D-Link DGS-3200 シリーズ

Layer2+ Gigabit Managed Switch

ユーザマニュアル

ご注意

本書は、各製品ごとの機能の説明および設定方法を記載しています。本シリーズの仕様、設置方法など使用するために必要な基本的な取り扱い方法については、設置マニュアルをご覧ください。

D-Link®
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

⚠警告	この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。

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

⚠警告

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

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
故障の原因につながります。

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してください。

ぬれ手禁止　ぬれた手でさわらない
感電のおそれがあります。

水ぬれ禁止　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、または故障のおそれがあります。

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

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、または故障のおそれがあります。

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

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。

禁止　設置、移動のときは電源プラグを抜く
火災、感電、または故障のおそれがあります。

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
感電のおそれがあります。

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、または故障につながります。

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

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

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

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

⚠注意

❗　静電気注意
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

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

❗　振動が発生する場所では使用しない
接触不良や動作不良の原因となります。

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

電波障害自主規制について

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

ご使用上の注意

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

- 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあけたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。
- 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
  - 電源ケーブル、延長ケーブル、またはプラグが破損した。
  - 製品の中に異物が入った。
  - 製品に水がかかった。
  - 製品が落下した、または損傷を受けた。
  - 操作方法に従って運用しているのに正しく動作しない。
- 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔を塞がないようにしてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。
- 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。
- 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプがわからない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。
- システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
  - 東日本では 100V/50Hz、西日本では 100V/60Hz
- また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。
- 付属の電源ケーブルのみを使用してください。
- 感電を防止するために、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3 ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグが付いている 3 線式コードを使用してください。
- 延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動からシステムコンポーネントを保護するには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたりつまずいたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いてください。
- 製品の移動は気をつけて行ってください。キャスタやスタビライザがしっかり装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

ラック搭載型製品に関する一般的な注意事項

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

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

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

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

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

- ラックにシステム / コンポーネントを搭載した後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つのみとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。
- ラックに装置を搭載する前に、スタビライザがしっかりとラックに固定されているか、床面まで到達しているか、ラック全体の重量がすべて床にかかるようになっているかをよく確認してください。ラックに搭載する前に、シングルラックには前面および側面のスタビライザを、複数結合型のラックには前面用スタビライザを装着してください。
- ラックへの装置の搭載は、常に下から上へ、また最も重いものから行ってください。
- ラックからコンポーネントを引き出す際には、ラックが水平で、安定しているかどうか確認してから行ってください。
- コンポーネントレール解除ラッチを押して、ラックから、またはラックへコンポーネントをスライドさせる際は、指をスライドレールに挟まないよう、気をつけて行ってください。
- ラックに電源を供給する AC 電源分岐回路に過剰な負荷をかけないでください。ラックの合計負荷が、分岐回路の定格の 80 パーセントを超えないようにしてください。
- ラック内部のコンポーネントに適切な空気流があることを確認してください。
- ラック内の他のシステムを保守する際には、システムやコンポーネントを踏みつけたり、その上に立ったりしないでください。

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

静電気障害を防止するために

静電気は、システム内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネントを静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃してください。
2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。
3. 静電気に敏感なコンポーネントの取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

バッテリの取り扱いについて

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

電源の異常

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

本製品には電源ケーブル抜け防止金具が同梱されております。本製品を製品背面の電源コネクタ部分に取り付けます。電源ケーブルを接続して金具に固定すると、ケーブルの抜けを防止することができます。

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

- 本書および同梱されている製品保証書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
また、テクニカルサポートご提供のためにはユーザ登録が必要となります。
http://www.dlink-jp.com/

目次

はじめに

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

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

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

第 3 章 スイッチの接続
- スイッチをご使用のイーサネット、またはバックボーンなどに接続する方法を説明します。

第 4 章 スイッチ管理の導入
- パスワード設定、SNMP 設定、IP アドレス割り当て、および各種デバイスからの本スイッチへの接続などの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。

第 6 章 Configuration（スイッチの主な設定）
- スイッチ情報へのアクセス、IP アドレス、ユーザアカウント、システムログ、システム時刻、DHCP/BOOTP リレー設定、SNMP 設定などのスイッチの基本機能の設定について説明します。

第 7 章 L2 Features（L2 機能の設定）
- VLAN、トランキング、スパニングツリー、IGMP/MLD Snooping などスイッチの L2 機能について説明します。

第 8 章 QoS（QoS 機能の設定）
- スイッチの QoS の概要と設定について説明します。

第 9 章 Security（セキュリティ機能の設定）
- セーフガードエンジン、アクセス認証コントロール、MAC ベース認証などスイッチのセキュリティ機能について説明します。

第 10 章 ACL（ACL 機能の設定）
- アクセスコントロールの設定について説明します。

第 11 章 Monitoring（スイッチのモニタリング）
- モニタリング機能で使用するグラフや画面について説明します。

第 12 章 Maintenance（スイッチのメンテナンス）
- 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。

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

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

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

付録 D トラップログ
- スイッチで検出でき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 パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減
- ARP プロトコル、ARP スプーフィング攻撃、および D-Link スイッチが提供する ARP スプーフィング攻撃を防御する対策について説明します。

付録 F パスワードリカバリ手順
- 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。

付録 G 用語集
- 本マニュアルに使用される用語の定義を示します。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

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

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "（13 ページ）をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
courier 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
courier 斜体	コマンド項目（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。

第 1 章　本製品のご利用にあたって

DGS-3200 シリーズレイヤ 2+ ギガビットイーサネットスイッチは、充実したセキュリティ機能と高速、大容量通信をコンパクトサイズで提供するコスト効果の高い製品です。分散、拡張を続ける社内ネットワークのエンドポイントにおいてセキュリティの大幅な向上を実現します。高速ギガビット通信可能な 1000BASE-T および SFP ポートを搭載し、光ファイバへの接続も可能なほか、距離などの制限のない仮想スタックや先進的な L2+ 機能を組み合わせることで、デスクトップスイッチとして活用するだけでなく、バックボーンスイッチと共に全社的なネットワーク環境の増強まで可能です。また、ユーザフレンドリーな管理インタフェースもあわせて提供します。

本マニュアルでは、本製品の設置および管理、設定の方法について記述しています。

ギガビットイーサネット技術について

ギガビットイーサネットは IEEE 802.3 イーサネットの拡張技術で、イーサネットと同様のパケット構造、フォーマットを使用しています。CSMA/CD プロトコル、全二重伝送モード、フローコントロール、管理オブジェクトをサポートし、100Mbps のファーストイーサネットの 10 倍、10Mbps のイーサネットの 100 倍のスループットを実現します。10Mbps、100Mbps のイーサネットと互換性を持つため、既存のハードウェアやソフトウェア、また職員の教育などへの投資を無駄にすることなく、容易にアップグレードできます。

コンピュータやそのバスの高速化に伴い、さらに多くのユーザがアプリケーションを使用して大量のトラフィックを発生する今日、ギガビットイーサネットにより増強されるスピードや帯域は、ネットワークのボトルネックに対処するために必要不可欠であると言えます。バックボーンやサーバなどの重要なネットワーク構成要素を、ギガビットイーサネットに対応させることにより、ネットワークレスポンスを改善し、ご使用のサブネットワーク間のトラフィックを著しくスピードアップします。

ギガビットイーサネットは、ビデオカンファレンス、複雑な映像処理、またデータ量の多いアプリケーションに対応可能な光ファイバ接続を可能にします。ファーストイーサネットの 10 倍の速度でデータ伝送を行うことができるため、ギガビットイーサネット対応のネットワークインタフェースカードを装備したサーバでは、同じ時間内に 10 倍の処理を行うことができます。

さらに、ギガビットイーサネットがもたらす驚異的な帯域幅は、今日そして未来に向かってめまぐるしく変貌を遂げるスイッチングやルーティングのインターネットワーキング技術を享受するための最もコスト効果が高い方法です。

スイッチ概要

DGS-3200-10、DGS-3200-16/GE および DGS-3200-24/GE は、帯域幅 10Mbps、100Mbps、1000Mbps 用にそれぞれ 8 個、14 個、および 20 個の UTP ポート（Auto MDI-X/MDI-II）を装備し、他のスイッチとの接続が可能です。また、PC、プリンタ、サーバ、ハブ、ルータ、スイッチおよび他のネットワークデバイスとの接続に使用できます。UTP ケーブルを使用してこれらのポートに接続し、ネットワークを小さいサブネットワークに分割することでパフォーマンスを向上します。各 10BASE-T/100BASE-TX/1000BASE-T ポートは全二重モードで 2Gbps までのスループットをサポートします。
さらに、前面パネルに DGS-3200-10、DGS-3200-16/GE は 2 個、DGS-3200-24/GE は 4 個の 1000BASE-T/SFP コンボポートを装備しています。これらのギガビットコンボポートは、サーバやネットワークバックボーンへの接続に適しています。DGS-3200-24/GE は、ファイルの起動およびバックアップ用に SD カードスロット 1 ポート搭載しています。

本スイッチは、ネットワーク上で多くの帯域が要求されるマルチメディアや映像などのアプリケーションを、他のユーザアプリケーションと同時に、ボトルネックを発生させずに使用できます。内蔵のコンソールインタフェースは、優先キューイング、VLAN、ポートトランクグループ、ポートモニタリング、およびポートスピードなどの設定に使用できます。

注意　DGS-3200 シリーズを本マニュアル上では単に “スイッチ” あるいは “本製品” と記載します。

サポートする機能

- IEEE 802.3 10BASE-T 準拠
- IEEE 802.3u 100BASE-TX 準拠
- IEEE 802.3ab 1000BASE-T 準拠
- IEEE 802.3z 1000BASE-X 準拠
- IEEE 802.1p プライオリティキュー
- IEEE 802.3x 全二重モードフローコントロール
- IEEE 802.3ad リンクアグリケーションプロトコル（DGS-3200-10 : 5 グループ、DGS-3200-16/GE : 8 グループ、DGS-3200-24/GE : 12 グループ）
- IEEE 802.1X ポートベース、ホストベース認証
- IEEE 802.1Q VLAN
- IEEE 802.1D スパニングツリー、IEEE 802.1w ラピッドスパニングツリー、IEEE 802.1s マルチプルスパニングツリー
- ジャンボフレーム（最大 10K バイト）
- アクセスコントロールリスト（ACL）
- ISM VLAN
- Egress フィルタによる DFL/ マルチキャストパケットの破棄
- DHCP ローカルリレー
- シングル IP マネジメント（SIM）
- TACACS、XTACACS、TACACS+、RADIUS を使用したアクセス認証制御
- マルチプル認証
- デュアルイメージ・ファームウェア、デュアルコンフィグレーション
- 省電力モード
- ブロードキャスト Ping
- SNTP
- MAC 通知
- システム、ポート使用率
- システムログ、システム緊急度設定、SMTP ログ
- 最大パケットフォワーディングレート（64Byte）: 14.88Mpps（DGS-3100-10）、23.81Mpps（DGS-3200-16/GE）、35.7Mpps（DGS-3200-24/GE）
- アドレステーブル : デバイスごとの最大 MAC アドレス : 8K（DGS-3200-10）、16K（DGS-3200-16/GE、DGS-3200-24/GE）
- 最大パケットバッファ : 1M ビット（DGS-3200-10）、6M ビット（DGS-3200-16/GE、DGS-3200-24/GE）
- ポートベース VLAN、プライベート VLAN
- フレキシブル負荷分配機能、フェイルオーバ機能対応ポートトランキング
- RADIUS サーバフェイルオーバ
- IGMP/MLD Snooping（MLD v1/v2）
- IP-MAC- ポートバインディング（IMPB）v3.6
- SNMP
- SD カード用フラッシュファイルシステム（DGS-3200-24/GE のみ）
- SSL、SSH
- ポートミラーリング
- 以下の MIB のサポート
    - RFC1213 MIB II、RFC4188 Bridge、RFC1907 SNMP v2、RFC1757/2819 RMON、RFC1643/2358/2665 Ether-like MIB
    - RFC2233/2863 Interface MIB、D-Link プライベート MIB、IEEE 802.1p 対応 RFC2674、RFC2618 認証クライアント MIB、IEEE 802.1X MIB
- スイッチ管理用 RS-232 DCE コンソールポート
- パラレルポート状態 LED 表示（リンク、アクション、スピード等）
- 高パフォーマンスのスイッチングエンジンによる、ワイヤスピードで最大 20Gbps（DGS-3200-10）/ 32Gbps（DGS-3200-16/GE）/48Gbps（DGS-3200-24/GE）のフォワーディングおよびフィルタリング。
- 全ギガポートが全二重、半二重通信をサポート。全二重通信では、データの送受信を同時に行いますが、全二重通信可能なノードやスイッチとの通信に限られます。ハブとの接続には半二重通信を使用します。
- ブロードキャストストームフィルタリング
- ループバック検知（LBD）v4.0 トラップ
- レート適応およびプロトコル変換に対応するための、非ブロック型ストア & フォワードスイッチング機能
- ポート入出力速度制御
- ワイヤスピードでのフォワーディング速度に対応するための自己学習機能およびアドレス認識メカニズム
- セーフガードエンジン
- ケーブル診断
- Web ベース GUI（Internet Explorer 6.0 以降）

ポートについて

- エンドステーション、サーバ、ハブなどのネットワークデバイスとの接続用に 8 ポート（DGS-3200-10）/14 ポート（DGS-3200-16/GE）/20 ポート（DGS-3200-24/GE）の高パフォーマンス（Auto MDI-X/MDI-II）ギガポートを有します。
- すべての UTP ポートは 10Mbps/100Mbps/1000Mbps、半二重 / 全二重間のオートネゴシエーション機能、およびフローコントロール機能を搭載しています。
- 他のスイッチ、サーバ、ネットワークバックボーンへの接続用に 1000BASE-T/SFP コンボポートを 2 個（DGS-3200-10、DGS-3200-16/GE）または 4 個（DGS-3200-24/GE）有します。
- コンソール端末または端末エミュレーションプログラム使用の PC を RS-232C 診断用ポート（コンソールポート）と接続し、スイッチの設定、管理を行えます。

前面パネル

スイッチの前面パネルには、Power（電源）、Console、10/100/1000Mbps のツイストペアポート、および 1000BASE-T/SFP コンボポートと LED が配置されています。また、DGS-3200-24/GE には SD カード用スロットが搭載されています。

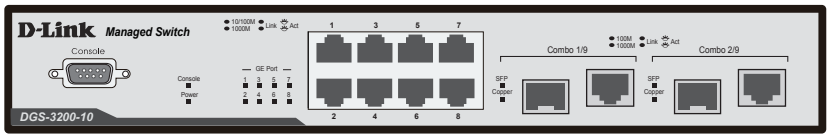


図 1-1　前面パネル図（DGS-3200-10）

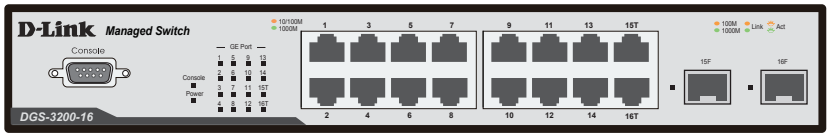


図 1-2　前面パネル図（DGS-3200-16/GE）

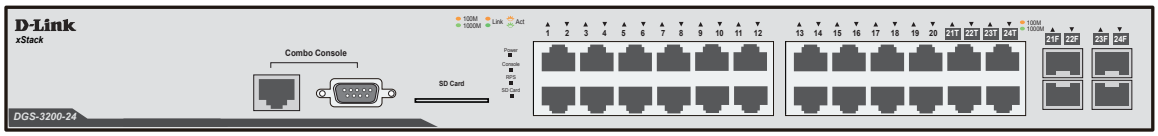


図 1-3　前面パネル図（DGS-3200-24/GE）

LED はスイッチとネットワークの状態を表示します。

LED 表示

DGS-3200-16 および DGS-3200-16/GE は、Power、Console、および各ポートについて LED をサポートします。以下に、スイッチ上の LED の配置と、各 LED の状態が表す意味を示します。

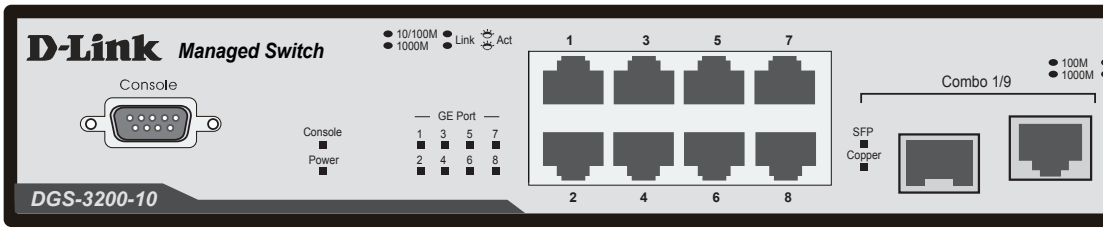


図 1-4　LED 配置図（DGS-3200-10）

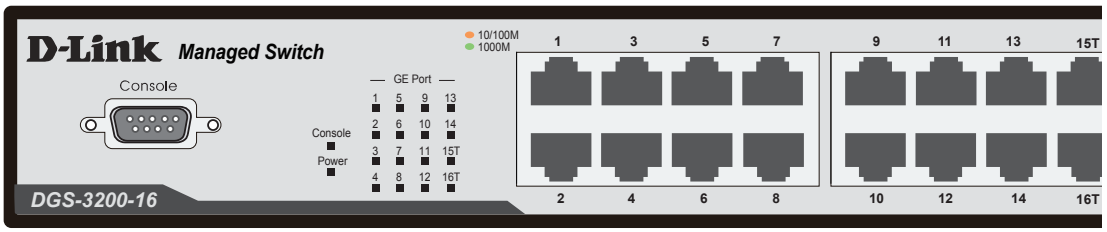


図 1-5　LED 配置図（DGS-3200-16/GE）

DGS-3200-24/GE は、Power、Console、RPS（オプション）、SD Card および各ポートについて LED をサポートします。以下に、スイッチ上の LED の配置と、各 LED の状態が表す意味を示します。

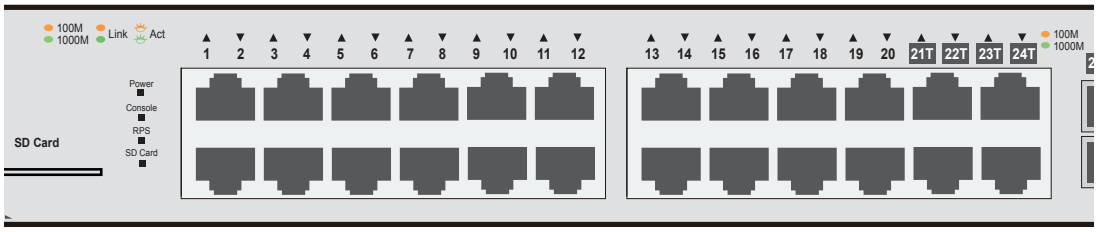


図 1-6　LED 配置図（DGS-3200-24/GE）

LED	状態	色	状態説明
Power	点灯	緑	スイッチに電源が供給され正常に動作しています。
	消灯	―	スイッチに電源が供給されていません。
Console	点滅	緑	電源投入後の Power ON Self Test（POST）中に点滅し、終了すると消灯します。
	点灯		コンソールポートのリンクが確立しています。
RPS （DGS-3200-24/GE のみ）	点灯	緑	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。
	消灯	―	リダンダント電源ユニットは動作していません。
SD Card （DGS-3200-24/GE のみ）	点灯	緑	SD カードが挿入されています。
	点滅		SD カードにアクセスしています。
	消灯	―	SD カードが挿入されていません。
ポート LED	点灯	緑	1000Mbps でリンクが確立しています。
	点滅		1000Mbps でデータを送受信しています。
	点灯	橙	10/100Mbps でリンクが確立しています。
	点滅		10/100Mbps でデータを送受信しています。
	消灯	―	リンクが確立していません。
コンボポート	スイッチ上の 2 つの 1000BASE-T/SFP ポートそれぞれに LED が配置されています。		
SFP	点灯	緑	1000Mbps でリンクが確立しています。
	点滅		1000Mbps でデータを送受信しています。
	点灯	橙	100Mbps でリンクが確立しています。
	点滅		100Mbps でデータを送受信しています。
	消灯	―	リンクが確立していません。
Copper	点灯	緑	1000Mbps でリンクが確立しています。
	点滅		1000Mbps でデータを送受信しています。
	点灯	橙	10/100Mbps でリンクが確立しています。
	点滅		10/100Mbps でデータを送受信しています。
	消灯	―	リンクが確立していません。

背面パネル

スイッチの背面パネルには AC 電源コネクタが配置されています。

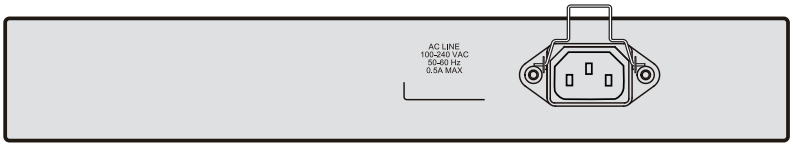


図 1-7　背面パネル図（DGS-3200-10）

図 1-8　背面パネル図（DGS-3200-16/GE）

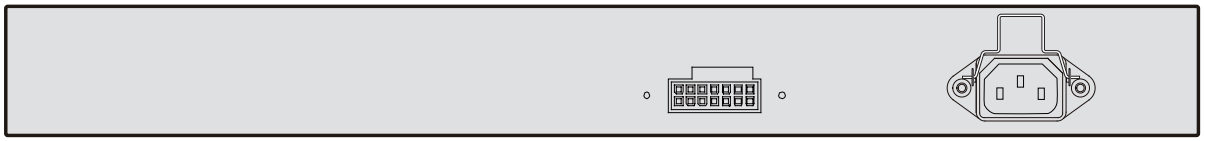


図 1-9　背面パネル図（DGS-3200-24/GE）

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。DGS-3200-24/GE の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（オプション）が自動的にスイッチに電源を供給します。

また、本製品付属の電源ケーブル抜け防止金具を取り付けます。電源ケーブルを取り付けの際に金具に固定すると、ケーブルの抜けを防止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。

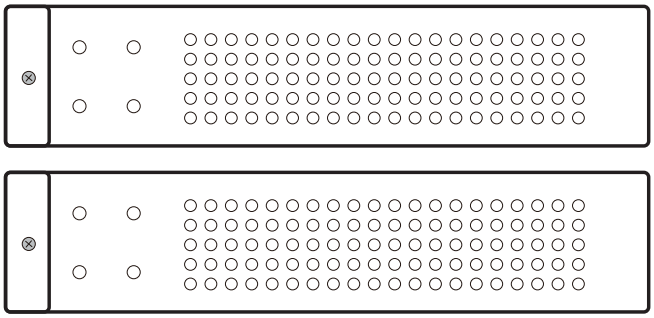


図 1-10　側面パネル図（DGS-3200-10）

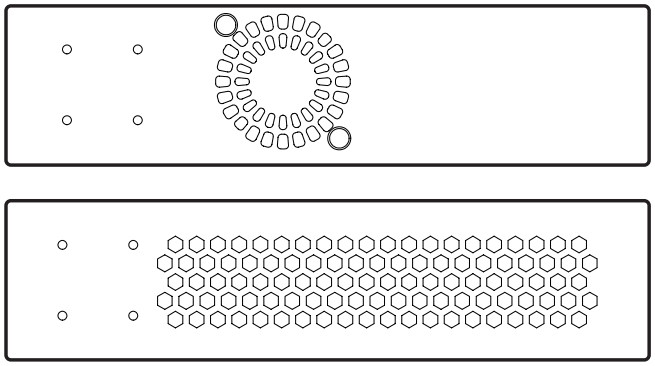


図 1-11　側面パネル図（DGS-3200-16/GE）

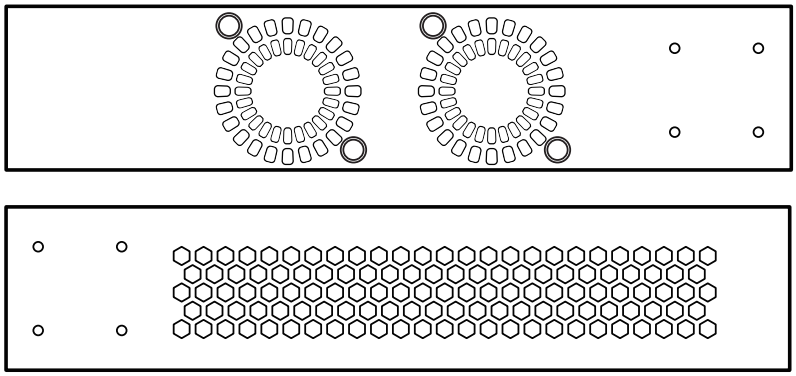


図 1-12　側面パネル図（DGS-3200-24/GE）

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（DGS-3200-10、DGS-3200-16/GE、または DGS-3200-24/GE）　x　1
- 電源ケーブル　x　1
- ラックマウントキット 1 式（ブラケット 2 枚、ネジ）
- 電源ケーブル抜け防止金具　x　1
- ゴム足（貼り付けタイプ）　x　4
- CD-ROM
- RS-232C コンソールケーブル
- クイックインストールガイド（英語版）
- 製品保証書

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

ネットワーク接続前の準備

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

- スイッチは、しっかりとした水平面で最低 3 キロの耐荷重性のある場所に設置してください。
- スイッチの上に重いものを置かないでください。
- 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本スイッチの周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後 16cm 以上の空間を保つようにしてください。
- スイッチは動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- スイッチは強い電磁場が発生するような場所（モータの周囲など）や、振動、ほこり、および直射日光を避けて設置してください。
- スイッチを水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

ゴム足の取り付け（19 インチラックに設置しない場合）

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

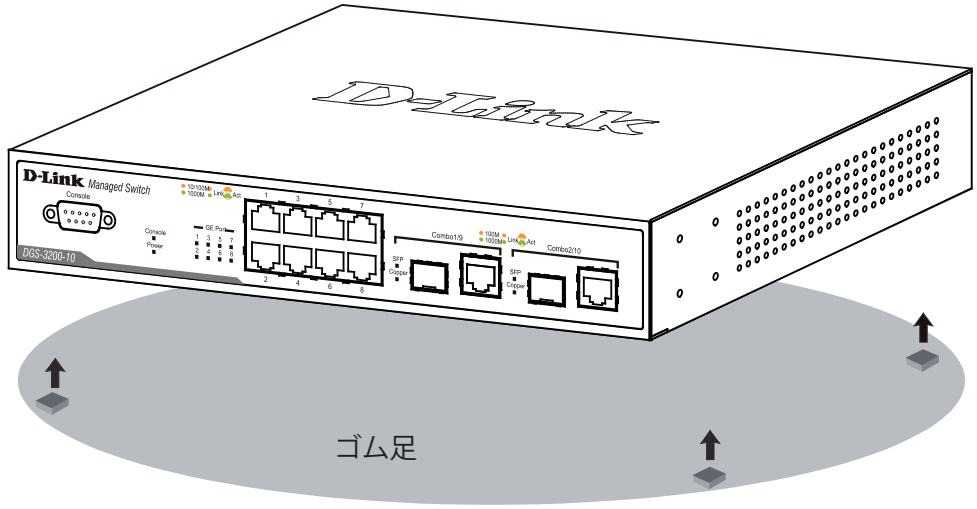


図 2-1　机や棚の上に設置する場合の準備図（DGS-3200-10）

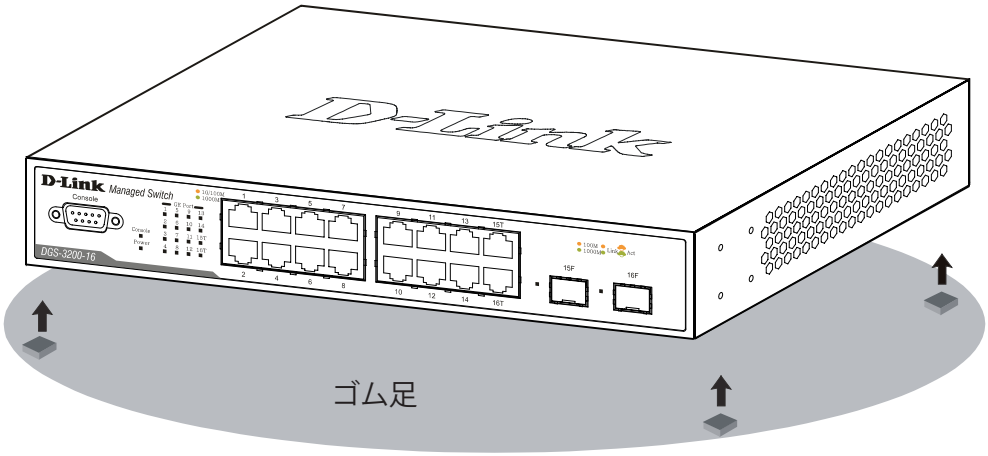


図 2-2　机や棚の上に設置する場合の準備図（DGS-3200-16/GE）

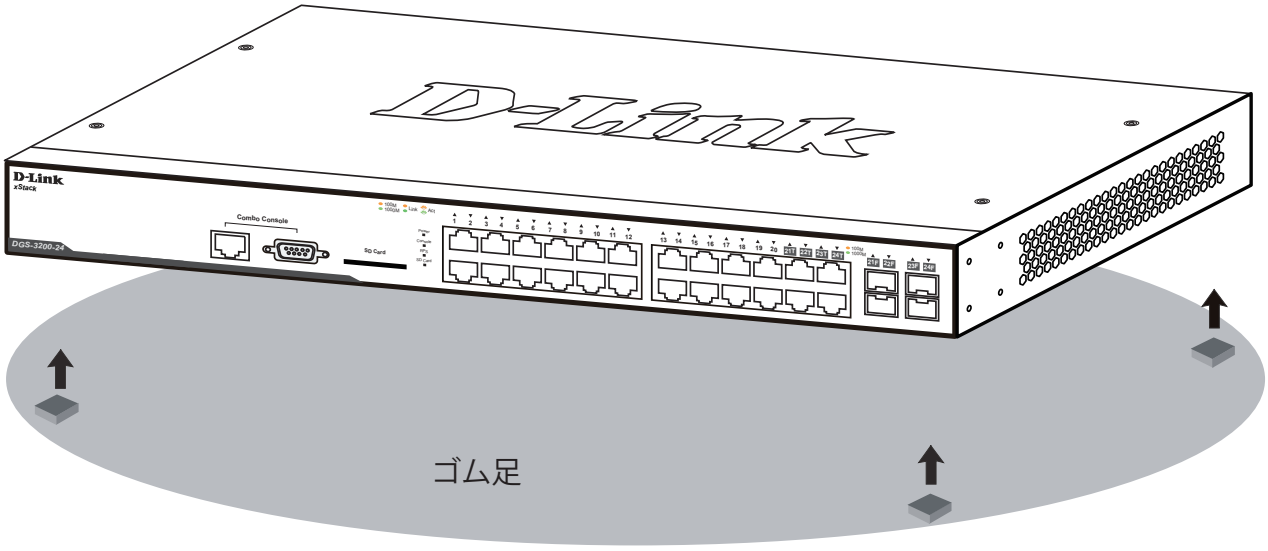


図 2-3　机や棚の上に設置する場合の準備図（DGS-3200-24/GE）

19 インチラックへの取り付け

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

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

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

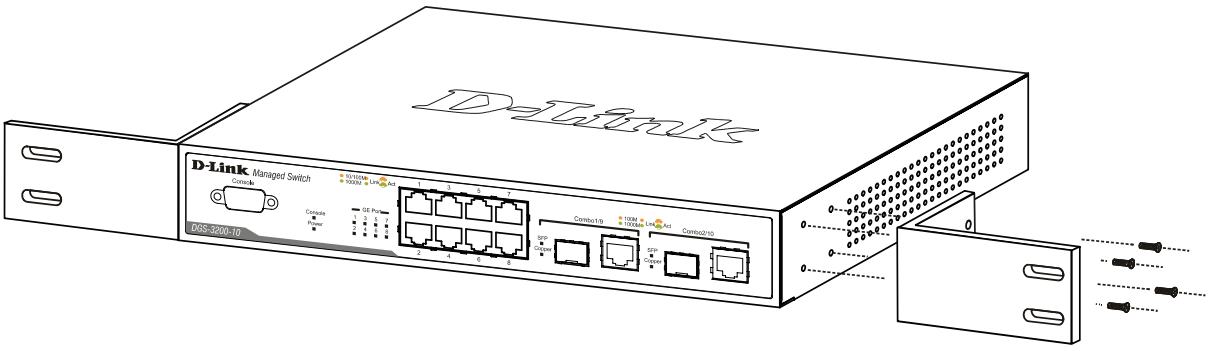


図 2-4　スイッチへのブラケットの取り付け図（DGS-3200-10）

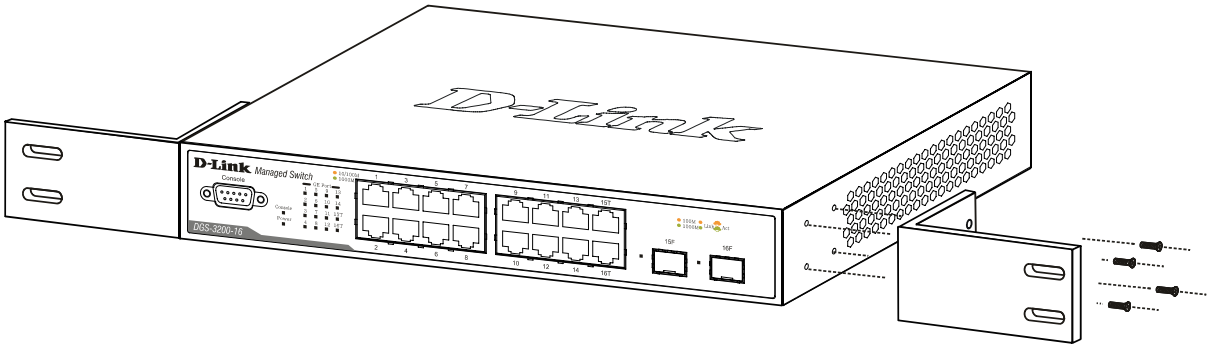


図 2-5　スイッチへのブラケットの取り付け図（DGS-3200-16/GE）

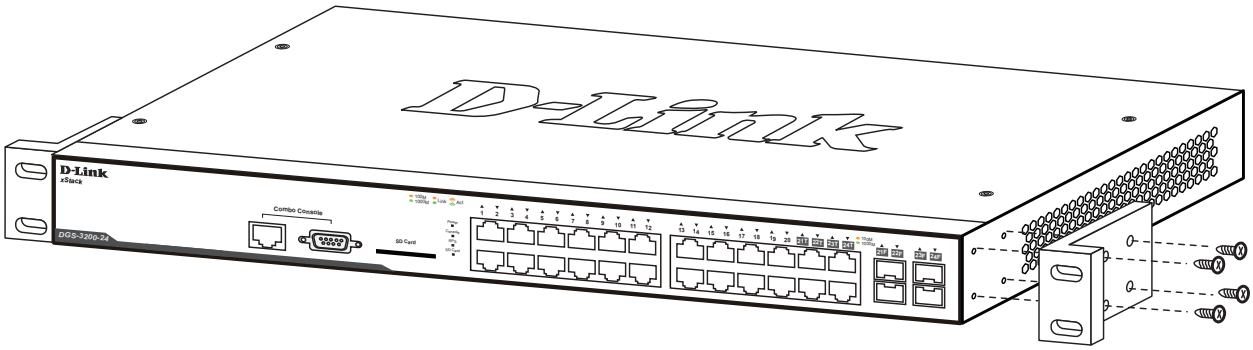


図 2-6　スイッチへのブラケットの取り付け図（DGS-3200-24/GE）

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

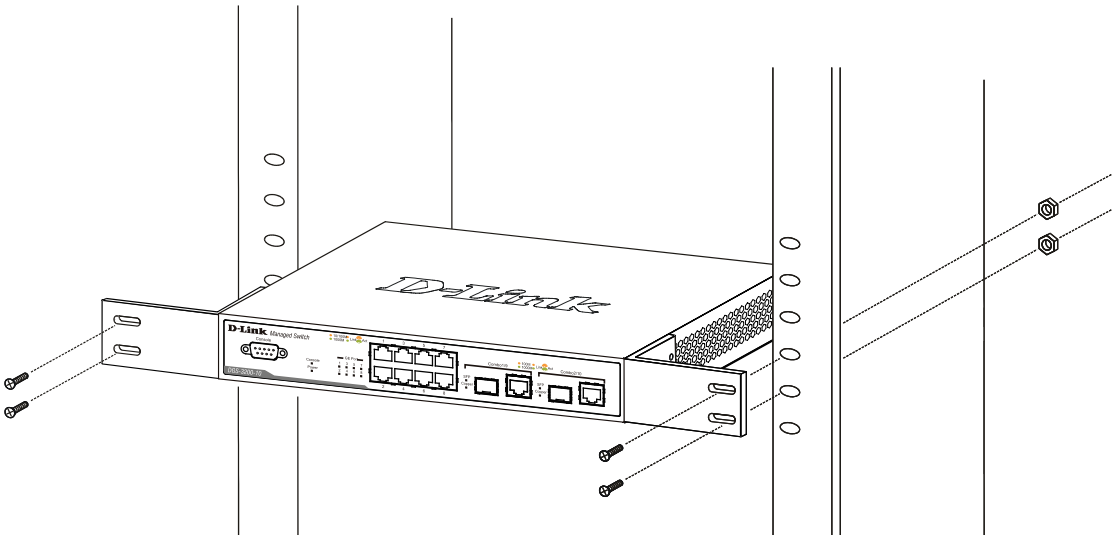


図 2-7　スイッチのラックへの設置図（DGS-3200-10）

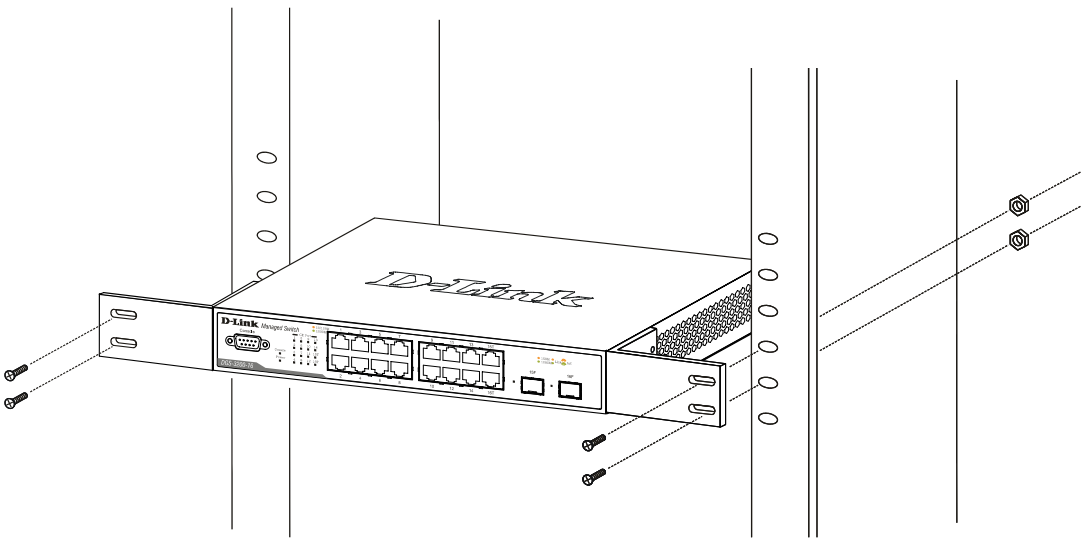


図 2-8　スイッチのラックへの設置図（DGS-3200-16/GE）

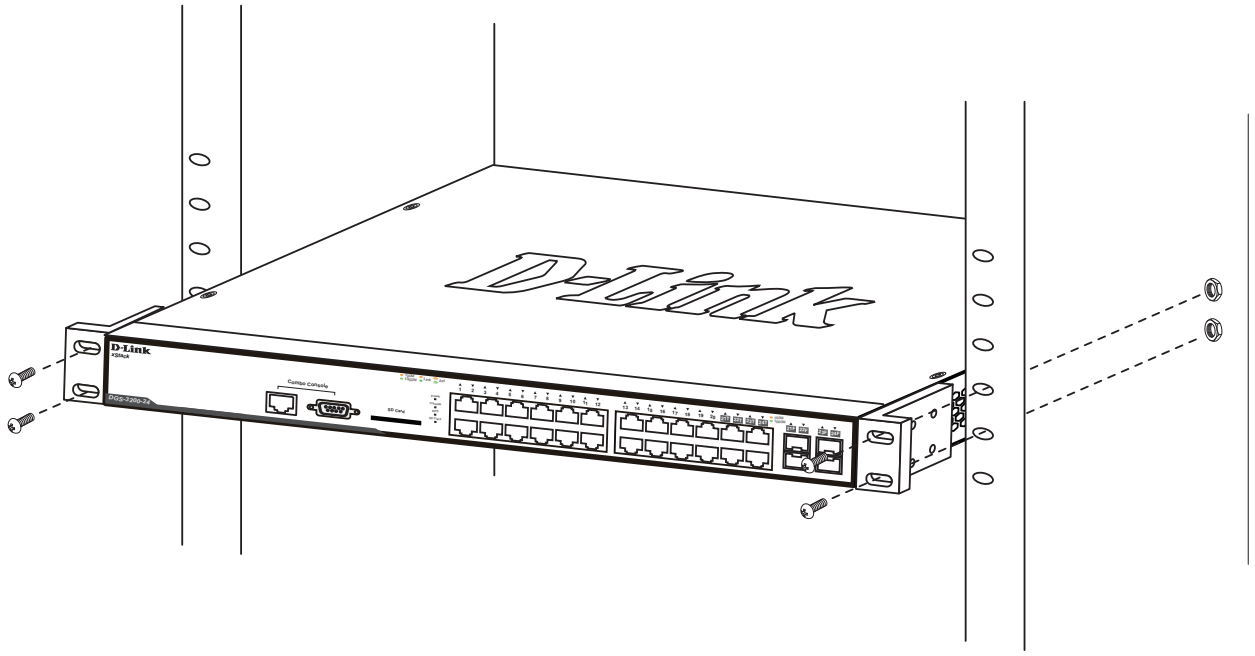


図 2-9　スイッチのラックへの設置図（DGS-3200-24/GE）

壁面への取り付け

DGS-3200-10 および DGS-3200-16/GE を壁面に取り付けることができます。以下の図と設置手順に従って取り付けてください。

注意　壁設置用ブラケットは、DGS-3200-10 のハードウェアバージョン A3 および B1 でのみサポートされています。

注意　壁設置用ブラケットは、DGS-3200-16/GE のハードウェアバージョン A2 でのみサポートされています。

DGS-3200-10 または DGS-3200-16/GE の背面の設置用ブラケットを壁にしっかり固定します。

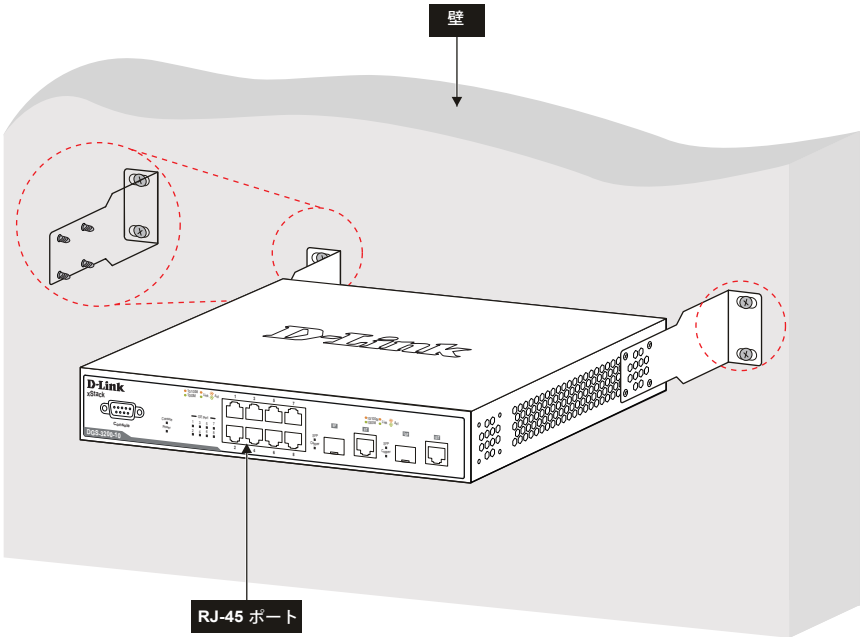


図 2-10　DGS-3200-10 の取り付け図

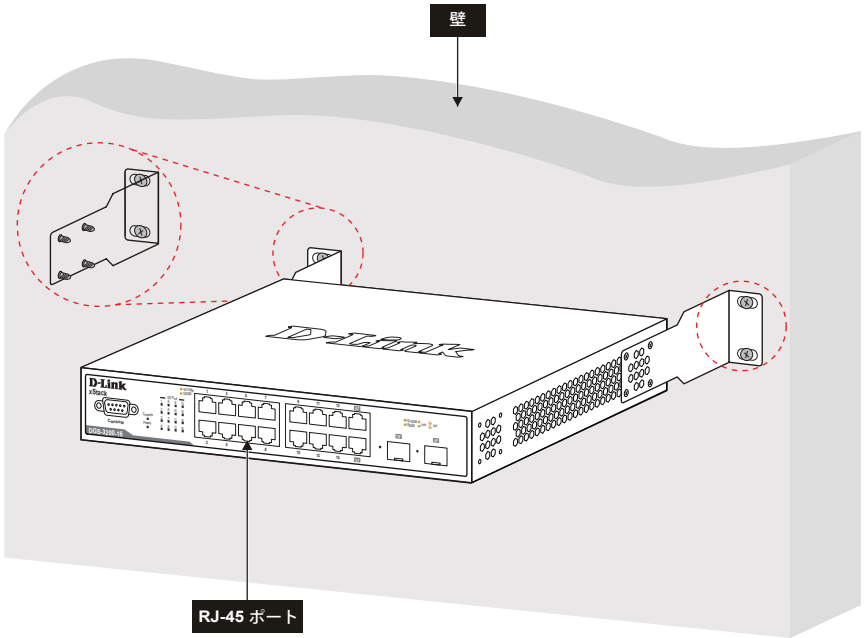
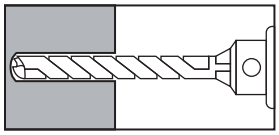


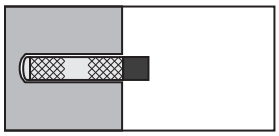
図 2-11　DGS-3200-16/GE の取り付け図

1. 設置を始める前に、壁設置用ブラケットを使用して楕円の穴位置の印を壁につけることでスイッチの取り付け位置を決めてください。これらの穴をコンクリート用のスリーブアンカーを取り付けるために壁取り付け用ブラケットと共に使用します。

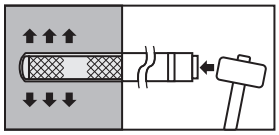
2. 直径 11mm のビットを持つパワードリルを使用して、あらかじめ印を付けた位置にそれぞれ 37 ～ 40mm の深さで 4 つの穴をあけます。



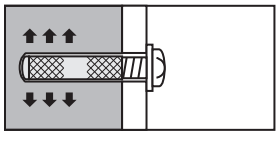
3. 各穴に、コンクリート用のスリーブアンカーの小さい方の端を入れます。



4. ハンマーを使用して、4 つの穴の一つ一つに各コンクリート用のスリーブアンカーをしっかりと打ち込みます。各スリーブアンカーはスイッチが固定される壁でほぼ同じ高さにする必要があります。



5. しっかりと各ネジを締めることによって、取り付けを完了します。



スイッチをセメントの壁面に固定する場合、以下に一部を図示した D-Link ウォールマントキット DRE-KIT018（オプション）コンクリートスリーブアンカーを使用することをお勧めします。D-Link ウォールマントキットは 8 個のネジと 4 個のコンクリート用のスリーブアンカーおよび壁設置用ブラケットから構成されています。

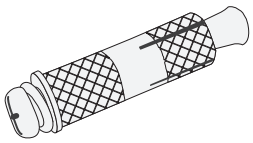


図 2-12　コンクリート用のスリーブアンカー

電源の投入

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

ギガビットコンボポート

10/100/1000Mbps ポートに加え、スイッチの前面パネルに 2 つのギガビットイーサネット・コンボポートを装備しています。これら 2 つのポートは 1000BASE-T ポートと SFP ポートの兼用ポートです。以下に、スイッチに SFP ポートモジュール（オプション）を挿入した図を示します。

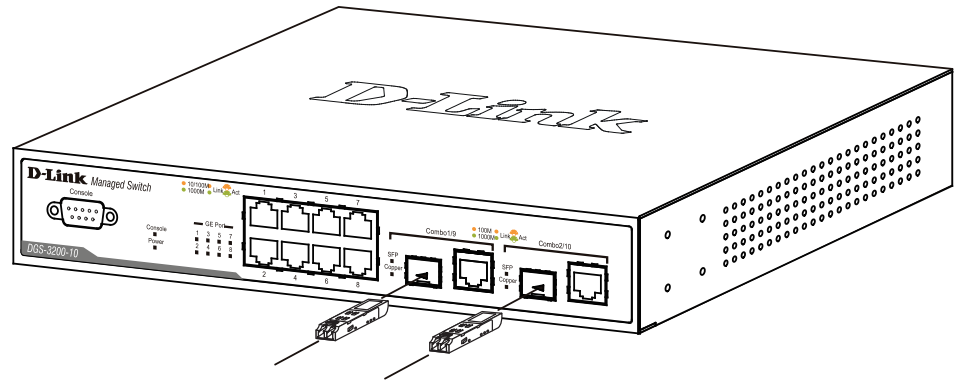


図 2-13　SFP モジュールを挿入（DGS-3200-10）

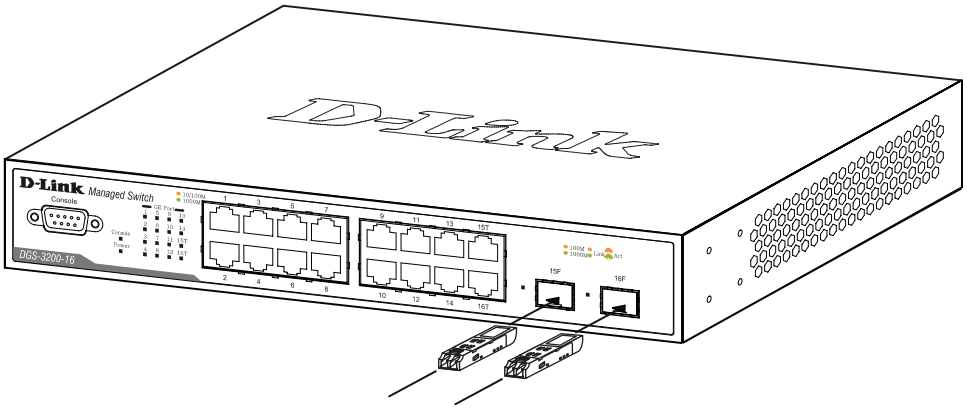


図 2-14　SFP モジュールを挿入（DGS-3200-16/GE）

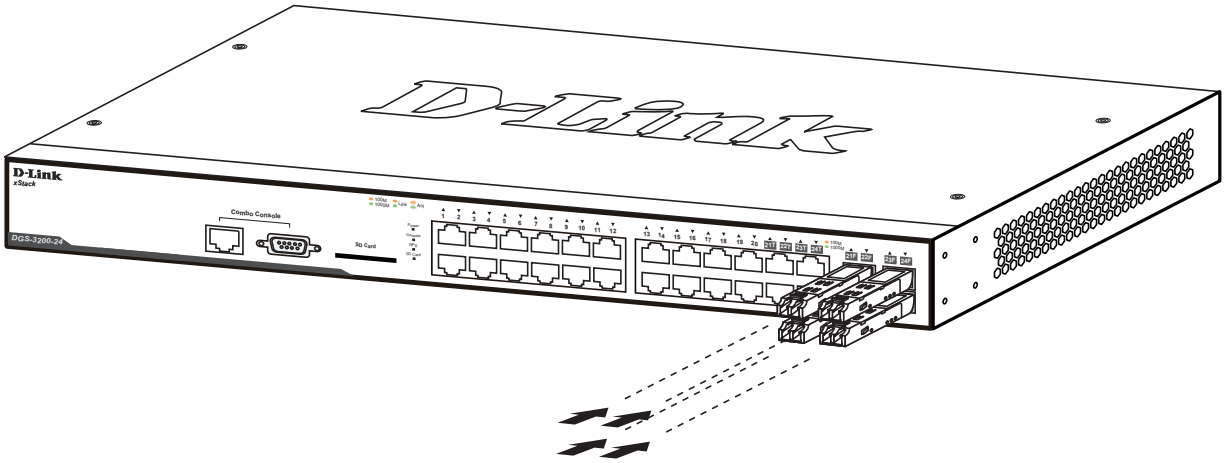


図 2-15　SFP モジュールを挿入（DGS-3200-24/GE）

注意　コンボポートのイーサネットポートがリンクしている場合、光トランシーバモジュールの DEM-211（オプション）を使用した SFP ポートはリンクエラーになります。DEM-211 を使用する場合は、イーサネットポートから接続している UTP ケーブルを抜いてください。

リダンダント電源システムの設置（DGS-3200-24/GE のみ）

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。

警告 DGS-3200-24/GE を DPS-200 以外のリダンダント電源ユニットに使用しないでください。

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

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

リダンダント電源との接続

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

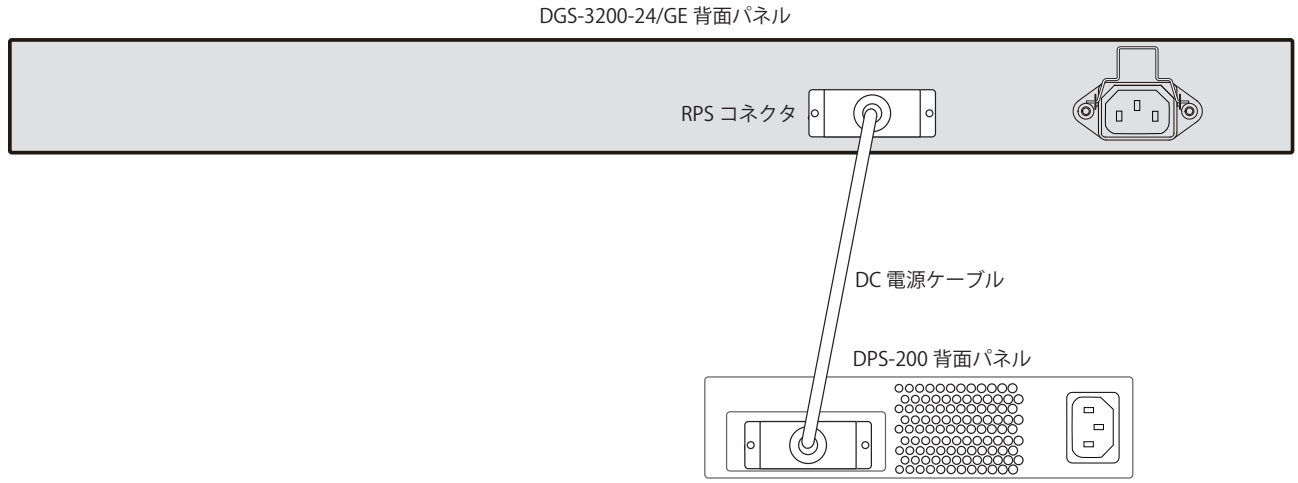


図 2-16　DPS-200 と DGS-3200-24/GE との接続図

1. 14 ピン DC 電源ケーブルの一端をスイッチのソケットに挿入し、もう一端をリダンダント電源装置に挿入します。
2. 標準の AC 電源ケーブルでリダンダント電源装置とメインの AC 電源を接続します。DPS-200 の前面の緑の LED 点灯により、正しく接続が行われたことが確認できます。
3. スイッチを再び AC 電源に接続します。DES-3828 などの機種では LED が点灯してリダンダント電源が動作していることを確認できます。
4. 本手順の実行による設定変更は必要ありません。

外部リダンダント電源システムとの接続

警告 前面および側面のスタビライザを装着せずにスイッチ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。ラックにスイッチを設置する前には、必ずスタビライザを装着してください。ラックにスイッチを搭載した後は、一度にスライド・アセンブリに乗せて引き出すスイッチは 1 つのみとしてください。2 つ以上のスイッチが引き出されると、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。

DPS-200 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。

DPS-900

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

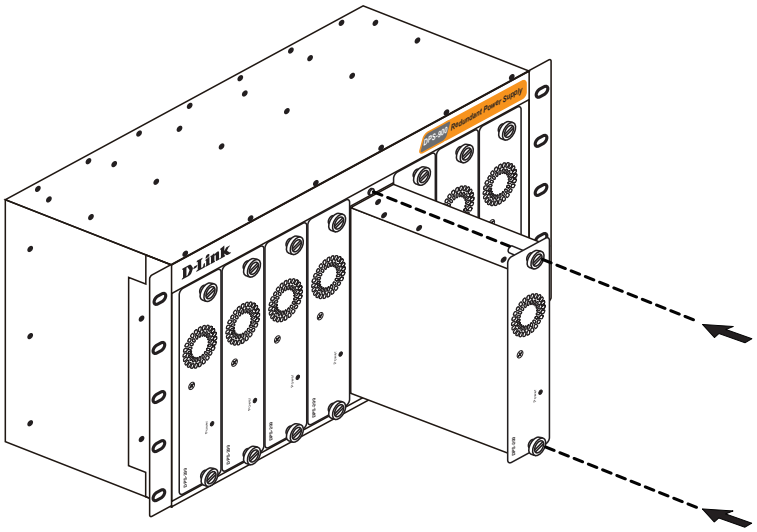


図 2-17　DPS-200 を DPS-900 に取り付ける

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

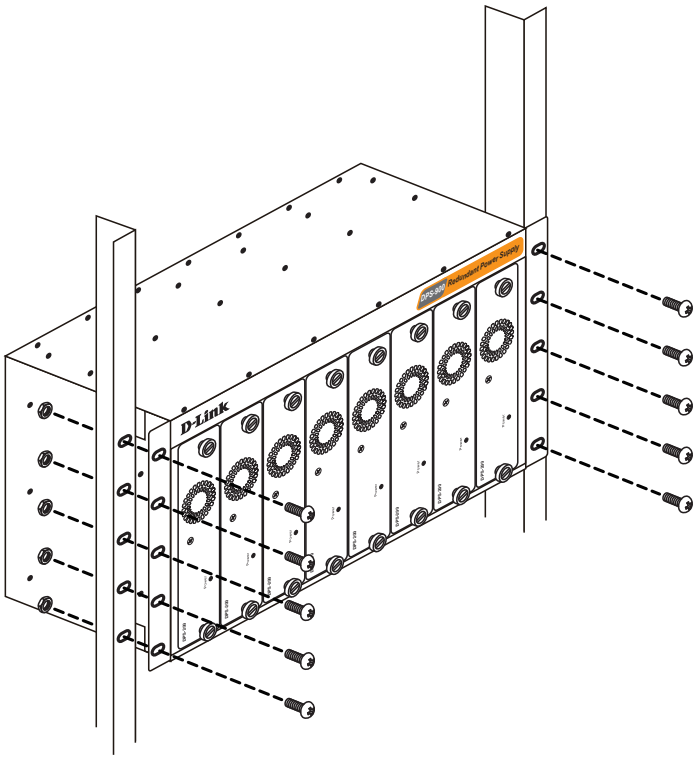


図 2-18　DPS-900 をラックに取り付ける

DPS-800

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

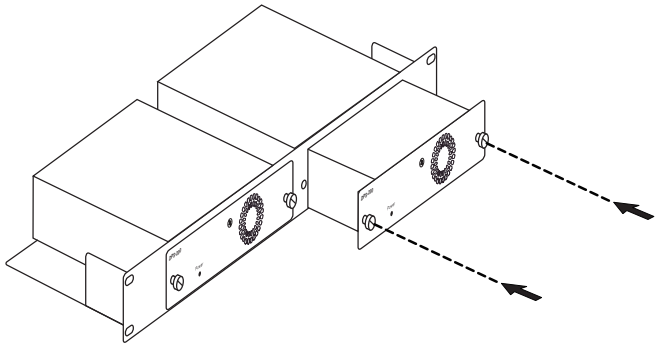


図 2-19　DPS-200 を DPS-800 に取り付ける

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

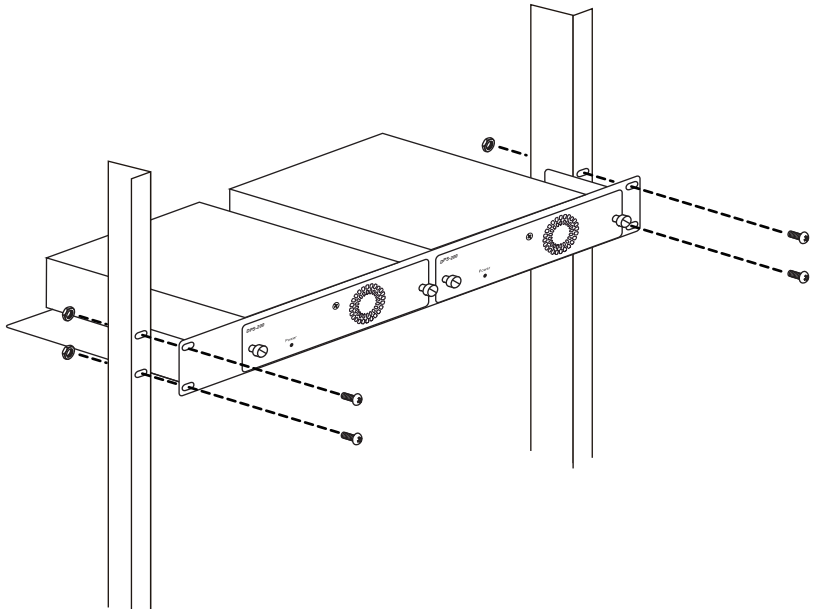


図 2-20　DPS-800 をラックに取り付ける

第 3 章　スイッチの接続

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

エンドノードと接続する

本スイッチの 1000BASE-T ポートとエンドノードをカテゴリ 3、4、5 の UTP ケーブルを使用して接続します。
エンドノードとは、RJ-45 コネクタ対応 10/100/1000Mbps ネットワークインタフェースカードを装備した PC やルータを指しています。エンドノードとスイッチ間はカテゴリ 3、4、または 5 の UTP ケーブルで接続できます。エンドノードへの接続はスイッチ上のすべてのポートから行えます。

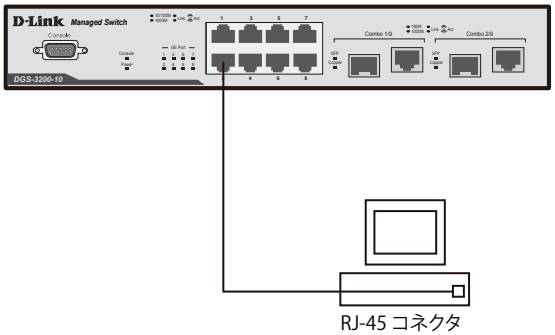


図 3-1　エンドノードと DGS-3200-10 の接続図

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

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

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

ケーブル仕様については 252 ページの「付録 A ケーブルとコネクタ」を参照してください。

スイッチ（DGS-3200-10）との接続例

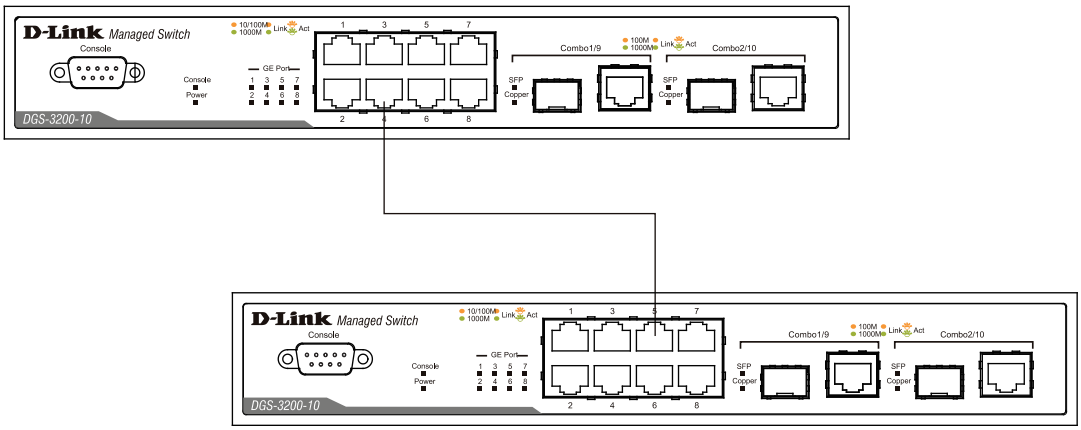


図 3-2　ストレート、クロスケーブルでスイッチ（DGS-3200-10）と接続する図

スイッチ（DGS-3200-16/GE）との接続例

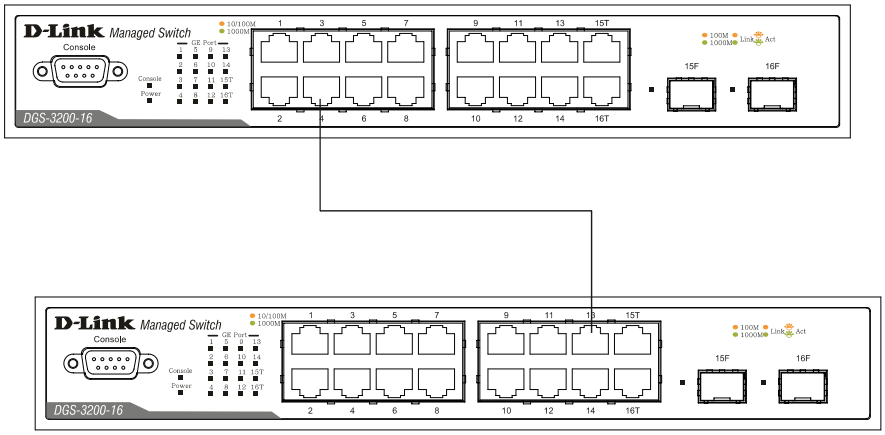


図 3-3　ストレート、クロスケーブルでスイッチ（DGS-3200-16/GE）と接続する図

スイッチ構成例（DGS-3200-10）

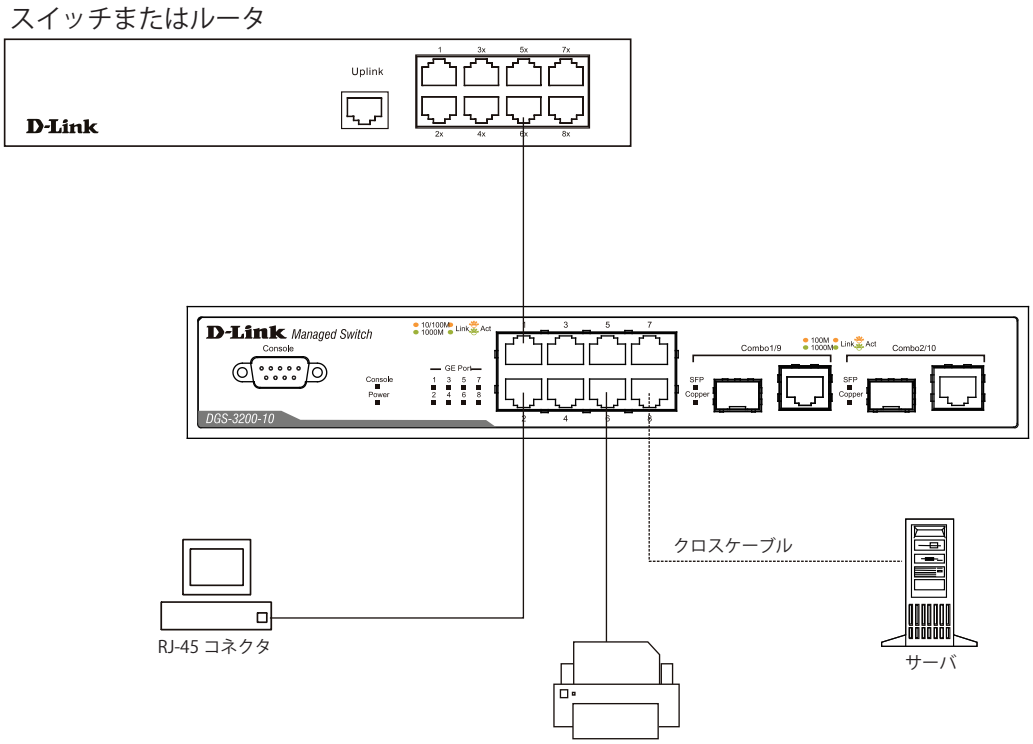


図 3-4　スイッチ構成例（DGS-3200-10）

スイッチ構成例（DGS-3200-16/GE）

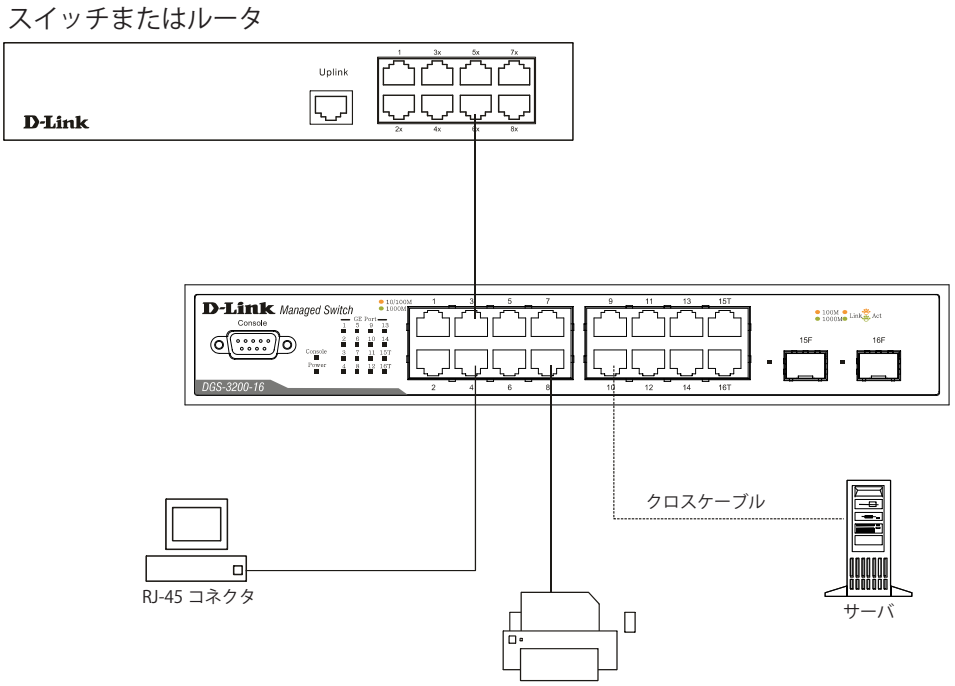


図 3-5　スイッチ構成例（DGS-3200-16/GE）

スイッチ構成例（DGS-3200-24/GE）

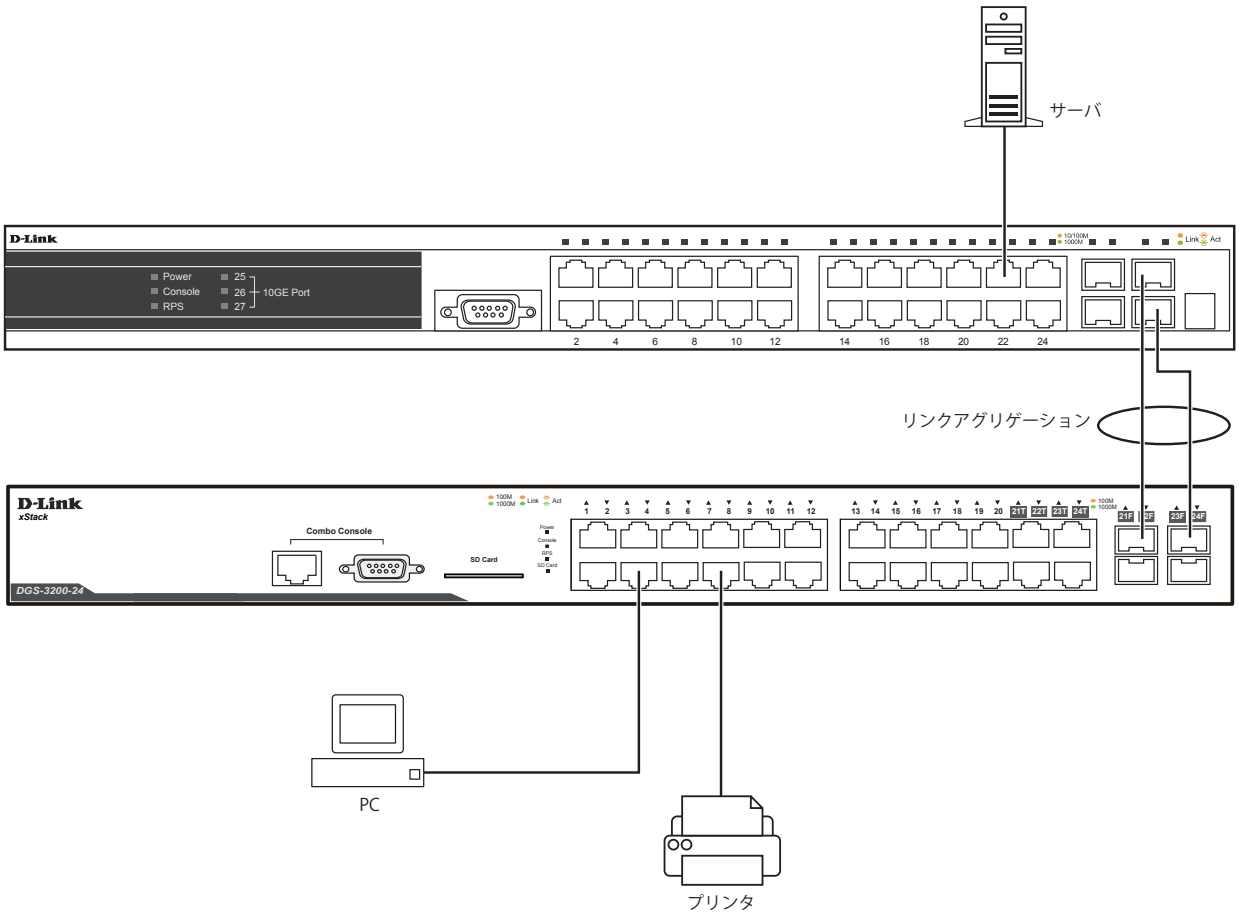


図 3-6　スイッチ構成例（DGS-3200-24/GE）

バックボーンまたはサーバと接続する

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

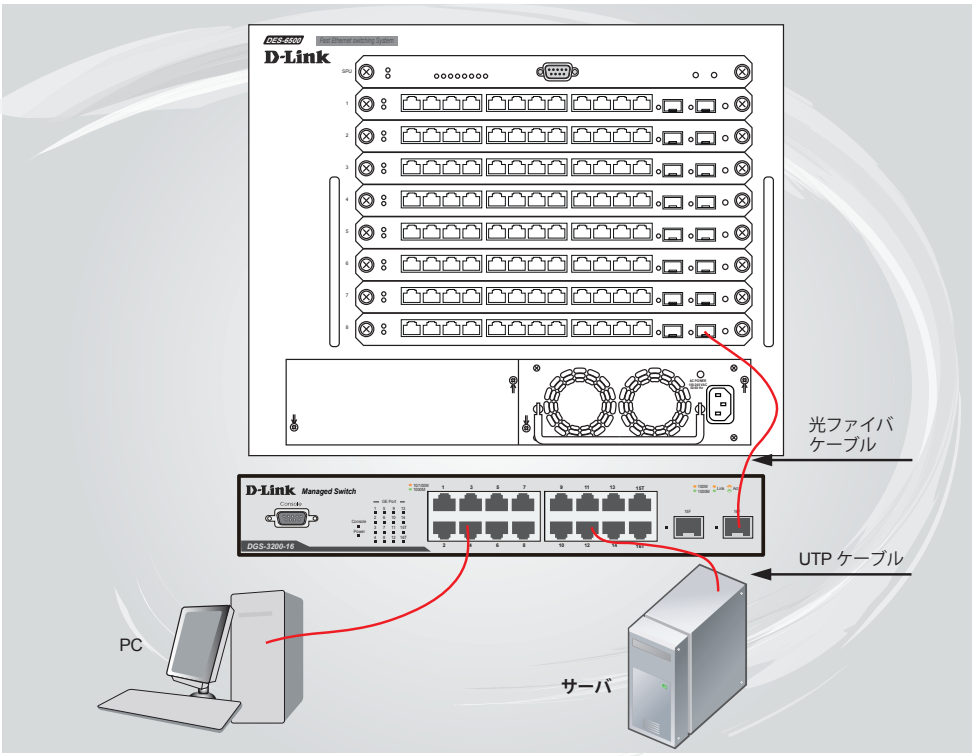


図 3-7　サーバ、PC、スイッチスタックとのアップリンク接続図（DGS-3200-16/GE）

第 4 章　スイッチ管理の導入

管理オプション

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

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

- SNMP ベースの管理
  SNMP をサポートするコンソールプログラムでスイッチの管理をすることができます。本スイッチは SNMP v1.0、v2.0、および v3.0 をサポートしています。SNMP エージェントは、受信した SNMP メッセージを復号化し、マネージャからの要求に対してデータベースに保存された MIB オブジェクトを参照して応答を返します。SNMP エージェントは MIB オブジェクトを更新し、統計情報およびカウンタ情報を生成します。

- コンソールポートの接続（RS-232 DCE）
  スイッチのモニタリングと設定のために RS-232C シリアルポート（D-Sub9 ピンメスコネクタ）を搭載しています。
  コンソールポートを使用するためには以下をご用意ください。

  - ターミナルソフトを操作するシリアルポート搭載の端末またはコンピュータ
  - D-Sub9 ピン メスコネクタを持つモデムケーブル、または RS-232C クロスケーブル

端末をコンソールポートに接続する

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

注意 Microsoft® Windows® 2000 でハイパーターミナルを使用する場合は、Windows 2000 Service Pack 2 以降がインストール済みであることを確認してください。Windows 2000 Service Pack 2 以降でないとハイパーターミナルの VT100 端末で矢印キーは使用できません。Windows 2000 Service Pack に関する情報はマイクロソフト社のホームページでご確認ください。

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

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

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

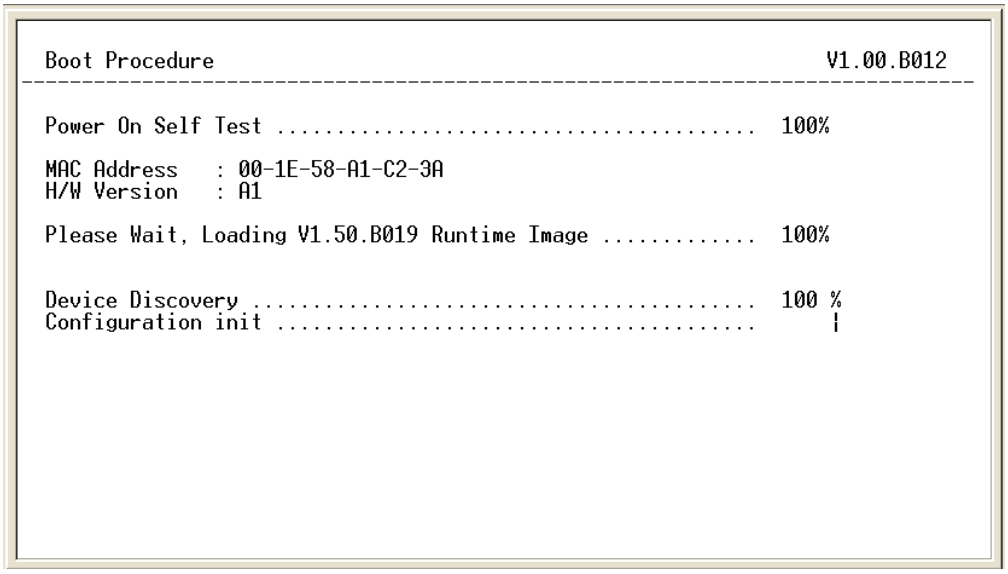


図 4-1　コンソールのブート画面

スイッチへの初回接続

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

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

スイッチに初めて接続すると、次のログイン画面が表示されます。

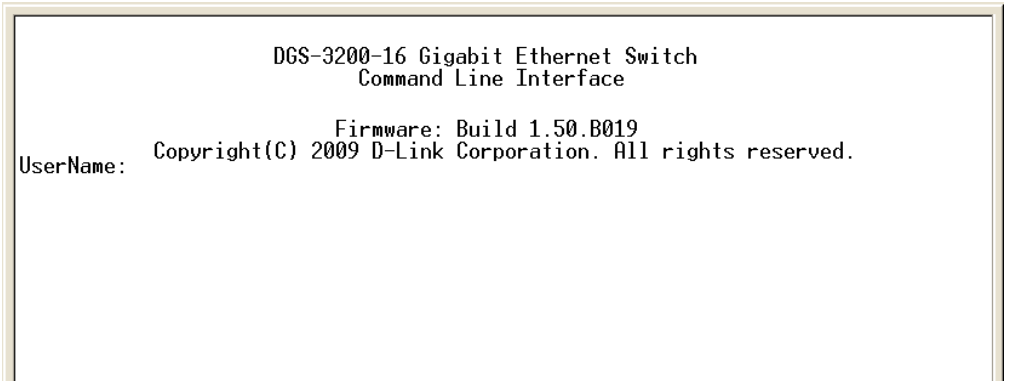


図 4-2　コマンドプロンプト

注意　「Ctrl」キーと「R」を同時に押下すると、コンソール画面のリフレッシュをします。本コマンドはコンソール画面をリフレッシュするために、いつでも実行することができます。

初回接続する場合、「UserName」または「PassWord」は登録されていません。「UserName」と「PassWord」には何も入力せず、「Enter」キーを押します。既に設定されている場合は、「UserName」と「PassWord」の両方を入力します。
「DGS-3200-10:4#」、「DGS-3200-16:4#」または「DGS-3200-24:4#」というコマンドプロンプトが表示されます。

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

パスワード設定

本スイッチは、初期値としてユーザ名およびパスワードの設定はありません。はじめにユーザアカウントの作成を行います。定義済みの管理者レベルのユーザ名でログインすることでスイッチ管理ソフトウェアに接続できます。
はじめてログインした際に本スイッチに対する不正アクセスを防ぐために 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-3200-16:4#create account admin newmanager
Command: create account admin newmanager

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

Success.

DGS-3200-16:4#
```

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

SNMP 設定

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

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

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

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

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

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

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

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

個別のユーザや SNMP マネージャグループに SNMP バージョン 3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。そのような管理機能の可否は、各 MIB に関連付けられる OID（Object Identifier）を使用して定義します。SNMP バージョン 3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。スイッチでの SNMP バージョン 3 の設定方法については 47 ページの「IP Address（IP アドレス）」をご参照ください。

トラップ

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

MIB

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

IP アドレスの割り当て

各スイッチに対して、SNMP ネットワークマネージャまたは他の TCP/IP アプリケーション（例 : BOOTP、TFTP）と通信するために IP アドレスを割り当てる必要があります。

本スイッチの IP アドレスの初期値は 10.90.90.90 です。

この IP アドレスはご使用のネットワークのアドレス計画に基づいて変更することができます。

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

```
Device Type        : DGS-3200-16 Gigabit Ethernet Switch
MAC Address        : 00-1E-58-B4-65-89
IP Address         : 10.90.90.90 (Manual)
VLAN Name          : default
Subnet Mask        : 255.0.0.0
Default Gateway    : 0.0.0.0
Boot PROM Version  : Build 1.00.B012
Firmware Version   : Build 1.50.B019
Hardware Version   : A1
Serial Number      : P4EU187000051
System Name        :
System Location    :
System Contact     :
Spanning Tree      : Disabled
GVRP               : Disabled
IGMP Snooping      : Disabled
MLD Snooping       : Disabled
VLAN Trunk         : Disabled
Telnet             : Enabled (TCP 23)
Web                : Enabled (TCP 80)
SNMP               : Disabled
RMON               : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

図 4-3　show switch コマンドによる表示画面

本スイッチの MAC アドレスは、Web ベース管理インタフェースの「Device Information」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。

```
DGS-3200-16:4#config ipif System ipaddress 10.24.22.100/255.0.0.0
Command: config ipif System ipaddress 10.24.22.100/8

Success.

DGS-3200-16:4#
```

図 4-4　スイッチへの IP アドレス割り当て時の表示画面

上記例では、スイッチに IP アドレス「10.24.22.100」とサブネットマスク「255.0.0.0」を割り当てています。CIDR 表記（10.24.22.100/8）でのアドレス指定も可能です。「Success.」というメッセージにより、コマンドの実行が成功したことが確認できます。スイッチのアドレス設定が終了すると、Telnet での CLI、または Web ベースによる管理を開始することができます。

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（以降、Web マネージャと記載）経由で管理、設定およびモニタできます。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。

Web マネージャとコンソールプログラム（および Telnet）は、異なるインタフェースを経由して同じスイッチ内部のソフトウェアにアクセスし、その設定を行います。つまり、Web マネージャ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。

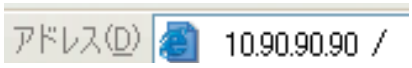


図 5-1　URL の入力画面

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。

注意　安全のためにネットワークに接続する前にユーザ名とパスワードを必ず設定してください。

以下のユーザ認証画面が表示されます。

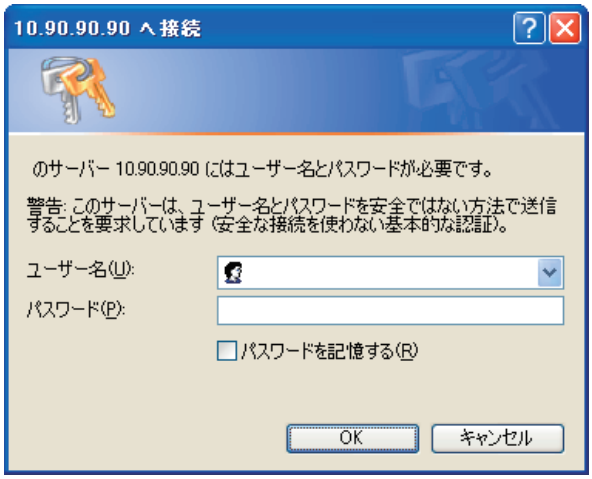


図 5-2　パスワード入力用画面

「ユーザー名」と「パスワード」を空白のまま「OK」をクリックします。Web マネージャに接続します。Web ブラウザによって使用可能な機能を以下で説明します。
CLI でユーザ名、パスワードを既に設定している場合は、設定した項目を入力します。

Web マネージャの画面構成

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

Web マネージャのメイン画面について

Web マネージャのメイン画面は 3 つのエリアで構成されています。

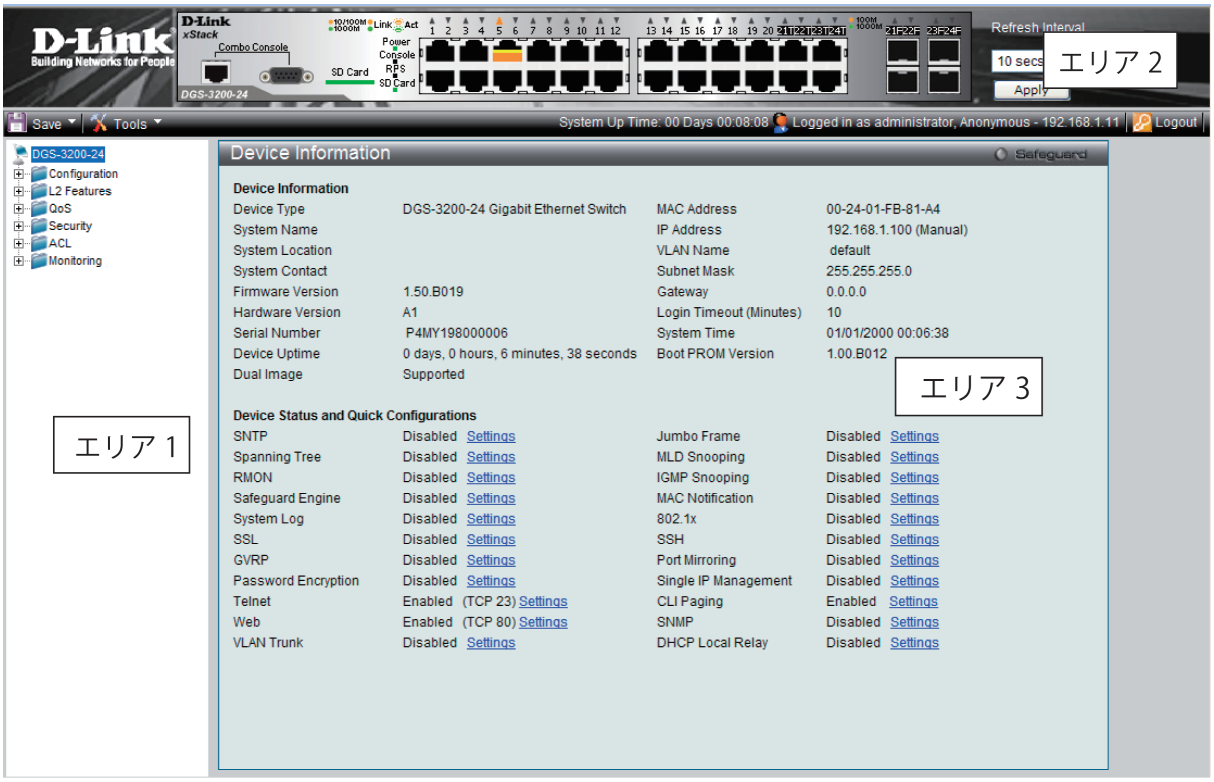


図 5-3　Web マネージャのメインページ

エリア	機能
エリア 1	表示するメニューまたは画面を選択します。フォルダをオープンしたり、ハイパーリンクする画面ボタンやサブフォルダをクリックすることで画面を表示します。
エリア 2	本スイッチの前面パネルをリアルタイムに近い画像で表示します。本エリアにはスイッチのポートや拡張モジュール、各ポートの状態、デュプレックスモード、フローコントロールの状態などが、指定したモードにより表示できます。D-Link のロゴをクリックすると D-Link のホームページに接続します。
エリア 3	ユーザの選択や設定データのエントリを元にスイッチの状態を表示します。さらにハイパーリンクはスイッチにすぐに有効にできる多くの機能を提供します。

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
Configuration	Device Information	スイッチの主な設定情報を表示します。	44 ページ
	System Information	スイッチの基本情報を表示します。	46 ページ
	Serial Port Settings	ボーレートの値と自動ログアウト時間を調整します。	46 ページ
	IP Address	IP アドレス設定を変更します。	47 ページ
	IPv6 Interface Settings	IPv6 インタフェース設定を行います。	49 ページ
	IPv6 Route Table	IPv6 ルートテーブルのアドレスを設定します。	50 ページ
	IPv6 Neighbor Settings	IPv6 Neighbor の設定を行います。	50 ページ
	Port Configuration	物理ポートの属性やプロパティなどの設定および情報を表示します。	51 ページ
	Static ARP Settings	IP アドレスを物理アドレスに変換し、IP アドレスと MAC アドレスを対応させます。	53 ページ
	User Accounts	ユーザおよびユーザの権限を設定します。	54 ページ
	System Log Configuration	フラッシュメモリにスイッチログを保存する方法、Syslog サーバの設定を行います。	55 ページ
	System Severity Settings	アラートのレベルおよびアラート発生時のアクションを設定します。	57 ページ
	DHCP/BOOTP Relay	DHCP/BOOTP リレーのグローバル設定、DHCP/BOOTP サーバの登録を行います。	58 ページ
	DHCP Local Relay Settings	DHCP/BOOTP ローカルリレーの設定を有効にして、設定を行います。	60 ページ
	DHCP Auto Configuration Settings	DHCP 自動設定機能を有効 / 無効にします。	60 ページ
	MAC Address Aging Time	MAC アドレスエージングタイムを設定します。	61 ページ
	Web Settings	スイッチに Web ステータスを設定します。	61 ページ
	Telnet Settings	スイッチに Telnet 設定をします。	61 ページ
	Password Encryption	スイッチのパスワードの暗号化設定をします。	62 ページ
	CLI Paging Settings	コマンドラインインタフェースの改頁処理を設定します。	62 ページ
	Firmware Information	スイッチに格納されているファームウェアイメージの情報の確認、起動ステータスの設定の削除を行います。	63 ページ
	Power Saving Settings	スイッチに搭載した省電力機能を実行することができます。	64 ページ
	Dual Configuration Settings	スイッチが次回の再起動時に使用する起動ファイルを設定します。	64 ページ
	SMTP Settings	問題が発生した場合に設定した E-mail アドレスに従ってスイッチのログファイルを送信する SMTP サーバを設定します。	66 ページ
	Ping Test	指定アドレスに ICMP Echo パケットを送信します。	67 ページ
	SNTP Settings	本製品に時刻設定をします。	68 ページ
	MAC Notification Settings	MAC 通知機能の設定を行います。	70 ページ
	SNMP Settings	SNMP 設定を行います。	72 ページ
	Single IP Management	SIM 設定を行います。	80 ページ
	SD Card FS Settings	SD フラッシュカードを使用してファームウェアイメージ、コンフィグレーションのバックアップまたはリストアを行います。	90 ページ
L2 Features	Jumbo Frame	ジャンボフレーム機能を有効 / 無効にします。	93 ページ
	Egress Filter Settings	イーグレスフィルタを設定します。	94 ページ
	802.1Q VLAN	802.1Q VLAN 設定を行います。	95 ページ
	Private VLAN Settings	プライベート VLAN を作成します。	101 ページ
	802.1v Protocol VLAN	802.1v プロトコル VLAN 設定を行います。	105 ページ
	MAC Based VLAN Settings	MAC ベース VLAN を設定します。	107 ページ
	GVRP Settings	VLAN 構成情報を共有するために GVRP 設定を行います。	108 ページ
	PVID Auto Assign Settings	PVID 自動割り当てを設定します。	108 ページ
	Trunking	ポートトランキング設定を行います。	109 ページ
	VLAN Trunk Settings	多くの VLAN ポートを集約して VLAN トランクを作成します。	111 ページ
	LACP Port Settings	ポートトランキンググループを設定します。	112 ページ
	Traffic Segmentation	トラフィックフローの分割設定を行います。	113 ページ
	IGMP Snooping Settings	IGMP Snooping 機能を設定します。	114 ページ
	MLD Snooping Settings	MLD Snooping 機能を設定します。	122 ページ
	Port Mirroring	ポートミラーリングの設定を行います。	125 ページ
	Loopback Detection Settings	ループバック検知機能の設定を行います。	126 ページ
	Spanning Tree	スパニングツリープロトコルの設定を行います。	127 ページ
	Forwarding & Filtering	ユニキャスト / マルチキャストフォワーディングとフィルタリングの設定を行います。	134 ページ

メインメニュー	サブメニュー	説明	参照ページ
QoS	Bandwidth Control	管理ステーションの IP アドレスを設定し、リモート管理を有効にします。	137 ページ
	Traffic Control	ユーザおよびユーザの権限を設定します。	138 ページ
	802.1p Default Priority	802.1X 認証、RADIUS サーバおよびゲスト VLAN の設定を行います。	139 ページ
	802.1p User Priority	TACACS/XTACACS/TACACS+/RADIUS 認証の設定を行います。	140 ページ
	QoS Scheduling Mechanism	ユーザ権限でログインしたユーザを管理者権限に変更します。	141 ページ
Security	Safeguard Engine	セーフガードエンジンの設定を行います。	142 ページ
	Trusted Host	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。	144 ページ
	IP-MAC-Port Binding	IP アドレスと MAC アドレスを結合し、レイヤ間通信を行います。	145 ページ
	Port Security	ダイナミックな MAC アドレス学習をロックします。	151 ページ
	DHCP Server Screening	指定ポートからの DHCP サーバパケットをフィルタします。	153 ページ
	Guest VLAN	802.1X ゲスト VLAN を設定します。	154 ページ
	802.1X	ポート単位の 802.1X 認証を設定します。	160 ページ
	SSL Settings	証明書の設定、暗号スイートの設定を行います。	164 ページ
	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。	166 ページ
	Access Authentication Control	TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。	169 ページ
	MAC Based Access Control	MAC アドレス認証機能を設定します。	176 ページ
	Web-based Access Control	Web ベースアクセスコントロールを設定します。	179 ページ
	JWAC	スイッチの拡張 Web ベースのアクセスコントロールを設定します。	184 ページ
	Multiple Authentication	同一のスイッチポートで異なる認証方式を実行しネットワークに接続します。	188 ページ
	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。	192 ページ
	ARP Spoofing Prevention Settings	ハッカーや権限のない第三者による ARP Spoofing を防御します。	192 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。	193 ページ
	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。	194 ページ
	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。	206 ページ
	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するために使用します。	216 ページ
Monitoring	Device Environment	ファンや温度などデバイスの状態を表示します。	217 ページ
	Cable Diagnostic	ケーブルの品質やエラーの種類を診断します。	218 ページ
	CPU Utilization	CPU 使用率を表示します。	219 ページ
	Port Utilization	ポートの帯域使用率を表示します。	220 ページ
	Packet Size	受信パケット数を表示します。	221 ページ
	Packets	パケット統計情報を表示します。	222 ページ
	Errors	エラー統計情報を表示します。	226 ページ
	Port Access Control	802.1X 統計情報をポートごとに表示します。	229 ページ
	Browse ARP Table	スイッチ上の現在の ARP エントリを表示します。	238 ページ
	Browse VLAN	各ポートの VLAN ステータスを VLAN ごとに表示します。	238 ページ
	Browse Router Port	ルータポートを参照します。	239 ページ
	Browse MLD Router Port	IPv6 ルータポートを参照します。	239 ページ
	Browse Session Table	最後に起動してからの管理セッションを表示します。	239 ページ
	IGMP Snooping Group	IGMP Snooping テーブルを表示します。	240 ページ
	MLD Snooping Group	MLD Snooping テーブルを表示します。	240 ページ
	WAC Authenticating State	現在の WAC 認証状態の表示、および WAC 認状態の設定を削除します。	241 ページ
	JWAC Host Table	JWAC ホストテーブルを表示します。	241 ページ
	MAC Address Table	ダイナミック MAC アドレスフォワーディングテーブルを表示します。	242 ページ
	System Log	ヒストリログを表示します。	243 ページ
	MAC Authentication State	MAC アドレス認証情報を表示します。	244 ページ

メインメニュー	サブメニュー	説明	参照ページ
Save	Save Configuration	スイッチのメモリにコンフィグレーションを保存します	246 ページ
	Save Log	スイッチのメモリにログを保存します	246 ページ
	Save All	スイッチのメモリにコンフィグレーションとログを保存します	246 ページ
Tools	Download Configuration File / Download Configuration File to NV-RAM	NV-RAM にコンフィグレーションファイルをダウンロードします。	248 ページ
	Download Configuration File to SD Card（DGS-3200-24/GE のみ）	SD カードにコンフィグレーションファイルをダウンロードします。	248 ページ
	Download Firmware / Download Firmware to NV-RAM	NV-RAM にファームウェアファイルをダウンロードします。	249 ページ
	Download Firmware to SD Card（DGS-3200-24/GE のみ）	SD カードにファームウェアファイルをダウンロードします。	249 ページ
	Upload Configuration File / Upload Configuration File to TFP	コンフィグレーションファイルをアップロードします。	250 ページ
	Upload Log File / Upload Log File to TFTP	ログファイルをアップロードします。	250 ページ
	Reset	工場出荷時設定に戻し、メモリに保存します。	251 ページ
	Reboot System	スイッチの再起動を行います。	251 ページ

第 6 章　Configuration（スイッチの主な設定）

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

サブメニュー	説明	参照ページ
Device Information（デバイス情報）	スイッチの主な設定情報を表示します。	44 ページ
System Information（システム情報）	スイッチの基本情報を表示します。	46 ページ
Serial Port Settings（シリアルポート設定）	ボーレートの値と自動ログアウト時間を調整します。	46 ページ
IP Address（IP アドレス）	IP アドレス設定を変更します。	47 ページ
IPv6 Interface Settings（IPv6 インタフェース設定）	IPv6 インタフェース設定を行います。	49 ページ
IPv6 Route Table（IPv6 ルートテーブル）	IPv6 ルートテーブルのアドレスを設定します。	50 ページ
IPv6 Neighbor Settings（IPv6 Neighbor 設定）	IPv6 Neighbor の設定を行います。	50 ページ
Port Configuration（ポート設定）	物理ポートの属性やプロパティなどの設定および情報を表示します。	51 ページ
Static ARP Settings（スタティック ARP 設定）	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。	53 ページ
User Accounts（ユーザアカウントの設定）	ユーザおよびユーザの権限を設定します。	54 ページ
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。	55 ページ
System Severity Settings（システムレベル設定）	アラートのレベルおよびアラート発生時のアクションを設定します。	57 ページ
DHCP/BOOTP Relay（DHCP/BOOTP リレー）	DHCP/BOOTP リレーのグローバル設定、DHCP/BOOTP サーバの登録を行います。	58 ページ
DHCP Local Relay Settings（DHCP ローカルリレー設定）	DHCP/BOOTP ローカルリレーの設定を有効にして、設定を行います。	60 ページ
DHCP Auto Configuration Settings（DHCP 自動設定）	DHCP 自動設定機能を有効 / 無効にします。	60 ページ
MAC Address Aging Time（MAC アドレスエージングタイム）	MAC アドレスエージングタイムを設定します。	61 ページ
Web Settings（Web 設定）	スイッチに Web ステータスを設定します。	61 ページ
Telnet Settings（Telnet 設定）	スイッチに Telnet 設定をします。	61 ページ
Password Encryption（パスワードの暗号化）	スイッチのパスワードの暗号化設定をします。	62 ページ
CLI Paging Settings（CLI ページング設定）	コマンドラインインタフェースの改頁処理を設定します。	62 ページ
Firmware Information（ファームウェア情報）	スイッチに格納されているファームウェアイメージの情報の確認、起動ステータスの設定の削除を行います。	63 ページ
Power Saving Settings（省電力設定）	スイッチに搭載した省電力機能を実行することができます。	64 ページ
Dual Configuration Settings（デュアル構成設定）	スイッチが次回の再起動時に使用する起動ファイルを設定します。	64 ページ
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。	66 ページ
Ping Test（Ping テスト）	指定アドレスに ICMP Echo パケットを送信します。	67 ページ
SNTP Settings（SNTP 設定）	本製品に時刻設定をします。	68 ページ
MAC Notification Settings（MAC 通知設定）	MAC 通知機能の設定を行います。	70 ページ
SNMP Settings（SNMP 設定）	SNMP 設定を行います。	72 ページ
Single IP Management（シングル IP マネジメント設定）	SIM 設定を行います。	80 ページ
SD Card FS Settings（SD カードファイルシステム設定）	SD フラッシュカードを使用してファームウェアイメージ、コンフィグレーションのバックアップまたはリストアを行います。	90 ページ

Device Information（デバイス情報）

本画面は、ログインを行うと自動的に表示される画面で、スイッチの主な設定情報を確認できます。本画面に戻るためには「DGS-3200-10、DGS-3200-16/GE、DGS-3200-24/GE」フォルダをクリックします。本画面には、スイッチの「MAC Address」（工場による設定のため変更不可）、「Boot PROM Version」と「Firmware Version」、「Hardware Version」などが表示されます。これらの情報は、PROM やファームウェアの更新状況の把握や他のネットワークデバイスのアドレステーブルにスイッチの MAC アドレスを登録する際の確認などに便利です。「System Name」、「System Location」、「System Contact」などを入力し、スイッチの定義を行う際にも利用します。さらに、スイッチの各機能の状態を表示し、現在のグローバルステータスにアクセス可能です。いくつかの機能は、各設定画面にリンクしており、本画面から接続できます。

図 6-1　Device Information 画面

画面には以下の項目があります。

項目	説明
Device Information	
Device Type	工場にて定義した機種名と型式を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。（半角英数字 160 文字以内）
System Contact	担当者名を表示します。（半角英数字 31 文字以内）
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。
System Up Time	最後のデバイスリセットからの経過時間を表示します。日、時、分、秒の形式で表示します。 例 : 41days 2 hours 22 mins 5 seconds
Dual Image	デュアルイメージ機能（複数のファームウェアコードを実行せずにスイッチ内に保存する）のサポート状況を表示します。
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。
VLAN Name	デバイスに割り当てられた VLAN 名を表示します。
Subnet 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。
Login Timeout (Minutes)	ユーザが何もしなかった場合にデバイスがタイムアウトするまでの時間を表示します。初期値は 10（分）です。
System Time	システムの日付を表示します。日 / 月 / 年で表示します。
Boot PROM version	デバイスのブートバージョンを表示します。
Device Status and Quick Configurations	
SNTP	SNTP 機能の状態（有効 / 無効）を表示します。SNTP 設定にリンクします。
Spanning Tree	STP 機能の状態（有効 / 無効）を表示します。STP 設定にリンクします。
RMON	RMON（リモートモニタリング）機能を有効 / 無効にします
Safeguard Engine	Safeguard エンジン機能の状態（有効 / 無効）の表示と、Safeguard エンジンの設定へのショートカットです。
Syslog	Syslog 機能をグローバルに有効 / 無効にします。初期値は無効です。

項目	説明
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	パスワードの暗号化機能を有効 / 無効にします。
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 ベースの管理機能を有効 / 無効にします。Web ベースの管理は初期値で有効になっています。無効に設定し、システムに適用すると、Web インタフェースによるシステム設定は行えなくなります。
VLAN Trunk	VLAN トランク機能を有効 / 無効にします。
Jumbo Frame	Jumbo Frame 機能の状態（有効 / 無効）の表示と、Jumbo Frame の設定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 通知機能の状態（有効 / 無効）を表示します。MAC 通知設定にリンクします。
802.1x	802.1X 機能の状態（有効 / 無効）の表示と、802.1X の設定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 Mirroring	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	SIM 機能の状態（有効 / 無効）を表示します。SIM 設定にリンクします。
CLI Paging	CLI ページング機能を有効 / 無効にします。
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。
DHCP Local Relay	DHCP ローカルリレー機能の状態（有効 / 無効）の表示と、DHCP ローカルリレー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 Setting をクリックし、選択したデバイスの機能の設定画面を表示します。「Apply」ボタンをクリックし、設定を適用します。

System Information（システム情報）

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

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

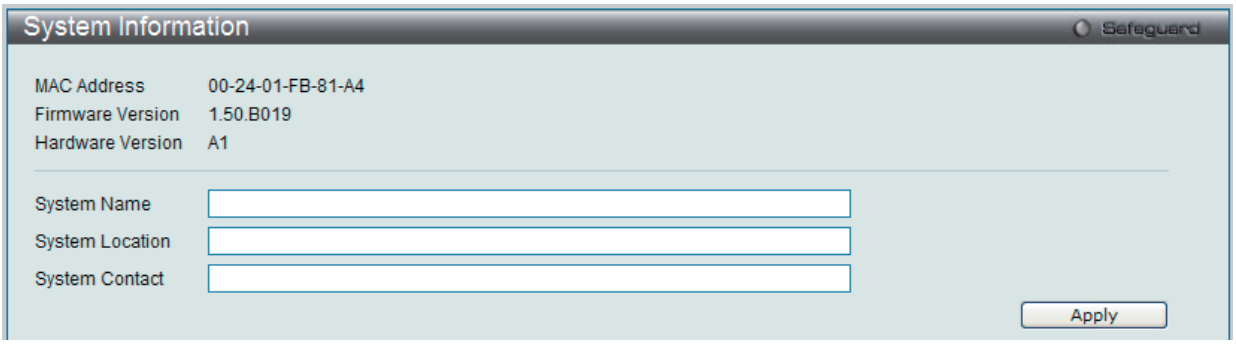


図 6-2　System Information 画面

画面には次の項目があります。

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

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

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、**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。

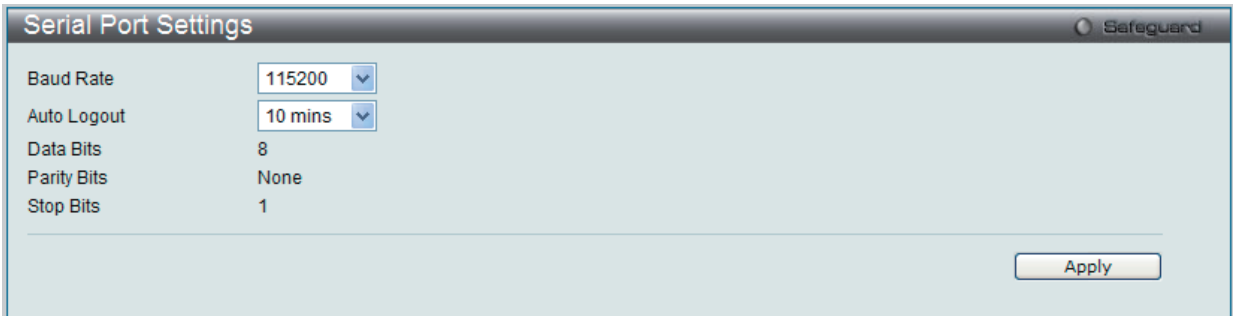


図 6-3　Serial Port Settings 画面

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 mins または Never（自動ログアウトを行わない）から選択できます。 初期値 :10 mins（分）。

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

IP Address（IP アドレス）

IP 設定を変更する場合は「Configuration」フォルダの「IP Address」メニューを使用します。

ネットワーク接続前に IP アドレスをコンソールより設定する必要があります。IP アドレスを設定または変更していない場合は、「DGS-3200 シリーズコマンドラインインタフェース（CLI）マニュアル」の「はじめに」、または本マニュアルの 33 ページの「端末をコンソールポートに接続する」を参照し、設定を行ってください。

IP アドレス設定

スイッチの IP アドレス設定を変更します。

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

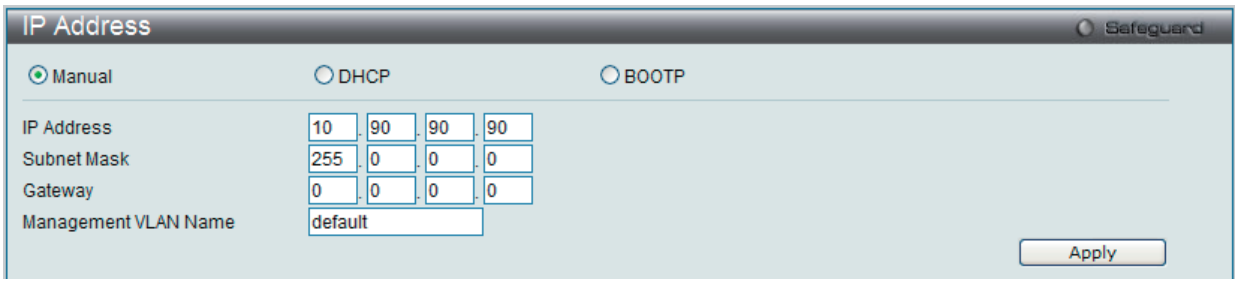


図 6-4　IP Address 画面

スイッチの現在の IP 設定が表示されます。

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

1. 画面先頭のメニューから「Manual」を選択します。
2. 適切な「IP Address」と「Subnet Mask」を入力します。
3. 異なるサブネットから本スイッチにアクセスする場合は、「Gateway」の IP アドレスを入力します。同じサブネットからスイッチを管理する場合は、この項目内は初期値（0.0.0.0）のままにします。
4. 本スイッチに VLAN 設定をしていない場合は、デフォルトの「Management VLAN Name」を使用できます。本スイッチは、購入時に VLAN「default」が設定されていて、すべてのポートが所属しています。既に VLAN 設定をしている場合は、本スイッチにアクセスする管理ステーションに接続しているポートが所属している VLAN の VLAN 名を入力します。画面に表示された VID と同じ VID を持つステーションからのアクセスを許可します。

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。

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
Manual	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、スイッチは初期設定や以前に登録された設定を使用する前に、DHCP サーバにアクセスし、これらの情報を取得します。
BOOTP	電源が投入されるとスイッチは BOOTP ブロードキャストリクエストを送信します。BOOTP プロトコルにより 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。
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。
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 144 ページの「Trusted Host（トラストホスト）」メニュー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。経由のインバンド「Security IP Management」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。

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

コンソールインタフェースを使用したスイッチの IP アドレス設定

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

IP アドレスは、Web マネージャを使用する前に設定してください。本スイッチの IP アドレスは、BOOTP または DHCP プロトコルを使用して自動的に設定することもできます。その場合は、スイッチに割り当てた本来のアドレスを知っておく必要があります。コンソールポートから Command Line Interface（CLI）を使用する設定方法は以下の通りです。

・コマンドラインプロンプトの後に、以下のコマンドを入力します。

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

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

・**`config ipif System ipaddress xxx.xxx.xxx.xxx/z`** とコマンド入力することも可能です。

（xxx.xxx.xxx.xxx: System という名前のインタフェースに割り当てる IP アドレス、z: CIDR 表記によるサブネットマスク数）

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

「Success.」というメッセージにより、コマンドの実行が成功したことを確認できます。スイッチのアドレス設定が終了すると、Telnet での CLI、または Web ベースによる管理を開始することができます。

IPv6 Interface Settings（IPv6 インタフェース設定）

スイッチの IPv6 インタフェース設定を行います。

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

Web マネージャにより、以下のようにスイッチの現在の IPv6 インタフェース設定が表示されます。

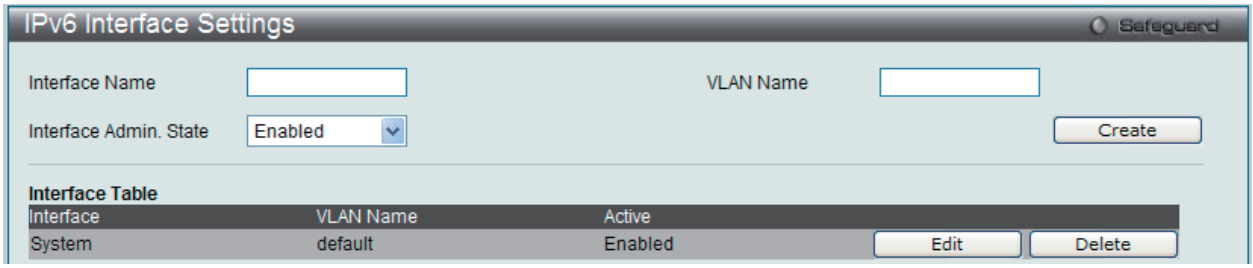


図 6-5　IPv6 Interface Settings 画面

IPv6 インタフェースの設定

1. 「Interface Name」および「VLAN Name」を入力し、「Interface Admin. State」を確認します。初期値ではステータスは「Enabled」（有効）です。
2. 「Create」ボタンをクリックすると、新しいエントリが上記画面下半分の「Interface Table」に表示されます。

エントリの変更

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。

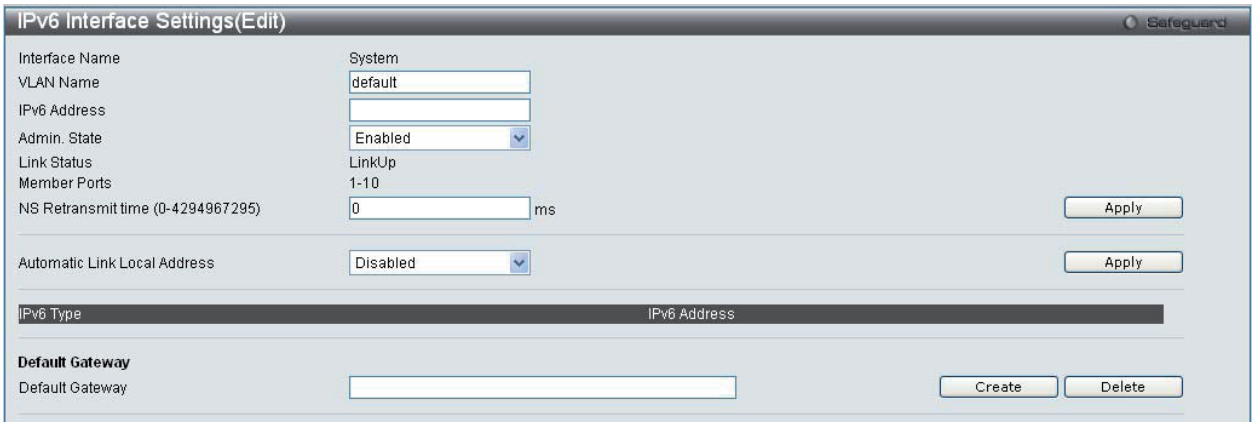


図 6-6　IPv6 Interface Settings（Edit）画面

IPv6 画面は 3 つセクションに分かれています。
以下の項目は画面の上部にあり、設定および参照できます。

項目	説明
Interface Name	IPv6 インタフェース名を入力します。
VLAN Name	IPv6 インタフェースの VLAN 名を入力します。
IPv6 Address	編集するインタフェースの IPv6 アドレスを入力します。
Admin. State	プルダウンメニューを使用して、ポート状態を「Enabled」（有効）または「Disabled」（無効）にします。
Link Status	IPv6 インタフェースが「Up」（アクティブ）または「Down」（ダウン）かを表示します。
Member Ports	IPv6 インタフェースのメンバであるポート番号を表示します。
NS Retransmit time (0-4294967295)	Neighbor ソリシテーションの再送タイマ (ミリ秒)。0-4294967295 の範囲で指定します。初期値は 0 です。

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

「Automatic Link Local」の設定をします。

項目	説明
Automatic Link Local Address	「Enabled」（有効）/「Disabled」（無効）にします。外部ソースのネットワークアドレス指定情報が無効の場合、有効にします。設定後、隣接する「Apply」ボタンをクリックします。

スイッチから IPv6 デフォルトゲートウェイアドレスの追加または削除をします。

項目	説明
Default Gateway	追加または削除するデフォルトゲートウェイの IPv6 アドレスを入力します。 • Create - クリックし、デフォルトゲートウェイを追加します。 • Delete - クリックし、デフォルトゲートウェイを削除します。

IPv6 Route Table（IPv6 ルートテーブル）

スイッチの IPv6 ルートテーブルのアドレスを設定します。

Configuration > 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。

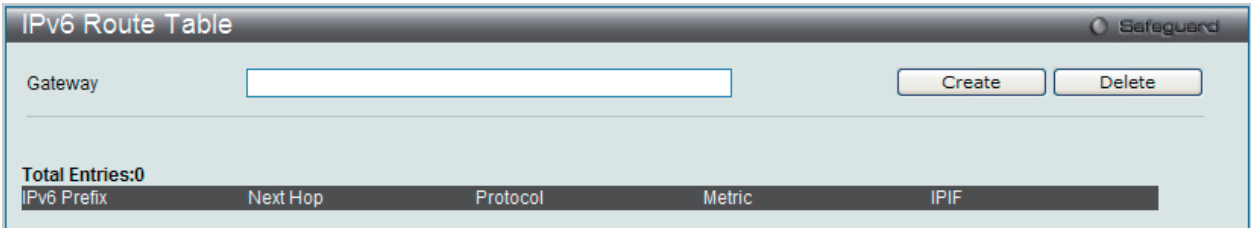


図 6-7　IPv6 Route Table 画面

「Gateway」を指定し、「Create」ボタンをクリックします。

IPv6 Neighbor Settings（IPv6 Neighbor 設定）

スイッチの IPv6 Neighbor 設定を行います。

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

図 6-8　IPv6 Neighbor Settings 画面

スイッチの現在の IPv6 Neighbor 設定が表示されます。

IPv6 Neighbor の新規登録

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

エントリの検索

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

エントリの削除

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

以下の項目が表示、または設定変更に使用できます。

項目	説明
Interface Name	IPv6 Neighbor 名を入力します。スイッチにおける現在の全インタフェースに対して検索するには、画面の中央部分にある 2 個目の「Interface Name」欄で「All」にチェックを入れ、「Find」ボタンをクリックします。
Neighbor IPv6 Address	Neighbor の IPv6 アドレスを入力します。
Link Layer MAC Address	Link Layer の MAC Address を入力します。
State	「All」、「Address」、「Static」または「Dynamic」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。

Port Configuration（ポート設定）

Port Configuration フォルダには「Port Settings」、「Port Description」、および「Port Error Disabled」の３つのメニューがあります。

Port Settings（スイッチのポート設定）

ここでは、ポート速度やフロー制御を含む、各物理ポートの属性やプロパティの設定情報を示します。

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

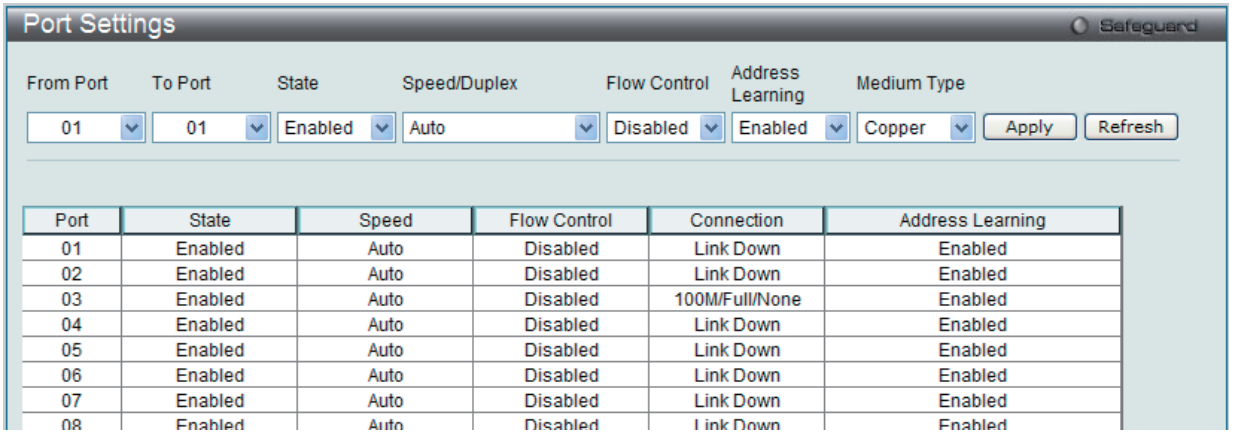


図 6-9　Port Settings 画面

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

項目	説明
State	指定したポートまたはポート範囲を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Speed/ Duplex	ポートの速度および全二重 / 半二重の指定を行います。「Auto」は、10/100Mbps のデバイス間（全二重または半二重モード時）のオートネゴシエーションを示します。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 オプションには「Auto」、「10M Half」、「10M Full」、「100M Half」、「100M Full」、「1000M Full_Master」、「1000M Full_Slave」、および「1000M Full」があります。Auto 以外のオプションのポート設定は固定となります。 次の２つのタイプ（1000M Full_Master、1000M Full_Slave）はギガビット接続設定ができます。ギガビット接続はフルデュプレックス接続だけをサポートしており、他の選択肢とは異なる特長を持っています。 1000M Full_Master（マスタ）および 1000M Full_Slave（スレーブ）項目は、ギガビット接続が可能なスイッチポートと他のデバイス間を 1000BASE-T で結ぶ接続を表示しています。マスタ設定（1000M Full_Master）によりポートはデュプレックス、速度および物理レイヤタイプに関連する情報を通知することができます。さらに２つの接続している物理レイヤ間のマスタおよびスレーブを決定します。この関係は２つの物理レイヤ間のタイミングコントロールを確立するために必要です。タイミングコントロールはローカルソースによってマスタ物理レイヤ上に設定されます。スレーブ設定（1000M Full_Slave）はループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わせます。一方の接続に 1000M Full_Master を設定するともう一方の接続は 1000M Full_Slave に設定する必要があります。それ以外の設定をすると両ポートともリンクダウンします。
Flow Control	各ポートのフローコントロール設定を選択します。Full-Duplex では 802.3x フローコントロールを、Half-Duplex ではバックプレッシャーによる制御を自動で行います。「Enabled」（フロー制御あり）または「Disabled」（フロー制御なし）を選択します。 初期値は「Disabled」（フロー制御なし）です。
Access Learning	選択ポートにおける MAC アドレスの学習の有無を設定します。 • Enabled - 終点と始点 MAC アドレスをフォワーディングテーブルに自動的にリストアップします。 • Disabled - MAC アドレスはフォワーディングテーブルに手動で登録します。セキュリティや効率上の理由で使用されることがあります。フォワーディングテーブルに MAC アドレスを登録する方法については、134 ページの「Forwarding & Filtering（フォワーディングとフィルタリングの設定）」を参照してください。初期値は「Enabled」です。
Medium Type	本設定はコンボポートだけに適用します。コンボポートを設定する場合、使用する変換メディアのタイプを選択します。SFP ポートの場合は「Fiber」、1000BASE-T の場合は「Copper」を設定します。

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

Port Description（ポート名）

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

ポートに名前を割り当てるためには **Configuration > Port Configuration > Port Description** の順にメニューをクリックし、以下の画面を表示します。

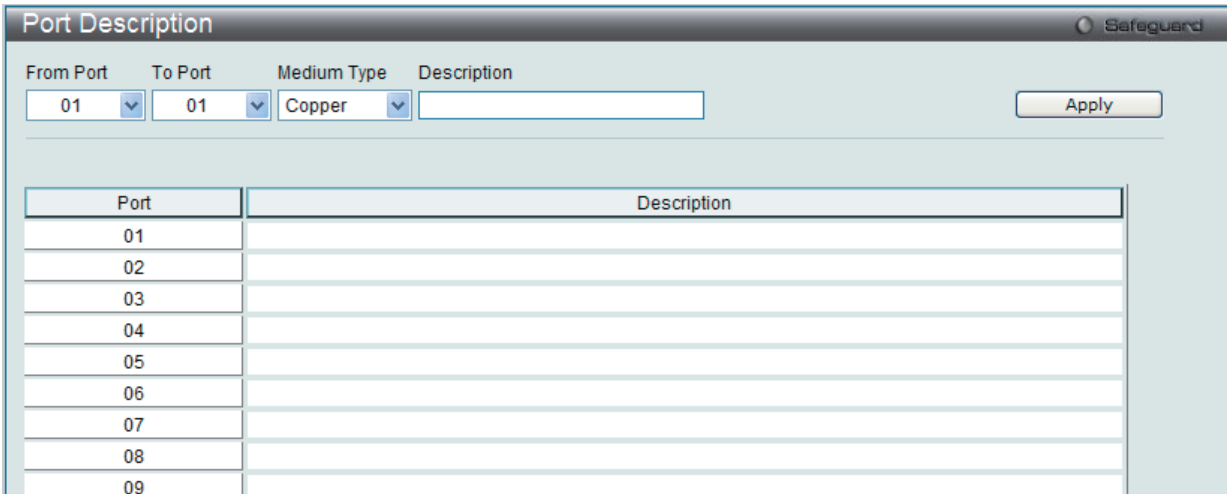


図 6-10　Port Description 画面

ポート、またはポート範囲を「From」と「To」プルダウンメニューから選択し、それらのポートについての名前や説明を入力します。
Medium Type はコンボポートにだけ適用されます。コンボポートを設定する場合、ここでは使用する転送メディアのタイプを定義します。SFP ポートの場合は「Fiber」を指定し、1000BASE-T ポートの場合は「Copper」を指定します。設定結果は適応するスイッチポート番号欄に表示されます（Copper ポートは C、Fiber ポートは F）。

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

Port Error Disabled（エラーによるポートの無効）

以下の画面では、接続が無効であるポートに関する情報（ストームコントロールの理由や接続ステータス）を表示します。

この画面を参照するためには、**Configuration > Port Configuration > Port Error Disabled** の順にメニューをクリックし、以下の画面を表示します。

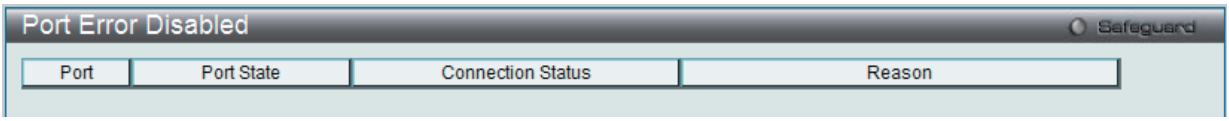


図 6-11　Port Error Disabled 画面

以下の項目が表示されます。

項目	説明
Port	エラーのために無効になっているポートを表示します。
Port State	現在のポートのステータス（「Enabled」または「Disabled」）を表示します。
Connection Status	各ポートのアップリンク状況（「Enabled」または「Disabled」）を表示します。
Reason	ストームコントロールのためにポートが無効になった理由を表示します。

Static ARP Settings（スタティック ARP 設定）

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

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

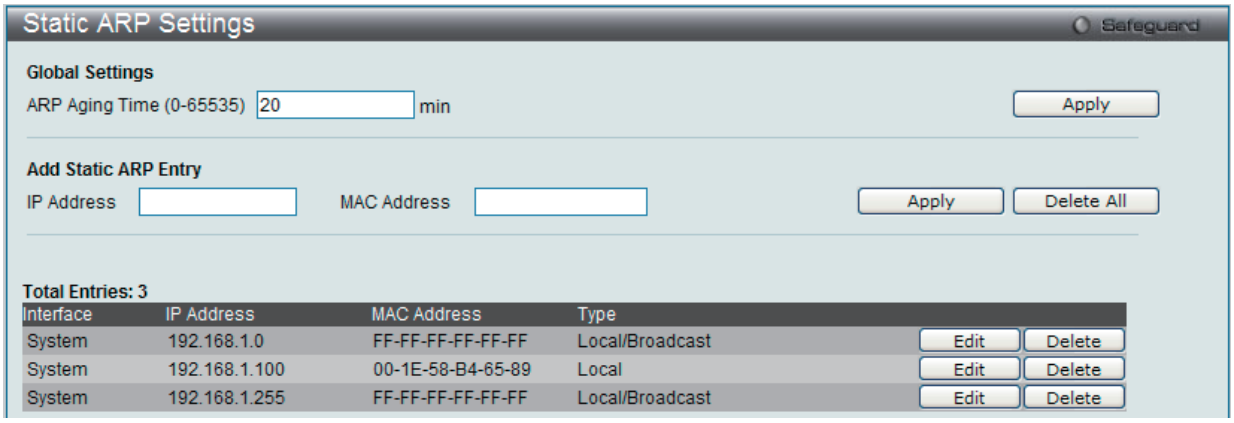


図 6-12　Static ARP Settings 画面

「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（秒）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。範囲は 0-65535（分）です。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。
スタティック ARP リスト	ユーザがスタティックに設定した IP アドレスと MAC アドレスの対応エントリを表示します。

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

Static ARP List のエントリの編集
1. 編集するエントリの「Edit」ボタンをクリックします。
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。

User Accounts（ユーザアカウントの設定）

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。以下の手順でユーザアカウント情報を設定します。

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

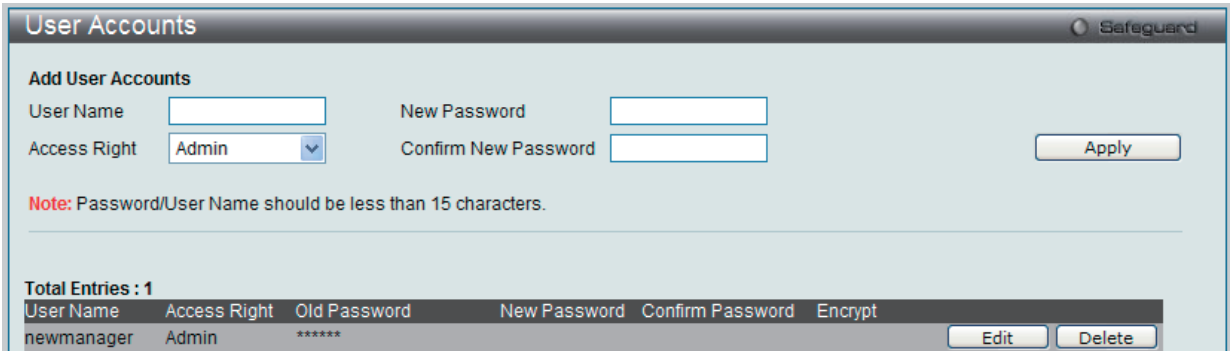


図 6-13　User Accounts 画面

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）
Access Right	アクセスレベルを設定します。 • Admin - ユーザに管理者としての権限を与えます。 • User - ユーザに参照のみの権限を与えます。
New 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 New Password	ユーザパスワードの確認入力をします。

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

User Accounts 画面の編集

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。

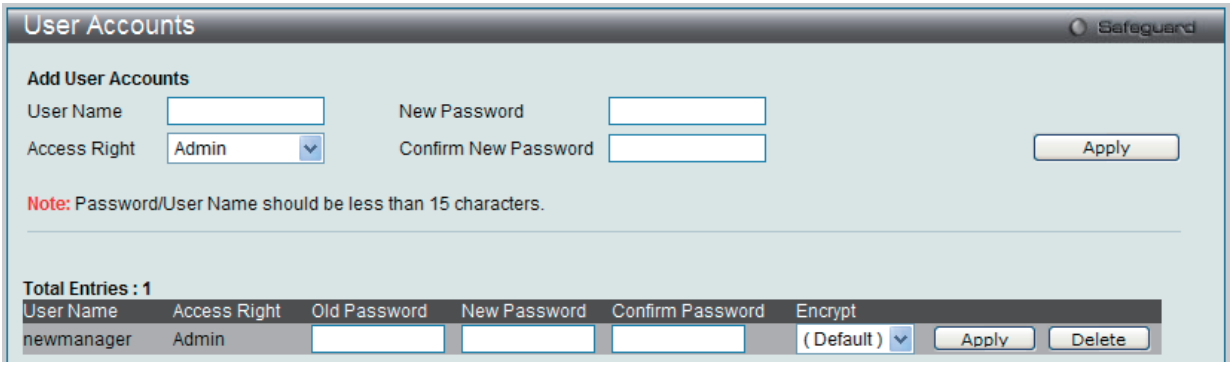


図 6-14　User Accounts 編集画面

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

注意 パスワードを忘れてしまった場合やパスワード不正の場合は、本マニュアル終わりにある 269 ページの「付録 F パスワードリカバリ手順」を参照してください。

User Accounts 画面のエントリの削除

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

Admin および User 権限
ユーザ権限には Admin と User の 2 つのレベルがあります。Admin 権限を持つユーザが利用可能なメニューのうちのいくつかは、User 権限では利用できません。

以下の表に、Admin レベルおよび User 権限の違いをまとめます。

表 6-1　Admin、User 権限

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

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）

「System Log Settings」画面では、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。

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。

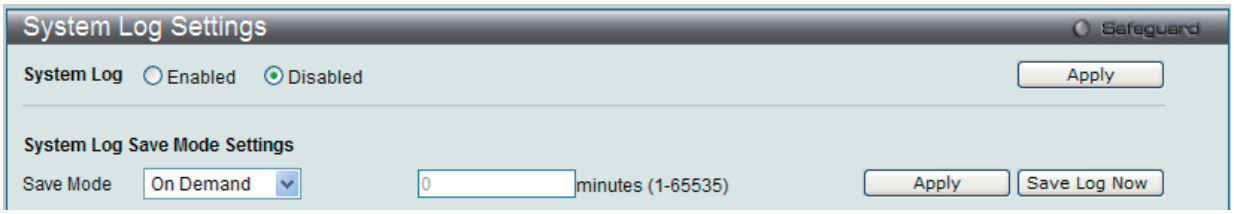


図 6-15　System Log Settings 画面

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 • Time Interval - 本項目横にある欄にログを保存する間隔（1-65535）（分）を設定します。 • On Demand - 手動でスイッチに、ログファイルを保存します。「Save」フォルダの「Save Log」リンクを使用するか、または本画面の「Save Log Now」ボタンをクリックして保存します。（初期値） • Log Trigger - スイッチにログイベントが発生すると、スイッチにログファイルを保存します。

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

System Log Host（システムログの管理）

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。

1. **Configuration > System Log Configuration > System Log Host** の順にクリックし、以下の「System Log Host」画面を表示します。
スイッチは、システムログサーバを使用して Syslog メッセージを最大 4 つまでのサーバに送信することができます。

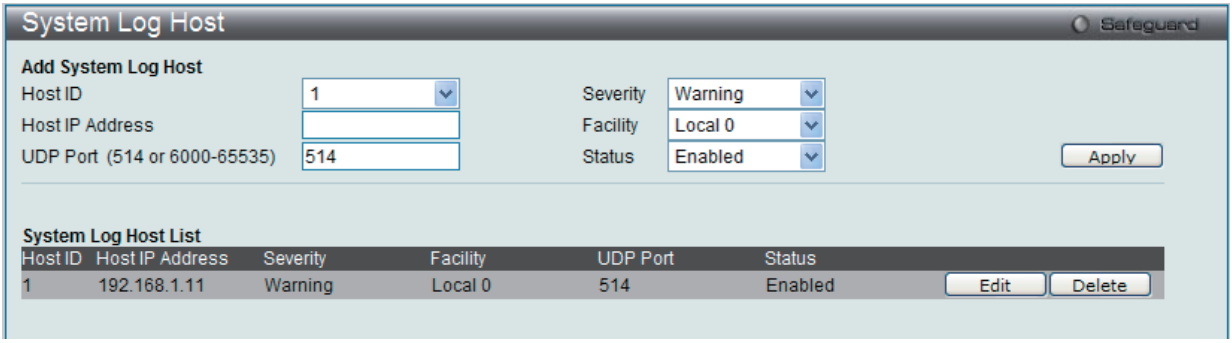


図 6-16　System Log Host 画面

本画面には次の項目があります。

項目	説明
Host ID	Syslog サーバ設定のインデックス（1-4）を設定します。
Host IP Address	ログを記録するサーバの IP アドレスを設定します。
UDP Port (514 or 6000-65535)	ログを送信するサーバの UDP ポートを設定します。514 または 6000-65535 が設定できます。初期値は 514 です。
Severity	サーバに送信する警告ログを選択するための重要度の識別名には 2 つのレベルがあります。重要度レベルが選択されると、それ以上重要なレベルもすべて自動的に選択されます。 • Warning - 最も低いレベルのデバイス警告。デバイスは機能しているが、動作上の問題が発生しています。 • Informational - デバイス情報の提供。 • All - すべてのレベルのシステムログの提供。
Facility	プルダウンメニューからリモートサーバに送信するシステムログのアプリケーションを設定します。「Local 0」、「Local 1」、「Local 2」、「Local 3」、「Local 4」、「Local 5」、「Local 6」または「Local 7」から選択します。
Status	「Enabled」（有効）または「Disabled」（無効）を選択します。

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

エントリの変更
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。

System Severity Settings（システムレベル設定）

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。「System Severity Settings」メニューを使用して、アラートの基準を設定します。

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

注意 画面中に表示されるログイベントの詳細情報については、本マニュアル中の 253 ページの「付録 C ログイベント」を参照してください。

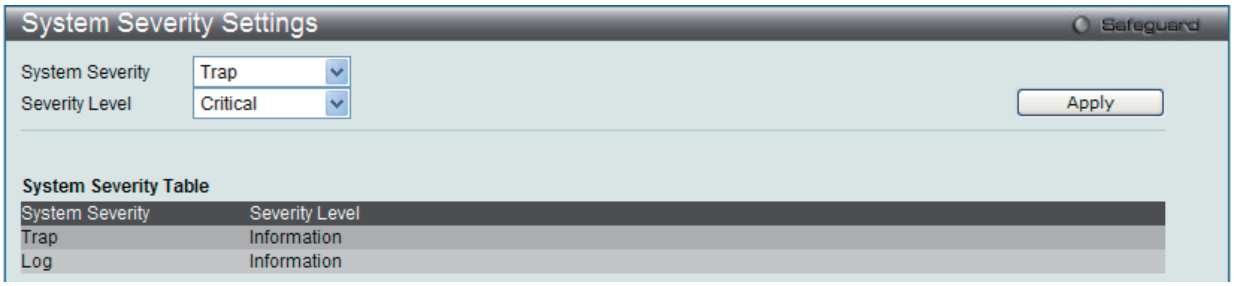


図 6-17　System Severity Settings 画面

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	ログエントリまたはトラップメッセージを送付するアラートレベルを選択します。 • Critical - 本スイッチのログまたは SNMP エージェントに Critical イベントだけを送付します。 • Warning - 本スイッチのログまたは SNMP エージェントに Warning イベントおよび Critical イベントを送付します。 • Information - 本スイッチのログまたは SNMP エージェントに Informational イベント、Warning イベントおよび Critical イベントを送付します。

「Apply」ボタンをクリックして、システムのログレベル設定を適用します。

DHCP/BOOTP Relay（DHCP/BOOTP リレー）

「DHCP/BOOTP Relay」フォルダには「DHCP/BOOTP Relay Global Settings」と「DHCP/BOOTP Relay Interface Settings」メニューがあります。

DHCP/BOOTP Relay Global Settings（DHCP/BOOTP リレーグローバル設定）

DHCP/BOOTP リレーグルーバル設定を行います。

DHCP/BOOTP メッセージが中継される最大のホップ（ルータの）数を Relay Hops Count Limit として、指定することができます。パケットのホップ数が、Relay Hops Count Limit より多くなれば、そのパケットは廃棄されます。値の範囲は 1-16 で、初期値は 4 です。Relay Time Threshold はスイッチが Boot Request パケットを送出する前に待つ最小の時間（秒）です。パケットの「Seconds」の値が Relay Time Threshold の値より小さければ、そのパケットは廃棄されます。値の範囲は 0-65536 で初期値は 0（秒）です。

Configuration > DHCP/BOOTP Relay > DHCP/BOOTP 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/BOOTP リレーのグローバル設定を有効にして、設定を行います。

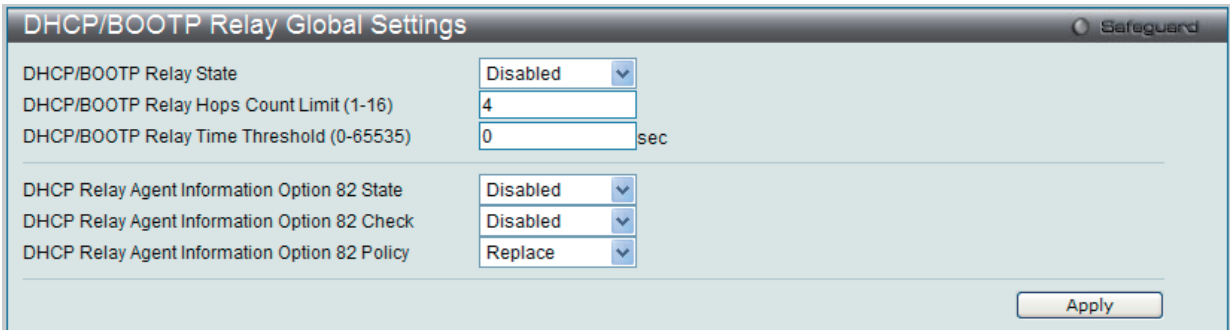


図 6-18　DHCP/BOOTP Relay Global Settings 画面

以下の項目が使用されます。

項目	説明
DHCP/BOOTP 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/BOOTP 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/BOOTP Relay Hops Count Limit (1-16)	DHCP/BOOTP 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/BOOTP Relay Time Threshold (0-65535)	DHCP/BOOTP 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 Agent Information Option 82 State	スイッチ上で DHCP Agent Information Option 82 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。 • Enabled - リレーエージェントは DHCP サーバとクライアント間で交わすメッセージに DHCP Relay Information（「Option 82」欄）を挿入 / 削除します。リレーエージェントが DHCP リクエストを受信すると、Option 82 情報と（設定があれば）リレーエージェントの IP アドレスをパケットに付加します。Option 82 情報が付加されたパケットは DHCP サーバに送信されます。Option 82 をサポートする DHCP サーバがパケットを受信すると、そのサーバは remote ID、circuit ID、またはそれらの両方を使用して IP アドレスを割り当て、単一の remote ID または circuit ID に割り当て可能な IP アドレス制限などのポリシーを適用できます。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。

「Apply」ボタンをクリックして設定内容を有効にします。

注意　スイッチが、DHCP クライアントから「Option-82」項目を含むパケットを受信し、チェック機能が「Enabled」（有効）になっている場合、スイッチはこのようなパケットは不正だとして、パケットを破棄します。しかし、場合によってはクライアント側で Option-82 情報が設定されることもあります。そのような状況では、チェック機能を無効にしてスイッチがパケットを破棄しないようにします。DHCP クライアントから受信したパケット内に既にリレー情報があった場合のスイッチの動作を「DHCP Agent Information Option 82 Policy」で指定します。

DHCP 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

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	モジュール	ポート
1 バイト	1 バイト	1 バイト	1 バイト	2 バイト	1 バイト	1 バイト

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

1.	2.	3.	4.	5.
2	8	0	6	MAC アドレス
1 バイト	1 バイト	1 バイト	1 バイト	6 バイト

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

図 6-19　Circuit ID と Remote ID のサブオプションフォーマット

DHCP/BOOTP Relay Interface Settings（DHCP/BOOTP リレーインタフェース設定）

「DHCP/BOOTP Relay Interface Settings」メニューでは、DHCP/BOOTP 情報をスイッチに中継するために、DHCP/BOOTP サーバの登録を行います。以下の画面を使用して、DHCP/BOOTP 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/BOOTP Relay Interface Table」にリスト表示されます。スイッチの 1 つの IP インタフェースに対して 4 件までのサーバ IP アドレスを登録できます。エントリの削除は「Delete」ボタンをクリックして行います。

Configuration > DHCP/BOOTP Relay > DHCP/BOOTP 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。

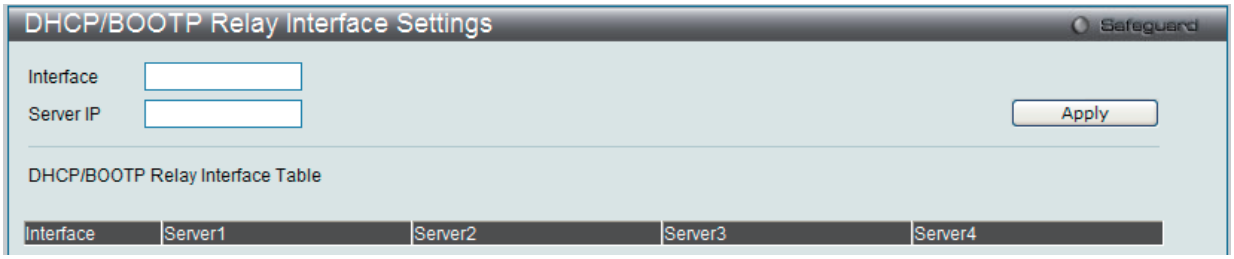


図 6-20　DHCP/BOOTP Relay Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface	DHCP/BOOTP サーバに直接接続するスイッチの IP インタフェース
Server IP	DHCP/BOOTP サーバの IP アドレス。1 つの IP インタフェースに対して 4 件までの入力が可能です。

「Apply」ボタンをクリックして設定内容を有効にします。

DHCP Local Relay Settings（DHCP ローカルリレー設定）

DHCP/BOOTP 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。

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

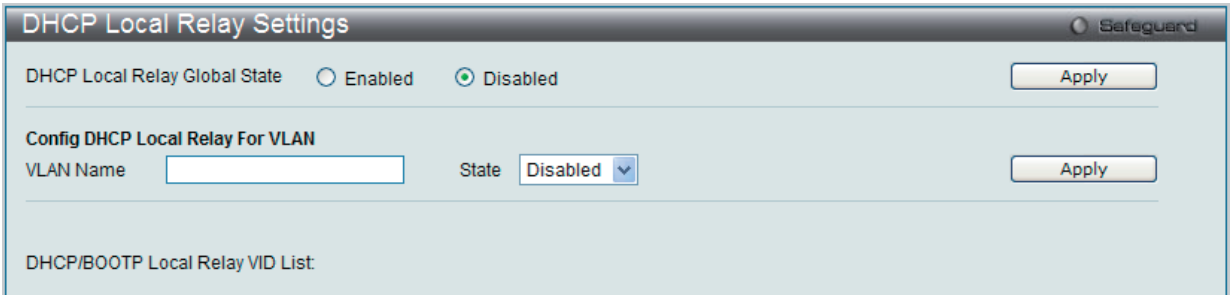


図 6-21　DHCP Local Relay Settings 画面

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 Global State	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。
VID List	VLAN ステートに使用する DHCP ローカルリレーの設定を「Enable」(有効) または「Disable」(無効) にします。
State	DHCP/BOOTP ローカルリレー設定を「Enable」（有効）または「Disable」（無効）にします。
DHCP/BOOTP Local Relay VID List	ユーザが DHCP/BOOTP ローカルリレーに適用する VLAN ID のリストです。

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。

DHCP Auto Configuration Settings（DHCP 自動設定）

本画面で本スイッチ上の 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。本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内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。本マニュアル 250 ページの「Upload Log File / Upload Log File to TFTP（ログファイルのアップロード）」の画面の説明を参照ください。
本スイッチが DHCP 自動設定を完了できない場合は、スイッチのメモリに保存済みの設定が使用されます。

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

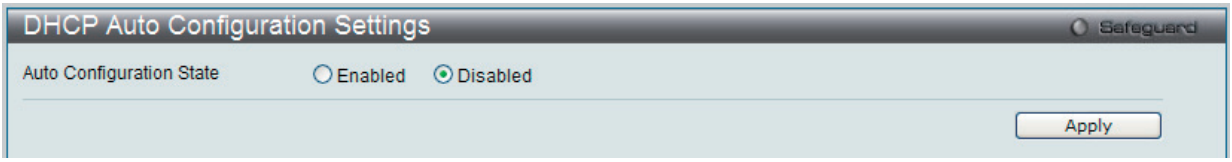


図 6-22　DHCP Auto Configuration Settings 画面

項目	説明
Auto Configuration State	スイッチの DHCP 自動設定機能を「Enabled」（有効）、また「Disabled」（無効）にします。

「Auto Configuration State」を有効にするためには、プルダウンメニューで「Enabled」を選択し、「Apply」ボタンをクリックします。

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

スイッチに MAC アドレスエージングタイムを設定します。

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

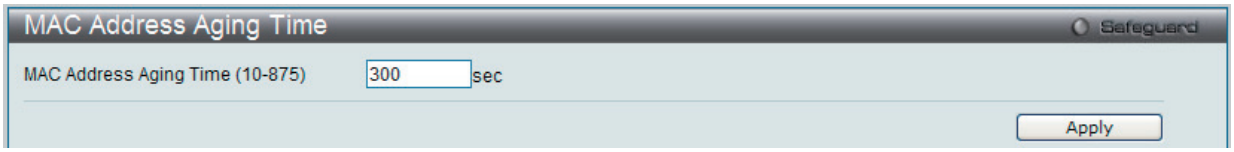


図 6-23　MAC Address Aging Time 画面

以下の項目を使用して設定、表示を行います。

項目	説明
MAC Address Aging Time (10-875)	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（10-875）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）。

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

Web Settings（Web 設定）

スイッチに Web ステータスを設定します。

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

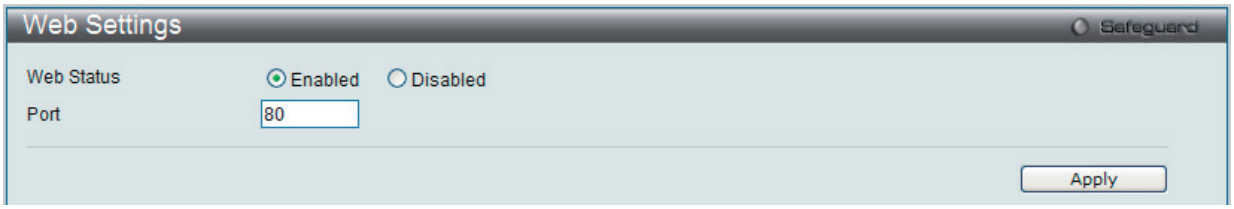


図 6-24　Web Settings 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」ボタンをクリックし、Web 設定を適用します。

Telnet Settings（Telnet 設定）

スイッチに Telnet 設定をします。

Configuration > 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。

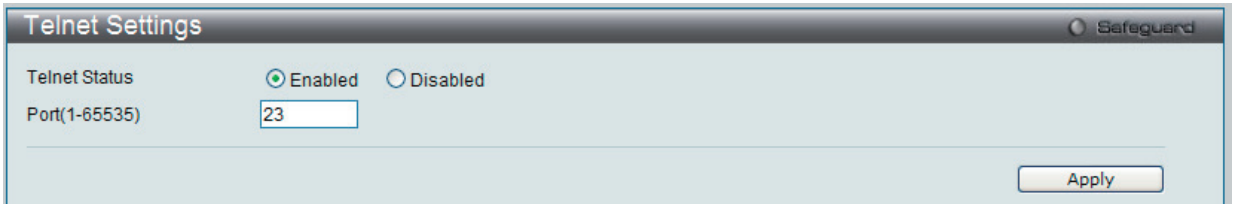


図 6-25　Telnet Settings 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」ボタンをクリックし、Telnet 設定を適用します。

Password Encryption（パスワードの暗号化）

スイッチのパスワードの暗号化設定をします。

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

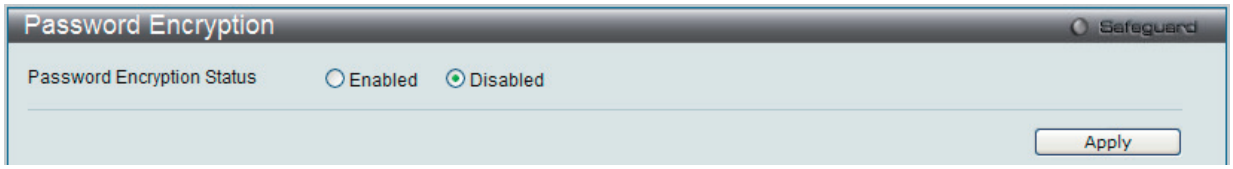


図 6-26　Password Encryption 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Password Encryption Status	パスワードの暗号化は初期値で「Disabled」（無効）です。「Enabled」を選択し、パスワードの暗号化を有効にします。

「Apply」ボタンをクリックし、パスワードの暗号化設定を適用します。

CLI Paging Settings（CLI ページング設定）

スイッチに CLI ページングを設定します。

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

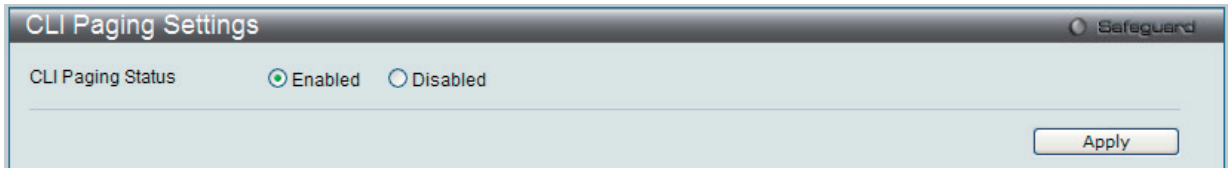


図 6-27　CLI Paging Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
CLI Paging Status	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。

「Apply」ボタンをクリックし、CLI ページング設定を適用します。

Firmware Information（ファームウェア情報）

以下に示す画面では、スイッチに格納されているファームウェアイメージの情報を確認、次回の起動ステータスの設定、および保存されている現在のファームウェアイメージの削除を行うことができます。

Configuration > Firmware Information の順にメニューを選択し、以下の画面を表示します。

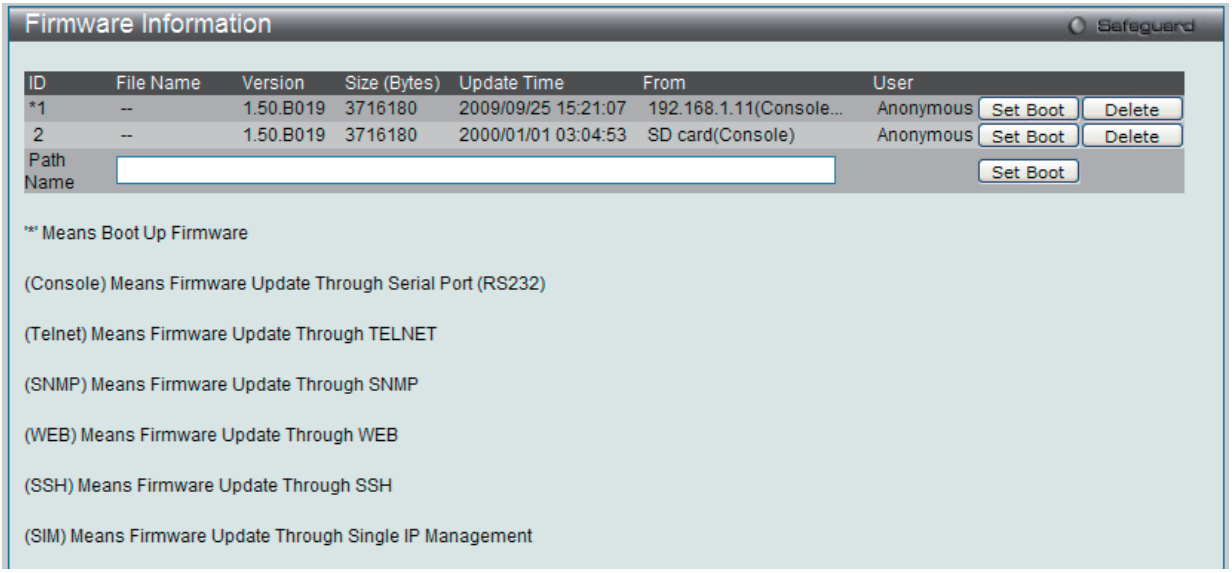


図 6-28　Firmware Information 画面

本画面には以下の情報が表示されます。

項目	説明
ID	スイッチのメモリにあるファームウェアのイメージ ID を示します。スイッチのメモリには 2 件のファームウェアイメージを格納できます。Image ID 1 が初期設定のブートアップファームウェアです。
Version	ファームウェアのバージョンを示します。
Size（Bytes）	ファームウェアのサイズ（バイト）を示します。
Update Time	ファームウェアがスイッチにダウンロードされた日時を示します。
From	ファームウェアのダウンロード元の IP アドレスを示します。スイッチへのダウンロード方法は以下の 6 種類のいずれかになります。起動ファイルには「*」が付加されています。 • Console - IP アドレスに R の文字が付加されている場合は、コンソールポート（RS-232）によってファームウェアの更新が行われたことを示します。 • Telnet - IP アドレスに T の文字が付加されている場合は、Telnet によってファームウェアの更新が行われたことを示します。 • SNMP - IP アドレスに S の文字が付加されている場合は、SNMP によってファームウェアの更新が行われたことを示します。 • WEB - IP アドレスに W の文字が付加されている場合は、Web ベースの管理インタフェースによってファームウェアの更新が行われたことを示します。 • SSH - IP アドレスに SSH の文字が付加されている場合は、Secure Shell（SSH）によってファームウェアの更新が行われたことを示します。 • SIM - IP アドレスに SIM の文字が付加されている場合は、シングル IP マネジメント機能によってファームウェアの更新が行われたことを示します。
User	ファームウェアのダウンロードを行ったユーザを表示します。ユーザが認識できない場合は、「Anonymous」または「Unknown」と表示されます。

「Set Boot」ボタンをクリックし、スイッチが次回の再起動時に使用する起動ファームウェアを設定します。
「Delete」ボタンをクリックし、本画面からファームウェアを削除します。

Power Saving Settings（省電力設定）

スイッチに搭載した省電力機能を実行することができます。省電力機能が有効の場合、リンクダウン状態のポートはスイッチの節電のためにオフになります。本機能はポートがリンクアップしている場合には、ポート性能に影響しません。「Length Detection State」が「Enabled」である場合、スイッチは自動的にケーブルの長さを測定して電力流を調整します。

Configuration > 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。

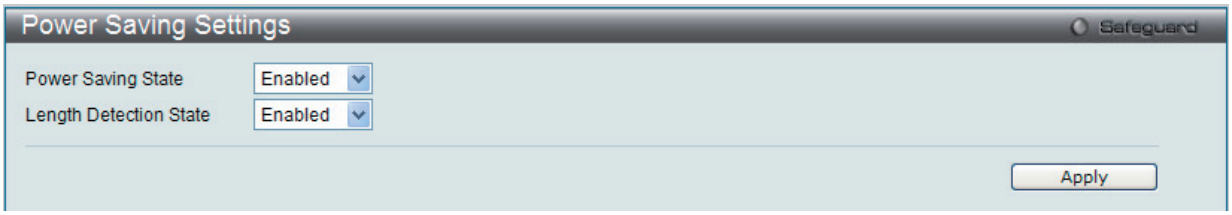


図 6-29　Power Saving Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Power Saving State	初期設定は「Enabled」(有効) です。省電力機能を無効にするためには、「Disabled」を指定します。
Length Detection State	省電力機能におけるケーブル長検出を有効または無効にします。本機能を無効にするためには、プルダウンメニューから「Disabled」を選択します。

「Apply」ボタンをクリックし、省電力機能設定を適用します。

Dual Configuration Settings（デュアル構成設定）

スイッチのデュアルコンフィグレーション設定の表示を行います。スイッチのメモリに 2 件のコンフィグレーションを保存し、いずれもスイッチの起動用のコンフィグレーションとして設定できます。また、DGS-3200-24/GE は、SD カードにコンフィグレーションを保存することができます。

「Boot」ボタンをクリックしてファイルを選択することで、スイッチに起動コンフィグレーションを指定することができます。これにより、次にスイッチが再起動される時にこの新たに選択したコンフィグレーションが使用されます。

隣接する「Delete」ボタンをクリックし、コンフィグレーションを削除します。

隣接する「Active」ボタンをクリックし、アクティブなコンフィグレーションとして設定します。

Configuration > Dual 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。

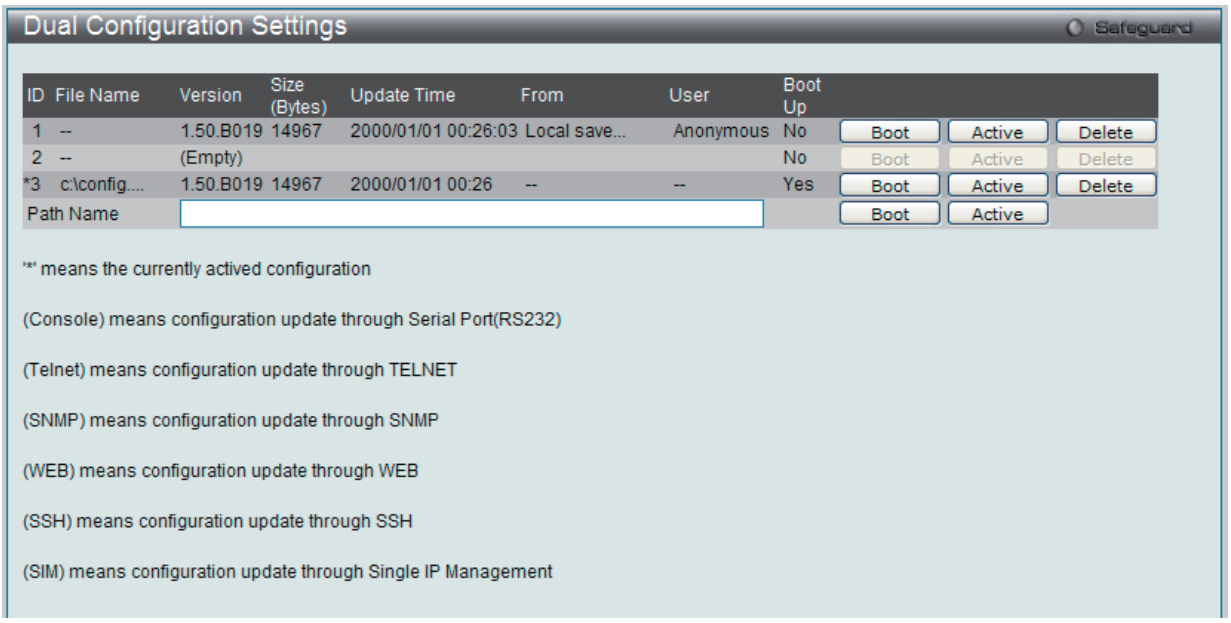


図 6-30　Dual Configuration Settings 画面（DGS-3200-10 、DGS-3200-16/GE）

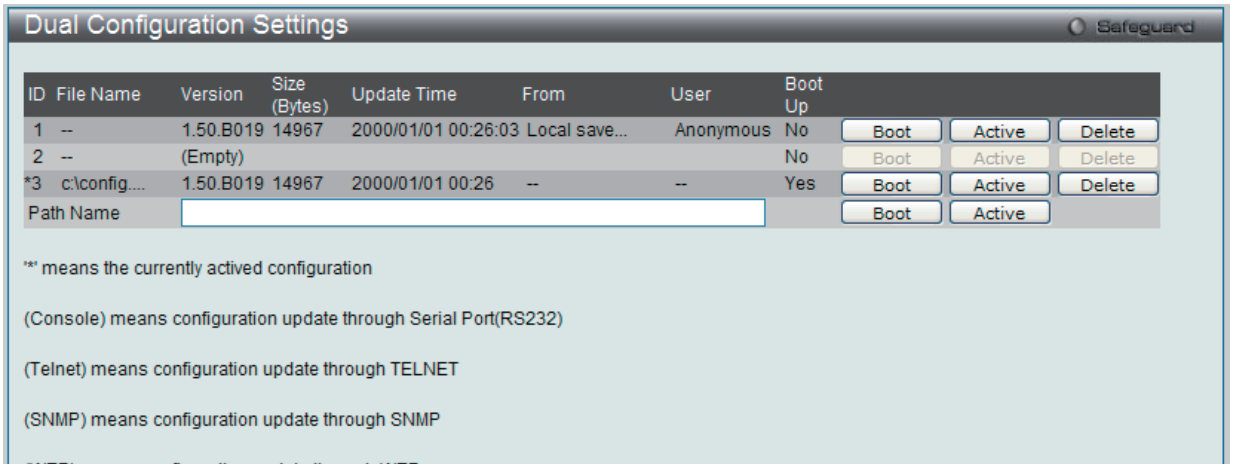


図 6-31　Dual Configuration Settings 画面（DGS-3200-24/GE）

本画面には以下の項目が表示されます。

項目	説明
ID	スイッチのメモリにあるコンフィグレーションファイルの ID を示します。スイッチのメモリ内には 2 つのコンフィグレーションファイルを格納できます。ID 1 が初期設定でブートアップコンフィグレーションファイルに設定されています。
File Name	ファイル名を表示します。
Version	コンフィグレーションファイルのバージョンを示します。
Size（Bytes）	コンフィグレーションファイルのサイズ（バイト）を示します。
Update Time	コンフィグレーションファイルがスイッチにダウンロードされた日時を示します。
From	コンフィグレーションファイルのダウンロード元を示します。スイッチへのダウンロード方法は以下の 6 種類のいずれかになります。起動ファイルには「*」が付加されています。 • Console - IP アドレスに Console の文字が付加されている場合は、コンソールポート（RS-232）によってファイルの更新が行われたことを示します。 • Telnet - IP アドレスに Telnet の文字が付加されている場合は、Telnet によってファイルの更新が行われたことを示します。 • SNMP - IP アドレスに SNMP の文字が付加されている場合は、SNMP によってファイルの更新が行われたことを示します。 • WEB - IP アドレスに WEB の文字が付加されている場合は、Web ベースの管理インタフェースによってファイルの更新が行われたことを示します。 • SSH - IP アドレスに SSH の文字が付加されている場合は、Secure Shell ネットワークプロトコルによってファイルの更新が行われたことを示します。 • SIM - IP アドレスに SIM の文字が付加されている場合は、シングル IP マネジメント機能によってファイルの更新が行われたことを示します。
User	本コンフィグレーションファイルのダウンロードを行ったユーザ（デバイス）を示します。認識できない場合は、「Anonymous」と表示されます。
Boot Up	スイッチを再起動するためにコンフィグレーションを使用するか否かを指定します。 • Yes- スイッチの起動コンフィグレーションとして使用されることを示しています。 • No- スイッチの起動コンフィグレーションとして使用されないことを示しています。
Path Name (DGS-3200-24/GE のみ)	SD カードに保存されたファームウェアからスイッチを起動するのに使用します。 • SD カードにおけるファームウェアのパス (「c:\DGS3200.had」など) を入力します。 • 隣接する「Set Boot」ボタンをクリックして、起動コンフィグレーションとして SD カードに保存されているコンフィグレーションを使用します。 • 隣接する「Active」ボタンをクリックして、アクティブなコンフィグレーションとして SD カードに保存されているコンフィグレーションを使用します。

起動コンフィグレーションの設定

1. 起動コンフィグレーションとして使用するコンフィグレーションに隣接する「Boot」ボタンをクリックします。
2. スイッチの起動に使用するコンフィグレーションの変更に成功すると「Success」メッセージが表示されます。
3. スイッチの起動に使用されるコンフィグレーションに隣接する「Boot Up」パラメータが「Yes」と表示されます。

アクティブコンフィグレーションの設定

1. アクティブなコンフィグレーションとして使用するコンフィグレーションに隣接する「Active」ボタンをクリックしします。
2. アクティブなコンフィグレーションとして使用するコンフィグレーションの変更に成功すると「Success」メッセージが表示されます。
3. 「*」はアクティブなコンフィグレーションとして使用されるコンフィグレーションの ID の隣に表示されます。

コンフィグレーションの削除

1. 削除するコンフィグレーションに隣接する「Delete」ボタンをクリックしします。
2. コンフィグレーションの削除に成功すると「Success」メッセージが表示されます。

SMTP Settings（SMTP 設定）

SMTP（Simple Mail Transfer Protocol）は、以下の画面に入力した E-mail アドレスに基づいてメール受信者にスイッチの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のメッセージを受信し、E-mail に適切な情報を記載し、スイッチに設定した受信者に送信するリモートデバイスです。これはスイッチ上に発生した問題イベントの記録を行い、小ワークグループまたは配線用クローゼットの管理を簡素化し、緊急なスイッチイベントの処理速度を向上させ、セキュリティを強化することができます。

以下の画面でスイッチに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。

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

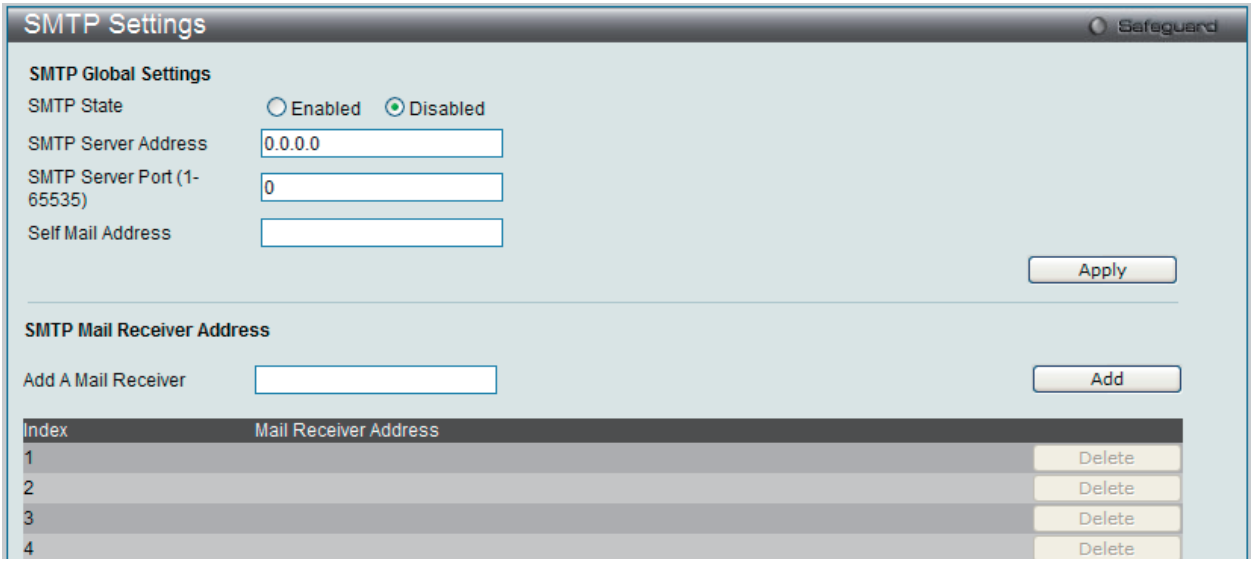


図 6-32　SMTP Settings 画面

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	ラジオボタンを使用してこのデバイスの SMTP サービスを「Enabled」（有効）または「Disabled」（無効）にします。
SMTP Server Address	リモートデバイスの 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。一般的なポート番号は 25 です。
Self Mail Address	メールメッセージを送信する E-mail アドレスを入力します。このアドレスは受信者に送信された E-mail メッセージにある"from"のアドレスとなります。本スイッチには Self Mail Address（半角英数字 64 文字以内）を 1 つだけ設定することができます。
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。

Ping Test（Ping テスト）

Ping とは、指定した IPv4 アドレスまたは IPv6 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。

Configuration > 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。

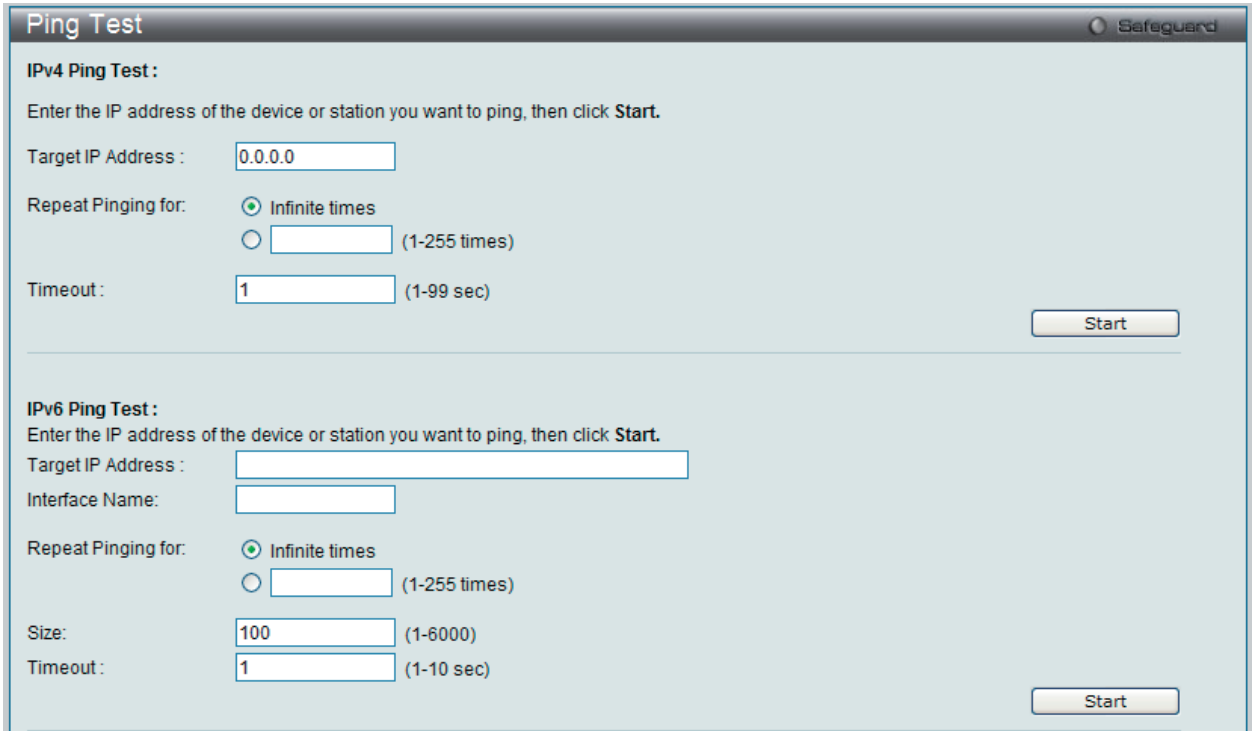


図 6-33　Ping Test 画面

「Repeat Pinging for」で「Infinite times」を選択すると、「Target IP Address」に指定した IP アドレス宛てに、ICMP Echo パケットをプログラムが停止するまで送信し続けます。または、「Repeat Pinging for」で 1-255 までの数字を指定して、送信回数を指定することもできます。

以下の項目を使用して設定、表示を行います。

項目	説明
Target IP Address	Ping する IP アドレスを入力します。
Interface Name	IPv6 の場合、Ping するインタフェース名を入力します。
Repeat Pinging for	送信先 IPv4 アドレスまたは IPv6 アドレスに Ping する回数（1-255）を指定します。 「Infinite times」を選択すると、ICMP Echo パケットをプログラムが停止するまで送信し続けます。
Size	IPv6 の場合、1-6000 の値を入力します。初期値は 100 です。
Timeout	IPv4 では、送信先への Ping メッセージの応答待ち時間 1-99（sec）で入力します。 IPv6 では、送信先への Ping メッセージの応答待ち時間 1-10（sec）で入力します。 いずれの場合もこの時間内に応答パケットの検出に失敗すると、Ping パケットを破棄します。

「Start」ボタンをクリックし、Ping プログラムを開始します。

SNTP Settings（SNTP 設定）

SNMP（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「Time Settings」と「Time Zone Settings」メニューがあります。

Time Settings（時刻設定）

スイッチに時刻を設定します。

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

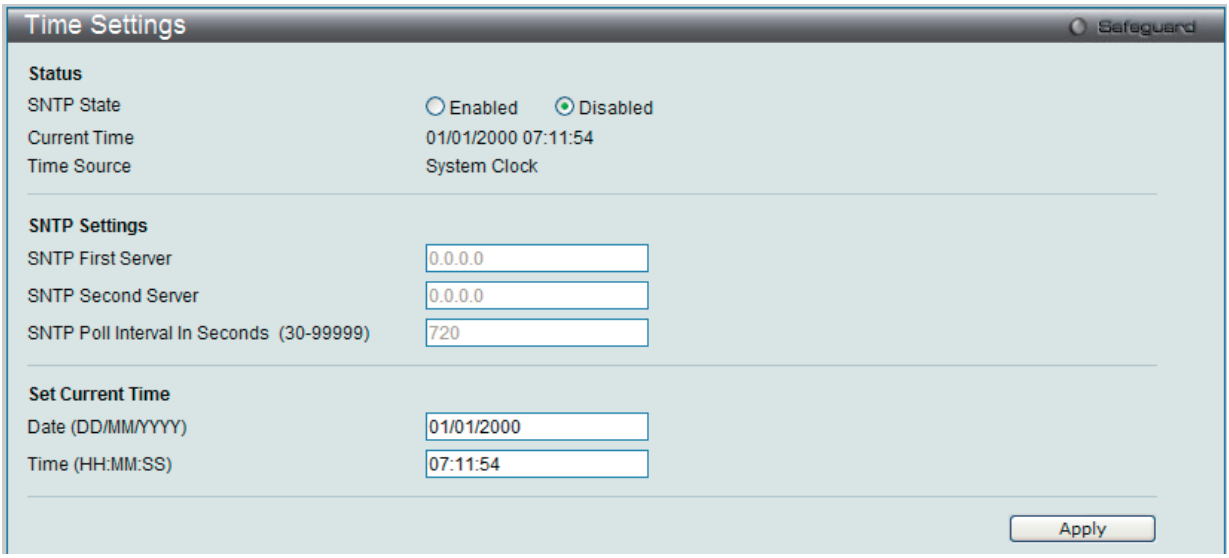


図 6-34　Time Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
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	
SNTP First Server	システム時刻を受け取るプライマリ SNTP サーバの IP アドレスを設定します。
SNTP Second Server	システム時刻を受け取るセカンダリ SNTP サーバの IP アドレスを設定します。
SNTP Poll Interval In Seconds (30-99999)	SNTP サーバにユニキャストによる問い合わせを行う間隔（30-99999 秒）を設定します。
Set Current Time	
Date（DD/MM/YY）	現在のシステム日付を設定します。項目のフォーマットは日 / 月 / 年です。
Time（HH:MM:SS）	現在のシステム時刻を時 : 分 : 秒（24 時間制）で設定します。例えば午後 9 時であれば 21:00:00 と指定します。

「Apply」ボタンをクリックし、デバイスに SNTP 設定を適用します。

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。

Configuration > SNTP Settings > TimeZone 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。

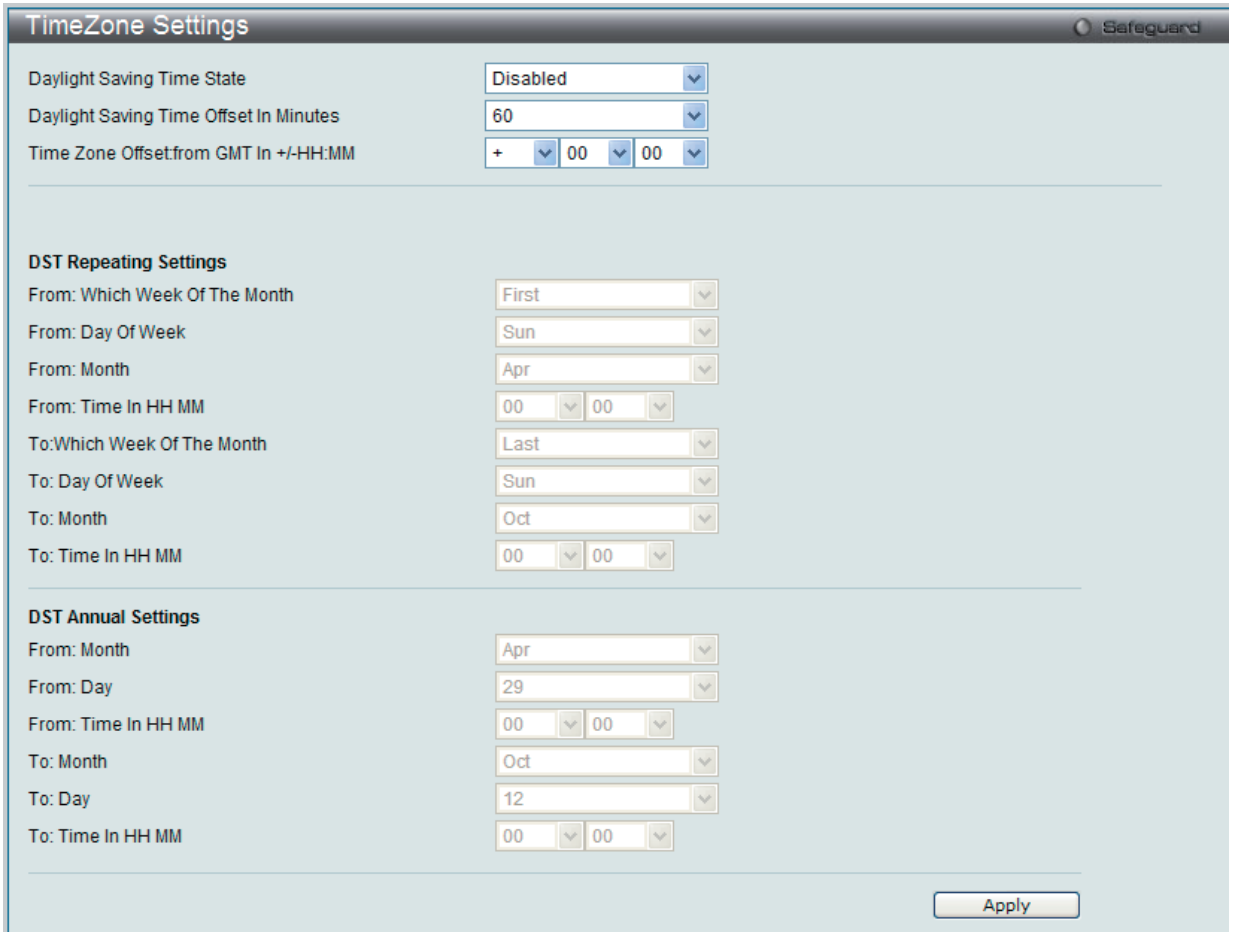


図 6-35　TimeZone Settings 画面

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。
To: Which Week Of The Month	月の第何週で DST が終わるかを設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。

項目	説明
To: Day Of Week	DST が終了する曜日を指定します。
To: Month	DST が終了する月を指定します。
To: Time In HH MM	DST が終了する時間を指定します。
DST Annual Settings	
Annual モードを使用すると、DST（サマータイム）設定を指定した詳細な期日で自動的に調整できるようになります。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。

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。
「MAC Notification Settings」フォルダには、「MAC Notification Global Settings」と「MAC Notification Port Settings」メニューがあります。

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

MAC Notification Global Settings（MAC 通知グローバル設定）

スイッチの MAC 通知機能をグローバル（全ポート）に設定します。

Configuration > MAC Notification Settings > MAC Notification 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。

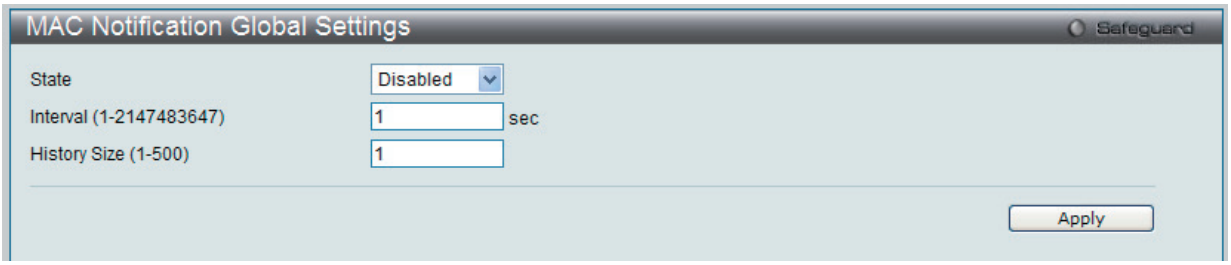


図 6-36　MAC Notification Global Settings 画面

以下の項目を使用して設定を行います。

項目	説明
State	スイッチ上の MAC 通知をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Interval (1-2147483647 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

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 Notification Port Settings（MAC 通知ポート設定）

ポートに MAC 通知設定を行います。

Configuration > MAC Notification Settings > MAC Notification 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。

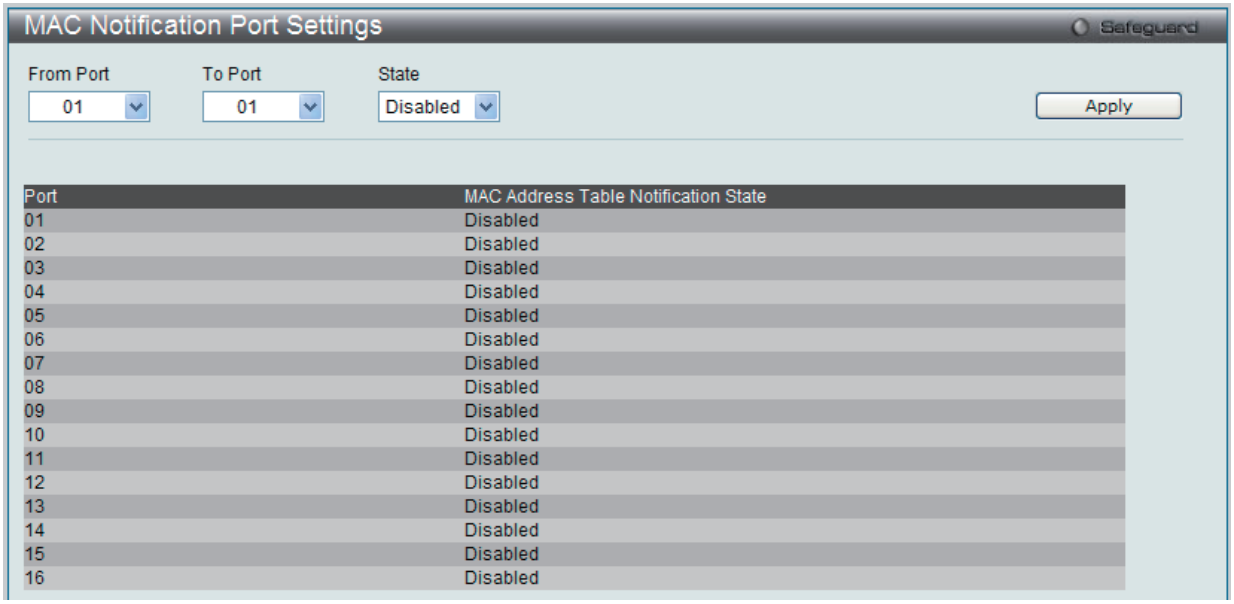


図 6-37　MAC Notification Port Settings 画面

以下の項目を使用し、MAC 通知設定をポートごと、またはポートグループごとに行います。

項目	説明
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。初期値は「Disabled」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。

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。

DGS-3200 シリーズは、SNMP バージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）をサポートしています。スイッチの監視と制御に使用する SNMP バージョンを選択することができます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

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

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

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

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

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

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

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

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

DGS-3200 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-3200 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。「Management Station IP Address」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 グローバルステート設定）

SNMP グローバルステート設定を「Enabled」（有効）または「Disabled」（無効）にします。

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

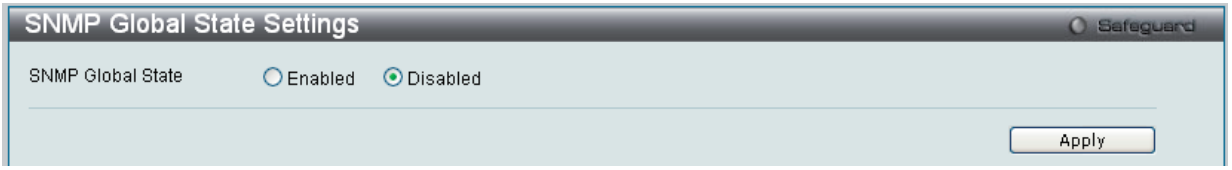


図 6-38　SNMP Global State Settings 画面

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

SNMP リンクチェンジトラップを設定します。

Configuration > SNMP Settings > SNMP Linkchange 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。

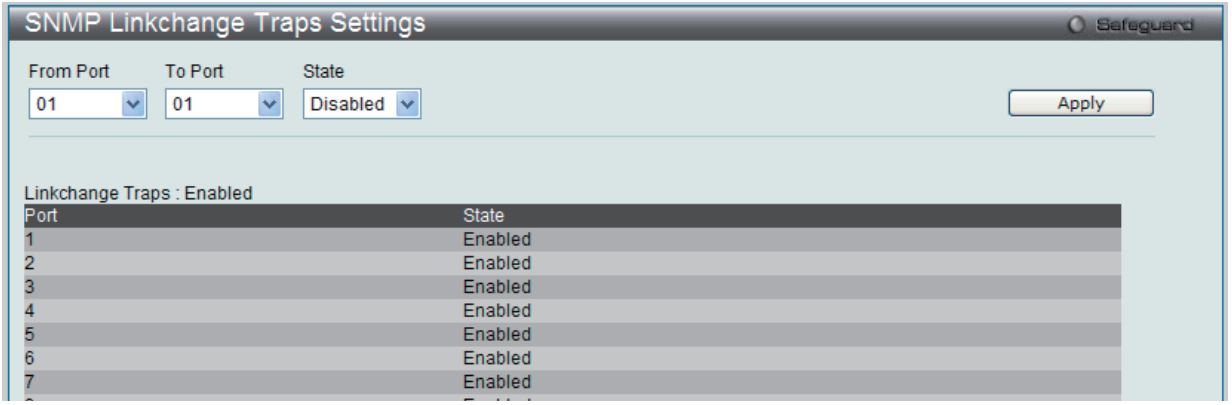


図 2-39　SNMP Linkchange Trap Settings 画面

スイッチに SNMP リンクチェンジトラップを設定するためには、「From Port」と「To Port」プルダウンメニューを使用してポート範囲を選択し、「State」を「Enabled」に変更します。

SNMP View Table（SNMP ビューテーブル）

「SNMP View Table」画面は、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。

Configuration > 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。

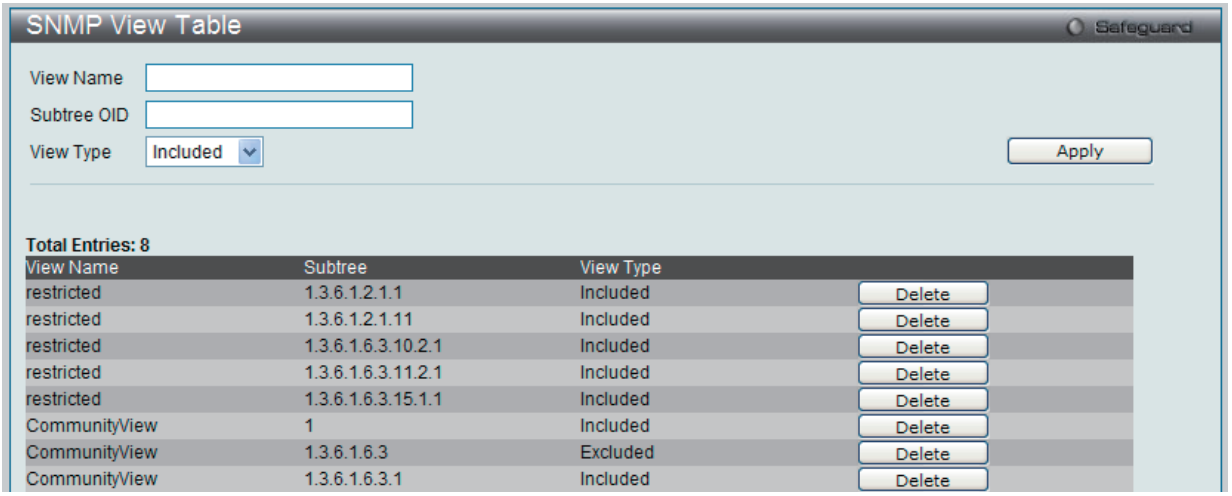


図 6-40　SNMP View Table 画面

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。

エントリの新規作成

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

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

以下の項目が使用されます。

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

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

SNMP Group Table（SNMP グループテーブル）

「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。

Configuration > 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。

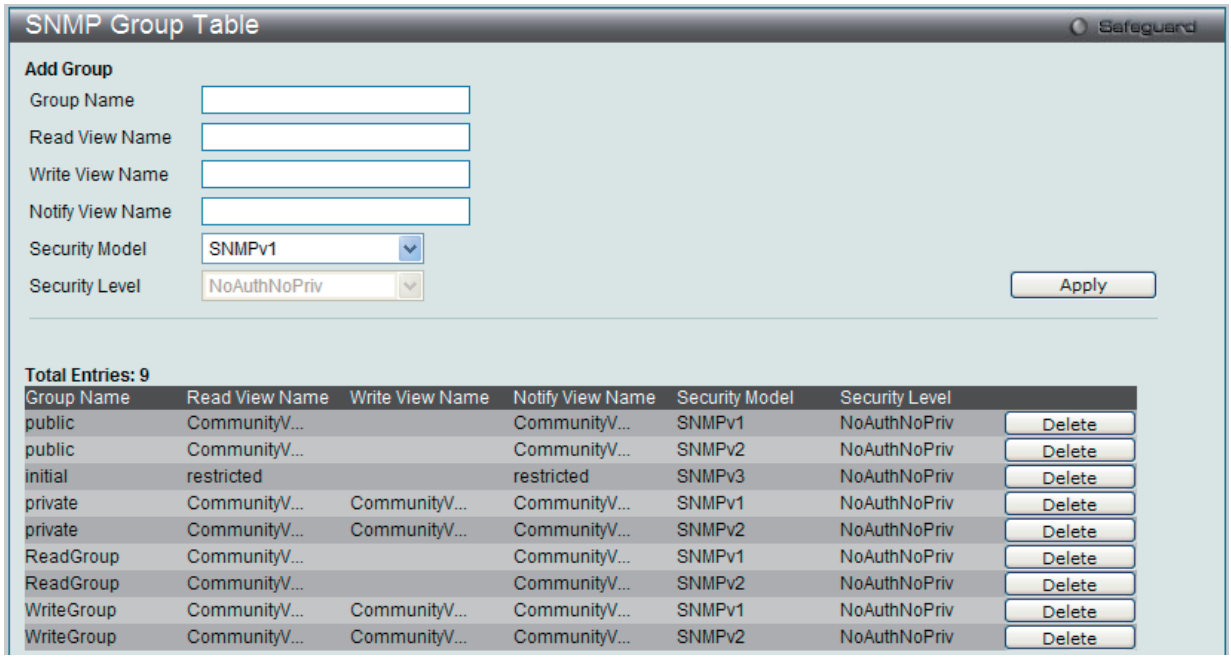


図 6-41　SNMP Group Table 画面

エントリの削除

削除するエントリの行の「Delete」ボタンをクリックします。

エントリの新規登録

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

以下の項目が使用されます。

項目	説明
Group Name	32 文字までの半角英数字を入力します。SNMP ユーザのグループの識別に使用します。
Read View Name	SNMP メッセージを要求する SNMP グループ名を入力します。
Write View Name	スイッチの SNMP エージェントに書き込み権限を与える SNMP グループ名を入力します。
Notify View Name	スイッチの SNMP エージェントによるトラップメッセージを送信する SNMP グループ名を入力します。
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 User Table（SNMP ユーザテーブル）

スイッチに現在設定されているすべての SNMP ユーザを表示します。

Configuration > 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。

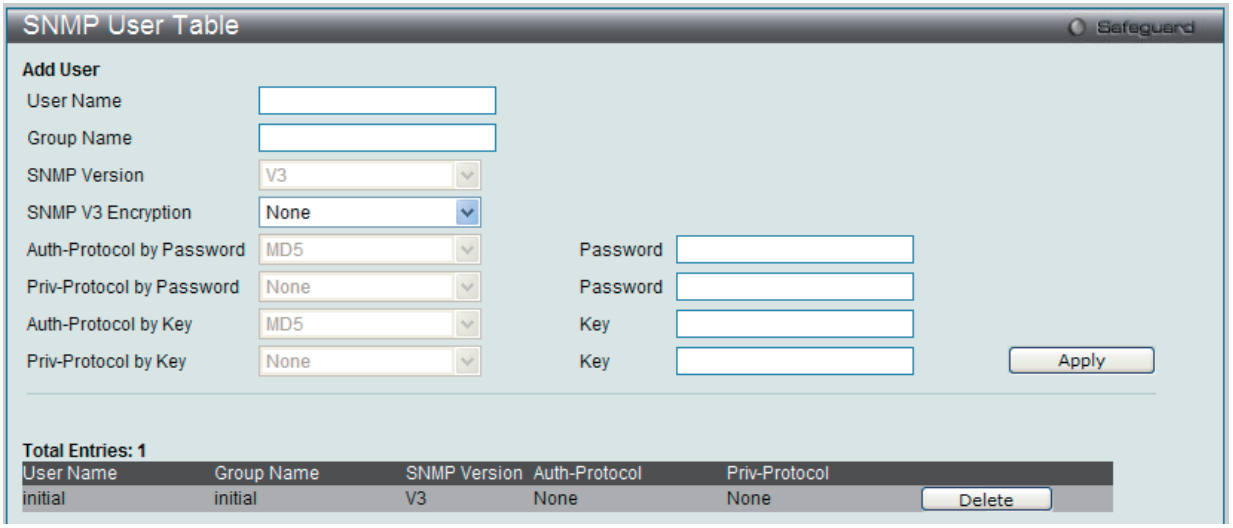


図 6-42　SNMP User Table 画面

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 by Password/Key	本項目は「SNMP Version」で「V3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。本項目を選択後、「Password」/「Key」にパスワードを入力します。 • MD5 - HMAC-MD5-96 認証レベルが使用されます。 • SHA - HMAC-SHA 認証プロトコルが使用されます。
Priv-Protocol by Password/Key	本項目は「SNMP Version」で「V3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 • None - 認証プロトコルは使用されていません。 • DES - CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されています。本項目を選択後、「Password」/「Key」にパスワード（半角英数字 8-16 文字）を入力します。

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

エントリの削除

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

SNMP Community Table（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、スイッチのエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。

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

エントリの設定

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

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

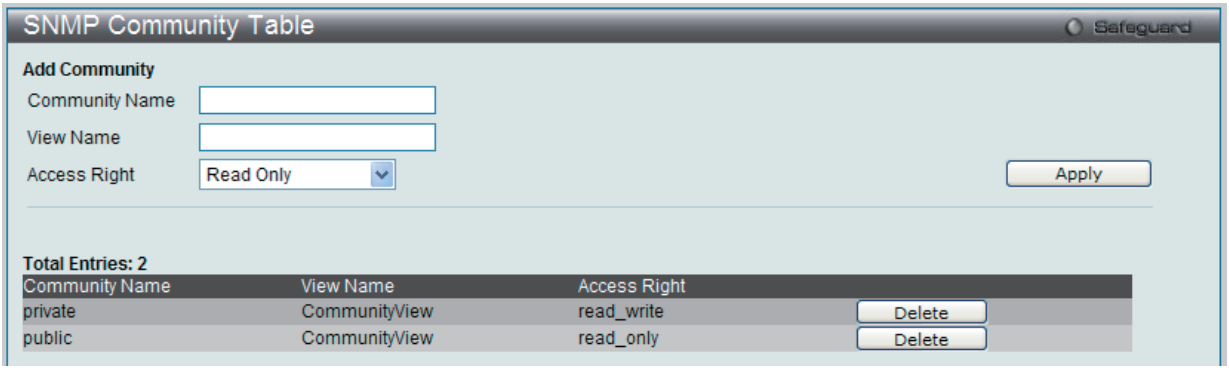


図 6-43　SNMP Community Table 画面

「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 の内容について読み出しのみ可能となります。 • Read Write - 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容について読み出し、および書き込みが可能です。

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

エントリの削除

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

SNMP Host Table（SNMP ホストテーブル）

IPv4 用の SNMP トラップの送信先を設定します。

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 6-44　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。
SNMP Version	• V1 : SNMP バージョン 1 が使用されます。 • V2c : SNMP バージョン 2c が使用されます。 • V3-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。 • V3-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。 • V3-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。

SNMP v6Host Table（SNMP IPv6 ホストテーブル）

IPv6 用の SNMP トラップの送信先を設定します。

Configuration > SNMP Settings > SNMP v6Host 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 6-45　SNMP v6Host Table 画面

エントリの新規登録

SNMP v6Host Table に新しいエントリを追加するには、画面の上部に情報を入力し、「Apply」ボタンをクリックします。

以下の項目を使用します。

項目	説明
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IP アドレスを入力します。
SNMP Version	• V1 : SNMP バージョン 1 が使用されます。 • V2c : SNMP バージョン 2c が使用されます。 • V3-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。 • V3-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。 • V3-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 v6Host Table」画面の定義済み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。

SNMP Engine ID（SNMP エンジン ID）

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。

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

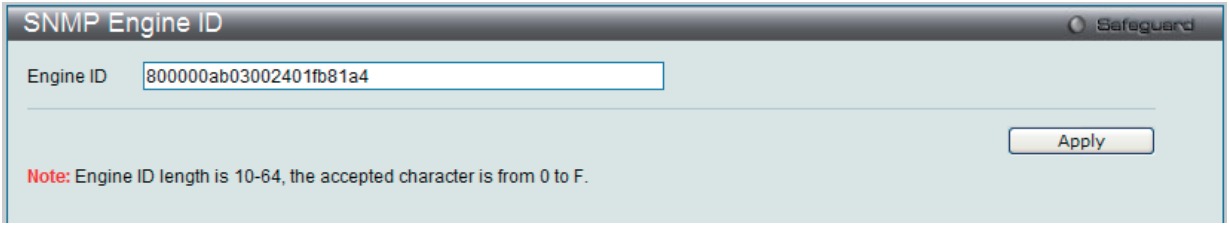


図 6-46　SNMP Engine ID 画面

以下の項目を使用します。

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

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

SNMP Trap Configuration（SNMP トラップ設定）

スイッチの SNMP トラップ、SNMP 認証エラーのトラップ、リンクチェンジトラップ、コールドスタートトラップおよびウォームスタートトラップを有効または無効にします。

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

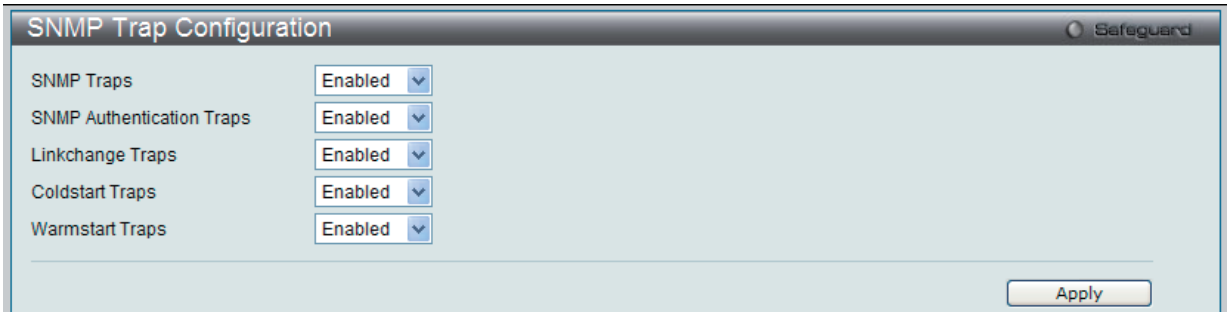


図 6-47　SNMP Trap Configuration 画面

それぞれのプルダウンメニューから「Enabled」（有効）、または「Disabled」（無効）にし、「Apply」ボタンをクリックします。

リンクチェンジトラップを指定ポートまたはポート範囲に有効にするためには、**Configuration > SNMP Settings > SNMP Linkchange Trap Settings** の順にメニューをクリックし、「SNMP Linkchange Trap Settings」画面で設定します。

RMON（RMON 設定）

ここでは、スイッチの SNMP 機能の RMON（remote monitoring）ステータスを有効または無効にします。さらに、「RMON Rising」と「Falling Alarm Traps」を「Enabled」(有効) または「Disabled」(無効) にすることができます。

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

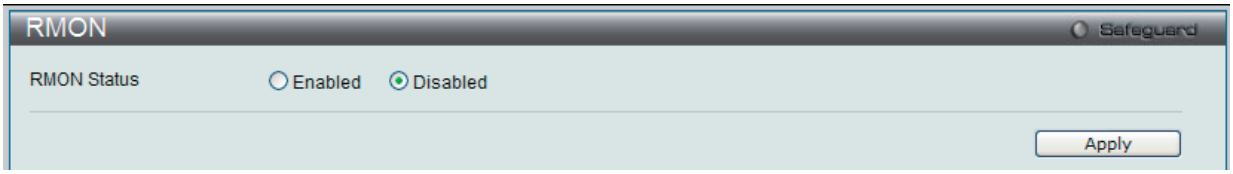


図 6-48　RMON 画面

SNMP に対する RMON を「Enabled」（有効）または「Disabled」（無効）にし、「Apply」ボタンをクリックします。

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

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

Configuration > 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。

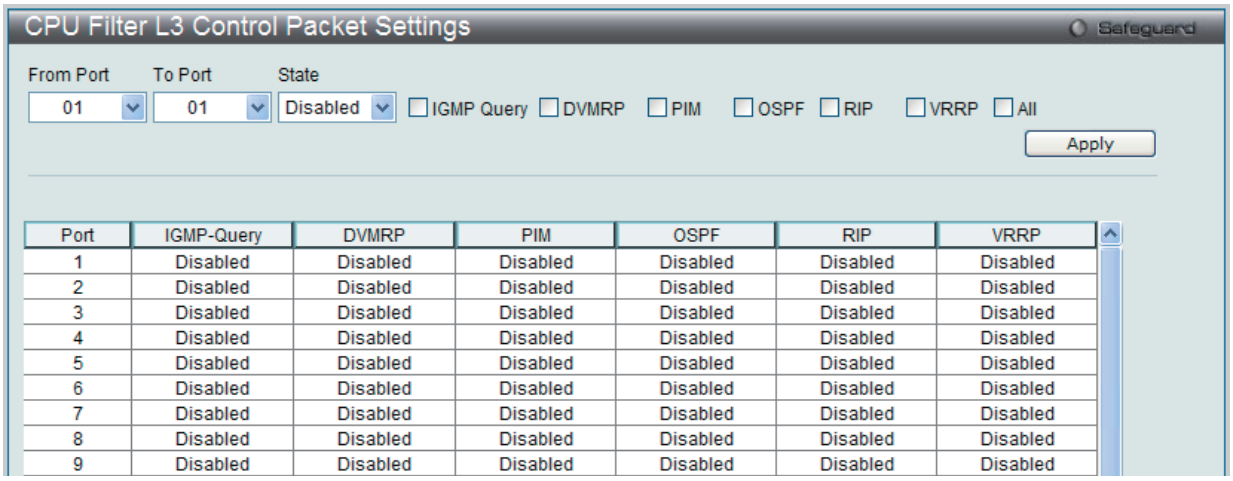


図 6-49　CPU Filter L3 Control Packet Settings 画面

スイッチに CPU L3 コントロールパケットのフィルタ設定を設定するためには、「From Port」と「To Port」プルダウンメニューを使用してポート範囲を選択し、「State」を「Enabled」に変更します。さらに希望するレイヤ 3 カテゴリ (IGMP Query、DVMRP、PIM、OSPF、RIP、VRRP または All) をチェックします。
「Apply」ボタンをクリックして終了します。

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

シングル IP マネジメント（SIM）の概要

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

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

D-Link シングル IP マネジメント（以下 SIM と呼びます）機能を搭載するスイッチには、以下の基本的なルールがあります。

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

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

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

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

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

上記の役割には、以下のルールを適用します。

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

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

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

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

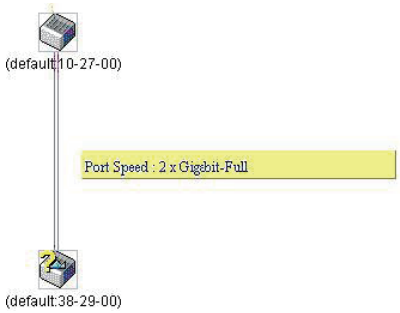
バージョン 1.61 へのアップグレード

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

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

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

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



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

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

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

Single IP Settings（シングル IP 設定）

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

1. Web インタフェースを使用してスイッチの SIM を有効にするためには **Configuration** > **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。
2. 以下の画面のようにトポロジマップにはポートトランキングのメンバで接続という新しい機能があります。このポートトランキンググループに設定した速度やイーサネット接続数を表示します。

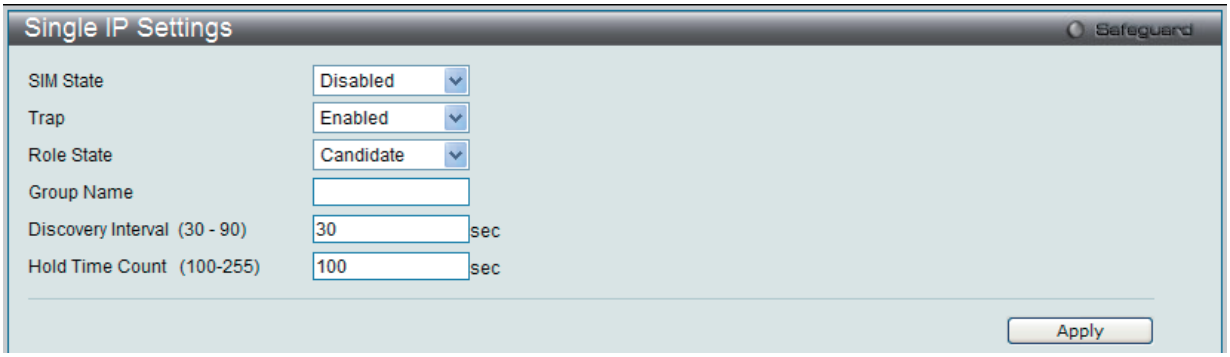


図 6-50　Single IP Settings 画面（CaS 無効状態）

「SIM State」のプルダウンメニューから「Enabled」を選択して、「Apply」ボタンをクリックします。画面が更新されます。

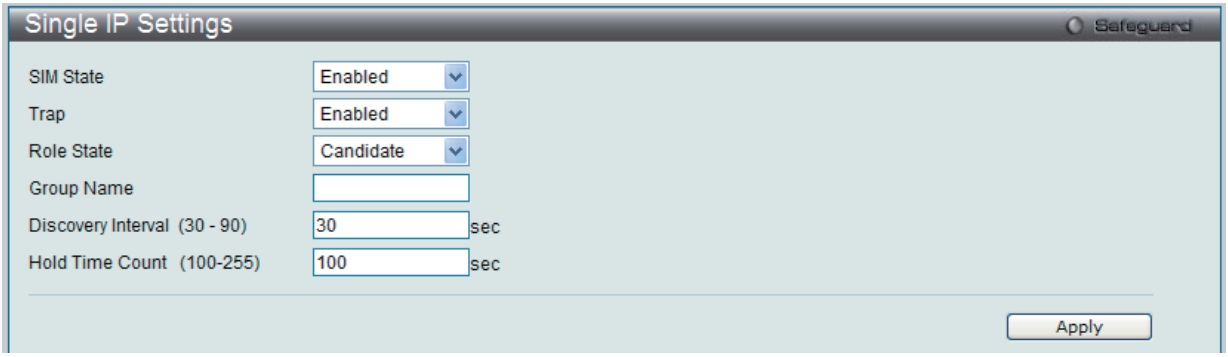


図 6-51　Single IP Settings 画面（CaS 有効状態）

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	プルダウンメニューを使用してトラップを「Enabled」(有効) または「Disabled」(無効) にします。メンバスイッチから発行されるトラップの送信を制御します。
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。
「Single IP Settings」画面は以下のように表示されます。

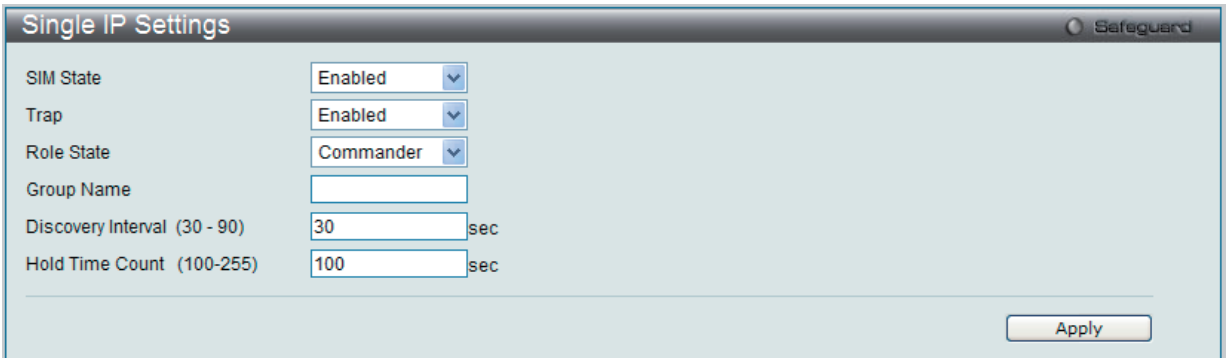


図 6-52　Single IP Settings 画面（CS 有効状態）

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。

Configuration > **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。

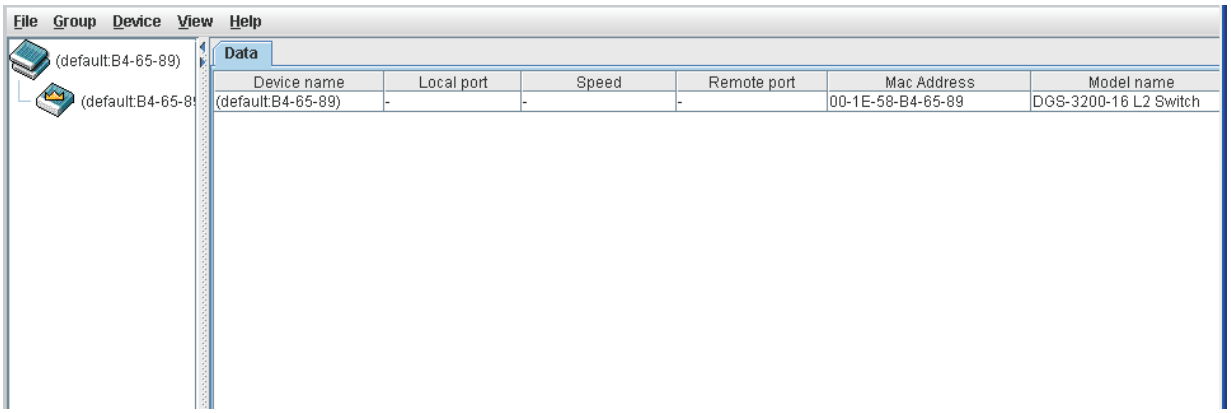


図 6-53　トポロジ画面

トポロジ画面の「Data」タブには以下の情報が表示されます。

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

トポロジマップの表示

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

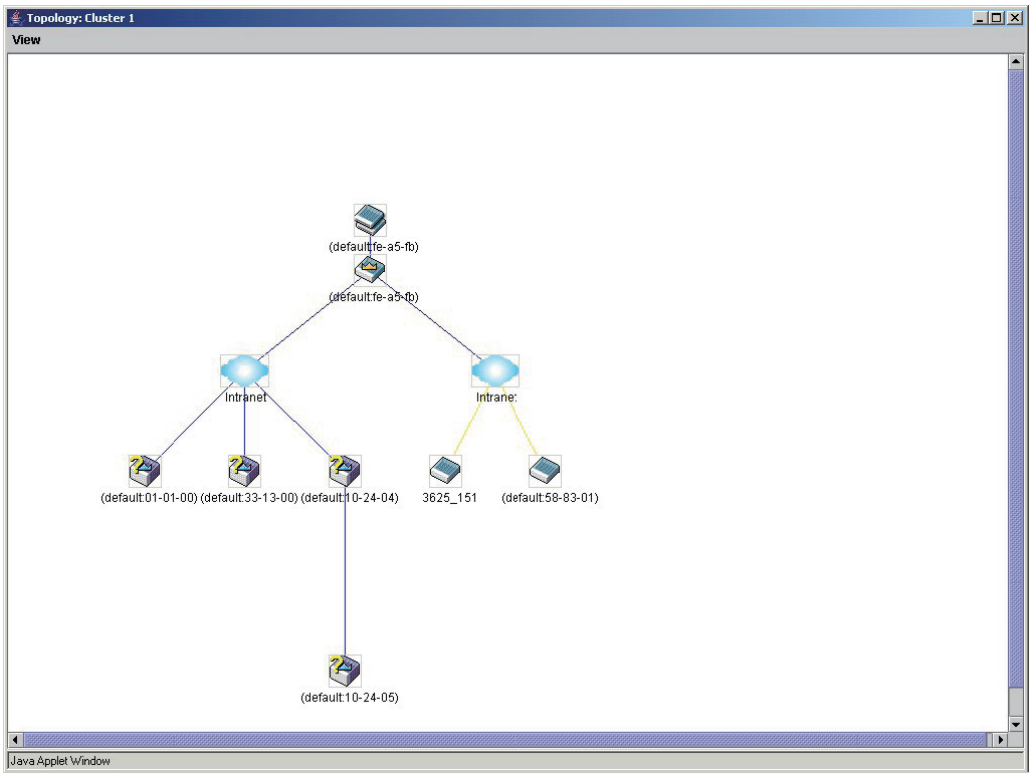


図 6-54　Topology 画面

Configuration（スイッチの主な設定）

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。

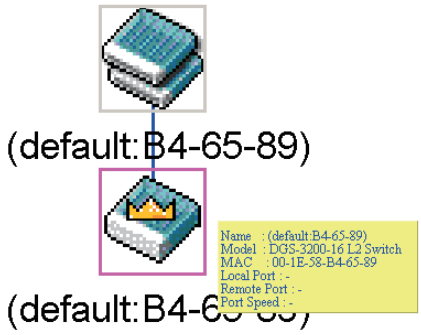


図 6-55　ツールヒントを利用したデバイス情報の表示

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。

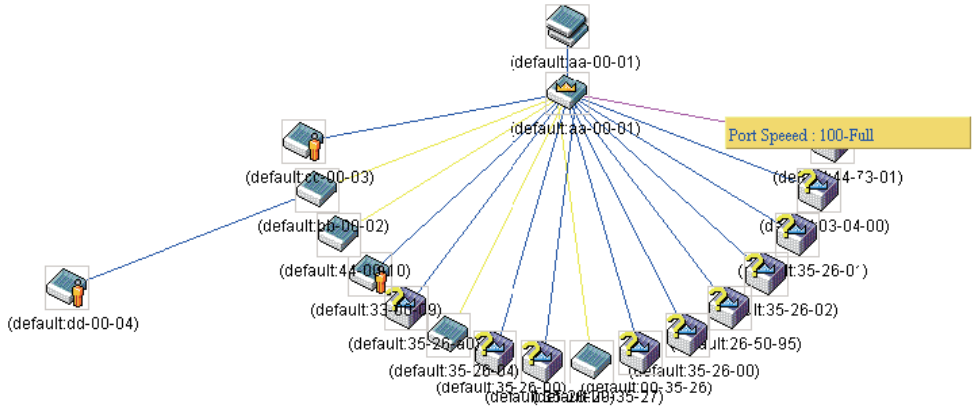


図 6-56　ツールヒントを利用したポート速度の表示

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

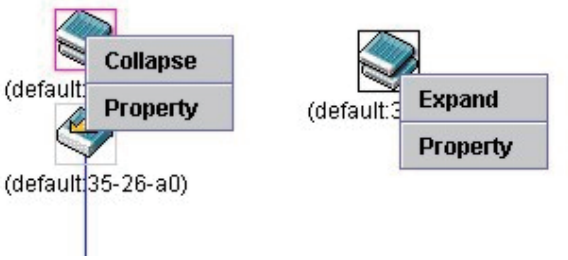


図 6-57　グループアイコン上での右クリック

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。

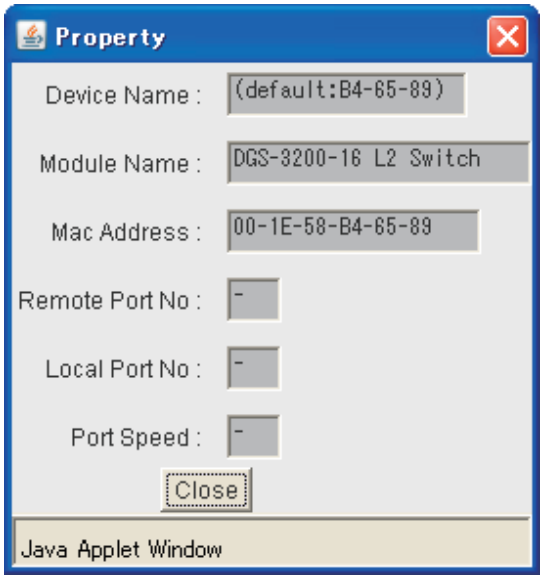


図 6-58　Property 画面

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

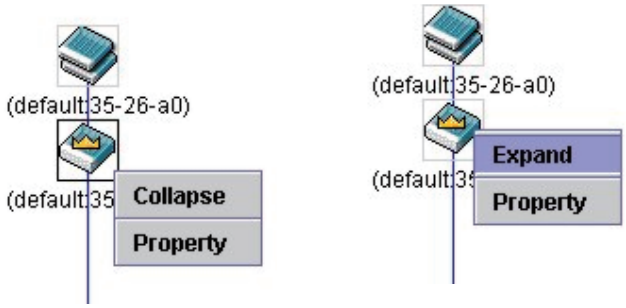


図 6-59　Commander スイッチアイコン上での右クリック

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

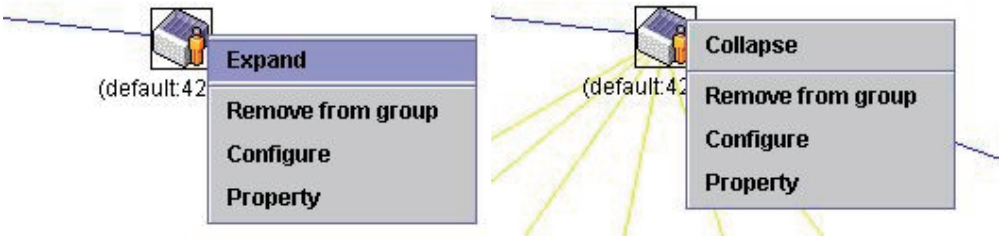


図 6-60　Member スイッチアイコン上での右クリック

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

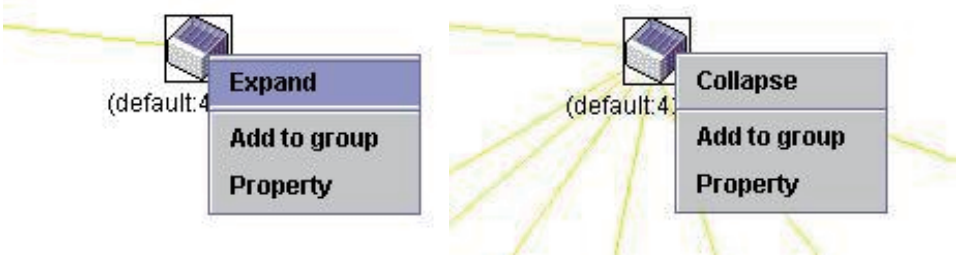


図 6-61　Candidate スイッチアイコン上での右クリック

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。

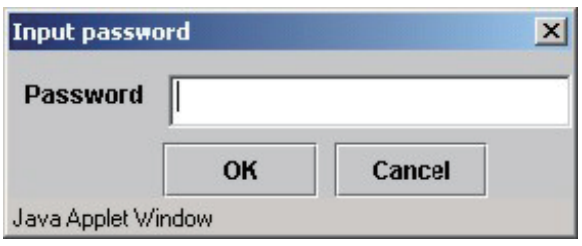


図 6-62　Input password ダイアログボックス

- 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 6-63　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 6-64　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。

Firmware Upgrade（ファームウェア更新）

CS から MS へのファームウェアの更新を行います。

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。

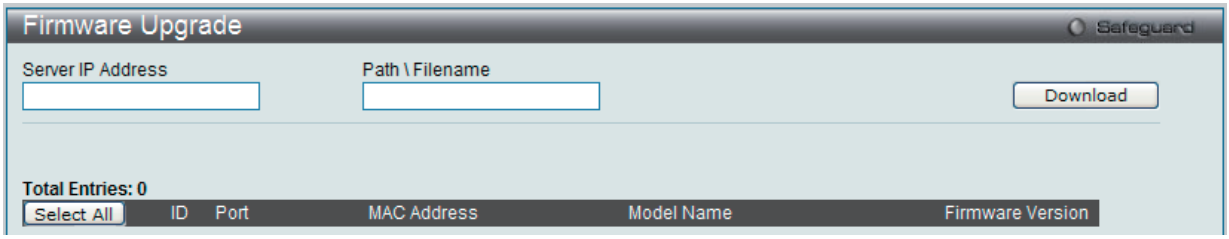


図 6-65　Firmware Upgrade 画面

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）

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

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。

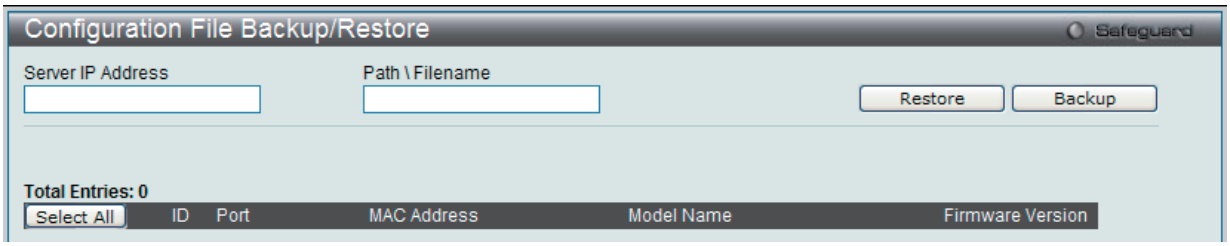


図 6-66　Configuration File Backup/Restore 画面

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）

CS は、MS から指定したサーバに送信したログファイルを依頼することができます。

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

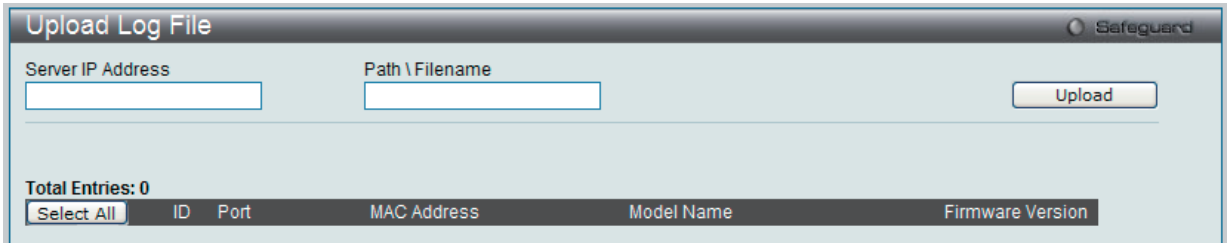


図 6-67　Upload Log File 画面

ログを格納する「Server IP Address」と MS のログファイルの「Path\Filename」を入力します。「Upload」ボタンをクリックすると TFTP サーバにログファイルを送信します。

SD Card FS Settings（SD カードファイルシステム設定）

DGS-3200-24/GE の前面パネルに SD フラッシュカードを挿入します。(DGS-3200-10 と DGS-3200-16/GE は本機能をサポートしていません。)
SD フラッシュカードで以下項目を行うことができます。

- SD カードにスイッチのログ、コンフィグレーション、ランタイムイメージ、または PROM イメージを保存します。
- SD カードからスイッチのフラッシュメモリにイメージをコピーして、ランタイムイメージ 1 または 2 を置き換えます。
- SD カードからスイッチのフラッシュメモリにコンフィグレーションファイルをコピーして、コンフィグレーション 1 または 2 を置き換えます。
- SD カードからスイッチのフラッシュメモリに PROM イメージをコピーして、PROM イメージを置き換えます。
- ランタイムイメージまたはコンフィグレーションをダウンロードして SD カードに保存します。
- PC（例えば、Microsoft Windows）を使用して SD カードのファイルにアクセスします。
- SD カードに保存されているランタイムイメージまたはコンフィグレーションを使用してスイッチを再起動します。
- SD カードはホットスワップ対応です。
- スイッチは、SD カードに自動的に新しいディレクトリとファイルを作成します。

注意 アダプタを使用した miniSD カードや microSD カードは未対応です。

注意 同じ名前を持つファイルまたはフォルダが存在すると、警告メッセージを表示し、既存ファイルまたはフォルダを上書きするか、またはそのままにするかを聞いてきます。

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

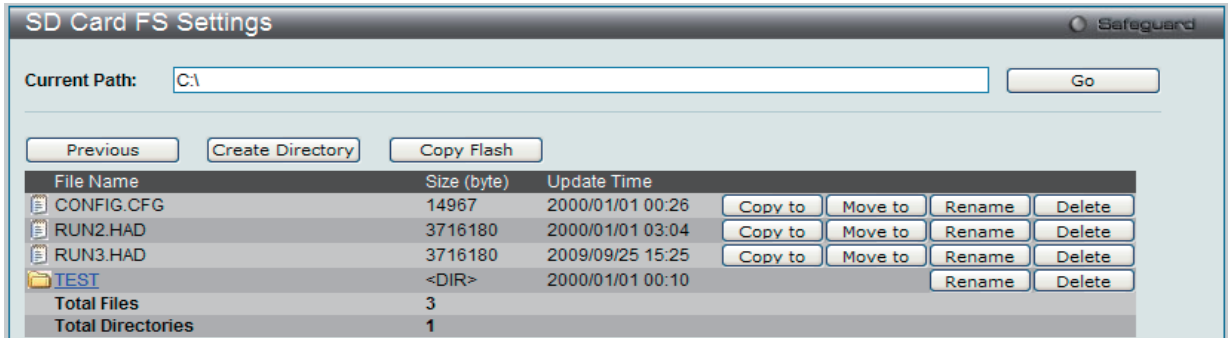


図 6-68　SD Card FS Settings 画面

SD カードにあるファームウェアイメージおよびコンフィグレーションを使用するためには、以下の手順を行います。

1. スイッチの前面パネルにある SD カードスロットに SD フラッシュカードを挿入します。
2. 「Current Path」にファームウェアイメージのパスを入力します。
3. 「Go」をクリックします。

SD フラッシュカードからファームウェアイメージとコンフィグレーションを使用することに加えて、「SD Card FS Settings」画面では、ユーザは SD カードに保存されたディレクトリとファイルを管理することができます。

以下の表では SD フラッシュカードに保存されたファイルとディレクトリを管理するのに使用されるボタンについて記述してます。

項目	説明
Previous	本ボタンをクリックして前フォルダを検索します。
Create Directory	本ボタンをクリックして、新しいディレクトリを作成します。
Copy Flash	本ボタンをクリックして、SD フラッシュカードまたは内蔵のフラッシュメモリから (に) ファイルをコピーします。
Format	新しい SD フラッシュカードを挿入すると、本ボタンが表示されます。 本ボタンをクリックして、新しい SD フラッシュカードを初期化します。
Copy to	本ボタンをクリックしてファイルを別の場所にコピーします。
Move to	本ボタンをクリックしてファイルを別の場所に移動します。
Rename	本ボタンをクリックして対応するファイルまたはフォルダ名を変更します。
Delete	本ボタンをクリックして対応するファイルかフォルダを削除します。

新しいディレクトリの作成

1. 「Create Directory」ボタンをクリックし、以下の画面を表示します。

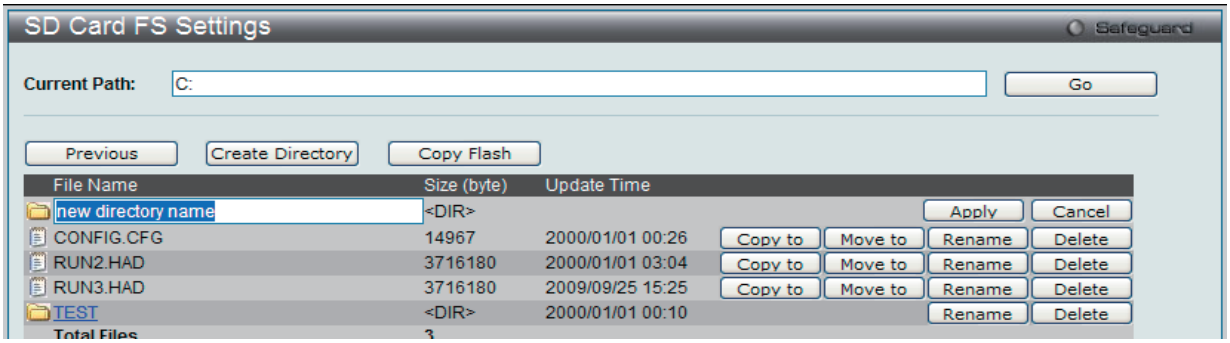


図 6-69　SD Card FS Settings 画面 - Create Directory

2. 新しいディレクトリ名を入力し、「Apply」ボタンをクリックします。

ファイルのコピー

1. 「Copy Flash」ボタンをクリックし、以下の画面を表示します。

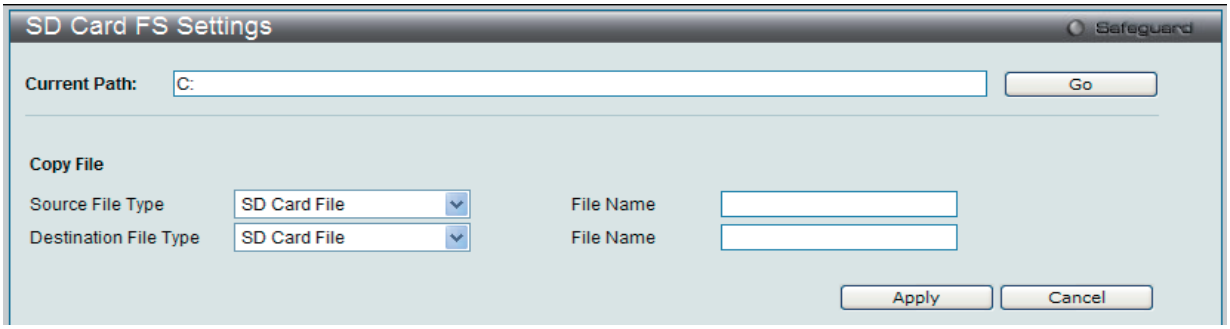


図 6-70　SD Card FS Settings 画面 - Copy Flash

2. 「Source File Type」（コピー元のファイルタイプ）を「SD Card File」、「Image File」、「Config File」、「Prom File」または「Log File」から選択し、ファイル名を「File Name」に入力します。新しいディレクトリ名を入力し、「Apply」ボタンをクリックします。

3. 「Destination File Type」（コピー先のファイルタイプ）を「SD Card File」、「Image File」、「Config File」、「Prom File」または「Log File」から選択し、ファイル名を「File Name」に入力します。

4. 「Apply」ボタンをクリックし、コピーを実行します。

テーブル内のファイルのコピー

1. テーブルに表示されている特定ファイルをコピーする場合は、対象ファイルの「Copy to」ボタンをクリックし、以下の画面を表示します。

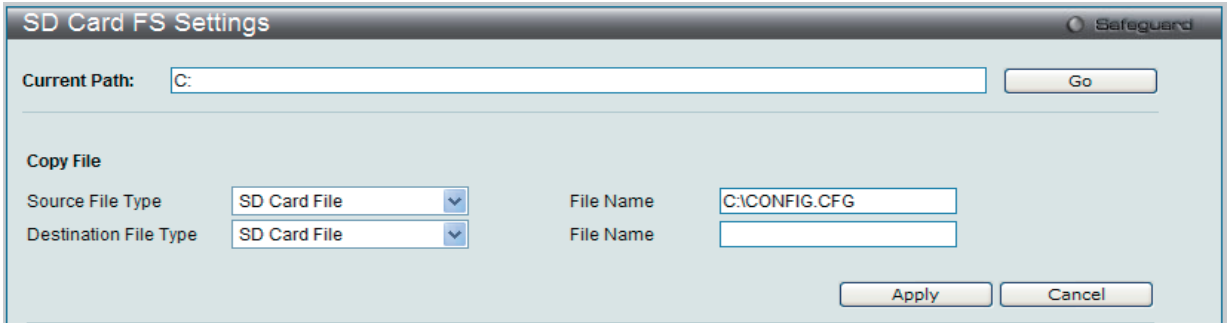


図 6-71　SD Card FS Settings 画面 - Copy to

2. 「Destination File Type」（コピー先のファイルタイプ）を「SD Card File」、「Image File」、「Config File」、「Prom File」または「Log File」から選択し、ファイル名を「File Name」に入力します。

3. 「Apply」ボタンをクリックし、コピーを実行します。

ファイルの移動

1. テーブル内のファイルを移動する場合は、対象のファイルの「Move to」ボタンをクリックし、以下の画面を表示します。

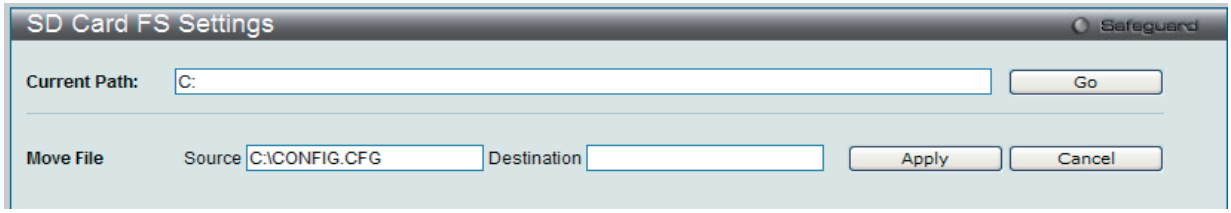


図 6-72　SD Card FS Settings 画面 - Move to

2. 「Destination」に移動先のパスを入力後、「Apply」ボタンをクリックし、移動を実行します。

ファイル名の変更

1. テーブル内のファイル名を変更する場合は、「Rename」ボタンをクリックし、以下の画面を表示します。

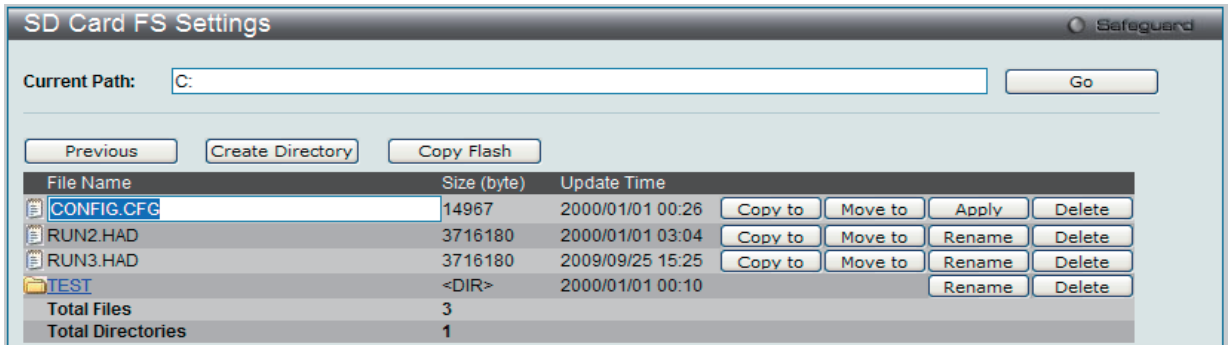


図 6-73　SD Card FS Settings 画面 - Rename

2. ファイル名を変更後、「Apply」ボタンをクリックします。

ファイルの削除

1. テーブル内の削除するファイルの「Delete」ボタンをクリックします。

第 7 章　L2 Features（L2 機能の設定）

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

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

サブメニュー	説明	参照ページ
Jumbo Frame（ジャンボフレームの有効化）	ジャンボフレーム機能を有効 / 無効にします。	93 ページ
Egress Filter Settings（Egress フィルタ設定）	Egress フィルタを設定します。	94 ページ
802.1Q VLAN（VLAN 設定）	802.1Q VLAN 設定を行います。	95 ページ
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。	101 ページ
802.1v Protocol VLAN（802.1v プロトコル VLAN）	802.1v プロトコル VLAN 設定を行います。	105 ページ
MAC Based VLAN Settings（MAC ベース VLAN の設定）	MAC ベース VLAN を設定します。	107 ページ
GVRP Settings（GVRP の設定）	VLAN 構成情報を共有するために GVRP 設定を行います。	108 ページ
PVID Auto Assign Settings（PVID 自動割り当て設定）	PVID 自動割り当てを設定します。	108 ページ
Trunking（トランキングの設定）	ポートトランキング設定を行います。	109 ページ
VLAN Trunk Settings（VLAN トランク設定）	多くの VLAN ポートを集約して VLAN トランクを作成します。	111 ページ
LACP Port Settings（LACP の設定）	ポートトランキンググループを設定します。	112 ページ
Traffic Segmentation（トラフィックセグメンテーション）	トラフィックフローの分割設定を行います。	113 ページ
IGMP Snooping Settings（IGMP Snooping の設定）	IGMP Snooping 機能を設定します。	114 ページ
MLD Snooping Settings（MLD Snooping 設定）	MLD Snooping 機能を設定します。	122 ページ
Port Mirroring（ポートミラーリングの設定）	ポートミラーリングの設定を行います。	125 ページ
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。	126 ページ
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。	127 ページ
Forwarding & Filtering（フォワーディングとフィルタリングの設定）	ユニキャスト / マルチキャストフォワーディングとフィルタリングの設定を行います。	134 ページ

以下のセクションでは、ユーザがスイッチにセキュリティ機能を設定します。スイッチにはさまざまな VLAN 機能、トランキング、IGMP Snooping、MLD Snooping、スパニングツリー、およびフォワーディング & フィルタリング機能があり、ここではその詳細について記述しています。

Jumbo Frame（ジャンボフレームの有効化）

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。ジャンボフレームは、1500 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。「Jumbo Frame」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。

L2 Features > Jumbo Frame の順にクリックし、以下の画面を表示します。

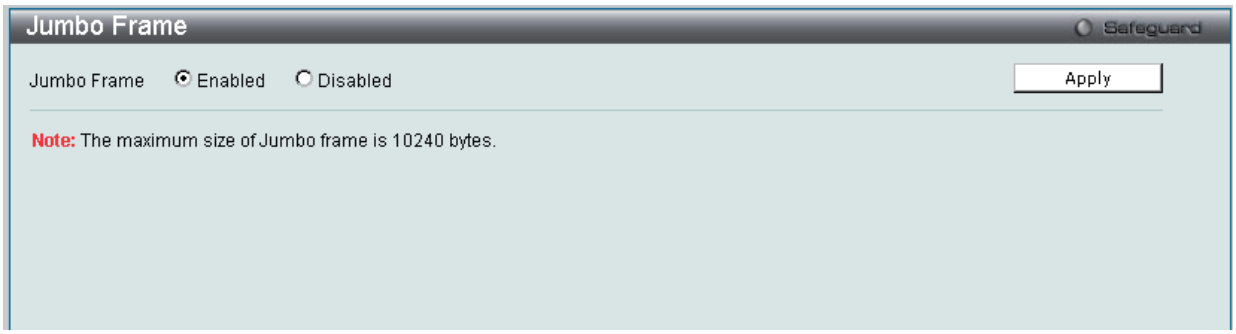


図 7-1　Jumbo Frame 画面

本画面には次の項目があります。

項目	説明
Jumbo Frame	ジャンボフレームを扱うかどうかを設定します。最大フレームサイズは 10240 バイトです。 • Enabled - デバイスでジャンボフレームを有効に設定します。 • Disabled - デバイスでジャンボフレームを無効に設定します。（初期値）

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

Egress Filter Settings（Egress フィルタ設定）

指定のポートに不明のユニキャストや未登録のマルチキャストパケットに対する Egress フィルタを設定することができます。

スイッチは、Egress ポートに送信された不明のユニキャスト / マルチキャストパケットを検知すると、それらをすべて Egress ポートで廃棄します。ユーザは、不明のユニキャスト / マルチキャストパケットの受信を許可、または拒否するポートを選択することができます。

L2 Features > Egress 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。

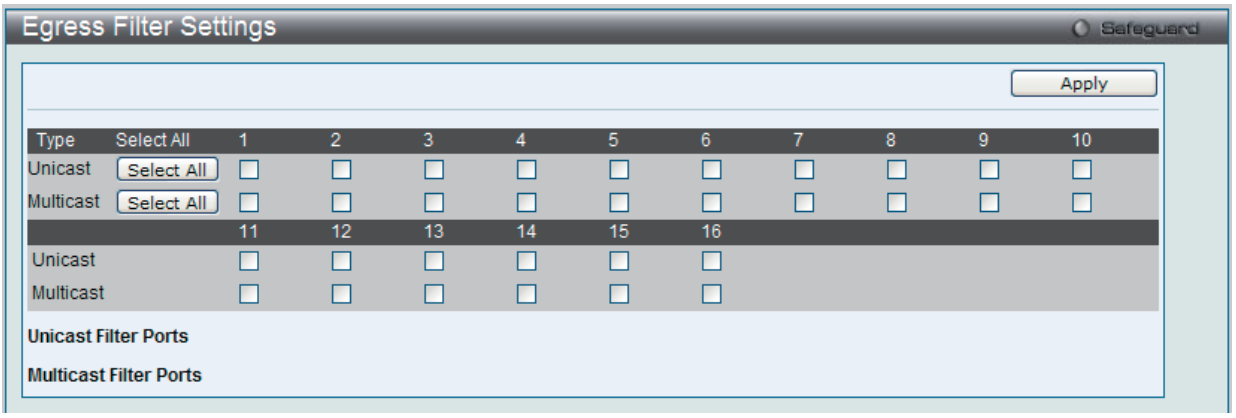


図 7-2　Egress Filter Settings 画面

以下のパラメータを使用して、設定および表示を行います。

項目	説明
Unicast	不明のユニキャストパケットをフィルタするポートを指定します。これらのパケットは指定したポートには送信されません。指定しないポートは不明のユニキャストパケットをフィルタしないため、パケットはポートに送信されます。
Multicast	未登録のマルチキャストパケットをフィルタするポートを指定します。これらのパケットは指定したポートに送信されません。指定しないポートは未登録のマルチキャストパケットをフィルタしないため、パケットはポートに送信されます。

「Apply」ボタンをクリックし、変更を有効にします。

802.1Q VLAN（VLAN 設定）

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

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

VLAN 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

本スイッチにおける VLAN の特長は以下の通りです。

- 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。
- 本スイッチは IEEE 802.1Q VLAN をサポートします。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。
Ingress 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。
Egress 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。
- Ingress 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。
- Egress 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。

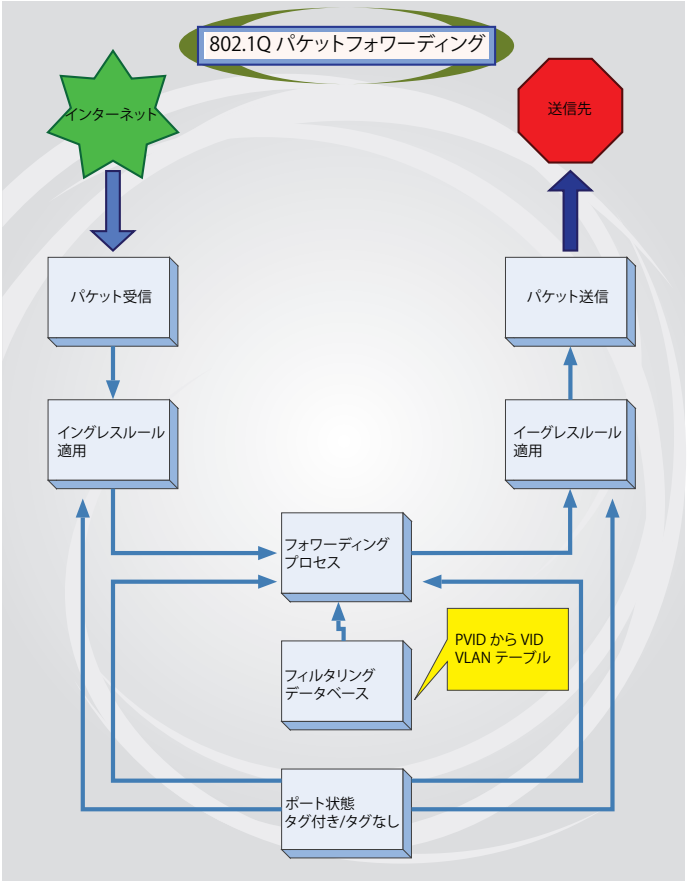


図 7-3　IEEE 802.1Q パケットフォワーディング

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 ビットからなります。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。

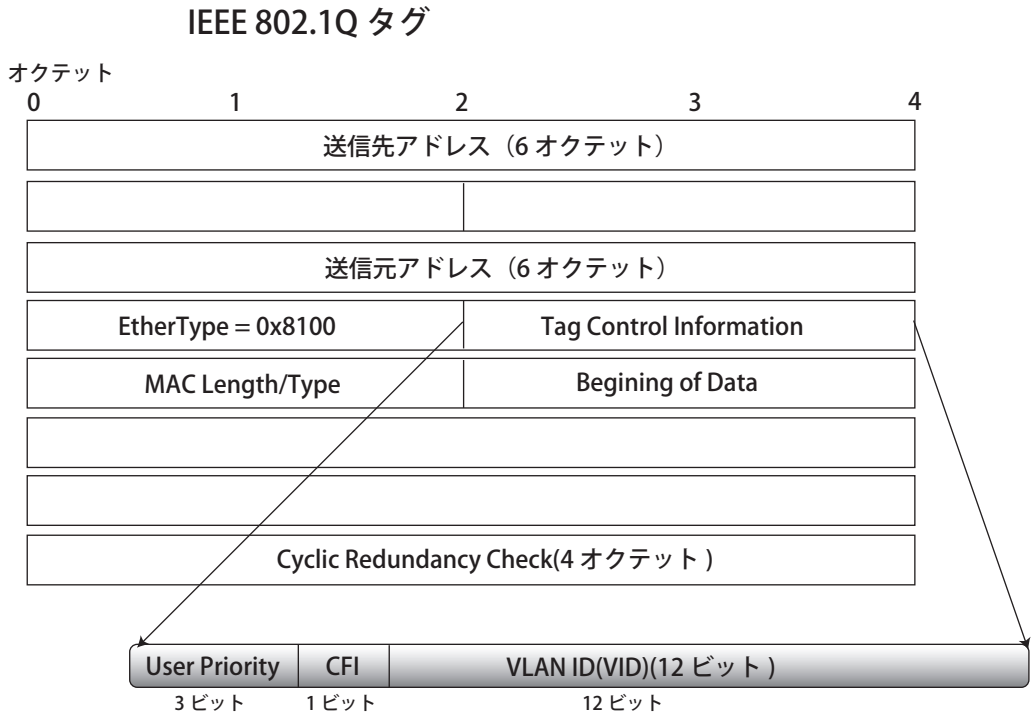


図 7-4　IEEE 802.1Q タグ

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

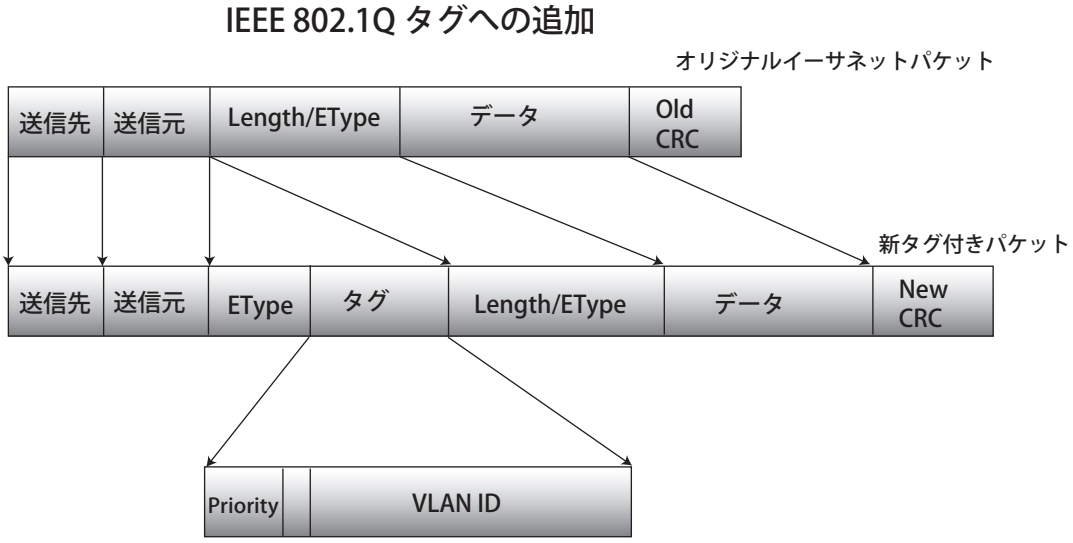


図 7-5　IEEE 802.1Q タグの挿入

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。

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

スイッチのすべての物理ポートは PVID を持っています。802.1Q にも PVID が割り当てられ、スイッチ内で使用されます。スイッチ上に VLAN が定義されていなければ、すべてのポートはデフォルト VLAN と PVID 1 が割り当てられます。タグなしのパケットはそれらを受信したポートの PVID を割り当てられます。フォワーディングはこの PVID を元に決定され、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 対応のスイッチの全ポートは、タグ付きかタグなしに設定できます。
タグ付きのポートは受信、送信するすべてのパケットのヘッダに、VID、プライオリティ、そしてそのほかの VLAN 情報を埋め込みます。パケットが既にタグ付けされていたなら、VLAN 情報を完全に保つためにポートはパケットを変更しません。ネットワーク上の他の 802.1Q 対応デバイスも、タグの VLAN 情報を使用してパケットの転送を決定します。
タグなしのポートは、受信、送信するすべてのパケットから 802.1Q タグを削除します。パケットに 802.1Q VLAN タグがなければ、ポートはパケットを変更しません。つまり、タグなしのポートが受信して、転送したすべてのパケットは 802.1Q VLAN 情報をまったく持ちません。PVID はスイッチの内部で使用されるだけです。タグなしはパケットを 802.1Q 対応のデバイスから、非対応のデバイスにパケットを送信するのに使用します。

Ingress フィルタリング

スイッチ上のポート内に、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 Ingress ポートと呼びます。Ingress 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、Ingress 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。Ingress 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、Ingress ポートはそのパケットに VID として自分の PVID を付加します（ポートがタグ付きポートである場合）。するとスイッチは、送信先ポートは Ingress 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、Ingress フィルタリングと呼ばれ、同じ Ingress ポートと同じ VLAN 上のものではないパケットを受信時に廃棄することにより、スイッチ内での帯域を有効利用するために使用されます。これにより送信先ポートに届いてから廃棄されるだけとなるパケットを事前に処理することができるようになります。

デフォルト VLAN

スイッチでは、最初に「default」という名で VID が 1 の VLAN が設定されています。本製品の初期設定ではスイッチ上のすべてのポートが「default」に割り当てられています。

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 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 7-1　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 VLAN2 に所属しているか、否か（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 とトランクグループ

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

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

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

VLAN リストの表示

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

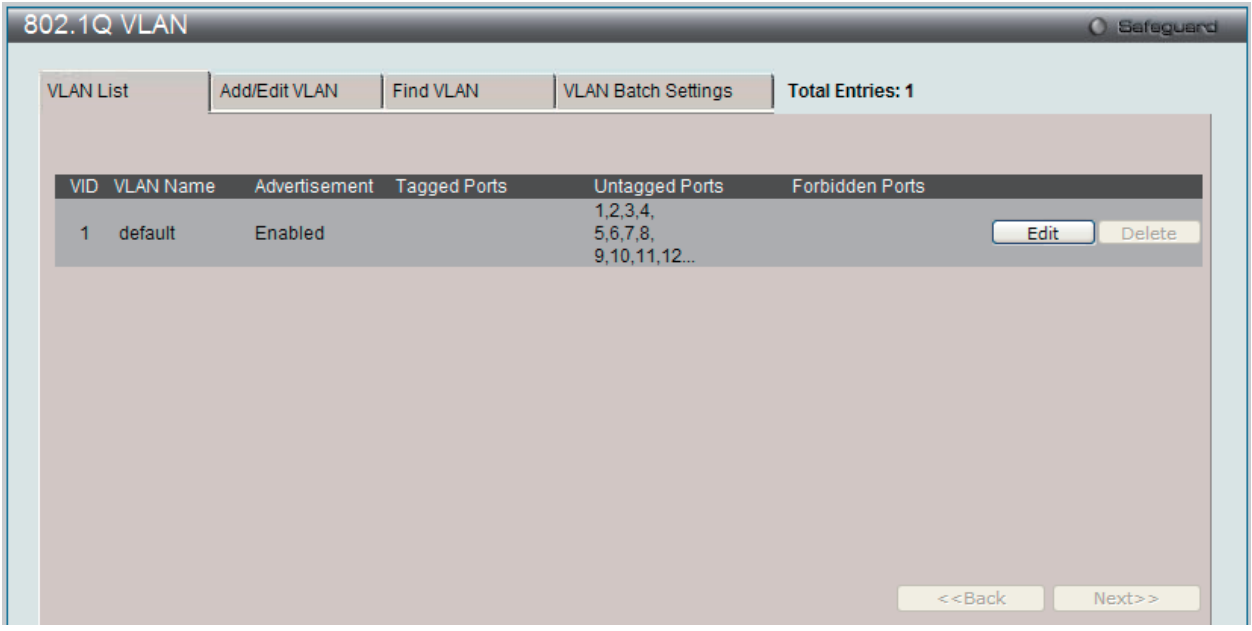


図 7-6　802.1Q VLAN - VLAN List 画面

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

新規 802.1Q VLAN の登録

「Add/Edit VLAN」タブをクリックします。以下の画面でポート設定と新しい VLAN に固有の名前と番号を割り当てます。

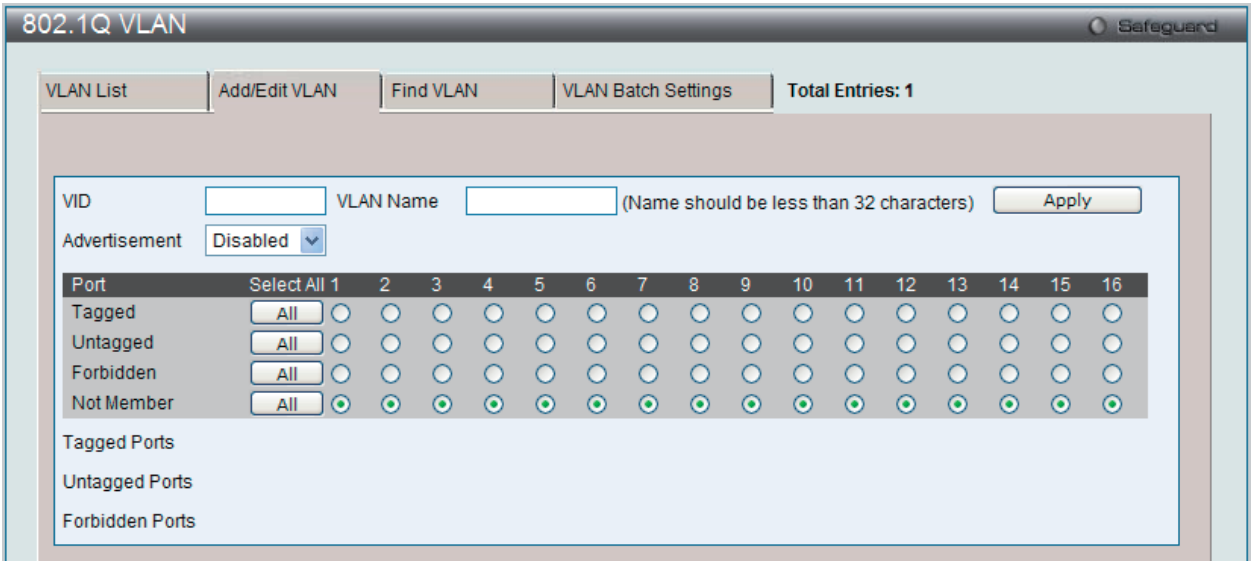


図 7-7　802.1Q VLAN - Add/Edit VLAN タブ画面

「Add/Edit VLAN」タブには以下の項目が含まれます。

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

「Apply」ボタンをクリックし、デバイスに VLAN 設定を適用します。

VLAN の検索

「Find VLAN」タブをクリックします。以下の画面が表示されます。

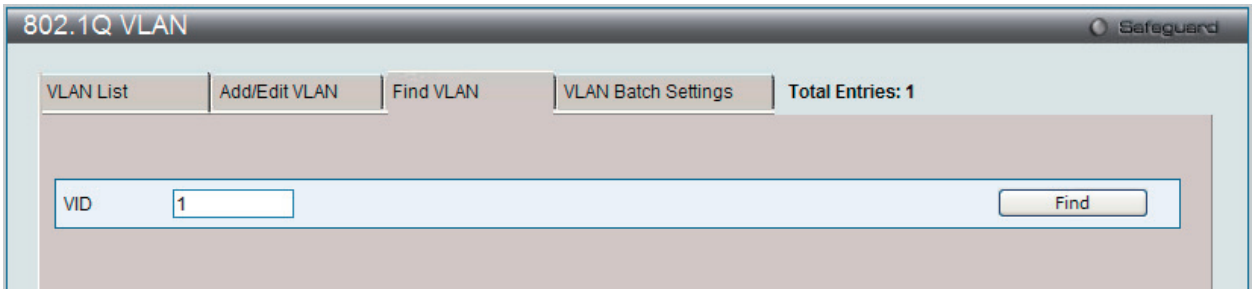


図 7-8　802.1Q VLAN - Find VLAN タブ画面

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

注意　本スイッチは 4K スタティック VLAN エントリをサポートしています。

802.1Q VLAN バッチの作成

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

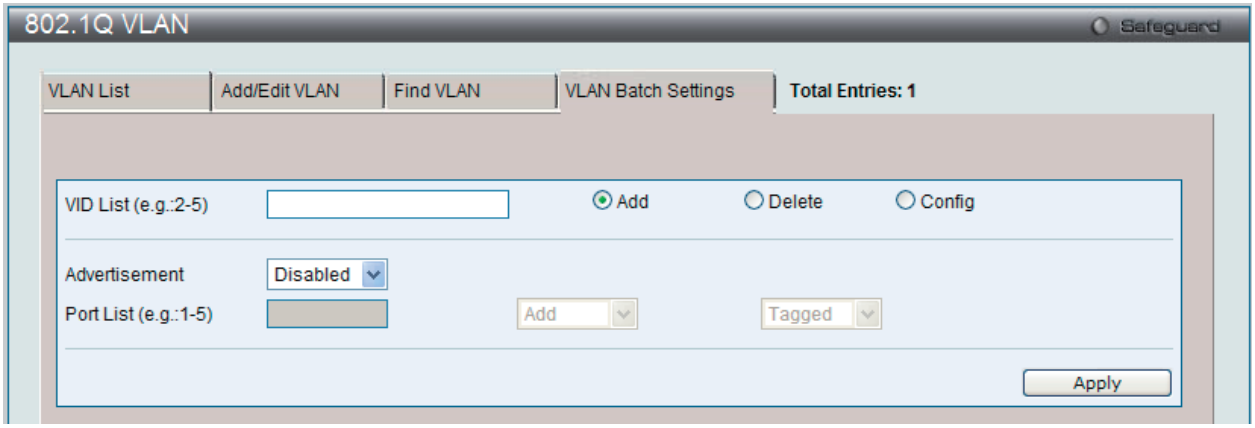


図 7-9　802.1Q VLAN Batch Settings 画面

以下の項目を使用して設定します。

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

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

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

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。

以下の図はプライベート VLAN ドメインの構造を示しています。

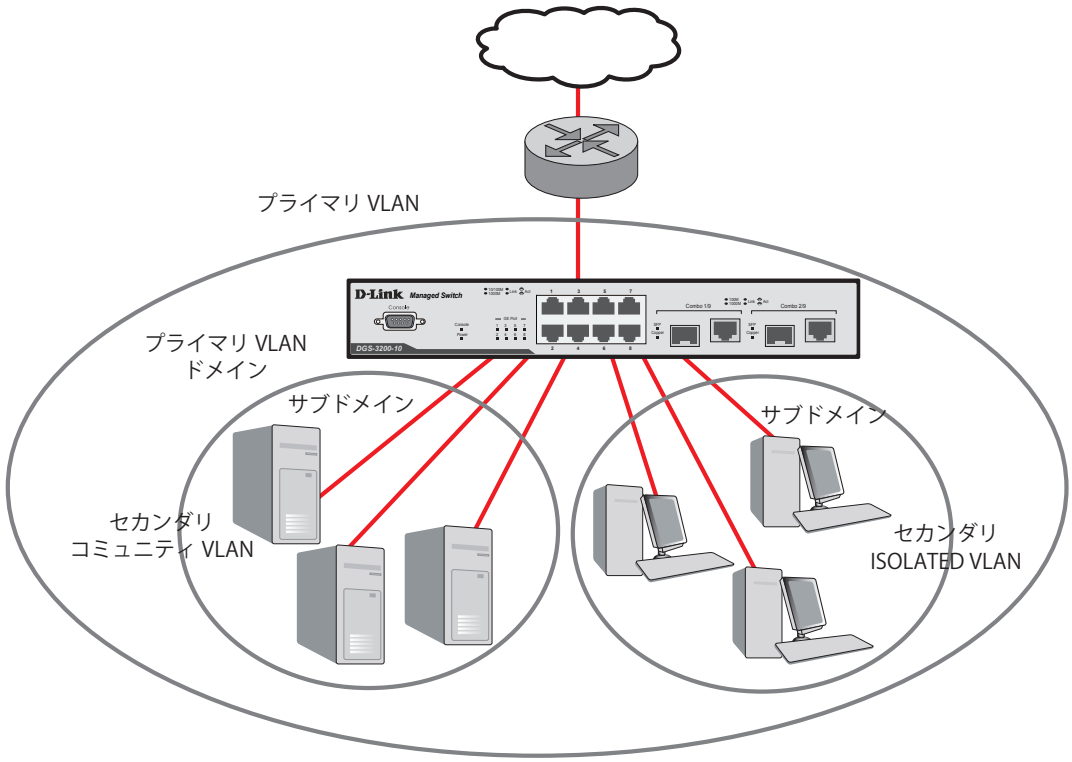


図 7-10　プライベート VLAN ドメイン

プライベート VLAN におけるポートは以下の 3 つのタイプのいずれかです。

ポートタイプ	説明
Promiscuous	Promiscuous ポートは、プライマリ VLAN に関連するセカンダリ VLAN 上の Community として設定されたポートと Isolated ポートを含むすべてのインタフェースと通信できるプライマリ VLAN のメンバであるポートです。
Isolated	Isolated ポートは、Isolated セカンダリ VLAN のメンバであるホストポートについて説明するために使用されます。Isolated ポートは、Promiscuous ポートを別としてレイヤ 2 で同じプライベート VLAN ドメイン内の他のポートから完全に隔離されます。Promiscuous ポートから送信されるトラフィックを除き、Isolated ポートに到達するすべてのトラフィックをブロックします。Isolated ポートから送信されるどんなトラフィックも Promiscuous ポートに転送されるだけです。
Community	Community ポートは、Community セカンダリ VLAN のメンバであるホストポートについて説明するために使用されます。Community ポートは、同じ Community VLAN のメンバであるポートと Isolated ポートの両方と通信できます。Community ポートとして設定されるインタフェースは、レイヤ 2 において異なる Community のメンバであるすべてのインタフェース、および同じプライベート VLAN ドメインのメンバである Isolated ポートから隔離されます。

L2 Features > 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。

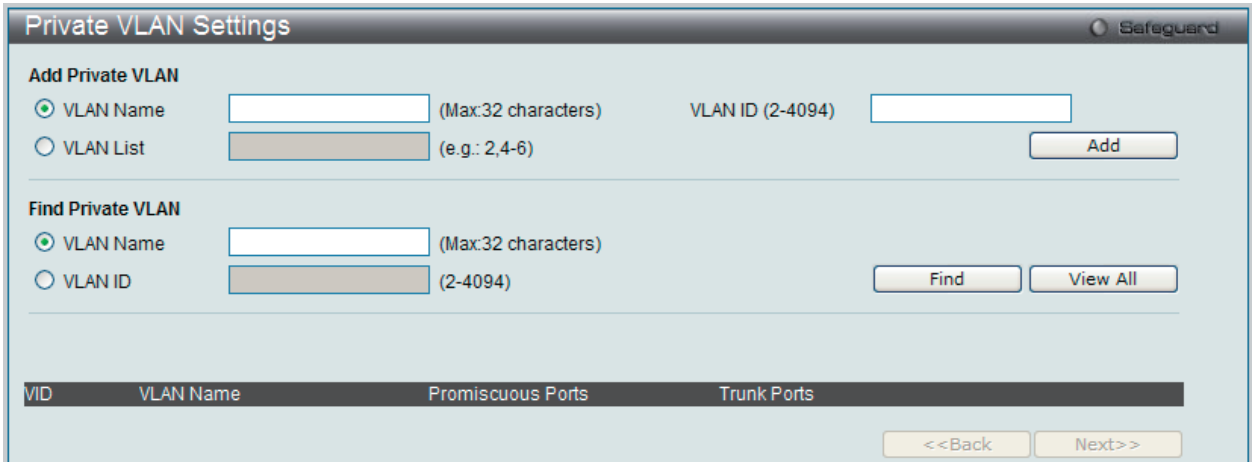


図 7-11　Private VLAN Settings 画面

新しいプライベート VLAN の作成

「Add Private VLAN」セクションで以下の項目を設定し、新しいプライベート VLAN を作成します。

項目	説明
VLAN Name	「VLAN Name」をチェックし、プライベート VLAN 名を指定します。
VLAN ID(2-4094)	「VLAN Name」をチェックし、プライベート VLAN の VLAN ID を指定します。

「Add」ボタンをクリックして、新しいプライベート VLAN エントリを作成します。新しいプライベート VLAN が画面下半分に表示されます。

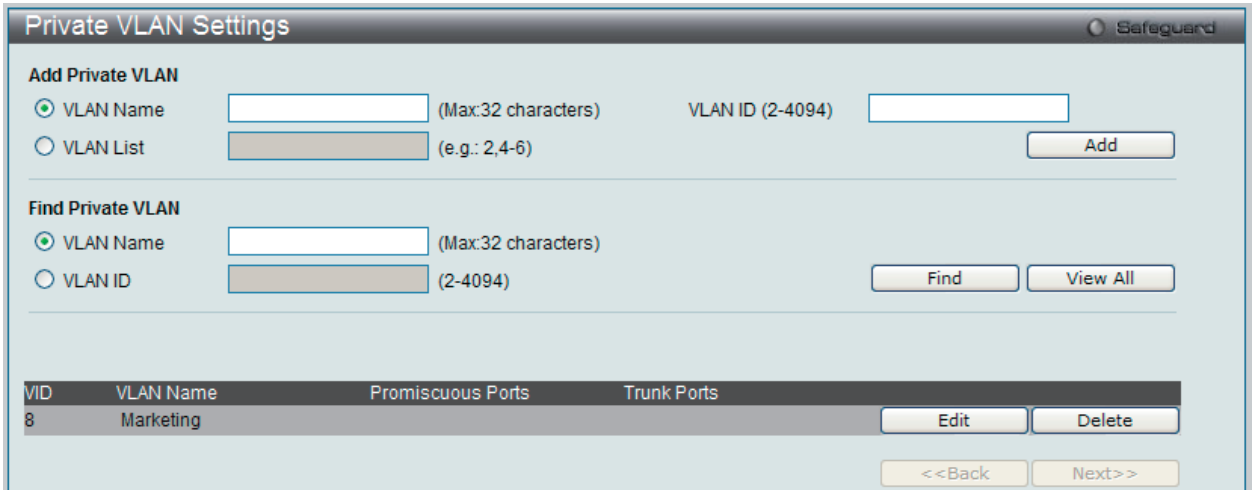


図 7-12　Private VLAN Settings 画面

既存のプライベート VLAN の検索

「Find Private VLAN」セクションで以下の項目を設定し、既存のプライベート VLAN を検索します。

項目	説明
VLAN Name	VLAN 名を使用してプライベート VLAN を検索する場合、ここをチェックし、隣接する欄にプライベート VLAN 名を指定します。
VLAN ID (2-4094)	「VLAN List」をチェックし、プライベート VLAN の VLAN ID を指定します。

「Find」ボタンをクリックして、プライベート VLAN を検索します。プライベート VLAN が検索条件に一致すると画面下半分に表示されます。

画面下半分に以下のプライベート VLAN に関する情報が表示されます。

項目	説明
VID	プライベート VLAN の VLAN ID を表示します。
VLAN Name	プライベート VLAN 名を表示します。
Promiscuous Ports	プライベート VLAN 用の Promiscuous ポートとして設定されているポート番号を表示します。
Trunk Ports	プライベート VLAN 用のトランクポートとして設定されているポート番号を表示します。

既存のプライベート VLAN の参照

「View All」ボタンをクリックし、スイッチに設定されているすべてのプライベート VLAN を表示します。プライベート VLAN が画面下半分に表示されます。

既存のプライベート VLAN の削除

画面下半分にあるリストから削除するプライベート VLAN に隣接する「Delete」ボタンをクリックします。

既存のプライベート VLAN の編集

画面下半分にあるリストから編集するプライベート VLAN に隣接する「Edit」ボタンをクリックして以下の画面を表示します。

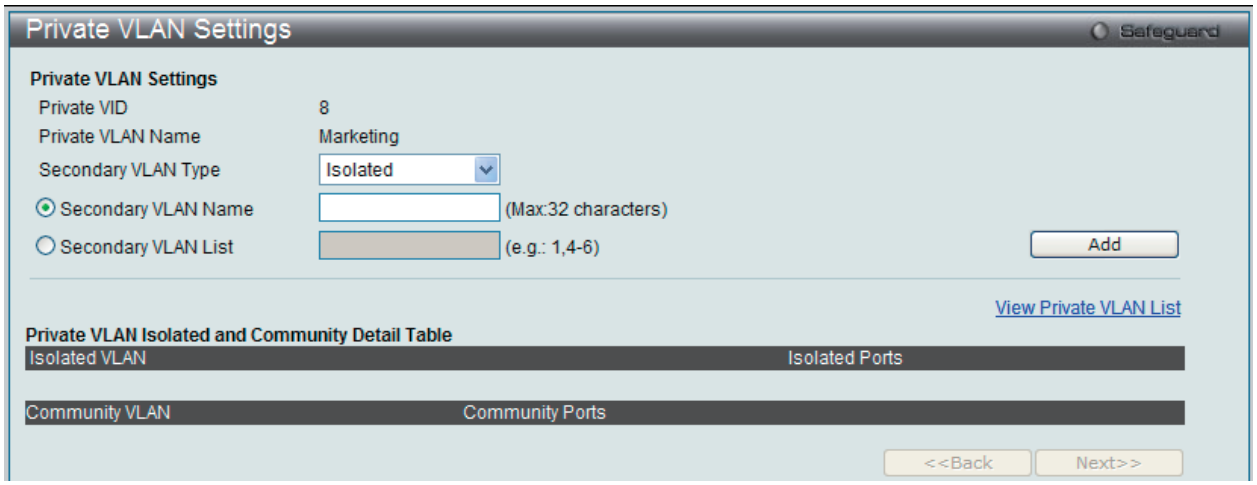


図 7-13　Private VLAN Settings 画面

本画面は「Private VLAN Settings」と「Private VLAN Isolated and Community Detail Table」の 2 つのメインセクションに分かれています。

「Private VLAN Settings」セクションには以下の項目があります。

項目	説明
Private VID	プライベート VLAN の VLAN ID を表示します。
Private VLAN Name	プライベート VLAN 名を表示します。
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。

「Add」ボタンをクリックして、プライベート VLAN を更新します。

「Private VLAN Isolated and Community Detail Table」セクションには以下の項目があります。

項目	説明
Isolated VLAN	Isolated VLAN として設定されているすべての VLAN の VLAN ID または VLAN 名を表示します。
Isolated Ports	Isolated VLAN として設定されているすべての VLAN のポート番号を表示します。
Community VLAN	Community VLAN として設定されているすべての VLAN の VLAN ID または VLAN 名を表示します。
Community Ports	Community VLAN として設定されているすべての VLAN のポート番号を表示します。

プライベート Isolated VLAN エントリの削除

削除するプライベート Isolated VLAN エントリに隣接する「Delete」ボタンをクリックします。

プライベート Community VLAN エントリの削除

削除するプライベート Community VLAN エントリに隣接する「Delete」ボタンをクリックします。

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

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

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

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

L2 Features > 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。

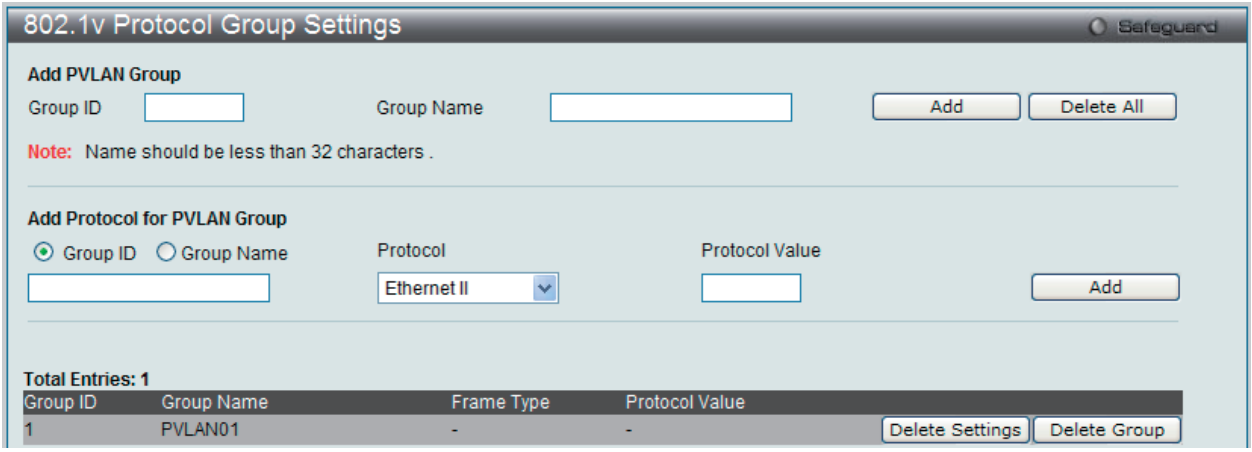


図 7-14　802.1v Protocol Group Settings 画面

テーブルの下半分は定義済みのすべてのグループを表示します。

以下の項目を使用して、設定します。

項目	説明
Add PVLAN Group	
Group ID	グループの ID 番号を 1-2147483647 の範囲から指定します。
Group Name	新しいプロトコル VLAN グループの識別に使用します。32 文字までの半角英数字を入力します。
Add Protocol for PVLAN Group	
Group ID	グループの ID 番号を 1-2147483647 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 または IEEE802.3 SNAP から選択します。
Protocol Value	グループに対してプロトコル値を入力します。プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。入力形式は 0x0 から 0xffff です。オクテット文字列は、フレームタイプによって、以下に示す値の 1 つを持っています。 • Ethernet II - 16 ビット (2 オクテット) の 16 進数です。例えば、IPv4 は 800、IPv6 は 86dd、ARP は 806 などです。 • IEEE802.3 SNAP - 16 ビット（2 オクテット）の 16 進数です。 • IEEE802.3 LLC - 2 オクテットの IEEE 802.2 Link Service Access Point（LSAP）ペアです。はじめのオクテットは、Destination Service Access Point（DSAP）のための値であり、2 番目のオクテットは送信元のための値です。

プロトコル VLAN グループの新規追加

「Add PVLAN 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 PVLAN 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 > 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。

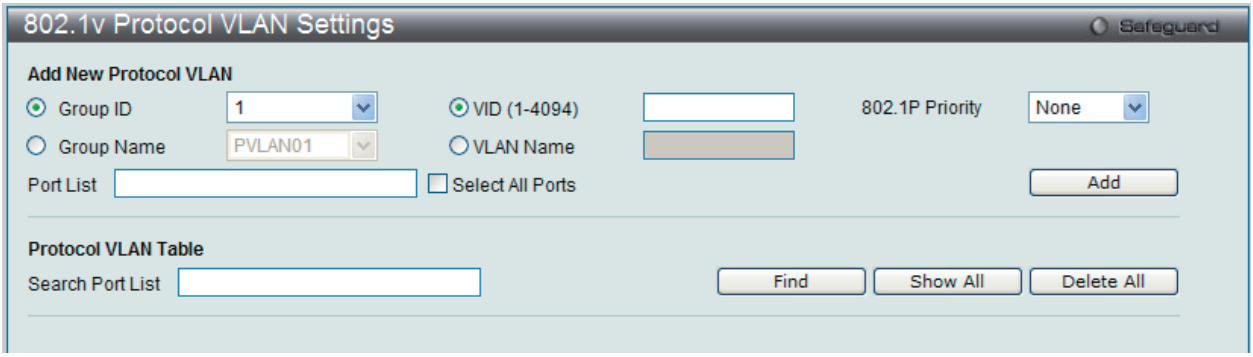


図 7-15　802.1v Protocol VLAN Settings 画面

以下の項目を使用して、設定します。

項目	説明
Add New Protocol VLAN	
Group ID	対応するボタンをチェックし、プルダウンメニューから定義済みの Group ID を選択します。
Group Name	対応するボタンをチェックし、プルダウンメニューから定義済みの Group Name を選択します。
VID (1-4094)	対応するボタンをチェックし、VID を入力します。これは、VLAN 名と共に、ユーザが作成する VLAN を識別するために使用する ID です。
VLAN Name	対応するボタンをチェックし、VLAN Name を入力します。これは、VLAN ID と共に、ユーザが作成する VLAN を識別するために使用する VLAN 名です。
802.1P Priority	スイッチに設定済みの 802.1p デフォルトプライオリティ（パケットが送られる CoS キューを決定するために使用）の設定を書き換える場合に使用します。本項目を選択すると、スイッチが受信したパケットの中の、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。 プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの 136 ページの「第 8 章 QoS（QoS 機能の設定）」を参照してください。
Port List	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「Select All Ports」チェックボックスをチェックします。
Protocol VLAN Table	
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、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。

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。

エントリがポートに作成される場合、ポートは指定した VLAN のタグなしメンバポートに自動的になります。スタティック MAC ベース VLAN のエントリがユーザに作成されると、このユーザからのトラフィックはこのポートで動作する認証機能に関わらず指定 VLAN の下で行われます。

L2 Features > 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。

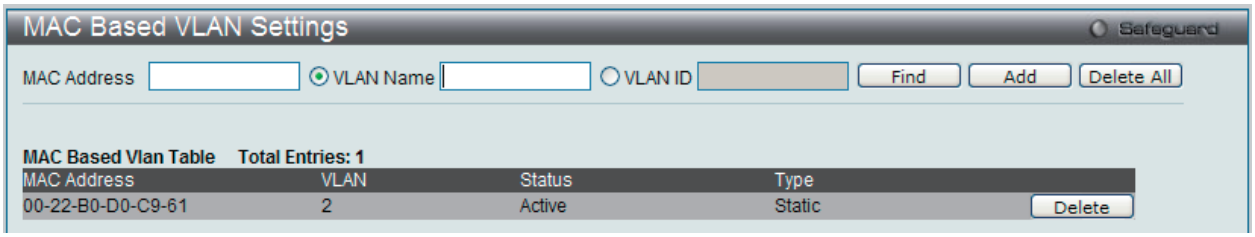


図 7-16　MAC Based VLAN Settings 画面

以下の項目を使用して設定します。

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

エントリの新規登録

MAC ベース VLAN に登録する MAC アドレスを「MAC Address」に入力し、関連付ける「VLAN Name」または「VLAN ID」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」、「VLAN Name」または「VLAN ID」を入力し、「Find」ボタンをクリックします。結果は「MAC Based Vlan Table」に表示されます。

エントリの削除

「MAC Based Vlan Table」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。

注意 MAC ベース VLAN はテーブルを下記の機能と共有しています。そのため下記の機能と組み合わせて使う場合は合計で 240 エントリーまでの利用となりますので、ご注意ください。また、スタティック登録で使う場合は最大 128 エントリーまでとなりますのでご注意ください。

1. MAC-based VLAN entry
2. IMPB(ACL mode) entry
3. MBA entry
4. IGMPv3 snooping entry
5. MLDv2 snooping entry
6. WAC entry
7. JWAC entry
8. 802.1X entry

GVRP Settings（GVRP の設定）

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

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

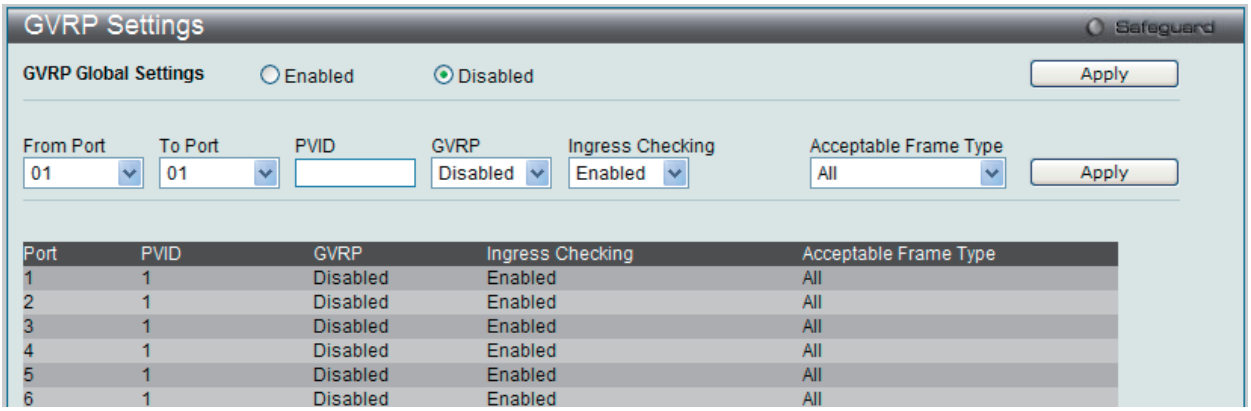


図 7-17　GVRP Setting 画面

本画面には次の項目があります。

項目	説明
GVRP Global Settings	デバイスで GVRP を有効にするかを設定し、「Apply」ボタンをクリックします。 • Enabled - デバイスで GVRP を有効に設定します。 • Disabled - デバイスで GVRP を無効に設定します。（初期値）
From Port	ポートベース VLAN に含まれるポート範囲の開始のポート番号を設定します。
To Port	ポートベース VLAN に含まれるポート範囲の最後のポート番号を設定します。
PVID	PVID を VLAN に手動で割り当てます。スイッチには初期状態ですべてのポートが default VLAN（VID=1）に割り当てています。PVID はポートが送信時にタグなしパケットにタグ付けをしたり、受信時にフィルタリングをするためのものです。ポートがタグ付きフレームのみを受信すると指定し、タグ付けや、転送のためにタグなしパケットを送られた場合は、ポートはタグに組み込む VID として PVID を使用し 802.1Q タグを付加します。パケットが送信先に到着した時には、受信デバイスは PVID に基づき VLAN による転送を行います。ポートがパケットを受信し、Ingress フィルタリングが有効ならば、ポートは VID と自身の PVID を比較します。2 つが異なる場合、パケットは破棄され、同一ならばパケットは受信されます。
GVRP	GVRP が各ポートをダイナミックに VLAN メンバにするかどうかを設定します。 • Enabled - 選択したポートで GVRP を有効に設定します。 • Disabled - 選択したポートで GVRP を無効に設定します。（初期値）
Ingress Checking	Ingress フィルタリングの有効 / 無効を設定します。 デバイスで Ingress チェックを有効にするかを設定します。 • Enabled - デバイスで Ingress チェックを有効に設定します。Ingress チェックにより、受信したタグ付きパケットの VID とポートに割り当てられた PVID を比較します。PVID が異なっていれば、ポートはパケットを破棄します。（初期値） • Disabled - デバイスで Ingress チェックを無効に設定します。
Acceptable FrameType	ポートが受け入れる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。 • 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。

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。初期値は「Enabled」です。

L2 Features > 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。

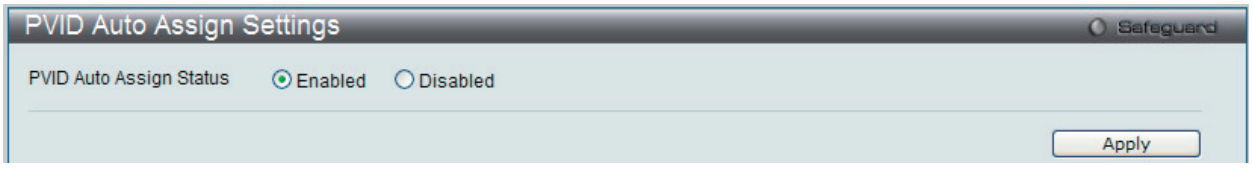


図 7-18　PVID Auto Assign Settings 画面

「Apply」ボタンをクリックし、デバイスに設定を適用します。PVID に関する詳細は、上記セクションを参照してください。

Port Trunking（ポートトランキングの設定）

ポートトランクグループについて

ポートトランクグループは、多くのポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。さらに、ポートまたはリンクの 1 つがポートトランクグループでエラーになると、リモートスイッチへのネットワーク接続が維持されるという冗長性という利点があります。

以下の表では、各トランクグループでサポートされる最大グループ数と各スイッチのビットレートを示しています。

表 7-2　DGS-3200-10、DGS-3200-16/GE、DGS-3200-24/GE のポートトランクグループテーブル

製品名	グループの最大数	ポートの最大数	ポテンシャルビットレート
DGS-3200-10	5	8	8000 Mbps
DGS-3200-16/GE	8	8	8000 Mbps
DGS-3200-24/GE	12	8	8000 Mbps

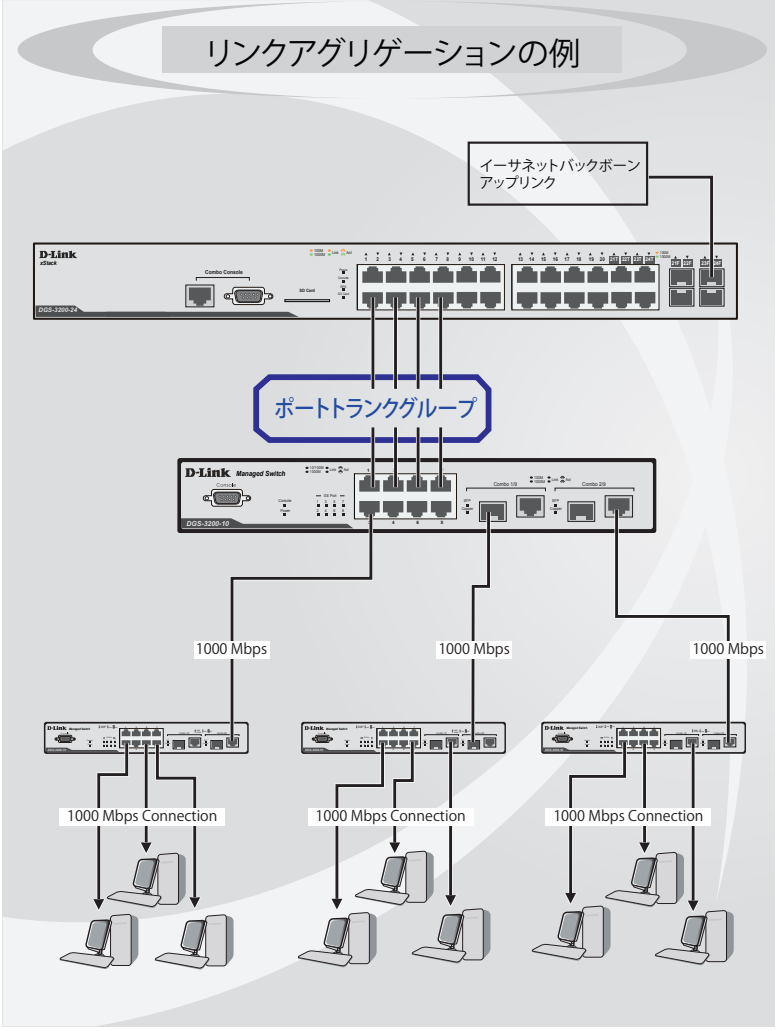


図 7-19　ポートトランクグループの例

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。

DGS-3200 スイッチシリーズは、以下のリンクアグリゲーショングループをサポートしています。
- DGS-3200-10 では、2 から 8 のリンク (ポート) で構成する最大 5 個のリンクアグリゲーショングループをサポートします。
- DGS-3200-16/GE では、2 から 8 のリンク (ポート) で構成する最大 8 個のリンクアグリゲーショングループをサポートします。
- DGS-3200-24/GE では、2 から 8 のリンク (ポート) で構成する最大 12 個のリンクアグリゲーショングループをサポートします。

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

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

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

スパニングツリープロトコル（STP）は、スイッチレベルにおいて、リンクアグリゲーショングループを 1 つのリンクとしてとらえます。STP に関しては、リンクアグリゲーショングループのパスコストは、リンクアグリゲーショングループのアクティブなポート番号によって決定されます。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。

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

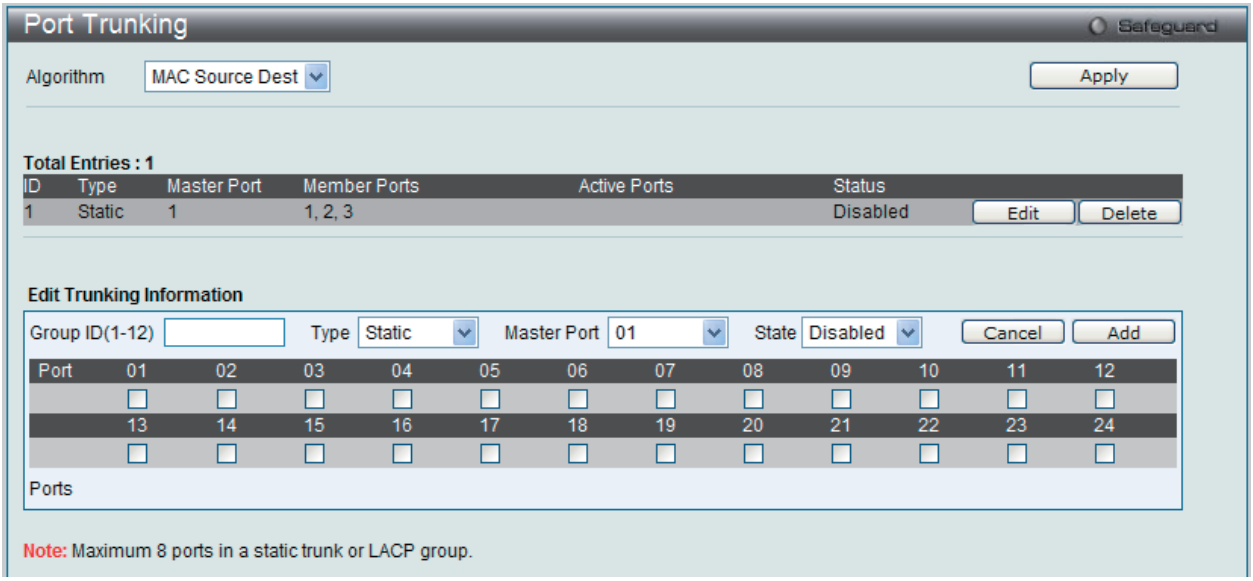


図 7-20　Trunking 画面

ポートトランキンググループの設定
画面下部にある「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
画面上部で編集するグループの「Edit」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
ポートトランキンググループを削除するためには、画面上部で削除するグループの「Delete」ボタンをクリックします。

本画面には次の項目があります。

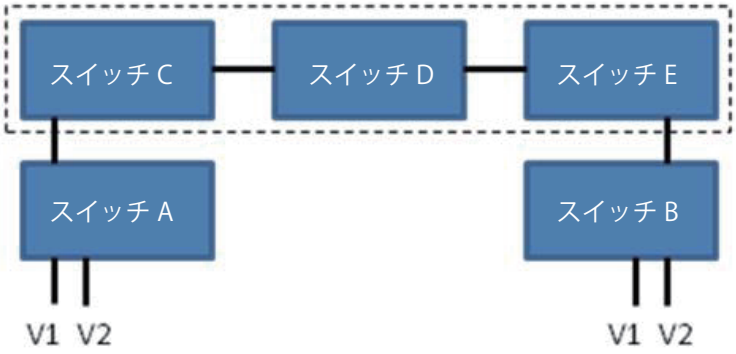
項目	説明
Algorithm	「MAC Source Dest」と「IP Source Dest」を切り替えます。
Edit Trunking Information	
Group ID (1-5)	グループ番号は、DGS-3200-10 には 1-5 と、DGS-3200-16/GE には 1-8、DGS-3200-24/GE には 1-12 を指定します。
Type	トランキンググループの種類を設定します。 • Static - スタティックです。 • LACP - ポートトランキンググループのリンクを自動的に検出します。
Master Port	トランキンググループのマスタポートを選択します。
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、これは診断、迅速に帯域が集中するネットワークデバイスの迅速な分離、または自動制御下にない独立したバックアップアグリゲーショングループを持つ場合に有益です。
Member Ports	トランキンググループのメンバポートを選択します。グループには 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。

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。

VLAN Trunk Settings（VLAN トランク設定）

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

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



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

L2 Features > VLAN 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。

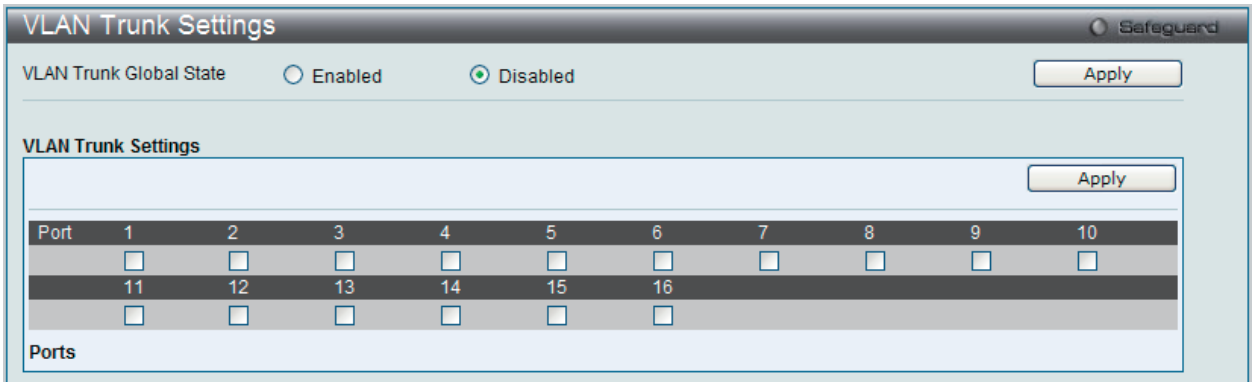


図 7-21　VLAN Trunk Settings 画面

本画面には次の項目があります。

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

スイッチに VLAN トランクポートを設定するためには、設定するポートを指定し、ステータスを「Enabled」に変更して「Apply」ボタンをクリックします。新しい設定が画面下の「Vlan Trunk Port Settings Table」に表示されます。

LACP Port Settings（LACP の設定）

「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 > 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 7-22　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
From Port	設定の対象となるポートの最初の番号を設定します。
To Port	設定の対象となるポートの最後の番号を設定します。
Mode	• 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。

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、１つのポートまたはポートグループから、スイッチのポートグループへ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を行うこの方法は、VLAN によるトラフィック制限に似ていますが、さらに限定的であると言えます。

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

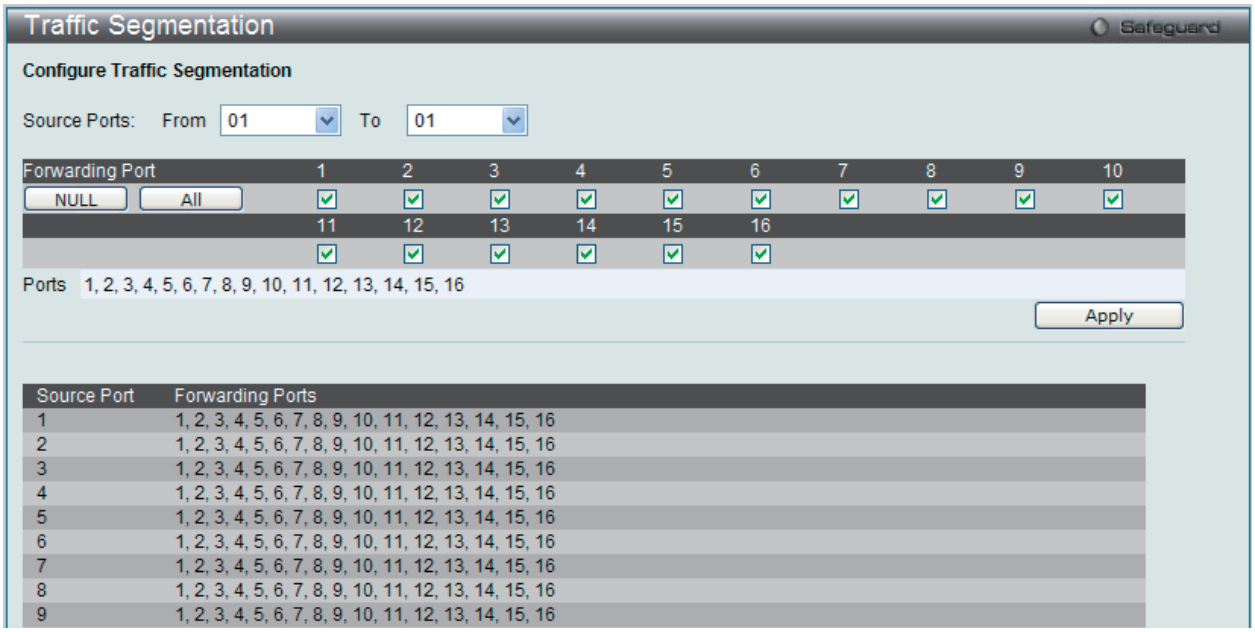


図 7-23　Traffic Segmentation 画面

スイッチにトラフィックセグメンテーションを設定するためには、はじめに本画面上部の「From」と「To」のプルダウンメニューを使用して「Source Ports」を指定します。次に、指定したポートからパケットを受信できるポートを指定します。
「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。

IGMP Snooping（IGMP Snooping の設定）

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

IGMP Snooping Settings（IGMP Snooping グローバル設定）

IGMP Snooping のグローバル設定を行います。

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

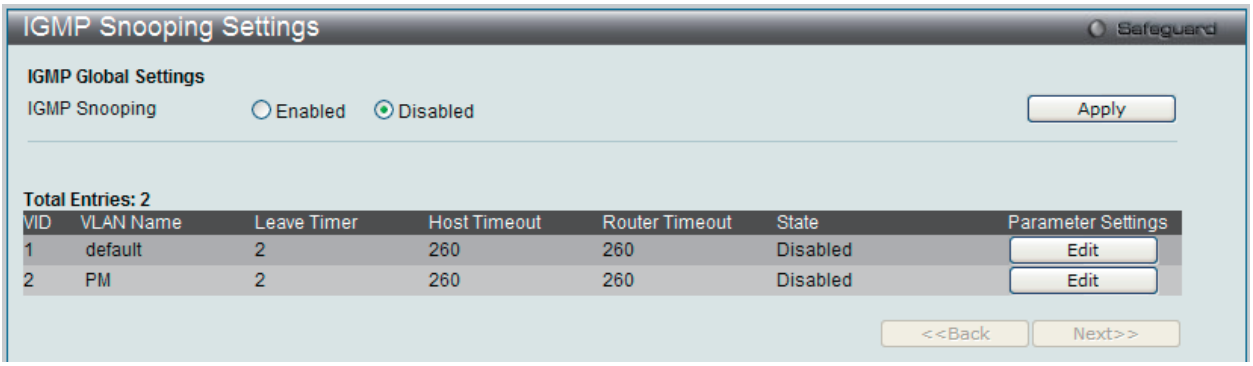


図 7-24　IGMP Snooping Settings 画面

IGMP Snooping 機能の利用

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。

1. 「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 Settings」画面では以下のパラメータを参照できます。

項目	説明
IGMP Snooping	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）
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。
Leave Timer	スイッチがホストから leave group message を受信してから group membership query を発行するまでの最大時間（秒）。本タイマ時間が経過するまでに membership クエリへの response が受信されない場合、そのホストに対する（マルチキャスト）フォワーディングエントリは削除されます。初期値は 2（秒）です。
Host Timeout	スイッチが Host membership report を受け取らない場合に、ホストがマルチキャストグループのメンバである最大時間（秒）。初期値は 260（秒）です。
Router Timeout	スイッチが Host membership report を受信しない時に経路がフォワーディングテーブルに保持される最大時間（秒）。初期値は 260（秒）です。
State	IGMP Snooping を使用するためには、「Enabled」（有効）を指定します。初期値は「Disabled」（無効）です。
Parameter Settings	IGMP Snooping 項目を編集する VLAN に隣接する「Edit」ボタンをクリックします。

IGMP Snooping 機能の詳細設定

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

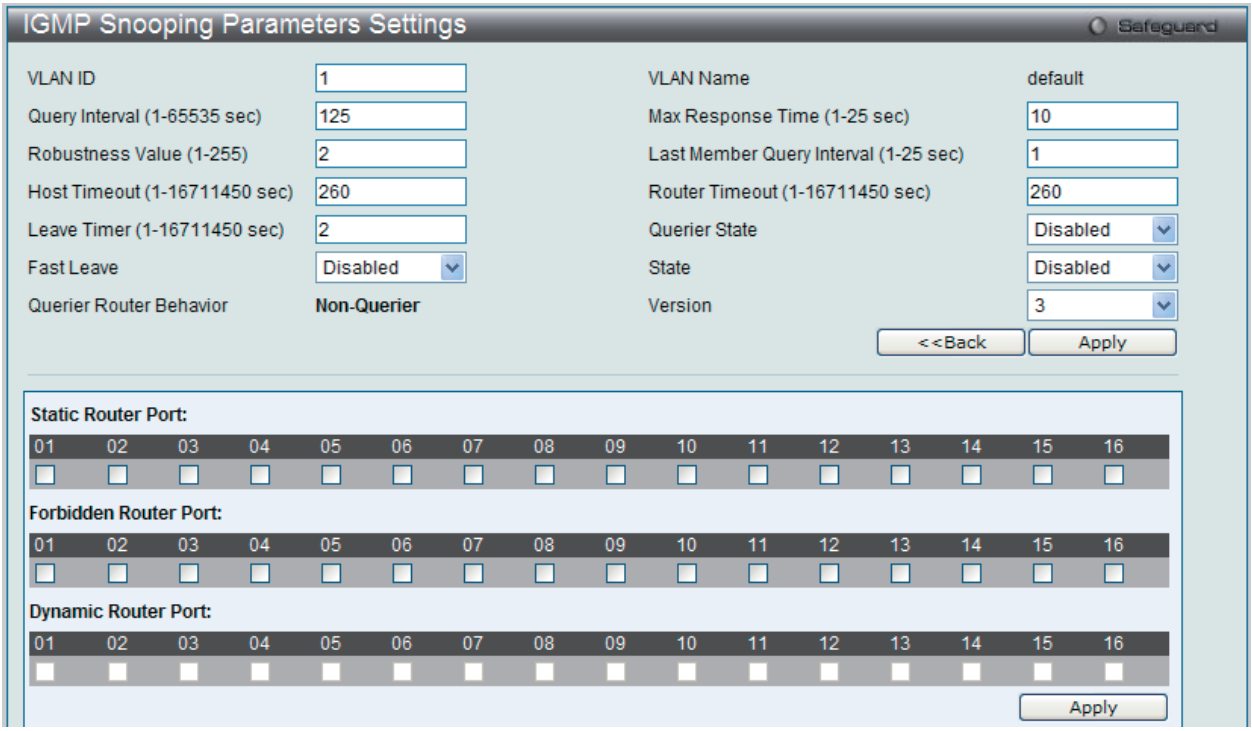


図 7-25　IGMP Snooping Parameter Settings 画面

「IGMP Snooping Parameters Settings」画面は 2 つのセクションに分かれています。画面の上半分で以下の項目を参照または編集することができます。

項目	説明
VLAN ID	VLAN 名と共に、IGMP Snooping 設定の対象となる VLAN を識別するために使用する ID です。
VLAN Name	VLAN ID と共に、IGMP Snooping 設定を行う対象の VLAN を識別します。
Query Interval (1-65535 sec)	IGMP クエリを送信する間隔を指定します。初期値は 125 です。
Max Response Time (1-25 sec)	IGMP response report を送信するまでの最大時間 (秒)。初期値は 10 です。
Robustness Variable (1-255)	サブネットワークで失われる多くのパケットを許容する調整の変数として使用します。1-255 で指定します。ご使用のサブネットワークで多くのパケットが失われると予想される場合、高い値を指定します。初期値は 2 です。
Last Member Query Interval (1-25 Sec)	Leave Group メッセージへの応答として送信するメッセージを含む Group-Specific Membership Query メッセージ間の最大値を設定します。初期値は 2 です。
Host Timeout (1-16711450 sec)	スイッチが Host membership report を受信しない場合に、ホストがマルチキャストグループのメンバのままとなります。初期値は 260 です。
Router Timeout（1-16711450 sec)	ダイナミックに学習されたルータポートにタイムアウトを指定します。初期値は 260 です。
Leave Timer (1-16711450 sec)	スイッチがホストから leave group message を受け取ってから、group membership query を発行するまでの最大時間 (秒)。本タイマ時間の経過前に membership query への応答を受信しないと、そのホストへの (マルチキャスト) フォワーディングエントリが削除されます。初期値は 2 です。
Querier State	「Enabled」を選択し、IGMP Query パケットの伝送を有効にします。または、「Disabled」を選択し、IGMP Query パケットの伝送を無効にします。初期値は「Disabled」です。
Fast Leave	「Enabled」または「Disabled」を選択し、Fast Leave 機能を有効または無効にします。初期値は「Disabled」です。本機能を Enable(有効) にした場合、IGMP leave をスイッチが受信するとすぐにメンバは削除されます。
State	指定した VLAN への IGMP Snooping 機能を「Enabled」(有効)/「Disabled」(無効) にします。
Querier Router Behavior	現在の Querier 状態を表示します。
Version	指定ポートによって送信される IGMP パケットのバージョンを指定します。インタフェースが受信した IGMP パケットが指定のバージョン以降のバージョンを持つ場合、パケットは破棄されます。

上記項目設定後、画面上にあるセクション内の「Apply」ボタンをクリックして変更を有効にします。

画面下半分にある以下の項目を表示または編集します。

項目	説明
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。

上記項目設定後、画面下にあるセクション内の「Apply」ボタンをクリックして変更を有効にします。

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

Data Driven Learning Settings（Data Driven Learning 設定）

IGMP 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、IGMP Snooping グループが作成されます。エントリの学習は IGMP 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 IGMP Snooping エントリのために、IGMP 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、IGMP メンバポートが後で学習されると、エントリは、通常の IGMP 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、IGMP 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。

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

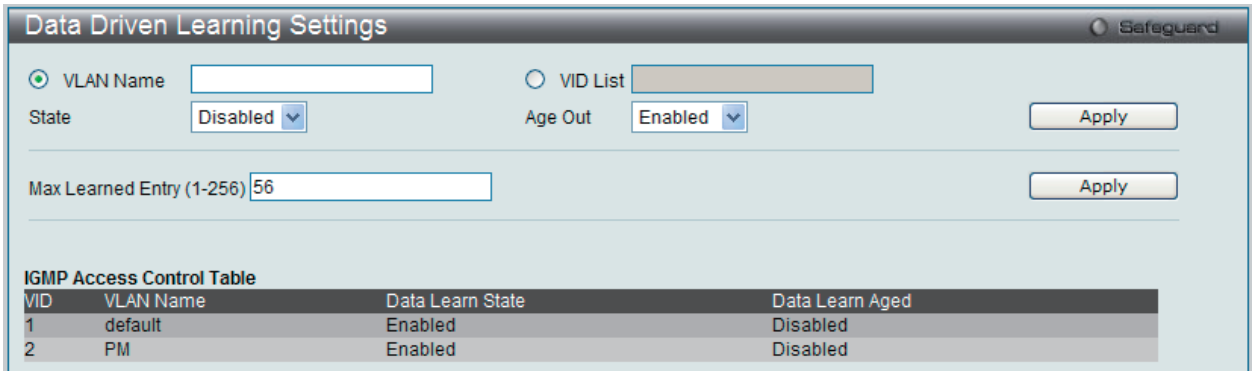


図 7-26　Date Driven Learning Settings 画面

「Data Driven Learning Settings」画面は 3 つの主要なセクションに分かれています。一番上のセクションでは VLAN を Data Driven Learning を使用するように設定し、中央のセクションでは学習するエントリの最大数を設定し、一番下のセクションでは既存の Data Driven Learning 設定のサマリを表示します。

Data Driven Learning を使用するための VLAN 設定

以下で記述するように画面上のセクションに項目を設定します。

項目	説明
VLAN Name	選択後、設定する VLAN を入力します。
VID List	選択後、設定する VID リストを入力します。
State	IGMP Snooping グループの Data Driven Learning を有効または無効にします。
Age Out	本エントリのエージングを有効または無効にします。
Max Learned Entry (1-256)	Data Driven 方式が学習するグループの最大エントリ数を指定します。初期値は 56 エントリです。

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。

学習するエントリの最大数の設定

以下で記述するように画面中央のセクションに項目を設定します。

項目	説明
Max Learned Entry (1-256)	選択後、設定する VLAN を入力します。

隣接する「Apply」ボタンをクリックし、新しい設定適用します。

ISM VLAN Settings（ISM VLAN 設定）

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。

L2 Features > IGMP Snooping > ISM 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。

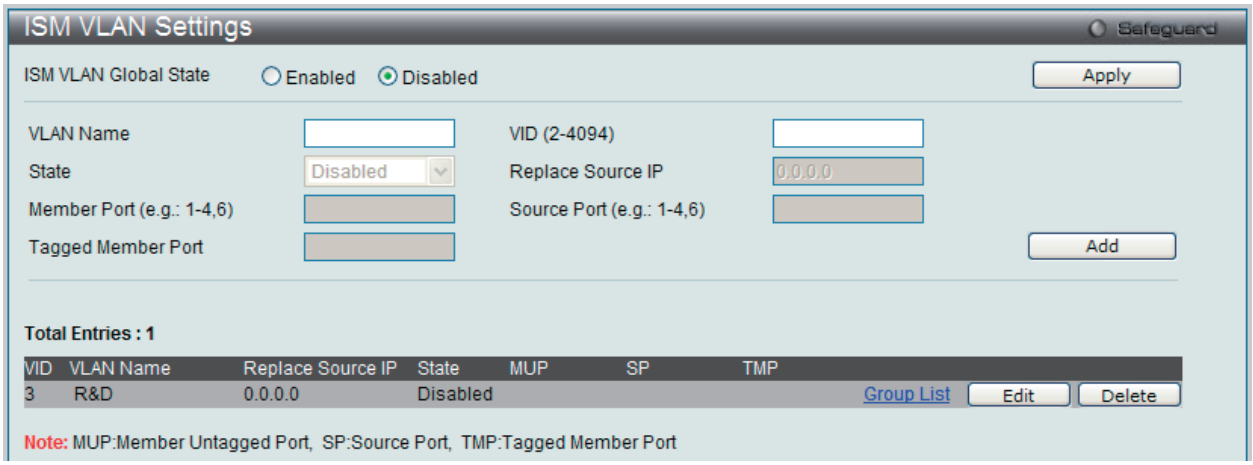


図 7-27　ISM VLAN Settings 画面

マルチキャスト VLAN の登録

1. 「ISM VLAN Global 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追加します。

以下の項目を使用して、設定します。

項目	説明
ISM VLAN Global State	IGMP Snooping Multicast（ISM）VLAN のグローバルな状態を有効または無効にします。
VLAN Name	作成するマルチキャスト VLAN 名（半角英数字 32 文字以内）を入力します。「Modify」画面では定義済みのマルチキャスト VLAN 名を表示します。
VID (2-4094)	マルチキャスト VLAN に対応する VLAN ID を追加または編集します。2-4094 の値を指定します。
State	マルチキャスト VLAN の「Enabled」（有効）、「Disabled」（無効）を設定します。
Tagged Member Port	マルチキャスト VLAN のタグ付きメンバとするポートまたはポートリストを入力します。
Member Ports (e.g.: 1-4,6)	マルチキャスト VLAN に追加するポートリストを入力します。メンバポートはマルチキャスト VLAN のタグなしメンバになります。
Source Ports	マルチキャスト VLAN に追加するポートリストを入力します。送信元ポートはマルチキャスト VLAN のタグ付きメンバになります。
Replace Source IP (e.g.: 1-4,6)	アップリンクサーバに接続する ISM VLAN のソースポートの置換を指定します。本項目は、転送する前にホストが送信した入力パケットの送信元 IP アドレスを送信先ポートに変更します。

マルチキャスト VLAN の変更

1. 画面下部のテーブルで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。

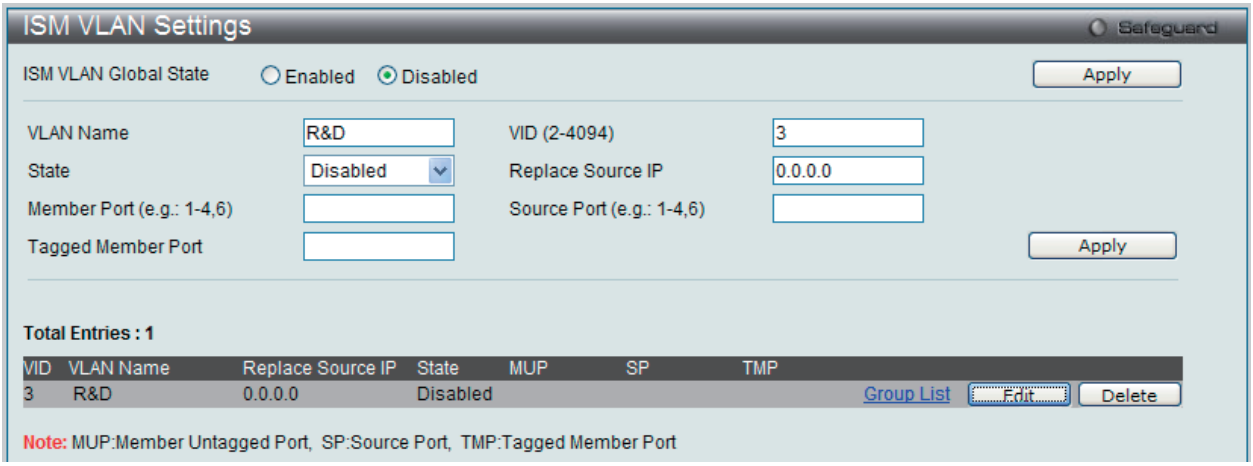


図 7-28　ISM VLAN Settings 画面 - Edit

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. エントリの「Group List」のリンクをクリックし、以下の画面を表示します。

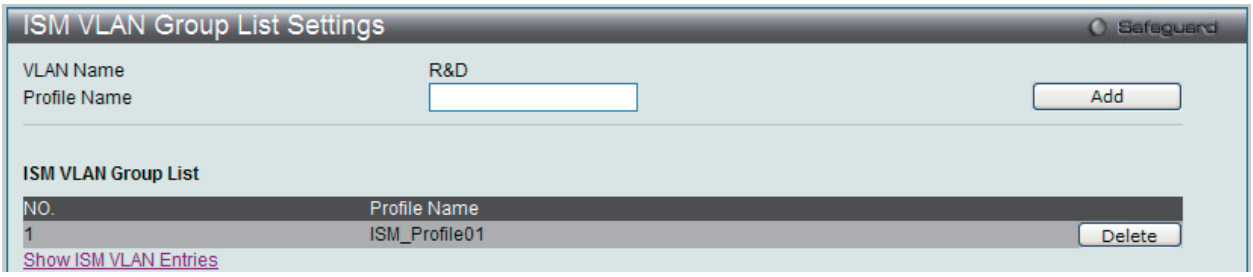


図 7-29　ISM VLAN Group List Settings 画面

2. 「ISM Profile Settings」画面で設定した「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. ISM VLAN グループリストを削除する場合は、該当する行の「Delete」ボタンをクリックします。

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

ISM Profile Settings（ISM プロファイル設定）

マルチキャスト VLAN のプロファイル設定を行います。

L2 Features > IGMP Snooping > ISM 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。

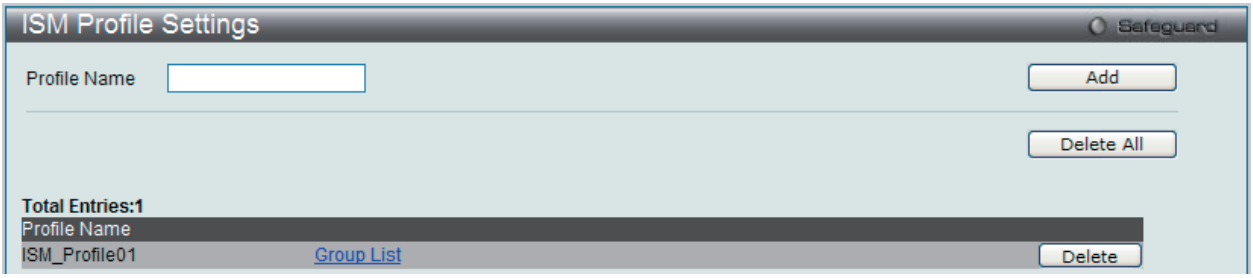


図 7-30　ISM Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile Name	マルチキャスト VLAN のプロファイル名（半角 32 文字以内）を入力します。

エントリの追加

「Add」ボタンをクリックし、プロファイルを追加します。

エントリの削除

削除するプロファイル名の「Delete」ボタンをクリックします。「Delete All」ボタンをクリックすると、すべてのプロファイルを削除します。

プロファイルへのマルチキャストアドレスエントリの追加

1. 「ISM Profile Settings」画面で該当するプロファイル名の「Group List」リンクをクリックし、以下の画面を表示します。

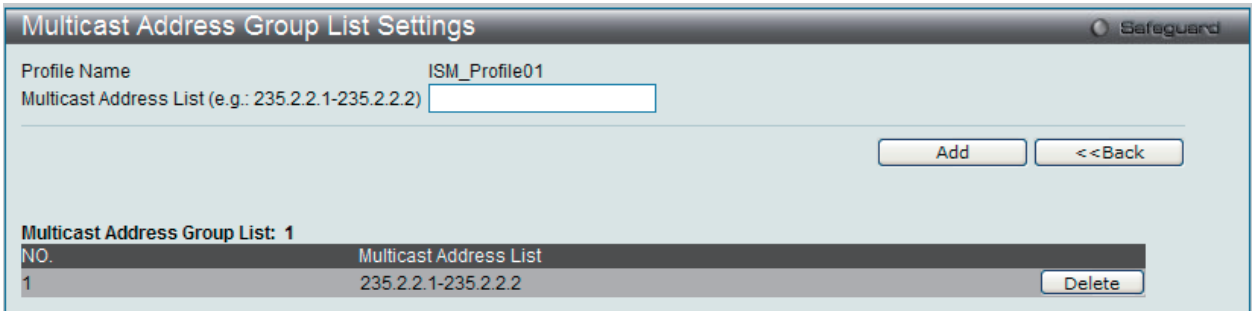


図 7-31　Multicast Address Group List Settings 画面

2. プロファイルに関連付けるマルチキャストアドレスリストを指定し、「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

1. 「Multicast Address Group List」テーブルの該当する行の「Delete」ボタンをクリックします。

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

IP Multicast Profile Settings（IP マルチキャストプロファイル設定）

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）IP アドレス /IP アドレス範囲を設定することができます。

IP Multicast Profile 設定を行うには、**L2 Features > IGMP Snooping > IP Multicast Profile Settings** をクリックします。

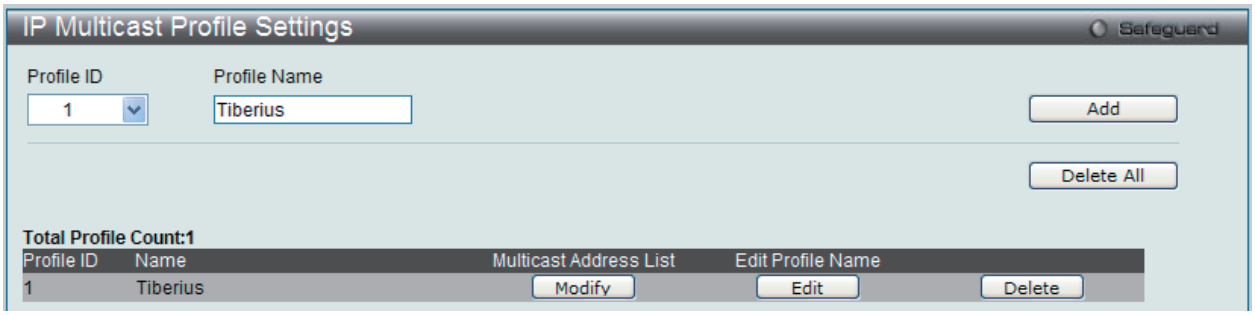


図 7-32　IP Multicast Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile ID	1-24 の Profile ID を指定します。
Profile Name	IP マルチキャストプロファイル名を入力します。

エントリ名の変更

「Edit Profile Name」欄の対応する「Edit」ボタンをクリックし、以下の画面を表示します。

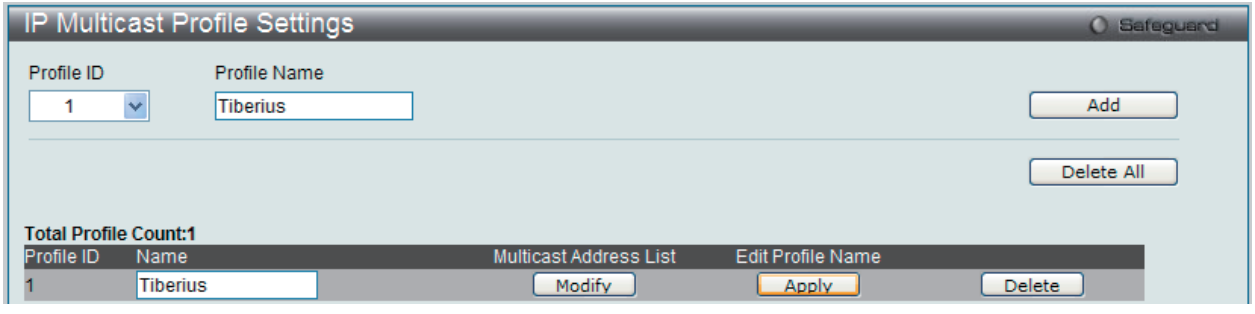


図 7-33　IP Multicast Profile Settings 画面 - エントリ名の変更

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。

エントリの変更

1. 「Multicast Address List」欄の対応する「Modify」ボタンをクリックし、以下の画面を表示します。

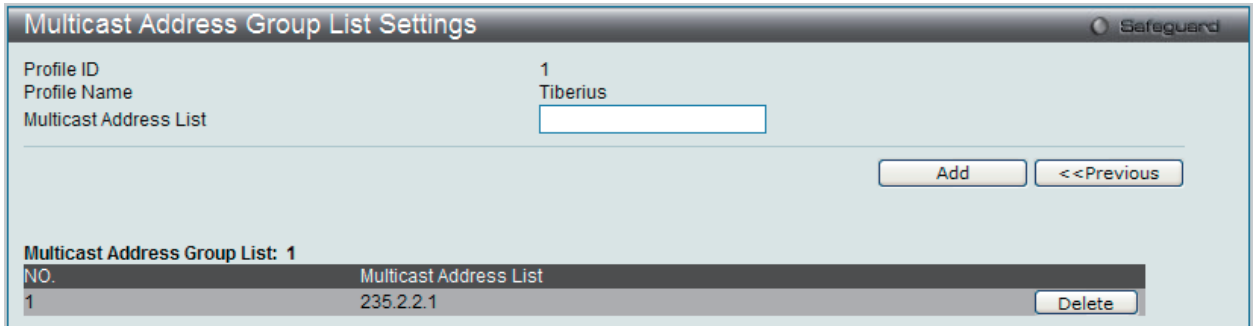


図 7-34　Multicast Address Group List Settings 画面

2. 「Multicast Address Group List」で範囲内の最も小さい開始アドレスを入力し、「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。

「IP Multicast Profile Settings」画面に戻るには、「<<Previous」ボタンをクリックします。

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

ここでは、「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 > IGMP Snooping > Limited Multicast Address 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。

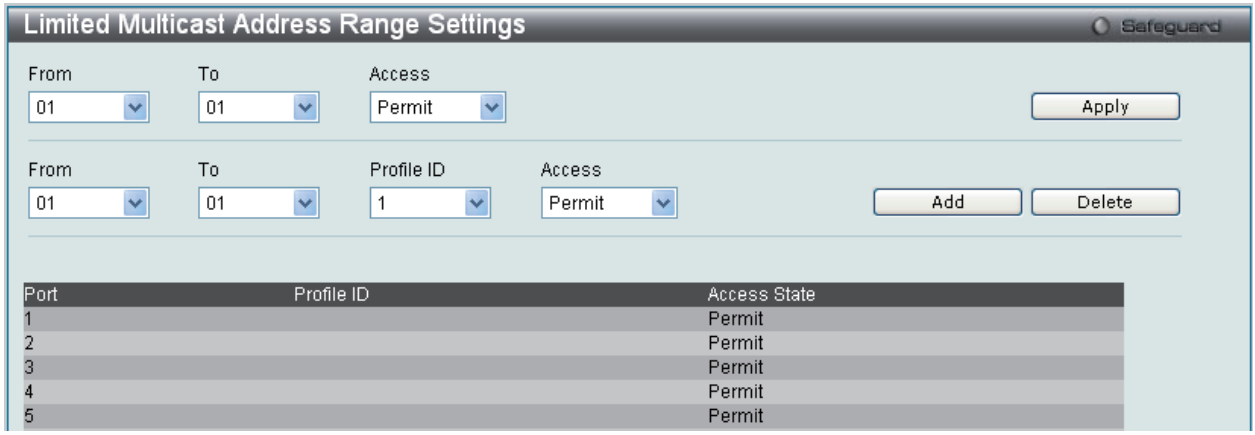


図 7-35　Limited Multicast Address Range Settings 画面

以下の項目を指定してポートにマルチキャストアドレスフィルタリング機能を設定します。

項目	説明
From/To	プルダウンメニューを使用して、マルチキャストアドレスフィルタ機能を追加または削除するポート範囲を指定します。
Access	プルダウンメニューを使用して、以下のオプションの一つを選択します。 • Permit -「From/To」プルダウンメニューで指定したポートに一致するパケットを許可することを指定します。 • Deny -「From/To」プルダウンメニューで指定したポートに一致するパケットを破棄することを指定します。

「Apply」ボタンをクリックし、設定を適用します。

以下の通り、画面中央にある項目を設定し、指定のプロファイルのポートにマルチキャストアドレスフィルタリング機能を設定します。

項目	説明
From/To	プルダウンメニューを使用して、マルチキャストアドレスフィルタ機能を追加または削除するポート範囲を指定します。
Profile ID	プルダウンメニューを使用して、指定したポート範囲に (から) 追加または削除するプロファイル ID を選択します。
Access	プルダウンメニューを使用して、以下のオプションの一つを選択します • Permit - プロファイル内に指定されているアドレスに一致するパケットを許可することを指定します。 • Deny - プロファイル内に指定されているアドレスに一致するパケットを破棄することを指定します。

新しいマルチキャストアドレス範囲の追加

適切な情報を入力し、「Add」ボタンをクリックします。

マルチキャストアドレス範囲の削除

情報を入力し、「Delete」ボタンをクリックします。

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

ここでは、最大のフィルタグループ（最大 256 まで）に所属するスイッチポートを設定します。

これらの設定を行うには、**L2 Features > IGMP Snooping > Max Multicast Group Settings** の順にメニューをクリックします。

図 7-36　Max Multicast Group Settings 画面

エントリを追加するためには、適切な情報を入力し「Apply」ボタンをクリックします。

MLD Snooping Settings（MLD Snooping 設定）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じように使用される IPv6 機能です。マルチキャストデータを要求する VLAN に接続しているポートを検出するために使用されます。選択した VLAN 上のすべてのポートにマルチキャストトラフィックが流れる替わりに、MLD Snooping は、リクエストポートとマルチキャストの送信元によって生成する MLD クエリと MLD レポートを使用してデータを受信したいポートにのみマルチキャストデータを転送します。
MLD Snooping は、エンドノードと MLD ルータ間で交換される MLD コントロールパケットのレイヤ 3 部分を調査することで実行されます。ルータがマルチキャストトラフィックをリクエストしていることをスイッチが検出すると、該当ポートを IPv6 マルチキャストテーブルに直接追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のこのエントリは該当ポート、その VLAN ID、および関連する IPv6 マルチキャストグループアドレスを記録し、このポートをアクティブな Listening ポートと見なします。アクティブな Listening ポートはマルチキャストグループデータの受信だけをします。

MLD コントロールメッセージ

MLD Snooping 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、132 および 143 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 Version1 – IGMPv2 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。
3. Multicast Listener Done – IGMPv2 の Leave Group Message と類似のものです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからマルチキャストデータを受信せず、このアドレスからのマルチキャストデータとともに”done”（完了）した旨を伝えます。スイッチは本メッセージを受信すると、この Listening ポートには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しません。
4. Multicast Listener Report 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。

MLD Snooping 設定

MLD Snooping を設定するためには **L2 Features > MLD Snooping Settings** とクリックし、以下の画面を表示します。

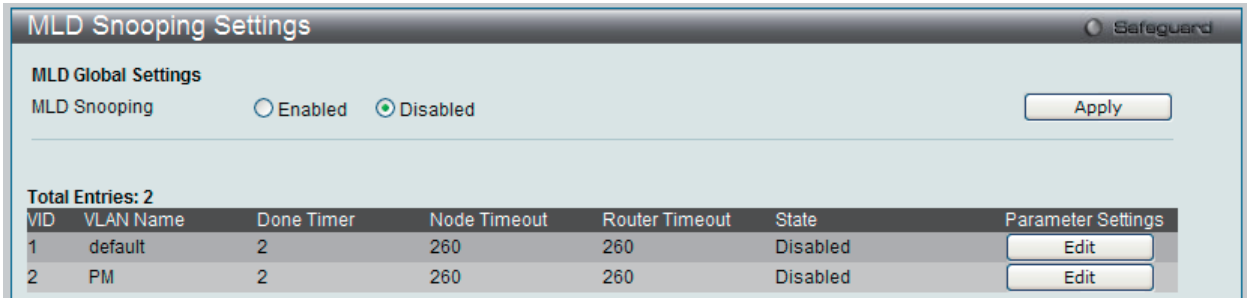


図 7-37　MLD Snooping Settings 画面

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

以下の項目を参照または変更できます。

項目	説明
MLD Snooping	MLD Snooping を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
VID	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。
Done Timer	node listener report なしでマルチキャストグループから done メッセージを受信後、ルータがスイッチ内に保持される最大の時間（秒）を設定します。1-16711450 で設定でき、初期値は 2（秒）です。
Node Timeout	リンクノードのタイムアウト（秒）を指定します。この時間に達すると、このノードはリスニングノードとして見なされません。1 から 16711450 で設定でき、初期値は 260（秒）です。
Router Timeout	node listener report なしでマルチキャストグループのリスニングノードとしてスイッチのルーティングテーブルに保持される最大の時間（秒）を設定します。1-16711450 で設定でき、初期値は 260（秒）です。
State	指定の VLAN に対して MLD Snooping の有効 / 無効を表示します。

「Apply」ボタンをクリックし、変更を有効にします。

MLD Snooping に特定の VLAN を設定する

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

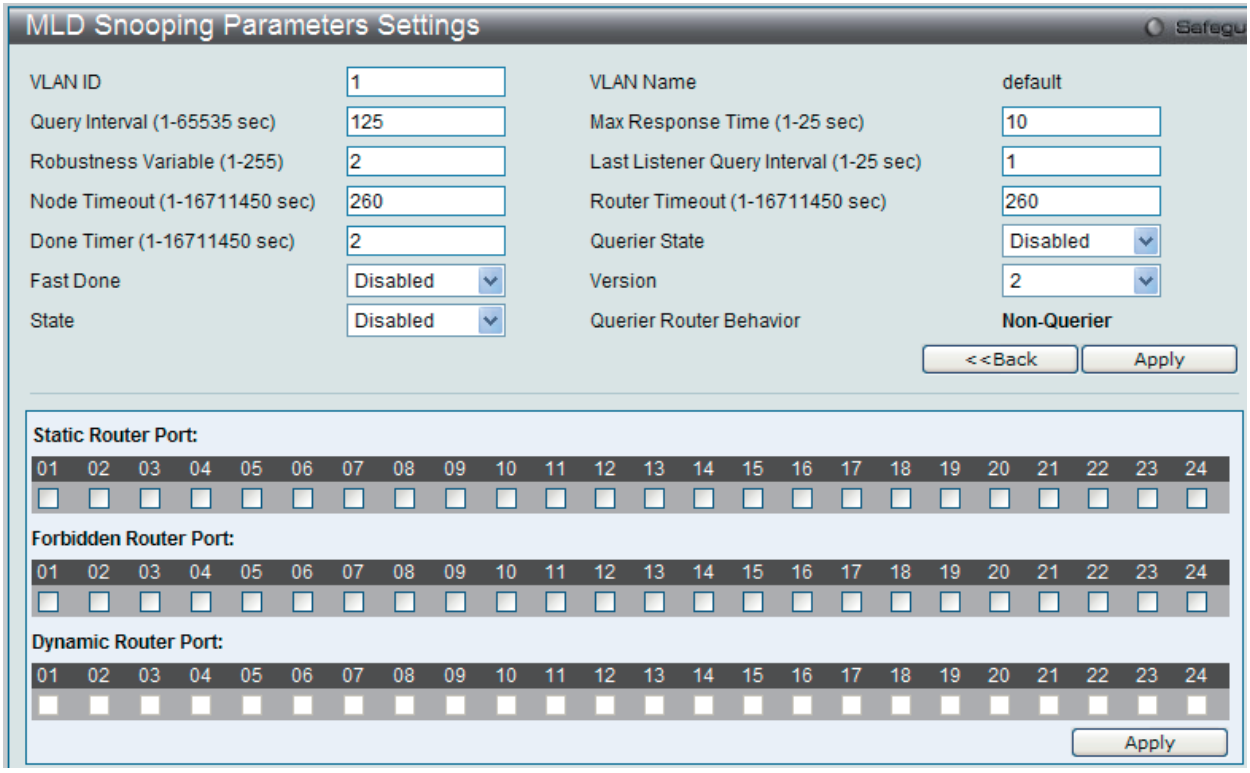


図 7-38　MLD Snooping Parameters Settings 画面

以下の項目を設定します。

項目	説明
VLAN ID	VLAN 名と共に、MLD Snooping 設定の編集を行う VLAN を識別するために使用する ID です。
VLAN Name	VLAN ID と共に、IGMP Snooping 設定の編集を行う VLAN を識別するために使用する名称です。
Query Interval (1-65535 sec)	一般的なクエリア送信間隔 (秒) を指定します。初期値は 125(秒) です。
Max Response Time (1-25 sec)	Listener からのレポートを待つ最大時間 (秒) で指定します。初期値は 10(秒) です。
Robustness Variable (1-255)	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。サブネットが多くのパケットを失ったと予想する場合には、この値を増やしたくなるかもしれません。
Last Listener Query Interval (1-25 Sec)	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。
Node Timeout (1-16711450 sec)	リンクノードのタイムアウト（秒）を指定します。この時間に達すると、このノードはリスニングノードとして見なされません。初期値は 200（秒）です。
Router Timeout (1-16711450 sec)	ノードリスナーレポートの受信なしでマルチキャストグループのリスニングノードとしてスイッチに保持される最大の時間（秒）で設定します。初期値は 200（秒）です。
Done Timer (1-16711450 sec)	「node listener」レポートを受信せずにグループから「done」メッセージを受信後、グループがスイッチ内に保持される最大の時間を設定します。初期値は 2（秒）です。
Querier State	• Enabled - スイッチは MLD Querier として動作します。MLD クエリパケットを送信します。 • Disabled - スイッチは Non-Querier として動作します。MLD クエリパケットは送信しません。
Fast Done	指定した VLAN が MLD Snooping Fast Done 機能を「Enabled」（有効）または「Disabled」（無効）とするかを指定します。本機能を Enable（有効）にすると、done メッセージをシステムが受信した際にメンバは直ちにグループから削除されます。
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。
State	指定した VLAN からの MLD Snooping 機能を「Enabled」(有効)/「Disabled」(無効) にします。
Querier Router Behavior	スイッチに設定された MLD Querier または Non-Querier 機能を表示します。

上記項目設定後、画面上にあるセクション内の「Apply」ボタンをクリックして変更を有効にします。

画面下半分にある以下の項目を表示または編集します。

項目	説明
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。

上記項目設定後、画面下にあるセクション内の「Apply」ボタンをクリックして変更を有効にします。

「<<Back」ボタンをクリックすると、「MLD Snooping Settings」画面に戻ります。

Port Mirroring（ポートミラーリングの設定）

本スイッチはポート上で送受信したフレームをコピーし、別のポートに転送します。スニファーやRMON probeのようなモニタデバイスをミラーポートに接続し、最初のポートを通過するパケット情報を参照できます。ネットワーク監視とトラブルシューティングの目的で使用します。

ポートミラーリングの設定を行うには、**L2 Features > Port Mirroring** の順にメニューをクリックし、以下の画面を表示します。

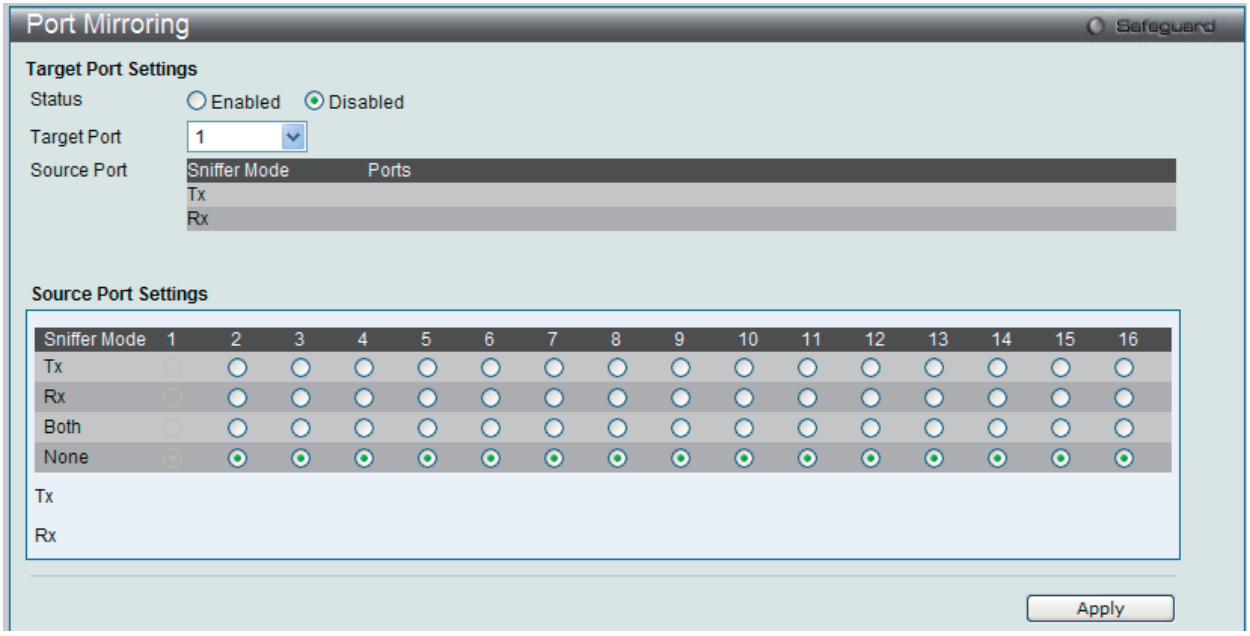


図 7-39　Port Mirroring 画面

ミラーポートの設定手順：

1. 「Target Port Setting」セクションの「Status」の「Enabled」（有効）を選択します。
2. フレームのコピーを行う対象の「Source port」（ソースポート）と、ソースポートからフレームのコピーを受信する「Target Port」（ターゲット）を選択します。
3. コピーを行うフレームの方向（入力：Tx、出力：Rx、両方：Both、なし：None）を選択します。
4. 設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 転送速度の速いポートを遅いポートにミラーリングはできません。例えば、100Mbps ポートからのトラフィックを 10Mbps ポートにミラーリングしようとすると、スループットの問題が起こります。ソースポートの速度はターゲットポートと同じかそれ以下としてください。

注意 また、ターゲットポートはトランクグループに属することはできません。設定をしようとするとエラーメッセージが表示され、設定は無効になります。ターゲットポートとソースポートを同じポートにはできませんのでご注意ください。

本画面には次の項目があります。

項目	説明
Target Port Setting	
Status	ターゲットポートを「Enabled」（有効）/Disabled（無効）に設定します。初期値は「Disabled」です。
Target Port	ターゲットポートを設定します。
Source Port	ソースデータの方向とソースポートを表示します。
Source Port Setting	
Tx	ポートから送信されるデータをモニタします。
Rx	ポートで受信するデータをモニタします。
Both	ポートで送受信するデータ両方をモニタします。
None	ポートのデータはモニタしません。

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、ポートは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。

L2 Features > 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。

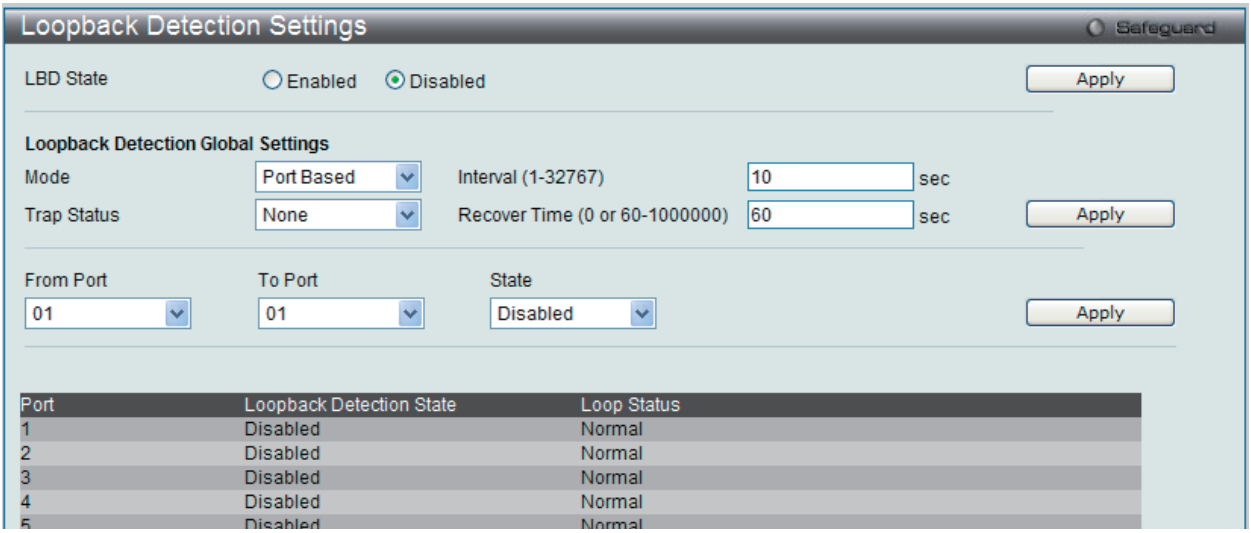


図 7-40　Loopback Detection Settings - ポートベース画面

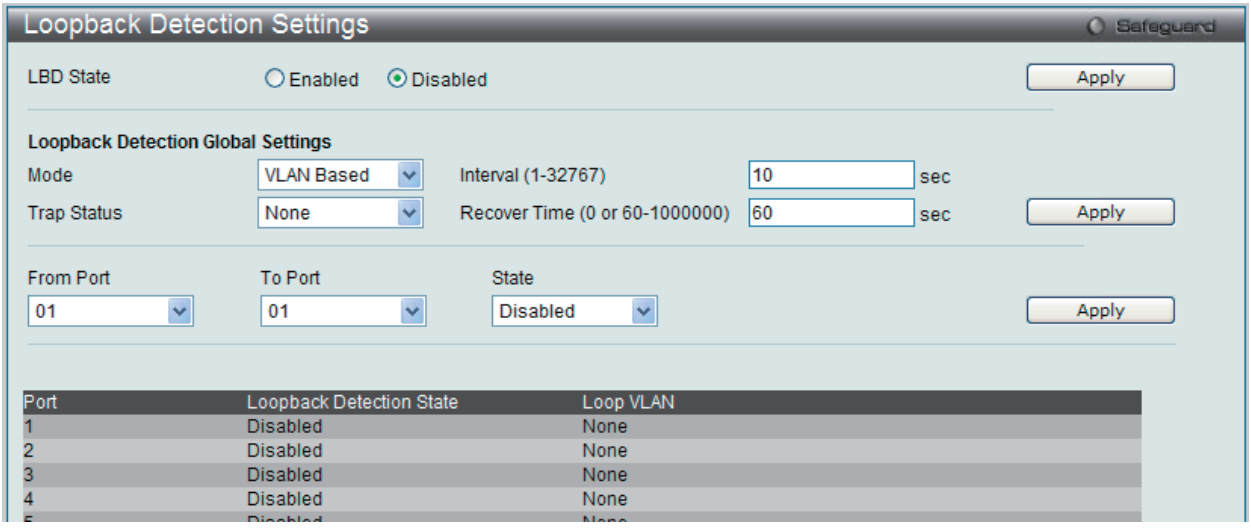


図 7-41　Loopback Detection Settings - VLAN ベース画面

項目	説明
LBD Status	プルダウンメニューで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。
Loopdetect Interval (1-32767)	ループ検知間隔を設定します。（1-32767 秒）
Loopdetect Recover Time (0 or 60-1000000)	ループが検知された場合にリカバリする時間（秒）を指定します。指定時間に到達すると、スイッチはループをチェックします。ループが検知されないと、ポートが再度有効になります。0 または 60-1000000（秒）に設定します。0 を指定すると、Loopdetect Recover Time は無効になります。初期値は 60（秒）です。
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	プルダウンメニューで「Enabled」（有効）または「Disabled」（無効）を指定します。

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

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。

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

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

1. 32 文字までの半角英数字で定義された「Configuration 名」。「MST Configuration Identification」画面中の「Configuration Name」で設定します。
2. 「Configuration Revision 番号」（「MST Configuration Identification」画面内の「Revision Level」）。
3. 4096 エレメントテーブル（「MST Configuration Identification」画面内の「VID List」）。スイッチがサポートする 4096 件までの VLAN とインスタンスとの関連付けです。

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

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

802.1D-2004 Rapid Spanning Tree

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

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

ポートの状態遷移

3 つのプロトコル間の根本的な相違は、ポートがフォワーディング状態に遷移する方法と、この遷移とトポロジの中でのポートの役割（Forwarding/Not Forwarding）の関連性にあります。MSTP と RSTP では、802.1D-1998 で使用されていた 3 つの状態、「Disabled」、「Blocking」、「Listening」が、「Discarding」という 1 つの状態に統合されました。どちらのケースにおいてもポートはパケットの送信を行わない状態です。STP の「Disabled」、「Blocking」、「Listening」であっても RSTP/MSTP の「Discarding」であっても、ネットワークトポロジ中では「アクティブではない状態」であり、機能の差はありません。表 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 準拠のブリッジリンクからのフィードバックに反応するようになりました。ポートは、フォワーディング状態の遷移の間トポロジが安定するまで待つ必要がなくなりました。この急速な遷移を実現するために、RSTP プロトコルでは以下の 2 つの新しい変数（Edge Port と P2P Port）が使用されます。

Edge Port

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

P2P Port

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

802.1D-1998/802.1D-2004/802.1Q-2005 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。
「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。

図 7-42　STP Bridge Global Settings 画面 : RSTP（初期値）

図 7-43　STP Bridge Global Settings 画面 : MSTP

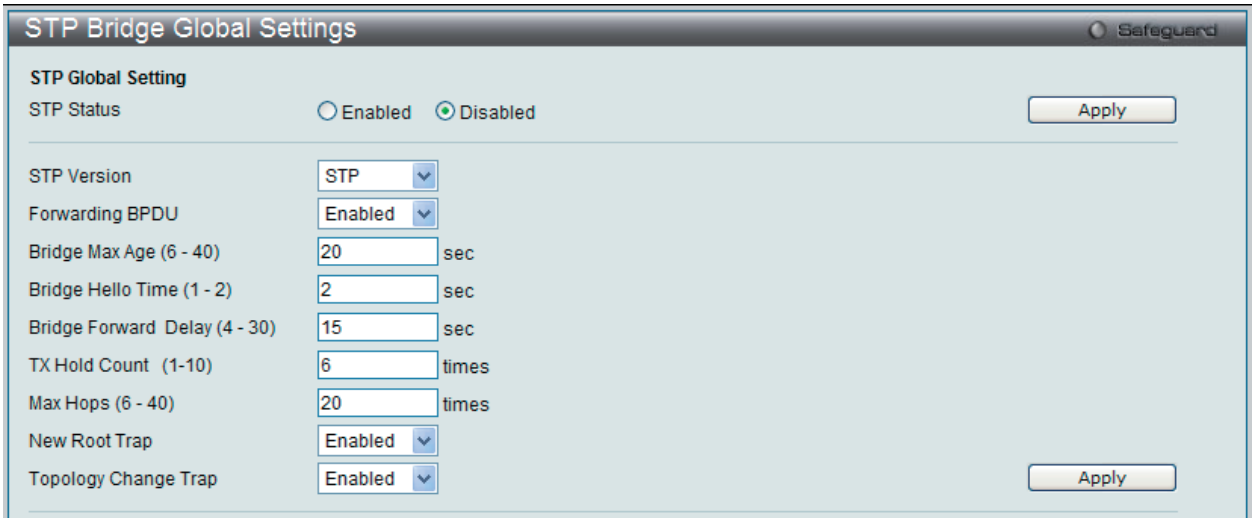


図 7-44　STP Bridge Global Settings 画面 : STP 互換

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 Status	STP をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
STP Version	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。 • MSTP - スイッチ上で MSTP がグローバルに使用されます。
Forwarding BPDU	「Enabled」（有効）または「Disabled」（無効）にします。「Enabled」にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は「Enabled」です。
Bridge Max Age (6-40)	本項目は、古い情報がネットワーク内の冗長パスを永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40（秒）の範囲から値を指定します。初期値では 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「STPVersion」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。
New Root Trap	新しいルートトラップの送信を有効または無効にします。初期値は「Enabled」です。
Topology Change Trap	トポロジチェンジトラップの送信を有効または無効にします。初期値は「Enabled」です。

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

STP Port Settings（STP ポートの設定）

STP をポートごとに設定します。

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

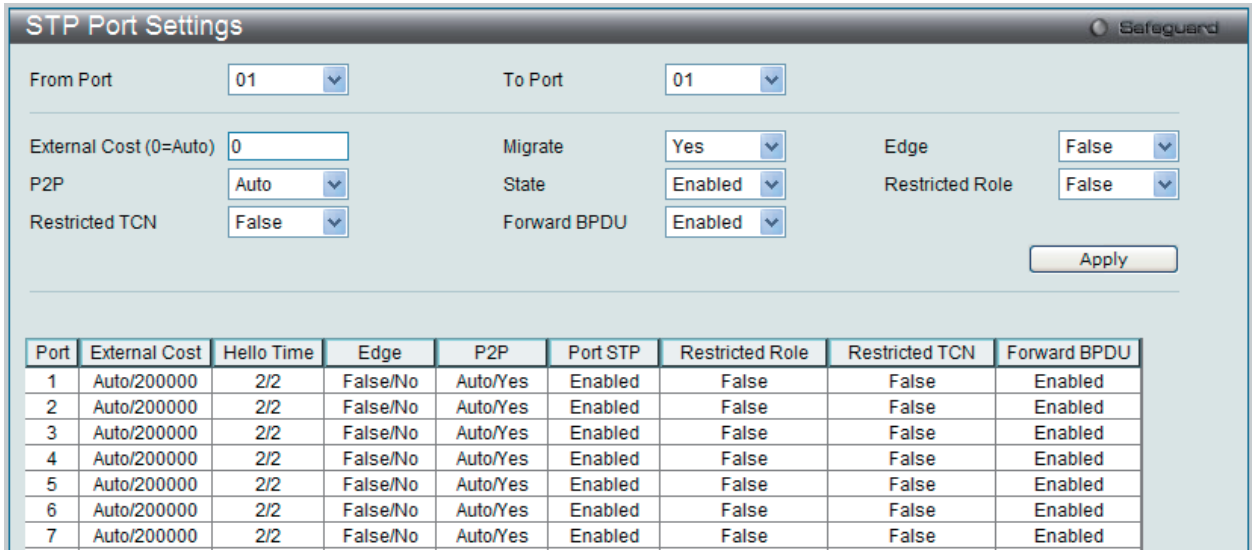


図 7-45　STP Port Setting 画面

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
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。
State	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。
Hello Time	RSTP においてはブリッジとのパラメータで、MSTP ではポートごとのパラメータとなります。初期値は 2（秒）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）

ここでは、スイッチ上で MST インスタンスの設定を行うために使用します。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。

MST インスタンスの設定を行うには、**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。

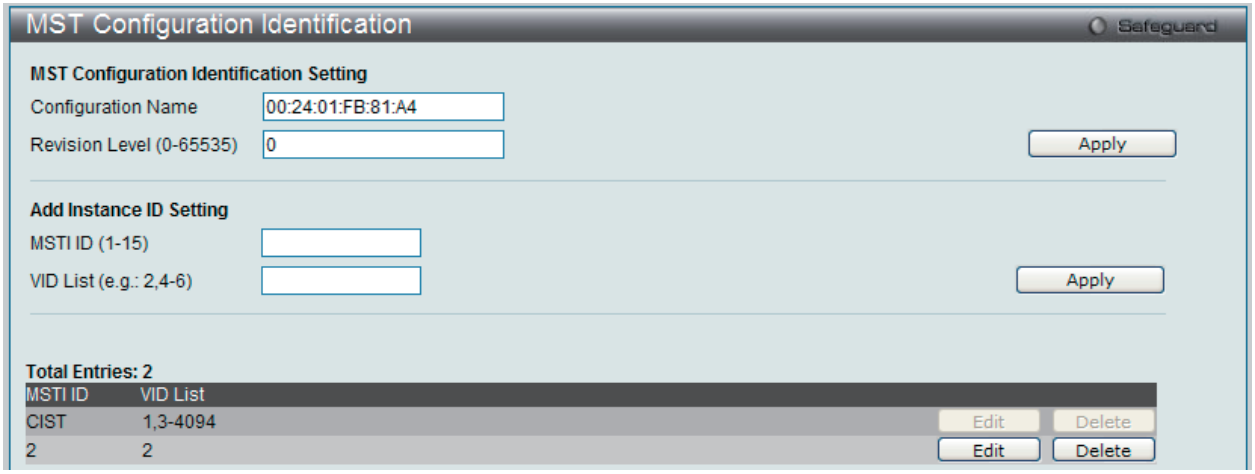


図 7-46　MST Configuration Identification 画面

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。
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

編集するエントリ横の「Edit」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）

以下の画面は、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。

MSTI を表示するためには、**L2 Features > Spanning Tree > STP Instance Settings** をクリックし、以下のテーブルを表示します。

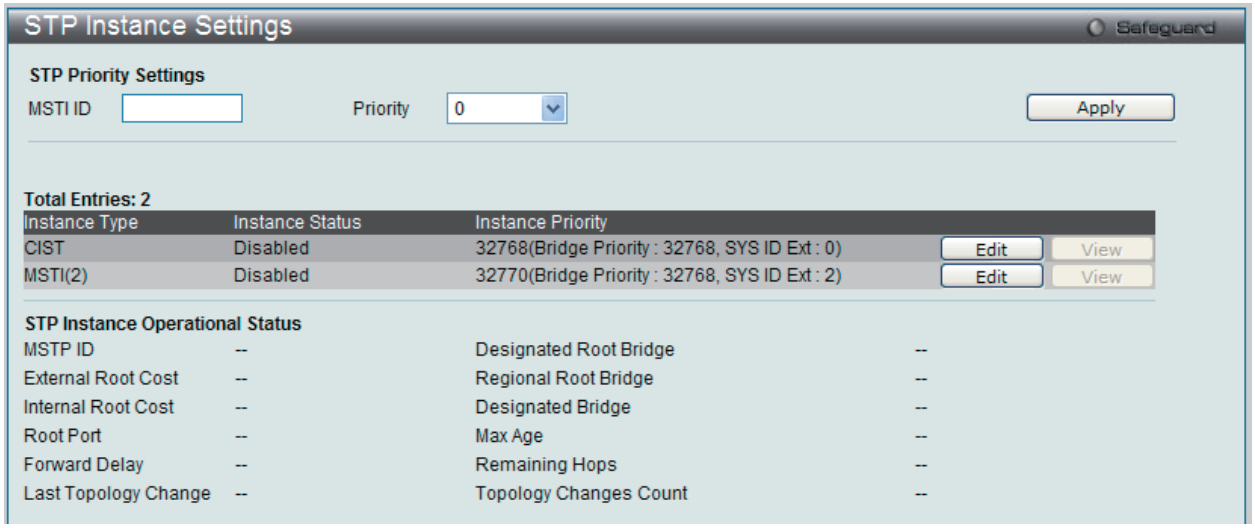


図 7-47　STP Instance Settings 画面

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）

本画面では現在の MSTP ポート情報が表示され、MSTI ID 単位でポート構成の更新を行うために使用します。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。

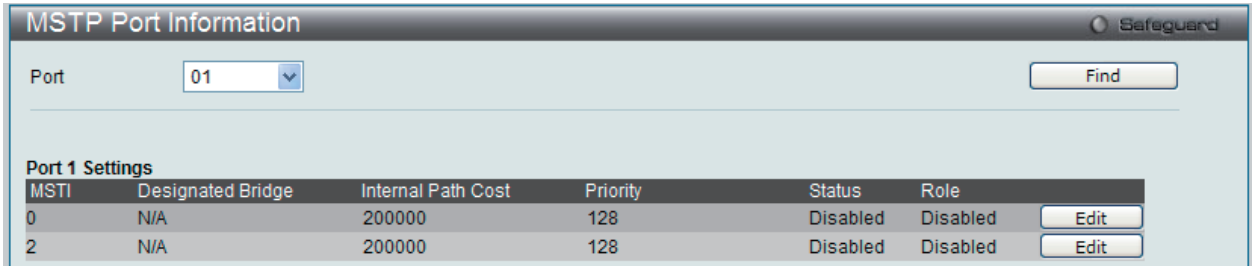


図 7-48　MSTP Port Information 画面

指定ポートの MSTP 設定の参照

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

指定ポートの MSTI インスタンス設定の編集

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。

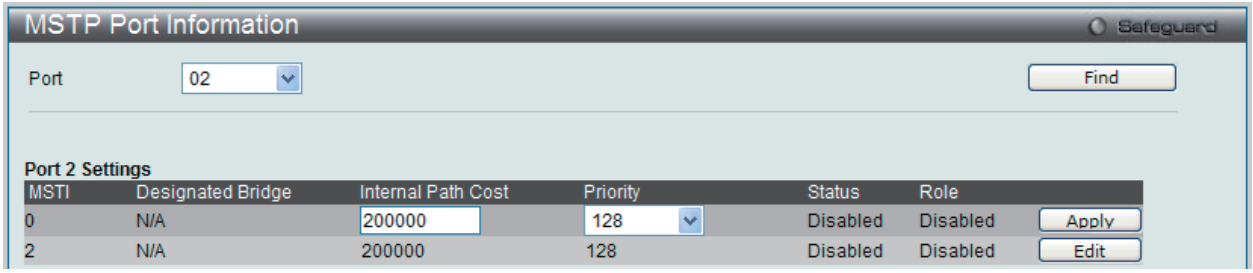


図 7-49　MSTP Port Information 画面

「Internal Path Cost」に値を入力し、「Priority」のプルダウンメニューでプライオリティを選択し、「Apply」ボタンをクリックします。

以下の項目を設定または参照できます。

項目	説明
MSTI	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	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。

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。

Forwarding & Filtering（フォワーディングとフィルタリングの設定）

「Forwarding & Filtering」フォルダには「Unicast Forwarding」、「Multicast Forwarding」および「Multicast Filtering Mode」のメニューがあります。

Unicast Forwarding（ユニキャストフォワーディング）

スイッチのユニキャストフォワーディングを設定します。

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

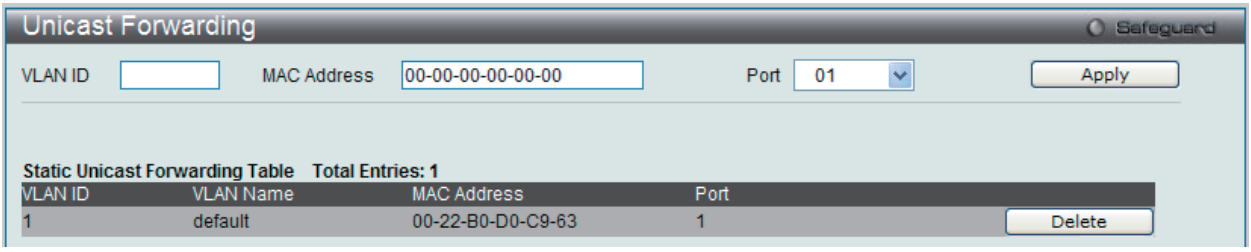


図 7-50　Unicast Forwarding 画面

エントリの追加

「Static Unicast Forwarding Table」にエントリを追加するためには、以下の項目を定義します。

エントリの編集

編集するためには、編集するエントリ横の「Edit」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、削除するエントリ横の「Delete」ボタンをクリックします。

以下の項目を設定できます。

項目	説明
VLAN ID	ユニキャスト MAC アドレスが存在する VLAN ID。
MAC Address	パケットが静的に送信される宛先の MAC アドレス。ユニキャスト MAC アドレスを指定します。
Port	MAC アドレスが存在するポートの番号を選択します。

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

Multicast Forwarding（マルチキャストフォワーディングの設定）

スイッチのマルチキャストフォワーディングを設定します。

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

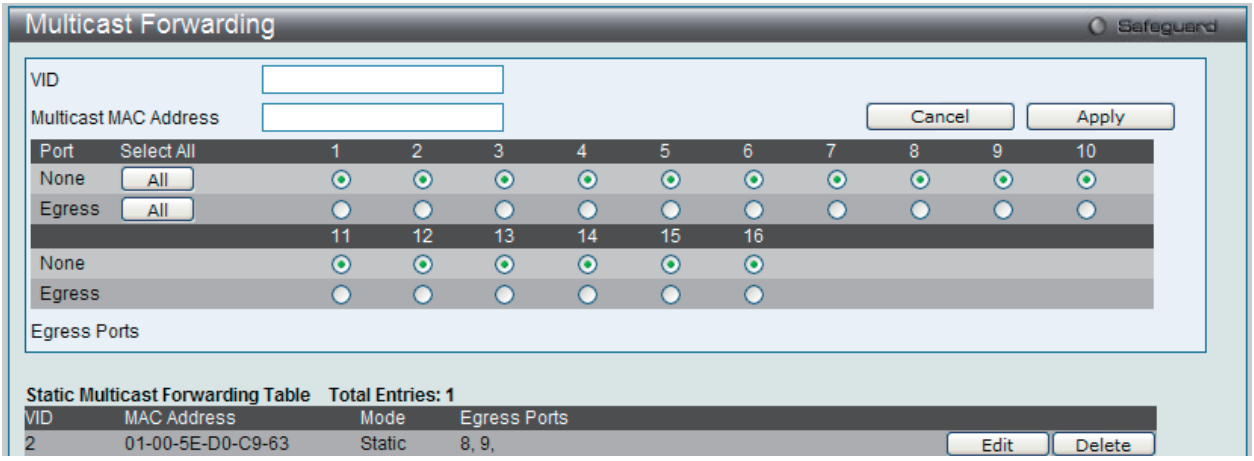


図 7-51　Multicast Forwarding 画面

本画面はスイッチに設定されたスタティックマルチキャスト転送テーブルのすべてのエントリを表示します。

エントリの削除

「Static Multicast Forwarding Table」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。

以下の項目を設定できます。

項目	説明
VID	指定の Multicast MAC アドレスが属する VLAN の VLAN ID。
Multicast MAC Address	マルチキャストパケットのスタティックソースの MAC アドレス。マルチキャスト MAC アドレスを指定します。
Port	スタティックマルチキャストグループのメンバとなるポート、および GMRP によってダイナミックにグループに参加させるポート、参加させないポートを選択します。「All」ボタンをクリックすると、全ポートが選択されます。 • None - ダイナミックにマルチキャスト参加を行います。指定すると、ポートはスタティックマルチキャストグループのメンバにはなりません。 • Egress - ポートはマルチキャストグループのスタティックメンバとなります。

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。

Multicast Filtering Mode（マルチキャストフィルタリングモード）

スイッチのマルチキャストフィルタリングモードの設定を行います。

L2 Features > Forwarding & Filtering > Multicast Filtering Mode の順にクリックし、以下の画面を表示します。

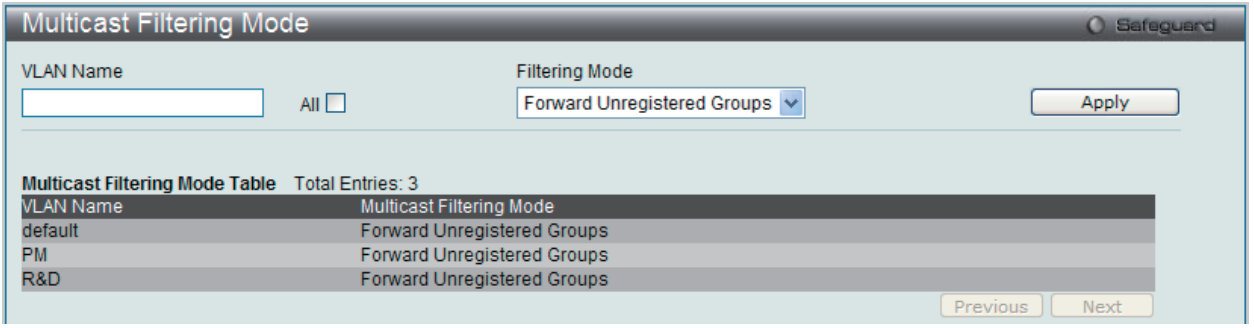


図 7-52　Multicast Filtering Mode 画面

以下の項目を設定できます。

項目	説明
VLAN Name	フィルタリングが適用される VLAN。「All」をチェックするとスイッチ上のすべての VLAN にフィルタリングが適用されます。
Filtering Mode	指定した VLAN ポートに転送されるマルチキャストパケットを受信した時の動作を指定します。 • Forward Unregistered Groups - 指定ポート範囲に存在する登録されていないマルチキャストグループが受信先のマルチキャストパケットを転送します。 • Filter Unregistered Groups - 指定ポート範囲に存在する登録されていないマルチキャストグループが受信先のマルチキャストパケットを廃棄します。

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 8 章　QoS（QoS 機能の設定）

本シリーズは、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
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。	137 ページ
Traffic Control（トラフィックコントロールの設定）	ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整します。	138 ページ
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）	ポート単位にプライオリティを割り当てます。	139 ページ
802.1p User Priority（プライオリティのクラス（キュー）への割り当て）	クラス（キュー）にのプライオリティタグの割り当てをします。	140 ページ
QoS Scheduling Mechanism（QoS スケジュールメカニズムの設定）	QoS スケジューリングを設定します。	141 ページ

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。

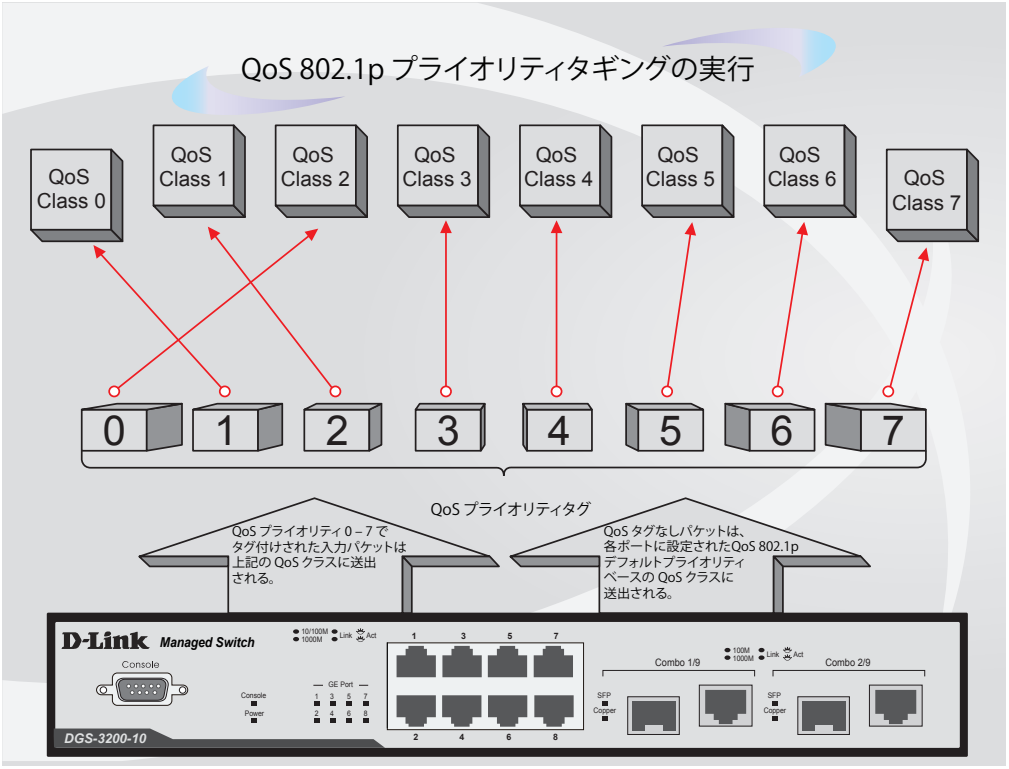


図 8-1　スイッチ上での QoS マッピングの例

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 はスイッチにある 7 つのプライオリティキューの中で、最も高い優先権を持っています。QoS を実行するためには、ユーザはスイッチに対し、パケットのヘッダに適切な識別タグが含まれているかを確認するように指示する必要があります。そして、ユーザはそれらのタグ付きパケットをスイッチ上の指定されたキューに送り、優先順序に従って送出するようにします。

例えば、遠隔地に設置した 2 台のコンピュータ間でビデオ会議を行うとします。管理者は Access Profile コマンドを使用して、送信するビデオパケットにプライオリティタグを付加します。次に受信側ではスイッチにそのタグの確認するよう指示を行い、タグ付きパケットを受信したら、それをスイッチのクラスキューに関連付けを行うようにします。また、管理者はこのキューに優先順位を与え、他のパケットが送出されるよりも前に送信されるように設定を行います。この結果、このサービス用のパケットは、できるだけ早く送信され、キューが最優先されることにより、中断されることなくパケットを受け取ることができるため、このビデオ会議用に帯域を最適化することが可能になります。

QoS について

本スイッチは、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 7 つのプライオリティキュー（と 7 つの CoS）を持っています。

注意 本スイッチは内部的にはポートに対して 8 つのサービスクラスを持っています。そのうちひとつは最初からスイッチが使用するように予約されていて変更できません。以下のサービスクラスに関する説明はすべて管理者が使用および変更できる 7 つのサービスクラスについて行っています。

Bandwidth Control（帯域幅の設定）

帯域制御の設定を行うことにより、すべての選択ポートに対して、送信と受信のデータレートを制限することができます。

ポートの帯域制御の設定を行うには、**QoS > Bandwidth Control** の順にメニューをクリックし、以下の画面を表示します。

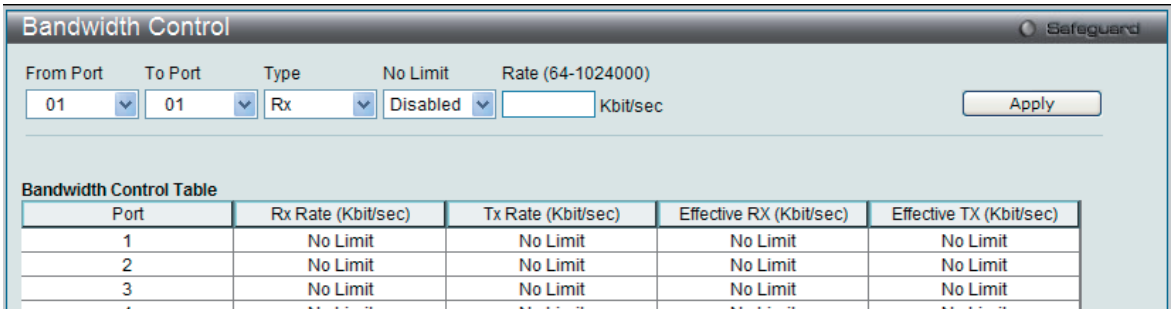


図 8-2　Bandwidth Control 画面

以下の項目を設定または表示できます。

項目	説明
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	ポートに対する帯域制限を設定します。 • Enabled - ポートで帯域制限を行いません。 • Disabled - ポートで帯域制限を行います。（初期値）
Rate (512-1024000)	選択ポートのデータ入力レートの制限値を指定します。範囲は 512-1024000Kbit/ 秒です。
Effective RX	RADIUS サーバが RX の帯域幅を割り当てると、それは有効な RX 帯域幅となります。RADIUS サーバを使用した認証は、ポートごとかユーザごとに行われます。ユーザごとの認証のために、指定ポートに複数ユーザが割り当てられていると、割り当てられる RX 帯域幅が複数あります。最終的な RX 帯域幅は、これら複数の RX 帯域幅の中で最も大きいものとなります。
Effective TX	RADIUS サーバが TX の帯域幅を割り当てると、それは有効な TX 帯域幅となります。RADIUS サーバを使用した認証は、ポートごとかユーザごとに行われます。ユーザごとの認証のために、指定ポートに複数ユーザが割り当てられていると、割り当てられる TX 帯域幅が複数あります。最終的な TX 帯域幅は、これら複数の TX 帯域幅の中で最も大きいものとなります。

「Apply」ボタンをクリックし、選択ポートの帯域制御を設定します。設定の結果は、画面下部の「Bandwidth Control Table」に表示されます。

Traffic Control（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」欄の「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。
本時間経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」（永久シャットダウン）モードに遷移し、トラップレシーバに送信する警告メッセージを生成します。一度「Shutdown Forever」モードに入ると、本ポートを通常の状態に戻すには、**Configuration > Port Setting** 画面で、無効になっているポートを手動で有効状態に戻すしか方法はありません。このようなストームコントロール機能を利用するためには、次に示す画面の「Action」欄で「Shutdown」オプションを選択してください。
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 の順にクリックし、以下の画面を表示します。

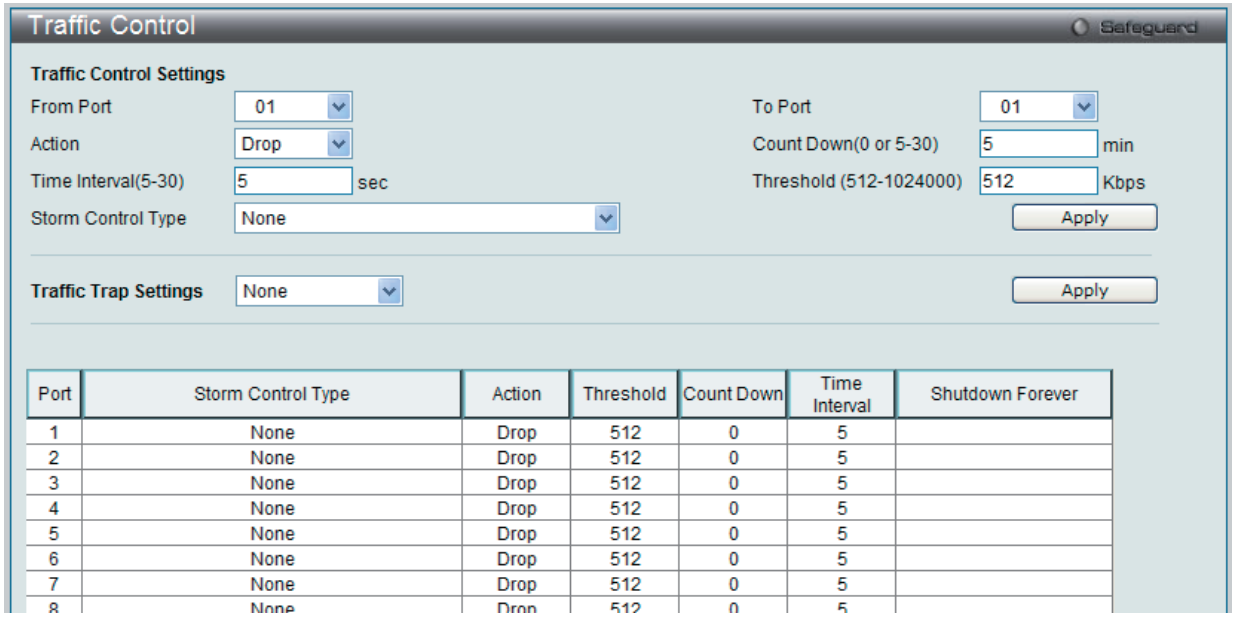


図 8-3　Traffic Control 画面

本画面には次の項目があります。

項目	説明
From Port	ストームコントロールを表示するポート範囲の最初の番号を設定します。
To Port	ストームコントロールを表示するポート範囲の最後の番号を設定します。
Action	トラフィックコントロールの方法をプルダウンメニューで指定します。以下の方法を指定できます。 • Drop – ハードウェアトラフィックコントロールメカニズムを使用します。スイッチのハードウェアがしきい値に基づき収束するまでパケットを破棄します。 • Shutdown – ソフト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。検出すると STP を維持するのに必要な STP、BPDU パケットを除くすべての受信パケットに対してポートを閉鎖します。「Count down」タイマが 0 になってもパケットストームが継続していたならば、ポートは Shutdown Forever モードになり、この画面の一番上の Storm Control Recover 設定を使用し、手動でリセットするまで何も操作ができなくなります。このオプションを選んだ場合、Interval も設定する必要があります。この値はパケットストームが起こっているかを判断するためにスイッチチップからパケット数を取得する間隔です。
Count Down (0 or 5-30)	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。0、5-30（分）が指定できます。

項目	説明
Time Interval (5-30)	マルチキャストやブロードキャストのパケット数をチップからトラフィックコントロール機能に渡す間隔を指定します。これらのパケット数により受信パケットがしきい値を超えているかを決定します。5-30（秒）まで指定でき、初期値は 5（秒）です。
Threshold (512-1024000)	トラフィックコントロール機能を実行するトリガとなる 1 秒あたりのパケットの最大数を指定します。512-1024000Kbps までで指定でき、初期値は 512Kbps です。
Storm Control Type	デバイスで有効なストームコントロールタイプを設定します。 None、Broadcast、Multicast、Unknown Unicast、Broadcast + Multicast、Broadcast + Unknown Unicast、Multicast + Unknown Unicast および Broadcast + Multicast + Unknown Unicast
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関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（「Action」項目で「Drop」が指定されている時）では使用できません。

「Apply」ボタンをクリックし、各項目の変更を適用します。

注意 トラフィックコントロールは、リンクアグリケーション（ポートトランキング）が設定されたポートに対しては行うことができません。

注意 Shutdown Forever モードになったポートは、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。

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

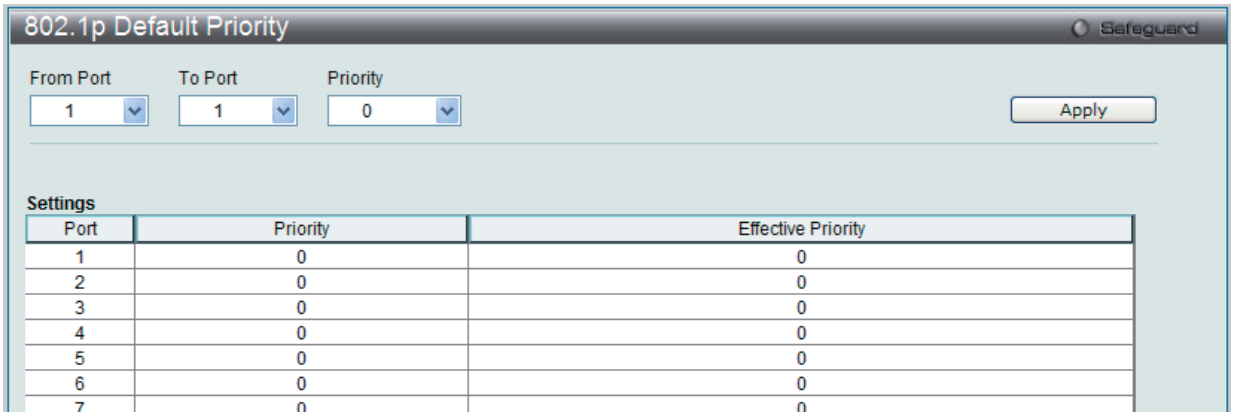


図 8-4　802.1p Default Priority 画面

本画面では、それぞれのポートにデフォルトの 802.1p プライオリティを割り当てます。プライオリティキューと有効なプライオリティタグは最低の 0 から最高の 7 まで指定できます。有効なプライオリティは、RADIUS に割り当てられた実際のプライオリティを示しています。RADIUS が割り当てた値が指定した制限を超えると、値はデフォルトプライオリティに設定されます。例えば、RADIUS が制限値に 8、デフォルトプライオリティに 0 を割り当てている場合、有効なプラオリティは 0 になります。

新しいデフォルトプライオリティを実行するためには、はじめに「From 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（プライオリティのクラス（キュー）への割り当て）

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 User Priority の順にクリックし、以下の画面を表示します。

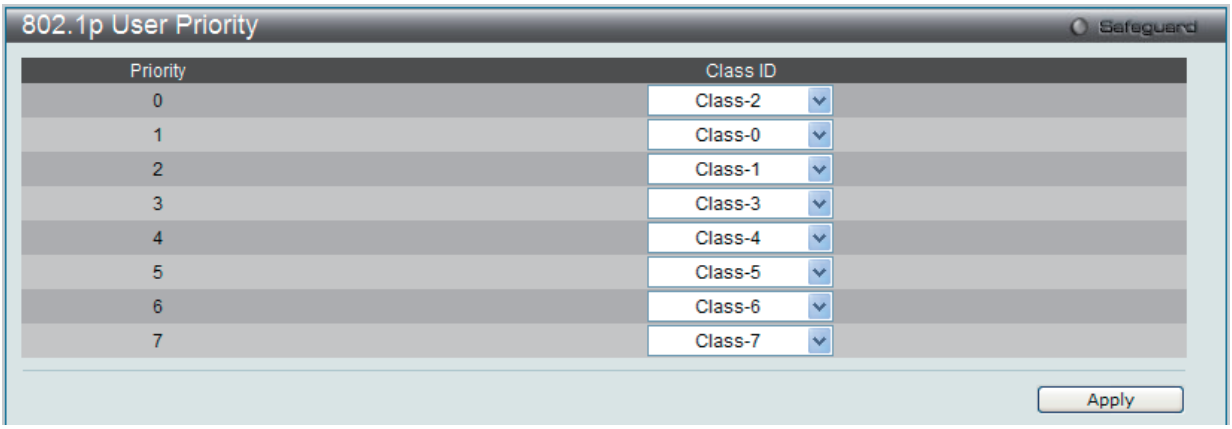


図 8-5　802.1P User Priority 画面

スイッチ上のポートグループにプライオリティを割り当てると、本画面のプルダウンメニューを使用して 802.1p プライオリティの 8 レベルのそれぞれに対してクラスを設定することができます。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。

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。

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

Scheduling Mechanism メニューでプライオリティクラスのキューを空にするためのメカニズムを「Weight Fair」と「Strict」から選択します。

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

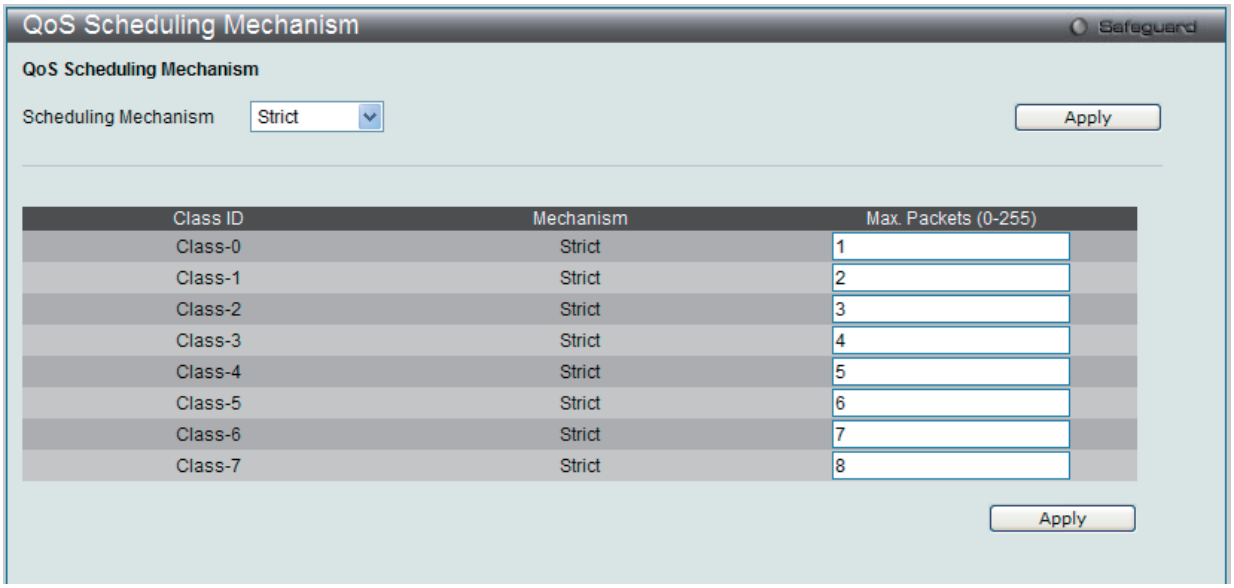


図 8-6　QoS Scheduling Mechanism 画面

本画面には以下の項目があります。

項目	説明
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。 • Weight Fair - 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。
Max. Packets (0-255)	次にプライオリティが低いキューが送信するまでに、該当するハードウェアプライオリティサービスクラスが送信することのできるパケットの最大数を指定します。0 から 255 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。

第 9 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
Safeguard Engine（セーフガードエンジン）	セーフガードエンジンの設定を行います。	142 ページ
Trusted Host（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。	144 ページ
IP-MAC-Port Binding（IP-MAC- ポートバインディング）	IP アドレスと MAC アドレスを結合し、レイヤ間通信を行います。	145 ページ
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。	151 ページ
DHCP Server Screening（DHCP サーバスクリーニング）	指定ポートからの DHCP サーバパケットをフィルタします。	153 ページ
Guest VLAN（ゲスト VLAN の設定）	802.1X ゲスト VLAN を設定します。	154 ページ
802.1X（802.1X ポートベース / ホストベースアクセスコントロール）	ポート単位の 802.1X 認証を設定します。	160 ページ
SSL Settings（Secure Socket Layer の設定）	証明書の設定、暗号スイートの設定を行います。	164 ページ
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。	166 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。	169 ページ
MAC-based Access Control（MAC アドレス認証）	MAC アドレス認証機能を設定します。	176 ページ
Web Authentication（WAC 設定）	Web ベースアクセスコントロールを設定します。	179 ページ
JWAC（JWAC 設定）	スイッチの拡張 Web ベースのアクセスコントロールを設定します。	184 ページ
Multiple Authentication（マルチプル認証方式）	同一のスイッチポートで異なる認証方式を実行し、ネットワークに接続します。	188 ページ
IGMP Access Control Settings（IGMP アクセスコントロール設定 : IGMP 認証）	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。	192 ページ
ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）	ハッカーや権限のない第三者による ARP Spoofing を防御します。	192 ページ

Safeguard Engine（セーフガードエンジン）

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 ブローキャストパケットを 5 秒間停止させます。その 5 秒後に、スイッチは再びパケットの入力フローをチェックします。フラッディングが解消されていれば、スイッチは再びすべてのパケットを受信し始めます。逆に、まだフラッディングが認められれば、前回の 2 倍の時間（10 秒）、すべての入力 ARP および IP ブローキャストパケットを停止させます。パケットの停止時間は、最大時間（320 秒）に達するまで倍増していき、それ以降は、通常の入力フローに戻るまで 320 秒で行われます。このしくみを以下に例示します。

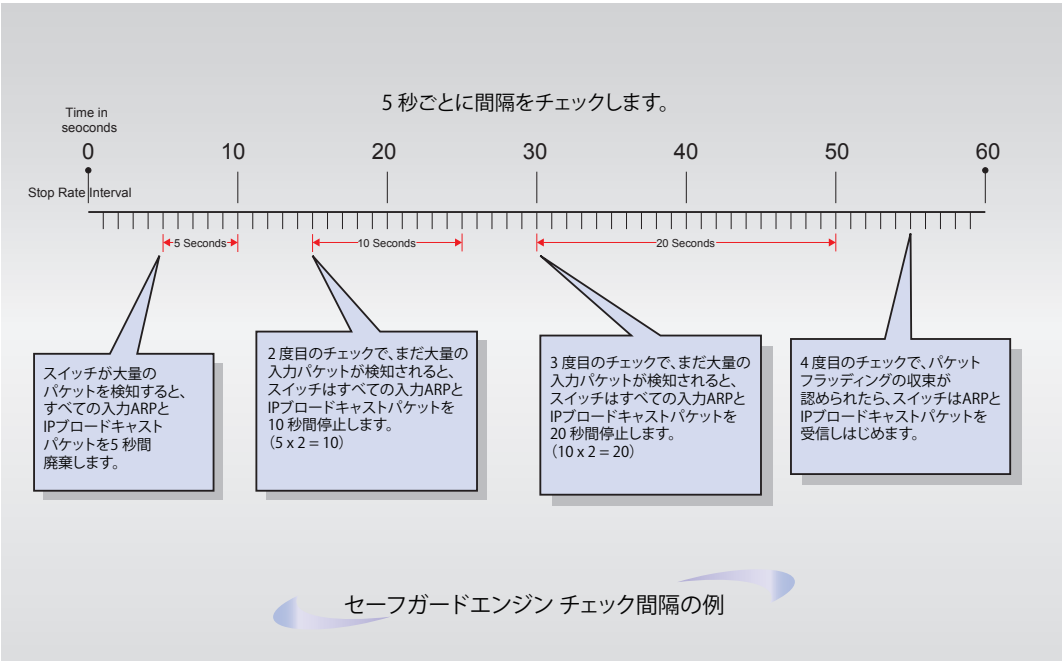


図 9-1　　セーフガードエンジンの例

パケットのフラッディングの問題を軽減するためにすべての継続したチェック間隔に対してスイッチは、信頼できない IP アドレスからの受信 ARP および IP ブロードキャストパケットを破棄する時間を倍にします。上の例題では継続したパケットのフラッディング問題が 5 秒間隔で検出された場合は ARP および IP ブロードキャストパケットを破棄する時間を倍にしています。（最初の破棄 = 5 秒、2 回目の破棄 = 10 秒、3 回目の破棄 = 20 秒）パケットのフラッディングを検出しなくなると ARP および IP ブロードキャストパケットを破棄する間隔を 5 秒に戻してプロセスを再開します。

Fuzzy モードでは、一度セーフガードエンジンは Exhausted モードになると、パケットフローは本モード開始時の半分のレベルまで減少させます。Normal モードに戻ると、パケットを 25%ずつ増加させます。スイッチは、その後間隔をチェックし、スイッチのオーバロードを避けるように動的に通常のパケットフローに戻します。

注意 セーフガードエンジンが有効の場合、本スイッチは FFP（Fast Filter Processor）メータリングテーブルを使用し、各トラフィックフロー（ARP、IP）に帯域を割り当て、CPU 使用率を制御することでトラフィックを制限します。これは、ネットワーク上のトラフィックのルーティング速度を制限します。

スイッチのセーフガードエンジン機能の有効化およびセーフガードエンジンの設定を行います。

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

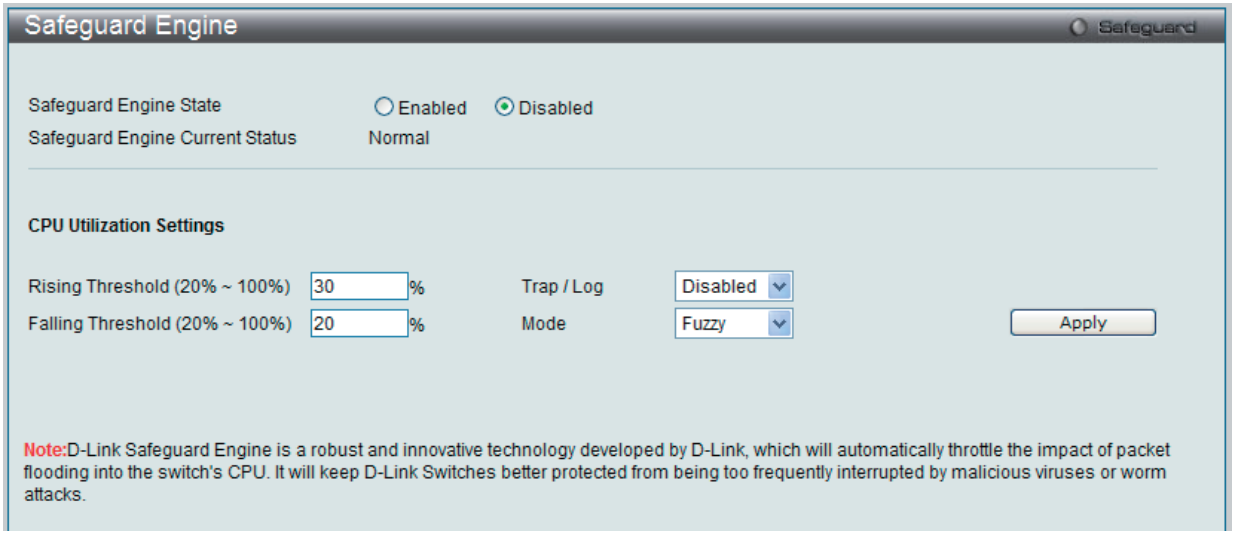


図 9-2　Safeguard Engine 画面

セーフガードエンジンオプションの有効化
「Safeguard Engine State」を「Enabled」にします。

高度なセーフガードエンジン設定
以下の項目を設定し、「Apply」をクリックします。

以下の項目を使用し、設定を行います。

項目	説明
Safeguard Engine State	セーフガードエンジン機能を「Enabled」（有効）/「Disabled」（無効）にします。
Safeguard Engine Current Status	現在のセーフガードエンジンの状態を表示します。
Rising Threshold (20% ~ 100%)	Safeguard Engine を有効にする前に許容可能な CPU 使用率のレベルを設定します。CPU 使用率がこのしきい値に到達すると、ここで設定した項目に基づいて、Exhausted モードに入ります。
Falling Threshold (20% ~ 100%)	許容可能な CPU 使用率のレベルを設定します。スイッチは CPU 使用率がこのしきい値に到達すると Safeguard Engine 状態から Normal モードに戻ります。
Trap/Log	CPU 使用率が高くなりセーフガードエンジン機能が作動した際にデバイスの SNMP エージェントとスイッチのログにメッセージを送信する機能を「Enabled」（有効）/「Disabled」（無効）にします。
Mode	CPU 高使用率に到達した際に起動する Safeguard Engine のタイプを選択します。 • Fuzzy – 本機能はすべてのトラフィックフローに対し平等に動的な帯域割り当てを行うことで CPU に対する IP と ARP トラフィックフローを最小化します。（初期値） • Strict – 本機能はストームがおさまるまで本スイッチ行きではないすべての ARP パケットの受信をストップし、不必要なブロードキャスト IP パケットの受信をストップします。

Trusted Host（トラストホスト）

最大 10 個までのトラストホストのセキュアな IP アドレスが、リモートのスイッチ管理のために設定され、使用できます。1 個以上のトラストホストが使用可能な状態にあると、スイッチは直ちに指定 IP アドレスからのリモートアクセスのみ許可することにご注意ください。この機能を有効にする場合、はじめに現在使用している IP アドレスを入力してください。

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

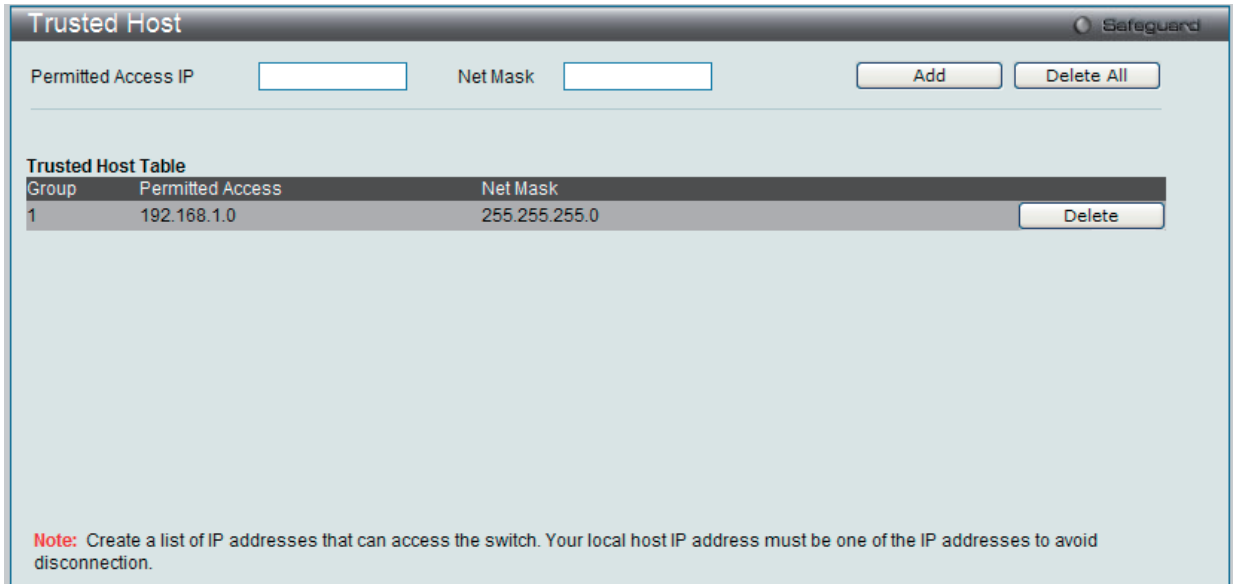


図 9-3　Trusted Host 画面

スイッチのトラストホスト管理のためにセキュアな IP アドレスを設定するためには、2 つの欄に現在使っているステーションの IP アドレスを入力し、さらに 9 個までのトラストホストの追加 IP アドレスを同様に 1 つずつ入力します。トラストホストステータスを IP アドレスに割り当てるために、「Apply」ボタンをクリックします。本設定は、直ちに適用されます。

IP-MAC-Port Binding（IMPB : IP-MAC- ポートバインディング）

IMPB について

DGS-3200 シリーズスイッチは、IP-MAC- ポートバインディング (IMPB) 提供します。これは、ネットワークホストに直接接続されているエッジスイッチで非常に多く使用される D-Link のセキュリティアプリケーションです。IMPB は、さらに D-Link の End-to-End セキュリティソリューション (E2ES) に不可欠の部分です。IP-MAC- ポートバインディングの第一の目的は、管理者がスイッチを経由してネットワークに接続することを許可されるクライアントの MAC アドレスと IP アドレスのペアを設定することによりスイッチにアクセスするクライアントを制限することです。具体的には、IMPB は、レイヤ間のデータ伝送を許可するために 4 バイトの IP アドレスと 6 バイトのイーサネットリンクレイヤの MAC アドレスをバインドします。

IMPB 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または無効にすることができます。一度 IMPB をスイッチポートで有効にすると、スイッチは「IMPB ホワイトリスト」として知られている定義済みのデータベースと共に IP-MAC アドレスのペアをチェックすることでクライアントのアクセスを制限または許可します。未認証ユーザが IMPB が有効なポートにアクセスしようとすると、システムはパケットを廃棄することでアクセスをブロックします。認証クライアントのリストは、CLI または Web により手動で作成できます。

一般的な IP マネージメントのセキュリティ問題

現在、IP マネージメント構造における制限と問題は重大なセキュリティ問題を引き起こしています。syslog などのメカニズムの監査、アプリケーションのログ、ファイアウォールログなどはクライアントの IP 情報に主として基づいています。しかし、容易にクライアント IP アドレスを変更できるとしたら、そのようなログ情報は無意味と言えます。IP のコンフリクトは今日のネットワークで最も一般的な問題ですが、もう一つの重要な心配事でもあります。どのユーザも、IMPB がないと、手動で IP アドレスを変更し、他の PC、コアスイッチ、ルータまたはサーバなどの他のリソースとのコンフリクトを引き起こす場合があります。また、この重複する IP は検証の問題を起こすだけでなく、それがネットワーク全体に潜在的な危険性を引き起こします。

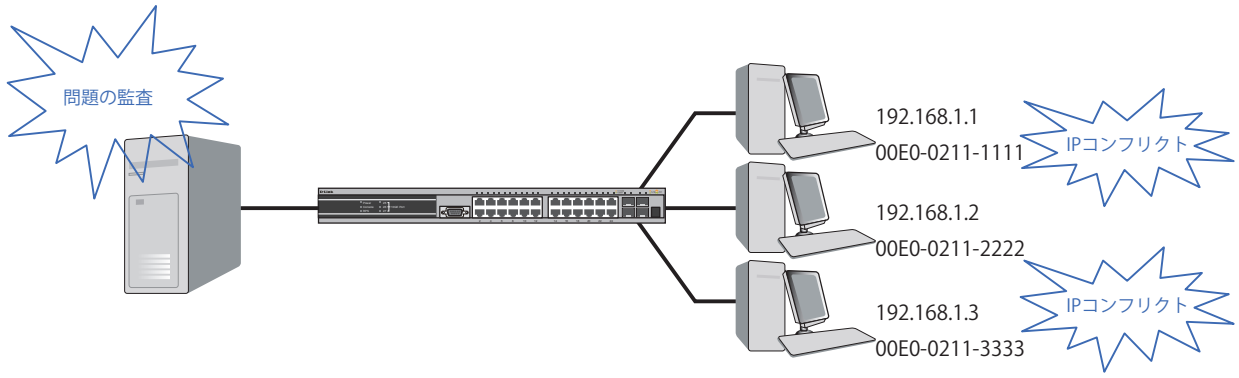


図 9-4　一般的な IP セキュリティ問題の図

悪意あるユーザが ARP パケットを操作することによってトラフィックを傍受し、または接続を遮断する ARP スプーフィング攻撃が今日のネットワークの保証においてまた別の重大な挑戦であります。ARP Spoofing 攻撃の動作方法に関する詳しい情報については、本マニュアルの263 ページの「付録 D 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。

IP マネージメントセキュリティを改良するソリューション

DGS-3200 シリーズスイッチは、攻撃からネットワークを保護する IMPB 技術を導入しています。IP-MAC- ポートバインディングを使用することによって、MAC アドレス、IP アドレス、および接続されたポートが IMPB のホワイトリストにない場合、スイッチはすべてのパケットを破棄します。IMPB では ARP または ACL モードのどちらかを選択します。さらに、DHCP Snooping オプションを使用して IMPB ホワイトリストをダイナミックに作成することができます。DHCP Snooping は、グローバル設定であり、ACL または ARP モードの上で有効にすることができます。各オプションには、長所と短所があります。

ARP モード

ARP モードでは、スイッチは、それが ARP パケット内の IP-MAC のペアをチェックするという ARP パケット検査を実行し、権限のないパケットは破棄します。ARP モードの長所は、スイッチのすべての ACL ルールを使用しないという点です。それでも、スイッチが ARP パケットをチェックするだけであるので、ARP パケットを送信しない未認可のクライアントを防御することはできません。

ACL モード

ACL モードでは、スイッチは ARP パケット検査に加えて IP パケット検査も行います。本質的には、ACL ルールは、IMPB エントリを静的に設定し、不正な IP-MAC のペアを持つ他の IP パケットを破棄するために使用されます。ACL モードの明確な長所は、ARP パケットと IP パケットの両方をチェックすることによって、より高いセキュリティを確保することです。しかし、それを行うためには ACL ルールの使用が必要です。ACL モードが選択されると、ARP モードが初期値で有効となるため、ARP モードのエンハンスバージョンとして ACL モードは見なされます。

Strict と Loose ステート

また、ACL と ARP モードより別に細かい制御のためにポートにステートを設定することができます。Strict と Loose の 2 つのステートがあり、どちらか一つを選択することができます。ポートが「Strict」ステートに設定されると、初期値ではポートに送信されたすべてのパケットが破棄されます。スイッチは、常にポートに受信するすべての IP および ARP パケットを IMPB エントリと照合します。パケットの IP と MAC のペアが IMPB エントリに一致すると、MAC アドレスはブロックされずにこのクライアントから送信されるその後のパケットを転送します。一方、ポートが「Loose」ステートに設定されると、初期値ではポートに送信されるすべてのパケットが許可されます。スイッチは、常にポートに受信するすべての ARP パケットを IMPB エントリと照合します。ARP パケットの IP と MAC のペアが IMPB エントリに一致しないと、MAC アドレスはブロックされてこのクライアントから送信されるその後のパケットを破棄します。

DHCP Snooping オプション

DHCP Snooping を有効にすると、スイッチは、自動的に DHCP パケットについて検索し、IP-MAC- ポートバインディングホワイトリストにそれら保存することで IP-MAC のペアを学習します。管理者が手動で各 IMPB エントリを入力する必要はないため、面倒な設定がなくなります。これに対する前提として、有効な DHCP サーバの IP-MAC のペアがスイッチの IMPB リストに存在する必要があります。そうでない場合、DHCP サーバのパケットは破棄されます。DHCP Snooping は、通常すべてのクライアントが DHCP サーバを経由で IP を入手させるため、より安全性が高いとであると見なされています。

以下の図は PC-A と PC-B が DHCP サーバから IP アドレスを取得するという DHCP Snooping の例題です。スイッチは PC-A、PC-B、および DHCP サーバ間の DHCP 通信の会話についてトレースします。IP アドレス、MAC アドレス、および PC-A と PC-B を接続するポートは、学習されてスイッチの IMPB ホワイトリストに保存されます。そのため、これらの PC はネットワークに接続することができます。そして、IP アドレスをユーザが手動で設定している PC-C があります。この PC の IP-MAC のペアがスイッチの IMPB ホワイトリストの一つに一致しないため、PC-C からのトラフィックはブロックされます。

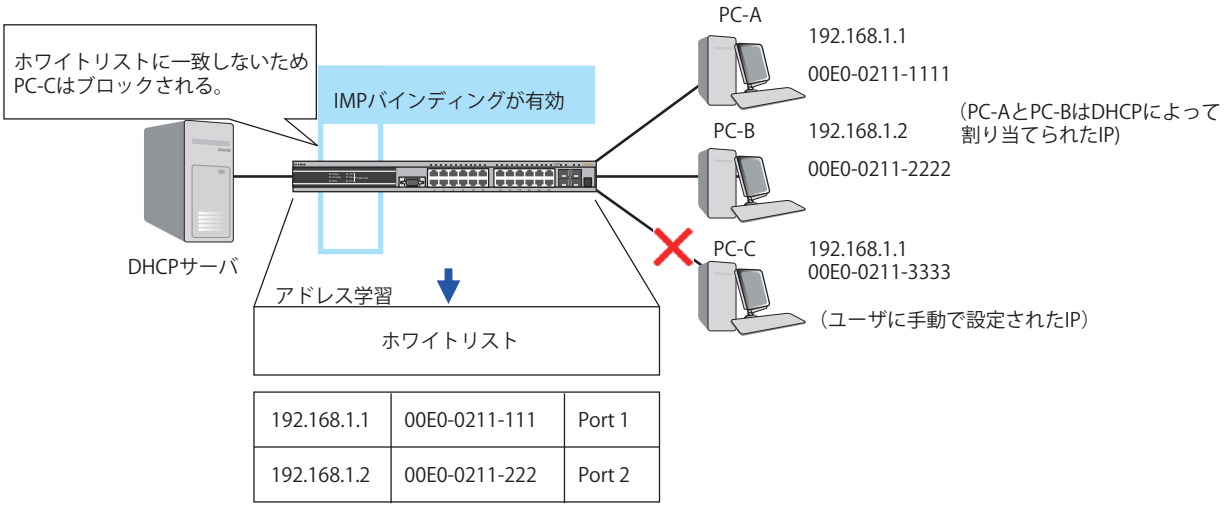


図 9-5　DHCP Snooping の例

IP-MAC-Port Binding フォルダコマンドには以下の 5 つの画面があります。
IMPB Global Settings、IMPB Port Settings、IMPB Entry Settings、DHCP Snooping Entries、および MAC Blocked List です。

IMPB Global Settings（IMPB グローバル設定）

スイッチのグローバルな IMPB 設定（トラップログステータスおよび DHCP Snoop ステータス）を有効または無効にするのに使用します。「Trap/Log」欄では、IP-MAC 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 の順にメニュークリックして、以下の画面を表示します。

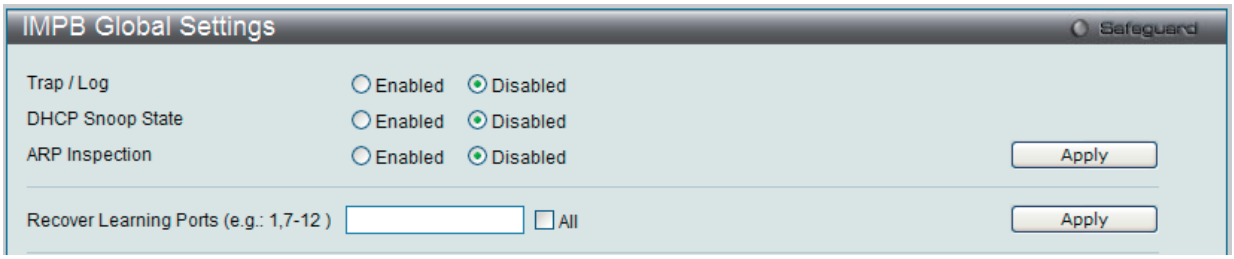


図 9-6　IMPB Global Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
Trap/Log	IP-MAC バインディングのトラップログメッセージ送信を有効または無効にします。有効にすると、スイッチはスイッチに設定された IP-MAC バインディングに一致しない ARP パケットを受信した場合に、SNMP エージェントとスイッチログにトラップログメッセージを送信します。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 Snoop State	IP-MAC バインディングの DHCP Snooping オプションを「Enabled」(有効) または「Disabled」(無効) にします。DHCP Snooping が有効にされると、スイッチは、自動的に DHCP パケットについて検索し、IMPB ホワイトリストにそれら保存することで IP-MAC のペアを学習します。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。
ARP Inspection	IP-MAC バインディングの ARP Inspection オプションを「Enabled」(有効) または「Disabled」(無効) にします。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。
Recover Learning Ports	動作を停止している ARP チェック機能を回復します。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。

IMPB Port Settings（IMPB ポート設定）

ポートベースで IMPB 設定を行います。

「From Port」と「To Port」欄でポートまたはポート範囲を指定します。「Strict」または「Loose」ステートを有効または無効にし、「Allow Zero IP」および「Forward DHCP Packet」欄を有効または無効にして、ポートの「Max IMPB」エントリを設定します。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。

Security > IP-MAC Port Binding（IMPB）> IMPB Port Settings の順にメニューをクリックし、以下の画面を表示します。

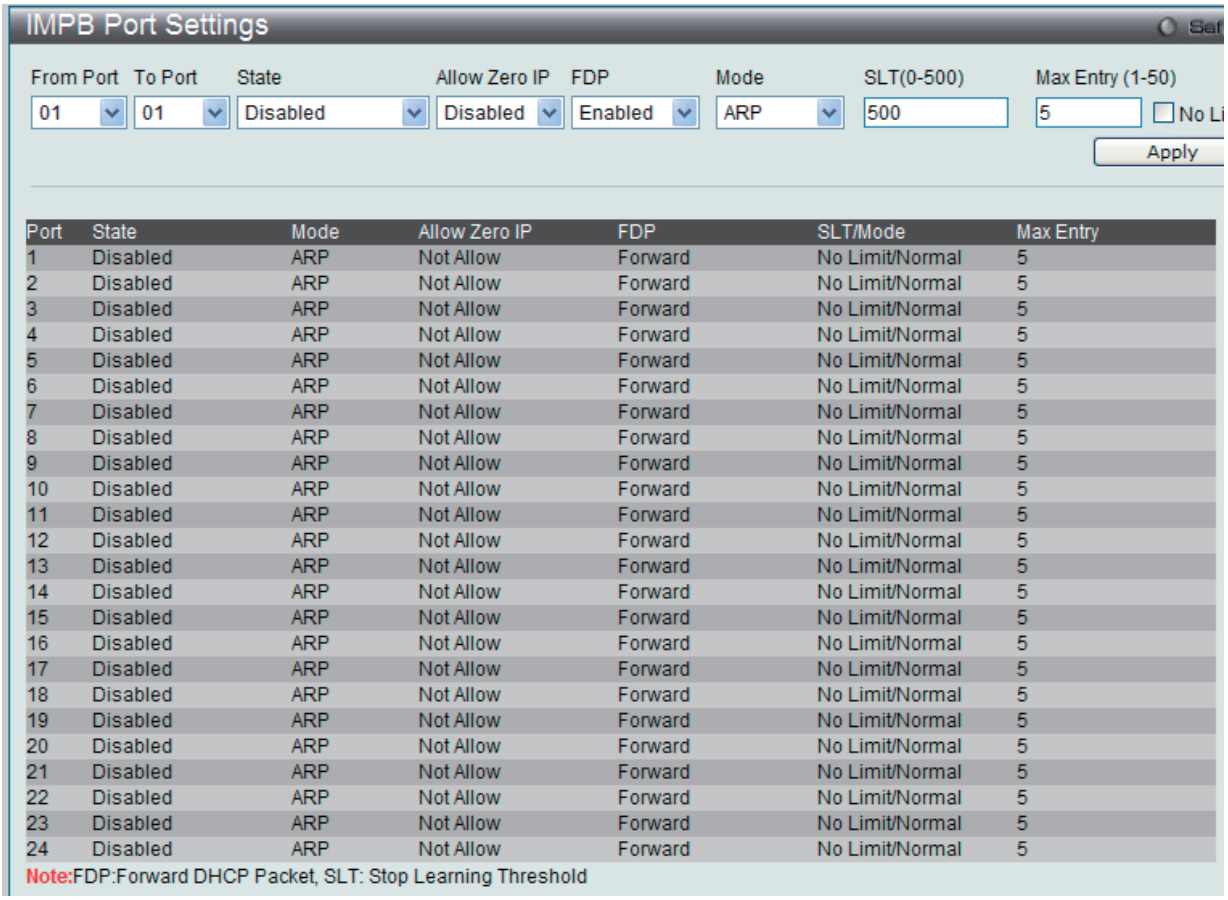


図 9-7　IMPB Port Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
From Port/To Port	IP-MAC- ポートバインディングを設定する対象のポートを指定します。
State	IP-MAC バインディングを「Enabled」(有効) または「Disabled」(無効) にします。 • Enabled(Strict) - より厳しいコントロール方法を提供します。本モード選択すると、すべてのパケットが初期状態でスイッチに防御されます。スイッチは、すべての到来する ARP/IP パケットを比較し、IMPB ホワイトリストとそれらの突き合わせを試みます。IP-MAC のペアがホワイトリストのエントリに一致すると、MAC アドレスからのパケットは防御されません。一致しない場合、MAC アドレスはブロックされたままとなります。Strict 状態では到来する ARP および IP パケットのチェックに対してより多くの CPU のリソースを使用しますが、より高いセキュリティを提供するため、本設定をお勧めします。 • Enabled(Loose) - より緩いコントロール方法を提供します。「loose」モードを選択すると、スイッチは初期値ですべてのパケットを転送します。しかし、スイッチは到来する ARP パケットを検証し、スイッチの IMPB ホワイトリストのエントリとそれらを比較します。パケットの IP-MAC のペアがホワイトリストに見つけられないと、スイッチは MAC アドレスを防御します。loose 状態を実行する主な利点は、スイッチが入力 ARP パケットだけをチェックするため、より少ない CPU リソースの使用だけですむという点です。しかし、それは「Loose」ステートは、ユニキャスト IP パケットだけを送信するユーザを防御できないことを意味します。この例は、悪意あるユーザが彼らの PC の上に静的に ARP テーブルを設定することによって DoS 攻撃を行うものです。この場合、スイッチは、PC が ARP パケットも送信しないために、そのような攻撃を防御することができません。
Allow Zero IP	本機能を「Enabled」（有効）/「Disabled」（無効）にします。一度有効にすると、スイッチは、0.0.0.0 の送信元 IP を持つ ARP パケットは通過することを許可します。DHCP サーバから IP アドレスを受け付ける前にクライアント (例 : 無線アクセスポイント) が ARP リクエストパケットを送出するというシナリオで有効です。この場合、クライアントから送出された ARP リクエストパケットは、0.0.0.0 の送信元 IP を含んでいます。スイッチは、そのようなパケットの通過を容認する必要があります。そうでないとクライアントは、ネットワークで別の重複 IP アドレスがあるかどうかを知ることができません。

項目	説明
FDP Forward DHCP Packet	初期値では、スイッチはすべてのパケットを転送します。しかし、ポートステートが「Strict」に設定されると、すべての DHCP パケットが破棄されます。その場合、「Enabled」を選択すると、ポートが「Strict」ステート下でも DHCP パケットを送信します。また、本機能を有効にすると、DHCP Snooping は適切に動作します。
Mode	プルダウンメニューを使用して、「ARP」または「ACL」モードを選択します。 • ARP - 本モードを選択すると、スイッチは ARP パケットの検査だけを行い、ACL ルールは使用されません。 • ACL - 本モードを選択すると、スイッチは ARP パケットの検査に加えて IP パケットの検査も行います。ACL ルールはこのモードの元で使用されます。
SLT (0-500) (Stop Learning Threshold)	MAC アドレスがスイッチによって防御される場合は、スイッチの L2 フォワーディングデータベース (FDB) と指定ポートに関連する各エントリに記録されます。スイッチの FDB を ARP DoS 攻撃の際の過負荷から保護するために、管理者は、ポートが不正な MAC アドレスの学習をやめるしきい値を設定します。0-500 の範囲で学習を停止するしきい値を指定します。 • 500 - ポートが 500 個の不正な MAC エントリの後に Stop Learning 状態に入り、追加の MAC エントリを許可せず、正しい MAC アドレスまたは不正な MAC アドレスのどちらも本ポート上で学習されなくなるということを意味します。また、Stop Learning 状態では、ポートは自動的にこのポート上でブロックされたすべての MAC エントリをクリアします。まだ正しい MAC エントリからのトラフィックは以前として送信されます。 • 0 - 制限を設定せずに、ポートは不正な MAC アドレスの学習を継続することを意味します。
Max Entry (1-50)	「From Port」/「To Port」で指定されたポートで学習できる DHCP 入力します。ポートで学習できる DHCP Snooping エントリ数を制限しない場合には。「No Limit」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。

IMPB Entry Settings（IMPB エントリ設定）

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 Setting の順にメニューをクリックし、以下の画面を表示します。

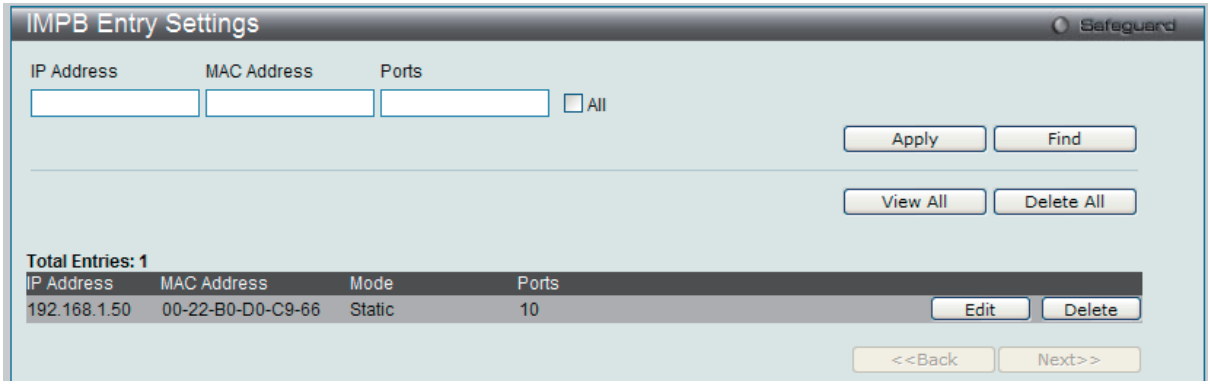


図 9-8　IMPB Entry Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
IP Address	MAC アドレスにバインドする IP アドレスを入力します。
MAC Address	IP アドレスとバインドする MAC アドレスを入力します。
Mode	「Static」または「Auto」が表示されます。
Ports	本 IP-MAC バインディングエントリ（IP アドレス +MAC アドレス）を設定する対象のポートを指定します。「All」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。

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。

エントリの検索
「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
「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。

DHCP Snooping Entries（DHCP Snooping エントリ）

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 Entries の順にクリックして、以下の画面を表示します。

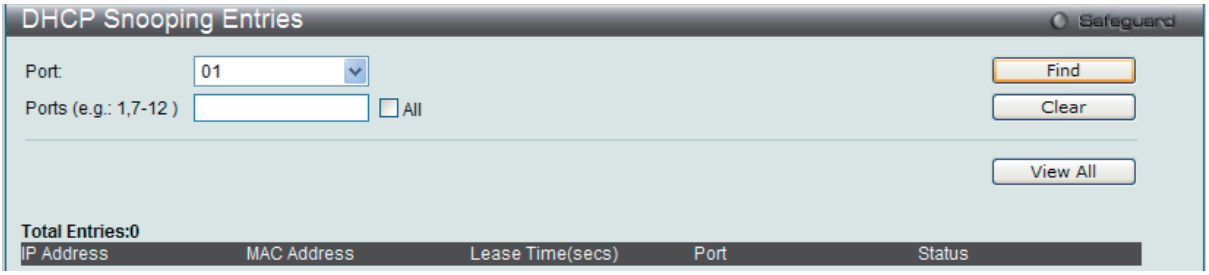


図 9-9　DHCP Snooping Entries 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
Port	プルダウンメニューか設定するポートを選択します。
Ports (e.g.: 1, 7-12)	DHCP Snooping エントリを表示するポートを指定します。「All」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。

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。

特定ポートの設定の表示

ポート番号を入力して「Find」ボタンをクリックします。

すべてのエントリの表示

「View All」ボタンをクリックします。

エントリの削除

「Clear」ボタンをクリックします。

MAC Block List（MAC ブロックリスト）

IP-MAC バインディング機能によりブロックされた未承認のデバイスを参照します。

Security > IP-MAC-Port Binding (IMPB) > MAC Block List の順にメニューをクリックして、以下の画面を表示します。

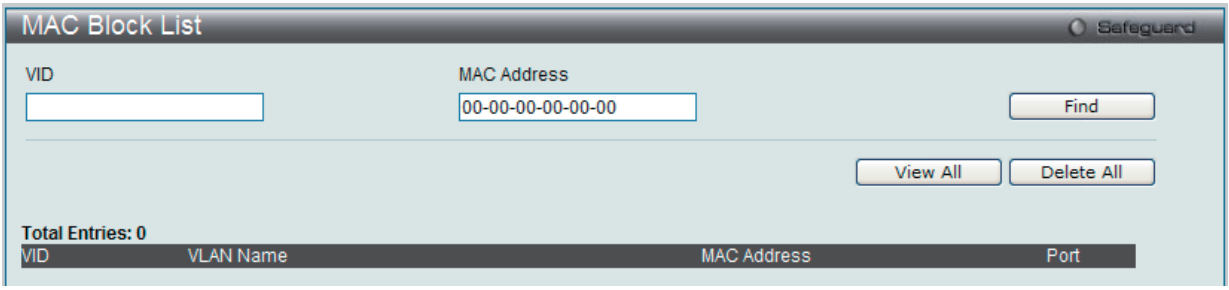


図 9-10　MAC Block List 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
ID	検出または削除する VLAN の VLAN ID を入力します。
MAC Address	検出または削除する MAC アドレスを入力します。

VIP-MAC バインディング機能によりブロックされた未承認デバイスの検索

「VLAN ID」と「MAC Address」を入力し、「Find」ボタンをクリックします。

エントリの削除

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

エントリの表示

すべてのエントリを表示するためには、「View All」ボタンをクリックします。

Port Security（ポートセキュリティ）

「Port Security」フォルダには、「Port Security Settings」と「Port Lock Entries」メニューがあります。

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。

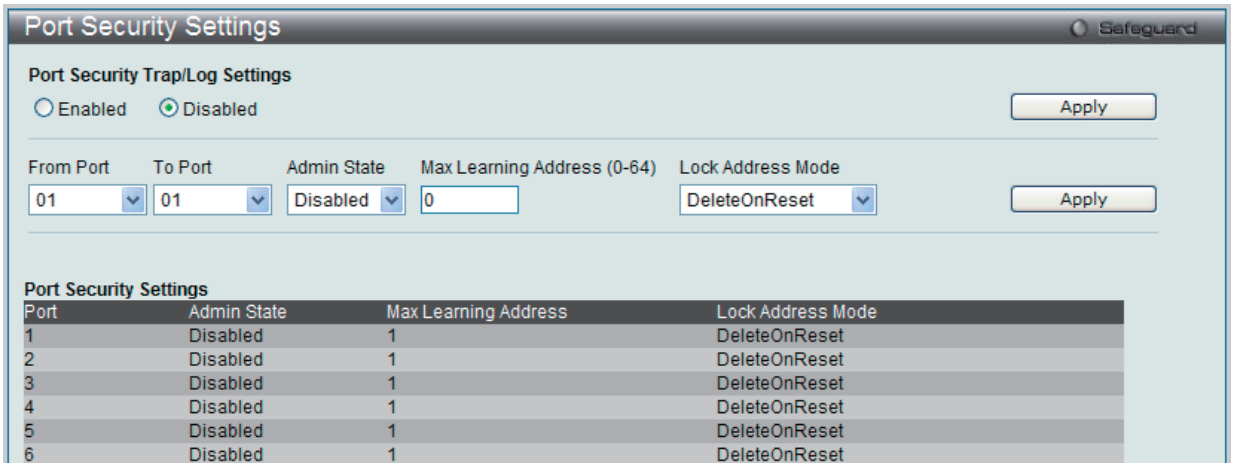


図 9-11　Port Security Settings 画面

本画面には次の項目があります。

項目	説明
Port Security Trap/Log Settings	スイッチのポートセキュリティトラップとログ設定を「Enabled」（有効）または「Disabled」（無効）にします。
From Port	ポートセキュリティ項目を表示するポートの最初の番号を設定します。
To Port	ポートセキュリティ項目を表示するポートの最後の番号を設定します。
Admin State	ポートセキュリティの有効 / 無効をプルダウンメニューで指定します。「Enabled」にすると、該当ポートは MAC アドレステーブルがロックされます。
Max Learning Address (0-16)	選択したスイッチとポートグループの MAC アドレス転送テーブルに保存できる MAC アドレス数を指定します。
Lock Address Mode	プルダウンメニューでスイッチの選択ポートグループに対して MAC アドレステーブルのロック動作の詳細を指定します。オプションは以下の通りです。 • Permanent – ロックされたアドレスは、エージングタイム経過後に削除されません。 • DeleteOnTimeout – 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。 • DeleteOnReset – 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。

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 Lock Entries（ポートロックエントリ）

ポートセキュリティエントリからエントリを削除するには、「Port Lock Entries」テーブルを使用します。このポートセキュリティエントリはスイッチが学習して転送データベースに登録したものです。

Security > Port Security > Port Lock 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。

本機能は、「Port Security Settings」画面の「Lock Address Mode」で「Permanent」か「DeleteOnReset」が選択されている時に使用します。別の言い方をすると、アドレスが永続的にスイッチに記録されている時しか削除できません。正確な情報により定義されたエントリが画面の中にある場合は、対応する MAC アドレスの行の「Delete」ボタンをクリックし、削除します。「Next」ボタンをクリックし、エントリリストの次のページを参照します。

「From Port」および「To Port」でポート範囲を選択し、「Clear」ボタンをクリックしてエントリを削除します。

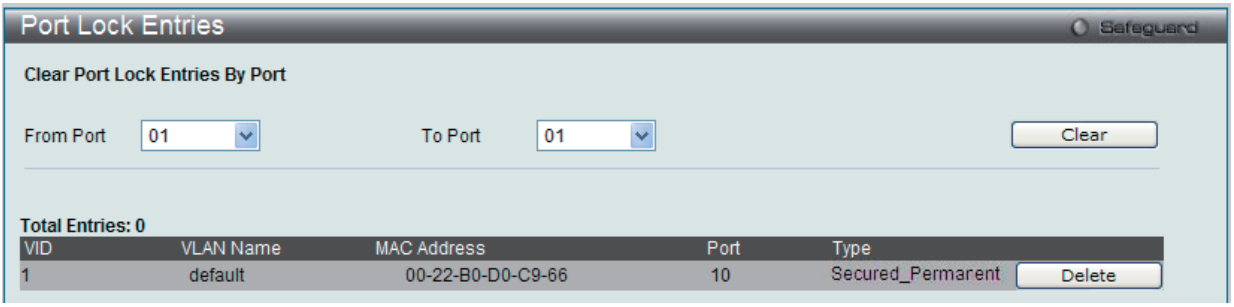


図 9-12　Port Lock Entries 画面

この画面では以下の情報を表示できます。

項目	説明
VID	スイッチの転送データベーステーブルに登録されているエントリの VLAN ID です。
VLAN Name	スイッチの転送データベーステーブルに登録されているエントリの VLAN 名です。
MAC Address	スイッチの転送データベーステーブルに登録されているエントリの MAC アドレスです。
Port	MAC アドレスを記録しているポート番号です。
Type	転送データベーステーブルに登録されている MAC アドレスの種類です。「Permanent」または「DeleteOnReset」となっているエントリのみ削除できます。
Clear	ボタンをクリックすると該当の MAC アドレスが削除されます。

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。

DHCP Server Screening（DHCP サーバスクリーニング）

DHCP Server Screening フォルダには次の 2 つの画面があります。:「DHCP Screening Port Settings」画面および「DHCP Offer Filtering」画面

DHCP Screening Port Settings（DHCP スクリーニングポート設定）

不正な DHCP サーバへの接続を拒否する DHCP サーバスクリーニング機能をサポートしています。DHCP サーバフィルタ機能が有効の場合、指定されたポートからのすべての DHCP サーバパケットはフィルタリングされます。

Security > DHCP Server Screening > DHCP Screening Port Settings の順にメニューをクリックして画面を表示します。

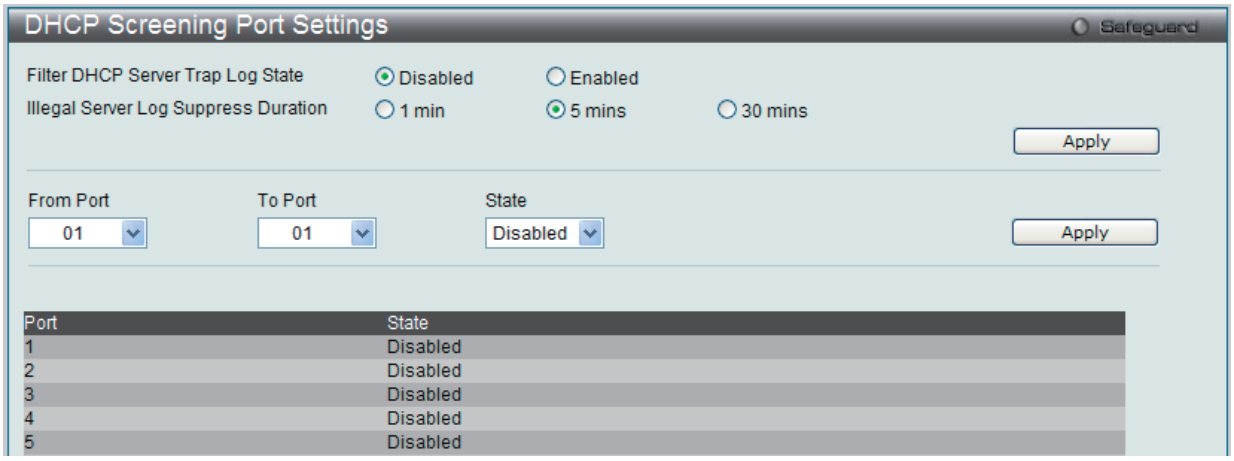


図 9-13　DHCP Screening Port Settings 画面

本画面には次の項目があります。

項目	説明
Filter DHCP Server Trap Log State	DHCP サーバのトラップログのフィルタを「Enable」（有効）または「Disable」（無効）にします。
Illegal Server Log Suppress Duration	不正なサーバログのサプレッション時間を 1、5、または 30 分から選択します。
From Port/To Port	設定の対象となるポートを指定します。
State	DHCP サーバスクリーニングを「Enable」（有効）または「Disable」（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 Filtering（DHCP Offer フィルタリング）

本機能では、ユーザはすべての DHCP サーバパケットを制限できるだけでなく、指定したどの DHCP クライアントからの DHCP サーバパケットも受信することが可能になります。この機能は 1 つ以上の DHCP サーバがネットワークに存在する場合に DHCP サービスを異なるクライアントグループを区別するのに役に立ちます。初めて DHCP フィルタを有効にした時にアクセスプロファイルエントリとポートエントリごとのアクセスルールとその他のアクセスルールが作成されます。これらのルールは、すべての DHCP サーバパケットをブロックするのに使用します。さらに、DHCP エントリの許可については、初めて DHCP クライアント MAC アドレスがクライアント MAC アドレスとして使用される時に、1 つのアクセスプロファイルと 1 つのアクセスルールエントリが作成されます。送信元 IP アドレスは DHCP サーバの IP アドレスと同じになります（UDP ポート番号は 67 です）。これらのルールは、ユーザが設定した特定のフィールドを持つ DHCP サーバパケットを許可するのに使用します。

Security > DHCP Server Screening > DHCP Offer Filtering の順にクリックし、画面を表示します。

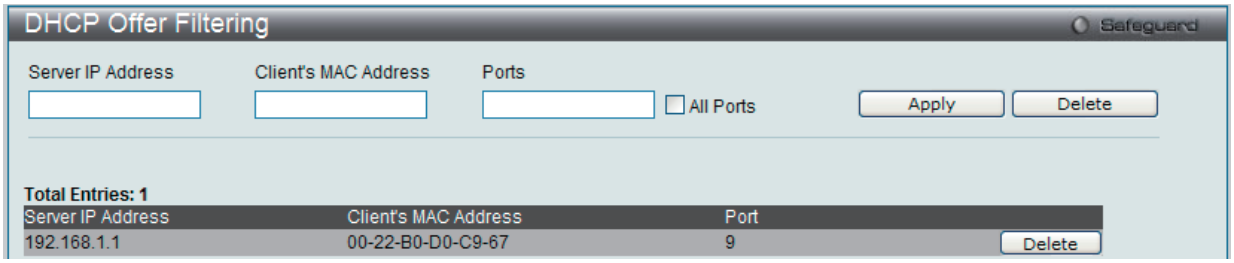


図 9-14　DHCP Offer Filtering 画面

本画面には次の項目があります。

項目	説明
Server IP Address	フィルタする DHCP サーバの IP アドレス。
Client's MAC Address	DHCP クライアントの MAC アドレス。ネットワーク上の正しい DHCP サーバが複数ある場合にだけ入力します。ネットワーク上に正しい DHCP サーバが 1 つしか存在しない場合は、入力することはできません。
Ports	フィルタする DHCP サーバのポート番号を入力します。スイッチのすべてのポートを使用する場合は「All Ports」をチェックします。

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

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。

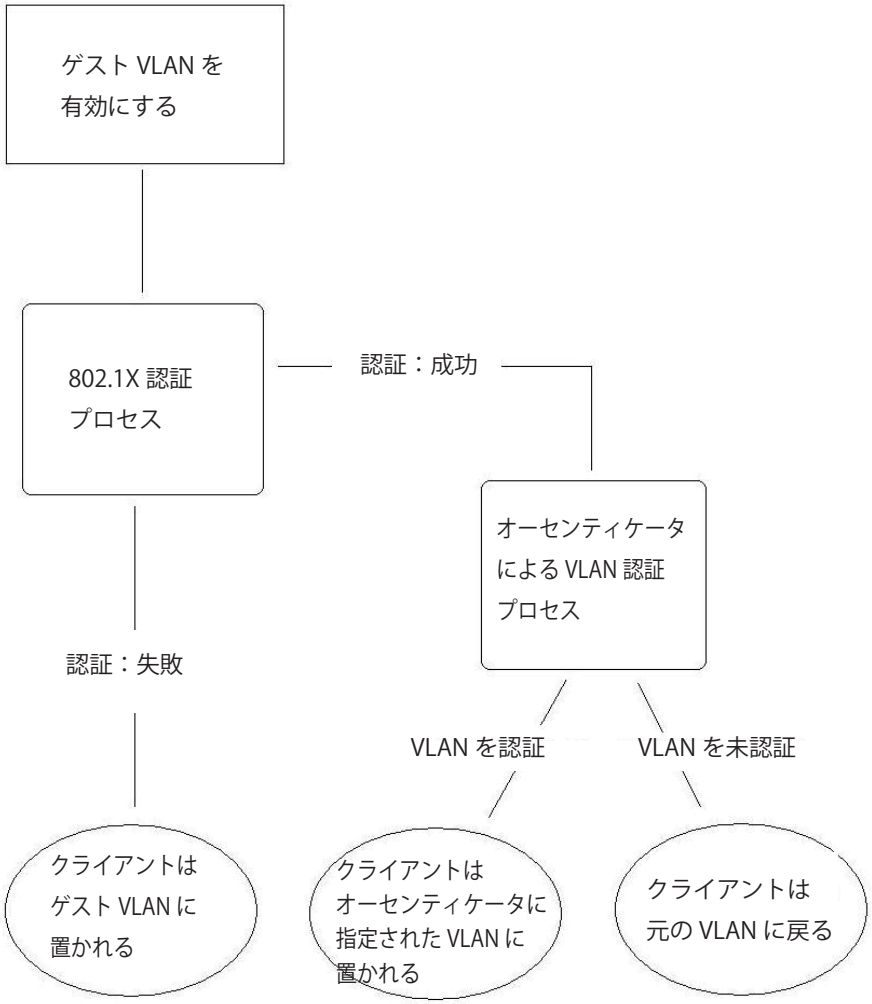


図 9-15　ゲスト VLAN 認証プロセス画面

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。
2. 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。
3. 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。
4. ポートがマルチ VLAN のメンバである場合、ゲスト VLAN のメンバになることはできません。

Security > Guest VLAN の順にクリックし、以下の設定画面を表示します。

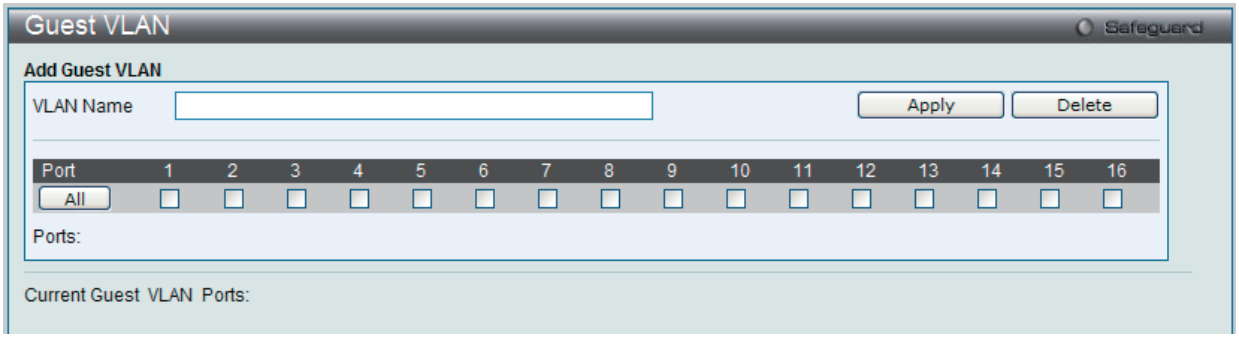


図 9-16　Guest VLAN 画面

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。

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。
Port	802.1X ゲスト VLAN を有効にするポートを設定します。

「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。一つの VLAN だけが 802.1X ゲスト VLAN としてアサインされます。

802.1X（802.1X ポートベース / ホストベース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。

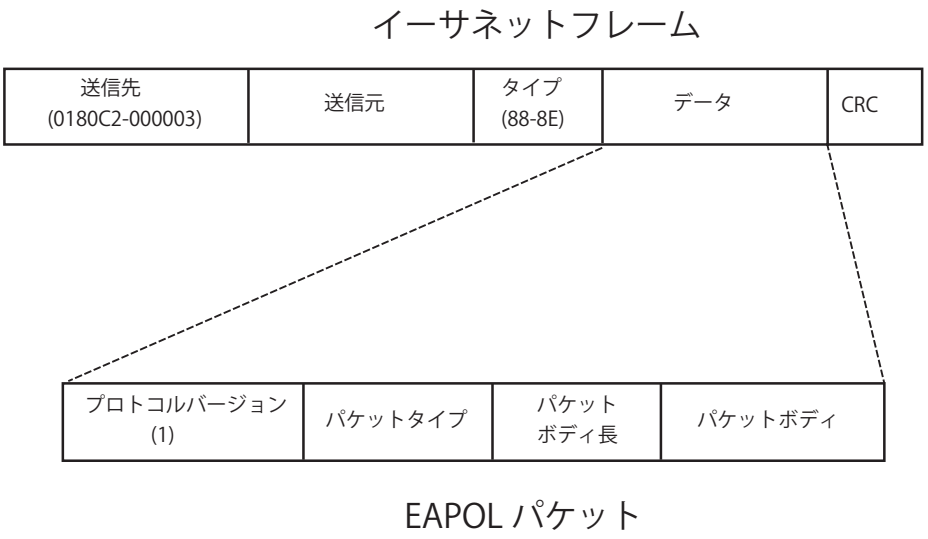


図 9-17　EAPOL パケット

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。

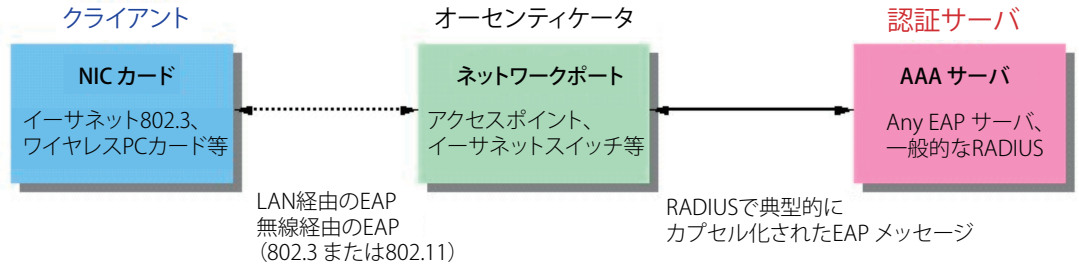


図 9-18　802.1X の 3 つの要素

以下の項では、クライアント、オーセンティケータ、および認証サーバのそれぞれの役割について詳しく説明します。

認証サーバ

認証サーバはクライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。認証サーバ上では RADIUS サーバプログラムを実行し、またそのサーバのデータがオーセンティケータ側（スイッチ）に正しく登録されている必要があります。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを受ける前に、認証サーバ（RADIUS）による認証を受ける必要があります。認証サーバは、RADIUS サーバとクライアントの間で EAPOL パケットを通じて信頼できる情報を交換し、そのクライアントの LAN やスイッチのサービスに対するアクセス許可の有無をスイッチに通知します。このように、認証サーバの役割は、ネットワークにアクセスを試みるクライアントの身元を保証することです。

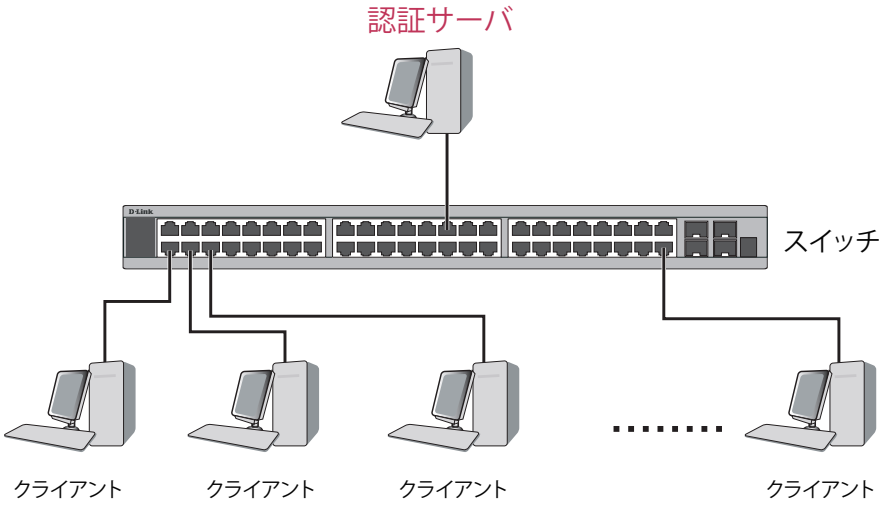


図 9-19　認証サーバ

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 Settings**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > 802.1X > Authentic RADIUS Server**）

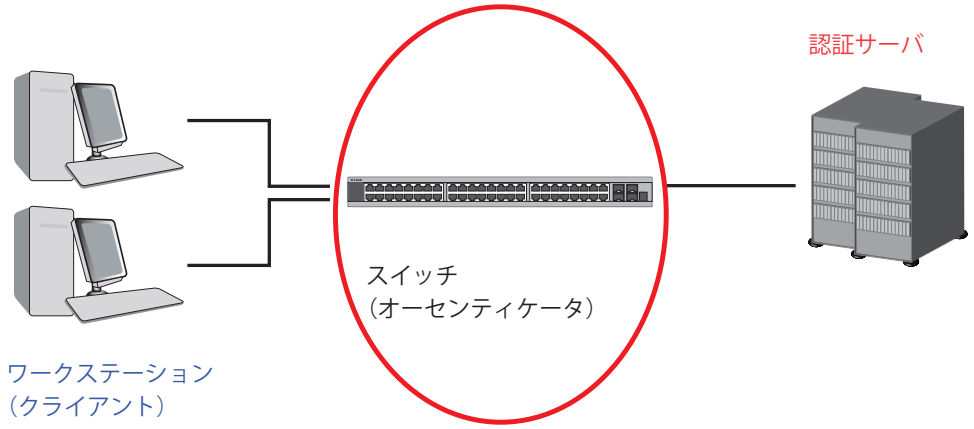


図 9-20　オーセンティケータ

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。

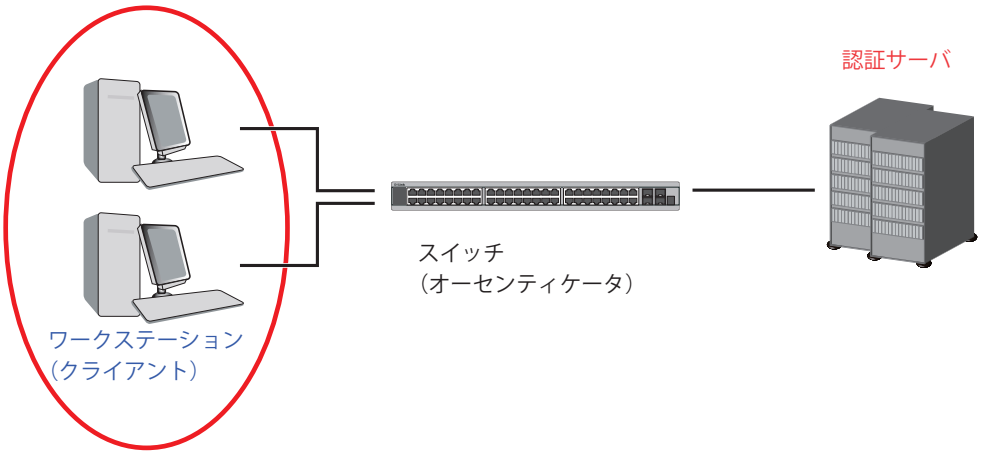


図 9-21　クライアント

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。

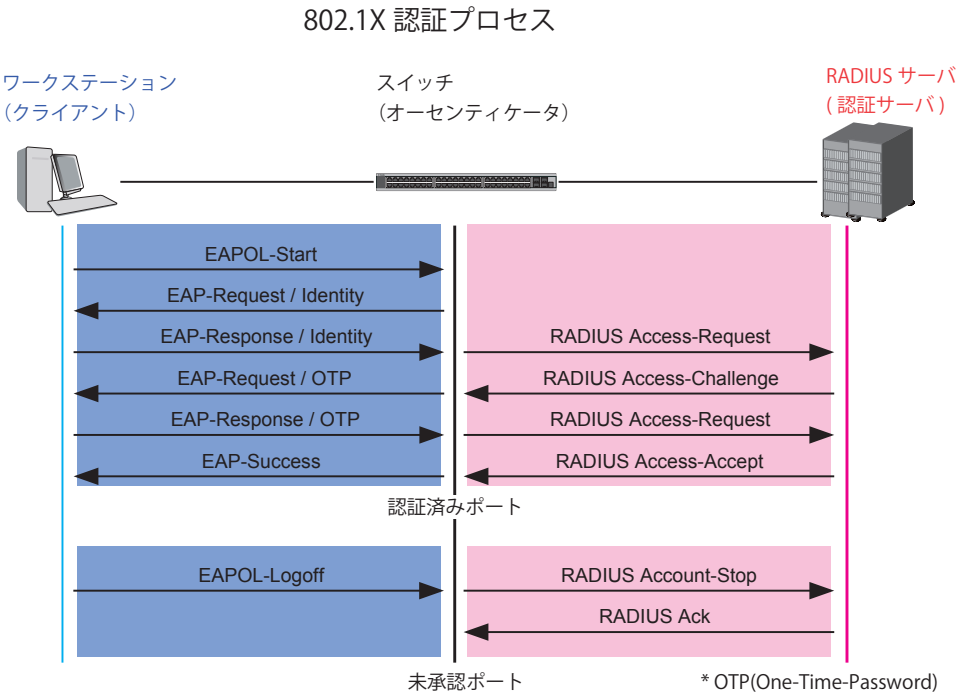


図 9-22　802.1X 認証プロセス

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. ホストベースのアクセスコントロール
   本方式では、スイッチは自動的に各ポートに対して 16 件までの MAC アドレスを自動的に学習してリストに追加します。スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に各 MAC アドレスの認証を行います。

802.1X ポートベース / ホストベースネットワークアクセスコントロール

802.1X 開発の本来の目的は、LAN 上で Point to Point プロトコルの機能を利用することでした。インフラストラクチャのように単一の LAN セグメントが 2 個以上のデバイスを持たない場合、どちらかがブリッジポートとなります。ブリッジポートは、リンクのリモートエンドにあるアクティブなデバイスの接続を示すイベントや、アクティブなデバイスが非アクティブ状態に遷移することを示すイベントの検知を行います。これらのイベントをポートの認証状態の制御に利用し、ポートでの認証が行わない場合に接続デバイスの認証プロセスを開始します。これをポートベースのアクセスコントロールと呼びます。

ポートベースのネットワークアクセスコントロール

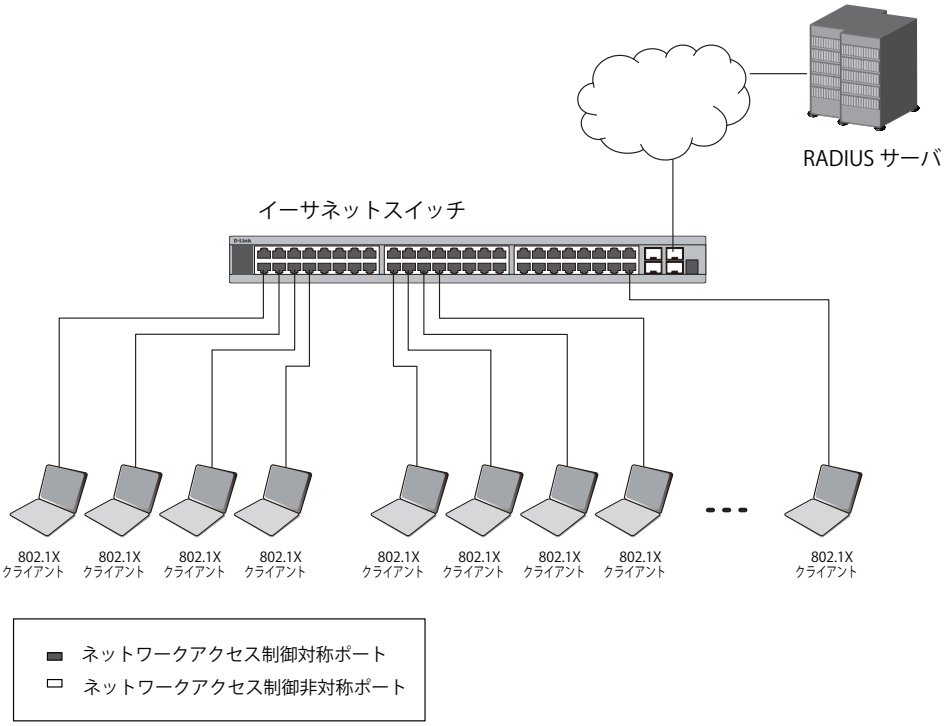


図 9-23　典型的なポートベースアクセスコントロールのネットワーク構成例

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

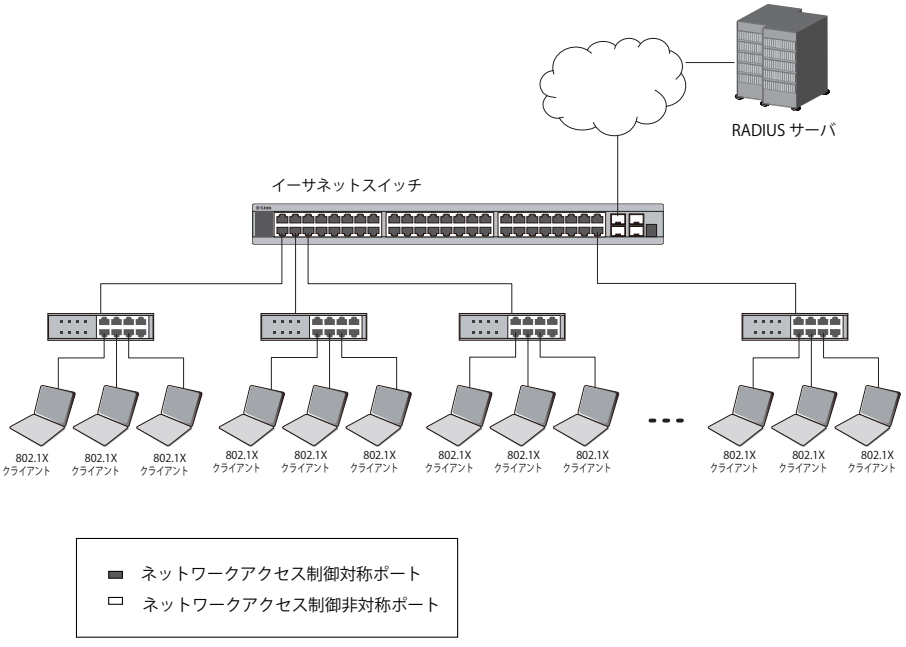


図 9-24　典型的な MAC アドレス認証のネットワーク構成例

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 Settings（802.1X 設定）

802.1X 認証設定を行います。

Security > 802.1X > 802.1X Settings の順にメニューをクリックします。

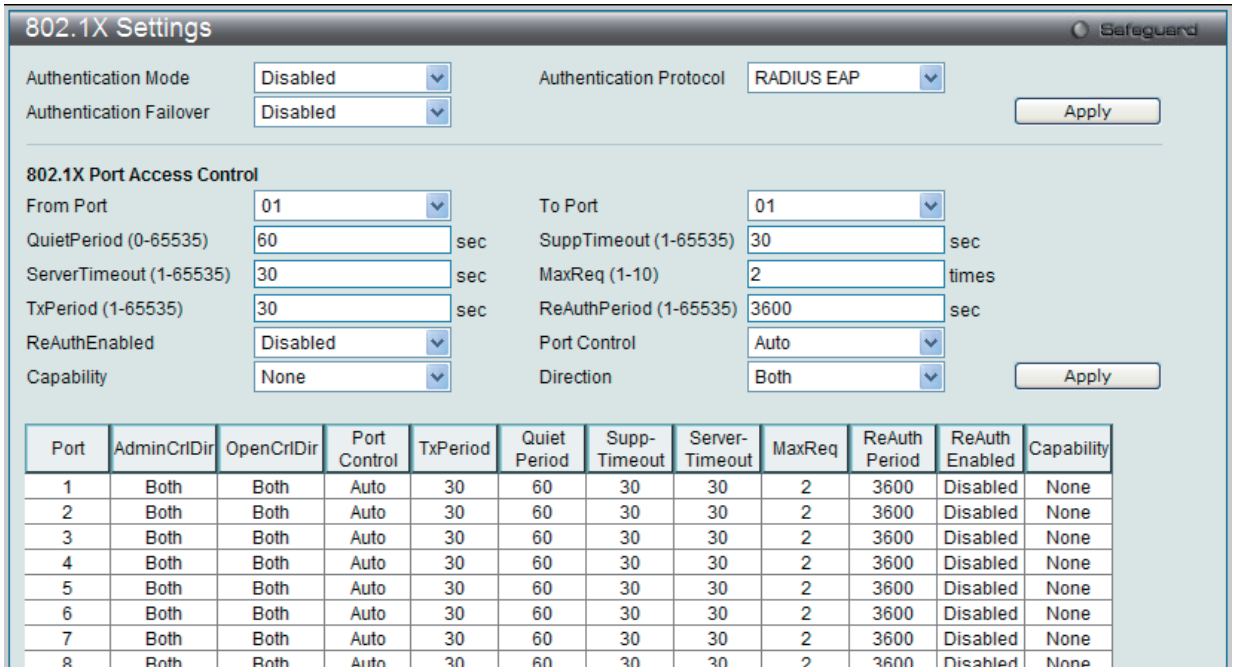


図 9-25　802.1X Settings 画面

「From Port」および「To Port」を使用して、ポート単位の設定を行います。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。
Authentication Protocol	認証プロトコルを「Local」または「RADIUS EAP」から選択します。
Authentication Failover	「Enabled」または「Disabled」を選択します。初期値では認証フェイルオーバは無効です。RADIUS サーバに到達しないと、認証エラーとなります。認証フェイルオーバが有効な場合に RADIUS サーバ認証には到達しないとローカルデータベースが認証が行われます。
From Port	設定するポートまたはポート範囲の最初の番号を設定します。
To Port	設定するポートまたはポート範囲の最後の番号を設定します。
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。
ReAuthEnabled	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	認証の方向を Both（双方向）に指定します。 • 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。 **注意** オプション「In」は本ファームウェアではサポートしていません。

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。

802.1X User（802.1X ユーザ）

スイッチに異なるローカルユーザを設定します。

Security > 802.1X > 802.1X User の順にクリックし、以下の画面を表示します。

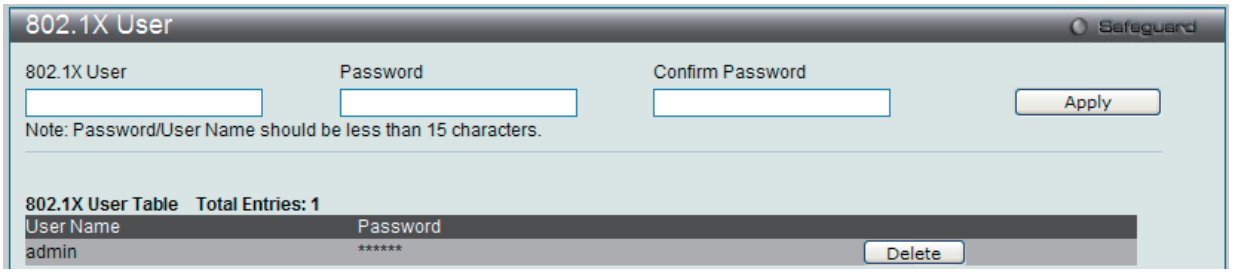


図 9-26　802.1X User 画面

「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。

Initialize Port(s)（ポートの初期化）

既存の 802.1X ポートとホスト設定が表示されます。以下の 2 つ画面で表示および設定をします。

ポートベース 802.1X ポートの初期化

802.1X のポートを初期化するためには、はじめに「802.1X Settings」画面の「Auth Mode」で「Port-Based」を選択しておく必要があります。

Security > 802.1X > Initialize Port(s) の順にクリックし、以下の画面を表示します。

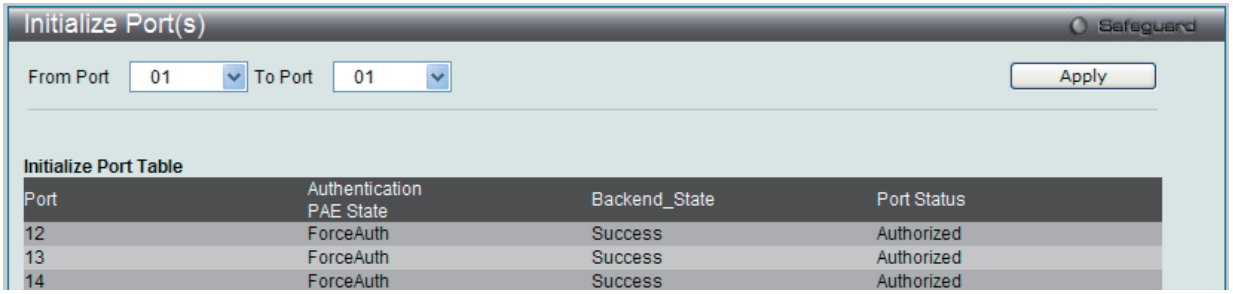


図 9-27　Initialize Port(s)（ポートベース 802.1X）画面

ここではポートまたはポート範囲の初期化を行います。画面の下部の「Initialize Port Table」はポートの現在のステータスを表示します。
ポートを初期化するためには、「From Port」および「To Port」でポート範囲を選択します。「Apply」ボタンをクリックすると、初期化を開始します。

ホストベース 802.1X ポートの初期化

802.1X のホスト側のポートを初期化するためには、はじめに「802.1X Settings」画面の「Auth Mode」で「MAC-Based」を選択しておく必要があります。

Security > 802.1X > Initialize Port(s) の順にクリックし、以下の画面を表示します。

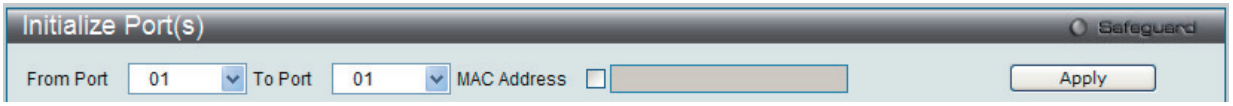


図 9-28　Initialize Port(s)（MAC ベース 802.1X）画面

注意　ポートの初期化の前に「802.1X Settings」画面（**Security > 802.1X > 802.1X Settings**）で 802.1X をグローバルに有効にする必要があります。「Initialize Port Table」の情報は、「Port based 802.1X」または「Host based 802.1X」が有効でないと参照できません。

ポートの初期化画面では以下の情報が表示または設定できます。

項目	説明
From Port	初期化する開始ポートを選択します。
To Port	初期化する終了ポートを選択します。
Port	スイッチのポートを示す参照用項目です。
Auth PAE State	Authenticator PAE の状態を以下の項目のいずれかで表示します。: Initialize、Disconnected、Connecting、Authenticating、Authenticated、Aborting、Held、ForceAuth、ForceUnauth および N/A
Backend_State	Backend Authentication の状態を以下の項目のいずれかで表示します。: Request、Response、Success、Fail、Timeout、Idle、Initialize および N/A
Port Status	コントロールポートのステータスは Authorized、Unauthorized または N/A で表示します。
MAC Address	対応ポートに接続しているクライアントの認証 MAC アドレスです。

Reauthenticate Port(s)（ポートの再認証）

既存の 802.1X ポートとホストのポートを以下の 2 つ画面を使用して、表示および再認証設定をします。

ポートベース 802.1X ポートの再認証

ポートベースの 802.1X ポートを再認証するためには、はじめに「802.1X Settings」画面の「Auth Mode」で「Port Based」を選択しておく必要があります。

Security > 802.1X > Reauthenticate Port(s) の順でクリックし、以下の画面を表示します。

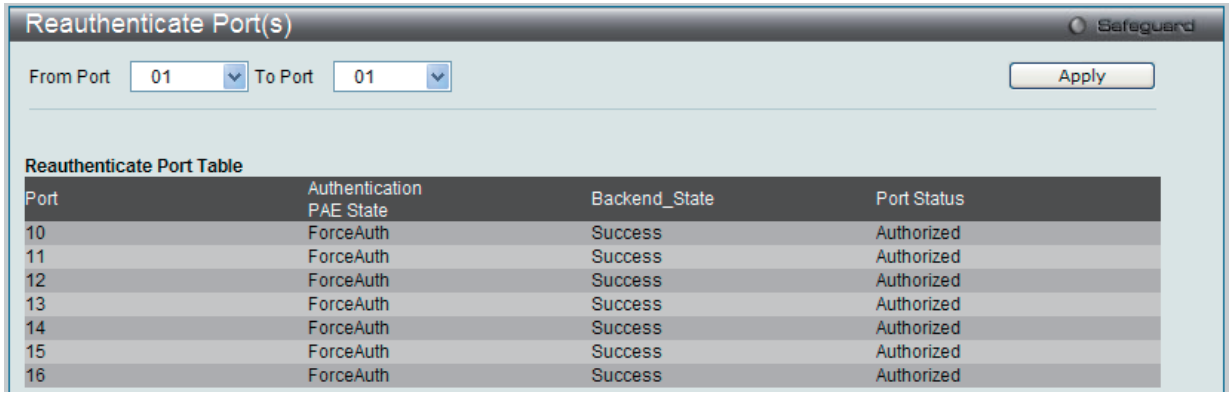


図 9-29　Reauthenticate Port(s)（ポートベース 802.1X）画面

「From Port」と「To Port」のプルダウンメニューでポートまたはポート範囲を選択し、「Apply」ボタンをクリックすることでポートの再認証を行います。「Apply」をクリックすると「Reauthenticate Port Table」には再認証ポートの現在のステータスが表示されます。

注意　ポートの再認証の前に「802.1X Settings」画面（**Security > 802.1X > 802.1X Settings**）で 802.1X をグローバルに有効にする必要があります。「Reauthenticate Port(s)」画面の情報は、「Port based 802.1X」または「Host based 802.1X」が有効でないと参照できません。

ホストベース 802.1X ポートの再認証

ホストベースの 802.1X のポートを再認証するためには、はじめに「802.1X Settings」画面の「Auth Mode」で「Host Based」を選択しておく必要があります。

Security > 802.1X > Reauthenticate Port(s) の順でクリックし、以下の画面を表示します。

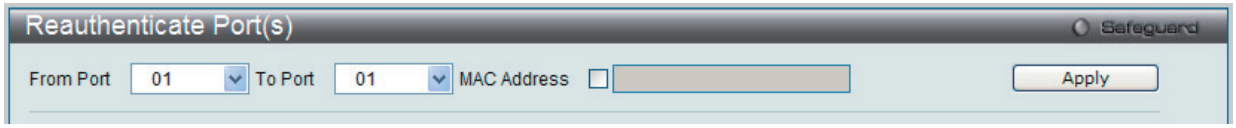


図 9-30　Reauthenticate Port(s)（Host ベース 802.1X）画面

「From Port」と「To Port」のプルダウンメニューでポートまたはポート範囲を選択し、「Apply」ボタンをクリックすることでポートの再認証を行います。MAC アドレスを編集するためには、「MAC Address」をチェックし、隣接する欄に再認証する MAC アドレスを入力します。「Apply」ボタンをクリックすることでポートの再認証を行います。

ポートの再認証画面では以下の情報が表示または設定できます。

項目	説明
From Port	再認証する開始ポートを選択します。
To Port	再認証する終了ポートを選択します。
MAC Address	対応ポートに接続しているスイッチの MAC アドレスです
Auth PAE State	Authenticator PAE の状態を以下の項目のいずれかで表示します。: Initialize、Disconnected、Connecting、Authenticating、Authenticated、Aborting、Held、ForceAuth、ForceUnauth および N/A
Backend State	Backend Authentication の状態を以下の項目のいずれかで表示します。: Request、Response、Success、Fail、Timeout、Idle、Initialize および N/A
Port Status	コントロールポートのステータスは Authorized、Unauthorized または N/A で表示します。

Authentic RADIUS Server（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。Web 管理用には 3 つの画面があります。

Security > 802.1X > Authentic RADIUS Server をクリックし、以下の画面を表示します。

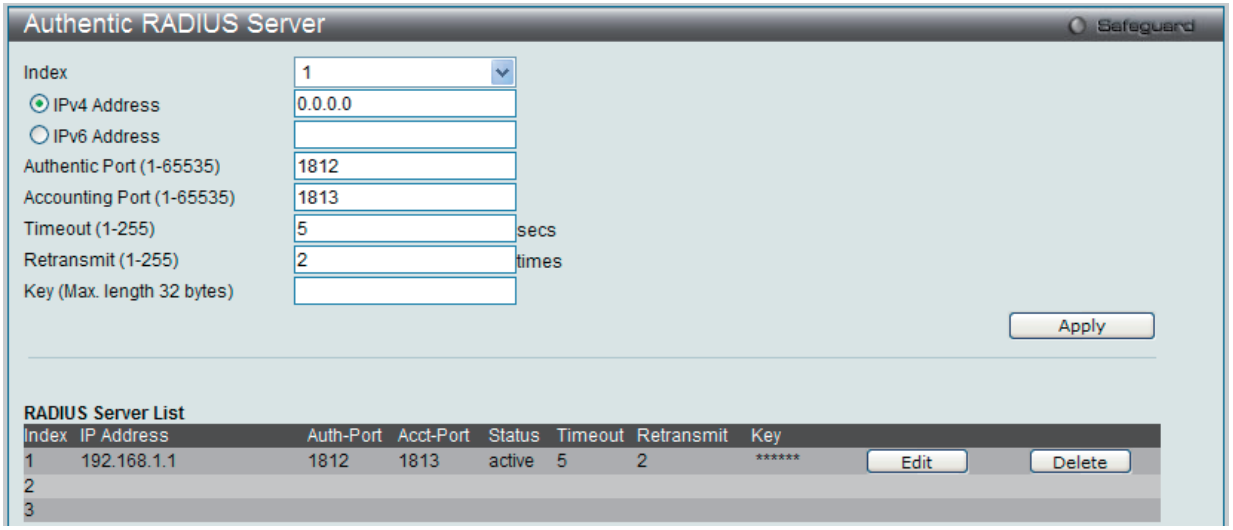


図 9-31　Authentic RADIUS Server 画面

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 また、「IPv4 Address」または「IPv6 Address」のいずれかを選択し、右側の欄に RADIUS サーバの IP アドレスを入力します。
Authentic Port (1-65535)	スイッチと RADIUS サーバ間で RADIUS データを通信するために使用する RADIUS 認証サーバの UDP ポートを指定します。初期値は 1812 です。
Accounting Port (1-65535)	スイッチと RADIUS サーバ間で RADIUS アカウンティング統計情報を通信するために使用する RADIUS アカウントサーバの UDP ポートを指定します。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。
Retransmit (1-255)	RADIUS サーバの再転送間隔（秒）を設定します。
Key (Max. length 32 bytes)	RADIUS サーバに設定したものと同一の鍵を指定します。

SSL Settings（Secure Socket Layer の設定）

Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、認証セッションに使用する厳密な暗号パラメータ、特定の暗号化アルゴリズムおよびキー長を決定する、暗号スイートと呼ばれるセキュリティ文字列により実現しています。SSL は、以下の 3 つの段階で構成されます。

1. 鍵交換
暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。

2. 暗号化
暗号スイートの次の段階は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
- ストリーム暗号 – スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとホスト間で一致させる必要があります。
- CRC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義する 3 DES EDE 暗号化コードをサポートし、暗号文を生成します。

3. ハッシュアルゴリズム
暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）の 2 種類のハッシュアルゴリズムをサポートします。

これら 3 つのパラメータは、スイッチ上での 4 つの選択肢として独自に組み合わされ、サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。本スイッチは、SSLv3 および TLSv1 をサポートしています。SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する場合があります。

「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。

本画面では、SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者の情報や認証のための鍵やデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバとクライアントが一致した証明書ファイルを持つ必要があります。スイッチは、拡張子 “.der” を持つ証明書のみをサポートします。スイッチは証明書が既にロードされている形で発送されますが、ユーザの環境によっては、さらにダウンロードが必要になる場合があります。

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。

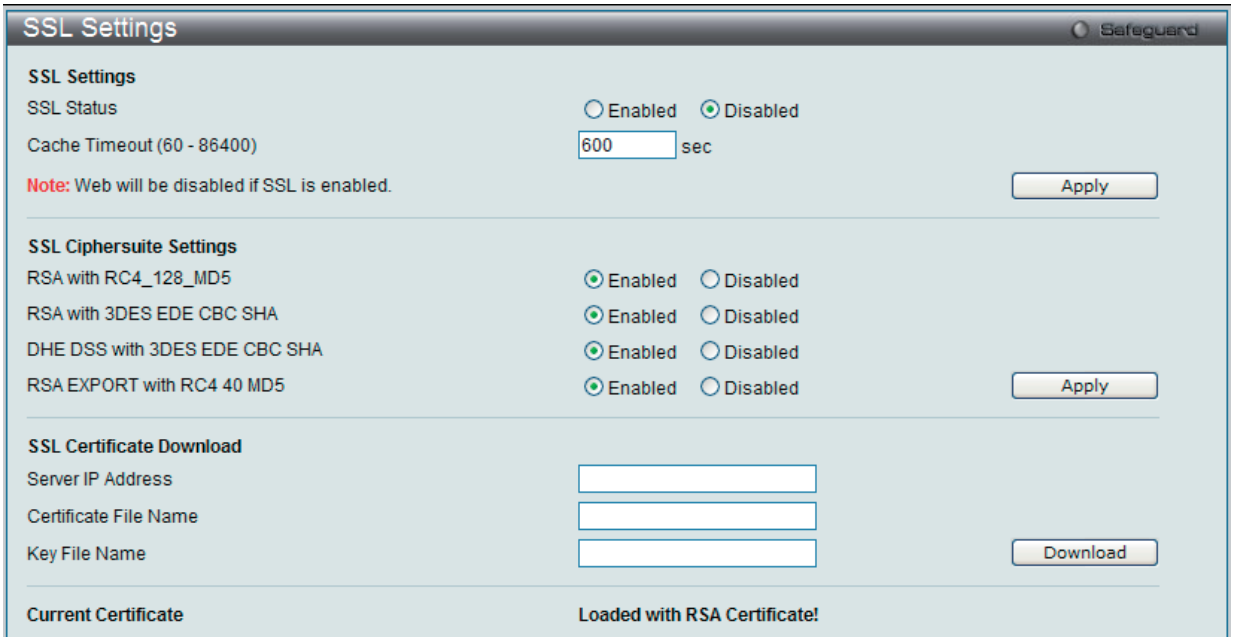


図 9-32　SSL Settings 画面

SSL 機能の設定

「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。

SSL 暗号スイート機能の設定

「SSL Ciphersuite Settings」セクションの項目を設定し、「Apply」ボタンをクリックします。

SSL 証明書のダウンロード

「SSL Certificate Download」セクションの項目を設定し、「Download」ボタンをクリックします。

項目	説明
SSL Settings	
SSL Status	スイッチの SSL の「Enabled」（有効）、「Disabled」（無効）を指定します。初期値は「Disabled」です。
Cache Timeout (60-86400)	クライアントとホストの間の SSL による新しい鍵交換の間隔を指定します。クライアントとホストが鍵交換をすると常に新しい SSL セッションが確立します。この値を長くすると SSL セッションによる特定のホストとの再接続には主鍵が再利用されます。それためネゴシエーション処理は速くなります。初期値は 600（秒）です。
SSL Ciphersuite Settings	
RSA with RC4_128_MD5	この暗号スイートは RSA key exchange、stream cipher C4（128-bit keys）、MD5 Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
RSA with 3DES EDE CBC SHA	この暗号スイートは RSA key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
DHS DSS with 3DES EDE CBC SHA	この暗号スイートは DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
RSA EXPORT with RC4 40 MD5	この暗号スイートは RSA Export key exchange、stream cipher RC4（40-bit keys）、MD5 Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
SSL Certificate Download	
Server IP Address	証明書のファイルがある TFTP サーバの 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 ベースマネー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。SSL の情報と機能についての詳しい情報については、「DGS-3200 シリーズ コマンドラインインタフェース（CLI）マニュアル」を参照してください。

注意　SSL 機能が有効になると Web ベースマネージメントは無効になります。再度本スイッチにログオンするには URL の最初を http:// で始まるアドレスを Web ブラウザのアドレスに指定してもエラーになり、認証はされません。

SSH（Secure Shell の設定）

SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。SSH は、リモートのホストコンピュータへの安全なログインや、リモートのエンドノードでの安全なコマンド実行メソッドを可能にし、信頼関係を結んでいないホスト間に暗号化と認証を利用した安全な通信を提供します。高度なセキュリティ機能を備えた SSH は、今日のネットワーク環境に必要不可欠なツールです。ネットワーク通信を脅かす数々のセキュリティハザードに対して、強力な監視者としての役割を担います。

リモート PC（SSH クライアント）とスイッチ（SSH サーバ）間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

1. **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 Configuration（SSH サーバ設定）

本画面は SSH サーバの設定および設定内容の確認に使用します。

Security > SSH > SSH Configuration の順にメニューをクリックします。

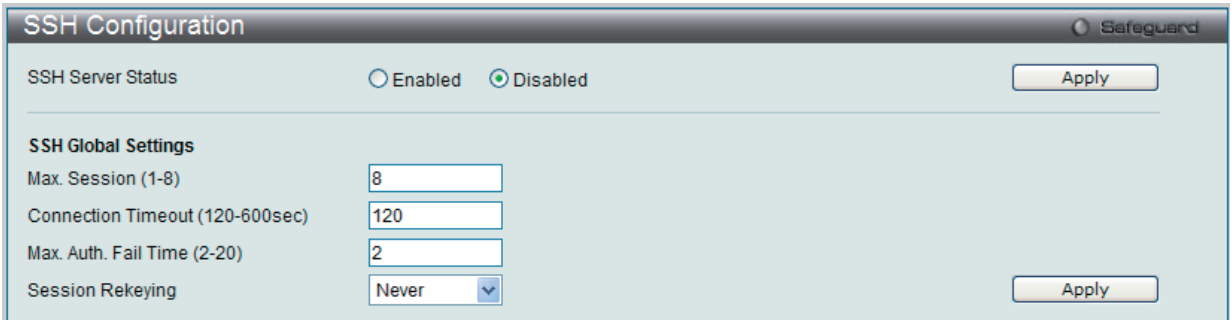


図 9-33　SSH Configuration 画面

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
SSH Server Status	スイッチ上で SSH 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Max Session (1-8)	同時にスイッチに接続できる数を 1 から 8 の数字を設定します。初期値は 8 です。
Connection Timeout (120-600 Sec)	接続のタイムアウト時間を指定します。120 から 600（秒）が指定できます。初期値は 120（秒）です。
Max. Auth. Fail Time (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。
Session Rekeying	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。

SSH Authmode and Algorithm Settings（SSH 認証モードとアルゴリズム設定）

本画面は、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 Authmode 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。

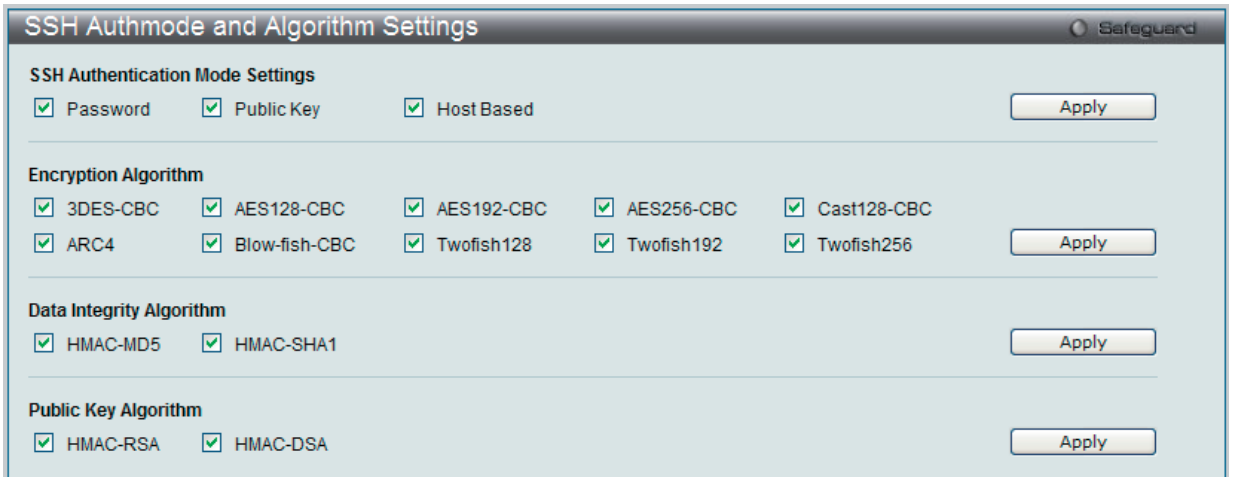


図 9-34　SSH Authmode and Algorithm Settings 画面

以下のアルゴリズムが設定できます。

項目	説明
SSH Authentication Mode Settings	
Password	スイッチにおける認証にローカルに設定したパスワードを使用する場合に「Enabled」（有効）にします。初期値は「Enabled」です。
Public Key	スイッチにおける認証に SSH サーバに設定した公開鍵を使用する場合に「Enabled」（有効）にします。初期値は「Enabled」です。
Host Based	認証にホストコンピュータを使用する場合に「Enabled」（有効）にします。本項目は SSH 認証機能を必要とする Linux ユーザ向けに設定されます。ホストコンピュータには SSH プログラムがインストールされ、Linux OS が起動している必要があります。初期値は「Enabled」です。
Encryption Algorithm	
3DES-CBC	CBC 方式で 3DES 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Blow-fish-CBC	CBC 方式で Blowfish 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES128-CBC	CBC 方式で AES128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES192-CBC	CBC 方式で AES192 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES256-CBC	CBC 方式で AES256 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
ARC4	ARC4 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Cast128-CBC	CBC 方式で Cast128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish128	Twofish128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish192	Twofish192 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish256	Twofish256 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Data Integrity Algorithm	
HMAC-SHA1	SHA1（セキュアハッシュ）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
HMAC-MD5	MD5（メッセージダイジェスト）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Public Key Algorithm	
HMAC-RSA	RSA 暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
HMAC-DSA	DSA（デジタル署名）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。

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

SSH User Authentication Mode（SSH ユーザ認証モード）

以下の画面では、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 Mode の順にメニューをクリックし、以下の画面を表示します。

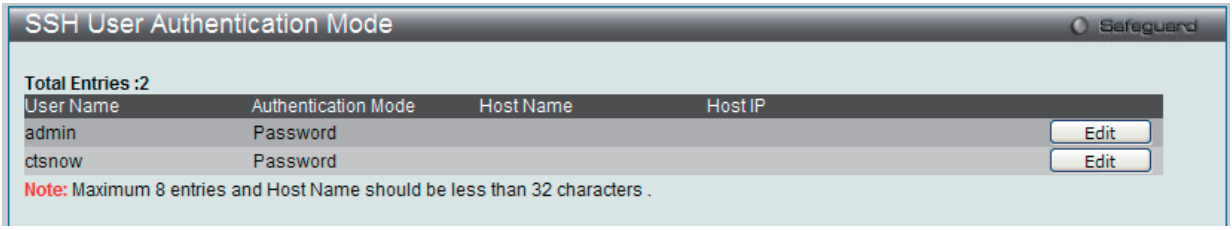


図 9-35　SSH User Authentication Mode 画面

上記画面例のユーザアカウント「ctsnow」は **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ます。

以下の項目を使用して、参照または設定を行います。

項目	説明
User Name	SSH ユーザを識別するユーザ名を 15 文字までの半角英数字で指定します。本ユーザ名はスイッチにユーザアカウントとして登録済みである必要があります。
Auth. Mode	スイッチにアクセスを試みるユーザの認証モードを以下から指定します。 • Host Based - 認証用にリモート SSH サーバを使用する場合に選択します。本項目を選択すると、SSH ユーザ識別のために以下の情報を入力することが必要になります。 　- Host Name - リモート SSH ユーザを識別する 31 文字までの半角英数字を入力します。 　- Host IP - SSH ユーザの IP アドレスを入力します。 • Password - 管理者定義のパスワードを使用して認証を行う場合に選択します。本項目を選択すると、スイッチは管理者にパスワードの入力（確認のため 2 回）を促します。 • Public Key - SSH サーバ上の公開鍵を使用して認証を行う場合に選択します。
Host Name	リモート SSH ユーザを識別する 31 文字までの半角英数字を入力します。本項目は「Auth. Mode」で「Host Based」を選択した場合のみ入力が必要です。
Host IP	SSH ユーザの IP アドレスを入力します。本項目は「Auth. Mode」で「Host Based」を選択した場合のみ入力が必要です。

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

注意　SSH User Authentication Mode の項目を設定するためには、事前にユーザアカウントを登録しておく必要があります。

Access Authentication Control（アクセス認証コントロール）

TACACS/ XTACACS/ TACACS+/ RADIUS コマンドは、TACACS/ XTACACS/ TACACS+ /RADIUS プロトコルを使用してスイッチへの安全なアクセスを可能にします。ユーザがスイッチへのログインや、管理者レベルの特権へのアクセスを行おうとする時、パスワードの入力を求められます。TACACS/ XTACACS/ TACACS+/ RADIUS 認証がスイッチで有効になると、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバと連絡し、ユーザの確認をします。確認が行われたユーザは、スイッチへのアクセスを許可されます。

現在 TACACS セキュリティプロトコルには異なるエンティティを持つ 3 つのバージョンが存在します。本スイッチのソフトウェアは TACACS の以下のバージョンをサポートします。

•TACACS（Terminal Access Controller Access Control System）
　セキュリティのためのパスワードチェック、認証、およびユーザアクションの通知を、1 台またはそれ以上の集中型の TACACS サーバを使用して行います。パケットの送受信には UDP プロトコルを使用します。
• XTACACS（拡張型 TACACS）
　TACACS プロトコルの拡張版で、TACACS プロトコルより多種類の認証リクエストとレスポンスコードに対応します。パケットの送受信に UDP プロトコルを使用します。
• TACACS+（Terminal Access Controller Access Control System plus）
　ネットワークデバイスの認証のために詳細なアクセス制御を提供します。TACACS+ は、1 台またはそれ以上の集中型のサーバを経由して認証コマンドを使用することができます。TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間のすべてのトラフィックを暗号化します。また、TCP プロトコルを使用して信頼性の高い伝達を行います。

TACACS/ XTACACS/ TACACS+/ RADIUS のセキュリティ機能が正常に動作するためには、スイッチ以外の認証サーバホストと呼ばれるデバイス上で認証用のユーザ名とパスワードを含む TACACS/ XTACACS/ TACACS+/ RADIUS サーバの設定を行う必要があります。スイッチがユーザにユーザ名とパスワードの要求を行う時、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバにユーザ認証の問い合わせを行います。サーバは以下の 3 つのうちの 1 つの応答を返します。

• サーバは、ユーザ名とパスワードを認証し、ユーザにスイッチへの通常のアクセス権を与えます。
• サーバは、入力されたユーザ名とパスワードを受け付けず、スイッチへのアクセスを拒否します。
• サーバは、認証の問い合わせに応じません。この時点でスイッチはサーバからタイムアウトを受け取り、メソッドリスト中に設定された次の認証方法へと移行します。

本スイッチには TACACS、XTACACS、TACACS+、RADIUS の各プロトコル用に 4 つの認証サーバグループがあらかじめ組み込まれています。これらの認証サーバグループはスイッチにアクセスを試みるユーザの認証に使用されます。認証サーバグループ内に任意の順番で認証サーバホストを設定し、ユーザがスイッチへのアクセス権を取得する場合、1 番目の認証サーバホストに認証を依頼します。認証が行われなければ、リストの 2 番目のサーバホストに依頼し、以下同様の処理が続きます。実装されている認証サーバグループには、特定のプロトコルが動作するホストのみを登録できます。例えば TACACS 認証サーバグループは、TACACS 認証サーバホストのみを登録できます。

スイッチの管理者は、ユーザ定義のメソッドリストに 6 種類の異なる認証方法（TACACS/ XTACACS/ TACACS+/ RADIUS/ local/ none）を設定できます。これらの方法は、任意に並べ替えることが可能で、スイッチ上での通常のユーザ認証に使用されます。リストには最大 8 つの認証方法を登録できます。ユーザがスイッチにアクセスしようとすると、スイッチはリストの 1 番目の認証方法を選択して認証を行います。1 番目の方法で認証サーバホストを通過しても認証が返ってこなければ、スイッチはリストの次の方法を試みます。この手順は、認証が成功するか、拒否されるか、またはリストのすべての認証方法を試し終わるまで繰り返されます。

スイッチへのアクセス権を取得したユーザは、通常のアクセス権を与えられていることにご注意ください。管理者特権レベルの権利を取得するためには、ユーザは「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

注意 TACACS、XTACACS、TACACS+、RADIUS は独立したエンティティであり、互換性はありません。スイッチとサーバ間は、同じプロトコルを使用した全く同じ設定を行う必要があります。（例えば、スイッチに TACACS 認証を設定した場合、ホストサーバにも同様の設定を行います。）

Authentication Policy and Parameter Settings（認証ポリシーとパラメータ設定）

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

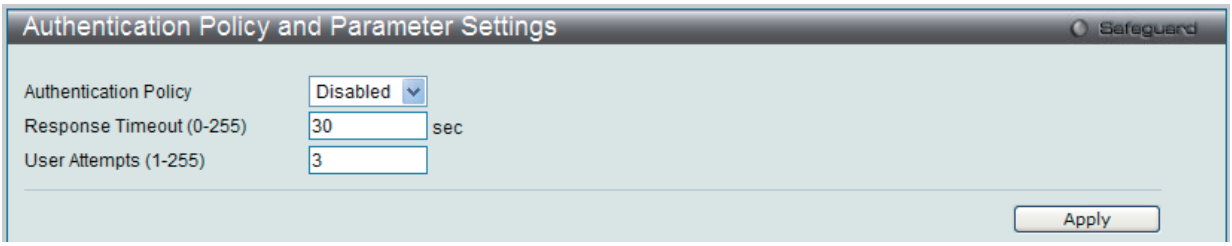


図 9-36　Authentication Policy and Parameter Settings 画面

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。
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、Web）を設定します。

Security > Access Authentication Control > Application Authentication Settings の順にクリックし、以下の画面を表示します。

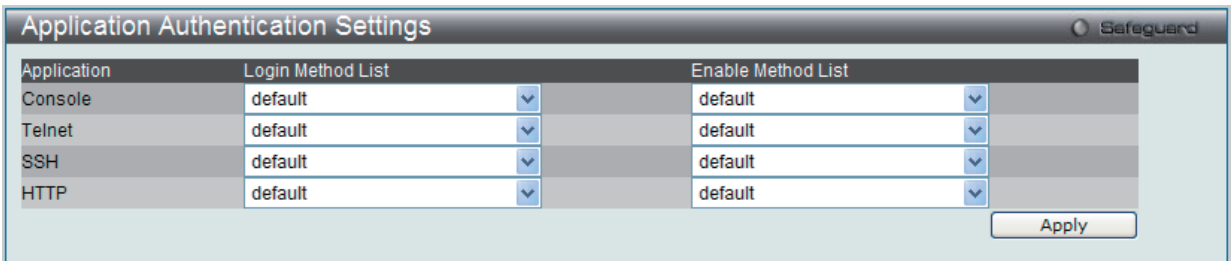


図 9-37　Application Authentication Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Application	スイッチ上の設定用アプリケーションをリスト表示しています。それぞれのアプリケーション（コンソール、Telnet、SSH、HTTP）を使用するユーザ認証用の「Login Method List」と「Enable Method List」を指定できます。
Login Method List	プルダウンメニューを使用し、登録済みのメソッドリストから、ユーザレベルの通常ログインを行うアプリケーションに適用するリストを選択します。初期設定のメソッドリスト、またはユーザ定義のメソッドリストを選択できます。詳細な情報は、後述の「Login Method Lists」画面を参照してください。
Enable Method List	プルダウンメニューを使用し、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」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。

Authentication Server Group（認証サーバグループ）

本画面では、スイッチ上に認証サーバグループの設定を行います。サーバグループとは、TACACS/ XTACACS/ TACACS+/ RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。プロトコルによって、または定義済みのサーバグループに組み込むことによりグループ分けを行います。スイッチには 4 つの認証サーバグループがあらかじめ組み込まれています。これらは削除することができませんが、内容の変更は可能です。1 つのグループにつき最大 8 個までの認証サーバホストを登録できます。

Security > Access Authentication Control > Authentication Server Group の順にメニューをクリックし、以下の画面を表示します。

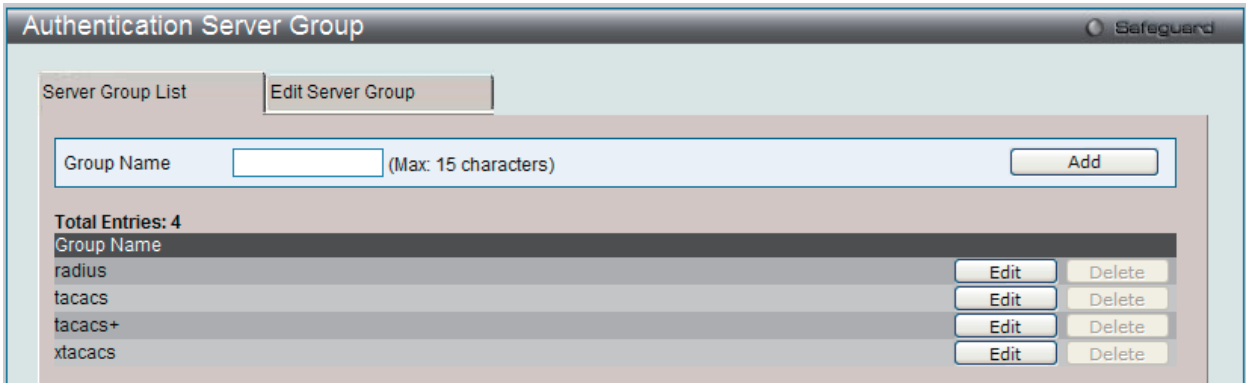


図 9-38　Authentication Server Group - Server Group List タブ画面

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。

サーバグループの新規登録

「Group Name」に名前を入力し、「Add」ボタンをクリックします。

サーバグループの編集

「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。

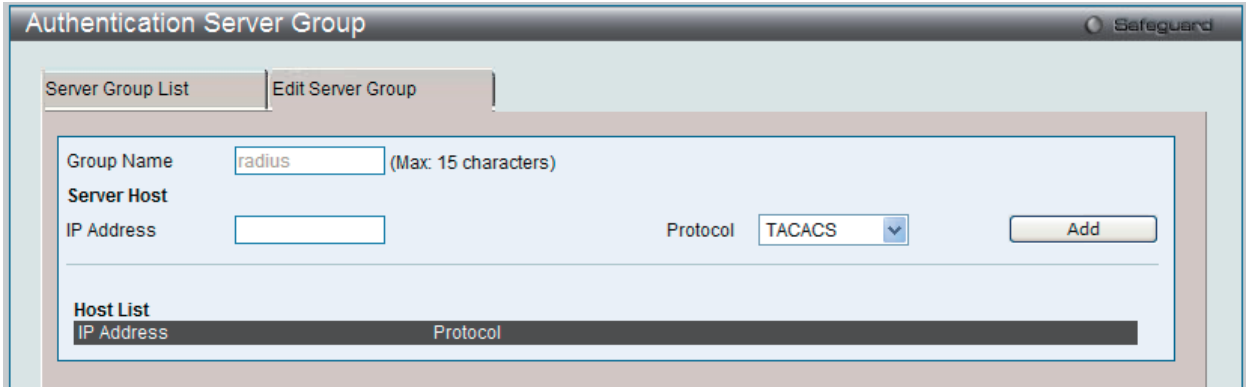


図 9-39　Authentication Server Group - Edit Server Group タブ画面

Authentication Server Host のリストへの追加

「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 を選択します。「Add」ボタンをクリックし、Authentication Server Host をグループに加えます。本タブの下部の 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 Hosts」画面にてホストの登録を行う必要があります。本機能を正しく動作させるためには、リモートの中央管理サーバ上でプロトコルを指定して認証サーバホストの設定を行う必要があります。

注意　あらかじめ組み込まれている 4 つのサーバグループには、同じ TACACS デーモンが起動されているサーバホストのみを入れることができます。TACACS/XTACACS/TACACS+ プロトコルは別のエンティティで、互換性はありません。

Authentication Server Host（認証サーバホスト）

本画面では、スイッチに TACACS/ XTACACS/ TACACS+/ RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを設定します。ユーザが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストに認証パケットを送信します。すると TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/ XTACACS/ TACACS+/ RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

Security > Access Authentication Control > Authentication Server Host の順にメニューをクリックし、以下の画面を表示します。

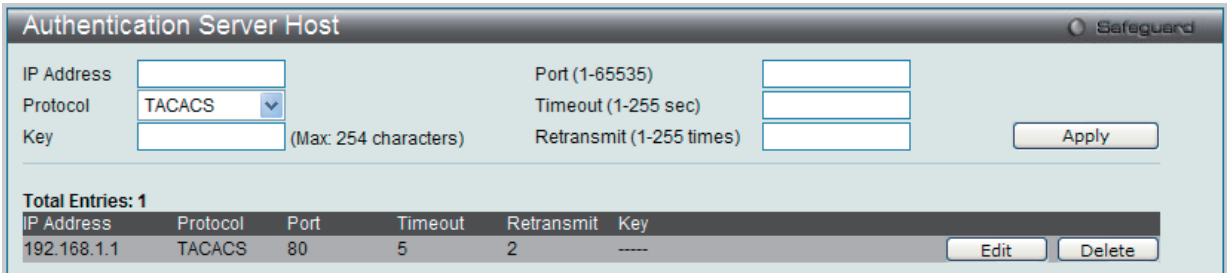


図 9-40　Authentication Server Host 画面

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	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 1813 です。独自の番号を設定してセキュリティを向上することも可能です。
Timeout (1-255 secs)	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 (1-255 times)	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。

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。

Login Method Lists（ログインメソッドリスト）

本メニューでは、ユーザがスイッチにログインする際の認証方法を規定するユーザ定義または初期設定のログインメソッドリストを設定します。本メニューで設定した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS-XTACACS-Local の順番で認証方法を指定すると、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに認証リクエストを送信します。そのサーバホストから応答がない場合、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリストの次の方法（XTACACS）を試します。それでも認証が行われなければ、スイッチ内に設定したローカルアカウントデータベースを使用して認証を行います。Local メソッドが使用される時、ユーザの権限はスイッチに設定されたローカルアカウントの権限に依存します。

これらの認証方法によって、認証に成功したユーザには「User」の権限のみが与えられます。ユーザが管理者レベルの権限を必要とするのであれば、「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。詳細については、175 ページの「Enable Admin（管理者レベルの認証）」を参照してください。

Security > Access Authentication Control > Login Method Lists の順にメニューをクリックし、以下の画面を表示します。

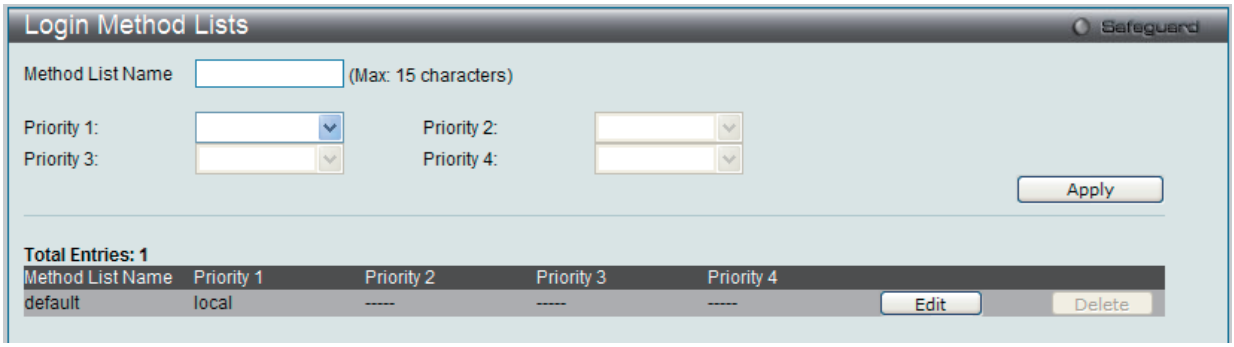


図 9-41　Login Method Lists 画面

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。

ユーザ定義の Login Method List 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。

Login Method List の変更

対応する「Edit」ボタンをクリックして行います。

Login Method List の新規登録

以下の項目を設定し、「Apply」ボタンをクリックします。

項目	説明
Method List Name	15 文字までの半角英数字でメソッドリスト名を入力します。
Priority 1, 2, 3, 4	本メソッドリストに追加する認証方法を最大 4 件まで指定します。 • tacacs – リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs – リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ – リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 • radius – リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 • 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。

Enable Method Lists（メソッドリストの有効化）

「Enable Method Lists」画面では、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 175 ページの「Configure Local Enable Password（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 の順にメニューをクリックし、以下の画面を表示します。

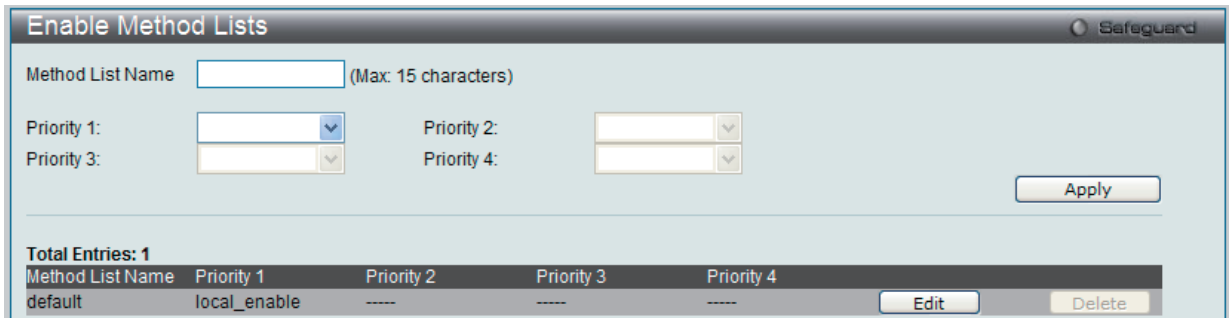


図 9-42　Enable Method Lists 画面

ユーザ定義の Enable メソッドリストの削除
対象の行で「Delete」ボタンをクリックします。

メソッドリストの変更
対応するメソッドリスト名の「Edit」ボタンをクリックして行います。

以下の項目を使用して、Enable Method List の設定を行います。入力後、「Apply」ボタンをクリックします。

項目	説明
Method List Name	15 文字までの半角英数字でメソッドリスト名を入力します。
Priority 1, 2, 3, 4	本メソッドリストに追加する認証方法を最大 4 件まで指定します。 • local_enable – スイッチ上のローカル Enable パスワードデータベースを使用してユーザ認証を行います。Local enable password は次セクションの 175 ページの「Configure Local Enable Password（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。

Configure Local Enable Password（ローカルユーザパスワード設定）

本画面では、「Enable Admin」コマンド用の Local Enable Password を設定します。ユーザがその権限をユーザレベルから管理者レベルに変更する際の認証方法に、「local_enable」を選択している場合、本画面でスイッチに登録したパスワードの入力が要求されます。

Security > Access Authentication Control > Configure Local Enable Password の順にメニューをクリックし、以下の画面を表示します。

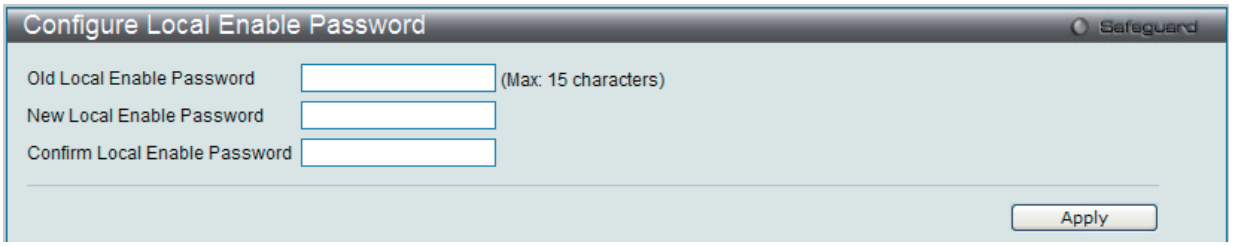


図 9-43　Configure Local Enable Password 画面

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。

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。

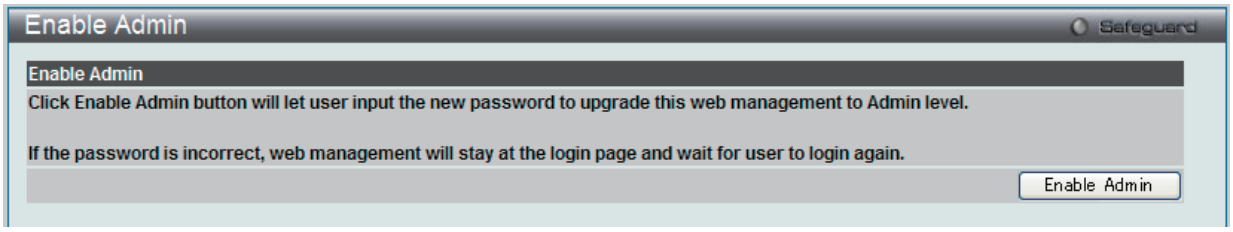


図 9-44　Enable Admin 画面

本画面を表示後、「Enable Admin」ボタンをクリックしてダイアログボックスを表示し、ユーザ名とパスワードを入力します。ユーザ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。

MAC-based Access Control（MAC アドレス認証）

MAC アドレス認証は、ポートまたはホストを使用してアクセスを認証および認可する方式です。本方式は、ポートベース MAC にはポートアクセス権を決定し、一方ホストベース MAC には MAC アクセス権を決定します。

ネットワークへのアクセスを許可する前に MAC ユーザが認証される必要があります。本スイッチは、ローカル認証とリモート RADIUS サーバ認証の両方の方法をサポートしています。MAC アドレス認証では、ローカルデータベースまたは RADIUS サーバデータベース内の MAC ユーザ情報が認証のために検索されます。認証結果に基づいて、ユーザは異なるレベルの許可を取得します。

MAC 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 の物理ポートごとに最大 200 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を MAC アドレス認証用に有効にすることはできません。

MAC-based Access Control Settings（MAC：MAC アドレス認証設定）

以下の画面では、スイッチの MAC アクセスコントロール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 Settings の順にメニューをクリックし、以下の画面を表示します。

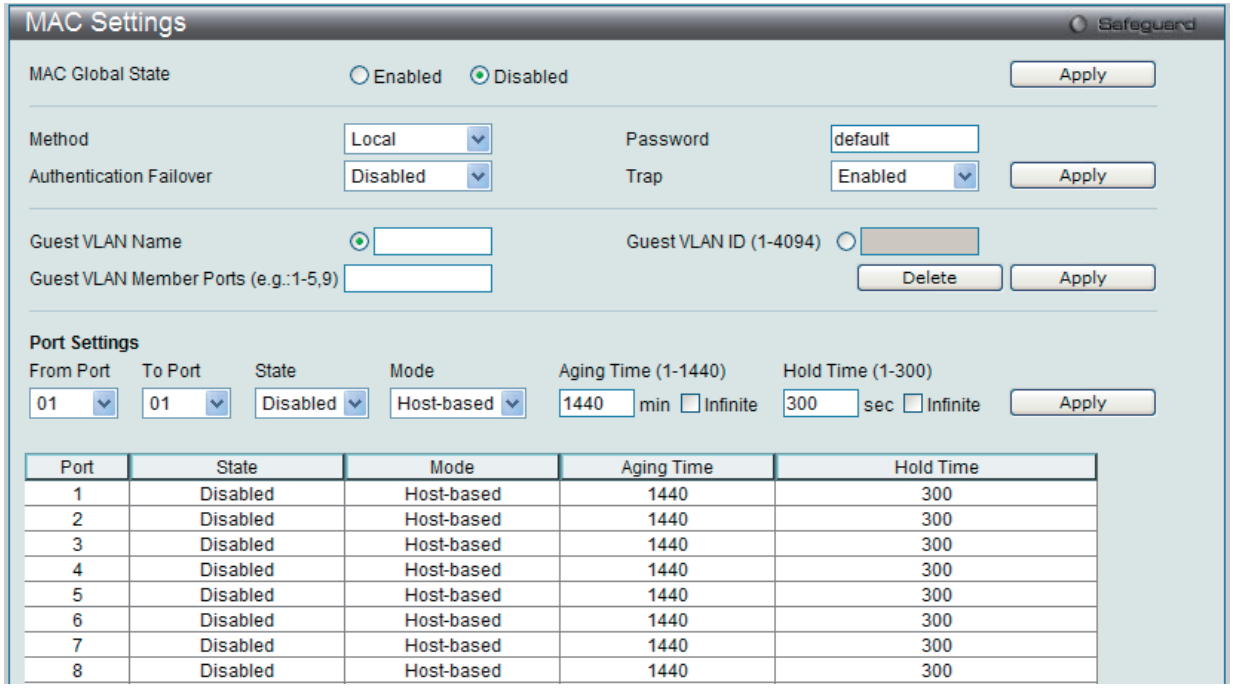


図 9-45　MAC Settings 画面

本画面は 4 つの主要なセクションに分かれています。
最初のセクションでは、MAC グローバル状態を設定します。2 つ目のセクションでは、認証に使用する方式を指定および設定します。3 つ目のセクションでは、ゲスト VLAN 設定を行い、4 つ目のセクションでは、MAC 設定を必要とするポートを設定します。

以下の項目を参照、または設定可能です。

項目	説明
MAC のグローバル設定	
MAC Global State	「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。

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。

認証方式の設定

以下の項目を設定します。

項目	説明
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	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。
Authentication Failover	初期値では認証フェイルオーバは無効です。RADIUS サーバに到達しないと、認証エラーとなります。認証フェイルオーバが有効で RADIUS サーバ認証には到達しない場合、ローカルデータベースを使用して認証を行います。
Trap	MAC アドレス認証トラップを有効または無効にします。 初期値は「Enabled」です。

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。

ゲスト VLAN の設定

以下の項目を設定します。

項目	説明
Guest VLAN Name	本機能で使用する設定済みのゲスト VLAN 名を表示します。
Guest VLAN ID (1-4094)	チェックして、ゲスト VLAN ID を入力します。
Guest VLAN Member Ports (e.g. : 1-5, 9)	ゲスト VLAN に設定されているポートリストを表示します。

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、ゲスト VLAN の設定を削除します。

ポート設定

以下の項目を設定します。

項目	説明
Port Settings	
From Port	MAC アドレス認証に設定されるポート範囲の開始ポート番号。
To Port	MAC アドレス認証に設定されるポート範囲の終了ポート番号。
State	選択したポートまたはポート範囲の MAC アドレス認証を「Enabled」（有効）または「Disabled」（無効）にします。
Mode	「Port Based」（ポートベース）または「Host Based」（ホストベース）を指定します。
Aging Time (1-1440)	エージングタイムを 1-1440（分）の範囲で設定します。初期値は 1440（分）です。隣接している「Infinite」をチェックして、エージングを無効にします。
Hold Time (1-300)	保持時間を 1-300（秒）の範囲で設定します。初期値は 300（秒）です。隣接している「Infinite」をチェックして、ホールドタイムを無効にします。

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。

MAC Local Settings（MAC アドレス認証ローカル MAC 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 Local Settings をクリックし、以下の画面を表示します。

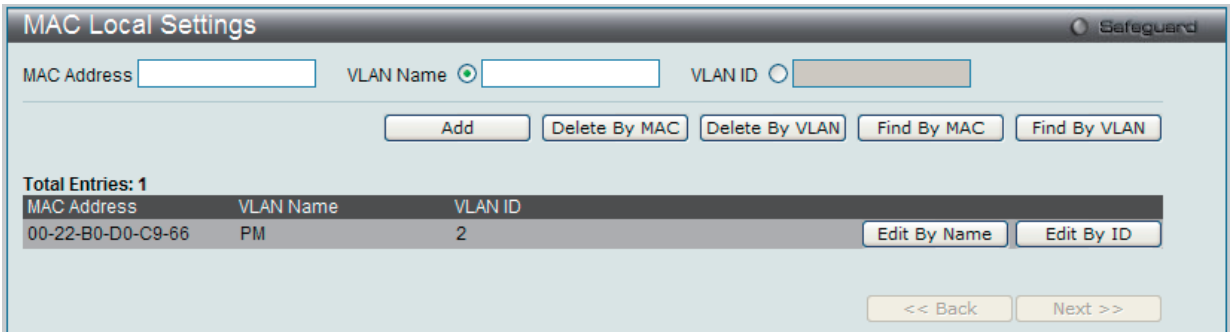


図 9-46　MAC Local Settings 画面

エントリの追加

MAC アドレスを Local Authentication List に追加するためには、「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。

エントリの変更

リストの MAC アドレスまたは VLAN を変更するためには、設定項目を適切な欄に入れて、「Edit」ボタンをクリックします。

エントリの削除

MAC アドレスエントリを削除するために、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 名を削除するためには、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。

エントリの検索

特定の MAC アドレスを検索するためには、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 名を検索するためには、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。

Web-based Access Control（WAC : WAC 設定）

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 プロトコルを使用します。Web ブラウザ経由で Web ページ (例 : http://www.dlink.com) の閲覧を行う場合に、スイッチは認証段階に進みます。スイッチは、HTTP パケットを検出し、このポートが未認証である場合に、ユーザ名とパスワードの画面を表示して、ユーザに問い合わせます。認証処理を通過するまで、ユーザはインターネットにアクセスすることはできません。

スイッチは、認証サーバとなってローカルデータベースに基づく認証を行うか、または RADIUS クライアントとなってリモート RADIUS サーバと共に RADIUS プロトコルを介する認証処理を実行します。Web へのアクセスを試みることによって、クライアントユーザは WAC の認証処理を開始します。

D-Link の WAC の実行には、WAC 機能が排他的に使用し、スイッチの他のモジュールに知られていない仮想 IP を使用します。実際は、スイッチの他の機能への影響を避ける場合にだけ、WAC は仮想 IP アドレスを使用してホストとの通信を行います。そのため、すべての認証要求を仮想 IP アドレスに送信し、スイッチの物理インタフェースの IP アドレスには送信しないようする必要があります。

ホスト PC が仮想 IP 経由で WAC スイッチと通信する場合、仮想 IP は、スイッチの物理的な IPIF(IP インタフェース) アドレスに変換されて通信を可能にします。ホスト PC と他のサーバの IP 構成は WAC の仮想 IP に依存しません。仮想 IP は、ICMP パケットまたは ARP リクエストに応答しません。つまり、仮想 IP は、スイッチの IPIF(IP インタフェース) と同じサブネット、またはホスト PC のサブネットと同じサブネットには設定することはできません。

認証済みおよび認証中のホストから仮想 IP に送信されるすべてのパケットがスイッチの CPU にトラップされるため、仮想 IP が他のサーバまたは PC と同じであると、WAC が有効なポートに接続するホストは、IP アドレスを実際に所有しているサーバまたは PC とは通信ができません。ホストがサーバまたは PC にアクセスする必要がある場合、仮想 IP をサーバまたは PC の 1 つと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、PC のユーザは、認証を適切に実行するために、プロキシ設定の例外として仮想 IP を加える必要があります。仮想 IP を指定するかどうかに関わらず、ユーザはスイッチのシステム IP を経由して WAC ページにアクセスします。仮想 IP を指定しない場合、認証中の Web のリクエストは、スイッチのシステム IP にリダイレクトされます。

スイッチの WAC の実行は、ユーザ定義のポート番号により HTTP または HTTPS プロトコルのいずれかに対して TCP ポートを設定できることを特徴としています。HTTP か HTTPS に対するこの TCP ポートは、認証処理のために CPU にトラップされる HTTP か HTTPS パケットを識別するためやログインページにアクセスするために使用されます。指定しない場合、HTTP に対するポート番号の初期値は 80、HTTPS に対するポート番号の初期値は 443 となります。プロトコルも指定されないと、プロトコルの初期値は HTTP になります。

以下の図は、Web 認証処理を成功させるために通過する基本的な 6 段階を示しています。

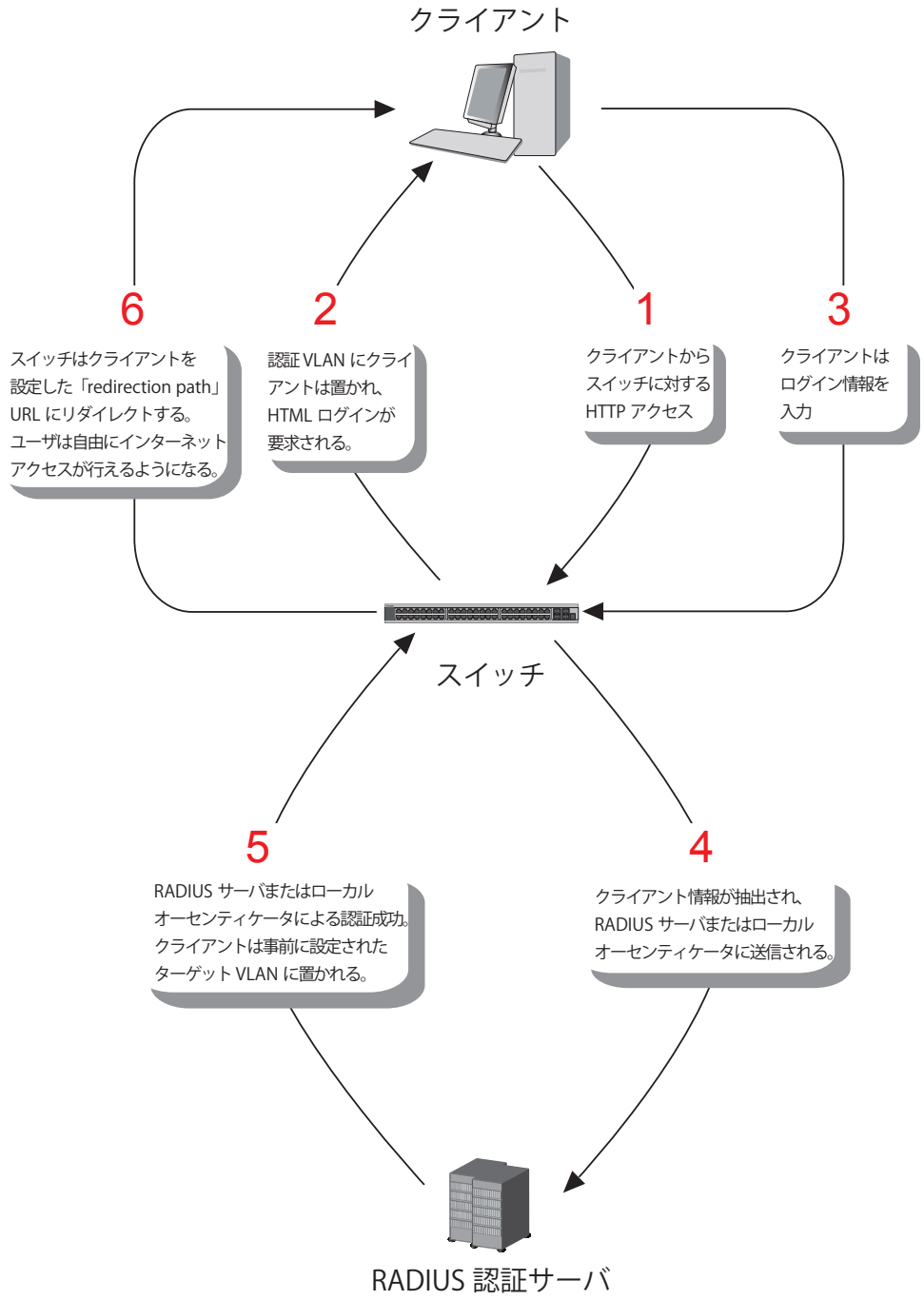


図 9-47　Web 認証処理に成功するために通過する 6 つの基本的な設定

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、スイッチの Web 認証を有効にする前に、ターゲット VLAN を含む必要なパラメータを入力して RADIUS サーバの設定を行います。
4. WAC/JWAC 認証では、System インタフェースが Up している必要があります。

WAC Global Settings（WAC グローバル設定）

スイッチに Web 認証設定を行います。

Security > Web-based Access Control (WAC) > WAC Global Settings をクリックして、以下の画面を表示します。

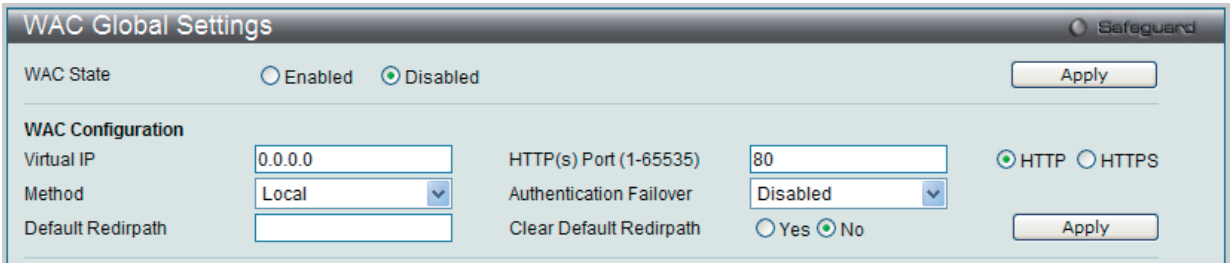


図 9-48　WAC Global Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
WAC State	Web ベースアクセスコントロール機能を「Enabled」（有効）/「Disabled」（無効）にします。隣接する「Apply」ボタンをクリックし、新しい設定を適用します。
Virtual IP	仮想 IP アドレスを入力します。このアドレスは、WAC に使用されるだけで、スイッチの他のモジュールが知ることはありません。
HTTP(s) Port (1-65535)	HTTP ポート番号を入力します。ポート番号の初期値は 80 です。
Method	プルダウンメニューを使用して、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以下の 2 つから選択します。 • 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「Web Authentication User Settings」画面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「RADIUS User Settings」画面（**Security > Web-based Access Control (WAC) > WAC User Server**）を使用して、事前に設定しておく必要があります。
Authenticating Failover	WAC 認証フェイルオーバを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。RADIUS サーバが無反応の場合、認証エラーとなります。認証フェイルオーバが有効な場合に RADIUS サーバ認証が無反応であるとローカルデータベースが認証のために使用されます。
Default Redirpath	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。この入力は、Web ベースアクセスコントロールを有効にする前に必ず行われている必要があります。
Clear Default Redirpath	ラジオボタンを使用し、認証に成功した場合にクライアントを別の URL に誘導するかどうかを指定します。 • Yes - クライアントは認証成功後に「Default Redirpath」欄で指定した URL にリダイレクトされます。 • No - クライアントは認証成功後に別の URL にリダイレクトされません

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。

注意 本機能を有効にするには、「Default Redirpath」欄に、ユーザがターゲット VLAN に割り当てられた際に導かれるサイトの URL が入力されていなければなりません。本入力を行わずに「Apply」ボタンをクリックすると、エラーメッセージが表示され、本機能を有効にできません。（URL の形式例 : http(s)://www.dlink-jp.com/）

注意 認証 VLAN の IP インタフェースのサブネットは、クライアントのものと一致している必要があります。この設定が正しく行われないと、クライアントは認証を拒否されます。

注意 認証に成功すると、クライアントは事前に設定したサイトへ誘導されます。このサイトが開かなくても「Fail」メッセージが表示されない場合は、そのクライアントは既に認証されています。その場合はブラウザの画面を更新するか、他の Web サイトへ接続してみてください。

WAC User Settings（WAC ユーザ設定）

スイッチによる 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。

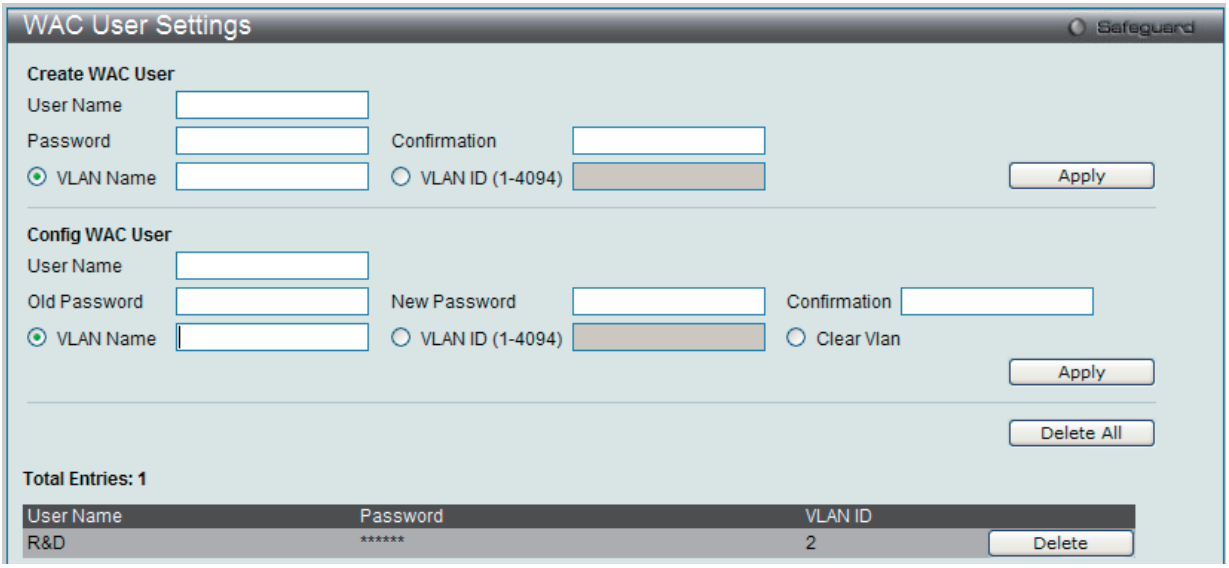


図 9-49　WAC User Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Create WAC 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。
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。
Confirmation	上記パスワードを再度入力します。
Config WAC User	
User Name	本プロセスを通じ、ゲスト認証するユーザのユーザ名を選択します。認証されると、制限付きの権利で設定済みの VLAN に割り当てられます。
Old Password	現在のパスワードを入力します。
New Password	新しいパスワードを入力します。
Confirmation	確認のために再度同じパスワードを入力します。
VLAN Name	作成済みの VLAN から、上記ユーザが認証に成功した Web ユーザに割り当てる VLAN 名を指定します。
VLAN ID (1-4094)	先頭のラジオボタンをクリックして VLAN ID を入力します。

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 Port Settings（WAC ポート設定）

Web 認証のためポート設定の表示またはポート設定を行います。

Security > Web-based Access Control (WAC) > WAC Port Settings の順にメニューをクリックし、以下の画面を表示します。

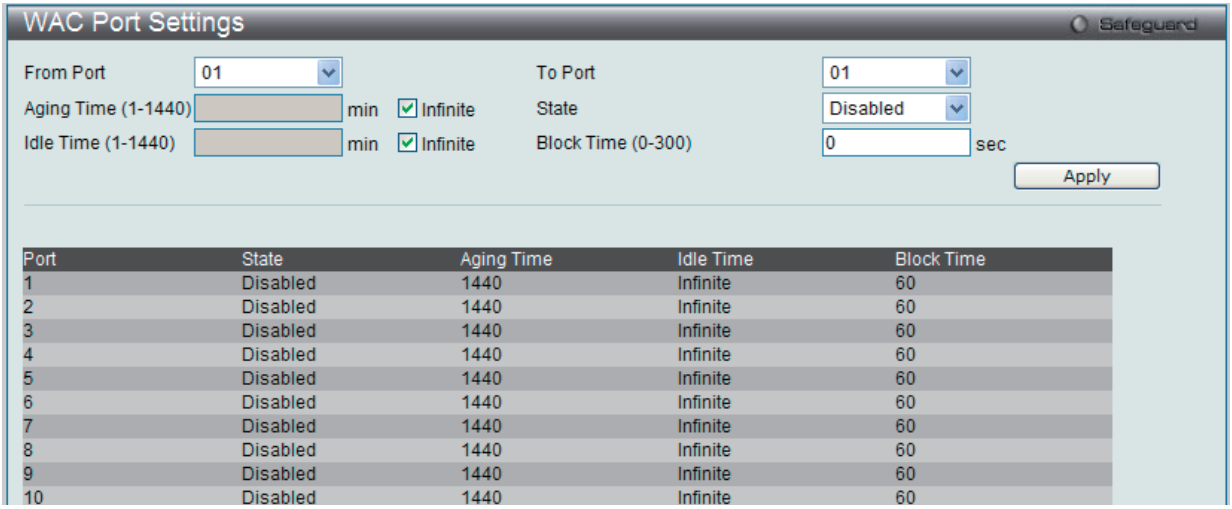


図 9-50　WAC Port Settings 画面

スイッチの各ポートに WAC 設定を行うには、以下の項目を指定します。

項目	説明
From Port / To Port	プルダウンメニューを使用して WAC ポートとして有効にするポート範囲を指定します。
Aging Time (1-1440)	認証ホストが認証状態を保つ時間を指定します。0-1440（分）の範囲で指定します。0 は、認証ホストがポート上でエージングしないことを示しています。初期値は 1440 分（24 時間）です。隣接している「Infinite」をチェックしてエージングを無効にします。
State	プルダウンメニューを使用して WAC ポートとして設定するポートを有効にします。
Idle Time (1-1440)	本設定時間にトラフィックがない場合、ホストは未認証状態に戻ります。0-1440（分）の範囲で指定します。0 を指定すると、ポート上の認証ホストのアイドル状態がチェックされません。隣接している「Infinite」をチェックするとアイドルタイムが無効になります。初期値は「infinite」です。
Block Time (0-300)	認証に失敗した後にホストがブロック状態を維持する期間を指定します。1-300（秒）の範囲で指定します。初期値は 30（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。

Japanese Web-based Access Control（JWAC : JWAC 設定）

「Japanese Web-based Access Control (JWAC)」フォルダには次のメニューがあります。:「JWAC Global Settings」、「JWAC Port Settings」、「JWAC User Settings」、「JWAC Customize Page Language」、および「JWAC Customize Page」

注意 WAC/JWAC 認証では、System インタフェースが Up している必要があります。

JWAC Global Settings（JWAC グローバル設定）

スイッチにおける JWAC（Japanese Web-based Access Control）の有効化および設定をします。

JWAC と Web 認証が相互に排他的な機能であり、それらを同時に使用することができませんのでご注意ください。JWAC 機能を使用するためには、PC ユーザは、2 段階の認証を通過する必要があります。最初のステップは、検疫サーバで検疫を行い、2 番目のステップでユーザ認証が行われます。2 番目のステップは、ホストが認証を通過した後にポートの VLAN メンバシップ変更がないという点を除き、Web 認証に似ています。RADIUS サーバは、802.1X コマンドセットによって定義されたサーバ設定を共有します。

スイッチに JWAC グローバル設定を行うためには、**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。

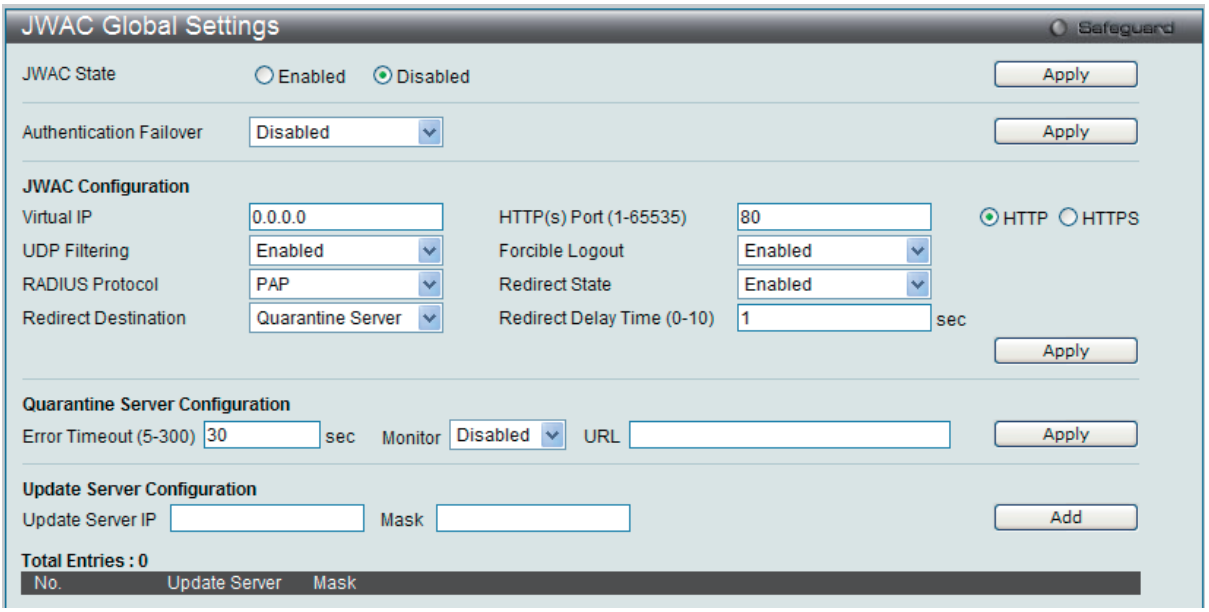


図 9-51　JWAC Global Settings 画面

以下の項目を設定可能です。

項目	説明
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。
Authentication Failover	「Enabled」(有効)/「Disabled」(無効) にします。JWAC 認証フェイルオーバを設定するために使用されます。初期値では認証フェイルオーバは無効です。RADIUS サーバに到達しないと、認証エラーとなります。認証フェイルオーバが有効な場合に RADIUS サーバ認証には到達せずローカルデータベースが認証のために使用されます。
JWAC Configuration	
Virtual IP	未認証ホストから認証リクエストを受け入れるために使用する JWAC バーチャル IP アドレスを指定します。この IP に送信されたリクエストだけが正しい応答を取得します。 注意 この IP は、ARP リクエストまたは ICMP パケットには応答しません。
HTTP(s) Port (1-65535)	JWAC スイッチがリッスンし、認証プロセスを終了するために使用する TCP ポートを指定します。
UDP Filtering	JWAC UDP フィルタリングを「Enabled」（有効）/「Disabled」（無効）にします。本項目を「Enabled」にすると、DHCP と DNS を除く未認証ホストからの UDP と ICMP パケットは破棄されます。
Forcible Logout	JWAC Forcible Logout を「Enabled」（有効）/「Disabled」（無効）にします。「Enabled」の場合、認証ホストから JWAC スイッチに TTL=1 を持つ ping パケットはログアウトリクエストと見なされ、ホストは未認証状態に戻ります。
Radius Protocol	JWAC に使用される RADIUS プロトコルを指定し、RADIUS 認証を完了します。: Local、EAP MD5、PAP、CHAP、MS CHAP および MS CHAPv2

項目	説明
Redirect State	JWAC リダイレクト機能を「Enabled」（有効）/「Disabled」（無効）にします。リダイレクト検疫サーバが「Enabled」な場合、ランダムな URL にアクセスしようとすると、未認証ホストは検疫サーバにリダイレクトされます。リダイレクト先に JWAC Login Page を指定した場合、未認証ホストは、スイッチの JWAC Login Page にリダイレクトされ、Web 認証画面に移行します。リダイレクトが無効な場合、未認証ユーザは検疫サーバへのアクセスと未認証ホストからの JWAC Login Page だけが許可され、他のすべての Web アクセスは拒否されます。 注意 Quarantine Server（検疫サーバ）へのリダイレクトを有効にする場合、はじめに検疫サーバを設定する必要があります。
Redirect Destination	未認証ホストがリダイレクト Quarantine Server または JWAC Login Page のいずれかにリダイレクトされるかを指定します。
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。
Quarantine Server Configuration	
Error Timeout (5-300)	Quarantine Server のエラータイムアウトを設定します。Quarantine Server モニタが有効な場合、JWAC スイッチは、定期的に検疫が問題なく動作するかどうかをチェックします。スイッチが設定された時間に Quarantine Server から応答を受信しないと、スイッチは適切に動作していないと見なします。5-300（秒）で指定します。
Monitor	JWAC Quarantine Server モニタを「Enabled」（有効）/「Disabled」（無効）にします。「Enabled」な場合、JWAC スイッチは、サーバが問題ないことを保証するために Quarantine Server をモニタします。スイッチが Quarantine Server を検出しないと、リダイレクトが有効で、「Redirect Destination」が「Quarantine Server」に設定されている場合、強制的に JWAC Login Page に未認証のすべての HTTP アクセスをリダイレクトします。
URL	JWAC Quarantine Server URL を指定します。リダイレクトが有効で、未認証ホストが HTTP リクエストパケットをランダムな Web サーバに送信する場合、「Redirect Destination」が「Quarantine Server」であると、スイッチは、この HTTP パケットを処理し、設定された URL を持つ Quarantine Server へのアクセスを許可するためにホストにメッセージを送り返します。コンピュータが指定 URL に接続している場合、Quarantine Server は、ユーザ名とパスワードの入力をユーザにリクエストし、認証プロセスを完了します。
Update Server Configuration	
Update Server IP	更新用サーバの IP アドレスを指定します。
Mask	サーバ IP アドレスのネットマスクを指定します。

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。

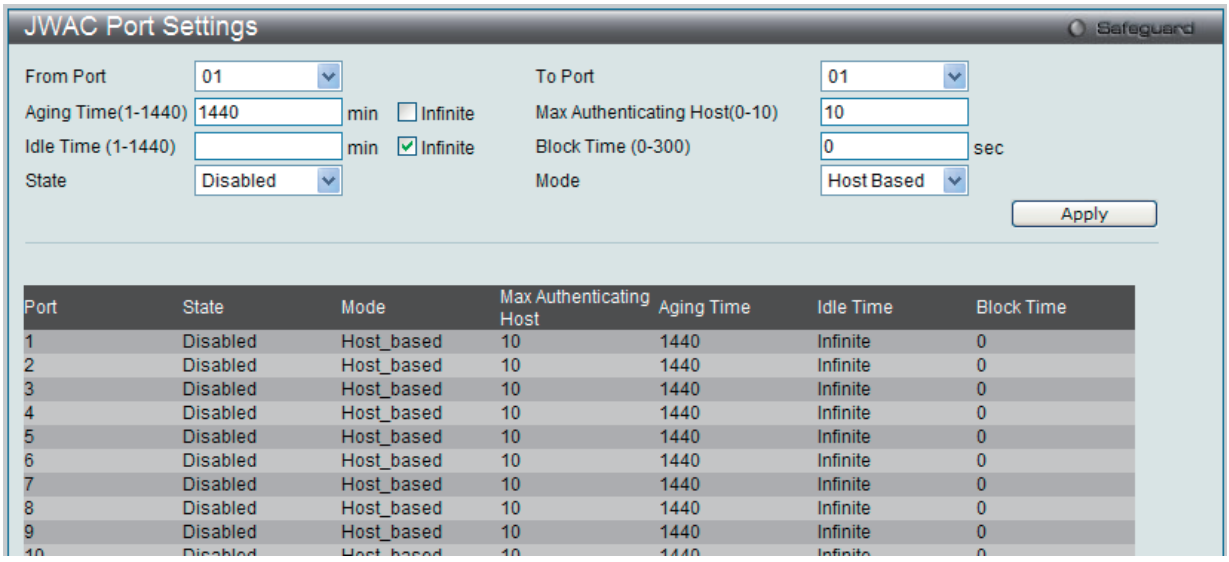


図 9-52　JWAC Port Settings 画面

スイッチの各ポートに JWAC を設定するためには、以下の項目を設定します。

項目	説明
From Port	JWAC ポートとして有効になるポート範囲の開始ポートをプルダウンメニューから選択します。
To Port	JWAC ポートとして有効になるポート範囲の終了ポートをプルダウンメニューから選択します。
Aging Time (1-1440)	認証ホストが認証状態を保つ時間を 0-1440（分）の範囲で指定します。「Infinite」または 0 を指定すると、認証ホストは、ポートにエージングを行いません。初期値は 1440（分）です。
Max Authenticating Host (1-10)	同時に各ポートに許可されるホストの認証処理の試みの最大数 1-10（回）を指定します。初期値は 10 です。

項目	説明
Idle Time (1-1440)	本設定時間にトラフィックがない場合、ホストは未認証状態に戻ります。値を変更するためには「Infinite」のチェックを外して 0-1440（分）で指定します。「Infinite」を指定すると、ポート上の認証ホストのアイドル状態がチェックされません。初期値は「Infinite」です。
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。
Mode	「Host Based」（ホストベース）または「Port Based」（ポートベース）を指定します。
State	JWAC ポートとして設定されたポートを「Enabled」（有効）または「Disabled」（無効）にします。

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

JWAC User Settings（JWAC ユーザ設定）

JWAC ユーザ設定をするためには、**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。

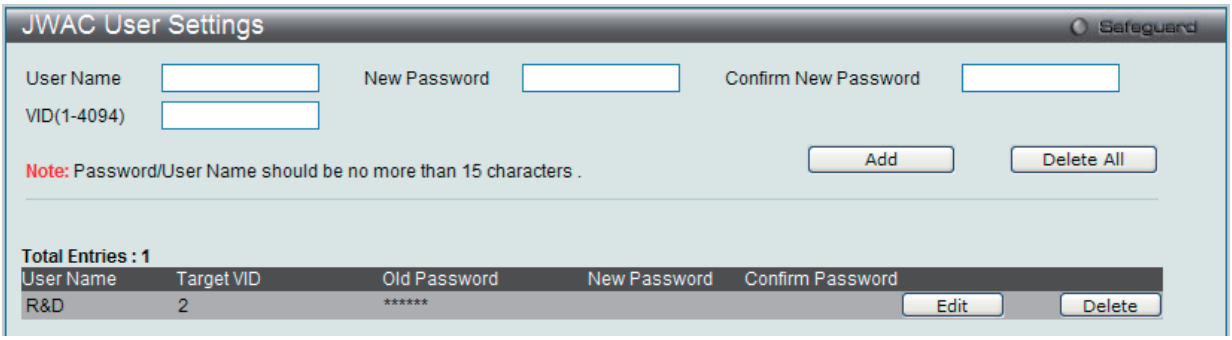


図 9-53　JWAC User Settings 画面

スイッチが JWAC にユーザアカウント設定をするためには、以下の項目を入力後、「Add」ボタンをクリックします。

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

変更するエントリの「Edit」ボタンをクリックします。

項目	説明
User Name	半角英数字 15 文字以内でユーザ名を入力します。
New Password	管理者が選択ユーザのために設定するパスワードを英数字（大文字小文字の区別あり）で入力します。
Confirm New Password	上記で入力したパスワードを再度入力します。
VID(1-4094)	VLAN ID 番号（1-4094）を入力します。

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 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。

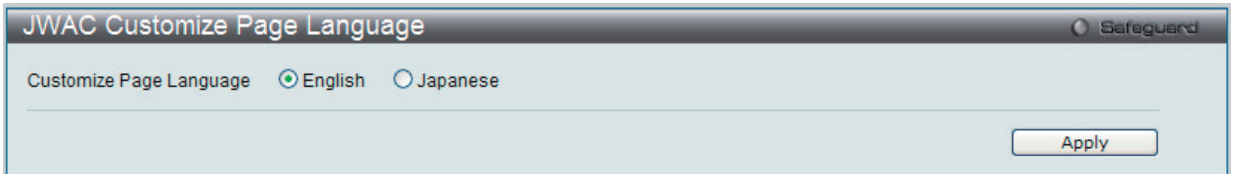


図 9-54　JWAC Customize Page Language 画面

JWAC 画面に使用する言語を設定するためには、「English」または「Japanese」のボタンをクリックし、「Apply」ボタンをクリックして、変更を保存します。

JWAC Customize Page（JWAC 画面のカスタマイズ）

JWAC 画面の設定を行います。

Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

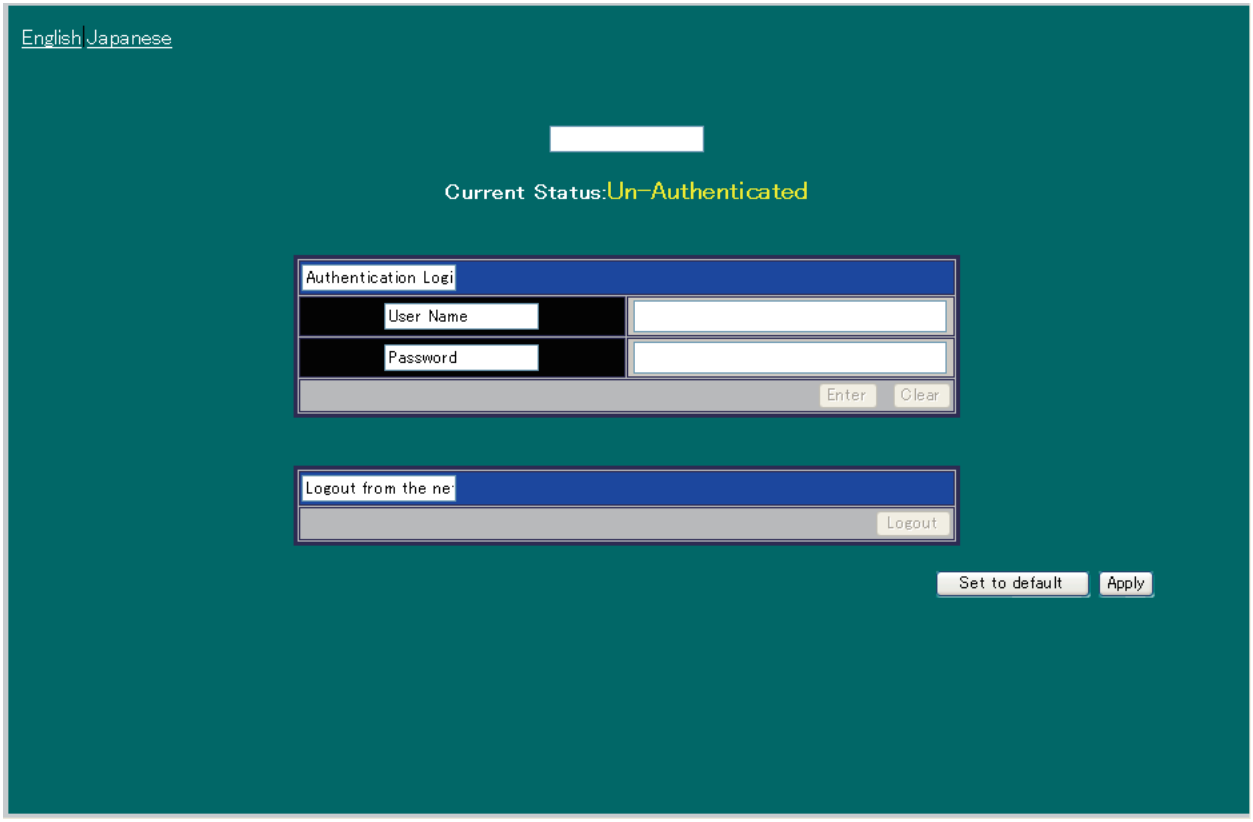


図 9-55　JWAC Customize Page 画面（English）

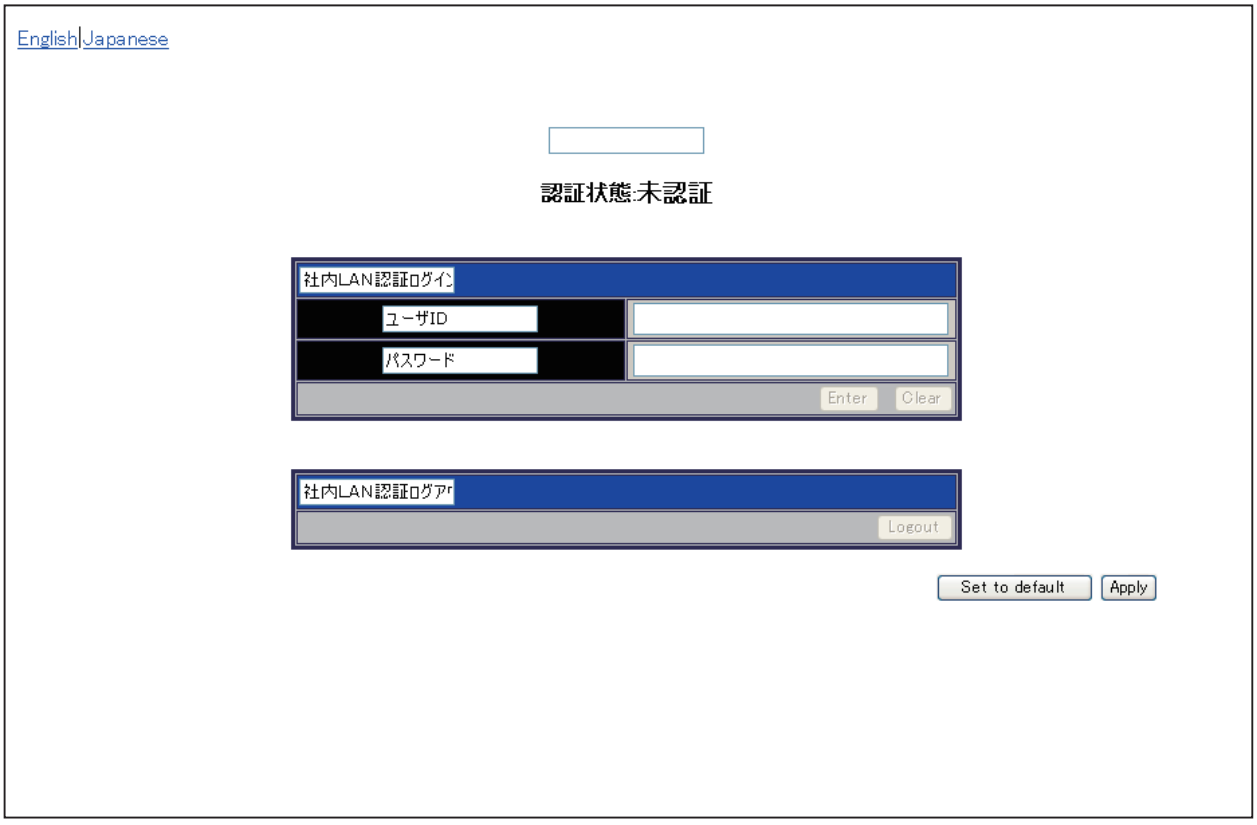


図 9-56　JWAC Customize Page 画面（Japanese）

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。

Multiple Authentication（マルチプル認証方式）

新しいネットワークでは多くの認証方式を採用しています。本製品は、IEEE 802.1X、MAC アドレス認証 (MBAC)、Web ベースアクセスコントロール（WAC）、JWAC、および IP-MAC- ポートバインディング（IMPB）を含むマルチプル認証方式をサポートしています。マルチプル認証機能により、クライアントは同一のスイッチポートで異なる認証方式を実行しネットワークに接続することが可能です。

マルチプル認証機能は以下のモードから 1 つ選択して実行します。

Any（MAC、802.1X、または WAC）モード

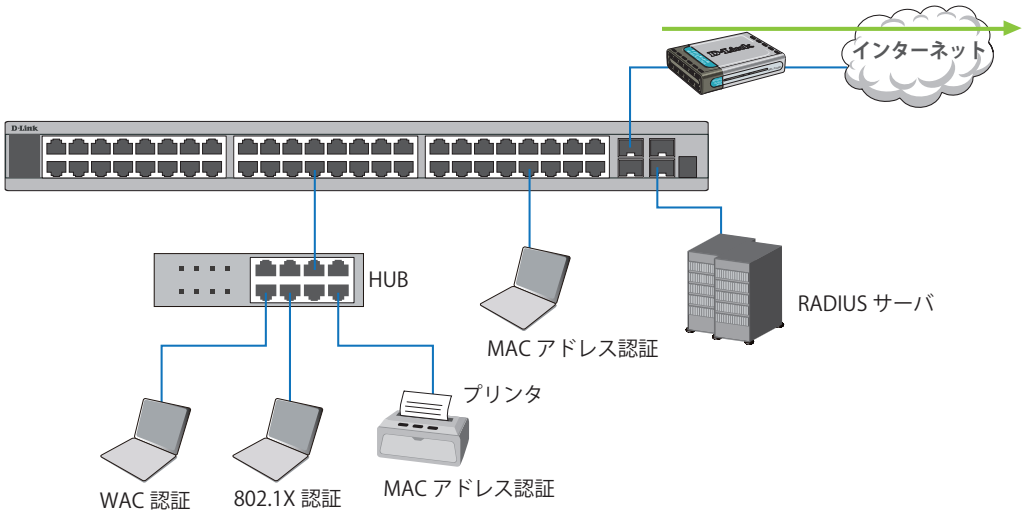


図 9-57　Any（MAC、802.1X、または WAC）モードの図

上の図では、スイッチポートは 802.1X、MAC アドレス認証、または WAC を使用して認証を行うことができるように設定されています。クライアントがネットワークに接続を試みると、本製品はこれらの認証方式のうち 1 つを使用してクライアントの認証を行い、認証されるとそのクライアントはネットワークに接続することができます。

Any（MAC、802.1X、または JWAC）モード

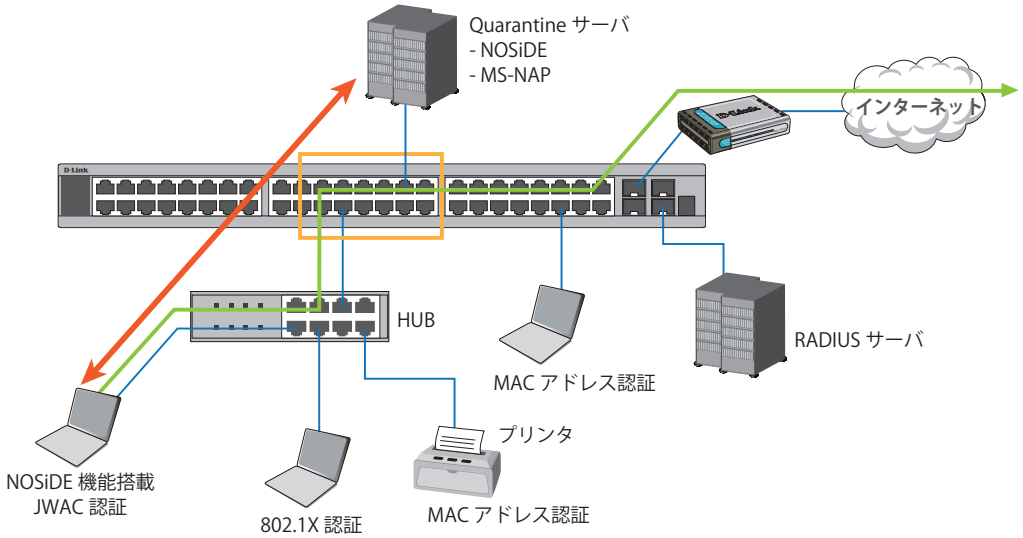


図 9-58　Any（MAC、802.1X、または JWAC）モードの図

上の図では、スイッチポートは 802.1X、MAC アドレス認証、または JWAC を使用して認証を行うことができるように設定されています。クライアントがネットワークに接続を試みると、本製品はこれらの認証方式のうち 1 つを使用してクライアントの認証を行い、認証されるとそのクライアントはネットワークに接続することができます。

802.1X & IMPB モード

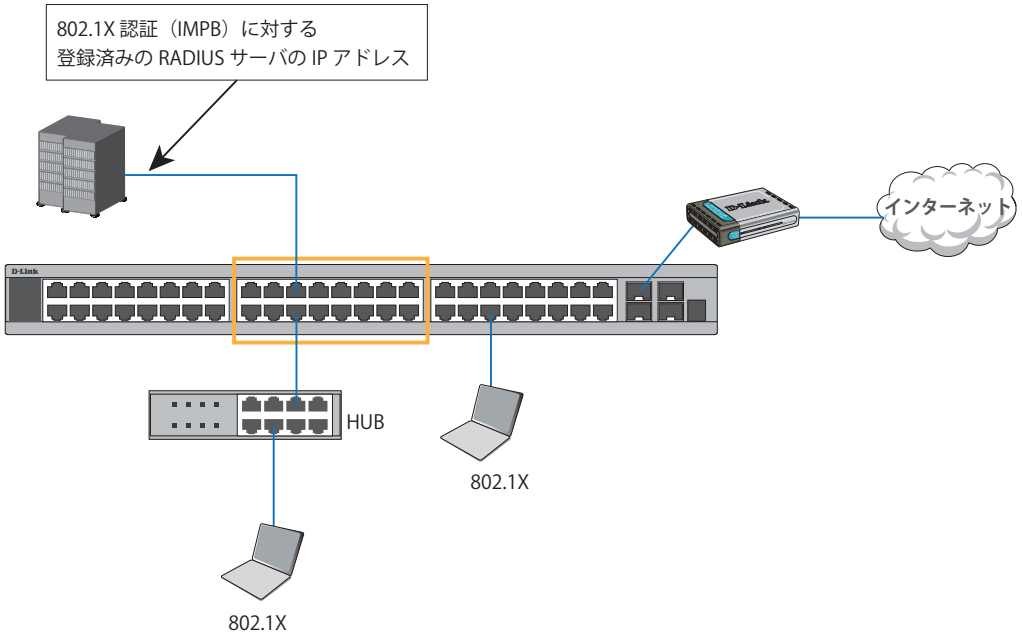


図 9-59　802.1X & IMPB モードの図

本モードでは、サポートしている認証方式での認証を行う前に IP-MAC- ポートバインディングテーブルをチェックすることで特別なセキュリティレイヤを追加しています。IP-MAC- ポートバインディングテーブルは、認証ホストが送信した IP ストリームが許可済みであるかをチェックする「ホワイトリスト」を作成するのに使用されます。上の図では、スイッチポートは 802.1X 認証を使用して認証を行うように設定されています。IP-MAC- ポートバインディングテーブルにあるクライアントがこの認証方式を使用してネットワークに接続を試みる場合、そのクライアントが適切な IP/MAC/ ポートチェックのホワイトリストに載っていると接続は許可されます。クライアントが認証方式のうち 1 つに失敗すると、接続は拒否されます。

IMPB & WAC/JWAC モード

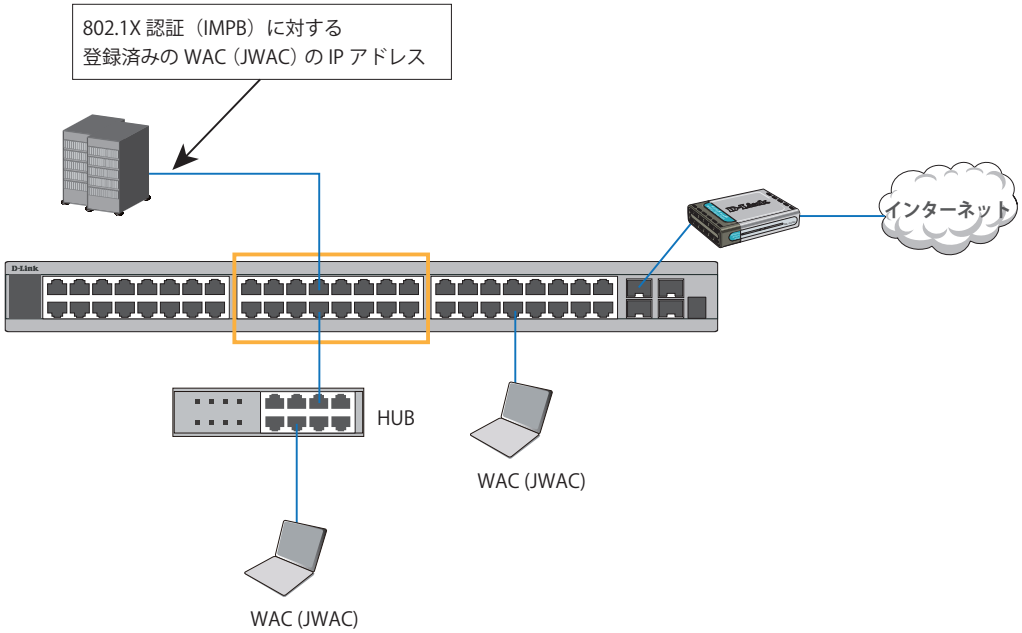


図 9-60　IMPB & WAC/JWAC モードの図

本モードでは、サポートしている認証方式で認証を行う前に IP-MAC- ポートバインディングテーブルをチェックすることで特別なセキュリティレイヤを追加しています。IP-MAC- ポートバインディングテーブルは、認証ホストが送信した IP ストリームが許可済みであるかをチェックする「ホワイトリスト」を作成するのに使用されます。上の図では、スイッチポートは MAC アドレス認証、または WAC を使用して認証を行うように設定されています。IP-MAC- ポートバインディングテーブルにあるクライアントがこれらのうちいずれかの認証方式を使用してネットワークに接続を試みる場合、そのクライアントが適切に IP/MAC/ ポートチェックのホワイトリストに載っていると接続は許可されます。クライアントが認証方式のうちの 1 つで認証エラーになると、接続は拒否されます。

「Multiple Authentication」フォルダには以下の 3 つの画面があります。:「Authorization Network State Settings」画面、「Multiple Authentication Settings」画面、および「Guest VLAN Settings」画面

Authorization Network State Settings（認証ネットワークの状態設定）

本製品の認証ネットワークの状態設定を行います。

Security > Multiple Authentication > Authorization Network 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。

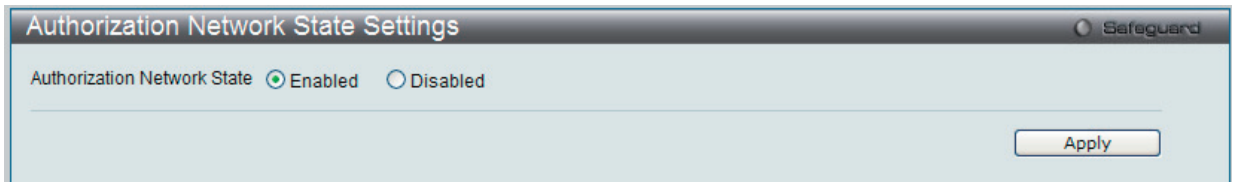


図 9-61　Authorization Network State Settings 画面

認証ネットワークの状態を「Enabled」（有効）または「Disabled」（無効）に設定し、「Apply」ボタンをクリックして設定を適用します。

Multiple Authentication Settings（マルチプル認証の設定）

ポートまたはポート範囲に対するマルチプル認証方式を設定します。

Security > Multiple Authentication > Multiple 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。

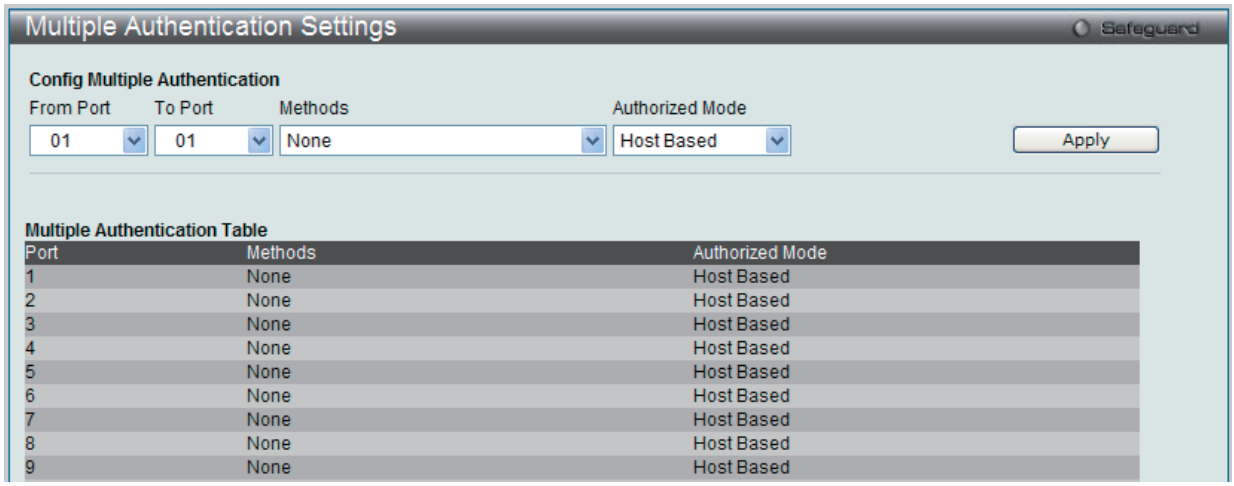


図 9-62　Multiple Authentication Settings 画面

スイッチの各ポートにマルチプル認証を設定するには、以下の項目を指定します。

項目	説明
From Port / To Port	マルチプル認証ポートとして設定するポート範囲を指定します。
Methods	マルチプル認証方式には以下のオプションがあります。 • None - すべてのマルチプル認証方式を無効にします。 • Any（MAC、802.1X or WAC/JWAC）- 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。
Authorized Mode	「Host Based」または「Port Based」を選択します。 • Port Based - 対応するホストの 1 つが認証を通過すると、同じポート上のホストはすべてネットワークへの接続が許可されます。認証に失敗するとこのポートは続いて次の認証方式を実行します。 • Host Based - ユーザは個別に認証されます。

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

Guest VLAN（ゲスト VLAN）

ポートをゲスト VLAN に割り当て、または削除することができます。

Security > Multiple Authentication > Guest 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。

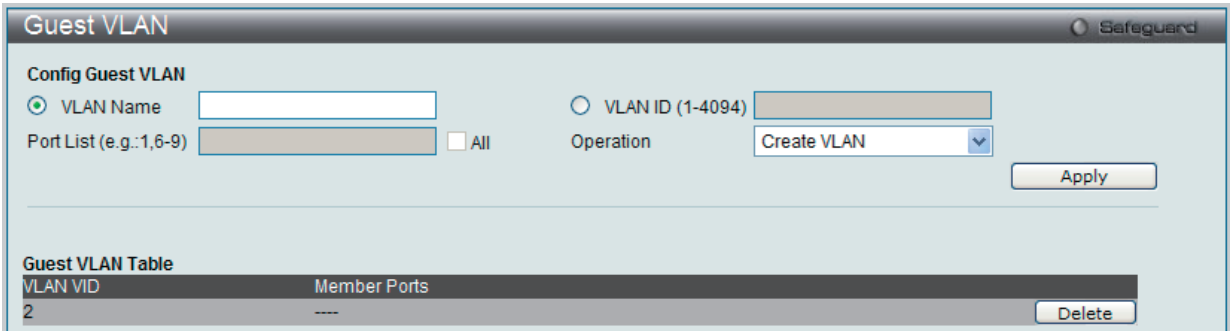


図 9-63　Guest VLAN 画面

以下の項目を使用して、ゲスト VLAN の設定をします。

項目	説明
VLAN Name	VLAN をゲスト VLAN として割り当てます。必ず定義済みのスタティック VLAN を割り当てます。
VLAN ID (1-4094)	VLAN ID をゲスト VLAN に割り当てます。この VLAN ID には、必ず定義済みのスタティック VLAN に割り当てます。
Port List (e.g : 1,6-9)	設定するポート範囲を指定します。または、「All」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。
Operation	プルダウンメニューを使用して操作する機能を選択します。 • Create VLAN - VLAN を作成します。 • Add Ports - ポートを追加します。 • Delete Ports - ポートを削除します。

「Apply」ボタンをクリックし、ゲスト VLAN を実行します。正しく設定されるとゲスト VLAN 名と対象のポートが画面の下部に表示されます。

IGMP Access Control Settings（IGMP アクセスコントロール設定 : IGMP 認証）

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、スイッチはマルチキャストグループ / ポートを学習済みであり、再度認証を行いません。スイッチはパケットを標準的に処理します。

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 の順にメニューをクリックし、以下の画面を表示します。

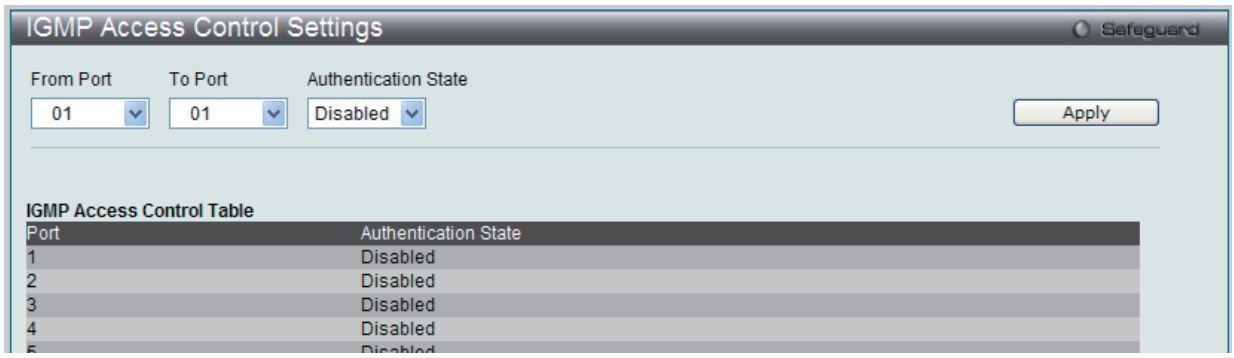


図 9-64　IGMP Access Control Settings 画面

本製品の各ポートに IGMP アクセスコントロールの設定を行うには、以下の項目を設定します。

項目	説明
From Port / To Port	IGMP アクセスコントロールを設定するポート範囲を指定します。
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。

「Apply」ボタンをクリックし、設定を適用します。

ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）

以下のセキュリティ機能を使用して、スイッチにアクセスしようとするハッカーや権限のない第三者による ARP Spoofing を防御します。

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。

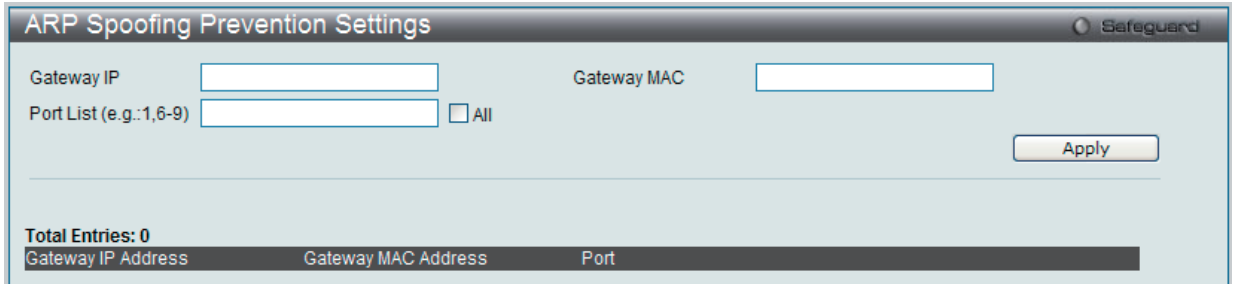


図 9-65　ARP Spoofing Prevention Settings 画面

「Gateway IP」（ゲートウェイの IP アドレス）、「Gateway MAC」（ゲートウェイの MAC アドレス）および「Port List」を入力し、「Apply」ボタンをクリックします。

注意 ARP Spoofing 攻撃を防ぐ方法についての詳しい情報は 263 ページの「付録 E パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減」を参照してください。

第 10 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。	193 ページ
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。	194 ページ
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。	206 ページ
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するために使用します。	216 ページ

ACL Configuration Wizard（ACL 設定ウィザード）

アクセスプロファイルとルールをより容易に作成するために、ACL ウィザードが現在のファームウェアリリースから導入されています。アドバンスドユーザは、次の「Access Profile List」セクションで手動によりアクセスプロファイルとルールを設定することもできます。

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。

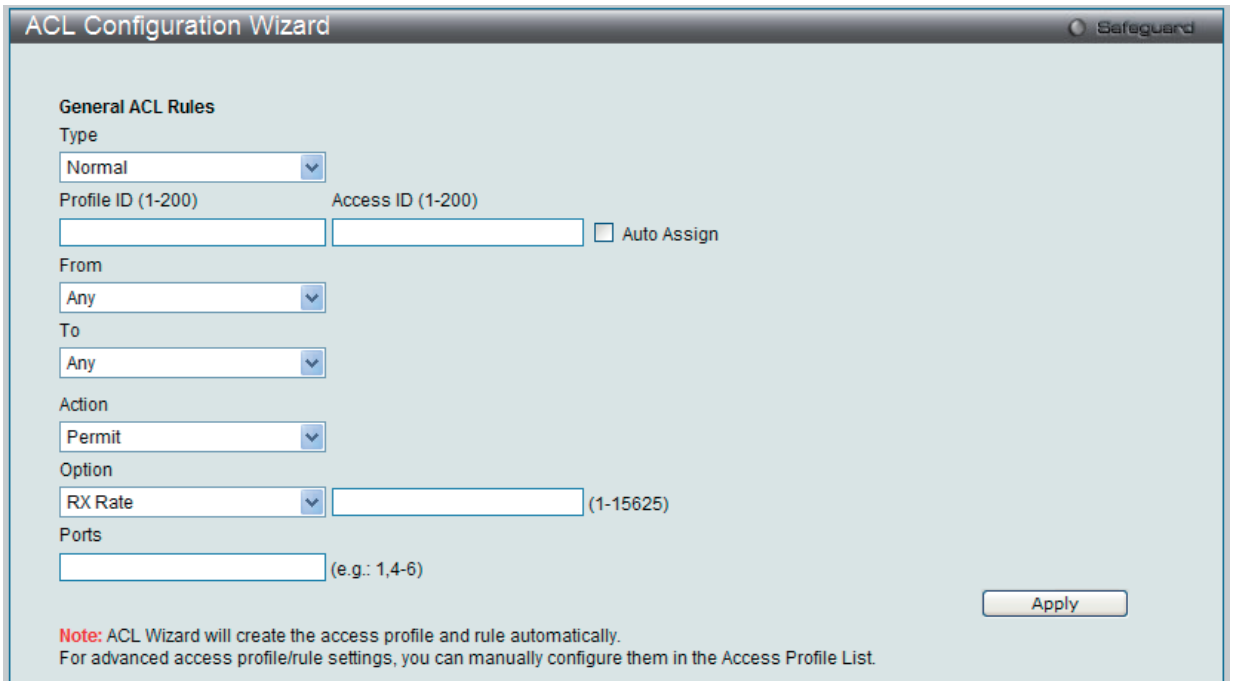


図 10-1　ACL Configuration Wizard 画面

1. ACL の種類 (Normal または CPU) を選択します。プルダウンメニューから「Normal」を選択して、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。プルダウンメニューから「CPU」を選択して、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(1-200) と Access ID(1-200) 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 Address) と To(Any、MAC Address、IPv4 Address または IPv6 Address) で選択します。

4. 「Action」を「Permit」、「Deny」または「Mirror」から選択します。

5. 「オプション」を「Rx Rate」、「Replace Priority」、または「Replace DSCP」から選択し、隣接している欄に 1-15625 の値を入力します。

6. 新しい ACL ルール用のポートを入力し、「Apply」ボタンをクリックして設定を適用します。

注意 ACL ウィザードで使用する項目についての詳しい情報は、本章の残りの部分にある ACL ルールの各タイプに関する詳細名説明を参照してください。

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 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。

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。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。

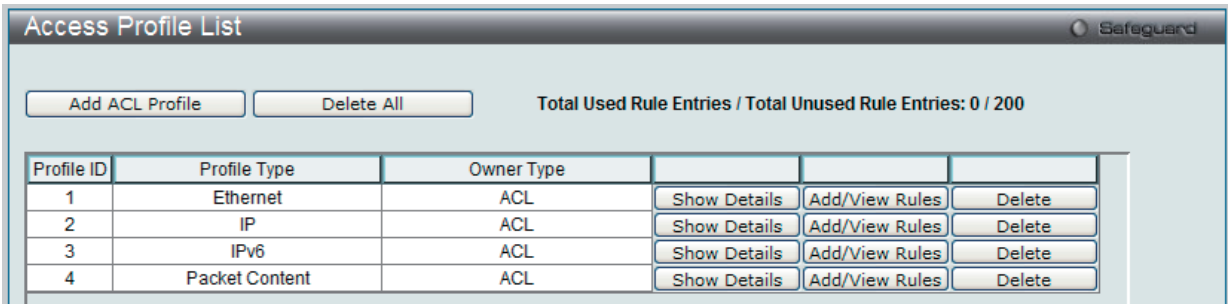


図 10-2　Access Profile List 画面

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。

エントリの削除

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。

「Add Access Profile」画面には 4 種類あります。
イーサネット（MAC アドレスベース）プロファイル設定用、IPv6 アドレスベースプロファイル設定用、IPv4 アドレスベースプロファイル設定用およびパケットコンテンツマスクプロファイル設定用です。
この 4 種類の「Add ACL Profile」画面の「Select 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画面を切り替えることができます。

イーサネットの「Add ACL Profile」画面

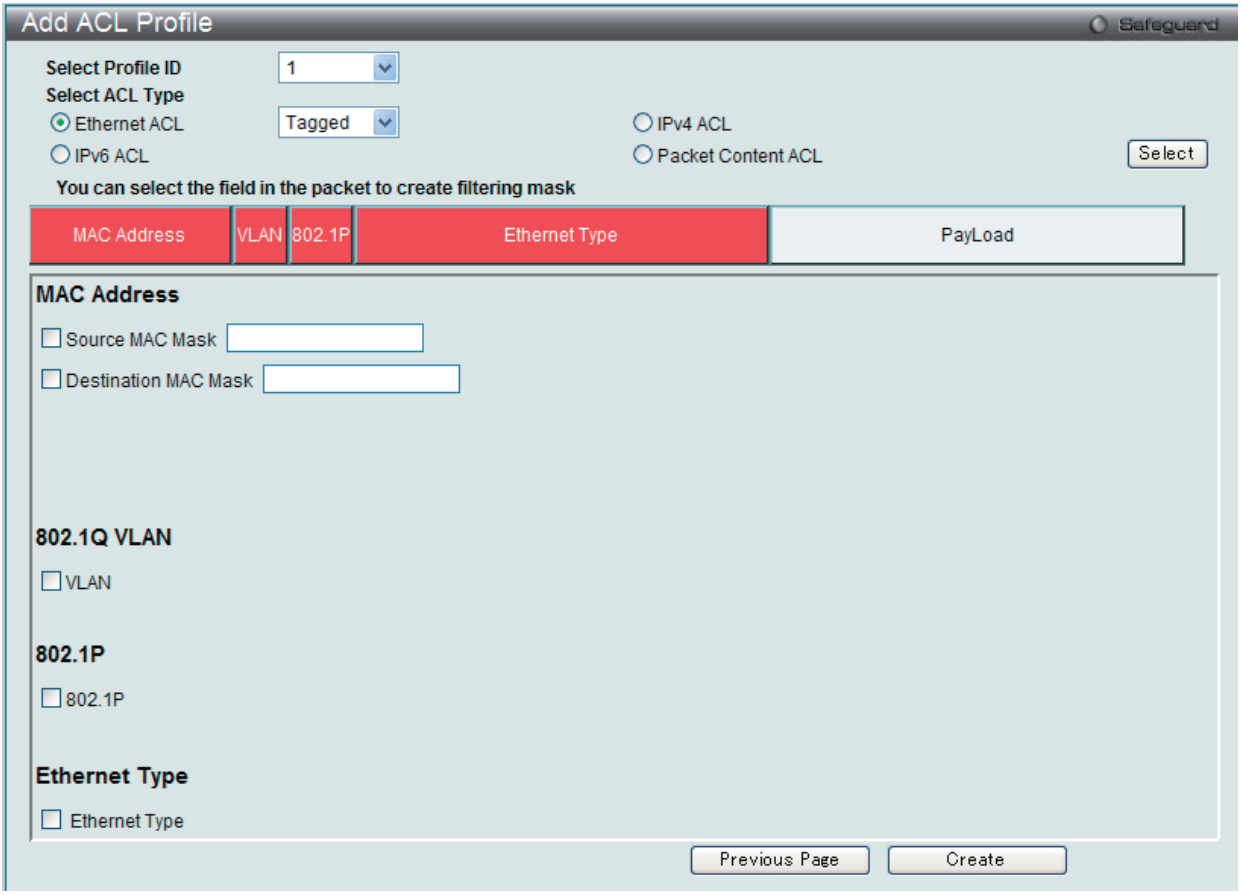


図 10-3　Add ACL Profile - Ethernet ACL 画面

以下の項目を Ethernet 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 200 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたは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。ここでは、「Ethernet ACL」を選択します。 • Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
MAC Address	• Source MAC Mask - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。 • Destination MAC Mask - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。
802.1Q VLAN	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。

作成したプロファイルの詳細の参照

「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

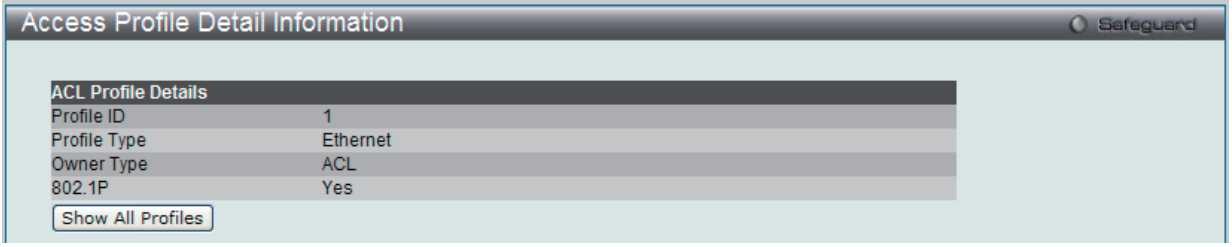


図 10-4　Access Profile Detail Information - Ethernet 画面

IPv4 の「Add ACL Profile」画面

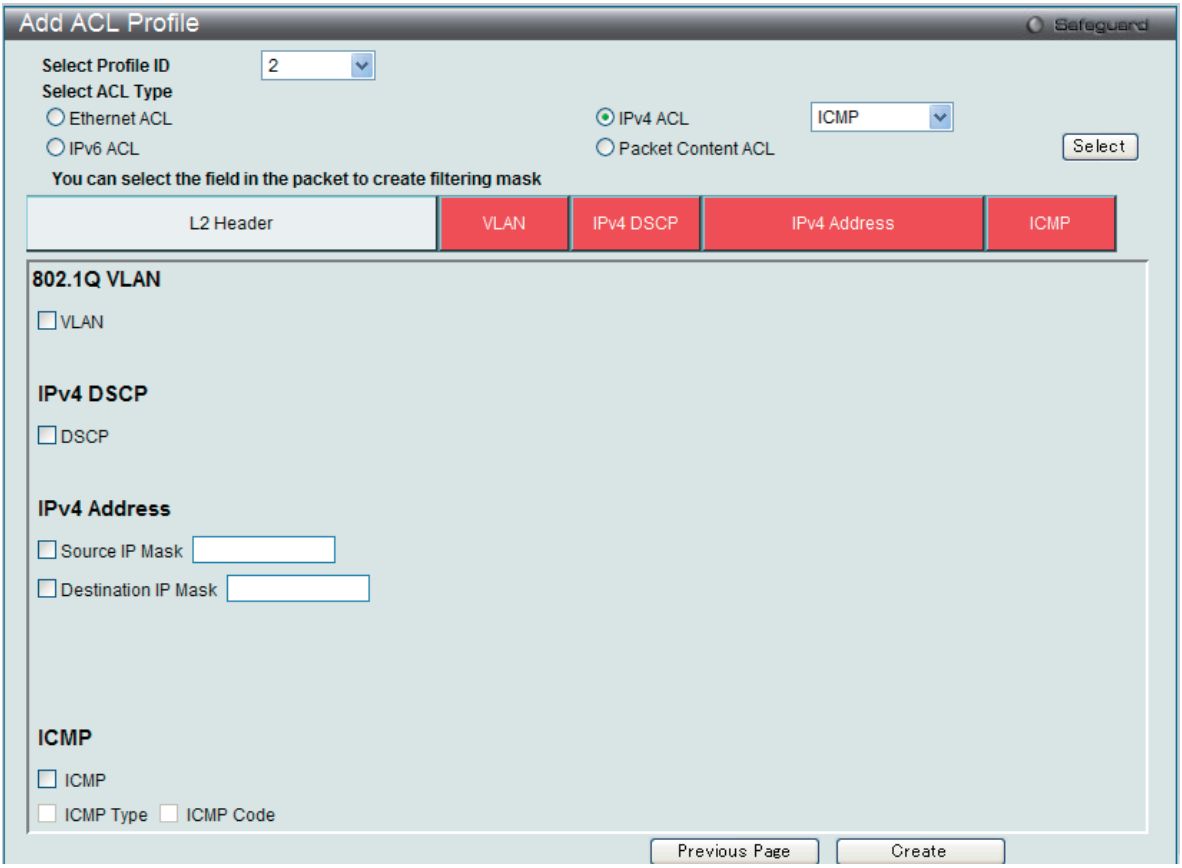


図 10-5　Add ACL Profile - IPv4 ACL 画面

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 200 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4 ACL」を選択します。 • IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。
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	それぞれのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（もしくは）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク（source port mask）と（もしくは）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。「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、設定を適用します。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照するには、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

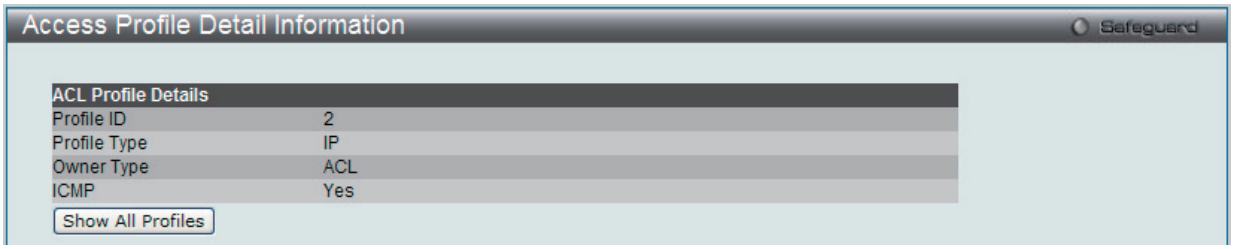


図 10-6　Access Profile Detail Information - IPv4 画面

IPv6 の「Add ACL Profile」画面

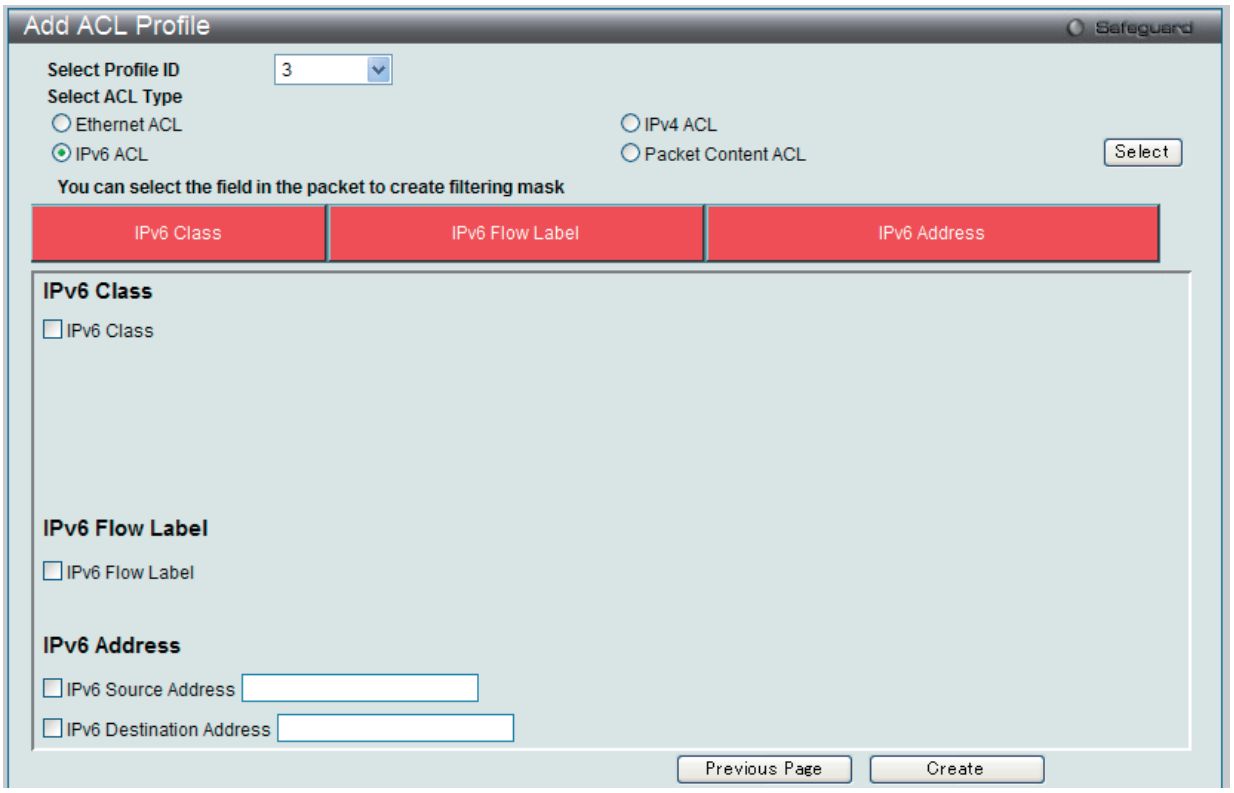


図 10-7　Add ACL Profile - IPv6 ACL 画面

以下の項目を IPv6 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 200 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv6 ACL」を選択します。 • IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
IPv6 Class	この項目を選ぶと IPv6 ヘッダの「Class」を調べます。「Class」は IPv4 における「Type of Service」（ToS）、「Precedence bits」のようなパケットヘッダの一部です。
IPv6 Flow Label	この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 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。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照する場合は、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

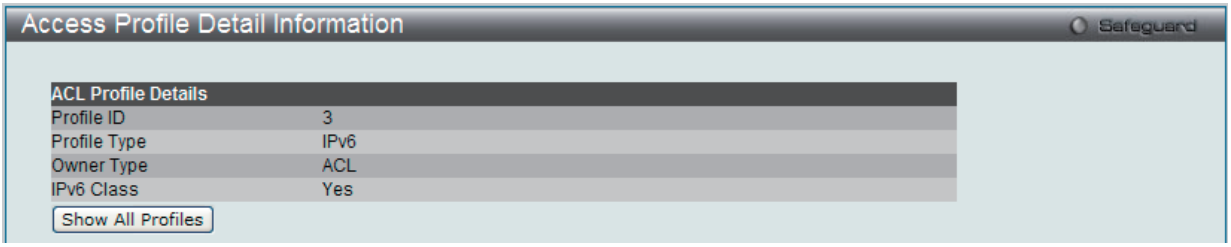


図 10-8　Access Profile Detail Information - IPv6 ACL 画面

パケットコンテンツの「Add ACL Profile」画面

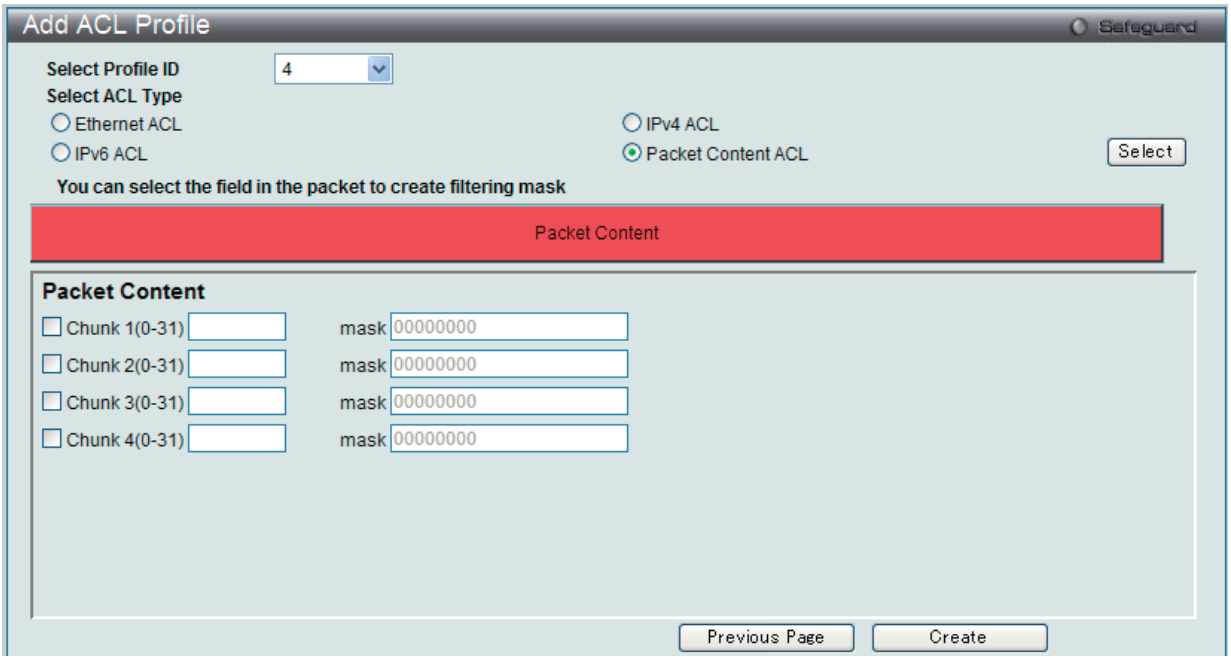


図 10-9　Add ACL Profile 画面 - パケットコンテンツ

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>Select 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 200 が指定できます。</td></tr>
<tr><td>Select ACL Type</td><td>Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Packet Content」を選択します。
• Packet Content - フレームヘッダのパケットコンテンツを検証します。</td></tr>
<tr><td 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を検証できます。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></td><td>offset_chunk_1
offset_chunk_2
offset_chunk_3
offset_chunk_4
<table>
<tr><th>chunk0</th><th>chunk1</th><th>chunk2</th><th>……</th><th>chunk29</th><th>chunk30</th><th>chunk31</th></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、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 スイッチファミリの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）機能は、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。
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>

「Apply」ボタンをクリックし、変更を有効にします。

作成したプロファイルの詳細の参照

作成したプロファイル設定を参照するためには、「Access Profile List」画面の対応する「Show Details」ボタンをクリックし、以下の画面を表示します。

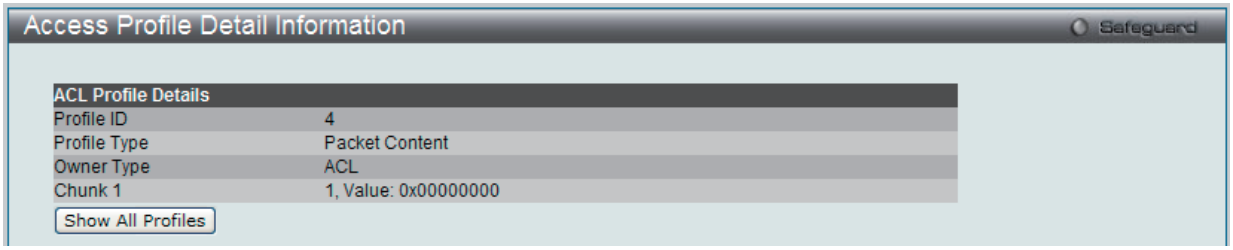


図 10-10　Access Profile Detail Information 画面 - パケットコンテンツ

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 スプーフィング攻撃を防ぐために 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 263 ページの「付録 E パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減」を参照してください。

ルール設定

作成したアクセスプロファイルに対するルールの設定手順（Ethernet）：

Ethernet アクセスルールの設定

「Access Profile List」画面を表示し、Ethernet 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。

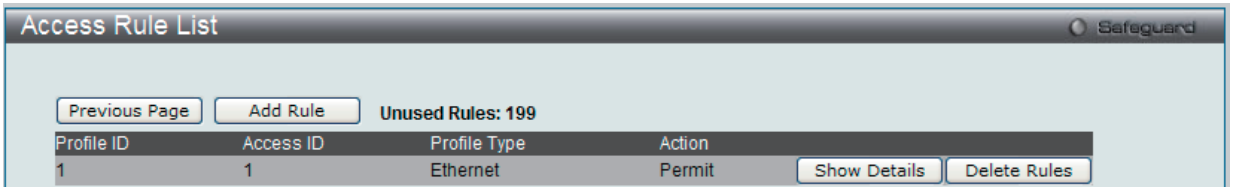


図 10-11　Access Rule List - Ethernet 画面

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ます。

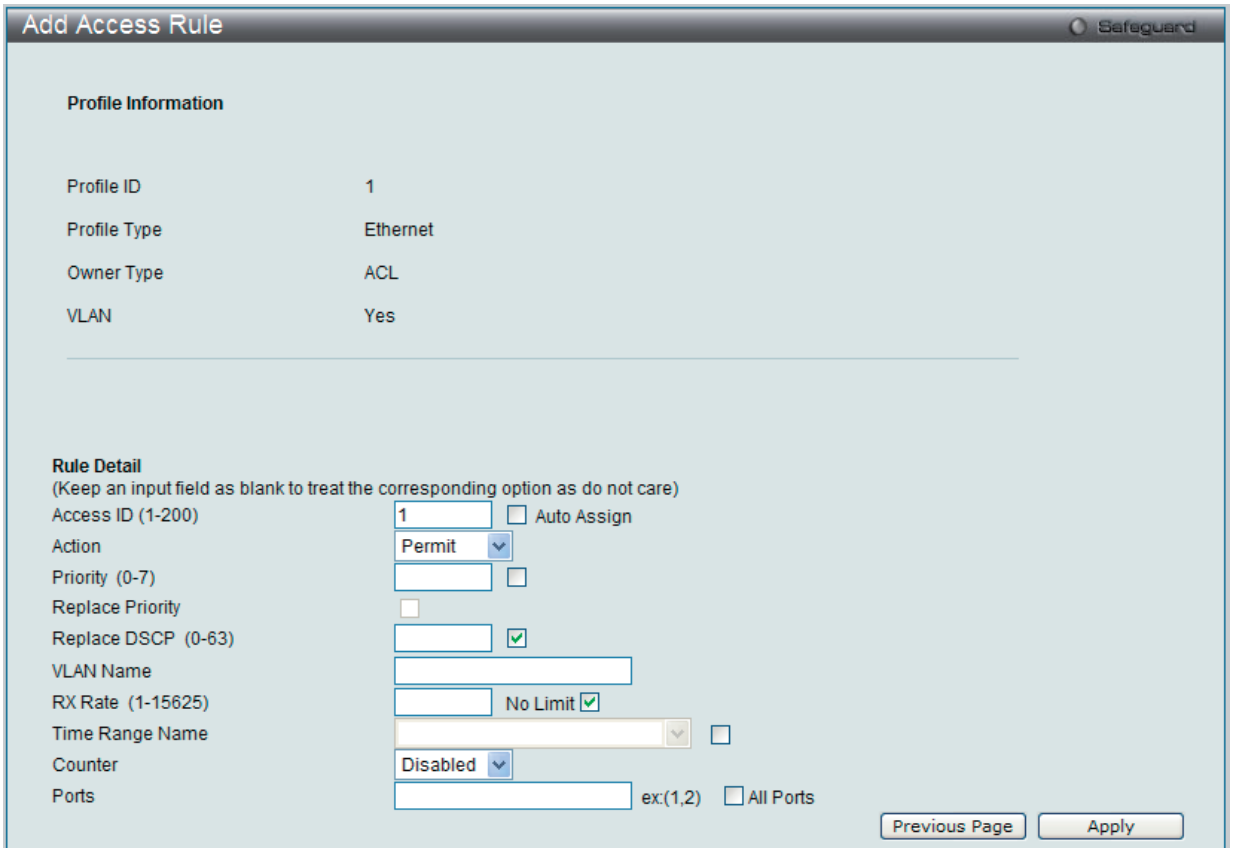


図 10-12　Add Access Rule - Ethernet 画面

Ethernet のアクセスルールを設定するためには以下の項目を設定して、「Apply」ボタンをクリックします。

項目	説明
Access ID (1-200)	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 200 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Action	• Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。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 136 ページの「第 8 章 QoS（QoS 機能の設定）」を参照してください。
VLAN Name	既に設定されている VLAN 名を指定します。
802.1P (0-7)	802.1p プライオリティ値を 0-7 で入力します。アクセスプロファイルをこの値を持つパケットに適用します。
Ethernet Type (0-FFFF)	アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数（hex 0x0-0xffff）で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff（a-f の半角英文字、と 0-9999 の数字を使用します。）
Rx Rate (1-15625)	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 Ingress レートは 640Kbit/sec となります。）1-15625 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	プルダウンメニューを使用して、「Counter」機能を「Enabled」(有効)/「Disabled」(無効) にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。例えば、送信元 MAC アドレス 00-00-00-00-00-01 がスイッチへのアクセスを許可するイーサネット ACL を作成し、スイッチが送信元 MAC アドレス 00-00-00-00-00-01 を持つ 1000 個のパケットを受信した場合、カウンタ値は 1000 となり、ACL が 1000 個のパケットを照合したことを示します。
Ports	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します。ポート範囲を指定する場合は、「Access ID」の「Auto Assign」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。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

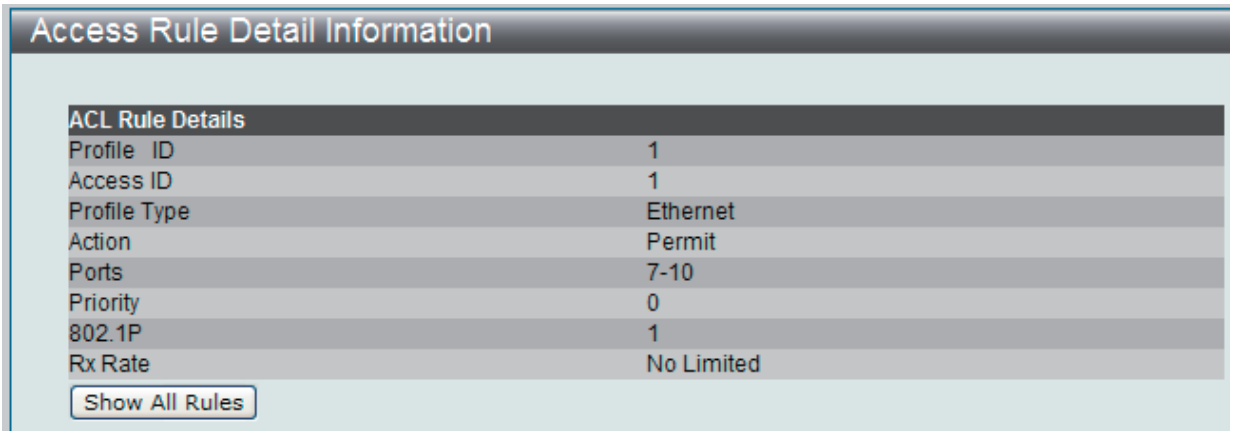


図 10-13 Access Rule Detail Information - Ethernet 画面

作成したアクセスプロファイルに対するルールの設定手順（IPv4）：

IPv4 アクセスルールの設定

「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。

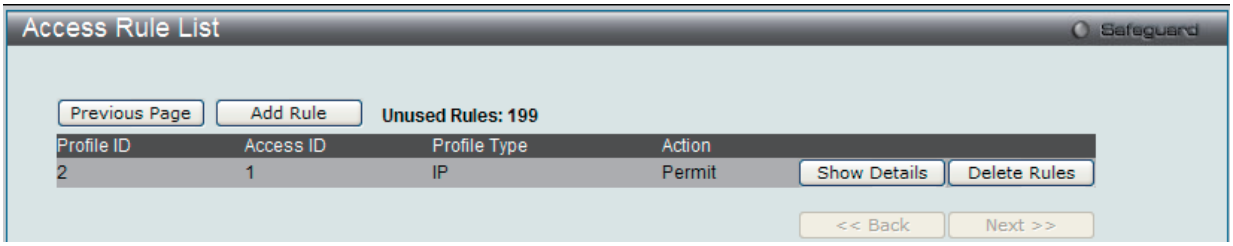


図 10-14 Access Rule List - IP 画面

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ます。

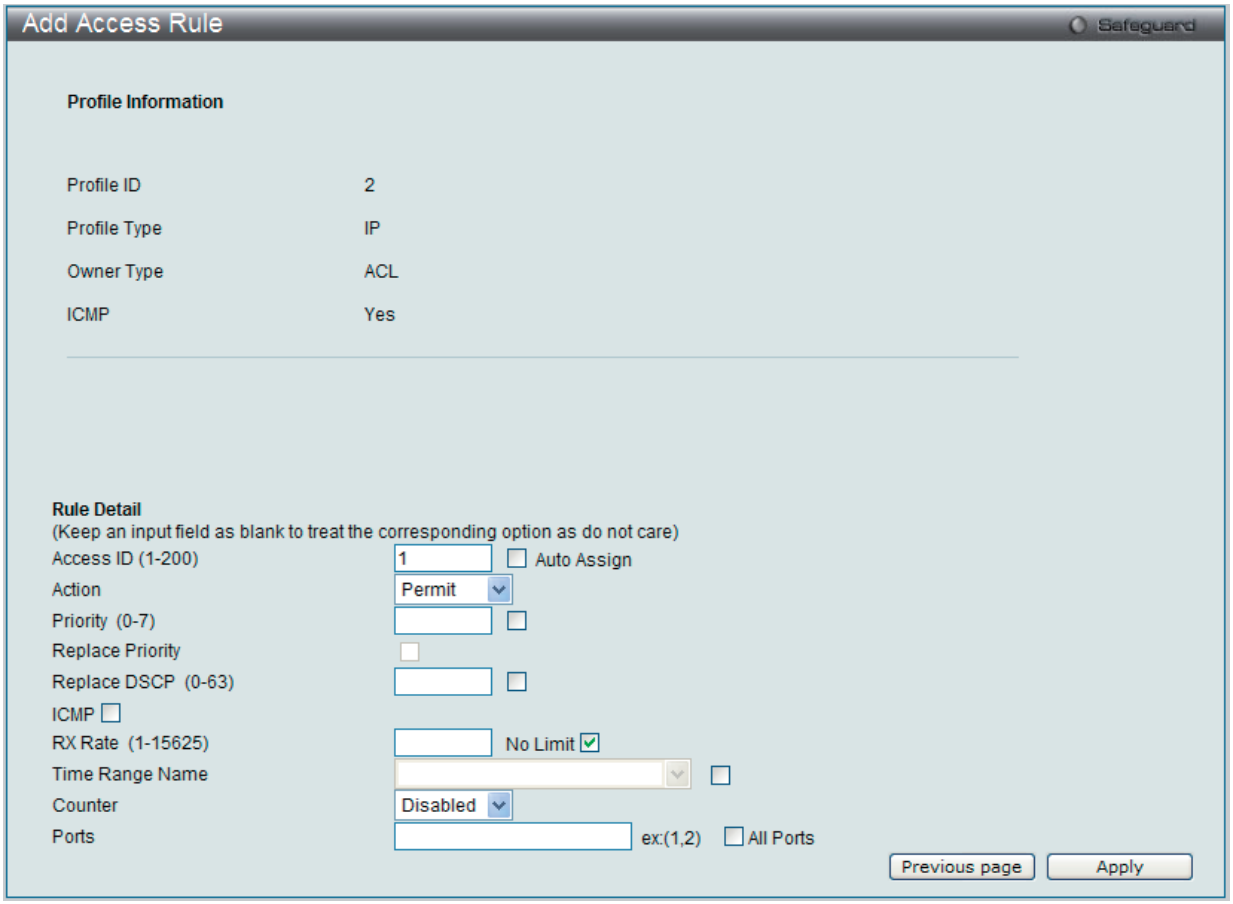


図 10-15 Add Access Rule - IP 画面

以下の項目を設定します。

項目	説明
Access ID (1-200)	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 200 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。
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する場合に指定します。本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。本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。 • 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 136 ページの「第 8 章 QoS（QoS 機能の設定）」を参照してください。

項目	説明
Replace DSCP (0-63)	このオプションを選ぶと条件に合ったパケットの DSCP 値は指定した値に入れ替わります。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
VLAN Name	提供されたスペースに VLAN 名を入力します。そして各パケットヘッダの VLAN 識別子を確認するようにします。
DSCP	DSCP 値（0-63）を指定すると各パケットヘッダの DiffServ コードを調べて、部分的または全体を転送基準として使用します。
Rx Rate (1-15625)	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 Ingress レートは 640Kbit/sec となります。）1-15625 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	プルダウンメニューを使用して、「Counter」g 機能を「Enabled」(有効)/「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。

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

「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。

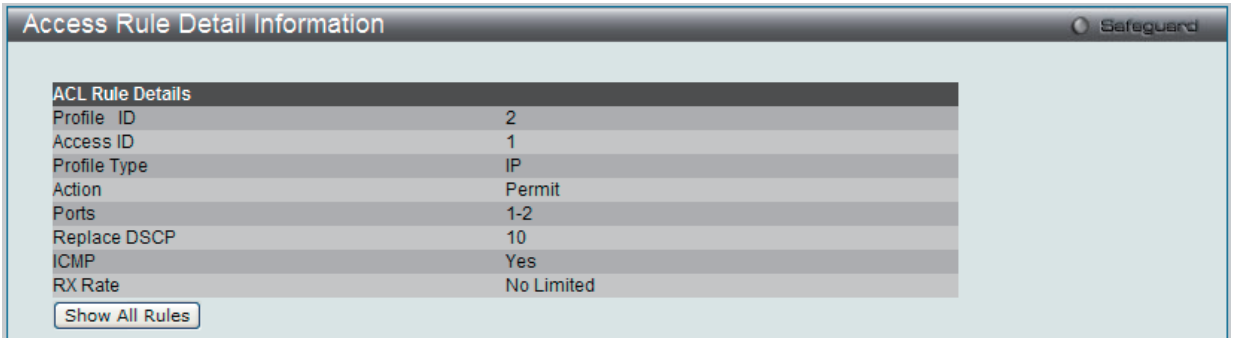


図 10-16 Access Rule Detail Information - IP 画面

作成したアクセスプロファイルに対するルールの設定手順（IPv6）：

IPv6 アクセスルールの設定

「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。

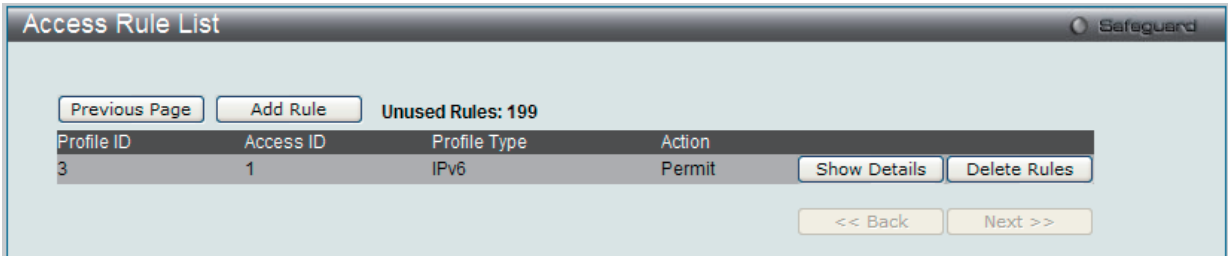


図 10-17 Access Rule List - IPv6 画面

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。

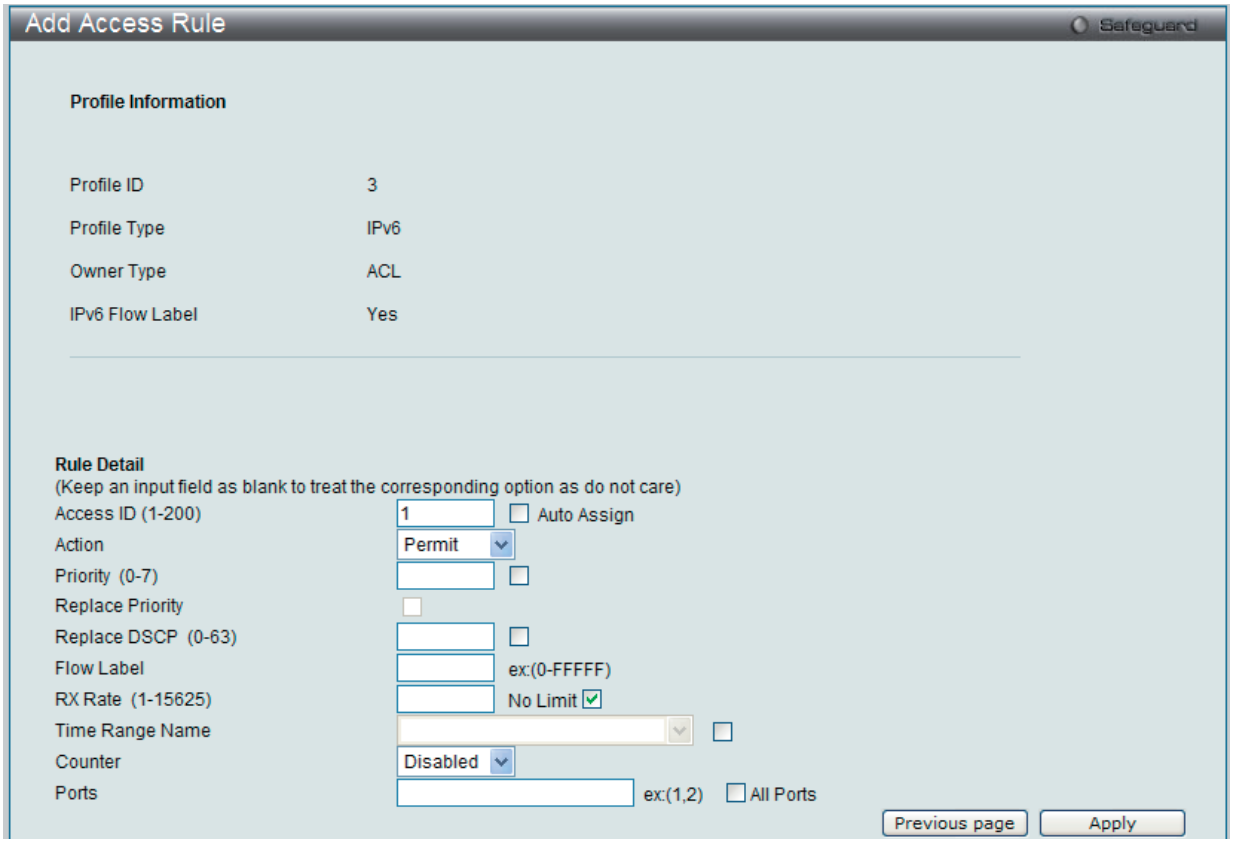


図 10-18 Add Access Rule - IPv6 画面

以下の項目を設定します。

項目	説明
Access ID (1-200)	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 200 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • 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 136 ページの「第 8 章 QoS（QoS 機能の設定）」を参照してください。
Replace Priority	本オプションを選ぶと条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	このオプションを選ぶと条件に合ったパケットの DSCP 値は指定した値に入れ替わります。ACL ルールがプライオリティと IPv6 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Class	本オプションを使用して IPv6 クラスマスクを指定します。
Rx Rate (1-15625)	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 Ingress レートは 640Kbit/sec となります。）1-15625 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	プルダウンメニューを使用して、「Counter」機能を「Enabled」(有効)/「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。

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。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

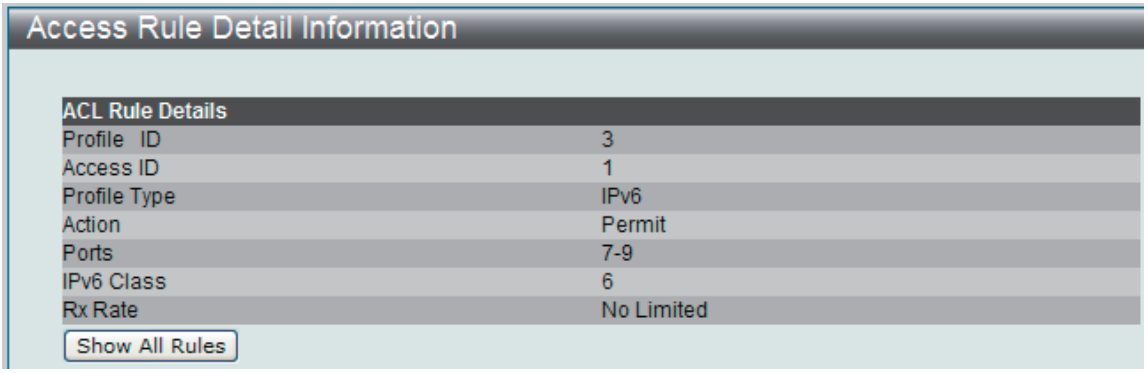


図 10-19 Access Rule Detail Information - IPv6 画面

作成したアクセスプロファイルに対するルールの設定手順（パケットコンテンツ）：

パケットコンテンツアクセスルールの設定

「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。

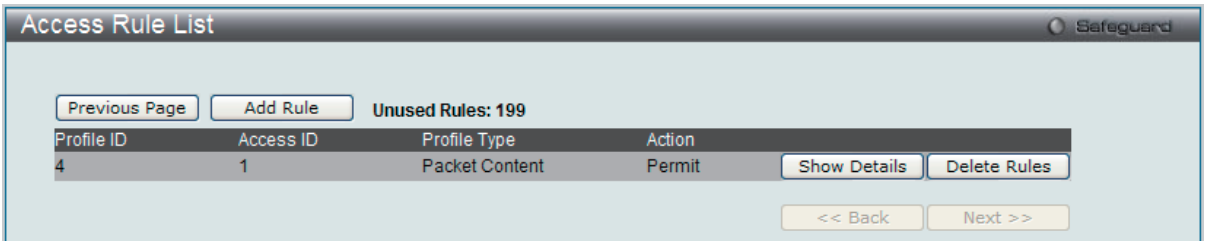


図 10-20 Access Rule List 画面 - パケットコンテンツ

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

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

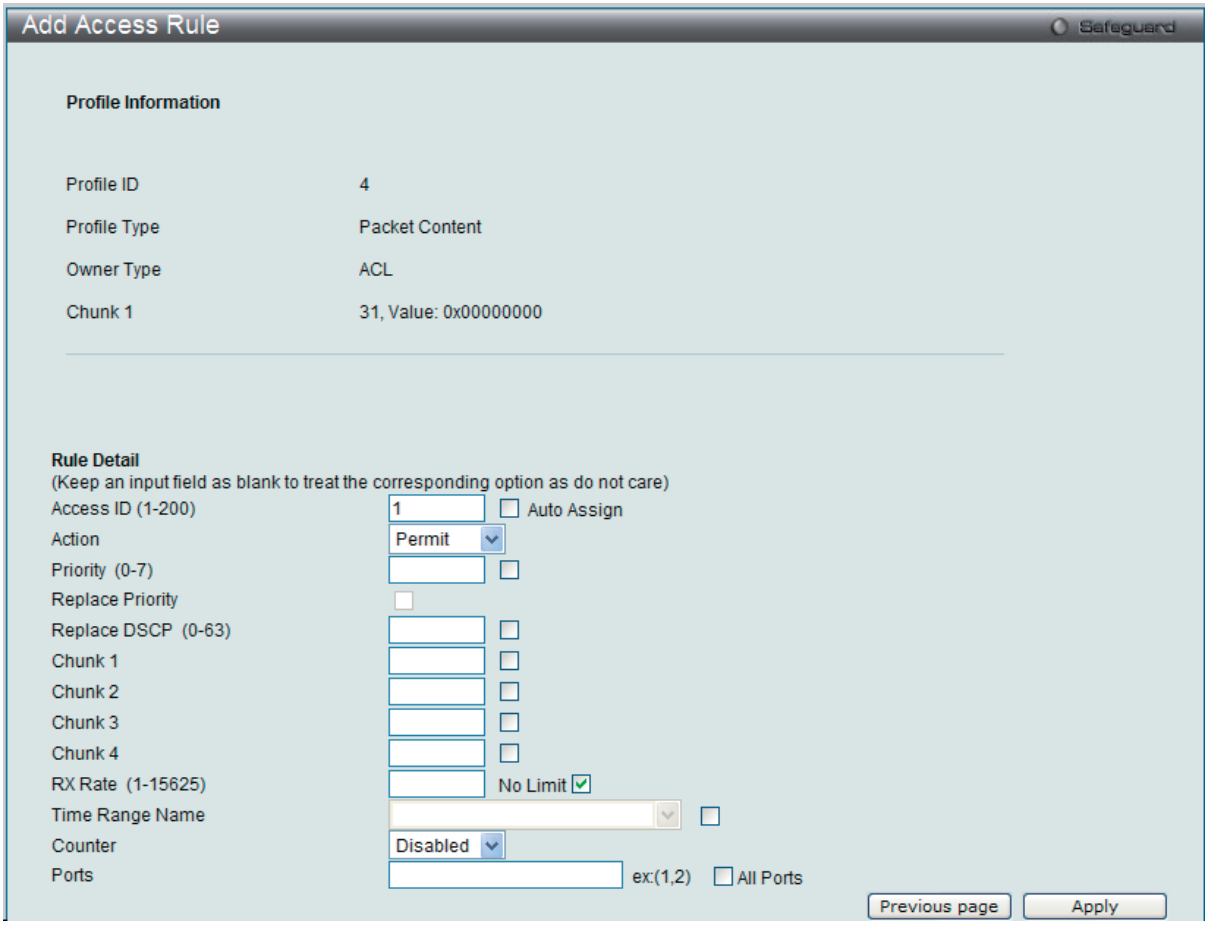


図 10-21 Add ACL Rule 画面 - パケットコンテンツ

以下の項目を設定します。

項目	説明
Access ID (1-200)	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 200 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • 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136 ページの「第 8 章 QoS（QoS 機能の設定）」を参照してください。
Replace DSCP (0-63)	DSCP 値を指定するとそれぞれのパケットヘッダの 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。0 から 63 までで指定できます。
Chunk	本項目の設定により、スイッチは指定したオフセット値で始まるパケットヘッダをマスクします。
Rx Rate (1-15625)	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 Ingress レートは 640Kbit/sec となります。）1-15625 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	プルダウンメニューを使用して、「Counter」機能を「Enabled」(有効)/「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」項目の「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。

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。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

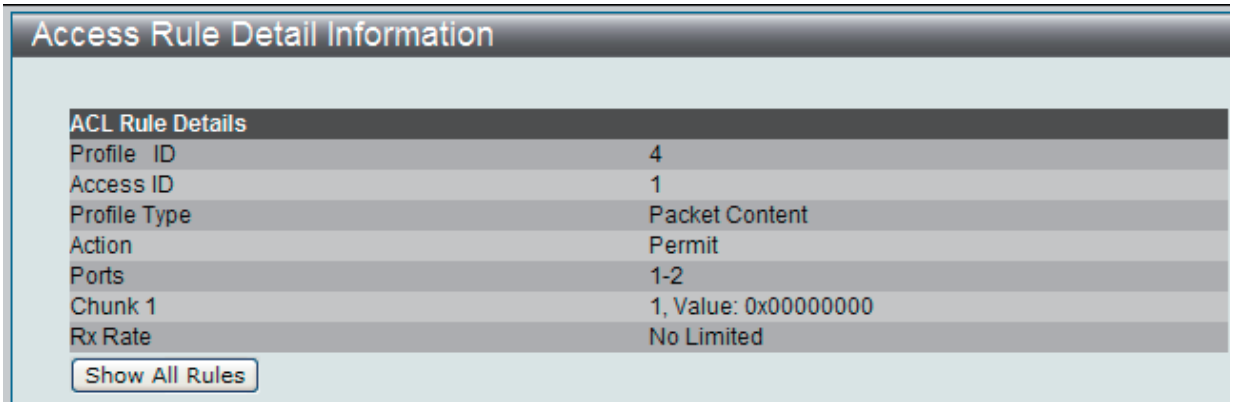


図 10-22　Access Rule Detail Information - パケットコンテンツ画面

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。

CPU アクセスプロファイルの作成

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State メカニズム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。「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。

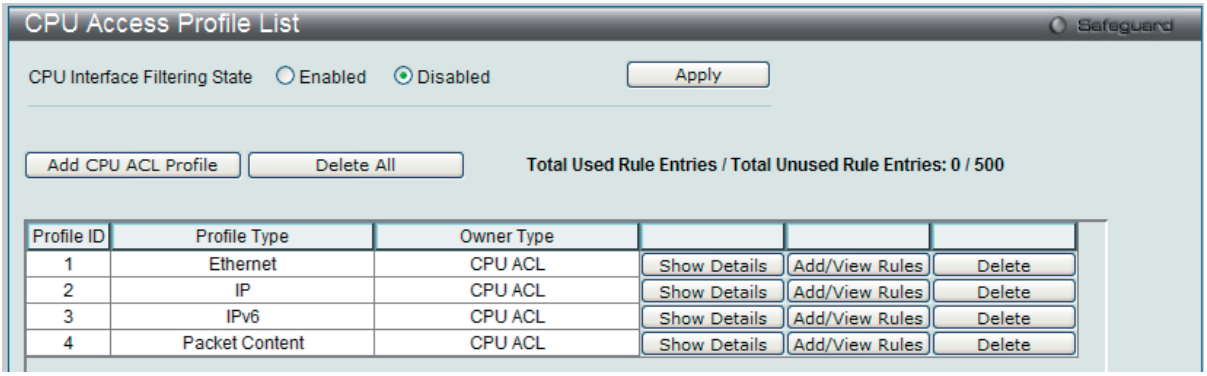


図 10-23　CPU Access Profile List 画面

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。

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 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。

CPU Access Profile List の全エントリの削除

全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。

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。

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）および「Select All Type」（ACL タイプ）を選択し、「Select」ボタンをクリックします。

イーサネットの「Add CPU ACL Profile」画面

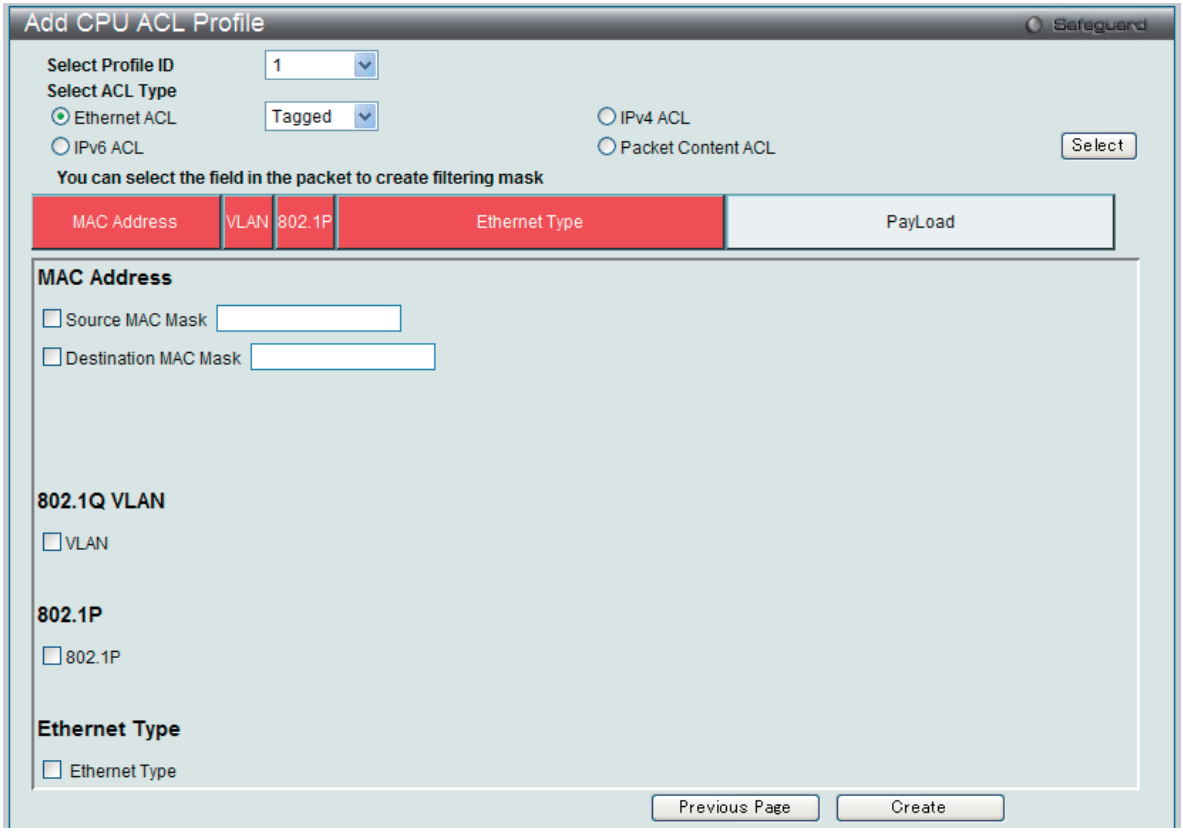


図 10-24　Add CPU ACL Profile - Ethernet 画面

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Ethernet」を選択します。 • Ethernet - パケットヘッダのレイヤ 2 部分を対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
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。

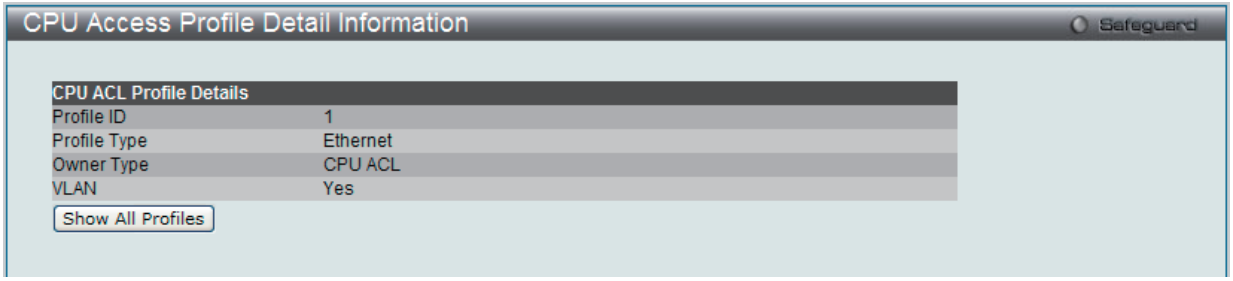


図 10-25　CPU Access Profile Detail Information - Ethernet 画面

IPv4 の「Add CPU ACL Profile」画面

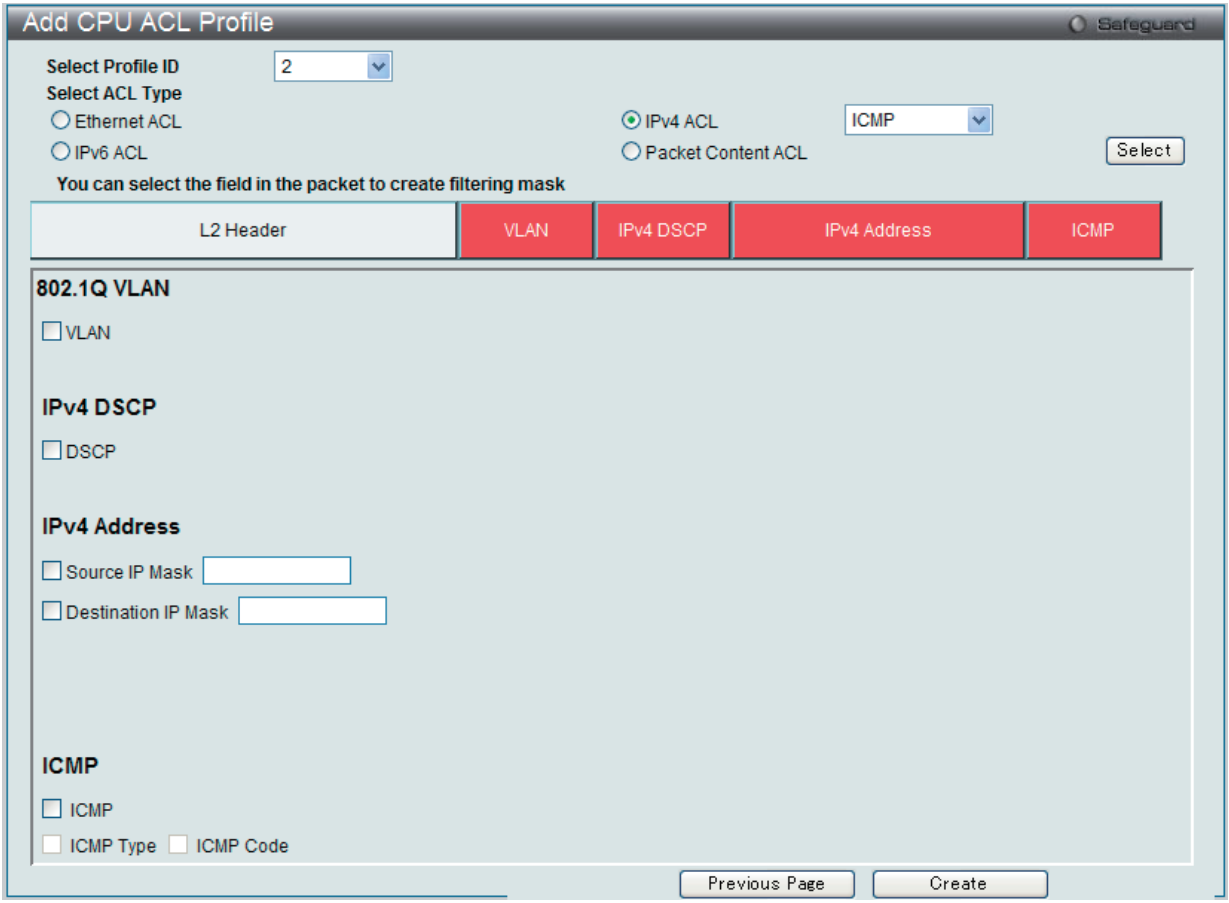


図 10-26 Add CPU ACL Profile - IPv4 画面

以下の項目を IP（IPv4）フィルタに設定できます。

項目	説明
Select Profile ID (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。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4」を選択します。 • IPv4 - フレームヘッダの IP アドレスを対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
802.1Q VLAN	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。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには TCP 項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）を選ぶことができます。
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。CLI で以下のコマンドを使用します。 `DGS-3200-10:4# create access_profile access_profile_id1 ip protocol_mask 0x0FF user_define_mask <hex 0x0-0xffffffff>`

「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。

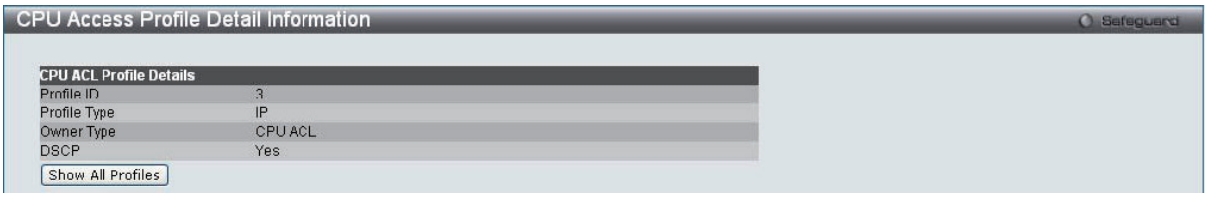


図 10-27　CPU Access Profile Detail Information - IP（IPv4）画面

IPv6 の「Add CPU ACL Profile」画面

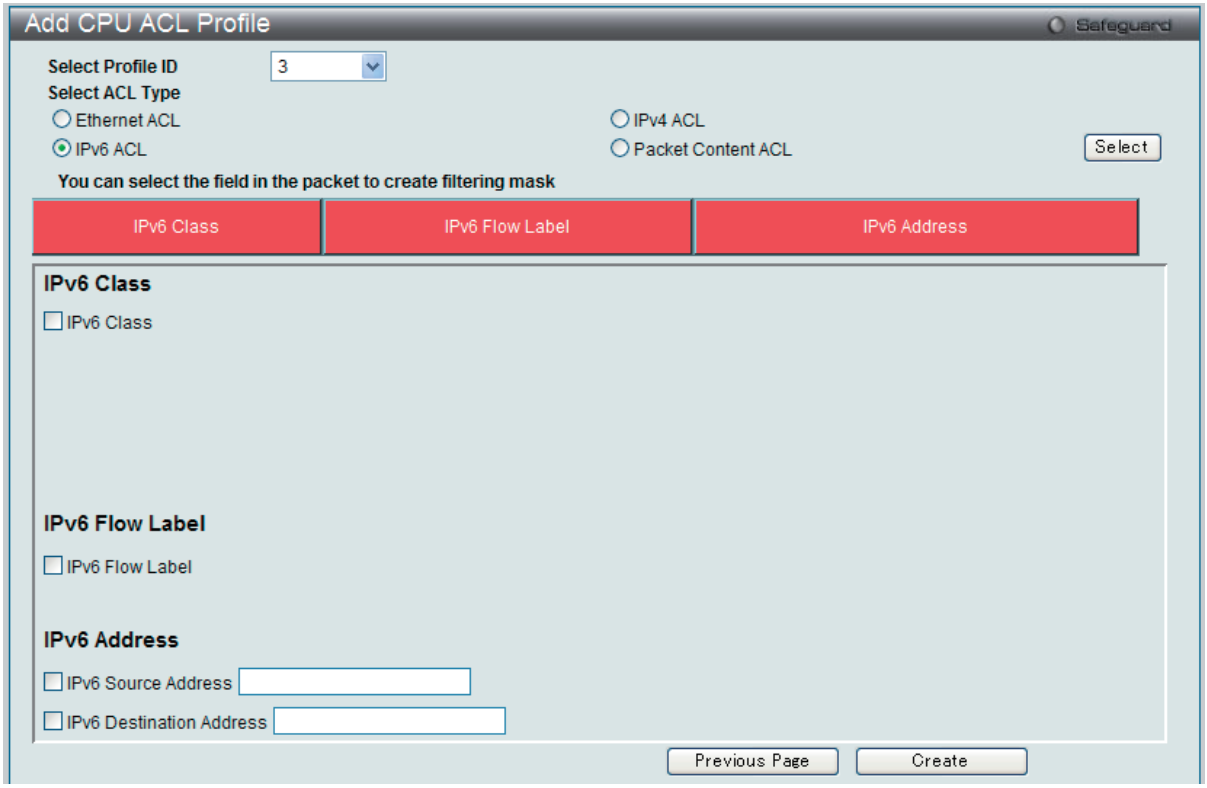


図 10-28　Add CPU ACL Profile - IPv6 画面

以下の項目を IP（IPv6）フィルタに設定できます。

項目	説明
Select Profile ID (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。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは、「IPv6」を選択します。 • IPv6 - フレームヘッダの IP アドレスを対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
IPv6 Class	この項目を選ぶと IPv6 ヘッダの「Class」項目を調べます。「Class」項目は IPv4 における Type of Service（ToS）、「Precedence bits」項目のようなパケットヘッダの一部です。
IPv6 Flow Label	この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 Address	• IPv6 Source 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、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。

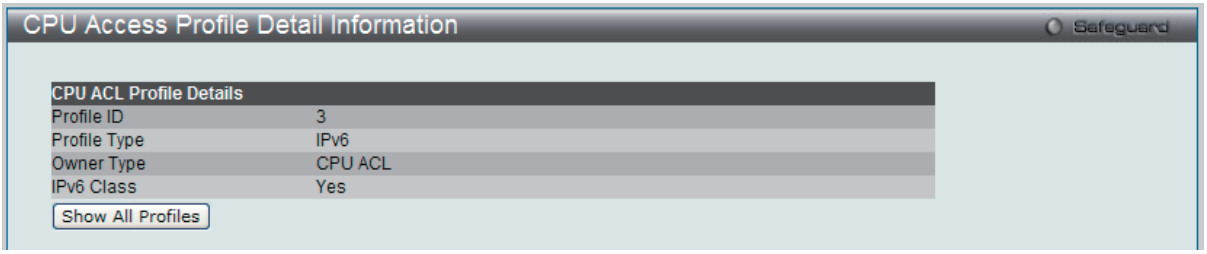


図 10-29 CPU Access Profile Detail Information - IPv6 画面

パケットコンテンツの「Add CPU ACL Profile」画面

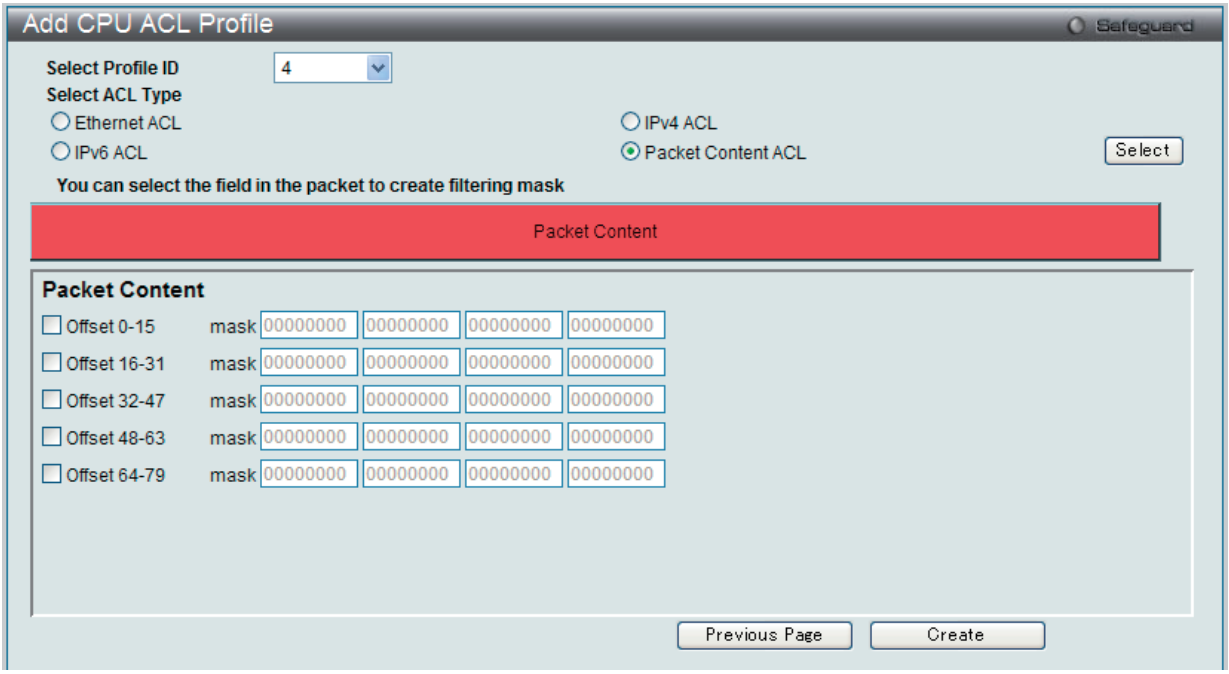


図 10-30 Add CPU ACL Profile - Packet Content 画面

以下の項目を Packet Content フィルタに設定できます。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Packet Content」を選択します。 • Packet Content - パケットヘッダの内容をマスクして隠します。
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。

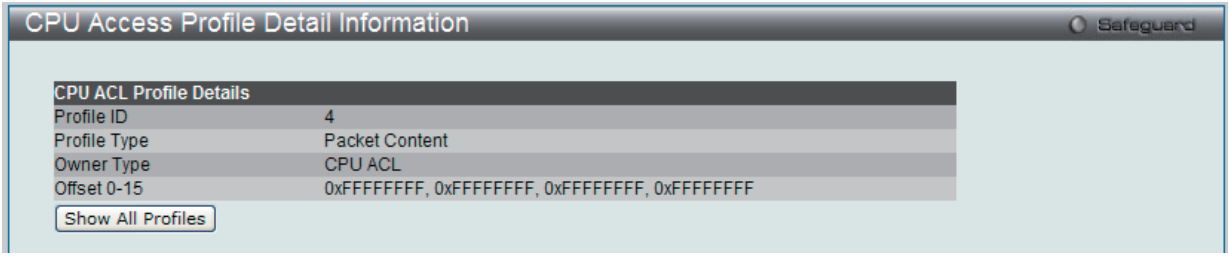


図 10-31 CPU Access Profile Detail Information - Packet Content 画面

ルール設定

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

「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。

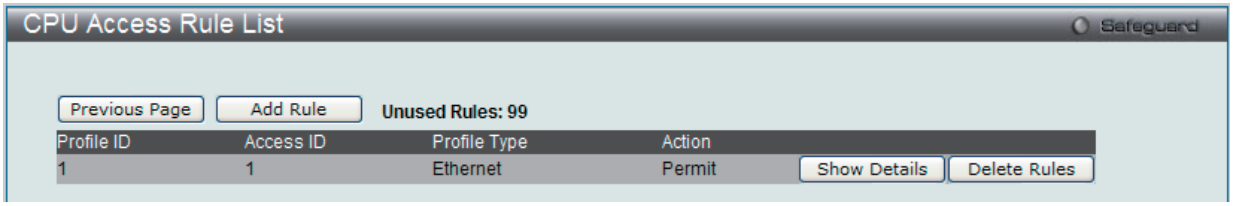


図 10-32 CPU Access Rule List - Ethernet 画面

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。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。

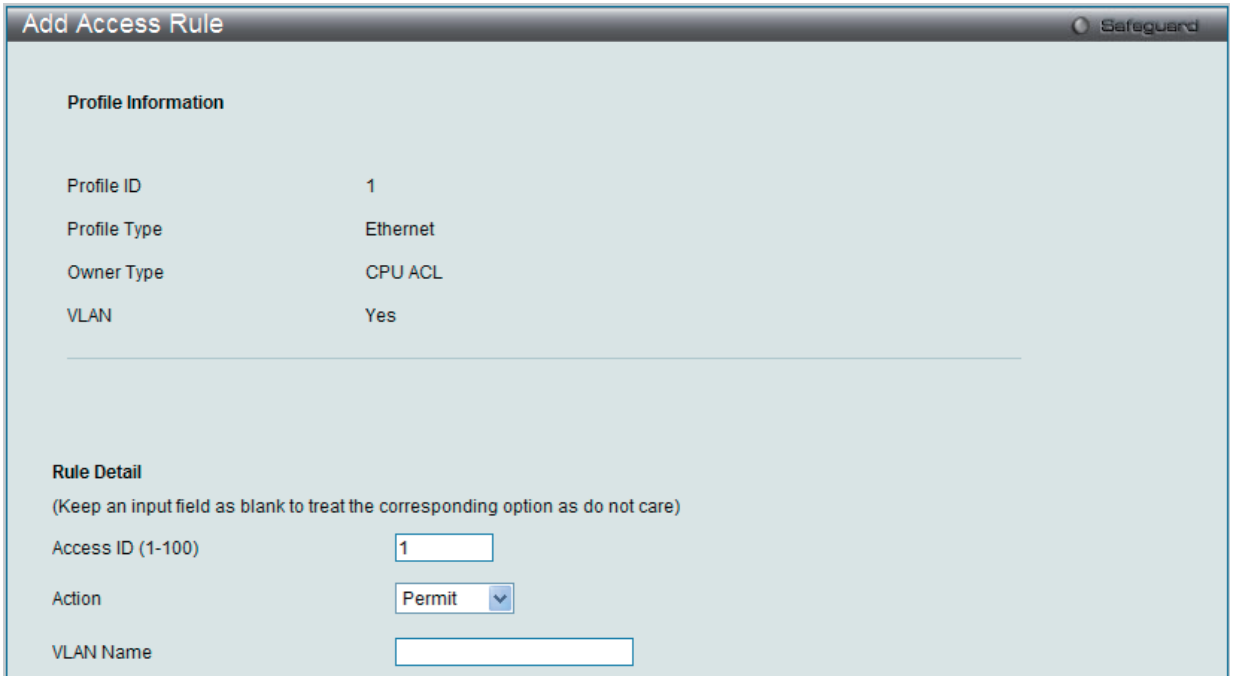


図 10-33 Add Access Rule - Ethernet 画面

項目	説明
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。
Ethernet Type (0-FFFF)	適切なイーサネットタイプ情報を入力します。
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	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。「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。

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。

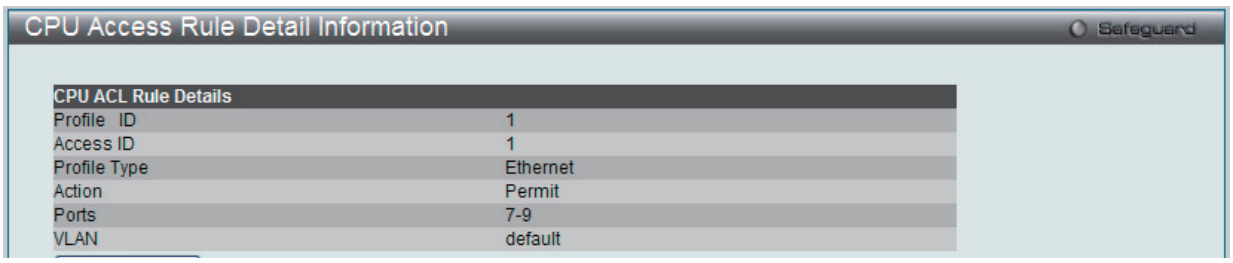


図 10-34 CPU Access Rule Detail Information - Ethernet 画面

作成した CPU アクセスプロファイルに対するルールの設定手順（IP）：

IP アクセスルールの設定

「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。

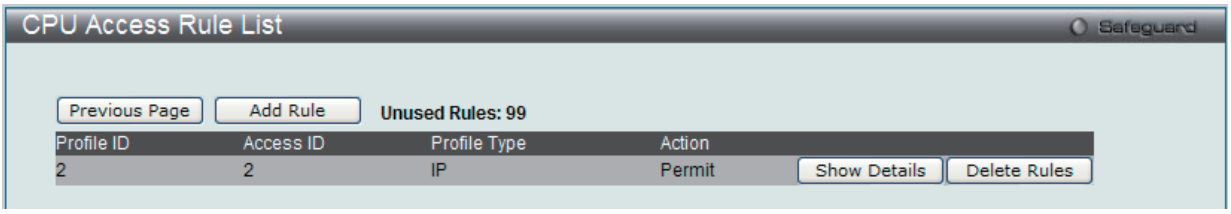


図 10-35　CPU Access Rule List - IP 画面

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」ボタンをクリックします。

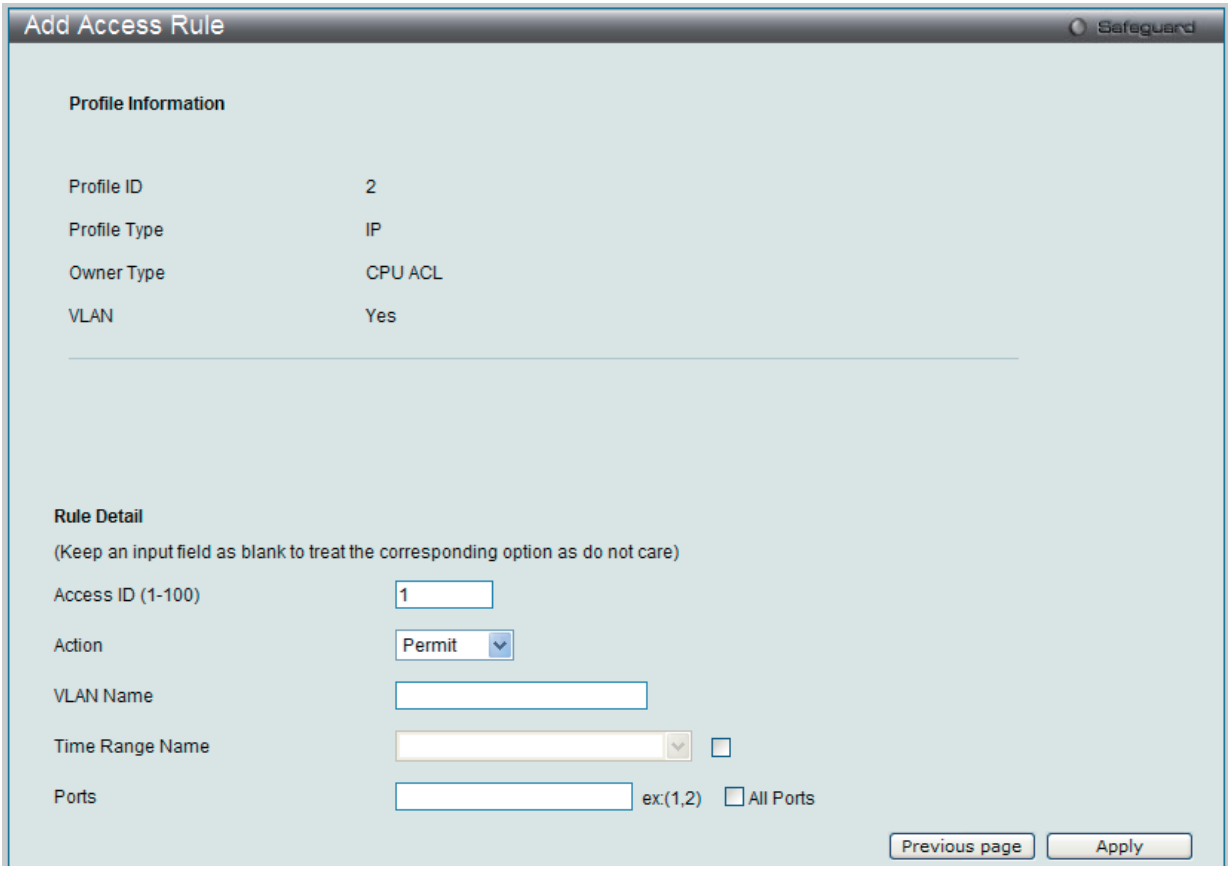


図 10-36　Add Access Rule - IP 画面

項目	説明
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。
Action	• Permit - アクセスプロファイルに一致したパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。
VLAN Name	既に設定している VLAN 名を指定します。
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	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。「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。

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。

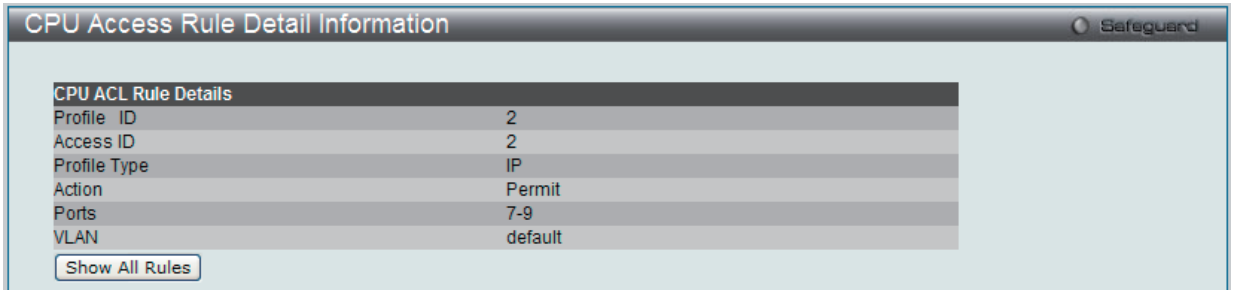


図 10-37 CPU Access Rule Detail Information - IP 画面

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

「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。

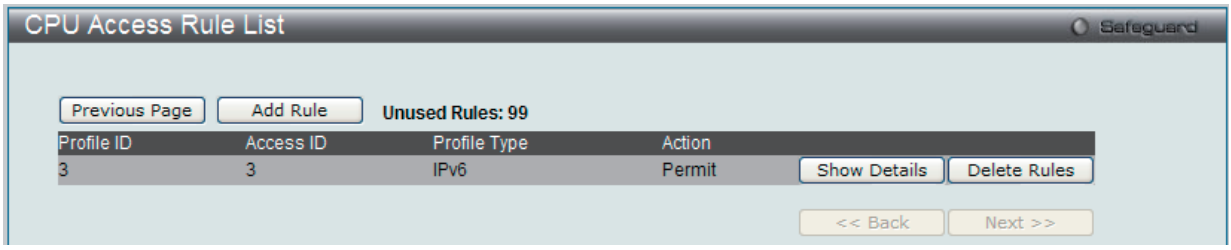


図 10-38 CPU Access Rule List - IPv6 画面

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」ボタンをクリックします。

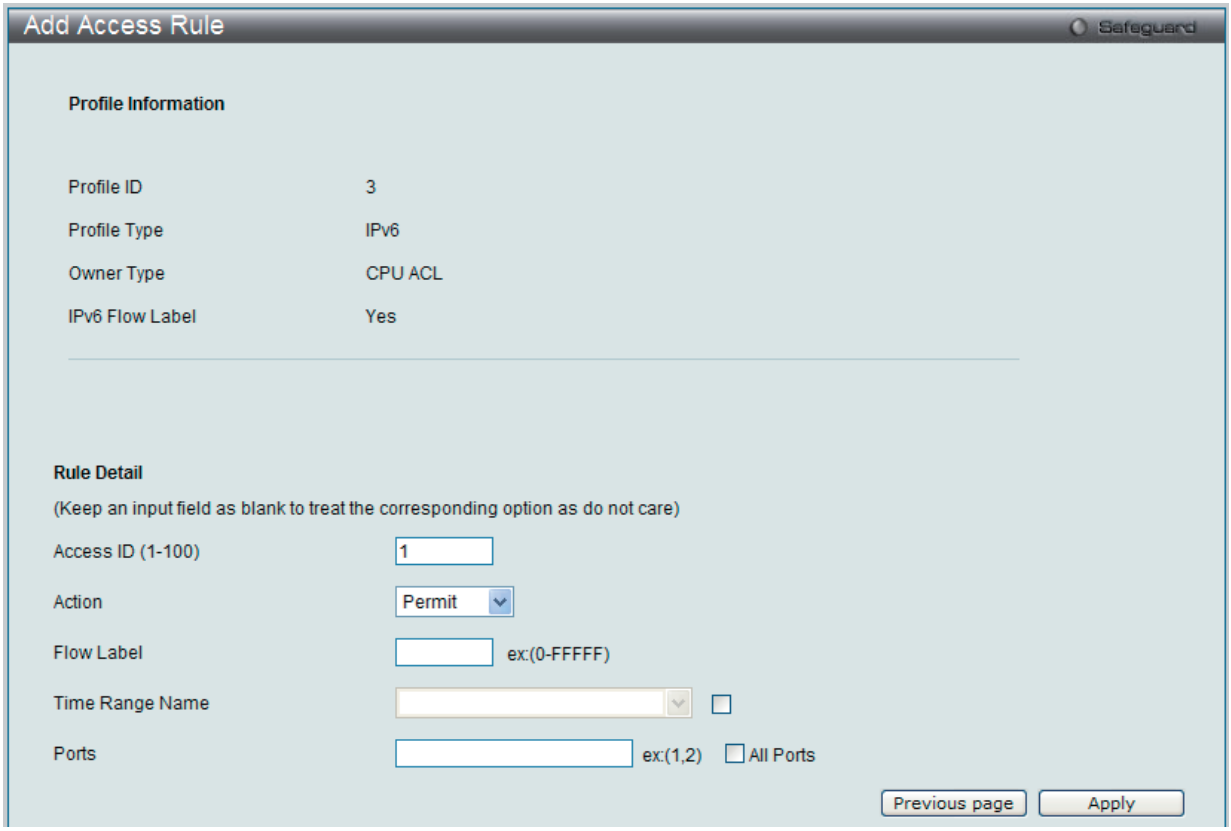


図 10-39 Add Access Rule - IPv6 画面

項目	説明
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。
Flow Label	この項目を選ぶと IPv6 ヘッダの flow label 項目を調べます。flow label 項目は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
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	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。「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。

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。

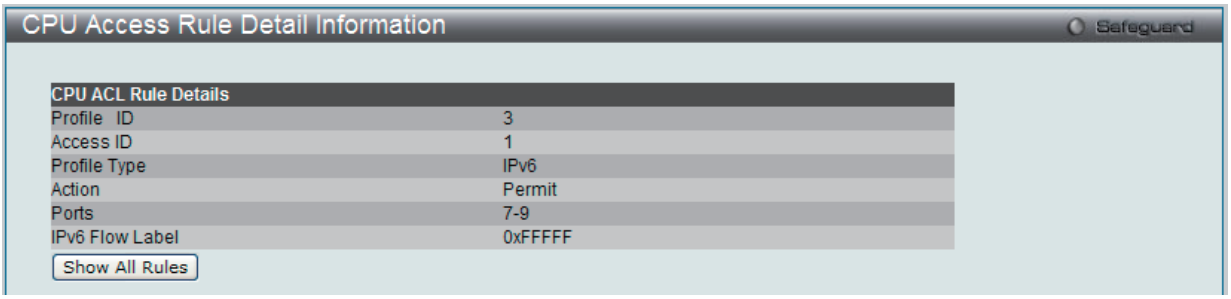


図 10-40 CPU Access Rule Detail Information - IPv6 画面

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

「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。

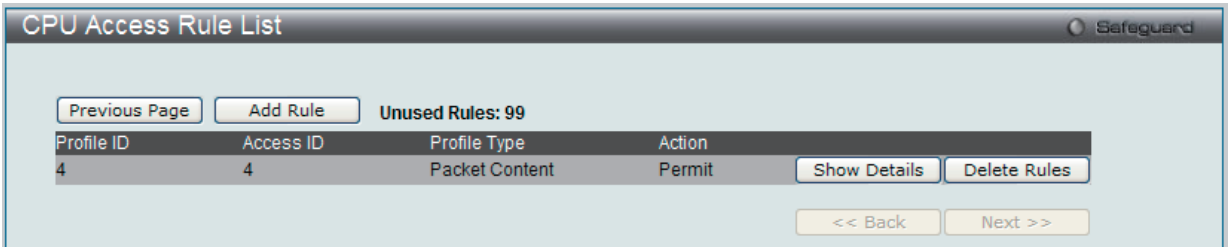


図 10-41 CPU Access Rule List - Packet Content 画面

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。

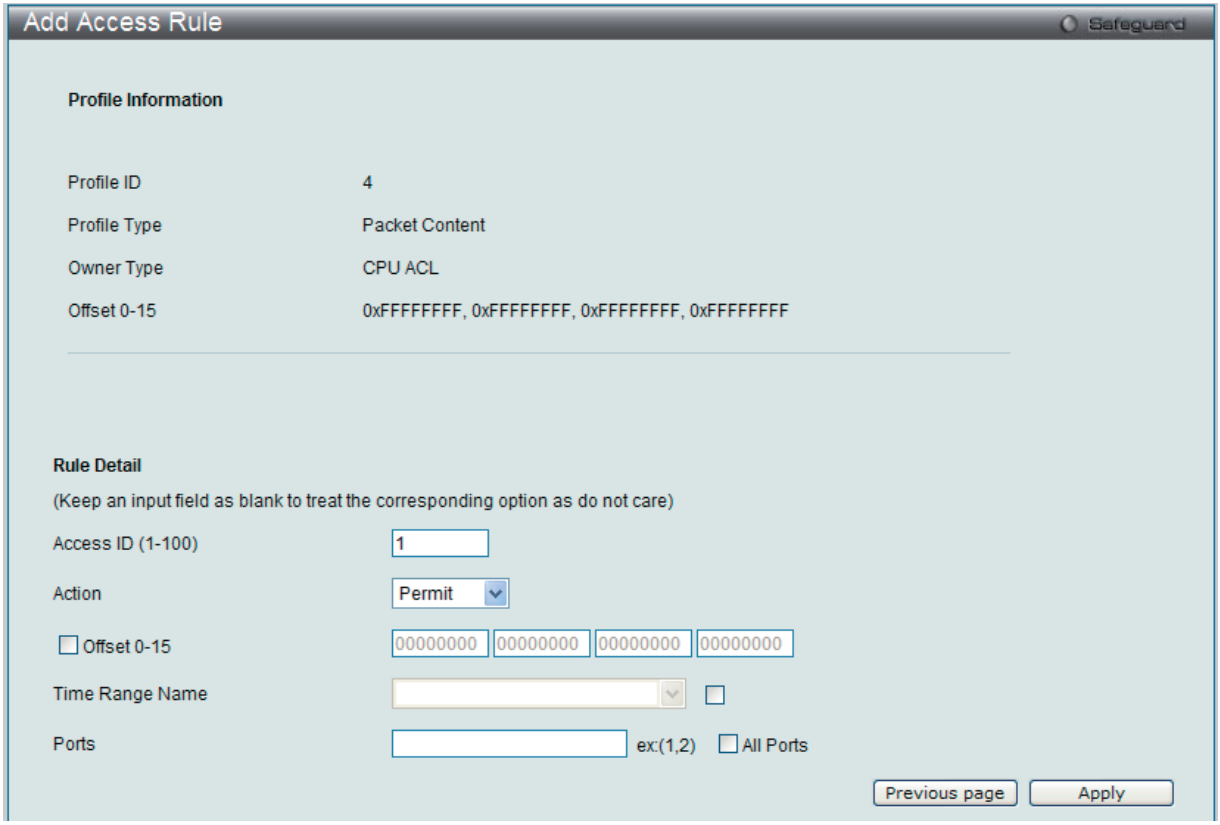


図 10-42　Add Access Rule - Packet Content 画面

項目	説明
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。
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	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。「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。

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。

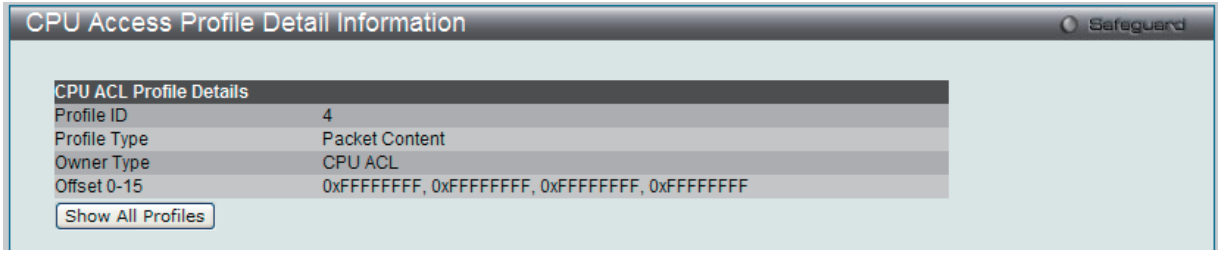


図 10-43　CPU Access Rule Detail Information - Packet Content 画面

Time Range Settings（タイムレンジ設定）

「Time Range Settings」画面は、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するために使用します。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。

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

ACL > 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。

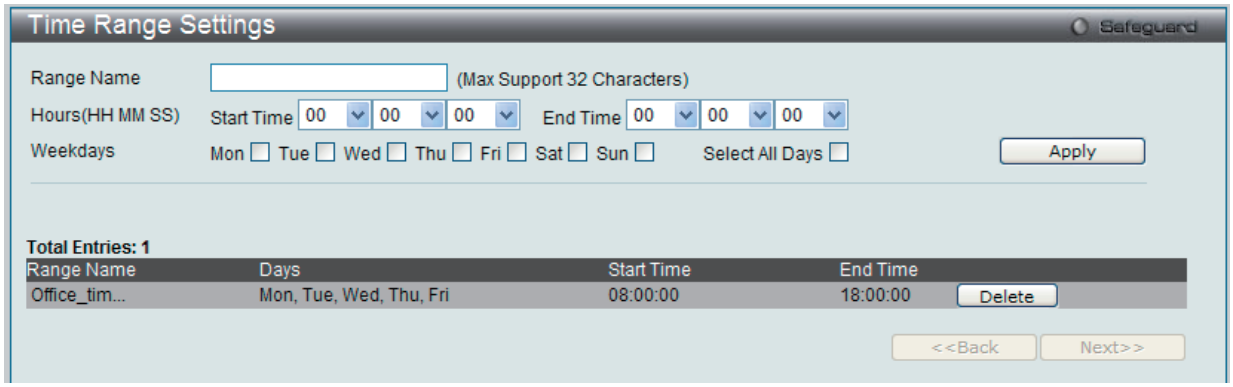


図 10-44 Time Range Settings 画面

以下の項目を設定することができます。

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

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

第 11 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
Device Environment（デバイス環境情報）	ファンや温度などデバイスの状態を表示します。	217 ページ
Cable Diagnostic（ケーブル診断機能）	ケーブルの品質やエラーの種類を診断します。	218 ページ
CPU Utilization（CPU 使用率）	CPU 使用率を表示します。	219 ページ
Port Utilization（ポート使用率）	ポートの帯域使用率を表示します。	220 ページ
Packet Size（パケットサイズ）	受信パケット数を表示します。	221 ページ
Packets（パケット統計情報）	パケット統計情報を表示します。	222 ページ
Errors（パケットエラー）	エラー統計情報を表示します。	226 ページ
Port Access Control（ポートアクセスコントロール）	802.1X 統計情報をポートごとに表示します。	229 ページ
Browse ARP Table（ARP テーブルの参照）	スイッチ上の現在の ARP エントリを表示します。	238 ページ
Browse VLAN（VLAN の参照）	各ポートの VLAN ステータスを VLAN ごとに表示します。	238 ページ
Browse Router Port（ルータポートの参照）	ルータポートを参照します。	239 ページ
Browse MLD Router Port（MLD ルータポートの参照）	IPv6 ルータポートを参照します。	239 ページ
Browse Session Table（セッションテーブルの参照）	最後に起動してからの管理セッションを表示します。	239 ページ
IGMP Snooping Group（IGMP Snooping グループ）	IGMP Snooping テーブルを表示します。	240 ページ
MLD Snooping Group（MLD Snooping グループ）	MLD Snooping テーブルを表示します。	240 ページ
WAC Authenticating State（WAC 認証状態）	現在の WAC 認証状態の表示、および WAC 認状態の設定を削除します。	241 ページ
JWAC Host Table（JWAC ホストテーブル）	JWAC ホストテーブルを表示します。	241 ページ
MAC Address Table（MAC アドレステーブル）	ダイナミック MAC アドレスフォワーディングテーブルを表示します。	242 ページ
System Log（システムログ）	ヒストリログを表示します。	243 ページ
MAC Authentication State（MAC アドレス認証状態）	MAC ベースアクセスコントロールの認証情報を表示します。	244 ページ

Device Environment（デバイス環境情報）

「Device Environment」画面では、現在のスイッチのファン状態（DGS-3200-16/GE のみ）や温度の情報を表示します。

Monitoring > Device Environment メニューをクリックし、以下の画面を表示します。

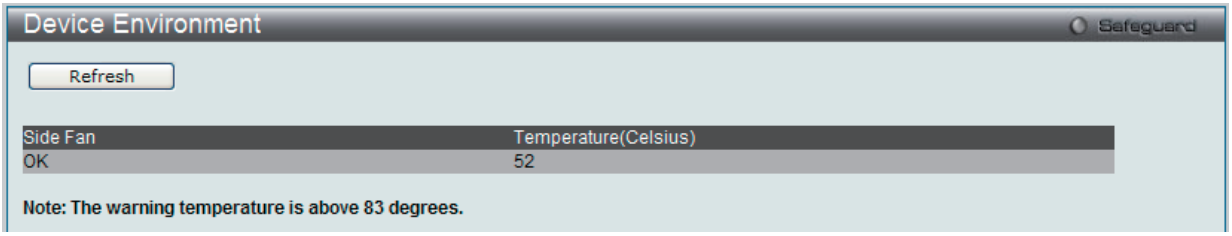


図 11-1　Device Environment 画面（DGS-3200-16/GE）

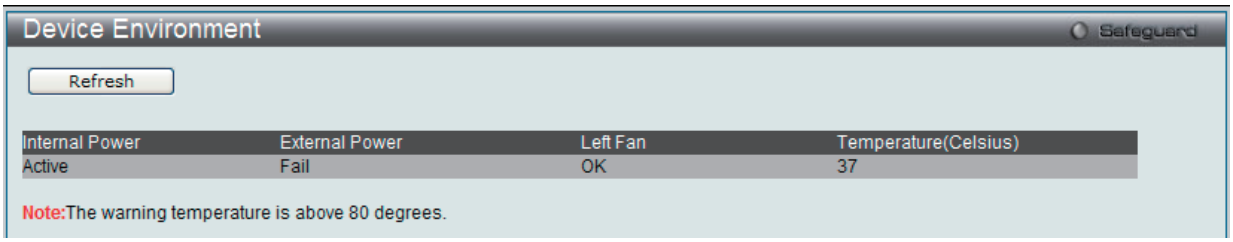


図 11-2　Device Environment 画面（DGS-3200-24/GE）

「Refresh」ボタンをクリックすると、最新の情報に更新されます。

Cable Diagnostic（ケーブル診断機能）

ケーブル診断機能は主に管理者とカスタマサービス担当者が UTP ケーブルを検査、テストするために設計されています。ケーブルの品質やエラーの種類を即座に診断します。

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

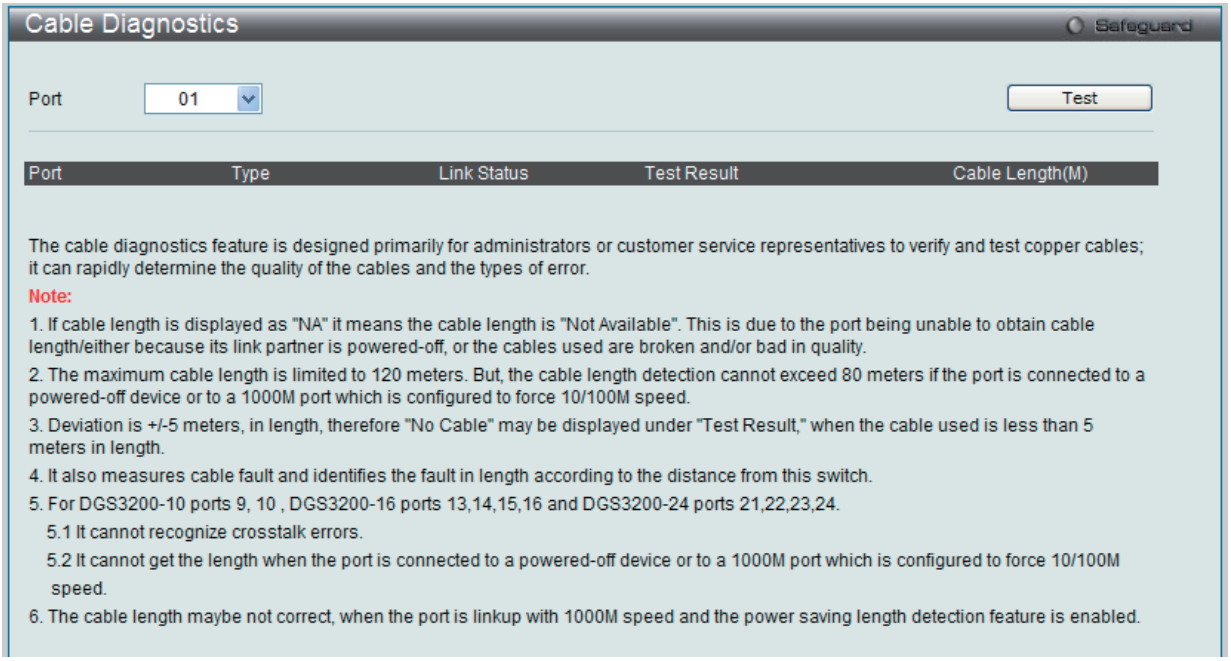


図 11-3　Cable Diagnostic 画面

特定のポートに対するケーブル診断を表示するためには、プルダウンメニューを使用してポートを選択し、「Test」ボタンをクリックします。情報が画面に表示されます。

ケーブル診断機能の注意点

1. DGS-3200-10 のポート 9 と 10、DGS-3200-16/GE のポート 13-16 および DGS-3200-24/GE のポート 21 - 24 には以下の 2 つの注意点があります。
   - クロストークエラーは認識されません。
   - ポートが 10/100M バイトの通信速度になっているか、または電源オフである 1000M バイトのポートに接続している場合、ケーブル長を取得することはできません。

2. 診断結果でケーブル長が「NA」の場合、診断不可であることを意味します。

3. ポートが電源オフのデバイスに接続している場合や 10/100M バイトの速度に接続している場合は、ケーブル長は 80 メートルを超えることはできません。

4. ケーブルが 1 メートル未満の場合、正確な測定値は得られません。

5. 長さの誤差は +/-5m です。

6. ケーブル障害および障害距離はスイッチからの距離により確認します。

CPU Utilization（CPU 使用率）

「CPU Utilization」画面では、現在の CPU 使用率をパーセント表示し、また指定した時間間隔で計算した平均値も表示します。

Monitoring > CPU Utilization メニューをクリックし、以下の画面を表示します。

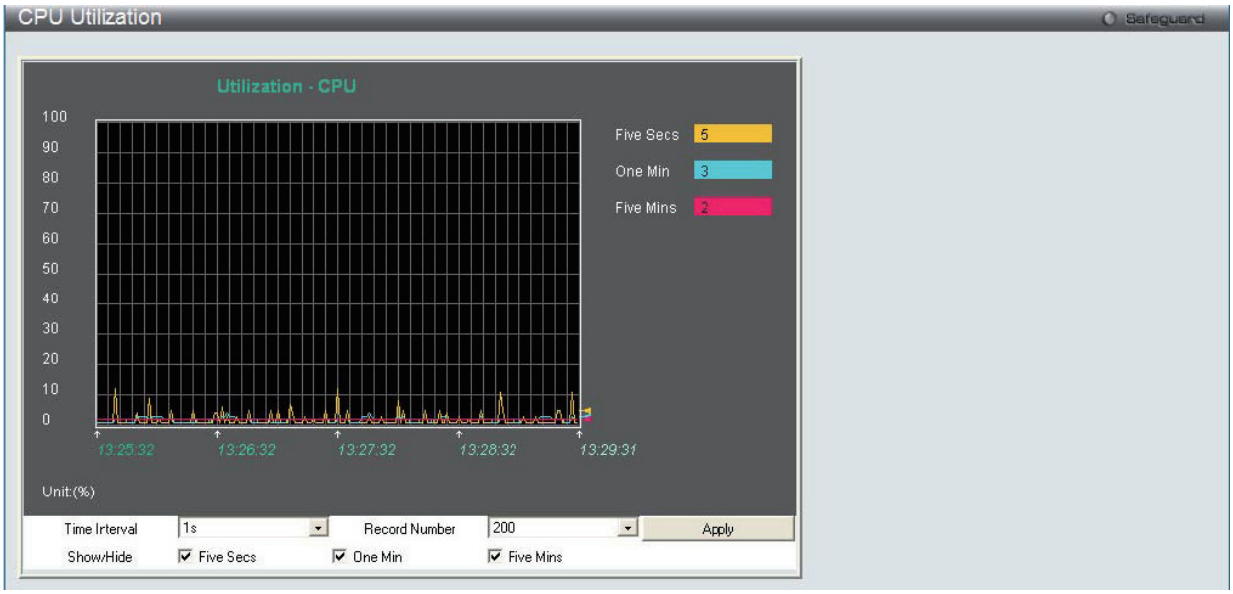


図 11-4　CPU Utilization 画面

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。

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 > 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。

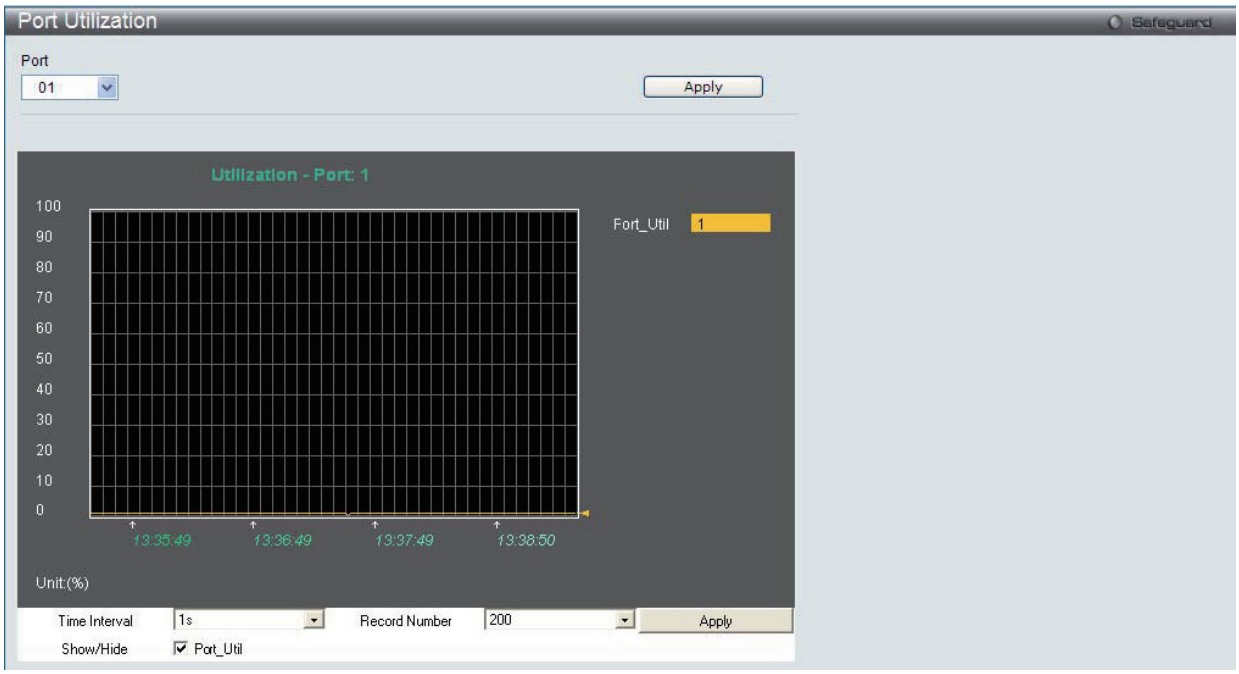


図 11-5　Port Utilization 画面

統計情報を参照するためには、プルダウンメニューでポート番号を選択します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

以下の設定項目が使用できます。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Show/ Hide	「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。

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 > 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。

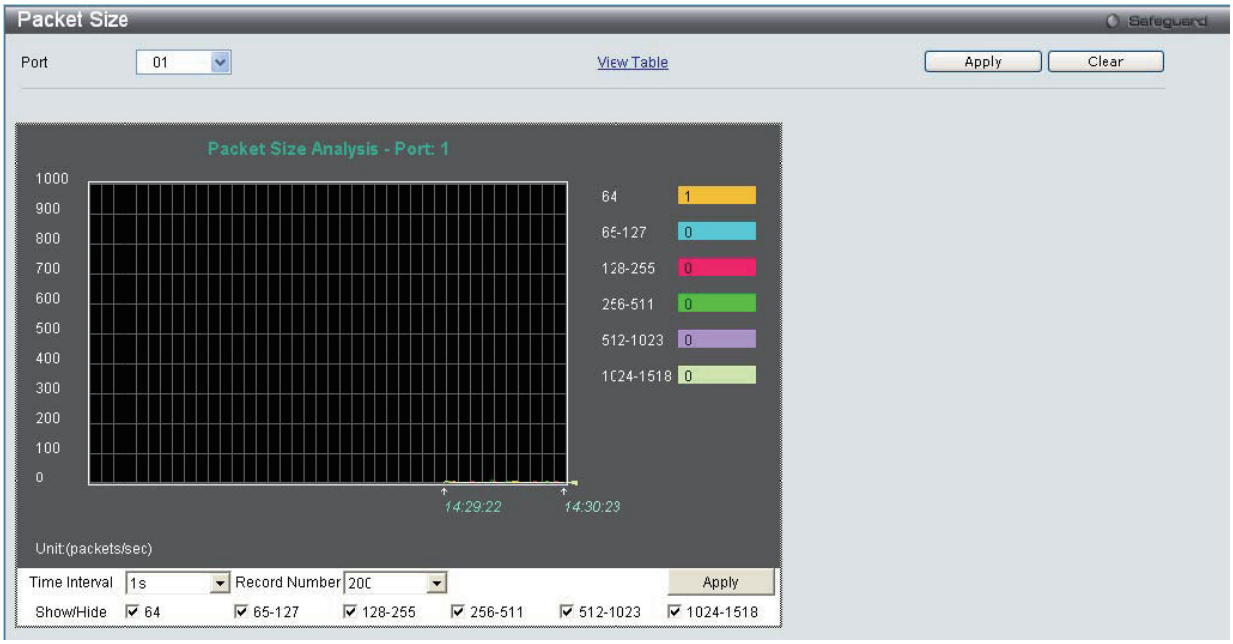


図 11-6　Packet Size 画面（折れ線グラフ）

「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 11-7　Packet Size Table 画面（表形式）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
64	サイズが 64 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
65-127	サイズが 65 から 127 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
128-255	サイズが 128 から 255 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
256-511	サイズが 256 から 511 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
512-1023	サイズが 512 から 1023 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
1024-1518	サイズが 1024 から 1518 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
Show/ Hide	64、65-127、128-255、256-511、512-1023、または 1024-1518 の受信パケットを表示 / 非表示にします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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

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 > 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。

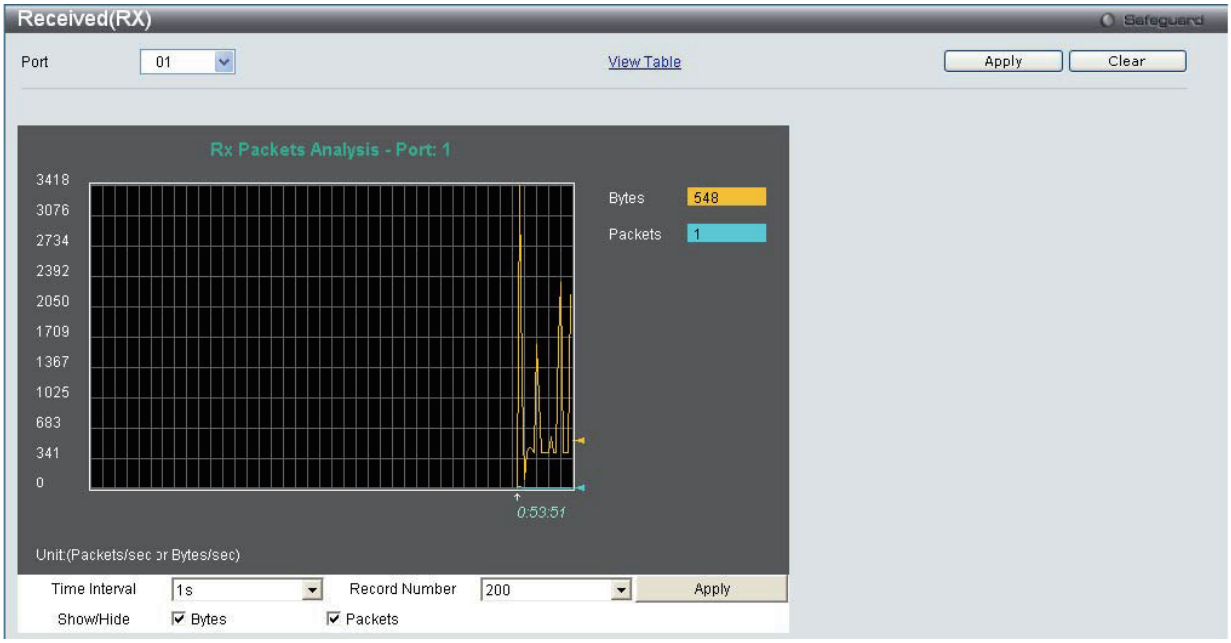


図 11-8　Received（RX）Table 画面（バイトとパケットの折れ線グラフ）

「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。

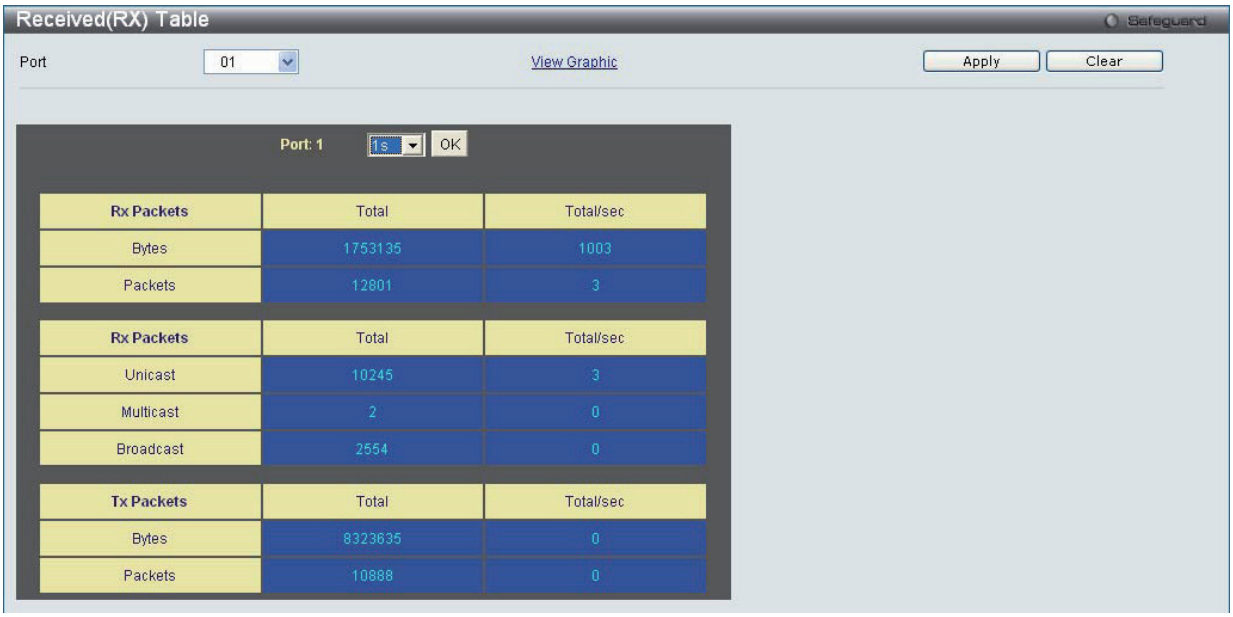


図 11-9　Received（RX）Table 画面（バイトとパケットの表）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Bytes	ポートに受信したパケット量（バイト）
Packets	ポートに受信したパケット数
Unicast	ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストキャストアドレスが受信した正常なパケットの合計数をカウントします。
Show/ Hide	Bytes と Packets を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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

UMB_cast（RX）（UMB Cast パケット統計情報の参照）

UMB（ユニキャスト、マルチキャスト、ブロードキャスト）に関する折れ線グラフを表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > 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。

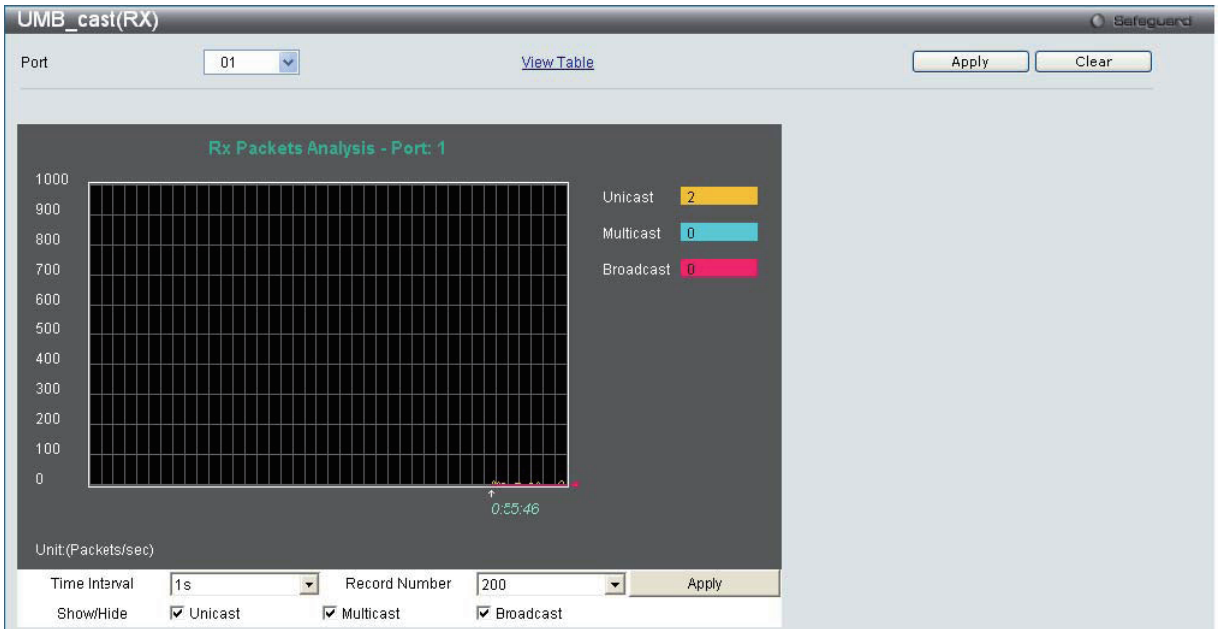


図 11-10　UMB_cast（RX）画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の折れ線グラフ）

「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 11-11　UMB_cast（RX）Table 画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の表形式表示）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Unicast	ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが受信した正常なパケットの合計数をカウントします。
Show/ Hide	Unicast、Multicast、Broadcast を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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

Transmitted（TX）（送信パケット統計情報）

スイッチから送信したパケットの情報をグラフ表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > 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。

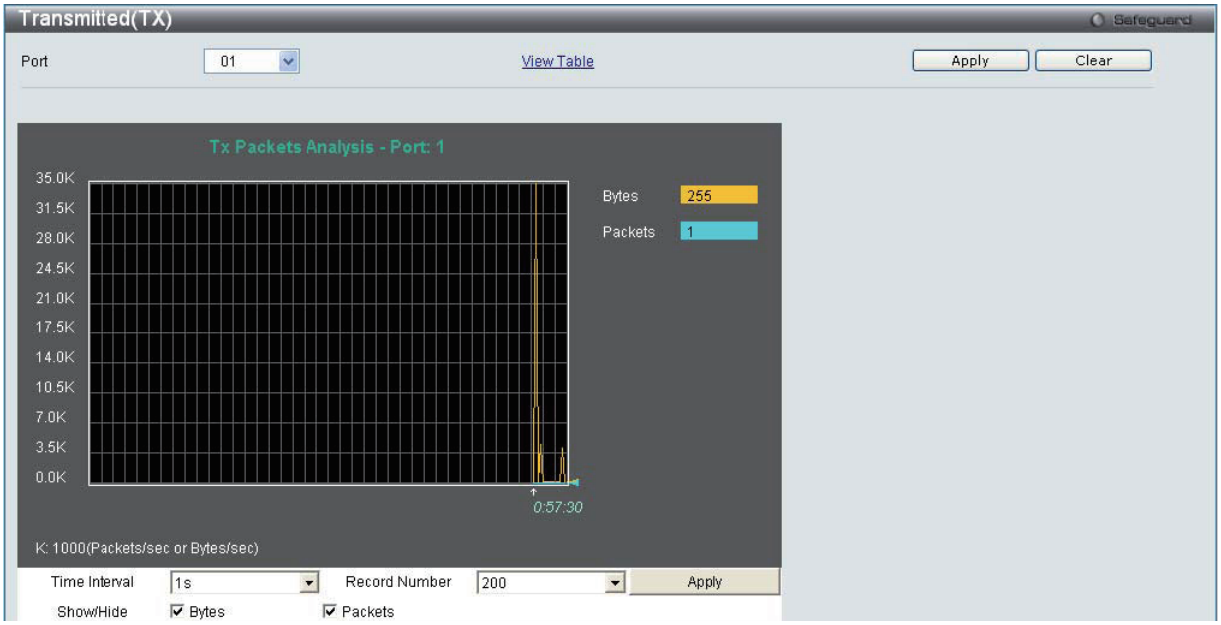


図 11-12　Transmitted（TX）画面（パケットサイズ、パケット数の折れ線グラフ表示）

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。

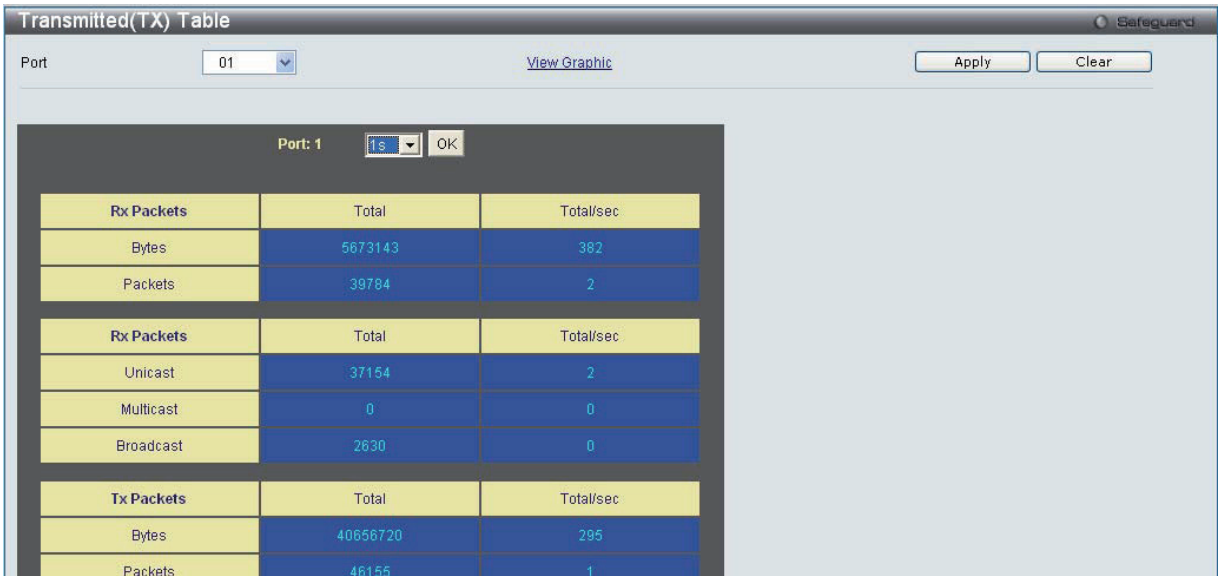


図 11-13　Transmitted（TX）Table 画面（パケットサイズ、パケット数の表示）

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Bytes	ポートから送信に成功したパケット量（バイト）。
Packets	ポートから送信に成功したパケット数。
Unicast	ユニキャストアドレスが送信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが送信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが送信した正常なパケットの合計数をカウントします。
Show/ Hide	Bytes と Packets を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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

Errors（パケットエラー）

Web マネージャは、スイッチの管理エージェントが集計したエラー統計情報を、折れ線グラフまたは表形式で表示します。以下の 4 つの画面で表示できます。

Received（Rx）（受信エラーパケット統計情報の参照）

スイッチが受信したエラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Error > 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。

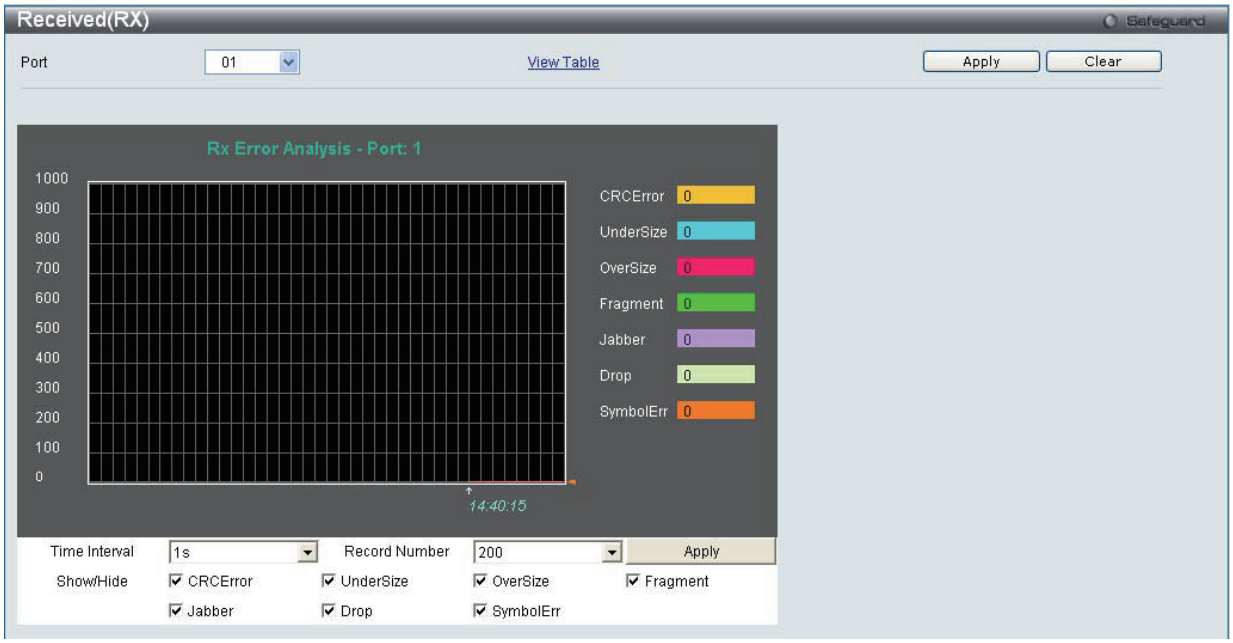


図 11-14　Received（RX）- Error 画面（折れ線グラフ形式）

表形式の「Received（RX）Table」画面を表示するためには、「View Table」リンクをクリックします。

図 11-15　Received（RX）Table - Error 画面（表形式）

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
CRCError	CRC エラーがある受信パケット数。パケットの許容値のバイト（オクテット）で終了しない正常なパケットの数。
UnderSize	パケットの最小許容値である 64 バイト以下で、CRC 値は正常なパケットの受信数。アンダーサイズパケットはコリジョンの発生を示しています。
OverSize	エラーパケットが 1518 オクテットより長く、さらに MAX_PKT_LEN より短い正常な受信パケットをカウントします。内部的には MAX_PKT_LEN は 1536 オクテットです。
Fragment	64 バイト以下でフレーミングエラーや無効な CRC を含むパケット受信数。これらのパケットはコリジョンの発生に起因します。
Jabber	エラーパケットが 1518 オクテットより長く、さらに MAX_PKT_LEN より短い不正な受信パケットをカウントします。内部的には MAX_PKT_LEN は 1536 オクテットです。
Drop	前回の再起動からその時点までに廃棄したパケット数。
Symbol	物理的に配下にあるシンボル内に受信したエラーパケット数。
Show/ Hide	CRCError、UnderSize、OverSize、Fragment、Jabber、Drop および SymbolErr を表示するかどうかをチェックします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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

Transmitted（TX）（送信エラーパケット統計情報の参照）

スイッチでの送信エラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Error > Transmitted（TX）の順にメニューをクリックし、以下の画面を表示します。

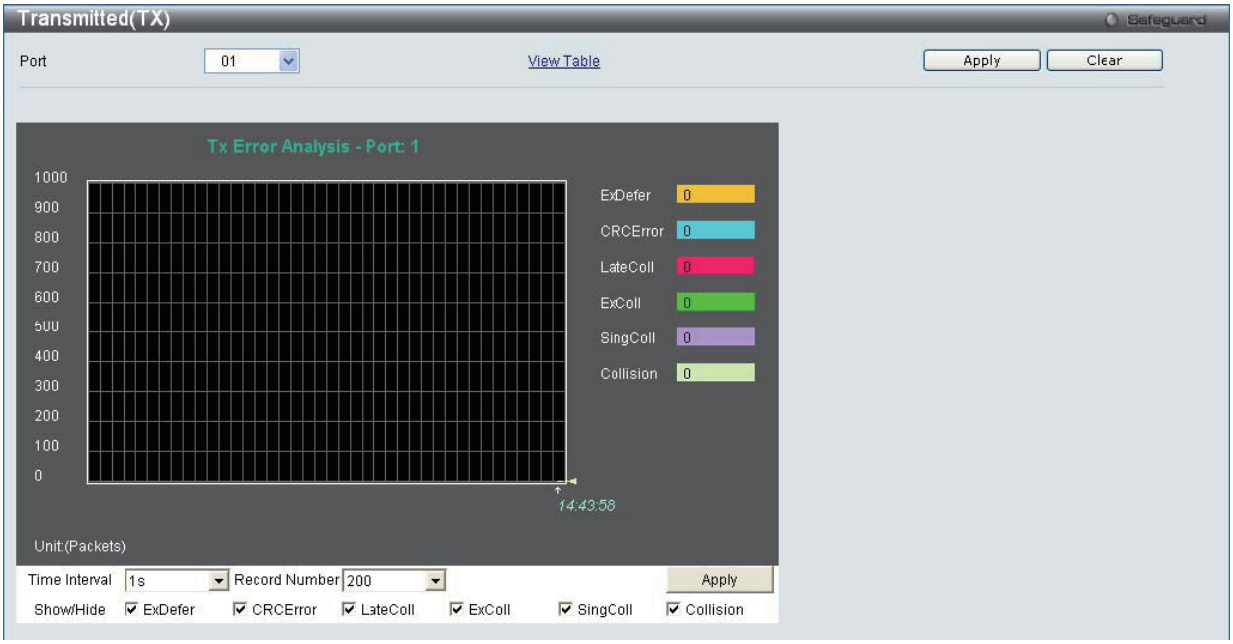


図 11-16　Transmitted（TX）- Error 画面（折れ線グラフ形式）

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 11-17　Transmitted（TX）Table - Error 画面（表形式）

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
ExDefer	特定のインタフェースに対する最初の送信が回線ビジーのために遅延したパケット数をカウントします。
CRC Error	CRC エラーがある受信パケット数。パケットの許容値のバイト（オクテット）で終了しない正常なパケットの数。
LateColl	パケットの送信に 512bit times より大きい往復遅延時間を検出されたコリジョンの回数をカウントします。
ExColl	過度のコリジョンのために送信エラーとなったパケット数。
SingColl	シングルコリジョンフレーム数。1 個以上のコリジョンにより送信されていなかったパケットで送信に成功した数。
Collision	ネットワークセグメントにおける推定総コリジョン数。
Show/ Hide	CRCError、UnderSize、OverSize、Fragment、Jabber、Drop および SymbolErr を表示するかどうかをチェックします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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

Port Access Control（ポートアクセスコントロール）

以下の画面ではスイッチ上の 802.1X の統計情報をポートごとに表示します。「Port Access Control」フォルダ中の画面はスイッチの 802.1X 統計情報をポートごとに表示する際に使用します。

Monitoring > Port Access Control の順にメニューをクリックします。このセクションには 7 個のモニタ画面があります。

RADIUS Authentication（RADIUS 認証）

このテーブルは 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。

「RADIUS Authentication」画面を参照するためには、**Monitoring > Port Access Control > RADIUS Authentication** をクリックします。

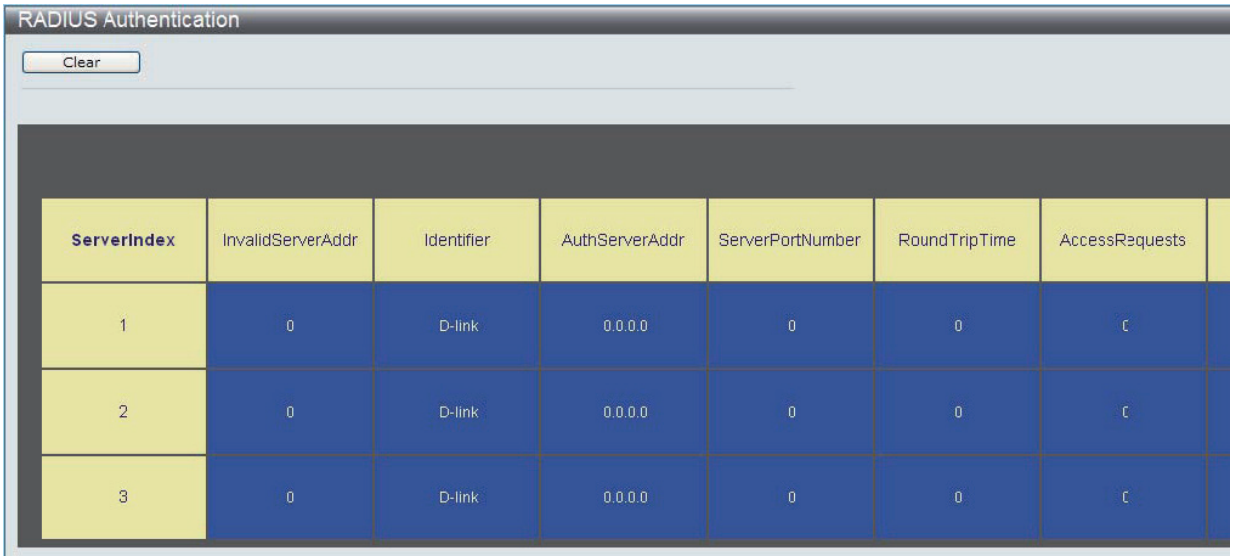


図 11-18　RADIUS Authentication 画面

統計情報の更新間隔を 1s から 60s（s：秒）で選択します。初期値は 1s（1 秒）です。現在の統計情報をクリアするためには左上角の「Clear」ボタンをクリックします。以下の情報が表示されます。

項目	説明
ServerIndex	クライアントが暗号鍵を共有している各 RADIUS 認証サーバに割り当てられた識別子の番号。
InvalidServerAddr	不明なアドレスから受信した RADIUS Access-Response パケット数。
Identifier	RADIUS 認証クライアントの NAS 識別子。（MIB II の sysName と同じである必要はありません。）
AuthServerAddr	クライアントが暗号鍵を共有している RADIUS 認証サーバを一覧にしているテーブル。
ServerPortNumber	クライアントがこのサーバにリクエストを送信するために使用する UDP ポート。
RoundTripTime	最も最近 RADIUS 認証サーバから送信された Access-Reply/Access-Challenge と Access-Request の間隔（1/100 秒単位）。
AccessRequests	サーバに送信された RADIUS Access-Request パケット数。再送信は含まれません。
AccessRetrans	本 RADIUS 認証サーバに再送信された RADIUS Access-Request パケット数。
AccessAccepts	本サーバから受信した RADIUS Access-Accept パケット数（有効 / 無効パケット）。
AccessRejects	本サーバより受信した RADIUS Access-Reject パケット数（有効 / 無効パケット）。
AccessChallenges	本サーバより受信した RADIUS Access-Challenge パケット数（有効 / 無効パケット）。
AccessResponses	本サーバより受信した不正な形式の RADIUS Access-Response パケット数。不正形式のパケットには不正な長さのパケットも含まれます。不正認証、署名属性、または不明なタイプは不正な Access Responses としては含まれません。
BadAuthenticators	本サーバより受信した不正認証や署名属性 RADIUS Access-Response パケット数。
PendingRequests	まだタイムアウトになっていない、またはレスポンスを受信していないこのサーバ行きの RADIUS Access-Request パケット数。この変数は Access-Request が送信されると 1 つ増加し、Access-Accept、Access-Reject または Access-Challenge の受信、タイムアウトまたは再転送時に 1 つ減少します。
Timeouts	本サーバへの認証タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Request としてカウントされます。
UnknownTypes	本サーバから認証ポートに受信した不明なタイプの RADIUS パケット数。
PacketsDropped	本サーバから認証ポートに受信し、何らかの理由で破棄した RADIUS パケット数。

RADIUS Account Client（RADIUS アカウンティングクライアント）

本画面では 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。

「RADIUS Accounting Client」画面を参照するためには、**Monitoring > Port Access Control > RADIUS Account Client** をクリックします。

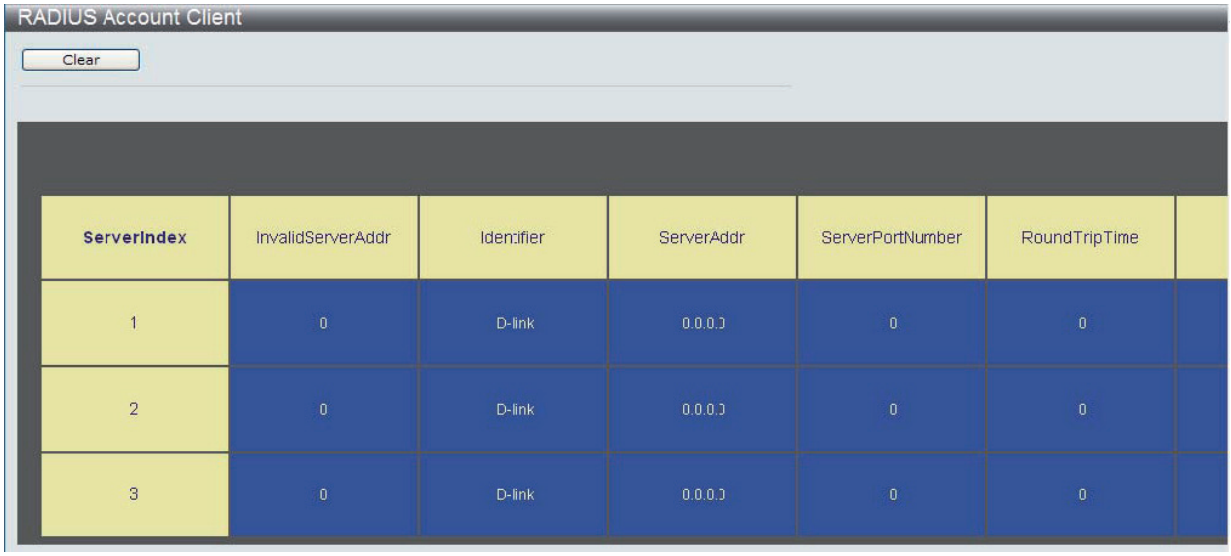


図 11-19　RADIUS Account Client 画面

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、またはレスポンスを受信していないサーバ行きの RADIUS Accounting-Request パケット数。この変数は Accounting-Request が送信された時に 1 つ加算し、Accounting-Response の受信、タイムアウトまたは再転送時に 1 つ減少します。
Timeouts	このサーバへの Accounting タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Accounting-Request としてカウントされます。
UnknownTypes	このサーバから Accounting ポートに受信した不明なタイプの RADIUS パケット数。
PacketsDropped	このサーバから Accounting ポートに受信し、何らかの理由で破棄した RADIUS パケット数。

Authenticator State（オーセンティケータの状態）

スイッチの 802.1X 認証状態を表示します。

Monitoring > **Port Access Control** > **Authenticator State** の順にメニューをクリックし、「Authenticator Status」画面を表示します。

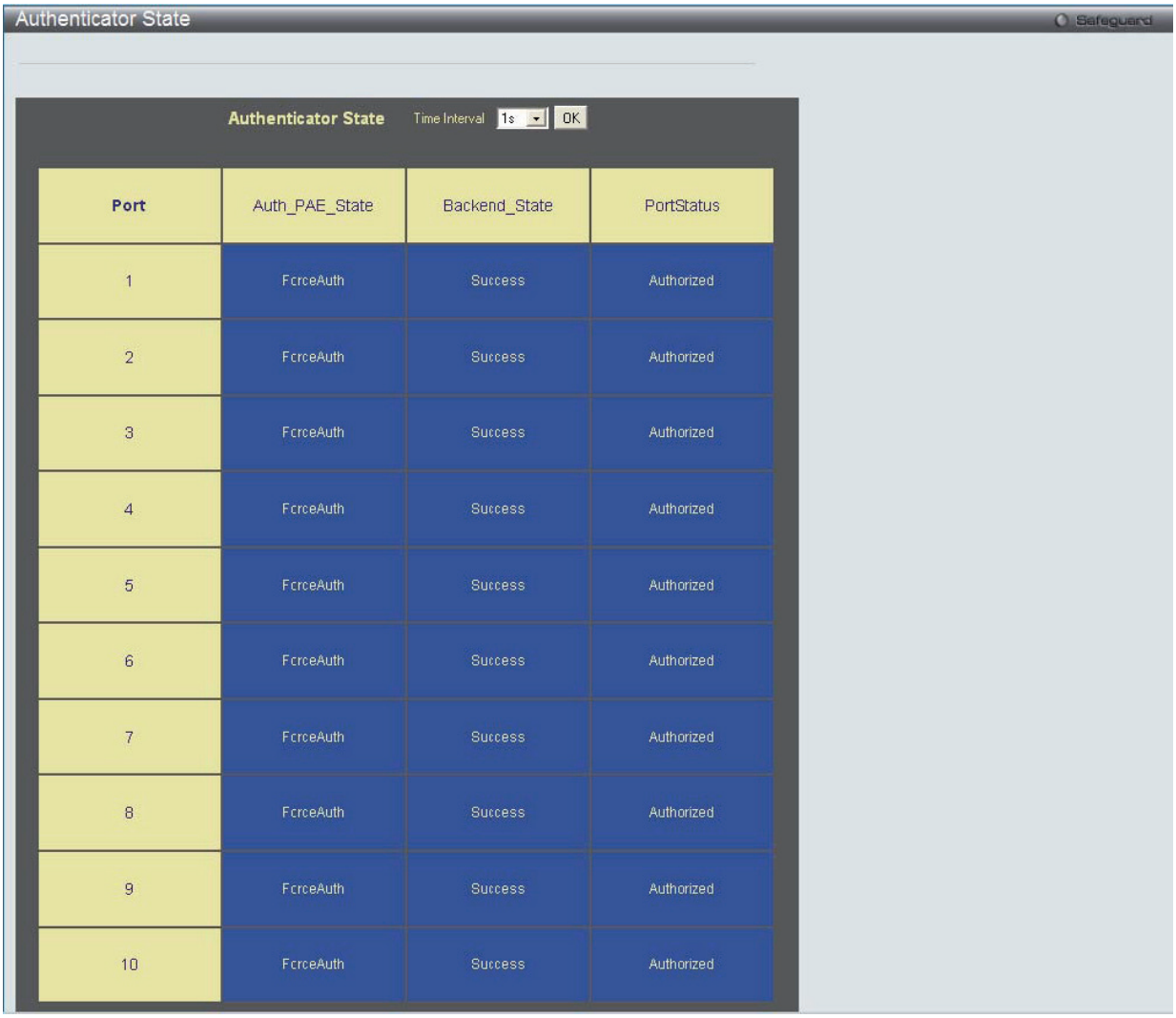


図 11-20　Authenticator State 画面（ポートベース 802.1X）

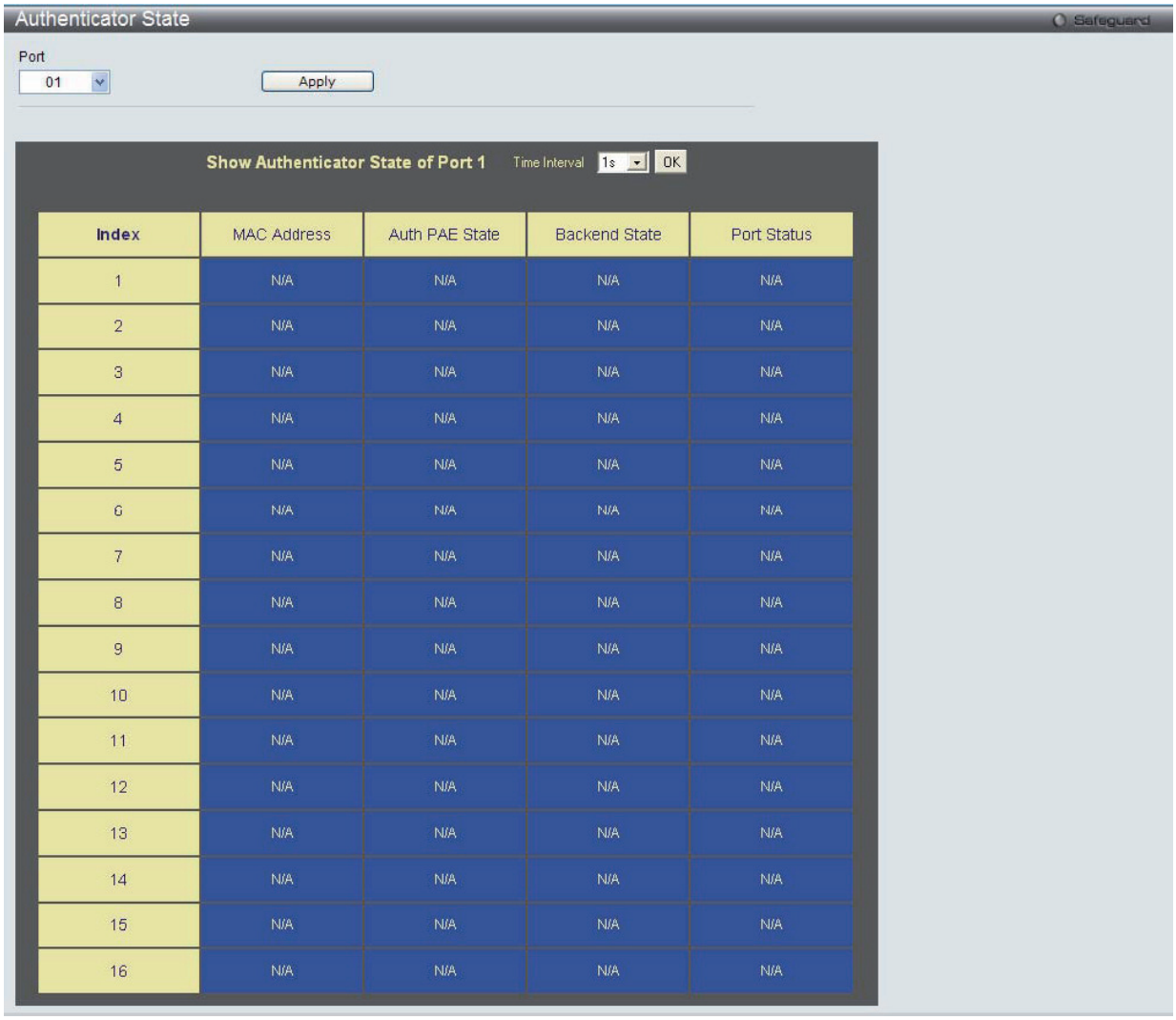


図 11-21　Authenticator State 画面（MAC ベース 802.1X）

本画面は、選択したデバイス上の各ポートについて、オーセンティケータの状態を表示します。プルダウンメニューを使用してポーリング間隔（モニタリング間隔）を 1 ～ 60 秒で選択し、「OK」ボタンをクリックします。

本画面で表示される内容は、以下の通りです。

項目	説明
Auth PAE State	オーセンティケータ PAE 状態として、「Initialize」、「Disconnected」、「Connecting」、「Authenticating」、「Authenticated」、「Aborting」、「Held」、「Force_Auth」、「Force_Unauth」、「N/A」のいずれかが表示されます。「N/A」（Not Available）はポートのオーセンティケータ機能が無効であることを示しています。
Backend State	バックエンド認証状態として、「Request」、「Response」、「Success」、「Fail」、「Timeout」、「Idle」、「Initialize」、「N/A」のいずれかが表示されます。「N/A」（Not Available）はポートのオーセンティケータ機能が無効であることを示しています。
Port Status	制御ポート状態として、「Authorized」、「Unauthorized」または「N/A」のいずれかが表示されます。
MAC Address	該当するインデックス番号のデバイスの MAC アドレスを表示します。

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。

Authenticator Statistics（Authenticator 統計情報）

この画面には各ポートに関連する Authenticator PAE に関する統計情報オブジェクトが含まれます。Authenticator 機能をサポートする各ポートの表にエントリが表示されます。

「Authenticator Statistics」画面を参照するためには、**Monitoring > Port Access Control > Authenticator Statistics** の順にクリックします。

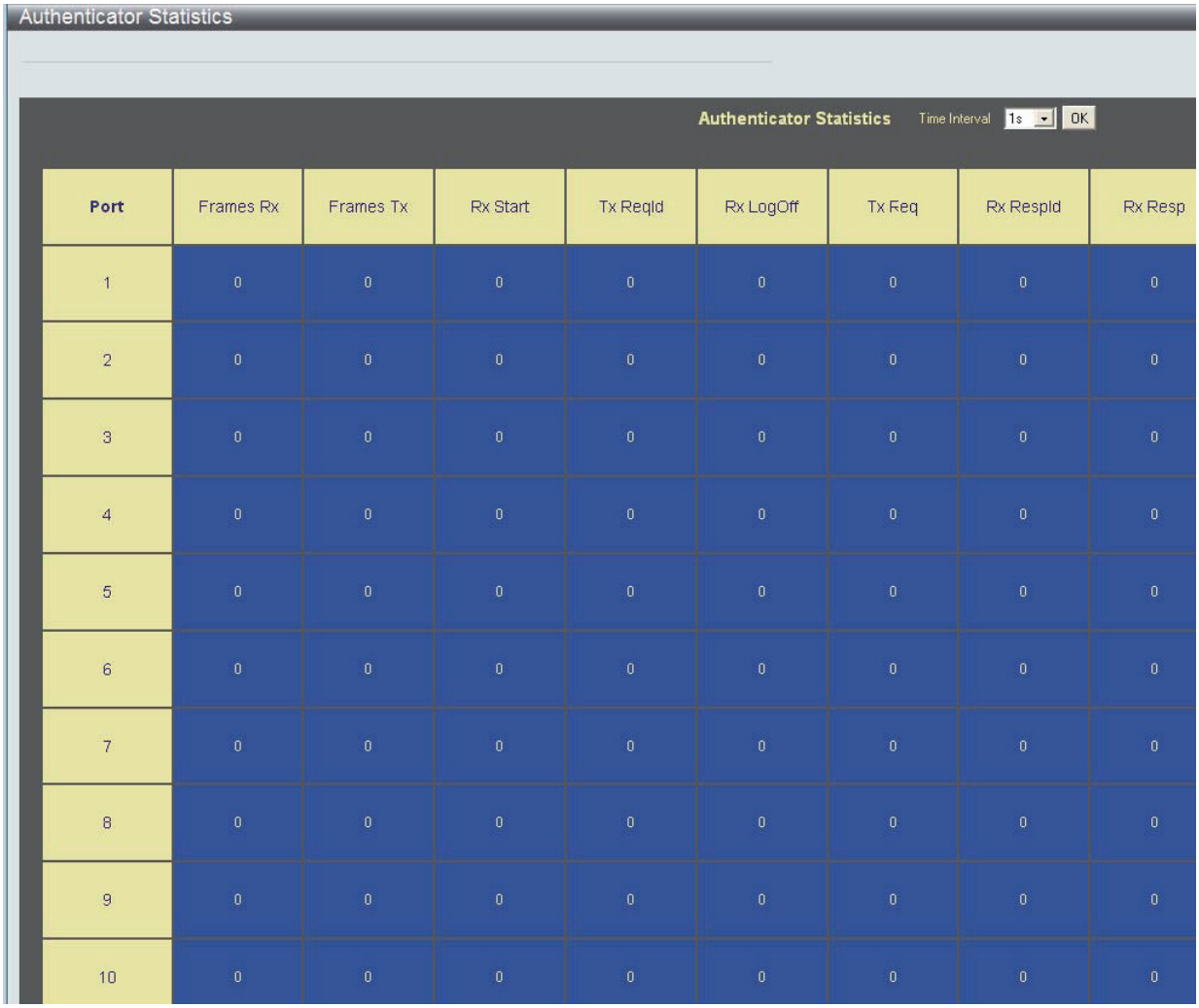


図 11-22　Authenticator Statistics 画面

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。
以下の情報が表示されます。

項目	説明
Port	システムによってポートに割り当てられた識別番号。
Frames Rx	Authenticator が受信した有効な EAPOL フレーム数。
Frames Tx	Authenticator が送信した EAPOL フレーム数。
Rx Start	Authenticator が受信した EAPOL Start フレーム数。
Tx ReqId	Authenticator が送信した EAP Req/Id フレーム数。
Rx LogOff	Authenticator が受信した EAPOL Logoff フレーム数。
Tx Req	Authenticator が送信した EAP Request フレーム（Rq/Id フレーム以外）数。
Rx RespId	Authenticator が受信した EAP Resp/Id フレーム数。
Rx Resp	Authenticator が受信した有効な EAP Response フレーム（Resp/Id フレーム以外）数。
Rx Invalid	Authenticator が受信した認識されないフレームタイプを含む EAPOL フレーム数。
Rx Error	Authenticator が受信した Packet Body Length が不正な EAPOL フレーム数。
Last Version	受信 EAPOL フレームを最も最近送信したプロトコルバージョン。
Last Source	受信 EAPOL フレームを最も最近送信した送信元 MAC アドレス。

Authenticator Session Statistics（Authenticator セッション統計情報）

この表には各ポートに関連する Authenticator PAE に関するセッションオブジェクト統計情報が含まれます。Authenticator 機能をサポートする各ポートの表にエントリが表示されます。

「Authenticator Session Statistics」画面を参照するためには、**Monitoring > Port Access Control > Authenticator Session Statistics** の順にクリックします。

図 11-23　Authenticator Session Statistics 画面（MAC ベース 802.1X 認証）

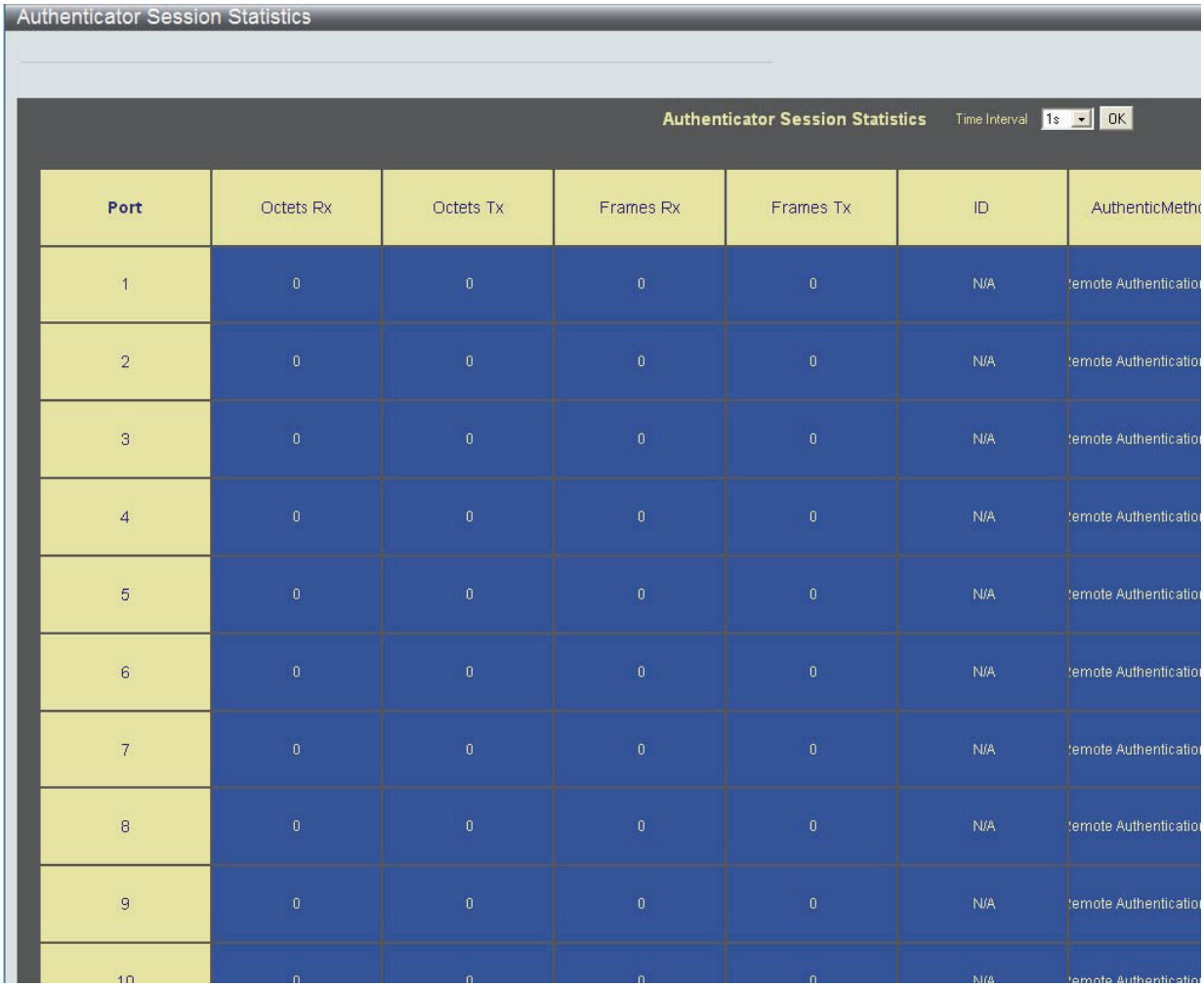


図 11-24　Authenticator Session Statistics 画面（ポートベース 802.1X 認証）

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。

項目	説明
Port / Index	ポートベースの 802.1X Authentication モードでは、システムがポートに割り当てた識別番号を表示します。MAC ベースの 802.1X Authentication モードでは、エントリのインデックス番号を表示します。
Octets Rx	このポートがセッション中にユーザデータフレーム内に受信したオクテット数。
Octets Tx	このポートがセッション中にユーザデータフレーム内に送信したオクテット数。
Frames Rx	このポートがセッション中に受信したユーザデータフレーム数。
Frames Tx	このポートがセッション中に送信したユーザデータフレーム数。
ID	セッションの識別子。（半角英数字 3 文字以上）。
Authentic Method	セッションを確立するために使用する認証方式。有効な方式は以下の通りです。 1）Remote Authentic Server - 認証サーバが Authenticator のシステムより外部にある。 2）Local Authentic Server - 認証サーバが Authenticator のシステム内にある。
Time	セッション時間（秒）。
Terminate Cause	セッションが終了した原因。以下の 8 個の原因があります。 1）Supplicant ログオフ 2）ポートのエラー 3）Supplicant 再起動 4）再認証の失敗 5）AuthControlledPortControl が ForceUnauthorized に設定された。 6）ポートの再初期化 7）ポート管理が無効 8）まだ終了していない
UserName	Supplicant PAE との一致を表すユーザ名。

Authenticator Diagnostics（Authenticator 診断）

この表には各ポートに関連する Authenticator の操作に関する診断情報が含まれ、Authenticator 機能をサポートする各ポートの表にエントリが表示されます。

「Authenticator Diagnostics」を参照するためには、**Monitoring > Port Access Control > Authenticator Diagnostics** の順にクリックします。

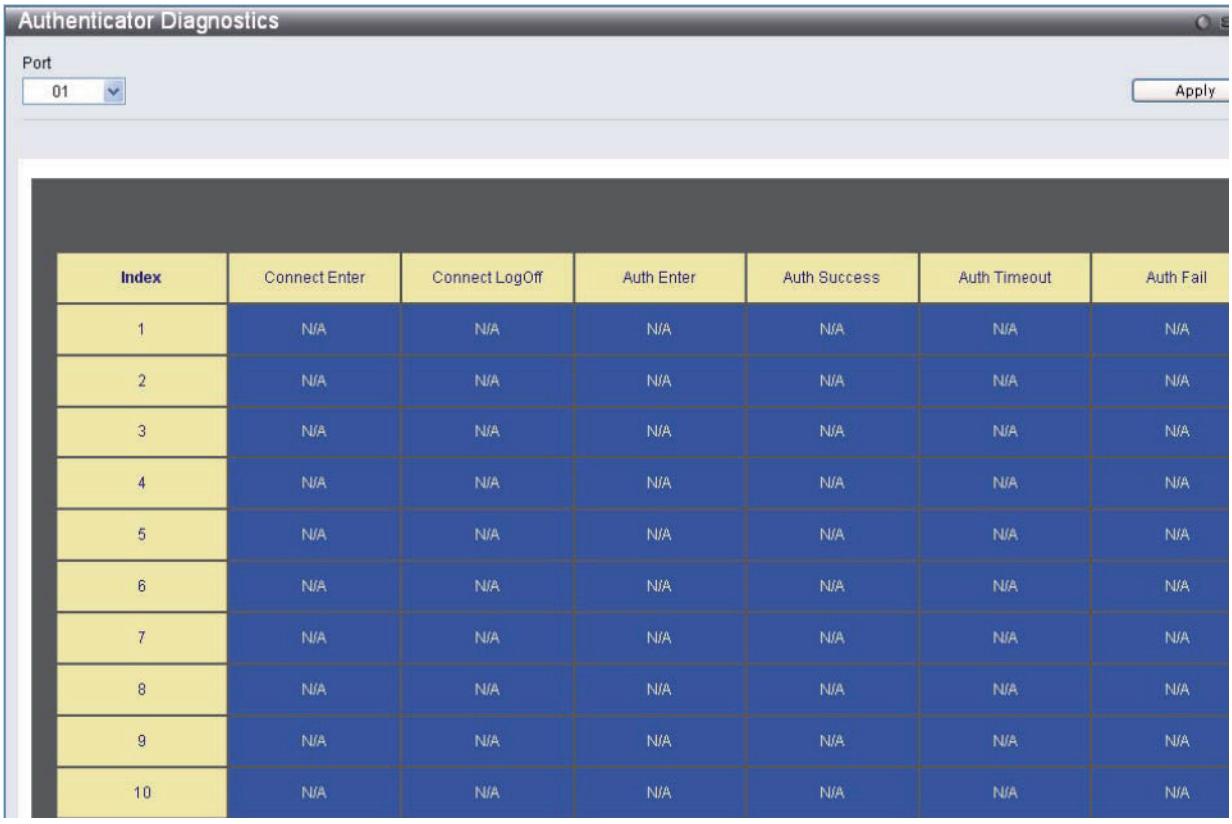


図 11-25　Authenticator Diagnostics 画面（MAC ベース 802.1X 認証モード）

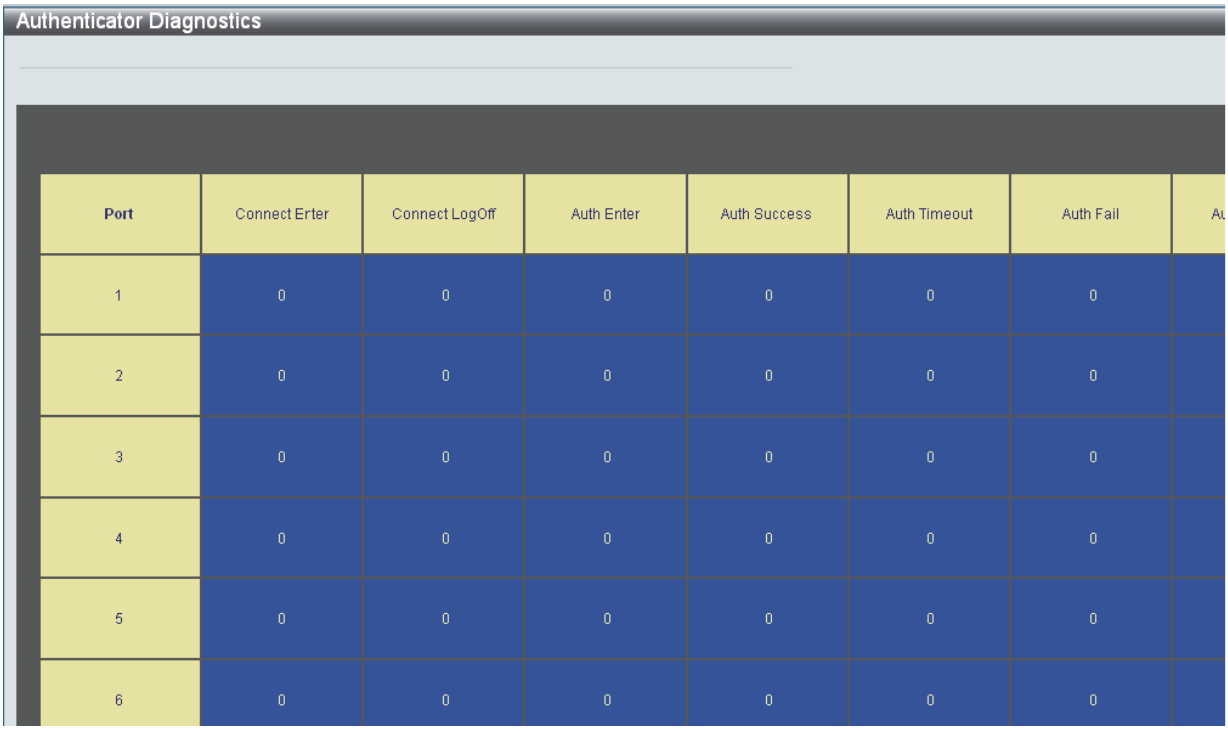


図 11-26　Authenticator Diagnostics 画面（ポートベース 802.1X 認証モード）

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。以下の情報が表示されます。

項目	説明
Port / Index	ポートベースの 802.1X Authentication モードでは、システムがポートに割り当てた識別番号を表示します。MAC ベースの 802.1X Authentication モードでは、エントリのインデックス番号を表示します。
Connect Enter	他の状態から CONNECTING 状態に状態遷移した回数をカウントします。
Connect LogOff	EAPOL-Logoff メッセージを受信した結果、CONNECTING から DISCONNECTED に状態遷移した回数をカウントします。
Auth Enter	サプリカントから EAP-Response/Identity メッセージを受信した結果、CONNECTING から AUTHENTICATING に状態遷移した回数をカウントします。
Auth Success	Backend Authentication 状態が Supplicant の認証成功（authSuccess = TRUE）となった結果、AUTHENTICATING から AUTHENTICATED に状態遷移した回数をカウントします。
Auth Timeout	Backend Authentication 状態が認証のタイムアウト（authTimeout = TRUE）となった結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
Auth Fail	Backend Authentication 状態が認証失敗（authFail = TRUE）となった結果、AUTHENTICATING から HELD に状態遷移した回数をカウントします。
Auth Reauth	再認証リクエスト（reAuthenticate = TRUE）の結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
Auth Start	サプリカントから EAPOL-Start メッセージを受信した結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
Auth LogOff	サプリカントから EAPOL-Logoff メッセージを受信した結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
Authed Reauth	再認証リクエスト（reAuthenticate = TRUE）の結果、AUTHENTICATED から CONNECTING に状態遷移した回数をカウントします。
Authed Start	サプリカントから EAPOL- Start メッセージを受信した結果、AUTHENTICATED から CONNECTING に状態遷移した回数をカウントします。
Authed LogOff	サプリカントから EAPOL-Logoff メッセージを受信した結果、AUTHENTICATED から DISCONNECTED に状態遷移した回数をカウントします。
Responses	State Machine が認証サーバに Initial Access-Request パケットを送信した（すなわちエントリ上の sendRespToServer が RESPONSE 状態となった）回数をカウントします。Authenticator が認証サーバとの通信を試みることを意味します。
AccessChallenges	State Machine が認証サーバから Initial Access-Challenge パケットを受信した（すなわち aReq が TRUE となり RESPONSE 状態を終了した）回数をカウントします。認証サーバが Authenticator との通信をしていることを意味します。
OtherReqToSupp	State Machine が EAP-Request パケット（Identity、Notification、Failure、または Success メッセージではない）をサプリカントに送信する（すなわちエントリ上の txReq が REQUEST 状態となった）回数をカウントします。Authenticator が EAP-method を選択したことを意味します。
OnNakRespFromSup	State Machine が Initial EAP-Request に対してパケットサプリカントからのレスポンスを受信し、そのレスポンスが EAP-NAK より他のものであった（すなわち rxResp が TRUE となり State Machine は REQUEST から RESPONSE 状態になったがそのレスポンスは EAP-NAK ではない）回数をカウントします。サプリカントが Authenticator の選択した EAP-method に応答することができることを意味します。
Bac Auth Success	State Machine が認証サーバから Accept メッセージを受信した（すなわち aSuccess が TRUE となり RESPONSE から SUCCESS に状態遷移した）回数をカウントします。サプリカントが認証サーバでの認証に成功したことを意味します。
Bac Auth Fail	State Machine が認証サーバから Reject メッセージを受信した（すなわち aFail が TRUE となり RESPONSE から FAIL に状態遷移した）回数をカウントします。サプリカントが認証サーバでの認証に失敗したことを意味します。

Browse ARP Table（ARP テーブルの参照）

本画面では、スイッチ上の現在の ARP エントリを表示します。

Monitoring > Browse ARP Table メニューをクリックし、「Browse ARP Table」画面を表示します。

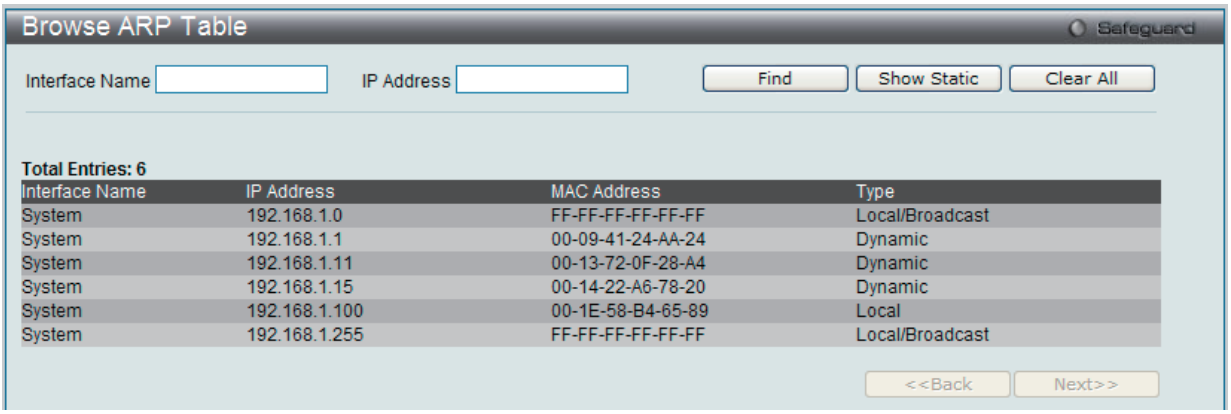


図 11-27　Browse ARP Table 画面

特定の ARP エントリを検索するためには、画面の上の「Interface Name」または「IP Address」を入力し、「Find」ボタンをクリックします。
スタティック ARP エントリを表示する場合は、「Show Static」ボタンをクリックします。
ARP Table をクリアする場合は、「Clear All」ボタンをクリックします。

Browse VLAN（VLAN の参照）

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

Monitoring > Browse VLAN メニューをクリックし、「Browse VLAN」画面を表示します。

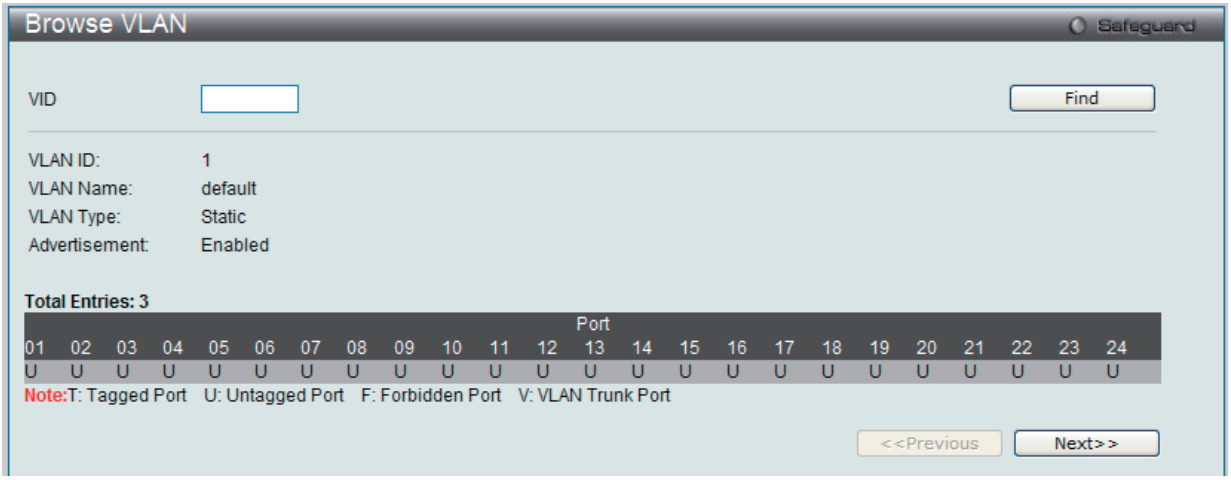


図 11-28　Browse VLAN 画面

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

Browse Router Port（ルータポート参照）

この画面ではスイッチのどのポートが現在ルータポートとして設定されているかを表示します。

Monitoring > Browse Router Port メニューをクリックし、「Browse Router Port」画面を表示します。

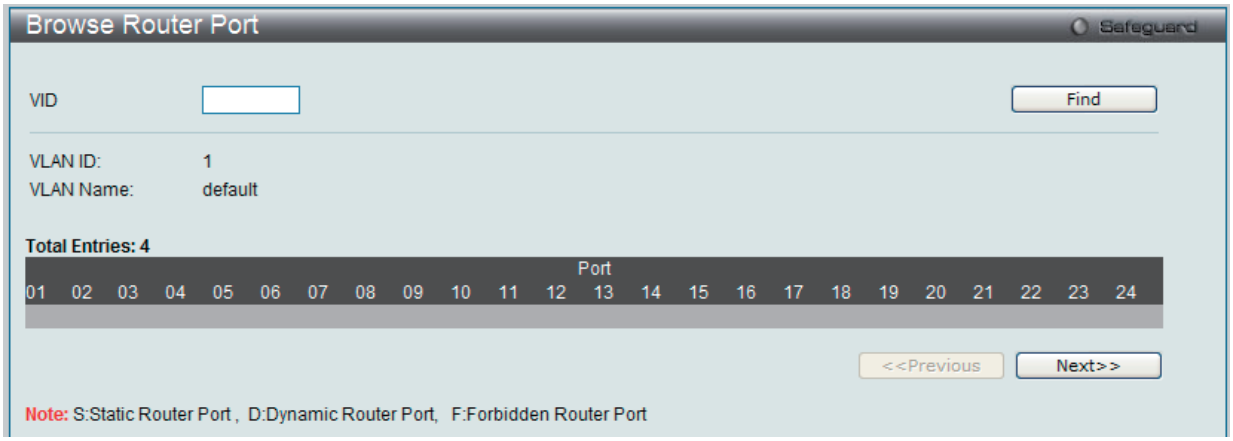


図 11-29　Browse Router Port 画面

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。

Browse MLD Router Port（MLD ルータポートの参照）

本画面では、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。

Monitoring > Browse MLD Router Port メニューをクリックし、「Browse MLD Router Port」画面を表示します。

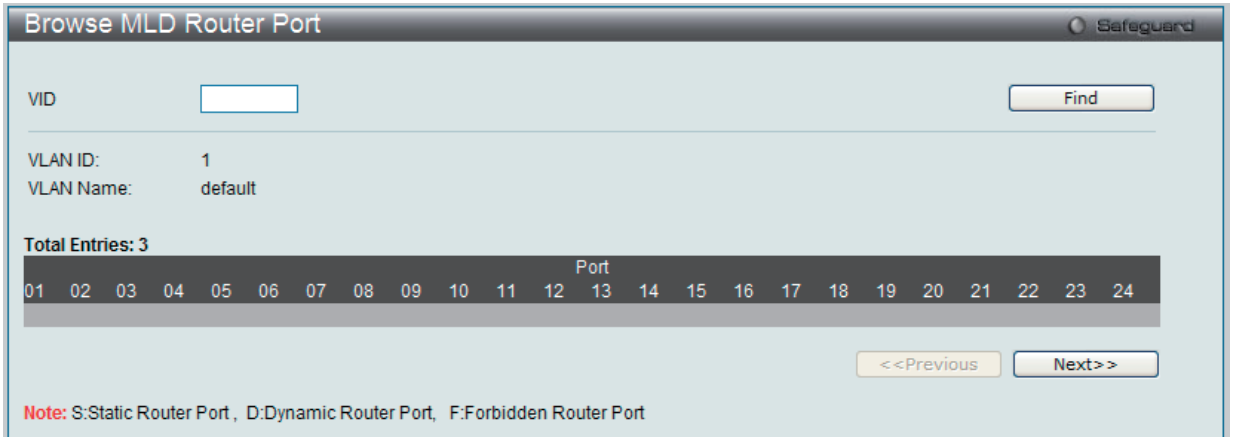


図 11-30　Browse MLD Router Port 画面

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。

Browse Session Table（セッションテーブルの参照）

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。

Monitoring > Browse Session Table メニューをクリックし、「Browse Session Table」画面を表示します。

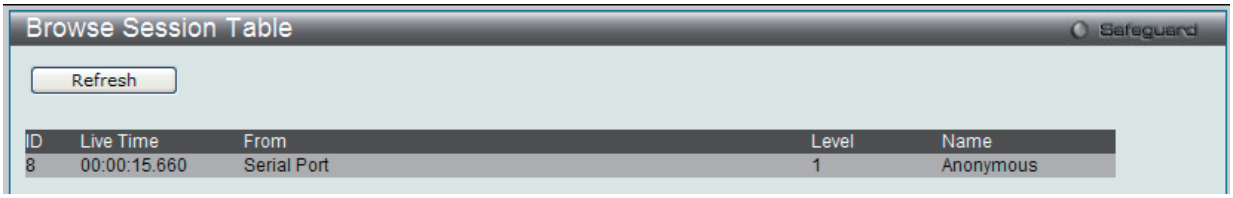


図 11-31　Browse Session Table 画面

IGMP Snooping Group（IGMP Snooping グループ）

本画面では、スイッチの「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 アドレスを取得することができます。

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

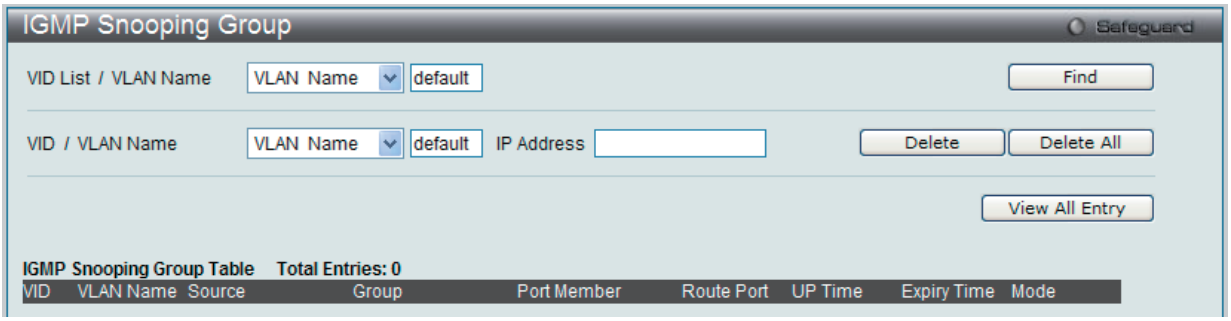


図 11-32　IGMP Snooping Group 画面

画面上の「VIDList / 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。

以下の項目が表示されます。

項目	説明
VID List / VLAN Name	マルチキャストグループの VID リストまたは VLAN 名。
VID / VLAN Name	マルチキャストグループの VID または VLAN 名。
IP Address	IP アドレスを入力します。
Source	マルチキャストグループのソース MAC アドレス。

「Delete」ボタンをクリックすると、Data Driven が学習した IGMP Snooping グループを削除します。
「Delete All」ボタンをクリックすると、Data Driven が学習したすべての IGMP Snooping グループを削除します。

注意　スイッチに IGMP Snooping の設定を行うためには、**L2 Features > IGMP Snooping > IGMP Snooping Settings** を選択します。

MLD Snooping Group（MLD Snooping グループ）

この画面でスイッチの 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。

Monitoring > MLD Snooping Group の順にメニューをクリックし、以下の画面を表示します。

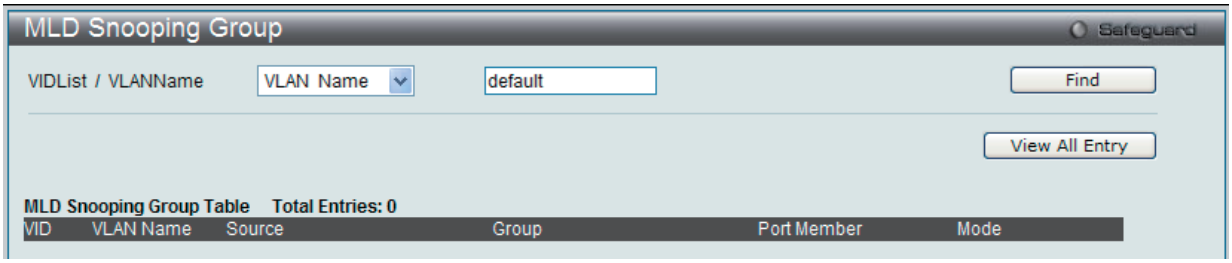


図 11-33　MLD Snooping Group 画面

画面上の「VIDList/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、本テーブルを検索することもできます。

以下の項目が表示されます。

項目	説明
VID List/VLAN Name	マルチキャストグループの VID リストまたは VLAN 名。
Source	マルチキャストグループのソース MAC アドレス。
Group	マルチキャストグループ。
Port Member	このグループのポートメンバ。
Mode	現在使用中のモード。

注意　スイッチに MLD Snooping の設定を行うためには、**L2 Features > MLD Snooping > MLD Snooping Settings** を選択します。

WAC Authenticating State（WAC 認証状態）

現在の WAC 認証状態の表示、および WAC 認状態の設定を削除します。

Monitoring > WAC Authenticating 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。

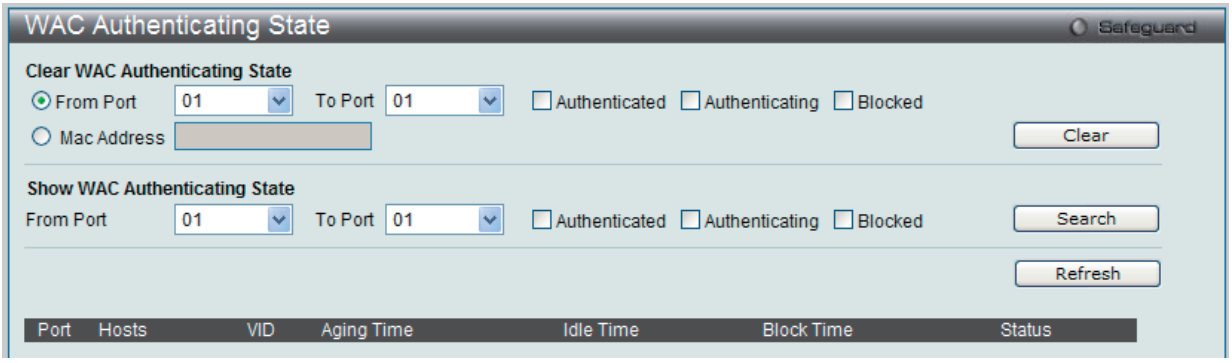


図 11-34 WAC Authenticating State 画面

以下の項目があります。

項目	説明
From Port/To Port	プルダウンメニューを使用して、ポート範囲を選択します。
MAC Address	WAC 認証状態を削除するデバイスの MAC アドレスを入力します。
Search	本ボタンをクリックして、検索を開始します。
Clear	本ボタンをクリックして、上で選択した WAC 認証状態情報を削除します。
Refresh	本ボタンをクリックして、本画面の情報を更新します。
Authenticated	チェックすると、ポートに対して認証済みユーザすべてを表示します。
Authenticating	チェックすると、ポートに対して認証中ユーザすべてを表示します。
Blocked	チェックすると、ポートに対してブロックされたユーザすべてを表示します。

ポート範囲を選択し、適切なチェックボックス（「Authenticated」（認証済み）、「Authenticating」（認証中）、および「Blocked」（ブロック））を選択します。

JWAC Host Table（JWAC ホストテーブル）

JWAC のホストテーブル情報を表示します。

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

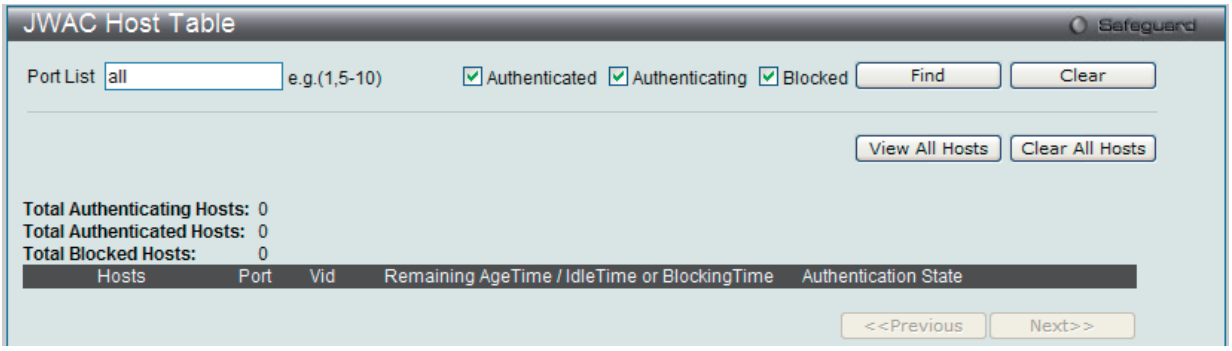


図 11-35 JWAC Host Table 画面

以下の項目があります。

項目	説明
Port List	ポートまたは範囲を指定します。
Find	本ボタンをクリックして、検索を開始します。
Clear	本ボタンをクリックして、画面の先頭の「Port List」データを削除します。
View All Hosts	本ボタンをクリックして、すべての JWAC ホストを参照します。
Clear All Hosts	本ボタンをクリックして、すべての JWAC ホストを削除します。
Authenticated	本ボタンをクリックして、認証されたクライアントホストだけを参照します。
Authenticating	本ボタンをクリックして、認証中のクライアントホストだけを参照します。
Blocked	本ボタンをクリックして、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参照します。

MAC Address Table（MAC アドレステーブル）

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。

Monitoring > 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。

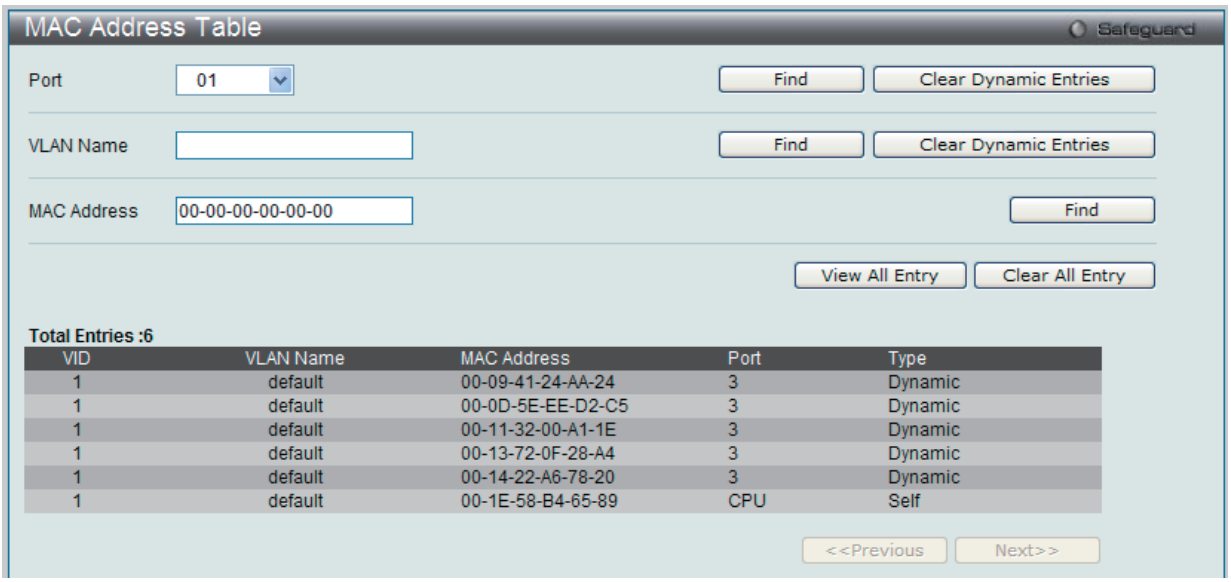


図 11-36　MAC Address Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	MAC アドレスと関連付けられるポート。
VLAN Name	フォワーディングテーブル内の検索のキーとする VLAN 名。
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。
Find	指定したポート、VLAN または MAC アドレスをキーとして検索をする際にクリックします。
Clear Dynamic Entries	アドレステーブルのすべてのダイナミックエントリを削除します。
View All Entry	アドレステーブルのすべてのエントリを表示します。
Clear All Entry	アドレステーブルのすべてのエントリを削除します。

System Log（システムログ）

Web マネージャでは、スイッチの管理エージェントでまとめたスイッチのヒストリログを表示します。

Monitoring > System Log の順にメニューをクリックし、ヒストリログの表示を行います。

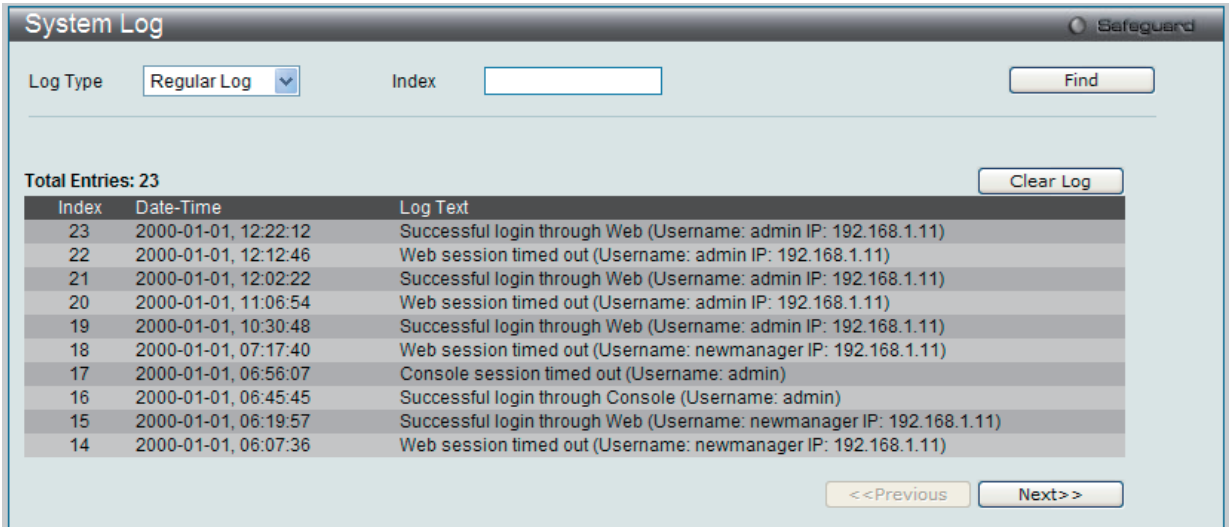


図 11-37　System Log 画面

スイッチはイベント情報を、自身のログおよび指定した SNMP トラップ受信ステーションやコンソールマネージャに接続した PC に記録することができます。「Next」ボタンをクリックすると、ヒストリログの次のページへ移動します。「Clear」ボタンをクリックすると、ヒストリログがすべて削除されます。

以下の項目が表示されます。

項目	説明
Type	ログの対応を選択します。 • Regular Log - ログインやファームウェア転送のような通常のログイベントを参照します。 • Attack Log - スプーフィング攻撃などの攻撃のログファイルを参照します。
Index	スイッチのヒストリログへのエントリが作成される時に加算されるカウンタ。最後のエントリ（最も高い数字の Sequence）を上に表示します。
Date-Time	最後の再起動からスイッチに発生したイベントの日時を表示します。
Log Text	ヒストリログエントリを発生させたイベントに関する説明を表示します。

注意　本画面中に表示されるログイベントについての詳細な情報については、本マニュアルの 253 ページの「付録 C ログイベント」を参照してください。

MAC Authentication State（MAC アドレス認証状態）

MAC アドレス認証の MAC アドレスを表示します。

Monitoring > MAC 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。

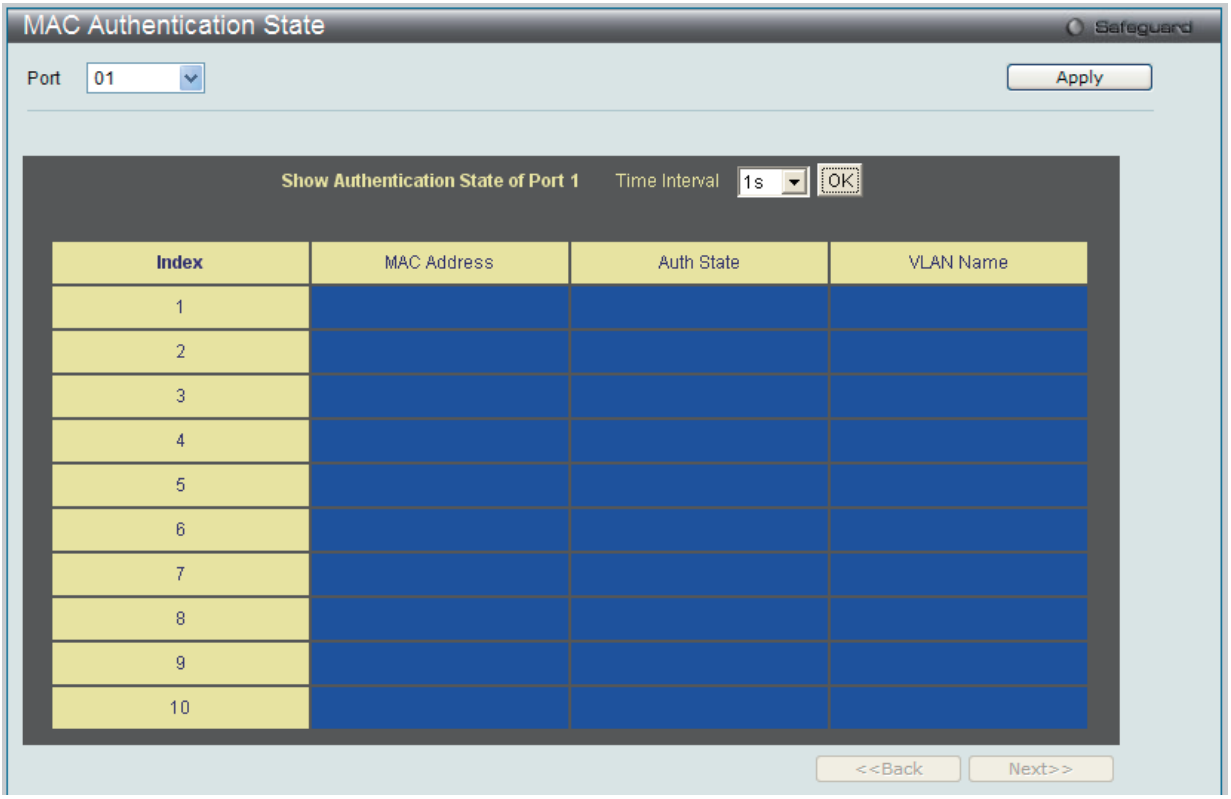


図 11-38 MAC Authentication State 画面

以下の項目が表示されます。

項目	説明
Port	プルダウンメニューを使用して、MAC 認証状態の情報を参照するポート選択します。「Apply」ボタンをクリックし、選択ポートの MAC 認証状態を参照します。
Timer Interval	選択ポートの MAC 認証状態の更新間隔を選択します。「OK」ボタンをクリックして、更新間隔を更新します。
Index	MAC 認証状態エントリのインデックス番号を表示します。
MAC Address	MAC 認証状態エントリの MAC アドレスを表示します。
Auth State	認証状態を表示します。
VLAN Name	MAC アドレスが割り当てられている VLAN 名を表示します。

第 12 章　Maintenance（スイッチのメンテナンス）

メンテナンス用のメニューを使用し、本スイッチのリセットおよび再起動等を行うことができます。

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

サブメニュー	説明	参照ページ
Save（コンフィグレーションとログの保存）		
Save Configuration（コンフィグレーションの保存）	スイッチのメモリにコンフィグレーションを保存します	246 ページ
Save Log（ログの保存）	スイッチのメモリにログを保存します	246 ページ
Save All（コンフィグレーションファイルとログの保存）	スイッチのメモリにコンフィグレーションとログを保存します	246 ページ
Tools（ツールメニュー）		
Download Configuration File / Download Configuration File to NV-RAM（コンフィグレーションファイルのダウンロード）	NV-RAM にコンフィグレーションファイルをダウンロードします。	248 ページ
Download Configuration File to SD Card（SD カードへのコンフィグレーションファイルのダウンロード）（DGS-3200-24/GE のみ）	SD カードにコンフィグレーションファイルをダウンロードします。	248 ページ
Download Firmware / Download Firmware to NV-RAM（ファームウェアのダウンロード）	NV-RAM にファームウェアファイルをダウンロードします。	249 ページ
Download Firmware to SD Card（SD カードへのファームウェアのダウンロード）（DGS-3200-24/GE のみ）	SD カードにファームウェアファイルをダウンロードします。	249 ページ
Upload Configuration File / Upload Configuration File to TFP（コンフィグレーションファイルのアップロード）	コンフィグレーションファイルをアップロードします。	250 ページ
Upload Log File / Upload Log File to TFTP（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。	250 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。	251 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。	251 ページ

Save（コンフィグレーションとログの保存）

「Save」メニューには、次の 3 つのメインメニューがあります。:「Save Configuration」、「Save Log」および「Save All」

オプションには以下のものがあります。

項目	説明
Save Configuration	Save Configuration「Active」、「ID 1」または「ID 2」のインデックスを付加してコンフィグレーションファイルを保存します。DGS-3200-24/GE は「SD Card」もサポートしています。
Save Log	現在のログを NV-RAM または SD カード（DGS-3200-24/GE のみ）に保存します。
Save All	現在のコンフィグレーションファイルとログを直ちに保存します。

Save Configuration（コンフィグレーションの保存）

Web マネージャ先頭の **Save > Save Configuration** をクリックし、以下の画面を表示します。

図 12-1　Save Configuration 画面（DGS-3200-10 および DGS-3200-16/GE）

プルダウンメニューを使用して、「Configuration ID」を 1 または 2 から選択し、「Apply」ボタンをクリックします。

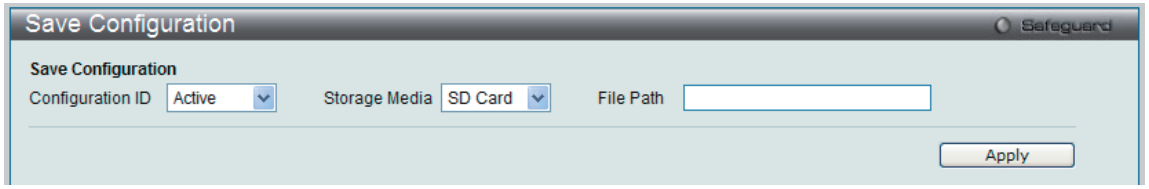


図 12-2　Save Configuration 画面（DGS-3200-24/GE）

プルダウンメニューを使用して、「Configuration ID」を 1、2 または Active から選択します。また、「Storage Media」に宛先（SD Card、NV-RAM）、「File Path」を入力して「Apply」ボタンをクリックします。

Save Log（ログの保存）

Web マネージャ先頭の **Save > Save Log** をクリックし、以下の画面を表示します。

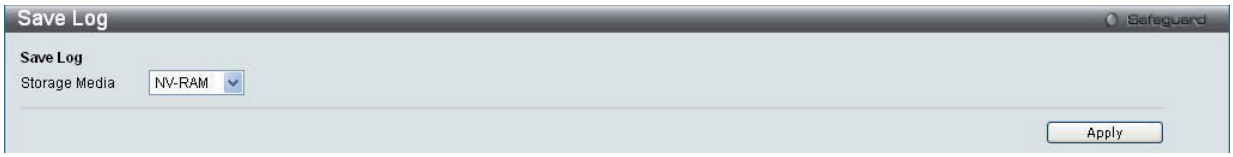


図 12-3　Save Log 画面 (DGS-3200-10 および DGS-3200-16/GE)

現在のログを NV-RAM に保存します。

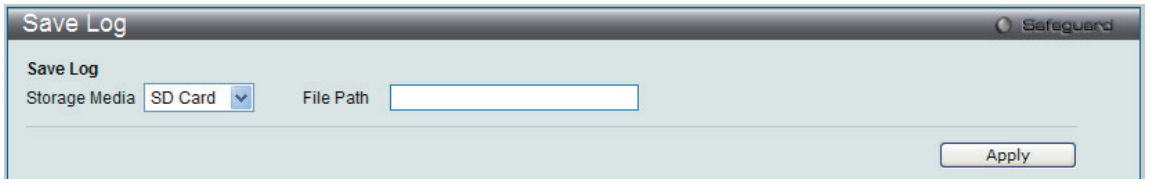


図 12-4　Save Log 画面 (DGS-3200-24/GE)

プルダウンメニューを使用して、「Storage Media」に宛先 (SD Card、NV-RAM)、「File Path」を入力して「Apply」ボタンをクリックします。

Save All（コンフィグレーションファイルとログの保存）

Web マネージャ先頭の **Save > Save All** を選択すると、現在のコンフィグレーションファイルとログを直ちに保存します。
以下の画面が表示されます。

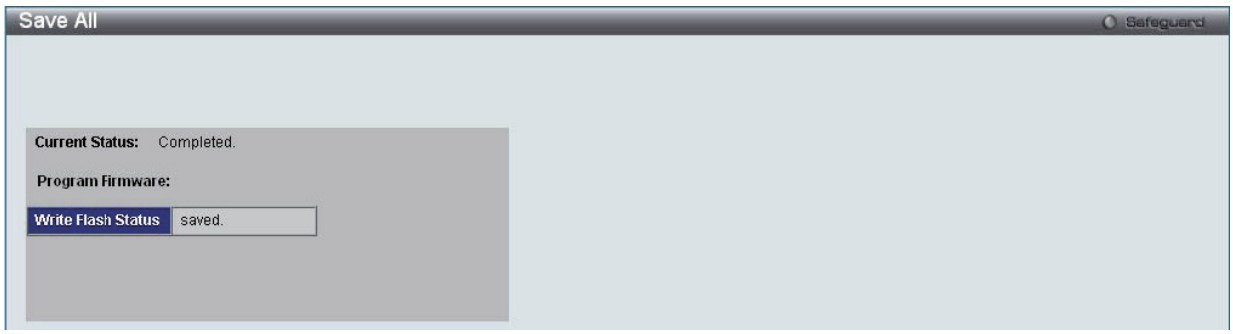


図 12-5　Save All 画面

Tools（ツールメニュー）

「Tools」メニューには、以下の 8 つのメインメニューがあります。:
「Download Configuration File/Download Configuration File to NV-RAM」、「Download Configuration File to SD Card」、「Download Firmware/Download Firmware to NV-RAM」、「Download Firmware to SD Card」、「Upload Configuration File/Upload Configuration File to TFTP」、「Upload Log File/Upload Log File to TFTP」、「Reset」および「Reboot System」

図 12-6　DGS-3200-10、DGS-3200-16/GE

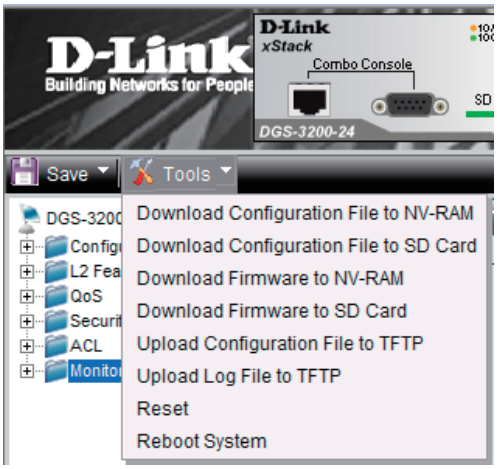


図 12-7　DGS-3200-24/GL

オプションには以下のものがあります。

DGS-3200-10、DGS-3200-16/GE のオプション

項目	説明
Download Configuration File	TFTP サーバから NV-RAM に「Active」、「ID 1」または「ID 2」のインデックスを付加してコンフィグレーションファイルをダウンロードします。
Download Firmware	TFTP サーバから NV-RAM に「Active」、「ID 1」または「ID 2」のインデックスを付加してファームウェアファイルをダウンロードします。
Upload Configuration File	TFTP サーバに「Active」、「ID 1」または「ID 2」のインデックスを付加してコンフィグレーションファイルをアップロードします。
Upload Log File	TFTP サーバにログファイルをアップロードします。
Reset	IP アドレス、ログ、ユーザアカウント、およびバナーを除いて、工場出荷時の初期設定に戻します。
Reboot System	現在のセッションの設定の保存を実施または実施せずにスイッチの再起動をします。

DGS-3200-24/GE のオプション

項目	説明
Download Configuration File to NV-RAM	TFTP サーバから NV-RAM に「Active」、「ID 1」または「ID 2」のインデックスを付加してコンフィグレーションファイルをダウンロードします。
Download Configuration File to SD Card	TFTP サーバから SD カードに「Active」、「ID 1」、または「ID 2」のインデックスを付加してコンフィグレーションファイルをダウンロードします。
Download Firmware to NV-RAM	TFTP サーバから NV-RAM に「Active」、「ID 1」または「ID 2」のインデックスを付加してファームウェアファイルをダウンロードします。
Download Firmware to SD Card	TFTP サーバから SD カードに「Active」、「ID 1」、または「ID 2」のインデックスを付加してファームウェアファイルをダウンロードします。
Upload Configuration File to TFTP	TFTP サーバに「Active」、「ID 1」または「ID 2」のインデックスを付加してコンフィグレーションファイルをアップロードします。
Upload Log File / Upload Log File to TFTP	TFTP サーバにログファイルをアップロードします。
Reset	IP アドレス、ログ、ユーザアカウント、およびバナーを除いて、工場出荷時の初期設定に戻します。
Reboot System	現在のセッションの設定の保存を実施または実施せずにスイッチの再起動をします。

Download Configuration File / Download Configuration File to NV-RAM（コンフィグレーションファイルのダウンロード）

スイッチは NV-RAM に 2 個のコンフィグレーションを保存することができます。コンフィグレーションファイルには「Active」、「1」または「2」のインデックスが付加されます。

DGS-3200-10、DGS-3200-16/GE の場合

Web マネージャ先頭の **Tools > Download Configuration** を選択し、以下の画面を表示します。

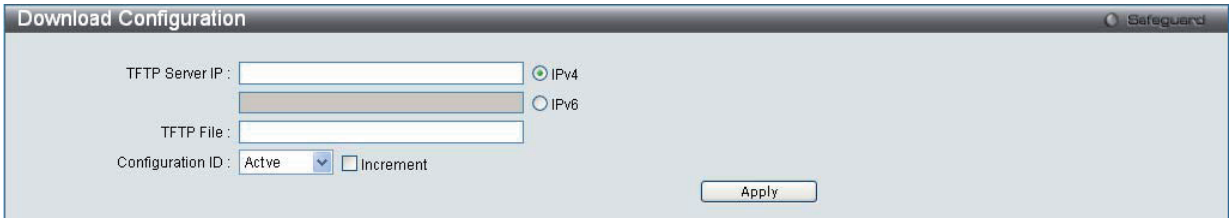


図 12-8　Download Configuration 画面 (DGS-3200-10 および DGS-3200-16/GE)

DGS-3200-124/GE の場合

Web マネージャ先頭の **Tools > Download Configuration File to NV-RAM** を選択し、以下の画面を表示します。

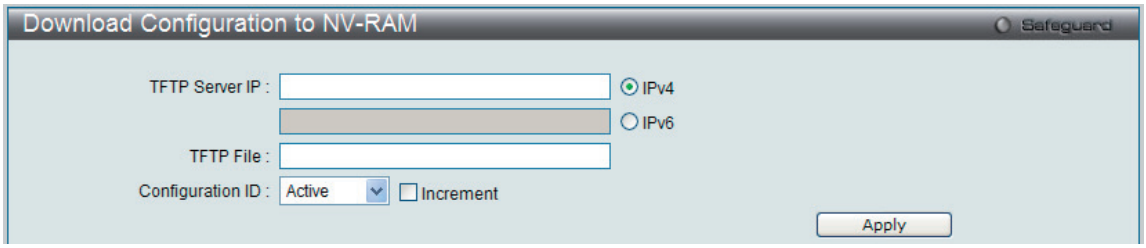


図 12-9　Download Configuration 画面 (DGS-3200-24/GE)

1. ラジオボタンを使用して、「IPv4」または「IPv6」を選択します。

2. 選択した IP のタイプに応じて TFTP サーバの IP アドレスを入力します。

3. さらに TFTP ファイルのパス / ファイル名を指定します。「Configuration ID」を「Active」、「1」または「2」から選択します。

4. 「Increment」をチェックすると部分的にスイッチのコンフィグレーションファイルをダウンロードすることができます。これはコンフィグレーションファイル内に明確に記述されているスイッチパラメータだけを変更するようにファイルをダウンロードできます。他のスイッチパラメータのすべてが変更されないままとなります。

5. 「Apply」ボタンをクリックすると、ファイル転送が開始されます。

Download Configuration File to SD Card（SD カードへのコンフィグレーションファイルのダウンロード）（DGS-3200-24/GE のみ）

Web マネージャ先頭の **Tools > Download Configuration File to SD Card** を選択し、以下の画面を表示します。

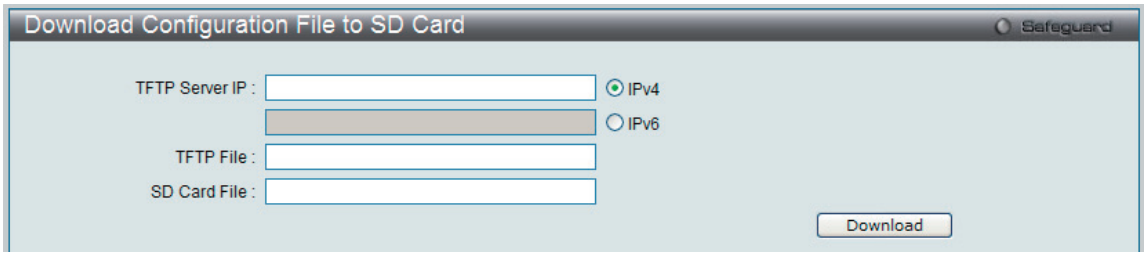


図 12-10　Download Configuration File to SD Card 画面 (DGS-3200-24/GE)

1. ラジオボタンを使用して、「IPv4」または「IPv6」を選択します。

2. 選択した IP のタイプに応じて TFTP サーバの IP アドレスを入力します。

3. TFTP ファイルのパス / ファイル名を指定します。SD Card のファイル名を指定します。

4. 「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。

Download Firmware / Download Firmware to NV-RAM（ファームウェアのダウンロード）

本スイッチはデュアルイメージストレージ機能をサポートしており、ファームウェアファイルのリストアをすることができます。

DGS-3200-10、DGS-3200-16/GE の場合

Web マネージャ先頭の **Tools > Download Firmware** を選択し、以下の画面を表示します。

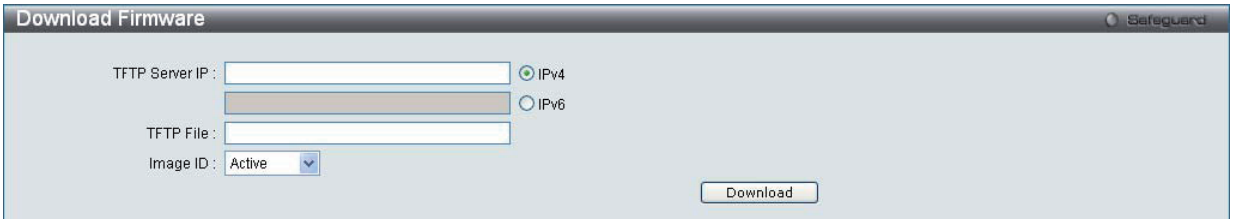


図 12-11 Download Firmware 画面（DGS-3200-10 および DGS-3200-16/GE）

DGS-3200-24/GE の場合

Web マネージャ先頭の **Tools > Download Firmware to NV-RAM** を選択し、以下の画面を表示します。

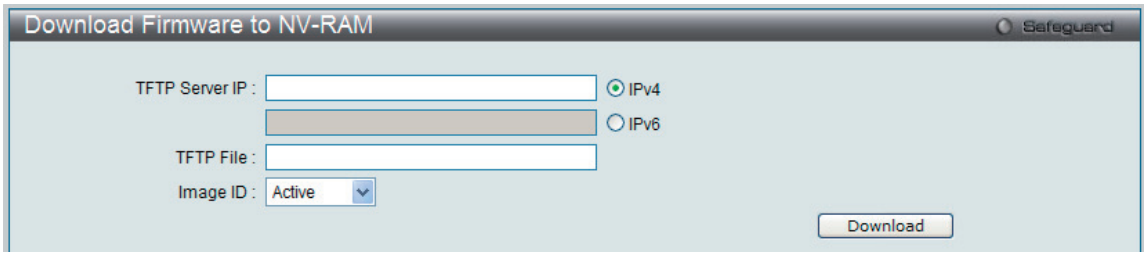


図 12-12 Download Firmware 画面（DGS-3200-24/GE）

1. ラジオボタンを使用して、「IPv4」または「IPv6」を選択します。

2. 選択した IP のタイプに応じて TFTP サーバの IP アドレスを入力します。

3. TFTP ファイルのパス / ファイル名を指定します。

4. 「Image ID」を「Active」、「1」または「2」から選択します。

5. 「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。

Download Firmware to SD Card（SD カードへのファームウェアのダウンロード）（DGS-3200-24/GE のみ）

SD カードにファームウェアをダウンロードします。

Web マネージャ先頭の **Tools > Download Firmware to SD Card** を選択し、以下の画面を表示します。

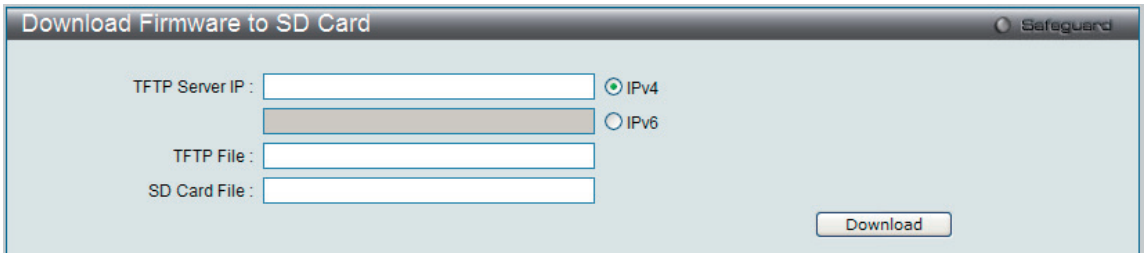


図 12-13 Download Firmware to SD Card 画面（DGS-3200-24/GE）

1. ラジオボタンを使用して、「IPv4」または「IPv6」を選択します。

2. 選択した IP のタイプに応じて TFTP サーバの IP アドレスを入力します。

3. TFTP ファイルのパス / ファイル名を指定します。

4. SD Card のファイル名を指定します。

5. 「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。

Upload Configuration File / Upload Configuration File to TFP（コンフィグレーションファイルのアップロード）

スイッチは TFTP サーバに 2 個のコンフィグレーションを保存することができます。コンフィグレーションファイルには「Active」、「1」または「2」のインデックスが付加されます。

DGS-3200-10、DGS-3200-16/GE の場合

Web マネージャ先頭の **Tools > Upload Configuration** を選択し、以下の画面を表示します。

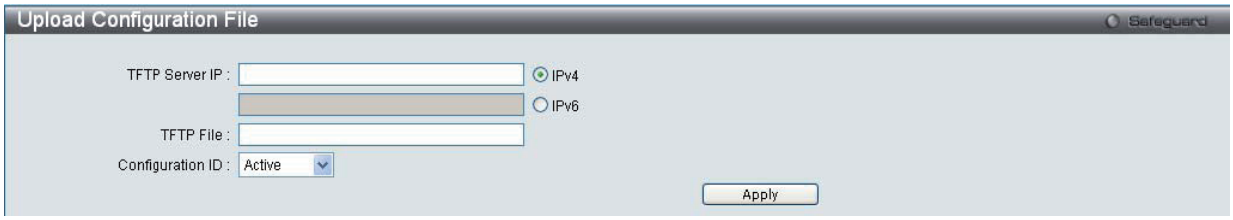


図 12-14 Upload Configuration 画面（DGS-3200-10 および DGS-3200-16/GE）

DGS-3200-24/GE の場合

Web マネージャ先頭の **Tools > Upload Configuration File to FTP** を選択し、以下の画面を表示します。

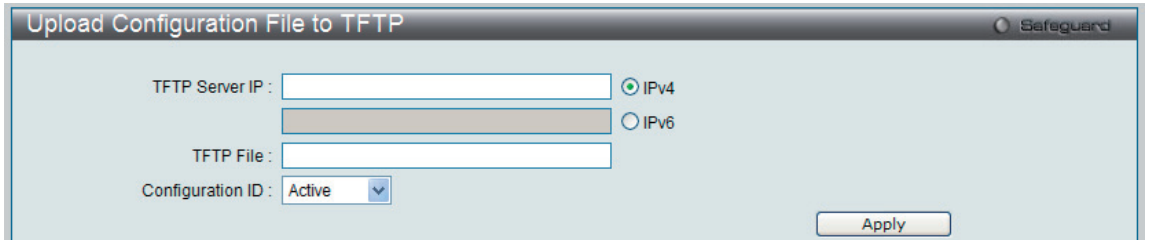


図 12-15 Upload Configuration File to TFTP 画面（DGS-3200-24/GE）

1. ラジオボタンを使用して、「IPv4」または「IPv6」を選択します。
2. 選択した IP のタイプに応じて TFTP サーバの IP アドレスを入力します。
3. TFTP ファイルのパス / ファイル名を指定します。
4. 「Configuration ID」を「Active」、「1」または「2」から選択します。
5. 「Apply」ボタンをクリックすると、ファイル転送が開始されます。

Upload Log File / Upload Log File to TFTP（ログファイルのアップロード）

スイッチのヒストリと攻撃ログを TFTP サーバにアップロードします。

DGS-3200-10、DGS-3200-16/GE の場合

Web マネージャ先頭の **Tools > Upload Log File** を選択し、以下の画面を表示します。

図 12-16 Upload Log File 画面（DGS-3200-10 および DGS-3200-16/GE）

DGS-3200-24/GE の場合

Web マネージャ先頭の **Tools > Upload Log File to TFTP** を選択し、以下の画面を表示します。

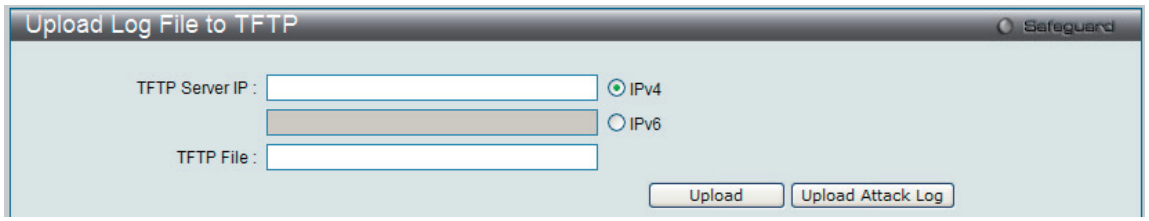


図 12-17 Upload Log File 画面（DGS-3200-24/GE）

1. ログファイルをアップロードするためには、TFTP サーバの IP アドレスとログのパスとファイル名を入力します。
2. 「IPv4」または「IPv6」を選択し、「Upload」または「Upload Attack Log」ボタンをクリックします。

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。スイッチのユーザアカウント、ヒストリログを除いて他のすべての設定を工場出荷時の初期設定に戻します。スイッチは、本画面を使用してリセットされ、「Save Configuration」も「Save All」も実行されていないと、スイッチは再起同時に最後に保存されたコンフィグレーションに戻ります。

Web マネージャ先頭の **Tools > Reset** を選択し、以下の画面を表示します。

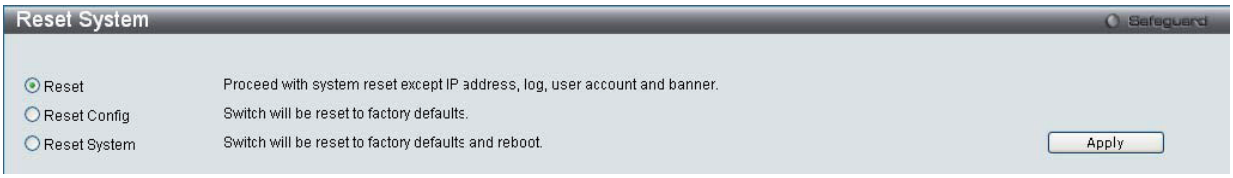


図 12-18 Reset System 画面

項目	説明
Reset	IP アドレス、ログ、ユーザアカウント、ログヒストリ、およびバナーを除くすべての設定が工場出荷時の初期設定に戻りますが、NV-RAM には書き込みません。本画面を使用してスイッチのリセットを行っても「Save Changes」を実行しなければ、リブート時には最後に保存されたコンフィグレーションに戻ります。
Reset Config	すべての設定が工場出荷時の初期設定に戻りますが、NV-RAM には書き込みません。本画面を使用してスイッチのリセットを行っても「Save Changes」を実行しなければ、リブート時には最後に保存されたコンフィグレーションに戻ります。
Reset System	すべての設定やエントリが工場出荷時の初期設定に戻し、その初期設定を NV-RAM に保存して再起動します。

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。

Reboot System（システムの再起動）

以下の画面を使用してスイッチの再起動を行います。

Tools > Reboot の順にクリックし、以下の画面を表示します。

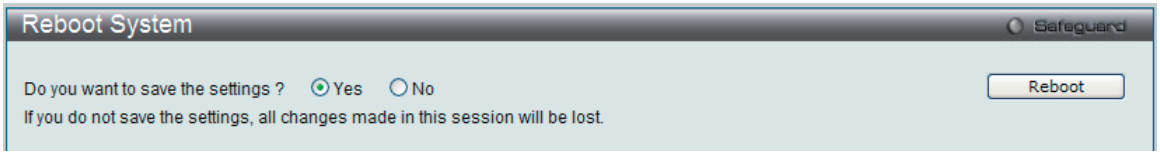


図 12-19 Reboot System 画面

項目	説明
Yes	スイッチは再起動する前に現在の設定を NV-RAM に保存します。
No	スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。
Reboot	スイッチは再起動します。

付録 A ケーブルとコネクタ

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。
以下の図と表は標準の RJ-45 プラグ / コネクタとピンアサインです。

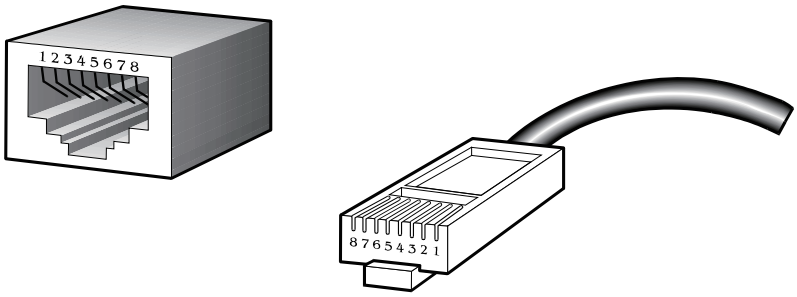


表 A-1　標準的な RJ-45 ピンアサイン

RJ-45 ピンアサイン		
コンタクト（ピン番号）	MDI-X 信号	MDI-II 信号
1	RD+（受信）	TD+（送信）
2	RD-（受信）	TD-（送信）
3	TD+（送信）	RD+（受信）
4	1000BASE-T	1000BASE-T
5	1000BASE-T	1000BASE-T
6	TD-（送信）	RD-（受信）
7	1000BASE-T	1000BASE-T
8	1000BASE-T	1000BASE-T

付録 B ケーブル長

以下の表は各規格に対応するケーブル長 (最大) です。

規格	メディアタイプ	最大伝送距離
Mini-GBIC	1000BASE-LX、シングルモードファイバモジュール 1000BASE-SX、マルチモードファイバモジュール 1000BASE-LH、シングルモードファイバモジュール 1000BASE-ZX、シングルモードファイバモジュール	10 km 550 m 40 km 80 km
1000BASE-T	エンハンスドカテゴリ 5 UTP ケーブル カテゴリ 5 UTP ケーブル（1000 Mbps）	100 m
100BASE-TX	カテゴリ 5 UTP ケーブル（100 Mbps）	100 m
10BASE-T	カテゴリ 3 UTP ケーブル（10 Mbps）	100 m

付録 C ログイベント

スイッチのシステムログに表示される可能性のあるログイベントとそれらの意味を以下に示します。

Critical（重大）、Warning（警告）、Informational（報告）

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
システム	Unit < ユニット ID>, System started up	Critical	システム起動	
	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 >, MAC: < MAC アドレス >）	Informational	フラッシュメモリへのコンフィグレーションファイル保存	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。
	Unit < ユニット ID>, System log saved to flash by console (Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >)	Informational	フラッシュメモリへのシステムログ保存	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。
	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 >, MAC: < MAC アドレス >)	Informational	フラッシュメモリへのコンフィグレーションとログ保存	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。
	Unit < ユニット ID>, Side Fan failed	Critical	側面ファンの異常	DGS-3200-16/GE のみ
	Unit < ユニット ID>, Left Side Fan 1/2 failed	Critical	左のファンの異常	DGS-3200-24/GE のみ
	Unit < ユニット ID>, Side Fan recovered	Critical	側面ファン回復	DGS-3200-16/GE のみ
	Unit < ユニット ID>, Left Side Fan 1/2 recovered	Critical	左のファン回復	DGS-3200-24/GE のみ
	Internal Power Failed	Critical	内蔵電源エラー	DGS-3200-24/GE のみ
	Internal Power is recovered	Critical	内蔵電源回復	DGS-3200-24/GE のみ
	Redundant Power failed	Critical	リダンダント電源エラー	DGS-3200-24/GE のみ
	Redundant Power is working	Critical	リダンダント電源が動作中	DGS-3200-24/GE のみ
アップロード / ダウンロード	Unit < ユニット ID>, Firmware upgraded by console successfully（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	ファームウェアの更新成功。	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。
	Unit < ユニット ID>, Firmware upgraded by console was unsuccessful!（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Warning	ファームウェアの更新失敗。	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。
	Unit < ユニット ID>, Configuration successfully downloaded by console（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	コンフィグレーションファイルのダウンロード成功。	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。
	Unit < ユニット ID>, Configuration download by console was unsuccessful!（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Warning	コンフィグレーションファイルのダウンロード失敗。	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。
	Unit < ユニット ID>, Configuration successfully uploaded by console（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	コンフィグレーションファイルのアップロード成功。	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。
	Unit < ユニット ID>, Configuration upload by console was unsuccessful!（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Warning	コンフィグレーションファイルのアップロード失敗。	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。
	Unit < ユニット ID>, Log message successfully uploaded by console（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	ログメッセージのアップロード成功。	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。
	Unit < ユニット ID>, Log message upload by console was unsuccessful!（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Warning	ログメッセージのアップロード失敗。	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。
インタフェース	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 Up	ポートリンク状態（例 : 100 Mbps 全二重）
	Port < ポート番号 > link down	Informational	ポートリンク Down	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
コンソール	Unit < ユニット ID: ユニット ID>, Successful login through Console（Username: < ユーザ名 >）	Informational	コンソール経由のログイン成功	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。
	Unit < ユニット ID>, Login failed through Console（Username: < ユーザ名 >）	Warning	コンソール経由のログイン失敗	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。
	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アウト	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。
	Unit < ユニット ID>, Console session timed out（Username: < ユーザ名 >）	Informational	コンソールセッション、タイムアウト	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	Successful login through Web（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	Web 経由のログイン成功	
	Login failed through Web（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Warning	Web 経由のログイン失敗	
	Logout through Web（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	Web 経由でログアウト	
	Successful login through Web（SSL）（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	Web（SSL）経由のログイン成功	
	Logout through Web（SSL）（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	Web（SSL）経由でログアウト	
	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）経由のログイン失敗	
	Web (SSL) session timed out (Username: <username>, IP: <ipaddr>, MAC: <MAC アドレス >)	Informational	Web (SSL) セッションタイムアウト	
Telnet	Successful login through Telnet（SSL）（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	Telnet 経由のログイン成功	
	Login failed through Telnet（SSL）（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Warning	Telnet 経由のログイン失敗	
	Logout through Telnet（SSL）（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	Telnet 経由でログアウト	
	Telnet session timed out（SSL）（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	Telnet セッションタイムアウト	
SNMP	SNMP request received from < IP アドレス > with invalid community string !	Informational	無効なコミュニティ名を含む SNMP request 受信	
STP	Topology changed (Instance: <InstanceID> port:<[ユニット ID:] ポート番号 >)	Informational	トポロジ変更	
	New root selected [([Instance: <InstanceID>] Root bridge MAC: <MAC アドレス > Priority :<value>)]	Informational	新規ルートを選択	
	Spanning Tree Protocol is enabled	Informational	スパニングツリープロトコル有効化	
	Spanning Tree Protocol is disabled	Informational	スパニングツリープロトコル無効化	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
DoS	Possible spoofing attack from <MAC アドレス > port < ユニット ID: ポート番号 >	Critical	Spoofing 攻撃	
SSH	Successful login through SSH（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	SSH 経由のログイン成功	
	Login failed through SSH（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Warning	SSH 経由のログイン失敗	
	Logout through SSH（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	SSH 経由のログアウト	
	SSH session timed out（Username: < ユーザ名 >, IP: < IP アドレス >, MAC: < MAC アドレス >）	Informational	SSH セッションタイムアウト	
	SSH server is enabled	Informational	SSH サーバ有効化	
	SSH server is disabled	Informational	SSH サーバ無効化	
AAA	Authentication Policy is enabled (Module : AAA)	Informational	認証ポリシー有効化	
	Authentication Policy is disabled (Module : AAA)	Informational	認証ポリシー無効化	
	Successful login through Console authenticated by AAA local method（Username: < ユーザ名 >）	Informational	AAA ローカルメソッドによるコンソール経由のログイン認証成功	
	Login failed through Console authenticated by AAA local method（Username: < ユーザ名 >）	Warning	AAA ローカルメソッドによるコンソール経由のログイン認証失敗	
	Successful login through Web from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA ローカルメソッドによる Web 経由のログイン認証成功	
	Login failed through Web from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA ローカルメソッドによる Web 経由のログイン認証失敗	
	Successful login through Web (SSL) from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA ローカルメソッドによる Web (SSL) 経由のログイン認証成功	
	Login failed through Web (SSL) from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA ローカルメソッドによる Web (SSL) 経由のログイン認証失敗	
	Successful login through Telnet from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA ローカルメソッドによる Telnet 経由のログイン認証成功	
	Login failed through Telnet from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA ローカルメソッドによる Telnet 経由のログイン認証失敗	
	Successful login through SSH from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA ローカルメソッドによる SSH 経由のログイン認証成功	
	Login failed through SSH from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA ローカルメソッドによる SSH 経由のログイン認証失敗	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
AAA	Successful login through Console authenticated by AAA none method（Username: < ユーザ名 >）	Informational	AAA none メソッドによるコンソール経由のログイン認証成功	
	Successful login through Web from < ユーザ IP > authenticated by AAA none method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA none メソッドによる Web 経由のログイン認証成功	
	Successful login through Web (SSL) from < ユーザ IP > authenticated by AAA none method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA none メソッドによる Web (SSL) 経由のログイン認証成功	
	Successful login through Telnet from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA none メソッドによる Telnet 経由のログイン認証成功	
	Successful login through SSH from < ユーザ IP > authenticated by AAA local method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA none メソッドによる SSH 経由のログイン認証成功	
	Successful login through Console authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >）	Informational	AAA サーバによるコンソール経由のログイン認証成功	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。
	Login failed through Console authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >）	Warning	AAA サーバによるコンソール経由のログイン認証失敗	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。
	Login failed through Console due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	AAA サーバタイムアウトまたは不正な設定によるコンソール経由のログイン失敗	
	Successful login through Web from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA サーバによる Web 経由のログイン認証成功	
	Login failed through Web from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバによる Web 経由のログイン認証失敗	
	Login failed through Web from < ユーザ IP > due to AAA server timeout or improper configuration（Username: < ユーザ名 >, MAC: < MAC アドレス >）	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	
	Successful login through Web (SSL) from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA サーバによる Web (SSL) 経由のログイン認証成功	
	Login failed through Web (SSL) from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバによる Web (SSL) 経由のログイン認証失敗	
	Login failed through Web (SSL) from < ユーザ IP > due to AAA server timeout or improper configuration（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバタイムアウトまたは不正な設定による Web (SSL) 経由のログイン認証失敗	
	Successful login through Telnet from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA サーバによる Telnet 経由のログイン認証成功	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
AAA	Login failed through Telnet from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバによる Telnet 経由のログイン認証失敗	
	Successful login through SSH from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA サーバによる SSH 経由のログイン認証成功	
	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 レベル遷移成功	
	Enable Admin failed through Console authenticated by AAA local_enable method（Username: < ユーザ名 >）	Warning	AAA local_enable メソッドによるコンソール経由の Admin レベル遷移失敗	
	Successful Enable Admin through Web from < ユーザ IP > authenticated by AAA local_enable method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA local_enable メソッドによる Web 経由の Admin レベル遷移成功	
	Enable Admin failed through Web from < ユーザ IP > authenticated by AAA local_enable method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA local_enable メソッドによる Web 経由の Admin レベル遷移失敗	
	Successful Enable Admin through Telnet from < ユーザ IP > authenticated by AAA local_enable method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA local_enable メソッドによる Telnet 経由の Admin レベル遷移成功	
	Enable Admin failed through Telnet from < ユーザ IP > authenticated by AAA local_enable method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA local_enable メソッドによる Telnet 経由の Admin レベル遷移失敗	
	Successful Enable Admin through SSH from < ユーザ IP > authenticated by AAA local_enable method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA local_enable メソッドによる SSH 経由の Admin レベル遷移成功	
	Enable Admin failed through SSH from < ユーザ IP > authenticated by AAA local_enable method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA local_enable メソッドによる SSH 経由の Admin レベル遷移失敗	
	Successful Enable Admin through Console authenticated by AAA none method（Username: < ユーザ名 >）	Informational	AAA none メソッドによるコンソール経由の Admin レベル遷移成功	
	Successful Enable Admin through Web from < ユーザ IP > authenticated by AAA none method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA none メソッドによる Web 経由の Admin レベル遷移成功	
	Successful Enable Admin through Web (SSL) from < ユーザ IP > authenticated by AAA none method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA none メソッドによる Web (SSL) 経由の Admin レベル遷移成功	
	Successful Enable Admin through Telnet from < ユーザ IP > authenticated by AAA none method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA none メソッドによる Telnet 経由の Admin レベル遷移成功	
	Successful Enable Admin through SSH from < ユーザ IP > authenticated by AAA none method（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA none メソッドによる SSH 経由の Admin レベル遷移成功	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
AAA	Successful Enable Admin through Console authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >）	Informational	AAA サーバによるコンソール経由の Admin レベル遷移成功	
	Enable Admin failed through Console authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >）	Warning	AAA サーバによるコンソール経由の Admin レベル遷移失敗	
	Enable Admin failed through Console due to AAA server timeout or improper configuration（Username: < ユーザ名 >）	Warning	AAA サーバタイムアウトまたは不正な設定によるコンソール経由の Admin レベル遷移失敗	
	Successful Enable Admin through Web from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA サーバによる Web 経由の Admin レベル遷移成功	
	Enable Admin failed through Web from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバによる Web 経由の Admin レベル遷移失敗	
	Enable Admin failed through Web from < ユーザ IP > due to AAA server timeout or improper configuration（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバタイムアウトまたは不正な設定による Web 経由の Admin レベル遷移失敗	
	Successful Enable Admin through Web (SSL) from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA サーバによる Web (SSL) 経由の Admin レベル遷移成功	
	Enable Admin failed through Web (SSL) from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバによる Web (SSL) 経由の Admin レベル遷移失敗	
	Enable Admin failed through Web (SSL) from < ユーザ IP > due to AAA server timeout or improper configuration（Username: < ユーザ名 >, MAC: < MAC アドレス >）	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	
	Successful Enable Admin through Telnet from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA サーバによる Telnet 経由の Admin レベル遷移成功	
	Enable Admin failed through Telnet from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバによる Telnet 経由の Admin レベル遷移失敗	
	Enable Admin failed through Telnet from < ユーザ IP > due to AAA server timeout or improper configuration（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバタイムアウトまたは不正な設定による Telnet 経由の Admin レベル遷移失敗	
	Successful Enable Admin through SSH from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Informational	AAA サーバによる SSH 経由の Admin レベル遷移成功	
	Enable Admin failed through SSH from < ユーザ IP > authenticated by AAA server < サーバ IP >（Username: < ユーザ名 >, MAC: < MAC アドレス >）	Warning	AAA サーバによる SSH 経由の Admin レベル遷移失敗	
	Enable Admin failed through SSH from < ユーザ IP > due to AAA server timeout or improper configuration（Username: < ユーザ名 >, MAC: < MAC アドレス >）	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	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
AAA	AAA server < サーバ IP > (Protocol : < プロトコル >) connection failed	Warning	AAA サーバタイムアウト	プロトコルは TACACS, XTACACS, TACACS+, RADIUS のいずれかが表示されます。
	AAA server < サーバ IP > (Protocol: < プロトコル >) response is wrong	Warning	AAA サーバ ACK エラー	<protocol> is one of TACACS, XTACACS, TACACS+, RADIUS
	AAA doesn't support this functionality	Informational	AAA はこの機能を未サポートです。	
IP-MAC ポートバインディング	Unauthenticated IP-MAC address and discarded by IP mac port binding（IP: < IP アドレス >, MAC: < MAC アドレス >, Port < ユニット ID: ポート番号 >）	Warning	IP-MAC ポートバインディング機能により、非認証の IP アドレスからのパケットを廃棄しました。	
	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	IP-MAC ポートバインディング機能により、非認証の IP アドレスが発見され、廃棄しました。	
	Dynamic IMPB entry is conflict 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 FDB とコンフリクトしています。	
	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 : ポート番号 >)	Warning	ダイナミック IMPB エントリが、スタティック ARP とコンフリクトしています。	
	Dynamic IMPB entry is conflict with static IMPB (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 とコンフリクトしています。	
	Creating IMPB entry Failed due to no ACL rule available (IP:< IP アドレス >, MAC:< MAC アドレス >, Port< ユニット ID: ポート番号 >)	Warning	有効な ACL ルールがないため、IMPB エントリの作成に失敗しました。	
	Port <[ユニット ID:] ポート番号 > enter IMPB block state	Warning	ポートは IMPB ブロック状態に入りました。	
	Port <[ユニット ID:] ポート番号 > recover from IMPB block state	Warning	ポートは IMPB ブロック状態から回復しました。	
IP とパスワード変更	Unit <unitID>, Management IP address was changed by (Username: < ユーザ名 >,IP< ユニット ID: IP アドレス >,MAC:< MAC アドレス >)	Informational	IP アドレス変更操作	
	Unit <unitID>, Password was changed by (Username: < ユーザ名 >,IP:< IP アドレス >,MAC:< MAC アドレス >)	Informational	パスワード変更操作	
デュアルコンフィグレーション	Configuration had <int> syntax error and <int> execute error	Warning	システム再起動中に実行エラー発生	
セーフガードエンジン	SafeGuard Engine enters NORMAL mode	Informational	セーフガードエンジン機能がノーマルモードに遷移しました。	
	Safeguard Engine enters EXHAUSTED mode	Warning	セーフガードエンジン機能がフィルタリングパケットモードに遷移しました。	
パケットストーム	Broadcast storm is occurring (port< ユニット ID: ポート番号 >)	Warning	ブロードキャストストーム発生中。	
	Broadcast storm is cleared (port< ユニット ID: ポート番号 >)	Informational	ブロードキャストストーム停止。	
	Multicast storm is occurring (port< ユニット ID: ポート番号 >)	Warning	マルチキャストストーム発生中。	
	Multicast storm is cleared (port< ユニット ID: ポート番号 >)	Informational	マルチキャストストーム停止。	
	Port < ユニット ID: ポート番号 > is currently shut down due to a packet storm	Warning	パケットストームのためにポートはシャットダウン。	

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
JWAC	JWAC login successful (Username:< ユーザ名 >,IP< IP アドレス >,MAC:< MAC アドレス >,Port:< ユニット ID: ポート番号 >)	Informational	ログイン成功。	
	JWAC login rejected (Username:< ユーザ名 >,IP< IP アドレス >,MAC:< MAC アドレス >,Port:< ユニット ID: ポート番号 >)	Warning	ログイン失敗。	
	JWAC host logout normally(Username:< ユーザ名 >,IP< IP アドレス >,MAC:< MAC アドレス >,Port:< ユニット ID: ポート番号 >)	Informational	通常のログアウト。	
	JWAC host logout forcibly (Username:< ユーザ名 >,IP:< IP アドレス >,MAC:< MAC アドレス >,Port:< ユニット ID: ポート番号 >)	Warning	強制的なログアウト。	
	JWAC host age out (Username:< ユーザ名 >,IP:< IP アドレス >,MAC:< MAC アドレス >,Port:< ユニット ID: ポート番号 >)	Informational	JWAC ホストがエージング実施。	
ループバック検知	Port <[ユニット ID:] ポート番号 > LBD loop occurred. Port blocked.	Warning	ポートにループが発生しました。	
	Port <[ユニット ID:] ポート番号 > LBD port recovered. Loop detection restarted.	Warning	待機時間経過後、ポートのループ検知が再スタートしました。	
	Port <[ユニット ID:] ポート番号 > VID <vlanID> LBD loop occurred. Packet discard begun.	Warning	VID を持つポートにループが発生しました。	
	Port <[ユニット ID:] ポート番号 > VID <vlanID> LBD recovered. Loop detection restarted.	Warning	待機時間経過後、VID を持つポートのループ検知が再スタートしました。	
802.1X	Radius server <ipaddr> assigned vid :<vlanID> to port <[ユニット ID:] ポート番号 > (account :< ユーザ名 >)	Informational	RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから VID が割り当てられました。この VID はポートに割り当てられ、このポートは VLAN タグなしメンバになります。	• スタンドアロンデバイスのポートの場合 : < ポート番号 > • スタッカブルデバイスのポートの場合 : < ユニット番号 : ポート番号 >
	Radius server <ipaddr> assigned ingress bandwidth :<ingressBandwidth> to port <[ユニット ID:] ポート番号 > (account : < ユーザ名 >)	Informational	RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから Ingress 帯域が割り当てられました。この Ingress 帯域はポートに割り当てられます。	• スタンドアロンデバイスのポートの場合 : < ポート番号 > • スタッカブルデバイスのポートの場合 : < ユニット番号 : ポート番号 >
	Radius server <ipaddr> assigned egress bandwidth :<egressBandwidth> to port <[ユニット ID:] ポート番号 > (account: < ユーザ名 >)	Informational	RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから Egress 帯域が割り当てられました。この Egress 帯域はポートに割り当てられます。	• スタンドアロンデバイスのポートの場合 : < ポート番号 > • スタッカブルデバイスのポートの場合 : < ユニット番号 : ポート番号 >
	Radius server <ipaddr> 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 クライアントが RADIUS サーバによって認証された後、RADIUS サーバから 802.1p デフォルトプライオリティが割り当てられました。802.1p デフォルトプライオリティはポートに割り当てられます。	• スタンドアロンデバイスのポートの場合 : < ポート番号 > • スタッカブルデバイスのポートの場合 : < ユニット番号 : ポート番号 >

カテゴリ	ログの内容	緊急度	イベントの説明	摘要
802.1X	802.1x Authentication failure [for <reason>] from (Username: < ユーザ名 >, Port: <[ユニット ID:] ポート番号 >, MAC: < MAC アドレス >)	Warning	802.1X 認証の失敗。	• スタンドアロンデバイスのポートの場合 : < ポート番号 > • スタッカブルデバイスのポートの場合 : < ユニット番号 : ポート番号 >
	802.1x Authentication success from (Username: < ユーザ名 >, Port: <[ユニット ID:] ポート番号 >, MAC: < MAC アドレス >)	Informational	802.1X 認証の成功。	• スタンドアロンデバイスのポートの場合 : < ポート番号 > • スタッカブルデバイスのポートの場合 : < ユニット番号 : ポート番号 >
DHCP	Detected untrusted DHCP server(IP: <IP アドレス >, Port: <[ユニット番号 :] ポート番号 >)	Informational	信頼性の低い DHCP サーバの IP アドレスを検出。	
MBAC	MAC-AC login successful (MAC: <MAC アドレス >, port: <[ユニット ID:] ポート番号 >, VID: <vlanID>)	Informational	ログインの成功。	
	MAC-AC login rejected (MAC: <MAC アドレス >, port: <[ユニット ID:] ポート番号 >, VID: <vlanID>)	Warning	ログインの失敗。	
	MAC-AC host aged out (MAC: <MAC アドレス >, port: <[ユニット ID:] ポート番号 >, VID: <VLAN ID>)	Informational	エージング済み。	

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。

トラップ名	説明	OID
MACNotificationTrap	本トラップは、アドレステーブル内の MAC アドレスの変化を示します。	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.1
PortSecurityViolationTrap	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。	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.2
PortLoopOccurredTrap	ポートにループが発生すると、本トラップを送信します。	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.3
PortLoopRestart	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。	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.4
VlanLoopOccurred	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。	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.5
VlanLoopRestart	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。	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.6
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
PktStormOccurred	パケットストームメカニズムがパケットストームを検出し、アクションとしてシャットダウンする場合に本トラップを送信します。	1.3.6.1.4.1.171.12.25.5.0.1
PktStormCleared	パケットストームメカニズムがパケットストームをクリアした場合に本トラップを送信します。	1.3.6.1.4.1.171.12.25.5.0.2
IpMACBindTrap	IP-MAC バインディングトラップが有効な場合、定義済みのポートセキュリティ設定に違反する新しい MAC があると、トラップが送信されます。	1.3.6.1.4.1.171.12.23.5.0.1
MacBasedAuthLoggedSuccess	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。	1.3.6.1.4.1.171.12.35.11.1.0.1
MacBasedAuthLoggedFail	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。	1.3.6.1.4.1.171.12.35.11.1.0.2
MacBasedAuthAgesOut	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。	1.3.6.1.4.1.171.12.35.11.1.0.3
FilterDetectedTrap	不正な DHCP サーバを検出する時、本トラップを送信します。ログ取得を停止する未許可期間に検出された同じ不正な DHCP サーバの IP アドレスをトラップ送信先に一度だけ送信します。	1.3.6.1.4.1.171.12.37.100.0.1

トラップ名	説明	OID
SingleIPMSColdStart	Commander スイッチは、メンバがコールドスタート通知を生成する場合に指定ホストに swSingleIPMSColdStart 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.11
SingleIPMSWarmStart	Commander スイッチは、メンバがウォームスタート通知を生成する場合に指定ホストに swSingleIPMSWarmStart 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.12
SingleIPMSLinkDown	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。	1.3.6.1.4.1.171.12.8.6.0.13
SingleIPMSLinkUp	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。	1.3.6.1.4.1.171.12.8.6.0.14
SingleIPMSAuthFail	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。	1.3.6.1.4.1.171.12.8.6.0.15
SingleIPMSnewRoot	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。	1.3.6.1.4.1.171.12.8.6.0.16
SingleIPMSTopologyChange	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。	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。	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。	1.3.6.1.6.3.1.1.5.4
authenticationFailure	SNMP 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
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
PowerFailure	PowerFailure トラップは、少なくとも一つの電源がエラーになったことを示しています。	1.3.6.1.4.1.171.12.11.2.2.2.0.2
PowerRecover	PowerRecover トラップは、電源エラーから回復したことを示しています。	1.3.6.1.4.1.171.12.11.2.2.2.0.3
FanFailure	FanFailure トラップは、少なくとも一つのファンがエラーになったことを示しています。	1.3.6.1.4.1.171.12.11.2.2.2.0.1
FanRecover	FanRecover トラップは、ファンエラーから回復したことを示しています。	1.3.6.1.4.1.171.12.11.2.2.3.0.2

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

ARP を動作させる方法

ARP（Address Resolution Protocol）は、IP アドレスだけがわかっている場合にホストのハードウェアアドレス（MAC アドレス）を検索するための標準的な方法です。しかし、クラッカーが ARP パケット内の IP および MAC 情報を偽造して LAN への攻撃（ARP スプーフィングとして、知られている）を行うために、このプロトコルは被害を受けやすいと言えます。ここでは ARP プロトコル、ARP スプーフィング攻撃、および D-Link スイッチが提供する ARP スプーフィング攻撃を防御する対策について紹介します。

ARP 処理中に、PC-A は、はじめに、PC-B の MAC アドレスを問い合わせする ARP リクエストを発行します。そのネットワーク構造は図 E-1 の通りです。

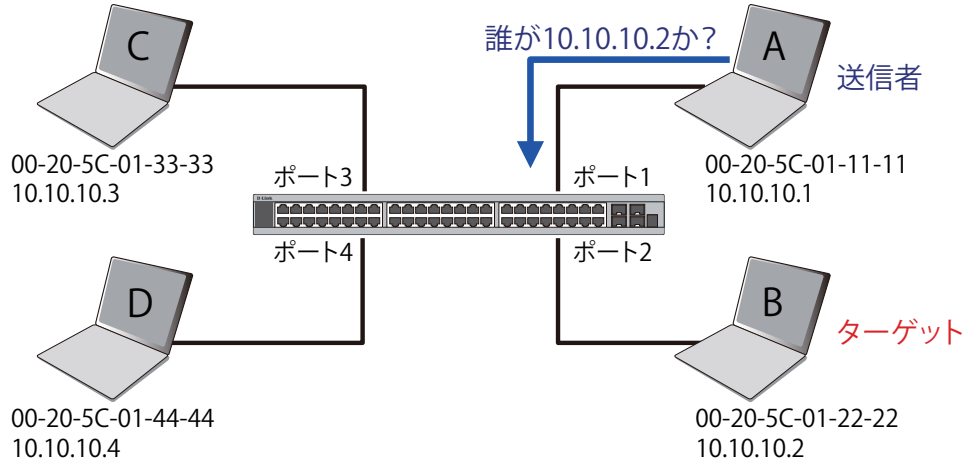


図 E-1

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 E-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 E-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 E-2 の通り、イーサネットフレーム内の「送信元アドレス」は、PC-A の MAC アドレスとなります。ARP リクエストは、ブロードキャスト経由で送信されるため、イーサネットのブロードキャスト（FF-FF-FF-FF-FF-FF）のフォーマットには「宛先アドレス」があります。

表 E-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 E-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。

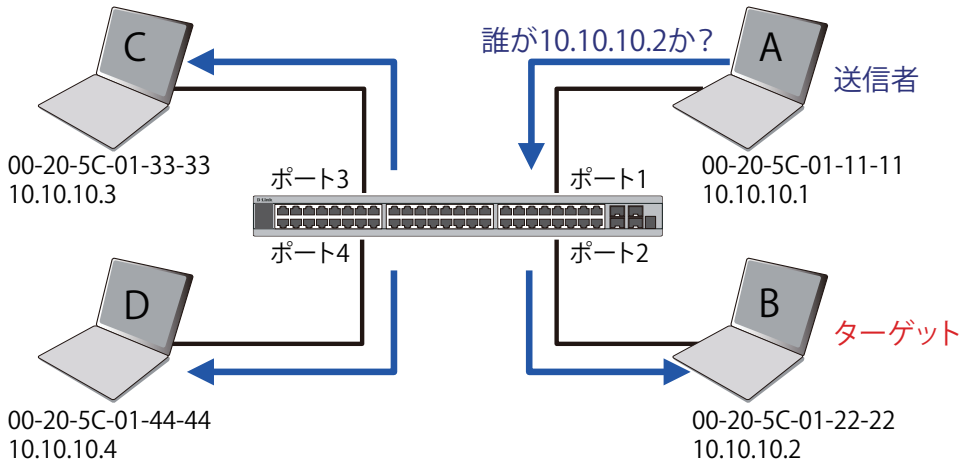


図 E-2

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 E-3 参照）。

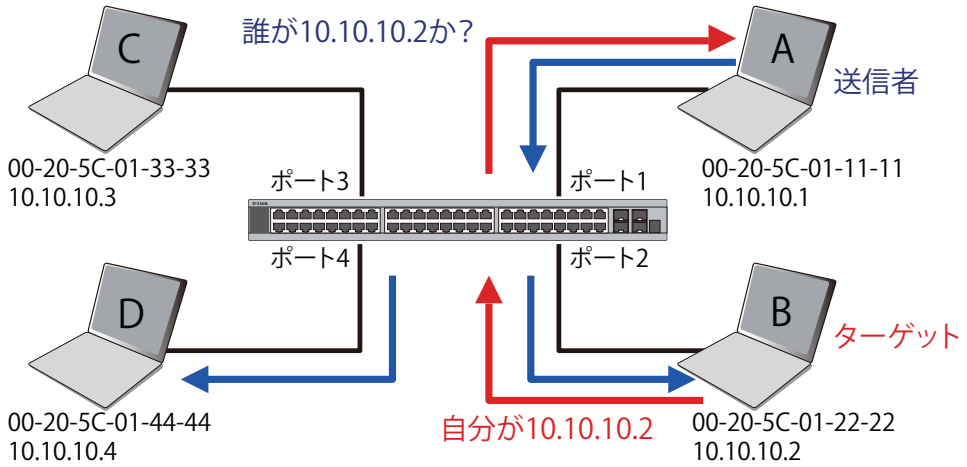


図 E-3

PC-B が ARP リクエストに応答すると、その MAC アドレスは表 E-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 E-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	00-00-00-00-00-00	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 E-4 参照）。

表 E-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の別のノードの IP アドレスに攻撃者の MAC アドレスかでたらめの MAC アドレスを割り当ててしまうことです。その IP アドレスに向かう予定だったトラフィックが、攻撃者に指定されたノードに誤ってリダイレクトされてます。

IP スプーフィング攻撃は、ホストが自身の IP アドレスを解決するため ARP リクエストを送信する場合に発生する Gratuitous ARP によって引き起こされます。図 E-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。

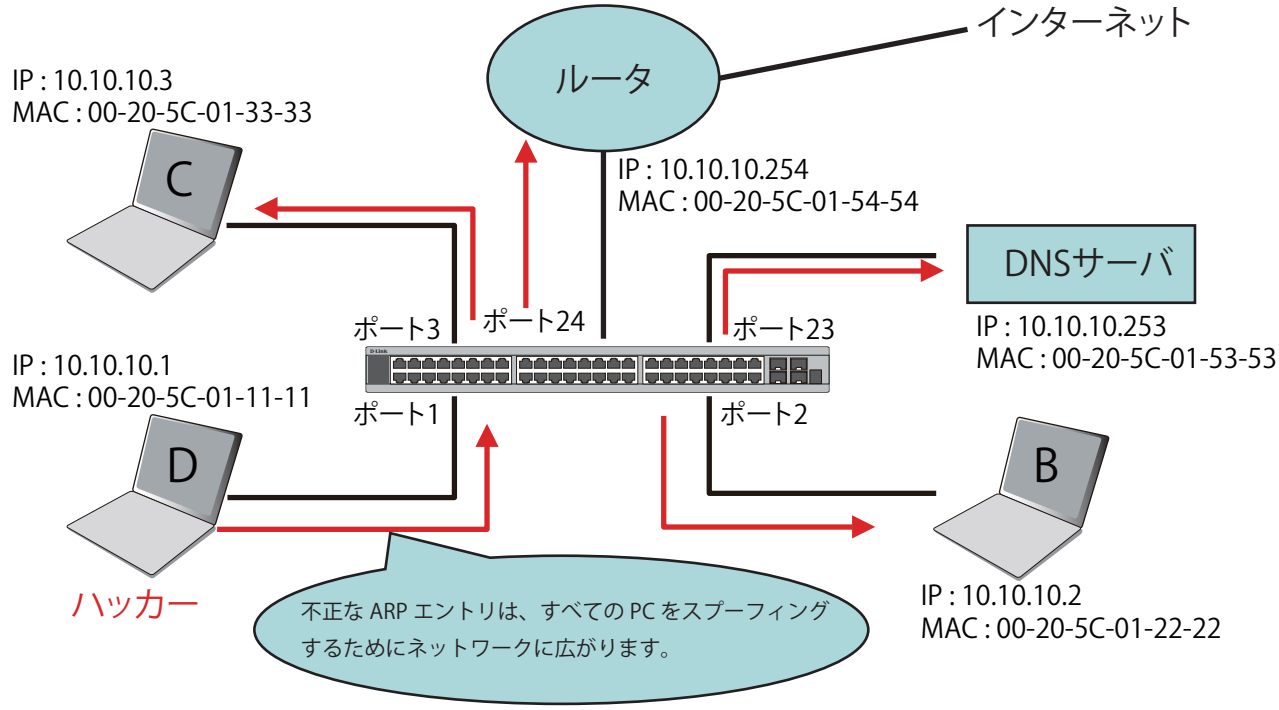


図 E-4

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 E-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 E-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。

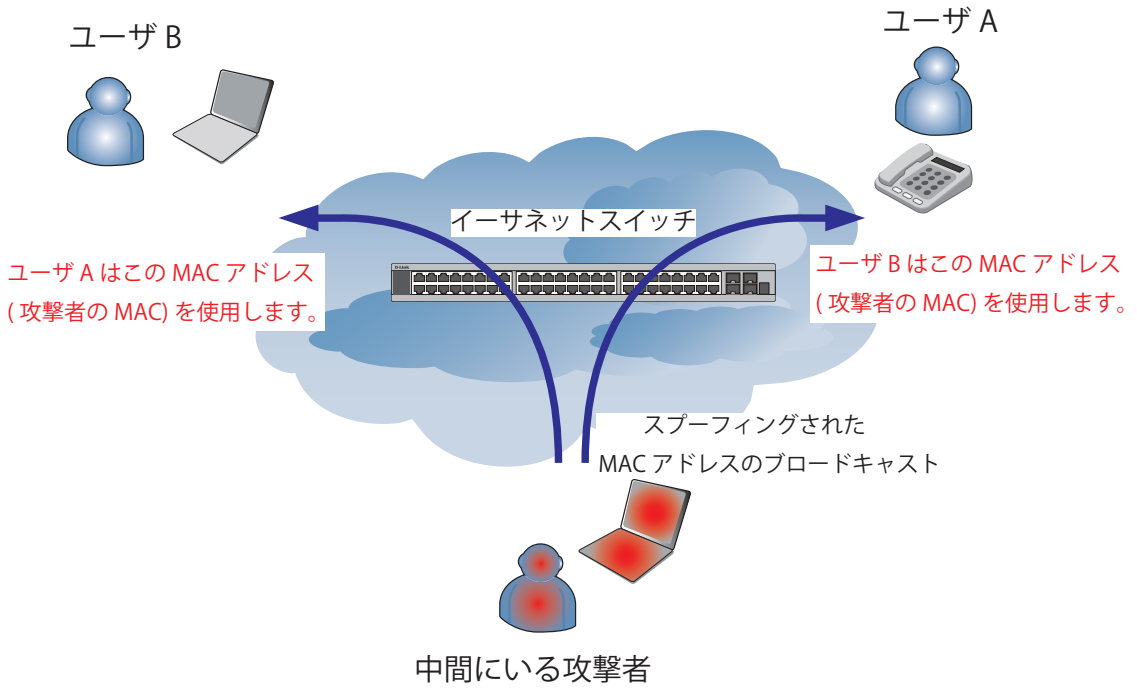


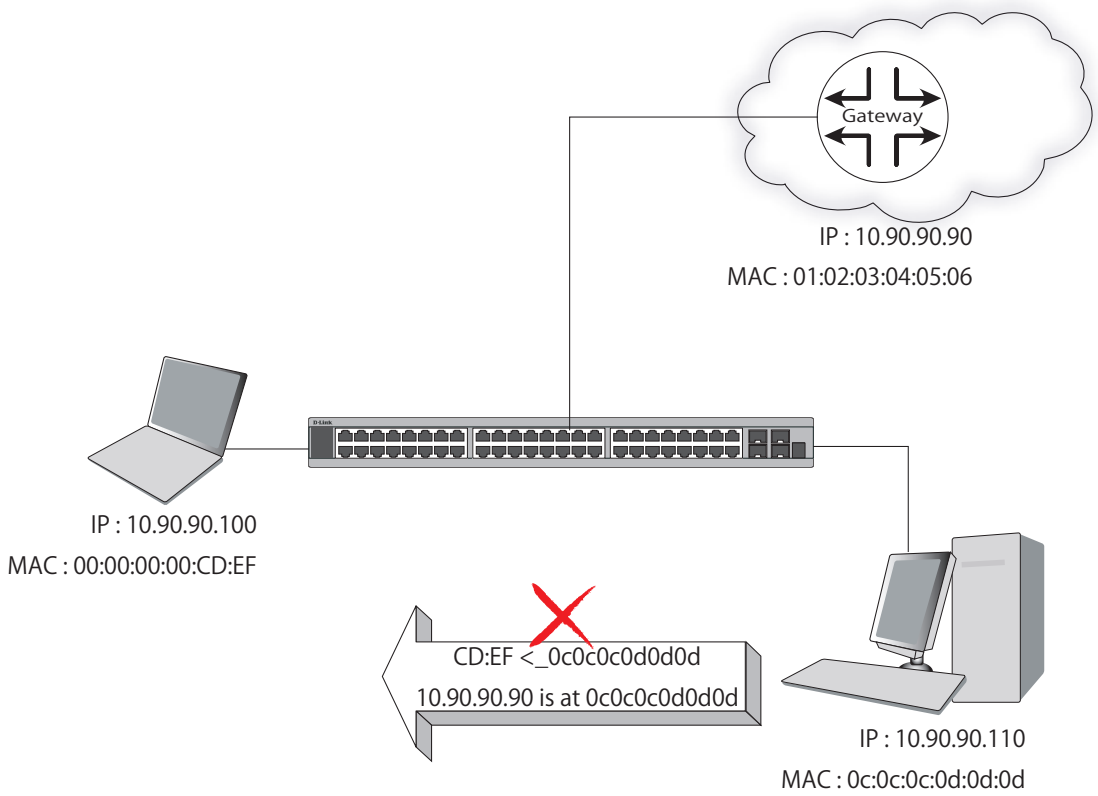
図 E-5

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 E-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 E-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 E-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 E-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 E-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 E-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 F パスワードリカバリ手順

ここでは、弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用するこうとです。時々パスワードが忘れられたり、壊れたりするため、ネットワーク管理者は、これらのパスワードをリセットする必要があります。ここでは、パスワードリカバリ機能は、そのような場合にネットワーク管理者を助けるものです。以下の手順で、容易にパスワードを回復するパスワードリカバリ機能の使用方法を説明します。

これらの手順を終了するとパスワードはリセットされます。

1. セキュリティの理由のため、パスワードリカバリ機能は物理的にデバイスにアクセスすることが必要です。そのため、デバイスのコンソールポートへの直接接続を行っている場合だけ、本機能を適用することが可能です。ユーザは端末エミュレーションソフトを使用して、スイッチのコンソールポートに端末または PC を接続する必要があります。

2. 電源をオンにします。runtime image が 100% までロードされた後に、「Password Recovery Mode」に入るために、2 秒以内に、ホットキー「 ^ 」（シフト +6）を押します。「Password Recovery Mode」に一度入ると、スイッチのすべてのポートが無効になります。

```
Boot Procedure                                                    V1.00.B012
--------------------------------------------------------------------------------
Power On Self Test ..................................... 100%
MAC Address : 00-19-5B-EC-32-15
H/W Version : A2

Please wait, loading V1.50.B019 Runtime image.............. 00%
The switch is now entering Password Recovery Mode:_
```

```
The switch is currently in Password Recovery Mode.
>
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
reset config	リセットし、全設定を工場出荷時設定に戻します。
reboot	「Password Recovery Mode」を終了し、スイッチを再起動します。現在の設定を保存するように確認メッセージが表示されます。
reset account	作成済みのアカウントのすべてを削除します。
reset password	指定ユーザのパスワードをリセットします。
{<username>}	ユーザ名を指定しないと、すべてのユーザのパスワードがリセットされます。
show account	設定済みのすべてのアカウントを表示します。

付録 G 用語解説

用語	説明
1000BASE-LX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。長い光波長で長距離伝送用に使用されます。伝送距離 (最大) はシングルモード光ファイバを使用した場合で 10km。
1000BASE-SX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。短い光波長でマルチモード光ファイバを使用した場合伝送距離 (最大) は 550km。
100BASE-FX	光ファイバを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
100BASE-TX	カテゴリ 5 以上の UTP ケーブルを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
10BASE-T	IEEE 802.3 準拠でカテゴリ 3 以上の UTP ケーブルを使用する最大伝送速度 10Mbps の Ethernet の規格のひとつ。
エージング	タイムアウトし、無効のスイッチのダイナミックデータベースを自動的に消去します。
ATM	非同期転送モード。セルと呼ばれる固定長のセル (パケット) ベースで転送するプロトコル。ATM は音声、データおよびビデオ信号を含むユーザトラフィックの完全な列を転送するために開発されたものです。
オートネゴシエーション	スピード、デュプレックスおよびフローコントロールを自動的に認識する機能。オートネゴシエーションをサポートする端末と接続すると、リンクは自動的に最適なリンク条件に設定されます。
バックボーンポート	デバイスのアドレスを学習せず不明なアドレスを持つすべてのフレームを受信するポート。バックボーンポートは通常ご使用のネットワークのバックボーンにスイッチを接続するために使用されるポートです。バックボーンポートは以前はダウンリンクポートとして知られていました。
バックボーン	ネットワークセグメント間でトラフィックが転送される場合に優先パスとして使用されるネットワークの一部分。
帯域	1 秒あたりのビット数で計算される 1 チャンネルが転送できる情報量。イーサネットの帯域は 10Mbps、ファーストイーサネットは 100Mbps。
ボーレート	ラインのスイッチングスピード。ネットワークセグメント間のラインスピードとして知られています。
BOOTP	BOOTP プロトコルはデバイスが起動するたびに IP アドレスを MAC アドレスに自動マッピングします。さらにデバイスにサブネットマスク、デフォルトゲートウェイを割り当てます。
ブリッジ	たとえ高いレベルのプロトコルが関連してもローカルまたはリモートネットワークを相互接続するデバイス。ブリッジはネットワーク管理を中央に集めて 1 個の論理ネットワークを形成します。
ブロードキャスト	ネットワーク上のすべての終点デバイスに送信されるメッセージ。
ブロードキャストストーム	が主として可能なネットワーク帯域を奪い、ネットワークエラーを引き起こす Multiple simultaneous ブロードキャスト。
コンソールポート	端末またはモデムコネクタと接続可能なスイッチ上のポート。コンピュータ内でパラレル配列のデータをデータ転送リンクで使用されるシリアル形式に変換します。このポートはほとんどの場合ローカル管理のために使用されます。
CSMA/CD	イーサネットと IEEE 802.3 標準によって使用されるチャンネルアクセス方法で検索したデータチャンネルが一定期間後クリアされた後にだけデバイスに転送します。2 つのデバイスが同時に転送する場合、コリジョンが発生し、コリジョンを発生したデバイスは任意の時間再転送を遅らせます。
データセンタースイッチング	スイッチがサーバファームへの高パフォーマンスアクセス、高速バックボーン接続、およびネットワーク管理とセキュリティのためのコントロールポイントを提供するコーポレートネットワーク内のアグリゲーションポイント
イーサネット	Xerox、Intel および DEC が共同で開発した LAN 仕様。イーサネットネットワークは CSMA/CD を使用して 10Mbps で処理を行います。
ファーストイーサネット	Ethernet/CD ネットワークアクセス方法をベースにした 100Mbps 技術。
フローコントロール	(IEEE 802.3z) 端末に接続した転送ポートへのパケットを抑止します。受信バッファがあふれそうになった場合にパケットロスを防ぎます。
フォワーディング	中間のネットワークデバイスによりパケットを到達点に向けて送信するプロセス。
フルデュプレックス	同時にパケットの送受信を可能とし、スループットを 2 倍にするシステム。
ハーフデュプレックス	パケットの送受信を行うが、同時には行えないシステム。
IP アドレス	Internet Protocol アドレス。TCP/IP を使用するネットワークに付属するデバイスの固有な識別子。IPv4 アドレスは 8 ビットずつピリオドで区切られ、ネットワークセクション、サブネットセクション、ホストセクションで構成されます。
IPX（Internetwork Packet Exchange）	ネットワーク通信で使用するプロトコル。
LAN – ローカルエリアネットワーク	通常フロアもしくはビルのような規模の小さいエリアで PC、プリンタ、サーバのようなコンピュータリソースを接続するネットワーク。高速で低エラー率が特長です。
レイテンシ	デバイスがパケットを受信する時間とパケットが到達点ポートに転送される時間の遅延。
ラインスピード	ボーレートを参照。
メインポート	通常の操作条件でデータトラフィックを送信する Resilient リンク内のポート。
MDI（Medium Dependent Interface）	1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。
MDI-X（Medium Dependent Interface Cross-over）	接続送受信のラインが交差しているイーサネットポート接続。
MIB（Management Information Base）	デバイスの管理特性と設定項目を保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。
マルチキャスト	シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。
プロトコル	ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。
Resilient link	他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。
RJ-45	10BASE-T や 100BASE-TX などで使用する標準 8 線コネクタ
RMON	リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。

用語	説明
RPS （リダンダント電源システム）	スイッチに接続されて、バックアップ電源を供給するデバイス。
サーバファーム	大量のユーザにサービスを提供する中央に位置するサーバグループ。
SLIP（Serial Line Internet Protocol）	IP がシリアルライン接続を経由して動作することが可能なプロトコル。
SNMP（Simple Network Management Protocol）	当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。
スパニングツリープロトコル (STP)	ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。
スタック	1 個の論理的なデバイスの形をとするために統合されたネットワークデバイスのグループ。
スタンバイポート	リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。
スイッチ	パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。
TCP/IP	Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。
telnet	仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。
TFTP（Trivial File Transfer Protocol）	スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する (ソフトウェアアップグレードなど) ことができます。
UDP（User Datagram Protocol）	インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。
VLAN（Virtual LAN）	物理的に接続した LAN のように通信する位置やトポロジが独立しているデバイスのグループ。
VLT（Virtual LAN Trunk）	各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。
VT100	ASCII コードを使用するターミナルタイプ。VT100 画面はテキストベースの表示をします。