (ポート、VLAN の) ペアを使用できます。

Pseudo-Wire (PW)

PW は、1 つの PE から PSN 上の別の PE までエミュレートされた回線の重要な要素を送るメカニズムです。PW-ID と PW- タイプは、Pseudo-Wire を識別するのに使用されます。PW-ID は non-zero、32 ビット、接続 ID です。両方のエンドポイントでは PW-ID および PW- タイプを同じとします。

Tunnel Label

Tunnel Label は、カプセル化されたイーサネットパケットがトンネル LSP を通じて MPLS ネットワークを通過することを許可するのに使用されます。

VC Label

VC Label は、単一のトンネルに複数の PW を送ることができるように、de-multiplexer フィールドとして使用されます。イングレスとイーグレス PE、LDP シグナリング、またはスタティック設定のいずれかを使用することによって、特定の VC Label 値に同意する必要があります。VC Label を MPLS ラベルスタックの最後のラベルとします。QoS 情報を送信するために VC Label の EXP フィールドを使用できます。イングレス PE は、VC Label の TTL 値を 2 に設定する必要があります。

VPWS Settings（VPWS 設定）

VPWS 設定を行います。

VPN > VPWS > VPWS 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。

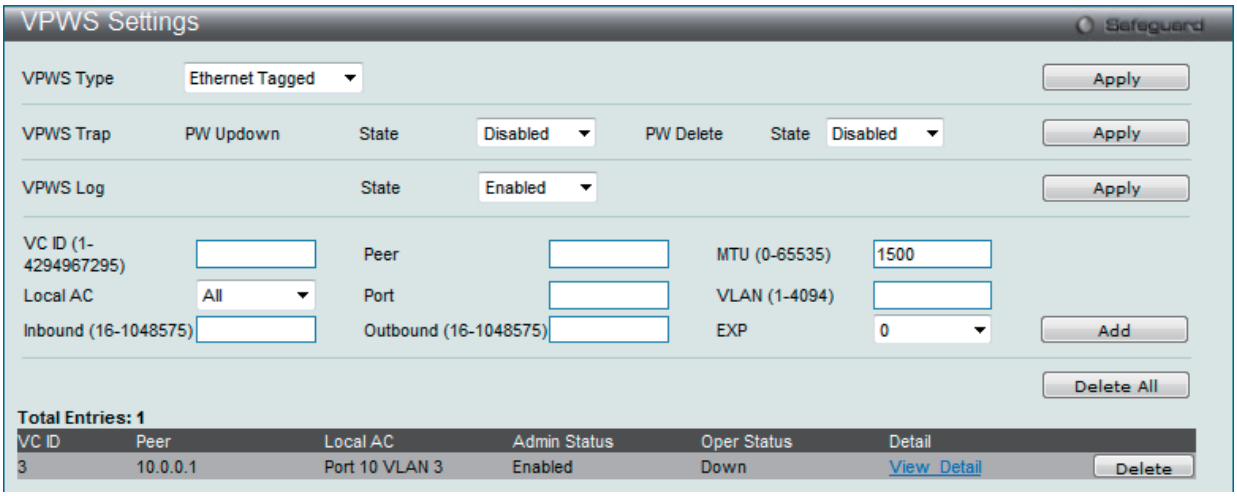


図 7-25　VPWS Settings 画面

以下の項目を設定します。

項目	説明
VPWS Type	使用する VPWS タイプを選択します。VPWS タイプは、異なる VPWS サービスを区別するために使用されます。 イーサネットサービスには定義済みの 2 つの VPWS タイプ（Ethernet Raw、Ethernet Tagged）があります。 VPWS タイプはグローバルに設定されます。すべての PW は Ethernet Raw モードで動作し、S- タグは Ethernet Raw タイプ VPWS に対する PW には送信されません。一方の代替手段は、Ethernet tagged モードで動作する PW で、PW に送信されたあらゆるフレームが Ethernet tagged タイプの VPWS に S- タグを持つ必要があります。VPWS タイプは VPWS エンドの両側で同じにする必要があります。
VPWS Trap	VPWS トラップ状態を有効または無効にします。
PW Updown State	有効な場合、PW のアップまたはダウンのイベントがあるとトラップが送信されます。無効な場合、PW のアップまたはダウンのイベントに関してトラップは送信されません。
PW Delete State	有効な場合、削除イベントがあるとトラップが送信されます。無効な場合、削除イベントに関するトラップは送信されません。
VPWS Log State	VPWS ログの状態を有効または無効にします。
VC ID	使用する VC ID を入力します。この値は 1-4294967295 である必要があります。
Peer	PW のピア IP アドレスを入力します。ピア IP アドレスはその LSR ID とします。
MTU	リモートピアに通知されるローカルな CE PE リンクの MTU 値を入力します。MTU に 0 を指定すると、LDP はローカルな MTU に通知されません。MTU はローカルとリモートの両方で同じである必要があり、違う場合、PW は成功しません。指定しないと、MTU の初期値を使用します。MTU 値の初期値は 1500 です。この値は 0-65535 である必要があります。
Local AC	使用する Local AC 方式を選択しします。オプションを All、Port、および VLAN から選択します。
Port	Local AC が Port または All（Port、VLAN）によって識別される場合、PW の AC のイングレスのポート番号を入力します。
VLAN	Local AC が VLAN または All（Port、VLAN）によって識別される場合、PW の AC のイングレスの VLAN ID を入力します。
Inbound	内向き VC ラベルを入力します。この値は 16-1048757 である必要があります。
Outbound	使用する外向きの VC ラベル値を入力します。この値は 16-1048757 である必要があります。
EXP	使用する VC の EXP 値を入力します。指定しないと、すべての VC に対する外向きラベルの EXP 値は、入力パケットの QoS に従って設定されます。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの新規登録

VPWS エントリを追加するためには、上記画面に情報を入力し、「Add」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。

エントリの詳細表示

エントリに関するより詳細な情報を表示します。

「View Detail」リンクをクリックして、以下の画面を表示します。

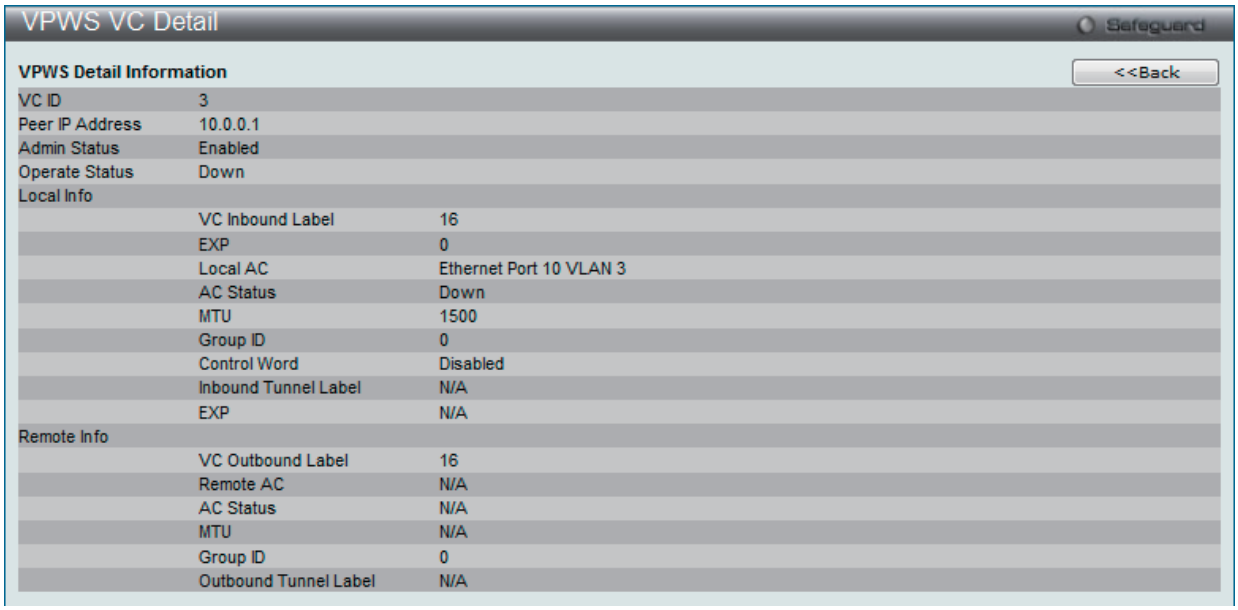


図 7-26　VPWS VC Detail 画面

「<<Back」をボタンをクリックして前のページに戻ります。

第 9 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）	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）、Private VLAN Settings（プライベート VLAN 設定）、PVID Auto Assign Settings（PVID 自動割り当て設定）、Subnet VLAN（サブネット VLAN）、VLAN Counter Settings（VLAN カウンタの設定）、Voice VLAN（音声 VLAN）、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）	117
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）、Double Tagged VLAN Translation Settings（ダブルタグ VLAN 変換の設定）、VLAN Translation Port Mapping Settings（VLAN 変換ポートのマッピング設定）、VLAN Translation Profile List（VLAN 変換プロファイルリスト）	135
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。	141
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）	142
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）	150
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）	153
L2 Multicast Control（L2 マルチキャストコントロール）	IGMP プロキシ、MLD プロキシ、IGMP Snooping、MLD Snooping の設定を行います。以下のメニューがあります。 IGMP Proxy（IGMP プロキシ）、IGMP Snooping（IGMP Snooping の設定）、MLD Proxy（MLD プロキシ）、MLD Snooping（MLD Snooping 設定）、Multicast VLAN（マルチ VLAN）、IP Multicast VLAN Replication（IP マルチキャスト VLAN レプリケーション）	157
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）	187
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。	194
Local Loopback Port Settings（ローカルループバックポート設定）	ローカルループバックポートのパラメータを設定します。	197
LLDP（LLDP 設定）	LLDP 設定を行います。以下のメニューがあります。 LLDP（LLDP 設定）、LLDP-MED（LLDP-MED 設定）	198
NLB FDB Settings（NLB FDB 設定）	NLB 機能を設定します。	208

VLAN（802.1Q 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が、必ずしもそうである必要はありません。

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。

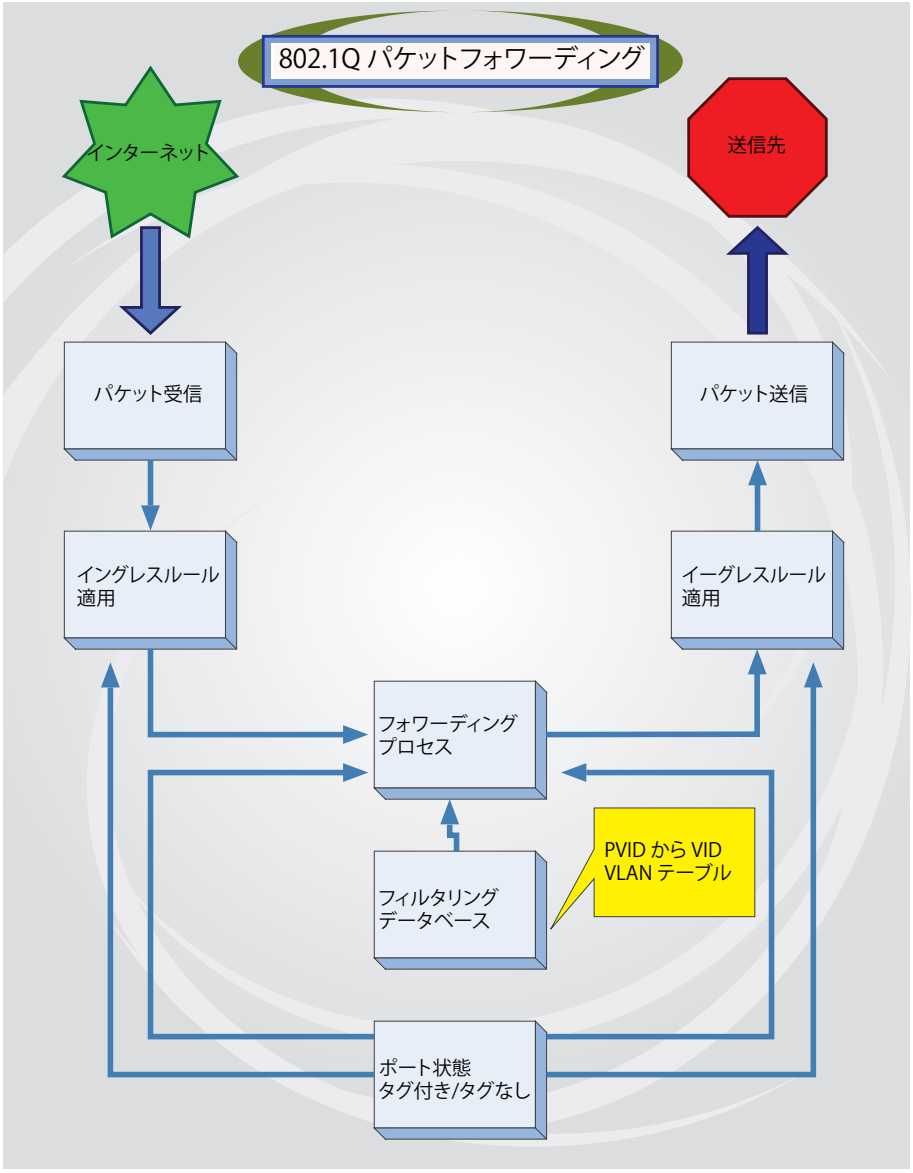


図 9-1　IEEE 802.1Q パケットフォワーディング

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 0×8100 になります。つまり、パケットの EtherType フィールドが 0×8100 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。

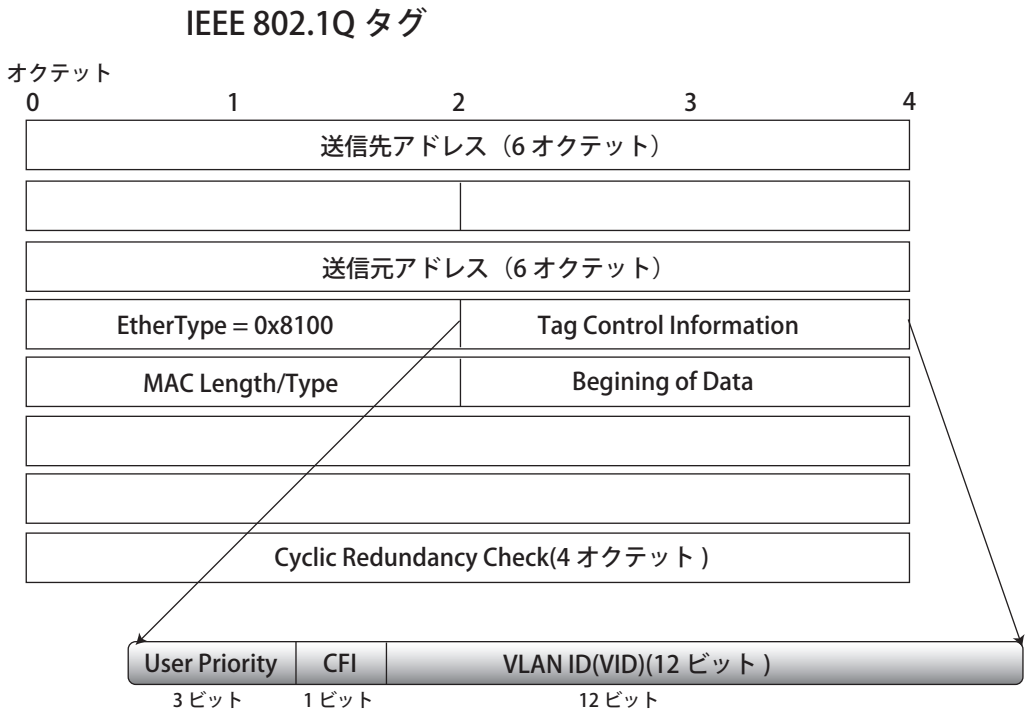


図 9-2　IEEE 802.1Q タグ

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。

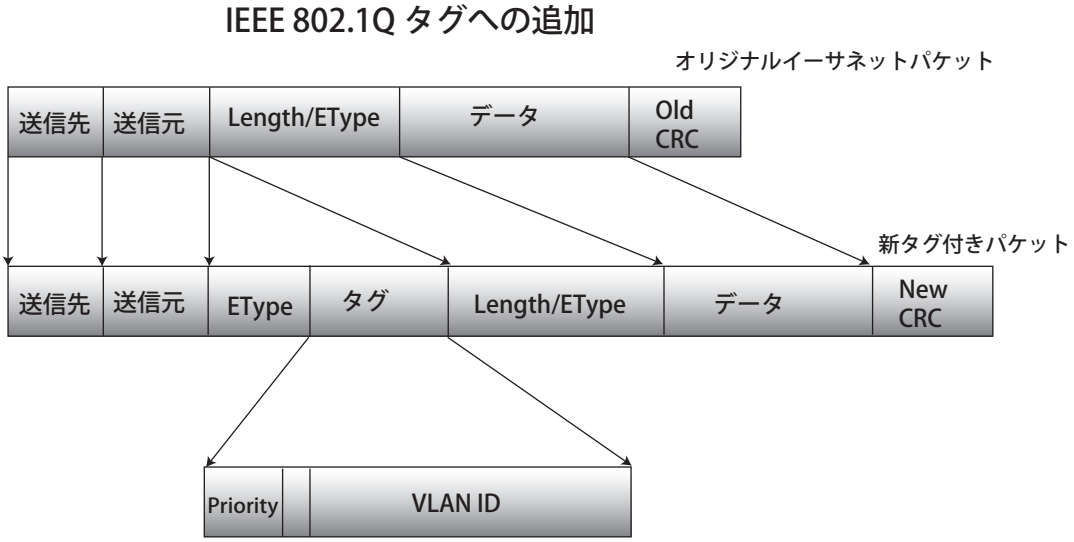


図 9-3　IEEE 802.1Q タグの挿入

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 対応の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付き 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「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）

トランクグループに属するメンバは、同じ VLAN 設定内容を持ちます。トランクグループメンバの VLAN 設定は他のメンバのポートにも適用されます。

注意 VLAN セグメンテーションをポートトランクグループと併用するためには、まずポートトランクグループの設定を行ってから、VLAN の設定を行ってください。設定済みの VLAN のポートトランクグループを変更する場合、ポートトランクグループの設定変更の後に VLAN 設定を変更する必要はありません。VLAN 設定は、ポートトランクグループの変更に伴って自動的に変更されます。

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。

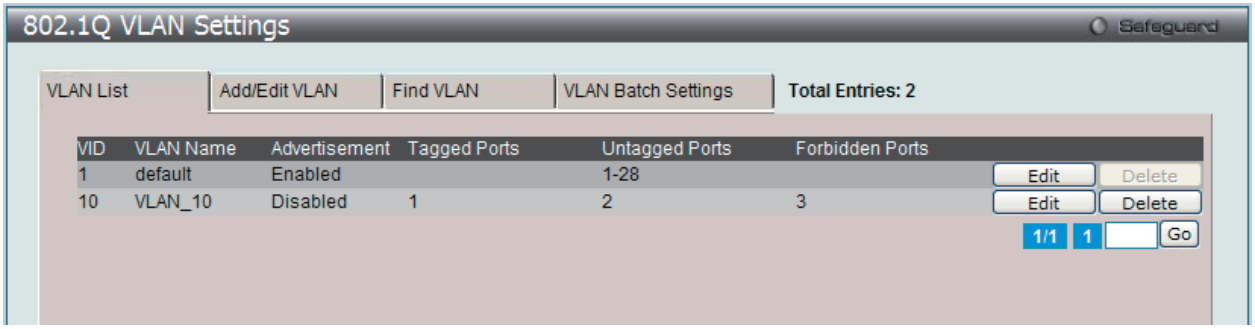


図 9-4　802.1Q VLAN Settings - VLAN List タブ画面

「Edit」ボタンをクリックして、指定エントリを編集します。
エントリを削除するためには、対象のエントリの行の「Delete」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。
新規の 802.1Q VLAN の登録、または既存の 802.1Q VLAN を編集するためには、「Add/Edit VLAN」タブをクリックします。

新規 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。

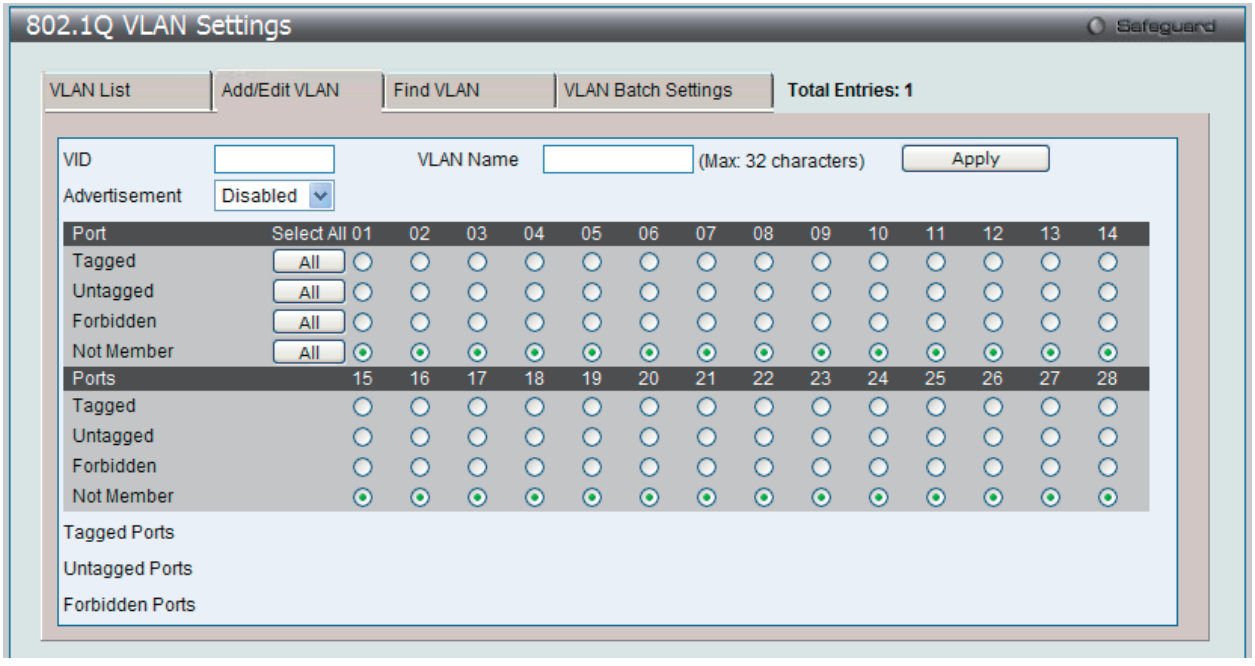


図 9-5　802.1Q VLAN Settings - Add/Edit VLAN タブ画面（Add）

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。以下の画面でエントリの設定を変更します。

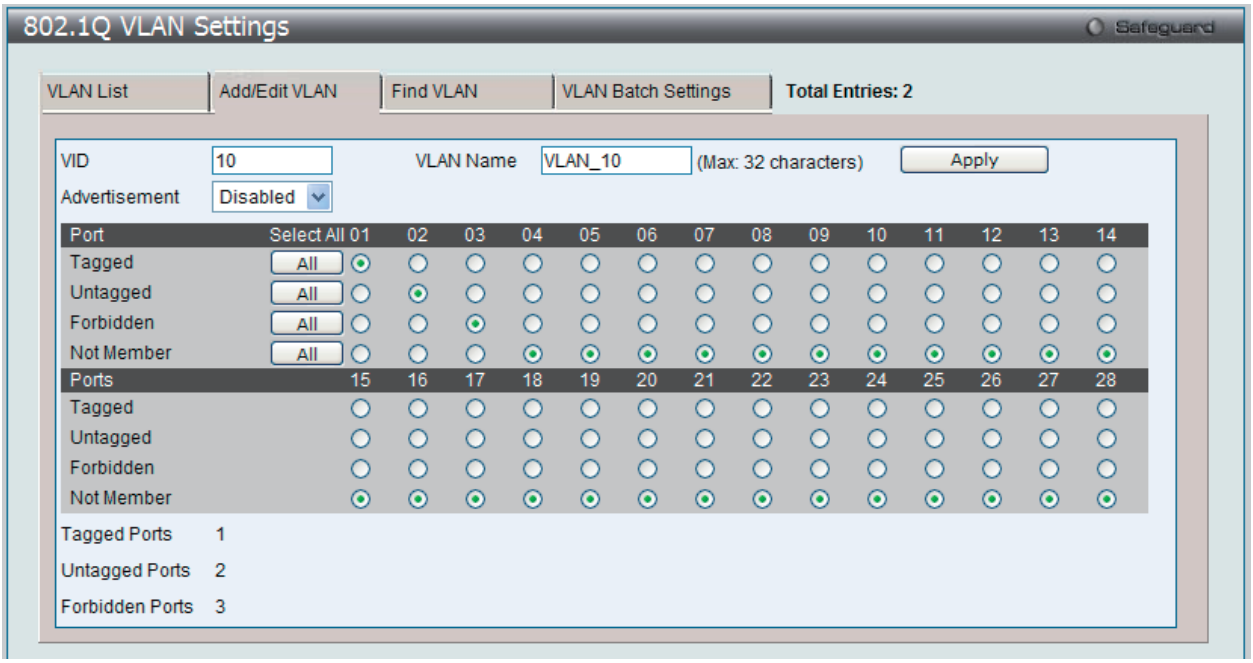


図 9-6　802.1Q VLAN Settings - Add/Edit VLAN タブ画面（Edit）

「802.1Q VLAN Settings」画面内の追加 / 変更の設定内容については、以下の表を参照してください。

「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

「Find VLAN」タブをクリックします。以下の画面が表示されます。

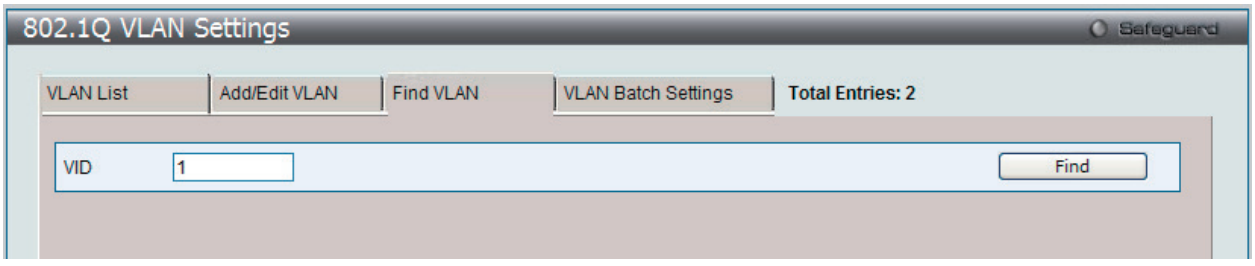


図 9-7　802.1Q VLAN Settings - Find VLAN タブ画面

「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。

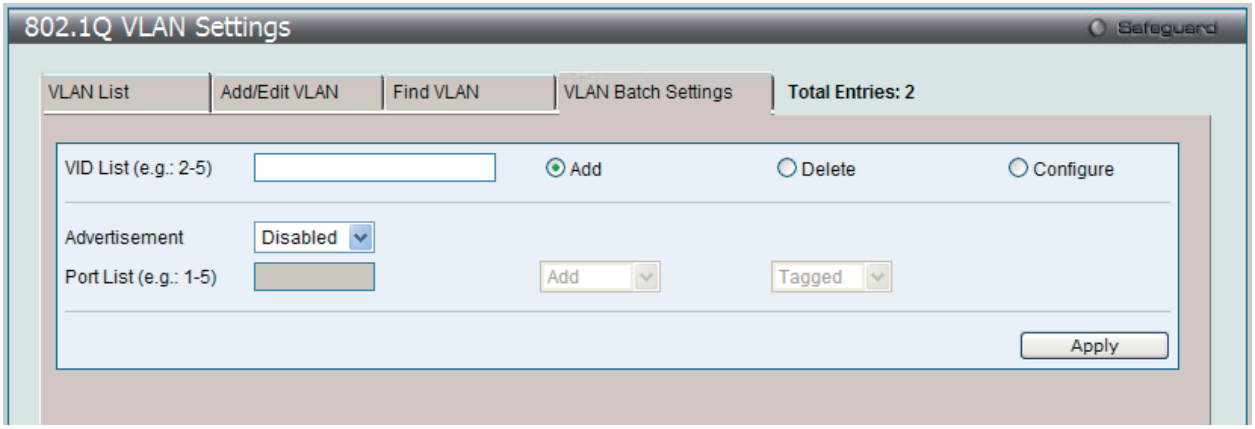


図 9-8　802.1Q VLAN Settings - VLAN Batch Settings タブ画面

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. : 1-5)	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複数の 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。

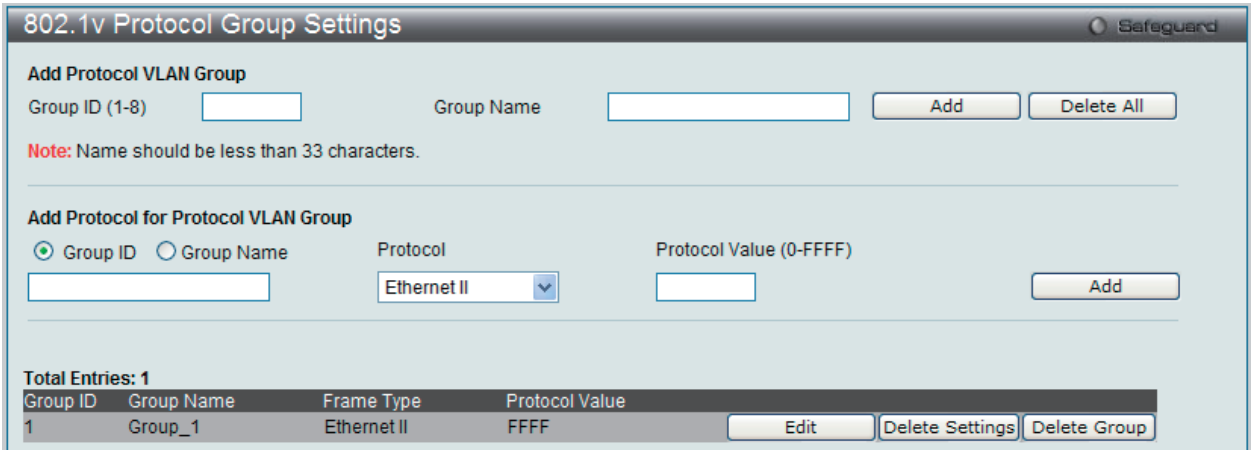


図 9-9　802.1v Protocol Group Settings 画面

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 (1-8)	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。
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。プロトコル値は、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。

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、以下の画面を表示します。

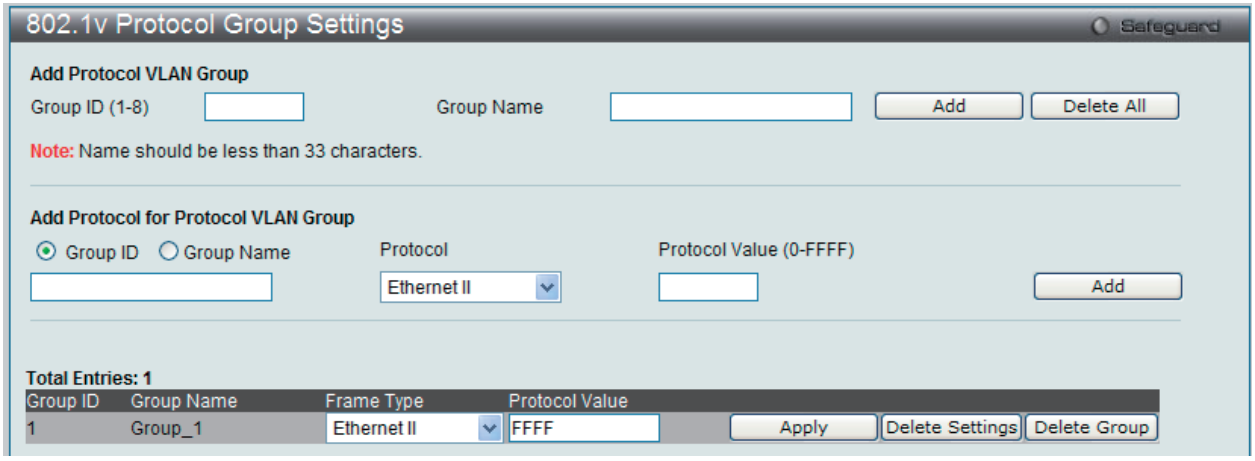


図 9-10　802.1v Protocol Group Settings 画面 - Edit

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。

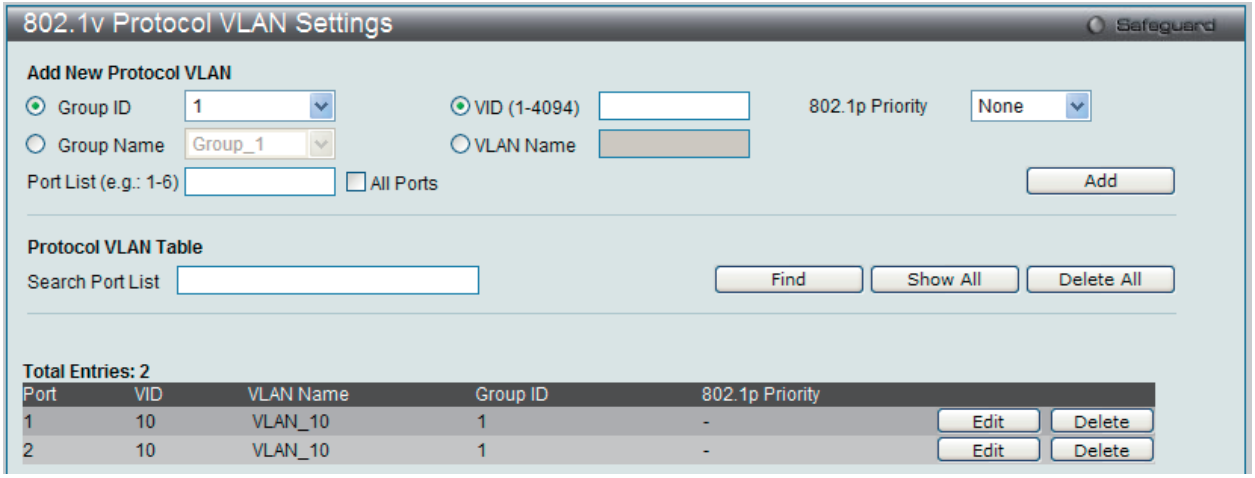


図 9-11　802.1v Protocol VLAN Settings 画面

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 271 ページの「第 11 章　QoS（QoS 機能の設定）」を参照してください。
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、以下の画面を表示します。

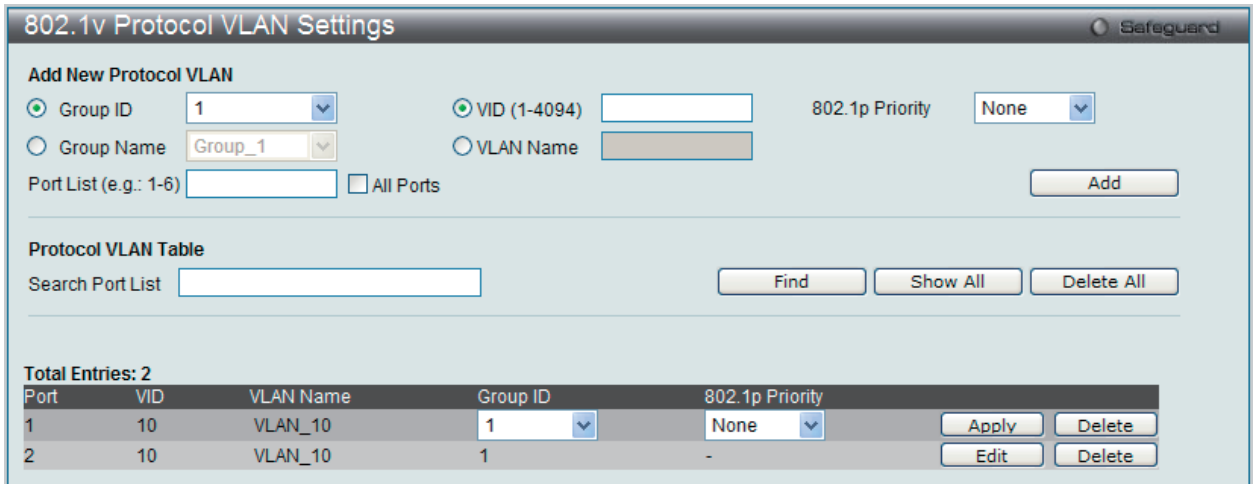


図 9-12　802.1v Protocol VLAN Settings 画面 - Edit

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。

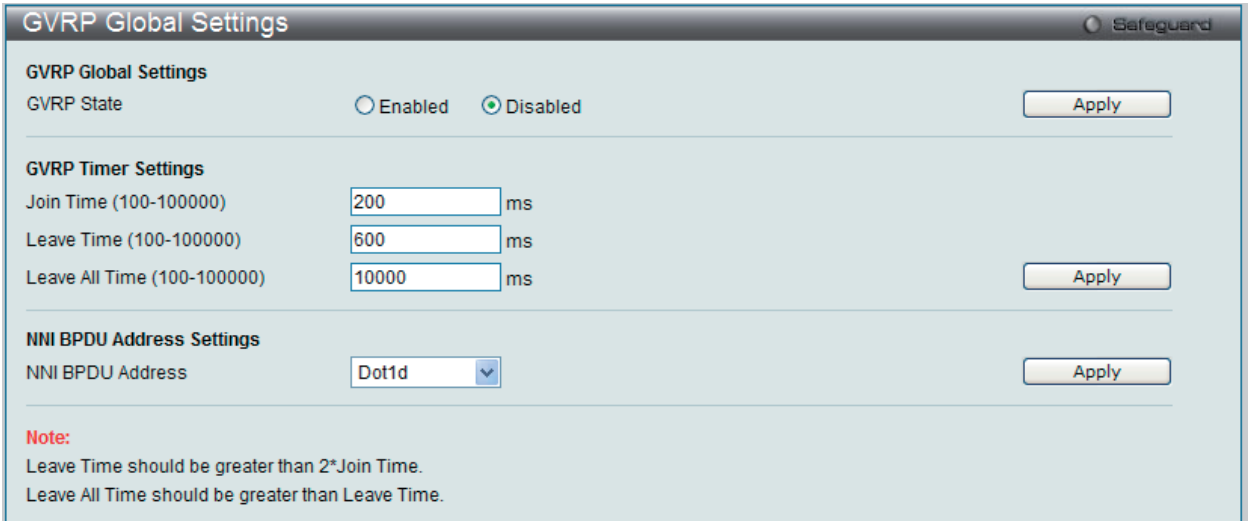


図 9-13　GVRP Global Settings 画面

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、802.1ad サービスプロバイダの GVRP アドレスまたはユーザ定義のマルチキャストを使用します。

「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。

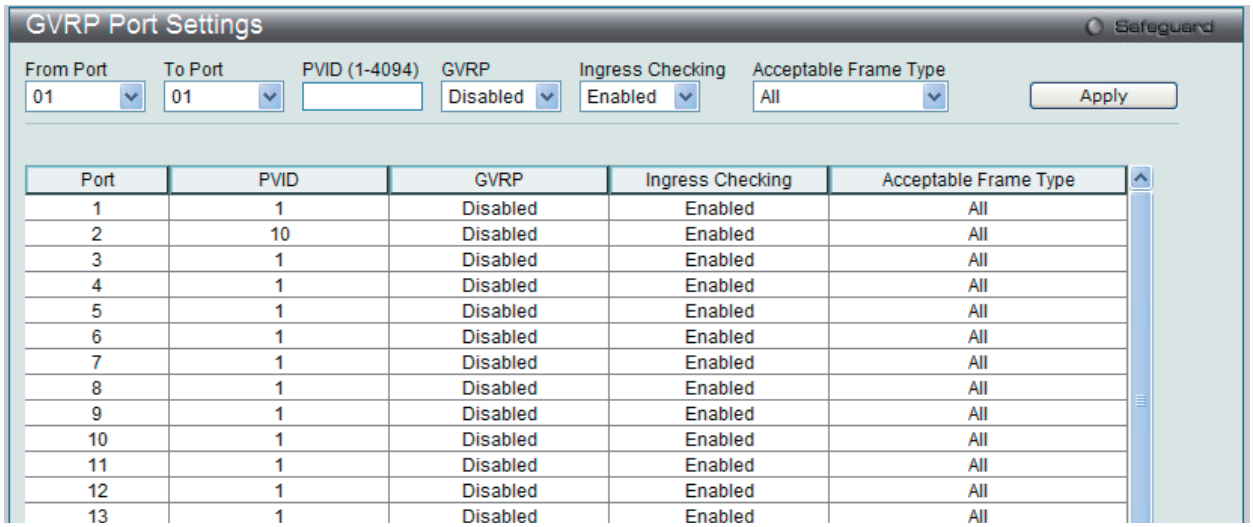


図 9-14　GVRP Port Settings 画面

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。ポートがタグ付きフレームのみを受信すると指定し、タグ付けや、転送のためにタグなしパケットを送られた場合は、ポートはタグに組み込む VID として PVID を使用して 802.1Q タグを付加します。パケットが送信先に到着した時には、受信デバイスは PVID に基づき VLAN による転送を行います。ポートがパケットを受信し、Ingress フィルタリングが有効ならば、ポートは VID と自身の PVID を比較します。2 つが異なる場合、パケットは破棄され、同一ならばパケットは受信されます。
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	Ingress フィルタリングの有効 / 無効を設定します。デバイスで Ingress チェックを有効にするかを設定します。 • Enabled - デバイスで Ingress チェックを有効に設定します。Ingress チェックにより、受信したタグ付きパケットの VID とポートに割り当てられた PVID を比較します。PVID が異なっていれば、ポートはパケットを破棄します。（初期値） • Disabled - Ingress チェックを無効に設定します。
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このポートで動作する認証機能に関わらず指定 VLAN の下で送られます。

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。

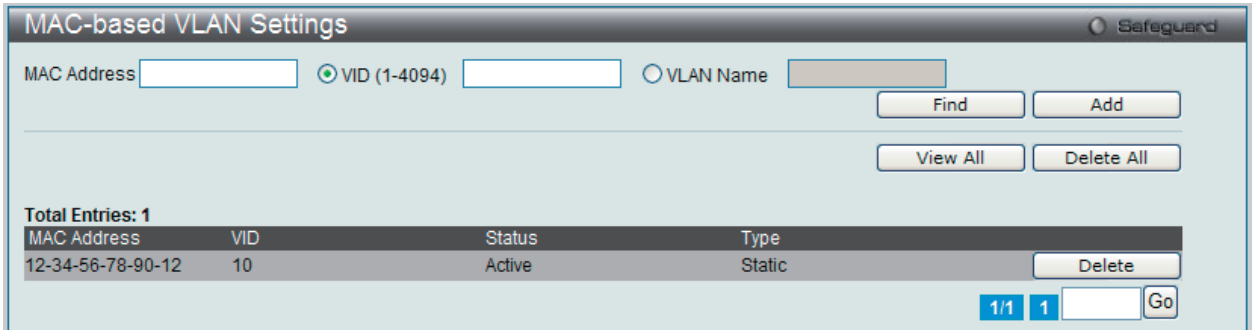


図 9-15　MAC-based VLAN Settings 画面

以下の項目を使用して設定します。

項目	説明
MAC Address	再認証を行う MAC アドレスを入力します。
VLAN Name	作成済みの VLAN の VLAN 名を指定します。
VLAN ID	VLAN ID を入力します。

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。

Private VLAN Settings（プライベート VLAN 設定）

プライベート VLAN はプライマリ VLAN、Isolated VLAN、および多くのコミュニティ VLAN から作成されます。プライベート VLAN ID はプライマリ VLAN の VLAN ID によって示されます。コマンドはセカンダリ VLAN をプライマリ VLAN と関連付けるため、または切り離すために使用されます。

セカンダリ VLAN は複数のプライマリ VLAN に関連付けることはできません。プライマリ VLAN のタグなしメンバポートはプロミスキャスポートとして名前をつけられます。プライマリ VLAN のタグ付きメンバポートはトランクポートとして名前をつけられます。プライベート VLAN のプロミスキャスポートは他のプライベート VLAN のプロミスキャスポートになることはできません。プライマリ VLAN メンバポートは、同時にセカンダリ VLAN メンバであることはできません。逆もまた同様です。セカンダリ VLAN は、タグなしのメンバポートを含むことのみできます。セカンダリ VLAN のメンバポートは、他のセカンダリ VLAN のメンバであることはできません。VLAN がセカンダリ VLAN としてプライマリ VLAN に関連付けされる場合、プライマリ VLAN のプロミスキャスポートはセカンダリ VLAN のタグなしメンバとして動作し、プライマリ VLAN のトランクポートはセカンダリ VLAN のタグ付きメンバとして動作します。通知を使用してセカンダリ VLAN を指定することはできません。プライマリ VLAN だけがレイヤ 3 インタフェースとして設定できます。プライベート VLAN メンバポートをトラフィックセグメンテーション機能に設定できません。

プライベート VLAN のパラメータを設定します。

L2 Features > VLAN > Private 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。

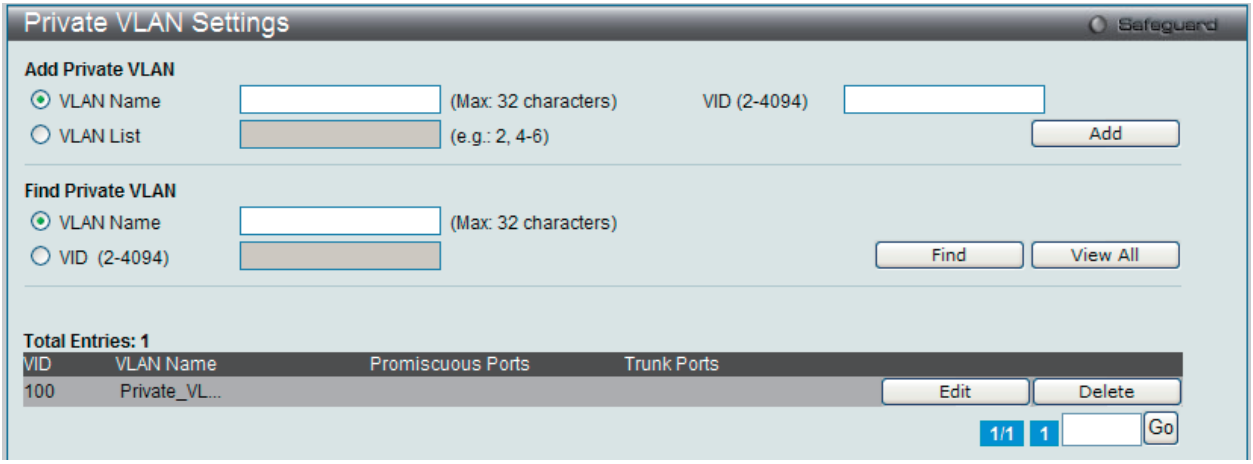


図 9-16　Private VLAN Settings 画面

以下の項目を使用して設定します。

項目	説明
VLAN Name	VLAN 名を入力します。
VID (2-4094)	VID 値を入力します。
VLAN List	VLAN List を入力します。

エントリの新規登録

「Add Private VLAN」セクションでプライベート VLAN に登録する「VLAN Name」/「VID」または「VLAN List」を指定後、「Add」ボタンをクリックします。

エントリの検索

「Find Private VLAN」セクションで「VLAN Name」または「VID」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。「View All」ボタンをクリックすると、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

削除するエントリの「Delete」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、以下の画面を表示します。

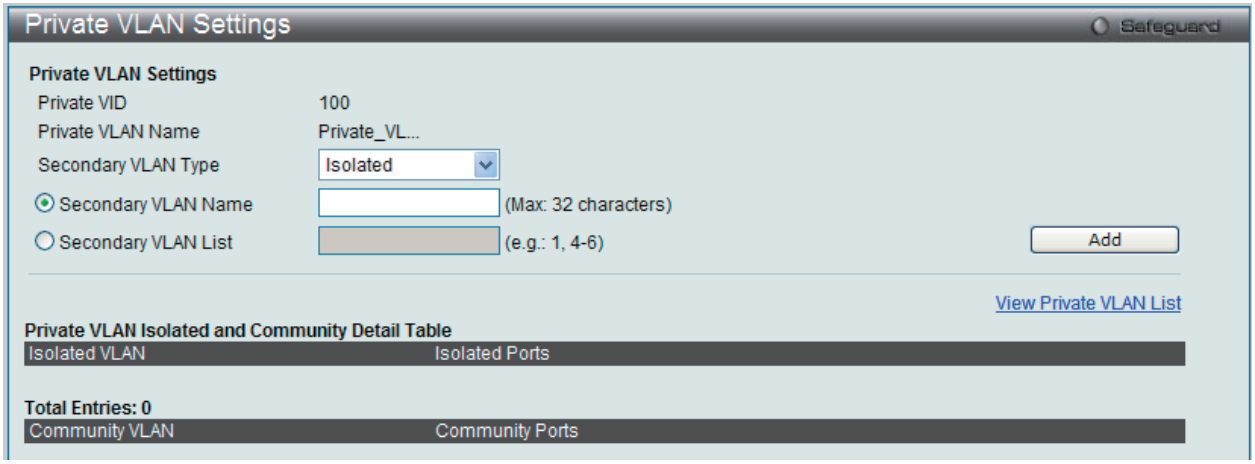


図 9-17　Private VLAN Settings 画面 - Edit

2. 項目を編集し、エントリの「Add」ボタンをクリックします。

以下の項目を使用して設定します。

項目	説明
Secondary VLAN Type	プルダウンメニューを使用してセカンダリ VLAN のタイプ (「Isolated」または「Community」) を選択します。
Secondary VLAN Name	セカンダリ VLAN 名を入力します。
Secondary VLAN List	セカンダリ VLAN ID のリストを入力します。

View Private VLAN List リンクをクリックすると前の画面に戻ります。

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

PVID 自動割り当て設定を「Enabled」（有効）または「Disabled」（無効）にします。

PVID は、スイッチが転送やフィルタリングの目的のために使用する VLAN です。PVID の自動割り当てを有効にした場合、PVID は設定済みの PVID または VLAN により変更可能になります。ポートを VLAN x のタグなしメンバに設定する場合、このポートの PVID は VLAN x に従って更新されます。VLAN コマンドでは、PVID は VLAN コマンド構文の最後のパラメータを指定することで更新されます。PVID の VLAN におけるタグなしメンバからポートを削除すると、ポートの PVID は「default VLAN」に割り当てられます。PVID の自動割り当てを無効にすると、PVID はユーザによる PVID 設定だけで変更可能です。VLAN 設定により PVID が自動的に変更されることはありません。初期値は「Enabled」（有効）です。

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。

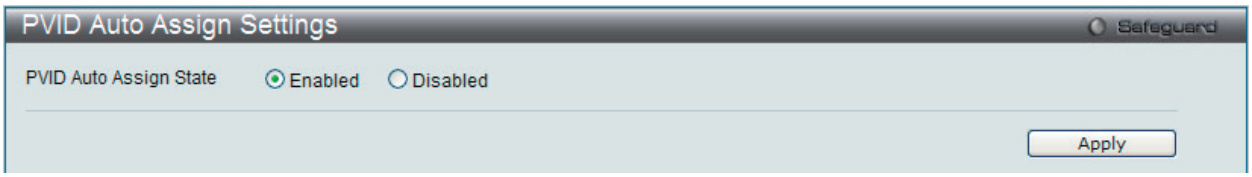


図 9-18　PVID Auto Assign Settings 画面

「Apply」ボタンをクリックし、デバイスに設定を適用します。

Subnet VLAN（サブネット VLAN）

Subnet VLAN Settings（サブネット VLAN 設定）

サブネット VLAN エントリは IP サブネットベースの VLAN クラシフィケーションルールです。ポートにタグなしまたはプライオリティタグを持つ IP パケットを受信すると、送信元 IP アドレスがサブネット VLAN エントリへの照合のために使用されます。エントリのサブネットに送信元 IP があると、パケットはこのサブネットのために定義された VLAN に分類されます。

サブネット VLAN のパラメータを設定します。

L2 Features > VLAN > Subnet VLAN > Subnet 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。

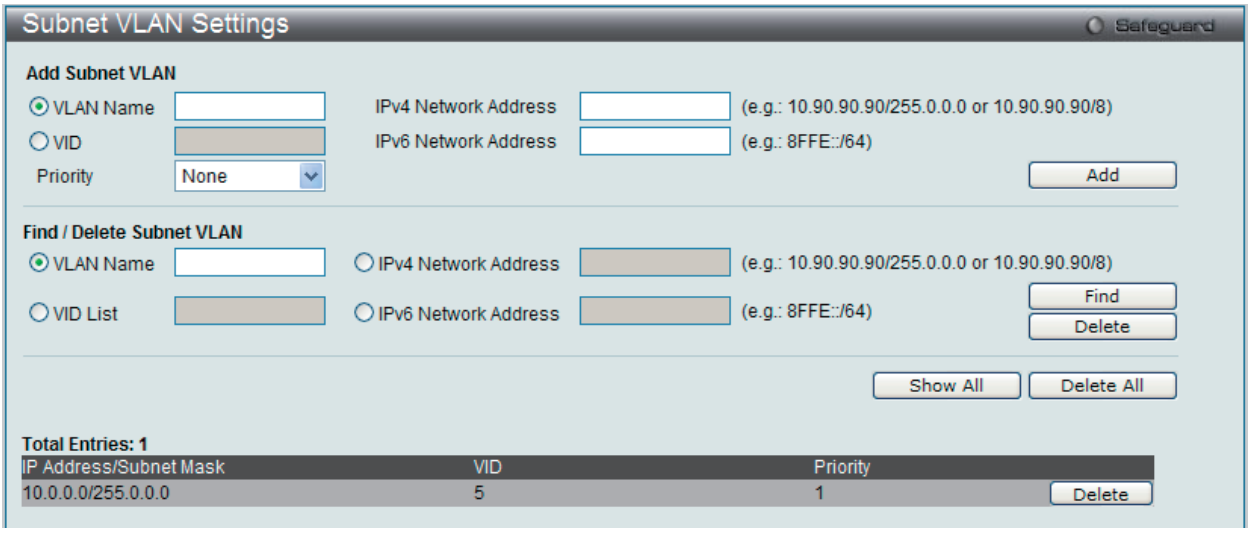


図 9-19　Subnet VLAN Settings 画面

以下の項目を使用して設定します。

項目	説明
VLAN Name	VLAN 名を入力します。
VID	VID 値を入力します。
IPv4 Network Address	使用する IPv4 アドレスを入力します。「/」表記を使用してサブネットマスクを含めることを忘れないでください。
IPv6 Network Address	使用する IPv6 アドレスを入力します。「/」表記を使用してサブネットマスクを含めることを忘れないでください。

エントリの新規登録

「Add Subnet VLAN」セクションでサブネット VLAN に登録する「VLAN Name」/「VID」、「IPv4 Network Address」/「IPv6 Network Address」または「Priority」を指定後、「Add」ボタンをクリックします。

エントリの検索

「Find Subnet VLAN」セクションで「VLAN Name」/「VID」、「IPv4 Network Address」/「IPv6 Network Address」または「Priority」を指定後、「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。「View All」ボタンをクリックすると、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

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。

VLAN Counter Settings（VLAN カウンタの設定）

指定 VLAN の統計情報のカウント、または指定 VLAN の指定ポートの統計情報のカウントのためにコントロールエントリを作成します。統計情報はバイトのカウントまたはパケットのカウントです。異なるフレームタイプに対して統計情報をカウントできます。

L2 Features > VLAN > VLAN Counter 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。

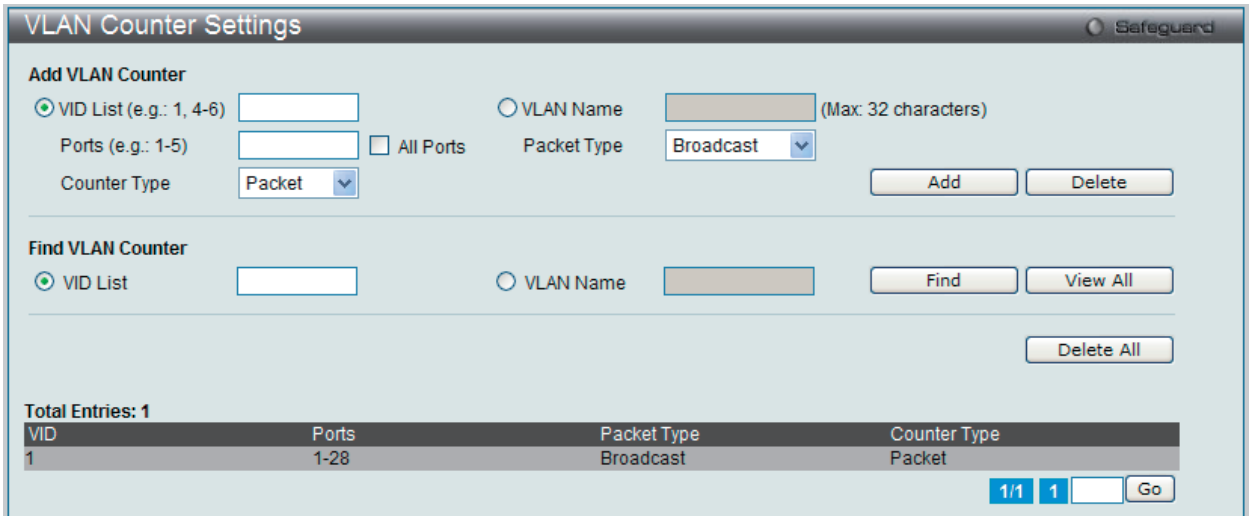


図 9-20　VLAN Counter Settings 画面

以下の項目を使用して設定します。

項目	説明
ID List	VLAN ID により VLAN リストを指定します。
VLAN Name	VLAN 名を指定します。
Ports	指定 VLAN の指定ポートの統計情報のカウントを有効にします。
Packet Type	このオプションは次のパケットタイプを指定します。 • Broadcast - ブロードキャストパケットをカウントします。 • Multicast - マルチキャストパケットをカウントします。 • Unicast - ユニキャストパケットをカウントします。 • All - 統計情報はすべてのパケットに対してカウントされます。
Counter Type	このオプションは以下のカウンタタイプを指定します。 • Packet - パケットレベルでカウントします。 • Byte - バイトレベルでカウントします。

エントリの新規登録

「Add VLAN Counter」セクションで統計情報をカウントする VLAN「VLAN Name」/「VID」、ポート「Ports」、パケットタイプ「Packet Type」およびカウンタタイプ「Counter Type」を指定後、「Add」ボタンをクリックします。

エントリの検索

「Find VLAN Counter」セクションで検出する VLAN「VLAN Name」/「VID」、ポート「Ports」、パケットタイプ「Packet Type」およびカウンタタイプ「Counter Type」を指定後、「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。「View All」ボタンをクリックすると、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

テーブル内の削除するエントリを「Add VLAN Counter」セクションに入力して「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。

Voice VLAN（音声 VLAN）

Voice VLAN Global Settings（音声 VLAN グローバル設定）

音声 VLAN は、IP 電話からの音声トラフィックを送信するのに使用される VLAN です。不規則にデータを送信すると IP 電話の音の品質を低くださせるため、音声トラフィックの QoS（Quality of Service）が音声パケットの伝送優先度を通常のトラフィックより確実に高くするように設定される必要があります。

スイッチは、送信元 MAC アドレスをチェックすることで受信パケットが音声パケットであるかどうか判断します。パケットの送信元 MAC アドレスがシステムによって定義される OUI（Organizationally Unique Identifier : 組織で一意な識別子）アドレスを受諾すると、パケットは音声パケットとして判断されて、音声 VLAN に送信されます。

音声 VLAN をグロバールに有効 / 無効にします。

L2 Features > VLAN > Voice VLAN > Voice VLAN 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。

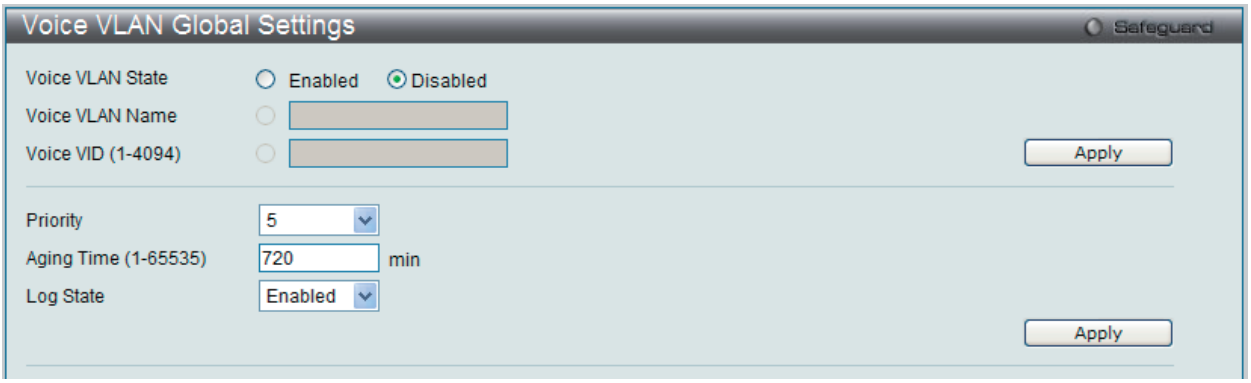


図 9-21　Voice VLAN Global Settings 画面

以下の項目を使用して設定します。

項目	説明
Voice VLAN State	音声 VLAN の状態を有効 / 無効にします。
Voice VLAN Name	音声 VLAN 名を指定します。
Voice VID	音声 VLAN の VLAN ID を指定します。
Priority	音声 VLAN の優先度（0-7）を指定します。優先度の初期値は 5 です。
Aging Time	エージングタイム（1-65535 分）を指定します。初期値は 720(分) です。エージングタイムは、ポートが自動 VLAN メンバである場合に音声 VLAN からポートを削除するために使用されます。最後の音声デバイスが、トラフィックの送信を止めて、この音声デバイスの MAC アドレスがエージングタイムに到達すると、音声 VLAN エージングタイマが開始されます。ポートは音声 VLAN のエージングタイム経過後に音声 VLAN から削除されます。音声トラフィックがエージングタイム内に再開すると、エージングタイマは停止し、リセットされます。
Log State	音声 VLAN ログの送信を有効または無効にします。

音声 VLAN の有効化

「Voice VLAN State」を「Enabled」にして音声 VLAN を有効にする VLAN を「Voice VLAN Name」または「Voice VID」で指定後、「Apply」ボタンをクリックします。

音声 VLAN のパラメータ設定

音声 VLAN の有効後、「Priority」、「Aging Time」または「Log State」を設定後、「Apply」ボタンをクリックします。

Voice VLAN Port Settings（音声 VLAN のポート設定）

ポートの音声 VLAN 情報を表示します。

L2 Features > VLAN > Voice VLAN > Voice VLAN 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。

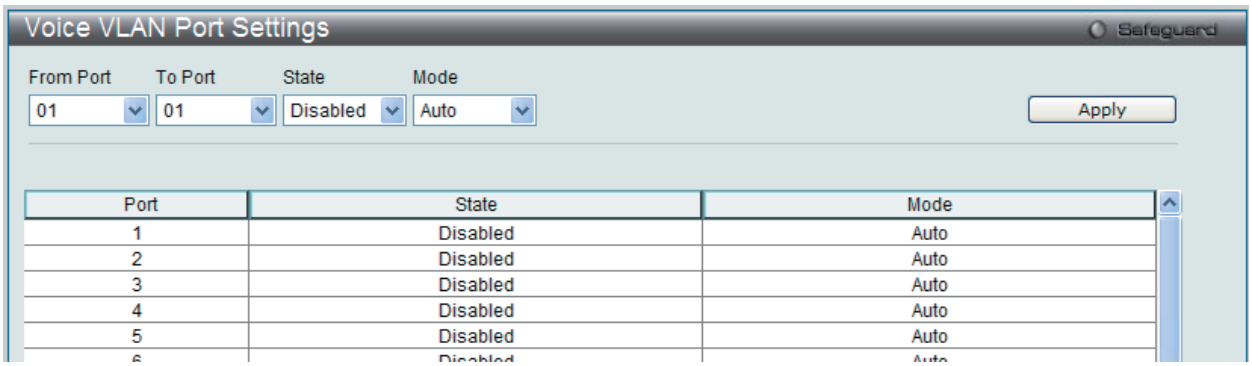


図 9-22　Voice VLAN Port Settings 画面

以下の項目を使用して設定します。

項目	説明
From Port / To Port	表示するポート範囲を選択します。
State	ポートの状態を設定します。
Mode	ポートのモードを設定します。

「Apply」ボタンをクリックして行った変更を適用します。

Voice VLAN OUI Settings（音声 VLAN OUI 設定）

ユーザ定義の音声トラフィックの OUI を設定します。

OUI は音声トラフィックを識別するの使用されます。多くの定義済み OUI があり、必要に応じて、さらにユーザ定義の OUI を定義できます。
ユーザ定義 OUI は定義済みの OUI と同じとすることはできません。

L2 Features > VLAN > Voice VLAN > Voice VLAN OUI 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。

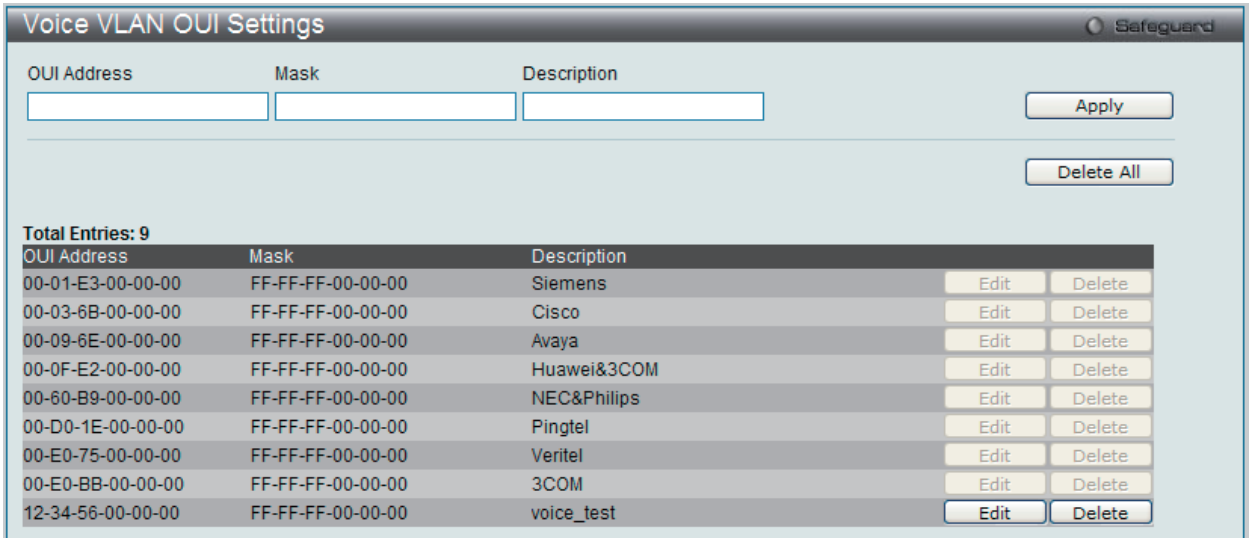


図 9-23　Voice VLAN OUI Settings 画面

以下の項目を使用して設定します。

項目	説明
OUI Address	ユーザ定義の OUI MAC アドレス。
Mask	ユーザ定義 OUI MAC アドレスマスク。
Description	ユーザ定義 OUI に関する説明文。

「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。または、「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。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

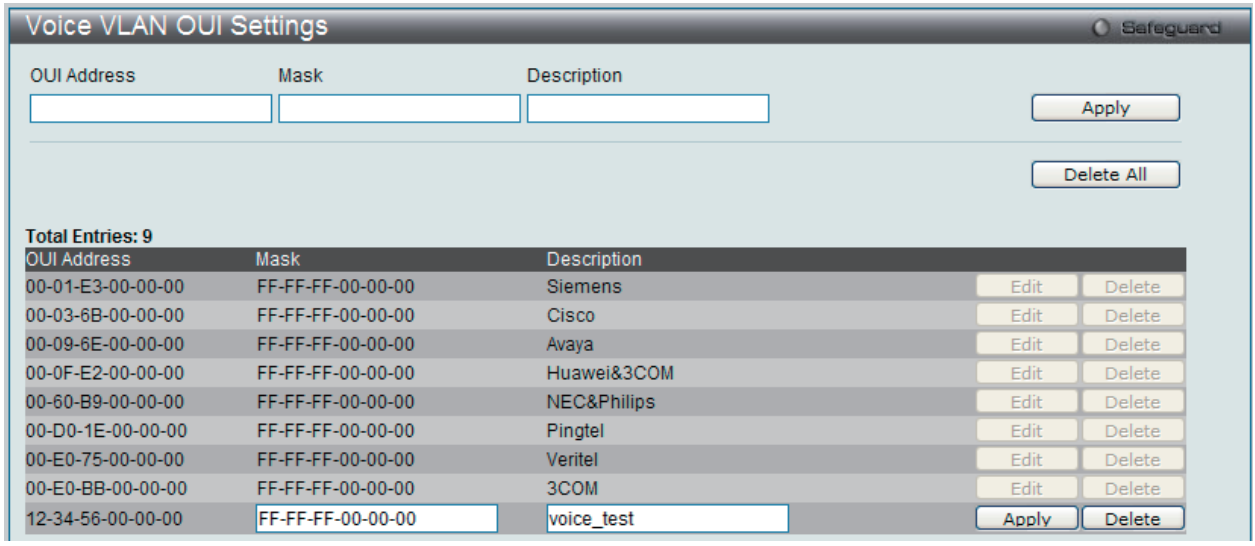


図 9-24　Voice VLAN OUI Settings 画面 - Edit

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

Voice VLAN Device（音声 VLAN デバイス）

ポートに接続する音声デバイスを表示します。開始時刻はデバイスがこのポートで検出される時間です。また、アクティベート時間はデバイスが一番最近トラフィックを送信した時間です。

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

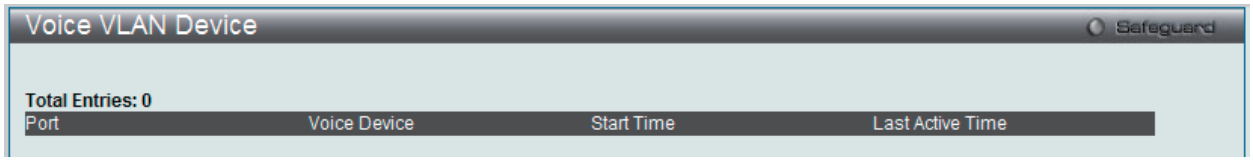
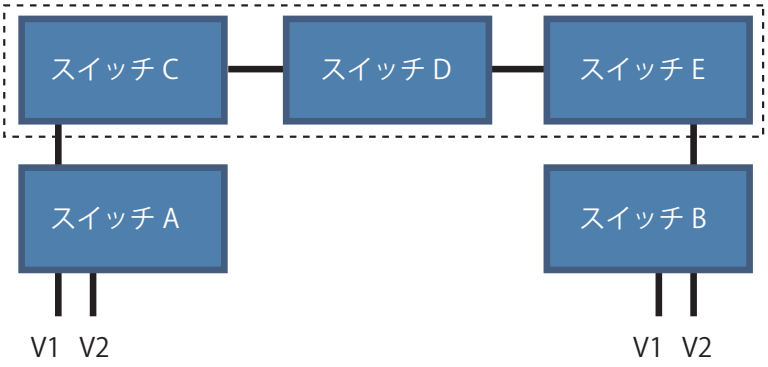


図 9-25　Voice VLAN Device 画面

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。

以下の図例を参照してください。
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。



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。

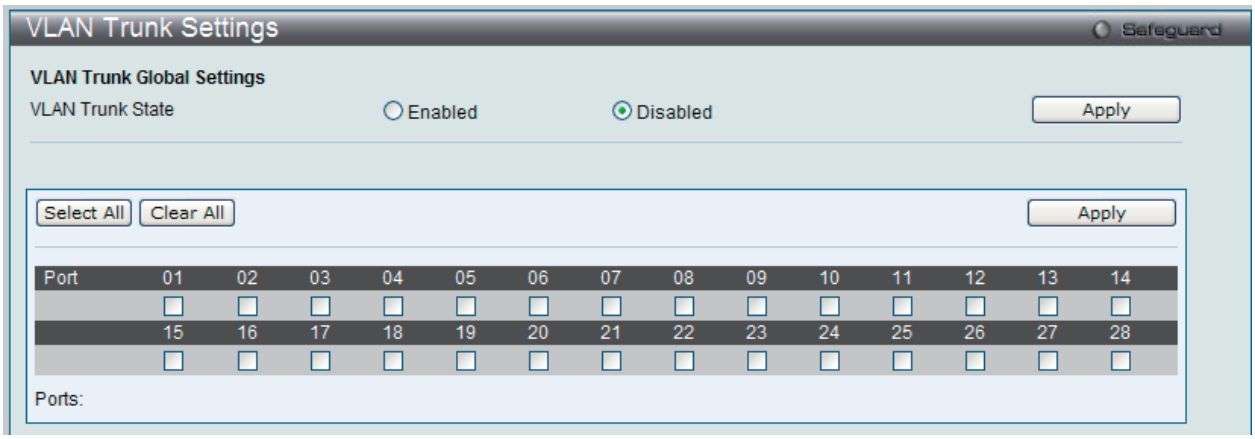


図 9-26　VLAN Trunk Settings 画面

本画面には次の項目があります。

項目	説明
VLAN Trunk Global 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。

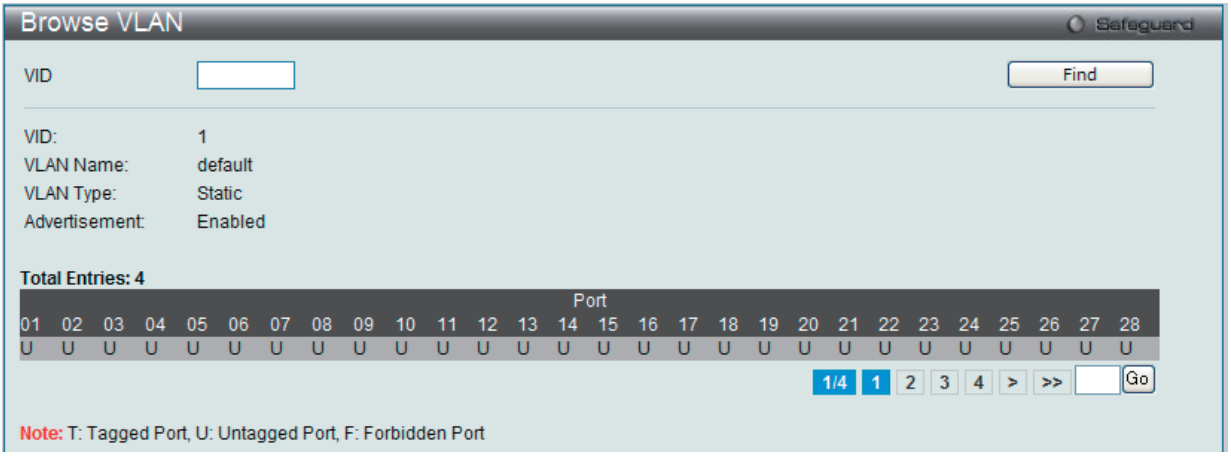


図 9-27　Browse VLAN 画面

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。

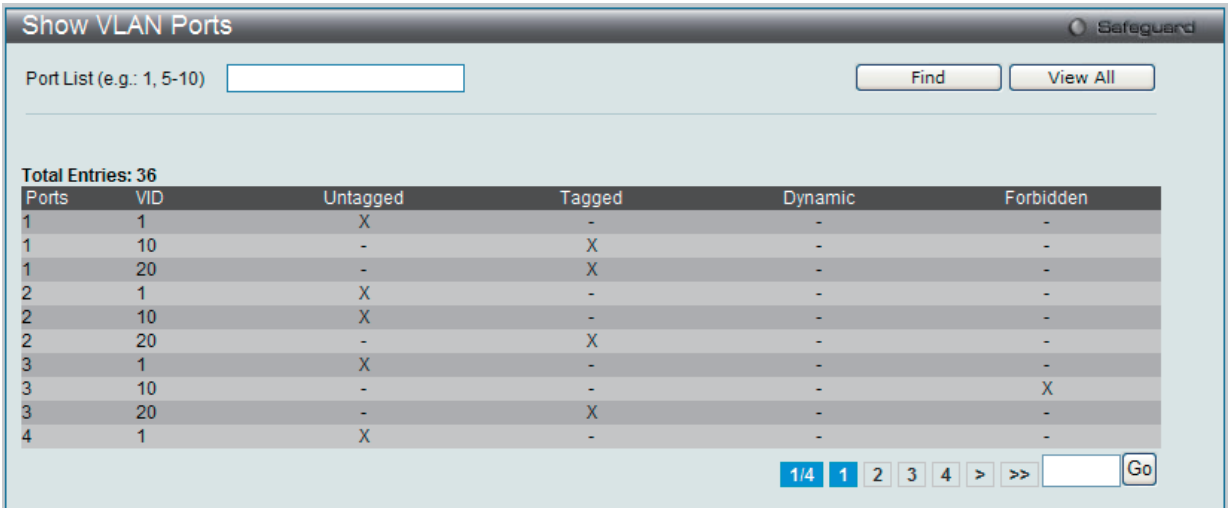


図 9-28　Show VLAN Ports 画面

画面の上にある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）

ダブル 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。

ダブル 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。

以下にダブル 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

以下にダブル VLAN を使用した ISP ネットワークの例を示します。

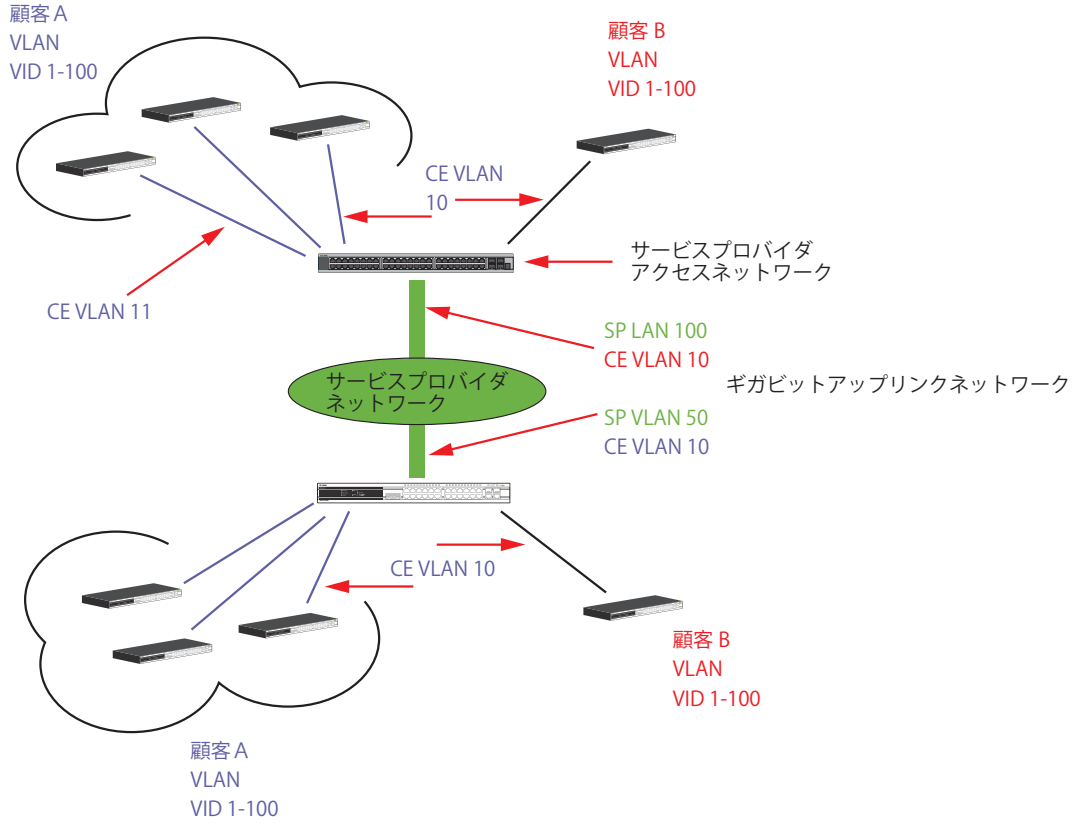


図 9-29　ダブル VLAN を使用したネットワーク例

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 を持つダブル 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において 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、またアップリンクポートはサービスプロバイダ VLAN のタグ付きポートとします。
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）

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。

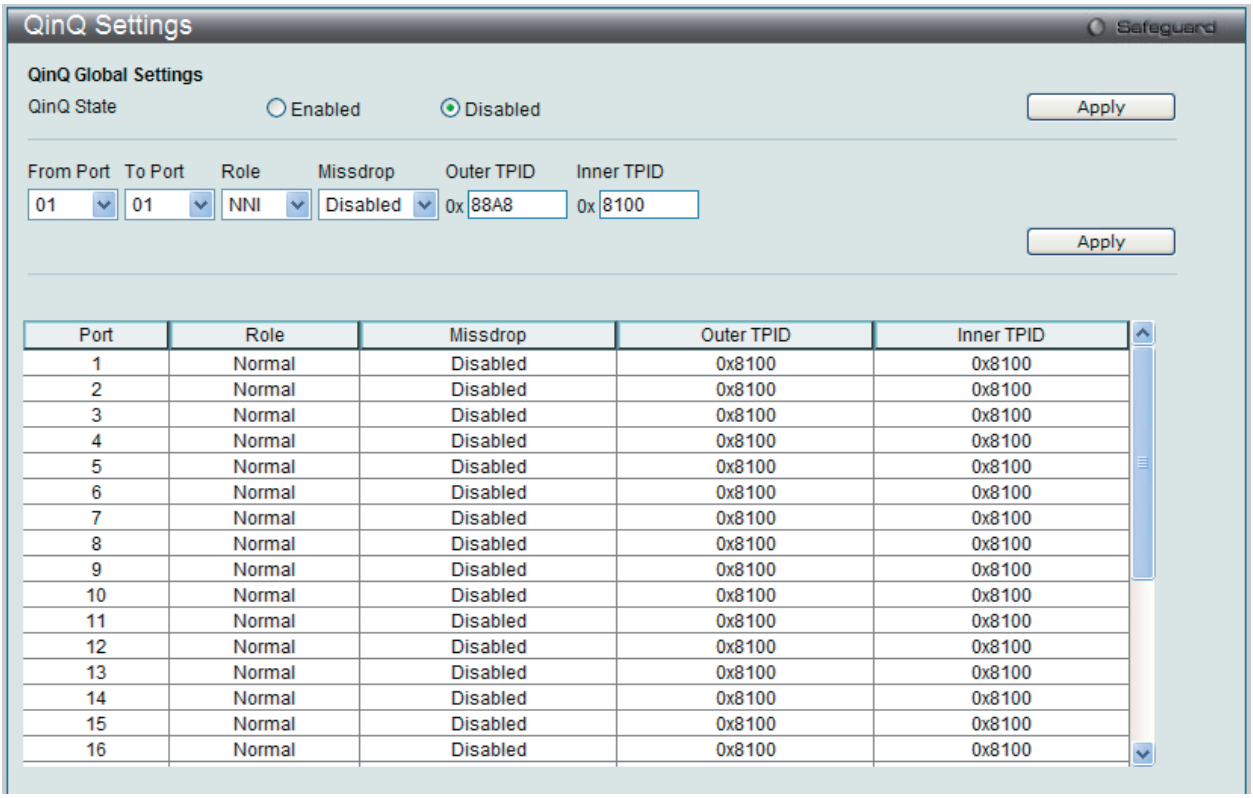


図 9-30　QinQ Settings 画面

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。
From Port/To Port	VLAN 設定を行うポートグループの最初と最後の番号を設定します。
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。
Inner TPID	SP-VLAN タグに Inner TPID 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。

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。

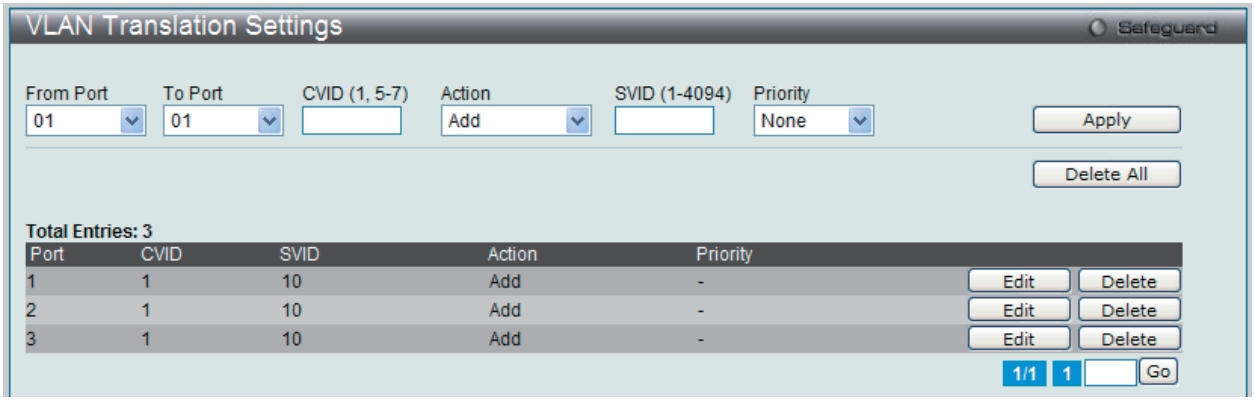


図 9-31　VLAN Translation Settings 画面

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	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	SP-VLAN ID を入力します。
Priority	S- タグの優先度（0-7）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。

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、以下の画面を表示します。

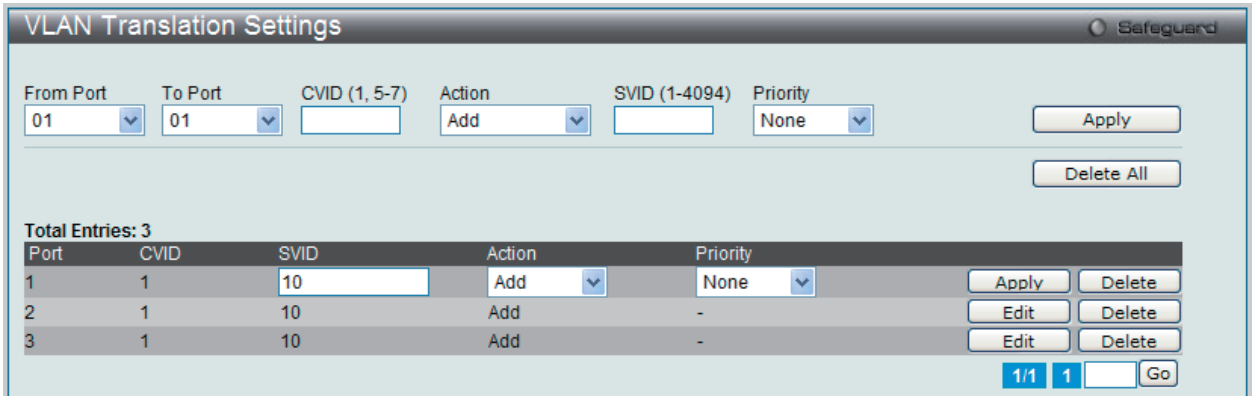


図 9-32　VLAN Translation Settings 画面 - Edit

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。

Double Tagged VLAN Translation Settings（ダブルタグ VLAN 変換の設定）

ダブルタグ VLAN 変換のパラメータを設定します。

L2 Features > QinQ > Double Tagged 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。

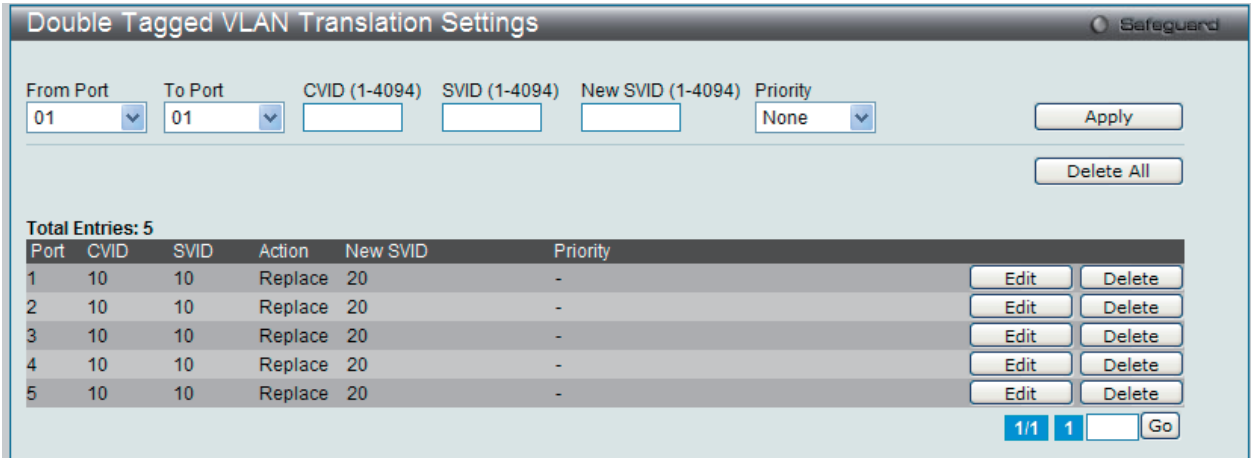


図 9-33　Double Tagged VLAN Translation Settings 画面

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	照合する C-VLAN ID を指定します。
SVID	照合する S-VLAN ID を指定します。
New SVID	SVID と CVID が一致する場合、オリジナルの SVID を新しい SVID に交換します。
Priority	S- タグの優先度を選択します。

「Apply」ボタンをクリックして行った変更を適用します。

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、以下の画面を表示します。

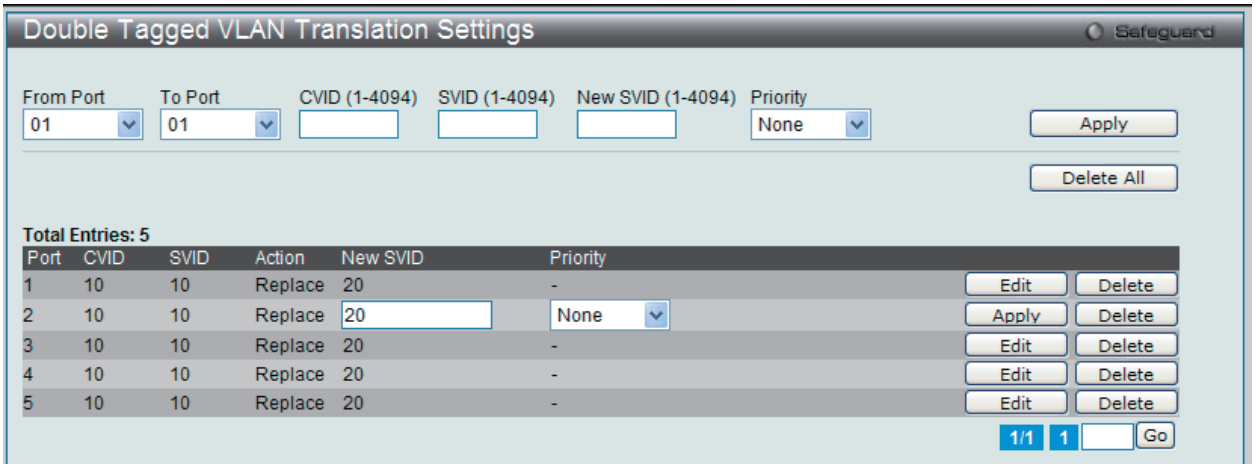


図 9-34　Double Tagged VLAN Translation Settings 画面 - Edit

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。

VLAN Translation Port Mapping Settings（VLAN 変換ポートのマッピング設定）

ポートの QinQ S-VLAN 割り当てのルールを設定します。これらのルールは QinQ プロファイルに含まれます。1 つの QinQ プロファイルをポートに追加できます。この設定は QinQ モードが無効の場合には有効になりません。

L2 Features > QinQ > VLAN Translation Port Mapping 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。

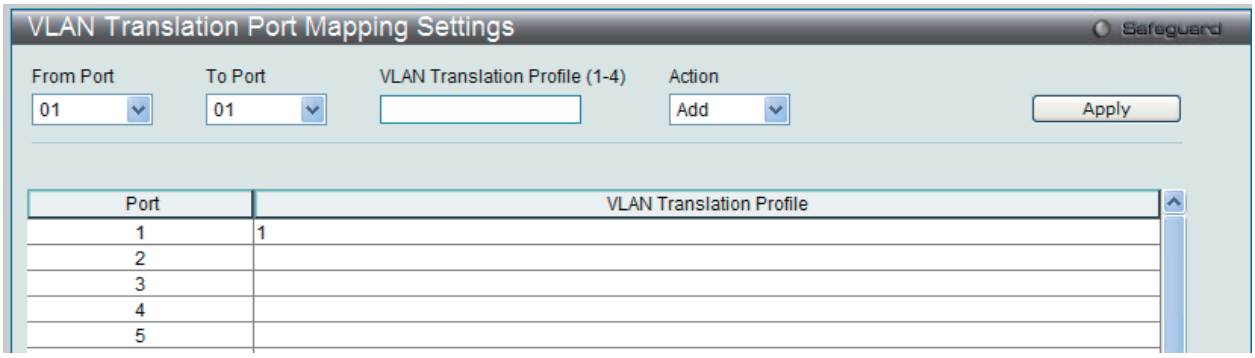


図 9-35　VLAN Translation Port Mapping Settings 画面

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。
VLAN Translation Profile	VLAN 変換プロファイル番号を入力します。
Action	適用する操作を選択します。「Add」または「Delete」を選択できます。

「Apply」ボタンをクリックして行った変更を適用します。

VLAN Translation Profile List（VLAN 変換プロファイルリスト）

QinQ プロファイルの作成と、SP-VLAN を割り当てます。QinQ プロファイルに複数のルールを指定できます。変換プロファイルに一致するようにフレームに Outer タグの追加または交換が行われます。

L2 Features > QinQ > VLAN Translation 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。

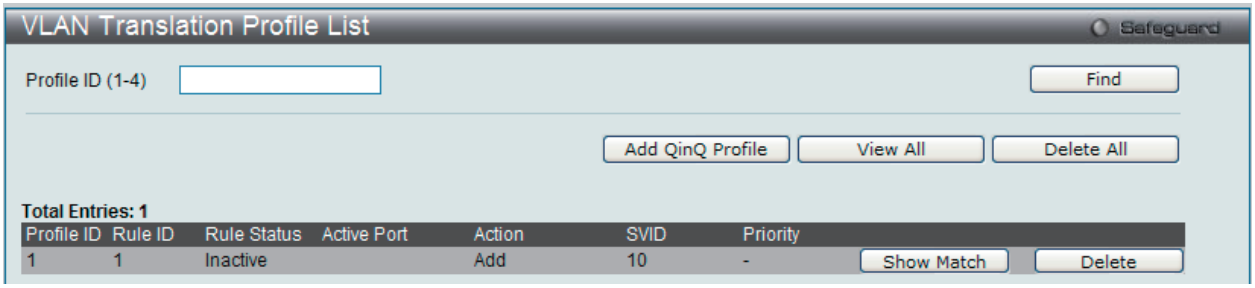


図 9-36　VLAN Translation Profile List 画面

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
Profile ID	プロファイル番号を入力します。

「Apply」ボタンをクリックして行った変更を適用します。

「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。
「Add QinQ Profile」ボタンをクリックして、新しいエントリ QinQ プロファイルを追加します。
「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。
「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。

QinQ プロファイルの登録

「Add QinQ Profile」ボタンをクリックすると、以下の画面が表示されます。

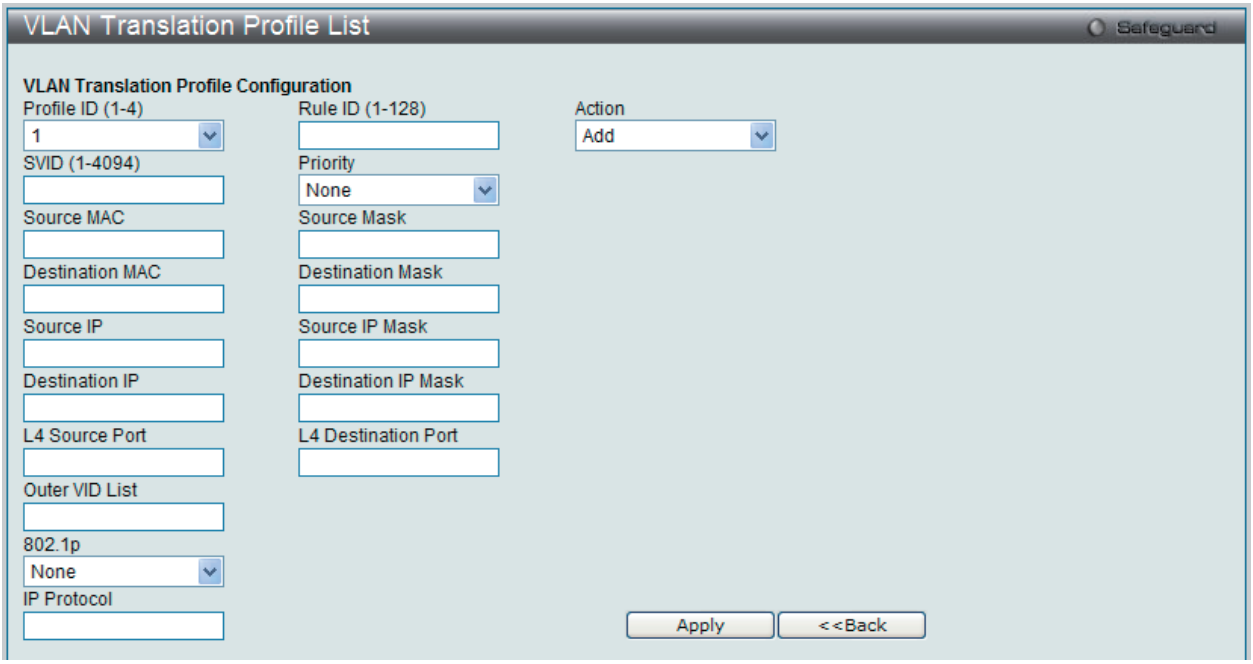


図 9-37　VLAN Translation Profile List 画面 - Add

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
Profile ID	設定するプロファイル ID 番号を指定します。
Rule ID	プロファイルに追加するルール ID を指定します。
Action	• Add - C-VLAN タグの前に割り当てられた SP-VLAN にタグを追加するします。S-TAG がパケットにないとこのルールは実施されません。 • Replace - タグ内の C-VLAN を SP VLAN と交換することを示すアクションを選択します。パケットに C-TAG がパケットにないとこのルールは実施されません。
SVID	一致するパケットに割り当てられるように SP-VLAN ID を指定します。
Priority	SP-VLAN の優先度を指定します。優先度を指定しない場合はポート優先度の初期値を使用します。
Source MAC	送信元 MAC アドレスを指定します。
Source Mask	送信元 MAC アドレスマスクを指定します。
Destination MAC	送信先 MAC アドレスを指定します。
Destination Mask	送信先 MAC アドレスマスクを指定します。
Source IP	送信元 IPv4 アドレスまたは IPv4 サブネットを指定します。
Source IP Mask	送信元 IPv4 アドレスマスクを指定します。
Destination IP	送信先 IPv4 アドレスまたは IPv4 サブネットを指定します。
Destination IP Mask	送信先 IPv4 アドレスマスクを指定します。
L4 Source Port	L4 送信元ポート ID を指定します。
L4 Destination Port	L4 送信先ポート ID を指定します。
Outer VID List	パケットの Outer VID 範囲を指定します。
802.1p	パケットの 802.1p 優先度を指定します。
IP Protocol	使用する IP プロトコルを指定します。

「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。

QinQ VLAN 変換ルール情報の参照

「Show Match」ボタンをクリックして以下の画面を表示します。

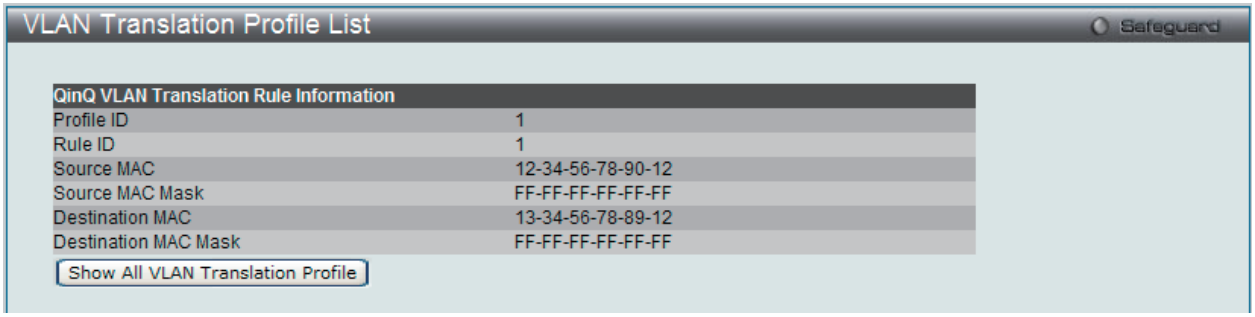


図 9-38　VLAN Translation Profile List 画面 - Show Match

「Show All VLAN Translation Profile」ボタンをクリックして前の画面に戻ります。

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機能を設定します。

QinQ ダブル VLAN 機能を使用する場合、サブスクライバのレイヤ 2 トラフィックは ISP ネットワークに対して透過状態です。しかし、QinQ は、ネットワークを少し危険で不便にするレイヤ 2 制御プロトコルを処理することはできません。レイヤ 2 プロトコルトンネリング（L2PT）機能を使用すると、L2 制御プロトコルを各リモートサイトにトンネリングすることで問題を解決するため、会社の中央管理が可能になります。

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。

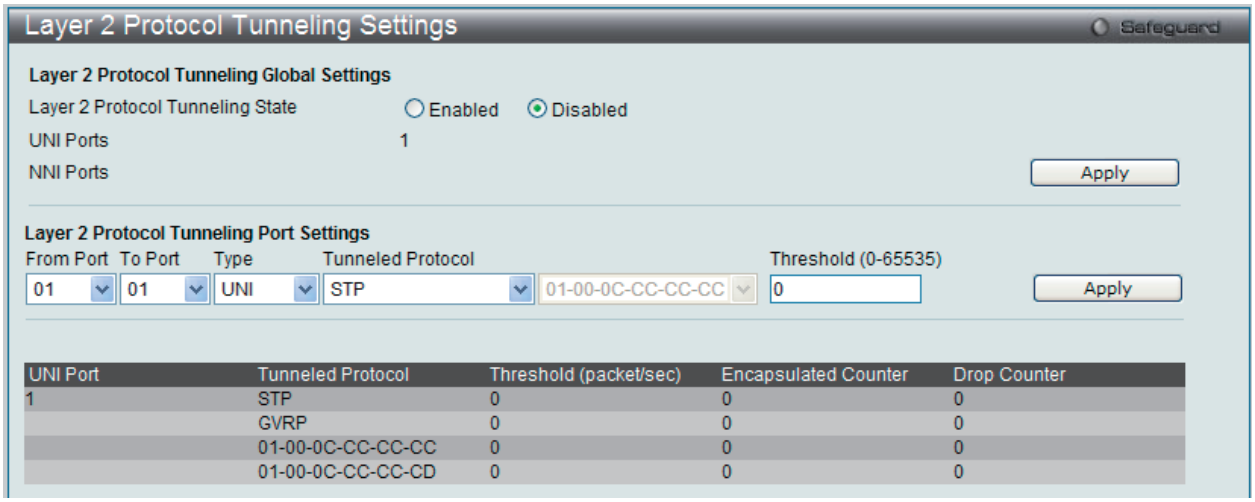


図 9-39　Layer 2 Protocol Tunneling Settings 画面

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. 4096 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 4096 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 準拠のブリッジリンクから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。

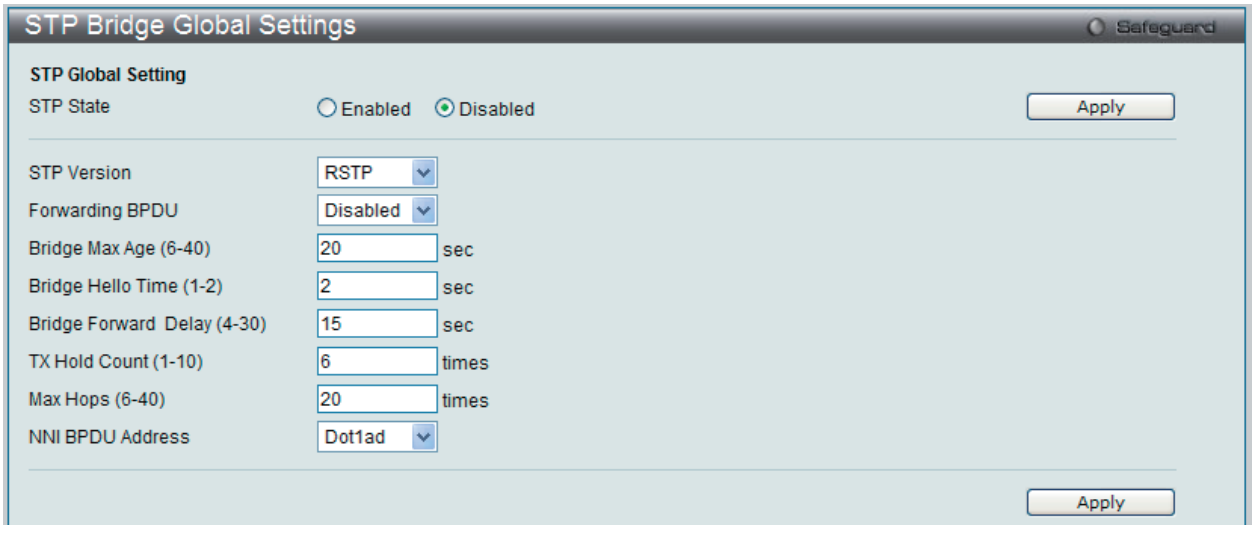


図 9-40　STP Bridge Global Settings 画面 : RSTP（初期値）

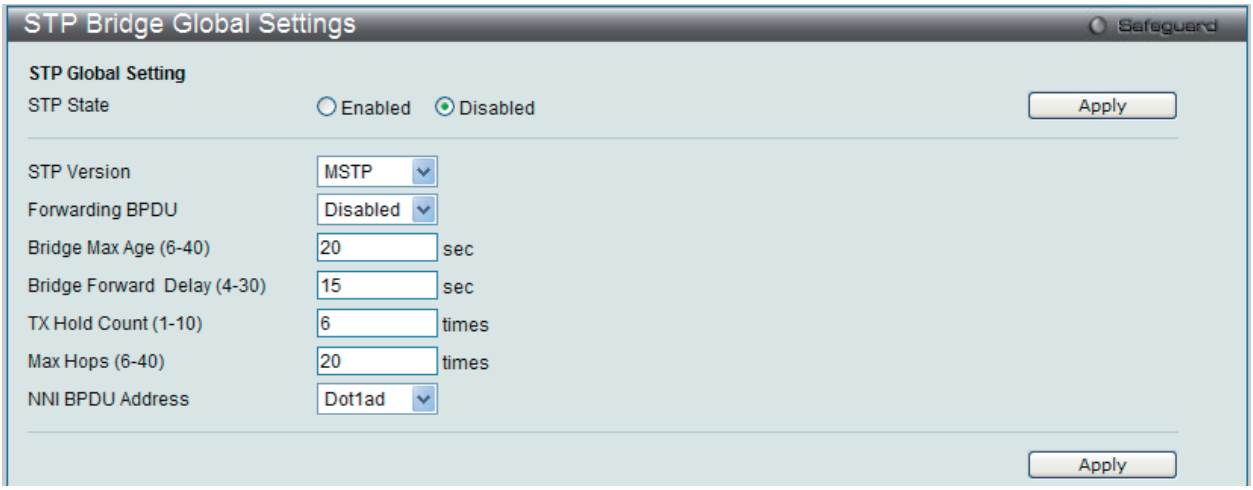


図 9-41　STP Bridge Global Settings 画面 : MSTP

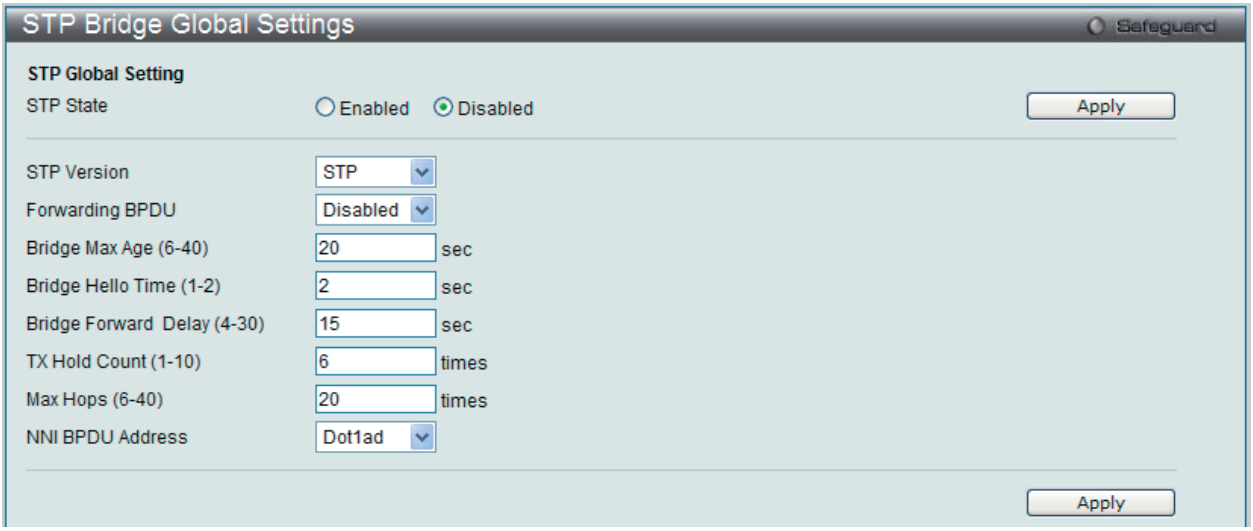


図 9-42　STP Bridge Global Settings 画面 : STP

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。

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）

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「Enabled」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。

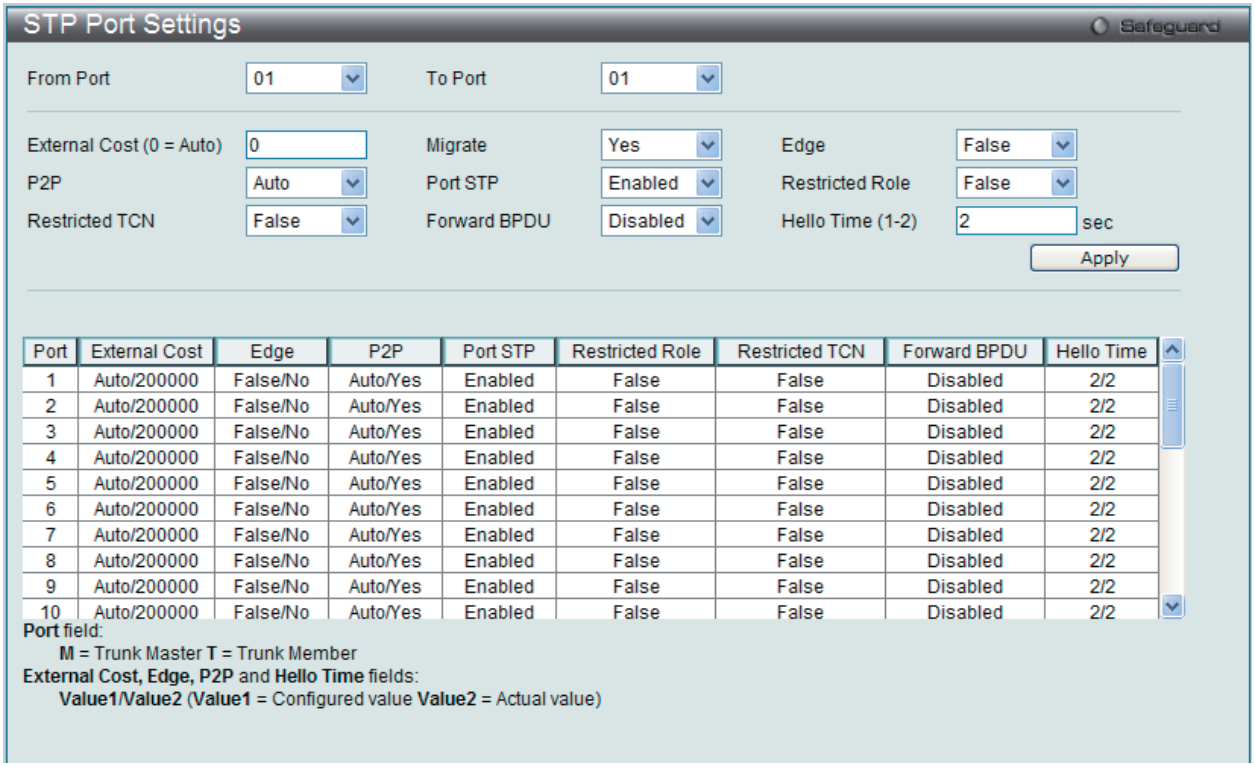
項目	説明
Bridge Hello Time (1-2)	ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために BPDU パケットを 2 回送信します。本値は、1 回目の送信と 2 回目の送信の間隔です。STP または RSTP が「STP Version」で選択された場合にだけ本項目は表示されます。MSTP に対して、Hello Time はポートごとに設定される必要があります。詳しくは「STP ポート設定」セクションを参照してください。1-2 秒で指定します。初期値は 2（秒）です。
Bridge Forward Delay (4-30)	スイッチ上のすべてのポートは、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 BDPU 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	使用する NNI BPDU アドレスを入力します。「Dot1d」または「Dot1ad」を選択します。

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。

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。



Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDU	Hello Time
1	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
2	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
3	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
4	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
5	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
6	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
7	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
8	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
9	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
10	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2

図 9-43　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	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。

項目	説明
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。（初期値） • 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。
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の BPDU パケットの転送を行うようになります。
Hello Time	RSTP の各ブリッジのパラメータであり、MSTP 内のポートごとのパラメータになります。初期値は 2（秒）です。

「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。

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

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。

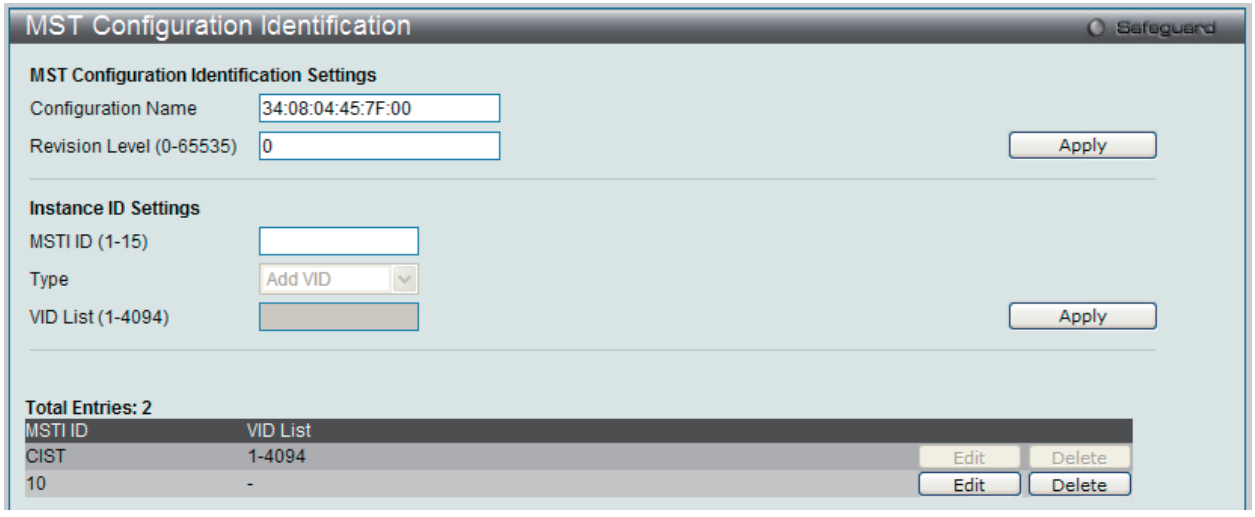


図 9-44　MST Configuration Identification 画面

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 (1-15)	新規の MSTI ID を 1-15 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(1-4094)	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、以下の画面を表示します。

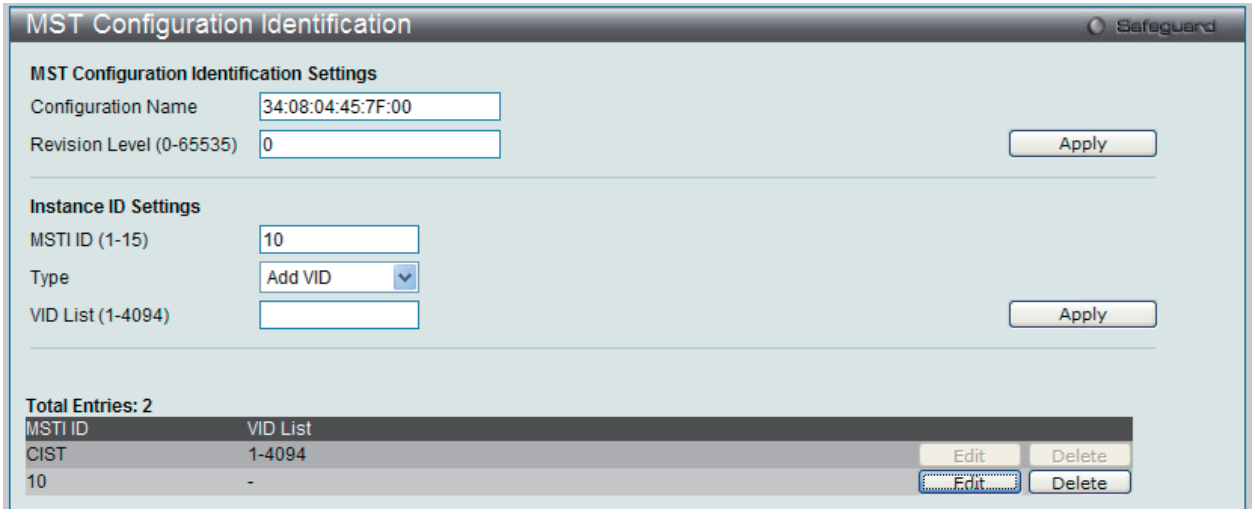


図 9-45　MST Configuration Identification 画面 - Edit

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。

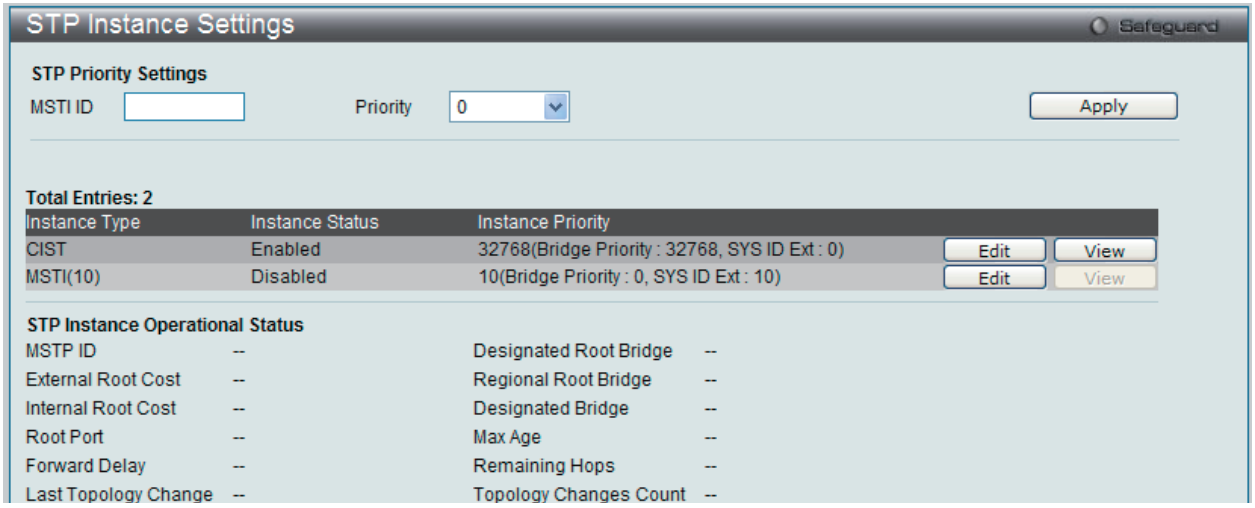


図 9-46　STP Instance Settings 画面

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、以下の画面を表示します。

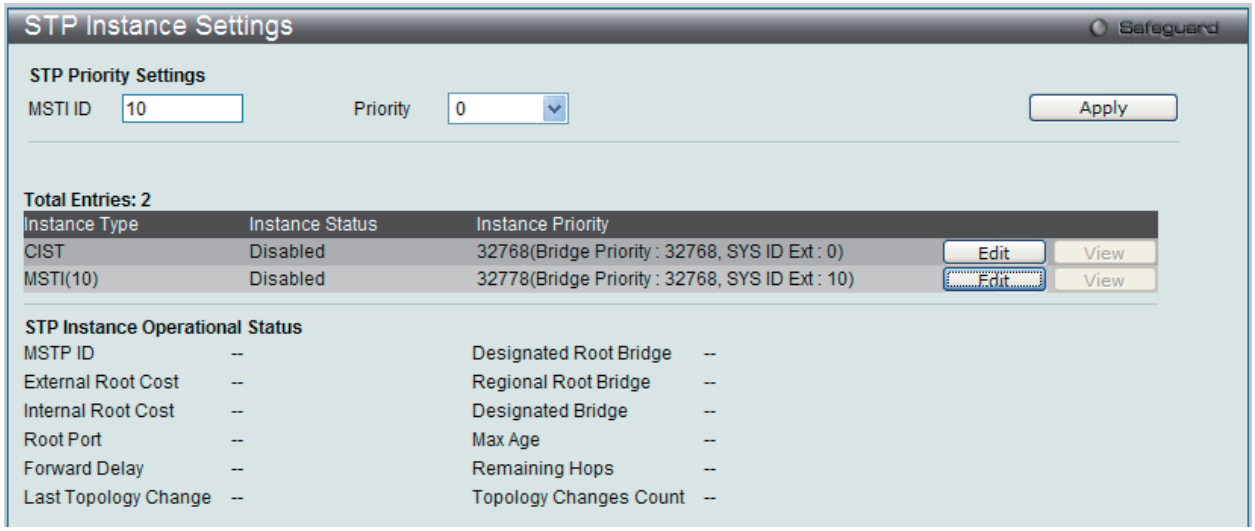


図 9-47　STP Instance Settings 画面 - Edit

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

1. 参照するエントリ横の「View」ボタンをクリックし、以下の画面を表示します。

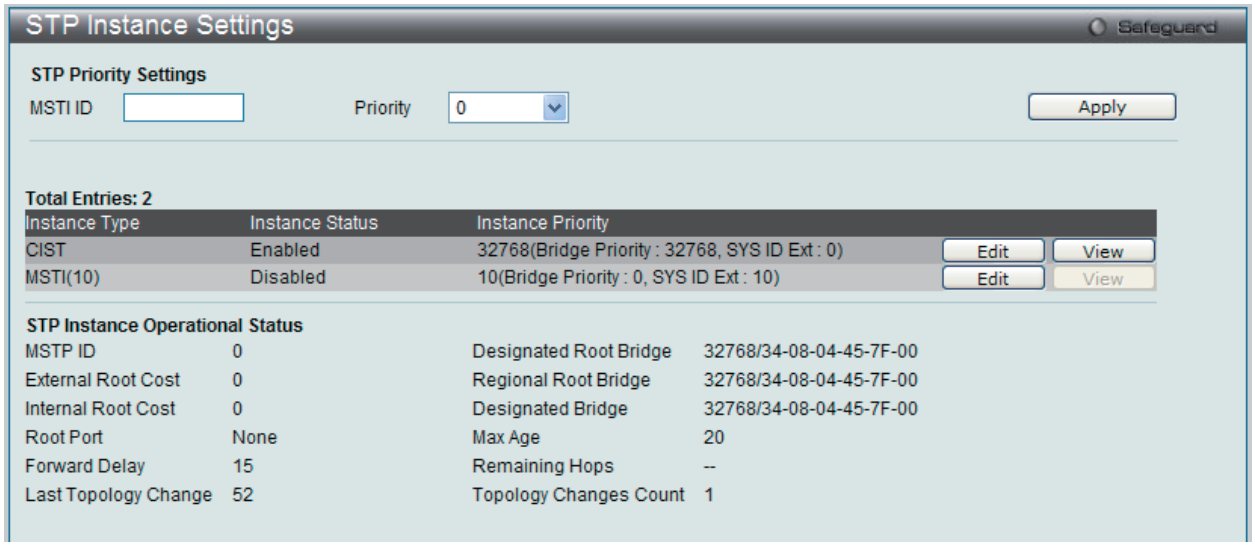


図 9-48　MST Configuration Identification 画面 - View

2. 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。

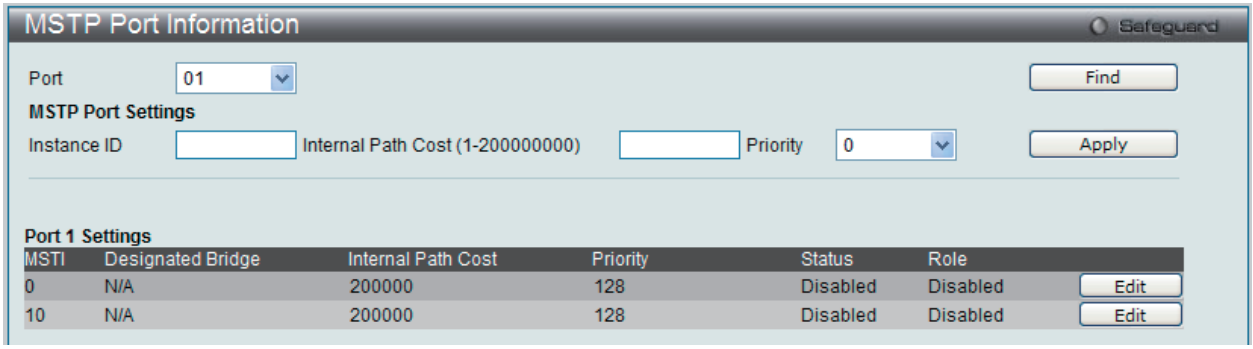


図 9-49　MSTP Port Information 画面

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、編集する MSTI の「Edit」ボタンをクリックし、以下の画面を表示します。

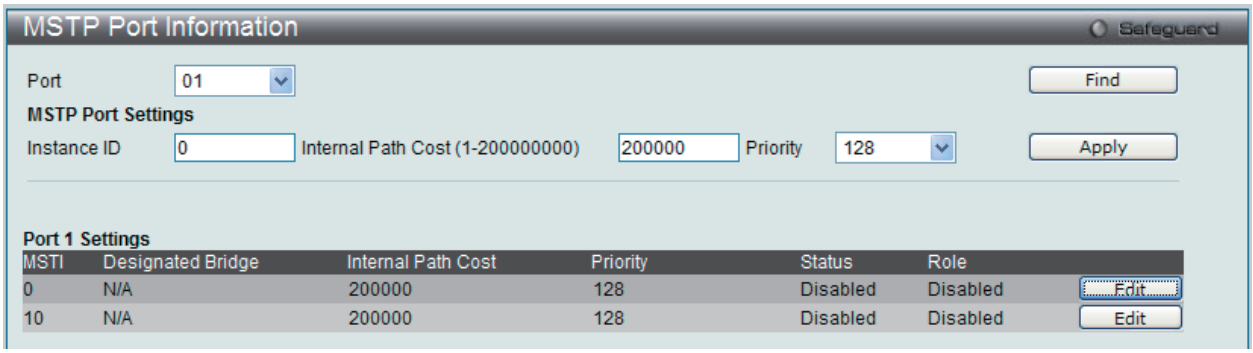


図 9-50　MSTP Port Information 画面

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 は CIST を意味します（初期値は MSTI）。
Internal Path Cost (1-200000000)	インタフェースが STP インスタンス内で選択された場合にこのポートにパケットを転送するためにかかるコストを指定します。設定内容は以下の 2 種類に分けることができます。 • 0（auto）- 自動的に最も速い経路、最適なインタフェースを設定します。インタフェースに接続されたメディアの速度を元に計算されます。（初期値） • 値 1-200000000 - ループが発生した場合、最も速く最適な経路を設定します。低いコストを指定するほど速い転送となります。
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 14 個（DES-3810-28）、最大 26 個（DES-3810-52）のポートトランクグループをサポートしています。

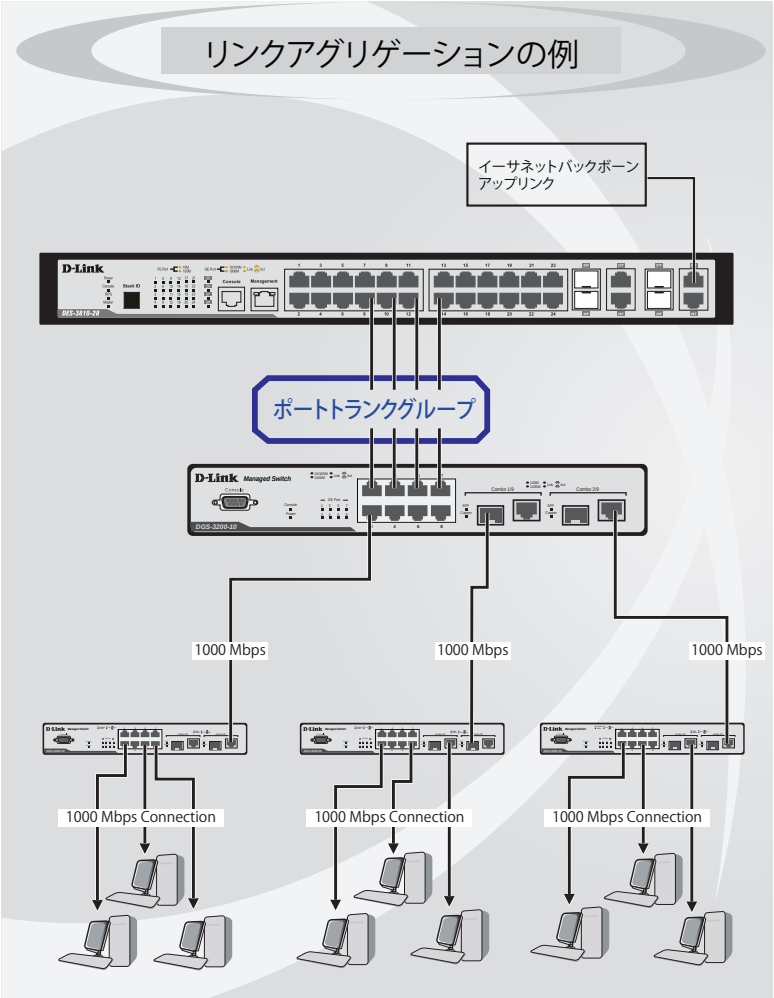


図 9-51　ポートトランクグループの例

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 14 個（DES-3810-28）、最大 26 個（DES-3810-52）のリンクアグリゲーショングループをサポートします。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。

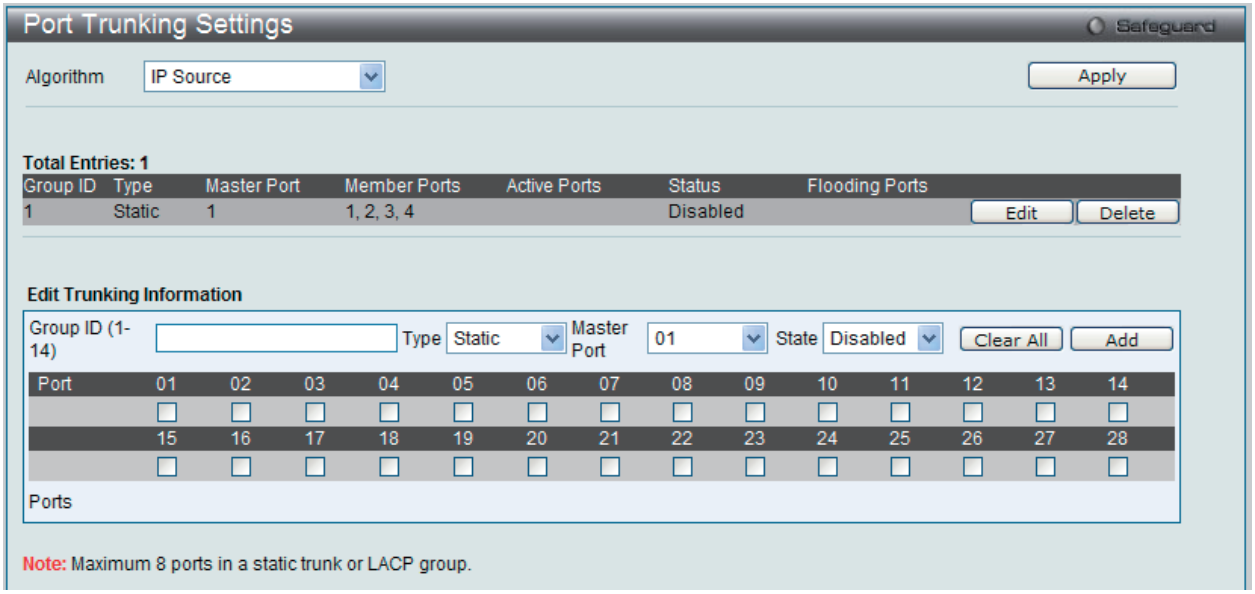


図 9-52　Port Trunking Settings 画面

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 Des」、「MAC Source Dest」、「IP Source」、「IP Dest」、「IP Source Dest」、「Layer4 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。
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、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。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、以下の画面を表示します。

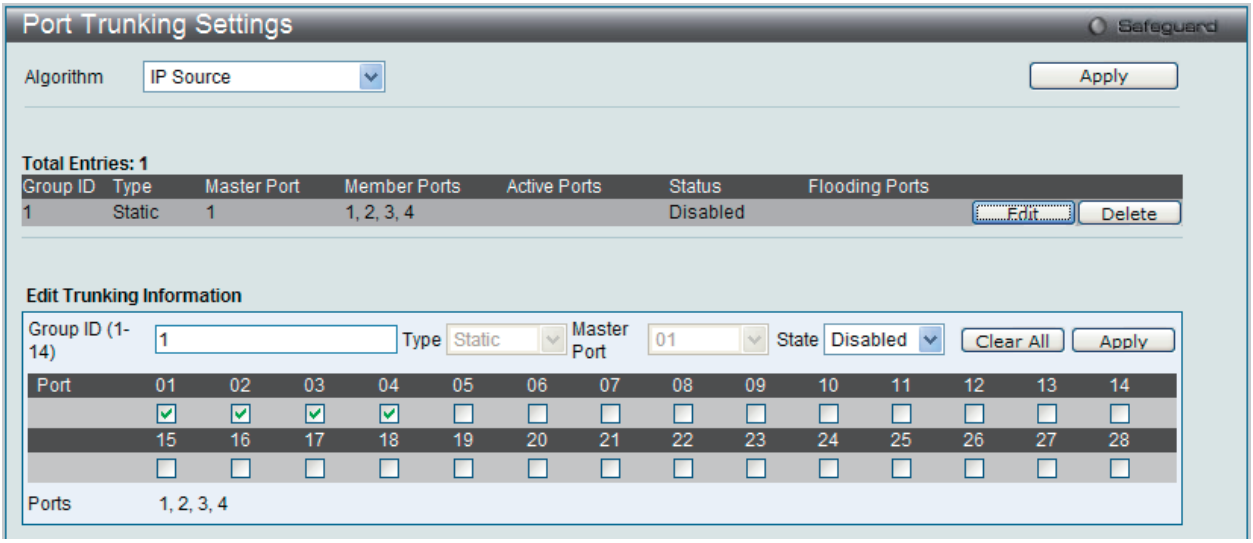


図 9-53　Port Trunking 画面 - Edit

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　1 つのスタティックトランクグループまたは LACP グループに設定できるポートの最大数は 8 ポートです。

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。

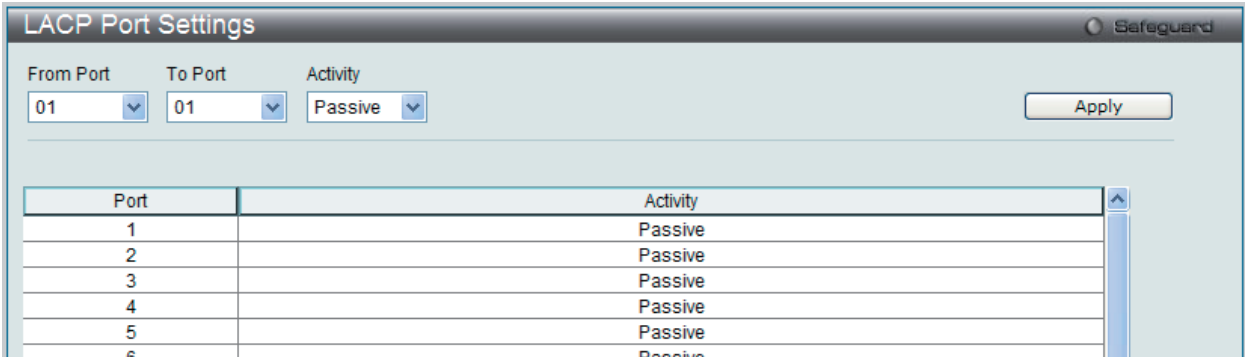


図 9-54　LACP Port Settings 画面

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。

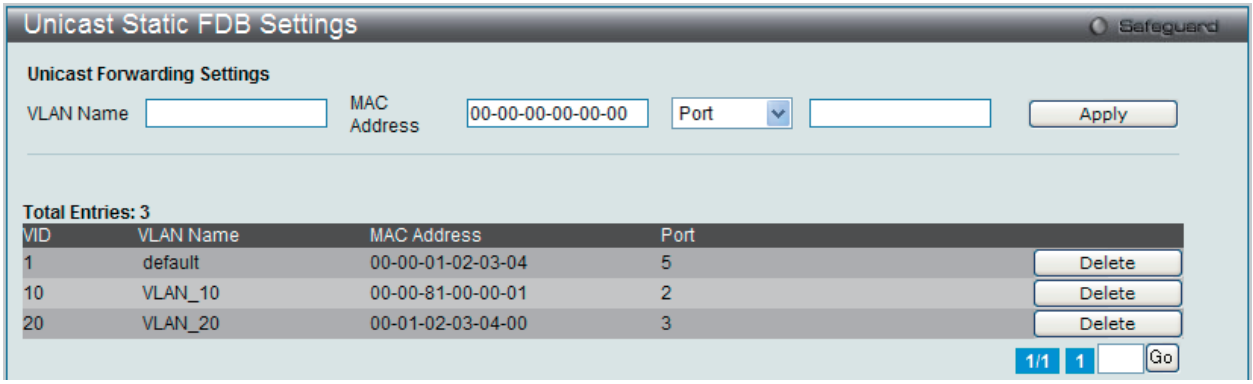


図 9-55　Unicast Static FDB Settings 画面

以下の項目を使用して設定を行います。

項目	説明
VLAN Name	関連するユニキャスト MAC アドレスが存在する VLAN 名。
MAC Address	パケットが静的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	• 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。
「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。

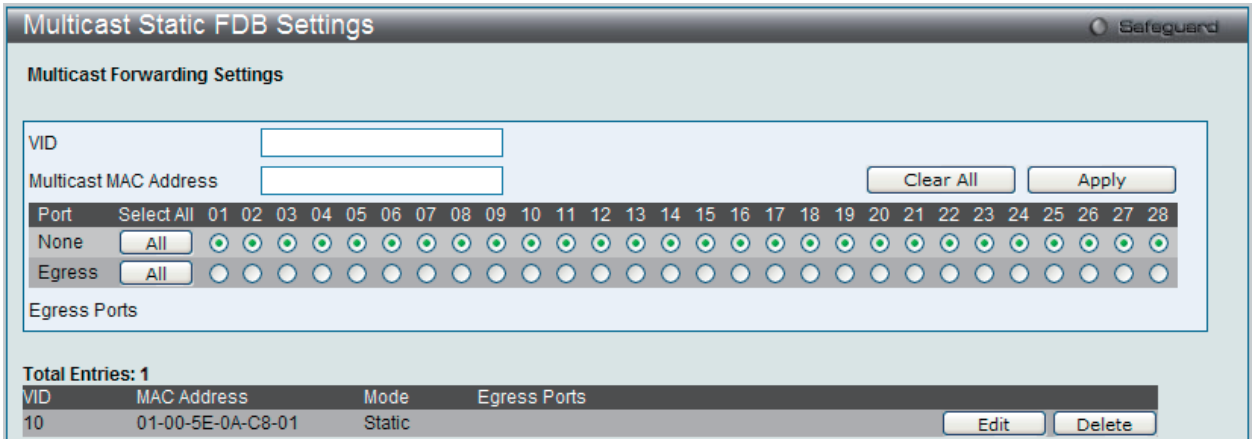


図 9-56　Multicast Static FDB Setting 画面

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以下の画面を表示します。

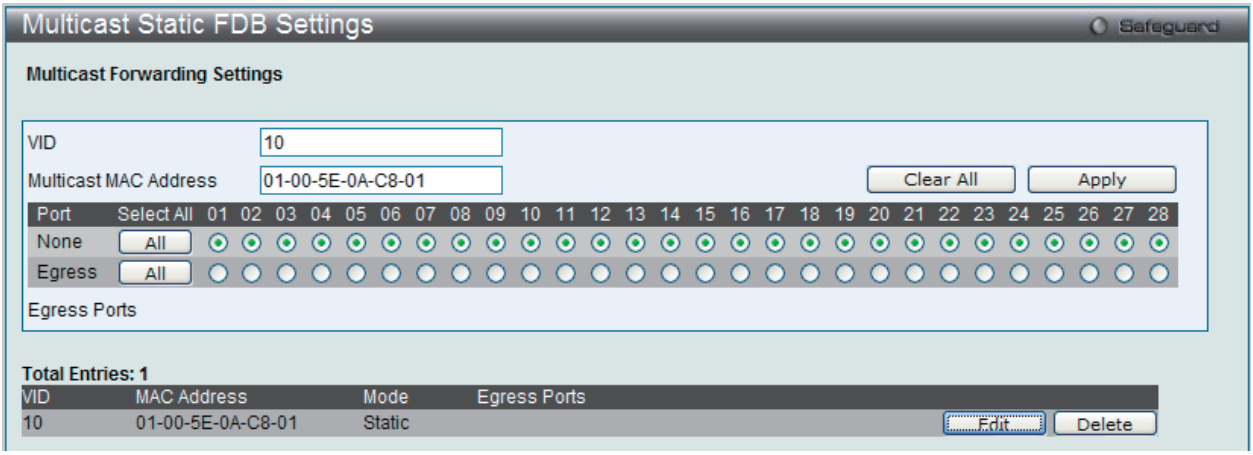


図 9-57　Multicast Static FDB Setting 画面

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。

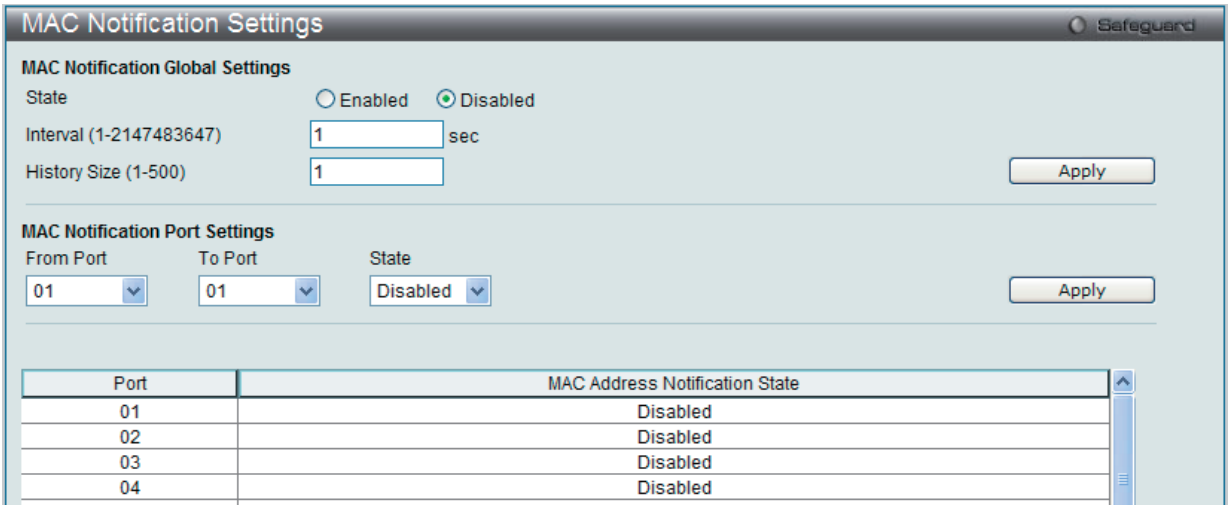


図 9-58　MAC Notification Settings 画面

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。

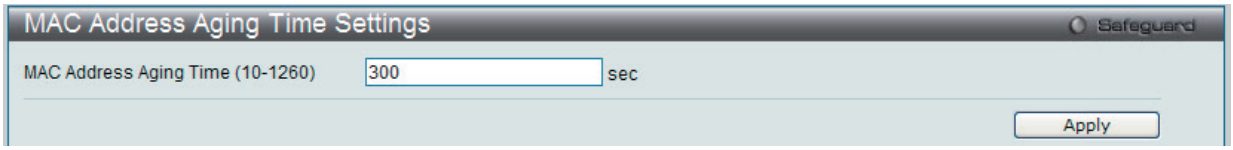


図 9-59　MAC Address Aging Time Settings 画面

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 (10-1260)	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。10-1260（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。

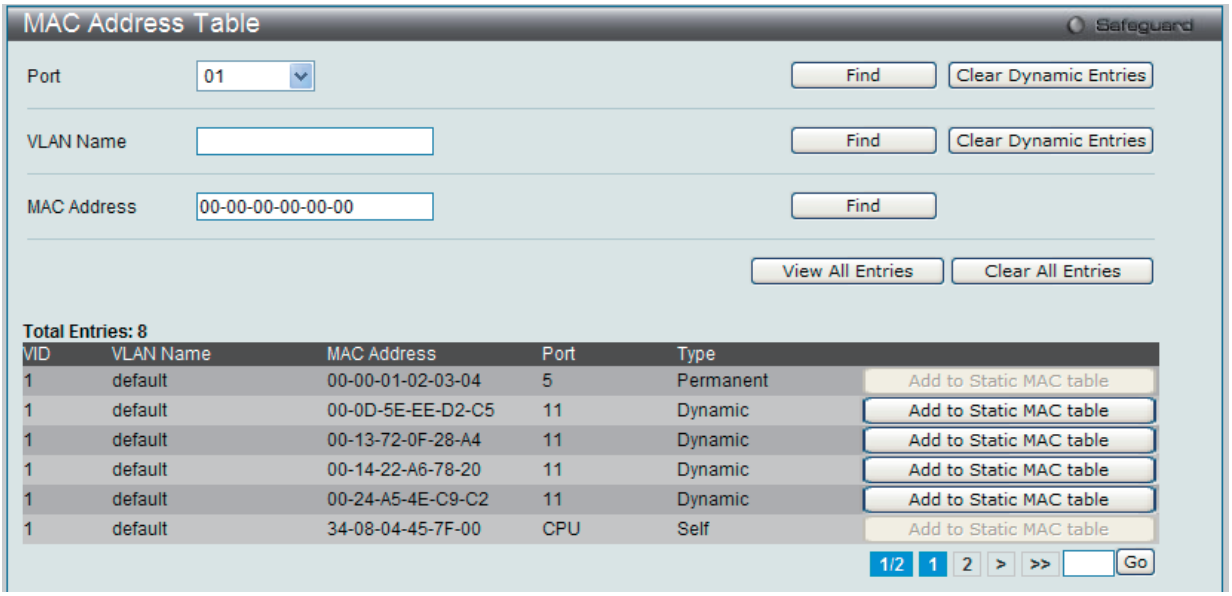


図 9-60　MAC Address Table 画面

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	フォワーディングテーブル内の検索のキーとする VLAN 名を入力します。
MAC Address	フォワーディングテーブル内の検索のキーとする MAC アドレスを入力します。
Find	指定したポート、VLAN または MAC アドレスをキーとして検索をする際にクリックします。
Clear Dynamic Entries	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。
View All Entry	アドレステーブルのすべてのエントリを表示します。
Clear All Entry	アドレステーブルのすべてのエントリを削除します。
Add to Static MAC table	スタティックテーブルに指定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。

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 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。

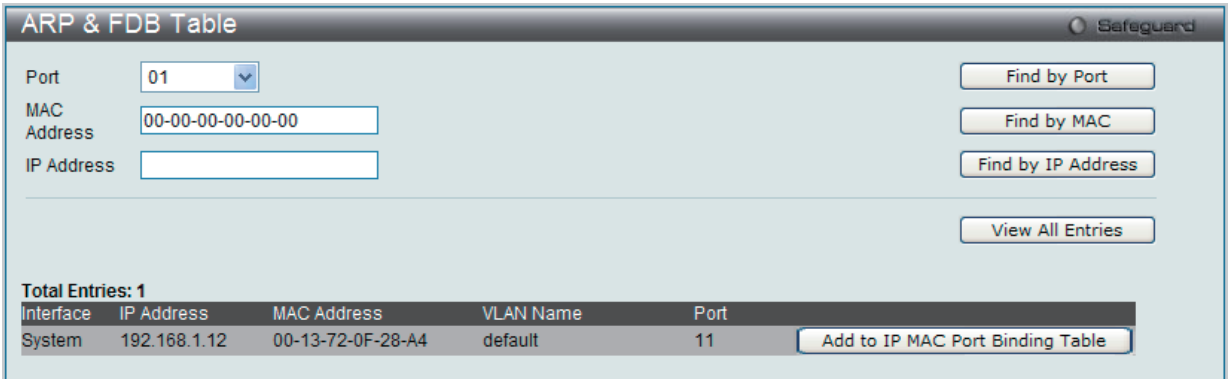


図 9-61　ARP & FDB Table 画面

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。
Find by Port	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。
Find by MAC	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。
Find by IP Address	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。
View All Entries	すべての既存エントリを表示します。
Add to IP MAC Port Binding Table	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 Proxy（IGMP プロキシ）

IGMP プロキシは、IGMP フォワーディングに基づいてアップストリームでは IGMP のホスト部分を、ダウンストリームでは IGMP のルータ部分を実行して、エッジボックスなどのデバイスに VLAN を横切るマルチキャストトラフィックを複製します。これによりコアネットワークに送信される IGMP コントロールパケット数を削減します。

IGMP Proxy Settings（IGMP プロキシ設定）

IGMP プロキシの状態と IGMP プロキシのアップストリームインタフェースを設定します。

L2 Features > L2 Multicast Control > IGMP Proxy > IGMP Proxy 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。

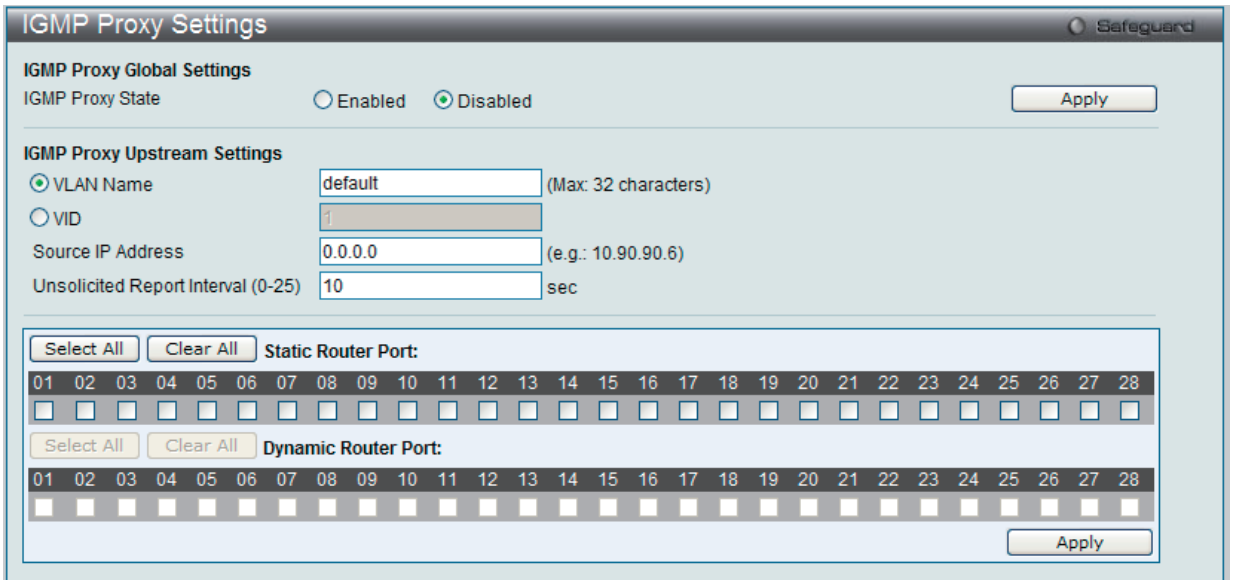


図 9-62　IGMP Proxy Settings 画面

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
IGMP Proxy State	IGMP プロキシのグローバル状態を有効または無効にします。
VLAN Name	インタフェースの VLAN 名を指定します。
VID	インタフェースの VID を指定します。
Source IP Address	プロトコルパケットの送信元 IP を指定します。指定しないと、インタフェースの IP アドレスがプロトコルの送信元 IP アドレスとして使用されます。IP インタフェースを指定しないと、システムの IP アドレスが使用されます。
Unsolicited Report Interval	Unsolicited レポート間隔を指定します。グループ内のメンバシップに関するホストの開始レポートの送信する間隔。初期値は 10（秒）です。0 に設定すると、1 つのレポートパケットだけを送信することを意味します。
Port(s)	本設定を適用するポートを選択します。

「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。
「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 Proxy Downstream Settings（IGMP プロキシダウンストリーム設定）

IGMP プロキシのダウンストリームインタフェースを設定します。IGMP プロキシのダウンストリームインタフェースは IGMP Snooping が有効である VLAN である必要があります。

L2 Features > L2 Multicast Control > IGMP Proxy > IGMP Proxy Downstream 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。

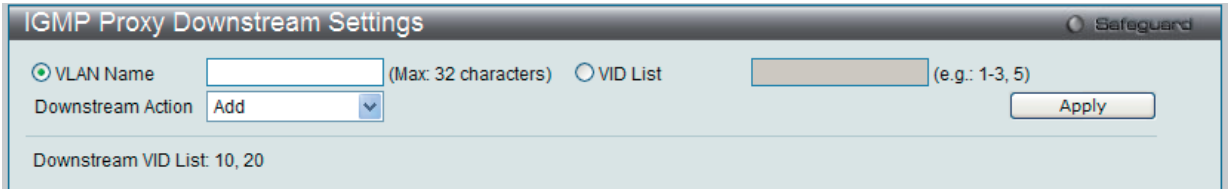


図 9-63　IGMP Proxy Downstream Settings 画面

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
VLAN Name	IGMP プロキシダウンストリームインタフェースに所属する VLAN 名を指定します。
VID List	IGMP プロキシダウンストリームインタフェースに所属する VLAN のリストを指定します。
Downstream Action	ダウンストリームインタフェースの「Add」（追加）または「Delete」（削除）を行います。

「Apply」ボタンをクリックして行った変更を適用します。

IGMP Proxy Group（IGMP プロキシグループ）

IGMP プロキシグループ設定を参照します。

L2 Features > L2 Multicast Control > IGMP Proxy > IGMP Proxy 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。

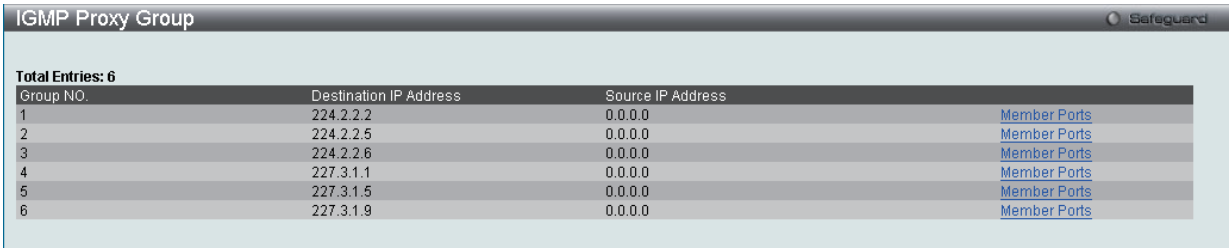


図 9-64　IGMP Proxy Group 画面

「Member Ports」リンクをクリックして、IGMP プロキシメンバポートを参照します。以下の画面が表示されます。

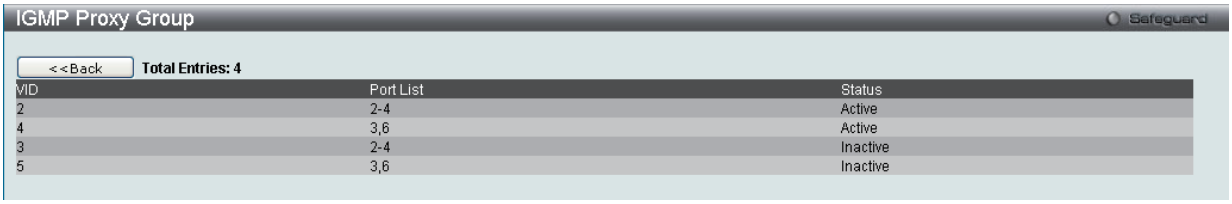


図 9-65　IGMP Proxy Group 画面

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。

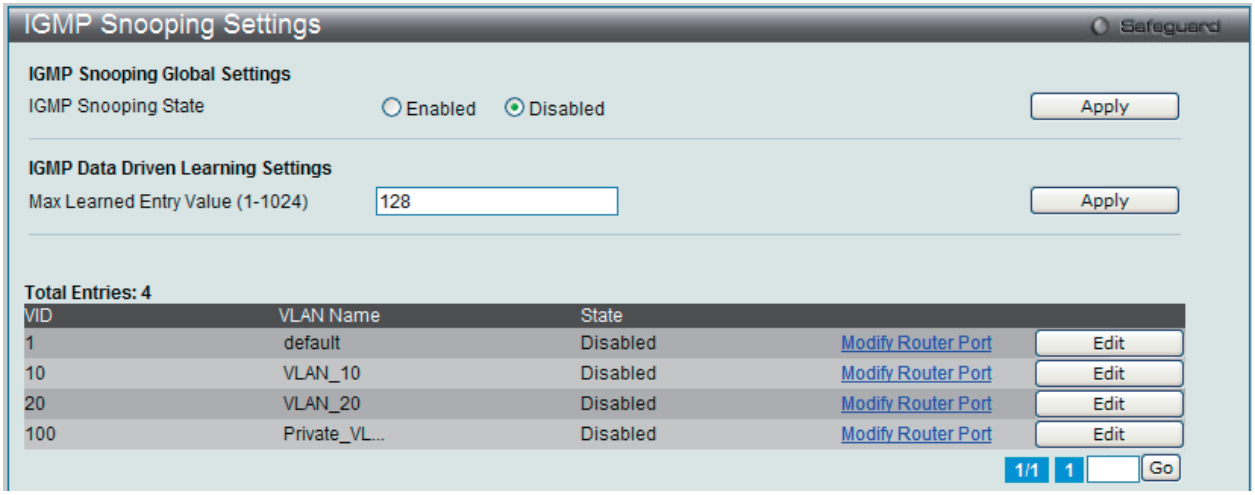


図 9-66　IGMP Snooping Settings 画面

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）
IGMP Data Driven Learning Settings	
Max Learned Entry Value (1-1024)	学習エントリの最大値を 1 から 1024 で入力します。

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 Data Driven Learning の設定

1. 「IGMP Data Driven Learning Settings」セクションの「Max Learned Entry Value (1-1024)」に学習エントリの最大値を 1 から 1024 で入力します。
2. 「Apply」ボタンをクリックして、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 に対しての詳細な設定を行います。

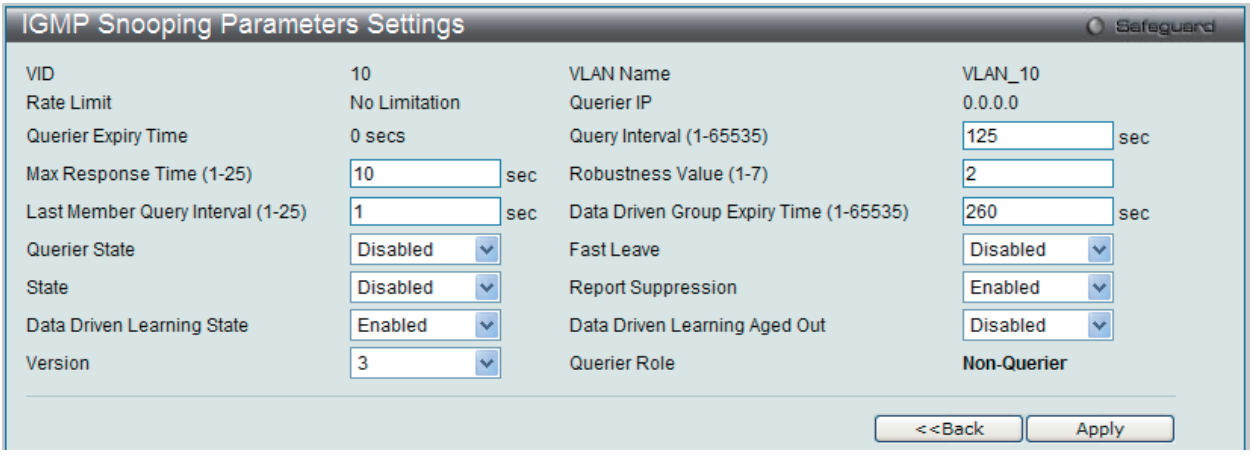


図 9-67　IGMP Snooping Parameters Settings 画面

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
VLAN ID	VLAN ID を指定します。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 名を指定します。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 / 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 アドレスを入力します。
Querier Expiry Time	クエリアの有効時間を表示します。
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。
Query Interval (1-65535)	IGMP クエリを送信する間隔を 1-65535（秒）の範囲から指定します。初期値は 125（秒）です。
Robustness Value (1-255)	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 メッセージ間隔を計算して使用されます。1-255 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 Drive Group Expiry Time	Data Driven グループのライフタイム (秒) を指定します。
Querier State	有効または無効にして、IGMP Query パケットの送信を可能または不可能にします。初期値は無効です。
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。 • 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 - スイッチは 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 Driven Learning Aged Out	指定した VLAN の IGMP Snooping data driven データ学習のタイムアウトを有効または無効にします。
Version	指定ポートによって送信される IGMP パケットのバージョンを指定します。インタフェースが受信した IGMP パケットが指定のバージョン以降のバージョンを持つ場合、パケットはルータポートから転送されるか、または VLAN にフラッドされます。初期値は 3 です。
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 IGMP Query パケットの送信を行います。 • Non-Querier - スイッチが IGMP 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。

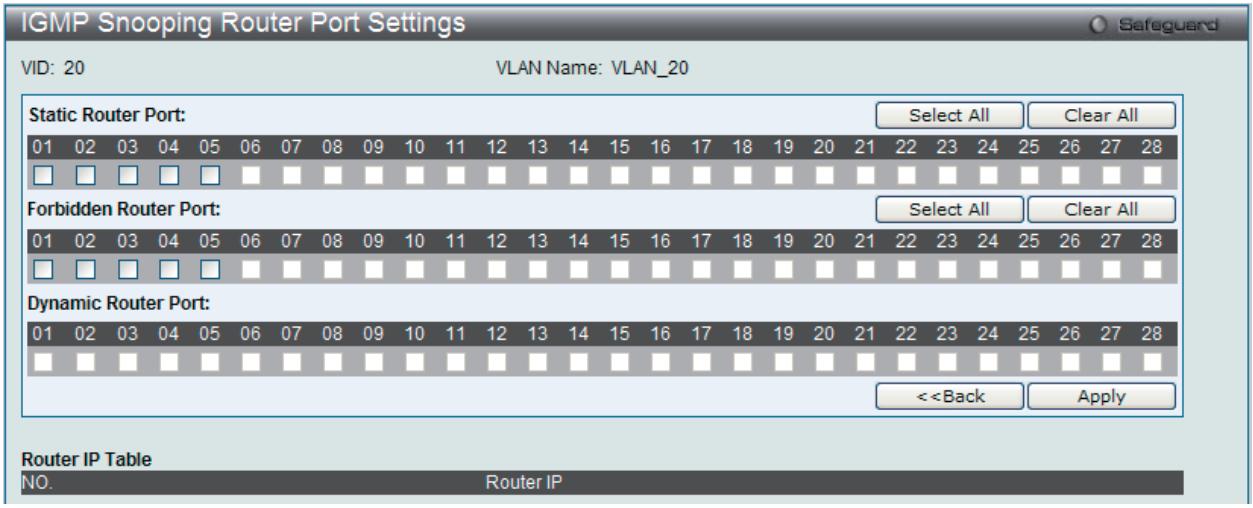


図 9-68　IGMP Snooping Router Ports Settings 画面

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。
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。

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。

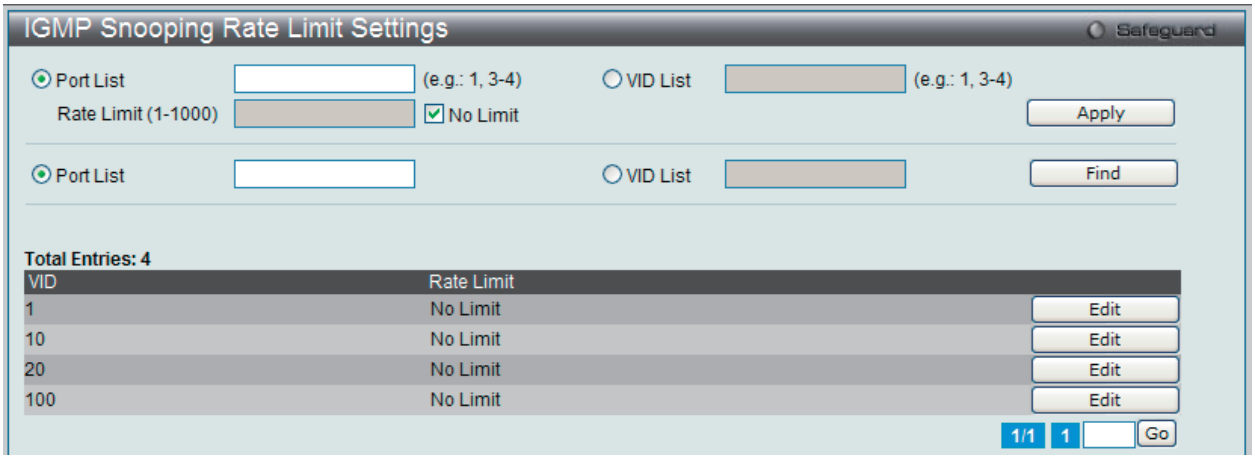


図 9-69　IGMP Snooping Rate Limit Settings 画面

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	使用する IGMP Snooping レート制限を入力します。「No Limit」オプションを選択することで、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、以下の画面を表示します。

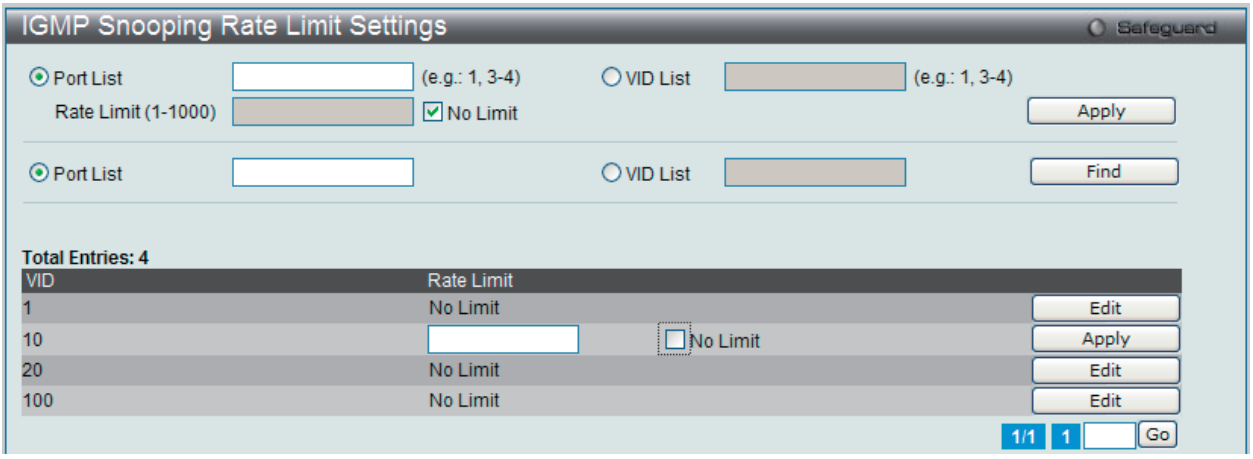


図 9-70　IGMP Snooping Rate Limit Settings 画面

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 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 9-71　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。
VID List	マルチキャストグループの VID リスト。
IPv4 Address	IPv4 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。
「Create」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、入力した情報に基づいて指定エントリを削除します。
「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。
「Edit」ボタンをクリックして、指定エントリを編集します。
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。

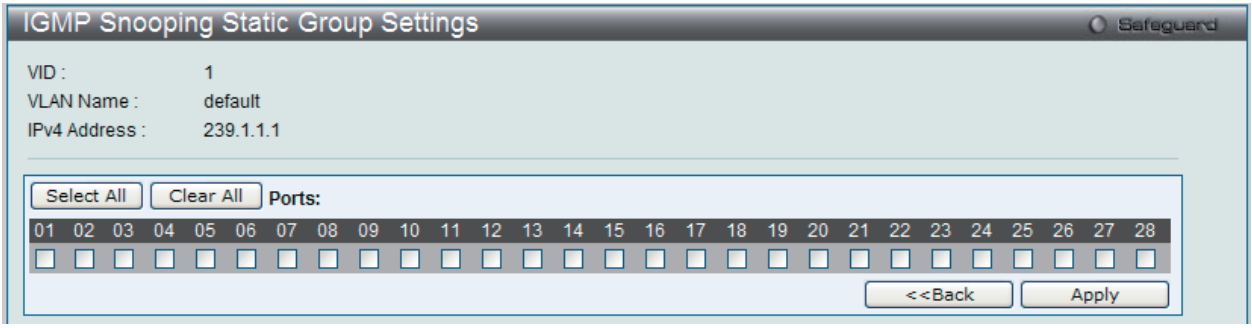


図 9-72　IGMP Snooping Static Group Settings 画面

「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。

IGMP Router Port（ルータポート参照）

この画面では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 Router Port メニューをクリックし、「Browse Router Port」画面を表示します。

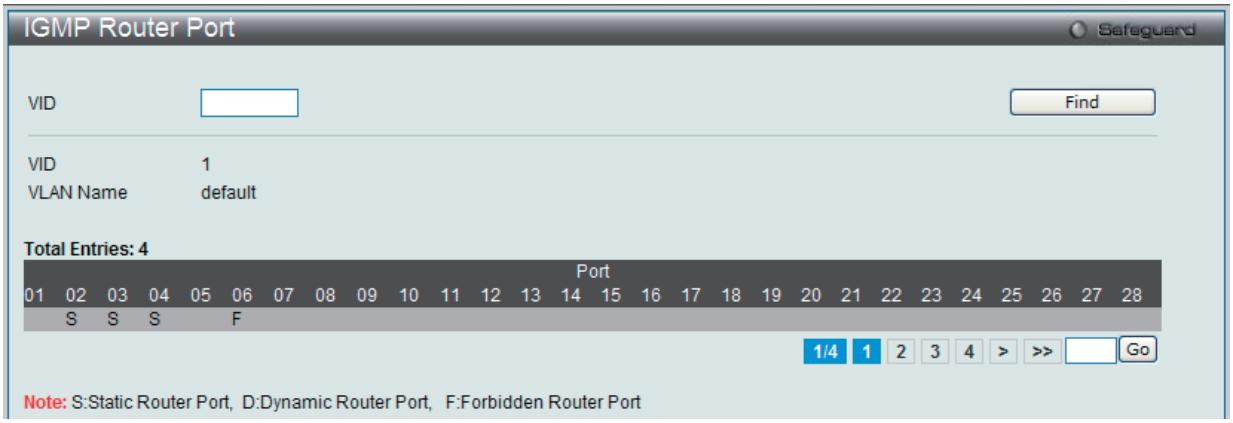


図 9-73　IGMP Router Port 画面

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。

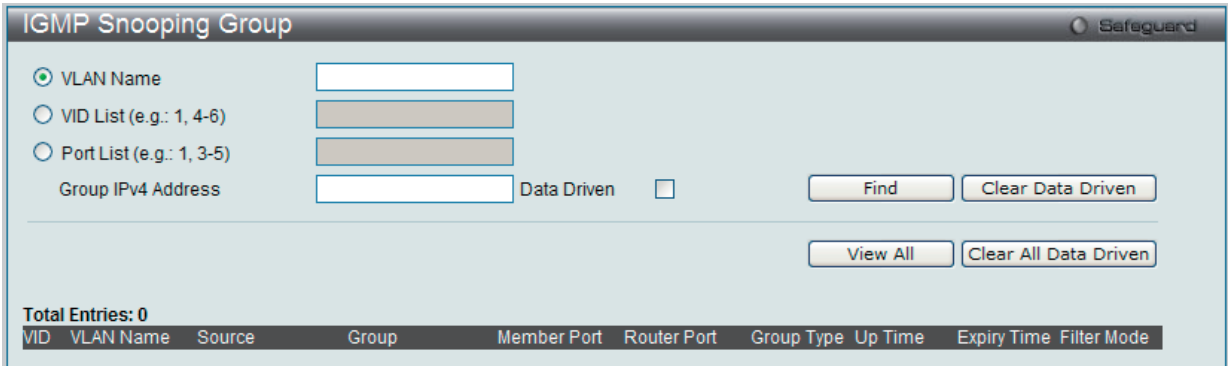


図 9-74　IGMP Snooping Group 画面

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。

以下の項目を使用して、検索します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List (e.g.: 1, 4-6)	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	Data Driven を選択すると、Data Driven グループだけが表示されます。

検索されたエントリは「IGMP 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。
「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 IGMP 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、Data Driven 機能が学習したすべての IGMP Snooping グループを削除します。

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。

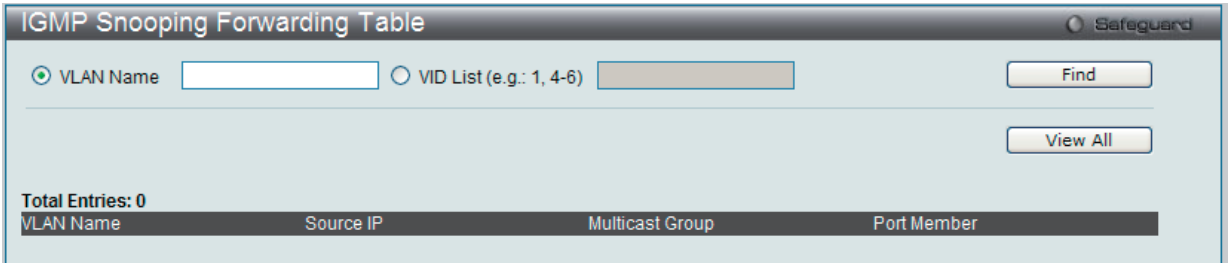


図 9-75　IGMP Snooping Forwarding Table 画面

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。

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。

「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 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。

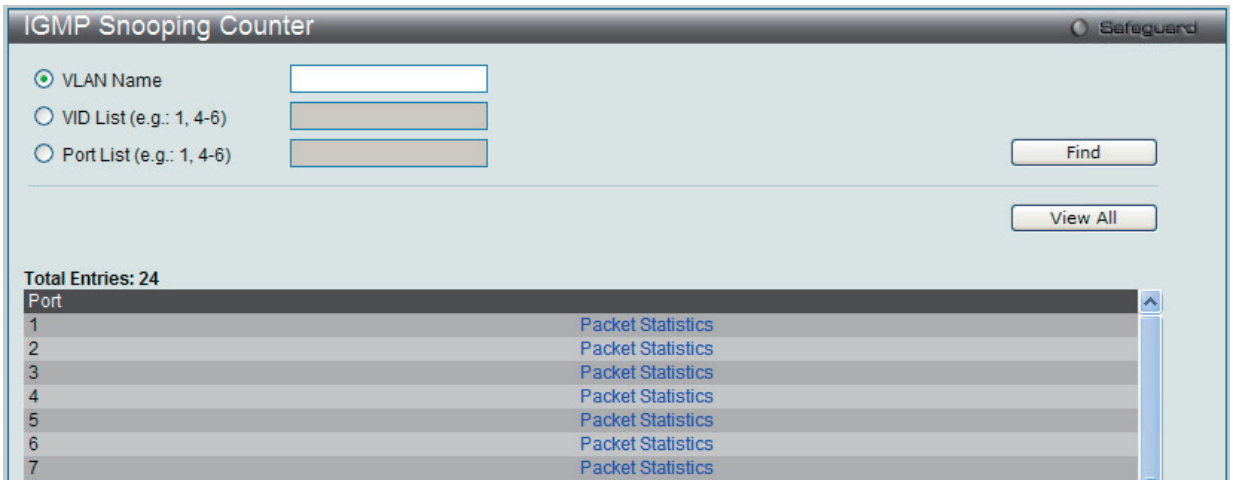


図 9-76　IGMP Snooping Counter 画面

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。

「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。

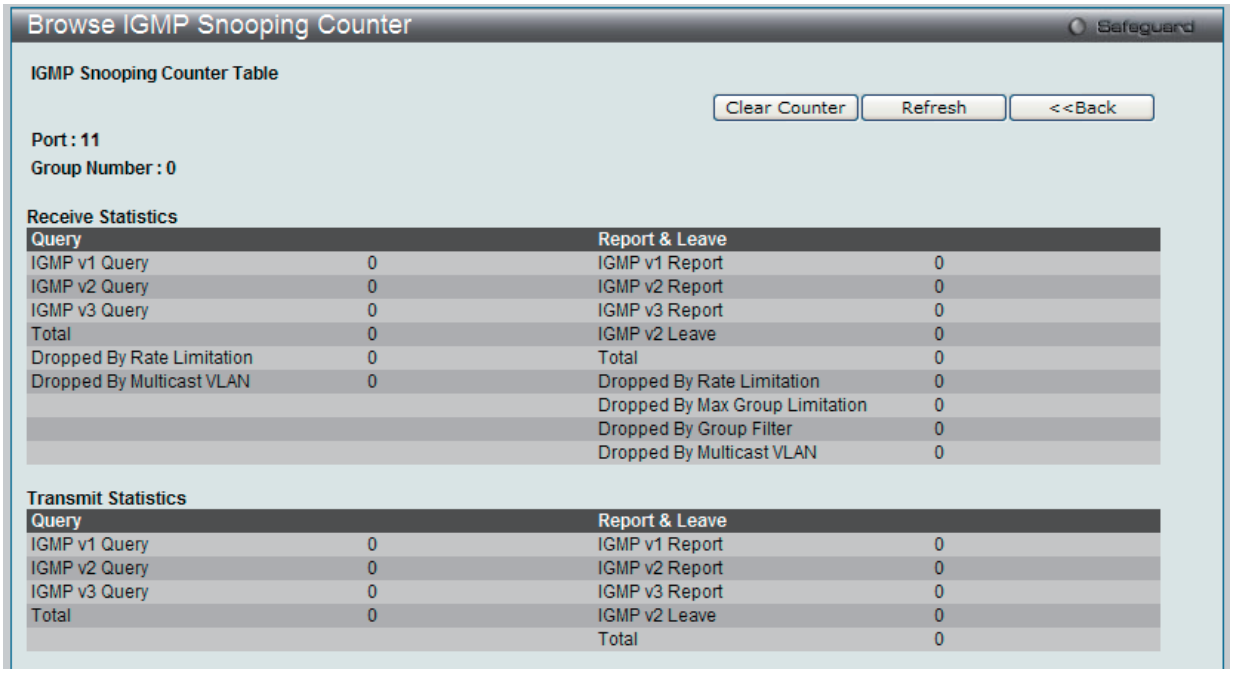


図 9-77　Browse IGMP Snooping Counter 画面

「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。

IGMP Host Table（IGMP ホストテーブル）

IGMP ホストテーブルを参照します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Host 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。

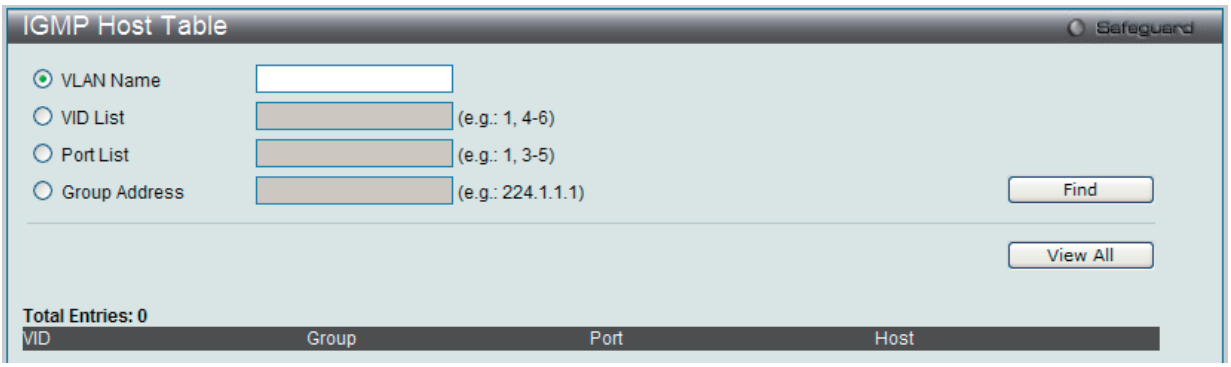


図 9-78　IGMP Host Table 画面

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。
Port List	マルチキャストグループのポートリスト。
Group Address	マルチキャストグループのグループアドレス。

「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。

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

いくつかの DoS（Denial of Service）攻撃は大量のネットワーク制御プロトコルをブロードキャストすることで行われます。初期値では、スイッチの CPU は、これらのプロトコルを処理して、ローカルデータベースを更新します。しかし、ハッカーが偽装した、または、大量の制御パケットを送信すると、スイッチ CPU は過負荷状態となり、正常なトラフィックを処理できなくなります。

L3 制御パケットフィルタリングによって、スイッチはそれらを持つべきではないポート（つまり UNI ポート）から受信した異常な制御パケットを破棄します。

レイヤ 3 制御パケットフィルタ用のポートの状態を有効または無効にします。有効にすると、レイヤ 3 制御パケットは破棄されます。

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。

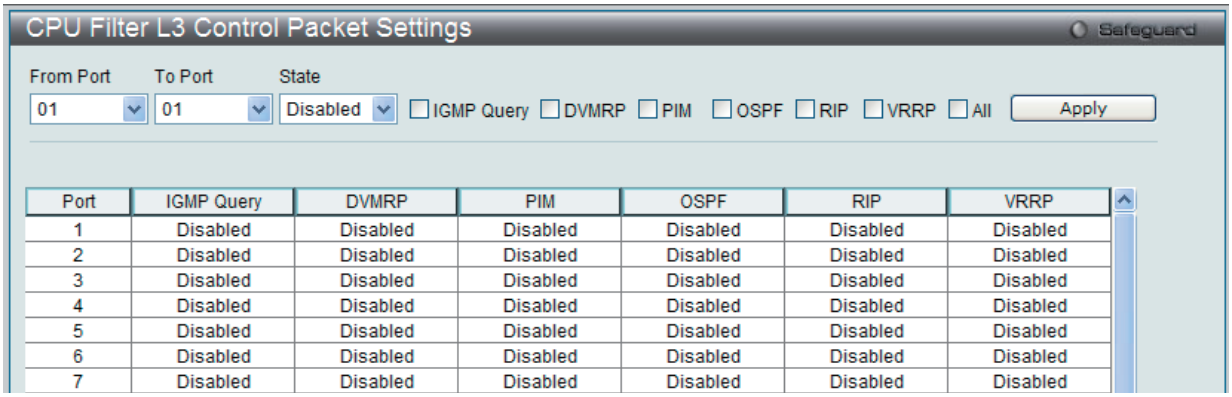


図 9-79　CPU Filter L3 Control Packet Settings 画面

以下の項目が表示されます。

項目	説明
From Port / To Port	CPU フィルタリング設定に使用するポート範囲を選択します。
State	CPU フィルタリングを有効または無効にします。
IGMP Query	CPU フィルタリングに IGMP クエリを含めます。
DVMRP	CPU Filtering フィルタリングに DVMRP を含めます。
PIM	CPU フィルタリングに PIM を含めます。
OSPF	CPU フィルタリングに OSPF を含めます。
RIP	CPU フィルタリングに RIP を含めます。
VRRP	CPU フィルタリングに VRRP を含めます。
All	CPU フィルタリングにすべての情報を含めます。

「Apply」ボタンをクリックして行った変更を適用します。

注意 CPU が高負荷である場合にだけこれらの機能を有効にすることをお勧めします。不当なフィルタリングルールはシステムに異常な動作を引き起こす可能性があります。

MLD Proxy（MLD プロキシ）

MLD プロキシはアップストリームインタフェースでホストの役割を果たします。MLD Report パケットはルータポートに送信されます。MLD プロキシはダウンストリームインタフェースでルータの役割を果たします。これによりコアネットワークに送信される MLD コントロールパケット数を削減します。

MLD Proxy Settings（MLD プロキシ設定）

MLD プロキシの状態と MLD プロキシのアップストリームインタフェースを設定します。

L2 Features > L2 Multicast Control > MLD Proxy > MLD Proxy 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。

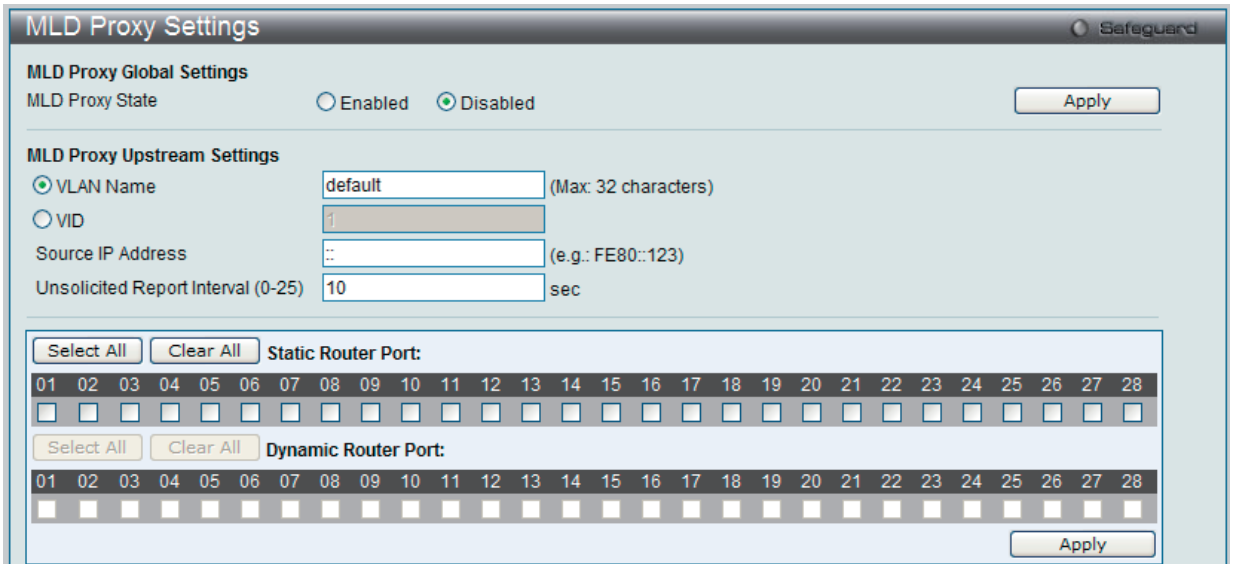


図 9-80　MLD Proxy Settings 画面

以下の項目が表示されます。

項目	説明
MLD Proxy Global Settings	
MLD Proxy State	MLD プロキシのグローバル状態を有効または無効にします。
MLD Proxy Upstream Settings	
VLAN Name	インタフェースの VLAN 名。
VID	インタフェースの VID。
Source IP Address	プロトコルパケットの送信元 IP。指定しないと、ゼロ IP アドレスが使用されます。
Unsolicited Report Interval	Unsolicited レポート間隔。グループ内のメンバシップに関するホストの開始レポートの送信する間隔。初期値は 10(秒) です。0 に設定されると、1 つのレポートパケットだけを送信することを意味します。
Static Router Port	設定に適用するスタティックルータポートを入力します。
Dynamic Router Port	マルチキャストが有効なルータに接続するポートリストを表示します。

「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。
「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。

MLD Proxy Downstream Settings（MLD プロキシダウンストリーム設定）

MLD プロキシのダウンストリームインタフェースを設定します。MLD プロキシのダウンストリームインタフェースは MLD Snooping が有効である VLAN である必要があります。

L2 Features > L2 Multicast Control > MLD Proxy > MLD Proxy Downstream 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。

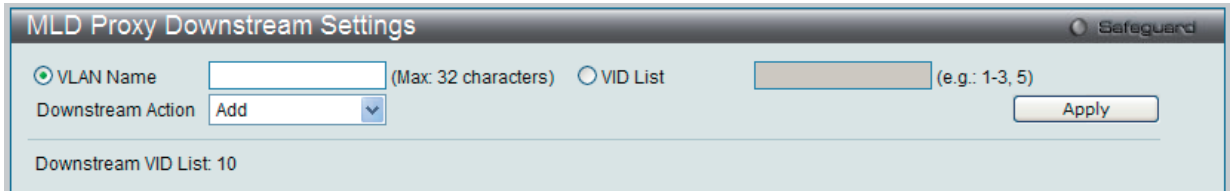


図 9-81　MLD Proxy Downstream Settings 画面

以下の項目が表示されます。

項目	説明
VLAN Name	インタフェースの VLAN 名。
VID List	インタフェースの VID リスト。
Downstream Action	適切な操作を選択します。 • Add - ダウンストリームインタフェースを追加します。 • Delete - ダウンストリームインタフェースを削除します。

「Apply」ボタンをクリックして行った変更を適用します。

MLD Proxy Group（MLD プロキシグループ）

MLD プロキシグループ設定を参照します。

L2 Features > L2 Multicast Control > MLD Proxy > MLD Proxy 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。

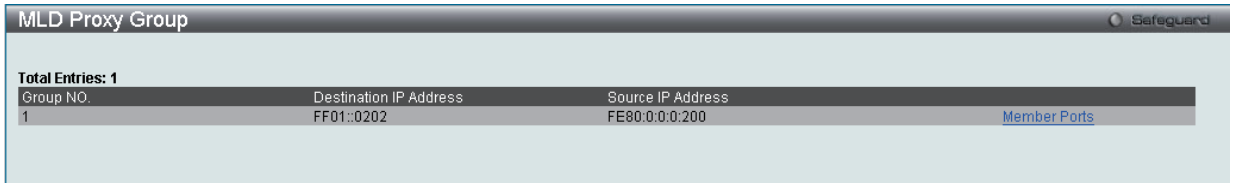


図 9-82　MLD Proxy Group 画面

MLD プロキシメンバポートの参照

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

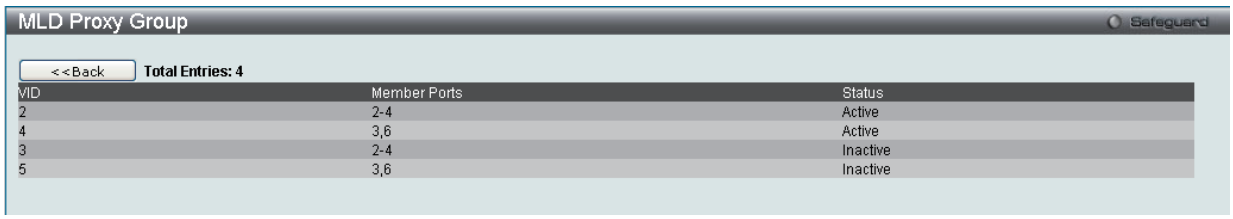


図 9-83　MLD Proxy Group 画面

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替わりに、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 ICMPv6 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 ICMPv6 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。
MLD Snooping 機能を有効にするためには、「MLD Snooping Global Settings」欄の「Enable」をチェックして「Apply」ボタンをクリックします。

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。

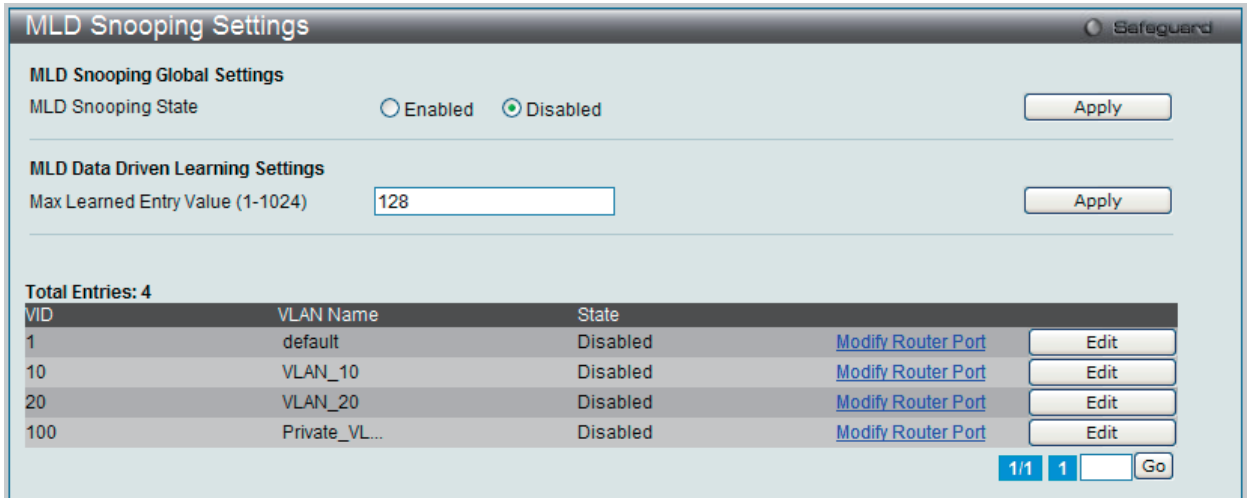


図 9-84　MLD Snooping Settings 画面

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。

MLD Snooping のグローバル設定

「MLD Snooping State」で MLD Snooping 機能を「Enabled」（有効）または「Disabled」（無効）にします。

以下の項目を指定します。

項目	説明
MLD Snooping State	MLD Snooping を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Max Learning Entry Value	学習する最大エントリ数を入力します。

「Apply」ボタンをクリックし、変更を有効にします。

「Edit」ボタンをクリックして指定エントリの MLD Snooping 項目を設定します。
「Modify Router Port」リンクをクリックして、指定ポートに MLD Snooping ルータポート設定を行います。

MLD Snooping に特定の VLAN を設定する

対応する VLAN の「Edit」ボタンをクリックして以下の画面を表示します。

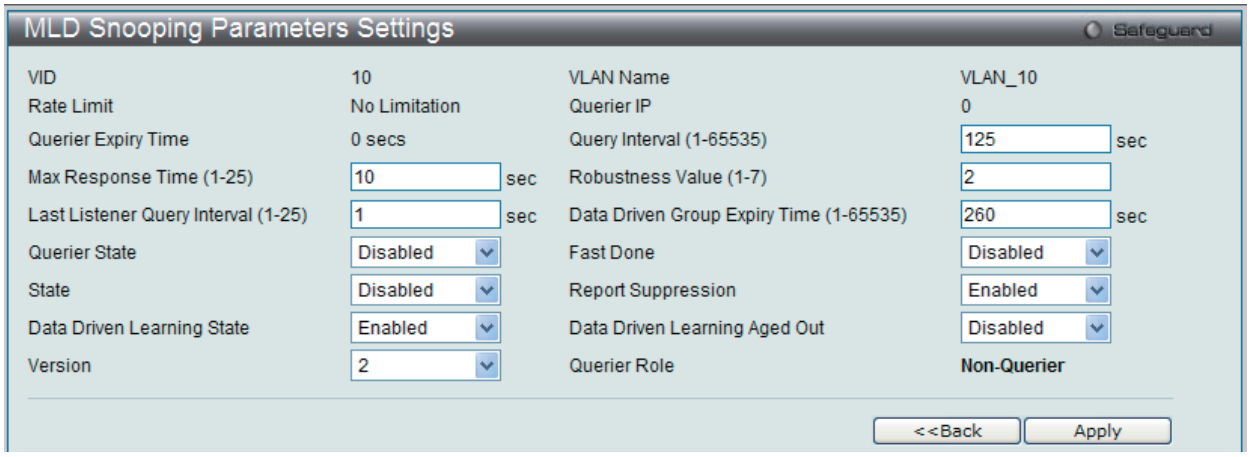


図 9-85　MLD Snooping Parameters Settings 画面

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。
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 メッセージ間隔を計算して使用されます。1-255 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。初期値は 260(秒) です。次の計算式で計算されます。: Group Listener=(Robustness Variable*Query Interval)+(1*Query Interval)。 • 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。初期値は 255（秒）です。次の計算式で計算されます。: Querier Present Interval=(Robustness Variable*Query Interval)+(0.5*Query Response Interval)。 • 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 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。 次の計算式で計算されます。: (last listener query interval * robustness variable)
Data Drive Group Expiry Time (1-65535)	Data Driven グループのライフタイム（秒）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	Report Suppression（レポート抑制）機能を有効または無効にします。この機能は、重複するレポートがマルチキャストデバイスに送信されるのを防止します。MLD レポートの抑制機能を無効にすると、すべての MLD レポートがマルチキャストルータに転送されます。
Data Driven Learning State	Data Driven Learning 状態を有効または無効にします。
Data Driven Learning Aged Out	指定した VLAN の MLD Snooping Data Driven エントリにおけるデータ学習のタイムアウトを有効または無効にします。
Version	指定ポートによって送信される MLD パケットのバージョンを指定します。インタフェースが受信した MLD パケットが指定のバージョン以降のバージョンを持つ場合、パケットはルータポートから転送されるか、または VLAN にフラッドされます。初期値は 3 です。
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。

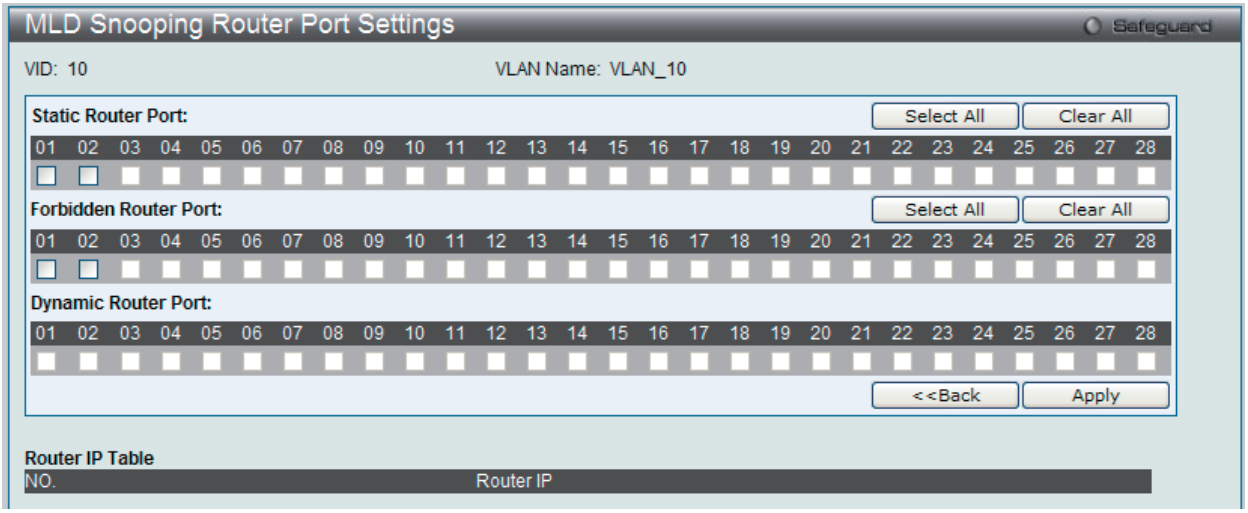


図 9-86　MLD Snooping Router Port Settings 画面

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。

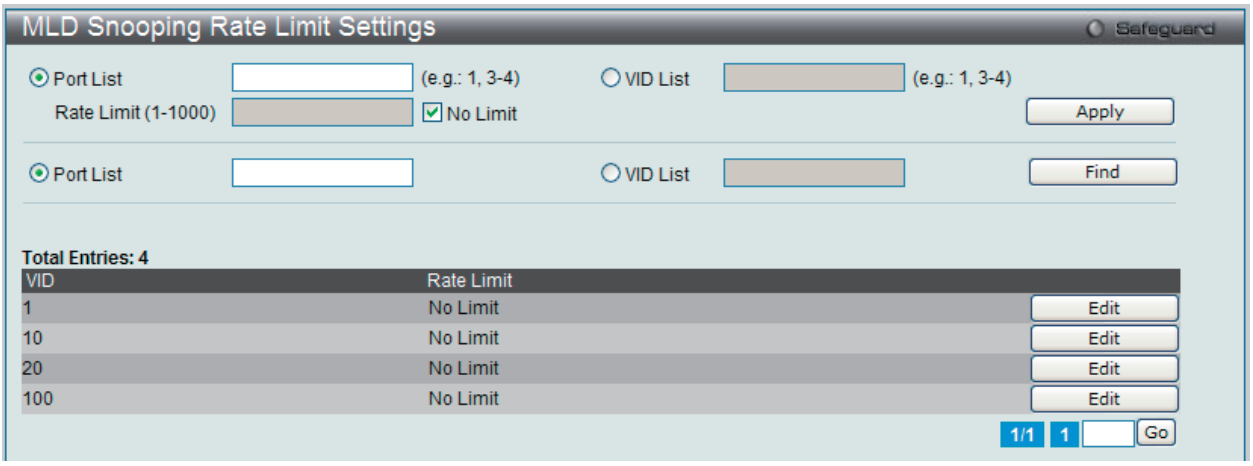


図 9-87　MLD Snooping Rate Limit Settings 画面

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。
「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、以下の画面を表示します。

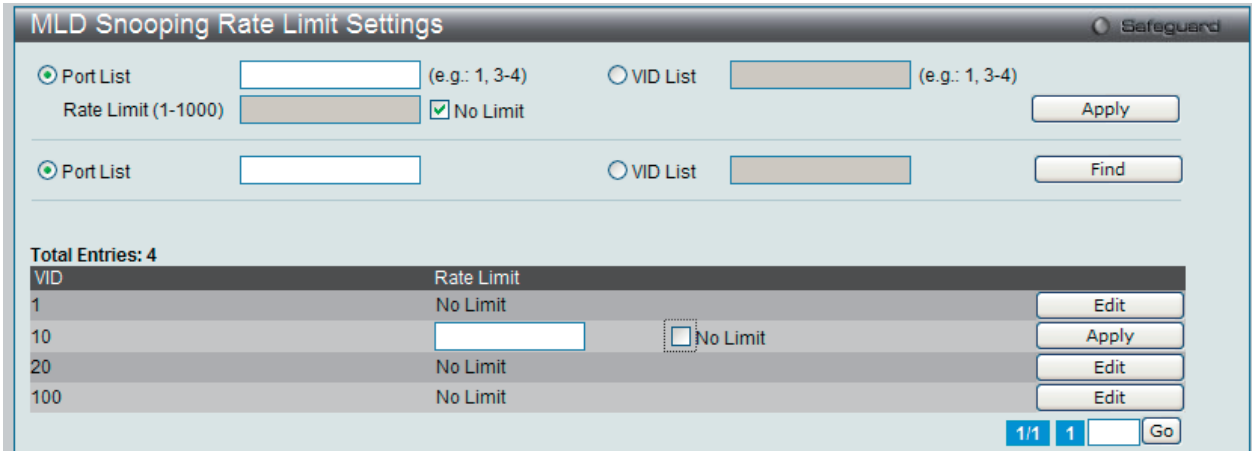


図 9-88　MLD Snooping Rate Limit Settings 画面 - Edit

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。

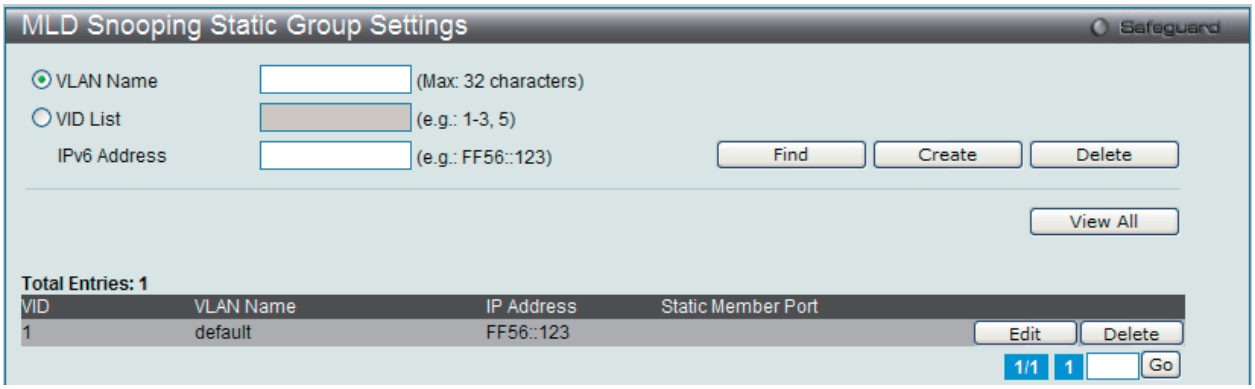


図 9-89　MLD Snooping Static Group Settings 画面

I 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。
VID List	マルチキャストグループの 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。

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

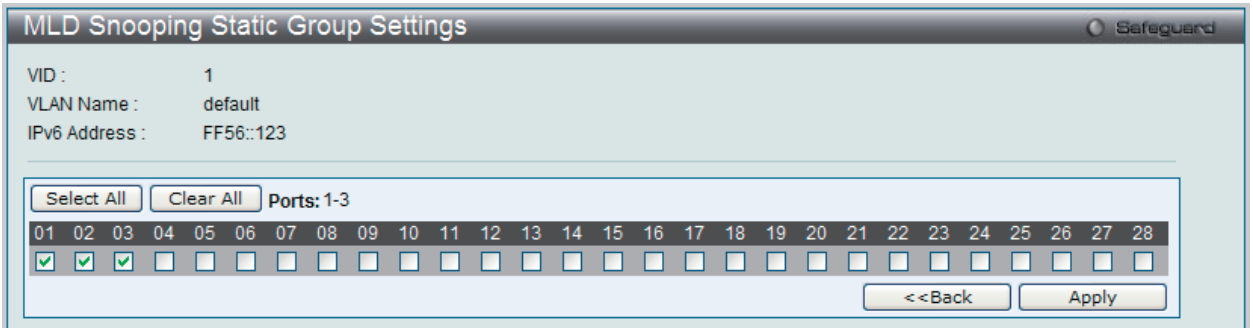


図 9-90　MLD Snooping Static Group Settings 画面

「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 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 9-91　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。

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。

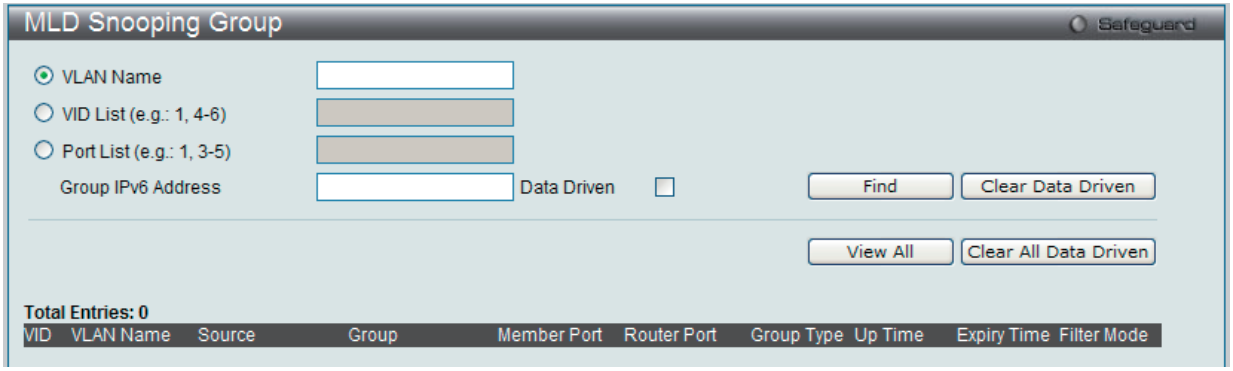


図 9-92　MLD Snooping Group 画面

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、MLD Snooping グループテーブルを検索することができます。

以下の項目を使用して、検索します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List (e.g.: 1, 4-6)	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 IPv6 Address	IPv6 アドレスを指定します。
Data Driven	Data Driven を選択すると、Data Driven グループだけが表示されます。

適切な情報を入力して、「Find」ボタンをクリックします。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。
「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、Data Driven 機能が学習したすべての MLD Snooping グループを削除します。

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。

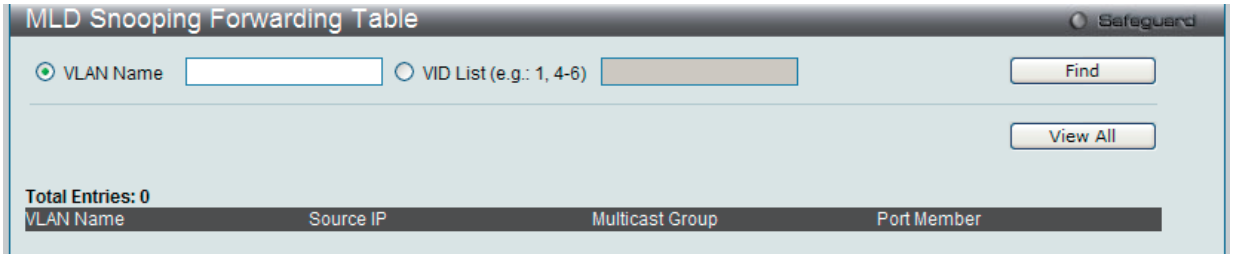


図 9-93　MLD Snooping Forwarding Table 画面

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。

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。

「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。

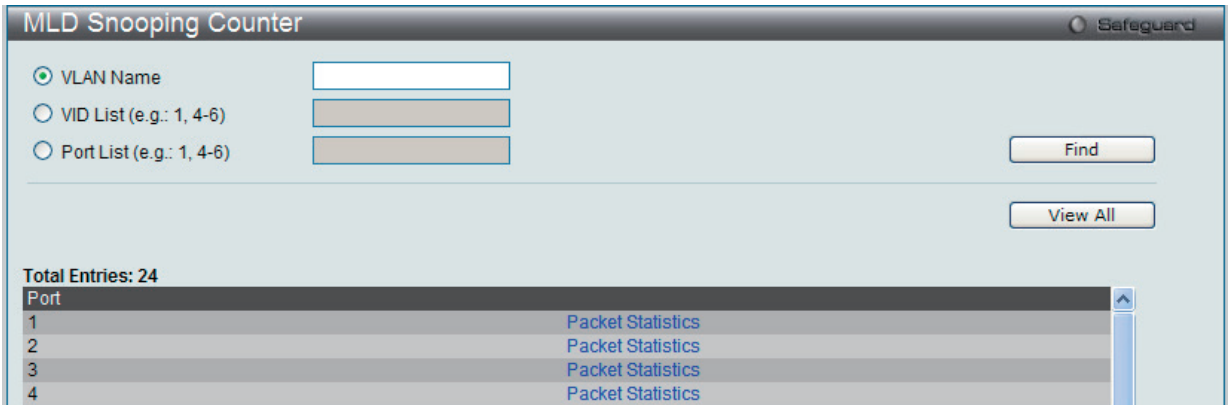


図 9-94　MLD Snooping Counter 画面

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。

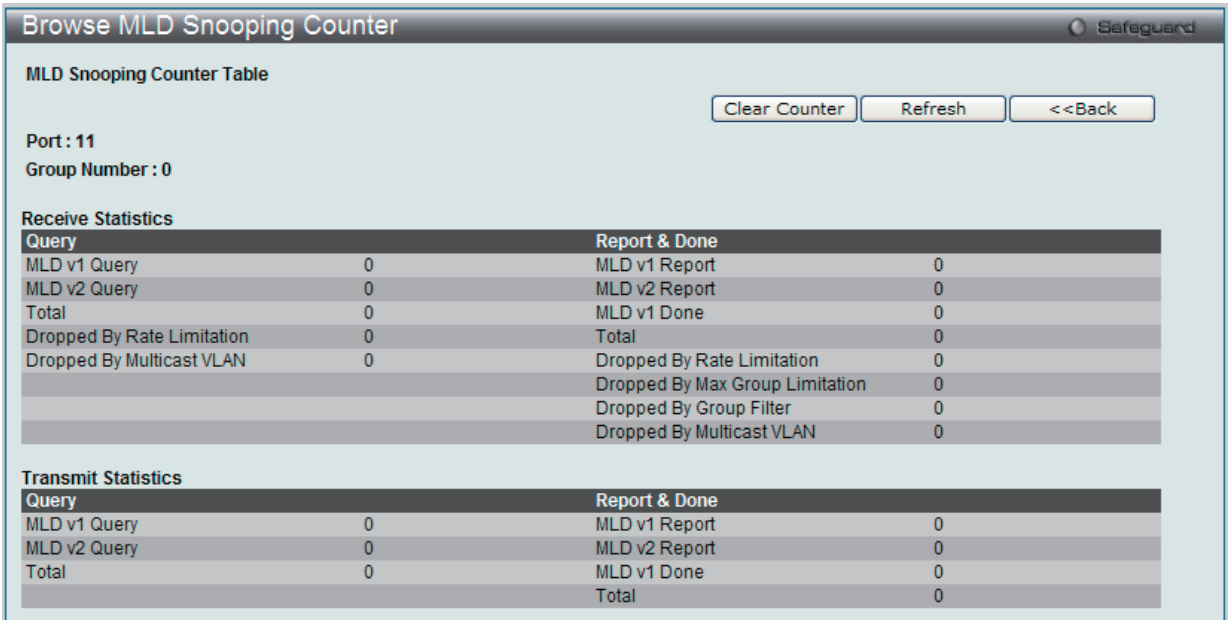


図 9-95　Browse MLD Snooping Counter 画面

「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。

MLD Host Table（MLD ホストテーブル）

スイッチの現在のホスト、ポート、またはグループを表示します。Fast Leave が有効とされると、ホストだけが有効になります。パラメータを指定しないと、スイッチの全ホストを表示します。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Host 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。

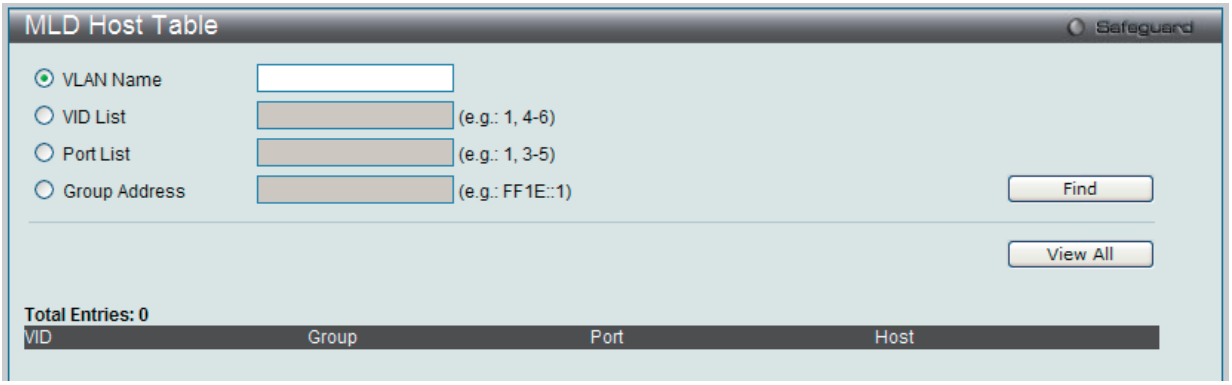


図 9-96　MLD Host Table 画面

以下の項目が表示されます。

項目	説明
VLAN Name	情報を表示するホストが所属する VLAN 名を指定します。
VID List	情報を表示するホストが所属する VLAN ID を指定します。
Port List	情報を表示するホストが所属するポート範囲を指定します。
Group Address	情報を表示するホストが所属するグループの IPv6 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。
「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。

Multicast VLAN（マルチキャスト VLAN）

スイッチング環境には、複数の VLAN が存在します。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複数の 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複数の 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 ISM 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 Group 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。

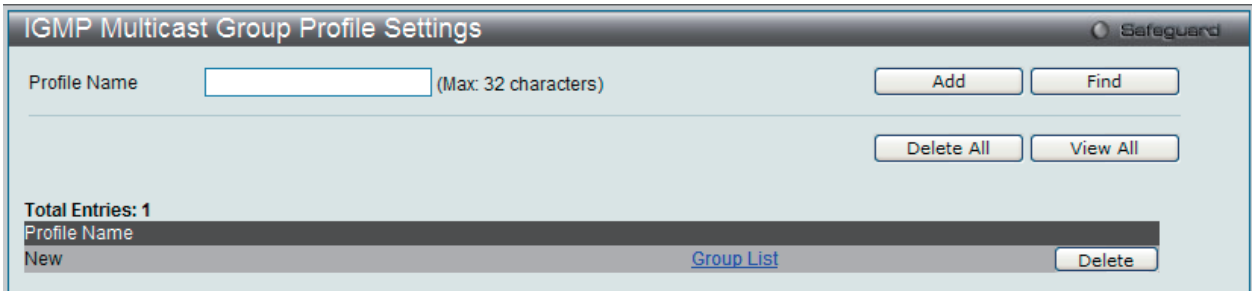


図 9-97　IGMP Multicast Group Profile Settings 画面

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。
「Group List」リンクをクリックして、指定エントリのマルチキャストグループプロファイルアドレス設定を行います。

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。

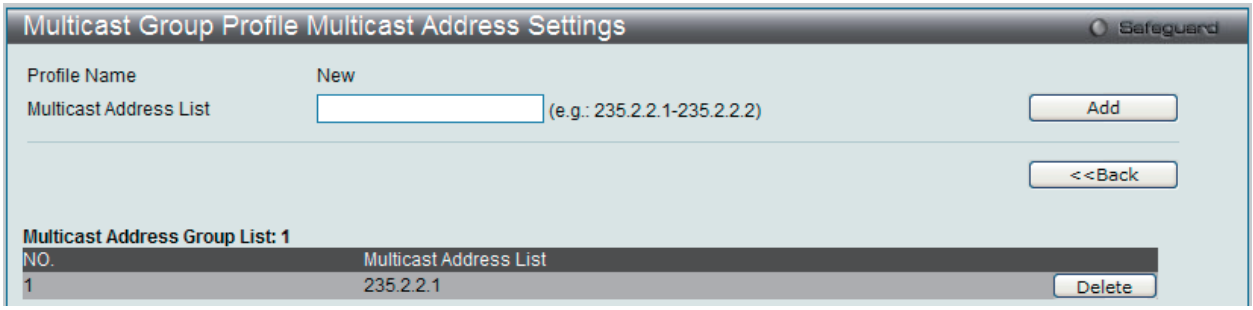


図 9-98　Multicast Group Profile Multicast Address Settings 画面

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 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。

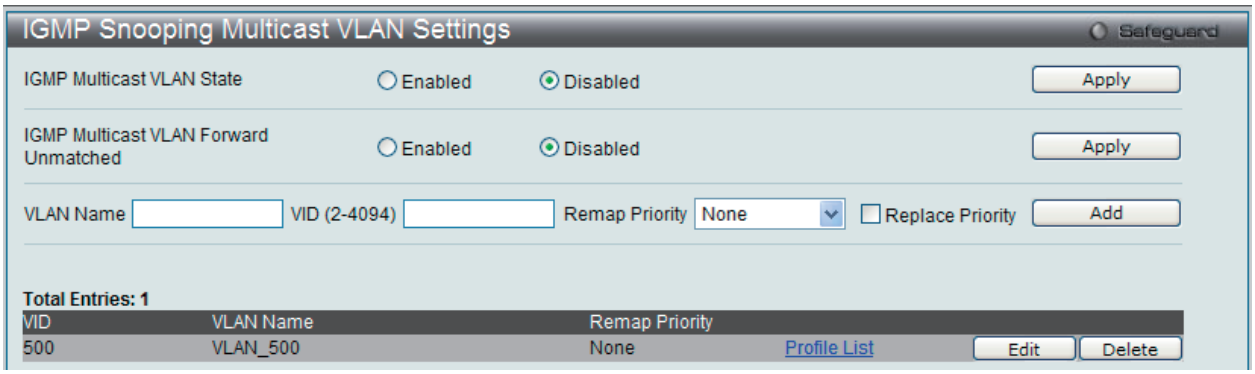


図 9-99　IGMP Snooping Multicast VLAN Settings 画面

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	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。
「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。
「Edit」ボタンをクリックして指定エントリの IGMP Snooping マルチキャスト VLAN 設定を行います。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Profile List」リンクをクリックして、指定エントリの IGMP Snooping マルチキャスト VLAN 設定を行います。

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。

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。

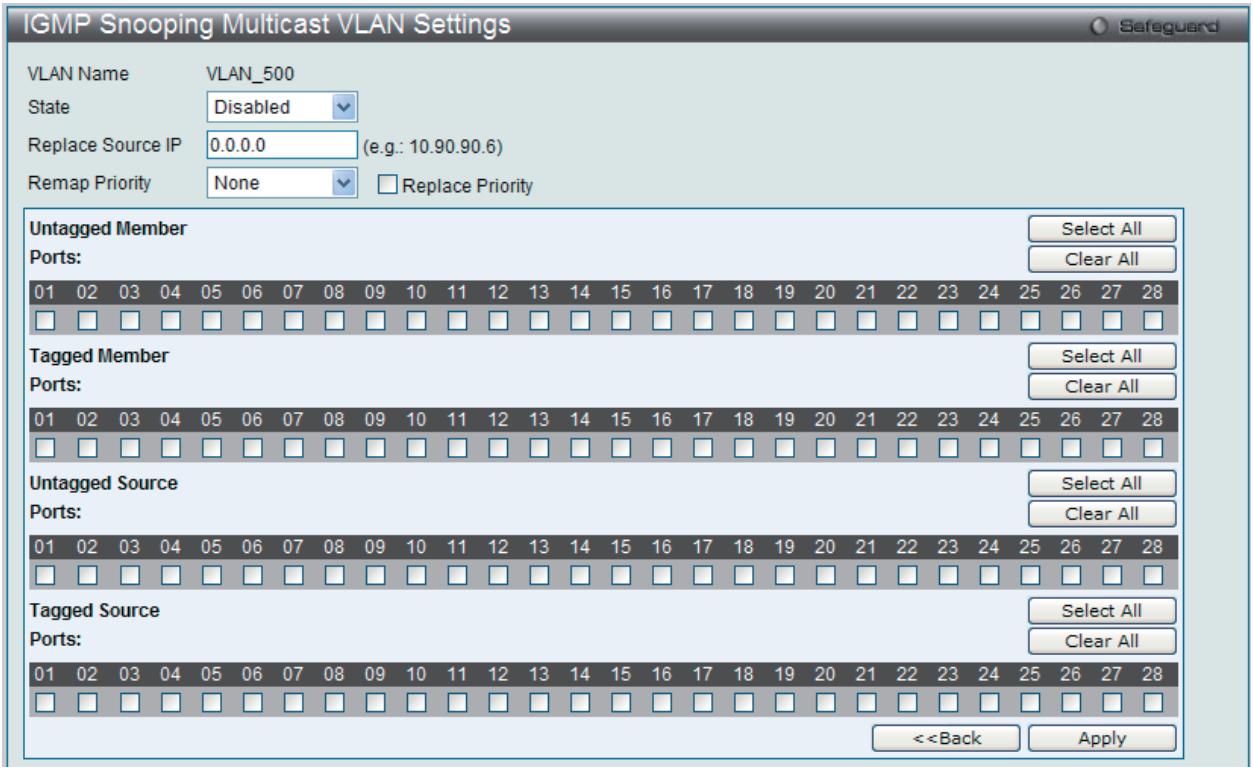


図 9-100 IGMP Snooping Multicast VLAN Settings 画面 - Edit

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。設定しない場合、送信元 IP アドレスは「0」に変換されます。
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 VLAN のタグなしメンバとしてソースポートまたはソースポートの範囲を指定します。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。

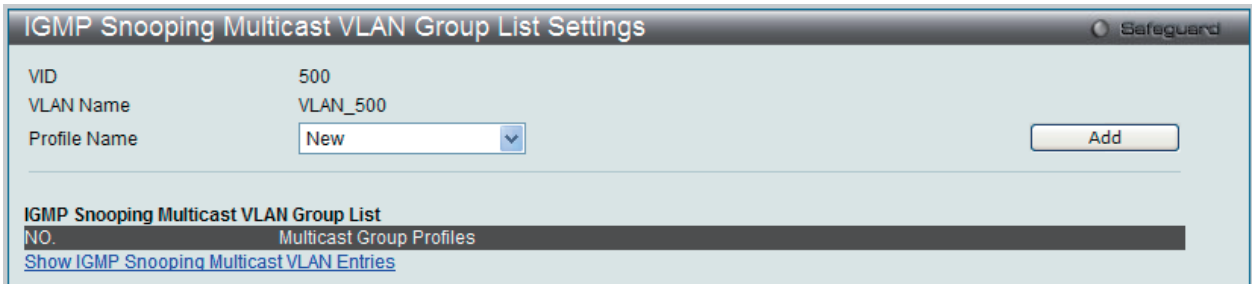


図 9-101 IGMP Snooping Multicast VLAN Group List Settings 画面

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. ISM 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。

MLD Multicast Group Profile Settings（MLD 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 > MLD 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。

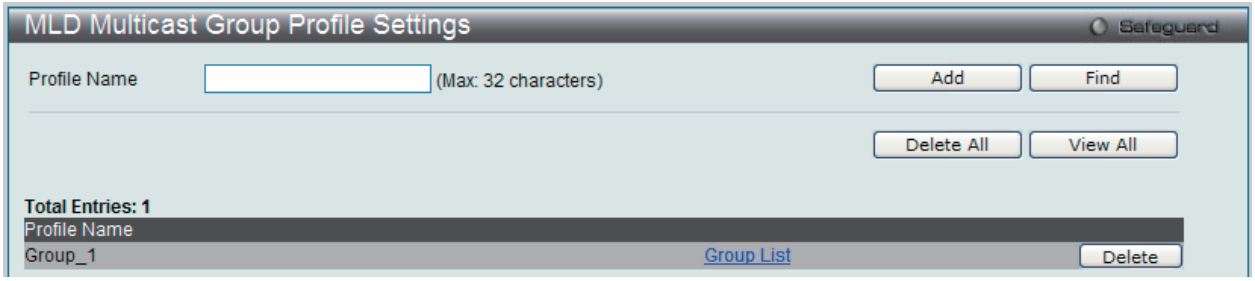


図 9-102 MLD Multicast Group Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile Name	MLD 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。

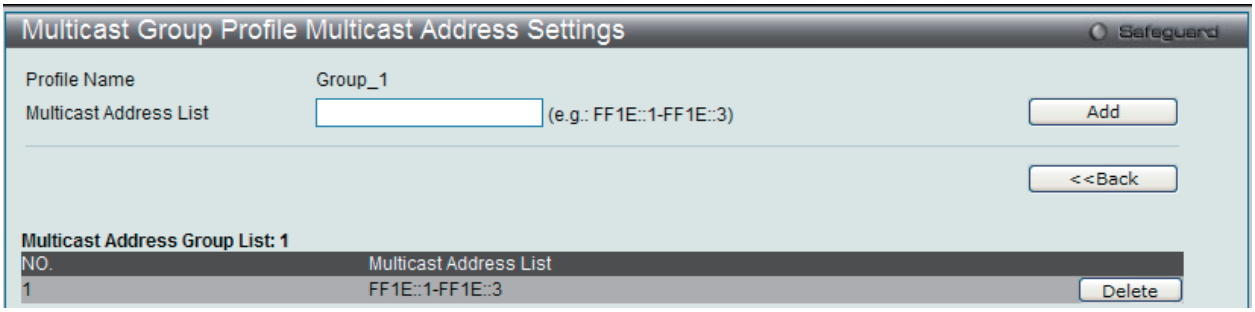


図 9-103 Multicast Group Profile Multicast Address Settings 画面 - Edit

2. 「Multicast Address List」でマルチキャストアドレス範囲を入力し、「Add」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。

MLD Snooping Multicast VLAN Settings（MLD Snooping マルチキャスト VLAN 設定）

MLD 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 > MLD Snooping Multicast 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。

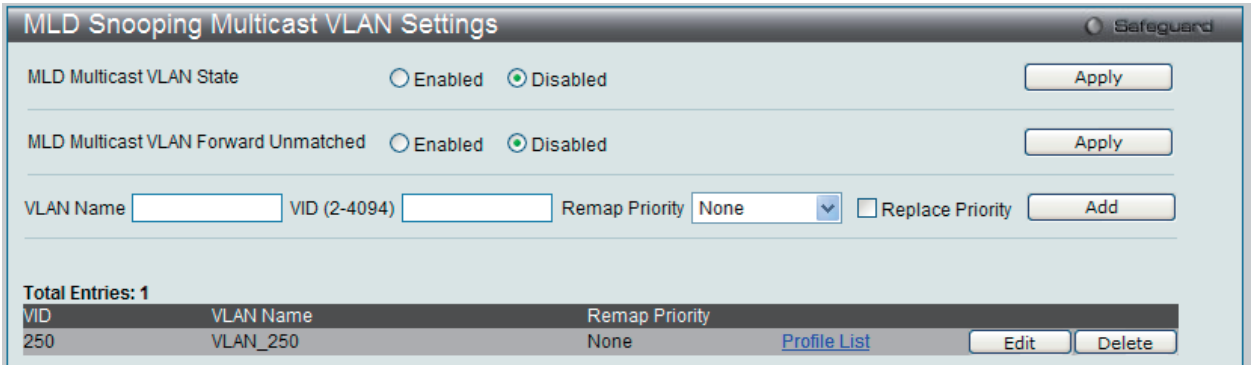


図 9-104 MLD Snooping Multicast VLAN Settings 画面

以下の項目を使用して設定します。

項目	説明
MLD Multicast VLAN State	MLD マルチキャスト VLAN 状態を有効または無効にします。
MLD Multicast VLAN Forward Unmatched	MLD 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	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。
「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。
「Edit」ボタンをクリックして指定エントリの MLD Snooping マルチキャスト VLAN 設定を行います。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Profile List」リンクをクリックして、指定エントリの MLD Snooping マルチキャスト VLAN 設定を行います。

マルチキャスト VLAN の登録

1. 「MLD 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。

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。

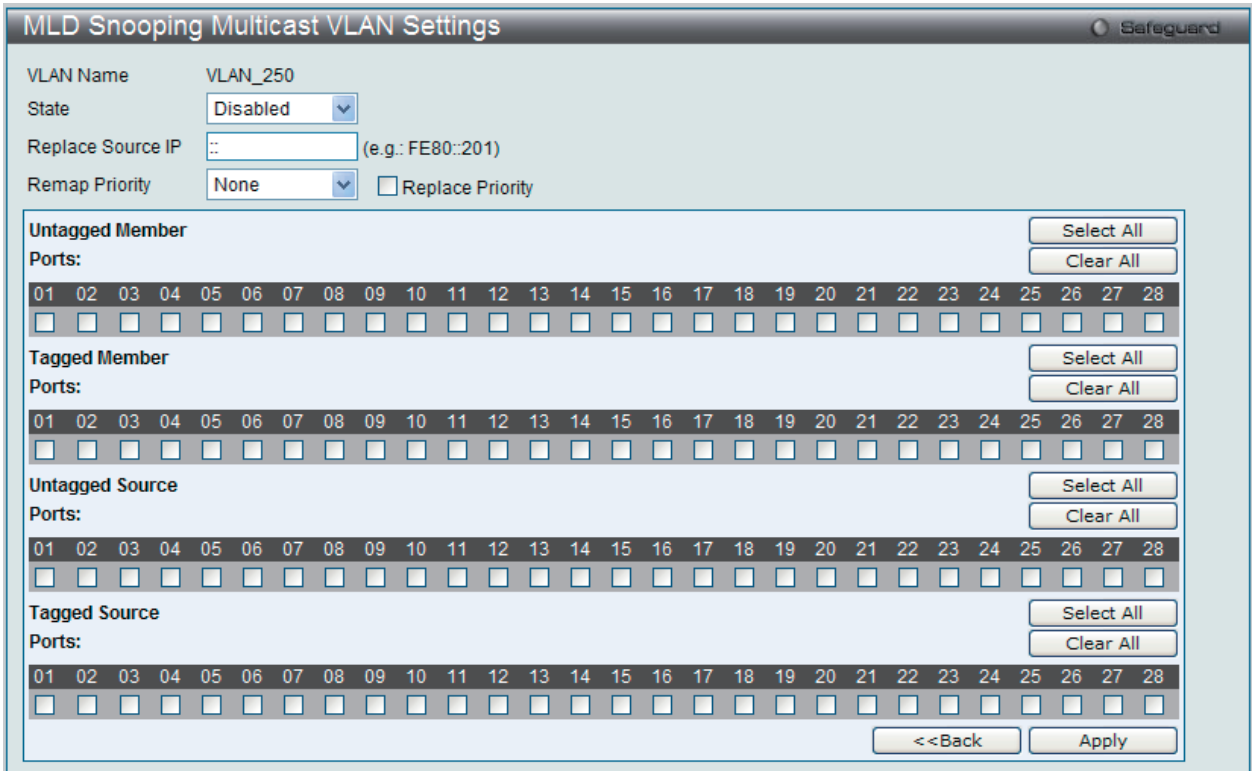


図 9-105　MLD Snooping Multicast VLAN Settings 画面 - Edit

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	MLD Snooping 機能を使用すると、ホストが送信した MLD 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。設定しない場合、送信元 IP アドレスは「::」に変換されます。
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 -「none」が指定されると、パケットの元の優先度が使用されます。（初期値）
Replace Priority	選択すると、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 VLAN のタグなしメンバとしてソースポートまたはソースポートの範囲を指定します。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。

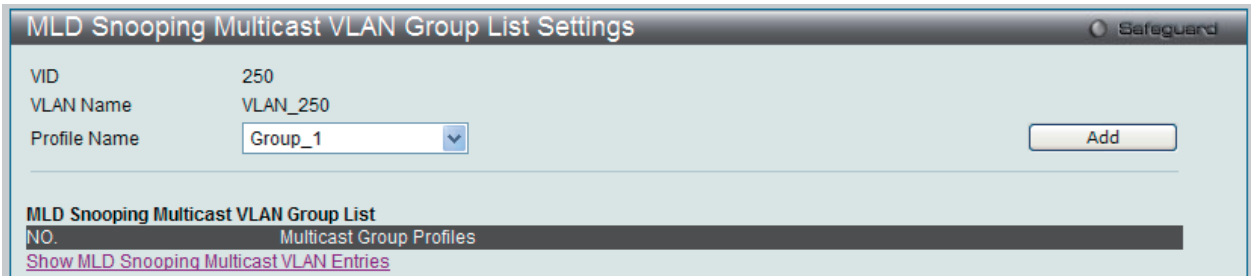


図 9-106　MLD Snooping Multicast VLAN Group List Settings 画面

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	MLD 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。

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. ISM 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。

「MLD Snooping VLAN Settings」画面に戻るためには、「Show MLD Snooping Multicast VLAN Entries」リンクをクリックします。

IP Multicast VLAN Replication（IP マルチキャスト VLAN レプリケーション）

IP Multicast VLAN Replication Global Settings（IP マルチキャスト VLAN レプリケーションのグローバル設定）

IP マルチキャスト VLAN のレプリケーションパラメータを設定します。

L2 Features > L2 Multicast Control > IP Multicast VLAN Replication > IP Multicast VLAN Replication 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。

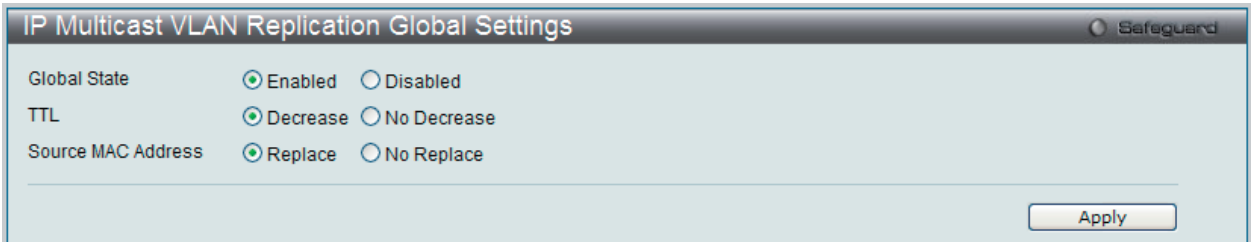


図 9-107　IP Multicast VLAN Replication Global Settings 画面

以下の項目を使用して設定します。

項目	説明
Global State	グローバル状態を有効または無効にします。
TTL	パケット内の TTL（Time to live）値に対して「Decrease」（減らす）または「No decrease」（減らさない）を選択します。
Source MAC Address	パケットの送信元 MAC アドレスの交換の有無を選択します。

「Apply」ボタンをクリックして行った変更を適用します。

IP Multicast VLAN Replication Settings（IP マルチキャスト VLAN レプリケーション設定）

IP マルチキャスト VLAN のレプリケーションテーブルの追加または参照を行います。

L2 Features> L2 Multicast Control > IP Multicast VLAN Replication > IP Multicast VLAN Replication 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。

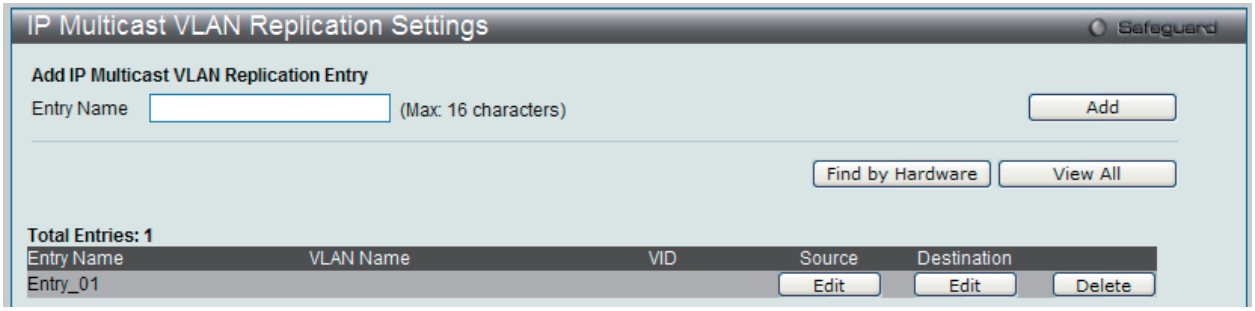


図 9-108 IP Multicast VLAN Replication Settings 画面

以下の項目を使用して設定します。

項目	説明
Entry Name	マルチキャストレプリケーションエントリ名を入力します。

「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。

「Find by Hardware」をクリックしてハードウェアに基づいてエントリを検索します。
「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。
「Source」の下にある「Edit」ボタンをクリックして、指定エントリを編集します。
「Destination」の下にある「Edit」ボタンをクリックして、指定エントリを編集します。
「Delete」ボタンをクリックして、指定エントリを削除します。

送信元エントリの変更

「Source」の下にある「Edit」ボタンをクリックして、以下の画面を表示します。

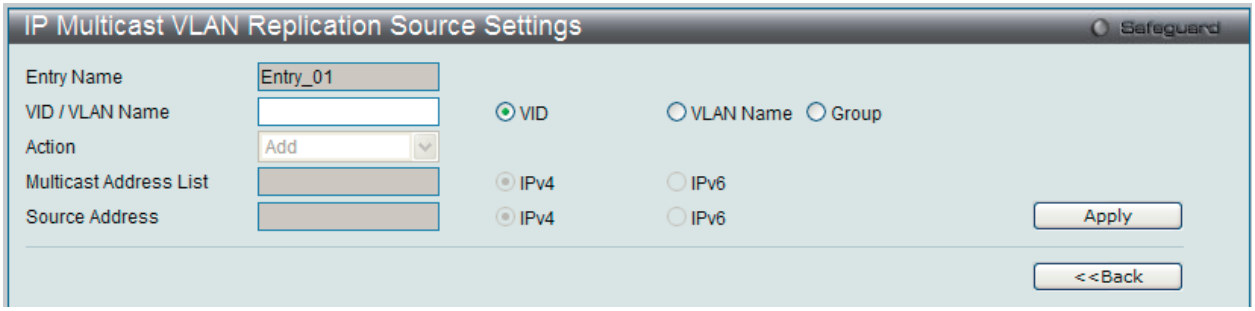


図 9-109 IP Multicast VLAN Replication Source Settings 画面

以下の項目を使用して設定します。

項目	説明
Entry Name	IP マルチキャスト VLAN レプリケーションソースエントリ名が表示されます。
VID / VLAN Name	「VLAN Name」、「VID」または「Group」を選択して、値を入力します。
Action	適用する操作を選択します。
Multicast Address List	マルチキャストアドレスリストを入力します。
Source Address	送信元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。

「<<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。

送信先エントリの変更

「Destination」の下にある「Edit」ボタンをクリックして、以下の画面を表示します。

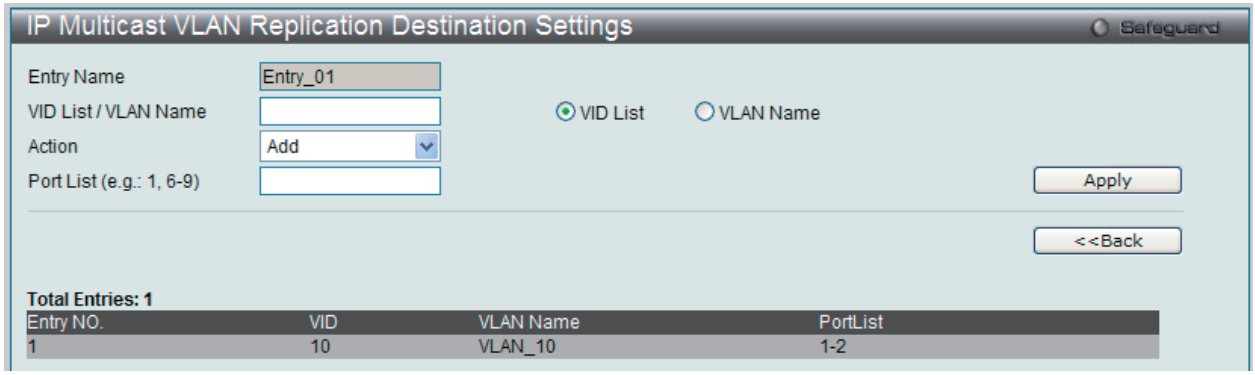


図 9-110　IP Multicast VLAN Replication Destination Settings 画面

以下の項目を使用して設定します。

項目	説明
Entry Name	IP マルチキャスト VLAN レプリケーション宛先エントリ名が表示されます。
VID / VLAN Name	「VLAN Name」、「VID」または「Group」を選択して、値を入力します。
Action	適用する操作を選択します。
Port List	ポートリストを指定します。

「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。

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 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。

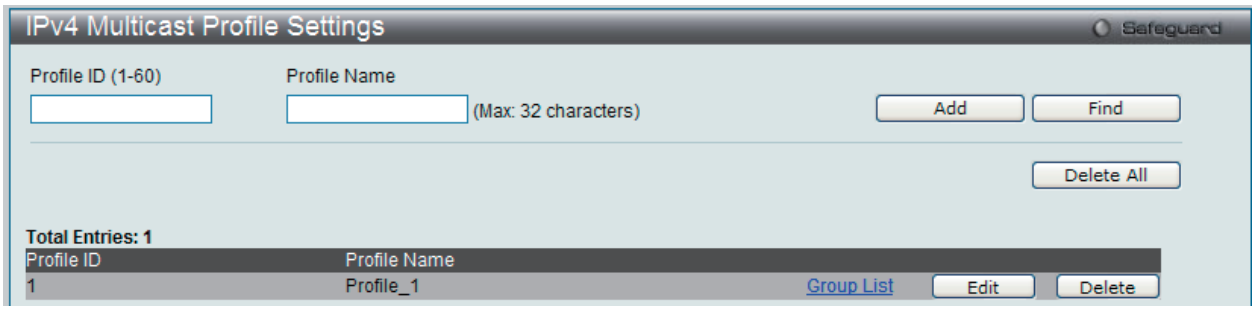


図 9-111　IPv4 Multicast Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile ID	1-60 のプロファイル 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。

「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。
「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、以下の画面を表示します。

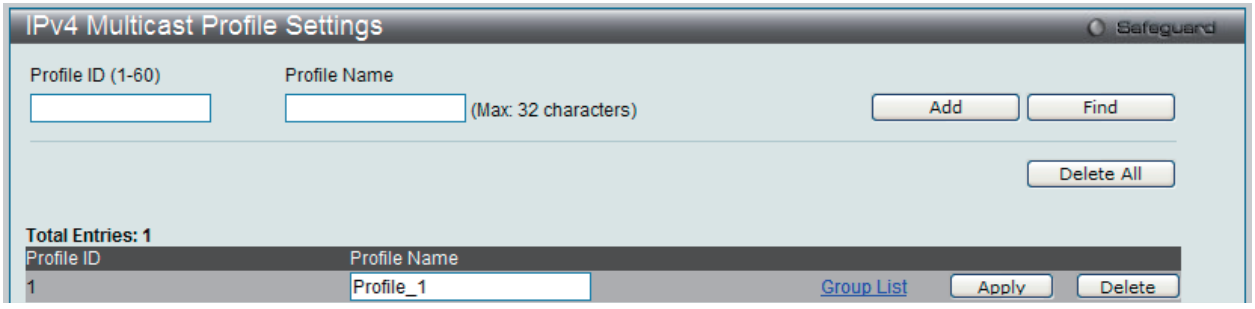


図 9-112　IPv4 Multicast Profile Settings 画面 - Edit

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」リンクをクリックすると、以下の画面が表示されます。

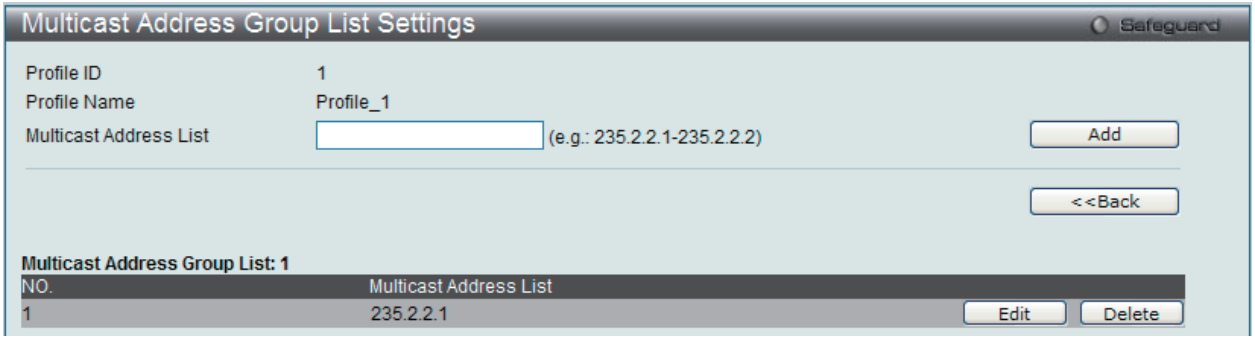


図 9-113　Multicast Address Group List Settings 画面

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。

「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、以下の画面を表示します。

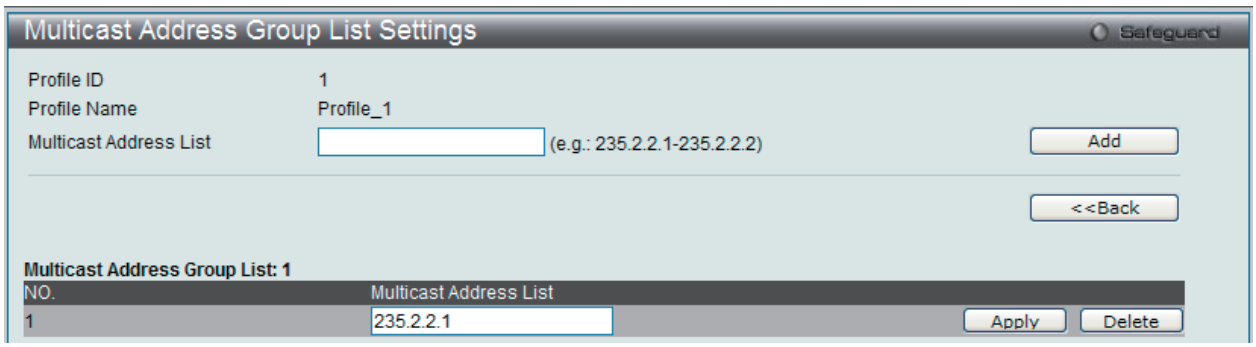


図 9-114 IPv4 Multicast Profile Settings 画面 - Edit

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。

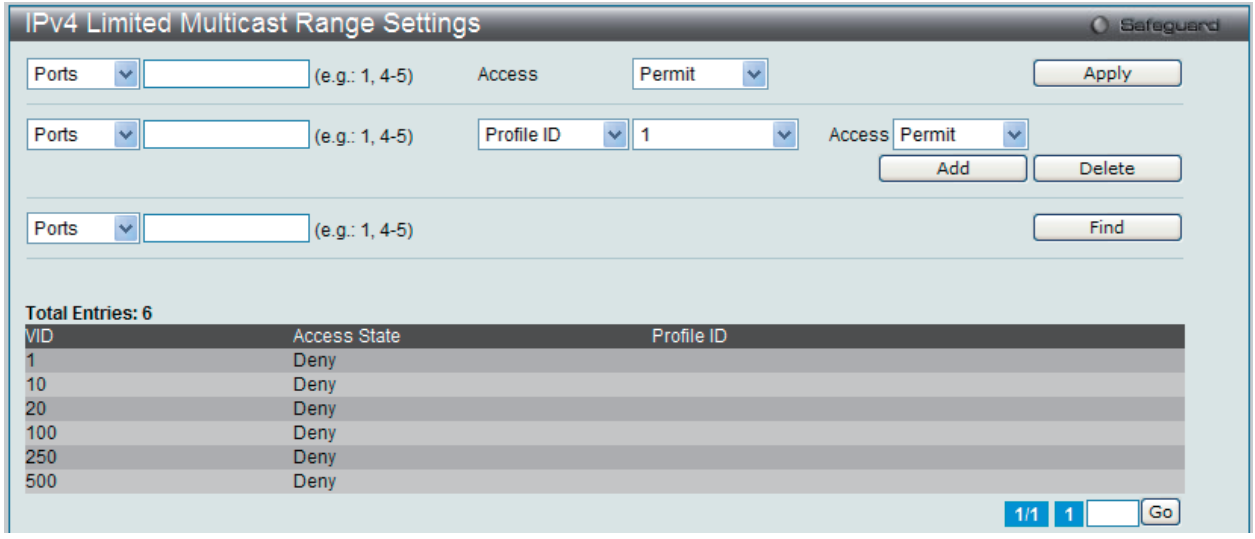


図 9-115 IPv4 Limited Multicast Range Settings 画面

「Limited IP Multicast Range」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	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することを指定します。 • 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することを指定します。

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）

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 > 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。

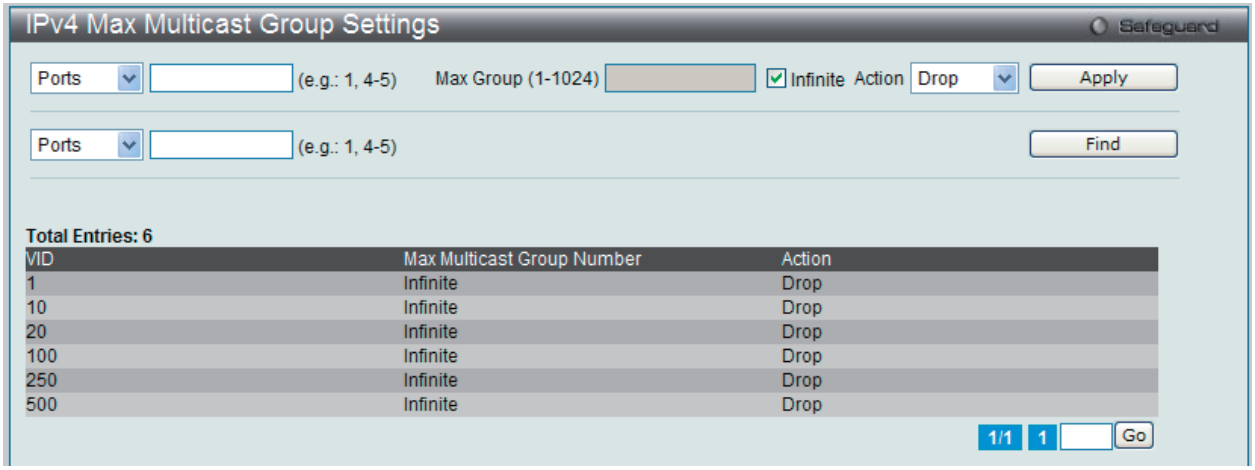


図 9-116　IPv4 Max Multicast Group Settings 画面

以下の項目を使用して、設定します。

項目	説明
Ports	本設定に使用される適切なポートまたはポート範囲を選択します。
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。

エントリを追加するためには、適切な情報を入力し「Apply」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。

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。

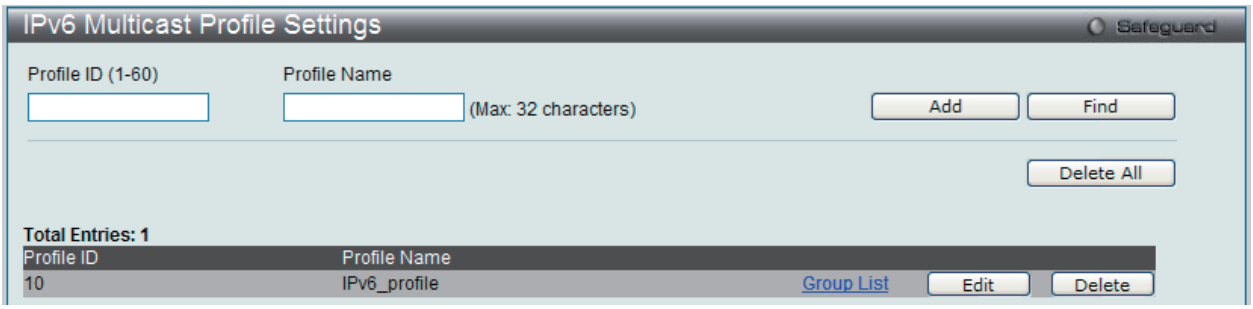


図 9-117 IPv6 Multicast Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile ID	1-60 のプロファイル 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。

「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。
「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、以下の画面を表示します。

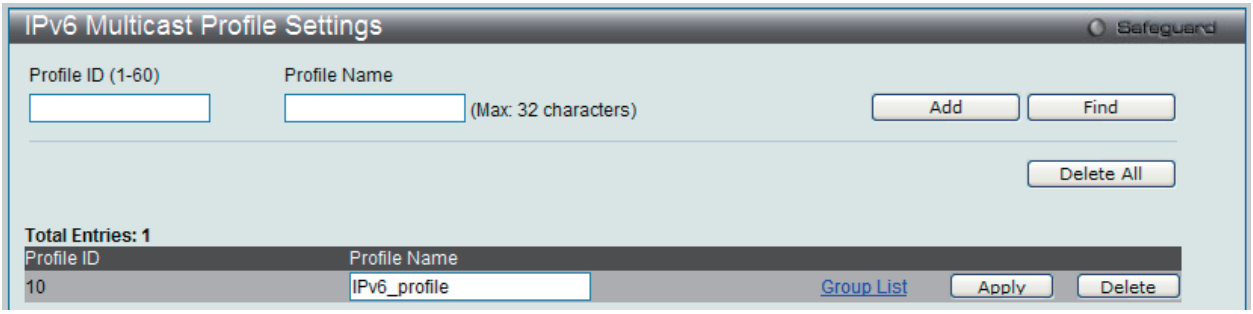


図 9-118 IPv6 Multicast Profile Settings 画面 - Edit

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。

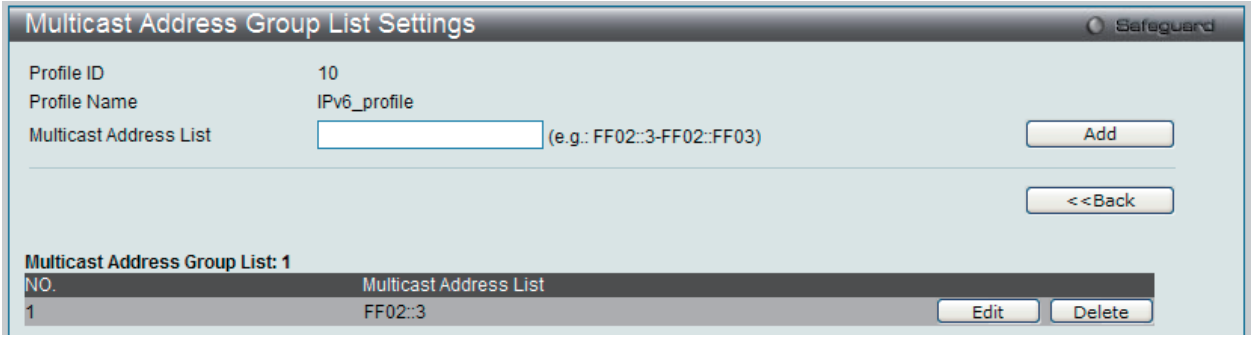


図 9-119 Multicast Address Group List Settings 画面

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。

「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、以下の画面を表示します。

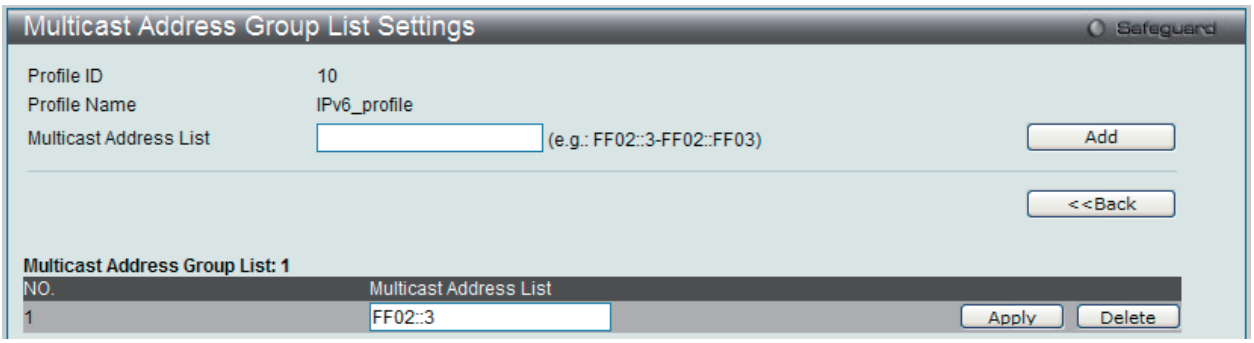


図 9-120 Multicast Address Group List Settings 画面 - Edit

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。

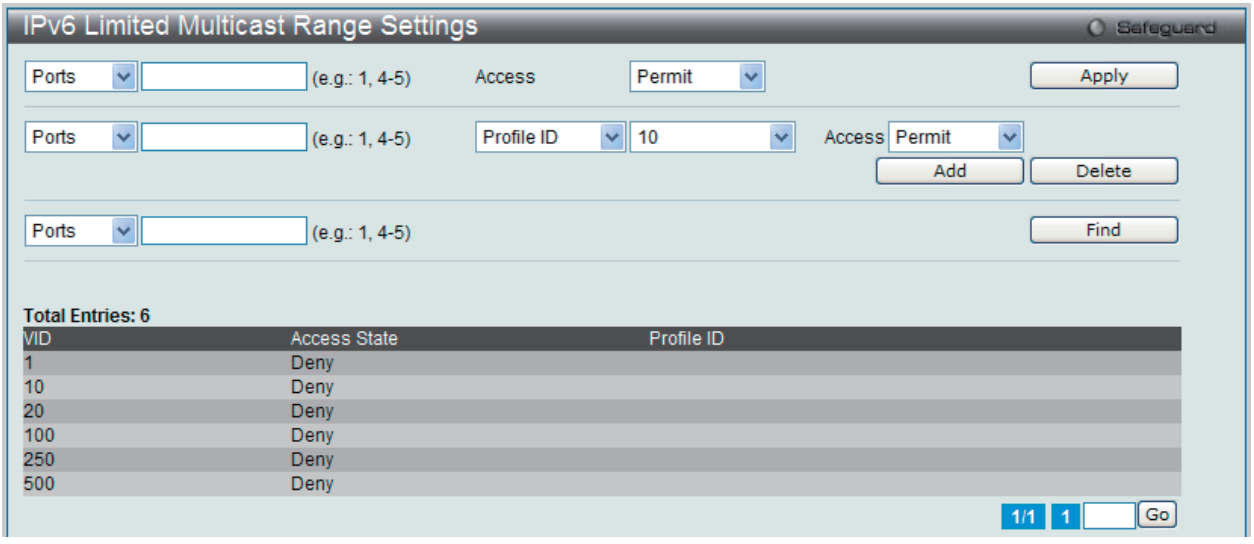


図 9-121 IPv6 Limited Multicast Range Settings 画面

「Limited IP Multicast Range」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	プルダウンメニューを使用して、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することを指定します。 • 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することを指定します。

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。

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。

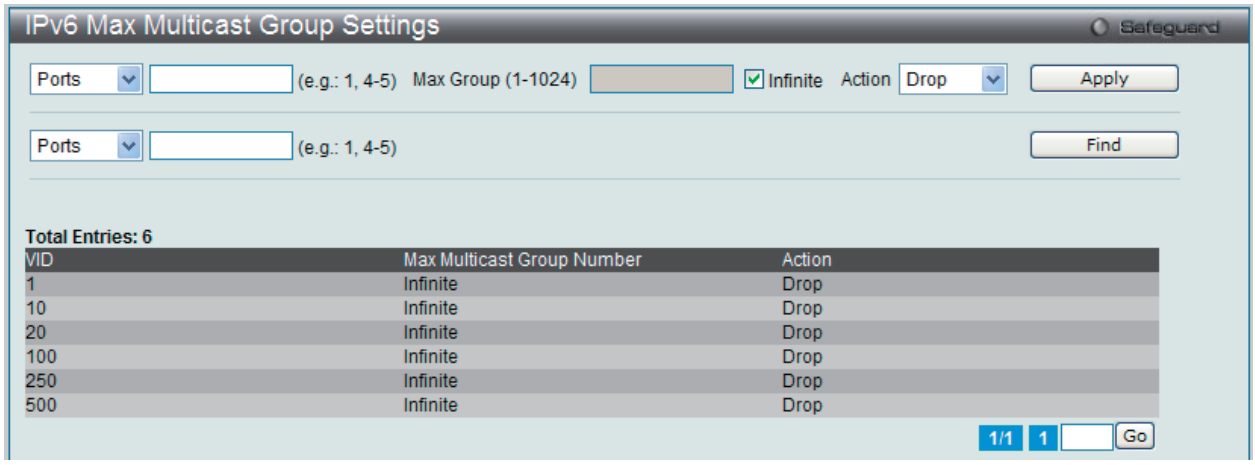


図 9-122　IPv6 Max Multicast Group Settings 画面

以下の項目を使用して設定します。

項目	説明
Ports	本設定に使用される適切なポートまたはポート範囲を選択します。
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。

エントリを追加するためには、適切な情報を入力し「Apply」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。

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。

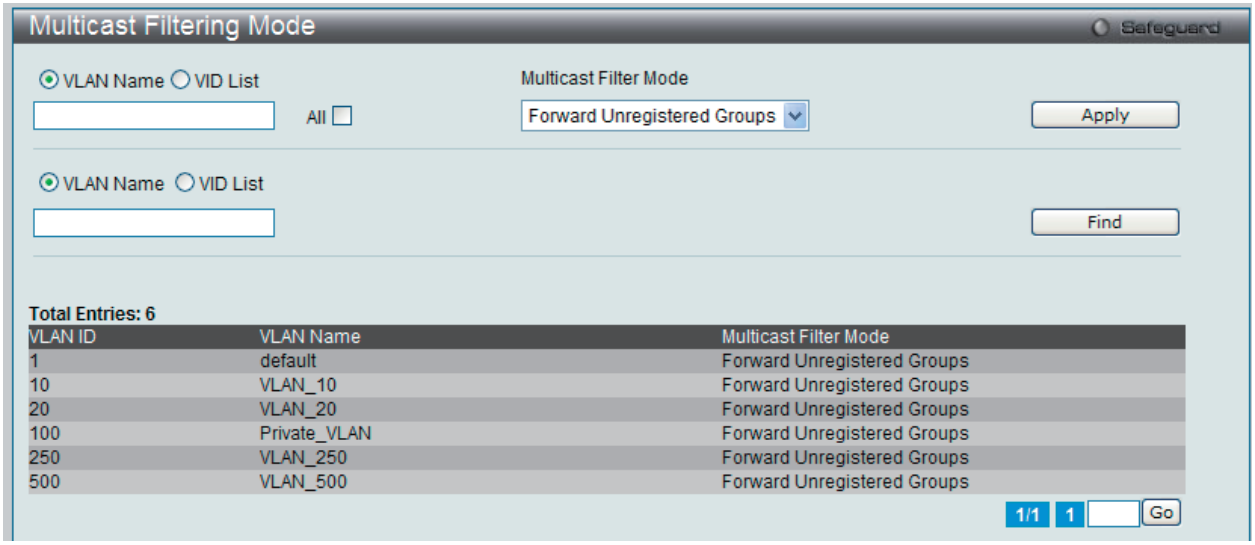


図 9-123　Multicast Filtering Mode 画面

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。「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 Filtering 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 Unregistered Groups - 指定ポート範囲に存在する登録されていないマルチキャストグループが受信先のマルチキャストパケットを転送します。 • Filter Unregistered Groups - 指定ポート範囲に存在する登録されていないマルチキャストグループが受信先のマルチキャストパケットを廃棄します。

「Apply」ボタンをクリックして行った変更を適用します。
「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の調整のために使用される 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ないことにご注意ください。

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。

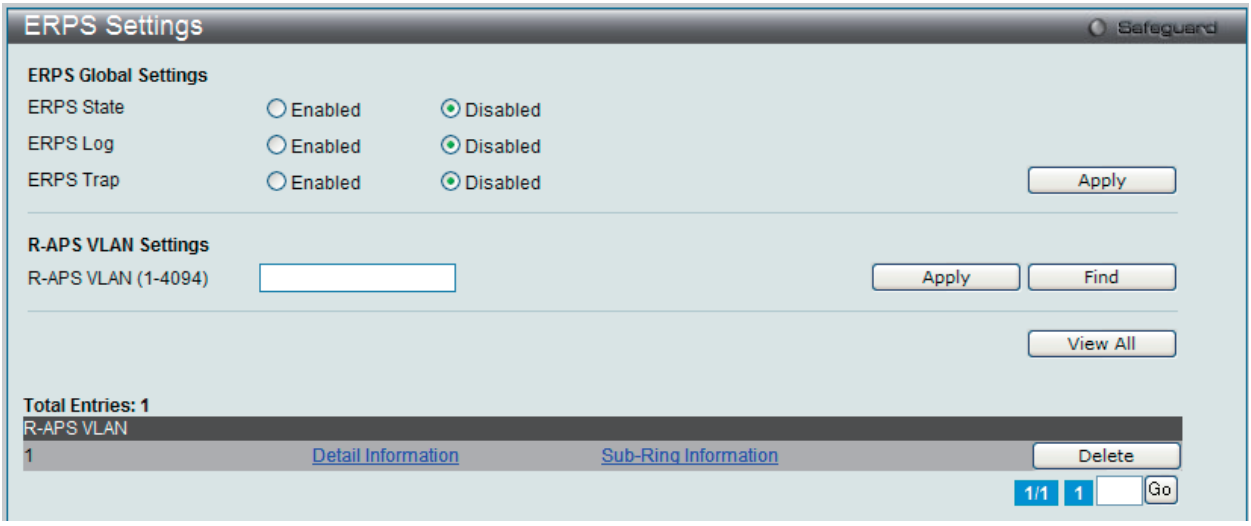


図 9-124 ERPS Settings 画面

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。

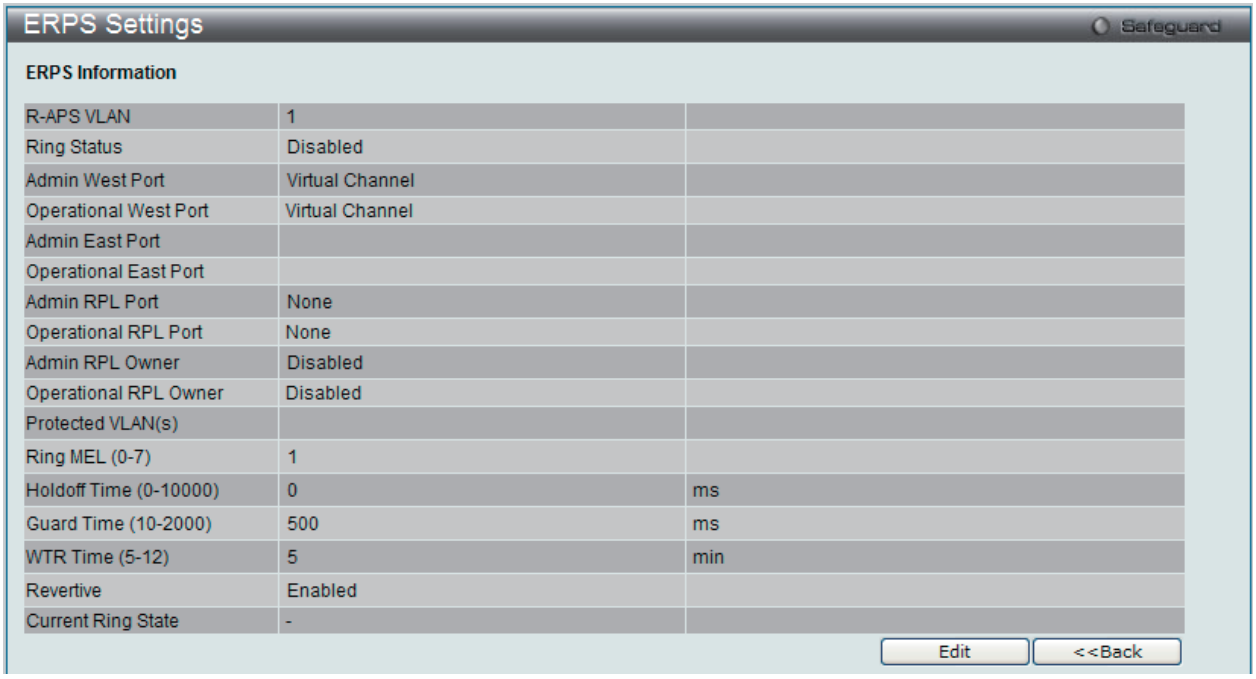


図 9-125 ERPS Settings 画面 - ERPS Information

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。

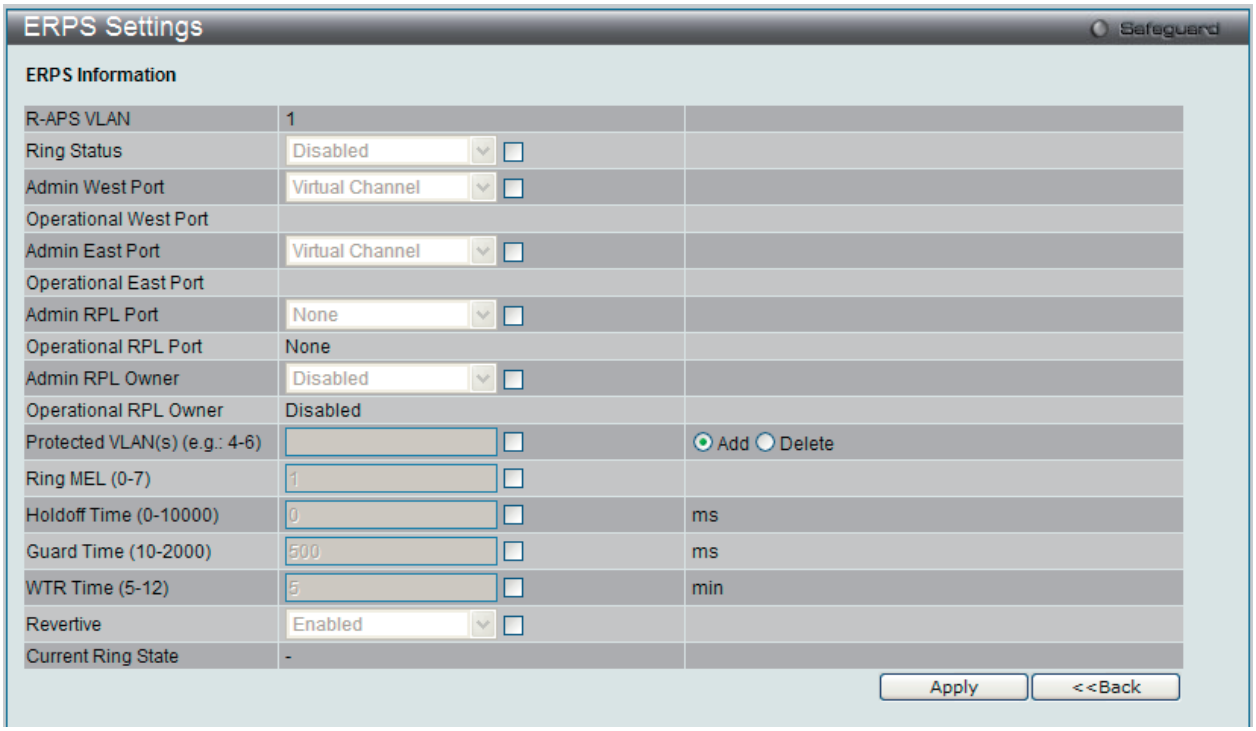


図 9-126 ERPS Settings 画面 - Edit

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。

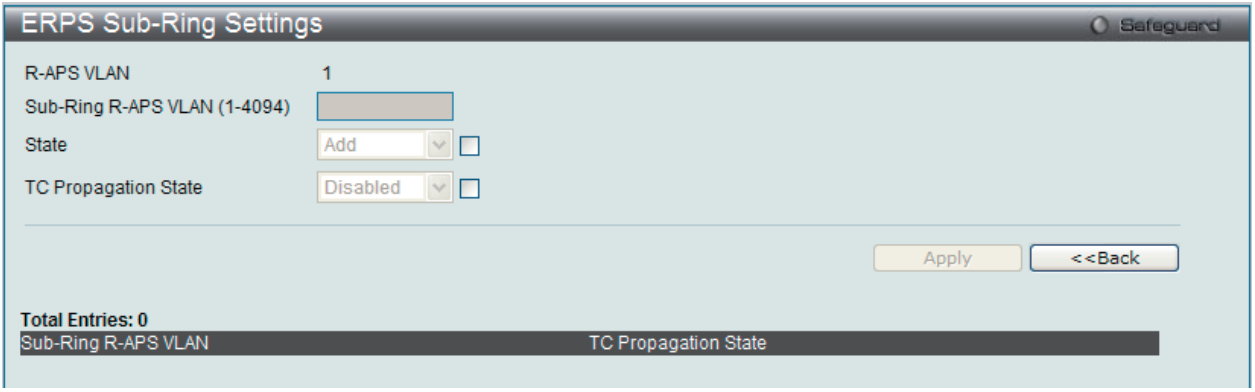


図 9-127 ERPS Sub-Ring Settings 画面

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	チェックを行い、プルダウンメニューを使用して、ERPS のサブリングステートを追加または削除にします。
TC Propagation State	チェックを行い、プルダウンメニューを使用して、TC 伝搬の状態を「Enabled」(有効)/「Disabled」(無効) にします。

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。

Local Loopback Port Settings（ローカルループバックポート設定）

ローカルループバックポートのパラメータを設定します。

L2 Features > Local Loopback 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。

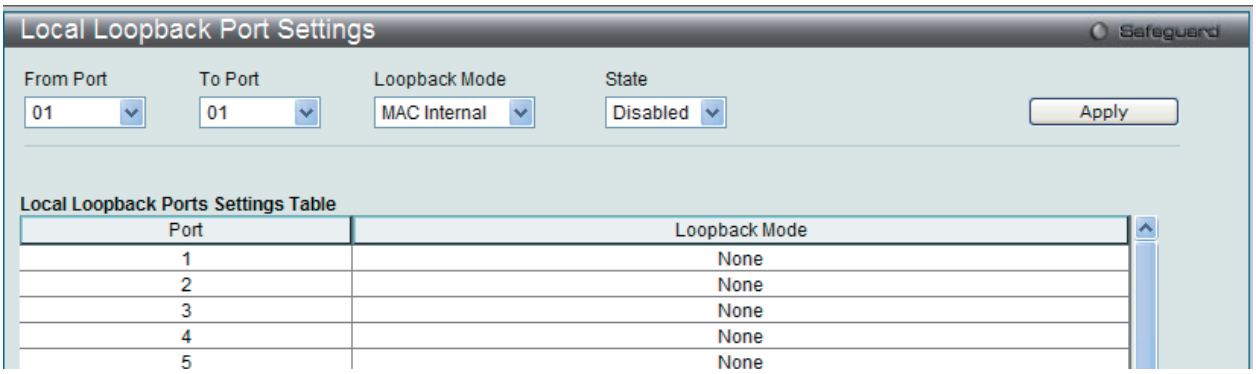


図 9-128　Local Loopback Port Settings 画面

以下の項目を使用して設定します。

項目	説明
From Port / To Port	この設定に使用するポート番号を選択します。
Loopback Mode	使用するループバックモードを選択します。MAC Internal、MAC External、PHY Internal および PHY External からモードを選択します。物理 (PHY) モードの使用を選択すると、「Medium Type」を設定できます。
State	状態を有効または無効にします。
Medium Type	メディアタイプを「Copper」または「Fiber」に設定します。

「Apply」ボタンをクリックして行った変更を適用します。

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 ネットワークへの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）に格納されるので、SNMP（Simple Network Management Protocol）などの管理プロトコル使っ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。

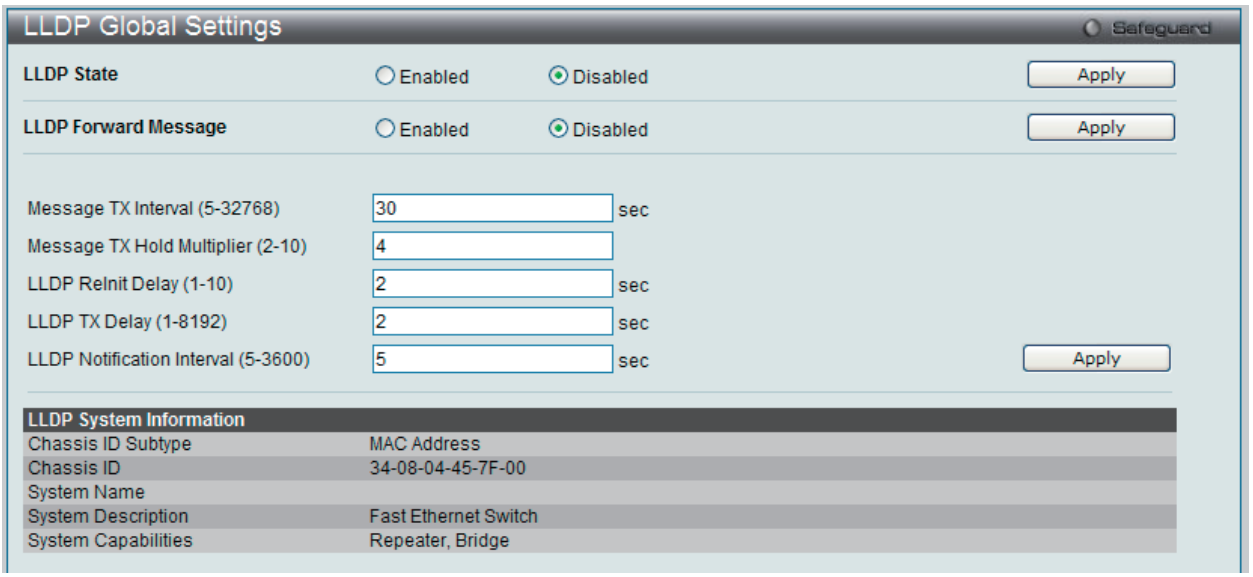


図 9-129 LLDP Global Settings 画面

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 の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に定義済みの 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。

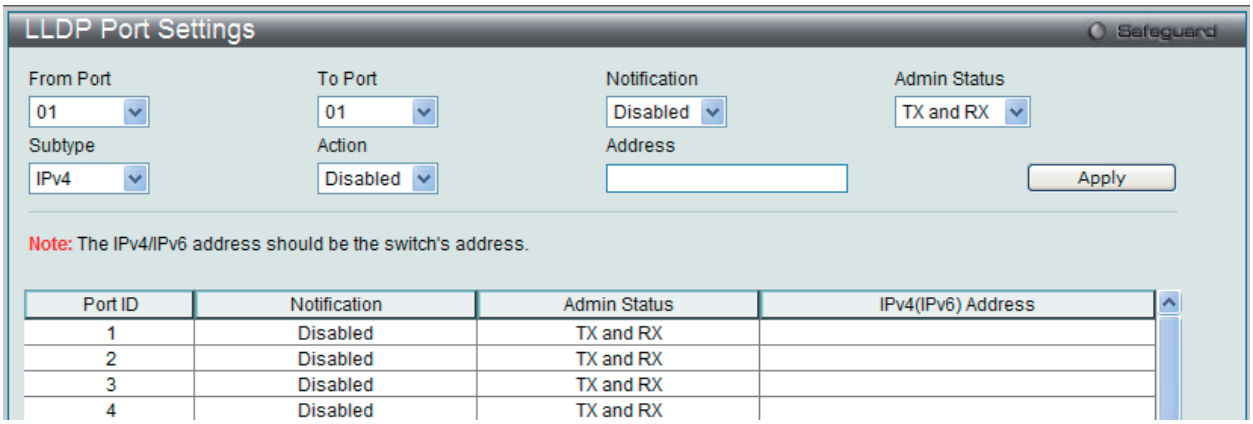


図 9-130　LLDP Port Settings 画面

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設定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。本アドレスは管理 IP アドレスである必要があります。

「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 アドレスが、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。

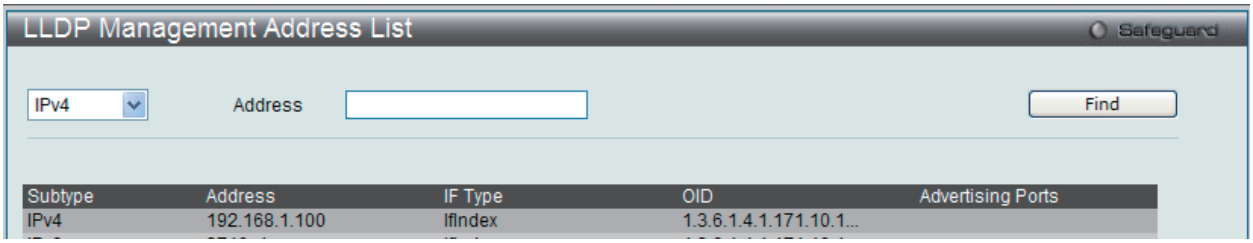


図 9-131　LLDP Management Address List 画面

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、「mgt_addr config」が有効である場合に 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。

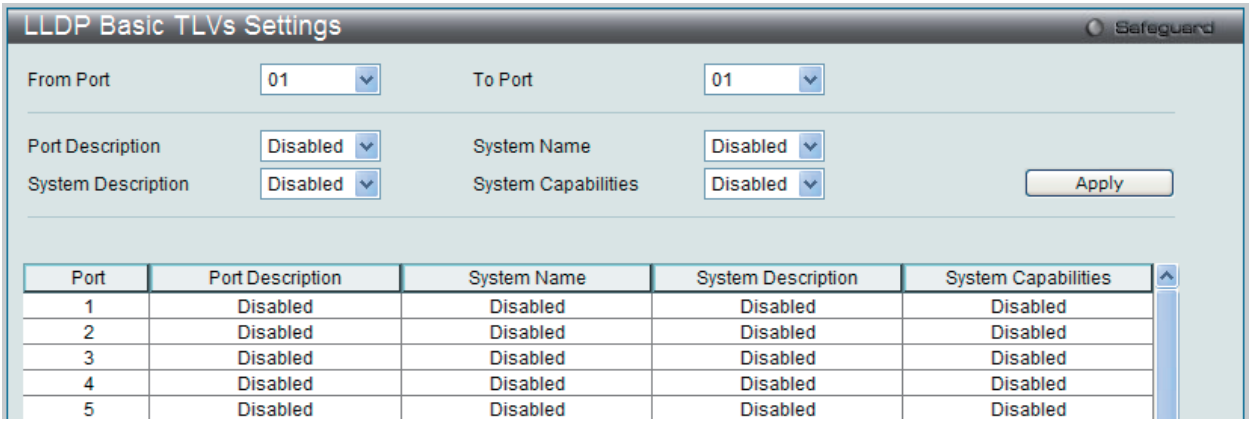


図 9-132　LLDP Basic TLVs Settings 画面

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。

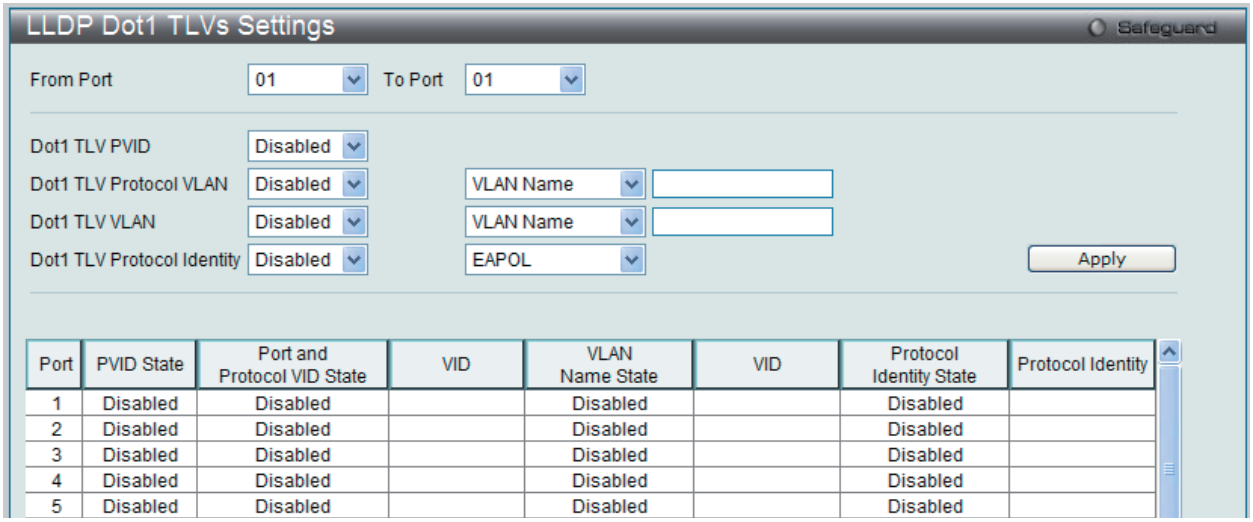


図 9-133　LLDP Dot1 TLVs Settings 画面

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。

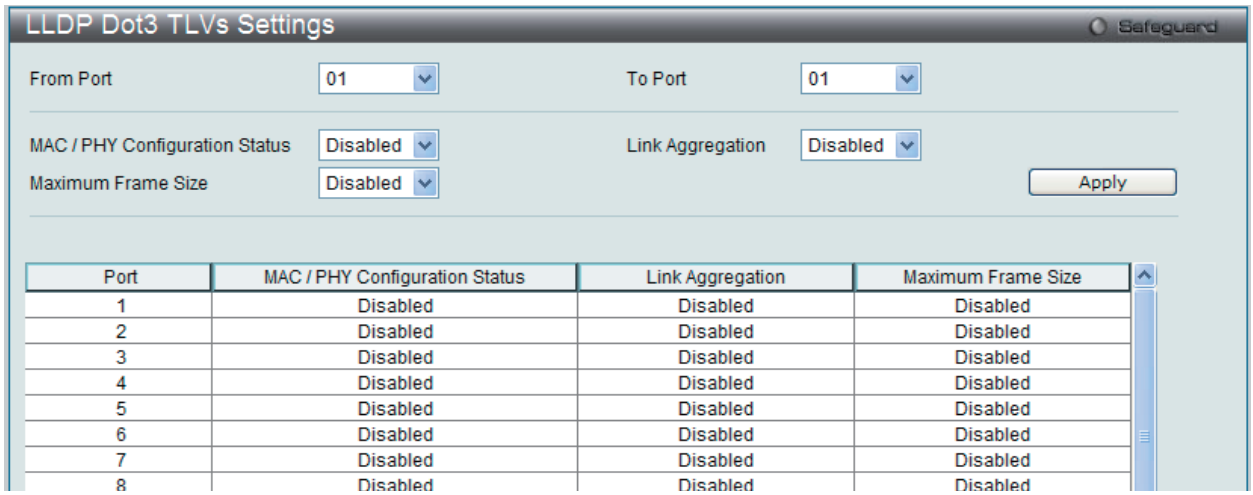


図 9-134　LLDP Dot3 TLVs Settings 画面

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。

「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。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。

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。

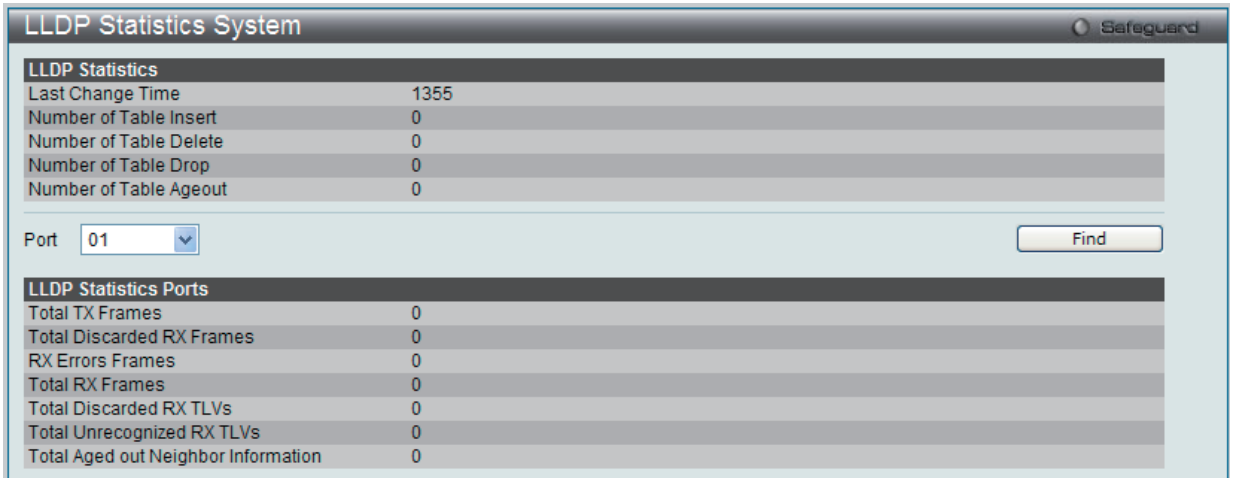


図 9-135　LLDP Statistics System 画面

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 :

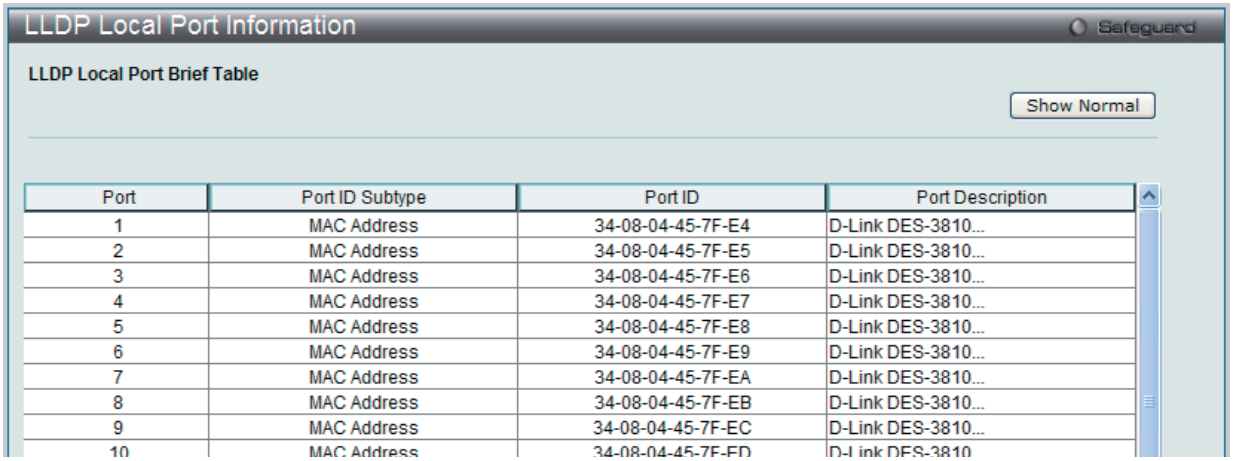


図 9-136　LLDP Local Port Information 画面 - Brief

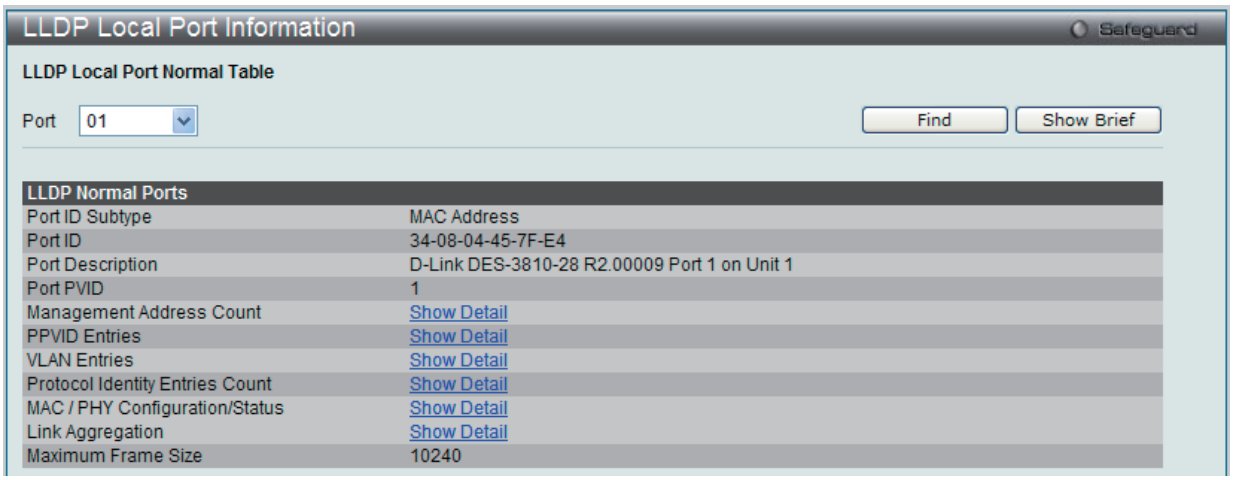


図 9-137　LLDP Local Port Information 画面 - Normal

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、「Show Detail」リンクをクリックします。

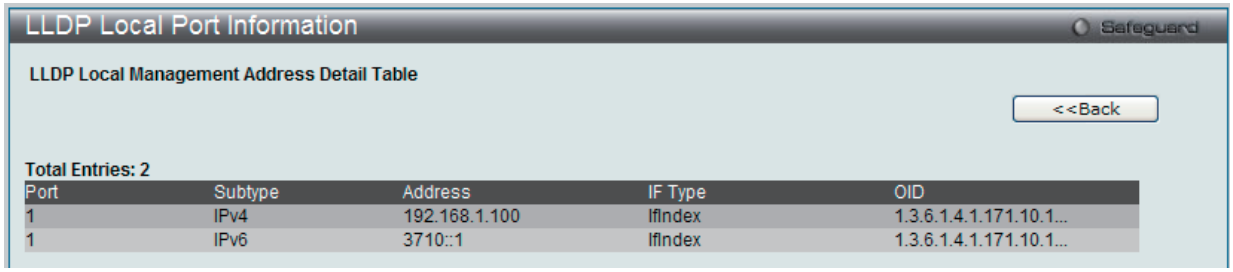


図 9-138　LLDP Local Port Information 画面 - Detail

「<<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。

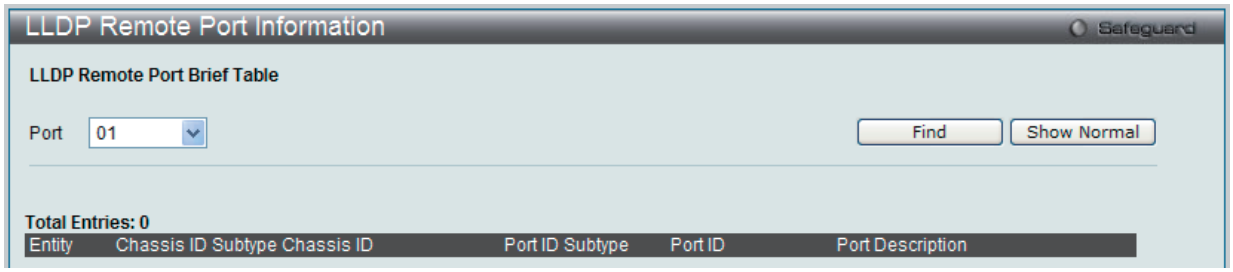


図 9-139　LLDP Remote Port Information 画面 - Brief

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。

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。

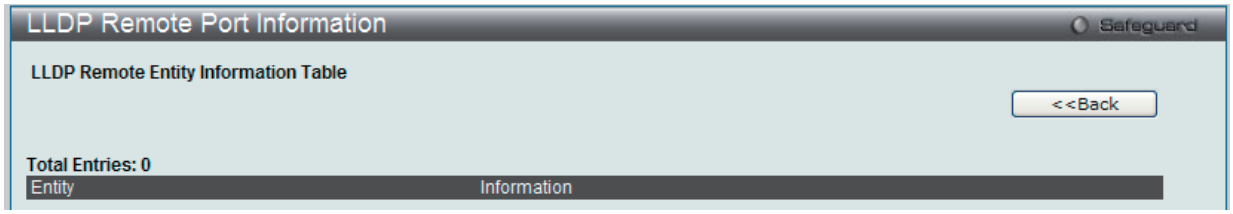


図 9-140　LLDP Remote Port Information 画面 - Normal

「<<Back」をボタンをクリックして前のページに戻ります。

LLDP-MED（LLDP-MED 設定）

LLDP-MED（Media-Endpoint-Discovery）は、専門的なケーパビリティと LLDP-MED 規格に準拠した機能を持つネットワークエッジに高度な機能をサポートするために LLDP 業界標準を拡張したものです。

LLDP-MED System Settings（LLDP-MED システム設定）

「Fast Start Repeat Count」（ファストスタート実行回数）を設定します。

L2 Features > LLDP > LLDP-MED > LLDP-MED 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。

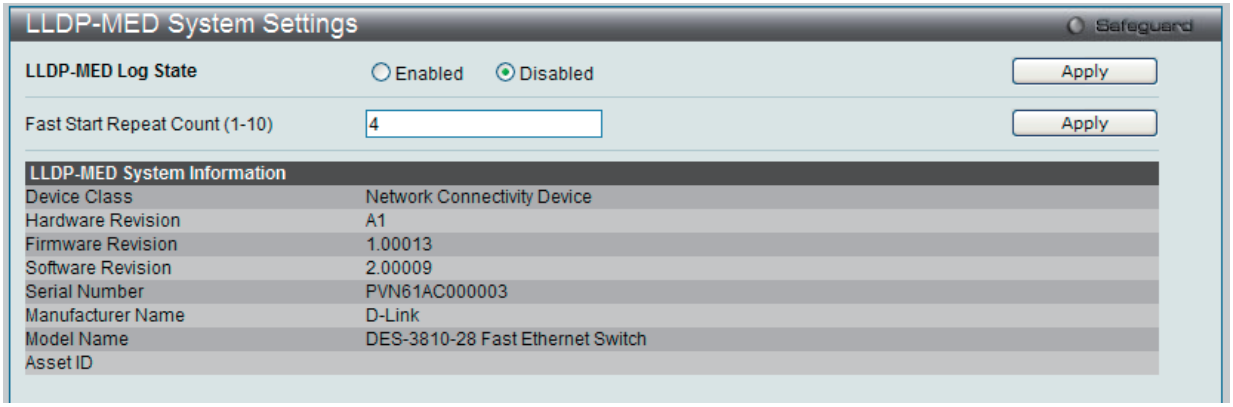


図 9-141　LLDP-MED System Settings 画面

以下の項目が使用できます。

項目	説明
LLDP-MED Log State	LLDP-MED ログ状態を有効または無効にします。
Fast Start Repeat Count	リピートカウントの範囲は 1-10 です。初期値は 4 です。
LLDP-MED System Information	LLDP-MED システムに関する情報のリストを表示します。

「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。

LLDP-MED Port Settings（LLDP-MED ポート設定）

LLDP-MED TLV の送信を有効または無効にします。

「Capability」をサポートなしに設定すると機能は動作せず、管理アプリケーションには矛盾した値のエラーが戻されるという結果になります。事実上、TLV の送信のケーパビリティを無効にすることによってポート単位に LLDP-MED を無効にします。この場合、各ポートに対応する LLDP-MED MIB におけるリモートテーブルのオブジェクトは入力されません。

L2 Features > LLDP > LLDP-MED > LLDP-MED 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。

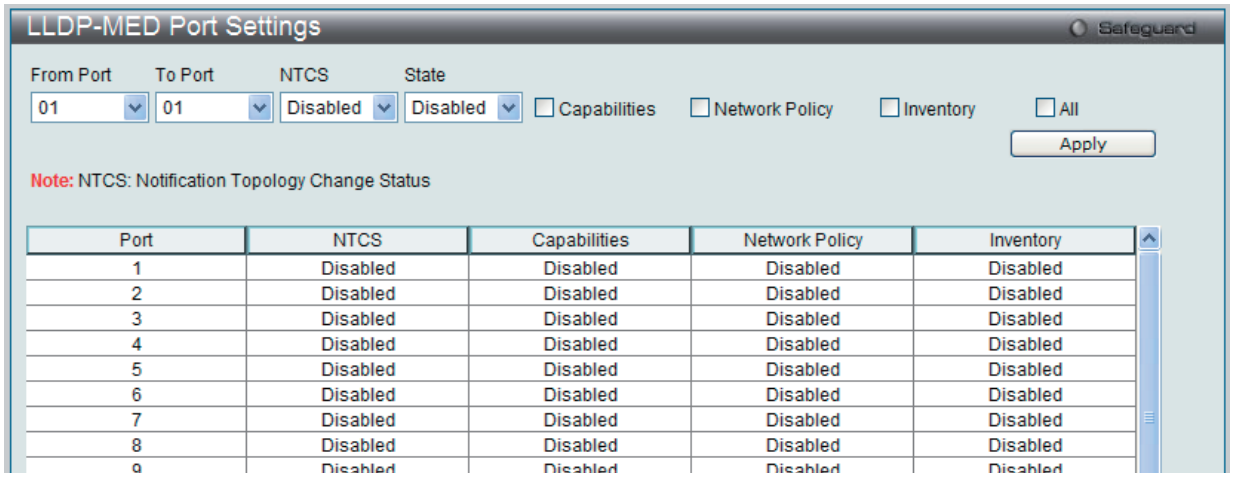


図 9-142　LLDP-MED Port Settings 画面

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。
NTCS	NTCS（トポロジ変更状態の通知）を有効または無効にします。
State	TLV を有効または無効にします。
Capabilities	この TLV タイプは、LLDP エージェントが「LLDP-MED capabilities TLV」を送信する必要があることを示します。LLDP-MED PDU を送信する場合、この TLV タイプを有効にする必要があります。そうでないと、このポートは LLDP-MED PDU を送信することができません。
Network Policy	この TLV タイプは、LLDP エージェントが「LDP-MED network policy TLV」を送信する必要があることを示します。
Inventory	この TLV タイプは、LLDP エージェントが「LLDP-MED inventory TLV」を送信する必要があることを示します。
All	このオプションを選択すると、設定に「Capabilities」、「Network Policy」および「Inventory」を含めます。

「Apply」ボタンをクリックして行った変更を適用します。

LLDP-MED Local Port Information（LLDP-MED ローカルポート情報）

ポート単位で LLDP-MED ローカルポート情報を表示します。

L2 Features > LLDP > LLDP-MED > LLDP-MED 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。

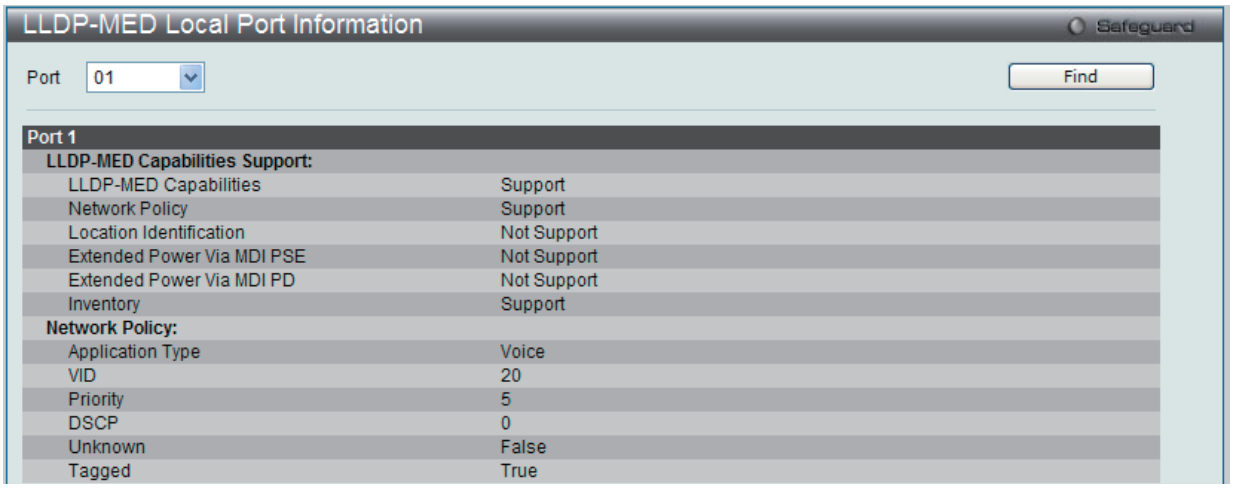


図 9-143　LLDP-MED Local Port Information 画面

「Port」を選択し、「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-MED Remote Port Information（LLDP-MED ローカルポート情報）

LLDP-MED リモートポート情報を表示します。

L2 Features > LLDP > LLDP-MED > LLDP-MED Remote 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。

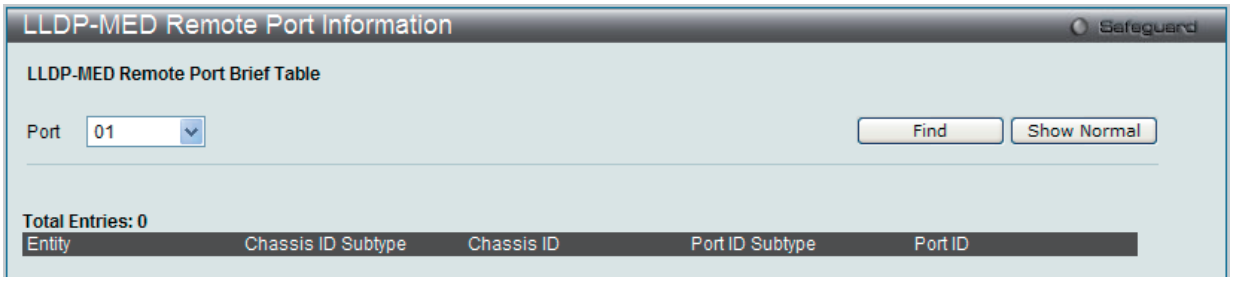


図 9-144　LLDP-MED Remote Port Information 画面 - Brief

「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 Normal」ボタンをクリックして、リモートポート情報の通常のレイアウトを参照します。

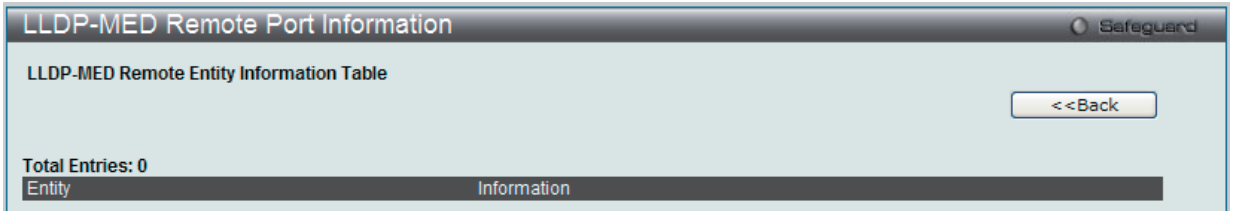


図 9-145　LLDP-MED Remote Port Information 画面 - Normal

「<<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。

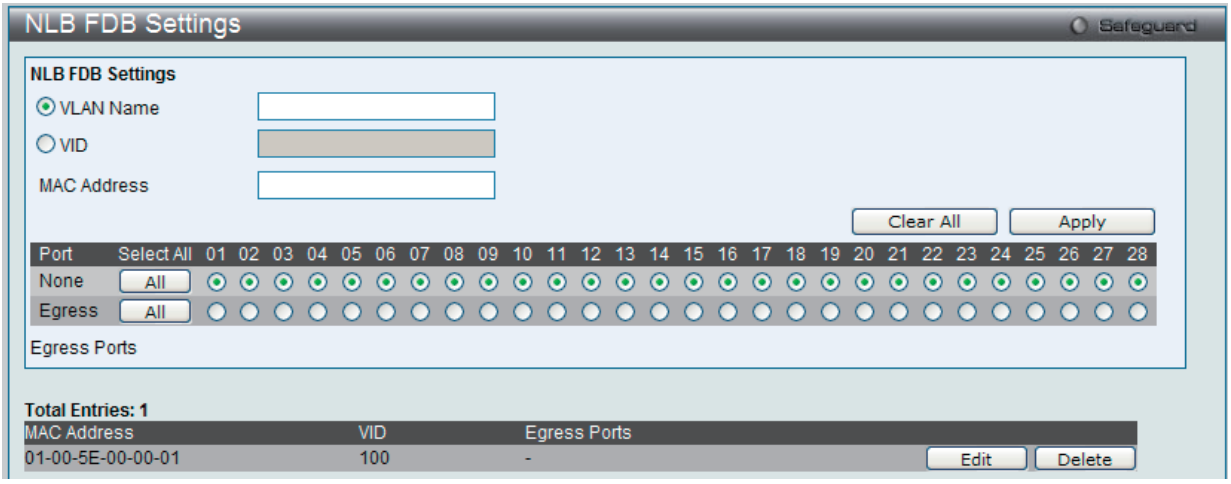


図 9-146　NLB FDB Settings 画面

以下の項目が設定可能です。

項目	説明
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	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、以下の画面を表示します。

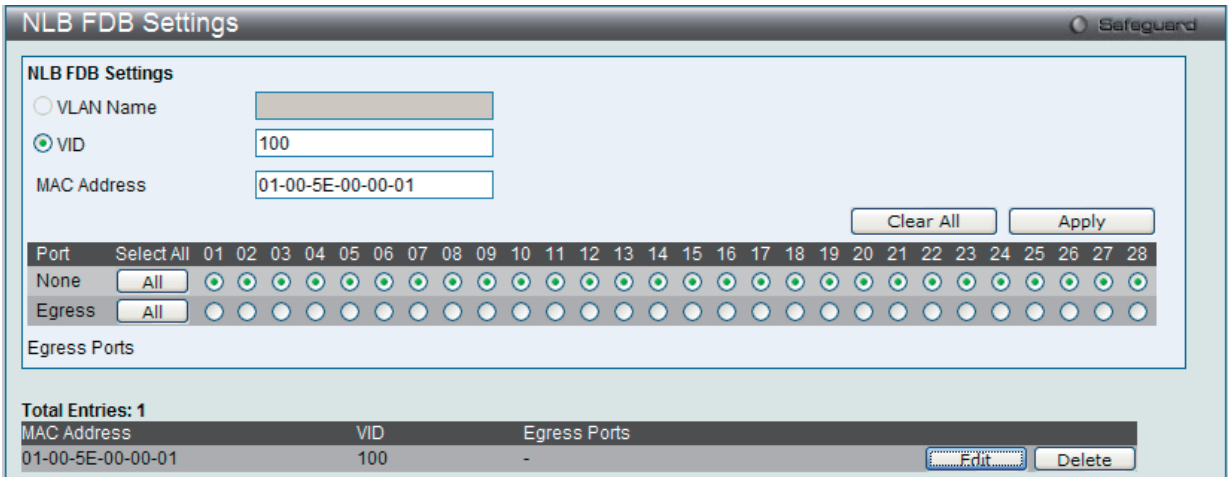


図 9-147　NLB FDB Settings 画面 - Edit

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 10 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。	210
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。	211
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。	211
IPv6 Route Table（IPv6 ルートテーブル）	IPv6 ルーティングテーブルの外部経路情報を参照します。	212
Policy Route Settings（ポリシールート設定）	ポリシールート機能を設定します。	213
IP Forwarding Table（IP フォワーディングテーブル）	直接接続するすべての IP 情報を参照します。	215
IP Multicast Forwarding Table（IP マルチキャストフォワーディングテーブル）	直接接続するすべての IP マルチキャスト情報を参照します。	215
IP Multicast Interface Table（IP マルチキャストインタフェーステーブル）	直接接続するすべての IP マルチキャストインタフェース 情報を参照します。	216
Route Preference Settings（ルート優先度設定）	ルート優先度の設定を行います。	216
ECMP Algorithm Settings（ECMP アルゴリズム設定）	ECMP OSPF の 状態を設定します。	217
Route Redistribution Settings（ルート再配送設定）	OSPF または RIP が動作するネットワーク上のルータに OSPF と RIP 間のルーティング情報を再配送する設定を行います。	217
IP Tunnel（IP トンネル）	IP トンネルを設定します。以下のメニューがあります。 IP Tunnel Settings（IP トンネル設定）、IP Tunnel GRE Settings（IP トンネル GRE 設定）	218
OSPF（OSPF 設定）	OSFP の設定を行います。以下のメニューがあります。 OSPFv2（OSPFv2 設定）	221
RIP（RIP 設定）	RIP の設定を行います。以下のメニューがあります。: RIP Settings（RIP 設定）	246
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）	IP マルチキャスティング設定を行います。以下のメニューがあります。 IGMP（IGMP 設定）、DVMRP（DVMRP 設定）、PIM（PIM 設定）	251
VRRP（VRRP 設定）	VRRP リレーの設定を行います。以下のメニューがあります。 VRRP Global Settings（VRRP グローバル設定）、VRRP Virtual Router Settings（VRRP 仮想ルータ設定）、VRRP Authentication Settings（VRRP 認証設定）	266
MD5 Key Settings（MD5 キー設定）	MD キーを登録します。	270

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 と IPv6 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、IPv6 には最大 128 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と、ARP 応答は送信されません。

また、スイッチはフローティングスタティックルートをサポートしています。これは、同じネットワークにある異なるネクストホップデバイスに代替のスタティックルートを作成できるものです。この 2 個目のネクストホップデバイスのルートは、プライマリスタティックルートがダウンした場合のバックアップ用スタティックルートであると見なされます。プライマリルートをなくした場合、バックアップルートがリンクアップし、アクティブな状態になります。本スイッチのフォワーディングテーブル内へのエントリは IP アドレスのサブネットマスクとゲートウェイの両方を使用して行います。

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。

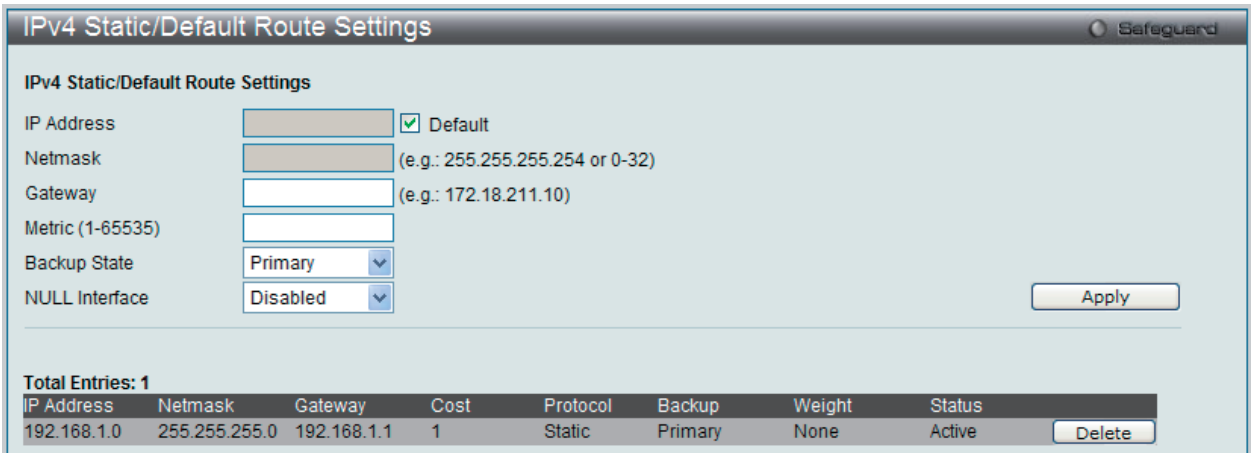


図 10-1　IPv4 Static/Default Route Settings 画面

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またはデフォルトルートに割り当てる IPv4 アドレスを入力します。
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。
Backup State	Primary、Backup、または Weight から選択します。 各 IP アドレスは 1 つのプライマリルートを持っており、一方、他のルートはバックアップ状態に割り当てられる必要があります。プライマリルートに障害が発生すると、スイッチはルートが回復するまでルーティングテーブルが学習した順番に従ってバックアップルートを試します。スタティックおよびデフォルトルートが設定されるバックアップ状態を示します。
NULL Interface	ルートの NULL 機能を有効または無効にします。Null インタフェースはトラフィックをフィルタする別の方法を提供します。Null インタフェースに送信されるパケットはスイッチに破棄されます。

エントリの登録
情報を入力後、「Apply」ボタンをクリックします。

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。

IPv4 Route Table（IPv4 ルートテーブル）

IPv4 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 10-2　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	検索に使用する IPv4 ネットワークアドレスを指定します。ネットワークアドレスは使用するサブネットマスクのために CIDR 表記に従うべきです。
IP Address	CIDR 表示を使用しないで検索するために使用される特定の IPv4 アドレスを指定します。
RIP	RIP に関連するルートを表示します。
OSPF	OSPF に関連するルートを表示します。
Hardware	チップに記述されているルートだけを表示します。

「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。

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。

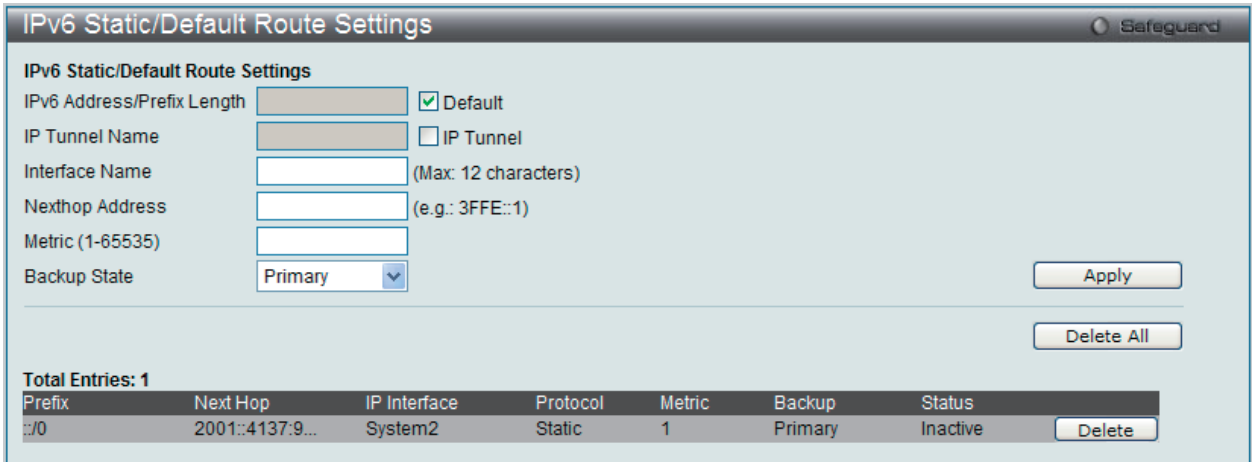


図 10-3　IPv6 Static/Default Route Settings 画面

画面には以下の項目が表示されます。

項目	説明
IPv6 Address/Prefix Length	IPv6 スタティックルートエントリの IPv6 アドレスと対応するプレフィックス長を指定します。
IP Tunnel Name	「IP Tunnel」オプションをチェックして、IP トンネル名を入力します。
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	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。
Backup State	各 IP アドレスは 1 つのプライマリルートを持っており、一方、他のルートはバックアップ状態に割り当てられる必要があります。プライマリルートに障害が発生すると、スイッチはルートが回復するまでルーティングテーブルが学習した順番に従ってバックアップルートを試します。IPv6 が設定されるバックアップ状態を示します。「Primary」または「Backup」を指定します。

エントリの登録
情報を入力後、「Apply」ボタンをクリックします。

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。

IPv6 Route Table（IPv6 ルートテーブル）

IPv6 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 > IPv6 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。

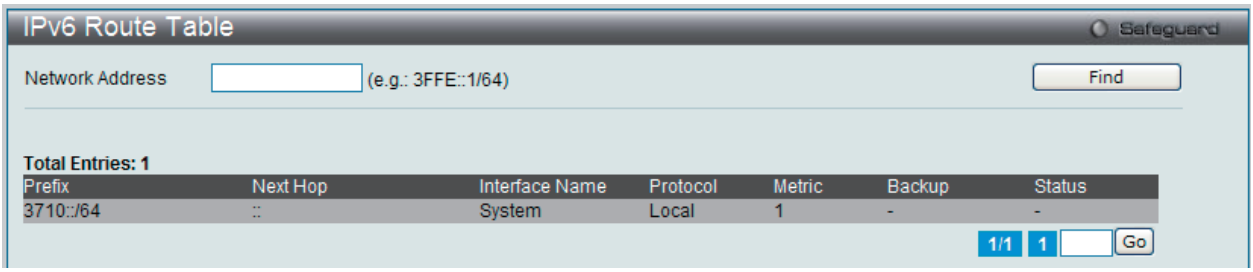


図 10-4　IPv6 Route Table 画面

画面には以下の項目が表示されます。

項目	説明
Network Address	検索に使用する IPv6 ネットワークアドレスを指定します。ネットワークアドレスは使用するサブネットマスクのために CIDR 表記に従うべきです。

「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。

Policy Route Settings（ポリシールート設定）

ポリシーベースルーティングは、指定したデバイスにインターネットへの最適な経路を与えるためにスイッチに使用される方法です。アクセスプロファイル機能と連携して使用される場合、スイッチはデバイスから送信されたトラフィックについてアクセスプロファイル機能を使用して識別し、ご使用のネットワークの通常のルーティング体系よりもインターネットにより直接的に接続するネクストホップルータに転送します。

下の図は例です。

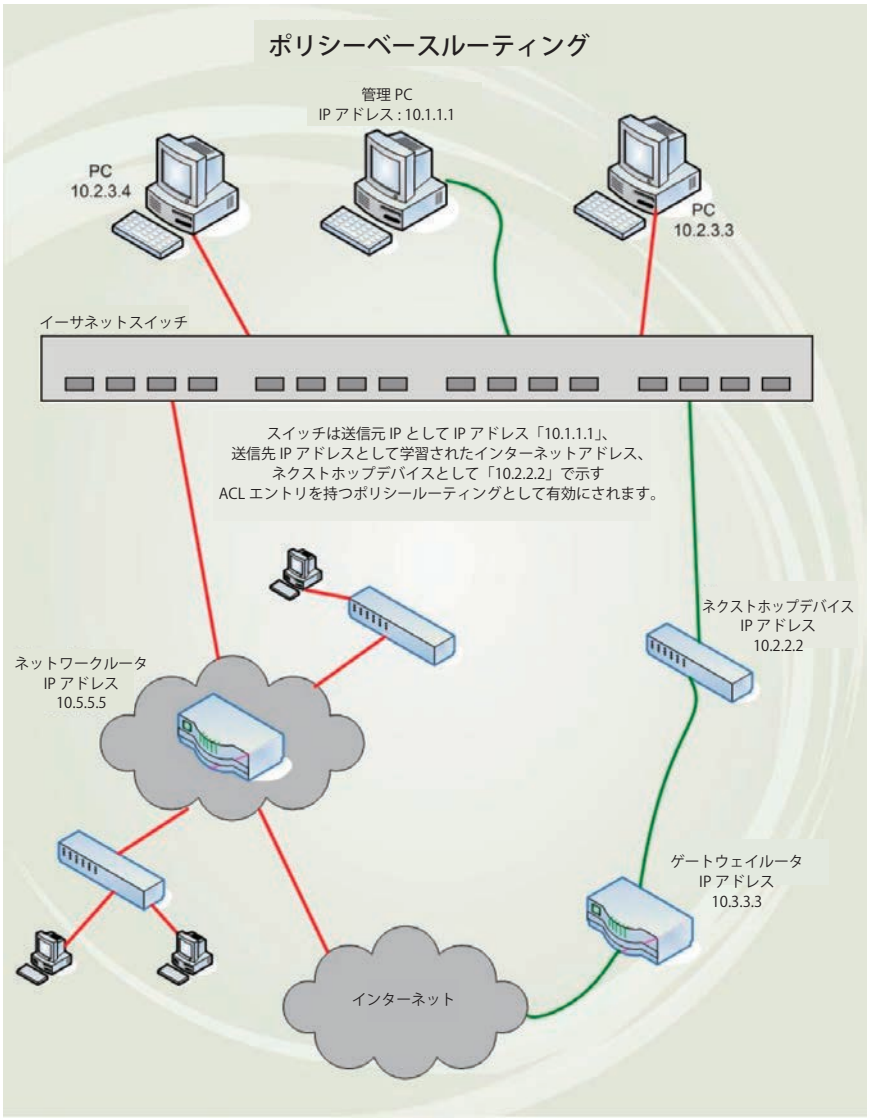


図 10-5　ポリシーベースルート例

IP アドレス「10.1.1.1」の PC が会社のマネージャに所属し、他の PC が従業員に所属しているとします。ネットワーク管理者は、ポリシールーティングスイッチをゲートウェイルータ「10.3.3.3」に直接接続しているネクストホップデバイス「10.2.2.2」を使用してインターネットにより直接的な接続を行うように設定し、ネットワークトラフィックを回避することを望みます。このようにノーマルなネットワークとそのトラフィックを避けることができます。これを実行するためには、スイッチのアクセスプロファイル機能を使用し、適切な情報に従って送信元 IP アドレスとして IP アドレス「10.1.1.1」を、送信先 IP アドレスとして（ルーティングプロトコル経由で学習した）インターネットアドレスを PC に設定する必要があります。次に、管理者は「Policy Route」画面で設定を行い、アクセスプロファイルとその関連ルールを有効にし、さらにネクストホップルータの IP アドレス「10.2.2.2」を設定します。最後にポリシールートエントリを有効にします。

設定を完了すると、アクセスプロファイル機能を使用して IP アドレスを識別し、ポリシーベースルートがあることを認知します。その後、ゲートウェイルータにパケットをリレーする指定のネクストホップルータに対して情報をフォワードします。このようにしてインターネットへの新しい経路が設定されます。

本機能の実行には以下の制限および注意があります。

1. アクセスプロファイルはルールに従ってはじめに作成される必要があります。管理者がアクセスプロファイルなしで本機能を有効にしようとすると、エラーメッセージが表示されます。
2. アクセスプロファイルが Deny に設定されると、パケットは破棄され、ネクストホップルータにフォワードされません。
3. 管理者が設定済みのポリシールートに直接リンクするルールまたはプロファイルを削除すると、エラーメッセージが直ちに現れます。

ポリシールート機能を設定するためには、**L3 Features > Policy 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。

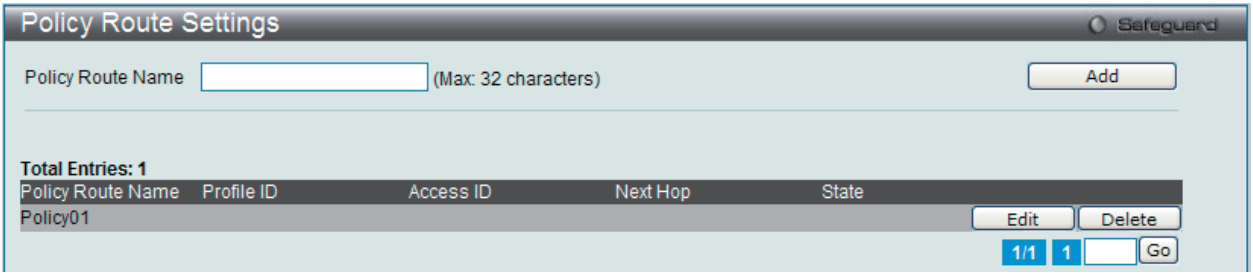


図 10-6　Policy Route Settings 画面

「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。
「Edit」ボタンをクリックして、指定エントリを編集します。
「Delete」ボタンをクリックして、指定エントリを削除します。
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

ポリシールートの編集をするためには、「Edit」ボタンをクリックして以下の画面を表示します。

図 10-7　Policy Route Settings 画面 - Edit

以下の項目を設定します。

項目	説明
Policy Route Name	ポリシールート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。
Profile ID (1-1024)	作成済みのアクセスプロファイルの Profile ID 番号を入力します。これはパケットを以下に続くこのポリシールートとして識別するために使用されます。このアクセスプロファイルはアクセスルールに従っており、このポリシールートの作成前に作成される必要があります。
Access ID (1-1024)	作成済みのアクセスプロファイルの Access ID 番号を入力します。これはパケットを以下に続くこのポリシールートとして識別するために使用されます。このアクセスルールはアクセスプロファイルに従っており、このポリシールートの作成前に作成される必要があります。
Next Hop IPv4 Address	インターネットに接続しているゲートウェイルータも直接接続しているネクストホップルータの IP アドレスを入力します。
State	プルダウンメニューを使用して、ポリシールートを「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。

IP Forwarding Table（IP フォワーディングテーブル）

IP フォワーディングテーブルは直接接続するすべての IP 情報を保存しています。ここでは直接接続するすべての IP 情報を参照します。

L3 Features > IP Forwarding Table をクリックし、以下の画面を表示します。

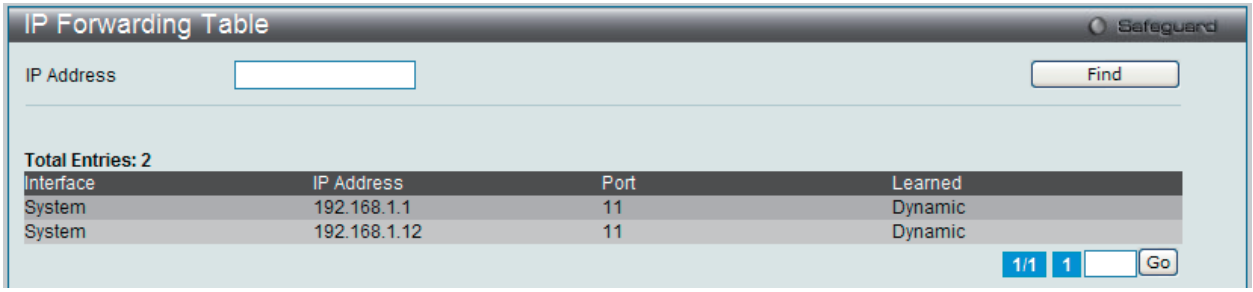


図 10-8　IP Forwarding Table 画面

以下の項目が使用できます。

項目	説明
IP Address	インタフェースの IP アドレスを入力します。

「IP Address」を入力後、「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。

IP Multicast Forwarding Table（IP マルチキャストフォワーディングテーブル）

本画面では、スイッチ上の現在の IP マルチキャスト情報が確認できます。

L3 Features > IP Multicast Forwarding Table 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 10-9　IP Multicast Forwarding Table 画面

エントリの参照

「Group Address」および「Network Address」を入力し、「Find」ボタンをクリックして情報を検索します。
「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。

IP Multicast Interface Table（IP マルチキャストインタフェーステーブル）

スイッチにおける現在のマルチキャストインタフェースを表示します。

L3 Features > IP Multicast Interface Table 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。

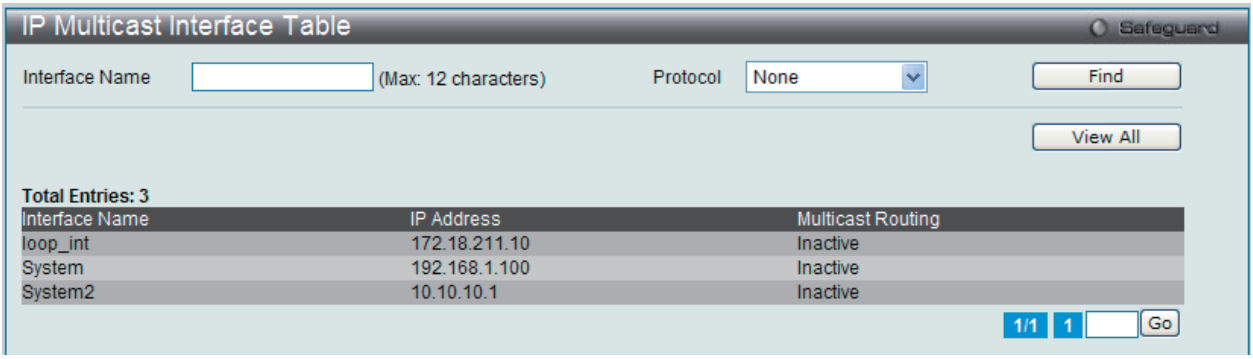


図 10-10　IP Multicast Interface Table 画面

エントリの参照

特定のエントリを検索するためには、「Interface Name」にマルチキャスト名を入力するか、「Protocol」メニューからプロトコルを選択して、「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。

Route Preference Settings（ルート優先度設定）

このスイッチにルート優先度を設定します。

L3 Features > Route Preference 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。

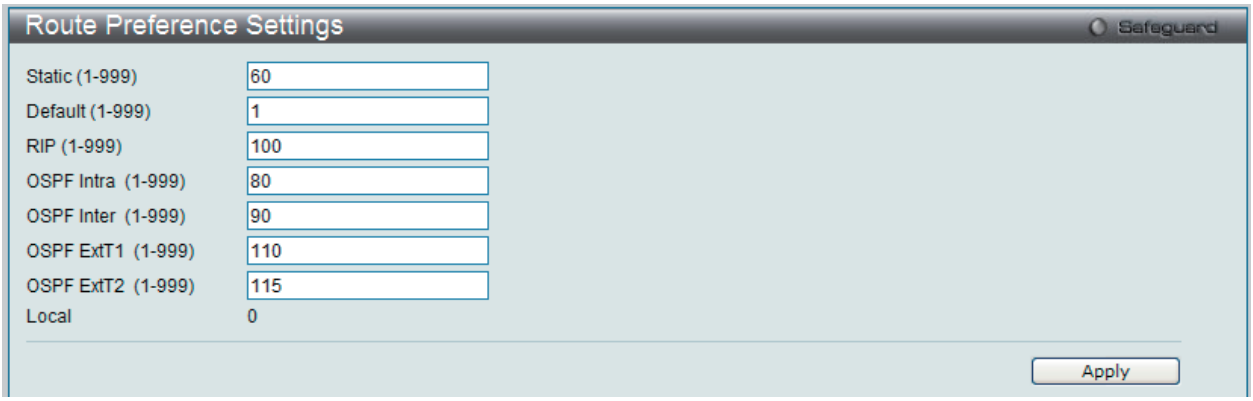


図 10-11　Route Preference Settings 画面

以下の項目が設定、表示に使用されます。

項目	説明
Static (1-999)	1 から 999 の範囲から、Static のルート優先度を指定します。初期値は 60 です。
Default (1-999)	デフォルトルートの優先度値を設定します。初期値は 1 です。
RIP	RIP ルートに優先度値を設定します。初期値は 100 です。
OSPF Intra	OSPF Intra-area ルートに優先度値を設定します。初期値は 80 です。
OSPF Inter	OSPF Inter-area ルートに優先度値を設定します。初期値は 90 です。
OSPF ExtT1	OSPF external type-1 ルートに優先度値を設定します。初期値は 110 です。
OSPF ExtT2	OSPF external type-2 ルートに優先度値を設定します。初期値は 115 です。
Local	ローカルルートの優先度値を表示します。

「Apply」ボタンをクリックし、設定を有効にします。

ECMP Algorithm Settings（ECMP アルゴリズム設定）

このスイッチに ECMP OSPF 状態を設定します。

L3 Features > ECMP Algorithm Settings をクリックし、以下の画面を表示します。

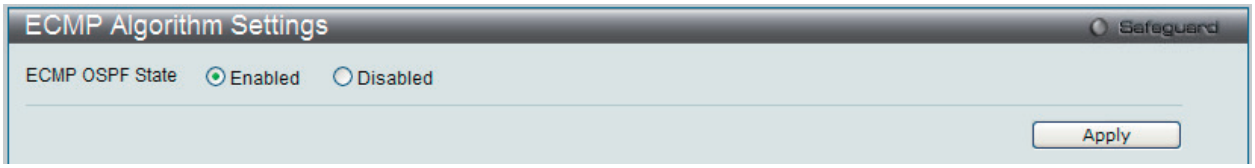


図 10-12 ECMP Algorithm Settings 画面

以下の項目が使用できます。

項目	説明
ECMP OSPF State	ECMP OSPF 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。

Route Redistribution Settings（ルート再配布設定）

1 つのルーティングプロトコルから別のルーティングプロトコルまでルーティング情報を再配布するように設定します。

L3 Features > Route Redistribution 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。

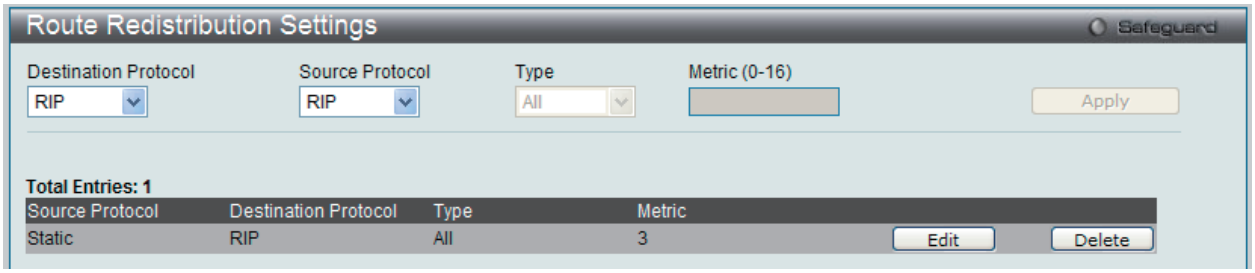


図 10-13 Route Redistribution Settings 画面

以下の項目が使用されます。

項目	説明
Destination Protocol	送信先プロトコルを指定します。「RIP」または「OSPF」を選択します。
Source Protocol	送信元プロトコルを指定します。「RIP」、「OSPF」、「Static」または「Local」を選択します。
Type	再配布するルートのタイプを指定します。「All」、「Internal」、「External」、「Ext Type1」、「Ext Type2」、「Inter-E1」または「Inter-E2」から選択します。すべてのルートタイプを再配布するためには、「All」オプションを選択します。
Metric (0-16)	再配布ルートのメトリック値を指定します。

「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

編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

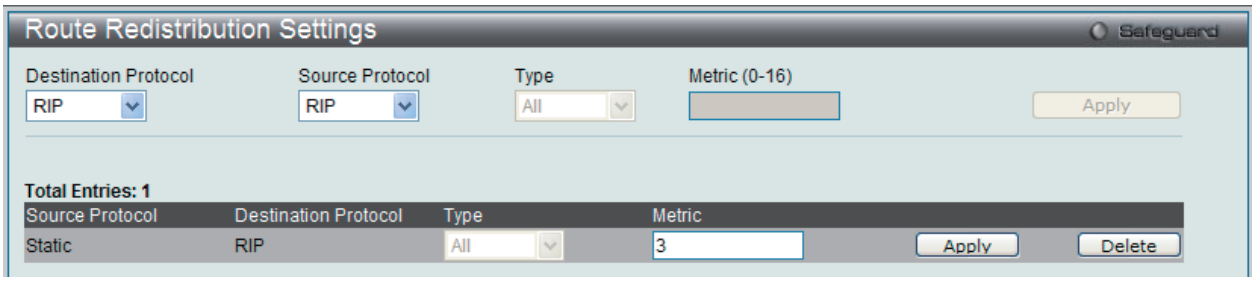


図 10-14 Route Redistribution Settings 画面 - Edit

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。

IP Tunnel（IP トンネル）

IP Tunnel Settings（IP トンネル設定）

IP トンネルを設定します。

L3 Features > IP Tunnel > IP Tunnel 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。

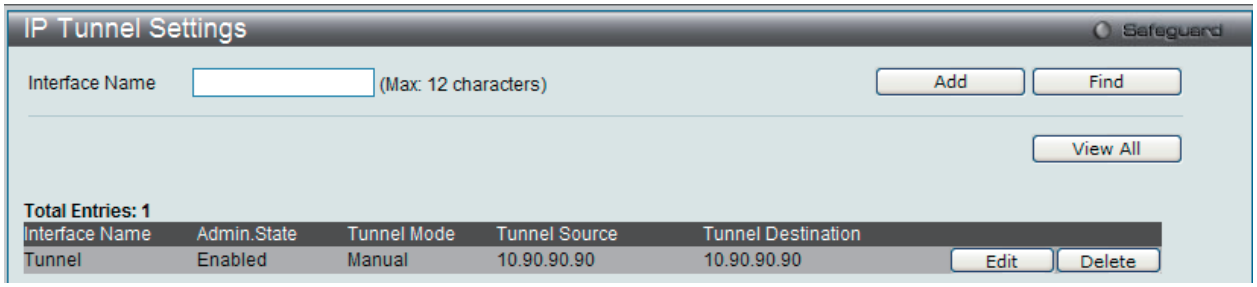


図 10-15 IP Tunnel Settings 画面

以下の項目が使用されます。

項目	説明
Interface Name	IP トンネルのインタフェース名を入力します。

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。「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

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。

エントリの編集

1. 編集するポートの「Edit」ボタンをクリックし、以下の画面を表示します。

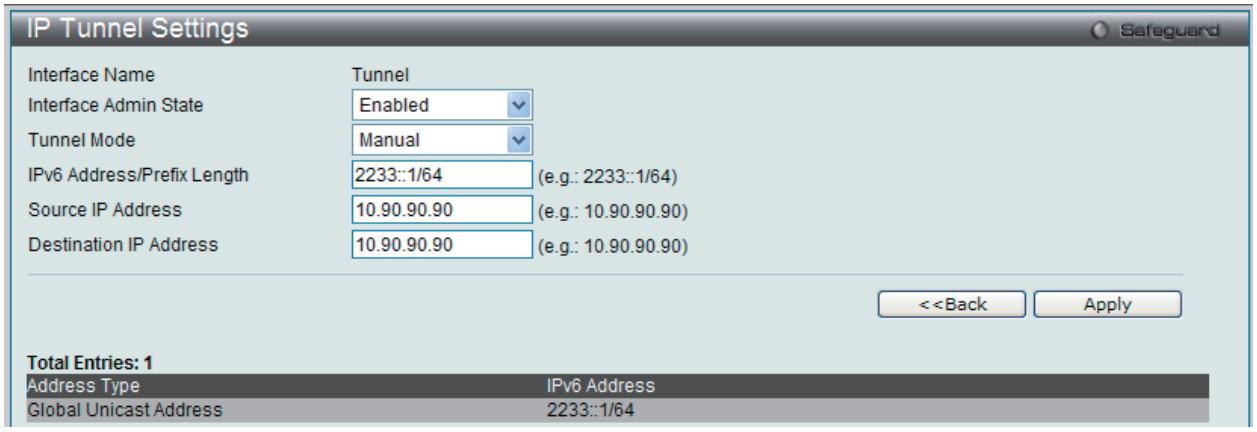


図 10-16 IP tunnel Settings - Edit 画面

以下の項目が使用されます。

項目	説明
Interface Admin State	プルダウンメニューを使用して、「Interface Admin State」を「Enabled」（有効）/「Disabled」（無効）にします。
Tunnel Mode	プルダウンメニューを使用してトンネルモードを選択します。None、Manual、6to4、および ISATAP から選択できます。
IPv6 Address/Prefix Length	IPv6 アドレスネットワークアドレスを入力します。
Source IP Address	送信元 IP アドレスを指定します。
Destination IP Address	送信先 IP アドレスを指定します。

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックして前のページに戻ります。

IP Tunnel GRE Settings（IP トンネル GRE 設定）

スイッチにおいて既存のトンネルを GRE トンネル (IPv6-in-IPv4) として設定します。このトンネルが以前に別のモードで設定されていると、トンネルの情報はデータベースにまだ存在します。しかし、トンネルの以前の情報が有効かどうかは、現在のモードに依存します。

GRE トンネルは、単にサイト内またはサイト間で使用できる point-to-point トンネルです。

GRE IPv6/IPv4-in-IPv4 トンネルを設定する場合、送信プロトコルが IPv4 プロトコルであるため、送信元と送信先アドレスの双方とも IPv4 アドレスである必要があります。送信元と送信先アドレスタイプが一致していないと、GRE トンネルは動作しません。

GRE IPv6/IPv4-in-IPv4 トンネルを設定する場合、送信プロトコルが IPv6 プロトコルであるため、送信元と送信先アドレスの双方とも IPv6 アドレスである必要があります。送信元と送信先アドレスタイプが一致していないと、GRE トンネルは動作しません。

L3 Features > IP Tunnel > IP Tunnel GRE 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 :

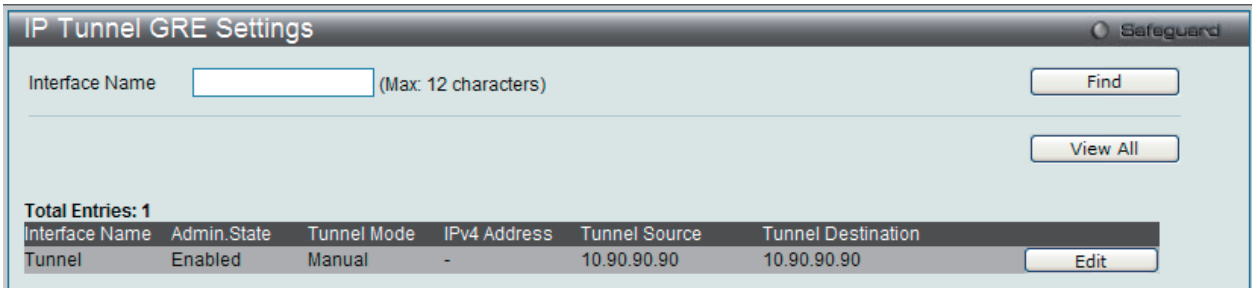


図 10-17 IP Tunnel GRE Settings 画面

以下の項目が使用されます。

項目	説明
Interface Name	IP トンネルのインタフェース名を入力します。

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。
「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。

エントリの編集

1. 編集するポートの「Edit」ボタンをクリックし、以下の画面を表示します。

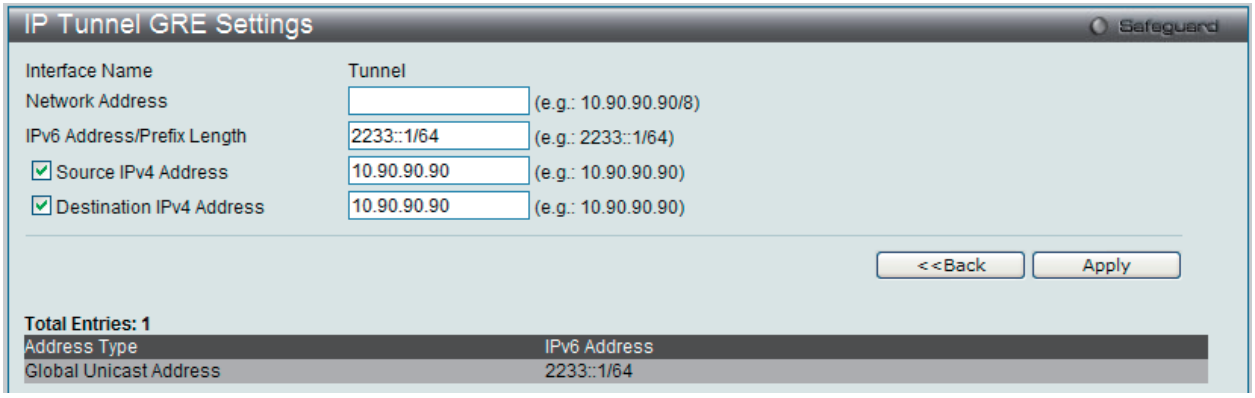


図 10-18 IP tunnel GRE Settings - Edit 画面

以下の項目が使用されます。

項目	説明
Network Address	GRE トンネルインタフェースに割り当てた IPv4 アドレスを入力します。IPv4 アドレスが設定される場合、IPv4 の処理はこの IPv4 トンネルインタフェースで有効となります。この IPv4 アドレスはトンネルの送信元または送信先の IPv4 アドレスには接続していません。
IPv6 Address/Prefix Length	GRE トンネルインタフェースに割り当てた IPv6 アドレスを入力します。IPv6 アドレスが設定される場合、IPv4 の処理はこの IPv6 トンネルインタフェースで有効となります。この IPv6 アドレスはトンネルの送信元または送信先の IPv6 アドレスには接続していません。
Source IPv4 Address	ラジオボタンをクリックして、GRE トンネルインタフェースの送信元 IPv4 アドレスを入力します。これは、このトンネルのパケットに送信元アドレスとして使用されます。使用するアドレスタイプは送信プロトコルに依存します。送信元と送信先の両方で使用されるアドレスタイプが一致していないと、GRE トンネルは動作しません。
Destination IPv4 Address	ラジオボタンをクリックして、GRE トンネルインタフェースの送信先 IPv4 アドレスを入力します。これは、このトンネルのパケットに送信先アドレスとして使用されます。使用するアドレスタイプは送信プロトコルに依存します。送信元と送信先の両方で使用されるアドレスタイプが一致していないと、GRE トンネルは動作しません。

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックして前のページに戻ります。

OSPF（OSPF 設定）

OSPF（Open Shortest Path First）ルーティングプロトコルは、Link-State アルゴリズムを使用して宛先ネットワークまでのルートを決定します。「リンク」はルータ上のインタフェースを指し、「State」（状態）はそのインタフェースと隣接するルータ間の関係を指しています。「State」には、IP アドレス、サブネットマスク、インタフェースに接続しているネットワークタイプ、そのネットワークに接続する他のルータなどの情報があります。「Link-State」情報は、Link-State データベースに集められ、OSPF が動作するルータによって維持されます。

OSPF では、ルータがどのように通信を行い、Link-State データベースを維持するかについて規定し、また OSPF を使用するネットワークトポロジについての概念を定義しています。

ルータ間の Link-State アップデートのトラフィックを制限するために、OSPF ではエリアという概念が定義されています。1 つのエリア内にあるすべてのルータは、1 つの Link-State データベースを共有し、1 つのルータによってデータベースに変更が生じると、それをトリガーとして同一エリア内にあるすべてのルータの Link-State データベースが更新されます。ルータのうち、複数のエリアに接続しているものを境界ルータ（Border Router）と呼びます。境界ルータはエリア間のルーティング情報を配信する役割を担います。

1 つのエリアは、エリア 0 またはバックボーンとして定義されます。このエリアは、ネットワークの中心的なエリアで、他のすべてのエリアはこのバックボーンエリアに（ルータを経由して）接続します。バックボーンエリアにはルータのみが接続し、あるエリアでルーティング情報の変更が発生するとバックボーンに伝えられ、そこから他のネットワークへ伝播されるような構造になっています。

OSPF を使用したネットワークを構築する際は、まずバックボーン（エリア 0）を構築し、そこからネットワークを広げるように構築することをお勧めします。

Link-State アルゴリズム

OSPF ルータは、Link-State アルゴリズムを使用して、すべての宛先への最短なパスツリーを構築します。以下にアルゴリズムの各段階を簡単にして説明します。

- OSPF の起動時、またはルーティング情報に変化が生じた時、ルータは Link-State Advertisement（通知）を生成します。この通知は OSPF 用の特別な形式のパケットでルータ上のすべての Link-State が格納されています。
- 本 Link-State Advertisement がエリア内のすべてのルータに伝達されます。Link-State Advertisement を受け取った各ルータは、それを保存し、またコピーを他のルータに送信します。
- 各ルータの Link-State データベースが更新されると、各ルータは自身をルート（根元）としたすべての宛先への最短パスツリーを計算します。IP ルーティングテーブルには、宛先アドレス、コスト、そして各宛先にたどり着くためのネクストホップのアドレスが書き込まれます。OSPF プロトコルは、RIP と異なりすべての宛先に対する複数のイコールコストルートを保持します。本スイッチシリーズは、ハードウェアチップに同じ宛先ネットワーク用に最大 8 個のイコールコストをサポートしています。
- 一度 Link-State データベースが更新され、パスツリーが計算され、IP ルーティングテーブルに書き込みがされると、OSPF ネットワークにリンクダウンなどの変化が起こらない限り、OSPF トラフィックの発生は少なく抑えられます。

最短パスアルゴリズム

宛先への最短パスは Dijkstra アルゴリズムを使用して計算されます。各ルータをツリーの根元の部分とした宛先への数あるルートの中から、累積コストに基づいて各宛先への最短パスが計算されます。エリア内のルータのそれぞれが同一の Link-State データベースを持つものの、各ルータは（ネットワークエリア内での自身の位置を考慮した）自身の最短パスツリーを持つようになります。

以下の項に最短パスツリーの構築のために使用する情報を紹介します。

OSPF コスト

各 OSPF インタフェースは、そのインタフェースからのパケット送信に必要なオーバヘッドを表すコスト（メトリックとも呼ばれます）を持ちます。コストはインタフェースの帯域幅と反比例します。つまり、広帯域のインタフェースは低いコストを持つことになります。パケットを 56Kbps のダイアルアップ接続にて送信する場合は、10Mbps イーサネット接続で送信する場合よりコストが高く（また遅延が長く）なります。OSPF コストの計算公式は以下の通りです。
Cost = 100,000,000 / 帯域（bps）

例えば、10Mbps イーサネットケーブルのコストは 10、また 1.544Mbps T1 ケーブルを介するコストは 64 になります。

最短パスツリー

以下の図中のルータ A の最短パスツリーを構築するために、ルータ A をツリーの根元に置き、各宛先ネットワークへの最小コストを計算します。

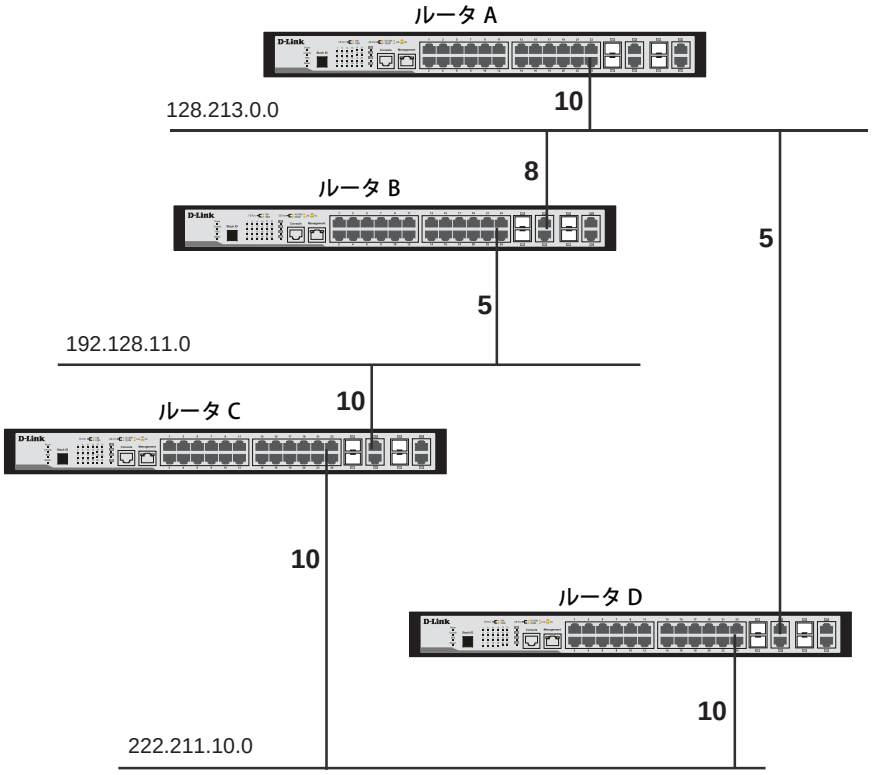


図 10-19　最短パスツリーの構築

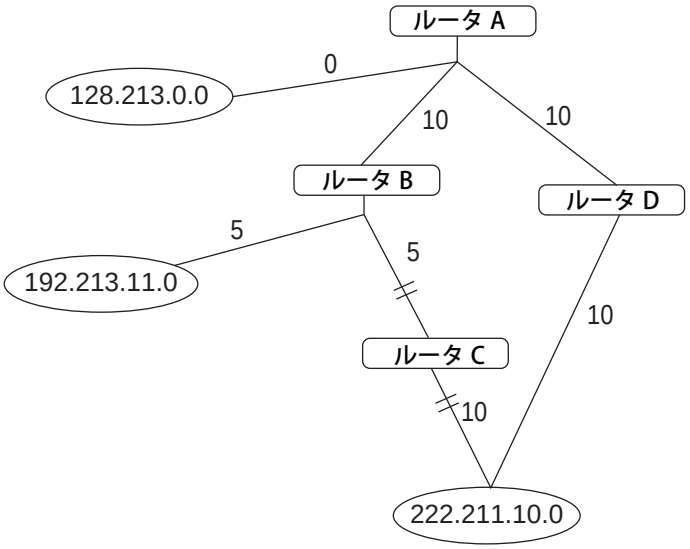


図 10-20　最短パスツリーの構築

上の図はルータ A から見たネットワークを示しています。ルータ A は、ルータ B を経由して 192.213.11.0 のネットワークに到達し、そのコストは 10 + 5 = 15 となります。ルータ A は、ルータ C を経由して 222.211.10.0 のネットワークに到達し、そのコストは 10 + 10 = 20 になります。

また、ルータ A は、ルータ B とルータ D を通って、222.211.10.0 に到達し、この時コストは 10 + 5 + 10 = 25 となります。しかし、そのコストはルータ C を通る時よりも高くなります。コストの高いルートは、ルータ A の最短パスツリーに入ることはできません。最終的なツリーは、以下のようになります。

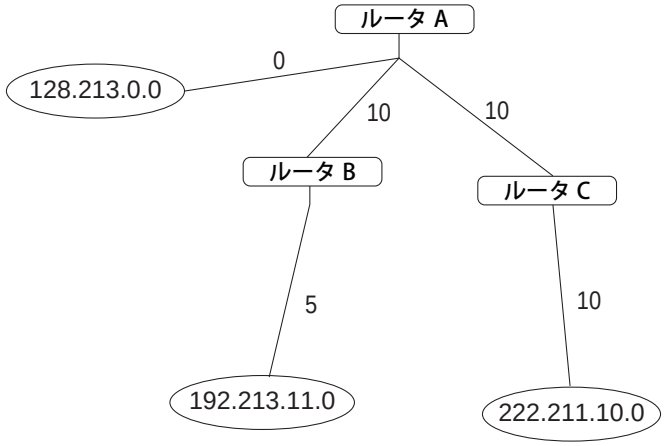


図 10-21　最短パスツリーの構築 – 完了

このパスツリーはルータ A から見たものであることに注意が必要です。例えばルータ B からルータ A へのリンクのコストは、ルータ A の最短パスツリー構築の上では重要ではありません。しかし、ルータ B の最短パスツリー構築には大変重要になってきます。

直接接続されるネットワークはコスト 0 で到達します。一方、他のネットワークは最短パスツリーで算出されたコストで到達します。

ルータ A は、ネットワークアドレスと最短パスツリー構築の際に算出したコストを使用して、ルーティングテーブルを作成することができます。

エリアと境界ルータ

OSPF Link-State アップデートはネットワーク上のすべてのルータにフラッディングすることにより送信されます。OSPF はエリアの概念を利用して、Link-State アップデートを受け取る必要のあるルータのネットワーク上の場所を定義します。これにより、ルーティングアップデートがネットワーク中にフラッディングされなくなり、数多くのルータのルーティングテーブルを更新する際の帯域消費を軽減できるようになります。

エリアには、Link-State アップデートのフラッディングが必要でなくなる境界線があります。そのため Link-State データベースの交換や、最短パスツリーの算出はルータが接続するエリア内に限定することができます。

複数のエリアと接続するルータを境界ルータ（BR）と呼びます。この境界ルータは、必要なルーティング情報とその変更をエリア間に配布する義務を持ちます。

エリアはルータインタフェースに対して指定されます。自身のすべてのインタフェースが同じエリア内にあるルータを、内部ルータ（Internal Router）と呼びます。自身のインタフェースが複数のエリア内にあるルータを境界ルータと呼びます。（他のルーティングプロトコルを使用して）他のネットワークへのゲートウェイの役割を担うルータを Autonomous System 境界ルータ（ASBR）と呼びます。

Link-State パケット

Link-State パケットには様々なタイプがあります。そのうちの 4 つの説明を以下に示します。

- Router Link-State Updates - 1 つのエリアのルータから宛先へのリンクを示します。
- Summary Link-State Updates - 境界ルータが発行し、エリア外で自律システム（AS）内のネットワークへのリンクを示します。
- Network Link-State Updates - 複数のルータが接続されるマルチアクセスエリアが発行します。1 つのルータが代表ルータ（DR）として選出され、このルータがセグメント上のすべてのルータに関する Link-State Update を発行します。
- External Link-State Updates - AS 境界ルータにより発行され、AS 外へのルート、または AS 外へのデフォルトルートを示します。

これらの Link-State アップデートのフォーマットについて以下に説明します。

Router Link-State Updates は、エリア内のすべてのルータにフラッディングされます。これらのアップデートには、すべてのルータのインタフェースから到達可能な宛先が記述されています。

Summary Link-State Updates は、境界ルータにより生成され、AS 内の他のネットワークのルーティング情報を伝達するために使用されます。通常すべての Summary Link-State Updates は、バックボーン（エリア 0）に送信され、その後ネットワーク内の他のすべてのエリアに送信されます。また、境界ルータは AS 境界ルータからのルーティング情報を伝達する任務を持ち、ネットワーク内のルータが他の AS へのルートを獲得し、記録するために有益です。

Network Link-State Updates は、（複数のルータが接続する）マルチアクセスセグメントに代表ルータとして選定されたルータが生成します。これらのアップデートには、セグメント上のすべてのルータとそれらのネットワーク接続情報が記述されています。

External Link-State Updates には、AS の外のネットワークへのルーティング情報が記述されます。これらのアップデートの生成と伝達は、AS 境界ルータが行います。

OSPF 認証
事前に定義されるパスワードを使用し、OSPF パケットに対して信頼のおけるルータから送信されてきたものかを判断するための認証を行うことができます。初期値では認証を行わない設定になっています。

認証の方法には、シンプルパスワード認証とメッセージダイジェスト認証（MD-5）を採用しています。

メッセージダイジェスト認証（MD-5）
MD-5 は暗号化方式です。各ルータにキーとキー ID が設定されます。ルータはアルゴリズムを使用して、OSPF パケット、キーおよびキー ID から、数学的な「メッセージダイジェスト」を生成します。生成されたメッセージダイジェストはパケットに付加されます。このキーがネットワーク上で交換されることはなく、非減少シーケンス番号が付加されて、リプレイアタックを防止します。

シンプルパスワード認証
パスワード（またはキー）をエリアごとに設定します。ルーティングドメインに参加する、同一エリア内のルータには同じキーを設定する必要があります。この方法は、リンクアナライザを使用してパスワードを盗聴するパッシブアタックに対しては、脆弱であると言えます。

バックボーンとエリア 0
OSPF は、ルータ間で交換する Link-State アップデートの数を制限するために、ルータが稼動するエリアを定義します。複数のエリアを登録する時、そのうちの 1 つのエリアを「エリア 0」として登録し、そのエリアをバックボーンと呼びます。

バックボーンは他のエリアの中心に位置します。ネットワークのすべてのエリアは、ルータを経由してバックボーンへの物理的な（または仮想の）コネクションを持ちます。OSPF では、ルーティング情報を、まずエリア 0 に送信し、そこからネットワーク上の他のすべてのエリアへ（そして他のすべてのルータへ）伝達されます。

エリアが必要な状況でありながら、バックボーンへの物理接続が難しい場合は、仮想リンクを定義することができます。

仮想リンク
仮想リンクは以下の 2 つの目的のために使用されます。
- バックボーンへの物理接続を持たないエリアにリンクを提供する。
- エリア 0 に不連続箇所が発生した場合の臨時接続。

エリア 0 に物理的に接続していないエリア
OSPF ネットワークのすべてのエリアは、バックボーンへの物理接続を持たなければなりません。しかし、リモートエリアとバックボーンを物理的に接続することが不可能な場合があります。そのような場合には、仮想リンクを定義してリモートエリアとバックボーンを接続します。仮想パスとは、共通エリアを持つ 2 つの境界ルータ間の論理パスです。2 つの境界ルータのうち、 1 つはバックボーンに接続されます。

バックボーンの分割
OSPF では、バックボーンが不連続になった場合、分断されたバックボーンを接続するために仮想リンクが使用されます。これは異なるエリア 0 間を論理パスを使用してリンクするのと同じと考えられます。仮想リンクは、ルータの故障時などに備えて冗長性を持たせるためにも利用できます。仮想リンクの設定は、各エリア 0 への接続を持つ 2 つの境界ルータに対して行います。

Neighbor ルータ（近接ルータ）
同一エリアまたはセグメントに接続しているルータ同士を、そのエリアでの Neighbor ルータと呼びます。Neighbor ルータは Hello プロトコルにより選出されます。IP マルチキャストを利用して Hello パケットをセグメント上の他のルータに送信します。同一セグメントの他のルータが送信した Hello パケット内に、お互いが記載されている時、そのルータ同士は Neighbor ルータとなります。このように双方向通信が確立された近接関係にあるルータが近接ルータです。

Neighbor ルータになるためには、以下の条件が満たされている必要があります。
- Area ID - 2 つのルータが共通のセグメントを持ち、それらのインタフェースはセグメントの同じエリアに属していること。もちろん、それらインタフェースは同じサブネットに属し、同一のサブネットマスクを持ちます。
- Authentication - OSPF では、エリアにパスワードの設定が認められています。同一セグメントの同一エリア内にある 2 つのルータは、同じ OSPF パスワードを持っている必要があります。
- Hello and Dead Interval - Hello インターバルとは、ルータが OSPF インタフェースから送信する Hello パケットの送信間隔（秒）です。Dead インターバルとは、Hello パケットが受信されなくなってから、Neighbor ルータがそのルータがダウンしていると判断するまでの時間（秒）です。OSPF ルータは、各セグメント上で Hello パケットを交換し、お互いの存在を知らせたり、マルチアクセスセグメントでの代表ルータの選出を行います。OSPF では、Neighbor ルータ間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません。
- Stub Area Flag - 双方のルータの Hello パケット中にあるスタブエリアフラグが同じである必要があります。

隣接関係（Adjacency）

隣接関係にあるルータ同士は、ただ Hello パケットの交換や Link-State データベースの交換に参加するだけではありません。OSPF では、各マルチアクセスセグメント上で、1 つのルータを代表ルータ（DR）、もう 1 つのルータをバックアップ代表ルータ（BDR）として選出します。BDR は DR に障害が発生した場合に代理として働きます。同じセグメントの他のすべてのルータは DR と連絡し、Link-State データベースの更新や交換を行います。この方法により、Link-State データベースの更新に必要な帯域を低減することができます。

代表ルータの選出

DR と BDR の選出は、Hello プロトコルを用いて行います。あるマルチアクセスセグメントにおいて、最も高い OSPF プライオリティを持つルータが DR として選出されます。同じプライオリティを持つルータが他にもある場合は、大きなルータ ID を持つ方が選出されます。デフォルトの OSPF プライオリティは 1 です。プライオリティ 0 は DR として選出されてはいけないことを示します。

隣接関係（Adjacency）の構築

2 つのルータは、いくつかの段階を踏んで隣接関係を構築します。以下にその段階を簡素化して説明します。

- Down - セグメント上のどのルータからも情報が受信されていない状態です。
- Attempt - 非ブロードキャスト・マルチアクセスネットワーク上では（例えばフレームリレーまたは X.25 など）、本状態は隣接ルータからの情報がしばらく受信されていないことを示します。Hello パケットを Poll インターバルで指定された方法で送信し、隣接ルータにコンタクトを試みるべき状態です。
- Init - インタフェースで隣接ルータからの Hello パケットを検出しました。しかし、双方向通信はまだ確立されていません。
- Two-way - 隣接ルータとの双方向通信が確立されました。隣接ルータから受信した Hello パケットの中に自身のアドレスを見つけました。本段階の最後に DR と BDR の選出が行われます。ルータは隣接関係を築くかどうかを決定します。その決定は、どちらかのルータが DR であるか BDR であるか、またはリンクが Point-to-point であるか仮想リンクであるかに基づいて行われます。
- Exstart（Exchange Start）- ルータは情報交換パケット中に使用する最初のシーケンス番号を生成します。シーケンス番号はルータが常に最新の情報を受け取っていることを確認するために使用されます。1 つのルータがプライマリとなり、もう 1 つがセカンダリとなります。プライマリルータはセカンダリに情報のポーリングを行います。
- Exchange - ルータは Database description packet を送信して、すべての Link-State データベースを交換し合います。
- Loading - ルータの情報交換が完了します。ルータは Link-State request リストと Link-State retransmission リストを取得します。送信されるアップデートは認識されるまでの間、Link-State retransmission リストに置かれます。
- Full - 隣接ルータ同士は、完全な隣接関係を築きました。隣接ルータ同士は同じ Link-State データベースを持つようになります。

Point-to-Point インタフェースでの隣接関係

Point-to-Point インタフェースを使用して接続する（シリアルリンクなど）OSPF ルータは常に隣接関係を持っています。DR や BDR という概念は必要ありません。

OSPF パケットフォーマット

すべての OSPF パケットタイプは標準の 24 バイトヘッダで始まり、5 つのパケットデータタイプが存在します。まずヘッダについて説明し、次に各パケットデータについて説明します。

Hello パケットを除くすべての OSPF パケットでは、Link-State Advertisement が送信されます。例えば、Link-State Update パケットは、OSPF ルーティングドメイン内にアドバタイズメントをフラッディングします。

・OSPF パケットヘッダ
・Hello パケット
・Database Description パケット
・Link-State Request パケット
・Link-State Update パケット
・Link-State Acknowledgment パケット

OSPF パケットヘッダ

すべての OSPF パケットは 24 バイトのヘッダから始まります。このヘッダには、受信するルータがこのパケットを受け取って処理を行うかどうかを決定するための情報が含まれています。

OSPF パケットヘッダのフォーマットを以下に示します。

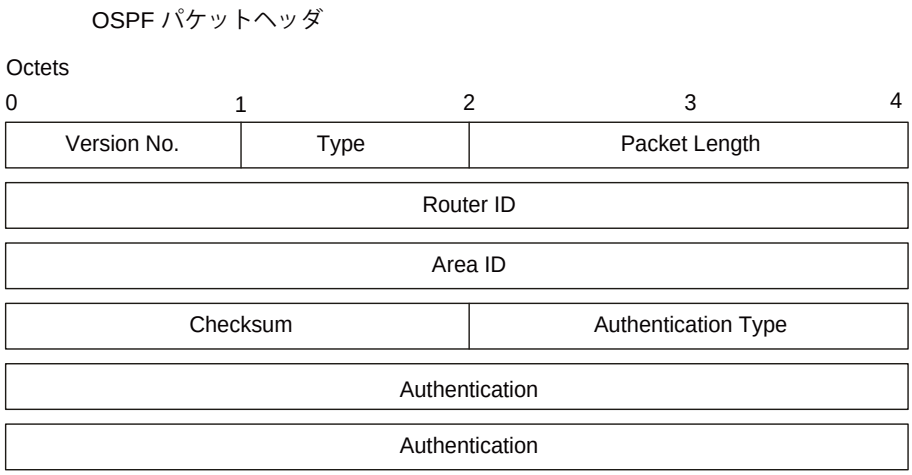


図 10-22 OSPF パケットヘッダフォーマット

項目	説明
Version No.	OSPF バージョン番号。
Type	OSPF パケットのタイプは以下の通りです。1 は Hello パケット、2 は Database Description パケット、3 は Link-State Request パケット、4 は Link-State Update パケット、5 は Link State Acknowledgement パケットを意味します。
Packet Length	パケット長（byte）。パケット長は 24 バイトのヘッダを含みます。
Router ID	パケット送信元のルータ ID。
Area ID	パケットが属するエリアが 32 ビットの番号を識別します。すべての OSPF パケットは 1 つのエリアに関連付けられています。仮想リンク上にパケットが送信される場合、バックボーンエリア ID は 0.0.0.0 です。
Checksum	標準の IP チェックサムに 64 ビットの認証欄以外のパケットの内容を含みます。
Authentication Type	パケットに使用する認証タイプ。
Authentication	認証スキームに使用される 64 ビットの項目。

Hello パケット

Hello パケットは、OSPF パケットのタイプ 1 として定義されています。この種類のパケットは、仮想リンクを含むすべてのインタフェース上で送信され、Neighbor ルータとの関係を構築し保持するために使用されます。さらに Hello パケットは、物理ネットワーク上でマルチキャストやブロードキャストが可能で、Neighbor ルータの動的な検出のために役立ちます。

ある共通のネットワークに接続するルータ間では、ネットワークマスク、Hello Interval、Router Dead Interval などの項目において一致した値を持つ必要があります。これらの項目は Hello パケット内に含まれ、これらの値が異なると、近接関係の構築が行われない仕組みになっています。

Hello パケットのフォーマットを以下に示します。

Hello パケット

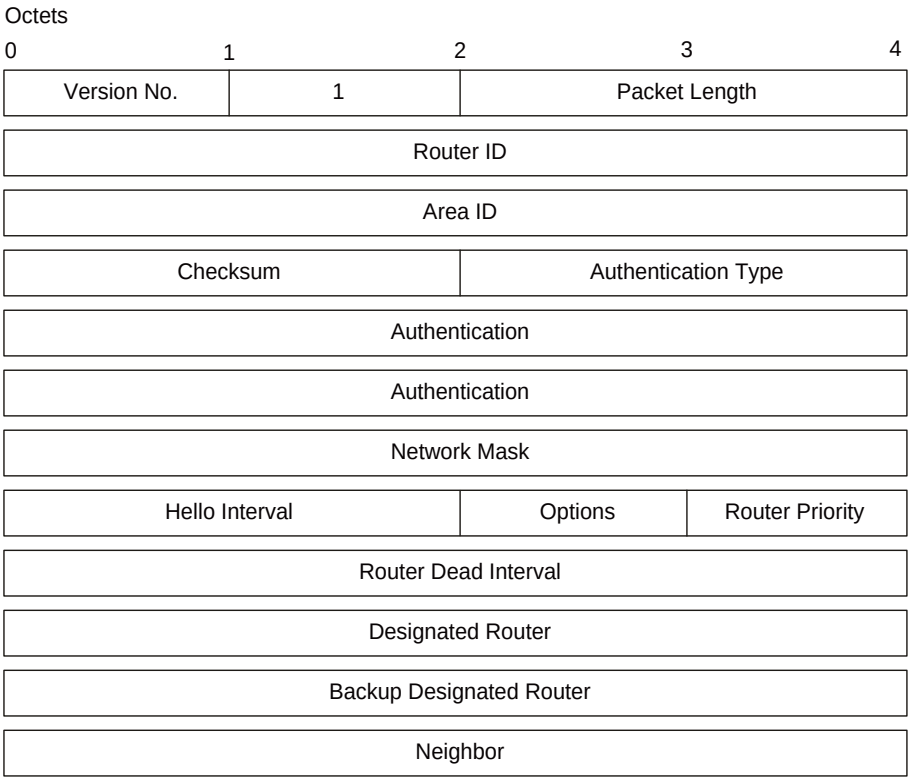


図 10-23　Hello パケット

項目	説明
Network Mask	パケットが送信されたインタフェースのネットワークマスク。
Options	ルータがサポートするオプションの機能。
Hello Interval	Hello パケットの送信間隔（秒）。
Router Priority	ルータプライオリティ。DR や BDR の選出に使用されます。本項目に 0 が設定されていれば、そのルータは DR や BDR には選出されません。
Router Dead Interval	ルータがダウンであると見なされるまでの時間（秒）。
Designated Router	マルチアクセスネットワーク上の DR のインタフェース IP アドレス。DR が選定されていなかったり、ポイントツーポイントネットワークであるなど DR/BDR の選定が行われない場合は、本欄は、0.0.0.0 という値がセットされます。
Backup Designated Router	マルチアクセスネットワーク上の BDR のインタフェース IP アドレス。BDR が選定されていなかったり、ポイントツーポイントネットワークであるなど DR/BDR の選定が行われない場合は、本欄は、0.0.0.0 という値がセットされます。
Neighbor	有効な Hello パケットを Router Dead Interval 時間内に送信したルータの Router ID。

Database Description パケット

Database Description パケットは、OSPF パケットタイプ 2 として定義されています。この種類のパケットは、隣接関係を確立中に交換されます。パケットにはトポロジデータベースの内容が記述されています。データベースの記述には複数のパケットが使用されます。パケットの送受信にはポール・レスポンスという方法を採用し、片方のルータをマスタ、もう片方をスレーブとします。マスタ側が Data description パケット（ポール）を送信し、スレーブ側が送信する Database description パケット（レスポンス）がこれを認識します。レスポンスとポールとは、パケット内のシーケンス番号によって関連付けされます。

Database Description パケットのフォーマットを以下に示します。

Database Description パケット

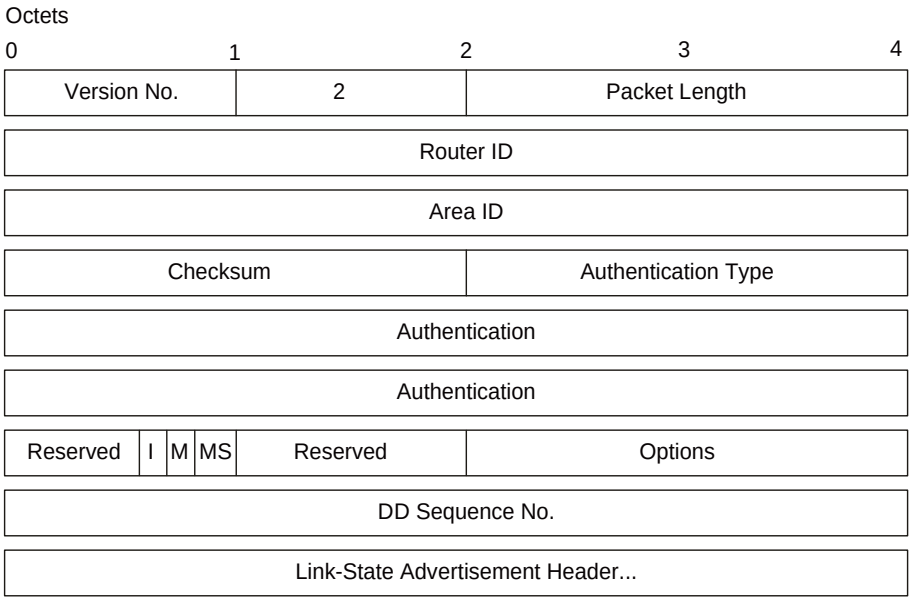


図 10-24 Database Description パケット

項目	説明
Options	ルータがサポートするオプション機能。
I – bit	Initial ビット。1 がセットされていれば、このパケットが一連の Database Description パケットの最初のパケットです。
M – bit	More ビット。1 がセットされていれば、このパケットの後に続きのパケットがあることを示しています。
MS – bit	マスタ・スレーブビット。1 がセットされていれば、データベース交換プロセス中、そのルータがマスタであることを示します。0 はスレーブです。
DD Sequence Number	Database Description パケットを順序付けるために使用します。1 番目のパケットの値（1 番目であることは I-bit で表示）は一意の番号で、それに続く番号は、一連のデータの最後のパケットが送信されるまで、増加していきます。

パケットの残りは、トポロジデータベースのリストで構成されます。データベース中の各 Link-State Advertisement は、Link-State Advertisement ヘッダに記述されます。

Link-State Request パケット

Link-State Request パケットは、OSPF パケットのタイプ 3 として定義されています。Neighbor ルータと Database Description パケットを交換することにより、ルータはトポロジデータベースの一部が最新のものでないことに気づく場合があります。Link-State Request パケットは、Neighbor ルータのデータベースの一部を最新のものにするよう要求する際に使用します。これには複数の Link-State Request パケットが必要になります。Link-State Request パケットの送信は隣接関係を築く上での最終段階です。

Link-State Request パケットを送信するパケットは、要求するデータベースの具体的な内容を、LS sequence number、LS checksum、LS age に定義します。しかし、それらの項目は Link-State Request パケット自体には明記されません。ルータは要求したものよりさらに新しいインスタンスをレスポンスとして受け取る場合もあります。
Link-State Request パケットのフォーマットを以下に示します。

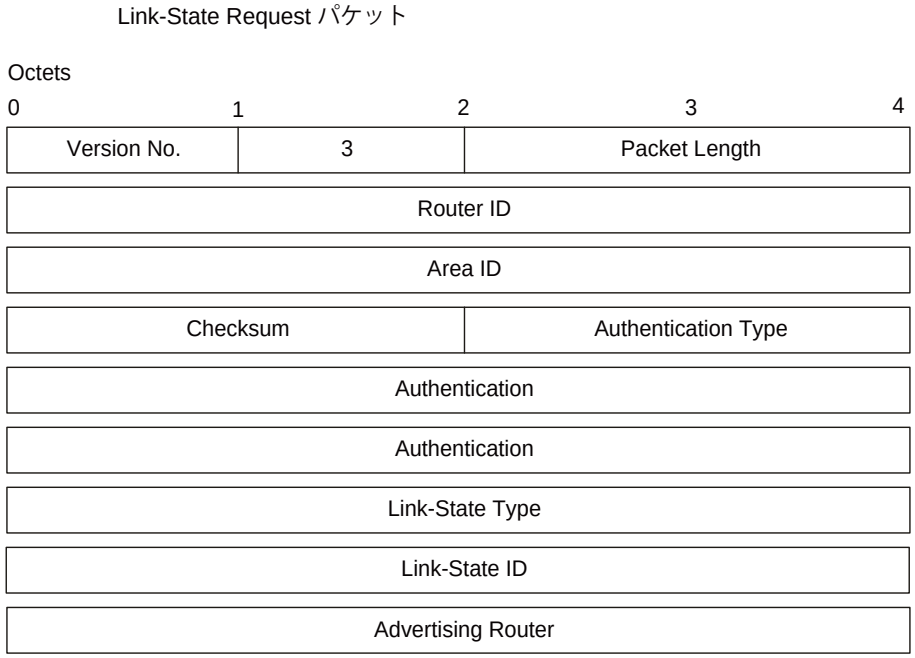


図 10-25 Link-State Request パケット

要求するアドバタイズメントは Link-State Type、Link-State ID、Advertising Router によって指定します。これによりアドバタイズメントが識別されますが、インスタンスの識別までは行いません。Link-State Request パケットは、最新のインスタンスの要求を行うものとして捉えられます。

Link-State Update パケット

Link-State Update パケットは、OSPF パケットのタイプ 4 として定義されています。このタイプのパケットにより Link-State Advertisement のフラッディングが実行されます。Link-State Update パケットは、Link-State Advertisement の集まりを、送信元から 1 ホップ先に運びます。1 つのパケットには、いくつかの Link-State Advertisement が含まれている場合があります。

Link-State Update パケットは、マルチキャスト / ブロードキャストをサポートするネットワーク上で、マルチキャストされます。フラッディングの確実性を高めるために、フラッディングされたアドバタイズメントには、Link-State Acknowledgement パケットを返します。アドバタイズメントの再送が必要な時は、ユニキャストの Link-State Update パケットが使用されます。

Link-State Update パケットのフォーマットを以下に示します。

Link-State Update パケット

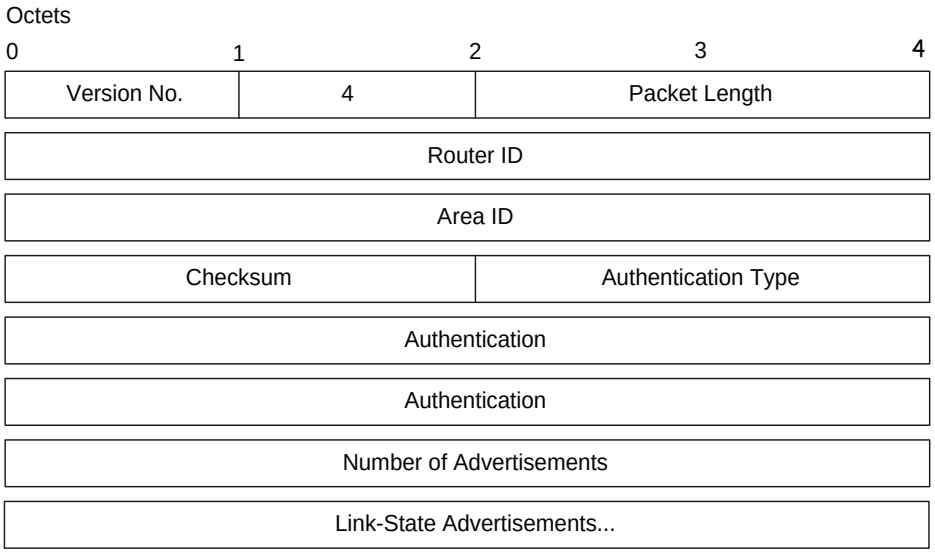


図 10-26　Link-State Update パケット

Link-State Update パケットのボディは、Link-State Advertisement のリストで構成されています。各 Advertisement、Link-State advertisement header という 20 バイトのヘッダで始まります。それ以外のアドバタイズメントのフォーマットは 5 つのタイプにより異なります。

Link-State Acknowledgment パケット

Link-State Acknowledgment パケットは、OSPF パケットのタイプ 5 として定義されます。Link-State Advertisement のフラッディングを確実にするために、フラッディングされたアドバタイズメントに明示的に応答を返します。この応答は Link-State Acknowledgment パケットの送受信により行います。複数の Link-State Advertisement に対して、1 つの Link-State Acknowledgment パケットで応答することも可能です。

送信するインタフェースの状態や、応答の対象となるアドバタイズメントの種類により、マルチキャストアドレス AllSPFRouters や AllDRouters 宛てに Link-State Acknowledgment パケットまたはユニキャストパケットとして送信されます。

本パケットのフォーマットは Data Description パケットと似ています。どちらのパケットのボディも Link-State Advertisement ヘッダのリストで構成されます。

Link-State Acknowledgment パケットのフォーマットは以下の通りです。

Link-State Acknowledgment パケット

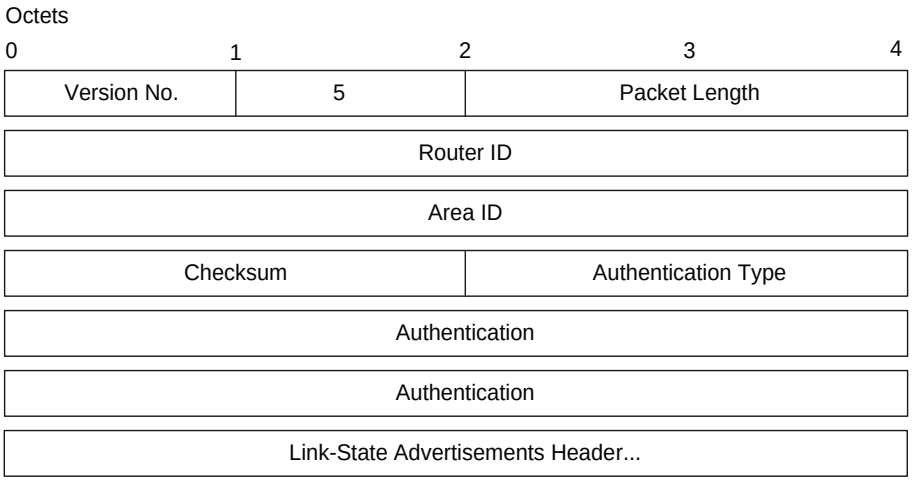


図 10-27　Link State Acknowledge パケット

応答する Link-State Advertisement は、それらのヘッダによって記述されます。ヘッダには、Link-State Advertisement と現在のインスタンスを識別するために必要な情報が組み込まれています。

Link-State Advertisement フォーマット

Link-State Advertisement には、5 つの異なるタイプが存在します。各 Link-State Advertisement は、20 バイトの Link-State Advertisement ヘッダで始まります。以下の項にそれぞれの Link-State Advertisement タイプの詳細を示します。

各 Link-State Advertisement には OSPF ルーティングドメインの一部が記述されます。すべてのルータは Router Links Advertisement を生成します。また、代表ルータとして選出された時、そのルータは Network Links Advertisement を生成します。Link-State Advertisement には他にも種類があります。確実性のあるフラッディングアルゴリズムにより、すべてのルータが同じ Link-State Advertisement の集合体を持つようになります。その Link-State Advertisement の集合体を Link-State データベース、またはトポロジデータベースと呼びます。

Link-State データベースを元に、各ルータは自分自身を根元とした最短パスツリーを構築します。

Link-State Advertisement には以下の 4 つの種類があり、いずれも共通の Link-State ヘッダを持ちます。

- Routers Link Advertisement
- Network Links Advertisements
- サマリリンク Advertisements
- 自律システム（AS）リンク Advertisements

Link-State Advertisement ヘッダ

すべての Link-State Advertisement は共通の 20 バイトヘッダで始まります。このヘッダの内容（Link State Type、Link State ID、Advertising Router）で Advertisement を十分識別できるようになっています。Link-State Advertisement のインスタンスがルーティングドメイン内に同時に複数存在する場合には、どのインスタンスが最新のものであるかを割り出す必要が出てきます。その割り出しは Link State Advertisement ヘッダ内に含まれる、Link Stage Age、Link State Sequence Number、Link State checksum フィールドを確認することにより実行できます。

Link State Advertisement ヘッダのフォーマットを以下に示します。

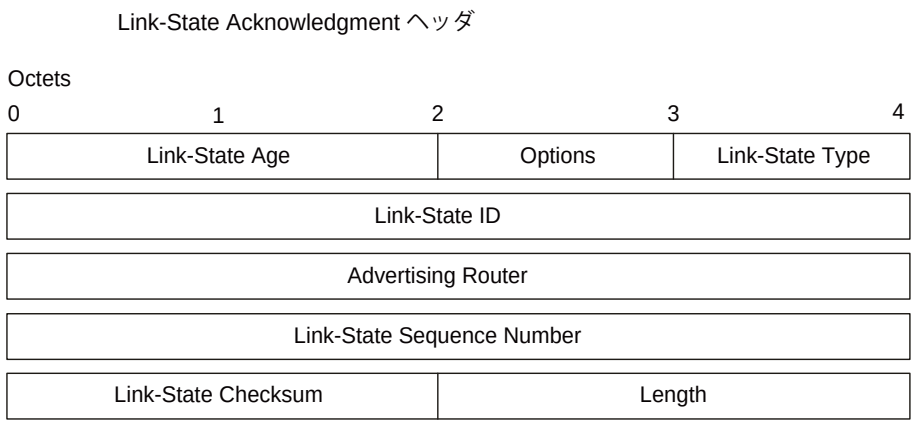


図 10-28　Link State Advertisement ヘッダ

項目	説明
Link-State Age	Link-State Advertisement が送信されてからの時間（秒）。
Options	該当ルーティングドメインでサポートするオプションの機能。
Link-State Type	Link-State Advertisement のタイプ。各タイプは異なるフォーマットを持ちます。以下のタイプが存在します。ルータリンク、ネットワークリンク、サマリリンク（IP ネットワーク）、サマリリンク（ASBR）、AS 外部リンク。
Link-State ID	同じ Link-State Type を使用している LSA 同士を区別するために使用されます。項目の内容は Link-State Type により異なります。
Advertising Router	Link-State Advertisement を送信したルータのルータ ID。例えば、Network Links Advertisement の場合であれば、本欄にはネットワークの代表ルータのルータ ID がセットされます。
Link-State Sequence Number	古い、または冗長な Link-State Advertisement を検出します。Link-State Advertisement の連続したインスタンスには、連続した Link-State Sequence Number が与えられます。
Link-State Checksum	Link-State Advertisement ヘッダを含む、Link-State Advertisement のデータ破損を検知するために使用します。Link-State Age 欄は計算されません。
Length	Link-State Advertisement のパケット長（バイト）。これは 20 バイトのヘッダを含みます。

Routers Links Advertisements

Routers Links Advertisement タイプ 1 の Link-State Advertisement です。エリア内の各ルータが Routers Links Advertisement を送信します。Advertisement には、ルータからエリアへのリンクの状態とコストが記述されます。あるエリアへのルータからのリンクはすべて、 1 つの Routers Links Advertisement に記述されます。

Routers Links Advertisement のフォーマットは以下の通りです。

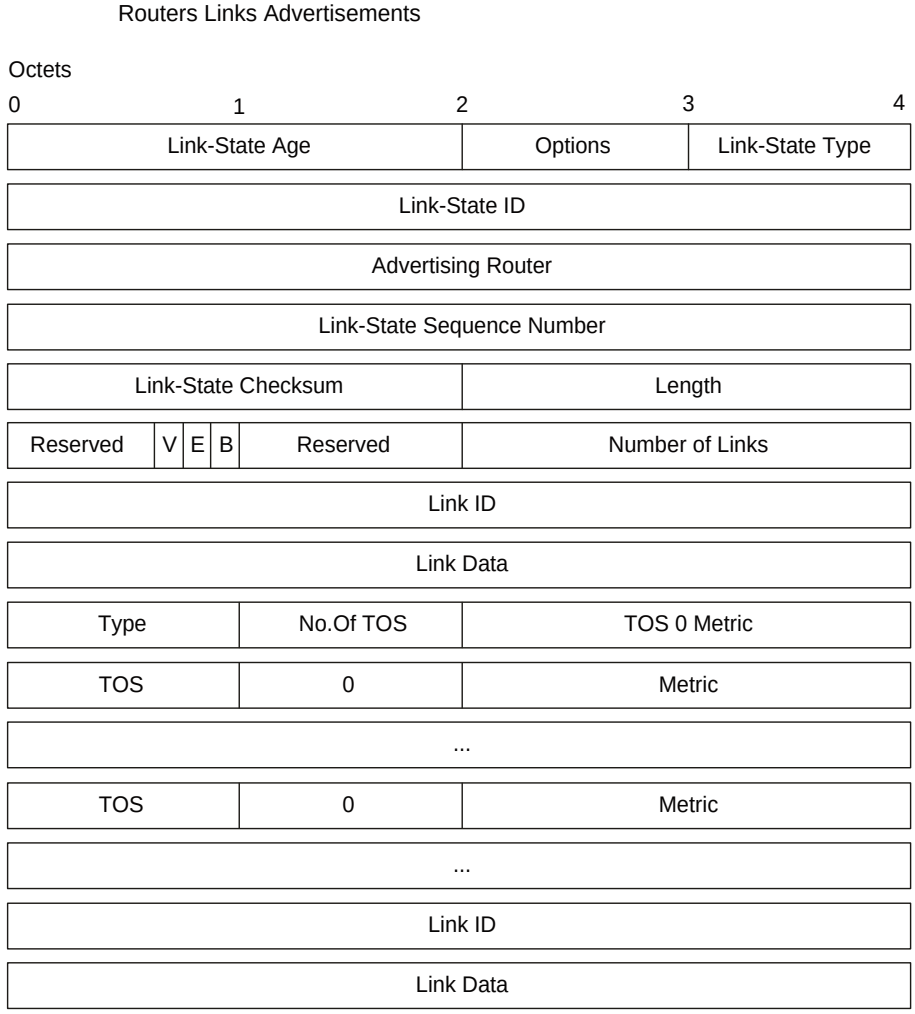


図 10-29　Routers Links Advertisement

Routers Links Advertisement では、Link-State ID 欄にルータの OSPF ルータ ID がセットされます。ルータが各 IP TOS に対してそれぞれ別のルートを算出することが可能である場合にのみ、Option 欄に T-bit がセットされます。Routers Links Advertisement は 1 つのエリアにのみフラッディングされます。

項目	説明
V-bit	セット（オン）される時、ルータはアクティブな仮想リンクのエンドポイントで、当該エリアをトランジットエリアとして使用していることを示します。（V : Virtual Link）
E-bit	セット（オン）される時、ルータは AS 境界ルータであることを示します。（E : External）
B-bit	セット（オン）される時、ルータはエリアボーダルータであることを示します。（B : Border）
Number of Links	ルータリンクの数。ルータから当該エリアへのリンク数の合計。

以下の項目は、各ルータリンク（インタフェース）を記述するために使用されます。ルータリンクはタイプ分けされています。Type フィールドは記述されているリンクの種類を示します。リンクには、トランジット（透過）ネットワークと接続するもの、他のルータと接続するもの、またはスタブネットワークと接続するものなどがあります。

ルータリンクについて記述する他のすべての値はリンクのタイプにより異なります。例えば、各リンクには 32 ビットのデータフィールドがあり、スタブネットワークへのリンクの場合、このフィールドにはネットワークの IP アドレスマスクが指定されます。他のリンクタイプの場合は、Link Data フィールドにはルータの IP インタフェースアドレスが指定されます。

項目	説明
Type	ルータリンクを迅速に分類します。以下の 1 つを選択します。: タイプの説明 : • 別のルータへの Point-to-Point 接続。 • トランジットネットワークへの接続。 • スタブネットワークへの接続。 • 仮想リンク。
Link ID	ルータリンクが接続する対象を識別します。値はリンクタイプにより異なります。Link-State Advertisement を送信する相手と接続している場合（他のルータやトランジットネットワークの場合）、本欄の値は隣接 Advertisement の Link-State ID と同じです。これらの値は Link-State データベース内で Advertisement を検索する際のキーとなります。リンクタイプにより、以下のどれかが設定されます。代表ルータの IP インタフェースアドレス。IP ネットワークアドレス。隣接ルータのルータ ID。
Link Data	本欄の値も Type フィールドの値により異なります。スタブネットワークへの接続の場合は、ネットワークの IP アドレスマスク。Point-to-Point（Unnumbered）の接続の場合は、MIB-II ifIndex の値。他のリンクタイプの場合は、ルータの IP インタフェースアドレスが記述されます。本情報はルーティングテーブル作成プロセス中のネクストホップの IP アドレスを計算する際に必要となります。
No. Of TOS	サービスタイプ（TOS）数。デフォルト TOS 以外のメトリックエントリ数。他に TOS メトリックがなければ、ここには 0 がセットされます。
TOS 0 Metric	デフォルトサービスタイプ（TOS = 0）のメトリック。

各リンクに、各サービスタイプ（TOS）についてのメトリックを指定します。TOS = 0 のメトリックは常に含まる必要があります。0 以外の TOS のメトリックはその後に記述されます。0 以外の TOS のコストが指定されていなければ､TOS 0 に指定されたコストがデフォルトとなります。メトリックは TOS の値の小さいものから順に並べる必要があります。例えば、TOS 16 のメトリックは TOS 8 のメトリックより後に記述されます。

項目	説明
TOS	本メトリックのサービスタイプ（TOS）。
Metric	指定した TOS のトラフィック用に本ルータリンクを使用する時のコスト。

Network Link Advertisements

Network Link Advertisements は、タイプ 2 の Link-State Advertisement です。Network Link Advertisements は、エリア内の各トランジットネットワーク宛てに送信されます。トランジットネットワークとは、複数のルータが接続するマルチアクセスネットワークを意味します。Network Link Advertisements には、代表ルータ自身を含むネットワークに接続するすべてのルータが記述されます。この Link-State ID フィールドには代表ルータの IP インタフェースアドレスが記述されます。

すべての TOS について、ネットワークから接続するすべてのルータへの距離は 0 とされます。このため、本タイプには TOS およびメトリックフィールドの記述は必要ありません。

Network Link Advertisements のフォーマットを以下に示します。

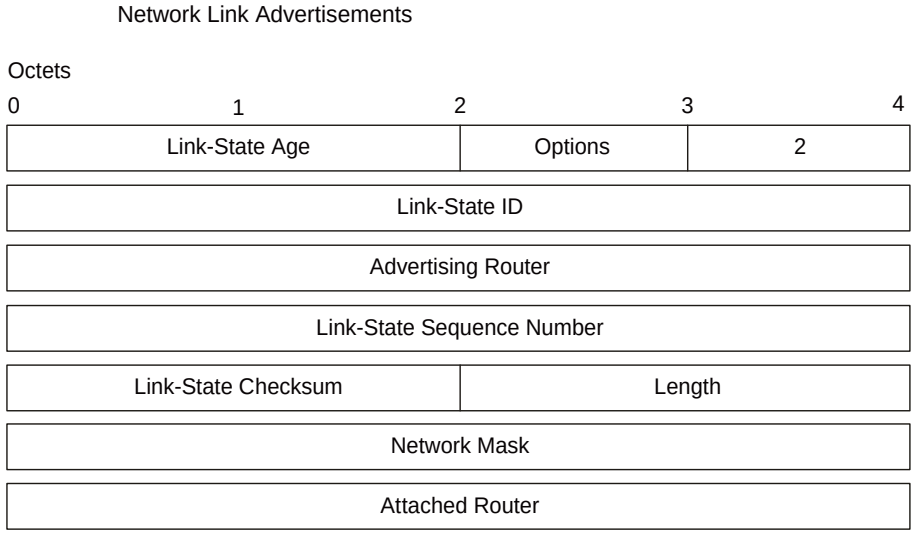


図 10-30　Network Links Advertisement

項目	説明
Network Mask	ネットワークの IP アドレスマスク。
Attached Router	ネットワークに接続する各ルータのルータ ID。代表ルータと完全に隣接関係であるルータが記述されます。代表ルータ自身も含まれます。

Summary Link Advertisements

Summary Link Advertisement は、タイプ 3 とタイプ 4 の Link-State Advertisements として定義されています。これらはエリアボーダルータによって生成されます。本 Advertisement は、（エリア外を含む）自律システムに属する宛先別に作成されます。

タイプ 3 の Link-State Advertisements は宛先が IP ネットワークである時に使用されます。この場合、Advertisement 中の Link-State ID フィールドには、IP ネットワークアドレスが記述されます。宛先が AS 境界ルータである場合には、タイプ 4 の Advertisement が使用されます。この場合、Advertisement 中の Link-State ID フィールドには、AS 境界ルータの OSPF ルータ ID が記述されます。タイプ 3 とタイプ 4 には、それ以外の違いはありません。

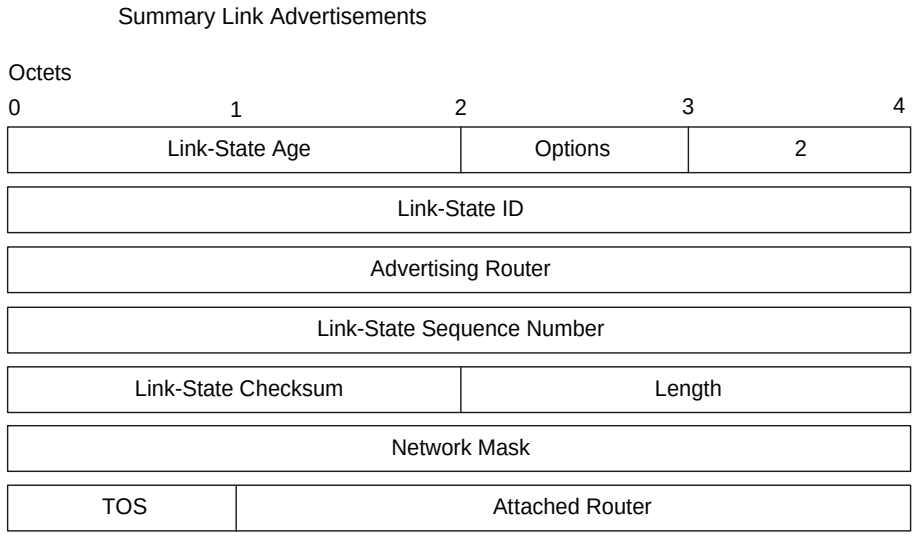


図 10-31　Summary Link Advertisements

スタブエリア向けにも、タイプ 3 の Summary Link Advertisements は使用され、エリアベースのデフォルトルートが記述されます。デフォルトサマリルートは、スタブエリア内ですべての外部ルートをフラッディングする代わりに使用されます。デフォルトサマリルートを記述する時、Link-State ID には、常にデフォルトの宛先 0.0.0.0 とネットワークマスク 0.0.0.0 がセットされます。

各 IP サービスタイプにはそれぞれのコストが通知されます。TOS 0 のコストは必ず含まれ、常に 1 番目に記述されます。Option 欄に T-bit がリセットされると、TOS 0 のルートのみが記述されることになります。そうでない場合、他の TOS 値のルートが併せて記述されます。ある TOS のコストが記述されないと、そのコストには TOS 0 に指定されるコストがデフォルトとして記述されます。

項目	説明
Network Mask	Type3 の場合の宛先ネットワークの IP アドレスマスク。例えば、クラス A ネットワークの場所を通知する場合、値は 0ff000000 となります。
TOS	以下のコストに関連付けるサービスタイプ。
Metric	本ルートのコスト。Routers Link Advertisement 中のインタフェースのコストと同様に表現されます。

Autonomous System External Link Advertisements

Autonomous System(AS) Link Advertisements は、タイプ 5 の Link-State Advertisement として定義されています。本タイプの Advertisement は AS 境界ルータ (ASBR) により、AS 外部の宛先ごとに生成されます。

AS External Link Advertisement は、通常特定の AS 外部の経路情報を含みます。この Advertisement の Link-State ID フィールドには IP ネットワークアドレスが記述されます。さらに、AS External Link Advertisement はデフォルトルートの記述にも使用されます。デフォルトルートは、宛先までのルートが存在しない時に使用されるルートです。デフォルトルートの記述が行われる時、Link-State ID には常にデフォルトの宛先アドレス 0.0.0.0 とネットワークマスク 0.0.0.0 がセットされます。

AS External Link Advertisements のフォーマットを以下に示します。

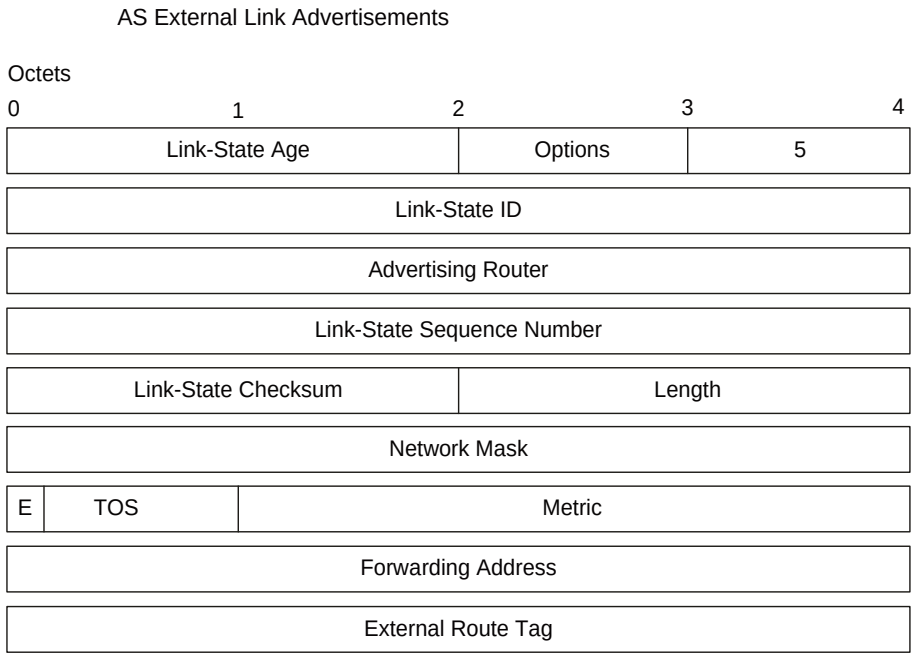


図 10-32　AS External Link Advertisements

項目	説明
Network Mask	宛先 IP アドレスマスク。
E - bit	外部メトリックタイプ。E-bit がセット（オン）されていれば、メトリックはタイプ 2 外部メトリックです。これはメトリックが Link-State パスの値よりも大きいことを表します。E-bit が 0 であれば、メトリックはタイプ 1 外部メトリックです。Link-State メトリックと同等であることを表します。
Forwarding Address	宛先へのデータを転送するアドレス。このアドレスが 0.0.0.0 の場合、デフォルトルートが示され 、データは通知元ルータに転送されます。
TOS	以下のコストに関連付けるサービスタイプ。
Metric	このルートのコスト。本メトリックの解釈は、上記の E-bit の状態に依存します。
External Route Tag	32 ビットの外部ルートタグは 、OSPF では実際には使われません。

NSSA について

NSSA（Not So Stubby Area）は AS（Autonomous Systems）からの外部経路が OSPF エリアにインポートできるように OSPF に追加された機能です。Stub エリアの拡張版である NSSA 機能は境界ルータ（BR）に使用されるパケット中継システムを使用して外部経路を OSPF エリアに中継します。以下の例を参照ください。

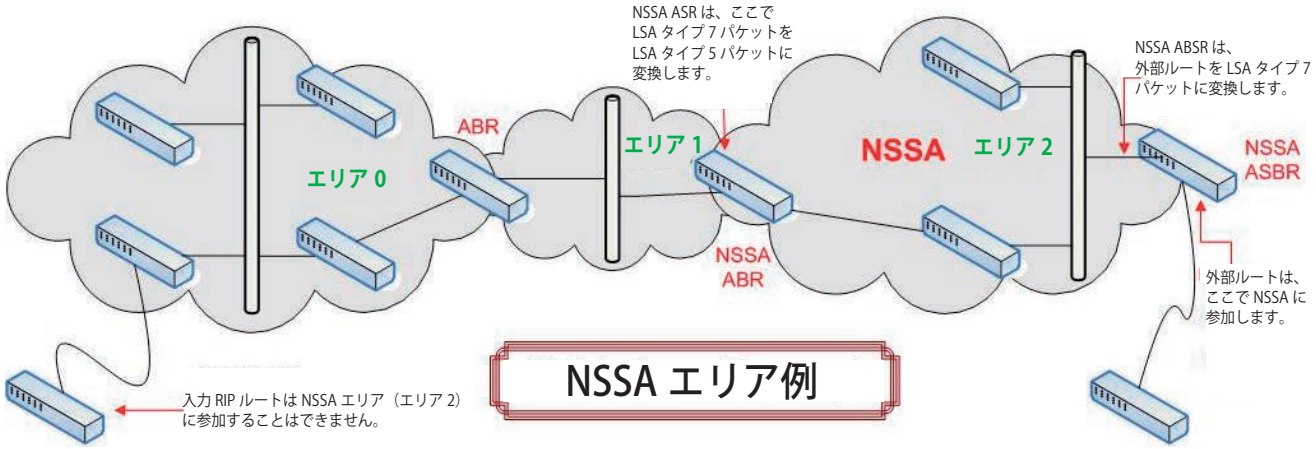


図 10-33　NSSA エリア例

NSSA ASBR（Not So Stubby Area Autonomous System Border Router）は外部経路情報を受信し、その情報を NSSA（上の例題のエリア 2）内にあるスイッチにだけ分配される LSA タイプ 7 パケットとして中継しています。この経路情報が他のエリアに入力されるためには、LSA タイプ 7 パケットは NSSA ABR（エリア境界ルータ）によって LSA タイプ 5 パケットに変換される必要があり、その後、他の OSPF エリア（上の例題のエリア 1 とエリア 2）内にある他のスイッチに配布されます。完了すると、新しい経路が学習され、新しい最短経路が決定されます。

新しい経路とパケットが原因で OSPF Summary ルーティングに発生する問題を緩和するためには、すべての NSSA エリア境界ルータ（ABR）が NSSA 内への LSA タイプ 3 Summary パケットをインポートするオプションをサポートする必要があります。

タイプ 7 LSA パケット

タイプ 7 LSA（Link-State Advertisement）パケットは NSSA に外部経路をインポートするために使用されます。これらのパケットは NSSA ASBR または NSSA ABR から生成され、LSA タイプ 7 パケットヘッダに P-Bit を設定することで定義されます。外部経路から学習した各到達点のネットワークはタイプ 7 パケットに変換されます。これらのパケットは NSSA スイッチを特定し、ABR によってタイプ 5 LSA パケットに変換されない限りこれらのパケット内に含まれる経路情報はエリアを出ることはできません。LSA タイプ 7 パケットのより優れた記述のために以下のテーブルを参照してください。

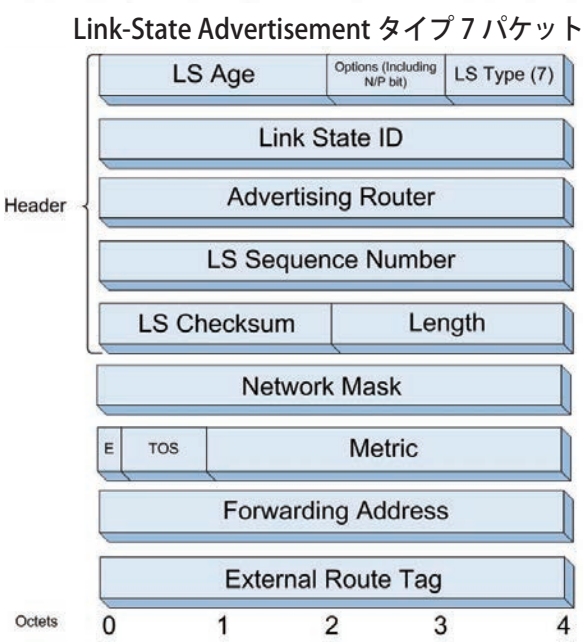


図 10-34 LSA タイプ 7 パケット

項目	説明
Link State Packet Header	本フィールドには次の情報があります。LS Checksum、L ength、LS Sequence Number、Advertising Router、Link State ID、LS Age、パケットタイプ、（タイプ 7）およびオプションフィールド。オプションフィールドにはこのセクションのもっと後で記述されている N-Bit に関する情報があります。
Network Mask	通知される到達点の IP アドレスマスク。
E - bit	外部メトリックのタイプ。E-bit が設定される場合、指定されるメトリックはタイプ 2 外部メトリックです。これはメトリックがどの Link-State 経路よりも大きいことを意味します。E-bit が 0 である場合、指定されるメトリックはタイプ 1 外部メトリックになります。これは Link-State メトリックに相当することを意味しています。通知される到達点へのデータトラフィックは、このアドレスに転送されます。
Forwarding Address	Forwarding Address に 0.0.0.0 が設定されると、データトラフィックは通知の生成者に転送されます。しかし、NSSA、ASBR および Adjacent AS 間のネットワークが内部の OSPF 経路としてエリアに通知されると、このアドレスはネクストホップアドレスとなります。反対にネットワークが内部経路として通知されないと、このフィールドはどんなルータのアクティブ OSPF インタフェースにもなります。
TOS	以下のコストに関連するサービスタイプ。
Metric	この経路のコスト。メトリックの解釈は外部メトリックタイプ（上記 E-bit）の記述によって異なります。
External Route Tag	各外部経路につけられる 32 ビットのフィールド。これは OSPF プロトコル自身に使用されません。

N-Bit

Link-State パケットヘッダのオプションフィールドに N-Bit が含まれる場合、N-Bit は NSSA のすべてのメンバがエリア設定に同意していることを保証するために使用されます。E-Bit に一致している場合に使用されると、これらの 2 つのビットは外部にフラッディングすることができます。タイプ 5 LSA は NSSA にフラッドされないため、E-Bit がクリアされている間 N-Bit には LSA タイプ 7 パケットを送受信するための情報があります。これらのパケットを 2 つのビット（N と E-Bit）の検証のために引き受ける機能に対し、追加のチェックが作成される必要があります。他のビットの組み合わせが破棄される間、特徴をチェックするというビットの照合が許可されます。

P-Bit

さらに LSA タイプ 7 パケットのオプションフィールドに P-Bit が含まれると、P-Bit（propagate）は NSSA の外にパケットを配布するために LSA タイプ 7 パケットを LSA タイプ 5 パケットに変換するかどうかを定義するために使用されます。

LSA タイプ 7 パケットの特長

- LSA タイプ 7 アドレスは IP アドレスとマスクから成るペアで定義されます。パケットは通知するかどうかを明らかにし、外部経路のタグも持っています。
- NSSA ASBR は外部経路を NSSA に配布されるタイプ 7 LSA に変換します。NSSA ABR はオプションでこのタイプ 7 パケットを他の OSPF エリア上に配布されるタイプ 5 パケットに変換します。これらのタイプ 5 パケットは他のタイプ 5 パケットとは識別できません。NSSA はタイプ 5 LSA をサポートしていません。
- NSSA の境界ルータ（BR）がタイプ 7 LSA をタイプ 5 LSA に変換することやグループ化することを終了すると、タイプ 5 LSA は他のタイプ 7 LSA の変換と収集のためにフラッシュまたはリセットされる必要があります。
- 一致する LSA アドレス範囲を除き、変換されたタイプ 5 LSA に含まれる転送アドレスが設定される必要があります。

OSPFv2（OSPFv2 設定）

OSPF Global Settings（OSPF グローバル設定）

OSPF 機能をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。

L3 Features > OSPF > OSPFv2 > OSPF 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。

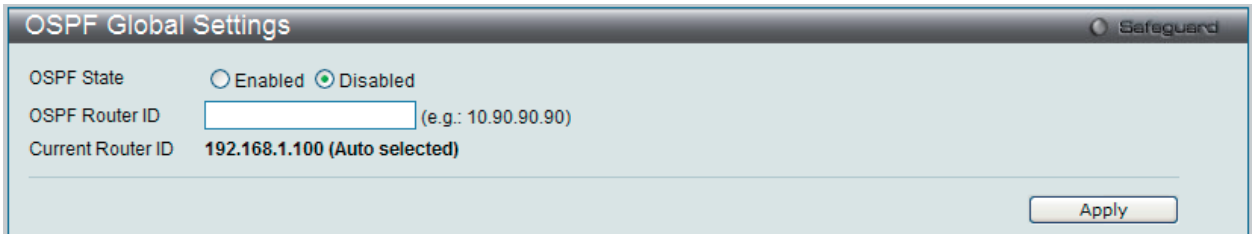


図 10-35　OSPF Global Settings 画面

以下の項目があります。

項目	説明
OSPF State	スイッチの OSPF 機能をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
OSPF Router ID	OSPF ドメイン中のスイッチを識別する 32 ビットの番号（IP アドレスと同じ xxx.xxx.xxx.xxx 形式）。スイッチ（ルータ）に割り当てられた中で最も大きい値の IP アドレスの使用が一般的です。
Current Router ID	スイッチで現在使用している OSPF Router ID が表示されます。この値はスイッチの OSPF Router ID を変更する際の参照用に表示されます。

「Apply」ボタンをクリックして行った変更を適用します。

OSPF Area Settings（OSPF エリア設定）

このスイッチに OSPF エリア設定を行います。OSPF は、隣接するネットワークとホストを集めてグループ化することができます。そのようなグループは含まれるネットワークのどれに対してもルータがインタフェースを持っていて、エリアと呼ばれます。

L3 Features > OSPF > OSPFv2 > OSPF 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。

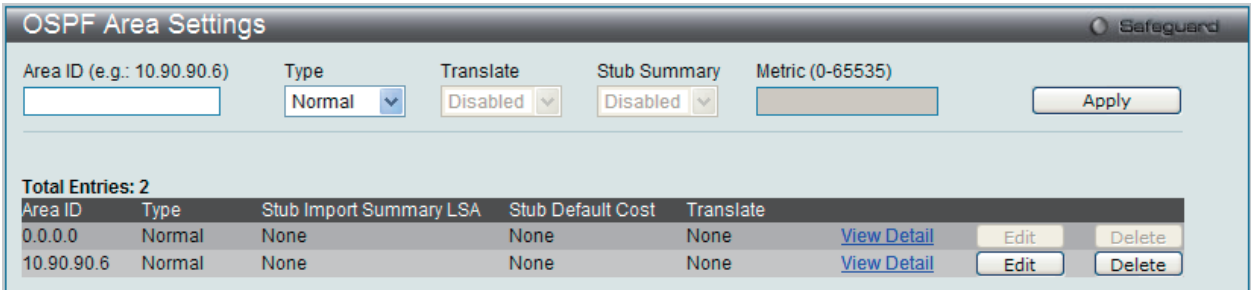


図 10-36 OSPF Area Settings 画面

以下の項目があります。

項目	説明
Area ID	OSPF ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) を指定します。
Type	プルダウンメニューを使用し「Normal」、「Stub」または「NSSA」から選択します。いくつかの AS では、トポロジのデータベースの大部分が AS external Advertisements からなっているかもしれません。OSPF AS External Advertisement は、通常 AS 全体にフラッドされます。しかし、OSPF は特定のエリアを「Stub エリア」として設定できます。AS External Advertisement は Stub エリア内または Stub エリアを通じてフラッドされません。これらの AS の外部送信先へのルーティングは（エリアごとに）デフォルトにだけ基づいています。これは、Stub エリアの内部ルータのためにトポロジデータベースのサイズを減少させるため、メモリの必要量も減少します。
Translate	プルダウンメニューでタイプ 7 LSAs を NSSA の外に配布するためにタイプ 5 LSAs に変換することを有効または無効にします。初期値は「Disabled」です。本欄は「NSSA」が Type フィールドで選択された場合にだけ設定できます。
Stub Summary	Summary Link-State Advertisement(Summary LSA) が他のエリアからエリア内にインポートされることを選択エリアが許可するかどうかを表示します。
Metric	このエリアのメトリック（1-65535、0 は自動コスト）を入力します。本欄は NSSA エリアに入力するトラフィックのコストを決定します。

「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、以下の画面を表示します。

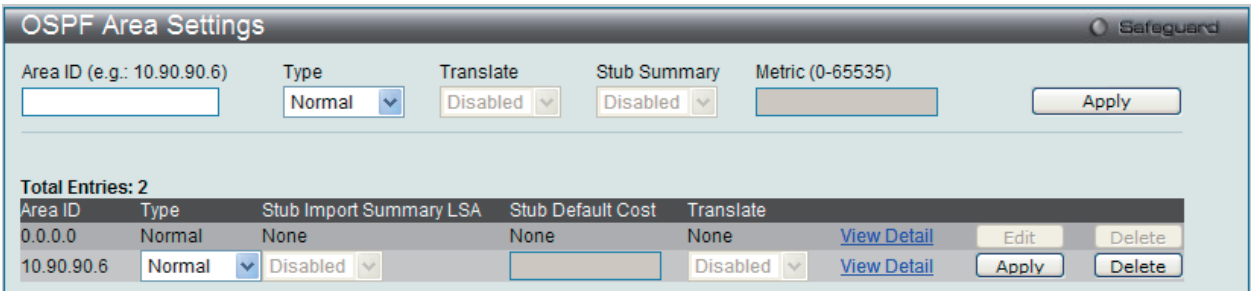


図 10-37 OSPF Area Settings 画面 - Edit

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。

OSPF エリア設定の表示

「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。

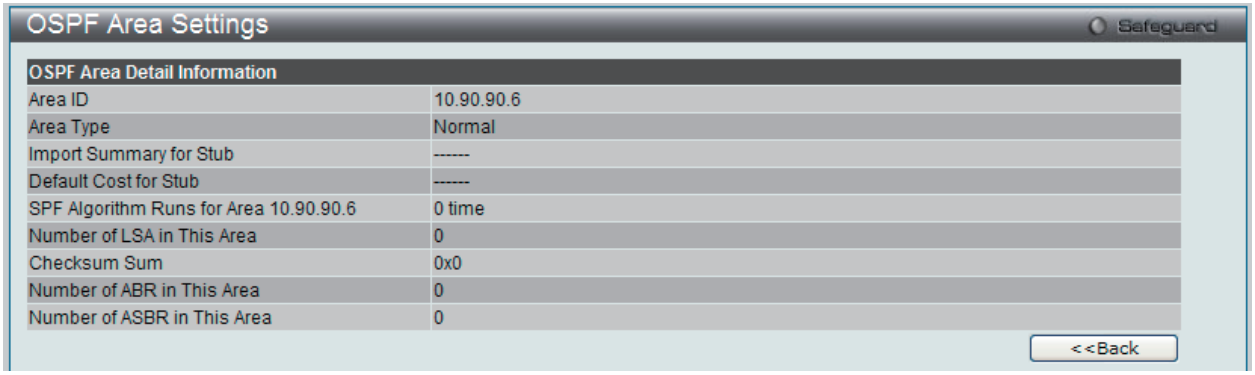


図 10-38 OSPF Area Settings 画面

「<<Back」をボタンをクリックして前のページに戻ります。

OSPF Interface Settings（OSPF インタフェース設定）

このスイッチの OSPF インタフェースを設定します。

L3 Features > OSPF > OSPFv2 > OSPF 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。

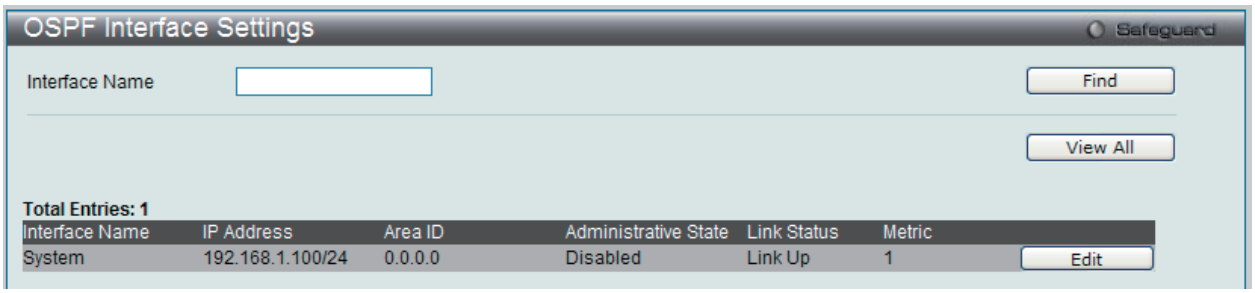


図 10-39 OSPF Interface Settings 画面

以下の項目があります。

項目	説明
Interface Name	IP インタフェース名を入力します。

「Find」ボタンをクリックして、入力したインタフェースを検出します。

「View All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

エントリの編集

「Edit」ボタンをクリックすると、以下の画面が表示されます。

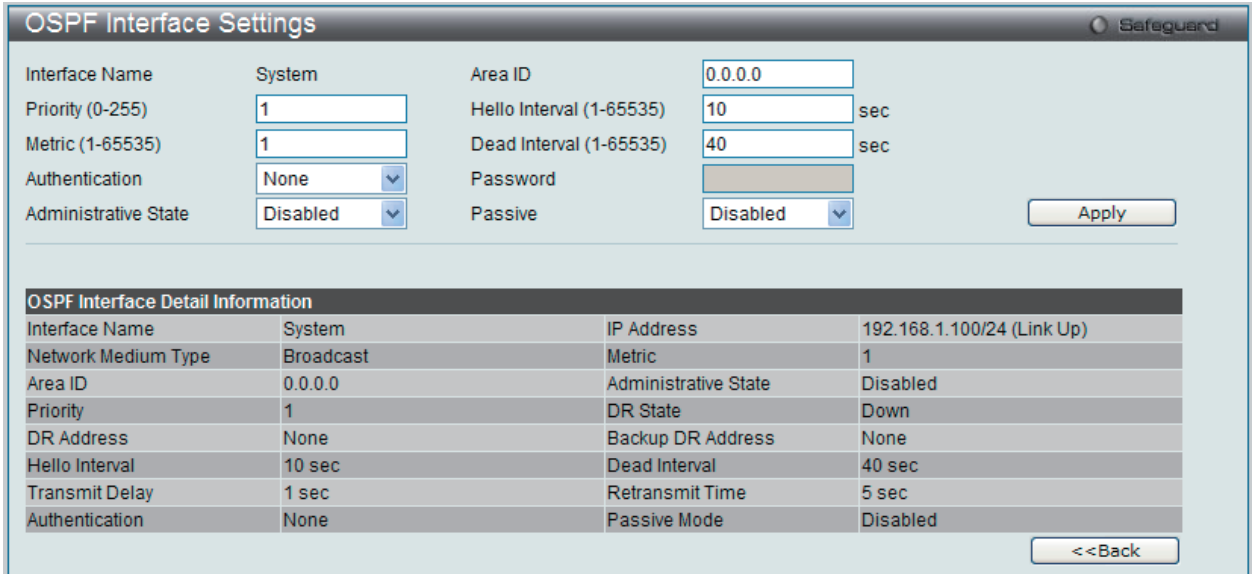


図 10-40 OSPF Interface Settings – Edit 画面

以下の項目があります。

項目	説明
Interface Name	IP インフェース名を表示します。
Priority	代表ルータ選出のプライオリティを指定します。ルータプライオリティ 0 が指定されると、スイッチはそのネットワークの代表ルータとして選出されなくなります。
Metric (1-65535)	指定 OSPF インタフェースに到達する際の OSPF コストを指定します。初期値は 1 です。
Authentication	OSPF ルーティングドメインでの OSPF パケットの送受信時における認証方法を設定します。 • None - 認証を行いません。 • Simple - パケットが認証済みルータからのものであるかを判断するためにシンプルパスワードを使用します。本モードを選択した場合、「Password/ Auth. Key ID」フィールドに 8 文字までのパスワードを指定します。指定するパスワードは隣接 OSPF ルータの設定と同じものである必要があります。 • MD5 -「MD5 Key Table Configuration」メニューで登録された暗号キーを使用します。本モードを選択した場合、「Key ID」欄に、登録済みのキーの中から 1 つを入力します。この値も隣接ルータと同じものである必要があります。
Administrative State	管理状態を有効または無効にします。
Area ID	インタフェースが割り当てられるエリアを指定します。エリア ID は、OSPF ドメイン内の OSPF エリアをユニークに識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) です。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔（秒）。同一ネットワークのルータには同じ「Hello Interval」、「Dead Interval」、「Authorization Type」、「Authorization Key」が設定される必要があります。
Dead Interval (1-65535)	隣接ルータが Hello パケットを最後に受信してから、送信側のルータがダウンしたと判断するまでの時間（秒）。本値には Hello Interval の倍数を指定します。
Key ID	シンプルパスワードまたは MD5 暗号キーを入力します。
Passive	この OSPF インタフェースに対して Active または Passive モードを指定します。Active インタフェースは指定した OSPF グループの属さない他のイントラネット上のルータにも積極的に通知します。Passive インタフェースは OSPF イントラネット以外のルータには通知しません。本フィールドが「Disabled」の場合は Active インタフェース、「Enabled」の場合は Passive モードとなります。

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」をボタンをクリックして前のページに戻ります。

OSPF Virtual Link Settings（OSPF 仮想リンク設定）

このスイッチに OSPF 仮想インタフェースを設定します。

L3 Features > OSPF > OSPFv2 > OSPF Virtual Link 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。

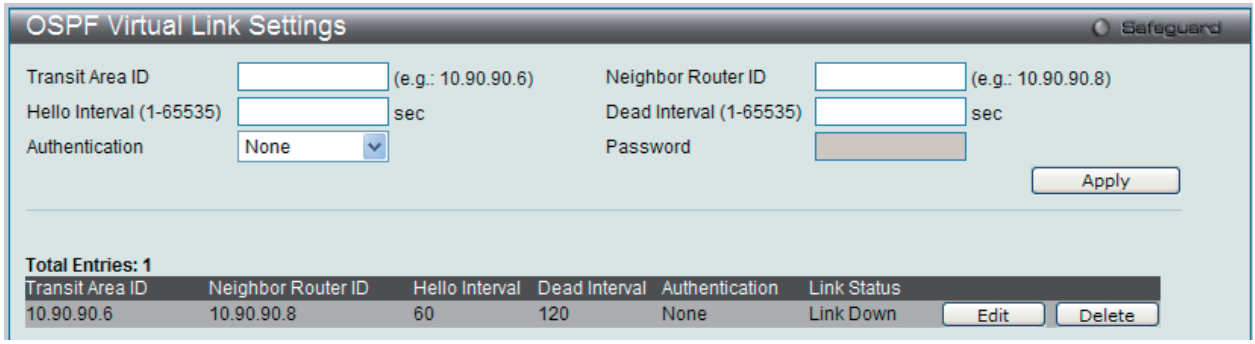


図 10-41　OSPF Virtual Link Settings 画面

エントリの編集

「Edit」ボタンをクリックすると、以下の画面が表示されます。

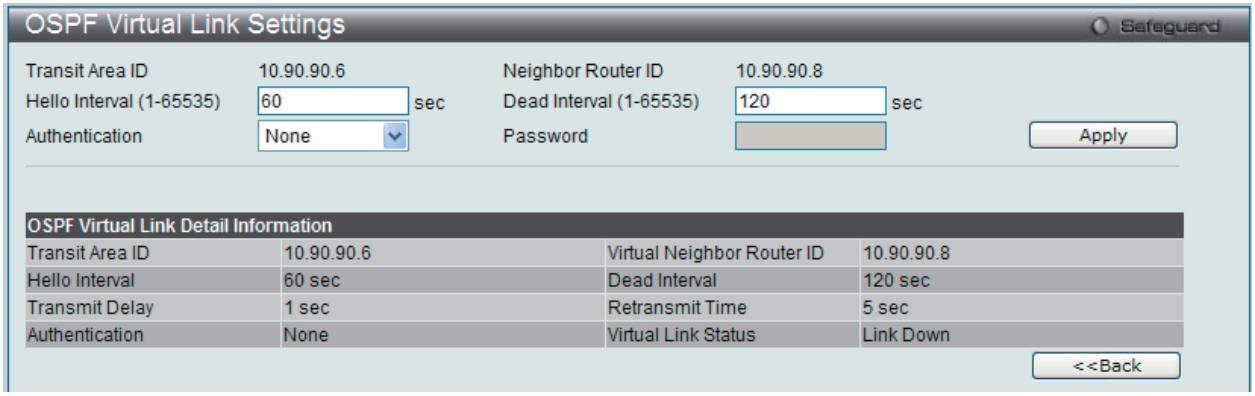


図 10-42　OSPF Virtual Link Settings 画面 - Edit

OSPF 仮想インタフェースの登録や変更は、以下の項目を使用して行います。

項目	説明
Transit Area ID	OSPF ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) を指定します。
Neighbor Router ID	リモートエリアの OSPF ルータ ID。リモートエリアの Area Border Router(エリア境界ルータ) を識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) を指定します。これは Neighbor ルータのルータ ID です。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔（秒）。同一ネットワークのルータには同じ「Hello Interval」、「Dead Interval」、「Authorization Type」、「Authorization Key」が設定される必要があります。
Dead Interval (1-65535)	隣接ルータが Hello パケットを最後に受信してから、送信側のルータがダウンしたと判断するまでの時間（秒）。本値には Hello Interval の倍数を指定します。1 から 65535（秒）で指定します。ネットワークのすべてのルータで共通である必要があります。
Authentication	使用する認証を選択します。「None」、「Simple」または「MD5」を選択します。「Simple」認証を選択するとパスワードの入力が必要です。「MD5」認証を選択すると KEY ID の入力が必要です。
Password/ Auth. Key ID	シンプルパスワード（大文字、小文字の区別あり）または「MD5 Key Settings」メニューで登録した MD5 キーを入力します。
Transmit Delay	この仮想リンクに Link-State Update パケットを転送するために要する遅延時間（秒）。ここで設定した値が、LSA の Age に加算されます。本フィールドの値は 1（秒）に固定されています。
Retransmit Interval	本仮想リンクに属する隣接ルータ（Adjacency）に対する Link-State Advertisement の再送信間隔（秒）。本フィールドの値は 5（秒）に固定されています。Transit delay は Account transmission と Propagation delay を含みます。

OSPF Area Aggregation Settings（OSPF エリア集約設定）

このスイッチに OSPF エリア集約設定を行います。

L3 Features > OSPF > OSPFv2 > OSPF Area Aggregation 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。

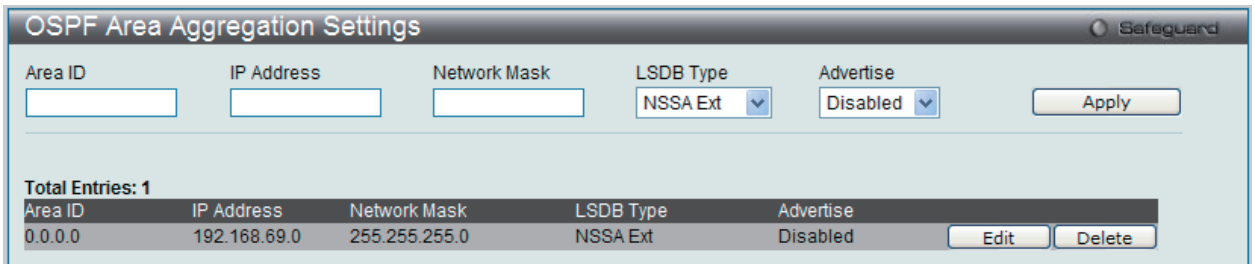


図 10-43　OSPF Area Aggregation Settings 画面

OSPF エリア集約の設定は、以下の項目を使用して行います。

項目	説明
Area ID	OSPF ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) を指定します。
IP Address	OSPF エリアに対応するネットワークを識別する IP アドレス。
Network Mask	OSPF エリアに対応するネットワークを識別するネットマスク。
LSDB Type	アドレス集約のタイプ。「NSSA Ext」または「Summary」を選択します。
Advertise	選択した OSPF エリアが自身のサマリ LSDB を通知すること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。

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、以下の画面を表示します。

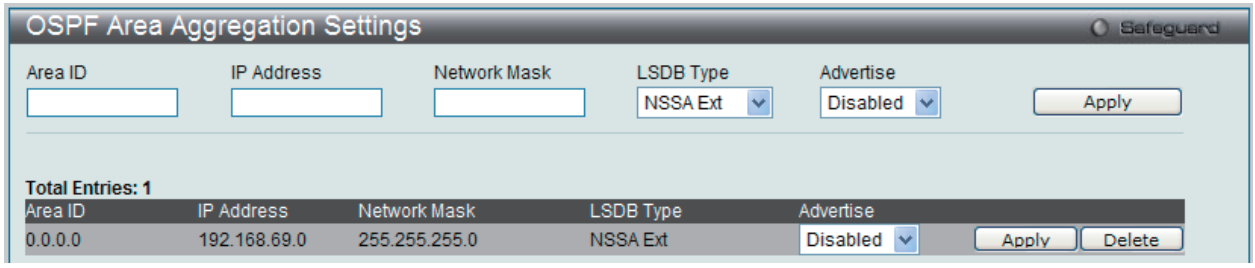


図 10-44 OSPF Area Aggregation Settings 画面 - Edit

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。

OSPF Host Router Settings（OSPF ホストルータ設定）

OSPF ホスト経路設定を行います。

L3 Features > OSPF > OSPFv2 > OSPF Host 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。

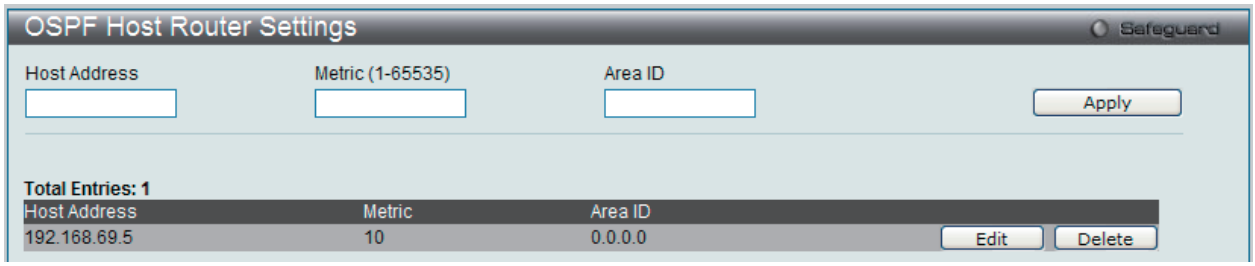


図 10-45 OSPF Host Route Settings 画面

以下のフィールドを使用して OSPF ホストルートの設定を行います。

項目	説明
Host Address	使用するホストの IP アドレス。
Metric	通知されるメトリック (1-65535)。
Area ID	OSPF ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) を指定します。

「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、以下の画面を表示します。

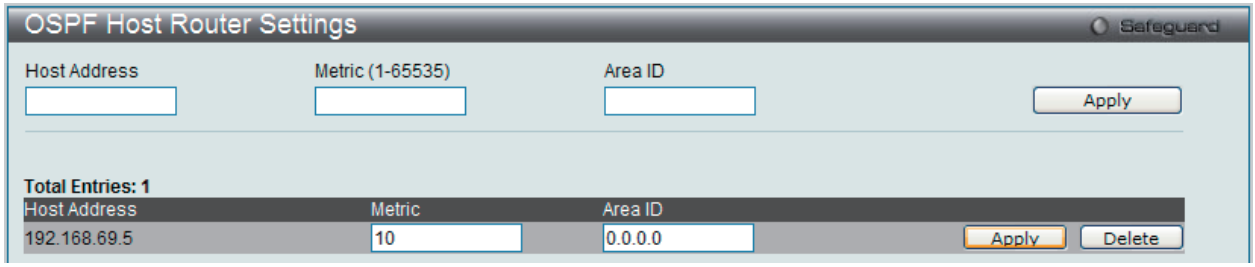


図 10-46 OSPF Host Route Settings 画面 - Edit

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。

OSPF Default Information Originate Settings（OSPF デフォルト情報オリジネート設定）

生成する OSPF デフォルト外部ルートの状態を変更します。

L3 Features > OSPF > OSPFv2 > OSPF Default Information Originate 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。

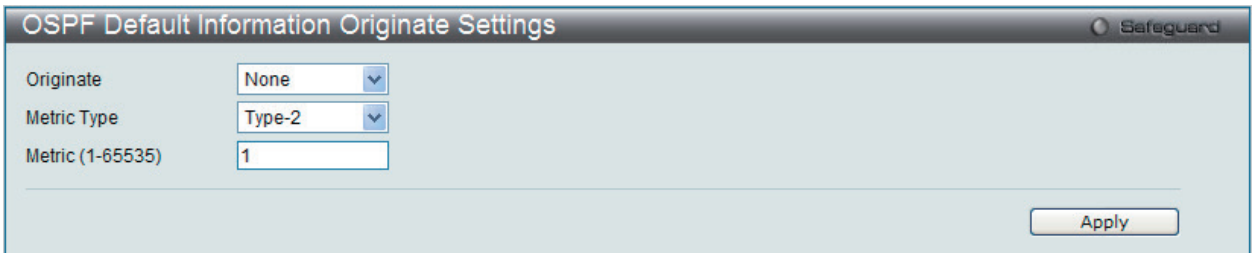


図 10-47　OSPF Default Information Originate Settings 画面

以下の項目を使用します。

項目	説明
Originate	生成するデフォルト情報の状態を選択します。 • Default - 1 つのデフォルトルートが既に存在する時だけ、外部デフォルトルートが生成されます。 • Always - デフォルトルートの存在の有無に関係なく、外部デフォルトルートが生成されます。 • None - 外部デフォルトルートは生成されません。（初期値）
Metric Type	OSPF にインポートされたデフォルト外部ルートを含む LSA のタイプを選択します。 • Type-1 -「metric」欄に入力したメトリックに対してインタフェースコストを追加することでメトリックを使用した本デフォルト外部ルートの算出が行われます。 • Type-2 -「metric」に入力したメトリックを変更しないで使用することで本デフォルト外部ルートの算出が行われます。（初期値）
Metric	生成するデフォルト外部ルートが使用するメトリック値を入力します。この値は 1-65535 とする必要があります。

「Apply」ボタンをクリックして行った変更を適用します。

OSPF LSDB Table（OSPF LSDB テーブル）

OSPF Link State Database(LSDB) を表示します。

L3 Features > OSPF > OSPFv2 > OSPF 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。

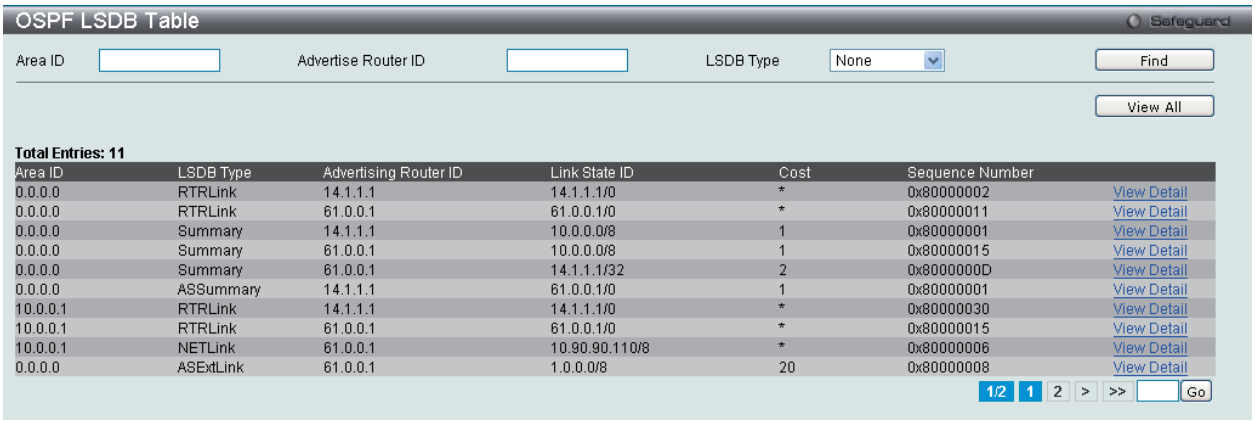


図 10-48　OSPF Global Settings 画面

以下の項目を使用します。

項目	説明
Area ID	OSPF ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) を指定します。
Advertise Router ID	Advertising ルータのルータ ID を入力します。
LSDB Type	表示する LSDB タイプを指定します。「RTRLink」、「NETLink」、「Summary」、「ASSummary」、「ASExtLink」、「NSSA Ext」または「Stub」を選択します。

「Find」ボタンをクリックして、指定したエントリを検索します。
「View All」ボタンをクリックして、すべての OSPF Link-State データベースエントリを表示します。
「View Detail」リンクをクリックすると、指定エントリの OSPF LSDB の詳細を表示します。

OSPF LSDB の詳細表示

「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。

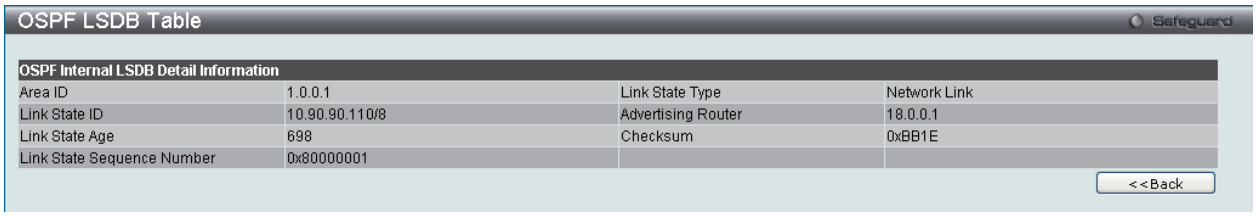


図 10-49 OSPF LSDB Table 画面（View Detail）

「<<Back」をボタンをクリックして前のページに戻ります。

OSPF Neighbor Table（OSPF Neighbor テーブル）

インタフェースごとに OSPF-Neighbor 情報を表示します。

L3 Features > OSPF > OSPFv2 > OSPF Neighbor 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。

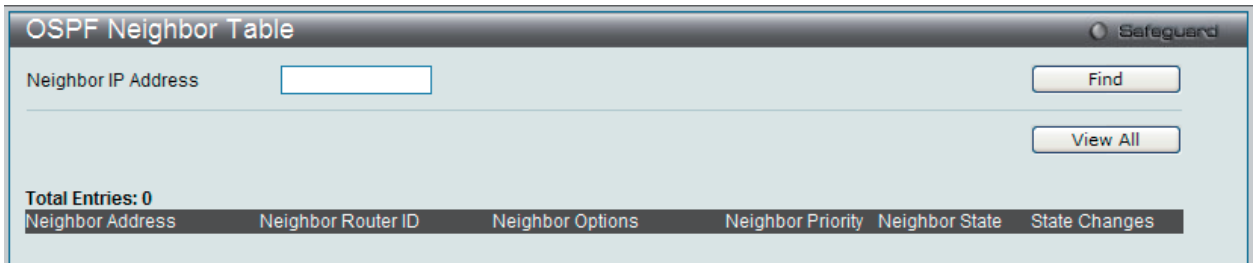


図 10-50 OSPF Neighbor Table 画面

以下の項目を使用します。

項目	説明
Neighbor IP Address	Neighbor ルータの IP アドレスを入力します。

「Find」ボタンをクリックして、指定したエントリを検索します。

「View All」ボタンをクリックして、すべてのエントリを表示します。

OSPF Virtual Neighbor Table（OSPF Virtual Neighbor テーブル）

OSPF 仮想リンクの OSPF-Neighbor 情報を表示します。

L3 Features > OSPF > OSPFv2 > OSPF Neighbor 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。

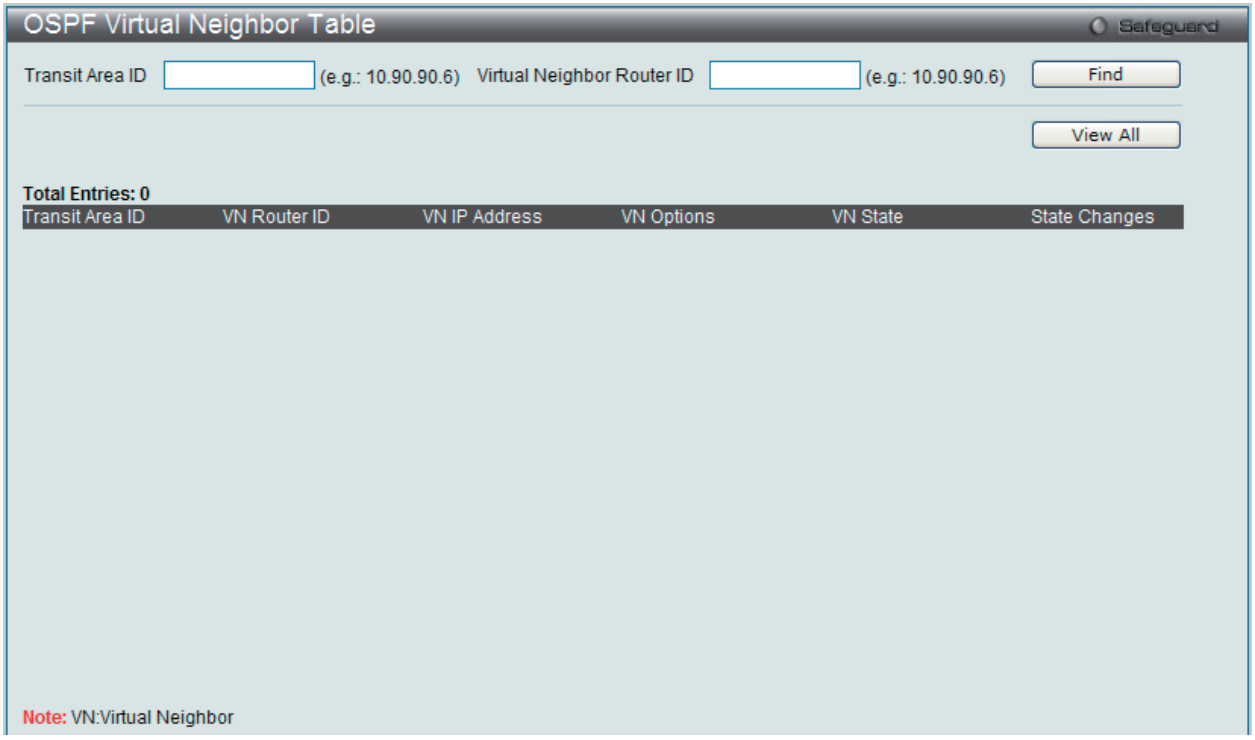


図 10-51　OSPF Virtual Neighbor Table 画面

以下の項目を使用します。

項目	説明
Transit Area ID	OSPF ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) を指定します。
Virtual Neighbor Router ID	リモートエリアの OSPF ルータ ID。リモートエリアの Area Border Router(エリア境界ルータ) を識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) を指定します。

「Find」ボタンをクリックして、指定したエントリを検索します。
「View All」ボタンをクリックして、すべてのエントリを表示します。

RIP（RIP 設定）

RIP（Routing Information Protocol）は、距離ベクトル型のルーティングプロトコルです。RIP を使用するデバイスには、RIP アクティブが稼動しているものと RIP パッシブが稼動しているものの 2 種類があります。RIP アクティブのデバイスは、RIP メッセージを使用して他のデバイスに対してルートの通知（Advertise）を行います。一方、パッシブのデバイスはこれらのメッセージをリッスンするだけです。アクティブデバイスが送信する RIP メッセージに基づき、アクティブ、パッシブ両方のルーティングテーブルが更新されます。アクティブ側になることができるのはルータだけです。

RIP を使用するルータは、30 秒ごとにネットワークアドレスと距離情報（通知ルータとリモートネットワークの間のルータの数（ホップ）で表現）を含むルーティングアップデートをブロードキャストします。

RIP では、距離を 1 つのネットワークから他のネットワークへのホップ数（整数）で計ります。直接接続されるネットワークに接続するルータを 1 ホップ、そのルータを経由して到達する次のルータが 2 ホップと数えられます。送信元から宛先の間のルータの数が増えるほど、RIP での距離（またはホップカウント）は大きくなります。

ネットワークのパフォーマンスと安定性を高めるために使用されるルーティングテーブルの更新プロセスには、いくつかのルールがあります。ルータは新しいルートを学習した際、そのルートと同じホップカウント（コスト）のルートが既にテーブル内にあれば、更新を行いません。つまり、学習されたルートは、小さいホップカウントを持つルートが学習されるまで保持されます。

学習されたルートがルーティングテーブルに組み込まれる時、タイマが始動します。このタイマは、そのルートが通知される度に、再始動します。もし、ルートが一定期間（通常は 180 秒）通知されなければ、そのルートはルーティングテーブルから削除されます。

RIP は、ループ検出を行うための明示的な方法を持ちません。しかし、ルータが権限のないルータから間違ったルートを学習するのを防ぐための認証メカニズムを多く使用しています。

安定性を高めるため、RIP が使用するホップカウントには、低い値の最大値が設けられています。16 ホップは無限大（ネットワーク到達不可能）として定義されています。言い換えると、ローカルルータは、送信元から 16 ルータ以上離れたネットワークへは、到達不可能であると見なすということです。

RIP メッセージのネットワークでの伝播が比較的遅いため、RIP は収束（矛盾、到達不可能、またはループ状態のルートをルーティングテーブルから削除する）に時間がかかると指摘されています。

収束に時間がかかるという問題については、スプリットホライズンによって解決を図っています。スプリットホライズンは、あるルートを通知する際に、そのルートを学習したインタフェースからは通知しないという原則で成り立ちます。これにより一時的なルーティングループの発生を抑えることができます。

ホールドダウンという方法を使用して、ルータが新しいルートアップデートを受信後、新規のルートアップデートをある期間（通常は 60 秒）無視するようにすることもできます。これにより、ネットワーク上のすべてのルータがアップデートメッセージを受信できるようになります。

ルータは、「ポイズンリバース」という手法により、ルートの通知に無限大のホップカウント（16）を付加します。この方法は通常トリガーアップデートと組み合わせて使用され、到達不可のネットワークのアップデートメッセージを受信すると、ルータは直ちにブロードキャストを行うようにします。

RIP バージョン 1 メッセージフォーマット

RIP メッセージには、Routing information message と Information request の 2 種類があります。どちらも同じ形式を使用しています。

コマンドフィールドには、以下の表に示すオペレーションが指定されます。

コマンド	意味
1	一部またはすべてのルーティング情報のリクエスト
2	送信元のルーティングテーブルからのネットワークと距離の情報を含むレスポンス
3	トレースモードオン（サポートなし）
4	トレースモードオフ（サポートなし）
5	Sun Microsystems 専用領域
9	アップデート・リクエスト
10	アップデート・レスポンス
11	アップデート・アクノリッジメント（確認）

RIP コマンドコード

「Version」フィールドには、プロトコルのバージョン（ここでは 1）が格納され、パケットの受信者は RIP のどのバージョンのパケットが送信されたかを知ることができます。

RIP1 メッセージ

RIP は、TCP/IP のみに限定されるわけではありません。RIP では、宛先ネットワークアドレスとして 14 オクテットまでのフィールドが確保されています（IP 使用の場合は、残りの 10 オクテットはゼロ）。他のネットワークプロトコルスイートはアドレスファミリ識別子フィールドに指定されます（IP の値は 2）。これにより、アドレスフィールドの解釈の仕方が決定されます。

RIP では、IP アドレス 0.0.0.0 がデフォルトルートとして指定されています。
ルータのホップ数で測る距離は、「Distance to Source Network」および「Distance to Destination Network」フィールドに格納されます。

RIP1 ルートの解釈

RIP は、クラス分けされるアドレスに使用されるように設計され、明示的なサブネットマスクは使用されません。バージョン 1 の拡張機能では、ルータがサブネットアドレスの交換を行う仕様になっていますが、これは、ネットワークが使用するサブネットマスクとアドレスが使用するサブネットマスクが同じであるに場合のみ適用されます。このため RIP バージョン 1 ではクラスのないアドレスを伝播できません。

RIP バージョン 1 を使用するルータは、各 IP インタフェースの異なるアップデートメッセージを接続するインタフェースに送信します。ルータのネットワークと同じサブネットマスクを使用するインタフェースは、サブネット化されたルートを持ちますが、他のインタフェースは持ちません。その場合、ルータはネットワークへのルートを一つだけ通知します。

RIP バージョン 2 の拡張機能

RIP バージョン 2 は、明示的なサブネットマスクを含みます。そのため、可変長のサブネットアドレスや CIDR 表記のクラスレスアドレスを使用することができます。さらに、明示的なネクストホップを含むため、収束までの速度が上がり、ルーティングループの発生を防止します。

RIP2 メッセージフォーマット

RIP2 で使用するメッセージフォーマットは RIP1 フォーマットの拡張版です。
RIP バージョン 2 では、さらに 16 ビットのルートタグが付加されています。ルートタグは維持され、またルータアップデートと共に送信されます。ルートの基点を識別するために使用されます。
RIP2 のバージョンは、RIP1 と同じオクテットを使用するため、1 つのルータ上で両方のバージョンを同時に使用することも可能です。

RIP Settings（RIP 設定）

1 つ以上の IP インタフェースに RIP 設定を行います。

L3 Features > RIP > RIP 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。RIP の設定を行ったインタフェースのリストが表示されます。

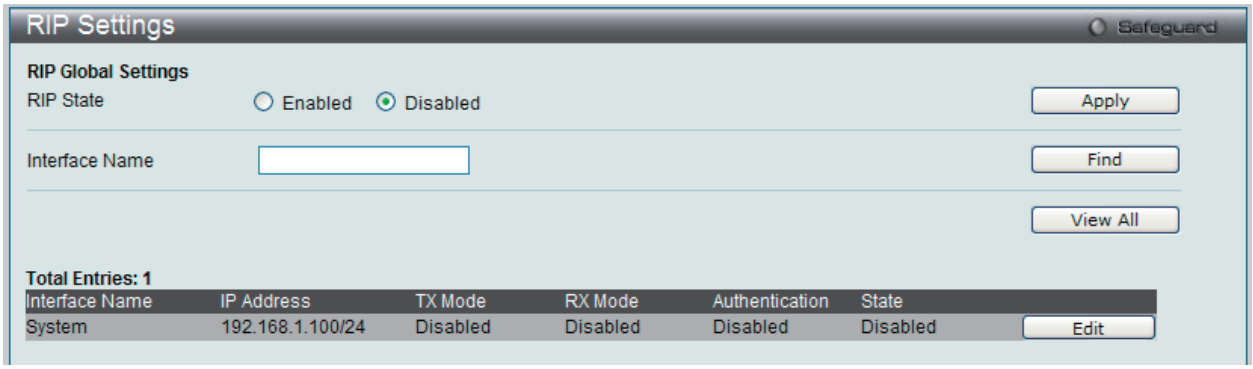


図 10-52　RIP Settings 画面

以下の項目があります。

項目	説明
RIP State	RIP 状態を有効または無効にします。状態が無効にされると、RIP パケットはインタフェースによって送受信されません。このインタフェースで設定されたネットワークは RIP データベースにはありません。
Interface Name	本設定に使用する IP インタフェース名を指定します。

「Apply」ボタンをクリックして行った変更を適用します。
「Find」ボタンをクリックして、指定したエントリを検索します。
「View All」ボタンをクリックして、すべてのエントリを表示します。

エントリの編集

「Edit」ボタンをクリックすると、以下の画面が表示されます。

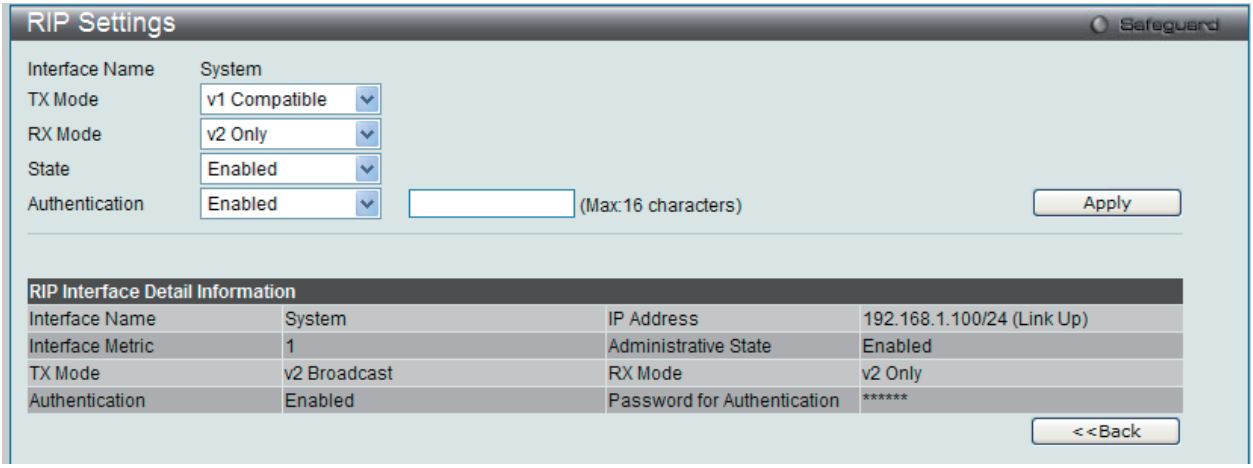


図 10-53　RIP Settings 画面 – Edit 画面

RIP インタフェースの設定に使用する項目は以下の通りです。

項目	説明
Interface Name	本設定に使用 IP インタフェース名を指定します。
TX Mode	「Disabled」、「v1 Only」、「v1 Compatible」、「v2 Only」から選択します。ここで指定する RIP プロトコルのバージョンで RIP パケットを送出します。「Disabled」を指定すると、RIP パケットの送信をしません。
RX Mode	「Disabled」、「v1 Only」、「v2 Only」、「v1 or v2」、から選択します。ここで指定する RIP プロトコルのバージョンが受信した RIP パケットの解釈に使用されます。「Disabled」を指定すると、RIP パケットの受信をしません。
State	RIP インタフェースとしての使用を「Enabled」（有効）/「Disabled」（無効）にします。状態が無効にされると、RIP パケットは、インタフェースによって送受信されません。このインタフェースで設定されたネットワークは RIP データベースにはありません。
Authentication	ネットワーク上のルータがテーブルの交換の際に認証を行うかどうかを指定します。認証状態を有効にした場合、提供されたスペースで使用するパスワードを入力します。

「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て前のページに戻ります。

RIPng（RIPng 設定）（EI モードのみ）

スイッチは、RIPng（Routing Information Protocol next generation）をサポートしています。RIPng は、ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルであり、IPv6 ベースのネットワーク用です。

RIPng Global Settings（RIPng グローバル設定）

本画面では、RIPng の設定を行います。

L3 Features > RIP > RIPng > RIPng Global 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。

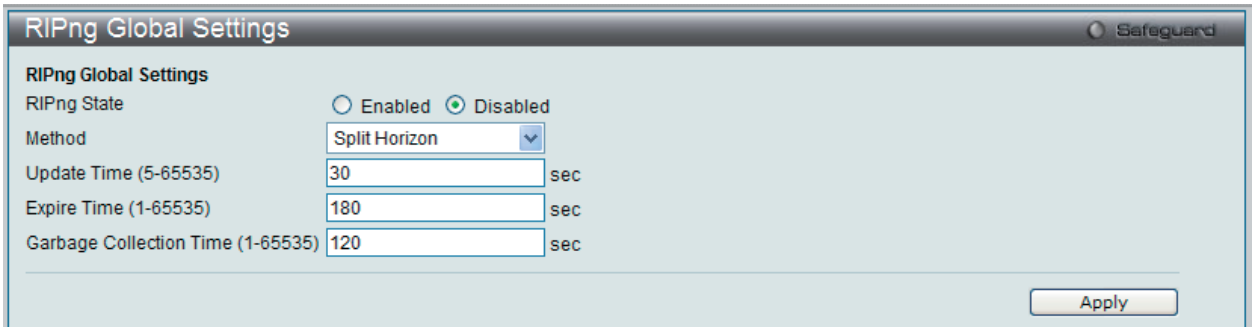


図 10-54 RIPng Global Settings 画面

以下の項目を使用します。

項目	説明
RIPng State	ラジオボタンを使用して RIPng を「Enabled」(有効)/「Disabled」(無効) にします。初期値は「Disabled」です。
Method	プルダウンメニューを使用して「No Horizon」、「Split Horizon」、および「Poison Reverse」から選択します。 • No Horizon - どのホライズンも使用しません。 • Split Horizon - 基本的なスプリットホライズンを使用します。これは初期設定です。 • Poison Reverse - ポイズンリバースを持つスプリットホライズンを使用します。
Update Time (5-65535)	アップデートタイマの値（秒）を入力します。
Expire Time (1-65535)	期限終了タイマの値（秒）を入力します。
Garbage Collection Time (1-65535)	ガーベージコレクションタイマの値（秒）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。

RIPng Interface Settings（RIPng インタフェース設定）

本画面では、RIPng インタフェースの設定を行います。

L3 Features > RIP > RIPng > RIPng Interface 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。

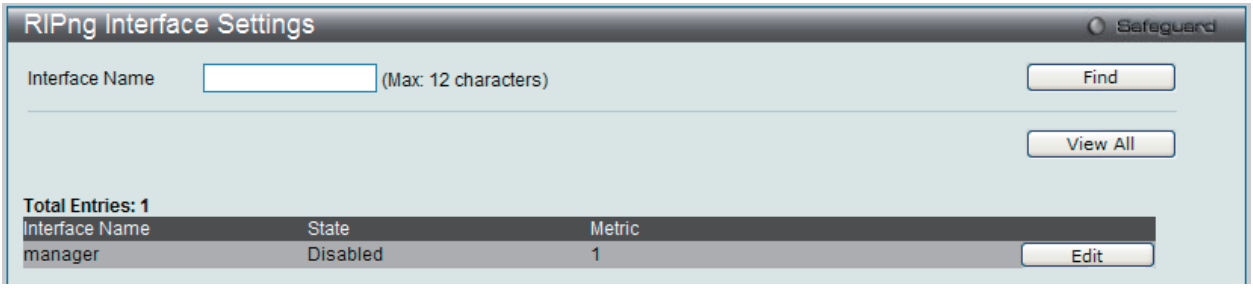


図 10-55　RIPng Interface Settings 画面

以下の項目を使用します。

項目	説明
Interface Name	RIPng 設定のインタフェース名を入力します。

「Find」ボタンをクリックして、入力したインタフェースを検出します。
「View All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

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以下の画面を表示します。

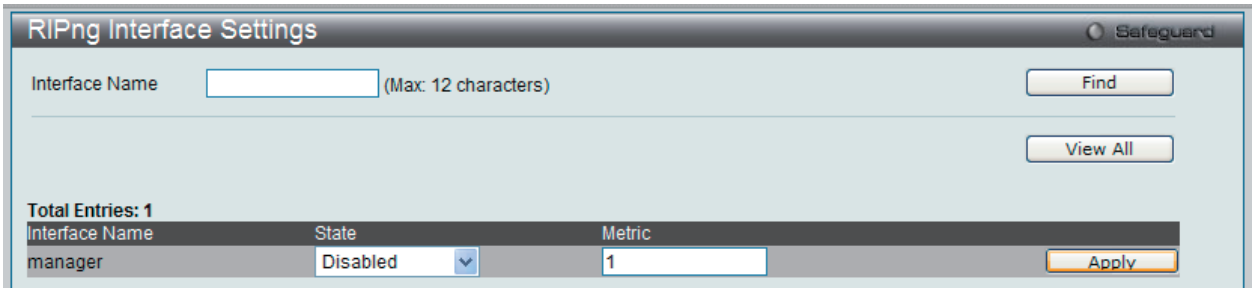


図 10-56　RIPng Interface Settings 画面 - Edit

2. 項目を編集後「Apply」ボタンをクリックします。

IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）

IGMP（IGMP 設定）

IGMP Interface Settings（IGMP インタフェース設定）

IGMP（Internet Group Management Protocol）は、IP インタフェースごとを基本にスイッチに設定されます。スイッチに設定した各 IP インタフェースは、以下の「IGMP Interface Settings」画面に表示されます。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Interface 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。

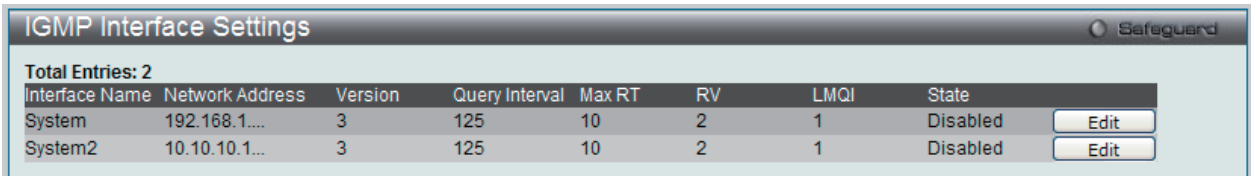


図 10-57 IGMP Interface Settings 画面

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。

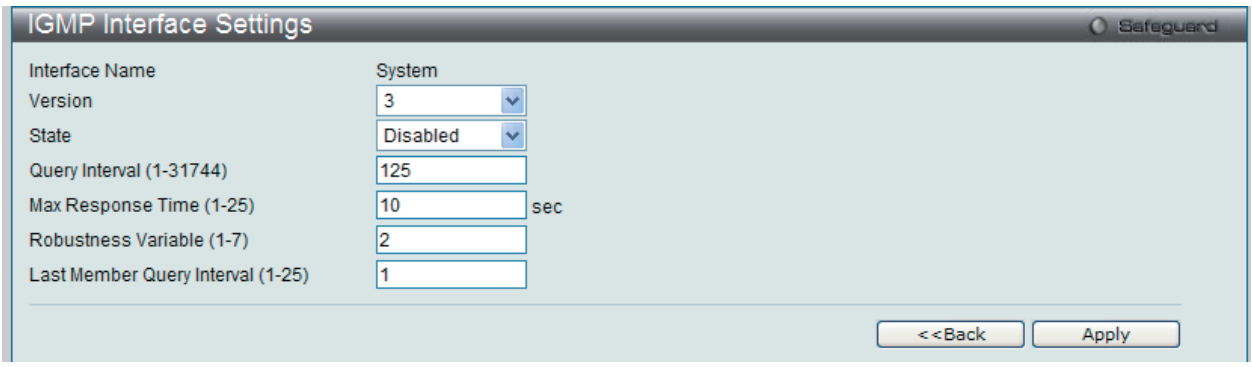


図 10-58 IGMP Interface Settings - Edit 画面

以下の項目を使用します。

項目	説明
Version	インタフェースにおける IGMP クエリを解釈するのに使用する IGMP のバージョンを選択します。
State	プルダウンメニューを使用して、IP インタフェースの IGMP を「Enabled」（有効）/「Disabled」（無効）にします。初期値は Disabled です。
Query Interval (1-31744)	IGMP クエリを送信する間隔（1-31744）を指定します。初期値は 125（秒）です。
Max Response Time (1-25)	IGMP response report を送信するまでの最大時間（1-25 秒）を入力します。初期値は 10（秒）です。
Robustness Variable (1-7)	大量のパケットの喪失が予想されるサブネットワークで許可される調整変数。1-7 の範囲で入力します。大量のパケットの喪失が予想されるサブネットワークでは大きい数値を使用します。初期値は 2 です。
Last Member Query Interval (1-25)	Leave Group メッセージをへの応答で送信するものも含め。Group-Specific Query メッセージの送信間隔（1-25）を入力します。初期値は 1（秒）です。

2. 項目を編集後「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックして前のページに戻ります。

IGMP Check Subscriber Source Network Settings（IGMP チェックサブスクライバの送信元ネットワーク設定）

本画面では、IGMP チェックサブスクライバの送信元ネットワークの設定を行います。チェックサブスクライバの送信元ネットワークがインタフェースで有効になると、インタフェースが受信したすべての IGMP Report または Leave メッセージは、送信元 IP がインタフェースと同じネットワークにあるかどうかを判断するためにチェックされます。チェックが無効であると、どんな送信元 IP を持つ IGMP Report または Leave メッセージも IGMP プロトコルによって処理されます。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Check Subscriber Source Network 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。

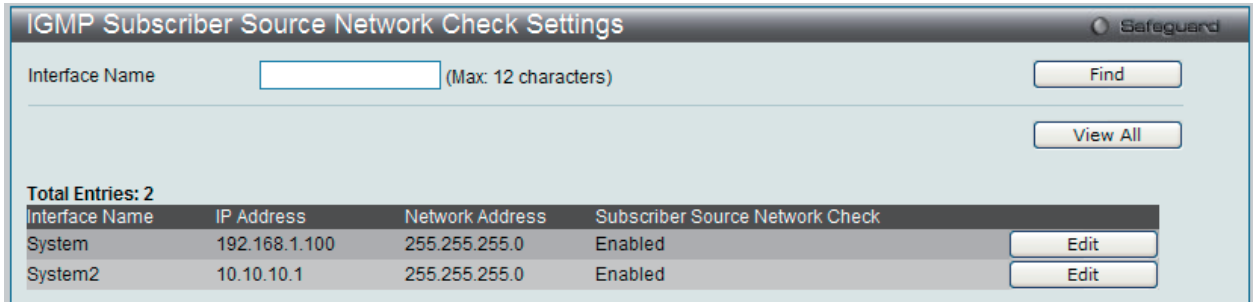


図 10-59 IGMP Check Subscriber Source Network Settings 画面

以下の項目を使用します。

項目	説明
Interface Name	本設定に使用する IP インタフェース名を指定します。

「Find」ボタンをクリックして、入力したインタフェースを検出します。
「View All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

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以下の画面を表示します。

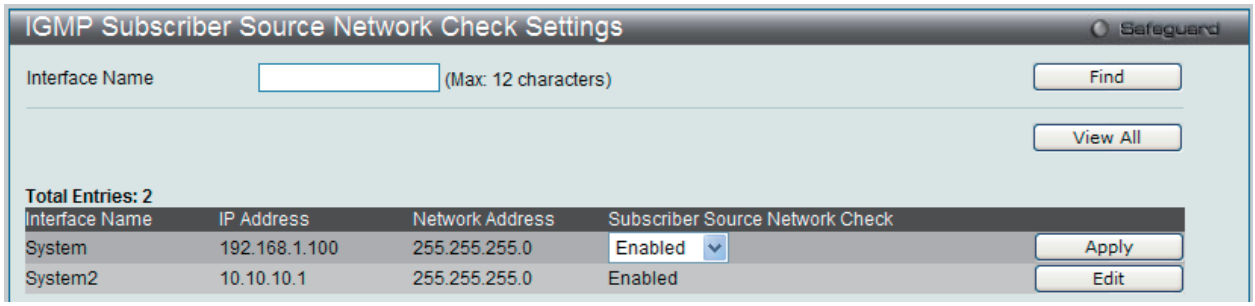


図 10-60 IGMP Check Subscriber Source Network Settings 画面 - Edit

2. 項目を編集後「Apply」ボタンをクリックします。

IGMP Group Table（IGMP グループテーブル）

スイッチスタックにおける IGMP スタティックグループを表示します。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Group Tables 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。

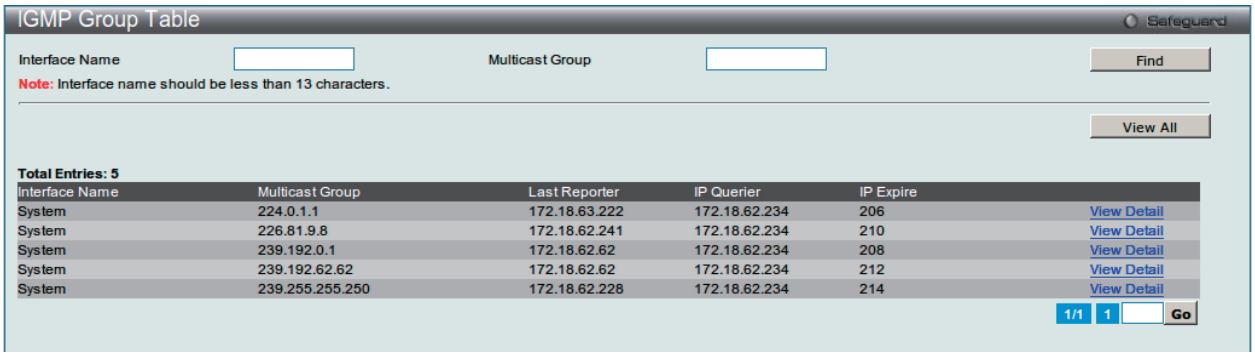


図 10-61　IGMP Group Table 画面

以下の項目を使用します。

項目	説明
Interface Name	本設定に使用する IP インタフェース名を指定します。
Multicast Group	マルチキャストグループ IP 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、入力した情報を検出します。
「View All」ボタンをクリックして、すべての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。

エントリの詳細情報の表示

「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。

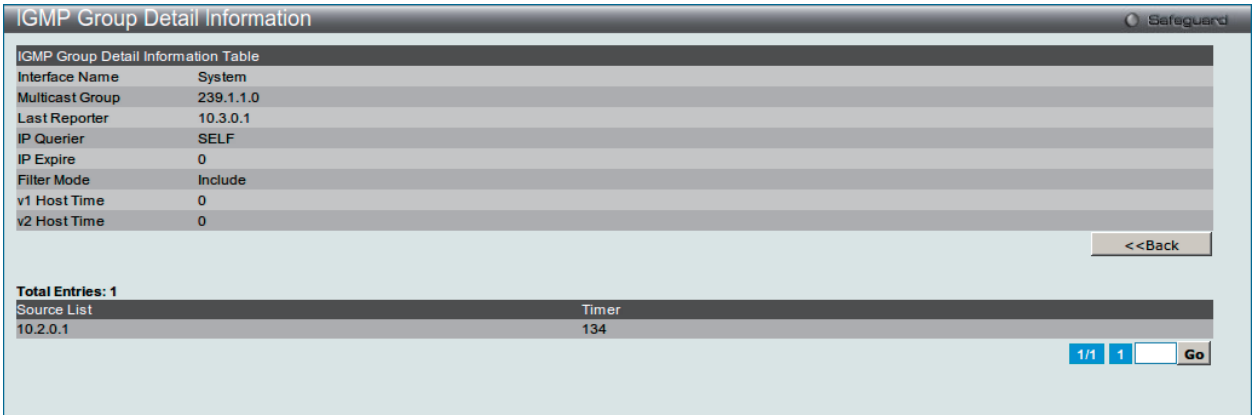


図 10-62　IGMP Group Detail Information 画面

「<<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。

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

スイッチに IGMP スタティックグループを作成します。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Static Group 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。

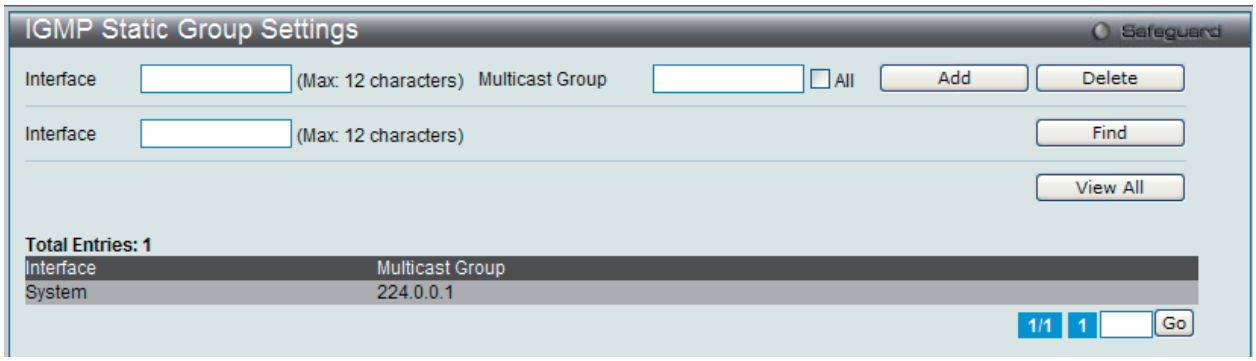


図 10-63　IGMP Static Group Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Interface	IGMP スタティックグループが存在する IP インタフェースを入力します。IP インタフェースはプライマリ IP インタフェースである必要があります。
Multicast Group	マルチキャスト IP アドレスを指定します。

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、入力した情報を検出します。
「View All」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。

DVMRP

DVMRP（Distance Vector Multicast Routing Protocol）は、マルチキャストソースを頂点として、あるネットワーク上のすべてのノードに対するマルチキャスト配送ツリーを構築するホップベースの方法です。配送ツリーでは「Pruned」が行われ、かつ「最短パス」であるため、DVMRP は比較的有効なマルチキャスト配送方法と見られています。マルチキャストグループのメンバシップ情報は、距離ベクトルアルゴリズムによって送信されるため、伝播スピードは遅いといえます。DVMRP は、高遅延で比較的低帯域のネットワーク用に最適化されており、ベストエフォート型のマルチキャストプロトコルであると言えます。

DVMRP は Routing Information Protocol（RIP）に似ていますが、マルチキャスト送信を拡張したものです。DVMRP はルーティングテーブルを作成し、マルチキャストメッセージの送信元に戻る最短経路を計算します。しかし、マルチキャスト送信ツリーが完成すると、この送信ツリー内の経路を使用した本当のコストを表す相対的な番号としてルートコスト（RIP のホップカウントに類似）を定義します。

送信者がマルチキャストメッセージを発信すると、DVMRP は、まずネットワーク上のすべてのユーザがマルチキャストメッセージの受信を望んでいるものと仮定します。隣接するルータがメッセージを受信すると、そのルータのユニキャストルーティングテーブルを確認し、ソースへ戻る最短パス（最小コスト）を提供するインタフェースを決定します。マルチキャストが最短パスにより受信されると、隣接するルータは自身の持つテーブルにその情報を追加し、メッセージを送信します。メッセージが最短パスを通ってソースに戻らなければ、そのメッセージは廃棄されます。

ルートコストは、マルチキャスト配送ツリーのどの枝葉を刈り込むかを計算するために DVMRP に使用される相対的な番号です。コストはネットワークの至る所にある他の DVMRP 経路に割り当てられる他のコストに関係します。

他に代替ルートが存在すれば、ルートコストが高いほど、現在のマルチキャスト配送ツリーの有効な枝葉になるようにルートが選ばれる可能性が低くなります。

DVMRP Interface Settings（DVMRP インタフェース設定）

スイッチに DVMRP グローバル設定を行い、定義済みの各 IP インタフェースに DVMRP を設定します。スイッチに設定した各 IP インタフェースは、以下の「DVMRP Interface Settings」画面に表示されます。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Interface 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。

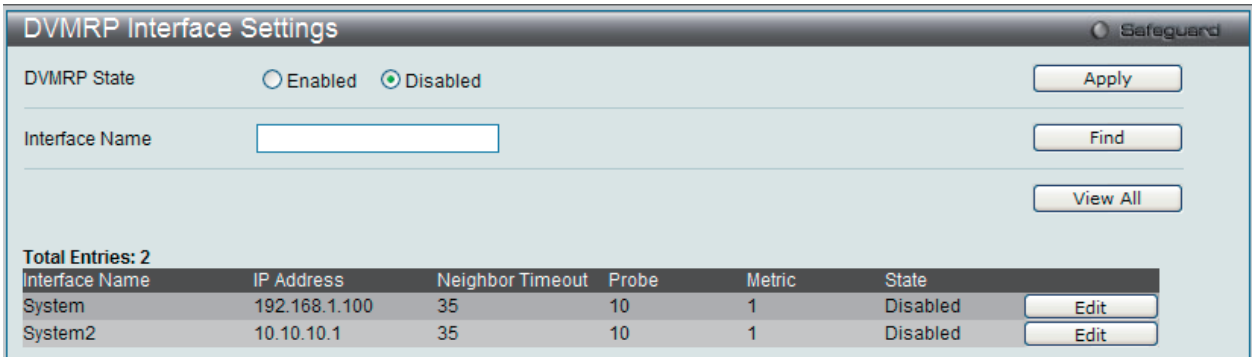


図 10-64 DVMRP Interface Settings 画面

以下の項目を使用します。

項目	説明
DVMRP State	ラジオボタンを使用して DVMRP 状態を「Enabled」（有効）/「Disabled」（無効）にします。
Interface Name	DVMRP のインタフェース名を入力します。これは定義済みの IP インタフェースである必要があります。

エントリの追加

「Apply」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、入力したインタフェースを検出します。「View All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

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以下の画面を表示します。

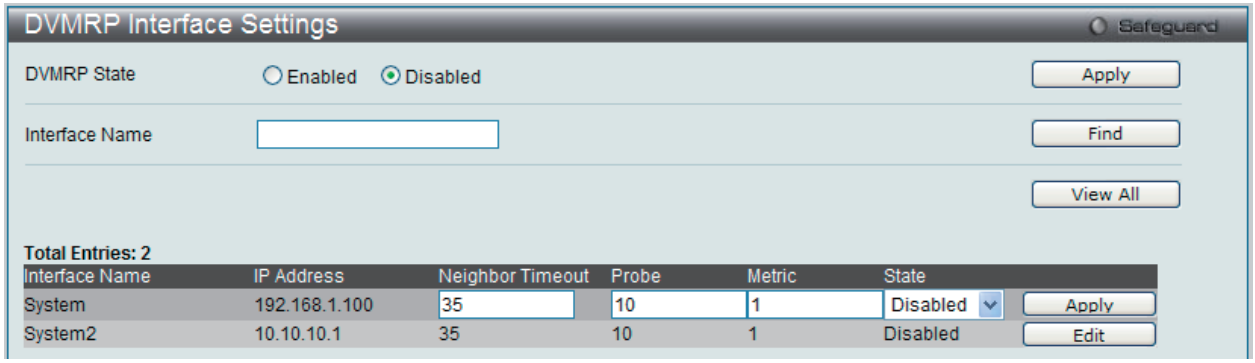


図 10-65 DVMRP Interface Settings 画面 - Edit

2. 項目を編集後「Apply」ボタンをクリックします。

DVMRP Routing Table（DVMRP ルーティングテーブル）

スイッチにおける DVMRP ルーティングテーブルを表示します。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Routing Table 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。

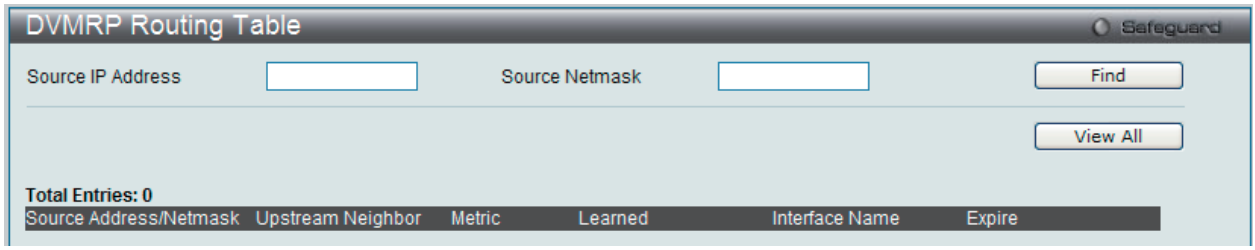


図 10-66 DVMRP Routing Table 画面

以下の項目を使用します。

項目	説明
Source IP Address	送信先の IP アドレスを入力します。
Source Netmask	送信先のネットマスクを入力します。

「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、本スイッチに定義済みの全インタフェースを表示します。

DVMRP Neighbor Table（DVMRP Neighbor テーブル）

スイッチにおける DVMRP Neighbor テーブルを表示します。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Neighbor Table 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。

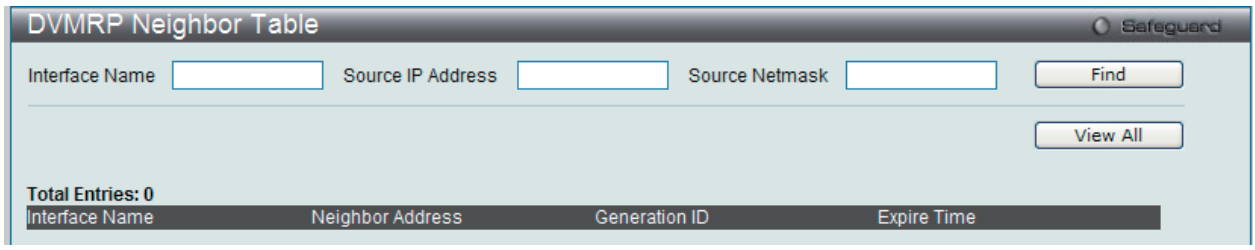


図 10-67 DVMRP Neighbor Table 画面

以下の項目を使用します。

項目	説明
Interface Name	インタフェース名を入力します。
Source IP Address	送信先の IP アドレスを入力します。
Source Netmask	送信先のネットマスクを入力します。

「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、本スイッチに定義済みの全インタフェースを表示します。

DVMRP Routing Next Hop Table（DVMRP ルーティングネクストホップテーブル）

スイッチにおける DVMRP ルーティングネクストホップテーブルを表示します。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Routing Next Hop Table 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 :

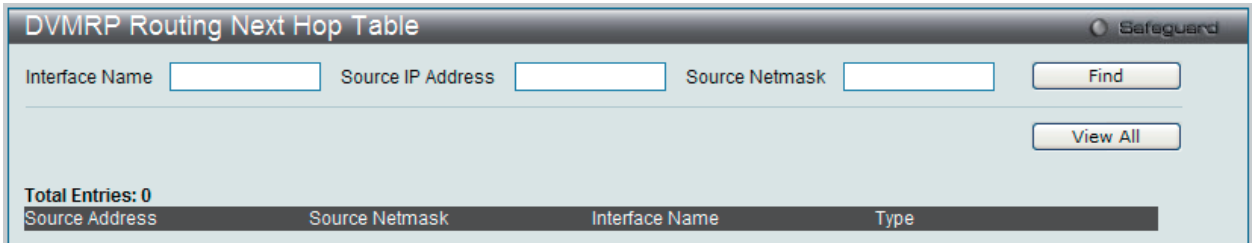


図 10-68 DVMRP Routing Next Hop Table 画面

以下の項目を使用します。

項目	説明
Interface Name	インタフェース名を入力します。
Source IP Address	送信先の IP アドレスを入力します。
Source Netmask	送信先のネットマスクを入力します。

「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、本スイッチに定義済みの全インタフェースを表示します。

PIM（PIM 設定）

PIM（Protocol Independent Multicast）は、LAN、WAN またはインターネット上にデータの 1 対多および多対多の配布を提供する IP（Internet Protocol）ネットワーク用のマルチキャストルーティングプロトコルのファミリです。PIM は、自身のトポロジ検出メカニズムを含まないため、プロトコルに依存しませんが、RIP または OSPF など他の従来型ルーティングプロトコルが提供するルーティング情報を使用します。本スイッチは PIM、Dense Mode (PIM-DM)、Sparse Mode (PIM-SM)、PIM Source Specific multicast (PIM-SSM)、および Sparse-Dense Mode (PIM-DM-SM) の 4 つの PIM タイプをサポートしています。

PIM-SM（Protocol Independent Multicast-Sparse Mode）

Sparse Mode (PIM-SM) は、基本的なユニキャストルーティング情報または個別のマルチキャストが可能なルーティング情報をベースに使用できるマルチキャストルーティングプロトコルです。これは、グループごとの RP（Rendezvous Point）を元に単方向の共有ツリーを構築し、オプションで送信元ごとに最短パスツリーを作成します。

PIM-SM は、ネットワークをマルチキャストパケットでフラッドさせる多くのマルチキャストルーティングプロトコルと異なり、Rendezvous Point(RP) を使用してトラフィックをマルチキャストグループの一部であるルータに明確に転送します。この RP は PIM-SM が有効であるルータからすべてのリクエストを取得し、その情報を分析してネットワーク内でリクエストしているルータに対して送信元から受信したマルチキャスト情報を返します。この方法を通じ、配信ツリーは、ルートとしての RP とともに作成されます。この配信ツリーは、すべての PIM-SM が有効である全ルータを保持しています。RP はこれらのルータから収集した情報をここに保存しています。

多くのルータがマルチアクセスネットワークの一部である場合に、代表ルータ (DR) が選出されます。DR の第一の機能は RP に Join/Prune メッセージを送信することです。LAN 上で最も高いプライオリティを持つルータが DR として選出されます。最も高いプライオリティへの接続がある場合、より高い IP アドレスを持つルータが選出されます。

PIM-SM 設定で作成される 3 番目のルータタイプは、Boot Strap Router(BSR) です。BSR の目的は、RP 情報を収集し、LAN 上の PIM-SM が有効であるルータにリレーすることです。RP はスタティックに設定されますが、BSR メカニズムが RP を決定することもできます。複数の Candidate BSR(C-BSR) がネットワーク上に設定されますが、1 つの BSR だけが、RP 情報を処理するために選出されます。どの C-BSR が、BSR になるかが明白でない場合、すべての C-BSR は、PIM-SM が有効であるネットワークに Boot Strap Messages(BSM) を放出し、より高いプライオリティを持つ C-BSR が BSR として選出されます。一度決定されると、BSR は、PIM-SM ネットワークで Candidate RP から送信される RP データを収集し、それを編集し、周期的な BSM を使用して LAN 上に送信します。すべての PIM-SM ルータは Boot Strap メカニズムから RP 情報を取得し、データベースに保持します。

マルチキャストグループの検出（Discovery）と接続（Join）

Hello パケットは PIM-SM ルータを検出しますが、これらのルータは DR と RP 間で交換される Join/Prune メッセージを使用することでマルチキャストグループからの接合または「Pruned」を行います。Join/Prune メッセージは、マルチキャストデータを受信するためにどのインタフェースがあるのか、またはないのかを効果的に記述しているルータ間で中継されるパケットです。これらのメッセージは、頻繁に設定されネットワーク上に送信され、Hello パケットがはじめに受信される場合にだけルータに有効となります。Hello パケットは、ルータが存在し、RP の配信ツリーの一部になる準備中であることを簡単に記述しています。ルータが IGMP グループのメンバを受け入れて、PIM-SM が有効である場合、興味があるルータは明確な Join/Prune メッセージを RP に送信します。それは、送信元から興味があるルータにマルチキャストデータを順番に送信し、グループのための一定方向の配布ツリーを作成します。マルチキャストパケットは、その後これらのツリー上の全ノードに送信されます。一度 Prune メッセージが RP の送信ツリーのメンバであるルータに受信されると、ルータはその配信ツリーからそのインタフェースを削除します。

配信ツリー

2 つのタイプの配信ツリーが PIM-SM プロトコル、Rendezvous-Point Tree(RPT) および最短経路ツリー (Shortest Path Tree:SPT) に存在します。RP は、マルチキャストデータを受信することが可能なすべての外向きインタフェースに、送信元から受信した特定のマルチキャストデータを送信します。しかし、一度ルータが送信元の位置を決定すると、SPT は、RP などの送信元と送信先の間のホップを除去して作成されます。これは、マルチキャストデータ転送速度のしきい値を設定することで設定されます。しきい値を越えると、データの経路は SPT に切り換えます。従って、より近いリンクが送信元と宛先の間で作成され、以前に使われたホップを取り除き、マルチキャストパケットが送信元から最終到達先に送信される時間を短縮します。

Register と Register Suppression メッセージ

マルチキャストソースは、いつも意図する受信グループに接合するわけではありません。最初のホップルータ (DR) は、グループのメンバでなくても、または明示された送信元も持たなくてもマルチキャストデータを送信することができます。それは本質的に、この情報を RP 配信ツリーに中継する方法についての情報を持っていないと言うことを意味しています。この問題は、Register と Register-Stop メッセージを通じて緩和されます。DR が受信したはじめのマルチキャストパケットがカプセル化され、RP に送信されます。RP は逆にカプセル化を解いて RP 配信ツリーの下に向かってパケットを送信します。ルートが確立すると、SPT が作成され、ルータを直接ソースに接続するか、マルチキャストトラフィックフローを開始して、DR から RP への通信を行います。後者の場合、カプセル化されているタイプとカプセル化されていないタイプで同じパケットが 2 回送信される可能性があります。RP はこの不備を検出し、カプセル化されたパケットの送信を停止するようにリクエストをしている DR に Register-stop メッセージを戻します。

Assert メッセージ

PIM-SM が使用可能なネットワークにおいて、時々パラレルパスが送信元から受信先に対して作成されます。これは複数の受信先が 2 回同じマルチキャストパケットを受信することを意味しています。この状況を改善するために、Assert メッセージが受信デバイスから両方のマルチキャストソースに送信され、どのルータが受信者に必要なマルチキャストデータを送信するかを決定します。最短メトリック (ホップカウント) を持つ送信元がプライマリマルチキャストソースとして選出されます。このメトリックは Assert メッセージ内に含まれています。

PIM-SSM

SSM（Source Specific Multicast）機能は、IP マルチキャストの拡張機能です。ここではデータトラフィックは受信者が明確に参加しているというマルチキャスト送信元だけから受信者に送信されます。SSM 範囲のマルチキャストグループにおいて、送信元を指定したマルチキャスト配信ツリー (共有ツリーはない) だけが作成されます。

IANA（Internet Assigned Numbers Authority）は SSM アプリケーションとプロトコルのために 232.0.0.0 ～ 232.255.255.255 のアドレス範囲を予約しています。スイッチは IP マルチキャストアドレス範囲 224.0.0.0 ～ 239.255.255.255 の任意のサブセットに SSM を設定できます。

PIM-DM

PIM-DM(Protocol Independent Multicast-Dense Mode) プロトコルは、オーバヘッド削減の目的ではなく、マルチキャストパケットの配送を保証するために利用されるため、低遅延で高帯域のネットワークに適したプロトコルです。

PIM-DM マルチキャストルーティングプロトコルは、下流のルータがマルチキャストメッセージの受信を希望していると仮定し、下流のルータからのプルーンメッセージ (削除メッセージ) を受けて、マルチキャスト配信ツリーから、マルチキャストグループメンバの存在しない枝葉を Pruned します (削除します)。

PIM-DM には明示的な “Join" メッセージは存在しません。その代わりに、すべてのインタフェースマルチキャストメッセージの定期的なフラッディングに依存し、タイマの期限切れ (Join/Prune インターバル) を待つか、または下流のルータが明示的な “Prune" メッセージを送信して、その枝にはマルチキャストメンバが存在しない旨を示すのを待ちます。PIM-DM はその後マルチキャスト配信ツリーからこれらの枝を削除します。

マルチキャスト配信ツリーから刈り込まれた枝も、マルチキャスト配信グループへの参加を (将来的に) 希望している可能性があります。そのため、プロトコルは定期的にデータベースから “Prune(削除)" 情報を削除し、その枝のすべてのインタフェース宛てにマルチキャストメッセージのフラッディングを行います。この、“Prune" 情報の削除を行う間隔が Join/Prune インターバルです。

PIM-SM-DM

PIM-SM では、RP は送信側の最初のホップルータです。最初のホップは、送信側がいつデータを送信するか RP を持っていないと、パケットを破棄し、何も実行しません。Sparse-Dense モードはこの条件で有益です。Sparse-Dense モードで、パケットがすべての外向きのインタフェースでフラッドし、pruning/joining(prune/graft) が RP が検出されない場合にと外向きのインタフェースを制御することが可能です。つまり、PIM Sparse-Dense モードは、マルチキャストグループがどのモードで操作するかによって操作の Sparse モードまたは Dense モードのどちらかで扱われます。インタフェースがマルチキャストトラフィックを受信する場合、グループに既知の RP があれば、インタフェースの現在の操作モードは Sparse モードになり、そうでない場合、インタフェースの現在の操作モードは Dense モードになります。

PIM for IPv4（IPv4 用 PIM の設定）

PIM Global Settings（PIM グローバル設定）

スイッチに PIM グローバル状態と PIM 配信ツリーの設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Global 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。

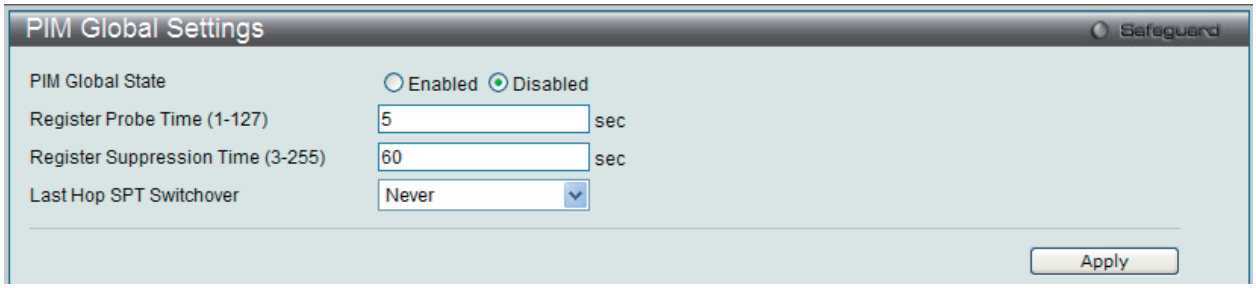


図 10-69 PIM Global Settings 画面

以下の項目を使用します。

項目	説明
PIM Global State	ラジオボタンを使用して PIM のグローバル状態を「Enabled」（有効）/「Disabled」（無効）にします。
Register Probe Time (1-127)	Register Suppression 時間になる前に DR から RP にプローブメッセージを送信する時間を設定します。Register Stop メッセージを DR が受信すると、Register Suppression Time は再度開始します。プローブタイムに Register Stop メッセージを受信しない場合、Register パケットが RP に再送されます。1-127（秒）で指定します。初期値は 5（秒）です。
Register Suppression Time (3-255)	送信元から最初のホップルータに設定されます。このルータが RP に Register メッセージを送信し、RP が Register Stop メッセージで応答した後に、ここで設定された時間待機し、他の RP に Register メッセージを送信します。3-255（秒）で指定します。初期値は 60（秒）です。
Last Hop SPT Switchover	ラストホップルータが共有ツリーから最短パスツリーまでのマルチキャストデータを受信するか、スイッチから最短パスツリーまでのマルチキャストデータを受信するかを決定します。 • Never - ラストホップルータは通常共有ツリーからマルチキャストデータを受信します。 • Immediately - ラストホップルータは通常最短パスツリーからデータを受信します。

「Apply」ボタンをクリックして行った変更を適用します。

PIM Interface Settings（PIM インタフェース設定）

IP ごとに PIM プロトコルの設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Interface 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 :

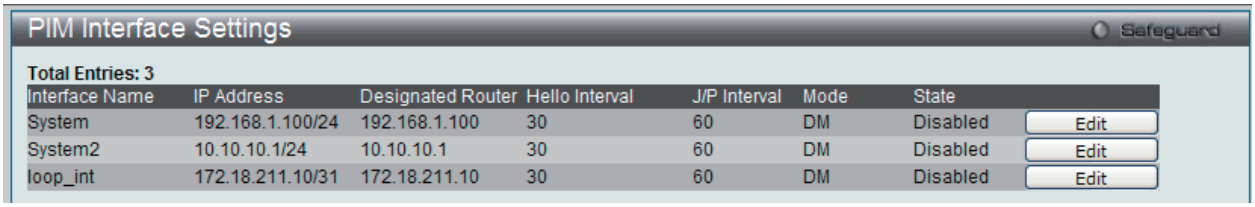


図 10-70 PIM Interface Settings 画面

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。

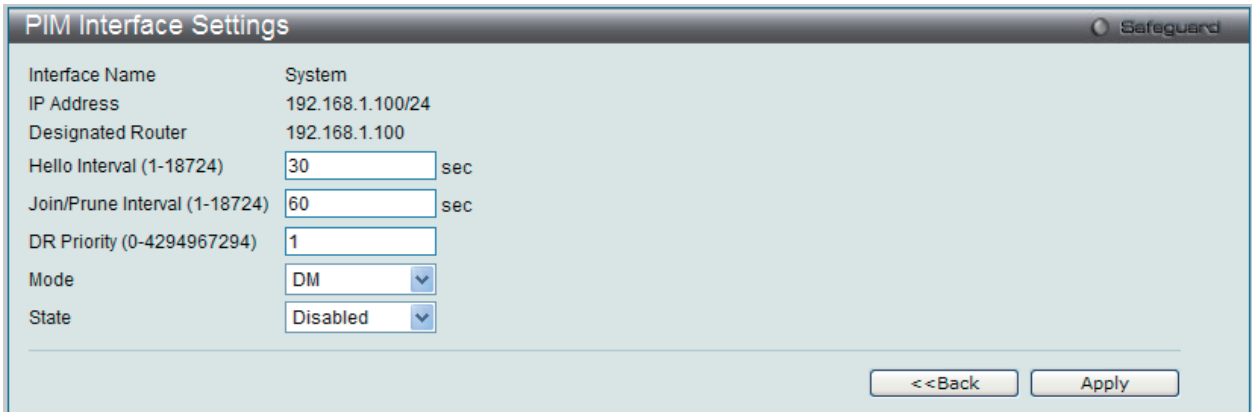


図 10-71 PIM Interface Settings - Edit 画面

以下の項目を使用します。

項目	説明
Hello Interval (1-18724)	この IP インタフェースから 1 ホップ隣の隣接ルータに Hello パケットを送信する間隔を設定します。これらの Hello パケットは他の PIM が有効なルータを検出し、PIM が有効なネットワーク上の DR としてプライオリティを指定するために使用されます。1-18724（秒）で指定します。初期値は 30（秒）です。
Join/Prune Interval (1-18724)	どのマルチキャストグループが PIM の有効なネットワークに接合し、そのグループから削除または「Pruned」を設定する Join/Prune パケットを送信する間隔を設定します。1-18724（秒）で指定します。初期値は 60（秒）です。
DR Priority (0-4294967294)	IP インタフェースのマルチアクセスネットワークで DR になるためのプライオリティを入力します。0-4,294,967,294 で入力します。初期値は 1 です。
Mode	使用する PIM プロトコルのタイプ (Sparse Mode(SM)、Dense Mode(DM)、または Spare-Dense Mode(SM-DM)) を選択します。初期値は「DM」です。
State	この IP インタフェースの PIM を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。

2. 項目を編集後「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックして前のページに戻ります。

PIM Candidate BSR Settings（PIM Candidate BSR 設定）

PIM が有効なネットワークで Boot Strap Router（BSR）になるために、Candidate Boot Strap Router（C-BSR）設定と指定 IP インタフェースのプライオリティを設定します。Boot Strap Router はネットワーク上のどのルータがマルチキャストグループに対して RP として選出され、他の PIM-SM が有効なルータに RP 情報を収集して、配布するのかを決定する情報を保持しています。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Candidate BSR 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。

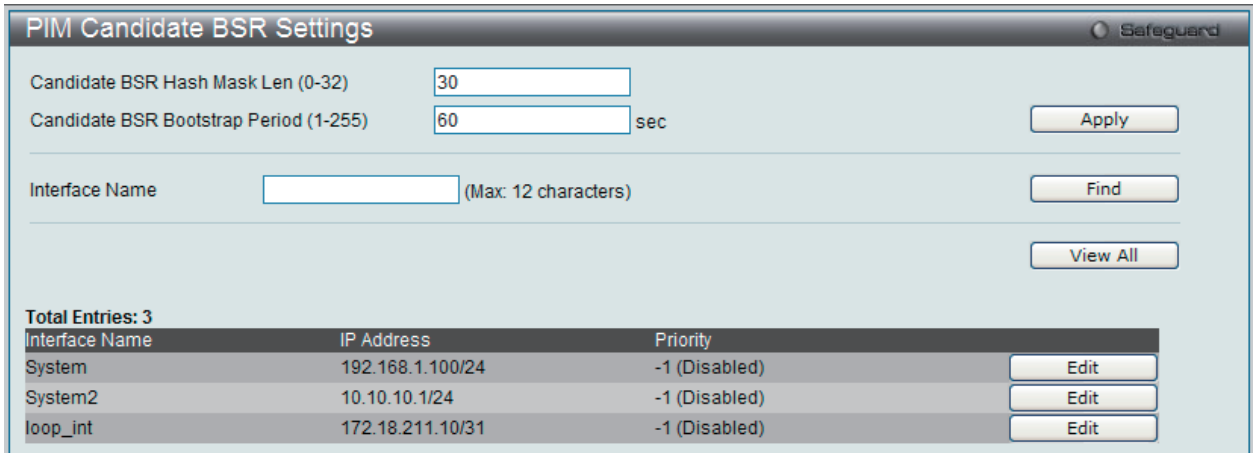


図 10-72　PIM Candidate BSR Settings 画面

以下の項目を使用します。

項目	説明
Candidate BSR Hash Mask Len (0-32)	ハッシュマスク長を入力します。これは Candidate RP の IP アドレスとマルチキャストグループアドレスと共に使用されます。ルータに使用されるハッシュアルゴリズムが PIM-SM の有効なネットワークでどの C-RP が RP になるかを決定するために計算します。0-32 で指定します。初期値は 30 です。
Candidate BSR Bootstrap Period (1-255)	スイッチが PIM の有効なネットワークに Boot Strap Messages(BSM) を送信する間隔を 1-255 で入力します。初期値は 60（秒）です。
Interface name	インタフェース名を入力します。

「Apply」ボタンをクリックして行った変更を適用します。
「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、本スイッチに定義済みの全インタフェースを表示します。

エントリの編集

1. 特定の BSR プライオリティを設定します。「Edit」ボタンをクリックして、以下の画面を表示します。

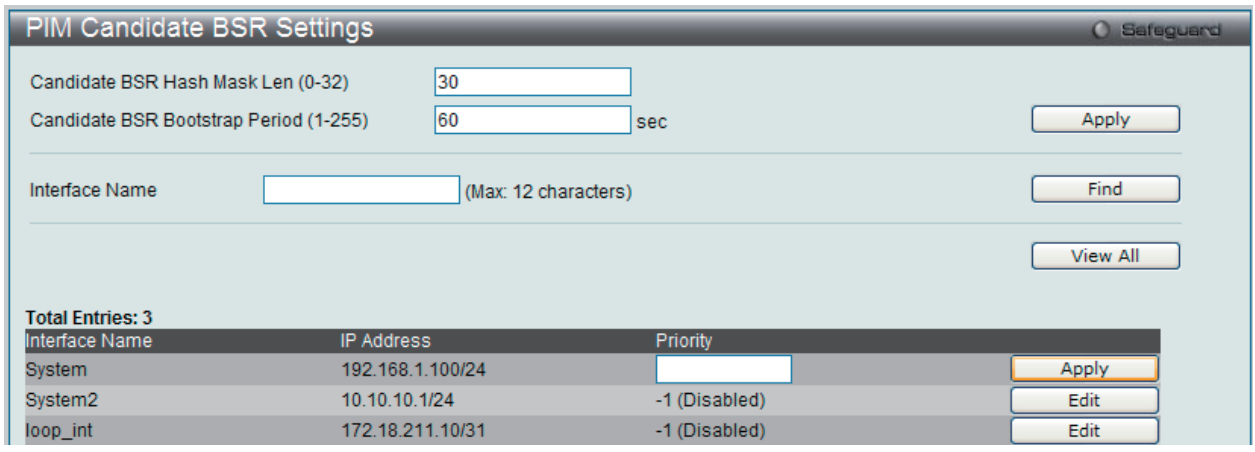


図 10-73　PIM Candidate BSR Settings - Edit 画面

以下の項目を使用します。

項目	説明
Priority	-1、または 0 から 255 までの値を入力します。初期値は -1 で、BSR 状態が無効であることを意味します。

2. 項目を編集後「Apply」ボタンをクリックします。

PIM Candidate RP Settings（PIM Candidate RP 設定）

以下の画面では、本スイッチが Candidate RP になるためのパラメータを設定します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Candidate RP 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。

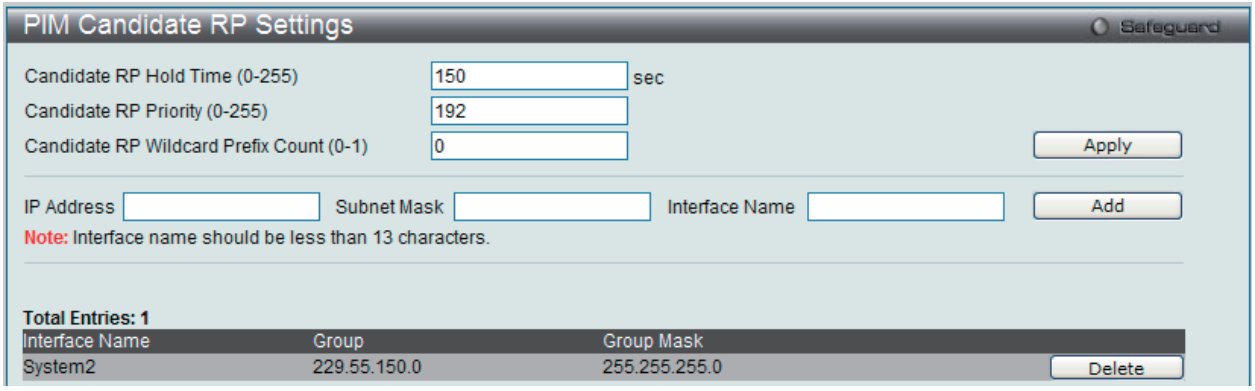


図 10-74　PIM Candidate RP Settings 画面

以下の項目を使用します。

項目	説明
Candidate RP Hold Time (0-255)	PIM-SM が有効なネットワークで Candidate RP(CRP)advertisement が有効である時間を設定します。CRP advertisement がこの時間フレーム内で BSR に受信されないと、CRP は candidate(候補) リストから削除されます。0-255（秒）で指定します。初期値は 150（秒）です。0 を指定すると、PIM-SM ネットワークにおいて CRP ステータスから直ちに削除されるべきことを BSR に記述する Advertisement を送信します。
Candidate RP Priority (0-255)	どの CRP が配信ツリーに対して RP になるかを決定する優先度値を入力します。この優先度値はルータの CRP Advertisement に含まれます。低い値がより高い優先度を意味しており、最も高い優先度が関連付けられている場合、最も高い IP アドレスを持つルータが RP になります。0-255 で指定します。初期値は 192 です。
Candidate RP Wildcard Prefix Count (0-1)	ワイルドカードグループアドレスへの Prefix Count 値を設定します。0-1 で指定します。初期値は 0 です。
IP Address	Candidate RP として追加されるデバイスの IP アドレスを入力します。
Subnet mask	Candidate RP として追加されるデバイスの対応するサブネットマスクを入力します。
Interface Name	デバイスが位置する IP インタフェースを指定します。

「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。

PIM Static RP Settings（PIM スタティック RP 設定）

以下の画面では、本スイッチがスタティック RP になるためのパラメータを設定します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Static RP 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。

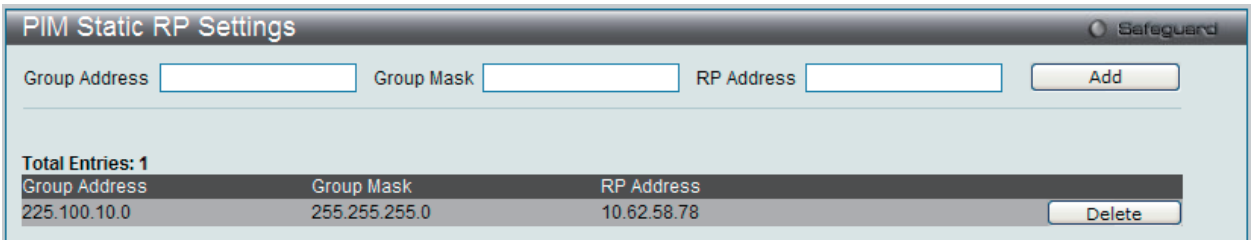


図 10-75　PIM Static RP Settings 画面

以下の項目を使用します。

項目	説明
Group Address	スタティック RP のマルチキャストグループアドレスを指定します。このアドレスはクラス D のアドレスである必要があります。
Group Mask	上記のマルチキャストグループアドレスのマスクを入力します。
RP Address	Rendezvous Point の IP アドレスを入力します。

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。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

PIM Register Checksum Settings（PIM レジスタチェックサム設定）

RP アドレスを設定します。データ部分は、最初のホップルータの RP に PIM レジスタメッセージに対するチェックサムを計算する場合に含められます。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Register Checksum 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。

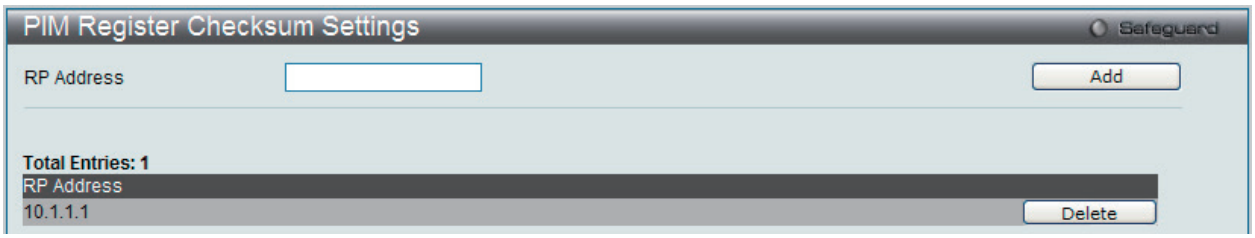


図 10-76　PIM Register Checksum Settings 画面

以下の項目を使用します。

項目	説明
RP Address	RP へのパケット登録用にチェックサムを計算する場合に、データ部分を含める RP の IP アドレスを入力します。

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。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

PIM Neighbor Table
現在の PIM Neighbor ルータテーブルを表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Neighbor Table 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。

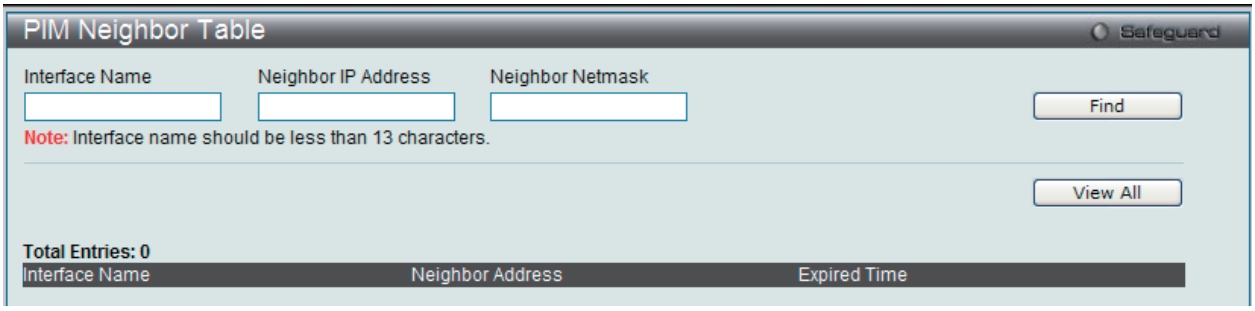


図 10-77　PIM Neighbor Table 画面

以下の項目を使用します。

項目	説明
Interface Name	現在の PIM Neighbor ルーティングテーブルを表示する IP インタフェース名を指定します。
Neighbor IP Address	送信先の IP アドレスを入力します。
Neighbor Netmask	送信先のネットマスクを入力します。

「Find」ボタンをクリックして、入力したインタフェースを検出します。
「View All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

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。

PIM Multicast Route Table（PIM マルチキャストルートテーブル）
現在の PIM Neighbor ルータテーブルを表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Multicast Route Table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。

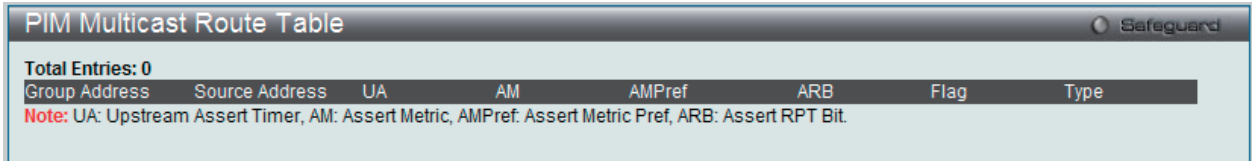


図 10-78　PIM Multicast Route Table 画面

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。

PIM RP-Set Table（PIM RP-Set テーブル）
すべての RP-Set 情報を表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP-Set Table 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。

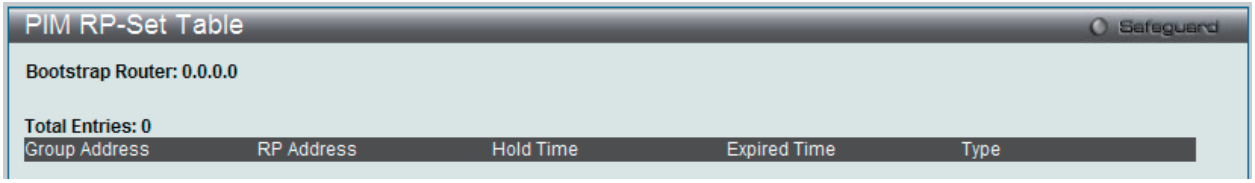


図 10-79　PIM RP-Set Table 画面

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。

PIM SSM Settings（PIM SSM 設定）

スイッチの PIM-SM における SSM（Source-Specific Multicast）サービスモデルを有効または無効にします。PIM-SSM 機能は、SSM サービスモデルと PIM-SM 状態の両方が有効である場合にだけアクティブになります。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM SSM 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。

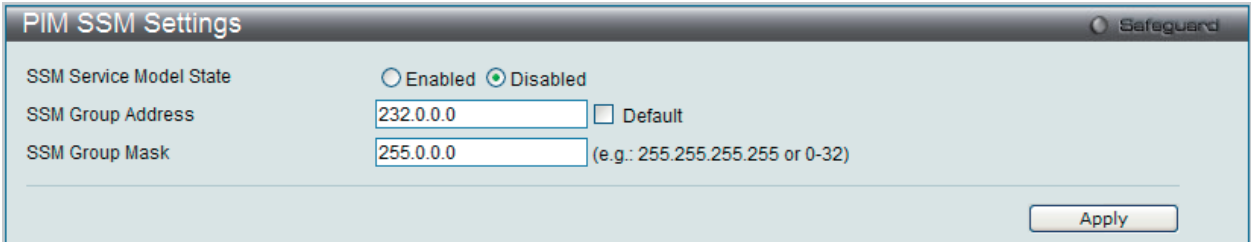


図 10-80　PIM SSM Settings 画面

以下の項目を使用します。

項目	説明
SSM Service Model State	スイッチの SSM サービスモデルを「Enabled」（有効）/「Disabled」（無効）にします。
SSM Group Address	IPv4 における SSM サービス用のグループアドレス範囲に入力します。「Default」をチェックすると、グループアドレス範囲は「232.0.0.0/8」であることを示します。
SSM Group Mask	SSM グループのネットマスクを入力します。

「Apply」ボタンをクリックして行った変更を適用します。

VRRP（VRRP 設定）

VRRP（Virtual Routing Redundancy Protocol）は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です。VRRP ルータのうち、仮想ルータと対向する IP アドレスの制御を行うものをマスタルータと呼び、このルータが本 IP アドレス向けのパケットを送出します。また、エンドホストは LAN 上の仮想ルータの IP アドレスをデフォルトのファーストホップとして使用できます。VRRP 機能を使用して、管理者はすべてのエンドホストにダイナミックルーティングやルート検出プロトコルの設定を行わなくても、デフォルトパスコストを取得することができます。

LAN 上に静的に設定されたデフォルトルートは、障害発生箇所となる傾向があります。VRRP 機能はこの障害を回避するために、選出プロトコルを使用して LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を割り当てるよう設計されています。仮想ルータがダウンすると、選出プロトコルが優先度の最も高い仮想ルータを選び、LAN 上のマスタルータに任命します。これによりダウンした箇所に関係なく、リンクとコネクションはその状態を保つことができます。

VRRP では、1 台の物理的ルータの代わりに、物理的ルータのグループから構成される仮想ルータを導入します。仮想ルータは 2 台以上の物理ルータから構成され、その中で実際に稼動するのは 1 台のみです。その仮想ルータの中で実際に稼動しているルータが停止した場合、自動的に別のルータに切り替わり稼動を開始します。実際に稼動している物理ルータをマスタルータと呼び、マスタルータ異常時に備えて待機している物理ルータをバックアップルータと呼びます。

スイッチに仮想ルータ用の VRRP 機能を設定するためには、IP インタフェースが存在し、その IP アドレスが VLAN に所属している必要があります。VRRP 用 IP インタフェースはスイッチの VLAN（IP インタフェース）ごとに設定します。VRRP 機能が正しく動作するために、同じ VRRP グループ内の VRRP ルータは、同じ設定内容を持つ必要があります。

VRRP Global Settings（VRRP グローバル設定）

スイッチの VRRP 機能をグローバルに有効にします。

L3 Features > VRRP > VRRP 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。

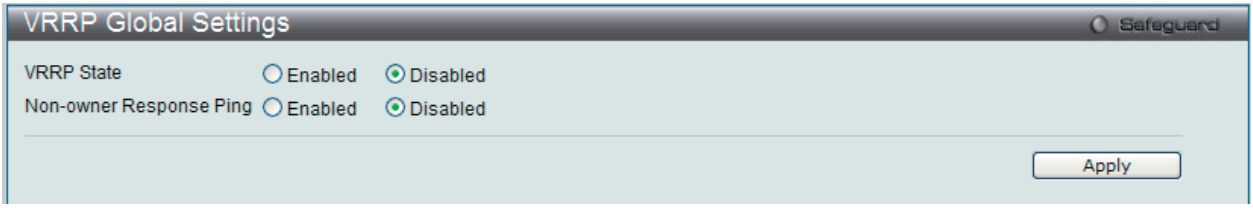


図 10-81　VRRP Global Settings 画面

以下の項目を使用して設定を行います。

項目	説明
VRRP State	スイッチの VRRP 機能をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Non-owner Response Ping	「Enabled」（有効）にすると、仮想 IP アドレスが他のホストに ping を行い、接続性を確認することができます。初期値は「Disabled」（無効）です。

「Apply」ボタンをクリックし、設定を有効にします。

VRRP Virtual Router Settings（VRRP 仮想ルータ設定）

VRRP 仮想ルータ設定を行います。

L3 Features > VRRP > VRRP Virtual Router 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仮想ルータの設定内容を参照します。

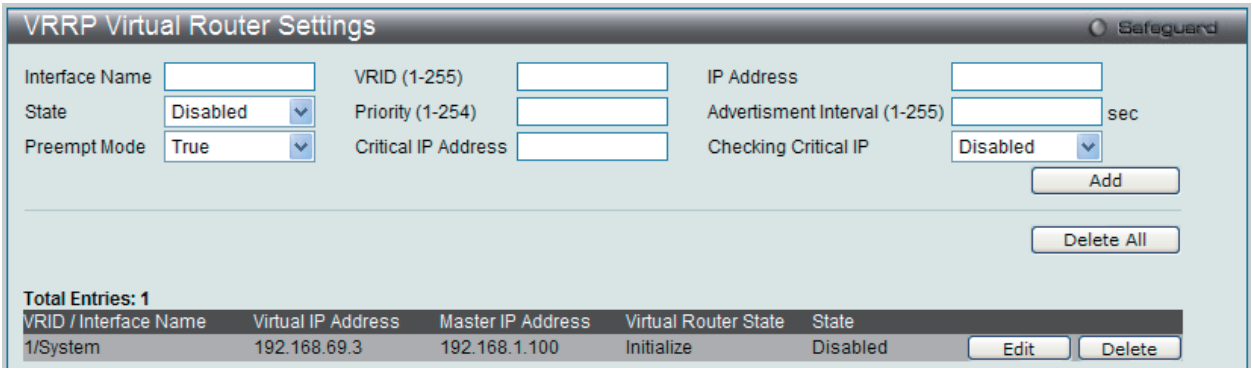


図 10-82　VRRP Virtual Router Settings 画面

インタフェースの仮想ルータの状態を指定します。

項目	説明
Interface Name	VRRP エントリを作成するのに使用する IP インタフェース名を指定します。この IP インタフェースには VLAN が割り当てられている必要があります。
VRID (1-255)	使用する仮想ルータの ID を指定します。本グループに参加するルータには同じ VRID 値が割り当てられる必要があります。スイッチの他の VRRP グループとは異なる値を入力します。
IP Address	使用するルータの IP アドレスを指定します。本 IP アドレスは、エンドホストに静的に割り当てられるデフォルトゲートウェイのアドレスでもあります。同じグループに属するルータには、同じ値を設定する必要があります。
State	VRRP IP インタフェースを「Enabled」（有効）/「Disabled」（無効）にします。
Priority (1-254)	仮想ルータのマスタ選出のプライオリティを指定します。
Advertisement Interval (1-255)	VRRP メッセージパケットの送出間隔（秒）。本値はグループ内で同じものが設定されている必要があります。初期値は 1（秒）です。
Preempt Mode	より高いプライオリティのバックアップルータが、より低いプライオリティのマスタから役割を取り戻すかどうかを制御します。初期値は「True」です。 • True - 高いプライオリティのバックアップルータはマスタルータに代わります。 • False - 高いプライオリティのバックアップルータはマスタに代わることができません。本設定はグループ内で統一させる必要があります。
Critical IP Address	本仮想ルータから、インターネットやクリティカルなネットワークへ最も直接的なルートを提供する物理デバイスの IP アドレスを入力します。本アドレスは、ネットワーク上のデバイスの物理アドレスである必要があります。仮想ルータから本 IP アドレスへの接続がダウンすると、仮想ルータは自動的にダウンします。この場合、VRRP グループ内のバックアップルータから新しいマスタが選出されます。VRRP グループ内の別のルータには異なる Critical IP Address を指定できます。それによりインターネットやクリティカルなネットワークに複数のルートを定義することができます。
Checking Critical IP	クリティカルな IP アドレスのステータス (Active または Inactive) をチェックする状態を指定します。

「Add」ボタンをクリックして、新しいエントリを追加します。

エントリの編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

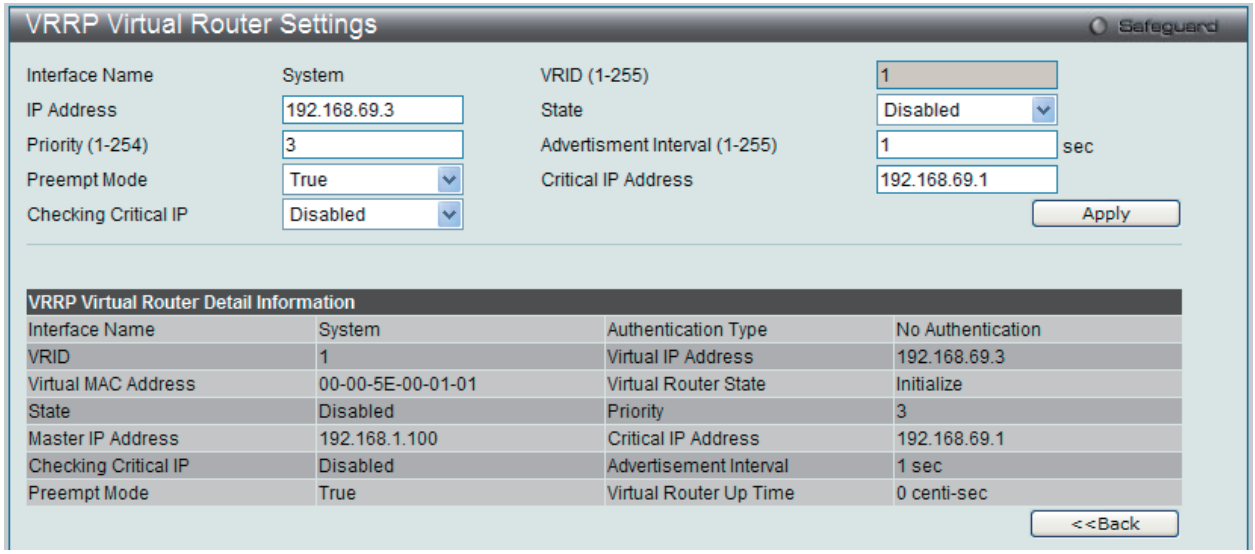


図 10-83　VRRP Virtual Router Settings – Edit 画面

2. エントリの編集を行い、「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。

「<<Back」をボタンをクリックして前のページに戻ります。

VRRP Authentication Settings（VRRP 認証設定）

インタフェースにおける仮想ルータの認証設定を行います。

L3 Features > VRRP > VRRP 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。

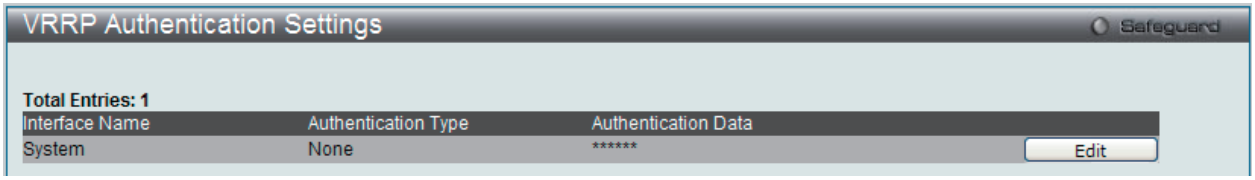


図 10-84 VRRP Authentication Settings 画面

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

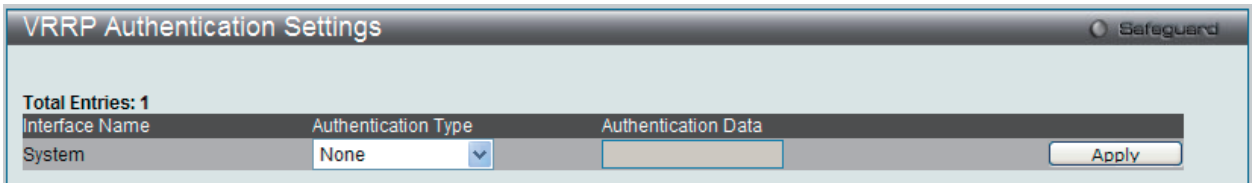


図 10-85 VRRP Authentication Settings – Edit 画面

以下の項目が表示されます。

項目	説明
Interface Name	VRRP 認証情報を設定する IP インタフェース。
Authentication Type	VRRP 認証タイプを指定します。「None」、「Simple」または「IP」を選択します。 • None - VRRP プロトコル交換は認証されないことを意味します。 • Simple - Authentication フィールドへのシンプルパスワード設定が必要になります。ルータが受信した VRRP メッセージを照合するデータフィールド。2 つのパスワードが正確に一致しない場合、パケットは破棄されます。 • IP- ルータが受信した VRRP メッセージを照合する認証のために IP 設定が必要になります。2 つの値が正確に一致しない場合、パケットは破棄されます。
Authentication Data	本欄は、「Authentication Type」欄で「Simple」または「IP」が指定されている場合に有効です。「Simple」と「IP」認証アルゴリズムで使用する認証データを指定します。同じ IP インタフェースに所属する全ルータが同じ設定を行う必要があります。 • Simple - ルータが受信した VRRP パケットを識別するために 8 文字以内の半角英数字を入力します。 • IP - ルータが受信した VRRP パケットを照合するために 16 文字以内の半角英数字を入力します。

2. エントリの編集を行い、「Apply」ボタンをクリックします。

MD5 Settings（MD5 キー設定）

OSPF ルータ間で交換するパケットごとの認証に使用される 16 文字の MD5（Message Digest version 5）キーを指定します。これは、OSPF ルーティングドメインに対するネットワークトポロジ情報の交換を制限するセキュリティメカニズムです。MD5 キーとパスワードを設定します。

L3 Features > MD5 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。

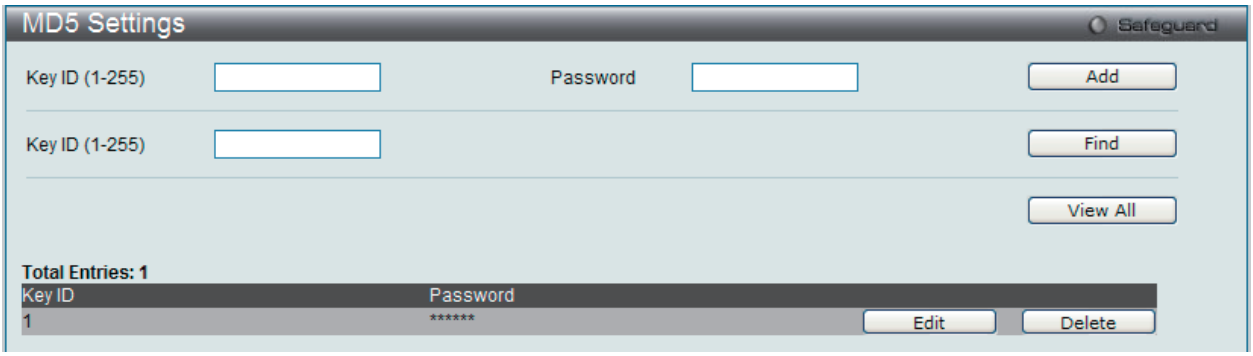


図 10-86 MD5 Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Key ID	MD5 キーを識別する 1-255 の数字を指定します。
Password	16 文字までの文字列を入力します。大文字、小文字は区別されます。このキーは OSPF ルーティングドメインでの OSPF パケットの認証に順番に使用されます。

「Add」ボタンをクリックして、新しい Key ID をパスワード共に追加します。
「Find」ボタンをクリックすると、入力した Key ID を検索します。
「View All」ボタンをクリックして、すべてのエントリを表示します。

エントリの編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

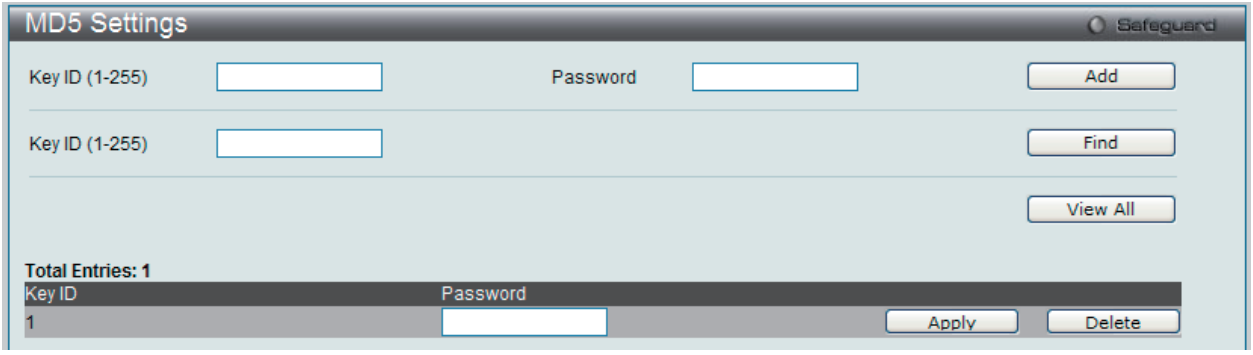


図 10-87 MD5 Settings – Edit 画面

2. エントリの編集を行い、「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。

第 11 章　QoS（QoS 機能の設定）

以下は QoS の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）	273
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）	275
Traffic Control （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。	277
DSCP（DSCP 設定）	DSCP を設定します。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）	278
HOL Blocking Prevention （HOL ブロッキング防止）	HOL ブロッキング防止機能を有効または無効にします。	279
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。 Scheduling Profile Settings（スケジュールプロファイル設定）、Scheduling Group Settings（スケジューリンググループ設定）	280

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。

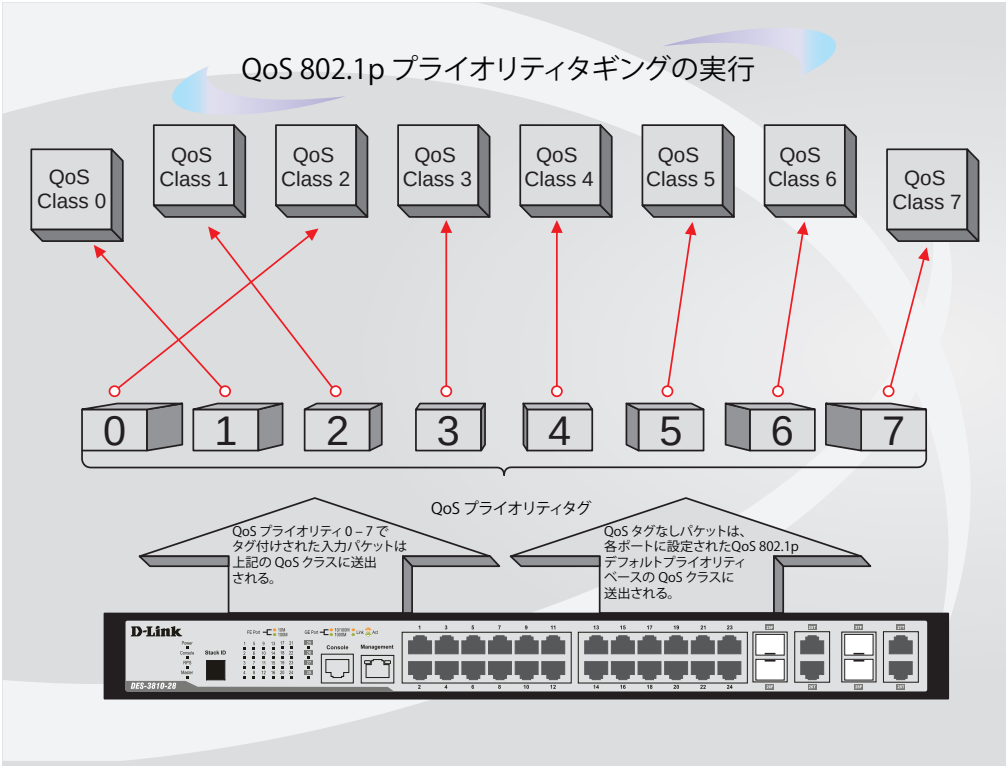


図 11-1　スイッチ上での QoS マッピングの例

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、スイッチ上の 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。

本スイッチは、スイッチ上の各ポートに 8 つのプライオリティキュー (と 8 つの CoS) を持っています。

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。

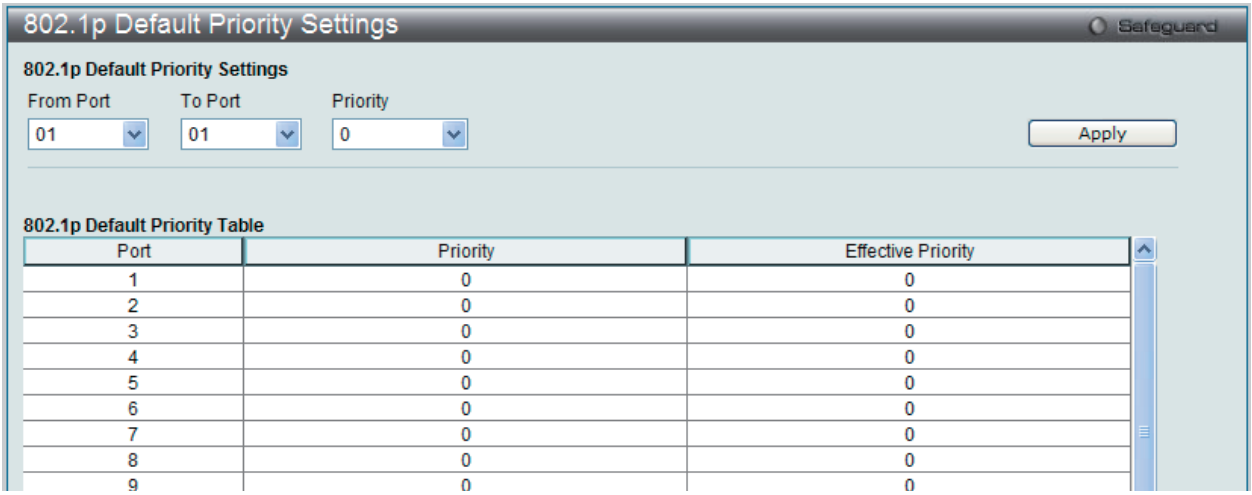


図 11-2　802.1p Default Priority Settings 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	本設定に使用するポートリストを指定します。
Priority	選択ポートに適用するプライオリティ値を指定します。オプションを 0-7 からを選択します。

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。

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。

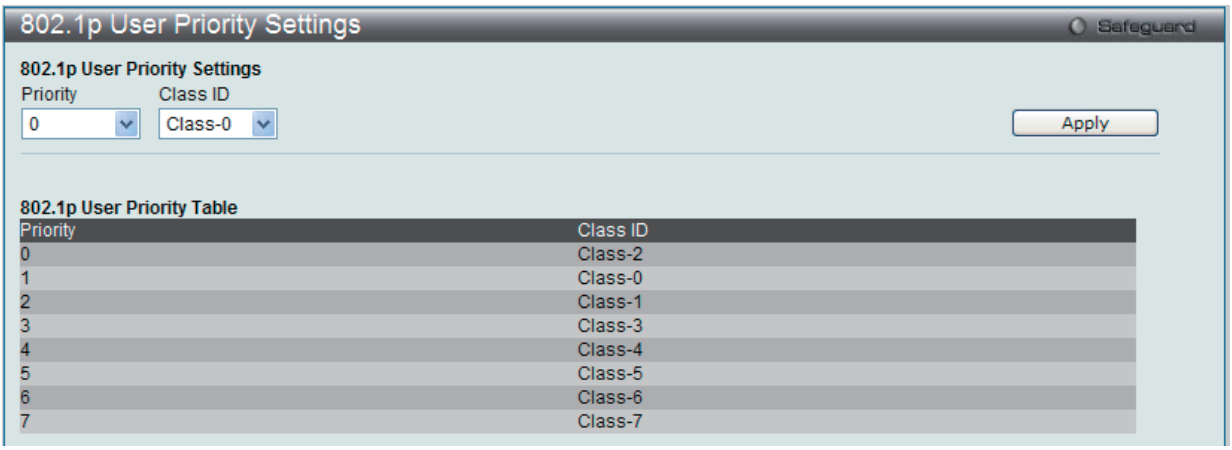


図 11-3　802.1P User Priority Settings 画面

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	選択した Class ID に適用するプライオリティ値を指定します。
Class ID	使用する Class ID を入力します。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。

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。

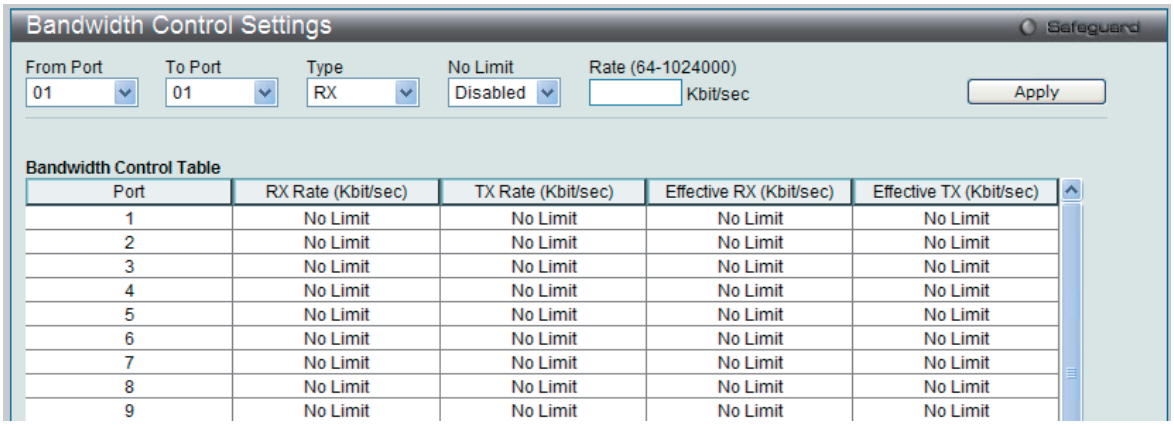


図 11-4　Bandwidth Control Settings 画面

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。

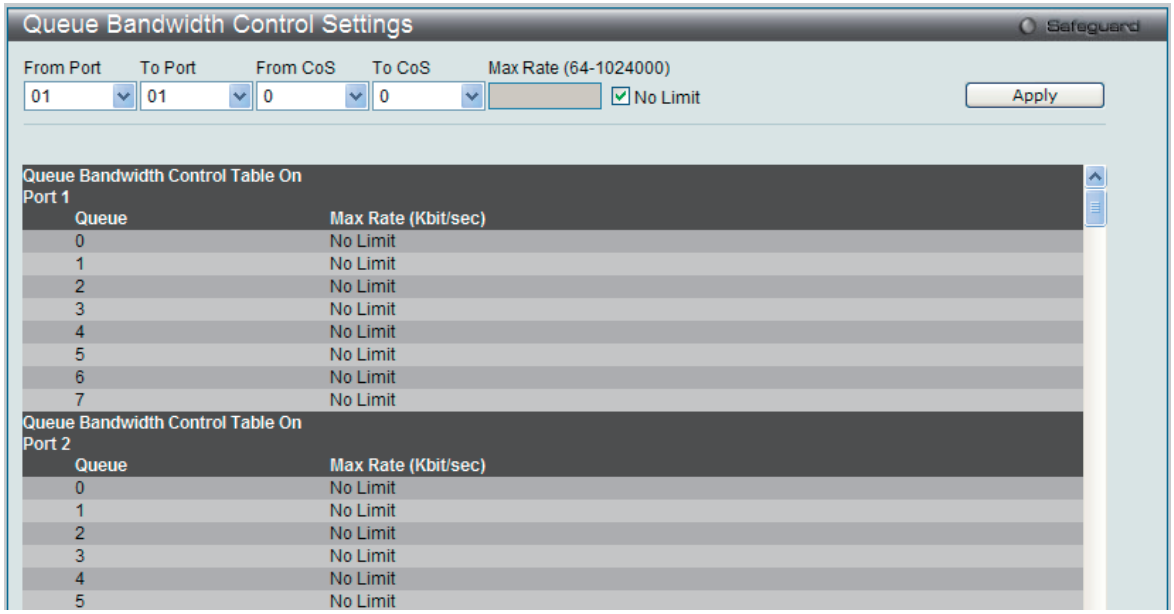


図 11-5　Queue Bandwidth Control Settings 画面

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 CoS / To CoS	この設定に使用するキュー範囲を選択します。
Max Rate	キューの最大速度を入力します。「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 1.85Mbps です。システムは自動的に 1850 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** 画面で手動で有効状態に戻すか、または 5 分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 の順にクリックし、以下の画面を表示します。

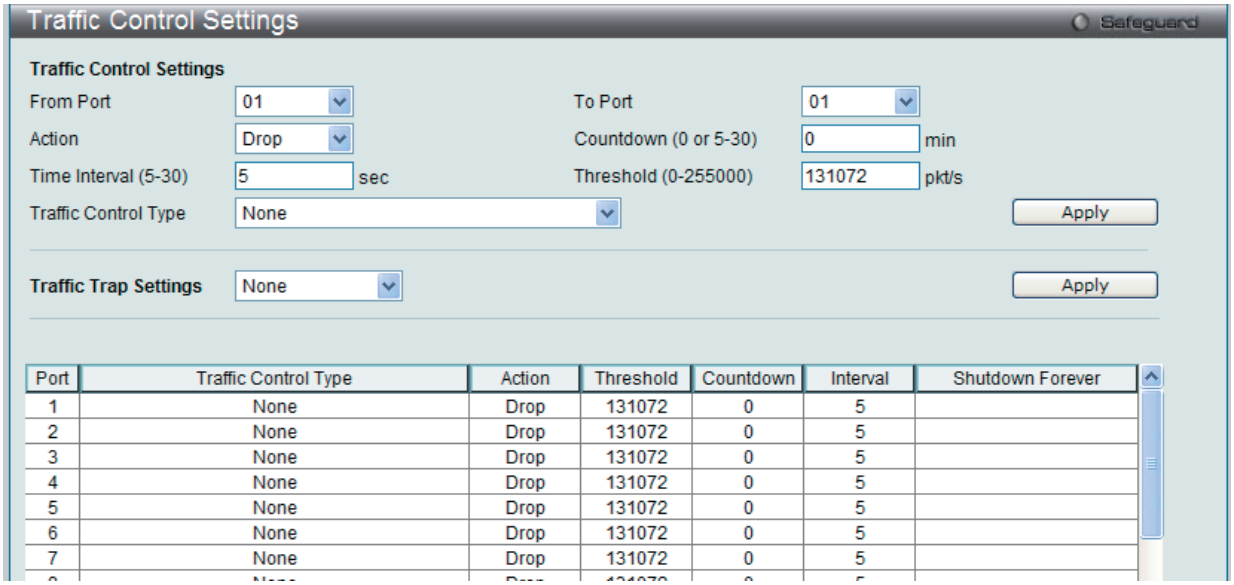


図 11-6　Traffic Control Settings 画面

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 – ハードウェアトラフィックコントロールメカニズムを使用します。スイッチのハードウェアがしきい値に基づき収束するまでパケットを破棄します。 • 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。
Count Down (0 or 5-30)	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」フィールドで「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、5-30(分) が指定できます。0 は、ポートが「Shutdown Rest」モードに入らないことを意味します。
Time Interval (5-30)	マルチキャストやブロードキャストのパケット数をチップからトラフィックコントロール機能に渡す間隔を指定します。これらのパケット数により受信パケットがしきい値を超えているかを決定します。5-30 (秒) まで指定でき、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 130560 パケット / 秒です。

項目	説明
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 - トラフィックコントロールメカニズムの動作に関わらず、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」フィールドで「Drop」が選択された時) は実行できません。

「Apply」ボタンをクリックし、各項目の変更を適用します。

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 最小のストームコントロールしきい値のグラニュラリティ : FE ポートは 500pps、GE ポートは 640pps 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。

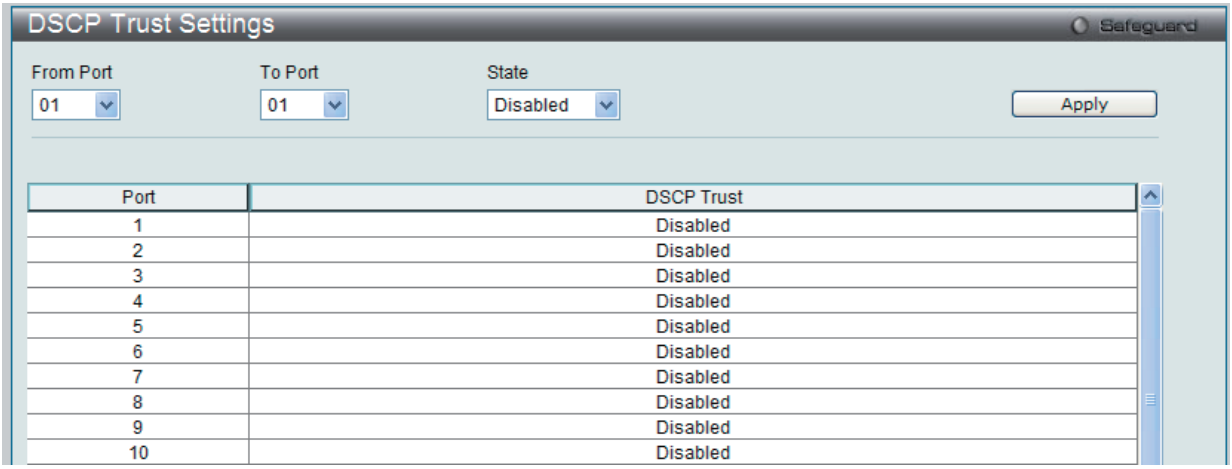


図 11-7　DSCP Trust Settings 画面

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。

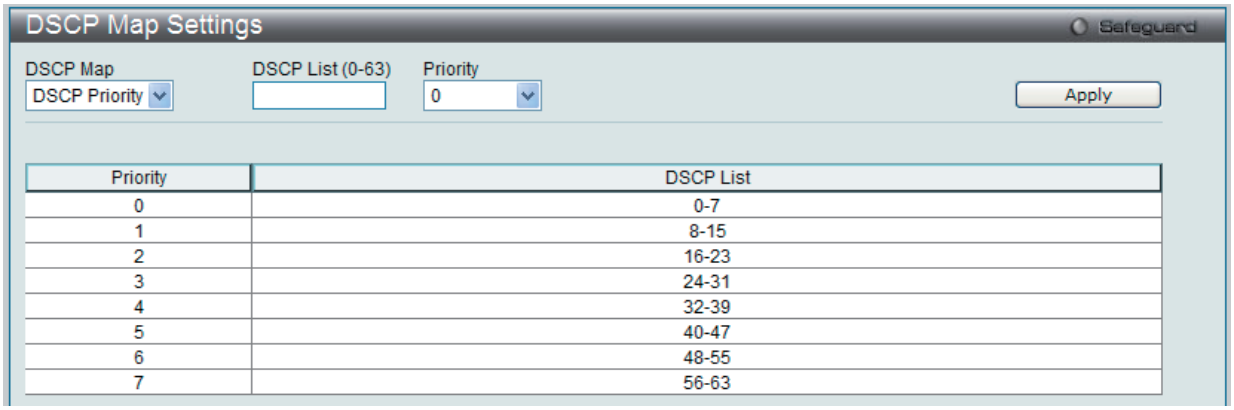


図 11-8　DSCP Map Settings 画面

本画面には次の項目があります。

項目	説明
DSCP Map	2 つのオプションの 1 つを選択します。 • DSCP Priority - 指定プライオリティにマップされる 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 List	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。

「Apply」ボタンをクリックして行った変更を適用します。

HOL Blocking Prevention（HOL ブロッキング防止）

HOL (Head of Line) ブロッキングはブロードキャストまたはマルチキャストパケットの送信先ポートの 1 つが使用中である場合に発生します。スイッチはバッファにこのパケットを保持し、一方他の送信先ポートは使用中でなくてもパケットを送信しません。HOL ブロッキング防止機能は、より低い待ち時間と、より高い性能を持つために、使用中のポートを無視して、直接パケットを転送します。HOL ブロッキング防止機能を有効または無効にします。

QoS > HOL Blocking Prevention の順にクリックし、以下の画面を表示します。

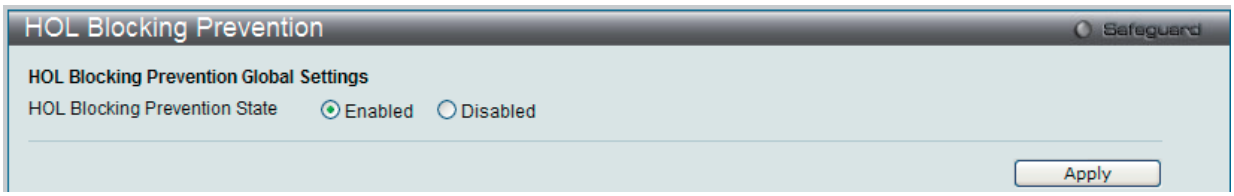


図 11-9　HOL Blocking Prevention 画面

HOL ブロッキング防止のグローバル設定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。

Scheduling Settings（スケジュール設定）

Scheduling Profile Settings（スケジュールプロファイル設定）

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

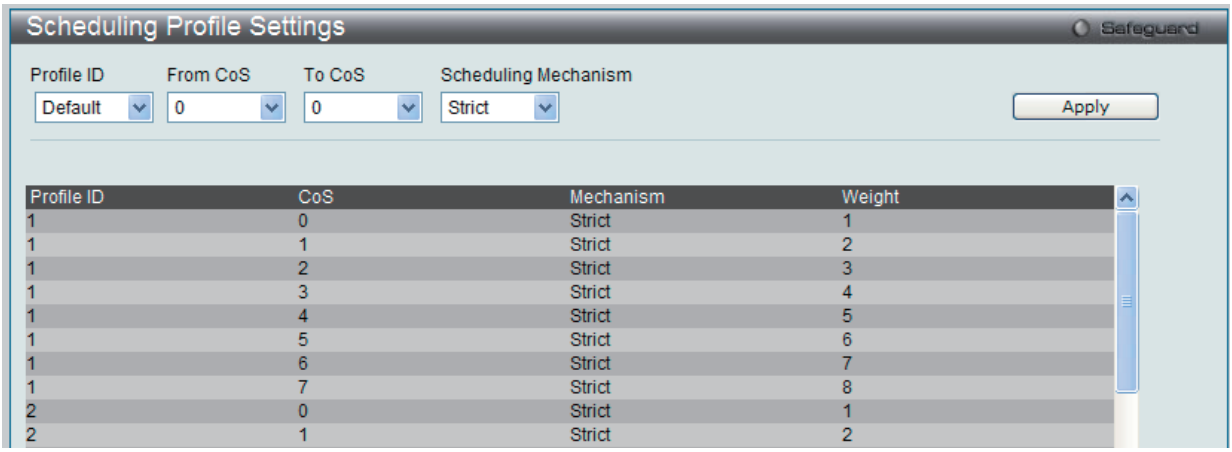


図 11-10 Scheduling Profile Settings 画面

本画面には以下の項目があります。

項目	説明
Profile ID	設定するプロファイル ID を選択します。
From CoS / To CoS	設定する CoS の範囲を選択します。
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 - キューが strict モードで動作します。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 - 重み付けラウンドロビンに設定します。1 から n の間の値を指定します。ポートモードが WRR であると、WRR モードで動作します。ポートモードが Strict であると、Strict モードで動作します。n の値はプロジェクトによって異なります。

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。

Scheduling Group Settings（スケジューリンググループ設定）

スケジューリンググループパラメータを設定します。

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

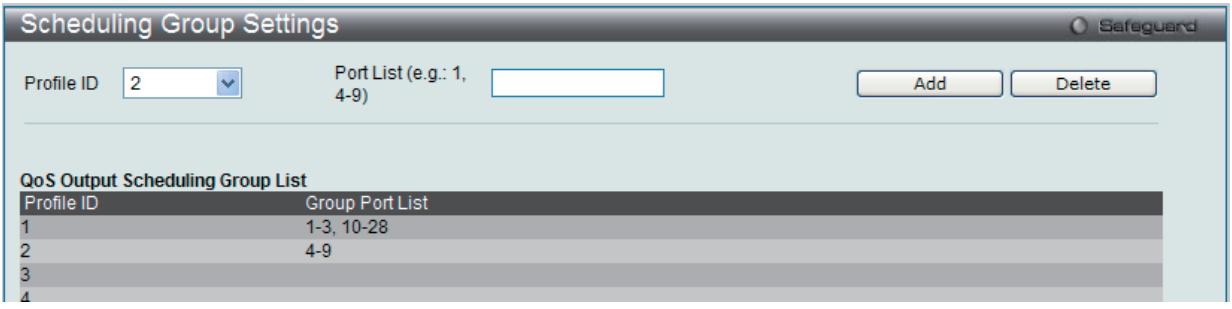


図 11-11 Scheduling Group Settings 画面

本画面には以下の項目があります。

項目	説明
Profile ID	設定するプロファイル ID を選択します。
Port List	設定するポート範囲を選択します。

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。

「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、入力した情報に基づいて指定エントリを削除します。

第 12 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 の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。	281
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。	283
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。	299
ACL Finder（ACL 検索）	ACL エントリを検索します。	314
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。	315
Egress Access Profile List（Egress アクセスプロファイルリスト）	フローごとのパケット処理を実行します	319
Egress ACL Flow Meter（Egress ACL フローメータリング）	Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。	333

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。

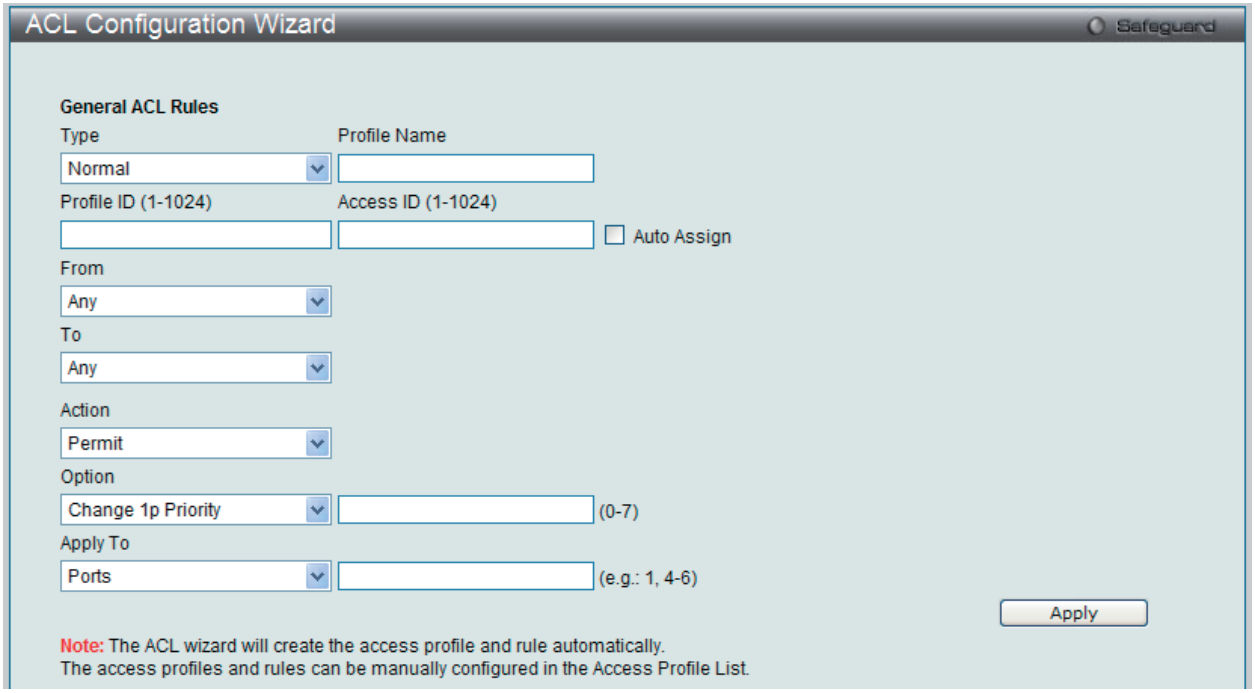


図 12-1　ACL Configuration Wizard 画面

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 (1-1024) と Access ID (1-1024) 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 IP 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	作成する ACL の種類を 3 つの一般的な ACL タイプから選択します。 • 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」または「Egress」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 (1-1024)	新しいルールに対するプロファイル ID を入力します。
Access ID (1-1024)	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。
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。
Service Type	「From / To」欄でサブジェクトを選択した後、以下のサービスの 1 つを選択することができます。 •「IPv4 Address」を選択した場合 - Any - このルールをすべてのサービスタイプに適用します。 - ICMP All - このルールにすべての ICMP トラフィックを適用します。 - IGMP - このルールに ICMP トラフィックを適用します。 - TCP All - このルールにすべての TCP トラフィックを適用します。 - TCP Source Port - このルールに TCP トラフィックを適用します。 - TCP Destination Port - このルールに送信先ポートからの TCP トラフィックだけを適用します。 - UDP All - このルールにすべての UDP トラフィックを適用します。 - UDP Source Port - このルールに送信元ポートからのすべての UDP トラフィックを適用します。 - UDP Destination Port - このルールに送信先ポートからのすべての UDP トラフィックを適用します。 - VLAN Mask (Name) - このルールに VLAN 名を適用します。 •「IPv6」を選択した場合 - Any - このルールをすべてのサービスタイプに適用します。 - Flow Label - このルールにフローラベルを適用します。 - Class - このルールに IPv6 クラスを適用します。 - TCP All - このルールにすべての TCP トラフィックを適用します。 - TCP Source Port - このルールに TCP トラフィックを適用します。 - TCP Destination Port - このルールに送信先ポートからの TCP トラフィックだけを適用します。 - UDP All - このルールにすべての UDP トラフィックを適用します。 - UDP Source Port - このルールに送信元ポートからのすべての UDP トラフィックを適用します。 - UDP Destination Port - このルールに送信先ポートからのすべての UDP トラフィックを適用します。 •「MAC Address」を選択した場合 - Any - このルールをすべてのサービスタイプに適用します。 - 802.1p - このルールに 802.1p プライオリティ値を適用します。 - VLAN Mask (Name) - このルールに VLAN 名を適用します。
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、余分なの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。

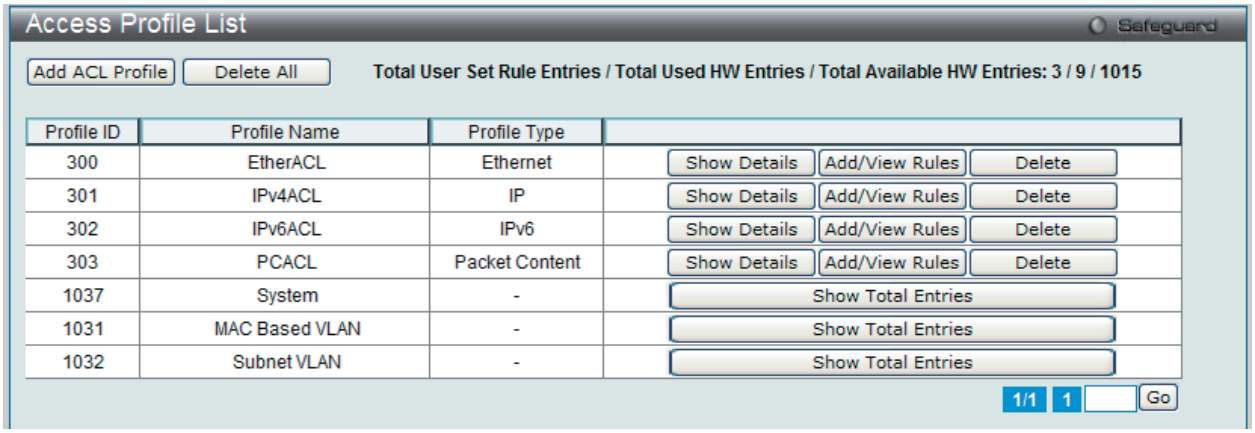


図 12-2　Access Profile List 画面

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。
Show Total Entries	使用されているハードウェアエントリの合計を参照します。
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およびパケットコンテンツマスクプロファイル設定用です。

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。

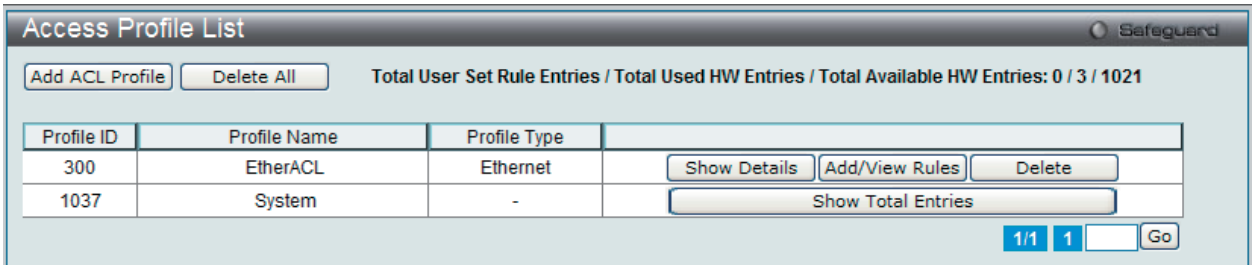


図 12-3　Access Profile List 画面

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

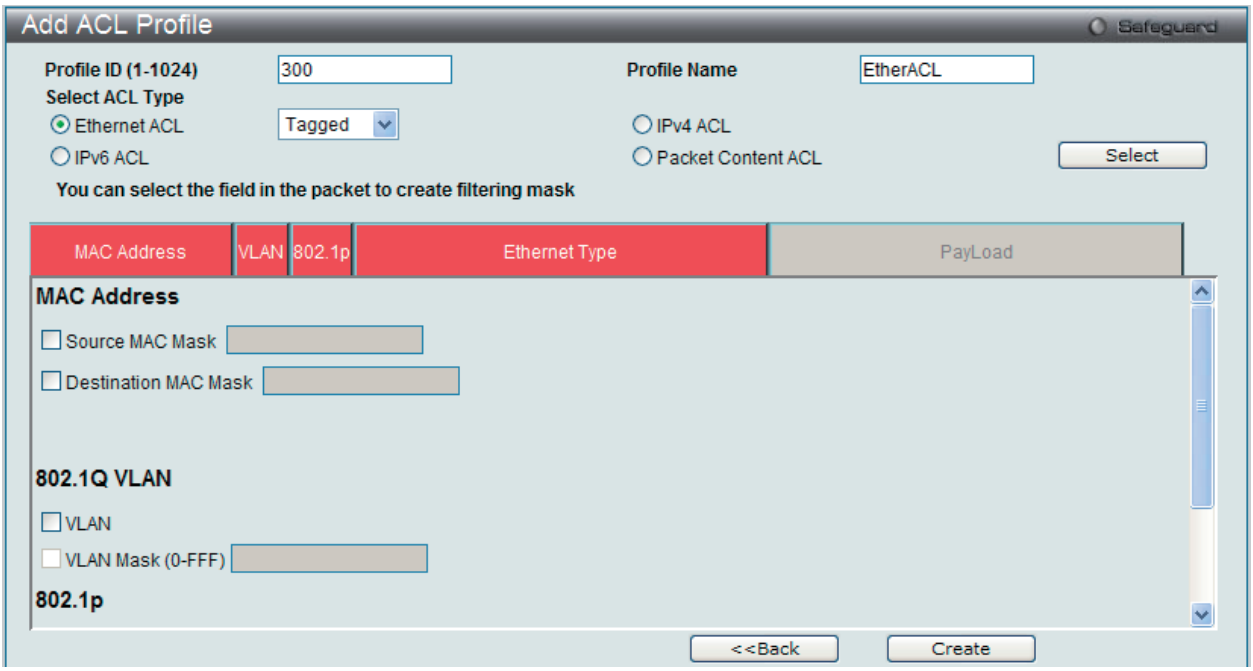


図 12-4　Add ACL Profile - Ethernet ACL 画面

「Profile ID」でプロファイル番号を 1-1024 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 1024 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。 • 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 - 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。

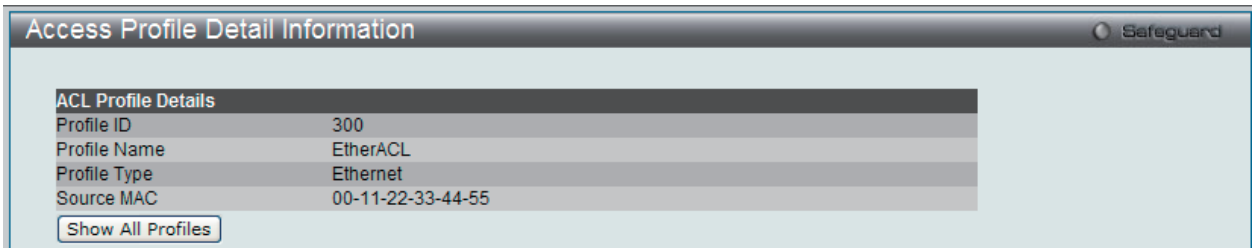


図 12-5　Access Profile Detail Information - Ethernet 画面

「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。

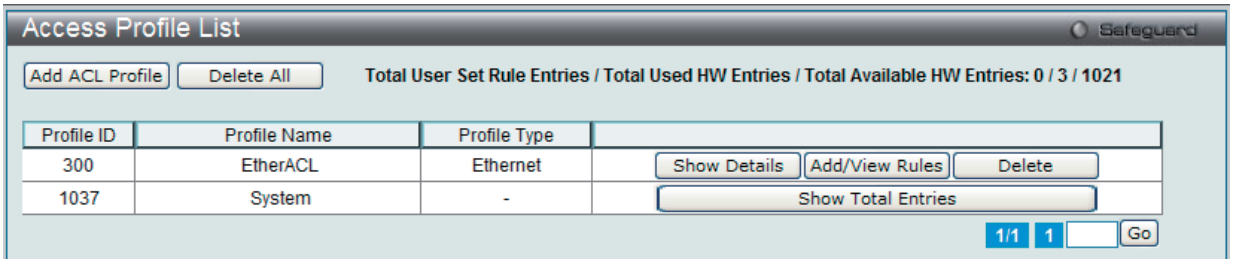


図 12-6　Access Profile List 画面

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。

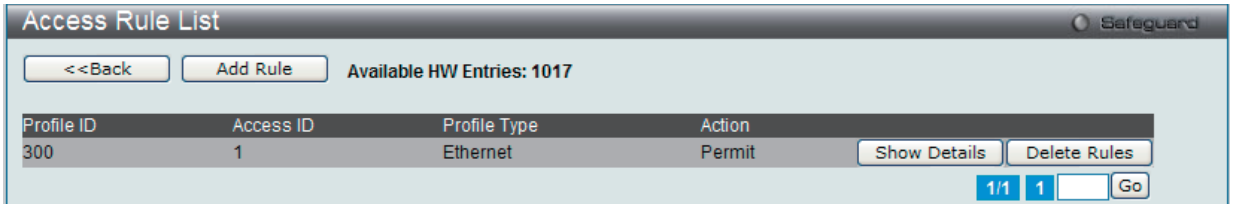


図 12-7　Access Rule List - Ethernet 画面

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。

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。

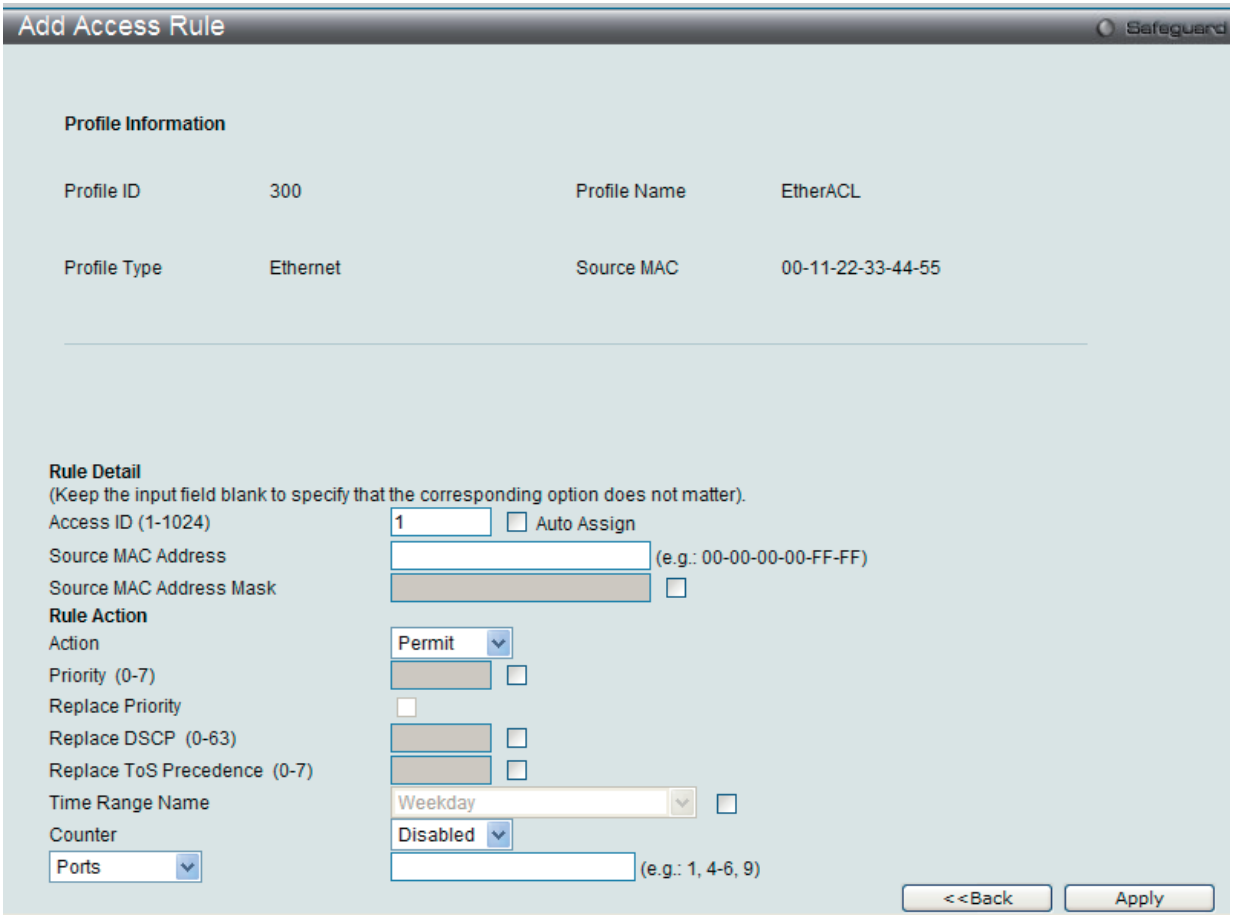


図 12-8　Add Access Rule - Ethernet 画面

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 (1-1024)	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 1024 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 (0-FFF)	VLAN マスク値 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 - 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271 ページの「第 11 章　QoS（QoS 機能の設定）」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	使用するポートリストを入力します。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。「All Ports」をチェックすると、スイッチのすべてのポートを選択できます。
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 - 使用するポートリストを入力します。 • 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。
「<<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。

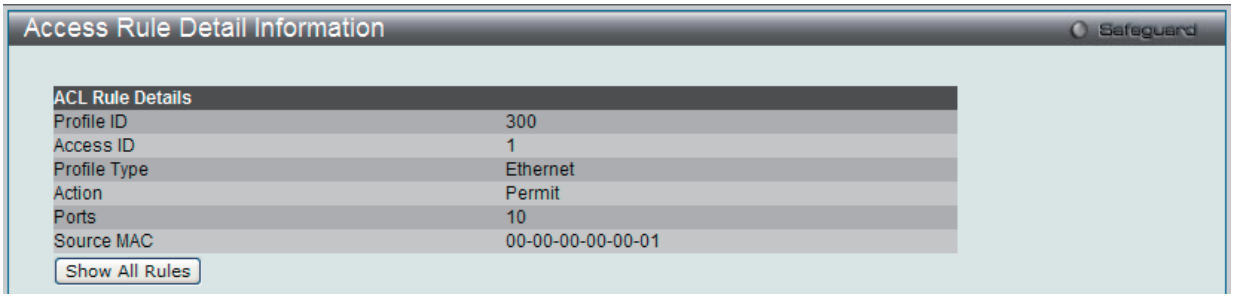


図 12-9　Access Rule Detail Information - Ethernet 画面

「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。

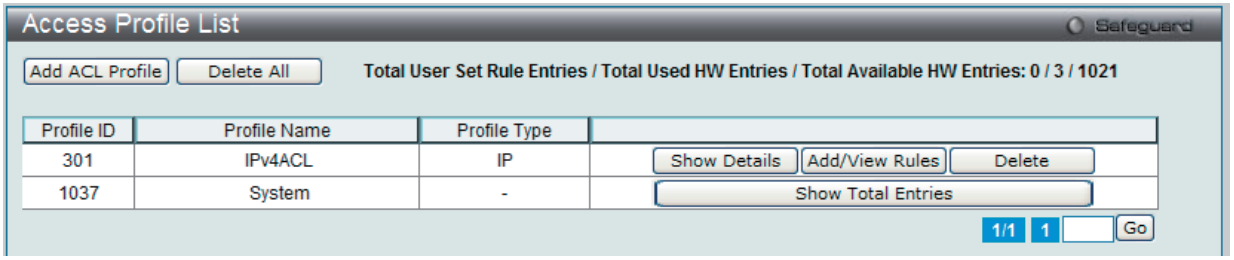


図 12-10　Access Profile List 画面

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。

IPv4 の「Add ACL Profile」画面

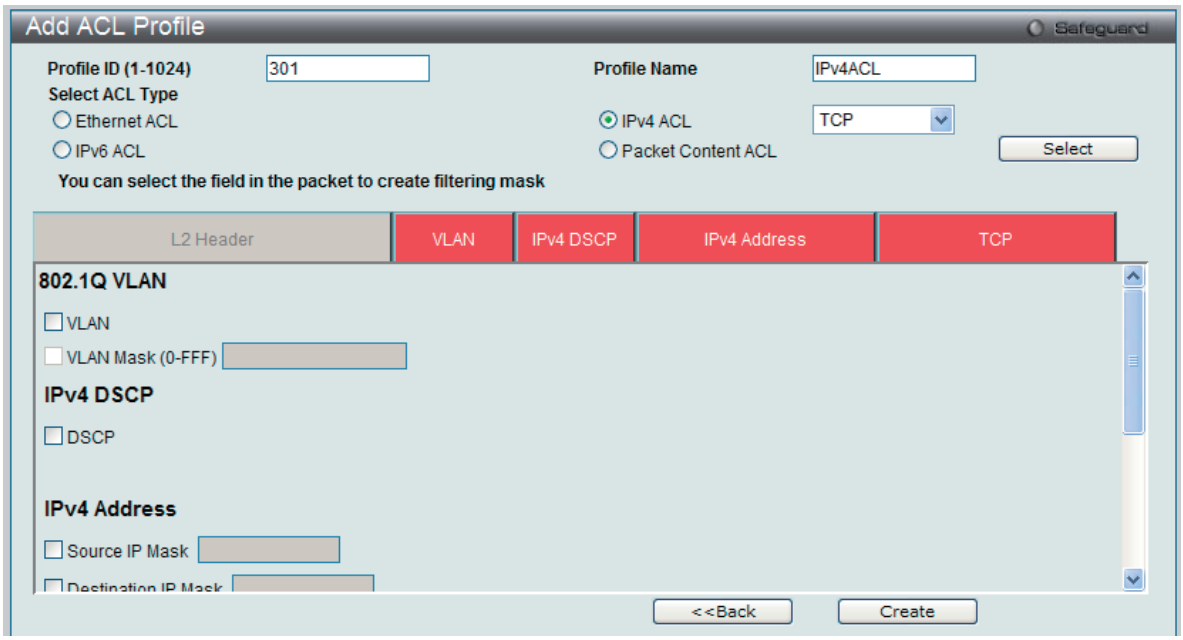


図 12-11　Add ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-1024 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 1024 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の TCP ポートマスクを 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の TCP ポートマスクを 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の UDP ポートマスクを 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の UDP ポートマスクを 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（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。

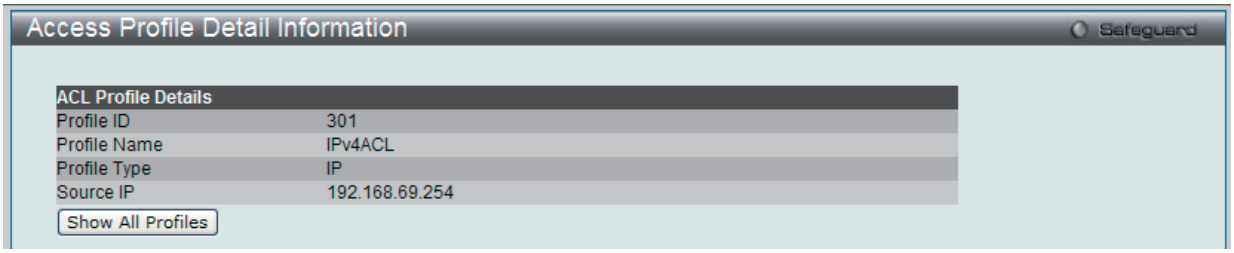


図 12-12 Access Profile Detail Information - IPv4 画面

「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。

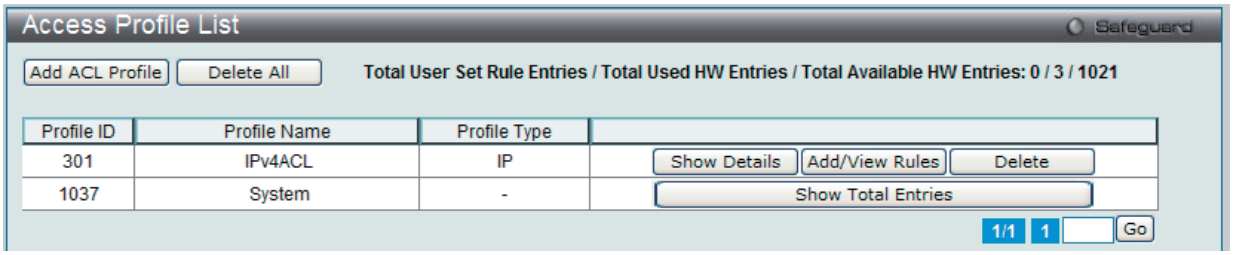


図 12-13 Access Profile List 画面

2. 「Access Profile List」画面を表示し、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。

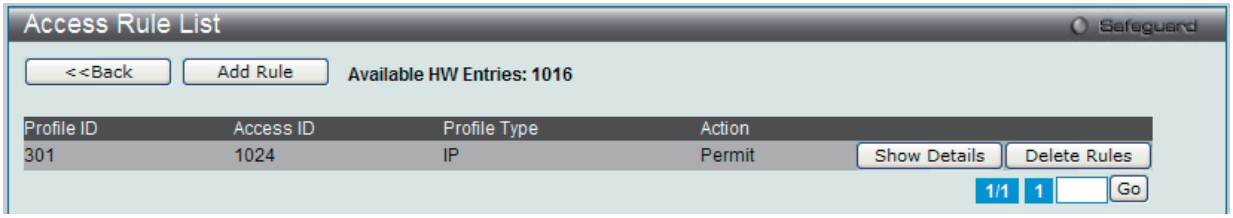


図 12-14 Access Rule List - IPv4 画面

「<<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。

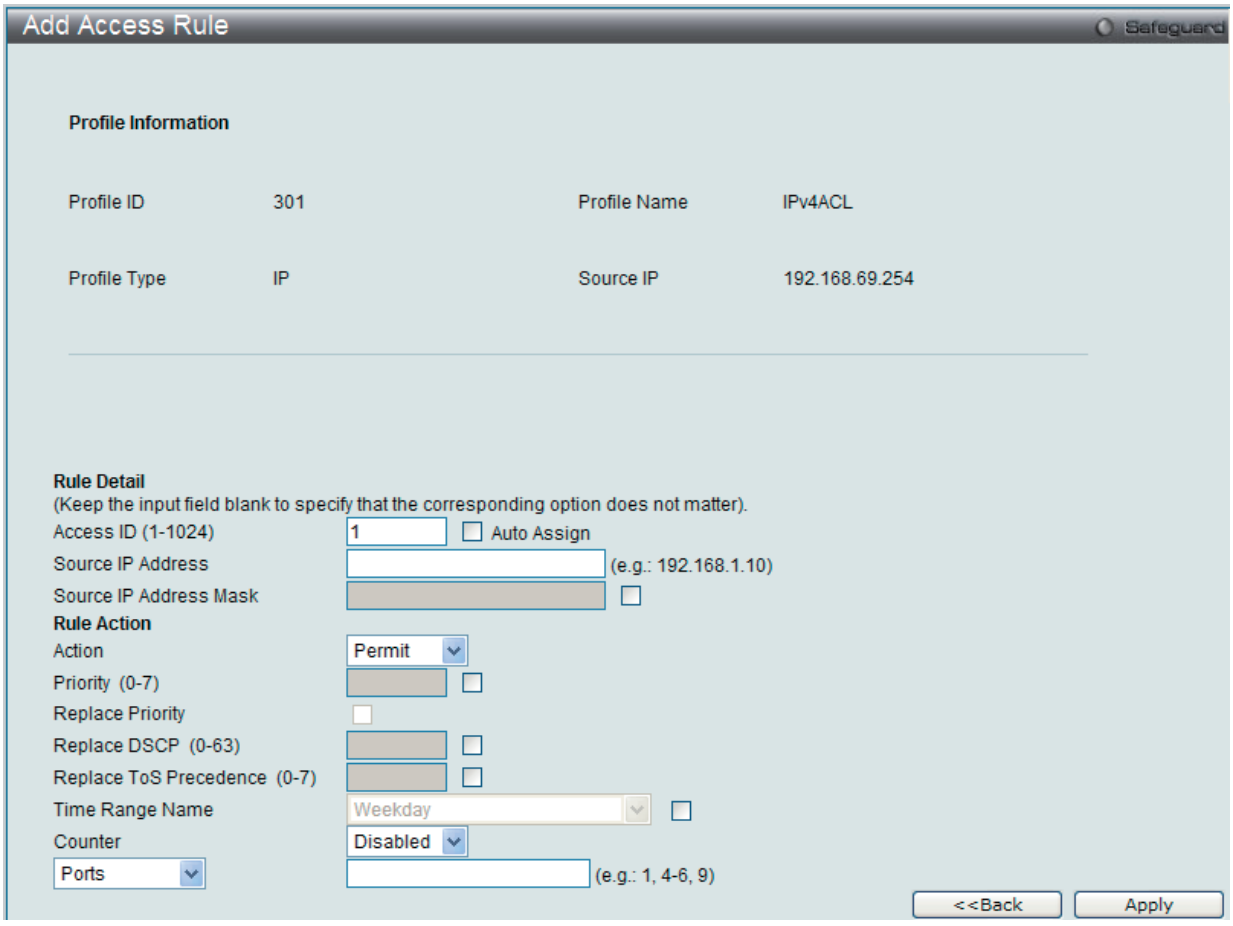


図 12-15 Add Access Rule - IPv4 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-1024)	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 1024 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(1-4094)	VLAN ID を入力します。「Mask」（0-FFF）にマスク値を入力します。
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 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 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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）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の UDP ポートマスクを 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の UDP ポートマスクを 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 271 ページの「第 11 章　QoS（QoS 機能の設定）」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。

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 - 使用するポートリストを入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

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。

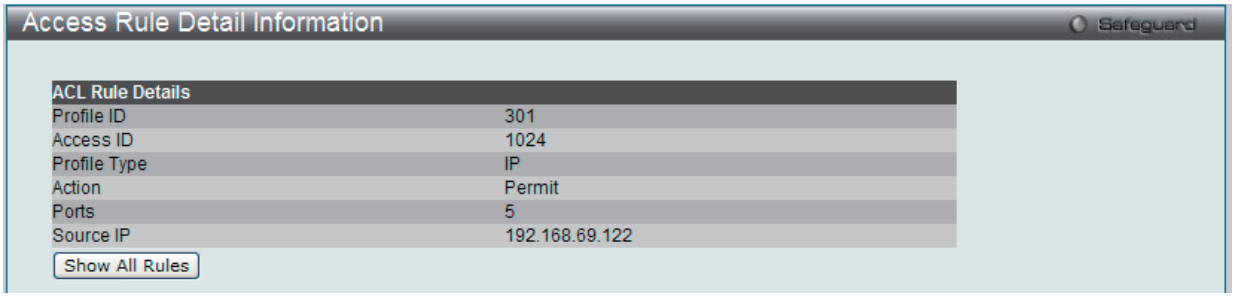


図 12-16　Access Rule Detail Information - IP 画面

「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。

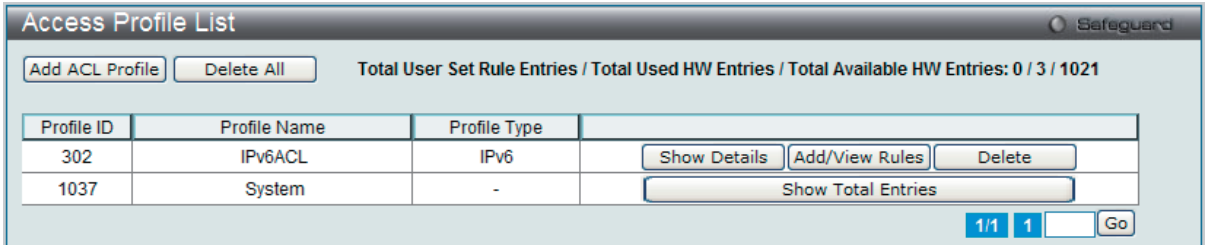


図 12-17　Access Profile List 画面

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

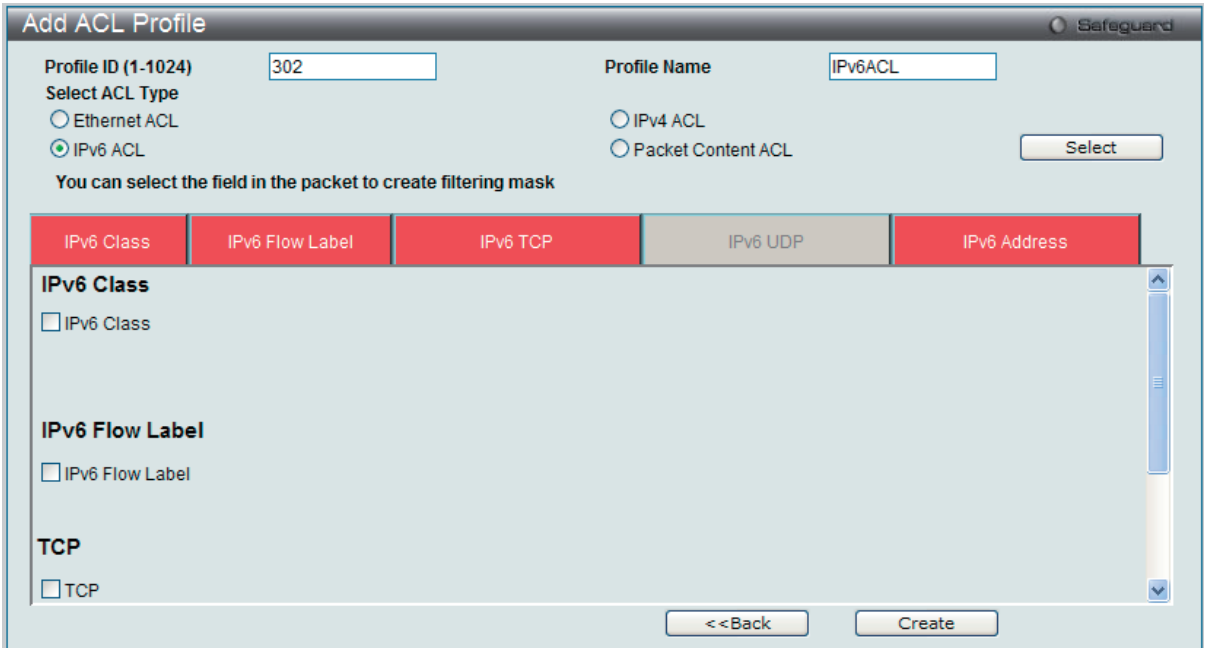


図 12-18　Add ACL Profile - IPv6 ACL 画面

「Profile ID」でプロファイル番号を 1-1024 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 1024 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。
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) - フィルタリングしたい送信先ポートの TCP ポートマスクを 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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）で指定します。
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) - フィルタリングしたい送信元ポートの UDP ポートマスクを 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の UDP ポートマスクを 16 進数（hex 0x0-0xffff）で指定します。
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。

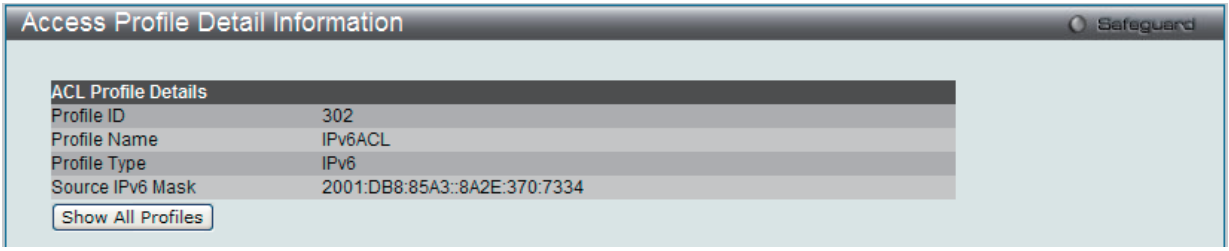


図 12-19　Access Profile Detail Information - IPv6 ACL 画面

「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。

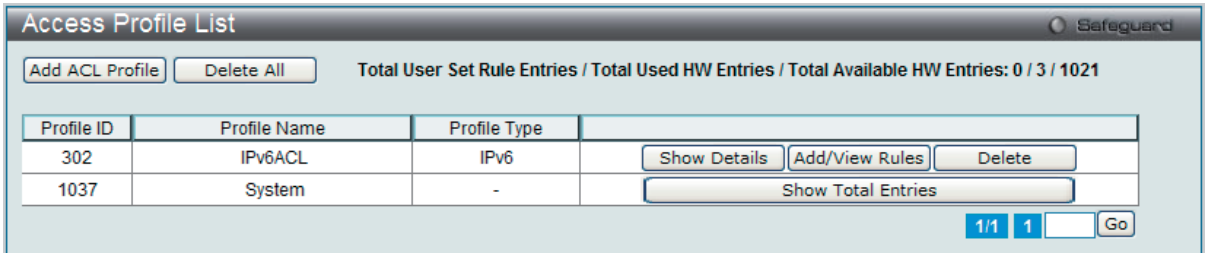


図 12-20　Access Profile List 画面

2. 「Access Profile List」画面を表示し、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。

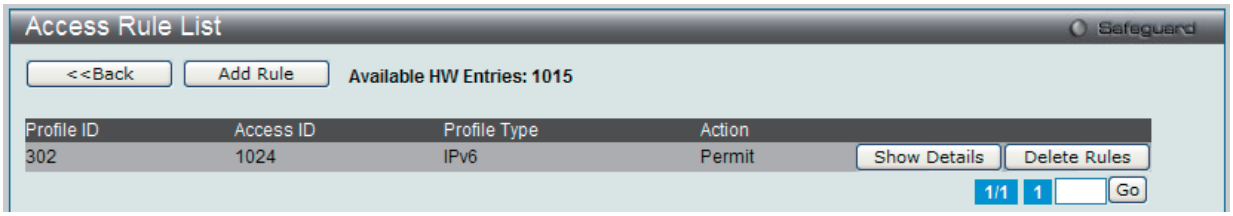


図 12-21　Access Rule List - IPv6 画面

「<<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。

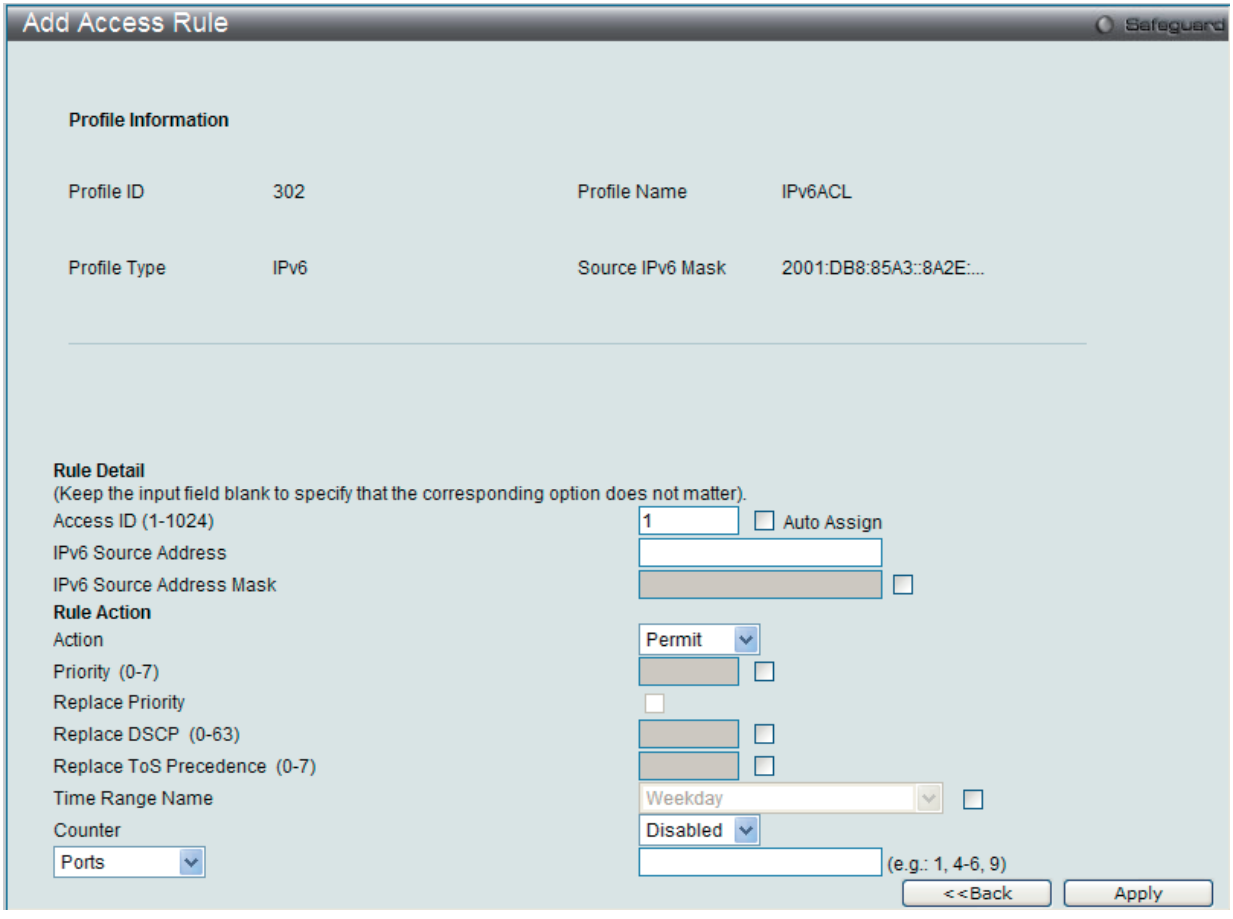


図 12-22　Add Access Rule - IPv6 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-1024)	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 1024 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	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	IPv6 フローラベルマスクを指定します。0-FFFFF の範囲で指定します。
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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）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の UDP ポートマスクを 16 進数（hex 0x0-0xffff）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の UDP ポートマスクを 16 進数（hex 0x0-0xffff）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271 ページの「第 11 章　QoS（QoS 機能の設定）」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 - 使用するポートリストを入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

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。

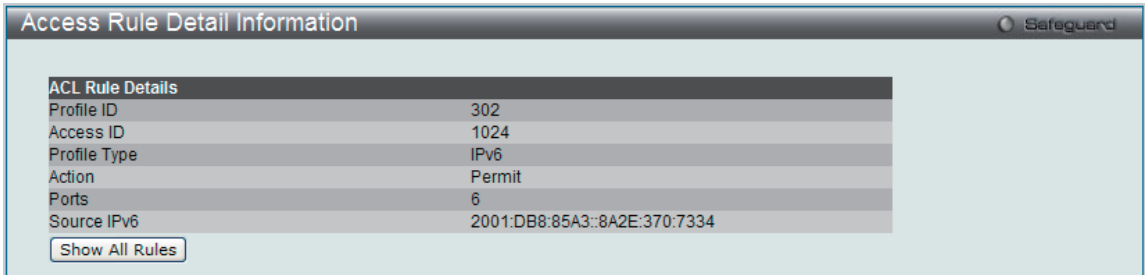


図 12-23　Access Rule Detail Information - IPv6 画面

「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。

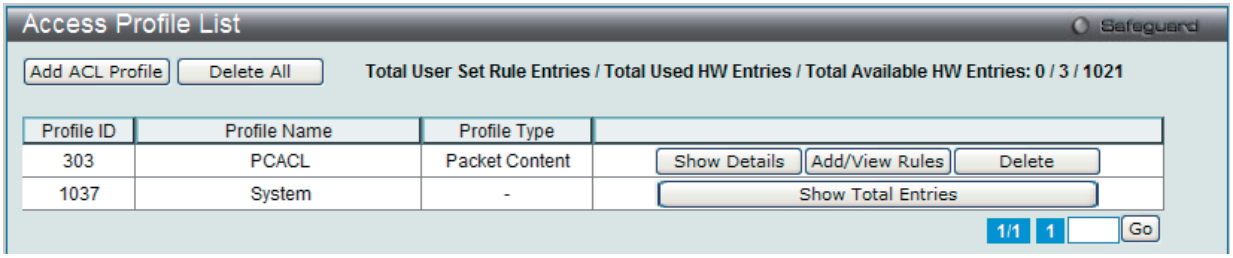


図 12-24　Access Profile List 画面

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。

パケットコンテンツの「Add ACL Profile」画面

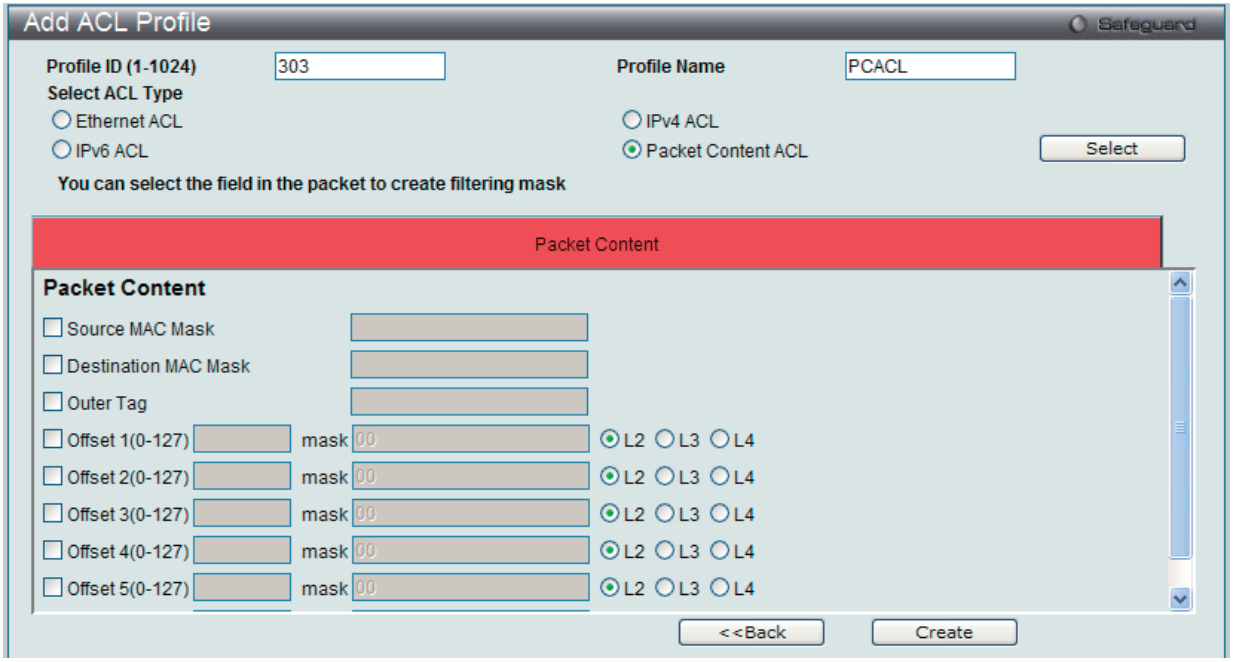


図 12-25　Add ACL Profile 画面 - パケットコンテンツ

「Profile ID」でプロファイル番号を 1-1024 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。

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 1024 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。 • 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。
Packet Content	• Source MAC Mask - 送信元 MAC マスクを指定します。 • Destination MAC Mask - 送信先 MAC マスクを指定します。 • Outer Tag - マスクするパケット外側 VLAN タグを指定します。これは 12 ビットの VID フィールドだけで構成します。 • Offset1, Offset2, Offset3, Offset4, Offset5, Offset6 - デバイスがフィルタする UDF フィールドを定義します。各 UDF フィールドは 1 バイトのデータから成っており、オフセットレファレンスから n バイト離れています。（n はオフセット値）オフセットの範囲は 0-127 です。オフセットレファレンスは以下のタイプの 1 つです。: - L2 - オフセットは VLAN タグの最後のバイトからカウントを開始します。（イーサタイプの開始） - L3 - オフセットはイーサタイプフィールドの直後からカウントを開始します。パケットには認識される有効な L2 ヘッダと認識可能なイーサタイプを持っている必要があります。 - L4 - オフセットは IP ヘッダの直後からカウントを開始します。パケットには認識される有効な IP ヘッダが必要です。

「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。

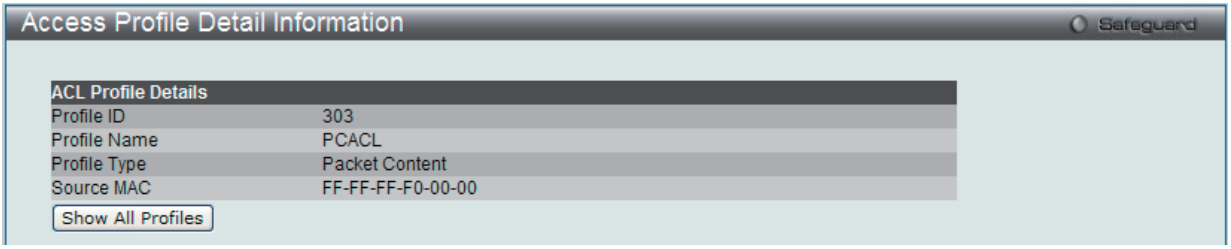


図 12-26 Access Profile Detail Information 画面 - パケットコンテンツ

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

注意 ARP(Address Resolution Protocol) は、ホストのハードウェアアドレス (MAC アドレス) を検索するための標準規格です。しかし、LAN を攻撃する (つまり、ARP スプーフィング攻撃) ために容易に利用できるため、ARP は被害を受けやすいという弱点があります。ARP プロトコルの動作方法、および ARP Spoofing 攻撃を防ぐために D-Link 独自のパケットコンテンツ ACL を使用する方法について本マニュアル最後にある 512 ページの「付録 F パスワードのリカバリ手順」を参照してください。

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。

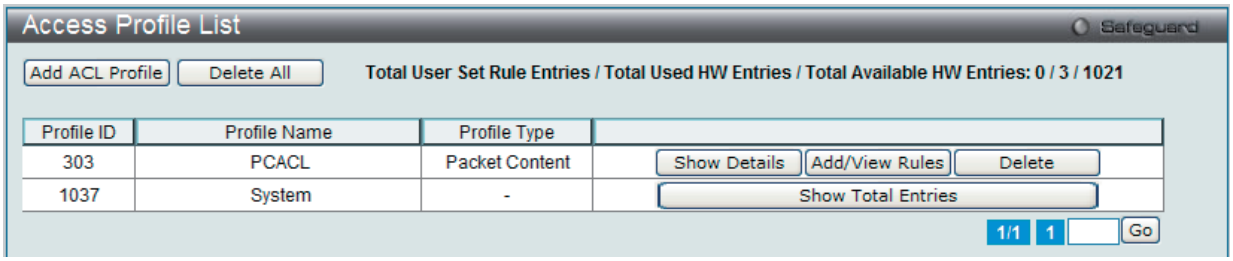


図 12-27　Access Profile List 画面

2. 「Access Profile List」画面を表示し、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。

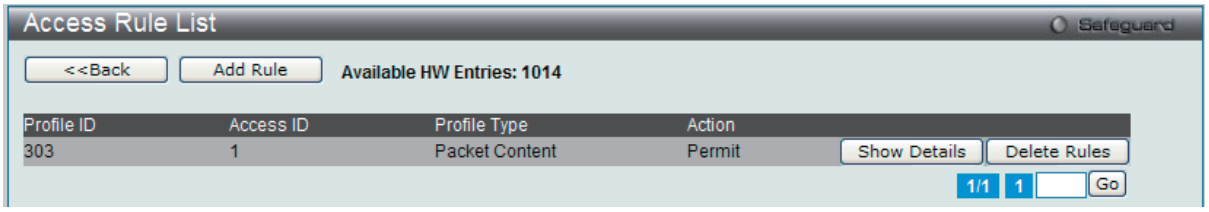


図 12-28　Access Rule List 画面 - パケットコンテンツ

「<<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。

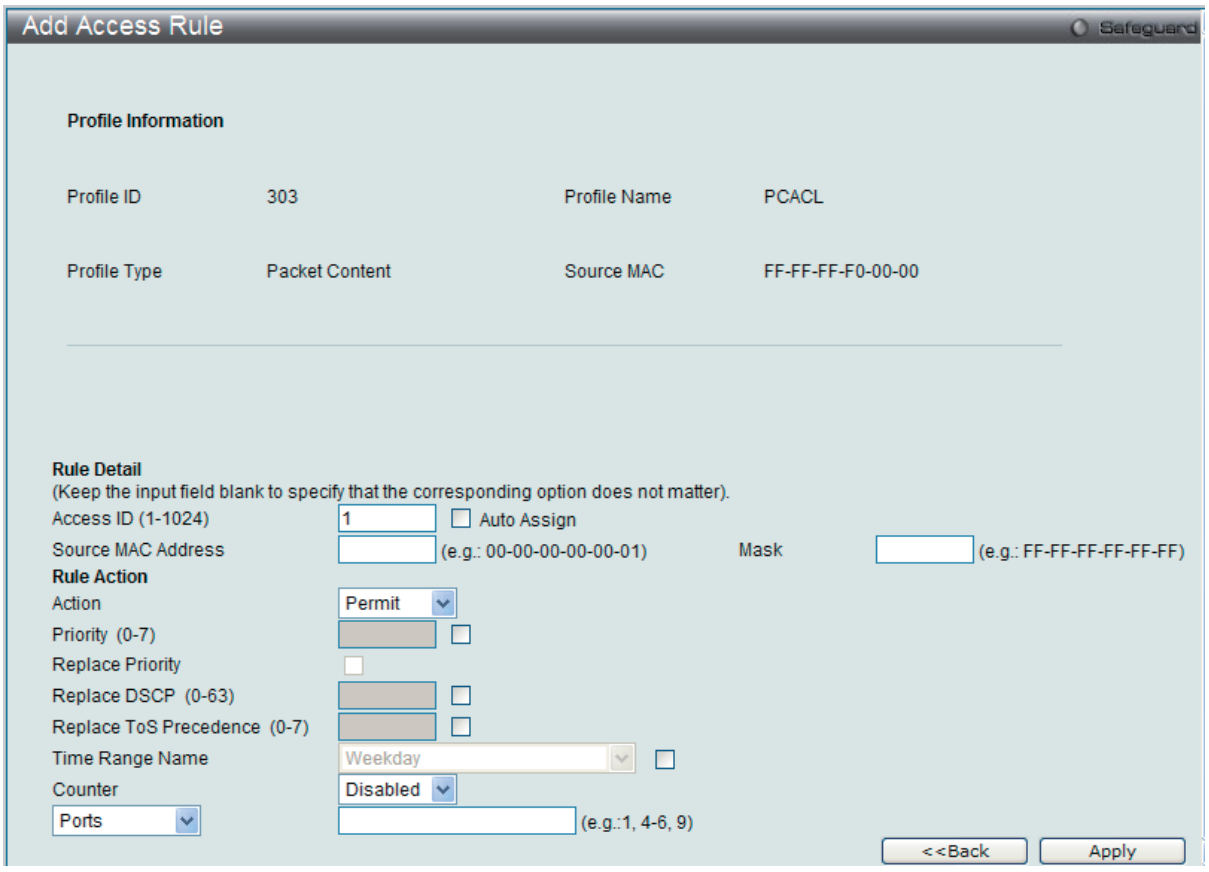


図 12-29　Add Access Rule 画面 - パケットコンテンツ

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-1024)	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 1024 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。
Source MAC Address	調べる必要のあるパケットの送信元 MAC アドレスを指定します。 • Mask - 送信元 MAC アドレスのマスクを指定します。このマスクと送信元 MAC アドレスの AND 演算の結果、フィルタリングを行います。
Destination MAC Address	調べる必要のあるパケットの送信先 MAC アドレスを指定します。 • Mask - 送信先 MAC アドレスのマスクを入力します。このマスクと送信先 MAC アドレスの AND 演算の結果、フィルタリングを行います。
Outer Tag	マスクするパケットの外側 VLAN タグを入力します。これは 12 ビットの VID フィールドだけで構成します。 • Mask - 使用する外側タグのマスク値を入力します。
Offset1-6	プロファイルに定義した各 UDF データフィールドに照合するデータを入力します。 • Mask - 使用す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271 ページの「第 11 章　QoS（QoS 機能の設定）」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 - 使用するポートリストを入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

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。

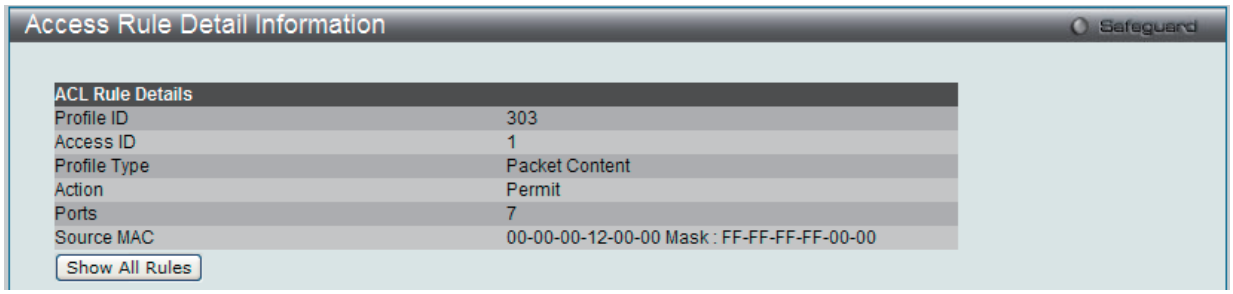


図 12-30　Access Rule Detail Information - パケットコンテンツ画面

「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、IP 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、この詳しい調査は許可されません。

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。

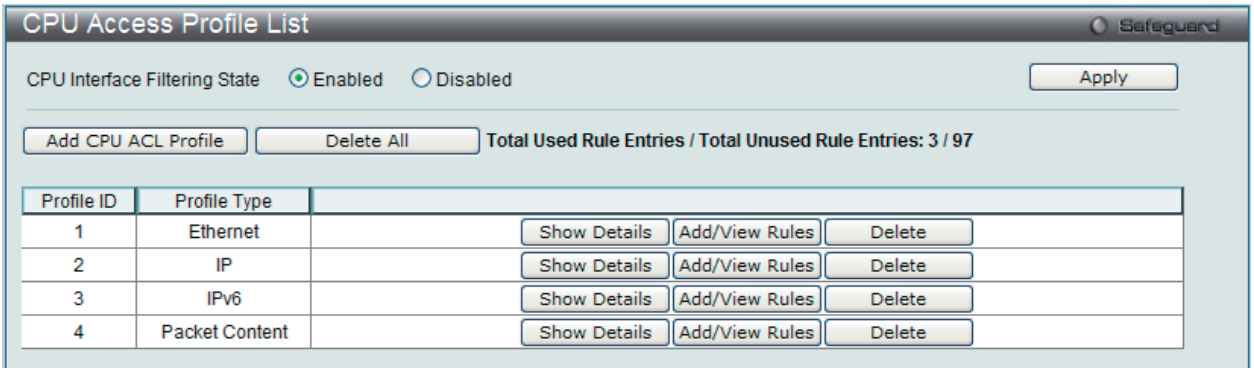


図 12-31 CPU Access Profile List 画面

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およびパケットコンテンツマスクプロファイル設定用です。

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。

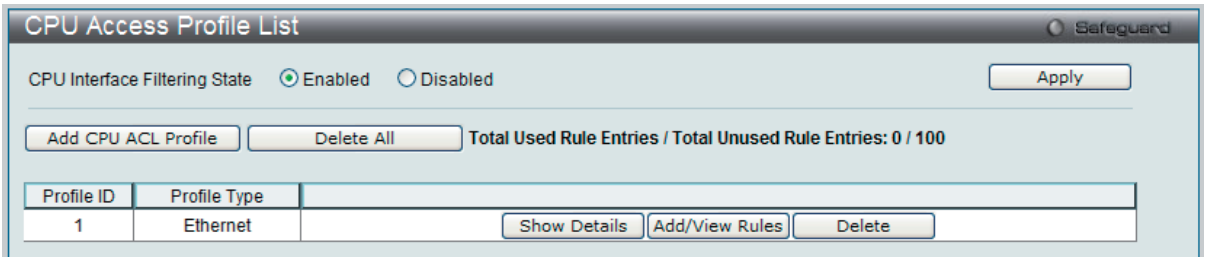


図 12-32　CPU Access Profile List 画面

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

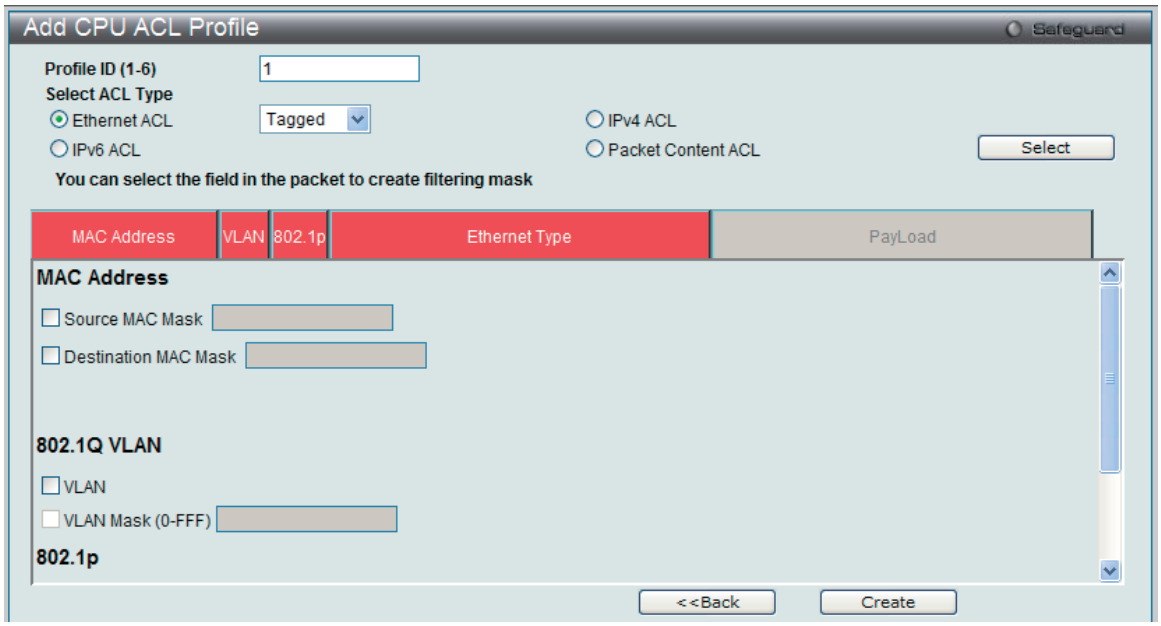


図 12-33　Add CPU ACL Profile - Ethernet 画面

「Add CPU ACL Profile」画面で「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
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 6 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。

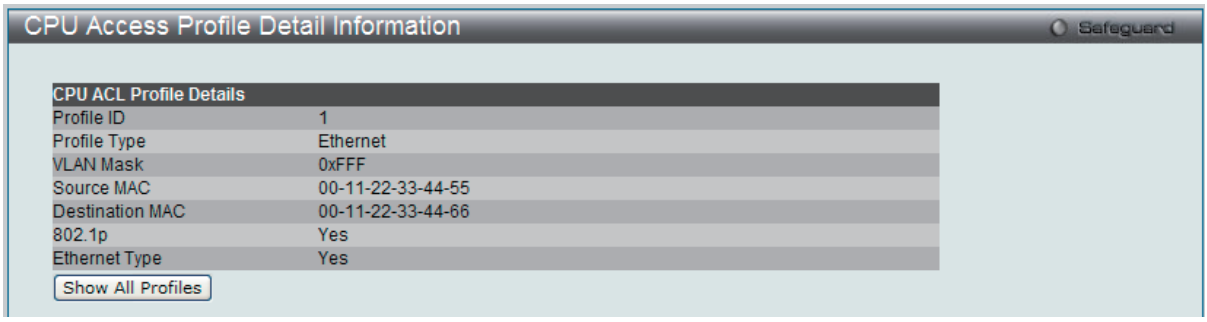


図 12-34 CPU Access Profile Detail Information - Ethernet 画面

「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 12-35 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、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。

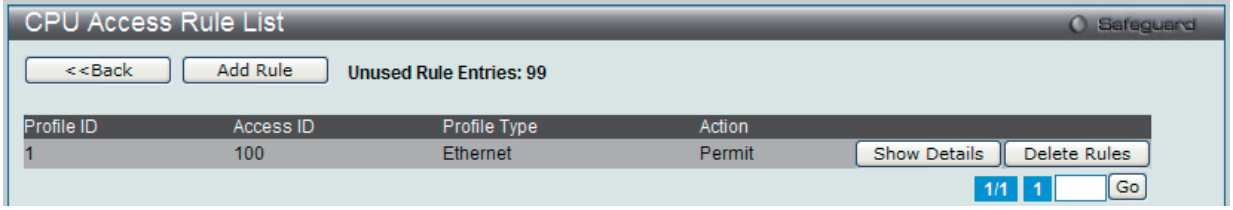


図 12-36 CPU Access Rule List - Ethernet 画面

「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。

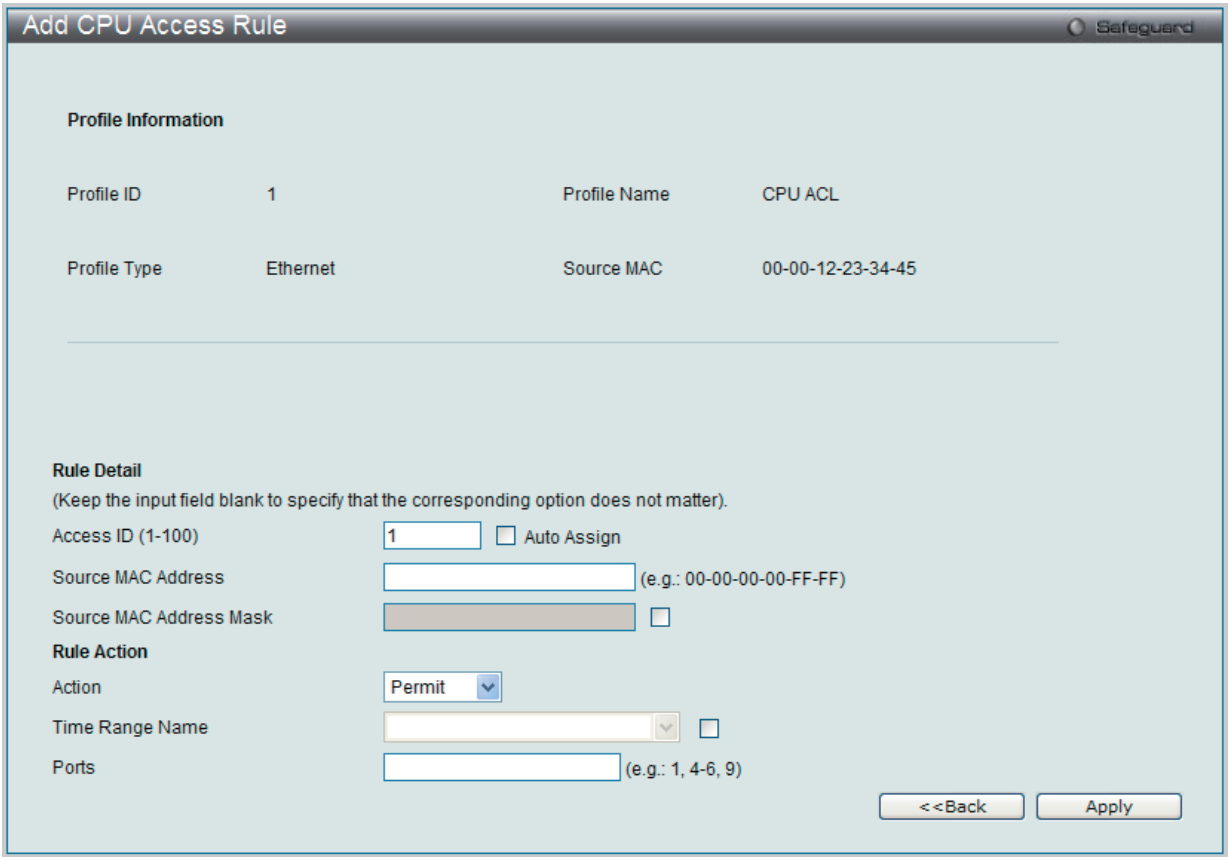


図 12-37　Add Access Rule - Ethernet 画面

以下の項目を設定します。

項目	説明
Rule Action	
Access ID (1-100)	本アクセスの識別番号を入力します。1 から 100 が指定できます。
VLAN Name	使用する VLAN 名を入力します。
VLAN ID	使用する VLAN ID を入力します。
VLAN Mask (0-FFF)	使用する VLAN マスク値を入力します。
Source MAC Address	使用する送信元 MAC アドレスを指定します。
Source MAC Address Mask	使用する送信元 MAC アドレスマスクを指定します。
Destination MAC Address	使用する送信先 MAC アドレスを指定します。
Destination MAC Address Mask	使用する送信先 MAC アドレスマスクを指定します。
802.1p (0-7)	使用する 802.1p 優先度タグ値を入力します。この値は 0-7 である必要があります。
Ethernet Type (0-FFFF)	使用するイーサネットタイプ値を入力します。
Rule Detail	
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。

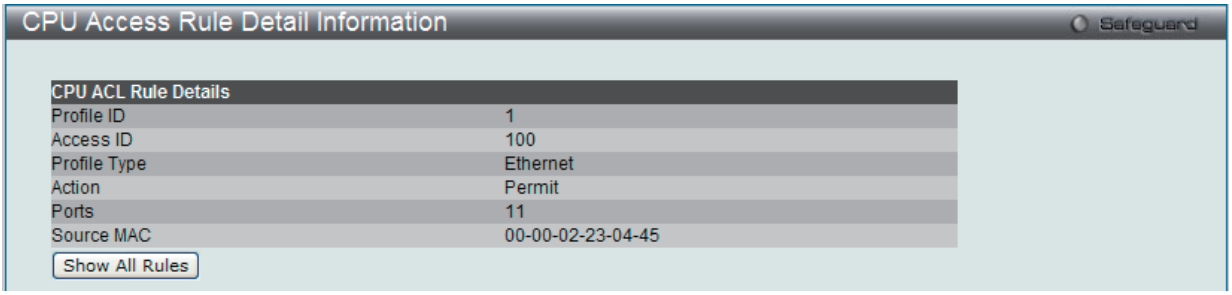


図 12-38 CPU Access Rule Detail Information - Ethernet 画面

「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 12-39 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

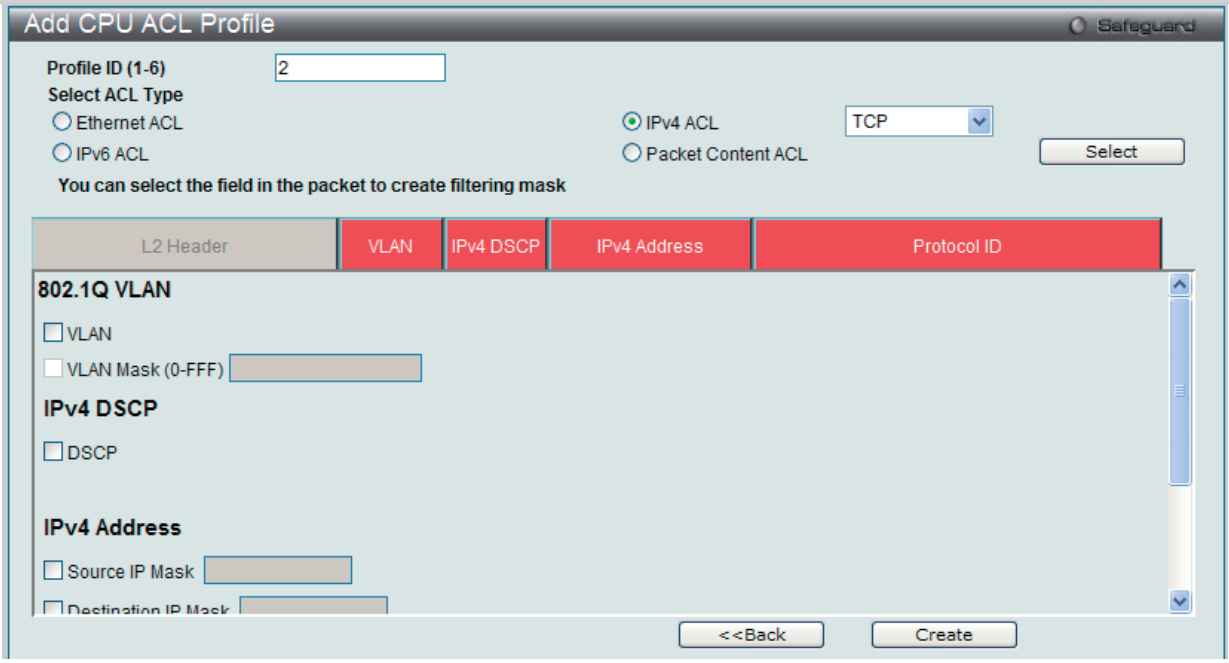


図 10-38 Add CPU ACL Profile - IPv4 画面

「Add CPU ACL Profile」画面で「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
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 6 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。 • 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。
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。
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の TCP ポートマスクを 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の TCP ポートマスクを 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。

項目	説明
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。 • UDP Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートの UDP ポートマスクを 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の UDP ポートマスクを 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 12-40 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（IP）：

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 12-41 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、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。

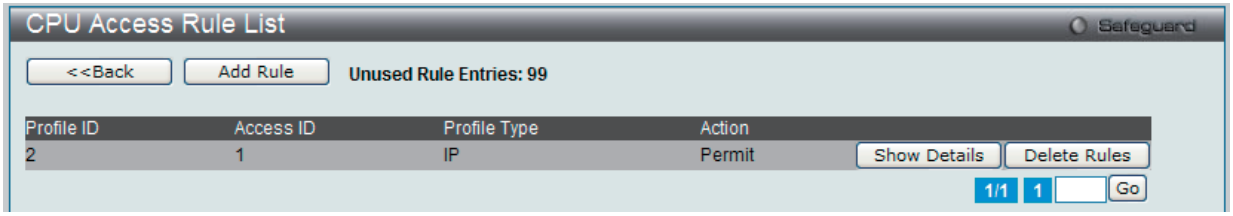


図 12-42 CPU Access Rule List - IP 画面

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。

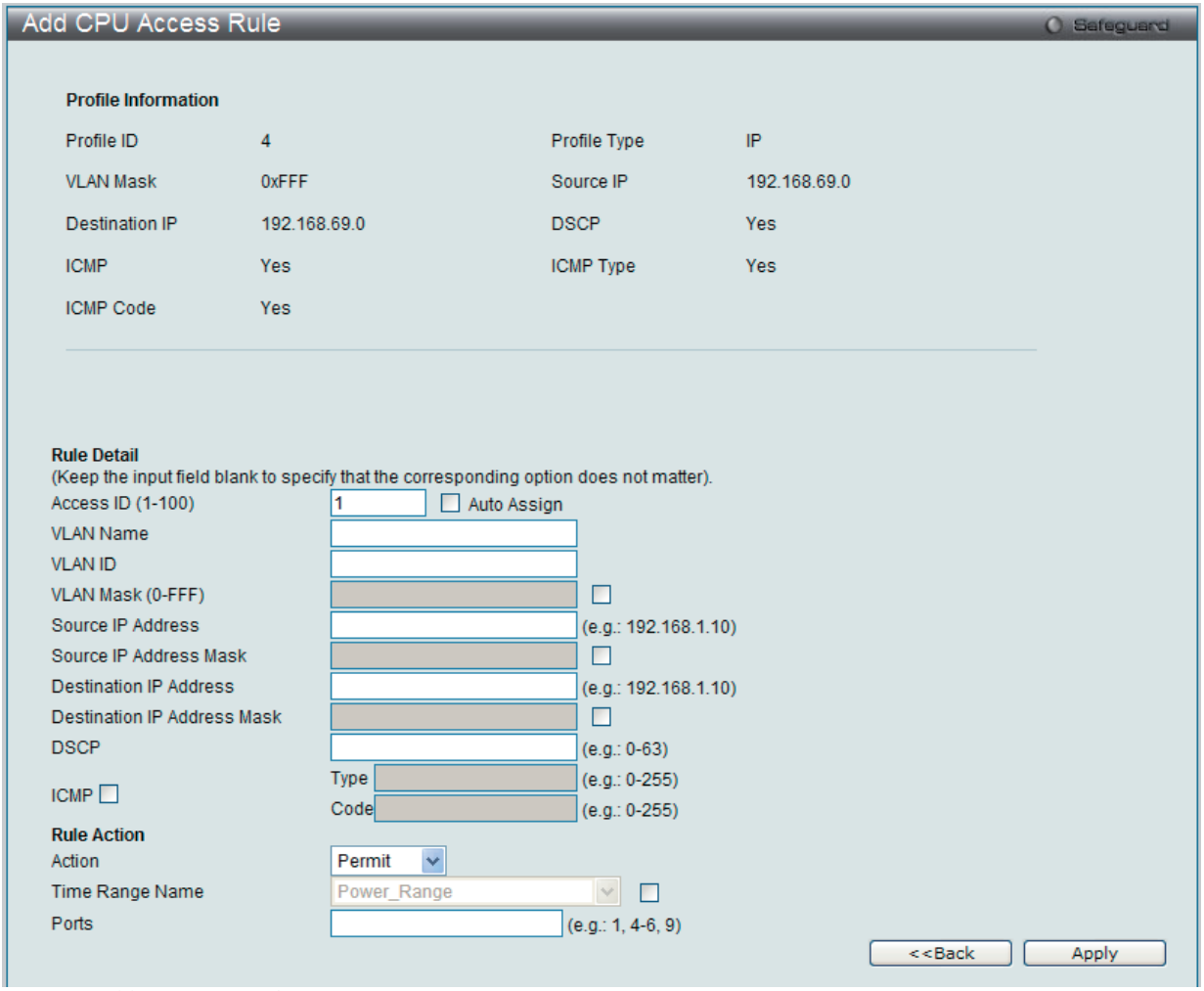


図 12-43　Add CPU Access Rule - IPv4 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-100)	本アクセスの識別番号を入力します。1 から 100 が指定できます。
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	使用する VLAN 名を入力します。
VLAN ID	使用する VLAN ID を入力します。
VLAN Mask	使用する VLAN マスク値を入力します。
Source IP Address	送信元 IP アドレスを入力します。
Source IP Address Mask	送信元 IP アドレスマスクを入力します。
Destination IP Address	送信先 IP アドレスを入力します。
Destination IP Address Mask	送信先 IP アドレスマスクを入力します。
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。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートの TCP ポートマスクを 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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）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。

項目	説明
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。 - Source Port Mask - フィルタリングしたい送信元ポートの UDP ポートマスクを 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の UDP ポートマスクを 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 Define」マスクは 16 進数（0-FF）で指定します。
DSCP	DSCP 値を入力します。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	本オプションを選択して、ICMP トラフィックに適用するルールを指定します。 - Type - 使用する ICMP パケットタイプを入力します。 - Code - 使用する ICMP コード値を入力します。
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。
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。

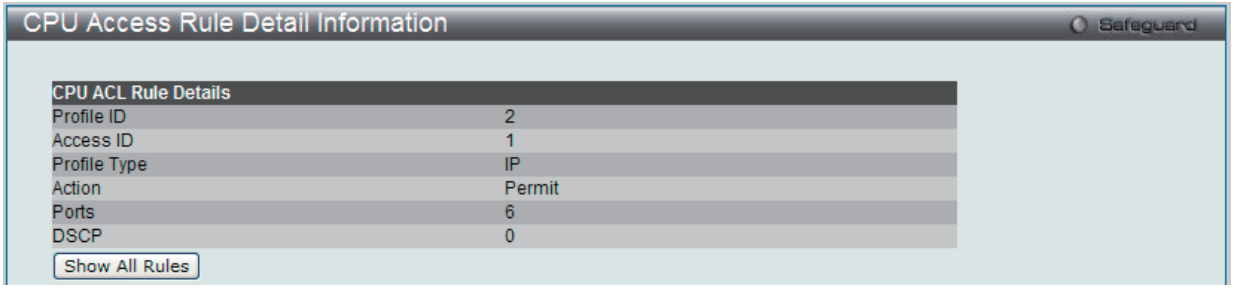


図 12-44 CPU Access Rule Detail Information - IP 画面

「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 12-45 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

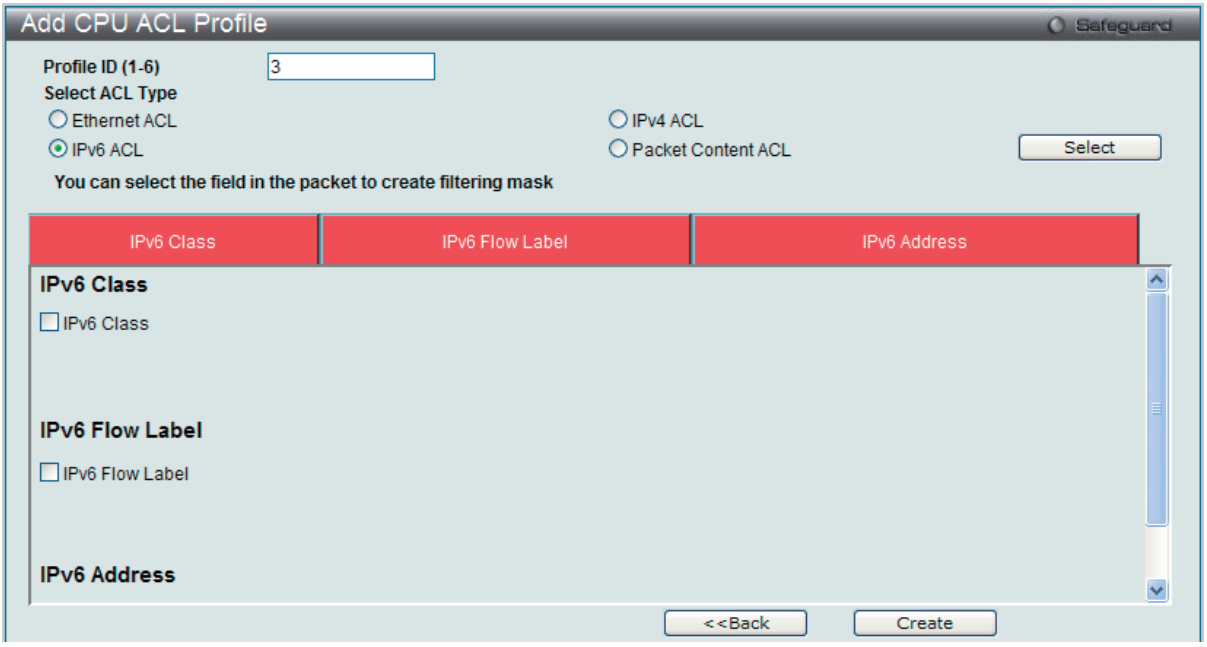


図 12-46　Add CPU ACL Profile - IPv6 画面

「Add CPU ACL Profile」画面で「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 6 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。

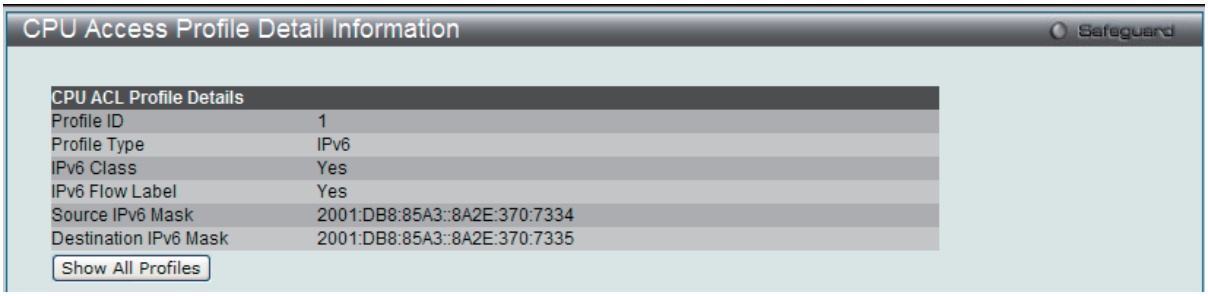


図 12-47　CPU Access Profile Detail Information - IPv6 画面

「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 12-48 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、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。

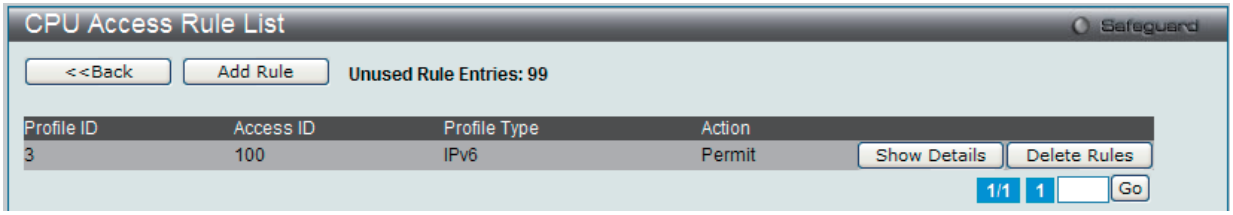


図 12-49 CPU Access Rule List - IPv6 画面

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。

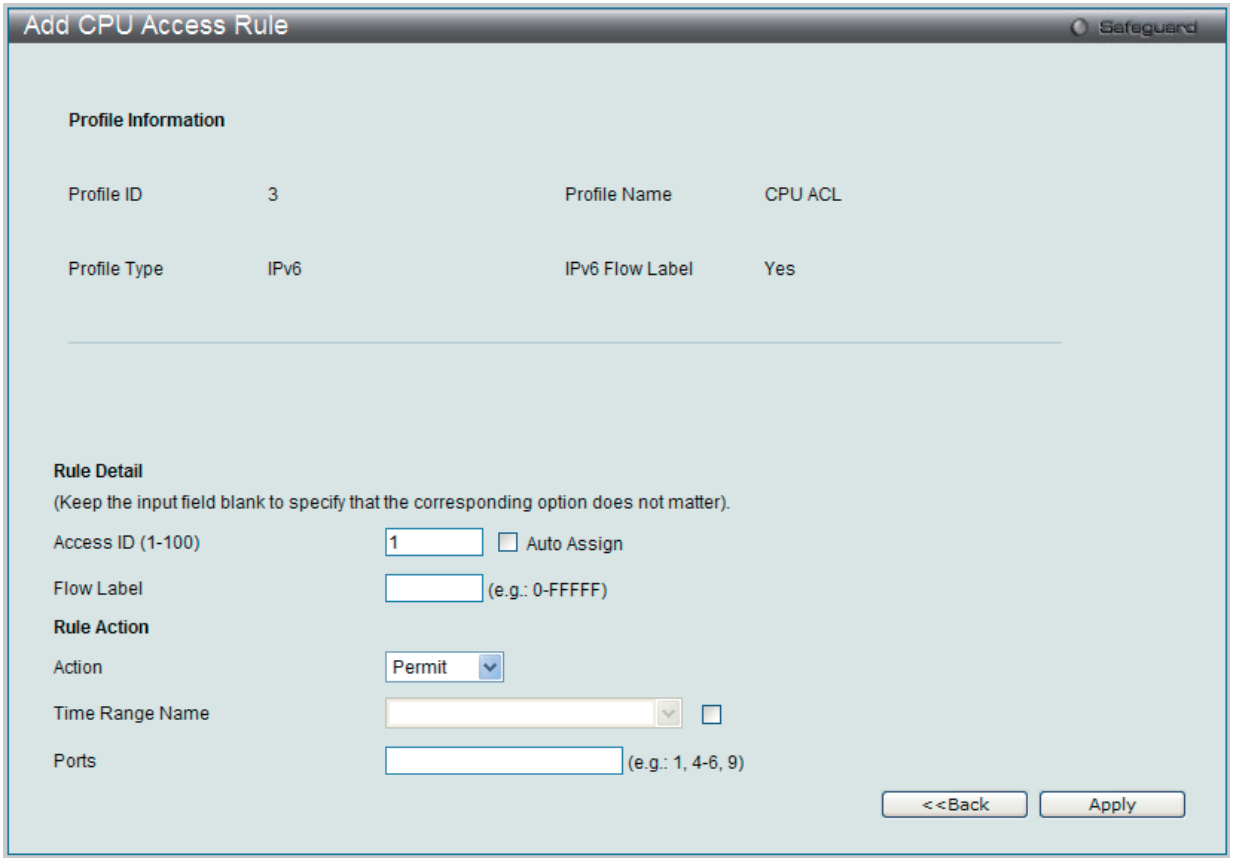


図 12-50 Add Access Rule - IPv6 画面

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。
Class	使用する IPv6 クラスのマスク値を入力します。
Flow Label	使用する IPv6 フローラベルのマスク値を指定します。
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。
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続くフィールドで設定する追加ルールに従って行います。 • 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。

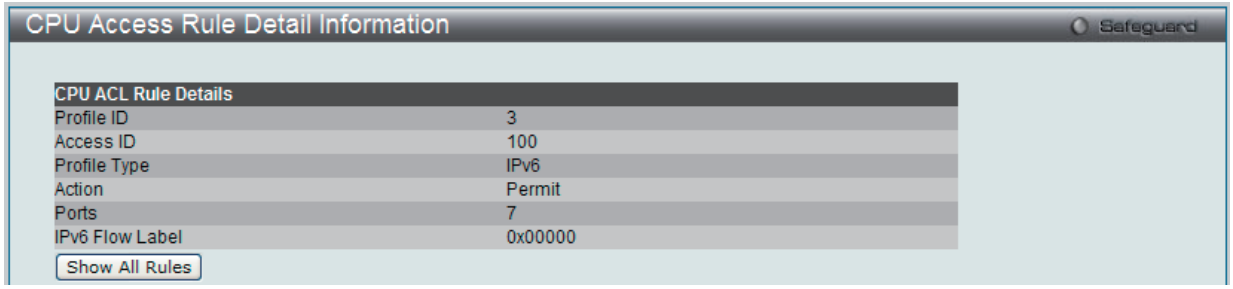


図 12-51　CPU Access Rule Detail Information - IPv6 画面

「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。

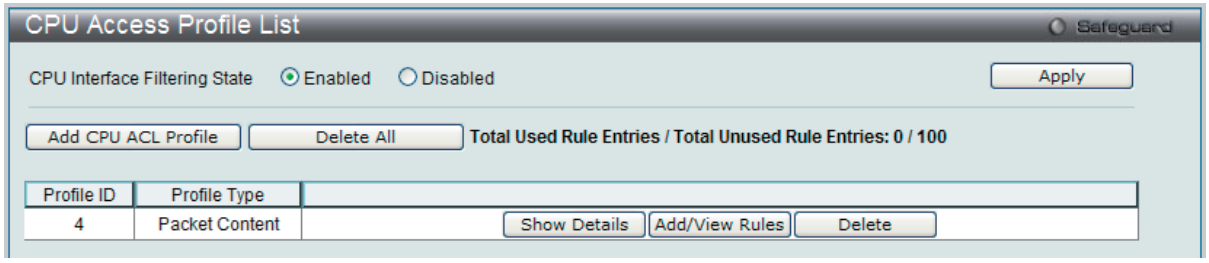


図 12-52　CPU Access Profile List 画面

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

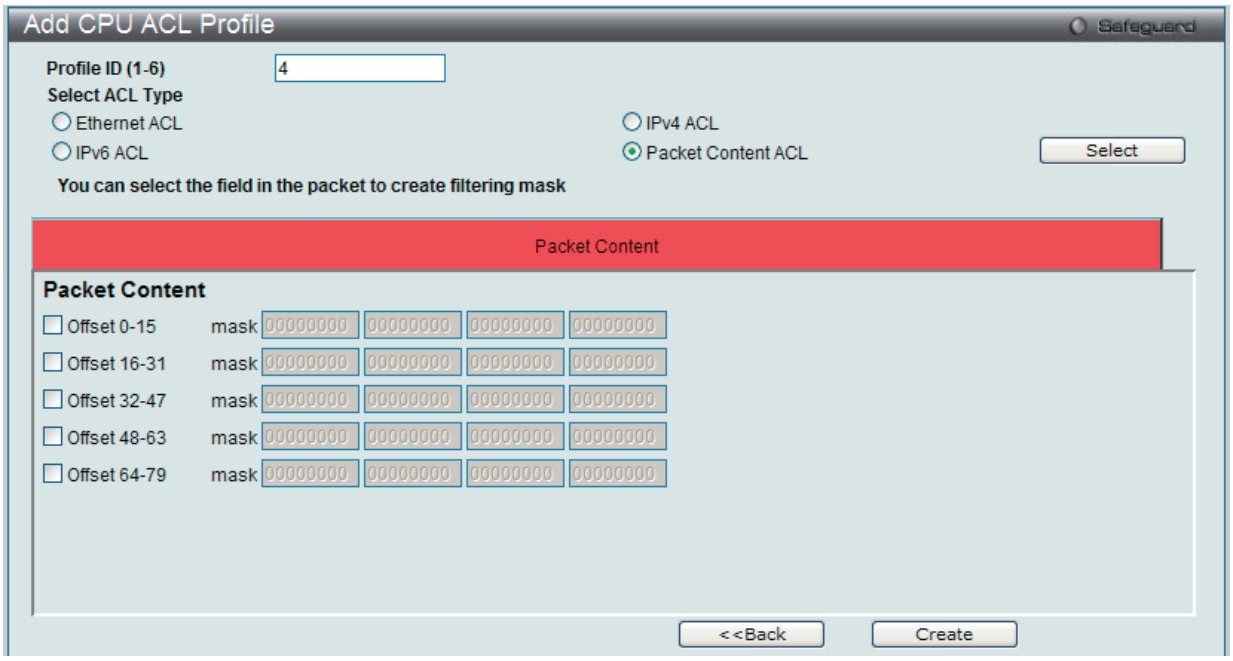


図 12-53　Add CPU ACL Profile - Packet Content 画面

「Add CPU ACL Profile」画面で「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 6 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。 **注意** 作成できるパケットコンテンツマスクプロファイルは 1 つだけです。本スイッチは、高度なパケットコンテンツマスク (またはパケットコンテンツアクセスコントロールリスト -ACL として知られる) 機能を使用して、ARP Spoofing などの一般的なネットワーク攻撃を効果的に軽減することができます。このため、パケットコンテンツ ACL が異なるプロトコル層におけるパケットのどんな指定コンテンツも検証できます。

「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。

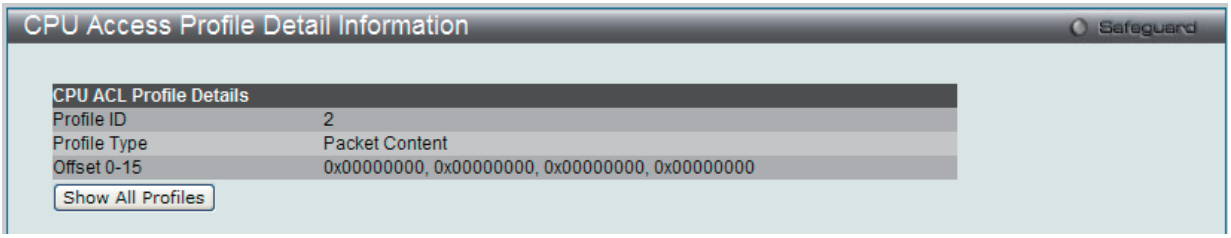


図 12-54 CPU Access Profile Detail Information - Packet Content 画面

「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。

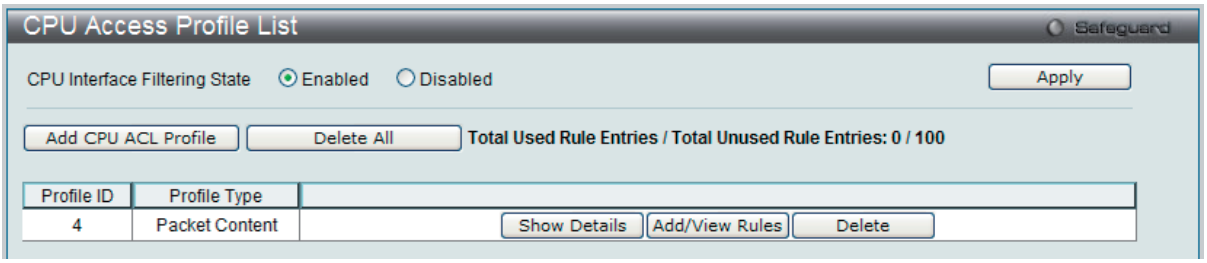


図 12-55 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、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。

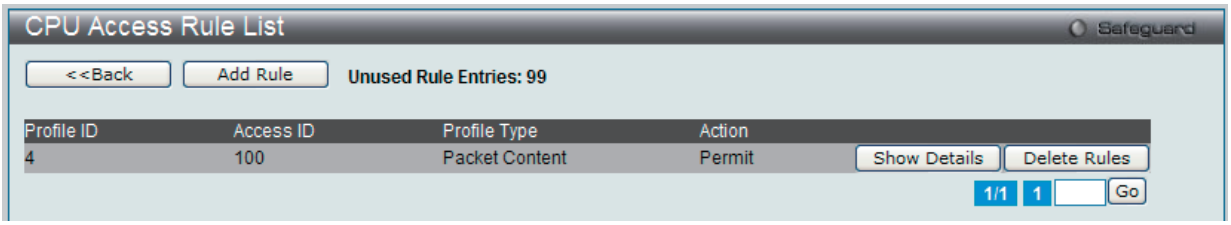


図 12-56 CPU Access Rule List - Packet Content 画面

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。

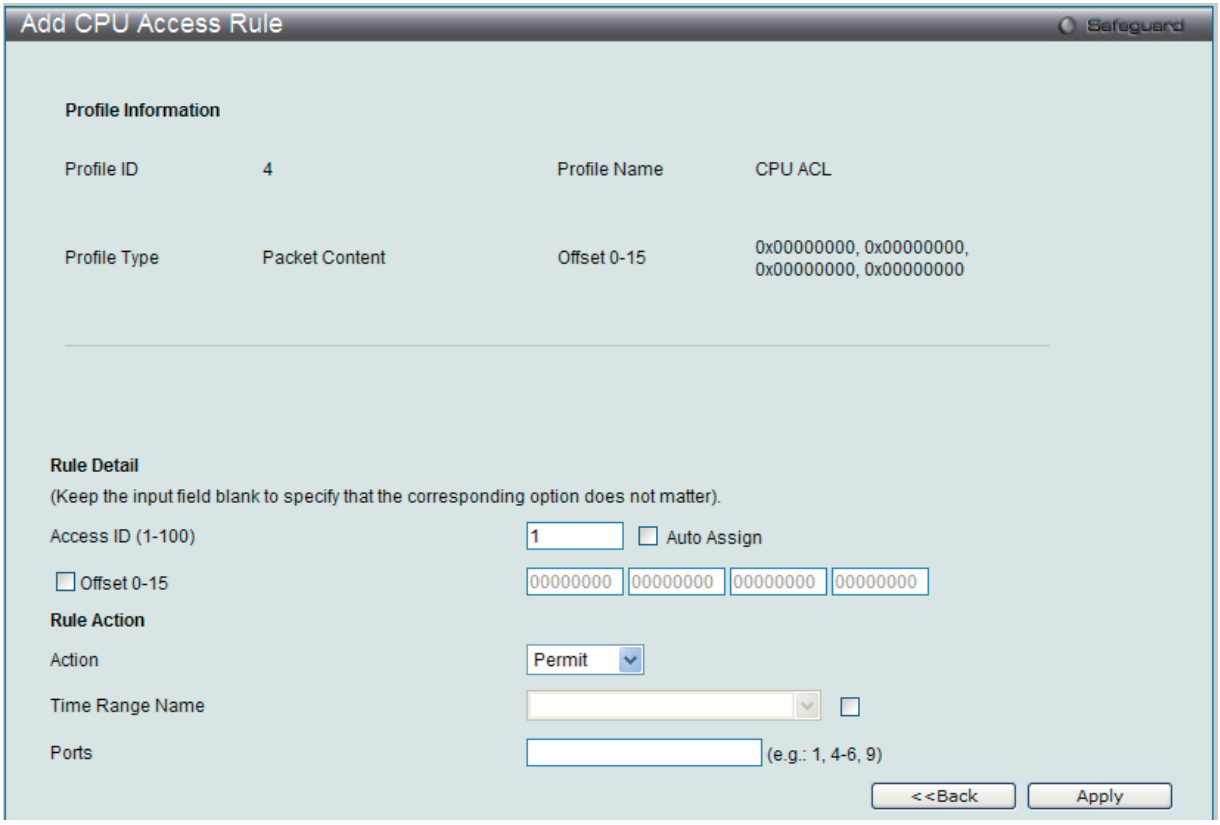


図 12-57 Add Access Rule - Packet Content 画面

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。
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 - 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続く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 - 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。

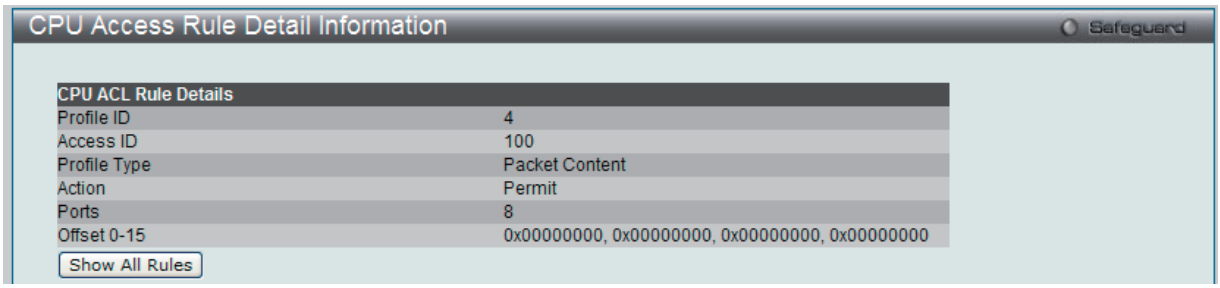


図 12-58 CPU Access Rule Detail Information - Packet Content 画面

「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。

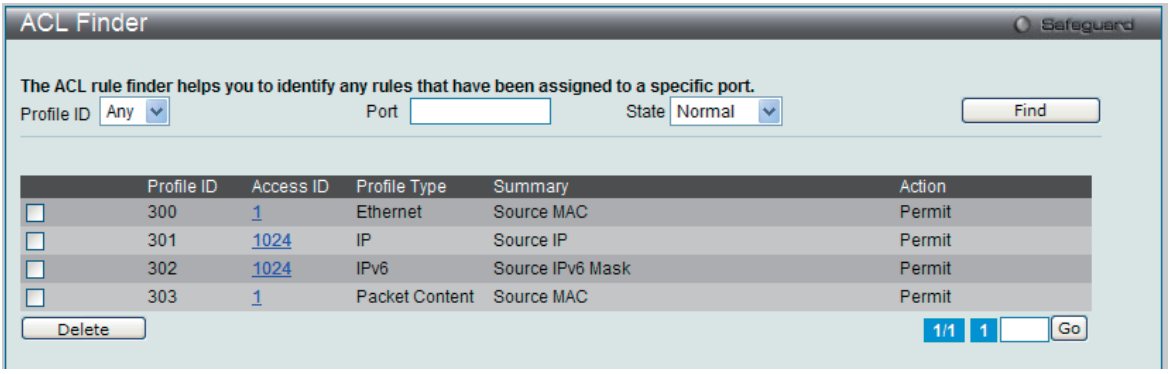


図 12-59　ACL Finder 画面

以下の項目を使用して設定を行います。

項目	説明
Profile ID	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選択します。
State	状態を選択します。

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」（Normal または CPU）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、trTTCM 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、「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。
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。

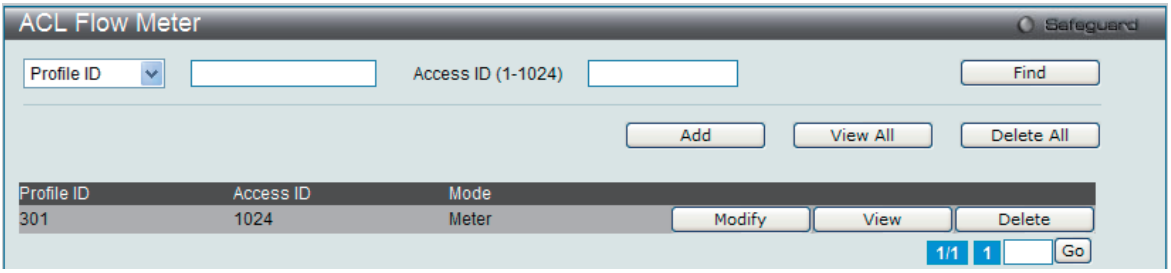


図 12-60　ACL Flow Meter 画面

以下の項目を使用して設定を行います。

項目	説明
Profile ID	ACL フローメータリングパラメータを設定する定義済みプロファイル ID を指定します。
Profile Name	ACL フローメータリングパラメータを設定する定義済みプロファイル名を指定します。
Access ID	ACL フローメータリングパラメータを設定する定義済みアクセス 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。

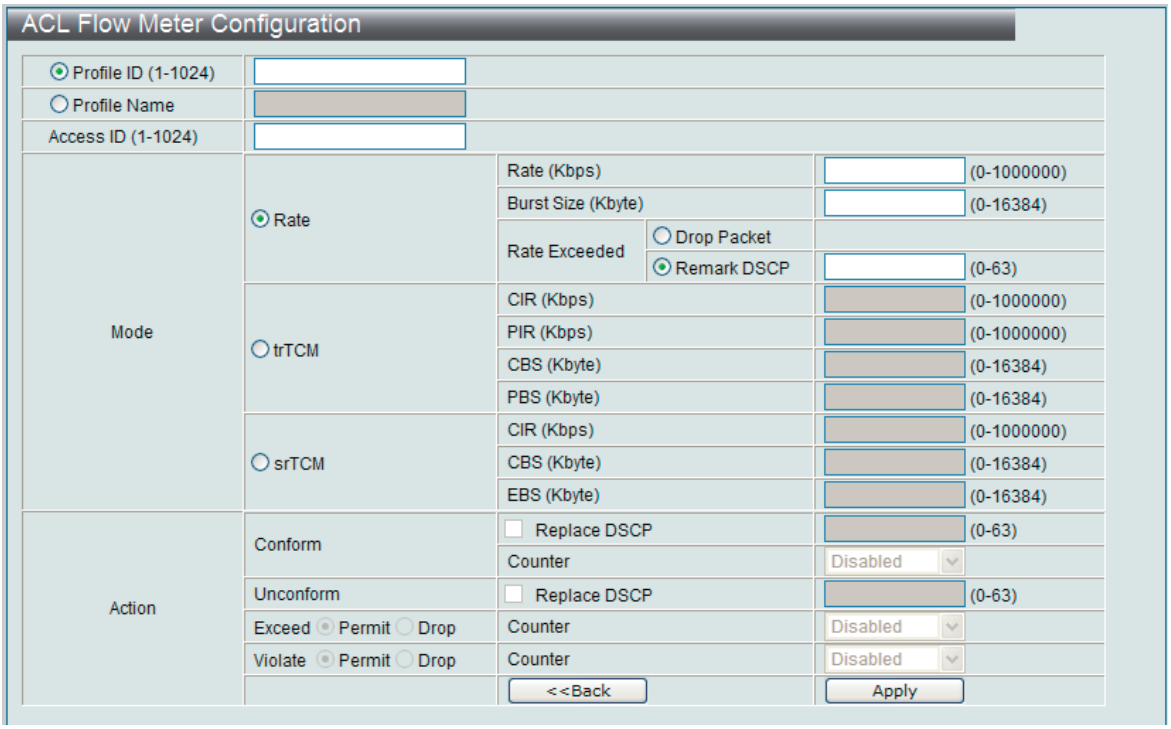


図 12-61　ACL Flow Meter Configuration 画面 - Add

以下の項目を使用して、設定を行います。

項目	説明
Profile ID	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 (1-1024)	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 1-1024 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。単位は Kbps です。 • PBS - ピークバーストサイズの値を入力します。単位は Kbps です。 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。単位は Kbps です。 • CBS -「コミットバーストサイズ」の値を入力します。単位は Kbps です。 • EBS -「超過バーストサイズ」を指定します。単位は Kbps です。
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

対応する「Modify」ボタンをクリックし、以下の画面を表示します。

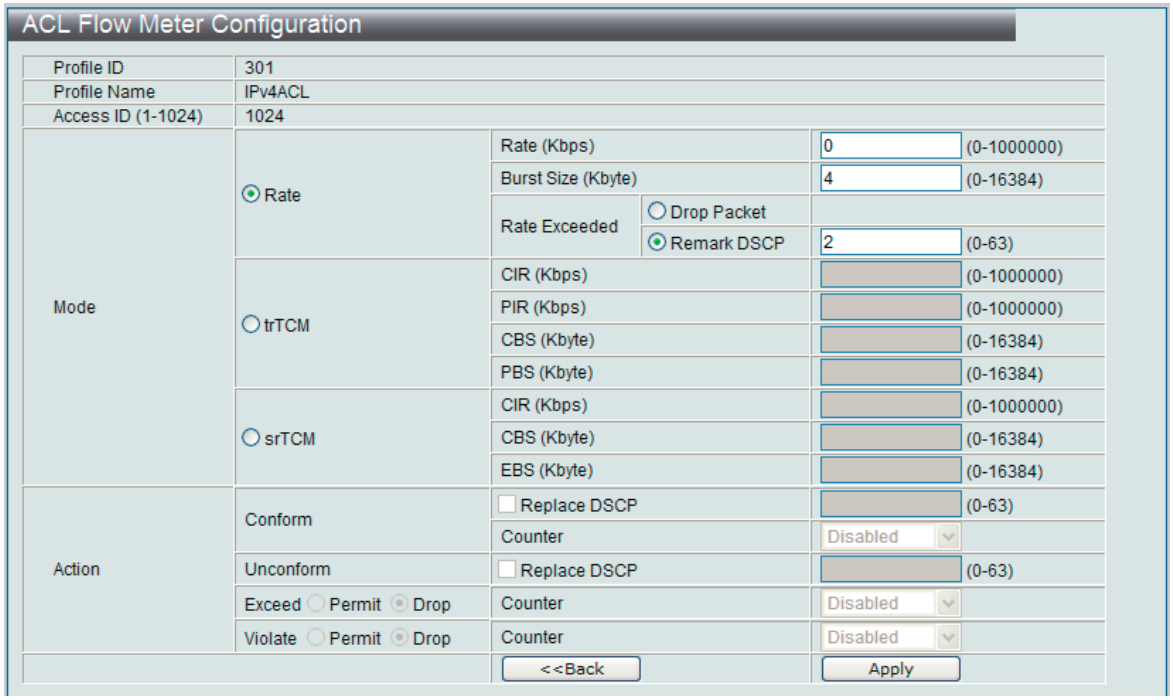


図 12-62　ACL Flow Meter Configuration 画面 - Modify

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。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。

「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。

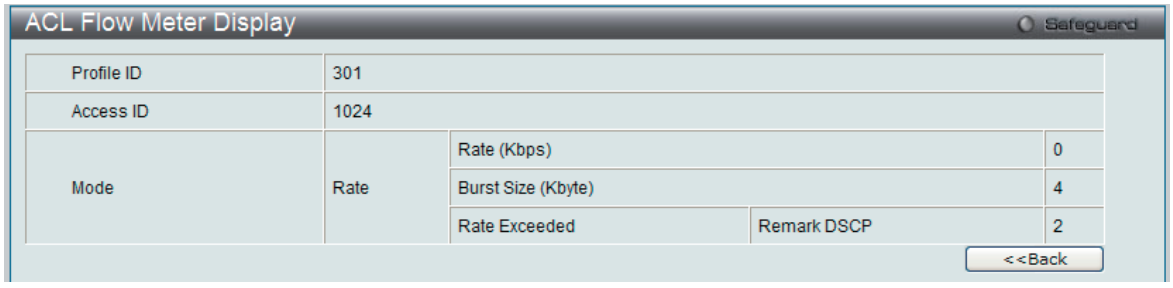


図 12-63　ACL Flow Meter Display 画面

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

Egress Access Profile List（Egress アクセスプロファイルリスト）

イーグレス ACL は、スイッチポートから送出される場合に、フローごとのパケット処理を実行します。スイッチは、3 つのプロファイルタイプ（イーサネット ACL、IPv4 ACL、および IPv6 ACL）をサポートしています。

ACL > Egress 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。

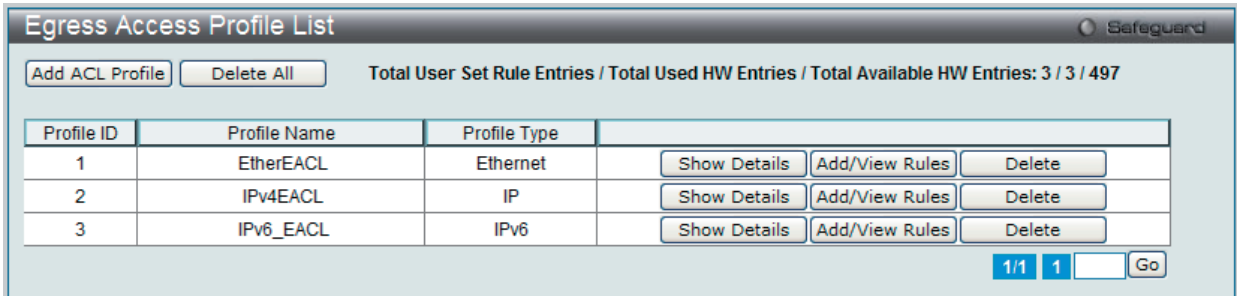


図 12-64　Egress Access Profile List 画面

項目	説明
Add Egress Profile	Egress 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。

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 > Egress 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。

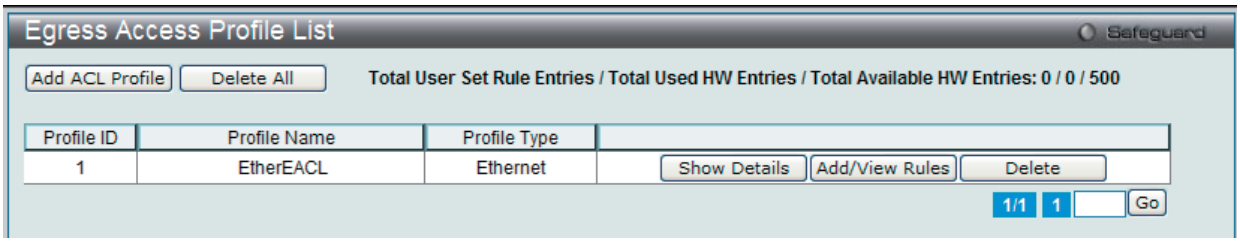


図 12-65　Egress Access Profile List 画面

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 Egress ACL」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

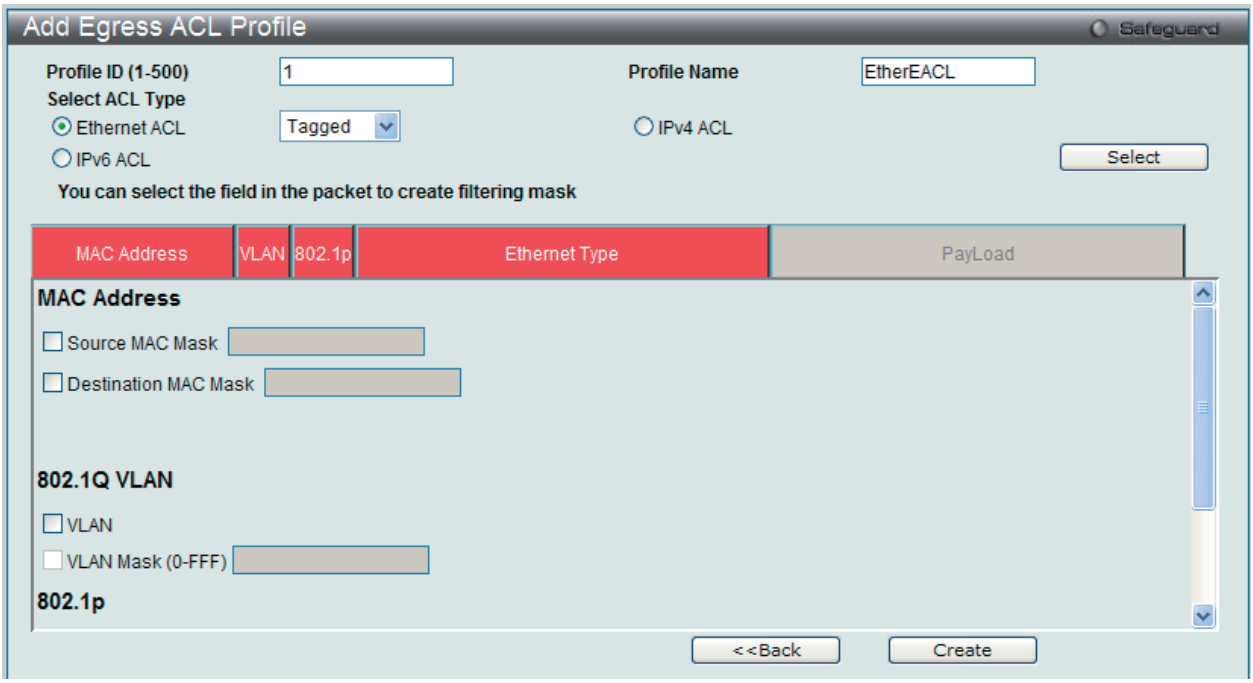


図 12-66　Add Egress ACL Profile - Ethernet ACL 画面

「Profile ID」でプロファイル番号を 1-500 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 500 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、または IPv6 アドレス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。

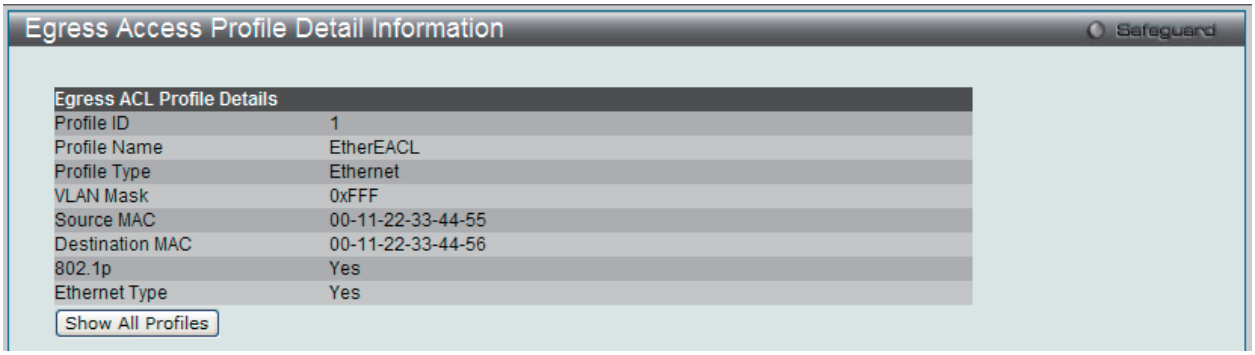


図 12-67 Egress Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Egress 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。

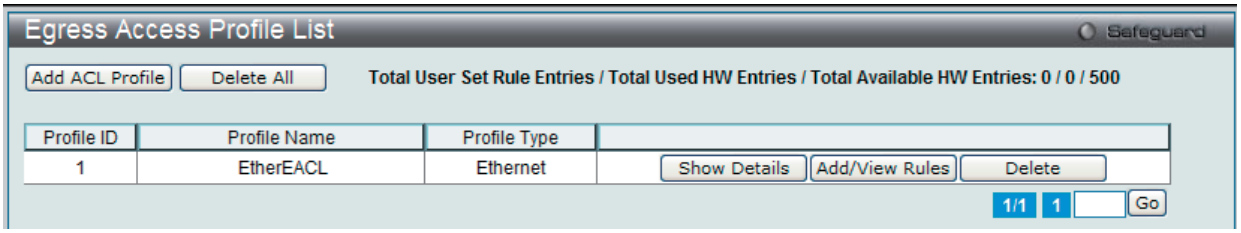


図 12-68 Egress Access Profile List 画面

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。

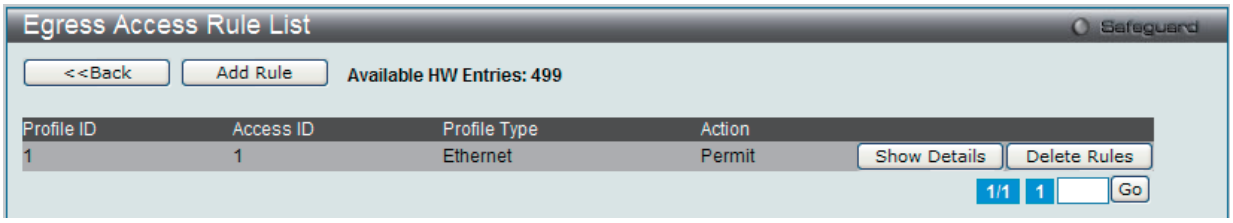


図 12-69 Egress Access Rule List - Ethernet 画面

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。

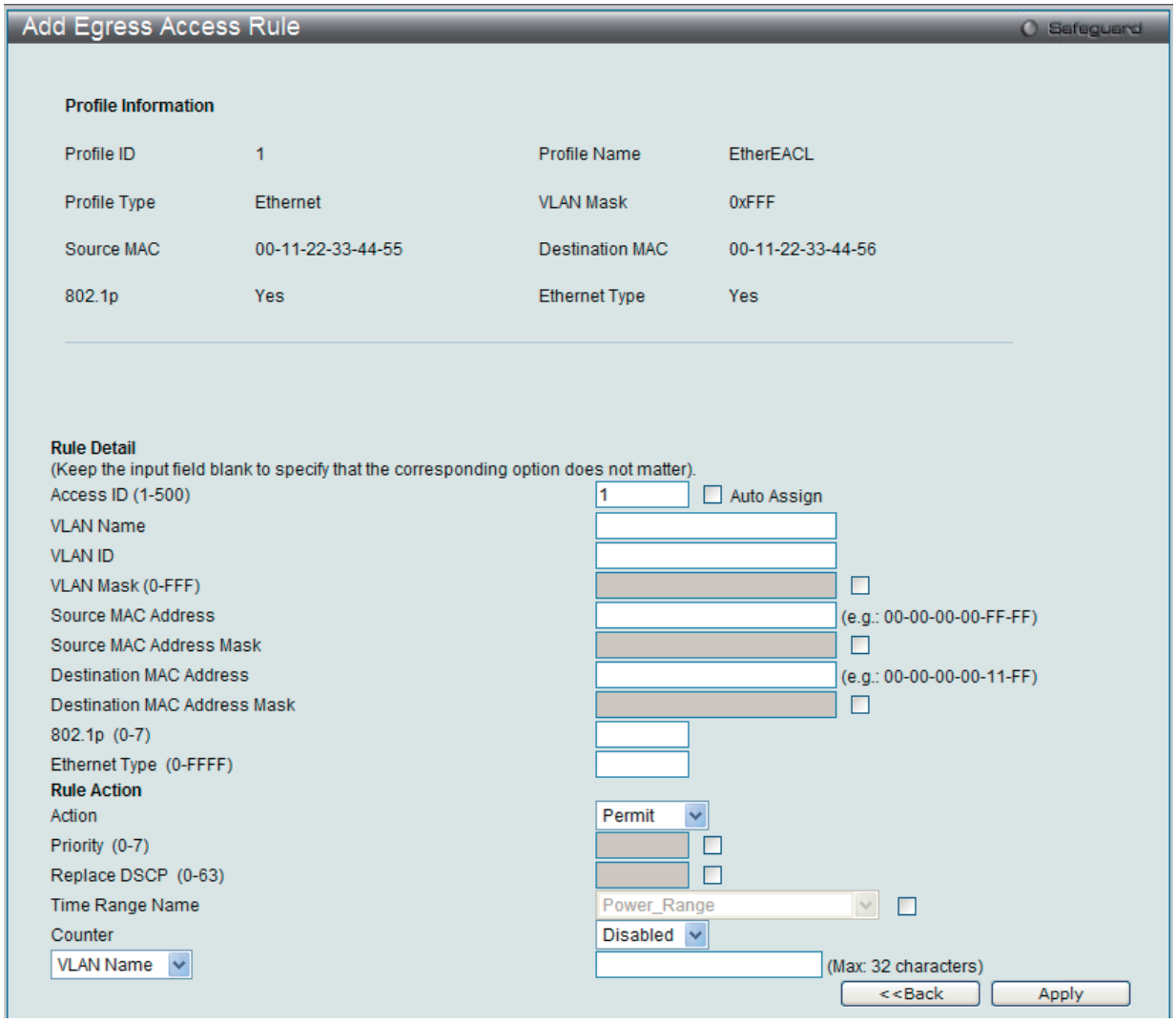


図 12-70　Add Access Rule - Ethernet 画面

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 (1-500)	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 500 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 (0-FFF)	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。

項目	説明
Priority (0-7)	スイッチが設定した 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 271 ページの「第 11 章　QoS（QoS 機能の設定）」を参照してください。
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。
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 - 使用するポートリストを入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

「<<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。
「Apply」ボタンをクリックして行った変更を適用します。

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。

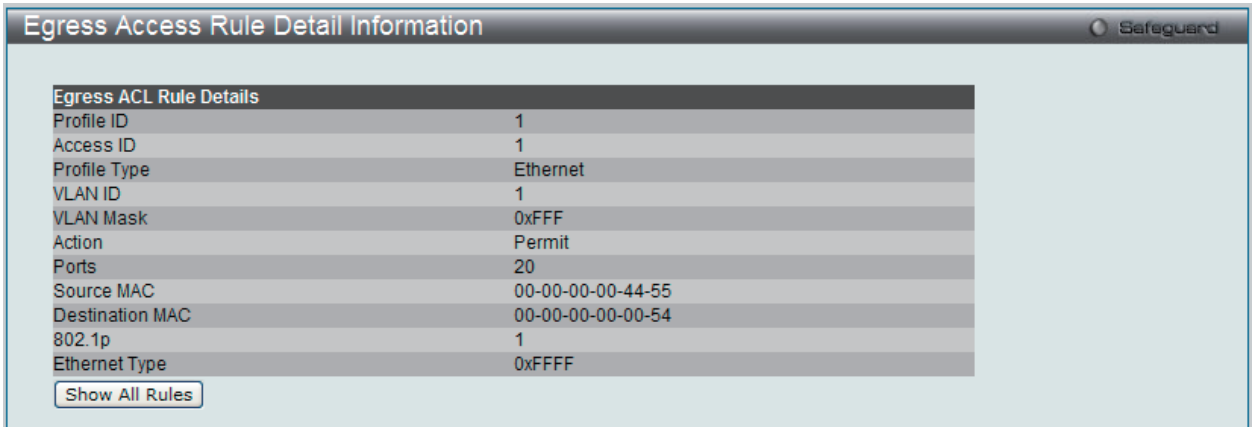


図 12-71　Egress Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

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 > Egress 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。

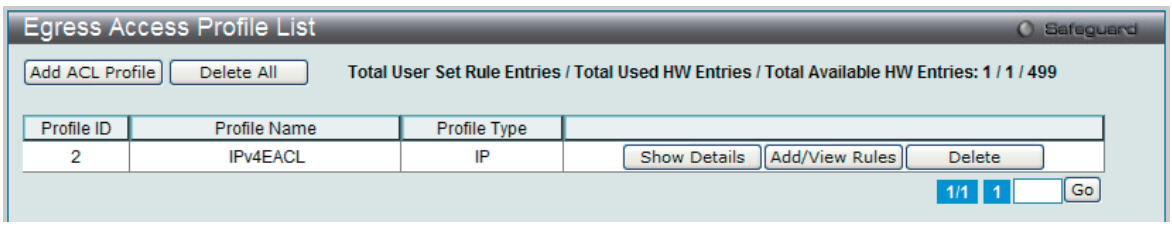


図 12-72　Egress Access Profile List 画面

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。

IPv4 の「Add ACL Profile」画面

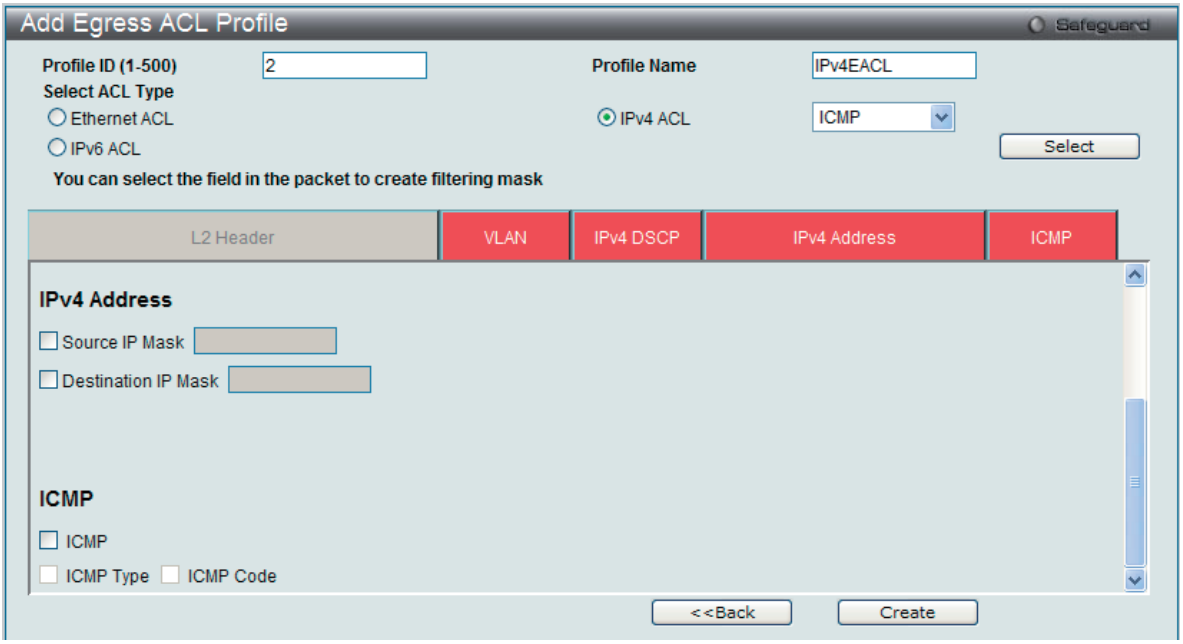


図 12-73　Add Egress ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-500 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 500 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の TCP ポートマスクを 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の TCP ポートマスクを 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。

項目	説明
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のUDPポートマスクを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のUDPポートマスクを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 - レイヤ4パートマスクを指定します。

「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には、「Egress 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。

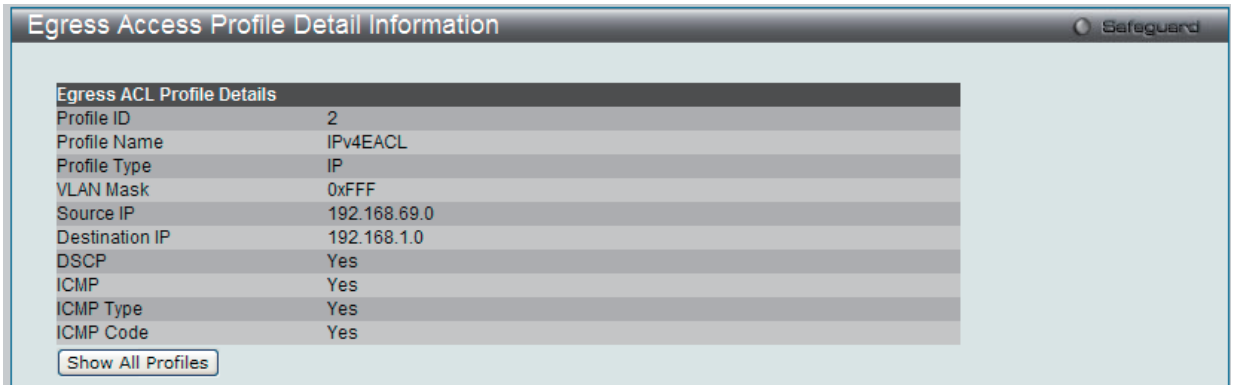


図 12-74　Egress Access Profile Detail Information - IPv4 画面

「Show All Profiles」ボタンをクリックすると、「Egress 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. 「Egress Access Profile List」画面を表示します。

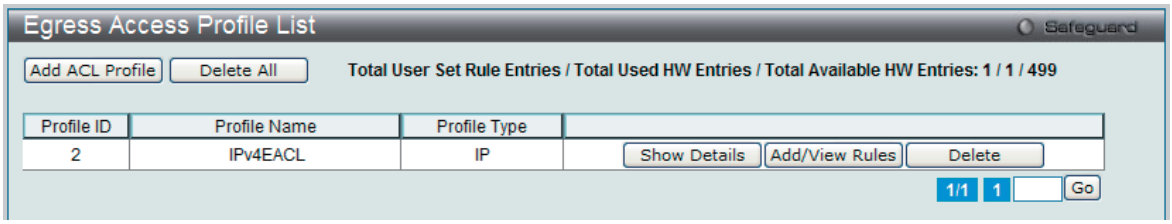


図 12-75　Egress Access Profile List 画面

2. 「Egress Access Profile List」画面を表示し、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。

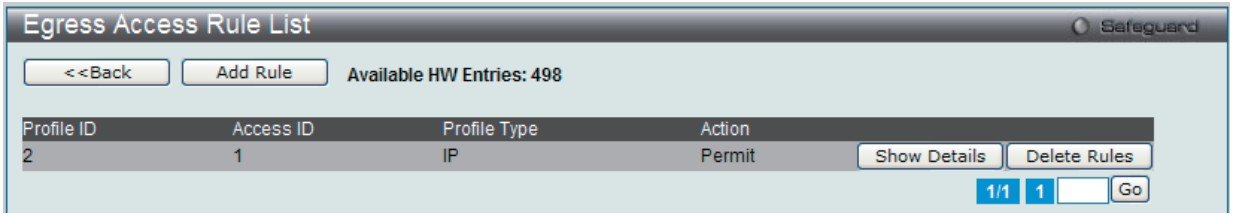


図 12-76　Egress Access Rule List - IPv4 画面

「<<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。

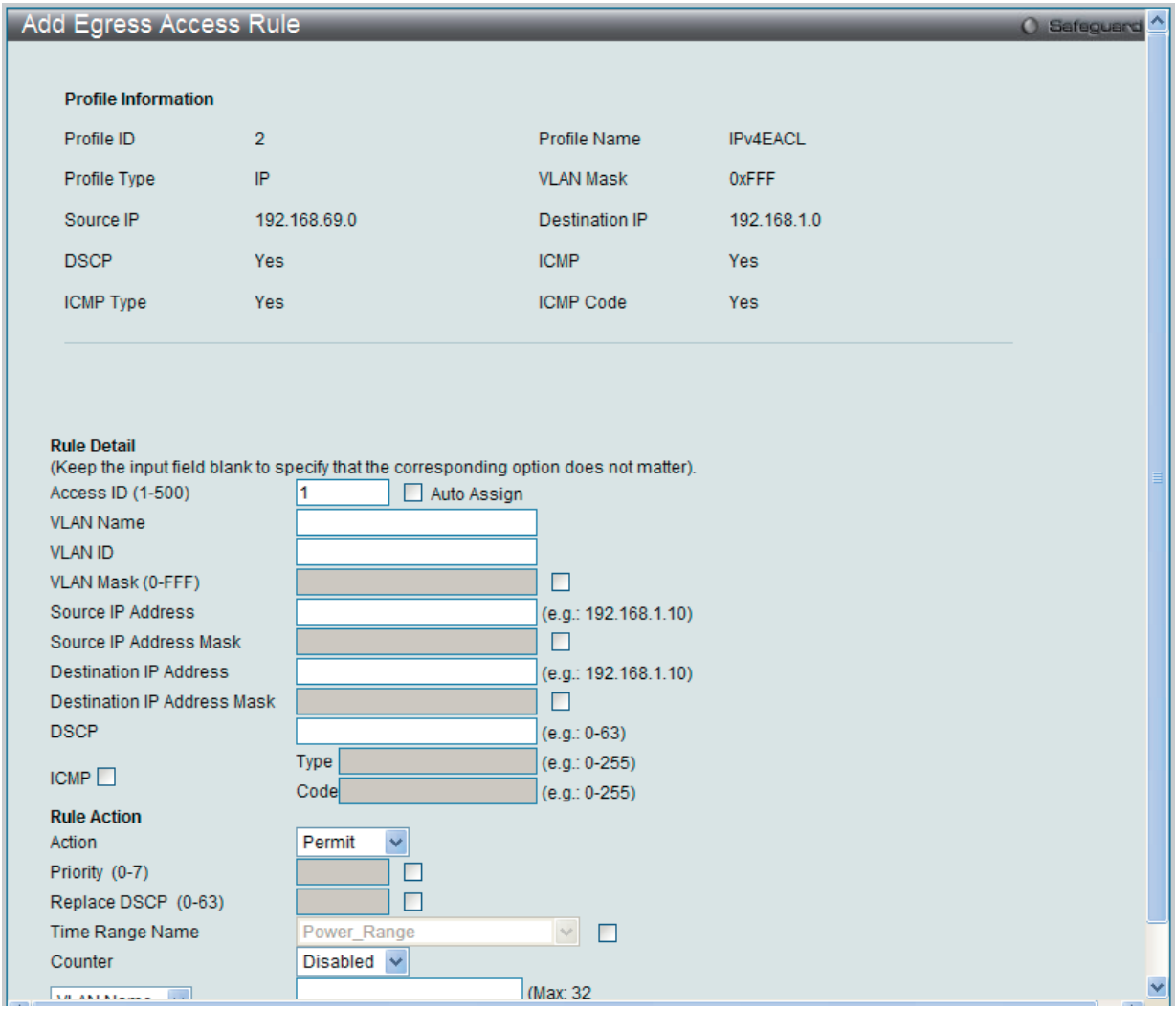


図 12-77　Add Egress Access Rule - IPv4 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-500)	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 500 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 (0-FFF)	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。

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（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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）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の UDP ポートマスクを 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の UDP ポートマスクを 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。
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 271 ページの「第 11 章　QoS（QoS 機能の設定）」を参照してください。
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。
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 - 使用するポートリストを入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

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。

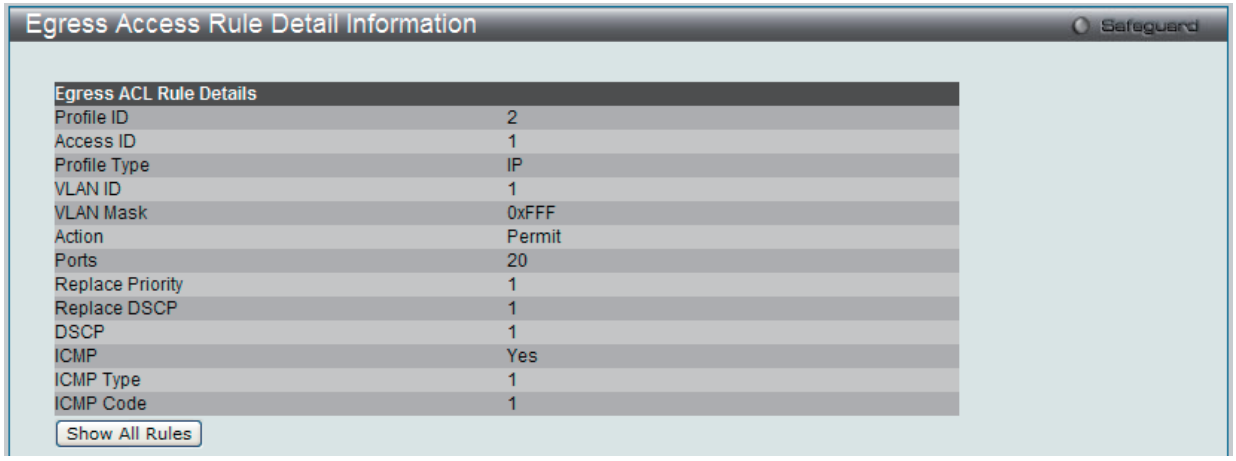


図 12-78 Egress Access Rule Detail Information - IP 画面

「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 > Egress 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。

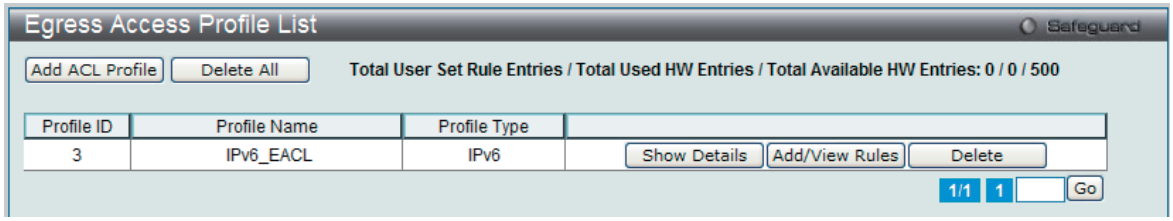


図 12-79 Egress Access Profile List 画面

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

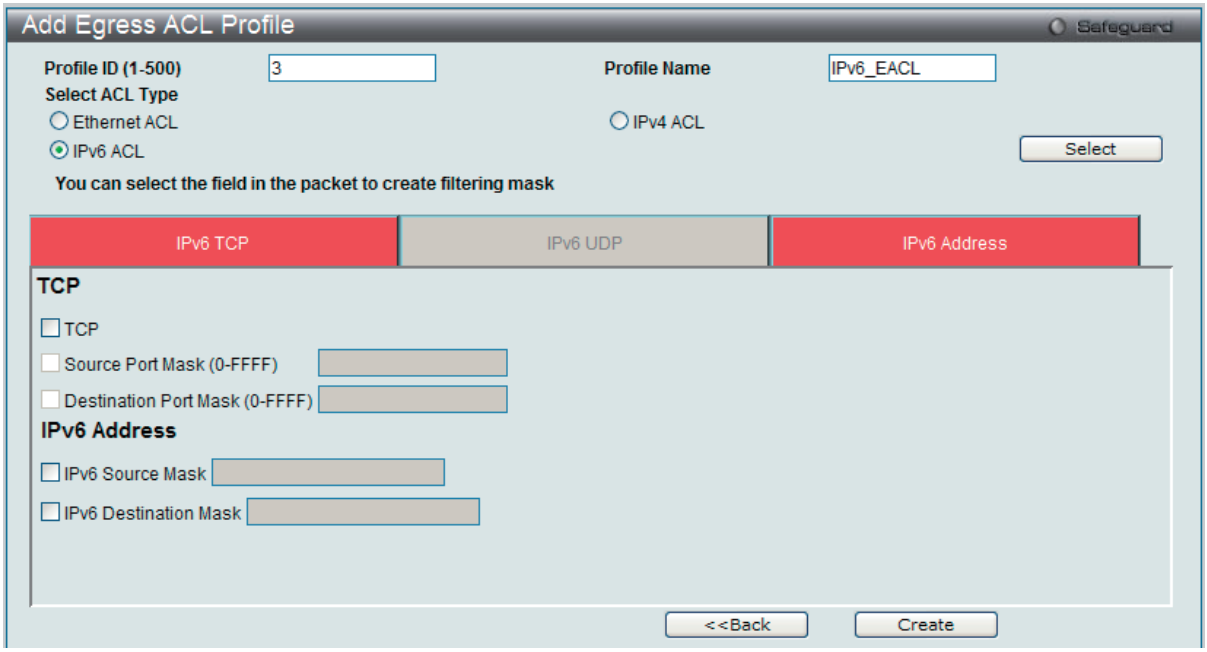


図 12-80 Add Egress ACL Profile - IPv6 ACL 画面

「Profile ID」でプロファイル番号を 1-6 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。
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) - フィルタリングしたい送信先ポートの TCP ポートマスクを 16 進数で指定します。 • Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートの TCP ポートマスクを 16 進数（hex 0x0-0xffff）で指定します。
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) - フィルタリングしたい送信元ポートの UDP ポートマスクを 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の UDP ポートマスクを 16 進数（hex 0x0-0xffff）で指定します。
IPv6 Address	• IPv6 Source Address - 対応するボックスをチェックして、IPv6 アドレスマスク（例 FFFF:FFFF::FFFF）を入力することで送信元 IPv6 アドレスのマスク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、IPv6 アドレスマスク（例 FFFF:FFFF::FFFF）を入力することで送信先 IPv6 アドレスのマスク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。

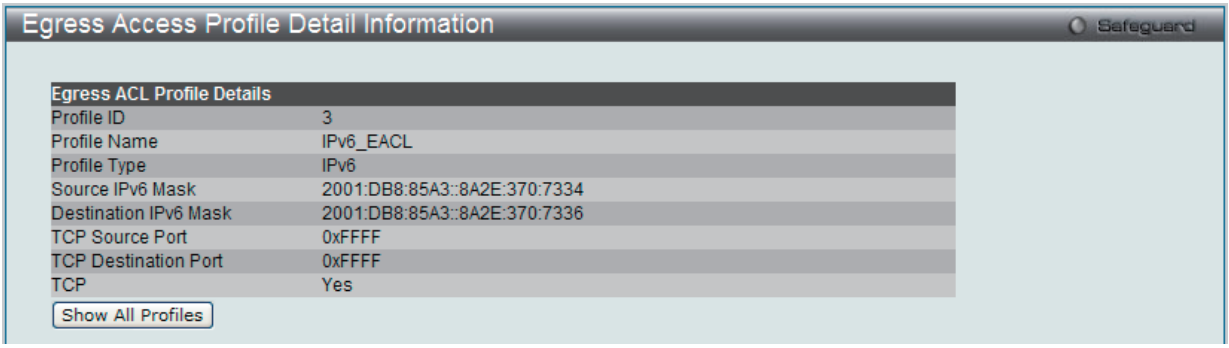


図 12-81　Egress Access Profile Detail Information - IPv6 ACL 画面

「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. 「Egress Access Profile List」画面を表示します。

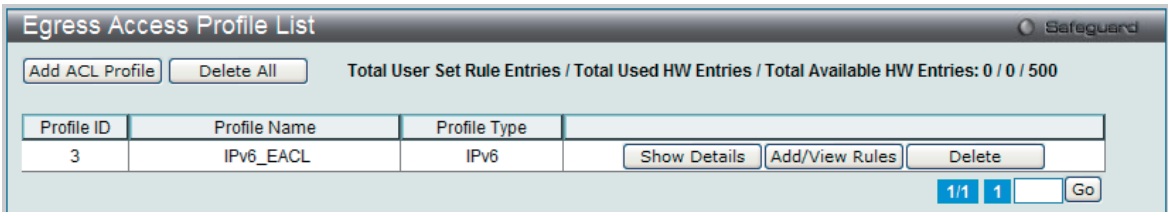


図 12-82　Egress　Access Profile List 画面

2. 「Access Profile List」画面を表示し、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。

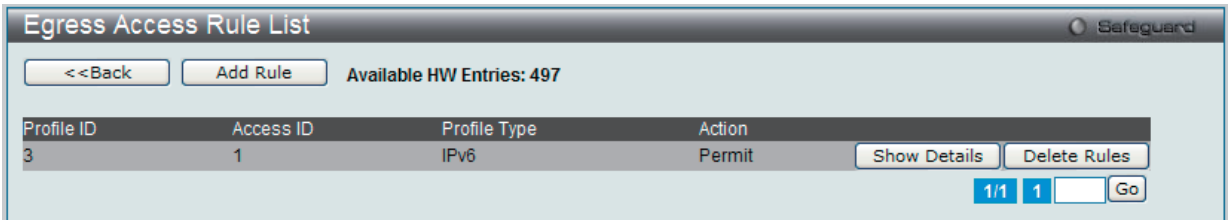


図 12-83　Egress Access Rule List - IPv6 画面

「<<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。

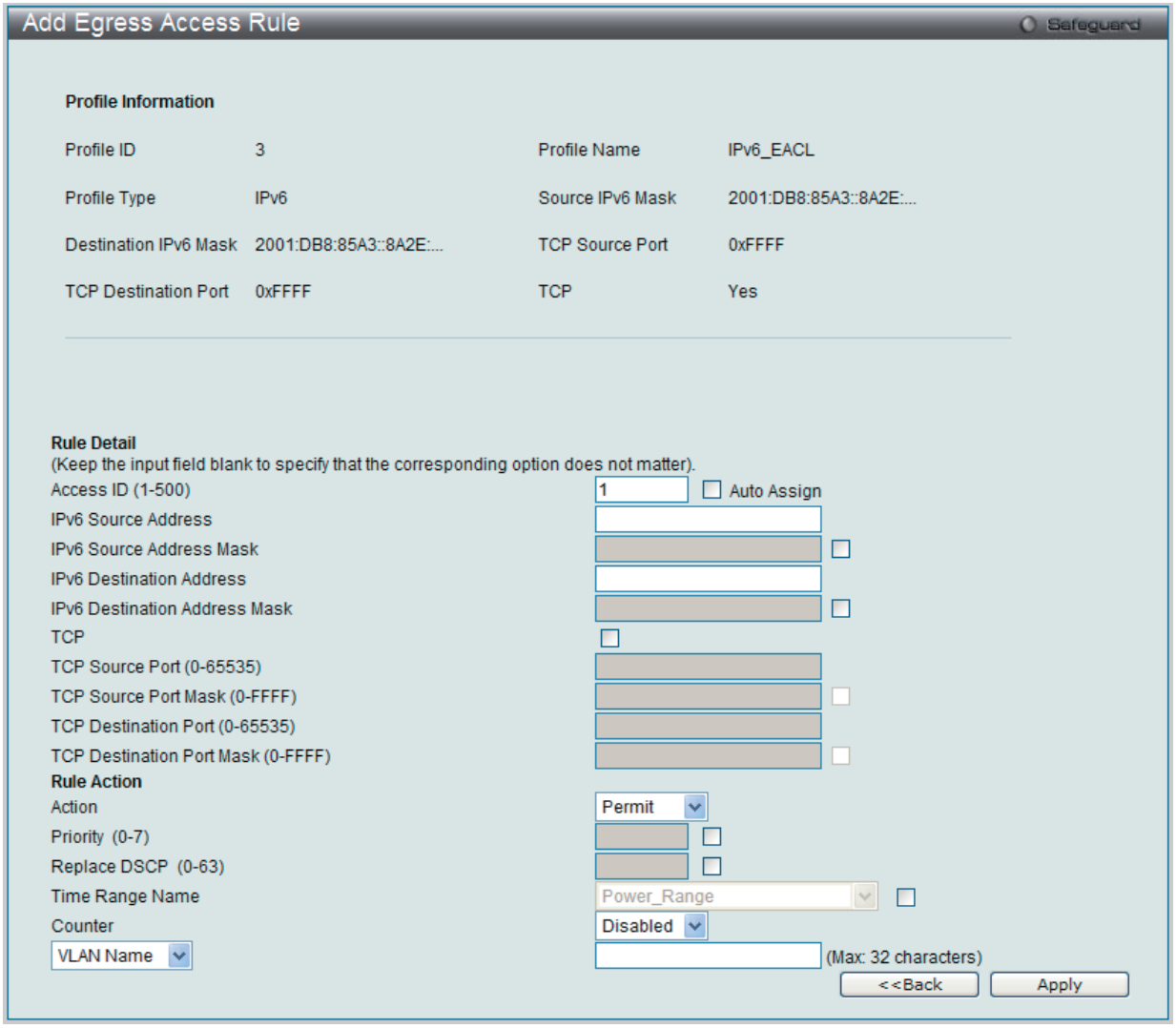


図 12-84　Add Egress Access Rule - IPv6 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-128)	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 500 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	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	IPv6 フローラベルマスクを指定します。0-FFFFF の範囲で指定します。
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。送信先 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	IPv6 送信先アドレスの IPv6 アドレスを入力します。
IPv6 Destination Address Mask	IPv6 送信先サブマスクを指定します。送信先 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。
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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）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の TCP ポートマスクを 16 進数（hex 0x0-0xffff）で指定します。

項目	説明
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の UDP ポートマスクを 16 進数（hex 0x0-0xffff）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の UDP ポートマスクを 16 進数（hex 0x0-0xffff）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 271 ページの「第 11 章　QoS（QoS 機能の設定）」を参照してください。
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 をボックスの右側の欄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。
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 - 使用するポートリストを入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

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

「Egress 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。

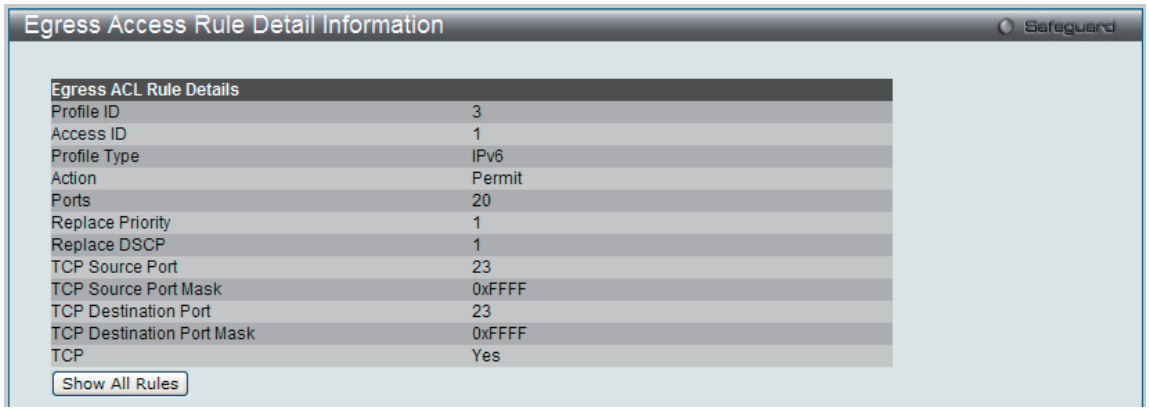


図 12-85　Egress Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「Egress Access Rule List」画面に戻ります。

Egress ACL Flow Meter（Egress ACL フローメータリング）

Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。

ACL > Egress 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。

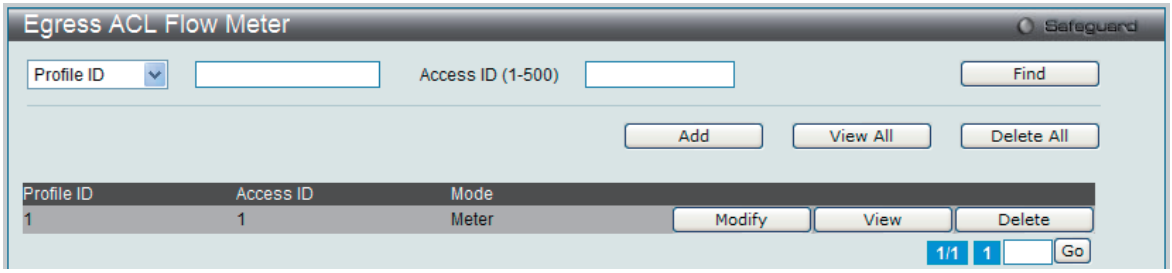


図 12-86 Egress ACL Flow Meter 画面

以下の項目を使用して設定を行います。

項目	説明
Profile ID	ACL フローメータリングパラメータを設定する定義済みプロファイル ID を指定します。
Profile Name	ACL フローメータリングパラメータを設定する定義済みプロファイル名を指定します。
Access ID (1-128)	ACL フローメータリングパラメータを設定する定義済みアクセス 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。

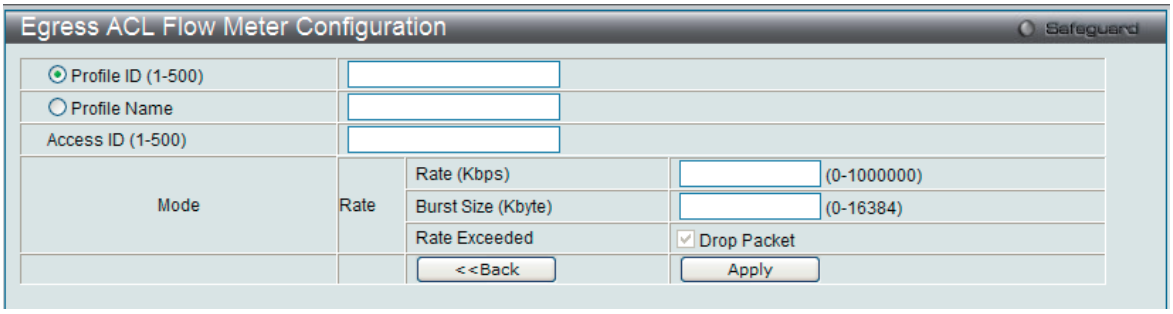


図 12-87 Egress ACL Flow Meter Configuration 画面 - Add

以下の項目を使用して、設定を行います。

項目	説明
Profile ID	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 (1-500)	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 1-500 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。単位は Kbps です。 • PBS - ピークバーストサイズの値を入力します。単位は Kbps です。 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。単位は Kbps です。 • CBS -「コミットバーストサイズ」の値を入力します。単位は Kbps です。 • EBS -「超過バーストサイズ」を指定します。単位は Kbps です。

項目	説明
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。

「Egress 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

対応する「Modify」ボタンをクリックし、以下の画面を表示します。

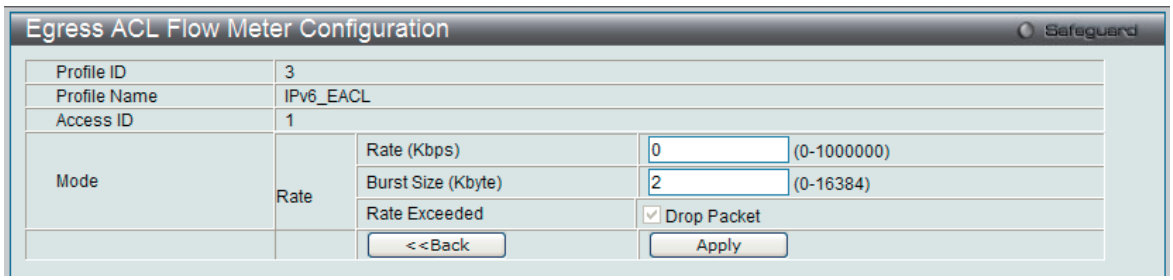


図 12-88 Egress ACL Flow Meter Configuration 画面 - Modify

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。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。

「Apply」ボタンをクリックして、設定を適用します。

「Egress 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。

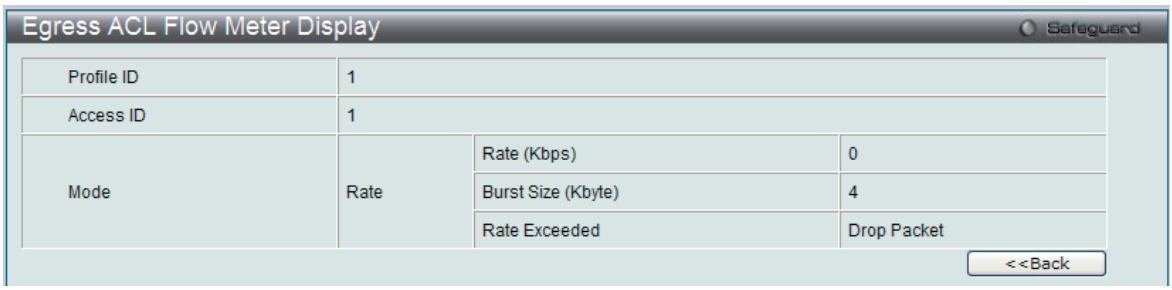


図 12-89 Egress ACL Flow Meter Display 画面

「Egress 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 13 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 の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）	337
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）	349
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）、ND Snooping（ND Snooping 設定）	353
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）	359
Web-based Access Control (WAC)（Web ベースのアクセス制御）	Web ベースアクセスコントロールを設定します。以下のメニューがあります。 WAC Global Settings（WAC グローバル設定）、WAC User Settings（WAC ユーザ設定）、WAC Port Settings（WAC ポート設定）、WAC Authentication State（WAC 認証状態）	362
Japanese Web-based Access Control（JWAC : JWAC 設定）	JWAC の有効化および設定をします。以下のメニューがあります。 JWAC Global Settings（JWAC グローバル設定）、JWAC Port Settings（JWAC ポート設定）、JWAC User Settings（JWAC ユーザ設定）、JWAC Authentication State（JWAC 認証状態）、JWAC Customize Page Language（JWAC 画面言語のカスタマイズ）、JWAC Customize Page（JWAC 画面のカスタマイズ）	368
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。以下のメニューがあります。 Compound Authentication Settings（コンパウンド認証設定）、Compound Authentication Guest VLAN Settings（コンパウンド認証ゲスト VLAN の設定）	373
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）	378
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。	382
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。	383
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。	384
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	385
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。	386
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）	387
Access Authentication Control（アクセス認証コントロール）	TACACS/XTACACS/TACACS+/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）	389

サブメニュー	説明	参照ページ
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。	397
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）	399
Trusted Host Settings（トラストホスト設定）	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。	402
Safeguard Engine Settings（セーフガードエンジン設定）	セーフガードエンジンの設定を行います。	403

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。

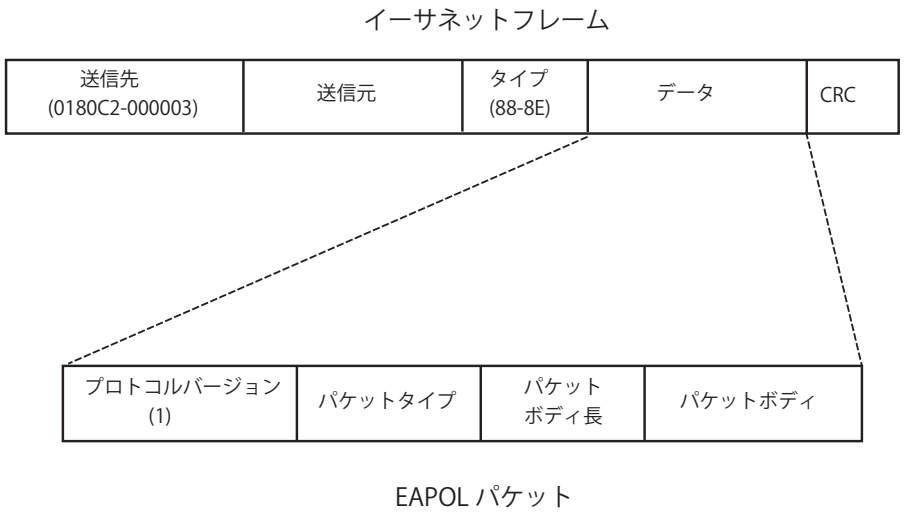


図 13-1　EAPOL パケット

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。

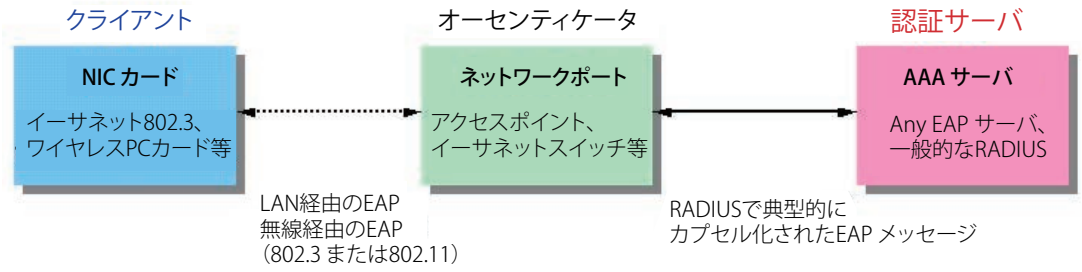


図 13-2　802.1X の 3 つの要素

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。

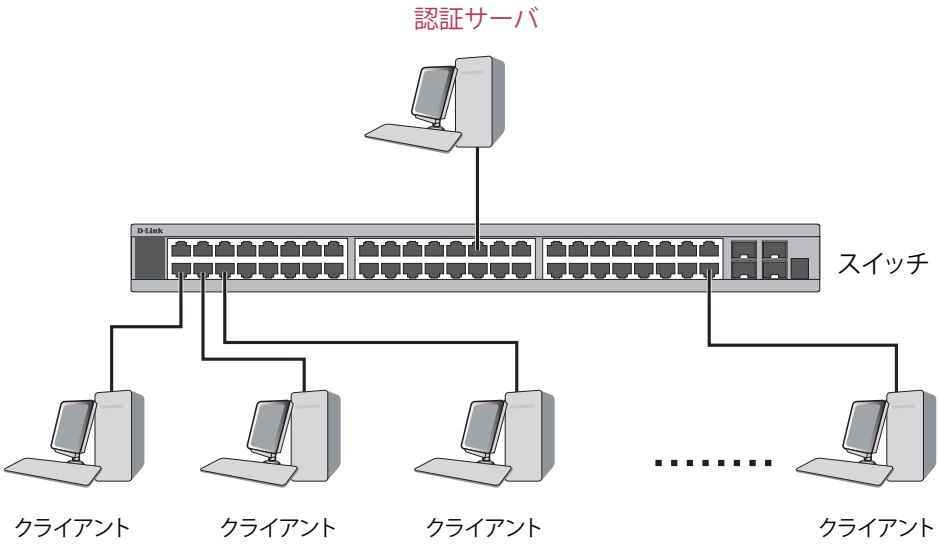


図 13-3　認証サーバ

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-3810 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**）

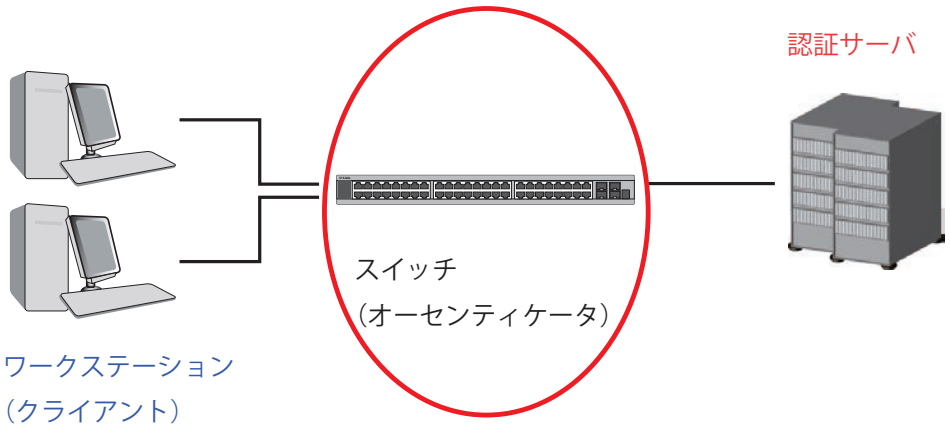


図 13-4　オーセンティケータ

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。

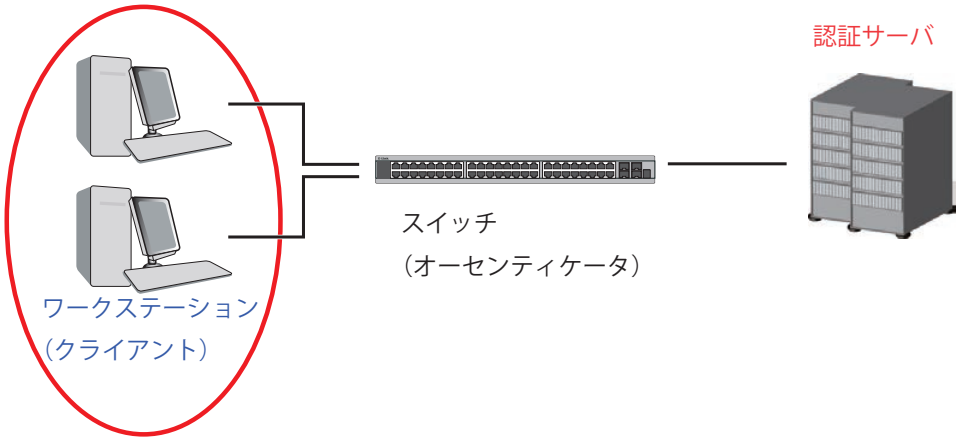


図 13-5　クライアント

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。

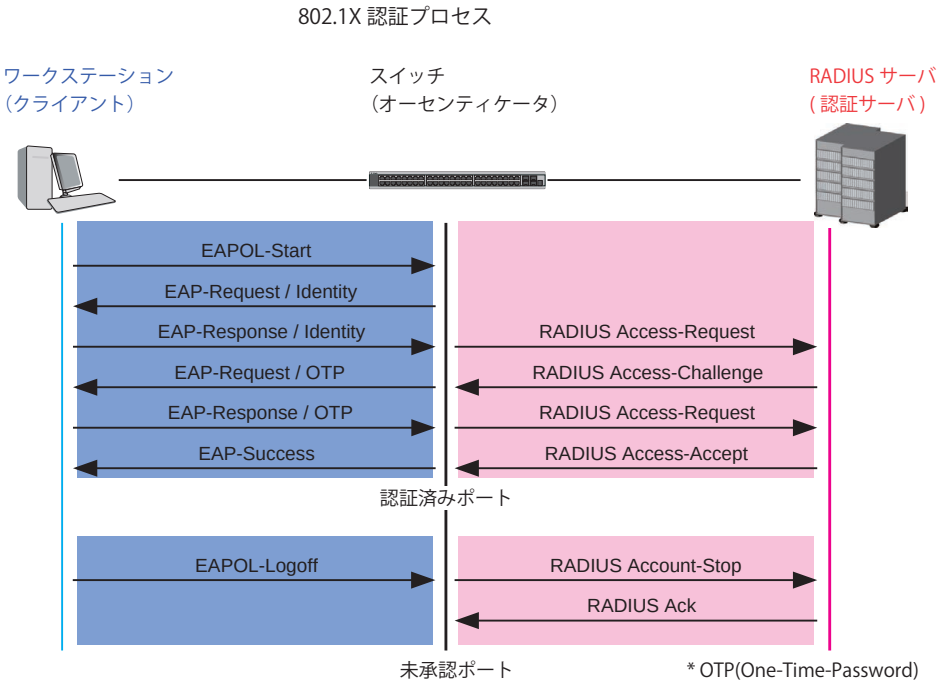


図 13-6　802.1X 認証プロセス

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 16 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。

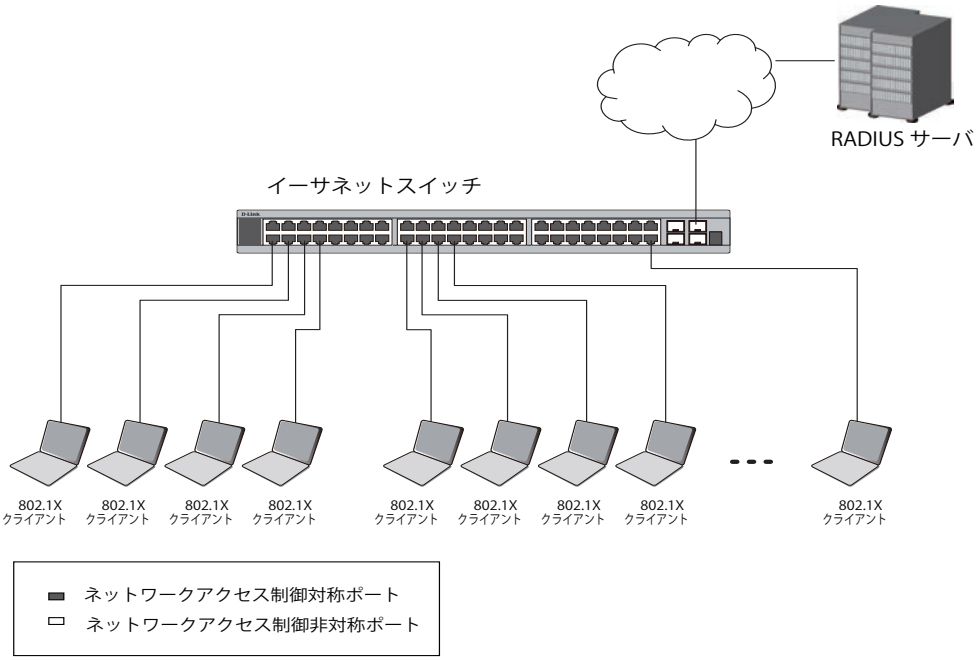


図 13-7　典型的なポートベースアクセスコントロールのネットワーク構成例

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

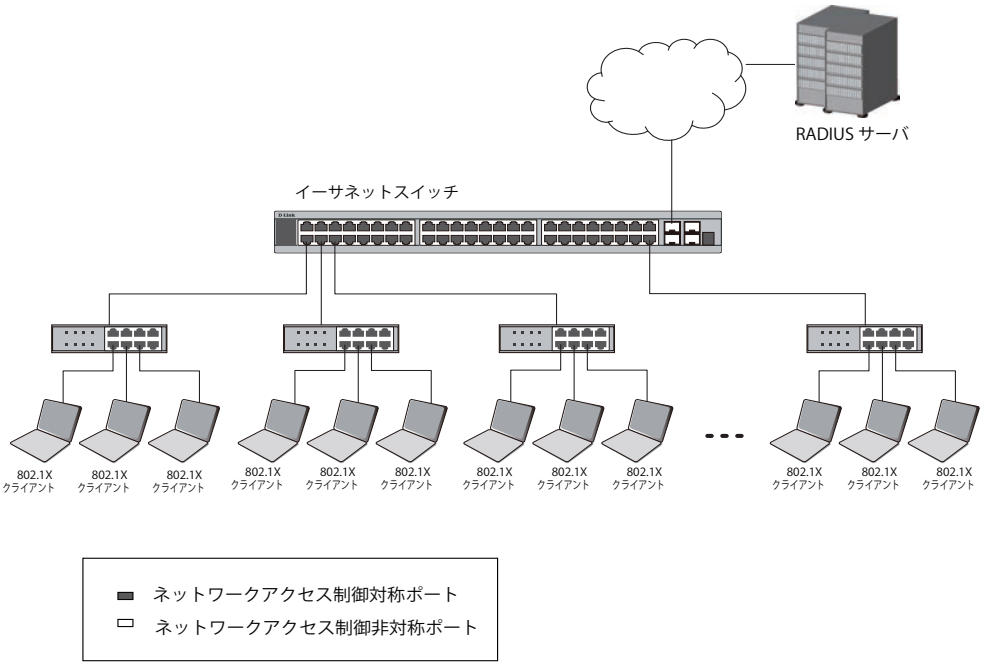


図 13-8　典型的な MAC ベースアクセスコントロールのネットワーク構成例

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。

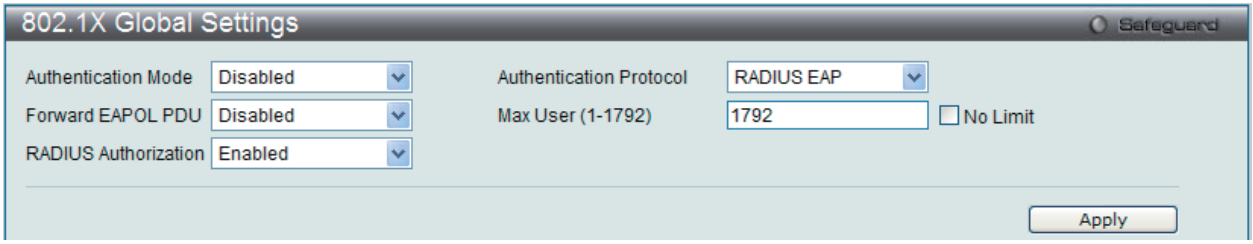


図 13-9　802.1X Global Settings 画面

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 認証モードを「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	ユーザの最大数を指定します。最大ユーザ数は 1792 です。
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。

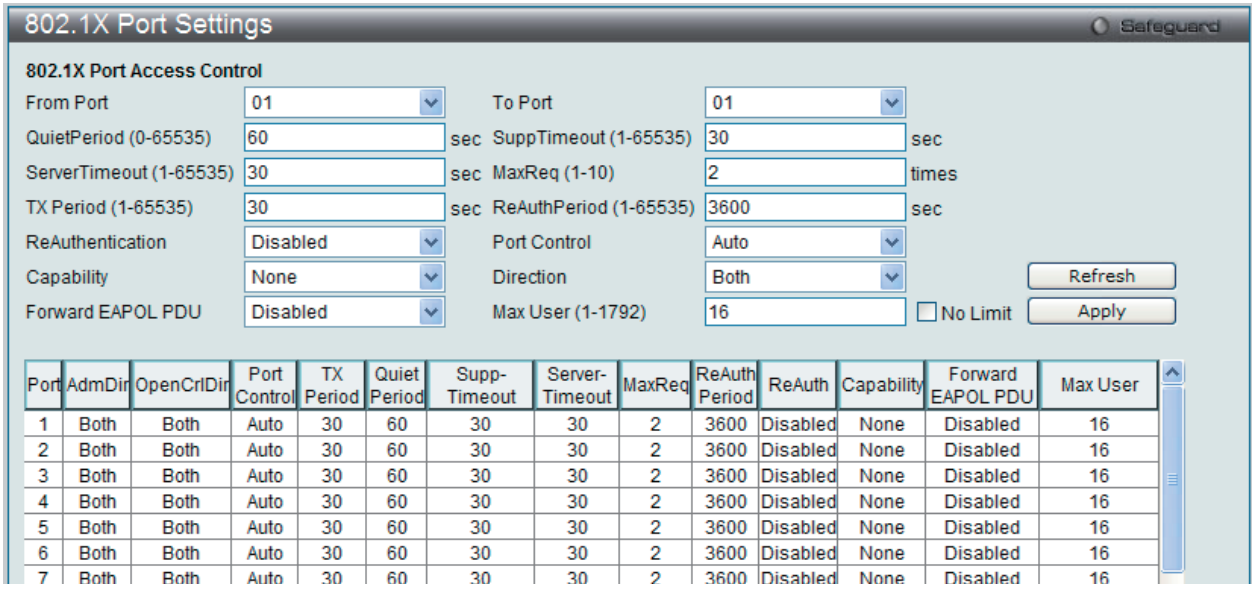


図 13-10　802.1X Port Settings 画面

以下の項目を使用して設定を行います。

項目	説明
From / To	設定対象のポート（範囲）を指定します。
QuietPeriod	クライアントの認証に失敗した後、クライアントとの通信を拒否する期間。初期値は 60（秒）です。
Supp Timeout	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。
Server Timeout	オーセンティケータが RADIUS サーバに Access-Request を送信した後、応答を待つ時間。初期値は 30（秒）です。
MaxReq	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。
TxPeriod	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	0 以外の定数で、クライアントの再認証間隔を指定します。初期値は 3600（秒）です。
ReAuthentication	指定したポート上で通常の再認証を行うかを指定します。初期値は「Disabled」です。
PortControl	ポートの認証状態を制御できます。初期値は「Auto」です。 • 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。
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 - 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	制御するトラフィックの方向を指定します。初期値は「both」です。 • In - 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。 • 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。
Forward EAPOL PDU	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	ユーザの最大数を指定します。最大ユーザ数は 1792 です。初期値では、最大数が選択されています。

「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。

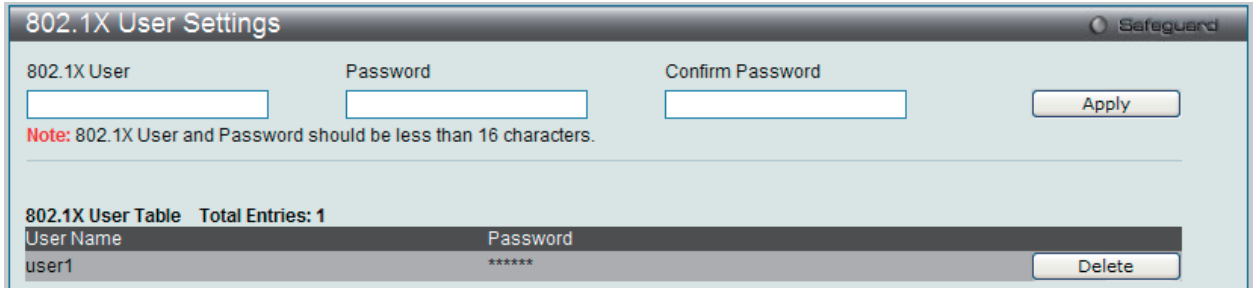


図 13-11 802.1X User Settings 画面

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。次に管理者は、ゲスト VLAN 内のスイッチにアクセスするゲストアカウントを作成します。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。

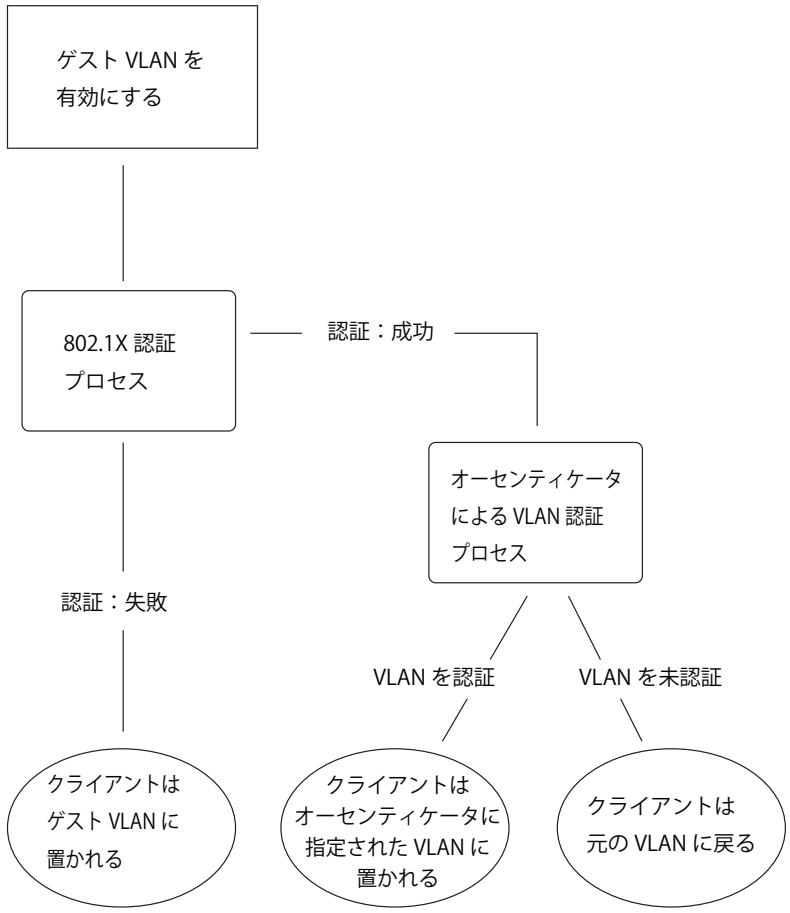


図 13-12　ゲスト VLAN 認証プロセス画面

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。

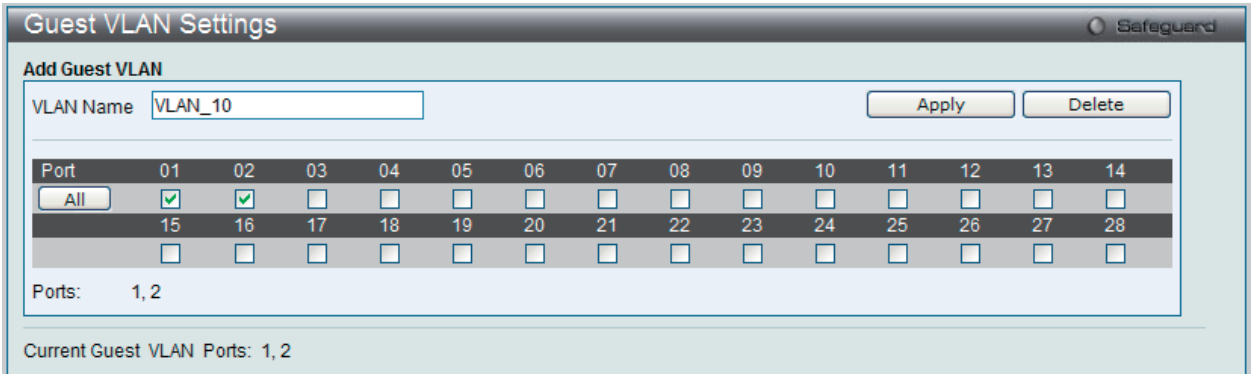


図 13-13 Guest VLAN Settings 画面

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。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

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。

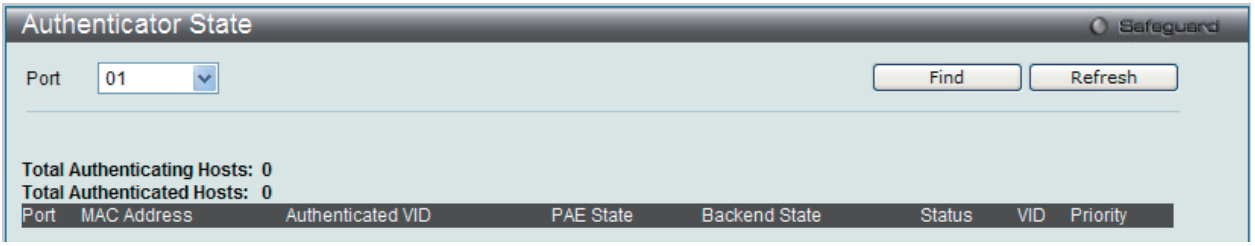


図 13-14 Authenticator State 画面

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。

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。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

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。

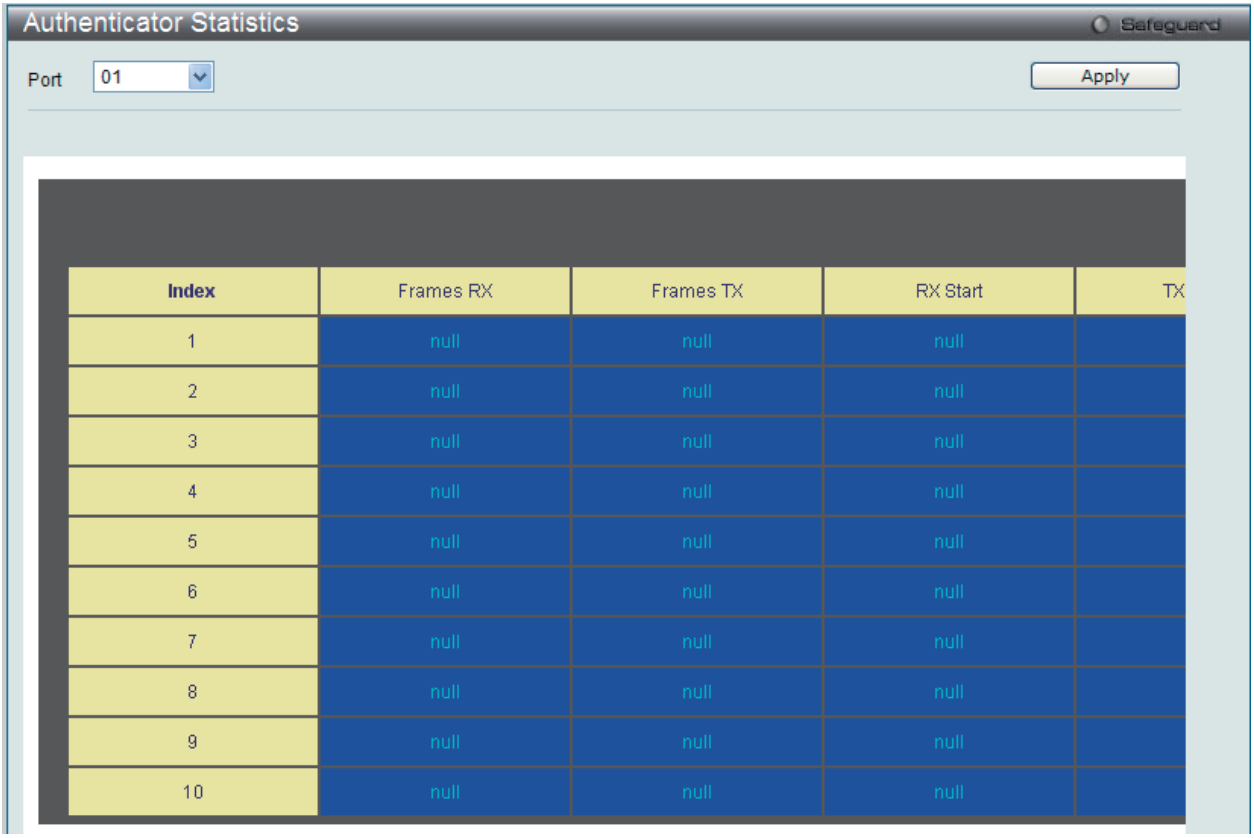


図 13-15　Authenticator Statics 画面（ポートベース）

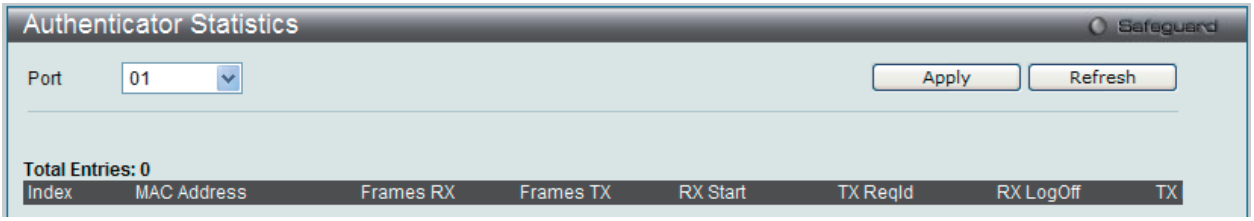


図 13-16　Authenticator Statics 画面（MAC ベース）

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。

「Apply」ボタンをクリックして行った変更を適用します。

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。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

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 13-17　Authenticator Session Statistics 画面（ポートベース）

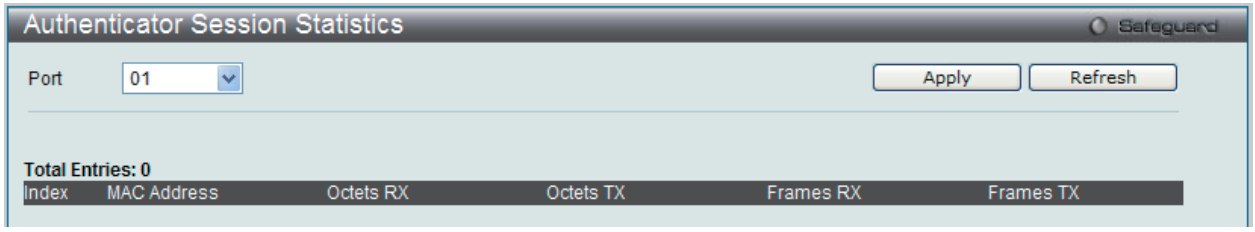


図 13-18　Authenticator Session Statistics 画面（MAC ベース）

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。

「Apply」ボタンをクリックして行った変更を適用します。

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。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

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。

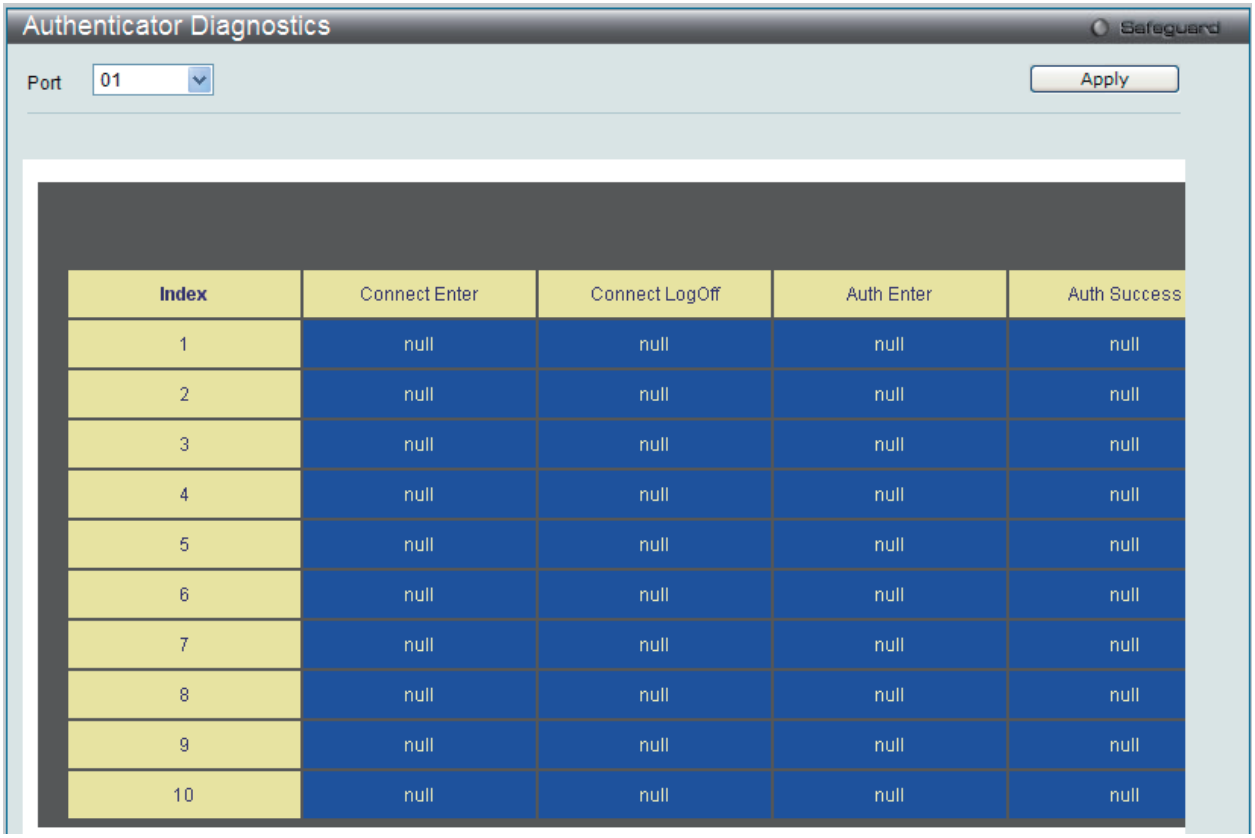


図 13-19　Authenticator Diagnostics 画面（ポートベース）

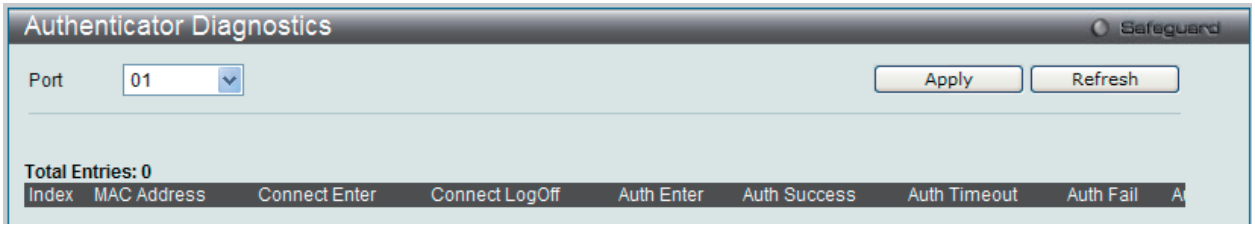


図 13-20　Authenticator Diagnostics 画面（MAC ベース）

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。

「Apply」ボタンをクリックして行った変更を適用します。

Initialize Port(s)（初期化ポート）

ポートの 802.1X 認証ステートマシンの初期化と現在の初期化されているポートを表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Initialize Port(s) の順にメニューをクリックし、以下の画面を表示します :

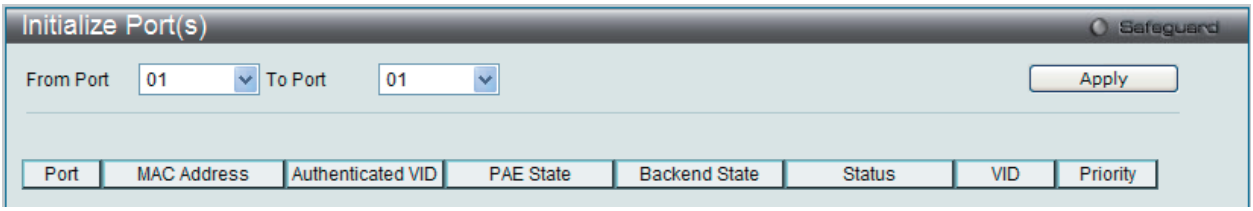


図 13-21 Initialize Port(s) 画面（ポートベース）

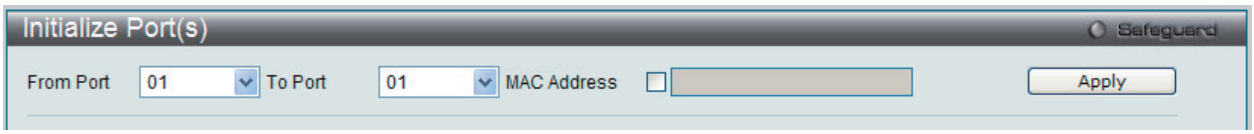


図 13-22 Initialize Port(s) 画面（MAC ベース）

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	プルダウンメニューを使用して初期化するポート範囲を指定します。
MAC Address	選択し、適切な MAC アドレスを入力します。「802.1X Global Settings」画面で「Authentication Mode」が「MAC-based」に設定されている場合だけ、本オプションは利用可能です。

「Apply」ボタンをクリックして行った変更を適用します。

Reauthenticate Port(s)（再認証ポート）

ポートに接続するデバイスの再認証の実行、および現在の再認証ポート（ポートベース）の状態の表示を行います。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Reauthenticate Port(s) の順にメニューをクリックし、以下の画面を表示します。

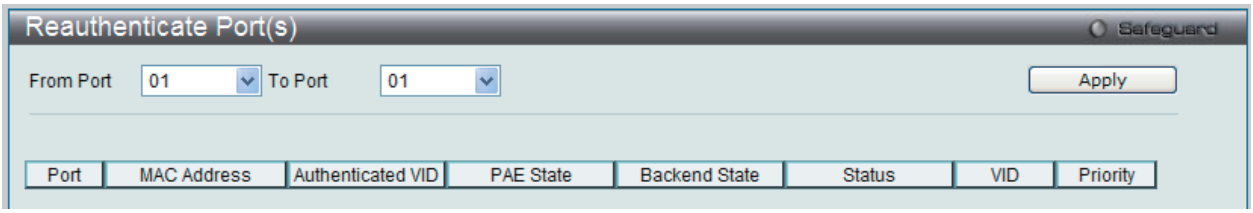


図 13-23 Reauthenticate Port(s) 画面（ポートベース）

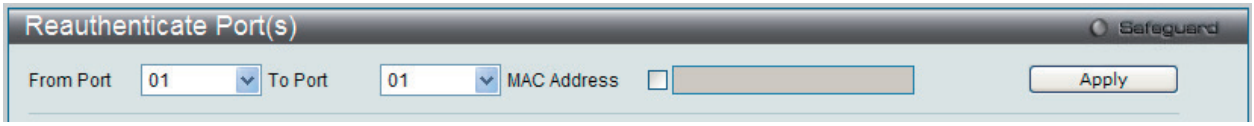


図 13-24 Reauthenticate Port(s) 画面（MAC ベース）

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	プルダウンメニューを使用して再認証するポート範囲を指定します。
MAC Address	選択して、本設定に使用する MAC アドレスを入力します。「802.1X Global Settings」画面で「Authentication Mode」が「MAC-based」に設定されている場合だけ、本オプションは利用可能です。

「Apply」ボタンをクリックして行った変更を適用します。

RADIUS（RADIUS 設定）

Authentication RADIUS Server Settings（認証 RADIUS サーバ設定）

スイッチの認証 RADIUS サーバを設定します。本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による攻撃から保護します。

Security > 802.1X > 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。

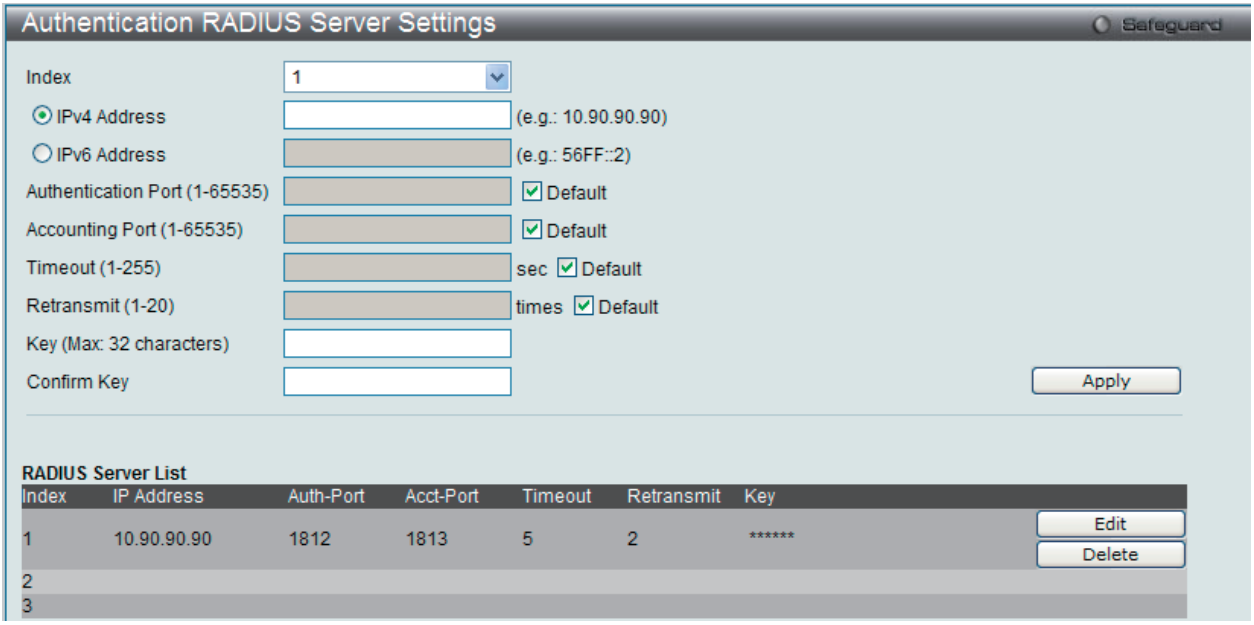


図 13-25　Authentic RADIUS Server Settings 画面

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」、「IPv4 Address」または「IPv6 Address」から設定を行う RADIUS サーバを選択します。 • IPv4 Address - RADIUS サーバの IPv4 アドレスを入力します。 • IPv6 Address - RADIUS サーバの IPv6 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 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。
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。
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、以下の画面を表示します。

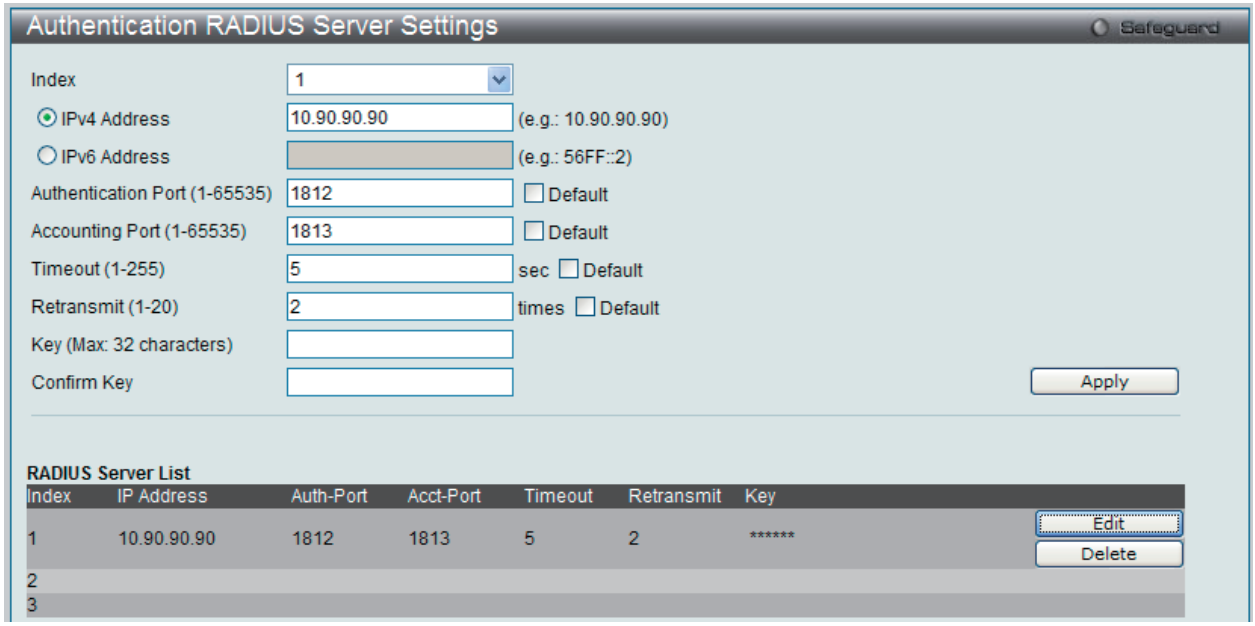


図 13-26 Authentic RADIUS Server Settings 画面 - Edit

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 > 802.1X > 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。

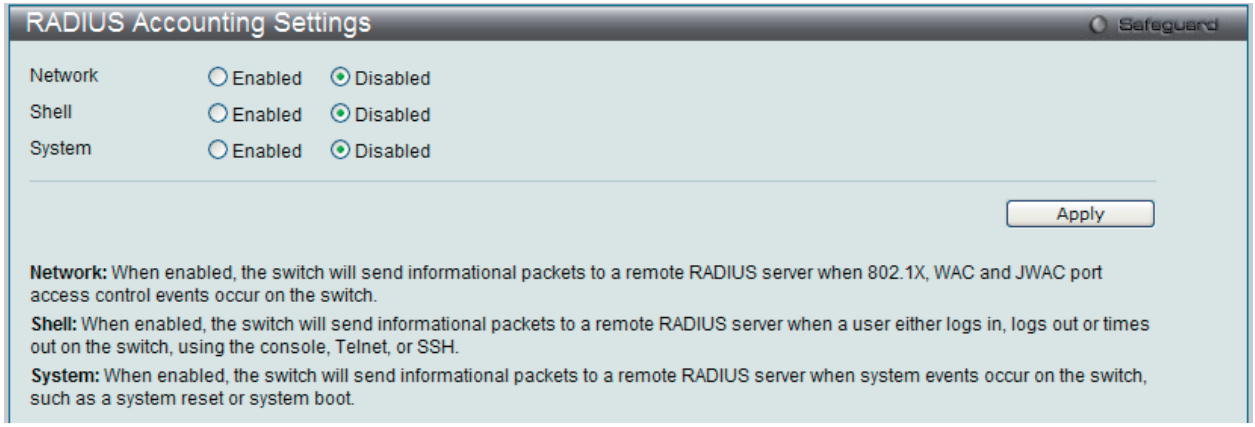


図 13-27 RADIUS Accounting Settings 画面

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、WAC および JWAC 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 > 802.1X > RADIUS Authentication をクリックし、以下の画面を表示します。

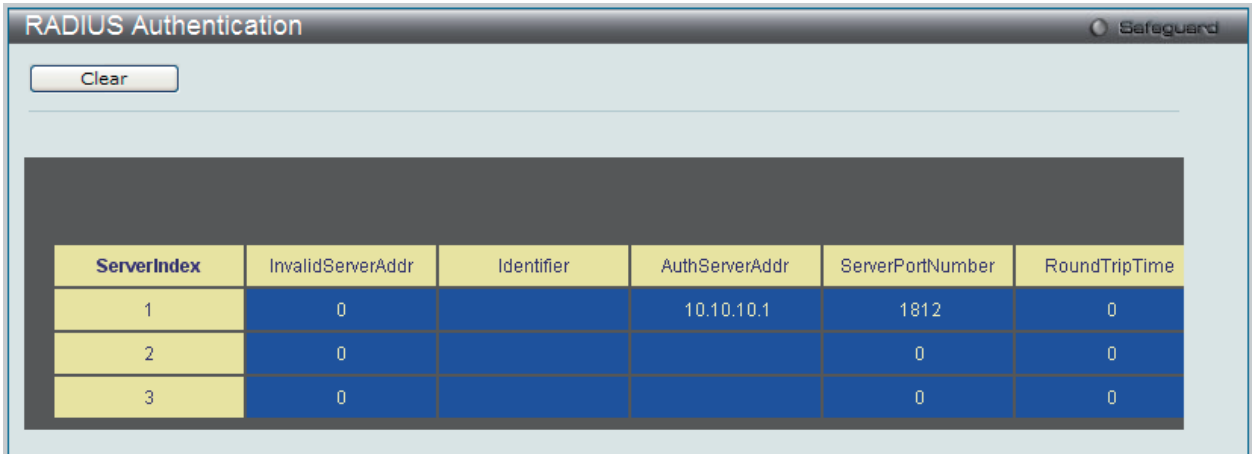


図 13-28 RADIUS Authentication 画面

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。
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 > 802.1X > RADIUS Accounting Client をクリックし、以下の画面を表示します。

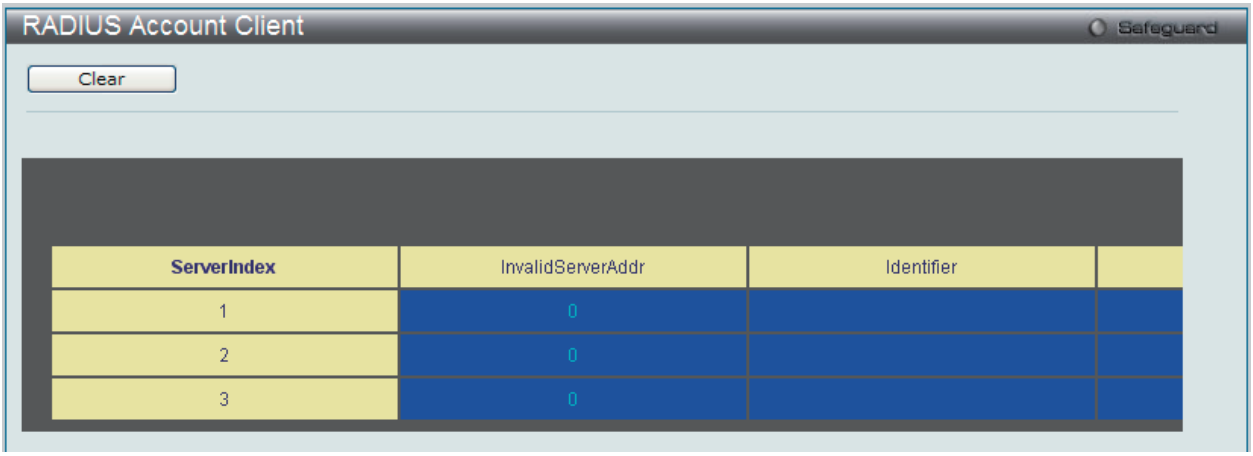


図 13-29　RADIUS Accounting Client 画面

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ます。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。IP-MAC バインディングが有効なポートに未認証ユーザが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。xStack DES-3810 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。最大エントリ数は 511 です。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）は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 パケットをスイッチに受信した場合に、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 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。

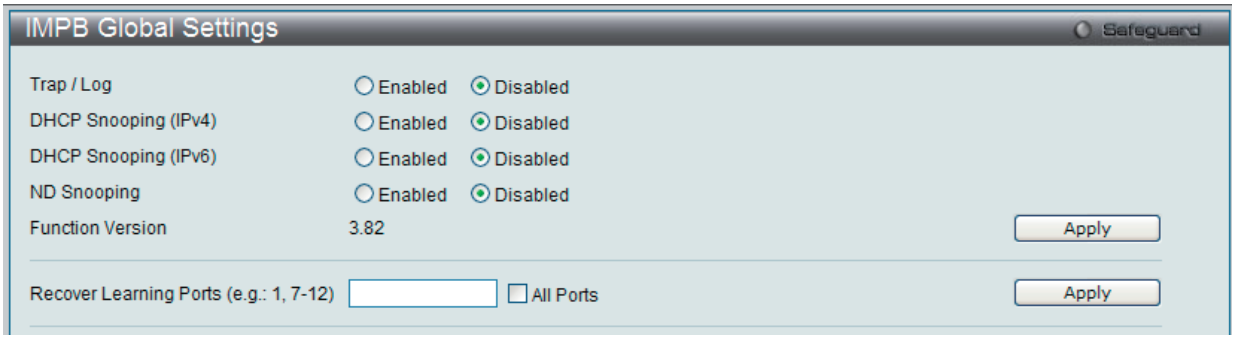


図 13-30　IMPB Global Settings 画面

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 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 (IPv4)	IP-MAC- ポートバインディングの DHCP Snooping(IPv4) 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。
DHCP Snooping (IPv6)	IP-MAC- ポートバインディングの DHCP Snooping(IPv6) 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。
ND Snooping	スイッチの ND Snooping を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Recover Learning Ports (e.g.: 1, 7-12)	学習状態を回復するポート番号を選択します。「All Ports」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 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。

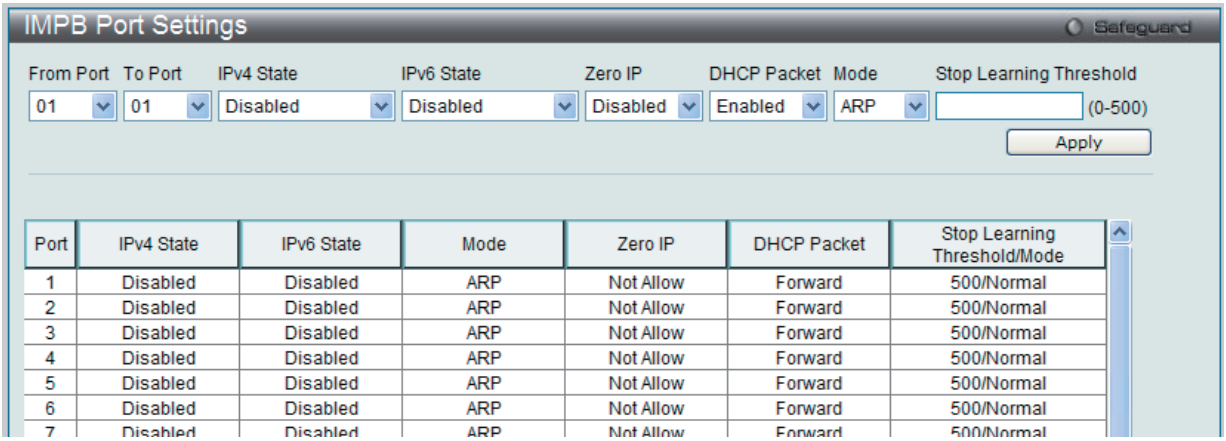


図 13-31　IMPB Port Settings 画面

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。
IPv4 State	これらのポートの IPv4-MAC バインディングを「Enabled」（有効）または「Disabled」（無効）にします。
IPv6 State	これらのポートの IPv6-MAC バインディングを「Enabled」（有効）または「Disabled」（無効）にします。
IPv4/IPv6 State	IP-MAC バインディングを「Enabled」（有効）または「Disabled」（無効）にします。 • Enabled (Strict) - 本モードはより厳しいコントロール方法を提供します。本モードを選択した場合、すべてのパケットは CPU に送られ、その結果 S/W にポートのエントリを入力するまで、ハードウェアはすべてのパケットを送信しません。ポートは、IP-MAC- ポートバインディングエントリによって ARP パケットと IP パケットをチェックします。パケットがエントリにあった場合、MAC アドレスは「dynamic」に設定されます。パケットがエントリにない場合、MAC アドレスは「block」に設定されます。そのほかのパケットは破棄されます。（初期値） 「strict」モードのポートは、ACL モジュールを通るユニキャスト DHCP パケットを捕捉します。IP-MAC バインディングの DHCP Snooping の状態が有効な時に IP-MAC バインディングポートを「strict」モードに設定すると、ポートに基づいて ACL プロファイルとルールを作成します。ACL プロファイルまたはルールテーブルに十分なプロファイルまたはルールの空きスペースがない場合、警告メッセージを返し、ユニキャスト DHCP パケットをキャプチャする ACL プロファイルとルールは作成されません。 • Enabled (Loose) - 本モードは、より緩いコントロール方法を提供します。本モードを選択した場合、ARP パケットと IP ブロードキャストパケットは CPU に送信されます。パケットは、特定の送信元 MAC アドレスがソフトウェアによってブロックされるまで、ハードウェアによって転送されます。ポートは、IP-MAC- ポートバインディングエントリに従って ARP パケットと IP ブロードキャストパケットをチェックします。パケットがエントリにあった場合、MAC アドレスは「dynamic」に設定されます。パケットがエントリにない場合、MAC アドレスは「block」に設定されます。その他のパケットは迂回します。
Zero IP	本機能を「Enabled」（有効）/「Disabled」（無効）にします。一度有効にすると、スイッチは、0.0.0.0 の送信元 IP を持つ ARP パケットが通過することを許可します。
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。
Mode	ARP または ACL を選択して、IP-MAC バインディング設定のモードを設定します。 • ACL - スイッチはこのポートのエントリに対応する ACL アクセスエントリを作成します。 • ARP - すべての ACL アクセスエントリが自動的に削除されます。（初期値）
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。

IP-MAC- ポートバインディングの設定

1. 「From Port」と「To Port」欄でポートまたはポート範囲を指定します。
2. 「State」、「Zero IP」、「DHCP Packet」を「Enabled」（有効）または「Disabled」（無効）にして、ポートの「Mode」および「Stop Learning Threshold」を設定します。
3. 「Apply」ボタンをクリックして設定を適用します。

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 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。

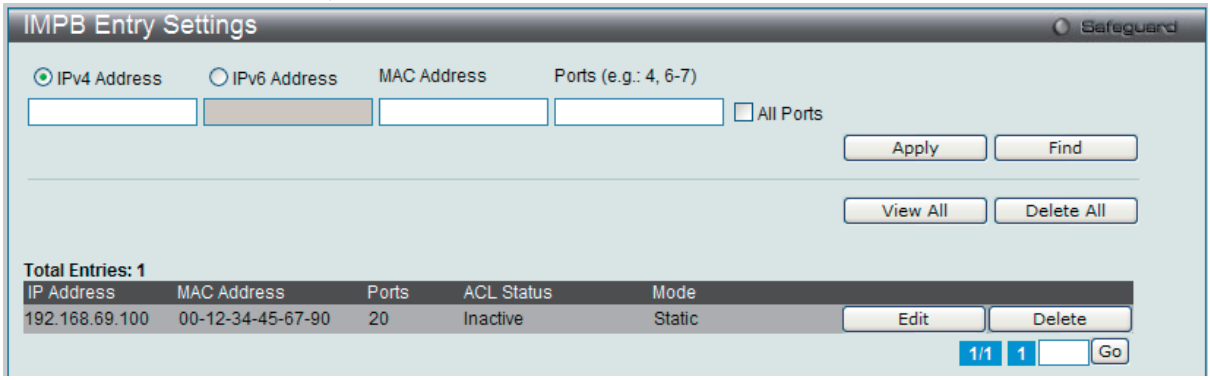


図 13-32 IMPB Entry Settings 画面

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
IPv4 Address	MAC アドレスにバインドする IPv4 アドレスを入力します。
IPv6 Address	MAC アドレスにバインドする IPv6 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- ポートバインディングエントリを設定する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、以下の画面を表示します。

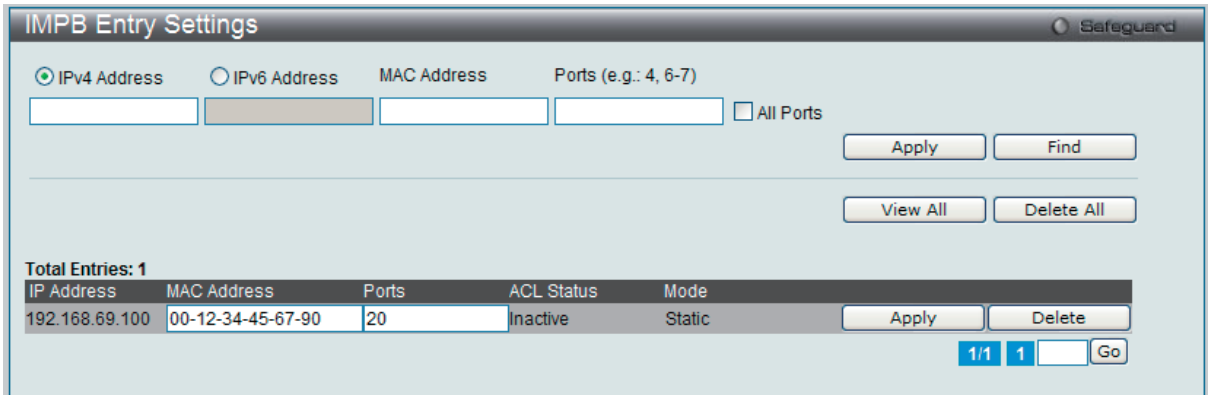


図 13-33 IMPB Entry Settings 画面 - Edit

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。

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 > 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。

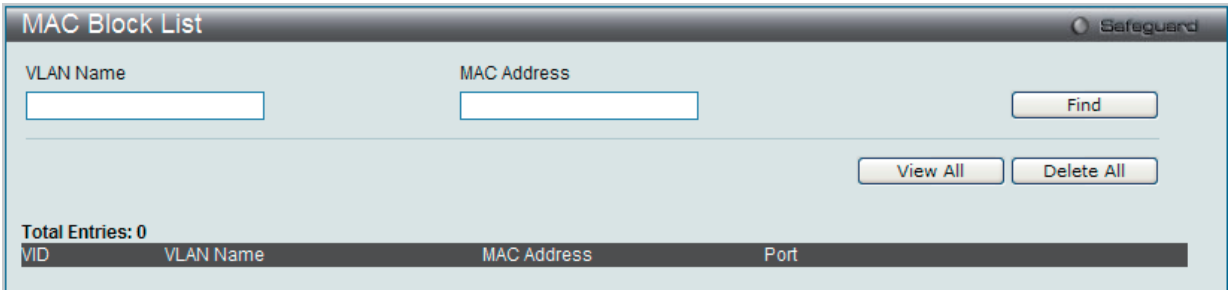


図 13-34　MAC Block List 画面

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 ID 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 Max 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 > DHCP Snooping > DHCP Snooping Max Entry Settings の順にクリックして、以下の画面を表示します。

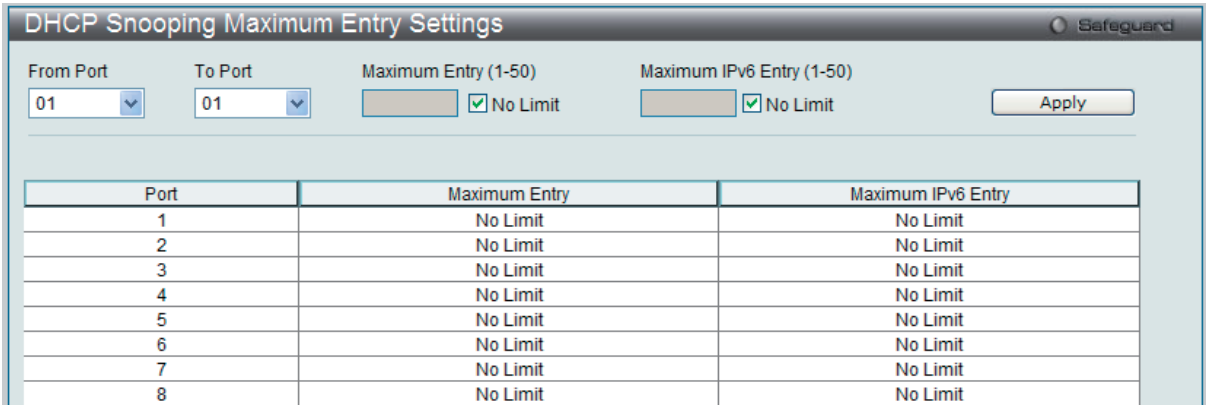


図 13-35　DHCP Snooping Max Entry Settings 画面

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制限がなくなります。
Maximum IPv6 Entry (1-50)	IPv6 DHCP Snooping の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制限がなくなります。

「Apply」ボタンをクリックして行った変更を適用します。

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 > 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。

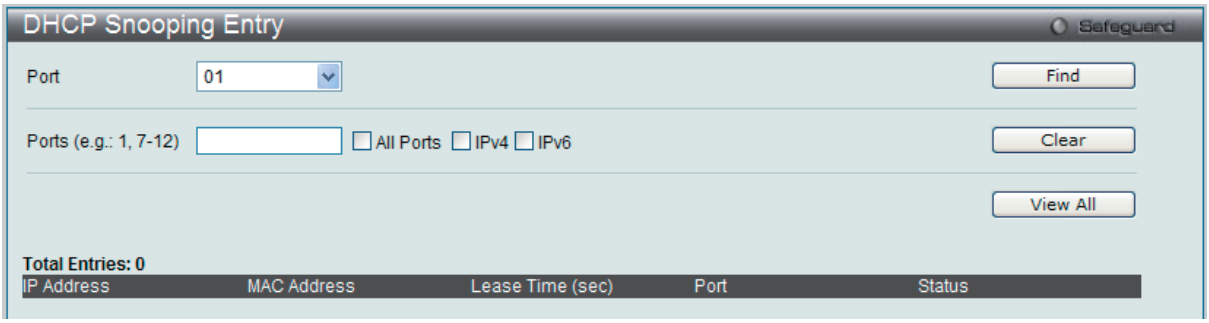


図 13-36 DHCP Snooping Entry 画面

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 (e.g.: 1, 7-12)	DHCP Snooping エントリのポートを指定します。「All Ports」を選択すると、すべてのポートの全エントリを選択します。 • IPv4 - IPv4 DHCP Snooping が学習したエントリを選択します。 • IPv6 - IPv6 DHCP Snooping が学習した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。

ND Snooping（ND Snooping 設定）

ND Snooping Maximum Entry Settings（ND Snooping 最大エントリ設定）

ND Snooping の最大エントリをポートに設定します。

Security > IP-MAC-Port Binding (IMPB) > ND Snooping > ND Snooping Maximum 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。

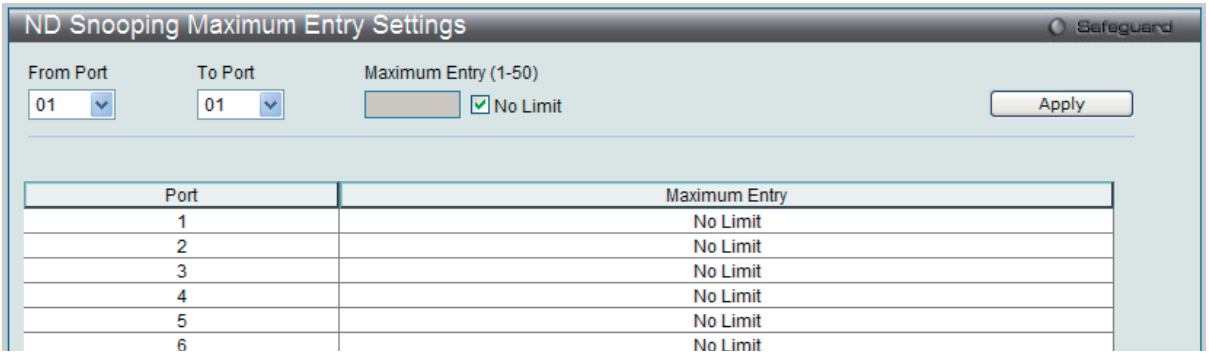


図 13-37 ND Snooping Maximum Entry Settings 画面

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	プルダウンメニューにより、ND Snooping を使用して学習可能な最大エントリ数の制限を必要とするポート範囲を指定します。
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制限がなくなります。

「Apply」ボタンをクリックして行った変更を適用します。

ND Snooping Entry（ND Snooping エントリ）

指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) > ND Snooping > ND Snooping Entry の順にメニューをクリックし、以下の画面を表示します。

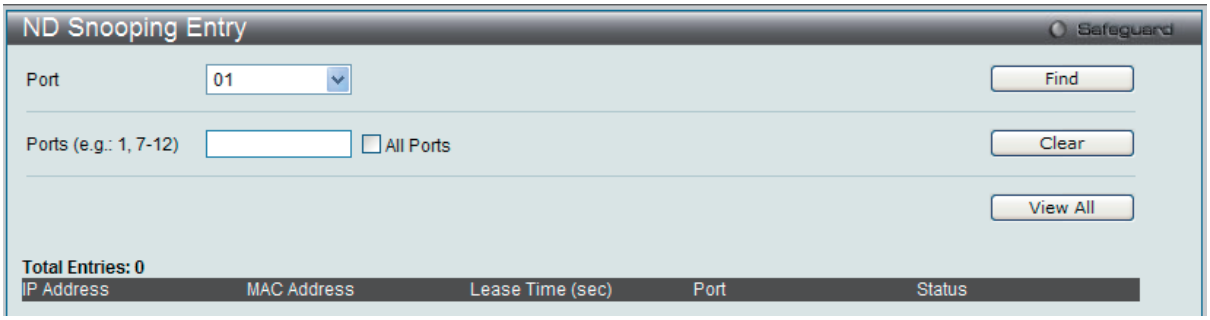


図 13-38 ND Snooping Entry 画面

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	ND Snooping エントリのポートを指定します。「All Ports」を選択すると、すべてのポートの全エントリを選択します。

「Find」ボタンをクリックして、選択したポート番号に基づいて指定エントリを検出します。
「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。
「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-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 MAC にはポートアクセス権を決定し、一方ホストベース 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、802.1X 認証、802.1X ゲスト VLAN、ポートセキュリティ、GVRP または Web ベース認証が有効なポートは、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

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ませんできないことにご注意ください。

Security > MAC-based Access Control > 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。

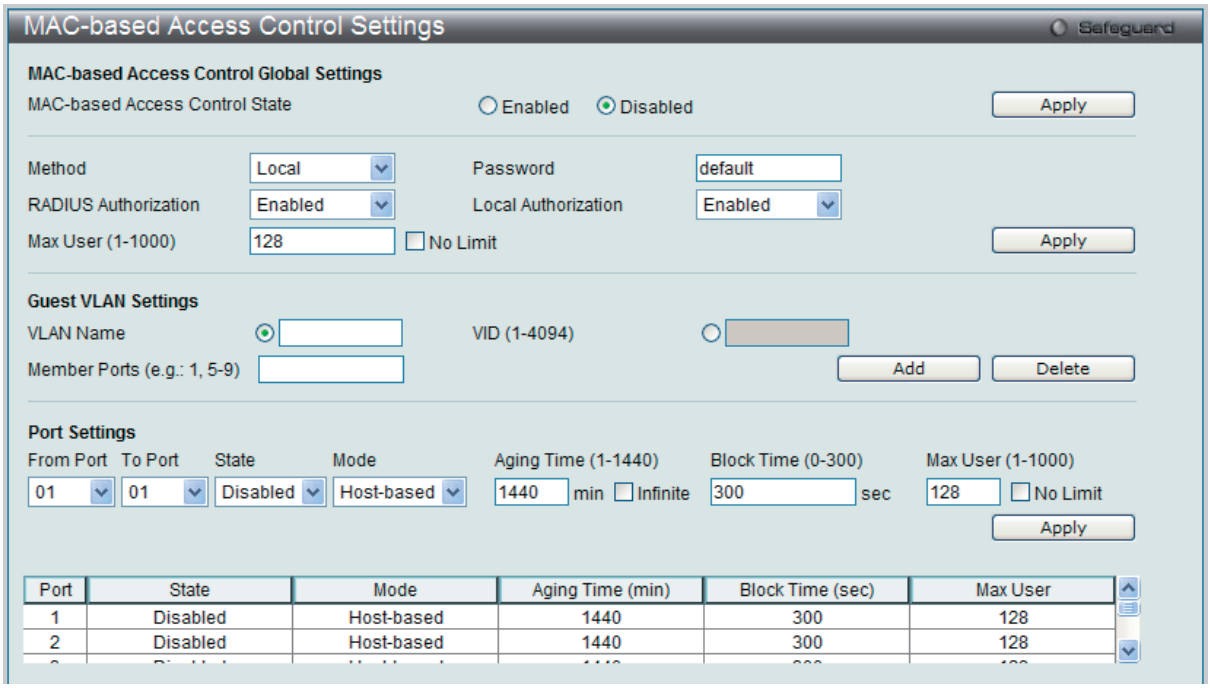


図 13-39　MAC-based Access Control Settings 画面

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。MAC リストははじめに RADIUS サーバに設定されている必要があり、サーバの設定もスイッチに設定されている必要があることにご注意ください。
Password	認証リクエストのパケットの送信に使用する 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。
Max User	スイッチの最大ユーザ数を指定します。「No Limit」をチェックすると無制限になります。
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。
VLAN ID	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。
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」と「Host-based」の切り換えをします。
Aging Time (1-1440)	1-1440(分) の範囲で指定します。初期値は 1440 です。
Block Time (0-300)	1-300（秒）の値を入力します。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、本ルールにユーザの制限はなくなります。

「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 と共に 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-based Access Control Local Settings をクリックし、以下の画面を表示します。

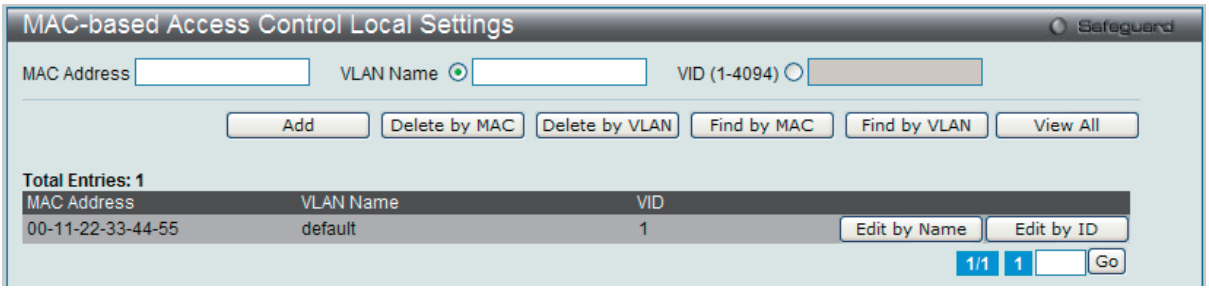


図 13-40 MAC-based Access Control Local Settings 画面

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 Local Authentication List 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。

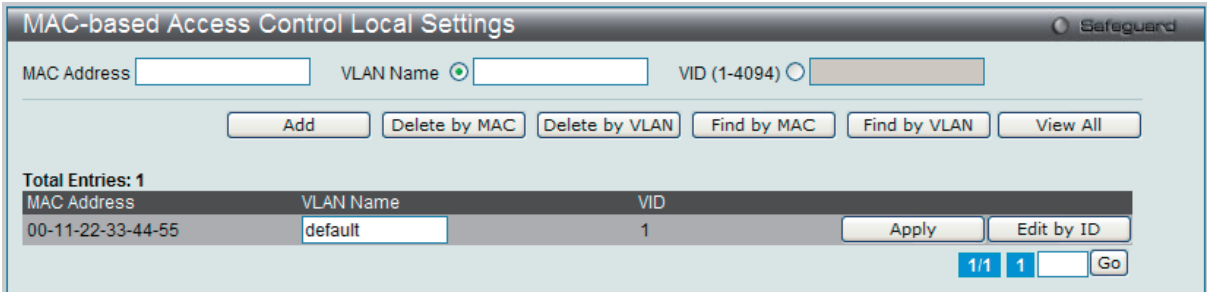


図 13-41　Edit by VLAN Name 画面

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。

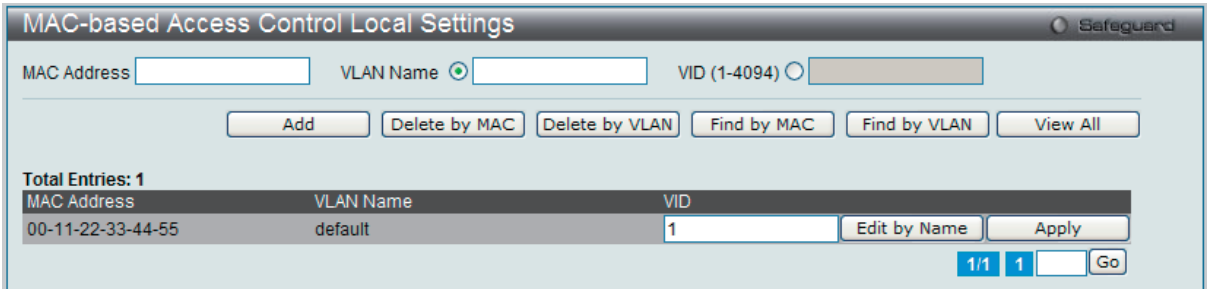


図 13-42　Edit by VID 画面

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。

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-based Access Control Authentication State をクリックし、以下の画面を表示します。

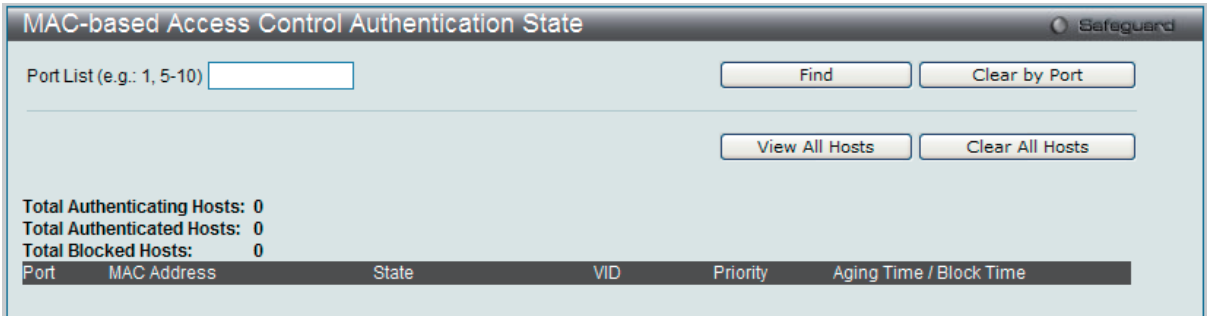


図 13-43　MAC-based Access Control Authentication State

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。

Web-based Access Control (WAC)（Web ベースのアクセス制御）

Web ベース認証のログインは、スイッチを経由してインターネットにアクセスを試みる場合に、ユーザを認証するように設計された機能です。認証処理には HTTP プロトコルを使用します。Web ブラウザ経由で Web ページ (例 : http://www.dlink.com) の閲覧を行う場合に、スイッチは認証段階に進みます。スイッチは、HTTP パケットを検出し、このポートが未認証である場合に、ユーザ名とパスワードの画面を表示して、ユーザに問い合わせます。認証処理を通過するまで、ユーザはインターネットにアクセスすることはできません。

スイッチは、認証サーバとなってローカルデータベースに基づく認証を行うか、または RADIUS クライアントとなってリモート RADIUS サーバと共に RADIUS プロトコルを介する認証処理を実行します。Web へのアクセスを試みることによって、クライアントユーザは WAC の認証処理を開始します。

D-Link の WAC の実行には、WAC 機能が排他的に使用し、スイッチの他のモジュールに知られていない仮想 IP を使用します。実際は、スイッチの他の機能への影響を避ける場合にだけ、WAC は仮想 IP アドレスを使用してホストとの通信を行います。そのため、すべての認証要求を仮想 IP アドレスに送信し、スイッチの物理インタフェースの IP アドレスには送信しないようする必要があります。

ホスト PC が仮想 IP 経由で WAC スイッチと通信する場合、仮想 IP は、スイッチの物理的な IPIF(IP インタフェース) アドレスに変換されて通信を可能にします。ホスト PC と他のサーバの IP 構成は WAC の仮想 IP に依存しません。仮想 IP は、ICMP パケットまたは ARP リクエストに応答しません。つまり、仮想 IP は、スイッチの IPIF(IP インタフェース) と同じサブネット、またはホスト PC のサブネットと同じサブネットには設定することはできません。

認証済みおよび認証中のホストから仮想 IP に送信されるすべてのパケットがスイッチの CPU にトラップされるため、仮想 IP が他のサーバまたは PC と同じであると、WAC が有効なポートに接続するホストは、IP アドレスを実際に所有しているサーバまたは PC とは通信ができません。ホストがサーバまたは PC にアクセスする必要がある場合、仮想 IP をサーバまたは PC の 1 つと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、PC のユーザは、認証を適切に実行するために、プロキシ設定の例外として仮想 IP を加える必要があります。仮想 IP を指定するかどうかに関わらず、ユーザはスイッチのシステム IP を経由して WAC ページにアクセスします。仮想 IP を指定しない場合、認証中の Web のリクエストは、スイッチのシステム IP にリダイレクトされます。

スイッチの WAC の実行は、ユーザ定義のポート番号により HTTP または HTTPS プロトコルのいずれかに対して TCP ポートを設定できることを特徴としています。HTTP か HTTPS に対するこの TCP ポートは、認証処理のために CPU にトラップされる HTTP か HTTPS パケットを識別するためやログインページにアクセスするために使用されます。指定しない場合、HTTP に対するポート番号の初期値は 80、HTTPS に対するポート番号の初期値は 443 となります。プロトコルも指定されないと、プロトコルの初期値は HTTP になります。

以下の図は、Web 認証処理を成功させるために通過する基本的な 6 段階を示しています。

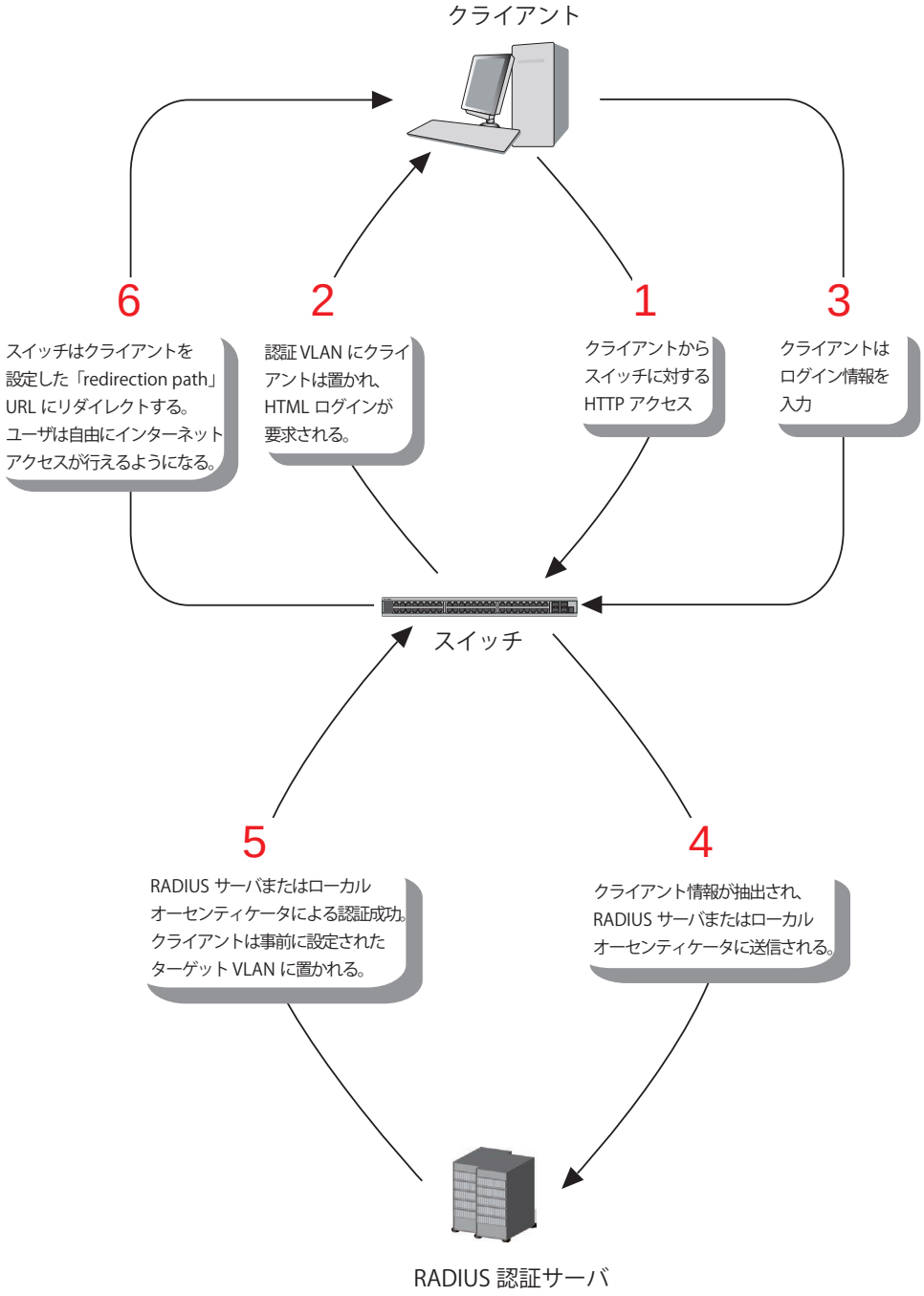


図 13-44 Web 認証プロセス画面

条件および制限

Web ベースアクセスコントロールにはいくつかの制限と規則があります。

1. クライアントが IP アドレス取得のために DHCP を使用している場合、認証 VLAN はクライアントが IP アドレス取得を行えるように、DHCP サーバまたは DHCP リレー機能を持つ必要があります。
2. アクセスプロファイル機能のように、スイッチ上に存在する機能の中には HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
3. 認証に RADIUS サーバを使用する場合、Web 認証を有効にする前に、ターゲット VLAN を含む必要なパラメータを入力して RADIUS サーバの設定を行います。

注意 WAC/JWAC 認証では、System インタフェースがアップ状態である必要があります。

WAC Global Settings（WAC グローバル設定）

MAC ベースアクセスコントロール機能をスイッチに設定します。

Security > Web-based Access Control > WAC Global Settings をクリックし、以下の画面を表示します。

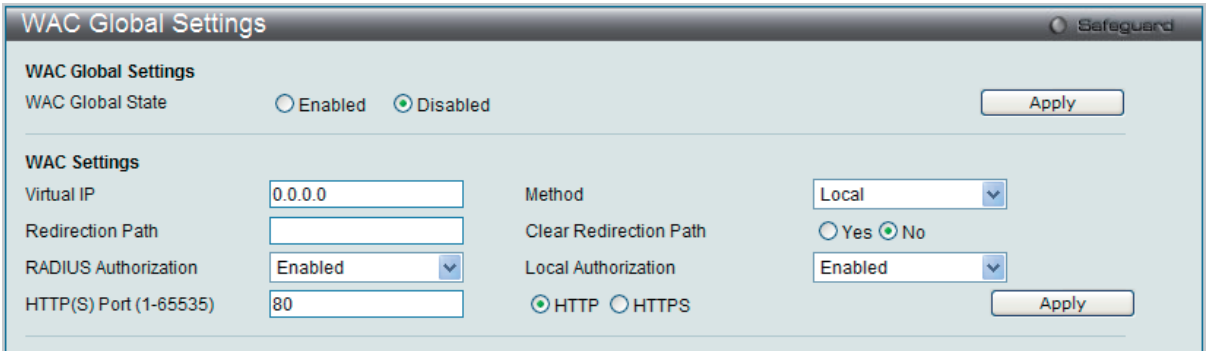


図 13-45　WAC Global Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
WAC Global State	Web ベースアクセスコントロール機能を「Enable」（有効）/「Disable」（無効）にします。
Virtual IP	仮想 IP アドレスを入力します。このアドレスは WAC にだけ使用され、スイッチの他のモジュールには知られません。
Method	Web ベースアクセスコントロールのオーセンティケータを選択します。 • Local - スイッチを経由してネットワークにアクセスを行うユーザの認証方法として、スイッチでのローカル認証を行う場合に指定します。後に示す「WAC User Settings」画面（**Security > Web-based Access Control > WAC User Settings**）を使用して設定する、スイッチへのアクセス用のユーザ名とパスワードがローカルで参照するデータベースとなります。 • RADIUS - スイッチを経由してネットワークにアクセスを行うユーザの認証方法として、リモート RADIUS サーバを使用する場合に指定します。管理者は、この RADIUS サーバを「Authentication RADIUS Server Settings」画面 (**Security > RADIUS > Authentication RADIUS Server Settings**) を使用して、事前に設定しておく必要があります。
Redirection Path	認証に成功し、ターゲット VLAN に割り当てられたユーザを導く Web サイトの URL を入力します。
Clear Redirection Path	リダイレクションパスのクリアを有効または無効にします。
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。
HTTP(S) Port (1-65535)	HTTP ポート番号を入力します。ポートの初期値は 80 です。 • HTTP - TCP ポートが WAC HTTP プロトコルを実行します。初期値は 80 です。HTTP ポートは TCP ポート 443 で動作しません。 • HTTPS - TCP ポートは WAC HTTPS プロトコルを実行します。初期値は 443 です。HTTPS は TCP ポート 80 で動作しません。

「Apply」ボタンをクリックし、設定を有効にします。

注意　認証に成功すると、クライアントは事前に設定したサイトへ誘導されます。このサイトが開かなくても「Fail」メッセージが表示されない場合は、そのクライアントは既に認証されています。その場合はブラウザの画面を更新するか、他の Web サイトへ接続してみてください。

WAC User Settings（WAC ユーザ設定）

Web 認証用のローカルデータベースのユーザアカウントの参照および設定を行います。

Security > Web-based Access Control > WAC User Settings をクリックし、以下の設定用画面を表示します。

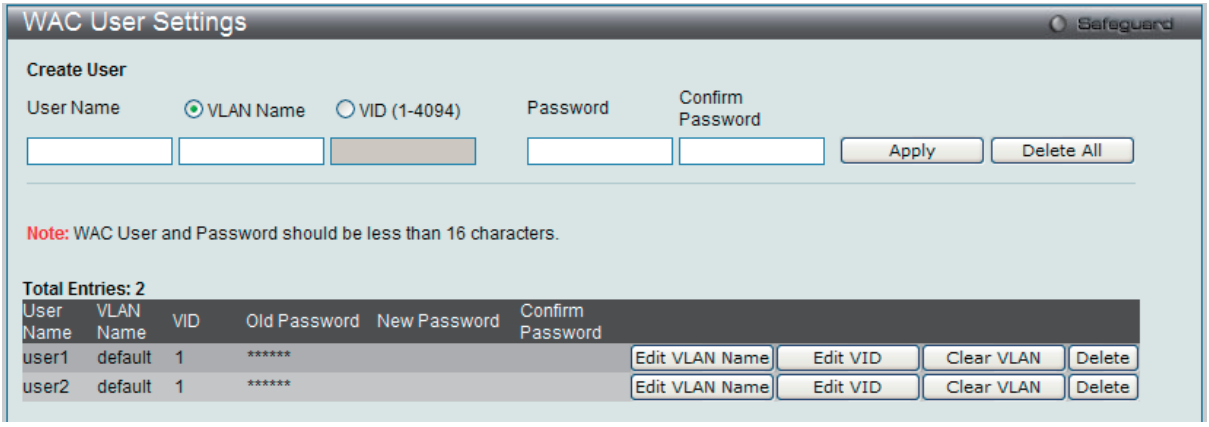


図 13-46　User Account Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
User Name	本プロセスを通して Web にアクセスを希望するユーザのユーザ名を 15 文字までの半角英数字で指定します。本項目は、オーセンティケータに「Local」を指定した場合、入力が必要です。
VLAN Name	先頭のラジオボタンをクリックして VLAN 名を入力します。
VLAN ID (1-4094)	先頭のラジオボタンをクリックして VLAN ID を入力します。
Password	上記ユーザ用に管理者が指定するパスワードを半角英数字で指定します。大文字、小文字は区別されます。本欄は、Web ベースのオーセンティケータに「Local」を選択した場合に管理者が使用します。
Confirm Password	確認のために再度同じパスワードを入力します。

「Apply」ボタンをクリックして行った変更を適用します。

VLAN 名の編集

1. 編集するエントリの「Edit VLAN Name」ボタンをクリックして、以下の画面を表示します。

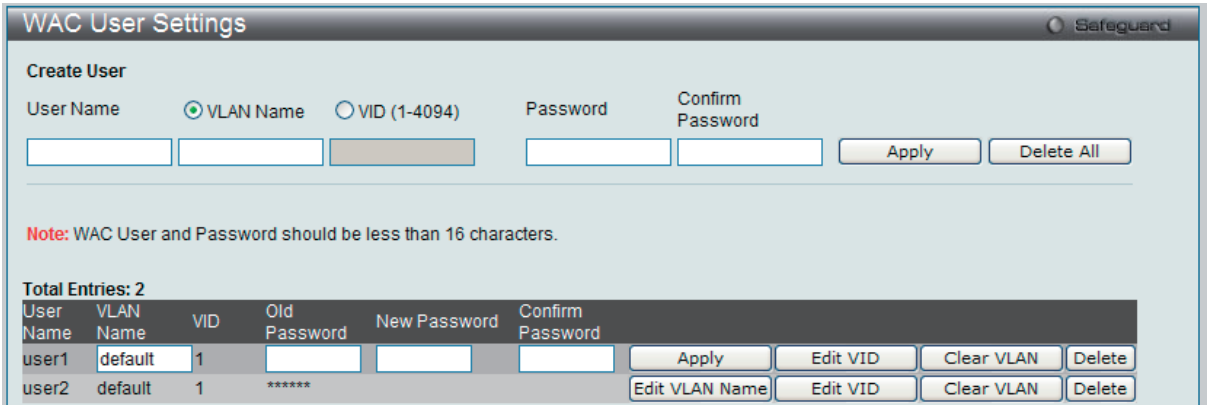


図 13-47　User Account Settings 画面 - Edit VLAN Name

2. VLAN 名を編集して「Apply」ボタンをクリックします。

VLAN ID の編集

1. 編集するエントリの「Edit VID」ボタンをクリックして、以下の画面を表示します。

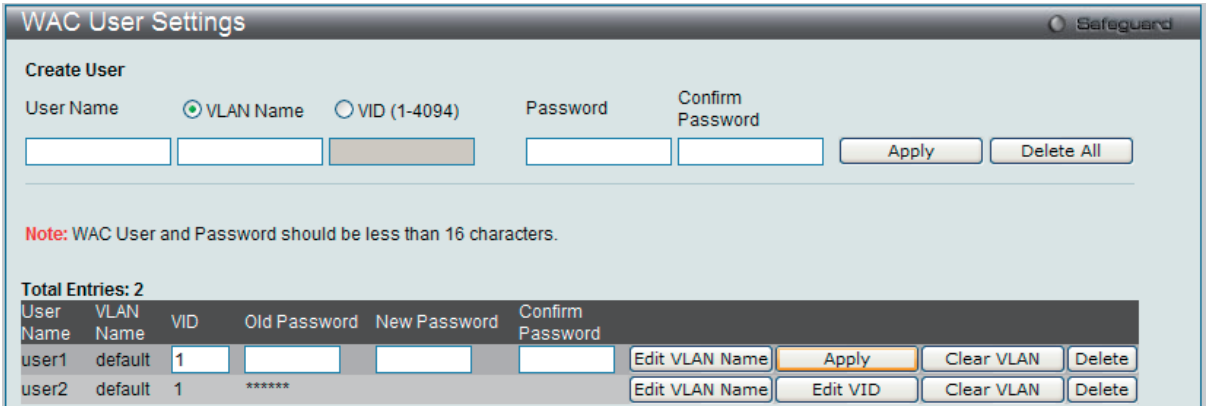


図 13-48 User Account Settings 画面 - Edit VID

2. VLAN ID を編集して「Apply」ボタンをクリックします。

エントリの削除

「Clear VLAN」ボタンをクリックして、指定エントリから VLAN 情報を削除します。

「Delete」ボタンをクリックして、指定エントリを削除します。「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 WAC ユーザ名とパスワードは 16 文字以内とします。

WAC Port Settings（WAC ポート設定）

Web 認証のためポート設定の表示またはポート設定を行います。

Security > Web-based Access Control > WAC Port Settings をクリックし、以下の設定用画面を表示します。

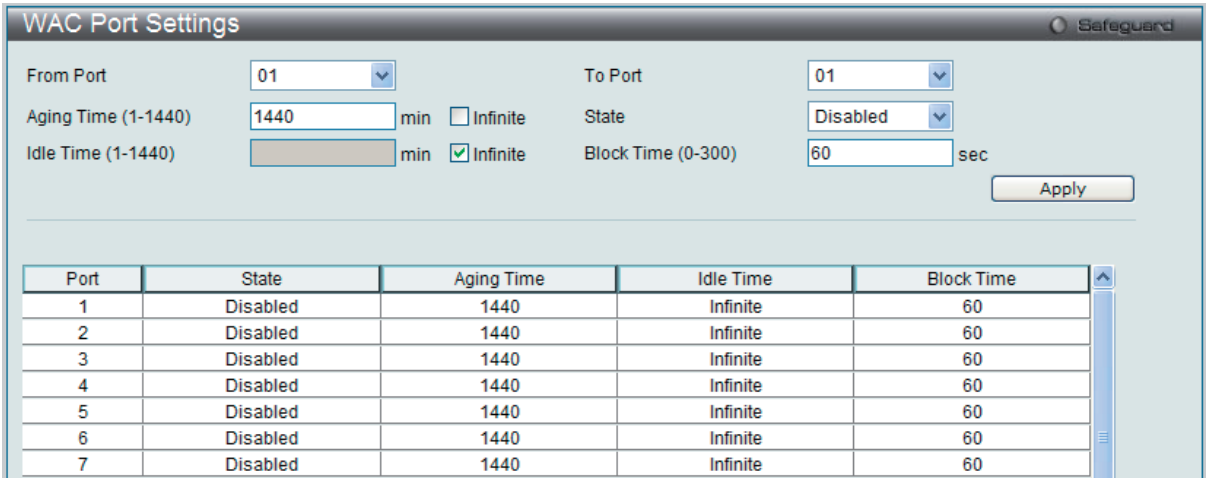


図 13-49 WAC Port Settings 画面

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	プルダウンメニューを使用して WAC ポートとして有効にするポート範囲を指定します。
Aging Time (1-1440)	認証ホストが認証状態を保つ時間を指定します。0-1440(分) の範囲で指定します。0 は、認証ホストがポート上でエージングしないことを示しています。初期値は 1440 分 (24 時間) です。
State	プルダウンメニューを使用して WAC ポートとして設定するポートを有効にします。
Idle Time (1-1440)	本設定時間にトラフィックがない場合、ホストは未認証状態に戻ります。0-1440(分) の範囲で指定します。0 を指定すると、ポート上の認証ホストのアイドル状態がチェックされません。初期値は「infinite」です。
Block Time (0-300)	認証に失敗した後にホストがブロック状態を維持する期間を指定します。1-300（秒）の範囲で指定します。初期値は 60（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。

WAC Authentication State（WAC 認証状態）

Web 認証用のホストの表示および削除を行います。

Security > Web-based Access Control > WAC Port Settings をクリックし、以下の設定用画面を表示します。

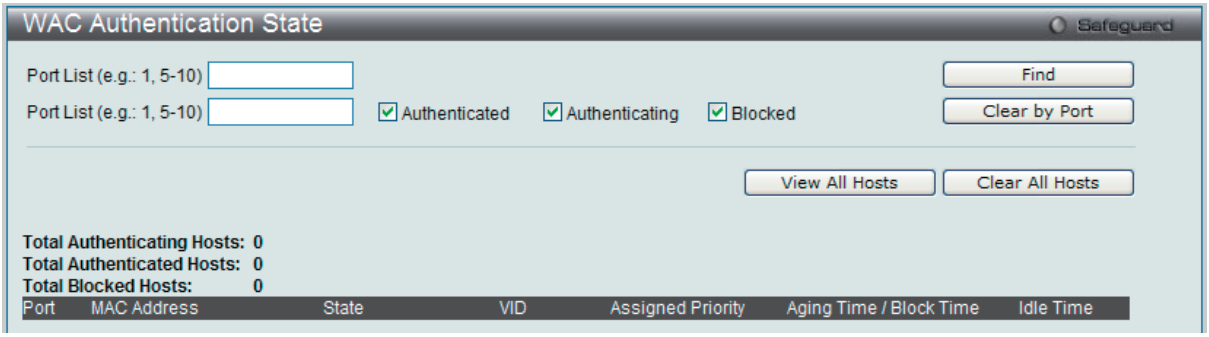


図 13-50 WAC Authentication State 画面

以下の項目を使用して、設定を行います。

項目	説明
Port List	プルダウンメニューを使用して、ポート範囲を選択し、適切なチェックボックス（「Authenticated」（認証済み）、「Authenticating」（認証中）、および「Blocked」（破棄））を選択します。
Authenticated	ポートに対して認証済みユーザのすべてをクリアします。
Authenticating	ポートに対して認証中ユーザのすべてをクリアします。
Blocked	ポートに対してブロックされたユーザすべてをクリアします。

「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。
「Clear by Port」ボタンをクリックして、入力したポートリストに基づくエントリを削除します。
「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、表示されたすべてのエントリを削除します。

Japanese Web-based Access Control（JWAC : JWAC 設定）

JWAC Global Settings（JWAC グローバル設定）

スイッチにおける JWAC（Japanese Web-based Access Control）の有効化および設定をします。

JWAC と Web 認証が相互に排他的な機能であり、それらを同時に使用することができませんのでご注意ください。JWAC 機能を使用するためには、PC ユーザは、2 段階の認証を通過する必要があります。最初のステップは、検疫サーバで検疫を行い、2 番目のステップでユーザ認証が行われます。2 番目のステップは、ホストが認証を通過した後にポートの VLAN メンバシップ変更がないという点を除き、Web 認証に似ています。RADIUS サーバは、802.1X コマンドセットによって定義されたサーバ設定を共有します。

注意 WAC/JWAC 認証では、System インタフェースがアップ状態である必要があります。

Security > Japanese Web-based Access Control (JWAC) > JWAC 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。

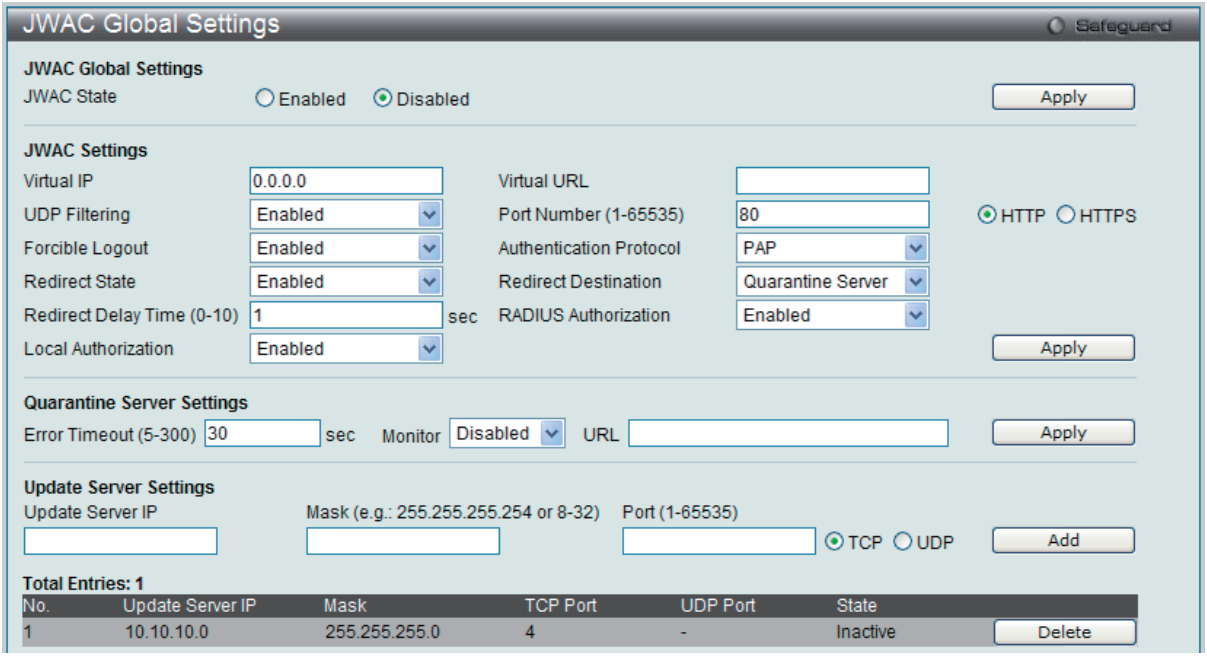


図 13-51 JWAC Global Settings 画面

以下の項目を設定可能です。

項目	説明
JWAC Global Settings	
JWAC State	JWAC 機能を「Enabled」（有効）/「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。
JWAC Settings	
Virtual IP	未認証ホストから認証リクエストを受け入れるために使用する JWAC バーチャル IP アドレスを指定します。この IP に送信されたリクエストだけが正しい応答を取得します。 注意 この IP は、ARP リクエストまたは ICMP パケットには応答しません。
Virtual URL	使用する仮想 URL を入力します。
HTTP(s) Port (1-65535)	JWAC スイッチがリッスンし、認証プロセスを終了するために使用する TCP ポートを指定します。
UDP Filtering	JWAC UDP フィルタリングを「Enabled」（有効）/「Disabled」（無効）にします。本項目を「Enabled」にすると、DHCP と DNS を除く未認証ホストからの UDP と ICMP パケットは破棄されます。
Forcible Logout	JWAC Forcible Logout を「Enabled」（有効）/「Disabled」（無効）にします。「Enabled」の場合、認証ホストから JWAC スイッチに TTL=1 を持つ ping パケットはログアウトリクエストと見なされ、ホストは未認証状態に戻ります。
Authentication Protocol	JWAC に使用される RADIUS プロトコルを指定し、RADIUS 認証を完了します。: Local、EAP MD5、PAP、CHAP、MS CHAP および MS CHAPv2
Redirected State	JWAC リダイレクト機能を「Enabled」（有効）/「Disabled」（無効）にします。リダイレクト検疫サーバが「Enabled」な場合、ランダムな URL にアクセスしようとすると、未認証ホストは検疫サーバにリダイレクトされます。リダイレクト先に JWAC Login Page を指定した場合、未認証ホストは、スイッチの JWAC Login Page にリダイレクトされ、Web 認証画面に移行します。リダイレクトが無効な場合、未認証ユーザは検疫サーバへのアクセスと未認証ホストからの JWAC Login Page だけが許可され、他のすべての Web アクセスは拒否されます。 注意 Quarantine Server（検疫サーバ）へのリダイレクトを有効にする場合、はじめに検疫サーバを設定する必要があります。
Redirect Destination	未認証ホストがリダイレクト Quarantine Server または JWAC Login Page のいずれかにリダイレクトされるかを指定します。

項目	説明
Redirect Delay Time (0-10)	未認証ホストが Quarantine Server または JWAC Login Page にリダイレクトされる場合の遅延時間 0-10（秒）を指定します。0 はリダイレクトの遅延がないことを示します。
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。
Quarantine Server Settings	
Error Timeout (5-300)	Quarantine Server のエラータイムアウトを設定します。Quarantine Server モニタが有効な場合、JWAC スイッチは、定期的に検疫が問題なく動作するかどうかをチェックします。スイッチが設定された時間に Quarantine Server から応答を受信しないと、スイッチは適切に動作していないと見なします。5-300（秒）で指定します。
Monitor	JWAC Quarantine Server モニタを「Enabled」（有効）/「Disabled」（無効）にします。「Enabled」な場合、JWAC スイッチは、サーバが問題ないことを保証するために Quarantine Server をモニタします。スイッチが Quarantine Server を検出しないと、リダイレクトが有効で、「Redirect Destination」が「Quarantine Server」に設定されている場合、強制的に JWAC Login Page に未認証のすべての HTTP アクセスをリダイレクトします。
URL	JWAC Quarantine Server URL を指定します。リダイレクトが有効で、未認証ホストが HTTP リクエストパケットをランダムな Web サーバに送信する場合、「Redirect Destination」が「Quarantine Server」であると、スイッチは、この HTTP パケットを処理し、設定された URL を持つ Quarantine Server へのアクセスを許可するためにホストにメッセージを送り返します。コンピュータが指定 URL に接続している場合、Quarantine Server は、ユーザ名とパスワードの入力をユーザにリクエストし、認証プロセスを完了します。
Update Server Settings	
Update Server IP	更新用サーバの IP アドレスを指定します。
Mask	サーバ IP アドレスのネットマスクを指定します。
Port	更新サーバが使用するポート番号を選択します。

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。

JWAC Port Settings（JWAC ポート設定）

スイッチに JWAC ポート設定を行います。

Security > Japanese Web-based Access Control (JWAC) > JWAC 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。

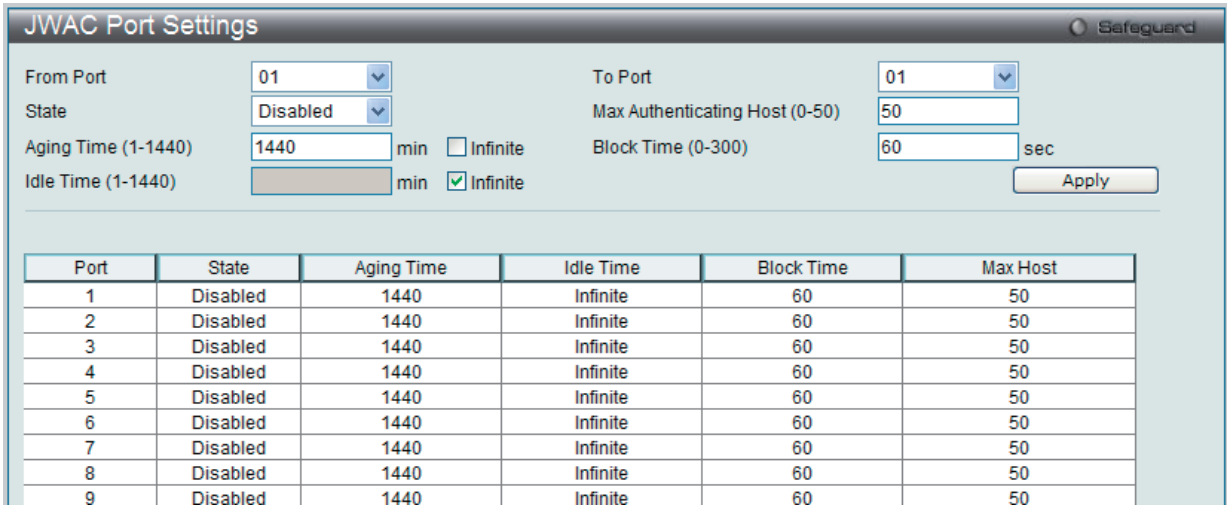


図 13-52　JWAC Port Settings 画面

スイッチの各ポートに JWAC を設定するためには、以下の項目を設定します。

項目	説明
From Port / To Port	JWAC ポートとして有効になるポート範囲を選択します。
Max Authenticating Host (1-50)	同時に各ポートに許可されるホストの認証処理の試みの最大数 1-50（回）を指定します。初期値は 50 です。
Aging Time (1-1440)	認証ホストが認証状態を保つ時間を 0-1440（分）の範囲で指定します。「Infinite」または 0 を指定すると、認証ホストは、ポートにエージングを行いません。初期値は 1440（分）です。
Block Time (0-300)	認証を通過することに失敗した場合にホストがブロックされる時間を指定します。0-300（秒）で指定します。初期値は 60 です。
Idle Time (1-1440)	本設定時間にトラフィックがない場合、ホストは未認証状態に戻ります。値を変更するためには「Infinite」のチェックを外して 0-1440（分）で指定します。「Infinite」を指定すると、ポート上の認証ホストのアイドル状態がチェックされません。初期値は「infinite」です。0 を指定すると、ポート上の認証ホストのアイドル状態がチェックされません。

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。

JWAC User Settings（JWAC ユーザ設定）

スイッチのローカルデータベースに JWAC ユーザを設定します。

Security > Japanese Web-based Access Control (JWAC) > JWAC User Settings をクリックし、以下の画面を表示します。

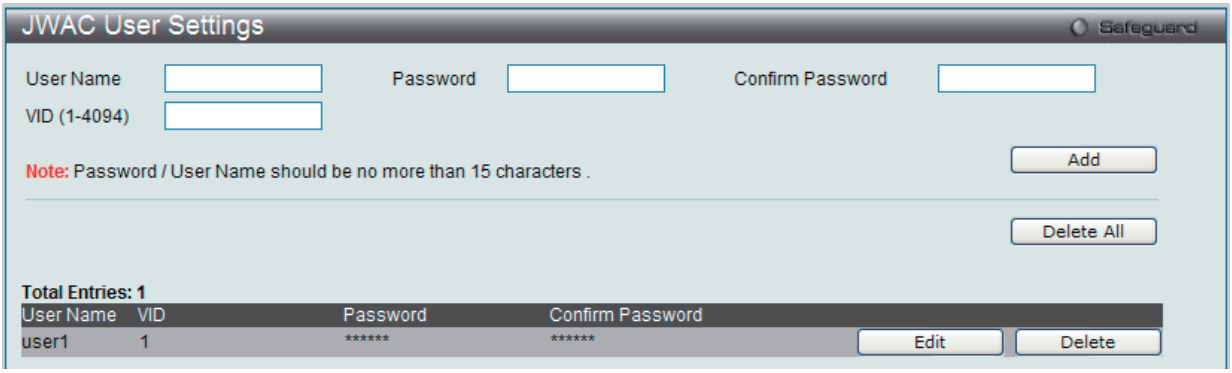


図 13-53 JWAC User Settings 画面

スイッチが JWAC にユーザアカウント設定をするためには、以下の項目を入力後、「Add」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
User Name	半角英数字 15 文字以内でユーザ名を入力します。
New Password	管理者が選択ユーザのために設定するパスワードを英数字（大文字小文字の区別あり）で入力します。
Confirm New Password	上記で入力したパスワードを再度入力します。
VID(1-4094)	VLAN ID 番号（1-4094）を入力します。

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。画面下部に表示されている現在の JWAC ユーザ設定を削除するためには、「Delete All」ボタンをクリックします。

エントリの変更

1. 変更するエントリの「Edit」ボタンをクリックして以下の画面を表示します。

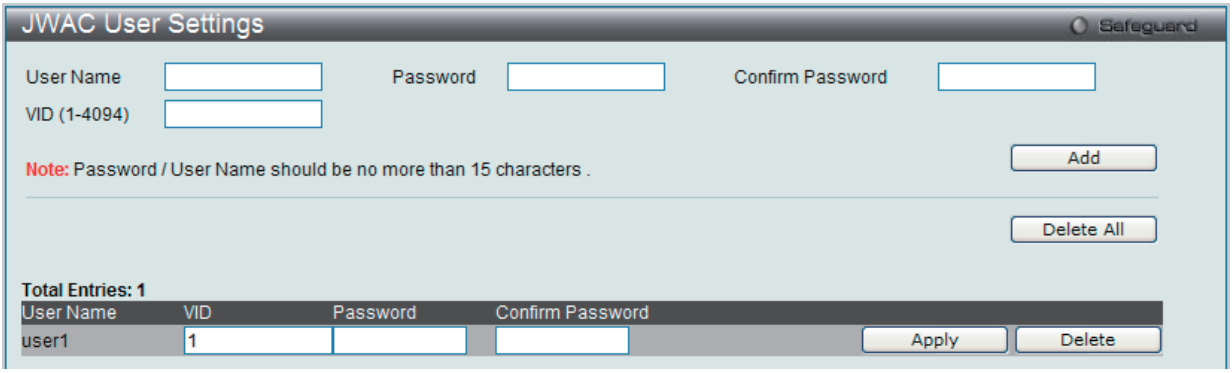


図 13-54 JWAC User Settings 画面 - Edit

2. エントリを編集して「Apply」ボタンをクリックします。

注意 ユーザ名とパスワードは 16 文字以内とします。

JWAC Authentication State（JWAC 認証状態）

スイッチにおける JWAC の認証情報を表示します。

Security > Japanese Web-based Access Control (JWAC) > JWAC Authentication State をクリックし、以下の画面を表示します。

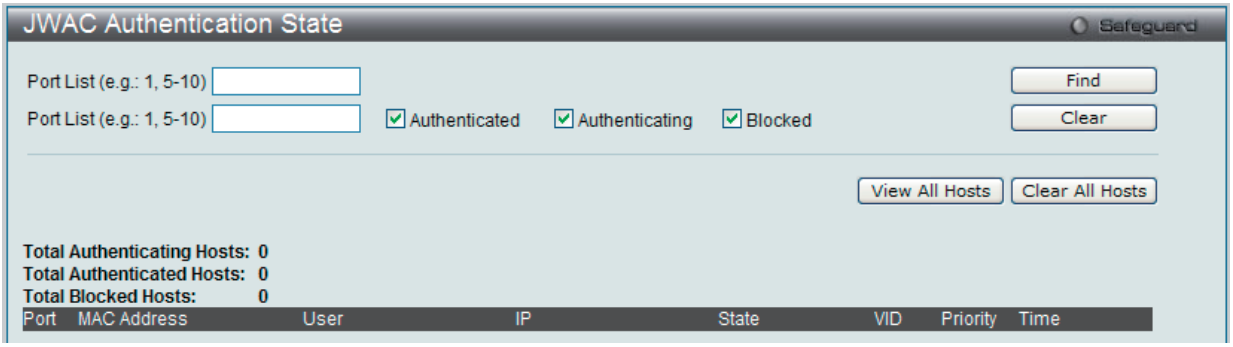


図 13-55　JWAC Authentication State 画面

以下の項目を設定します。

項目	説明
Port List	ポートまたはポート範囲を指定します。
Authenticated	本ボックスをクリックして、認証されたクライアントホストだけをクリアします。
Authenticating	本ボックスをクリックして、認証中のクライアントホストだけをクリアします。
Blocked	本ボックスをクリックして、認証エラーのために一時的にブロックされたクライアントホストだけをクリアします。

「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。
「Clear」ボタンをクリックして、入力したポートリストに基づくエントリを削除します。
「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、表示されたすべてのエントリを削除します。

JWAC Customize Page Language（JWAC 画面言語のカスタマイズ）

JWAC 画面言語の設定を行います。現在のファームウェアは英語および日本語をサポートしています。

Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page Language の順にメニューをクリックし、以下の画面を表示します。

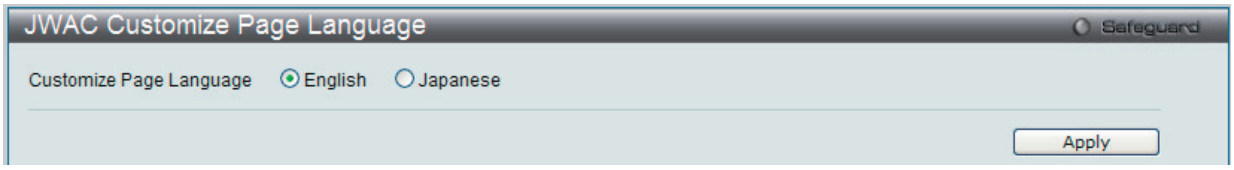


図 13-56　JWAC Customize Page Language 画面

JWAC 画面に使用する言語を設定するためには、「English」または「Japanese」のボタンをクリックし、「Apply」ボタンをクリックして、変更を保存します。

JWAC Customize Page（JWAC 画面のカスタマイズ）

JWAC 画面の設定を行います。

Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

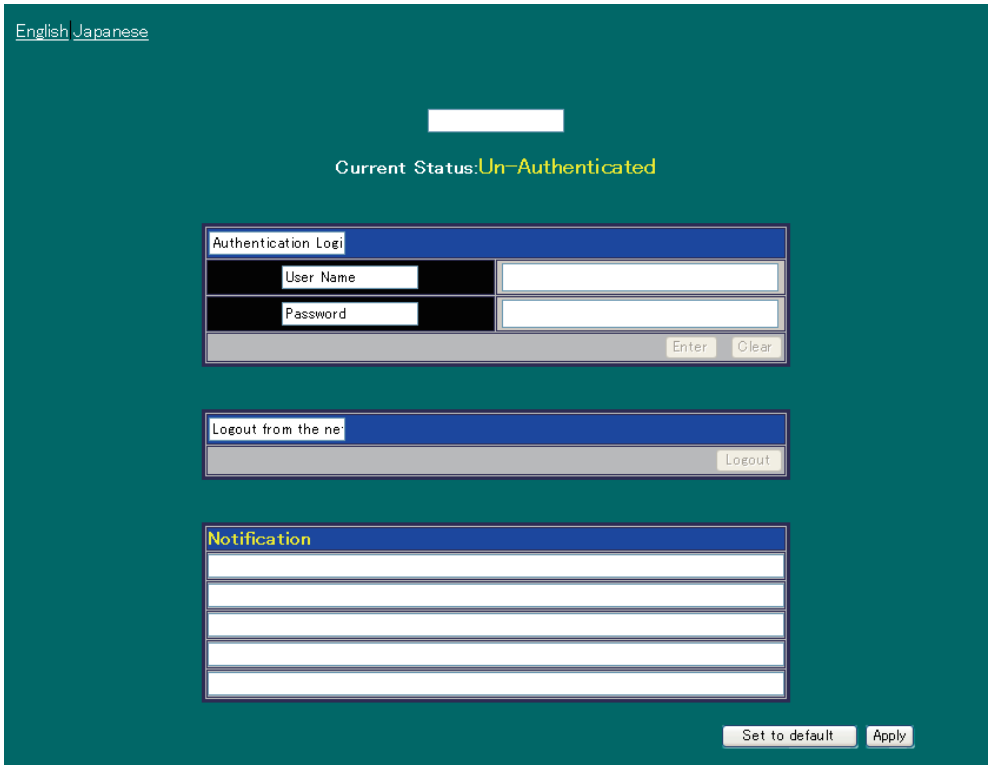


図 13-57　JWAC Customize Page 画面（English）

図 13-58　JWAC Customize Page 画面（Japanese）

JWAC 認証情報を入力して、JWAC 画面の設定を行います。最初の欄に認証名を入力し、「Apply」ボタンをクリックします。次にユーザ名とパスワードを入力し、「Enter」ボタンをクリックします。

Compound Authentication（コンパウンド認証）

新しいネットワークでは多くの認証方式を採用しています。本製品は、IEEE 802.1X、MAC ベースアドレスコントロール (MAC)、Web ベースアクセスコントロール（WAC）、JWAC、および IP-MAC- ポートバインディング（IMPB）を含むコンパウンド認証方式をサポートしています。コンパウンド認証機能により、クライアントは同一のスイッチポートで異なる認証方式を実行しネットワークに接続することが可能です。

コンパウンド認証機能は以下のモードから 1 つ選択して実行します。

Any（MAC、802.1X、または WAC）モード

下の図では、スイッチポートは 802.1X、MAC、または WAC を使用して認証を行うことができるように設定されています。クライアントがネットワークに接続を試みると、本製品はこれらの認証方式のうち 1 つを使用してクライアントの認証を行い、認証されるとそのクライアントはネットワークに接続することができます。

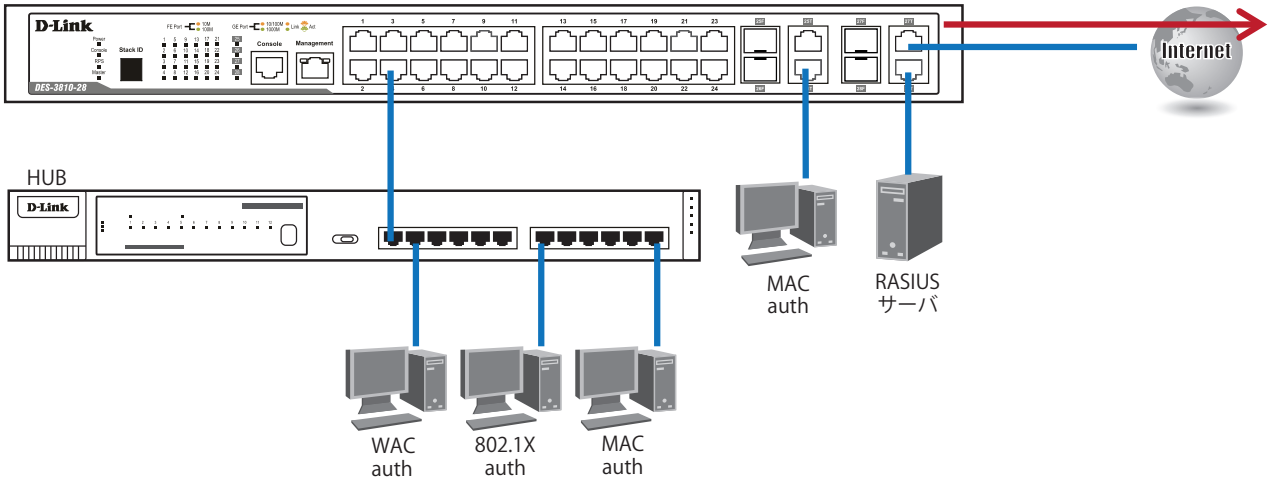


図 13-59　Any（MAC、802.1X、または WAC）モードの図

Any（MAC、802.1X、または JWAC）モード

下の図では、スイッチポートは 802.1X、MAC 認証、または JWAC を使用して認証を行うことができるように設定されています。クライアントがネットワークに接続を試みると、本製品はこれらの認証方式のうち 1 つを使用してクライアントの認証を行い、認証されるとそのクライアントはネットワークに接続することができます。

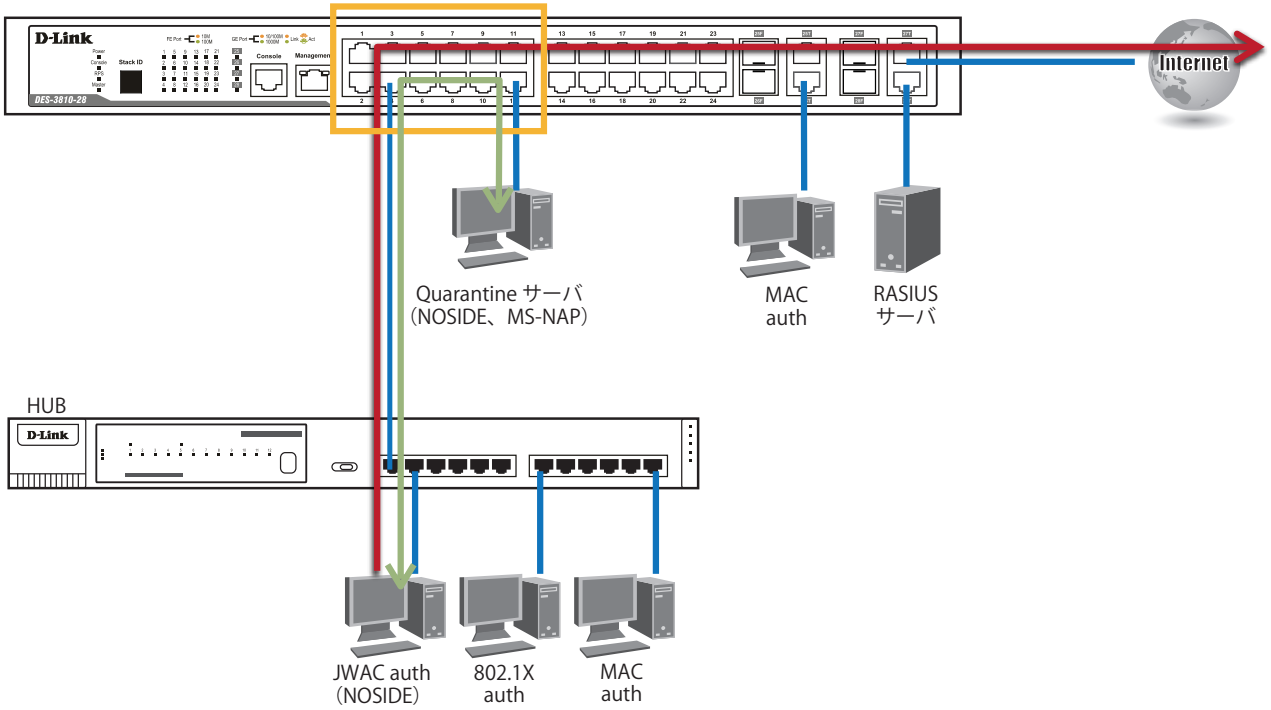


図 13-60　Any（MAC、802.1X、または JWAC）モードの図

802.1X & IMPB モード

本モードでは、サポートしている認証方式での認証の後に IP-MAC- ポートバインディングテーブルをチェックすることで特別なセキュリティレイヤを追加しています。IP-MAC- ポートバインディングテーブルは、認証ホストが送信した IP ストリームが許可済みであるかをチェックする「ホワイトリスト」を作成するのに使用されます。下の図では、スイッチポートは 802.1X 認証を使用して認証を行うように設定されています。IP-MAC- ポートバインディングテーブルにあるクライアントがこの認証方式を使用してネットワークに接続を試みる場合、そのクライアントが適切な IP/MAC/ ポートチェックのホワイトリストに載っていると接続は許可されます。クライアントが認証方式のうち 1 つに失敗すると、接続は拒否されます。

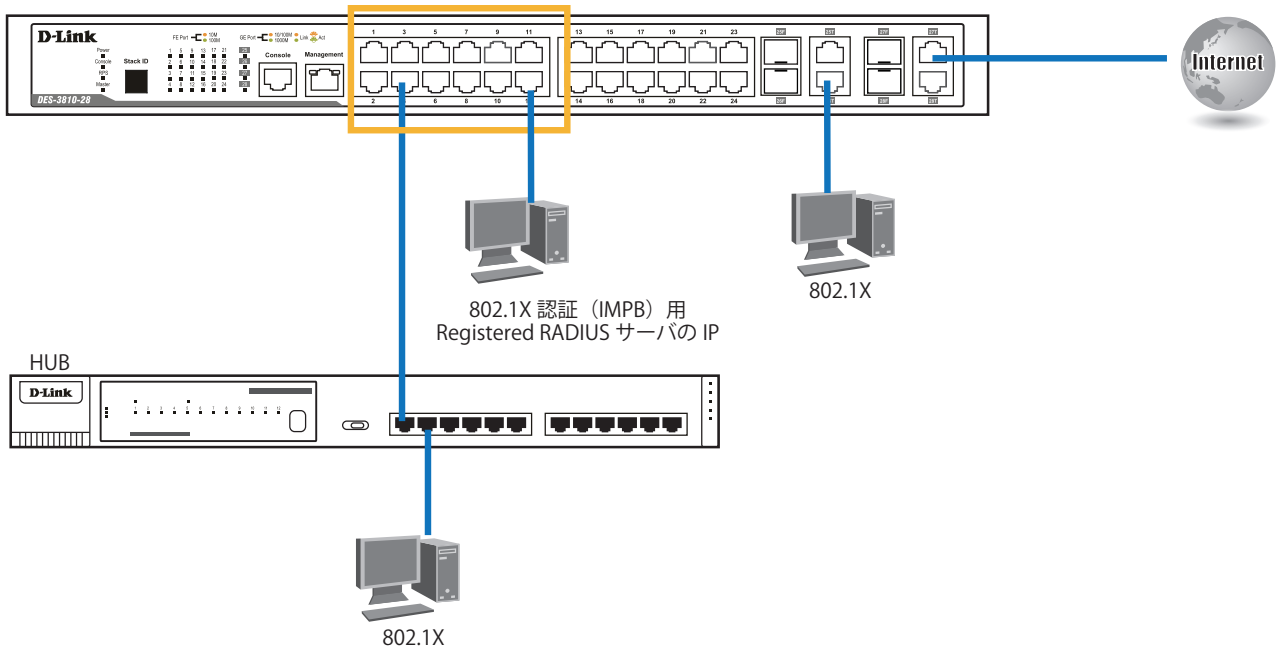


図 13-61　802.1X & IMPB モードの図

IMPB & WAC/JWAC モード

本モードでは、サポートしている認証方式で認証の後に IP-MAC- ポートバインディングテーブルをチェックすることで特別なセキュリティレイヤを追加しています。IP-MAC- ポートバインディングテーブルは、認証ホストが送信した IP ストリームが許可済みであるかをチェックする「ホワイトリスト」を作成するのに使用されます。下の図では、スイッチポートは MAC アドレス認証、または WAC を使用して認証を行うように設定されています。IP-MAC- ポートバインディングテーブルにあるクライアントがこれらのうちいずれかの認証方式を使用してネットワークに接続を試みる場合、そのクライアントが適切に IP/MAC/ ポートチェックのホワイトリストに載っていると接続は許可されます。クライアントが認証方式のうちの 1 つで認証エラーになると、接続は拒否されます。

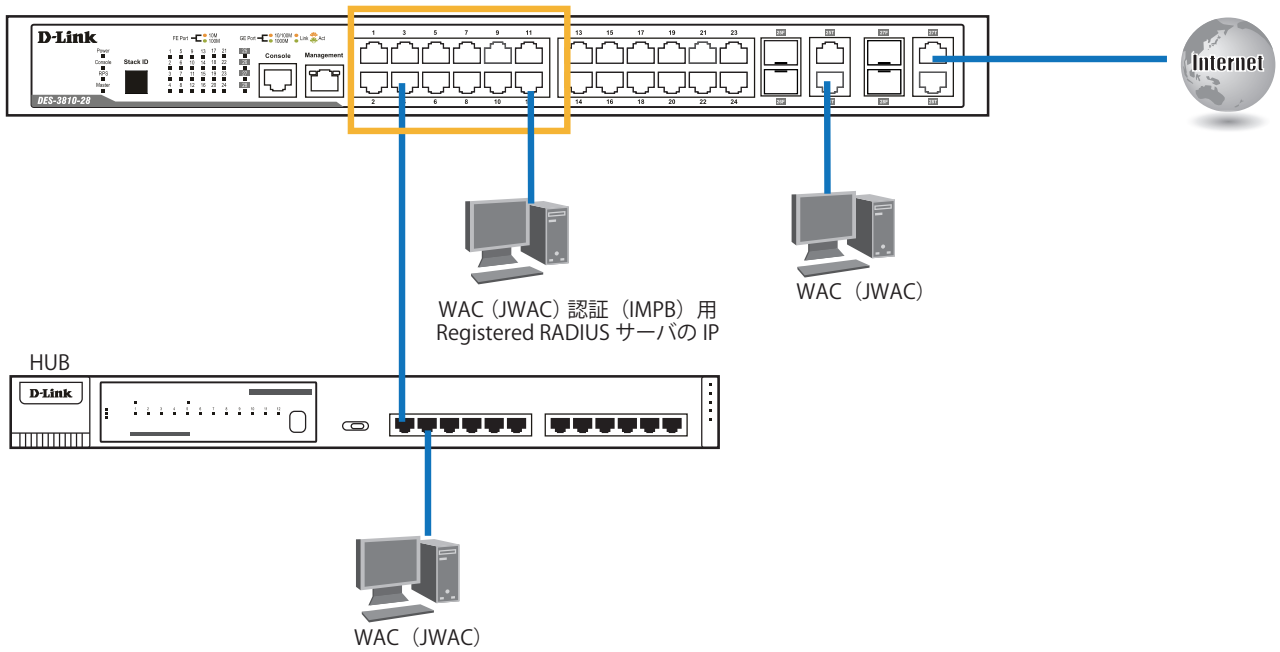


図 13-62　IMPB & WAC/JWAC モードの図

MAC & IMPB モード

本モードは、サポートしている認証方法の 1 つを試みた後に、IP-MAC- ポートバインディング (IMPB) テーブルをチェックすることによって、特別なセキュリティレイヤを追加します。認証ホストが送信した IP ストリームの許可の有無をチェックする「ホワイトリスト」を作成するために IMPB テーブルを使用します。下の図では、MAC を使用してクライアントを認証するようにスイッチポートを設定しています。クライアントが IMPB テーブルにあり、この認証方法を使用してネットワークへの接続を試みて、さらにクライアントが適切な IP/MAC/ ポートチェック用のホワイトリストにあれば、アクセスは許可されます。クライアントが認証方法の 1 つに失敗すると、アクセスは拒否されます。

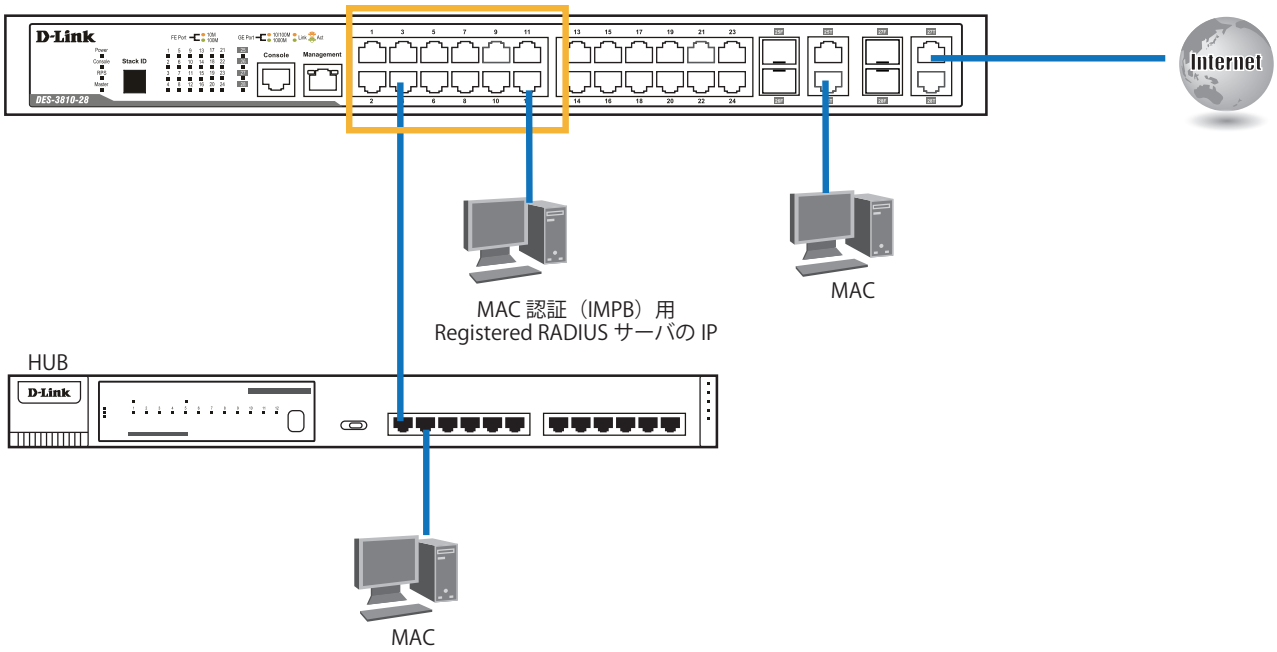


図 13-63　MAC & IMPB モードの図

「Compound Authentication」フォルダには次の 2 つの画面があります。:「Compound Authentication Settings」画面、「Compound Authentication Guest VLAN Settings」画面

Compound Authentication Settings（コンパウンド認証設定）

スイッチポートに認可ネットワーク状態の設定および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。

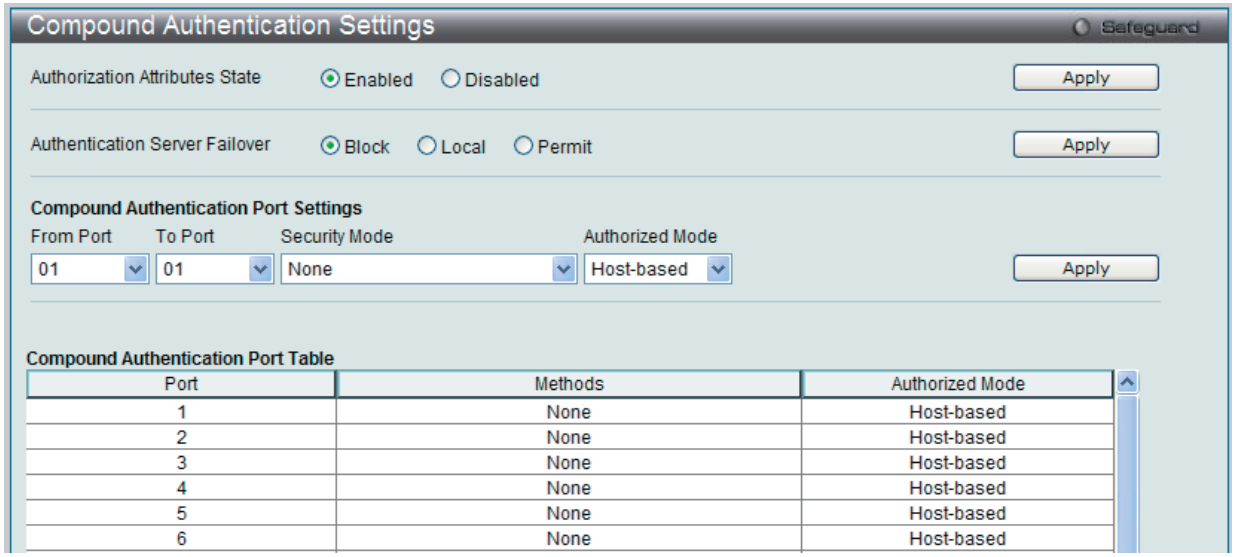


図 13-64 Compound Authentication Settings 画面

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、クライアントは認証されなかったとみなされます。そうでない場合認証されます。 • Permit - クライアントは、通常認証されたものとして見なされます。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 - クライアントは通常認証されなかったものとして見なされます。（初期値）
From Port / To Port	コンパウンド認証ポートとして設定するポート範囲を指定します。
Security Mode	コンパウンド認証方式には以下のオプションがあります。 • None - すべてのコンパウンド認証方式を無効にします。 • Any（MAC, 802.1X, JWAC or WAC）- これらのうちいずれかの認証方式を通過すると接続を許可します。本モードでは、1 つのポートに対し一度に MAC、802.1X、および WAC/JWAC 認証を有効にします。各セキュリティモジュールがポートに対して有効か否かはそのシステムの状態に依存します。WAC と JWAC のシステム状態は相互に排他的であるため、1 つのポートに対して、どちらか 1 つだけが有効になります。 • 802.1X+IMPB - はじめに 802.1X 認証を行い、次に IP-MAC- ポートバインディング認証を行います。両方の認証方式を通過する必要があります。 • IMPB+JWAC - はじめに IMPB 認証を行い、次に JWAC 認証を行います。両方の認証方式を通過する必要があります。 • IMPB+WAC - はじめに IMPB 認証を行い、次に WAC 認証を行います。両方の認証方式を通過する必要があります。 • MAC+IMPB - はじめに MAC を行い、次に IMPB 認証を行います。両方の認証方式を通過する必要があります
Authorized Mode	「Host-based」または「Port-based」を選択します。 • Port-based - 対応するホストの 1 つが認証を通過すると、同じポート上のホストはすべてネットワークへの接続が許可されます。認証に失敗するとこのポートは続いて次の認証方式を実行します。 • Host-based - ユーザは個別に認証されます。

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。

Compound Authentication Guest VLAN Settings（コンパウンド認証ゲスト VLAN の設定）

ポートをゲスト VLAN に割り当て、または削除することができます。

Security > Compound Authentication > Compound Authentication Guest 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。

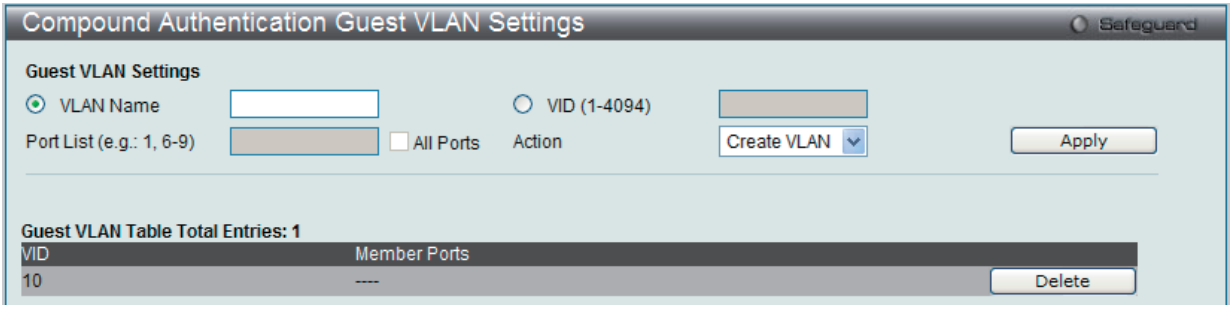


図 13-65　Compound Authentication Guest VLAN Settings 画面

以下の項目を使用して、ゲスト VLAN の設定をします。

項目	説明
VLAN Name	VLAN をゲスト VLAN として割り当てます。必ず定義済みのスタティック VLAN を割り当てます。
VLAN ID (1-4094)	VLAN ID をゲスト VLAN に割り当てます。この VLAN ID には、必ず定義済みのスタティック VLAN に割り当てます。
Port List (e.g : 1,6-9)	設定するポート範囲を指定します。または、「All Ports」のチェックボタンをチェックしてすべてのポートを一度に設定します。
Action	プルダウンメニューを使用して操作する機能を選択します。 • Create VLAN - VLAN を作成します。 • Add Ports - ポートを追加します。 • Delete Ports - ポートを削除します。

「Apply」ボタンをクリックし、ゲスト VLAN を実行します。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、指定エントリを削除します。

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。

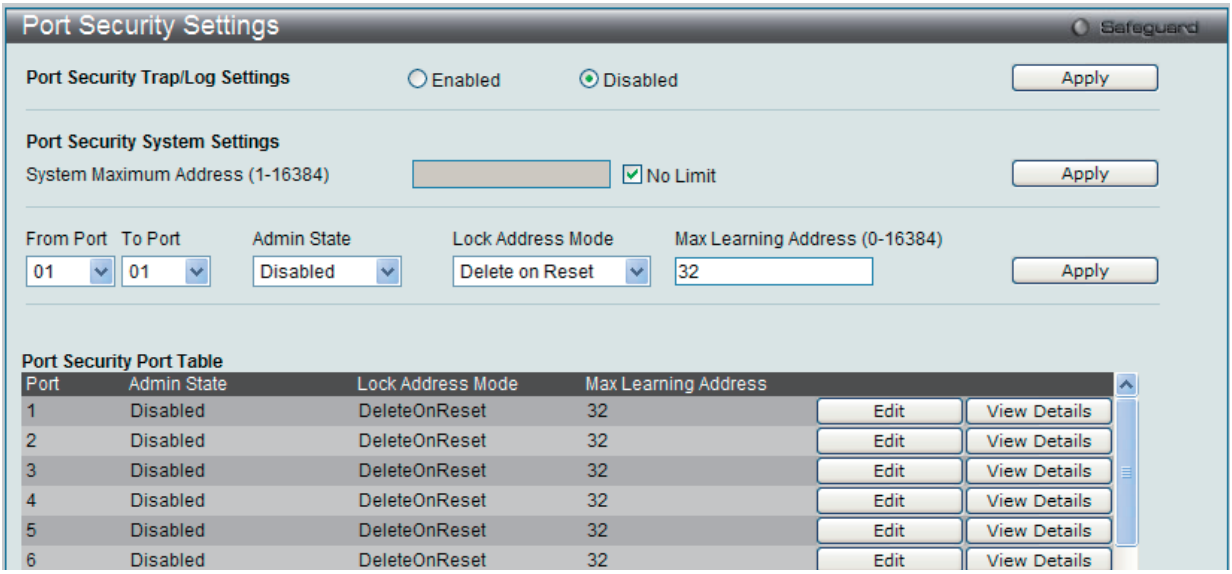


図 13-66　Port Security Settings 画面

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	システムの最大アドレス数を入力します。
From Port	ポートセキュリティ項目を表示するポートの最初の番号を設定します。
To Port	ポートセキュリティ項目を表示するポートの最後の番号を設定します。
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、エージングタイム経過後に削除されません。 • 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 (0-16384)	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、以下の画面を表示します。

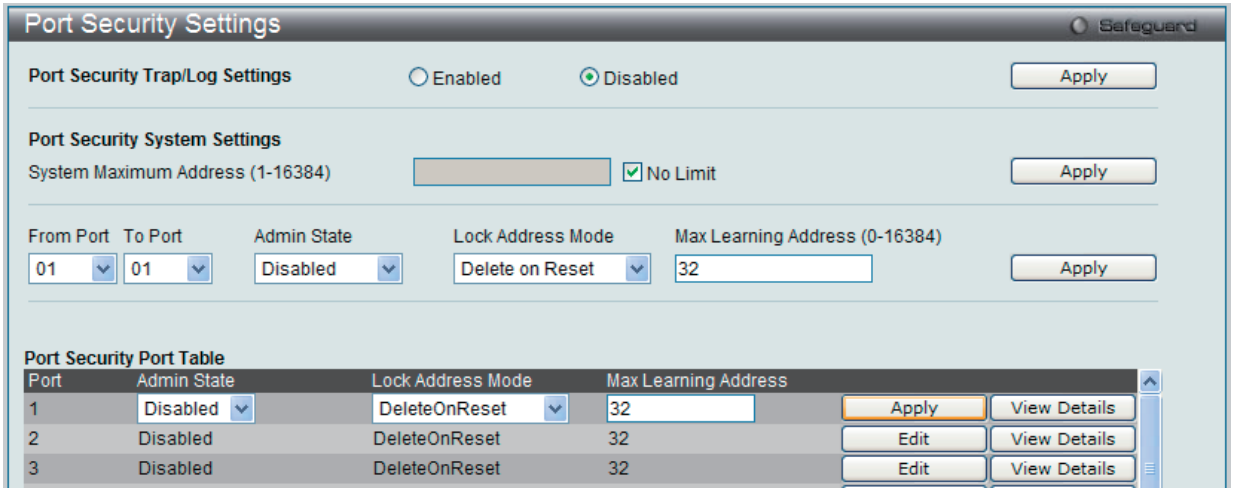


図 13-67　Port Security Settings 画面 - Edit

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。

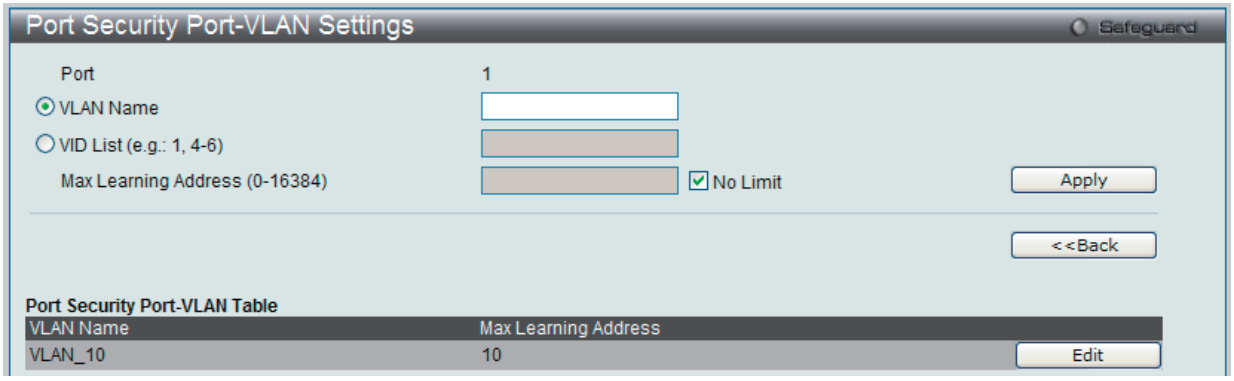


図 13-68　Port Security Port-VLAN Settings 画面

本画面には次の項目があります。

項目	説明
VLAN Name	選択して、本設定に使用する VLAN 名を入力します。
VLAN List	選択して、本設定に使用する VLAN ID を入力します。
Max Learning Address	本ポートに学習できるポートセキュリティエントリの最大数を入力します。「No Limit」オプションを選択すると、この欄は無制限となります。

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、以下の画面を表示します。

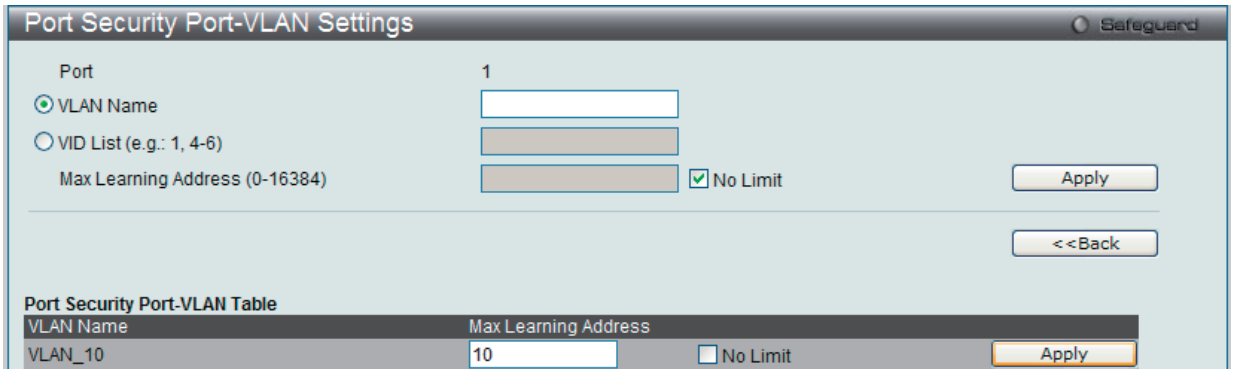


図 13-69　Port Security Port-VLAN Settings 画面 - Edit

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。

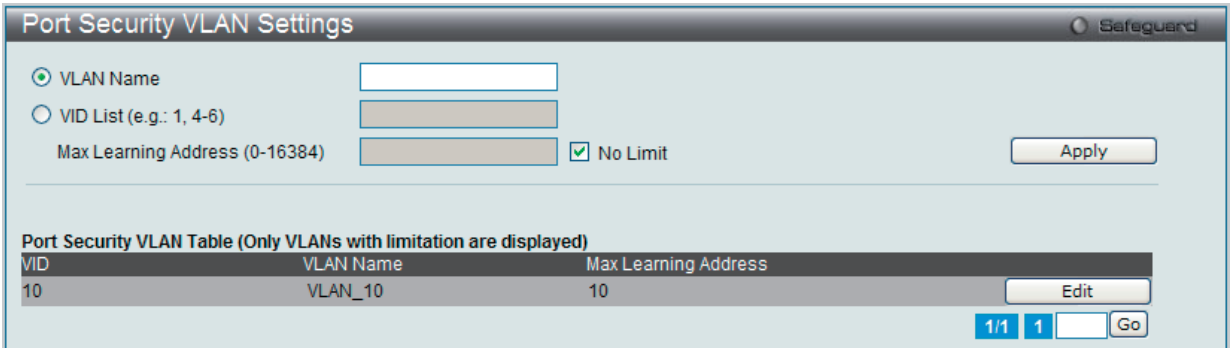


図 13-70 Port Security VLAN Settings 画面

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 ID により VLAN リストを指定します。
Max Learning Address	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」オプションを選択すると、この欄は無制限となります。

「Apply」ボタンをクリックして行った変更を適用します。

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、以下の画面を表示します。

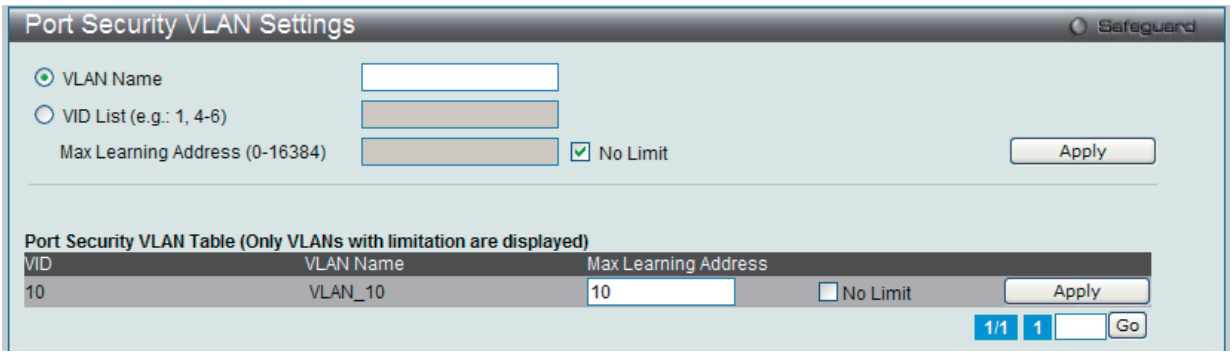


図 13-71 Port Security VLAN Settings 画面 - Edit

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。

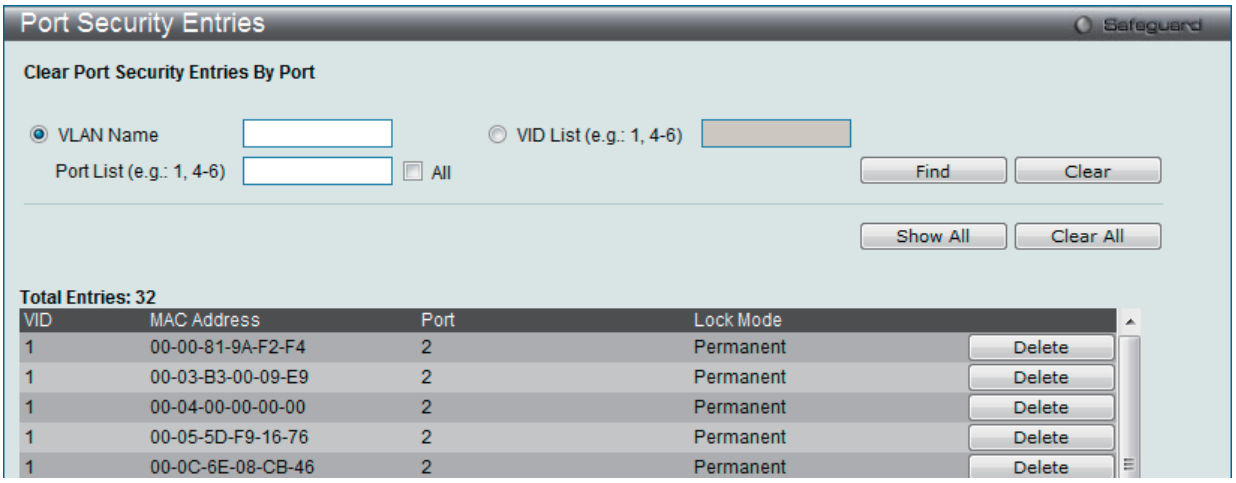


図 13-72　Port Security Entries 画面

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	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 アドレスです。
Lock Mode	転送データベーステーブルに登録されている MAC アドレスの種類です。「Permanent」または「DeleteOnReset」となっているエントリのみ削除できます。

「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。
「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。
「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。
「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。
「Delete」ボタンをクリックして、指定エントリを削除します。

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。

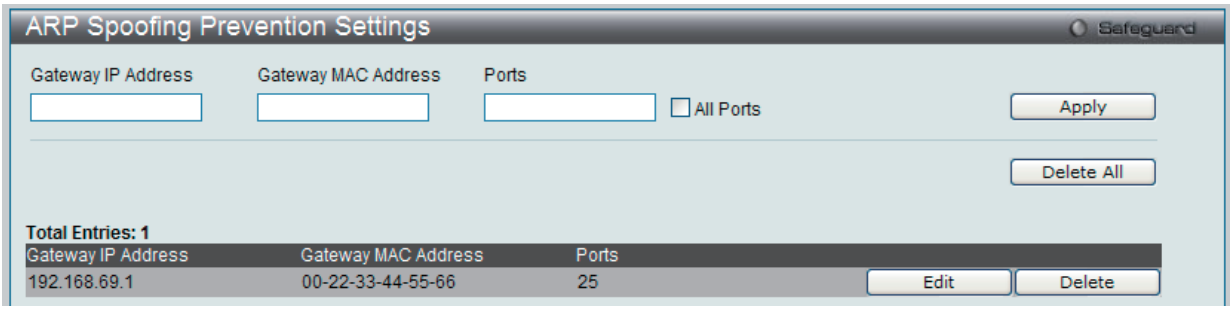


図 13-73　ARP Spoofing Prevention Settings 画面

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 Address」（ゲートウェイの IP アドレス）、「Gateway MAC Address」（ゲートウェイの MAC アドレス）およびポートリストを入力し、「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て、以下の画面を表示します。

図 13-74　ARP Spoofing Prevention Settings 画面 - Edit

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。

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** 画面で BPDU ポートを STP に設定していると、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。

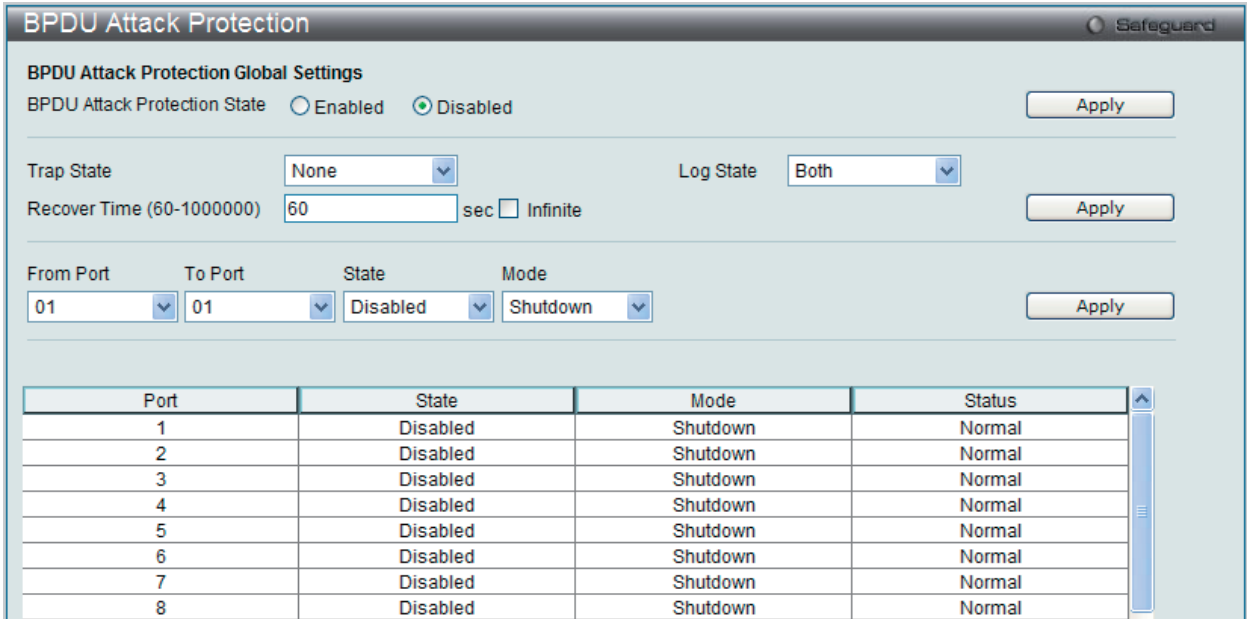


図 13-75　BPDU Attack Protection 画面

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	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 (Discarding 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。

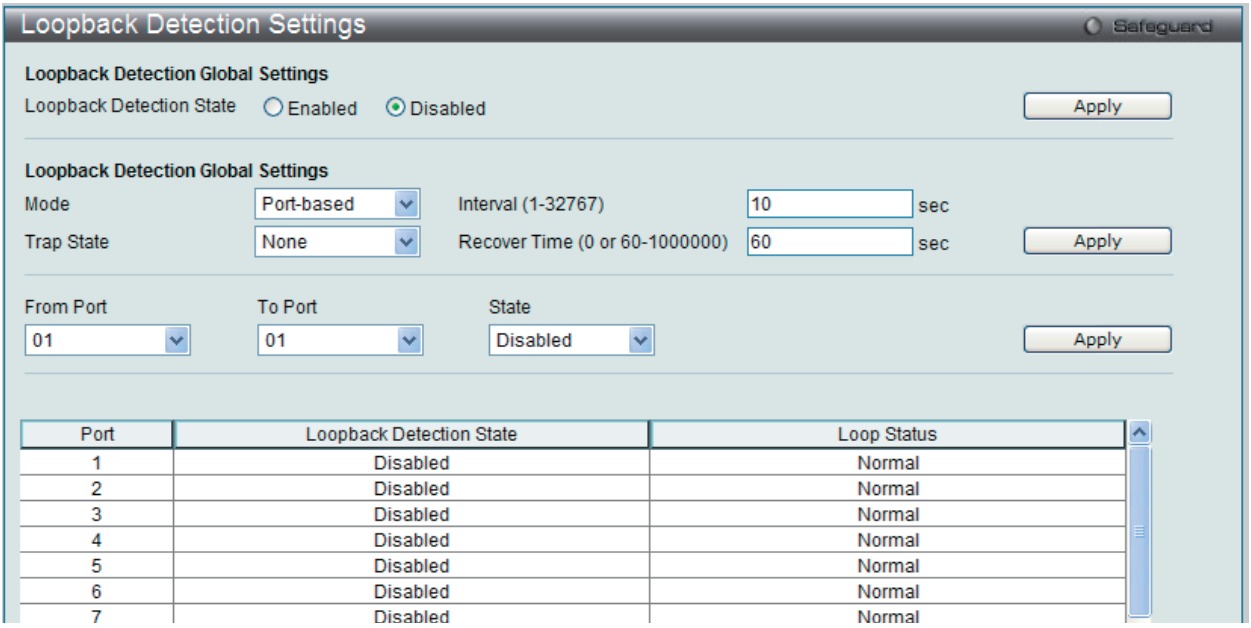


図 13-76　Loopback Detection Settings 画面

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。
Interval (1-32767)	ループ検知間隔を設定します。（1-32767 秒）初期値は 10（秒）です。
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。
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。

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、1 つのポート（ポートグループ）からポートグループへのトラフィックフロー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を行うこの方法は、VLAN によるトラフィック制限に似ていますが、さらに限定的であるといえます。本機能は、マスタスイッチ CPU のオーバヘッドを増加させないでトラフィックを直接操作します。

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。

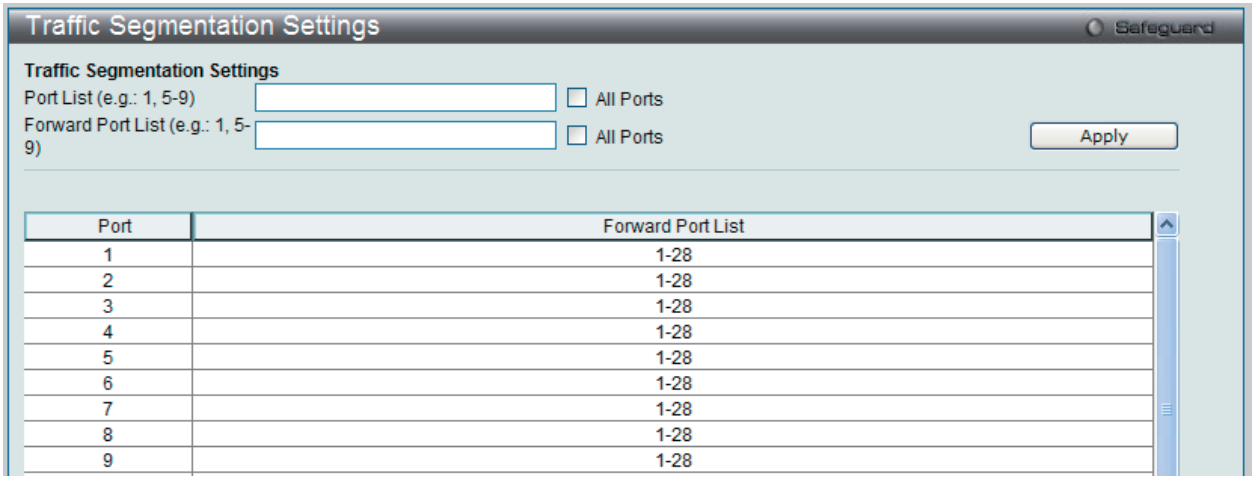


図 13-77　Traffic Segmentation Settings 画面

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。
Ports	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。

ポートは上記「Port」欄で指定したポートからのパケットを受信します。「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フィルタする 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。

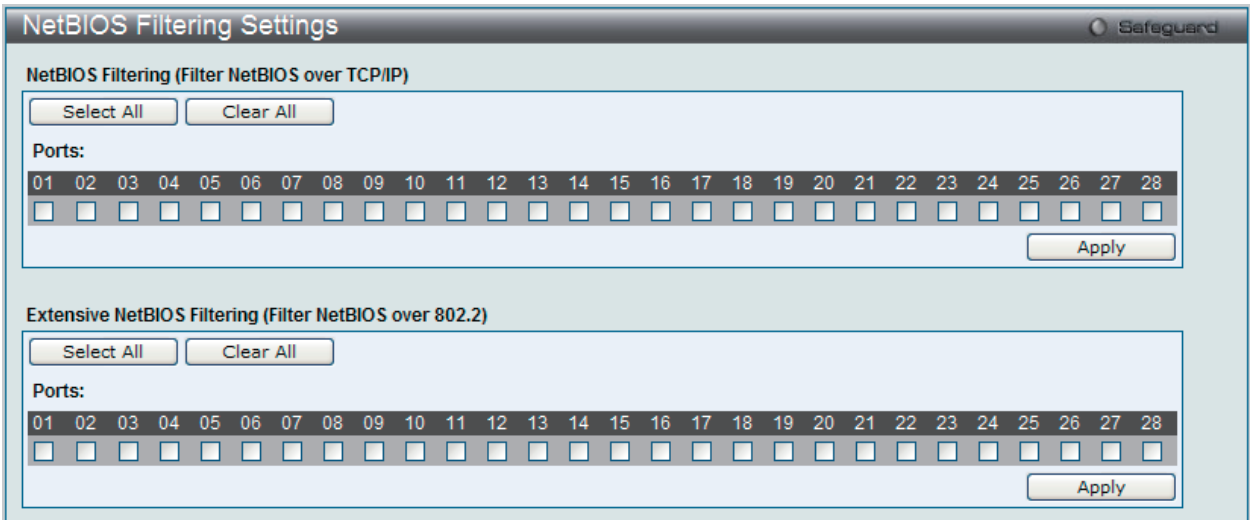


図 13-78　NetBIOS Filtering Settings 画面

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	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。
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。

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）

スイッチは 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する機能）をサポートしています。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。

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。

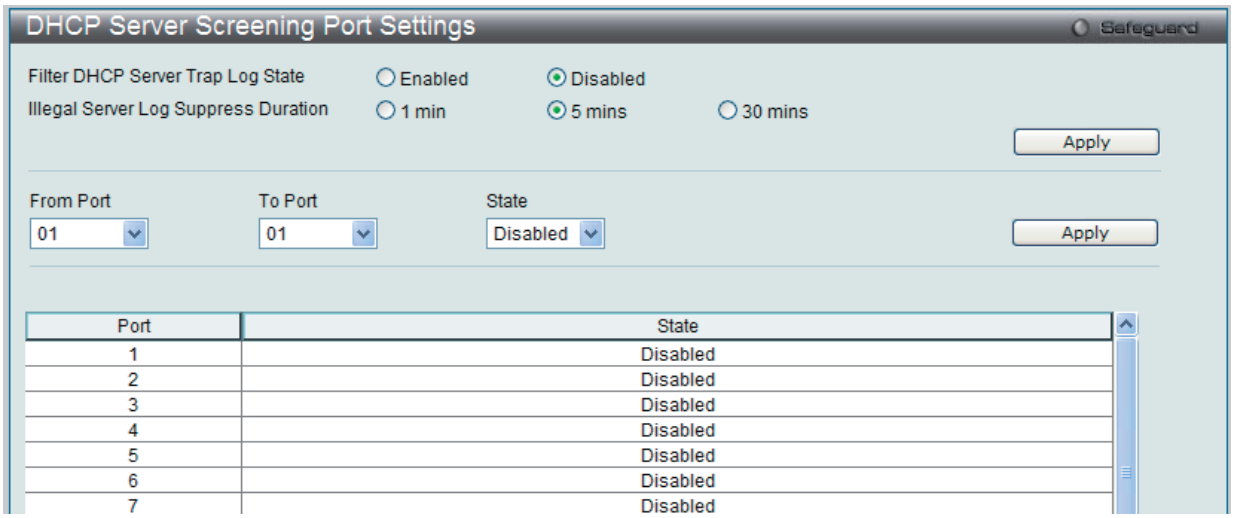


図 13-79　DHCP Screening Port Settings 画面

本画面には次の項目があります。

項目	説明
Filter DHCP Server 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。
Illegal Server Log Suppress Duration	不正なサーバログのサプレッション時間を 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。

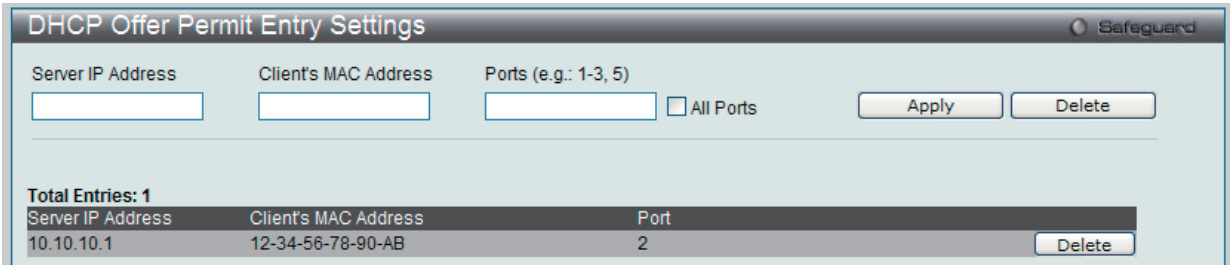


図 13-80　DHCP Offer Permit Entry Settings 画面

本画面には次の項目があります。

項目	説明
Server IP Address	フィルタする DHCP サーバの IP アドレスを指定します。
Client's MAC Address	DHCP クライアントの MAC アドレスを指定します。ネットワーク上の正しい DHCP サーバが複数ある場合にだけ入力します。ネットワーク上に正しい DHCP サーバが 1 つしか存在しない場合は、入力することはできません。
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。

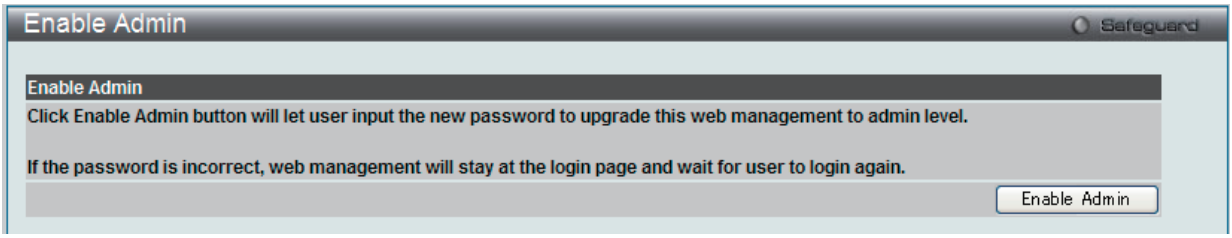


図 13-81　Enable Admin 画面

「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。

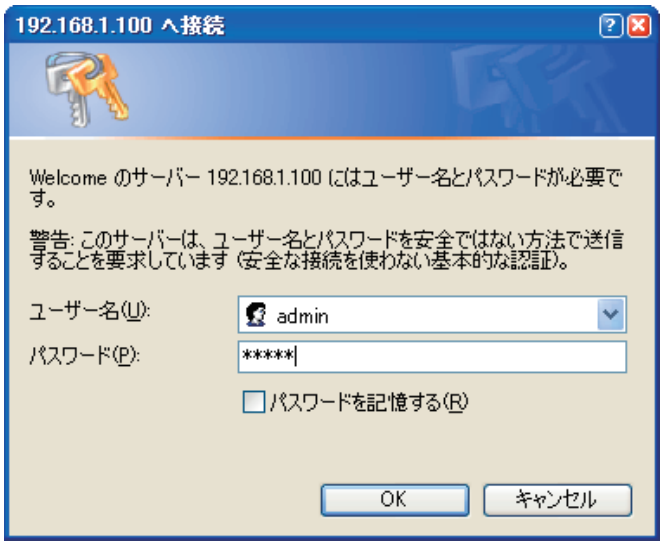


図 13-82　ユーザ名とパスワード入力ダイアログボックス

「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。

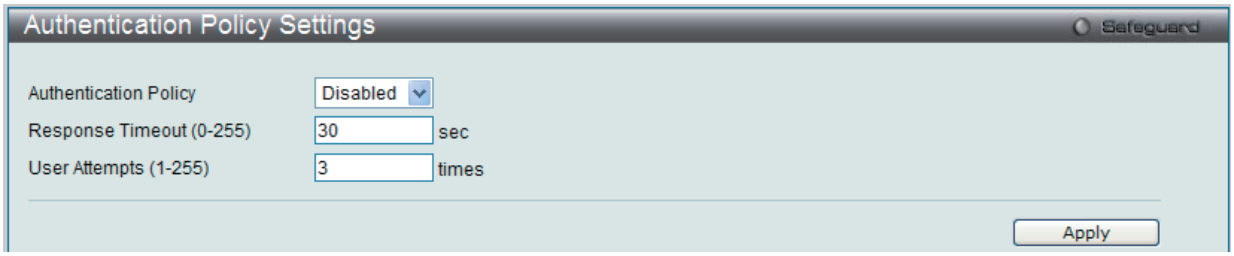


図 13-83　Authentication Policy Settings 画面

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の「Enabled」（有効）、「Disabled」（無効）を設定します。
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（コンソール、Telnet、SSH、Web）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。

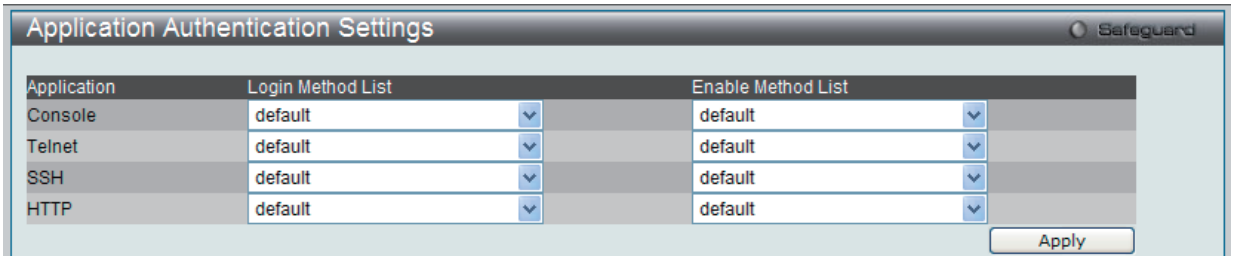


図 13-84　Application Authentication Settings 画面

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（コンソール、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」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」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。

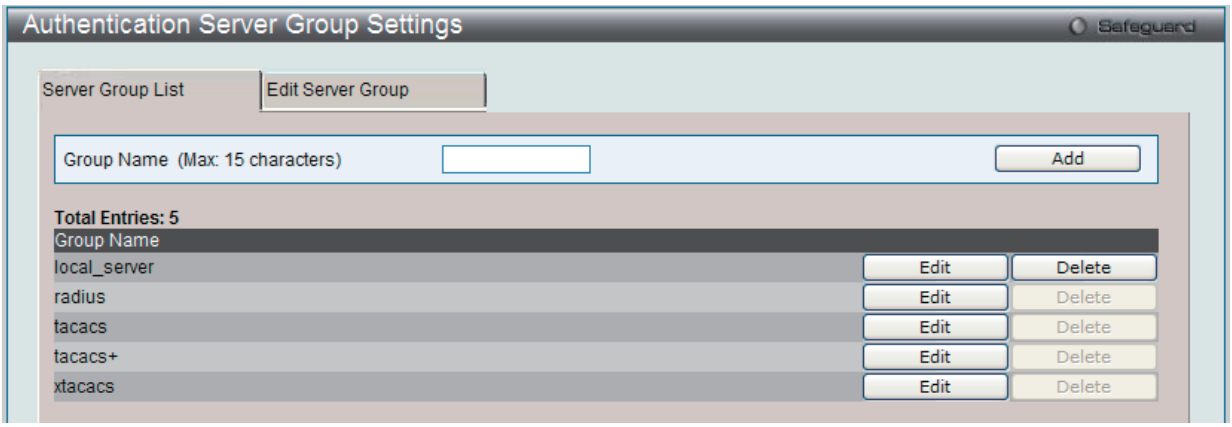


図 13-85 Authentication Server Group Settings 画面

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。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 13-86 Authentication Server Group Settings (Edit) 画面

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 Hosts」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。

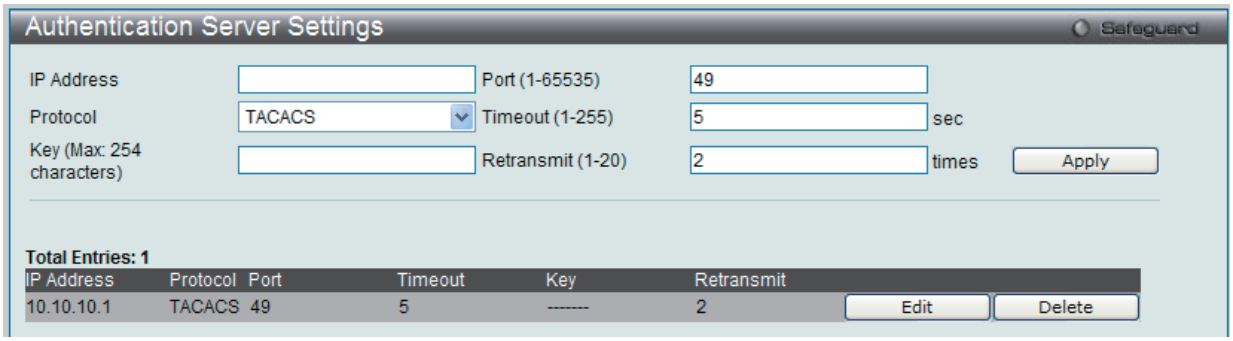


図 13-87　Authentication Server Settings 画面

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 1813 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 (1-255)	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。

「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、以下の画面を表示します。

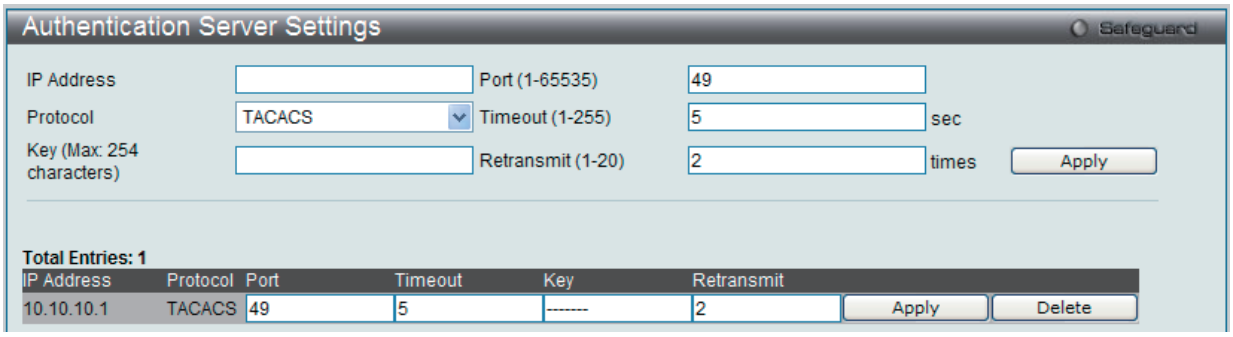


図 13-88　Authentication Server Settings 画面 - Edit

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。

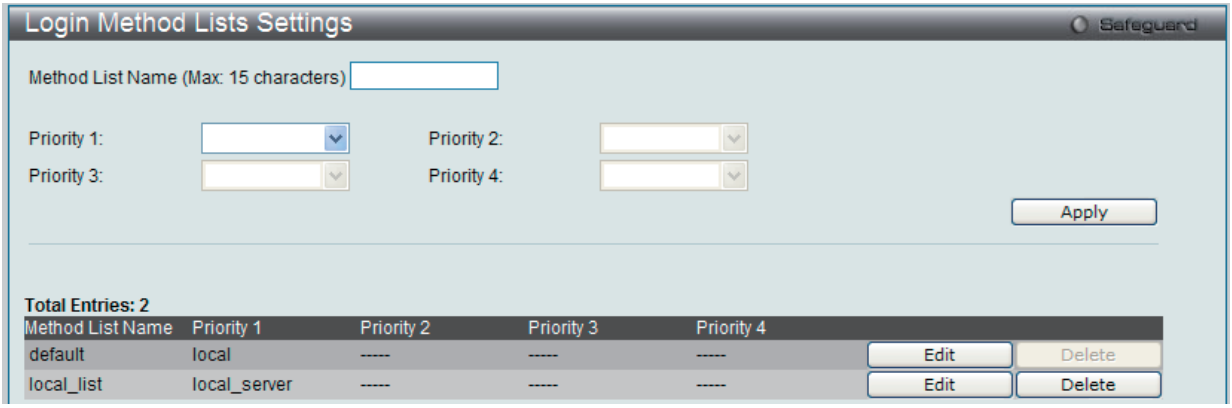


図 13-89 Login Method Lists Settings 画面

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、以下の画面を表示します。

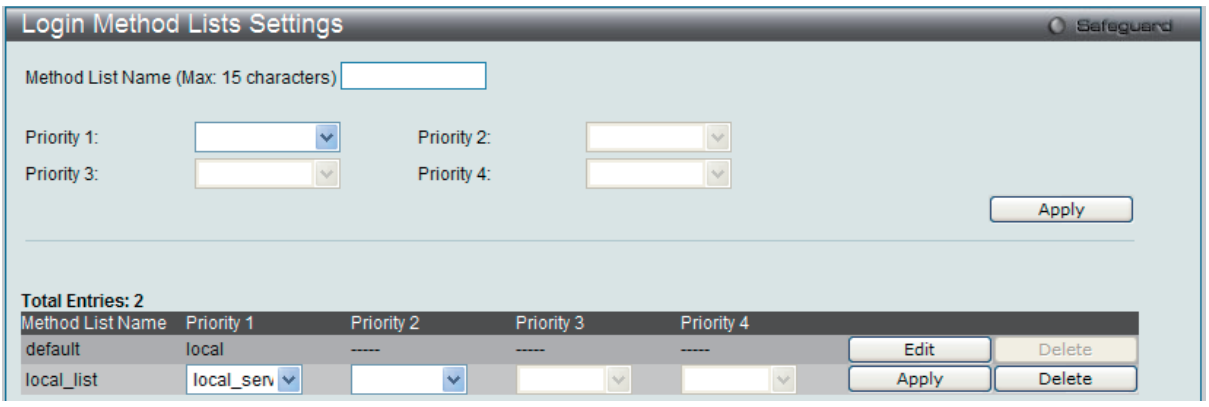


図 13-90 Login Method Lists 画面 - Edit

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 396 ページの「Local Enable Password Settings（ローカルユーザパスワード設定）」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。

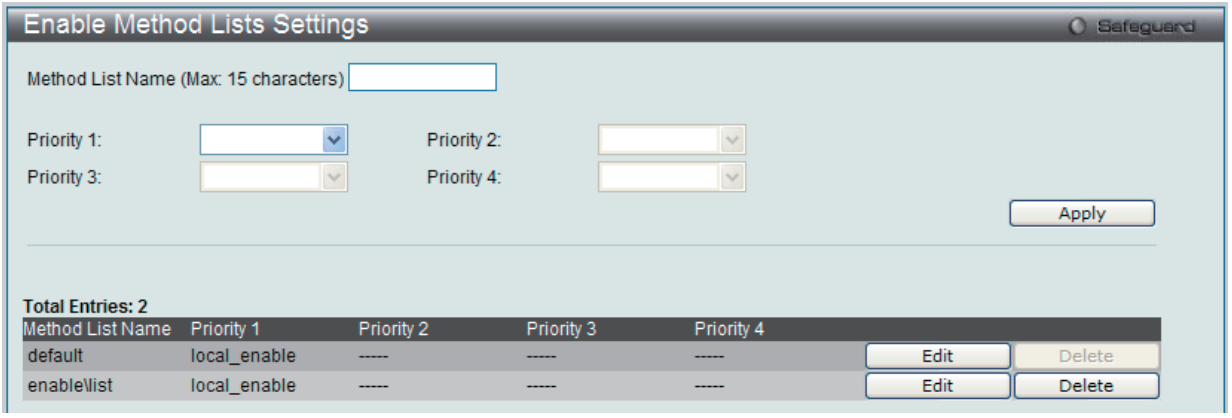


図 13-91　Enable Method Lists Settings 画面

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 396 ページの「Local Enable Password Settings（ローカルユーザパスワード設定）」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の認証を行います。 • 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。 • 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、以下の画面を表示します。

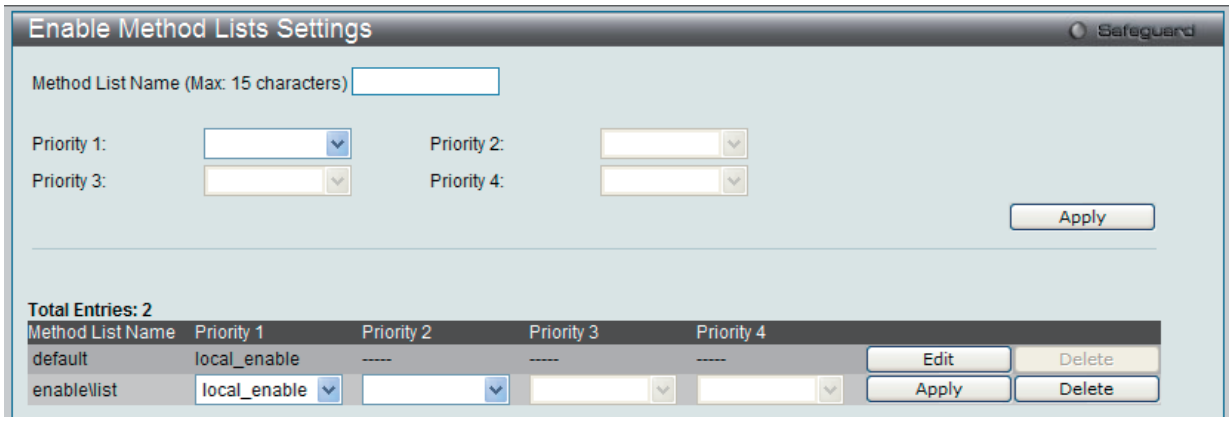


図 13-92 Enable Method Lists 画面 - Edit

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。

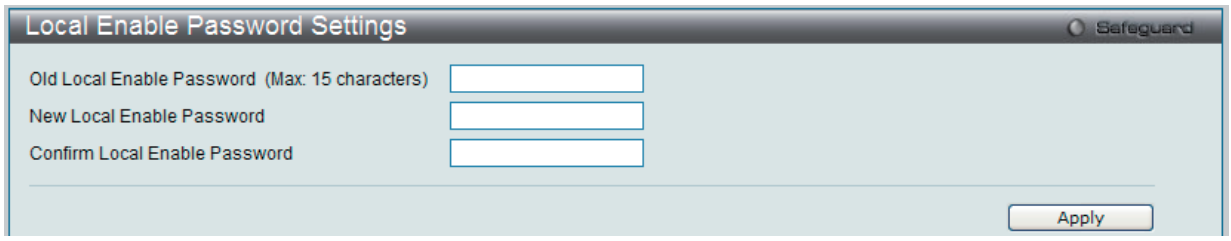


図 13-93 Local Enable Password Settings 画面

以下の項目を使用して、Local Enable Password を設定します。入力が完了後、「Apply」ボタンをクリックします。

項目	説明
Old Local Enable Password (Max: 15 characters)	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。

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。

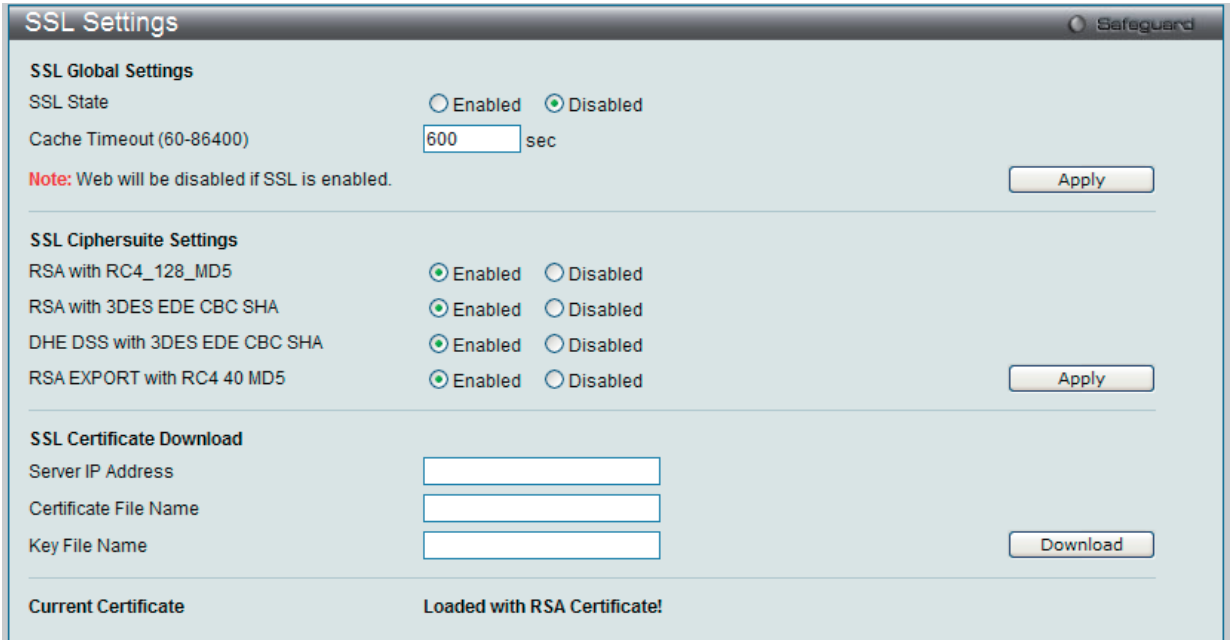


図 13-94 SSL Settings 画面

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 ベースマネー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 の最初を https:// で始まるアドレスを Web ブラウザのアドレスに指定してもエラーになり、認証はされません。

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。

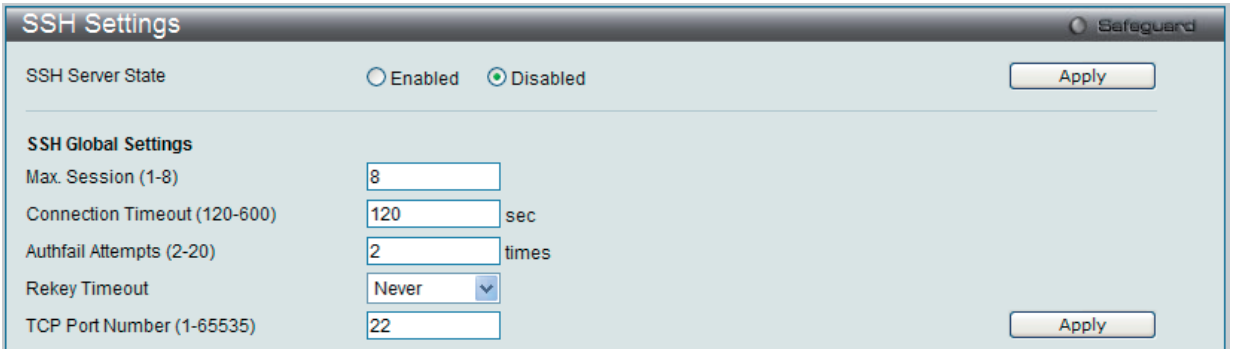


図 13-95　SSH Settings 画面

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。

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。

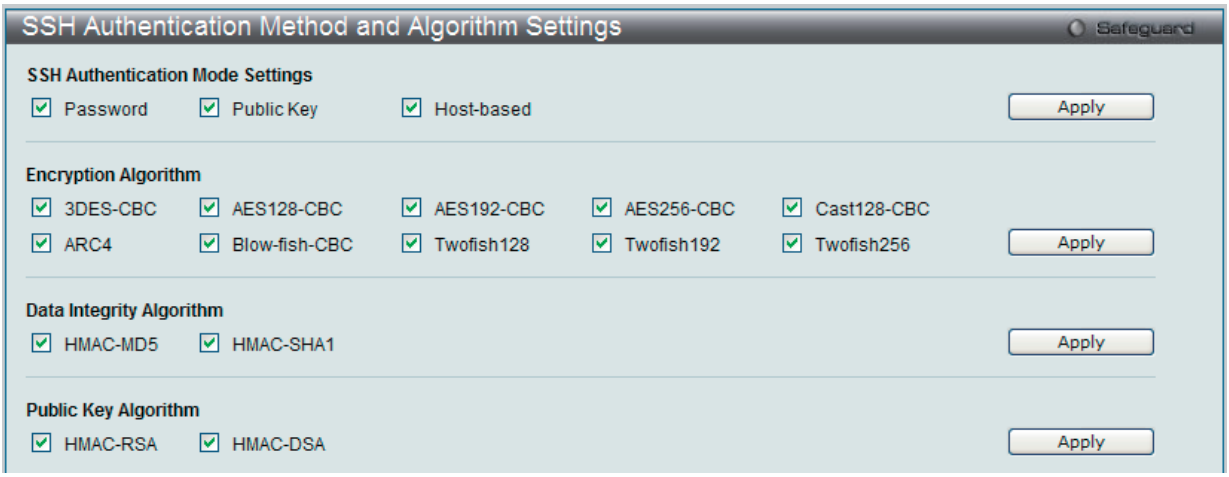


図 13-96 SSH Authentication Method and Algorithm Settings 画面

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 List（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。

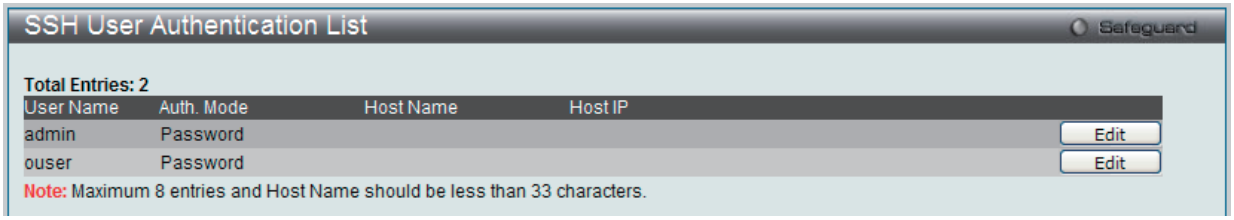


図 13-97 SSH User Authentication Lists 画面

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

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、以下の画面を表示します。

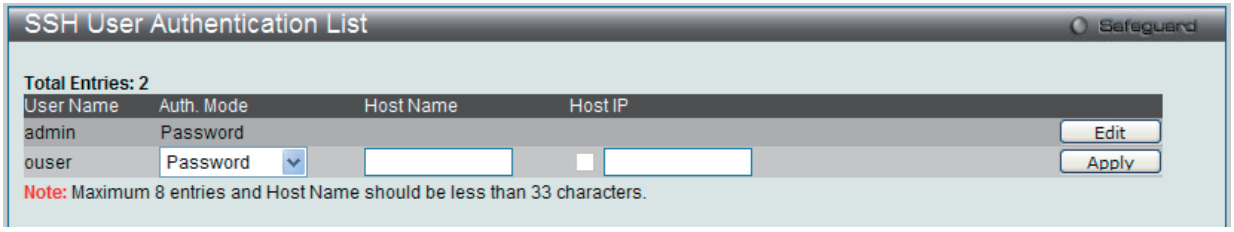


図 13-98 SSH User Authentication Lists 画面 - Edit

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。
Auth. Mode	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 31 文字までの半角英数字を入力します。本項目は「Auth. 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「Auth. 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 57 ページの「User Accounts Settings（ユーザアカウントの設定）」を参照してください。

Trusted Host Settings（トラストホスト設定）

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。

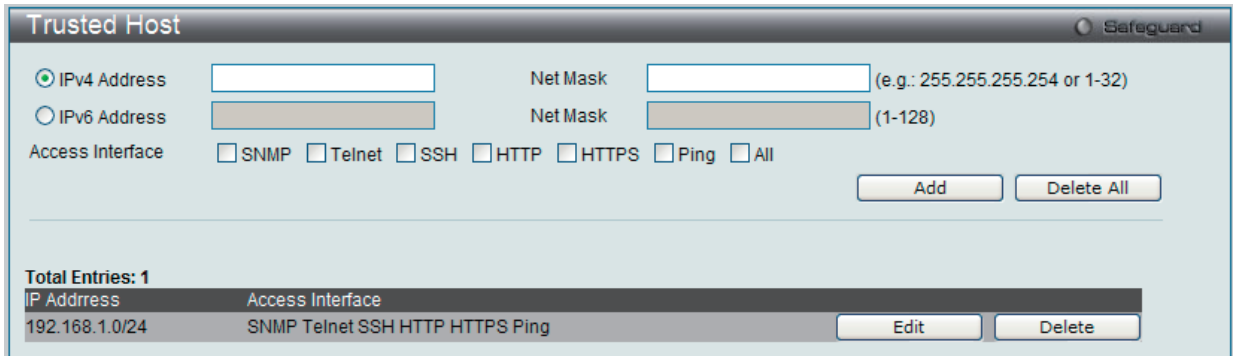


図 13-99 Trusted Host 画面

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。
IPv6 Address	IPv6 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	IPv6 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. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

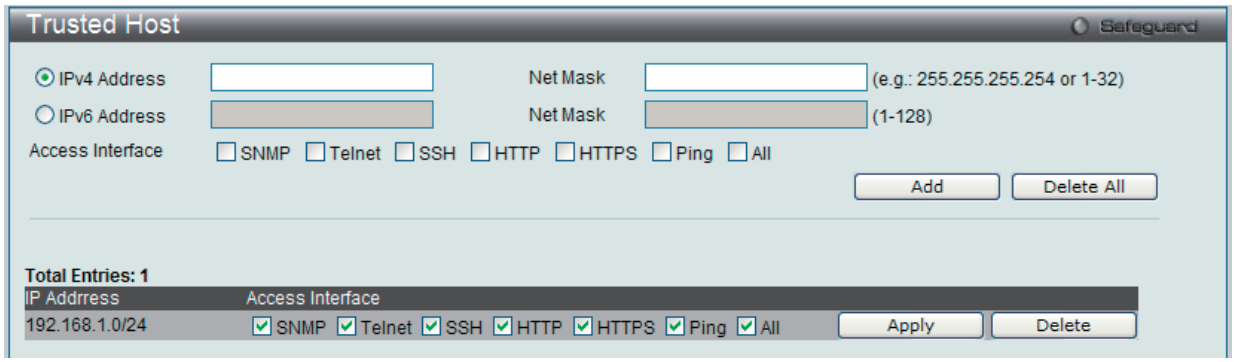


図 13-100 Trusted Host 画面 - Edit

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、スイッチが (a) 処理能力を超えた量のパケットを受信した場合、または (b) メモリ使用率が高すぎる場合には、「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、すべての ARP と IP ブロードキャストパケットを廃棄します。スイッチは 5 秒おきにパケットフラッディングが発生していないかチェックをします。パケット数がしきい値を超えると、スイッチはまず、すべての入力 ARP および IP ブローキャストパケットを 5 秒間停止させます。その 5 秒後に、スイッチは再びパケットの入力フローをチェックします。フラッディングが解消されていれば、スイッチは再びすべてのパケットを受信し始めます。逆に、まだフラッディングが認められれば、前回の 2 倍の時間（10 秒）、すべての入力 ARP および IP ブローキャストパケットを停止させます。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。このしくみを以下に例示します。

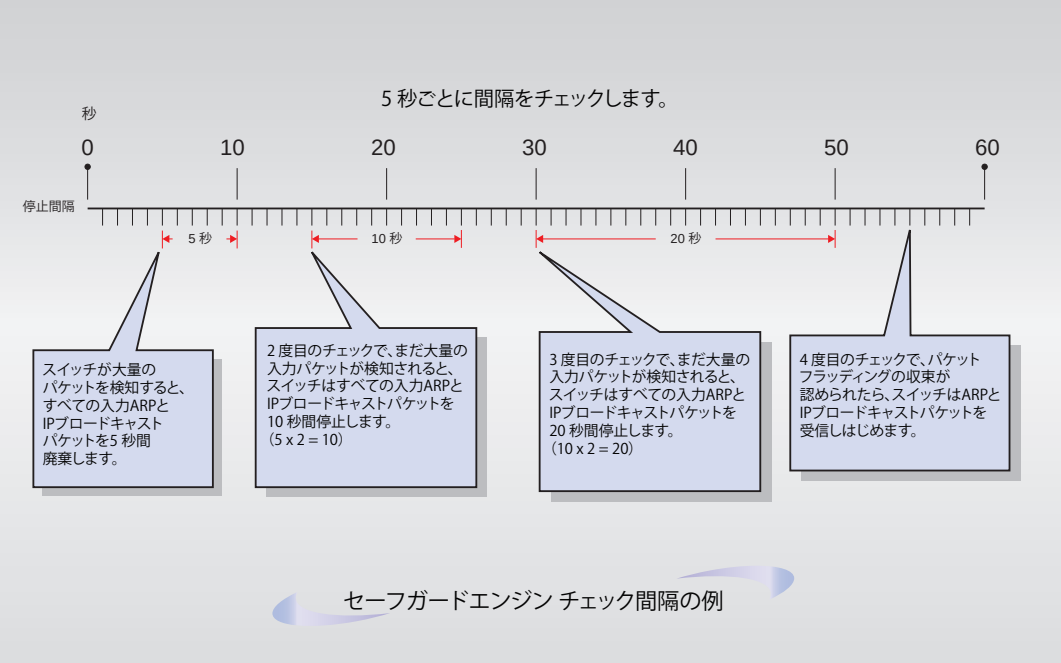


図 13-101 セーフガードエンジンの例

パケットのフラッディングの問題を軽減するためにすべての継続したチェック間隔に対してスイッチは、信頼できない IP アドレスからの受信 ARP および IP ブロードキャストパケットを破棄する時間を倍にします。上の例題では継続したパケットのフラッディング問題が 5 秒間隔で検出された場合は ARP および IP ブロードキャストパケットを破棄す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）パケットのフラッディングを検出しなくなると ARP および IP ブロードキャストパケットを破棄する間隔を 5 秒に戻してプロセスを再開します。

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、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。

注意 セーフガードエンジンが有効の場合、本スイッチは FFP（Fast Filter Processor）メータリングテーブルを使用し、各トラフィックフロー（ARP、IP）に帯域を割り当て、CPU 使用率を制御することでトラフィックを制限します。これは、ネットワーク上のトラフィックのルーティング速度を制限します。

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。

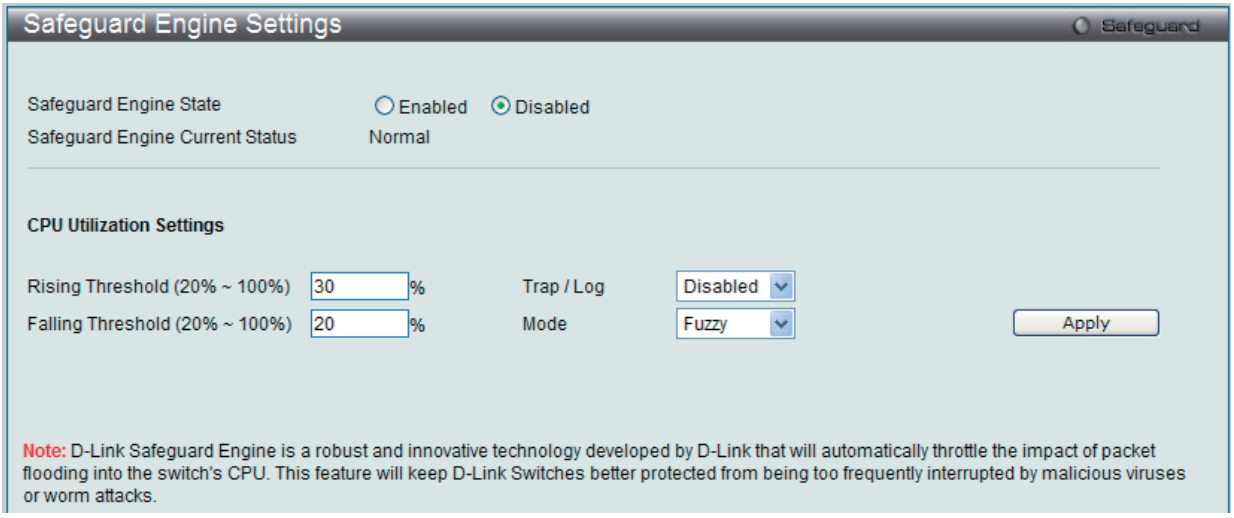


図 13-102 Safeguard Engine Settings 画面

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、「Apply」をクリックします。

以下の項目を使用し、設定を行います。

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 – 本機能はすべてのトラフィックフローに対し平等に動的な帯域割り当てを行うことで CPU に対する IP と ARP トラフィックフローを最小化します。（初期値） • Strict – 本機能はストームがおさまるまで本スイッチ行きではないすべての ARP パケットの受信をストップし、不必要なブロードキャスト IP パケットの受信をストップします。

第 14 章　Network Application（ネットワークアプリケーション）

以下は Network Application の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 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 Server（DHCP サーバ）、DHCP Local Relay Settings（DHCP ローカルリレー設定）、DHCPv6 Relay（DHCPv6 リレー）	405
DNS（ドメインネームシステム）	DNS リレーの設定を行います。以下のメニューがあります。 DNS Relay（DNS リレー）	417
PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入）	受信した PPPoE Discovery および Request パケットへの Circuit ID タグの挿入および削除を行います。	419
RCP Server Settings（RCP サーバ設定）	RCP サーバの設定を行います。	419
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。	420
SNTP Settings（SNTP 設定）	本製品に時刻設定をします。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）	421
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。	423

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、Relay Hops Count Limit より多くなれば、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。DHCP Relay Time Threshold はスイッチが Boot Request パケットを送出する前に待つ最小の時間（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。

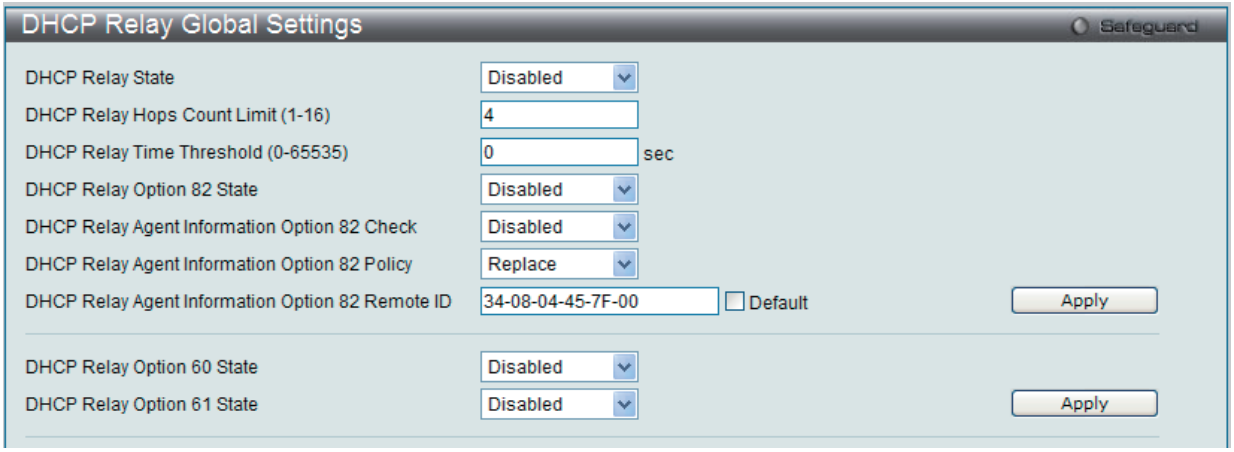


図 14-1　DHCP Relay Global Settings 画面

以下の項目が使用されます。

項目	説明
DHCP Relay State	プルダウンメニューから「Enabled」または「Disabled」を選択し、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 が指定されると、スイッチは DHCP パケットの「Seconds」内の値のプロセスを行いません。0 を指定すると、スイッチは DHCP パケットの「Seconds」フィールドの値のを処理しません。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。

項目	説明
DHCP Relay Agent Information 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	プルダウンメニューから「Replace」、「Drop」または「Keep」を選択します。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 Option 60 State	DHCP Relay Option 60 State 機能を有効または無効にします。
DHCP Relay Option 61 State	DHCP Relay Option 61 State 機能を有効または無効にします。

「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

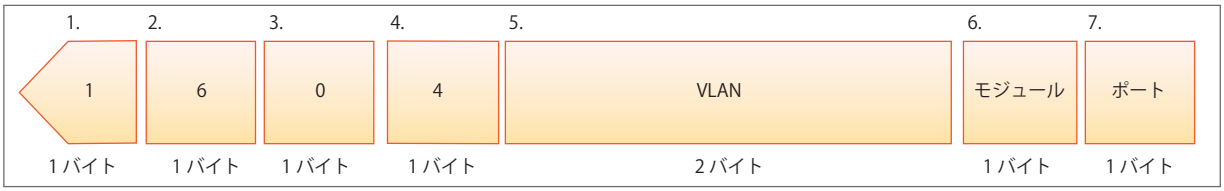


図 14-2　サーキット ID サブオプション形式

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 14-3　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 DHCP サーバに中継するために、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。エントリの削除は「Delete」ボタンをクリックして行います。

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。

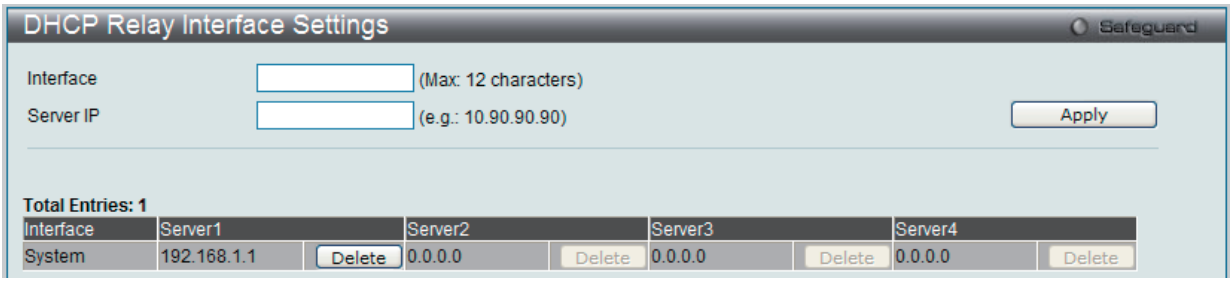


図 14-4　DHCP Relay Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface	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	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 ローカルリレー設定では、DHCP クライアントが同じ VLAN から IP アドレスを取得する際、DHCP リクエストパケットにオプション 82 を追加できるようにします。DHCP ローカルリレー設定を行わない場合、スイッチはパケットを VLAN にフラッドします。DHCP リクエストパケットにオプション 82 を追加させるためには、DHCP ローカルリレー設定とグローバル VLAN のステートを有効にする必要があります。

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。

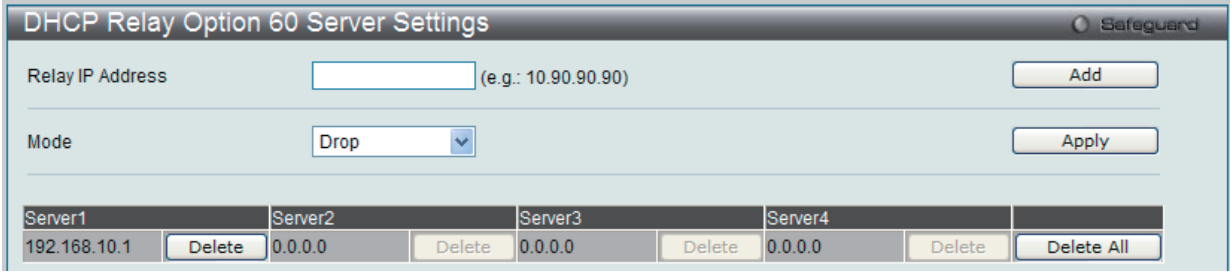


図 14-5　DHCP Relay Option 60 Server Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Relay IP Address	リレー IP アドレスを指定します。
Mode	DHCP リレーオプション 60 サーバのモードを選択します。

「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。
「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。
「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。

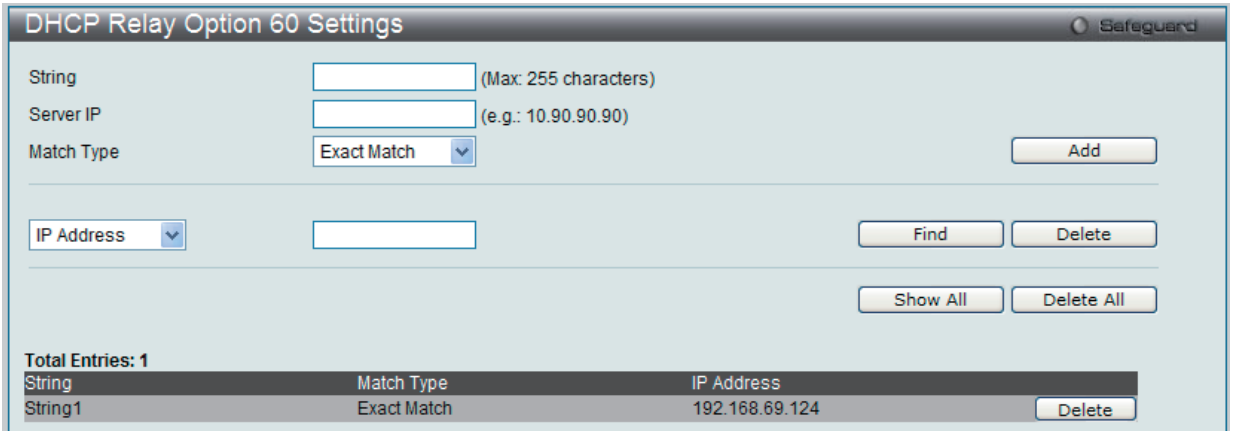


図 14-6　DHCP Relay Option 60 Settings 画面

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。

「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。
「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」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。
「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。
「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 のパラメータを設定します。

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。

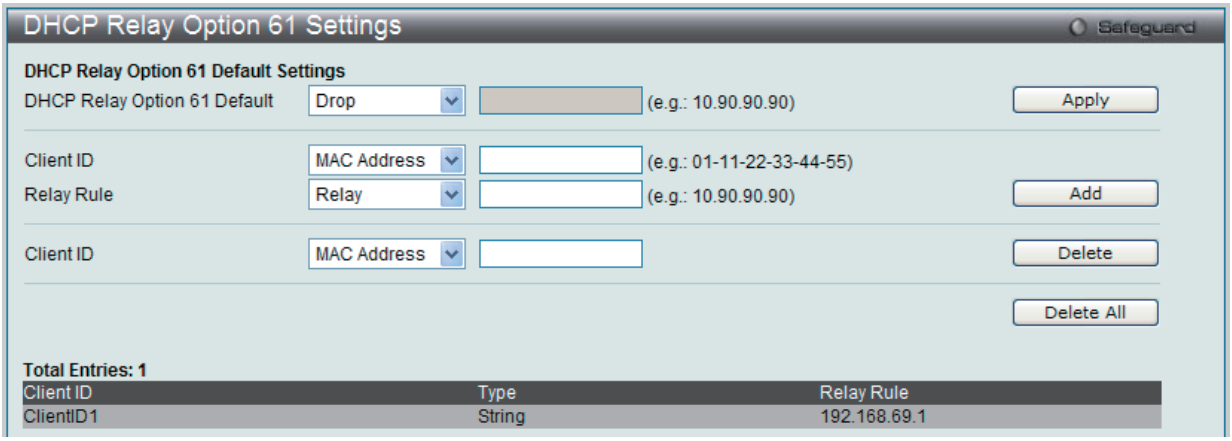


図 14-7　DHCP Relay Option 61 Settings 画面

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。
「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、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 Server（DHCP サーバ）

DHCP（Dynamic Host Configuration Protocol）によってスイッチは、IP アドレス、サブネットマスク、デフォルトゲートウェイ、および他の IP パラメータをこの情報を要求するデバイスに発行することができます。DHCP が有効なデバイスが起動すると、ローカルなネットワークに割り当てられます。このデバイスは DHCP クライアントであり、有効にすると、IP パラメータが設定される前にネットワークにクエリメッセージを送信します。DHCP サーバがこのリクエストを受信すると、DHCP クライアントがローカル設定に利用する上記 IP 情報を含む応答をクライアントに返します。

ローカルに割り当てられたネットワークを利用するために、DHCP に関連する多くのパラメータを設定できます。これにより、割り当てた IP アドレスのリースタイム、DHCP プール内で許可されている IP アドレス範囲、ネットワークに同一のエントリを作成しないようにアドレスプール内の各 IP アドレスを排除する機能など自動 IP 設定を希望するクライアントの IP 設定をコントロールおよび制限します。また、DNS サーバまたはデフォルトルートの IP アドレスなどネットワークの別のデバイスに重要なデバイスの IP アドレスを割り当てることができます。

さらに、スタティック IP アドレスを必要とするネットワークメンテナンスに重要なデバイスの IP アドレスを同一に保つために、DHCP プール内の IP アドレスを指定した MAC アドレスに割り当てることができます。

DHCP Server Global Settings（DHCP サーバグローバル設定）

DHCP サーバグローバルパラメータを設定します。

Network Application > **DHCP** > **DHCP Server** > **DHCP Server 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。

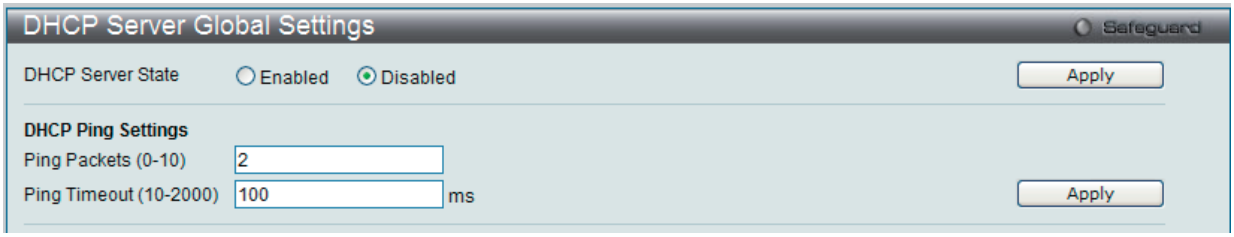


図 14-8　DHCP Server Global Settings 画面

以下のパラメータを設定できます。

パラメータ	説明
DHCP Server State	スイッチを DHCP サーバとしてグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
Ping Packets (0-10)	割り当て済みの IP アドレスを含むネットワークにスイッチが送信する ping パケットの数（0-10）を指定します。ping リクエストが戻らない場合、その IP アドレスは、ローカルネットワークに対して固有であると見なされて、要求側クライアントに割り当てられます。0 は ping テストを行わないことを意味します。初期値は 2 パケットです。
Ping Timeout (10-2000)	ping パケットがタイムアウトになる前に DHCP サーバが待つ時間を選択します。初期値は 100 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。

DHCP Server Exclude Address Settings（DHCP サーバ除外アドレス設定）

DHCP サーバがクライアントに割り当てない IP アドレスを指定します。除外する複数のグループを定義するために本コマンドを繰り返して使用します。DHCP サーバは、DHCP プールサブネットにあるすべての IP アドレスを DHCP クライアントに割り当てることができるものとします。

Network Application > DHCP > DHCP Server > DHCP Server Exclude 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。

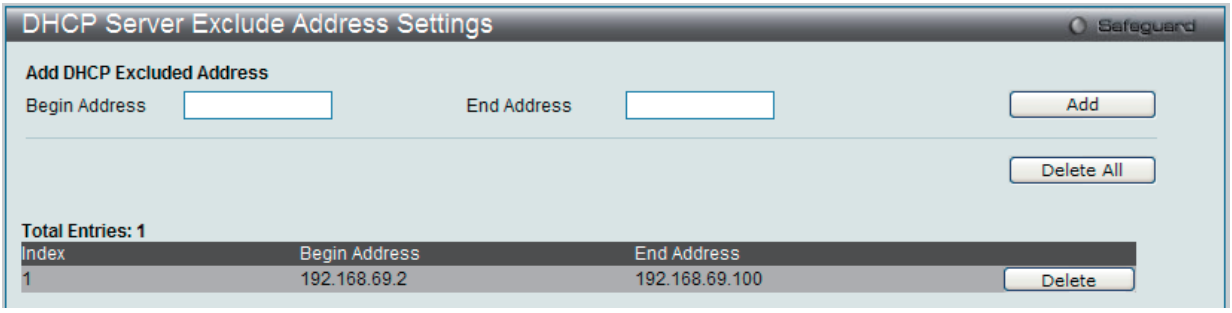


図 14-9　DHCP Server Exclude Address Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Begin Address	除外する開始 IP アドレスを指定します。
End Address	除外する終了 IP アドレスを指定します。

IP アドレスまたは IP アドレス範囲を設定するために、範囲の「Begin Address」（開始アドレス）と「End Address」（終了アドレス）を入力し、「Add」ボタンをクリックします。設定したアドレス範囲は以下の画面下半分に表示されます。

「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。

DHCP Server Pool Settings（DHCP サーバプール設定）

DHCP サーバプールの追加および削除を行います。

Network Application > DHCP > DHCP Server > DHCP Server Pool 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。

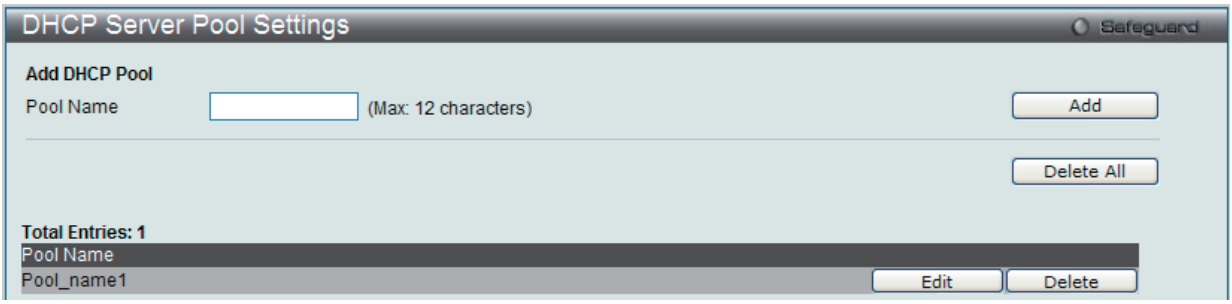


図 14-10　DHCP Server Pool Settings 画面

はじめに「Pool Name」欄に名前（半角英数字 12 文字以内）を入力して、「Add」をクリックすることによって、プールを作成します。一度作成されると、対応する「Edit」ボタンをクリックして、プールの設定を編集することができます。

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。

「Edit」ボタンをクリックすると、以下の画面が表示されます。

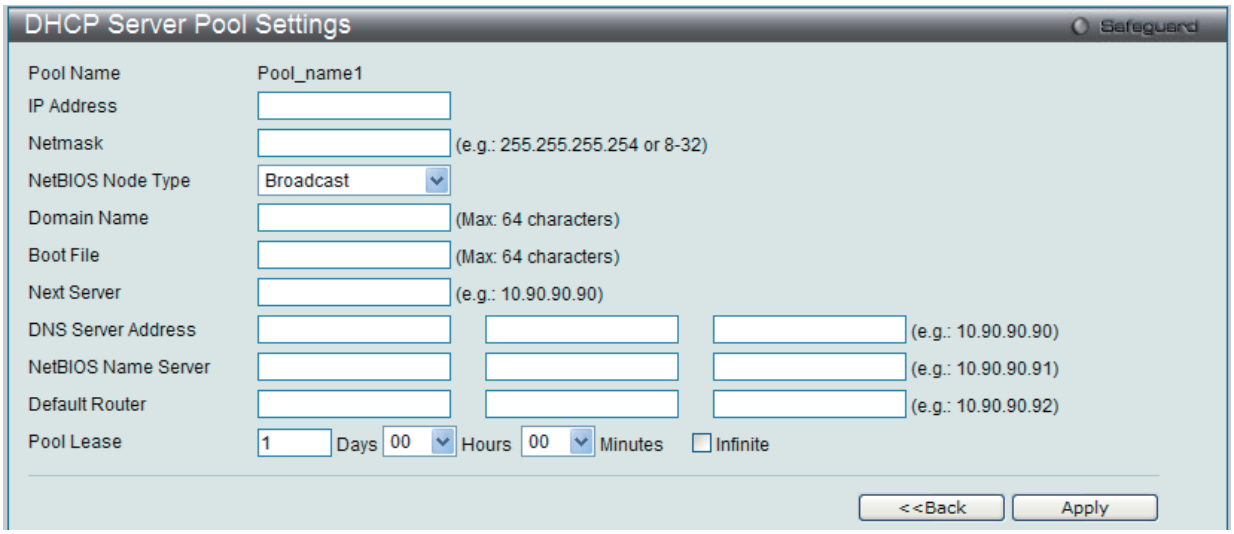


図 14-11　DHCP Server Pool Settings (Edit) 画面

以下のパラメータを使用して設定、表示を行います。

パラメータ	説明
Pool Name	パラメータを調整する DHCP プール名を表示します。
IP Address	DHCP クライアントに割り当てる IP アドレスを入力します。
Netmask	上記フィールドに割り当てられた IP アドレスに対応するネットマスクを入力します。
NetBIOS Node Type	マイクロソフト DHCP クライアントの NetBIOS のノードタイプのタイプを設定します。プルダウンメニューを使用して、4 つのノードタイプ（Broadcast、Peer to Peer、Mixed および Hybrid）から選択します。
Domain Name	クライアントのドメイン名を入力します。ここで設定したドメイン名は、クライアントにデフォルトドメイン名として使用されます。
Boot File	ブートイメージのファイル名。ブートファイルは、クライアント用のブートイメージを保存するのに使用されます。通常、本イメージは、クライアントがロードするのに使用するオペレーティングシステムです。このオプションが二度同じプールに入力されると、2 番目のコマンドは最初のコマンドを上書きします。ブートファイルを指定しないと、ブートファイル情報はクライアントに提供されません。
Next Server	ネクストサーバの IP アドレスを指定します。
DNS Server Address	DNS サーバの IP アドレス。DHCP クライアントが使用可能である DNS サーバの IP アドレスを入力します。1 つのコマンドラインで最大 3 つの IP アドレスを指定できます。
NetBIOS Name Server	WINS サーバの IP アドレス。WINS(Windows Internet Naming Service) は、マイクロソフト DHCP クライアントが通常グループ分けされているネットワーク内の IP アドレスにホスト名を関連付けるために使用する名前解決サービスです。1 つのコマンドラインで最大 3 つの IP アドレスを指定できます。
Default Router	デフォルトルータの IP アドレス。DHCP クライアントにデフォルトルータの IP アドレスを入力します。1 つのコマンドラインで最大 3 つの IP アドレスを指定できます。
Pool Lease	初期値では、DHCP サーバに割り当てられる各 IP アドレスのリース期間（アドレスが有効であることの時間）は 1 日です。 • Days - リースする日 • Hours - リースする時間（時） • Minutes - リースする時間（分） 「Infinite」を指定すると無制限になります。

「Apply」ボタンをクリックして行った変更を適用します。
「<<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。

DHCP Server Manual Binding（DHCP サーバマニュアルバインディング）

アドレスバインディングはクライアントの IP アドレスと MAC アドレスの間のマッピングです。クライアントの IP アドレスを管理者が手動で割り当てるか、または DHCP サーバがプールから自動的に割り当てることができます。プールネットワークのアドレスからクライアントに IP アドレスを割り当てると、ダイナミックバインディングエントリが作成されます。

Network Application > **DHCP** > **DHCP Server** > **DHCP Server Manual Binding** の順にメニューをクリックし、以下の画面を表示します。

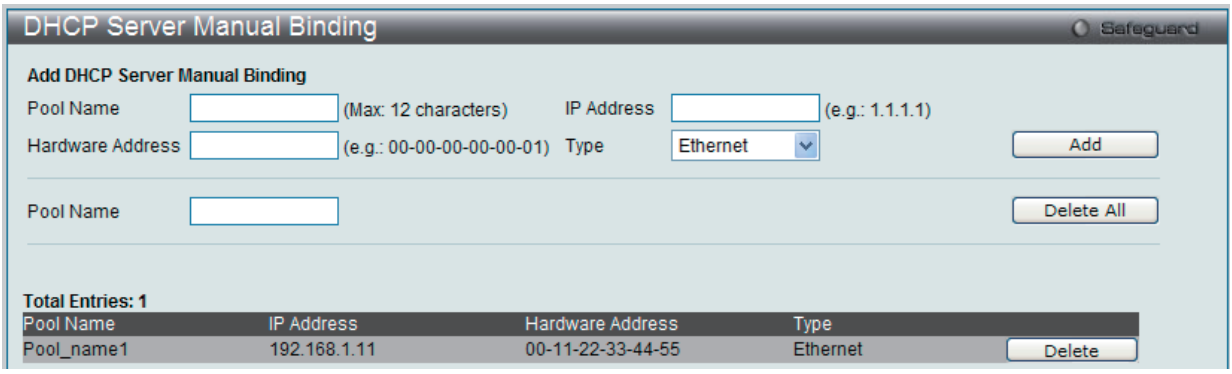


図 14-12 DHCP Server Manual Binding 画面

以下の項目を使用して設定、表示を行います。

パラメータ	説明
Pool Name	マニュアルバインディングエントリを作成する DHCP プール名を入力します。
IP Address	特定のクライアントに割り当てられる IP アドレスを入力します。
Hardware Address	デバイスの MAC アドレスを入力し、前欄で入力した IP アドレスにスタティックに連結します。
Type	この手動連結するエントリが設定される接続タイプを指定します。 • Ethernet - 手動で連結したデバイスがスイッチに直接マニュアルで制限されたデバイスが直接スイッチに接続します。 • IEEE802 - 手動で連結したデバイスがスイッチのローカルネットワークより外側であることを示します。

「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 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。

DHCP Server Dynamic Binding（DHCP サーバダイナミックバインディング）

DHCP サーバダイナミックバインディングテーブルの表示と削除を行います。

Network Application > **DHCP** > **HCP Server** > **DHCP Server Dynamic Binding** の順にメニューをクリックし、以下の画面を表示します。

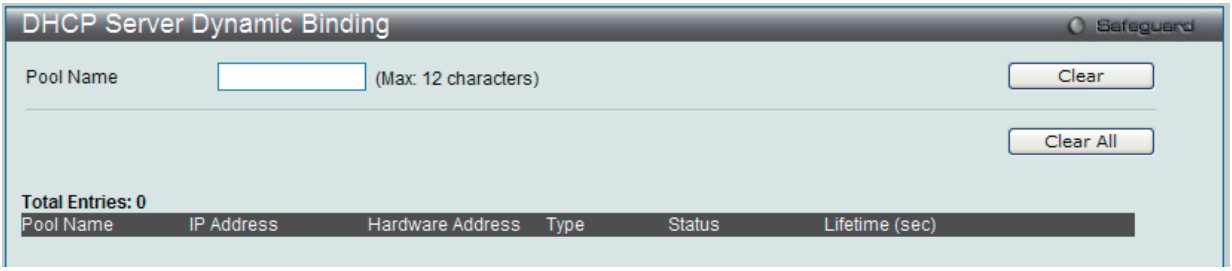


図 14-13 DHCP Server Dynamic Binding 画面

「Pool Name」に DHCP サーバプール名を入力します。
「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。
「Clear All」ボタンをクリックして、テーブルに表示されたすべてのエントリを削除します。

表示されるテーブルの各項目は以下の通りです。

パラメータ	説明
Pool Name	ダイナミックにバインドされている DHCP エントリのプール名を表示します。
IP Address	本スイッチの DHCP サーバ機能によってこのデバイスに割り当てられた IP アドレスを表示します。
Hardware Address	対応する IP アドレスにバインドされているデバイスの MAC アドレスを表示します。
Type	本エントリに定義済みの NetBIOS ネームサーバのノードサーバのタイプを表示します。
Status	ダイナミックまたはマニュアルでバインドされているかというエントリのステータスを表示します。
Life Time (sec)	本 IP アドレスのリースタイムの残り時間（秒）を表示します。

DHCP Conflict IP（DHCP コンフリクト IP）

DHCP サーバは、この IP をバインディングする前にその IP アドレスが他のホストとコンフリクトしているかどうかを判断するために ping パケットを使用します。コンフリクトを確認された IP アドレスはコンフリクト IP データベースに移動します。ユーザがコンフリクト IP データベースからそれをクリアしない限り、システムは、コンフリクト IP データベースの IP アドレスを割り当てません。

Network Application > DHCP > DHCP Server > DHCP Conflict IP の順にメニューをクリックし、以下の画面を表示します。

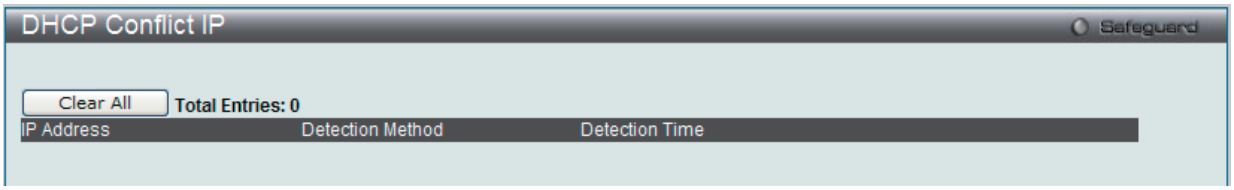


図 14-14 DHCP Conflict IP 画面

「Clear All」ボタンをクリックして、テーブルに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 のローカルリレーが DHCP 要求を受信した VLAN で有効であると、DHCP のローカルなリレー設定では、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 > 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。

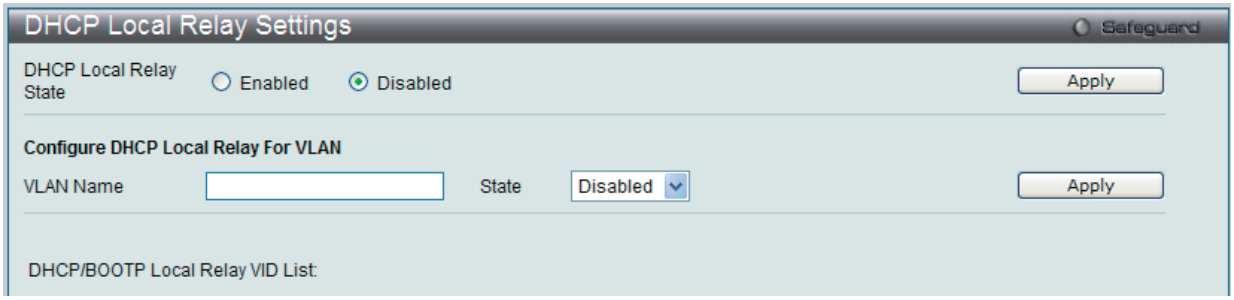


図 14-15 DHCP Local Relay Settings 画面

以下の項目を使用して設定、表示を行います。

パラメータ	説明
DHCP Local Relay Global 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。
VLAN Name	DHCP ローカルリレー操作に適用する VLAN を識別するために使用する 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。

DHCPv6 Relay（DHCPv6 リレー）

DHCPv6 Relay Global Settings（DHCPv6 リレーグローバル設定）

スイッチの DHCPv6 リレー機能を設定します。

Network Application > DHCP > DHCPv6 Relay > DHCPv6 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。

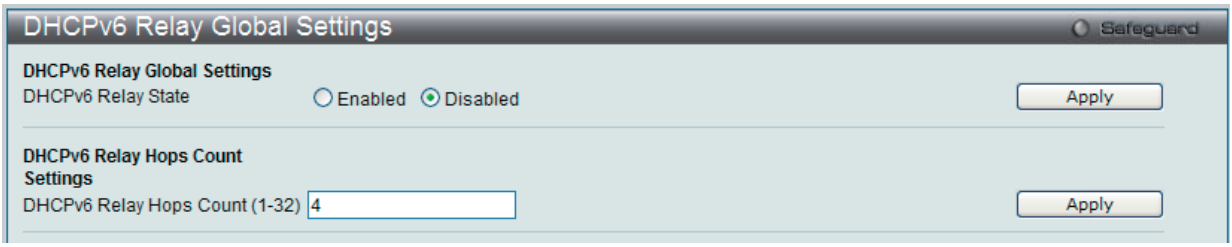


図 14-16 DHCPv6 Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCPv6 Relay State	DHCPv6 リレー機能を「Enabled」(有効)/「Disabled」(無効) にします。
DHCPv6 Relay Hops Count (1-32)	このメッセージ内にリレーすべきリレーエージェントの数を入力します。初期値は 4 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。

DHCPv6 Relay Settings（DHCPv6 リレー設定）

1 つまたはすべての指定インタフェースの DHCPv6 リレー状態を設定し、スイッチの DHCPv6 リレーテーブルから (に) 宛先 IP アドレスを追加または削除します。

Network Application > DHCP > DHCPv6 Relay > DHCPv6 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。

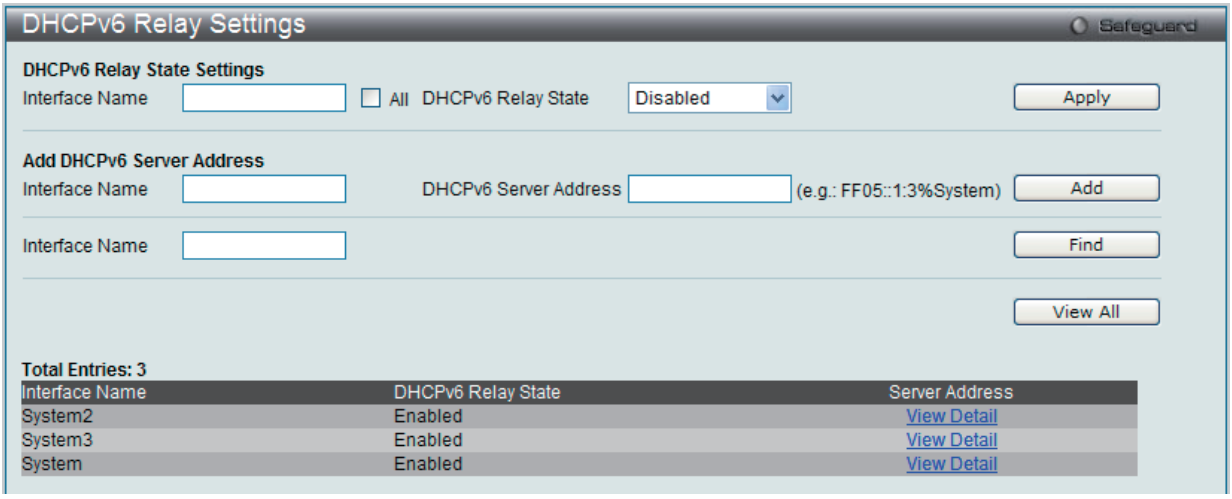


図 14-17 DHCPv6 Relay Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCPv6 Relay State Settings	
Interface Name	IPv6 インタフェース名を入力します。「All」を選択すると、すべての IPv6 インタフェースを選択します。
DHCPv6 Relay State	インタフェースの DHCPv6 リレーの状態を「Enabled」(有効)/「Disabled」(無効) にします。
Add DHCPv6 Address	
Interface Name	追加する IPv6 インタフェース名を入力します。
DHCPv6 Server Address	DHCPv6 サーバの IPv6 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。

新規エントリの追加

「Add DHCPv6 Address」セクションの項目入力後、「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。「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。

「View Detail」をクリックすると、DHCPv6 リレーインタフェースの詳細情報を表示します。

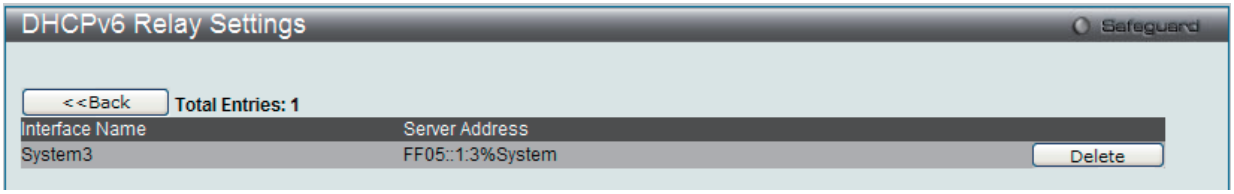


図 14-18 DHCPv6 Relay Settings 画面 - View

「<<Back」をボタンをクリックすると、前のページに戻ります。

DNS（ドメインネームシステム）

コンピュータのユーザは外部と接続するコンピュータの名前として、テキスト形式のものを使用する方が使い勝手が良いといえます。コンピュータ自身には 32 ビットの IP アドレスが必要です。このため、ネットワークデバイスのテキスト形式の名前（ドメイン名）とそれに対応する IP アドレスのデータベースがどこかに保持される必要があります。

DNS（Domain Name System）は、そのようなドメイン名と IP アドレスの関連付けをインターネット経由で行い、イントラネットでもこれが使用されるようになってきました。異なるサブネットを通して通信する DNS サーバの間には、中継を行うために DNS リレー機能が必要になります。DNS サーバは IP アドレスにより識別します。

ドメイン名とアドレスのマッピング
ドメイン名とアドレスの関連付けはネームサーバというプログラムにより行われます。クライアントプログラムはネームリゾルバと呼ばれます。ネームリゾルバは、ドメイン名とアドレスの変換を行うためにいくつかのネームサーバと連絡を取る必要があります。

DNS サーバ群は、ドメイン名に対応した階層構造になっています。1 台のサーバは通常 1 つのネットワークにドメイン名を持ち、これが上位に位置するルート DNS サーバ（通常 ISP が管理）に接続を行います。

ドメイン名の解決
ドメイン名の解決はその都度ネームサーバに問い合わせる場合と、DNS にまとめて解決を求める場合があります。クライアントは、ドメイン名、必要な応答の種類、およびクエリを受信したサーバが名前の解決をできない場合に、DNS によってすべてのドメイン名の解決を行うか、または次の DNS サーバのアドレスのみを返せばよいのかを指定したコードを含むクエリを作成します。

DNS サーバがクエリを受信すると、その名前がサブドメイン中に存在するかどうかをチェックします。存在していればサーバは名前を解決し、クエリへの応答としてクライアントに返します。自分で解決できない場合は、クライアントが要求する方法の名前解決を実行します。 1 つは再帰的解決と呼ばれる方法で、サーバは名前の解決が完了するまで、他の DNS サーバと連絡を取り合います。もう 1 つは反復的解決と呼ばれる方法で、DNS サーバが自分で解決できない場合は、クライアントが連絡すべき次の DNS サーバのアドレスのみを返します。

各 DNS クライアントは、最低 1 台の DNS サーバに連絡可能で、各 DNS サーバは最低 1 台のルートサーバに連絡する手段を持たなければなりません。

ドメインネームサービスを行うデバイスのアドレスは、DHCP または BOOTP サーバから得る場合と、初期設定時に手動で OS に設定する場合があります。

DNS Relay（DNS リレー）

DNS Relay Global Settings（DNS リレーグローバル設定）

DNS リレーのグローバル設定を行います。

Network Application > DNS > DNS Relay > DNS 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。

図 14-19 DNS Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

パラメータ	説明
DNS State	スイッチの DNS リレーサービス機能を「Enabled」（有効）/「Disabled」（無効）にします。
Primary Name Server	プライマリドメインネームサーバ（DNS）の IP アドレスを指定します。
Secondary Name Server	セカンダリドメインネームサーバ（DNS）の IP アドレスを指定します。
DNSR Cache Status	スイッチの DNS キャッシュを「Enabled」（有効）/「Disabled」（無効）にします。
DNSR Static Table State	スタティック DNS テーブルを「Enabled」（有効）/「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。

DNS Relay Static Settings（DNS リレースタティック設定）

スイッチ名前解決テーブルにスタティックなエントリの追加または削除を行います。

Network Application > DNS > DNS Relay > DNS Relay Static 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。

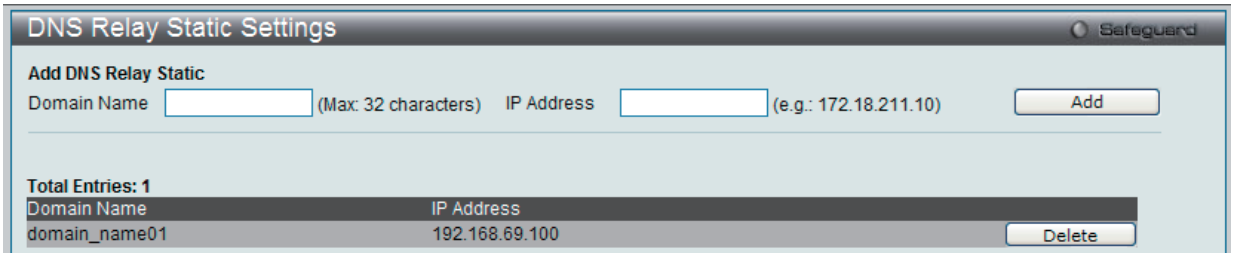


図 14-20 DNS Relay Static Settings 画面

以下の項目を使用して設定、表示を行います。

パラメータ	説明
Domain Name	ドメイン名を入力します。
IP Address	DNS 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。

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。

PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入設定）

本設定を有効にすると、システムは、受信した PPPoE Discovery および Request パケットにタグがない場合に Circuit ID タグを挿入します。また、受信 PPPoE Offer および Session Confirmation パケットから Circuit ID タグを削除します。

挿入する Circuit ID は次の情報を含んでいます。：クライアント MAC アドレス、Device ID、およびポート番号。
さらに、ユーザが定義する文字列のオプションを Circuit ID に挿入できます。初期値では、スイッチの IP アドレスが、Circuit ID オプションをコード化するためにデバイス ID として使用されます。

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。

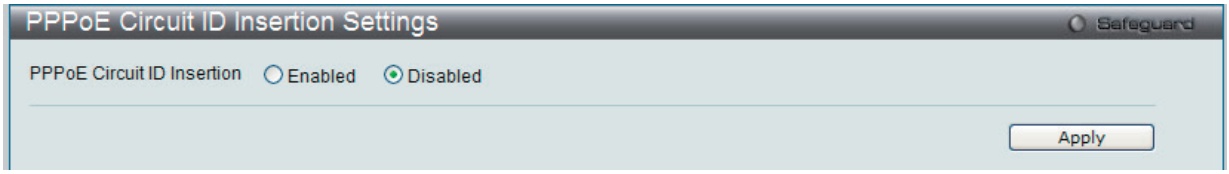


図 14-21　PPPoE Circuit ID Insertion Settings 画面

選択ポートにおける PPPoE Circuit ID の挿入を「Enabled」（有効）または「Disabled」（無効）にして「Apply」ボタンをクリックします。

RCP Server Settings（RCP サーバ設定）

RCP サーバ情報を設定するために使用されます。サーバまたはリモートユーザ名が指定されない場合に、このグローバル RCP サーバ設定を使用できます。各システムに 1 つの RCP サーバだけが設定可能です。CLI コマンドで RCP サーバを指定せず、グローバルな RCP サーバが設定されていない場合、スイッチは、RCP コマンドの実行中、サーバの IP アドレスまたはリモートユーザ名を入力するように求めます。

Network Application > RCP 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。

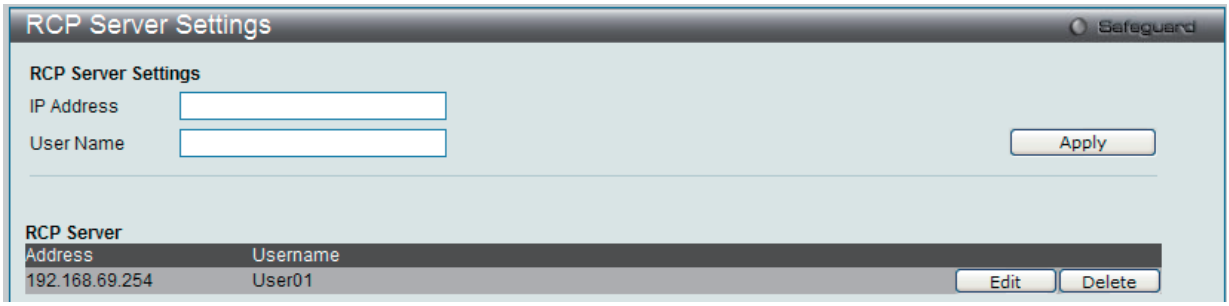


図 14-22　RCP Server Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IP Address	グローバルな RCP サーバの IP アドレス。初期値では、未設定です。
User Name	グローバルな RCP サーバにログインするためのリモートユーザ名。初期値では、グローバルなサーバのリモートユーザ名は未設定です。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

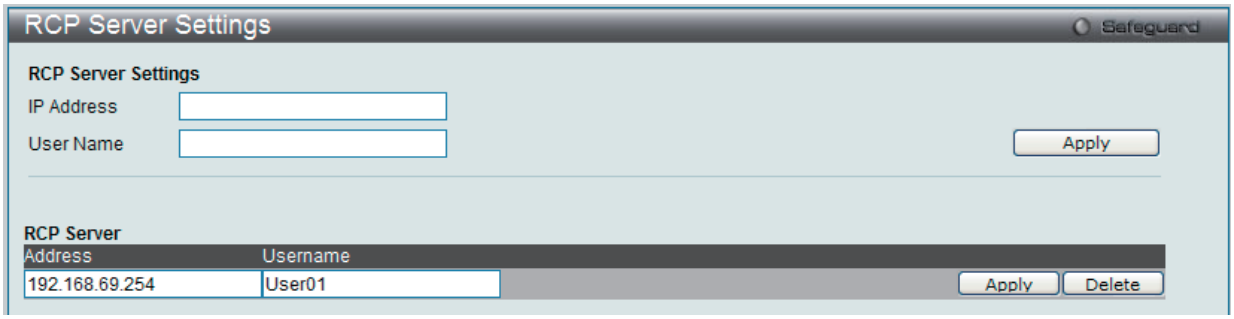


図 14-23　RCP Server Settings 画面 - Edit

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。

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。

スイッチは、以下のイベントが 1 つ以上起きた場合に受信者に E-mail を送信します。
- スイッチでコールドスタートが起きた場合。
- リンクダウン状態でポートが接続した場合。
- リンクアップ状態でポートが接続した場合。
- SNMP 認証がスイッチによって拒否された場合。
- スイッチがスイッチ設定エントリを NVRAM に保存した場合。
- ファームウェアのダウンロードが行われている間に TFTP に異常が起きた場合。この異常には、「in-process」、「invalid-file」、「violation」、「filenot-found」、「complete」、「time-out」の各メッセージが TFTP サーバから送られた場合を含みます。
- スイッチでシステムリセットが行われた場合。

スイッチイベントに関する、SMTP サーバからの E-mail 内の情報は以下の通りです。
- 送信元デバイス名および IP アドレス。
- メッセージを送信した SMTP サーバとクライアントのアイデンティティを示すタイムスタンプ、およびスイッチからメッセージを受信した日時。リレーされているメッセージは、各リレーごとにタイムスタンプがあります。
- E-mail メッセージの送信をさせた、スイッチで起きたイベント。
- ユーザがイベントに対し保存やファームウェアの更新などの処理を行うと、そのタスクを行ったユーザの IP アドレス、MAC アドレスおよびユーザ名がイベントが起きたことを知らせるシステムメッセージと共に送信されます。
- 同じイベントが 2 回以上起きる場合、2 回目のメールメッセージと続いて繰り返されるメールメッセージには、メールメッセージのタイトルにシステムエラーメッセージを記載されます。

送信過程で起こるイベントについて以下に詳細を説明します。
- 緊急メールは即座に受信者に割り当てられて最優先で送信され、通常のメールは後の順番になります。
- キューに置かれる未送信のメールメッセージの最大数は 30 を超えることはできません。送信待ちキューがフルの場合は新しいメッセージはすべて廃棄されます。
- メール受信者への最初のメッセージが受け取られない場合、そのメッセージは送信待ちキューに置かれて順番を待ち、他のメッセージの送信が行われます。
- 受信者へのメール送信指示の最大数は 3 です。メールメッセージ送信指示は指示数が最大数になるまで 5 分ごとに行われます。送信指示数が最大の時に送信に失敗した場合、そのメッセージはドロップされメール受信者には送信されません。
- スイッチがシャットダウンまたは再起動された場合、送信待ちキュー内のメッセージは消失します。

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。

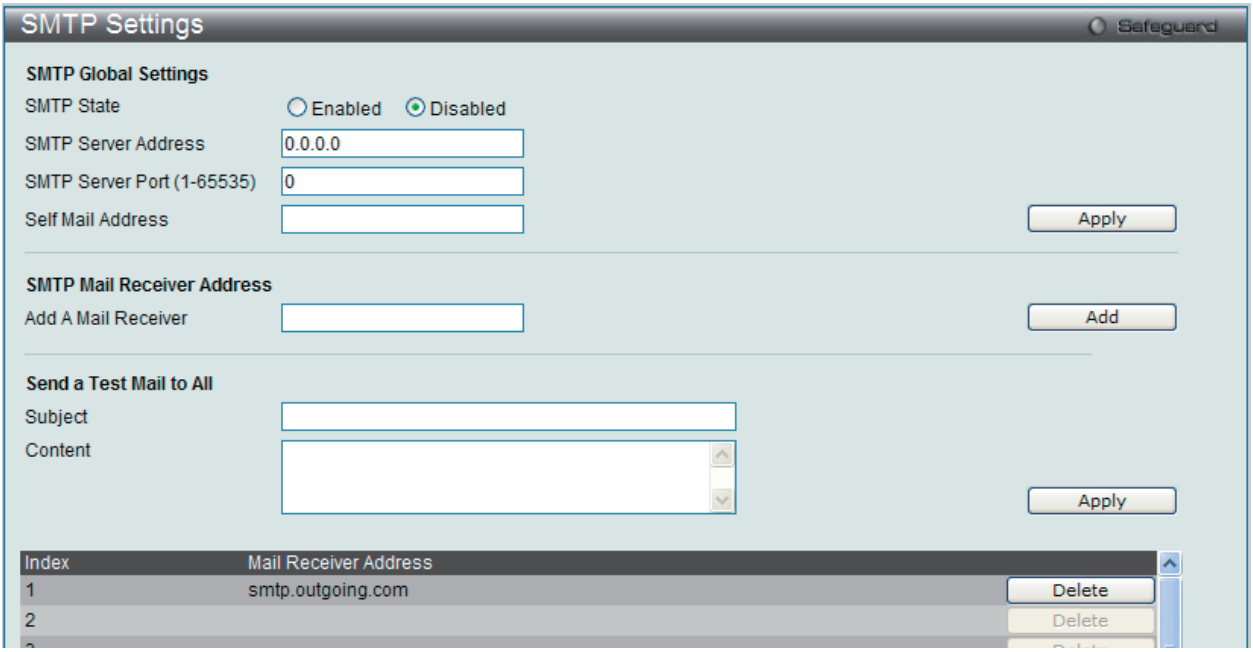


図 14-24 SMTP Service Settings 画面

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	設定したすべてのアドレスに送信するテストメールの題名を入力します。
Content	設定したすべてのアドレスに送信する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。

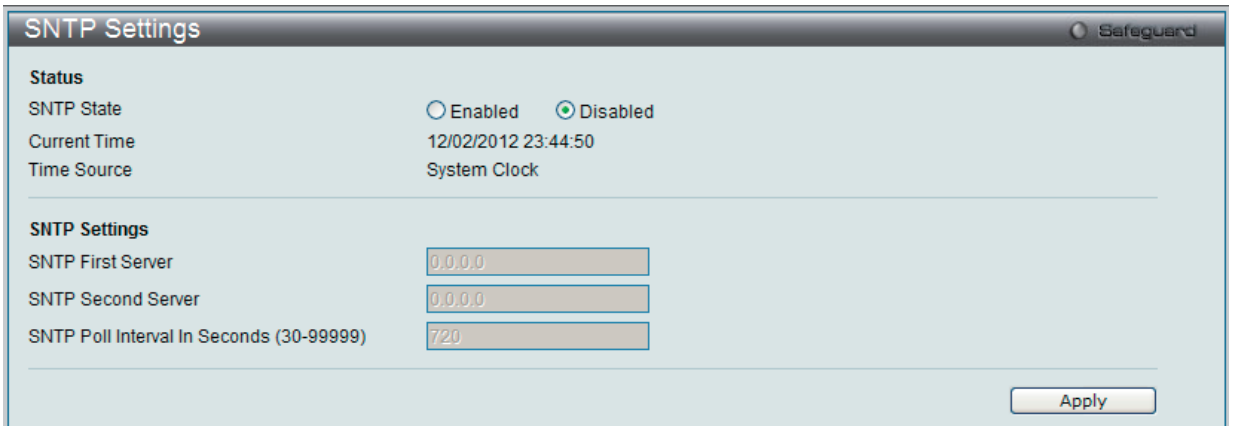


図 14-25　SNTP Settings 画面

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。

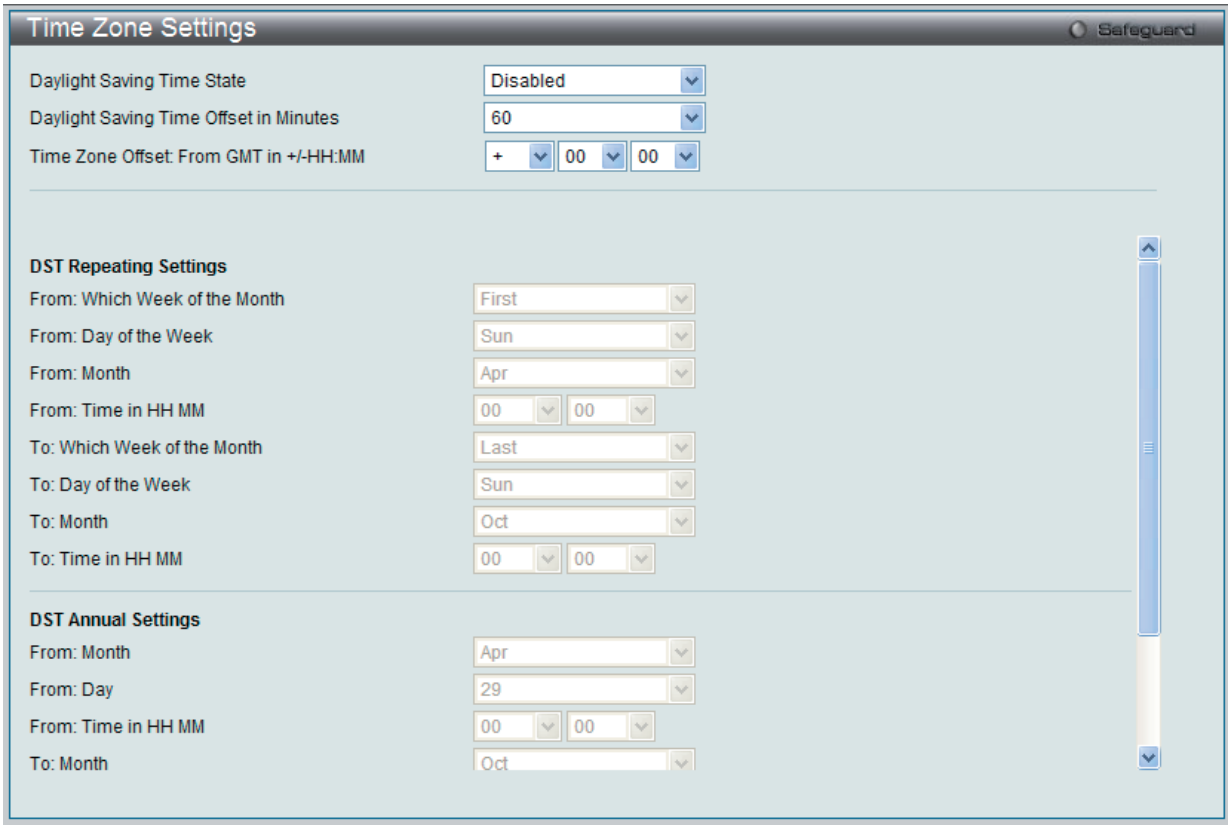


図 14-26　TimeZone Settings 画面

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 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。

項目	説明
To: Day Of 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。
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。（ごと年）
From: Day	DST が開始する日を指定します。（ごと年）
From: Time In HH MM	DST が開始する時間を指定します。（ごと年）
To: Month	DST が終了する月を指定します。（ごと年）
To: Day	DST が終了する日を指定します。（ごと年）
To: Time In HH MM	DST が終了する時間を指定します。（ごと年）

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。

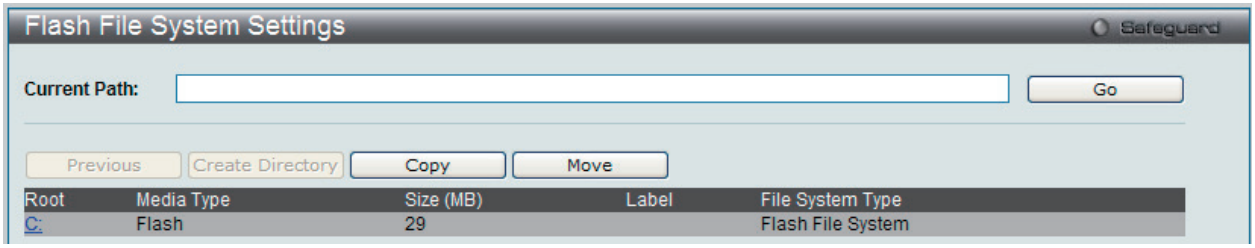


図 14-27　Flash File System Settings 画面

「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。

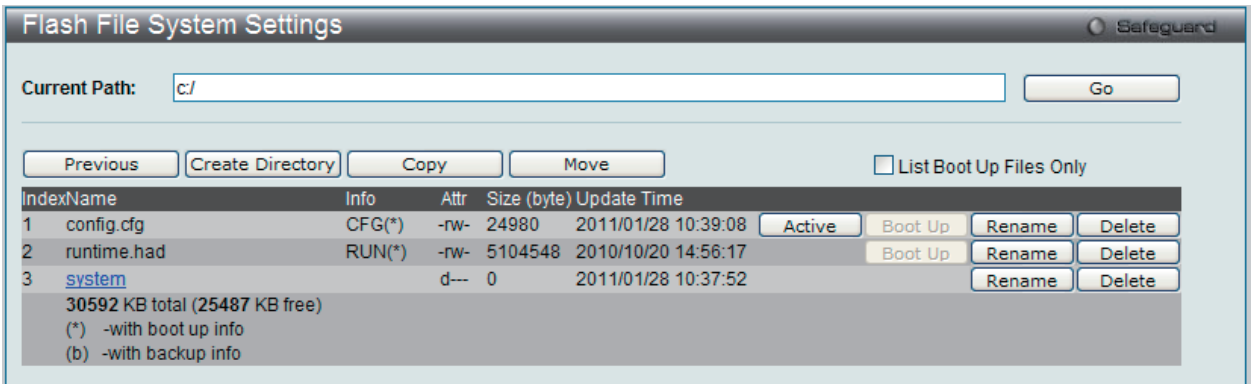


図 14-28 Flash File System Settings 画面

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。

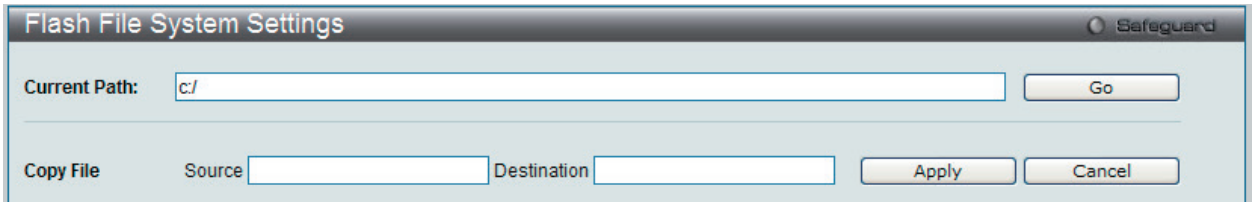


図 14-29 Flash File System Settings 画面 - Copy

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。

ファイル名の変更

1. 「Rename」ボタンをクリックすると、以下の画面が表示されます。

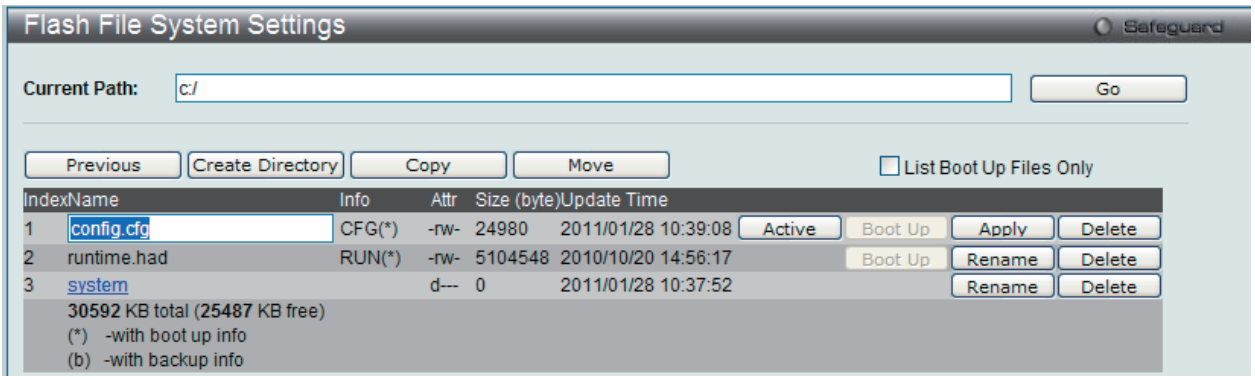


図 14-30 Flash File System Settings 画面 - Rename

2. ファイル名を変更して「Apply」ボタンをクリックします。

第 15 章　OAM（Object Access Method : オブジェクトアクセス方式）

以下は OAM の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）	425
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）	438
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。	441
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。	442

CFM（Connectivity Fault Management : 接続性障害管理）

CFM またはイーサネット CFM は、エンドツーエンドのイーサネットレイヤ OAM プロトコルです。CFM は IEEE 802.1ag によって定義されており、大規模なイーサネットの MAN（メトロポリタンエリアネットワーク）と WAN における接続性のモニタリング、Fault Notification（障害通知）、および障害を隔離する手段を持っています。

イーサネットは隔離されている企業内 LAN を従来通りに動作させます。イーサネットが複数の管理ドメインを包含するよりスケールの大きいキャリアネットワークで動作するように拡張されているため、さらに大きく複雑なネットワークの需要から新しい OAM 機能が要求されています。これらのよりスケールの大きいネットワークは、多大なユーザベースを持ち、様々なネットワークアプリケーションを搭載し、通常、リンクの動作時間が重要である従来の企業イーサネット LAN よりはるかに広域に及ぶことから、イーサネットで動作可能な接続性障害に対処する手段が必要となりました。既存の OAM プロトコルのいずれも適切にこの新しい状況を扱うことができなかったため、イーサネット CFM は MAN と WAN にイーサネット技術を適用することで起こる新しい操作管理の必要に応じるように発展しました。

イーサネット CFM は、身近なイーサネットプラットホームの上位ですべてが操作される場合にイーサネットのネットワークサービスプロバイダにエンドツーエンドのサービスレベルの OAM と低い運用コストなど、様々な利益を提供します。

CFM はいくつかの新しい期間と概念をイーサネットに導入しており、これらを以下で簡単に説明します。

Maintenance Domain（メンテナンスドメイン）
メンテナンスドメインは、ネットワークを管理する目的のために作成される管理エリアについて言及する一般的な用語です。メンテナンスドメインは、単一のエンティティまたはオーナーによって操作されます。また、境界内部に 1 セットのポートを持つ境界によって定義されます。

イーサネット CFM メンテナンスドメイン（本マニュアルでは MD として呼ぶ）は、他の MD と階層関係を構成します。通常、MAN または WAN は、カスタマ、サービスプロバイダ、およびオペレータの構造的な関係を反映するドメインのサイズに基づいた階層に分割することができます。オペレータがサブネットワークを経由したサービスの送信を提供している間、サービスプロバイダには、エンドツーエンドのサービスの責任があります。階層は 0-7 の範囲のメンテナンスレベル値で定義されます。7 が最も高いレベルで、0 が最も低いレベルとなります。MD が大きいほど、メンテナンスレベルは高くなります。例えば、カスタマのドメインが最も大きい MD である場合、メンテナンスレベル 7 が割り当てられる必要があり、オペレータ MD が最もレベルが低い場合、メンテナンスレベル 0 が割り当てられ、サービスプロバイダドメインはこれらの値の間となります。メンテナンスレベルは、ネットワーク管理者によって手動で割り当てられます。MD 階層のすべてのレベルが共に動作する必要があります。

MD のネストは許可されていますが、MD の管理が単一のオーナーによって実施されるという要求に違反するために、それらは交わることはできません。2 つ以上のドメインをネストさせる場合、外側のドメインにネストするドメインより高いメンテナンスレベルを割り当てる必要があります。

CFM の操作とメッセージ交換は、ドメインごとに行われます。これは、例えば、レベル 3 で動作する CFM が、より高いレベルによるレベル 3 のネットワーク検出を許可しないことを意味します。

Maintenance Association（メンテナンスアソシエーション）
CFM のメンテナンスアソシエーション (MA) は、同じ管理ドメインレベルとメンテナンスアソシエーション（MAID）で構成された MEP のセットです。

MD 内の異なる MA は、異なる MA 名を持つ必要があります。異なる MD の異なる MA は、同じ MA 名を持つことができます。MA に指定される MEP リストは、異なるデバイスに位置することができます。MEP は、これらのデバイスのポートに明示的に作成される必要があります。MEP は MA を経由して定期的に CCM パケットを送信します。受信する MEP は、構成の保全性チェックのために、本 MEP リストに対して他の MEP から受信した CCM パケットを検証します。

Maintenance Point（メンテナンスポイント）
CFM のメンテナンスポイントは、メンテナンスドメイン内のポートにおける境界のポイントです。メンテナンスポイントは、正しいメンテナンスレベルに所属しないフレームを破棄することで MD の境界内の CFM フレームをフィルタします。メンテナンスポイントには 2 つのタイプ、Maintenance Endpoint : MEP（メンテナンスエンドポイント）、および Maintenance Intermediate Point : MIP（メンテナンス中間ポイント）があります。MEP と MIP はネットワーク管理者によって手動で設定されます。

MEP は、メンテナンスドメインの端に存在し、MD の境界を定義しています。MEP 機能は、MD に制限されるようにフィルタする CFM メッセージを含みます。MEP は Connectivity Check Messages (CCM : 接続性チェックメッセージ) を転送するために設定され、設定されると、Traceroute およびループバックメッセージを送信します。MEP は、内向きまたは外向きが可能です。

内向き MEP は、MEP が設定されているブリッジポートを経由しないでブリッジリレー機能に CFM フレームを送信します。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。内向き MEP が設定されているポートがスパニングツリープロトコルによりブロックされると、MEP はもう CFM メッセージの送信も受信もできません。

外向き MEP は、ブリッジポートにフレームを送信し、送信されるポートにだけ設定されます。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。外向き MEP が設定されているポートがスパニングツリープロトコルによりブロックされても、MEP はブリッジポートを経由して CFM メッセージの送信と受信が可能です。

MIP は、境界ではなく、MD 内部にあるメンテナンスポイントです。MIP は他の MIP および MEP から CFM フレームを受信します。これらのフレームは、ブリッジリレー機能とブリッジポートを使用することで分類されて送信されます。MIP より低レベルにあるすべての CFM フレームがブロックされ、送信元にかかわらず破棄されます。より高いレベルにあるすべての CFM フレームは、送信元にかかわらず転送されます。MIP が設定されているポートがスパニングツリープロトコルによりブロックされると、MIP はブリッジリレー機能側への CFM メッセージの受信、またはリレーはできません。しかし、MIP は、ブリッジポートから CFM メッセージの受信、または応答は可能です。

CFM メッセージには Continuity Check Message (CCM : 連続性チェックメッセージ)、Loopback Message（LBM : ループバックメッセージ）、および Link Trace Message（LTM : リンクトレースメッセージ）が含まれます。CFM はブリッジにより送信、停止、処理、およびリレーされる標準のイーサネットフレームを使用します。ルータは、限定的な CFM 機能をサポートしています。

Continuity Check Message (CCM : 連続性チェックメッセージ)
MEP 内で交換されるマルチキャストメッセージです。CCM は、ドメイン内の他の MEP に対して MIP の検出を許可し、また、MIP が MEP を検出することを許可します。CCM はメンテナンスドメインに対して制限されます。CCM は、同じメンテナンスレベルにある MIP によって分類され、同じメンテナンスレベルにあるリモート MEP によって停止されます。それらは、単方向 (無応答ソリシテーション) であり、MEP が設定されているポートの状態を伝送します。LBM は宛先に到達可能かどうかだけを示し、各ホップの発見を許可しないという点において Ping または ICMP メッセージに似ています。

Link Trace Messages (LTM : リンクトレースメッセージ)
同じメンテナンスレベルにあるリモート MEP および MIP と近接関係を示すために MEP が送信するマルチキャスト CFM フレームです。LTM のメッセージ本体は、リンクトレースを終了するターゲット MEP の宛先 MAC アドレスを含んでいます。MIP または MEP が LTM を受信すると、始動している MEP に対してユニキャスト Link Trace Reply（LTR : リンクトレースリプライ）を生成します。また、ターゲット MEP の宛先 MAC アドレスに LTM を送信します。LTM はターゲット MEP または MIP までのパスを効果的にトレースします。

Loopback Messages (LBM : ループバックメッセージ)
宛先に到達可能かどうかだけを示し、各ホップの発見を許可しないという点において Ping または ICMP メッセージに似ています。

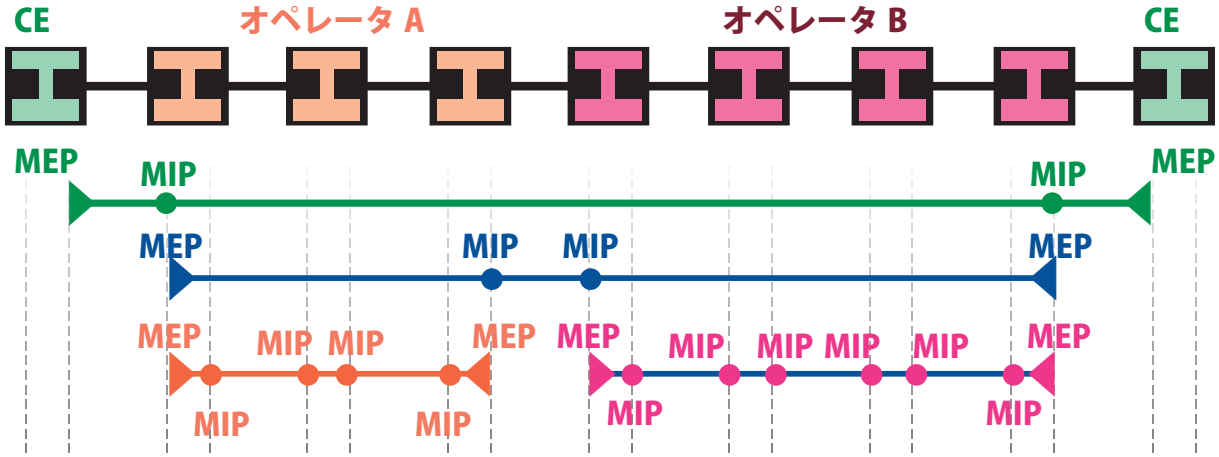


図 15-1　OAM ドメイン構造

- Maintenance Association (MA) - 管理者がネットワークをモニタリングしている部分の境界
- Maintenance Domain (MD) - 階層内のモニタリングのレベル
- Maintenance End Points (MEP) - MA または MD のエンドポイント
- Maintenance Intermediate Points (MIP) - MA または MD 内の中間点
- Customer Equipment (CE)

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。

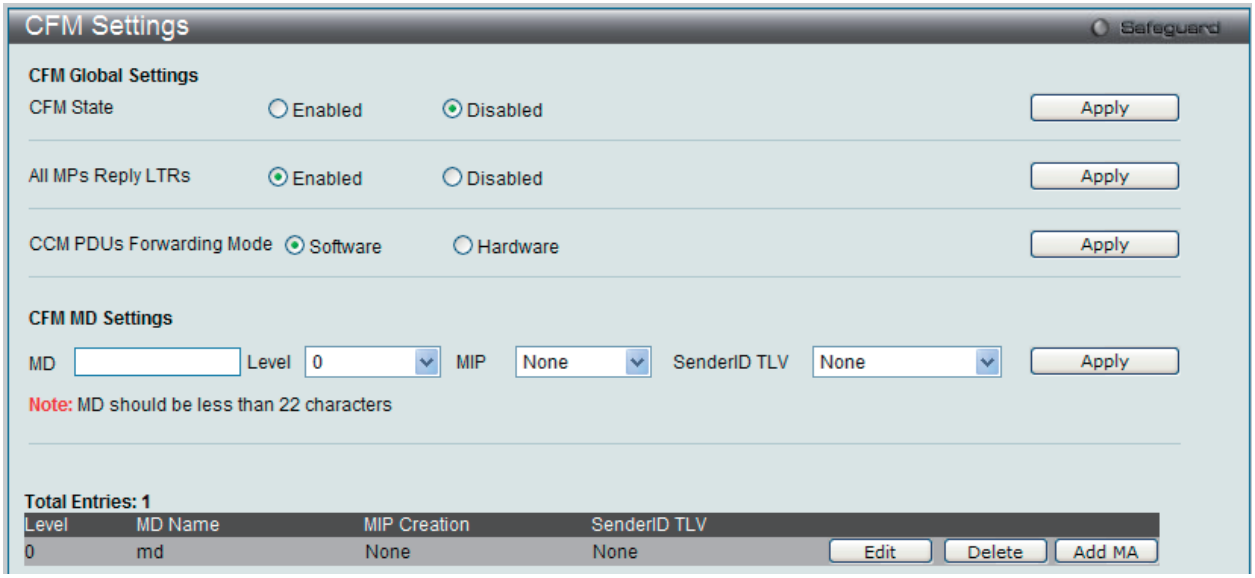


図 15-2　CFM Settings 画面

以下の項目を設定できます。

項目	説明
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。
CCM PDUs Forwarding	使用する CCM PDU フォワーディングモードを選択します。「Software」または「Hardware」オプションを選択します。
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。
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。
Sender ID 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、以下の画面を表示します。

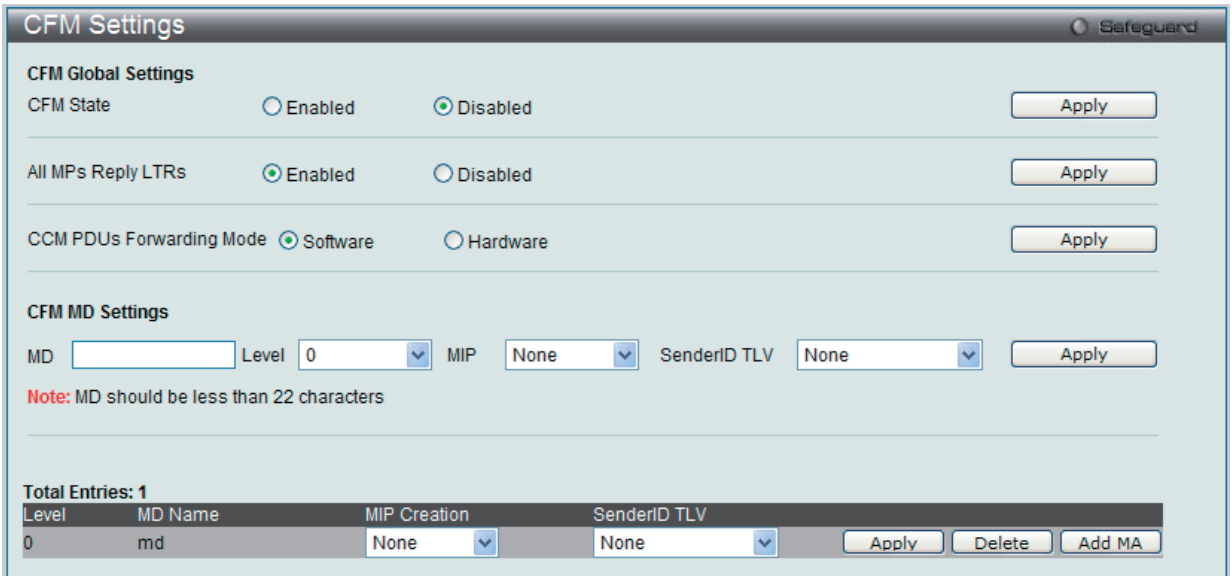


図 15-3　CFM Settings 画面 - Edit

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。

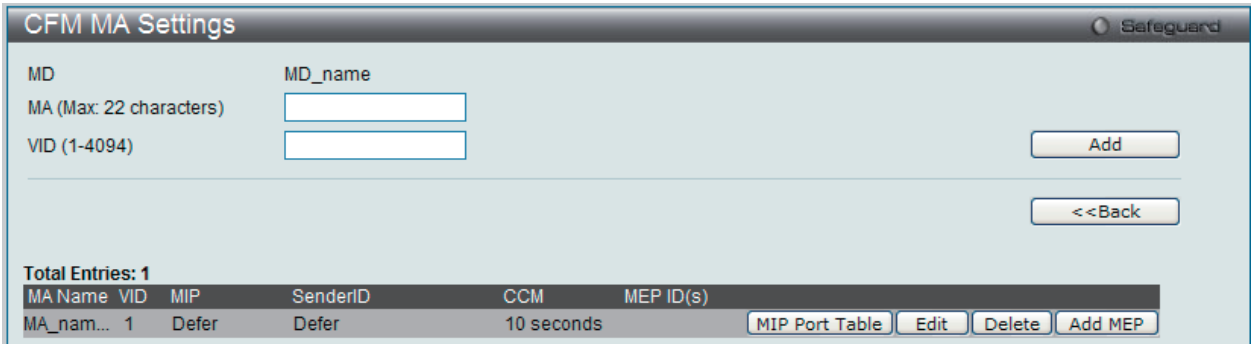


図 15-4　CFM MA Settings 画面

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。
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。

エントリの編集
1. 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。

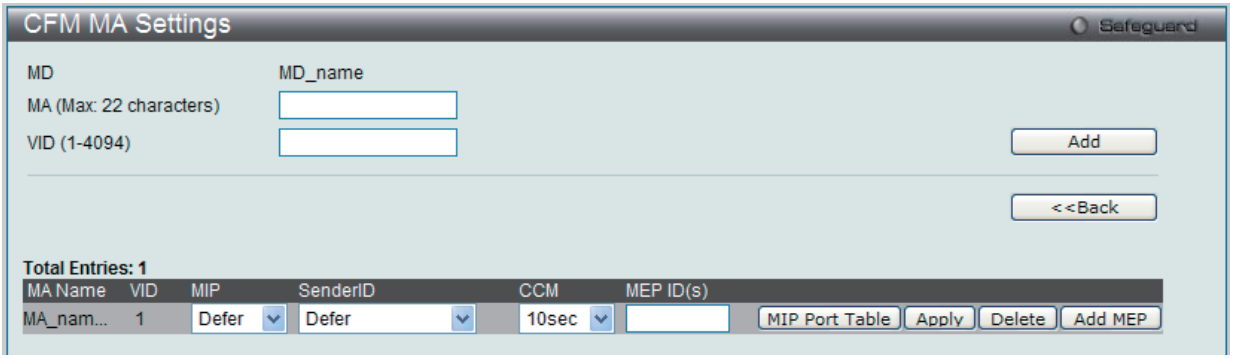


図 15-5　CFM MA Settings 画面 - Edit

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。
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。
MIP	MIP の作成を制御します。 • None - MIP を作成しません。（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。（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。

項目	説明
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）推奨されません。テストの目的のために使用します。 • 100ms - 100（ミリ秒）推奨されません。テストの目的のために使用します。 • 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。 • Add - MEP ID を追加します。 • Delete - MEP ID を削除します。 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 MA」ボタンをクリック後、「Add MEP」ボタンをクリックし、以下の画面を表示します。

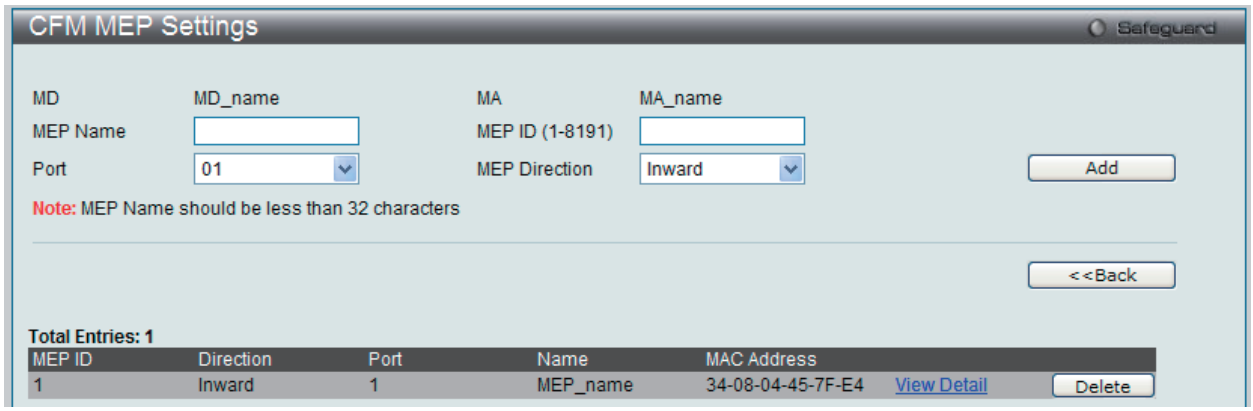


図 15-6　CFM MEP Settings 画面

以下の項目を設定できます。

項目	説明
MEP Name	MEP 名。デバイスに設定されたすべての MEP 内で固有です。
MEP ID	MEP ID。MA の MEP ID リストで設定される必要があります。
Port	ポート番号。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。
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。

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「Add MA」ボタンをクリック後、「MIP Port Table」ボタンをクリックします。

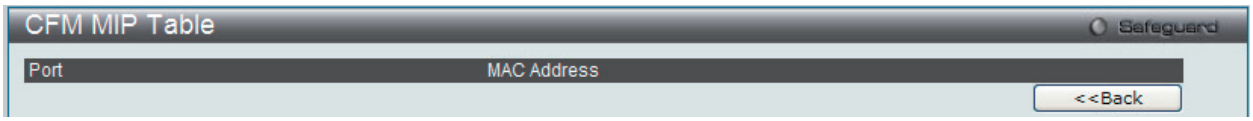


図 15-7　CFM MIP Table 画面

MEP エントリに関する詳細情報の参照

OAM > CFM > CFM Settings 画面で「Add MA」ボタンをクリック後、「Add MEP」ボタンをクリックします。さらに、「View Detail」ボタンをクリックし、以下の画面を表示します。

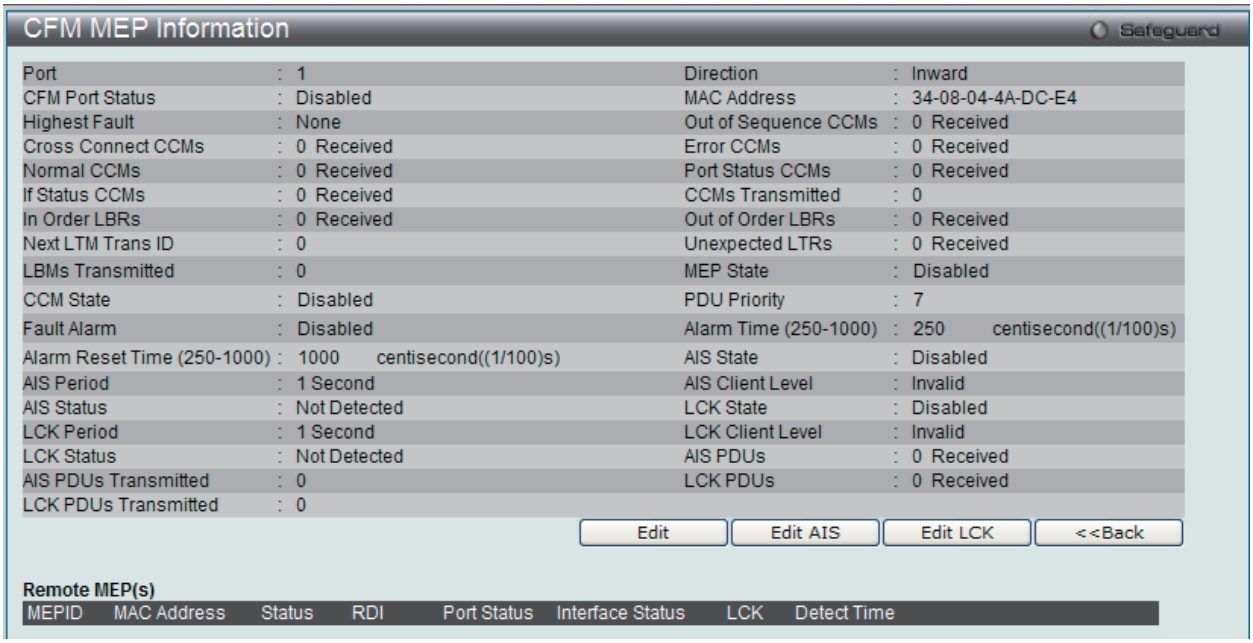


図 15-8　CFM MEP Information 画面

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。

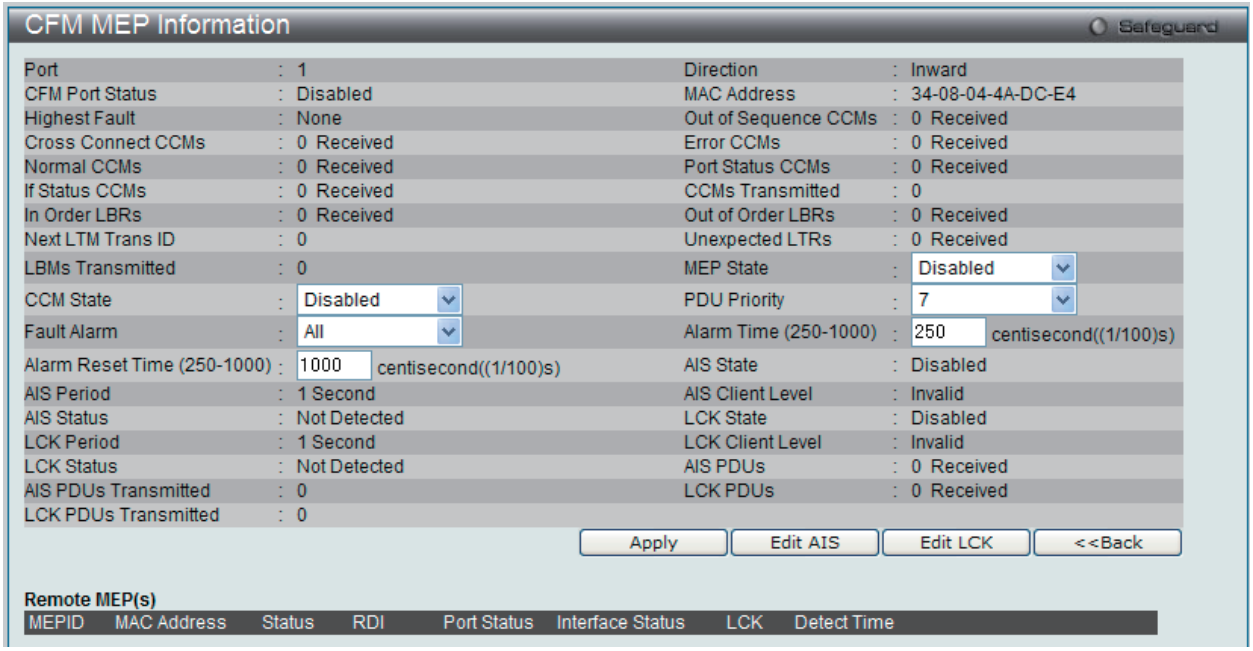


図 15-9　CFM MEP Information 画面 - Edit

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。
Remote MEP (s) テーブル	リモート MEP の読み出し用情報が表示されます。情報は、リモートの MEPID、MAC アドレス、ステータス、RDI、ポートステータス、インタフェースステータス、最後の CCM シリアル番号、送信元のシャーシ ID、送信元の管理アドレス、および検出時間を含みます。

AIS の編集

「Edit AIS」ボタンをクリックすると、以下の画面が表示されます。

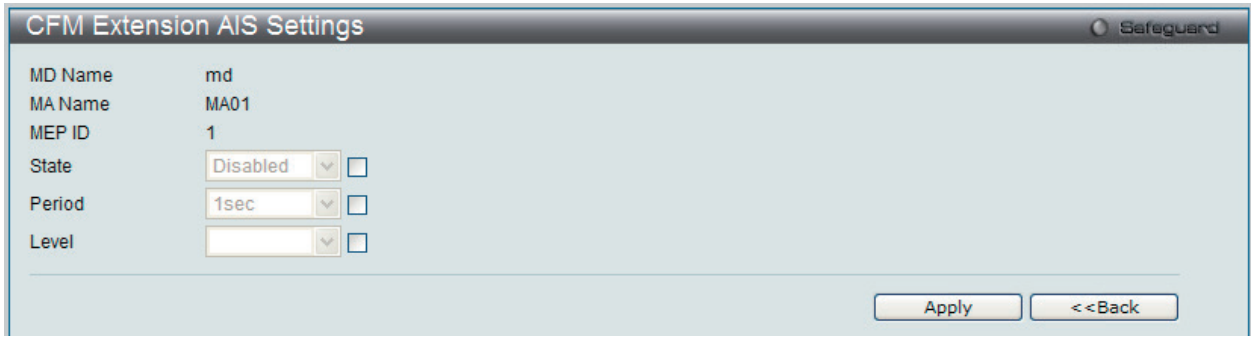


図 15-10 CFM Extension AIS (Edit) 画面

以下の項目を設定できます。

項目	説明
State	チェックし、プルダウンメニューを使用して、AIS 機能を「Enabled」(有効)/「Disabled」(無効) にします。
Period	チェックし、プルダウンメニューを使用して、AIS PDU 送信間隔を選択します。
Level	チェックし、プルダウンメニューを使用して、MEP が AIS PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。オプションを 0-7 からを選択します。

「Apply」ボタンをクリックして行った変更を適用します。

「<<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。

LCK の編集

「Edit LCK」ボタンをクリックすると、以下の画面が表示されます。

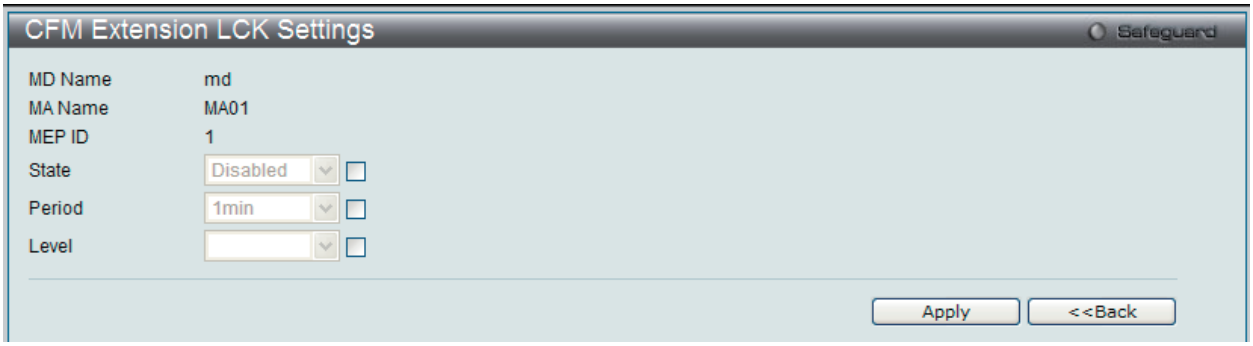


図 15-11　CFM Extension LCK Settings (Edit) 画面

以下の項目を設定できます。

項目	説明
State	チェックし、プルダウンメニューを使用して、LCK 機能を「Enabled」(有効)/「Disabled」(無効) にします。
Period	チェックし、プルダウンメニューを使用して、LCK PDU 送信間隔を選択します。
Level	チェックし、プルダウンメニューを使用して、MEP が LCK PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。オプションを 0-7 からを選択します。

「Apply」ボタンをクリックして行った変更を適用します。

「<<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）

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。

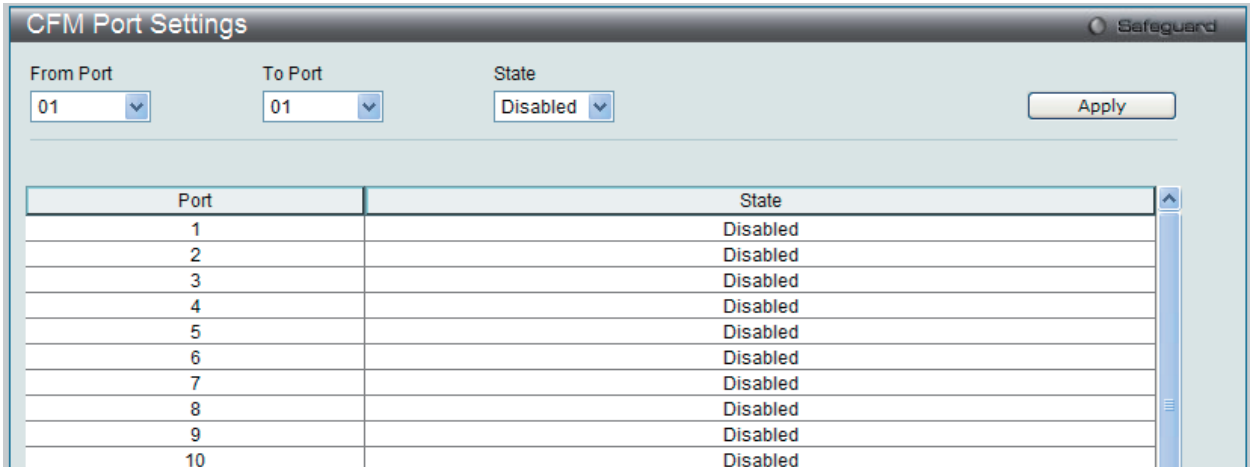


図 15-12　CFM Port Settings 画面

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 データベースエントリを参照します。

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。

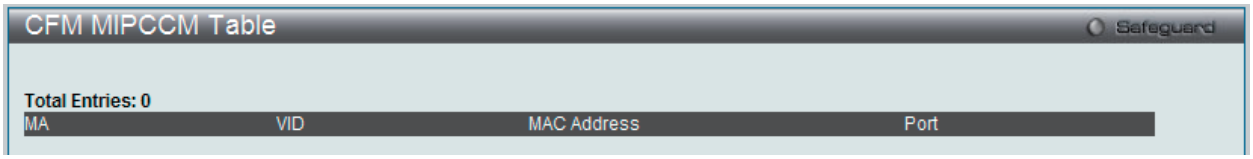


図 15-13　CFM MIPCCM Table 画面

CFM Loopback Settings（CFM ループバック設定）

CFM ループバックを設定します。

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。

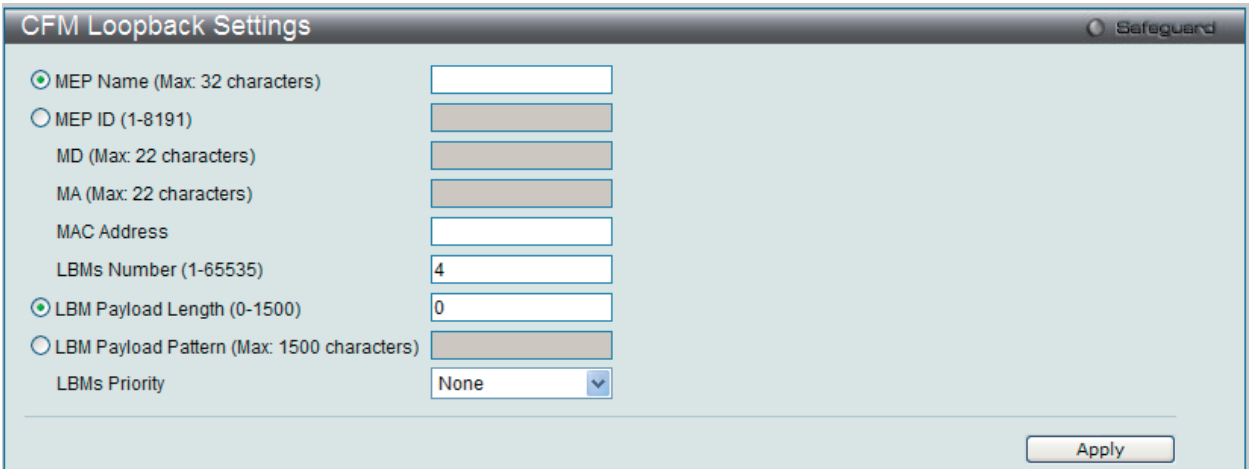


図 15-14 CFM Loopback Settings 画面

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 (Max:22 characters)	メンテナンスドメインの名称を入力します。
MA (Max:22 characters)	メンテナンスアソシエーションの名称を入力します。
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 ～ 65525 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を設定します。

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。

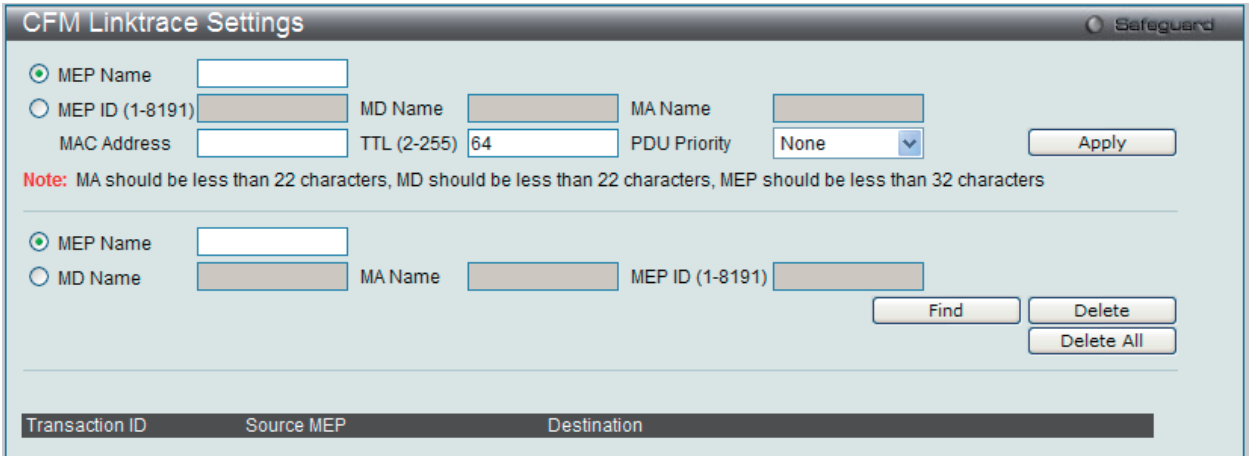


図 15-15　CFM Linktrace Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
MEP Name	MEP 名を入力します。
MEP ID (1-8191)	MEP ID を入力します。
MD Name	メンテナンスドメインの名称を入力します。
MA Name	メンテナンスアソシエーションの名称を入力します。
MAC Address	宛先 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。

「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」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 パケットの送信 / 受信カウンタを参照します。

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。

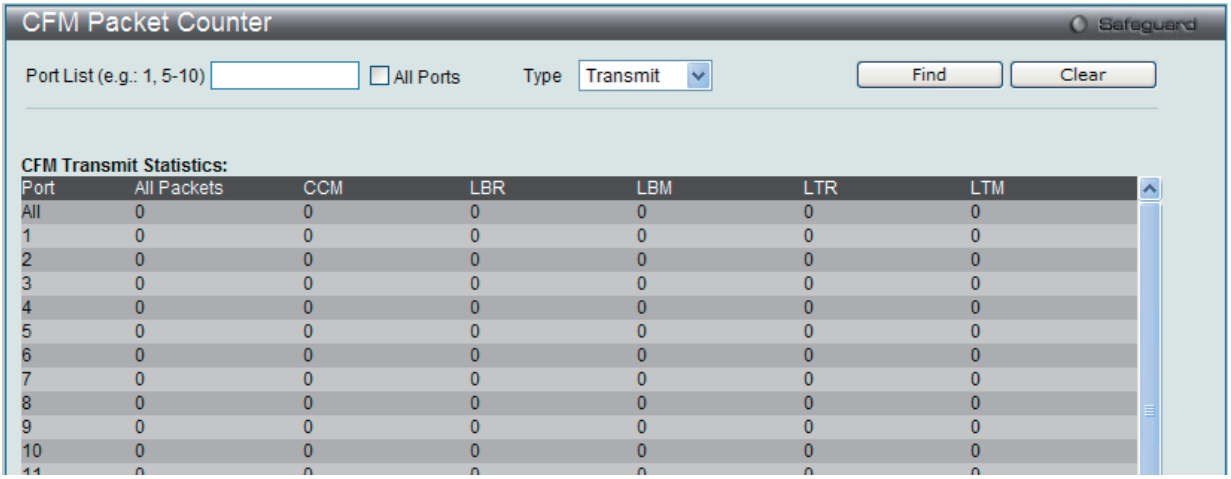


図 15-16　CFM Packet Counter 画面

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。ポートを指定しない場合、すべてのポートの情報を表示します。
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 CFM 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）

スイッチの MEP によって検出された障害状態を表示します。

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。

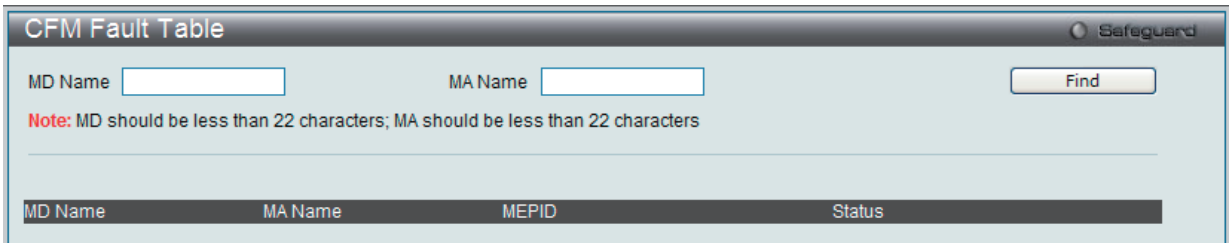


図 15-17　CFM Fault MEP 画面

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入力します。
MA Name	表示するメンテナンスアソシエーション名を入力します。

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）

スイッチの CFM ポート MP リストを参照します。

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。

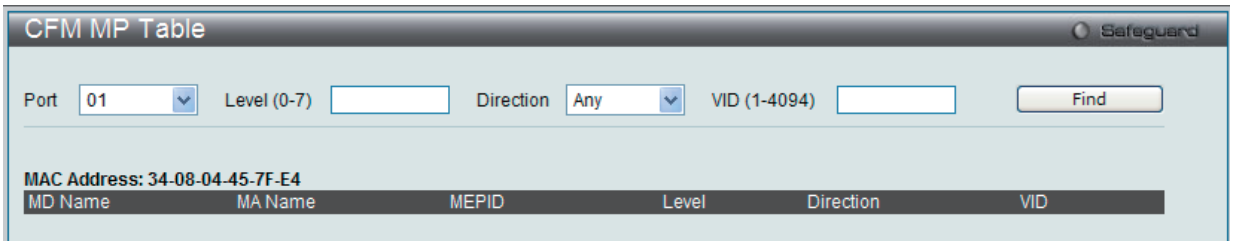


図 15-18　CFM MP Table 画面

画面には以下の項目があります。

項目	説明
Port	以下の MAC アドレスに対応するポートを指定します。
Level (0-7)	参照するエントリの MD レベルを指定します。
Direction	MEP の方向を指定します。 • Inward - 内向き MEP を示します。 • Outward - 外向き MEP を示します。
VLAN ID	参照するエントリの VLAN 識別子を指定します。

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。Active モードでは、ポートは、OAM 発見を開始してリモートループバックの開始 / 終了を行うことができます。OAM でポートが有効であると、OAM モードへのどんな変更も、OAM 発見の再起動が起こります。

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。

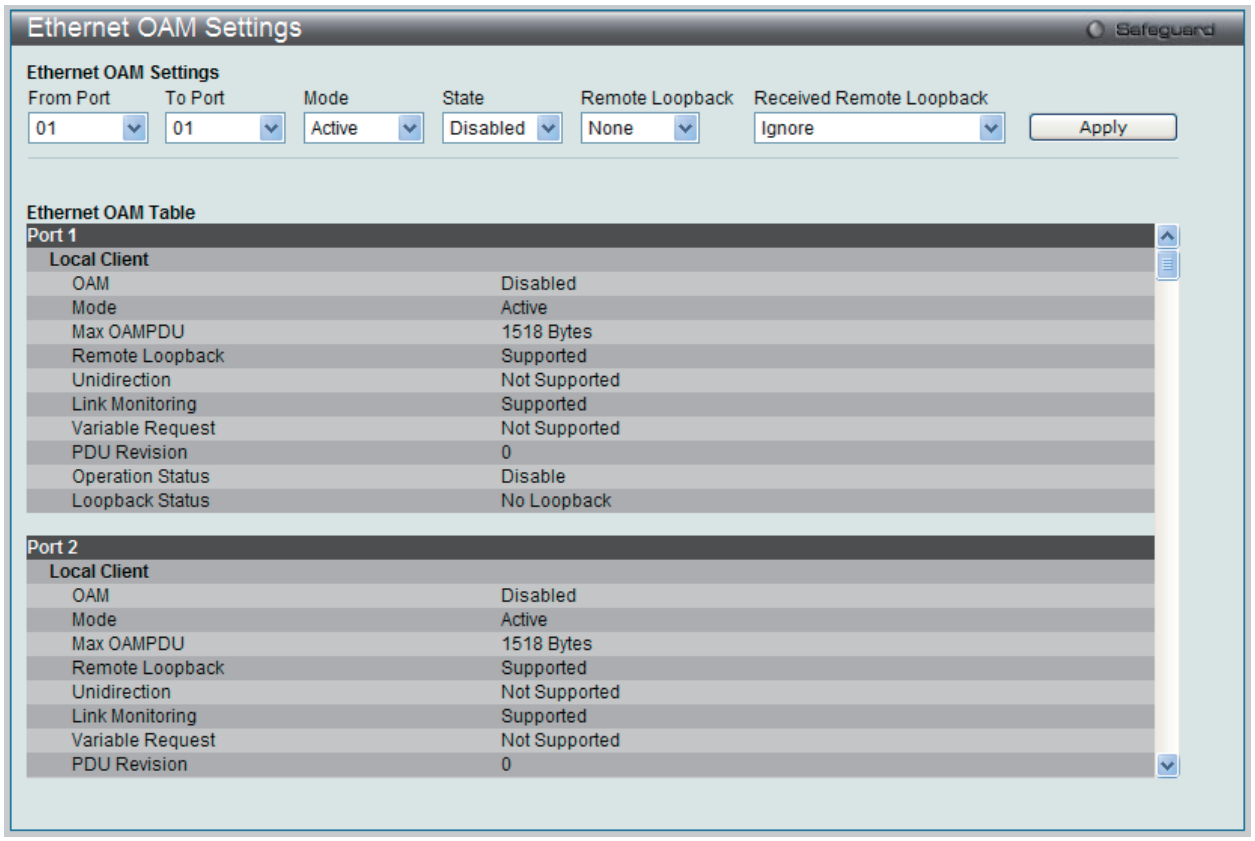


図 15-19 Ethernet OAM Settings 画面

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	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 - 処理します。 • Ignore - 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。

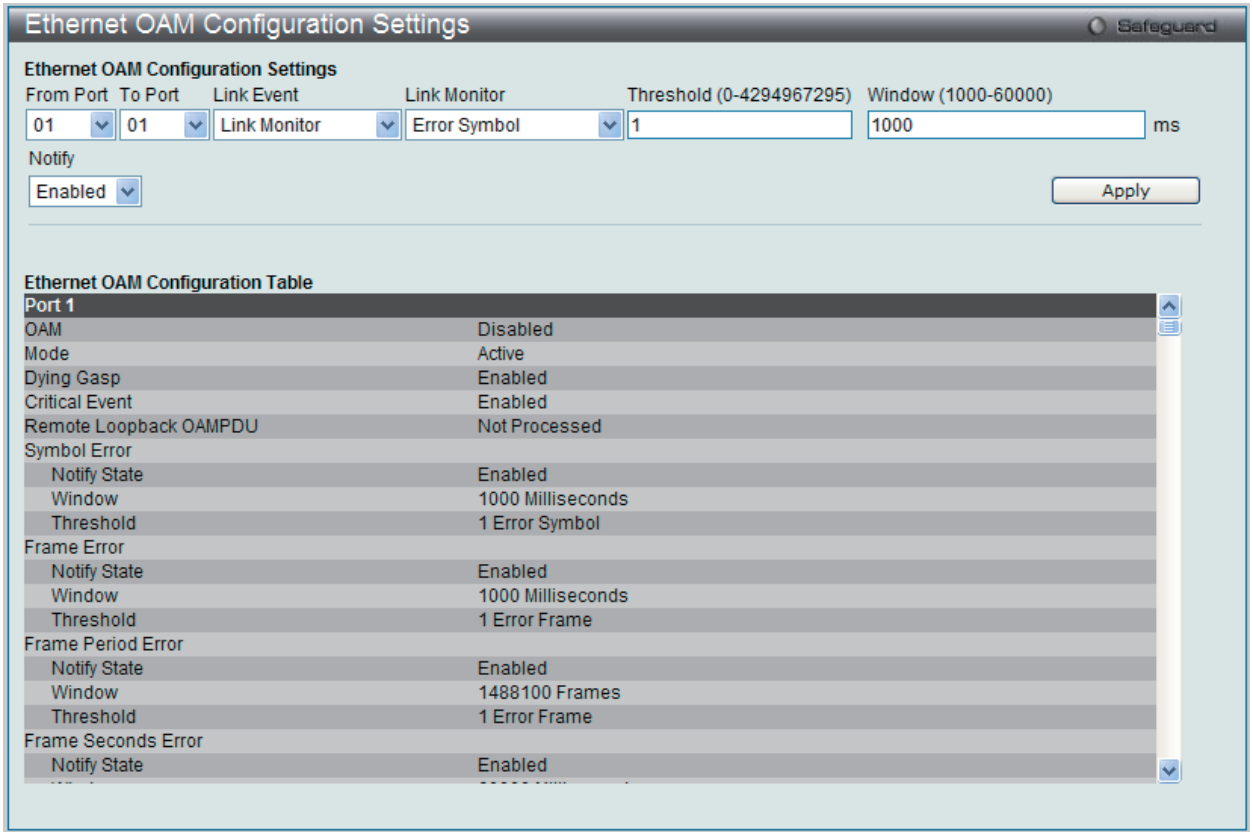


図 15-20　Ethernet OAM Configuration Settings 画面

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。 Error Symbol、Error Frame、Error Frame Period、Error Frame Seconds から選択します。
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 (0-4294967295)	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。しきい値の初期値は 1 シンボルエラーです。しきい値は 0 - 4294967295 の範囲です。初期値は 1 です。
Window (1000-6000)	エラーシンボルとエラーフレームの有効範囲は、1000 - 60000 ms（ミリ秒）で、初期値は 1000 ms です。エラーフレーム周期の有効範囲は、14881 - 89286000 で、初期値はファーストイーサネットポートに対して 148810 です。エラーフレーム秒数の有効範囲は、10000 - 900000 で、初期値は 60000 です。
Notify	イベント通知を有効または無効にします。初期値は有効です。

「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。本スイッチは 1000 個のイベントログをバッファに保存できます。イベントログは Syslog とは異なるもので、Syslog より詳しい情報を提供します。各 OAM イベントは OAM イベントログとシステムログに両方に記録されます。

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。

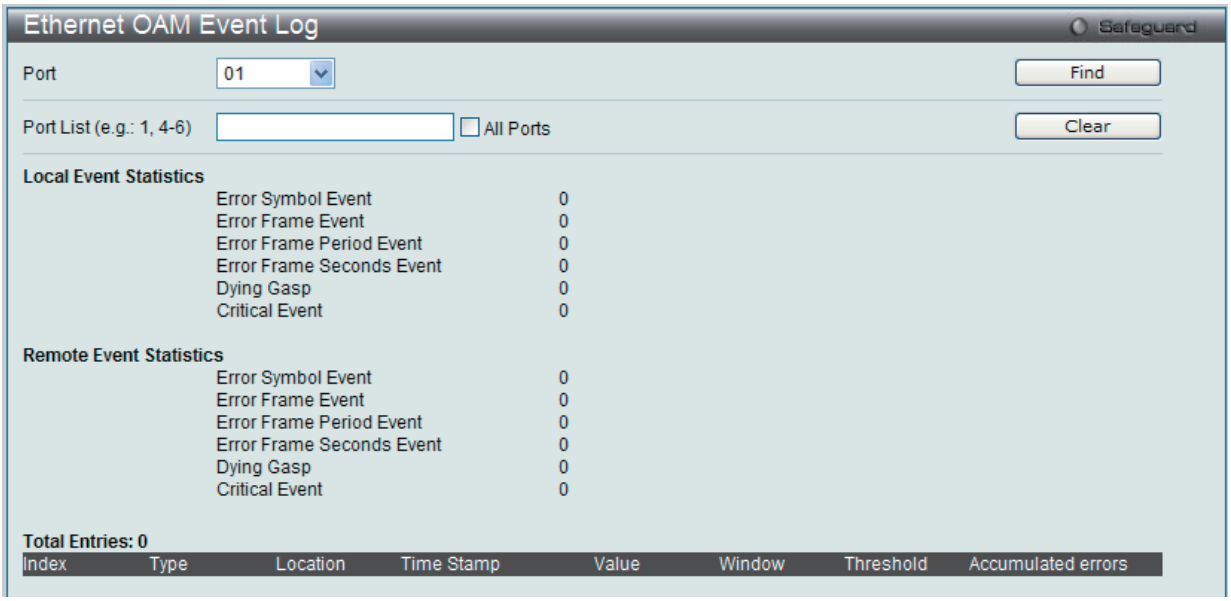


図 15-21　Ethernet OAM Event Log 画面

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。また、「All Port」を選択するとスイッチのすべてのポートの情報を表示します。
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。

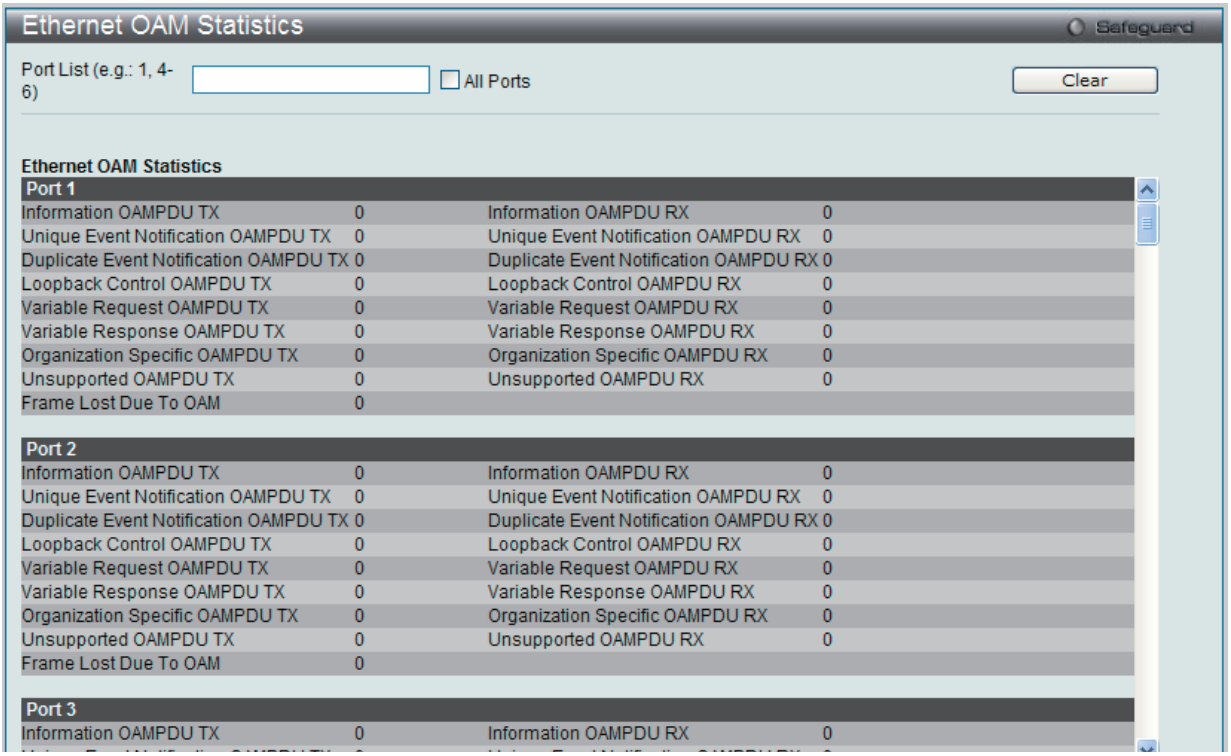


図 15-22　Ethernet OAM Statistics 画面

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。また、「All Port」を選択するとスイッチのすべてのポートの情報をクリアします。

DULD Settings（単方向リンク検出設定）

スイッチは D-Link DULD（Unidirectional Link : 単方向リンク検出）モジュール機能を搭載しています。この単方向リンク検出は、PHY が単方向 OAM 操作をサポートしないイーサネットスイッチ用に単方向リンクの検出に使用されるメカニズムを提供します。本機能は OAM に基づいて確立されるため、検出の開始前に、OAM を有効にする必要があります。

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。

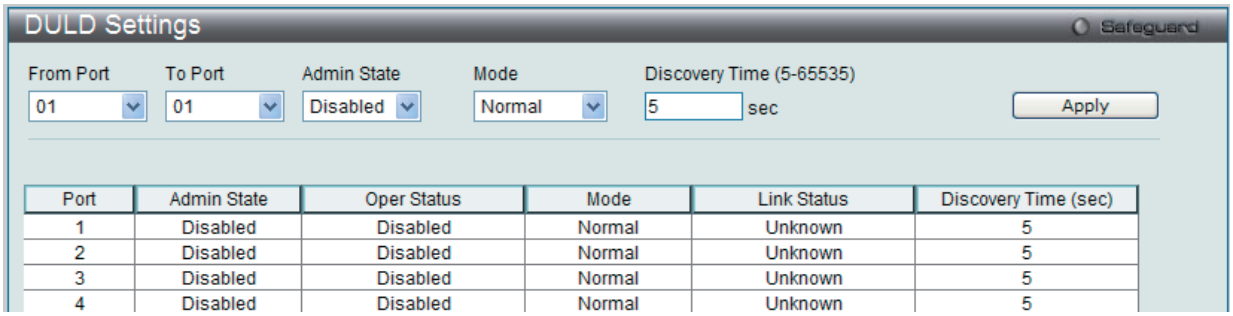


図 15-23　DULD Settings 画面

以下の項目を設定できます。

項目	説明
Unit	設定するユニットを選択します。
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を使用して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 - 単方向のリンクを検出すると、ポートを無効にしてイベントをログに出力します。 • Normal - 単方向のリンクを検出すると、イベントをログに出力します。
Discovery Time (5-65535)	指定ポートの 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。

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 ケーブルを検査、テスト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。

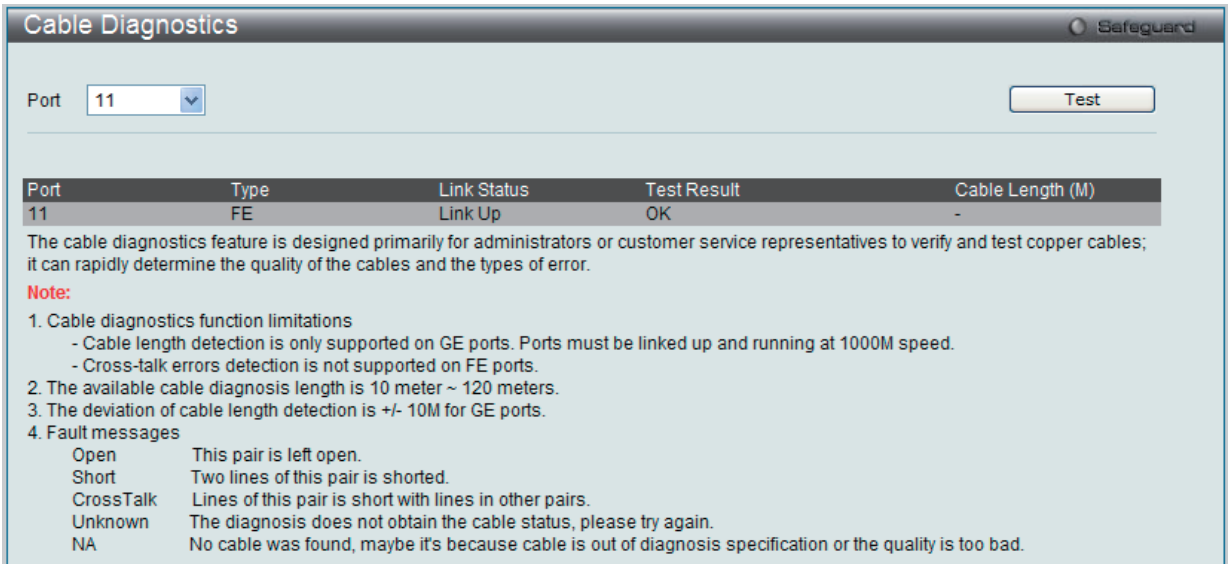


図 15-24 Cable Diagnostics 画面

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。

エラーメッセージは以下の通りです。

項目	説明
Open	このペアはオープン状態です。
Short	このペアの 2 つのラインがショートしています。
CrossTalk	このペアのラインは他の組がライン共にショートしています。
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。
NA	ケーブルが見つかりません。ケーブルが診断の仕様外であるか品質が非常に悪い可能性があります。

注意 ケーブル診断機能の制限

ケーブル長検出は GE ポートでのみサポートされています。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ていません。

注意 有効なケーブル診断の長さは 10-120m です。

注意 ケーブル長検出の誤差は GE ポートで +/-10M です。

第 16 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 の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）	444
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）、Packet Size（パケットサイズ）、VLAN Counter Statistics（VLAN カウンタの設定）、Historical Counter & Utilization（ヒストリカウンタと利用率）	446
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）、RSPAN Settings（RSPAN 設定）	458
sFlow（sFlow 設定）	sFlow 機能の設定を行います。次のメニューがあります。 sFlow Global Settings（sFlow グローバル設定）、sFlow Analyzer Server Settings（sFlow アナライザ設定）、sFlow Flow Sampler Settings（sFlow サンプラ設定）、sFlow Counter Poller Settings（sFlow カウンタポーラ設定）	460
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。	463
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。	464
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。	465

注意　リアルタイムのためのモニタリングエンジンでは Java ランタイム v1.6 以上のプラットフォームが必要です。http://www.java.com/getjava からソフトウェアをダウンロードしてください。

Utilization（使用率）

CPU Utilization（CPU 使用率）

「CPU Utilization」画面では、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。

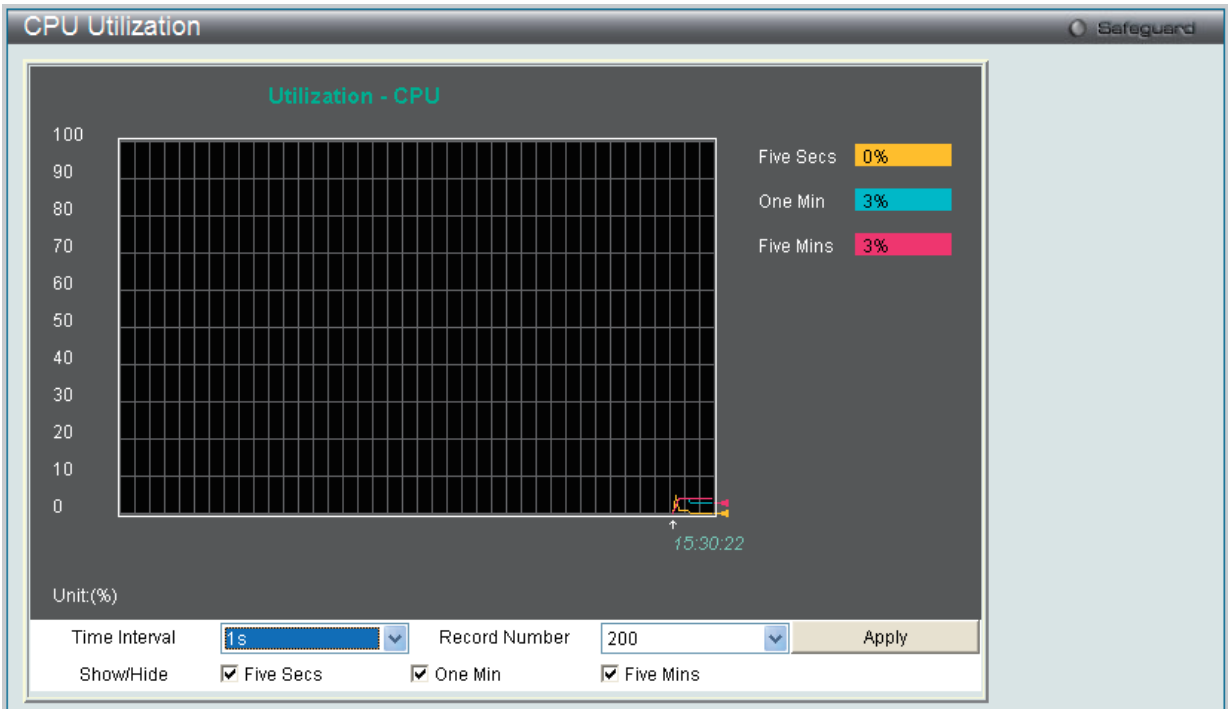


図 16-1　CPU Utilization 画面

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。

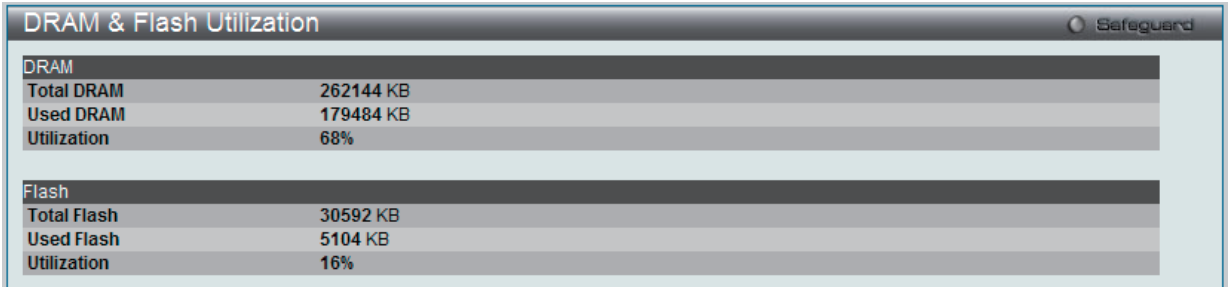


図 16-2　DRAM & Flash Utilization 画面

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。

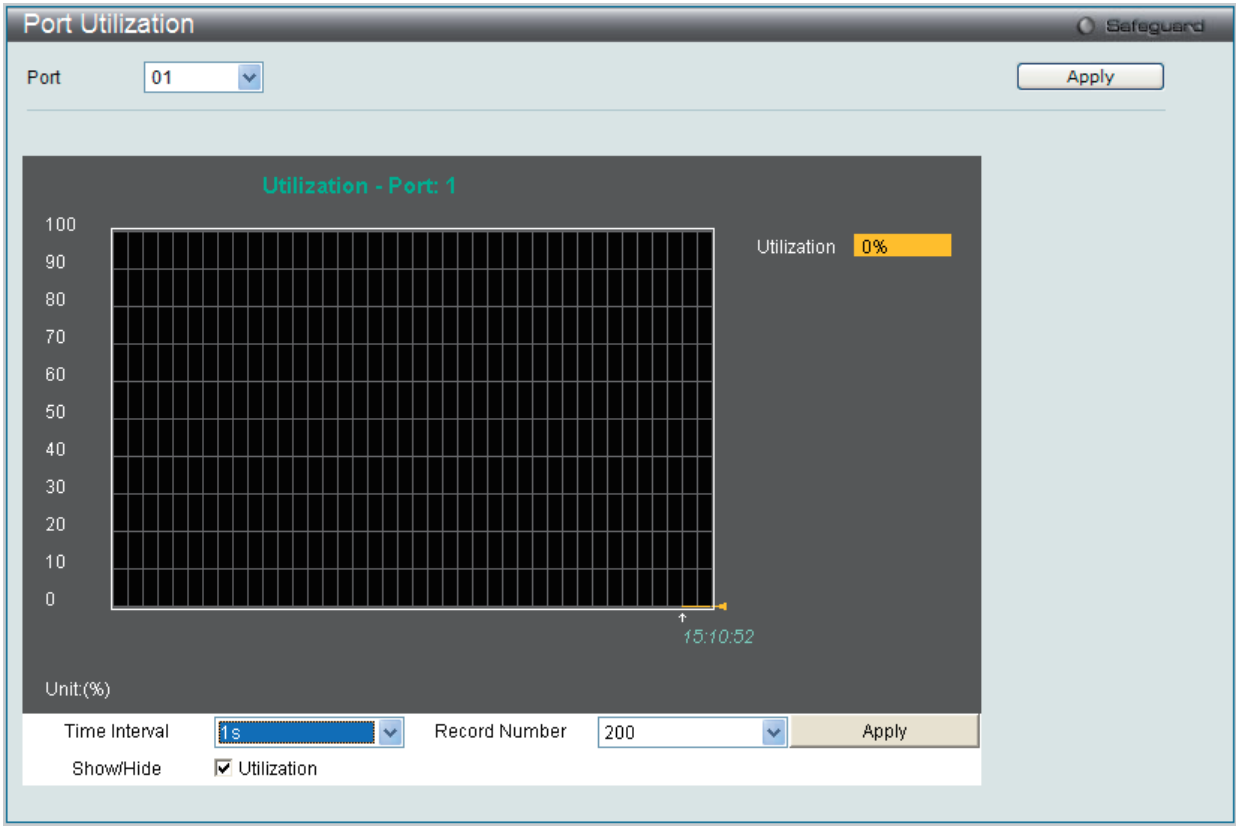


図 16-3　Port Utilization 画面

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。

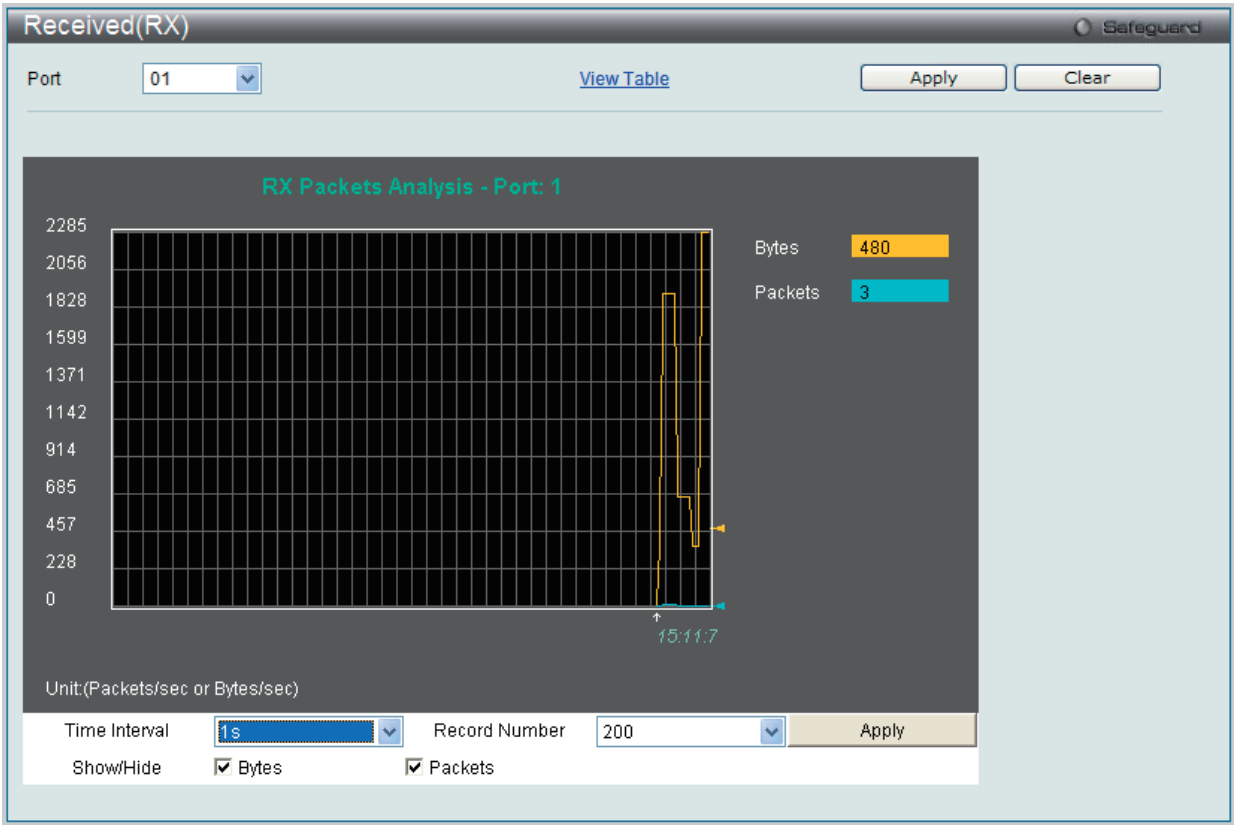


図 16-4　Received（RX）画面（バイトとパケットの折れ線グラフ）

「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 16-5　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）
Packets	ポートに受信したパケット数
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。

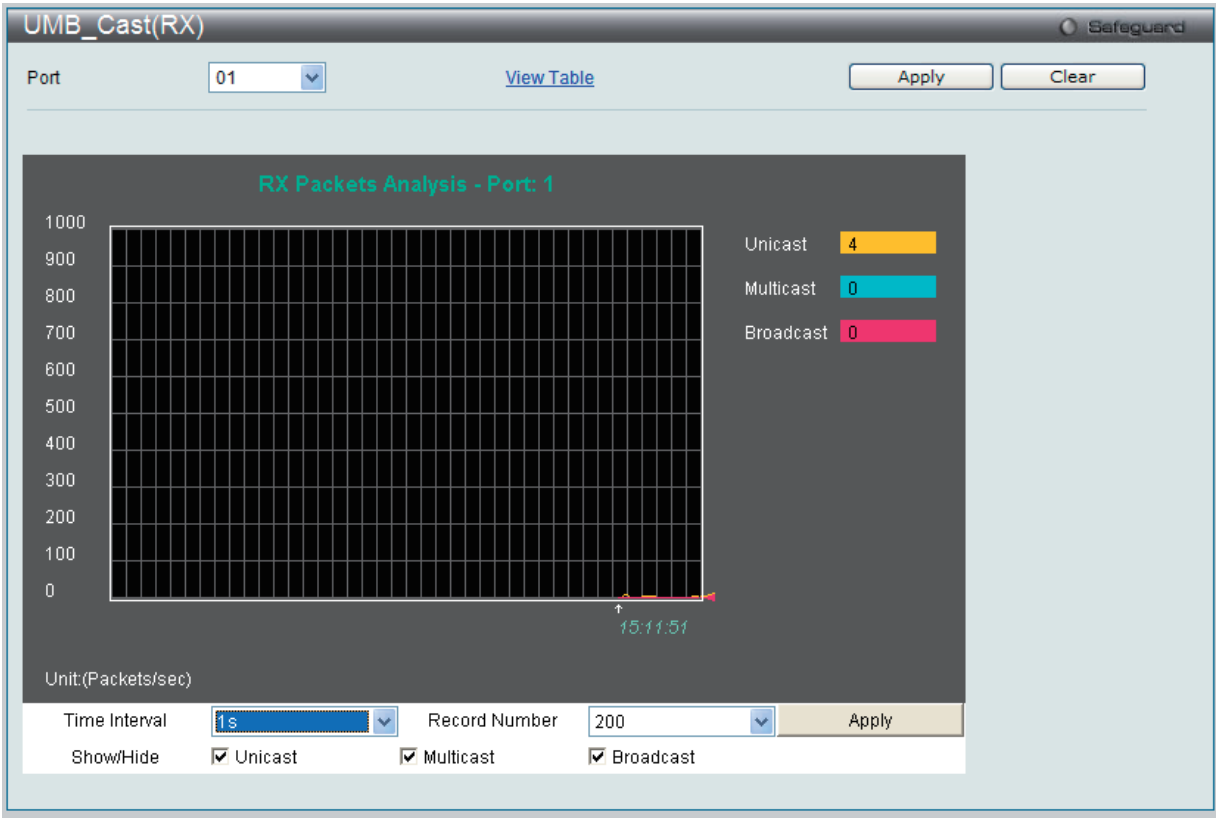


図 16-6　UMB_Cast（RX）画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の折れ線グラフ）

「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。

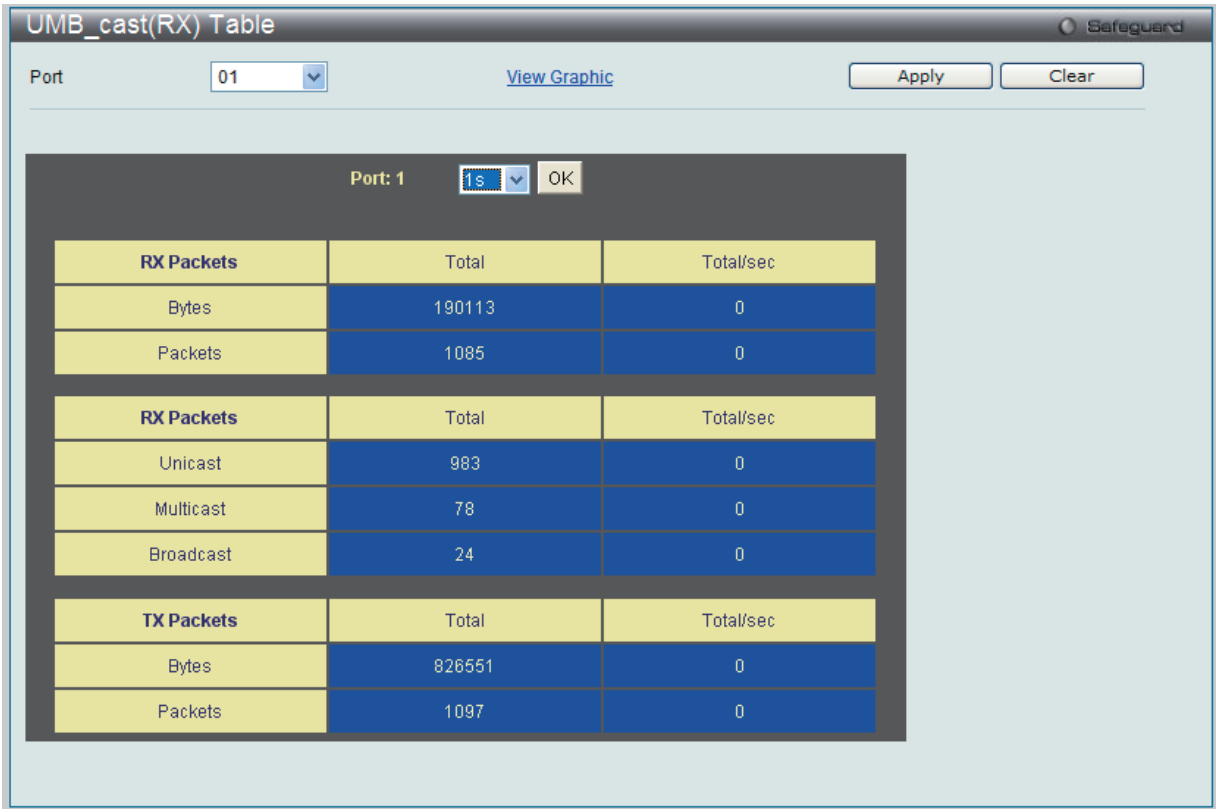


図 16-7　UMB_Cast（RX）Table 画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の表形式表示）

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。

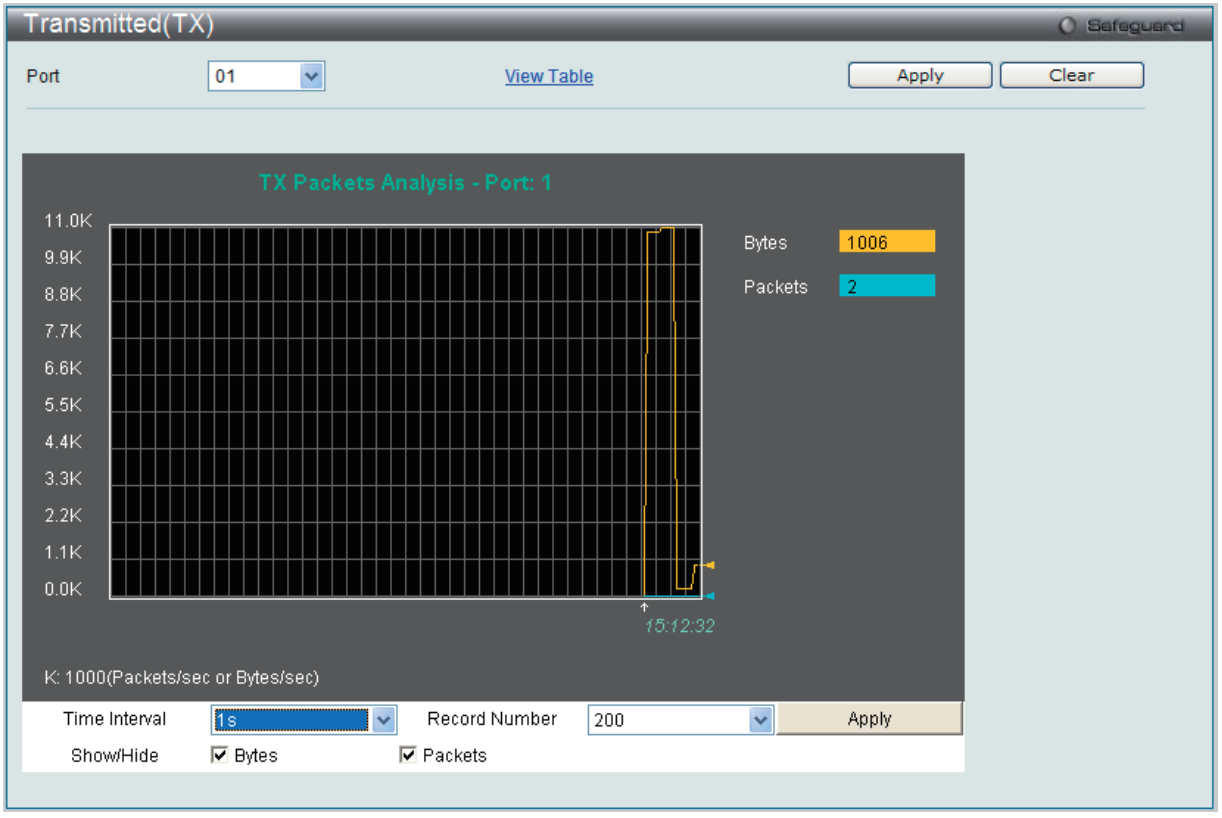


図 16-8　Transmitted（TX）画面（パケットサイズ、パケット数の折れ線グラフ表示）

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 16-9　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。

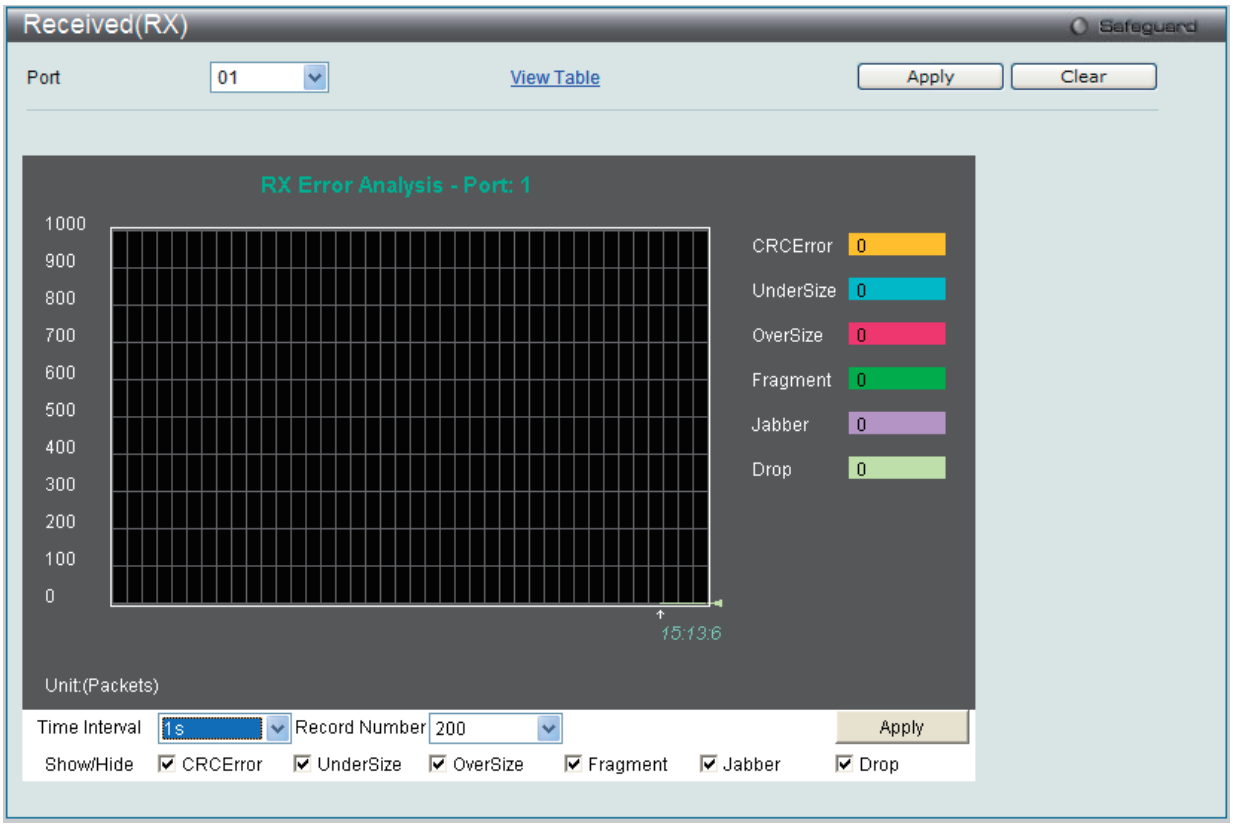


図 16-10　Received（RX）- Error 画面（折れ線グラフ形式）

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 11-14　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 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。

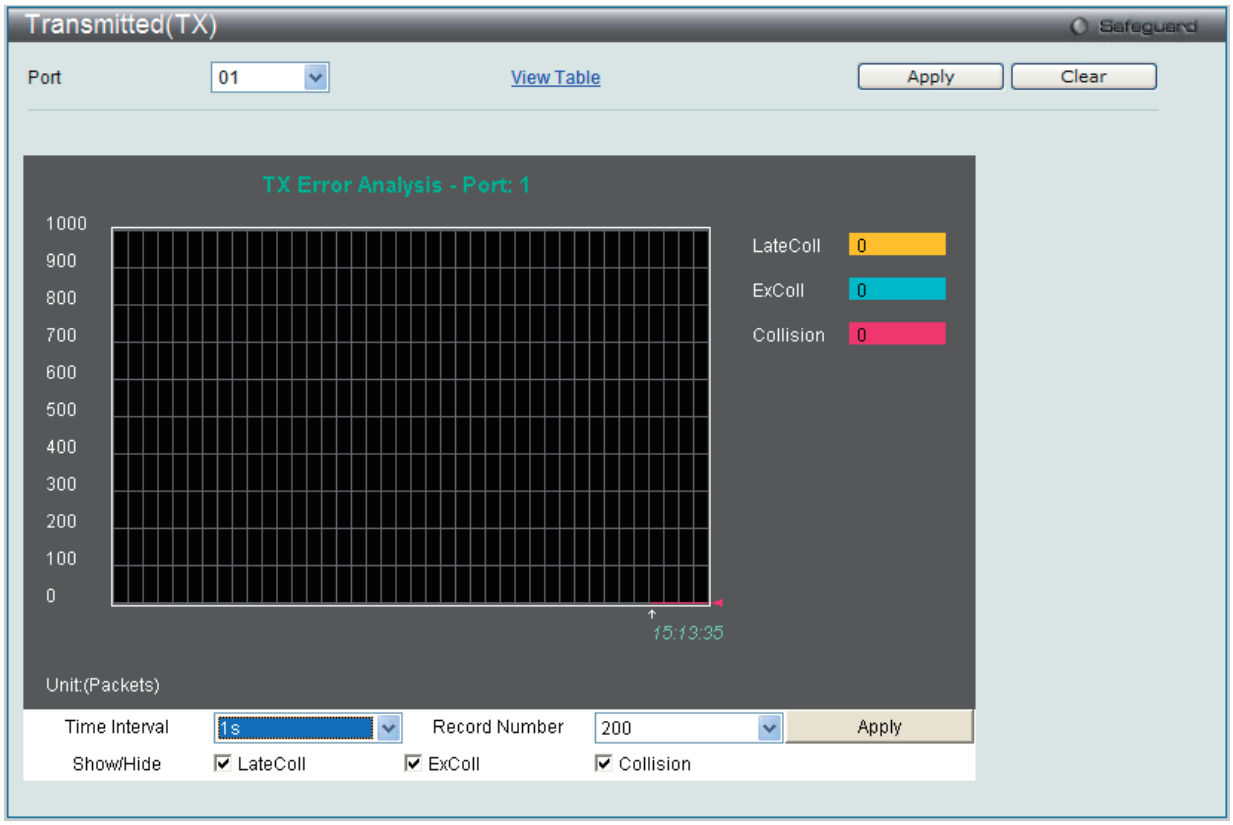


図 11-15　Transmitted（TX）- Error 画面（折れ線グラフ形式）

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。

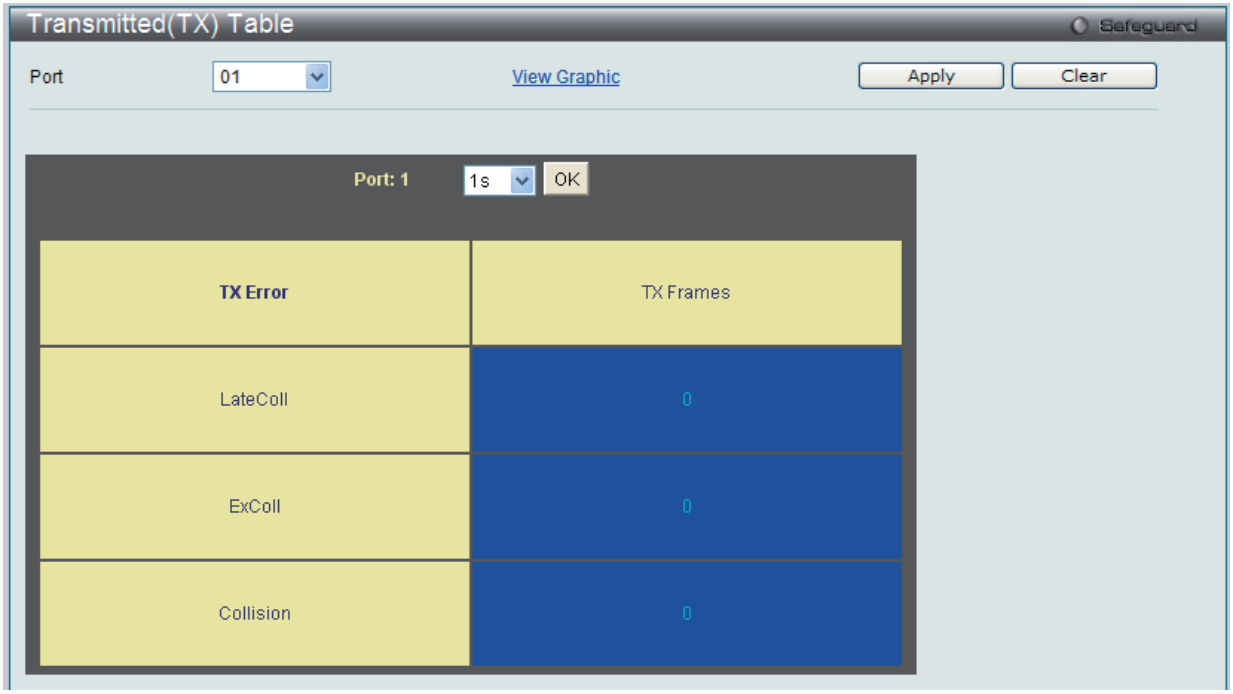


図 16-11　Transmitted（TX）Table - Error 画面（表形式）

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 > 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。

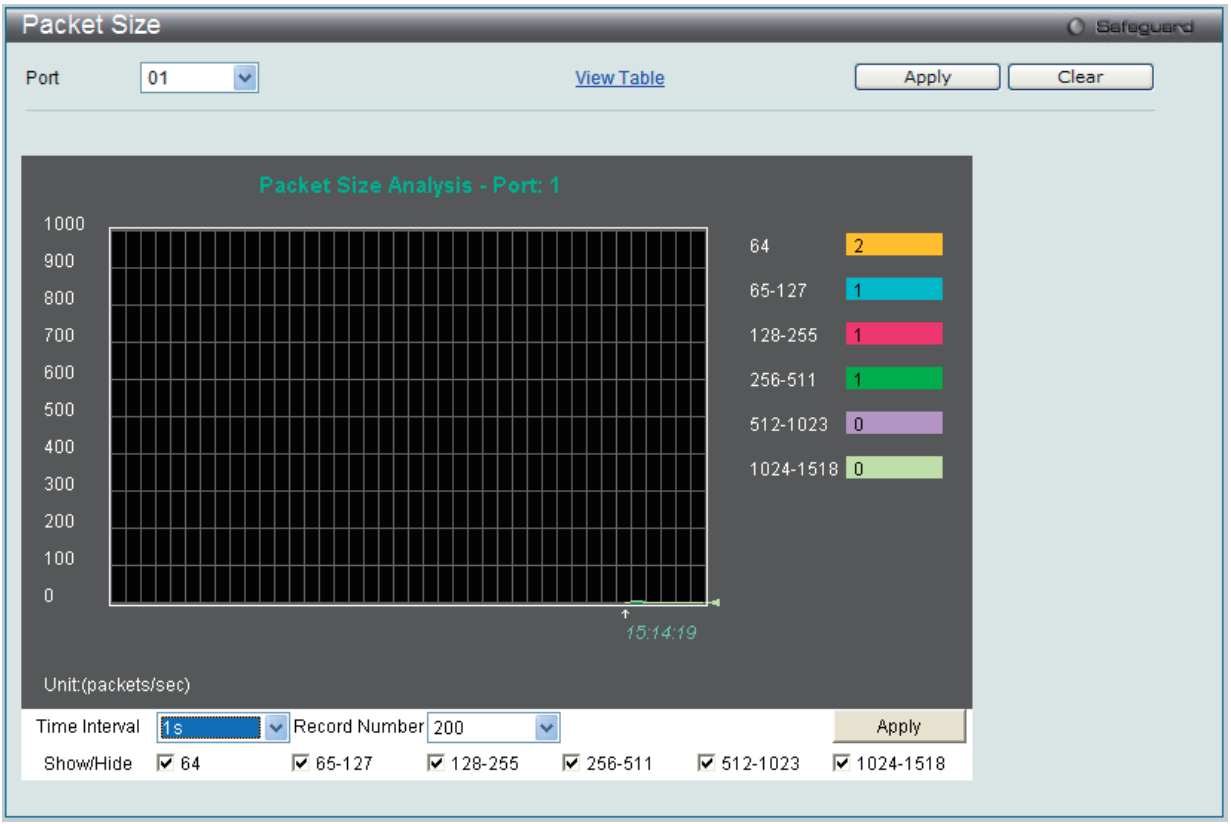


図 16-12　Packet Size 画面（折れ線グラフ）

「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 16-13　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）。
Show/ Hide	64、65-127、128-255、256-511、512-1023、または 1024-1518 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。

VLAN Counter Statistics（VLAN カウンタの設定）

VLAN カウンタ統計情報を参照します。

Monitoring > Statistics > VLAN Counter 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。

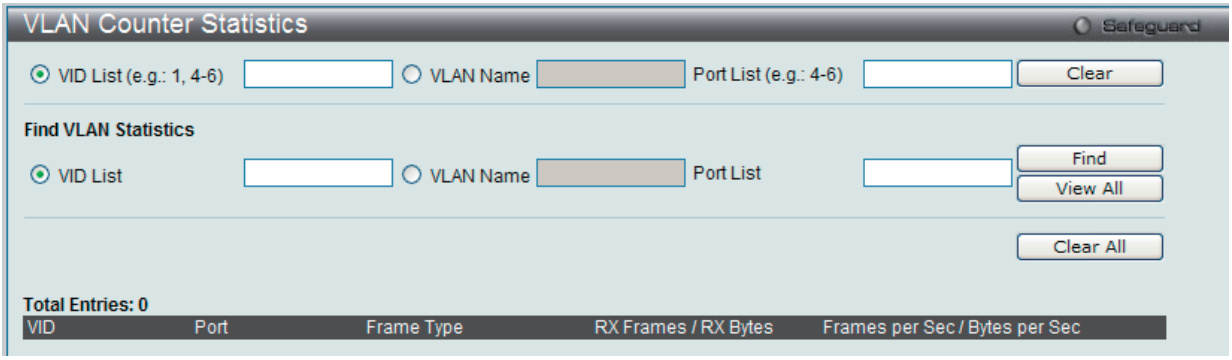


図 16-14　VLAN Counter Statistics 画面

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
VID List	参照する VID リストを入力します。
VLAN Name	参照する VLAN 名を入力します。
Port List	参照する適切なポートを入力します。
Clear	本欄に入力したすべてのエントリをクリアします。
Find	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	すべての定義済みエントリを表示します。
Clear All	テーブルに表示されたすべてのエントリを削除します。

Historical Counter & Utilization（ヒストリカウンタと利用率）

Historical Counter（ヒストリカウンタ）

ヒストリカウンタに関する情報を参照します。

Monitoring > Statistics > Historical Counter & Utilization > Historical 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。

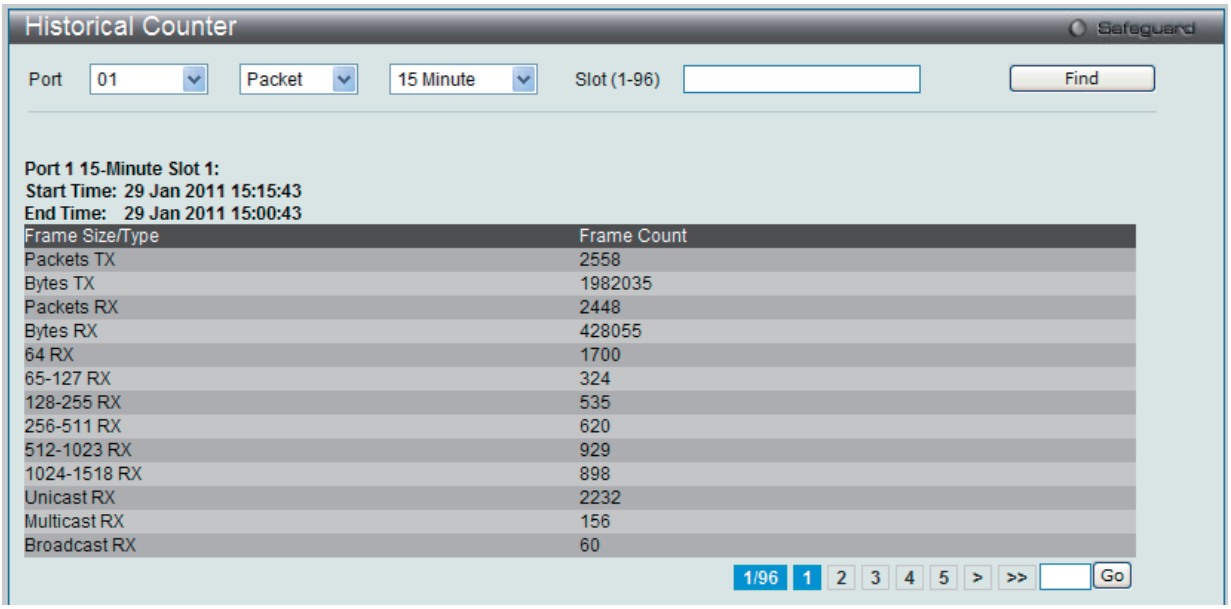


図 16-15　Historical Counter 画面

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	参照する適切なポートを選択します。
Packet	送受信したパケットに基づいてフレームカウントを表示します。
Error	送受信したパケットエラーに基づいてフレームカウントを表示します。
Time	タイムスロットを選択します。この指定した経過時間に基づいた量の情報が表示されます。15 Minute（分）または 1 Day（1 日）を選択します。
Slot	スロット番号を入力します。

「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。
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。

Historical Utilization（利用率のヒストリ）

利用のヒストリに関する情報を参照します。

Monitoring > Statistics > Historical Counter & Utilization > Historical 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。

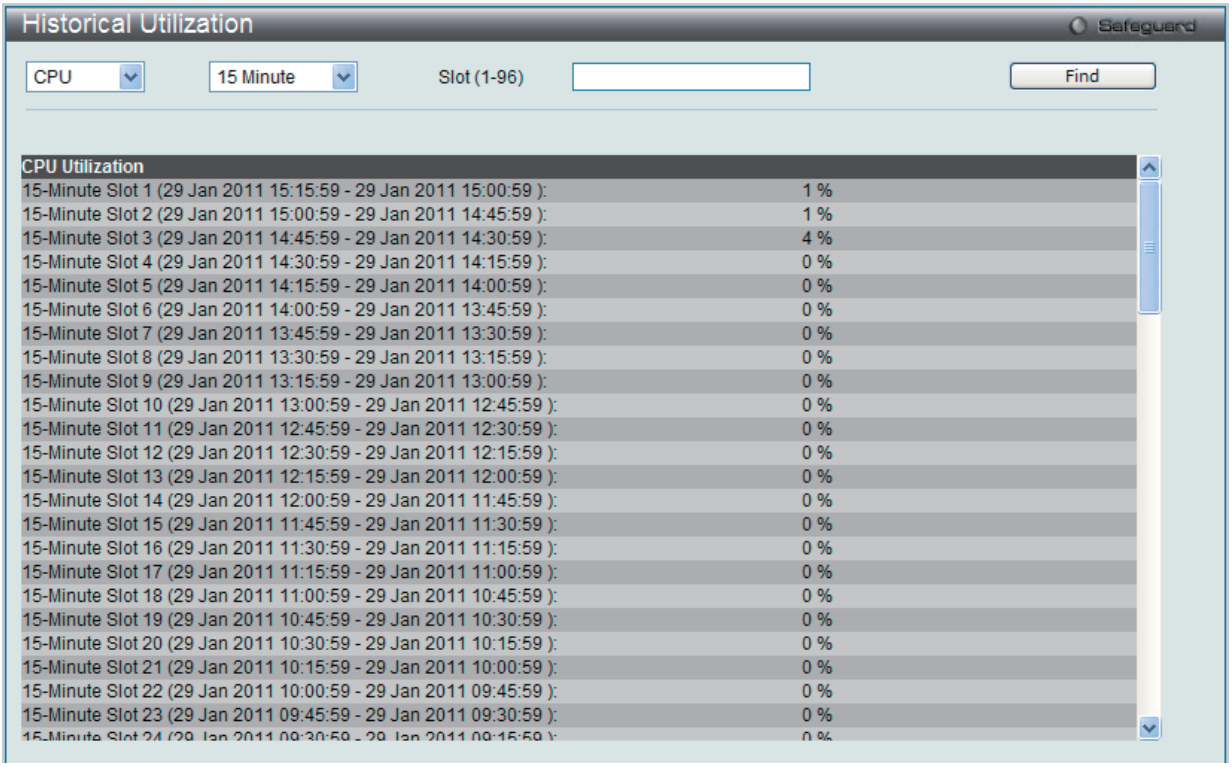


図 16-16　Historical Utilization (CPU) 画面

「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。

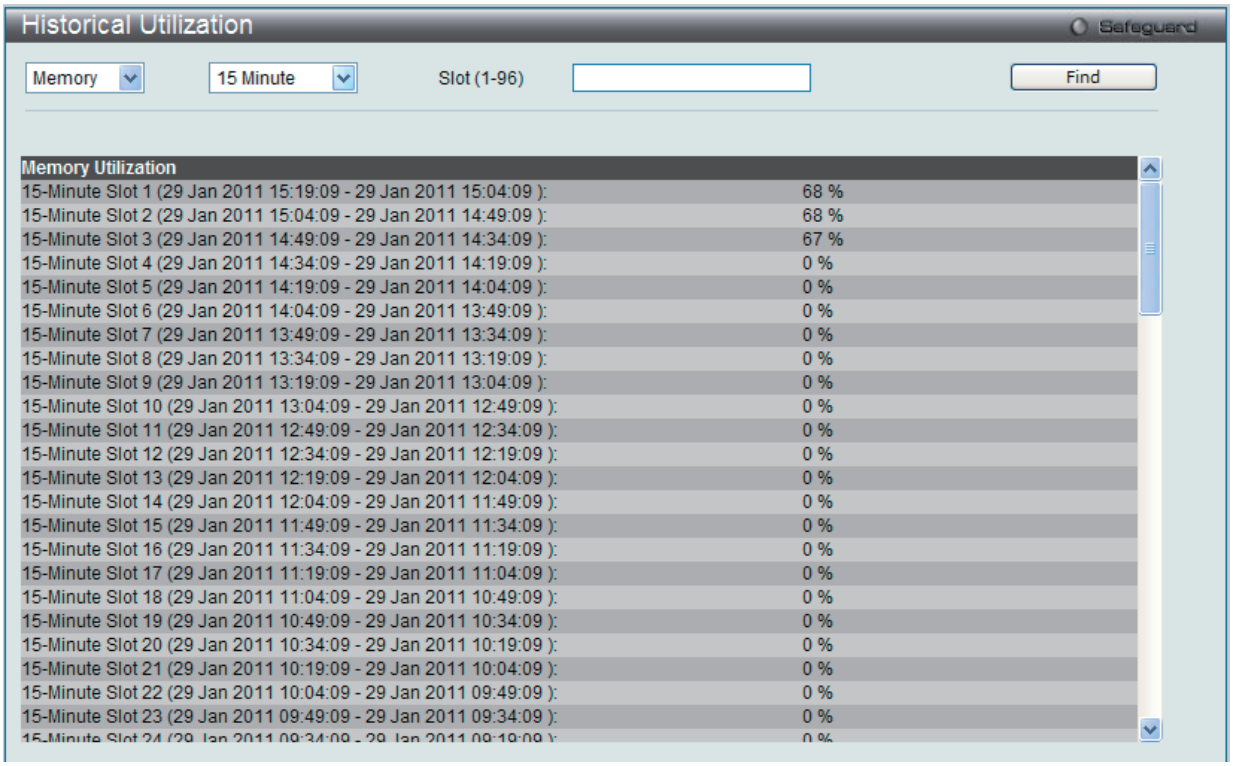


図 16-17　Historical Utilization (Memory) 画面

「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。

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。

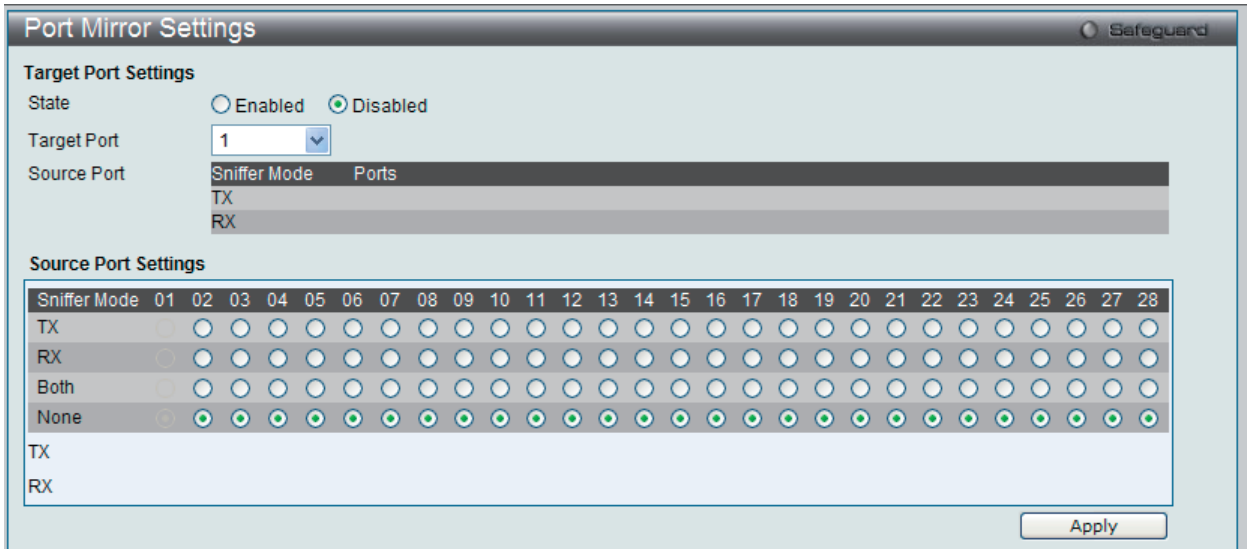


図 16-18　Port Mirror Settings 画面

ミラーポートの設定手順：

1. 「Mirror Port 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。

RSPAN Settings（RSPAN 設定）

RSPAN機能をコントロールします。RSPAN機能の目的は、パケットをリモートスイッチにミラーリングすることです。パケットは、ミラーされるパケットを受信したスイッチから、中間スイッチを通過し、スニファーが接続するスイッチに送信されます。また、最初のスイッチはソーススイッチと言われます。

RSPAN 機能を動作するためには、ソーススイッチに RSPAN VLAN ソース設定を行います。中間スイッチと最後のスイッチに関しては、RSPAN VLAN のリダイレクト設定を行います。

注意 RSPAN が有効な場合だけ (1 つの RSPAN VLAN がソースポートに設定されている場合)、RSPAN VLAN ミラーリングは動作します。RSPAN が有効になり、少なくとも 1 つの RSPAN VLAN がリダイレクトポートに設定されると、RSPAN リダイレクト機能は動作します。

Monitoring > Mirror > RSPAN 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。

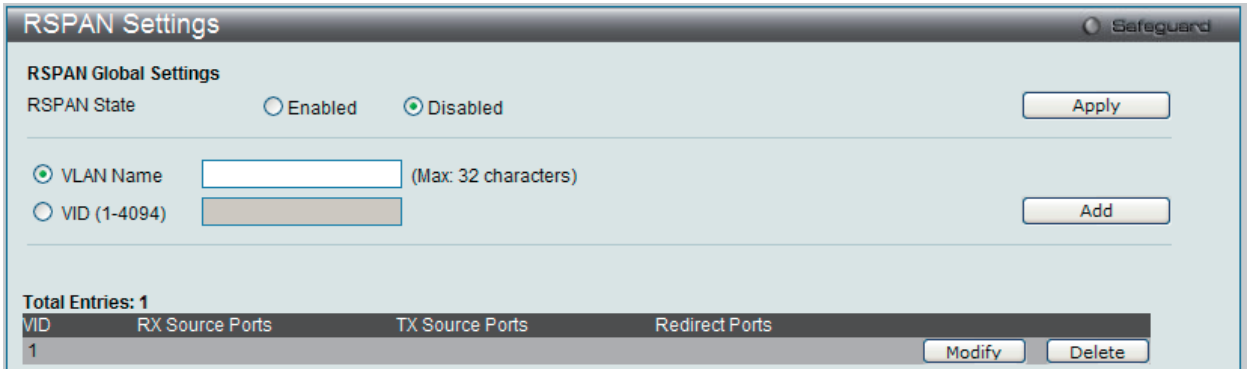


図 16-19 RSPAN Settings 画面

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
RSPAN State	RSPAN 機能を有効または無効にします。
VLAN Name	VLAN 名により RSPANVLAN を指定します。
VID	VLAN ID により RSPANVLAN を指定します。

「Apply」ボタンをクリックして行った変更を適用します。
「Add」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。
「Modify」ボタンをクリックして、指定エントリを編集します。
「Delete」ボタンをクリックして、指定エントリを削除します。

RSPAN 設定の編集

「Modify」ボタンをクリックして、以下の画面を表示します。

図 16-20 RSPAN Settings (Modify) 画面

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
VID	VLAN ID により RSPAN VLAN を表示します。
VLAN Name	VLAN 名により RSPAN VLAN を表示します。
Source Ports	ポートがこのオプションで指定されないと、RSPAN のソースは「mirror」コマンドによって指定されるソースまたは ACL によって指定されたフローベースのソースとなります。ソースにパラメータが指定されないと、設定されたソースパラメータは削除されます。パケットをモニタする方向（RX、TX、Both）を選択します。「Add」または「Delete」ボタンをクリックしてソースポートを追加または削除します。
Redirect Port List	RSPAN VLAN パケットに出力ポートリストを指定します。リダイレクトポートがリンクアグリゲーションポートであると、RSPAN パケットにリンクアグリゲーションの動作を行います。「Add」または「Delete」ボタンをクリックしてリダイレクトポートを追加または削除します。

「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。

sFlow（sFlow 設定）

sFlow（RFC3176）はスイッチとルータを含むデータネットワークのトラフィックをモニタリングする技術です。sFlow モニタリングシステムは、(スイッチまたはルータに組み込まれている、またはスタンドアロンの検査装置にある)sFlow エージェントと中央の sFlow コレクタから成っています。sFlow モニタリングシステムで使用されるアーキテクチャとサンプリング手法は、高速でスイッチされて、ルートを決定されるネットワークに対して連続したサイト全体（企業全体）のトラフィックモニタリングを提供するように設計されています。

sFlow Global Settings（sFlow グローバル設定）

sFlow 機能を有効または無効にします。

Monitoring > sFlow > sFlow 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。

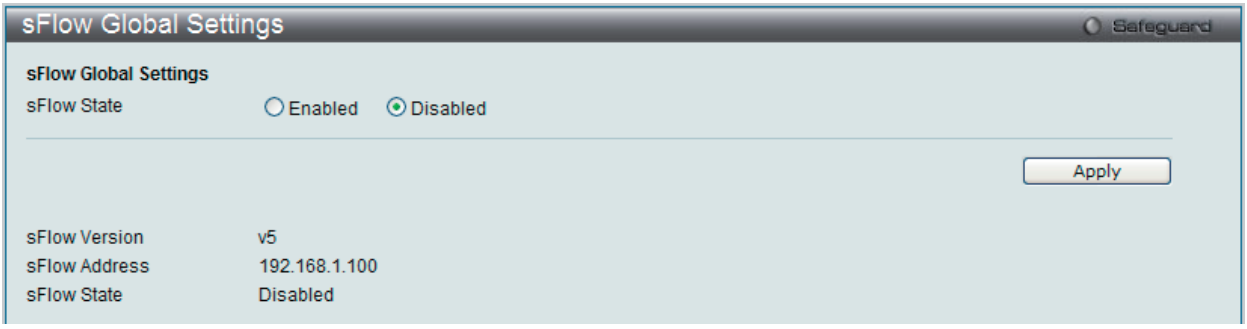


図 16-21　sFlow Global Settings 画面

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
sFlow State	sFlow 機能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。

sFlow Analyzer Server Settings（sFlow アナライザ設定）

sFlow アナライザサーバのパラメータを設定します。同時に 4 個の異なるアナライザサーバをサポートすることができ、各サンプラまたはポーラはコレクタを選択してサンプルを送信します。異なるサンプラまたはポーラから異なるコレクタに異なるサンプルを送信できます。

Monitoring > sFlow > sFlow Analyzer 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。

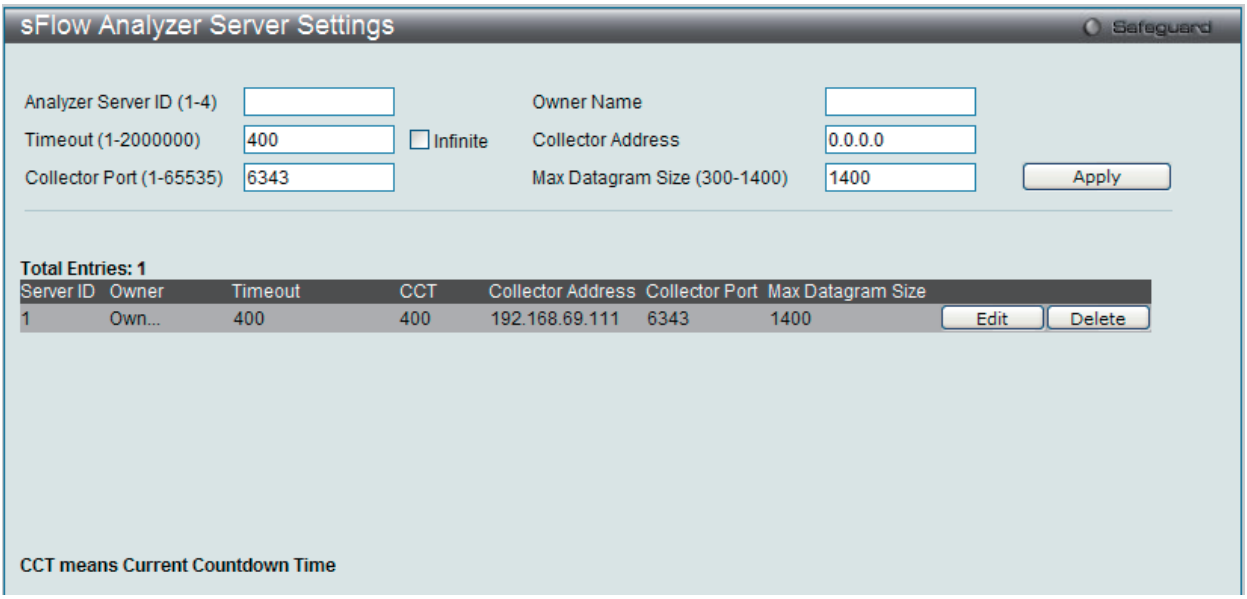


図 16-22　sFlow Analyzer Server Settings 画面

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
Analyzer Server ID	パケットが転送されるアナライザサーバの ID を指定します。
Owner Name	この sFlow アナライザサーバを利用するエンティティ。オーナが設定または変更される場合、タイムアウト値は自動で 400 になります。
Timeout	サーバがタイムアウトになる前の時間。アナライザサーバがタイムアウトになると、すべての sFlow サンプラとこのアナライザサーバに関連するカウンタポーラは削除されます。指定しないと、初期値は 400 です。
Collector Address	アナライザサーバの IP アドレスを指定します。指定しないか、0 のアドレスを設定すると、エントリは非アクティブになります。
Collector Port	sFlow データが送信される宛先 UDP ポート。指定しない場合、初期値は 6343 です。
Max Datagram Size	1 つのサンプルデータでパックされるデータの最大数 (バイト)。指定しない場合、初期設定は 1400 です。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

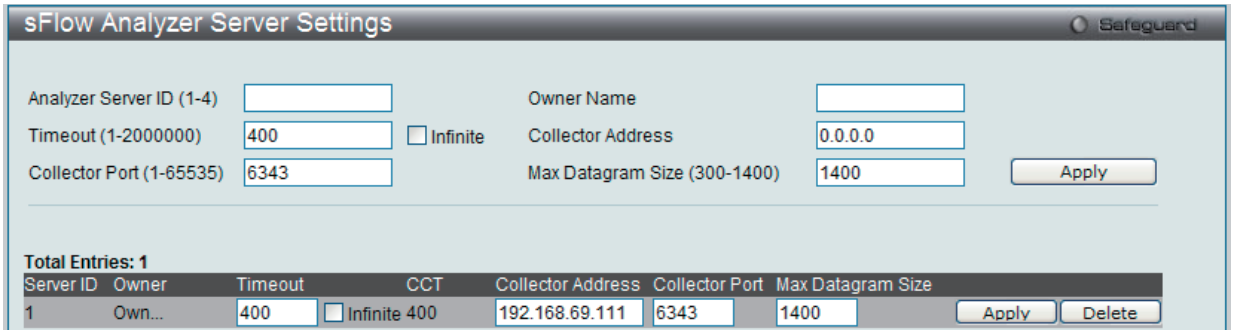


図 16-23　sFlow Analyzer Server Settings 画面 - Edit

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。

sFlow Flow Sampler Settings（sFlow サンプラ設定）

sFlow アナライザサーバのパラメータを設定します。ポートにサンプリング機能を設定することによって、このポートが受信したサンプルパケットはカプセル化されて指定間隔でアナライザサーバに転送されます。

注意　アナライザサーバ ID の変更のために、はじめにフローサンプラを削除し、次に新しいものを作成する必要があります。

Monitoring > sFlow > sFlow Flow Sampler 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。

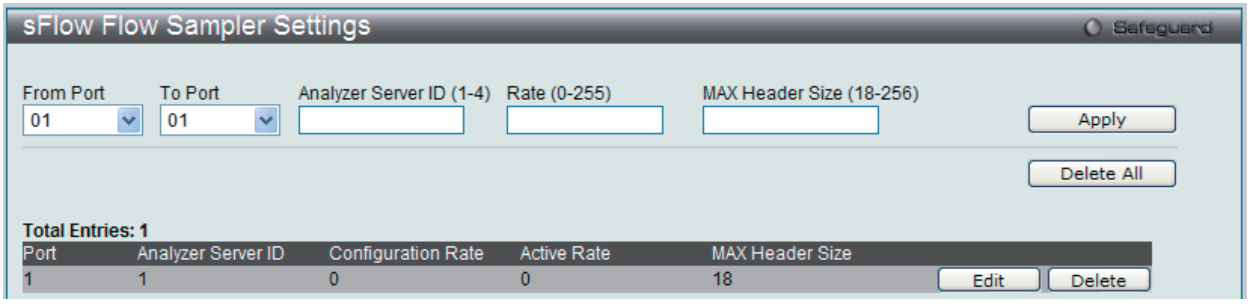


図 16-24　sFlow Flow Sampler Settings 画面

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
From Port / To Port	設定するポートリストを指定します。
Analyzer Server ID	パケットが転送されるアナライザサーバの ID を指定します。
Rate	受信パケットサンプリングのためのサンプリングレート。256 の倍数で設定されたレートが実効レートです。例えば、レートが 20 であれば、実効レートは 5120 です。あるパケットが 5120 のパケットごとに抽出されます。0 に設定されると、サンプラは無効になります。レートを指定しないと、初期値は 0 です。
MAX Header Size	カプセル化してサーバに送信するサンプリングパケットの主なバイトの最大数。指定しない場合、初期設定は 128 です。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

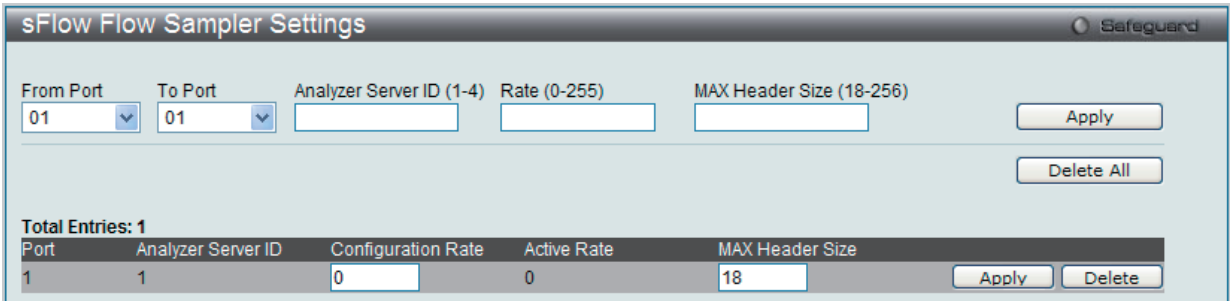


図 16-25 sFlow Flow Sampler Settings 画面 - Edit

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。

sFlow Counter Poller Settings（sFlow カウンタポーラ設定）

sFlow カウンタポーラのパラメータを設定します。アナライザサーバ ID の変更のためには、はじめにカウンタポーラを削除し、次に新しいものを作成する必要があります。

Monitoring > sFlow > sFlow Counter Poller 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。

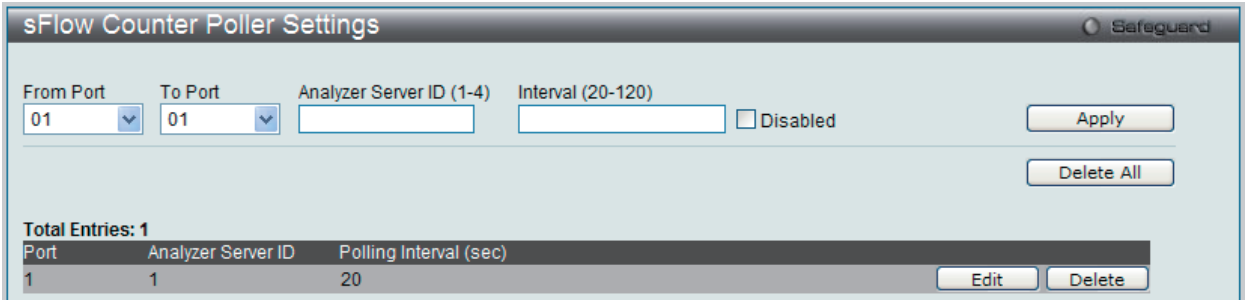


図 16-26 sFlow Counter Poller Settings 画面

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
From Port / To Port	設定するポートリストを指定します。
Analyzer Server ID	パケットが転送されるアナライザサーバの ID を指定します。
Interval	カウンタの連続するサンプルの間隔 (秒)。

「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、以下の画面を表示します。

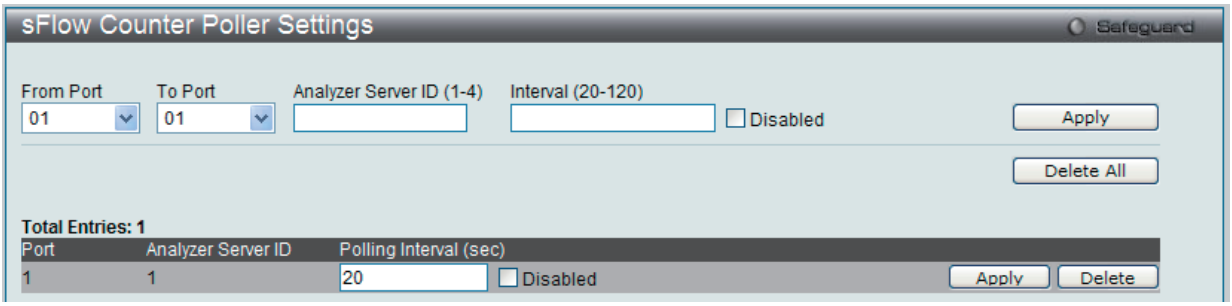


図 16-27 sFlow Counter Poller Settings 画面 - Edit

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。

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。

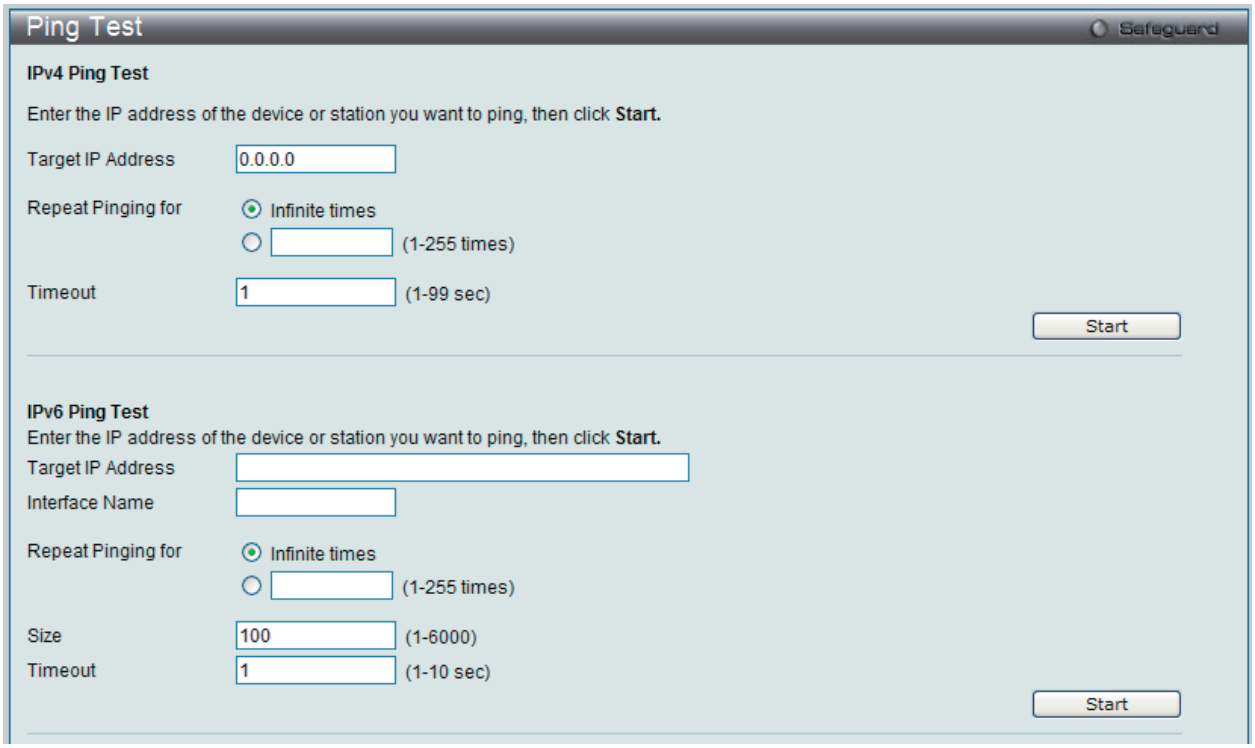


図 16-28　Ping Test 画面

「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。
Interface Name	IPv6 の場合、Ping するインタフェース名を入力します。
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	IPv4 では、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。 IPv6 では、送信先への Ping メッセージの応答待ち時間 1-10（秒）で入力します。 いずれの場合も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。

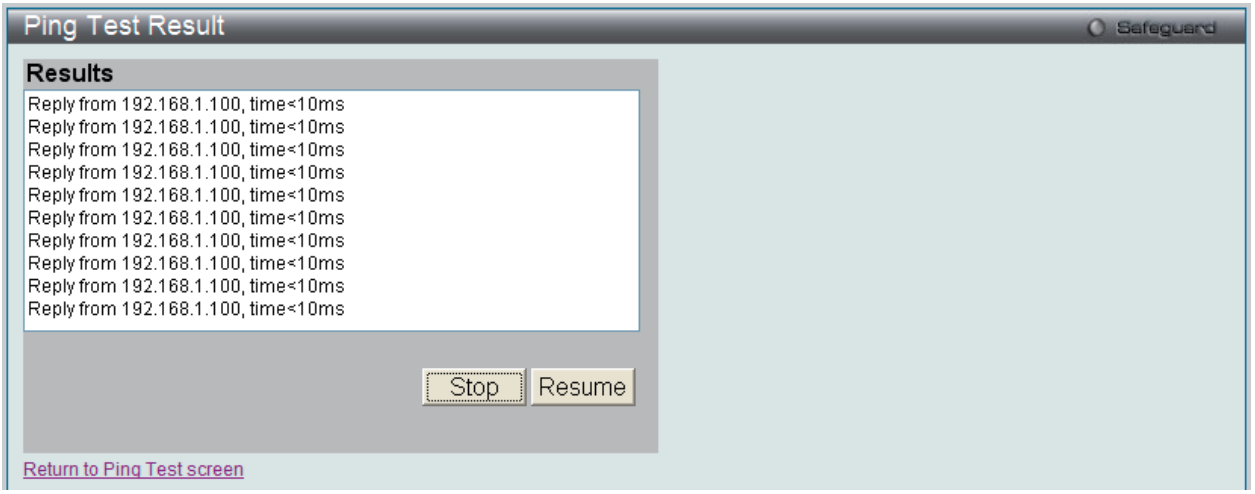


図 16-29 Ping Test (Result) 画面

「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。

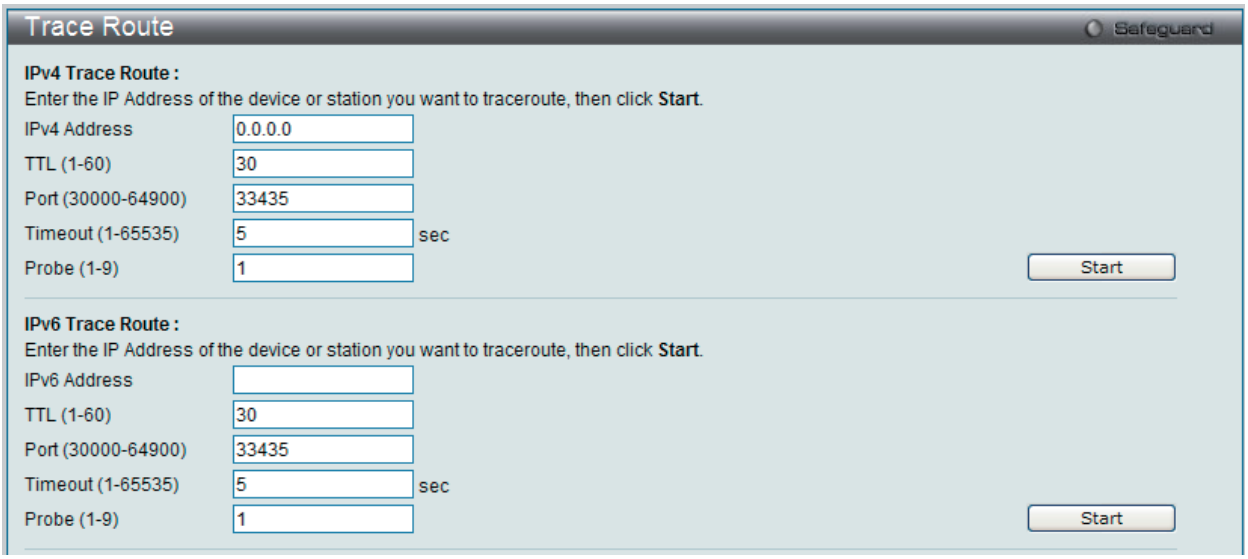


図 16-30 Trace Route 画面

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 / IPv6 Address	宛先ステーションの IP アドレス。
TTL (1-60)	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 (30000-64900)	ポート番号。値の範囲は、30000-64900 です。
Timeout (1-65535)	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 (1-9)	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。

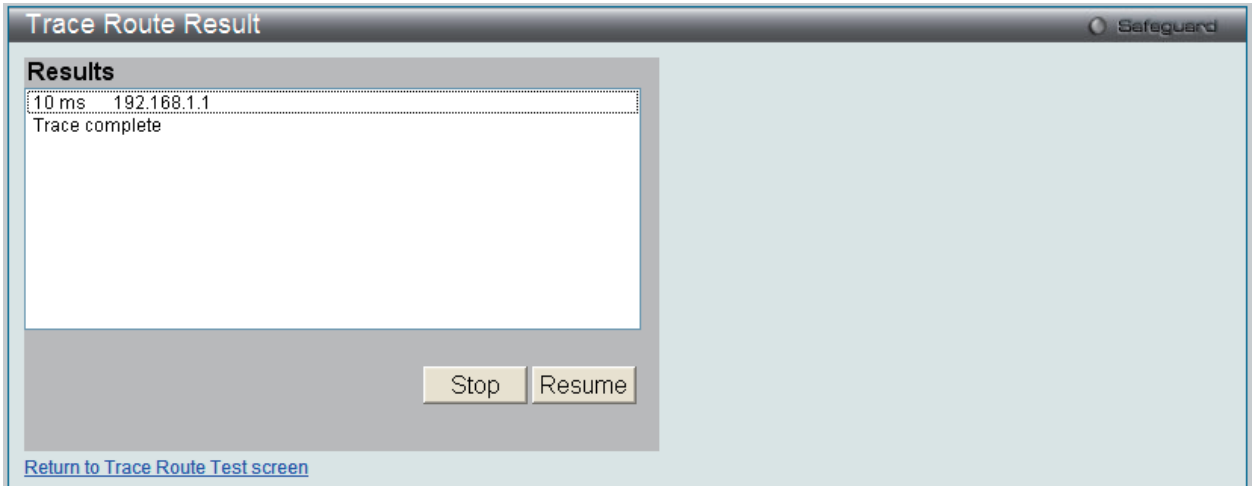


図 16-31 Trace Route (Result) 画面

「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。

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 > 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。

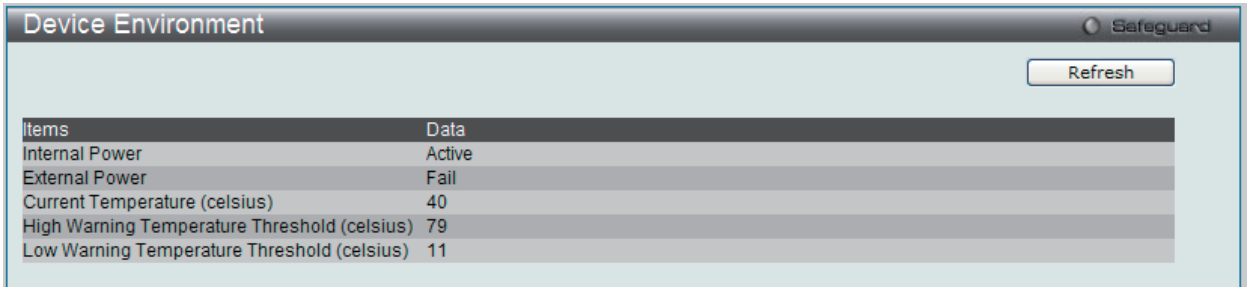


図 16-32 Device Environment 画面

「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 17 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）	スイッチのメモリにコンフィグレーションとログを保存します	467
Tools（ツールメニュー）		
License Management（ライセンス管理）	EI 版ライセンスのアクティベーションを行います。	468
Download Firmware（ファームウェアのダウンロード）	コンフィグレーションファイルをアップロードします。	469
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。	471
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。	472
Upload Configuration（コンフィグレーションファイルのアップロード）	コンフィグレーションファイルをアップロードします。	475
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。	477
Reset（リセット）	工場出荷時設定に戻し、メモリに保存します。	479
Reboot System（システムの再起動）	スイッチの再起動を行います。	480

メンテナンスメニューは以下の通りです。

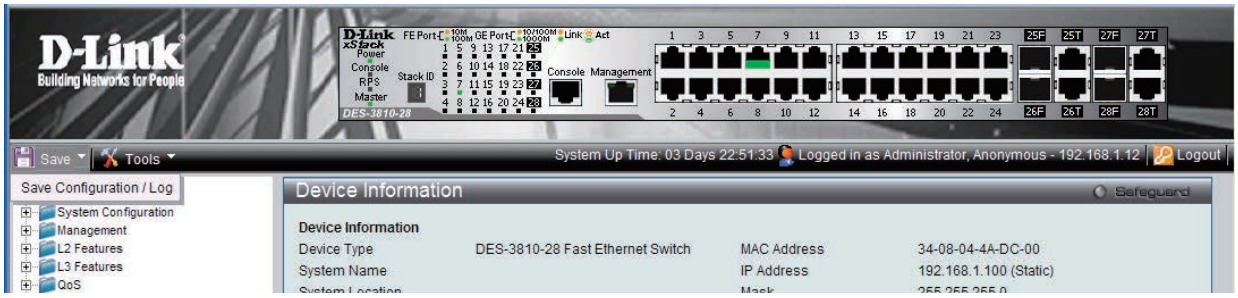


図 17-1　Save Configuration / Log 画面

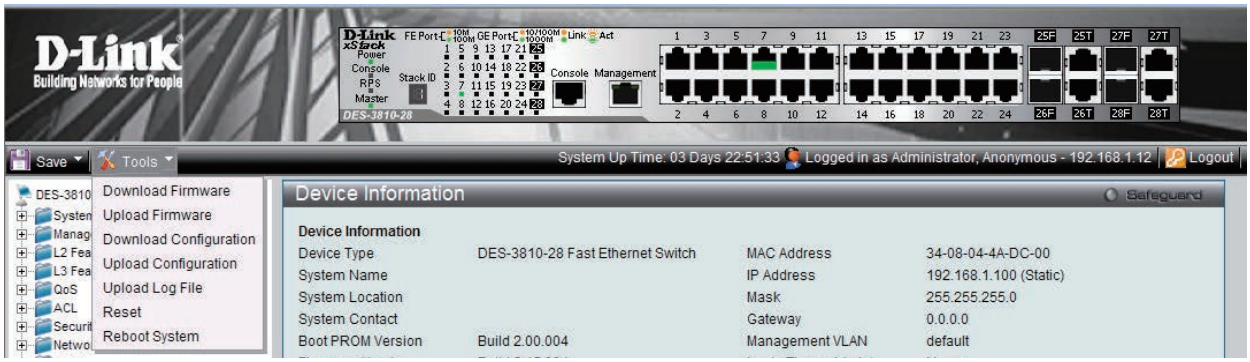
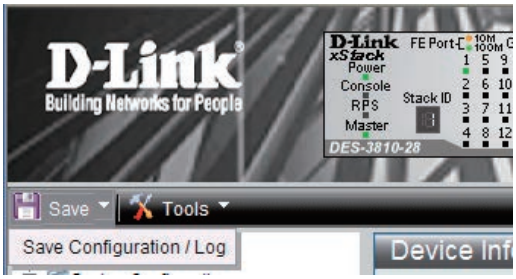


図 17-2　Tools 画面

Save Configuration / Log（コンフィグレーションとログの保存）

「Save Configuration」により、コンピュータでのフォルダにスイッチのコンフィグレーションをバックアップすることができます。「Type」欄から「Configuration」を選択し、提供されたスペースにファイルパスを入力して「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

スイッチのコンフィグレーションファイルをバックアップすることができます。「Type」欄から「Configuration」を選択して、「Apply」ボタンをクリックします。

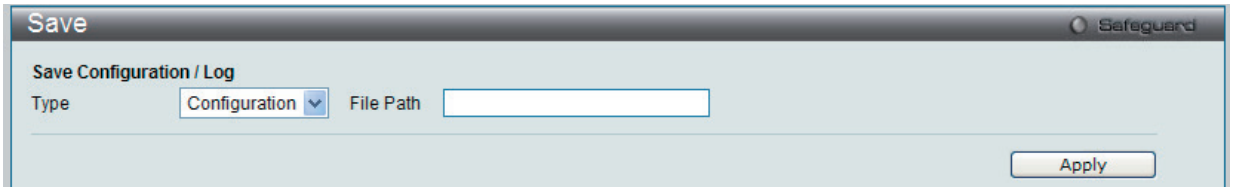


図 17-3　Save 画面 - Configuration

ログの保存

スイッチに関するログファイルをバックアップすることができます。「Type」欄から「Log」を選択して、「Apply」ボタンをクリックします。

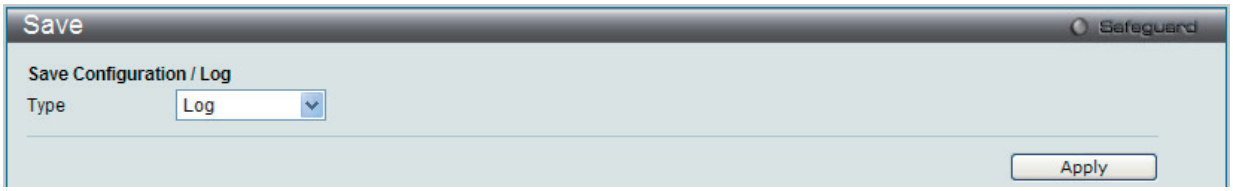


図 17-4　Save 画面 - Log

すべての保存

コンフィグレーション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。

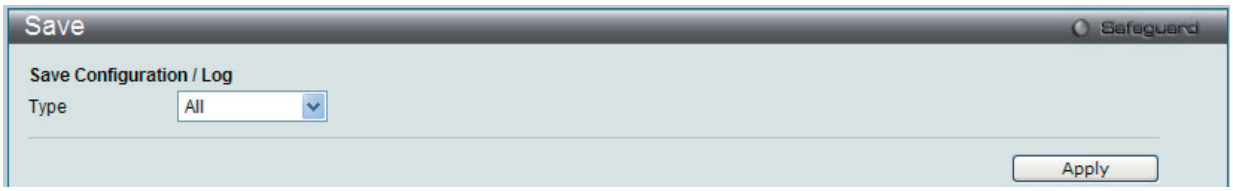
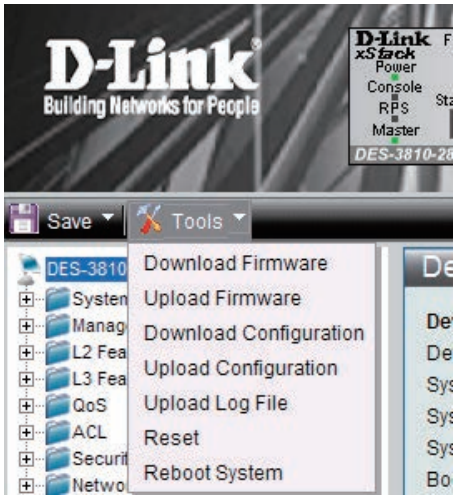


図 17-5　Save 画面 - All

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、以下のメニューからオプションを選択します。



License Management（ライセンス管理）

DGS-3810 シリーズの SI 版（スタンダードイメージ版）の機種に「EI 版（エンハンスイメージ版）」のライセンスを導入することで、DGS-3810 にお使いのネットワーク環境に適した機能を追加することが可能です。ライセンスアクティベーションを行うには、まず以下の D-Link の Web サイト：GRP（Global Registration Portal）からアクティベーションコードを取得する必要があります。アクティベーションコードの取得には、GRP にてお使いの機器のシリアル番号とライセンスキーの入力を行う必要があります。

Global Registration Portal：https://register.dlink.com/

「Activation Code」の取得方法

a. 機器に同梱してある「ライセンスキー」と機器の底面にある「シリアル番号」を確認します。
b. Web ブラウザで https://register.dlink.com へアクセスし「D-Link Global Registration Portal」に必要事項を入力します。
（アカウントを保持していない場合、新しくアカウントを作成します。）
c. 設定したユーザ名とパスワードでログインします。
d. 表示される指示に従い入力を行い、アクティベーションコードを取得します。
（事前に確認した「ライセンスキー」と「シリアル番号」の入力が必要です。）

Web GUI でのライセンスアクティベーション

以下に、取得したアクティベーションコードを機器にインストールする手順を示します。

1. **Tools > License Management** 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 17-6　ライセンスのインストール

2. 提供された有効なアクティベーションコードを「Activation Code」欄に指定し、「Install」をクリックします。

図 17-7　ライセンスのインストール（アクティベーションコードの指定）

3. アクティベーション終了の画面が表示されたあと、機器を再起動してライセンスアクティベーションを有効にします。
4. **Tools > Reboot** の順にメニューをクリックし、以下の画面を表示し、「Yes」を選択してから「Reboot」をクリックします。

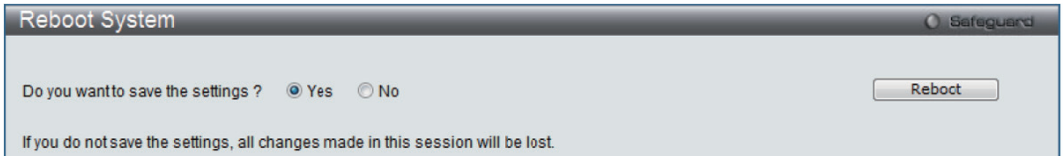


図 17-8　機器の再起動

注意　「Yes」を選択していない状態で再起動してしまうと、アクティベーションが有効になりません。ご注意ください。

5. 機器の再起動中です。電源は切らないようにします。

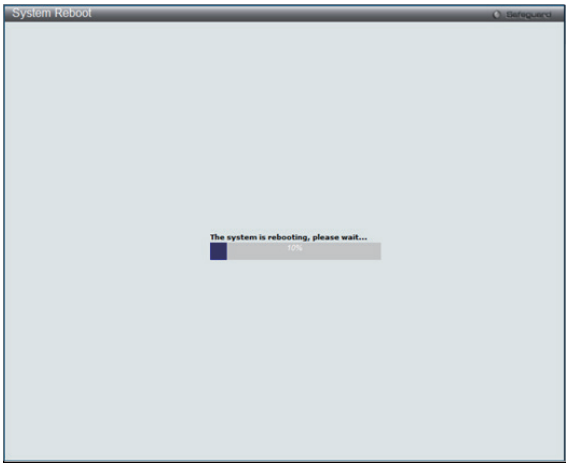


図 17-9　再起動中

6. 再起動後、**License Management** を再度表示し、表示される画面で有効ライセンスの状況を確認します。

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。

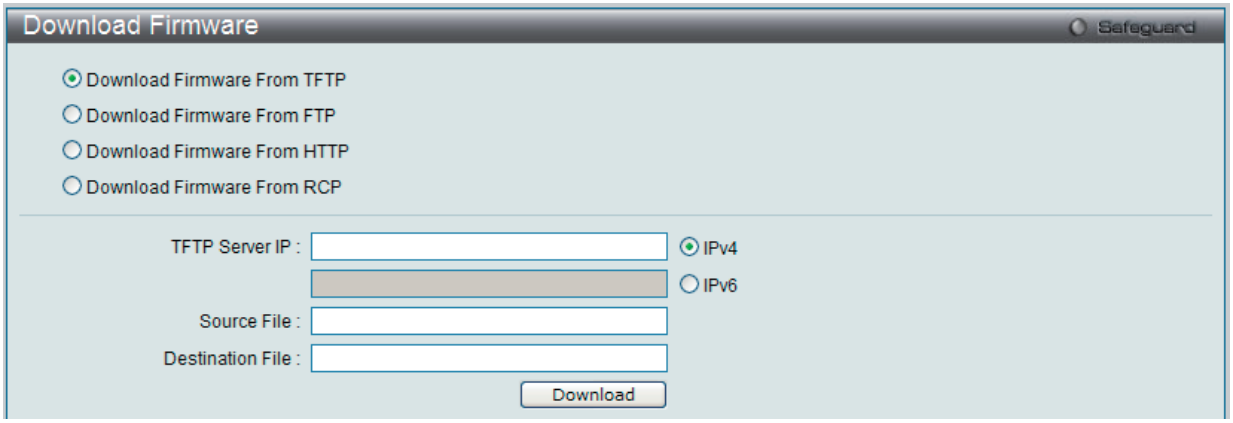


図 17-10　Download Firmware From TFTP 画面

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。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。
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。

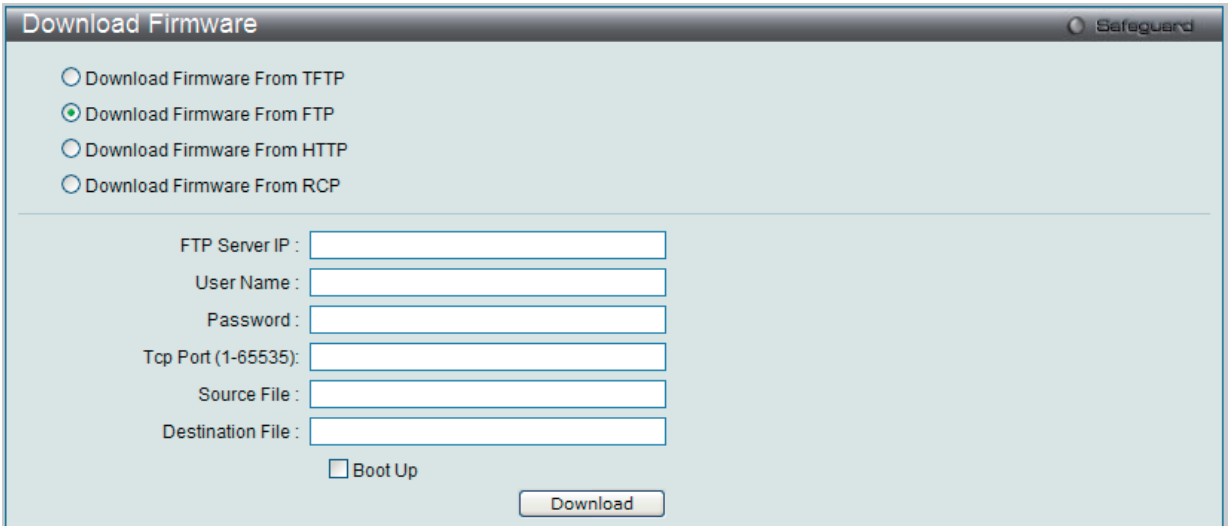


図 17-11　Download Firmware From FTP 画面

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 17-12　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。

Download Firmware From RCP（RCP からファームウェアをダウンロード）

RCP 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 RCP」を選択して以下の画面を表示します。

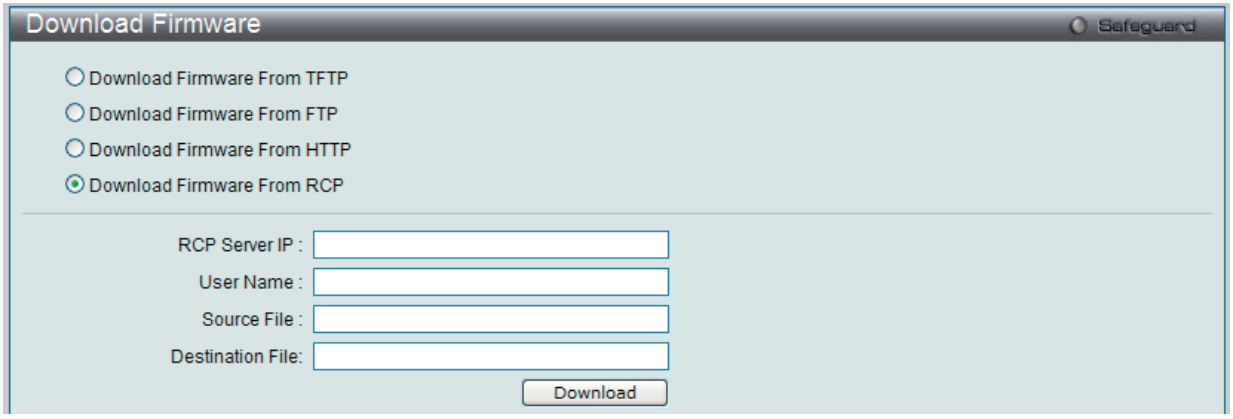


図 17-13　Download Firmware From RCP 画面

以下の項目があります。

項目	説明
RCP Server IP	使用する RCP 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。
User Name	使用する適切なユーザ名を指定します。
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。

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。

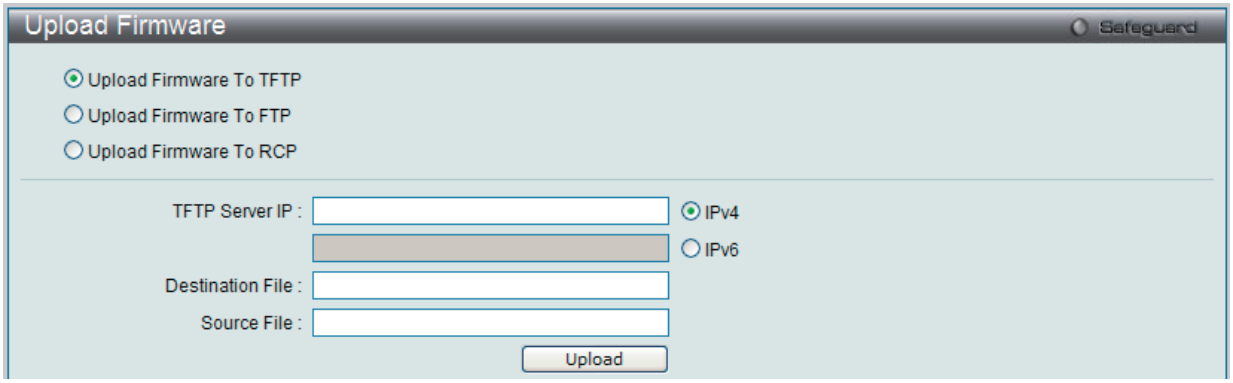


図 17-14　Upload Firmware To TFTP 画面

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。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。
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。

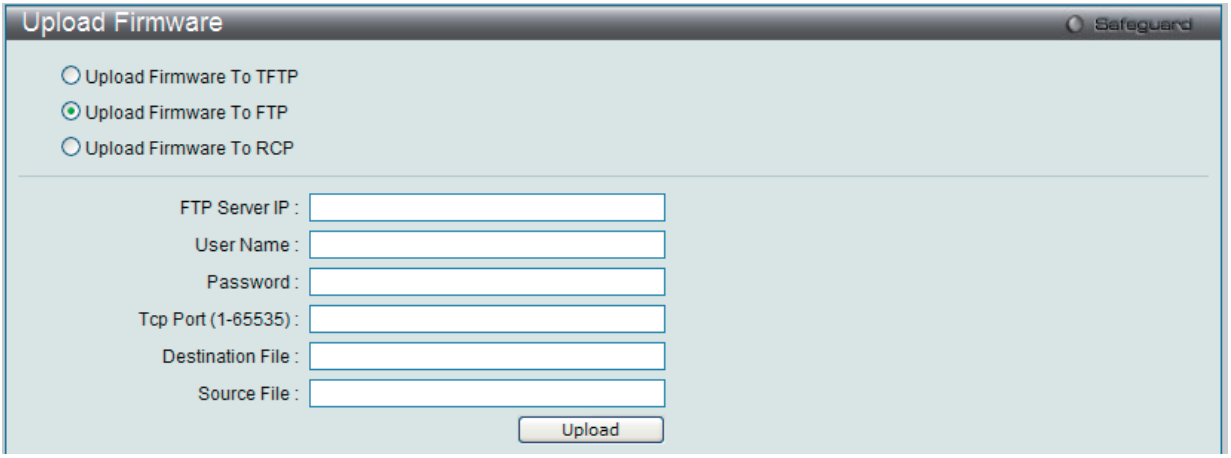


図 17-15 Upload Firmware To FTP 画面

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。

Upload Firmware To RCP(ファームウェアを RCP にアップロードする)

スイッチから RCP 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 RCP」を選択して以下の画面を表示します。

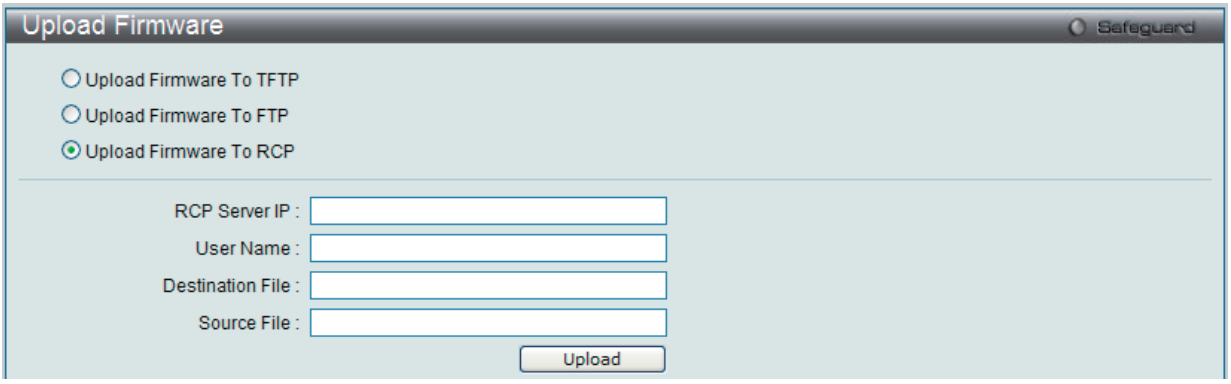


図 17-16 Upload Firmware To RCP 画面

以下の項目があります。

項目	説明
RCP Server IP	使用する RCP 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。
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。

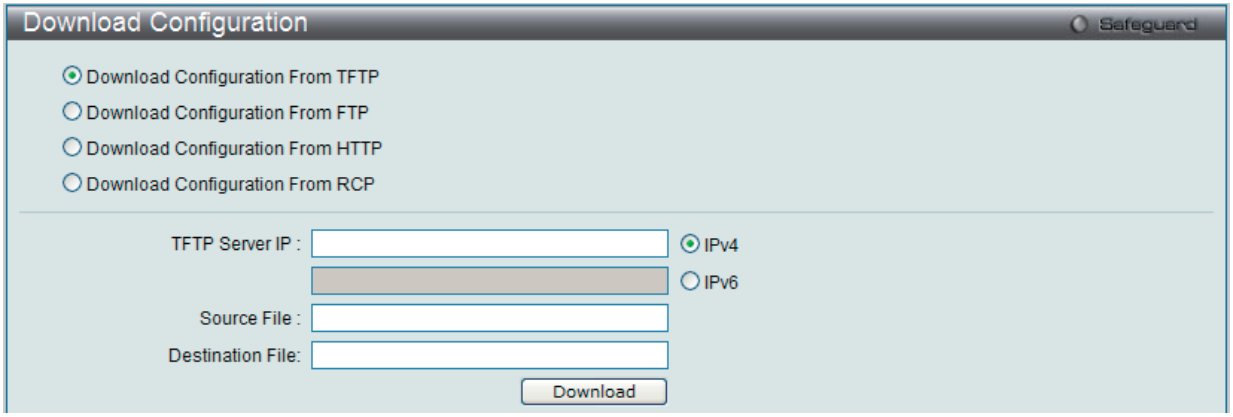


図 17-17 Download Configuration From TFTP 画面

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。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。
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。

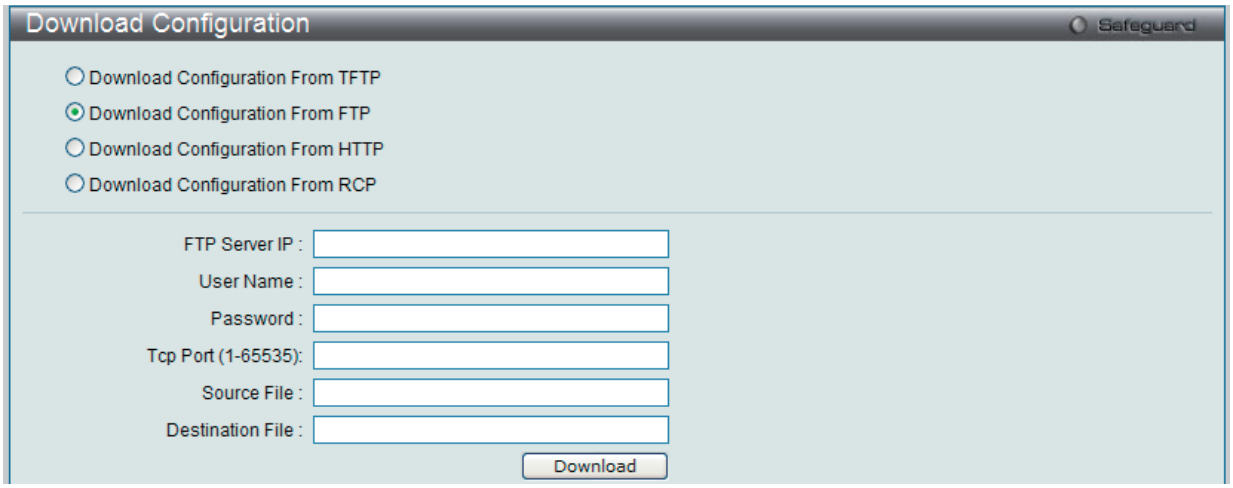


図 17-18 Download Configuration From FTP 画面

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 17-19 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。

Download Configuration From RCP（RCP 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）

RCP 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 RCP」を選択して以下の画面を表示します。

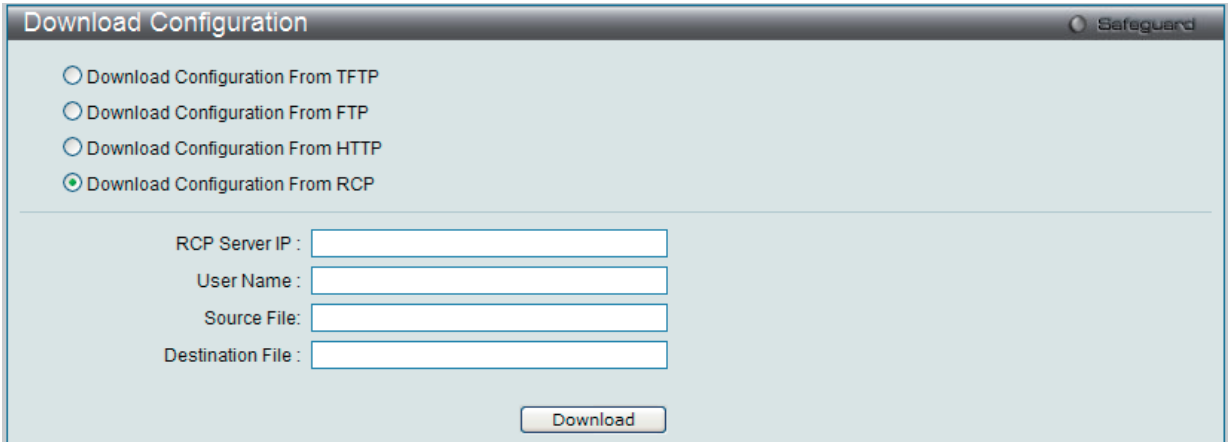


図 17-20 Download Configuration From RCP 画面

以下の項目があります。

項目	説明
RCP Server IP	使用する RCP 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。
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。

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。

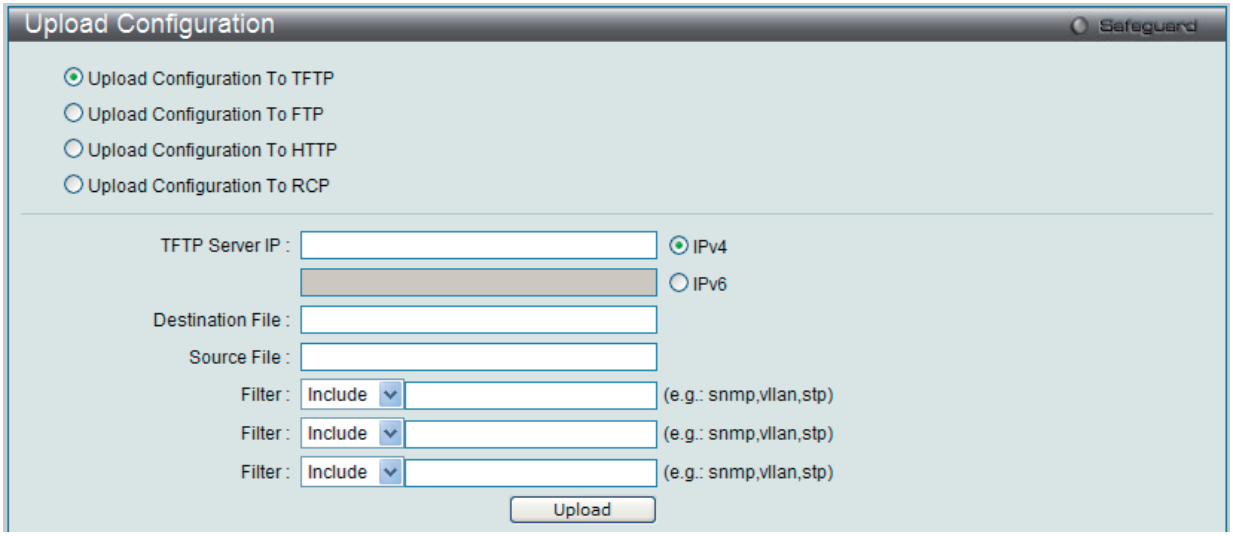


図 17-21　Upload Configuration To TFTP 画面

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。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。
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。

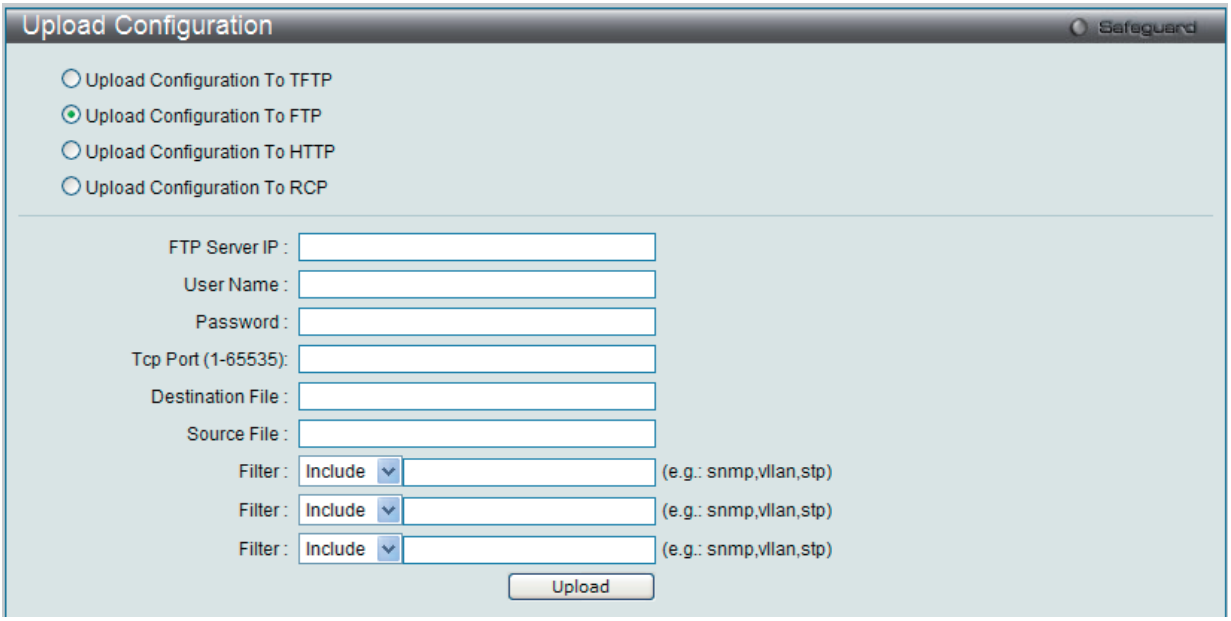


図 17-22 Upload Configuration To FTP 画面

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。

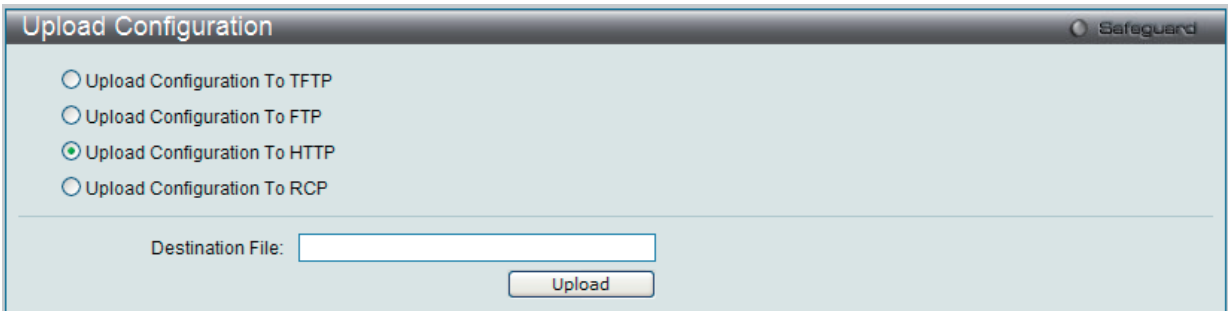


図 17-23 Upload Configuration To HTTP 画面

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。

「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 RCP（コンフィグレーションを RCP サーバにアップロードする）

スイッチから RCP 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 RCP」を選択して以下の画面を表示します。

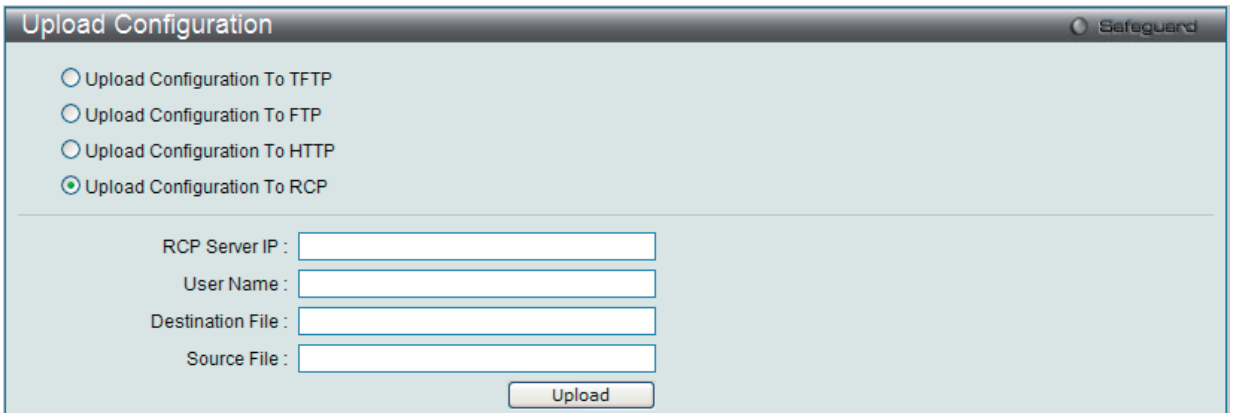


図 17-24　Upload Configuration To RCP 画面

以下の項目があります。

項目	説明
RCP Server IP	使用する RCP 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。
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 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。

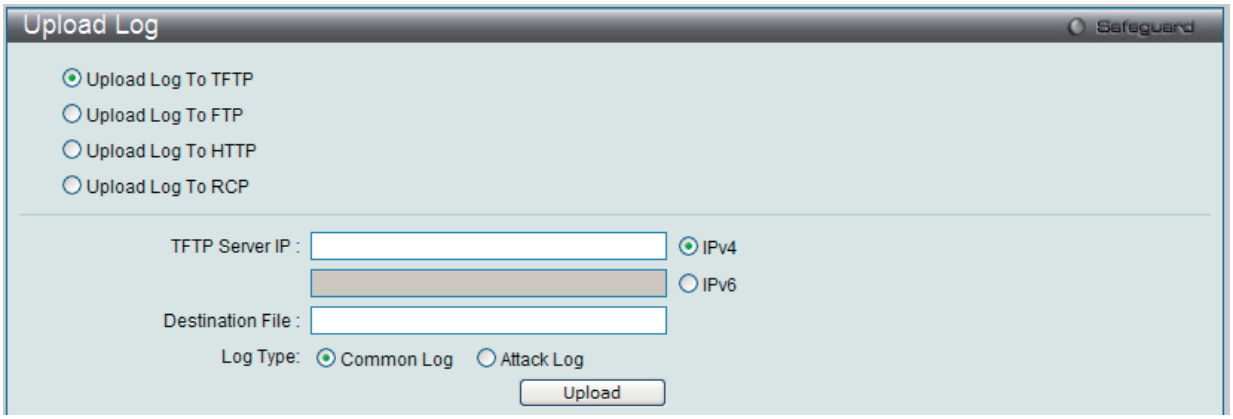


図 17-25　Upload Log To TFTP 画面

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。

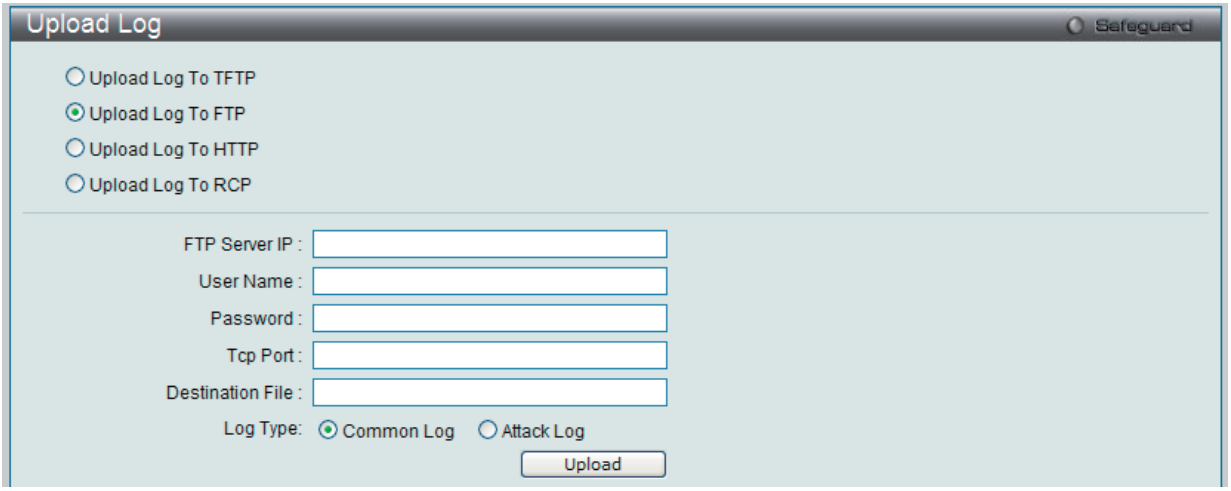


図 17-26 Upload Log To FTP 画面

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。

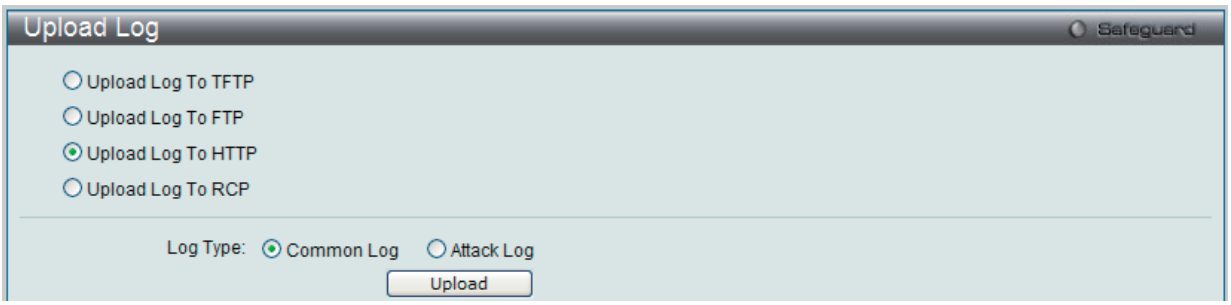


図 17-27 Upload Log To HTTP 画面

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。

Upload Log To RCP（RCP サーバにログをアップロードする）

スイッチから RCP 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 RCP」を選択して以下の画面を表示します。

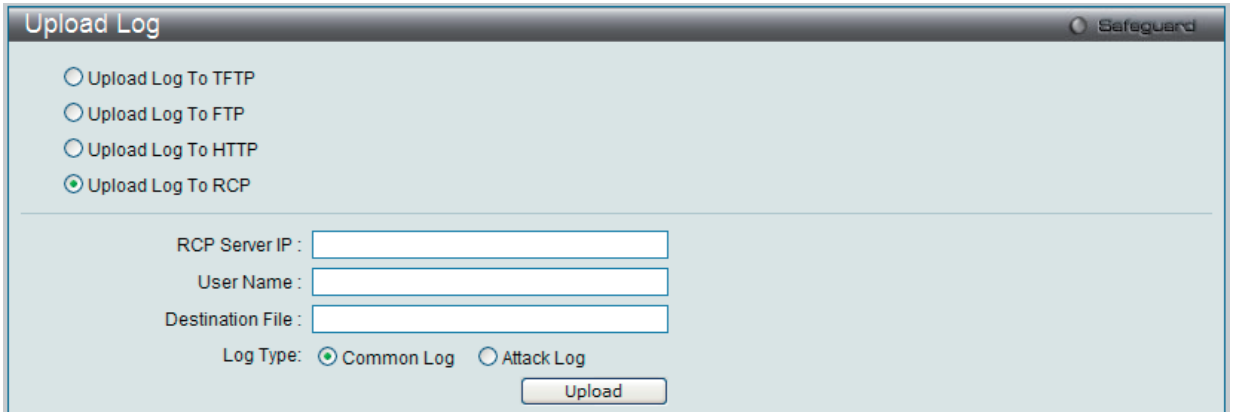


図 17-28 Upload Log To RCP 画面

以下の項目があります。

項目	説明
RCP Server IP	使用する RCP 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。
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。

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」はスイッチのユーザアカウント、ヒストリログ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 Changes」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。

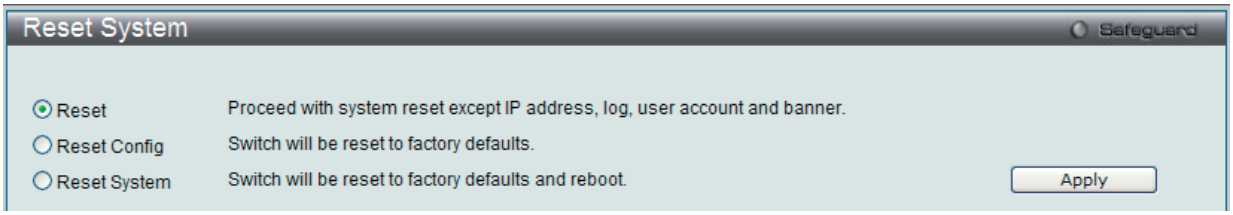


図 17-29 Reset System 画面

項目	説明
Reset	IP アドレス、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。

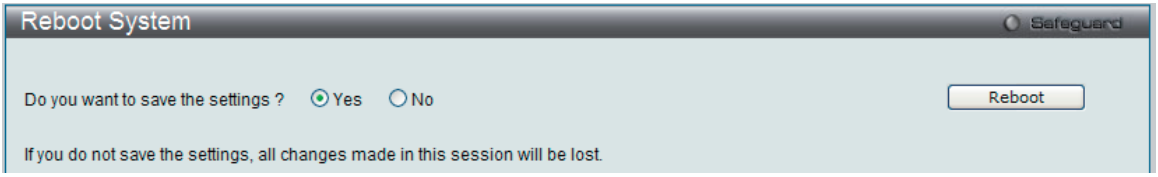


図 17-30　Reboot System 画面

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。

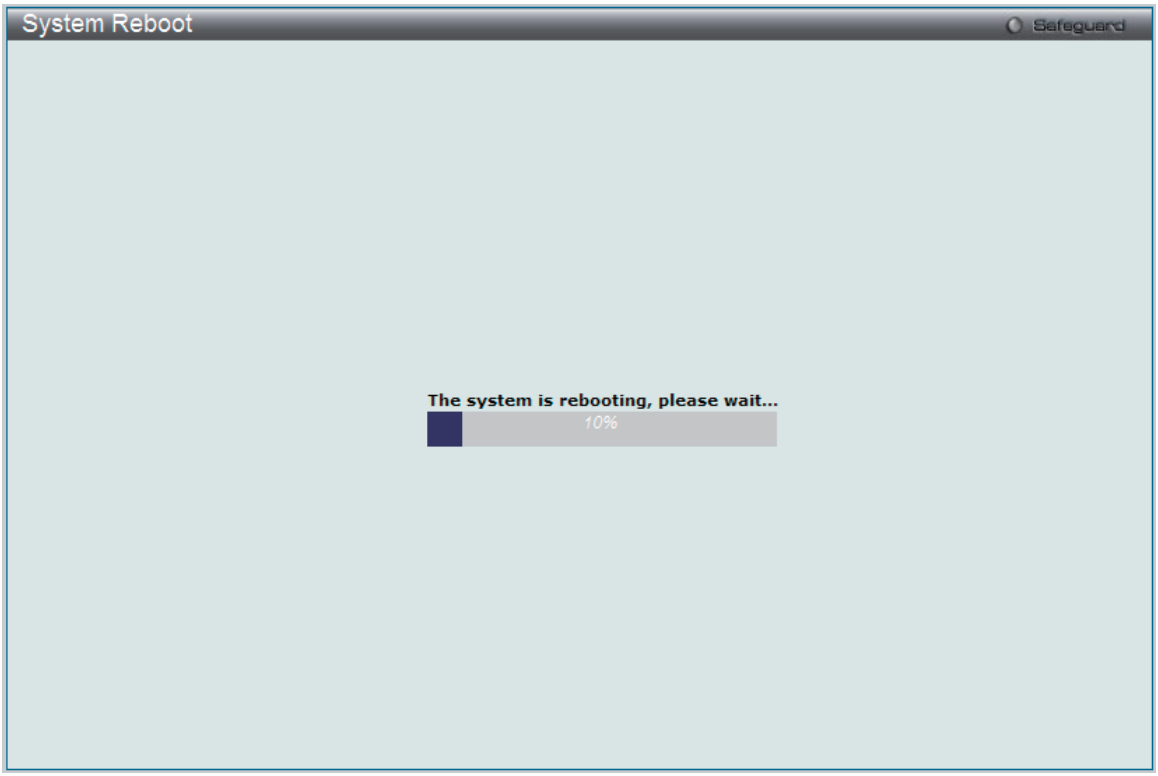


図 17-31　System Reboot 画面

付録 A ケーブルとコネクタ

イーサネットケーブル

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。

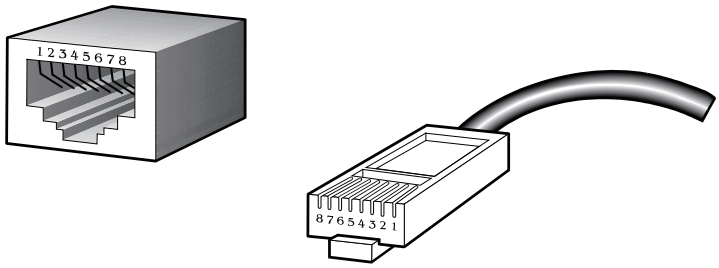


図 A-1　標準的な RJ-45 プラグとコネクタ

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

コンソールケーブル

スイッチを PC に接続する場合、付属のコンソールケーブルが必要です。以下の図と表は標準のコンソール -RJ45 へのソケット / コネクタとそれらのピンアサインです。

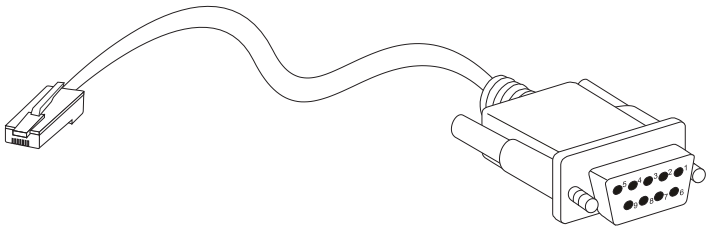


図 A-2　標準的なコンソール -RJ-45 ケーブル

コンソール -RJ-45 ピンアサイン		
ピン番号	コンソール（D-Sub9 / RS232）	RJ-45
1	未使用	未使用
2	RXD	未使用
3	TXD	TXD
4	未使用	GND
5	GND（共有）	GND
6	未使用	RXD
7	未使用	未使用
8	未使用	未使用

リダンダント電源（RPS）ケーブル

スイッチをリダンダント電源に接続する場合、RPS ケーブルが必要です。製品がケーブルのピンアサインに一致することを確認してください。以下の図と表は標準の RPS のソケット / コネクタとそれらのピンアサインです。

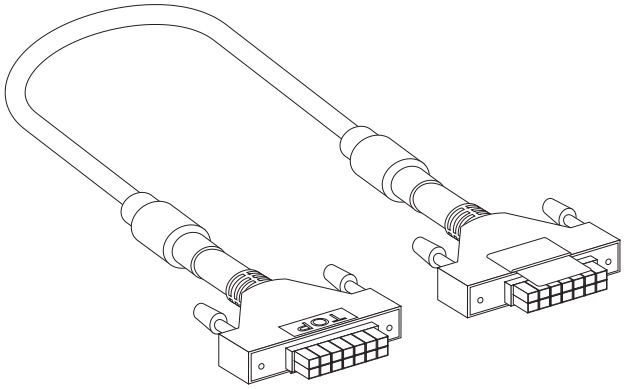


図 A-3　リダンダント電源ケーブル

RPS ケーブルピンアサイン		
ピン番号	デバイス	DPS-200
1	GND	GND
2	NC	NC
3	+12V	+12V
4	+12V	+12V
5	+12V	+12V
6	+12V	+12V
7	GND	GND
8	GND	GND
9	NC	電力良好
10	NC	電力供給
11	電力良好	NC
12	電力供給	NC
13	GND	GND
14	GND	GND

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。

表 B-1　ケーブル長

規格	メディアタイプ	最大伝送距離
SFP	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	10km 550m 40km 80km
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（1000Mbps）	100m
100BASE-TX	カテゴリ 5 UTP ケーブル（100Mbps）	100m
10BASE-T	カテゴリ 3 UTP ケーブル（10Mbps）	100m

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	摘要
システム	System started up	Critical	システム起動	
	Log Message: Configuration saved to flash (Username: <username>) username : コンフィグレーションを保存するユーザ名	Informational	フラッシュメモリへのコンフィグレーションファイル保存	
	System log saved to flash(Username: <username>) Parameters Description: username : コンフィグレーションを保存するユーザ名	Informational	フラッシュメモリへのシステムログ保存	
	Configuration and log saved to flash (Username: <username> username : コンフィグレーションを保存するユーザ名	Informational	フラッシュメモリへのコンフィグレーションとログ保存	
周辺機器	Log Message: Temperature sensor <sensorID> enters alarm state (current temperature: <temperature>) sensorID: センサ ID temperature: 温度	Informational	温度センサの警告状態に入りました。	
	Temperature sensor <sensorID> recovers to normal state (current temperature: <temperature>) sensorID: センサ ID. temperature: 温度	Informational	温度が正常に回復	
	Internal Power Failed	Critical	内蔵電源エラー	
	Internal Power is recovered	Critical	内蔵電源回復	
	Redundant Power failed	Critical	リダンダント電源エラー	
	Redundant Power is working	Critical	リダンダント電源が動作中	
SNMP	SNMP request received from <ipAddress> with invalid community string! ipAddress: IP アドレス	Informational	無効なコミュニティ名を含む SNMP リクエスト受信	
インタフェース	Port <portNum> link up, <link state> portNum: ポート番号 link state: ポートのリンク状態（例 : 100Mbps FULL duplex）	Informational	ポートリンクアップ	
	Port <portNum> link down portNum: ポート番号	Informational	ポートリンクダウン	
デバッグ	System re-start reason: system fatal error	Emergency	システムの致命的なエラー	
	System re-start reason: CPU exception	Emergency	CPU 例外	
DDM	Port < ポート番号 > SFP [しきい値タイプ] [超過タイプ] the [しきい値サブタイプ] alarm threshold	Critical	DDM アラームしきい値の超過、または回復	
	Port < ポート番号 > SFP[しきい値タイプ] [超過タイプ] the [しきい値サブタイプ] warning threshold	Warning	DDM 警告しきい値の超過、または回復	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
TFTP クライアント	Firmware upgrade by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC アドレス	Informational	ファームウェアのアップグレード成功。	
	Firmware upgrade by <session> was unsuccessful (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC アドレス	Warning	ファームウェアのアップグレード失敗。	
	Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC アドレス	Informational	ファームウェアのアップロード成功。	
	Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC アドレス	Warning	ファームウェアのアップロード失敗。	
	Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC 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 <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC 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 <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC 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 <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC 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 <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC アドレス	Informational	ログメッセージのアップロード成功。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
TFTP クライアント	Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション Username: 現在のログインユーザ Ipaddr: クライアント IP アドレス macaddr : クライアント MAC アドレス	Warning	ログメッセージのアップロード失敗。	
RCP	Firmware download by RCP successfully (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Informational	ファームウェアのダウンロード成功。	
	Firmware download by RCP fail ! (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	ファームウェアのダウンロード失敗。	
	Firmware upload by RCP successfully (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Informational	ファームウェアのアップロード成功。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
RCP	Firmware upload by RCP fail ! (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	ファームウェアのアップロード失敗。	
	Log Message: Firmware applied successfully (Username: <username>, IP <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Informational	ファームウェアの適用成功。	
	Log Message: Firmware apply fail ! (Username: <username>, IP <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	ファームウェアの適用失敗。	
	Log Message: Configuration download by RCP successfully (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Informational	CFG ダウンロード成功。	
	Log Message: Configuration download by RCP fail ! (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	CFG ダウンロード失敗。	
	Log Message: Configuration uploaded by RCP successfully (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Informational	CFG アップロード成功。	
	Log Message: Configuration upload by RCP fail ! (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	CFG アップロード失敗。	
	Log Message: configuration apply successfully (Username: <username>, IP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Informational	CFG の適用成功。	
	Log Message: configuration apply fail ! (Username: <username>, IP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	CFG の適用失敗。	
	Log Message: Log uploaded by RCP successfully (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Informational	ログのアップロード成功。	
	Log Message: Log upload by RCP fail ! (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	ログのアップロード失敗。	
	Log Message: Attack log uploaded by RCP successfully (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	攻撃ログのアップロード成功。	
	Log Message: Attack log upload by RCP fail ! (Username: <username>, RCP: <ipaddr>) username: ユーザ名 ipaddr : RCP サーバアドレス	Warning	攻撃ログのアップロード失敗。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
MSTP デバッグ拡張	Topology changed [([Instance:<InstanceID>] ,port : <portNum> [,MAC: <macaddr>])] InstanceID: インスタンス ID. portNum: ポート ID macaddr: MAC アドレス	Informational	トポロジ変更	
	[CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <InstanceID>] MAC:<macaddr>, Priority: <value>) InstanceID: インスタンス ID. macaddr: ルートブリッジの MAC アドレス value: ルートブリッジの優先度	Informational	新規ルートを選択	
	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	
	Spanning Tree instance create (Instance:<InstanceID>) InstanceID: インスタンス ID	Informational	スパニングツリーインスタンスが作成されました。	
	Spanning Tree instance delete (Instance:<InstanceID>) InstanceID: インスタンス ID	Informational	スパニングツリーインスタンスが削除されました。	
	Spanning Tree version changed.(new version:<new_version>) new_version: 新しい STP バージョン	Informational	スパニングツリーのバージョンが変更されました。	
	Spanning Tree MST configuration ID name and revision level changed (name:<name> revision level <revision_level>). name : 新しい名称 revision_level : 新しいリビジョンレベル	Informational	スパニングツリー MST コンフィグレーション ID 名とリビジョンが変更されました。	
	Spanning Tree MST configuration ID VLAN mapping table change (Instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]). InstanceID: インスタンス ID startvlanid- endvlanid : VLAN リスト	Informational	スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが削除されました。	
	Log Message: Spanning Tree MST configuration ID VLAN mapping table changed (Instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]). InstanceID: インスタンス ID startvlanid- endvlanid : VLAN リスト	Informational	スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが追加されました。	
	New root port selected [([Instance:<InstanceID>], port:<portNum>)] InstanceID: インスタンス ID portNum: ポート ID	Notice	新しいルートポート	
	Spanning Tree port status change [([Instance:<InstanceID>], port:<portNum>)] <old_status> -> <new_status> InstanceID: インスタンス ID portNum: ポート ID old_status: 古いステータス new_status: 新しいステータス	Notice	スパニングツリーポートステータスが変更されました。	
	Spanning Tree port role change [([Instance:<InstanceID>], port:<portNum>)] <old_role> -> <new_role> InstanceID: インスタンス ID portNum: ポート ID old_status: 古いロール new_status: 新しいロール	Informational	スパニングツリーポートロールが変更されました。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
ERPS	Signal fail detected on node <macaddr> macaddr: ノードのシステム MAC	Notice	信号のエラーを検出しました。	
	Signal fail cleared on node <macaddr> macaddr: ノードのシステム MAC	Notice	信号のエラーがクリアされました。	
	RPL owner conflicted on the ring <macaddr> macaddr: ノードのシステム MAC	Warning	RPL オーナが重複しています。	
LLDP MED	LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) portNum: ポート番号 chassisType: シャーシ ID サブタイプ 値のリスト : 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: シャーシ ID. portType: ポート ID サブタイプ 値のリスト : 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ポート ID deviceClass: LLDP-MED デバイスタイプ	Notice	LLDP-MED トポロジの変更が検出されました。	
	Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) portNum: ポート番号 chassisType: シャーシ ID サブタイプ 値のリスト : 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: シャーシ ID. portType: ポート ID サブタイプ 値のリスト : 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ポート ID deviceClass: LLDP-MED デバイスタイプ	Notice	LLDP-MED デバイスタイプの重複が検出されました。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
LLDP MED	Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) portNum: ポート番号 chassisType: シャーシ ID サブタイプ 値のリスト : 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: シャーシ ID. portType: ポート ID サブタイプ 値のリスト : 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ポート ID deviceClass: LLDP-MED デバイスタイプ	Notice	互換性のない LLDP-MED TLV が検出されました。	
CFM	CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <portNum>, Direction:<mepdirection>) Remote (MEPID:<mepid>, MAC:<macaddr>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection:「inward」または「outward」 mepid: MEP の MEPID macaddr: MEP の MAC アドレス	Critical	クロスコネクトが検出されました。	
	CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection:「inward」または「outward」 mepid: MEP の MEPID macaddr: MEP の MAC アドレス	Warning	エラー CFM CCM パケットが検出されました。	
	CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection:「inward」または「outward」	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:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection:「inward」または「outward」	Warning	リモート MEP の MAC がエラー状態をレポートしています。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
CFM	CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection:「inward」または「outward」	Informational	リモートの MEP が CFM の欠陥を検出しました。	
音声 VLAN	New voice device detected (MAC <macaddr>, Port <portNum>) portNum : ポート番号 macaddr: 音声デバイスの MAC アドレス	Informational	新しい音声 VLAN がポートに検出されました。	
	Port <portNum> add into voice VLAN <vid> portNum : ポート番号 vid: VLAN ID	Informational	自動音声 VLAN モードのポートを音声 VLAN に追加しました。	
	Port < portNum > remove from voice VLAN <vid > portNum : ポート番号 vid: VLAN ID	Informational	ポートが音声 VLAN から離脱し、同時にそのポートのエージングタイム内に音声 VLAN が見つからないとログメッセージを送信します。	
MAC ベースアクセスコントロール	MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <portNum>, VID: <vid>) macaddr: MAC アドレス portNum: ポート番号 vid: ホストが存在する VLAN ID	Critical	ホストは認証に失敗しました。	
	Port <portNum> enters MAC-based Access Control stop learning state. portNum: ポート番号	Warning	MAC ベースアクセス制御は学習停止状態に入りました。	ポートにおける認可ユーザ数が最大ユーザ数の制限に到達しました。
	Port <portNum> recovers from MAC-based Access Control stop learning state. portNum: ポート番号	Warning	MAC ベースアクセス制御は学習停止状態から回復しました。	ポートにおける認可ユーザ数は時間経過に存在する最大ユーザ数を下回っています。(間隔はプロジェクトによって異なります。)
	MAC-based Access Control enters stop learning state.	Warning	MAC ベースアクセス制御は学習停止状態に入りました。	デバイス全体の認可ユーザ数が最大ユーザ数に到達しました。
	MAC-based Access Control recovers from stop learning state.	Warning	MAC ベースアクセス制御は学習停止状態から回復しました。	ポートにおける認可ユーザ数は時間経過に存在する最大ユーザ数を下回っています。(間隔はプロジェクトによって異なります。)
	MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vid>) macaddr: MAC アドレス portNum: ポート番号 vid: ホストが存在する VLAN ID	Informational	ホストは認証を通過しました。	
	MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vid>) macaddr: MAC アドレス portNum: ポート番号 vid: ホストが存在する VLAN ID	Informational	ホストはエージングアウトします。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
802.1X	802.1X Authentication failure [for <reason>] from (Username: <username>, Port: <portNum>, MAC: <macaddr>) reason: 認証に失敗した理由 username: 認証されたユーザ portNum : ポート番号 macaddr: 認証されたデバイスの MAC アドレス	Warning	802.1X 認証の失敗。	
	8802.1X Authentication success from (Username: <username>, Port: <portNum>, MAC: <macaddr>) username: 認証されたユーザ portNum: ポート番号 macaddr: 認証されたデバイスの MAC アドレス	Informational	802.1X 認証の成功。	
AAA / SSH	Successful login through <Console | Telnet | Web | Web(SSL) | SSH>(Username: <username>, IP: <ipaddr | ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Informational	セッションからログインに成功。	コンソールの場合、IP アドレスはありません。
	Login failed through <Console | Telnet | Web | Web(SSL) |SSH> (Username: <username>, IP: <ipaddr | ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Warning	セッションからログインに失敗。	コンソールの場合、IP アドレスはありません。
	Logout through <Console | Telnet | Web | Web(SSL) | SSH> (Username: <username>, IP: <ipaddr | ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Informational	セッションからログアウトしました。	コンソールの場合、IP アドレスはありません。
	<Console | Telnet | Web | Web(SSL) | SSH> session timed out (Username: <username>, IP: <ipaddr | ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Informational	セッションタイムアウト	コンソールの場合、IP アドレスはありません。
	SSH server is enabled	Informational	SSH サーバ有効化	
	SSH server is disabled	Informational	SSH サーバ無効化	
	Login failed through <Console | Telnet | Web | Web(SSL) | SSH> [from <ipaddr | ipv6address>] due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Warning	AAA サーバのタイムアウトまたは不適切な設定のため、ログインに失敗。	文字列 "[from <ipaddr | ipv6address>]" はコンソールセッションにはありません。
	Enable Admin failed through <Console | Telnet | Web | Web(SSL) | SSH> [from <ipaddr | ipv6address>] due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Warning	AAA サーバのタイムアウトまたは不適切な設定のため、Enable Admin に失敗。	文字列 "[from <ipaddr | ipv6address>]" はコンソールセッションにはありません。

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
AAA / SSH	Enable Admin failed through <Console | Telnet | Web| Web(SSL) | SSH> [from <ipaddr |ipv6address>] authenticated by AAA < local | server <ipaddr | ipv6address>> (Username: <username>). local: AAA ローカル方式による enable admin server: AAA サーバ方式による enable admin ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Warning	AAA ローカルまたはサーバに認証されたセッション経由の Enable Admin に失敗。	文字列 "[from <ipaddr | ipv6address>]" はコンソールセッションにはありません。
	Successful Enable Admin through <Console | Telnet | Web | Web(SSL) | SSH> [from <ipaddr | ipv6address>] authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>). local: AAA ローカル方式による enable admin none: AAA none 方式による enable admin server: AAA サーバ方式による enable admin ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Informational	AAA ローカル、none、またはサーバにより認証されたセッション経由の Enable Admin に成功。	文字列 "[from <ipaddr | ipv6address>]" はコンソールセッションにはありません。
	Login failed through <Console | Telnet | Web | Web(SSL) | SSH> [from <ipaddr | ipv6address>] authenticated by AAA <local | server <ipaddr | ipv6address>> (Username: <username>). local: AAA ローカル方式を指定 server: AAA サーバ方式を指定 ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Warning	AAA ローカル、none、またはサーバにより認証されたセッション経由の Enable Admin に失敗。	文字列 "[from <ipaddr | ipv6address>]" はコンソールセッションにはありません。
	Successful login through <Console | Telnet | Web | Web(SSL) | SSH> [from < ipaddr | ipv6address >] authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>). local: AAA ローカル方式を指定 none: AAA none 方式を指定 server: AAA サーバ方式を指定 ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス	Informational	AAA ローカル、none、またはサーバにより認証されたセッション経由でログインに成功。	文字列 "[from <ipaddr | ipv6address>]" はコンソールセッションにはありません。
	Authentication Policy is enabled (Module: AAA)	Informational	認証ポリシーの有効化	
	Log Message: Authentication Policy is disabled (Module:AAA)	Informational	認証ポリシーの無効化	
ポートセキュリティ	Port security violation [([mac address:<macaddr>] on locking address full [port:< portNum>])] macaddr: MAC アドレス portNum: ポート番号	Warning	ポートにおけるアドレスフル	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
IMPB	Dynamic IMPB entry conflicts with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <portNum>) ipaddr: IP アドレス macaddr: MAC アドレス portNum : ポート番号	Warning	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 conflicts with static FDB(IP: [<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <portNum>) ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス portNum : ポート番号	Warning	ダイナミック IMPB エントリが、スタティック FDB とコンフリクトしています。	
IMPB	Dynamic IMPB entry conflicts with static IMPB(IP: [<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <portNum>). ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス portNum : ポート番号	Warning	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 being available(IP: [<ipaddr> | <ipv6addr>], MAC: <macaddr>, Port <portNum>) ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス portNum : ポート番号	Warning	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。	
	Unauthenticated IP-MAC address and discarded by IMPB (IP: [<ipaddr> | <ipv6addr>]], MAC :< macaddr >, Port <portNum >). ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス portNum : ポート番号	Warning	IMPB ホストの不正をチェックしました。	
	Dynamic IMPB entry conflicts with static NDP (IP: [< ipaddr > | < ipv6addr >], MAC: <macaddr>, Port <portNum>) ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス portNum : ポート番号	Information	ダイナミック IMPB エントリが、スタティック NDP とコンフリクトしています。	
BPDU アタック防御	Port <portNum> enter BPDU under protection state (mode: drop | block | shutdown) portNum : ポート番号 drop / block / shutdown: ログエントリにこれらの 1 つが存在します。	Informational	BPDU アタックが発生。	
	Port <portNum > recover from BPDU under protection state automatically portNum : ポート番号	Informational	BPDU アタックは自動的に回復。	
	Port <portNum > recover from BPDU under protection state manually portNum : ポート番号	Informational	BPDU アタックは手動で回復。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
WAC	WAC unauthenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>) string: ユーザ名 ipaddr: IP アドレス macaddr: MAC アドレス portNum : ポート番号	Warning	クライアントホストは認証に失敗しました。	
	WAC enters stop learning state.	Warning	WAC は学習停止状態に入りました。	認可ユーザ数がデバイス全体で最大ユーザ数の制限に到達した場合にこのログが発生します。
	WAC recovers from stop learning state.	Warning	WAC は学習停止状態から回復しました。	時間経過後認可ユーザ数が最大ユーザ数を下回るとこのログが発生します。（間隔はプロジェクトによって異なります。）
JWAC	WAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>) string: ユーザ名 ipaddr: IP アドレス macaddr: MAC アドレス portNum : ポート番号	Warning	クライアントホストが認証に成功。	
	JWAC unauthenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>). string: ユーザ名 ipaddr: IP アドレス macaddr: MAC アドレス portNum : ポート番号	Warning	クライアントホストが認証に失敗。	
	JWAC enters stop learning state.	Warning	JWAC は学習停止状態に入りました。	認可ユーザ数がデバイス全体で最大ユーザ数の制限に到達した場合にこのログが発生します。
	Log Message: JWAC recovers from stop learning state.	Warning	JWAC は学習停止状態から回復しました。	時間経過後認可ユーザ数が最大ユーザ数を下回るとこのログが発生します。（間隔はプロジェクトによって異なります。）
ループバック検知（LBD）	Port < portNum> LBD loop occurred. Port blocked. portNum: ポート番号	Critical	ポートベースモードでループが発生しました。	
	Port< portNum> LBD port recovered. Loop detection restarted portNum: ポート番号	Informational	ポートベースモードで LBD ブロック状態からポートは回復しました。	
	Port <portNum> VID <vlanID> LBD loop occurred. Packet discard begun portNum: ポート番号 vlanID: the VLAN ID	Critical	VLAN ベースモードでループが発生しました。	
	Port < portNum> VID <vlanID> LBD recovered. Loop detection restarted portNum: ポート番号 vlanID: the VLAN ID	Informational	VLAN ベースモードで LBD ブロック状態からポートは回復しました。	
	Loop VLAN number overflow.	Informational	ループバックが発生した VLAN の番号が指定番号と一致しました。。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
トラフィックコントロール	Port <portNum> Broadcast storm is occurring. portNum: ポート番号	Warning	ブロードキャストストームが発生。	
	Port <portNum> Broadcast storm has cleared. portNum: ポート番号	Informational	ブロードキャストストームが解消。	
	Log Message: Port <portNum> Multicast storm is occurring. portNum: ポート番号	Warning	マルチキャストストームが発生。	
	Port <portNum> Multicast storm has cleared. portNum: ポート番号	Informational	マルチキャストストームが解消。	
	Port <portNum> is currently shut down due to a packet storm portNum: ポート番号	Warning	パケットストームによるポートのシャットダウン	
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がノーマルモードに入りました。	
	Safeguard Engine enters EXHAUSTED mode	Warning	セーフガードエンジンがパケットフィルタリングモードに入りました。	
IP とパスワードの変更	Password was changed by console (Username: <username>) username: ユーザ名	Informational	パスワード変更のアクティビティ	
DoS 攻撃機能	Possible spoofing attack from IP: <ipaddr>, MAC: <macaddr>, port: <portNum> ipaddr: IP アドレス macaddr: MAC アドレス portNum : ポート番号	Critical	Spoofing 攻撃 1. 送信元がスイッチのインタフェースの IP と同じであるが、送信元 MAC が異なる。 2. 送信元が ARP パケット内のスイッチの IP と同じ。 3. 自身の IP パケットを検出。	
Gratuitous ARP	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: < intf-name>) ipaddr: IP アドレス macaddr: MAC アドレス portNum : ポート番号 intf-name: インタフェース名	Informational	IP コンフリクトの検出	
DHCP サーバスクリーニング	Detected untrusted DHCP server(IP: <ipaddr>, Port <portNum>) ipaddr: デバイスに検出した信頼性の低い IP アドレス portNum : デバイスの論理ポート番号	Informational	信頼性の低い DHCP サーバの IP アドレスを検出。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
OSPF デバッグ拡張	OSPF interface <intf-name> changed state to <Up | Down> intf-name: OSPF インタフェース名	Informational	OSPF インタフェースのリンクステートの変更。	
	OSPF protocol on interface <intf-name> changed state to <Enabled | Disabled> intf-name: OSPF インタフェース名	Informational	OSPF インタフェースの管理ステートの変更。	
	OSPF interface <intf-name> changed from area <area-id> to area <area-id> intf-name: OSPF インタフェース名 area-id: OSPF エリア ID	Notice	OSPF インタフェースが別のエリアに変更。	
	OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full intf-name: OSPF インタフェース名 nbr-id: Neighbor ルータ ID	Notice	OSPF Neighbor ステートが Loading から Full に変更。	
	OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down intf-name: OSPF インタフェース名 nbr-id: Neighbor's router ID	Notice	OSPF Neighbor ステートが Full から Down に変更。	
	Log Message: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired intf-name: OSPF インタフェース名 nbr-id: Neighbor ルータ ID	Notice	OSPF Neighbor ステートの dead タイマの期限切れ。	
	OSPF nbr <nbr-id> on virtual link changed state from Loading to Full nbr-id: Neighbor ルータ ID	Notice	OSPF 仮想 Neighbor ステートが Loading から Full に変更。	
	OSPF nbr <nbr-id> on virtual link changed state from Full to Down nbr-id: Neighbor ルータ ID	Notice	OSPF 仮想 Neighbor ステートが Full から Down に変更。	
	OSPF router ID changed to <router-id> router-id: OSPF ルータ ID	Informational	OSPF ルータ ID の変更。	
	OSPF state changed to Enabled	Informational	OSPF の有効化。	
	OSPF state changed to Disabled	Informational	OSPF の無効化。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
VRRP デバッグ拡張	VR <vr-id> at interface <intf-name> switch to Master vr-id: VRRP 仮想ルータ ID intf-name: 仮想ルータがベースとなるインタフェース名	Informational	1 つの仮想ルータがマスタに変更。	
	VR <vr-id> at interface <intf-name> switch to Backup vr-id: VRRP 仮想ルータ ID intf-name: 仮想ルータがベースとなるインタフェース名	Informational	1 つの仮想ルータがバックアップに変更。	
	VR <vr-id> at interface <intf-name> switch to Init. vr-id: VRRP 仮想ルータ ID intf-name: 仮想ルータがベースとなるインタフェース名	Informational	1 つの仮想ルータのステートが Init に変更。	
	Authentication type mismatch on VR <vr-id> at interface <intf-name>. vr-id: VRRP 仮想ルータ ID intf-name: 仮想ルータがベースとなるインタフェース名	Warning	受信した VRRP 通知メッセージの認証タイプの不一致。	
	Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type>. vr-id: VRRP 仮想ルータ ID intf-name: 仮想ルータがベースとなるインタフェース名 Auth-type: VRRP インタフェース認証タイプ	Warning	受信した VRRP 通知メッセージの認証チェックの失敗。	
	Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name>. vr-id: VRRP 仮想ルータ ID intf-name: 仮想ルータがベースとなるインタフェース名	Warning	受信した VRRP 通知メッセージの Checksum エラー。	
	Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name>. vr-id: VRRP 仮想ルータ ID intf-name: 仮想ルータがベースとなるインタフェース名	Warning	受信した VRRP 通知メッセージの仮想ルータ ID の不一致。	
	Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name>. vr-id: VRRP 仮想ルータ ID intf-name: 仮想ルータがベースとなるインタフェース名	Warning	受信した VRRP 通知メッセージの通知間隔の不一致。	
	Added a virtual MAC <vrrp-mac-addr> into L2 table. vrrp-mac-addr: VRRP 仮想 MAC アドレス	Notice	仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。	
	Deleted a virtual MAC <vrrp-mac-addr> from L2 table. vrrp-mac-addr: VRRP 仮想 MAC アドレス	Notice	仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。	
	Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. vrrp-ip-addr: VRRP 仮想 IP アドレス vrrp-mac-addr: VRRP 仮想 MAC アドレス	Notice	仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。	
	Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table. vrrp-ip-addr: VRRP 仮想 IP アドレス vrrp-mac-addr: VRRP 仮想 MAC アドレス	Notice	仮想 MAC アドレスがスイッチの L3 テーブルから削除されました。	
	Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode>. vrrp-mac-addr: VRRP 仮想 MAC アドレス vrrp-errcode: VRRP プロトコルの動作に関するエラーコード	Error	スイッチチップの L2 テーブルへの仮想 MAC の追加に失敗しました。	
	Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode>. vrrp-mac-addr: VRRP 仮想 MAC アドレス vrrp-errcode: VRRP プロトコルの動作に関するエラーコード	Error	スイッチチップの L2 テーブルから仮想 MAC の削除に失敗しました。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
VRRP デバッグ拡張	Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full. vrrp-ip-addr: VRRP 仮想 IP アドレス vrrp-mac-addr: VRRP 仮想 MAC アドレス	Error	スイッチチップの L3 テーブルへの仮想 MAC の追加に失敗しました。L3 テーブルはフルです。	
	Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid. vrrp-ip-addr: VRRP 仮想 IP アドレス vrrp-mac-addr: VRRP 仮想 MAC アドレス mac-port: VRRP 仮想 MAC のポート番号	Error	スイッチの L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したポートは不正です。	
	Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid. vrrp-ip-addr: VRRP 仮想 IP アドレス vrrp-mac-addr: VRRP 仮想 MAC アドレス mac-intf: VRRP 仮想 MAC アドレスがベースになるインタフェース番号	Error	スイッチの L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したインタフェースは不正です。	
	Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid. vrrp-ip-addr: VRRP 仮想 IP アドレス vrrp-mac-addr: VRRP 仮想 MAC アドレス mac-box: VRRP 仮想 MAC のスタックボックス番号	Error	スイッチの L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したボックスは不正です。	
	Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> vrrp-ip-addr: VRRP 仮想 IP アドレス vrrp-mac-addr: VRRP 仮想 MAC アドレス vrrp-errcode: VRRP プロトコルの動作に関するエラーコード	Error	スイッチチップの L3 テーブルへの仮想 MAC の追加に失敗しました。	
	Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode>. vrrp-ip-addr: VRRP 仮想 IP アドレス vrrp-mac-addr: VRRP 仮想 MAC アドレス vrrp-errcode: VRRP プロトコルの動作に関するエラーコード	Error	スイッチチップの L3 テーブルから仮想 MAC の削除に失敗しました。	
CFM 拡張	[CFM_EXT(1):]AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection: MEP の方向（「inward」または「outward」） mepid: MEP の MEPID	Notice	AIS 状態が検出されました。	
	[CFM_EXT(2):]AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection: MEP の方向（「inward」または「outward」） mepid: MEP の MEPID	Notice	AIS 状態がクリアされました。	
	[CFM_EXT(3):]LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection: MEP の方向（「inward」または「outward」） mepid: MEP の MEPID	Notice	LCK 状態が検出されました。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
CFM 拡張	[CFM_EXT(4):]LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル portNum: MEP の論理ポート番号 mepdirection: MEP の方向（「inward」または「outward」） mepid: MEP の MEPID	Notice	LCK 状態がクリアされました。	
DULD	Port: <portNum> is unidirectional. portNum : ポート番号	Informational	単方向リンクがこのポートで検出されました。	
SRM	The SRM mode has been changed to <srm_mode> srm_mode: SRM モード（Routing または VPWS）	Informational	SRM モードの変更	
RADIUS	RADIUS server <ipaddr> assigned VID :<vlanID> to port <portNum> (account :<username>) ipaddr: RADIUS サーバの IP アドレス vlanID: RADIUS 割り当てた VLAN の VID portNum : ポート番号 Username: 認証されるユーザ	Informational	RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから VID が割り当てられました。この VID はポートに割り当てられ、このポートは VLAN タグなしメンバになります。	
	RADIUS server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <portNum> (account : <username>) ipaddr: RADIUS サーバの IP アドレス ingressBandwidth: 割り当てる RADIUS のイングレス帯域 portNum : ポート番号 Username: 認証されるユーザ	Informational	RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバからイングレス帯域が割り当てられました。このイングレス帯域はポートに割り当てられます。	
	RADIUS server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <portNum> (account: <username>) ipaddr: RADIUS サーバの IP アドレス egressBandwidth: 割り当てる RADIUS のイーグレス帯域 portNum : ポート番号 Username: 認証されるユーザ	Informational	RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバからイーグレス帯域が割り当てられました。このイーグレス帯域はポートに割り当てられます。	
	RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <portNum> (account : <username>) ipaddr: RADIUS サーバの IP アドレス priority: 割り当てる RADIUS の優先度 portNum : ポート番号 Username: 認証されるユーザ	Informational	RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから 802.1p デフォルトプライオリティが割り当てられました。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。	
	RADIUS server <ipaddr> assigns <username> ACL failure at port <portNum> (<string>) ipaddr: RADIUS サーバの IP アドレス portNum : ポート番号 Username: 認証されるユーザ string: エラーとなった RADIUS ACL コマンドストリング	Warning	RADIUS サーバによる ACL プロファイル / ルールの割り当てに失敗しました。	
DHCPv6 Relay	[DHCPv6_RELAY(1):]DHCPv6 relay on interface <intf-name> changed state to <enabled | disabled> intf-name: DHCPv6 リレーエージェントインタフェース名	Informational	指定管理インタフェースの DHCPv6 リレーの状態変更	
VPWS	Pseudowire <vc_id> link down. vc_id: リンクダウンしている pseudowire ID	Informational	Pseudowire リンクダウン	
	Pseudowire <vc_id> link up. vc_id: リンクアップしている pseudowire ID	Informational	Pseudowire リンクアップ	
	Pseudowire <vc_id> is deleted. vc_id: 削除された pseudowire ID	Informational	Pseudowire は削除されました。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
LDP	Log Message: Session of peer <lsrid> initialization exceeded threshold < threshold > lsrid: ピアの LSR ID threshold: LDP セッション初期化のしきい値	Informational	セッション初期化メッセージの数が「mplsLdpEntityInitSessionThreshold」の値を超過しました。	
	LDP entity path vector limit <value> does not match the peer <lsrid> path vector limit <value> lsrid: ピアの LSR ID value: パスベクトル制限	Informational	パスベクトル制限の不一致	
	LDP session of peer <lsrid> is operational lsrid: ピアの LSR ID	Informational	LDP セッションは操作状態に入りました。	
	LDP session of peer <lsrid> restart lsrid: ピアの LSR ID	Informational	LDP セッションが再開しました。	
MPLS	LSP <lsp_id> is up lsp_id: 確立した LSP ID	Informational	LSP がアップしました。	
	LSP <lsp_id> is down lsp_id: 削除された LSP ID	Informational	LSP がダウンしました。	
RIPng	RIPng protocol on interface < インタフェース名 > changed state to <enabled | disabled>	Informational	インタフェースの RIPng 状態が変更されました。	

付録 D トラップログ

本製品では、以下のトラップログが検出されます。

カテゴリ	トラップ名	説明	摘要
SNMP	coldStart/1.3.6.1.6.3.1.1.5.1	coldStart トラップは、通知を生成するアプリケーションをサポートする SNMP エンティティが自身を再初期化し、そのコンフィグレーションを変更する可能性があることを示します。	(RFC1907 SNMPv2-MIB)
	warmStart/1.3.6.1.6.3.1.1.5.2	warmStart トラップは、通知を生成するアプリケーションをサポートする SNMP エンティティが自身を再初期化し、そのコンフィグレーションを変更しないことを示します。	(RFC1907 SNMPv2-MIB)
	linkDown/1.3.6.1.6.3.1.1.5.3	linkDown トラップは、通信リンクの 1 つに対する ifOperStatus オブジェクトが他のステートからダウンステートに入ったことをエージェントロールで動作する SNMP エンティティが検出したことを示します。この他のステートは ifOperStatus に含まれる値によって示されます。 関連オブジェクト : (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	(RFC2233 IF-MIB)
	linkUp/1.3.6.1.6.3.1.1.5.4	linkUp トラップは、通信リンクの 1 つに対する ifOperStatus オブジェクトがダウンステートから他のステートに入ったことをエージェントロールで動作する SNMP エンティティが検出したことを示します。この他のステートは ifOperStatus に含まれる値によって示されます。 関連オブジェクト : (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	(RFC2233 IF-MIB)
	authenticationFailure /1.3.6.1.6.3.1.1.5.5	authenticationFailure トラップは、SNMP エンティティが適切に認証されていないプロトコルメッセージを受信したことを示します。	(RFC1907 SNMPv2-MIB)

カテゴリ	トラップ名	説明	摘要
Bridge MIB	newRoot/1.3.6.1.2.1.17.0.1	newRoot トラップは、送信側のエージェントがスパニングツリーの新しいルートになったことを示します	
	topologyChange/1.3.6.1.2.1.17.0.2	topologyChange トラップは、構成するいずれかのポートが Learning 状態から Forwarding 状態に、Forwarding 状態から Blocking 状態に、または Forwarding 状態から Blocking 状態に遷移する場合にブリッジによって送信されます。	
OAM	dot3OamNonThresholdEvent /1.3.6.1.2.1.158.0.2	ローカルまたはリモートのしきい値のないクロスイベントが検出された場合に dot3OamNonThresholdEvent が送信されます。ローカルイベントはローカルエンティティによって検出され、リモートイベントはしきい値のないクロスイベントを示すイーサネット OAM イベント通知 OAMPDU の受信により検出されます。 関連オブジェクト : (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType （次の値のみサポート : dyingGaspEvent(257)） (4) dot3OamEventLogLocation (5) dot3OamEventLogEventTotal	(ie8023ah.mib)
MAC ベースアクセスコントロール	swMacBasedAccessControlLoggedSuccess /1.3.6.1.4.1.171.12.35.11.1.0.1	MAC ベースアクセスコントロールホストがログインに成功した場合に本トラップを送信します。 関連オブジェクト : (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID	
	swMacBasedAccessControlLoggedFail /1.3.6.1.4.1.171.12.35.11.1.0.2	MAC ベースアクセスコントロールホストがログインに失敗した場合に本トラップを送信します。 関連オブジェクト : (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID	
MAC ベースアクセスコントロール	swMacBasedAccessControlAgesOut /1.3.6.1.4.1.171.12.35.11.1.0.3	MAC ベースアクセスコントロールホストがエージングを行った場合に本トラップを送信します。 関連オブジェクト : (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID	
RMON (RFC2819.mib)	risingAlarm/1.3.6.1.2.1.16.0.1	SNMP トラップは、高性能のアラームエントリがしきい値の上限を超えて、SNMP トラップを送信するために設定されているイベントを生成する場合に生成されます。 関連オブジェクト : (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	
	fallingAlarm/1.3.6.1.2.1.16.0.2	SNMP トラップは、高性能のアラームエントリがしきい値の下限を超えて、SNMP トラップを送信するために設定されているイベントを生成する場合に生成されます。 関連オブジェクト : (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	

カテゴリ	トラップ名	説明	摘要
LLDP (lldp.mib)	lldpRemTablesChange/ 1.0.8802.1.1.2.0.0.1	lldpRemTablesChange 通知は、lldpStatsRemTableLastChangeTime の値が変更した場合に送信されます。LLDP リモートシステムテーブルのメンテナンスポーリングを引き起こすように NMS によって利用されます。 関連オブジェクト : (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	
LLDP-MED	lldpXMedTopologyChangeDetected /1.0.8802.1.1.2.1.5.4795.0.1	新しいリモートデバイスがローカルポートに割り当てられたこと、またはリモートデバイスが切断またはあるポートから別のポートに移動したことを示すトポロジの変化に気づいたローカルデバイスによって生成される通知。 関連オブジェクト : (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	
ポートセキュリティ	swL2PortSecurityViolationTrap /1.3.6.1.4.1.171.11.115.1.2.2.100.1.2.0.2	ポートセキュリティトラップが有効な場合、定義済みのポートセキュリティ設定に違反する新しい MAC アドレスがあると、トラップメッセージを送信します。 関連オブジェクト : (1) swPortSecPortIndex (2) swL2PortSecurityViolationMac	
FDB	swL2macNotification /1.3.6.1.4.1.171.11.115.1.2.2.100.1.2.0.1	本トラップはアドレステーブル内のMACアドレスの変化を示します。 関連オブジェクト : (1) swL2macNotifyInfo	
周辺機器	swHighTemperature /1.3.6.1.4.1.171.12.11.2.2.4.0.1	高温の場合。 関連オブジェクト : (1) swTemperatureUnitIndex (2) swTemperSensorID (3) swTemperatureCurrent	

カテゴリ	トラップ名	説明	摘要
周辺機器	swHighTemperatureRecover /1.3.6.1.4.1.171.12.11.2.2.4.0.2	高温から回復した場合。 関連オブジェクト : (1) swTemperatureUnitIndex (2) swTemperSensorID (3) swTemperatureCurrent	
	swLowTemperature / 1.3.6.1.4.1.171.12.11.2.2.4.0.3	低温の場合。 関連オブジェクト : (1) swTemperatureUnitIndex (2) swTemperSensorID (3) swTemperatureCurrent	
	swLowTemperatureRecover /1.3.6.1.4.1.171.12.11.2.2.4.0.4	低温から回復した場合。 関連オブジェクト : (1) swTemperatureUnitIndex (2) swTemperSensorID (3) swTemperatureCurrent	
	swPowerStatusChg /1.3.6.1.4.1.171.12.11.2.2.2.0.1	電源状態が変化した場合。 関連オブジェクト : (1) swPowerUnitIndex (2) swPowerID (3) swPowerStatus	
	swPowerFailure /1.3.6.1.4.1.171.12.11.2.2.2.0.2	電源エラーの場合。 関連オブジェクト : (1) swPowerUnitIndex (2) swPowerID (3) swPowerStatus	
	swPowerRecover /1.3.6.1.4.1.171.12.11.2.2.2.0.3	電源回復時。 関連オブジェクト : (1) swPowerUnitIndex (2) swPowerID (3) swPowerStatus	
セーフガード	swSafeGuardChgToExhausted /1.3.6.1.4.1.171.12.19.4.1.0.1	システムが「normal」から「exhausted」に操作モードを変更したことを示します。 関連オブジェクト : (1) swSafeGuardCurrentStatus	
	swSafeGuardChgToNormal /1.3.6.1.4.1.171.12.19.4.1.0.2	システムが「exhausted」から「normal」に操作モードを変更したことを示します。 関連オブジェクト : (1) swSafeGuardCurrentStatus	
トラフィックコントロール	swPktStormOccurred /1.3.6.1.4.1.171.12.25.5.0.1	パケットストームメカニズムがパケットストームを検出し、アクションとしてシャットダウンする場合に本トラップを送信します。 関連オブジェクト : (1) swPktStormCtrlPortIndex	
	swPktStormCleared /1.3.6.1.4.1.171.12.25.5.0.2	パケットストームメカニズムがパケットストームをクリアした場合に本トラップを送信します。 関連オブジェクト : (1) swPktStormCtrlPortIndex	

カテゴリ	トラップ名	説明	摘要
IMPB	swIpMacBindingViolation Trap/ /1.3.6.1.4.1.171.12.23.5.0.1	IMPB トラップが有効な場合、定義済みのポートセキュリティ設定に違反する新しい MAC があると、トラップが送信されます。 関連オブジェクト : (1) swIpMacBindingPortIndex (2) swIpMacBindingViolationIP (3) swIpMacBindingViolationMac	
	swIpMacBindingIPv6ViolationTrap/ 1.3.6.1.4.1.171.12.23.5.0.4	IP-MAC バインディングトラップが有効な場合、定義済みのポートセキュリティ設定に違反する新しい MAC があると、トラップが送信されます。 関連オブジェクト : (1) swIpMacBindingPortIndex (2) swIpMacBindingViolationIPv6Addr (3) swIpMacBindingViolationMac	
Gratuitous ARP	agentGratuitousARPTrap /1.3.6.1.4.1.171.12.1.7.2.0.5	IP アドレスの重複があると、本トラップは送信されます。 関連オブジェクト : (1) agentGratuitousARPIpAddr (2) agentGratuitousARPMacAddr (3) agentGratuitousARPPortNumber (4) agentGratuitousARPInterfaceName	
DHCP サーバスクリーニング	swFilterDetectedTrap /1.3.6.1.4.1.171.12.37.100.0.1	不正な DHCP サーバを検出すると、本トラップは送信されます。ログ取得を停止する未許可期間に検出された同じ不正な DHCP サーバの IP アドレスをトラップ送信先に一度だけ送信します。 関連オブジェクト : (1) swFilterDetectedIP (2) swFilterDetectedport	
LBD	swPortLoopOccurred /1.3.6.1.4.1.171.12.41.10.0.1	ポートにループが発生すると、本トラップを送信します。 関連オブジェクト : (1) swLoopDetectPortIndex	
	swPortLoopRestart /1.3.6.1.4.1.171.12.41.10.0.2	ポートにループが一定間隔後に再度発生すると、本トラップを送信します。 関連オブジェクト : (1) swLoopDetectPortIndex	
	swVlanLoopOccurred /1.3.6.1.4.1.171.12.41.10.0.3	LBD VLAN ベースモードでポートにループが発生すると、本トラップを送信します。 関連オブジェクト : (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	
	swVlanLoopRestart /1.3.6.1.4.1.171.12.41.10.0.4	LBD VLAN ベースモードでポートにループが一定間隔後に再度発生すると、本トラップを送信します。 関連オブジェクト : (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	

カテゴリ	トラップ名	説明	摘要
BPDU 攻撃防御	swBpduProtectionUnderAttackingTrap /1.3.6.1.4.1.171.12.76.4.0.1	BPDU トラップが有効な場合、指定ポートが「normal」から「attack」ステートに変更すると、トラップが送信されます。 関連オブジェクト : (1) swBpduProtectionPortIndex (2) swBpduProtectionPortMode	
	swBpduProtectionRecoveryTrap /1.3.6.1.4.1.171.12.76.4.0.2	BPDU 保護トラップが有効な場合、指定ポートが「attack」から「normal」ステートに変更すると、トラップが送信されます。 関連オブジェクト : (1) swBpduProtectionPortIndex (2) (2)swBpduProtectionRecoveryMethod	
ERPS	swERPSSFDetectedTrap /1.3.6.1.4.1.171.12.78.4.0.1	信号障害の発生時にトラップは生成されます。 関連オブジェクト : (1) swERPSNodeId	
ERPS	swERPSSFClearedTrap /1.3.6.1.4.1.171.12.78.4.0.2	信号障害が解消するとトラップは生成されます。 関連オブジェクト : (1) swERPSNodeId	
	swERPSRPLOwnerConflictTrap /1.3.6.1.4.1.171.12.78.4.0.3	コンフリクトの発生時にトラップは生成されます。 関連オブジェクト : (1) swERPSNodeId	
CFM	dot1agCfmFaultAlarm /1.3.111.2.802.1.1.8.0.1	MEP に持続的な欠損条件があります。通知（故障警報）は故障を検出した MEP の OID を持つ管理エンティティに送信されます。 関連オブジェクト : (1)dot1agCfmMepHighestPrDefect	
CFM 拡張	swCFMExtAISOccurred / 1.3.6.1.4.1.171.12.86.100.0.1	通知は、ローカル MEP が AIS ステータスに入ると生成されます。 関連オブジェクト : (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
	swCFMExtAISCleared / 1.3.6.1.4.1.171.12.86.100.0.2	通知は、ローカル MEP が AIS ステータスから出ると生成されます。 関連オブジェクト : (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
	swCFMExtLockOccurred / 1.3.6.1.4.1.171.12.86.100.0.3	通知は、ローカル MEP が Lock ステータスに入ると生成されます。 関連オブジェクト : (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
	swCFMExtLockCleared / 1.3.6.1.4.1.171.12.86.100.0.4	通知は、ローカル MEP が Lock ステータスから出ると生成されます。 関連オブジェクト : (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	
MPLS	mplsXCUp /1.3.6.1.2.1.10.166.2.0.1	通知は、mplsXCTable 内の 1 つ以上の連続する mplsXCOperStatus オブジェクトがアップ状態から他の状態に入ると生成されます。	
	mplsXCDown /1.3.6.1.2.1.10.166.2.0.2	通知は、mplsXCTable 内の 1 つ以上の連続する mplsXCOperStatus オブジェクトがダウン状態から他の状態に入ると生成されます。	

カテゴリ	トラップ名	説明	摘要
LDP	mplsLdpInitSessionThresholdExceeded /1.3.6.1.2.1.10.166.4.0.1	通知は、セッション初期化メッセージの数が「mplsLdpEntityInitSessionThreshold」の値を超過すると生成されます。	
	mplsLdpPathVectorLimitMismatch /1.3.6.1.2.1.10.166.4.0.2	通知は、「mplsLdpEntityPathVectorLimit」が指定エンティティのセッション初期化メッセージの「mplsLdpPeerPathVectorLimit」の値に一致しないと送信されます。	
	mplsLdpSessionUp /1.3.6.1.2.1.10.166.4.0.3	通知は、「mplsLdpSessionState」の値が「operational(5)」状態に入ると送信されます。	
	mplsLdpSessionDown /1.3.6.1.2.1.10.166.4.0.4	通知は、「mplsLdpSessionState」の値が「operational(5)」状態から出ると送信されます。	
VPWS	pwUp /1.3.6.1.2.1.10.246.0.1	通知は、pwTable にある 1 つ以上の連続するエントリに対する pwOperStatus オブジェクトが notPresent(5) 状態の場合、およびこれらのエントリに対して pwDown 通知が発行されている場合を除き、他の状態から「up(1)」状態に入った場合に生成されます。	
	pwDown /1.3.6.1.2.1.10.246.0.2	通知は、pwTable にある 1 つ以上の連続するエントリに対する pwOperStatus オブジェクトが notPresent(5) 状態を除き、他の状態から down(2) または lowerLayerDown(6) 状態に入った場合に生成されます。	
	pwDeleted /1.3.6.1.2.1.10.246.0.3	通知は、PW が削除された場合（つまり、pwRowStatus が destroy(6) に設定された場合、または PW が non-MIB アプリケーションもしくは自動検出処理によって削除された場合）に生成されます。	

付録 E パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減

ARP を動作させる方法

ARP（Address Resolution Protocol）は、IP アドレスだけがわかっている場合にホストのハードウェアアドレス（MAC アドレス）を検索するための標準的な方法です。しかし、クラッカーが ARP パケット内の IP および MAC 情報を偽造して LAN への攻撃（ARP スプーフィングとして、知られている）を行うために、このプロトコルは被害を受けやすいと言えます。ここでは ARP プロトコル、ARP スプーフィング攻撃、および D-Link スイッチが提供する ARP スプーフィング攻撃を防御する対策について紹介します。

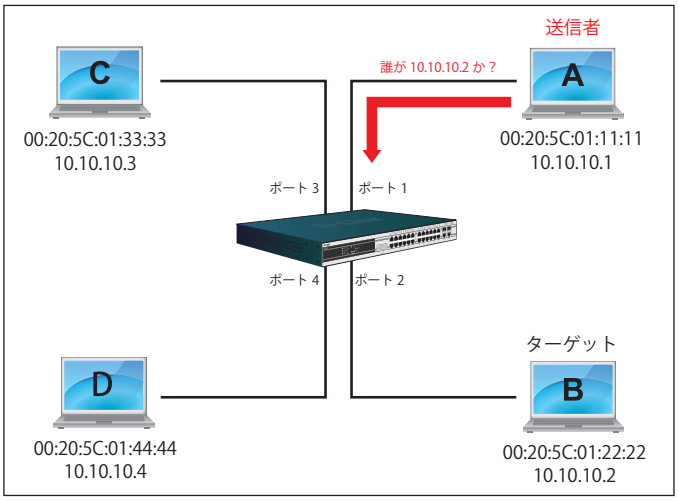


図 E-1　ARP の動作方法

ARP 処理中に、PC-A は、はじめに、PC-B の MAC アドレスを問い合わせする ARP リクエストを発行します。そのネットワーク構造は図 E-1 の通りです。

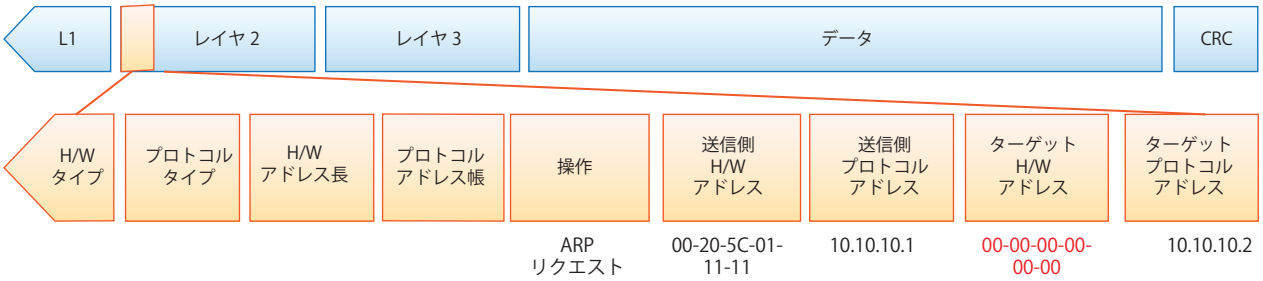


図 E-2　ARP ペイロード

ARP リクエストはイーサネットフレームにカプセル化されて送信されます。図 E-2 の通り、イーサネットフレーム内の「送信元アドレス」は、PC-A の MAC アドレスとなります。ARP リクエストは、ブロードキャスト経由で送信されるため、イーサネットのブロードキャスト（FF-FF-FF-FF-FF-FF）のフォーマットには「宛先アドレス」があります。

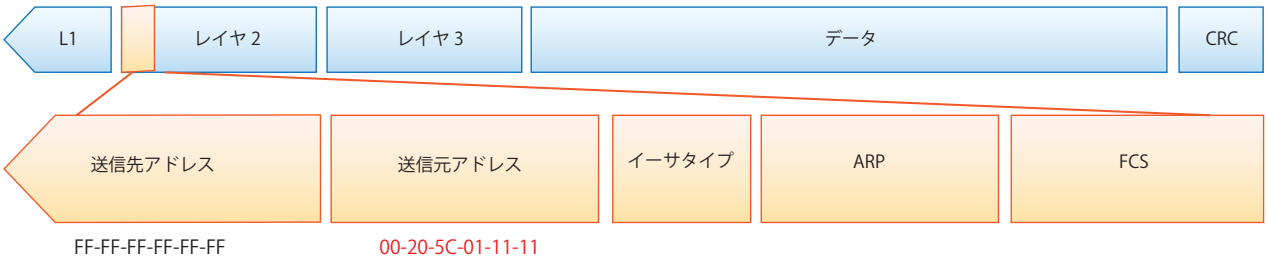


図 E-3　イーサネットフレームフォーマット

スイッチがフレームを受信すると、イーサネットフレームヘッダの「送信元アドレス」をチェックします。アドレスがフォワーディングテーブルにないと、スイッチは学習して PC-A の MAC アドレスと関連ポートをフォワーディングテーブルに追加します。

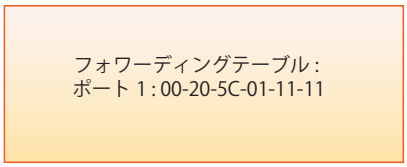


図 E-4　フォワーディングテーブル

さらに、スイッチがブロードキャストされた ARP リクエストを受信すると、送信元ポート（図 E-5 ではポート 1）を除くすべてのポートにフレームをフラッドします。

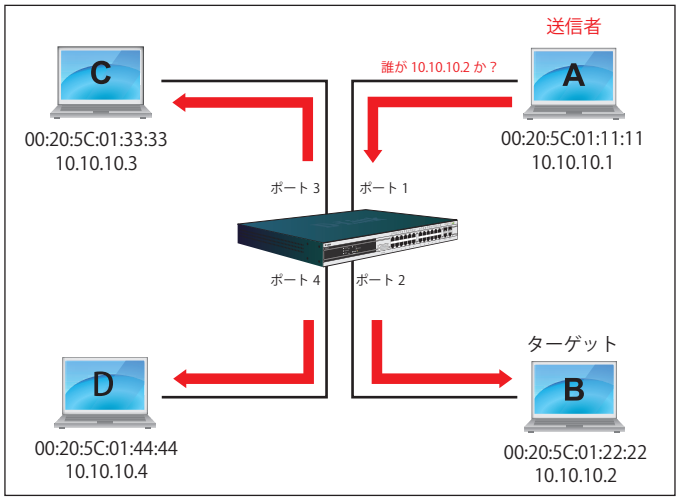


図 E-5　ポートフラッド画面

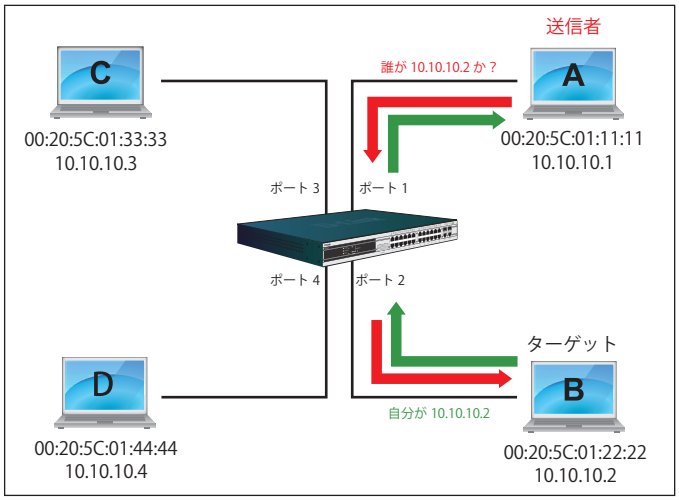


図 E-6　パケットコンテンツ ACL 画面

スイッチが ARP リクエストのフレームをネットワークにフラッドする場合、すべての PC が、フレームを受信し、検証を行いますが、PC-B だけが宛先 IP に一致するためにクエリに応答します（図 E-6 参照）。

PC-B が ARP リクエストに応答すると、その MAC アドレスは図 E-7 に示されている ARP ペイロード内の「ターゲット H/W アドレス」に書かれます。ARP リプライは、次に、再びイーサネットフレームにカプセル化されて、送信側に返送されます。ARP リプライはユニキャスト通信の形式です。

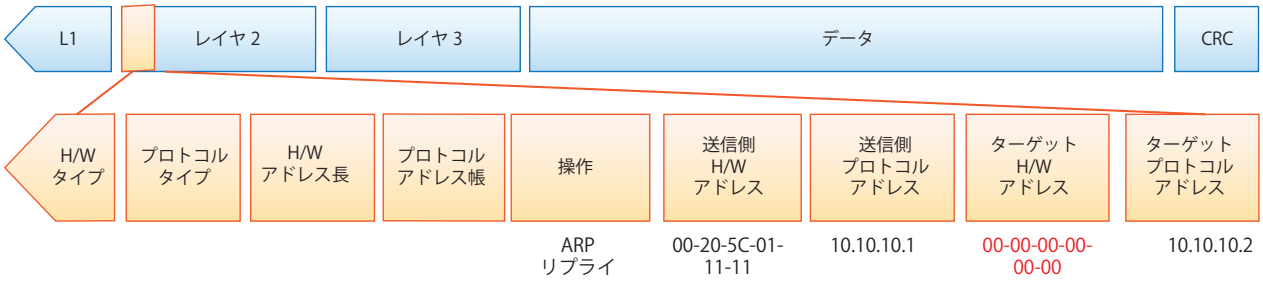


図 E-7　ARP ペイロード

PC-B がクエリに応答する場合、イーサネットフレーム内の「宛先アドレス」は、PC-A の MAC アドレスに変更されます。「送信元アドレス」は PC-B の MAC アドレスに変更されます（図 E-8 参照）。

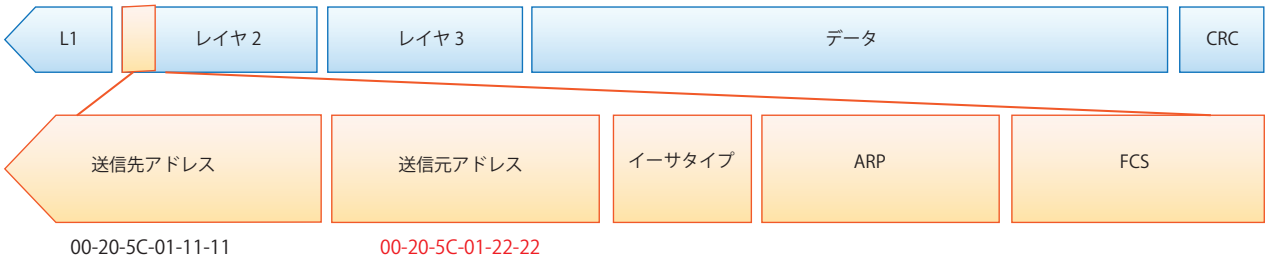


図 E-8　イーサネットフレームフォーマット

スイッチは、また、イーサネットフレームの「送信元アドレス」を調べて、フォワーディングテーブルにはアドレスがないことを見つけます。スイッチは PC の MAC アドレスを学習してフォワーディングテーブルを更新します。

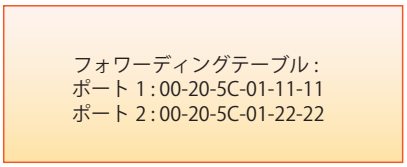


図 E-9　フォワーディングテーブル

ARP スプーフィングでネットワークを攻撃する方法

また、ARP を汚染することで知られている ARP スプーフィングは、イーサネットネットワークを攻撃する方法で、DoS（Denial of Service）として知られているように、攻撃者は LAN 上のデータフレームをかぎつけて、トラフィックを編集、またはトラフィックを停止させてしまう可能性があります。ARP スプーフィングの原則は、偽造または改ざんした ARP メッセージをイーサネットネットワークに送信することです。一般的に、目的は、デフォルトゲートウェイなどの別のノードの IP アドレスに攻撃者の MAC アドレスかでたらめの MAC アドレスを割り当ててしまうことです。その IP アドレスに向かう予定だったトラフィックが、攻撃者に指定されたノードに誤ってリダイレクトされてます。

IP スプーフィング攻撃は、ホストが自身の IP アドレスを解決するため ARP リクエストを送信する場合に発生する Gratuitous ARP によって引き起こされます。図 E-10 は、LAN のハッカーによる ARP スプーフィング攻撃の開始を示しています。

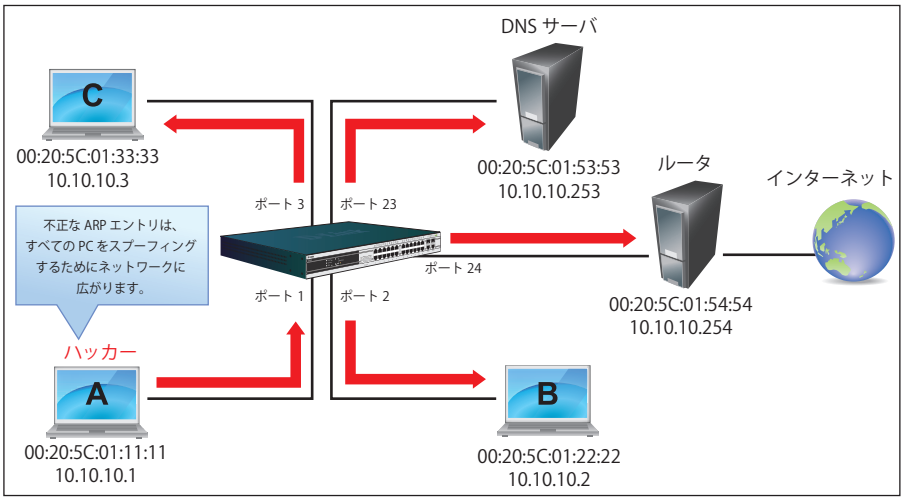


図 E-10　IP スプーフィング攻撃

Gratuitous ARP パケットでは、「送信側プロトコルアドレス」と「ターゲットプロトコルアドレス」は同じ送信元 IP アドレスとなります。「送信側 H/W アドレス」と「ターゲット H/W アドレス」は同じ送信元 MAC アドレスとなります。宛先の MAC アドレスは、イーサネットブロードキャストアドレス（FF-FF-FF-FF-FF-FF）となります。ネットワーク内のすべてのノードは、送信側の MAC アドレスおよび IP アドレスに従って、直ちに自身の ARP テーブルを更新します。Gratuitous ARP の書式は以下の表の通りです。

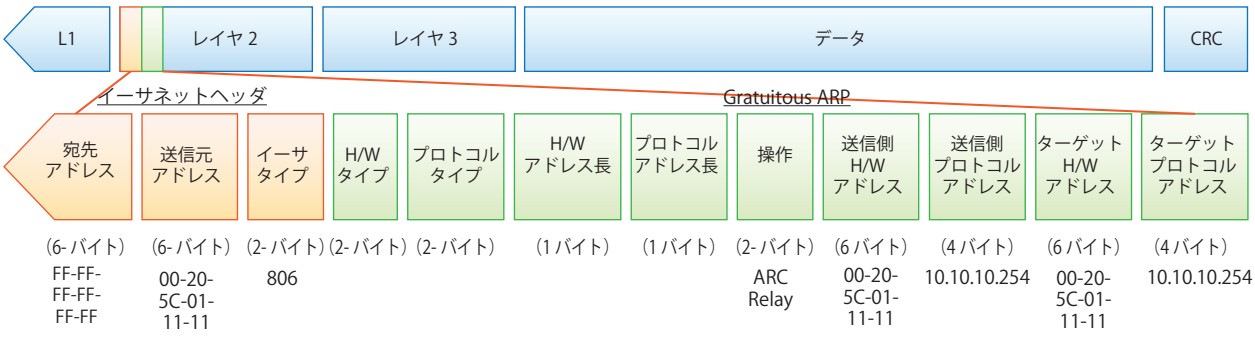


図 E-11　イーサネットフレームフォーマット

一般的な DoS 攻撃は、実在しない MAC アドレスやあらゆる指定 MAC アドレスをネットワークのデフォルトゲートウェイの IP アドレスに関連させることで行われます。悪意がある攻撃者は、一つの Gratuitous ARP をゲートウェイであると言っているネットワークに対してブロードキャストする必要があるだけであり、これによりすべてのネットワーク操作は、インターネットへの全パケットが間違ったノードに向けられるためにダウンさせられてしまいます。

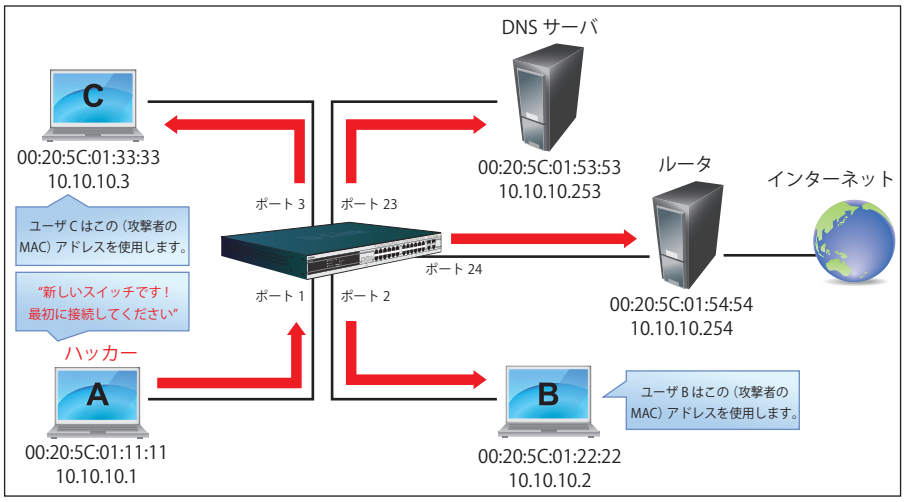


図 E-11　IP スプーフィング攻撃

同様に、攻撃者は、実際のデフォルトゲートウェイにトラフィックを転送する（パッシブスニッフィング）か、またはそれを転送する前にデータを更新する（man-in-the-middle 攻撃）を選択することが可能です。ハッカーは PC をだまし、犠牲者であるルータをだまします。図 E-11 で参照されるように、すべてのトラフィックはハッカーにスニッフィングされますが、ユーザはそれを発見できません。

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する

D-Link マネージドスイッチは、独自のパケットコンテンツ ACL 経由で ARP スプーフィングが引き起こした一般的な DoS を効果的に軽減することができます。基本的な ACL は、パケットタイプ、VLAN ID、送信元および送信先 MAC 情報に基づいて ARP パケットをフィルタするだけであるため、より詳細な ARP パケットの検証が必要となります。

ARP スプーフィング攻撃を防ぐために、スイッチでパケットコンテンツ ACL を使用し、偽造されたゲートウェイの MAC と IP バインディングを含む不正な ARP パケットを防御します。

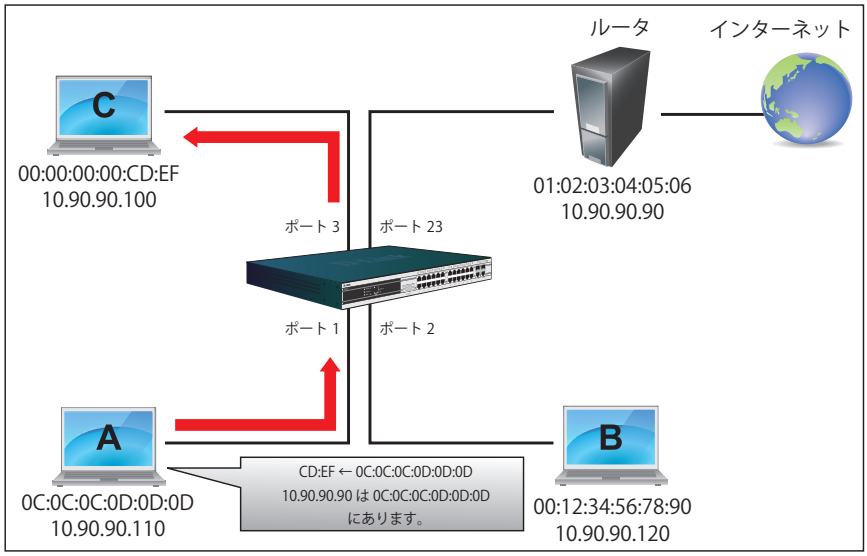


図 E-12　パケットコンテンツ ACL 経由の ARP スプーフィング防止

設定

設定のロジックは以下の通りです。

1. ARP がイーサネットにおける送信元 MAC アドレスに一致する場合にだけ、ARP プロトコルの送信者の MAC アドレスと送信者の IP アドレスはスイッチを通過することができます。（この例では、ゲートウェイの ARP です。）
2. スイッチはゲートウェイの IP アドレスから来ていると言う他のすべての ARP パケットを拒否します。

スイッチのパケットコンテンツ ACL の設計により、ユーザはどんなオフセットチャンクも検証することができます。オフセットチャンクは 16 進数形式の 4 バイトのブロックであり、イーサネットフレーム内の各項目に一致させるために利用されます。各プロファイルは、最大 4 つのオフセットチャンクを持つことができます。その上、パケットコンテンツ ACL に 1 個のプロファイルだけがスイッチごとサポートされます。つまり、最大 16 バイトのオフセットチャンクが各プロファイルとスイッチに適用されます。そのため、有効なオフセットチャンクの計画と設定が必要とされます。

表 E-1 で、Offset_Chunk0 が 127 バイト目から開始し、128 バイト目で終了することにご注意ください。されに、オフセットチャンクが 0 ではなく、1 から抽出されることがわかります。

表 E-1　チャンクとパケットオフセット

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
バイト	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
バイト	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
バイト	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
バイト	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk15	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30
バイト	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
バイト	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
バイト	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
バイト	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

以下の表は、パケットオフセットの計算のためのパターンであるイーサネットフレームに含まれる完全な ARP パケットを示しています。

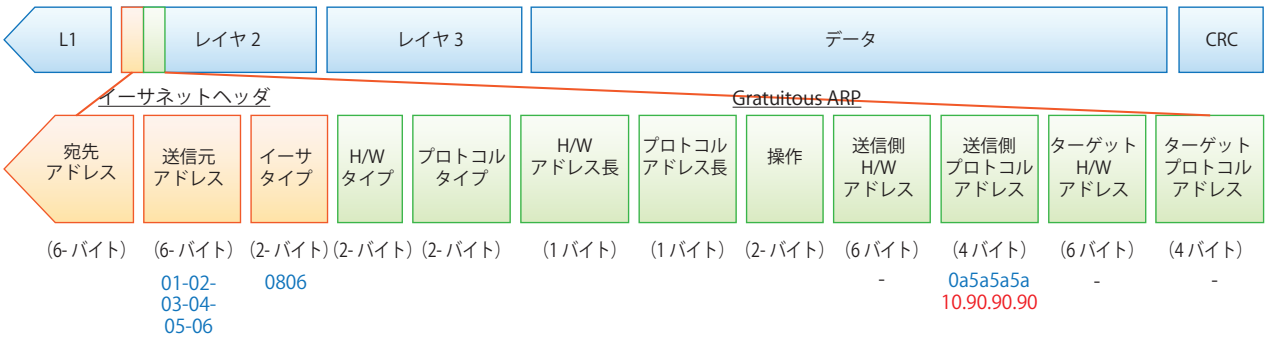


図 E-13 イーサネットフレームに含まれる完全な ARP パケット

	コマンド	記述
手順 1	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	• 「イーサネットタイプ」と「送信元 MAC アドレス」を一致させるアクセスプロファイル 1 を作成します。
手順 2	config access_profile profile_id 1 add access_id1 ethernet source_mac 01-02-03-04-04-06 ethernet_type 0x806 port 1-27 permit	• アクセスプロファイル 1 を設定します。 • ゲートウェイの ARP パケットがイーサネットフレームに正しい「送信元 MAC」を持っている場合だけスイッチを通過できます。
手順 3	create access_profile profile_id 2 packet_content_mask offset_chunk_1 3 0x0000FFFF ↑ イーサネットタイプ（1 バイト）: ARP offset_chunk_2 7 0x0000FFFF ↑ Sdr IP（始め 2 バイト） offset_chunk_3 8 0x0000FFFF ↑ Sdr IP（最後 2 バイト）	• アクセスプロファイル 2 を作成します。 • 2 つ目のチャンクは Chunk7 から開始します。 :「イーサネットタイプ」のマスク（表 E-1 : 13/14 バイト目の青色部分） • 1 つ目のチャンクは Chunk3 から開始します。 : ARP パケットの「Sender IP」（始め 2 バイト）のマスク（表 E-1 : 29/30 バイト目の緑色部分） • 1 つ目のチャンクは Chunk8 から開始します。 : ARP パケットの「Sender IP」（最後 2 バイト）のマスク（表 E-1 : 31/32 バイト目の茶色部分）

	コマンド	記述
手順 4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 ↑ イーサネットタイプ（1 バイト）: ARP offset_chunk_2 0x00000A5A ↑ Sdr IP（始め 2 バイト）: 10.90 offset_chunk_3 0x5A5A0000 ↑ Sdr IP（最後 2 バイト）: 90.90 port 1-27 deny	• アクセスプロファイル 2 を設定します。 • 「Sender IP」がゲートウェイの IP であると言う残りの ARP パケットは廃棄されます。
手順 5	save	• 設定を保存します。

付録 F パスワードのリカバリ手順

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。「UART init」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                                        V2.00.003
--------------------------------------------------------------------------------

  Power On Self Test ....................................  100%

  MAC Address   : 34-08-04-45-7F-00
  H/W Version   : A1

  Please Wait, Loading V2.10.018 Runtime Image ..............  100 %
  UART init .................................................  100 %
```

```
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 {< ユーザ名 >}	指定ユーザのパスワードをリセットします。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 InterfaceCross-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パラメータを保持します。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。