D-Link DGS-3120 シリーズ

Gigabit Stackable Layer2 Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

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

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

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

ご使用上の注意

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

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

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

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

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

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

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

目次

はじめに

DGS-3120 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 本製品のご利用にあたって
- 本スイッチの概要と前面、背面、側面の各パネル、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および電源接続の方法について紹介します。

第 3 章 スイッチの接続
- スイッチをご使用のイーサネットに接続する方法を説明します。

第 4 章 スイッチ管理について
- パスワード設定、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 ベースのスイッチ管理
- 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。また、設定の保存、リブートなどスイッチのユーティリティ機能について説明します。

第 6 章 System Configuration（システム設定）
- デバイス情報の確認、IP アドレスの設定、スタックの管理、ポートパラメータの設定、ユーザアカウントの設定、システムログの設定と管理、システム時刻の設定、SNMP システム管理について説明します。

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

第 8 章 L2 Features（L2 機能の設定）
- VLAN 設定、スパニングツリーの設定、リンクアグリゲーションの設定、FDB 設定、L2 マルチキャスト、LLDP 設定、NLB FDB 設定など L2 機能について説明します。

第 9 章 L3 Features（レイヤ 3 機能）
- IPv4 ルートテーブルや IP フォワーディングテーブルなどの L3 機能について説明します。

第 10 章 QoS（QoS 機能の設定）
- 802.1p 設定、帯域幅の設定、トラフィックコントロール、DSCP、HOL ブロッキング防止、QoS スケジュール設定について説明します。

第 11 章 ACL（ACL 機能の設定）
- アクセスコントロールリスト（ACL）関連の設定について説明します。

第 12 章 Security（セキュリティ機能の設定）
- 802.1X 認証、RADIUS 設定、MAC アドレス /WAC/JWAC 認証などデバイスのセキュリティの設定について解説します。

第 13 章 Network Application（ネットワークアプリケーション）
- DHCP、SNTP、フラッシュファイルシステム設定について解説します。

第 14 章 OAM（OAM の設定）
- ケーブル診断など障害検出のための設定について解説します。

第 15 章 Monitoring（スイッチのモニタリング）
- 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について表示します。

第 16 章 Save and Tools（Save と Tools メニュー）
- Web インタフェース画面左上部の「Save」「Tools」メニューを使用してスイッチの管理、設定を行います。

付録 A 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 スプーフィング攻撃を防ぐために、パケットコンテンツ ACL を使用した不正な ARP パケットからの防御について説明します。

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

付録 C ログエントリ
- システム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
- システムに表示される可能性のあるトラップログとそれらの意味について説明します。

付録 E RADIUS 属性の割り当て指定
- DGS-3120 における RADIUS 属性の割り当てについて説明します。

付録 F ケーブルとコネクタ

- スイッチに使用されるケーブルとコネクタ形状について説明します。

付録 G ケーブル長

- スイッチに使用されるケーブル長の最大値について説明します。

付録 H 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。

付録 I 機能設定例

- 機能設定例ついて説明します。

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	コマンド項目（可変または固定）。	*`value`*
< >	可変項目。< > にあたる箇所に値または文字を入力します。	<*`value`*>
[ ]	任意の固定項目。	[*`value`*]
[< >]	任意の可変項目。	[<*`value`*>]
{ }	{ } 内の選択肢から 1 つ選択して入力する項目。	{*`choice1`* | *`choice2`*}
|（垂直線）	相互排他的な項目。	*`choice1`* | *`choice2`*
Menu Name > Menu Option	メニュー構造を示します。	Device > Port > Port Properties は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。

製品名 / 品番一覧

製品名	概要	品番
DGS-3120-24TC	SI 版	DGS-3120-24TC/SI
	EI 版	DGS-3120-24TC/EI
DGS-3120-48TC	SI 版	DGS-3120-48TC/SI
	EI 版	DGS-3120-48TC/EI
DGS-3120-24PC	SI 版	DGS-3120-24PC/SI
	EI 版	DGS-3120-24PC/EI
DGS-3120-48PC	SI 版	DGS-3120-48PC/SI
	EI 版	DGS-3120-48PC/EI
DGS-3120-24SC	SI 版	DGS-3120-24SC/SI
	EI 版	DGS-3120-24SC/EI
DGS-3120-24SC-DC	SI 版	DGS-3120-24SC-DC/SI
	EI 版	DGS-3120-24SC-DC/EI

第 1 章　本製品のご利用にあたって

DGS-3120 シリーズギガビットイーサネットスイッチは、D-Link xStack ファミリーメンバの高性能スイッチです。10/100Mbps のエッジスイッチからコアギガビットスイッチまで xStack スイッチファミリーは高可用性、ポートの安定性、最適なセキュリティ、最高のスループットをネットワークプロフェッショナルのためのシンプルなインタフェース管理と共に実現する設計となっています。

DGS-3120 シリーズは最新のエントリレベル D-Link マネージドレイヤ 2+ ギガビットスイッチです。DGS-3120-24TC/PC、48TC/PC は高速スタック用 CX4 インタフェースを 2 ポート、コンボ SFP ポートを 4 ポート、および 10/100/1000Mbps ギガビットポートを 24/48 ポート搭載しています。費用対効果に優れた本ギガビットスイッチは、高速ネットワーク通信を構築する管理者への最適な解決策を、高速ギガビット接続と共に実現します。CX4 スタッキングポートにより DGS-3120 シリーズは 40 ギガの双方向の帯域幅まで対応するバックボーンソリューションとして利用が可能です。高度な ACL やユーザ認証機能により、エッジからコアまでネットワークセキュリティの対応範囲が大きく広がります。D-Link セーフガードエンジンはワームやウィルスの脅威から、DGS-3120 シリーズの総合的な信頼性、サービス性、および稼働率を保護します。

本マニュアルでは、DGS-3120-24TC、DGS-3120-24PC、DGS-3120-24SC、DGS-3120-24SC-DC、DGS-3120-48TC および DGS-3120-48PC を含む D-Link DGS-3120 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。本シリーズは機能設定やハードウェア構成は一部機能を除き同じであるため、本マニュアルの情報をすべての種類にほぼ適用できます。Web による管理画面例は、上に記載したいずれかの機種のものですが、一部機能、ポート数を除き設定内容はほぼ同じです。

スイッチ概要

DGS-3120 シリーズは以下の製品で構成されるギガビットスタッカブル L2 スイッチです。:

- DGS-3120-24TC : 10BASE-T/100BASE-TX/1000BASE-T x 24 ポート、10G BASE-CX4 x 2 ポート、コンボ SFP x 4 ポート搭載
- DGS-3120-24PC : 10BASE-T/100BASE-TX/1000BASE-T（PoE）x 24 ポート、10G BASE-CX4 x 2 ポート、コンボ SFP x 4 ポート搭載
- DGS-3120-24SC : 10BASE-T/100BASE-TX/1000BASE-T（SFP とのコンボ）x 8 ポート、10G BASE-CX4 x 2 ポート、SFP x 24 ポート搭載
- DGS-3120-24SC-DC : 10BASE-T/100BASE-TX/1000BASE-T（SFP とのコンボ）x 8 ポート、10G BASE-CX4 x 2 ポート、SFP x 24 ポート搭載
- DGS-3120-48TC : 10BASE-T/100BASE-TX/1000BASE-T x 48 ポート、10G BASE-CX4 x 2 ポート、コンボ SFP x 4 ポート搭載
- DGS-3120-48PC : 10BASE-T/100BASE-TX/1000BASE-T（PoE）x 48 ポート、10G BASE-CX4 x 2 ポート、コンボ SFP x 4 ポート搭載

DGS-3120 シリーズは、8/24/48 の高性能 1000BASE-T ポートを搭載しています。1000BASE-T ポートは、10/100/1000Mbps で通信可能で、バックボーン、エンドステーションおよびサーバとの接続が可能です。さらに、本シリーズは 4 個の SFP コンボポート（DGS-3120-24SC、SC-DC を除く）または専用の SFP ポート（DGS-3120-24SC、SC-DC）を搭載し、スイッチ、サーバおよびネットワークバックボーンを光ファイバで接続することが可能です。また、RJ-45 コンソールポートにより、端末または端末エミュレーションプログラム経由で管理することができます。

注意　DGS-3120 シリーズのすべての機種について、区別する必要がある場合を除き、本マニュアル上では単に “スイッチ” あるいは “DGS-3120” と記載します。

注意　ご購入のライセンスにより使用できる機能が違います。「Standard Image」（スタンダード版）をご使用の場合は「SI モード」、「Enhanced Image」（エンハンス版）をご使用の場合は「EI モード」の記述を参照ください。どちらも書いていない場合は共通の機能になります。

SFP について

本スイッチには PC やハブ、他のスイッチなど、様々なアップリンクネットワークデバイスとの全二重モードでの接続に使用される 1000BASE-T ポートと SFP ポートがあります。SFP（Small Form-Factor Pluggable）ポートは光ファイバトランシーバ用のケーブル配線に使用され、ギガビットデータの長距離伝送が可能なネットワークデバイスと通信を行います。これらの SFP ポートは、全二重モードをサポートして、次のトランシーバと共に使用が可能です。

注意 Combo Port において、SFP の RX が信号を受信している状態では、SFP Port、Coppoer Port とも Link Up しません。

DGS-3120 シリーズスイッチ対応 SFP トランシーバ

- DEM-310GT（1000BASE-LX）
- DEM-311GT（1000BASE-SX）
- DEM-312GT2（1000BASE-SX）
- DEM-314GT（1000BASE-LH）
- DEM-315GT（1000BASE-ZX）
- DEM-210（シングルモード 100BASE-FX）
- DEM-211（マルチモード 100BASE-FX）
- DGS-712（1000BASE-T）（SFP コンボスロットでは使用不可）

WDM トランシーバ

- DEM-330T（TX-1550/RX-1310 nm）
- DEM-330R（TX-1310/RX-1550 nm）
- DEM-331T（TX-1550/RX-1310 nm）
- DEM-331R（TX1310/RX-1550 nm）
- DEM-220T（100BASE-BX-D, TX-1550/RX-1310 nm）
- DEM-220R（100BASE-BX-U, TX-1310/RX-1550 nm）

前面パネル

スイッチの前面パネルには、電源、コンソール、RPS（リダンダント電源システム）、Master、S1、S2、Fan、SD、スタック ID および各ポートの Link/Act を示す各ポート（SPF ポートを含む）用の LED が配置されています。

DGS-3120-24TC

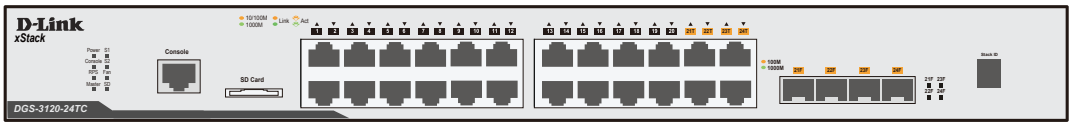


図 1-1　DGS-3120-24TC の前面パネル

DGS-3120-48TC

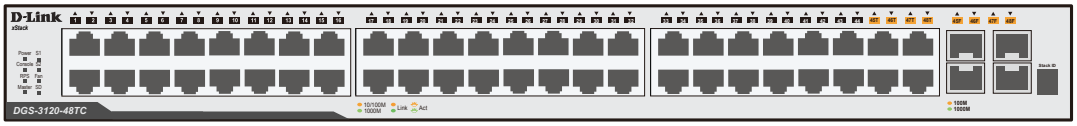


図 1-2　DGS-3120-48TC の前面パネル

DGS-3120-24PC

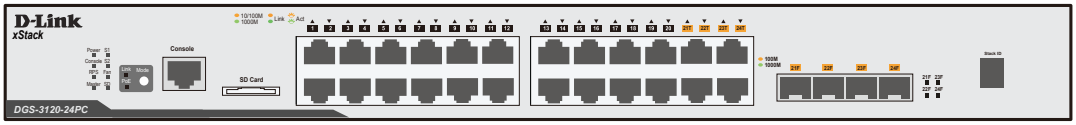


図 1-3　DGS-3120-24PC の前面パネル

DGS-3120-48PC

図 1-4　DGS-3120-48PC の前面パネル

DGS-3120-24SC、DGS-3120-24SC-DC

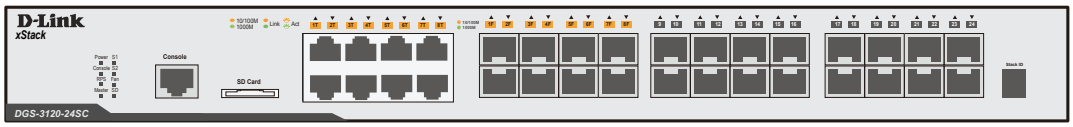


図 1-5　DGS-3120-24SC、DGS-3120-24SC-DC の前面パネル

LED 表示

スイッチは、Power、Console、RPS、Master（スタッキング制御）、S1、S2、SD、ファン、スタック ID およびギガビットポートを含む各ポートについての LED をサポートしています。

DGS-3120-24TC

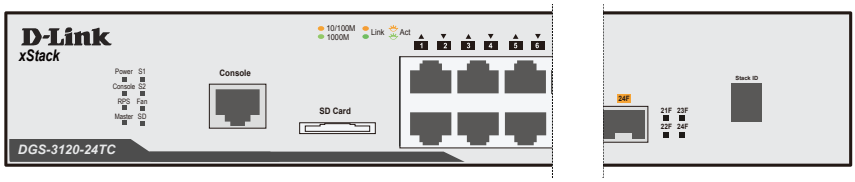


図 1-6　DGS-3120-24TC の LED 配置図

DGS-3120-24SC/SC-DC

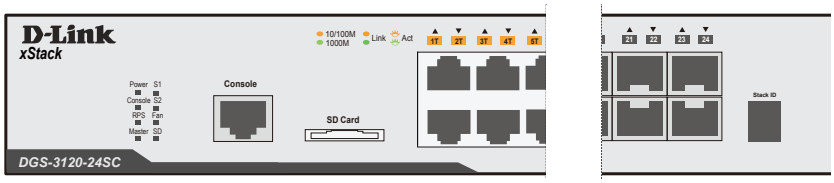


図 1-7　DGS-3120-24SC/SC-DC の LED 配置図

DGS-3120-24PC

図 1-8　DGS-3120-24PC の LED 配置図

DGS-3120-48TC

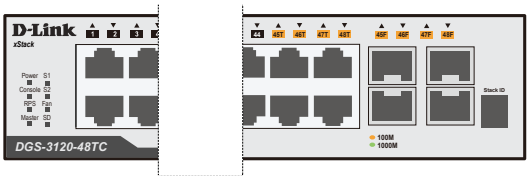


図 1-9　DGS-3120-48TC の LED 配置図

DGS-3120-48PC

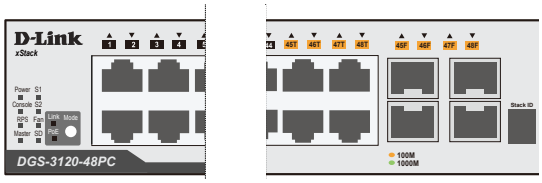


図 1-10　DGS-3120-48PC の LED 配置図

注意　Combo Port において、SFP の RX が信号を受信している状態では、SFP Port、Copper Port とも Link Up しません。

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	内容
システム LED			
Power	緑	点灯	電源が供給され正常に動作しています。
	ー	消灯	電源が供給されていません。
Console	緑	点灯	コンソール経由で本製品にログインしています。
	ー	消灯	コンソール経由で本製品にログインしていません。
RPS	緑	点灯	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。
		点滅	RPS ケーブルの接続を検出しています。
	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	緑	点灯	デバイスがスタックにおいてマスタとして動作しています。
	ー	消灯	デバイスはスタックにおいてスレーブとして動作しています。
S1	緑	点灯	CX-4 ポート 1（S1）にデバイスが正常に接続（リンク）されています。
		点滅	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。
S2	緑	点灯	CX-4 ポート 2（S2）にデバイスが正常に接続（リンク）されています。
		点滅	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。
Fan	赤	点滅	ファンのいずれかが故障しています。
	ー	消灯	ファンは正常に動作しています。
SD	緑	点灯	SD カードが挿入されています。
		点滅	リード / ライト中です。
	ー	消灯	SD カードは挿入されていません。
	赤	点灯	SD カードに不具合が生じています。
Stack ID	緑	番号点灯	スタック番号（1-6）が表示されます。
		「H」点灯	デバイスはスタッキング内マスタとして動作しています。
		「h」点灯	デバイスはスタッキング内バックアップマスタとして動作しています。
		「G」点灯	セーフガードエンジン機能が「exhausted」モードになっています。
GE ポート LED			
Link/ACT	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。
PoE （24/48PC のみ）	緑	点灯	接続中の PoE 受電機器に給電中です。
	橙	点灯	PoE ポートにエラーが発生しました。
	ー	消灯	給電をしていません。(受電機器が未検出または未接続)
SFP ポート LED			
Link/ACT	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	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。
	ー	消灯	リンクが確立していません。

注意 Combo Port において、SFP の RX が信号を受信している状態では、SFP Port、Copper Port とも Link Up しません。

背面パネル

DGS-3120-24TC

リダンダント電源コネクタ、AC 電源コネクタ、CX4 ポートが配備されています。

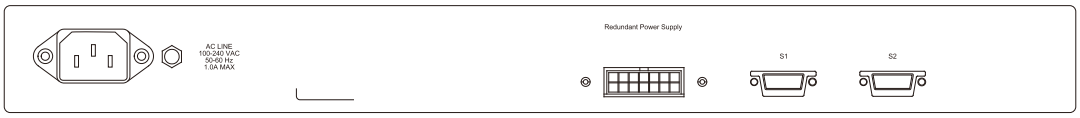


図 1-11　DGS-3120-24TC の背面パネル

DGS-3120-24SC

リダンダント電源コネクタ、AC 電源コネクタ、CX4 ポートが配備されています。

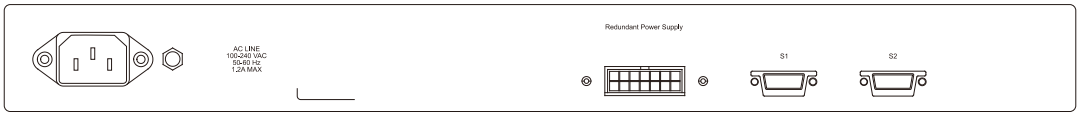


図 1-12　DGS-3120-24SC の背面パネル

DGS-3120-24SC-DC

DC 電源コネクタ、CX4 ポートが配備されています。

図 1-13　DGS-3120-24SC-DC の背面パネル

DGS-3120-24PC

リダンダント電源コネクタ、AC 電源コネクタ、CX4 ポートが配備されています。

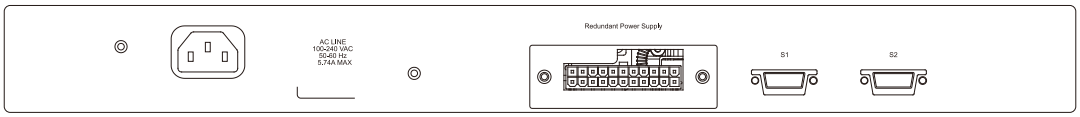


図 1-14　DGS-3120-24PC の背面パネル

DGS-3120-48TC

リダンダント電源コネクタ、AC 電源コネクタ、CX4 ポート、コンソールポートおよび SD カードスロットが配備されています。

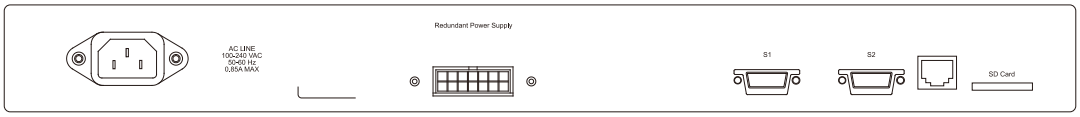


図 1-15　DGS-3120-48TC の背面パネル

DGS-3120-48PC

リダンダント電源コネクタ、AC 電源コネクタ、CX4 ポートおよびコンソールポート SD カードスロットが配備されています。

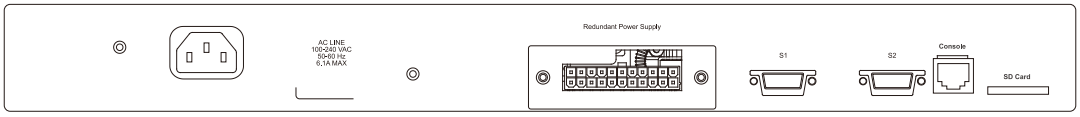


図 1-16　DGS-3120-48PC の背面パネル

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。背面パネルにはオプションの外部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電源ユニット「DPS-200（24TC/SC）、DPS-500/DPS-500DC（48TC）、DPS-700（24PC/48PC）」が自動的にスイッチに電源を供給します。また CX4 ポートを 2 ポート搭載し、ディーリンクジャパンが別売している CX4 ケーブルで接続することによってスタックを構築することができます。

側面パネル

警告 システムの通気口が両側面にあります。通気口はスイッチが持つ熱を放出する役割がありますので、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、必ず 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。

DGS-3120-24TC/SC/SC-DC

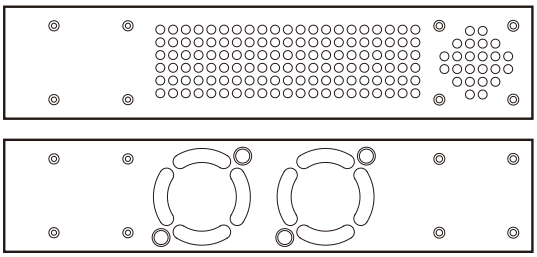


図 1-17　DGS-3120-24TC/SC/SC-DC の側面パネル

DGS-3120-48TC

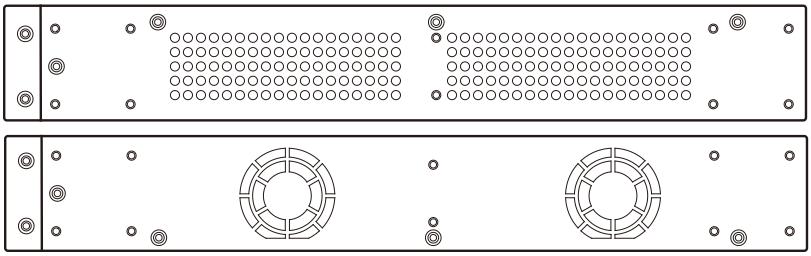


図 1-18　DGS-3120-48TC の側面パネル

DGS-3120-24PC

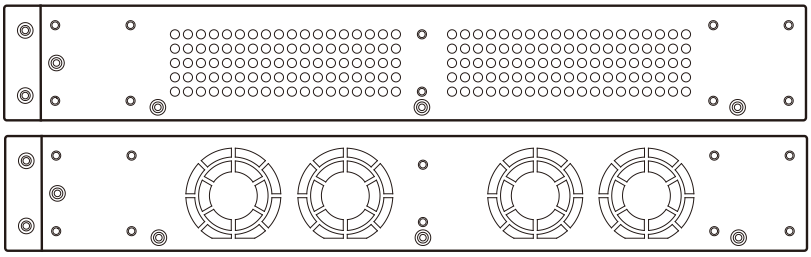


図 1-19　DGS-3120-24PC の側面パネル

DGS-3120-48PC

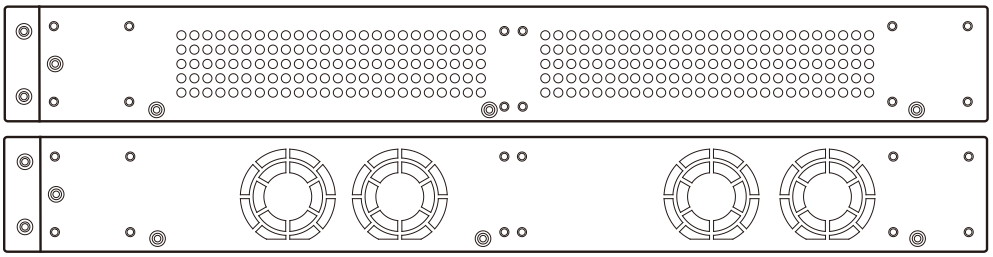


図 1-20　DGS-3120-48PC の側面パネル

第 2 章　スイッチの設置

パッケージの内容

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

- 本体　x　1
- 電源ケーブル　x　1
- ラックマウントキット 1 式（ブラケット 2 個、ネジ）
- ゴム足（貼り付けタイプ）　x　4
- RJ-45/RS-232C コンソールケーブル　x　1
- シリアルラベル　x　1
- 電源抜け防止金具　x　1（DGS-3120-24PC、48PC、24SC-DC は除く）
- クイックインストールガイド（英語版）
- CD-ROM　x　1
- 製品保証書

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最低 6.3 キロ以上の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 10cm 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。

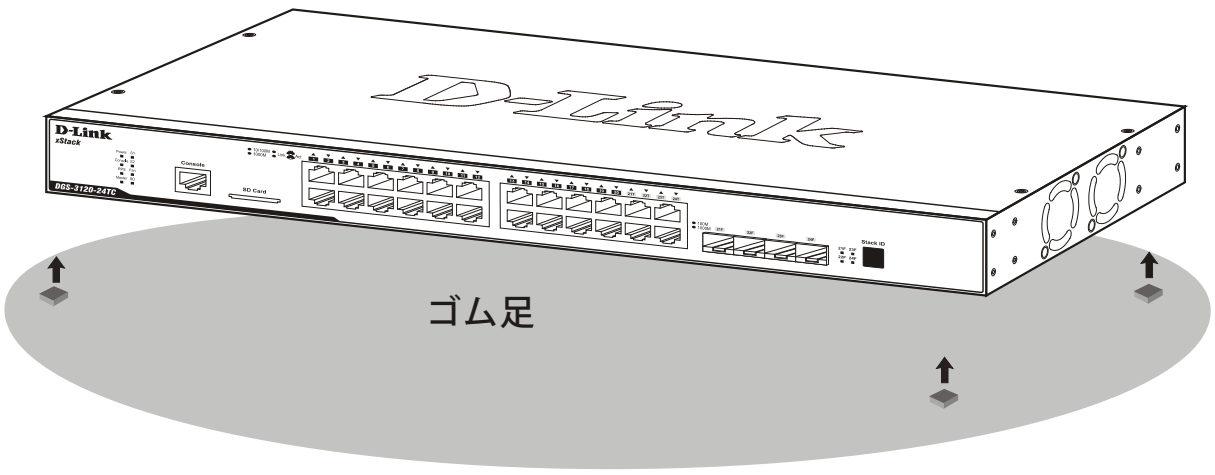


図 2-1　　机や棚の上に設置する場合の準備（DGS-3120-24TC）

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。

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

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、スイッチ両側面にブラケットを取り付けます。

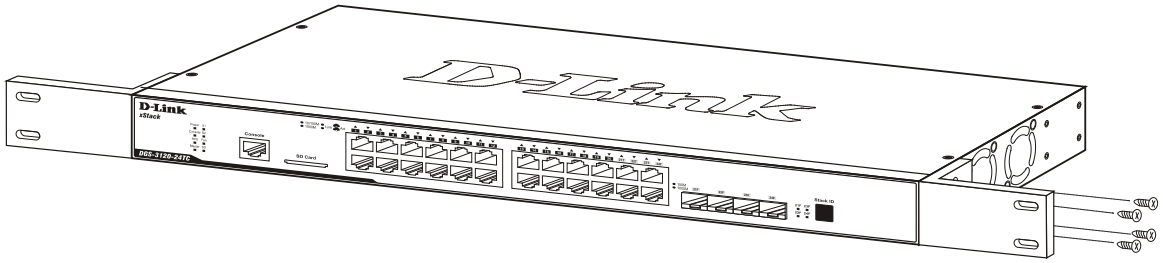


図 2-2　ブラケットの取り付け

3. 19 インチラックに付属のネジを使用し、シャーシをラックに固定します。

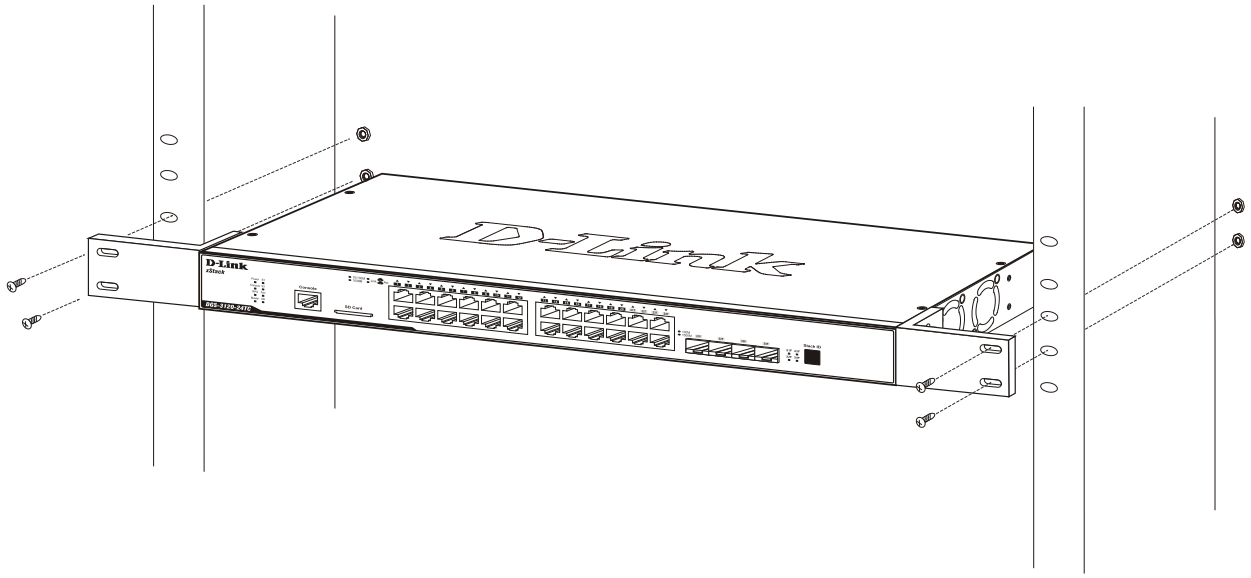


図 2-3　19 インチラックへの設置

電源の投入（AC 電源）

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。

電源の異常（AC 電源）

AC 電源に異常が発生した場合（停電等）、スイッチとの接続を解除してください。電力の回復後に再接続します。

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。

DGS-3120-24SC-DC への DC 電源接続

DGS-3210-24SC-DC の DC 電源ケーブルの接続方法を示します。

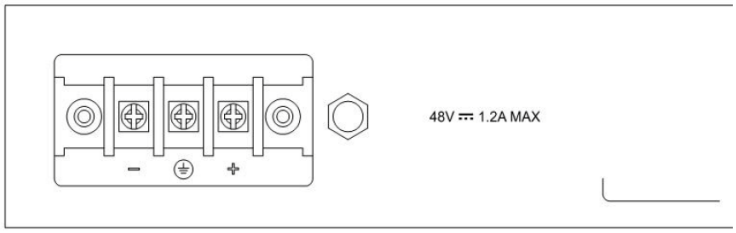


図 2-4　DC 電源ケーブルの端子盤への接続

1. DC 電源ケーブルを接続する端子盤にはマイナス端子、プラス端子、接地端子があります。
2. マイナス端子、プラス端子を電電ケーブルとしっかり接続します。
   - マイナスを -48V 端子に接続します。
   - プラス側を -48V Return 端子に接続します。
   - 接地の際には、接地線を中央の接地端子に接続します。

警告 最小 18 ゲージ (AWG) の結線を使用します。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。

警告 本製品は必ず接地を行ってください。

警告 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。

SFP ポートの設置

8 個、24 個または 48 個の 10/100/1000Mbps ポートに加え、スイッチの前面パネルに SFP コンボポートまたは SFP 専用ポートを装備しています。以下に、スイッチに SFP ポートモジュールを挿入した図を示します。

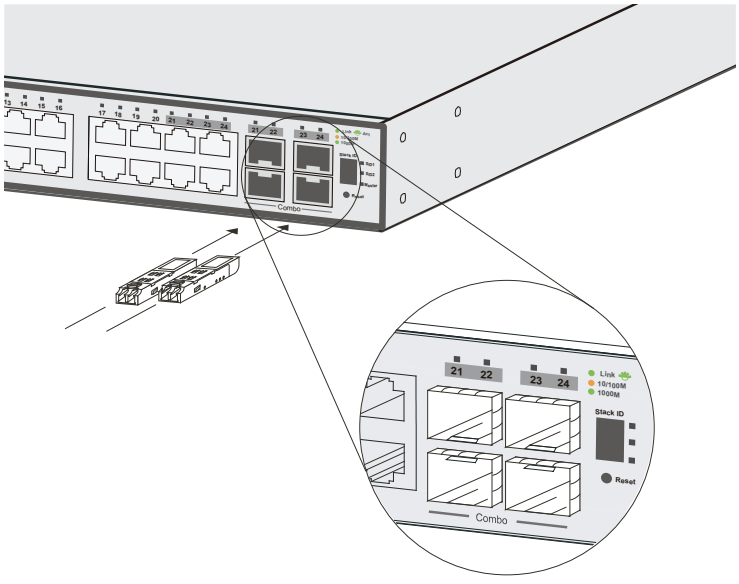


図 2-5　SFP ポートにモジュールを挿入

リダンダント電源システムの設置

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。

警告 本スイッチがサポートしていないリダンダント電源装置を使用しないでください。

警告 リダンダント電源の設置を行う前に、スイッチの電源ケーブルを抜いておいてください。

リダンダント電源システムをスイッチに取り付ける（DGS-3120-24SC/24TC には DPS-200、DGS-3120-48TC には DPS-500/DPS-500DC、DGS-3120-24PC/48PC には DPS-700）ためには、以下の手順を実行します。DPS-200、DPS-500/DPS-500DC および DPS-700 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 および DPS-500/DPS-500DC はリダンダント電源用シャーシ（DPS-900 または DPS-800）に取り付けることができます。

リダンダント電源システムの接続（DPS-200/500/500DC）

DPS シリーズ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。

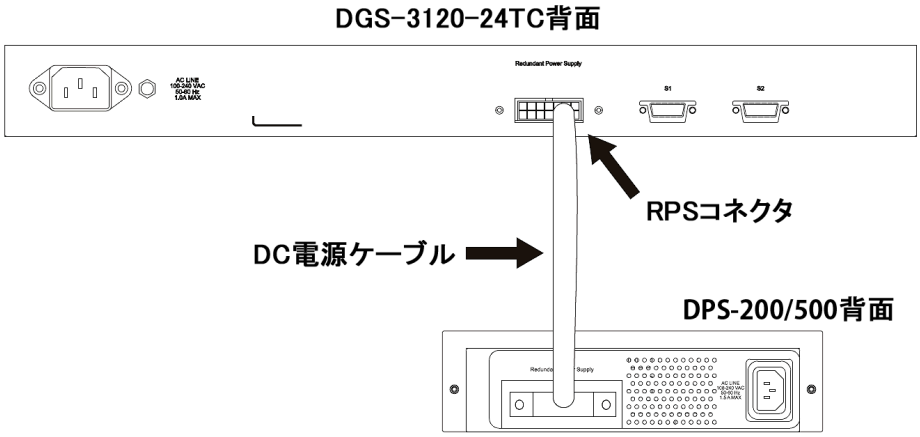


図 2-6　DPS-200/DPS-500/500DC に取り付ける

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。

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。リダンダント電源装置の前面にある緑の 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。スイッチの LED が点灯し、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。

注意 さらに詳細な情報については各リダンダント電源装置のマニュアルをご参照ください。

注意 DGS-3120-24TC/24SC には DPS-200 以外のリダンダント電源装置を使用しないでください。

注意 DGS-3120-48TC には DPS-500/DPS-500DC 以外のリダンダント電源装置を使用しないでください。

注意 DGS-3120-24PC/48PC には DPS-700 以外のリダンダント電源装置を使用しないでください。

リダンダント電源システムの接続（DPS-700）

DPS-700 は 22 ピンの DC 電源ケーブルを使用したスイッチに接続します。電源にはリダンダント電源同梱の AC 電源ケーブルをご使用ください。

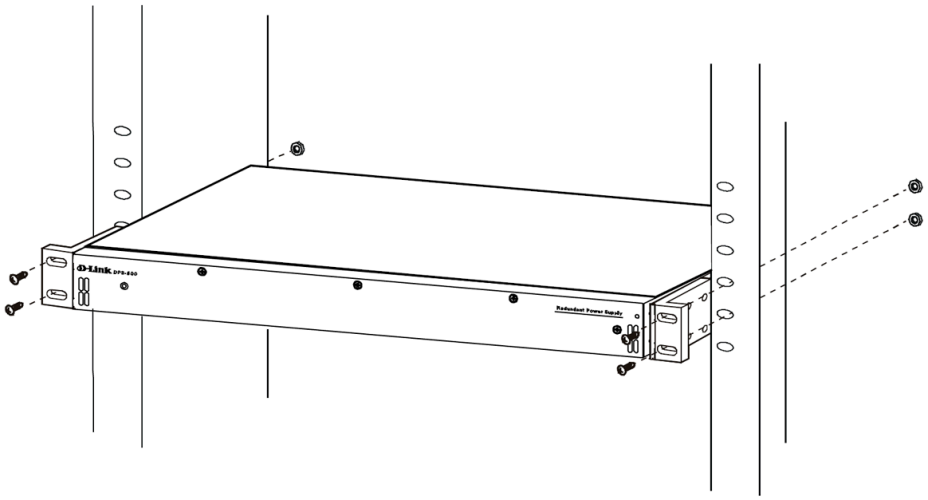


図 2-7　DPS-700 をラックに取り付ける

1. 22 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。リダンダント電源装置の前面にある緑の 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。スイッチの LED が点灯し、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。

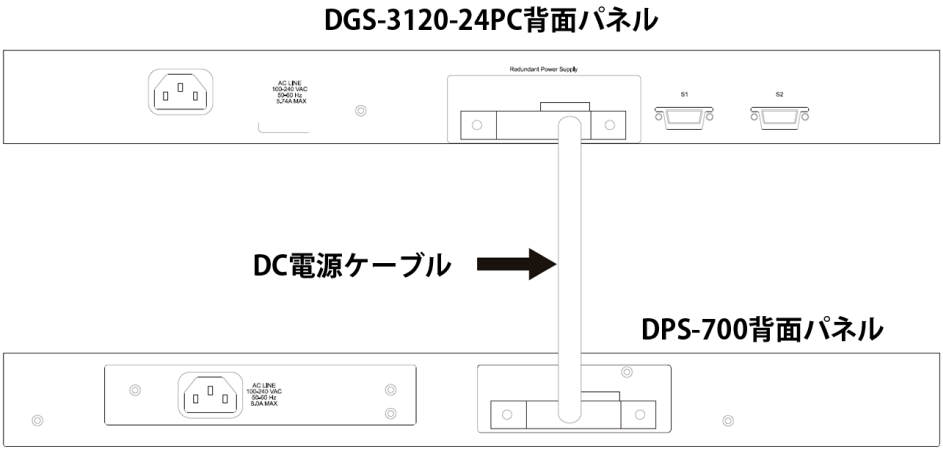


図 2-8　DPS-700 に取り付ける

注意　DGS-3120-24PC/48P と DPS-700 の接続には 22 ピンの DC 電源ケーブル以外使用しないでください。

RPS シャーシを使用する（DPS-800/DPS-900）

DPS-200/500/500DC は DPS-900、DPS-800 ラックマウントユニットに設置して使用することが可能です。
DPS-200 は DGS-3120-24TC と DGS-3120-24SC に使用可能です。DPS-500 は DGS-3120-48TC に使用可能です。DPS-700 は DGS-3120-24PC と DGS-3120-48PC に使用可能です。

注意 DGS-3120-24PC/48PC には DPS-700 以外のリダンダント電源装置を使用しないでください。

DPS-800

DPS-800 は標準サイズのラックマウント（1U サイズ）です。2 台までの DPS-200 または DPS-500/DPS-500DC を収容できます。

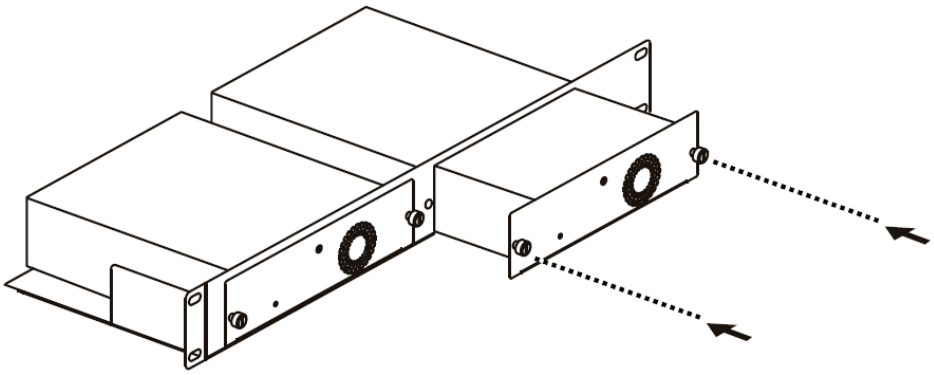


図 2-9　DPS-800 に DPS-200/500/500DC 取り付ける

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。

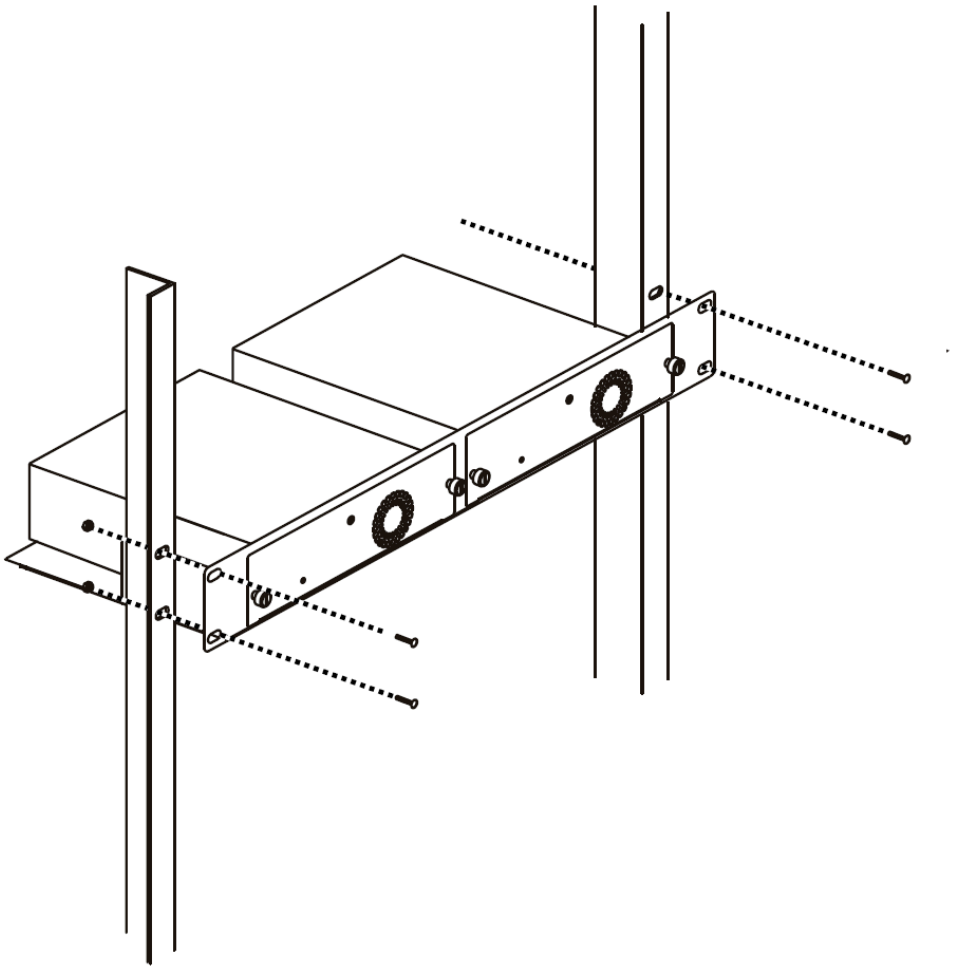


図 2-10　DPS-800 をラックに取り付ける

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 または DPS-500/DPS-500DC を収容できます。

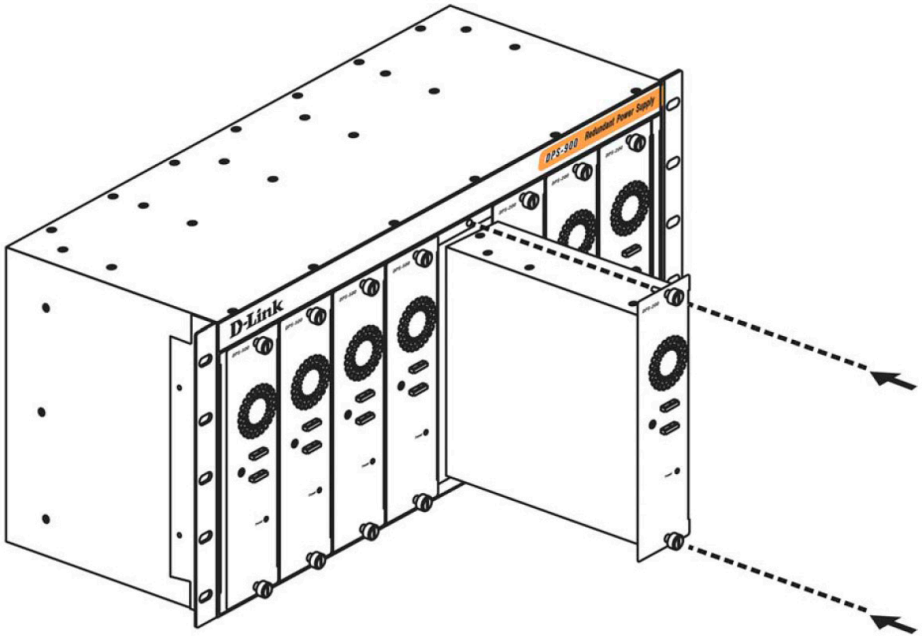


図 2-11　DPS-200/500/500DC を DPS-900 に取り付ける

DPS-900 は、標準 19 インチラックにも取り付けることができます。

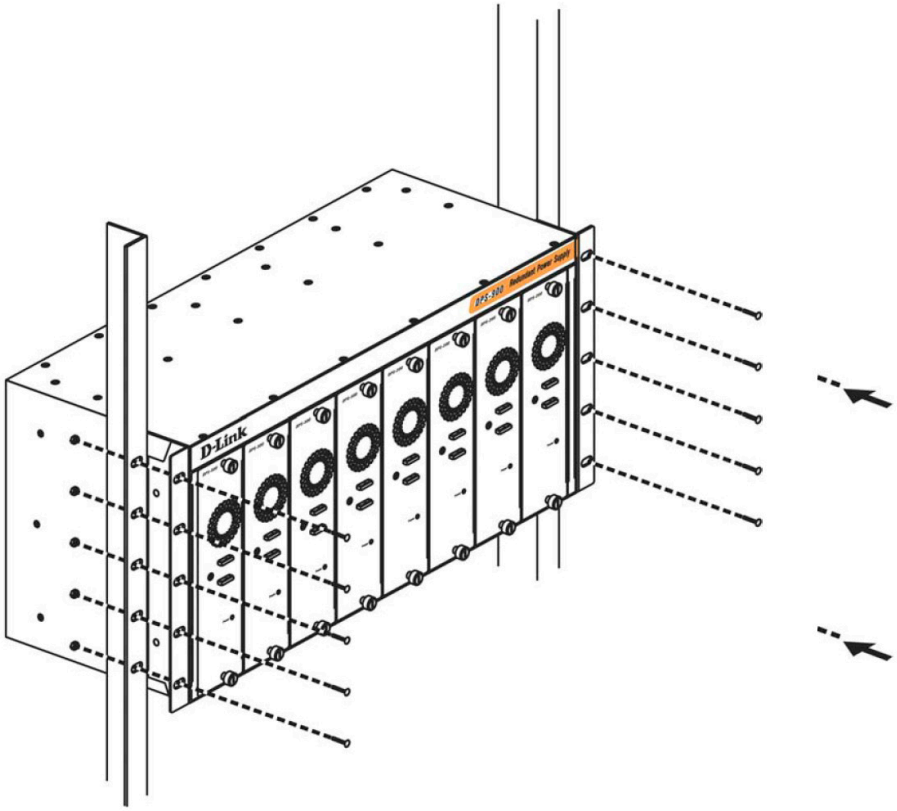


図 2-12　DPS-900 を 19 インチラックに取り付ける

第 3 章　スイッチの接続

参照 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

UTP ケーブルを使用して本スイッチの 1000BASE-T ポートとエンドノードを接続します。
エンドノードとは、RJ-45 コネクタ対応 10/100/1000Mbps イーサネット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。
さらにエンドノードとスイッチ間も 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。

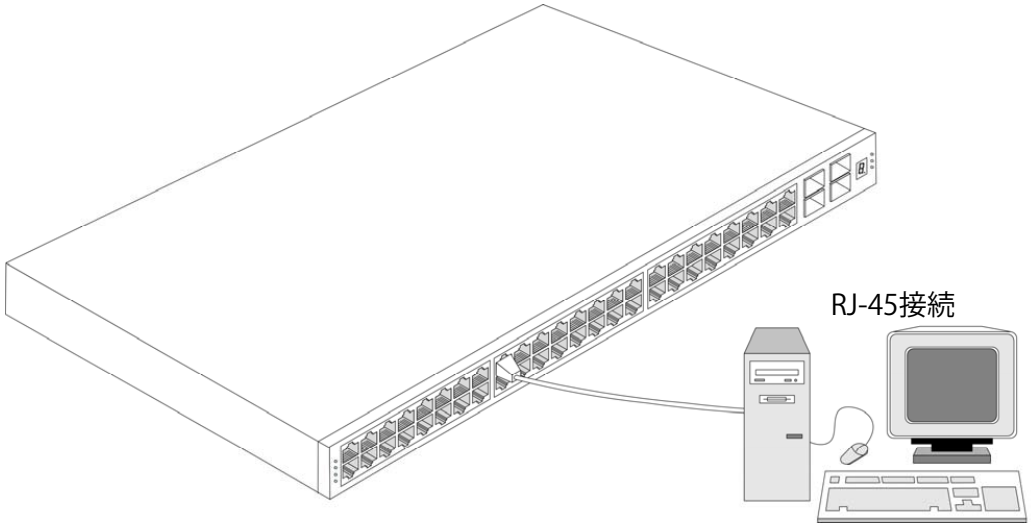


図 3-1　エンドノードと接続したスイッチ

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。

ケーブル仕様については「【付録 F】　ケーブルとコネクタ」（414 ページ）を参照してください。

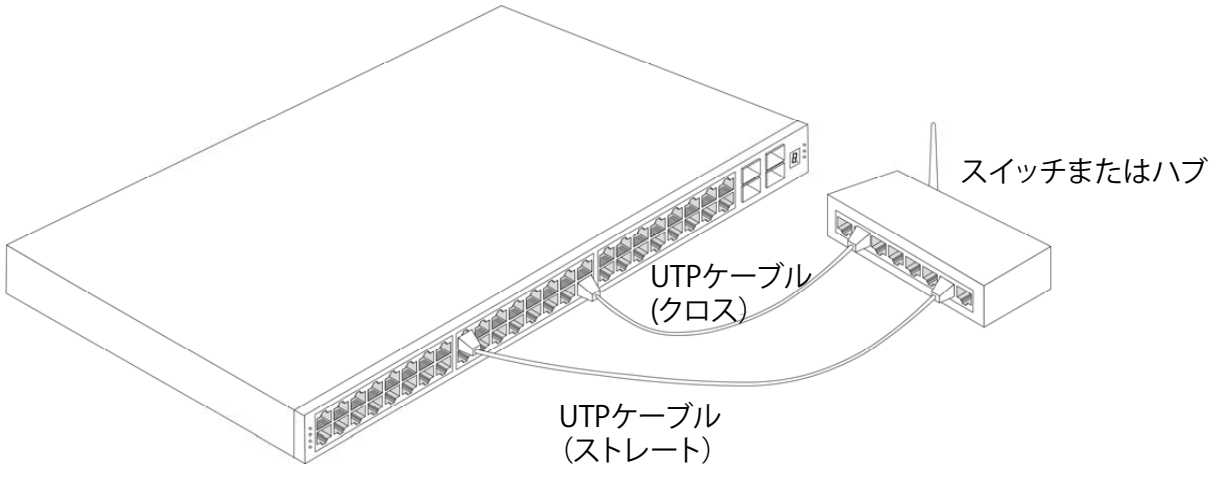


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する

バックボーンまたはサーバと接続する

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

第 4 章　スイッチ管理について

管理オプション

本システムはコンソールポート接続や 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 5.5 以上）Netscape (バージョン 8 以上)、Mozilla Firefox (バージョン 2.0 以上)、Safari (バージョン 4.0 以上) および Google Chrome (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、v2c、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

スイッチのモニタリングと設定のために、RJ-45 コンソールポートを搭載しています。コンソールポートを使用するためには、以下をご用意ください。

- ターミナルソフトを操作するシリアルポート搭載の端末またはコンピュータ
- 同梱の RJ-45/RS-232C 変換ケーブル

端末をコンソールポートに接続する

1. 同梱の変換ケーブルのオス DB-9 コネクタ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、次に RJ-45 コネクタをスイッチのコンソールポートに接続します。
2. 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。

Microsoft® Windows® 2000 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されていることをご確認ください。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。

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（User Name）プロンプトで「admin」を入力し、「Enter」キーを押します。本スイッチには、パスワード（Password）の初期値はありません。既にユーザアカウントを作成している場合は、ユーザ名（User Name）とパスワード（Password）を入力してログインし、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、製品付属の CD-ROM に収録された「DGS-3120 Series CLI Manual」を参照してください。
13. 管理プログラムを終了する場合は、logout コマンド使用するか、ターミナルソフトを終了します。
14. 接続する端末または PC が以上の通り設定されたことを確認してください。

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

コンソールに接続すると、コンソール画面が表示されます。ここ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。

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、次の画面が表示されます。

```
                    DGS-3120-24TC Gigabit Ethernet Switch
                           Command Line Interface

                                Firmware: Build 3.00.010
                    Copyright(C) 2013 D-Link Corporation. All rights reserved.
  UserName:
```

図 4–1　初回接続時の初期画面

初回接続する場合、「User Name」は「admin」で「Password」は登録されていません。「User Name」に「admin」を入力し、「Enter」キーを押します。既に設定されている場合は、「User Name」と「Password」の両方を入力します。
ログインに成功すると、以下の画面のように「DGS-3120-24TC:admin# 」というコマンドプロンプトが表示されます。

パスワード設定

本スイッチは、初期値として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、User Name 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。

```
DGS-3120-24TC:admin#create account admin newmanager
Command: create account admin newmanager

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

DGS-3120-24TC: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働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います。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参照することができます。

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「Configuration」フォルダの「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。

CIDR 表記（例 : 10.41.44.254/8）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の確認や変更を行うことができます。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。

DGS-3120 シリーズは、SNMP のバージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）を実装しています。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のように利用します。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る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「第 8 章　L2 Features（レイヤ 2 機能の設定）」（101 ページ）をご参照ください。

トラップ

トラップとは、スイッチ上で発生したイベントを、ネットワーク管理者に警告するためのメッセージです。イベントには、再起動（誰かが誤ってスイッチの電源を切ってしまった）などの重大なものから、ポートの状態変化を知らせる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。Web ベースでスイッチ管理を実行して行う設定は、コンソール接続によっても行うことができます。

Web マネージャへのログイン

スイッチの管理を行うには、はじめにコンピュータでブラウザを起動し、本スイッチに定義した IP アドレスを入力します。ブラウザのアドレスバーに以下のように URL を入力します。例 : http://10.90.90.90（10.90.90.90 はスイッチの IP アドレス）。この接続においてはプロキシ設定を無効とする必要があります。

ここでは D-Link の Web ベースインタフェースの利用方法について説明します。

Web ベースユーザインタフェースに接続する :

1. Web ブラウザを開きます。ブラウザのポップアップブロックが無効になっていることを確認してください。ポップアップブロックが有効な場合、画面が開けない場合があります。

2. アドレスバーに本スイッチの IP アドレスを入力し、「Enter」キーを押下します。

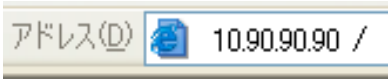


図 5-1　URL の入力

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合わせるか、本スイッチを端末側の IP インタフェースに合わせてください。

3. 以下のユーザ認証画面が表示されます。

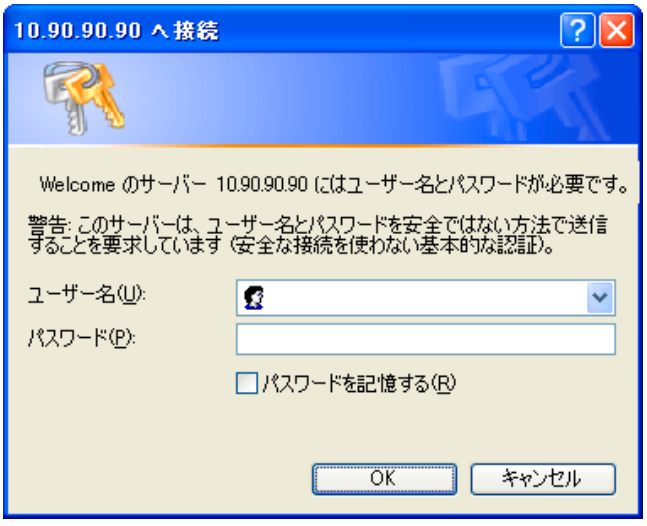


図 5-2　ユーザ認証画面

「ユーザー名」および「パスワード」欄を入力し、「OK」ボタンをクリックし、Web ベースユーザインタフェースに接続します。Web ブラウザで使用可能な機能を以下で説明します。
ご購入後、はじめてログインする場合は、「ユーザー名」に「admin」、「パスワード」は空白のまま「OK」ボタンをクリックします。

Web ベースのユーザインタフェース

Web ユーザインタフェースではスイッチの設定、管理画面にアクセスし、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。
本マニュアルの図では、主に 24 ポートのスイッチを例としています。

ユーザインタフェース内の各エリア

Web ベースインタフェースの「Device Information」画面では以下の情報を参照することができます。

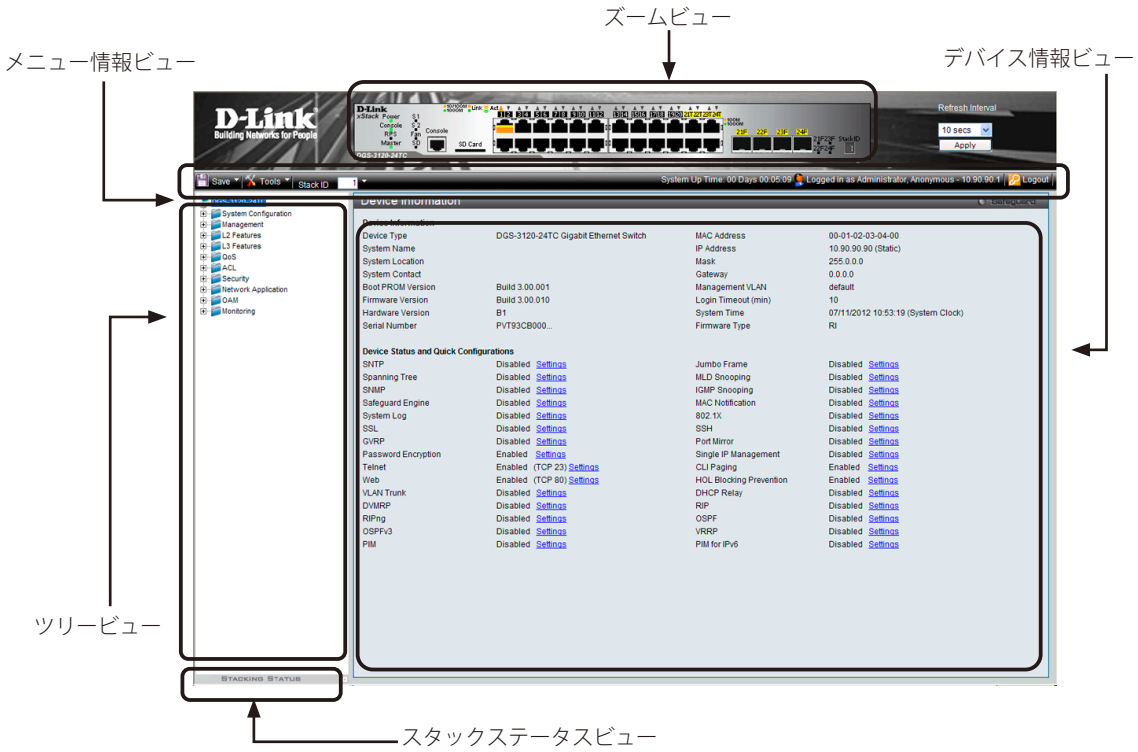


図 5-3　Device Information 画面

次の表では「Device Information」画面の主要な 5 つの領域について説明します。

表 5-1　メイン領域

ビュー	説明
ツリービュー	システムの機能、設定オプションごとに分類して表示します。 表示されているフォルダか画面を選択します。フォルダアイコンを開くことにより、ハイパーリンクメニューボタンやさらにその下のサブフォルダを表示することができます。
ズームビュー	ホームページの最上部に位置し、スイッチの前面パネル上のポートについて、ポート LED の状態をリアルタイムに近いグラフィック表示で提供します。この領域はスイッチのポートや拡張モジュールを表示し、設定したポートの動作、デュプレックスモード、フロー制御に従って表示します。 このグラフィックのさまざまな部分は、設定を含む管理機能を使用するために選択することができます。
メニュー情報ビュー	ズームビューの下で「Save」、「Tools」メニューや、「Stack ID」、「Logout」ボタンを提供します。また、Up Time 情報やログインユーザ名も表示します。
デバイス情報ビュー	ホームページの主となる部分にあり、デバイス情報ビューは選択されたスイッチの情報、テーブル、設定についての指示を表示します。
スタックステータスビュー	ホームページの左下隅に位置するスタックステータスビューは、スタックのリンクとポートステータスを表示します。

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	参照 ページ
System Configuration	Device Information	スイッチの主な設定情報を表示します。	42
	System Information Settings	スイッチの基本情報を表示します。	44
	Port Configuration Settings	ポート設定、ジャンボフレーム設定などを行います。: DDM、Port Settings、Port Description Settings、Port Error Disabled、Port Media Type、Jumbo Frame、EEE Settings	44
	PoE	PoE システムの設定を行います。: PoE System Settings、PoE Port Settings	53
	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。	55
	Warning Temperature Settings	システムの警告温度パラメータを設定します。	55
	Trap Settings	ファンと電力トラップ状態を設定します。	56
	System Log Configuration	フラッシュメモリにスイッチのログを保存する方法、Syslog サーバの設定を行います。: System Log Settings、System Log Server Settings、System Log、System Log & Trap Settings、System Severity Settings	56
	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。	60
	Port Group Settings (EI モードのみ)	ポートグループを作成します。	60
	Time Settings	スイッチに時刻を設定します。	61
	User Accounts Settings	ユーザおよびユーザの権限を設定します。	61
	Command Logging Settings	コマンドログ設定を有効または無効にします。	63
	Configuration Trap Settings	コンフィグレーションの保存、アップロード / ダウンロード時のトラップ送信についての設定します。	63
	Stacking	複数のスイッチを 1 つに結合し、Telnet、Web などのインタフェースから管理します。: Stacking Device Table、Stacking Mode Settings	64
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。: Static ARP Settings、Proxy ARP Settings、ARP Table	68
	Gratuitous ARP	Gratuitous ARP の設定をします。: Gratuitous ARP Global Settings、Gratuitous ARP Settings	70
	IPv6 Neighbor Settings	IPv6 ネイバの設定を行います。	71
	IP Interface	スイッチの IP インタフェース設定を行います。: System IP Address Settings、Interface Settings	72
	Management Settings	CLI ページング、DHCP 自動設定などの管理設定を行います。	76
	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。	77
	Single IP Management	シングル IP マネジメント機能を設定します。: Single IP Settings、Firmware Upgrade、Configuration File Backup/ Restore、Upload Log File	
	SNMP Settings	SNMP 設定を行います。: SNMP Global Settings、SNMP Trap Settings、SNMP Link Change Traps Settings、SNMP View Table Settings、SNMP Community Table Settings、SNMP Group Table Settings、SNMP Engine ID Settings、SNMP User Table Settings、SNMP Host Table Settings、SNMP v6Host Table Settings、RMON Settings、SNMP Community Encryption Settings、SNMP Community Masking Settings	88
	Telnet Settings	スイッチに Telnet 設定をします。	96
	Web Settings	スイッチに Web ステータスを設定します。	96
	Power Saving Settings	リンクダウン状態のポートの電源をオフにしてスイッチへの電力を節約します。: LED State Settings、Power Saving Settings、Power Saving LED Settings、Power Saving Port Settings	96
	SD Card Management	SD カードを使用して、ログやコンフィグレーションの保存を行います。: SD Card Backup Settings、SD Card Execute Settings	98

メイン メニュー	サブメニュー	説明	参照 ページ
L2 Features	VLAN	802.1Q スタティック VLAN 設定を行います。: 802.1Q VLAN Settings、802.1v Protocol VLAN、Asymmetric VLAN Settings、GVRP、MAC-based VLAN Settings、Private VLAN Settings、PVID Auto Assign Settings、Voice VLAN、Surveillance VLAN、Surveillance VLAN OUI Settings、VLAN Trunk Settings、Browse VLAN、Show VLAN Ports	110
	QinQ（EI モードのみ）	Q-in-Q 機能を有効または無効にします。: QinQ Settings、VLAN Translation Settings	124
	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。	127
	Spanning Tree	スパニングツリープロトコルの設定を行います。: STP Bridge Global Settings、STP Port Settings、MST Configuration Identification、STP Instance Settings、MSTP Port Information	128
	Link Aggregation	ポートトランキング設定を行います。: Port Trunking Settings、LACP Port Settings	135
	FDB	スタティック FDB、MAC アドレスエージングタイム、MAC アドレステーブルなどを設定します。: Static FDB Settings、MAC Notification Settings、MAC Address Aging Time Settings、MAC Address Table、ARP & FDB Table	138
	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。: IGMP Snooping、MLD Snooping、Multicast VLAN	142
	Multicast Filtering	マルチキャストフィルタリングの設定を行います。: IPv4 Multicast Filtering、IPv6 Multicast Filtering、Multicast Filtering Mode	164
	ERPS Settings（EI モードのみ）	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。	170
	LLDP	LLDP 設定を行います。: LLDP Statistics System、LLDP-MED	174
	NLB FDB Settings	NLB 機能を設定します。	182
L3 Features	IPv4 Default Route Settings（SI モードのみ）	IPv4 デフォルトルートを設定します。	184
	IPv4 Static/Default Route Settings（EI モードのみ）	IPv4 スタティック / デフォルトルートの設定を行います。	185
	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。	186
	IPv6 Static/Default Route Settings（EI モードのみ）	IPv6 スタティック / デフォルトルートの設定を行います。	186
	IPv6 Route Table（EI モードのみ）	IPv6 ルーティングテーブルの外部経路情報を参照します。	187
	IP Forwarding Table	直接接続するすべての IP 情報を参照します。	187
	Route Preference Settings（EI モードのみ）	スイッチのルートプリファレンス（経路選択）の設定をします。	187
	ECMP Algorithm Settings（EI モードのみ）	ECMP ルートロードバランスアルゴリズムの設定をします。	188
QoS	802.1p Settings	ポート単位にプライオリティを割り当てます。: 802.1p Default Priority Settings、802.1p User Priority Settings	191
	Bandwidth Control	送信と受信のデータレートを制限します。: Bandwidth Control Settings、Queue Bandwidth Control Settings	192
	Traffic Control Settings	ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整します。	194
	DSCP	DSCP トラスト設定、DSCP マップ設定を行います。: DSCP Trust Settings、DSCP Map Settings	196
	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。	197
	Scheduling Settings	QoS スケジューリングを設定します。: QoS Scheduling、QoS Scheduling Mechanism	197
	WRED	WRED の状態、ポート設定、プロファイル設定を行います。: WRED Port Settings、WRED Profile Settings	199

メインメニュー	サブメニュー	説明	参照ページ
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。	201
	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。	202
	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。	218
	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。	232
	Egress Access Profile List (EI モードのみ)	フローごとのパケット処理を実行します。	236
	Egress ACL Flow Meter (EI モードのみ)	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。	246
Security	802.1X	802.1X 認証を設定します。: 802.1X Global Settings、802.1X Port Settings、802.1X User Settings、Guest VLAN、Authenticator State、Authenticator Statistics、Authenticator Session Statistics、Authenticator Diagnostics、Initialize Port-based Port(s)、Initialize Host-based Port(s)、Reauthenticate Port-based Port(s)、Reauthenticate Host-based Port(s)	250
	RADIUS	RADIUS サーバの設定を行います。: Authentication RADIUS Server Settings、RADIUS Accounting Setting、RADIUS Authentication、RADIUS Account Client	261
	IP-MAC-Port Binding (EI モードのみ)	IP アドレス、MAC アドレスおよびポートを結合し、レイヤ間通信を行います。: IMPB Global Settings、IMPB Port Settings、IMPB Entry Settings、MAC Block List、DHCP Snooping、ND Snooping	264
	MAC-based Access Control	MAC アドレス認証機能を設定します。: MAC-based Access Control Settings、MAC-based Access Control Local Settings、MAC-based Access Control Authentication State	
	Web-based Access Control	Web ベースアクセスコントロールを設定します。: WAC Global Settings、WAC User Settings、WAC Port Settings、WAC Authentication State、WAC Customize Page	274
	Japanese Web-based Access Control	JWAC の有効化および設定をします。: JWAC Global Settings、JWAC Port Settings、JWAC User Settings、JWAC Authentication State、JWAC Customize Page Language、JWAC Customize Page	280
	Compound Authentication (EI モードのみ)	コンパウンド認証方式を設定します。: Compound Authentication Settings、Compound Authentication Guest VLAN Settings、Compound Authentication MAC Format Settings	285
	IGMP Access Control Settings	各ポートに IGMP 認証（IGMP アクセスコントロール）を設定します。	288
	Port Security	ダイナミックな MAC アドレス学習をロックします。: Port Security Settings、Port Security VLAN Settings、Port Security Entries	289
	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。	293
	BPDU Attack Protection	ポートに BPDU 防止機能を設定します。	294
	Loopback Detection Settings	ループバック検知機能の設定を行います。	295
	RPC PortMapper Filter Settings	RPC ポートマップフィルタの設定を指定のポートに行います。	296
	NetBIOS Filtering Setting	NetBIOS フィルタ設定を行います。	297
	Traffic Segmentation Settings	ポートのトラフィックフローを制限します。	298
	DHCP Server Screening	不正な DHCP サーバへのアクセスを拒否します。: DHCP Server Screening Port Settings、DHCP Offer Permit Entry Settings	299
	Access Authentication Control	TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。: Enable Admin、Authentication Policy Settings、Application Authentication Settings、Accounting Settings、Authentication Server Group Settings、Authentication Server Settings、Login Method Lists Settings、Enable Method Lists Settings、Accounting Method Lists Settings、Local Enable Password Settings	300
	SSL Settings	証明書の設定、暗号スイートの設定を行います。: SSL Settings、SSL Certification Settings	309
	SSH	SSH サーバ、SSH アルゴリズム、SSH ユーザ認証の設定を行います。: SSH Settings、SSH Authentication Method and Algorithm Settings、SSH User Authentication List	311
	DoS Attack Prevention Settings	各 DoS 攻撃に対して防御設定を行います。	315
	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。	316
	Safeguard Engine Settings	セーフガードエンジンの設定を行います。	317

メイン メニュー	サブメニュー	説明	参照 ページ
Network Application	DHCP	DHCP リレーの設定を行います。: DHCP Relay、DHCPv6 Relay、DHCP Local Relay Settings	319
	PPPoE Circuit ID Insertion Settings（EI モードのみ）	システムは、受信した PPPoE Discovery および Request パケットに対して Circuit ID タグを挿入または削除します。	327
	SMTP Settings	スイッチのイベントを送信する SMTP サーバを設定します。	328
	SNTP	本製品に時刻設定をします。: SNTP Settings、Time Zone Settings	329
	UDP	UDP 送信先ポートに応じて、特定のブロードキャストをサーバに送信します。: UDP Helper、UDP Helper Server Settings	331
	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。	333
OAM	CFM（EI モードのみ）	CFM 機能を設定します。: CFM Settings、CFM Port Settings、CFM MIPCCM Table、CFM Loopback Settings、CFM Linktrace Settings、CFM Packet Counter、CFM Fault Table、CFM MP Table	335
	Ethernet OAM（EI モードのみ）	ポートにイーサネット OAM モード、イベント、ログを設定します。: Ethernet OAM Settings、Ethernet OAM Configuration Settings、Ethernet OAM Event Log、Ethernet OAM Statistics	347
	DULD Settings（EI モードのみ）	ポートにおいて単方向リンク検出の設定および表示を行います。	350
	Cable Diagnostics	ケーブル診断を行います。	351
Monitoring	Utilization	CPU 使用率、ポートの帯域使用率を表示します。: CPU Utilization、DRAM & Flash Utilization、Port Utilization	352
	Statistics	パケット統計情報とエラー統計情報を表示します。: Port Statistics、Packet Size	354
	Mirror	ポートミラーリングの設定を行います。: Port Mirror Settings、RSPAN Settings	363
	sFlow（EI モードのみ）	sFlow 機能の設定を行います。: sFlow Global Settings、sFlow Analyzer Server Settings、sFlow Flow Sampler Settings、sFlow Counter Poller Settings	365
	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。: Broadcast Ping Relay Settings、Ping Test	368
	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。	369
	Peripheral	デバイス環境機能はスイッチの内部温度ステータスを表示します。: Device Environment	370

第 6 章　System Configuration（システム設定）

本章ではデバイス情報の確認、IP アドレスの設定、スタックの管理、ポートパラメータの設定、ユーザアカウントの設定、システムログの設定と管理、システム時刻の設定、SNMP システム管理について説明します。

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

サブメニュー	説明	参照ページ
Device Information（デバイス情報）	スイッチの主な設定情報を表示します。	42
System Information Settings（システム情報 ）	スイッチの基本情報を表示します。	44
Port Configuration Settings（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（ポート名の設定）、Port Error Disabled（エラーによるポートの無効）、Jumbo Frame（ジャンボフレーム設定）、Port Media Type（ポートメディアタイプ）、EEE Settings（EEE 設定）（H/W バージョン B1 のみ）	44
PoE（PoE の管理）	PoE システムの設定を行います。以下のメニューがあります。 PoE System Settings（PoE システム設定）、PoE Port Settings（PoE ポート設定）	53
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。	55
Warning Temperature Settings（温度警告設定）	システムの警告温度パラメータを設定します。	55
Trap Settings（トラップ設定）	ファンと電力トラップ状態を設定します。	56
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（システムログの設定）、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）	56
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。	60
Port Group Settings（ポートグループ設定）（EI 版のみ）	ポートグループを作成します。	60
Time Settings（時刻設定）	スイッチに時刻を設定します。	61
User Accounts Settings（ユーザアカウント設定）	ユーザおよびユーザの権限を設定します。	61
Command Logging Settings（コマンドログ設定）	コマンドログ設定を有効または無効にします。	63
Configuration Trap Settings（コンフィグレーショントラップ設定）	コンフィグレーションの保存、アップロード / ダウンロード時のトラップ送信についての設定します。	63
Stacking（スタック設定）	複数のスイッチを 1 つに結合し、Telnet、Web などのインタフェースから管理します。以下のメニューがあります。 Stacking Device Table（スタックデバイステーブル）、Stacking Mode Settings（スタックモード設定）	64

Device Information（デバイス情報）

ログイン時に自動的に表示されるスイッチの主な機能の設定内容です。他の画面から「Device Information」画面に戻るためには、「DGS-3120 Series」をクリックします。
「Device Information」画面にはデバイスの一般的な情報として設定する項目があります。これには、システム名、場所、接続、システム MAC アドレス、システム稼働時間、IP アドレス、ファームウェア、ブート、およびハードウェアのバージョン情報などが含まれます。また、デバイスの各機能へのショートカットを提供します。以下の手順で一般的なシステム情報を定義します。

ツリービューの製品名（例 : DGS-3120-24TC）をクリックし、以下の画面を表示します。

図 6-1　Device Information 画面（SI モード）

図 6-2　Device Information 画面（EI モード）

「Device Information」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 /PROM 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	管理 VLAN の状態を表示します。
Login Timeout (min)	ユーザが何もしなかった場合にデバイスがタイムアウトするまでの時間を表示します。初期値は 10（分）です。
System Time	システムの日付を表示します。日 / 月 / 年で表示します。
Firmware Type	ファームの種類を表示します。SI（スタンダード）/EI（エンハンスド）の 2 つがあります。
Device Status and Quick Configurations	
SNTP	システムクロックの設定を参照するためのショートカットです。
Spanning Tree	STP 機能の状態（有効 / 無効）の表示と、STP の設定へのショートカットです。
SNMP	SNMP トラップ機能の状態（有効 / 無効）の表示と、SNMP トラップの設定へのショートカットです。
Safeguard Engine	Safeguard エンジン機能の状態（有効 / 無効）の表示と、Safeguard エンジンの設定へのショートカットです。
System Log	System Log 機能の状態と（有効 / 無効）の表示と、System Log 機能の設定へのショートカットです。
SSL	SSL（Secure Socket Layer）機能の状態（有効 / 無効）の表示と、SSL の設定へのショートカットです。
GVRP	GVRP（Group VLAN Registration Protocol）機能の状態（有効 / 無効）の表示と、GVRP の設定へのショートカットです。
Password Encryption	パスワード暗号化の状態（有効 / 無効）の表示と、パスワード設定へのショートカットです。
Telnet	Telnet 機能の状態（有効 / 無効）の表示と、Telnet 設定へのショートカットです。
Web	Web 管理の状態（有効 / 無効）の表示と、Web 設定へのショートカットです。
VLAN Trunk	VLAN Trunk の状態（有効 / 無効）の表示と、VLAN Trunk 設定へのショートカットです。
Jumbo Frame	Jumbo Frame 機能の状態（有効 / 無効）の表示と、Jumbo Frame の設定へのショートカットです。
MLD Snooping	MLD Snooping 機能の状態（有効 / 無効）の表示と、MLD の設定へのショートカットです。
IGMP Snooping	IGMP Snooping 機能の状態（有効 / 無効）の表示と、IGMP の設定へのショートカットです。
MAC Notification	MAC Notification 機能の状態（有効 / 無効）の表示と、MAC Notification の設定へのショートカットです。
802.1X	802.1X 機能の状態（有効 / 無効）の表示と、802.1X の設定へのショートカットです。
SSH	SSH（Secure Shell Protocol）機能の状態（有効 / 無効）の表示と、SSH の設定へのショートカットです。
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へのショートカットです。
Single IP Management	Single IP Management 機能の状態（有効 / 無効）の表示と、Single IP Management の設定へのショートカットです。
CLI Paging	CLI Paging 機能の状態（有効 / 無効）の表示と、CLI Paging の設定へのショートカットです。
HOL Blocking Prevention	HOL Blocking Prevention 機能の状態（有効 / 無効）の表示と、HOL Blocking Prevention の設定へのショートカットです。
DHCP Relay	DHCP Relay 機能の状態（有効 / 無効）の表示と、DHCP Relay 設定へのショートカットです。

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 Settings 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。

System Information Settings（システム情報）

スタックメンバに設定されたデバイス情報を提供します。

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

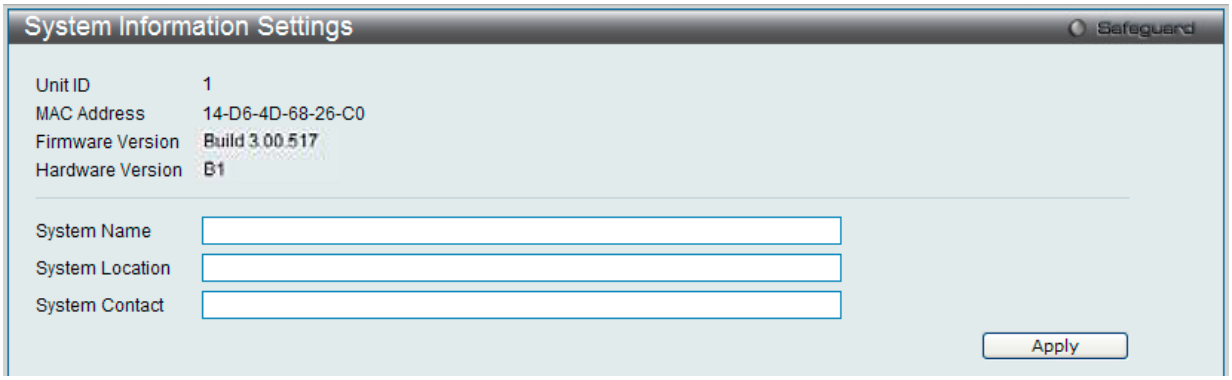


図 6-3　System Information Settings 画面

画面には以下の項目があります。

項目	説明
Unit ID	スタックマスタユニットの ID 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。
Firmware Version	スタックメンバのファームウェアバージョンを表示します。
Hardware Version	スタックメンバ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	担当者名を表示します。（半角英数字 160 文字以内）

「Apply」ボタンをクリックすると設定が更新されます。

Port Configuration（ポート設定）

各ポートの設定を行います。

DDM（DDM 設定）（EI モードのみ）

本フォルダにはスイッチに Digital Diagnostic Monitoring（DDM）機能を実行する画面があります。これらの画面により、スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定（アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx（送信）電力しきい値設定、および Rx（受信）電力しきい値設定）を行うことができます。

DDM Settings（DDM 設定）

超過しているアラームしきい値または警告しきい値を超過するイベントが発生した場合に、指定ポートに行う動作を設定します。

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。

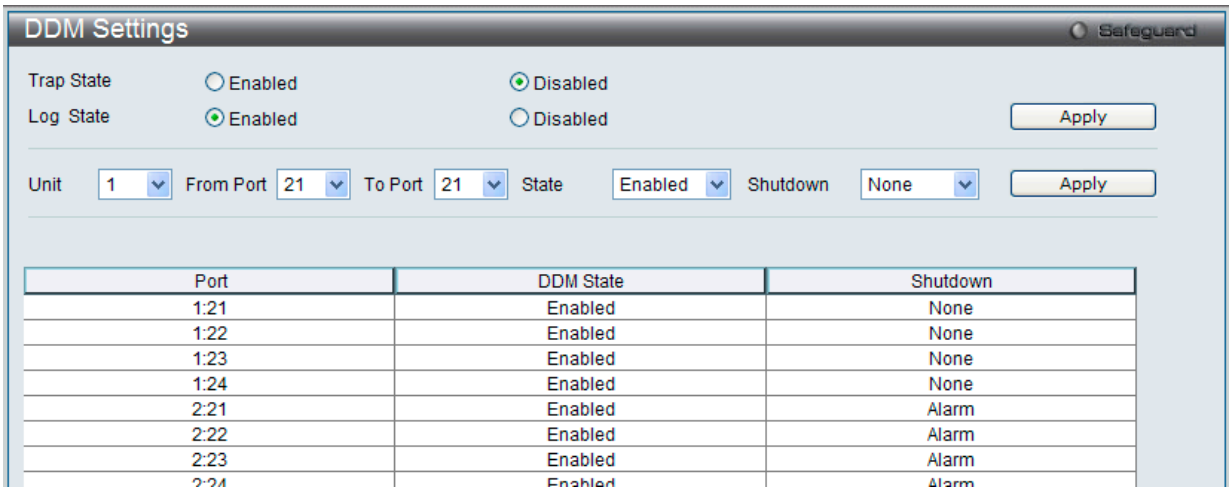


図 6-4　DDM Settings 画面

以下の項目を使用して設定します。

項目	説明
Trap State	操作パラメータがアラームまたは警告しきい値を超過した際にトラップを送信するか否かを指定します。
Log State	操作パラメータがアラームまたは警告しきい値を超過した際にログを送信するか否かを指定します。
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。
State	DDM の状態を有効または無効にします。
Shutdown	操作パラメータが Alarm または Warning しきい値を超過した際に、ポートをシャットダウンするか否か指定します。

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

スイッチの特定ポートに DDM 温度しきい値設定を行います。

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。

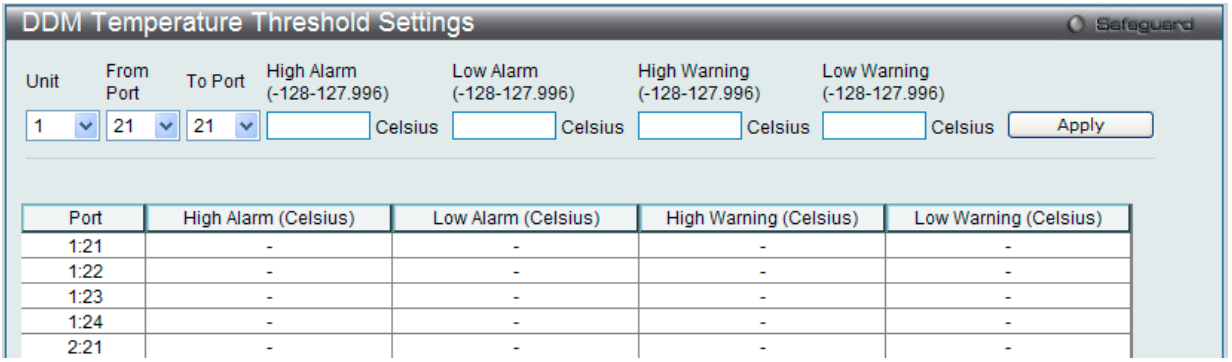


図 6-5　DDM Temperature Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm (-128-127.996)	警告温度の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。
Low Alarm (-128-127.996)	警告温度の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。
High Warning (-128-127.996)	注意温度の上限を指定します。操作パラメータが本値より高くなると、注意に関連するアクションが行われます。
Low Warning (-128-127.996)	注意温度の下限を指定します。操作パラメータが本値より低くなると、注意に関連するアクションが行われます。

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。

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

スイッチの特定ポートに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。

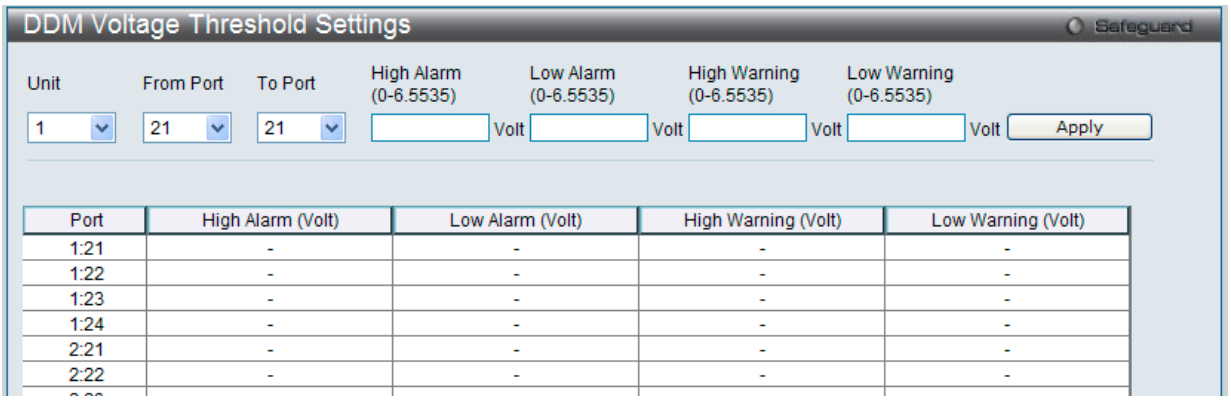


図 6-6　DDM Voltage Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm (0-6.5535)	警告電圧の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。
Low Alarm (0-6.5535)	警告電圧の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。
High Warning (0-6.5535)	注意電圧の上限を指定します。操作パラメータが本値より高くなると、注意に関連するアクションが行われます。
Low Warning (0-6.5535)	注意電圧の下限を指定します。操作パラメータが本値より低くなると、注意に関連するアクションが行われます。

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。

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

スイッチの特定ポートに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。

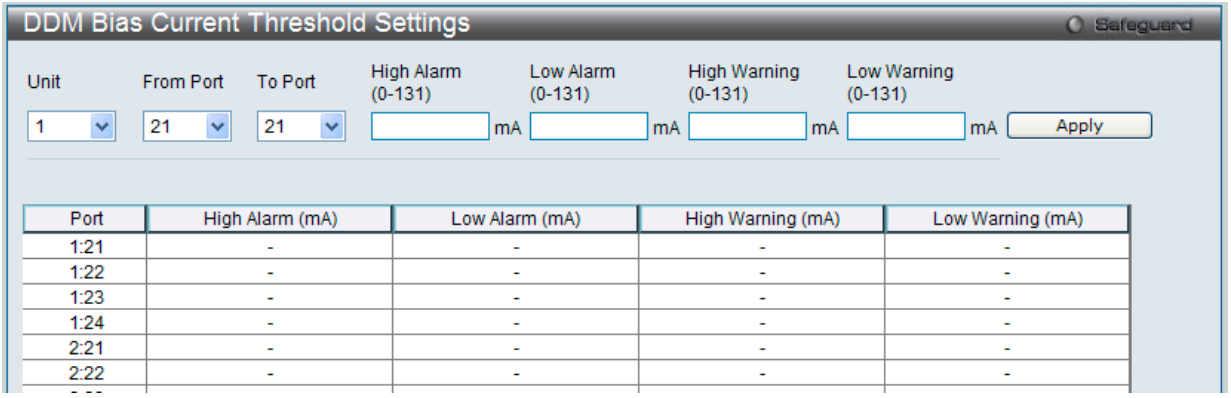


図 6-7　DDM Bias Current Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm (0-131)	警告電流の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。
Low Alarm (0-131)	警告電流の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。
High Warning (0-131)	注意電流の上限を指定します。操作パラメータが本値より高くなると、注意に関連するアクションが行われます。
Low Warning (0-131)	注意電流の下限を指定します。操作パラメータが本値より低くなると、注意に関連するアクションが行われます。

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。

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

スイッチの特定ポートに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。

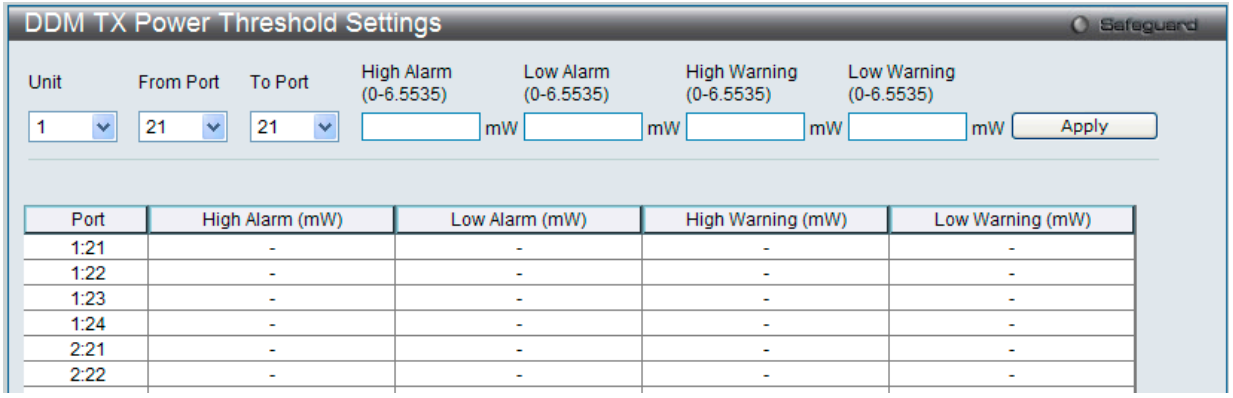


図 6-8　DDM TX Power Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm (0-6.5535)	警告送信電力の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。
Low Alarm (0-6.5535)	警告送信電力の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。
High Warning (0-6.5535)	注意送信電力の上限を指定します。操作パラメータが本値より高くなると、注意に関連するアクションが行われます。
Low Warning (0-6.5535)	注意送信電力の下限を指定します。操作パラメータが本値より低くなると、注意に関連するアクションが行われます。

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。

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

スイッチの特定ポートに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。

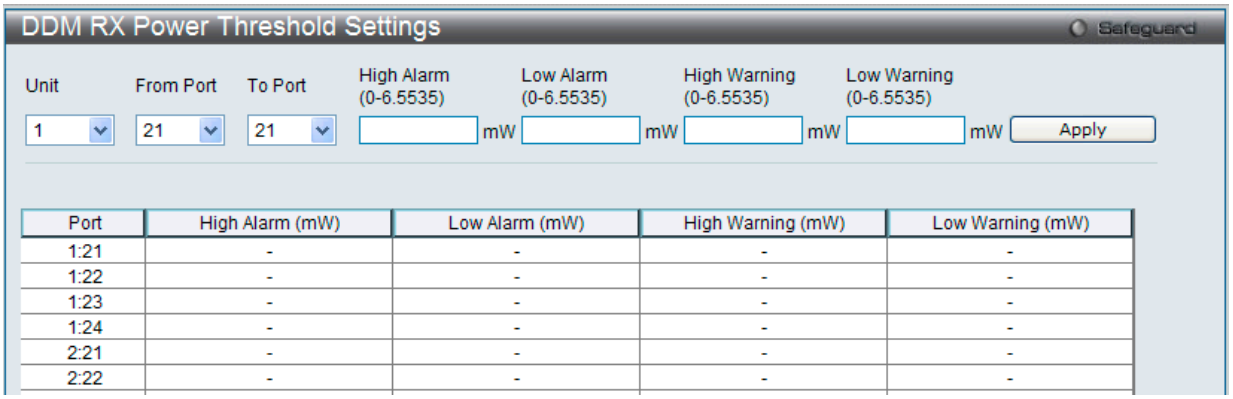


図 6-9　DDM RX Power Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
From / To Port	適用するポートまたはポート範囲を指定します。
High Alarm (0-6.5535)	警告受信電力の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。
Low Alarm (0-6.5535)	警告受信電力の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。
High Warning (0-6.5535)	注意受信電力の上限を指定します。操作パラメータが本値より高くなると、注意に関連するアクションが行われます。
Low Warning (0-6.5535)	注意受信電力の下限を指定します。操作パラメータが本値より低くなると、注意に関連するアクションが行われます。

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。

DDM Status Table（DDM ステータステーブル）

指定ポートで現在操作中の DDM パラメータと SFP モジュールの値を表示します。

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。

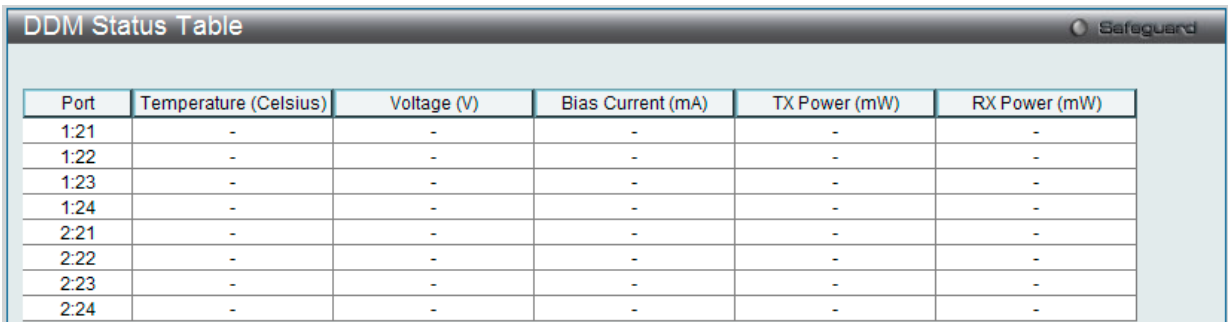


図 6-10　DDM Status Table 画面

以下の項目を使用して設定します。

項目	説明
ユニット : ポート	ユニットおよびポート番号を表示します。
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）

ポートのプロパティ設定を行います。ギガビットポートは全二重通信のみであり、他とは異なる特有のリストが表示されます。

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

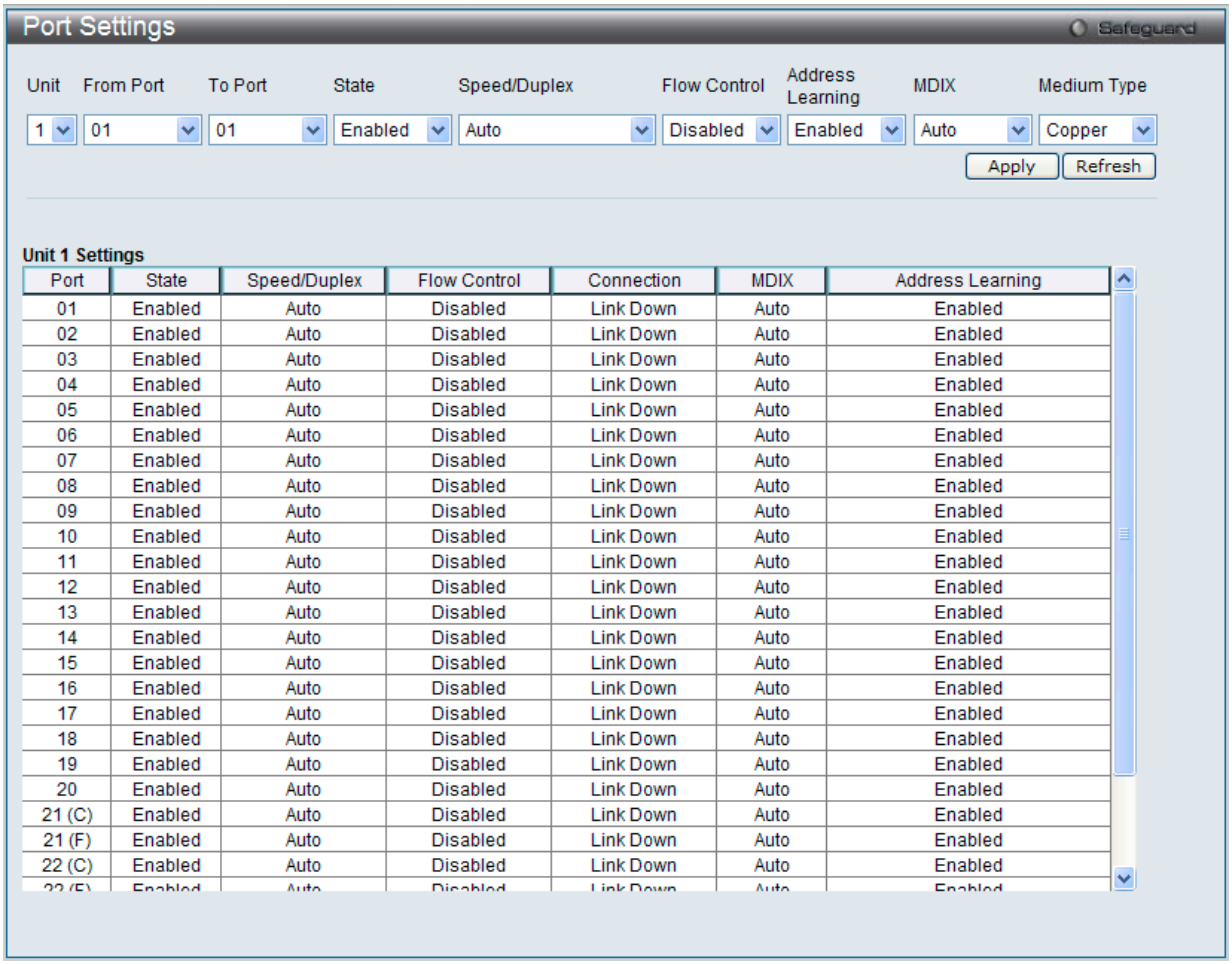


図 6-11　Port Setting 画面

画面には以下の項目があります。

項目	説明
Unit	ポート設定を表示するスタックメンバまたは LAG を設定します。
From Port/To Port	ポート設定を適用するポート範囲を設定します。本欄はユニット番号が選択された場合にだけ表示されます。
State	インタフェースが現在操作可能か否かを定義します。 • Enabled - インタフェースが現在トラフィックを送受信できることを示します。 • Disabled - インタフェースが現在トラフィックを送受信できないことを示します。
Speed/Duplex	「Speed/Duplex」欄を切り替えることでポートの速度および全二重 / 半二重状態を選択します。「Auto」は 10/100/1000Mbps 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。（常時全二重の 1000Mbps を除く）。「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。 他のオプションには「10M Half」、「10M Full」、「100M Half」、「100M Full」、「1000M Full_Master」、および「1000M Full_Slave」があります。「Auto」以外のオプションのポート設定は固定となります。 スイッチは 2 つのタイプ（「1000M Full_Master」および「1000M Full_Slave」）のギガビット接続設定ができます。 ギガビット接続はフルデュプレックス接続だけをサポートしており、他の選択肢とは異なる特徴を持っています。「1000M Full_Master」および「1000M Full_Slave」パラメータは、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 ケーブル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。タイミング制御は、ローカルソースによってマスタの物理層に設定されます。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、他方の接続は「1000M Full_Slave」とする必要があります。その他の設定は両ポートのリンクダウンを引き起こします。
Flow Control	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。「Auto」は自動的にいずれかを使用します。
Connection	現在の接続速度が表示されます。
MDIX	• Auto - 最適なケーブル接続を自動的に設定します。 • Normal - ケーブル接続に Normal を選択します。 • Cross - ケーブル接続に Cross を選択します。 「Normal」を選択すると、MDI モードにあるポートはストレートケーブルを通して PC のネットワークボード、またはクロスケーブルで別のスイッチのポート（MDI モード）に接続することができます。「Cross」を選択すると、MDIX モードにあるポートはストレートケーブルで別のスイッチのポート (MDI モード) に接続することができます。
Address Learning	インタフェースが MAC アドレスを学習するかを設定します。 • Enabled - インタフェースにおける MAC アドレスの学習を有効にします。MAC アドレスの学習を有効にすると、送受信の MAC アドレスが転送テーブルに記録されます。（初期値） • Disabled - インタフェースにおける MAC アドレスの学習を無効にします。
Medium Type	コンボポートを設定する場合、使用するケーブルメディアのタイプを定義します。

「Apply」ボタンをクリックすると設定が更新されます。

注意 コンボポートにおいて、SFP の RX が信号を受信している状態では、SFP Port、Coppoer ポートともリンクアップしません。

Port Description Settings（ポート名の設定）

デバイスのポートの詳細説明を設定します。

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

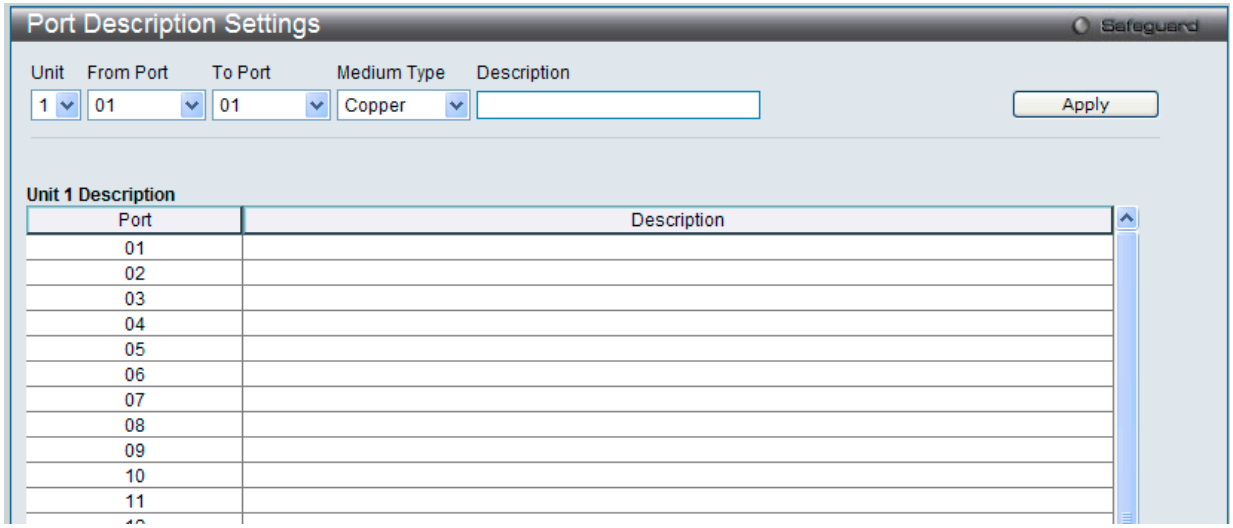


図 6-12　Port Description 画面

画面には以下の項目があります。

項目	説明
Unit	ポート設定を表示するスタックメンバを設定します。
From Port/To Port	ポートパラメータを設定するポートの最初 / 最後の番号を設定します。
Medium Type	コンボポートを設定する場合、使用するケーブルメディアのタイプを定義します。
Description	ユーザ定義によるポートの説明を設定します。

「Apply」ボタンをクリックすると設定が更新されます。

Port Error Disabled（エラーによるポート無効）

接続が無効であるポートに関する情報（ループ検出の理由や接続ステータス）を表示します。

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

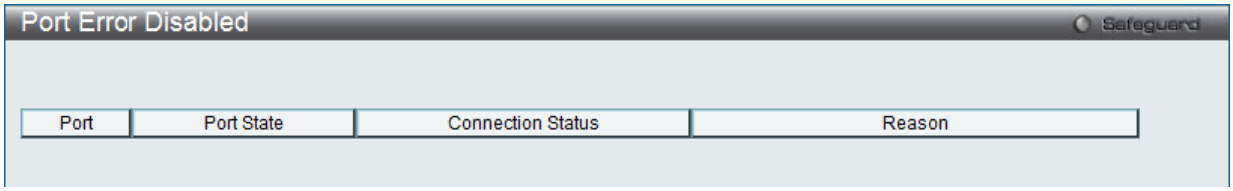


図 6-13　Port Error Disabled 画面

画面には以下の項目があります。

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」（有効）または「Disabled」（無効））を表示します。
Connection Status	各ポートのアップリンク状況を表示します。
Reason	ループの発生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。

「Apply」ボタンをクリックすると設定が更新されます。

Port Media Type（ポートメディアタイプ）

ポートメディアのタイプに関する情報を表示します。

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

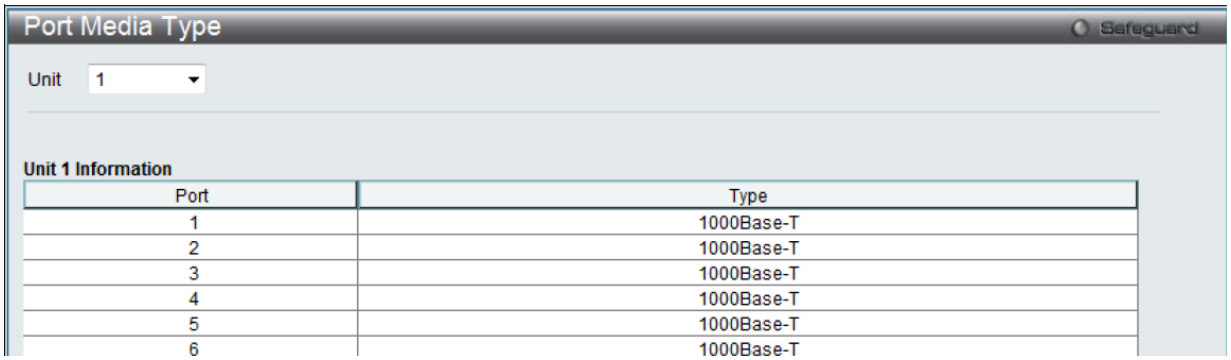


図 6-14　Port Media Type 画面

画面には以下の項目があります。

項目	説明
Unit	表示するユニットを指定します。
Port	メディアタイプを表示するポートです。
Type	ポートメディアのタイプです。

Jumbo Frame Settings（ジャンボフレーム設定）

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。ジャンボフレームは、1518 バイト以上のペイロードを持つイーサネットフレームです。本スイッチは最大 13312 バイトまでのジャンボフレームをサポートします。「Jumbo Frame Settings」画面では、スイッチでジャンボフレームを扱うことを可能にします。これによりオーバヘッド、処理時間、割り込みを確実に減らすことができます。

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

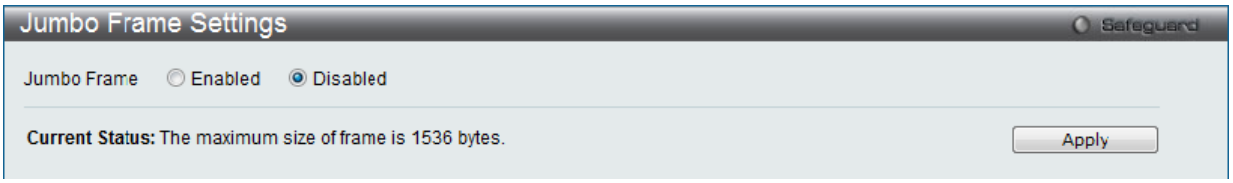


図 6-15　Jumbo Frame Settings 画面

画面には以下の項目があります。

項目	説明
Jumbo Frame	スイッチのジャンボフレーム機能を有効にします。初期値は無効です。無効の場合最大フレーム値は 1536 バイトです。有効にすると最大フレームサイズは 13312 です。

「Apply」ボタンをクリックすると設定が更新されます。

EEE Settings（EEE 設定）（H/W バージョン B1 のみ）

Energy Efficient Ethernet (EEE) は IEEE 802.3az によって定義され、パケットの送受信がない時に、スイッチの電力消費を抑える設計になっています。
System Configuration > Port Configuration > EEE Settings の順にクリックし、以下の画面を表示します。

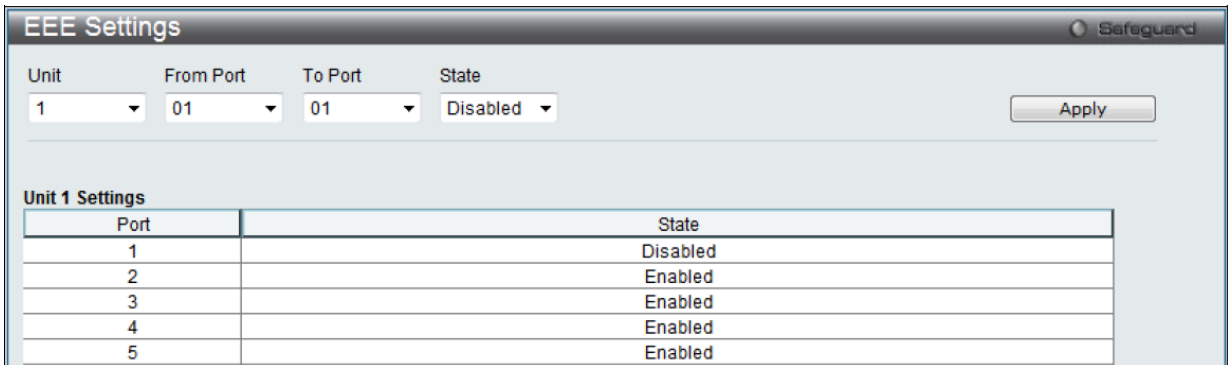


図 6-16　EEE Settings 画面

画面には以下の項目があります。

項目	説明
Unit	ポート設定を表示するユニットを設定します。
From Port/To Port	EEE を設定するポートの最初 / 最後の番号を設定します。
State	ポートのステータス（「Enabled」（有効）または「Disabled」（無効））を指定します。

「Apply」ボタンをクリックすると設定が更新されます。

注意　ハードウェアバージョン A1/A2 の機器には EEE 機能は実装されていません。

PoE（PoE の管理）

DGS-3120-24PC と DGS-3120-48PC は IEEE の 802.3af と IEEE802.3at 規格の PoE 機能をサポートしています。すべてのポートは 30W まで PoE をサポートしています。ポート 1-24 はカテゴリ 5 以上の UTP イーサネットケーブル経由で PoE 受電機器に約 48VDC 電力を供給できます。本スイッチは PSE pinout Alternative A を準拠しており、電力はピン 1、2、3、および 6 を通じて供給されます。本スイッチは全ての D-Link 802.3af 対応デバイスと接続できます。
本スイッチでは次の PoE 機能を使用することができます。

- Auto-discovery 機能は PD(受電機器) に自動的に電力を供給します。
- Auto-disable 機能は次の 2 つの条件が揃うと動作します。まず消費電力がシステム電源のリミットを超えている場合と各ポートの消費電力リミットを超えている場合です。
- Active circuit 防止機能は電力の不足が生じた場合、自動的にポートを無効にする機能です。他のポートは有効性は変わりません。

802.3af/at 準拠の受電機器の最大受信電力一覧：

クラス	受電機器の最大受信電力
0	12.95W
1	3.84W
2	6.49W
3	12.95W
4	29.5W

PSE を使用したの最大電力一覧：

クラス	受電機器の最大受信電力
0	15.4W
1	4W
2	7W
3	15.4W
ユーザ定義	35W

スイッチの PoE の設定は、**System Configuration > PoE** をクリックします。「PoE System Settings」画面では、PoE システムの電力制御と電力切断方法を設定します。PoE システムの電力制御を行う場合は、Power Limit の項目に 37W から 760W の間で数値を入力します。消費電力の合計が設定値を超えた場合は、PoE コントローラ（PSE）は電力のオーバーロードを避けるために電力供給を停止します。

PoE System Settings（PoE システム設定）

現在の電力消費、PoE トラップを含むデバイスの PoE 情報を参照および変更します。

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

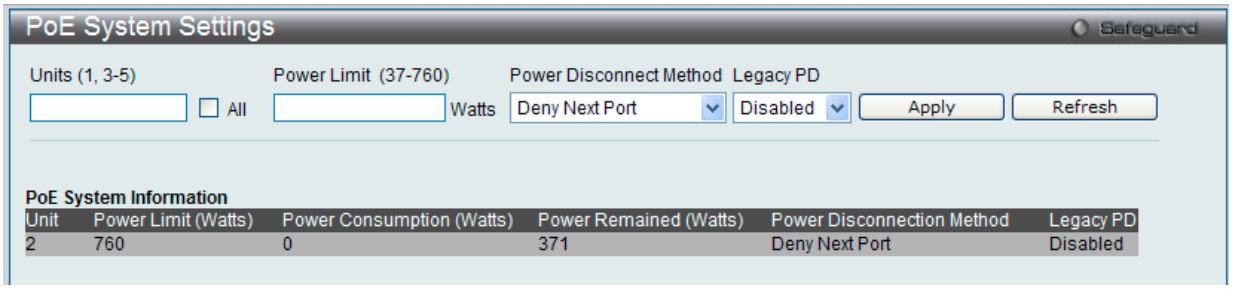


図 6-17　PoE System Settings 画面

画面には以下の項目があります。

項目	説明
Unit	ユニット番号を設定します。全てのユニットを選択する場合は「All」にチェックします。
Power limit（37-760）	インタフェースに利用可能な総電力供給量（W）を示します。37-760W の間で電力値を入力することが可能です。 初期値は 760W です。
Power Disconnect Method	PoE コントローラは、「Deny Next Port」または「Deny Low Priority Port」によって、供給可能な電力の上限値の超過を防ぎ、スイッチの給電レベルを一定内に保ちます。「Power Disconnect Method」のプルダウンメニューから方法を選択します。 • Deny Next Port - スイッチが給電できる最大電力に達した場合には、優先度に関わらず、新規に接続された Pd に給電しません。（初期値） • Deny Low Priority Port - スイッチが給電できる最大電力に達した場合に新規の PD が接続された場合は、ポート優先度の低いポートを切断し、新規に接続された PD に給電します。
Legacy PD	プルダウンメニューを使用して、レガシー PD の検索の有効 / 無効を設定します。

「Apply」ボタンをクリックすると設定が更新されます。

PoE Port Settings（PoE ポート設定）

PoE 機能の有効化、現在の電力消費の表示、PoE トラップの有効化などシステムの PoE 情報の操作を行います。

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

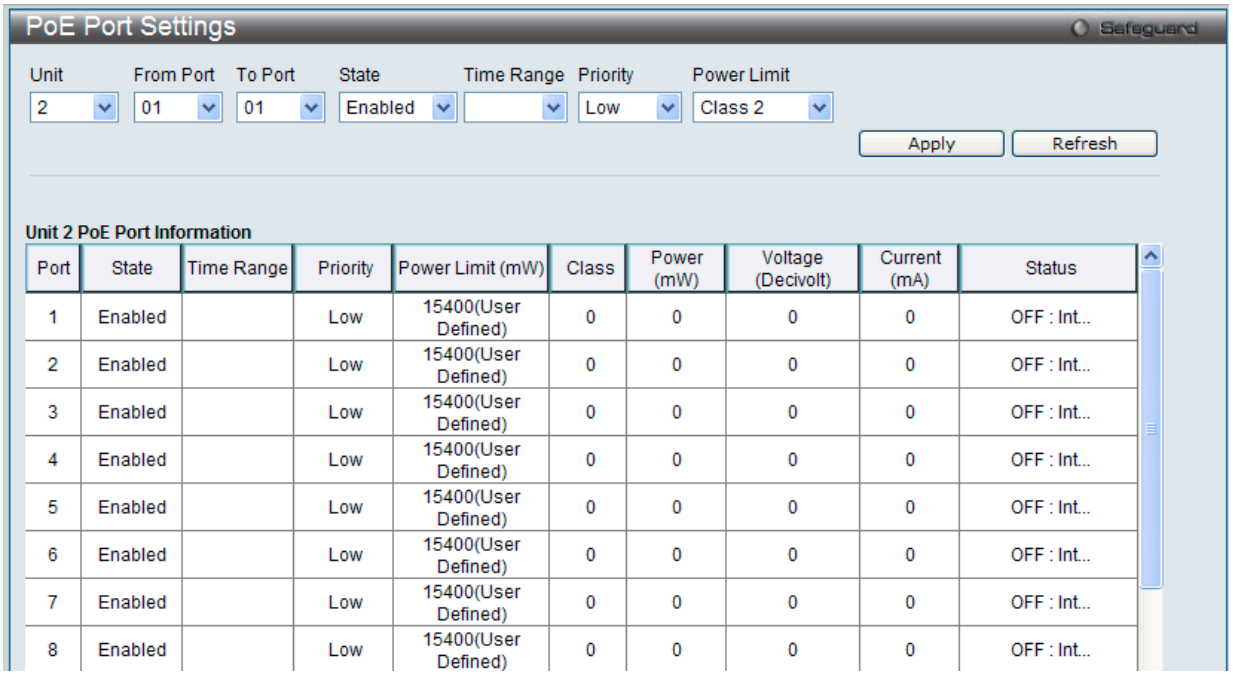


図 6-18　PoE Port Setting 画面

画面には以下の項目があります。

項目	説明
Unit	PoE 設定を表示するスタックメンバを設定します。
From Port/To Port	PoE 設定をするポートの最初 / 最後の番号を設定します。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>State</td><td>インタフェースで PoE を有効にするかを設定します。
• Enabled - インタフェースで PoE を有効にします。
• Disabled - インタフェースで PoE を無効にします。（初期設定）</td></tr>
<tr><td>Time Range</td><td>ポートの PoE 機能を有効にする時間設定を行います。ポートは設定した時間内のみ給電を行います。</td></tr>
<tr><td>Priority</td><td>プルダウンメニューを使ってポートの優先度（Critical、High、Low）を指定します。
ポート優先度はシステムがどのポートに優先的に電力供給を行うかを設定します。優先度には 3 段階あり「Critical」「High」「Low」で設定できます。複数のポートが同じ優先度を設定してある場合、ポート ID により優先度が決まります。低いポート ID 番号が高い優先度になります。優先度の設定は電力の供給順にも影響します。切断方法が優先度の低いポートに対し「deny」に設定されている場合、各ポートの優先度はシステムのポートへの電力供給に使用されます。</td></tr>
<tr><td>Power Limit</td><td>ポートごとの供給可能な電力の上限値。この値を超過すると前述の「Power Disconnect Method」を実行します。
802.3af/802.3at に基づき、PD（受電機器）のクラスにより最大使用電力の範囲が変わります。
<table>
<tr><th>クラス</th><th>PD の最大使用電力幅</th></tr>
<tr><td>0</td><td>0.44~12.95W</td></tr>
<tr><td>1</td><td>0.44~3.84W</td></tr>
<tr><td>2</td><td>3.84~6.49W</td></tr>
<tr><td>3</td><td>6.49~12.95W</td></tr>
<tr><td>4</td><td>29.5W</td></tr>
</table>
下記の表はポート対応した電力値のクラスになります。
各クラスは電力値の制限は消費電力値の範囲よりも大きくなっています。これらはケーブルでの電力ロスを計算に入れているためです。
<table>
<tr><th>クラス</th><th>最大出力電力値</th></tr>
<tr><td>0</td><td>15400mW</td></tr>
<tr><td>1</td><td>4000mW</td></tr>
<tr><td>2</td><td>7000mW</td></tr>
<tr><td>3</td><td>15400mW</td></tr>
<tr><td>ユーザ設定</td><td>35000mW</td></tr>
</table>
</td></tr>
</table>

「Apply」ボタンをクリックすると設定が更新されます。

Serial Port Settings（シリアルポート設定）

ボーレートの値と自動ログアウト時間を調整します。

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。

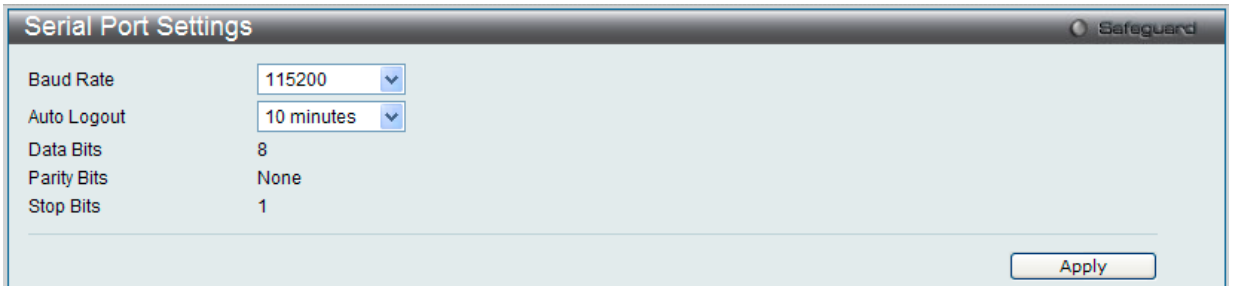


図 6-19　Serial Port Settings 画面

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 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。初期値は 10（分）です。
Data Bits	シリアルポート接続で使用されているデータビット値を表示します。
Parity Bits	シリアルポート接続で使用されているパリティビット値を表示します。
Stop Bits	シリアルポート接続で使用されているストップビット値を表示します。

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。スイッチをリセットまたはリブートしても、ボーレート設定は変更されません。ボーレートは、再び設定行った場合にだけ変更されます。シリアルポートのボーレート設定はスイッチの設定ファイルに保存されません。スイッチをリセットしてもボーレートは初期設定に復元されません。

Warning Temperature Settings（温度警告設定）

システムの警告温度の設定を行います。

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。

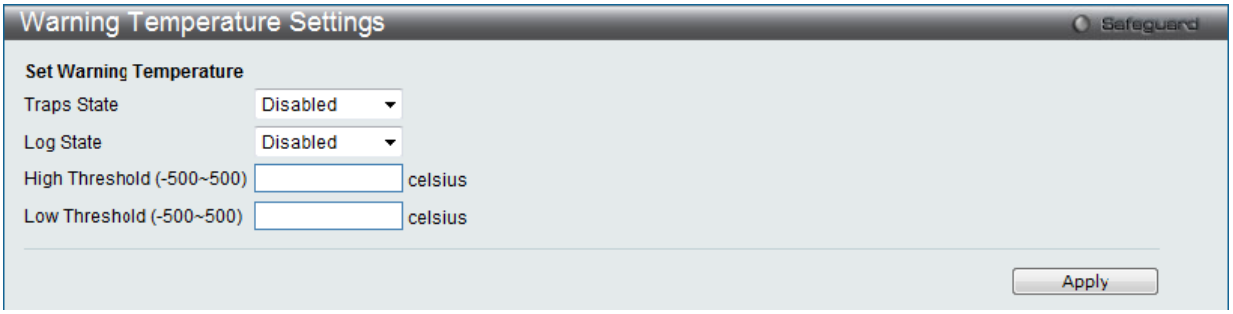


図 6-20　Warning Temperature Settings 画面

画面には次の項目があります。

項目	説明
Traps State	プルダウンメニューを使用して、警告温度設定のトラップを有効 / 無効に設定します。
Log State	プルダウンメニューを使用して、警告温度設定のログを有効 / 無効に設定します。
High Threshold	警告温度設定のしきい値（上限）を入力します。
Low Threshold	警告温度設定のしきい値（下限）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。

Trap Settings（トラップ設定）

ファンと電力トラップ状態を設定します。

System Configuration > Trap 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。

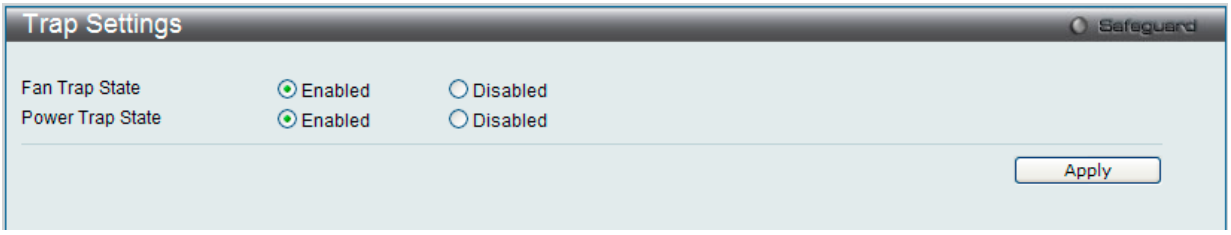


図 6-21　Trap Settings 画面

System Log Settings 画面には次の項目があります。

項目	説明
Fan Trap State	ファンのトラップ状態を有効または無効にします。
Power Trap State	電力のトラップ状態を有効または無効にします。

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

System Log Configuration（システムログ構成）

「System Log Configuration」フォルダには「System Log Settings」と「System Log Host」の 2 つのメニューがあります。

System Log Settings（システムログ設定）

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 Log」を有効または無効にし、「System Log Save Mode Settings」を設定します。

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。

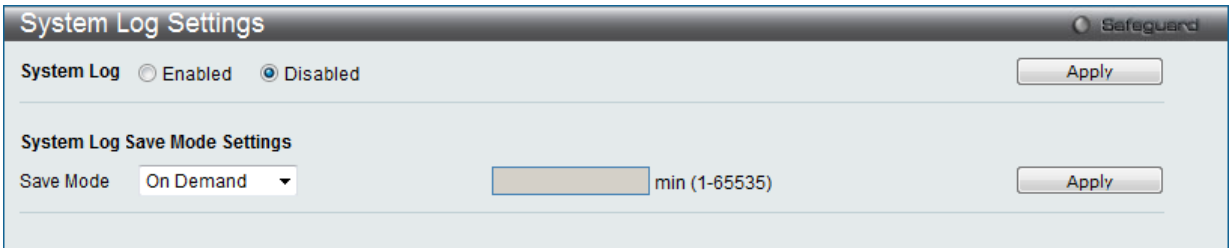


図 6-22　System Log Settings 画面

System Log Settings 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。初期値は「On Demand」です。 • 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」メニューを使用して保存します。 • 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。

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。

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

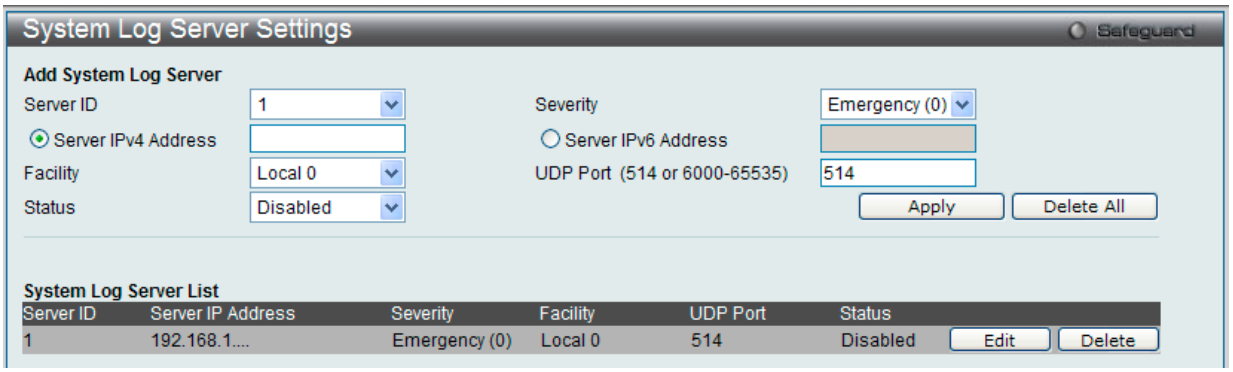


図 6-23　System Log Server 画面

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。
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。
UDP Port	ログを送信するサーバの UDP ポートを設定します。初期値は 514 です。
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。「Emergency」（緊急）、「Alert」（警告）、「Critical」（重大）、「Error」（エラー）、「Warning」（警告）、「Notice」（通知）、「Informational」（情報）、「Debug」（デバッグ）、「ALL」（すべて）「Level」（レベル）から選択します。
Facility	プルダウンメニューを使用して「Local 0」から「Local7」までの間を選択します。
Status	「Enabled」（有効）または「Disabled」（無効）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。

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。

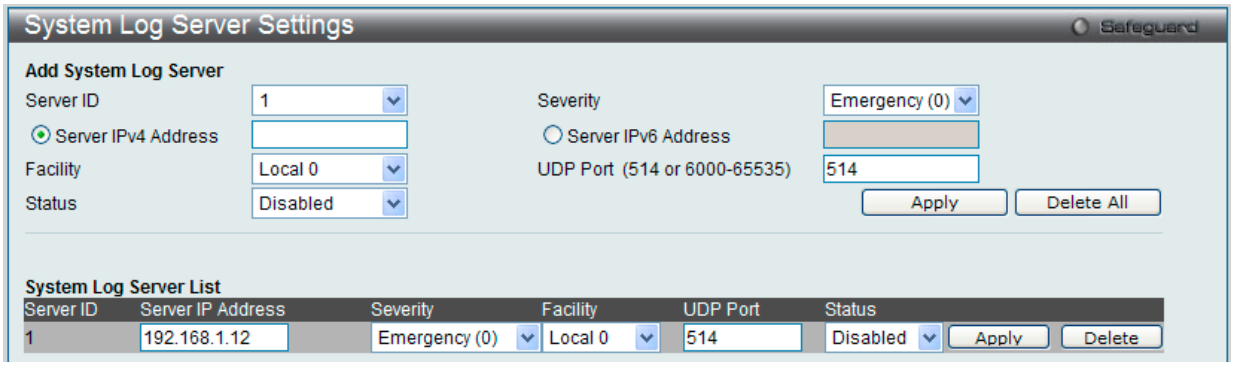


図 6-24　System Log Server Settings 画面 - Edit

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（システムログの設定）

管理者により設定されたシステムログの閲覧 / 消去を行うことが可能です。

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

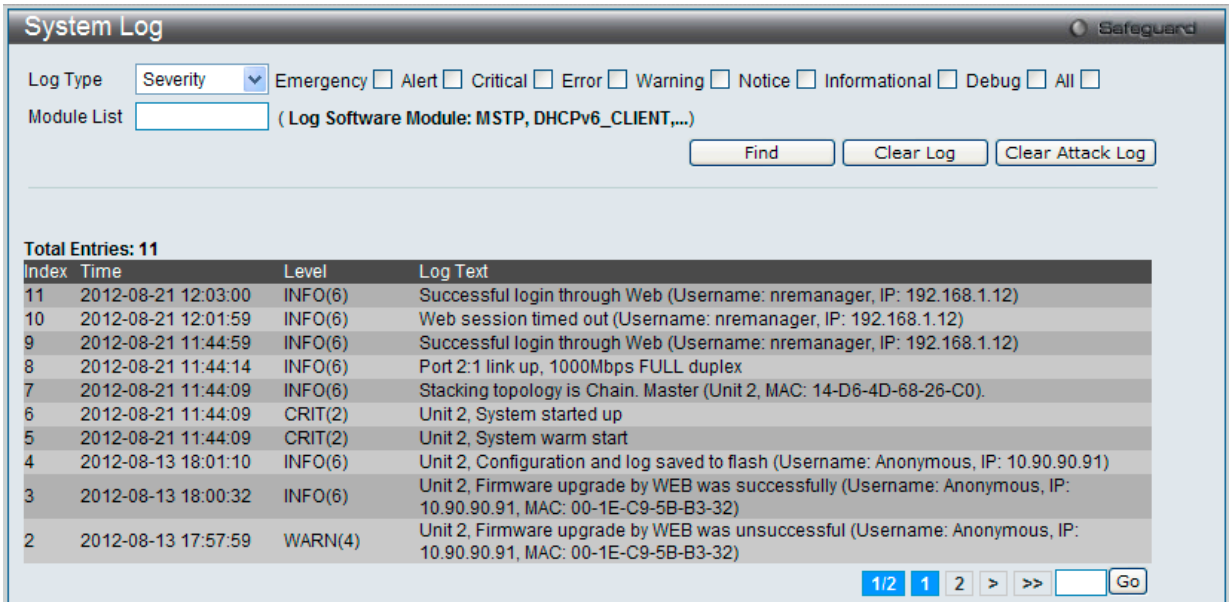


図 6-25　System Log 画面

本画面には次の項目があります。

項目	説明
Log Type	表示するログタイプをプルダウンメニューから選択します。 • Severity - プルダウンメニューから「Severity」を選択し、システムログレベルをプルダウンメニューから選択します。「Emergency」（緊急）、「Alert」（警告）、「Critical」（重大）、「Error」（エラー）、「Warning」（警告）、「Notice」（通知）、「Informational」（情報）、「Debug」（デバッグ）、「ALL」（すべて）「Level」（レベル）から選択します。全てのログを参照する場合「All」にチェックを入れます。 • Module List - 「Module List」を選択すると手動でモジュール名を入力する必要があります。有効なモジュールは「MSTP」「ERROR_LOG」「CFM_EXT」「ERPS」です。 • Attack Log - 「Attack Log」を選択すると全ての攻撃が表示されます。
Index	ヒストリログが作成された順に番号が振られています。高い番号が新しいログになります。
Time	スイッチが再起動されてからのログ作成日時が表示されます。
Level	ログエントリのレベルが表示されます。
Log Text	ログエントリの詳細について表示します。

「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アタックログからエントリをクリアします。

System Log & Trap Settings（システムログ / トラップの設定）

システムログの送信元 IP インタフェースアドレスの設定を行います。

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。

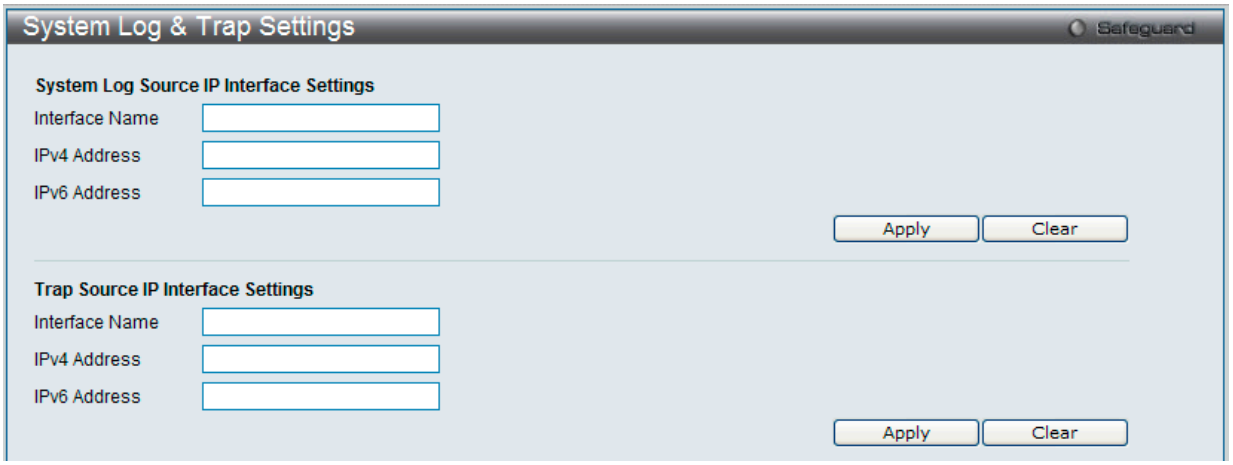


図 6-26　System Log & Trap 設定画面（EI モード）

本画面には次の項目があります。

項目	説明
Interface Name	IP インタフェース名を入力します。
IPv4 Address	IPv4 アドレスを入力します。
IPv6 Address	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、欄内に入力し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 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。

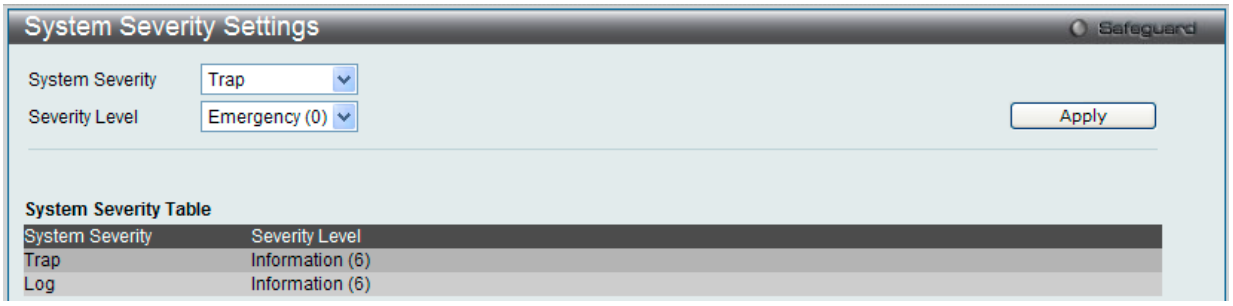


図 6-27　System Severity Settings 画面

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 - スイッチのログとして記録されます。 • Trap - SNMP エージェントに送信します。 • All - 両方のアクションが実行されます。
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。「Emergency」（緊急）、「Alert」（警告）、「Critical」（重大）、「Error」（エラー）、「Warning」（警告）、「Notice」（通知）、「Informational」（情報）、「Debug」（デバッグ）、「All」（すべて）「Level」（レベル）から選択します。

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。

Time Range Settings（タイムレンジ設定）

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。本設定は、Access Profile テーブルのアクセスプロファイルに適用されます。64 個のタイムレンジを入力することができます。

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。

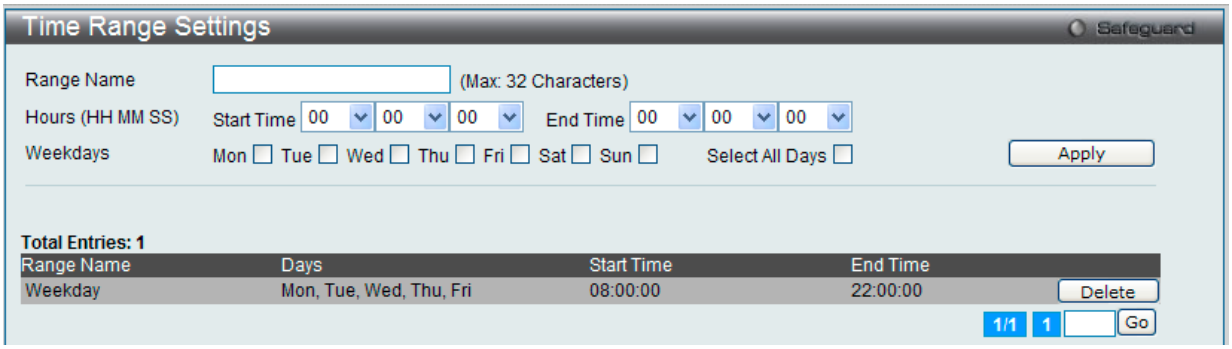


図 6-28　Time Range Settings 画面

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	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「Time Range Information」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。

Port Group Settings（ポートグループ設定）（EI モードのみ）

ポートグループの設定、ポートグループのポートの追加 / 削除を設定します。

System Configuration > Port 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。

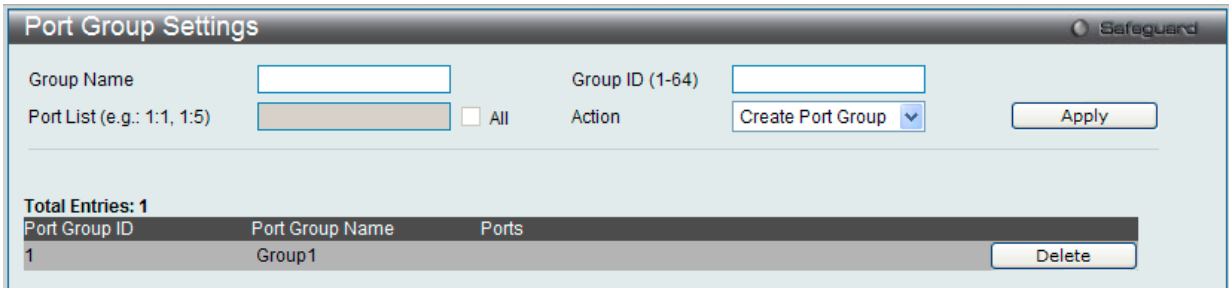


図 6-29　Port Group Settings 画面

以下の項目を設定することができます。

項目	説明
Group Name	ポートグループ名を入力します。
Group ID (1-64)	ポートグループの ID を入力します。
Port List	ポート / ポートリストを入力します。全てのポートを選択する場合は「All」にチェックをします。
Action	プルダウンメニューから「Create Port Group」（ポートグループ作成）、「Add Ports」（ポートの追加）、「Delete Ports」（ポートの削除）を選択します。

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。エントリを削除するには「Delete」を入力します。

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。

Time Settings（時間設定）

ここではスイッチの時間を設定します。

System Configuration > Time 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。

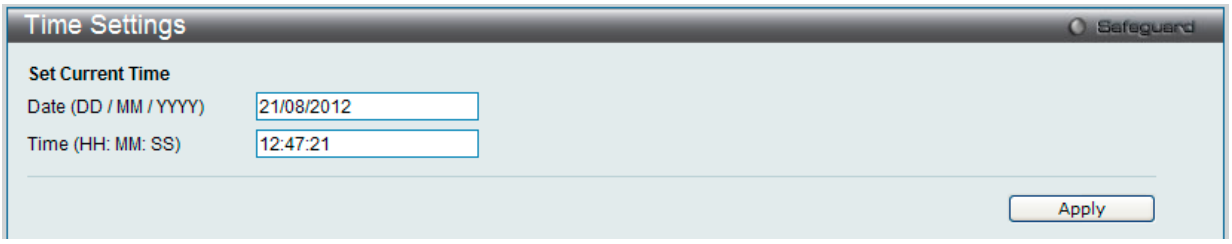


図 6-30　Time Settings 画面

以下の項目を設定することができます。

項目	説明
Date (DD/MM/YYYY)	システムに設定する日月年を設定します。
Time (HH:MM:SS)	システムに設定する秒分時を設定します。

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。

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。

User Accounts Settings（ユーザアカウント設定）

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。

System Configuration > User Accounts Settings の順にクリックし、次の画面を表示します。

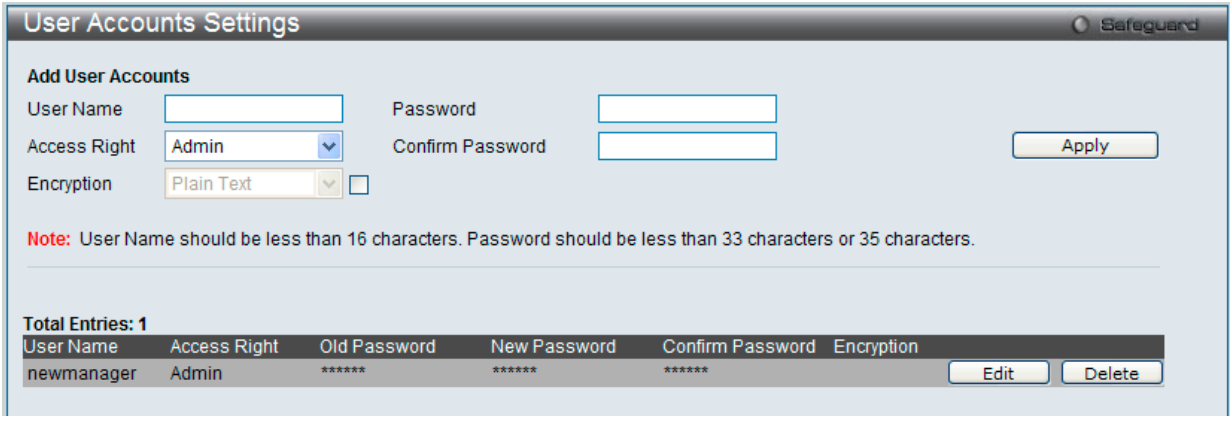


図 6-31　User Accounts Settings 画面

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）
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 15 文字以内）
Confirm Password	ユーザパスワードの確認入力をします。
Access Right	ユーザのアクセス権には、「Admin」（管理者）、「Operator」（オペレータ）、「Power_User」（管理ユーザ）および「User」（一般ユーザ）の 4 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。
Encryption	アカウントで使用する暗号化の方法を「Plain Text」「SHA-1」から選択します。

ユーザ追加の手順

1. ユーザの追加には「User Name」を設定します。
2. 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。
3. 「Access Right」でアクセス権限を設定します。
4. 「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。

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

表 6-1　Admin、Operator、Power_User、User 権限

管理	Admin	Operator	Power_User	User
コンフィグレーション設定	可	一部可	一部可	不可
ネットワークモニタリング	可	可	読み込みのみ	読み込みのみ
コミュニティ名とトラップステーション	可	読み込みのみ	読み込みのみ	読み込みのみ
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	可	可	不可	不可
システムユーティリティ	可	読み込みのみ	読み込みのみ	読み込みのみ
リセット（工場出荷状態へ）	可	不可	不可	不可
ユーザアカウント管理				
ユーザアカウントの登録、更新、変更	可	不可	不可	不可
ユーザアカウントの確認	可	不可	不可	不可

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。

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。

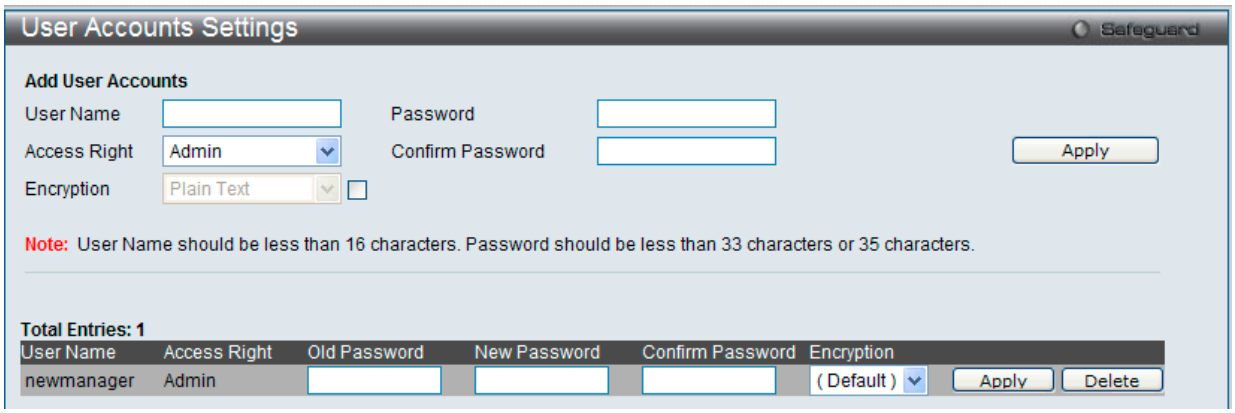


図 6-32　User Accounts Settings 画面 - 編集

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

注意　パスワードを忘れてしまった場合やパスワード不正の場合は、「【付録 B】 パスワードリカバリ手順」（385 ページ）を参照してください。本問題を解決する手順が記載されています。

注意　ユーザ名とパスワードは 16 文字未満である必要があります。

エントリの削除

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

Command Logging Settings（コマンドログ設定）

コマンドログの有効 / 無効の設定します。

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

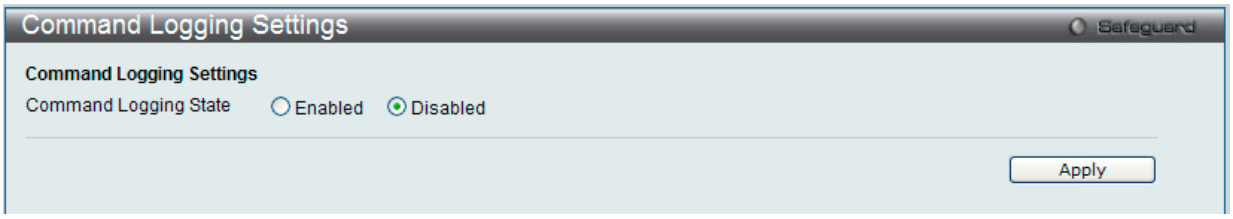


図 6-33　Command Logging Settings 画面

以下の項目を設定することができます。

項目	説明
Command Logging State	コマンドログの有効 / 無効の設定します。

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。

Configuration Trap Settings（コンフィグレーショントラップ設定）

コンフィグレーションの保存、アップロード / ダウンロード時のトラップ送信についての設定します。

System Configuration > Configuration 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。

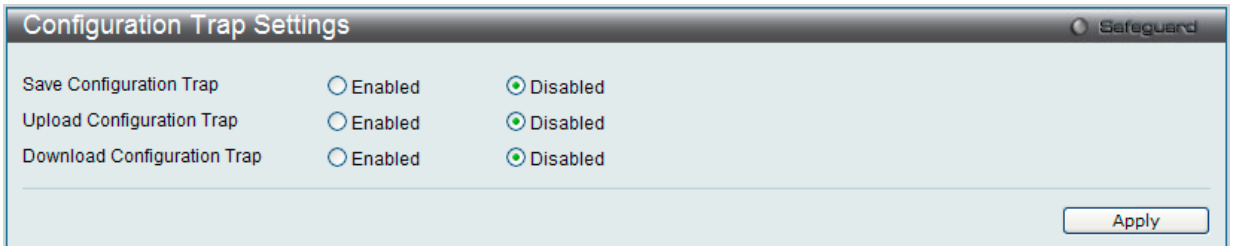


図 6-34　Configuration Trap Settings 画面

以下の項目を設定することができます。

項目	説明
Save Configuration Trap	コンフィグレーションが NVRAM に保存された時、SNMP によってトラップの送信の有無を設定します。
Upload configuration Trap	コンフィグレーションのアップロードが成功した時、SNMP によってトラップの送信の有無を設定します。
Download Configuration Trap	コンフィグレーションのダウンロードが成功した時、SNMP によってトラップの送信の有無を設定します。

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。

Stacking（スタック設定）

DGS-3120 シリーズは、ファームウェアリリース v1.00 からスイッチのスタックをサポートしています。これは、6 個のスイッチを 1 つに結合し、Telnet、GUI インタフェース（Web）、コンソールポートまたは SNMP 経由で 1 つの IP アドレスから管理することができます。本シリーズの各スイッチは、背面に 2 個のスタック用スロットを搭載しスタッキング可能なデバイスを接続することができます。スタックポートを追加した後、専用の同軸ケーブル（オプション）を使用して、スタックポート間を接続し、2 つのトポロジーのうちの 1 つを形成することができます。

- Duplex Chain - 下図のように、Duplex Chain トポロジはチェーン・リンク形式でスイッチをスタックします。この方法を使用すると、一方向のデータ転送だけが可能となります。そして、1 カ所中断が発生すると、データ転送は明らかに影響を受けます。
- Duplex Ring - 下図のように、Duplex Ring トポロジは、データが双方向に転送できるようにリング形式でスイッチをスタックします。このトポロジは、リングに 1 カ所中断が発生しても、データはスタック内の別のスイッチ間のスタックケーブル経由で転送されるため高い冗長性を確保します。

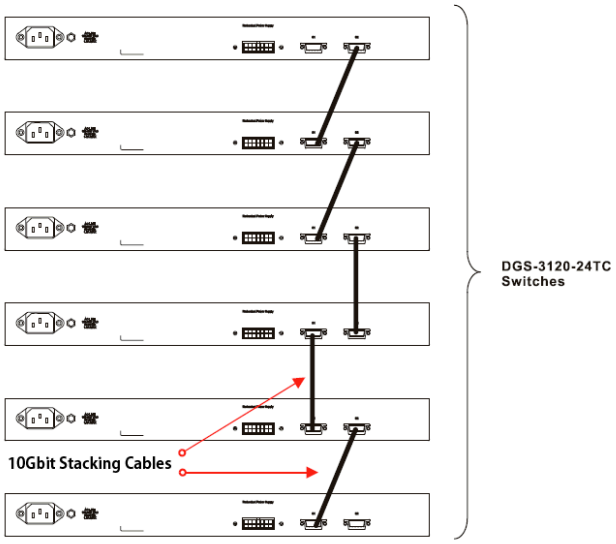


図 6-35　Duplex Chain でスタックされているスイッチ画面

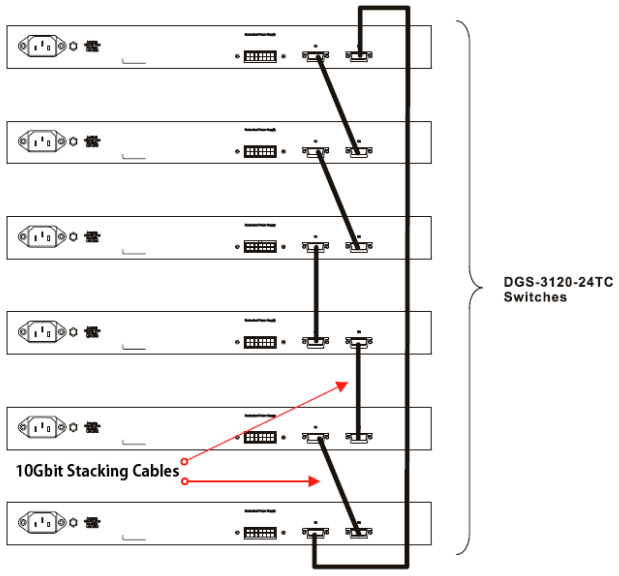


図 6-36　Duplex Ring でスタックされているスイッチ画面

各トポロジにおいて、各スイッチにスイッチスタックの役割を設定できます。また、スイッチスタック機能により自動的に決定することもできます。本スイッチシリーズのスタックには 3 つの役割があります。

- プライマリマスタ
  プライマリマスタはスタックの中心となるスイッチです。プライマリマスタは、通常のオペレーション、モニタ、スタックのトポロジー形成を維持します。このスイッチがスタックユニット ID のアサイン、設定同期、スイッチスタック内の残りのスイッチにコマンドを送信したりします。プライマリマスタはスタックを物理的に組む前にもっとも高いプライオリティ（小さい数字が高いプライオリティを意味する）を手動でスイッチにアサインするか、すべてのプライオリティ値が同じ場合には、自動選定プロセスにより最も小さい MAC アドレスのものが自動的に選定され、プライマリマスタとしてアサインされることにより決定されます。プライマリマスタはスイッチの前面パネルの一番右側の LED に、ボックス ID と "H" が交互に表示されます。

- バックアップマスタ
  バックアップマスタはプライマリマスタのバックアップであり、プライマリマスタが故障したり、スタックから外された場合に、プライマリマスタの機能を引き継ぎます。スタック内の隣接スイッチのステータスも監視しするとともに、プライマリマスタによりアサインされたコマンドを実行したり、プライマリマスタの動作状況を監視したりします。バックアップマスタはスタックを物理的に組む前に 2 番目に高いプライオリティを手動でスイッチにアサインするか、すべてのプライオリティ値が同じ場合には、自動選定プロセスにより 2 番目に小さい MAC アドレスのものが自動的に選定され、バックアップマスタとしてアサインされることにより決定されます。バックアップマスタはスイッチのフロントパネルの一番右側の LED に、ボックス ID と "h" が交互に表示されます。

- スレーブ
  スレーブスイッチは、プライマリもしくはバックアップマスタではない残りのスタックスイッチで構成されます。プライマリもしくはバックアップマスタが故障したりスタックから外された場合にその役割を引き継ぐことができます。スレーブスイッチはマスタにより要求されるオペレーションを実行したり、スタック内の隣接スイッチのステータスやスタックトポロジーを監視するとともに、バックアップマスタがプライマリマスタになるとすぐにバックアップマスタのコマンドに従います。スレーブスイッチはバックアップマスタがプライマリマスタになるかバックアップマスタが故障もしくはスタックから外された場合には自身がバックアップマスタになるかどうかを決定するためにセルフチェックを行います。プライマリ及びバックアップマスタの両方が故障した場合やスタックから外された場合には、自身がプライマリマスタになるかどうかを決定します。これらの役割は最初にプライオリティのものが担い、プライオリティが同じ場合には、最も小さい MAC アドレスのものが担います。

スイッチはユーザにより設計されたトポロジーで組み立てられ、起動するとすぐに、スタックは機能する状態になるまでに以下の 3 つのプロセスを経由します。

- 初期化状態 - これは、スタックの最初の状態で、ランタイムコードが設定および初期化され、システムは各スイッチが適切に機能していることを検証するために周辺機器の診断を行います。
- マスタ選定状態 - コードがロードされ、初期化されると、スタックはマスタ選定状態になり、使用されるトポロジのタイプを検出し、プライマリマスタ、バックアップマスタの順に選定します。
- 同期状態 - プライマリマスタとバックアップマスタが確立すると、プライマリマスタがスタック内のすべてのスイッチにスタックユニット番号を割り当て、すべてのスイッチに設定情報を同期します。プライマリマスタのユーザ設定に基づいて残りのスイッチにコマンドを送信します。

これらの手順が終了すると、スイッチスタックは正常な操作モードに入ります。

スタックスイッチ交換

スイッチのスタック機能はスタック動作状態のままスイッチを挿抜する " ホットスワップ " をサポートしています。いくつかの簡単な条件により、電源オフやスタック内のスイッチ間のデータ転送に大きな影響を与えずに、スタックからのスイッチの取り外しやスタックへの追加を行うことができます。

スイッチが動作中のスタックにホットインサートされる場合、設定された優先度や MAC アドレスなど新たに追加されたスイッチの設定によっては、新しいスイッチがバックアップマスタまたはスレーブとなる可能性があります。しかし、共に以前の選定プロセスを経て、その結果、プライマリマスタとバックアップマスタを持った 2 つのスタックが追加されると、新しいプライマリマスタが、優先度または MAC アドレスに基づいて、既存のプライマリマスタから選定されます。このプライマリマスタは、ホットインサートされた新しいスイッチすべてに対してのプライリマスタの役割のすべてを引き継ぎます。このプロセスは、検出処理が完了するまで 1.5 秒ごとにスイッチスタックを通して循環するディスカバリパケットを使用して行われます。

" ホットリムーブ " 動作はスタック動作状態のままスタックからスイッチを外すことを意味します。ホットリムーブはデバイスから特定の時間ハートビートパケットを受け取れなかった場合もしくは、スタッキングポートの一つがリンクダウンした場合に検出されます。デバイスが外されるとすぐに残りのスイッチは変更を反映するためにスタッキングトポロジーデータベースをアップデートします。プライマリマスタ、バックアップマスタ、スレーブの 3 つの役割のどれかひとつがスタックから外されますがどの役割かにより、以下のような異なるプロセスが発生します。

スレーブデバイスが取り外される場合、プライマリマスタは unit leave メッセージの使用を通じ、このデバイスのホットリムーブを他のスイッチに通知します。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。

バックアップマスタがホットリムーブされると、新しくバックアップマスタが前述の選定プロセスを経由して選ばれます。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。その後、データベース同期がスタックによって完了した際に、バックアップマスタはプライマリマスタのバックアップを開始します。

プライマリマスタが取り外されると、バックアップマスタはプライマリマスタの役割を引き受けて、新しいバックアップマスタが選定プロセスを経て選ばれます。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。新しいプライマリマスタは、スタックとネットワーク内の矛盾を避けるために、前のプライマスタの MAC と IP アドレスを引き継ぎます。

プライマリマスタとバックアップマスタの両方が取り外される場合、選定プロセスがすぐに実行され、新しいプライマリマスタとバックアップマスタを決定します。スタック内のスイッチは , 取り外されたユニットの設定をクリアし、ARP などのダイナミックに学習されたデータベースも同様にクリアされます。スタティック設定については、スタック内の残りのスイッチのデータベース内にまだ維持されこれらの機能に影響はありません。

注意 スタックがディスカバリフェーズにおいて、BOX ID が重複している場合には、そのデバイスは特別なスタンドアロントポロジモードに入ります。ユーザはデバイス情報の取得、Box ID の設定、保存、および再起動だけ行うことができます。すべてのスタックポートが無効とされ、エラーメッセージがスタック内の各デバイスのローカルコンソールポートに生成されます。ユーザは、Box ID を再設定し、スタックを再起動する必要があります。

注意 R3.00.xx において、B1 と Ax の HW バージョンの混在した環境で物理スタックをご利用した場合、ファームウェアアップグレードする際には、スタック状態のままマスタと異なる HW バージョンのデバイスをファームウェアアップグレードすることはできませんのでご注意ください。

Stacking Device Table（スタックデバイステーブル）

スイッチスタック中のデバイスを表示します。

System Configuration > Stacking > Stacking Device 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。

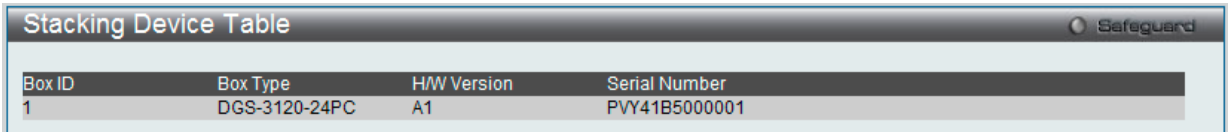


図 6-37　Stacking Device Table 画面

Stacking Mode Settings（スタックモード設定）

デバイスのスタック機能を有効にして、優先順位を設定します。

System Configuration > Stacking > Stacking Mode 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 6-38　Stacking Mode Settings 画面

以下の項目が表示されます。

項目	説明
Stacking Mode	「Enabled」/「Disabled」を選択し、機能の有効 / 無効を設定します。 • Enabled - 10G ポートはスタッキングポートとして機能します。 • Disabled - 10G ポートは通常の 10Gb ポートに戻ります。
Force Master Role	ラジオボタンから有効 / 無効を選択します。現在のスタッキングトポロジに新しいデバイスを追加する時、マスタの設定が変更されない様に設定します。有効にした場合、スタッキングが構築された後、マスタの優先値は 0（最上値）に設定されます。
Stacking Trap State	ラジオボタンを使用してスタッキングのトラップ送信の有効 / 無効を選択します。
Stacking Log State	ラジオボタンを使用してスタッキングのトラップログの有効 / 無効を選択します。
Current Box ID	プルダウンメニューを使い、設定するスイッチの現在のボックス番号（1-6）を選択します。
New Box ID	プルダウンメニューを使い、「Current Box ID」欄で選択したスタックに対して新しくボックス番号（1-6）を指定します。「Auto」は、スイッチスタック内のスイッチに自動的にボックス番号を割り当てます。
Priority (1-63)	スイッチの優先度番号を表示します。数字が低いほど、優先度は高くなります。スタック内で最も低い優先度番号を持つボックス（スイッチ）が、プライマリマスタです。プライマリマスタスイッチは、スイッチスタックにおけるアプリケーションを設定するために使用されます。1-63 の範囲で設定できます。

「Apply」ボタンをクリックし、設定項目を有効にします。

注意　EI モード機器と SI モード機器の組み合わせによるスタックはできません。

注意　スタックを構成するスイッチのファームウェアバージョンは同じである必要があります。

第 7 章　Management（スイッチの管理）

本章でスイッチの管理を行います。

以下は、Management サブメニューです。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）	68
Gratuitous ARP（Gratuitous ARP 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）	70
IPv6 Neighbor Settings （IPv6 ネイバ設定）	IPv6 ネイバの設定を行います。	71
IP Interface（IP インタフェース）	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）	72
Management Settings（管理設定）	CLI ページング、DHCP 自動設定などの管理設定を行います。	76
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。	77
Single IP Management （シングル IP マネジメント設定）	シングル IP マネジメント機能を設定します。次のメニューがあります。 Single IP Settings（シングル IP 設定）、Firmware Upgrade（ファームウェア更新）、Configuration File Backup/ Restore（コンフィグレーションファイルの更新）、Upload Log File（ログファイルのアップロード）	
SNMP Settings（SNMP 設定）	SNMP 設定を行います。次のメニューがあります。 SNMP Global Settings（SNMP グローバル設定）、SNMP Trap Settings（SNMP トラップ設定）、SNMP Link Change Traps Settings（SNMP リンクチェンジトラップ設定）、SNMP View Table Settings（SNMP ビューテーブル）、SNMP Community Table Settings（SNMP コミュニティテーブル設定）、SNMP Group Table Settings（SNMP グループテーブル設定）、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）、SNMP Community Encryption Settings（SNMP コミュニティ暗号化設定）、SNMP Community Masking Settings（SNMP コミュニティマスク設定）	88
Telnet Settings（Telnet 設定）	スイッチに Telnet 設定をします。	96
Web Settings（Web 設定）	スイッチに Web ステータスを設定します。	96
Power Saving Settings（省電力設定）	リンクダウン状態のポートの電源をオフにしてスイッチへの電力を節約します。次のメニューがあります。 LED State Settings（LED 設定）、Power Saving Settings（省電力設定）、Power Saving LED Settings（LED 省電力設定）、Power Saving Port Settings（ポート省電力設定）	96
SD Card Management（SD カード管理）	SD カードを使用して、ログやコンフィグレーションの保存を行います。次のメニューがあります。 SD Card Backup Settings（SD カードへのバックアップ設定）、SD Card Execute Settings（SD カード実行設定）	98

ARP（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し、IP アドレスと MAC アドレスを対応させます。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。

Static ARP Settings（スタティック ARP 設定）

ARP（Address Resolution Protocol：アドレス解決プロトコル）は、IP アドレスを物理アドレスに変換する TCP/IP プロトコルです。本テーブルを使用して、特定したデバイスの ARP 情報の確認や定義、変更および削除を行います。
スタティックエントリも ARP テーブル中に定義できます。スタティックエントリを定義すると、パーマネントエントリも登録でき、IP アドレスから MAC アドレスの変換に使用することができます。

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

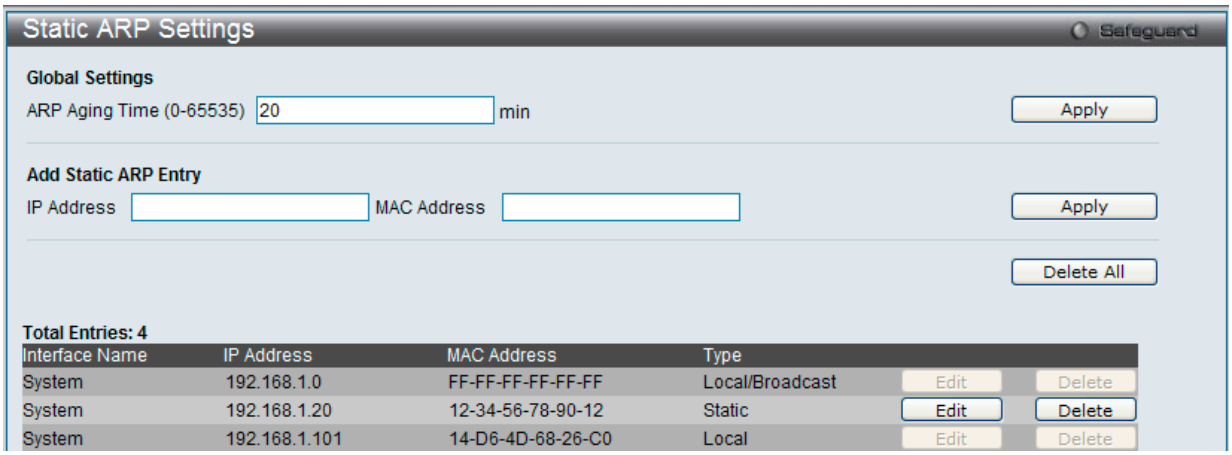


図 7-1　Static ARP Settings 画面

「Static ARP Settings」画面には次の項目があります。

項目	説明
ARP Aging Time (0-65535)	ARP テーブルエントリのリクエストから、エントリを保持する時間（分）設定します。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。設定値は、0-65535（分）の範囲で設定できます。初期値は 20 分です。
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。

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

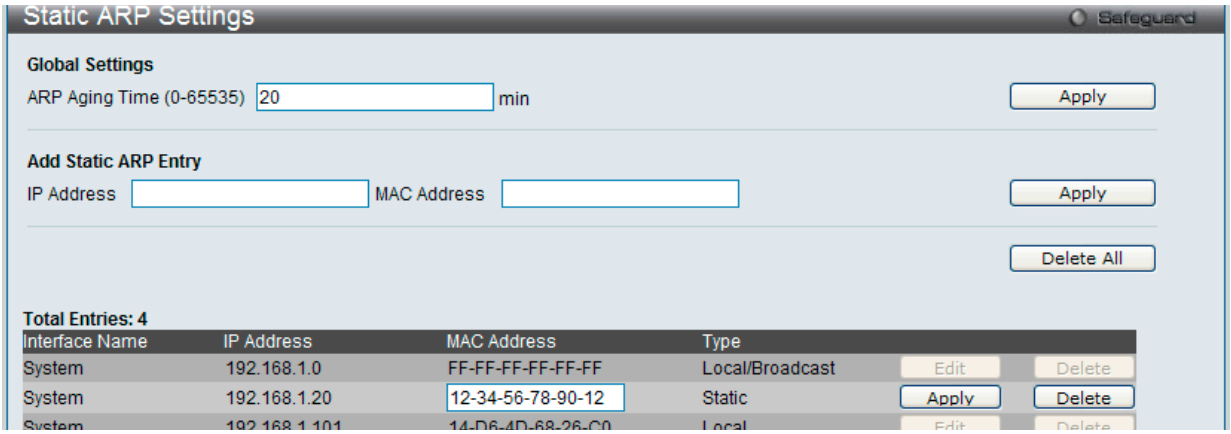


図 7-2　Static ARP Settings 画面

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）（EI モードのみ）

プロキシ ARP 機能は、別の機器に対し IP/MAC アドレスを見せかけて送信される ARP リクエストに対して、スイッチが本来の ARP 回答元として返答します。従って、スタティックのルーティングやデフォルトゲートウェイを設定せずに、目的の宛先にパケットをルートすることが可能です。ホスト（通常レイヤ 3 スイッチ）は別の機器に送信された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属している場合、B は A からの ARP ブロードキャストリクエストを受信も応答もしません。しかし、A の物理ネットワークがルータまたはレイヤ 3 スイッチを介して B に接続されると、ルータまたはレイヤ 3 スイッチは A からの ARP リクエストを参照することが可能です。ローカルプロキシ ARP 機能は送信元 IP アドレスと宛先 IP アドレスが同じ場合、スイッチがプロキシ ARP に応答することを許可します。

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

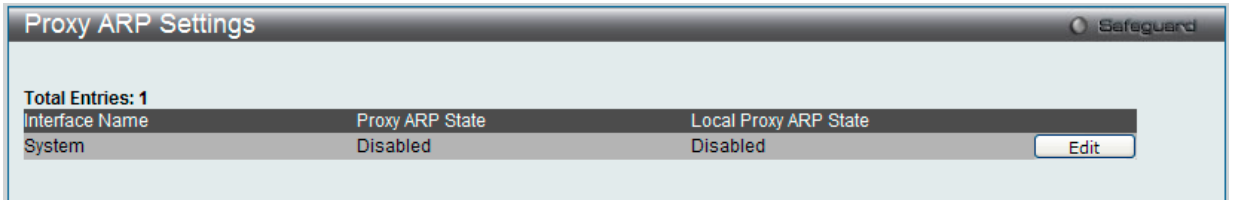


図 7-3　Proxy ARP Settings 画面

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。

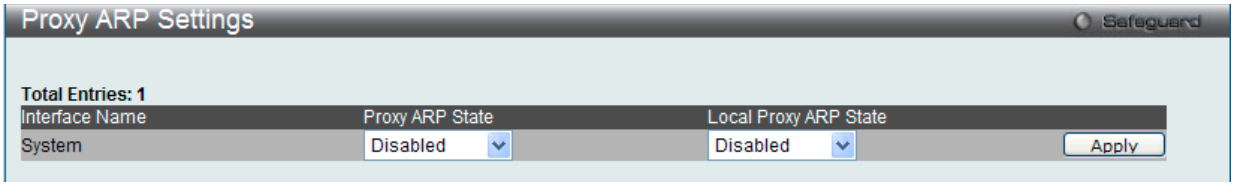


図 7-4　Static ARP Settings 画面

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」「Local Proxy ARP State」の両方とも無効になります。

ARP Table（ARP テーブル）

現在のスイッチの ARP エントリを表示します。

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

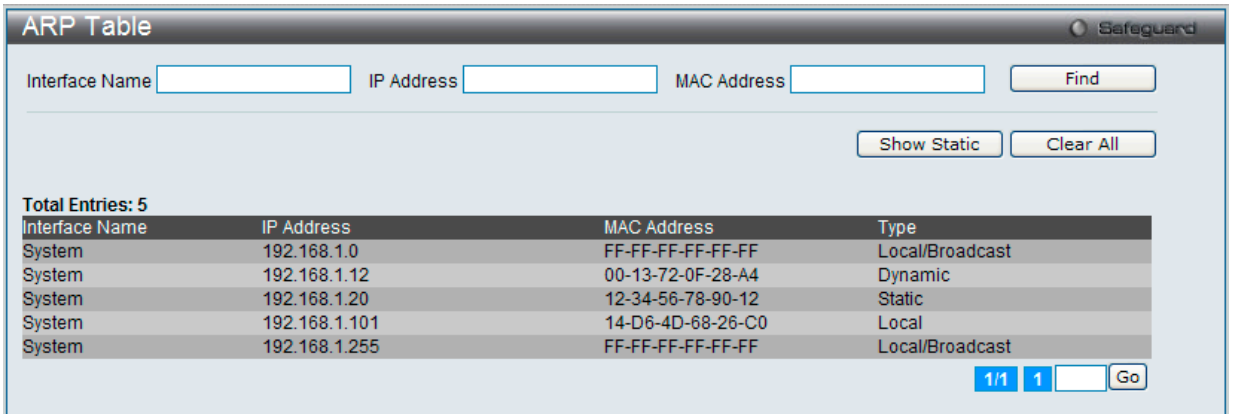


図 7-5　ARP Table 画面

「Static ARP Settings」画面には次の項目があります。

項目	説明
Interface Name	ARP テーブルエントリのリクエストから、エントリを保持する時間（分）設定します。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。設定値は、0-65535（分）の範囲で設定できます。初期値は 20 分です。
IP Address	使用している IP アドレスを入力 / 表示します。
MAC Address	使用している MAC アドレスを入力 / 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指定のエントリを検索します。「Show Static」ボタンをクリックしてスタティックエントリのみを表示します。「Clear All」ボタンをクリックするとテーブル上のエントリが全て消去されます。

Gratuitous ARP Settings（Gratuitous ARP 設定）

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

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。

Management > Gratuitous ARP > Gratuitous ARP 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。

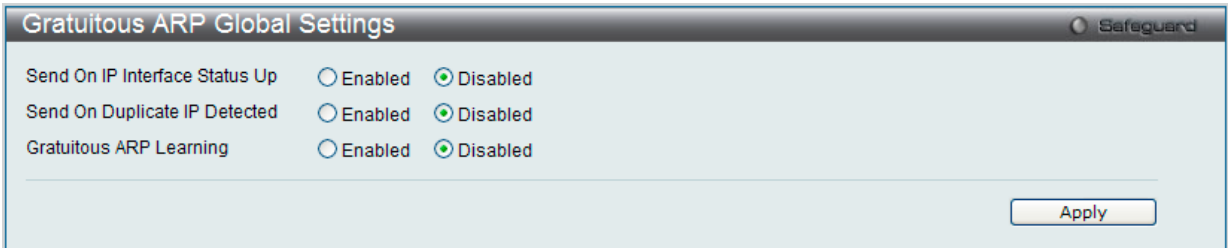


図 7-6　Gratuitous ARP Global Settings 画面

設定には以下の項目を使用します。

項目	説明
Send on IP Interface status up	IPIF インタフェースがアップ中に、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、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。初期値ではステータスは無効です。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。
Gratuitous ARP Learning	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。スイッチが ARP テーブルに Gratuitous ARP パケットと送信元の IP アドレスを受信すると、ARP エントリを更新する必要があります。初期値は「Disabled」です。

Gratuitous ARP Global 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。

Gratuitous ARP Settings（Gratuitous ARP 設定）

Gratuitous ARP についてより詳しい設定を行います。

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。

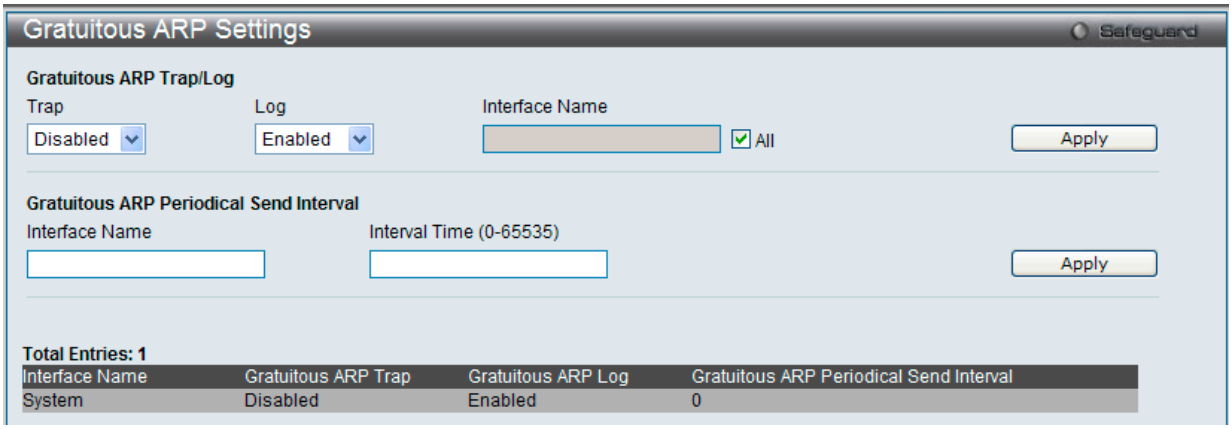


図 7-7　Gratuitous ARP Settings 画面

画面には以下の項目が表示されます。

項目	説明
Gratuitous ARP Trap/Log	
Trap	管理者に通知するためにトラップ（追跡）します。初期値では無効です。
Log	管理者に通知するために IP コンフリクトイベントのログを取得します。初期値ではイベントログは無効です。
IP Interface Name	編集中の IP インタフェース名が表示されます。
Gratuitous ARP 定期送信間隔	
IP Interface Name	編集中の IP インタフェース名が表示されます。
Interval Time (0-65535)	Gratuitous ARP リクエストパケットの定期な送信間隔を設定します。初期値は 0（秒）です。

「Apply」ボタンをクリックし、設定を有効にします。

IPv6 Neighbor Settings（IPv6 Neighbor 設定）

IPv6 Neighbor は、IPv6 デバイスして検出された Link-Local ネットワーク上のデバイスです。これらのデバイスは、パケットを転送し、ネットワーク上のノードの Link-Layer アドレスに変更が発生しているか、または同一のユニキャストアドレスがローカルリンク上に存在するかなどルータの到達性を絶えずモニタしています。以下の 2 つの画面では、IPv6 Neighbor の追加と参照、または Neighbor キャッシュからの削除を行います。

Management > IPv6 Neighbor 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。

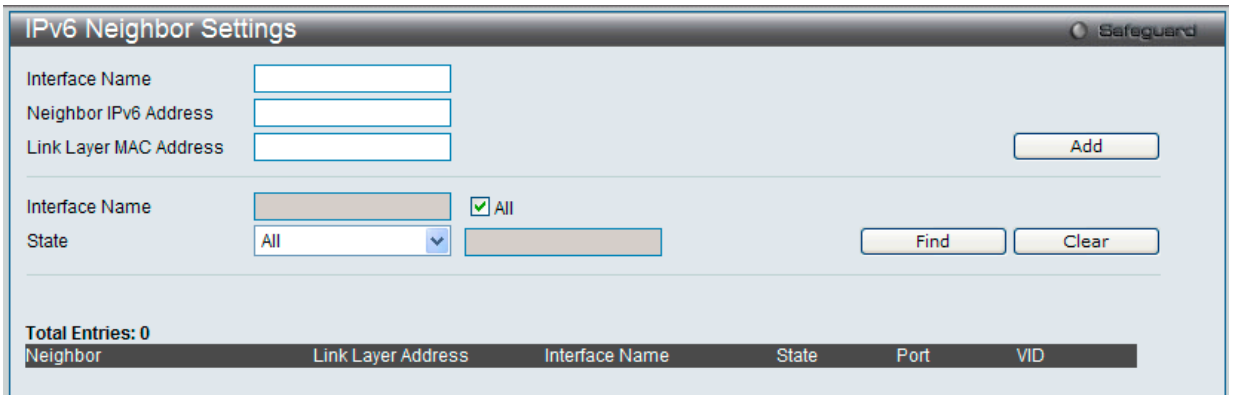


図 7-8　IPv6 Neighbor Settings 画面

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。

「IPv6 Neighbor Settings」画面には次の項目があります。

項目	説明
Interface Name	IPv6 Neighbor の IP インタフェース名を指定します
Neighbor IPv6 Address	IPv6 Neighbor の IPv6 アドレスを入力します
Link Layer MAC Address	対応する IPv6 デバイスの MAC アドレスを指定します。
Interface Name	IPv6 Neighbor を検索するデバイスの IP インタフェース名を指定します。スイッチ上の全てのインタフェースを検索する場合は「All」にチェックを入れます。
State	プルダウンメニューから「All」「Address」「Static」「Dynamic」を選択します。「Address」を選択した場合、IP アドレスを入力する項目に入力ができるようになります。

IP Interface（IP インタフェース）

IP インタフェースの設定を行う場合は **Management > IP Interface** から設定を行います。

System IP Address Settings（システム IP アドレス設定）

IP アドレスはイーサネット経由での接続の前にコンソールを利用して設定されている場合があります。管理者はスイッチの IP アドレス設定を表示します。工場出荷値は IP アドレス：「10.90.90.90」、サブネット：「255.0.0.0」、デフォルトゲートウェイ：「0.0.0.0」です。

Management > IP Interface > System IP Address Settings メニューをクリックします。以下のようにスイッチの現在の IP 設定が表示されます。

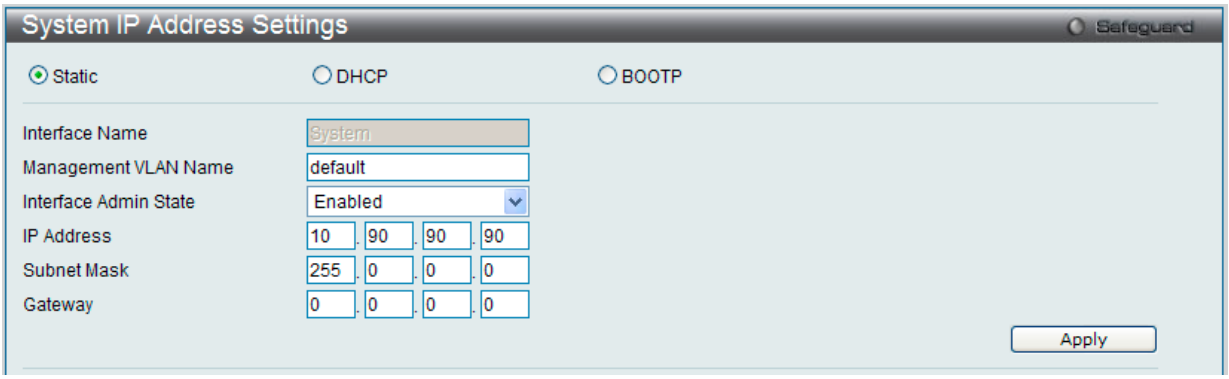


図 7-9　System IP Address Settings 画面

まず IP アドレス設定方法について以下の項目から選択します。項目は以下の通りです。

項目	説明
Static	本スイッチの IP 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 プロトコルにより 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は DHCP サーバにより割り当てられます。本オプションが選択されると、スイッチはデフォルトの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 プロトコルにより 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は BOOTP サーバにより割り当てられます。本オプションが選択されると、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。

次にシステムインタフェースの詳細について設定します。IP アドレス設定用の項目およびオプション項目は以下の通りです。

項目	説明
Interface Name	システムインタフェースの名前を表示します。
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「Trusted Host」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デフォルト VLAN に所属しています。初期設定では、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	プルダウンメニューを使用してインタフェースの有効 / 無効を選択します。無効の場合 IP インタフェースにはアクセスできません。
IP Address	本 IP インタフェースに設定する IPv4 アドレスを入力します。
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。

注意　工場出荷時は、IP アドレスに 10.90.90.90、サブネットマスクに 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。

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。

Interfaces Settings（インタフェース設定）

スイッチの IP インタフェース状況を表示します。

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

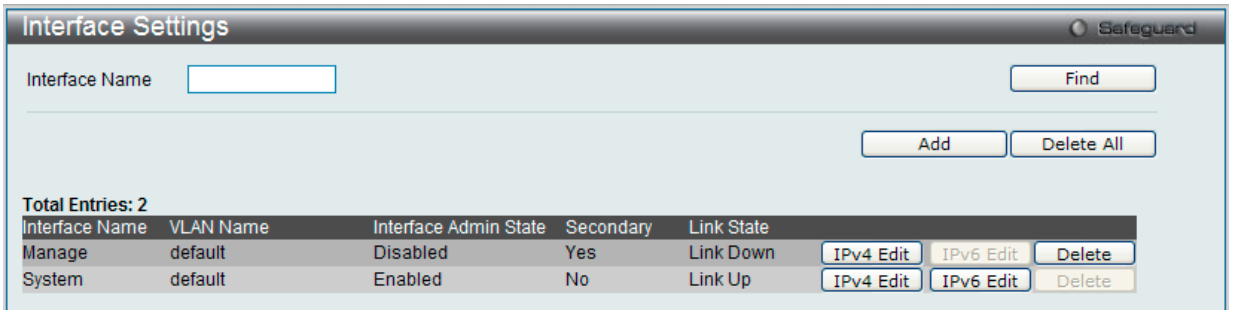


図 7-10　Interface Settings 画面

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 インタフェースを作成するには IPv4 インタフェースを作成し、IPv6 インタフェースに変更します。

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 - Add 画面

2. 追加する IPv4 インタフェースについて設定します。

項目	説明
Interface Name	IP インタフェース名を入力します。
IPv4 Address	本 IP インタフェースに設定する IPv4 アドレスを入力します。
Subnet Mask	サブネットを指定します。
VLAN Name	VLAN 名を入力します。
Interface Admin State	プルダウンメニューを使用してインタフェースの有効 / 無効を選択します。
Secondary Interface	チェックボックスにチェックを入れると指定のインタフェースをセカンダリインタフェースとして設定します。プライマリ IP が有効でない場合、VLAN はセカンダリインタフェースに移行します。プライマリ IP が復帰すると元に戻ります。

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。
入力 / 指定した変更を破棄し前のページに戻る場合は「<<Back」をクリックします。

IPv4 インタフェースの編集

1. 「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。

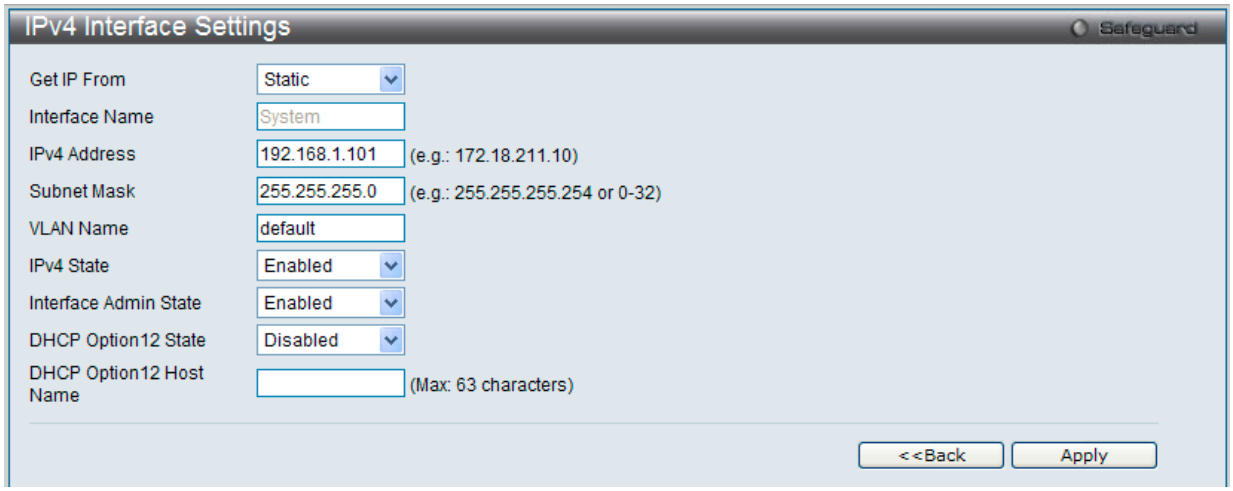


図 7-12　IPv4 Interface Settings - Edit 画面

2. 以下の項目を使用して設定を行います。

項目	説明
Get IP From	IPv4 アドレス、サブネットマスク、デフォルトゲートウェイに設定する「Static」「BOOTP」「DHCP」プロトコルを選択します。
Interface Name	IPv4 インタフェースの名前が表示されます。
IPv4 Address	IPv4 インタフェースに割り当てる IPv4 アドレスを入力します。
Subnet Mask	IPv4 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。
VLAN Name	IPv4 インタフェースが属する VLAN の名前を入力します。
IPv4 State	プルダウンメニューを使って IPv4 ステートの有効 / 無効を指定します。
Interface Admin State	プルダウンメニューを使用して、管理者ステートを「Enabled」（有効）または「Disabled」（無効）とします。
DHCP Option 12 State	プルダウンメニューを使用して「DHCPDISCOVER」「DHCPREQUEST」メッセージ内への Option12 の挿入を有効 / 無効を設定します。
DHCP Option 12 Host Name	「DHCPDISCOVER」「DHCPREQUEST」メッセージ内へ挿入するホスト名を入力します。

「Apply」ボタンをクリックし、設定を有効にします。入力 / 指定した変更を破棄し前のページに戻る場合は「<<Back」をクリックします。

IPv6 インタフェースの編集

1. 「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。

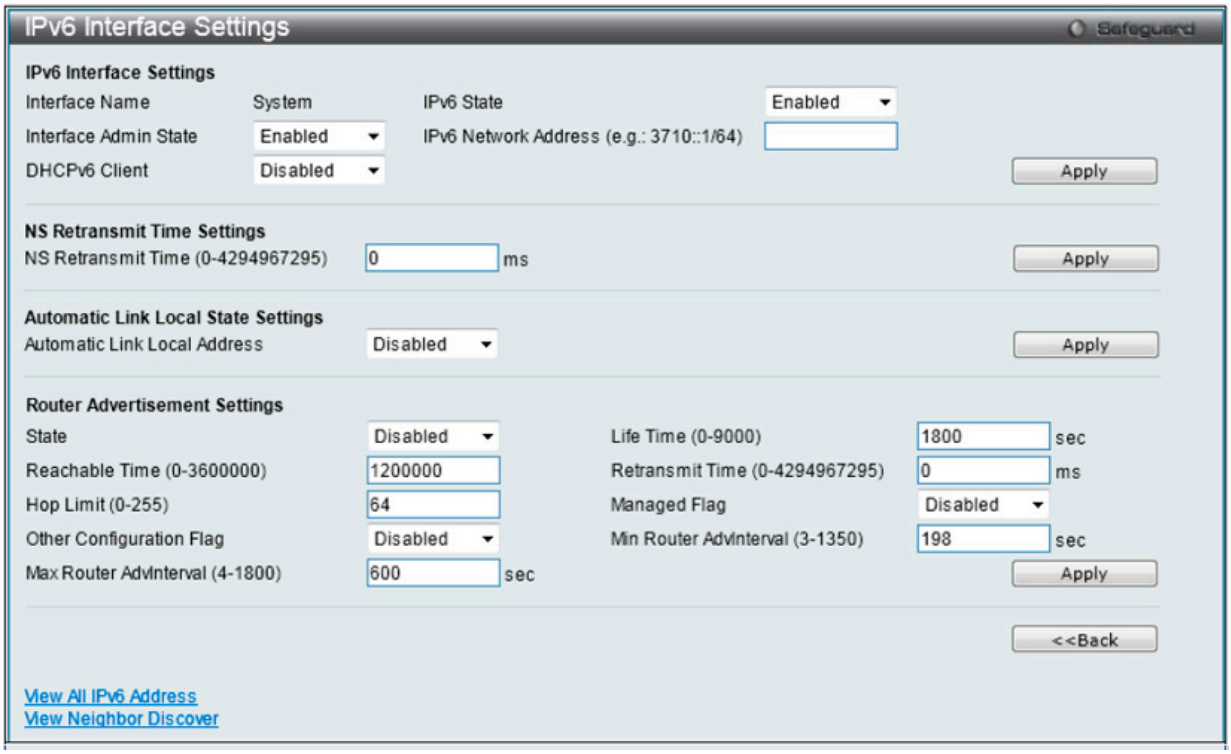


図 7-13　IPv6 Interface Settings - Edit 画面

2. 以下の項目を使用して設定を行います。

項目	説明
Interface Name	IPv6 インタフェースの名前が表示されます。
IPv6 State	プルダウンメニューを使って IPv6 ステートの有効 / 無効を指定します。
Interface Admin State	プルダウンメニューを使用して、管理者ステートを「Enabled」（有効）または「Disabled」（無効）とします。
IPv6 Network Address	ネイバのグローバル / ローカルリンクアドレスを入力できます。
DHCPv6 Client	プルダウンメニューを使用して、DHCPv6 クライアントの有効 / 無効を指定します。
NS Retransmit Time	ローカルネットワークに送信する Neighbor Solicitation パケットを生成する間隔（秒）を設定します。これは、ローカルリンク上の IPv6 近接を検出するために使用されます。0-65535（ミリ秒）の範囲から指定します。
Automatic Link Local Address	本機能を有効 / 無効にします。有効にすると、IPv6 Link-Local アドレスを自動的に作成します。本機能を有効にして「Apply」ボタンをクリックすると、IPv6 アドレスはスイッチの MAC アドレスに基づいて生成され、新規エントリが以下の「Link-Local Address」フィールドに表示されます。
Router Advertisement Settings	
State	ルータの通知状態を有効または無効にします。
Life Time (0-9000)	デフォルトルータとしてのルータの寿命（秒）を 0-9000（秒）で指定します。
Reachable Time (0-3600000)	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までの時間（ミリ秒）を指定します。
Retransmit Time (0-4294967295)	ルータ通知メッセージの再送の間隔（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 (0-255)	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	• Enabled - 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、アドレス取得の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。 • Disabled - アドレス取得のためにステートフルアドレス設定を使用した RA の受信を停止します。
Other Configuration Flag	• Enabled - 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、アドレス取得の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。 • Disabled - アドレス取得のためにステートフルアドレス設定を使用した RA の受信を停止します。
Min Router AdvInterval (3-1350)	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）を入力します。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 : 0.33 * MaxRtrAdvInterval
Max Router AdvInterval (4-1800)	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）を入力します。4-1800（秒）で指定します。初期値は 600（秒）です。

「Apply」ボタンをクリックし、設定を有効にします。入力 / 指定した変更を破棄し前のページに戻る場合は「<<Back」をクリックします。
現在の IPv6 アドレスを全て確認する場合「View All IPv6 Address」をクリックします。
「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 インタフェースの編集

「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。

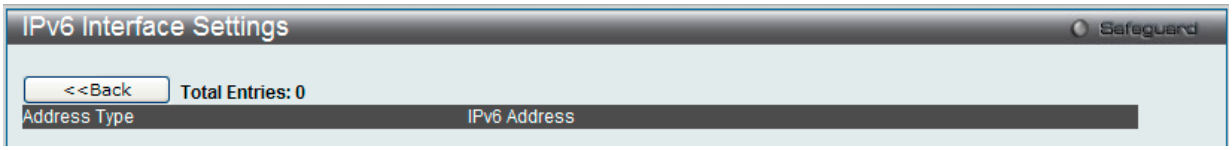


図 7-14　IPv6 Interface Settings -「View All IPv6 Address」画面

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。

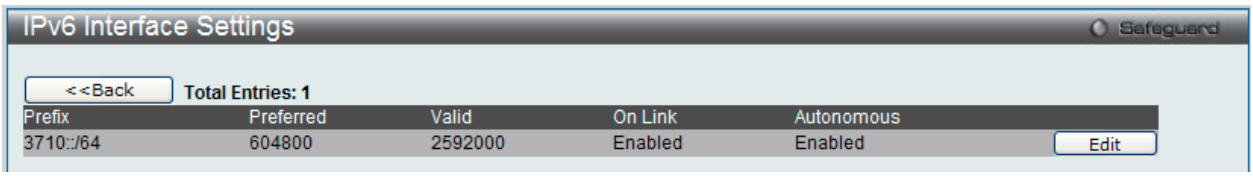


図 7-15　IPv6 Interface Settings 画面

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。

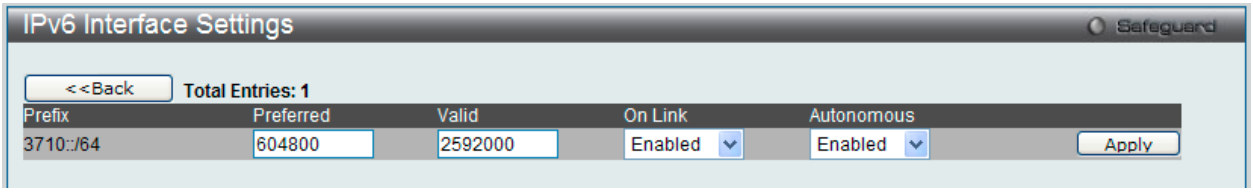


図 7-16　IPv6 Interface Settings 画面 - Edit

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。

Management Settings（管理設定）

コマンドラインインタフェースを使用時にコンソールの制限を超えて複数のページのスクロールを止めることが可能です。

本画面はまた本スイッチの DHCP 自動設定機能を有効にします。「Enabled」の時、本スイッチは TFTP サーバから設定ファイルを受信します。そしてブートアップ時に自動的に 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 サーバはリクエストを受け取ると起動し、動作する必要があります。また、そのベースディレクトリに格納されている必要な設定を保持する必要があります。クライアントが使用するための設定ファイルに関する詳しい情報は DHCP サーバまたは TFTP サーバソフトウェアの手順を参照してください。「Tools」の「Upload Log File」セクションの説明を参照してください。
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の以前に保存した設定が使用されます。

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

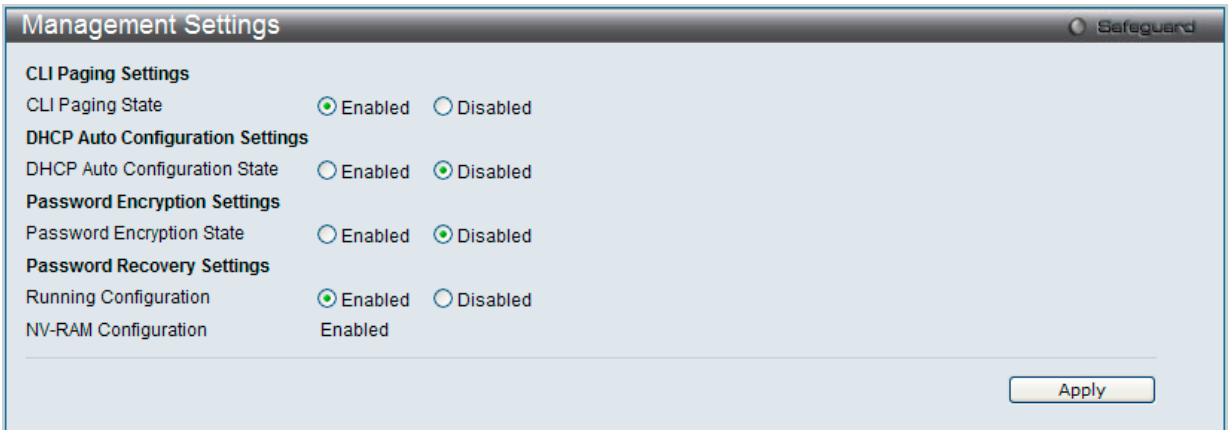


図 7-17　Management Settings 画面

以下のフィールドを使用して設定を行います。

項目	説明
CLI Paging State	コマンドラインインタフェースの改頁処理をコンソール画面の最後で停止します。コンソール画面の範囲を超えてテキストが複数ページにスクロールしないようにします。初期値は「Enabled」（有効）です。無効にする場合は、「Disabled」を選択します。
DHCP Auto Configuration State	DHCP 自動設定機能を有効 / 無効にします。有効の場合、スイッチは設定ファイルを TFTP サーバから受信し再起動時に自動的に DHCP クライアントに設定されます。本機能を実装するには DHCP サーバは IP アドレスとコンフィグレーションファイル、名称情報などを DHCP リレーパケット内で TFTP サーバに送信します。TFTP サーバはスイッチからのリクエスト受信時にベースディレクトリに必要なコンフィグレーションファイルを保持、起動、実行している必要があります。
Password Encryption State	コンフィグレーションファイルのパスワードを暗号化します。パスワード暗号化機能は初期値では無効です。有効にするには「Enabled」をクリックします。
Running Configuration	「Password Recovery」オプションとして「Running Configuration」の有効 / 無効を設定します。有効にすると実行中の設定のリカバリが可能になります。

「Apply」ボタンをクリックし、設定を有効にします。

Session Table（セッションテーブル）

現在のセッションテーブルを表示します。

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

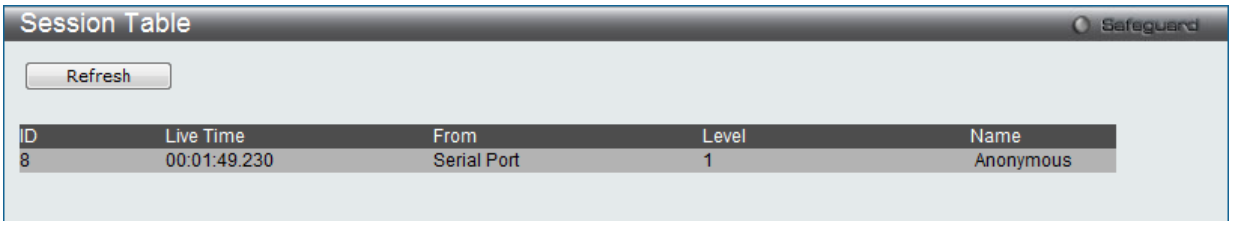


図 7-18　Session Table 画面

「Refresh」ボタンをクリックし表示を最新の状態にします。

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、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。

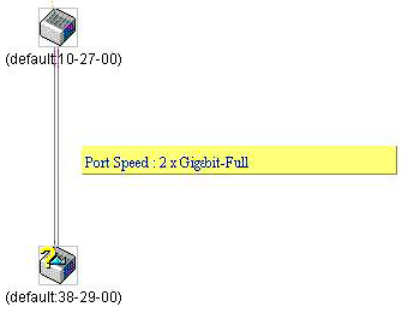
バージョン 1.61 へのアップグレード

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。トポロジマップには、ポートトランクグループのメンバとなる接続に関する新機能が加わりました。これは、以下の図に示すように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 MS 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。

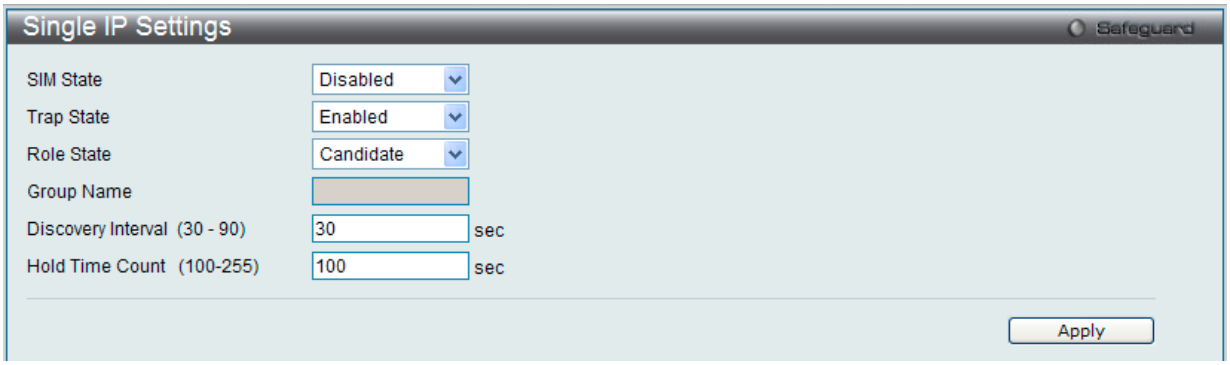


図 7-19　Single IP Settings 画面（CaS 無効状態）

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。

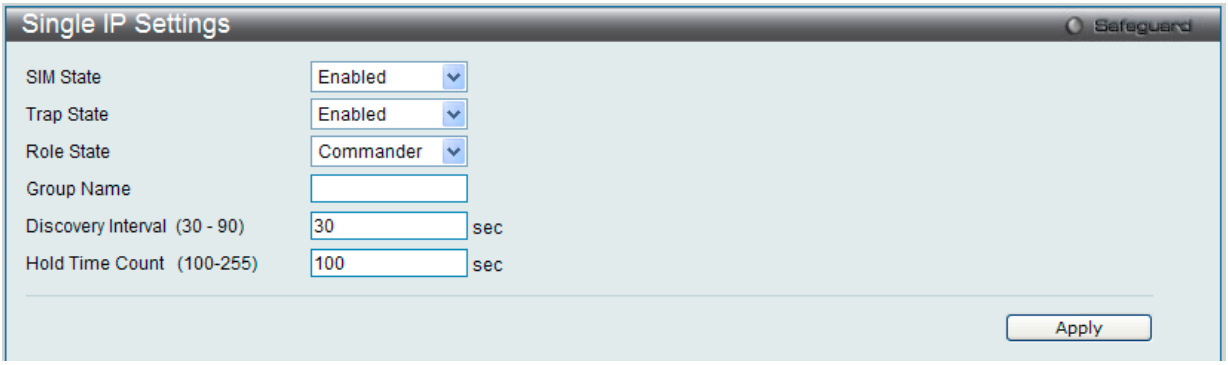


図 7-20　Single IP Settings 画面（CS 有効状態）

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。
Trap State	プルダウンメニューからトラップ送信の有効 / 無効を指定します。
Role State	プルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。 • Candidate - Candidate Switch（CaS）は SIM グループメンバではありませんが、Commander スイッチに接続しています。本スイッチの SIM 機能の初期設定です。 • Commander - Commander Switch（CS）。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオプションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。
Group Name	SIM グループ名を入力します。
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）

「Topology」画面は、SIM グループ内のスイッチの設定および管理に使用されます。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「Topology」画面が表示されます。

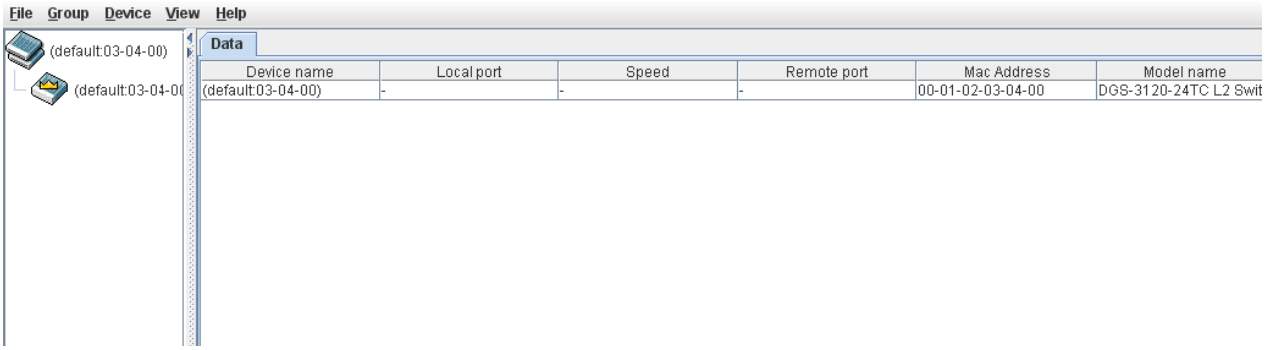


図 7-21　トポロジ画面

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。

トポロジマップを表示するためには、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。

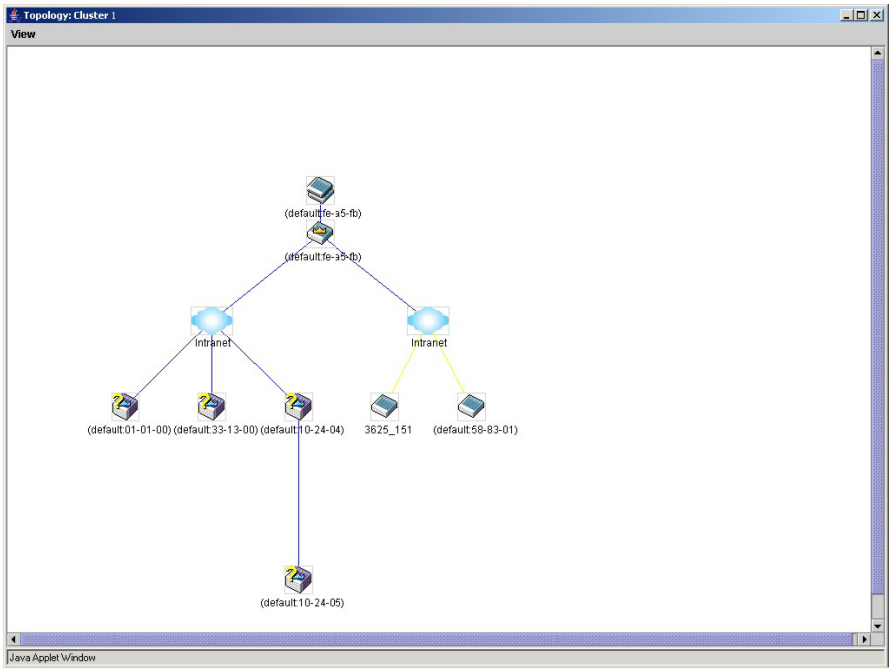


図 7-22　Topology 画面

Management（スイッチの管理）

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。

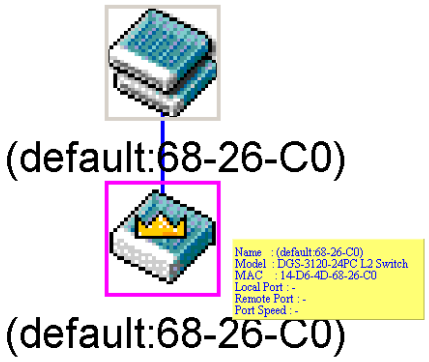


図 7-23　ツールヒントを利用したデバイス情報の表示

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。

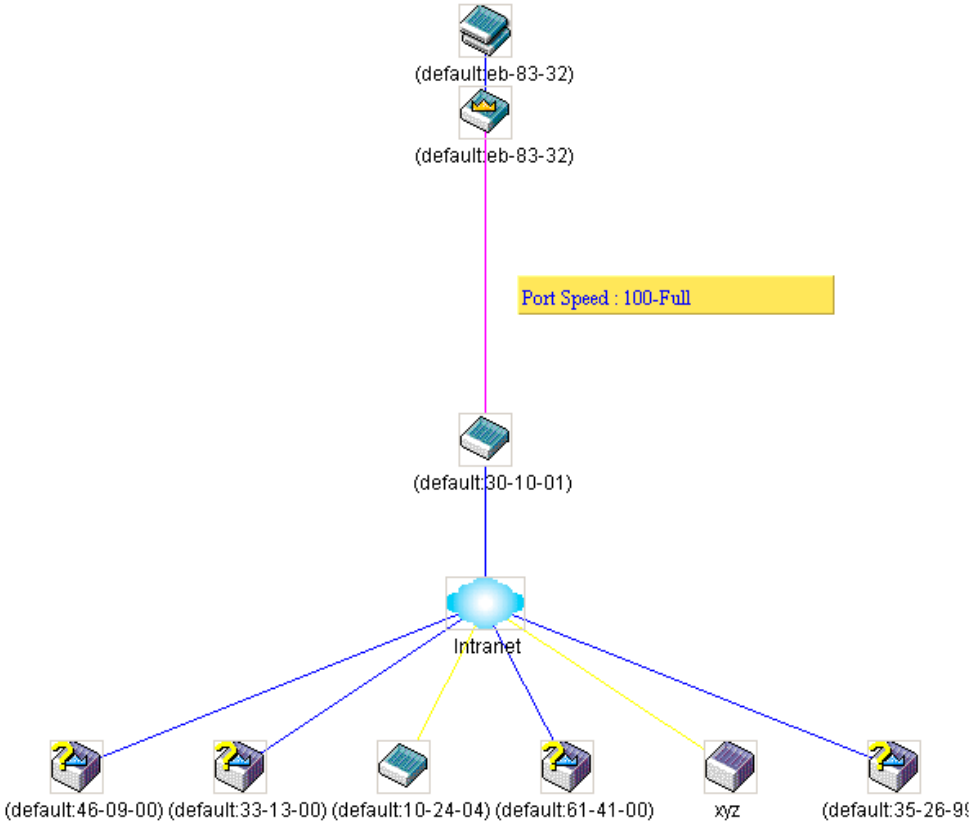


図 7-24　ツールヒントを利用したポート速度の表示

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

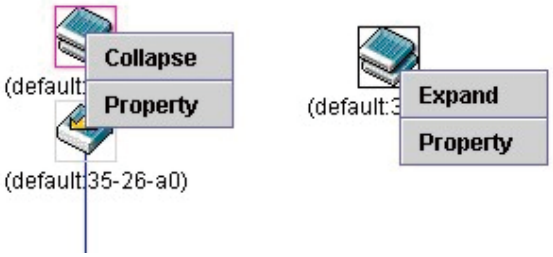


図 7-25　グループアイコン上での右クリック

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。

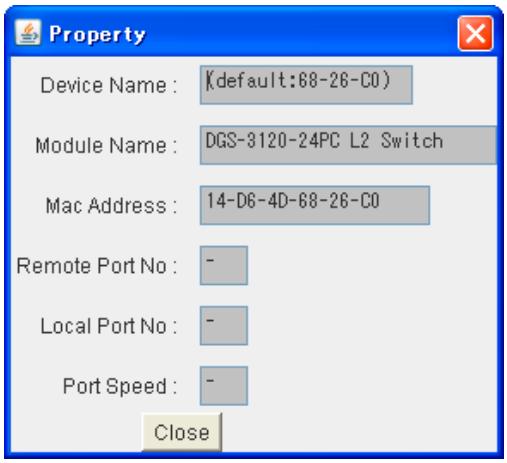


図 7-26　Property 画面

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

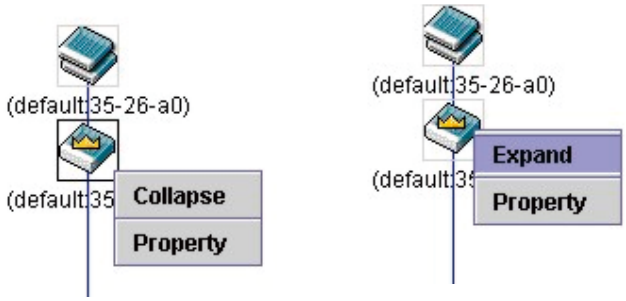


図 7-27　Commander スイッチアイコン上での右クリック

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

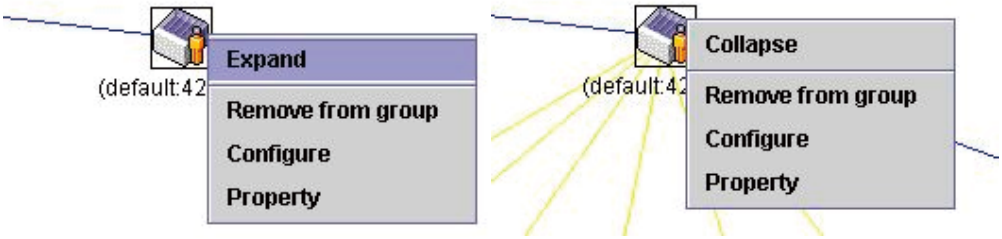


図 7-28　Member スイッチアイコン上での右クリック

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

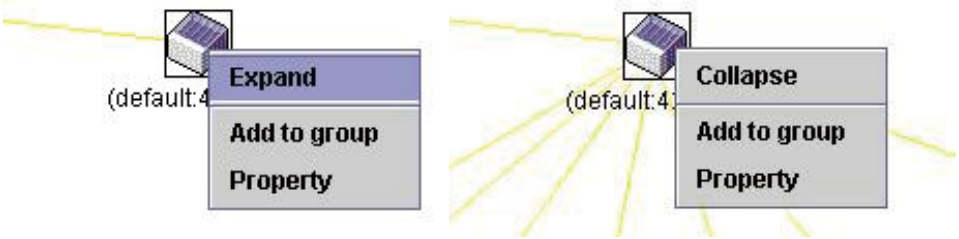


図 7-29　Candidate スイッチアイコン上での右クリック

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 7-30　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 7-31　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 7-32　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 7-33　SIM 情報

Firmware Upgrade（ファームウェア更新）

本画面は、CS から MS へのファームウェアの更新を行う場合に使用します。

Configuration > 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。

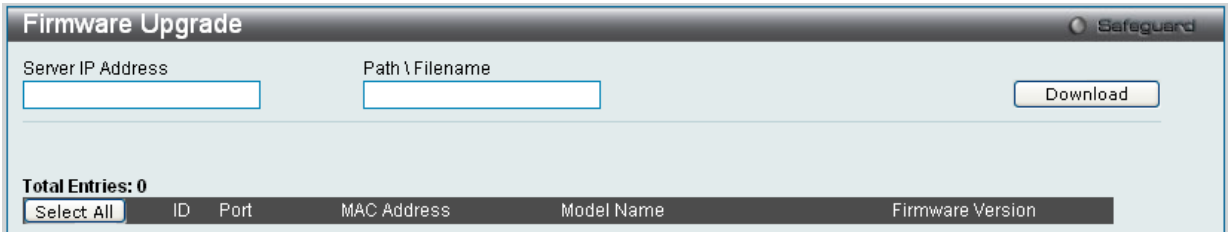


図 7-34　Firmware Upgrade 画面

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

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

本画面は、TFTP サーバを使用して CS から MS へのコンフィグレーションファイルの更新を行う際に使用します。

Configuration > 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。

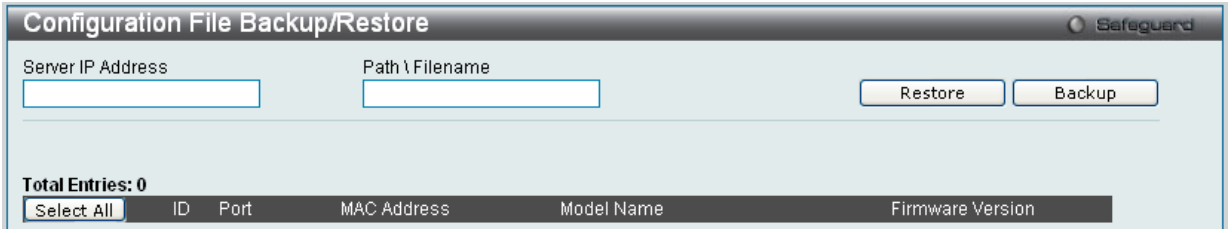


図 7-35　Configuration File Backup/Restore 画面

MS は「Port」（MS に接続する CS 上のポート）、「MAC Address」、「Model Name」、「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）

以下の画面は、SIM メンバスイッチから指定した PC へログファイルのアップロードを行う際に使用します。

Configuration > Single IP Management Setting > 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。

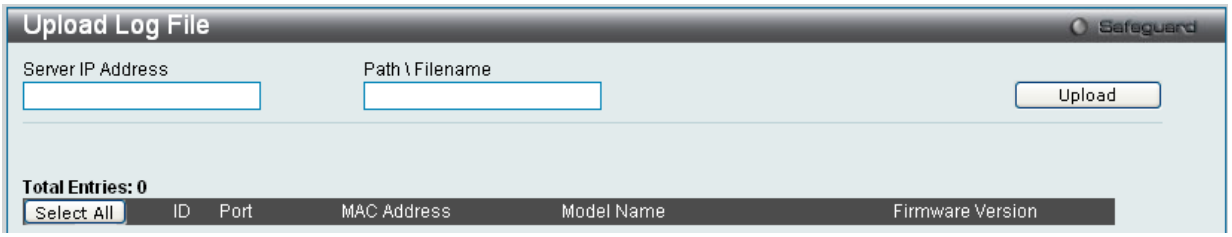


図 7-36　Upload Log File 画面

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

SNMP Settings（SNMP 設定）

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

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

—
本スイッチは、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。初期設定では SNMP 機能は無効になっているため、有効にする必要があります。SNMP 機能を有効にしたら、スイッチの監視と制御に使用する SNMP バージョンを選択します。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 2c 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 2c 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。

DGS-3120 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 Group Table」で行うことができます。

DGS-3120 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 Host Table」メニューを使用して、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 グローバル設定を「Enabled」（有効）または「Disabled」（無効）にします。

Management > SNMP Settings > SNMP Global 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。

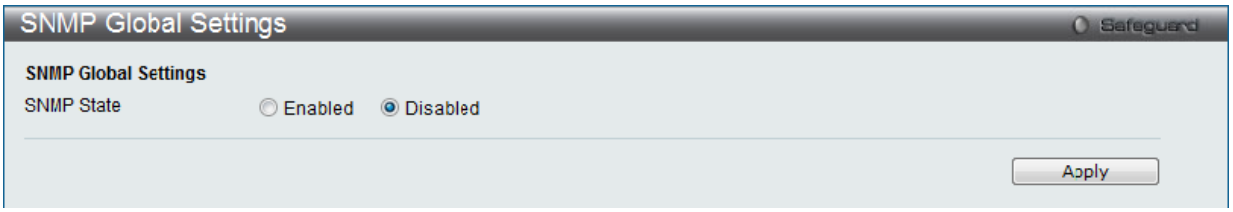


図 7-37　SNMP Global Settings 画面

「SNMP」機能の有効 / 無効を選択します。
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。

SNMP Traps Settings（SNMP トラップ設定）

以下の画面でスイッチの SNMP トラップを有効または無効にします。

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

図 7-38　SNMP Traps Settings 画面

以下の項目が使用されます。

項目	説明
SNMP Traps	「SNMP Traps」を有効 / 無効にします。
Authentication Trap	「Authentication Trap」を有効 / 無効にします。
Linkchange Traps	「Linkchange Traps」を有効 / 無効にします。
Coldstart Traps	「Coldstart Traps」を有効 / 無効にします。
Warmstart Traps	「Warmstart Traps」を有効 / 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。

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

スイッチの SNMP リンクチェンジトラップを有効または無効にします。

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

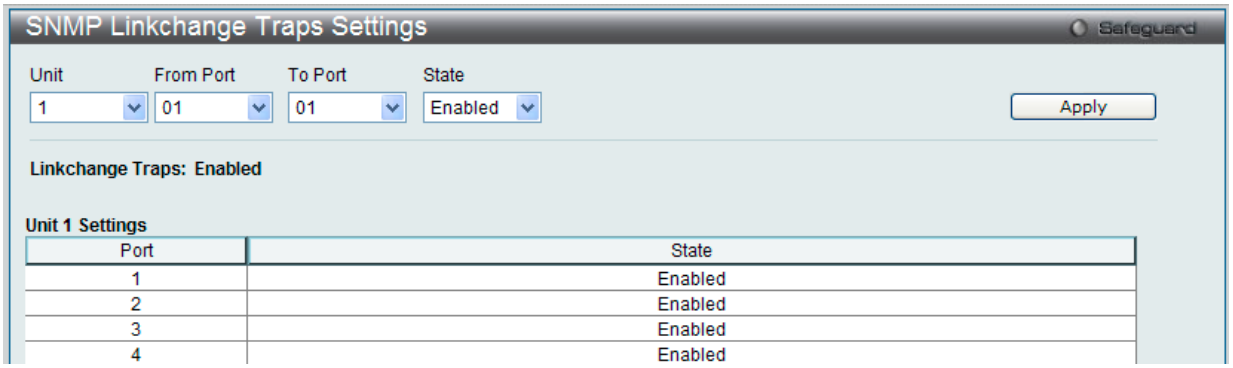


図 7-39　SNMP Linkchange Traps Settings 画面

以下の項目が使用されます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポートの始点 / 終点を設定します。
State	プルダウンメニューから SNMP リンクチェンジトラップの有効 / 無効を設定します。

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。

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

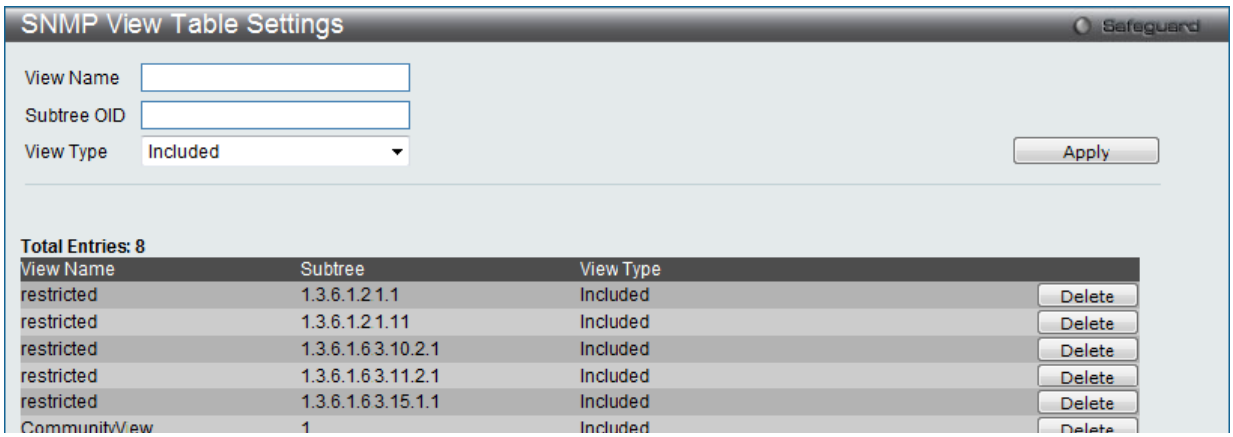


図 7-40　SNMP View Table 画面

エントリの削除

「SNMP View Table」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」を指定すると、アクセス可能に、「Excluded」を指定すると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）

「SNMP Community Table」は、SNMP コミュニティ名を登録し、SNMP マネージャとエージェントの関係を定義するために使用します。コミュニティ名は、スイッチ上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、スイッチ上の 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。

コミュニティエントリを設定するためには、**Management> SNMP Settings > SNMP Community Table** の順にクリックし、以下の画面を表示します。

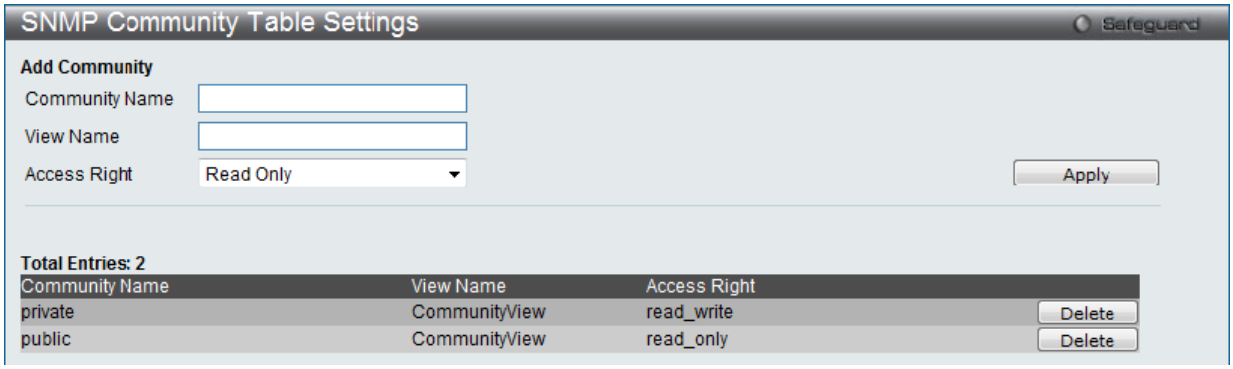


図 7-41　SNMP Community Table 画面

「SNMP Community Table」画面には、以下の項目があります。

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 の内容の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 の内容の読み出し、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 グループテーブル設定）

「SNMP Group Table」画面で登録する SNMP 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 の順にメニューをクリックし、以下の画面を表示します。

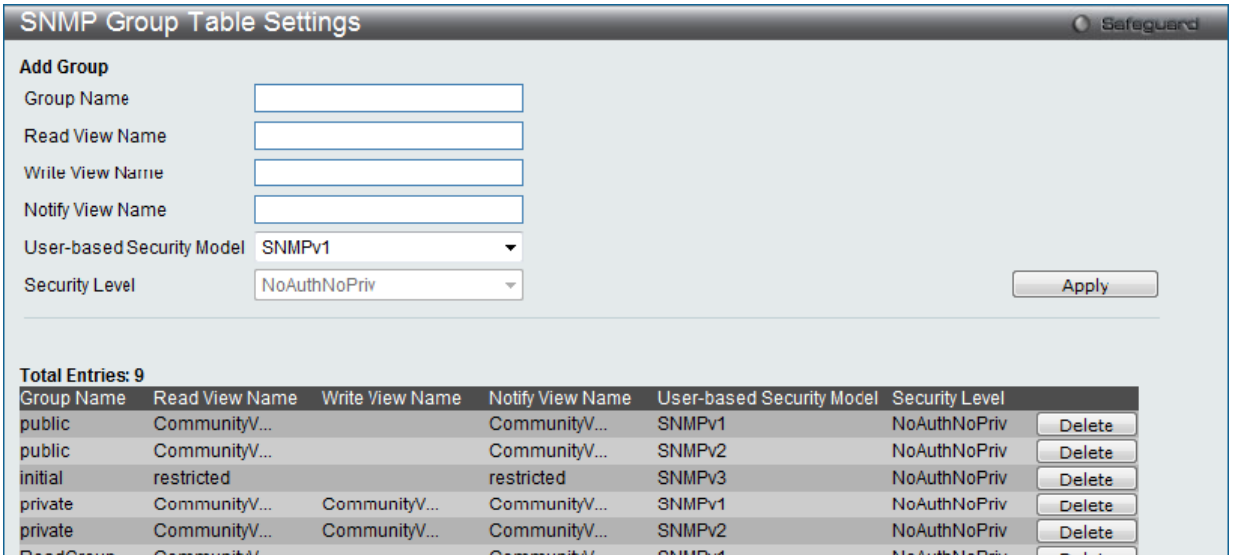


図 7-42　SNMP Group Table 画面

「SNMP Group Table」画面のエントリの削除
エントリの行の「Delete」ボタンをクリックします。

「SNMP Group Table」画面への新規エントリの追加
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	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	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。

スイッチの SNMP エンジン ID を表示します。

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

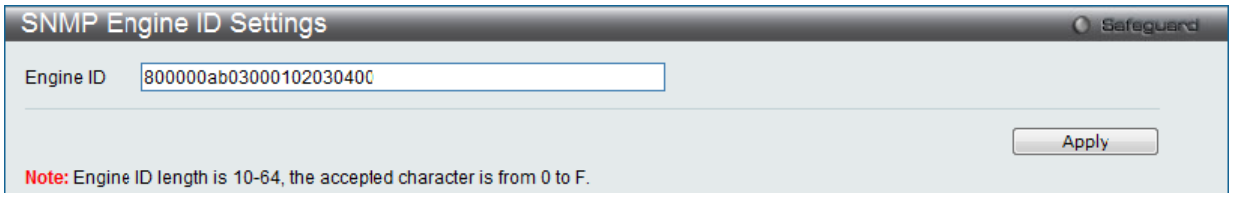


図 7-43　SNMP Engine ID 画面

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。

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

スイッチに現在設定されているすべての SNMP ユーザが表示されます。

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

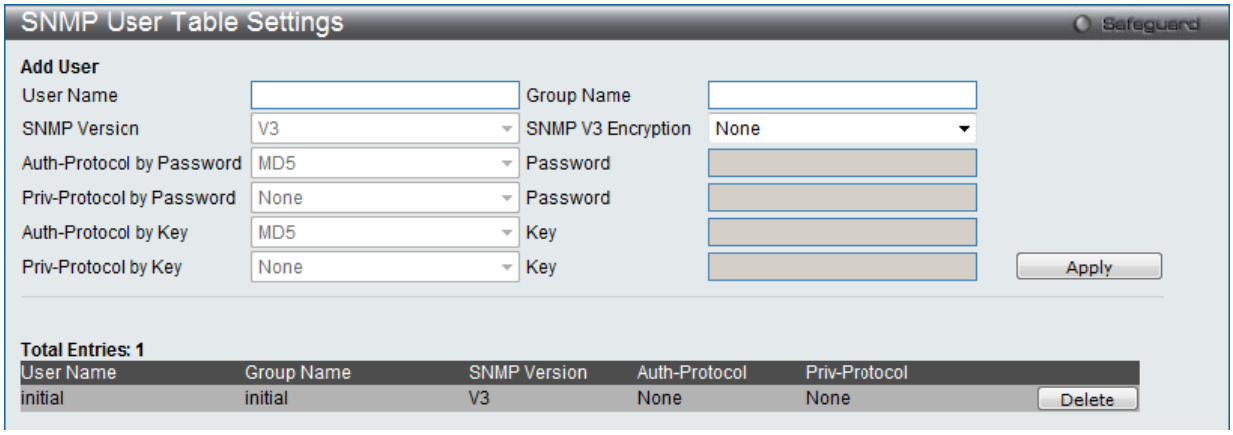


図 7-44　SNMP User Table 画面

エントリの削除

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。
Auth-Protocol	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	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）

SNMP トラップの送信先を登録します。

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

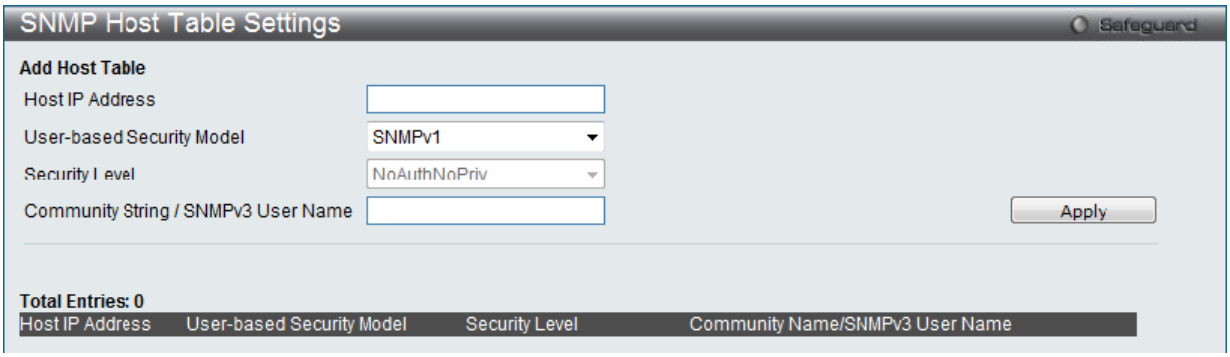


図 7-45　SNMP Host Table 画面

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の SNMP バージョン 3 が使用されます。 • AuthNoPriv : V3-Auth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。 • AuthPriv : V3-Auth-Priv セキュリティレベルの SNMP バージョン 3 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

「SNMP Host Table」画面内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。

SNMPv6 Host Table Settings（SNMPv6 ホストテーブル設定）

IPv6 の SNMP トラップの送信先を登録します。

Management > SNMP Settings > SNMPv6 Host Table の順にメニューをクリックし、以下の「SNMP Host Table」画面を表示します。

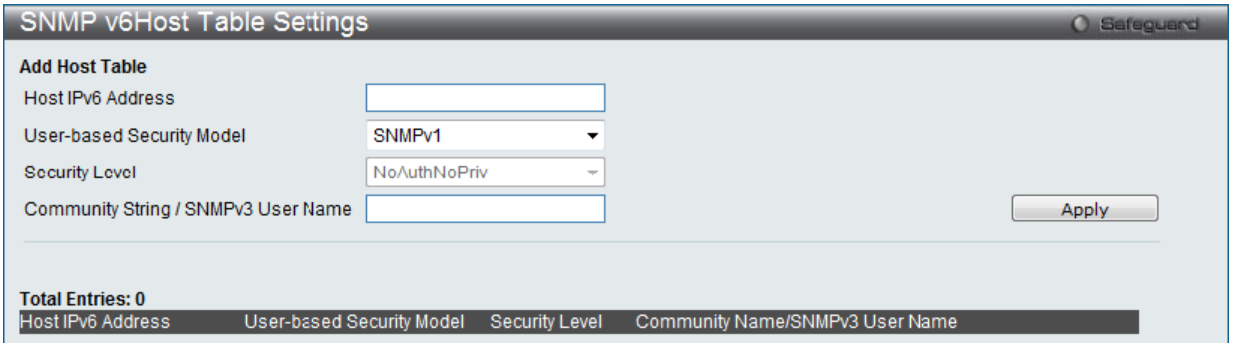


図 7-46　SNMPv6 Host Table 画面

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。

以下の項目が使用されます。

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。

項目	説明
Security Level	• NoAuthNoPriv : NoAuth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。 • AuthNoPriv : V3-Auth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。 • AuthPriv : V3-Auth-Priv セキュリティレベルの SNMP バージョン 3 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

「SNMP Host Table」画面内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。

RMON Settings（RMON 設定）

SNMP 機能のアラームトラップのを監視するリモートモニタリング機能（RMON）の有効 / 無効を設定します。

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

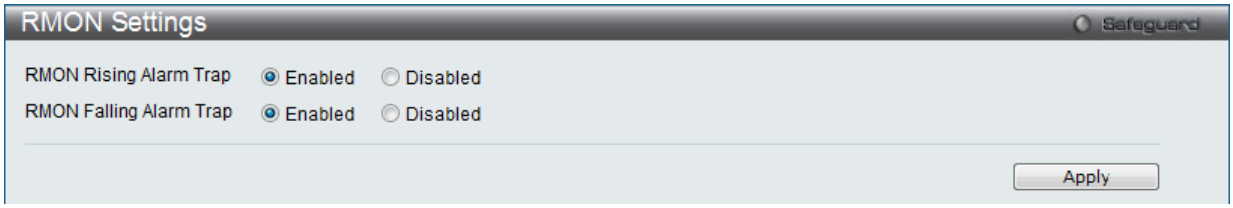


図 7-47　RMON Settings 画面

以下の項目が使用されます。

項目	説明
RMON Rising Alarm Trap	「RMON Rising Alarm Trap」を有効にします。
RMON Falling Alarm Trap	「RMON Falling Alarm Trap」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。

SNMP Community Encryption Settings（SNMP コミュニティ暗号化設定）

SNMP コミュニティ名の暗号化状態を有効または無効にします。

Management > SNMP Settings > SNMP Community Encryption 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。

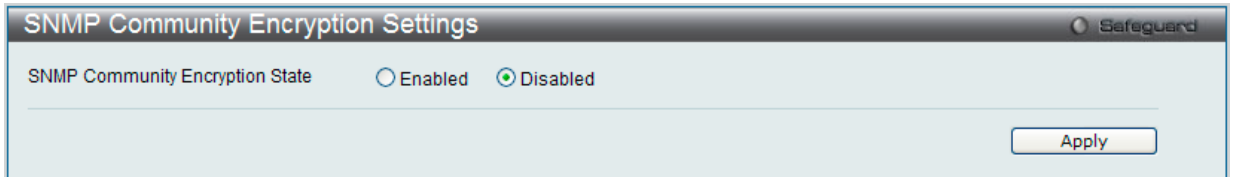


図 7-48　SNMP Community Encryption Settings 画面

以下の項目を設定します。

項目	説明
SNMP Community Encryption State	SNMP コミュニティ名の暗号化を「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。

SNMP Community Masking Settings（SNMP コミュニティマスク設定）

SNMP コミュニティ名を作成するためのセキュリティ方式を選択します。ただし、コミュニティ名の暗号化の有無は、SNMP コミュニティ暗号化状態に従います。

Management > SNMP Settings > SNMP Community Masking 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。

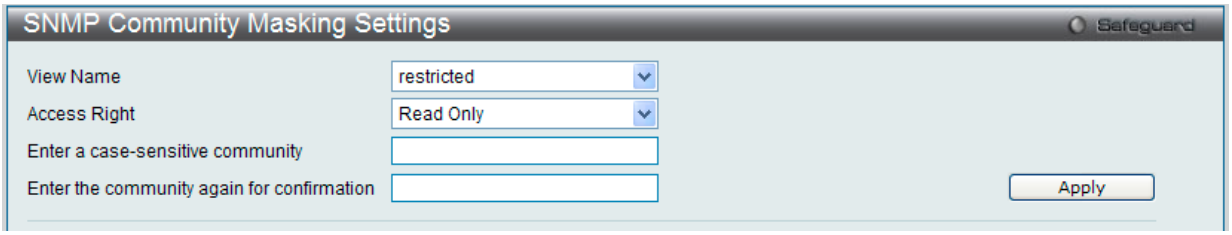


図 7-49　SNMP community Masking Settings 画面

以下の項目を設定します。

項目	説明
View Name	プルダウンメニューを使用して、MIB ビュー名を選択します。
Access Right	コミュニティ名を使用するユーザのアクセス権を選択します。 • Read_Only - 定義済みのコミュニティストリングを使用する SNMP コミュニティメンバは、スイッチにおける MIB コンテンツの読み出しのみ可能となります。 • Read_Write - 定義済みのコミュニティストリングを使用する SNMP コミュニティメンバは、スイッチにおける MIB コンテンツの読み出し、および書き込みが可能です。
Enter a case-sensitive community	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。本項目は、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。
Enter the community again for confirmation	確認のために、コミュニティを再度入力します。

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。

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。

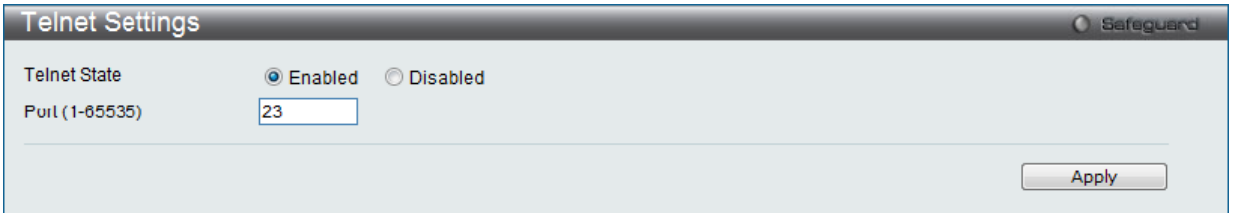


図 7-50　Telnet Settings 画面

以下の項目が使用されます。

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（1-65535）。Telnet プロトコルに通常使用される TCP ポートは 23 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。

Web Settings（Web 設定）

スイッチに Web 設定をします。

Management > Web 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。

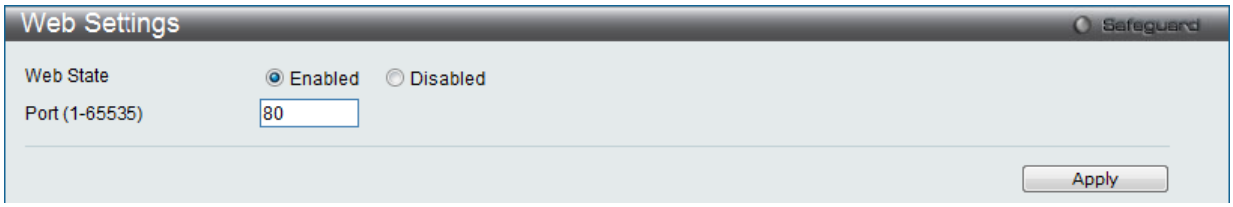


図 7-51　Web Settings 画面

以下の項目が使用されます。

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、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。

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。

Power Saving（省電力機能）

スイッチの電源を節電する機能を実装しています。

LED State Settings（LED 設定）

ポート LED の状態について設定します。

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。

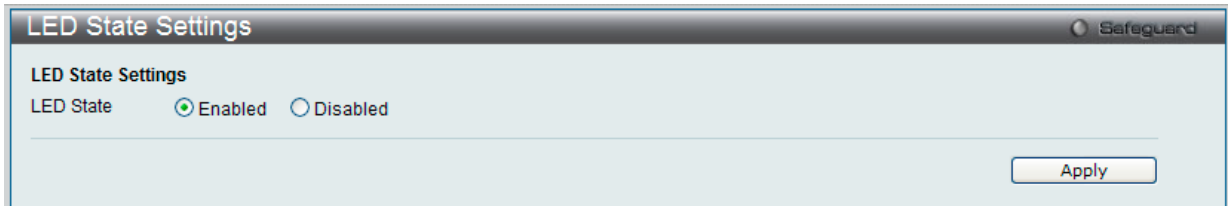


図 7-52　LED State Settings 画面

以下の項目が使用されます。

項目	説明
LED State	ポート LED の有効 / 無効を選択します。

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。

Power Saving Settings（省電力設定）

スイッチの内蔵電源を節電する機能を実装しています。省電力機能を使用する時間を設定します。

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。

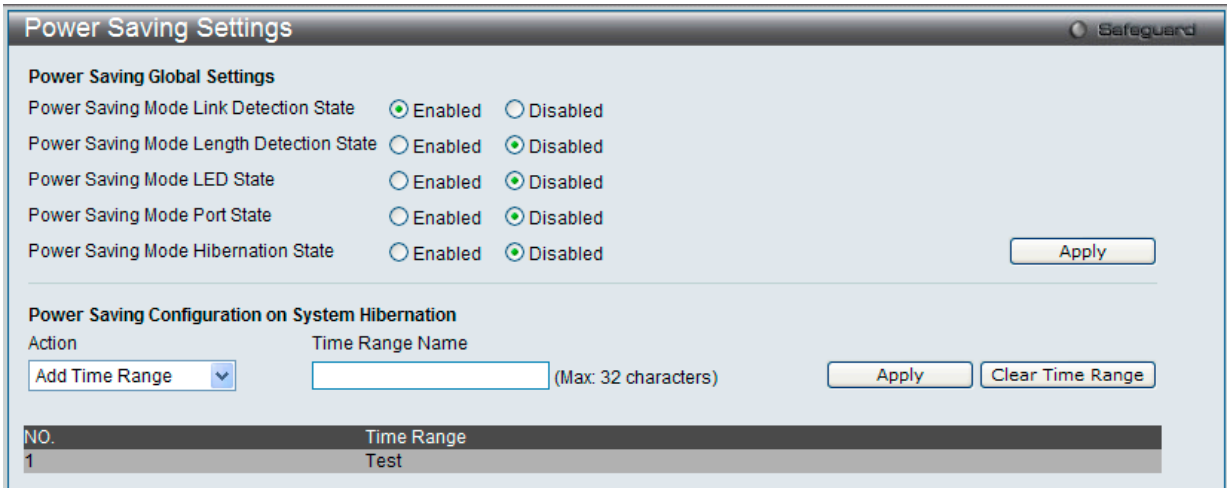


図 7-53　Power Saving Settings 画面

以下の項目が使用されます。

項目	説明
Power Saving Mode Link Detection State	リンク検知の有効 / 無効を設定します。有効の場合、リンクダウンしているポートへの電力供給は行われず、スイッチの電力消費を抑えます。ポートがリンクアップしている場合は通常通り動作します。
Power Saving Mode Length Detection State	ケーブル長検知の有効 / 無効を設定します。有効の場合、スイッチは自動的にケーブルの長さを検知しトラフィックに必要な電力をポートへの供給します。
Power Saving Mode LED State	LED の有効 / 無効を設定します。有効の場合、設定した時間内にポート LED は点灯されません。
Power Saving Mode Port State	ポート起動の有効 / 無効を設定します。有効の場合、設定した時間内ポートはシャットダウンされます。
Power Saving Mode Hibernation State	スイッチ休止の有効 / 無効を設定します。有効の場合、設定した時間内スイッチは低電力モードに移行し、アイドリング状態となり全ポート / 全ネットワーク機能（telnet、ping、その他）はシャットダウンされます。RS232 ポートを使用したコンソール機能のみ有効です。スイッチに PoE 給電機能がある場合も、ポートに電力は給電されません。
Action	スケジュールの追加 / 削除を行います。
Time Range Name	スケジュール名を設定します。

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。
全エントリを削除する際は、「Clear Time Range」ボタンをクリックします。

Power Saving LED Settings（LED 省電力設定）

ポート LED 省電力機能の設定を行います。

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。

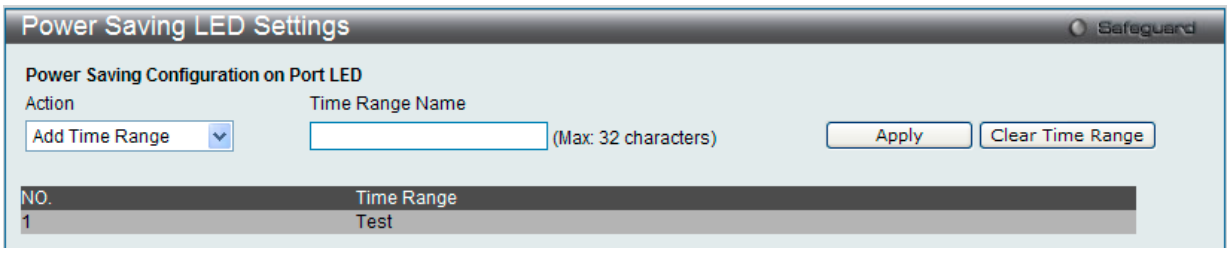


図 7-54　Power Saving LED Settings 画面

以下の項目が使用されます。

項目	説明
Action	スケジュールの追加 / 削除を行います。
Time Range Name	スケジュール名を設定します。

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。
全エントリを削除する際は、「Clear Time Range」ボタンをクリックします。

Power Saving Port Settings（ポート省電力設定）

ポート省電力機能の設定を行います。

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。

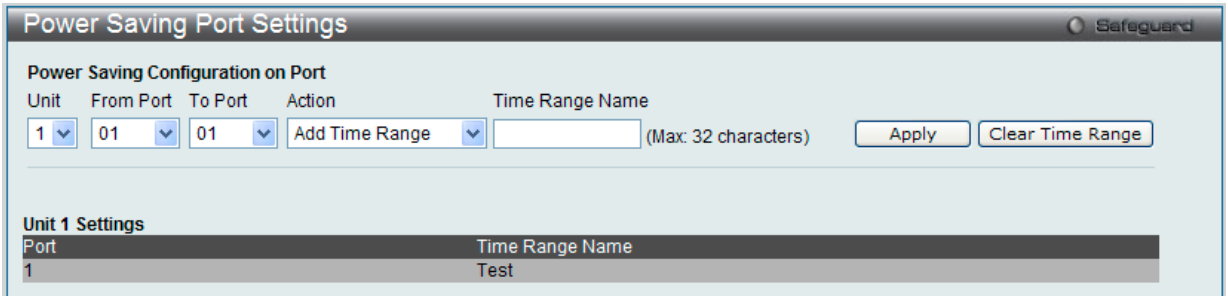


図 7-55　Power Saving Port Settings 画面

以下の項目が使用されます。

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選択します。
Action	スケジュールの追加 / 削除を行います。
Time Range Name	スケジュール名を設定します。

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。
全エントリを削除する際は、「Clear Time Range」ボタンをクリックします。

SD Card Management（SD カード管理）

SD カードを使用して、ログやコンフィグレーションの保存を行います。

SD Card Backup Settings（SD カードへのバックアップ設定）

ログやコンフィグレーションをバックアップするスケジュールを設定します。

Management > SD Card Management > SD Card Backup 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。

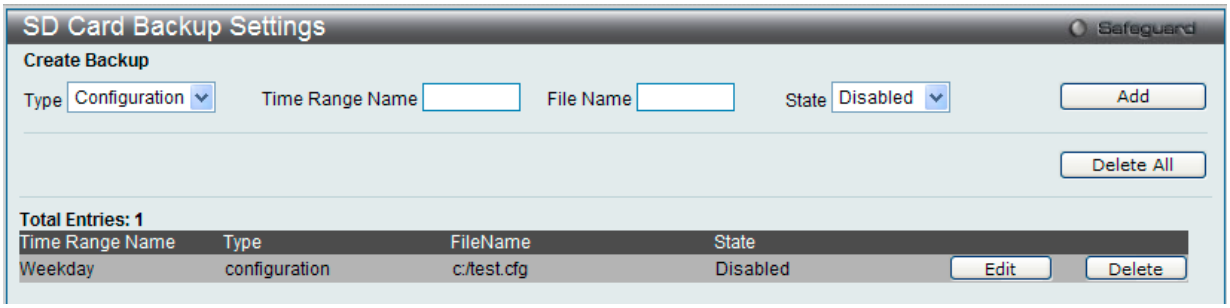


図 7-56　SD Card Backup Settings 画面

エントリの新規登録

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、「Add」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
Type	設定するコンフィグレーション / ログのどちらか選択します。
Time Range Name	スケジュール名を設定します。
File Name	バックアップファイルを命名します。
State	バックアップスケジュールの有効・無効を設定します。

エントリの削除

削除するのエントリの「Delete」ボタンをクリックします。「Delete All」ボタンをクリックし、テーブル上の全エントリを新削除します。

エントリの編集

「Edit」ボタンをクリックし、以下の画面を表示します。

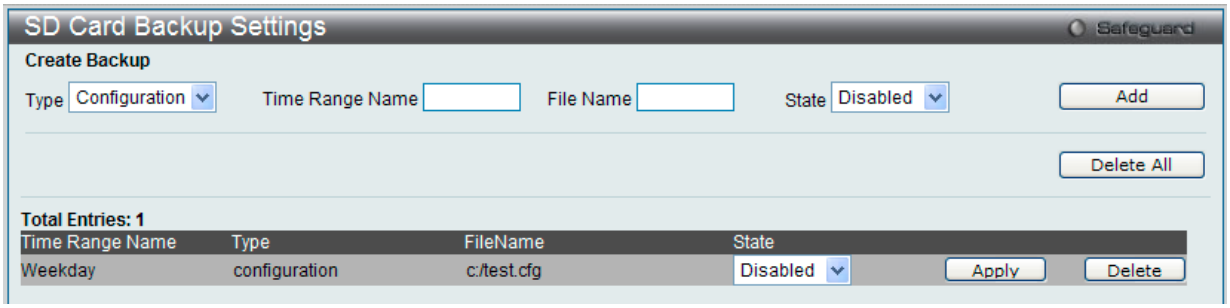


図 7-57　SD Card Backup Settings 画面 - 編集

指定のエントリを編集し、「Apply」ボタンをクリックします。

SD Card Execute Settings（SD カード実行設定）

SD カード内の設定ファイルをスイッチのファイルシステム上で実行します。

Management > SD Card Management > SD Card SD Card Execute 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。

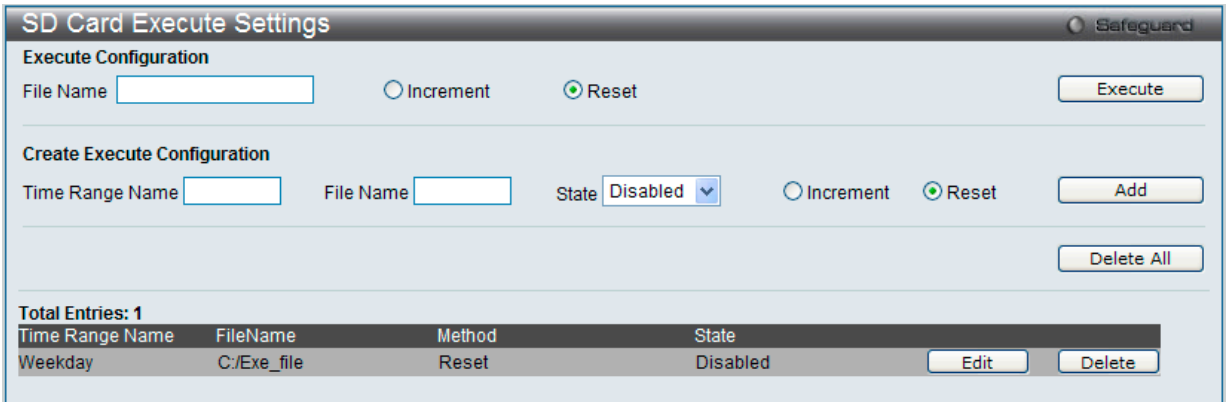


図 7-58　SD Card Execute Settings 画面

エントリの新規登録

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、「Add」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
File Name	設定ファイル名です。
Increment	本オプションが設定されると、実行前に現在の設定がリセットされません。
Reset	本オプションが設定されると、実行前に現在の設定がリセットされます。
Time Range Name	スケジュールを設定します。
State	ファイル実行の時間を設定します。

システムの設定ファイルの実行
実行するファイル名を指定後、「Execute」ボタンをクリックします。

エントリの削除
削除するのエントリの「Delete」ボタンをクリックします。「Delete All」ボタンをクリックし、テーブル上の全エントリを新削除します。

エントリの編集
「Edit」ボタンをクリックし、以下の画面を表示します。

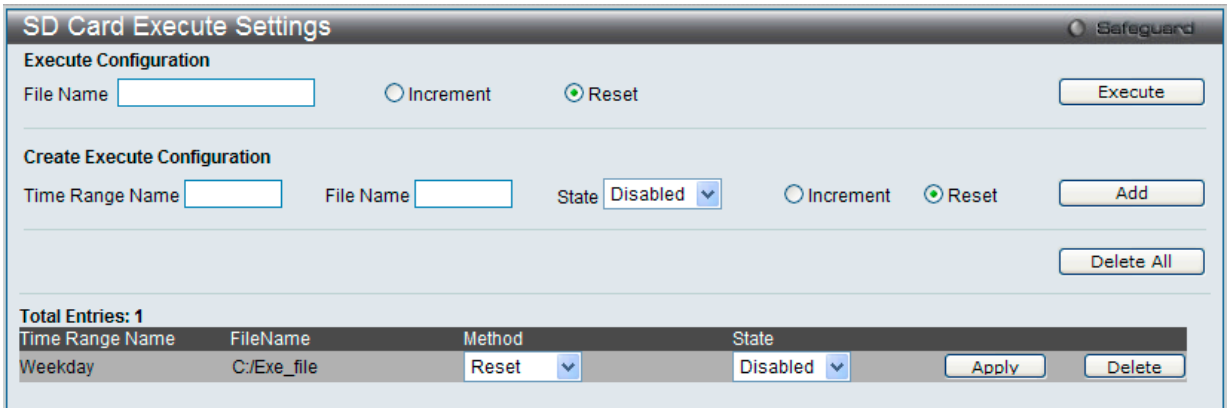


図 7-59　SD Card Execute Settings 画面 - 編集

指定のエントリを編集し、「Apply」ボタンをクリックします。

第 8 章　L2 Features（レイヤ 2 機能の設定）

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

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

サブメニュー	説明	参照ページ
VLAN（ VLAN 設定）	802.1Q スタティック VLAN 設定を行います。以下のメニューがあります。 802.1Q VLAN Settings（802.1Q VLAN 設定）、802.1v Protocol VLAN（802.1v プロトコル VLAN）、Asymmetric VLAN Settings（Asymmetric VLAN 設定）、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）、Voice VLAN（音声 VLAN）、Surveillance VLAN（サーベイランス VLAN）、Surveillance VLAN OUI Settings（サーベイランス VLAN OUI 設定）、VLAN Trunk Settings（VLAN トランク設定）、Browse VLAN（VLAN の参照）、Show VLAN Ports（VLAN ポートの参照）	110
QinQ（QinQ 設定）（EI モードのみ）	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）	124
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。	127
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）	128
Link Aggregation（リンクアグリゲーションの設定）	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）	135
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）	138
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 Snooping（IGMP スヌーピングの設定）、MLD Snooping（MLD スヌーピング設定）、Multicast VLAN（マルチキャスト VLAN）	142
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）	164
ERPS Settings（イーサネットリングプロテクション設定）（EI モードのみ）	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。	170
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 Statistics System（LLDP 統計情報システム）、LLDP-MED（LLDP-MED 設定）	174
NLB FDB Settings（NLB FDB 設定）	NLB 機能を設定します。	182

VLAN の概要

IEEE 802.1p プライオリティについて

プライオリティのタグ付けは 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。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、ネットワークにおけるプライオリティタグ付きのデータパケットを処理するための定義を強化しました。データ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データの相対的な優先度を設定できます。2 つ以上の異なるタグ付きパケットを同じキューに分類することが有利である場合に行われます。一般的には最高の優先度のキュー（キュー 3）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。

スイッチは、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 8 : 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 3）が 8 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 について

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、帯域を浪費せずに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、IEEE802.1Q VLAN をサポートしています。ポートアンタギング機能は、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

項目	内容
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 種類のルールに基づいて決定されます。
- イングレスルール - 受け取ったパケットがどの VLAN に所属するかの分類に関するルール。
- ポート間のフォワーディングルール - 転送するかしないかを決定します。
- イーグレスルール - パケットが送信される時にタグ付きかタグなしかを決定します。

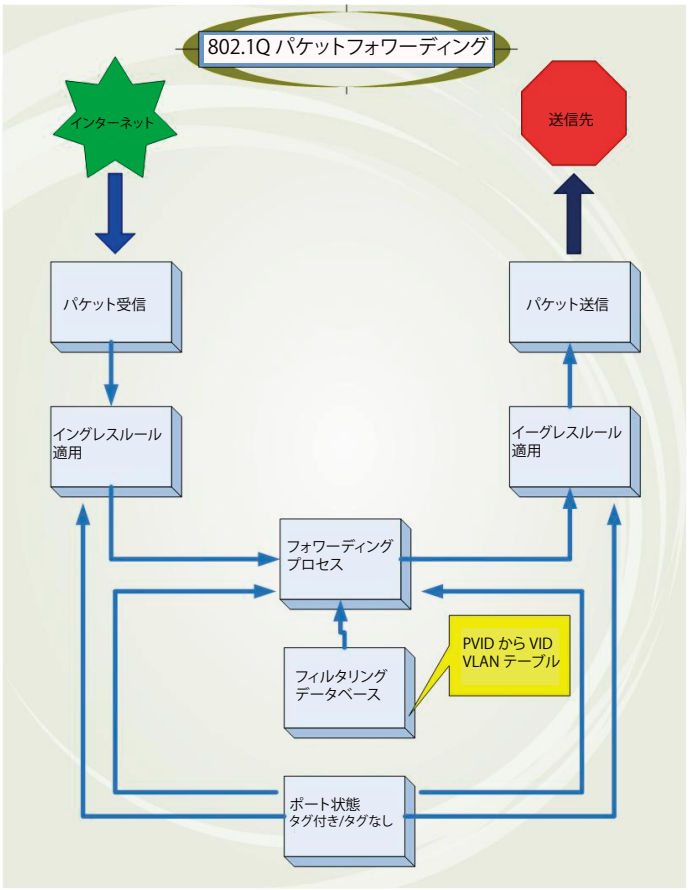


図 8-1　IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

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

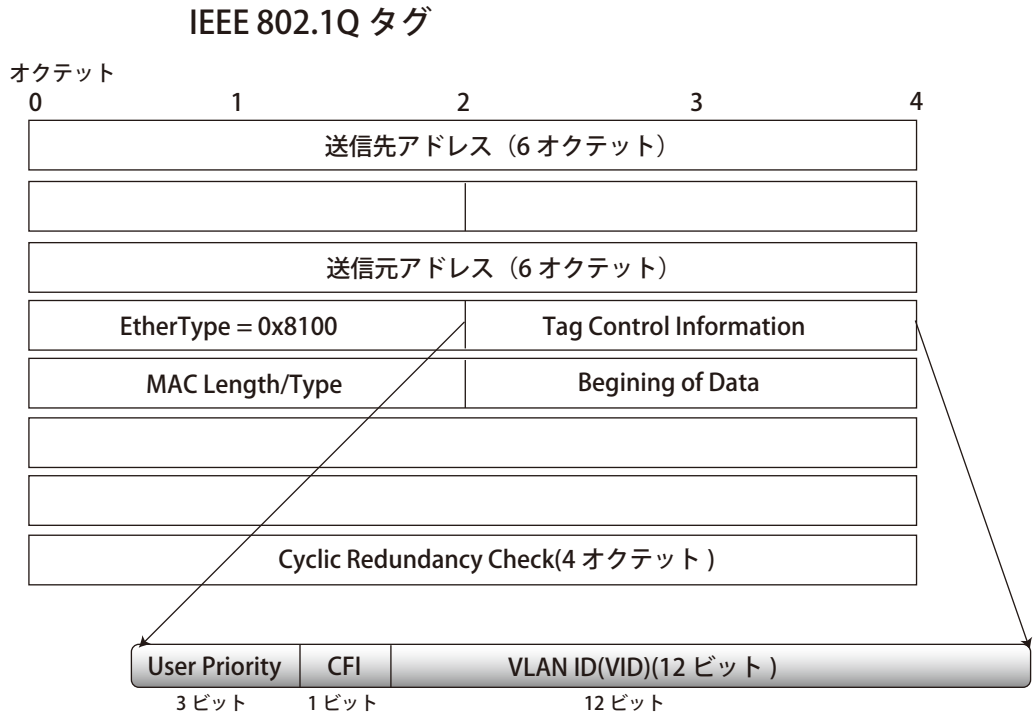


図 8-2　IEEE 802.1Q タグ

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

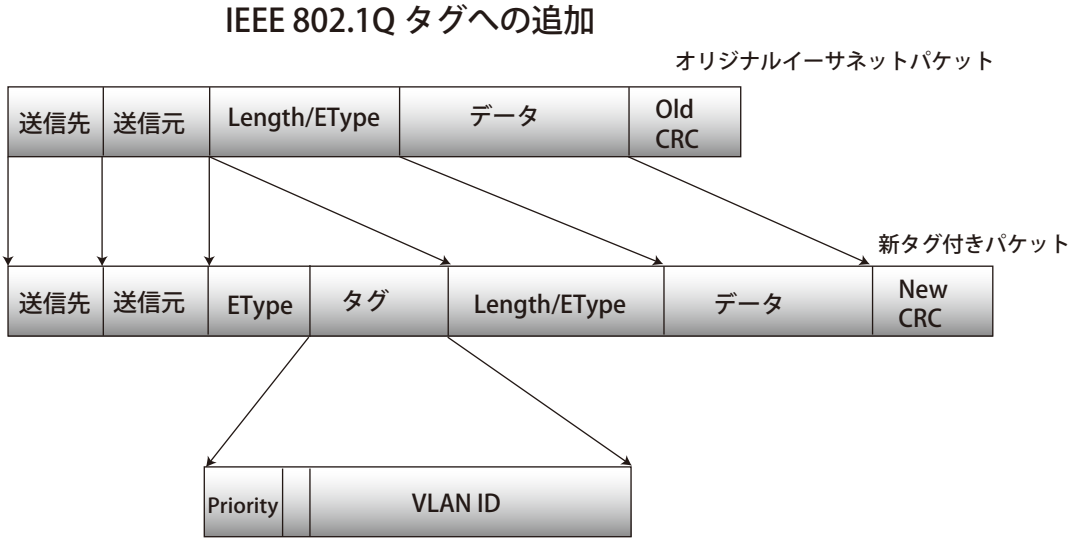


図 8-3　IEEE 802.1Q タグの挿入

ポート VLAN ID

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

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

802.1Q VLAN が採用される以前は、ポートベースや MAC ベースの VLAN が主流でした。これらの VLAN でのパケット送信はポート VLAN ID（PVID）を元に行われます。あるポートで受信したパケットには、そのポートの PVID を割り当てて、パケットの宛先アドレス（スイッチのフォワーディングテーブルで参照）へと送信されます。もしパケットを受信したポートの PVID がパケットの宛先ポートの 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、スイッチで使用されます。スイッチに 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 PVID1 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。

タギングとアンタギング

802.1Q に対応するスイッチのすべてのポートは、タグ付きかタグなしに設定できます。
タグ付きのポートは受信、送信するすべてのパケットのヘッダに、VID、プライオリティ、そしてそのほかの VLAN 情報を埋め込みます。パケットが既にタグ付けされていた場合、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 として自身の 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、はじめに「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のすべてのポートが「default」に割り当てられています。

ポートをデフォルト VLAN から削除することはできません。ポートが他の VLAN にタグなしメンバとして設定されている場合には、デフォルト VLAN から自動的に削除されます。

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。

表 8-1　VLAN 設定例 – ポートの割り当て

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）

VLAN リストでは、VLAN、VLAN メンバおよびメンバタイプを表示します。また、現在イーグレスまたはタグ付きポートであるスイッチポートを表示します。

802.1Q VLAN Settings（802.1Q VLAN 設定）

「VLAN List」画面は、事前に設定した VLAN を VLAN ID、VLAN 名と共に表示します。

L2 Features > VLAN > 802.1Q VLAN の順にクリックし、次の画面を表示します。

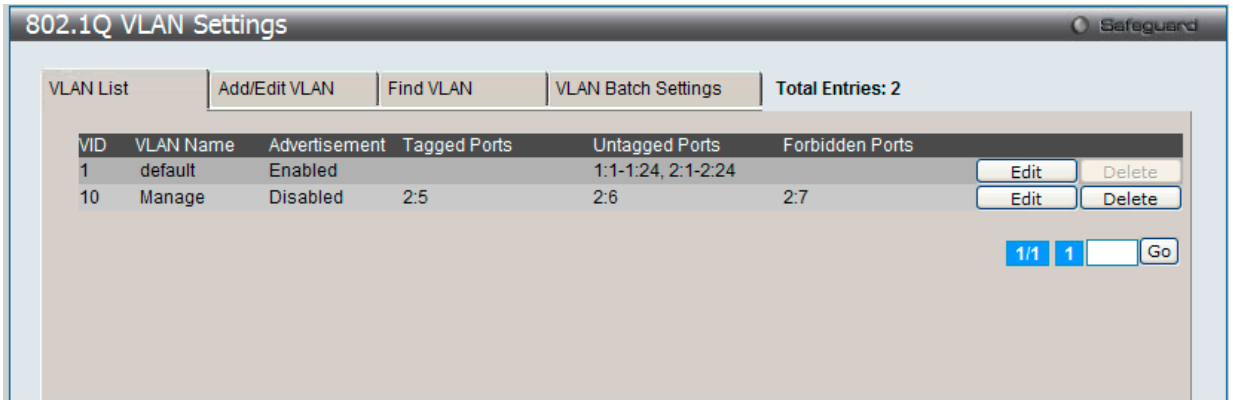


図 8-4　802.1Q VLAN - VLAN Settings –VLAN List タブ画面

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

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

新しい VLAN の作成や既存の VLAN の編集

1. 「Add/Edit VLAN」タブをクリックし、以下の画面を表示します。

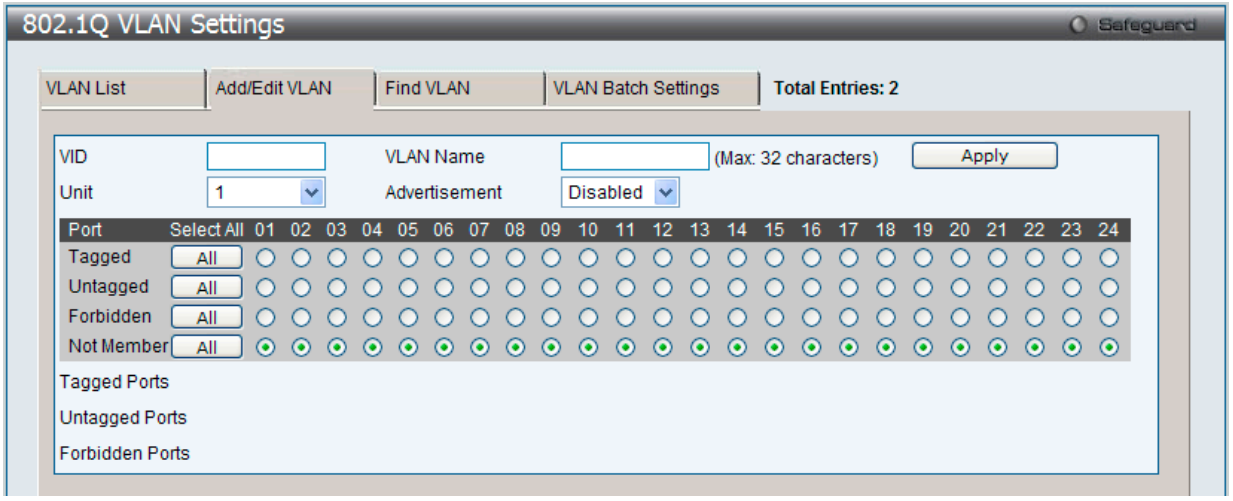


図 8-5　802.1Q VLAN - Add/Edit VLAN タブ画面

2. ポートの設定と新しい VLAN に固有の名前と番号を割り当てます。

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。

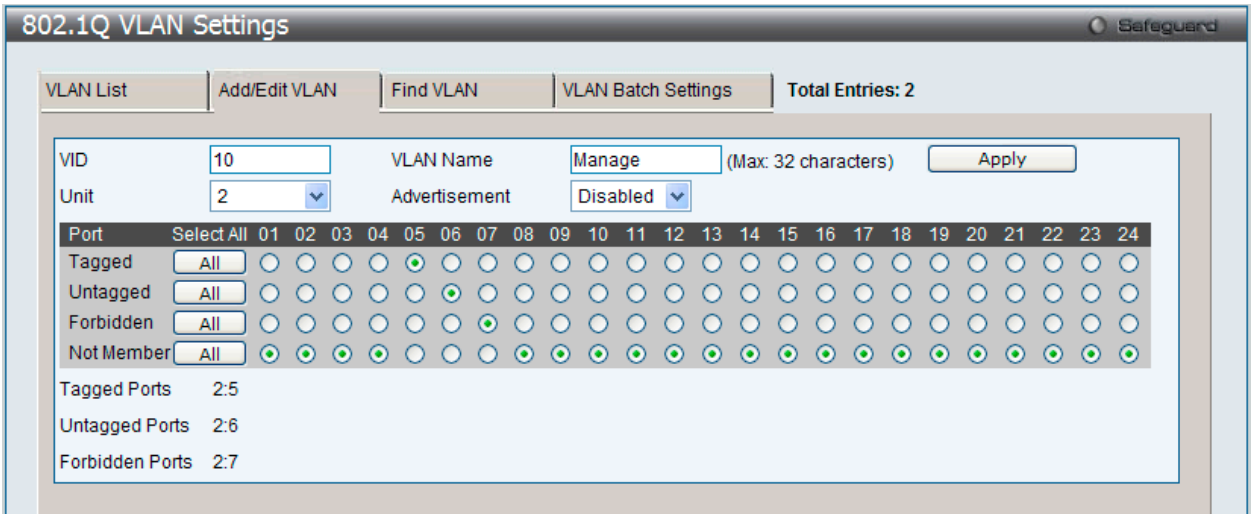


図 8-6　802.1Q VLAN Settings - Add/Edit VLAN タブ画面（Edit）

「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」タブ画面には以下の項目が含まれます。

項目	内容
VID	802.1Q 標準によって使用される VLAN 識別子（VID）を定義します。VID タグはパケットヘッダに挿入され、4 オクテットでより長いパケットを増加させます。パケットに元々含まれている情報のすべてが保持されています。
VLAN Name	ユーザ定義の VLAN 名を定義します。（1 ～ 29 文字の半角英数字）
Advertisement	既存の VLAN に追加するかどうかの通知する GVRP パケットを外部ソースに送信します。
Unit	VLAN パラメータが表示されるスタックメンバを定義します。
Port	スイッチの設定可能なポートです。
Tagged	インタフェースがタグ付きメンバであることを定義します。インタフェースによって転送されるパケットはタグ付きです。パケットは VLAN 情報を含んでいます。「All」ボタンをクリックすると、すべてのポートがタグ付きとなります。
Untagged	インタフェースがタグなしメンバであることを定義します。インタフェースによって転送されるパケットはタグなしです。「All」ボタンをクリックすると、すべてのポートがタグなしとなります。
Forbidden	自動的に VLAN メンバに設定されないポートを指定します。「All」ボタンをクリックすると、すべてのポートが Forbidden ポートとなります。
Not Member	インタフェースが VLAN のメンバでないことを定義します。

「Apply」ボタンをクリックし、設定を適用します。

VLAN の検索

1. 「Find VLAN」タブをクリックし、以下の画面を表示します。

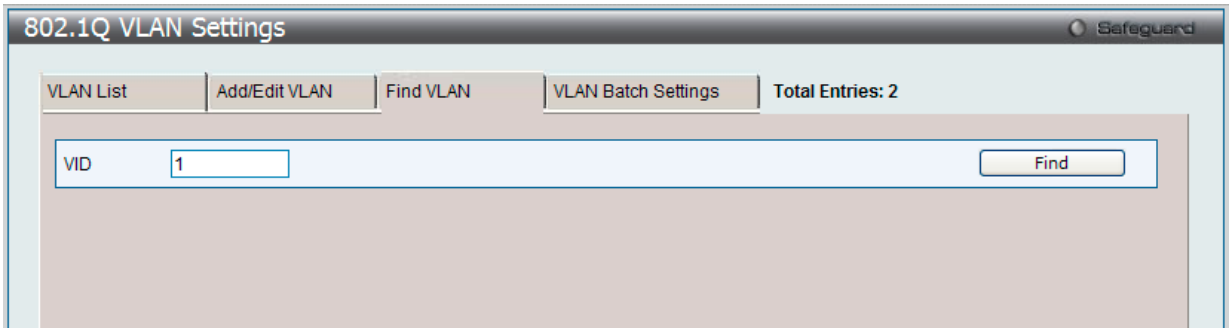


図 8-7　802.1Q VLAN - Find VLAN タブ画面

2. VLAN ID を入力して「Find」ボタンをクリックします。「VLAN List」タブに移動します。

VLAN バッチエントリの作成、削除、編集

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

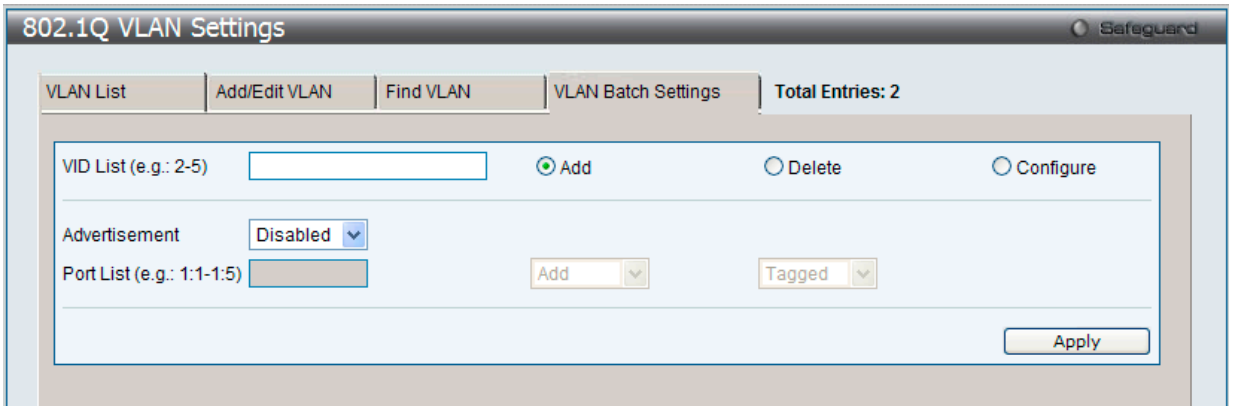


図 8-8　802.1Q VLAN - VLAN Batch Settings タブ画面

「VLAN Batch Settings」タブ画面には以下の項目が含まれます。

項目	内容
VID List	追加、削除、設定する VLAN ID リストを入力します。
Advertisement	既存の VLAN に追加するかどうかを通知する GVRP パケットを外部ソースに送信します。
Port List	VLAN メンバとして追加、削除するポートリストです。
Tagged	インタフェースがタグ付きメンバであることを定義します。インタフェースによって転送されるパケットはタグ付きです。パケットは VLAN 情報を含んでいます。「All」ボタンをクリックすると、すべてのポートがタグ付きとなります。
Untagged	インタフェースがタグなしメンバであることを定義します。インタフェースによって転送されるパケットはタグなしです。「All」ボタンをクリックすると、すべてのポートがタグなしとなります。
Forbidden	自動的に VLAN メンバに設定されないポートを指定します。「All」ボタンをクリックすると、すべてのポートが Forbidden ポートとなります。

「Apply」ボタンをクリックし、設定を適用します。

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

802.1v Protocol VLAN では次の 2 つの項目を設定します。:「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。

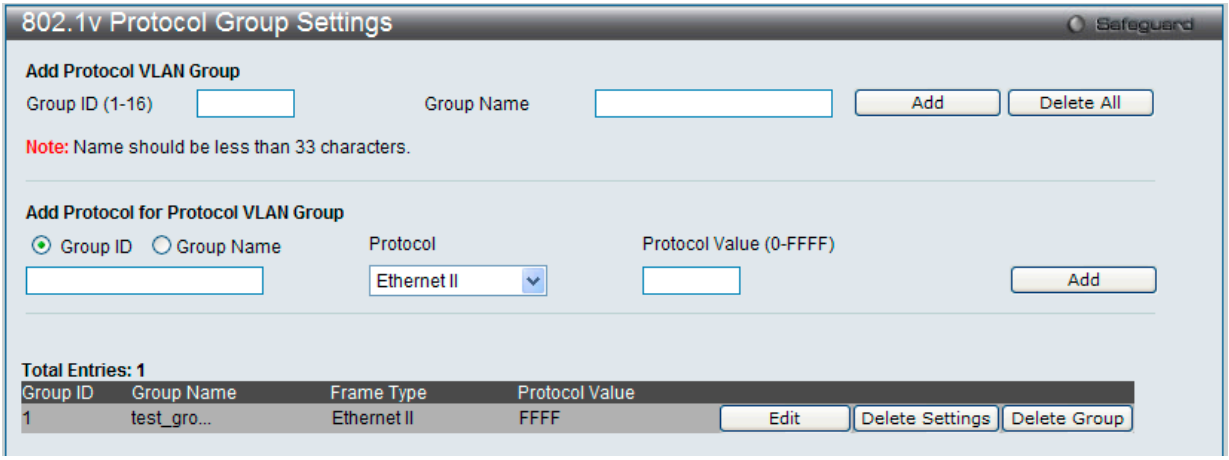


図 8-9　802.1v Protocol VLAN Group Settings 画面

以下の項目を使用して、設定します。

項目	説明
Group ID（1-16）	グループの ID 番号。1-16 の範囲から指定します。
Group Name	新しいプロトコル VLAN グループの識別に使用します。32 文字までの半角英数字を入力します。
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 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。

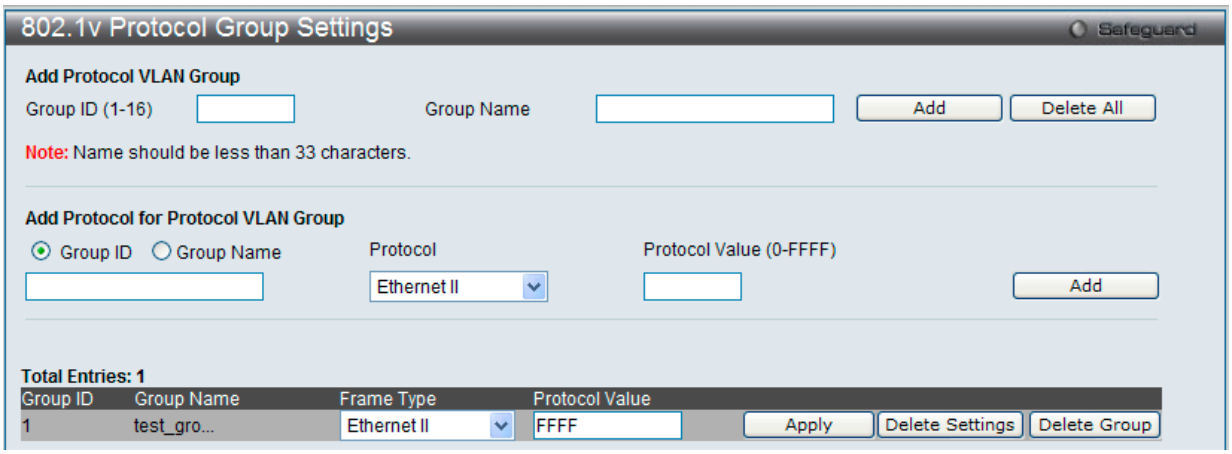


図 8-10　802.1v Protocol Group Settings 画面 - Edit

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）

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

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

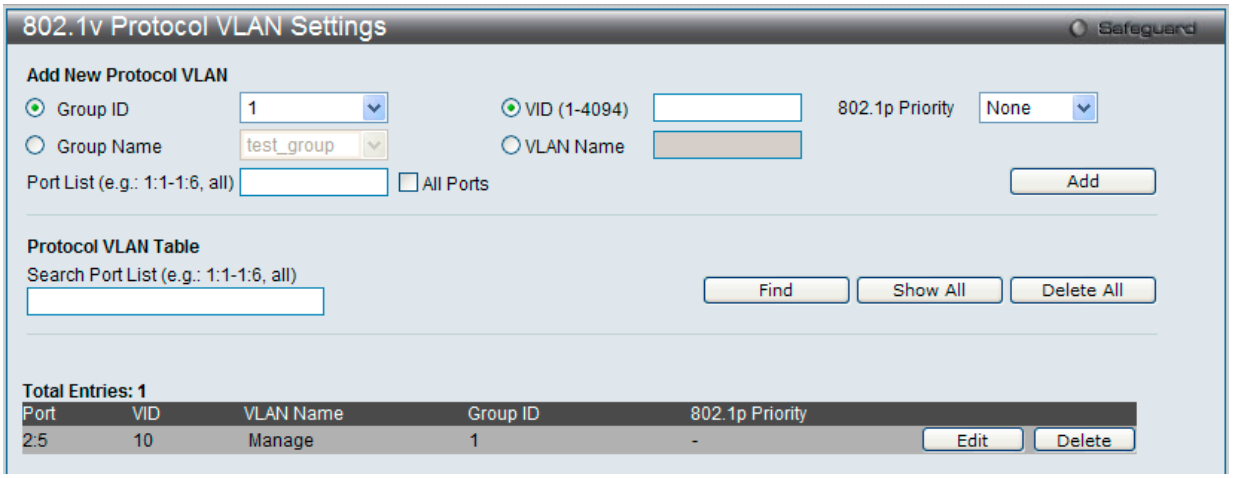


図 8-11　Protocol VLAN Settings 画面

以下の項目を使用して、設定します。

項目	説明
Group ID	対応するラジオ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	対応するラジオ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)	ラジオボタンをクリックして、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	ラジオ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の中の、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。
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」チェックボックスをチェックします。
Search Port List	本機能で、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。

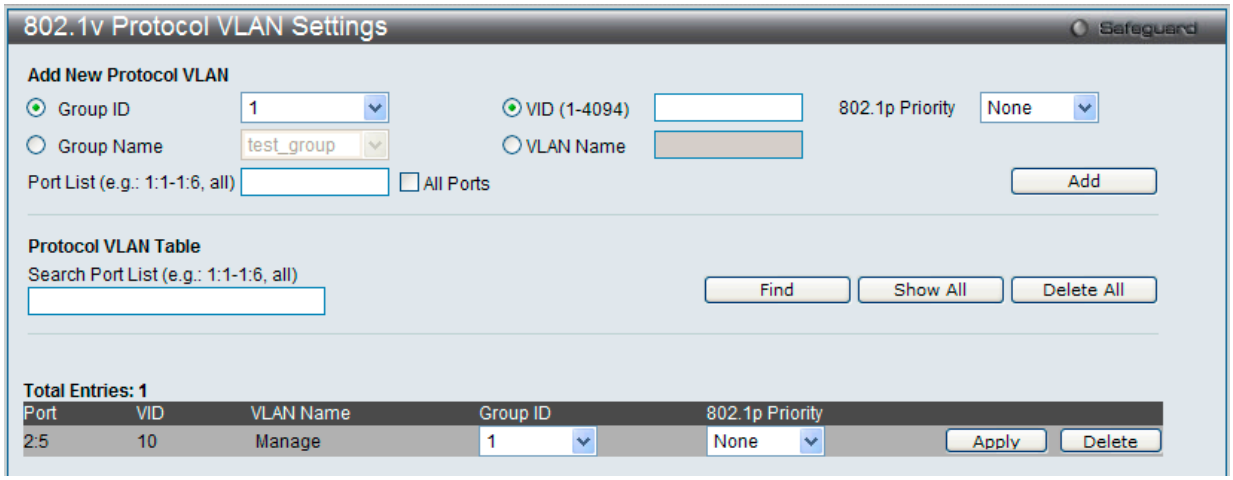


図 8-12　802.1v Protocol VLAN Settings 画面 - Edit

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。

Asymmetric VLAN Settings（Asymmetric VLAN 設定）

共有 VLAN 学習（SVL : Shared VLAN Learning）は Asymmetric VLAN が必要となる主な例です。通常の環境下では、VLAN 環境で通信する 1 組の装置は、同じ VLAN を使用して送受信します。しかし、Asymmetric VLAN が必要とされる場合、B に送信するために A に使用される VLAN と A に送信するために使用される VLAN の 2 つの異なる VLAN を使用することが便利です。このタイプの設定が必要とされる例は、クライアントが異なる IP サブネットにある場合、または機密に関連する必要性があり、クライアント間のトラフィックを分ける場合です。

L2 Features > VLAN > Asymmetric VLAN Settings の順にクリックし、次の画面を表示します。

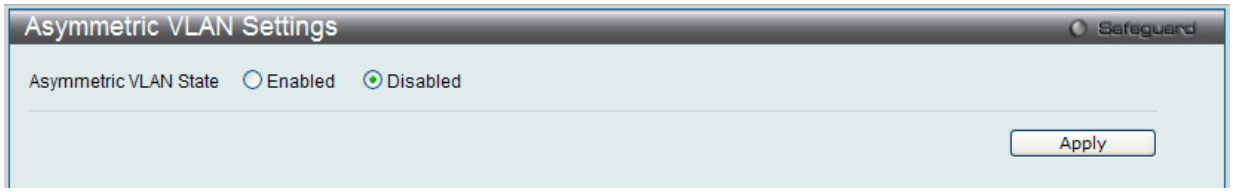


図 8-13　Asymmetric VLAN Settings 画面

「Apply」ボタンをクリックし、設定を適用します。

GVRP（GVRP 設定）

GVRP（Generic Attribute Registration Protocol）は VLAN のメンバ構成情報を、VLAN を使用可能なブリッジ間で自動的に配布します。

GVRP Global Settings（GVRP のグローバル設定）

GVRP タイマは、レイヤ 2 に接続するすべてのデバイスの初期値にある必要があります。GVRP タイマがレイヤ 2 に接続するデバイスで異なる設定がされていると、GVRP アプリケーションはうまく動作しません。GVRP は、各ブリッジにおいて VLAN 構成を登録せずに、VLAN を使用可能なブリッジで自動的に VLAN のポートマッピングを行います。以下の手順で GVRP を設定します。

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

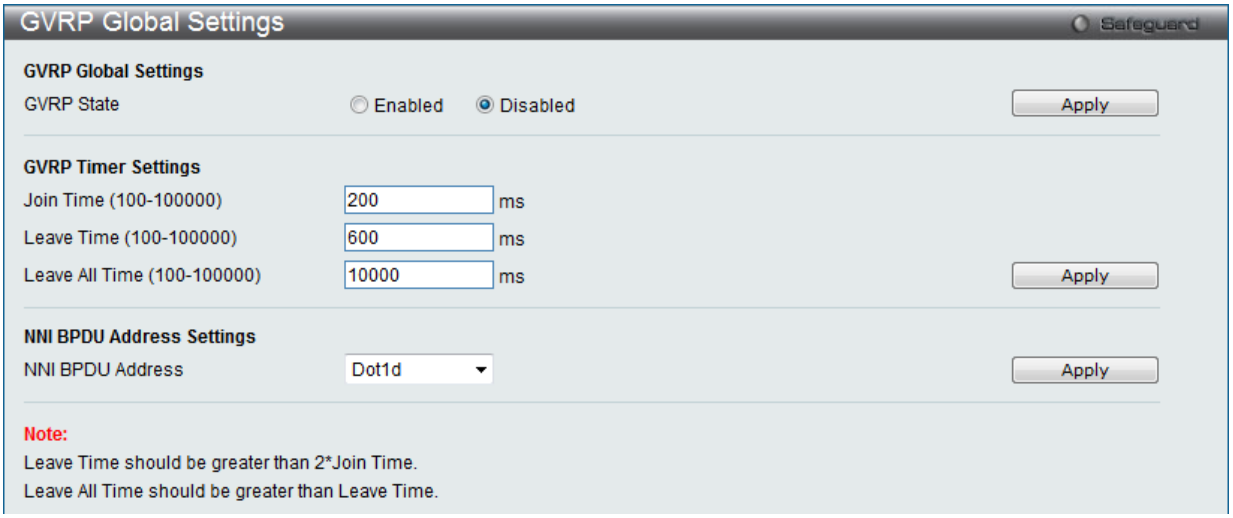


図 8-14　GVRP Global Setting 画面

画面には次の項目があります。

項目	説明
GVRP State	デバイスで GVRP を有効にするかを設定します。 • Enabled - デバイスで GVRP を有効にします。 • Disabled - デバイスで GVRP を無効にします。（初期値）
Join Time（100-100000）	ミリ秒で開始時間を設定します。
Leave Time（100-100000）	ミリ秒で終了時間を設定します。
Leave All Time（100-100000）	ミリ秒で全終了時間を設定します。
NNI BPDU Address	サービスプロバイダの GVRP 用 BPDU プロトコルアドレスを指定します。802.1d GVRP アドレスまたはユーザ定義のマルチキャストアドレスを使用します。ユーザ定義のマルチキャストアドレスの範囲は「0180C2000000 - 0180C2FFFFFF」です。

「Add」ボタンをクリックし、新しいエントリを追加します。

GVRP Port Settings（GVRP のポート設定）

GVRP のポート設定を行います。

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

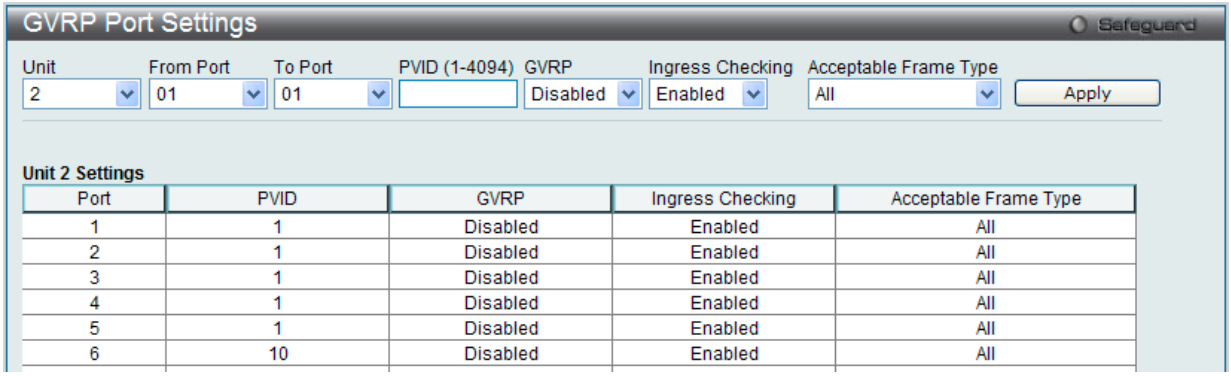


図 8-15　GVRP Port Setting 画面

画面には以下の項目があります。

項目	説明
Unit	GVRP パラメータを表示するスタックメンバのユニット ID を設定します。
From Port	表示する GVRP が設定されたポートの最初の番号を設定します。
To Port	表示する GVRP が設定されたポートの最後の番号を設定します。
PVID（1-4094）	ポートに割り当てられた現在の PVID を設定します。 VLAN に PVID を手動で割り当てます。初期値では全てのポートは初期値の VLAN に「VID1」と共に割り当てられます。PVID は送信タグ、タグ無しパケット、そして受信パケットのフィルタリングを決定します。指定のポートがタグフレームのみを受け入れる設定の場合、そしてタグ無しパケットは送信のためのポートに転送される場合、ポートはタグに VID を書き込む PVID を使用して、802.1Q タグを追加します。 パケットが宛先に着くと、受領した機器が PVID を使用して VLAN 転送の決定を行います。ポートがパケットを受領し Ingress フィルタリングが有効の場合、ポートは受領パケットの VID とポートの PVID を比較します。もし双方が同等でない場合、パケットはポートにより破棄されます。同等の場合はポートはパケットを受領します。
GVRP	GVRP が各ポートで有効かどうかを設定します。 • Enabled - 選択したポートで GVRP を有効にします。 • Disabled - 選択したポートで GVRP を無効にします。（初期値）
Ingress Checking	デバイスでイングレスチェックを有効にするかを設定します。 • Enabled - デバイスでイングレスチェックを有効にします。イングレスチェックにより、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 - デバイスでイングレスチェックを無効にします。
Acceptable FrameType	ポートが受け入れるパケットの種類を設定します。 • Tagged_Only - タグ付きパケットのみポートは受け入れます。 • Admit_All - タグ付き、タグなし両方のパケット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）

本テーブルを使用して、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。

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

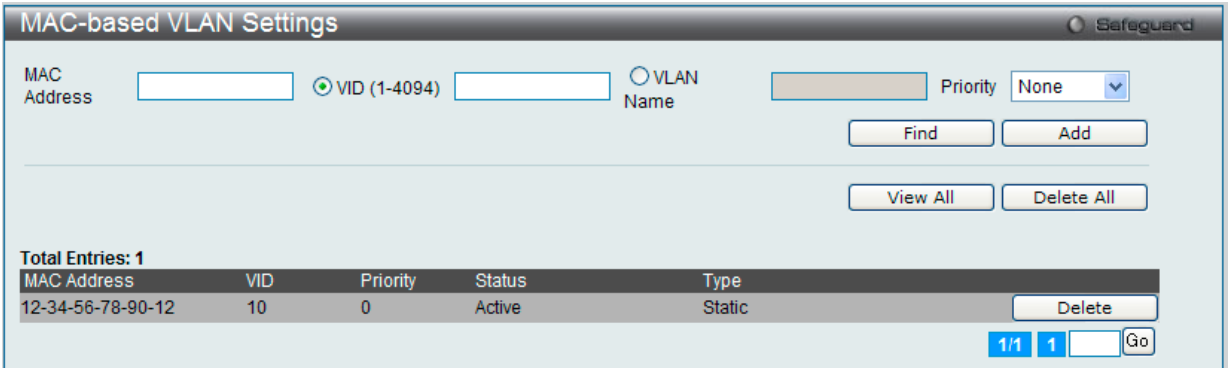


図 8-16　MAC-based VLAN Settings 画面

以下の項目を使用して、設定します。

項目	説明
MAC Address	MAC アドレスを入力します。
VID（1-4094）	作成済みの VLAN の VLAN ID を入力します。
VLAN Name	作成済みの VLAN の VLAN 名を指定します。
Priority	タグなしパケットにアサインする優先度を設定します。

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 を作成します。プライベート VLAN は、VLAN のレイヤ 2 ブロードキャストドメインをサブドメインに分割して、各カスタマに固有の VLAN を割り当てる必要があるサービスプロバイダに特に便利です。各サブドメインは、プライマリおよびセカンダリの VLAN からなる各プライベート VLAN のペアと共に数個のプライベート VLAN のペアで構成されます。プライベート VLAN のドメインにある VLAN のペアのすべてが同じプライマリ VLAN のメンバです。各サブドメインは、セカンダリ VLAN ID を使用して識別されます。

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。

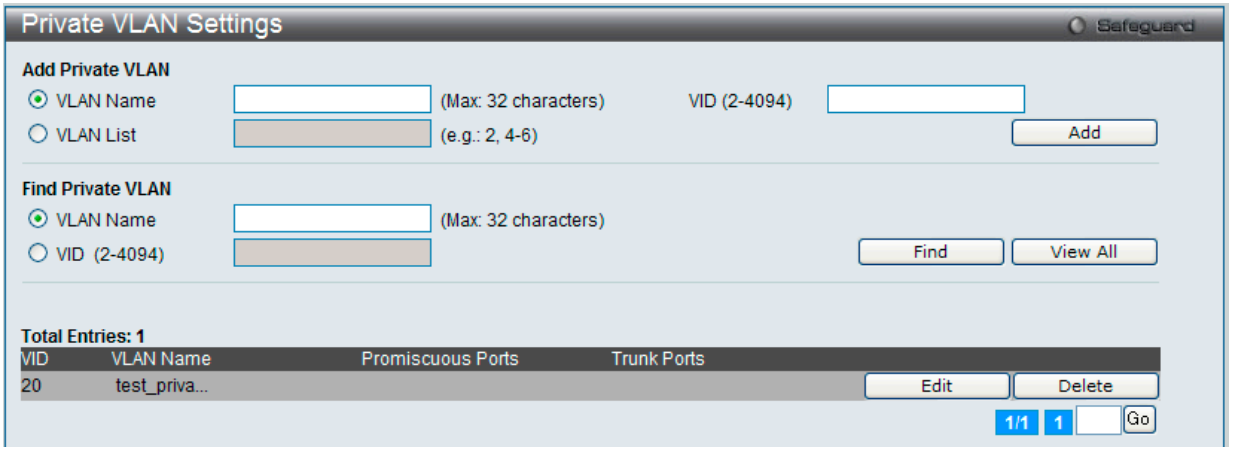


図 8-17　Private VLAN Settings 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Name	VLAN 名を指定します。
VID（2-4094）	VLAN ID を入力します。
VLAN List	VLAN の VLAN ID のリストを指定します。

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

「Edit」ボタンをクリックすると以下の画面が表示されます。

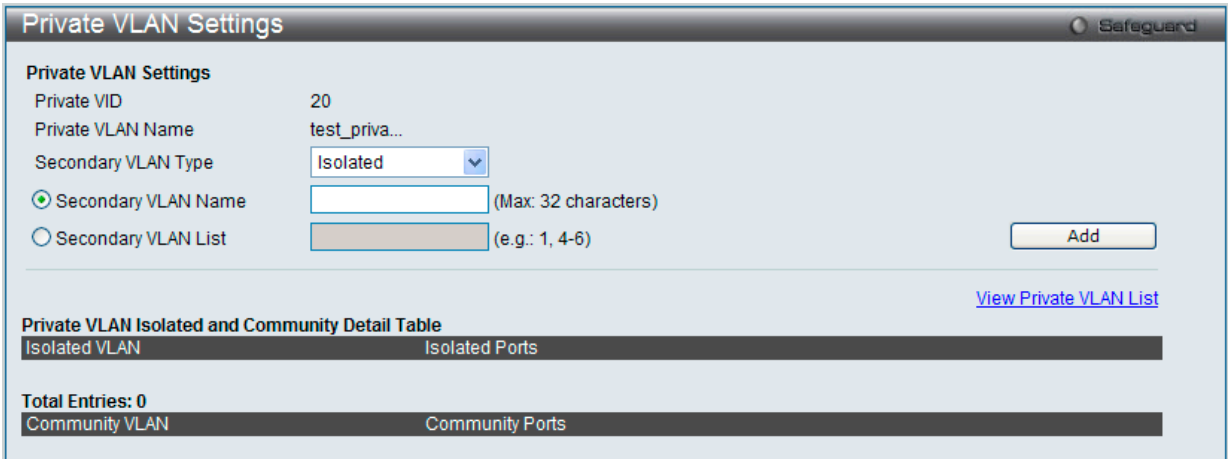


図 8-18　Private VLAN Settings - Edit 画面

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 のタイプを選択します。以下のオプションが利用できます。 • Isolated - Isolated VLAN は、ポートに接続しているすべてのホストがレイヤ 2 で隔離されるという異なる特性を持つセカンダリ VLAN です。Isolated VLAN の第一の長所は、プライベート VLAN が 2 つの VLAN 識別子を使用するだけでポートの分離を行い、多くのエンドユーザにサービスを提供することができるということです。プライベート VLAN は、1 つの Isolated VLAN のみサポートしています。 • Community - コミュニティ VLAN は、信頼関係を持つエンドデバイスの特定の「コミュニティ」に接続するポートグループに関連付けるセカンダリ VLAN です。プライベート VLAN ドメインには、複数の異なるコミュニティ VLAN が存在することができます。
Secondary VLAN Name	プライベート VLAN 名を指定する場合、「Secondary VLAN Name」をチェックします。隣接する欄にセカンダリ VLAN の名前を入力します。
Secondary VLAN List	セカンダリ VLAN の範囲を指定する場合、「Secondary VLAN List」をチェックします。隣接する欄にセカンダリ VLAN として追加する VID または VID の範囲を入力します。

新規にプライベート VLAN エントリを登録する場合には、「Add」ボタンをクリックします。

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。

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

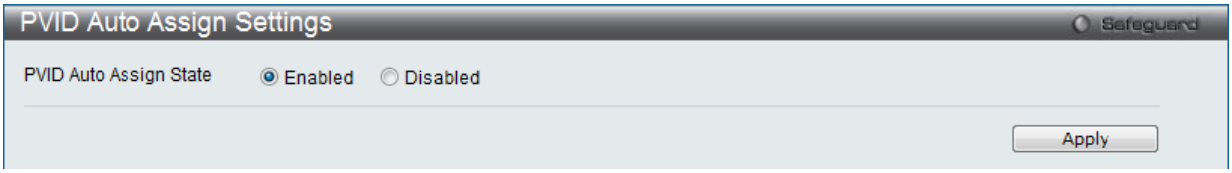


図 8-19　PVID Auto Assign Settings 画面

「Apply」ボタンをクリックし、デバイスに設定を適用します。

Voice VLAN（音声 VLAN）

Voice VLAN は IP 電話からの音声トラフィックを送信する上で使用される VLAN です。IP 電話の音声品質が劣化するなどの理由から音声トラフィックの QoS を通常のトラフィックより優先的に送信されるように設定します。
送信元の MAC アドレスから受信したパケットが音声パケットであると判断します。パケットの送信元 MAC アドレスが OUI アドレスだとシステムが認識した場合、パケットは音声 VLAN に送信された音声パケットであると判断されます。

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

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。

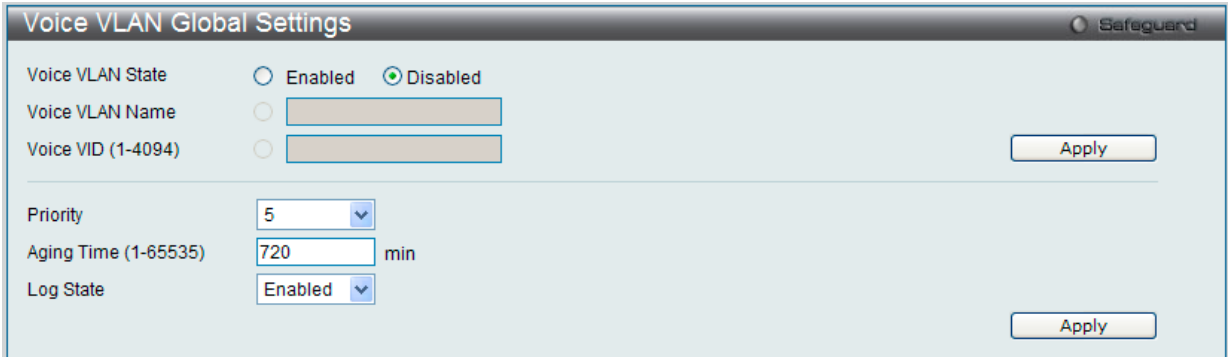


図 8-20　Voice VLAN Global Settings 画面

以下の項目を使用して、設定します。

項目	説明
Voice VLAN State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Voice VLAN Name	選択をして音声 VLAN の名前を入力します。
Voice VID (1-4094)	選択をして音声 VLAN の VLAN ID を入力します。
Priority	プルダウンメニューを使用して音声 VLAN の優先度を設定します。音声 VLAN 優先度はデータトラフィック中の音声トラフィックの QoS を判別する上で使用されます。範囲は 0-7 の間で設定できます。初期値は 5 です。
Aging Time (1-65535)	ポートが自動 VLAN の一部の場合、音声 VLAN からポートを削除するまでの時間を設定します。最新の音声機器がトラフィックを送信しなくなり、音声機器の MAC アドレスが期限切れになると、音声 VLAN タイマは開始されます。ポートは音声 VLAN タイマの時間切れのあと、音声 VLAN から削除されます。
Log State	プルダウンメニューを使用して、音声 VLAN の Log 機能を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、デバイスに設定を適用します。

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

音声 VLAN のポート設定を行います。

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。

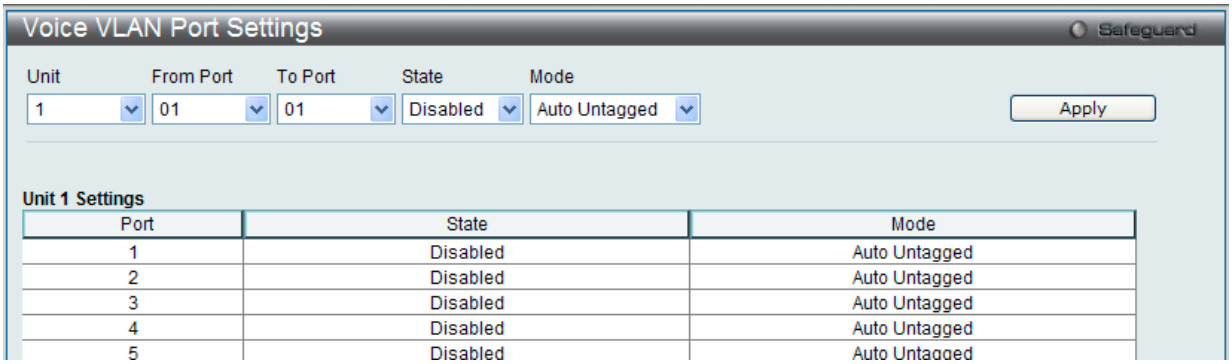


図 8-21　Voice VLAN Port Settings 画面

以下の項目を使用して、設定します。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	音声 VLAN を設定するポートの範囲を設定します。
State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Mode	「Auto」か「Manual」で設定します。「Auto」で設定した場合、ポートは自動的に音声 VLAN の一部として設定されます。受信パケットの MAC アドレスが設定した OUI アドレスを一致した場合、ポートは自動的に音声 VLAN の一部であると認識されます。自動認識はタイマ設定で削除されます。「Manual」モードに設定した場合、802.1Q VLAN 設定コマンドを使用して、ポートは手動で音声 VLAN の一部として追加 / 削除する必要があります。

「Apply」ボタンをクリックし、デバイスに設定を適用します。

Voice VLAN OUI Settings（音声 VLAN OUI 設定）

ユーザ設定音声トラフィックの OUI を設定します。OUI は事前に設定済みのものがありますので、ユーザが手動で OUI を設定する場合、事前に設定されている下記の OUI は避けて設定する必要があります。

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。

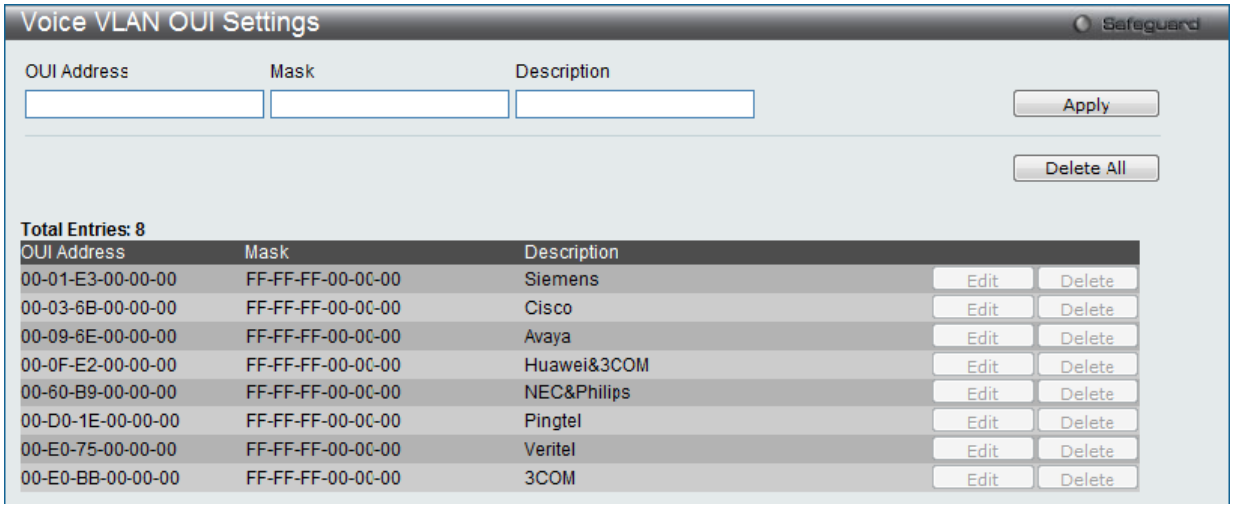


図 8-22　Voice VLAN OUI Settings 画面

以下の項目を使用して、設定します。

項目	説明
OUI Address	OUI MAC アドレスを入力します。
Mask	OUI MAC アドレスマスクを入力します。
Description	設定する OUI についての説明を入力します。

「Apply」ボタンをクリックし、デバイスに設定を適用します。

Voice VLAN Device（音声 VLAN 機器）

各スイッチポートに接続中の音声 VLAN が使用可能なデバイスを表示します。

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。

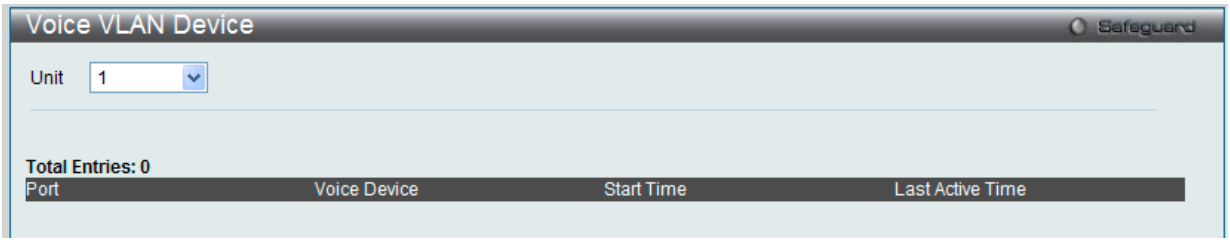


図 8-23　Voice VLAN Device 画面

Voice VLAN LLDP-MED Voice Device（音声 VLAN LLDP-MED 音声機器）

LLDP-MED で検出された音声バイスを表示します。

L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Voice 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。

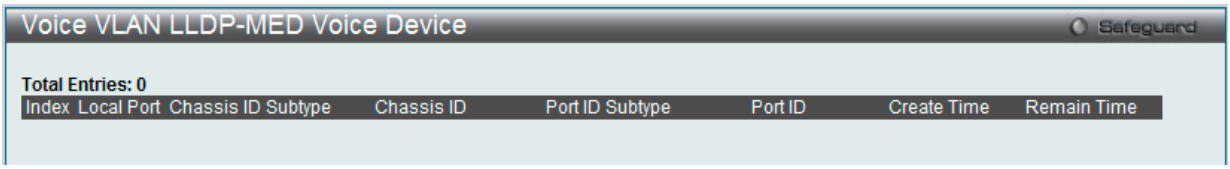


図 8-24　Voice VLAN LLDP-MED Voice Device 画面

Surveillance VLAN（サーベイランス VLAN）

Surveillance VLAN Global Settings（サーベイランス VLAN グローバル設定）

サーベイランス VLAN は、サーベイランスデバイスからビデオトラフィックを送信するのに使用される VLAN です。サーベイランス VLAN グローバル設定を行います。

L2 Features > VLAN > Surveillance VLAN > Surveillance VLAN 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。

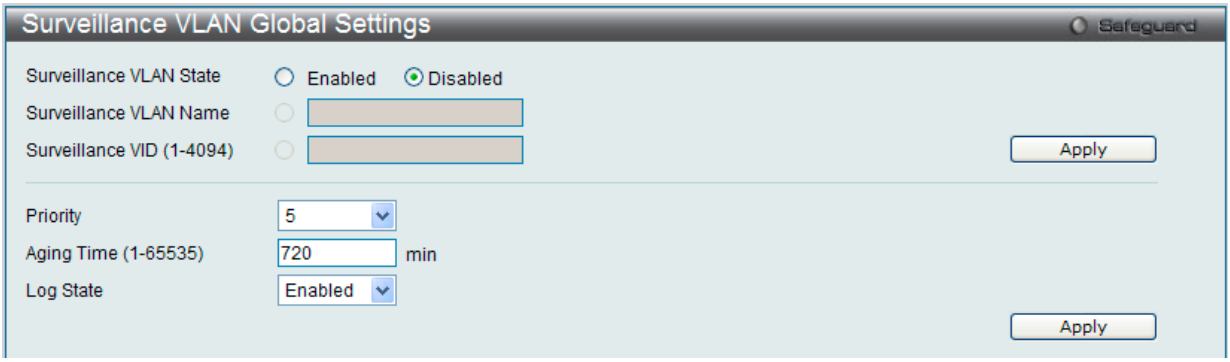


図 8-25　Surveillance VLAN Global Settings 画面

以下の項目を使用して、設定します。

項目	説明
Surveillance VLAN State	サーベイランス VLAN の状態。
Surveillance VLAN Name	サーベイランス VLAN の名前。
Surveillance VID (14094)	サーベイランス VLAN の VLAN ID。
Priority	サーベイランス VLAN の優先度（0-7）。優先度の初期値は 5 です。
Aging Time (1-65535)	エージングタイム（1-65535 分）。 初期値は 720（分）です。 エージングタイムは、ポートがオートサーベイランス VLAN メンバである場合にサーベイランス VLAN からポートを削除するために使用されます。最後のサーベイランスデバイスが、トラフィックの送信を止めて、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。 サーベイランス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	サーベイランス VLAN ログの送信を有効または無効にします。

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

Surveillance VLAN Port Settings（サーベイランス VLAN ポート設定）

ポートのサーベイランス VLAN 情報を表示します。

L2 Features > VLAN > Surveillance VLAN > Surveillance VLAN Port Setting 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。

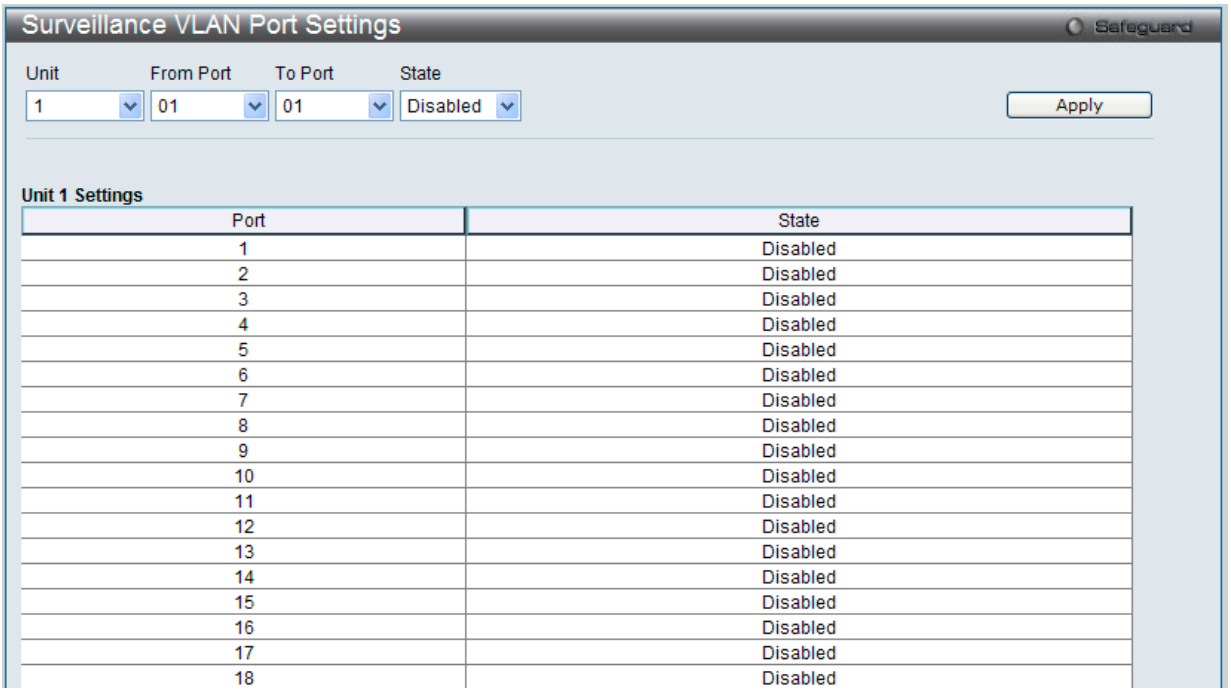


図 8-26　Surveillance VLAN Port Settings 画面

以下の項目を使用して、設定します。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	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。
State	ポートの状態を有効または無効にします。

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

Surveillance VLAN OUI Settings（サーベイランス VLAN OUI 設定）

ユーザ定義のサーベイランストラフィックの OUI を設定します。OUI はサーベイランス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 がありますが、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 > Surveillance VLAN > Surveillance VLAN OUI 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。

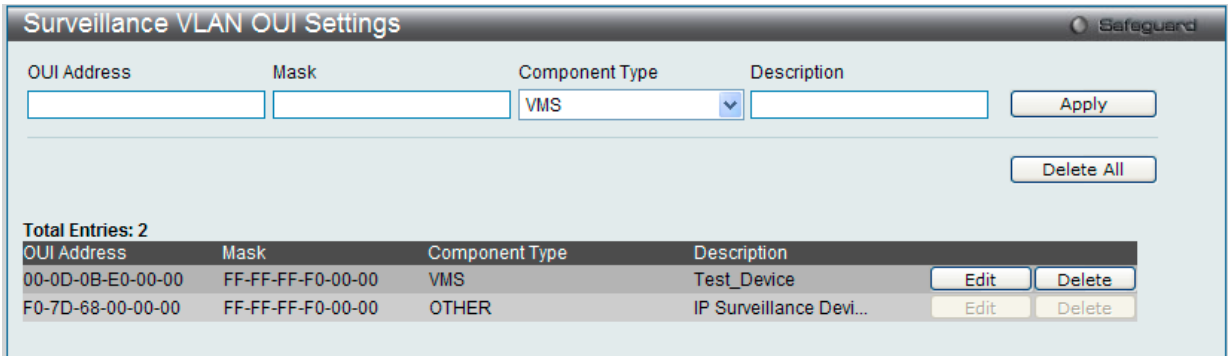


図 8-27　Surveillance VLAN OUI Settings 画面

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。
Component Type	プルダウンメニューを使用して、サーベイランス VLAN が自動検出可能なサーベイランスコンポーネントを選択します。選択可能項目は次の通りです。: VMS、VMS_CLIENT、VIDEO_ENCODER、NETWORK_STORAGE、および OTHER
Description	ユーザ定義 OUI に関する説明文。

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

「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。

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。

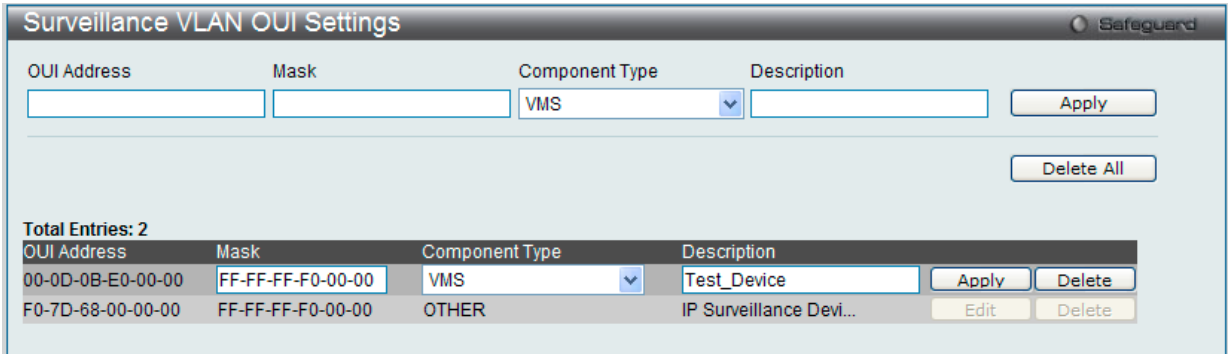


図 8-28　Surveillance VLAN OUI Settings 画面 - 編集

編集後、「Apply」ボタンをクリックします。

Surveillance VLAN Device（サーベイランス VLAN デバイス）

ポートに接続するサーベイランスデバイスを表示します。

L2 Features > VLAN > Surveillance VLAN > Surveillance VLAN Device 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。

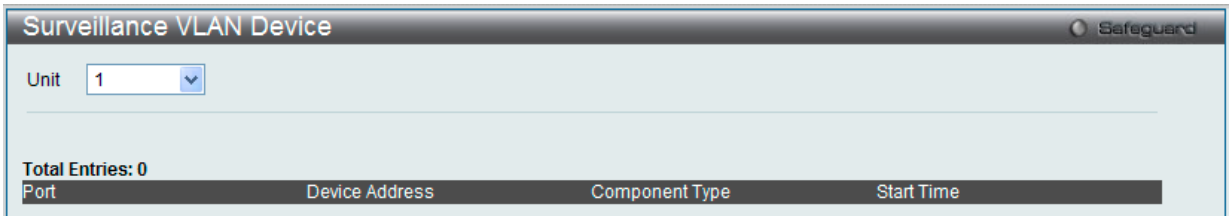


図 8-29　Surveillance VLAN Device 画面

「Start Time」はデバイスがこのポートで検出された時間です。また、アクティベート時間はデバイスが最も最近トラフィックを送信した時間です。

VLAN Trunk Settings（VLAN トランク設定）

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

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。

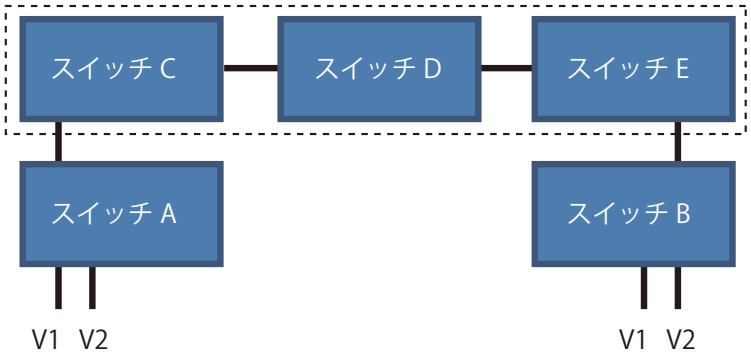


図 8-30　Private VLAN Settings 画面

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

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

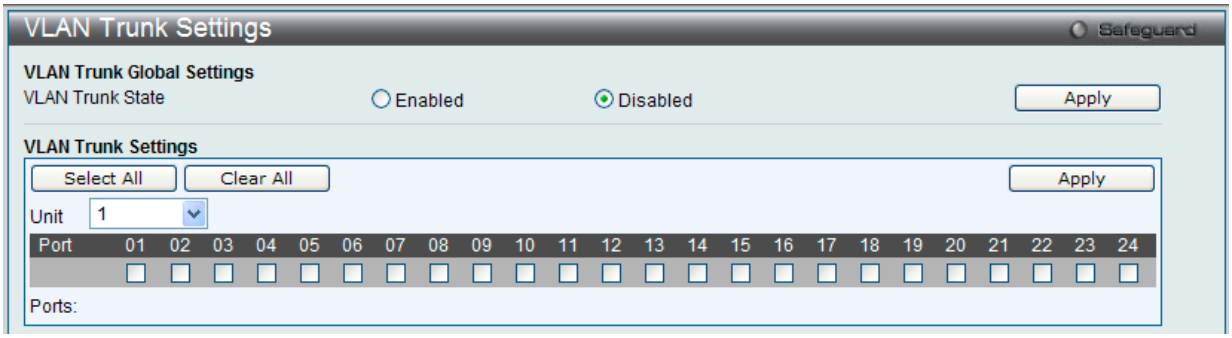


図 8-31　VLAN Trunk Settings 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Trunk State	VLAN トランクのグローバル設定を行います。
Unit	設定するユニットを指定します。
Ports	設定するポートを指定します。「Select All」ボタンをクリックして全てのポートを選択します。「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。

「Apply」ボタンをクリックし、デバイスに設定を適用します。

Browse VLAN（VLAN の参照）

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 の順にメニューをクリックし、以下の画面を表示します。

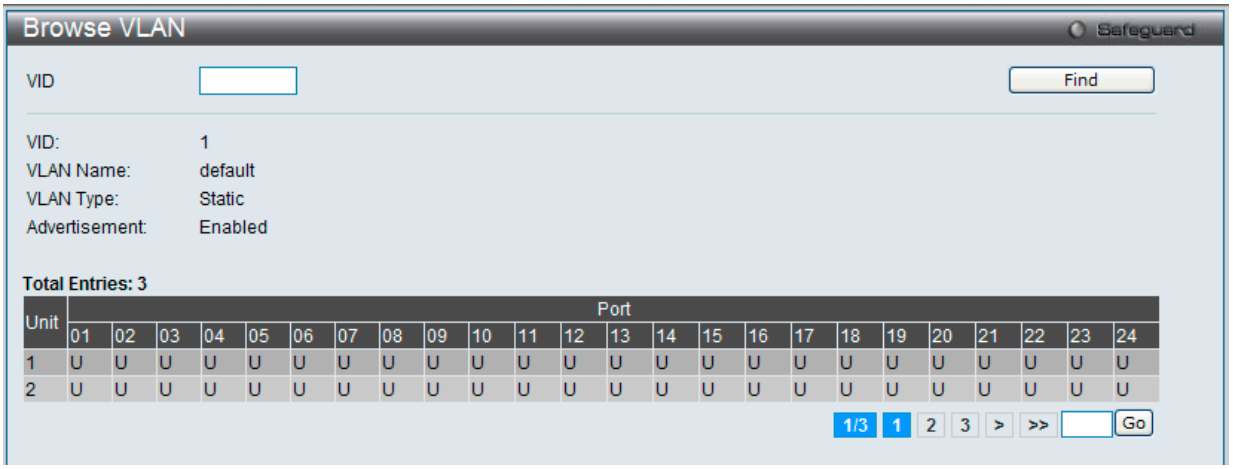


図 8-32　Browse VLAN 画面

Show VLAN Ports（VLAN ポートの表示）

スイッチの各ポートの VLAN ポートを VLAN ID ごとに表示します。ポートかポートリストを画面上部の項目に入力し、「Find」をクリックします。

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

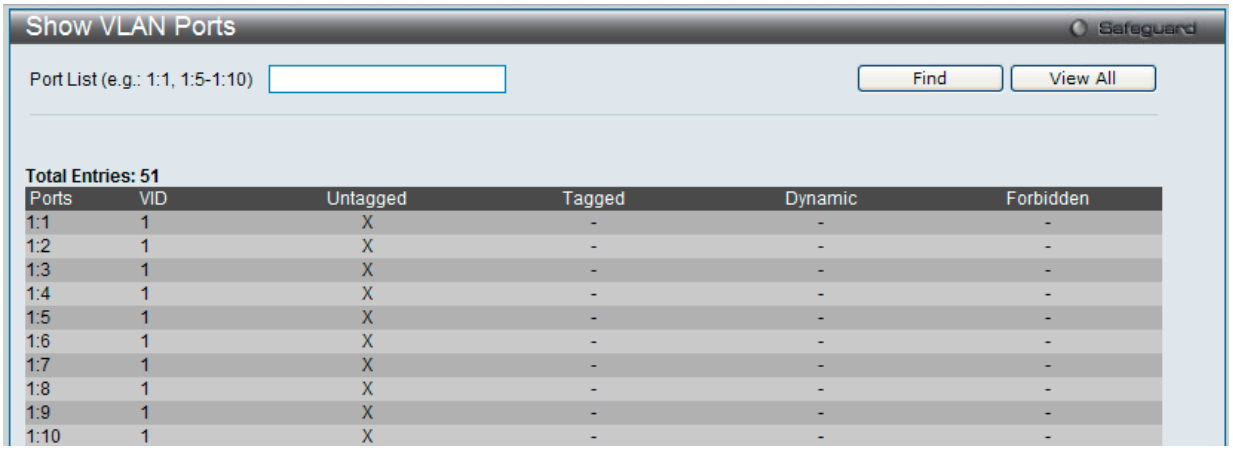


図 8-33　Show VLAN Ports 画面

QinQ（QinQ 設定）（EI モードのみ）

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。

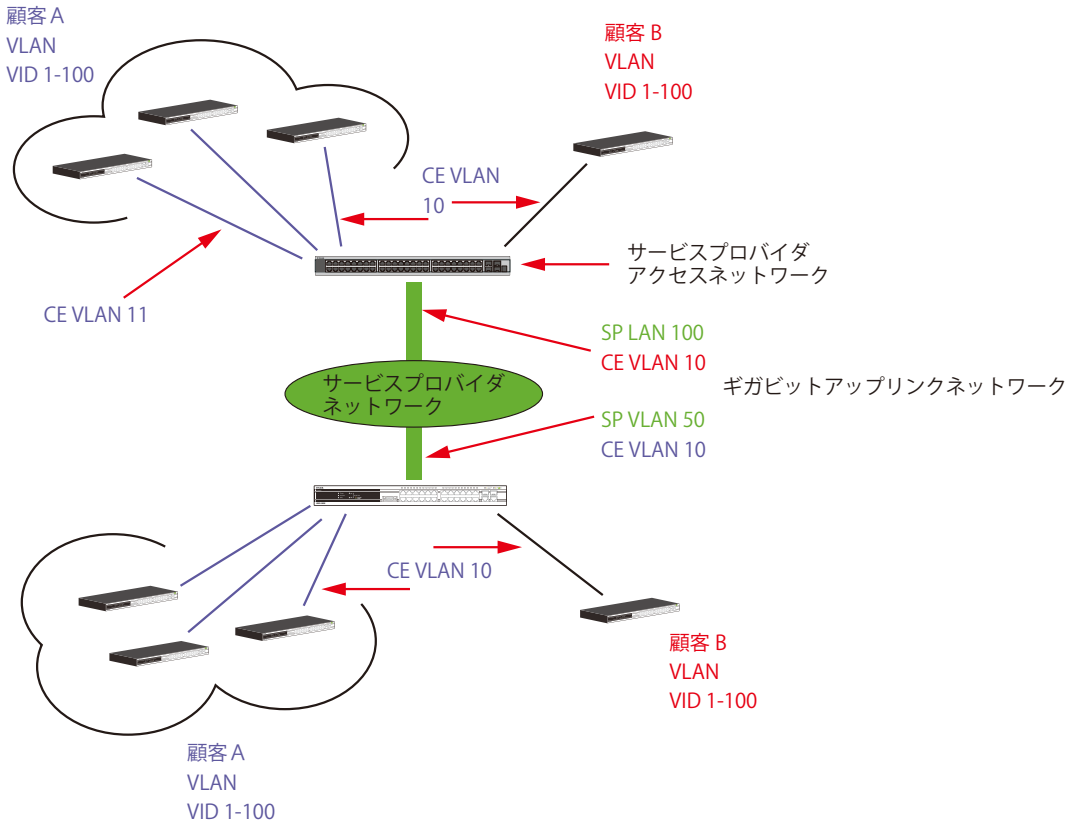


図 8-34　ダブル VLAN を使用したネットワーク例

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）

QinQ のパラメータを設定します。

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

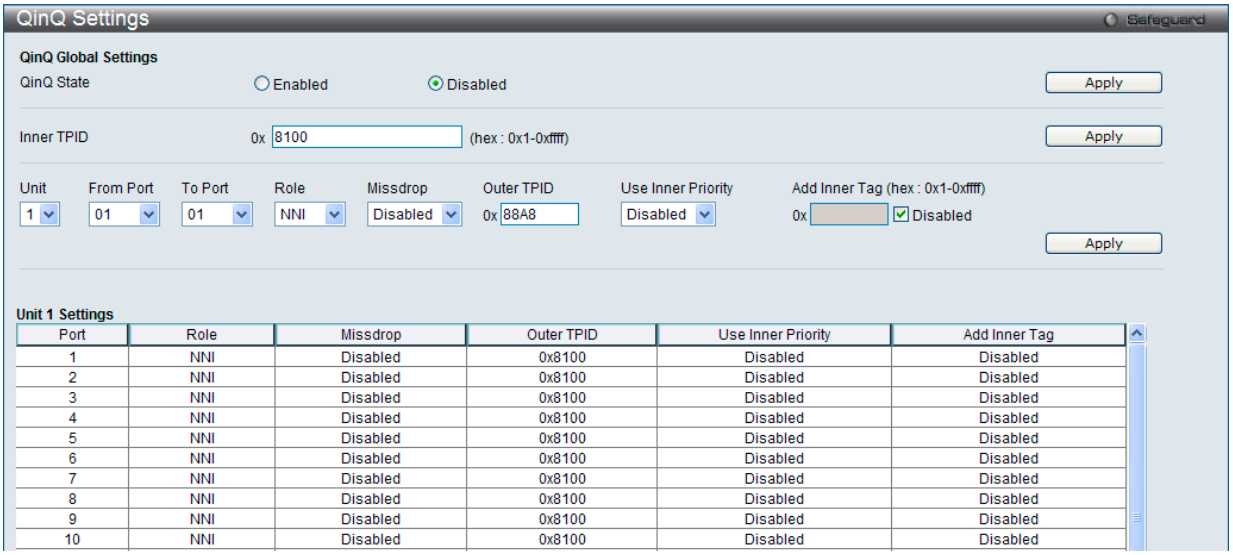


図 8-35　QinQ Settings 画面

以下の項目を使用して設定します。

項目	説明
QinQ State	QinQ 機能をグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
Inner TPID	SP-VLAN タグに Inner TPID を入力します。
Unit	設定するユニットを指定します。
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 - パケットは送信され、S-VLAN 割当て方式に基づく S-VLAN に割り当てられます。
Outer TPID	SP-VLAN タグに Outer TPID を入力します。
Use Inner Priority	S-VLAN タグの優先度として C-VLAN タグの優先度を使用するかどうかを指定します。初期値では「Disabled」が選択されています。
Add Inner Tag	インナータグをエントリに追加する / しないを設定します。初期値は「しない」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。

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

C-VLAN と SP-VLAN 間の変換関係を追加します。

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

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

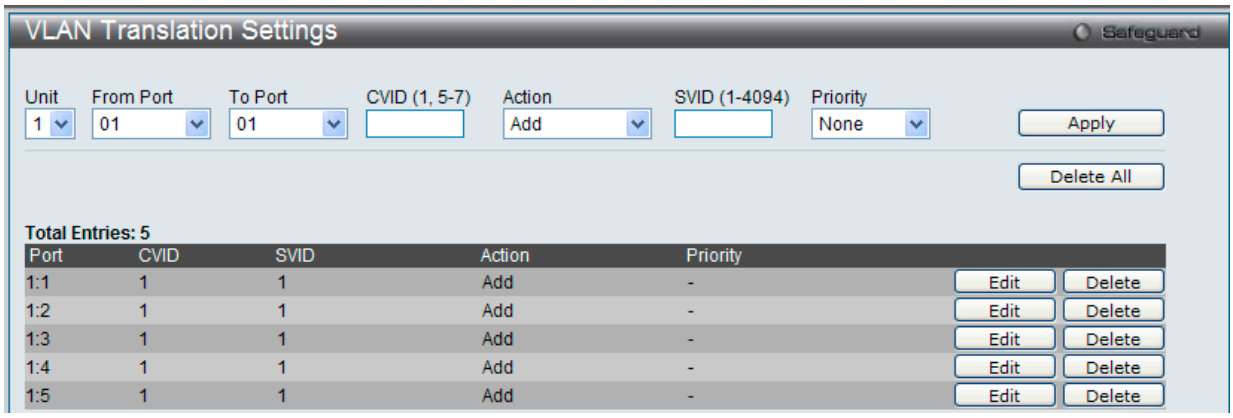


図 8-36　VLAN Translation Settings 画面

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

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

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。

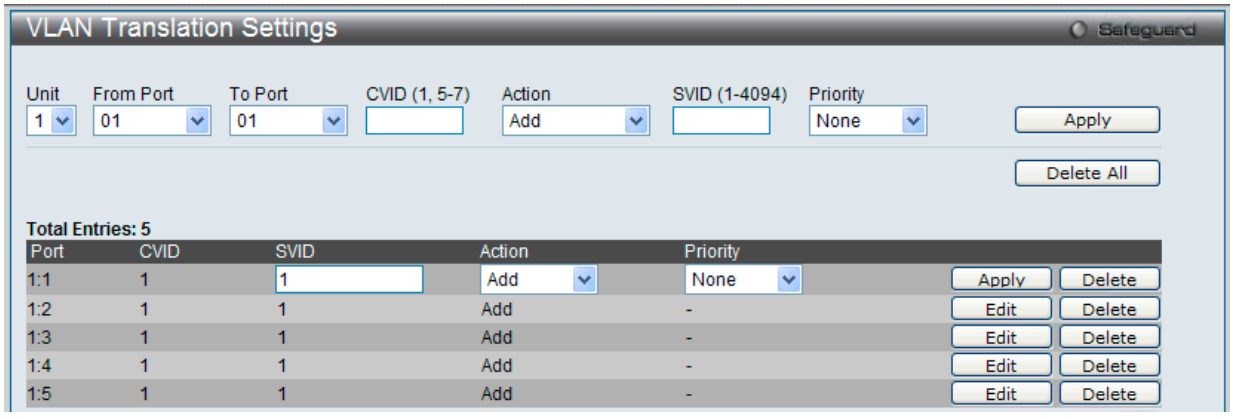


図 8-37　VLAN Translation Settings 画面 - Edit

「Apply」ボタンをクリックし、設定を適用します。

エントリの削除

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

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

レイヤ 2 プロトコルトンネリングポートを設定します。

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

図 8-38　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。
Unit	設定するユニットを選択します。
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、新しいエントリを追加します。

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（802.1D-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 Rapid STP、802.1Q-2005 MSTP それぞれの設定方法についても、本章中に記述します。

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。

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、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 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 7-3 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。

表 7-3　ポート状態の比較

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

RSTP では、タイマの設定への依存をやめ、フォワーディング状態への急速な遷移が可能になりました。RSTP 準拠のブリッジは他の RSTP に準拠するブリッジリンク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 間の互換性

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 をグローバルに設定します。

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。

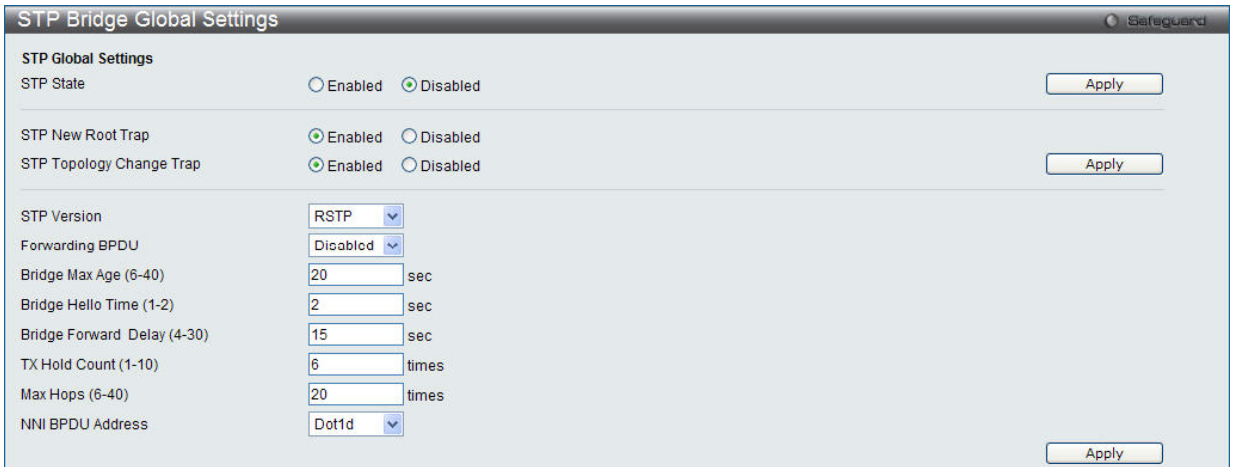


図 8-39　STP Bridge Global Settings 画面

「STP Status」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。STP バージョンと対応する設定オプションの説明は、以下のテーブル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。

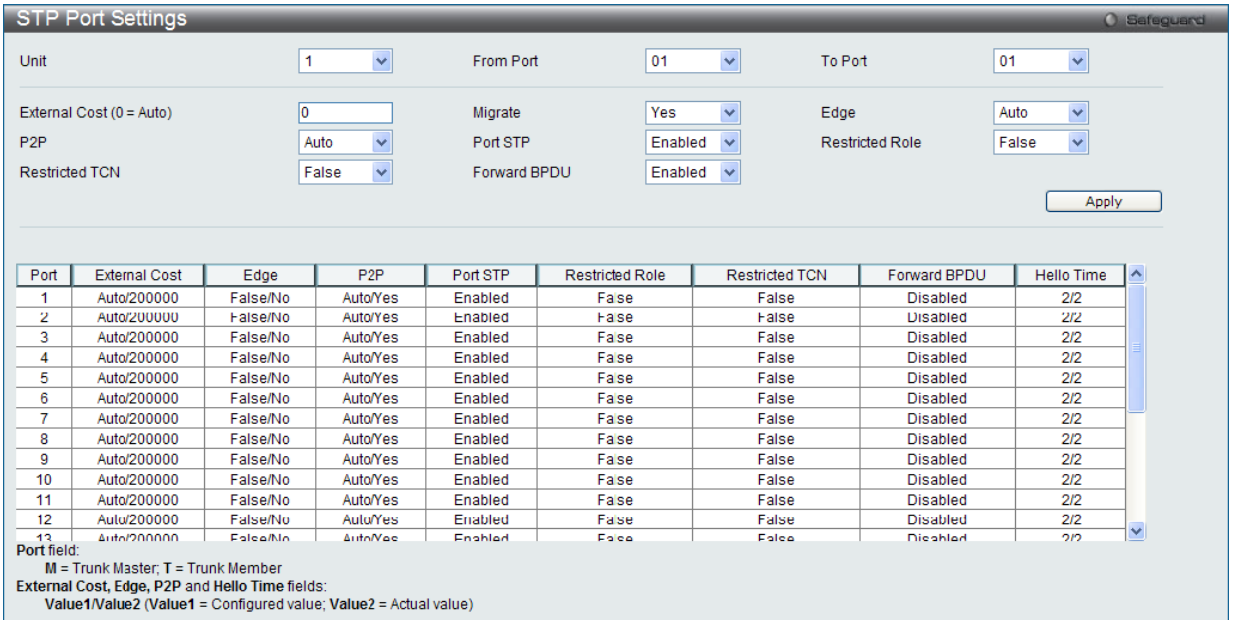
項目	説明
STP State	STP をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
STP new Root Trap	新しいルートトラップ送信の有効 / 無効を設定します。
STP Topology Change Trap	トポロジ変更トラップ送信の有効 / 無効を設定します。
STP Version	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。 • MSTP - スイッチ上で MSTP がグローバルに使用されます。
Forwarding BPDU	「Enabled」（有効）または「Disabled」（無効）にします。「Enabled」にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は「Disabled」です。
Bridge Max Age (6-40)	本項目は、古い情報がネットワーク内の冗長パスを永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40（秒）の範囲から値を指定します。初期値では 20（秒）が指定されています。
Bridge Hello Time (1-2)	ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために BPDU パケットを 2 回送信します。本値は、1 回目の送信と 2 回目の送信との間の時間です。STP または RSTP が「STP Version」で選択された場合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	サービス提供サイトにおける STP の BPDU プロトコルアドレス（「Dot1d」または「Dot1ad」）を決定します。802.1d STP アドレス、または 802.1ad サービスプロバイダの STP アドレスを使用します。

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

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
11	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
12	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
13	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2

図 8-40　STP Port Setting 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。

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port	連続するポートグループの最初の番号を設定します。
To Port	連続するポートグループの最後の番号を設定します。
External Cost (0=Auto)	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。ポートのコストは自動か、メトリックの値で設定します。初期値は 0（Auto）です。 • 0（Auto）- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。 ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。 • 値 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほどパケット転送は頻繁に行われるようになります。
P2P	P2P ポートとするかどうかを設定します。初期値は「Auto」です。 • True - P2P（point-to-point）ポートとしてリンクを共有します。P2P ポートはエッジポートと似ていますが、P2P ポートは全二重でなくてはならないという制限があります。P2P ポートはエッジポートのように RSTP による高速な転送状態の変更が可能です。 • False - ポートは P2P ポートではなくなります。 • Auto - 可能であれば常に True と同様の P2P 状態になるように設定します。ポートが、例えば強制的に半二重になるなど状態を維持できない場合には、False と同様の状態になります。
Restricted TCN	TCN（Topology Change Notification）は、トポロジ変化を信号で伝えるために、ブリッジがそのルートポートに送信するシンプルな BPDU です。「True」と「False」を切り替えます。「True」に設定すると、受信した TCN とトポロジ変化を他のポートに伝えることをやめます。初期値は「False」です。
Migrate	RSTP モードの時に「Yes」にするとポートが RSTP BPDU を送信するようになります。
Port STP	ポートグループでの STP の「Enabled」（有効）/「Disabled」（無効）を設定します。初期値は「Enabled」です。
Forward BPDU	STP が無効である場合に、BPDU パケットの転送を「Enabled」（有効）または「Disabled」（無効）にします。
Edge	選択したポートをエッジポートとするかどうかを指定します。 • True - ポートはエッジポートになります。エッジポート自体はループを発生させることはありませんが、トポロジの変化によりループの可能性が生じると、エッジポートはエッジポートではなくなります。エッジポートは通常 BPDU パケットを受信しません。BPDU パケットを受信すると自動的にエッジポートではなくなります。 • False - ポートはエッジポートではなくなります。 • Auto - 自動。
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設定されることはありません。初期値は「False」です。

「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）

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

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

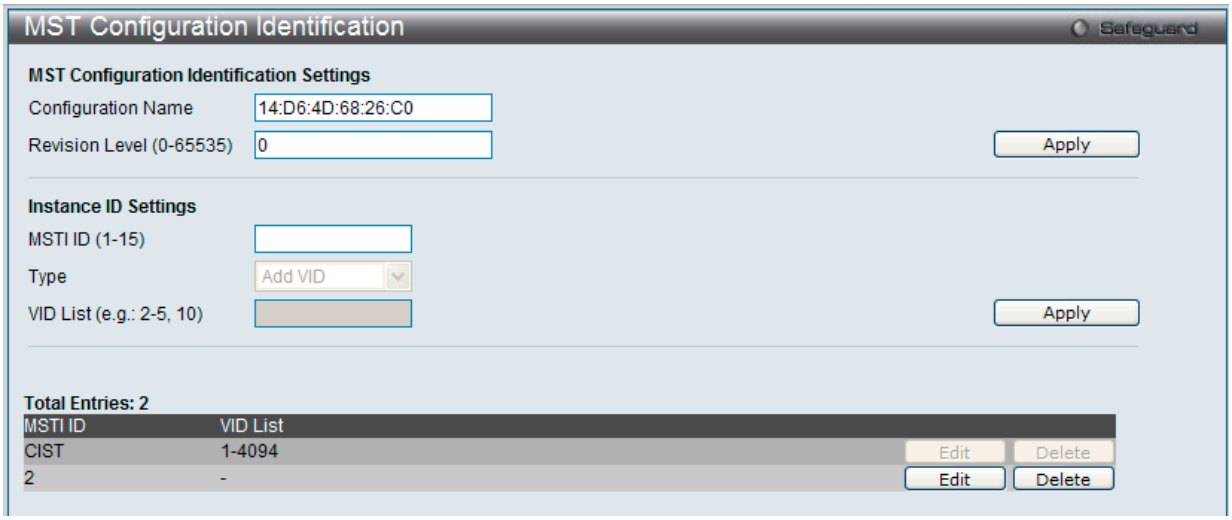


図 8-41　MST Configuration Identification 画面

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 MST リージョンの値を設定します。Configuration Name に同期しています。
MSTI ID	1-15 の番号を入力し、スイッチに新しい MSTI を設定します。
Type	MSTI に行う変更を選択します。 • Add VID - VID List 項目に指定された VID を MSTI ID に追加します。 • Remove VID - VID List 項目に指定された VID を MSTI ID から削除します。
VID List (1-4094)	この MSTI ID に設定する VLAN の 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。

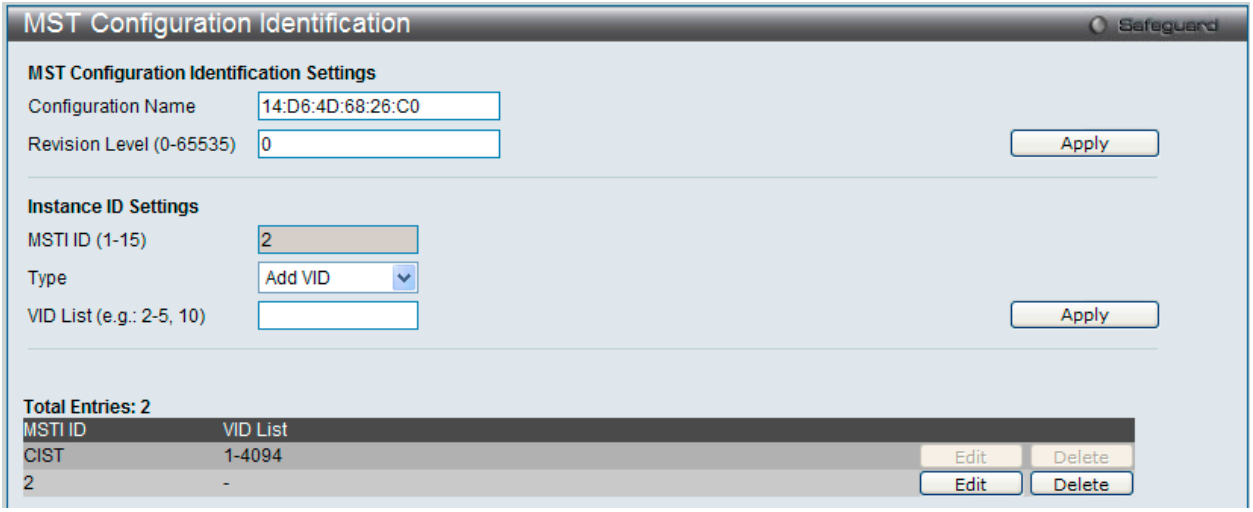


図 8-42　MST Configuration Identification 画面 - Edit

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。

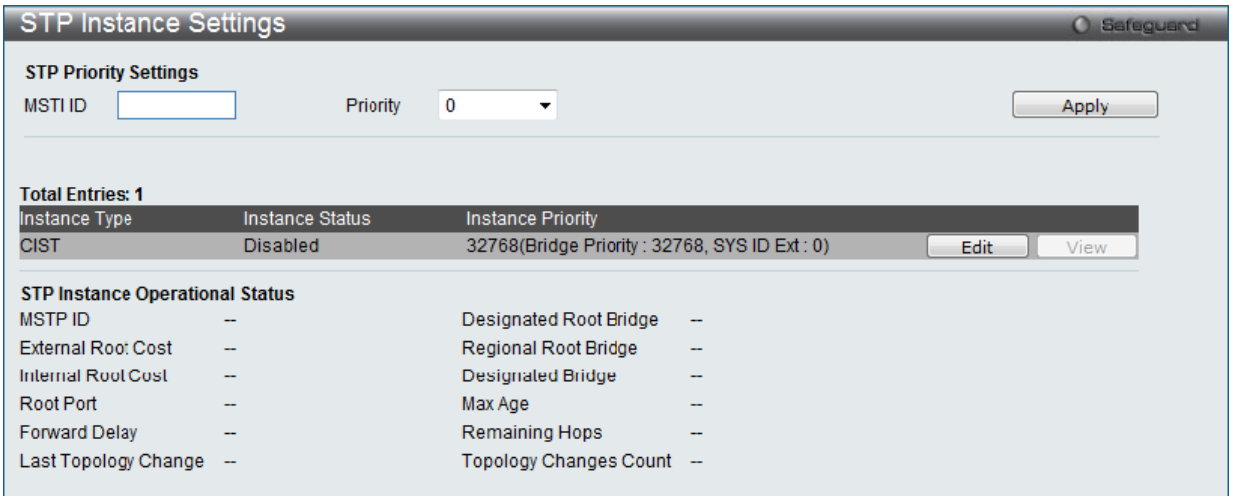


図 8-43　STP Instance Settings 画面

エントリの編集

編集するエントリ横の「Edit」ボタンをクリックし、エントリの編集を行います。

エントリの詳細情報の参照

エントリの詳しい情報の参照は、参照するエントリ横の「View」ボタンをクリックします。

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 を表します。初期値は MSTI です。
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。

MSTP Port Information（MSTP ポート情報）

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

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

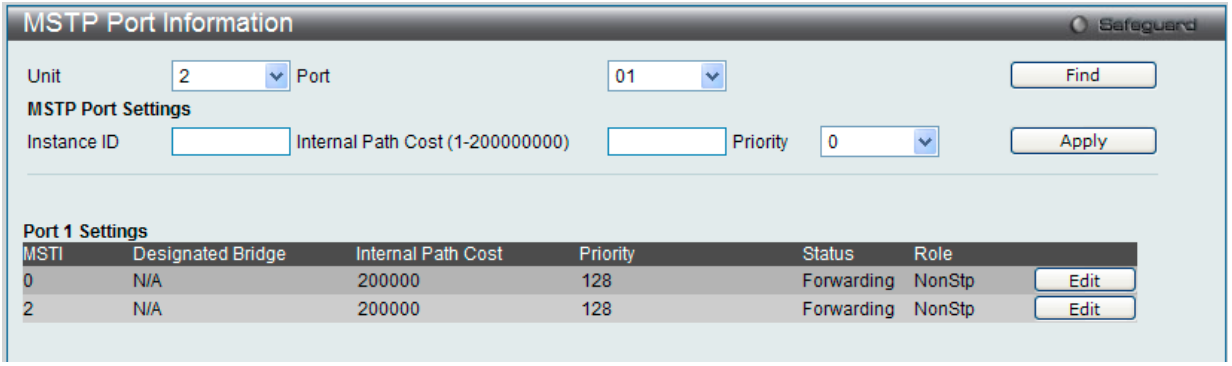


図 8-44　MSTP Port Information 画面

本画面には以下の情報があります。

項目	説明
Unit	設定するユニットを選択します。
Port	プルダウンメニューを使用して、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。初期値は 0（自動）。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。 • 値 1-200000000 - 最も速い経路、最適なルートを設定します。低いコストを指定するほど速い転送となります。200000 固定となっています。
Priority	ポートインタフェースのプライオリティとして 0 から 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。

「Apply」ボタンをクリックし、新しい設定を適用します。

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。

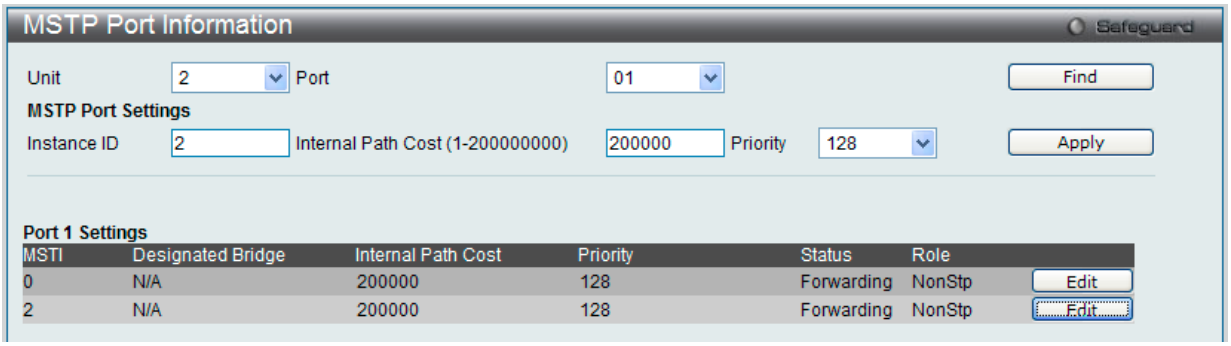


図 8-45　MSTP Port Information 画面 - Edit

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。

Link Aggregation（リンクアグリゲーション）

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、複数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。スイッチは 2 から 8 のポートを束ねた 32 個までのトランクグループをサポートします。この機能により最大 8000Mbps の通信速度が実現されます。

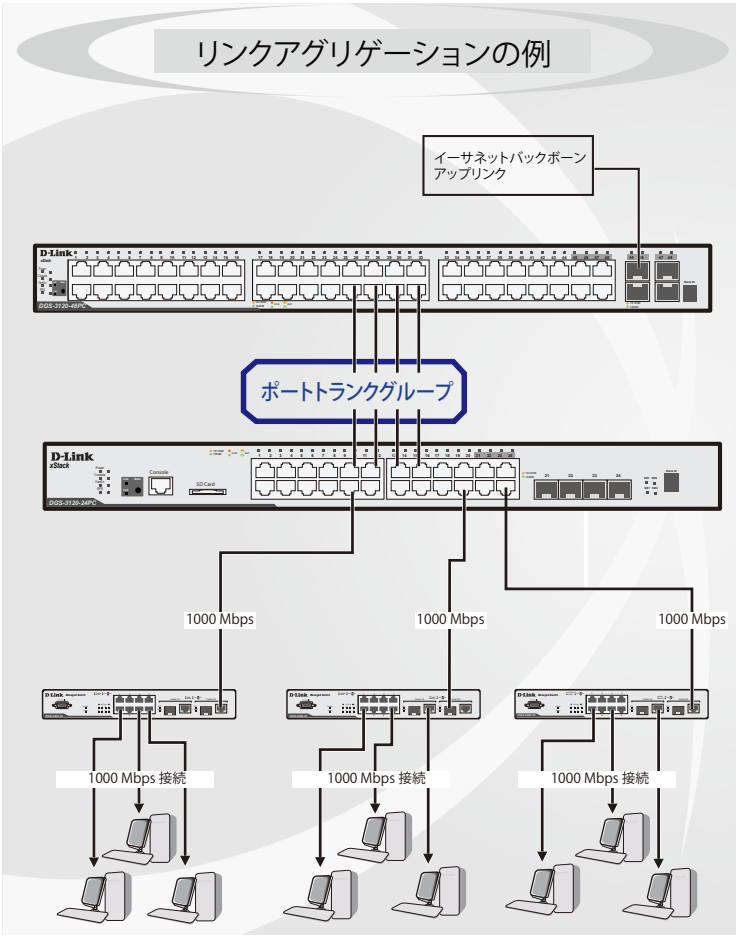


図 8-46　ポートトランクグループの例

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。

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。

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 32 個のリンクアグリゲーショングループの構築が可能です。ギガビットポート（オプション）だけは、 1 つのリンクアグリゲーショングループに所属します。

1 つのグループ内のポートはすべて同じ 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 は無効にする必要があります。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。

Port Trunking Settings（ポートトランキング設定）

ポートトランキングの設定を行います。

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

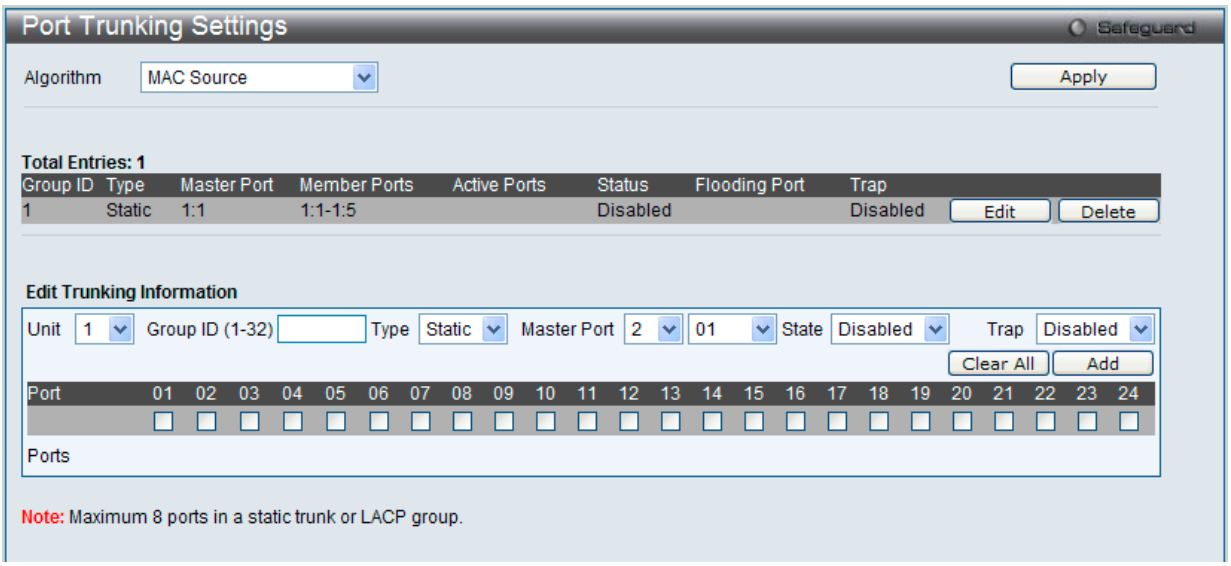


図 8-47　Port Trunking Settings 画面

本画面には次の項目があります。

項目	説明
Algorithm	ポートトランクグループを構成するポートのロードバランスに使用するアルゴリズムを選択します。「MAC Source」、「MAC Destination」、「MAC Source Destination」、「IP Source」、「IP Destination」、「IP Source Destination」、「L4 Port Source」、「L4 Port Destination」、「L4 Port Source Dest」から指定してください。（詳細は「Link Aggregation」メニューの項参照）。
Unit	設定するユニットを指定します。
Group ID (1-32)	グループの ID 番号（1-32）を設定します。
Type	トランキンググループの種類を設定します。 • Static - スタティックです。 • LACP - ポートトランキンググループのリンクを自動的に検出します。
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。本項目は、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。
Trap	プルダウンメニューを使用して、リンクアグリゲーショングループのリンクアップとリンクダウンの有効 / 無効を設定します。
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。グループには 8 ポートまで割り当てることができます。
Active Ports	現在パケットを転送しているポートを表示します。
Flooding Port	トランキンググループはブロードキャストもしくは未知のユニキャストを 1 ポートは許可する必要があります。

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。

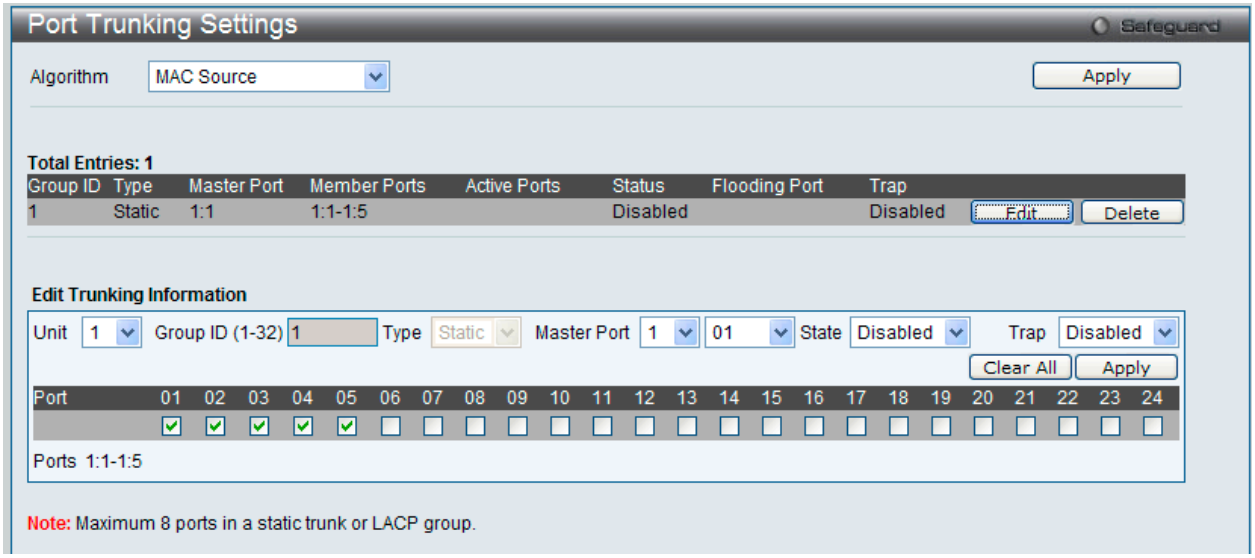


図 8-48　Port Trunking 画面 - Edit

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

LACP Port Settings（LACP ポート設定）

「LACP Port Settings」画面は、「Trunking」画面と関連し、スイッチにポートトランキンググループを作成するために使用します。

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

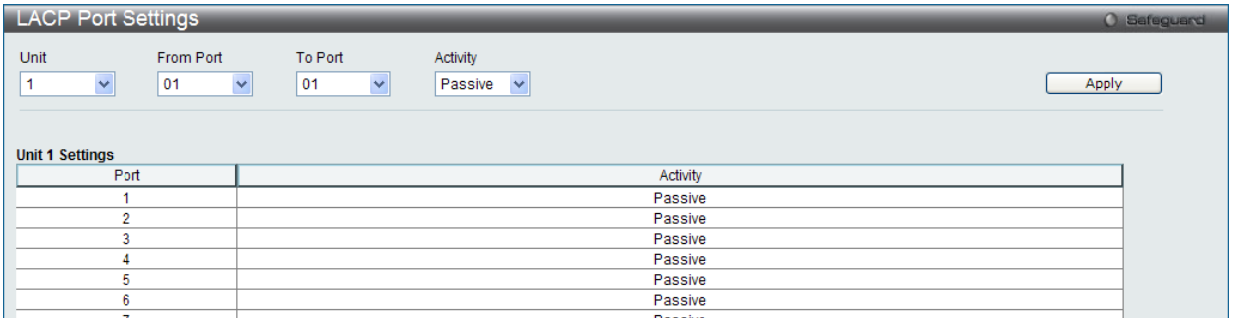


図 8-49　LACP Port Settings 画面

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」の役割を行うかを指定します。

以下の項目を使用して設定を行います。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定の対象となるポート範囲を設定します。
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、コネクションのどちらか一端が 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 設定）

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

スタティックユニキャスト転送の設定を行います。

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

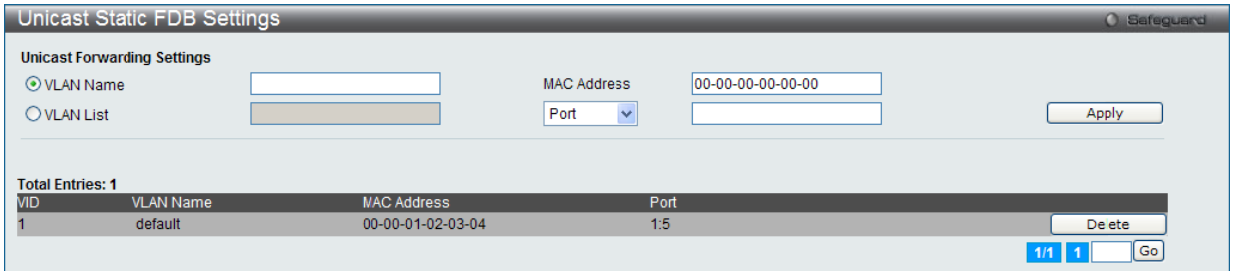


図 8-50　Unicast Static FDB 設定

画面には以下の項目があります。

項目	説明
VLAN Name	ラジオボタンをクリックしてユニキャスト MAC アドレスのある VLAN 名を入力します。
VLAN List	ラジオボタンをクリックしてユニキャスト MAC アドレスのある VLAN リストを入力します。
MAC Address	パケットが手動で転送される MAC アドレスを指定します。これはユニキャスト MAC アドレスです。
Port/Drop	上記で入力した MAC アドレスの存在する、ポート番号の選択を行います。このオプションは同時にユニキャストスタティック FDB からの MAC アドレスを破棄するのに使用されます。ポート番号を項目に入力します。ユニット番号の初期値は 1 です。入力形式は次の通りです。 「ユニット番号 : ポート番号」（例 : 1:5） 「ポート番号」（例 : 5）

項目を設定後、「Apply」ボタンをクリックし、デバイスに設定を適用します。「Delete」をクリックすると指定の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 設定）

スタティックマルチキャスト転送の設定を行います。

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

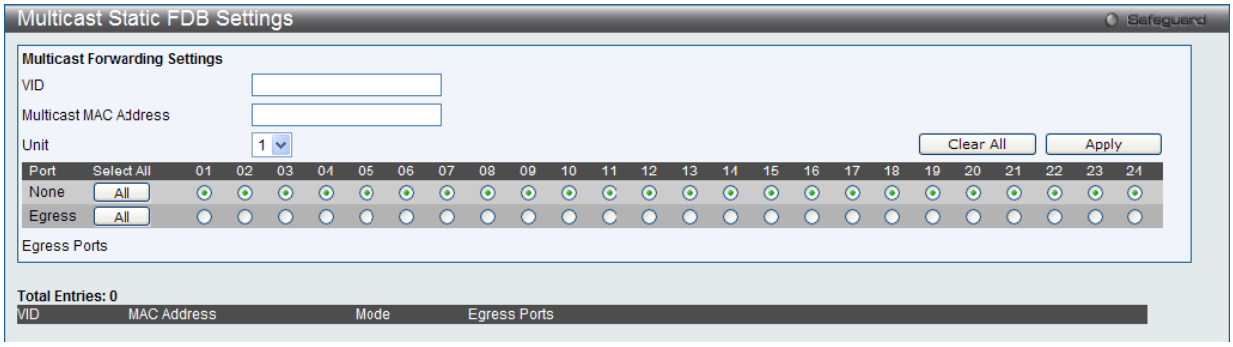


図 8-51　Multicast Static FDB 設定

画面には以下の項目があります。

項目	説明
VLAN Name	関連の MAC アドレスが属する VLAN の VLAN ID です。
Multicast MAC Address	スタティックフォワーディングテーブルに追加するマルチキャスト MAC アドレスを入力します。 BPDU には 01-80-C2-XX-XX-XX、IPv4 MAC アドレスには 01-00-5EXXXX-XX、また IPv6 マルチキャスト MAC アドレスには 33-33-XX-XX-XX の範囲のアドレスが予約されています。
Unit	設定するユニットを指定します。
Port	スタティックマルチキャストグループのメンバになるポートの選択、または自動的にメンバになる事を拒否するポートの選択をします。GMRP を使用します。 • None - 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なることはありません。全てのポートを選択するには「All」をクリックします。 • Egress - 指定の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になります。全てのポートを選択するには「All」をクリックします。

項目を設定後、「Apply」ボタンをクリックしデバイスに設定を適用します。「Clear All」をクリックすると入力した情報を破棄します。

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。

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

MAC 通知を行うためには、**L2 Features > FDB > MAC Notification Settings** の順にメニューをクリックし、以下の画面を表示します。

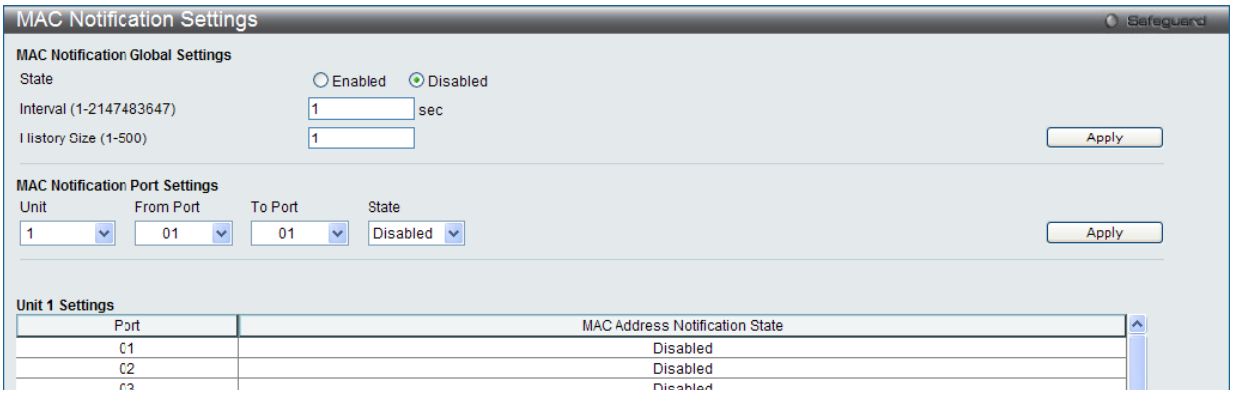


図 8-52　MAC Notification Settings 画面

以下の項目を使用して設定を行います。

項目	説明
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。
Interval (1-2147483647 sec)	通知を行う間隔（秒）。初期値 : 1（秒）
History Size (1-500)	通知用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
Unit	設定するユニットを選択します。
From Port /To Port	プルダウンメニューから、MAC 通知設定を有効または無効にするポートを指定します。
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 : Disabled

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。

MAC Address Aging Time Settings（MAC アドレスエージング設定）

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 Settings の順にメニューをクリックし、以下の画面を表示します。

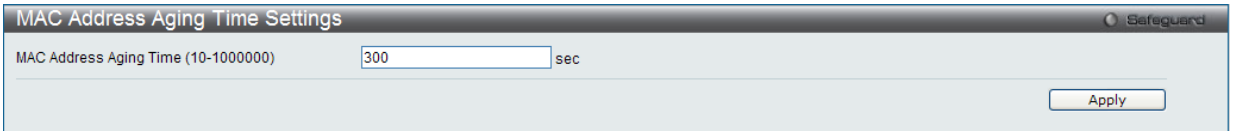


図 8-53　MAC Address Aging Time Settings 画面

以下の項目を使用して設定を行います。

項目	説明
MAC Address Aging Time (10-1000000)	学習した MAC アドレスが、アクセスされないでフォワーディングテーブルに保持される（つまりどれくらい学習した MAC アドレスが、アイドル状態を続けることが許可される）時間（10-1000000）を指定します。これを変更するためには、現在の MAC アドレスが破棄される時間（秒）とは異なる値を入力します。初期値は 300（秒）。

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。

MAC Address Table（MAC アドレステーブル）

ここでは、スイッチのダイナミック MAC アドレスフォワーディングテーブルの表示を行います。スイッチが MAC アドレスとポート番号の関連性を学習すると、フォワーディングテーブルにエントリとして登録を行います。それらのエントリは、スイッチ経由でパケットを転送するために使用されます。

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

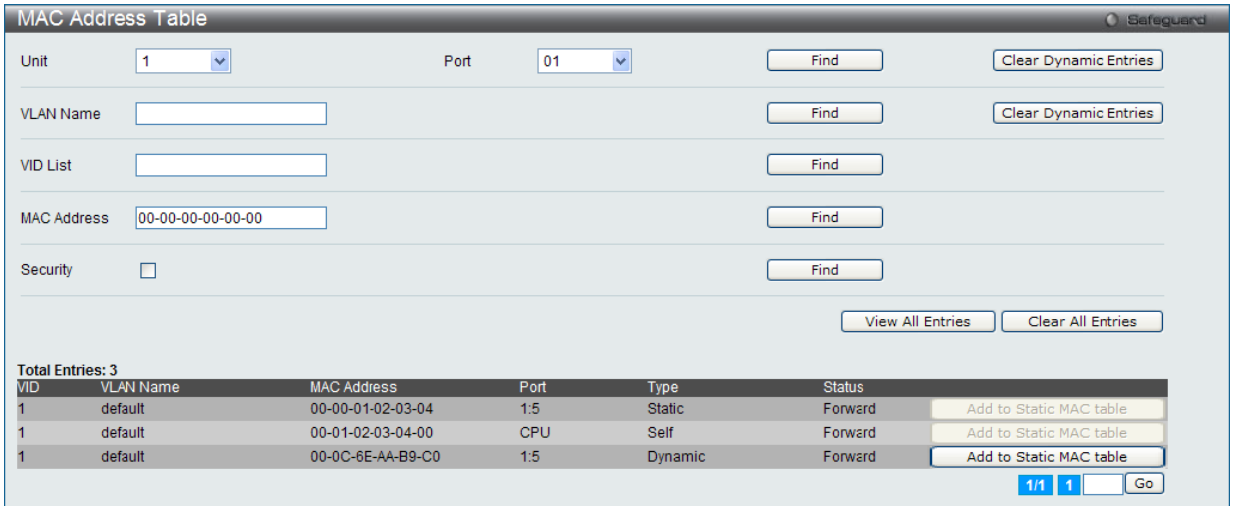


図 8-54　MAC Address Table 画面

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
Unit	設定するユニットを選択します。
Port	MAC アドレスと関連付けられるポート。
VLAN Name	参照するフォワーディングテーブルの VLAN 名を入力します。
VID List	参照するフォワーディングテーブルの VLAN リストを入力します。
MAC Address	参照するフォワーディングテーブルの MAC アドレスを入力します。
Security	セキュリティモジュールによって作成される FDB エントリを表示します。

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

エントリの検索

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

ダイナミックエントリの削除

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

エントリの表示

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

全エントリの削除

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

エントリの追加

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

ARP & FDB Table（ARP & FDB テーブル）

現在の ARP & FDP エントリについて表示します。特定の「ARP」または「FDB」エントリを検索する場合、プルダウンメニューからポートを選択するか、MAC/IP アドレスを画面上部に入力します。

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。

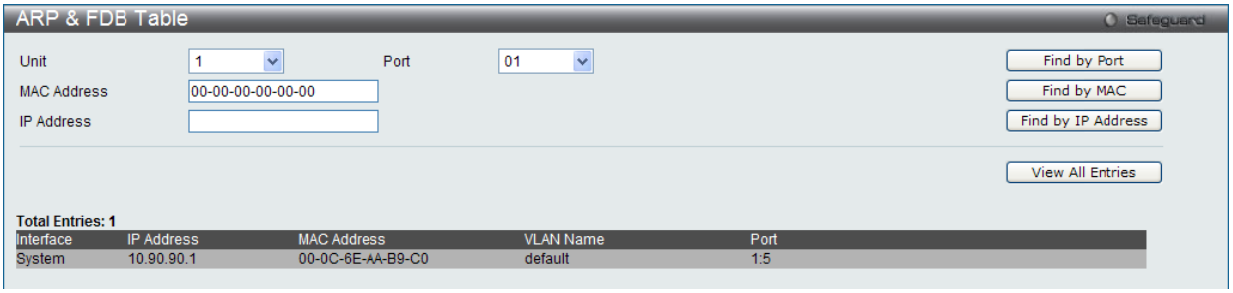


図 8-55　ARP & FDB Table 画面（SI モード）

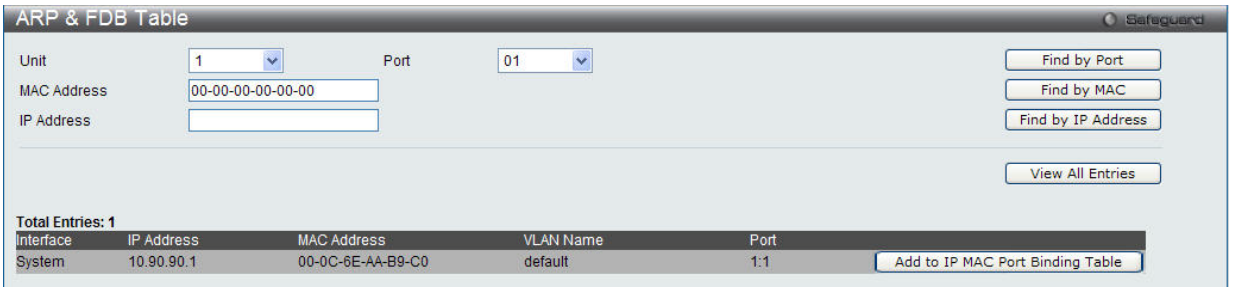


図 8-56　ARP & FDB Table 画面（EI モード）

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	MAC アドレスと関連付けられるポート。
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。
IP Address	参照するテーブルの IP アドレスを入力します。

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

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

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

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

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

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

IGMP Snooping（IGMP スヌーピング）

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追加 / 削除できるようになります。

IGMP Snooping Settings（IGMP スヌーピング設定）

IGMP Snooping 設定を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、画面上部の「IGMP Global Settings」セクションでスイッチ全体に機能を有効にします。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開閉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ると、マルチキャストパケットの送信を停止します。

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

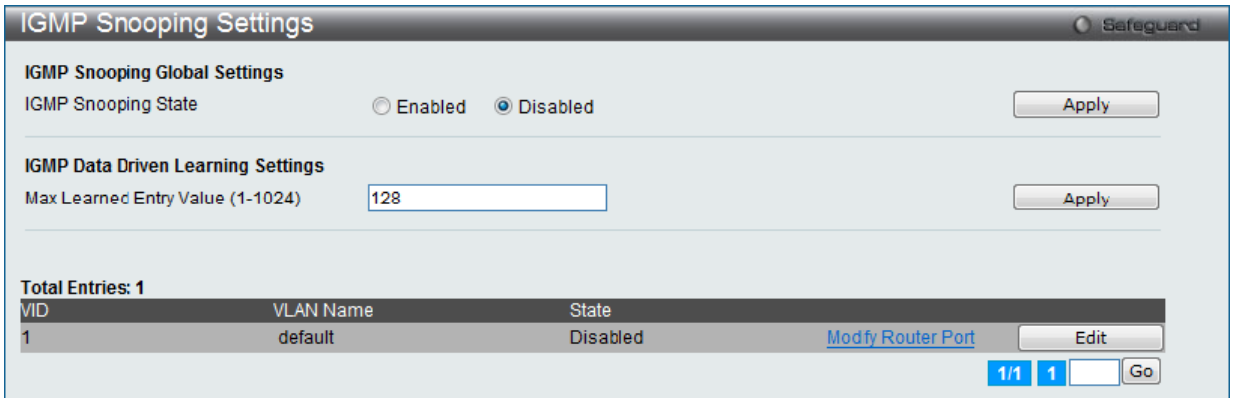


図 8-57　IGMP Snooping Settings 画面

画面には以下の項目があります。

項目	説明
IGMP Snooping Global Setting	
IGMP Snooping State	IGMP Snooping の有効 / 無効を設定します。IGMP Snooping を有効にするためには、はじめにマルチキャストフィルタリングのブリッジを有効にする必要があります。 • 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 Learning Entry Value (1-1024)	最大学習エントリ数を入力します。

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 Snooping 機能の詳細設定

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

図 8-58 IGMP Snooping Parameters Settings 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
VID	IGMP Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
VLAN Name	IGMP Snooping 設定を変更する VLAN を識別する VLAN 名を表示します。
Rate Limit	レート制限を表示します。
Querier IP	IGMP クエリアへ送信するクエリア IP アドレス。
Querier Expiry Time	クエリアの期限時間を表示します。
Query Interval (1-65535)	IGMP query 送信間隔（秒）。1-65535 の範囲から指定します。初期値は 125 です。
Max Response Time (1-25)	IGMP response report を送信するまでの最大時間（秒）。1-25 の範囲から指定します。初期値は 10（秒）です。
Robustness Value (1-7)	パケットロスへの抵抗力を示します。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。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)	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の Max Response Time 欄に設定する値（Last Member Query Interval）。また、同 Query の送信間隔でもあります。初期値は 1 です。
Data Drive Group Expiry Time (1-65535)	ユーザが特定の VLAN に対するラーニンググループの IGMP スヌーピングデータが期限切れになるまでの時間を設定します。初期値は 260（秒）です。
Proxy Reporting Source IP	プロキシレポーティングの送信元 IP アドレスを指定します。
Proxy Reporting State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Querier State	「Enabled」（有効）にすると IGMP Query パケットを送信可能になります。初期値は「Disabled」（無効）です。
Fast Leave	「Enabled」（有効）にすると、Fast Leave 機能が有効になります。この機能が有効になると、スイッチが IGMP Leave Report パケットを受信する時、マルチキャストグループのメンバは（Last Member Query Time の失効を待たずに）直ちにグループから脱退します。初期値は「Disabled」（無効）です。
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	特定の VLAN への IGMP スヌーピングレポートの抑制を「Enabled」（有効）/「Disabled」（無効）にします。
Data Driven Learning State	指定した VLAN の IGMP スヌーピングの Data Driven Learning を「Enabled」（有効）/「Disabled」（無効）にします。
Data Driven Learning Aged Out	指定した VLAN の IGMP スヌーピングの Data Driven Learning の有効期限設定を「Enabled」（有効）/「Disabled」（無効）にします。
Version	スイッチで使用する IGMP のバージョンを設定します。初期値は「3」です。
Querier Role	Query パケット送信についてのルータの動作を表示します。 • Querier - ルータは IGMP query パケットの送信を行うことを示します。 • Non-Querier - ルータは IGMP query パケットの送信を行わないことを示します。本欄は「Querier State」と「State」欄で「Enabled」を指定した場合には「Querier」と表示されます。

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。

IGMP Snooping ルータポート設定の変更

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

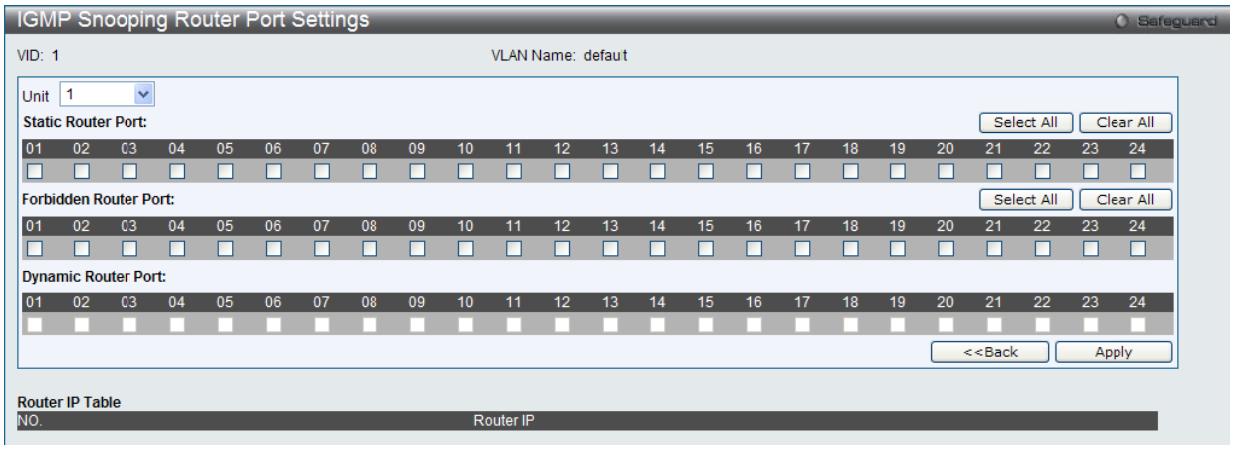


図 8-59　IGMP Snooping Router Port Settings 画面

画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
Static Router Port	マルチキャストが有効なルータと接続するポート範囲を設定します。プロトコルに関係なくマルチキャスト有効ルータに全てのパケットが届くことを確実にします。
Forbidden Router Port	マルチキャストが有効なルータと接続しないポート範囲を設定します。禁止されたルータポートはルーティングパケットを送信しません。
Dynamic Router Port	自動設定されたポートを表示します。

「Select All」をクリックすると全てのポートが選択されます。「Clear All」を選択すると選択した全てのポートが解除されます。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。

IGMP Snooping Rate Limit Settings（IGMP Snooping レートリミット設定）

各 VLAN またはポートの IGMP snooping コントロールパケットのレートを設定します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Rate Limit Settings をクリックして表示します。

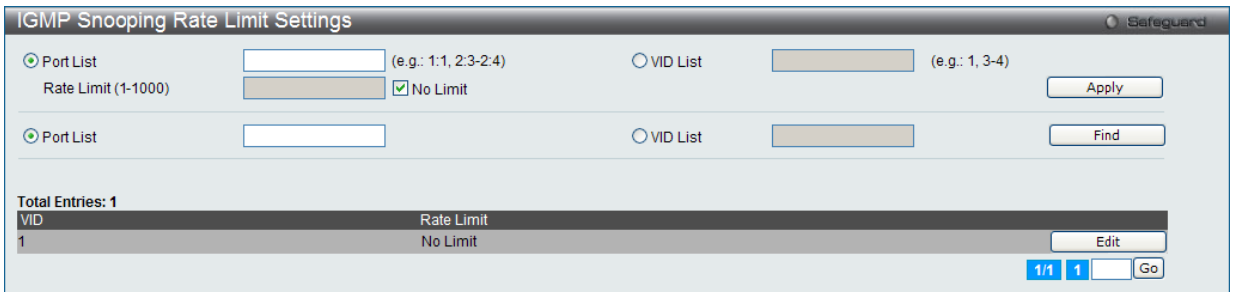


図 8-60　IGMP Snooping Rate Limit Settings 画面

以下の項目を使用して、設定します。

項目	説明
Port List	設定するポート / ポート範囲を指定します。
VLAN List	設定する VLAN/ VLAN 範囲を指定します。
Rate Limit (1-1000)	各ポート /VLAN に許可される IGMP コントロールパケットのレートを設定します。「No Limit」を選択するとレートに限度がなくなります。

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。

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

IGMP snooping スタティックグループ情報をスイッチに設定します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Static Group Settings をクリックして表示します。

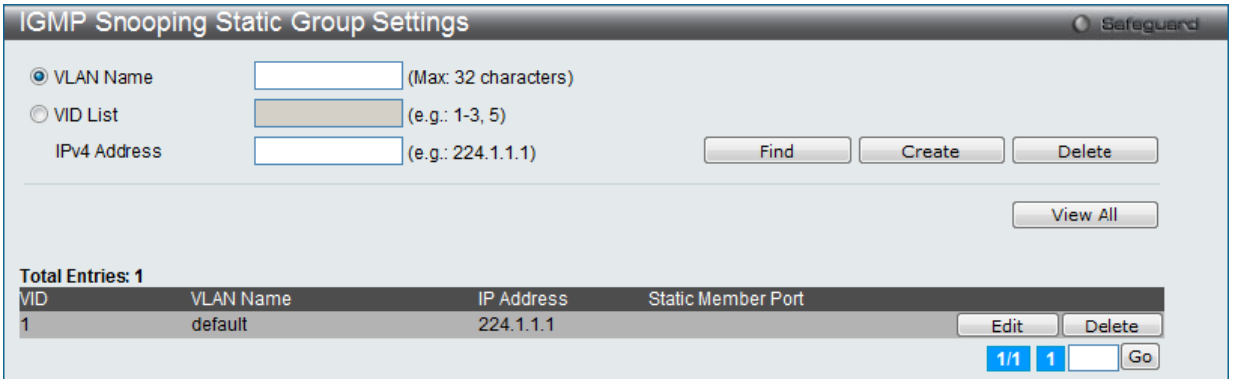


図 8-61　IGMP Snooping Static Group Settings 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Name	IGMP snooping スタティックグループ情報を作成する VLAN 名を入力します。
VLAN List	IGMP snooping スタティックグループ情報を作成する VLAN ID リストを入力します。
IPv4 Address	IGMP snooping スタティックグループ情報を作成するスタティックグループアドレスです。

エントリの参照

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

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

エントリの登録

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

エントリの削除

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

エントリの編集

IGMP スタティックグループエントリの編集には、対応する「Edit」ボタンをクリックして以下の画面を表示します。

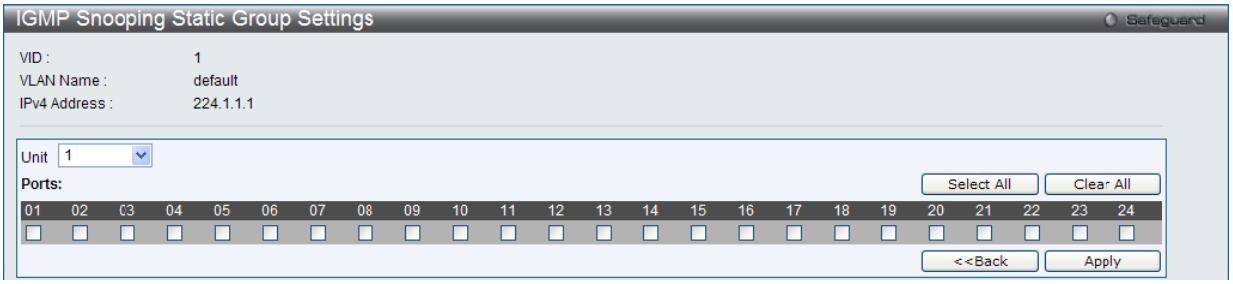


図 8-62　IGMP Snooping Static Group Settings - Edit 画面

以下の項目を設定または表示します。

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

「Apply」ボタンをクリックして行った変更を適用します。
「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

IGMP Router Port（IGMP ルータポートの参照）

現在ルータポートとして設定されているスイッチのポートを表示します。ユーザによって手動で設定済みのルータポートはスタティックルータポートとして表示されます。これらは「S」と表示されます。スイッチによって自動的に設定されたルータポートは「D」と表示されます。禁止ポート（Forbidden Port）は「F」と表示されます。VLAN ID を画面上部に入力して「Find」ボタンをクリックします。

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

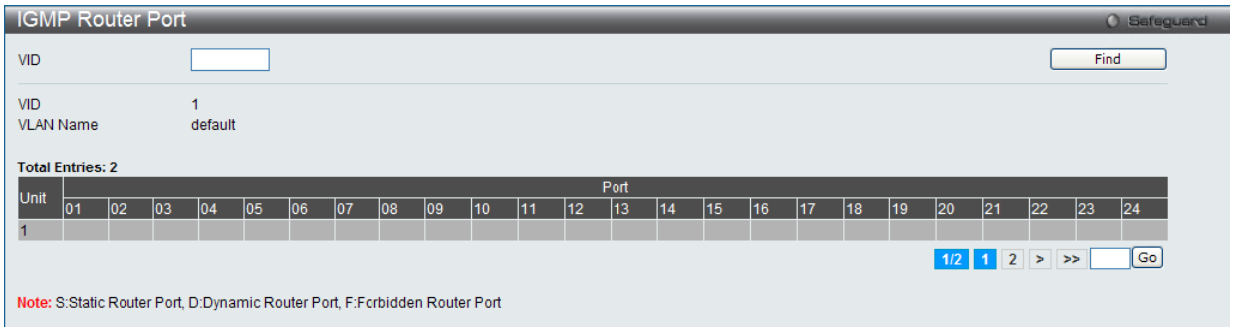


図 8-63　IGMP Router Port 画面

IGMP Snooping Group（IGMP Snooping グループ）

「IGMP Snooping Group Table」を表示します。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 Group の順にメニューをクリックし、以下の画面を表示します。

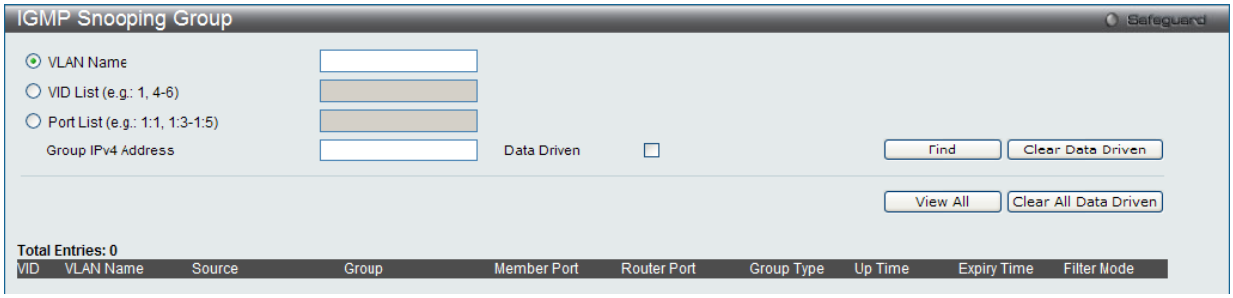


図 8-64　IGMP Snooping Group 画面

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。
Port List	マルチキャストグループのポート番号
Group IP Address	マルチキャストグループの IP アドレス。
Data Driven	データドリブングループのみ表示。

画面上の「VID List / VLAN Name」欄に VLAN Name または VID List を入力して「Find」ボタンをクリックすることにより、「IGMP Snooping Group Table」テーブルを検索することもできます。

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

IGMP Snooping によって学習した現在のマルチキャストフォワーディングテーブルのエントリを表示します。

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

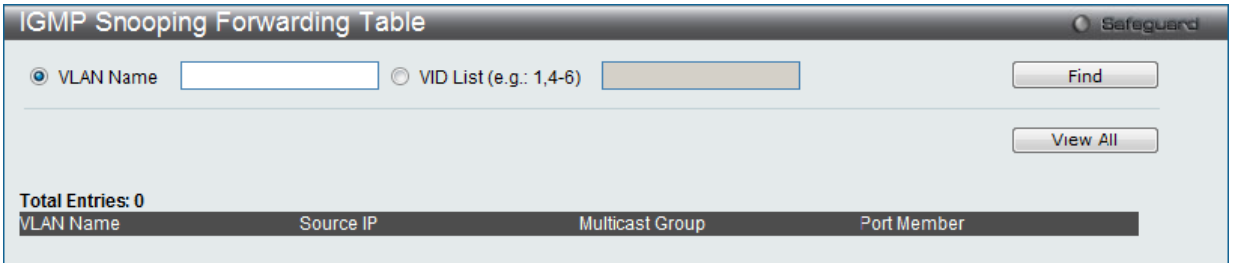


図 8-65　IGMP Snooping Forwarding Table 画面

以下の項目が表示されます。

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

画面左上の「VLAN Name」フィールドに 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。

IGMP Snooping Counter（IGMP Snooping カウンタ）

現在の IGMP Snooping の統計情報を表示します。

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

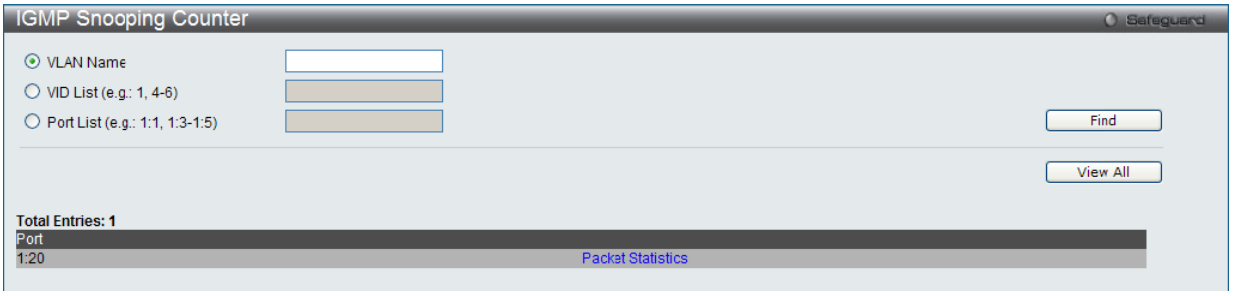


図 8-66　IGMP Snooping Counter 画面

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。
Port List	マルチキャストグループのポート番号

エントリの参照

画面左上の「VLAN Name」「VLAN List」「Port List」フィールドに入力して「Find」ボタンをクリックすることにより、テーブル内を検索することができます。

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

カウンタテーブルの参照

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

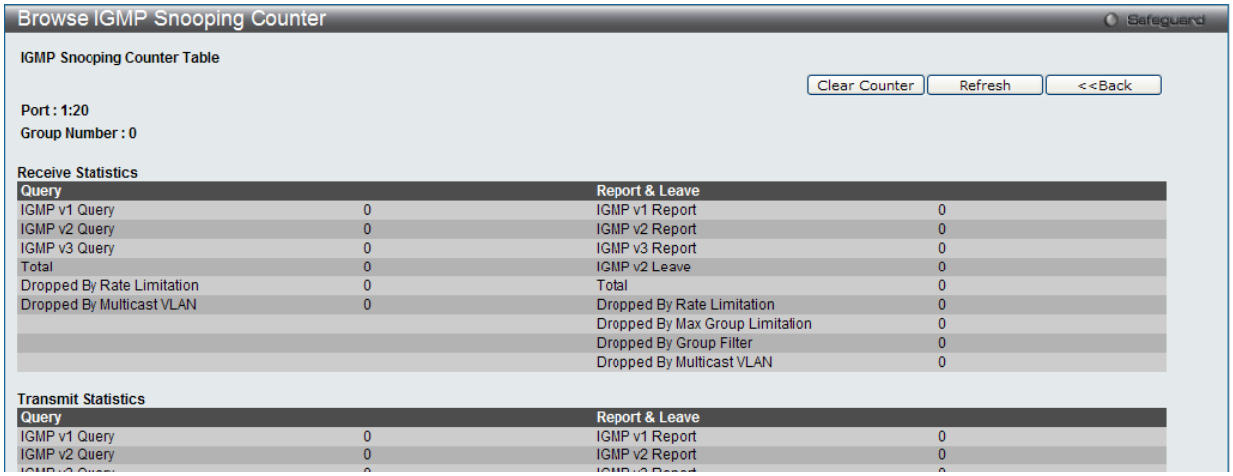


図 8-67　IGMP Snooping Counter Table 画面

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

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

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。

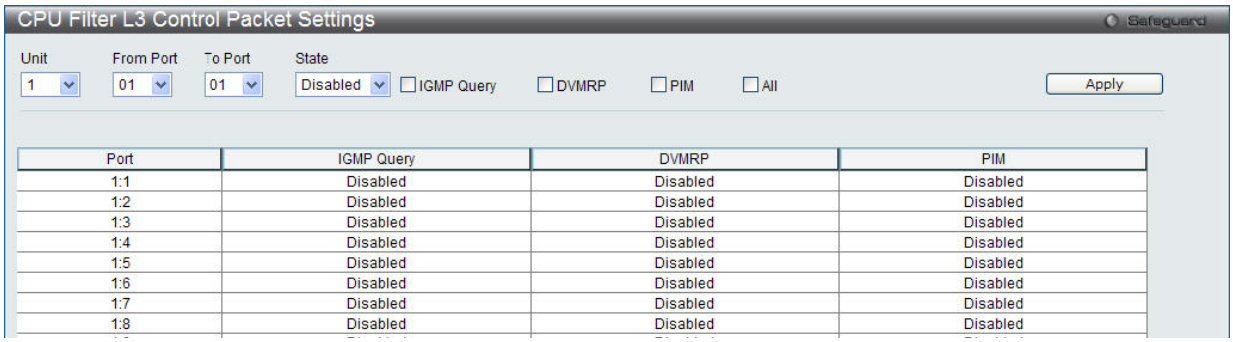


図 8-68　CPU Filter L3 Control Packet Settings 画面

以下の項目が表示されます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	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 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。
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。

MLD Snooping Settings（MLD スヌーピング）

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 を使用するデバイス間で 3 つのタイプのメッセージを交換します。これらのメッセージは、130、131 および 132 にラベル付けされた 4 つの 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 – IGMPv2 の Host Membership Report（HMR）と類似のものです。Listening ホストは、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 ホス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 Version2 – 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（Data Driven ラーニング）

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ラッドされることを意味します。

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 エントリになることに注意してください。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 IGMP 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 IGMP Snooping 機能で破棄されます。

MLD Snooping Settings（MLD スヌーピング設定）

MLD Snooping を設定します。

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

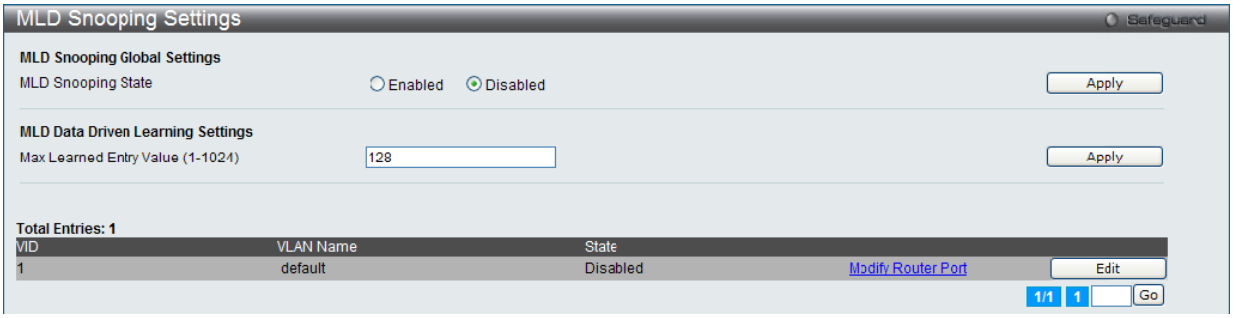


図 8-69　MLD Snooping Settings 画面

以下の項目を使用して、設定します。

項目	説明
MLD Snooping State	本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Max Learned Entry Value (1-1024)	MLD Snooping データドリブンラーニングの最大値を設定します。

「Apply」をクリックして編集した設定を適用します。「Edit」をクリックして指定エントリの MLD スヌーピングパラメータを設定します。

MLD Snooping のグローバル設定

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

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

MLD Snooping 機能の詳細設定

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

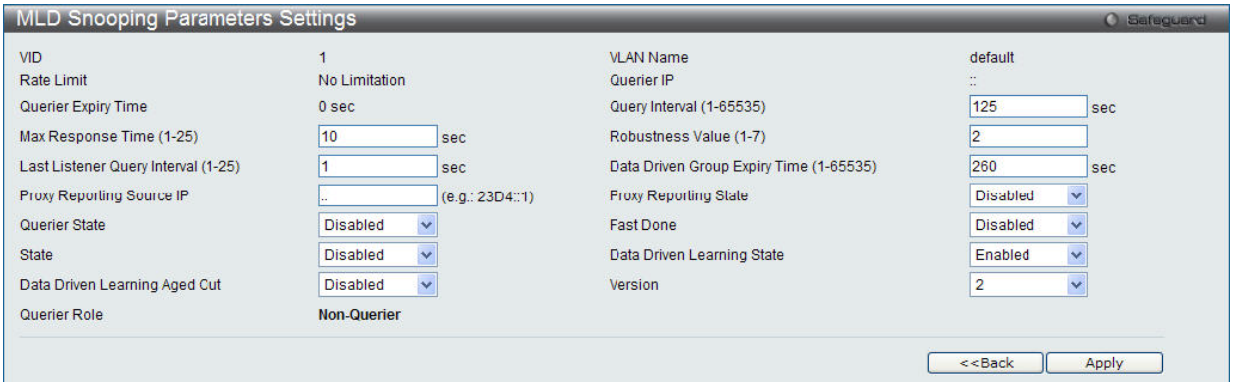


図 8-70　MLD Snooping Parameters Settings 画面

以下の項目を参照または変更できます。

項目	説明
VLAN ID	MLD Snooping の設定を変更する VLAN の VLAN ID です。VLAN Name と同期しています。
VLAN Name	MLD Snooping の設定を変更する VLAN の VLAN 名です。VLAN ID と同期しています。
Rate Limit	レート制限を表示します。
Querier IP	MLD クエリに送信するクエリア IP アドレスです。
Querier Expiry Time	クエリアの制限時間を表示します。
Query Interval (1-65535)	1 から 65535 で設定でき、初期値は 125（秒）です。IGMP クエリを送信する間隔を指定します。
Max Response Time (1-25 sec)	MLD ポート Listener へのレスポンスを待つ最大許容時間を秒単位で設定します。1-25 の範囲から指定します。初期値は 10 です。
Robustness Value (1-7)	予想されるサブネット上のパケット損失の許容量を微調整します。本値は以下の MLD メッセージ間隔を計算する場合に使用されます。 • 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。次の計算式で計算されます。 (robustness variable*query interval)+(1*query response 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。次の計算式で計算されます。 (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。初期値は 2 です。サブネットが失われたと予想する場合には、この値を増やすことができます。
Last Listener Query Interval（1-25）	done-group メッセージに応答するために送信されるものも含む Group-Specific Query メッセージ間隔の最大値を指定します。この間隔はルータがラストメンバグループ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（秒）です。
Data Driven Group Expiry Time (1-65535)	特定の VLAN の「MLD Snooping data driven learning group」の期限を設定します。初期値は 260 です。
Proxy Reporting Source IP	プロキシレポーティングの送信元 IPv6 アドレスを指定します。
Proxy Reporting State	プルダウンメニューを使用して、本機能を「Enabled」(有効)/「Disabled」(無効) にします。
Querier State	初期値は Disabled です。「Disabled」が表示されている場合、MLD Snooping が Non-Querier 状態あることを示します。
Fast Done	fast done 機能を有効にします。この機能を「Enabled」（有効）にするとマルチキャストグループのメンバは done メッセージがスイッチに受信されるとすぐにグループから抜けることができます。
State	指定の VLAN に対して MLD Snooping の「Enabled」（有効）/「Disabled」（無効）を設定します。初期値は「Disabled」です。
Data Driven Learning State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Data Driven Learning Aged Out	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
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、パケットは破棄されます。

「Apply」ボタンをクリックして、設定を適用します。「MLD Snooping Settings」画面に戻るためには、「<<Back」ボタンをクリックします。

MLD Snooping ルータポートの設定

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

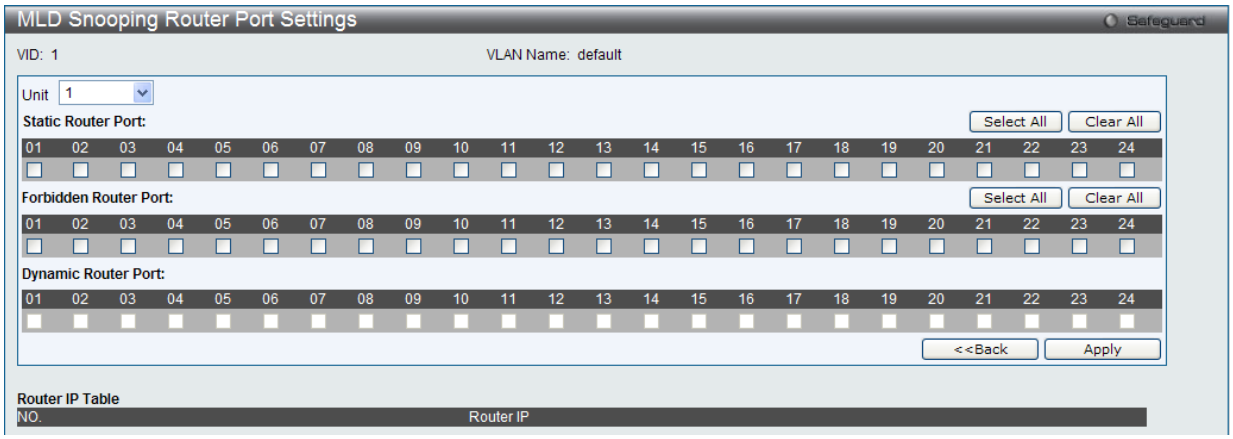


図 8-71　MLD Snooping Router Port Settings 画面

以下の項目を使用して、設定します。

項目	説明
Unit	設定するユニットを選択します。
Static Router Port	指定ポートがマルチキャストが有効であるルータに接続するために、対応するポート番号の下のチェックボックスをチェックします。これは、プロトコルなどにかかわらず、これらのポートが宛先としてマルチキャストが有効であるルータを持つすべてのパケットを転送し、ルータに到達することを保証します。
Forbidden Router Port	対応するポート番号の下のチェックボックスをチェックすると指定ポートがマルチキャストが有効であるルータに接続しないようにします。これは、禁止ポートがルーティングパケットを外部に送信しないように設定します。
Dynamic Router Port	対応するポート番号の下のチェックボックスをチェックすると、指定ポートがマルチキャストが有効であるルータに接続するかどうかを自動的に決定します。
Ports	ルータポート設定を行うポートを選択します。

「Apply」ボタンをクリックします。

MLD Snooping Rate Limit Settings（MLD スヌーピング レートリミット設定）

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。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Rate Limit Settings の順にメニューをクリックします。

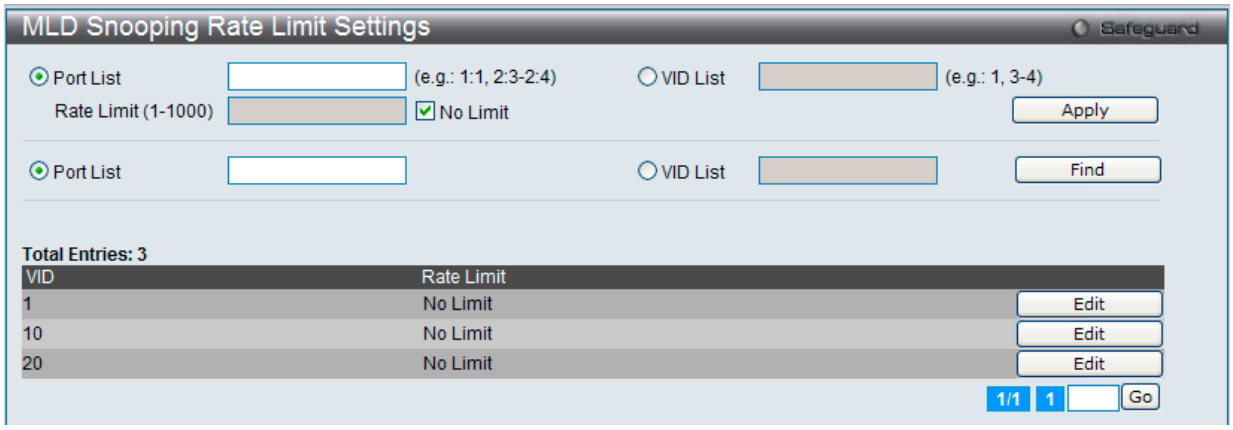


図 8-72　MLD Snooping Rate Limit Settings 画面

以下の項目を使用して、設定します。

項目	説明
Port List	表示 / 設定するポート / ポート範囲を設定します。
VLAN List	表示 / 設定する VLAN/VLAN 範囲を設定します。
Rate Limit	特定のポートもしくは VLAN の MLD コントロールパケットのレートを指定します。レートは毎秒のパケットに設定できます。制限を超えたパケットは廃棄されます。「No Limit」を選択すると制限がなくなります。

「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。

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。

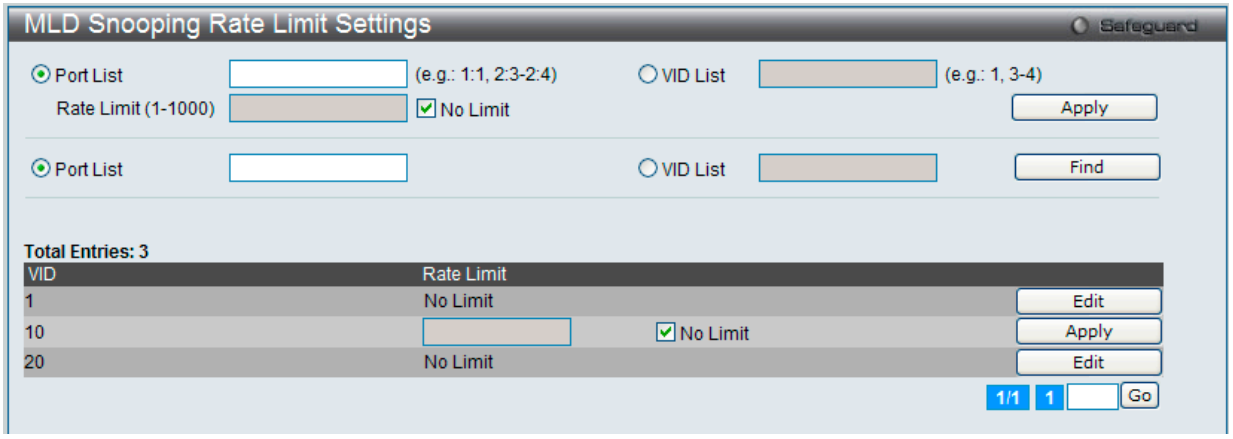


図 8-73　MLD Snooping Rate Limit Settings 画面 - Edit

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 スヌーピング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 の順にメニューをクリックします。

図 8-74　MLD Snooping Static Group Settings 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Name	MLD snooping スタティックグループ情報を設定する VLAN 名を指定します。
VLAN ID List	MLD snooping スタティックグループ情報を設定する VLAN リストを指定します。
IPv6 Address	MLD snooping スタティックグループ情報を設定するスタティックグループ v6 アドレスを指定します。

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

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

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

エントリの登録
「VLAN Name」または「VID List」、および「IPv6 Address」入力後、「Create」ボタンをクリックします。

エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

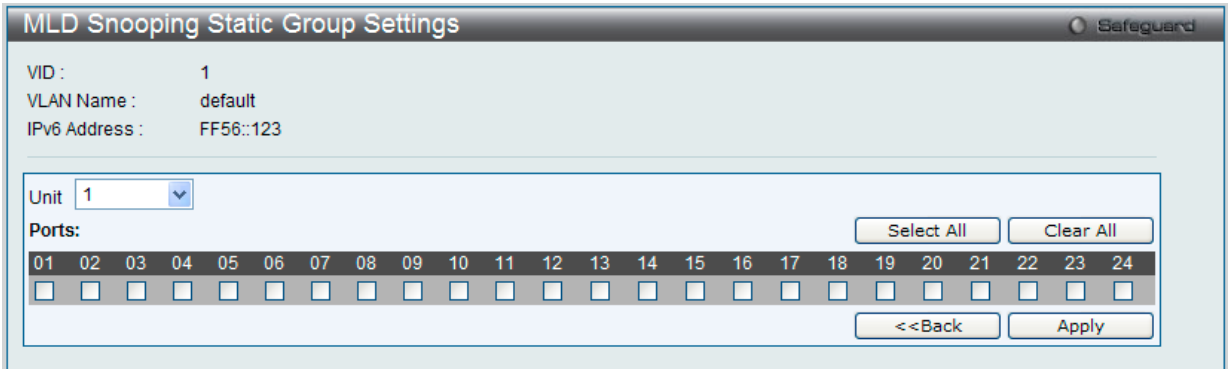


図 8-75　MLD Snooping Static Group Settings 画面

「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（MLD ルータポートの参照）

スイッチのどのポートが現在 IPv6 のルータポートとして設定されているかを表示します。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Router Port メニューをクリックし、「MLD Router Port」画面を表示します。

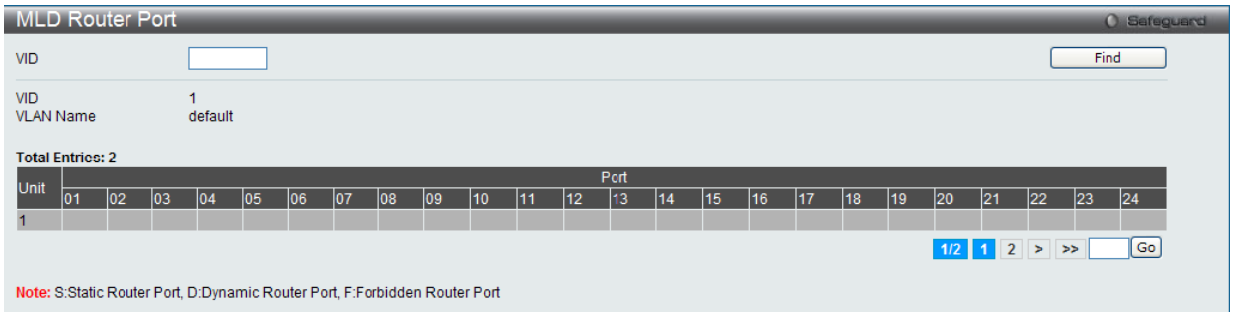


図 8-76　MLD Router Port 画面

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。画面上の「VID」に VLAN ID を入力し、「Find」ボタンをクリックします。

MLD Snooping Group（MLD スヌーピンググループ）

スイッチの MLD Snooping Group Table を参照します。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 メニューをクリックし、以下の画面を表示します。

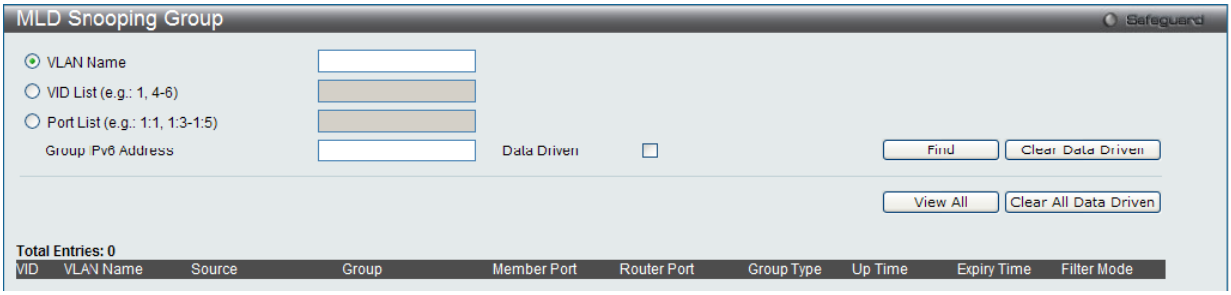


図 8-77　MLD Router Port 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Name	MLD マルチキャストグループの VLAN 名
VID List	MLD マルチキャストグループの VLAN ID リスト
Port List	MLD マルチキャストグループを検索するためのポート番号
Group IPv6 Address	使用する IPv6 アドレス。指定の MLD スヌーピンググループに適用するデータドリブン機能を有効にするには「Data Driven」を選択します。
Data Driven	「Data Driven」を有効にするとデータドリブングループのみ表示されます。

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。

エントリの削除

「Clear Data Driven」ボタンをクリックして、Data Driven 情報をクリアします。
「Clear All Data Driven」ボタンをクリックして、すべての Data Driven 情報をクリアします。

MLD Snooping Forwarding Table（MLD スヌーピングフォワーディングテーブル）

MLD Snooping によって学習した現在のマルチキャストフォワーディングテーブルのエントリを表示します。

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

図 8-78　MLD Snooping Forwarding Table 画面

以下の項目を使用して、設定します。

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

情報を入力して「Find」をクリックして検索します。設定済みのエントリをすべて表示する場合、「View All」をクリックします。

MLD Snooping Counter（MLD スヌーピングカウンタ）

スイッチに適用している MLD Snooping カウンタを表示します。

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

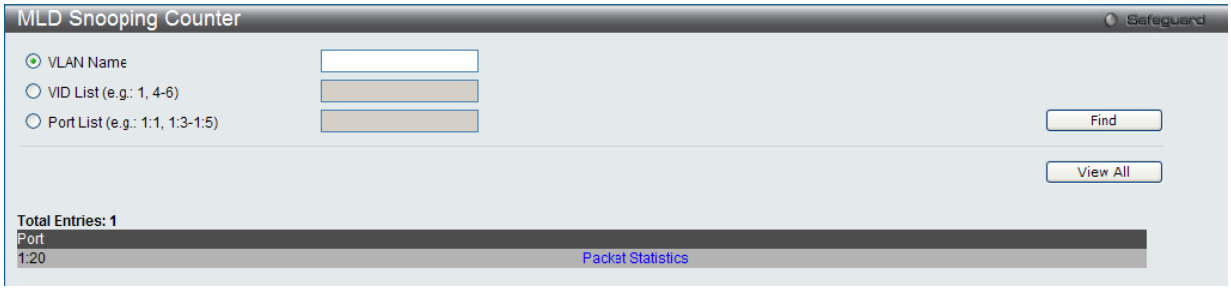


図 8-79　MLD Snooping Counter 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Name	MLD スヌーピンググループの VLAN 名
VID List	MLD スヌーピンググループの VLAN ID リスト
Port List	MLD スヌーピンググループのポートリスト

情報を入力して「Find」をクリックして検索します。設定済みのエントリをすべて表示する場合、「View All」をクリックします。

MLD Snooping カウンタテーブルの参照

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

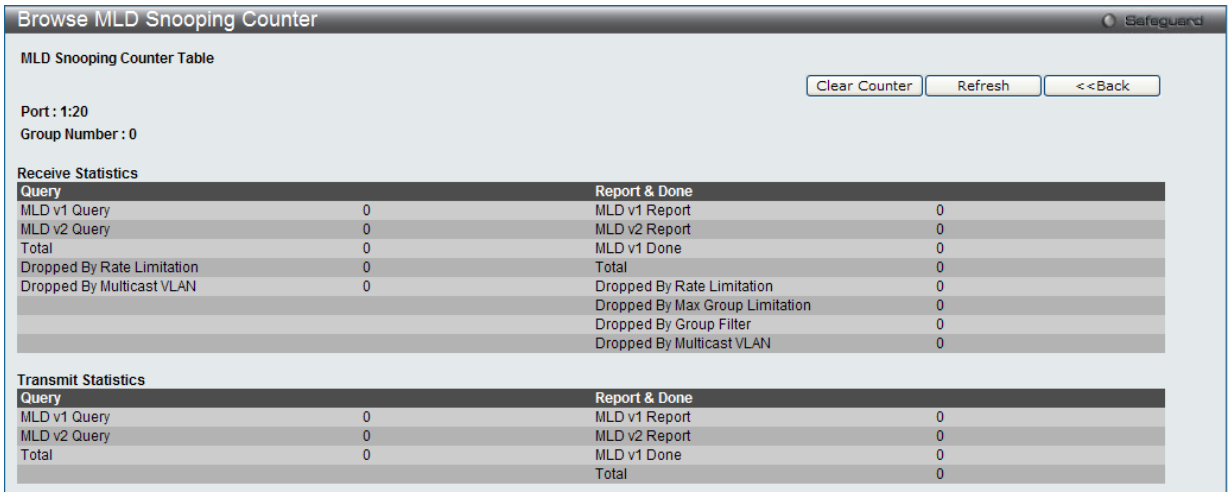


図 8-80　Browse MLD Snooping Counter 画面

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

Multicast VLAN（マルチキャスト VLAN）

スイッチング環境には、マルチプル VLAN が存在する可能性があります。マルチキャストクエリがスイッチを通過する度に、スイッチはシステム上の各 VLAN にそれぞれ異なるデータのコピーを送信する必要があります。これは順々にデータトラフィックを増加していき、トラフィックのパスを塞いでしまう可能性があります。トラフィックの負荷を軽減するために、マルチキャスト VLAN を組み込むことができます。これらのマルチキャスト VLAN は、複数のコピーの代わりにこのマルチキャストトラフィックを 1 つのコピーとしてマルチキャスト VLAN の受信者に送信します。

スイッチに組み込まれている他の一般的な VLAN に関係なく、マルチキャストトラフィックを送信したいマルチプル VLAN に対してどんなポートも追加することができます。マルチキャストトラフィックがスイッチに入力されるソースポートを設定した後、入力マルチキャストトラフィックが送信され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、そのように設定されると、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はるかに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。

制限と条件

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。

1. マルチキャスト VLAN はエッジおよびエッジでないスイッチで実行することができます。
2. メンバポートとソースポートはマルチプル ISM VLAN で使用できます。しかし、特定の ISM VLAN では、メンバポートとソースポートを同じポートにはできませんのでご注意ください。
3. マルチキャスト VLAN はノーマルな 802.1Q VLAN とは排他的です。これは、802.1Q VLAN と ISM VLAN の VLAN ID（VID）と VLAN 名は同じにはできないことを意味します。VID または VLAN 名がどんな VLAN でも一度選択されると、別の VLAN に使用することはできません。
4. 設定された VLAN の通常の表示は設定されたマルチキャスト VLAN を表示しません。
5. 一度、ISM VLAN が有効になると、この VLAN に対応する IGMP Snooping 状態も有効になります。有効になった 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。

スイッチにマルチキャスト VLAN の作成と設定を行います。

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）

指定したポートに受信するマルチキャストアドレスレポートにプロファイルを追加します。本機能は受信レポートの数と設定されたマルチキャストグループの数を制限します。指定のポートにレポートを受信する (Permit) またはレポートを拒否する (Deny)IP マルチキャスト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 メニューをクリックし、以下の画面を表示します。

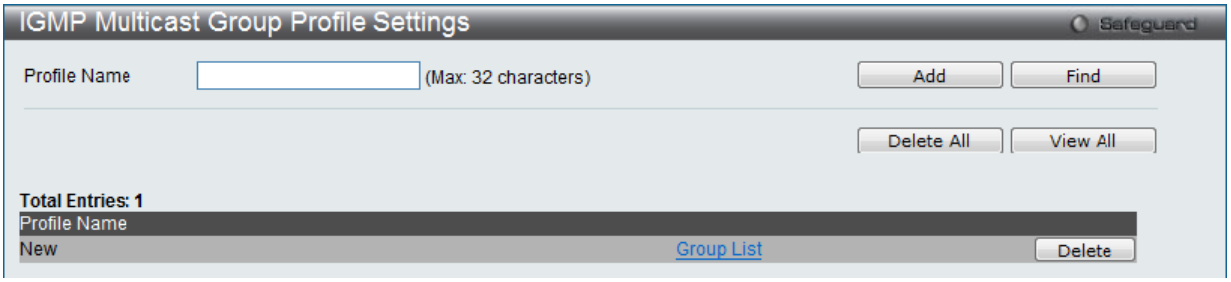


図 8-81　IGMP Multicast Group Profile Settings 画面

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。

エントリの検索

情報を入力して「Find」をクリックしてエントリを検索します。設定済みのエントリをすべて表示する場合、「View All」をクリックします。

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。

エントリの編集

1. 「Multicast Address List」欄の対応する「Group List」リンクをクリックし、以下の画面を表示します。

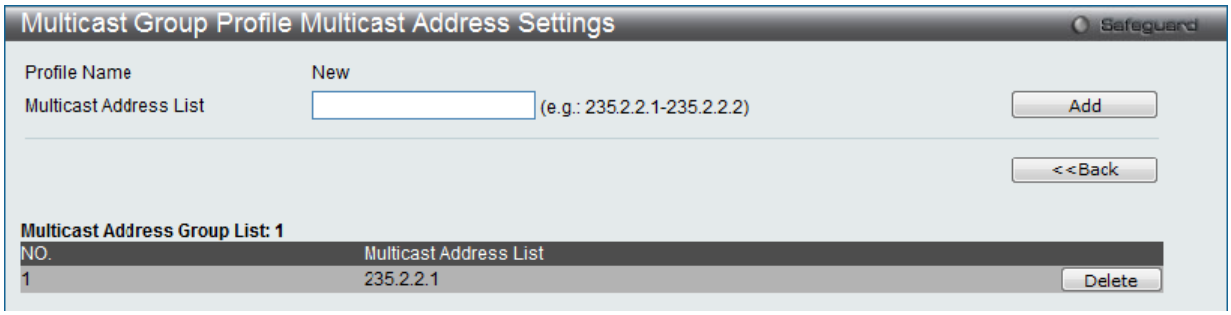


図 8-82　Multicast Group Profile Multicast Address Settings 画面

以下の項目が表示されます。

項目	説明
Multicast Address List	マルチキャストアドレスリストの値を入力します。

2. 「Multicast Address List」でアドレス範囲を入力し、「Add」ボタンをクリックします。

エントリの削除

該当するエントリの「Delete」ボタンをクリックします。

「<<Back」をボタンをクリックし、前のページに戻ります。

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

スイッチの IGMP Snooping マルチキャスト VLAN 設定を行います。

L2 Features > L2 Multicast Control > Multicast VLAN > IGMP Snooping Multicast Group VLAN Settings をクリックして表示します。

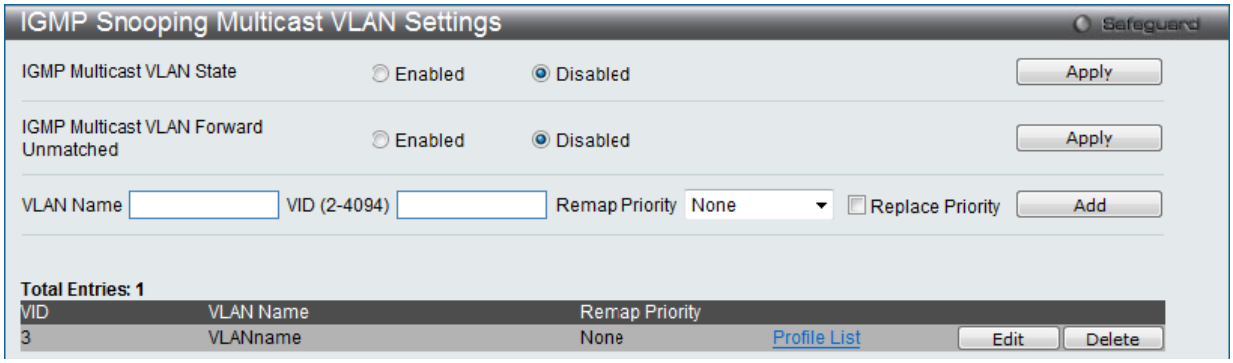


図 8-83　IGMP Snooping Multicast VLAN Settings 画面

以下の項目を使用して、設定します。

項目	説明
IGMP Multicast VLAN State	選択した VLAN のマルチキャスト VLAN 機能を「Enabled」（有効）/「Disabled」（無効）にします。
IGMP Multicast VLAN Forward Unmatched	スイッチは IGMP パケットを受信した場合、そのパケットを対応するマルチキャスト VLAN を決めるマルチキャストプロファイルに、対抗したパケットと合致させます。「Enable」を選択するとパケットを転送し、「Disable」を選択するとパケットは廃棄されます。
VLAN Name	IGMP Snooping 設定を変更する VLAN 名と VLAN ID です。
VID (2-4094)	IGMP Snooping 設定を変更する VLAN ID と VLAN 名です。
State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Remap Priority	VLAN に転送するデータトラフィックに関連する優先度を再配置（リマップ）します。「None」を選択した場合、元々のパケットの優先度が使用されます。初期値は「none」です。
Replace Priority	スイッチの「Remap Priority」での再配置に基づきパケットの優先度を変更するオプションです。「Remap Priority」が設定されている場合のみ有効です。

マルチキャスト VLAN の登録

1. 「IGMP Multicast VLAN State」を「Enabled」（有効）を選択し、「Apply」ボタンをクリックします。

2. 各項目を入力後、「Add」ボタンをクリックしてエントリを追加します。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

マルチキャスト VLAN の編集

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

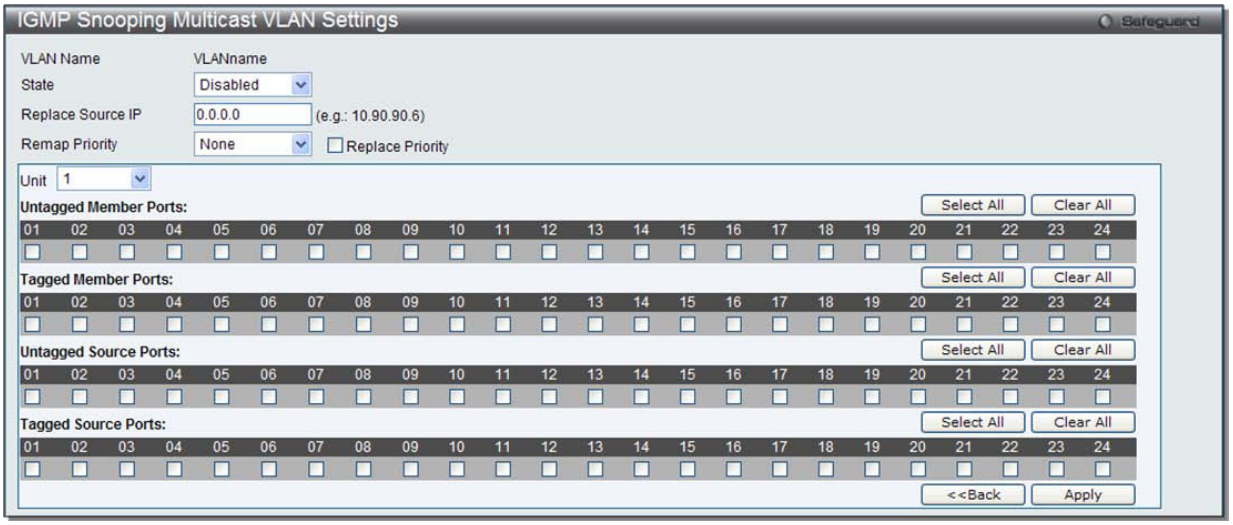


図 8-84　IGMP Snooping Multicast VLAN Settings – Edit 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Name	設定した VLAN の VLAN 名を表示します。
State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Replace Source IP	使用する新しい IP アドレスを入力します。 IGMP Snooping 機能を有効にしているとホストから送信された IGMP レポー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はジョインパケット内の送信元 IP アドレスはここで設定する IP アドレスに変更されます。「Not Replaced」が設定された場合、送信元 IP アドレスは変更されます。
Remap Priority	• 0-7 - VLAN に転送するデータトラフィックに関連する優先度を再配置（リマップ）します。 • None - 元々のパケットの優先度が使用されます。（初期値）
Replace Priority	スイッチの「Remap Priority」での再配置に基づきパケットの優先度を変更するオプションです。「Remap Priority」が設定されている場合のみ有効です。
Unit	設定するユニットを選択します。
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。「Select All」ボタンをクリックすると全てのポートを選択し、「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。
Tagged Member Ports	マルチキャスト VLAN のメンバーとしてタグ付けするポートを選択します。「Select All」ボタンをクリックすると全てのポートを選択し、「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。
Untagged Source Port	マルチキャスト VLAN に追加するタグつけをしない送信元ポート（ポート範囲）を選択します。タグなし送信元ポートの PVID は自動的にマルチキャスト VLAN に変更されます。送信元ポートは必ずタグ付き / タグなしとして各マルチキャスト VLAN に認識される必要があります。両方のタイプで同じマルチキャスト VLAN のメンバになりえません。「Select All」ボタンをクリックすると全てのポートを選択し、「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。
Tagged Source Ports	マルチキャスト VLAN に追加するタグつけをする送信元ポート（ポート範囲）を選択します。「Select All」ボタンをクリックすると全てのポートを選択し、「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。

「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。
「Apply」ボタンをクリックして行った変更を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

2. 画面上部に表示される定義済みの項目を変更し、「Apply」ボタンをクリックします。

マルチキャスト VLAN グループリストの設定

1. 既に作成したプロファイルにマルチキャスト VLAN を追加する場合は、追加するグループリストの「Profile List」のリンクをクリックし、以下の画面を表示します。

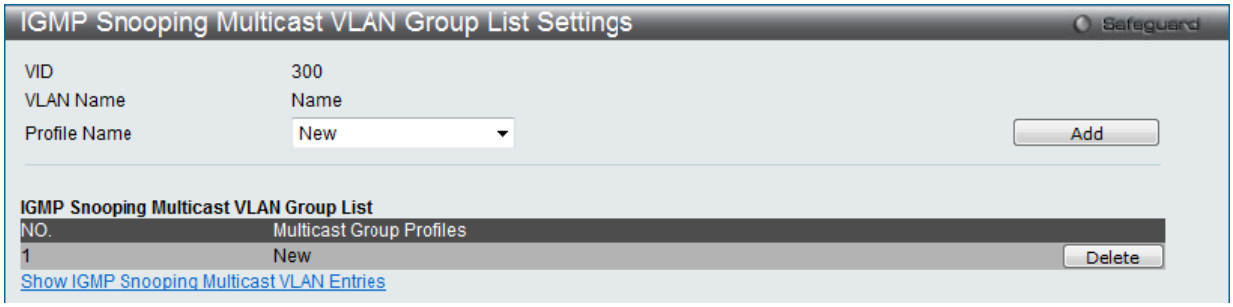


図 8-85　IGMP Snooping Multicast VLAN Group List Settings 画面

以下の項目を使用して、設定します。

項目	説明
VID	VLAN ID を表示します。
VLAN Name	VLAN 名を表示します。
Profile Name	プルダウンメニューを使って IGMP スヌーピングマルチキャスト VLAN グループ名を選択します。

2. 「Profile Name」を入力し、「Add」ボタンをクリックしてエントリを追加します。

マルチキャスト VLAN グループリストの削除

1. マルチキャスト VLAN グループリストを削除する場合は、該当する行の「Delete」ボタンをクリックします。

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

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）

IP Multicast Profile 設定を行います。

L2 Features > L2 Multicast Control > Multicast VLAN > MLD Multicast Group Profile Settings をクリックします。

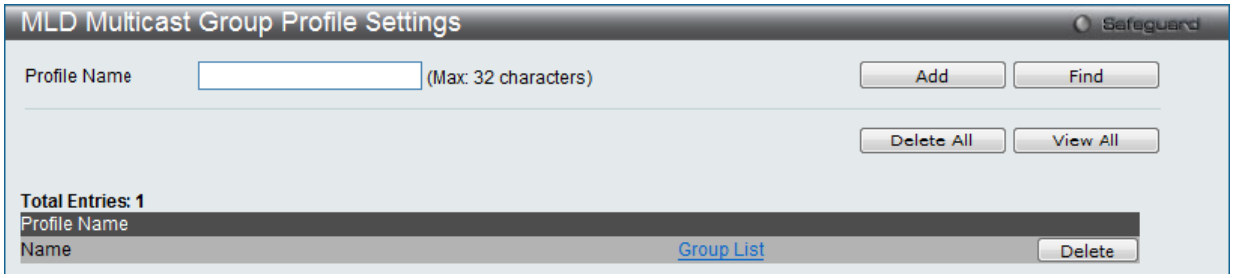


図 8-86　MLD Multicast Group Profile Settings 画面

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。

エントリの編集

1. 「Multicast Address List」欄の対応する「Group List」リンクをクリックし、以下の画面を表示します。

図 8-87　Multicast Group Profile Multicast Address Settings 画面 - エントリ名の変更

以下の項目を使用して、設定します。

項目	説明
Multicast Address List	MLD マルチキャストアドレスリストを入力します。

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）

スイッチに IGMP Snooping マルチキャスト VLAN 設定を行います。

L2 Features > L2 Multicast Control > Multicast VLAN > MLD Snooping Multicast Group VLAN Settings をクリックして表示します。

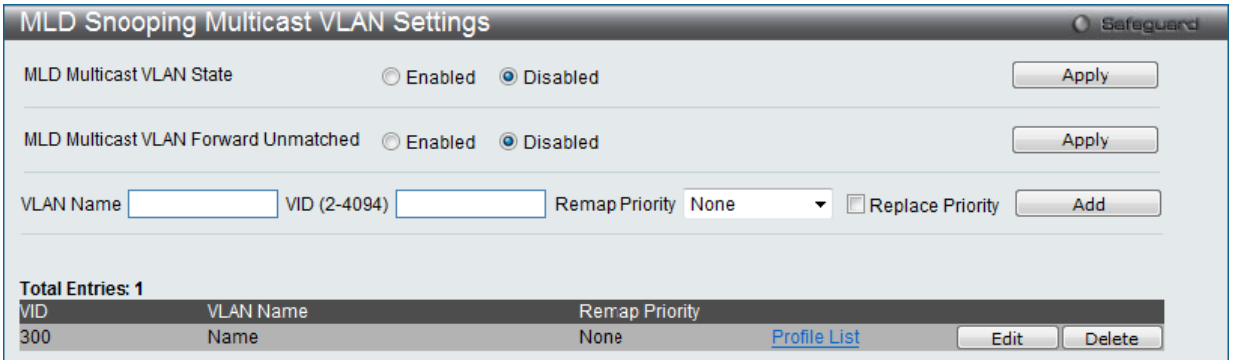


図 8-88　MLD Snooping Multicast VLAN Settings 画面

以下の項目を使用して、設定します。

項目	説明
MLD Multicast VLAN State	選択した VLAN の MLD マルチキャスト VLAN 機能を「Enabled」（有効）/「Disabled」（無効）にします。
MLD Multicast VLAN Forward Unmatched	スイッチは MLD パケットを受信した場合、そのパケットを対応するマルチキャスト VLAN を決めるマルチキャストプロファイルに、対抗したパケットと合致させます。「Enable」を選択するとパケットを転送し、「Disable」を選択するとパケットは廃棄されます。
VLAN Name	設定を変更する VLAN 名です。
VID (2-4094)	設定を変更する VLAN ID です。
Remap Priority	VLAN に転送するデータトラフィックに関連する優先度を再配置（リマップ）します。「None」を選択した場合、元々のパケットの優先度が使用されます。初期値は「None」です。
Replace Priority	スイッチの「Remap Priority」での再配置に基づきパケットの優先度を変更するオプションです。「Remap Priority」が設定されている場合のみ有効です。

「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。

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。

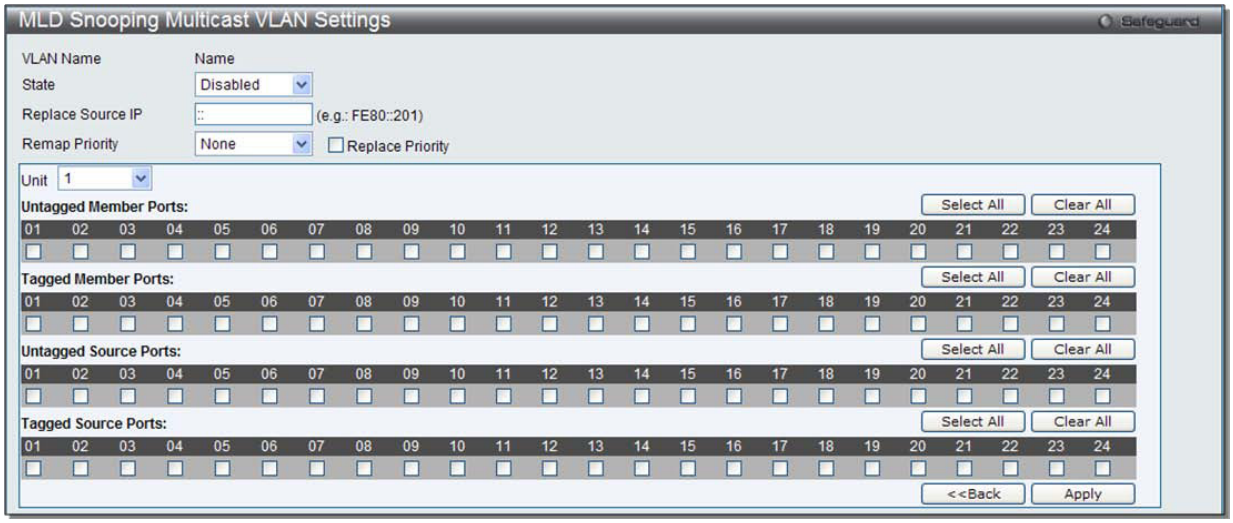


図 8-89　MLD Snooping Multicast VLAN Settings – Edit 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Name	設定した VLAN の VLAN 名を表示します。
State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Replace Source IP	使用する新しい IP アドレスを入力します。 MLD Snooping 機能を有効にしているとホストから送信された MLD レポー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はジョインパケット内の送信元 IP アドレスはここで設定する IP アドレスに変更されます。「Not Replaced」が設定された場合、送信元 IP アドレスは変更されます。
Remap Priority	• 0-7 - VLAN に転送するデータトラフィックに関連する優先度を再配置（リマップ）します。 • None - 元々のパケットの優先度が使用されます。（初期値）
Replace Priority	スイッチの「Remap Priority」での再配置に基づきパケットの優先度を変更するオプションです。「Remap Priority」が設定されている場合のみ有効です。
Unit	設定するユニットを選択します。
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。「Select All」ボタンをクリックすると全てのポートを選択し、「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。
Tagged Member Ports	マルチキャスト VLAN のメンバーとしてタグ付けするポートを選択します。「Select All」ボタンをクリックすると全てのポートを選択し、「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。
Untagged Source Port	マルチキャスト VLAN に追加するタグつけをしない送信元ポート（ポート範囲）を選択します。タグなし送信元ポートの PVID は自動的にマルチキャスト VLAN に変更されます。送信元ポートは必ずタグ付き / タグなしとして各マルチキャスト VLAN に認識される必要があります。両方のタイプで同じマルチキャスト VLAN のメンバになりえません。「Select All」ボタンをクリックすると全てのポートを選択し、「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。
Tagged Source Ports	マルチキャスト VLAN に追加するタグつけをする送信元ポート（ポート範囲）を選択します。「Select All」ボタンをクリックすると全てのポートを選択し、「Clear All」ボタンをクリックすると全てのポートの選択が解除されます。

「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

2. 画面上部に表示される定義済みの項目を変更し、「Apply」ボタンをクリックします。

マルチキャスト VLAN グループリストの設定

1. 既に作成したプロファイルにマルチキャスト VLAN を追加する場合は、追加するグループリストの「Profile List」のリンクをクリックし、以下の画面を表示します。

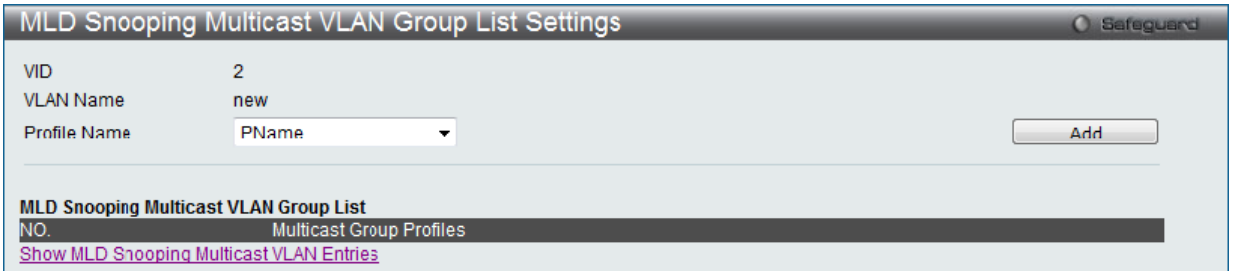


図 8-90　MLD Snooping Multicast VLAN Group List Settings 画面

以下の項目を使用して、設定します。

項目	説明
VID	VLAN ID を表示します。
VLAN Name	VLAN 名を表示します。
Profile Name	プルダウンメニューを使って MLD スヌーピングマルチキャスト VLAN グループ名を選択します。

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. マルチキャスト VLAN グループリストを削除する場合は、該当する行の「Delete」ボタンをクリックします。

「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。

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）

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。この機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。特定のスイッチポートに到着するレポートを受信する（Permit）またはレポートを拒否する（Deny）IPv4 アドレス /IPv4 アドレス範囲を設定することができます。

L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Multicast Profile Settings をクリックし、以下の画面を表示します。

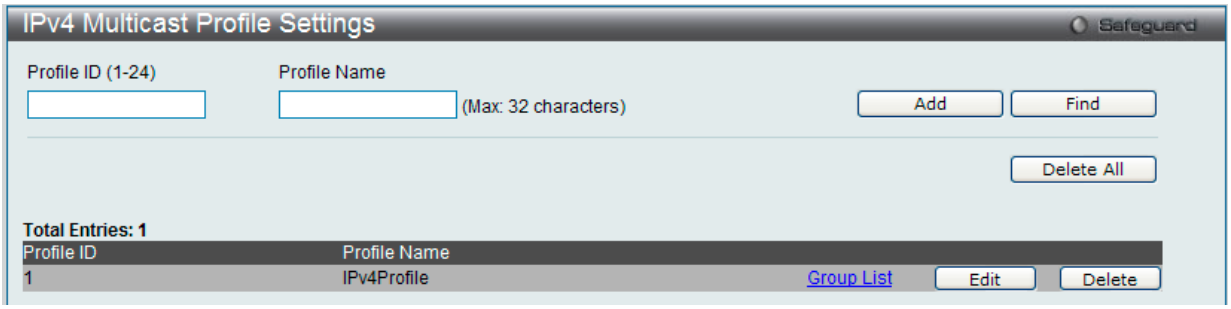


図 8-91　IPv4 Multicast Profile Settings 画面

以下の項目を使用して、設定します。

項目	説明
Profile ID (1-24)	プルダウンメニューを使用して、プロファイル ID を選択します。
Profile Name	IP マルチキャストプロファイル名を入力します。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

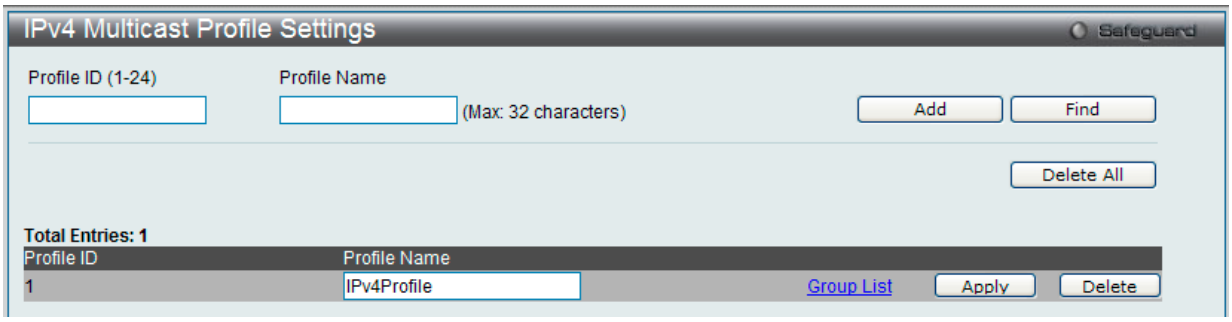


図 8-92　IPv4 Multicast Profile Settings 画面 - Edit

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

対応する「Delete」ボタンをクリックします。

マルチキャストグループリストの設定

「Group List」リンクをクリックすると、以下の画面が表示されます。

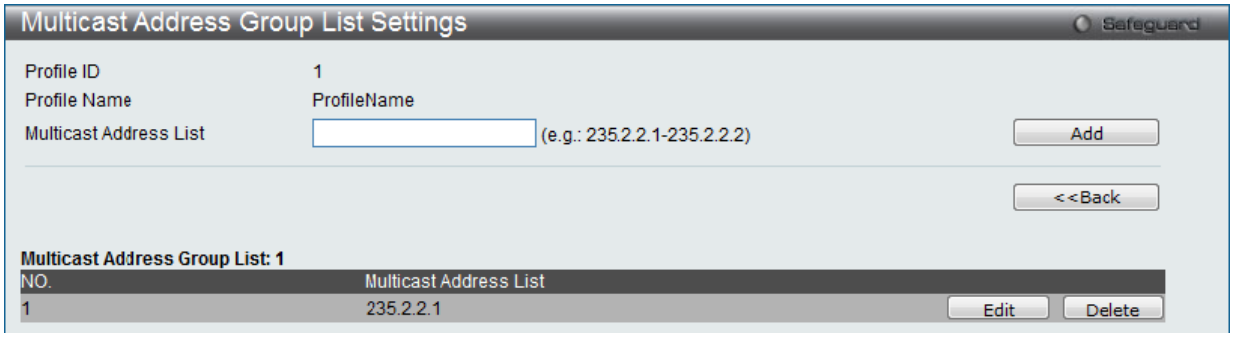


図 8-93　Multicast Address Group List Settings 画面

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 を表示します。
Profile Name	プロファイル名を表示します。
Multicast Address List	マルチキャストアドレスリストを入力します。

IPv4 Limited Multicast Range Settings（IPv4 マルチキャスト範囲の限定設定）

「Limited IP Multicast Range」に含まれるスイッチポートを設定します。送信元ポートによって受信ポートに送信可能だとして許容されるマルチキャストアドレスの範囲を設定します。

L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Limited Multicast Range Settings の順にメニューをクリックし、以下の画面を表示します。

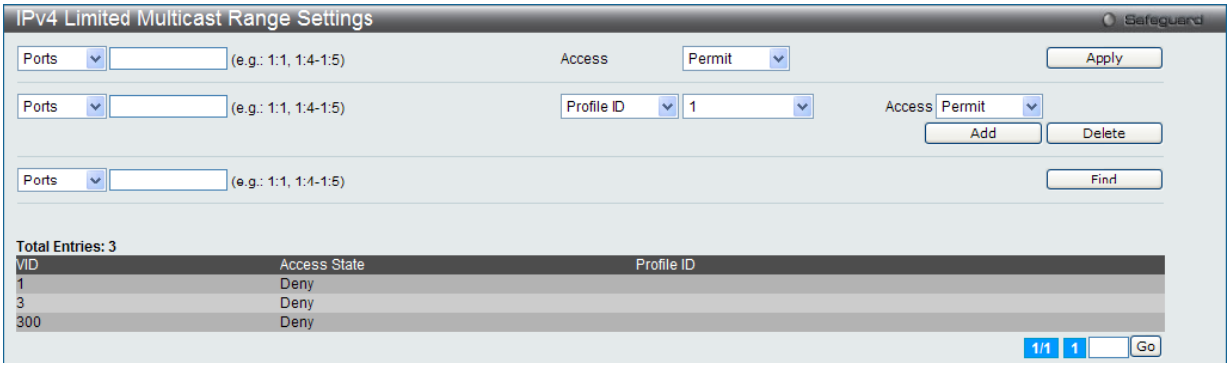


図 8-94　IPv4 Limited Multicast Range Settings 画面

新しい範囲の追加
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
情報を入力し、「Delete」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
Ports / VID List	設定に使用するポート、VLAN ID を選択します。
Access	「Permit」「Deny」からアクセス設定をします。
Profile ID/Profile Name	プルダウンメニューを使用してプロファイル ID またはプロファイル名を指定します。

「Apply」ボタンをクリックして変更を適用します。

「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。

IPv4 Max Multicast Group Settings（IPv4 最大マルチキャストグループ設定）

最大のフィルタグループ（最大 1024 まで）に所属するスイッチポートを設定します。

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ます。

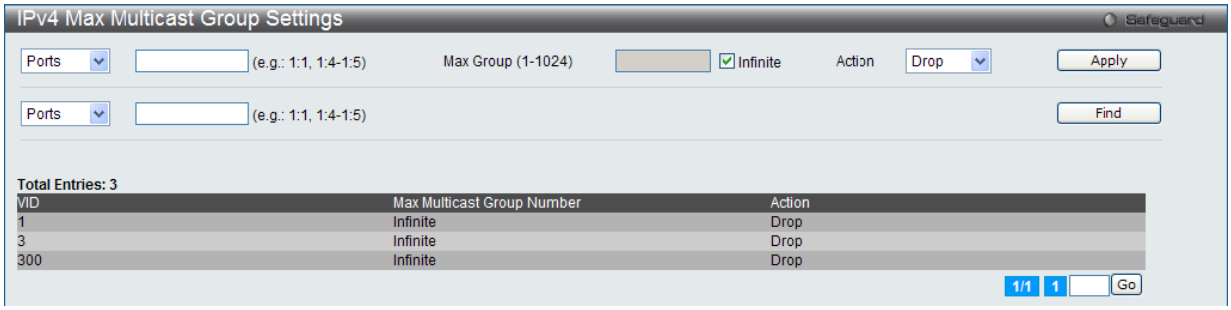


図 8-95　IPv4 Max Multicast Group Settings 画面

以下の項目を使用して、設定します。

項目	説明
Ports / VLAN ID	プルダウンメニューから「Ports」「VLAN ID」を選択します。
Max Group (1-1024)	Multicast グループの最大数を入力します。1 から 1024 の間で設定できます。「Infinite」を選択すると制限がありません。
Action	プルダウンメニューから登録が最大限に達した時、最新のグループの扱いについて選択します。 • drop - 最新のグループを破棄します。 • replace - 一番古いグループを最新のグループと入れ替えます。

適切な情報を入力し「Apply」ボタンをクリックします。

IPv6 Multicast Filtering（IPv6 マルチキャストフィルタリング）

ここでは、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。この機能は、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 Multicast Profile 設定を行うには、**L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Multicast Profile Settings** をクリックします。

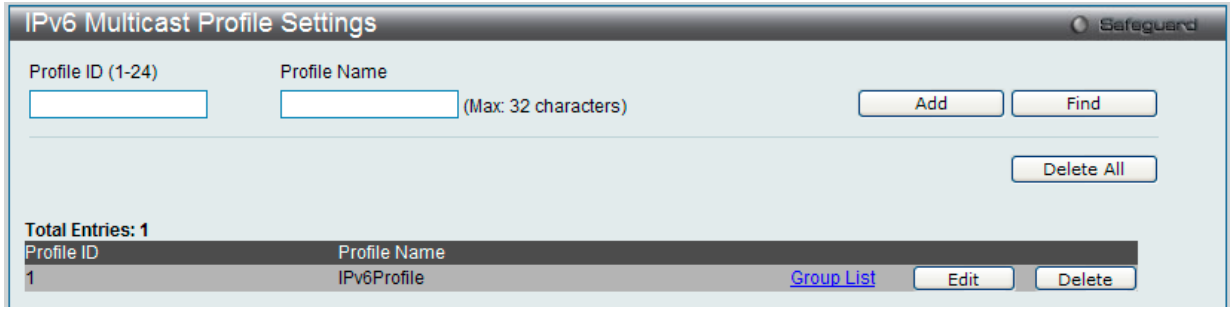


図 8-96　IPv6 Multicast Profile Settings 画面

以下の項目を使用して、設定します。

項目	説明
Profile ID (1-24)	プルダウンメニューを使用して、プロファイル ID を選択します。
Profile Name	IP マルチキャストプロファイル名を入力します。

エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの参照

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

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

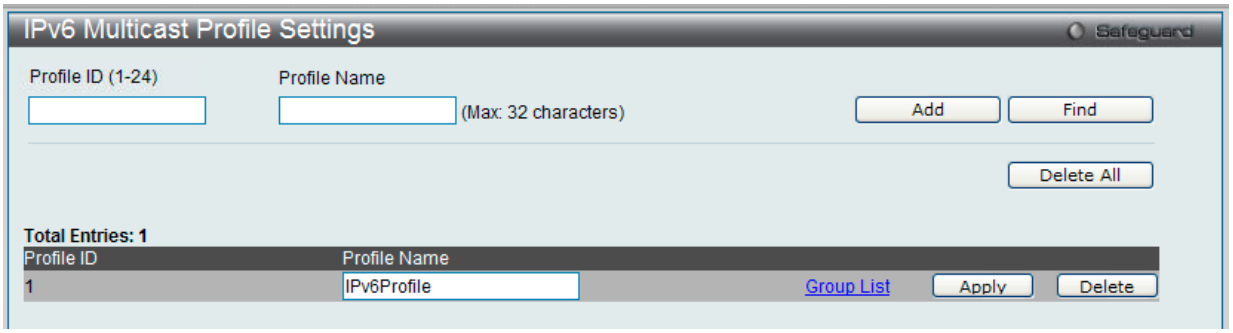


図 8-97　IPv6 Multicast Profile Settings 画面 - Edit

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 8-98　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 を表示します。
Profile Name	プロファイル名を表示します。
Multicast Address List	マルチキャストアドレスリストを入力します。

エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

IPv6 Limited Multicast Range Settings（IPv6 マルチキャスト範囲の限定設定）

「Limited IP Multicast Range」に含まれるスイッチポートを設定します。送信元ポートによって受信ポートに送信可能だとして許容されるマルチキャストアドレスの範囲を設定します。

L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Limited Multicast Range Settings の順にメニューをクリックし、以下の画面を表示します。

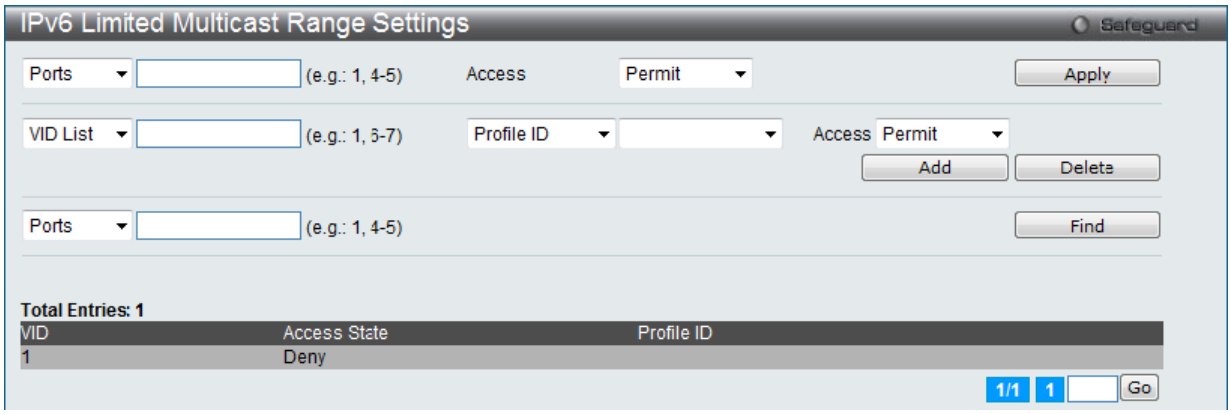


図 8-99　IPv6 Limited Multicast Range Settings 画面

以下の項目を使用して、設定します。

項目	説明
Ports / VID List	設定に使用するポート、VLAN ID を選択します。
Access	「Permit」「Deny」からアクセス設定をします。
Profile ID/Profile Name	プルダウンメニューを使用してプロファイル ID またはプロファイル名を指定します。

「Apply」ボタンをクリックして変更を適用します。「Add」ボタンをクリックして入力した情報に基づき新しいエントリを追加します。

新しいマルチキャストアドレス範囲の追加
適切な情報を入力し、「Add」ボタンをクリックします。

マルチキャストアドレス範囲の削除
情報を入力し、「Delete」ボタンをクリックします。

エントリの検索
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IPv6 Max Multicast Group Settings（IPv6 最大マルチキャストグループ設定）

最大のフィルタグループ（最大 1024 まで）に所属するスイッチポートを設定します。

L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Max Multicast Group Settings の順にメニューをクリックし、以下の画面を表示します。

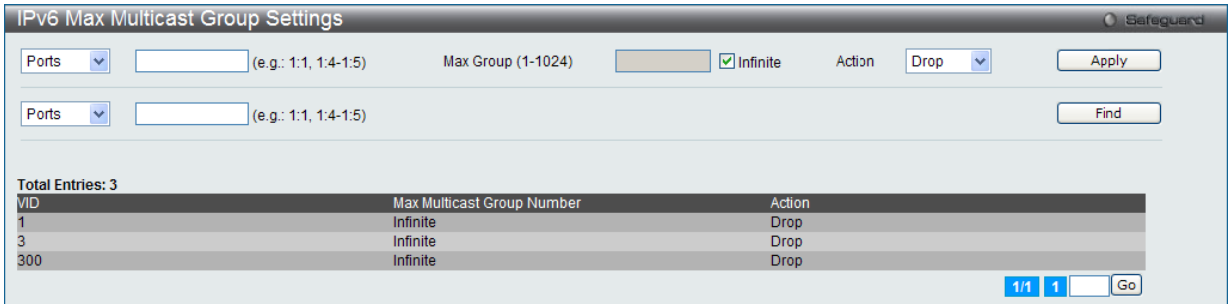


図 8-100　IPv6 Max Multicast Group Settings 画面

以下の項目を使用して、設定します。

項目	説明
Ports / VLAN ID	プルダウンメニューから「Ports」「VLAN ID」を選択します。
Max Group	マルチキャストグループの最大数を入力します。1 から 1024 の間で設定できます。「Infinite」を選択すると制限がありません。
Action	プルダウンメニューから登録が最大限に達した時、最新のグループの扱いについて選択します。 • Drop – 最新のグループを破棄します。 • Replace – 一番古いグループを最新のグループと入れ替えます。

適切な情報を入力し「Apply」ボタンをクリックします。

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 > IGMP Snooping > Multicast Filtering Mode の順にメニューをクリックします。

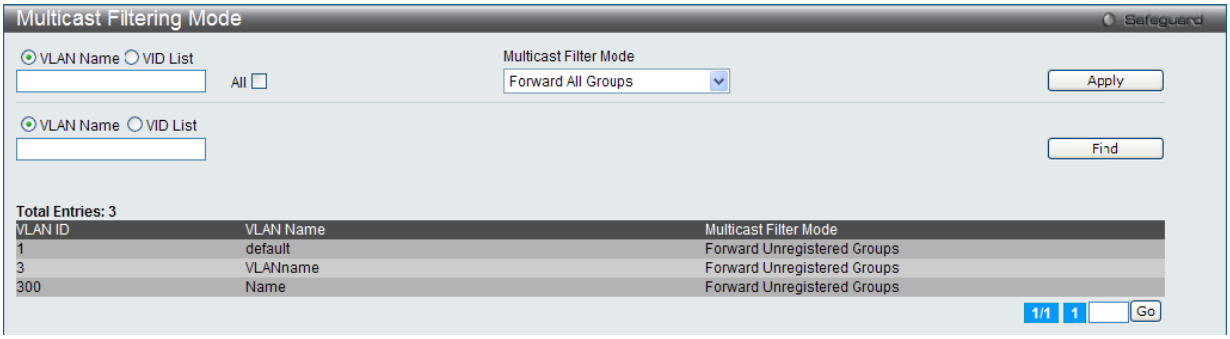


図 8-101　Multicast Filtering Mode 画面

以下の項目を使用して、設定します。

項目	説明
VLAN Name / VID List	「VLAN Name」か「VID List」を選択します。選択後下記の情報を入力します。
Multicast Filter Mode	プルダウンメニューを使用して Multicast パケットのフィルタ方法を選択します。 • Forward All Groups - VLAN に基づいて全てのマルチキャストグループは転送されます。 • Forward Unregistered Groups - 登録グループは登録テーブルに基づいて、転送されます。登録されていないグループは VLAN に基づいて転送されます。 • Filter Unregistered Groups - 登録グループは登録テーブルに基づいて転送され、登録されていないグループはフィルタされます。

適切な情報を入力し「Apply」ボタンをクリックします。

ERPS Settings（イーサネットリングプロテクション設定）（EI モードのみ）

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。

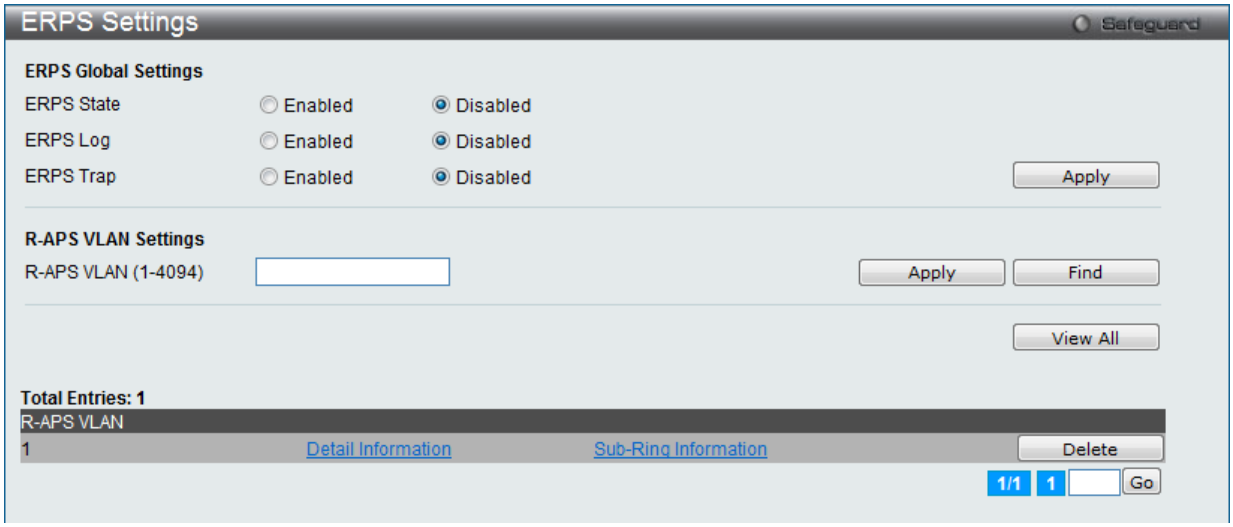


図 8-102 ERPS Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
ERPS Global Settings	
ERPS State	ERPS 状態を有効または無効にします。
ERPS Log	ERPS ログを有効または無効にします。
ERPS Trap	ERPS トラップを有効または無効にします。
R-APS VLAN Settings	
R-APS VLAN (1-4094)	R-APS VLAN とする VLAN を指定します。

エントリの追加

新しい R-APS VLAN を作成するためには、メニューで必要な項目の設定を行い、「Apply」ボタンをクリックします。

詳細情報の参照

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

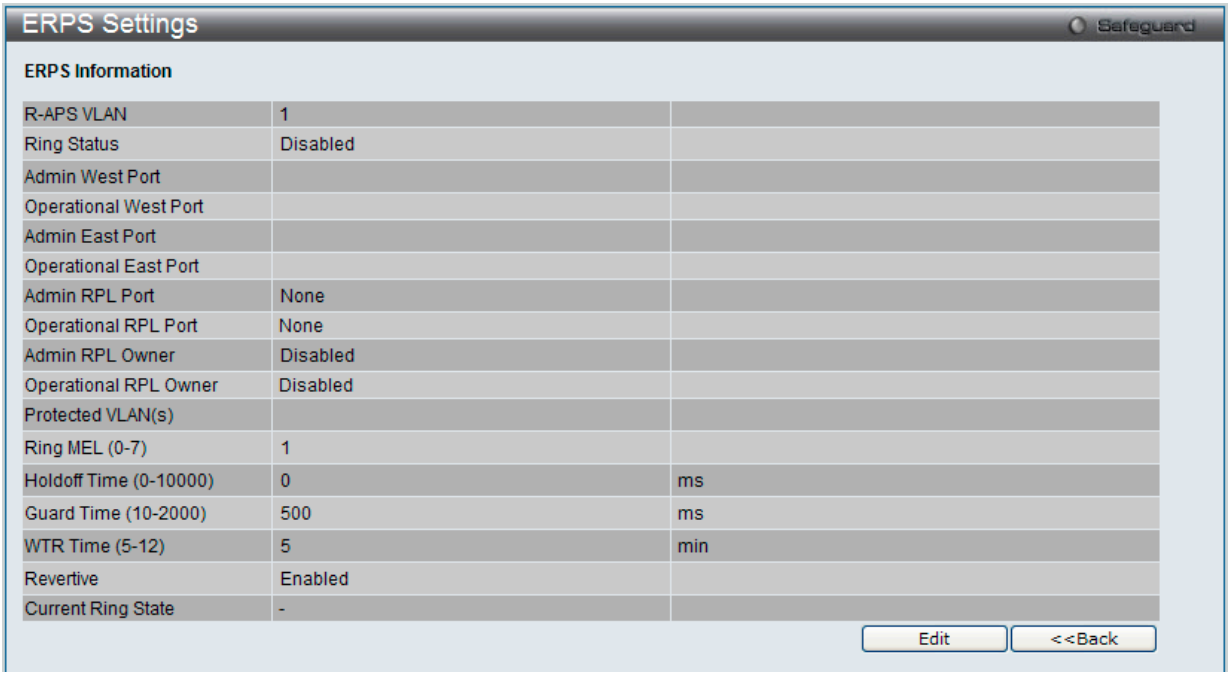


図 8-103 ERPS Settings 画面 - ERPS Information

エントリの編集

1. 「Edit」ボタンをクリックすると、画面上部に現在の設定が表示されます。

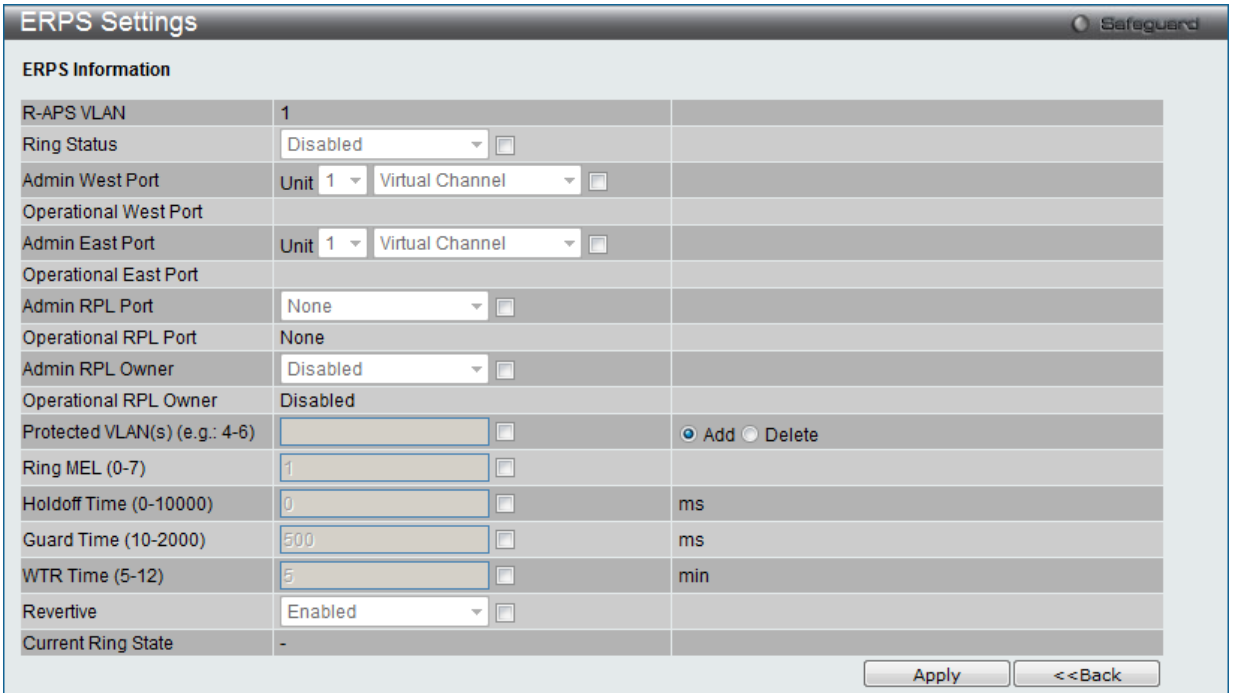


図 8-104 ERPS Settings 画面 - Edit

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 とする VLAN を指定します。
Ring Status	リングを有効 / 無効に設定します。
Admin West Port	West リングポートとしてポートを指定します。ERPS は、リング内のノードにおけるポートの方向付けのために「East」および「West」という基本的な方向を使用します。リング上の各ノードには、East ポートと West ポートがあります。あるノードの West ポートは、リング内の隣接ノードの East ポートにリンクされます。
Operational West Port	起動中の West port の状態が表示されます。
Admin East Port	East リングポートとしてポートを指定します。ERPS は、リング内のノードにおけるポートの方向付けのために「East」および「West」という基本的な方向を使用します。リング上の各ノードには、East ポートと West ポートがあります。あるノードの East ポートは、リング内の隣接ノードの West ポートにリンクされます。
Operational East Port	起動中の East port の状態が表示されます。
Admin RPL Port	Ring Protection Link (RPL : リングプロテクションリンク) ポートとしてリングポート（West / East / None）を指定します。RPL は、リング上のすべてのリンクが機能している時、待機状態のままでトラフィックをブロックします。しかし、リング上にリンク障害があると、RPL ポートは、リングの周りの代替経路を許可するために RPL オーナノードによってブロックを解除されます。
Operational RPL Port	起動中の RPL port の状態が表示されます。
Admin RPL Owner	デバイスを RPL オーナノードとして有効または無効にします。このノードは、ネットワーク状態により必要に応じて RPL をブロックまたはブロックを解除します。Ethernet Ring Automatic Protection Switching (R-APS) メッセージプロトコルは、リング上にある全ノードのプロテクション作業を調整します。リンク障害の場合、RPL オーナはエラーとなったリンクをブロックし、RPL のブロックを解除するためにこれらのメッセージを使用します。リング上には 1 つの RPL オーナのみ存在します。
Operational RPL Owner	起動中の RPL Owner 機器の状態が表示されます。
Protected VLANs	本コマンドは、ERPS 機能により防御される VLAN を設定するために使用されます。
Ring MEL	R-APS 機能のリング Maintenance Entity Group(MEG) レベル (MEL) を指定します。
Holdoff Time (0-10000)	R-APS 機能ホールドオフタイムを指定します。ホールドオフタイマは、複数のレベルで ERPS のタイミングを調整するのに使用されます。その目的は、例えば、サーバレイヤスイッチがクライアントレイヤに切り替えられる前に問題を修正できるようにすることです。 新しい不良またはさらにサーバの不良が検出される場合、イベントはすぐには報告されません。代わりに、ホールドオフタイマの期限が切れた後にタイマを始動した形跡を不良がまだ存在しているかどうか確認するためにチェックします。存在する場合、不良が報告され、ERPS は実施されます。
Guard Time (10-20000)	R-APS 機能のガードタイムを指定します。ガードタイマの動作中は、受信した R-APS メッセージを RPL オーナに転送しません。これは、2 つ以上の R-APS 信号エラーメッセージがリングのそれぞれの端から同時に送信される場合にループが形成される可能性を防ぐことです。
WTR Time (5-12)	R-APS 機能の WTR タイム（復帰までの待ち時間）を指定します。WTR タイムは、条件のクリア後に経過するのに必要な時間を定義します。WTR タイムの期限が切れた後に、RPL はアイドル状態に戻ります。(ブロック状態)。これは、断続的な信号エラーの検知による ERPS の過度の動作を防止するために使用されます。
Revertive	R-APS revertive オプションを指定します。
Current Ring State	現在のリングの状態を表示します。

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。

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。

サブリング情報

1. 「Sub-Ring Information」リンクをクリックすると、以下の画面が表示されます。

図 8-105　Sub-Ring Information 画面

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 です。
Sub-Ring R-APS VLAN	Sub-Ring R-APS VLAN ID を入力します。
State	ERPS Sub-Ring を Add /Delete から指定します。
TC Propagation State	TC Propagation を Enabled/Disabled から指定します。

2. 「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 ネットワークに接続するステーションの接続点の識別子を組み合わせることです。

本プロトコルによって送信される情報は、受信先によって標準の管理情報ベース（MIB）に格納されるので、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 Global Settings（LLDP グローバル設定）

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

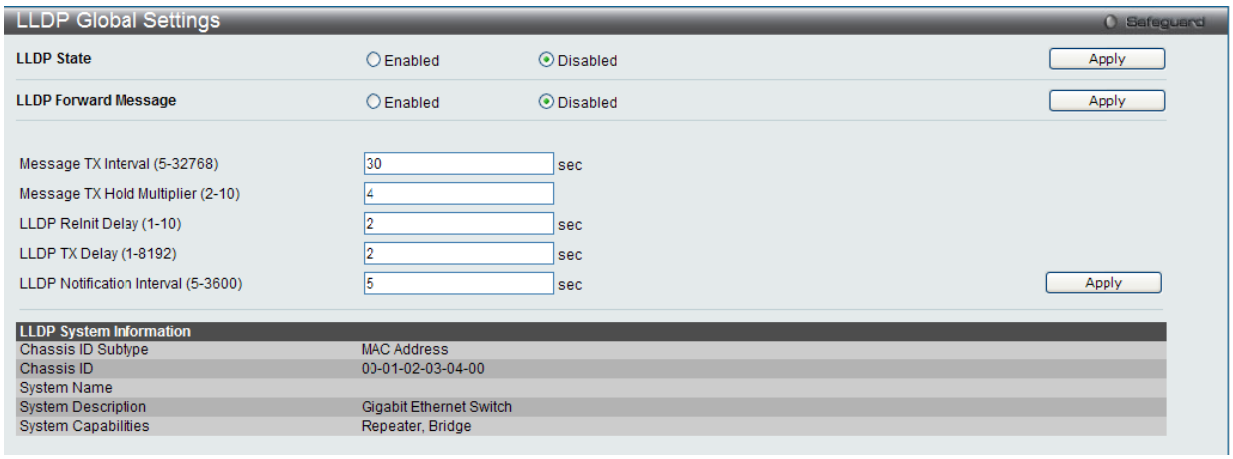


図 8-106　LLDP Global Settings 画面

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。
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最小時間です。LLDP Reinit Delay を変更するために、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時に定義済みの SNMP トラップレシーバに変更通知を送信する場合に使用されます。LLDP Notification Interval を設定するために、5-3600（秒）から値を入力します。

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

LLDP Port Settings（LLDP ポート設定）

LLDP ポートパラメータを設定します。

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

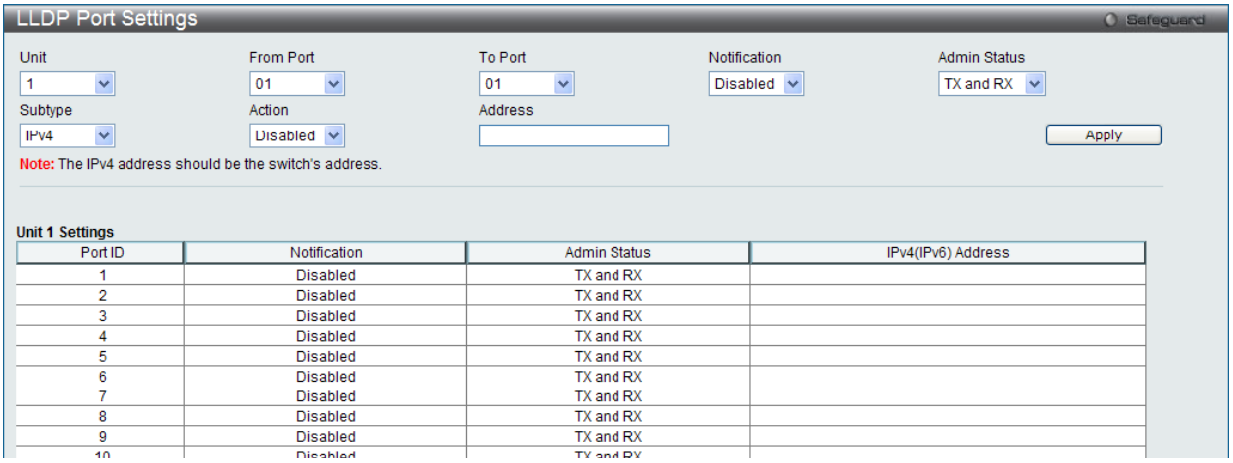


図 8-107　LLDP Port Settings 画面

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指定します。
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。
Admin Status	プルダウンメニューを通知のステータスを選択します。: Tx（送信のみ）、Rx（受信のみ）、Tx And Rx（送受信）または「Disabled」（無効）。
Subtype	プルダウンメニューを使用して送信する IP アドレスの種類を選択します。
IPv4 Address	通知するエンティティの管理アドレスを入力します。
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。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Management Address List（LLDP 管理アドレスリスト）

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

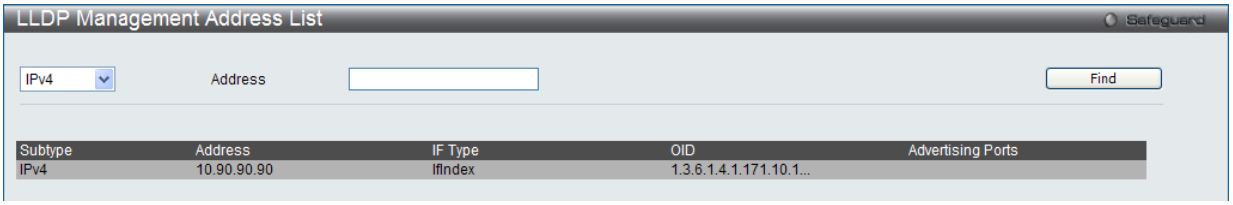


図 8-108　LLDP Management Address List 画面

以下の項目を設定できます。

項目	説明
IPv4/IPv6	通知するエンティティの管理 IP アドレスを選択します。
Address	管理 IP アドレスを入力します。

「Find」ボタンをクリックし、LLDP 管理情報を検索します。

LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）

本スイッチにおけるベーシック TLV 設定を有効にします。

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

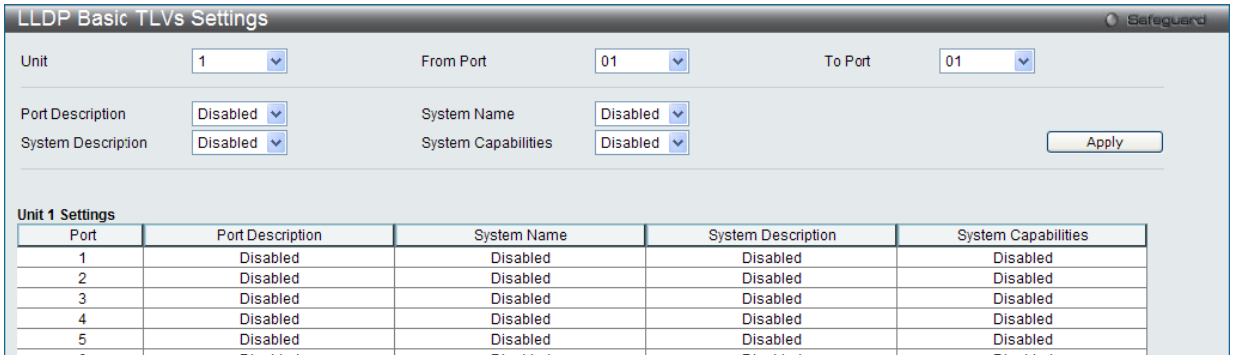


図 8-109　LLDP Basic TLVs Settings 画面

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
Unit	設定するユニットを指定します。
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	システム能力を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

LLDP Dot1 TLV は、IEEE 802.1 によって組織的に定義されている TLV で、送信する LLDP 通知から IEEE 802.1 規定のポート VLAN ID の TLV データタイプを除外するようにポートやポートグループを設定する時に使用します。

L2 Features > LLDP > LLDP > LLDP Dot1 TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

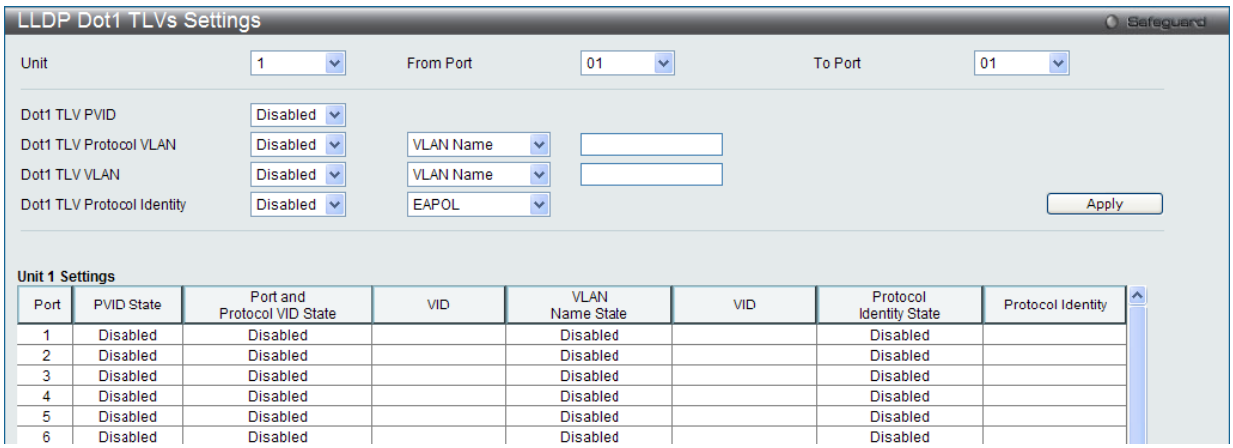


図 8-110　LLDP Dot1 TLVs Settings 画面

以下の項目が使用できます。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
PVID	PVID の通知を「Enabled」（有効）/「Disabled」（無効）にします。
Dot1 TLV Protocol VLAN ID	プロトコル VLAN ID の通知を「Enabled」（有効）/「Disabled」（無効）にします。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。 • VID - VLAN ID を指定します。 • All - すべてを対象とします。
Dot1 TLV VLAN	VLAN 名の通知を「Enabled」（有効）/「Disabled」（無効）にします。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。 • VID - VLAN ID を指定します。 • All - すべてを対象とします。
Dot1 TLV Protocol Identity	プロトコル識別子の通知を「Enabled」（有効）/「Disabled」（無効）にします。次に対象とするプロトコルを EAPOL、LACP、GVRP、STP または All から選択します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

個別のポートやポートグループが送信する LLDP 通知から IEEE 802.3 規定のポート VLAN ID TLV データタイプを除外するように設定します。

L2 Features > LLDP > LLDP > LLDP Dot3 TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

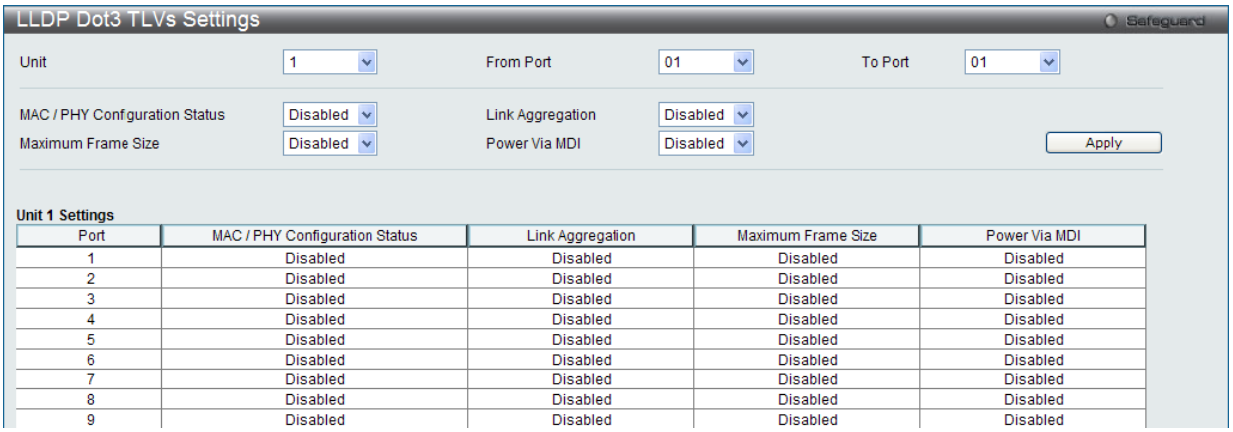


図 8-111　LLDP Dot3 TLVs Settings 画面

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指定します。
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。
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。
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。
Power Via MDI	プルダウンメニューを使用して、LLDP エージェントが MDI TLV を通した電力供給の有無を指定します。MDI TLV 経由の電力供給により、ネットワーク管理が通知を行い、送信する IEEE 802.3 LAN ステーション MDI 電力のサポート機能を検出します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Statistics System（LLDP 統計情報システム）

スイッチにおける LLDP 統計情報と各ポートの設定を参照できます。

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

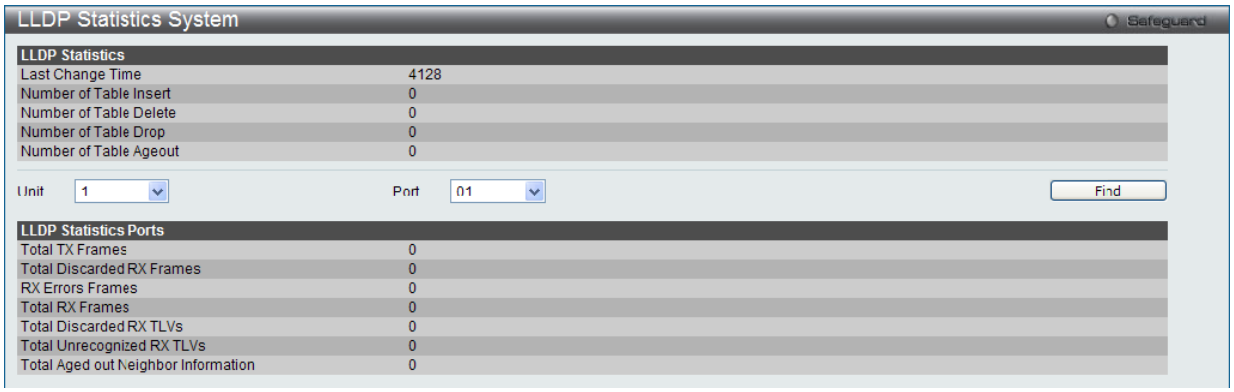


図 8-112　LLDP Statistics System 画面

プルダウンメニューを使用して、特定のユニット、ポートをチェックし、「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。

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

以下のローカルポートの要約テーブルにポートベースの情報を表示します。

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

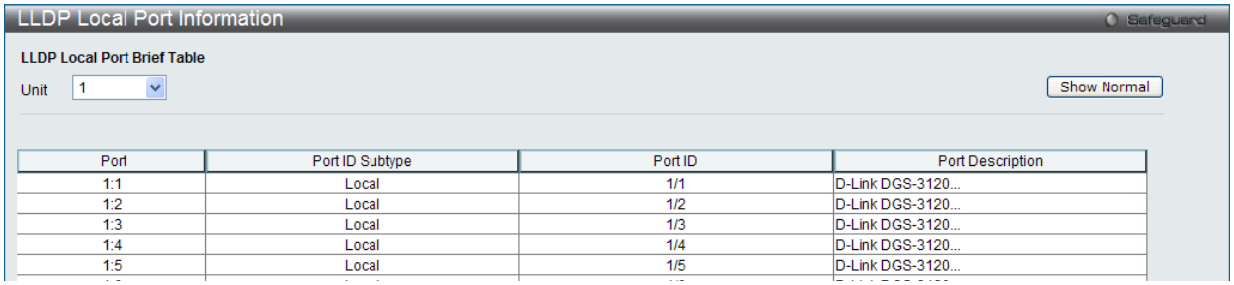


図 8-113　LLDP Local Port Information 画面

ポートベース情報の参照

ユニットを選択し、「Show Normal」ボタンをクリックし、以下の画面を表示します。

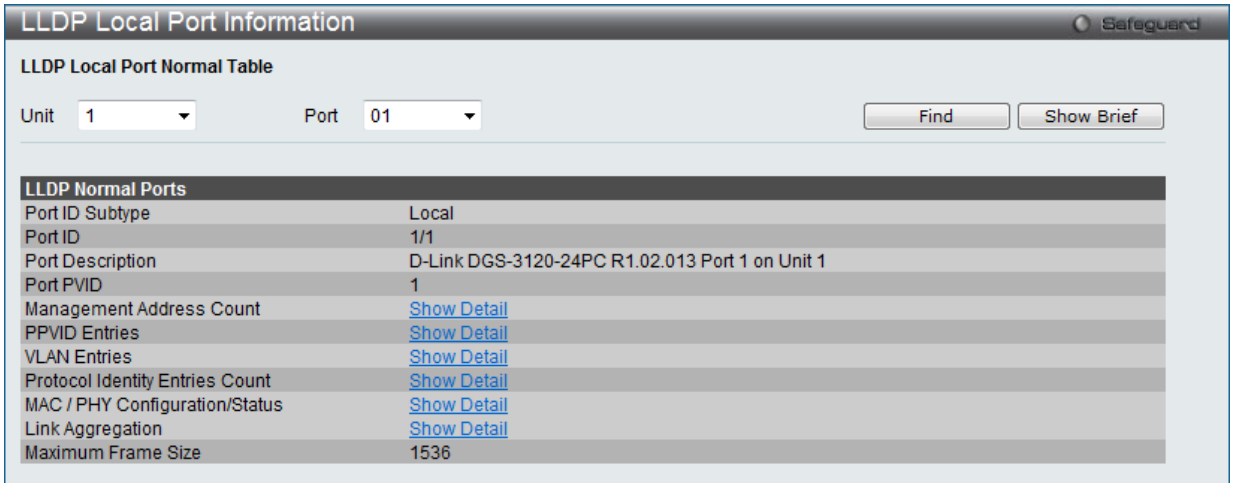


図 8-114　LLDP Local Port Information（Show Normal）画面

プルダウンメニューを使用して、ポートを選択し、「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。
前画面に戻るためには、「Show Brief」ボタンをクリックします。

各パラメータの詳細の参照

「Management Address Count」の「Show Detail」リンクをクリックし、以下の画面を表示します。

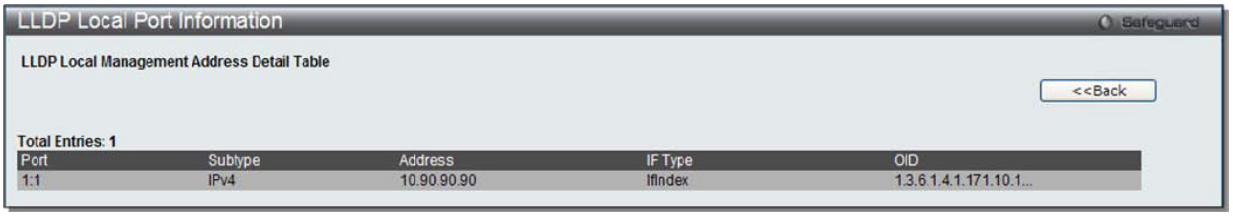


図 8-115　LLDP Local Port Information（Show Detail）画面

前画面に戻るためには、「<<Back」ボタンをクリックします。

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。

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

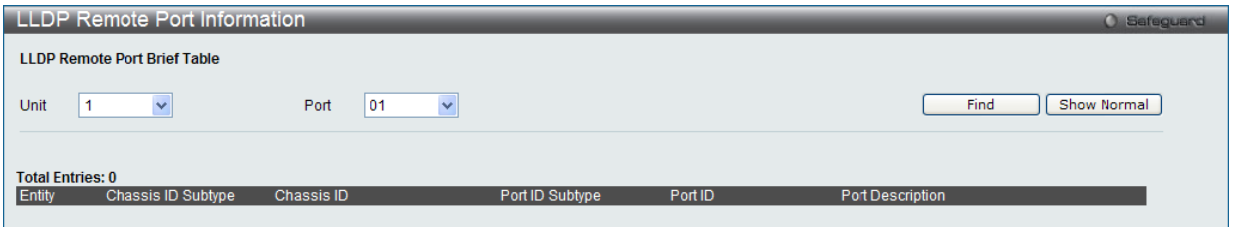


図 8-116　LLDP Remote Port Information 画面 - Brief

プルダウンメニューを使用して、ポートを選択し、「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。

各ポートの設定を参照する

ポートを選択し、「Show Normal」ボタンをクリックし、以下の画面を表示します。

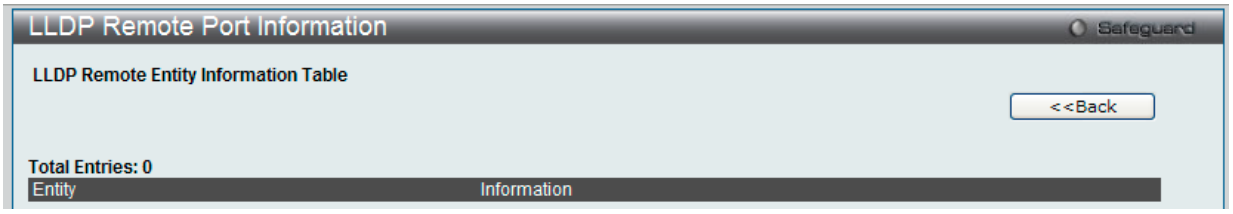


図 8-117　LLDP Remote Port Information 画面 - Normal

「<<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、専門的なケイパビリティと 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）

LLDP-MED のログ状態と「Fast Start Repeat Count」（ファストスタート実行回数）の設定と LLDP MED システム情報の表示を行います。

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。

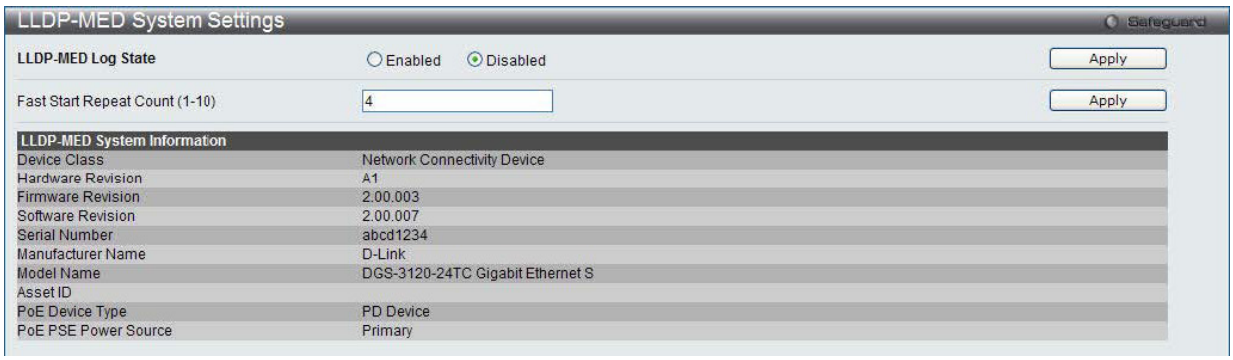


図 8-118　LLDP-MED System Settings 画面

以下の項目が使用できます。

項目	説明
LLDP-MED Log State	ラジオボタンを使用して LLDP-MED のログ状態を「Enabled」（有効）/「Disabled」（無効）にします。
Fast Start Repeat Count (1-10)	ファストスタート実行回数（1-10）を入力します。LLDP MED ケイパビリティの TLV が存在する LLDP リモートシステム MIB と関連しない MSAP 識別子で検出される場合、アプリケーションレイヤはファストスタートメカニズムを開始し、「medFastStart」タイマを「medFastStartRepeatCount」回数 1 に設定します。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。

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。

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。

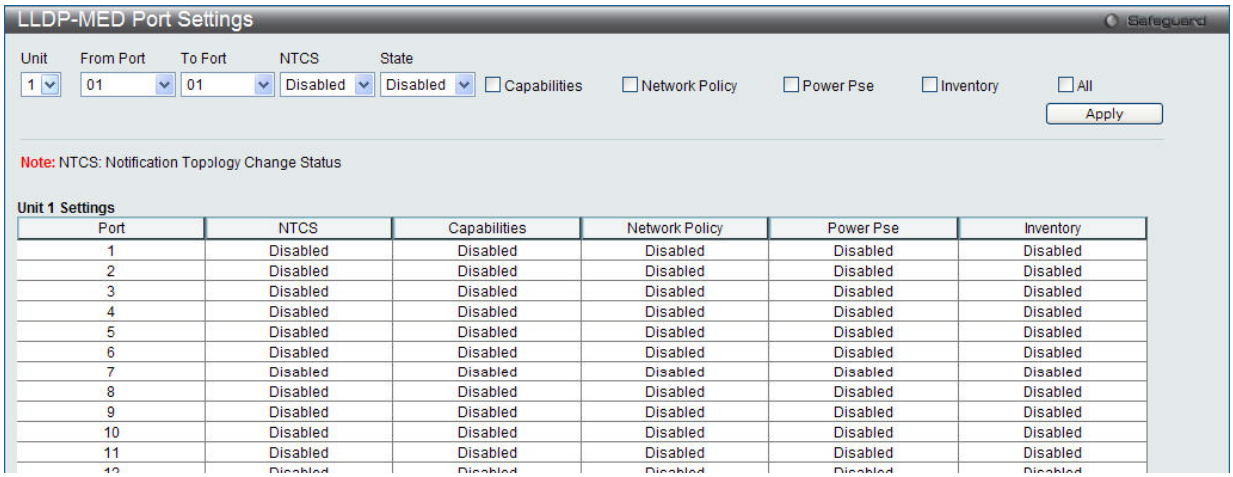


図 8-119　LLDP-MED Port Settings 画面

以下の項目が使用できます。

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。
Port Description	「Port Description」（ポート定義）を有効または無効にします。
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	「LLDP-MED TLV」の送信を有効または無効にします。また、LLDP エージェントが送信すべき TLV タイプをチェックします。TLV タイプは Capabilities、Network Policy、Power Pse、および Inventory です。「All」を選択すると、すべての TLV タイプを選択します。
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）

外向きの LLDP-MED 通知を組み込むためにポートごとの現在の情報を表示します。

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。

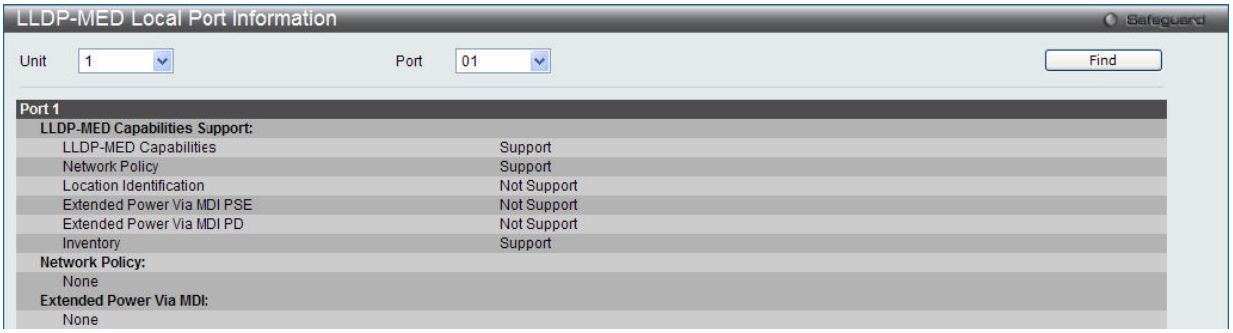


図 8-120　LLDP-MED Local Port Information 画面

「Unit」および「Port」を選択し、「Find」ボタンをクリックして、特定ポートの統計情報を参照します。

LLDP-MED Remote Port Information（LLDP-MED リモートポート情報）

Neighbor デバイスのパラメータから学習した情報を表示します。

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。

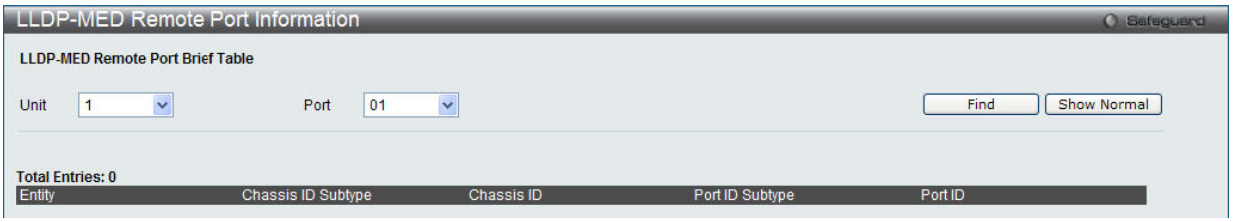


図 8-121　LLDP-MED Remote Port Information 画面 - Brief

ユニットおよび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。

ポートごとに LLDP リモートポート情報を参照するには、「Show Normal」ボタンをクリックします。

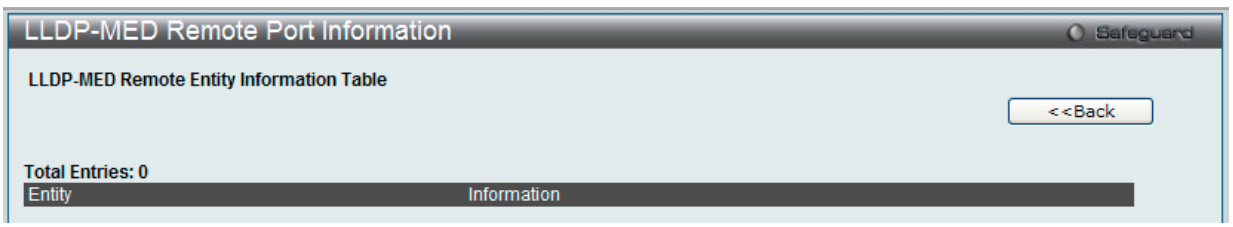


図 8-122　LLDP-MED Remote Port Information 画面 - Show Normal

「<<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）

本スイッチはネットワークロードバランシング (NLB) をサポートしています。これは、複数のサーバは同じ IP アドレスと MAC アドレスを共有する Microsoft サーバロードバランシングアプリケーションの 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このリクエストは、全てのサーバに転送されますが、その中の 1 つのみにより行われます。サーバは 2 つのモード「ユニキャストモード」と「マルチキャストモード」で動作可能です。ユニキャストモードの場合、クライアントはユニキャスト MAC アドレスをサーバへの宛先 MAC として使用します。マルチキャストモードではクライアントはマルチキャスト MAC アドレスをサーバへの宛先 MAC として使用します。宛先となる MAC は共有 MAC になります。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排他的な状態になります。

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

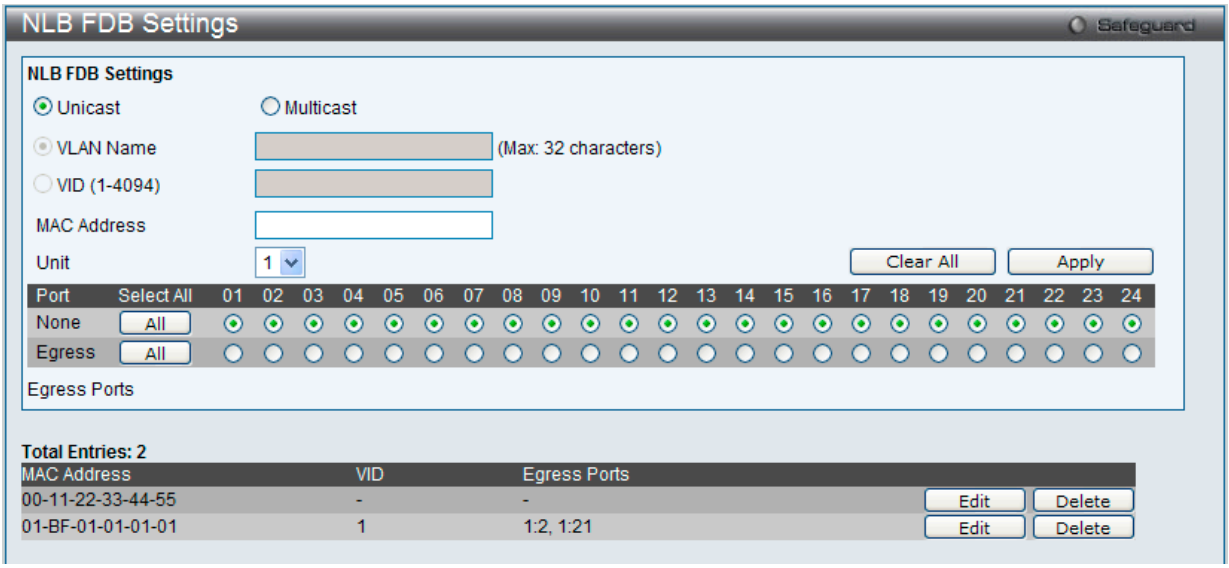


図 8-123　NLB FDB Settings 画面

以下の項目を設定または表示できます。

項目	説明
Unicast	NLB ユニキャスト FDB エントリを作成します。
Multicast	NLB マルチキャスト FDB エントリを作成します。
VLAN Name	ラジオボタンをクリックして、作成する NLB マルチキャスト FDB エントリの VLAN を入力します。
VID (1-4094)	ラジオボタンをクリックして VLAN ID を入力します。
MAC Address	作成する NLB マルチキャスト / ユニキャスト FDB エントリの MAC アドレスを入力します。
Unit	設定するユニットを選択します。
Ports	設定するポートを選択します。すべてのポートを選択する場合、「All」をクリックします。

「Apply」ボタンをクリックし、設定を適用します。

「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。

注意　物理スタックしているスイッチにおいて、L3 の NLB を行っているサーバを筐体またぎの LAG（リンクアグリゲーショングループ）では接続できません。物理スタックとの併用はしないでください。

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。

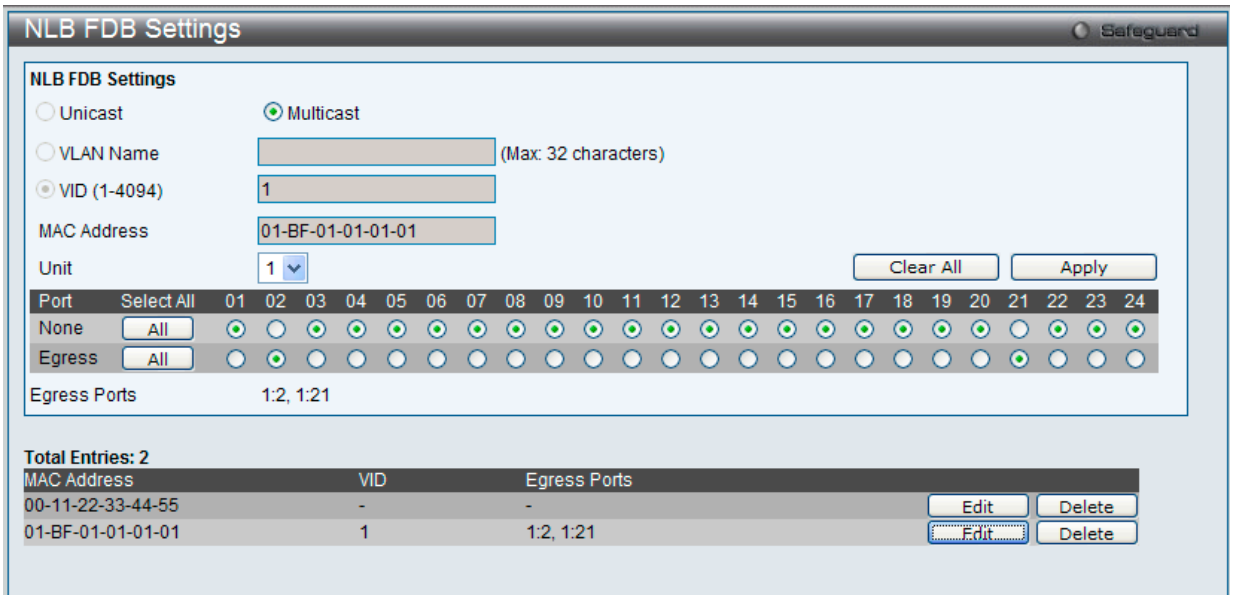


図 8-124　NLB FDB Settings 画面 - Edit

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 9 章　L3 Features（レイヤ 3 機能）

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 Default Route Settings（IPv4 デフォルトルート設定）（SI モードのみ）	IPv4 デフォルトルートを設定します。	184
IPv4 Static/Default Route Settings（IPv4 スタティック / デフォルトルート設定）（EI モードのみ）	IPv4 スタティック / デフォルトルートの設定を行います。	185
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。	186
IPv6 Static/Default Route Settings（IPv6 スタティック / デフォルトルート設定）（EI モードのみ）	IPv6 スタティック / デフォルトルートの設定を行います。	186
IPv6 Route Table（IPv6 ルートテーブル）（EI モードのみ）	IPv6 ルーティングテーブルの外部経路情報を参照します。	187
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。	187
Route Preference Settings（EI モードのみ）	スイッチのルートプリファレンス（経路選択）の設定をします。	187
ECMP Algorithm Settings（EI モードのみ）	ECMP ルートロードバランスアルゴリズムの設定をします。	188

IPv4 Default Route Settings（IPv4 デフォルトルート設定）（SI モードのみ）

IPv4 デフォルトルートを設定します。スイッチのフォワーディングテーブルには、IP アドレスサブネットマスクとゲートウェイのどちらの登録も可能です。

L3 Features > IPv4 Default Route Settings の順にメニューをクリックし、以下の画面を表示します。

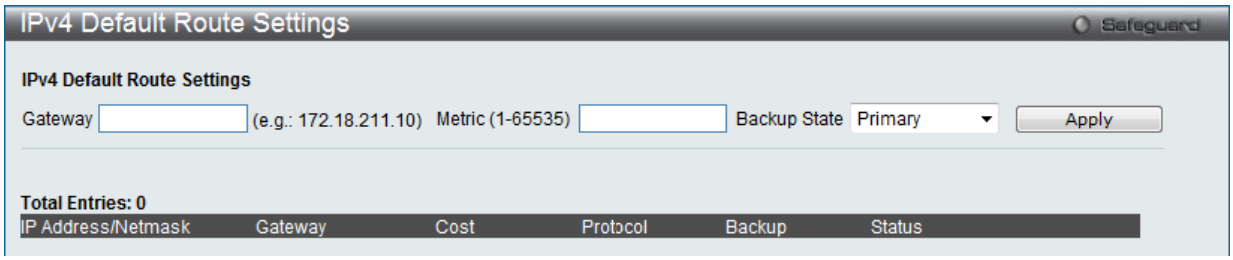


図 9-1　IPv4 Default Route Settings 画面

画面には以下の項目が表示されます。

項目	説明
Gateway	IP アドレスのゲートウェイアドレスを入力します。
Metric (1-65535)	テーブルに入力した IP インタフェースのメトリック値。範囲は 1-65535 です。
Backup State	作成したデフォルトルートのバックアップについて指定します。「Primary」と「Backup」から指定します。

「Apply」ボタンをクリックし、設定を有効にします。

IPv4 Static/Default Route Settings（IPv4 スタティック / デフォルトルート設定）（EI モードのみ）

本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。IPv4 でのスタティックルートを 512 エントリまで作成することができます。IPv4 スタティックルートにおいて、スタティックルートが設定されるとすぐに、スイッチはユーザにより設定されたネクストホップルータへ 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。

スイッチはフローティングスタティックルートもサポートしています。これは、異なるネクストホップに対して代替スタティックルートを作成することができることを意味しています。このセカンダリネクストホップデバイスルートは、プライマリスタティックルートがダウンした場合にバックアップスタティックルートとして動作します。プライマリルートが失われると、バックアップルートのステータスがアクティブになります。

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 9-2　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 / デフォルトルートの IP アドレス
Netmask	上記 IP アドレスのネットマスク
Gateway	上記 IP ルートのゲートウェイアドレス
Metric (1-65535)	IP ルートのメトリック値。範囲は 1-65535 です。
Protocol	IP ルートがルーティングテーブルとして使用するプロトコル。OSPF、RIP、スタティックまたはローカルが表示されます。
Backup State	IP ルートに設定されたバックアップ状態を表示します。「Primary」または「Backup」が表示されます。

「Apply」ボタンをクリックし、設定を有効にします。

エントリの削除
対象のエントリの行の「Delete」ボタンをクリックします。

IPv4 Route Table（IPv4 ルートテーブル）

IP ルーティングテーブルには、外部ルート情報が記載されています。

L3 Features > IPv4 Route Table の順にメニューをクリックし、以下の画面を表示します。

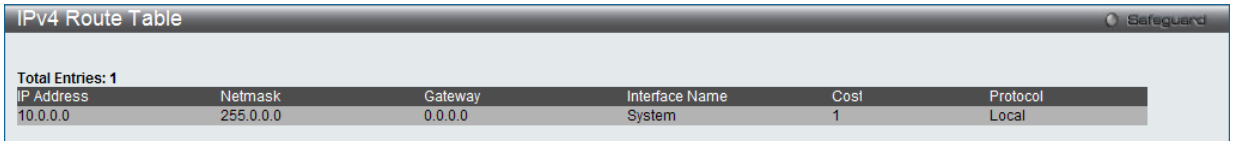


図 9-3　IPv4 Route Table（SI モード）画面

図 9-4　IPv4 Route Table（EI モード）画面

画面には以下の項目が表示されます。

項目	説明
Network Address	ラジオボタンをクリックし表示される宛先アドレスを入力します。
IP Address	ラジオボタンをクリックし表示される IP アドレスを入力します。一番長いルートに合致したプレフィクスが表示されます。
Hardware	チェックを入れるとチップに記録されたルートのみ表示されます。

「Apply」ボタンをクリックし、設定を有効にします。

IPv6 Static/Default Route Settings（IPv6 スタティック / デフォルトルート設定）（EI モードのみ）

本スイッチは 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。

L3 Features > IPv6 Static/Default Route Settings, の順にメニューをクリックし、以下の画面を表示します。

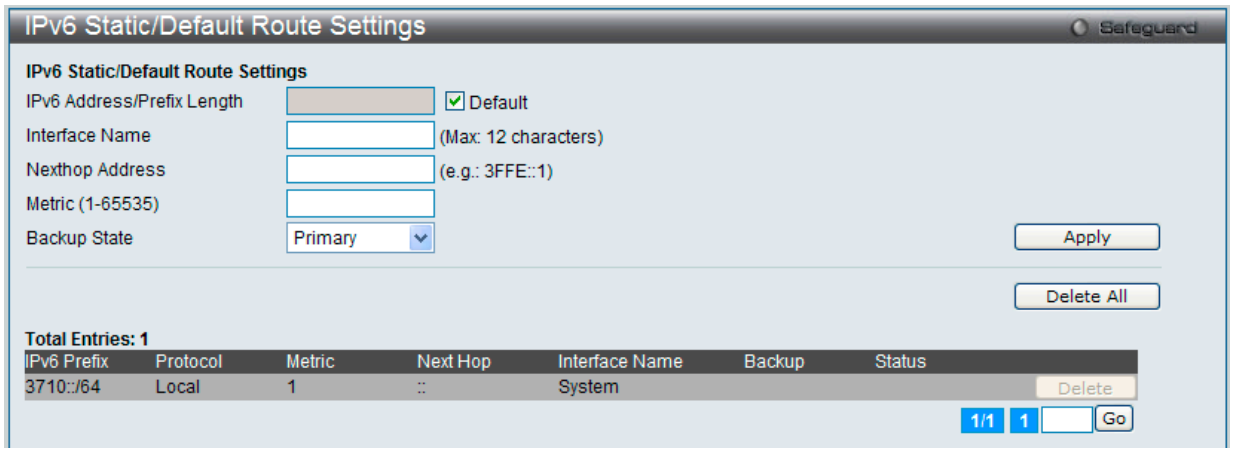


図 9-5　IPv6 Static/Default Route Settings 画面

画面には以下の項目が表示されます。

項目	説明
IPv6 Address/Prefix Length	スタティックルートの IPv6 アドレスを入力するか、「Default」をチェックしてデフォルトルートに割り当てます。
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
Next Hop 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
Metric (1-65535)	IPv6 インタフェースのメトリック値。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	スイッチの IPv6 ネットワーク接続のために本インタフェースの役割が「Primary」か「Backup」であるかを示します。

「Apply」ボタンをクリックし、設定を有効にします。

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）（EI モードのみ）

現在の IPv6 ルーティングテーブルを表示します。

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。

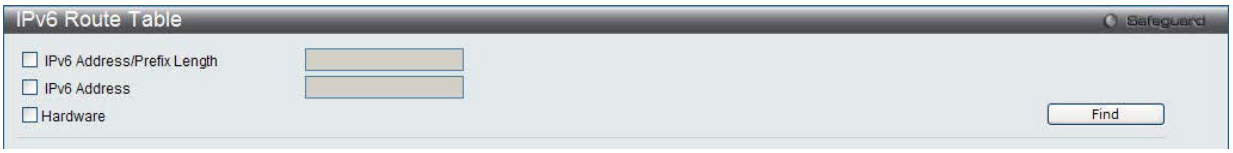


図 9-6　IPv6 Route Table 画面

画面には以下の項目が表示されます。

項目	説明
IPv6 Address/Prefix Length	チェックを行い、ルートの IPv6 宛先ネットワークアドレスを入力します。
IPv6 Address	チェックを行い、IPv6 アドレスを入力します。
Hardware	ハードウェアテーブル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。

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には全ての直接接続された IP 情報が保存されます。ユーザは直接接続された IP 情報を確認することができます。

L3 Features > IP 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 9-7　IP Forwarding Table 画面

「IP Address」「Interface Name」「Port」のどれかを選択し項目に入力、「Find」クリックし入力した情報に基づいたエントリを検索します。
複数のページにわたって検索結果が表示された場合、ページ番号を入力し「Go」をクリックすると指定のページへ移動します。

Route Preference Settings（ルートプリファレンス設定）（EI モードのみ）

スイッチのルートプリファレンス（経路選択）の設定をします。

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 9-8　Route Preference Settings 画面

画面には以下の項目が表示されます。

項目	説明
Static (1-999)	スタティックルートの経路を設定します。初期値は 60 です。
Default (1-999)	デフォルトルートの経路を設定します。初期値は 1 です。

「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）（EI モードのみ）

ECMP ルートロードバランスアルゴリズムの設定をします。

L3 Features > ECMP 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 9-9　ECMP Algorithm Settings 画面

画面には以下の項目が表示されます。

項目	説明
Destination IP	ECMP アルゴリズムが宛先 IP を含む場合チェックします。
Source IP	ECMP アルゴリズムが送信元 IP の低方から 5 ビットを含む場合チェックします。この属性は「CRC Low」と「CRC High」において相互排他的となります。設定した場合、「CRC Low」「CRC High」は除外されます。
CRC Low	ECMP アルゴリズムが CRC の低方から 5 ビットを含む場合チェックします。この属性は「送信元 IP」と「CRC High」において相互排他的となります。設定した場合、「送信元 IP」と「CRC High」は除外されます。
CRC High	ECMP アルゴリズムが CRC の高方から 5 ビットを含む場合チェックします。この属性は「送信元 IP」と「CRC Low」において相互排他的となります。設定した場合、「送信元 IP」と「CRC Low」は除外されます。
TCP/UDP Port	ECMP アルゴリズムが TCP/UDP ポートを含む場合チェックします。

「Apply」ボタンをクリックし、設定を有効にします。

第 10 章　QoS（QoS 機能の設定）

本スイッチは、802.1p キューイング QoS（Quality of Service）をサポートしています。QoS メニューを使用し、本スイッチにセキュリティ機能を設定することができます。

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

サブメニュー	説明	参照ページ
802.1p Settings（802.1p 設定）	ポート単位にプライオリティを割り当てます。次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設定）	191
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。次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）	192
Traffic Control Settings（トラフィックコントロール設定）	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。	194
DSCP（DSCP 設定）	DSCP トラスト設定、DSCP マップ設定を行います。次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）	196
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。	197
Scheduling Settings（QoS スケジュール設定）	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。 QoS Scheduling（QoS スケジュール作成）、QoS Scheduling Mechanism（QoS スケジュールメカニズム設定）	197
WRED（WRED 設定）	WRED の状態、ポート設定、プロファイル設定を行います。次のメニューがあります。 WRED Port Settings（WRED ポート設定）、WRED Profile Settings（WRED プロファイル設定）	199

以下の項では QoS の機能と、802.1p プライオリティキューイングを利用するメリットについて説明します。

QoS の長所

QoS は IEEE 802.1p 標準で規定される技術で、ネットワーク管理者に、VoIP（Voice-over Internet Protocol）、Web 閲覧用アプリケーション、ファイルサーバアプリケーション、またはビデオ会議などの広帯域を必要とする、または高い優先順位を持つ重要なサービスのために、帯域を予約する方法を提供します。より大きい帯域を作成可能なだけではなく他の重要度の低いトラフィックを制限することで、ネットワークが必要以上の帯域を使用しないようにします。スイッチは各物理ポートで受信した様々なアプリケーションからのパケットをプライオリティに基づき独立したハードウェアキューに振り分けます。以下の図に、802.1p プライオリティキューイングがどのように本スイッチに実装されているかを示しています。

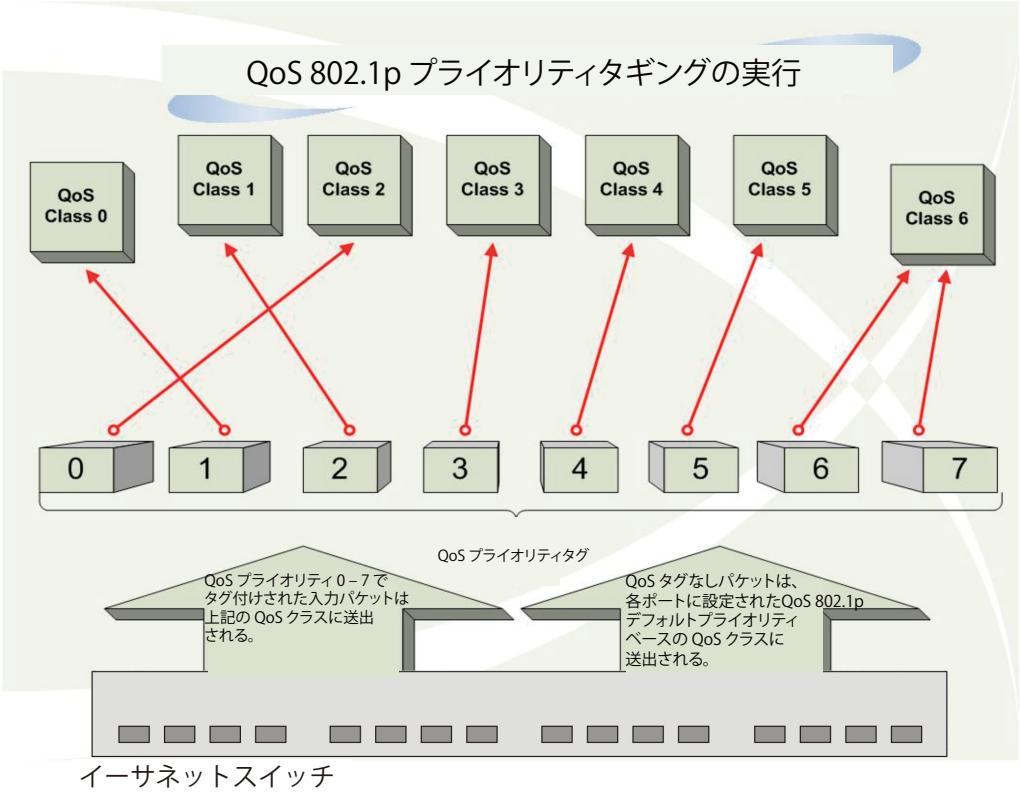


図 10-1　スイッチ上での QoS マッピングの例

上の図は本スイッチのプライオリティの初期設定です。クラス 7 はスイッチにおける 8 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

本スイッチは、802.1p プライオリティキューをサポートしており、8 個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 番キューから最低レベルの 0 番キューまでがあります。IEEE 802.1p（p0 から p7）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（Class of Service）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 CoS キューが同じ重み付けを持つならば、各 CoS 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。

802.1p Settings（802.1p 設定）

802.1p Default Priority（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。

QoS > 802.1p Settings > 802.1p Default Priority 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。

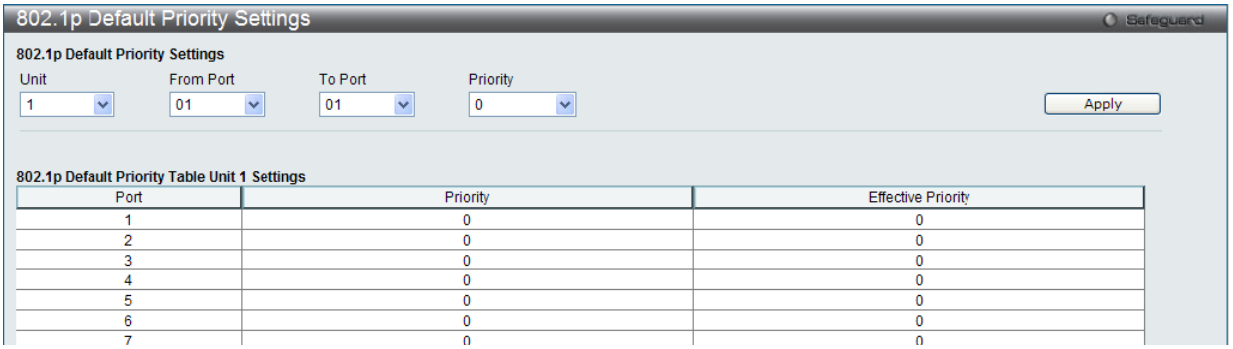


図 10-2　802.1p Default Priority 画面

本スイッチは、スイッチのそれぞれのポートにデフォルト 802.1p プライオリティをアサインすることができます。この画面はデフォルト 802.1p プライオリティをスイッチのポートにアサインする設定するために使用し、受信したアンタグパケットに 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もプライオリティの低い 0 から、最もプライオリティの高い 7 までをつけることができます。有効なプライオリティとは、RADIUS によりアサインされる実際のプライオリティを示します。RADIUS が指定した制限を超える値をアサインした場合は、デフォルトプライオリティが設定されます。例えば、RADIUS が 8 をアサインするとデフォルトプライオリティは 0、有効なプライオリティは 0 になります。

新しいデフォルトプライオリティを実行する

はじめに「From Port」、「To Port」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。

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

802.1p User Priority（802.1p ユーザプライオリティ設定）

スイッチは各 802.1p プライオリティにユーザプライオリティを割り当てることができます。

QoS > 802.1p Settings > 802.1p User Priority Settings の順にクリックし、以下の画面を表示します。

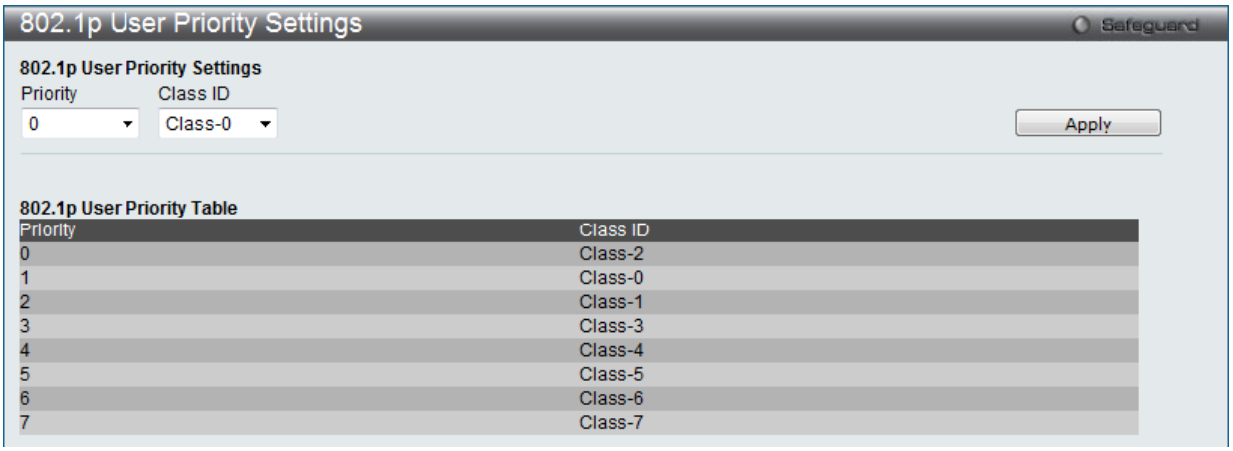


図 10-3　802.1P User Priority 画面

プライオリティはスイッチのポートグループにアサインされるとすぐに、クラスがこの画面のプルダウンメニューを使って設定された 802.1p プライオリティの 8 段階の値がアサインされます。ユーザプライオリティマッピングは最後のページで設定されたデフォルトプライオリティだけでなく 802.1p タグを持ったすべての入力タグパケットに対して行われます。

本画面には以下の項目があります。

項目	説明
Priority	キューに割り当てられるプライオリティを表示します。
Class ID	プライオリティを割り当てるクラス（キュー）を設定します。「Class-0」（クラス 0）は最も低い優先度のキューで、「Class-7」（クラス 7）が最も高くなります。

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

Bandwidth Control（帯域幅制御）

Bandwidth Control Settings（帯域幅設定）

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。

Effecticve RX/TX レートは、設定されたレートにマッチしていない場合には、スイッチポートの実際の帯域を参照します。これは、通常、帯域がより高いプライオリティリソース（RADIUS サーバのような）によってアサインされることを意味します。

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

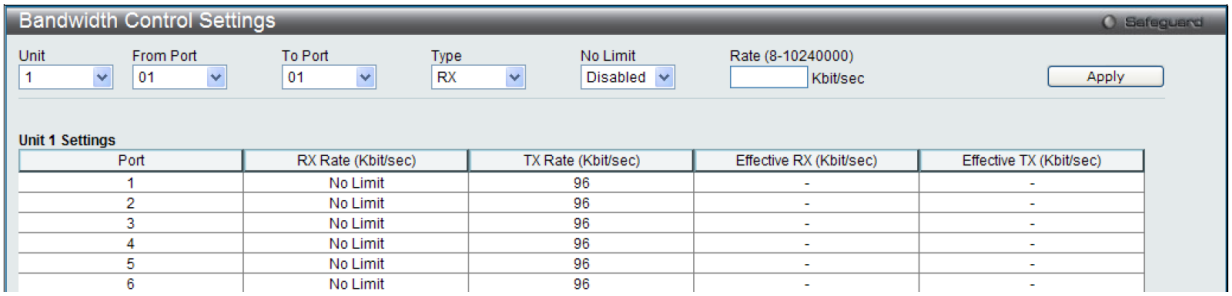


図 10-4　Bandwidth Control 画面

以下の項目を設定または表示できます。

項目	説明
Unit	設定するユニット名を選択します。
From Port	帯域幅設定を表示するポートグループの最初の番号を設定します。
To Port	帯域幅設定を表示するポートグループの最後の番号を設定します。
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	選択したポートで帯域制限を行うかどうかを指定します。 • 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** 設定した値がポートスピードよりも大きい場合、帯域制限なしとなります。
Rate (8-10240000)	指定したポートでのデータ速度の上限（Kbit/ 秒）。値は 8 から 1024000 の間の数を入力します。
Effective RX	RADIUS サーバが RX 帯域幅をアサインした場合、それが有効な RX 帯域幅となります。RADIUS サーバを使った認証はポート毎もしくはユーザ毎に行うことができます。ユーザ毎の認証においては、複数のユーザがこの特定ポートに接続されている場合複数の RX 帯域幅がアサインされる可能性があります。最終的な RX 帯域幅はこれらの複数の RX 帯域幅の中で最も大きいものになります。
Effective TX	RADIUS サーバが TX 帯域幅をアサインした場合、それが有効な TX 帯域幅となります。RADIUS サーバを使った認証はポート毎もしくはユーザ毎に行うことができます。ユーザ毎の認証においては、複数のユーザがこの特定ポートに接続されている場合複数の TX 帯域幅がアサインされる可能性があります。最終的な TX 帯域幅はこれらの複数の RX 帯域幅の中で最も大きいものになります。

「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（キュー毎帯域制御設定）

ポートに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。

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

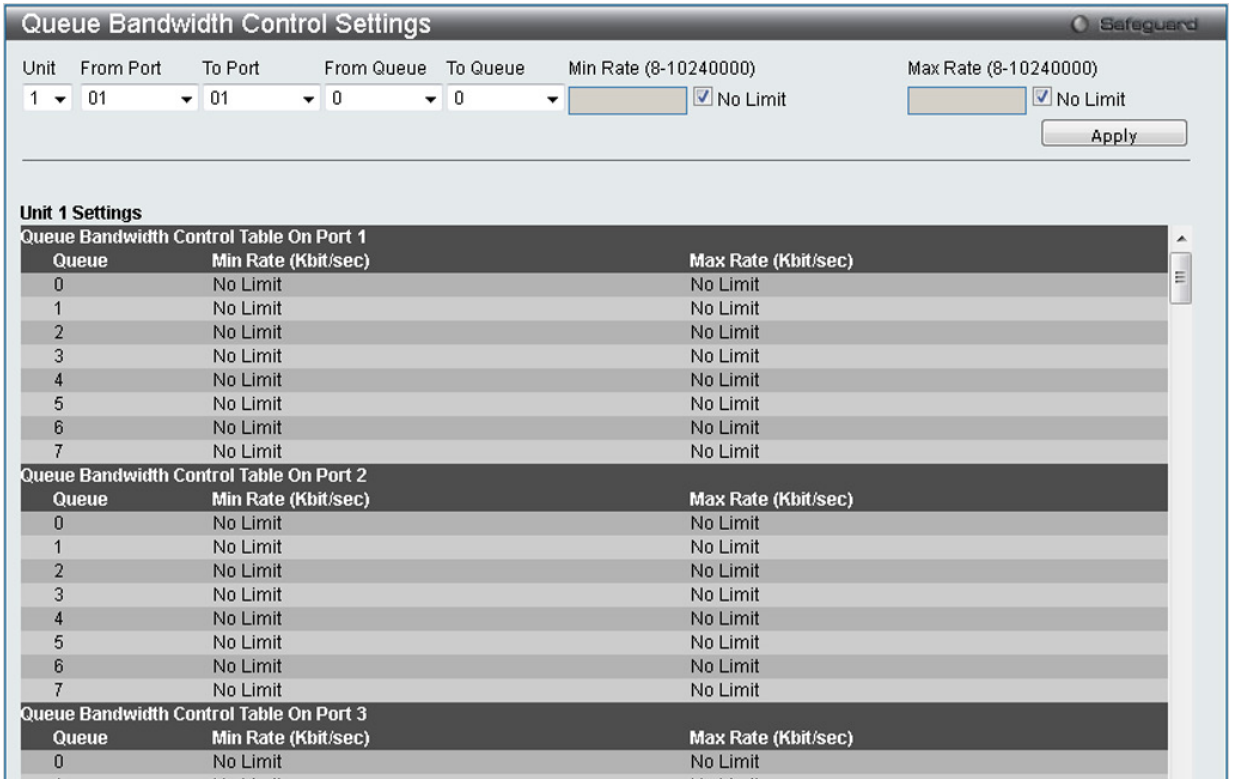


図 10-5　Queue Bandwidth Control Settings 画面

以下の項目を設定または表示できます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。
From Queue / To Queue	この設定に使用するキュー範囲を選択します。
Min Rate (8-10240000)	ポートが受信できるパケット制限 (Kbps) を指定します。「No Limit」をチェックすると指定キューが受信するパケットにレート制限がなくなります。
Max Rate (8-10240000)	キューの最大レートを入力します。「No Limit」オプションを選択すると、レート制限はなくなります。

「Apply」ボタンをクリックして行った変更を適用します。

注意　キュー帯域幅制御の最小グラニュラリティは 64Kbps です。システムは自動的に 64 倍の数に調整します。

Traffic Control Settings（トラフィックコントロールの設定）

コンピュータネットワーク上にはマルチキャストパケットやブロードキャストパケットなどのパケットが正常な状態でも絶えずあふれています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどが誤動作することにより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を基にパケットがネットワークにあふれているどうか判断します。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」欄で「Drop」オプションを設定します。

スイッチのチップカウンタを監視することによりスイッチに入力するパケットのスキャンとモニタを行います。チップにはブロードキャストとマルチキャストパケット用のカウンタのみ存在するため、この方法はブロードキャストストームとマルチキャストストームに対してのみ有効です。ストームが検出されると（次に示す画面で設定するパケット数のしきい値を超過すると）、スイッチは 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、「Count Down」欄で指定した時間、ポートをシャットダウンします。
トラフィックコントロールでポートに設定された時間間隔パラメータ時間を経過してもパケットストームが継続している場合、そのポートは「Shutdown Forever」（永久シャットダウン）になり、トラップレシーバに対して警告メッセージを送信します。一度「Shutdown Forever」モードになった場合には、System Configuration > Port configuration > Port Settings 画面を使って手動でポートを回復させるか、Traffic Auto Recover Time 欄で設定した時間が経過後、自動的に回復させる方法でポートを回復させます。無効となったポートを選択し、有効な状態に戻します。この方法を使用するためには以下の画面の「Action」欄で「Shutdown」オプションを選択します。
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するために本画面を使用します。

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

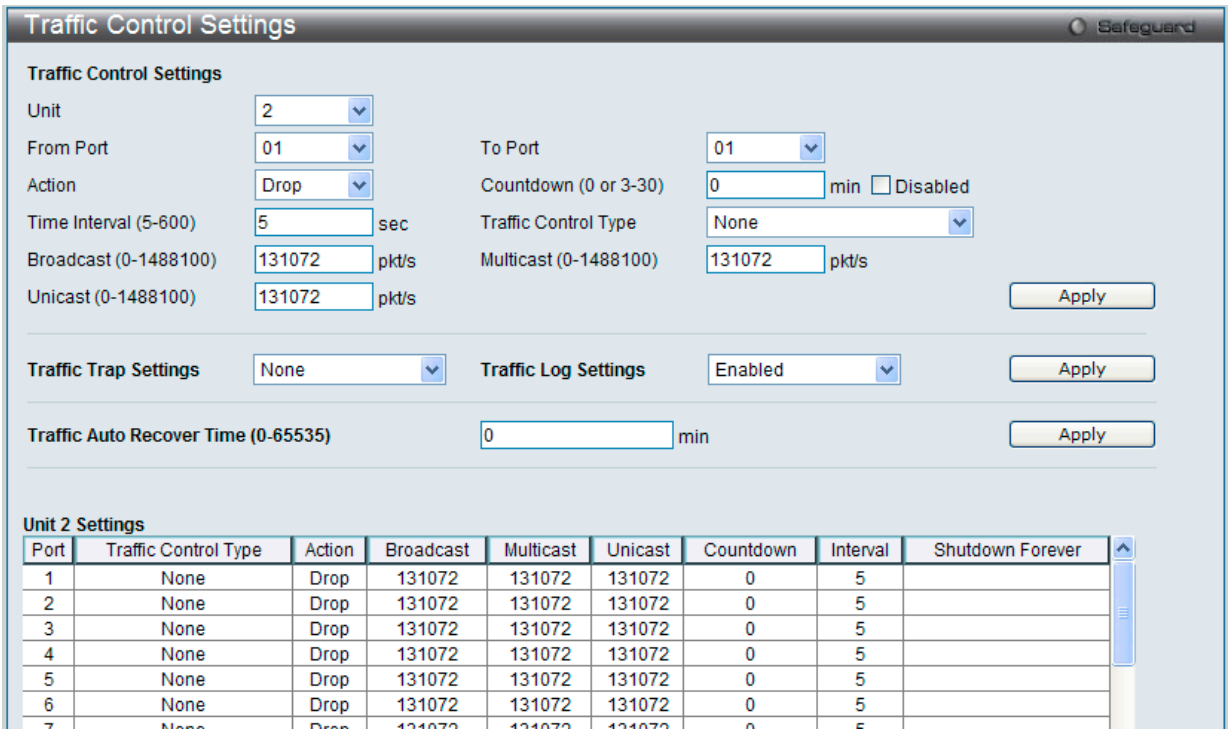


図 10-6　Traffic Control Settings 画面

本画面には次の項目があります。

項目	説明
Traffic Control Settings	
Unit	設定を行うユニットを指定します。
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いてパケットストームを判断し、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トラフィックコントロールメカニズムを利用してパケットストーム発生を判断します。検知するとすぐにポートは、スイッチでスパニングツリーを動作させるために不可欠な STP BPDU パケットを除くポートに入ってくるすべてのトラフィックを破棄します。カウントダウンタイマー経過後もまだパケットストームが続いている場合には、ポートは「Shutdown Forever」（永久シャットダウン）モードに移行し、ポートが 5 分後に自動的に回復するかポート設定画面（「**System Configuration> Port Configuration> Port Settings**」）を使って手動でポートをリセットするまで動作しません。このオプションを選択すると Interval 設定が必須となり、パケットストームが発生しているかどうかを判断するためにスイッチチップからパケット数のサンプリングを提供します。
Countdown (0 or 3-30)	スイッチがトラフィックストームによってポートを閉鎖するまでの時間を指定します。この項目は「Action」で「Shutdown」が指定されている時のみ有効で、ハードウェアベースのトラフィックコントロールでは使用できません。値の範囲は、0 および 3-30（分）です。0 はポートは、シャットダウン状態を無効として、シャットダウンされることはありません。
Time Interval (5-600)	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。値の範囲は 5-600 で、初期値は 5（秒）です。
Traffic Control Type	検知の対象となるストームの種類を「None」、「Broadcast」、「Multicast」、「Unicast」、「Broadcast + Multicast」、「Broadcast + Unicast」、「Multicast + Unicast」、「Broadcast + Multicast + Unicast」から選択します。選択後、「State」メニューを使用して、本ストーム検知を「Enable」（有効）/「Disable」（無効）にします。
Broadcast (0-1488100)	ストームトラフィックコントロール測定のトリガーとなるスイッチが受信するブロードキャスト（pps）の値を入力します。
Multicast (0-1488100)	ストームトラフィックコントロール測定のトリガーとなるスイッチが受信するマルチキャスト（pps）の値を入力します。
Unicast (0-1488100)	ストームトラフィックコントロール測定のトリガーとなるスイッチが受信するユニキャスト（pps）の値を入力します。
Traffic Trap Setting	
Traffic Trap Settings	トラフィックストームに基づくトラフィックコントロール機能による動作に応じて以下のそれぞれの状況でストームトラップメッセージを送ります。 • None - トラフィックコントロールメカニズムによる動作にかかわらずストームトラップ警告メッセージを送りません。 • Storm Occurred - トラフィックストームの発生時のみストームトラップ警告メッセージを送ります。 • Storm Cleared - スイッチによりトラフィックストームを収束できた時のみストームトラップメッセージを送ります。 • Both - トラフィックストームの発生時、スイッチによりトラフィックストームを収束できた時の両方で、ストームトラップメッセージを送ります。 本機能は、ハードウェアモード中（「Action」欄で「Drop」が選択された時）は実行できません。
Traffic Log Settings	プルダウンメニューを使用して「有効」「無効」を選択します。有効にするとストームの発生時 / 終息時のログを記録します。無効の場合トラフィックコントロールに関するイベントはログとして記録されません。
Traffic Auto Recover Time (0-65535)	ポートシャットダウンからの復帰の時間を入力します。初期値は 0 です。この場合自動リカバリが動作しておらずポートはシャットダウンしたまま復帰しません。CLI コマンドの「config ports [<portlist> | all] state enable」でポートをフォワーディングステートに復帰させる必要があります。

「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行うことができません。

注意 「Shutdown Forever」モードになったポートは、これらのポートがスイッチの CPU に BPDU パケットを転送していたとしても Spanning Tree 画面でも機能上でも「Discarding」になります。

注意 「Shutdown Forever」モードになったポートはユーザがこれらのポートを復旧するまですべての画面上でリンクダウンとして表示されます。

注意 ギガポートでのストームコントロールの最小グラニュラリティは 1pps です。

DSCP（DSCP 設定）

DSCP Trust Settings（DSCP トラスト設定）

本スイッチにおけるポートへの DSCP トラスト設定機能を有効にします。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 Map を使用してプライオリティタグをタグなしパケットに挿入します。

QoS > DSCP > DSCP Trust 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。

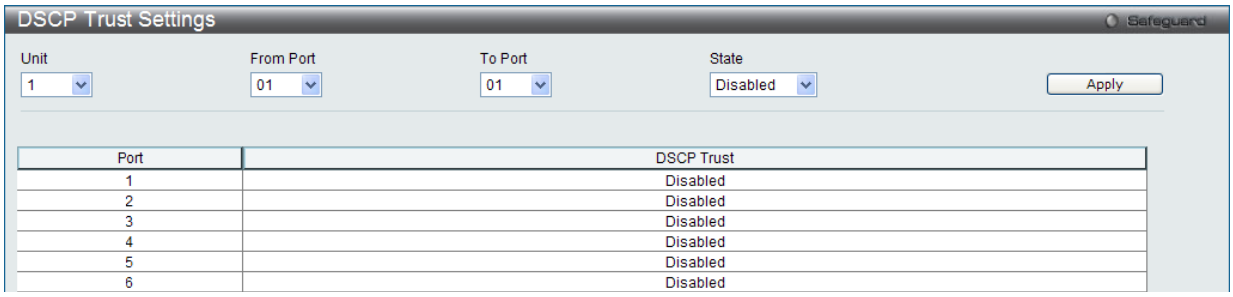


図 10-7　DSCP Trust Settings 画面

「From Port」および「To Port」で有効にするポートを選択し、その「State」を選択して「Apply」ボタンをクリックします。

DSCP Map Settings（DSCP マップ設定）

本スイッチにおける DSCP マップ設定機能を有効にします。ポートが DSCP トラストモードの場合、キューへの DSCP マッピングでパケットの優先値は決定します（スケジューリングキューも決定する）。「DSCP-to-DSCP」マッピングはパケットがポートに入る時に、パケットの DSCP を交換する機能です。新しい DSCP に基づきパケットのプロセスは残ります。初期値では DSCP は同じ DSCP にマッピングされます。

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

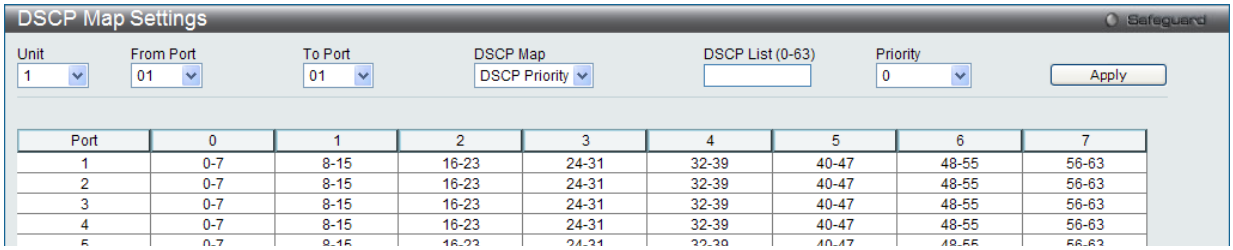


図 10-8　DSCP Map Settings - DSCP Priority 画面

QoS > DSCP > DSCP Map Settings の順にメニューをクリックし、「DSCP Map」のメニューから「DSCP DSCP」を選択すると以下の画面を表示します。

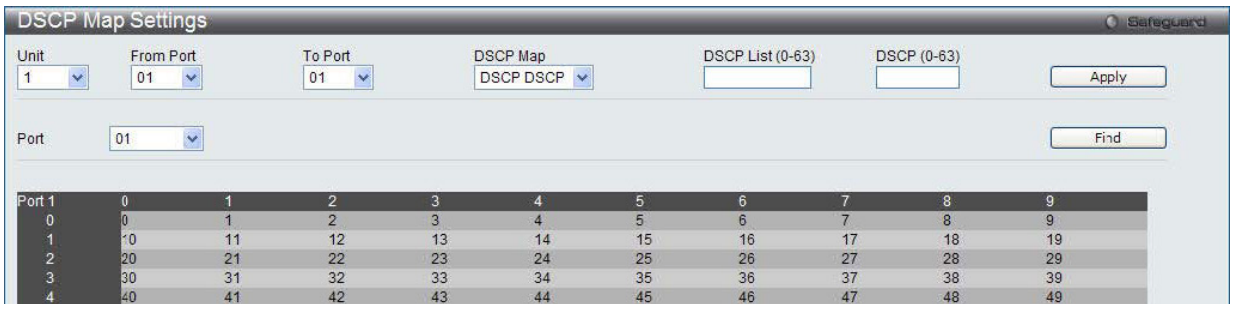


図 10-9　DSCP Map Settings DSCP to DSCP 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
DSCP Map	プルダウンメニューを使用して、DSCP マップ（DSCP Priority、DSCP DSCP）を選択します。
DSCP List (0-63)	DSCP リストの値を入力します。0 から 63 の範囲で設定します。
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。本フィールドを選択すると、スイッチが受信したパケットの中の、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。
DSCP (0-63)	DSCP 値を入力します。これは、「DSCP MAP」で「DSCP DSCP」を選択した場合にのみ表示されます。
Port	プルダウンメニューでポートを選択します。

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。

HOL Blocking Prevention（HOL ブロッキング防止）

ブロードキャストもしくはマルチキャストパケットの送信先ポートの一つが輻輳状態になった場合に HOL（Head of Line）ブロッキングが発生します。本スイッチは輻輳状態でない場合に他の送信先ポートがパケットを転送しない場合にでもバッファにこのパケットを保持します。HOL ブロッキング防止は、遅延を抑えより良いパフォーマンスを保つため、輻輳ポートを無視し、直接パケットを転送します。

この画面では HOL ブロッキング防止機能を有効化もしくは無効化します。

QoS > HOL Blocking Prevention の順にメニューをクリックし、以下の画面を表示します。

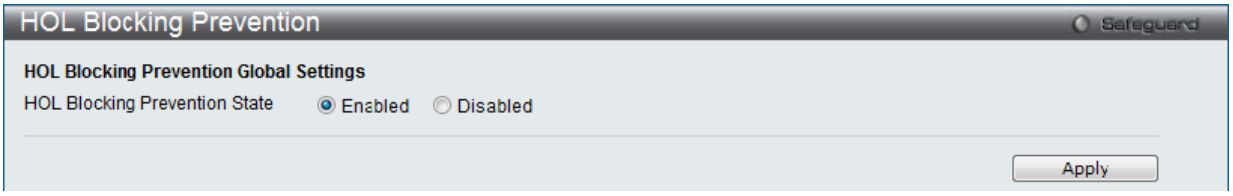


図 10-10 HOL Blocking Prevention 画面

「Enabled」（有効）または「Disabled」（無効）を選択し、「Apply」ボタンをクリックします。

Scheduling Settings（スケジュール設定）

QoS Scheduling（QoS スケジュール）

この画面はスイッチが 802.1p ユーザプライオリティに基づいてそれぞれのポートでの入力パケットを本スイッチで利用可能な 8 つのハードウェアプライオリティキューの一つにマッピングする方法を設定します。

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

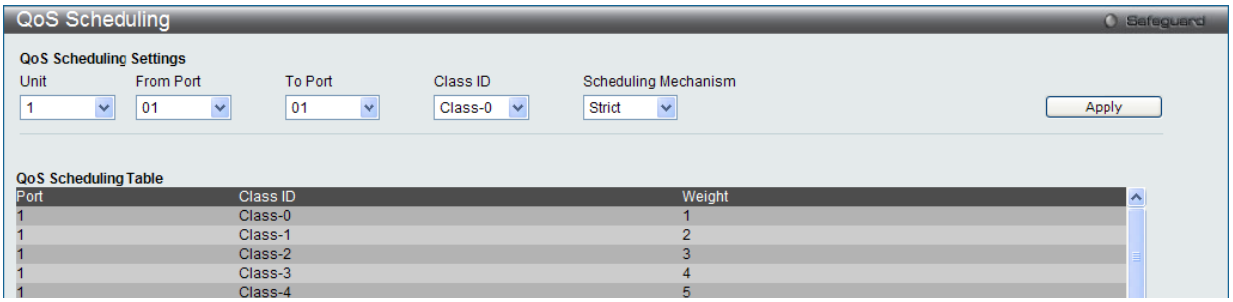


図 10-11 QoS Scheduling 画面

本画面には以下の項目があります。

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 / ポート範囲を入力します。
Class ID	QoS パラメータ設定のクラス ID を選択します。
Scheduling Mechanism	QoS におけるクラス（キュー）のスケジューリング方式を設定します。 • Strict - 最も高いサービスクラスのトラフィックを最初に処理します。最も高いサービスクラスの処理は他のキューが空になる前に完了します。 • WRR - プライオリティのサービスクラスで配分されたパケットを重み付けされたラウンドロビン（WRR）アルゴリズムによって処理します。

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。

QoS Scheduling Mechanism（QoS スケジュールメカニズムの設定）

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のネットワークパフォーマンスをモニタしながら行うことが重要です。

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

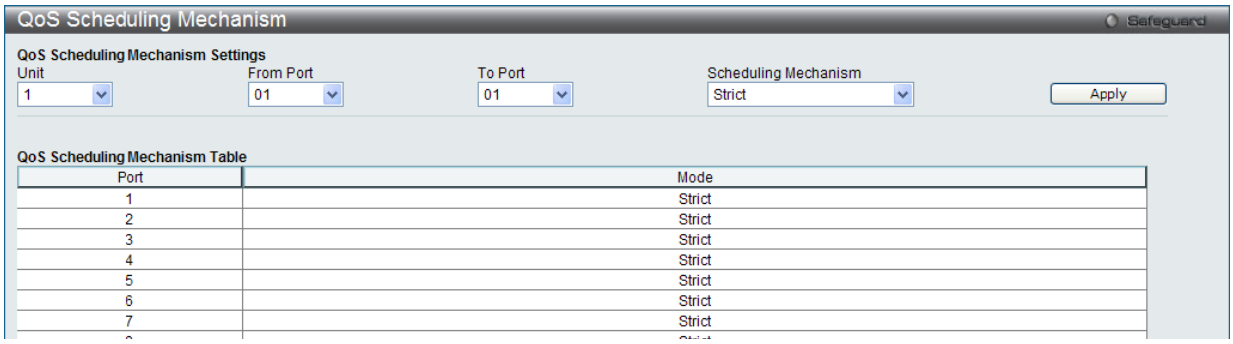


図 10-12　QoS Scheduling Mechanism 画面

本画面には以下の項目があります。

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 / ポート範囲を入力します。
Scheduling Mechanism	QoS におけるクラス（キュー）のスケジューリング方式を設定します。 • Strict - 最も高いサービスクラスのトラフィックを最初に処理します。最も高いサービスクラスの処理は他のキューが空になる前に完了します。 • WRR - プライオリティのサービスクラスで配分されたパケットを重み付けされたラウンドロビン（WRR）アルゴリズムによって処理します。

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

注意　キューに割り当てる 0 から 7 の番号は IEEE 802.1p プライオリティタグの番号を表しています。ポート番号の指定ではない点にご注意ください。

WRED（WRED 設定）

WRED Port Settings（WRED ポート設定）

WRED の状態とそのポート設定を行います。

QoS > WRED > WRED 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。

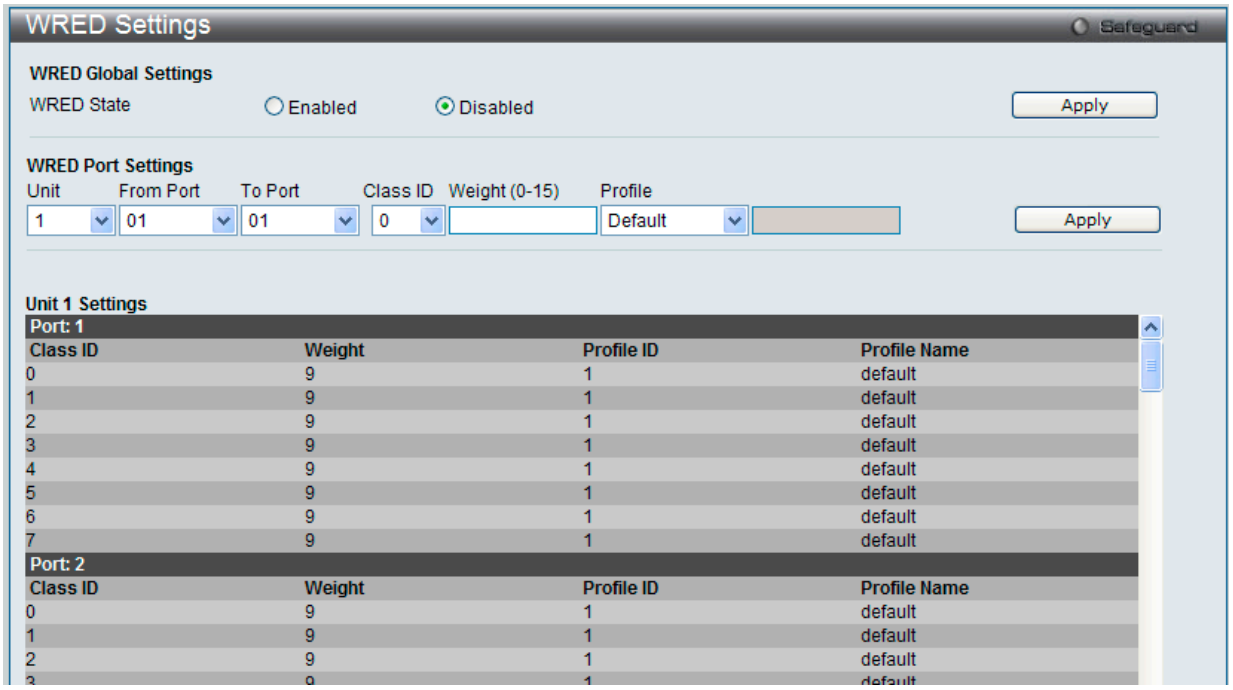


図 10-13　WRED Settings 画面

本画面には以下の項目があります。

項目	説明
WRED Global Settings	
WRED State	WRED グローバル状態を有効または無効にします。
WRED Port Settings	
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。
Class ID	プルダウンメニューを使用してハードウェアの優先度を選択します。
Weight (0-15)	通常のキューサイズ計算における重み付けを指定します。
Profile	プルダウンメニューを使用して、WERD ポートとキューに使用するプロファイルを選択します。 • Default - 使用するプロファイルの初期値を指定します。 • Profile ID - 選択して、使用するプロファイル ID を指定します。 • Profile Name - 選択して、使用するプロファイル名を指定します。

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。

WRED Profile Settings（WRED プロファイル設定）

WRED プロファイル設定を行います。

QoS > WRED > WRED 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。

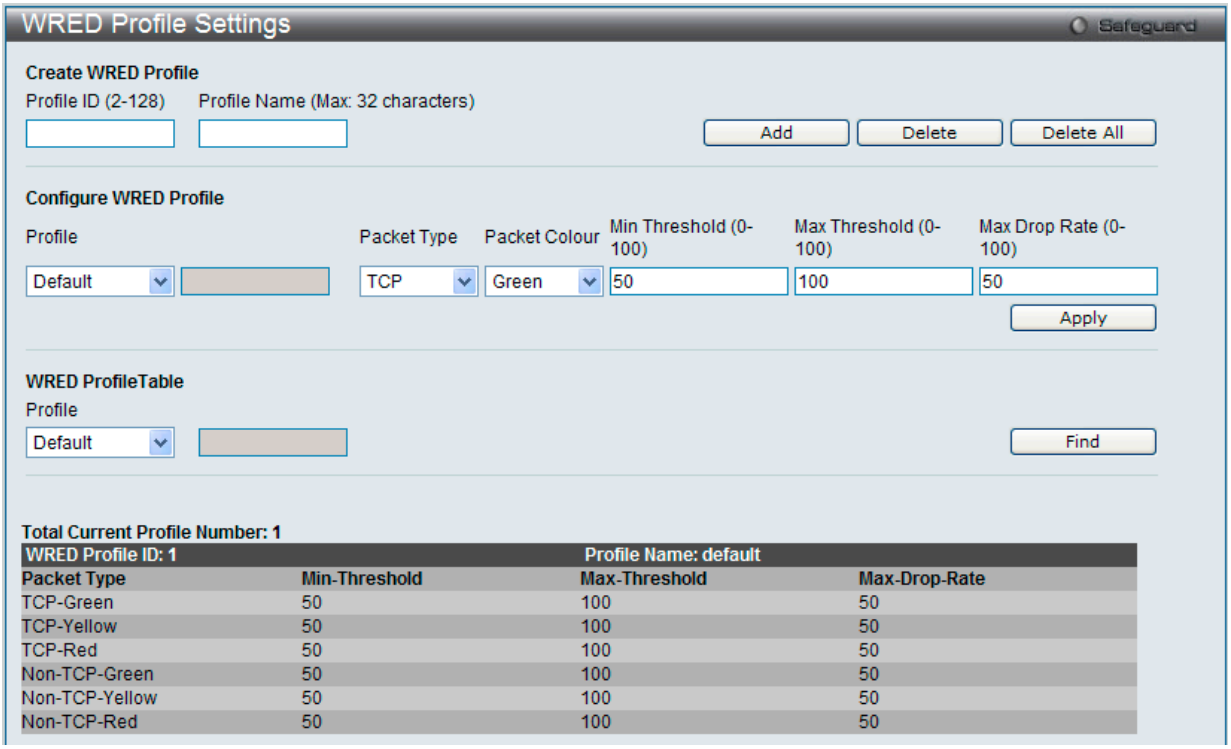


図 10-14　WRED Profile Settings 画面

本画面には以下の項目があります。

項目	説明
Create WRED Profile	
Profile ID (2-128)	追加または削除する WRED プロファイル ID を入力します。
Profile Name	追加または削除する WRED プロファイル名を入力します。
Configure WRED Profile	
Profile	プルダウンメニューを使用して、WERD ポートとキューに使用するプロファイルを選択します。 • Default - 使用するプロファイルの初期値を指定します。 • Profile ID - 選択して、使用するプロファイル ID を指定します。 • Profile Name - 選択して、使用するプロファイル名を指定します。
Packet Type	破棄するパケットタイプ（TCP または Non-TCP）を選択します。
Packet Colour	破棄するパケットカラー（Green、Yellow または Red）を選択します。
Min Threshold (0-100)	使用するしきい値（最小）を入力します。キューサイズがこの値より高いと、カラー「Yellow」が割り当てられます。キューサイズがこの値より低いと、カラー「Green」が割り当てられ、破棄されないことを保証されます。「Yellow」パケットの動作は、このカラーのプロファイル設定に依存します。
Max Threshold (0-100)	使用するしきい値（最大）を入力します。キューサイズがこの値より低いと、カラー「Yellow」が割り当てられます。キューサイズがこの値より高いと、カラー「Red」が割り当てられ、破棄されます。「Yellow」パケットの動作は、このカラーのプロファイル設定に依存します。
Max Drop Rate (0-100)	最大の破棄レートの値を入力します。

「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。
「Delete」ボタンをクリックして、入力した情報に基づいて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。
「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。

第 11 章　ACL（ACL 機能の設定）

ACL メニューを使用し、本スイッチにアクセスプロファイルおよびルールの設定を行うことができます。

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

サブメニュー	説明	参照ページ
ACL Configuration Wizard（ACL 設定ウィザード）	ウィザードを使用してアクセスプロファイルとルールを作成します。	201
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。	202
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。	218
ACL Finder（ACL 検索）	ACL エントリを検索します。	
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。	232
Egress Access Profile List（イーグレスアクセスプロファイルリスト）(EI モードのみ)	フローごとのパケット処理を実行します。	236
Egress ACL Flow Meter（Egress ACL フローメータリング）(EI モードのみ)	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。	246

ACL Configuration Wizard（ACL 設定ウィザード）

ACL 設定ウィザードは、アクセスプロファイルと ACL ルールの新規作成を行います。また、ACL ウィザードは自動的にアクセスルールとプロファイルを作成します。

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

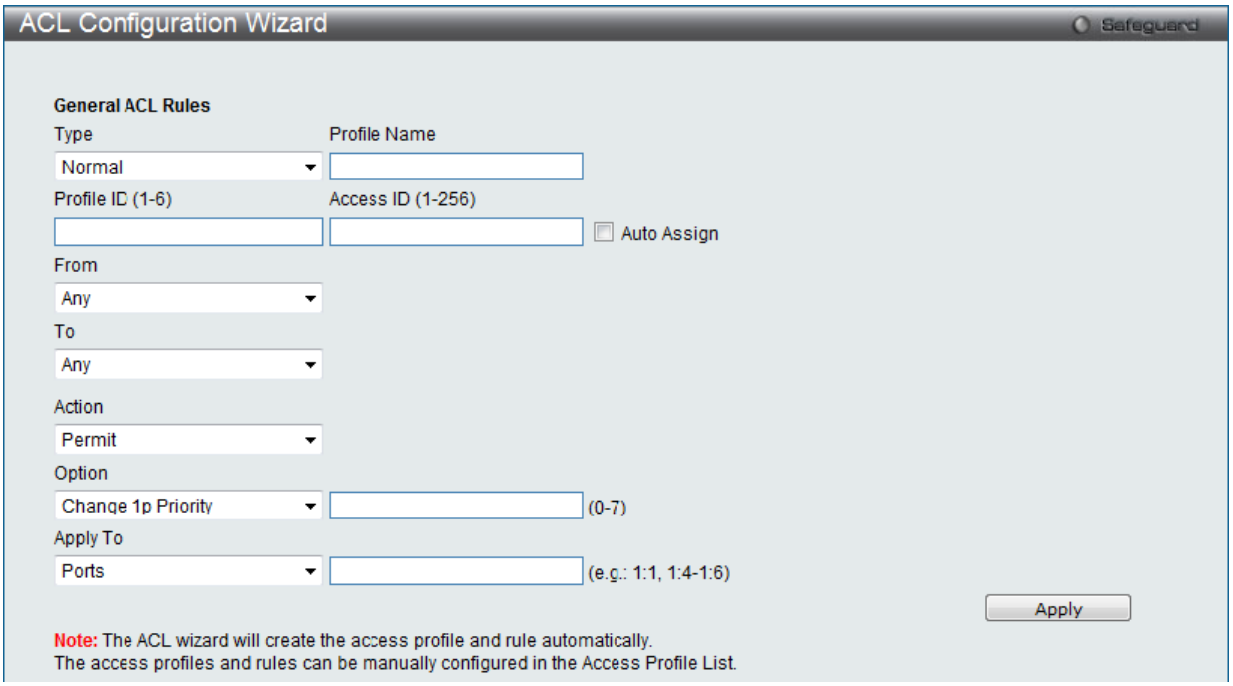


図 11-1　ACL Configuration Wizard 画面

1. ACL の種類 (Normal または CPU) を選択します。「Normal」を選択すると、スイッチのインタフェースの 1 つに受信したパケットに適用される ACL ルールを作成します。「CPU」を選択すると、スイッチに送信されるパケットにだけ適用される ACL ルールを作成します。
2. Profile ID (1-6) と Access ID (1-256) 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 の種類を選択します。 • Normal - ノーマル ACL ルールを選択します。 • CPU - CPU ACL ルールを選択します。 • Egress (EI モードのみ) - イーグレス ACL ルールを選択します。
Profile Name	プロファイル設定用の固有のプロファイル名を指定します。
Profile ID (1-6)	プロファイル設定用の固有の識別番号を指定します。低い値ほど高い優先度を示します。
Access ID (1-256)	本アクセスの識別番号を入力します。低い値ほど高い優先度を示します。
From	プルダウンメニューを使用して「Any」「MAC Address」、「IPv4 Address」または「IPv6 Address」（EI のみ）を選択します。
To	プルダウンメニューを使用して「Any」「MAC Address」、「IPv4 Address」または「IPv6 Address」（EI のみ）を選択します。「IPv6 Address」を選択した場合は、IPv6 送信元アドレスまたは IPv6 宛先アドレスのみ入力することができます。
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、以下の欄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の送信を行いません。 • 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「config mirror port」コマンド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	プルダウンメニューを使用して、オプション（「Change 1P Priority」、「Replace DSCP」および「Replace ToS Precedence」）を選択します。
Apply To	プルダウンメニューを使い事前に設定した項目を選択します。 • Ports – ポート番号 / 範囲を入力します。 • VLAN Name – VLAN 名を入力します。 • VLAN ID – VLAN ID 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。

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（EI のみ）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。

アクセスプロファイルの作成

現在のアクセスプロファイルを表示します。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。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。

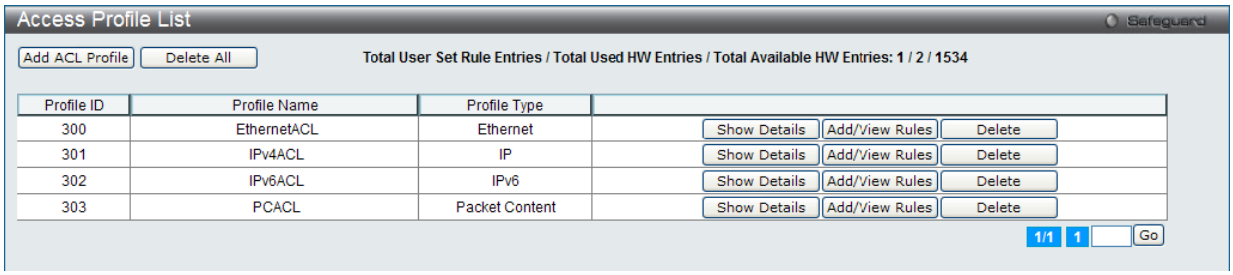


図 11-2　Access Profile List 画面

「Add Access Profile」画面には 4 種類あります。イーサネット（または MAC アドレスベース）プロファイル設定用、IPv4 アドレスベースプロファイル設定用、パケットコンテンツマスクプロファイル設定用および IPv6 アドレスベースプロファイル（EI のみ）設定用です。「Add ACL Profile」画面の「Profile Name」を入力し、「ACL Type」でタイプをチェック後、「Select」ボタンをクリックすることで 4 つの画面を切り替えることができます。

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。（このボタンによって Address Binding ACL エントリは削除されません。Address Binding ACL エントリは、「IP-MAC Binding」画面経由でだけ削除されます。）
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とルールの作成（Ethernet）

イーサネット用のアクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。

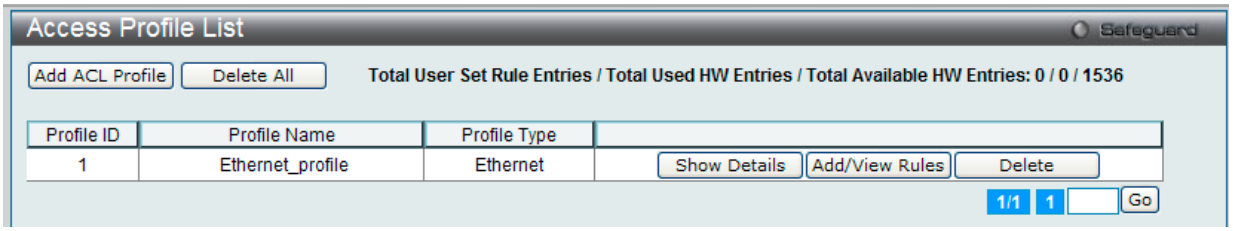


図 11-3　Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

アクセスプロファイルの作成（Ethernet）画面

イーサネット ACL を作成する場合、「Select Profile ID」および「Profile Name」を指定し、「Select」ボタンをクリックして以下の画面を表示します。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。

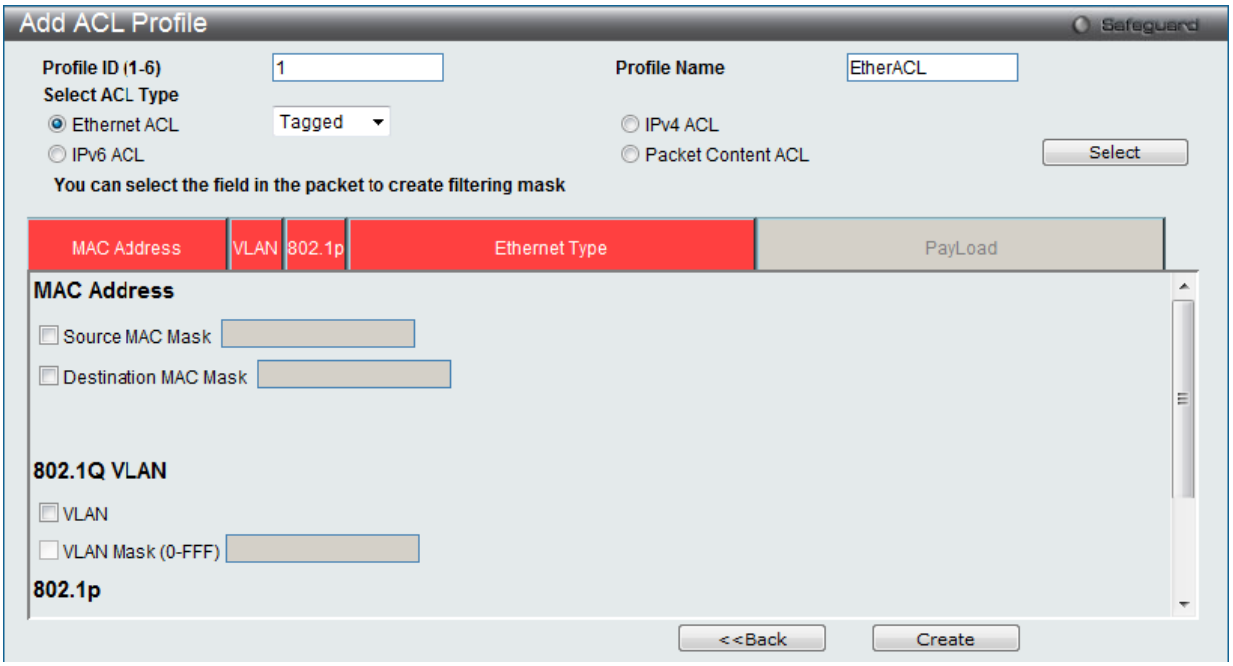


図 11-4　Add Access Profile（Ethernet）画面

以下の項目を Ethernet ACL タイプに設定します。

項目	説明
Profile ID (1-6)	プロファイルに設定する番号を入力します。1-6 の間で設定可能です。低い値ほど高い優先度を示します。
Profile Name	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。 • Ethernet を ACL - パケットヘッダのレイヤ 2 部分をチェックします。 • IPv4 ACL - フレームヘッダの IPv4 アドレスをチェックします。 • IPv6 ACL（EI のみ）- フレームヘッダの IPv6 アドレスをチェックします。 • Packet Content - フレームヘッダのパケットコンテンツをチェックします。
Ethernet ACL	Ethernet プロファイルを設定するためには、「Ethernet ACL」を選択し、プルダウンメニューを使用して「Tagged」（タグ付き）または「Untagged」（タグなし）を選択します。
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	このオプションを指定するパケットヘッダの 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。
802.1P	このオプションを指定するとそれぞれのパケットヘッダの 802.1p プライオリティを調べて、部分的もしくは全体を転送基準として使用します。
Ethernet Type	このオプションを指定すると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、設定を適用します。
「Access Profile List」画面に戻るためには、「<<Back」ボタンをクリックします。

以下の通り「Access Profile List」テーブルに新しいアクセスプロファイルリストが表示されます。

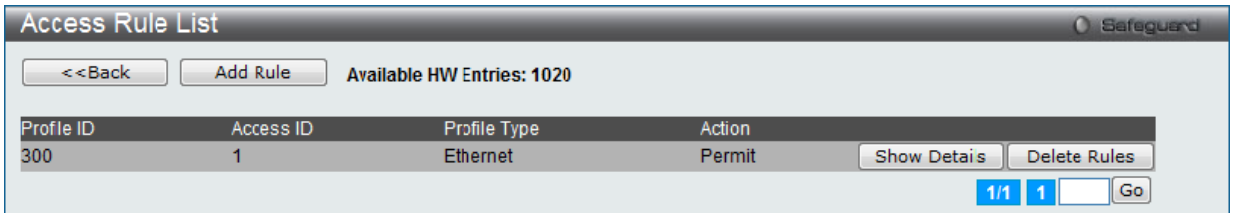


図 11-5　Access Rule List（Ethernet ACL）画面

作成したプロファイルの詳細の参照

「Show Details」ボタンをクリックし、以下の画面を表示します。

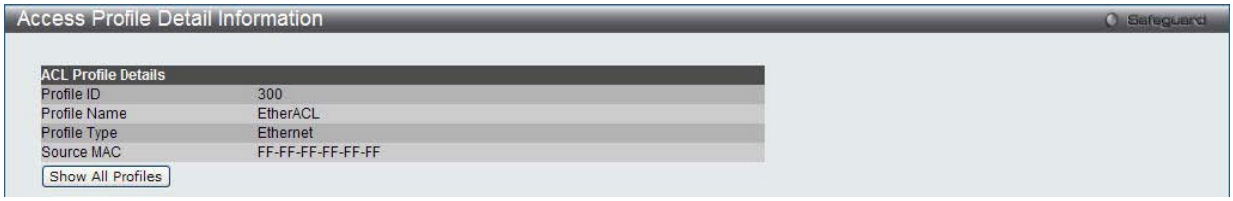


図 11-6　Access Profile Detail Information - Ethernet 画面

「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（Ethernet）

Ethernet アクセスルールの設定

1. 「Access Profile List」画面を表示します。

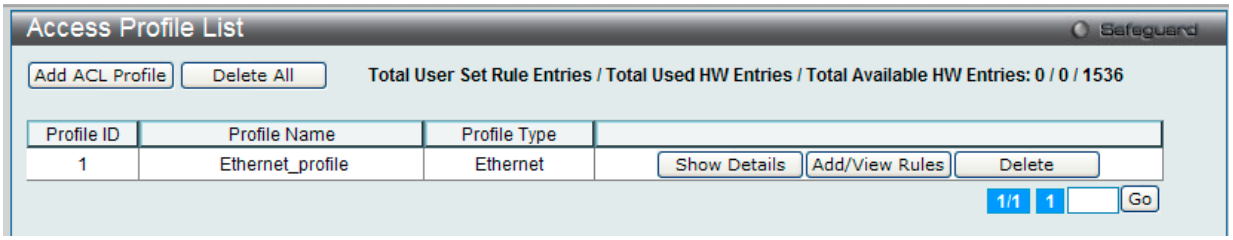


図 11-7　Access Profile List 画面

2. Ethernet エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

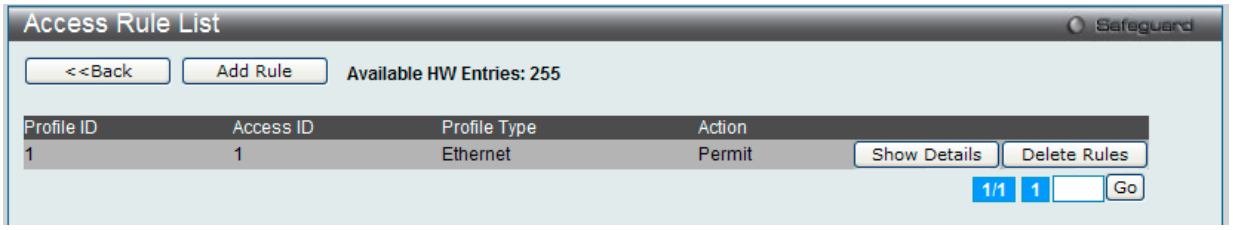


図 11-8　Access Rule List - Ethernet 画面

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

作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

ルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

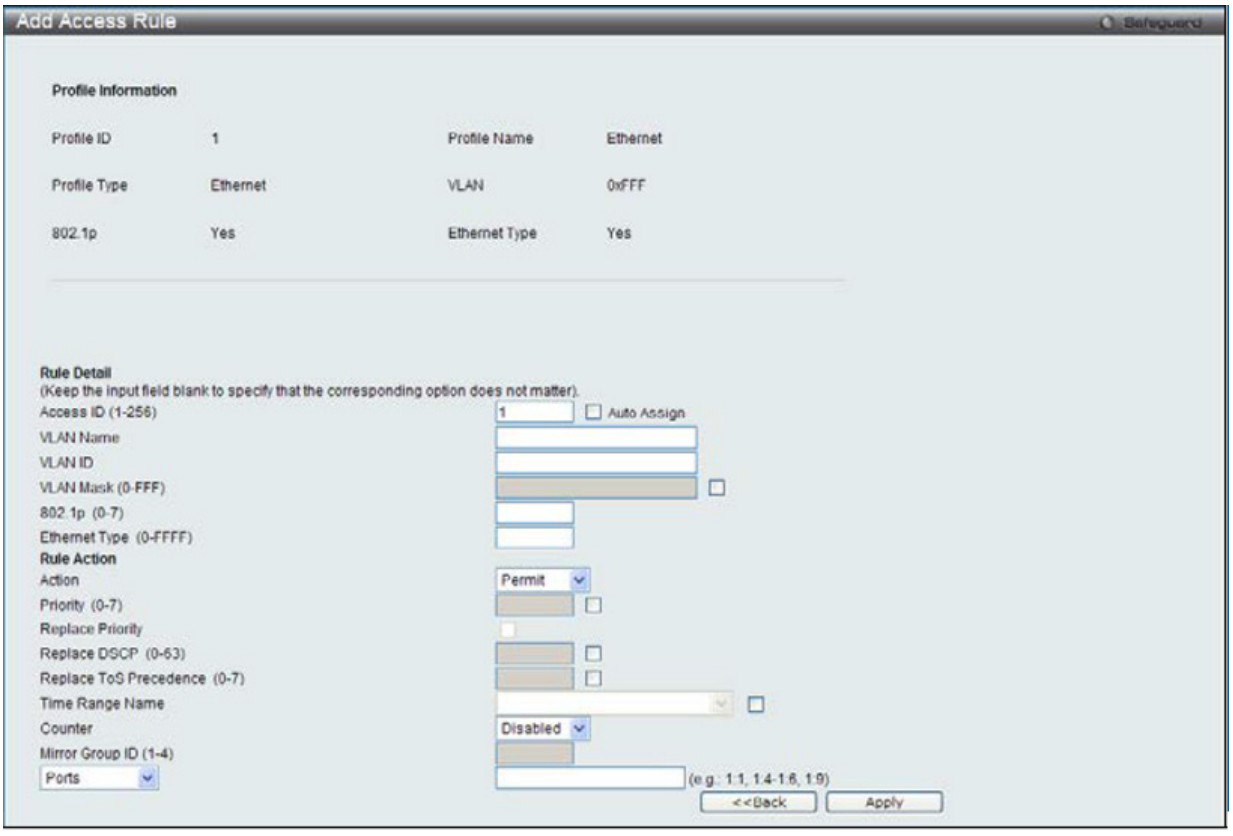


図 11-9　Add Access Rule - Ethernet 画面

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ます。

項目	説明
Access ID (1-256)	ルールに対する固有の識別番号を指定します。1 から 256 が指定できます。低い値ほど高い優先度を示します。 • 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。
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ない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。Port Mirroring 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。この項目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。 • ボックスをチェックするとパケットが条件に合った場合、CoS キューに送られる前にプライオリティフィールドの 802.1p デフォルトプライオリティが書き換えられます。しかし、パケットの 802.1p ユーザプライオリティはスイッチから転送される前に書き戻されます。 プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 189 ページの「第 10 章 QoS（QoS 機能の設定）」を参照してください。
Replace Priority	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」欄に指定した値に書き換える場合に使用します。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。
Replace DSCP (0-63)	本オプションを選択すると、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。 プライオリティと IPv4 パケットの DSCP の両方を変更を加える ACL ルールを加えた場合、プライオリティだけが変更されます。
Replace ToS Precedence	パケットの IP 優先度を新しい値に書き換えます。特に指定がない場合、パケットはデフォルトのトラフィッククラスに送られます。
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	カウンタ機能を「Enabled」（有効）または「Disabled」（無効）にします。これは、オプションです。初期値は「Disabled」（無効）です。ルールがフローメータにバインドされないと、一致するすべてのパケットが無効となります。ルールがフローメータにバインドされると、本「カウンタ」は上書きされます。
Mirror Group ID (1-4)	ミラーグループを入力します。アクセスルールにパケットがマッチした時、パケットは指定したミラーグループのミラーポートにコピーされます。
Ports / VLAN Name / VLAN ID	プルダウンメニューを使い、事前に設定した「Ports」「VLAN Name」「VLAN ID」から、アクセスルールが有効にする項目を選択します。

「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、変更を破棄して前のページに戻ります。

定義済みルールの参照

対象エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

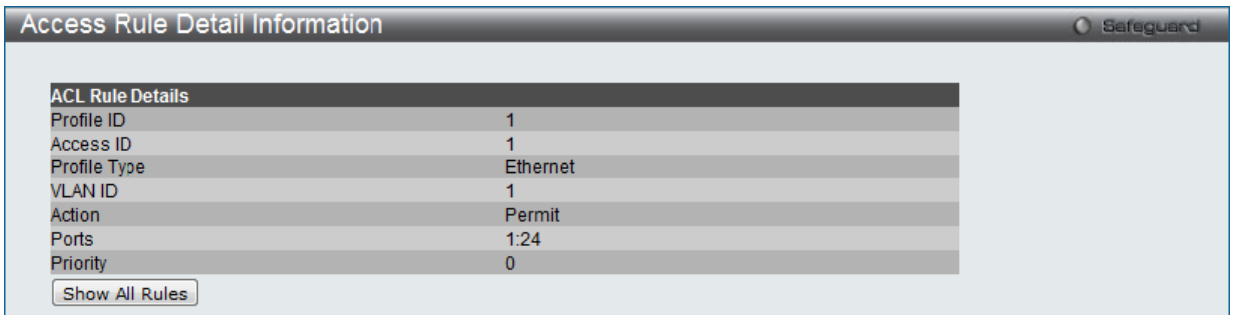


図 11-10　Access Rule Detail Information（Ethernet）画面

「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とルールの作成（IPv4）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。1 つのアクセスプロファイルが説明のために作成されています。

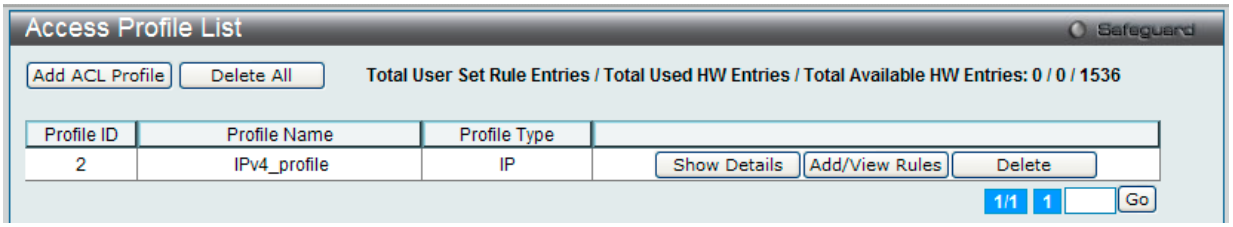


図 11-11　Access Profile List 画面

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ます。

アクセスプロファイルの作成（IPv4）画面

IPv4 ACL を作成する場合、「Select Profile ID」および「Profile Name」を指定し、「Select」ボタンをクリックして以下の画面を表示します。

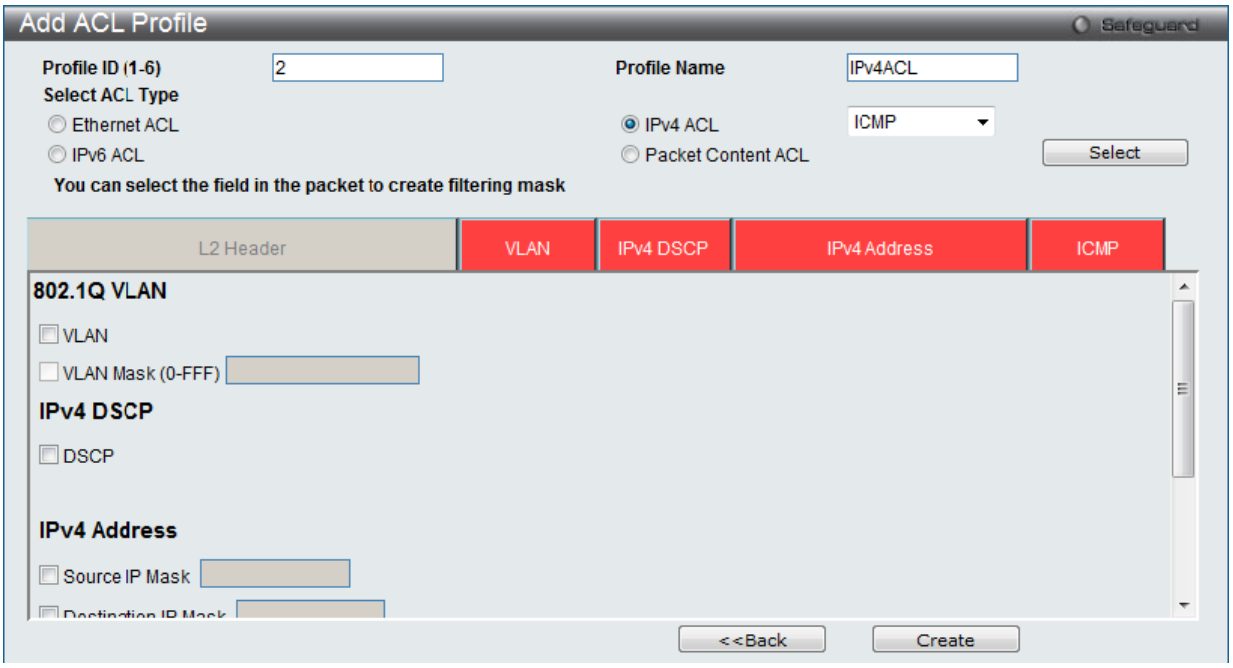


図 11-12　Add ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-6 から選択し、「Select ACL Type」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
Select 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 6 が指定できます。低い値ほど高い優先度を示します。
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。 • Ethernet ACL - パケットヘッダのレイヤ 2 部分をチェックします。 • IPv4 ACL - フレームヘッダの IPv4 アドレスをチェックします。 • IPv6 ACL - フレームヘッダの IPv6 アドレスをチェックします。 • Packet Content - フレームヘッダのパケットコンテンツをチェックします。 IPv4 プロファイルを設定するためには、「IPv4 ACL」を選択し、プルダウンメニューを使用して「ICMP」、「IGMP」、「TCP」、「UDP」または「Protocol ID」を選択します。
802.1Q VLAN	このオプションを指定するパケットヘッダの 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。
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	• 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。
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。	
ICMP	各パケット内の Internet Control Message Protocol（ICMP）フィールドを調査する場合に指定します。 • Type - アクセスプロファイルを ICMP Type 値（0-255）に適用します。 • Code - アクセスプロファイルを ICMP Code（0-255）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「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。 - src port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - dst port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - flag bit - 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（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。 - src port mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - dst port mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。「User Define」マスクは 16 進数（hex 0x0-0xffffffff）で指定します。

「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

「Show Details」ボタンをクリックし、以下の画面を表示します。

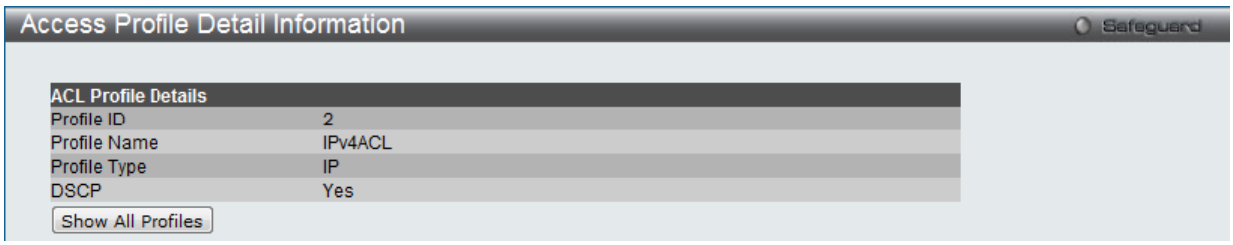


図 11-13 Access Profile Detail Information - IPv4 画面

「Access Profile List」戻るためには、「Show All Profiles」ボタンをクリックします。

作成したアクセスプロファイルに対するルールの設定（IPv4）

IPv4 アクセスルールの設定

1. 「Access Profile List」画面を表示します。

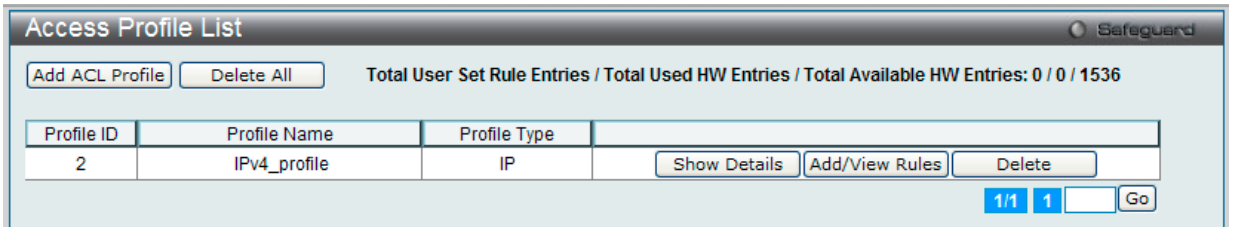


図 11-14　Access Profile List 画面

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。

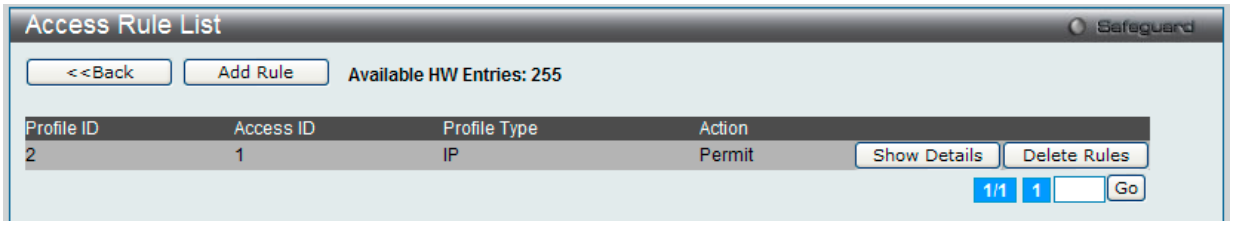


図 11-15　Access Rule List - IPv4 画面

「<<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。該当の「Delete Rules」ボタンをクリックします。

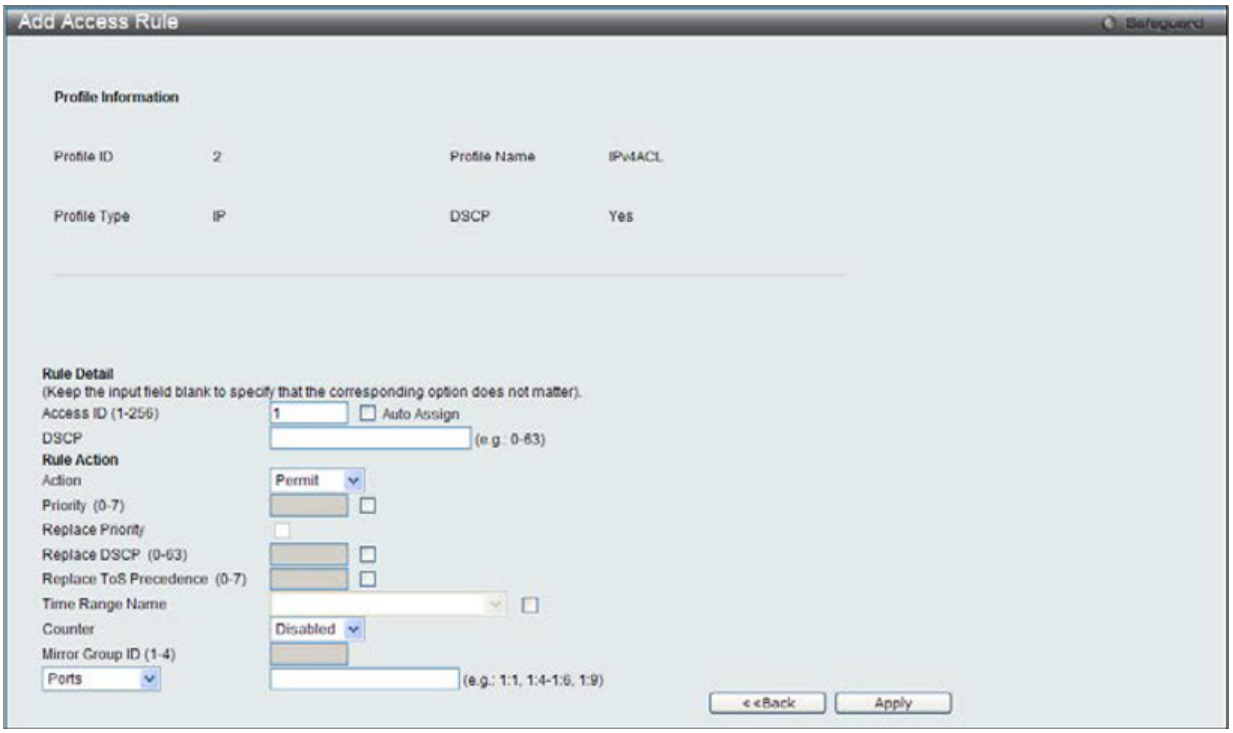


図 11-16　Add Access Rule (IPv4 ACL) 画面

IPv4 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ます。

項目	説明
Access ID (1-256)	ルールに対する固有の識別番号（1-256）を指定します。低い値ほど高い優先度を示します。 • 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。
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ない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。Port Mirroring 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。この項目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。 • ボックスをチェックするとパケットが条件に合った場合、CoS キューに送られる前にプライオリティフィールドの 802.1p デフォルトプライオリティが書き換えられます。しかし、パケットの 802.1p ユーザプライオリティはスイッチから転送される前に書き戻されます。 プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 189 ページの「第 10 章 QoS（QoS 機能の設定）」を参照してください。
Replace Priority	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」欄に指定した値に書き換える場合に使用します。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。
Replace DSCP (0-63)	本オプションを選択すると、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欄内に指定した値に書き換えます。プライオリティと IPv4 パケットの DSCP の両方を変更する ACL ルールを加えた場合、プライオリティだけが変更されます。
Replace ToS Precedence (0-7)	パケットの IP 優先度を新しい値に書き換えます。特に指定がない場合、パケットはデフォルトのトラフィッククラスに送られます。
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	カウンタ機能を「Enabled」（有効）または「Disabled」（無効）にします。
Mirror Group ID (1-4)	ミラーグループを入力します。アクセスルールにパケットがマッチした時、パケットは指定したミラーグループのミラーポートにコピーされます。
Ports	本項目にスタックスイッチ内のスイッチのポート番号を入力し、ポート単位にアクセスルールを設定指定します。ポート範囲を指定する場合は、「Access ID」の「Auto Assign」チェックボックスにチェックを入れる必要があります。チェックが入っていないと、エラーメッセージが表示され、アクセスルールは設定されません。「All Ports」チェックボックスにチェックを入れると、スイッチの全ポートを意味します。

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。

定義済みルールの参照

対象エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

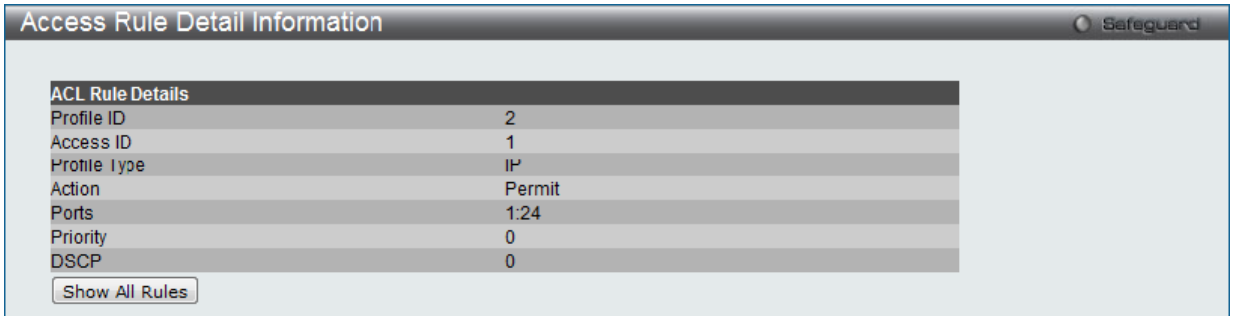


図 11-17　Access Rule Detail Information（IPv4）画面

「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とルールの作成（IPv6）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。1 つのアクセスプロファイルが説明のために作成されています。

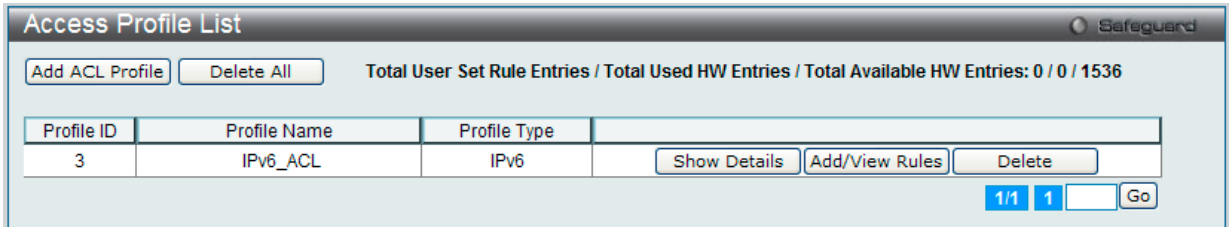


図 11-18 Access Profile List 画面

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。

アクセスプロファイルの作成（IPv6）画面

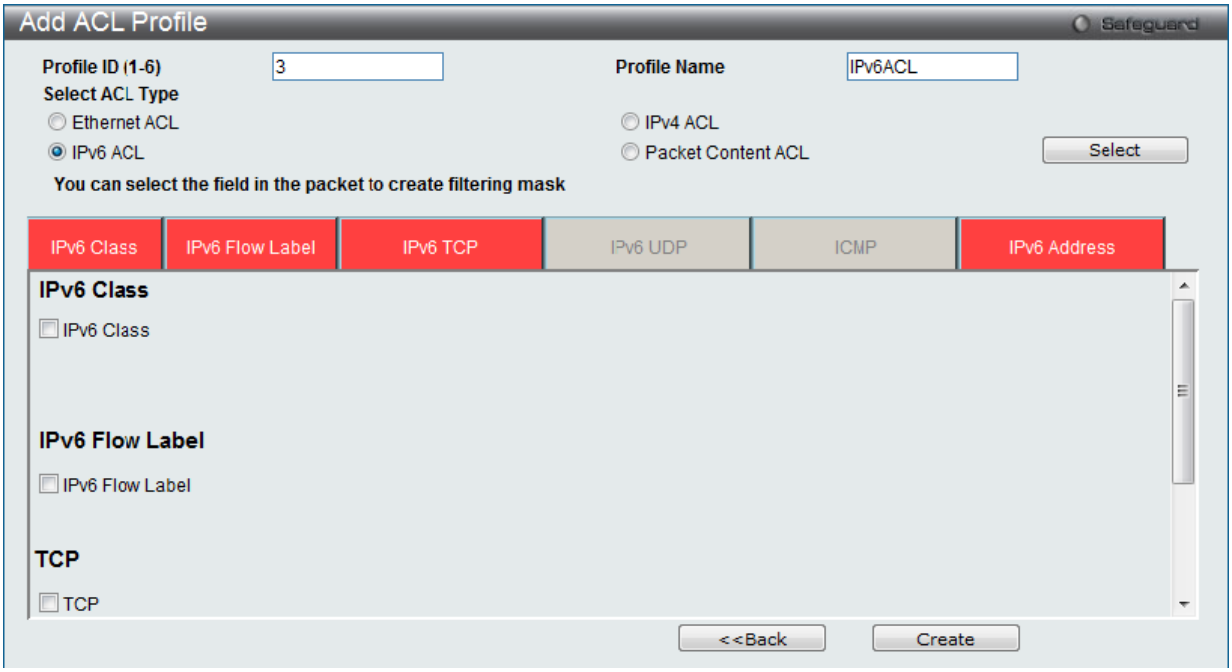


図 11-19 Add ACL Profile - IPv6 ACL 画面

「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 (1-6)	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 6 が指定できます。低い値ほど高い優先度を示します。
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。 • Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。 • IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。 • IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。 • 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。 IPv6 プロファイルを設定するためには、「IPv6 ACL」を選択します。
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。 注意 どんな場合も、IPv6 Class と IPv6 Flow Label は共に選択し、IPv6 アドレスは単体で選択します。	
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。

項目	説明
IPv6 Flow Label	この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 TCP	TCP トラフィックに当ルールを適用する場合、チェックボックスにチェックします。 指定の TCP 送信元ポートマスクが TCP 宛先ポートマスクを入力します。
IPv6 UDP	UDP トラフィックに当ルールを適用する場合、チェックボックスにチェックします。 指定の UDP 送信元ポートマスクが UDP 宛先ポートマスクを入力します。
ICMP	「ICMP」を選択するとスイッチは各フレーム内のヘッダの ICMP を確認します。
IPv6 Address	• IPv6 Source Address - ボックスにチェックをつけて送信元 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 - ボックスにチェックをつけて送信先 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
「Show Details」ボタンをクリックし、以下の画面を表示します。

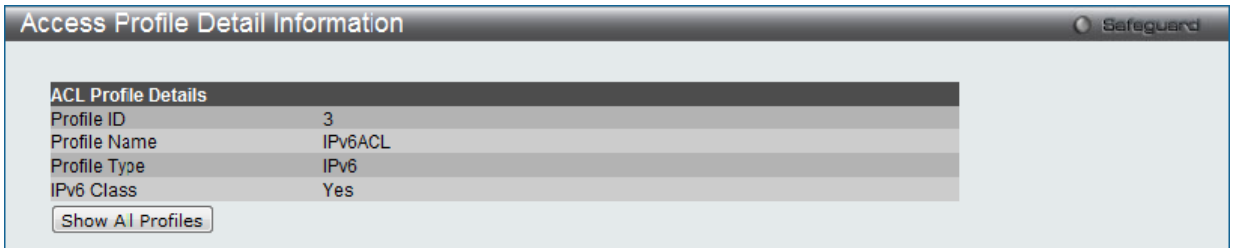


図 11-20 Access Profile Detail Information - IPv6 画面

「Access Profile List」戻るためには、「Show All Profiles」ボタンをクリックします。

作成したアクセスプロファイルに対するルールの設定（IPv6）

IPv6 アクセスルールの設定

1. 「Access Profile List」画面を表示します。

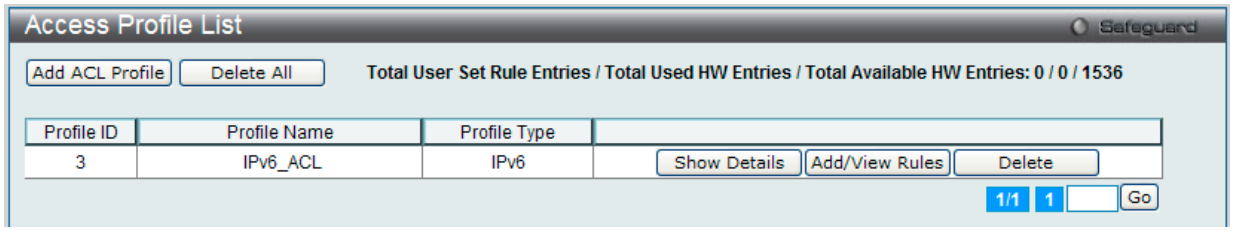


図 11-21 Access Profile List 画面

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。

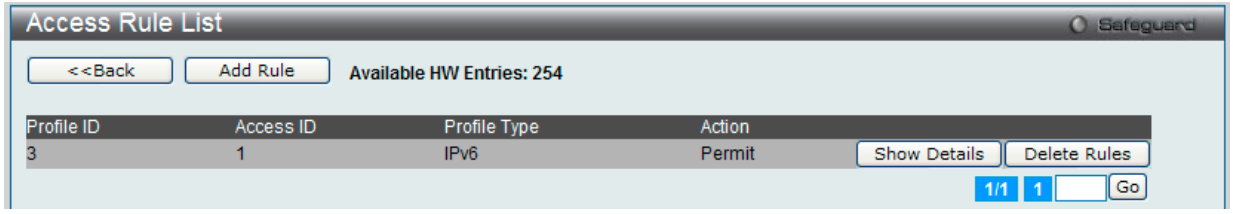


図 11-22 Access Rule List - IPv6 画面

「<<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。

作成済みルールの削除
該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

新しいルールを作成するためには、「Add Rule」ボタンをクリックします。

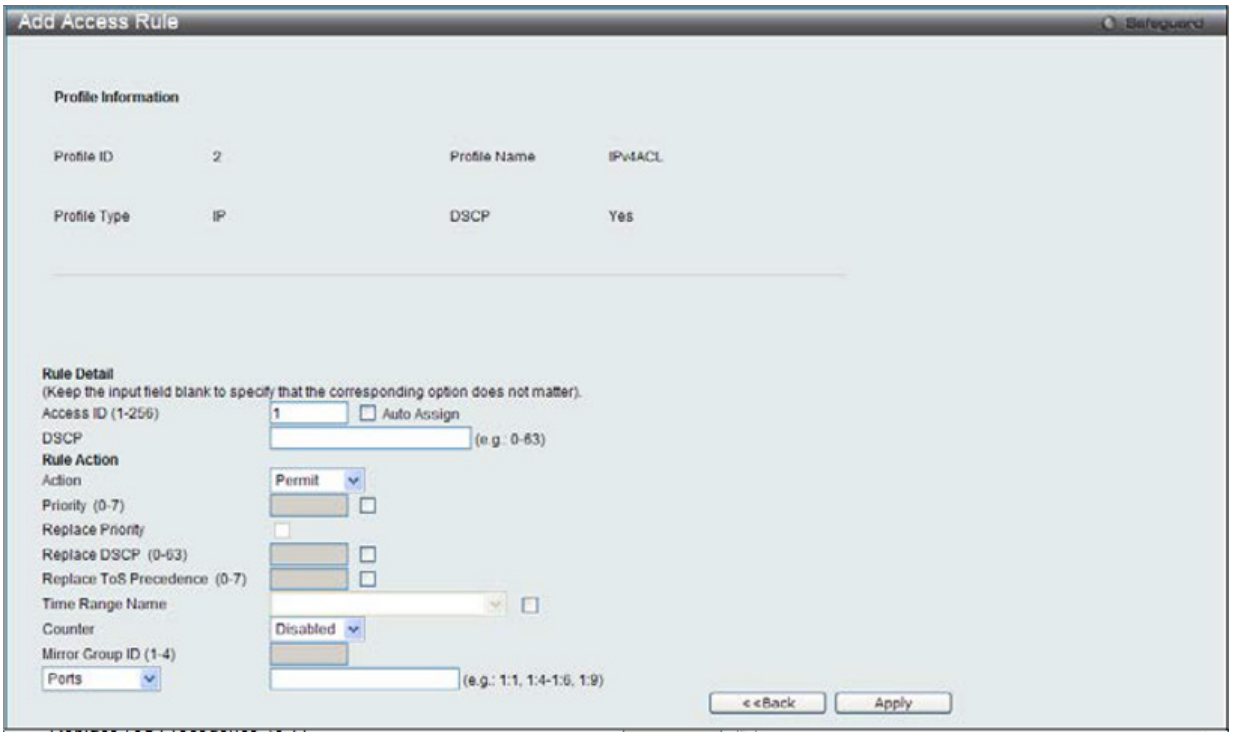


図 11-23　Add Access Rule - IPv6 画面

IPv6 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ます。

項目	説明
Access ID (1-256)	作成したルールに対する固有の識別番号を指定します。1 から 256 が指定できます。低い値ほど高い優先度を示します。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Class	IPv6 ヘッダのクラス項目にスイッチを構成するクラスを入力します。パケットヘッダの一部である本項目は ToS や IPv4 Precedence ビットと類似しています。
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ない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。Port Mirroring 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により使用される CoS キューが決まります。この項目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。 • ボックスをチェックするとパケットが条件に一致した場合、CoS キューに送られる前にプライオリティ欄の 802.1p デフォルトプライオリティが書き換えられます。しかし、パケットの 802.1p ユーザプライオリティはスイッチから転送される前に書き戻されます。 プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 189 ページの「第 10 章　QoS（QoS 機能の設定）」 を参照してください。
Replace Priority	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」欄に指定した値に書き換える場合に使用します。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。
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欄に指定した値に書き換えます。パケットの IP 優先度を新しい値に書き換えます。特に指定がない場合、パケットはデフォルトのトラフィッククラスに送られます。
Replace ToS Precedence (0-7)	パケットの IP 優先度を新しい値に書き換えます。特に指定がない場合、パケットはデフォルトのトラフィッククラスに送られます。
Rx Rate (1-15624)	アクセスルールで受信するデータレートの上限を指定します。このレートは次の式を使用します。: 1 value = 64Kbit/sec（例：Rx rate に 10 を選択するとイングレスレートは 640Kbit/sec となります。）1-15624 の範囲で値を指定するか、または「No Limit」をチェックします。初期値は「No Limit」です。
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	カウンタ機能を「Enabled」（有効）または「Disabled」（無効）にします。

項目	説明
Mirror Group ID (1-4)	ミラーグループを入力します。アクセスルールにパケットがマッチした時、パケットは指定したミラーグループのミラーポートにコピーされます。
Ports / VLAN Name / VLAN ID	プルダウンメニューを使い、事前に設定した「Ports」「VLAN Name」「VLAN ID」から、アクセスルールが有効にする項目を選択します。

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。

定義済みルールの参照

対象エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

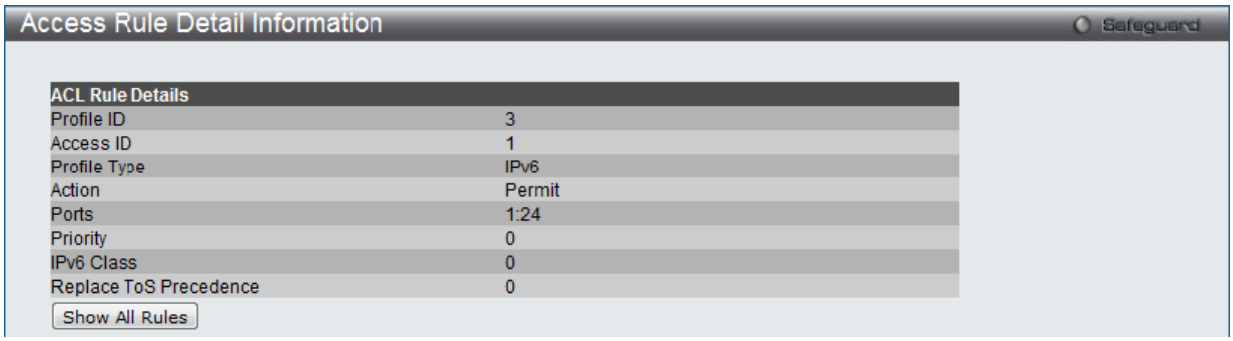


図 11-24　Access Rule Detail Information（IPv6）画面

「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とルールの作成（パケットコンテンツ）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。 1 つのアクセスプロファイルが説明のために作成されています。

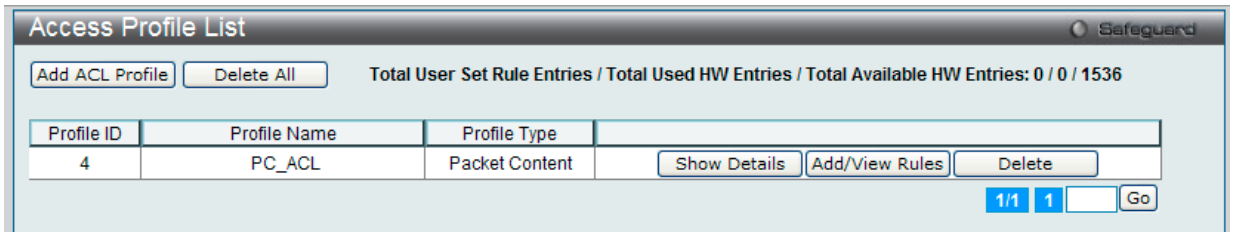


図 11-25　Access Profile List 画面

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。

アクセスプロファイルの作成（パケットコンテンツ）画面

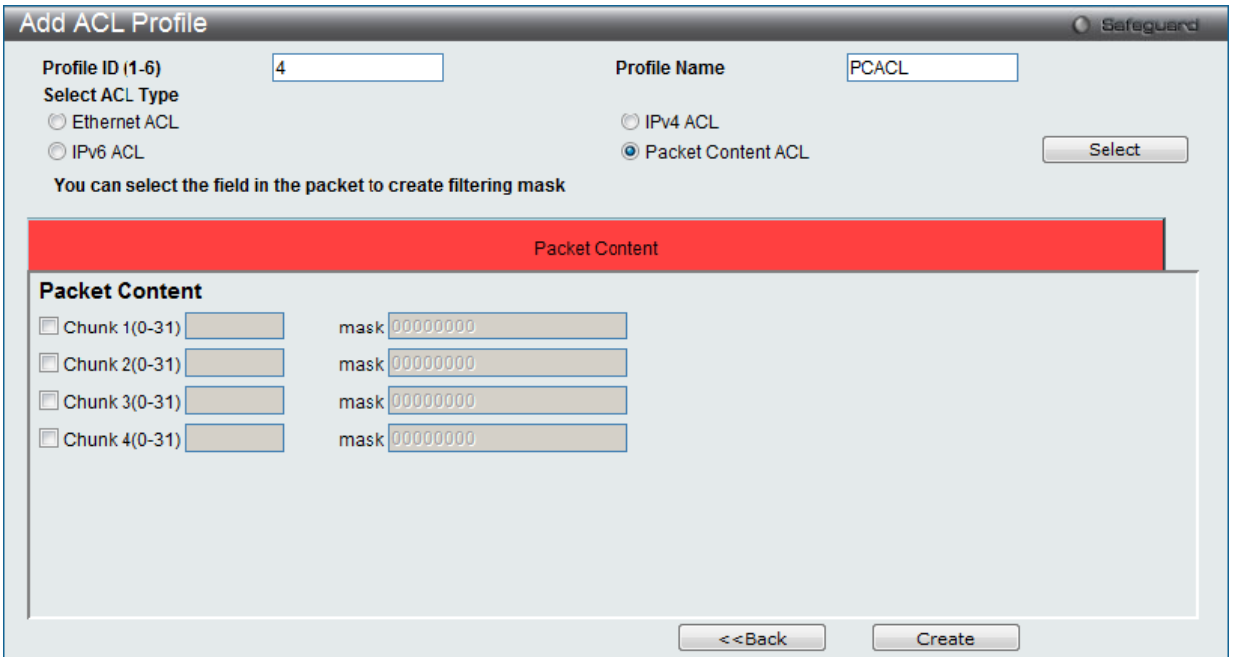


図 11-26　Add ACL Profile 画面 - パケットコンテンツ

「Profile ID」でプロファイル番号を 1-6 から選択し、「Select ACL Type」で「Packet Content ACL」をチェック後、「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目をパケットコンテンツタイプに設定します。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>Profile ID</td><td>プロファイル設定のための固有の識別番号を指定します。1 から 6 が指定できます。低い値ほど高い優先度を示します。</td></tr>
<tr><td>Select ACL Type</td><td>Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。
• Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。
• IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。
• IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。
• 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。
パケットコンテンツプロファイルを設定するためには、「Packet Content ACL」を選択します。</td></tr>
<tr><td colspan="2">パケットコンテンツは、同時にパケット内の 4 個のオフセットチャンクと、そのフレームコンテンツとオフセットを検証できます。
設定可能な 4 個のチャンクオフセットとマスクがあります。チャンクマスクは 4 バイトを示します。
以下で説明するように、32 個の定義済みオフセットチャンクから 4 つのオフセットチャンクを選択することができます。</td></tr>
<tr><td>Chunk</td><td>offset_chunk_1
offset_chunk_2
offset_chunk_3
offset_chunk_4
<table>
<tr><td>chunk0</td><td>chunk1</td><td>chunk2</td><td>……</td><td>chunk29</td><td>chunk30</td><td>chunk31</td></tr>
<tr><td>B126</td><td>B2</td><td>B6</td><td>……</td><td>B114</td><td>B118</td><td>B122</td></tr>
<tr><td>B127</td><td>B3</td><td>B7</td><td></td><td>B115</td><td>B119</td><td>B123</td></tr>
<tr><td>B0</td><td>B4</td><td>B8</td><td></td><td>B116</td><td>B120</td><td>B124</td></tr>
<tr><td>B1</td><td>B5</td><td>B9</td><td></td><td>B117</td><td>B121</td><td>B125</td></tr>
</table>
使用例 :
offset_chunk_1 0 0xffffffff はパケットバイトオフセット 126、127、0、1 に一致します。
offset_chunk_1 0 0x0000ffff はパケットバイトオフセット 0、1 に一致します。

注意 一度に、1 個のパケットコンテンツマスクプロファイルしか作成できません。D-Link xStack スイッチファミリは、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、スイッチのパケットコンテンツ ACL の実装により、プロトコルレイヤに関係なくどんなパケットの特定コンテンツの検証も可能になります。</td></tr>
</table>

「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参照

エントリに指定した設定を参照するためには、「Show Details」ボタンをクリックし、以下の画面を表示します。

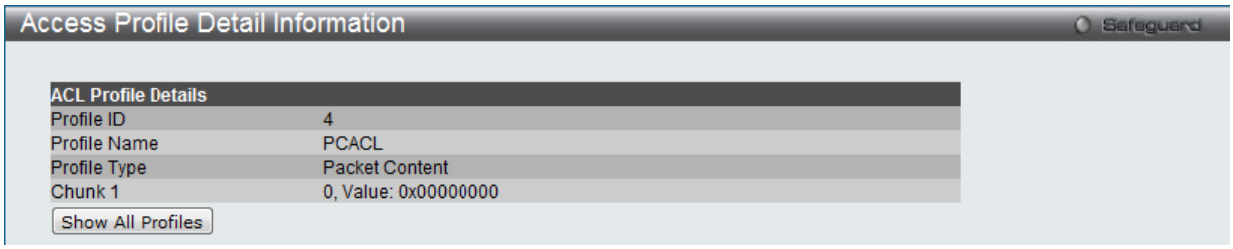


図 11-27　Access Profile Detail Information - パケットコンテンツ画面

「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（パケットコンテンツ）

パケットコンテンツアクセスルールの設定

1. 「Access Profile List」画面を表示します。

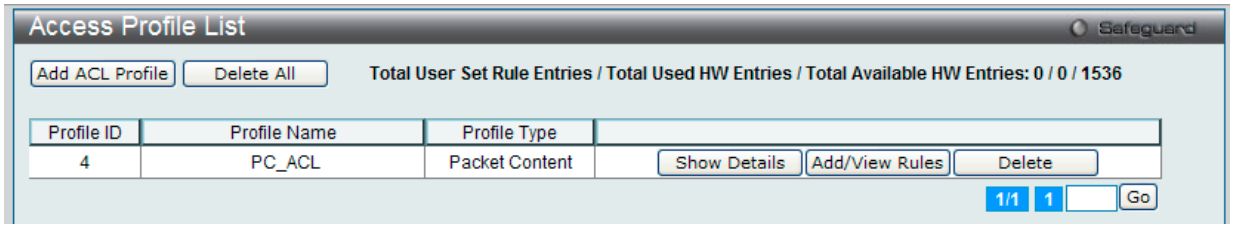


図 11-28　Access Profile List 画面

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。

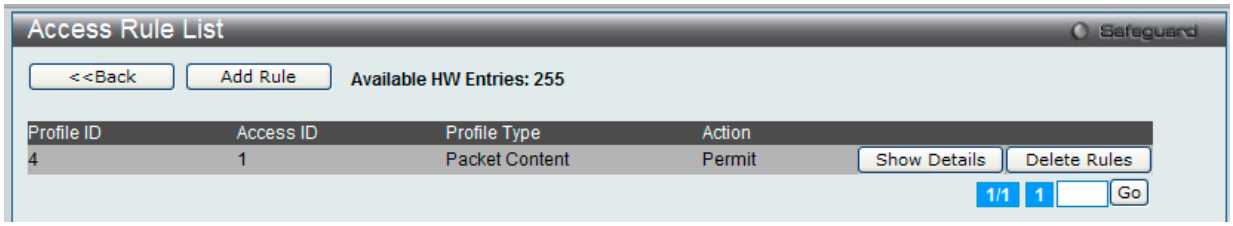


図 11-29　Access Rule List 画面 - パケットコンテンツ

「<<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。

定義済みルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

新しいルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

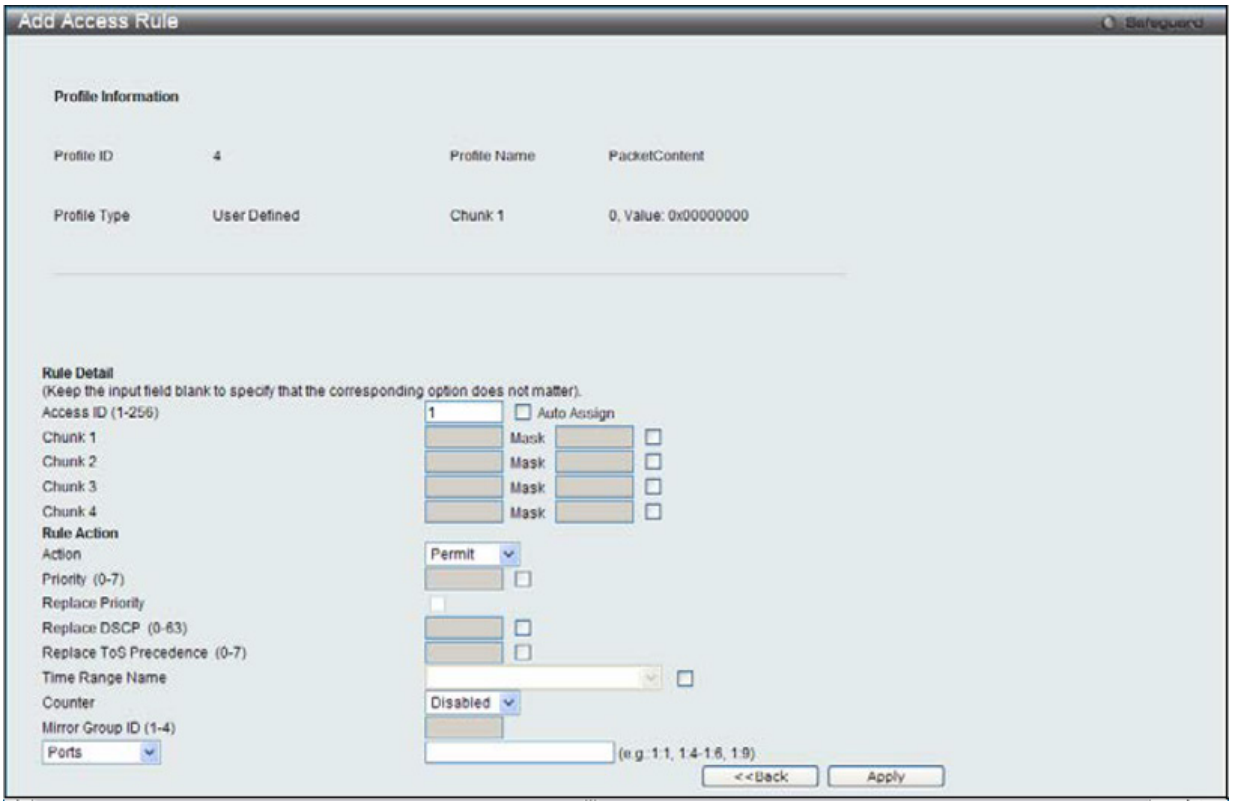


図 11-30 Add Access Rule - パケットコンテンツ画面

パケットコンテンツ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ます。

項目	説明
Access ID (1-256)	ルールに対する固有の識別番号を指定します。1 から 256 が指定できます。低い値ほど高い優先度を示します。 • 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。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致しない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。Port Mirroring 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。この項目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。 • ボックスをチェックするとパケットが条件に合った場合、CoS キューに送られる前にプライオリティフィールドの 802.1p デフォルトプライオリティが書き換えられます。しかし、パケットの 802.1p ユーザプライオリティはスイッチから転送される前に書き戻されます。 プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 189 ページの「第 10 章 QoS（QoS 機能の設定）」を参照してください。
Replace Priority	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」欄に指定した値に書き換える場合に使用します。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。
Replace DSCP (0-63)	本オプションを選択すると、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。プライオリティと IPv4 パケットの DSCP の両方を変更する ACL ルールを加えた場合、プライアリティだけが変更されます。
Replace ToS Precedence (0-7)	パケットの IP 優先度を新しい値に書き換えます。特に指定がない場合、パケットはデフォルトのトラフィッククラスに送られます。
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	カウンタ機能を「Enabled」（有効）または「Disabled」（無効）にします。
Mirror Group ID (1-4)	ミラーグループを入力します。アクセスルールにパケットがマッチした時、パケットは指定したミラーグループのミラーポートにコピーされます。
Ports / VLAN Name / VLAN ID	プルダウンメニューを使い、事前に設定した「Ports」「VLAN Name」「VLAN ID」から、アクセスルールが有効にする項目を選択します。

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。

定義済みルールの参照

対象エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

図 11-31　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。

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 379 ページの「【付録 A】 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」を参照してください。

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

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。

CPU 用のアクセスプロファイルの作成は 2 段階に分かれます。はじめにフレームのどの部分を調べるのか、送信元 MAC アドレスか、送信先 IP アドレスか、などを決定します。次に、そのフレームに対してどのような処理を行うのかという基準になる値を入力します。詳しくは以下で 2 つに分けて説明します。

動作状態を変更するためには、ラジオボタンを使用して、CPU インタフェースフィルタリング機能をグローバルに「Enabled」（有効）または「Disabled」（無効）にします。「Enabled」を選択するとスイッチは CPU パケットを詳しく調べます。「Disabled」にするとこの動作は行われません。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

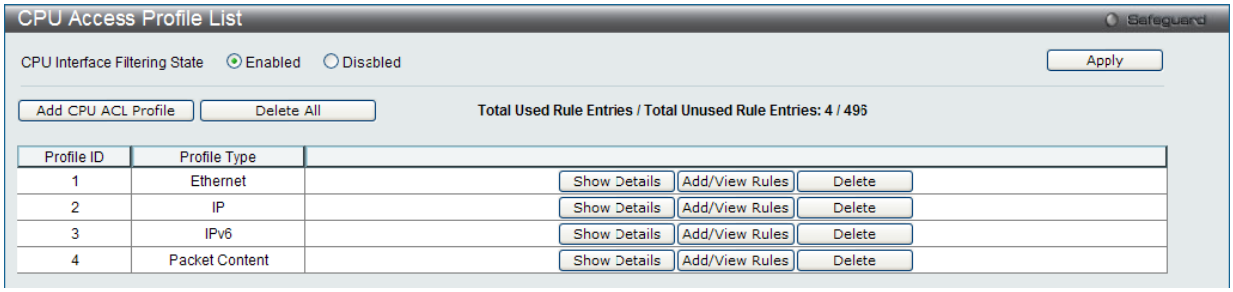


図 11-32　CPU Access Profile List 画面

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。

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。

スイッチは、4 つの CPU アクセスプロファイルタイプ（イーサネット（MAC アドレスベース）プロファイル設定、IP（IPv4）アドレスベースのプロファイル設定、IP（IPv6）アドレスベースのプロファイル設定、パケットコンテンツのマスク設定）をサポートしています。

CPU アクセスプロファイルとルールの作成（Ethernet）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、「CPU Interface Filtering State」をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

図 11-33　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。

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

イーサネットの「Add CPU ACL Profile」画面

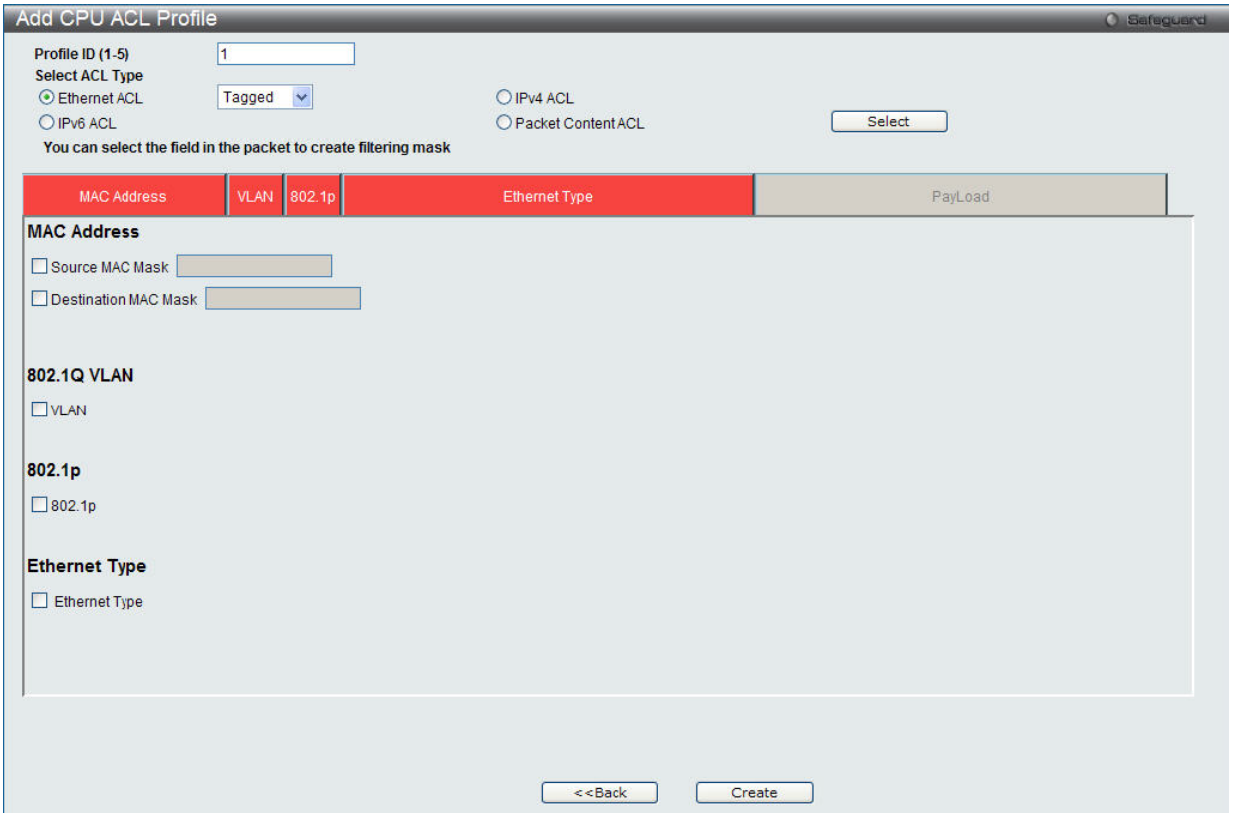


図 11-34　Add CPU ACL Profile - Ethernet 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「Ether ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を設定します。

項目	説明
Profile ID	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。低い値ほど高い優先度を示します。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または 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。 • Ethernet - パケットヘッダのレイヤ 2 部分を対象にします。 • IPv4 - フレームヘッダの IP アドレスを対象にします。 • IPv6 - フレームヘッダの IP アドレスを対象にします。 • Packet Content ACL - パケットヘッダの内容をマスクして隠します。
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。	
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	このオプションを指定するパケットヘッダの 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。
802.1P	このオプションをチェックすると、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	このオプションをチェックすると、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を参照する

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

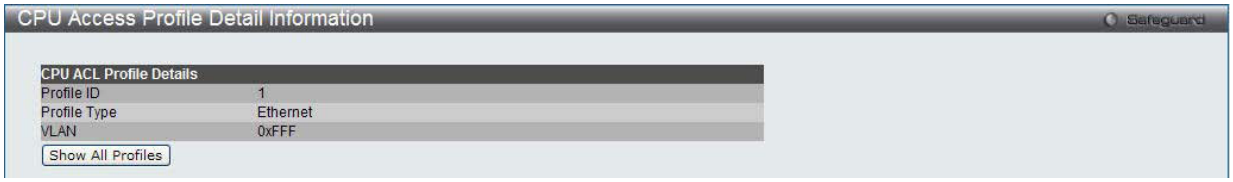


図 11-35 CPU Access Profile Detail Information - Ethernet 画面

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

作成した CPU アクセスプロファイルに対するルールの設定手順（Ethernet）

Ethernet アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

図 11-36 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。

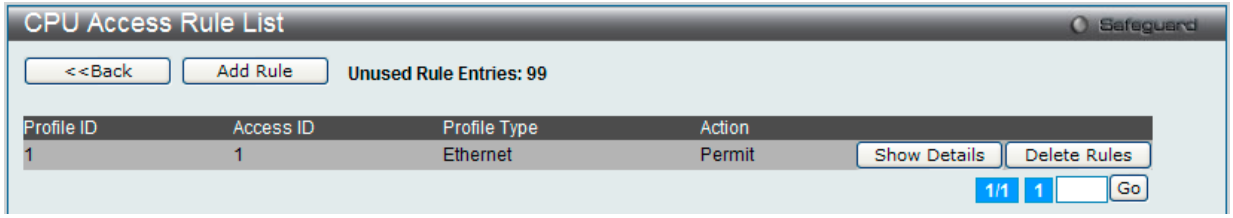


図 11-37 CPU Access Rule List - Ethernet 画面

「Show Details」ボタンをクリックし、作成した指定ルールに関する詳しい情報を表示します。
「Delete Rules」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

新しいルールの作成

「Add Rule」ボタンをクリックし、以下の画面を表示します。

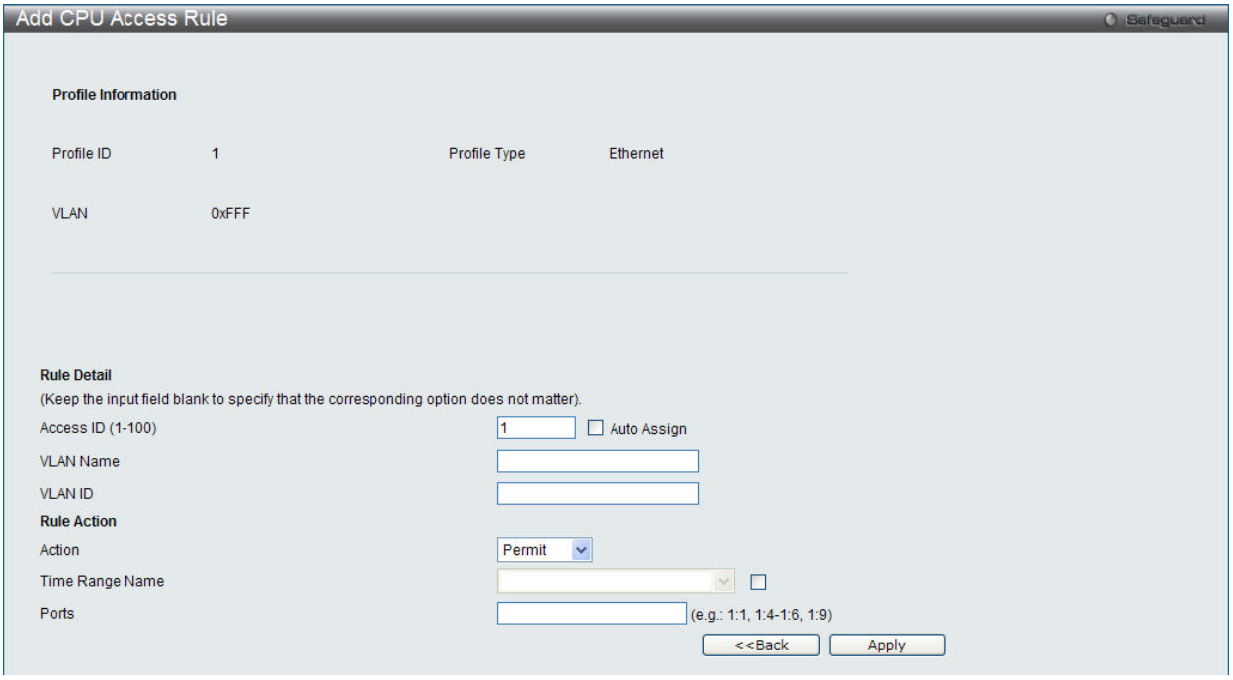


図 11-38　Add CPU Access Rule (Ethernet ACL) 画面

項目	説明
Access ID (1-100)	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 100 が指定できます。低い値ほど高い優先度を示します。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致しないパケットは転送せずにフィルタリングします。
Ethernet Type (0-FFFF)	適切なイーサネットの種類を入力します。
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	「All Ports」チェックボックスにチェックすると全てのポートが選択されます。

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。

作成したルールの参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

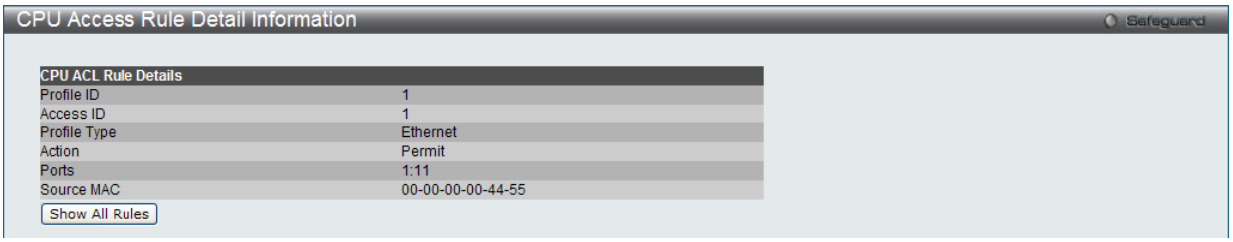


図 11-39　CPU Access Rule Detail Information (Ethernet ACL) 画面

「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とルールの作成（IPv4）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

図 11-40　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

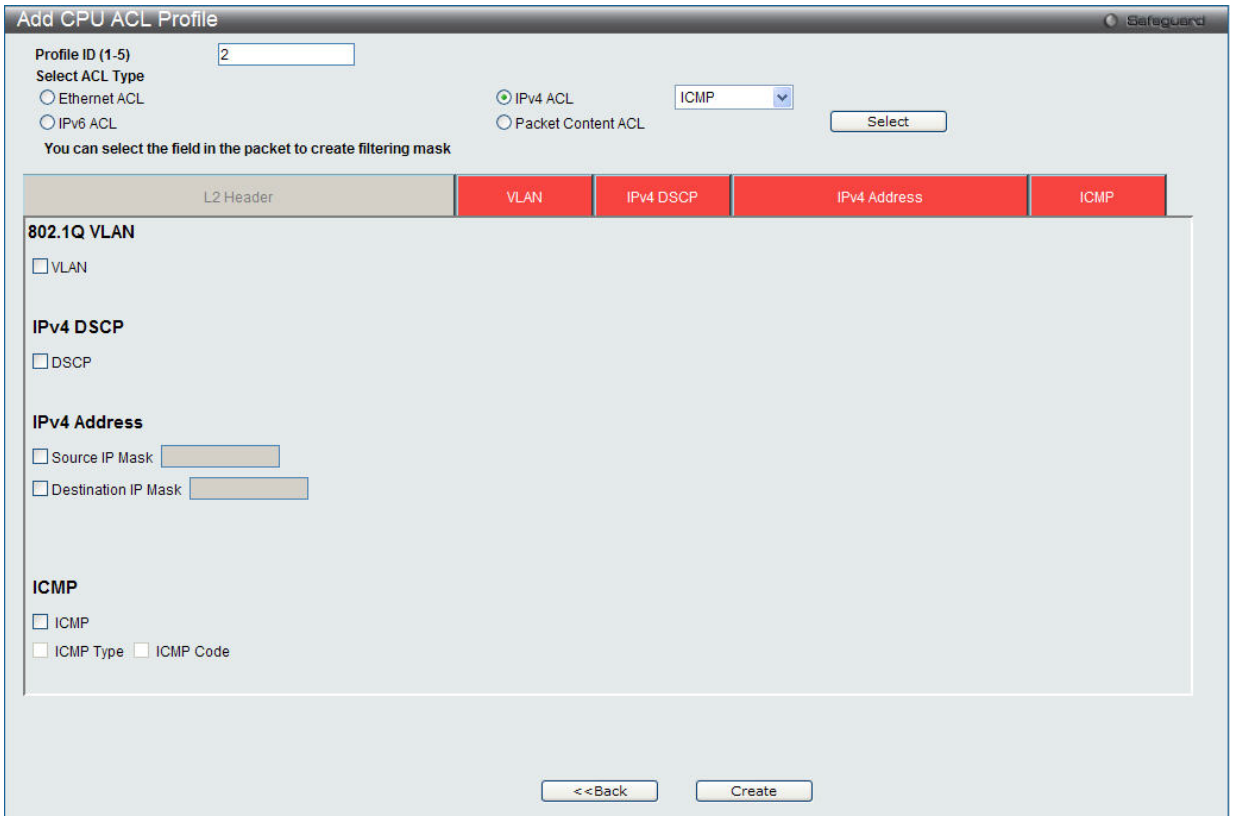


図 11-41　Add CPU ACL Profile - IPv4 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「IPv4 ACL」を選択します。さらに、隣接する欄で設定するフレームヘッダ（ICMP、IGMP、TCP、UDP、Protocol ID）を指定して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を IP（IPv4）フィルタに設定できます。

項目	説明
Profile ID (1-5)	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。低い値ほど高い優先度を示します。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または 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。 • Ethernet - パケットヘッダのレイヤ 2 部分を対象にします。 • IPv4 - フレームヘッダの IP アドレスを対象にします。 • IPv6 - フレームヘッダの IP アドレスを対象にします。 • Packet Content - パケットヘッダの内容をマスクして隠します。
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	このオプションを指定するパケットヘッダの 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。
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	• 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	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。 - src port mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - dst port mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには TCP 項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）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。 - src port mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - dst port mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。「User Define」マスク <hex 0x0-0xffffffff> は 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。16 進数（hex 0x0-0xffffffff）で指定します。

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

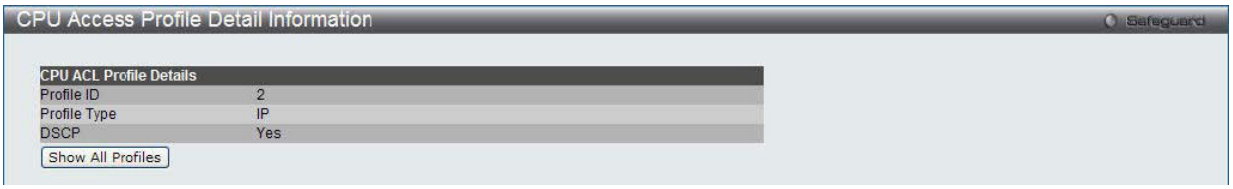


図 11-42 CPU Access Profile Detail Information - IP（IPv4）画面

「Show All Profiles」をクリックして「CPU ACL Profile List」へ戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（IPv4）

IP アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

図 11-43 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。

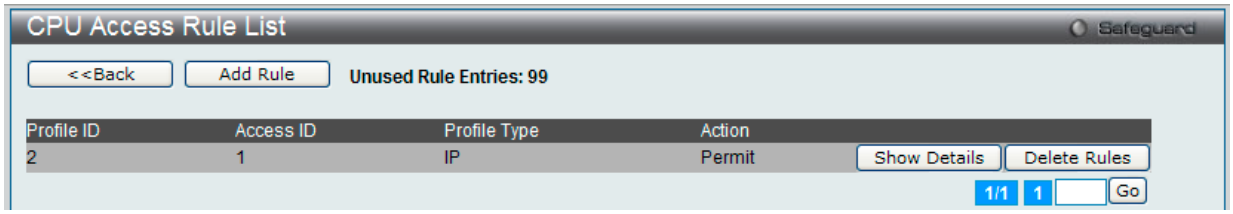


図 11-44 CPU Access Rule List - IP 画面

作成ルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」ボタンをクリックします。

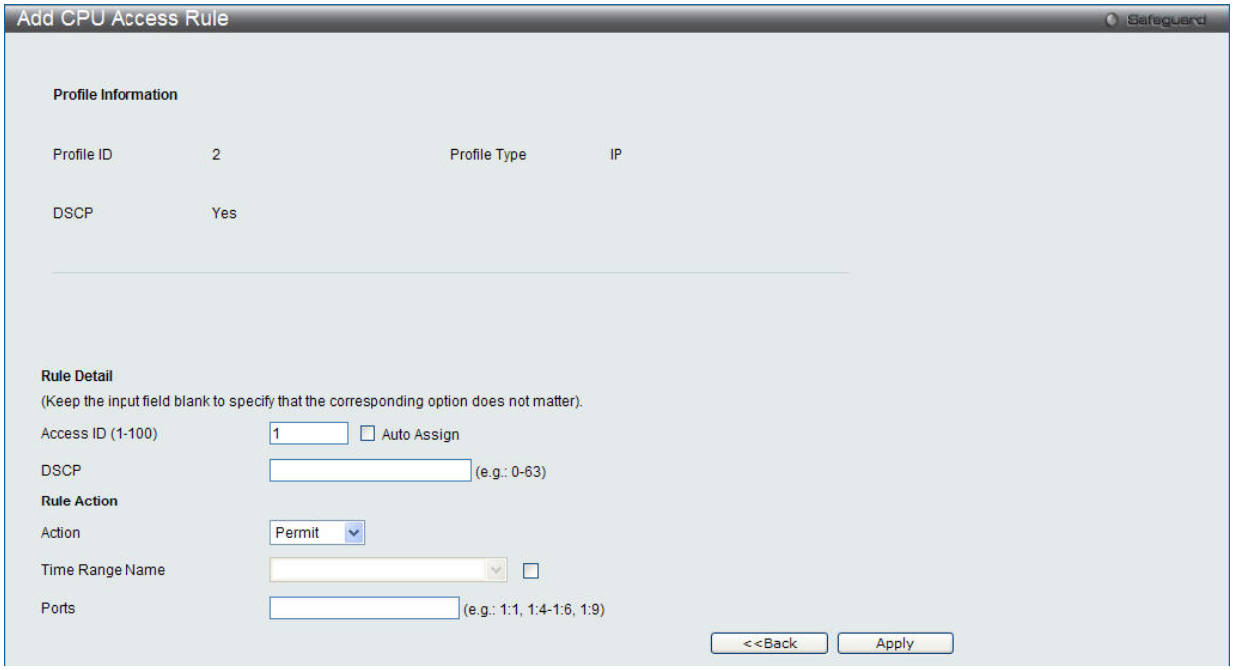


図 11-45 Add CPU Access Rule (IPv4 ACL) 画面

以下の項目を設定します。

項目	説明
Access ID (1-100)	ルールに対する固有の識別番号を指定します。1 から 100 が指定できます。低い値ほど高い優先度を示します。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致しないパケットは転送せずにフィルタリングします。
VLAN Name	設定した VLAN 名を入力します。
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	「All Ports」チェックボックスにチェックすると全てのポートが選択されます。

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参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

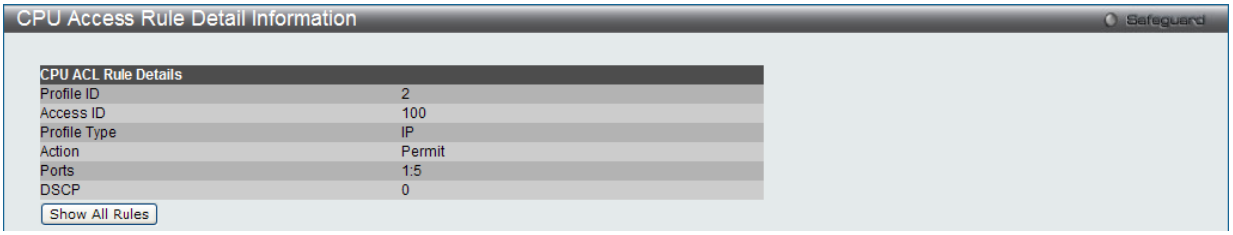


図 11-46 CPU Access Rule Detail Information (IPv4 ACL) 画面

「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とルールの作成（IPv6）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

図 11-47 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。 1 つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv6 の「Add CPU ACL Profile」画面

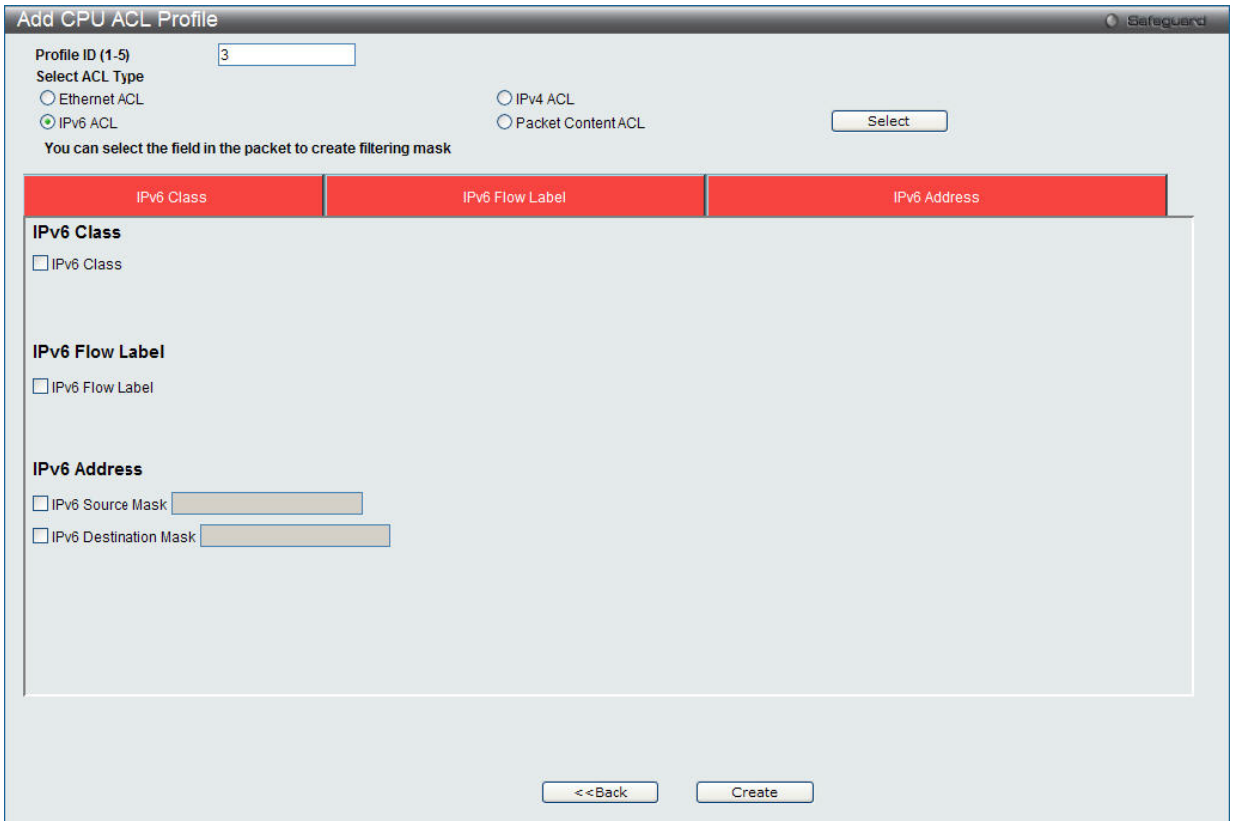


図 11-48　Add CPU ACL Profile - IPv6 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「IPv6 ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を IP（IPv6）フィルタに設定できます。

項目	説明
Profile ID (1-5)	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。低い値ほど高い優先度を示します。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または 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。 • Ethernet - パケットヘッダのレイヤ 2 部分を対象にします。 • IPv4 - フレームヘッダの IP アドレスを対象にします。 • IPv6 - フレームヘッダの IP アドレスを対象にします。 • Packet Content - パケットヘッダの内容をマスクして隠します。
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。 注意 どんな場合も、IPv6 Class と IPv6 Flow Label は共に選択し、IPv6 アドレスは単体で選択します。	
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 - ボックスにチェックをつけて送信元 IPv6 アドレスをマスクする IP アドレスを指定します。 • IPv6 Destination Mask - ボックスにチェックをつけて送信先 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、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

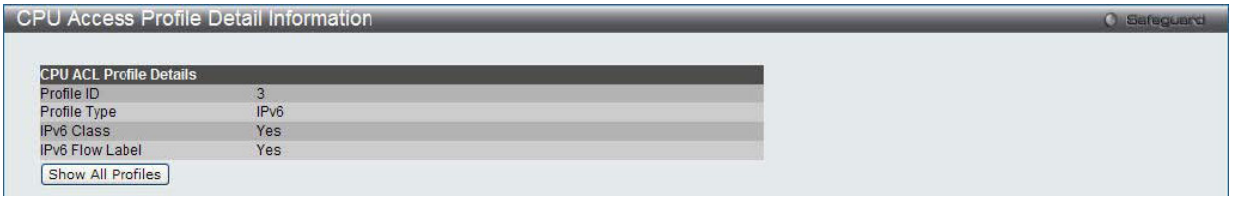


図 11-49 CPU Access Profile Detail Information - IP（IPv6）画面

「Show All Profiles」をクリックして「CPU ACL Profile List」へ戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（IPv6）

IPv6 アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

図 11-50 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。

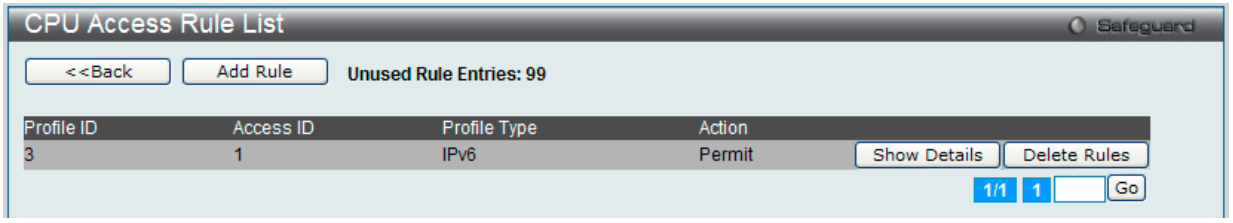


図 11-51 CPU Access Rule List - IPv6 画面

既に作成したルールの削除

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」ボタンをクリックし、以下の画面を表示します。

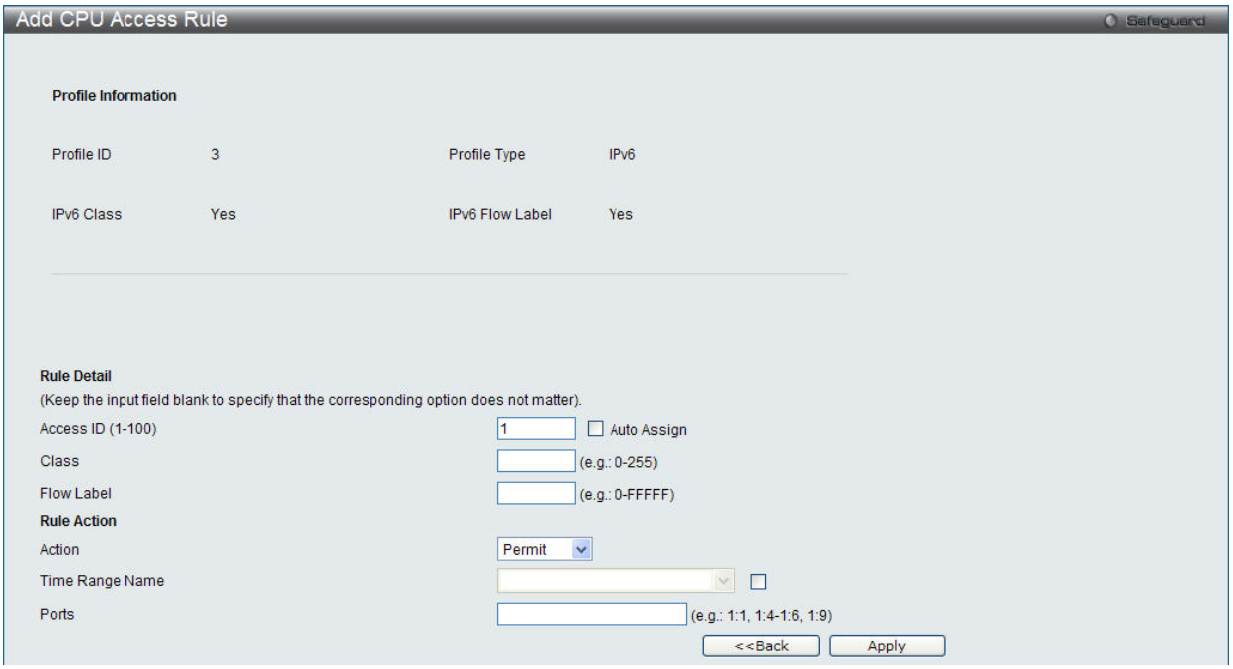


図 11-52 Add CPU Access Rule (IPv4 ACL) 画面

以下の項目があります。

項目	説明
Access ID (1-100)	ルールに対する固有の識別番号を指定します。1 から 100 が指定できます。低い値ほど高い優先度を示します。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致しないパケットは転送せずにフィルタリングします。
Flow Label	IPv6 ヘッダの flow label 項目を調べます。本項目は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
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	「All Ports」チェックボックスにチェックすると全てのポートが選択されます。

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

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

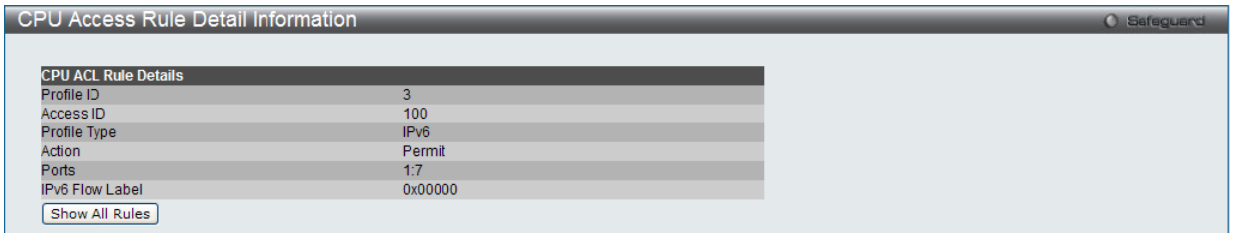


図 11-53 CPU Access Rule Detail Information (IPv6 ACL) 画面

「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とルールの作成（パケットコンテンツ）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、「CPU Interface Filtering State」をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

図 11-54 CPU Access Profile List 画面

本画面は、スイッチに作成した CPU アクセスプロファイルリストを表示します。各タイプに 1 つのアクセスプロファイルが説明のために作成されています。「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「CPU Interface Filtering State」に「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

パケットコンテンツの「Add CPU ACL Profile」画面

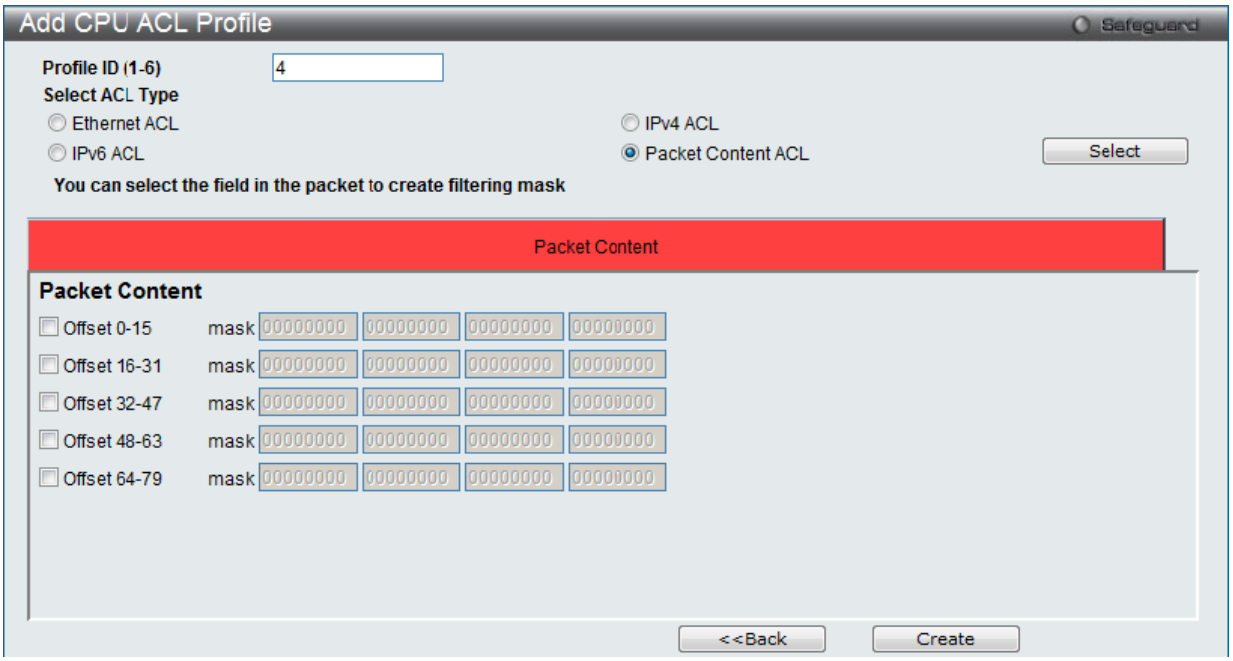


図 11-55　Add CPU ACL Profile - Packet Content 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「Packet Content ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を Packet Content フィルタに設定できます。

項目	説明
Profile ID（1-5）	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。低い値ほど高い優先度を示します。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または 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。 • Ethernet - パケットヘッダのレイヤ 2 部分を対象にします。 • IPv4 - フレームヘッダの IP アドレスを対象にします。 • IPv6 - フレームヘッダの IP アドレスを対象にします。 • Packet Content - パケットヘッダの内容をマスクして隠します。
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。

「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を参照する

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

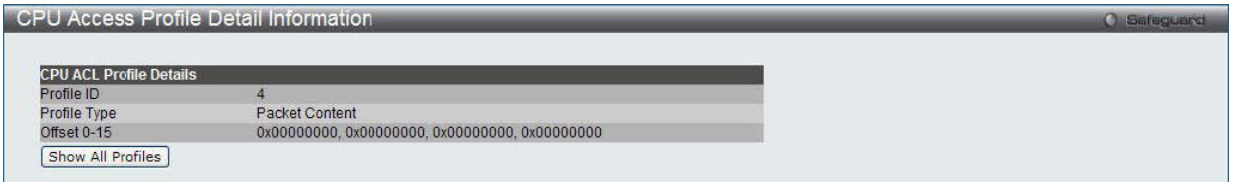


図 11-56　CPU Access Profile Detail Information - Packet Content 画面

「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。

作成した CPU アクセスプロファイルに対するルールの設定手順（Packet Content）

Packet Content アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

図 11-57　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。

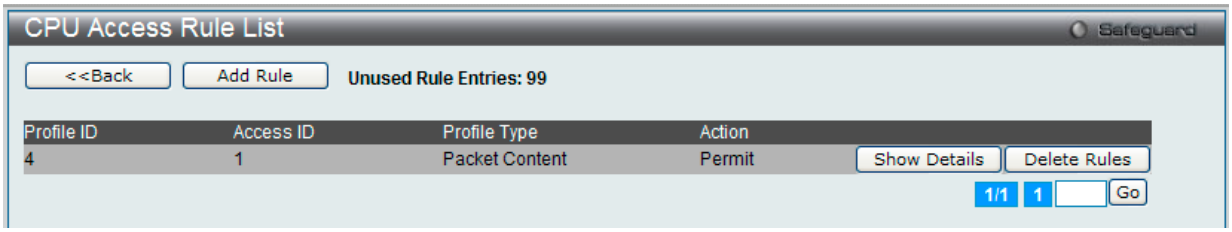


図 11-58　CPU Access Rule List - Packet Content 画面

作成済みのルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

「Add Rule」ボタンをクリックします。

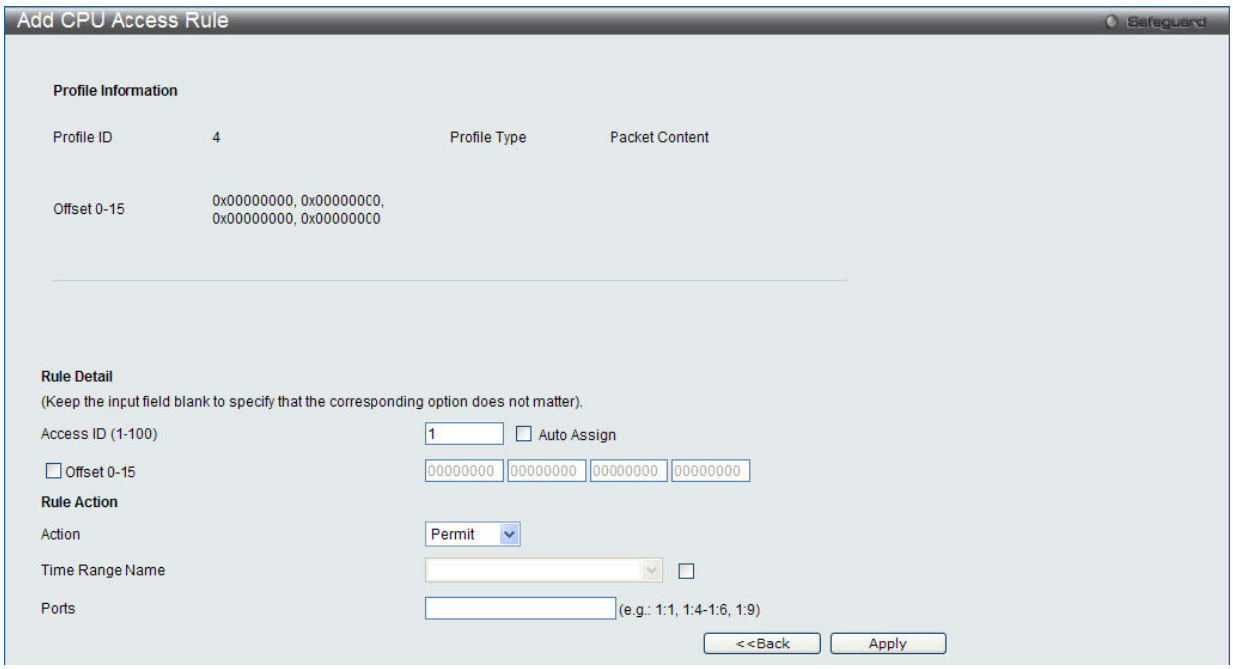


図 11-59　Add CPU Access Rule (Packet Content ACL) 画面

以下の項目があります。

項目	説明
Access ID (1-100)	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 100 が指定できます。低い値ほど高い優先度を示します。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致しないパケットは転送せずにフィルタリングします。
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。
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	「All Ports」チェックボックスにチェックすると全てのポートが選択されます。

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

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

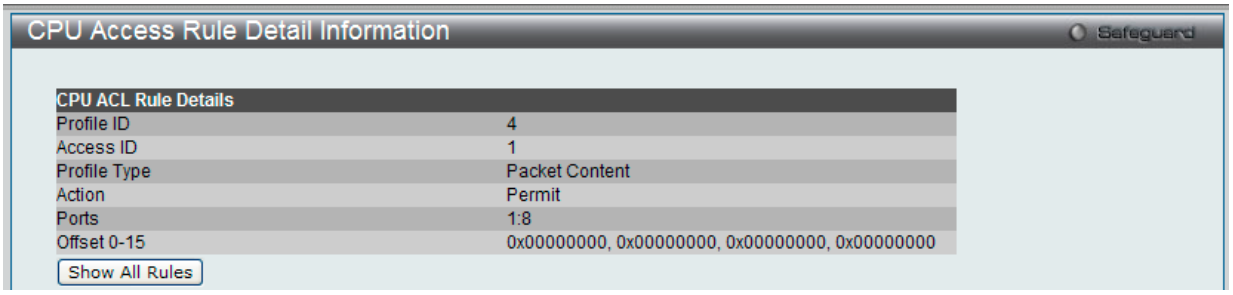


図 11-60　CPU Access Rule Detail Information - Packet Content 画面

「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）

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、プルダウンメニューからプロファイル ID を指定し、参照するポートを選択し、さらに「State」を定義して、「Find」ボタンをクリックします。画面下半分のテーブルにエントリは表示されます。

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

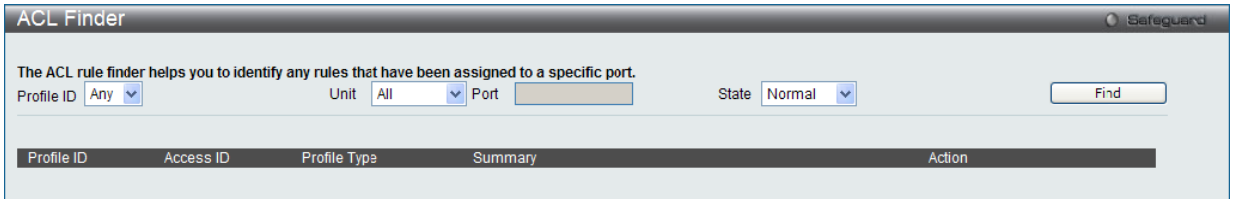


図 11-61　ACL Finder 画面

エントリの削除
対応する「Delete」ボタンをクリックします。

ACL Flow Meter（ACL フローメータ）

ACL フローメータを設定する前に、ユーザが知っておく必要がある頭文字語および項目のリストは次の通りです。

trTCM - Two Rate Three Color Marker。これは、srTCM と共にメータリングおよびパケットフローをマーキングするためにスイッチで可能な 2 つの方式です。trTCM が IP フローを計測し、2 つのレート（CIR および PIR）に基づいて、色でマークします。

CIR - Committed Information Rate。trTCM と srTCM の両方に共通で、CIR は IP パケットのバイト数を計測します。IP パケットのバイト数は、リンクする特定のヘッダではなく、IP ヘッダのサイズを取得することで計測します。trTCM に関しては、パケットフローは、CIR を超過していない場合に緑色でマークされ、CIR を超過している場合に黄色でマークされます。設定される CIR のレートは PIR のレートを超過してはなりません。また、CBS および PBS フィールドを使用して予期しないパケットバーストのために CIR を設定することができます。

- **CBS** - Committed Burst Size。バイト数を計測する場合、CBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、CBS を設定する必要があります。

PIR - Peak Information Rate。このレートは IP パケットのバイト数で計測されます。IP パケットのバイト数は、リンクする特定のヘッダではなく、IP ヘッダのサイズを取得することで計測します。パケットフローが PIR を超過すると、そのパケットフローは赤でマークされます。CIR のレートと同じかそれ以上になるように PIR を設定する必要があります。

- **PBS** - Peak Burst Size。バイト数を計測する場合、PBS は、PIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、PBS を設定する必要があります。

srTCM - Single Rate Three Color Marker。これは、trTCM と共にメータリングおよびパケットフローをマーキングするためにスイッチで可能な 2 つの方式です。srTCM は、設定された CBS と EBS に基づいて IP パケットフローをマークします。CBS に到達しないパケットフローは、緑色にマークされ、EBS ではなく CBS を超過している場合、黄色にマークされ、EBS を超過している場合、赤色にマークされます。

CBS - Committed Burst Size。バイト数を計測する場合、CBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、CBS を設定する必要があります。

EBS - Excess Burst Size。バイト数を計測する場合、EBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。EBS は、CBS と同じかさらに大きいレートに設定されます。

DSCP - Differentiated Services Code Point。色が追加されるパケットヘッダの部分。入力パケットの「DSCP」フィールドを変更することが可能です。ACL フローメータ機能により、入力パケットのレートに基づいて IP パケットフローにカラーコードを付加することができます。以前に説明した通り、２つのフローメータリングのタイプ（trTCM および srTCM）を選択することができます。パケットフローがカラーコードに置かれる時、その色分けされたレートを超過したパケットで何をするべきかを決めることができます。

緑 - IP フローが緑色のモードである時、設定可能なパラメータは、パケットがその「DSCP」フィールドを変更できる「Conform」フィールドにて設定されます。これは ACL フローメータ機能で許容できるフローレートです。

黄 - IP フローが黄色のモードである時、設定可能なパラメータは、「Exceed」フィールドにて設定されます。超過したパケットを「Permit」（許可）または「Drop」（廃棄）するかを選択します。パケットの「DSCP」フィールドを変更ために選択します。

赤 - IP フローが赤色のモードである時、設定可能なパラメータは、「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。

ACL フローメータ機能の設定を開始するためには、**ACL > ACL Flow Meter** の順にメニューをクリックし、以下の画面を表示します。

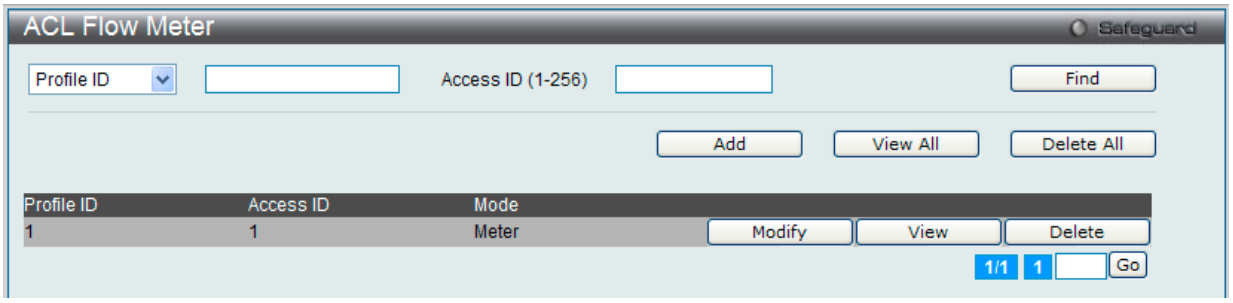


図 11-62　ACL Flow Meter 画面

以下の項目を使用して、設定を行います。

項目	説明
Profile ID /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 ID/Name を指定します。
Access ID (1-256)	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。

適切な情報を入力し、「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。

エントリの追加

対応する「Add」または「Modify」ボタンをクリックします。「Add」ボタンをクリックすると次の画面が表示されます。

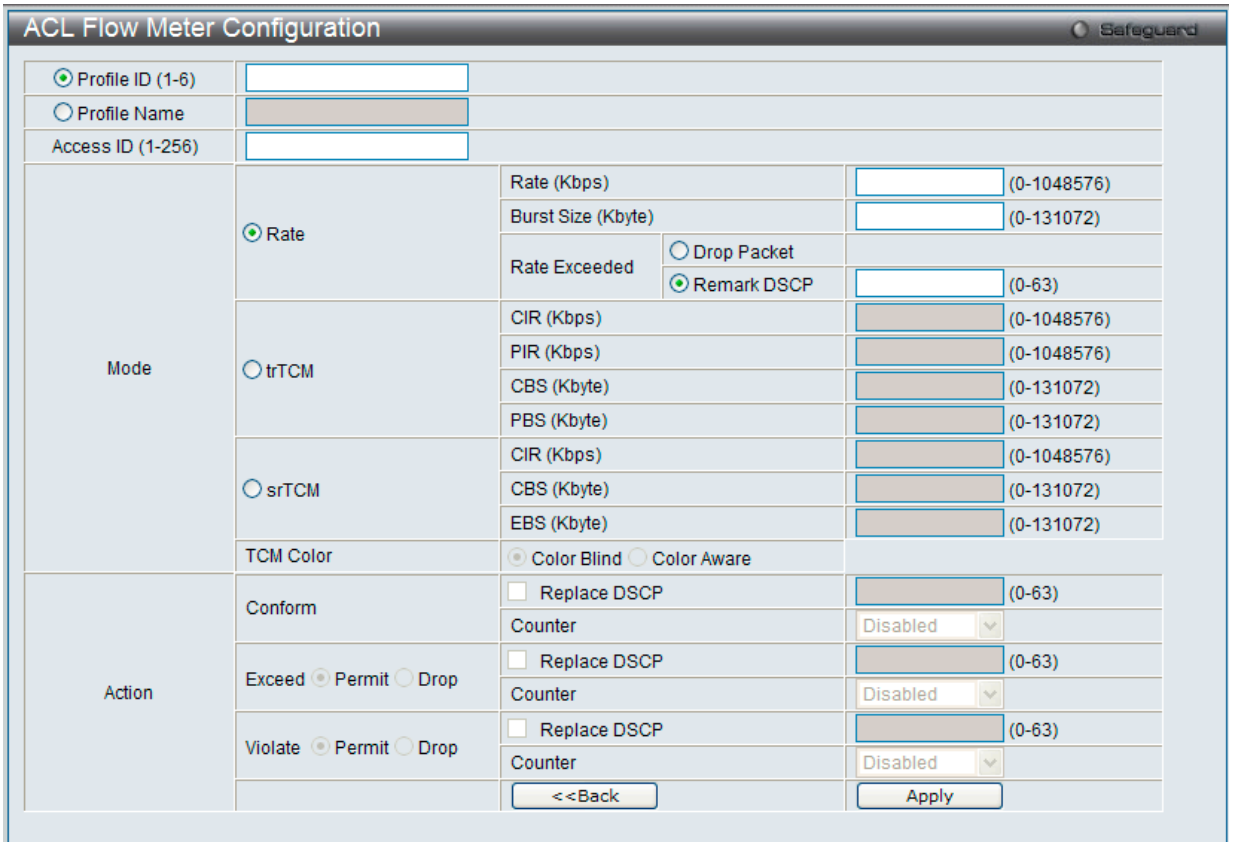


図 11-63　ACL Flow Meter Configuration 画面

以下の項目を設定します。

項目	説明
Profile ID (1-6)	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。低い値ほど高い優先度を示します。
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 (1-256)	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。低い値ほど高い優先度を示します。

項目	説明
Mode	ACL フローメータリング機能に使用するモードタイプとパケットフローの制限を選択します。 • Rate - Two Color Mode 方式のシングルレートを指定します。 - Rate - フローの帯域幅を Kbps で指定します。 - Burst Size- Two Color Mode 方式シングルレートのバーストサイズを指定します。単位は KB です。 - Rate Exceeded - Two Color Mode 方式シングルレートを越えた時のパケットの動作を指定します。次の中から選択することができます。 - Drop Packet - すぐにパケットを破棄します。 - Remark DSCP - 指定の DSCP としてパケットをマークします。 • trTCM - Two Rate Three Color Mode 方式を使用して、IP パケットフローのカラーレートを決定するために以下のパラメータを設定します。 - CIR - Committed Information Rate は 1-15624 で設定します。このレベル以下の IP フローレートは緑色とされます。PIR レートではなく、このレートを超過する IP フローレートは、黄色とされます。 - PIR - Peak Information Rate。本設定を超過する IP フローレートは、赤とされます。本フィールドは CIR 以上に設定される必要があります。 - CBS - Committed Burst Size。正常な IP パケットより大きいパケットを計測します。チェックボックスをクリックして、CBS を使用します。適切に動作するためには本機能を設定する必要はありませんが、CIR 設定に関連して使用されます。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。 - PBS - Peak Burst Size。このオプションフィールドは、PIR に関連して使用されます。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 Mode 方式を使って、IP パケットフローのカラーレートを決定するために以下のパラメータを設定します。 - CIR - Committed Information Rate は 1-15624 で設定します。カラーレートは CIR に関連して使用される以下の 2 つのフィールドに基づいています。 - 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します。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。この設定値未満のパケットフローは緑色にマークされます。この値を超過し、EBS 値以下であるパケットフローは黄色にマークされます。 - 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。この値を超過するパケットフローは、赤にマークされます。
Action	以下のフィールドに基づいて、パケットフローが色つけされる場合にアクションの過程を決定します。 • Conform - 緑色のパケットフローを表します。 - Replace DSCP - 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ます。 - Counter - チェックすることによって緑色の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。 • Exceed - 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「Permit」（許可）または「Drop」（廃棄）します。 - Replace DSCP - 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ます。 - Counter - チェックすることによって緑色の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。 • Violate - 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「Permit」（許可）または「Drop」（廃棄）します。 - Replace DSCP - 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ます。 - Counter - チェックすることによって緑色の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。

「Apply」ボタンをクリックし、設定を保存します。

エントリの変更

対応する「Modify」ボタンをクリックします。

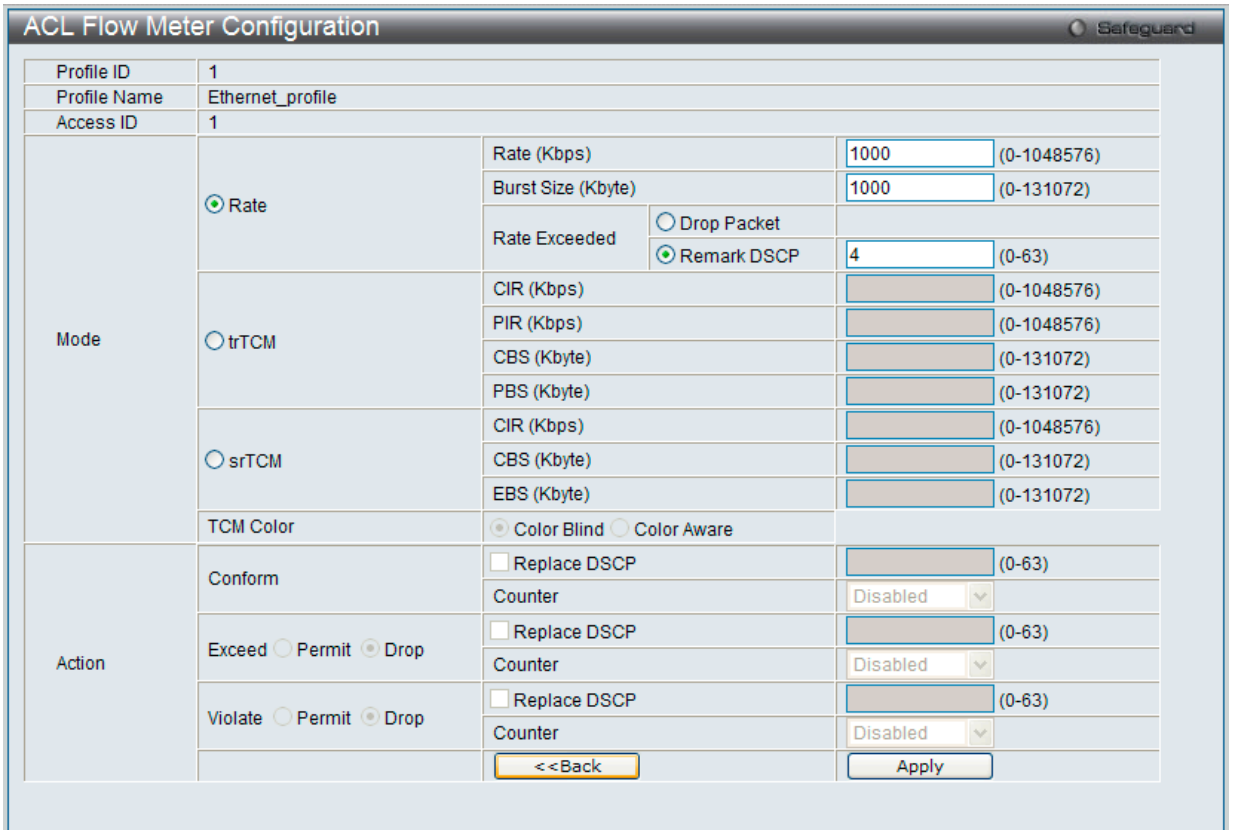


図 11-64　ACL Flow Meter Configuration 画面 - 編集

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

エントリを参照するためには、対応する「View」ボタンをクリックし、以下の画面を表示します。

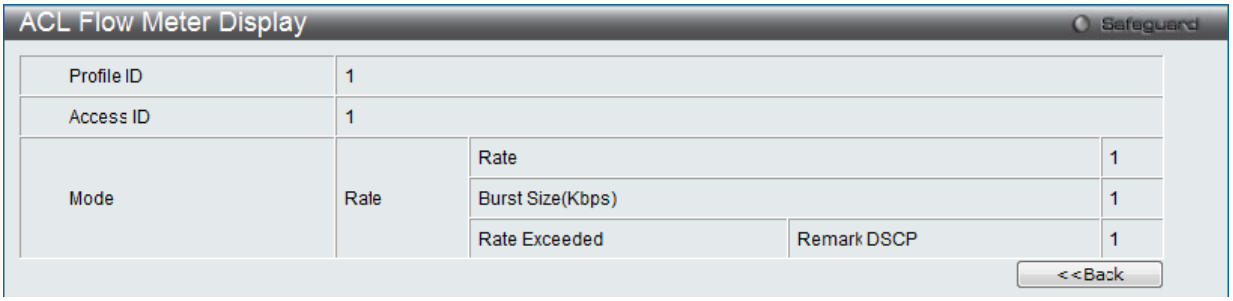


図 11-65　ACL Flow meter Display 画面

「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（イーグレスアクセスプロファイルリスト）（EI モードのみ）

イーグレス ACL はスイッチポートから送信されるパケットに対し、各フローで動作します。スイッチは「イーサネット ACL」「IPv4 ACL」「IPv6 ACL」の 3 つのプロファイルタイプをサポートします。

ACL > Egress Access Profile List の順にメニューをクリックし、表示される画面から設定します。

アクセスプロファイルとルールの作成（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。

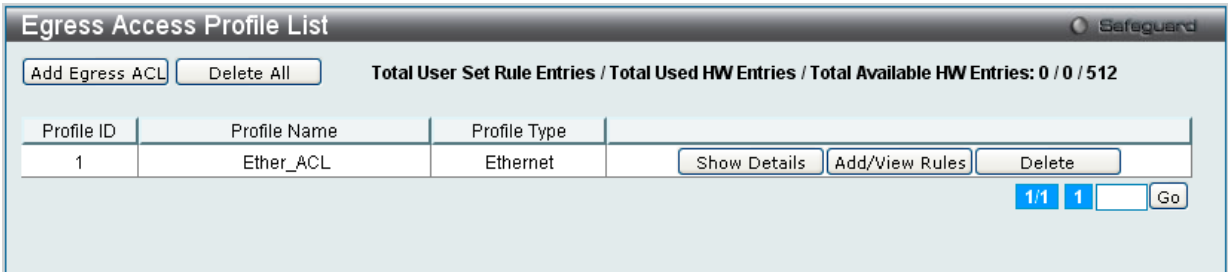


図 11-66 Egress Access Profile List 画面

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。

アクセスプロファイルの作成（Ethernet）画面

イーサネット ACL を作成する場合、「Add ACL Profile」ボタンをクリックして以下の画面を表示し、「Profile ID」および「Profile Name」を指定します。

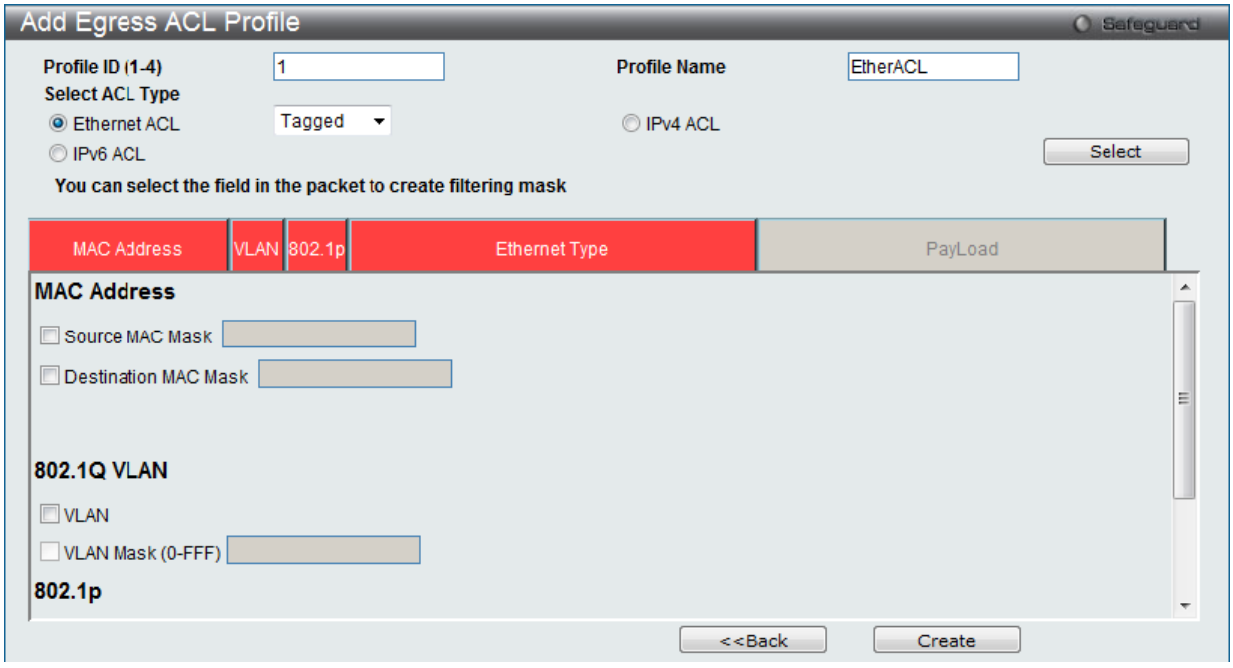


図 11-67 Add Egress ACL Profile（Ethernet ACL）画面

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」で「Ethernet ACL」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を Ethernet Egress ACL タイプに設定します。

項目	説明
Profile ID (1-4)	プロファイルに設定する番号を入力します。1-4 の間で設定可能です。低い値ほど高い優先度を示します。
Profile Name	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。 • Ethernet を ACL - パケットヘッダのレイヤ 2 部分を検証します。 • IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。 • IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。
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	このオプションを指定するパケットヘッダの 802.1Q VLAN 識別子を調べて、部分的または全体を転送基準として使用します。
802.1P	このオプションを指定するとそれぞれのパケットヘッダの 802.1p プライオリティを調べて、部分的もしくは全体を転送基準として使用します。
Ethernet Type	このオプションを指定すると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。

エントリに指定した設定の参照

「Show Details」ボタンをクリックし、以下の画面を表示します。

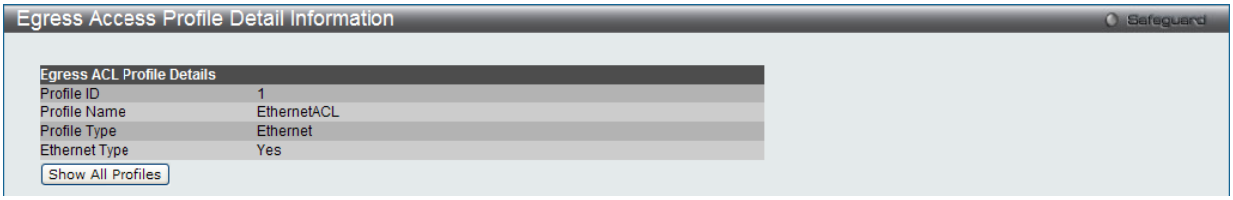


図 11-68 Egress Access Profile Detail Information（Ethernet ACL）画面

「Access Profile List」戻るためには、「Show All Profiles」ボタンをクリックします。

作成したアクセスプロファイルに対するイーグレスアクセスルールの設定手順（Ethernet）

1. 「Access Profile List」画面を表示します。

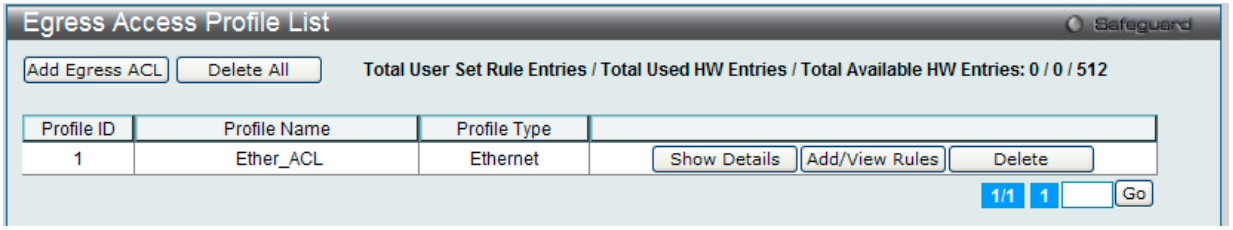


図 11-69 Egress Access Profile List 画面

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。

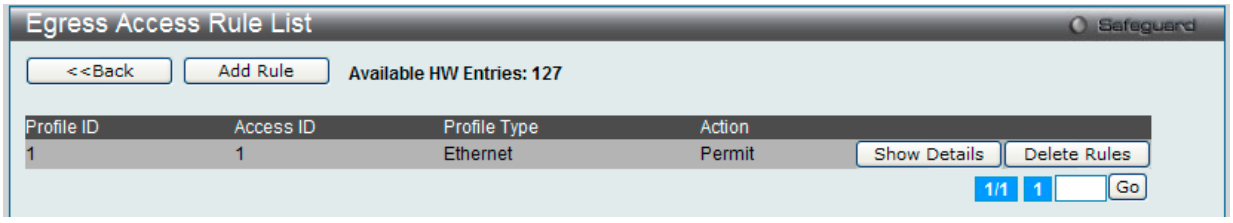


図 11-70 Egress Access Rule List - Ethernet 画面

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。

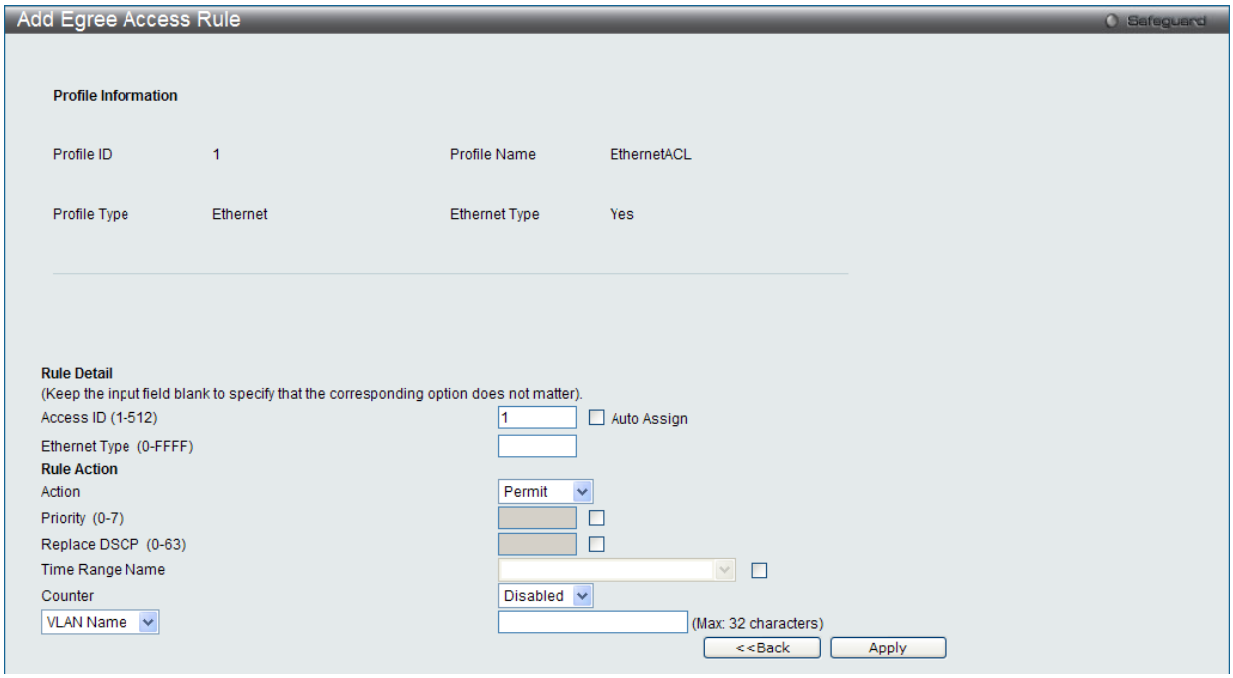


図 11-71　Add Egress Access Rule（Ethernet ACL）画面

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ます。

項目	説明
Access ID (1-128)	ルールに対して固有の識別番号を指定します。1 から 128 が指定できます。低い値ほど高い優先度を示します。 • 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。
Ethernet Type	イーサネットの種類を選択します。
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ないパケットは転送せずにフィルタリングします。
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。この項目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。 • ボックスをチェックするとパケットが条件に合った場合、CoS キューに送られる前にプライオリティフィールドの 802.1p デフォルトプライオリティが書き換えられます。しかし、パケットの 802.1p ユーザプライオリティはスイッチから転送される前に書き戻されます。 プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 189 ページの「第 10 章 QoS（QoS 機能の設定）」を参照してください。
Replace Priority	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」欄に指定した値に書き換える場合に使用します。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。
Replace DSCP (0-63)	本オプションを選択すると、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。
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	カウンタ機能を「Enabled」（有効）または「Disabled」（無効）にします。これは、オプションです。初期値は「Disabled」（無効）です。ルールがフローメータにバインドされないと、一致するすべてのパケットが無効となります。ルールがフローメータにバインドされると、本「カウンタ」は上書きされます。
Port /Port Group ID / Port Group Name/ VLAN Name / VLAN ID	プルダウンメニューを使い、事前に設定した「Port Group ID」「Port Group Name」「Ports」「VLAN Name」「VLAN ID」から、アクセスルールが有効にする項目を選択します。

「<<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。
定義済みのルールを参照するには、対象エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

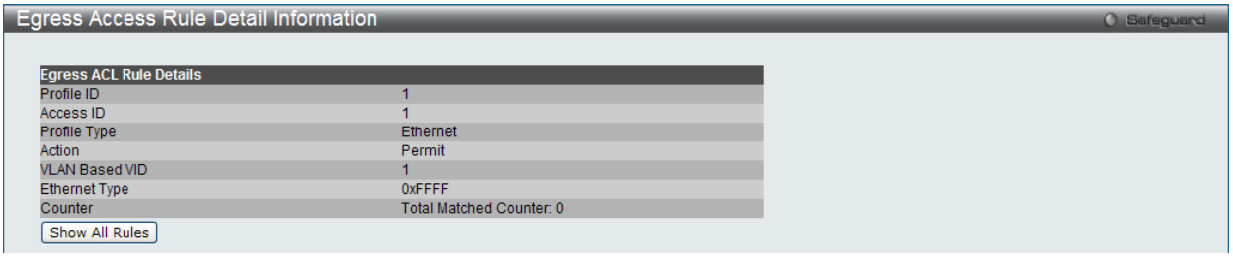


図 11-72 Egress Access Rule Detail Information（Ethernet ACL）画面

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

アクセスプロファイルとルールの作成（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。

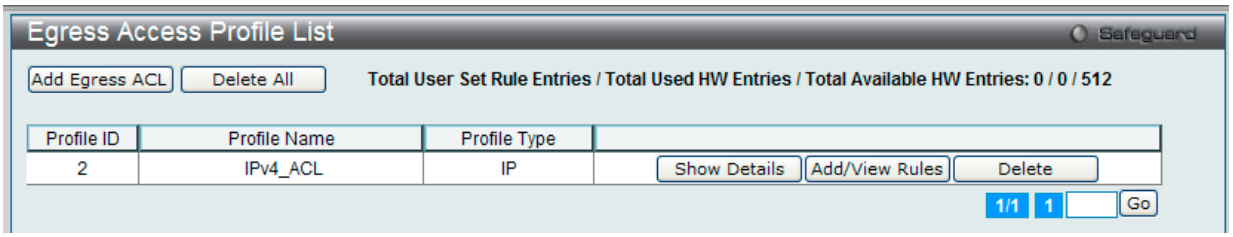


図 11-73 Egress Access Profile List 画面

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。

アクセスプロファイルの作成（IPv4）画面

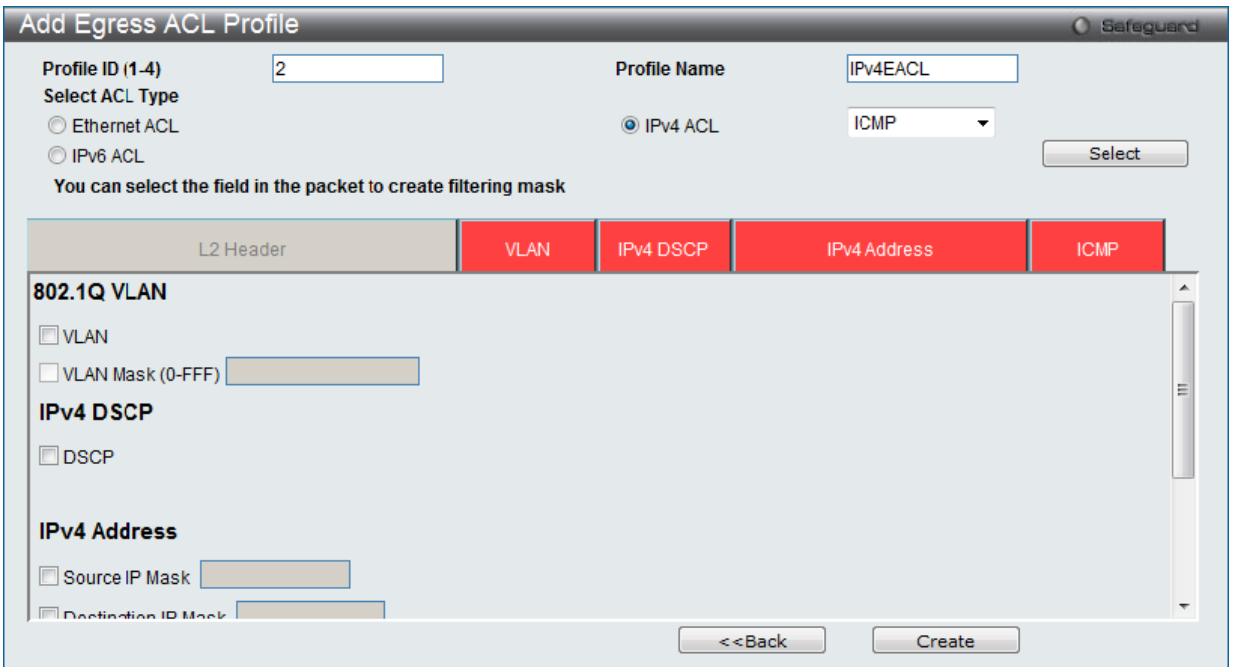


図 11-74 Add Egress ACL Profile（IPv4 ACL）画面

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」で「IPv4 ACL」をチェック後、隣接する欄で設定するフレームヘッダ（ICMP、IGMP、TCP、UDP、Protocol ID）選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を IPv4 ACL タイプに設定します。

項目	説明
Profile ID (1-4)	プロファイル設定のための固有の識別番号を指定します。1 から 4 が指定できます。低い値ほど高い優先度を示します。
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。 • Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。 • IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。 • IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。 IPv4 プロファイルを設定するためには、「IPv4 ACL」を選択し、プルダウンメニューを使用して「ICMP」、「IGMP」、「TCP」、「UDP」または「Protocol ID」を選択します。
802.1Q VLAN	このオプションを指定するパケットヘッダの 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。
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	• 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。
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。	
ICMP	各パケット内の Internet Control Message Protocol（ICMP）フィールドを調査する場合に指定します。 • Type - アクセスプロファイルを ICMP Type 値（0-255）に適用します。 • Code - アクセスプロファイルを ICMP Code（0-255）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「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。 - src port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - dst port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - flag bit - 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（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。 - src port mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - dst port mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。「User Define」マスクは 16 進数（hex 0x0-0xffffffff）で指定します。

「Create」ボタンをクリックして、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。

エントリに指定した設定の参照

「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。

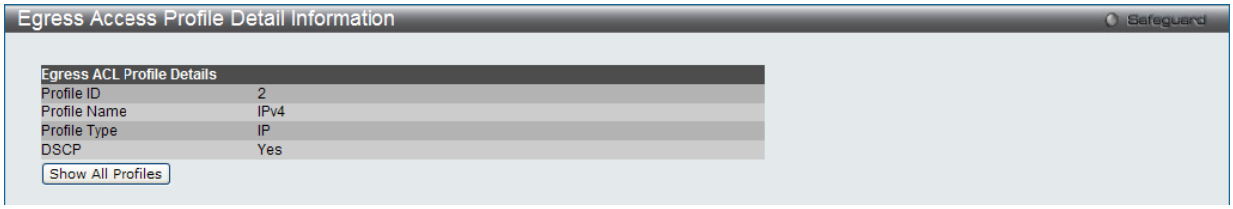


図 11-75　Egress Access Profile Detail Information (IPv4 ACL) 画面

「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イーグレスアクセスルールの設定（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。

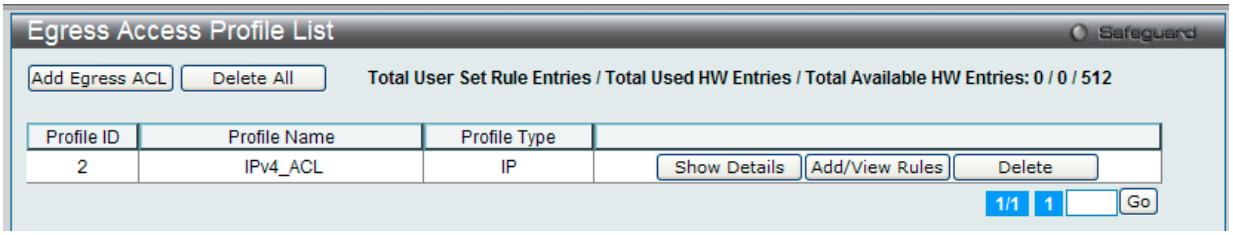


図 11-76 Egress Access Profile List 画面

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。

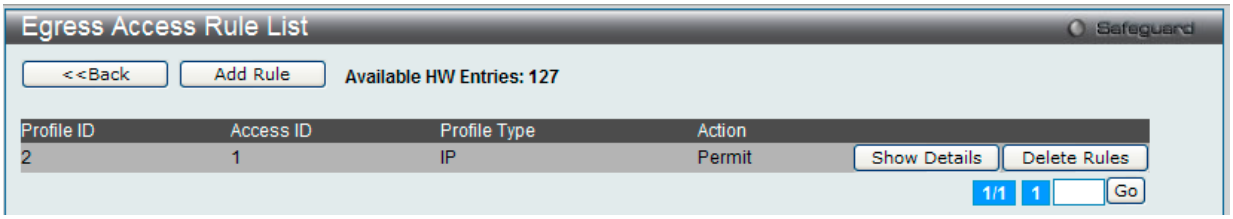


図 11-77 Egress Access Rule List - IPv4 画面

「<<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。

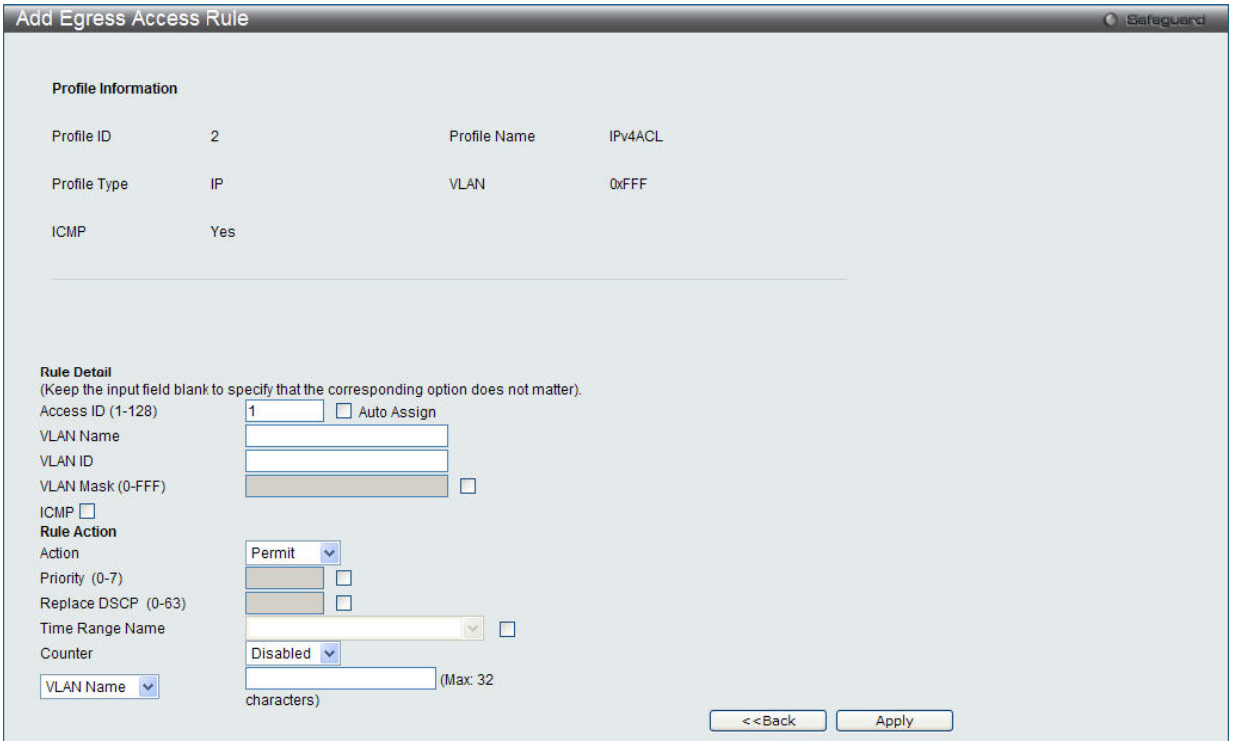


図 11-78 Add Egress Access Rule (IPv4 ACL) 画面

IPv4 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ます。

項目	説明
Access ID (1-128)	ルールに対して固有の識別番号を指定します。1 から 128 までで指定できます。低い値ほど高い優先度を示します。 • 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。
DSCP	DSCP 値を指定します。0 から 63 までで指定可能です。
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ないパケットは転送せずにフィルタリングします。
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。この項目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。 • ボックスをチェックするとパケットが条件に合った場合、CoS キューに送られる前にプライオリティフィールドの 802.1p デフォルトプライオリティが書き換えられます。しかし、パケットの 802.1p ユーザプライオリティはスイッチから転送される前に書き戻されます。 プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 189 ページの「第 10 章 QoS（QoS 機能の設定）」を参照してください。
Replace Priority（0-63）	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」欄に指定した値に書き換える場合に使用します。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。
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	カウンタ機能を「Enabled」（有効）または「Disabled」（無効）にします。
Ports	本項目にスタックスイッチ内のスイッチのポート番号を入力し、ポート単位にアクセスルールを設定指定します。ポート範囲を指定する場合は、「Access ID」の「Auto Assign」チェックボックスにチェックを入れる必要があります。チェックが入っていないと、エラーメッセージが表示され、アクセスルールは設定されません。「All Ports」チェックボックスにチェックを入れると、スイッチの全ポートを意味します。
Port Group ID / Port Group Name/ VLAN Name / VLAN ID	プルダウンメニューを使い、事前に設定した「Port Group ID」「Port Group Name」「Ports」「VLAN Name」「VLAN ID」から、アクセスルールが有効にする項目を選択します。

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。

定義済みルールの参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

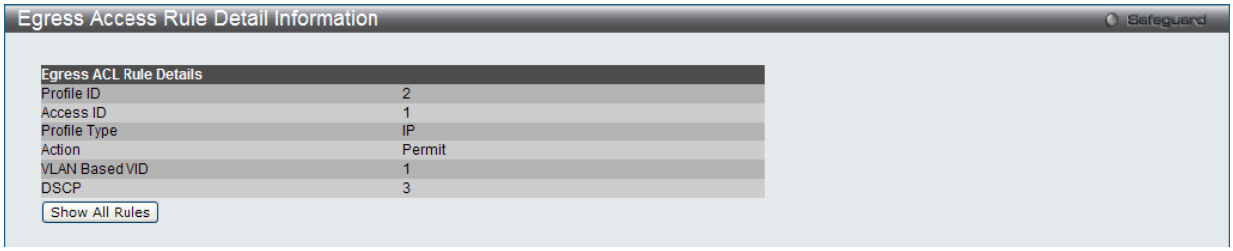


図 11-79 Egress Access Rule Detail Information (IPv4 ACL) 画面

「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とルールの作成（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。

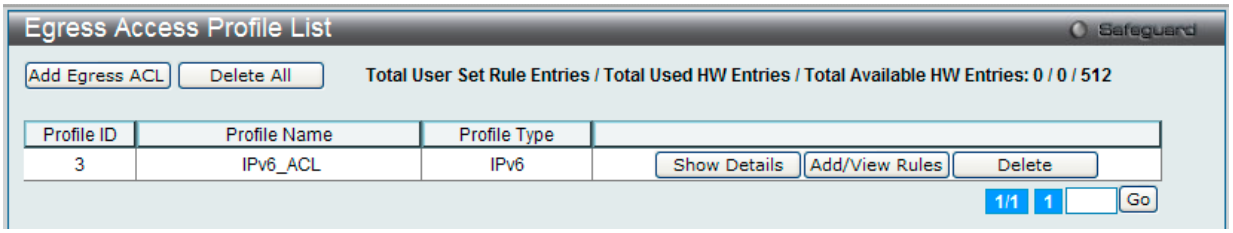


図 11-80　Egress Access Profile List 画面

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。

アクセスプロファイルの作成（IPv6）画面

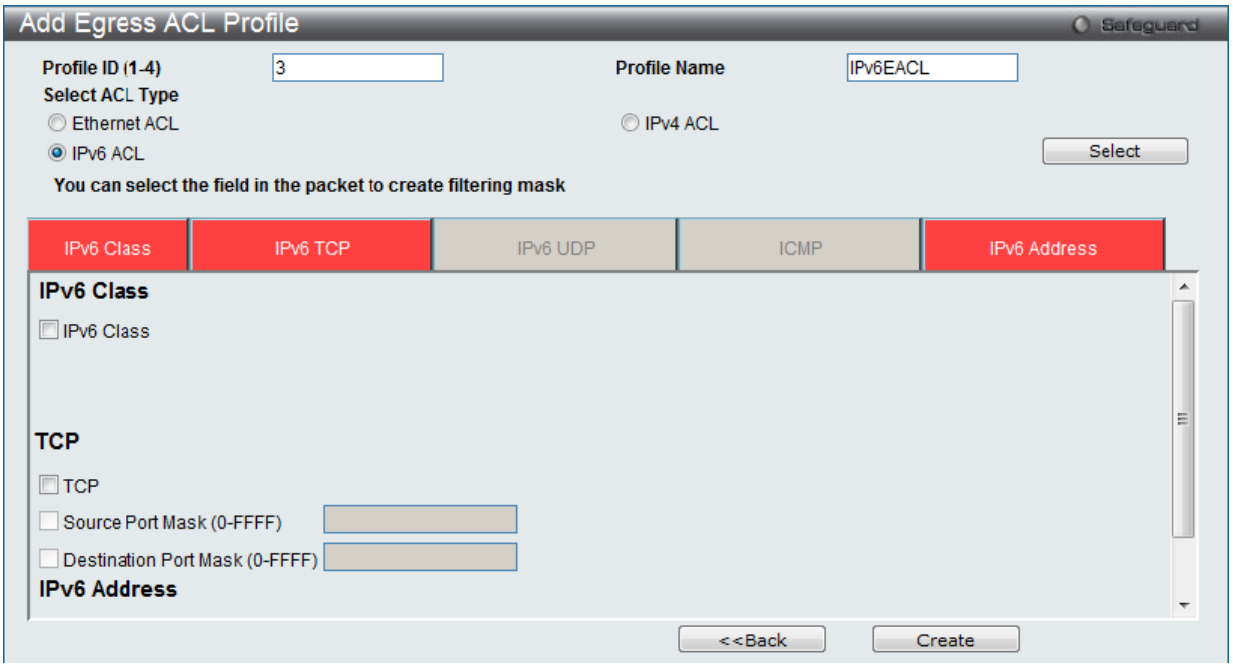


図 11-81　Add Egress ACL Profile（IPv6 ACL）画面

「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 (1-4)	ルールに対して固有の識別番号を指定します。1 から 4 が指定できます。低い値ほど高い優先度を示します。
Profile Name	作成したプロファイルの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。 • Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。 • IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。 • IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。 IPv6 プロファイルを設定するためには、「IPv6 ACL」を選択します。
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。 注意 どんな場合も、IPv6 Class と IPv6 Flow Label は共に選択し、IPv6 アドレスは単体で選択します。	
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 TCP	TCP トラフィックに当ルールを適用する場合、チェックボックスにチェックします。 指定の TCP 送信元ポートマスクが TCP 宛先ポートマスクを入力します。
IPv6 UDP	UDP トラフィックに当ルールを適用する場合、チェックボックスにチェックします。 指定の UDP 送信元ポートマスクが UDP 宛先ポートマスクを入力します。
ICMP	「ICMP」を選択するとスイッチは各フレーム内のヘッダの ICMP を確認します。
IPv6 Address	• IPv6 Source Address - ボックスにチェックをつけて送信元 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 - ボックスにチェックをつけて送信先 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。

エントリに指定した設定の参照

「Show Details」ボタンをクリックし、以下の画面を表示します。

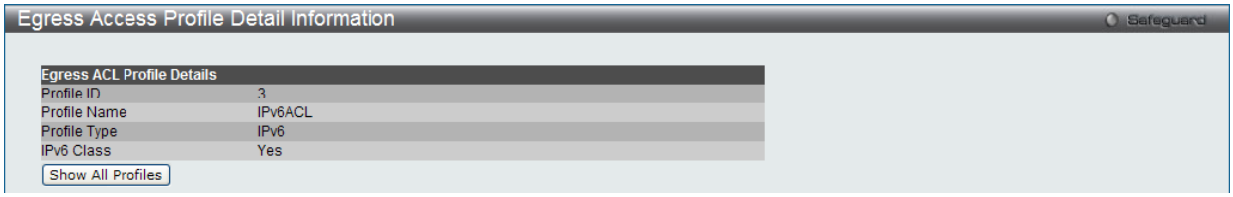


図 11-82 Egress Access Profile Detail Information（IPv6 ACL）画面

「Access Profile List」戻るためには、「Show All Profiles」ボタンをクリックします。

作成したアクセスプロファイルに対するイーグレスアクセスルールの設定（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。

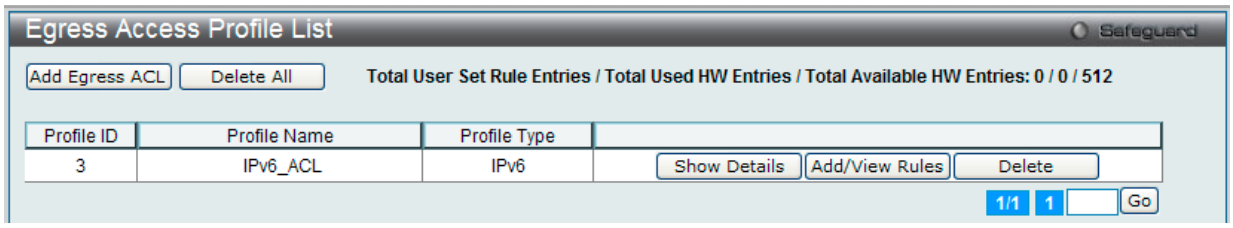


図 11-83 Egress Access Profile List 画面

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。

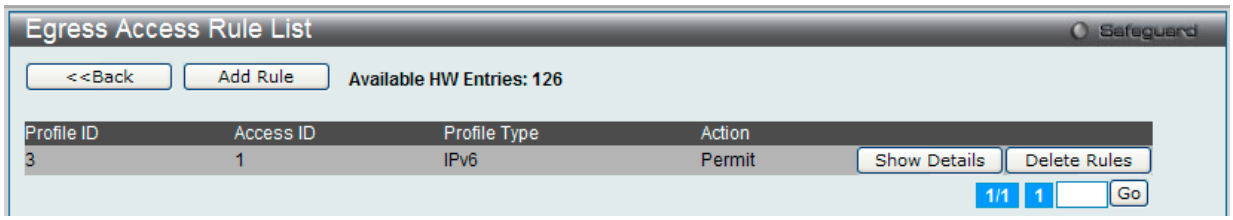


図 11-84 Egress Access Rule List - IPv6 画面

「<<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。

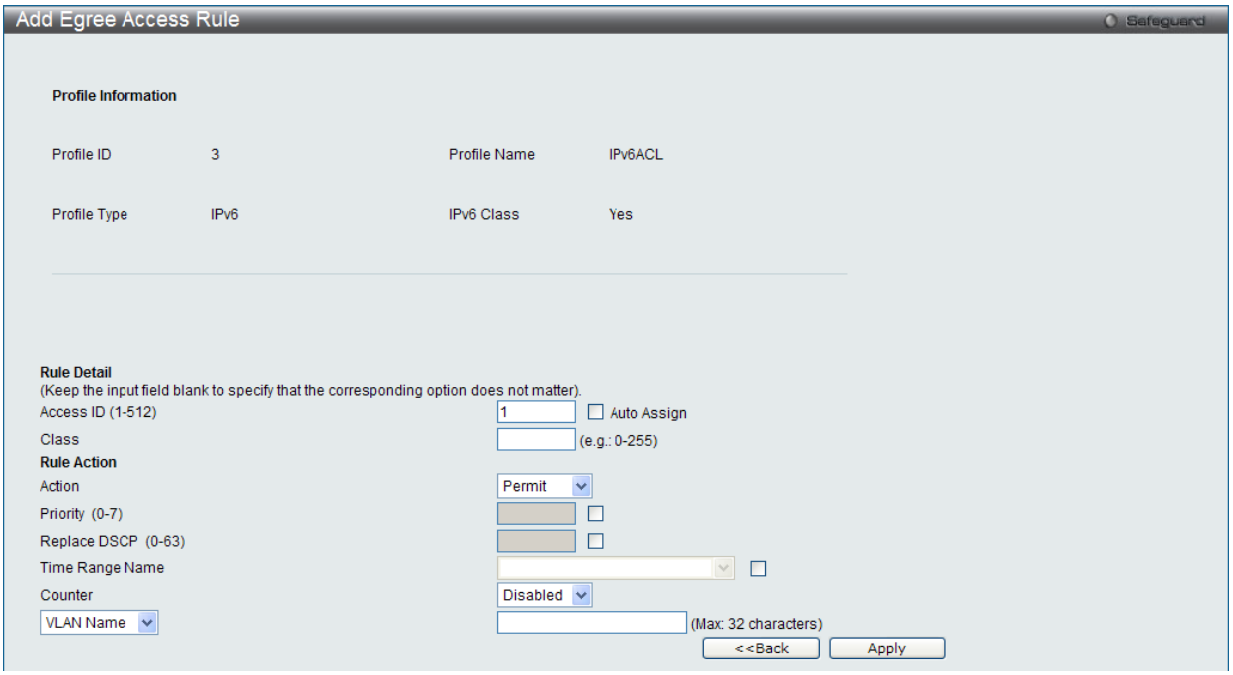


図 11-85　Add Egress Access Rule (IPv6 ACL) 画面

IPv6 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ます。

項目	説明
Access ID (1-128)	ルールに対して固有の識別番号を指定します。1 から 128 まで指定できます。低い値ほど高い優先度を示します。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Class	IPv6 ヘッダのクラス項目にスイッチを構成するクラスを入力します。パケットヘッダの一部である本項目は ToS や IPv4 Precedence ビットと類似しています。
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ないパケットは転送せずにフィルタリングします。
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により使用される CoS キューが決まります。この項目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。 • ボックスをチェックするとパケットが条件に一致した場合、CoS キューに送られる前にプライオリティ欄の 802.1p デフォルトプライオリティが書き換えられます。しかし、パケットの 802.1p ユーザプライオリティはスイッチから転送される前に書き戻されます。 プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 189 ページの「第 10 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欄に指定した値に書き換えます。
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	カウンタ機能を「Enabled」（有効）または「Disabled」（無効）にします。
Ports	本項目にスタックスイッチ内のスイッチのポート番号を入力し、ポート単位にアクセスルールを設定指定します。ポート範囲を指定する場合は、「Access ID」の「Auto Assign」チェックボックスにチェックを入れる必要があります。チェックが入っていないと、エラーメッセージが表示され、アクセスルールは設定されません。「All Ports」チェックボックスにチェックを入れると、スイッチの全ポートを意味します。
Port Group ID / Port Group Name/ VLAN Name / VLAN ID	プルダウンメニューを使い、事前に設定した「Port Group ID」「Port Group Name」「Ports」「VLAN Name」「VLAN ID」から、アクセスルールが有効にする項目を選択します。

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。

定義済みルールの参照

対象エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

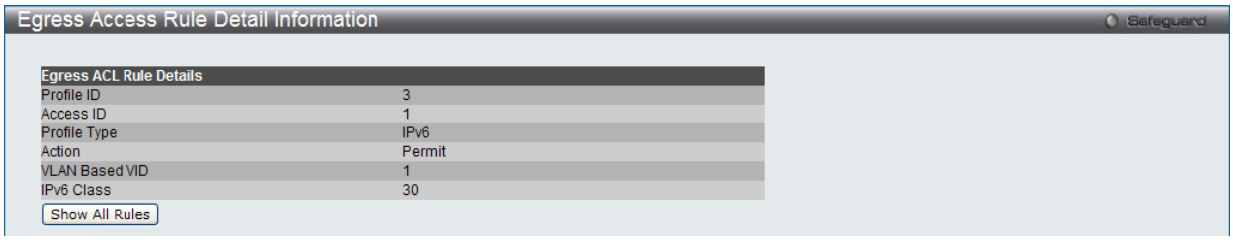


図 11-86 Egress Access Rule Detail Information (IPv6 ACL) 画面

Egress ACL Flow Meter（Egress ACL フローメータリング）（EI モードのみ）

Egress ACL フローメータ機能の設定を行います。

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。

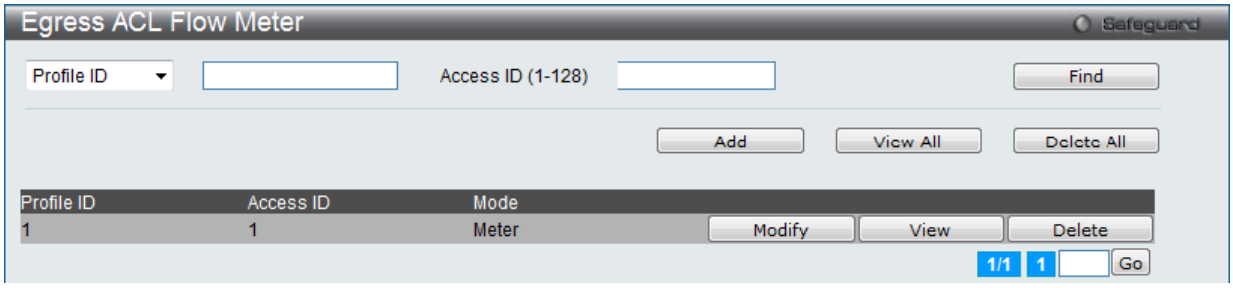


図 11-87 Egress ACL Flow Meter 画面

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。低い値ほど高い優先度を示します。
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。低い値ほど高い優先度を示します。

適切な情報を入力し、「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。

エントリの追加 / 編集

対応する「Add」または「Modify」ボタンをクリックします。「Add」ボタンをクリックすると以下の画面が表示されます。

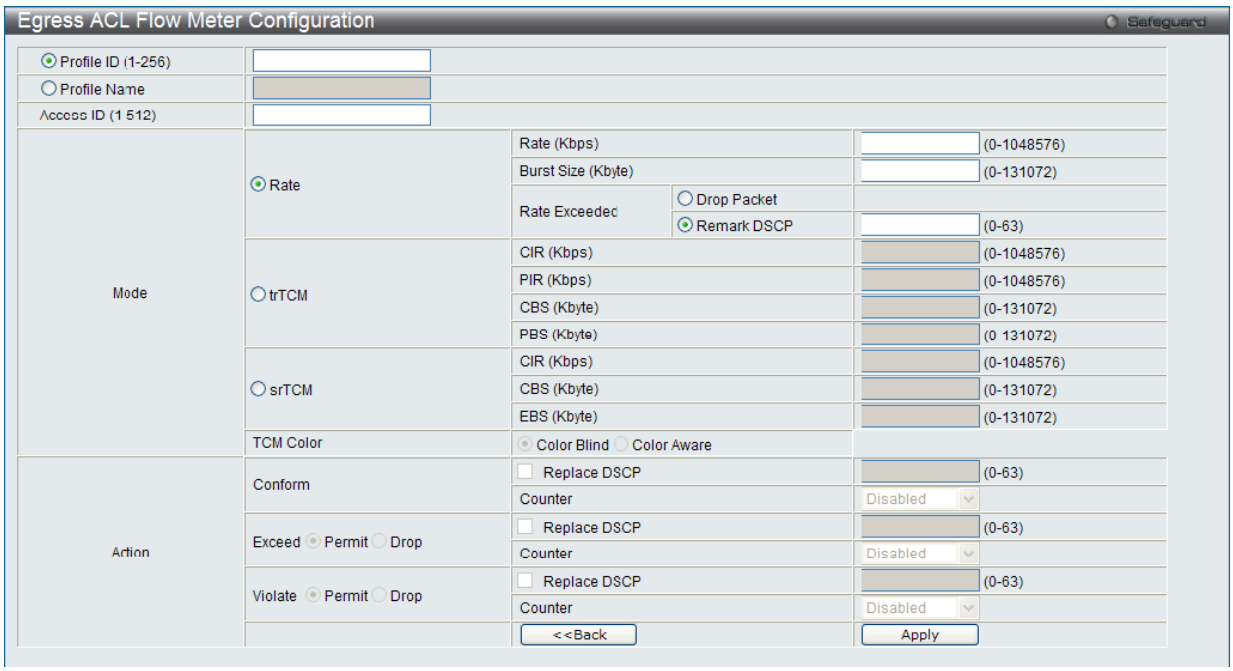


図 11-88 Egress ACL Flow Meter Configuration 画面

以下の項目を設定します。

項目	説明
Profile ID (1-4)	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。低い値ほど高い優先度を示します。
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。低い値ほど高い優先度を示します。
Mode	ACL フローメータリング機能に使用するモードタイプとパケットフローの制限を選択します。 • Rate - Two Color Mode 方式のシングルレートを指定します。 - Rate - フローの帯域幅を Kbps で指定します。 - Burst Size- Two Color Mode 方式シングルレートのバーストサイズを指定します。単位は KB です。 - Rate Exceeded - Two Color Mode 方式シングルレートを越えた時のパケットの動作を指定します。次の中から選択することができます。 - Drop Packet - すぐにパケットを破棄します。 - Remark DSCP - 指定の DSCP としてパケットをマークします。 • trTCM - Two Rate Three Color Mode 方式を使用して、IP パケットフローのカラーレートを決定するために以下のパラメータを設定します。 - CIR - Committed Information Rateは 1-15624 で設定します。このレベル以下の IP フローレートは緑色とされます。PIR レートではなく、このレートを超過する IP フローレートは、黄色とされます。 - PIR - Peak Information Rate。本設定を超過する IP フローレートは、赤とされます。本フィールドは CIR 以上に設定される必要があります。 - CBS - Committed Burst Size。正常な IP パケットより大きいパケットを計測します。チェックボックスをクリックして、CBS を使用します。適切に動作するためには本機能を設定する必要はありませんが、CIR 設定に関連して使用されます。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 を設定さする必要があります。 - PBS - Peak Burst Size。このオプションフィールドは、PIR に関連して使用されます。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 Mode 方式を使って、IP パケットフローのカラーレートを決定するために以下のパラメータを設定します。 - CIR - Committed Information Rate は 1-15624 で設定します。カラーレートは CIR に関連して使用される以下の 2 つのフィールドに基づいています。 - 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します。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。この設定値未満のパケットフローは緑色にマークされます。この値を超過し、EBS 値以下であるパケットフローは黄色にマークされます。 - EBS - Excess Burst Size。バイ数を計測する場合、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。この値を超過するパケットフローは、赤にマークされます。
Action	以下のフィールドに基づいて、パケットフローが色つけされる場合にアクションの過程を決定します。 • Confirm - 緑色のパケットフローを表します。 - Replace DSCP - 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ます。 - Counter - チェックすることによって緑色の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。 • Exceed - 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「Permit」（許可）または「Drop」（廃棄）します。 - Replace DSCP - 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ます。 - Counter - チェックすることによって緑色の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。 • Violate - 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「Permit」（許可）または「Drop」（廃棄）します。 - Replace DSCP - 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ます。 - Counter - チェックすることによって緑色の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。

「Apply」ボタンをクリックし、設定を保存します。

「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

「View」ボタンをクリックすると次の画面が表示されます。

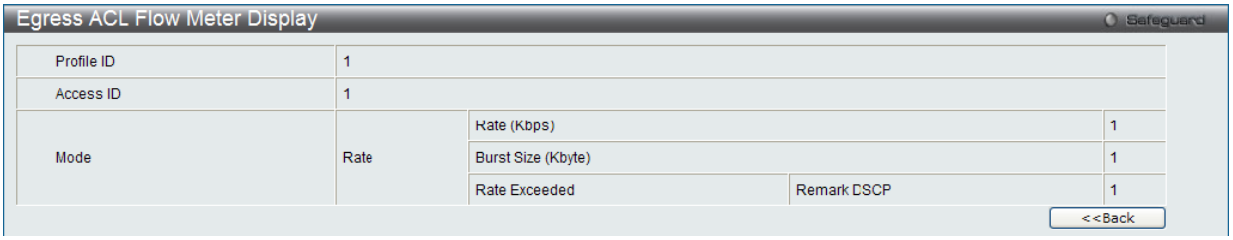


図 11-89 Egress ACL Flow meter Display 画面

第 12 章　Security（セキュリティ機能の設定）

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

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

サブメニュー	説明	参照ページ
802.1X（802.1X 設定）	802.1X 認証を設定します。以下のメニューがあります。 802.1X Global Settings（802.1X グローバル設定）、802.1X Port Settings（802.1X ポート設定）、802.1X User Settings（802.1X ユーザ設定）、Guest VLAN（ゲスト VLAN の設定）、Authenticator State（オーセンティケータの状態）、Authenticator Statistics（オーセンティケータ統計情報）、Authenticator Session Statistics（オーセンティケータセッション統計情報）、Authenticator Diagnostics（オーセンティケータ診断）、Initialize Port-based Port(s)（初期化ポート - ポートベース）、Initialize Host-based Port(s)（初期化ポート - ホストベース）、Reauthenticate Port-based Port(s)（再認証ポート - ポートベース）、Reauthenticate Host-based Port(s)（再認証ポート - ホストベース）	250
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）	261
IP-MAC-Port Binding（IP-MAC- ポートバインディング）（EI モードのみ）	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 スヌーピング設定）、ND Snooping Entry（ND Snooping エントリ）	264
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認証情報）	270
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）、WAC Customize Page（WAC カスタマイズページ設定）	274
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）	280
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）、Compound Authentication MAC Format Settings（コンパウンド認証 MAC 形式設定）	285
IGMP Access Control Settings（IGMP アクセスコントロール設定）	各ポートに IGMP 認証（IGMP アクセスコントロール）を設定します。	288
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）	289
ARP Spoofing Prevention Settings（ARP スプーフィング防止設定）	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。	293
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。	294
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。	295
RPC PortMapper Filter Settings（RPC ポートマップフィルタ設定）	RPC ポートマップフィルタの設定を指定のポートに行います。	296
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。	297
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。	298
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）	299

サブメニュー	説明	参照ページ
Access Authentication Control（アクセス認証コントロール）	TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。以下のメニューがあります。Enable Admin（管理者レベルの認証）、Authentication Policy Settings（認証ポリシー設定）、Application Authentication Settings（アプリケーションの認証設定）、Accounting Settings（アカウント設定）、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（メソッドリスト設定）、Accounting Method Lists Settings（アカウンティングメソッドリスト設定）、Local Enable Password Settings（ローカルユーザパスワード設定）	300
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。以下のメニューがあります。SSL Settings（SSL 設定）、SSL Certification Settings（SSL 証明書設定）	309
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）	311
DoS Attack Prevention Settings（DoS 攻撃防止設定）	各 DoS 攻撃に対して防御設定を行います。	315
Trusted Host Settings（トラストホスト）	リモートのスイッチ管理用トラストホストを設定します。	316
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。	317

802.1X（802.1X 認証設定）

802.1X（ポートベースおよびホストベースのアクセスコントロール）

IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。本方式は、ネットワークへアクセスするユーザを認証するために RADIUS サーバを使用し、EAPOL（Extensible Authentication Protocol over LAN）と呼ばれるパケットをクライアント・サーバ間で中継することにより実現します。以下の図は基本的な EAPOL パケットの構成を示しています。

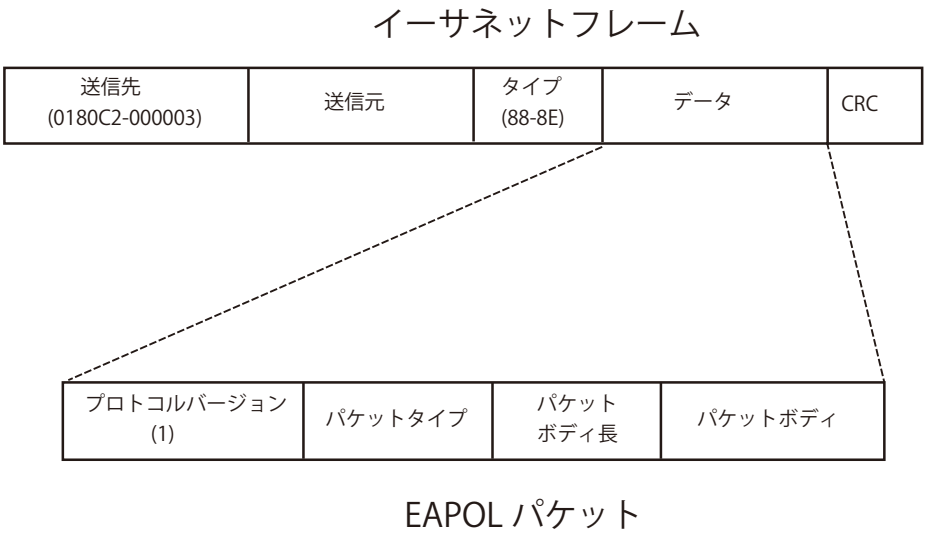


図 12-1　EAPOL パケット

本方法を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。EAPOL パケットは、承認が与えられるまでの間指定ポート経由で送受信される唯一のトラフィックです。802.1X アクセスコントロール方式は 3 つの役割を持っており、それぞれがアクセスコントロールセキュリティ方法の作成、状態の保持および動作のために必要不可欠です。

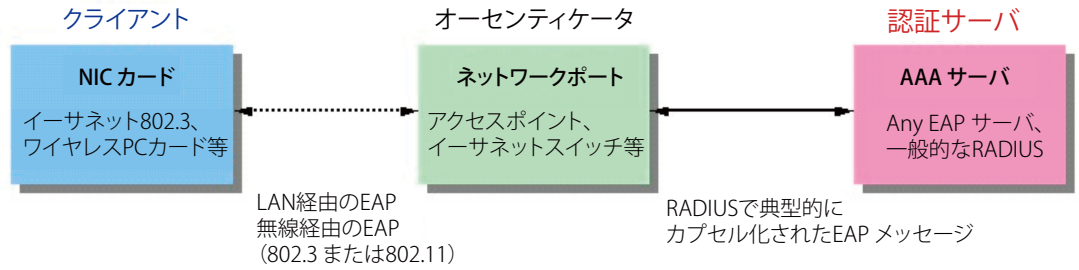


図 12-2　802.1X の 3 つの要素

以下の項では、クライアント、オーセンティケータ、および認証サーバのそれぞれの役割について詳しく説明します。

認証サーバ

認証サーバはクライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。認証サーバ上では RADIUS サーバプログラムを実行し、またそのサーバのデータがオーセンティケータ側（スイッチ）に正しく登録されている必要があります。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを受ける前に、認証サーバ（RADIUS）による認証を受ける必要があります。認証サーバは、RADIUS サーバとクライアントの間で EAPOL パケットを通じて信頼できる情報を交換し、そのクライアントの LAN やスイッチサービスへのアクセス許可の有無をスイッチに通知します。このように、認証サーバの役割は、ネットワークにアクセスを試みるクライアントの身元を保証することです。

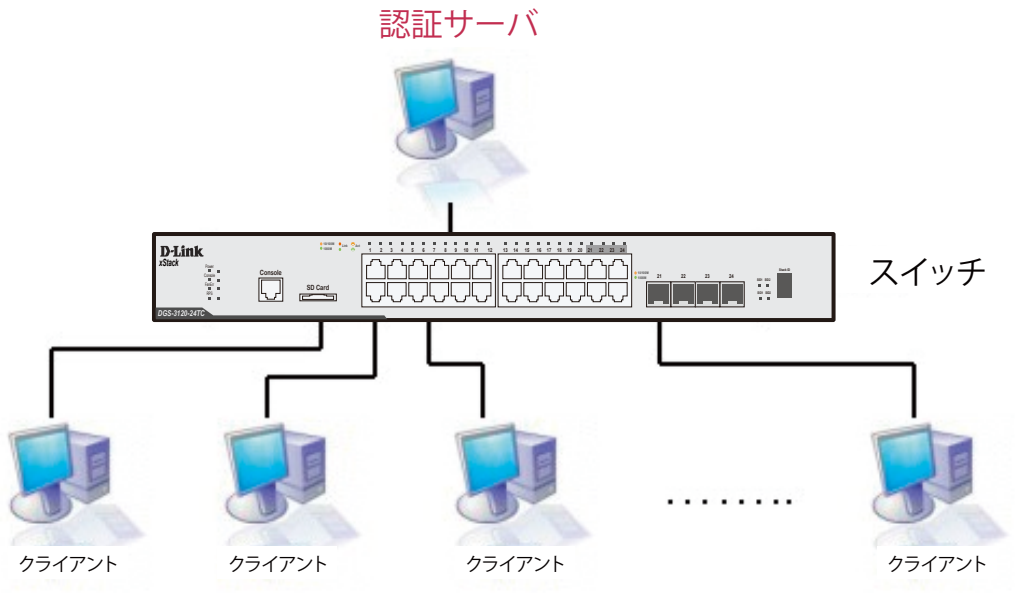


図 12-3　認証サーバ

オーセンティケータ

オーセンティケータ（スイッチ）は、認証サーバとクライアントの間を取り持つ、仲介の役割を果たします。802.1X を使用する場合、オーセンティケータサーバには 2 つの目的があります。 1 つ目の目的は、クライアントに EAPOL パケットを通して認証情報を提出するよう要求することです。EAPOL パケットはクライアントにアクセスが許可される前にオーセンティケータを通過することのできる唯一の情報です。2 つ目の目的はクライアントから収集した情報を、認証サーバに確認してもらい、その結果をクライアントに伝達することです。

スイッチをオーセンティケータとして正しく設定するためには、以下の 3 つの手順を実行する必要があります。

1. 802.1X 機能を有効にします。（**Security > 802.1X > 802.1X Global Settings**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Port Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > RADIUS > Authentication RADIUS Server Settings**）

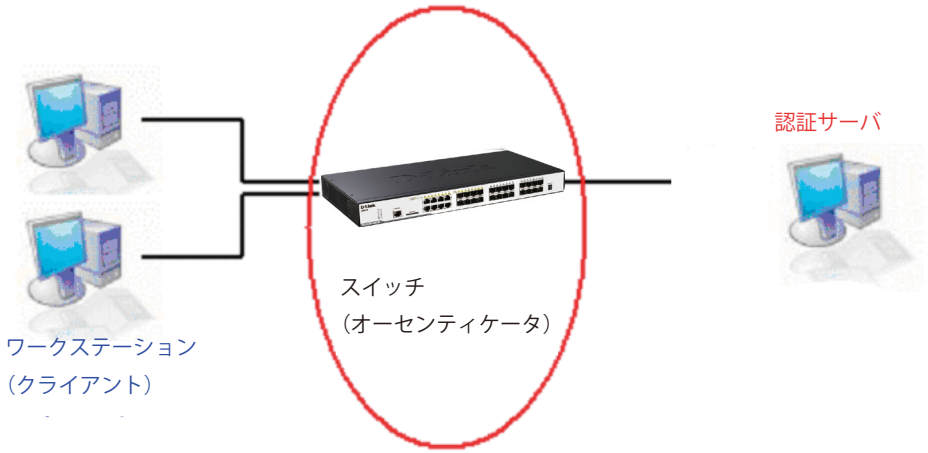


図 12-4　オーセンティケータ

クライアント

クライアントとは、簡単に言うと LAN やスイッチが提供するサービスへのアクセスを希望するワークステーションです。クライアントとなるワークステーションでは、802.1X プロトコルに準拠したソフトウェアが起動している必要があります。Windows XP 使用の場合には、OS 内に既にそのようなソフトウェアが組み込まれています。それ以外の場合には、802.1X クライアントソフトウェアを別途用意する必要があります。クライアントは EAPOL パケットを使用して LAN へのアクセスを要求し、またスイッチからの要求に対しても応答します。

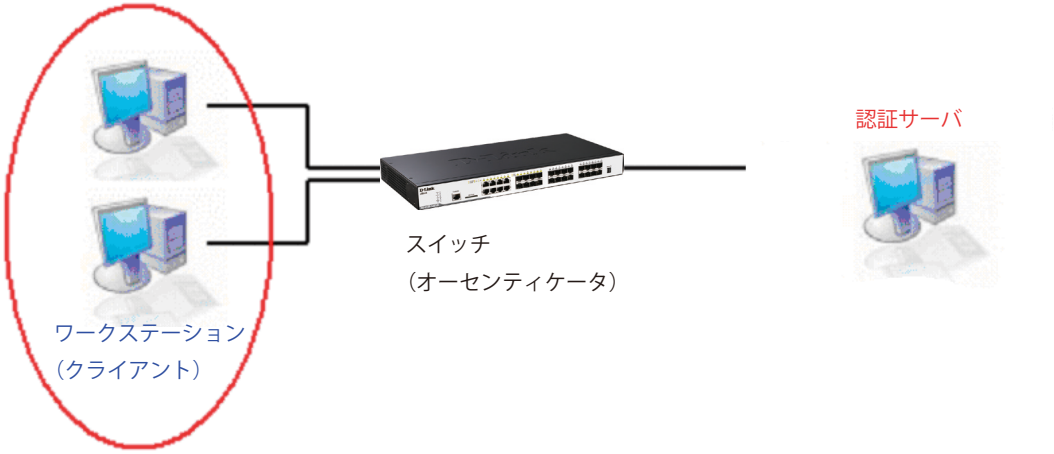


図 12-5　クライアント

認証プロセス

これらの 3 つの要素により、802.1X プロトコルはネットワークへのアクセスを試みるユーザの認証を安定的かつ安全に行います。認証に成功する前は、EAPOL トラフィックのみが特定ポートの通過を許可されます。このポートは、有効なユーザ名とパスワード（802.1X の設定で MAC アドレスも指定されている場合は MAC アドレスも）を持つクライアントがアクセス権を取得してポートのロックが解除されるまで、ロック状態を保ちます。ロックが解除されると、通常のトラフィックがポートを通過できるようになります。D-Link が実装する 802.1X では以下の 2 種類のアクセスコントロールが選択できます。

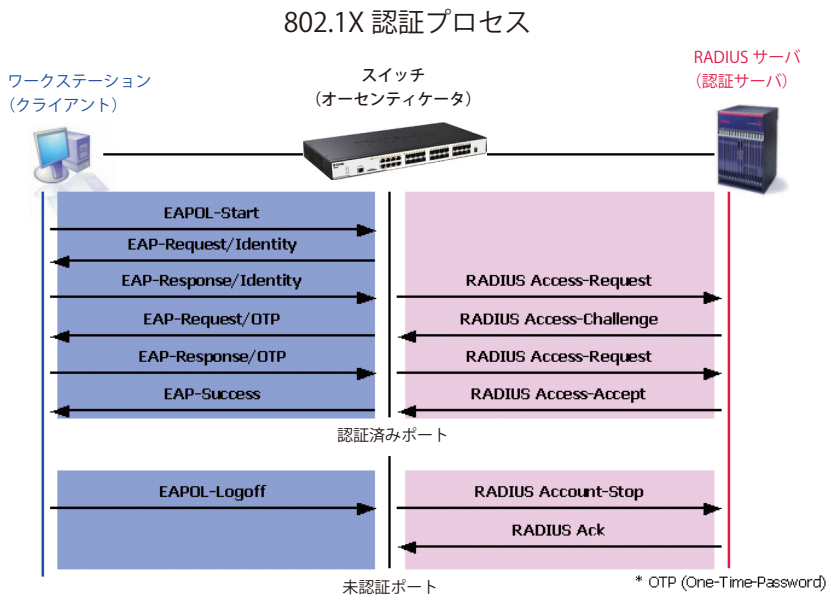


図 12-6　802.1X 認証プロセス

本スイッチの 802.1X 機能では、以下の 2 つのタイプのアクセスコントロールから選択することができます。

1. ポートベースのアクセスコントロール
   本方式では、 1 人のユーザがリモートの RADIUS サーバにポートごとの認証をリクエストし、残りのユーザも同じポートをアクセスできるようにします。
2. MAC ベースのアクセスコントロール
   本方式では、スイッチは自動的に各ポートに対して複数の 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 の開発の本来の目的は、LAN 上で Point to Point プロトコルの機能を利用することでした。インフラストラクチャのように単一の LAN セグメントが 2 個以上のデバイスを持たない場合、どちらかがブリッジポートとなります。ブリッジポートは、リンクのリモートエンドにあるアクティブなデバイスの接続を示すイベントや、アクティブなデバイスが非アクティブ状態に遷移することを示すイベントの検知を行います。これらのイベントをポートの認証状態の制御に利用し、ポートでの認証が行わない場合に接続デバイスの認証プロセスを開始します。これをポートベースのアクセスコントロールと呼びます。

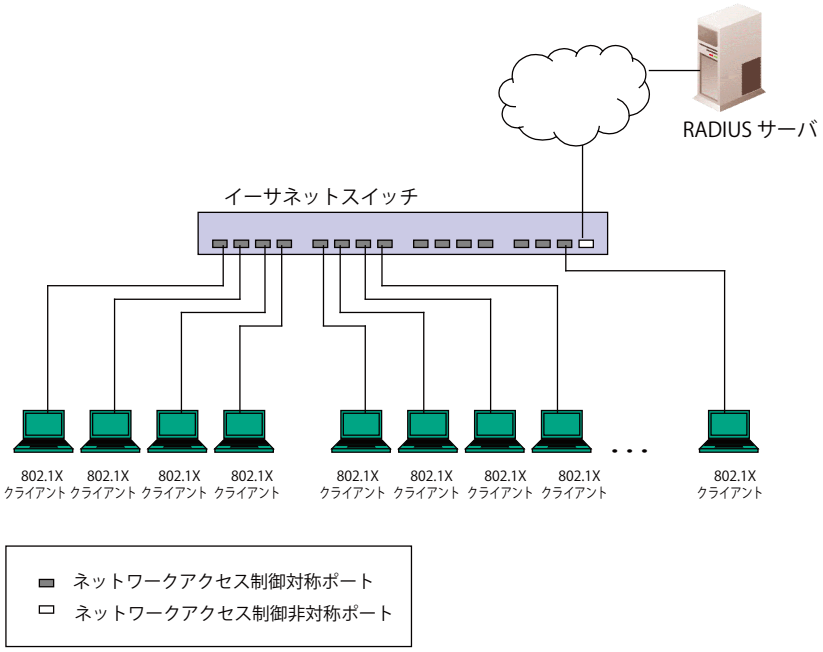


図 12-7　典型的なポートベースアクセスコントロールのネットワーク構成例

一度接続デバイスが認証に成功すると、ポートは Authorized（認証済み）状態になり、ポートが未認証になるようなイベントが発生するまでポート上のすべてのトラフィックはアクセスコントロール制限の対象となりません。そのため、ポートが 1 台以上のデバイスが所属する共有 LAN セグメントに接続される場合、接続デバイスの 1 つが認証に成功すると共有セグメント上のすべての LAN に対して事実上アクセスを許可することになります。このような状態のセキュリティは明らかに脆弱であると言えます。

ホストベースのネットワークアクセスコントロール

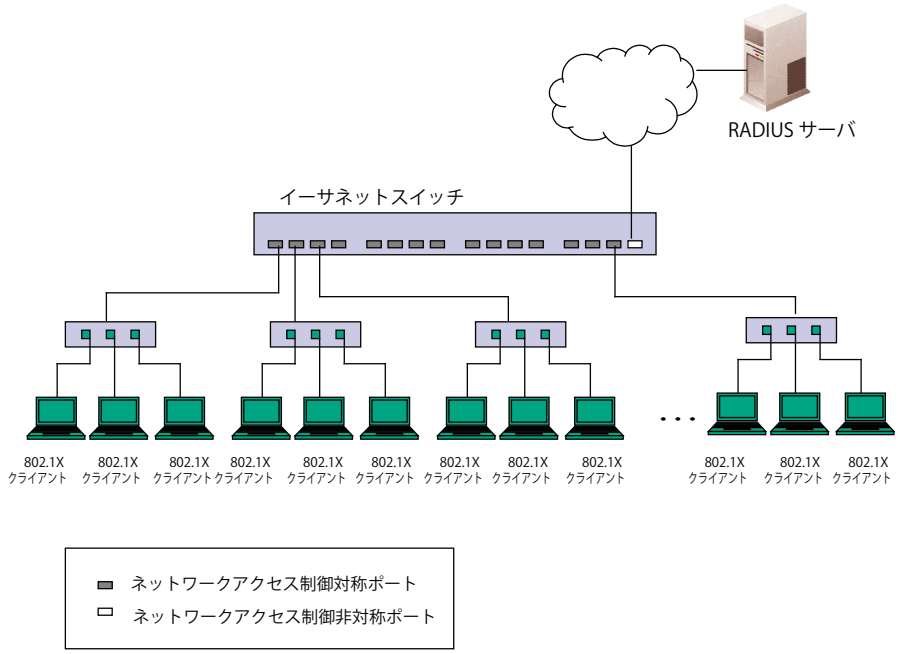


図 12-8　典型的な MAC ベースアクセスコントロールのネットワーク構成例

共有 LAN セグメント内で 802.1X を活用するためには、LAN へのアクセスを希望する各デバイスに「仮想」ポートを定義する必要があります。するとスイッチは共有 LAN セグメントに接続する 1 つの物理ポートを、異なる論理ポートの集まりであると認識し、それら仮想ポートを EAPOL の交換と認証状態に基づいて別々に制御します。スイッチは接続する各デバイスの MAC アドレスを学習し、それらのデバイスがスイッチ経由で LAN と通信するための仮想ポートを確立します。

802.1X Global Settings（802.1X グローバル設定）

本画面では 802.1X グローバル設定を行います。

802.1X 認証設定をするには、**Security > 802.1X > 802.1X Global Settings** の順にメニューをクリックします。

図 12-9　802.1X Global Settings 画面

この画面では以下の機能を設定できます。

項目	説明
Authentication Mode	802.1X 認証モードを「Disabled」、「Port Based」、「MAC Based」から選択します。「Mac Based」を選択した場合、ホストベースネットワークアクセスコントロールが、ポートに適用されます。
Authentication Protocol	認証プロトコルを「Auth Protocol」、「RADIUS EAP」または「Local」から選択します。
Forward EAPOL PDU	スイッチが EAPOL PDU 要求を再送するのを有効、または無効にします。
Max User (1-448)	802.1X 認証対象ユーザの最大数を指定します。
RADIUS Authorization	RADIUS 認証を有効 / 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。

802.1X Port Settings（802.1X ポート設定）

802.1X 認証ポートを設定します。

Security > 802.1X > 802.1X Port Settings の順にメニューをクリックします。

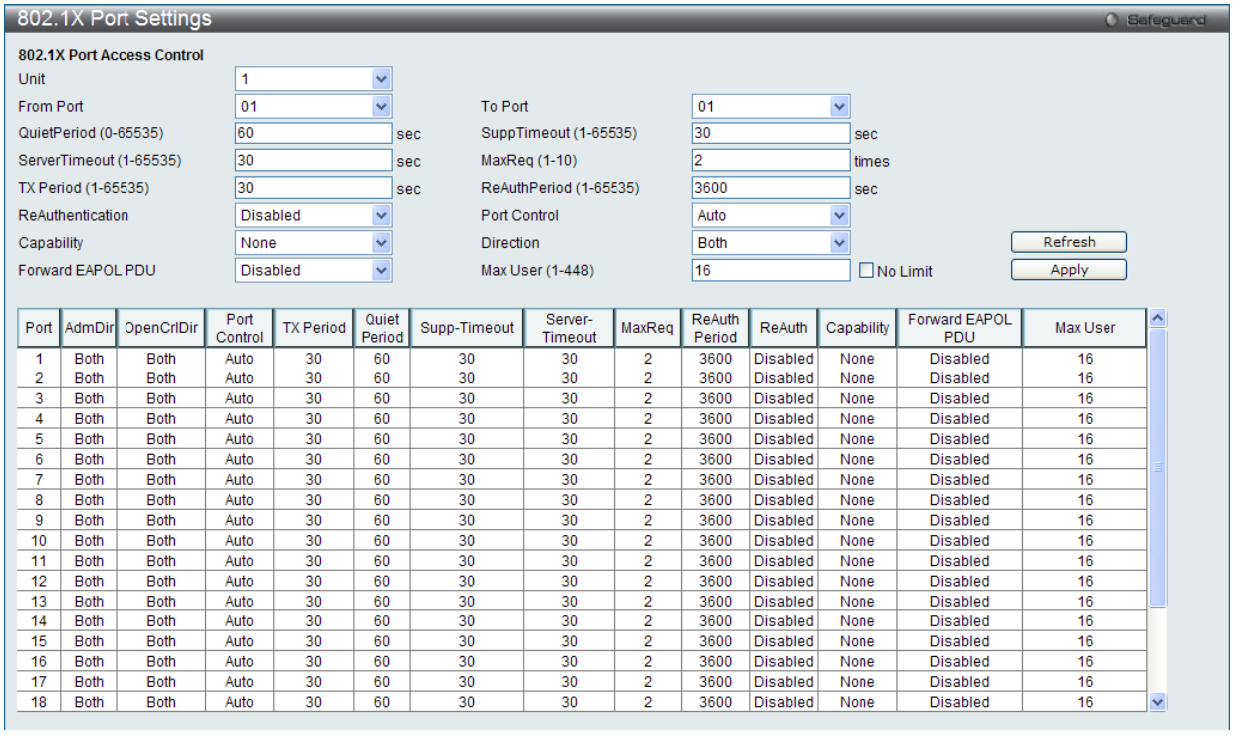


図 12-10　802.1X Settings 画面

この画面では以下の機能を設定できます。

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象のポート範囲を指定します。
QuietPeriod (0-65535)	クライアントと認証の交換を失敗した後スイッチが quiet 状態を維持する秒数を指定します。初期値は 60（秒）です。
SuppTimeout (1-65535)	Authenticator とクライアントの通信が切れてタイムアウト状態となる時間を指定します。初期値は 30（秒）です。
ServerTimeout (1-65535)	Authenticator と認証サーバの通信が切れてタイムアウト状態となる時間を指定します。初期値は 30（秒）です。
MaxReq (1-10)	認証セッションがタイムアウトになるまでに EAP リクエストをクライアントに送信する最大の回数を指定します。初期値は 2 です。
TxPeriod (1-65535)	PAE を管理する Authenticator の TxPeriod の値を指定します。EAP Request/Identity パケットがクライアントに送信される間隔を決定します。初期値は 30（秒）です。
ReAuthPeriod (1-65535)	定期的クライアントの再認証の間隔を 0 以外で指定します。初期値は 3600（秒）です。
ReAuthentication	規則的に再認証を行うかを指定します。初期値は「Disabled」（無効）です。
Port Control	ポートの認証状態を指定します。 • ForceAuthorized - 802.1X を無効にします。この場合、ポートが認証状態になるのに、どのような認証の交換も必要ありません。つまり、ポートは 802.1X ベースの認証無しのトラフィックを送受信します。 • ForceUnauthorized - ポートは常に認証されていない状態になり、クライアントからの認証要求を無視します。スイッチはクライアントに対して認証サービスを提供しません。 • Auto - 802.1X を有効にし、ポートはまず、認証されていない EAPOL フレームだけを送受信できる状態になります。リンク状態が接続、切断と変化したり、EAPOL-start フレームを受け取ると認証プロセスが始まります。スイッチはクライアントの識別を要求し、クライアントと認証サーバ間の認証メッセージの中継を開始します。（初期値）
Capability	802.1X Authenticator 設定が各ポートに適用されます。 • Authenticator - ポートに設定を適用します。設定が有効な場合、ネットワークアクセスするためには認証を通過する必要があります。 • None - ポートへの 802.1X 機能は無効になります。
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 - ポートが受信送信する両方向のトラフィックについて処理します。
Forward EAPOL PDU On Port	スイッチのポートベースごとの EAPOL PDU 要求の再送を有効、または無効にします。
Max User On Port (1-448)	802.1X 認証対象ユーザの最大数を指定します。No Limit にチェックした場合は、最大エントリ値に設定されます。

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。

802.1X User Settings（802.1X ユーザ設定）

新しい 802.1X ユーザを作成します。

Security > 802.1X > 802.1X User Settings の順にクリックし、以下の画面を表示します。

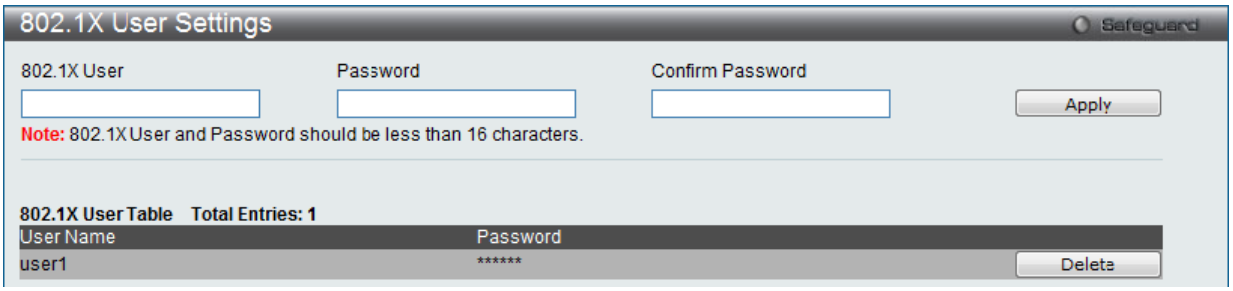


図 12-11 802.1X User Settings 画面

「802.1X User」（ユーザ名）、「Password」（パスワード）および「Confirm Password」（確認用パスワード）を入力します。ローカルユーザの設定が完了すると、同じ画面に 802.1X User Table 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。

注意 802.1X ユーザ名およびパスワードは 16 文字以内である必要があります。

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、802.1X ゲスト 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。

802.1X ゲスト 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ています。

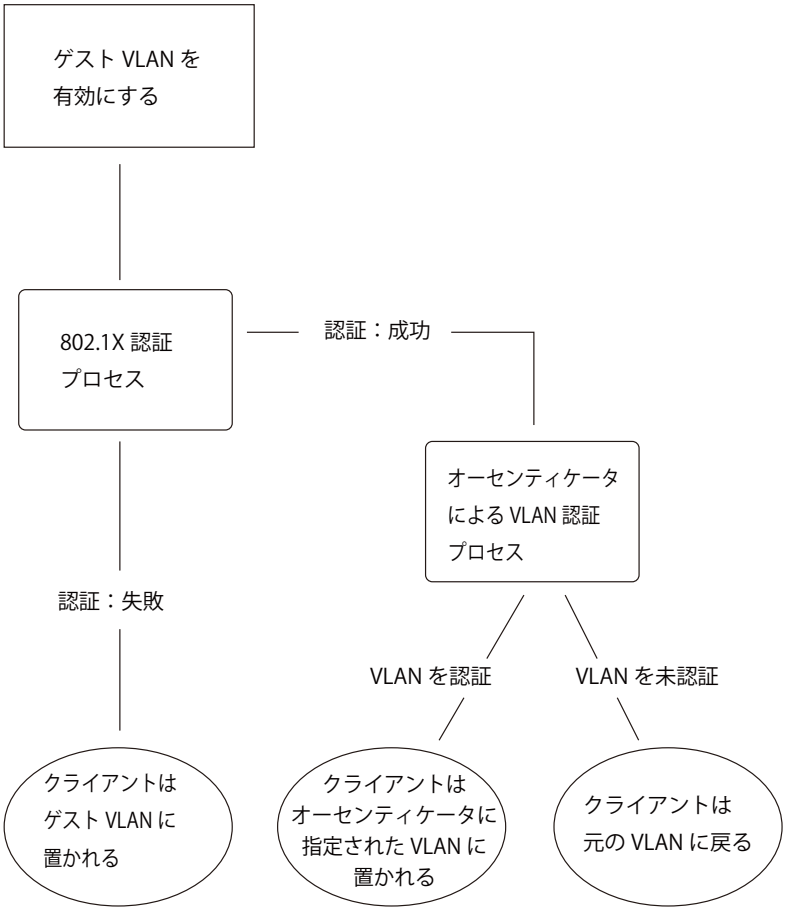


図 12-12　ゲスト VLAN 認証プロセス画面

ゲスト VLAN を使用する場合の制限事項

1. ゲスト VLAN はポートベースの VLAN にのみ対応しています。MAC ベースの VLAN では、本プロセスは行われません。
2. ゲスト VLAN をサポートしているポートは、GVRP を有効にすることはできません。同様に GVRP が有効な場合、ゲスト VLAN は使用できません。
3. ポートは同時にゲスト VLAN とスタティック VLAN のメンバになることはできません。
4. 一旦クライアントがターゲット VLAN に許可されると、ゲスト VLAN にアクセスすることはできません。
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 802.1X 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 Settings の順にクリックし、以下の設定画面を表示します。

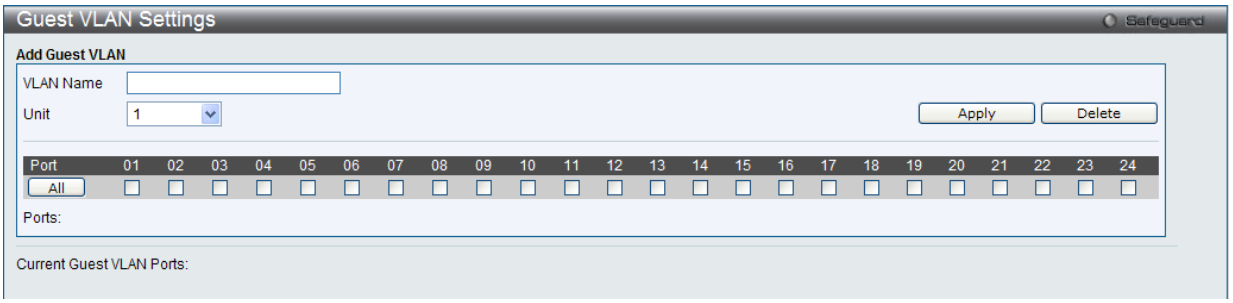


図 12-13　Guest VLAN 画面

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	802.1X ゲスト VLAN にする定義済みの VLAN 名を入力します。
Unit	設定するユニットを選択します。
Port	802.1X ゲスト VLAN を有効にするポートを設定します。「All」をクリックすると、すべてのポートを有効とします。

「Apply」ボタンをクリックし、入力したゲスト 802.1X 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。

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。

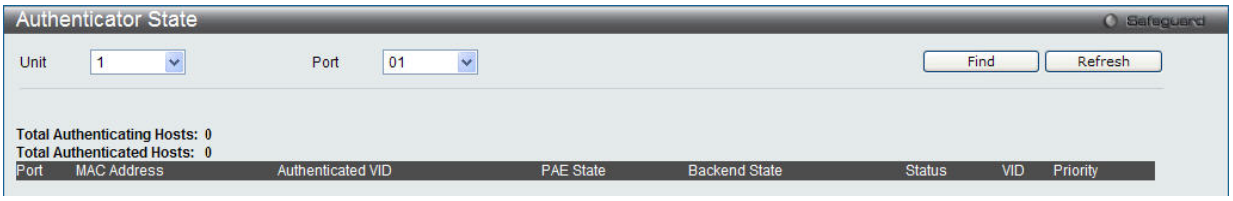


図 12-14　Authenticator State 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

注意 ユーザは最初にポートを初期化する前に 802.1X グローバル設定画面において、認証モードをグローバルに有効化する必要があります。この画面での情報はポートベースまたは MAC ベースのどちらかの認証モードを有効化する前に参照することはできません。

Authenticator Statistics（オーセンティケータ統計情報）

オーセンティケータの統計情報を表示します。「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。

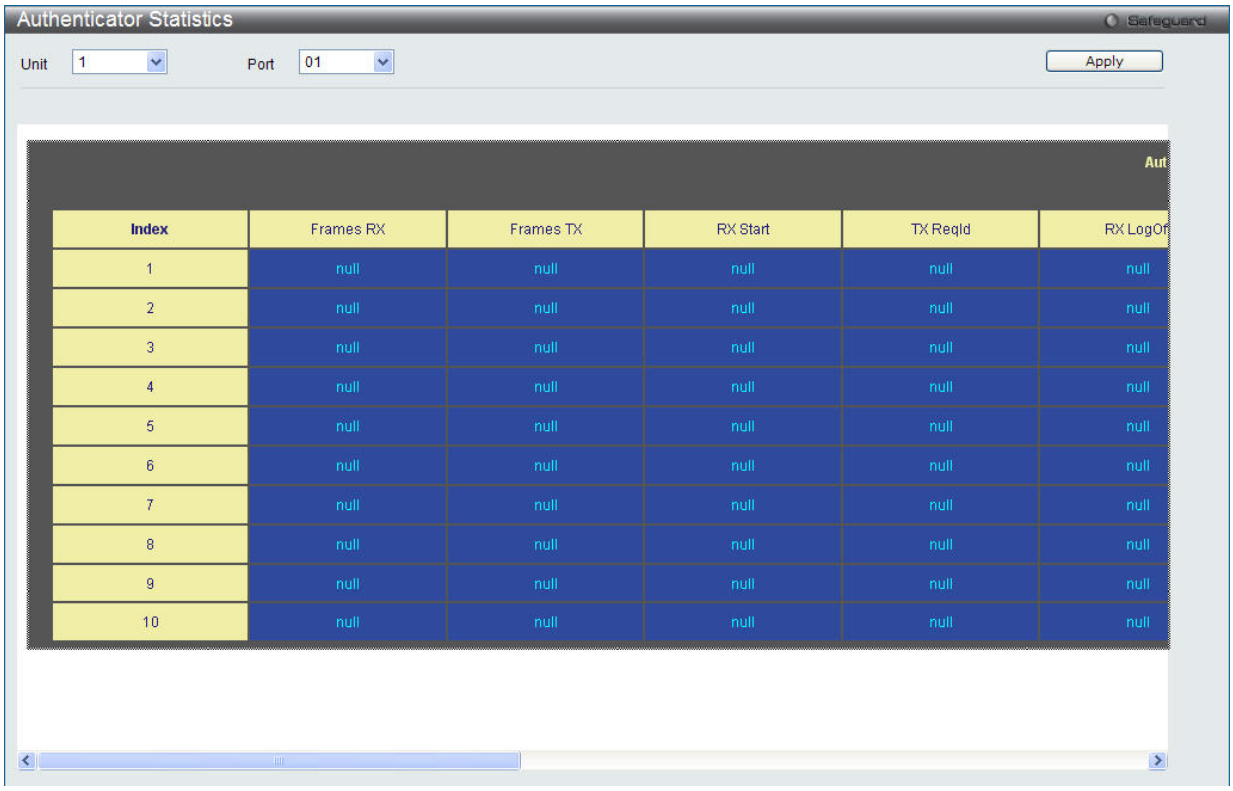


図 12-15　Authenticator Statics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
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。

注意　ユーザは最初にポートを初期化する前に 802.1X グローバル設定画面において、認証モードをグローバルに有効化する必要があります。この画面での情報はポートベースまたは MAC ベースのどちらかの認証モードを有効化する前に参照することはできません。

Authenticator Session Statistics（オーセンティケータセッション統計情報）

オーセンティケータセッションの統計情報を表示します。「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。

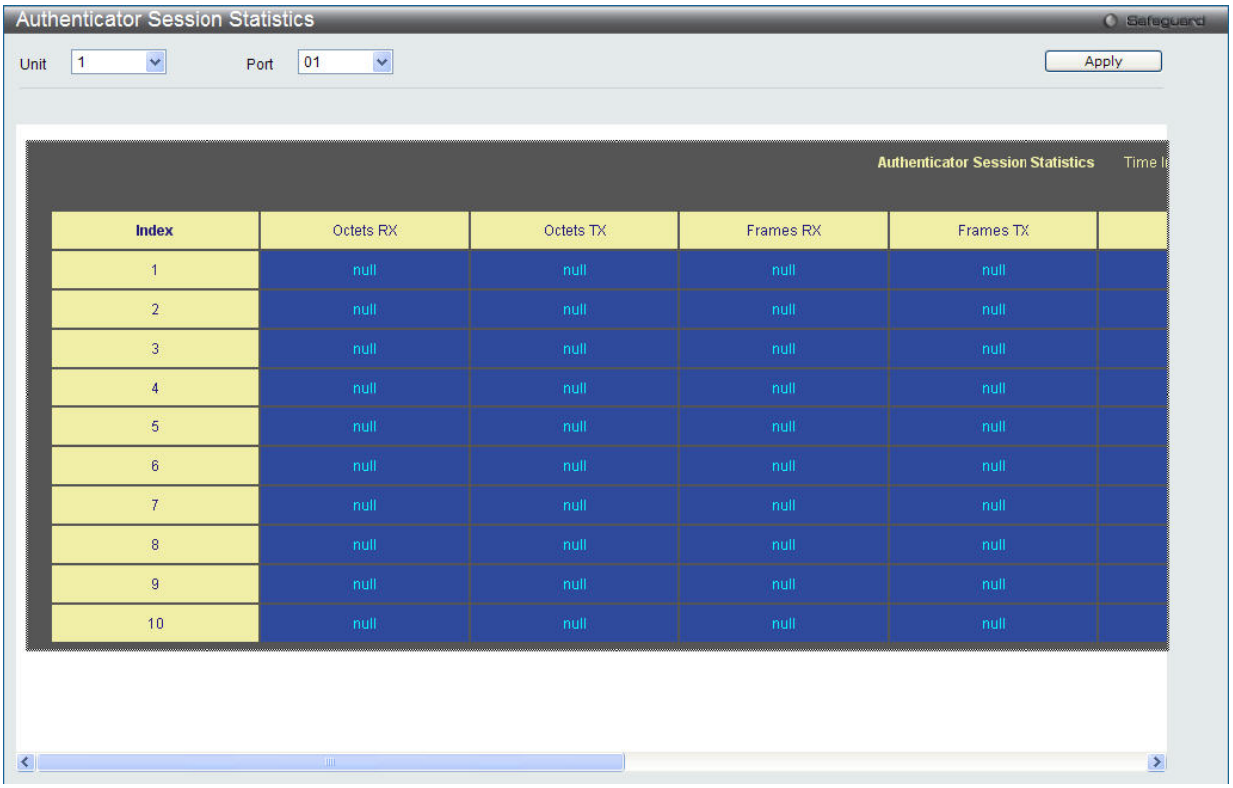


図 12-16　Authenticator Session Statistics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
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。
Time Interval	プルダウンメニューを使用して統計情報を更新する間隔を選択します。

「Apply」ボタンをクリックして行った変更を適用します。

注意　ユーザは最初にポートを初期化する前に 802.1X グローバル設定画面において、認証モードをグローバルに有効化する必要があります。この画面での情報はポートベースまたは MAC ベースのどちらかの認証モードを有効化する前に参照することはできません。

Authenticator Diagnostics（オーセンティケータ診断）

オーセンティケータ診断情報を表示します。「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。

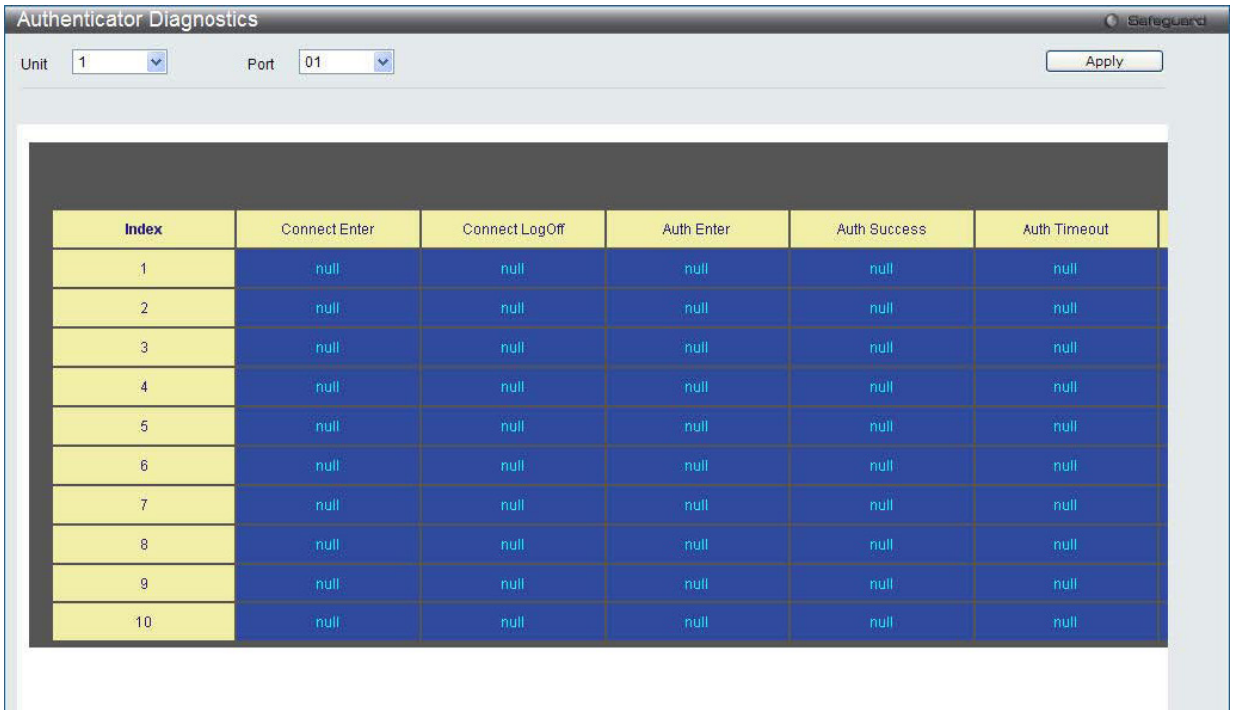


図 12-17　Authenticator Diagnostics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
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。
Time Interval	プルダウンメニューを使用して統計情報を更新する間隔を選択します。

「Apply」ボタンをクリックして行った変更を適用します。

注意　ユーザは最初にポートを初期化する前に 802.1X グローバル設定画面において、認証モードをグローバルに有効化する必要があります。この画面での情報はポートベースまたは MAC ベースのどちらかの認証モードを有効化する前に参照することはできません。

Initialize Port-based Port(s)（初期化ポート - ポートベース）

現在の初期化されているポート（ポートベース）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-based 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 :

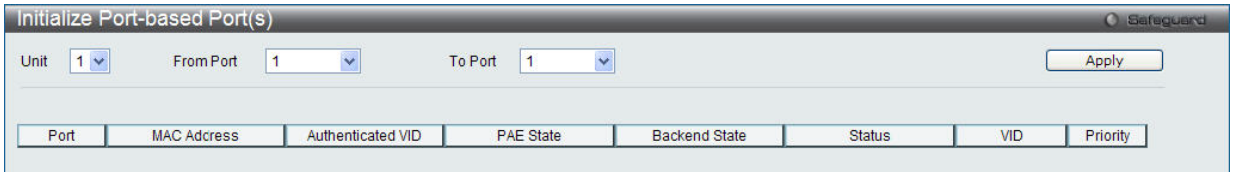


図 12-18　Initialize Port-based Port(s) 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
From Port / To 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。

注意　ユーザは最初にポートを初期化する前に 802.1X グローバル設定画面において、認証モードをグローバルに有効化する必要があります。この画面での情報はポートベースまたは MAC ベースのどちらかの認証モードを有効化する前に参照することはできません。

Reauthenticate Host-based Port(s)（再認証ポート - ホストベース）

現在の再認証ポート（ホストベース）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 > Reauthenticate Host-based 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 12-19 Reauthenticate Host-based Port(s)

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
From Port / To 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。
MAC Address	チェックを行い、MAC アドレスを入力します。

「Apply」ボタンをクリックして行った変更を適用します。

注意 ユーザは最初にポートを初期化する前に 802.1X グローバル設定画面において、認証モードをグローバルに有効化する必要があります。この画面での情報はポートベースまたは MAC ベースのどちらかの認証モードを有効化する前に参照することはできません。

RADIUS（RADIUS 設定）

Authentication RADIUS Server（認証 RADIUS サーバの設定）

RADIUS サーバによって集約したユーザ管理や Sniffing やハッカーからの保護が可能になります。

Security > RADIUS > Authentication RADIUS Server Settings をクリックし、以下の画面を表示します。

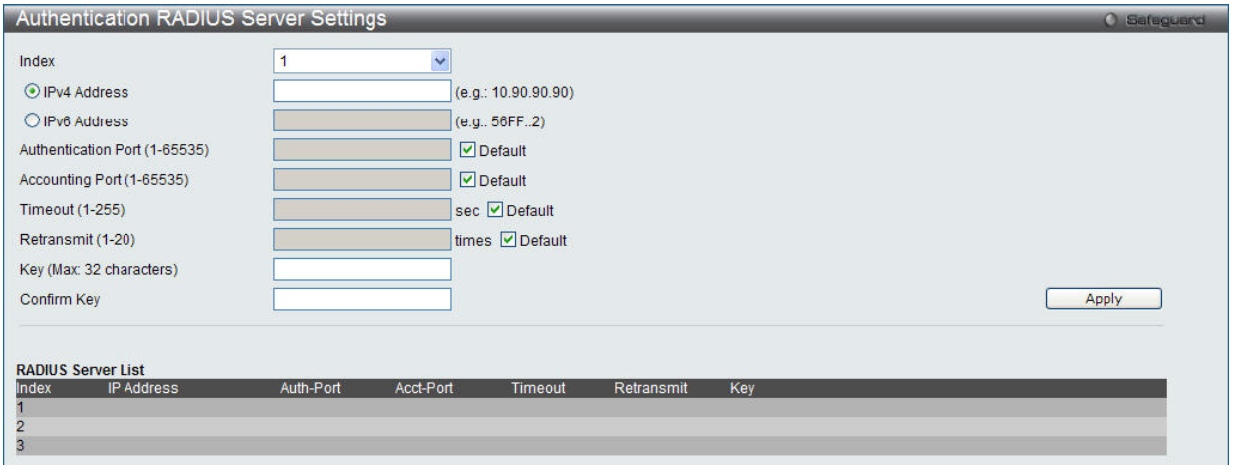


図 12-20 Authentication RADIUS Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Index	設定する RADIUS サーバを指定します。: 1、2 または 3
Server IP Address	RADIUS サーバの IP アドレスを入力します。
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)	RADIUS 認証サーバの UDP ポートです。初期値は 1812 です。
Accounting Port (1-65535)	RADIUS アカウントサーバの UDP ポートです。初期値は 1813 です。
Timeout (1-255)	RADIUS サーバのタイムアウト時間（秒）を設定します。初期値は 5（秒）です。
Retransmit (1-20)	RADIUS サーバの再転送間隔（秒）を設定します。初期値は 2（秒）です。
Key	RADIUS サーバに設定したものと同一の鍵を指定します。32 文字以内で指定します。
Confirm Key	鍵が RADIUS サーバと同一であるか確認します。

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。

RADIUS Accounting Settings（RADIUS アカウンティング設定）

スイッチのアカウンティング機能は、リモート RADIUS サーバを使用して、スイッチに発生しているイベントに関する情報を集めます。
指定した RADIUS アカウンティングサービスの状態を設定します。

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

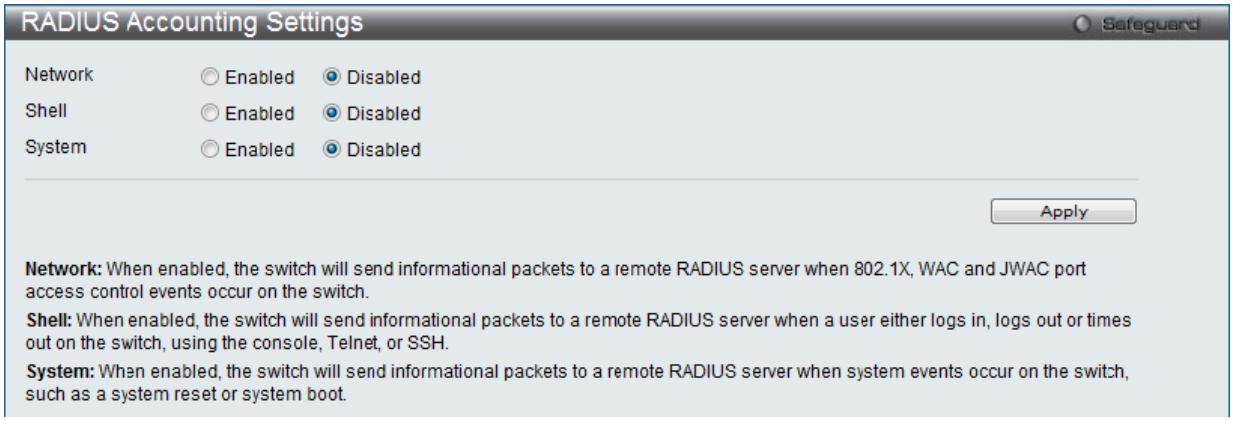


図 12-21　RADIUS Accounting Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
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。

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。

RADIUS Authentication（RADIUS 認証）

このテーブルでは、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。表の 1 列にはクライアントが秘密鍵を共有する 1 台の RADIUS 認証サーバが対応しています。

Security > RADIUS > RADIUS Authentication をクリックし、以下の画面を表示します。

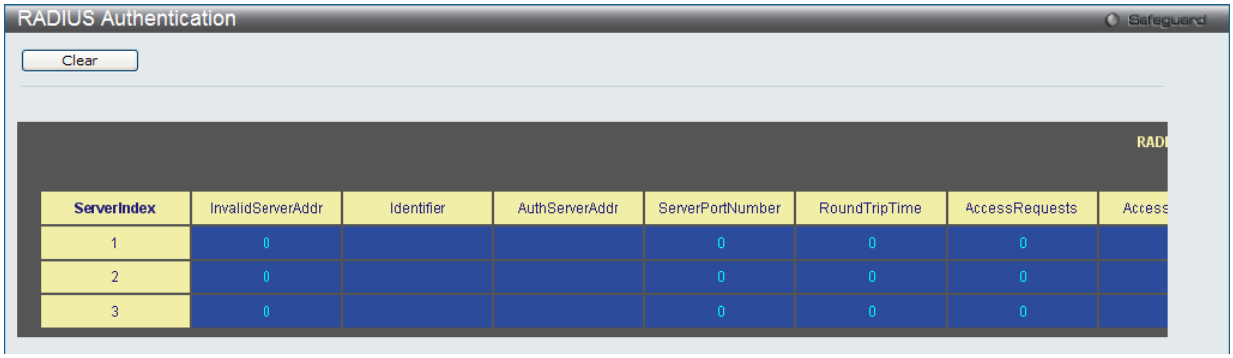


図 12-22　RADIUS Authentication 画面

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。以下の情報が表示されます。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。

項目	説明
InvalidServerAddr	不明なアドレスから受信した RADIUS Access-Response パケット数。
Identifier	RADIUS 認証クライアントの NAS 識別子。（MIB II の sysName と同じである必要はありません。）
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。
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）。

項目	説明
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。クライアントが暗号鍵を共有している RADIUS 認証サーバごとに列があります。

Security > RADIUS > RADIUS Account Client をクリックし、以下の画面を表示します。

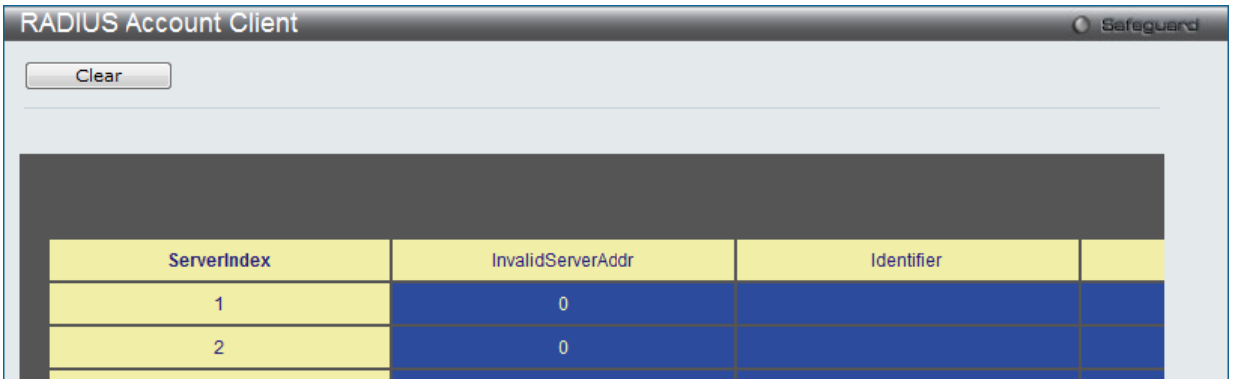


図 12-23　RADIUS Account Client 画面

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。）
ServerAddr	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、もしく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（IP-MAC- ポートバインディング）（EI モードのみ）

IP ネットワークレイヤ（IP レベル）では 4 バイトのアドレスを使用し、イーサネットリンクレイヤ（データリンクレベル）では 6 バイトの MAC アドレスを使用します。これらの 2 つのアドレスタイプを結合させることにより、レイヤ間のデータ転送を可能にします。IP-MAC 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ユーザ数を制限することです。IP アドレスと 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い、認証クライアントのみがスイッチのポートアクセスできるようにします。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。IP-MAC バインディングのエントリ数はチップの能力（例えば ARP テーブルサイズ）およびデバイスのストレージサイズによって異なります。本スイッチにおける IP-MAC バインディングの最大エントリ数は 510 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）

この画面は、スイッチの ACL モード、トラップログステータスおよび DHCP スヌープ状態を有効または無効にするのに使用します。IP-MAC バインディングの「ACL Mode」を有効にすると、スイッチに 2 つのアクセスプロファイルエントリを作成します。「Trap/Log」フィールドでは、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。

Security > IP-MAC-Port Binding (IMPB) > IMPB Global Settings の順にクリックして、以下の画面を表示します。

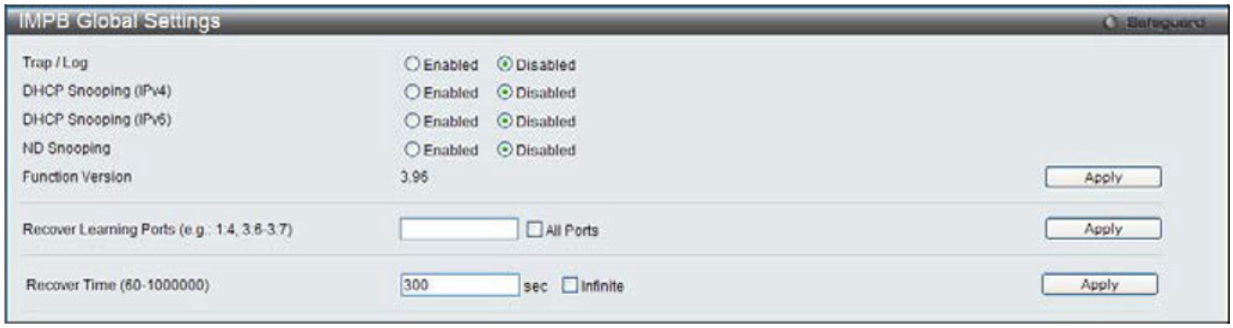


図 12-24 IMPB Global Settings 画面

本画面には以下の項目があります。

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の送信を「Enable」（有効）/「Disable」（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「Disable」（無効）です。
DHCP Snooping (IPv4)	プルダウンメニューから IP-MAC バインディングの DHCP スヌープ状態 (IPv4) を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disable」（無効）です。
DHCP Snooping (IPv4)	プルダウンメニューから IP-MAC バインディングの DHCP スヌープ状態 (IPv6) を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disable」（無効）です。
ND Snooping	ND スヌーピングを「Enable」（有効）/「Disable」（無効）にします。初期値は「Disable」（無効）です。
Recover Learning Ports	本機能を有効にするポートまたはポート範囲を指定します。「All」をチェックすると、すべてのポートで本機能を有効にします。「Apply」ボタンをクリックし、設定内容を適用してください。
Recover Time (60-1000000)	自動リカバリメカニズムを使用した間隔秒数を入力します。

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。

IMPB Port Settings（IMPB ポート設定）

「From Port」と「To Port」欄でポートまたはポート範囲を指定します。「State」、「Allow Zero IP」、および「Forward DHCP」欄を「Enabled」（有効）または「Disabled」（無効）にして、ポートのマックスエントリを設定します。

Security > IP-MAC-Port Binding (IMPB) > IMPB Port Settings の順にクリックして、以下の画面を表示します。

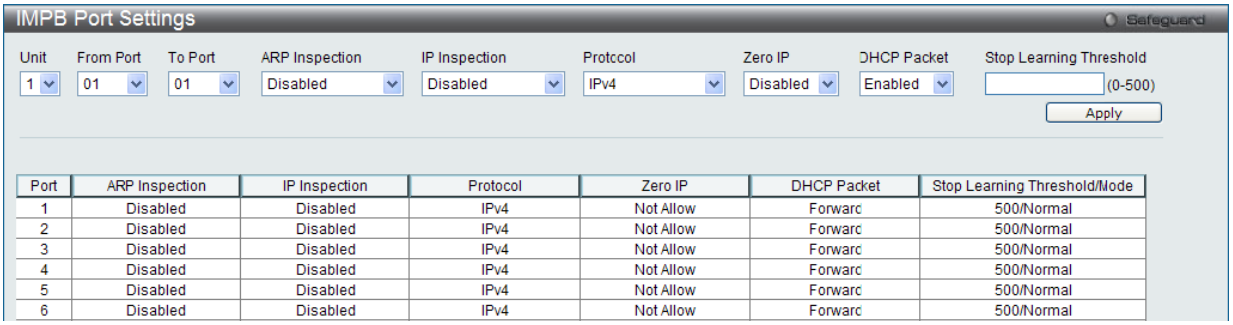


図 12-25　IMPB Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	IP-MAC バインディングを設定する対象のポートを指定します。
ARP Inspection	ARP 検知機能を「Enabled（Strict）」、「Enabled（Loose）」（有効）または「Disabled」（無効）から選択します。有効の場合正規の ARP パケットは転送され不正な ARP パケットは破棄されます。 • Disabled - ARP 検知機能は無効です。 • Enabled(Strict) - MAC アドレスによるハードウェアの記録を無効にします。正式な ARP または IP パケットが検出されるまで、全てのパケットは破棄されます。スイッチはポートの破棄された FDB エントリへの書き込みを停止します。正規のパケットを検出した場合、スイッチは転送 FDB エントリを書き込みます。 • Enabled(Loose) - 不正な ARP パケットが検出されるまで全てのパケットは転送されます。
IP Inspection	ARP/IP 検知が両方とも有効の場合、すべての IP パケットが検査されます。不正な IP パケットが破棄され、正規の IP パケットは転送されます。本機能が有効で ARP 検知が無効の場合、全ての非 -IP パケット（例えば、L2 パケット、または ARP パケット）は転送されます。初期値は無効です。
Protocol	プロトコルを選択します。「IPv4」「IPv6」「All」から選択します。
Zero IP	プルダウンメニューを使用して、この機能を「Enable」（有効）/「Disable」（無効）にします。「Zero IP」を設定すると、ステートが 0.0.0.0 送信元 IP の ARP パケットを許容します。
DHCP Packet	初期設定では、ブロードキャスト DA の DHCP パケットをフラッドします。無効にすると、ブロードキャスト DHCP パケットは特定のポートによって受信され、フォワードされません。この設定は、CPU でトラップした DHCP パケットがソフトウェアでフォワードされる必要があり、DHCP スヌーピングが有効に設定されている場合に効果的です。この設定はこの状況におけるフォワーディング実行をコントロールします。
Mode	設定する IP-MAC バインディング設定モードを以下から選びます。 • ARP - ARP モードに設定されます。アクセスエントリは追加されません。システムが ARP モードに設定された場合、「both ARP mode」「ACL mode」も有効になります。 • ACL -「ACL」モードとして設定されます。「ACL 」モードを有効にした場合、アクセスエントリとして追加されます。
Stop Learning Threshold	ストップラーニングのしきい値を 0-500 の間で設定します。各ポートの初期値は 500 です。

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

IMPB Entry Settings（IMPB エントリ設定）

本テーブルは、スイッチにスタティック IP MAC バインディングポートエントリを作成します。

Security > IP-MAC-Port Binding (IMPB) > IMPB Entry Settings の順にクリックして画面を表示します。

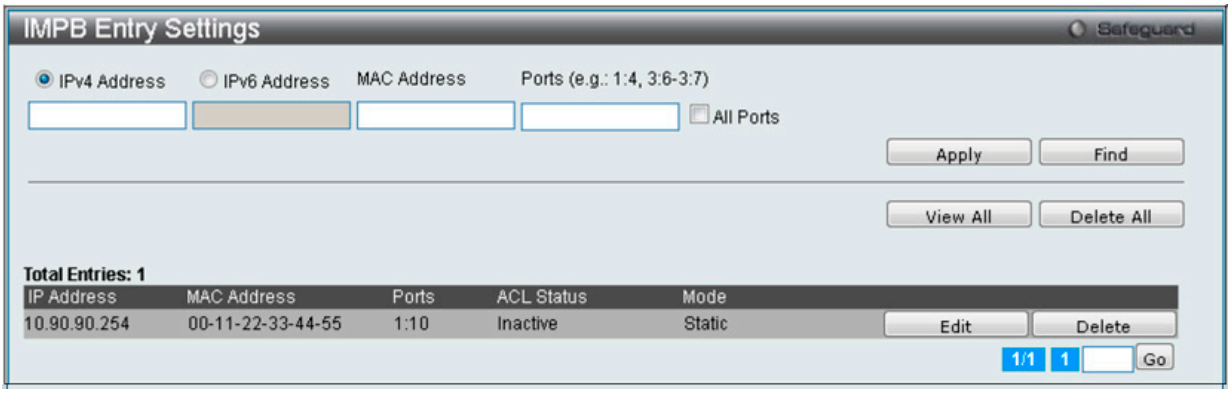


図 12-26 IMPB Entry Settings 画面

本画面には以下の項目があります。

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 バインディングエントリ（IP アドレス +MAC アドレス）を設定する対象のポートを指定します。本チェックボックスを選択すると、本 IP-MAC バインディングエントリ（IP アドレス +MAC アドレス）をスイッチのすべてのポートに設定します。「All Ports」をチェックすると、すべてのポートを指定します。

エントリの追加

1. 「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。

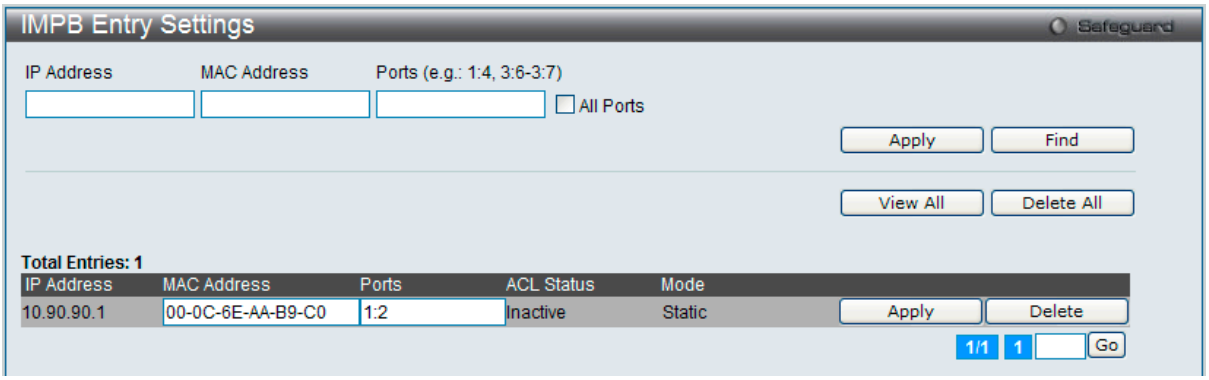


図 12-27 IMPB Entry Settings 画面 - Edit

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

「Find」をクリックするとエントリを検索します。

すべてのエントリの表示

「View All」をクリックするとすべてのエントリを表示します。

すべてのエントリの削除

「Delete All」をクリックするとすべてのエントリを削除します。

MAC Block List（MAC ブロックリスト）

本テーブルは、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の表示に使用します。

Security > IP-MAC-Port Binding (IMPB) > MAC Block List の順にクリックして、以下の画面を表示します。

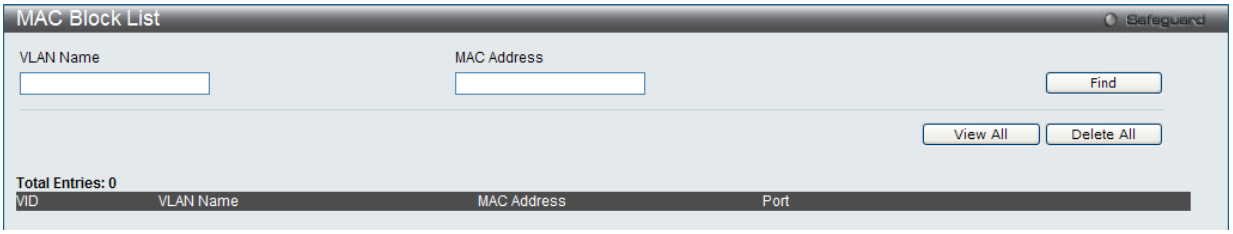


図 12-28　MAC Blocked List 画面

ブロックされた未承認のデバイスの検索

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検索するには、「VLAN Name」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

エントリポートの横の「Delete」ボタンをクリックします。リスト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。

DHCP Snooping（DHCP スヌーピング）

DHCP Snooping Maximum Entry Settings（DHCP スヌーピング最大エントリ）

本テーブルは、特定ポート上の最大 DHCP エントリの設定に使用します。

Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Maximum Entry Settings の順にクリックして、以下の画面を表示します。

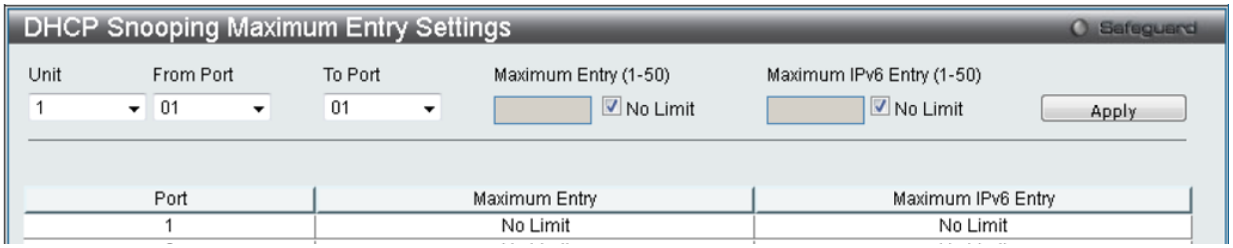


図 12-29　DHCP Snooping Max Entry Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	プルダウンメニューを使用してポート範囲を指定します。
Maximum Entry (1-50)	IPv4 DHCP Snooping の最大エントリ入力値を指定します。「No Limit」にチェックすると最大エントリ値に設定されます。
Maximum IPv6 Entry (1-50)	IPv6 DHCP Snooping の最大エントリ入力値を指定します。「No Limit」にチェックすると最大エントリ値に設定されます。

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。

DHCP Snooping Entry（DHCP スヌーピングエントリ）

本テーブルは、特定ポート上のダイナミックエントリの表示に使用します。

Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Entry の順にクリックして、以下の画面を表示します。

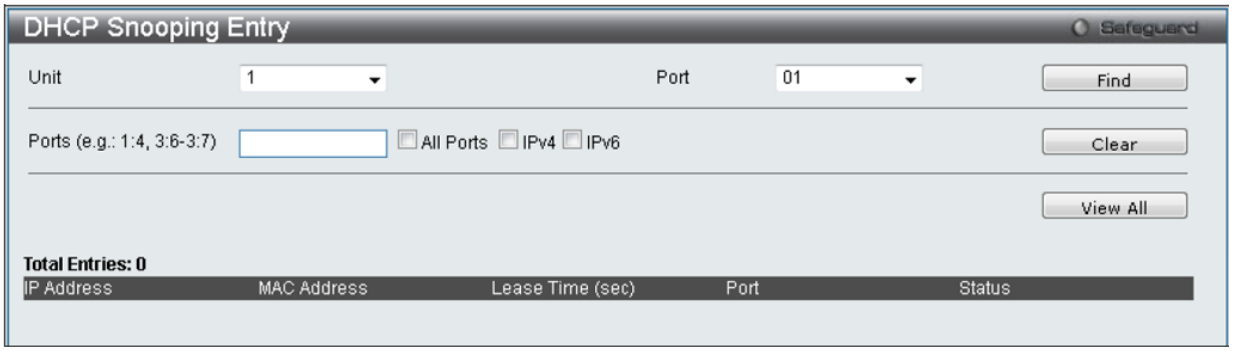


図 12-30　DHCP Snooping Entry 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
Port	プルダウンメニューを使用してポートを指定します。
Ports	DHCP スヌーピングエントリを表示するポートを指定します。「All Ports」をチェックすると全てのエントリを表示します。 IPv4 DHCP スヌーピングエントリを選択する場合は「IPv4」をチェックし、IPv6 DHCP スヌーピングエントリを選択する場合は「IPv6」をチェックします。

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。

注意 DHCPv6/DHCPv6 スヌーピングを組み合わせて利用する際には、Windows では DHCPv6 で IP アドレスを取得しても、ステートレス IP/ テンポラリ IP を使用するため通信できませんのでご注意ください。

DHCP Snooping Limit Rate Settings（DHCP スヌーピングリミットレート設定）

本テーブルは、DHCP スヌーピングのリミットレートエントリの表示に使用します。

Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Limit Rate Settings の順にクリックして、以下の画面を表示します。

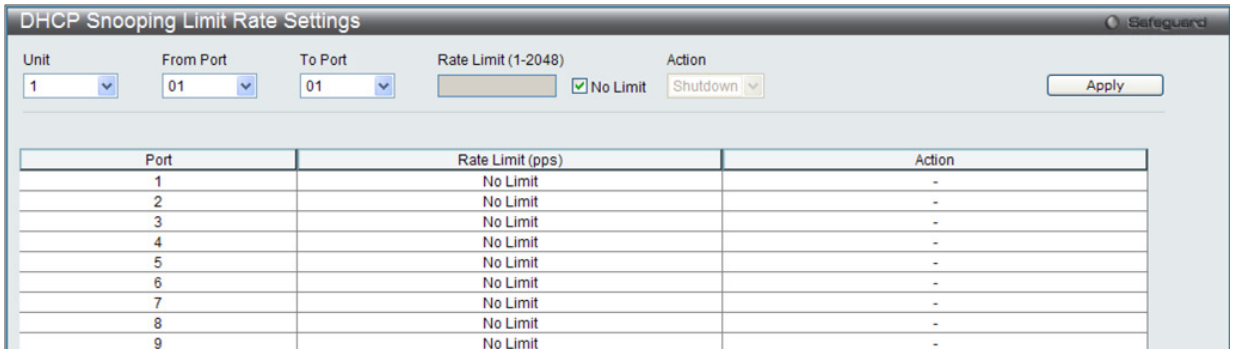


図 12-31　DHCP Snooping Limit Rate Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	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。
Rate Limit (1-2048)	毎秒インタフェースが受信できる DHCP メッセージの数を入力します。「No Limit」をチェックすると DHCP スヌーピングレートリミットを無効にします。
Action	ドロップダウンメニューを使用し「DHCP protection mode（DHCP 保護モード）」を指定します。 「Shutdown」– 攻撃状態になるとポートをシャットダウンします。 「Drop」– 攻撃状態になると全てのレートリミット DHCP パケットを破棄します。

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。

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。

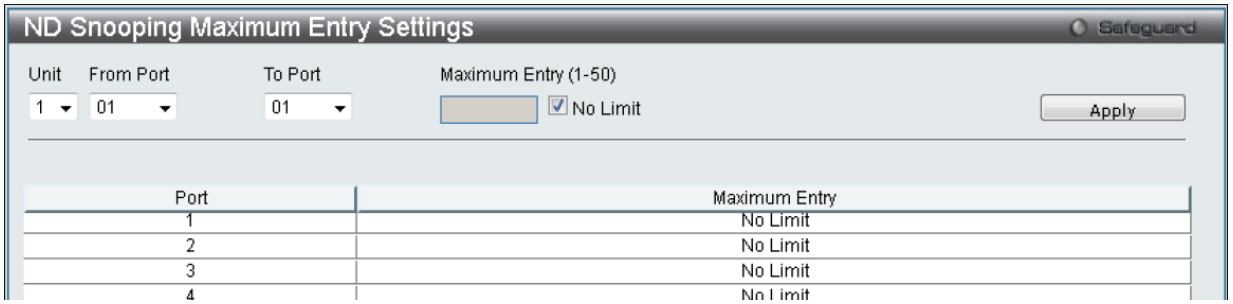


図 12-32　ND Snooping Maximum Entry Setting 画面

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
Unit	設定するユニットを選択します。
From Port / To Port	プルダウンメニューを使用して、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 にチェックした場合は、最大エントリ値に設定されます。

「Apply」ボタンをクリックして行った変更を適用します。

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。

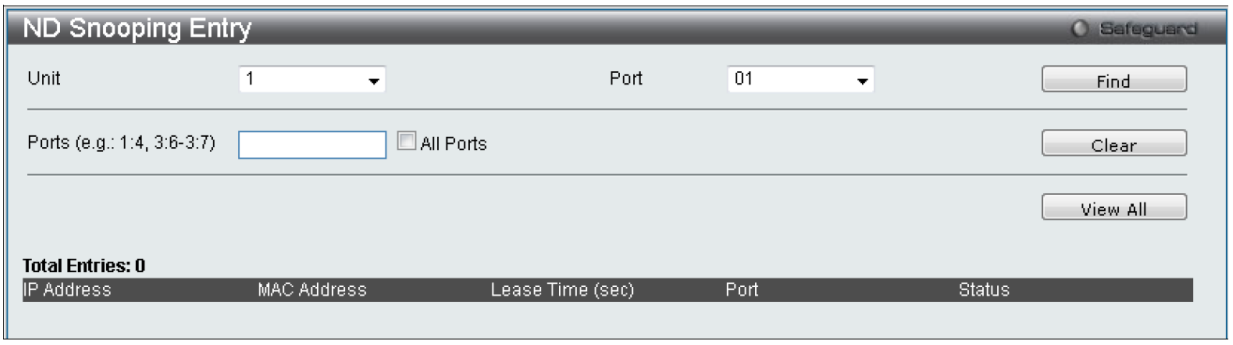


図 12-33　ND Snooping Entry 画面

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
Unit	設定するユニットを選択します。
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 Port」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 アドレス認証）

MAC アドレス認証機能は、ポートまたはホストを認証、アクセス権限を設定する方法です。ポートベースの MAC 認証はポート単位でのアクセス権を設定し、ホストベース MAC 認証は MAC 単位でのアクセス権を設定します。

MAC アドレスのユーザはネットワークへのログイン前に認証権限を付与されている必要があります。ローカル認証方式、RADIUS サーバ認証方式のどちらもサポートされています。MAC アドレス認証では MAC アドレス情報がローカルまたは RADIUS サーバに認証権限要にデータベース化されます。これらの認証方式を適用すると、ユーザは高レベルな認証によって保護されることになります。

MAC アドレス認証に関する注意

MAC アドレス認証に関するいくつかの制限と規則があります。

1. 本機能がポートに有効になると、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. ポートは、ゲスト VLAN ではない VLAN の物理ポートに対し、最大 1000 個の認証 MAC アドレスを受け入れます。既に最大数の認証済み MAC アドレスを持つポートに対して認証を試みても、他の MAC アドレスはブロックされます。

4. リンクアグリゲーション、ポートセキュリティ、または GVRP 認証が有効なポートは、MAC アドレス認証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）

以下の画面では、スイッチの MAC アドレス認証機能に設定項目を設定します。ここでは、ステータス、認証方法、RADIUS パスワードの設定、およびスイッチの MAC アドレス認証に関連するゲスト VLAN 設定を参照、および MAC アドレス認証機能の有効 / 無効を設定します。以前に記述した他の機能（MAC アドレス認証参照）で有効とされているポートは、MAC アドレス認証を使用できません。

Security > MAC-based Access Control (MAC) > MAC-based Access Control Settings の順にメニューをクリックし、以下の画面を表示します。

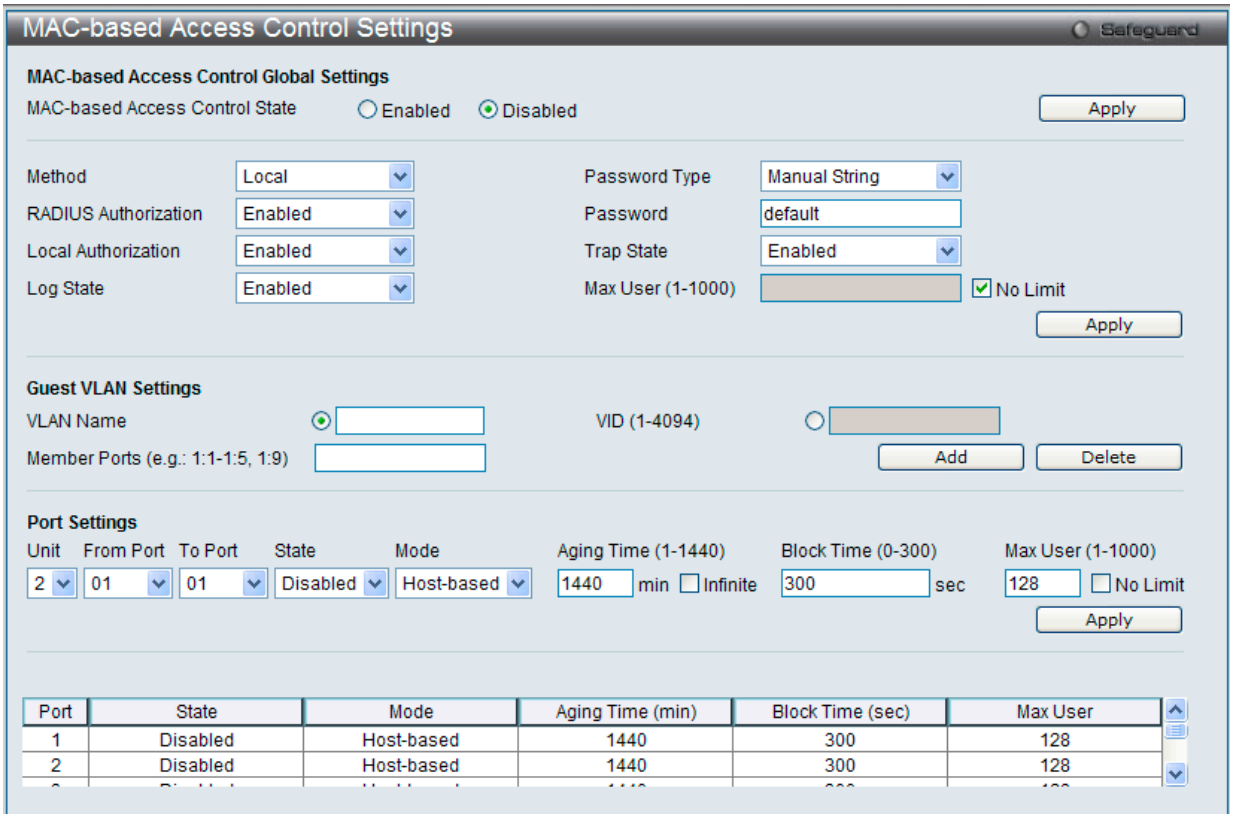


図 12-34　MAC-based Access Control Settings 画面

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	プルダウンメニューで「Enabled」（有効）または「Disabled」（無効）を選択し、スイッチの MAC アドレス認証をグローバルに設定します。初期値は「Disabled」です。
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 アドレス認証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 アドレス認証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 Type	プルダウンメニューを使用して、MAC ベースアクセスコントロール用の RADIUS 認証パスワードのタイプを選択します。 • Manual String -「Password」テキストボックス内と同じパスワードを使用します。 • Client MAC Address - パスワードとしてクライアントの MAC アドレスを使用します。
Password	認証リクエストのパケットを送信するために使用する RADIUS サーバのパスワードを入力します。初期値は「default」です。
RADIUS Authorization	本機能を「Enabled」（有効）/「Disabled」（無効）にします。有効の場合 RADUIS サーバによる権限付きデータはグローバル認証が有効の場合受け入れられます。
Local Authorization	本機能を「Enabled」（有効）/「Disabled」（無効）にします。有効の場合、ローカルデータベースによる権限を与えられた権限データは受け入れられます。
Trap State	トラップのステータスを有効 / 無効にします。
Log State	ログのステータスを有効 / 無効にします。
Max User (1-1000)	MAC ベースアクセス制御に登録されるユーザの最大数を入力します。「No Limit」にチェックすると制限はなくなります。
Guest VLAN Settings	
VLAN Name/ VID	本機能で使用する設定済みのゲスト VLAN 名 /VLAN ID を表示します。名前のハイパーリンクをクリックし、MAC ベース認証のために「Guest VLAN Configuration」画面を表示します。
Member Ports	ゲスト VLAN に設定されているポートリストを入力します。

項目	説明
Port Settings	
Unit	設定するユニットを指定します。
From Port/To Port	MAC アドレス認証に設定されるポート範囲を入力します。
State	プルダウンメニューで各ポートの MAC ベースアクセスコントロール機能を「Enabled」（有効）または「Disabled」（無効）に設定します。
Mode	「Host Based」または「Port Based」から選択します。「Host Based」を選択した場合、各ユーザはそれぞれの認証結果を保有することができます。「Port Based」を選択した場合、ポートに接続している全てのユーザは最初の認証結果を共有します。
Aging Time (1-1440)	認証ホストが認証を有効にする期間を設定します。設定した期間が過ぎた後はホストは非認証に戻ります。初期値は 1440 です。「Infinite」に設定するとホストが非認証に戻ることはありません。
Block Time (0-300)	ホストが認証に失敗した場合、手動でエントリを削除しない限り、本項目で設定した時間を過ぎるまで次の認証は始まりません。
Max User (1-1000)	各ポートの認証クライアントの最大数を設定します。No Limit にチェックした場合は、最大エントリ値に設定されます。

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。

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）

以下の画面を使用し、スイッチに対して認証されるターゲット VLAN とともに 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) > MAC-based Access Control Local Settings をクリックし、以下の画面を表示します。

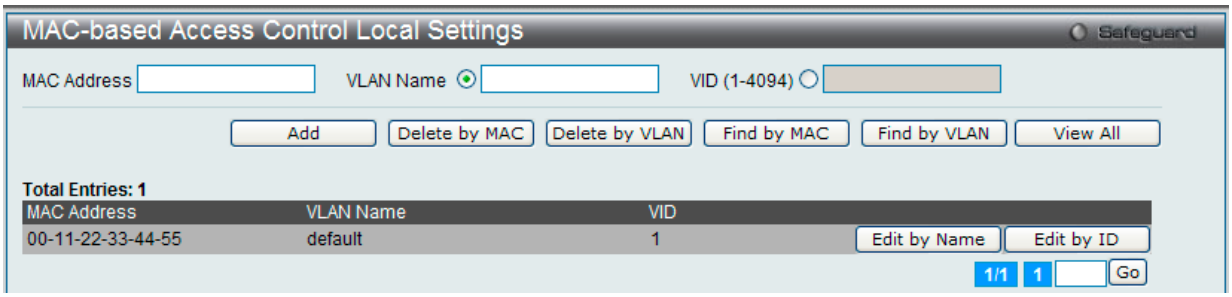


図 12-35　MAC-based Access Control Local Settings 画面

MAC アドレスを Local Authentication List に追加する

「MAC Address」と「VLAN Name」に MAC アドレスとターゲット VLAN 名をそれぞれ入力し、「Add」ボタンをクリックします。

MAC アドレスエントリを削除する

該当欄に設定項目を入力し、「Delete By MAC」ボタンをクリックします。

VLAN 名を削除する

該当欄に設定項目を入力し、「Delete By VLAN」ボタンをクリックします。

特定の MAC アドレスを検索する

はじめの欄に MAC アドレスを入力し、「Find By MAC」ボタンをクリックします。

特定の VLAN 名を検索する

2 番目の欄に VLAN 名を入力し、「Find By VLAN」ボタンをクリックします。

選択した MAC アドレスの VLAN 名を変更するには「Edit By Name」をクリックし、以下の画面を表示します。

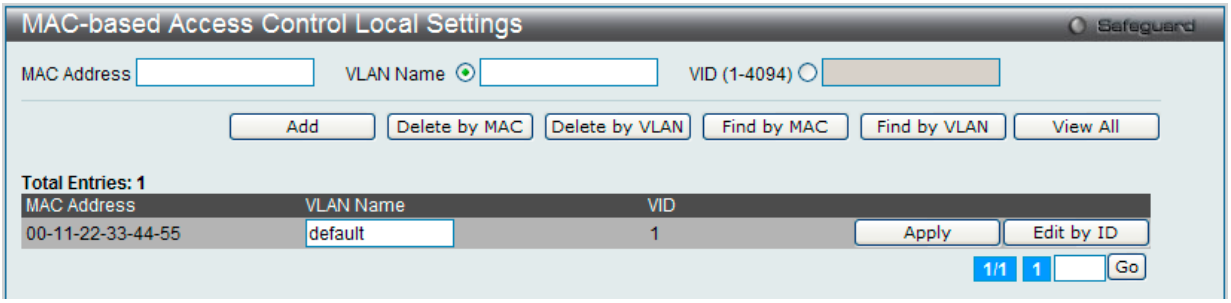


図 12-36　MAC-based Access Control Local Settings – Edit by Name 画面

選択した MAC アドレスの VLAN ID を変更するには「Edit By ID」をクリックし、以下の画面を表示します。

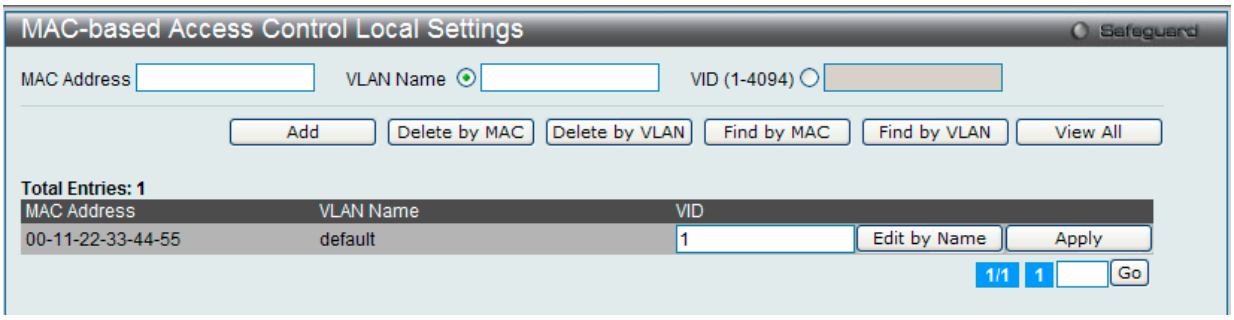


図 12-37　MAC-based Access Control Local Settings – Edit by ID 画面

MAC-based Access Control Authentication State（MAC ベースアクセスコントロール認証情報）

MAC ベースアクセスコントロールの認証状況を表示します。

Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State をクリックし、以下の画面を表示します。

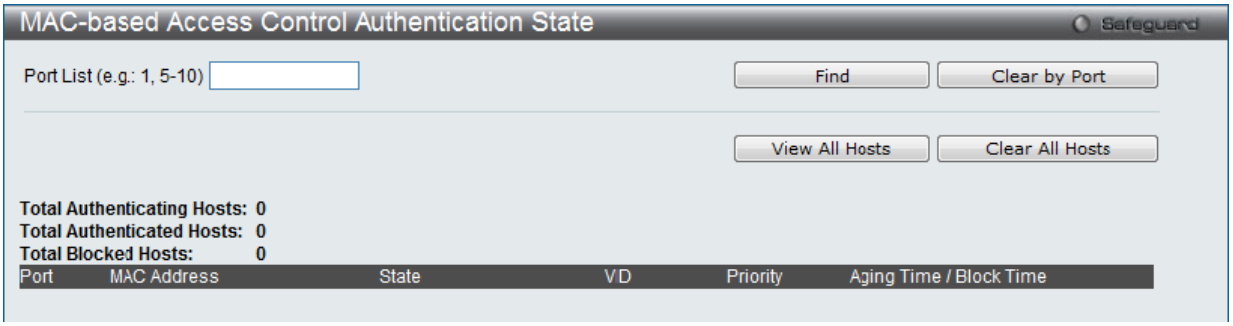


図 12-38　MAC-based Access Control Authentication State 画面

MAC ベースアクセスコントロール認証情報について表示するにはポート番号を入力して「Find」をクリックします。
「Clear by Port」ボタンをクリックして、入力したポート番号に関連する情報を消去します。「View All Hosts」ボタンをクリックして既存の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既存のホスト情報を消去します。

Web-based Access Control（Web 認証）

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、認証処理には HTTP/HTTPS 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/HTTPS 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。

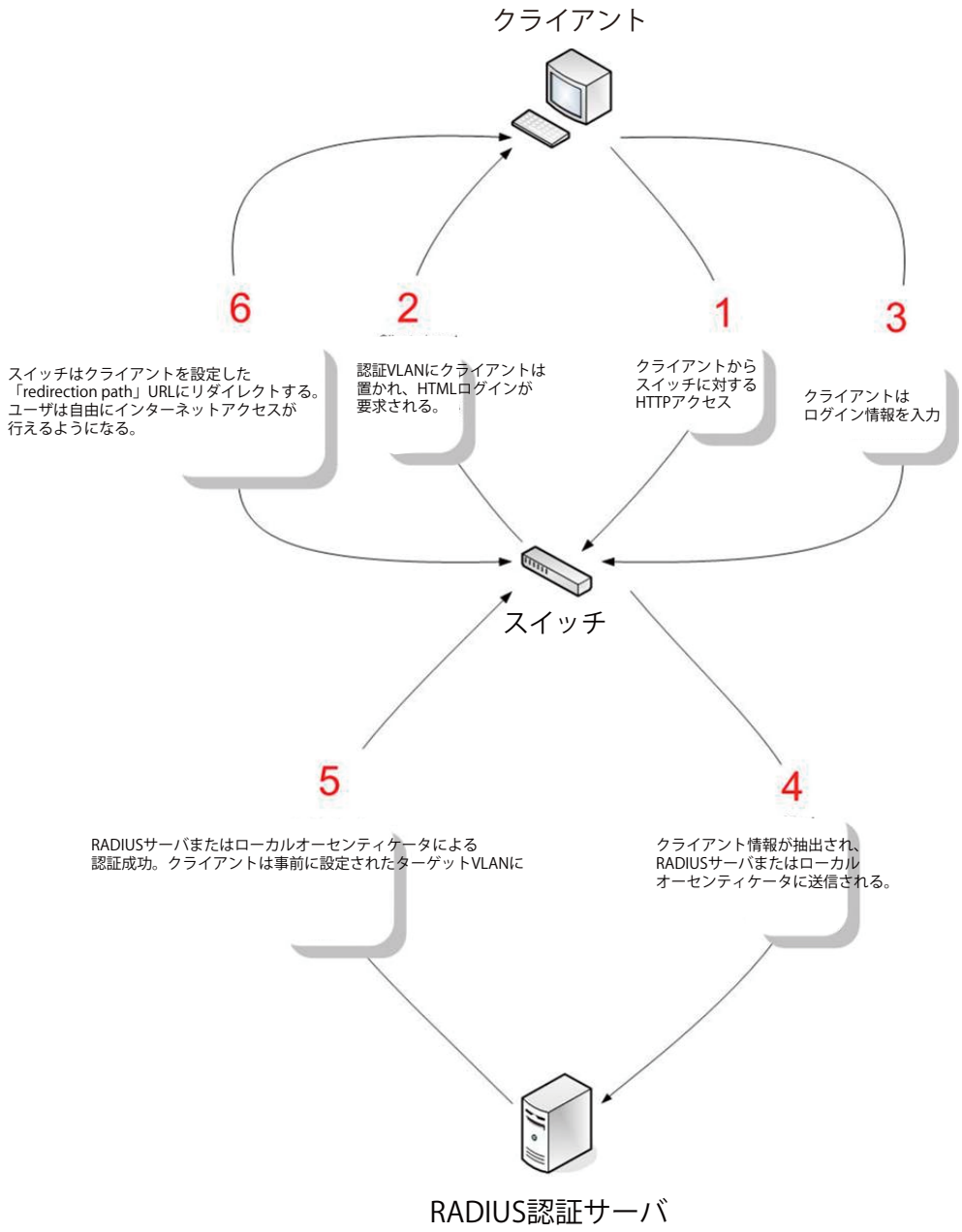
D-Link の WAC の実行には、WAC 機能が排他的に使用し、スイッチの他のモジュールに知られていない仮想 IP を使用します。実際は、スイッチの他の機能への影響を避ける場合にだけ、WAC は仮想 IP アドレスを使用してホストとの通信を行います。そのため、すべての認証要求を仮想 IP アドレスに送信し、スイッチの物理インタフェースの IP アドレスには送信しないようする必要があります。

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。

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。

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。

次の図は、Web ベースのアクセスコントロールを実現させるために、認証に関わる各ノードで行われる基本の 6 つのステップを例示しています。



条件および制限

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 を含む必要な項目を入力して RADIUS サーバの設定を行ってください。

注意 WAC 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。

注意 仮想 IP アドレスを「0.0.0.0」もしくはスイッチの IPIF（IP インタフェース）と同一のサブネットに設定した場合、WAC 機能は正常に動作しません。

WAC Global Settings（Web 認証のグローバル設定）

スイッチの Web 認証設定をグローバルに行います。

Security > Web-based Access Control (WAC) > WAC Global Settings をクリックして、以下の画面から設定します。

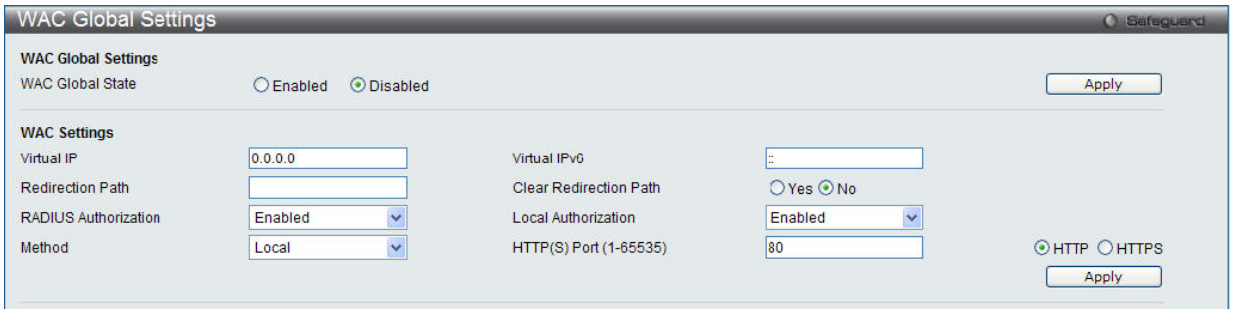


図 12-39 WAC Global Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
WAC Global Settings	
WAC Global State	Web 認証機能を「Enable」（有効）/「Disable」（無効）にします。
WAC Settings	
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。
Virtual IPv6	仮想 IPv6 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。
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。
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) > 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。
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（Web 認証ユーザ設定）

Web 認証用のユーザアカウントを登録します。

Security > Web-based Access Control (WAC) > WAC User Settings をクリックし、以下の設定用画面を表示します。

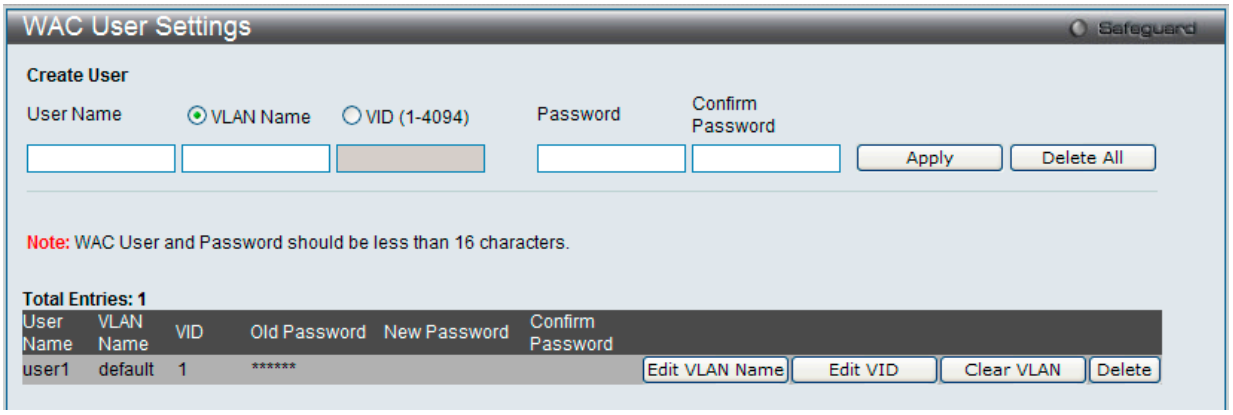


図 12-40　WAC User Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Create User	
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/VID	作成済みの VLAN から、上記ユーザが認証に成功した際に割り当てる VLAN 名 /VLAN ID を指定します。
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。
Confirm Password	上記パスワードを再度入力します。

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 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。

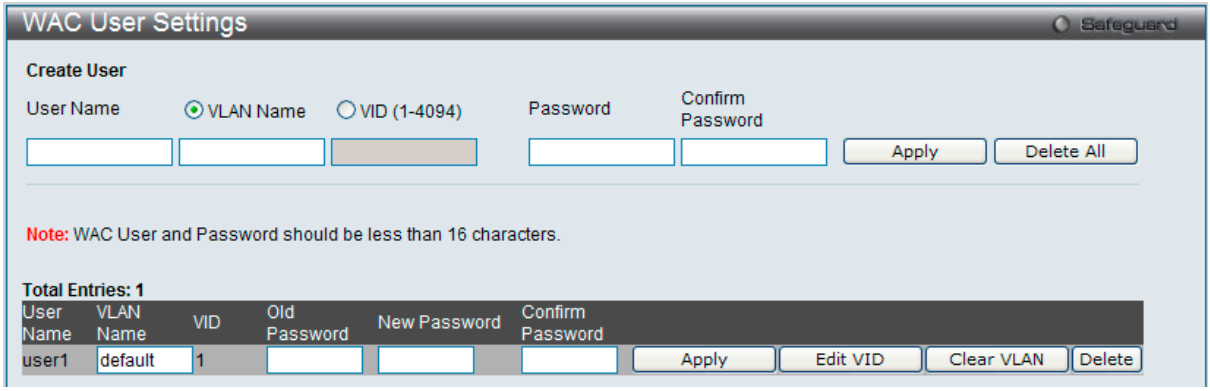


図 12-41　User Account Settings 画面 - Edit VLAN Name

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。

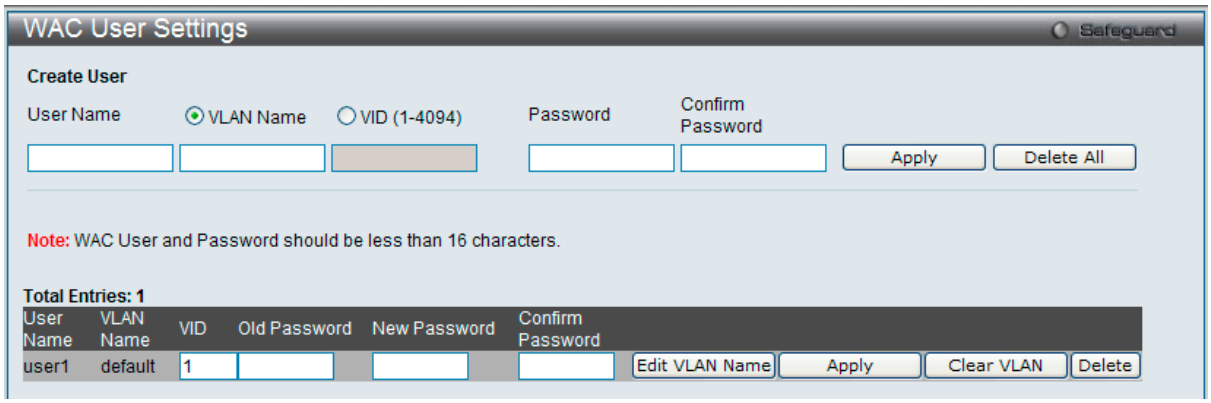


図 12-42 User Account Settings 画面 - Edit VID

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。

WAC Port Settings（Web 認証ポート設定）

Web 認証用のユーザアカウントを登録するには、**Security > Web-based Access Control (WAC) > WAC Port Settings** をクリックし、以下の設定用画面を表示します。

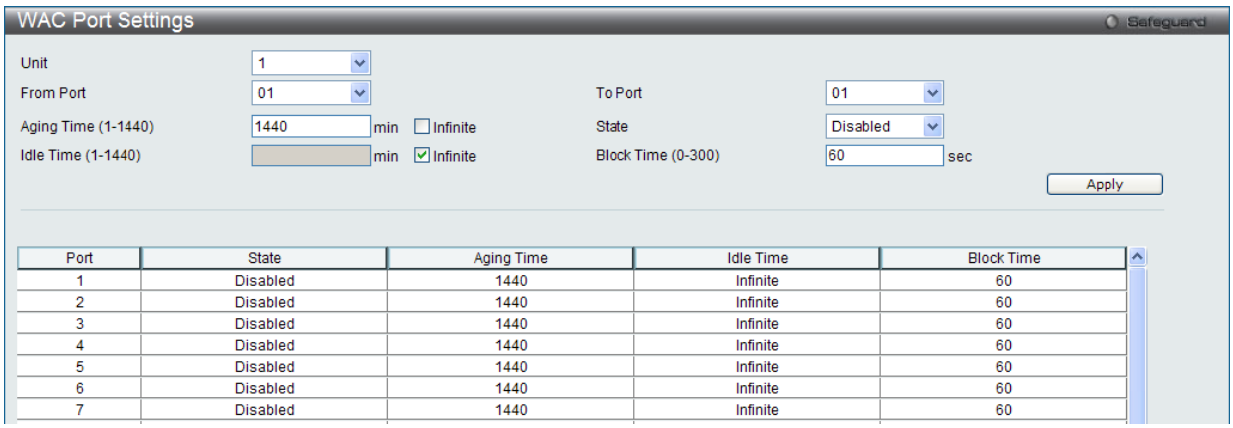


図 12-43 WAC Port Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Port 設定	
Unit	設定するユニットを選択します。
From Port / To Port	ポート範囲を設定します。
State	本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Aging Time (1-1440)	認証ホストが認証を有効にする期間（1 から 1440 分）を設定します。期間が過ぎるとホストは非認証ホストに戻ります。「Infinite」を設定すると制限はなくなります。初期値は「Infinite」です。
Idle Time (1-1440)	本パラメータは認証ホストに一定期間トラフィックがなかった場合、ホストを非認証にするための時間（1 から 1440 分）を設定します。「Infinite」に設定すると非認証には戻りません。初期値は「Infinite」です。
Block Time (1-300)	ホストが認証に失敗した場合、手動で解除しない限り次の認証までホストはブロックされます。

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。

WAC Authentication State（Web 認証情報）

本画面では WAC 認証情報について表示します。

Security > Web-based Access Control (WAC) > WAC Authentication State の順にメニューをクリックし、以下の画面を表示します。

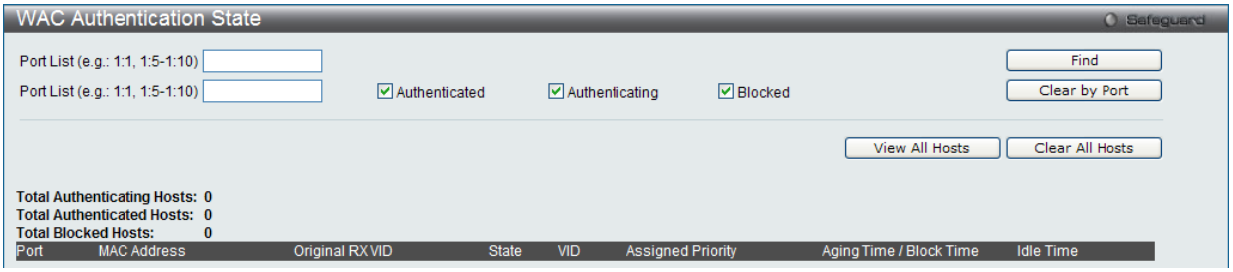


図 12-44　WAC Authentication State 画面

「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。
「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。

WAC Customize Page（WAC カスタマイズページ設定）

認証ページの項目をカスタマイズします。

Security > Web-based Access Control (WAC) > WAC 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。

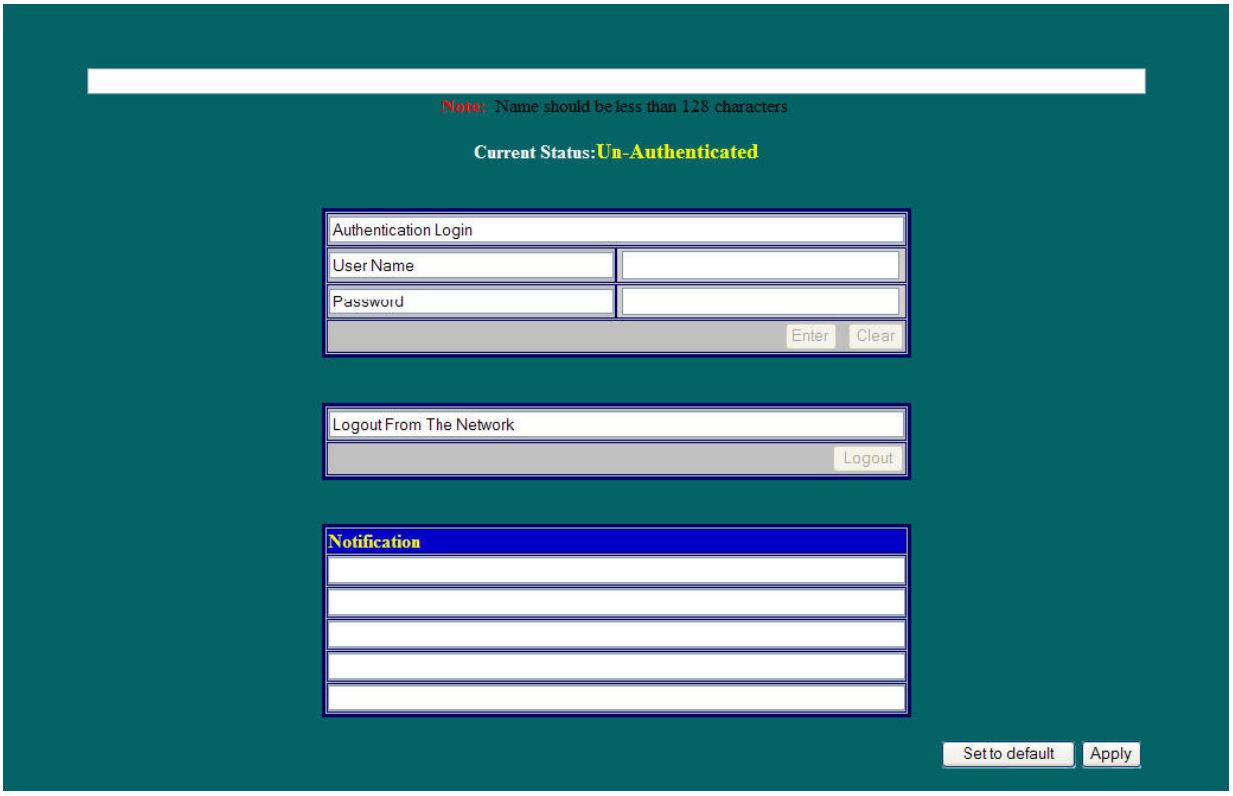


図 12-45　WAC Customize Page 画面

WAC ページの設定を行うためにはこの画面の WAC 認証情報をすべて入力して「Apply」ボタンをクリックして行った変更を適用します。
「Set to Default」ボタンをクリックして、全項目を初期設定に復元します。
「Edit」ボタンをクリックして、項目を編集します。

Japanese Web-based Access Control（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。

この画面ではスイッチ上で JWAC を有効化し、設定することができます。JWAC と WAC は相互に排他的な機能であり、同時に有効化することはできません。JWAC 機能を使って検疫を行うには、ユーザは 2 段階の認証をパスする必要があります。1 段階目は検疫サーバで認証をし、2 段階目はスイッチで認証を行うというものです。2 段階目に関しては、認証はホストが認証をパスした後 JWAC によりポート VLAN メンバーシップが変更されない場合を除いて、Web 認証に似ています。JWAC と WAC は同じ RADIUS サーバを共有することができます。

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。

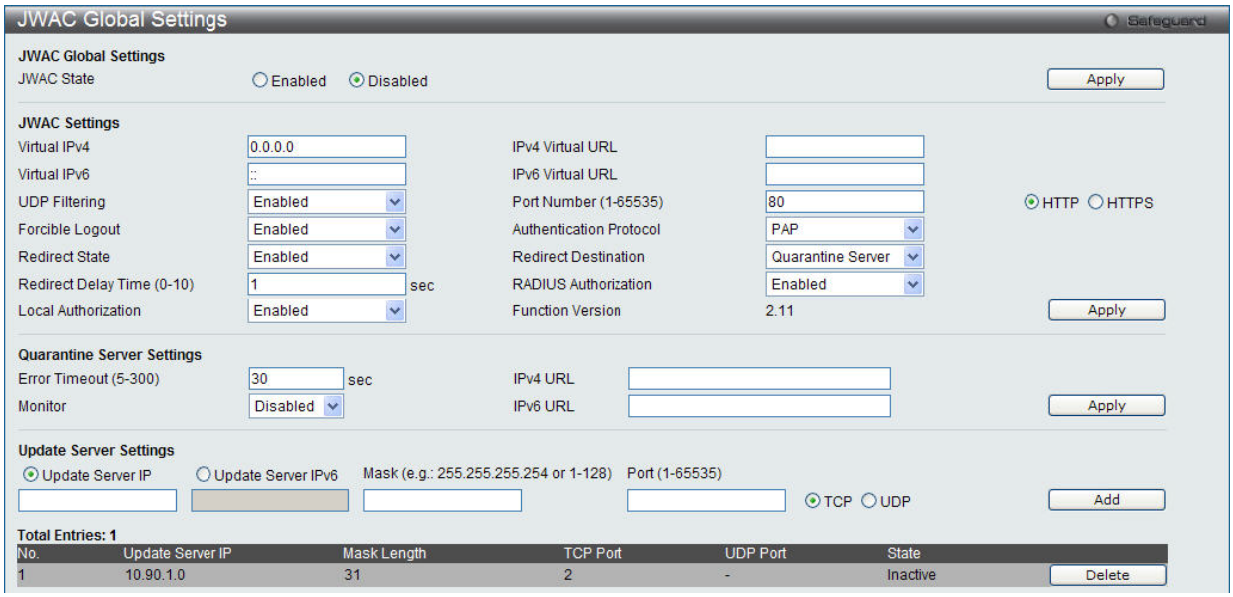


図 12-46 JWAC Global Settings

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 IPv4	未認証ホストからの認証リクエストを受け入れるために使用する JWAC 仮想 IPv4 アドレスを入力します。これは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 の仮想 IP アドレスです。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。
IPv4 Virtual URL	使用する IPv4 仮想 URL を入力します。
Virtual IPv6	未認証ホストからの認証リクエストを受け入れるために使用する JWAC 仮想 IPv6 アドレスを入力します。
IPv6 Virtual URL	使用する IPv6 仮想 URL を入力します。
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。
Port Number (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。
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。オプションには Local、EAP MD5、PAP、CHAP、MS CHAP、および MS CHAPv2 があります。
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。

項目	説明
Redirect Destination	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前にリダイレクトされる宛先を指定します。
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。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。Quarantine Server を検出できない場合、リダイレクト Quarantine Server を有効にし、リダイレクトする先を Quarantine Server として設定することによりすべての未認証 HTTP リクエストを JWAC Login Page にリダイレクトします。
IPv4 URL	JWAC Quarantine Server の IPv4 URL を指定します。リダイレクトが有効で、リダイレクトの宛先が Quarantine Server であると、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、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、PC ユーザにユーザ名とパスワードの入力を要求し、認証処理を終了します。
IPv6 URL	JWAC Quarantine Server の IPv6 URL を指定します。
Update Server Settings	
Update Server IP	更新用サーバの IPv4 アドレスを指定します。
Update Server IPv6	更新用サーバの IPv6 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 (1-65535)	更新サーバが使用するポート番号を選択します。 • TCP - TCP ポートを使う場合、選択します。 • UDP - UDP ポートを使う場合、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。

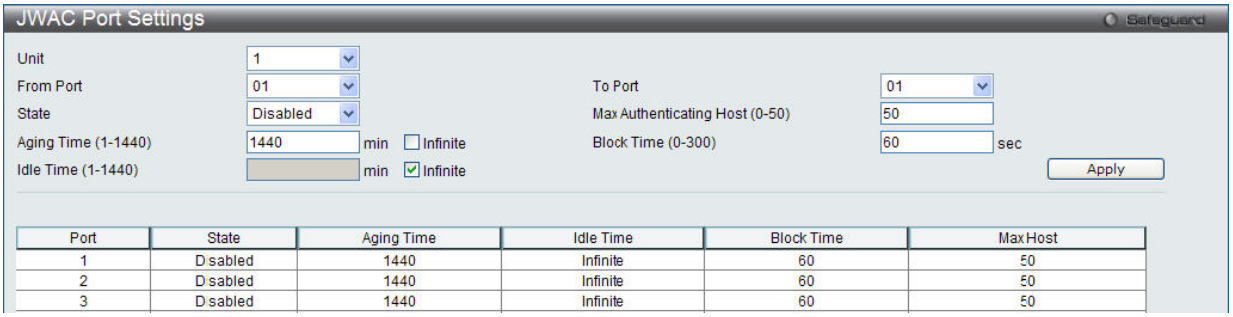


図 12-47　JWAC Port Settings 画面

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
Unit	設定するユニットを選択します。
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。
State	プルダウンメニューを使用して JWAC ポートとして設定するポートを有効にします。
Max Authenticating Host (0-50)	同時に各ポートに許可される認証処理を試みるホストの最大数を指定します。
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。「Infinite」をチェックすると、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 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。値を変更するにには「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をチェックしません。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。

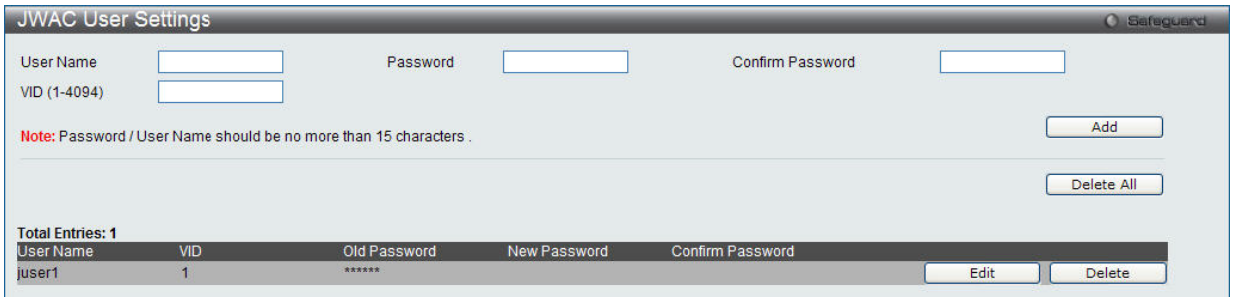


図 12-48 JWAC User Settings 画面

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。
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 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。

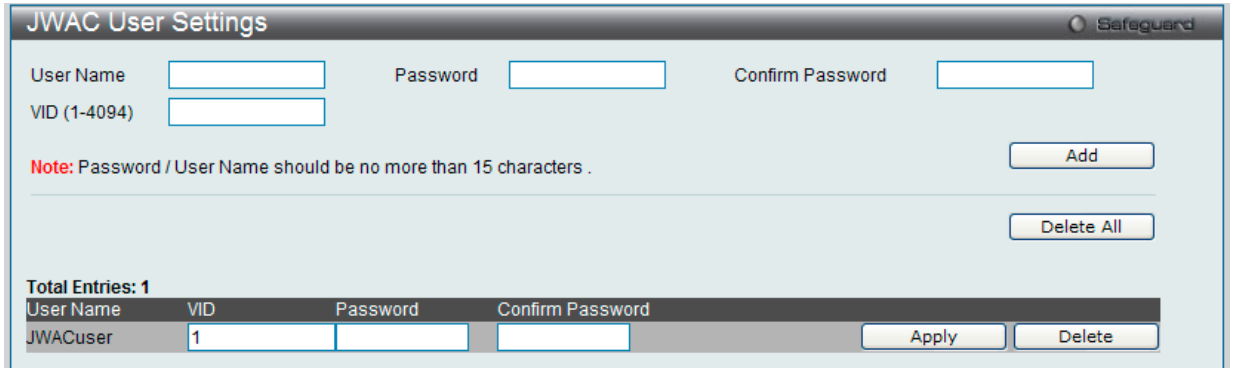


図 12-49 JWAC User Settings 画面 - Edit

2. エントリを編集して「Apply」ボタンをクリックします。

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。

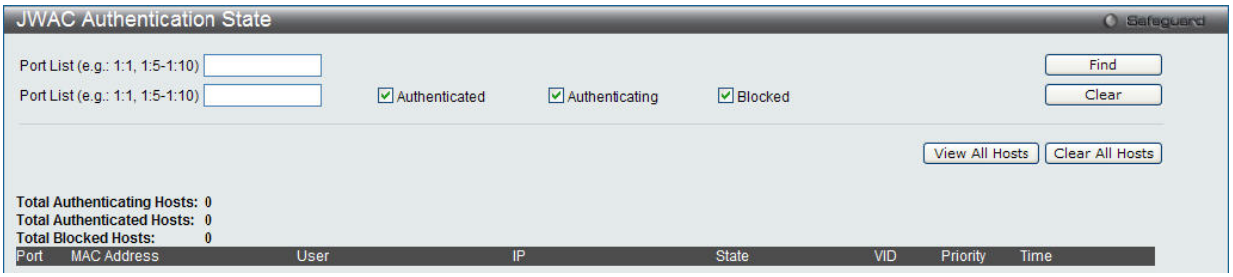


図 12-50　JWAC Authentication State 画面

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 12-51　JWAC Customize Page Language 画面

以下の項目を設定します。

項目	説明
Customize Page Language	ラジオボタンを使用して「English」または「Japanese」を選択します。

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。

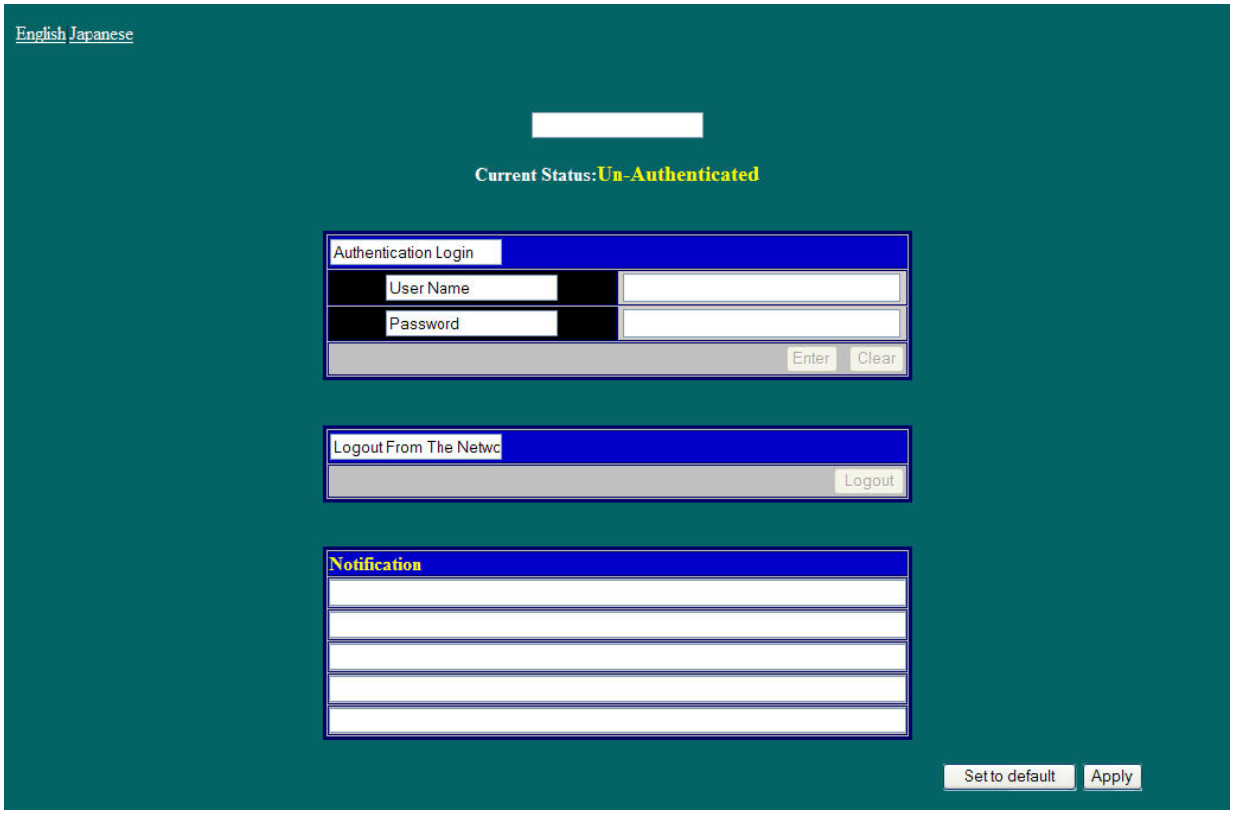


図 12-52　JWAC Customize Page 画面（English）

図 12-53　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）

コンパウンド認証により複数の認証をスイッチに設定することが可能です。

Compound Authentication Settings（コンパウンド認証設定）

コンパウンド認証の設定を行います。

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

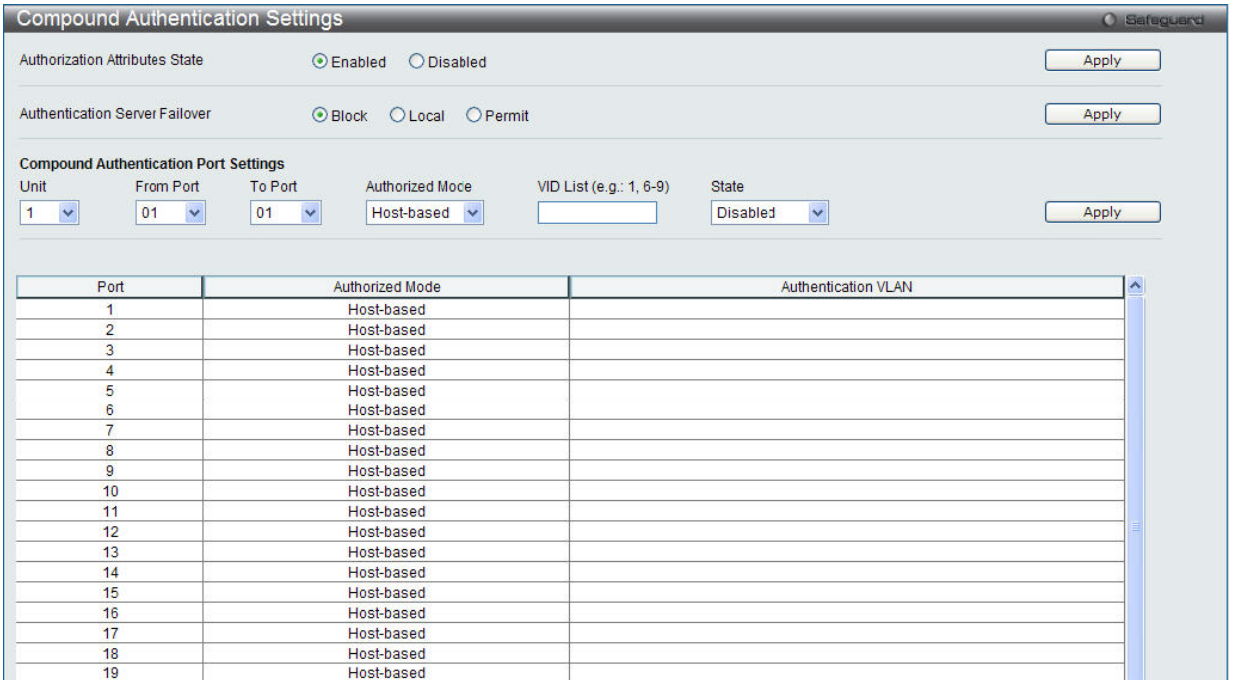


図 12-54　Compound Authentication Settings（SI モード時）画面

注意 SI モードでは Compound 認証機能はご利用になれませんのでご注意ください。

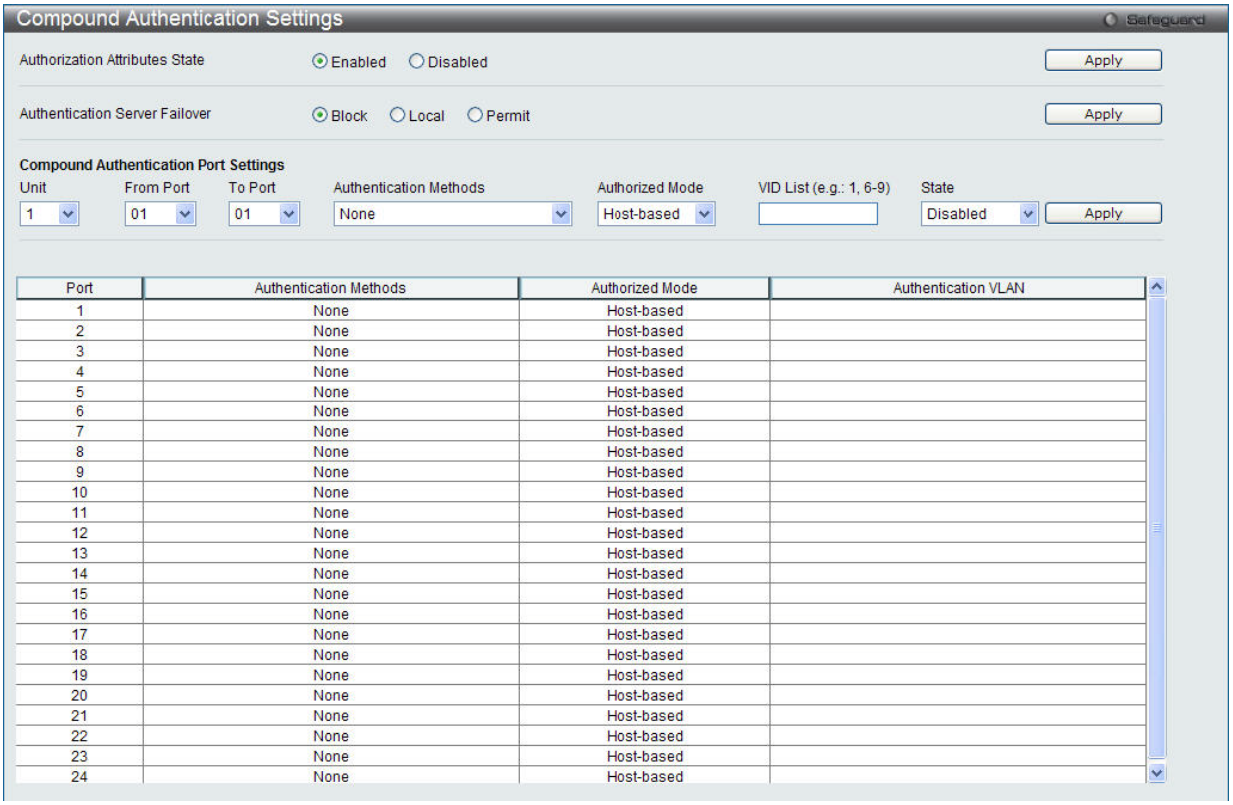


図 12-55　Compound Authentication Settings（EI モード時）画面

以下の項目を使用して設定を行います。

項目	説明
Authorization Network State	「Authorization Network」のステータスを有効 / 無効にします。
Authentication Server Failover	Authentication Server Failover 機能について設定します。 • Local -「Local」を選択するとローカルデータベースを使用してクライアントを認証します。クライアントがローカル認証に失敗した場合、クライアントは非認証として認識されます。 • Permit -「Permit」が選択した場合クライアントは常に認証状態で認識されます。ゲスト VLAN が有効の場合、クライアントはゲスト VLAN に残ります。そうでなければオリジナルの VLAN にステイします。 • Block -「Block」を選択するとクライアントは常に非認証（un-authenticated）として識別されます。
Unit	設定するスイッチを選択します。
From Port / To Port	認証ポートとして設定するポート範囲を指定します。
Authentication Methods (EI モードのみ)	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 アドレス認証、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 IP-MAC- ポートバインディング認証を行い、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 IP-MAC- ポートバインディング認証を行い、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 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。 • MAC+JWAC - MAC が最初に検証され、JWAC が検証されます。 「Both」では両方の認証が通過のために必要です。
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。
VID List	VLAN ID のリストを入力します。
State	プルダウンメニューで本機能の有効 / 無効を設定します。

「Apply」ボタンをクリックし、設定を有効にします。

注意 Compound 認証と DHCP スヌーピングは同じポートでは、動作できません。

Compound Authentication Guest VLAN Settings（コンパウンド認証ゲスト VLAN 設定）（EI モードのみ）

本画面ではコンパウンド認証ゲスト VLAN の設定を行います。

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。

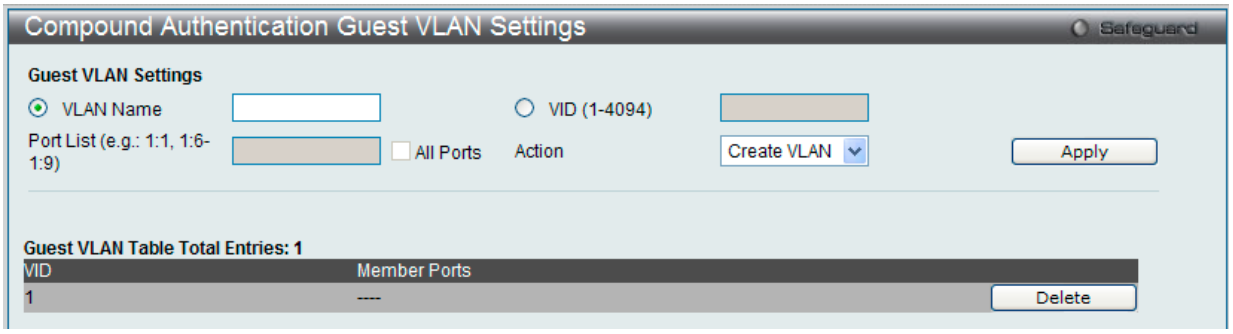


図 12-56 Compound Authentication Guest VLAN Settings 画面

以下の項目を使用して、SSH サーバの設定を行います。入力後、「Apply」ボタンをクリックします。

項目	説明
VID / VLAN Name	VLAN 名 /VLAN ID を入力し、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。
Port List	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 - ポートを追加します。 • Delete - ポートを削除します。

「Apply」ボタンをクリックし、設定を有効にします。
「Delete」ボタンをクリックして、指定エントリを削除します。

Compound Authentication MAC Format Settings（コンパウンド認証の MAC 形式設定）（EI モードのみ）

RADIUS サーバ経由の認証ユーザ名に使用される MAC アドレス形式を設定します。

Security > Compound Authentication > Compound Authentication MAC Format Settings の順にメニューをクリックし、以下の画面を表示します。

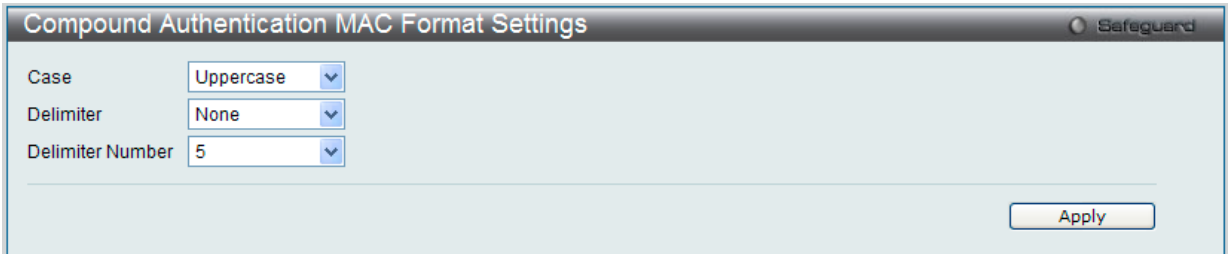


図 12-57 Compound Authentication MAC Format Settings 画面

本画面には以下の項目があります。

項目	説明
Case	使用する形式「uppercase」（大文字）または「lowercase」（小文字）を選択します。
Delimiter	MAC アドレスを入力する際の区切り「Hyphen」（ハイフン）、「Colon」（コロン）または「Dot」（ドット）を選択します。区切り文字を持たない場合には「None」を選択します。
Delimiter Number	MAC アドレスにおける区切り数を選択します。

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。

IGMP Access Control Settings（IGMP アクセスコントロール設定）

本製品の各ポートに IGMP 認証（IGMP アクセスコントロール）を設定することができます。本製品の認証状態が有効で IGMP の join リクエストを受信すると、RADIUS サーバに接続リクエストを送信して認証を行います。

IGMP 認証では IGMP レポートを以下のように処理します。ホストが希望するマルチキャストグループに join メッセージを送信する場合、本製品は、そのマルチキャストグループ / ポートを学習する前に認証を行う必要があります。本製品は、Access-Request（認証リクエスト）とホストの MAC、スイッチポート番号、スイッチ IP、およびマルチキャストグループ IP を含む情報を認証サーバに送信します。認証サーバが Access-Accept（アクセス許可）を返した場合、本製品はマルチキャストグループ / ポートを学習します。認証サーバが Access-Reject（アクセス拒否）を返した場合は、本製品はマルチキャストグループ / ポートを学習せず、パケットの処理を行いません。エントリ（ホスト MAC、スイッチポート番号、およびマルチキャストグループ IP）は認証エラーリストに入ります。T1 タイム後に認証サーバから何の応答もない場合、本製品はサーバに Access-Request（認証リクエスト）を再送信します。本製品が N1 タイム後に何の応答も受信しない場合、認証結果は拒否であり、エントリ（ホスト MAC、スイッチポート番号、およびマルチキャストグループ IP）は認証エラーリストに入ります。一般的に、マルチキャストグループ / ポートが学習済みの場合、再度認証が行われることはなく当該のパケットは通常のものとして処理されます。

IGMP 認証では IGMP leave を以下のように処理します。ホストが指定のマルチキャストグループに leave メッセージを送信する場合、本製品はグループ離脱の通常処理を行い、その後アカウンティングサーバに Accounting-Request（アカウンティングリクエスト）を送信して通知します。T2 タイム後にアカウンティングサーバから応答がない場合、本製品はサーバに Accounting-Request（アカウンティングリクエスト）を再送信します。リトライ時間の最大値は N2 です。

Security > IGMP Access Control Settings の順にクリックし、以下の画面を表示します。

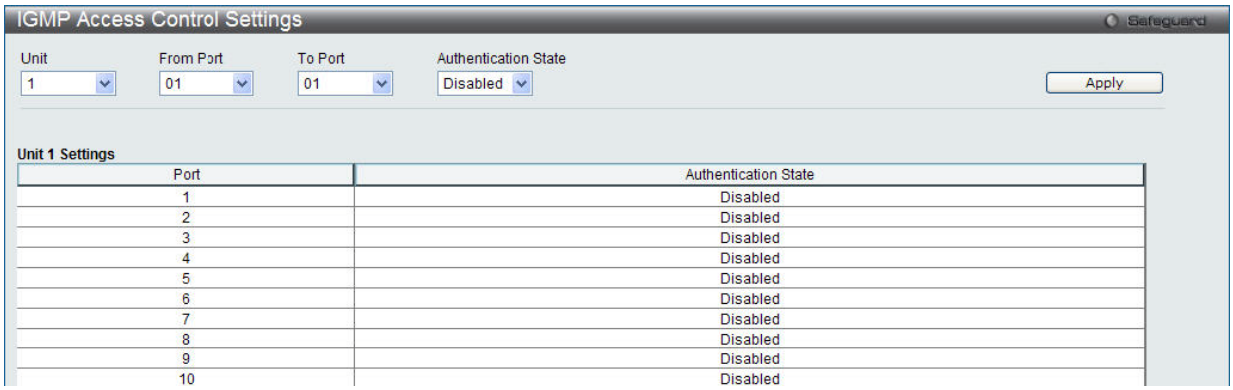


図 12-58　IGMP Access Control Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
Authentication State	指定ポートの RADIUS 認証機能を有効、または無効にします。

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

Port Security（ポートセキュリティ）

Port Security Settings（ポートセキュリティの設定）

ポートやポート範囲を指定して、ダイナミックなMACアドレス学習をロックすることにより、MACアドレスフォワーディングテーブルへ、新しいソース MAC アドレスが追加されないよう設定することができます。「Admin State」のプルダウンメニューで「Enabled」を選択し、「Apply」ボタンをクリックするとポートをロックできます。

ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

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

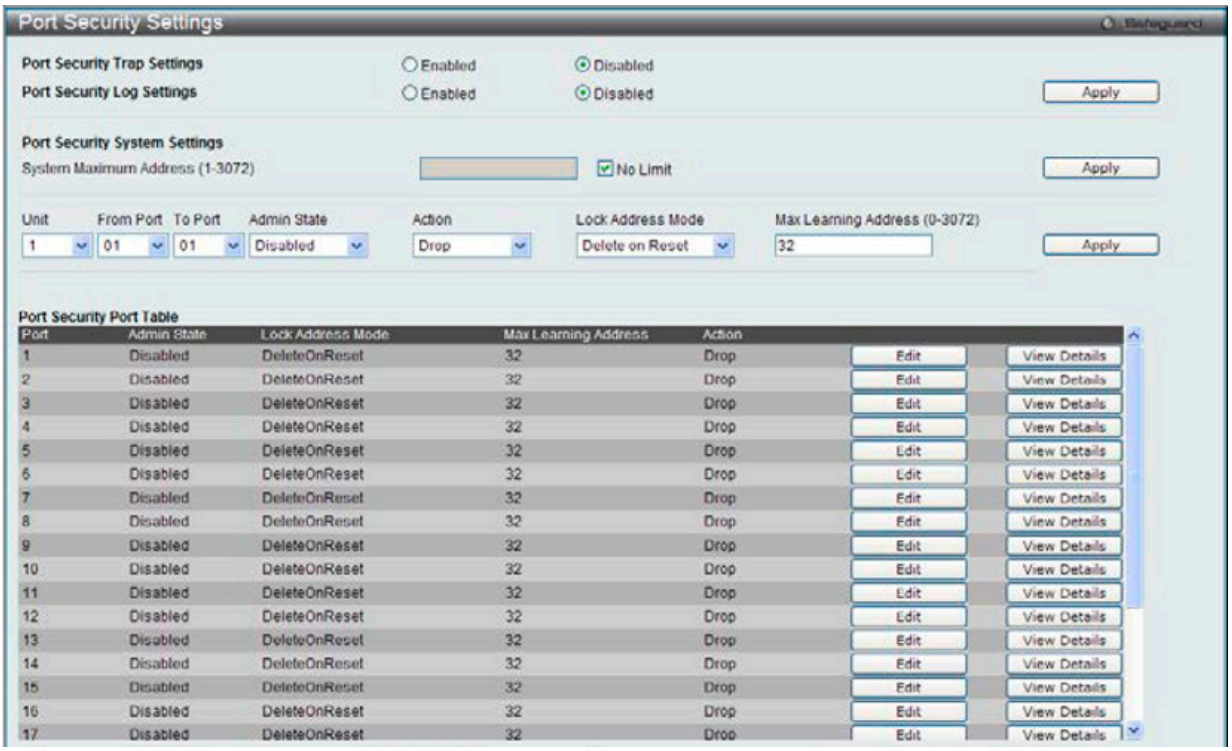


図 12-59　Port Security Settings 画面

本画面には以下の項目があります。

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 Max Address (1-3072)	システムの最大アドレス数を入力します。
Unit	ポートセキュリティ項目を表示するユニット番号を選択します。
From Port / To Port	ポートセキュリティ項目を表示するポート範囲を選択します。
Admin State	ポートセキュリティの有効 / 無効をプルダウンメニューで指定します。「Enabled」にすると、該当ポートは MAC アドレステーブルがロックされます。
Action	ドロップダウンメニューを使用してポートが習得可能な MAC アドレスの数が最大限に達した時に動作を選択します。 「Drop」- ポートが習得可能な MAC アドレスの数が最大限に達した時に新しいエントリは破棄されます。初期値です。 「Shutdown」- ポートが習得可能な MAC アドレスの数が最大限に達した時にポートはシャットダウンし、エラー無効状態に移行します。 ポートは手動でのみ復旧することが可能です。「Shutdown」はポートレベルでのセキュリティとして設定可能です。
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 – スイッチがリセットまたはリブートされても、ユーザが手動で削除するまでロックされたアドレスはエージングしません。 • Delete On Timeout – ロックされたアドレスは、エージングタイム経過後に削除されます。 • Delete On Reset – ロックされたアドレスはリセットか再起動されるまで削除されません。
Max Learning Address (0-3072)	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。

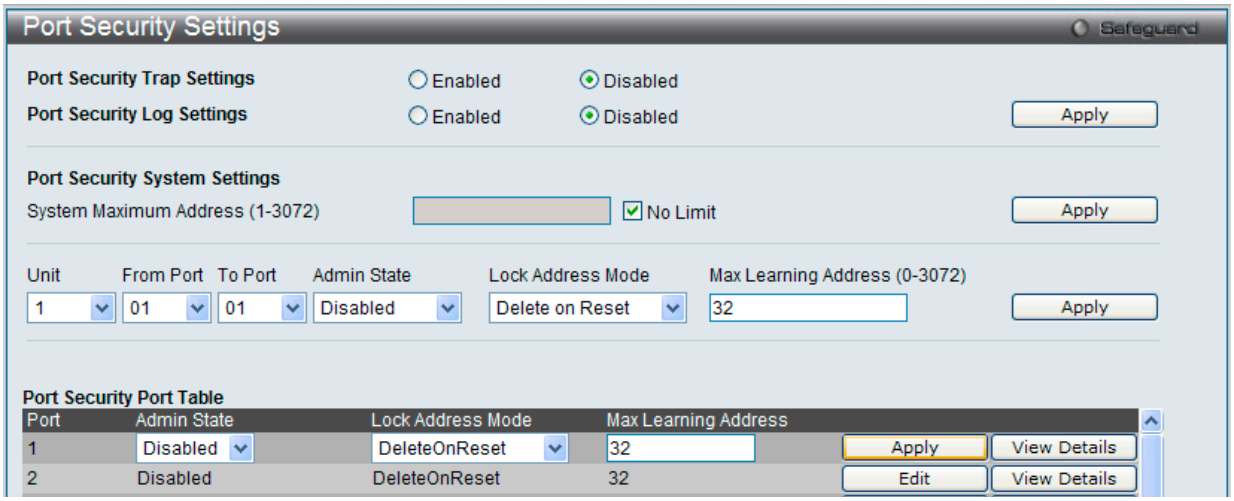


図 12-60　Port Security Settings 画面 - Edit

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」ボタンをクリックすると、以下の画面が表示されます。

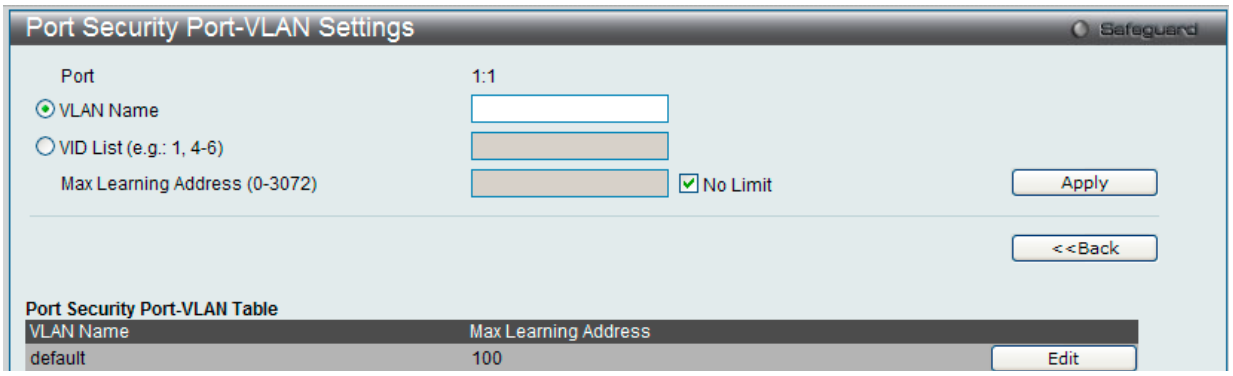


図 12-61　Port Security Port-VLAN Settings 画面

本画面には以下の項目があります。

項目	説明
VLAN Name	ラジオボタンをクリックして VLAN 名を入力します。
VID List	ラジオボタンをクリックして VLAN ID リストを入力します。
Max Learning Address (0-3072)	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。「No Limit」をチェックすると、VLAN が学習できるポートセキュリティエントリの最大数を制限しません。初期値は「No Limit」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。

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。

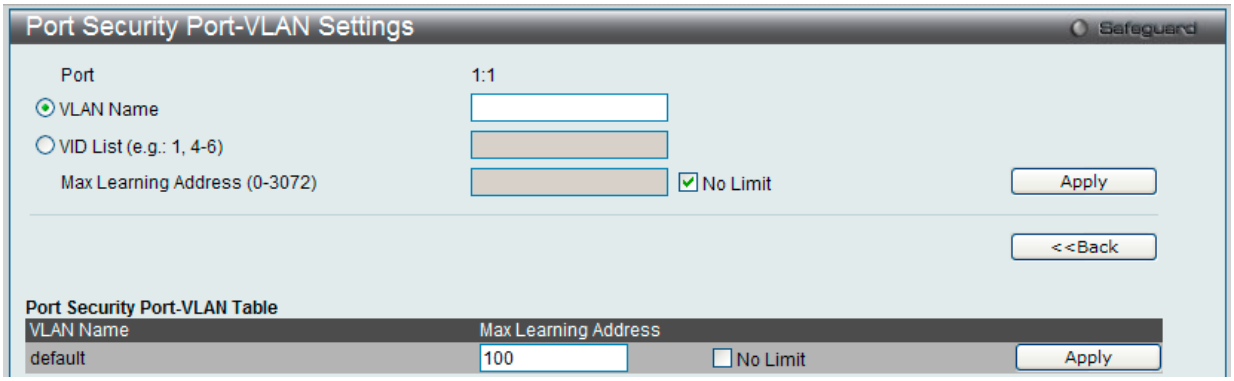


図 12-62　Port Security Port-VLAN Settings 画面 - Edit

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）

指定の VLAN の最大ポートセキュリティエントリ数を設定します。

Security > Port Security > Port Security 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。

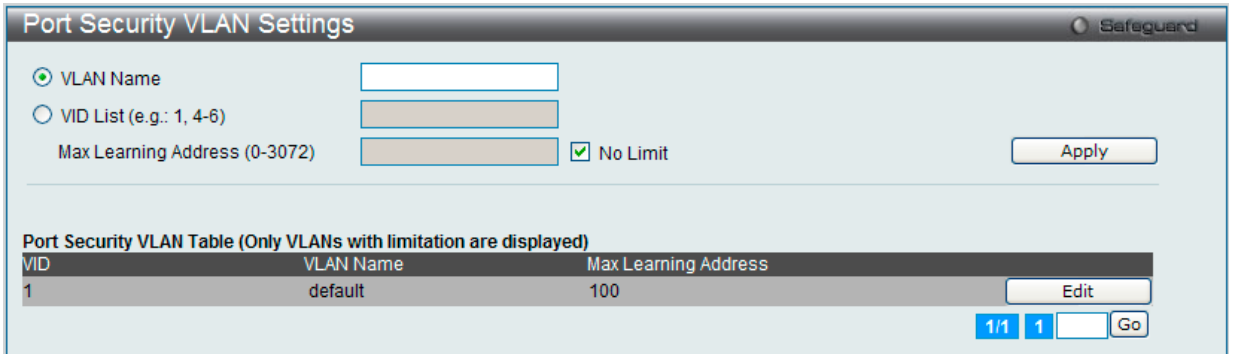


図 12-63 Port Security VLAN Settings 画面

本画面には以下の項目があります。

項目	説明
VLAN Name	VLAN 名を入力します。
VID List	VLAN ID のリストを指定します。
Max Learning Address	VLAN の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。

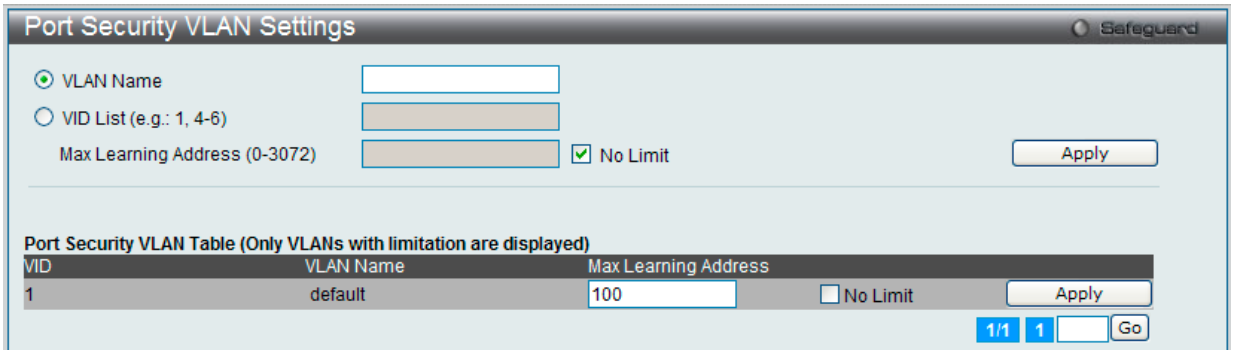


図 12-64 Port Security VLAN Settings 画面 - Edit

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）

スイッチに習得されたポートセキュリティエントリからエントリを削除し、フォワーディングデータベースに入力します。

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

図 12-65　Port Security Entries 画面

本画面には以下の項目があります。

項目	説明
VLAN Name	VLAN 名を入力します。
VID List	VLAN ID のリストを指定します。
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 / ポートリストを入力します。「All」を選択する場合、全てのポートが表示されます。
MAC Address	スイッチにより学習されたデータベーステーブルのエントリの MAC アドレス。
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。

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。

エントリの参照

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

エントリのクリア

「Clear」ボタンをクリックして、入力した情報に基づいてすべてのエントリを削除します。
「Clear All」ボタンをクリックして、表示されたすべてのエントリを削除します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

ARP Spoofing Prevention Settings（ARP スプーフィング防止設定）

ユーザは保護されたゲートウェイに対し、MAC のスプーフィングを防ぐためにスプーフィング防止を設定することができます。エントリーが作成された場合に、送信先 ARP パケットはエントリのゲートウェイ IP にマッチしているが、送信先 MAC フィールドもしくは送信元 MAC フィールドのどちらかがエントリのゲートウェイ MAC と合致しない場合はシステムにより破棄されます。

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

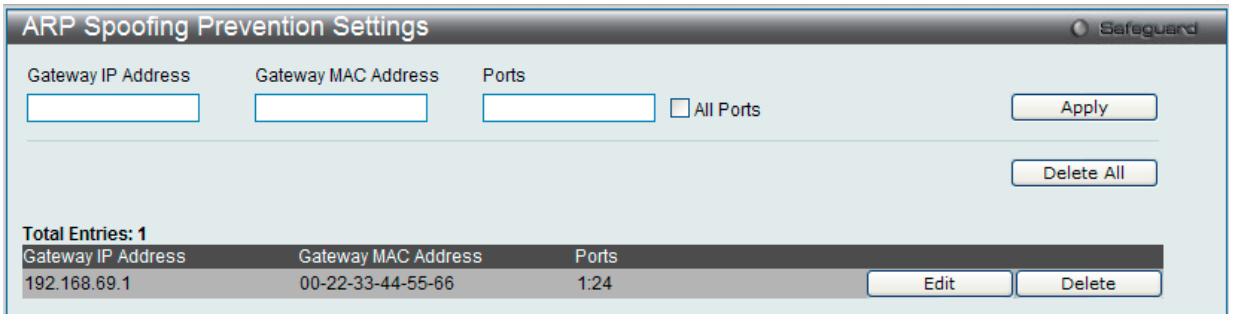


図 12-66　ARP Spoofing Prevention Settings 画面

以下の項目を使用して、設定します。

項目	説明
Gateway IP Address	ゲートウェイの IP アドレスを入力します。
Gateway MAC Address	ゲートウェイの MAC アドレスを入力します。
Ports	ARP Spoofing Prevention 設定を行うスイッチのポートを指定します。「All Ports」を指定すると、本エントリをスイッチのすべてのポートに設定します。

「Apply」ボタンをクリックし、変更を有効にします。

エントリの編集

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 12-67　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 BPDU 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「Tunnel STP Port(s)」で BPDU トンネルポートとして設定されていると、ポートは STP BPDU を転送します。しかし、ポートで BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

Security > BPDU Attack Protection の順にメニューをクリックし、以下の画面を表示します。

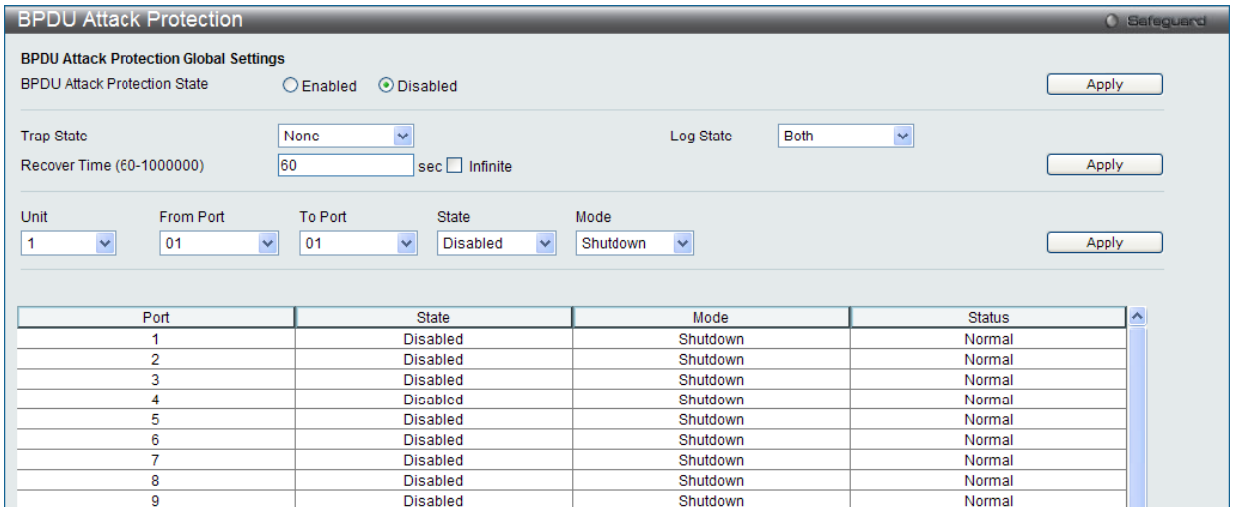


図 12-68　BPDU Protection Settings 画面

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	トラップの状態を指定します。「None」「Attack Detected」「Attack Cleared」「Both」から選択します。
Log State	ログ出力の状態を指定します。「None」「Attack Detected」「Attack Cleared」「Both」から選択します。
Recover Time(60-1000000)	BPDU 防止の自動復帰タイマを指定します。復帰タイマの初期値は 60 です。60 から 1000000（秒）の範囲で指定できます。「Infinite」ボックスをチェックすると、ポートは自動的に回復しません。
Unit	設定するユニットを選択します。
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。

「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）

ループバック検知機能は、特定のポートによって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。プルダウンメニューを使用し、機能を「Enabled」（有効）/「Disabled」（無効）にします。

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

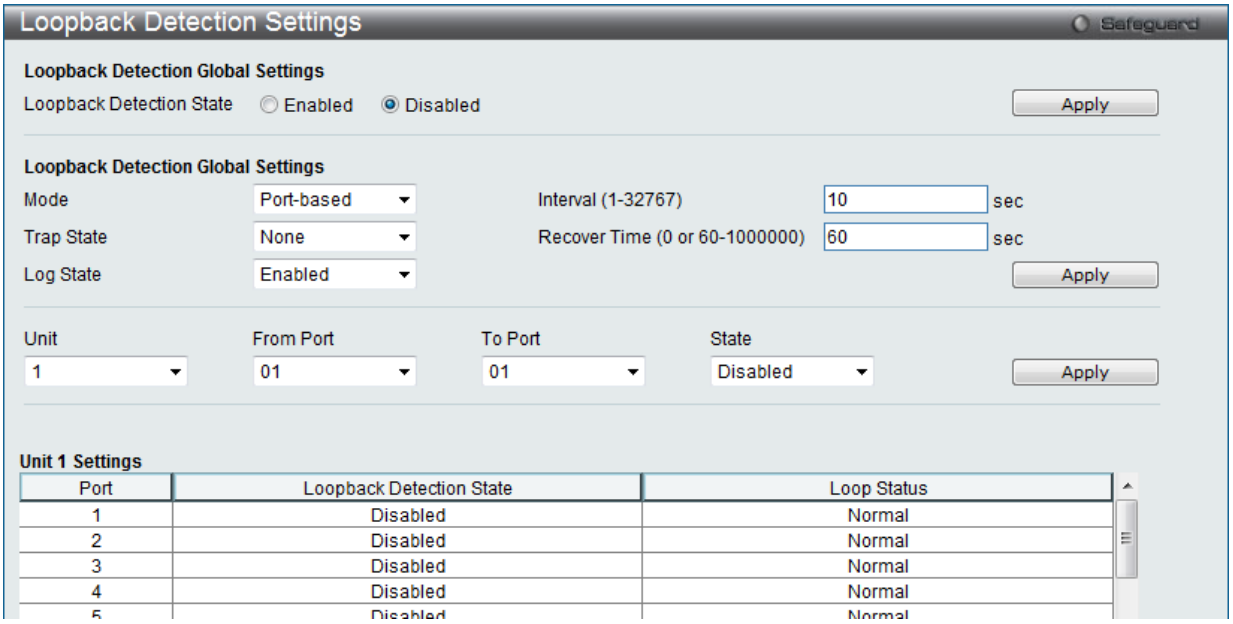


図 12-69　Loopback Detection Settings 画面

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で「Port Based」または「VLAN Based」を選択します。
Trap Status	トラップステータス（「None」（なし）、「Loop Detected」（ループの検出）、「Loop Cleared」（ループのクリア）または「Both」（ループの検出とクリア））を設定します。
Log State	ループバック検知機能のログ取得について設定します。
Interval (1-32767)	ループ検知間隔を設定します。（1-32767 秒）
Recover Time (0 or 60-1000000)	ループバック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 STP ループバックをチェックします。ループバックが検知されないと、STP は再開します。0 または 60-1000000（秒）に設定します。0 を指定すると、Loopdetect Recover Time は無効になります。初期値は 60（秒）です。
Unit	設定するユニットを指定します。
From Port	プルダウンメニューで開始ポートを選択します。
To Port	プルダウンメニューで終了ポートを選択します。
State	「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。

RPC PortMapper Filter Settings（RPC ポートマップフィルタ設定）

RPC ポートマップフィルタの設定を指定のポートに行います。RPC ポートマップサービスはスタティックポート（TCP または UDP ポート 135）をリッスンし、RPC プログラム番号を TCP/IP（または UDP/IP）プロトコルポート番号に変換します。Outlook や Exchange、Messenger などのアプリケーションはエンドポイントのマッピング用の TCP と UDP ポート 135 を同時にリッスンします。TCP/UDP ポート 135 の不正なサービスの使用禁止などの目的で本機能は使用されます。

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

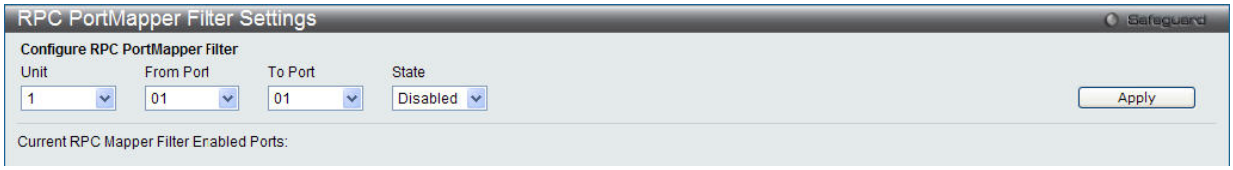


図 12-70　RPC PortMapper Filter Settings 画面

項目	説明
Unit	設定するユニットを指定します。
From Port	プルダウンメニューで開始ポートを選択します。
To Port	プルダウンメニューで終了ポートを選択します。
State	「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。

NetBIOS Filtering Settings（NetBIOS フィルタリング設定）

NetBIOS は、ネットワークをまたいで通信するために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されるプロトコルです。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取り組みをしました。

NetBEUI プロトコルを使用する 2 台以上のコンピュータにおける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 Settings の順にメニューをクリックし、以下の画面を表示します。

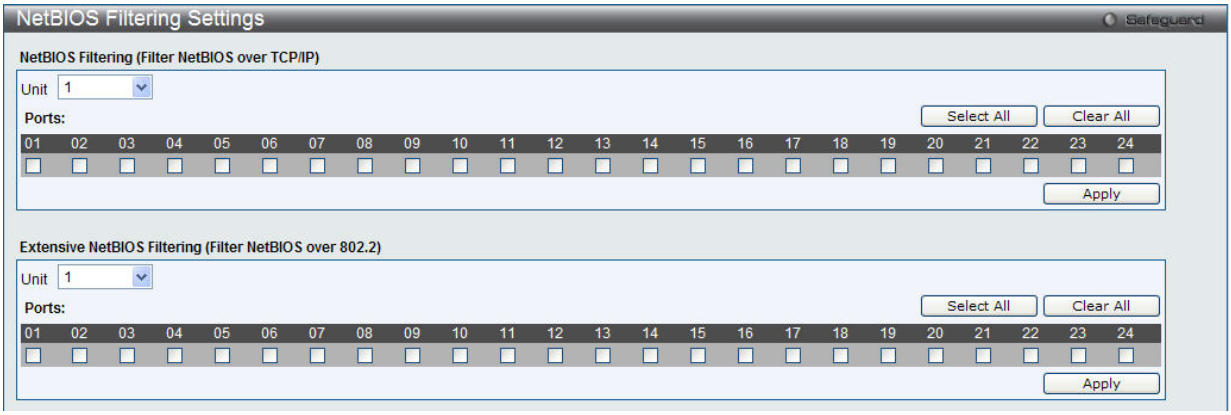


図 12-71　NetBIOS Filtering Settings 画面

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。	
Unit	設定するユニットを選択します。
Ports	NetBIOS フィルタリング設定に含める適切なポートを簡単にチェックできます。
Extensive NetBIOS Filtering Ports	
Extensive NetBIOS フィルタリング設定に含める適切なポートを選択します。Extensive NetBIOS は 802.3（TCP/IP）における NetBIOS です。スイッチはこれが有効なポートでは 802.3 における NetBIOS フレームを拒否します。	
Unit	設定するユニットを選択します。
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。
「Select All」ボタンをクリックすると設定用にすべてのポートを選択します。
「Clear All」ボタンをクリックして、すべてのポートを削除します。

Traffic Segmentation（トラフィックセグメンテーション）

トラフィックセグメンテーション機能は、（単一 / 複数）ポート間のトラフィックの流れを制限するために使用します。「トラフィックフローの分割」という方法は、「VLAN によるトラフィック制限」に似ていますが、さらに制限的です。本機能によりマスタスイッチ CPU のオーバヘッドを増加させないようにトラフィックを操作することが可能です。

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

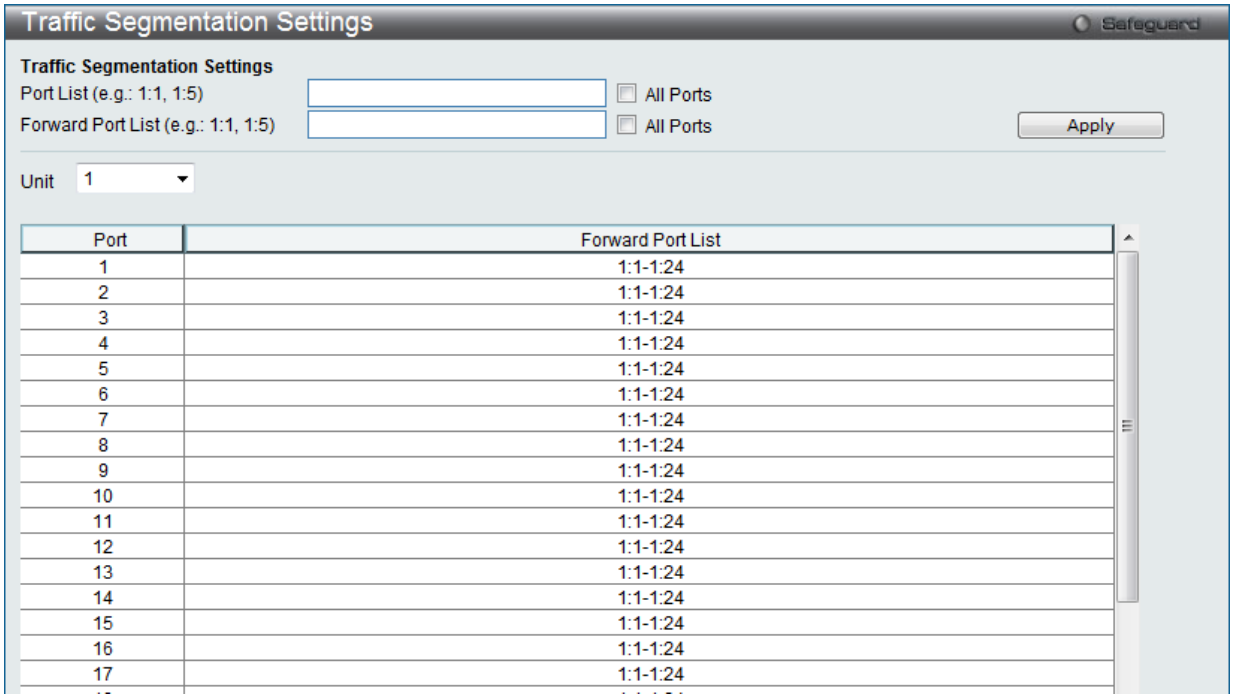


図 12-72 Traffic Segmentation 画面

以下の項目を使用して設定を行います。

項目	説明
Port List	トラフィックセグメンテーションを有効にするポートを指定します。
Forward Port List	パケットの送信先となるスイッチのポートを指定します。これらのポートは、上記「Port」フィールドで指定したポートからのパケットを受信します。 • Clear All - 設定した全てのポートを削除します。 • Select All - は全てのポートを選択します。
Unit	設定するユニットを指定します。
Ports	パケットを送信するポートが表示されます。

「Apply」ボタンをクリックすると、設定内容がテーブルに反映されます。

DHCP Server Screening Settings（DHCP サーバスクリーニング設定）

DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。この DHCP サーバフィルタ機能が有効になると指定ポートからのすべての DHCP サーバパケットはフィルタされます。

DHCP Screening Port Settings（DHCP スクリーニングポート設定）

スイッチのポートを設定します。

Security > DHCP Server Screening > DHCP Server Screening Port Settings の順にメニューをクリックして画面を表示します。

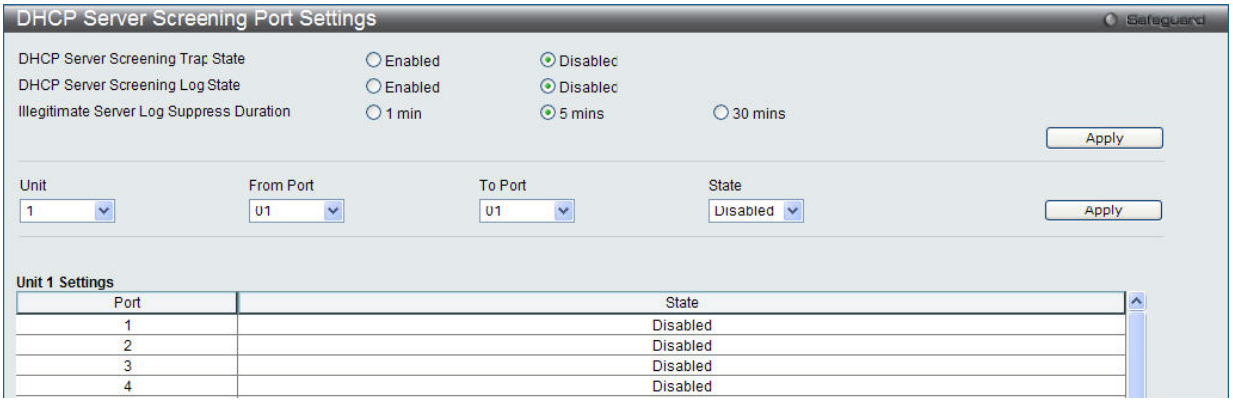


図 12-73　DHCP Server Screening Port Settings 画面

本画面には以下の項目があります。

項目	説明
Filter DHCP Server Trap State	不正 DHCP サーバパケットを検知した時に、記録したログトラップを送信する本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Filter DHCP Server Log State	不正 DHCP サーバパケットを検知した時に、ログに記録する本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Illegitimate Server Log Suppress Duration	DHCP サーバフィルタリング機能はあらゆる不正 DHCP サーバパケットをフィルタし、不正パケットを送信し続ける DHCP サーバをログに記録します。一度ログとして登録された不正パケットを送信する DHCP サーバは送信数に限らず不正 DHCP サーバとして検出されます。 ログは 1 分間に圧縮されますが 5 分か 30 分にも設定可能です。初期値は 5 分です。
Unit	設定するユニットを指定します。
From Port/To Port	選択したポートから連続した複数のポートを設定できます。
State	「Enabled」（有効）または「Disabled」を選択して、DHCP サーバを有効、または無効にします。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 / 削除を行います。

Security > DHCP Server Screening > DHCP Offer Permit Entry Settings の順にクリックし、画面を表示します。

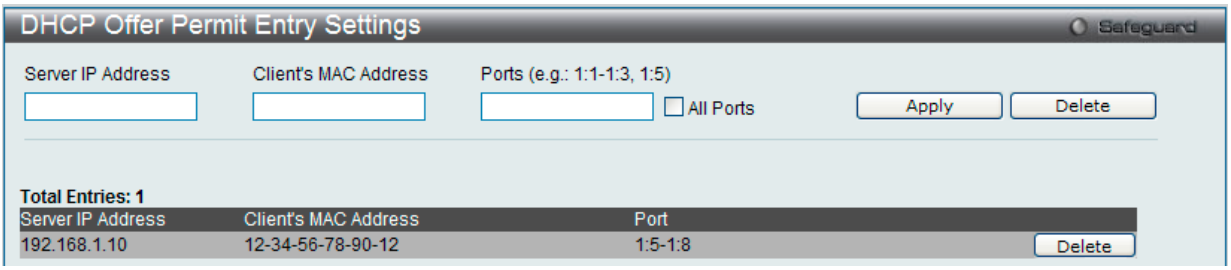


図 12-74　DHCP Offer Permit Entry Settings 画面

本画面には以下の項目があります。

項目	説明
Server IP Address	DHCP サーバの IP アドレス。
Client's MAC Address	クライアントの MAC アドレス。
Ports (e.g.:1-3,5)	DHCP サーバとして使用するポートの範囲を選択します。スイッチのすべてのポートを使用したい場合は「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。
- Extended TACACS (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 つのうちから 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）の方式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ていることにご注意ください。ユーザが管理者レベルの権限に更新したい場合、「Enable Admin」画面にアクセスし、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」画面を使用して、権限レベルを昇格させることはできません。

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）

「Enable Admin」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、管理者レベルに変更したい場合に使用します。スイッチにログインした後のユーザにはユーザレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本画面を開き、認証用パスワードを入力します。本機能における認証方法は、TACACS/ XTACACS/ TACACS+/ RADIUS、ユーザ定義のサーバグループ、local enable（スイッチ上のローカルアカウント）または、認証なし（none）から選択できます。XTACACS と TACACS は Enable の機能をサポートしていないため、ユーザはサーバホスト上に特別なアカウントを作成し、ユーザ名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「Disabled」（無効）である場合には実行できません。

Security > Access Authentication Control > Enable Admin の順にメニューをクリックし、以下の画面を表示します。

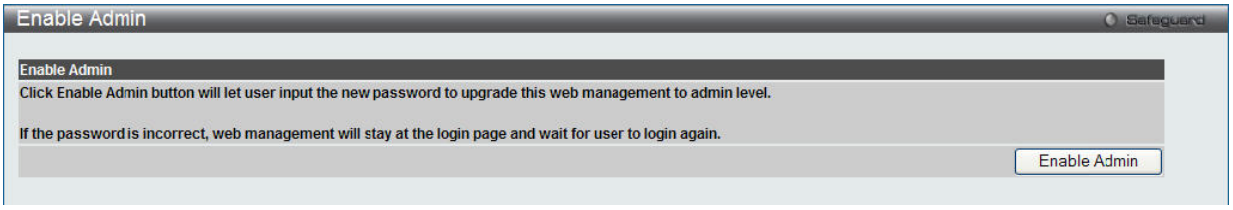


図 12-75　Enable Admin 画面

「Enable Admin」ボタンをクリックして以下のダイアログボックスを表示します。

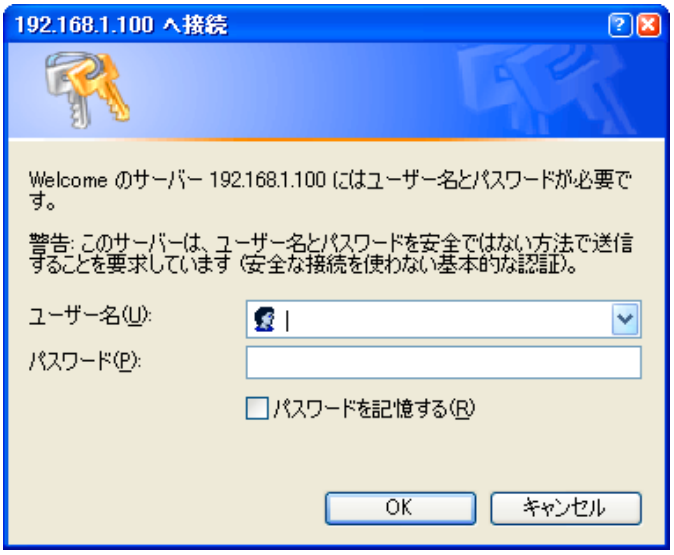


図 12-76　ユーザ名とパスワード入力ダイアログボックス

「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）

本メニューは、管理者が定義するスイッチにアクセスするユーザのための認証ポリシーを有効にするために使用します。有効にすると、デバイスはログインメソッドリストをチェックし、ログイン時のユーザ認証に使用する認証方法を選択します。

Security > Access Authentication Control > Authentication Policy Settings の順にメニューをクリックし、以下の画面を表示します。

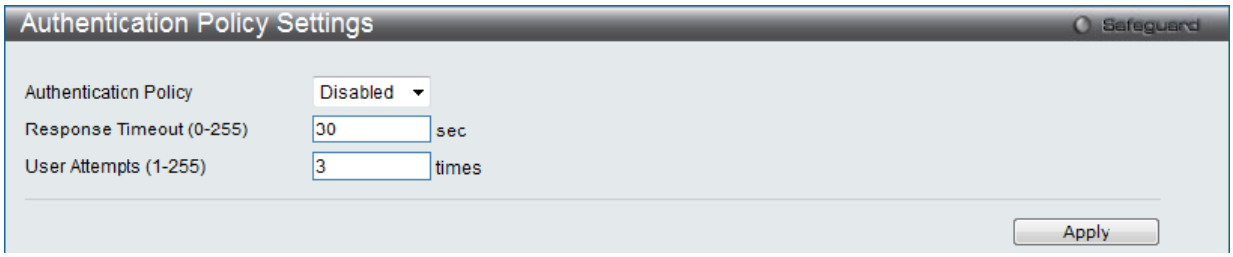


図 12-77 Authentication Policy Settings 画面

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）または「Disabled」（無効）を設定します。
Authentication Policy Encryption	認証ポリシー暗号化の状態を有効または無効にします。
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。

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。

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、HTTP）を設定します。

Security > Access Authentication Control > Application Authentication Settings の順にクリックし、以下の画面を表示します。

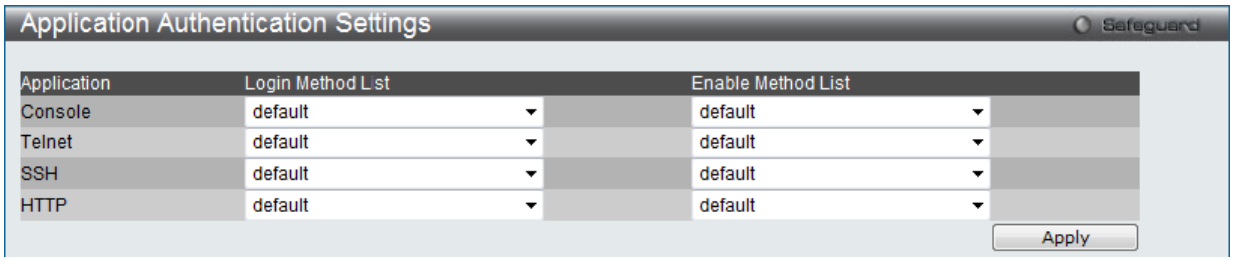


図 12-78 Application Authentication Settings 画面

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 Settings」画面を参照してください。
Enable 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「Enable Method Lists Settings」画面を参照してください。

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。

Accounting Settings（アカウント設定）

RADIUS アカウントサービスの状態を設定します。

Security > Access Authentication Control > Accounting Settings の順にクリックし、以下の画面を表示します。

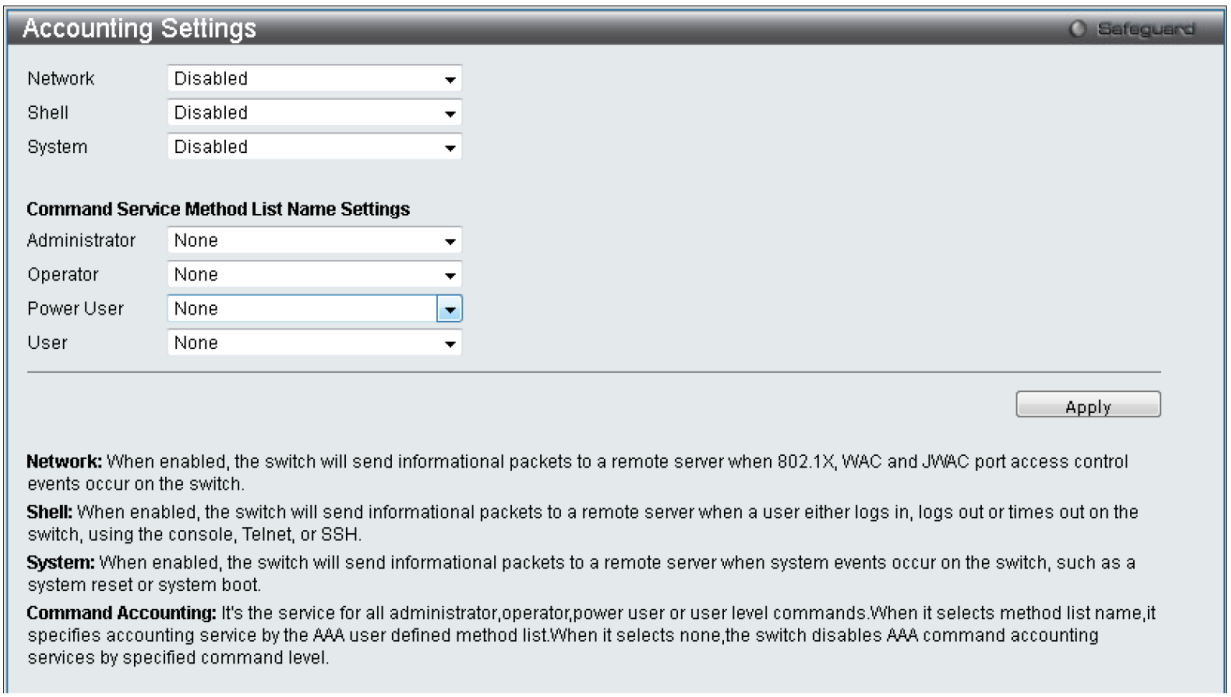


図 12-79　Accounting Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Network	「RADIUS Only」が選択された場合、リモート RADIUS サーバに「Network」情報パケットを送信します。 「Method List Name」が選択された場合、作成されたメソッドリストを基に「Network」情報パケットを送信します。
Shell	「RADIUS Only」が選択された場合、リモート RADIUS サーバに「Shell」情報パケットを送信します。 「Method List Name」が選択された場合、作成されたメソッドリストを基に「Shell」情報パケットを送信します。
System	「RADIUS Only」が選択された場合、リモート RADIUS サーバに「System」情報パケットを送信します。 「Method List Name」が選択された場合、作成されたメソッドリストを基に「System」情報パケットを送信します。
Administrator	選択されると「Administrator」レベルのコマンドが有効になります。
Operator	選択されると「Operator」レベルのコマンドが有効になります。
Power User	選択されると「Power User」レベルのコマンドが有効になります。
User	選択されると「User」レベルのコマンドが有効になります。

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。

Authentication Server Group Settings（認証サーバグループ設定）

本スイッチ上に認証サーバグループの設定を行います。

サーバグループとは、TACACS/ XTACACS/ TACACS+/ RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分け

したものです。プロトコルによって、または定義済みのサーバグループに組み込むことによりグループ分けを行います。スイッチには 4 つの認証サーバグループがあらかじめ組み込まれています。これらは削除することができませんが、内容の変更は可能です。1 つのグループにつき最大 8 個までの認証サーバホストを登録できます。

Security > Access Authentication Control > Authentication Server Group Settings の順にメニューをクリックし、以下の画面を表示します。

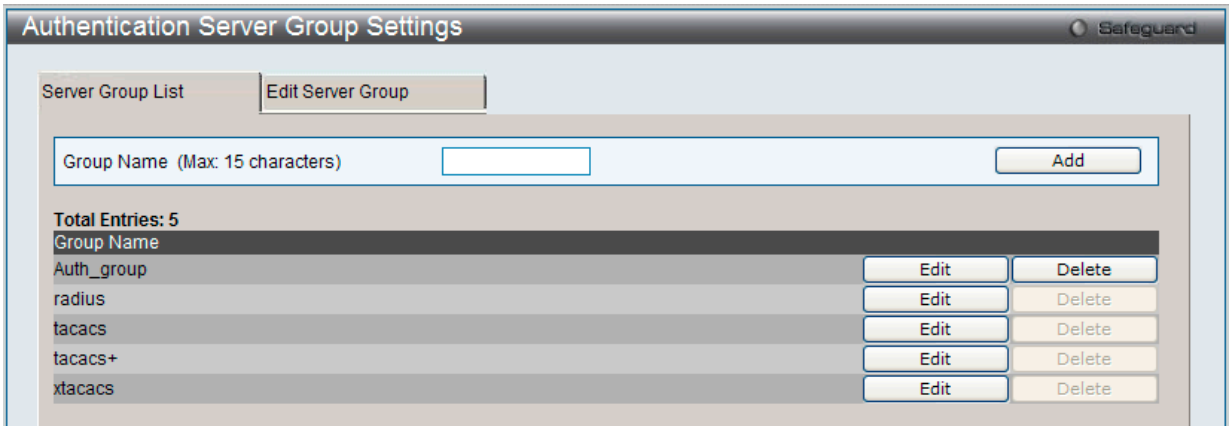


図 12-80　Authentication Server Group - Server Group List タブ画面

本画面では、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の登録

「Group Name」に名前を入力し、「Add」ボタンをクリックします。

特定のグループの編集

「Edit」ボタン（または「Edit Server Group」タブ）をクリックし、以下の画面を表示します。

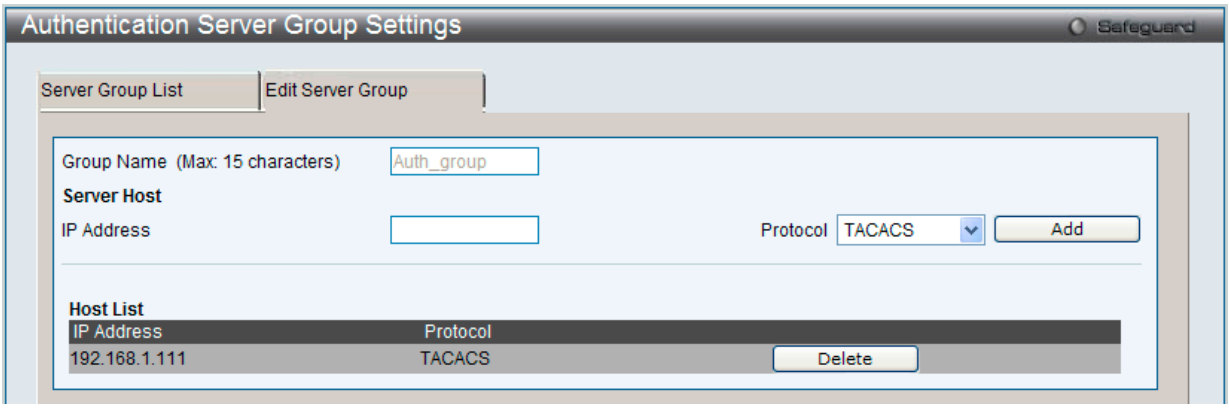


図 12-81　Authentication Server Group - Edit Server Group タブ画面

Authentication Server Host をリストに追加する

「Group Name」に名前、「IP Address」に IP アドレスを指定し、その IP アドレスを持つ Authentication Server Host の Protocol を選びます。「Add」ボタンをクリックし、Authentication Server Host をグループに加えます。
このタブの下部の Host List にエントリが表示されます。

注意　認証サーバホストをリストに追加する前に、「Authentication Server Settings」画面にてホストの登録を行う必要があります。本機能を正しく動作させるためには、リモートの中央管理サーバ上でプロトコルを指定して認証サーバホストの設定を行う必要があります。

注意　あらかじめ組み込まれている 4 つのサーバグループには、同じ TACACS デーモンが起動されているサーバホストのみを入れることができます。TACACS/XTACACS/TACACS+ プロトコルは別のエンティティで、互換性はありません。

Authentication Server Settings（認証サーバ設定）

スイッチに TACACS/ XTACACS/ TACACS+/ RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを設定します。

ユーザが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/ XTACACS/ TACACS+/ RADIUS サーバ

ホストに認証パケットを送信します。すると TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/ XTACACS/ TACACS+/ RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

Security > Access Authentication Control > Authentication Server Settings の順にメニューをクリックし、以下の画面を表示します。

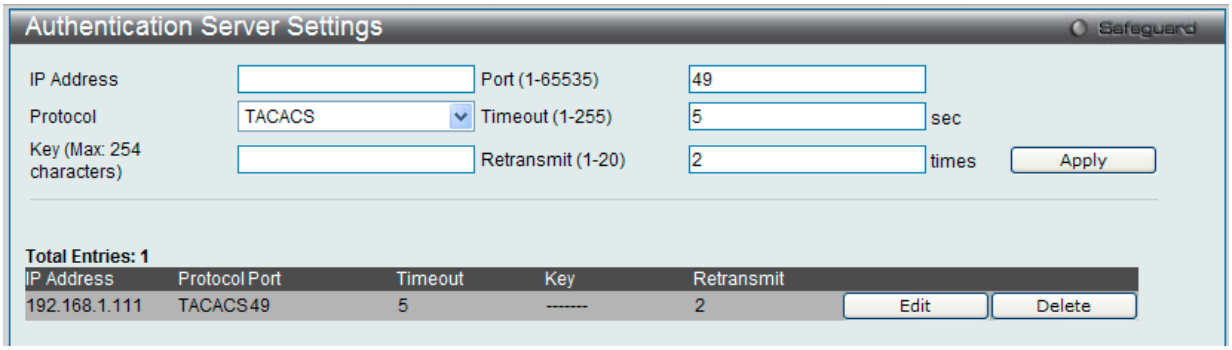


図 12-82　Authentication Server 画面

認証サーバホストを追加するためには、以下の項目を使用します。

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
Protocol	サーバホストで動作しているプロトコルを指定します。以下の一つを選ぶことができます。 • 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。
Key (Max 254 characters)	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。
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。ポート番号の初期値は、TACACS/ XTACACS/ TACACS+ サーバの場合は 49、RADIUS サーバの場合は 1812 です。独自の番号を設定してセキュリティを向上することも可能です。
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。
Retransmit (1-20)	TACACS サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数。

「Apply」ボタンをクリックしてサーバホストを追加します。エントリは本画面下半分のテーブルに表示されます。

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。

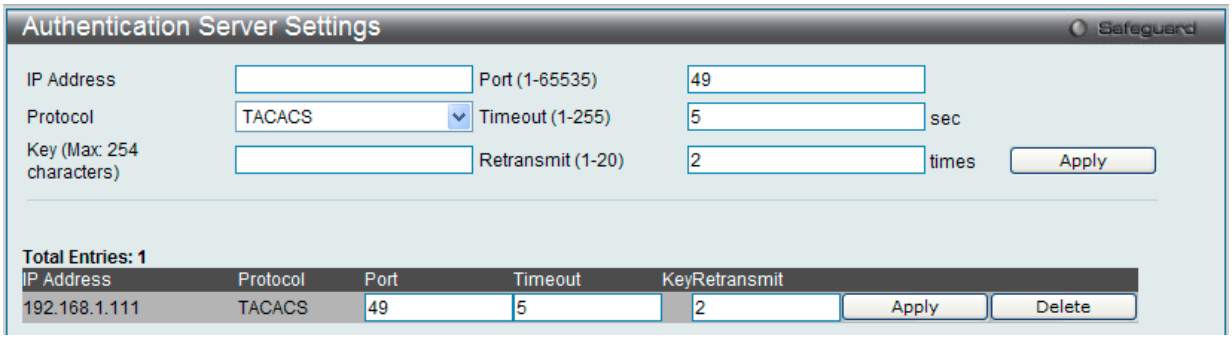


図 12-83　Authentication Server Settings 画面 - Edit

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設定）

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。

TACACS/XTACACS/TACACS+ または non（認証なし）の方式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ていることにご注意ください。ユーザが管理者レベルの権限に更新したい場合、「Enable Admin」画面にアクセスし、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」画面を使用して、権限レベルを昇格させることはできません。

Security > Access Authentication Control > Login Method Lists Settings の順にメニューをクリックし、以下の画面を表示します。

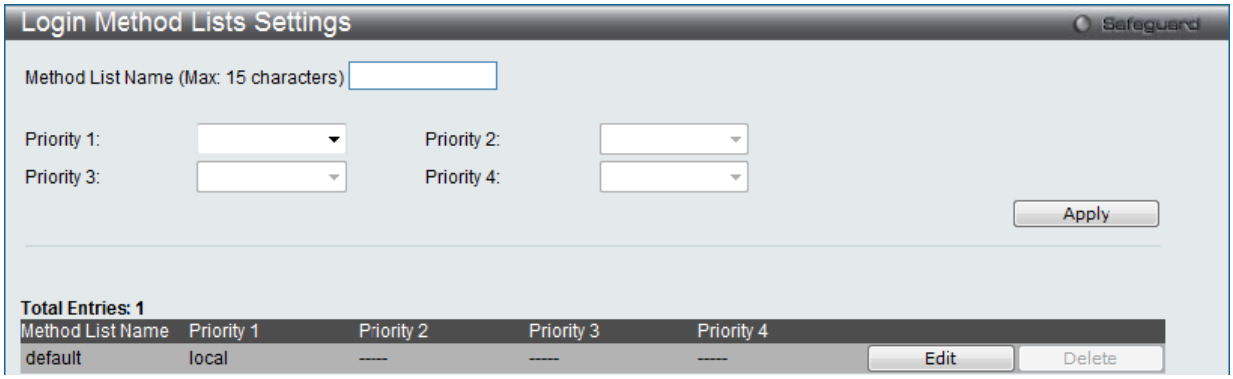


図 12-84　Login Method Lists Settings 画面

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。

エントリの新規登録

以下の項目を設定、「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。

エントリの編集

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。

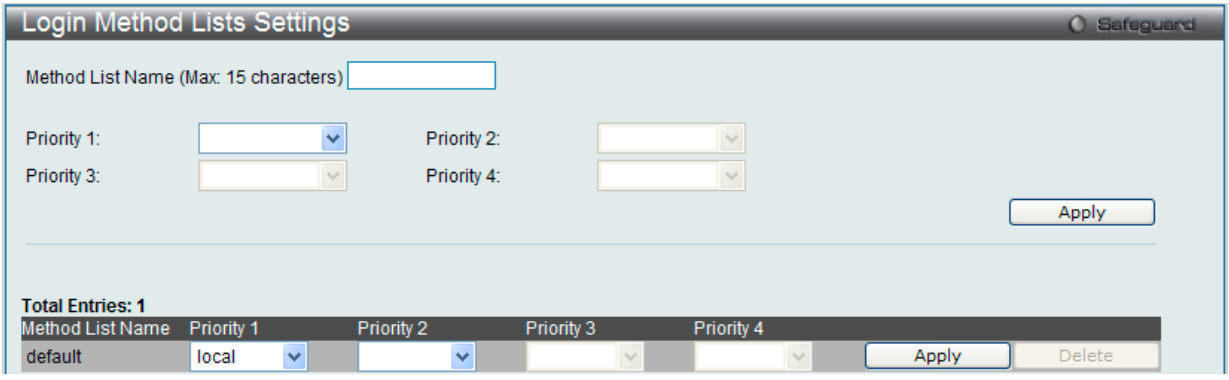


図 12-85　Login Method Lists 画面 - Edit

2. 項目を編集し、「Apply」ボタンをクリックします。

エントリの削除

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（メソッドリスト設定）

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 つはデフォルト Enable メソッドリストになります。本デフォルト Enable メソッドリストは内容の変更はできますが、削除はできません。

本メニューで定義した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS-XTACACS-Local の順番で認証方法を指定した場合、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに対して、認証リクエストを送信します。認証が確認できなければ、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリスト中の次の方法（XTACACS）を試します。それでも認証が行われなければ、スイッチ内に設定したローカル Enable パスワードを使用してユーザの認証を行います。

以上のいずれかの方法で認証されたユーザは、「Admin」（管理者）権限を取得することができます。

注意 ローカル Enable パスワードの設定については「Local Enable Password Settings（ローカルユーザパスワード設定）」の項を参照してください。

Security > Access Authentication Control > Enable method Lists Settings の順にメニューをクリックし、以下の画面を表示します。

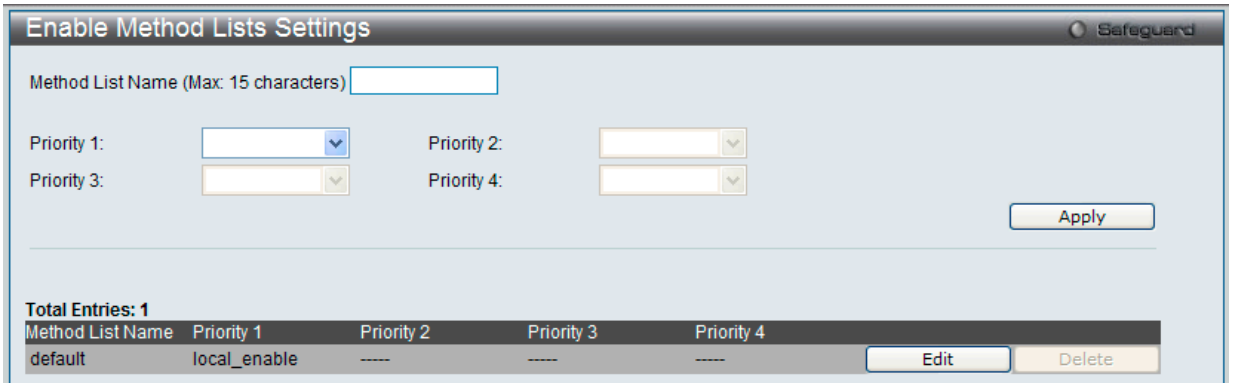


図 12-86 Enable method Lists Settings 画面

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。

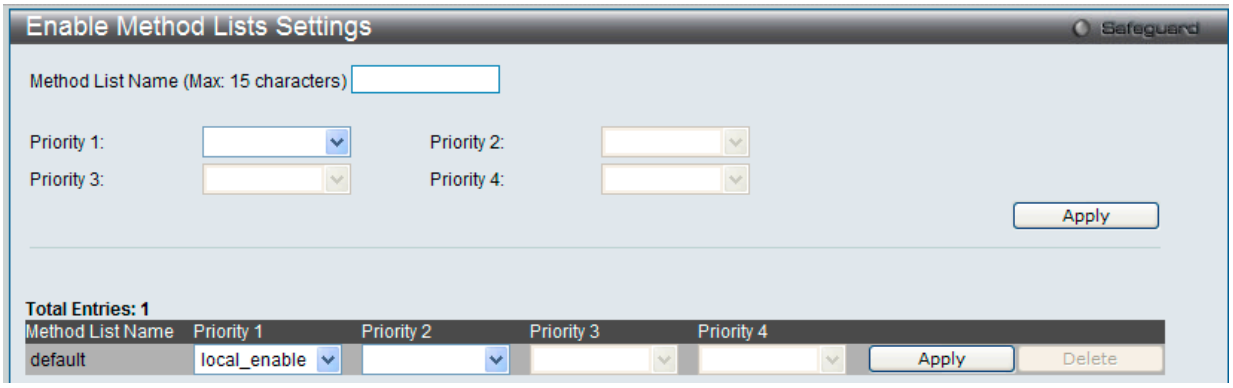


図 12-87 Enable Method Lists 画面 - Edit

2. 項目を編集後、エントリの「Apply」ボタンをクリックします。

以下の項目を使用して、「Enable Method List」の設定を行います。

項目	説明
Method List Name	15 文字までの半角英数字でメソッドリスト名を入力します。
Priority 1, 2, 3, 4	本メソッドリストに追加する認証方法を最大 4 件まで指定します。 • local_enable – スイッチ上のローカル Enable パスワードデータベースを使用してユーザ認証を行います。Local enable password は次セクションの「Local Enable Password Settings（ローカルユーザパスワード設定）」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。

入力後、「Apply」ボタンをクリックします。

Accounting Method Lists Settings（アカウンティングメソッドリスト設定）

スイッチ上でアカウンティングメソッドリストの作成を行います。

Security > Access Authentication Control > Accounting method Lists Settings の順にメニューをクリックし、以下の画面を表示します。

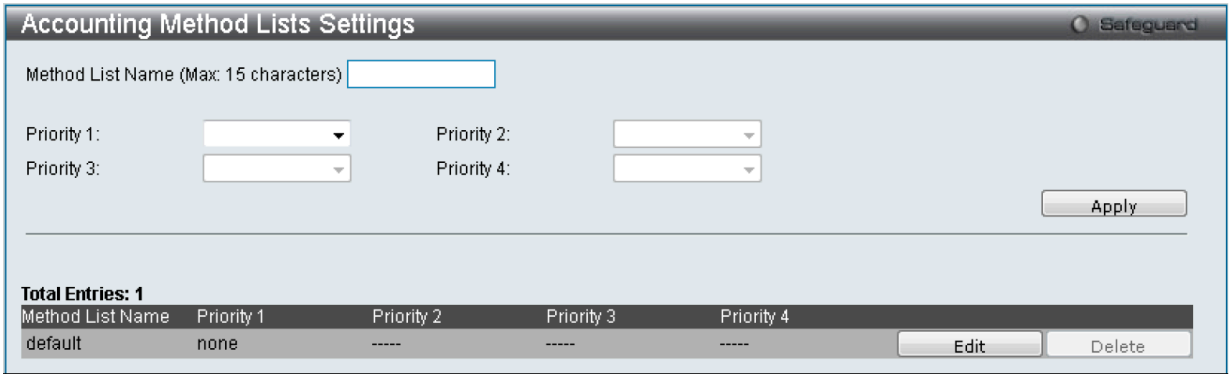


図 12-88　Accounting method Lists Settings 画面

以下の項目を使用して、「Accounting Method List」の設定を行います。

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。 • none - アカウンティングを必要としないパラメータです。 • 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。

入力後、「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）

「Enable Admin」コマンド用の Local Enable Password を設定します。

ユーザがその権限をユーザレベルから管理者レベルに変更する際の認証方法に、「local_enable」を選択している場合、本画面でスイッチに登録したパスワードの入力が要求されます。

Security > Access Authentication Control > Local Enable Password Settings の順にメニューをクリックし、以下の画面を表示します。

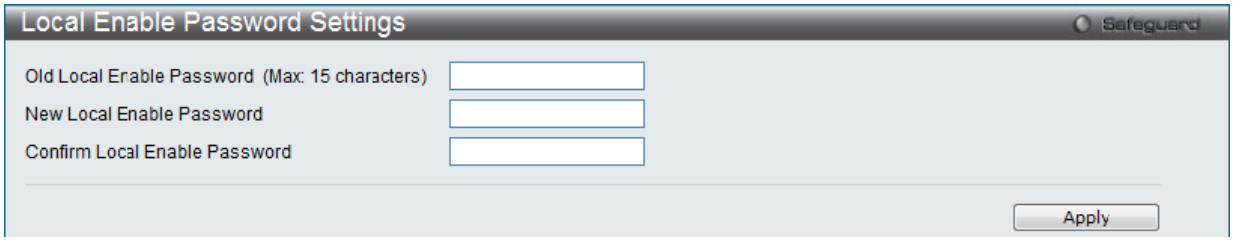


図 12-89　Local Enable Password Settings 画面

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	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。

SSL（Secure Socket Layer）

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/v2/v3 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。

「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。

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。

SSL Settings（SSL 設定）

SSL 設定を行います。

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

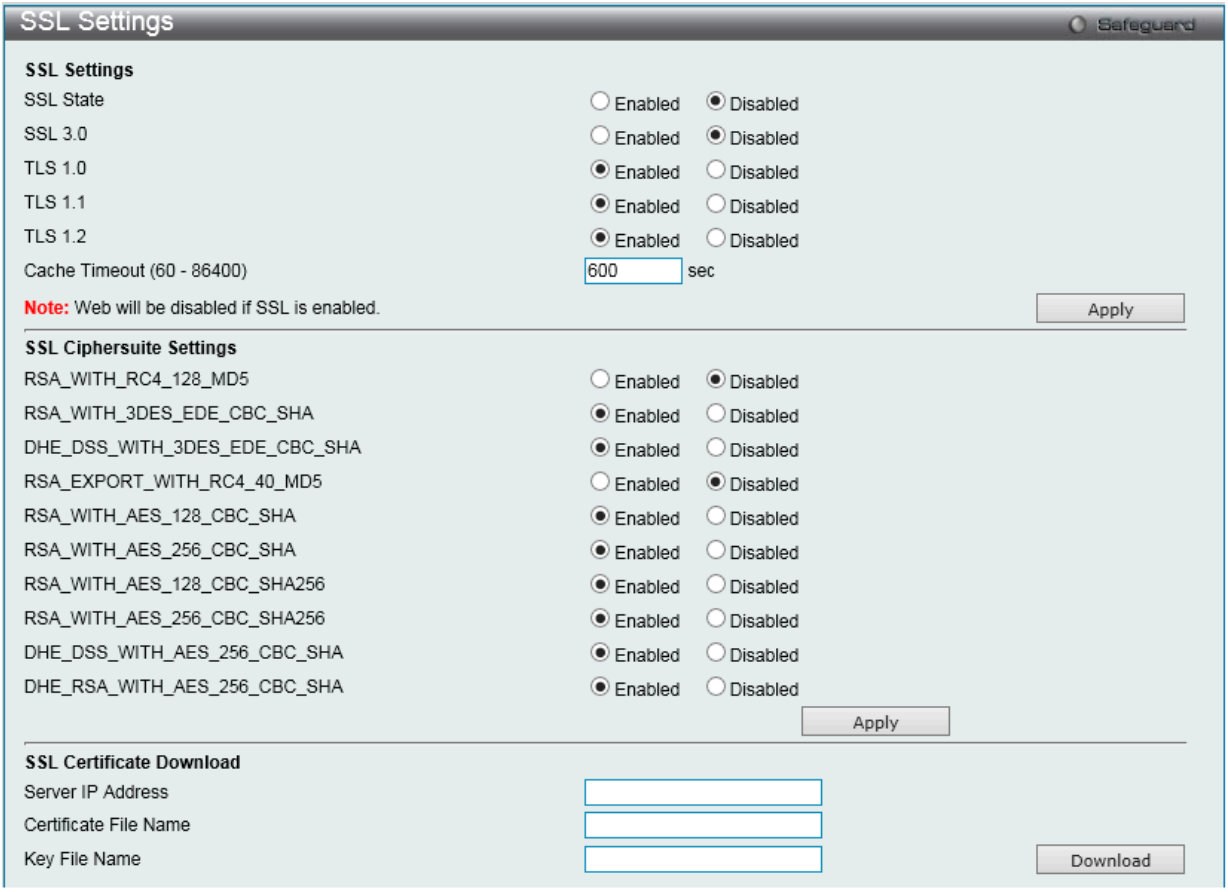


図 12-90　SSL Settings 画面

スイッチに SSL 機能を設定する

「SSL Settings」セクションで項目を設定し、「Apply」ボタンをクリックします。

スイッチに SSL 暗号スイート機能を設定する

「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 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。
SSL 3.0/TLS1.0/TLS1.1/TLS1.2	SSL/TLS の各バージョンについて「Enabled」（有効）、「Disabled」（無効）を指定します。
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	
SSL Ciphersuite Settings	各暗号スイートの「Enabled」（有効）、「Disabled」（無効）を指定します。
SSL Certificate Download	
Server IP Address	証明書のファイルがある TFTP サーバの IPv4 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。コマンドラインインタフェースを使用して設定します。

注意 SSL 機能が有効になると Web ベースマネジメントは無効になります。再度本スイッチにログオンするには Web ブラウザのアドレスフィールドに URL の最初が https:// で始まるアドレスを指定してください。他のアドレスを入力するとエラーとなり、認証はされません。

SSL Certification Settings（SSL 証明書設定）

SSL 証明書の設定を行います。

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

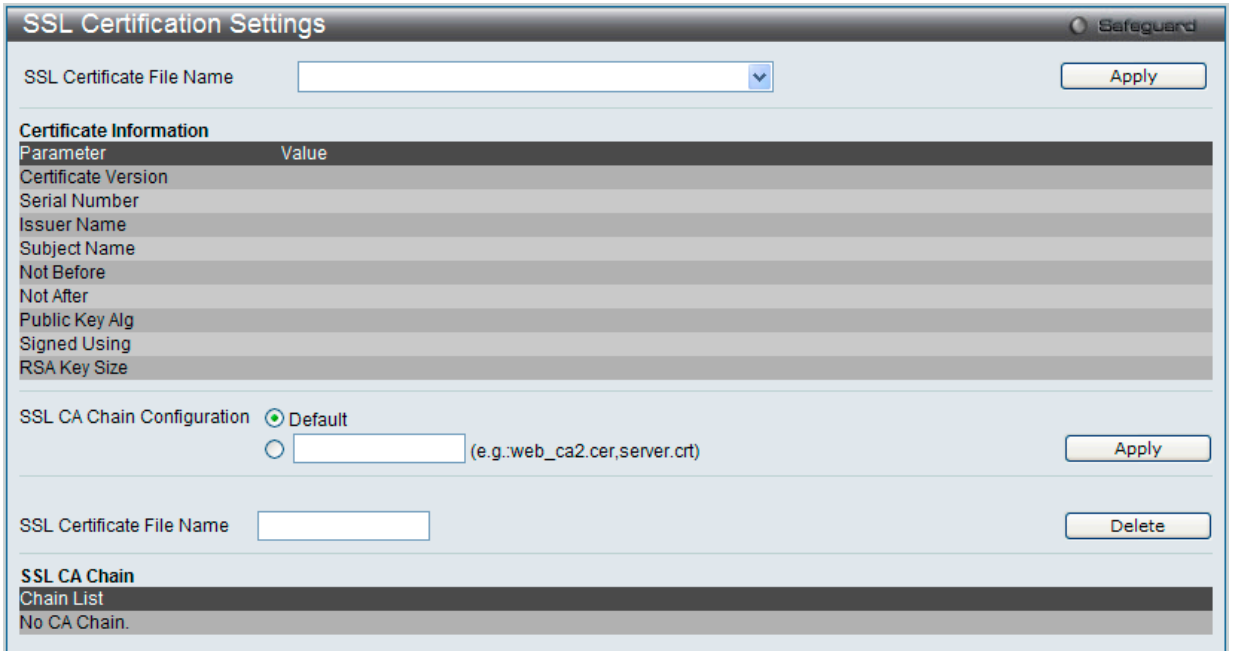


図 12-91　SSL Certification Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
SSL Certification File Name	プルダウンメニューを使用して、SSL 証明書名を選択します。
SSL CA Chain Configuration	スイッチにおける証明書のチェーンを入力します。「Default」ボタンをクリックすると、実装されている証明書を使用します。
SSL Certificate File Name	削除する SSL 証明書ファイル名を入力します。

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。

「Delete」ボタンをクリックして、指定エントリを削除します。

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. **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 Mode」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 Authmode 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 Configuration」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）

SSH サーバの設定および設定内容の確認に使用します。

Security > SSH > SSH Settings の順にメニューをクリックします。

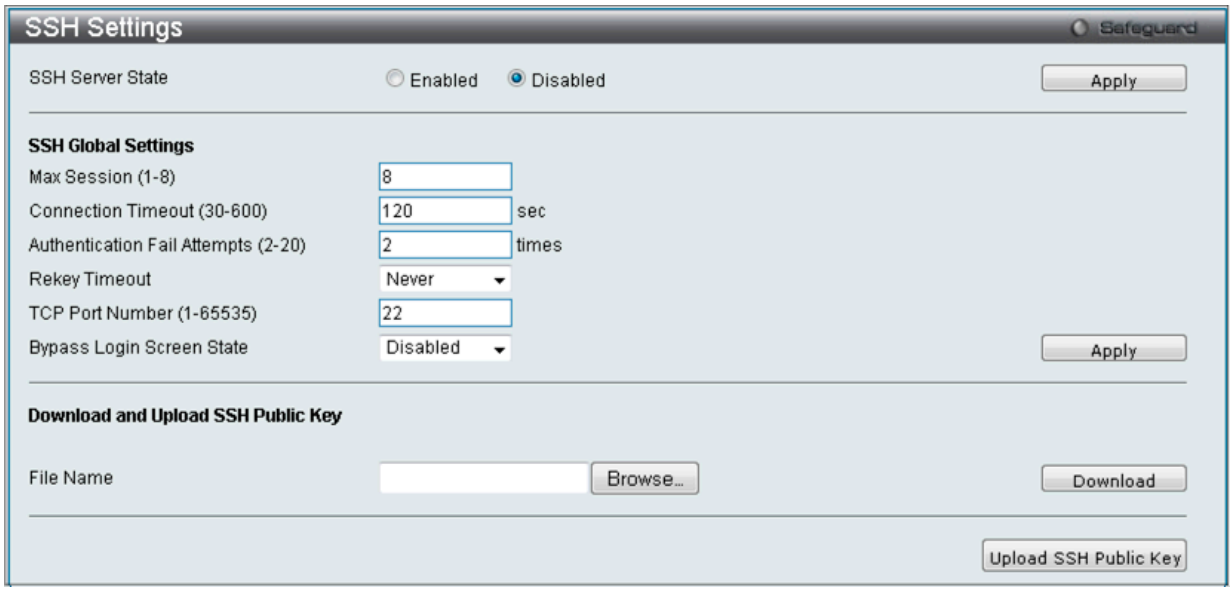


図 12-92 SSH Settings 画面

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 (30-600)	接続のタイムアウト時間を指定します。30 から 600（秒）が指定できます。初期値は 120（秒）です。
Authentication Fail Attempts (2-20)	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。指定した回数を超えるとスイッチは接続を切り、ユーザは再度スイッチに接続する必要があります。2 から 20 が指定できます。初期値は 2 です。
Rekey Timeout	スイッチが SSH 鍵の再交換を行う間隔をプルダウンメニューから選択します。「Never」、「10 min」、「30 min」、「60 min」です。初期値は「Never」（鍵再交換を行わない）です。
TCP Port Number (1-65535)	SSH クライアントとサーバの通信に使う TCP ポートを設定します。初期値は 22 です。
Bypass Login Screen State	「SSH public key authentication」を使用した後、セカンダリの認証を避けるためにユーザー名 / パスワードのログイン画面へのバイパスを設定します。もしこのログイン方式が設定されると、SSH パブリックキーを使用するログインユーザはログインユーザとしての初期権限レベルのコマンドを直接実行することができます。

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 本項目ではまた、TFTP プロトコルを通してスイッチの「SSH public key」ファイルをクライアントコンピュータにダウンロードできます。「Browse」ボタンをクリックしてキーファイルへのパスを参照、クライアントコンピュータのダウンロード先を指定し、「Download」ボタンでダウンロードを開始します。

注意 「Upload SSH Public Key」をクリックして「SSH public key」を TFTP プロトコル経由でアップロードすることも可能です。

SSH Authentication Method and Algorithm Settings（SSH 認証方式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 3 つの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 method and Algorithm Settings の順にメニューをクリックし、以下の画面を表示します。

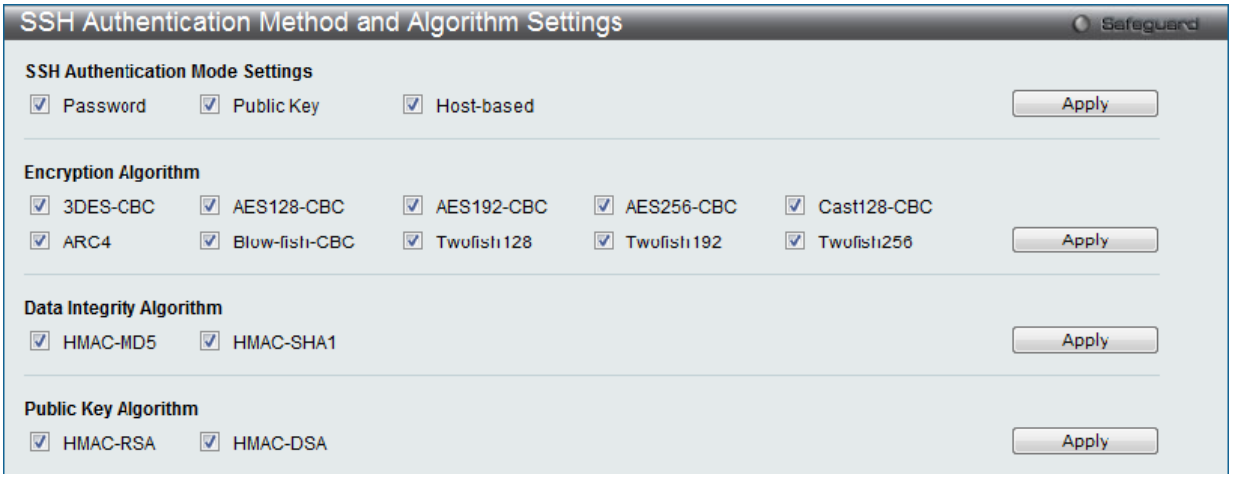


図 12-93　SSH Authentication Method and Algorithm Settings 画面

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、有効にします。初期値は有効です。
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、有効にします。初期値は有効です。
Host Based	認証にホストコンピュータを使用する場合有効にします。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。初期値は有効です。
Encryption Algorithm	
3DES-CBC	CBC 方式で 3DES 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
Blow-fish-CBC	CBC 方式で Blowfish 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
AES128-CBC	CBC 方式で AES128 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
AES192-CBC	CBC 方式で AES192 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
AES256-CBC	CBC 方式で AES256 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
ARC4	ARC4 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
Cast128-CBC	CBC 方式で Cast128 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
Twofish128	Twofish128 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
Twofish192	Twofish192 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
Twofish256	Twofish256 暗号化アルゴリズムを有効または無効にします。初期値は有効です。
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 メカニズムを有効または無効にします。初期値は有効です。
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 メカニズムを有効または無効にします。初期値は有効です。
Public Key Algorithm	
HMAC-RSA	RSA 暗号化アルゴリズムを使用した HMAC メカニズムを有効または無効にします。初期値は有効です。
HMAC-DSA	DSA（デジタル署名）暗号化アルゴリズムを使用した HMAC メカニズムを有効または無効にします。初期値は有効です。

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

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 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。

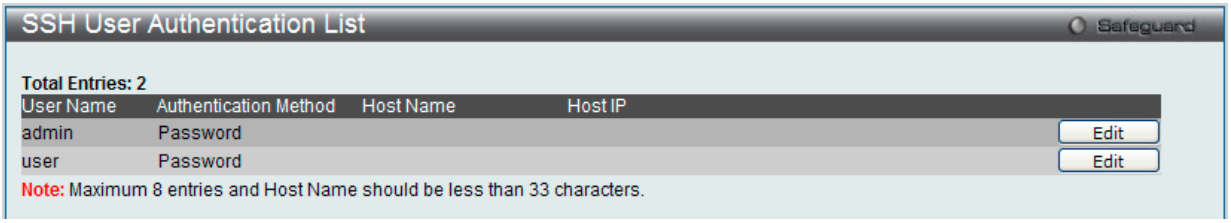


図 12-94 SSH User Authentication List 画面

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。

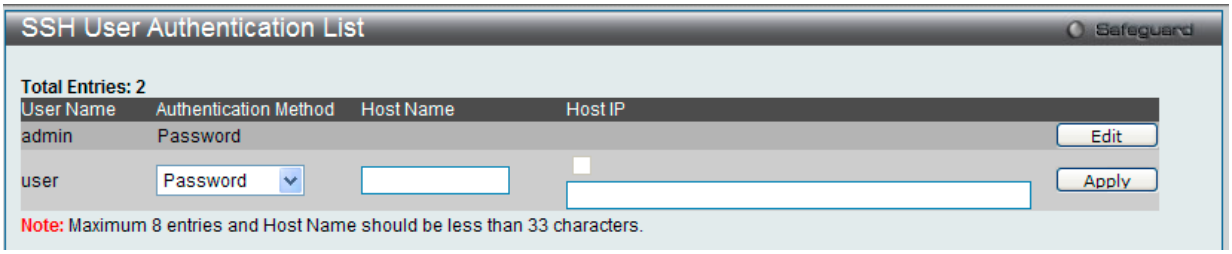


図 12-95 SSH User Authentication Lists 画面 - Edit

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「Authentication Mode」で「Host Based」を選択した場合のみ入力が必要です。

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

注意 SSH User Authentication Mode の項目を設定するためには、事前にユーザアカウントを登録しておく必要があります。

DoS Attack Prevention Settings（DoS 攻撃防止設定）

各 DoS 攻撃に対して防御設定を行います。

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

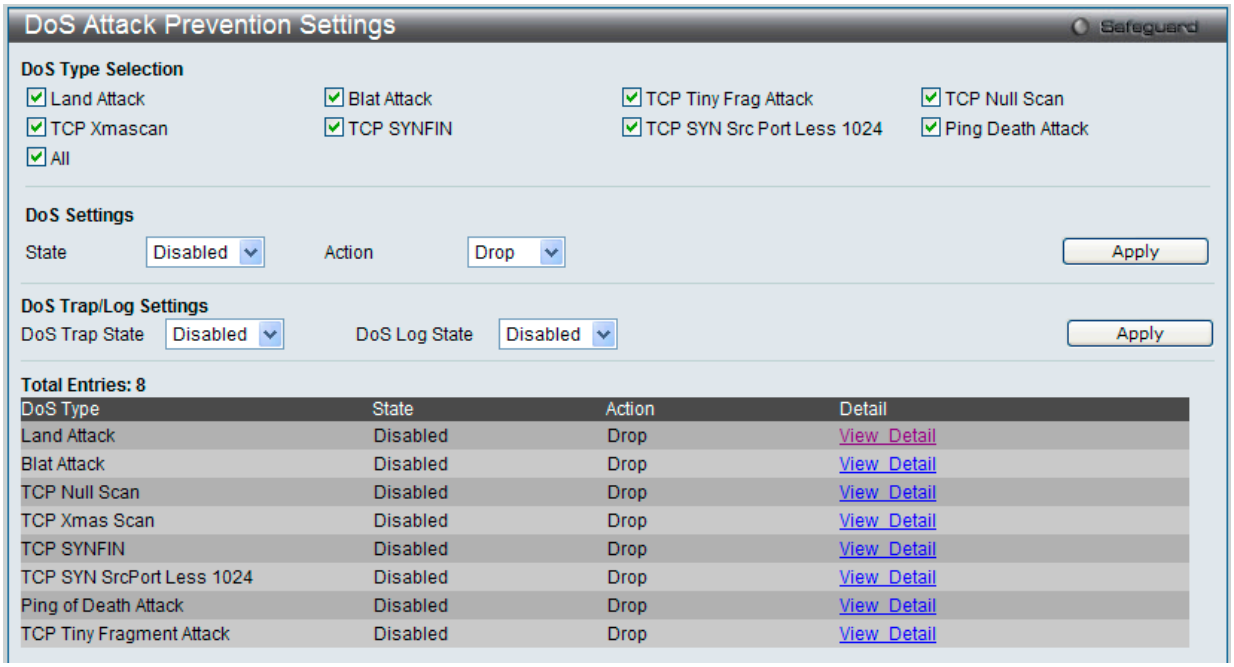


図 12-96 DoS Attack Prevention Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
DoS Type Selection	適切な DoS 攻撃防御のタイプを選択します。 • Land Attack - DoS 攻撃防止タイプに LAND 攻撃を指定します。 • Blat Attack - DoS 攻撃防止タイプに BLAT 攻撃を指定します。 • TCP Tiny Frag Attack - DoS 攻撃防止タイプに TCP Tiny Frag 攻撃を指定します。 • TCP Null Scan - DoS 攻撃防止タイプに TCP Null Scan 攻撃を指定します。 • TCP Xmascan - DoS 攻撃防止タイプに TCP Xmascan 攻撃を指定します。 • TCP SYNFIN - DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。 • TCP SYN Src Port Less 1024 - DoS 攻撃防止タイプに TCP SYN Source Port Less 1024 攻撃を指定します。 • Ping Death Attack - DoS 攻撃防止タイプに Ping Death Attack 攻撃を指定します。 • All - DoS 攻撃防止タイプにすべての攻撃を指定します。
DoS Settings	
State	DoS 攻撃防止の状態を指定します。 • Enabled - DoS 攻撃防止の状態を有効にします。 • Disabled - DoS 攻撃防止の状態を無効にします。
Action	DoS 攻撃防止機能により行われる操作を無効にします。 • Drop - 一致する DoS 攻撃パケットをすべて破棄します。
DoS Trap/Log Settings	
DoS Trap State	本オプションは、DoS 防止トラップ状態を有効または無効にします。
DoS Log State	DoS 防止ログ状態を有効または無効にします。

詳細情報の表示

「DoS Type」の横に表示される「View Detail」リンクをクリックすると、以下の画面が表示されます。

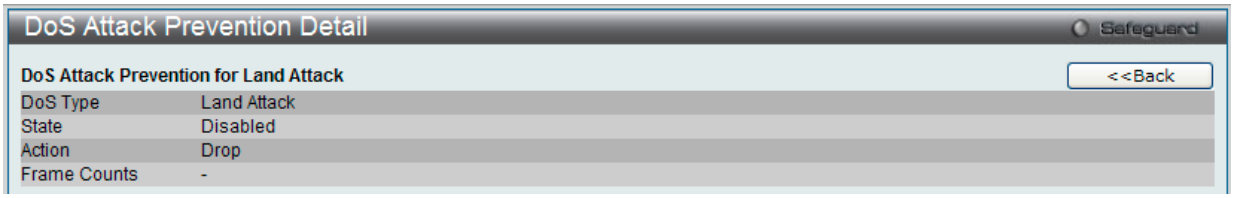


図 12-97 DoS Attack Prevention Detail 画面

「<<Back」をボタンをクリックして前のページに戻ります。

Trusted Host Settings（トラストホスト）

スイッチのリモート管理のために、30 までのトラストホスト IP アドレスもしくは IP レンジを設定して利用することができます。一つ以上のトラストホストが有効化された場合には、スイッチはすぐに特定の IP アドレスもしくはアドレスレンジからのみしかリモートアクセスを受け付けなくなりますので、ご注意ください。この機能を有効化する場合には、現在利用している端末の IP アドレスを必ず最初に入力するようにしてください。

Security > Trusted Host Settings の順にクリックし、以下の画面を表示してトラスト IP アドレスのリストを作成します。

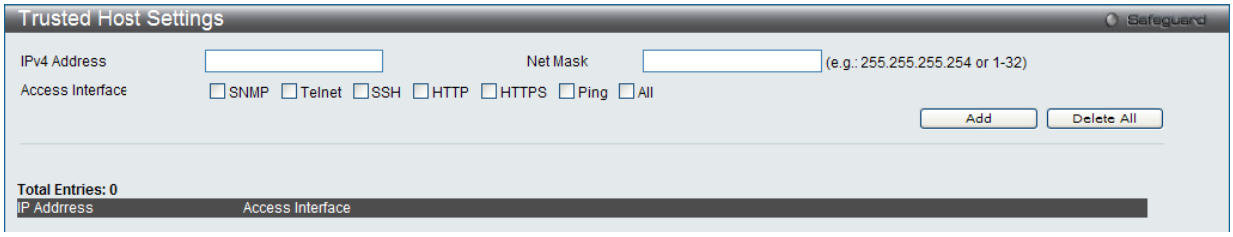


図 12-98 Trusted Host Settings (SI モード) 画面

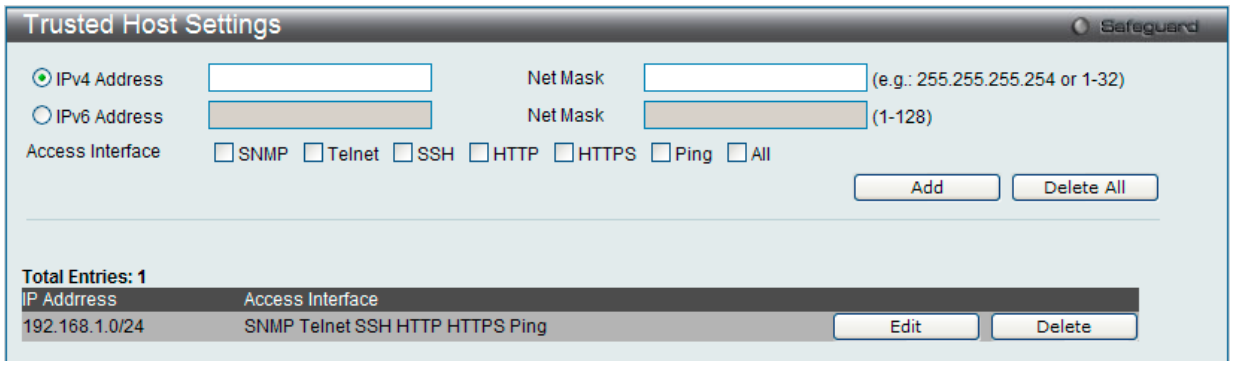


図 12-99 Trusted Host Settings (EI モード) 画面

以下の項目を使用して、設定を行います。

項目	説明
IPv4 Address	トラストホストリストに追加する IPv4 アドレスを入力します。
IPv6 Address (EI モードのみ)	トラストホストリストに追加する IPv6 アドレスを入力します。
Net Mask	トラストホストリストに追加するネットマスクを入力します。
Access Interface	トラストホストに許可するサービスをチェックします。

「Add」をクリックしてトラストホストリストに追加します。

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。

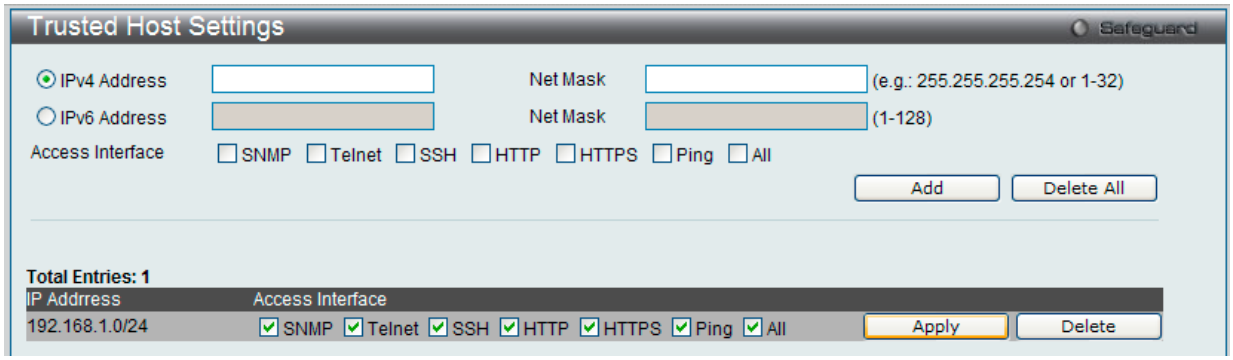


図 12-100 Trusted Host Settings (EI モード) 画面 - Edit

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。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 ブロード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 ブロード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。

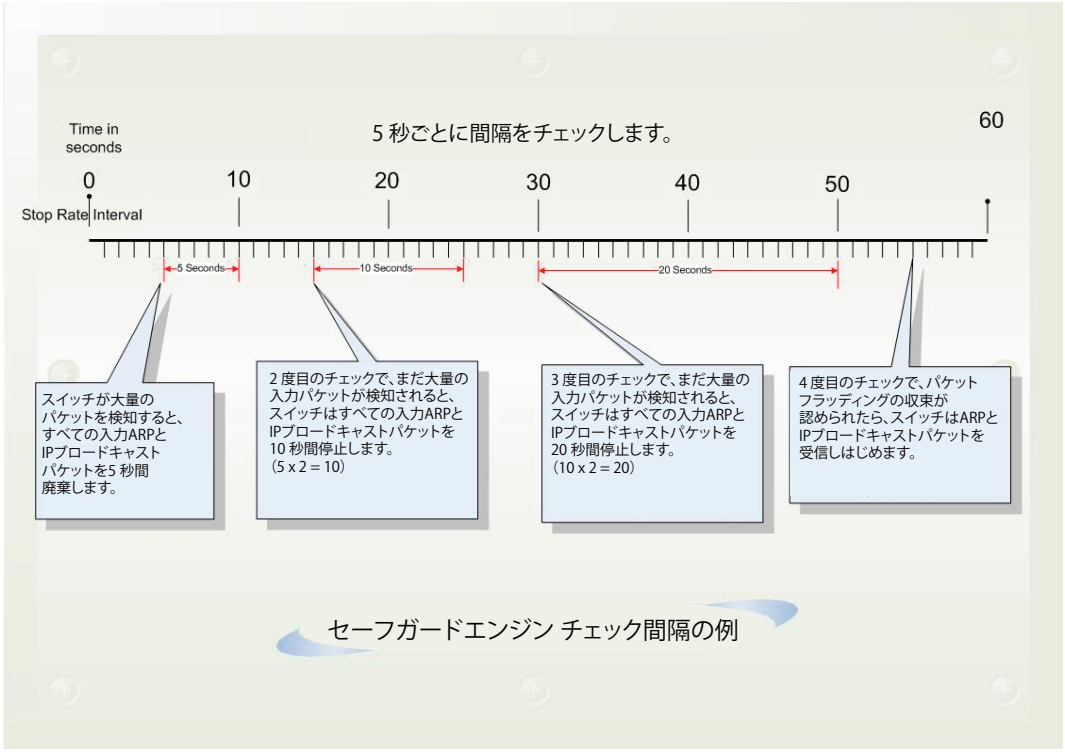


図 12-101 セーフガードエンジンの例

パケットのフラッディングの問題を明らかにする継続したチェック間隔ごとに、スイッチはわずかな受信 ARP および IP ブロードキャストパケットを受信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の破棄間隔を 5 秒に戻してプロセスを再開します。

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 エンジンガードが有効になっている場合、CPU 使用率とトラフィック制限を制御するために、スイッチは FFP（高速フィルタプロセッサ）メータリングテーブルを使用して、さまざまなトラフィックフロー（ARP、IP）に帯域幅を割り当てます。これはネットワークを介してトラフィックをルーティングするスピードが制限される場合があります。

スイッチにセーフガードエンジンの設定を行うためには、**Security > Safeguard Engine Settings** の順にクリックし、以下の画面を表示します。

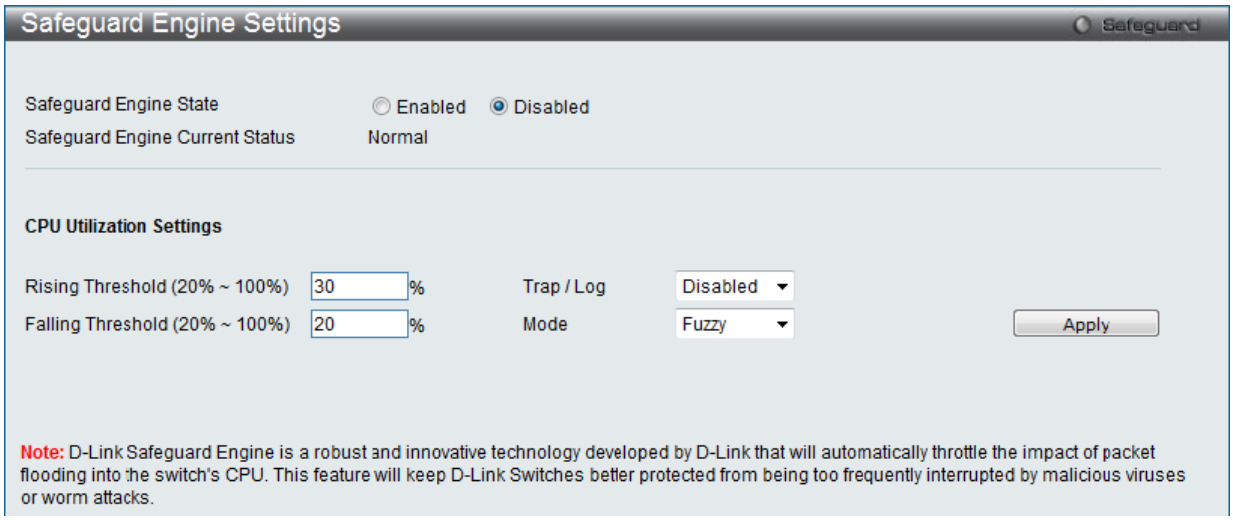


図 12-102 Safeguard Engine Settings 画面

スイッチのセーフガードエンジンを設定するには、「Safeguard Engine」を有効にして、その「State」を有効にします。すると、本画面上部のグレーのバーにある「Safeguard」の文字の隣にあるライトが緑色になります。

スイッチにセーフガードエンジンエンジンを設定するには、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。

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

第 13 章　Network Application（ネットワークアプリケーション）

本章では、DHCP、SNTP などのネットワークアプリケーションに関して設定を行います。

以下は、Network Application のサブメニューです。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明	参照ページ
DHCP（DHCP 設定）	DHCP リレーの設定を行います。以下のメニューがあります。 DHCP Relay（DHCP リレー）、DHCPv6 Relay（DHCPv6 リレー）、DHCP Local Relay Settings（DHCP ローカルリレー設定）	319
PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入設定）（EI モードのみ）	システムは、受信した PPPoE Discovery および Request パケットに対して Circuit ID タグを挿入または削除します。	327
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。	328
SNTP（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）	329
UDP（UDP 設定）	UDP 送信先ポートに応じて、特定のブロードキャストをサーバに送信します。以下のメニューがあります。 UDP Helper（UDP ヘルパー）、UDP Helper Server Settings（UDP ヘルパーサーバ設定）	331
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。	333

DHCP（DHCP 設定）

DHCP Relay（DHCP リレー）

DHCP メッセージが中継される最大のホップ（ルータ）数を Relay Hops Count Limit として指定します。パケットのホップ数が、Relay Hops Count Limit より多いと、そのパケットは廃棄されます。値の範囲は 1-16 で、初期値は 4 です。Relay Time Threshold はスイッチが Boot Request パケットを送出する前に待機する最小の時間（秒）です。パケットの「Seconds」の値が Relay Time Threshold の値より小さいと、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。

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。

Network Application > DHCP > DHCP Relay > DHCP Relay Global Settings の順にメニューをクリックし、以下の画面を表示します。DHCP リレーのグローバル設定を有効にして、設定を行います。

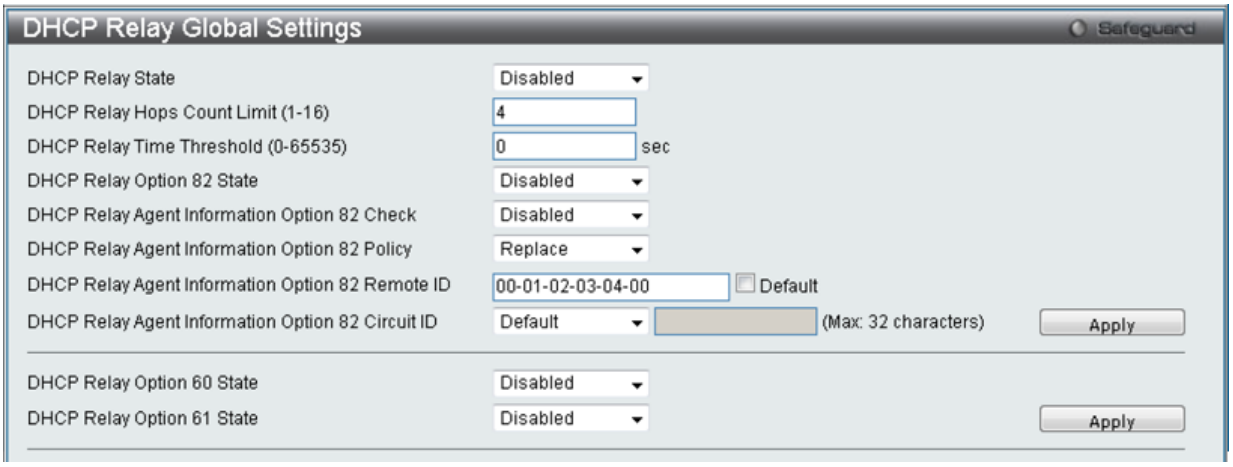


図 13-1　DHCP Relay Global Settings 画面

以下の項目が使用されます。

項目	説明
DHCP Relay State	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定義します。0 が指定されると、スイッチは BOOTP または DHCP パケットの「Seconds」内の値のプロセスを行いません。0 以外の値を指定すると、スイッチはその値を使用し、ホップカウントと併用しながら BOOTP または DHCP パケットの送出を決定します。初期値は 0 です。
DHCP Relay 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。それから、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	リモート ID を入力します。スイッチの MAC アドレスを初期値として使用する場合、「Default」をチェックしてください。
DHCP Relay Agent Information Option 82 Circuit ID	使用する「DHCP relay agent information Option 82 circuit ID」を選択します。 • Default - サーキット ID は元々のフォーマットで使用します。 • User Define - サーキット ID はユーザ定義の文字列を使用します。スペース使用可。 • Vendor1 - サーキット ID は事前に設定済みの文字列を「Alcatel-Lucent」サーバとの通信に使用します。 • Vendor2 - サーキット ID は事前に設定済みの文字列を使用します。 • Vendor4 - サーキット ID は事前に設定済みの文字列を使用します。
DHCP Relay Option 60 State	DHCP Relay Option 60 機能を「Enabled」（有効）/「 Disabled」（無効）にします。 「option 60」が有効の場合、パケットが option60 を保持していないと、リレーサーバは option 60 をベースにした設定がされません。結果リレーサーバは option 61 をベースにするか、各 IPIF 構成サーバとなります。リレーサーバが option 60 または 61 をベースにする場合、IPIF 構成サーバは無視されます。リレーサーバが option 60 または 61 によって設定されない場合、IPIF 構成サーバはリレーサーバを構成するのに使用されます。 enable – DHCP パケットのリレーに伴い DHCP Relay Option 60 state を有効にします。 disable - DHCP Relay Option 60 state を無効にします。
DHCP Relay Option 61 State	DHCP Relay Option 61 機能を「Enabled」（有効）/「 Disabled」（無効）にします。 「option 61」が有効の場合、パケットが option 61 を保持していないと、リレーサーバは option 61 をベースにした設定がされません。リレーサーバが option 60 または 61 をベースにする場合、IPIF 構成サーバは無視されます。リレーサーバが option 60/option 61 によって設定されない場合、IPIF 構成サーバはリレーサーバを構成するのに使用されます。 enable – DHCP パケットのリレーに伴い DHCP Relay Option 61 state を有効にします。 disable - DHCP Relay Option 60 state を無効にします。

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。

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

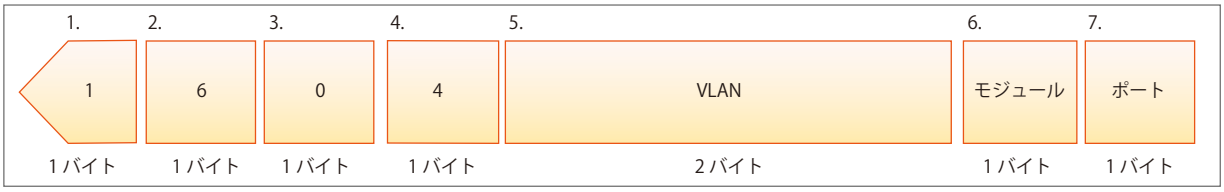


図 13-2　サーキット ID サブオプション形式

1. サブオプションタイプ
2. サブオプションタイプ長
3. Circuit ID タイプ
4. Circuit ID 長
5. VLAN : DHCP クライアントパケットを受信した VLAN
6. モジュール : スタンドアロンスイッチの場合は常に 0。スタッカブルスイッチの場合は Unit ID。
7. ポート : DHCP クライアントパケットを受信したポート番号。ポート番号は 1 から始まります。

リモート ID のサブオプションフォーマット（初期値）

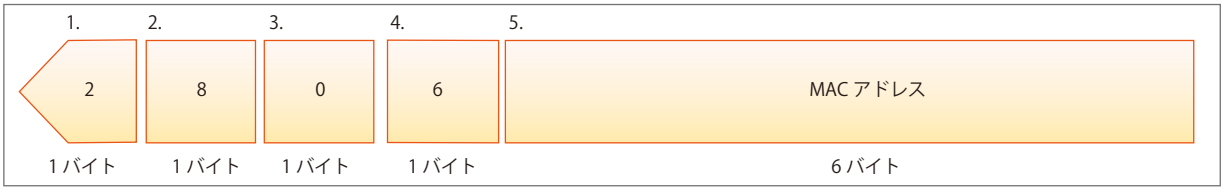


図 13-3　リモート ID サブオプション形式

1. サブオプションタイプ
2. サブオプション長
3. Remote ID タイプ
4. Remote ID 長
5. MAC アドレス : スイッチのシステム MAC アドレス

DHCP Relay Interface Settings（DHCP リレーインタフェース設定）

DHCP/BOOTP 情報をスイッチに中継するために、DHCP サーバの登録を行います。以下の画面を使用して、DHCP サーバに直接接続する、既に登録済みのスイッチの IP インタフェースアドレスを設定します。正しく入力を行い「Apply」ボタンをクリックすると、以下の画面の下部に位置する「DHCP Relay Interface Table」にリスト表示されます。スイッチの 1 つの IP インタフェースに対して 4 件までのサーバ IP アドレスを登録できます。

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

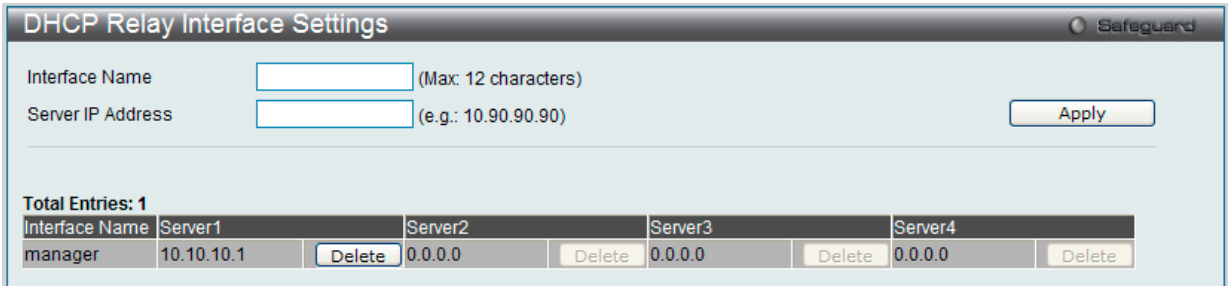


図 13-4　DHCP Relay Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface Name	DHCP サーバに直接接続するスイッチの IP インタフェース
Server IP Address	DHCP サーバの IP アドレス。1 つの IP インタフェースに対して 4 件までの入力が可能です。

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
エントリの削除は「Delete」ボタンをクリックして行います。

DHCP Relay VLAN Settings（DHCP リレー VLAN 設定）

DHCP/BOOTP パケットを転送（リレー）する宛先 IP アドレスを設定します。VLAN 内に IP インタフェースがあり、インタフェースレベルで DHCP サーバとして設定されている場合、その設定の優先度の方が高くなります。この場合 VLAN の DHCP サーバは DHCP パケットを転送しません。

Network Application > DHCP > DHCP Relay > DHCP Relay 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 13-5　DHCP Relay VLAN 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
VID List	設定する VLAN ID リストを入力します。
Server IP Address	DHCP/BOOTP サーバの IP アドレスを入力します。

「Add」ボタンをクリックしてエントリを追加します。

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「VID List」、「Server IP Address」を指定し、「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 Relay Option 60 サーバの初期設定を行います。option 60 に対応したパケットのサーバが見つからない場合、リレーサーバは本項目で設定するリレーサーバになります。

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。

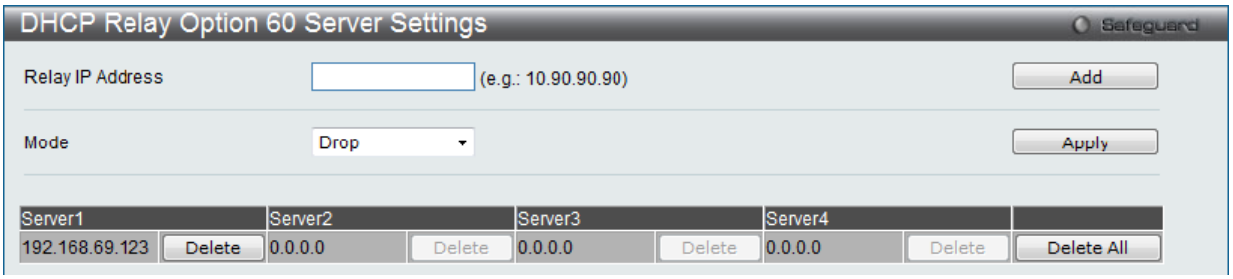


図 13-6　DHCP Relay Option 60 Server Settings 画面

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	初期値のリレーサーバの IP アドレスを入力します。
Mode	プルダウンメニューを使って「Relay」か「Drop」を選択します。「Drop」が選択された場合、ルールに合致しないパケットは破棄されます。「Relay」が選択された場合は、ルールに従いパケットは送信されます。

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。

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。

DHCP Relay Option 60 Settings（DHCP リレーオプション 60 設定）

Option 60 のリレールールの設定を行います。違う文字列が同じリレーサーバに指定されている場合や、同じ文字列が複数のサーバに適用されている場合に、本項目を設定してルールに合致したサーバにパケットを送信します。

Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Settings の順にメニューをクリックし、以下の画面を表示します。

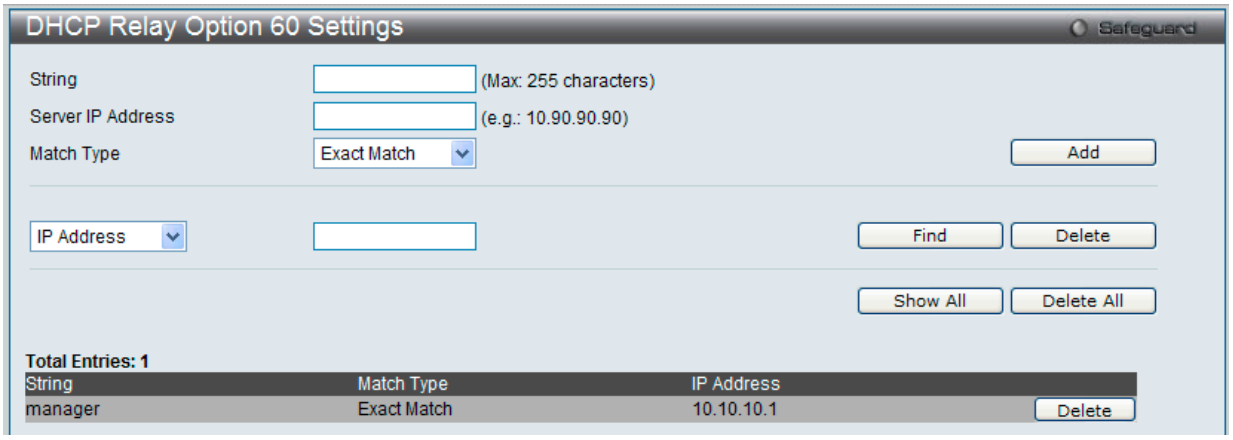


図 13-7　DHCP Relay Option 60 Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
String	文字列を入力します。255 文字までの英数字が使用できます。
Server IP	リレーサーバの IP アドレスを入力します。
Match Type	プルダウンメニューを使って「Exact Match」もしくは「Partial Match」を選択します。 ・Exact Match – パケットの option 60 文字列が指定した文字列と完全に一致した場合に有効です。 ・Partial Match – パケットの option 60 文字列が指定した文字列と部分的に一致した場合に有効です。
IP Address	DHCP リレーオプション 60 の IP アドレスを入力します。
String	DHCP リレーオプション 60 のストリング値を入力します。

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。

エントリの追加
「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

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

エントリの削除
「Delete」ボタンをクリックして、入力した情報に基づいて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 Relay Option 61 Settings（DHCP リレーオプション 61 設定）

Option 61 に基づいたリレーサーバのルールを追加します。ルールは MAC アドレスかユーザ設定の文字列になります。リレーサーバのみが MAC アドレスか文字列で指定することができます。「option 60」「option 61」のどちらも合致した DHCP パケットの設定に基づき、指定の DHCP サーバにアサインされます。いくつかのリレーサーバが option 60 に設定され、1 つだけ option 61 に設定された場合、最終的にリレーサーバは option 61/60 のどちらにも設定されます。

Network Application > DHCP > DHCP Relay > DHCP Relay Option 61 Settings の順にメニューをクリックし、以下の画面を表示します。

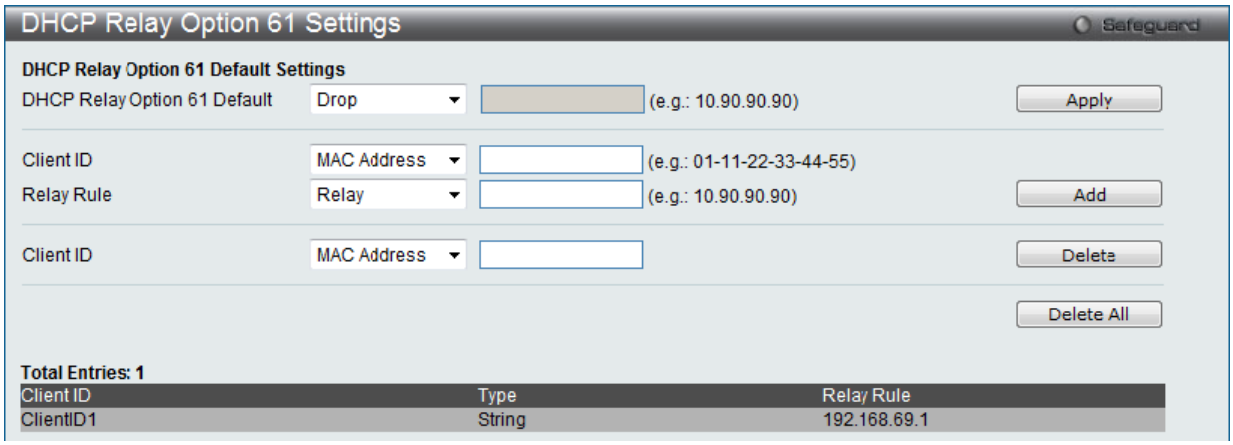


図 13-8　DHCP Relay Option 61 Settings 画面

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	プルダウンメニューを使って「Relay」か「Drop」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	プルダウンメニューを使い「Client ID」の識別方法を「MAC Address」か「String」から選択します。 • MAC Address - クライアントの MAC アドレスを指定します。 • String - クライアント ID を指定します。 上記方法を選択し必要情報を入力欄に入力します。
Relay Rule	プルダウンメニューを使って「Relay」か「Drop」を選択します。「Drop」が選択された場合、ルールに合致しないパケットは破棄されます。「Relay」が選択された場合は、ルールに従いパケットは送信されます。
Client ID	MAC Address - MAC アドレスをクライアントの ID として指定します。 String - ストリングをクライアントの ID として指定します。

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。

エントリの追加
「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

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。

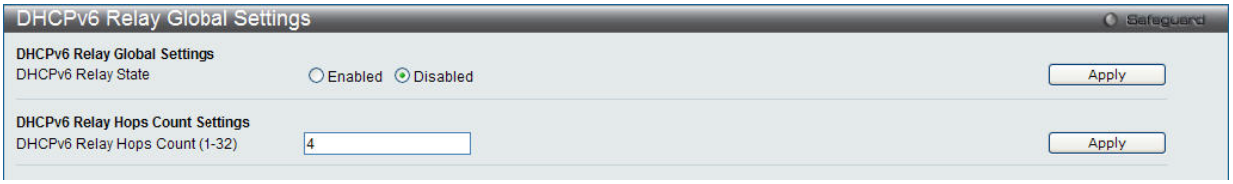


図 13-9　DHCPv6 Relay Global Settings 画面

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	ラジオボタンをクリックして 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、設定を適用します。

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。

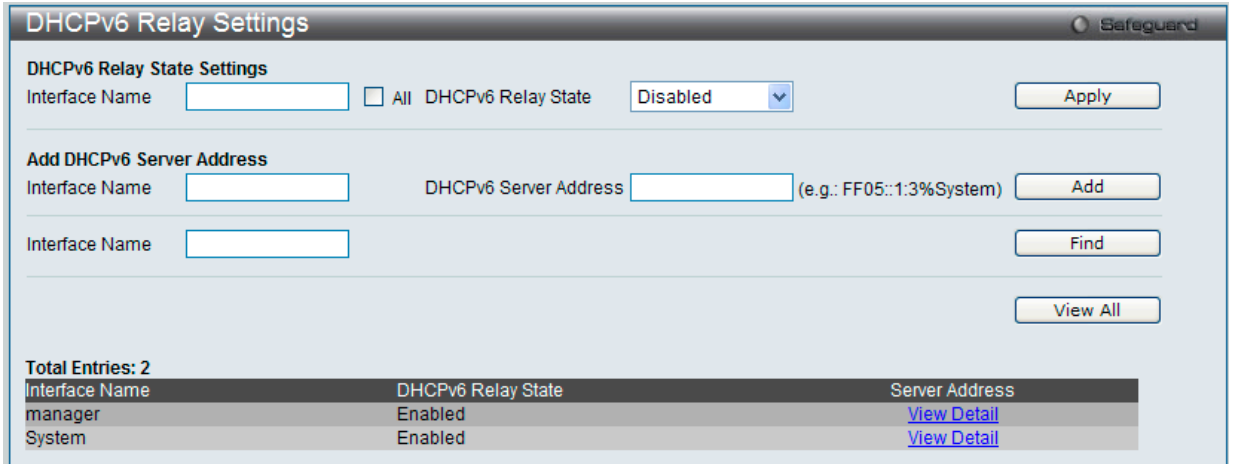


図 13-10　DHCPv6 Relay Settings 画面

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	プルダウンメニューを使用して、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	
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、設定を適用します。
「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。
「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。

エントリの詳細情報の表示

1. 「View Detail」ボタンをクリックすると、以下の画面が表示されます。

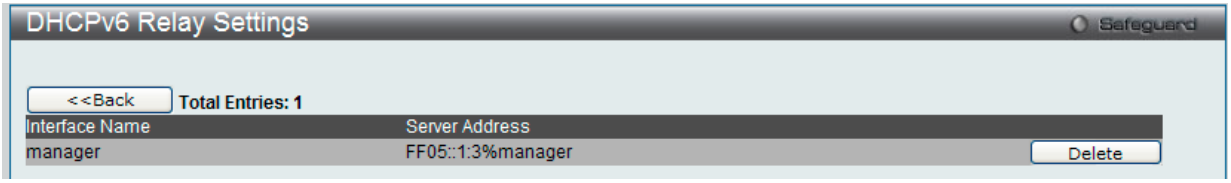


図 13-11 DHCPv6 Relay Settings 画面 - View Detail

DHCPv6 Relay Option 37 Settings（DHCPv6 リレーオプション 37 設定）

スイッチの DHCPv6 リレーエージェント情報を「Option 37」に合致させて設定します。

Network Application > DHCP > DHCPv6 Relay > DHCPv6 Relay Option 37 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。

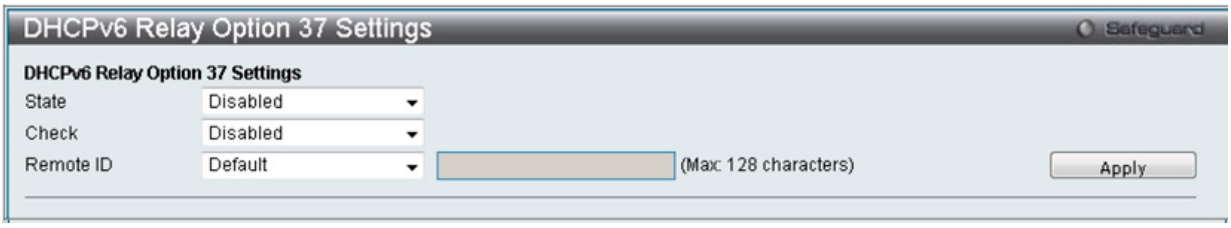


図 13-12 DHCPv6 Relay Option 37 Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
State	有効にすると「DHCP」パケットはサーバにリレーされる前に「Option 37」フィールドに挿入されます。無効にすると DHCP パケットは「Option 37」に挿入されることなく直接サーバへリレーされます。
Check	有効にすると、クライアントサイドからのパケットは「Option 37」フィールドを保持していません。もしクライアントによって「Option 37」フィールドを保持するパケットは破棄されます。
Remote ID	リモート ID のコンテンツを指定します。 • Default - リモート ID には「VLAN ID」「モジュール」「ポート」「システム MAC アドレス」が含まれています。 • CID With User Define - リモート ID には「VLAN ID」「モジュール」「ポート」「ユーザ定義の文字列」が含まれています。 • User Define - リモート ID「ユーザ定義の文字列になります。表示される項目に文字列を入力します。

「Apply」ボタンをクリックし、設定を適用します。

DHCP Local Relay Settings（DHCP ローカルリレー設定）

DHCP ローカルリレーの設定を有効にして、設定を行います。
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 Local Relay Settings の順にクリックし、以下の画面を表示します。

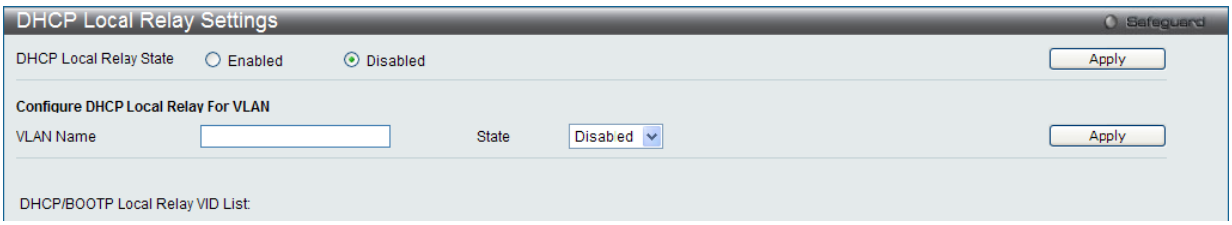


図 13-13 DHCP Local Relay Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCP Local Relay Status	ローカルリレーのグローバルステート機能を「Enable」(有効) または「Disable」(無効) にします。初期値は「Disabled」です。
VLAN Name	ユーザが DHCP ローカルリレーに適用する VLAN を識別するために使用する VLAN 名です。
State	DHCP ローカルリレー設定を「Enable」（有効）または「Disable」（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。

「Apply」ボタンをクリックし、設定を適用します。

PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入設定）（EI モードのみ）

本設定では PPPoE Circuit ID に挿入を行う設定をします。

Network Application > PPPoE Circuit ID Insertion Settings の順にクリックし、以下の画面を表示します。

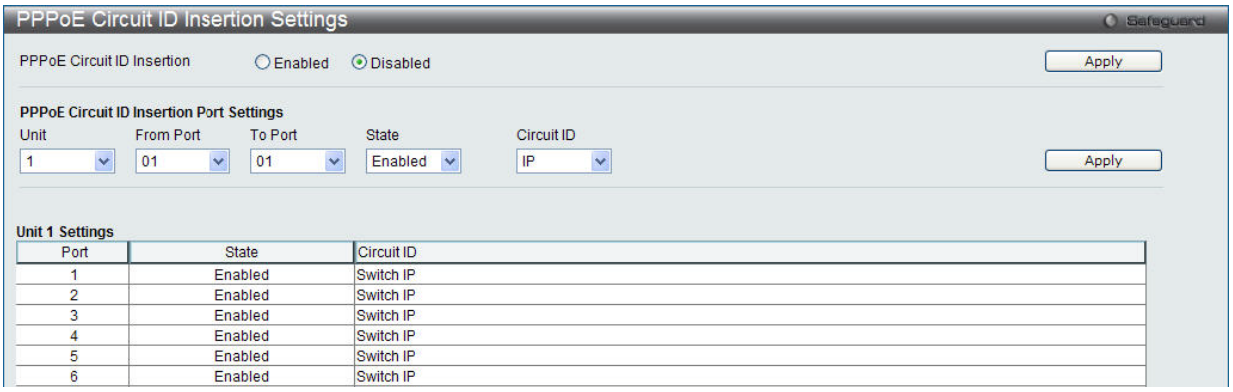


図 13-14　PPPoE Circuit ID Insertion Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
PPPoE Circuit ID Insertion	「PPPoE Circuit ID」挿入の有効 / 無効を設定します。
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートを指定します。
State	指定ポートの「PPPoE Circuit ID」挿入の有効 / 無効を設定します。
Circuit ID	「PPPoE Circuit ID」を選択します。

「Apply」ボタンをクリックし、設定を適用します。

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。

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

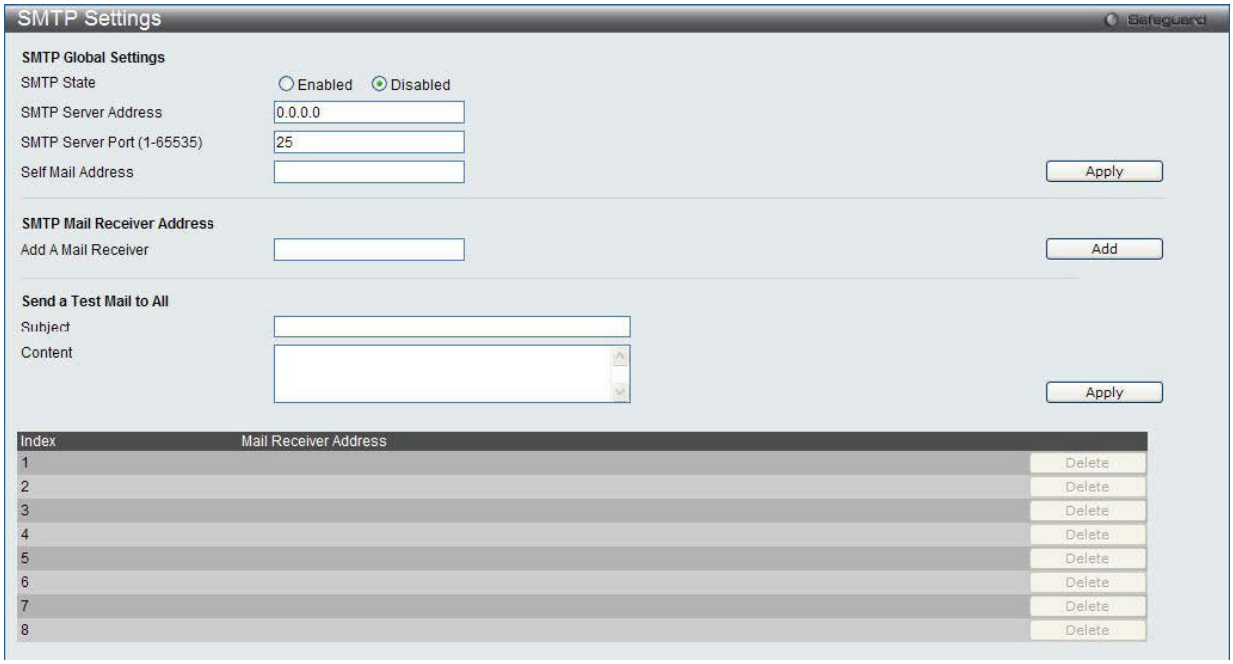


図 13-15　SMTP Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
SMTP Global Settings	
SMTP State	本デバイスの SMTP サービスを「Enabled」（有効）または「Disabled」（無効）にします。
SMTP Server Address	外部デバイスの SMTP サーバの IP アドレスを入力します。これはメールを送信するデバイスとなります。
SMTP Server Port(1-65535)	SMTP サーバに接続するスイッチの仮想ポート番号（1-65535）を入力します。SMTP の一般的なポート番号は 25 です。
Self Mail Address	メールメッセージの送信元 E-mail アドレスを入力します。このアドレスは受信者に送られる E-mail メッセージに送信元として記載されます。このスイッチに設定できるセルフメールアドレスは 1 つだけです。英数 64 文字以内で設定します。
SMTP Mail Receiver Address	
Add A Mail Receiver	E-mail アドレスを入力し、「Add」ボタンをクリックします。8 個までの E-mail アドレスを追加することができます。アドレスを削除する場合は、画面下部にある「Mail Receiver Address」テーブルで削除するエントリの「Delete」ボタンをクリックします。
Send a Test Mail to All	
Subject	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、設定を適用します。

SNTP（SNTP 設定）

SNTP（Simple Network Time Protocol）は、コンピュータのクロックにスイッチを同期させるために使用されます。SNTP 設定には「SNTP Settings」と「Time Zone Settings」メニューがあります。

SNTP Settings（SNTP 設定）

スイッチに時刻を設定します。

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

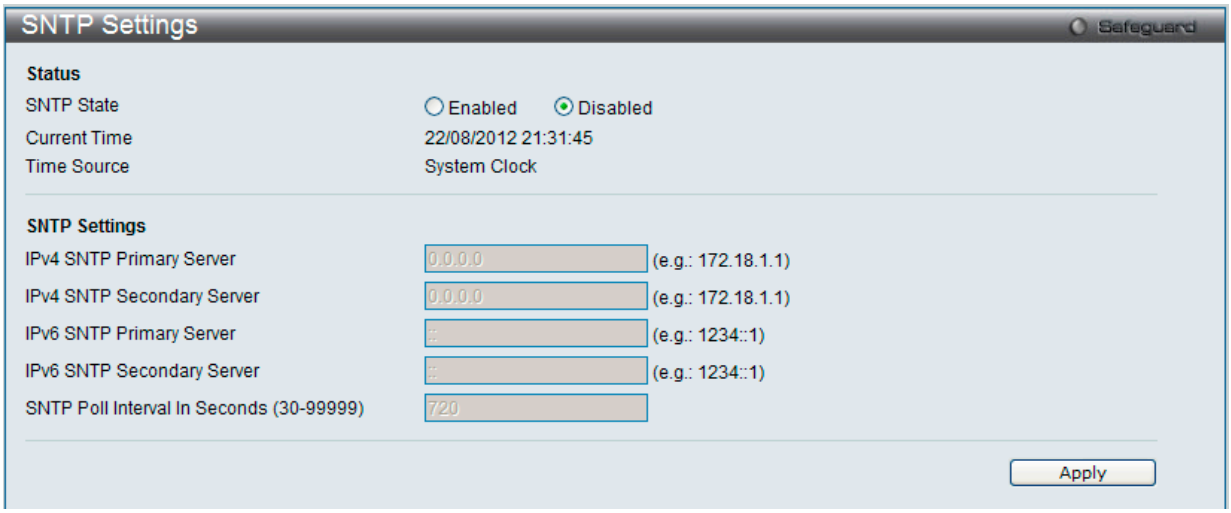


図 13-16　SNTP Settings 画面

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設定します。 • SNTP - システム時刻を SNTP サーバから受信するように設定します。 • System Clock - システム時刻をデバイスに対して直接設定します。
SNTP Settings	
IPv4 SNTP Primary Server	SNTP 情報の取得元であるプライマリサーバの IP アドレスを設定します。
IPv4 SNTP Secondary Server	SNTP 情報の取得元であるセカンダリサーバの IP アドレスを設定します。
IPv6 SNTP Primary Server	SNTP 情報の取得元であるプライマリサーバの IPv6 アドレスを設定します。
IPv6 SNTP Secondary Server	SNTP 情報の取得元であるセカンダリサーバの IPv6 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。

TimeZone Settings（タイムゾーン設定）

以下の画面では、SNTP 用のタイムゾーンとサマータイム（Daylight Saving Time）の設定を行います。

Network Application > SNTP > Time Zone Settings の順にメニューをクリックし、以下の設定画面を表示します。

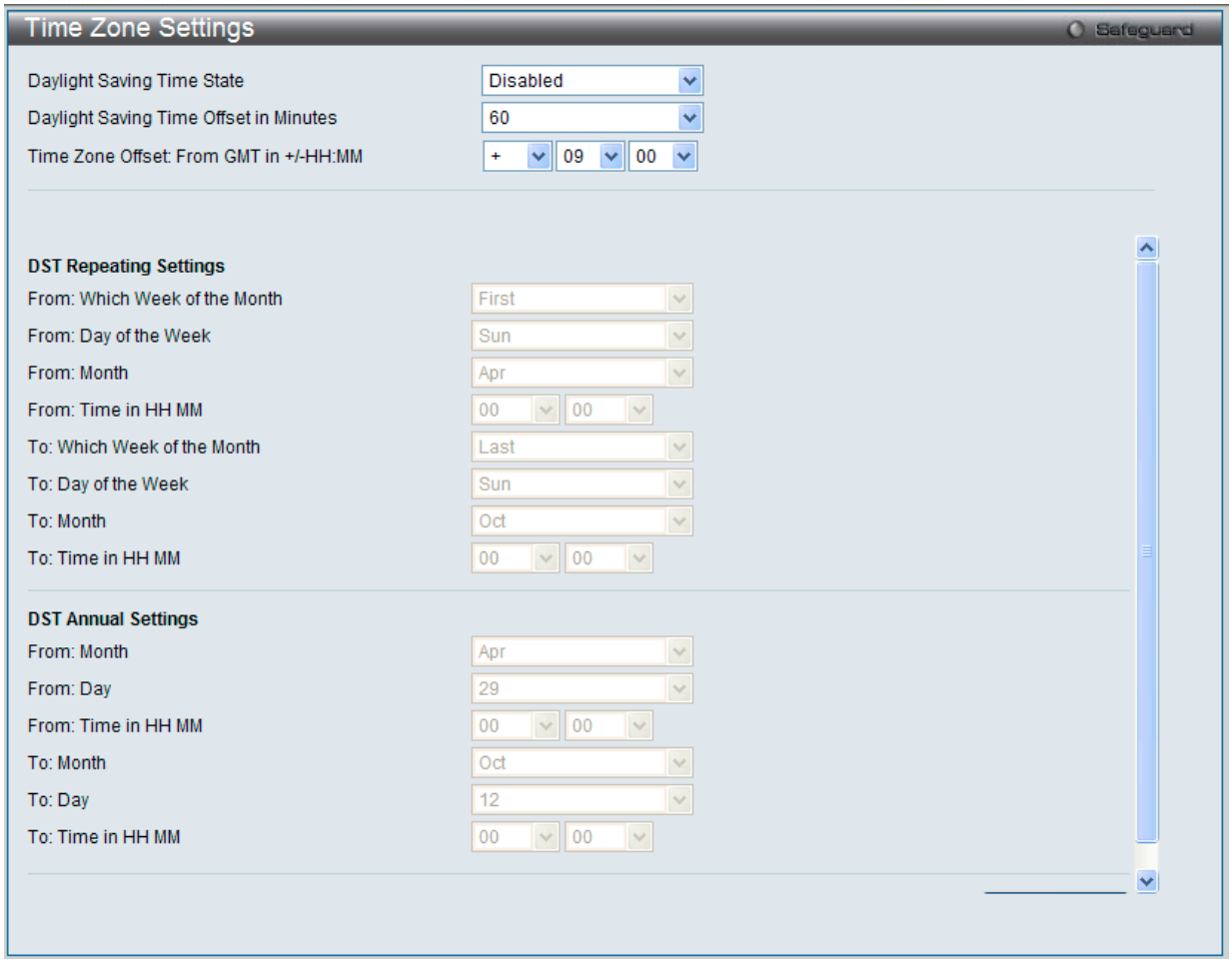


図 13-17　TimeZone Settings 画面

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。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。

項目	説明
To: Which Week Of The Month	月の第何週で DST が終わるかを設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
To: Day Of 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。例 : DST を 4 月 3 日から開始し、10 月 14 日を終了と設定します。	
From: Month	DST が開始する月を指定します。（毎年）
From: Day	DST が開始する日を指定します。（毎年）
From: Time In HH MM	DST が開始する時間を指定します。（毎年）
To: Month	DST が終了する月を指定します。（毎年）
To: Day	DST が終了する日を指定します。（毎年）
To: Time In HH MM	DST が終了する時間を指定します。（毎年）

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

UDP（UDP 設定）

UDP Helper（UDP ヘルパー）

UDP Helper Settings（UDP ヘルパー設定）

UDP ヘルパー設定を行います。

Network Application > UDP > UDP Helper > UDP Helper 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。

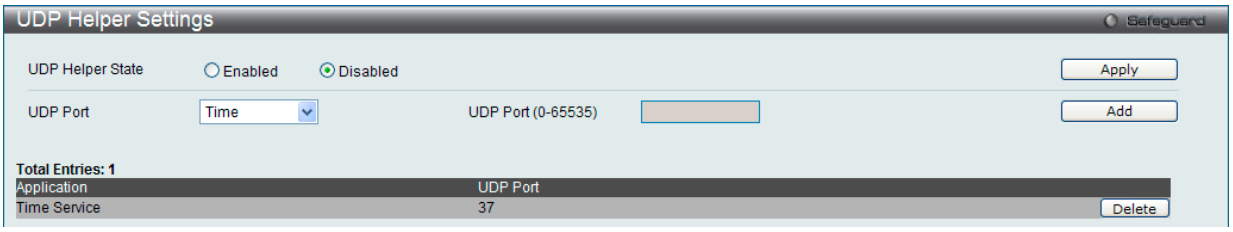


図 13-18 UDP Helper Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
UDP Helper State	UDP ヘルパー機能を有効または無効にします。
UDP Port	プルダウンメニューを使用してポートのタイプを指定します。「UDP Port」を選択した場合、「UDP Port」欄にポートを入力します。
UDP Port (0-65535)	UDP ポートを入力します。UDP Port が前のプルダウンメニューで選択した場合にだけ利用可能です。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの追加

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

UDP Helper Server Settings（UDP ヘルパーサーバ設定）

UDP ヘルパーサーバの設定を行います。

Network Application > UDP > UDP Helper > UDP Helper 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。

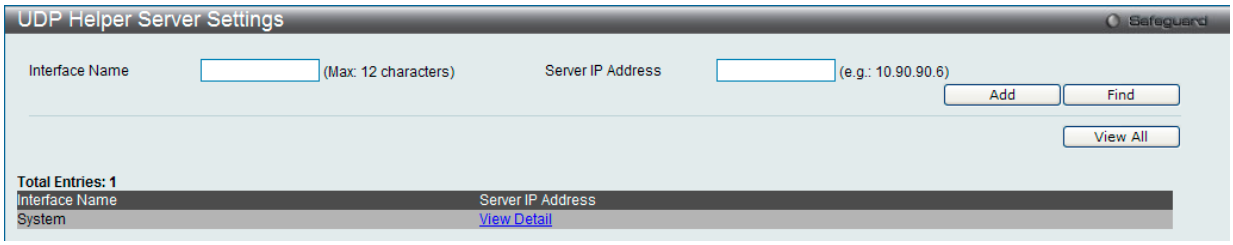


図 13-19 UDP Helper Server Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface Name	UDP ブロードキャストを受信する IP インタフェース名を入力します。
Server IP Address	UDP ヘルパーサーバの 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。

エントリの検出

「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。

「View Detail」リンクをクリックすると、指定エントリに関する詳細情報を表示します。

「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。

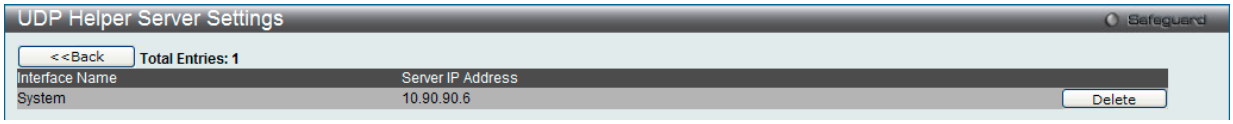


図 13-20 UDP Helper Server Settings - View Detail 画面

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。

「<<Back」をボタンをクリックして前のページに戻ります。

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について

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のアドレスとサイズで保存されます。これは実際のコンフィグレーションファイルの大きさが 40K であっても 2MB の最大ファイル値を確保するため、フラッシュ保存領域は 2MB 分使用されることを意味します。コンフィグレーションファイル番号やファームウェア番号もまた固定されています。コンフィグレーションファイルやファームウェアサイズが固定されたサイズを超えている場合、往々にしてこういった問題が発生します。

本製品のフラッシュファイルシステム

本製品のフラッシュファイルシステムでは、汎用性の高いフラッシュファイル管理を行うことが可能です。すべてのファームウェア、コンフィグレーションファイル、およびシステムログ情報など、全てのファイルが固定されずそのままのファイルサイズでフラッシュに保存されます。フラッシュ容量が十分あれば、ユーザはより多くのコンフィグレーションファイルやファームウェアファイルをダウンロードすることができ、コマンドを使用してフラッシュファイル情報を表示したり、ファイル名を編集、削除することも可能です。加えてランタイムイメージやランニングコンフィグレーションファイルの再起動なども行うことができます。ファイルシステムが崩壊してしまった場合も、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 Z- モデムを使用することができます。

Network Application > Flash File System Settings の順にクリックし、以下の画面を表示します。

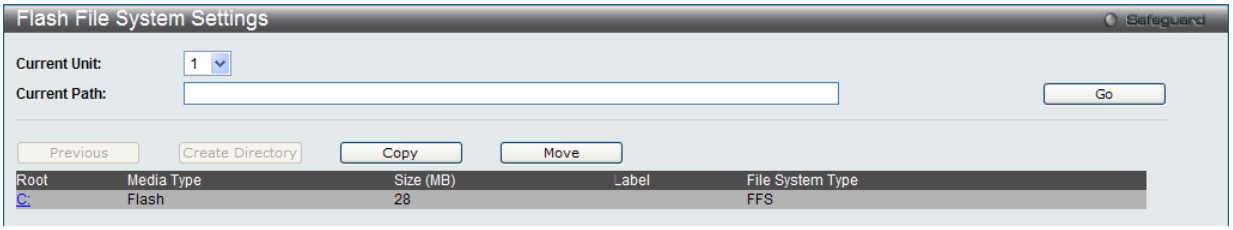


図 13-21　Flash File System Settings 画面

ユニットを選択、パスを入力し「Go」ボタンをクリックして入力したパスへ移動します。「C:」ドライブへ移動する場合は、「C:」をクリックします。「Format」ボタンをクリックすると、リムーバブルストレージドライブを初期化します。

「C:」リンクをクリックした後、次の画面が表示されます。

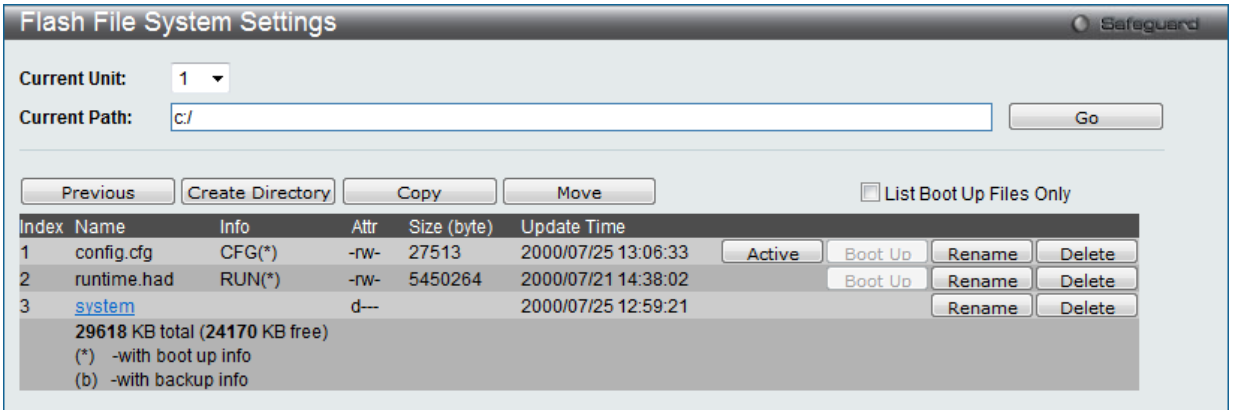


図 13-22　Flash File System Setting – Search for Drive 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Previous	前のページに戻ります。
Create Directory	スイッチのファイルシステムに新しいディレクトリを作成します。
Copy	指定ファイルをスイッチにコピーします。
Move	指定ファイルをスイッチに移動します。
List Boot Up Files Only	チェックすると起動ファイルだけを表示します。
Active	アクティブなランタイムコンフィグレーションとして指定したコンフィグファイルを設定します。
Boot Up	起動用のブートアップイメージとして指定したランタイムイメージを設定します。
Rename	指定ファイルを変更します。
Delete	ファイルシステムから指定ファイルを削除します。

ファイルのコピー

1. 「Copy」ボタンをクリックすると、以下の画面が表示されます。

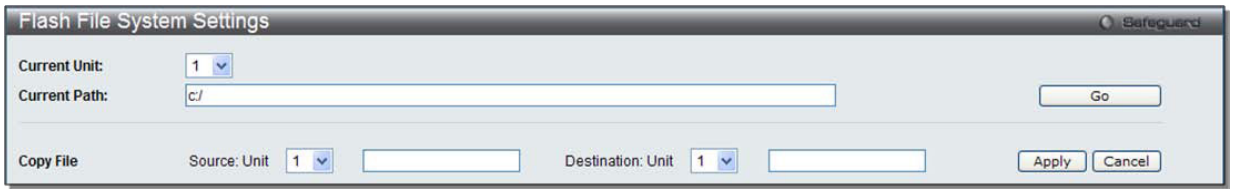


図 13-23 Flash File System Settings 画面 - Copy

2. スイッチのファイルシステムにファイルをコピーする時、送信元（Source）/ 宛先（Destination）のパスを入力します。

3. 「Apply」ボタンをクリックして、コピーを開始します。「Cancel」ボタンをクリックすると処理は破棄されます。

ファイルの移動

1. 「Move」ボタンをクリックすると、以下の画面が表示されます。

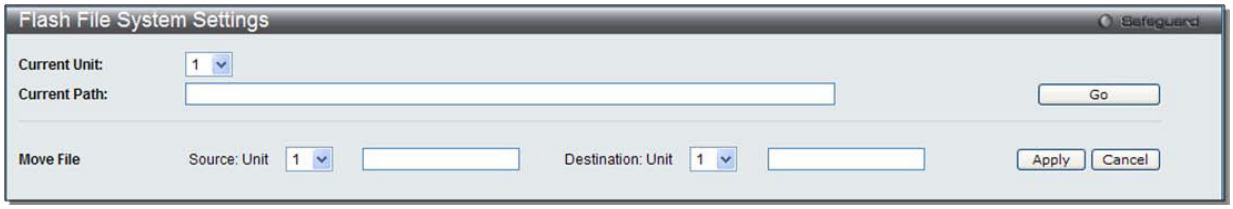


図 13-24 Flash File System Settings - Move 画面

2. ファイルを別の場所に移動する場合、「Source」（送信元）と「Destination」（送信先）のパスを入力します。

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。

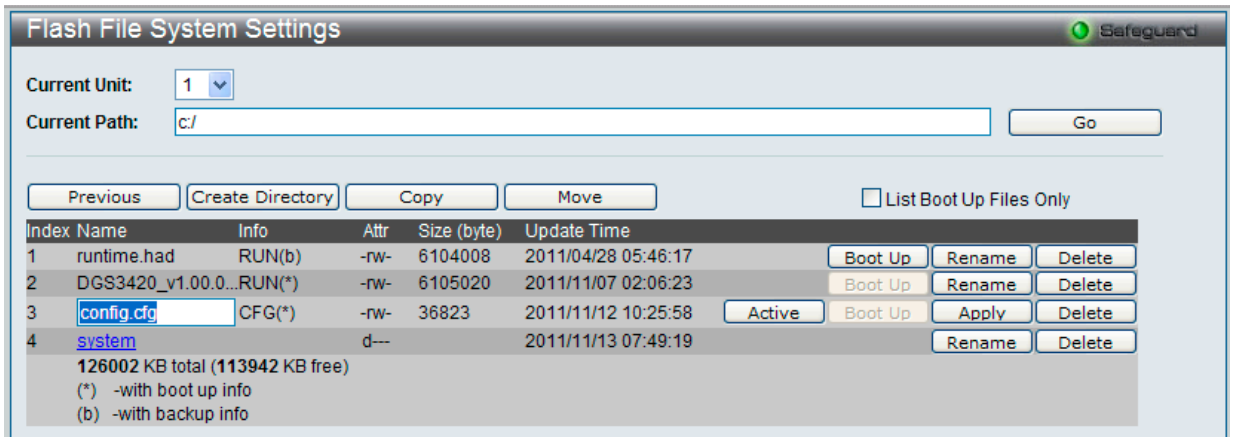


図 13-25 Flash File System Settings 画面 - Rename

2. ファイル名を変更して「Apply」ボタンをクリックします。

第 14 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)

故障診断機能を設定します。

以下は、OAM のサブメニューです。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）（EI モードのみ）	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）	335
Ethernet OAM（イーサネット OAM）（EI モードのみ）	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）	347
DULD Settings（単方向リンク検出設定）（EI モードのみ）	ポートにおいて単方向リンク検出の設定および表示を行います。	350
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。	351

CFM（Connectivity Fault Management : 接続性障害管理）（EI モードのみ）

CFM は IEEE 802.1ag に定義されており、ネットワークにおける接続性故障の検出、隔離、およびレポートを行う標準規格です。CFM は サービスインスタンスごとの End-to-End の OAM（Operations : 操作、Administration : 管理、および Maintenance : メンテナンス）のための機能です。802.1ag によって定義されるように、CFM 機能にはパスの発見、障害検出、故障検証、分離、および故障通知があります。

イーサネット CFM フレームには、特別なイーサネットタイプ（0x8902）があります。すべての CFM メッセージは VLAN ベースごとにメンテナンスドメインに制限されます。CFM フレームペイロードの固有のユニークな OpCode によって識別される様々なメッセージタイプがあります。

CFM メッセージタイプには Continuity Check Message（CCM: 連続性チェックメッセージ）、Loopback Message と Response（LBM: ループバックメッセージ、LBR: ループバックレスポンス）、および Link Trace Message と Response（LTM: リンクトレースメッセージ、LTR: リンクトレースレスポンス）が含まれます。

CFM Settings（CFM 設定）

CFM 機能を設定します。

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

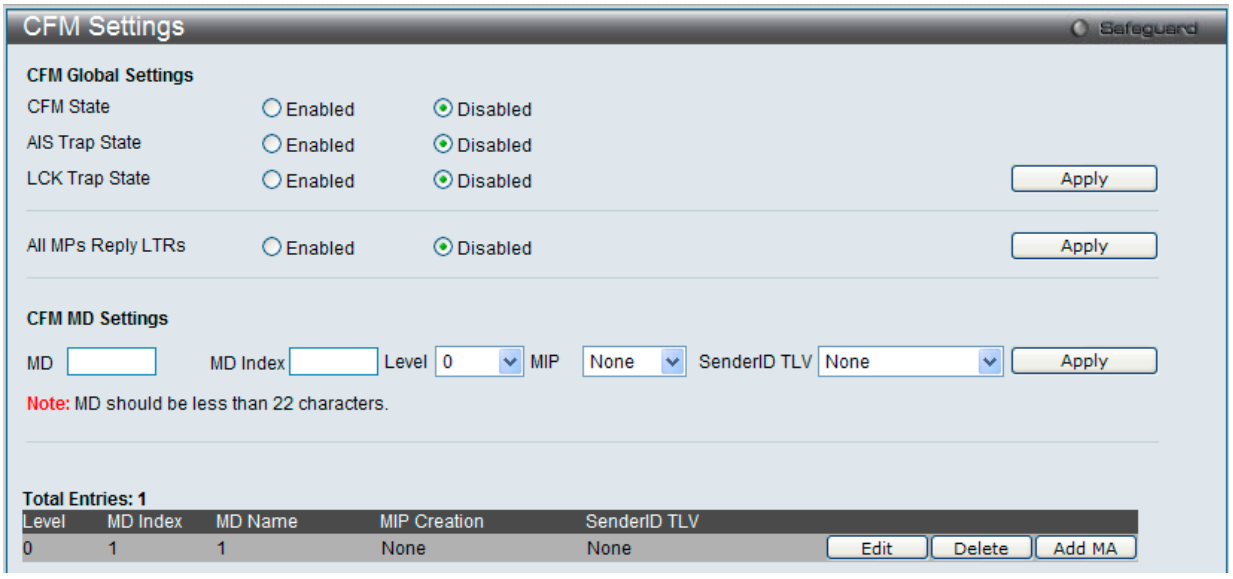


図 14-1　CFM Settings 画面

以下の項目を設定できます。

項目	説明
CFM State	CFM 機能を有効または無効にします。
AIS Trap State	AIS トラップ状態を有効または無効にします。
LCK Trap State	LCK トラップ状態を有効または無効にします。
All MPs Reply LTRs	Link Trace Reply（LTR）メッセージに応答するために、すべての MP（メンテナンスポイント）を有効または無効にします。
CFM MD Settings	
MD	メンテナンスドメインの名称を入力します。22 文字内で指定します。
MD Index	使用するメンテナンスドメインのインデックスを指定します。
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。

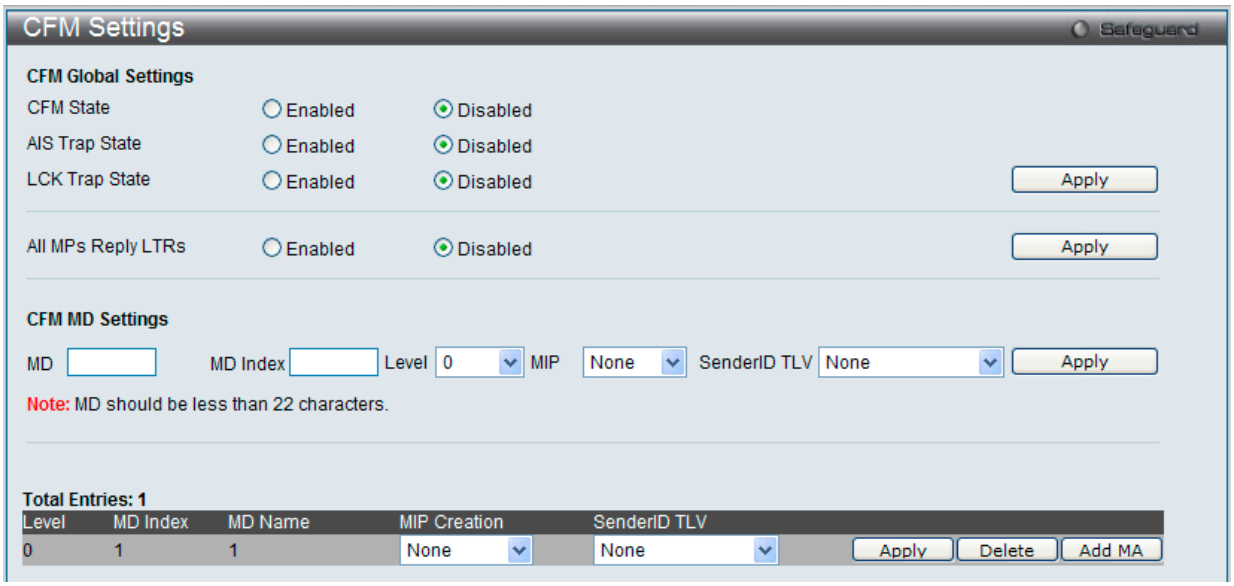


図 14-2　CFM Settings 画面 - Edit

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　MD 名は 22 文字未満とします。

CFM メンテナンスアソシエーション（MA）設定

メンテナンスアソシエーションを設定します。

OAM > CFM > CFM Settings 画面で「Add MA」ボタンをクリックし、以下の画面を表示します。

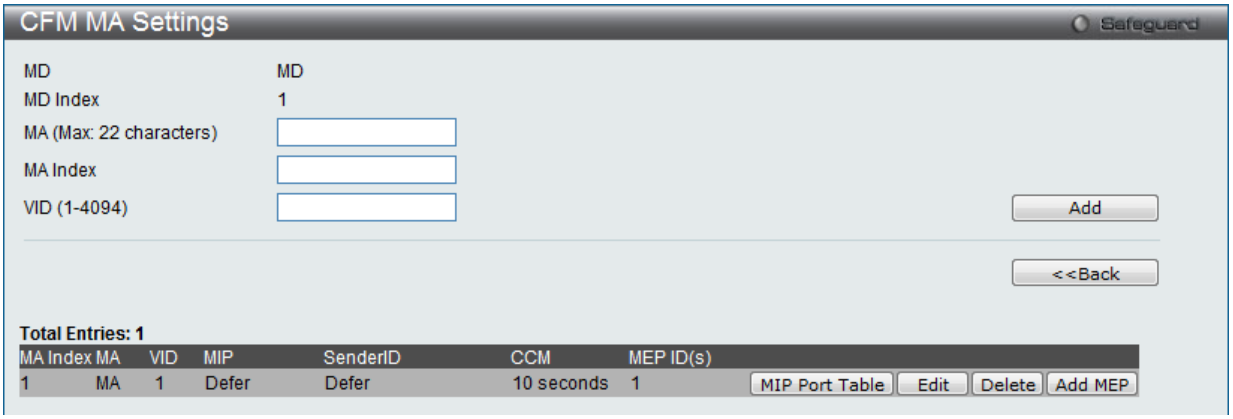


図 14-3　CFM MA Settings 画面

以下の項目が使用できます。

項目	説明
MA	メンテナンスアソシエーションの名称を入力します。
MA Index	メンテナンスアソシエーションのインデックスを入力します。
VID (1-4094)	VLAN 識別子。異なる MA は異なる VLAN に関連付ける必要があります。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。
「MIP Port Table」ボタンをクリックして、CFM MIP Table を参照します。
「Add MEP」ボタンをクリックして、MEP（Maintenance End Point）エントリを追加します。

エントリの削除
テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。

エントリの追加
項目入力後、「Add」ボタンをクリックします。

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。

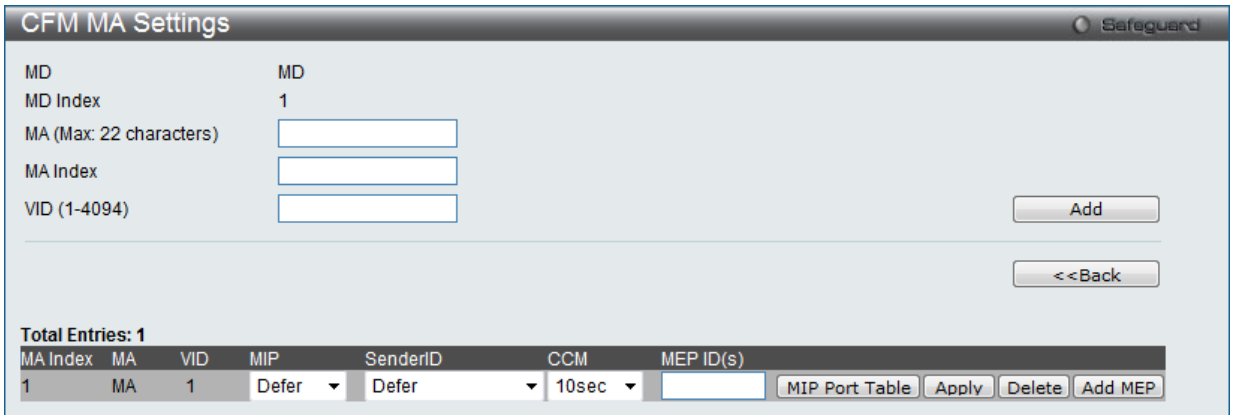


図 14-4　CFM MA Settings 画面 - Edit

以下の項目が使用できます。

項目	説明
MA	メンテナンスアソシエーションの名称を入力します。
MA Index	メンテナンスアソシエーションの名称を入力します。
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。
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。 • 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 MEP」ボタンをクリックし、以下の画面を表示します。

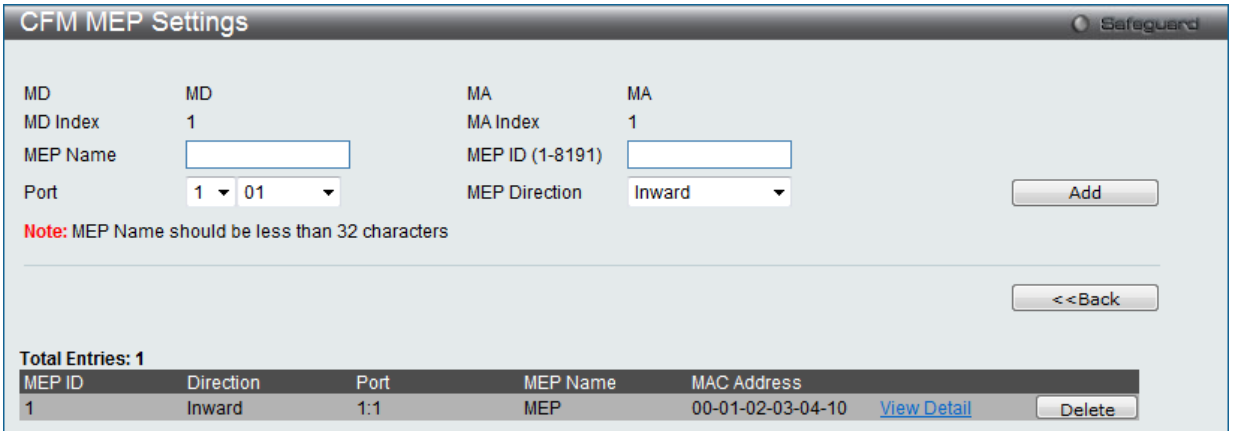


図 14-5　FM MEP Settings -Add 画面

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 (1-8191)	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。

注意　MEP 名は 32 文字以下である必要があります。

MIP ポートテーブルの参照

MIP ポートテーブルを参照します。

OAM > CFM > CFM Settings 画面で「MIP Port Table」ボタンをクリックします。

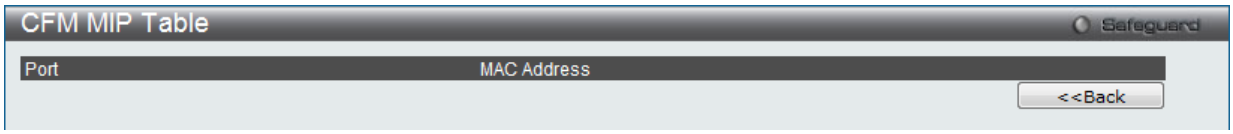


図 14-6　CFM MIP Table 画面

MEP エントリに関する詳細情報の参照

「View Detail」ボタンをクリックし、以下の画面を表示します。

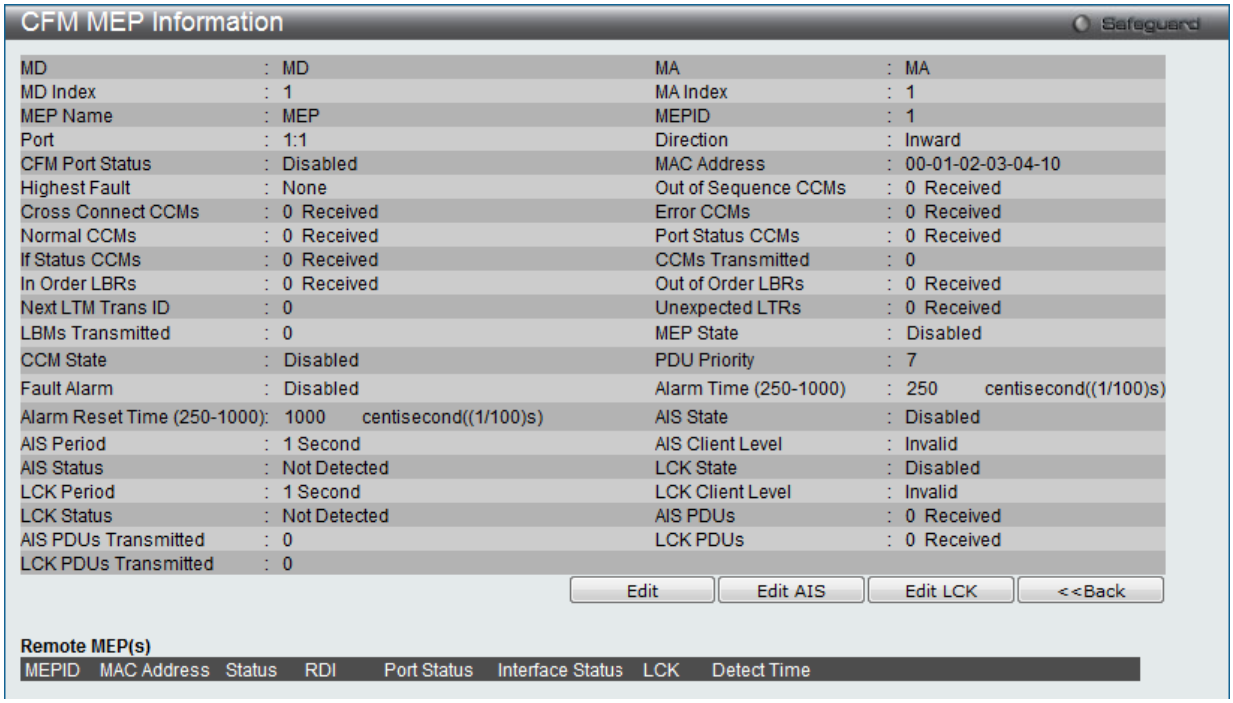


図 14-7　CFM MEP Information 画面

MEP の編集

「Edit」ボタンをクリックし、以下の画面を表示します。

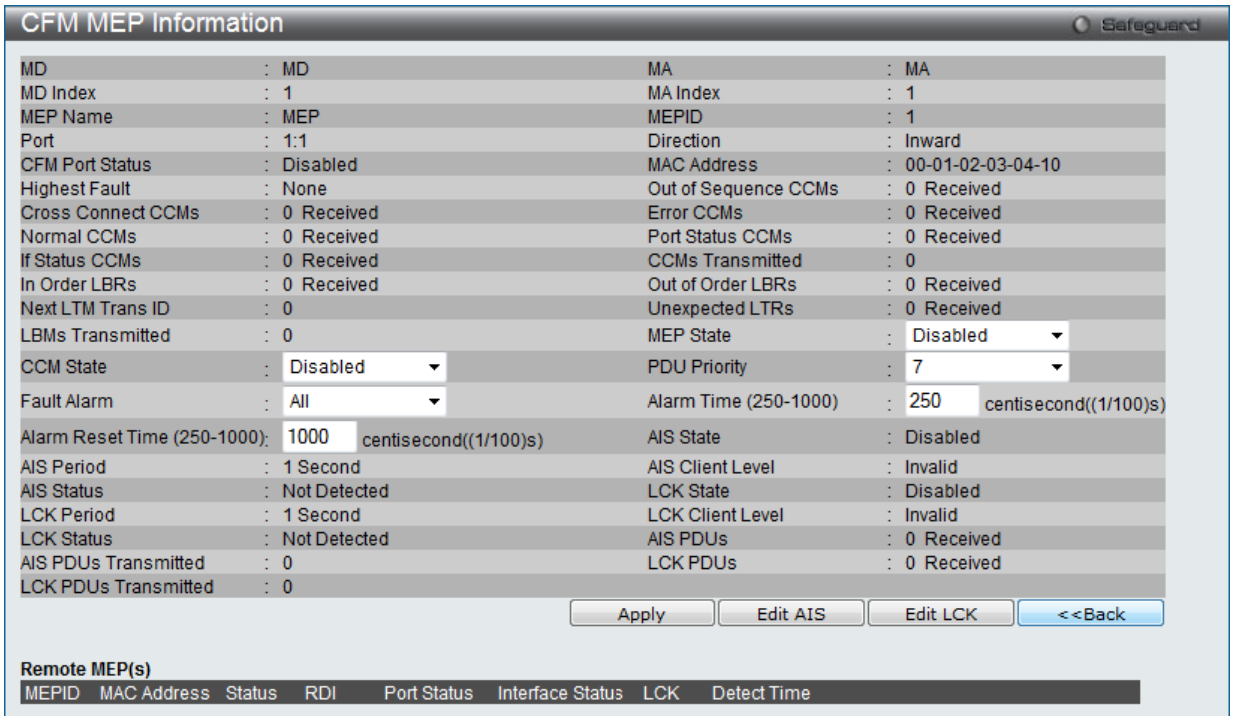


図 14-8　CFM MEP Information 画面 - Edit

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。

CFM Extension AIS の設定

「Edit AIS」ボタンをクリックし、以下の画面を表示します。

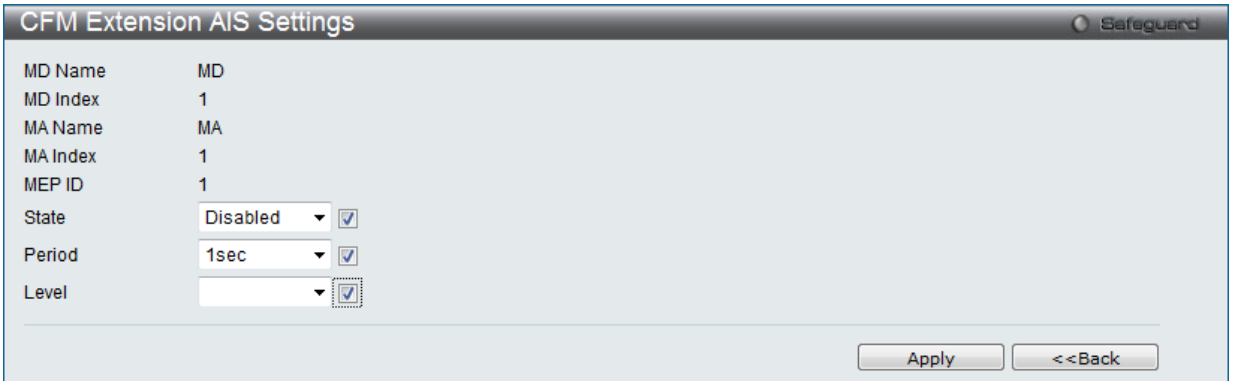


図 14-9　CFM Extension AIS (Edit) 画面

以下の項目を設定または表示できます。

項目	説明
State	AIS 機能の有効 / 無効を指定します。
Period	AIS PDU の送信インターバルについて設定します。初期値は 1 秒です。 • 1sec - AIS PDU の送信インターバルを 1 秒に設定します。 • 1min - AIS PDU の送信インターバルを 1 分に設定します
Level	MEP が AIS PDU を送信するクライアントレベルです。0-7 の間で設定可能です。

「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。

CFM Extension LCK の設定

「Edit LCK」ボタンをクリックし、以下の画面を表示します。

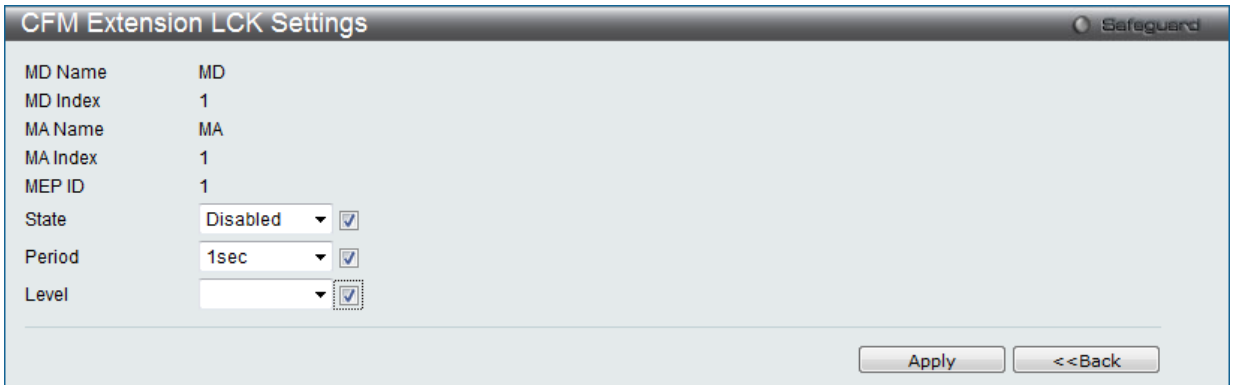


図 14-10 CFM Extension LCK (Edit) 画面

以下の項目を設定または表示できます。

項目	説明
State	LCK 機能の有効 / 無効を指定します。
Period	LCK PDU の送信インターバルについて設定します。初期値は 1 秒です。 • 1sec - LCK PDU の送信インターバルを 1 秒に設定します。 • 1min - LCK PDU の送信インターバルを 1 分に設定します
Level	MEP が LCK PDU を送信するクライアントレベルです。0-7 の間で設定可能です。

「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。

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。

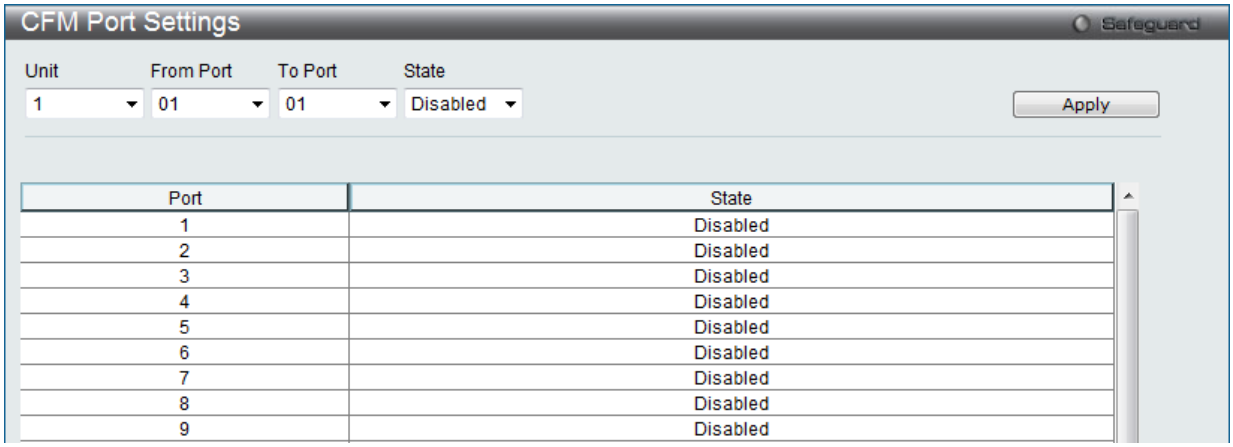


図 14-11 CFM Port Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	指定するユニットの ID です。
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。

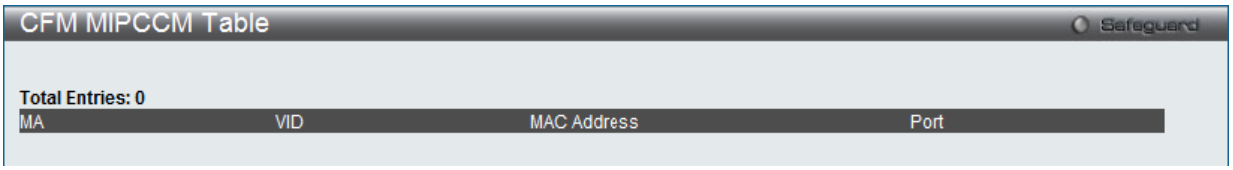


図 14-12 CFM MIPCCM Table 画面

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。

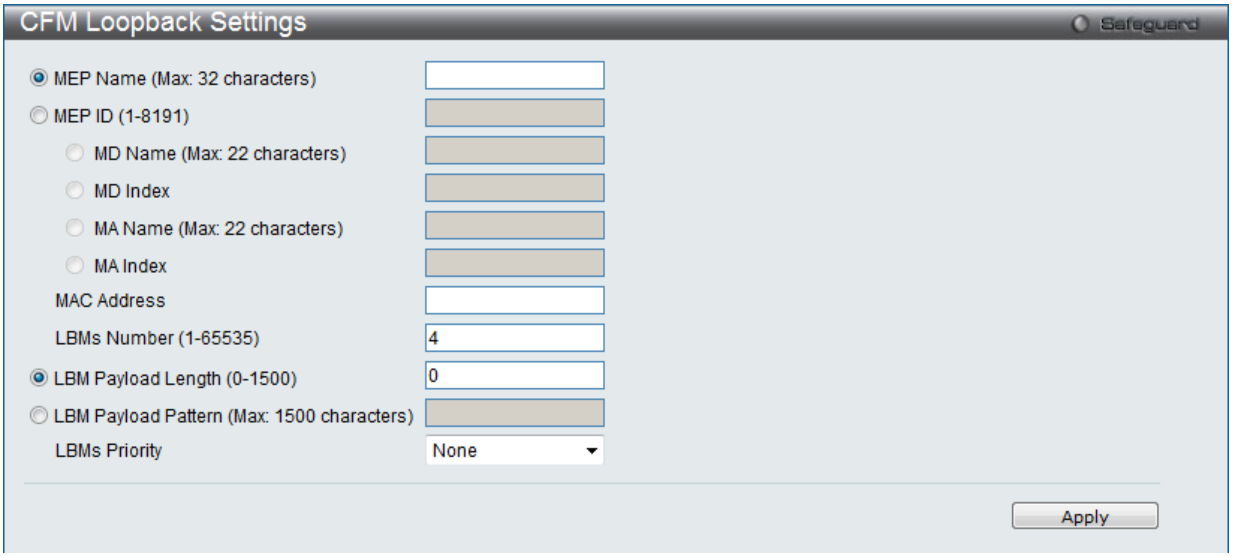


図 14-13 CFM Loopback Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
MEP Name (Max: 32 characters)	MEP 名を入力します。
MEP ID (1-8191)	MEP ID を入力します。
MD Name (Max:22 characters)	メンテナンスドメインの名称を入力します。
MD Index	メンテナンスドメインのインデックスを入力します。
MA Name (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。
MA Index	メンテナンスアソシエーションのインデックスを入力します。
MAC Address	宛先 MAC アドレスを入力します。
LBMs Number (1-65535)	送信する LBM 数。初期値は 4 です。1 ～ 65535 の範囲で指定します。
LBM Payload Length (0-1500)	送信される LBM のペイロード長。初期値は 0 です。
LBM Payload Pattern (Max: 1500 characters)	データ TLV が含まれるかどうかの指示に伴うデータ TLV に含める任意データの量。
LBMs Priority	送信される LBM に設定される 802.1p 優先度（0-7）。指定しない場合、MA が送信した CCM と LTM と同じ優先度を使用します。初期値は「None」（なし）です。

「Apply」ボタンをクリックし、変更を有効にします。

CFM Linktrace Settings（CFM リンクトレース設定）

CFM リンクトラックメッセージを設定します。

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。

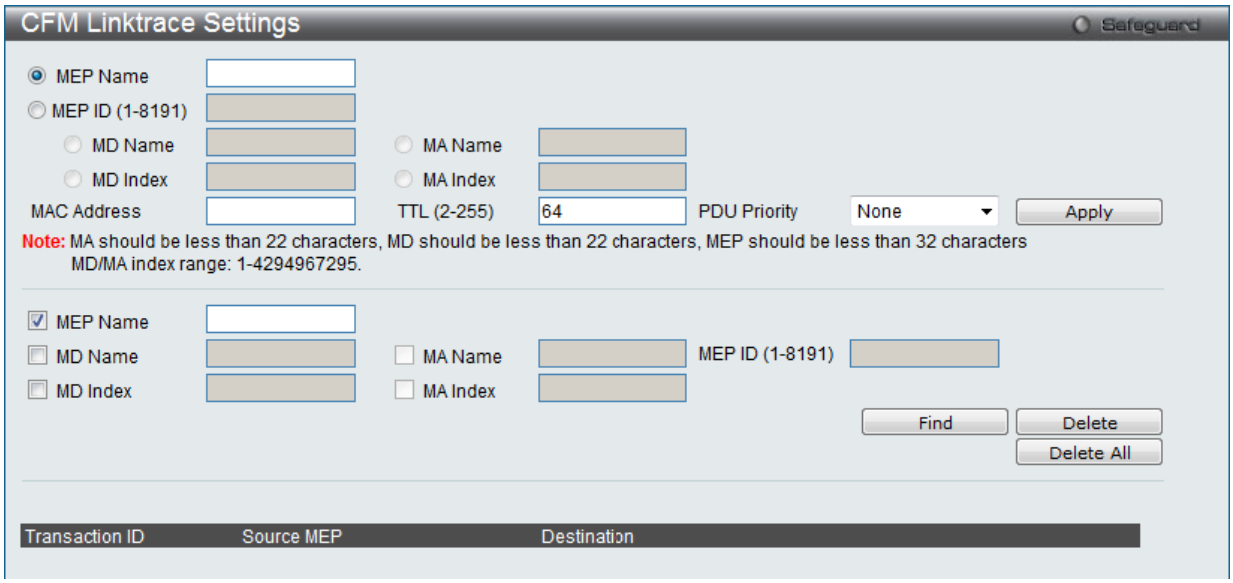


図 14-14 CFM Linktrace Settings 画面

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。
MD Index	メンテナンスドメインのインデックスを入力します。
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。
MA Index	メンテナンスアソシエーションのインデックスを入力します。
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。

エントリの削除

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

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

CFM Packet Counter（CFM パケットカウンタ）

CFM パケットの送信 / 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。

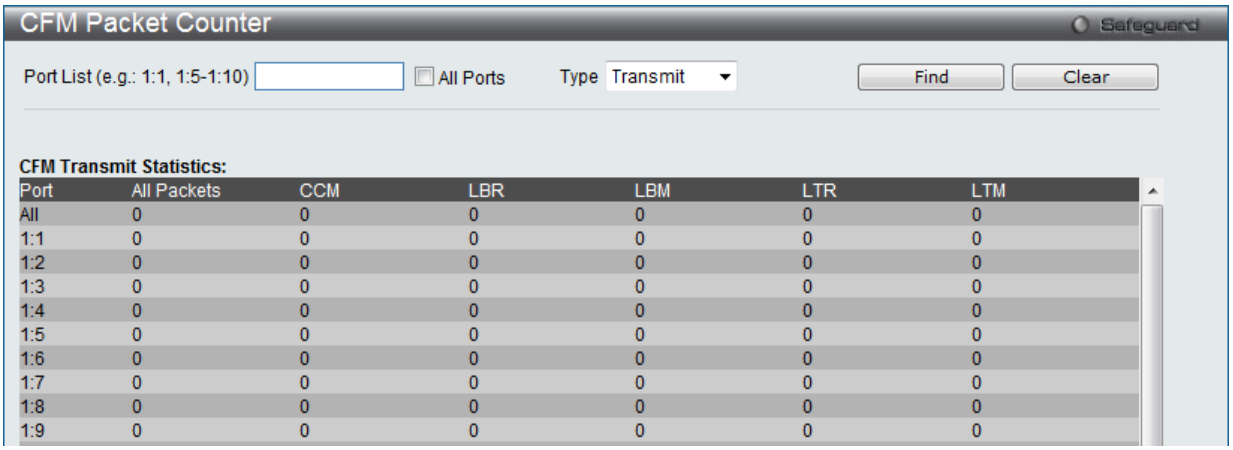


図 14-15 CFM Packet Counter 画面

画面には以下の項目があります。

項目	説明
Port List	参照するポートを選択します。
All Ports	すべてのポートを指定します。
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。

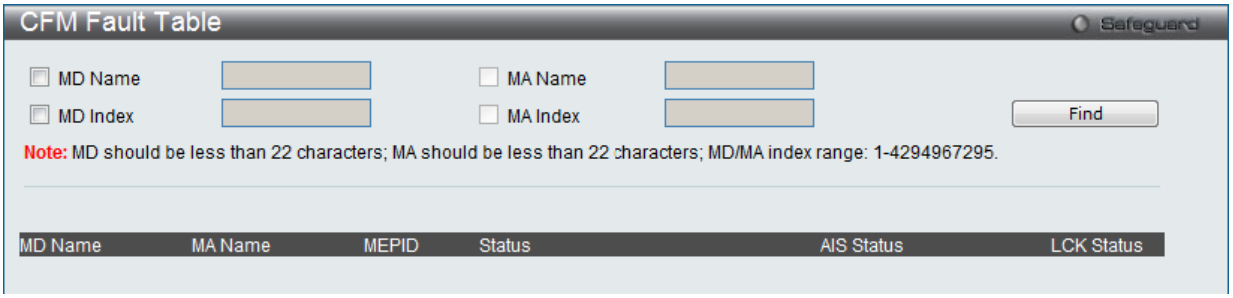


図 14-16 CFM Fault Table 画面

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。
MD Index	表示するメンテナンスドメインのインデックスを入力します。
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。
MA Index	表示するメンテナンスアソシエーションのインデックスを入力します。

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。

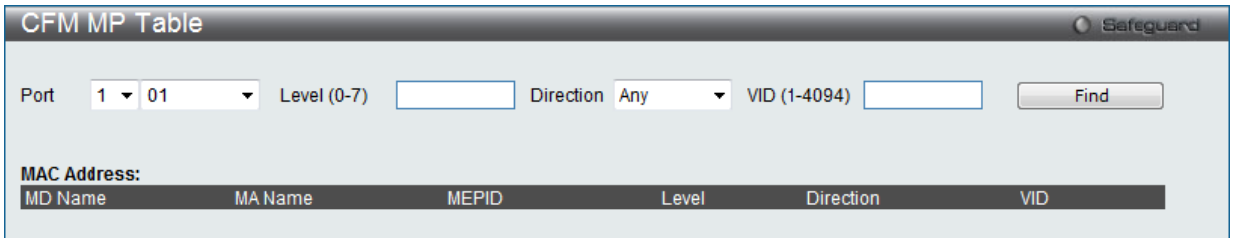


図 14-17 CFM MP Table 画面

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。
VID (1-4094)	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）（EI モードのみ）

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。

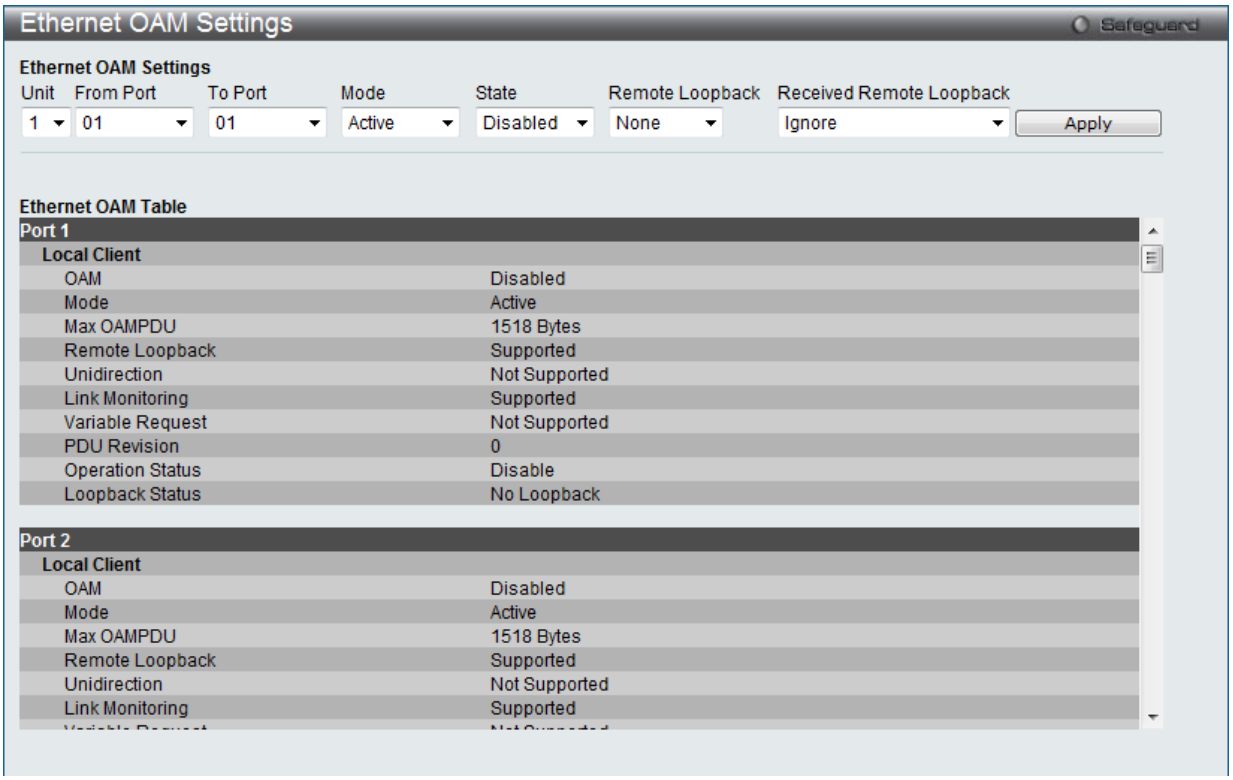


図 14-18 Ethernet OAM Settings 画面

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指定します。
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 14-19 Ethernet OAM Configuration 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指定します。
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。

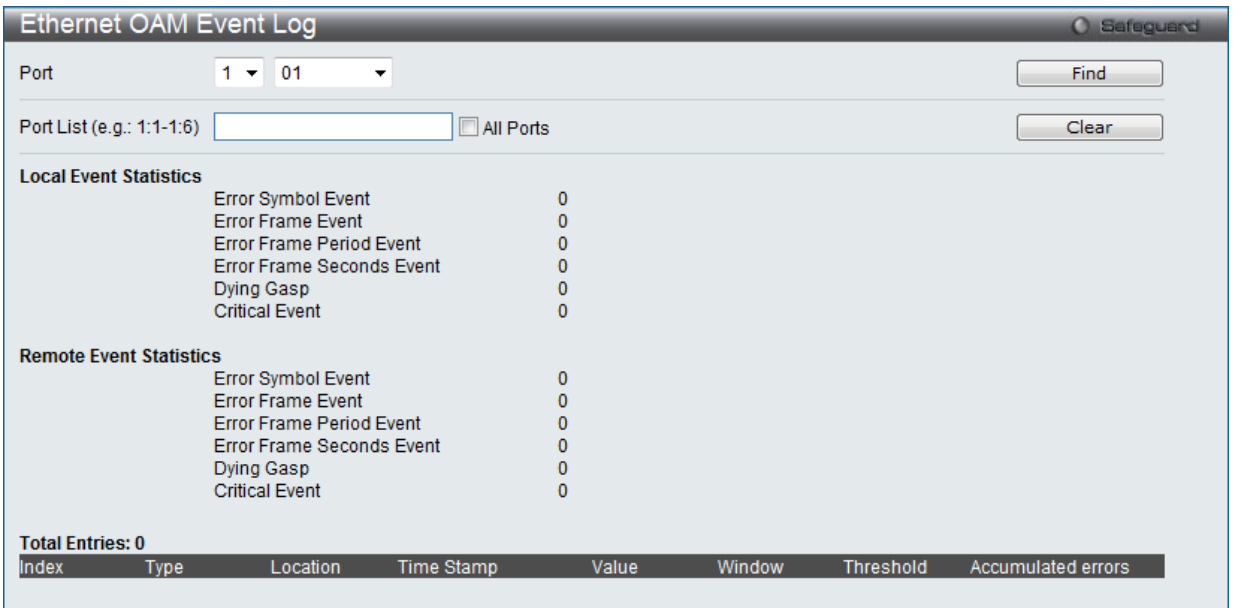


図 14-20 Ethernet OAM Event Log 画面

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における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 > EEthernet OAM > Ethernet OAM Statistics の順にメニューをクリックし、以下の画面を表示します。

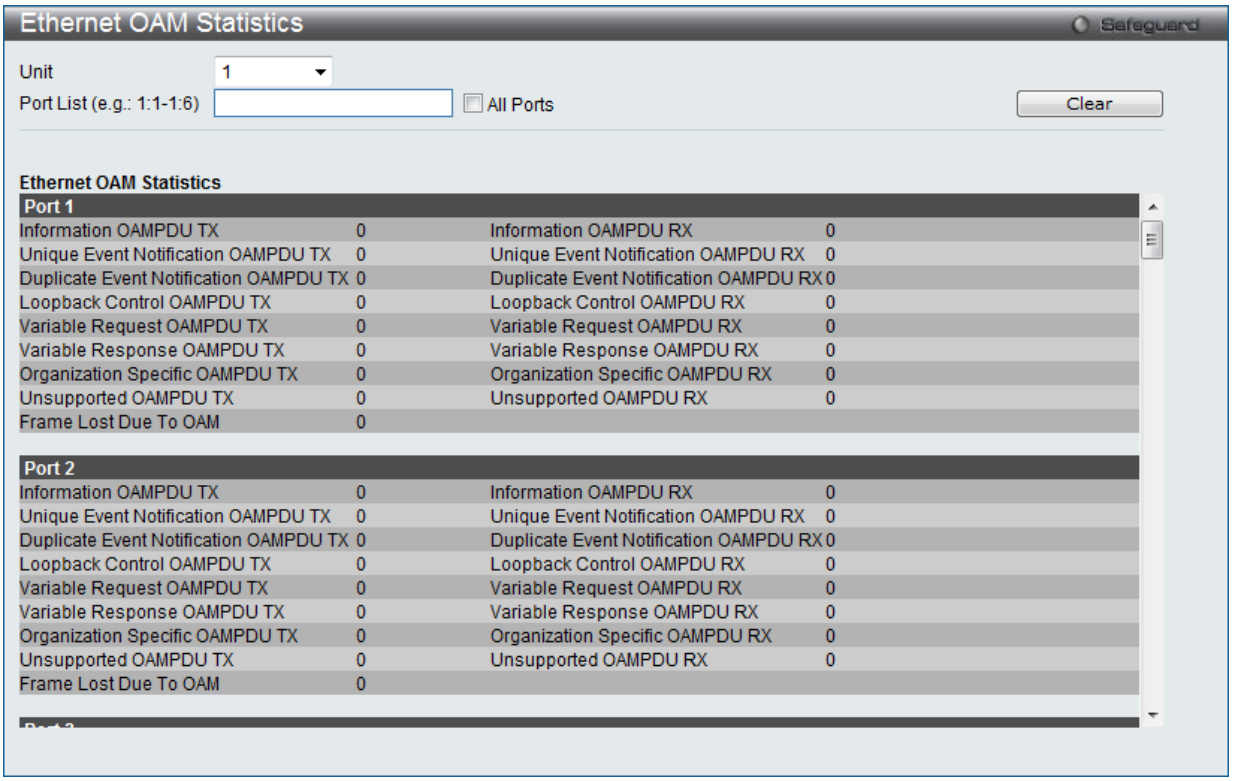


図 14-21 Ethernet OAM Statistics 画面

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）（EI モードのみ）

ポートにおいて単方向のリンク検出の設定および表示を行います。

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

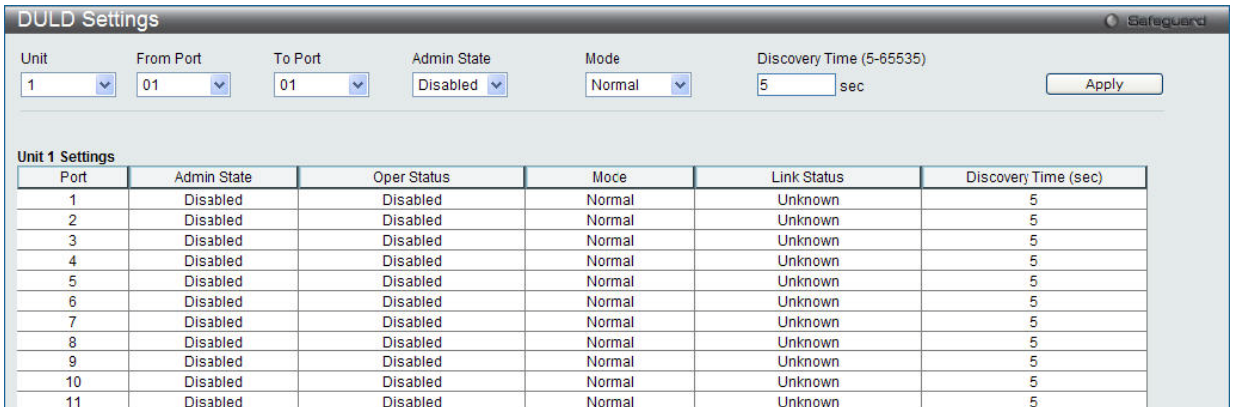


図 14-22 DULD Settings 画面

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か選択ポートの単方向リンク検出状態を「Enabled」(有効) または「Disabled」(無効) に設定します。
Mode	プルダウンメニューを使用してモード（「Shutdown」および「Normal」）を選択します。 • Shutdown - 単方向のリンクが検出されると、ポートを無効にしてイベントをログに出力します。 • Normal - 単方向のリンクが検出した場合にイベントを単にログに出力します。
Discovery Time (5-65535)	これらのポートの Neighbor 検出時間を入力します。検出がタイムアウトになると、単方向リンク検出が開始します。

「Apply」ボタンをクリックして行った変更を適用します。

Cable Diagnostics（ケーブル診断機能）

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は主に管理者とカスタマサービス担当者が UTP ケーブルを検査、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。

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

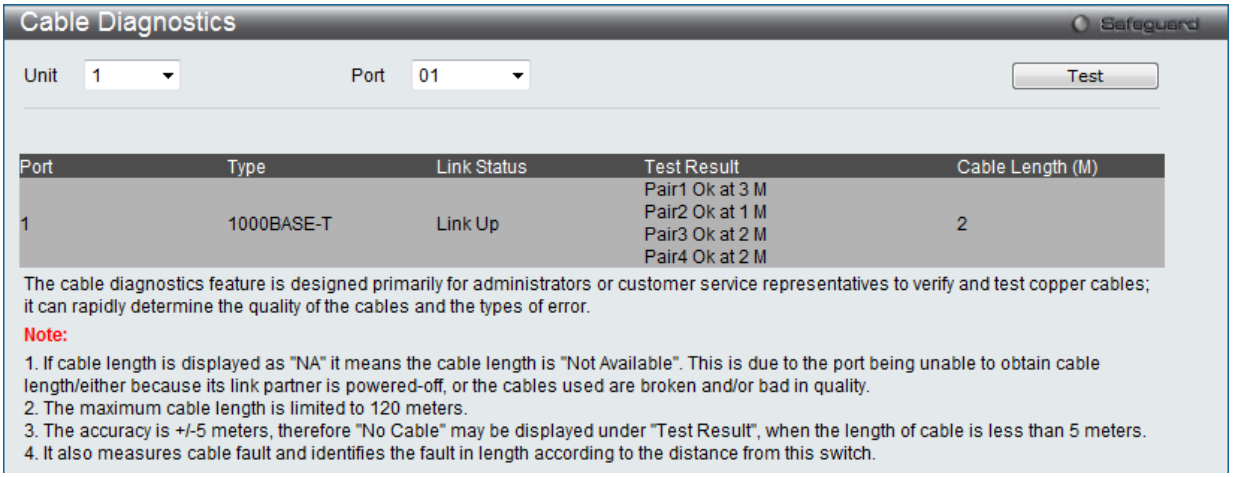


図 14-23 Cable Diagnostics 画面

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設定するユニットとポートを選択し、「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	エラーになっている 2 対のケーブルが特定箇所で接続していません。
Short	エラーになっている 2 対のケーブルが特定箇所でショートしています。
Crosstalk	エラーになっている 2 対のケーブルが特定箇所でクロストークの問題があります。
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 Copper ポートでのみサポートされています。ポートは 10/100/1000Mbps 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 ケーブルが挿入されていないポートでは診断結果が誤った値になる場合があります。

注意 ケーブル診断機能において、リンク速度が 100Mbps(対向が FE のみサポートの PHY) の場合には診断結果が正しく表示されません。

第 15 章　Monitoring（スイッチのモニタリング）

Monitoring メニューを使用し、本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報を提供することができます。

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

サブメニュー	説明	参照ページ
Utilization（利用分析）	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）	352
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）	354
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）	363
sFlow（sFlow 設定） （EI モードのみ）	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）	365
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。次のメニューがあります。 Broadcast Ping Relay Settings（ブロードキャスト Ping リレー設定）、Ping Test（Ping テスト）	368
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。	369
Peripheral（周辺機器）	デバイス環境機能はスイッチの内部温度ステータスを表示します。次のメニューがあります。 Device Environment（デバイス環境の参照）	370

Utilization（利用分析）

CPU Utilization（CPU 使用率）

現在の CPU 使用率をパーセント表示し、また指定した時間間隔で計算した平均値も表示します。

Monitoring > Utilization > CPU Utilization メニューをクリックし、以下の画面を表示します。

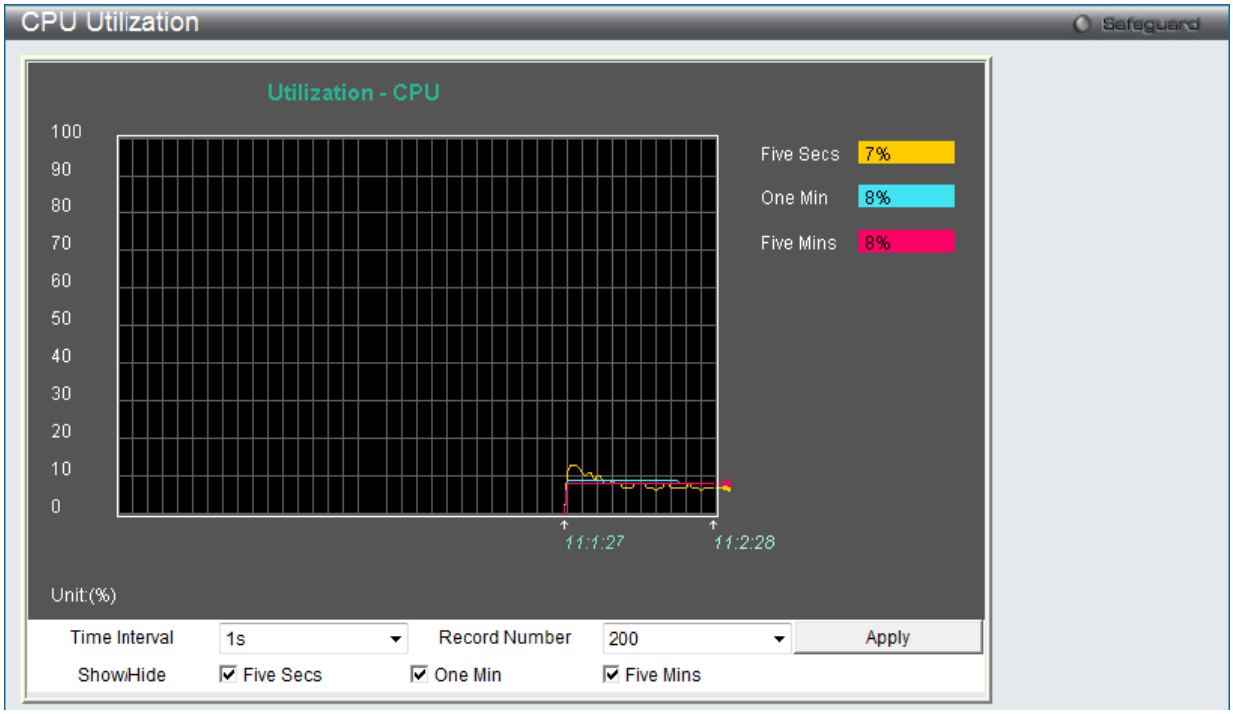


図 15-1　CPU Utilization 画面

以下の設定項目を使用して表示を変更します。

項目	説明
Timer Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Show/Hide	チェックボックスにて CPU 使用率を計算する時間経過を Five Secs、One Min および Five Mins から選択します。各時間経過は色分けされた線で表示されます。Five Secs は黄色、One Min は青、Five Mins はピンク色で表示されます。選択すると CPU 使用率を表示します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。

DRAM & Flash Utilization（DRAM & Flash 使用率）

「DRAM & Flash Utilization」画面では、現在の DRAM & Flash 使用率 / 使用情報を表示します。

Monitoring > Utilization > DRAM & Flash Utilization メニューをクリックし、以下の画面を表示します。

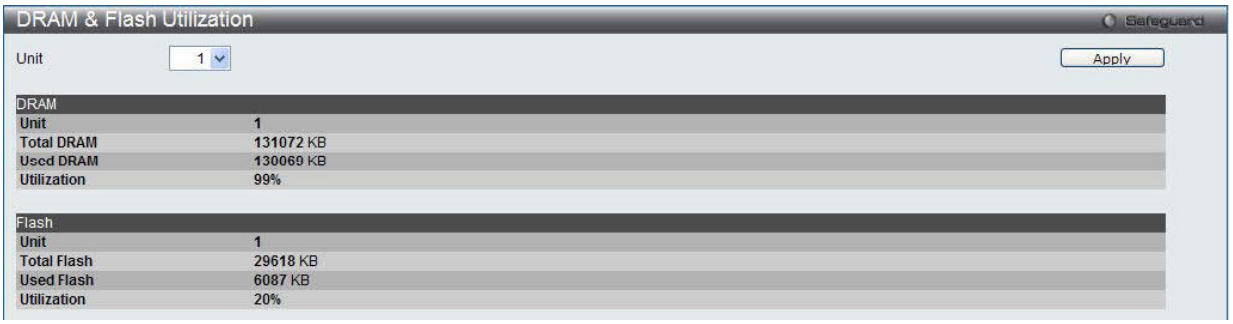


図 15-2　DRAM & Flash Utilization 画面

以下の設定項目が使用できます。

項目	説明
Unit	表示するユニットを指定します。

設定を適用する場合は、必ず「Apply」ボタンをクリックしてください。

Port Utilization（ポート使用率）

本画面では、ポートの帯域使用率を表示します。

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

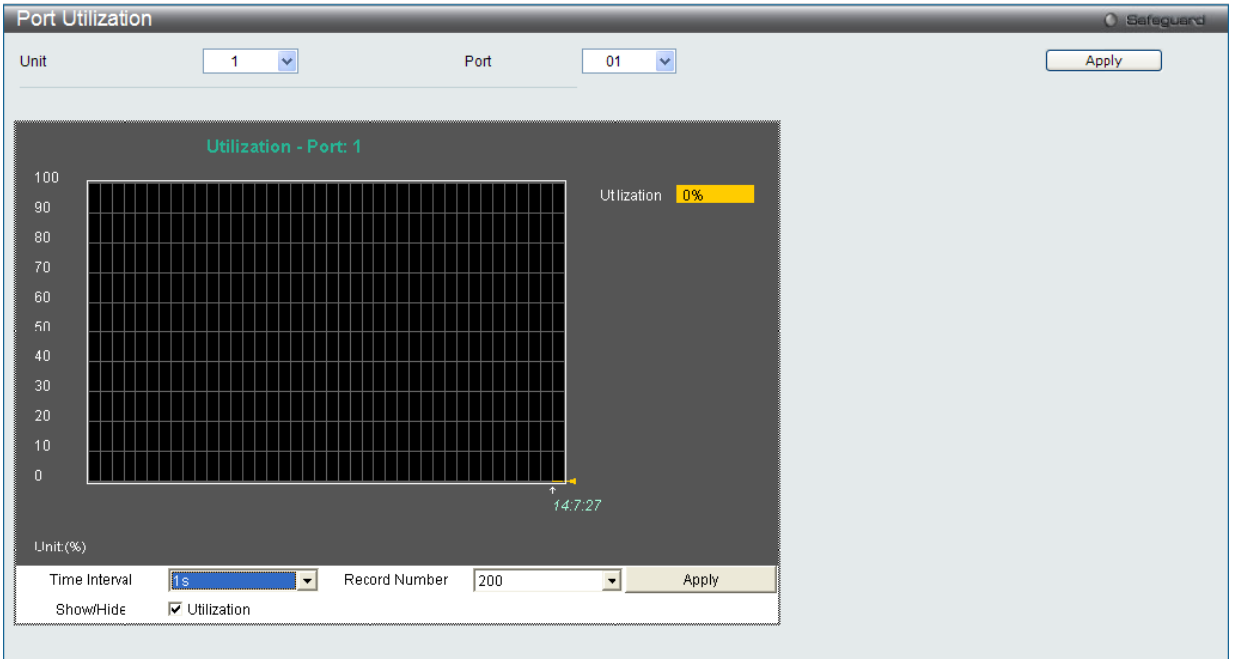


図 15-3　Port Utilization 画面

統計情報を参照するためには、プルダウンメニューでポート番号を選択します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

以下の設定項目が使用できます。

項目	説明
Unit	設定するユニットを指定します。
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	「Port_Util」にチェックすると、使用率を表示します。

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

Statistics（統計情報）

Port Statistics（ポート統計情報）

Packets（パケット統計情報）

Web マネージャは、パケットの統計情報を折れ線グラフまたは表の形式で表示します。6 個の画面が表示されます。

Received（Rx）（受信パケット状態の参照）

スイッチが受信したパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packets > Received (RX) の順にメニューをクリックし、以下の画面を表示します。

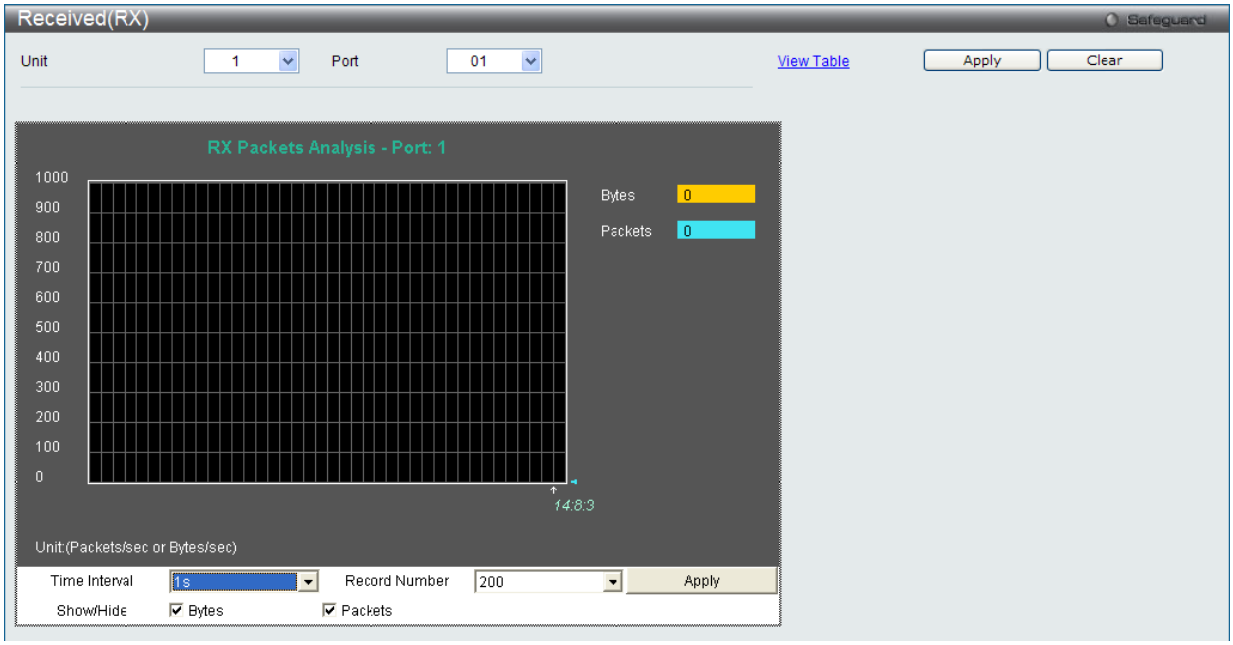


図 15-4　Received（Rx）Table 画面（バイトとパケットの折れ線グラフ）

「Received（RX）Table」を表示するには「View Table」リンクをクリックして、次の表を表示します。

図 15-5　RX Packets Analysis Table 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
Unit	表示するユニットを選択します。
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。

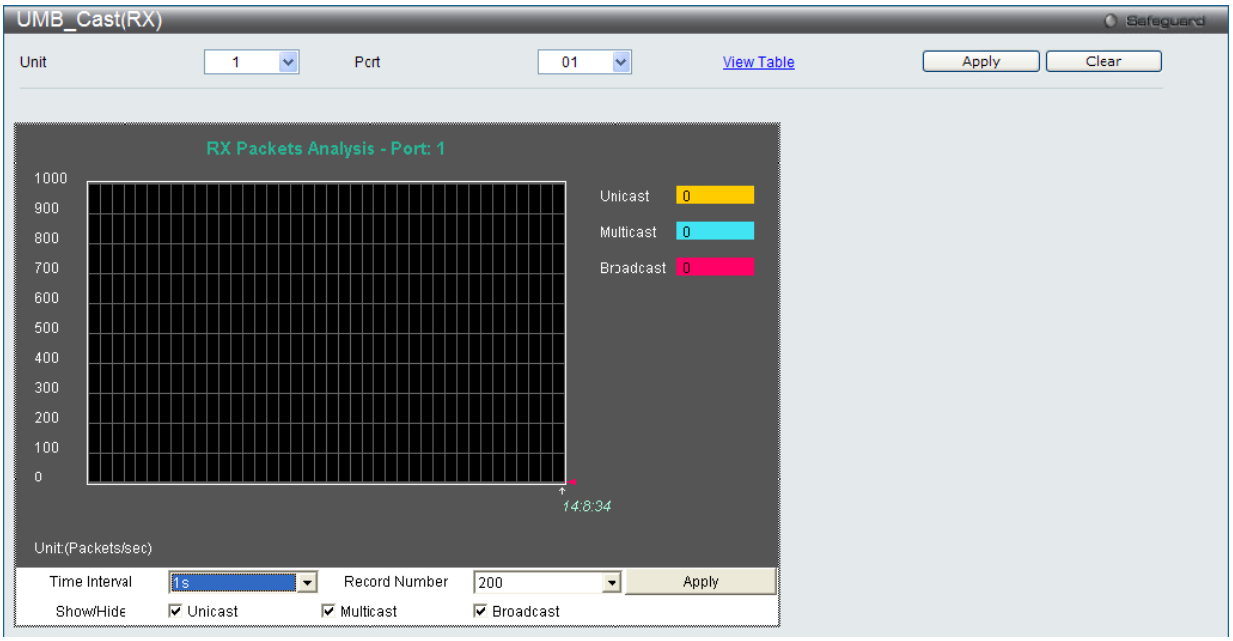


図 15-6　UMB_Cast（Rx）画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の折れ線グラフ）

「UMB_Cast（RX）Table」画面の表示を行うためには、「View Table」リンクをクリックします。

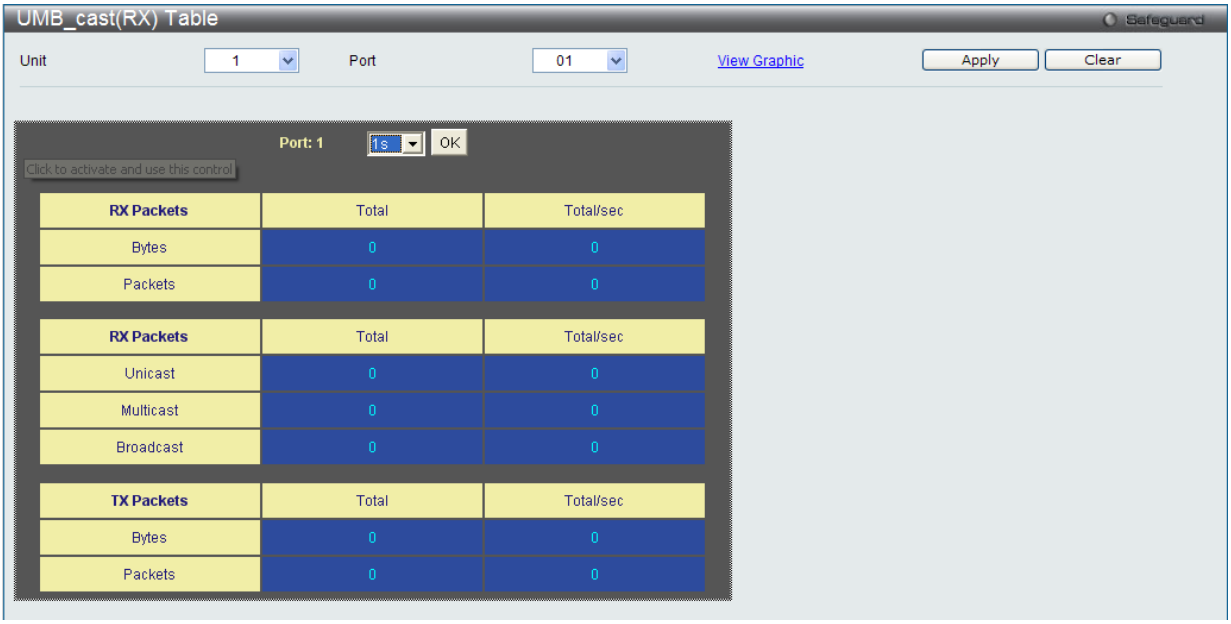


図 15-7　RX Packets Analysis 画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の表形式表示）

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
Unit	表示するユニットを選択します。
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Unicast	ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが受信した正常なパケットの合計数をカウントします。
Show/ Hide	Unicast、Multicast、Broadcast を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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

Transmitted（Tx）（送信パケット統計情報）

スイッチから送信したパケットの情報をグラフ表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packets > Transmitted (TX) の順にメニューをクリックし、以下の画面を表示します。

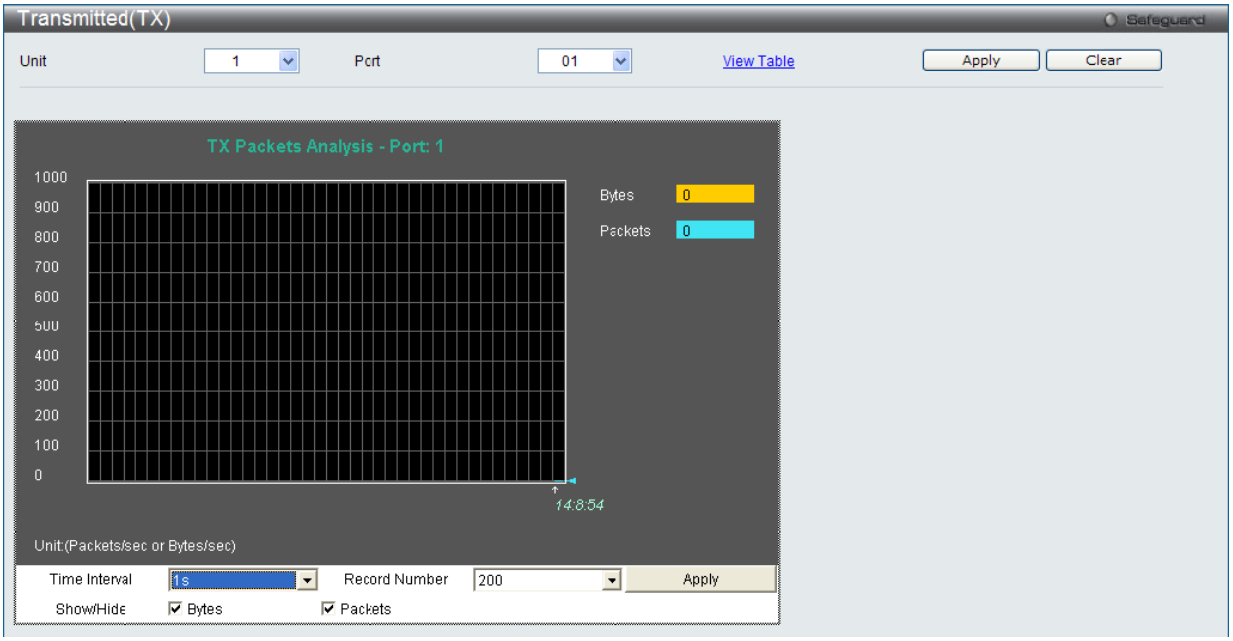


図 15-8　Transmitted（Tx）画面（パケットサイズ、パケット数の折れ線グラフ表示）

送信パケットの情報を、表形式で表示するには、「View Table」リンクをクリックし、「Transmitted（TX）Table」画面を表示します。

図 15-9　Transmitted（TX）Table 画面（パケットサイズ、パケット数の表示）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Bytes	ポートから送信に成功したパケット量（バイト）。
Packets	ポートから送信に成功したパケット数。
Unicast	ユニキャストアドレスが送信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが送信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが送信した正常なパケットの合計数をカウントします。
Show/ Hide	Bytes と Packets を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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

Errors（パケットエラー）

Web マネージャは、スイッチの管理エージェントが集計したエラー統計情報を、折れ線グラフまたは表形式で表示します。以下の 4 つの画面で表示できます。

Received（Rx）（受信エラーパケット統計情報の参照）

スイッチが受信したエラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Errors > Received (RX) の順にメニューをクリックし、以下の画面を表示します。

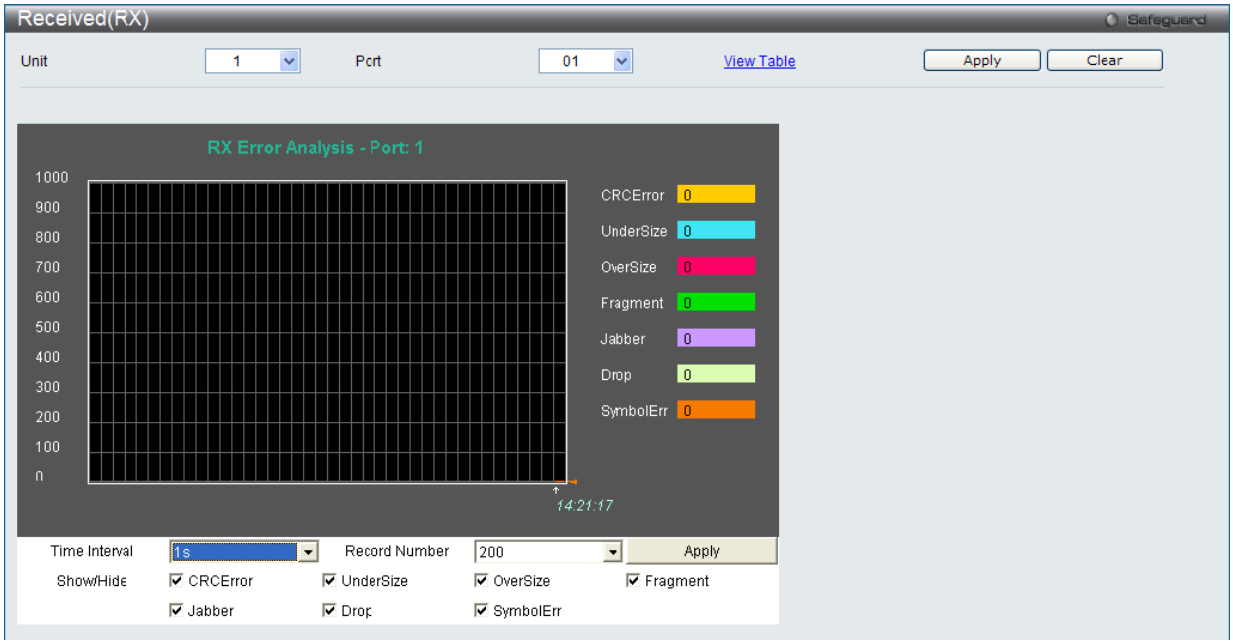


図 15-10　Received（Rx）- Error 画面（折れ線グラフ形式）

表形式の「Received（RX）Table」画面を表示するためには、「View Table」リンクをクリックします。

図 15-11　Received（RX）Table - Error 画面（表形式）

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	表示するユニットを選択します。
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 > Errors > Transmitted (TX) の順にメニューをクリックし、以下の画面を表示します。

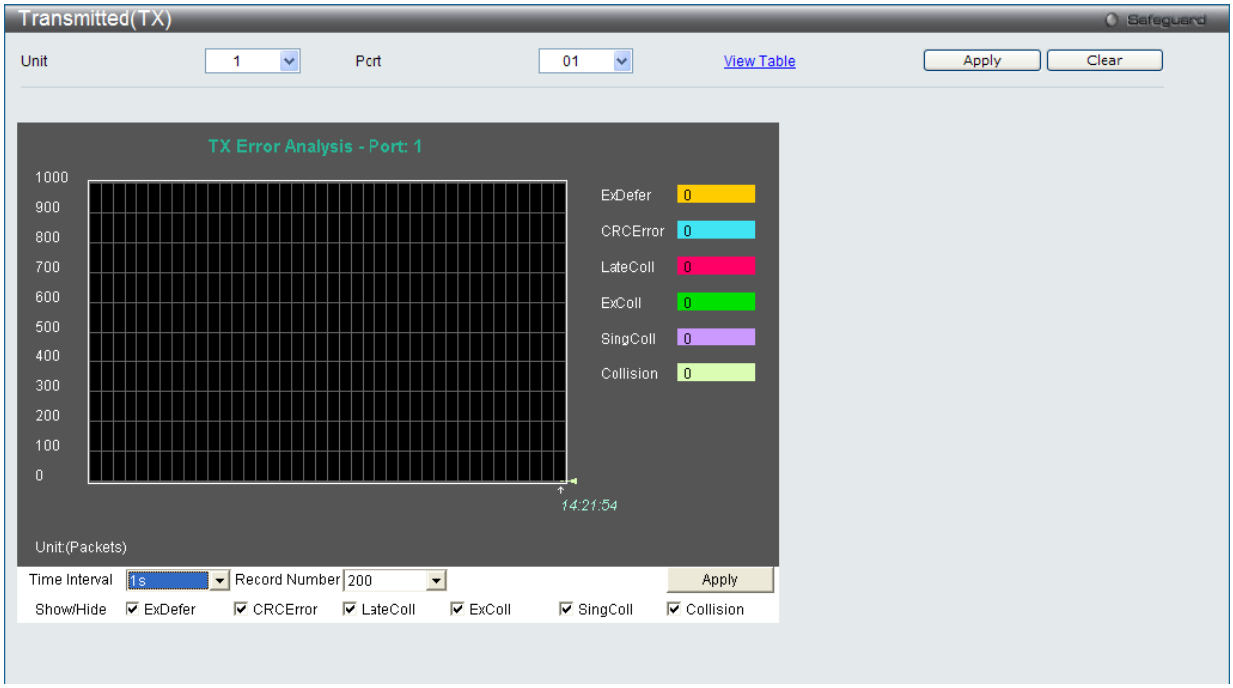


図 15-12　Transmitted（Tx）- Error 画面（折れ線グラフ形式）

表形式の「Transmitted（TX）」画面を表示するためには、「View Table」リンクをクリックします。

図 15-13　Transmitted（TX）Table - Error 画面（表形式）

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	表示するユニットを選択します。
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	パケット送信に入る 512 ビット時間よりも遅くに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。

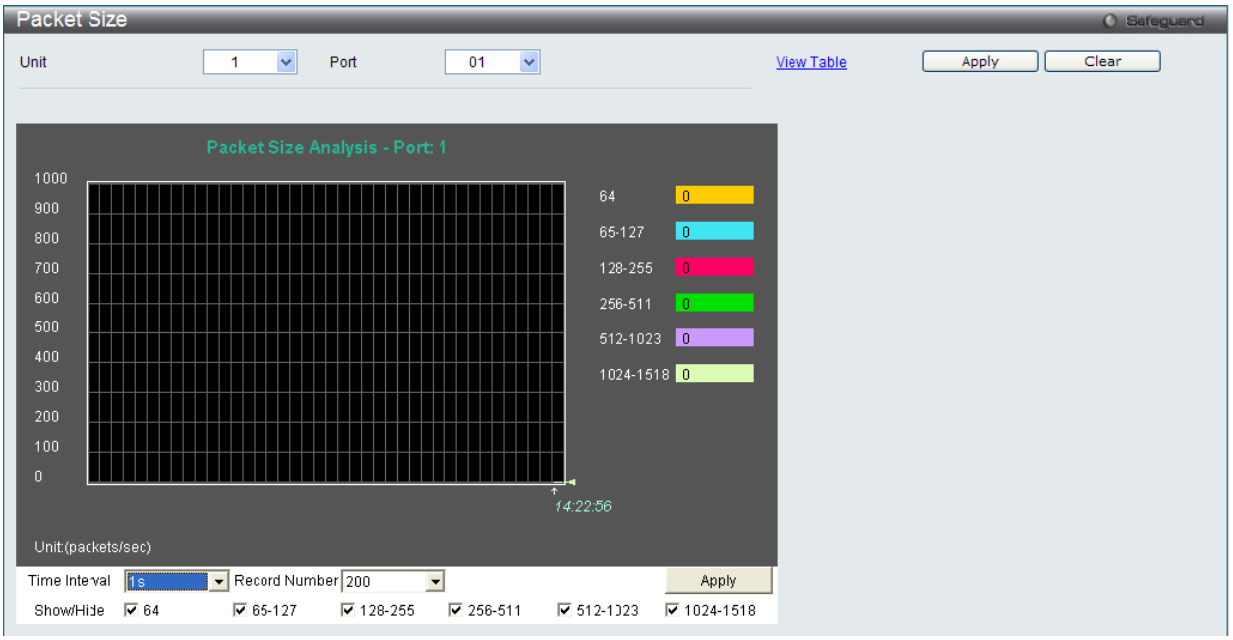


図 15-14　Packet Size 画面（折れ線グラフ）

「Packet Size Table」を表示するためには、「View Table」リンクをクリックします。

図 15-15　Packet Size Table 画面（表形式）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Unit	表示するユニットを選択します。
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。

Mirror（ミラーリング）

本スイッチは、対象ポートで送受信するフレームをコピーして、そのコピーしたフレームの出力先を他のポートに変更する機能（ポートミラーリング）を持っています。

Port Mirror Settings（ポートミラー設定）

ポートミラーリング機能を設定します。

Monitoring > Mirror > Port Mirror Settings をクリックします。

図 15-16　Port Mirror Settings 画面

以下の情報が表示されます。

項目	説明
Mirror Global State	プルダウンメニューから、ミラーグループ機能の有効 / 無効を選択します。
Group ID (1-4)	ミラーグループ ID を入力します。
Target Port	チェックボックスをチェックし送信元ポートからコピーを受信するポートを入力します。
Unit	設定するユニットを指定します。
TX (Egress)	ミラーグループの送信元ポートの受信パケットのみターゲットポートにミラーされます。
RX (Ingress)	ミラーグループの送信元ポートの送信パケットのみターゲットポートにミラーされます。
Both	「Both」を選択するとポートは送信 / 受信の両トラフィックに対応します。
None	「None」を選択するとポートはあらゆるトラフィックに対応しません。

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。
指定のエントリを検索するには情報を入力し「Find」をクリックします。
既存のエントリを全て表示するには「View All」をクリックします。
指定のエントリを編集する場合は「Modify」をクリックします。

「Modify」をクリックすると次の画面が表示されます。

図 15-17　Port Mirror 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
Group ID (1-4)	編集するミラーグループ ID です。
Target Port	「Unit」で設定するユニットを指定し、送信元ポートからコピーを受信するポートを入力します。
Source Ports	送信元ポートを指定します。 TX (Egress)：ミラーグループの送信元ポートの受信パケットのみターゲットポートにミラーされます。 RX (Ingress)：ミラーグループの送信元ポートの送信パケットのみターゲットポートにミラーされます。 Add/Delete：ポートを追加 / 削除します。
State	ミラーグループ機能の有効 / 無効を選択します。

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

注意　低速ポートに高速ポートをミラーすることはできません。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問題が発生します。フレームをコピーするポートはコピーを送信するポートと同等、または低速である必要があります。そして宛先 / 送信元ポートは同一に設定することはできません。

RSPAN Setting（RSPAN 設定）

RSPAN（Remote Switched Port Analyzer）はポートを通過するトラフィックパスをモニタ、分析する機能です。RSPAN の「R」は「Remote」をあらわしており、ミラー送信元ポートと宛先ポートが同じスイッチにないことを意味しています。つまりリモートミラーセッションは、少なくとも 2 つのスイッチから構成されます。リモートミラーリング機能の動作には、ミラートラフィックは RSPAN VLAN と呼ばれる VLAN にタグ付けされ、RSPAN VLAN は RSPAN にタグ付けをされたトラフィックが、関連する宛先ポートへミラーリングされている必要があります。

注意 RSPAN VLAN ミラーリングは RSPAN が有効化（ひとつの RSPAN VLAN だけが送信元ポートに設定されている場合）されている場合にだけ動作します。RSPAN リダイレクト機能は RSPAN が有効化され、少なくとも一つの RSPAN VLAN がリダイレクトされたポートに設定されている場合に動作します

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。

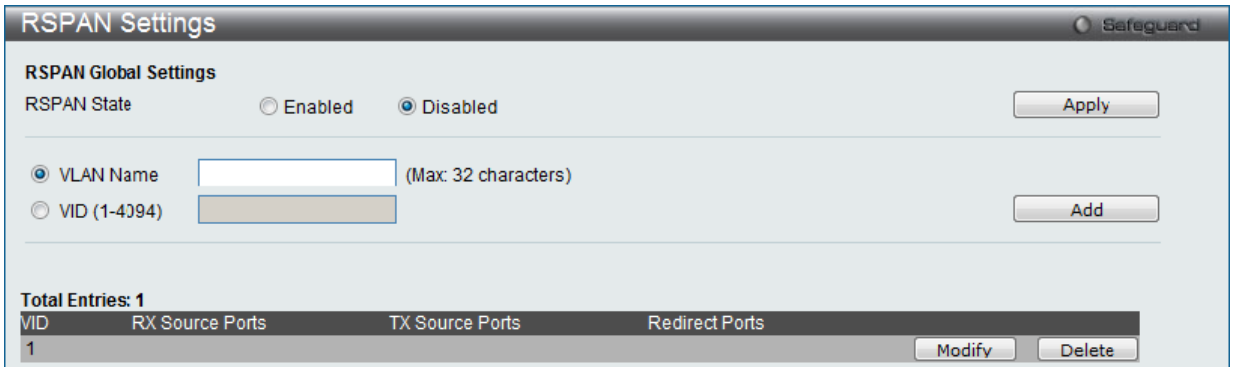


図 15-18　RSPAN Settings 画面

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 RSPAN VLAN を指定します。
VID (1-4094)	VLAN ID により RSPAN VLAN を指定します。

「RSPAN State」を「Enabled」または「Disabled」にして「Apply」ボタンをクリックして、RSPAN 機能を有効または無効にします。

エントリの追加

「RSPAN State」を「Enabled」（有効）にして「VLAN Name」または「VID」を指定後、「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。

RSPAN 設定の編集

エントリについて編集、変更する場合は、「Modify」ボタンをクリックして、以下の画面を表示します。

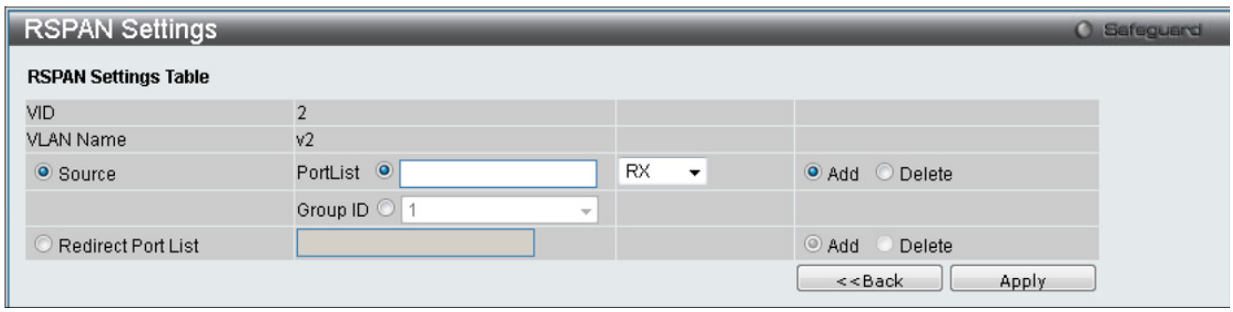


図 15-19　RSPAN Settings 画面 (Modify)

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	追加、検索、削除する VLAN 名を入力します。
VID	追加、検索、削除する VLAN ID を入力します。
Source Ports	変更、編集するポート番号を入力します。プルダウンメニューで Rx、Tx のどちらも選択することができます。
Redirect Port List	RSPAN が有効で、少なくとも 1 つの RSPAN VLAN がリダイレクトポートによって設定されている場合、RSPAN リダイレクト機能は動作します。プルダウンメニューを使用して RSPAN VLAN ポートの出力ポートを指定します。

「Add」「Delete」を選択してから「Apply」ボタンをクリックして設定を有効にします。

再度 RSPAN の設定をする場合は「<<Back」ボタンをクリックします。

sFlow（sFlow 設定）（EI モードのみ）

sFlow は（RFC3176）、スイッチのパケットサンプリングとパケットカウンタ情報からネットワークの問題を特定するためにスイッチを経由するネットワークトラフィックをモニタする機能です。スイッチ自身は問題解決のためにパケットデータを取得し、詳しく調査する sFlow アナライザにパケットデータを送信する sFlow エージェントです。スイッチは、sFlow アナライザの設定はできますが、リモートの sFlow アナライザデバイスには、sFlow エージェントから受信するデータを取得して、分析するために sFlow ユーティリティを動作させる必要があります。

sFlow Global Settings（sFlow グローバル設定）

sFlow 機能をグローバルに有効にします。

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。

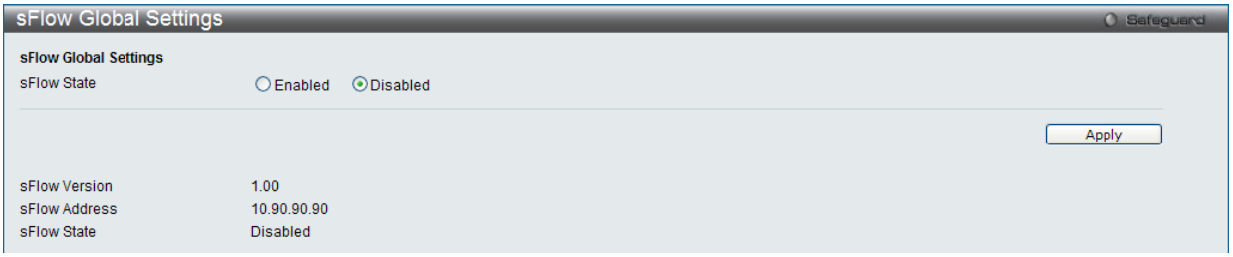


図 15-20　sFlow Global Settings 画面

以下の項目が表示されます。

項目	説明
sFlow State	sFlow をグローバルに有効または無効にします。
sFlow Version	現在の sFlow バージョンを表示します。
sFlow Address	sFlow IP アドレスを表示します。

「Apply」ボタンをクリックして、設定を有効にします。

sFlow Analyzer Server Settings（sFlow アナライザサーバ設定）

スイッチが生成する sFlow データグラムを収集して、分析するのに使用されるリモート sFlow アナライザ（コレクタ）サーバを設定します。分析のためにスイッチからデータを受信し、解析するためには、アナライザには適切な sFlow ソフトウェアを設定する必要があります。データを受信するために最大 4 個のユニークなアナライザを指定できますが、使用する仮想ポートは、各エントリに対して固有とする必要があります。

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。

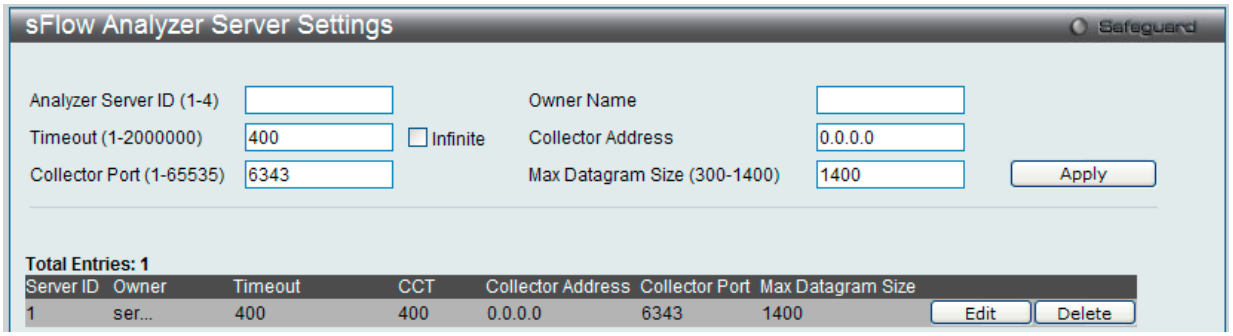


図 15-21　sFlow Analyzer Server Settings 画面

以下の項目が表示されます。

項目	説明
Analyzer Server ID（1-4）	追加する sFlow アナライザサーバの識別子（1-4）を指定します。最大 4 個のエントリを追加できますが、各エントリは、固有のコレクタポートを持っている必要があります。
Owner Name	本エントリを識別するために使用する名前を入力することをお勧めします。 エントリが本フィールドに作成されると、以下の「Timeout」フィールドはユーザが変更しない限り、自動的に 400（秒）に設定されます。
Timeout (1-2000000)	アナライザサーバにタイムアウトを指定します。サーバがタイムアウトになると、すべての sFlow のサンプルとこのサーバに関連するカウンタポーラは削除されます。1-2000000（秒）の範囲から指定します。「Infinite」を設定するとサーバはタイムアウトしません。初期値は 400（秒）です。
Collector Address	sFlow アナライザサーバの IP アドレスを指定します。本フィールドを指定しないと、エントリは 0.0.0.0 となり、エントリは無効となります。本項目を必ず設定してください。
Collector Port (1-65535)	sFlow データが送信される宛先 UDP ポートを指定します。初期値は 6343 です。
Max Datagram Size (300-1400)	1 つの sFlow データにパッケージ化する最大データバイト数を指定します。300 から 1400 で設定でき、初期値は 1400（バイト）です。

「Apply」ボタンをクリックして、設定を有効にします。

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。

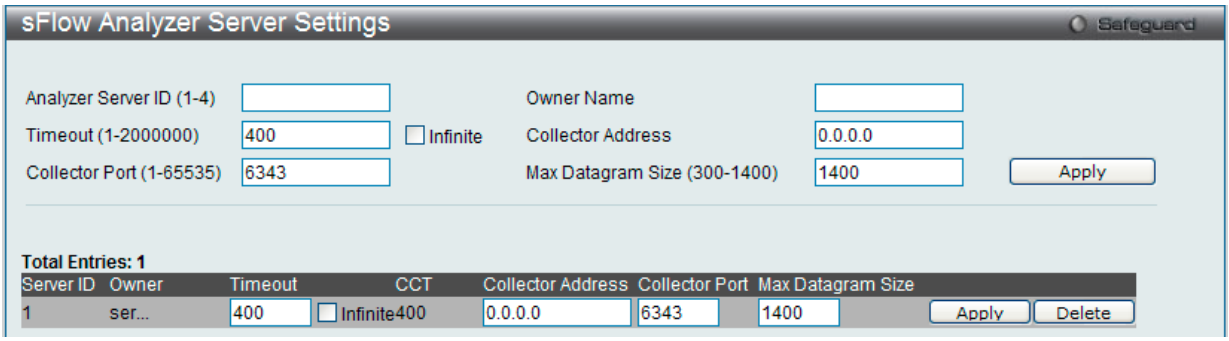


図 15-22 sFlow Analyzer Server Settings 画面 - Edit

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 フローサンプラ設定）

ネットワークからサンプルパケットを取得するための設定をします。これには、サンプリングのレートや抽出されるパケットヘッダの量も含まれます。

注意 アナライザサーバ ID を変更したい場合には、フローサンプラーを削除し、新しいものを作成する必要があります。

Monitoring > sFlow > sFlow 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。

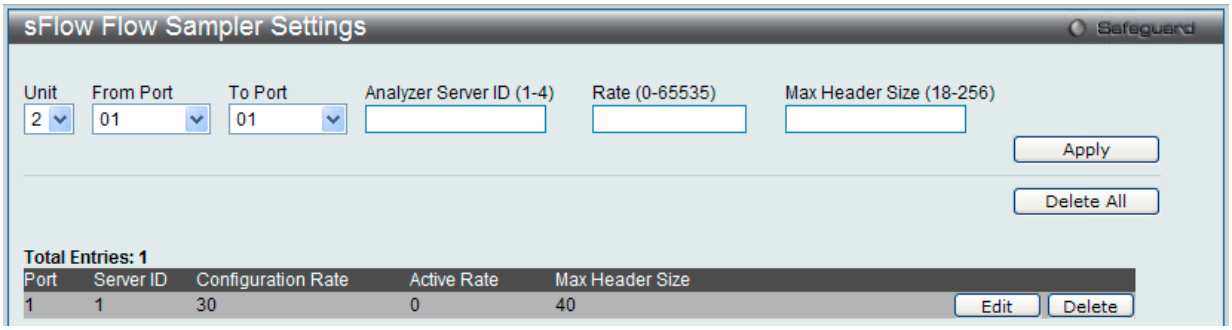


図 15-23 sFlow Flow Sampler Settings 画面

以下の項目が表示されます。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	パケットサンプリングの設定を行うポートおよびポート範囲を指定します。
Analyzer Server ID (1-4)	定義済みのアナライザサーバ ID を入力して、スイッチからデータを受信するデバイスを定義します。これらのデータには、ここで設定されたサンプリングメカニズムを使用して取得したサンプルパケットの情報も含まれます。
Rate (0-65535)	パケットサンプリングのレートを設定します。ここに入力される値は、256 倍にされ、サンプルされるパケットのその割合ごとに取得します。例えば、ユーザが 20 をこのフィールドに入力すると、スイッチは個々のポートを通過する 5120 パケット（20 x 256=5120）に 1 回サンプリングを行います。1-65535 の値を指定します。エントリ「0」は、パケットのサンプリングを無効にします。0 が初期値であるため、ここでレートを設定することを忘れないようにご注意ください。指定しないと本機能は動作しません。
MAX Header Size (18-256)	本項目はサンプリングされるパケットヘッダのバイト数を設定します。このサンプルサンプリングされるヘッダは、アナライザサーバに送信されるデータと共にカプセル化されます。18-256 バイトの値を設定します。

「Apply」ボタンをクリックして、設定を有効にします。

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。

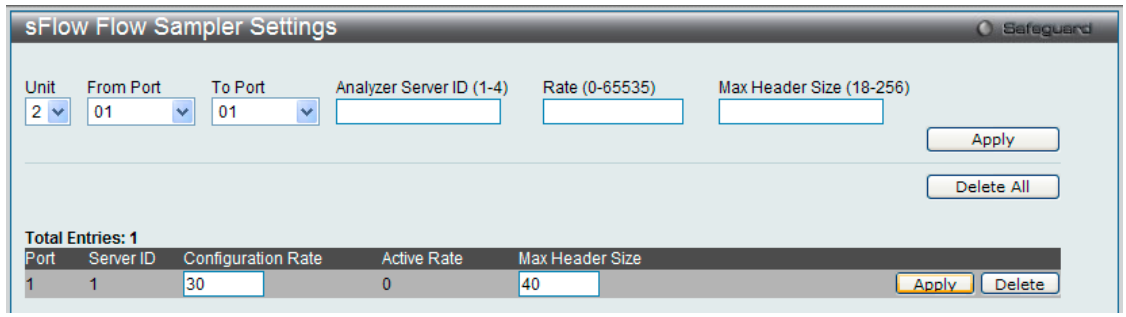


図 15-24 sFlow Flow Sampler Settings 画面 - Edit

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）

スイッチのカウンタポーラの設定を行います。このメカニズムは、スイッチの「IF」カウンタにポーリングを行い、調査のために sFlow アナライザサーバに送信されるデータを他の以前に記述したデータと共にパッケージ化します。

Configuration > 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。

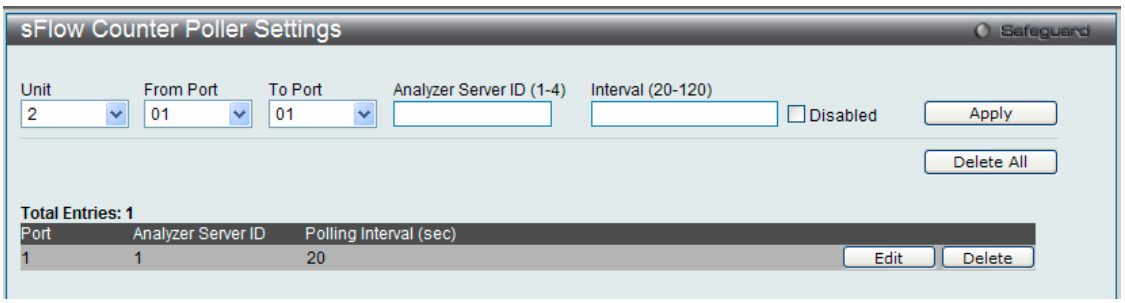


図 15-25 sFlow Counter Poller Settings 画面

以下の項目が表示されます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	カウンタポーリングの設定を行うポートおよびポート範囲を指定します。
Analyzer Server ID (1-4)	定義済みのアナライザサーバ ID を入力して、スイッチからデータを受信するデバイスを定義します。
Interval (20-120)	ポーリング間隔を設定します。この間隔が 0 に達するたびに、スイッチは「IF」カウンタのポーリングを行い、取得した情報は調査のために sFlow アナライザに送信される sFlow データに含められます。「Disabled」をチェックすると、このエントリのカウンタポーリングが無効になります。

「Apply」ボタンをクリックして、設定を有効にします。

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。

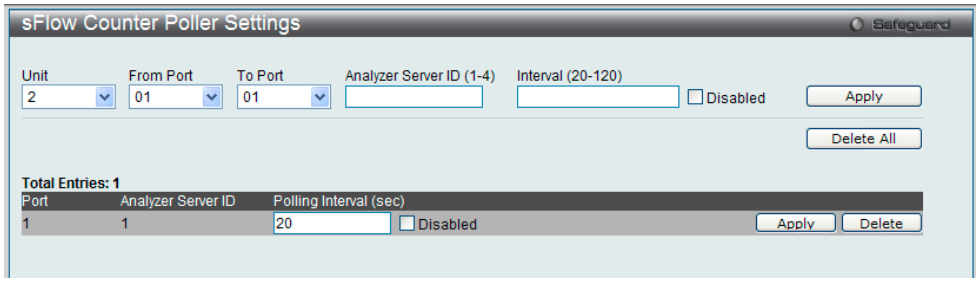


図 15-26 sFlow Counter Poller Settings 画面 - Edit

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）

Ping とは、指定した IP アドレスに ICMP Echo パケットを送信する簡単なプログラムです。送信先のノードは、送信元のスイッチに応答を返すか、送信されたパケットをエコーバックします。本機能はスイッチとネットワーク上の他のノードとの接続性を確認するために使用します。

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

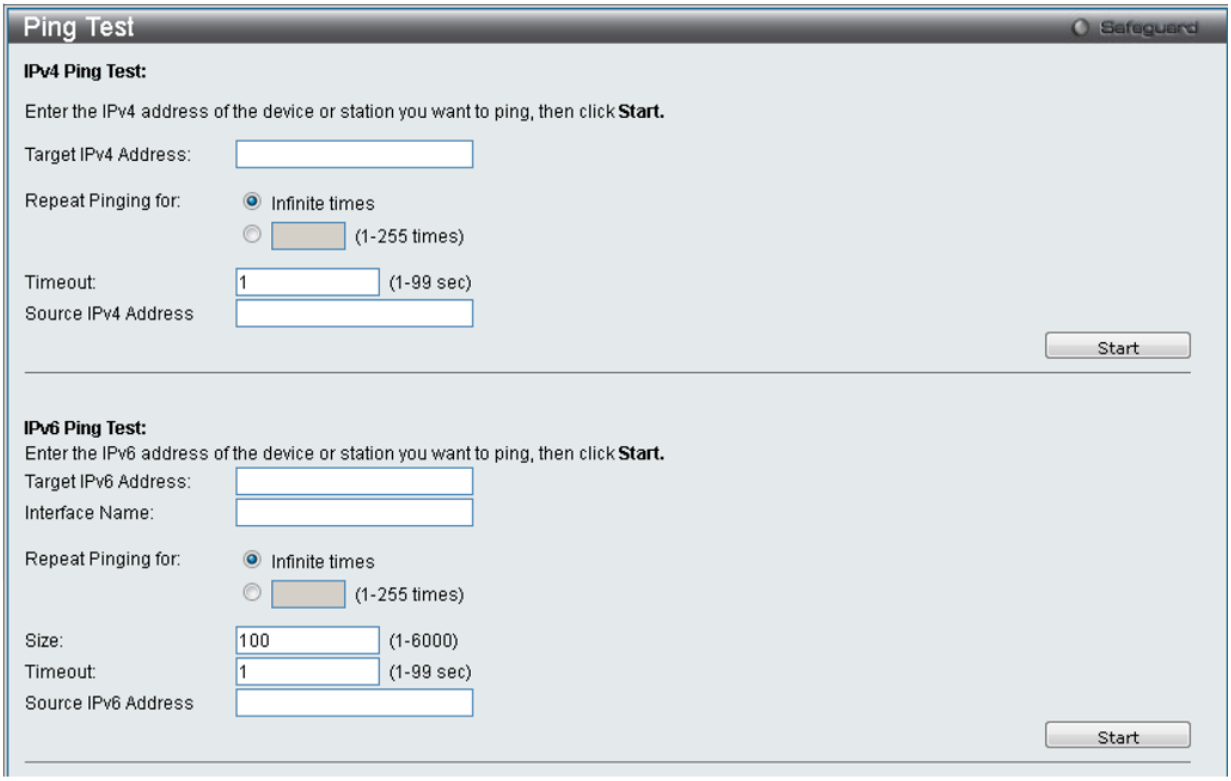


図 15-27 Ping Test 画面

「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 IPv4 Address	Ping される IP アドレスを入力します。
Target IPv6 Address	Ping される IP アドレスを入力します。
Repeat Pinging for	送信先 IP 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 のみ。1 から 6000 の間で指定します。初期値は 600 です。
Timeout	送信先への Ping メッセージの応答待ち時間（1-99）を入力します。 この時間内に応答パケットの検出に失敗すると、Ping パケットを破棄します。
Source IPv4 Address	「送信元 IPv4 アドレス」を入力します。」現在のスイッチがひとつ以上の IPv4 アドレスを保持している場合、そのうちのどれかを入力できます。入力した IPv4 アドレスは、リモートホストに送信されるパケットの送信元 IPv4 アドレスかプライマリ IP アドレスとして使用されます。
Source IPv6 Address	「送信元 IPv6 アドレス」を入力します。」現在のスイッチがひとつ以上の IPv6 アドレスを保持している場合、そのうちのどれかを入力できます。入力した IPv6 アドレスは、リモートホストに送信されるパケットの送信元 IPv6 アドレスかプライマリ IP アドレスとして使用されます。

「Start」ボタンをクリックし、Ping プログラムを開始します。

以下の結果画面が表示されます。

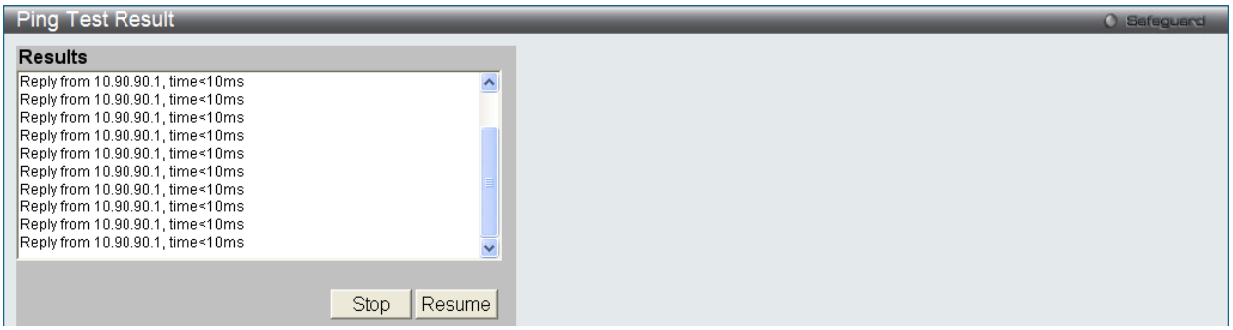


図 15-28 Ping Test Result 画面

「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）

パケットの経路をスイッチに到着する前に遡ってトレースすることができます。

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

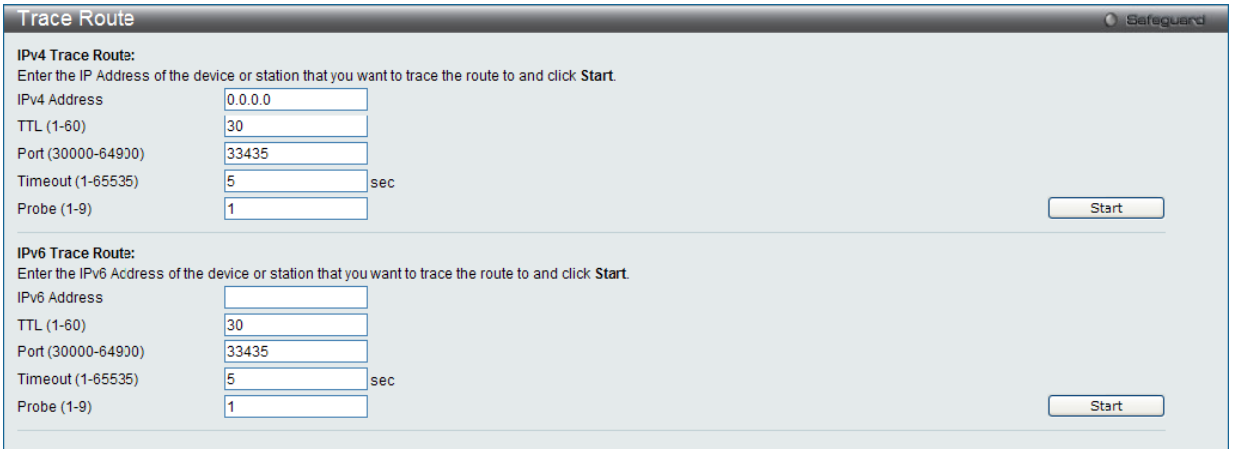


図 15-29 Trace Route 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IPv4 Address	宛先ステーションの IPv4 アドレス
IPv6 Address	宛先ステーションの IPv6 アドレス
TTL(1-60)	トレースルートリクエストの有効期間。２つのデバイス間のネットワークパスを検索する場合に traceroute コマンドが通過するルータの最大数です。
Port (30000-64900)	仮想ポート数。ポート番号は 1024 より大きな値で 30000 - 64900 で指定します。
Timeout (1-65535)	リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。1-65535（秒）で指定します。
Probe (1-9)	予定された traceroute パス上の次のホップに probe パケットをスイッチが送信する回数を指定します。初期値は 1 です。

「Start」ボタンをクリックし、Traceroute プログラムを開始します。

以下の結果画面が表示されます。

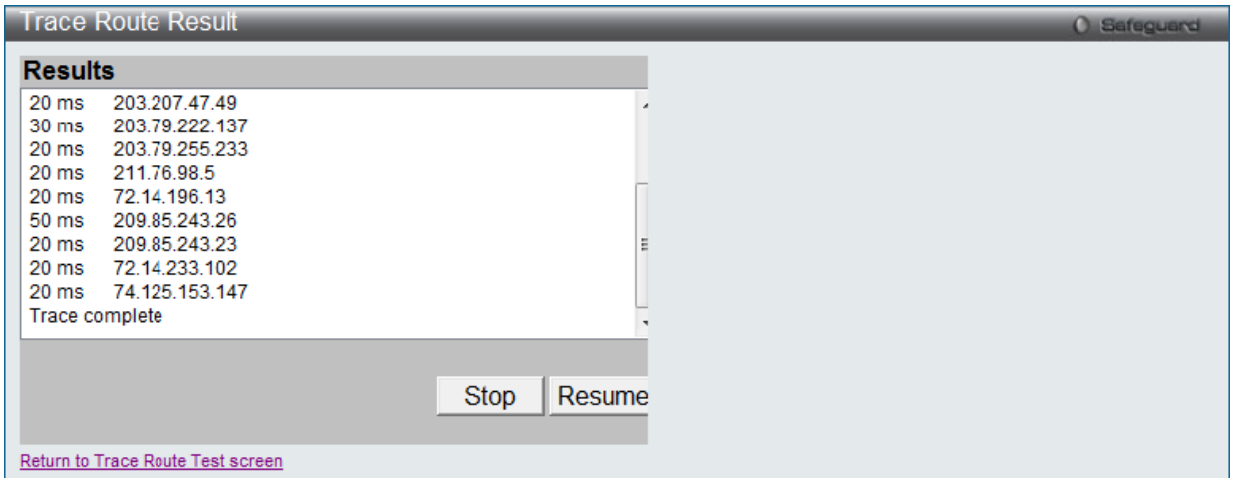


図 15-30 Trace Route Result 画面

「Stop」ボタンをクリックして、トレースルートを停止します。
「Resume」ボタンをクリックして、トレースルートを再開します。

Peripheral（周辺機器）

Device Environment（機器環境の確認）

本画面ではスイッチの内部温度状態を表示します。

Monitoring > Peripheral > Device Environment をクリックして次の画面を表示します。

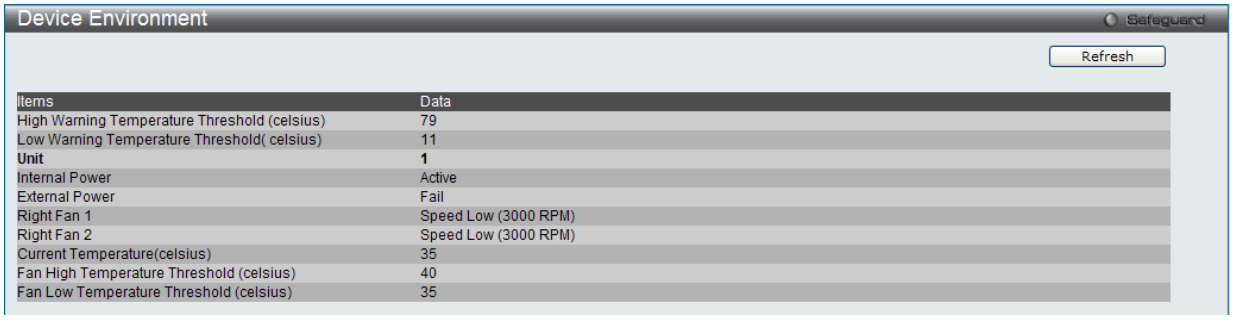


図 15-31 Device Environment 画面

「Refresh」をクリックして最新の状態に更新します。

第 16 章　Save and Tools（Save と Tools メニュー）

Web インタフェース画面左上部の「Save」「Tools」メニューを使用してスイッチの管理・設定を行います。

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

サブメニュー	説明	参照ページ
Save（コンフィグレーションとログの保存）		
Save Configuration / Log（コンフィグレーションとログの保存）	コンフィグレーションとログをスイッチに保存します。	371 ページ
Tools（ツールメニュー）		
License Management（ライセンス管理）	DLMS のアクティベーションコードをインストールして、表示します。	372 ページ
Stacking Information（スタック情報）	スイッチの初期状態のスタック情報を表示します。	372 ページ
Download Firmware（ファームウェアのダウンロード）	ファームウェアファイルをダウンロードします。	373 ページ
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。	374 ページ
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。	374 ページ
Upload Configuration（コンフィグレーションのアップロード）	コンフィグレーションファイルをアップロードします。	375 ページ
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。	376 ページ
Reset（リセット）	工場出荷時設定に戻し、メモリに保存します。	378 ページ
Reboot System（システムの再起動）	スイッチの再起動を行います。	378 ページ

Save（Save メニュー）

Save Configuration / Log（コンフィグレーション / ログの保存）

Web マネージャ先頭の **Save > Save Configuration / Log** をクリックし、以下の画面を表示します。

コンフィグレーションの保存

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Type」プルダウンメニューの「Configuration」を選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。

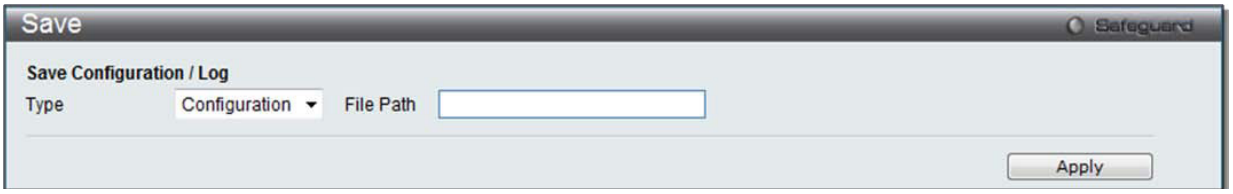


図 16-1　Save - Configuration 画面

ログの保存

「Save Log」では現在のログをスイッチに保存します。「Type」プルダウンメニューの「Log」を選択し、「Apply」ボタンをクリックします。

図 16-2　Save - Log 画面

全保存

「Save All」では変更したコンフィグレーションを永続的に保存します。このオプションではスイッチの再起動後も変更点について保存されます。「Type」プルダウンメニューの「All」を選択し「Apply」ボタンをクリックします。

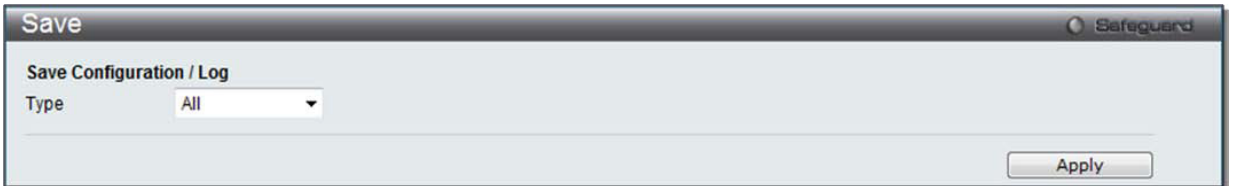


図 16-3　Save - All 画面

Tools（ツールメニュー）

License Management（ライセンス管理）

D-Link License Management System (DLMS) のアクティベーションコードをインストールして、表示します。

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。

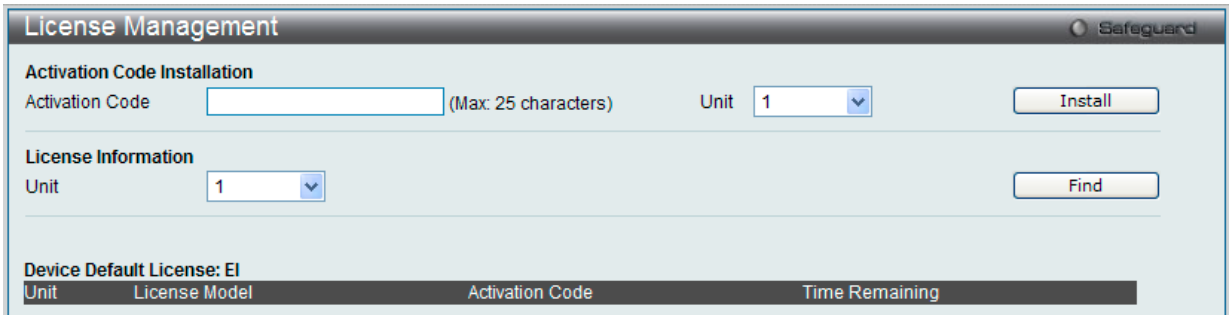


図 16-4　License Management 画面

以下の項目があります。

項目	説明
Activation Code	アクティベーションコードを入力します。
Unit	設定するユニットを選択します。

「Install」ボタンをクリックすると、DLMS アクティベーションコードをインストールします。
「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。

Stacking Information（スタック情報）

「Tools」プルダウンメニューの隣にスイッチスタック内のスイッチ数（最大 6 個）を表示します。アイコンは各ユニット番号と同じ順序となっており、Unit 番号 1 のスイッチはアイコングループの一番左上角のアイコンに対応しています。スタックモジュール（オプション）を経由してスイッチが相互接続する場合、スイッチスタックに関する情報は「Stack Information」に表示されます。

スイッチのスタック構成（例：スタックの順序）を変更させるには、**System Configuration > Stacking > Stacking Mode Settings** から設定します。

Tools > Stacking Information をクリックし、次の画面を表示します。

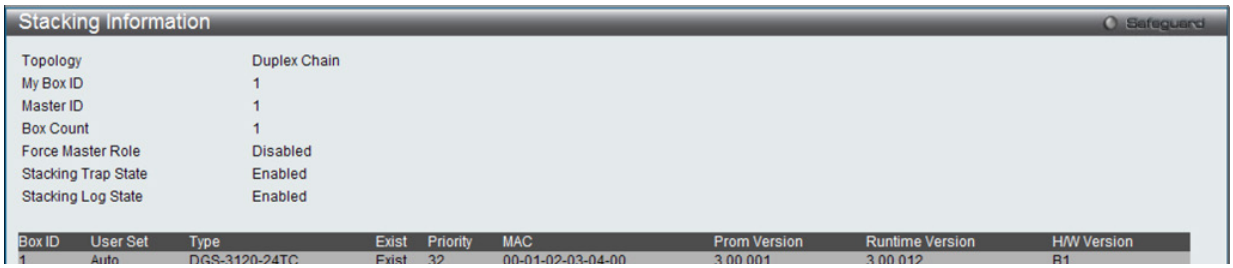


図 16-5　Stacking Information 画面

「Stacking Information」では次の情報について表示します。

項目	説明
Topology	本スイッチが採用されている現在のトポロジを表示します。
My Box ID	現在使用中のスイッチの「Box ID」を表示します。
Master ID	スイッチスタックのプライマリマスタのユニット ID を表示します。
Backup Master	スイッチスタックのバックアップマスタのユニット ID を表示します。
Box Count	スイッチスタック内のスイッチ数を表示します。
Box ID	スタック内のスイッチの順番を表示します。
User Set	スイッチ番号は自動的（Auto）またはスタティックに割り当てられます。初期値では「Auto」です。
Type	スタックないの関連スイッチの機種名を表示します。
Exist	スタック内に存在する / しないスイッチを表示します。
Priority	スイッチのプライオリティ ID を表示します。低番号ほど高優先値です。プライオリティ ID 値が一番低いスイッチ（ボックス）がプライマリマスタスイッチとして設定されます。
MAC	スイッチスタック内の関連スイッチの MAC アドレスを表示します。
Prom Version	スイッチに使用されている PROM を表示します。画像の値とは異なる場合もあります。
Runtime Version	スイッチのファームウェアバージョンを表示します。画像の値とは異なる場合もあります。
H/W Version	スイッチのハードウェアバージョンを表示します。画像の値とは異なる場合もあります。

Download Firmware（ファームウェアダウンロード）

スイッチにファームウェアをダウンロードします。
Tools > Download Firmware をクリックし、設定画面を表示します。

Download Firmware From TFTP（TFTP サーバからのファームウェアダウンロード）

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。

「Download Firmware From TFTP」を選択し、以下の画面を表示します。

図 16-6　Download Firmware - TFTP 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
Unit	更新するファームウェアを適用するユニットを選択します。「All」を選択すると全てのユニットに適用します。
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Source File	送信元ファイルの場所とファイル名を入力します。
Destination File	宛先ファイルの場所とファイル名を入力します。
Boot Up	ブートアップファイルとして設定します。

「Download」ボタンをクリックしてダウンロードを開始します。

Download Firmware From HTTP（HTTP サーバからのファームウェアダウンロード）

コンピュータからのファームウェアをダウンロード、スイッチの更新を行います。

「Download Firmware From HTTP」を選択し、以下の画面を表示します。

図 16-7　Download Firmware - HTTP 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
Unit	更新するファームウェアを適用するユニットを選択します。「All」を選択すると全てのユニットに適用します。
Destination File	宛先ファイルの場所とファイル名を入力します。
Source File	送信元ファイルの場所とファイル名を入力します。「参照」ボタンをクリックしダウンロードするファームウェアファイルを参照します。
Boot Up	ブートアップファイルとして設定します。

「Download」ボタンをクリックしてダウンロードを開始します。

Upload Firmware（ファームウェアアップロード）

TFTP サーバへのファームウェアアップロードを行います。

Upload Firmware To TFTP（TFTP サーバへのファームウェアアップロード）

Tools > Upload firmware をクリックし、設定画面を表示します。

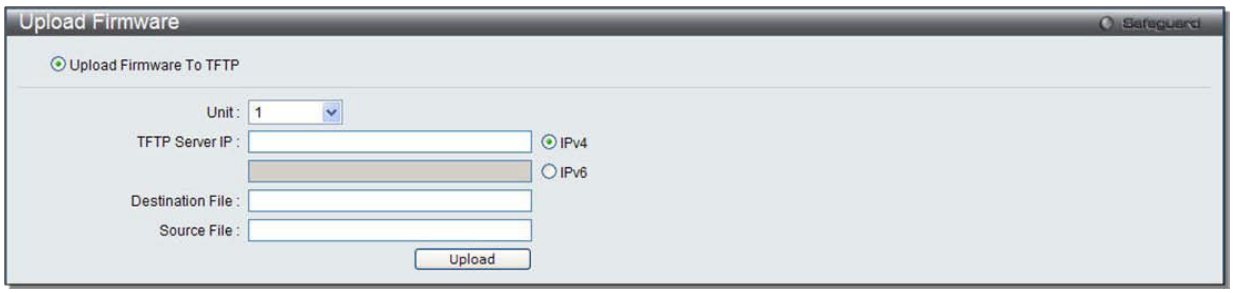


図 16-8　Upload Firmware - TFTP 画面

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
Unit	ファームウェアをアップロードするユニットを選択します。
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Destination File	宛先ファイルの場所とファイル名を入力します。
Source File	送信元ファイルの場所とファイル名を入力します。

「Upload」ボタンをクリックしてアップロードを開始します。

Download Configuration（コンフィグレーションダウンロード）

コンフィグレーションをダウンロードします。

Tools > Download Configuration をクリックし、設定画面を表示します。

Download Configuration From TFTP（TFTP サーバからのコンフィグレーションダウンロード）

TFTP サーバからのコンフィグレーションダウンロード、スイッチの設定更新を行います。

「Download Configuration From TFTP」を選択し、以下の画面を表示します。

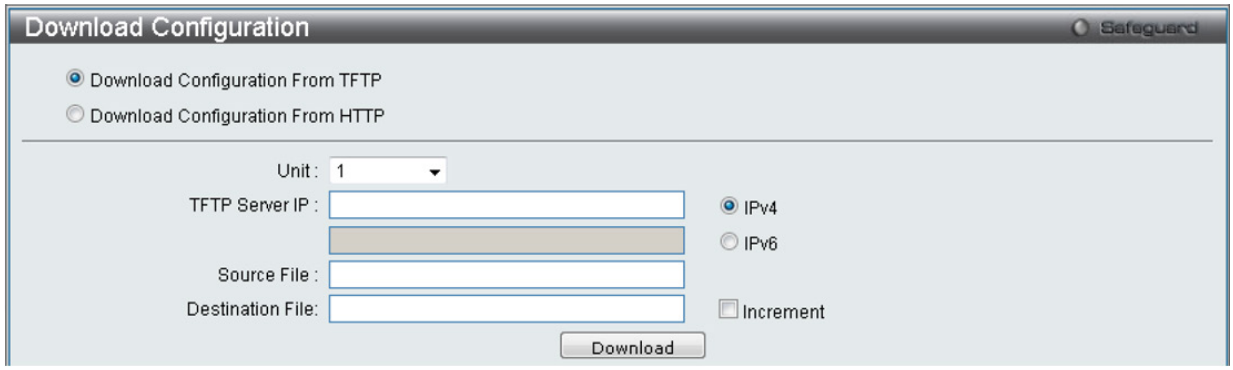


図 16-9　Download Configuration - TFTP 画面

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
Unit	更新するコンフィグレーションファイルを適用するユニットを選択します。「All」を選択すると全てのユニットに適用します。
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Source File	送信元ファイルの場所とファイル名を入力します。
Destination File	宛先ファイルの場所 (c:/) と " ファイル名 ".cfg を入力します。(入力例：c:/config.cfg) 尚、ファイルは (初期状態では)config.cfg として保存されています。
Increment	チェックを入れると既存のコンフィグレーションを新しいコンフィグレーションを適用する前に保存します。 チェックを外していると既存のコンフィグレーションは新しいコンフィグレーションを適用する前にクリアされます。

「Download」ボタンをクリックしてダウンロードを開始します。

Download Configuration From HTTP（HTTP サーバからのコンフィグレーションダウンロード）

コンピュータからのコンフィグレーションをダウンロード、スイッチの設定更新を行います。

「Download Configuration From HTTP」を選択し、以下の画面を表示します。

図 16-10 Download Configuration - HTTP 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
Unit	更新するファームウェアを適用するユニットを選択します。「All」を選択すると全てのユニットに適用します。
Destination File	宛先ファイルの場所とファイル名を入力します。
Source File	送信元ファイルの場所とファイル名を入力します。「参照」ボタンをクリックしダウンロードするファームウェアファイルを参照します。

「Download」ボタンをクリックしてダウンロードを開始します。

Upload Configuration（コンフィグレーションアップロード）

コンフィグレーションのアップロード方法について説明します。

Tools > Upload Configuration をクリックし、設定画面を表示します。

Upload Configuration To TFTP（TFTP サーバへのコンフィグレーションアップロード）

TFTP サーバへのコンフィグレーションアップロード、スイッチの設定更新を行います。

「Upload Configuration To TFTP」を選択し、以下の画面を表示します。

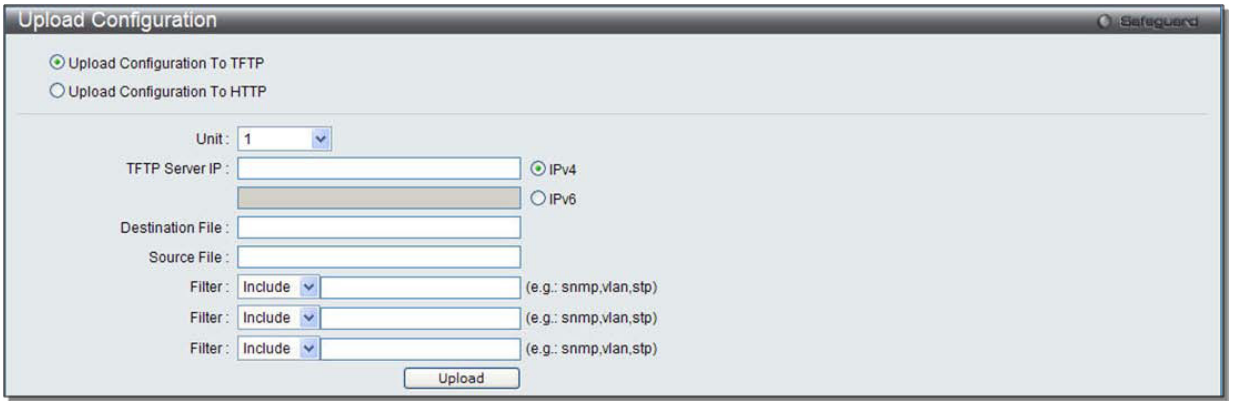


図 16-11 Upload Configuration - TFTP 画面

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
Unit	アップロードするコンフィグレーションファイルを適用するユニットを選択します。
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6- ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Destination File	宛先ファイルの場所とファイル名を入力します。
Source File	送信元ファイルの場所 (c:/) と " ファイル名 ".cfg を入力します。(入力例：c:/config.cfg) 尚、ファイルは (初期状態では)config.cfg として保存されています。
Filter	ドロップダウンメニューの「Include」「Begin」「Exclude」からフィルタ動作を選択し、対象となる SNMP や VLAN または STP などのフィルタの種類を入力します。

「Upload」ボタンをクリックしてアップロードを開始します。

Upload Configuration To HTTP（HTTP サーバへのコンフィグレーションアップロード）

コンピュータからのコンフィグレーションをアップロード、スイッチの設定更新を行います。

「Upload Configuration To HTTP」を選択し、以下の画面を表示します。

図 16-12 Upload Configuration - HTTP 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
Unit	アップロードするファームウェアを適用するユニットを選択します。「All」を選択すると全てのユニットに適用します。
Source File	送信元ファイルの場所とファイル名を入力します。

「Upload」ボタンをクリックしてアップロードを開始します。

Upload Log File（ログファイルのアップロード）

コンフィグレーションをアップロードします。

Tools > Upload Log File をクリックし、設定画面を表示します。

Upload Log To TFTP（TFTP サーバへのログファイルのアップロード）

TFTP サーバへのログファイルアップロード、スイッチの設定更新を行います。

「Upload Log To TFTP」を選択し、以下の画面を表示します。

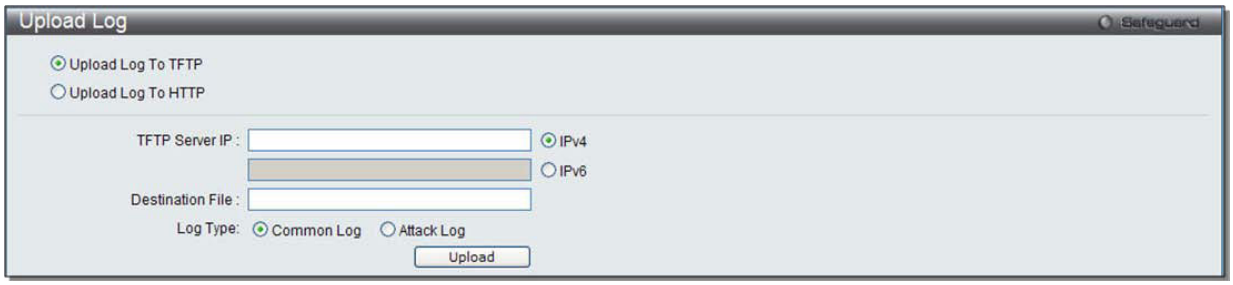


図 16-13 Upload Log - TFTP 画面

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
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Destination File	宛先ファイルの場所とファイル名を入力します。
Log Type	送信するログの種類を選択します。「Common Log」オプションを選択すると通常のログエントリをアップロードします。「Attack Log」オプションを選択すると攻撃関連のログをアップロードします。

「Upload」ボタンをクリックしてアップロードを開始します。

Upload Log To HTTP（HTTP サーバへのログファイルアップロード）

コンピュータからログファイルのアップロード行います。

「Upload Log To HTTP」を選択し、以下の画面を表示します。

図 16-14 Upload Log - HTTP 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
Log Type	送信するログの種類を選択します。「Common Log」オプションを選択すると通常のログエントリをアップロードします。 「Attack Log」オプションを選択すると攻撃関連のログをアップロードします。

「Upload」ボタンをクリックしてアップロードを開始します。

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。

「Reset」オプションはスイッチのユーザアカウント、ヒストリログ、「バナー」を除いて他のすべての設定を工場出荷時の初期設定に戻します。スイッチは、本画面を使用してリセットされ、「Save 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。

Tools > Reset をクリックし、次の設定画面を表示します。

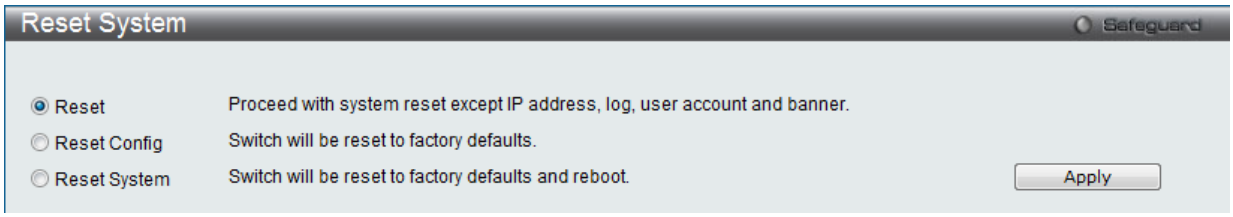


図 16-15　Reset System 画面

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（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

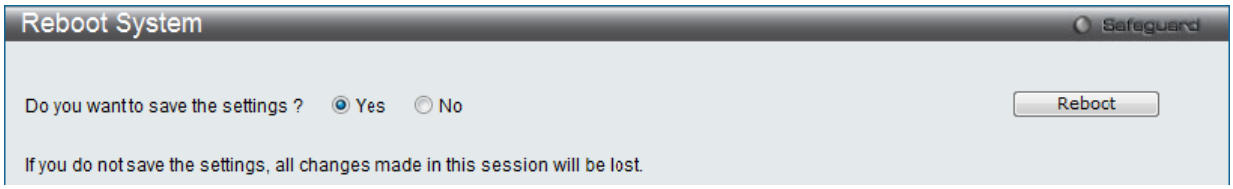


図 16-16　Reboot System 画面

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
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。

「Reboot」をクリックして再起動を開始します。

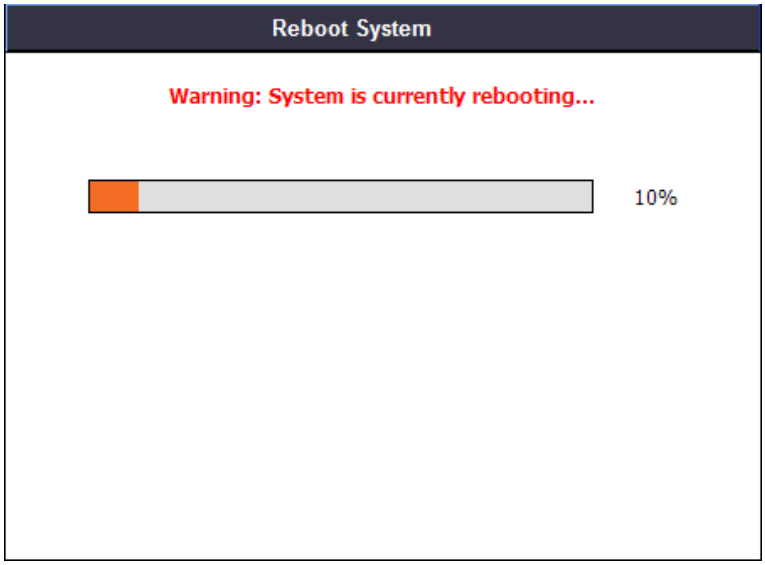


図 16-17　System Rebooting 画面

【付録 A】 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、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。

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 A-1 の通りです。

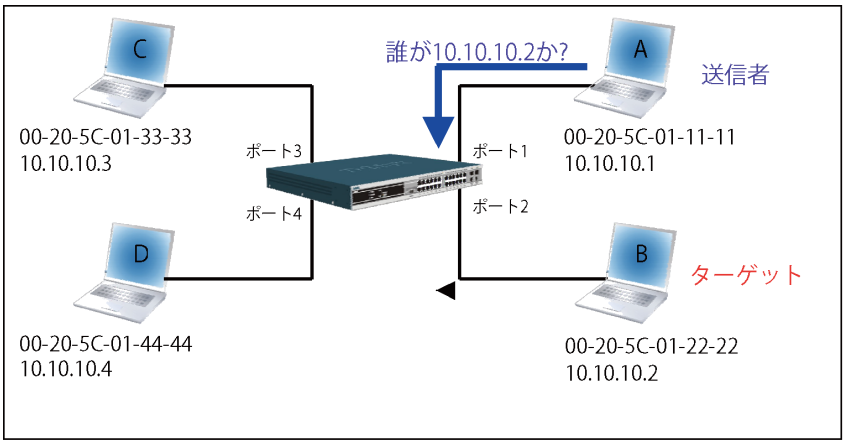


図 A-1

その間、PC-A の MAC アドレスは「送信側 H/W アドレス」に書かれ、その IP アドレスは ARP ペイロードの「送信側プロトコルアドレス」に書かれます。PC-B の MAC アドレスが未知である場合、「ターゲット H/W アドレス」は「00-00-00-00-00-00」であり、PC-B の IP アドレスは表 A-1 に示された「ターゲットプロトコルアドレス」に書かれます。

表 A-1　ARP ペイロード

H/W タイプ	プロトコルタイプ	H/W アドレス長	プロトコルアドレス長	操作	送信側 H/W アドレス	送信側プロトコルアドレス	ターゲット H/W アドレス	ターゲットプロトコルアドレス
				ARP request	00-20-5C-01-11-11	10.10.10.1	00-00-00-00-00-00	10.10.10.2

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。表 A-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。

表 A-2　イーサネットフレームフォーマット

宛先アドレス	送信元アドレス	Ether-type	ARP	FCS
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11			

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。

フォワーディングテーブル
ポート 1　00-20-5C-01-11-11

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 A-2 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。

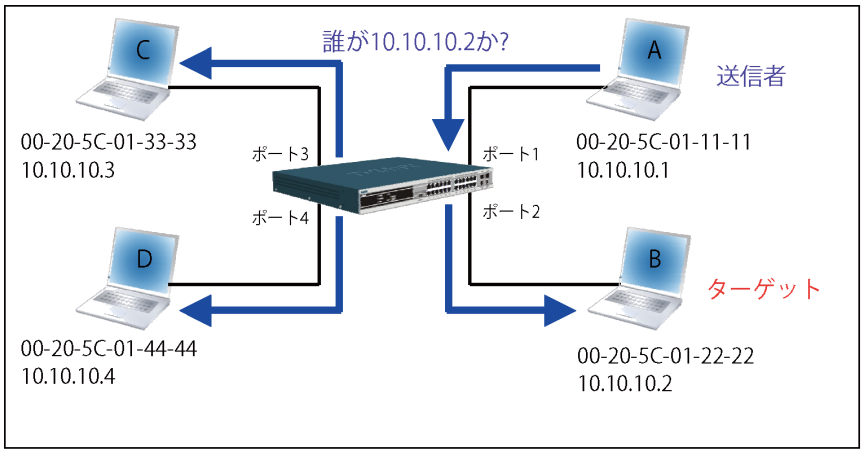


図 A-2

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 A-3 参照）。

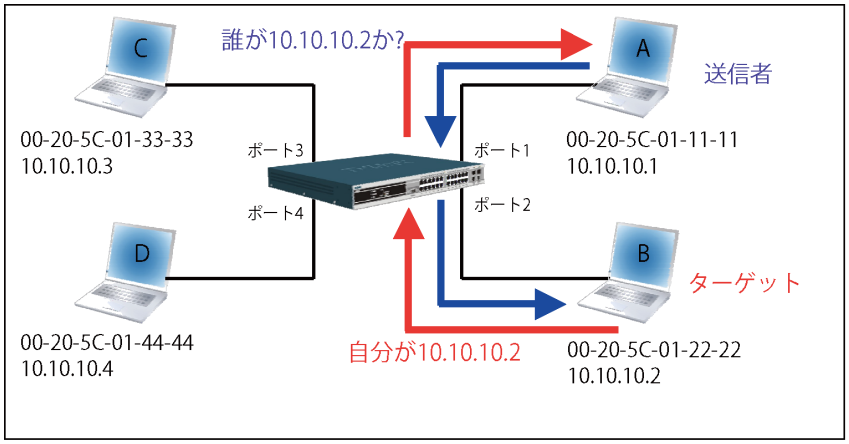


図 A-3

PC-B が ARP リクエストに応答すると、その MAC アドレスは表 A-3 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。

表 A-3　ARP ペイロード

H/W タイプ	プロトコルタイプ	H/W アドレス長	プロトコルアドレス長	操作	送信側 H/W アドレス	送信側プロトコルアドレス	ターゲット H/W アドレス	ターゲットプロトコルアドレス
				ARP reply	00-20-5C-01-11-11	10.10.10.1	00-20-5C-01-22-22	10.10.10.2

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（表 A-4 参照）。

表 A-4　イーサネットフレームフォーマット

宛先アドレス	送信元アドレス	Ether-type	ARP	FCS
00-20-5C-01-11-11	00-20-5C-01-22-22			

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。

フォワーディングテーブル	
ポート 1	00-20-5C-01-11-11
ポート 2	00-20-5C-01-22-22

ARP スプーフィングが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います。

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 A-4 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。

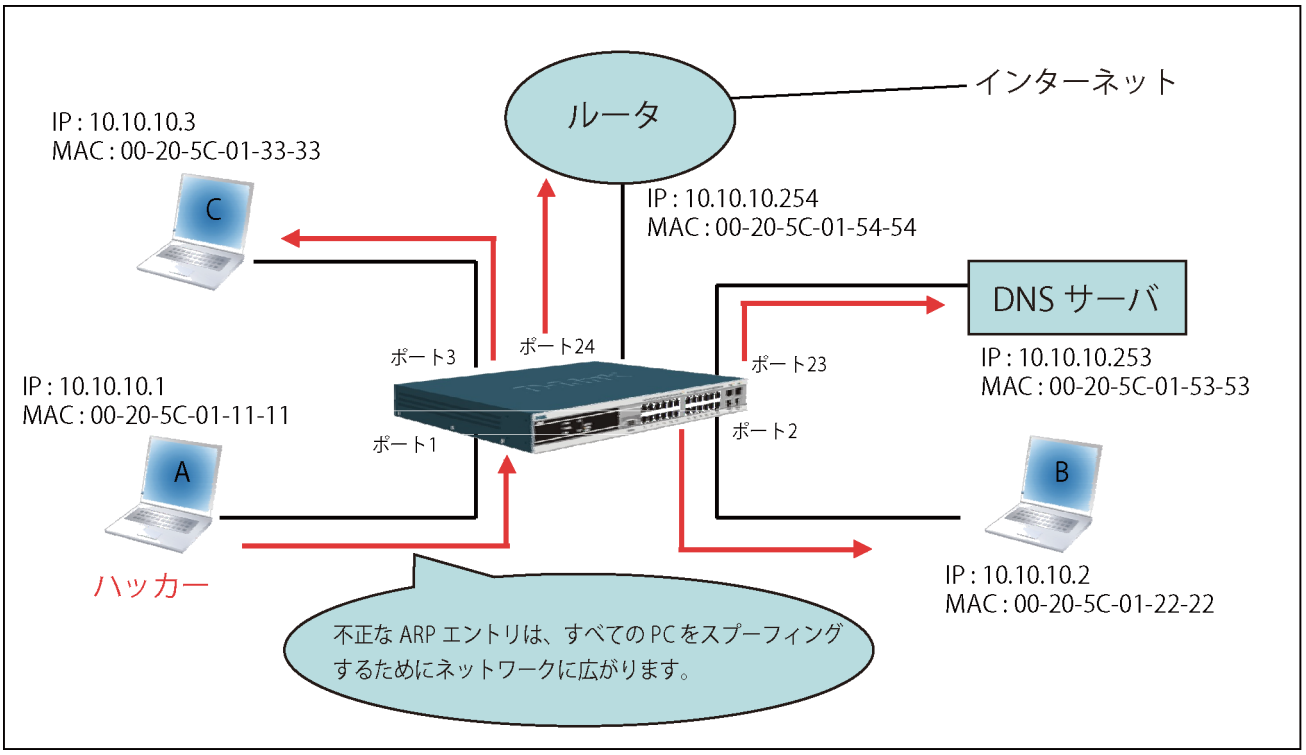


図 A-4

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。

表 A-5　Gratuitous ARP

イーサネットヘッダ			Gratuitous ARP								
宛先アドレス	送信元アドレス	イーサネットタイプ	H/W タイプ	プロトコルタイプ	H/W アドレス長	プロトコルアドレス長	操作	送信元 H/W アドレス	送信元プロトコルアドレス	ターゲット H/W アドレス	ターゲットプロトコルアドレス
6 バイト	6 バイト	2 バイト	2 バイト	2 バイト	1 バイト	1 バイト	2 バイト	6 バイト	4 バイト	6 バイト	4 バイト
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	806					ARP reply	00-20-5C-01-11-11	10.10.10.254	00-20-5C-01-11-11	10.10.10.254

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。
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 A-5 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。

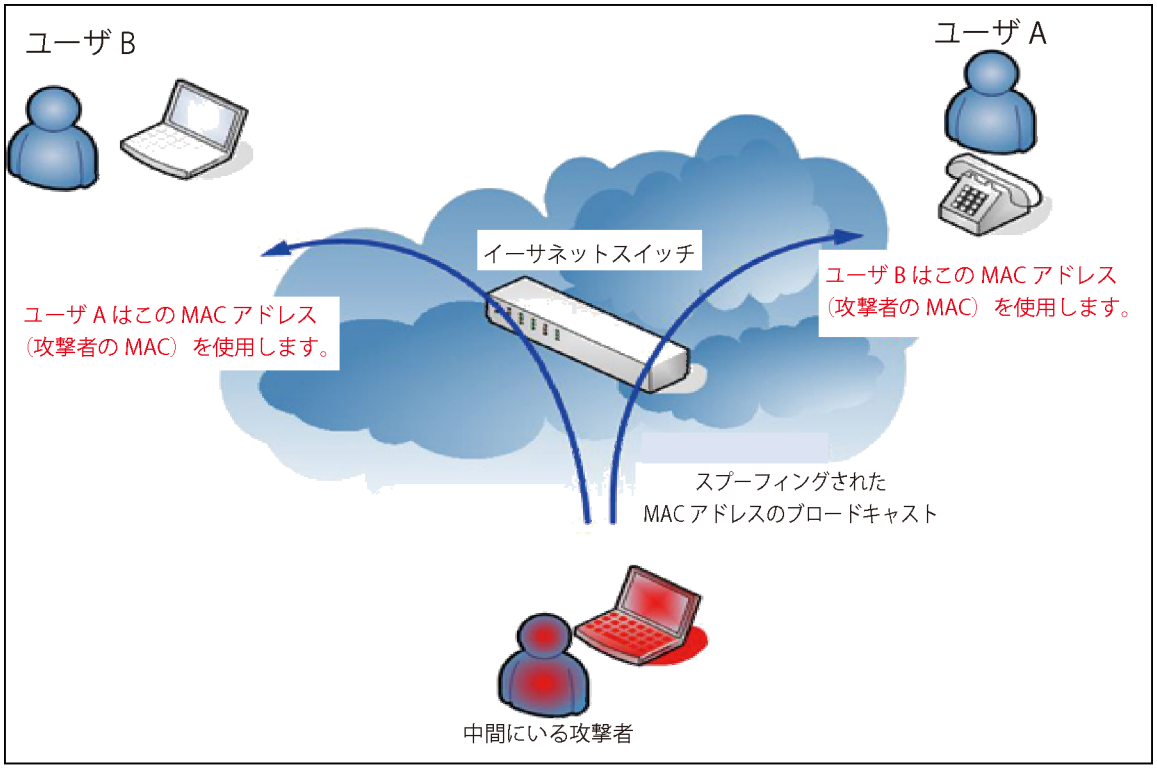


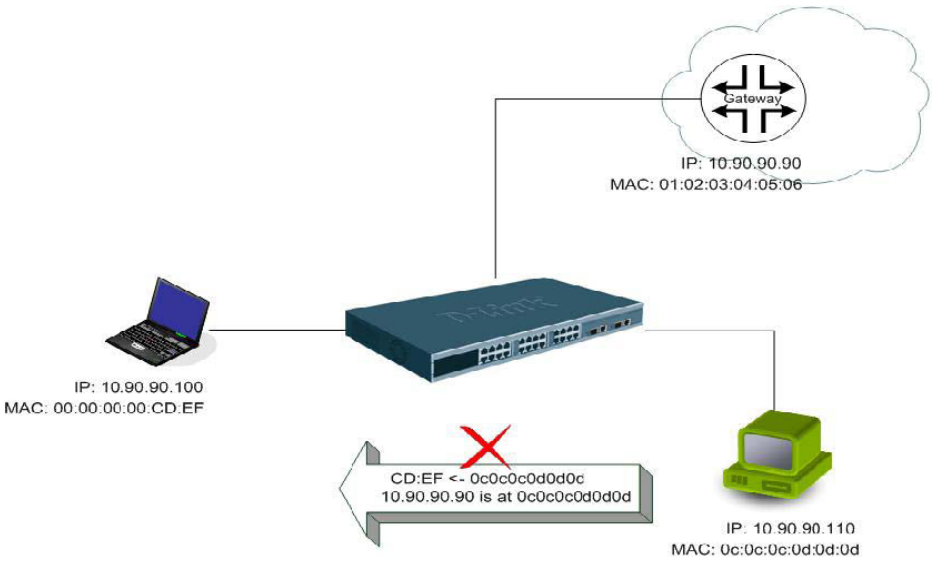
図 A-5

パケットコンテンツ ACL 経由で 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。

トポロジの例題



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 A-6 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 A-6　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。

表 A-7　イーサネットフレームに含まれる完全な ARP パケット

イーサネットヘッダ			ARP								
宛先アドレス	送信元アドレス	イーサネットタイプ	H/W タイプ	プロトコルタイプ	H/W アドレス長	プロトコルアドレス長	操作	送信元 H/W アドレス	送信元プロトコルアドレス	ターゲット H/W アドレス	ターゲットプロトコルアドレス
6 バイト	6 バイト	2 バイト	2 バイト	2 バイト	1 バイト	1 バイト	2 バイト	6 バイト	4 バイト	6 バイト	4 バイト
	01 02 03 04 05 06	0806							0a5a5a5a (10.90.90.90)		

	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 A-6 : 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 A-6 : 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 A-6 : 31/32 バイト目の茶色部分）
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 B】 パスワードリカバリ手順

ここでは、弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用することです。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「 ^ 」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                                                    V3.00.001
--------------------------------------------------------------------------------
Power On Self Test ..................................... 100%
MAC Address : 00-19-5B-EC-32-15
H/W Version : B1

Please wait, loading V3.00.007 Runtime image.............. 100%
UART init ................................................ 100 %
Starting runtime image
```

```
Password Recovery Mode
>
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
reset config {force_agree}	リセットし、全設定を工場出荷時設定に戻します。オプション「force_agree」は、ユーザの同意なしで全コンフィグレーションをリセットすることを意味します。
reboot {force_agree}	「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。オプション「force_agree」は、ユーザの同意なしで全コンフィグレーションをリセットすることを意味します。
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 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	イベントの説明	ログの内容	緊急度	摘要
システム	システム起動	Unit < ユニット ID>,System start up	Critical	
	システム起動（ウォーム）	Unit < ユニット ID>,System warm start	Critical	
	システム起動（コールド）	Unit < ユニット ID>,System cold start	Critical	
	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	Unit < ユニット ID>,Configuration saved to flash by console（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	フラッシュメモリへのシステムログファイル保存	Unit < ユニット ID>,System log saved to flash by console（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	フラッシュメモリへのコンフィグレーションとログファイル保存	Unit < ユニット ID>,Configuration and log saved to flash by console（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	内部電源異常	Unit < ユニット ID>,Internal Power failed	Critical	
	内部電源復旧	Unit < ユニット ID>,Internal Power is recovered	Critical	
	リダンダント電源異常	Unit < ユニット ID>,Redundant Power failed	Critical	
	リダンダント電源使用中	Unit < ユニット ID>,Redundant Power is working	Critical	
	サイドファンの異常	Unit < ユニット ID>,Side Fan failed	Critical	
	サイドファン回復	Unit < ユニット ID>,Side Fan recovered	Critical	
アップロード / ダウンロード	ファームウェアの更新成功	Unit < ユニット ID>,Firmware upgraded by console successfully（Username: < ユーザ名 >, IP: < IP アドレス >）	Informational	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	ファームウェアの更新失敗	Unit < ユニット ID>,Firmware upgraded by console was unsuccessful（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	コンフィグレーションファイルのダウンロード成功	Configuration successfully downloaded by console（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	コンフィグレーションファイルのダウンロード失敗	Configuration download by console was unsuccessful（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	コンフィグレーションファイルのアップロード成功	Configuration successfully uploaded by console（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	コンフィグレーションファイルのアップロード失敗	Configuration upload by console was unsuccessful!（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	ログメッセージのアップロード成功	Log message successfully uploaded by console（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	ログメッセージのアップロード失敗	Log message upload by console was unsuccessful!（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	コンソール経由でログインをしている場合は、IP 情報は表示されません。
	ファームウェアのアップロード成功	Firmware successfully uploaded by console (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	"console" と "IP: <IP アドレス >" は XOR（排他的論理和）です。これはコンソールでログインした場合、IP 情報は表示されません。
	ファームウェアのアップロード失敗	Firmware upload by console was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	"console" と "IP: <IP アドレス >" は XOR（排他的論理和）です。これはコンソールでログインした場合、IP 情報は表示されません。
インタフェース	ポートリンクアップ	Port < ユニット ID: ポート番号 > link up, < リンク状態 >	Informational	ポートリンク状態（例 : 100Mbps 全二重）
	ポートリンクダウン	Port< ユニット ID: ポート番号 > link down	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
スタッキング	ホットインサート	Unit< ユニット ID> MAC: <MAC アドレス > Hot insert	Informational	
	ホットリムーブ	Unit< ユニット ID> MAC: <MAC アドレス > Hot remove	Informational	
	スレーブへのファームウェア更新成功	Firmware upgraded to SLAVE by console successfully (Username: < ユーザ名 >)	Informational	
	スレーブへのファームウェア更新失敗	Firmware upgraded to SLAVE by console unsuccessfully! (Username: < ユーザ名 >)	Warning	
	スタッキングトポロジの変更	Stacking topology is <Stack_TP_TYPE>. Master(Unit< ユニット ID>, MAC:<MAC アドレス >)	Informational	
	バックアップマスタのマスタへの変更	Backup master changed to master. Master (Unit< ユニット ID>)	Informational	
	スレーブのマスタへの変更	Slave changed to master. Master (Unit< ユニット ID>)	Informational	
	ボックス ID の重複	Hot insert failed, box ID conflict: Unit< ユニット ID> conflict (MAC: <MAC アドレス > and MAC: <MAC アドレス >)	Critical	
コンソール	コンソール経由のログイン成功	Unit < ユニット ID>, Successful login through Console（Username: < ユーザ名 >）	Informational	コンソール経由でログインをしている場合は、IP や MAC アドレス情報は表示されません。
	コンソール経由のログイン失敗	Unit< ユニット ID>, Login failed through Console（Username: < ユーザ名 >）	Warning	コンソール経由でログインをしている場合は、IP や MAC アドレス情報は表示されません。
	コンソール経由でログアウト	Unit< ユニット ID>, Logout through Console（Username: < ユーザ名 >）	Informational	コンソール経由でログインをしている場合は、IP や MAC アドレス情報は表示されません。
	コンソールセッション、タイムアウト	Unit< ユニット ID>, Console session timed out（Username: < ユーザ名 >）	Informational	コンソール経由でログインをしている場合は、IP や MAC アドレス情報は表示されません。
Web	Web 経由のログイン成功	Successful login through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Web 経由のログイン失敗	Login failed through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	Web 経由でログアウト	Logout through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Web セッションタイムアウト	Web session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web（SSL）経由のログイン成功	Successful login through Web（SSL）（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Web（SSL）経由のログイン失敗	Login failed through Web（SSL）（Username: < ユーザ名 >, IP: <IP アドレス >, MAC: <MAC アドレス >）	Warning	
	Web（SSL）経由でログアウト	Logout through Web（SSL）（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Web（SSL）セッションタイムアウト	Web（SSL）session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
Telnet	Telnet 経由のログイン成功	Successful login through Telnet（SSL）（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet 経由のログイン失敗	Login failed through Telnet（SSL）（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	Telnet 経由でログアウト	Logout through Telnet（SSL）（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet セッションタイムアウト	Telnet session timed out（SSL）（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
SNMP	無効なコミュニティ名を含む SNMP request 受信	SNMP request received from <IP アドレス > with invalid community string!	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
STP	トポロジ変更	Topology changed(Instance:< インスタンス ID> ,Port:<[ユニット ID:] ポート番号 >,MAC:<MAC アドレス >)	Informational	
	新規ルートを選択	[CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: < インスタンス ID>]MAC: <MAC アドレス > Priority :< プライオリティ値 >)	Informational	
	スパニングツリープロトコル有効化	Spanning Tree Protocol is enabled	Informational	
	スパニングツリープロトコル無効化	Spanning Tree Protocol is disabled	Informational	
	新ルートポートの選択	New root port selected (Instance:< インスタンス ID>, port:<[ユニット ID:] ポート番号 >)	Notice	
	スパニングツリーポート状態の変更	Spanning Tree port status change (Instance:< インスタンス ID> , Port:<[ユニット ID:] ポート番号 >) <old_status> -> <new_status>	Notice	
	スパニングツリーポートロールの変更	Spanning Tree port role change (Instance:< インスタンス ID> , Port:< ユニット ID: ポート番号 >) < 旧ロール > -> < 新ロール >	Informational	
	スパニングツリーインスタンスの作成	Spanning Tree instance created (Instance:< インスタンス ID>)	Informational	
	スパニングツリーインスタンスの削除	Spanning Tree instance deleted (Instance:< インスタンス ID>)	Informational	
	スパニングツリーバージョンの変更	Spanning Tree version change (new version:< 新バージョン >)	Informational	
	スパニングツリー MST 設定 ID 名とリビジョンレベルの変更	Spanning Tree MST configuration ID name and revision level change (name:<ID 名 > ,revision level < 改訂レベル >).	Informational	
	スパニングツリー MST 設定 ID VLAN マッピングテーブルから VLAN の削除	Spanning Tree MST configuration ID VLAN mapping table change (instance: < インスタンス ID> delete vlan < 削除を開始する VLAN ID> [- < 削除終了する VLAN ID>])	Informational	
	スパニングツリー MST 設定 ID VLAN マッピングテーブルの追加	Spanning Tree MST configuration ID VLAN mapping table change (instance: < インスタンス ID> add vlan < 追加を開始する VLAN ID> [- < 追加を終了する VLAN ID>])	Informational	
DoS	スプーフィングアタック 1. 送信元 IP がスイッチと一致しているが MAC アドレスが異なる場合 2. ARP パケットの IP が送信元 IP と一致している場合 3. 自身の IP パケットが検出された場合	Possible spoofing attack from IP <IP アドレス > MAC<MAC アドレス > port < ポート番号 >	Critical	
	DoS アタック 1. 特定の DoS パケットが検出された場合	<dos 名 > is blocked from (IP: <IP アドレス > Port: <[ユニット ID:] ポート番号 >)	Informational	
SSH	SSH 経由のログイン成功	Successful login through SSH（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	SSH 経由のログイン失敗	Login failed through SSH（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	SSH 経由のログアウト	Logout through SSH（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	SSH セッションタイムアウト	SSH session timed out（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	SSH サーバ有効化	SSH server is enabled	Informational	
	SSH サーバ無効化	SSH server is disabled	Informational	
	クライアントパブリックキーのダウンロード成功	SSH client public keys file was upgraded successfully (Username: < ユーザ名 >, IP: < IP アドレス | IPv6 アドレス >)	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
AAA	認証ポリシー有効化	Authentication Policy is enabled (Module : AAA)	Informational	
	認証ポリシー無効化	Authentication Policy is disabled (Module : AAA)	Informational	
	AAA ローカルメソッドによるコンソール経由のログイン認証成功	Successful login through Console authenticated by AAA local method（Username: < ユーザ名 >）	Informational	
	AAA ローカルメソッドによるコンソール経由のログイン認証失敗	Login failed through Console authenticated by AAA local method（Username: < ユーザ名 >）	Warning	
	AAA ローカルメソッドによる Web 経由のログイン認証成功	Successful login through Web from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Informational	
	AAA ローカルメソッドによる Web 経由のログイン認証失敗	Login failed through Web from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Warning	
	AAA ローカルメソッドによる Web(SSL) 経由のログイン認証成功	Successful login through Web (SSL) from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Informational	
	AAA ローカルメソッドによる Web(SSL) 経由のログイン認証失敗	Login failed through Web (SSL) from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Warning	
	AAA ローカルメソッドによる Telnet 経由のログイン認証成功	Successful login through Telnet from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Informational	
	AAA ローカルメソッドによる Telnet 経由のログイン認証失敗	Login failed through Telnet from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Warning	
	AAA ローカルメソッドによる SSH 経由のログイン認証成功	Successful login through SSH from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Informational	
	AAA ローカルメソッドによる SSH 経由のログイン認証失敗	Login failed through SSH from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Warning	
	AAA none メソッドによるコンソール経由のログイン認証成功	Successful login through Console authenticated by AAA none method（Username: < ユーザ名 >）	Informational	
	AAA none メソッドによる Web 経由のログイン認証成功	Successful login through Web from < ユーザ IP> authenticated by AAA none method（Username: < ユーザ名 >）	Informational	
	AAA none メソッドによる Web(SSL) 経由のログイン認証成功	Successful login through Web (SSL) from < ユーザ IP> authenticated by AAA none method（Username: < ユーザ名 >）	Informational	
	AAA none メソッドによる Telnet 経由のログイン認証成功	Successful login through Telnet from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Informational	
	AAA none メソッドによる SSH 経由のログイン認証成功	Successful login through SSH from < ユーザ IP> authenticated by AAA local method（Username: < ユーザ名 >）	Informational	
	AAA サーバによるコンソール経由のログイン認証成功	Successful login through Console authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	コンソール経由でログインをしている場合は、IP や MAC アドレス情報は表示されません。
	AAA サーバによるコンソール経由のログイン認証失敗	Login failed through Console authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	コンソール経由でログインをしている場合は、IP や MAC アドレス情報は表示されません。
	AAA サーバタイムアウトまたは不正な設定によるコンソール経由のログイン失敗	Login failed through Console due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
AAA	AAA サーバによる Web 経由のログイン認証成功	Successful login through Web from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによる Web 経由のログイン認証失敗	Login failed through Web from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	
	AAA サーバタイムアウトまたは不正な設定による Web 経由のログイン認証失敗	Login failed through Web from < ユーザ IP> due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
	AAA サーバによる Web(SSL) 経由のログイン認証成功	Successful login through Web (SSL) from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによる Web(SSL) 経由のログイン認証失敗	Login failed through Web (SSL) from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	
	AAA サーバタイムアウトまたは不正な設定による Web(SSL) 経由のログイン認証失敗	Login failed through Web (SSL) from < ユーザ IP> due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
	AAA サーバによる Telnet 経由のログイン認証成功	Successful login through Telnet from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによる Telnet 経由のログイン認証失敗	Login failed through Telnet from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	
	AAA サーバタイムアウトまたは不正な設定による Telnet 経由のログイン認証失敗	Login failed through Telnet from < ユーザ IP> due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
	AAA サーバによる SSH 経由のログイン認証成功	Successful login through SSH from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによる SSH 経由のログイン認証失敗	Login failed through SSH from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	
	AAA サーバタイムアウトまたは不正な設定による SSH 経由のログイン認証失敗	Login failed through SSH from < ユーザ IP> due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
	AAA local_enable メソッドによるコンソール経由の Admin レベル遷移成功	Successful Enable Admin through Console authenticated by AAA local_enable method（Username: < ユーザ名 >）	Informational	
	AAA local_enable メソッドによるコンソール経由の Admin レベル遷移失敗	Enable Admin failed through Console authenticated by AAA local_enable method（Username: < ユーザ名 >）	Warning	
	AAA local_enable メソッドによる Web 経由の Admin レベル遷移成功	Successful Enable Admin through Web from < ユーザ IP> authenticated by AAA local_enable method（Username: < ユーザ名 >）	Informational	
	AAA local_enable メソッドによる Web 経由の Admin レベル遷移失敗	Enable Admin failed through Web from < ユーザ IP> authenticated by AAA local_enable method（Username: < ユーザ名 >）	Warning	
	AAA local_enable メソッドによる Web(SSL) 経由の Admin レベル遷移成功	Successful Enable Admin through Web (SSL) from < ユーザ IP> authenticated by AAA local_enable method（Username: < ユーザ名 >）	Informational	
	AAA local_enable メソッドによる Web(SSL) 経由の Admin レベル遷移失敗	Enable Admin failed through Web (SSL) from < ユーザ IP> authenticated by AAA local_enable method（Username: < ユーザ名 >）	Warning	
	AAA local_enable メソッドによる Telnet 経由の Admin レベル遷移成功	Successful Enable Admin through Telnet from < ユーザ IP> authenticated by AAA local_enable method（Username: < ユーザ名 >）	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
AAA	AAA local_enable メソッドによる Telnet 経由の Admin レベル遷移失敗	Enable Admin failed through Telnet from < ユーザ IP> authenticated by AAA local_enable method（Username: < ユーザ名 >）	Warning	
	AAA local_enable メソッドによる SSH 経由の Admin レベル遷移成功	Successful Enable Admin through SSH from < ユーザ IP> authenticated by AAA local_enable method（Username: < ユーザ名 >）	Informational	
	AAA local_enable メソッドによる SSH 経由の Admin レベル遷移失敗	Enable Admin failed through SSH from < ユーザ IP> authenticated by AAA local_enable method（Username: < ユーザ名 >）	Warning	
	AAA none メソッドによるコンソール経由の Admin レベル遷移成功	Successful Enable Admin through Console authenticated by AAA none method（Username: < ユーザ名 >）	Informational	
	AAA none メソッドによる Web 経由の Admin レベル遷移成功	Successful Enable Admin through Web from < ユーザ IP> authenticated by AAA none method（Username: < ユーザ名 >）	Informational	
	AAA none メソッドによる Web(SSL) 経由の Admin レベル遷移成功	Successful Enable Admin through Web (SSL) from < ユーザ IP> authenticated by AAA none method（Username: < ユーザ名 >）	Informational	
	AAA none メソッドによる Telnet 経由の Admin レベル遷移成功	Successful Enable Admin through Telnet from < ユーザ IP> authenticated by AAA none method（Username: < ユーザ名 >）	Informational	
	AAA none メソッドによる SSH 経由の Admin レベル遷移成功	Successful Enable Admin through SSH from < ユーザ IP> authenticated by AAA none method（Username: < ユーザ名 >）	Informational	
	AAA サーバによるコンソール経由の Admin レベル遷移成功	Successful Enable Admin through Console authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによるコンソール経由の Admin レベル遷移失敗	Enable Admin failed through Console authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	
	AAA サーバタイムアウトまたは不正な設定によるコンソール経由の Admin レベル遷移失敗	Enable Admin failed through Console due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
	AAA サーバによる Web 経由の Admin レベル遷移成功	Successful Enable Admin through Web from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによる Web 経由の Admin レベル遷移失敗	Enable Admin failed through Web from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	
	AAA サーバタイムアウトまたは不正な設定による Web 経由の Admin レベル遷移失敗	Enable Admin failed through Web from < ユーザ IP> due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
	AAA サーバによる Web(SSL) 経由の Admin レベル遷移成功	Successful Enable Admin through Web (SSL) from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによる Web(SSL) 経由の Admin レベル遷移失敗	Enable Admin failed through Web (SSL) from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	
	AAA サーバタイムアウトまたは不正な設定による Web(SSL) 経由の Admin レベル遷移失敗	Enable Admin failed through Web (SSL) from < ユーザ IP> due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
	AAA サーバによる Telnet 経由の Admin レベル遷移成功	Successful Enable Admin through Telnet from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによる Telnet 経由の Admin レベル遷移失敗	Enable Admin failed through Telnet from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
AAA	AAA サーバタイムアウトまたは不正な設定による Telnet 経由の Admin レベル遷移失敗	Enable Admin failed through Telnet from < ユーザ IP> due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
	AAA サーバによる SSH 経由の Admin レベル遷移成功	Successful Enable Admin through SSH from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Informational	
	AAA サーバによる SSH 経由の Admin レベル遷移失敗	Enable Admin failed through SSH from < ユーザ IP> authenticated by AAA server < サーバ IP>（Username: < ユーザ名 >）	Warning	
	AAA サーバタイムアウトまたは不正な設定による SSH 経由の Admin レベル遷移失敗	Enable Admin failed through SSH from < ユーザ IP> due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	
Port Security	ポートセキュリティの記録最大超過。新規アドレスは記録されません。	Port security violation (MAC address: <MAC アドレス > on port: <[ユニット ID:] ポート番号 >)	Warning	
RADIUS	RADIUS サーバは RADIUS クライアント認証後、VID を割り当てました。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 <IP アドレス > assigned VID :<VLAN ID> to port <[ユニット ID:] ポート番号 > (account :< ユーザ名 >)	Informational	
	RADIUS サーバは RADIUS クライアント認証後、Ingress 帯域を割り当てました。この Ingress 帯域はポートに割り当てられます。	RADIUS server <IP アドレス > assigned ingress bandwidth :<ingress 帯域 > to port <[ユニット ID:] ポート番号 > (account : < ユーザ名 >)	Informational	
	RADIUS サーバは RADIUS クライアント認証後、Egress 帯域を割り当てました。この Egress 帯域はポートに割り当てられます。	RADIUS server <IP アドレス > assigned egress bandwidth :<egress 帯域 > to port <[ユニット ID:] ポート番号 > (account: < ユーザ名 >)	Informational	
	RADIUS サーバは RADIUS クライアント認証後、802.1p デフォルトプライオリティを割り当てました。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 <IP アドレス > assigned 802.1p default priority:<priority> to port <[ユニット ID:] ポート番号 > (account : < ユーザ名 >)	Informational	
	RADIUS サーバは ACL プロファイル / ルールの割り当てに失敗しました。	RADIUS server <IP アドレス > assigns < ユーザ名 > ACL failure at port <[ユニット ID] ポート番号 > (< 文字列 >)	Warning	
802.1X	802.1X 認証失敗	802.1X Authentication failure [for < エラーの原因 >] from (Username: < ユーザ名 >, Port: <[ユニット ID:] ポート番号 >, MAC: <MAC アドレス >)	Warning	
	802.1X 認証成功	802.1X Authentication successful from (Username: < ユーザ名 >, Port: <[ユニット ID:] ポート番号 >, MAC: <MAC アドレス >)	Informational	
MAC ベースアクセスコントロール	ホストは認証に失敗しました。	MAC-based Access Control unauthenticated host(MAC: <MAC アドレス >, Port <[ユニット ID:] ポート番号 >, VID: <vid>)	Critical	
	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 <[ユニット ID:] ポート番号 > enters MAC-based Access Control stop learning state.	Warning	各ポート
	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。）	Port <[ユニット ID:] ポート番号 > recovers from MAC-based Access Control stop learning state.	Warning	各ポート

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
MAC ベースアクセスコントロール	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 enters stop learning state.	Warning	各システム
	デバイス全体の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 recovers from stop learning state.	Warning	各システム
	ホストは認証を通過しました。	MAC-based Access Control host login successful (MAC: <MAC アドレス >, port: <[ユニット ID] ポート番号 >, VID: <VLAN ID>)	Informational	
	ホストはエージングアウトします。	MAC-based Access Control host aged out (MAC: <MAC アドレス >, port: <[ユニット ID] ポート番号 >, VID: <VLAN ID>)	Informational	
JWAC	クライアントホストの認証成功	JWAC authenticated user (Username: < 文字列 >, IP: <IP アドレス | IP v6 アドレス >, MAC: <MAC アドレス >, Port: <[ユニット ID:] ポート番号 >)	Informational	
	クライアントホストの認証失敗	JWAC unauthenticated user (User Name: < 文字列 >, IP: <IP アドレス | IP v6 アドレス >, MAC: <MAC アドレス >, Port: <[ユニット ID:] ポート番号 >)	Warning	
	JWAC は学習停止状態に入りました。	JWAC enters stop learning state.	Warning	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。（各システム）
	JWAC は学習停止状態から回復しました。	JWAC recovered from stop learning state.	Warning	時間経過（5 分）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。（各システム）
WAC	クライアントホストの認証失敗	WAC unauthenticated user (Username: < 文字列 >, IP: <IPv4 アドレス | IPv6 アドレス >, MAC: <MAC アドレス >, Port: <[ユニット ID:] ポート番号 >)	Warning	
	クライアントは認証通過	WAC authenticated user (Username: < 文字列 >, IP: <IPv4 アドレス | IPv6 アドレス >, MAC: <MAC アドレス >, Port: <[ユニット ID:] ポート番号 >)	Informational	
	WAC は学習停止状態に入りました。	WAC enters stop learning state.	Warning	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。（各システム）
	WAC は学習停止状態から回復しました。	WAC recovers from stop learning state.	Warning	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。）（各システム）

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
IP-MAC ポートバインディング	IP-MAC ポートバインディング機能により、非認証の IP アドレスからのパケットを廃棄しました。	Unauthenticated IP-MAC address and discarded by IP mac port binding（IP: <IP アドレス >, MAC: <MAC アドレス >, Port : < ユニット ID: 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 と重複しています。	Dynamic IMPB entry is conflict with static ARP(IP: <IP アドレス >, MAC: <MAC アドレス >, Port <[ユニット ID:] 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 と重複しています。	Dynamic IMPB entry conflicts with static FDB(IP: <IP アドレス >, MAC: <MAC アドレス >, Port <[ユニット ID:] 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 と重複しています。	Dynamic IMPB entry conflicts with static IMPB: <IP アドレス >, MAC: <MAC アドレス >, Port <[ユニット ID:] ポート番号 >	Warning	
	ACL ルールがないため ACL モードに IMPB エントリを作成できません。	Creating IMPB entry failed due to no ACL rule being available(IP:<IP アドレス >, MAC: <MAC アドレス >, Port <[ユニット ID:] ポート番号 >)	Warning	
	DHCP レートがレート期限を越えたため、ポートがシャットダウンしました。	Port < [ユニット ID:] ポート番号 > is currently shut down due to the DHCP rate excludes the rate limiting	Warning	
	DHCP 自動リカバリタイマがタイムアウトしたため、ポートは復元しました。	Port < [ユニット ID:] ポート番号 > is currently recovery due to the DHCP auto- recovery timer is timeout	Informational	
IP とパスワード変更	IP アドレスの変更	Unit< ユニット ID>, Management IP address was changed by console(Username: < ユーザ名 >,IP:<IP アドレス >)	Informational	"console" と "IP: <IP アドレス >" は XOR（排他的論理和）です。これはコンソールでログインした場合、IP 情報は表示されません。
	パスワードの変更	Unit< ユニット ID>, Password was changed by console(Username: < ユーザ名 >,IP:<IP アドレス >)	Informational	"console" と "IP: <IP アドレス >" は XOR（排他的論理和）です。これはコンソールでログインした場合、IP 情報は表示されません。
セーフガードエンジン	セーフガードエンジン機能がノーマルモードに遷移しました。	Unit < ユニット ID>,SafeGuard Engine enters NORMAL mode	Informational	
	セーフガードエンジン機能がフィルタリングパケットモードに遷移しました。	Unit < ユニット ID>,Safeguard Engine enters EXHAUSTED mode	Warning	
パケットストーム	ブロードキャストストーム発生中。	Port < ユニット ID: ポート番号 > Broadcast storm is occurring	Warning	
	ブロードキャストストーム停止。	Port < ユニット ID: ポート番号 > Broadcast storm is cleared	Informational	
	マルチキャストストーム発生中。	Port < ユニット ID: ポート番号 > Multicast storm is occurring	Warning	
	マルチキャストストーム停止。	Port < ユニット ID: ポート番号 > Multicast storm is cleared	Informational	
	ストームのためにポートがシャットダウンしています。	Port < ユニット ID: ポート番号 > is currently shut down due to a packet storm	Warning	
ループバック検知（LBD）	ポートでループが発生	Port <[ユニット ID:] ポート番号 > LBD loop occurred. Port blocked	Critical	
	ポートでループが発生し、タイプアウト後にポートループ検知は再起動しました。	Port <[ユニット ID:] ポート番号 > LBD port recovered. Loop detection restarted	Informational	
	ポートで VID ループが発生。	Port <[ユニット ID:] ポート番号 > VID <VLAN ID> LBD loop occurred. Packet discard begun	Critical	
	ポートで VID ループが発生し、タイムアウト後にポートループ検知は再起動しました。	Port <[ユニット ID:] ポート番号 > VID <VLAN ID> LBD recovered. Loop detection restarted	Informational	
	複数の VLAN でループが発生しています。	Loop VLAN number overflow	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
Gratuitous ARP	IP コンフリクトの検出	Conflict IP was detected with this device (IP: <IP アドレス >, MAC: <MAC アドレス >, Port <[ユニット ID:] ポート番号 >, Interface: <ipif_name>).	Warning	
DHCP	信頼性の低い DHCP サーバの IP アドレスを検出	Detected untrusted DHCP server(IP: <IP アドレス >, Port: <[ユニット ID:] ポート番号 >)	Informational	DHCP サーバスクリーニング
BPDU 保護	BPDU アタックが発生	Port <[ユニット ID:] ポート番号 > enter BPDU under attacking state (mode: drop / block / shutdown)	Informational	
	BPDU アタックは自動的に回復	Port <[ユニット ID:] ポート番号 > recover from BPDU under attacking state automatically	Informational	
	BPDU アタックは手動で回復	Port <[ユニット ID:] ポート番号 > recover from BPDU under attacking state manually	Informational	
モニタ	温度が信頼レベルを超えています。	[Uint < ユニット ID>] Temperature Sensor < センサー ID> enter alarm state. (current temperature: < 温度 >)	Warning	
	温度が通常の値に戻りました。	[Uint < ユニット ID>] Temperature Sensor < センサー ID> recovers to normal state. (current temperature: < 温度 >)	Informational	
CFM	クロスコネクトを検出	CFM cross-connect. VLAN:<VLAN ID>, Local(MD Level:<mdlevel>, Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<MAC アドレス >)	Critical	
	エラー CFM CCM パケットを検出	CFM error ccm. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<MAC アドレス >)	Warning	
	リモート MEP の CCM パケットを受信できません	CFM remote down. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>)	Warning	
	リモート MEP の MAC がエラー状態をレポートしています。	CFM remote MAC error. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>)	Warning	
	リモートの MEP が CFM の欠陥を検出しました。	CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>)	Informational	
CFM 拡張	AIS 状態を検出	AIS condition detected. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
	AIS 状態が解消	AIS condition cleared. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
	LCK 状態を検出	LCK condition detected. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
	LCK 状態が解消	LCK condition cleared. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port <[ユニット ID:] ポート番号 >, Direction:<mepdirection>, MEPID:<mepid>)	Notice	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
音声 VLAN	新しい音声機器をポートに検出	New voice device detected (MAC:<MAC アドレス >,Port:<[ユニット ID:] ポート番号 >)	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 <[ユニット ID:] ポート番号 > add into voice VLAN <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。	Port <[ユニット ID:] ポート番号 > remove from voice VLAN <VLAN ID>	Informational	
ERPS	エラー信号を検出	Signal failure detected on node <MAC アドレス >	Notice	
	エラー信号がクリアされました。	Signal failure cleared on node <MAC アドレス >	Notice	
	RPL オーナが重複しています。	RPL owner conflicted on the ring <MAC アドレス >	Warning	
コマンドログ出力	コマンドログ	< ユーザ名 >: execute command "< 文字列 >".	Informational	
DDM	DDM アラームしきい値の超過、または回復	DDM Port <[ユニット ID:] ポート番号 > optic module [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 警告しきい値の超過、または回復	DDM Port <[ユニット ID:] ポート番号 > optic module [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	
LAC	リンクアグリゲーショングループのリンクダウンとリンクアップログ	Link aggregation Group <LAG インデックス > (Interface: <LAG インタフェースインデックス >) < リンク状態 >	Informational	
SD カード管理	コンフィグ実行エラー	Error when execute configuration < ファイル名 > line:< ライン番号 > at time < 時間範囲 >.	Warning	
	スケジュールバックアップ失敗	Backup < 種類 >:< ファイル名 > at time < 時間範囲 > failure.	Warning	
	コンフィグ実行成功	Execute configuration < ファイル名 > success at time < 時間範囲 >.	Informational	
	スケジュールバックアップ成功	Backup < 種類 >:< ファイル名 > success at time < 時間範囲 >.	Informational	
LLDP	LLDP-MED トポロジの変更が検出されました。	LLDP-MED topology change detected (on port < ポート番号 >. chassis id: < シャーシ種類 >, < シャーシ ID>, port id: < ポートタイプ >, < ポート ID>, device class: < デバイスクラス >)	notice	
	LLDP-MED デバイスタイプの重複が検出されました	Conflict LLDP-MED device type detected (on port < ポート番号 >, chassis id: < シャーシ種類 >, < シャーシ ID>, port id: < ポートタイプ >, < ポート ID>, device class: < デバイスクラス >)	notice	
	互換性のない LLDP-MED TLV が検出されました。	Incompatible LLDP-MED TLV set detected (on port < ポート番号 >, chassis id: < シャーシタイプ >, < シャーシ ID>, port id: < ポートタイプ >, < ポート ID>, device class: < デバイスクラス >)	notice	
サーベイランス VLAN	ポートに新しくサーベイランス機器が検出されました。	New surveillance device detected (Port < ポート番号 >, MAC <MAC アドレス >)	Informational	
	ポートのサーベイランス VLAN が有効であると、サーベイランス VLAN に自動的に参加します。	Port < ポート番号 > add into surveillance VLAN <VLAN ID >	Informational	
	ポートがサーベイランス VLAN から離脱し、同時にポートのエージングタイム内にサーベイランス VLAN が検出されない場合に、本ログメッセージが送信されます。	Port < ポート番号 > remove from surveillance VLAN <VLAN ID >	Informational	

【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。

ハードウエアバージョン A1、A2 のトラップログ

トラップ名	説明	OID
swL2macNotification	アドレステーブル内の MAC アドレスの変化を示します。 関連トラップ： swL2macNotifyInfo	1.3.6.1.4.1.171.11.117.1.1.2.100.1.2.0.1 (DGS-3120-24TC) 1.3.6.1.4.1.171.11.117.1.2.2.100.1.2.0.1 (DGS-3120-24PC) 1.3.6.1.4.1.171.11.117.1.3.2.100.1.2.0.1 (DGS-3120-24SC) 1.3.6.1.4.1.171.11.117.1.4.2.100.1.2.0.1 (DGS-3120-48TC) 1.3.6.1.4.1.171.11.117.1.5.2.100.1.2.0.1 (DGS-3120-48PC) 1.3.6.1.4.1.171.11.117.1.6.2.100.1.2.0.1 (DGS-3120-24SC-DC)
swL2PortSecurityViolationTrap	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。 関連トラップ： 1: swL2PortSecurityPortIndex 2: swL2PortSecurityViolationMac	1.3.6.1.4.1.171.11.117.1.1.2.100.1.2.0.2 (DGS-3120-24TC) 1.3.6.1.4.1.171.11.117.1.2.2.100.1.2.0.2 (DGS-3120-24PC) 1.3.6.1.4.1.171.11.117.1.3.2.100.1.2.0.2 (DGS-3120-24SC) 1.3.6.1.4.1.171.11.117.1.4.2.100.1.2.0.2 (DGS-3120-48TC) 1.3.6.1.4.1.171.11.117.1.5.2.100.1.2.0.2 (DGS-3120-48PC) 1.3.6.1.4.1.171.11.117.1.6.2.100.1.2.0.2 (DGS-3120-24SC-DC)
swIpMacBindingViolationTrap （EI モードのみ）	IP-MAC Binding トラップが有効の時、事前に設定したポートセキュリティに違反する MAC があるとトラップを送信します。 関連トラップ： 1: swIpMacBindingPortIndex 2: swIpMacBindingViolationIP 3: swIpMacBindingViolationMac	1.3.6.1.4.1.171.12.23.5.0.1
swIpMacBindingIPv6ViolationTrap （EI モードのみ）	IP-MAC Binding トラップが有効の時、定義済みの IPv6 IMPB 設定に違反する新しい MAC があると、トラップを送信します。 関連トラップ： 1: swIpMacBindingPortIndex 2: swIpMacBindingViolationIPv6Addr 3: swIpMacBindingViolationMac	1.3.6.1.4.1.171.12.23.5.0.4
swIpMacBindingShutdownTrap （EI モードのみ）	レートリミットがシャットダウンモードで DHCP レートがリミットを越えた場合、トラップを送信します。 関連トラップ： 1: swIpMacBindingPortIndex	1.3.6.1.4.1.171.12.23.5.0.5
swIpMacBindingRecoveryTrap （EI モードのみ）	ポートが DHCP レートリミットによってシャットダウンされていて、自動リカバリタイマがタイムアウトしていると、トラップを送信します。 関連トラップ： 1: swIpMacBindingPortIndex	1.3.6.1.4.1.171.12.23.5.0.6
swPktStormOccurred	パケットストームのメカニズムがパケットストームを検知し遮断した時に、本トラップは送信されます。 関連トラップ：swPktStormCtrlPortIndex	1.3.6.1.4.1.171.12.25.5.0.1

トラップ名	説明	OID
swPktStormCleared	パケットストームのメカニズムにより、パケットストームが消去された時に、本トラップは送信されます。 関連トラップ：swPktStormCtrlPortIndex	1.3.6.1.4.1.171.12.25.5.0.2
swPktStormDisablePort	パケットストームのメカニズムによってポートが無効になっています。 関連トラップ： 1:swPktStormCtrlPortIndex 2: swPktStormNotifyPktType	1.3.6.1.4.1.171.12.25.5.0.3
SafeGuardChgToExhausted	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。	1.3.6.1.4.1.171.12.19.4.1.0.1
SafeGuardChgToNormal	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。	1.3.6.1.4.1.171.12.19.4.1.0.2
agentGratuitousARPTrap	IP アドレスの競合が発生している時、本トラップは送信されます。 関連トラップ： 1. agentGratuitousARPIpAddr 2. agentGratuitousARPMacAddr 3. agentGratuitousARPPortNumber 4. agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.12.1.7.2.0.5
swDoSAttackDetected	指定の DoS パケットを受信しトラップが有効な時に、本トラップは送信されます。 関連トラップ： 1. swDoSCtrlType 2. swDoSNotifyVarIpAddr 3. swDoSNotifyVarPortNumber	1.3.6.1.4.1.171.12.59.4.0.1
swMacBasedAccessControlLoggedSuccess	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、本トラップを送信します。 関連トラップ： 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.1
swMacBasedAccessControlLoggedFail	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、本トラップを送信します。 関連トラップ： 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.2
swMacBasedAccessControlAgesOut	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、本トラップを送信します。 関連トラップ： 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.3
swFilterDetectedTrap	不正な DHCP サーバが検出された時、送信されます。ログが認証を止めている期間は、同じ不正な DHCP サーバの IP アドレスが検出されても、送信されるのは一度のみです。 関連トラップ： 1. swFilterDetectedIP 2. swFilterDetectedport	1.3.6.1.4.1.171.12.37.100.0.1
swPortLoopOccurred	ポートにループが発生すると、本トラップを送信します。 関連トラップ：swLoopDetectPortIndex	1.3.6.1.4.1.171.12.41.10.0.1
swPortLoopRestart	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。 関連トラップ：swLoopDetectPortIndex	1.3.6.1.4.1.171.12.41.10.0.2

トラップ名	説明	OID
swVlanLoopOccurred	VLAN に所属するポートにループが発生すると、本トラップを送信します。 関連トラップ： 1. swLoopDetectPortIndex 2. swVlanLoopDetectVID	1.3.6.1.4.1.171.12.41.10.0.3
swVlanLoopRestart	VLAN に所属する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。 関連トラップ： 1. swLoopDetectPortIndex 2. swVlanLoopDetectVID	1.3.6.1.4.1.171.12.41.10.0.4
swBpduProtectionUnderAttackingTrap	BPDU 防御トラップが有効の時、指定ポートが「normal」から「under attack」に変化した場合、本トラップは送信されます。 関連トラップ： 1. swBpduProtectionPortIndex 2. swBpduProtectionPortMode	1.3.6.1.4.1.171.12.76.4.0.1
swBpduProtectionRecoveryTrap	BPDU 防御トラップが有効の時、指定ポートが「under attack」から「normal」に変化した場合、本トラップは送信されます。 関連トラップ： 1. swBpduProtectionPortIndex 2. swBpduProtectionPortMode	1.3.6.1.4.1.171.12.76.4.0.2
swERPSSFDetectedTrap （EI モードのみ）	信号障害の発生時にトラップは生成されます。 関連トラップ：swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.1
swERPSSFClearedTrap （EI モードのみ）	信号障害が解消するとトラップは生成されます。 関連トラップ：swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.2
swERPSRPLOwnerConflictTrap （EI モードのみ）	競合が発生した時、本トラップが発生します。 関連トラップ：swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.3
dot1agCfmFaultAlarm （EI モードのみ）	MEP が持続性欠損状態です。マネジメントエントリに欠損が検出された MEP について OID と共に通知（失敗の警告）が送信されます。 関連トラップ：dot1agCfmMepHighestPrDefect	1.3.111.2.802.1.1.8.0.1
swCFMExtAISOccurred （EI モードのみ）	ローカル MEP が AIS 状態です。 関連トラップ： 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.1
swCFMExtAISCleared （EI モードのみ）	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。 関連トラップ： 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.2
swCFMExtLockOccurred （EI モードのみ）	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。 関連トラップ： 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.3
swCFMExtLockCleared （EI モードのみ）	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。 関連トラップ： 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.4
swFanFailure	ファンエラーの通知です。 関連トラップ： 1. swFanUnitIndex 2. swFanID	1.3.6.1.4.1.171.12.11.2.2.3.0.1

トラップ名	説明	OID
swFanRecover	ファンエラーから回復した通知です。 関連トラップ： 1. swFanUnitIndex 2. swFanID	1.3.6.1.4.1.171.12.11.2.2.3.0.2
swHighTemperature	高温状態の通知です。 関連トラップ： 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.1
swHighTemperatureRecover	高温状態が解消されると生成されます。 関連トラップ： 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.2
swLowTemperature	低温状態の通知です。 関連トラップ： 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.3
swLowTemperatureRecover	低温状態が解消されると生成されます。 関連トラップ： 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.4
agentFirmwareUpgrade	SNMP 経由のファームウェア更新が終了した通知です。 関連トラップ：swMultiImageVersion	1.3.6.1.4.1.171.12.1.7.2.0.7
agentCfgOperCompleteTrap	コンフィグレーションの保存、アップロード、ダウンロード完了の通知です。 関連トラップ： 1. unitID 2. agentCfgOperate 3. agentLogin ユーザ名	1.3.6.1.4.1.171.12.1.7.2.0.9
swPowerFailure	電源障害、停電の通知です。 関連トラップ： 1. swPowerUnitIndex 2. swPowerID 3. swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.2
swPowerRecover	電源障害、停電から復帰の通知です。 関連トラップ： 1. swPowerUnitIndex 2. swPowerID 3. swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.3
swUnitInsert	ユニットがホットインサートされた通知です。 関連トラップ： 1. swUnitMgmtId 2. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.1
swUnitRemove	ユニットがホットリムーブされた通知です。 関連トラップ： 1. swUnitMgmtId 2. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.2
swUnitFailure	ユニットに異常が発生しています。 関連トラップ：swUnitMgmtId	1.3.6.1.4.1.171.12.11.2.2.1.0.3

トラップ名	説明	OID
swUnitTPChange	スタッキングトポロジの変更通知です。 関連トラップ： 1. swStackTopologyType 2. swUnitMgmtId 3. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.4
swUnitRoleChange	スタッキングユニット変更通知です。 関連トラップ： 1. swStackRoleChangeType 2. swUnitMgmtId	1.3.6.1.4.1.171.12.11.2.2.1.0.5
lldpRemTablesChange	lldpStatsRemTableLastChangeTime の値が変化した時トラップを送信します。 関連トラップ： 1. lldpStatsRemTablesInserts 2. lldpStatsRemTablesDeletes 3. lldpStatsRemTablesDrops 4. lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
lldpXMedTopologyChangeDetected	新しいリモートデバイスがローカルポートに接続、またはリモートデバイスの切断、ポート移動などのトポロジの変更をローカルデバイスが検知した通知です。 関連トラップ： 1. lldpRemChassisIdSubtype 2. lldpRemChassisId 3. lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1
swDdmAlarmTrap （EI モードのみ）	トラップアクションの設定に基づいて、パラメータの値がアラームしきい値を超えると本トラップは送信されます。 関連トラップ： 1. swDdmPort 2. swDdmThresholdType 3. swDdmThresholdExceedType 4. swDdmThresholdExceedOrRecover	1.3.6.1.4.1.171.12.72.4.0.1
swDdmWarningTrap （EI モードのみ）	トラップアクションの設定に基づいて、パラメータの値が警告しきい値を超えると本トラップは送信されます。 関連トラップ： 1. swDdmPort 2. swDdmThresholdType 3. swDdmThresholdExceedType 4. swDdmThresholdExceedOrRecover	1.3.6.1.4.1.171.12.72.4.0.2
dot3OamNonThresholdEvent （EI モードのみ）	しきい値のないローカル / リモートイベントが検出された通知です。しきい値のないイベントを示す「Ethernet OAM Event Notification OAMPDU」の受信によりリモートイベントは検出され、ローカルエンティティによりローカルイベントは検出されます。 関連トラップ： 1. dot3OamEventLogTimestamp 2. dot3OamEventLogOui 3. dot3OamEventLogType 4. dot3OamEventLogLocation 5. dot3OamEventLogEventTotal	1.3.6.1.2.1.158.0.2
swSingleIPMSLinkDown	Commander スイッチは、メンバがリンクダウン通知を生成する場合に指定ホストに swSingleIPMSLinkDown 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr 3.ifIndex	1.3.6.1.4.1.171.12.8.6.0.13

トラップ名	説明	OID
swSingleIPMSLinkUp	Commander スイッチは、メンバがリンクアップ通知を生成する場合に指定ホストに swSingleIPMSLinkUp 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr 3.ifIndex	1.3.6.1.4.1.171.12.8.6.0.14
swSingleIPMSAuthFail	Commander スイッチは、メンバが認証エラー通知を生成する場合に指定ホストに swSingleIPMSAuthFail 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.15
swSingleIPMSnewRoot	Commander スイッチは、メンバが新しいルート通知を生成する場合に指定ホストに swSingleIPMSnewRoot 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.16
swSingleIPMSTopologyChange	Commander スイッチは、メンバがトポロジの変更通知を生成する場合に指定ホストに swSingleIPMSTopologyChange 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.17
coldStart	coldStart トラップは、送信側のプロトコルエンティティがエージェントの設定またはプロトコルエンティティの実行を変更するように再初期化することを意味します。	1.3.6.1.6.3.1.1.5.1
warmStart	warmStart トラップは、送信側のプロトコルエンティティがエージェントの設定またはプロトコルエンティティのどちらの実行も変更しないように再初期化することを意味します。	1.3.6.1.6.3.1.1.5.2
linkDown	linkDown トラップは、送信側のプロトコルエンティティがエージェントの設定内にある通信リンクの 1 つに発生したエラーを認識したことを意味します。 関連トラップ： 1: ifIndex 2: ifAdminStatus 3: ifOperStatus	1.3.6.1.6.3.1.1.5.3
linkUp	linkUp トラップは、送信側のプロトコルエンティティがエージェントの設定内にある通信リンクの 1 つのリンクアップを認識したことを意味します。 authenticationFailure トラップは、送信側のプロトコル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のアドレスであることを意味します。 関連トラップ： 1: ifIndex 2: ifAdminStatus 3: ifOperStatus	1.3.6.1.6.3.1.1.5.4
authenticationFailure	SNMPv2 の実行が本トラップを生成する必要がある間、実行用の特定のメカニズム経由でそのようなトラップの送信を抑制できる必要があります。 本トラップは、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る SNMP 通知です。	1.3.6.1.6.3.1.1.5.5
newRoot	トラップは、新しいルートとしての選出後すぐにブリッジによって送信され、その選出に続いてすぐに Topology Change Timer のアクションの起動などを行います。本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.1

トラップ名	説明	OID
topologyChange	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。本トラップは、newRoot トラップが同様の変更に対して送信される場合には送信されません。本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.2
risingAlarm	本トラップは SNMP トラップ送信で設定されたしきい値の上限を超えるイベントが発生した時に、高レベルの容量警告として SNMP 通知されます。 関連トラップ： 1: alarmIndex 2: alarmVariable 3: alarmSampleType 4: alarmValue 5: alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	本トラップは SNMP トラップ送信で設定されたしきい値の下限を超えるイベントが発生した時に、高レベルの容量警告として SNMP 通知されます。 関連トラップ： 1: alarmIndex 2: alarmVariable 3: alarmSampleType 4: alarmValue 5: alarmFailingThreshold	1.3.6.1.2.1.16.0.2
LLDP	リモート DB から LLDP エントリが追加 / 削除された時のトラップです。	1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.0.8802.1.1.2.1.2.2 1.0.8802.1.1.2.1.2.3 1.0.8802.1.1.2.1.2.4 1.0.8802.1.1.2.1.2.5

ハードウエアバージョン B1 のトラップログ

トラップ名	説明	OID
swL2macNotification	アドレステーブル内の MAC アドレスの変化を示します。 関連トラップ： swL2macNotifyInfo	1.3.6.1.4.1.171.11.117.1.1.2.100.1.2.0.1 (DGS-3120-24TC) 1.3.6.1.4.1.171.11.117.1.2.2.100.1.2.0.1 (DGS-3120-24PC) 1.3.6.1.4.1.171.11.117.1.3.2.100.1.2.0.1 (DGS-3120-24SC) 1.3.6.1.4.1.171.11.117.1.4.2.100.1.2.0.1 (DGS-3120-48TC) 1.3.6.1.4.1.171.11.117.1.5.2.100.1.2.0.1 (DGS-3120-48PC) 1.3.6.1.4.1.171.11.117.1.6.2.100.1.2.0.1 (DGS-3120-24SC-DC)
swL2PortSecurityViolationTrap	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。 関連トラップ： 1: swL2PortSecurityPortIndex 2: swL2PortSecurityViolationMac	1.3.6.1.4.1.171.11.117.1.1.2.100.1.2.0.2 (DGS-3120-24TC) 1.3.6.1.4.1.171.11.117.1.2.2.100.1.2.0.2 (DGS-3120-24PC) 1.3.6.1.4.1.171.11.117.1.3.2.100.1.2.0.2 (DGS-3120-24SC) 1.3.6.1.4.1.171.11.117.1.4.2.100.1.2.0.2 (DGS-3120-48TC) 1.3.6.1.4.1.171.11.117.1.5.2.100.1.2.0.2 (DGS-3120-48PC) 1.3.6.1.4.1.171.11.117.1.6.2.100.1.2.0.2 (DGS-3120-24SC-DC)
swIpMacBindingViolationTrap (EI モードのみ)	IP-MAC Binding トラップが有効の時、事前に設定したポートセキュリティに違反する MAC があるとトラップを送信します。 関連トラップ： 1: swIpMacBindingPortIndex 2: swIpMacBindingViolationIP 3: swIpMacBindingViolationMac	1.3.6.1.4.1.171.12.23.5.0.1
swIpMacBindingIPv6ViolationTrap (EI モードのみ)	IP-MAC Binding トラップが有効の時、定義済みの IPv6 IMPB 設定に違反する新しい MAC があると、トラップを送信します。 関連トラップ： 1: swIpMacBindingPortIndex 2: swIpMacBindingViolationIPv6Addr 3: swIpMacBindingViolationMac	1.3.6.1.4.1.171.12.23.5.0.4
swIpMacBindingShutdownTrap (EI モードのみ)	レートリミットがシャットダウンモードで DHCP レートがリミットを越えた場合、トラップを送信します。 関連トラップ： 1: swIpMacBindingPortIndex	1.3.6.1.4.1.171.12.23.5.0.5
swIpMacBindingRecoveryTrap (EI モードのみ)	ポートが DHCP レートリミットによってシャットダウンされていて、自動リカバリタイマがタイムアウトしていると、トラップを送信します。 関連トラップ： 1: swIpMacBindingPortIndex	1.3.6.1.4.1.171.12.23.5.0.6
swPktStormOccurred	パケットストームのメカニズムがパケットストームを検知し遮断した時に、本トラップは送信されます。 関連トラップ：swPktStormCtrlPortIndex	1.3.6.1.4.1.171.12.25.5.0.1
swPktStormCleared	パケットストームのメカニズムにより、パケットストームが消去された時に、本トラップは送信されます。 関連トラップ：swPktStormCtrlPortIndex	1.3.6.1.4.1.171.12.25.5.0.2

トラップ名	説明	OID
swPktStormDisablePort	パケットストームのメカニズムによってポートが無効になっています。 関連トラップ： 1:swPktStormCtrlPortIndex 2: swPktStormNotifyPktType	1.3.6.1.4.1.171.12.25.5.0.3
SafeGuardChgToExhausted	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。	1.3.6.1.4.1.171.12.19.4.1.0.1
SafeGuardChgToNormal	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。	1.3.6.1.4.1.171.12.19.4.1.0.2
agentGratuitousARPTrap	IP アドレスの競合が発生している時、本トラップは送信されます。 関連トラップ： 1. agentGratuitousARPIpAddr 2. agentGratuitousARPMacAddr 3. agentGratuitousARPPortNumber 4. agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.12.1.7.2.0.5
swDoSAttackDetected	指定の DoS パケットを受信しトラップが有効な時に、本トラップは送信されます。 関連トラップ： 1. swDoSCtrlType 2. swDoSNotifyVarIpAddr 3. swDoSNotifyVarPortNumber	1.3.6.1.4.1.171.12.59.4.0.1
swMacBasedAccessControlLoggedSuccess	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、本トラップを送信します。 関連トラップ： 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.1
swMacBasedAccessControlLoggedFail	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、本トラップを送信します。 関連トラップ： 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.2
swMacBasedAccessControlAgesOut	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、本トラップを送信します。 関連トラップ： 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.3
swFilterDetectedTrap	不正な DHCP サーバが検出された時、送信されます。ログが認証を止めている期間は、同じ不正な DHCP サーバの IP アドレスが検出されても、送信されるのは一度のみです。 関連トラップ： 1. swFilterDetectedIP 2. swFilterDetectedport	1.3.6.1.4.1.171.12.37.100.0.1
swPortLoopOccurred	ポートにループが発生すると、本トラップを送信します。 関連トラップ：swLoopDetectPortIndex	1.3.6.1.4.1.171.12.41.10.0.1
swPortLoopRestart	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。 関連トラップ：swLoopDetectPortIndex	1.3.6.1.4.1.171.12.41.10.0.2

トラップ名	説明	OID
swVlanLoopOccurred	VLAN に所属するポートにループが発生すると、本トラップを送信します。 関連トラップ： 1. swLoopDetectPortIndex 2. swVlanLoopDetectVID	1.3.6.1.4.1.171.12.41.10.0.3
swVlanLoopRestart	VLAN に所属する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。 関連トラップ： 1. swLoopDetectPortIndex 2. swVlanLoopDetectVID	1.3.6.1.4.1.171.12.41.10.0.4
swBpduProtectionUnderAttackingTrap	BPDU 防御トラップが有効の時､指定ポートが「normal」から「under attack」に変化した場合、本トラップは送信されます。 関連トラップ： 1. swBpduProtectionPortIndex 2. swBpduProtectionPortMode	1.3.6.1.4.1.171.12.76.4.0.1
swBpduProtectionRecoveryTrap	BPDU 防御トラップが有効の時、指定ポートが「under attack」から「normal」に変化した場合、本トラップは送信されます。 関連トラップ： 1. swBpduProtectionPortIndex 2. swBpduProtectionPortMode	1.3.6.1.4.1.171.12.76.4.0.2
swERPSSFDetectedTrap (EI モードのみ)	信号障害の発生時にトラップは生成されます。 関連トラップ：swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.1
swERPSSFClearedTrap (EI モードのみ)	信号障害が解消するとトラップは生成されます。 関連トラップ：swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.2
swERPSRPLOwnerConflictTrap (EI モードのみ)	競合が発生した時、本トラップが発生します。 関連トラップ：swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.3
dot1agCfmFaultAlarm (EI モードのみ)	MEP が持続性欠損状態です。マネジメントエントリに欠損が検出された MEP について OID と共に通知（失敗の警告）が送信されます。 関連トラップ：dot1agCfmMepHighestPrDefect	1.3.111.2.802.1.1.8.0.1
swCFMExtAISOccurred (EI モードのみ)	ローカル MEP が AIS 状態です。 関連トラップ： 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.1
swCFMExtAISCleared (EI モードのみ)	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。 関連トラップ： 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.2
swCFMExtLockOccurred (EI モードのみ)	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。 関連トラップ： 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.3
swCFMExtLockCleared (EI モードのみ)	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。 関連トラップ： 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.4
swFanFailure	ファンエラーの通知です。 関連トラップ： 1. swFanUnitIndex 2. swFanID	1.3.6.1.4.1.171.12.11.2.2.3.0.1

トラップ名	説明	OID
swFanRecover	ファンエラーから回復した通知です。 関連トラップ： 1. swFanUnitIndex 2. swFanID	1.3.6.1.4.1.171.12.11.2.2.3.0.2
swHighTemperature	高温状態の通知です。 関連トラップ： 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.1
swHighTemperatureRecover	高温状態が解消されると生成されます。 関連トラップ： 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.2
swLowTemperature	低温状態の通知です。 関連トラップ： 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.3
swLowTemperatureRecover	低温状態が解消されると生成されます。 関連トラップ： 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.4
agentFirmwareUpgrade	SNMP 経由のファームウェア更新が終了した通知です。 関連トラップ：swMultiImageVersion	1.3.6.1.4.1.171.12.1.7.2.0.7
agentCfgOperCompleteTrap	コンフィグレーションの保存、アップロード、ダウンロード完了の通知です。 関連トラップ： 1. unitID 2. agentCfgOperate 3. agentLogin ユーザ名	1.3.6.1.4.1.171.12.1.7.2.0.9
swPowerFailure	電源障害、停電の通知です。 関連トラップ： 1. swPowerUnitIndex 2. swPowerID 3. swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.2
swPowerRecover	電源障害、停電から復帰の通知です。 関連トラップ： 1. swPowerUnitIndex 2. swPowerID 3. swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.3
swUnitInsert	ユニットがホットインサートされた通知です。 関連トラップ： 1. swUnitMgmtId 2. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.1
swUnitRemove	ユニットがホットリムーブされた通知です。 関連トラップ： 1. swUnitMgmtId 2. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.2
swUnitFailure	ユニットに異常が発生しています。 関連トラップ：swUnitMgmtId	1.3.6.1.4.1.171.12.11.2.2.1.0.3

トラップ名	説明	OID
swUnitTPChange	スタッキングトポロジの変更通知です。 関連トラップ： 1. swStackTopologyType 2. swUnitMgmtId 3. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.4
swUnitRoleChange	スタッキングユニット変更通知です。 関連トラップ： 1. swStackRoleChangeType 2. swUnitMgmtId	1.3.6.1.4.1.171.12.11.2.2.1.0.5
lldpRemTablesChange	lldpStatsRemTableLastChangeTime の値が変化した時トラップを送信します。 関連トラップ： 1. lldpStatsRemTablesInserts 2. lldpStatsRemTablesDeletes 3. lldpStatsRemTablesDrops 4. lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
lldpXMedTopologyChangeDetected	新しいリモートデバイスがローカルポートに接続、またはリモートデバイスの切断、ポート移動などのトポロジの変更をローカルデバイスが検知した通知です。 関連トラップ： 1. lldpRemChassisIdSubtype 2. lldpRemChassisId 3. lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1
swDdmAlarmTrap (EI モードのみ)	トラップアクションの設定に基づいて、パラメータの値がアラームしきい値を超えると本トラップは送信されます。 関連トラップ： 1. swDdmPort 2. swDdmThresholdType 3. swDdmThresholdExceedType 4. swDdmThresholdExceedOrRecover	1.3.6.1.4.1.171.12.72.4.0.1
swDdmWarningTrap (EI モードのみ)	トラップアクションの設定に基づいて、パラメータの値が警告しきい値を超えると本トラップは送信されます。 関連トラップ： 1. swDdmPort 2. swDdmThresholdType 3. swDdmThresholdExceedType 4. swDdmThresholdExceedOrRecover	1.3.6.1.4.1.171.12.72.4.0.2
dot3OamNonThresholdEvent (EI モードのみ)	しきい値のないローカル / リモートイベントが検出された通知です。しきい値のないイベントを示す「Ethernet OAM Event Notification OAMPDU」の受信によりリモートイベントは検出され、ローカルエンティティによりローカルイベントは検出されます。 関連トラップ： 1. dot3OamEventLogTimestamp 2. dot3OamEventLogOui 3. dot3OamEventLogType 4. dot3OamEventLogLocation 5. dot3OamEventLogEventTotal	1.3.6.1.2.1.158.0.2
swSingleIPMSLinkDown	Commander スイッチは、メンバがリンクダウン通知を生成する場合に指定ホストに swSingleIPMSLinkDown 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr 3.ifIndex	1.3.6.1.4.1.171.12.8.6.0.13

トラップ名	説明	OID
swSingleIPMSLinkUp	Commander スイッチは、メンバがリンクアップ通知を生成する場合に指定ホストに swSingleIPMSLinkUp 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr 3.ifIndex	1.3.6.1.4.1.171.12.8.6.0.14
swSingleIPMSAuthFail	Commander スイッチは、メンバが認証エラー通知を生成する場合に指定ホストに swSingleIPMSAuthFail 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.15
swSingleIPMSnewRoot	Commander スイッチは、メンバが新しいルート通知を生成する場合に指定ホストに swSingleIPMSnewRoot 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.16
swSingleIPMSTopologyChange	Commander スイッチは、メンバがトポロジの変更通知を生成する場合に指定ホストに swSingleIPMSTopologyChange 通知を送信します。 関連トラップ： 1.swSingleIPMSID 2.swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.17
coldStart	coldStart トラップは、送信側のプロトコルエンティティがエージェントの設定またはプロトコルエンティティの実行を変更するように再初期化することを意味します。	1.3.6.1.6.3.1.1.5.1
warmStart	warmStart トラップは、送信側のプロトコルエンティティがエージェントの設定またはプロトコルエンティティのどちらの実行も変更しないように再初期化することを意味します。	1.3.6.1.6.3.1.1.5.2
linkDown	linkDown トラップは、送信側のプロトコルエンティティがエージェントの設定内にある通信リンクの 1 つに発生したエラーを認識したことを意味します。 関連トラップ： 1: ifIndex 2: ifAdminStatus 3: ifOperStatus	1.3.6.1.6.3.1.1.5.3
linkUp	linkUp トラップは、送信側のプロトコルエンティティがエージェントの設定内にある通信リンクの 1 つのリンクアップを認識したことを意味します。 authenticationFailure トラップは、送信側のプロトコル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のアドレスであることを意味します。 関連トラップ： 1: ifIndex 2: ifAdminStatus 3: ifOperStatus	1.3.6.1.6.3.1.1.5.4
authenticationFailure	SNMPv2 の実行が本トラップを生成する必要がある間、実行用の特定のメカニズム経由でそのようなトラップの送信を抑制できる必要があります。 本トラップは、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る SNMP 通知です。	1.3.6.1.6.3.1.1.5.5
newRoot	トラップは、新しいルートとしての選出後すぐにブリッジによって送信され、その選出に続いてすぐに Topology Change Timer のアクションの起動などを行います。本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.1

トラップ名	説明	OID
topologyChange	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。本トラップは、newRoot トラップが同様の変更に対して送信される場合には送信されません。本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.2
risingAlarm	本トラップは SNMP トラップ送信で設定されたしきい値の上限を超えるイベントが発生した時に、高レベルの容量警告として SNMP 通知されます。 関連トラップ： 1: alarmIndex 2: alarmVariable 3: alarmSampleType 4: alarmValue 5: alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	本トラップは SNMP トラップ送信で設定されたしきい値の下限を超えるイベントが発生した時に、高レベルの容量警告として SNMP 通知されます。 関連トラップ： 1: alarmIndex 2: alarmVariable 3: alarmSampleType 4: alarmValue 5: alarmFailingThreshold	1.3.6.1.2.1.16.0.2
LLDP	リモート DB から LLDP エントリが追加 / 削除された時のトラップです。	1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.0.8802.1.1.2.1.2.2 1.0.8802.1.1.2.1.2.3 1.0.8802.1.1.2.1.2.4 1.0.8802.1.1.2.1.2.5
pimNeighborLoss	pimNeighborLoss 通知は Neighbor との隣接関係の損失を示します。Neighbor タイマが期限が切れて、ルータが同じ IP バージョンで下位の IP アドレスを持つ他の Neighbor が同じインタフェースにないと、この通知が生成されます。 pimNieghborLossNotificationsPeriod によって指定されたレート制限に従って、pimNeighborLossCount のカウンタが増加する度に、本通知は生成されます。 関連トラップ： 1: pimNeighborUpTime	1.3.6.1.2.1.157.0.1
pimInvalidRegister	pimInvalidRegister 通知は、本デバイスが無効な PIM Register メッセージを受信したことを示します。 pimInvalidRegisterNotificationPeriod によって指定されたレート制限に従って、pimInvalidRegisterMsgsRcvd カウンタが増加する度に、本通知は生成されます。 関連トラップ： 1: pimGroupMappingPimMode 2: pimInvalidRegisterAddressType 3: pimInvalidRegisterOrigin 4: pimInvalidRegisterGroup 5: pimInvalidRegisterRp	1.3.6.1.2.1.157.0.2

トラップ名	説明	OID
pimInvalidJoinPrune	pimInvalidJoinPrune 通知は、本デバイスが無効な PIM Join/Prune ッセージを受信したことを示します。 pimInvalidJoinPruneNotificationPeriod によって指定されたレート制限に従って、pimInvalidJoinPruneMsgsRcvd カウンタが増加する度に、本通知は生成されます。 関連トラップ： 1: pimGroupMappingPimMode 2: pimInvalidJoinPruneAddressType 3: pimInvalidJoinPruneOrigin 4: pimInvalidJoinPruneGroup 5: pimInvalidJoinPruneRp 6: pimNeighborUpTime	1.3.6.1.2.1.157.0.3
pimRPMappingChage	pimRPMappingChange 通知は本デバイスにおける RP マッピングへの変更を示します。 pimRPMappingChangeNotificationPeriod によって指定されたレート制限に従って、pimRPMappingChangeCount カウンタが増加する度に、本通知は生成されます。 関連トラップ： 1: pimGroupMappingPimMode 2: pimGroupMappingPrecedence	1.3.6.1.2.1.157.0.4
pimInterfaceElection	pimInterfaceElection 通知は、ネットワークで新しい DR または DF が選出されたことを示します。 pimInterfaceElectionNotificationPeriod によって指定されたレート制限に従って、pimInterfaceElectionWinCount カウンタが増加する度に、本通知は生成されます。 関連トラップ： 1: pimInterfaceAddressType 2: pimInterfaceAddress	1.3.6.1.2.1.157.0.5

【付録 E】 RADIUS 属性の割り当て指定

DGS-3120 における RADIUS 属性の割り当ては、以下のモジュールで使用されます。
- 802.1X（ポートベースとホストベース）
- MAC ベースのアクセスコントロール
- Web ベースアクセスコントロール（WAC）
- Japanese Web ベースアクセスコントロール（JWAC）

以下の記述では、続く RADIUS 属性の割り当てのを説明します。
- Ingress/Egress 帯域
- 802.1p デフォルトプライオリティ
- VLAN
- ACL

RADIUS サーバで Ingress/Egress の帯域幅を割り当てるためには、適切なパラメータを RADIUS サーバに設定する必要があります。以下の表では帯域幅のパラメータを示しています。

ベンダー指定の属性の項目は以下の通りです。

ベンダー指定の属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171（DLINK）	必須
ベンダータイプ	本属性の定義	2（イングレス帯域用） 3（イーグレス帯域用）	必須
属性指定フィールド	ポートの帯域を割り当てるために使用します。	単位（Kbits）	必須

RADIUS サーバの帯域幅属性（例 : イングレス帯域幅 1000Kbps）を設定し、802.1X 認証に成功すると、RADIUS サーバに従ってデバイスは正しい帯域幅をポートに割り当てます。しかし、帯域幅属性を設定せずに認証に成功しても、デバイスは帯域幅をポートに割り当てません。帯域幅属性に 0 またはポートの有効帯域幅（イーサネットポートでは 100Mbps またはギガビットポートでは 1Gbps）より大きい数値を設定する場合、no_limit を指定します。

RADIUS サーバで 802.1p デフォルトプライオリティを割り当てるためには、適切な項目を RADIUS サーバに設定する必要があります。

ベンダー指定の属性の項目は以下の通りです。

ベンダー指定の属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171（DLINK）	必須
ベンダータイプ	本属性の定義	4	必須
属性指定フィールド	ポートの 802.1p デフォルトプライオリティを割り当てるために使用します。	0-7	必須

RADIUS サーバの 802.1p プライオリティ属性（例 : プライオリティ 7）を設定し、802.1X またはホストベース認証に成功すると、RADIUS サーバに従ってデバイスは 802.1p デフォルトプライオリティをポートに割り当てます。しかし、プライオリティ属性を設定せずに認証に成功しても、デバイスはプライオリティをポートに割り当てません。RADIUS サーバに設定されたプライオリティ属性が範囲外（7 より大きい）であると、そのデバイスには設定されません。

RADIUS サーバで VLAN を割り当てるためには、適切なパラメータを RADIUS サーバに設定する必要があります。VLAN の割り当てを使用するために、RFC3580 では RADIUS パケットに以下のトンネル属性を定義しています。

以下の表では VLAN の項目を示しています。

RADIUS トンネル属性	説明	値	摘要
トンネルタイプ	本属性はトンネルの開始に使用されるトンネリングプロトコルまたはトンネルの終了に使用されるトンネリングプロトコルを示します。	13 (VLAN)	必須
Tunnel-Medium-Type	本属性は使用されている伝送の媒体を示します。	6 (802)	必須
Tunnel-Private-Group-ID	本属性は特定のトンネルセッションのグループ ID を示します。	文字列（VID）	必須

「Tunnel-Private-Group-ID」属性フォーマットのサマリは次のようになります。

```
 0            1            2            3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type    |   Length   |    Tag     |  String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

タグフィールドの定義は次の通りです。（RFC 2868 とは違う）

タグフィールド値	文字列フィールドのフォーマット	備考
0x01	VLAN 名 (ASCII)	0x1F よりも大きいタグフィールドは続くフィールドの最初のオクテットとして認識されます。
0x02	VLAN ID (ASCII)	
その他 (0x00、0x03 ~ 0x1F、>0x1F)	**1.** スイッチが VLAN 設定の文字列を受信した場合、最初は VLAN ID として認識します。つまりスイッチは既存の VLAN ID をチェックし合致するものがあるか調べます。 **2.** スイッチが合致する VLAN ID を発見した場合、その VLAN へ移動します。 **3.** スイッチが合致する VLAN ID を発見できなかった場合、VLAN 設定の文字列は VLAN 名として認識されます。 **4.** そして合致する VLAN 名を発見します。	

RADIUS サーバの VLAN 属性 (例 : VID 3) を設定し、802.1X または MAC ベースアクセスコントロール認証に成功すると、ポートは VLAN 3 に追加されます。しかし、VLAN 属性を設定せずに認証に成功しても、ポートは元の VLAN に置かれます。RADIUS サーバに設定された VLAN 属性が存在しないと、ポートは要求された VLAN に割り当てられません。

RADIUS サーバが ACL を割り当てるためには、適切な項目を RADIUS サーバに設定する必要があります。以下の表では ACL の項目を示しています。RADIUS ACL の割り当ては、MAC ベースアクセスコントロールにて使用されるだけです。

ベンダー指定の属性の項目は以下の通りです。

RADIUS トンネル属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171 (DLINK)	必須
ベンダータイプ	属性を定義します。	12（ACL プロファイル用） 13 (ACL ルール用)	必須

属性指定フィールド	ACL プロファイルまたはルールを割り当てるために使用されます。	ACL コマンド
		例 :
		ACL プロファイル :
		`create access_profile ethernet vlan 0xFFF profile_id 100`
		ACL ルール :
		`config access_profile profile_id 100 add access_id auto_assign ethernet vlan_id default port all deny`
			必須

RADIUS サーバの ACL 属性（例 : ACL プロファイル :「`create access_profile ethernet vlan 0xFFF profile_id 100`」、ACL ルール :「`config access_profile profile_id 100 add access_id auto_assign ethernet`」）を設定し、MAC ベースアクセスコントロール認証に成功すると、RADIUS サーバに従ってデバイスは ACL プロファイルとルールを割り当てます。ACL モジュールに関する詳しい情報については、「DGS-3120 CLI マニュアル」の「アクセスコントロールリスト（ACL）コマンド」を参照してください。

【付録 F】 ケーブルとコネクタ

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。
以下の図と表は標準の RJ-45 プラグ / コネクタとピンアサインです。

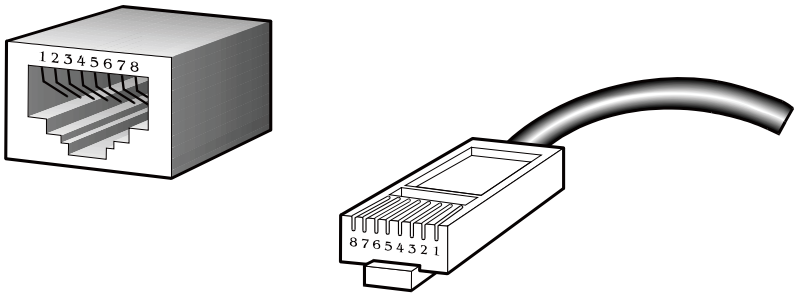


図 A-1　標準的な RJ-45 プラグとコネクタ

表 A-1　標準的な RJ-45 ピンアサイン

RJ-45 ピンアサイン		
コンタクト（ピン番号）	MDI-X 信号	MDI-II 信号
1	RD+（受信）	TD+（送信）
2	RD-（受信）	TD-（送信）
3	TD+（送信）	RD+（受信）
4	未使用	未使用
5	未使用	未使用
6	TD-（送信）	RD-（受信）
7	未使用	未使用
8	未使用	未使用

【付録 G】 ケーブル長

以下の表は各規格に対応するケーブル長（最大）です。

規格	メディアタイプ	最大伝送距離
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	10 km 550 m 40 km 80 km
1000BASE-T	エンハンスドカテゴリ 5 UTP ケーブル カテゴリ 5 UTP ケーブル（1000 Mbps）	100 m
100BASE-TX	カテゴリ 5 UTP ケーブル（100 Mbps）	100 m
10BASE-T	カテゴリ 3 UTP ケーブル（10 Mbps）	100 m

【付録 H】 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 550m。
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 802.3x) 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。

用語	説明
MDI（Medium Dependent Interface）	1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。
MDI-X（Medium Dependent Interface Cross-over）	接続送受信のラインが交差しているイーサネットポート接続。
MIB（Management Information Base）	デバイスの管理特性と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。
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。

【付録 I】 機能設定例

本項では、一般によく使う機能についての設定例を記載します。実際に設定を行う際の参考にしてください。

- Traffic Segmentation（トラフィックセグメンテーション）
- VLAN
- Link Aggregation（リンクアグリゲーション）
- Access List（アクセスリスト）

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DGS-3620
- DGS-3420
- DGS-3120
- DGS-3000
- DES-3200

注意 当項目において機器イラストは機種に依らず、共通化して掲載しています。そのため、製品によっては、ポート数や種別が異なる場合などがありますので、予めご了承ください。実際の設定については、ポート番号等、お使いの状況に置き換えてお考えください。

Traffic Segmentation（トラフィックセグメンテーション）

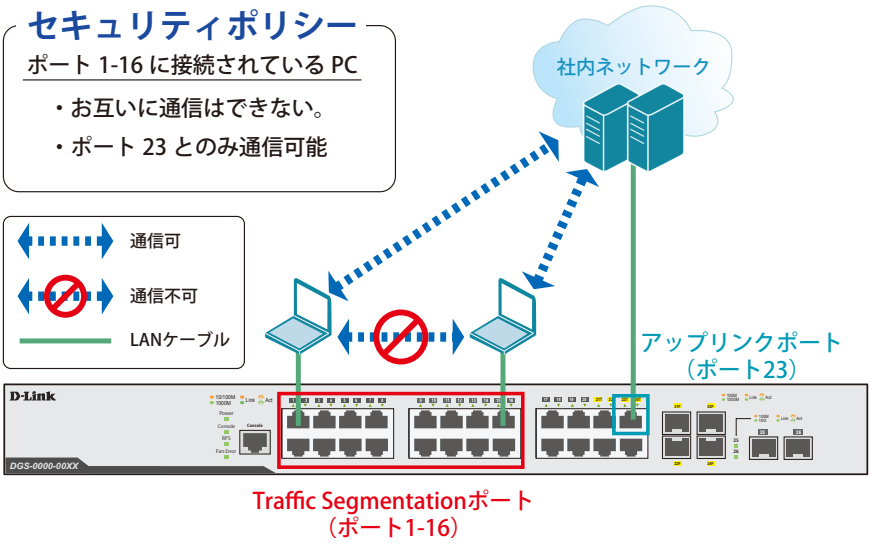


図 1-1　Traffic Segmentation

概要

ポート 1 ～ 16 に対し、トラフィックセグメンテーションを設定します。1 ～ 16 のポート間ではお互いに通信ができないようにし、ポート 1 ～ 16 は、アップリンクポートとして使用するポート 23 とのみ通信ができるようにします。

設定手順

1. ポート（1-16）のトラフィックセグメンテーション設定をします。

```
# config traffic_segmentation 1-16 forward_list 23
```

2. 設定を保存します。

```
# save
```

3. 情報確認

```
# show traffic_segmentation
```

注意 本機能を利用する場合、Unknown ユニキャストについては全ポートにブロードキャストされます。各 PC 間の Unknown ユニキャストも止めたい場合は、下記の設定が追加で必要になります。

4. （必要に応じて）Traffic Control 機能により、Unknown ユニキャストを破棄する設定をします。

```
# config traffic control 1-16 unicast enable action drop threshold 0
```

5. 設定を保存します。

```
# save
```

6. 情報確認

```
# show traffic control
```

VLAN

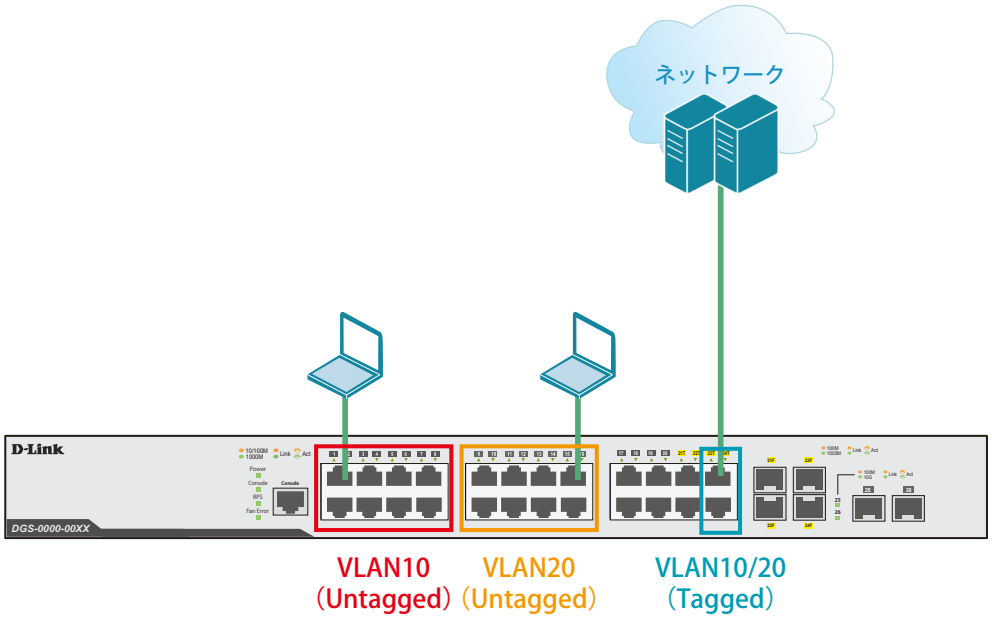


図 1-2　VLAN

概要

VLAN を設定します。ポート 1 ～ 8 に VLAN10 を「Untagged」で割り当て、ポート 9 ～ 16 に VLAN20 を「Untagged」で割り当て、ポート 23 ～ 24 のポートにおいて、VLAN10 と VLAN20 を「Tagged」で割当ます。

設定手順

1. VLAN10、VLAN20 を作成します。

```
# create vlan vlan10 tag 10
# create vlan vlan20 tag 20
```

2. default の VLAN を削除します。

```
# config vlan default delete 1-24
```

3. ポート 1-8 に VLAN10、ポート 9-16 に VLAN20 を Untagged ポートとして割り付けます。

```
# config vlan vlan10 add untagged 1-8
# config vlan vlan20 add untagged 9-16
```

4. ポート 23-24 に VLAN10、VLAN20 を Tagged ポートとして割り付けます。

```
# config vlan vlan10 add tagged 23-24
# config vlan vlan20 add tagged 23-24
```

5. 設定を保存します。

```
# save
```

6. 情報確認

```
# show vlan
# show vlan ports <portlist>
```

Link Aggregation（リンクアグリゲーション）

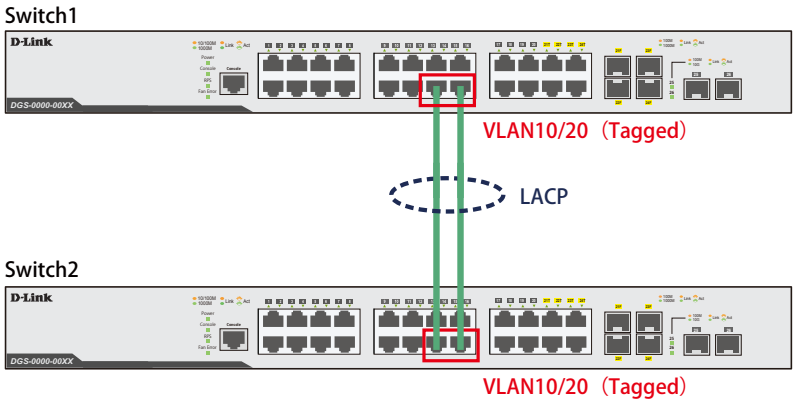


図 1-3　Link Aggregation

概要

VLAN10 と 20 の Tagged VLAN を設定したポートにリンクアグリゲーションを設定します。ポート 14 と 16 に VLAN10 と VLAN20 を「Tagged」で割り当て、ポート 14 と 16 をグループ 1 として LACP によるリンクアグリゲーションに設定します。

設定手順（Switch1、Switch2 共通）

1. VLAN10、VLAN20 を作成します。

```
# create vlan vlan10 tag 10
# create vlan vlan20 tag 20
```

2. ポート 14,16 に VLAN10、VLAN20 を Tagged ポートとして割り付けます。

```
# config vlan vlan10 add tagged 14,16
# config vlan vlan20 add tagged 14,16
```

3. Link Aggregation（LACP）のグループを作成します。

```
# create link_aggregation group_id 1 type lacp
```

4. Master ポートをポート 14 とし、ポート 14 と 16 をグループのメンバポートを設定します。

```
# config link_aggregation group_id 1 master_port 14 ports 14,16 state enable
```

5. LACP のモードをアクティブ設定します。

```
# config lacp_port 14,16 mode active
```

6. 設定を保存します。

```
# save
```

7. 情報確認

```
# show vlan
# show vlan ports <portlist>
# show link_aggregation
# show lacp_port <portlist>
```

Access List（アクセスリスト）（DGS-3000 を除く）

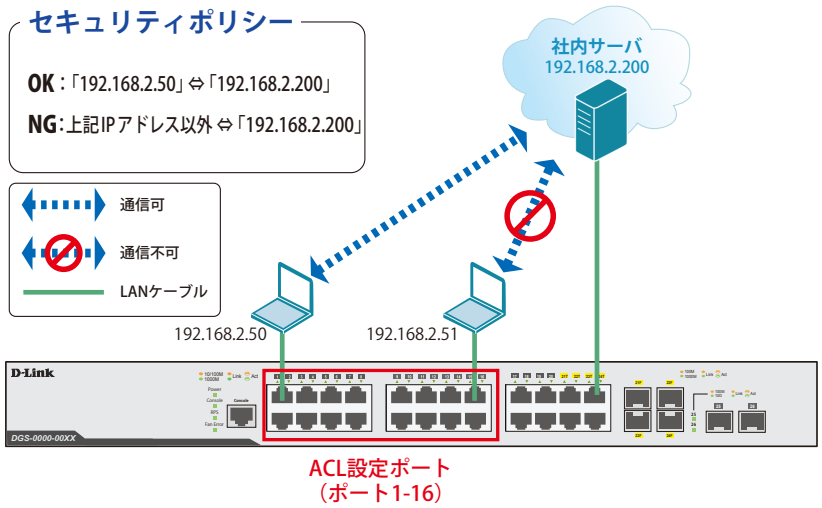


図 1-4　Access List

概要

ポート 1~16 に対し、アクセスリストを設定します。ポート 1~16 に接続される端末の IP の中から ,192.168.2.50 の端末から社内サーバ（192.168.2.200）へのアクセスは許可し、それ以外の端末から社内サーバへのアクセスは禁止するように設定します。

設定手順

1. 特定端末間の IP 通信を制御するためのプロファイルを作成します。

```
# create access_profile profile_id 1 profile_name 1 ip source_ip_mask 255.255.255.255
destination_ip_mask 255.255.255.255
```

2. プロファイルに「192.168.2.50」⇔「192.168.2.200」間の通信を許可するルールを追加します。

```
# config access_profile profile_id 1 add access_id 1 ip source_ip 192.168.2.50
destination_ip 192.168.2.200 port 1-16 permit
```

3. 「192.168.2.200」への通信をすべて拒否するためのプロファイルを作成します。

```
# create access_profile profile_id 2 profile_name 2 ip source_ip_mask 0.0.0.0
destination_ip_mask 255.255.255.255
```

4. 「192.168.2.200」へのすべての通信を拒否するルールを追加します。

```
# config access_profile profile_id 2 add access_id 1 ip source_ip 0.0.0.0
destination_ip 192.168.2.200 port 1-16 deny
```

5. 設定を保存します。

```
# save
```

6. 情報確認

```
# show access_profile
```