D-Link DGS-1210 シリーズ
（DGS-1210-10P/20/28/28P/52）
Layer2 Web Smart Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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、記載事項にしたが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。

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ついている 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。

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

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

⚠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。

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。

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。

- 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。
- 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。

商品名 / 品番一覧

商品名	品番
DGS-1210-10P	DGS-1210-10P
DGS-1210-20	DGS-1210-20
DGS-1210-28	DGS-1210-28
DGS-1210-52	DGS-1210-52
DGS-1210-28P	DGS-1210-28P

目次

はじめに

本 DGS-1210 シリーズユーザマニュアルは HW バージョンが C1 の製品に対するインストールおよび操作方法を例題とともに記述しています。

第 1 章　本製品のご利用にあたって
- 製品の概要とその機能について説明します。また、前面および背面などの各パネルと LED 表示について説明します。

第 2 章　スイッチの設置
- スイッチの基本的な設置方法について説明します。また、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についても紹介します。

第 4 章　DNA (D-Link Network Assistant) について
- DNA (D-Link Network Assistant) のインストール、概要について説明します。

第 5 章　Web マネージャによる詳細設定
- Web ベースの管理機能への接続方法および詳細な設定方法について説明します。

第 6 章　コマンドラインインタフェース
- コマンドラインインタフェース（CLI）を使用した基本的な管理、設定方法について説明します。

第 7 章　スイッチのメンテナンス
- リセットボタンを使用してスイッチを初期設定状態に戻す方法を説明します。

【付録 A】　ケーブルとコネクタ
- RJ-45 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】　用語解説
- 本マニュアルに使用される用語の定義を示します。

付録 D 機能設定例
- 機能設定例ついて説明します。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、使用にあたっての注意事項について説明します。

警告 警告では、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。

補足 補足では、特長や技術についての詳細情報について説明します。

参照 参照では、別項目での説明へ誘導します。

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」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 " をご参照ください。
`courier` フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
`courier` 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
`courier` 斜体	コマンドパラメータ（可変または固定）。	*`value`*
< >	可変パラメータ。< > にあたる箇所に値または文字を入力します。	<*`value`*>
[ ]	任意の固定パラメータ。	[*`value`*]
[< >]	任意の可変パラメータ。	[<*`value`*>]
{ }	{ } 内の選択肢から 1 つ選択して入力するパラメータ。	{*`choice1`* | *`choice2`*}
|（垂直線）	相互排他的なパラメータ。	*`choice1`* | *`choice2`*
[{ }]	任意のパラメータで、指定する場合はどちらかを選択します。	[{*`choice1`* | *`choice2`*}]

第 1 章　本製品のご利用にあたって

スイッチ概要

DGS-1210 シリーズは、低コストで高信頼性に加え、プラグアンドプレイの簡便さも兼ね備えている中小規模（SMB）ネットワーク用スイッチです。すべてのモデルは、見やすい前面パネルの診断用 LED を搭載するメタルケースに収納されており、ネットワークセキュリティ、Asymmetric VLAN、QoS 及び多様な管理機能を搭載しています。

柔軟なポート設定
DGS-1210 シリーズは Web スマートシリーズの新世代スイッチです。8、16、24、48 ポートの 10/100/1000Mbps ポートに加えて、SFP スロットを 2 または 4 つ搭載したラインナップを揃えています。さらに PoE モデルがあり、DGS-1210-28P では 10/100/1000Mbps PoE ポートを 24 ポートと SFP スロットを 4 つ備えており、1 ～ 4 ポートで最大 30W まで給電可能な IEEE802.3at に対応、DGS-1210-10P では 10/100/1000Mbps PoE ポートを 8 ポートと SFP スロットを 2 つ備えており、全ポートで最大 30W まで給電可能な IEEE802.3at に対応しています。これにより高い壁面や天井、AC 電源の設置が困難な場所にも配置することが可能です。

D-Link グリーンテクノロジー
D-Link グリーン製品は、高性能で環境に優しい製品を提供します。D-Link Green 技術にはポートシャットダウン、LED インジケータの消灯による電力調整のような消費電力を削減する数多くのイノベーションが盛り込まれています。DGS-1210-10P/28P のような PoE モデルに関しては、ポートごとに利用時間外の電力供給をシャットダウンするタイムベース PoE 機能を実装しています。

レイヤ 2 機能
本スイッチは、IGMP Snooping、MLD Snooping、ポートミラーリング、スパニングツリー、リンクアグリゲーションおよびループバック検知などの L2 機能を搭載しており、性能とネットワークの柔軟性を強化しています。

Asymmetric VLAN、QoS 及び自動サーベイランス VLAN
スイッチはネットワークセキュリティとパフォーマンスを強化するために 802.1Q VLAN をサポートしています。また、ネットワーク上のトラフィックを優先順位付けすることによりストリームマルチメディアのような帯域を使うアプリケーションを実行するために、802.1p プライオリティキューもサポートしています。これらの機能はネットワーク上のトラフィックをシームレスに通信することを可能にします。
自動サーベイランス VLAN は事前に定義された IP サーベイランスデバイスからの映像トラフィックに対して、自動的に高いプライオリティをつけます。これにより、通常のデータトラフィックと分割することができます。AsymmetricVLAN はサーバやゲートウェイデバイスのような共有資源をより有効的に利用するために実装されています。

ネットワークセキュリティ
セーフガードエンジン機能は、ウィルス攻撃により引き起こされるトラフィックのフラッドからスイッチを保護します。また、IEEE 802.1X ポートベース認証をサポートしており、ネットワークを外部の RADIUS サーバと共に設定することができます。ACL 機能は不要な IP/MAC のトラフィックに対応する強力なツールです。ストームコントロールにより、異常なトラフィックによるフラッドからネットワークを保護します。ポートセキュリティはネットワークデバイスの安全を保つことのできる、シンプルですが有効な認証方法です。

多様な管理
D-Link Web スマートスイッチは管理者にポートレベルでのネットワークダウンをリモート監視することを可能にする直観的な操作が可能な D-Link Network Assistant（DNA）もしくは Web ベース管理インタフェースを使ってネットワークをシンプルかつ簡単に管理することを可能にし、ビジネスの成長を助けます。D-Link Network Assistant（DNA）を使用すると、同じネットワーク内の D-Link スマートスイッチや D-Link Discover Protocol (DDP) に対応したスイッチを検出し、初期設定やファームウェアのアップデートなどの管理を簡単に行うことができます。ユーザのローカル PC に接続されているのと同じ L2 ネットワークセグメント内のスイッチは、簡単なアクセスで画面に表示されます。検出されたデバイスの様々な設定やパスワード変更やファームアップグレードなどを可能にします。

ユーザは Telnet を使用してスイッチへ接続することもできます。IP アドレスの変更、工場出荷時設定へのリセット、再起動およびファームウェアの更新などの基本的なタスクはコマンドライン（CLI）を使用することができます。

さらに、スイッチステータスに関する情報のために、実装されている MIB ブラウザを使用してスイッチへのポーリングや異常なイベントのトラップ送信が可能です。MIB をサポートすることで SNMP 環境における管理のためにサードパーティのデバイスと本スイッチを統合化することができます。本スイッチはまた「D-View 6.0」に対応したプラグインモジュールを実装しており、視覚的なインタフェースによる効果的な操作、管理が可能です。

注意 D-Link 独自開発の SNMP 管理ソフトウェア、D-View は、D-Link のホームページ（http://dlink-jp.com）からマニュアルのダウンロードが可能です。

サポートする機能

- IEEE 802.3 10BASE-T、IEEE 802.3u 100BASE-TX、IEEE 802.3ab 1000BASE-T、IEEE 802.3z 1000BASE-X、IEEE 802.3x Flow Control
  IEEE 802.1D Spanning Tree、IEEE 802.1w Rapid Spanning Tree、IEEE 802.3ad Link Aggregation、IEEE 802.1Q VLAN Tagging
  IEEE 802.1X Port Based Network Access Control、IEEE 802.1p Class of Service、IEEE 802.3az Energy Efficient Ethernet
  IEEE 802.3af Power over Ethernet（DGS-1210-28P のみ）、IEEE 802.3at PoE Plus（DGS-1210-10P/28P のみ）
- L2 機能
  - IGMP スヌーピング：v1/v2/v3 ※1
    スヌーピンググループ数：256、スタティックマルチキャストアドレス数：64
    VLAN 毎の IGMP、IGMP スヌーピングクエリア
  - MLD スヌーピング：v1/v2 ※1
  - スパニングツリー：IEEE 802.1D STP、IEEE 802.1w RSTP
  - ループバック検知（STP 無し）
  - ポートトランキング：IEEE 802.3ad/ スタティック
    DGS-1210-10P：5 グループ / デバイス、8 ポート / グループ
    DGS-1210-20：10 グループ / デバイス、8 ポート / グループ
    DGS-1210-28/28P：14 グループ / デバイス、8 ポート / グループ
    DGS-1210-52：26 グループ / デバイス、8 ポート / グループ
  - ポートミラーリング：1 ポート対 1 ポート / 多対 1 ポート
  - ジャンボフレーム：9,216 Bytes
- VLAN
  - IEEE 802.1Q タグ VLAN、ポートベース VLAN、VLAN グループ数：256（スタティック）
    VLAN ID レンジ：1-4094、Voice VLAN、Asymmetric VLAN、自動サーベイランス VLAN
- QoS
  - 帯域制御、キュー：8 レベル / ポート
  - キューのスケジューリング：Strict/WRR
  - CoS：IEEE 802.1p プライオリティ、DSCP、TCP/UDP ポート、IPv6 トラフィッククラス
- ACL
  - 最大 50 プロファイル、768 ルール / デバイス
  - ACL 定義パラメータ：802.1p プライオリティ、VID、MAC アドレス、Ether タイプ、IPv4 アドレス、TCP/UDP ポート、DSCP、プロトコルタイプ、IPv6 アドレス、IPv6 トラフィッククラス
- セキュリティ
  - SSLv3（IPv4/IPv6）
  - IEEE 802.1X 認証：ポートベース認証
  - ブロードキャスト / マルチキャストストームコントロール
  - D-Link セーフガードエンジン
  - DoS 攻撃防御
  - ポートセキュリティ：64MAC アドレス / ポート
  - スタティック MAC：256
  - DHCP サーバスクリーニング
  - ARP スプーフィング防止
  - トラフィックセグメンテーション
  - IP-MAC ポートバインディング：ARP モード /DHCP スヌーピングモード /DHCPv6 スヌーピングモード
  - 管理アクセス認証用：ローカル、ユーザ認証用：RADIUS
- マネジメント
  - LLDP、LLDP-MED、Web ベース GUI（IPv4/IPv6）、CLI、Telnet サーバ（IPv4/IPv6）、
  - SNMPv1/v2c/v3、SNMP over IPv6、SNMP トラップ
  - RMONv1：4 グループ、トラストホスト（IPv4/IPv6）、DHCP 自動設定、DHCP/BOOTP クライアント、
  - DHCPv6 クライアント、Syslog（IPv4/IPv6）、TFTP クライアント（IPv4/IPv6）、SNTP クライアント（IPv4/IPv6）、
  - 設定バックアップ / リストア、ファームウェアバックアップ / リストア、IPv6 Neighbor Discovery（ND）、
  - ケーブル診断、EEE（802.3az）
- 以下の MIB のサポート
  - MIB II（ RFC1213）
  - Bridge MIB（RFC1493）
  - SNMPv2 MIB（RFC1907）
  - RMON MIB（RFC1757, RFC2819）
  - MIB Traps Convention（RFC1215）
  - Interface Group MIB（RFC2233）
  - Ether-like MIB（RFC1398, RFC1643, RFC1650, RFC2358, RFC2665）
  - 802.1p MIB（RFC2674, RFC4363）
  - Power-Ethernet-MIB（RFC3621）（DGS-1210-10P/28P のみ）
  - LLDP-MIB
  - Private MIB、ZoneDefense MIB

※ 1 : Source フィルタ未サポート

搭載ポート

DGS-1210 シリーズスイッチは以下のポートを搭載しています。

DGS-1210-10P
- 10BASE-T/100BASE-TX/1000BASE-T ポート x　8
- SFP スロット　x　2

DGS-1210-20
- 10BASE-T/100BASE-TX/1000BASE-T ポート x　16
- SFP スロット　x　4

DGS-1210-28
- 10BASE-T/100BASE-TX/1000BASE-T ポート x　24
- SFP スロット　x　4

DGS-1210-52
- 10BASE-T/100BASE-TX/1000BASE-T ポート x　48
- SFP スロット　x　4

DGS-1210-28P
- 10BASE-T/100BASE-TX/1000BASE-T ポート x　24（PoE 給電）
- SFP スロット　x　4

前面パネル

前面パネルには、Power、リセットボタン、オプションモジュール用の SFP ポート、ポートの Link/Act の状態を表示する LED を搭載しています。

参照　LED 表示については、LED 表示を参照してください。

補足　リセットボタンを押下すると、すべての設定が工場出荷時の状態にリセットされます。

補足　DGS-1210-10P/28P の「Mode」ボタンでは、Link/Act モードと PoE モードの切り替えを行います。

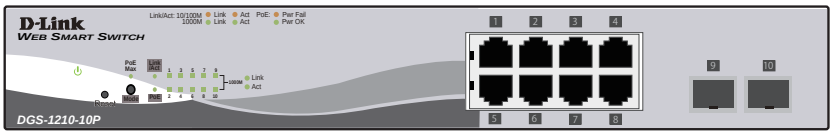


図 1-1　DGS-1210-10P の前面パネル図

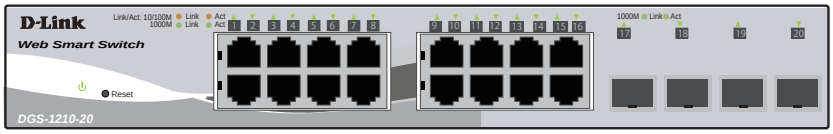


図 1-2　DGS-1210-20 の前面パネル図

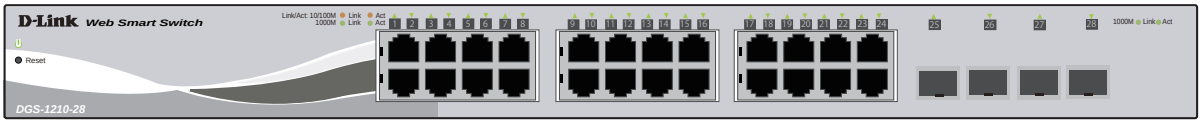


図 1-3　DGS-1210-28 の前面パネル図

図 1-4　DGS-1210-52 の前面パネル図

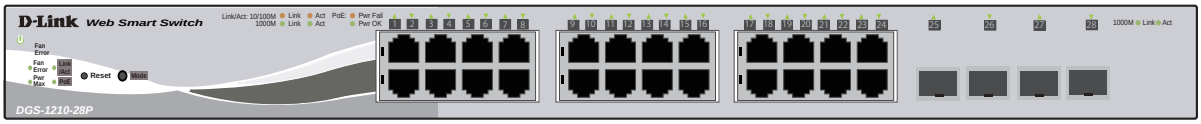


図 1-5　DGS-1210-28P の前面パネル図

LED 表示

各機種の LED 表示は、以下のイラストと表のとおりです。

DGS-1210-20

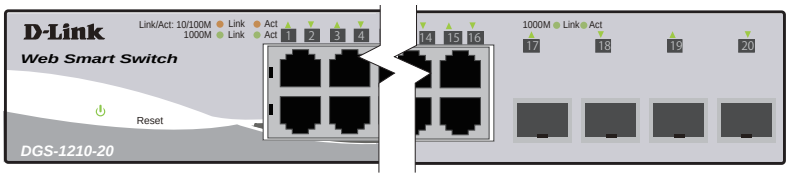


図 1-6　DGS-1210-20 の前面パネルの LED 配置図

DGS-1210-28

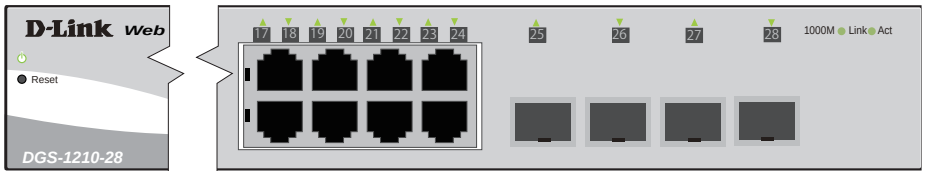


図 1-7　DGS-1210-28 の前面パネルの LED 配置図

DGS-1210-52

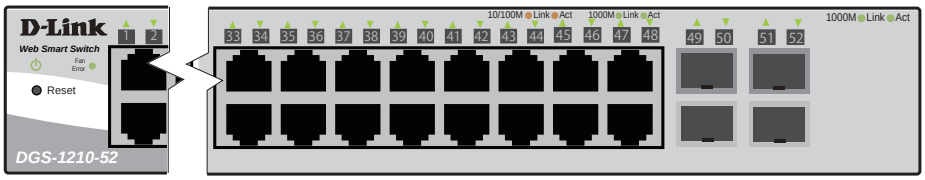


図 1-8　DGS-1210-52 の前面パネル LED 配置図

LED	状態	色	内容
システム LED			
Power	点灯	緑	電源が供給されています。
	消灯	ー	電源が供給されていません。
Fan Error (DGS-1210-52 のみ)	点灯	緑	ファンが正常に動作しています。
	点灯	赤	ファンに障害が発生し、動作が止まっています。
ポート LED			
10/100/1000 Mbps ポート LED	点灯	緑	1000Mbps でリンクが確立しています。
	点滅	緑	1000Mbps でデータを送受信しています。
	点灯	橙	100/10Mbps でリンクが確立しています。
	点滅	橙	100/10Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。
SFP スロット LED	点灯	緑	1000Mbps でリンクが確立しています。
	点滅	緑	1000Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。

DGS-1210-10P

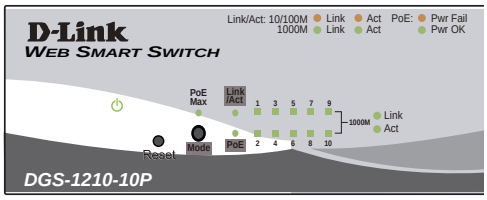


図 1-9　DGS-1210-10P の前面パネルの LED 配置図

DGS-1210-28P

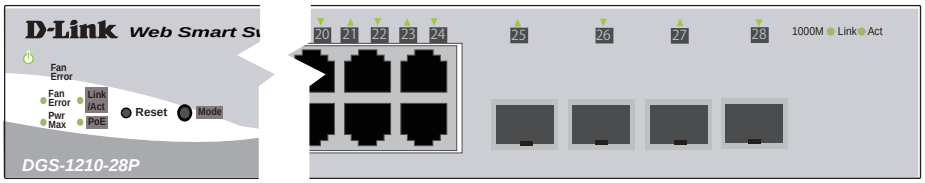


図 1-10　DGS-1210-28P の前面パネルの LED 配置図

LED		状態	色	内容
システム LED				
Power		点灯	緑	電源が供給され正常に動作しています。
		消灯	―	電源コードが接続していない、あるいは接触不良であることを示します。
Fan Error （DGS-1210-28P のみ）		点灯	緑	ファンが正常に動作しています。
		点灯	赤	ファンに障害が発生し、動作が止まっています。
PoE Max（DGS-1210-10P） Pwr Max（DGS-1210-28P）		点灯	赤	供給可能電力 に到達しました。
		消灯	―	供給可能電力 に到達していません。PoE 受電機器に給電可能です。
Link/Act		点灯	緑	Link/Act モードに設定されています。
		消灯	―	PoE モードに設定されています。
PoE		点灯	緑	PoE モードに設定されています。
		消灯	―	Link/Act モードに設定されています。
ポート LED				
10/100/1000 Mbps ポート LED	Link/Act モードの場合	点灯	緑	1000Mbps でリンクが確立しています。
		点滅	緑	1000Mbps でデータを送受信しています。
		点灯	橙	100/10Mbps でリンクが確立しています。
		点滅	橙	100/10Mbps 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。
	PoE モードの場合	点灯	緑	電力が供給されています。
		点灯	橙	正常に動作していません。
		消灯	―	電力が供給されていません。
SFP スロット LED		点灯	緑	1000Mbps でリンクが確立しています。
		点滅	緑	1000Mbps 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

背面パネルには電源コネクタ、接地コネクタ、電源抜け防止クリップ挿入口、およびセキュリティロックがあります。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-1210-10P

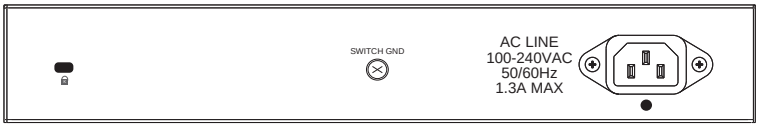


図 1-11　DGS-1210-10P 背面パネル図

DGS-1210-20

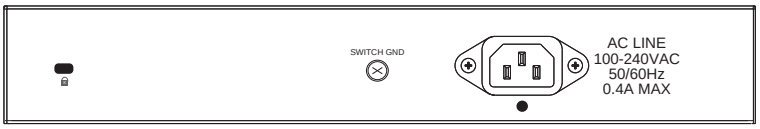


図 1-12　DGS-1210-20 背面パネル図

DGS-1210-28

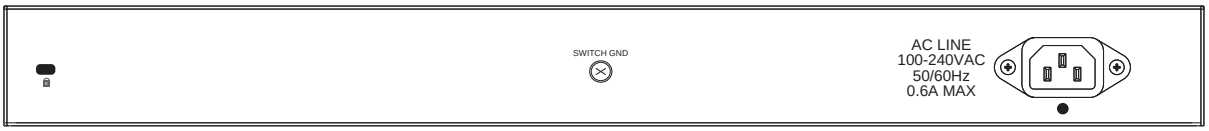


図 1-13　DGS-1210-28 背面パネル図

DGS-1210-28P

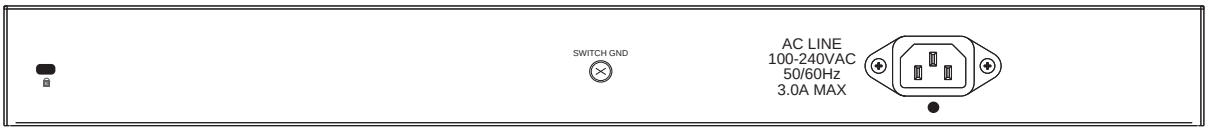


図 1-14　DGS-1210-28P 背面パネル図

DGS-1210-52

図 1-15　DGS-1210-52 背面パネル図

SFP スロット

DGS-1210 シリーズスイッチは、スイッチの前面パネルに SFP モジュール用スロットを装備しています。

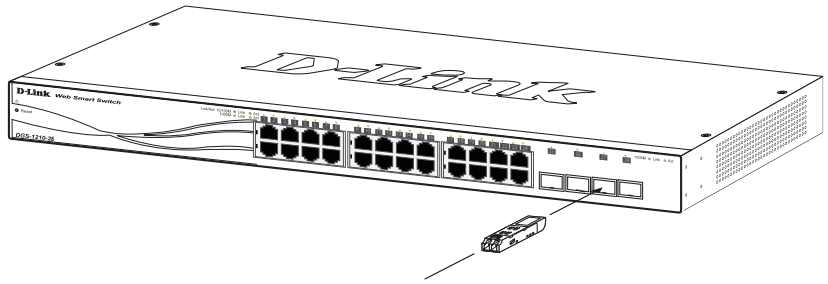


図 1-16　スイッチに光トランシーバを取り付ける

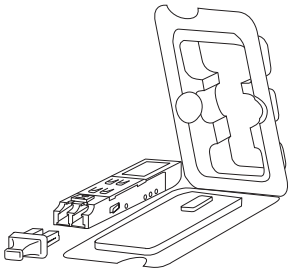


図 1-17　SFP モジュール図

第 2 章　スイッチの設置

パッケージの内容

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

- 本体
- AC 電源ケーブル（100V 用）
- 19 インチラックマウントキット
- 電源抜け防止クリップ
- マニュアル
- ゴム足
- CD-ROM
- シリアルラベル
- PL シート

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、交換のために弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

ネットワーク接続前の準備

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

- スイッチは、しっかりとした水平面で、耐荷重性のある場所に設置してください。
- 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るゴム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。

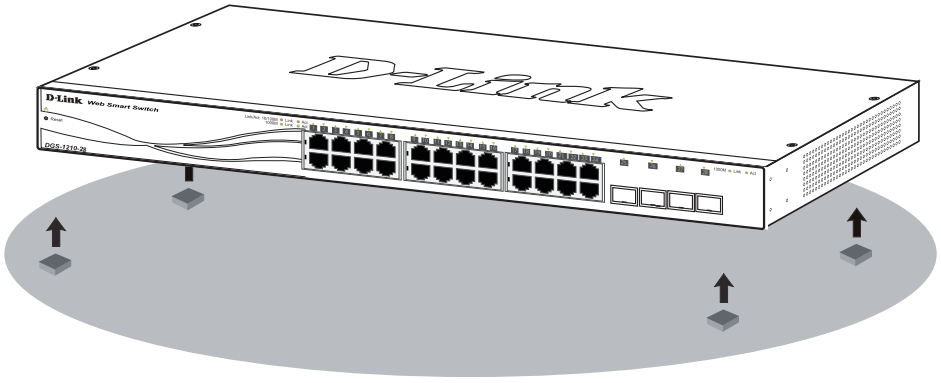


図 2-1　ゴム足の取り付け

19 インチラックへの取り付け

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

ブラケットの取り付け

ラックマウントキットに含まれるネジを使用して、本スイッチにブラケットを取り付けます。

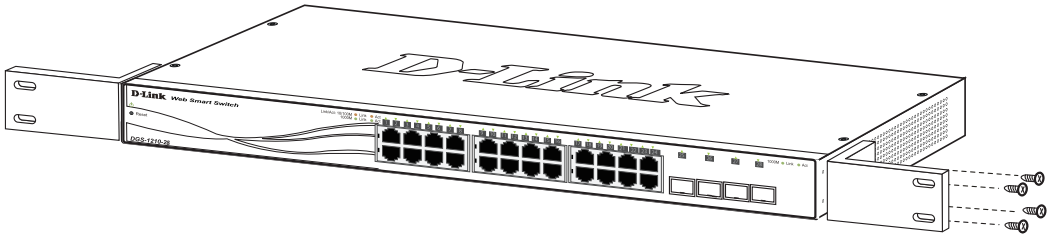


図 2-2　スイッチへのブラケットの取り付け

完全にブラケットが固定されていることを確認してから、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。

19 インチラックにスイッチを取り付ける

19 インチラックにスイッチを取り付けます。作業を行う際は、安全のため以下の点を確認してください。

A. 動作時の周囲温度の上昇
密閉型のラックや、多くの製品が搭載されたラックに設置した場合、動作時のラック周囲の温度が室温を上回ることがあります。
本製品の最大動作温度に準拠する環境に設置するよう注意してください。

B. 通気量の低下
ラック内で、機器の安全な動作に必要な通気量が確保されるようにしてください。

C. 機械的荷重
ラックへ取り付ける場合、機械的荷重がかたよると危険です。荷重が不均等にならないよう注意してください。

D. 回路の過負荷
電源回路に装置を接続する際は、回路が過負荷状態になったときに、過電流保護機能および配線に及ぼす影響に注意してください。
この問題に対応する際は、装置の銘板に記載されている定格を考慮してください。

E. 信頼性の高い接地
ラックに取り付けられている製品が、信頼できる方法で接地されている状態を維持してください。
電源タップの使用など、分岐回路に直接接続する以外の方法を使用する場合は、その接続部に特に注意してください。

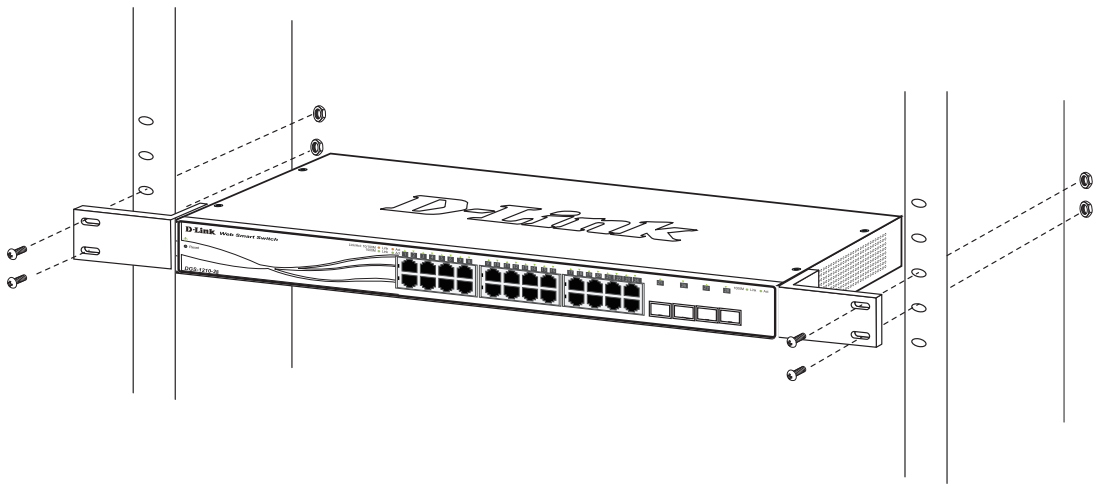


図 2-3　スイッチのラックへの設置

電源抜け防止クリップの装着

アクシデントにより AC 電源コードが抜けてしまうことを防止するために、スイッチに電源抜け防止クリップを装着します。
以下の手順に従って電源抜け防止クリップを装着します。

1. スイッチの背面の電源プラグの下にある穴に、付属の電源抜け防止クリップのタイラップ（挿し込み先のあるバンド）を下記の図のように差し込みます。

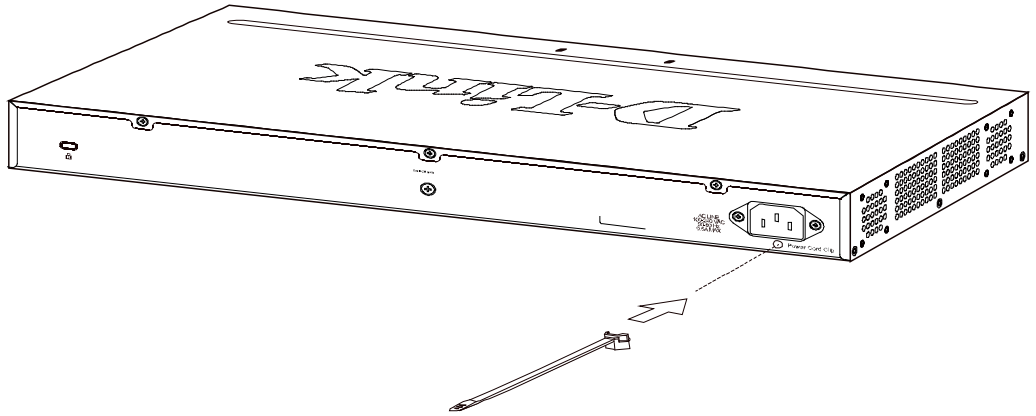


図 2-4　　タイラップの挿し込み

2. AC 電源コードをスイッチの電源プラグに挿し込みます。

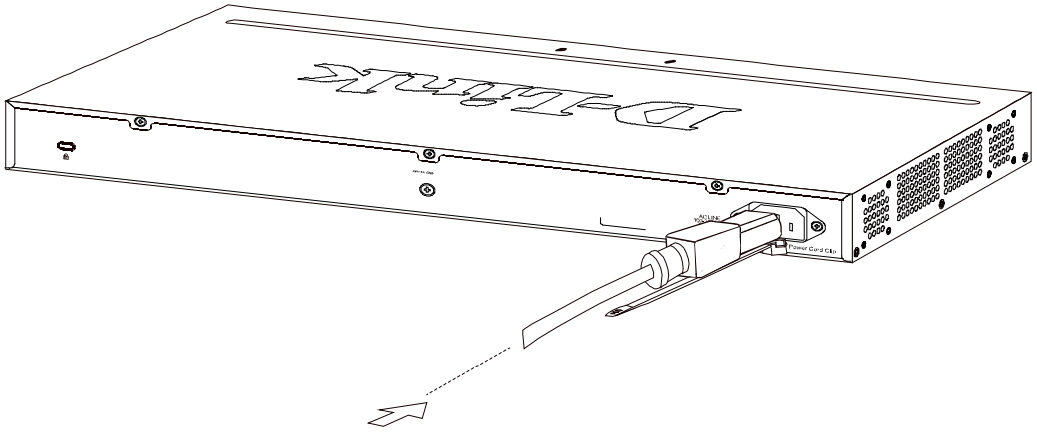


図 2-5　　電源コード挿し込み

3. 以下の図のように挿し込んだタイラップにリテイナー（固定具）をスライドさせ装着します。

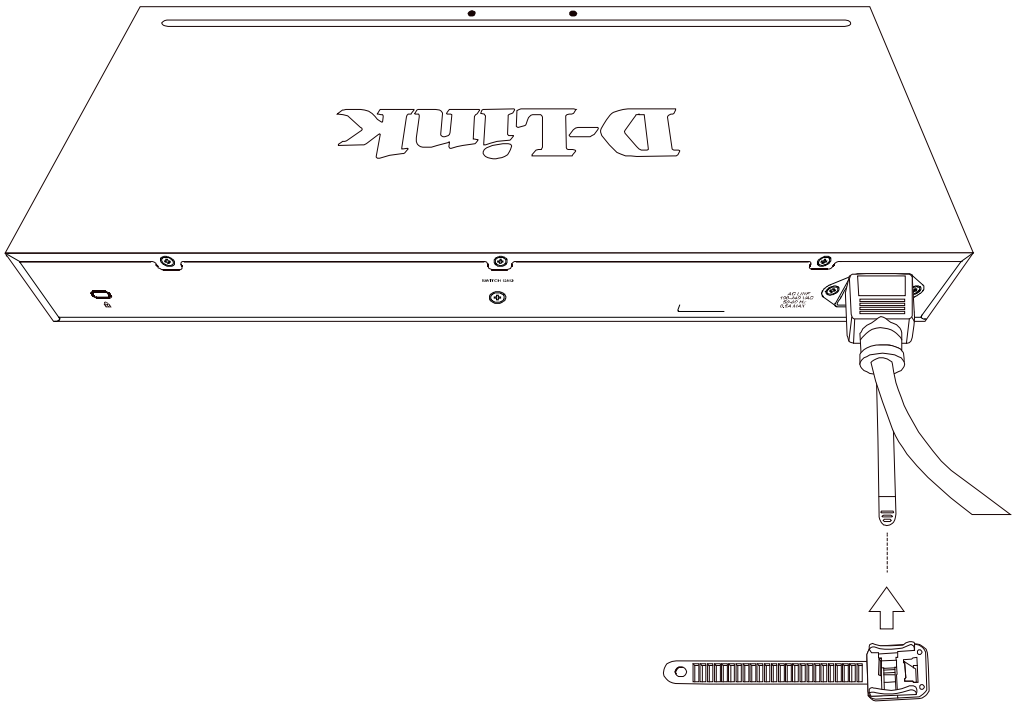


図 2-6　　リテイナー（固定具）のスライド

4. 以下の図のようにリテイナーを電源コードに巻き付け、リテイナーのロック部分に挿し込みます。

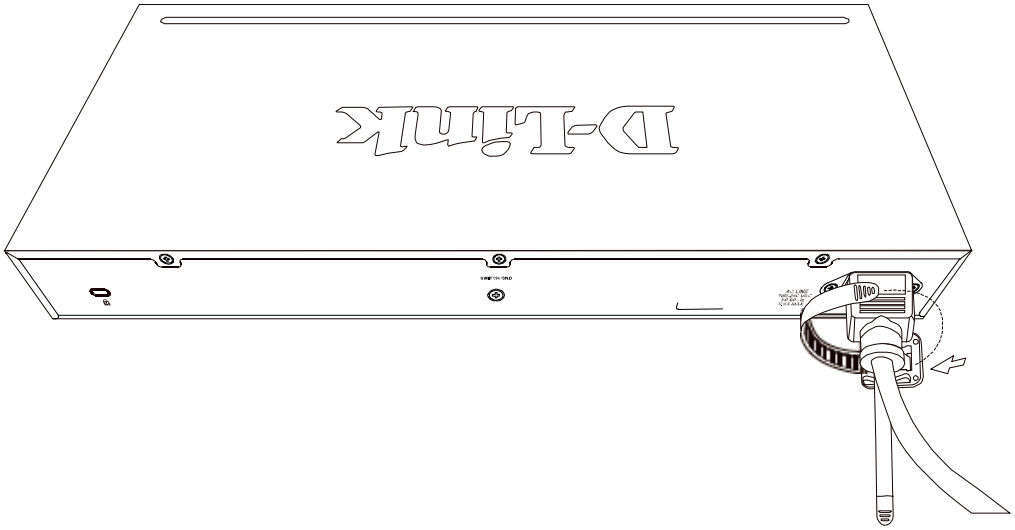


図 2-7　リテイナーの巻き付け、固定

4. リテイナーを電源コードにしっかりと巻き付けた後、電源コードが抜けないか確かめます。

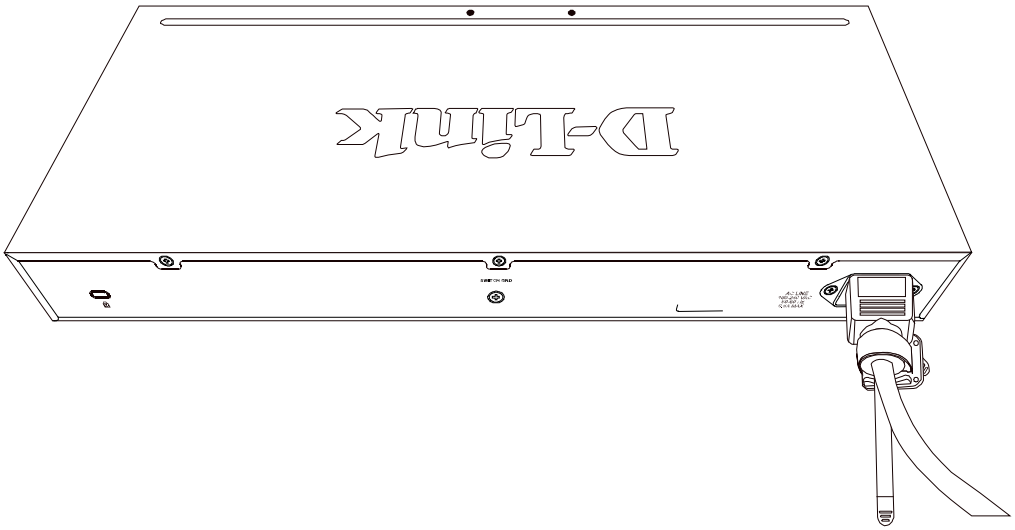


図 2-8　電源抜け防止クリップの固定確認

スイッチの接地

本スイッチを接地する方法について説明します。

注意　スイッチの電源をオンにする前に、本手順を完了する必要があります。

接地に必要なツールと機器

- 接地ネジ（M4x6mm のパンヘッドネジ）1 個
- 接地線（同梱されていません）
- スクリュードライバ（同梱されていません）

注意　接地線は国の設置必要条件に従ったサイズにする必要があります。商用に利用可能な 6 AWG 導線をお勧めします。また、ケーブル長は適切な接地設備にスイッチの距離に従います。

以下の手順でスイッチを保安用接地に接続します。

1. システムの電源がオフであることを確認します。

2. 接地ケーブルを使用して、以下の図のように、オープン状態の接地ネジ穴の上に #8 リング型ラグ端子を置きます。

3. 接地ネジ穴に接地端子を挿入します。

4. ドライバを使用して、接地ネジをしめて、スイッチに接地ケーブルを固定します。

5. スイッチが設置されるラック上の適切な設置スタッドまたはボルトに接地線の一端にあるリング型ラグ端子を取り付けます。

6. スイッチとラック上の設置コネクタの接続がしっかりと行われていることを確認します。

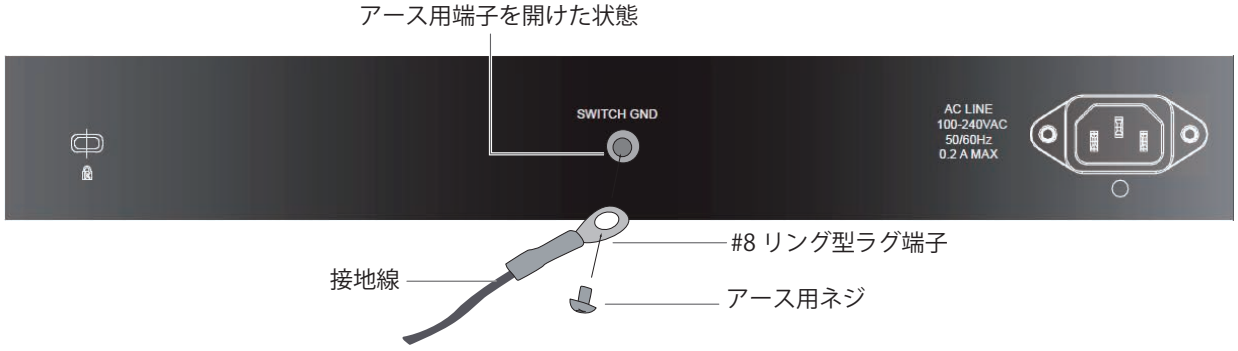


図 2-9　　スイッチへのラグ端子の接続

電源の投入

1. 電源ケーブルを本スイッチの電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。
2. 本スイッチに電源が供給されると、Power LED が点灯します。

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

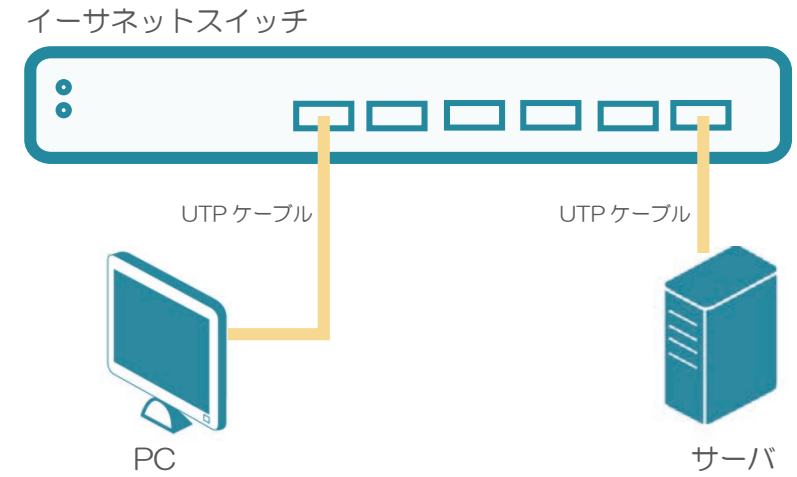


図 3-1　エンドノードと接続した図

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。PoE 給電に使用する。（DGS-1210-10P/28P のみ）

ケーブル仕様については、【付録 A】　ケーブルとコネクタを参照してください。

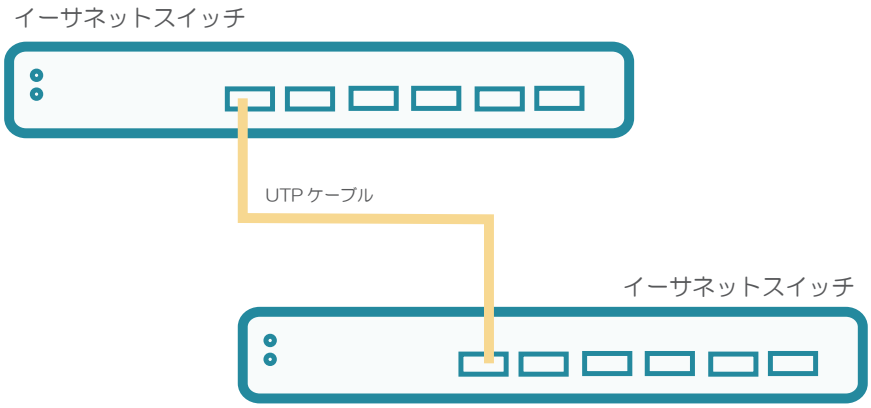


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

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

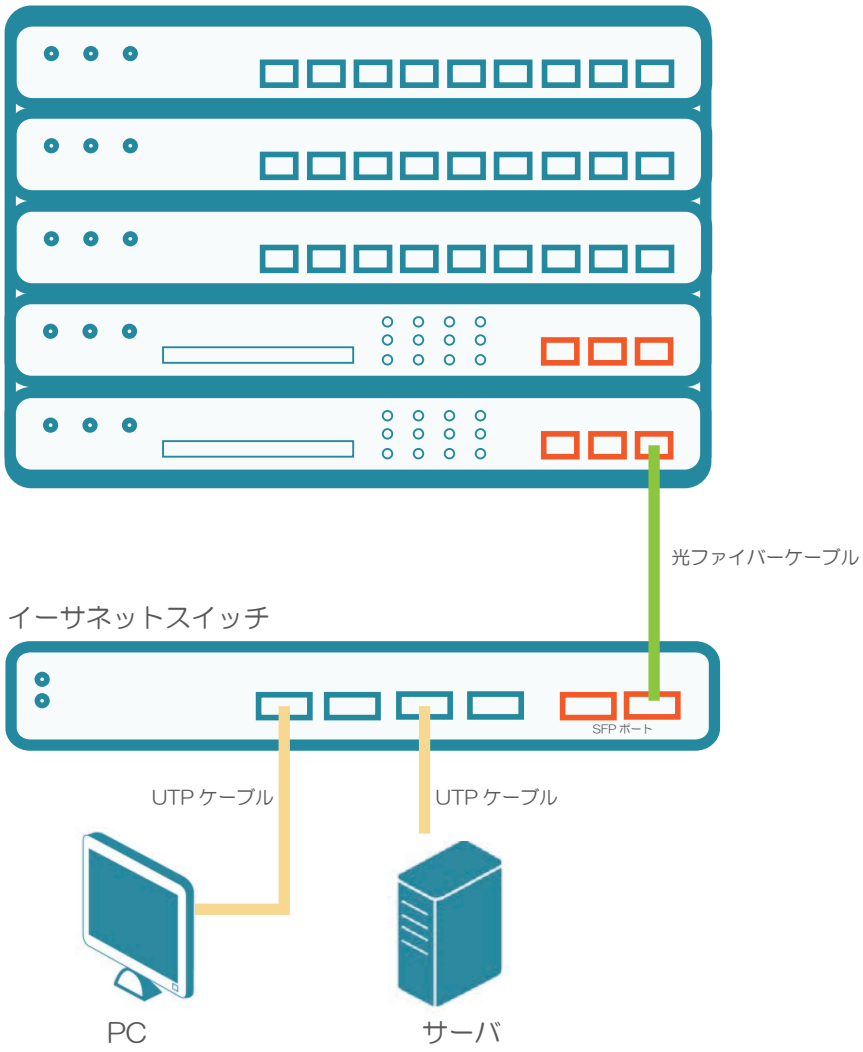


図 3-3　サーバ、PC、スイッチスタックとのアップリンク接続図

第 4 章　DNA (D-Link Network Assistant) について

インストール CD に含まれている DNA（D-Link Network Assistant）は PC に接続している同じ L2 ネットワークセグメント内の Smart スイッチを検出、管理するためのプログラムです。このツールは Windows2000、XP、Vista、Windows7 をサポートしています。
DNA（DLink Network Assistant）のインストールには 2 つの方法があります。1 つはインストール CD の自動実行プログラムに従う方法、もう 1 つは手動でインストールする方法です。

DNA (D-Link Network Assistant) の自動インストール

インストール CD の自動実行プログラムを介して DNA（D-Link Network Assistant）をインストールする手順です。

1. 製品に付属の CD-ROM を管理用 PC の CD-ROM ドライブに挿入します。
   自動的に起動し、起動画面を表示が表示されます。
2. 自動実行プログラムが自動的にポップアップされます。
3. ”Install DNA（D-Link Network Assistant）” ボタンをクリックするとインストールウィザードが段階的に案内します。
4. DNA のインストールに成功した後、**Start > Programs > D-Link > DNA** に DNA を見つけることができます。
5. PC と同じ L2 ネットワークセグメントに接続されている Smart スイッチを DNA（D-Link Network Assistant）を使って検出します。

DNA (D-Link Network Assistant) の手動インストール

DNA（D-Link Network Assistant）を手動でインストールする手順です。

1. 製品に付属の CD-ROM を管理用 PC の CD-ROM ドライブに挿入します。
   自動的に起動し、起動画面を表示が表示されます。
2. Windows デスクトップ上のスタートメニューからコンピュータを選択します。
3. CD-ROM/DVD-ROM ドライブをダブルクリックし、自動実行メニューを開始します。もしくは、ドライブを右クリックしてフォルダを開きます。DNA（D-Link Network Assistant）を選択し、setup.exe ファイルをダブルクリックします。
4. ユーティリティをインストールするため、スクリーン上の指示に従います。
5. 完了後、**Start > Programs > D-Link > DNA** に移動し、DNA（D-Link Network Assistant）を開きます。
6. PC と同じ L2 ネットワークセグメントに接続されている Smart スイッチを DNA（D-Link Network Assistant）を使って検出します。

注意　DNA の詳細情報に関しては、CD-ROM 内のユーザマニュアル（D-Link Network Assistant User Guide）を参照してください。

注意　最新の DNA をインストールする前に既存の DNA を必ずアンインストールしてください。

第 5 章　Web マネージャによる詳細設定

Web ベースの管理について

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

対応しているブラウザ

- Inrternet Explorer 6 以降
- Firefox 3.0 以降
- Mozilla 最新版
- Netscape 8 以降
- Opera 10 以降

Web マネージャへのログイン

1. コンピュータでブラウザを起動します。
2. スイッチの IP アドレスを入力します。

図 5-1　　URL の入力

注意　工場出荷時設定では、IP アドレス「10.90.90.90」、サブネットマスク「255.0.0.0」が設定されています。
Web マネージャへログインするには、PC の IP アドレスを本スイッチに合わせるか、本スイッチを PC の IP アドレスに合わせてください。

【例】スイッチの IP アドレスが 10.90.90.90 の場合：

以下のとおりに設定します。
管理 PC のアドレス：10.x.y.z（x/y は 0 ～ 254 の間の整数、z は 1 ～ 254 の間の整数）
サブネットマスク：255.0.0.0

3. ユーザ認証画面で、パスワードを入力し、「OK」をクリックします。

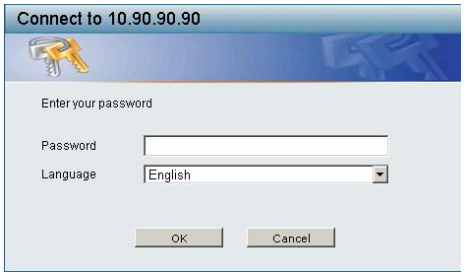


図 5-2　パスワード入力画面

補足　パスワードの初期値は「admin」です。

補足　「Language」で表示言語を選択することができます。

4. スマートウィザード画面が表示されます。

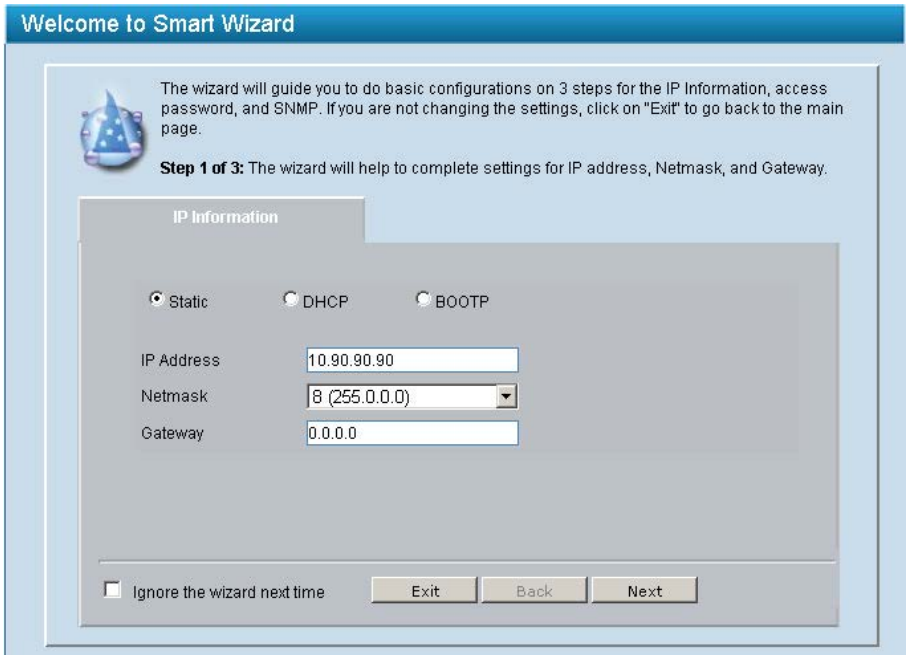


図 5-3　Smart Wizard 画面

ウィザード画面では、IP アドレス・パスワード・SNMP の設定を行うことができます。
ウィザードを使用して設定する場合は、Smart Wizard 設定を参照してください。

5. ウィザードを使用しない場合は、「Exit」をクリックします。

6. 以下の Web マネージャのメイン画面が表示されます。

図 5-4　Web マネージャメイン画面

Smart Wizard 設定

「Smart Wizard」で基本的なシステム設定 (IP アドレス、パスワード、SNMP) を行います。

補足 Smart Wizard では、IPv4 アドレスのみ設定可能です。

補足 Web マネージャメイン画面の「Smart Wizard」から、Smart Wizard 画面に移動できます。

補足 「Ignore the wizard next time」にチェックをいれた場合は、次回のログイン時に Smart Wizard 画面が表示されません。

1. IP アドレスの設定を行います。

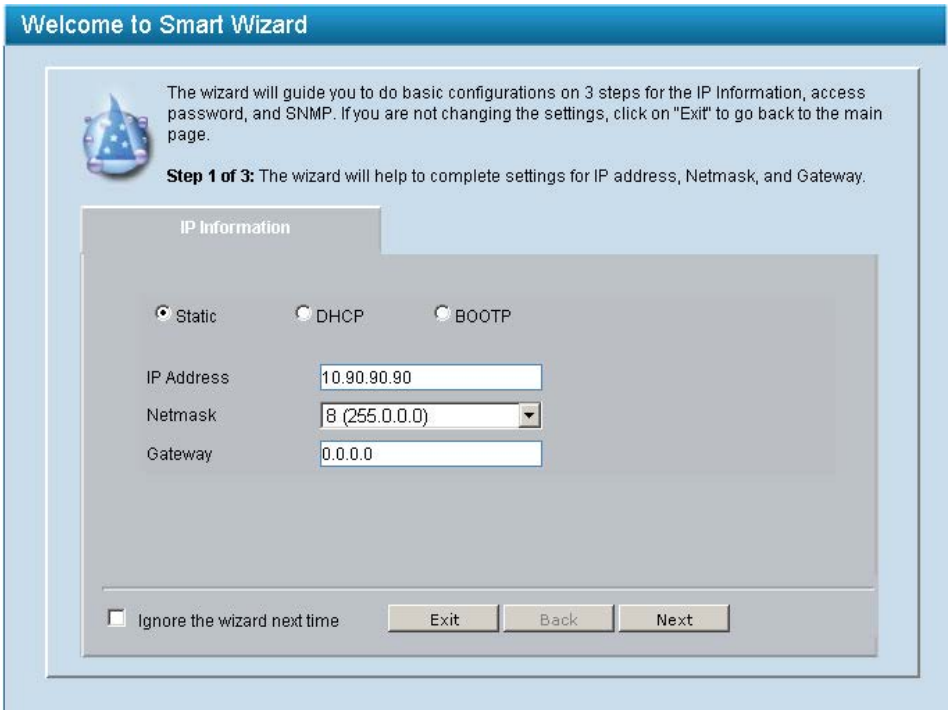


図 5-5　IP Information 設定画面

1. 「Static」「DHCP」「BOOTP」のいずれかをクリックします。
   - 「Static」：固定設定
   - 「DHCP」：DHCP による自動取得
   - 「BOOTP」：BOOTP による自動取得
2. 「Static」を選択した場合は、「IP Address」「Netmask」「Gateway」を入力します。
3. 「Next」をクリックします。

補足 スイッチの IP アドレスを変更すると、現在の PC とスイッチの接続が切断します。Web ブラウザに正しい IP アドレスを入力して、必ずご使用のコンピュータをスイッチと同じサブネットに設定してください。

2. パスワードの設定を行います。

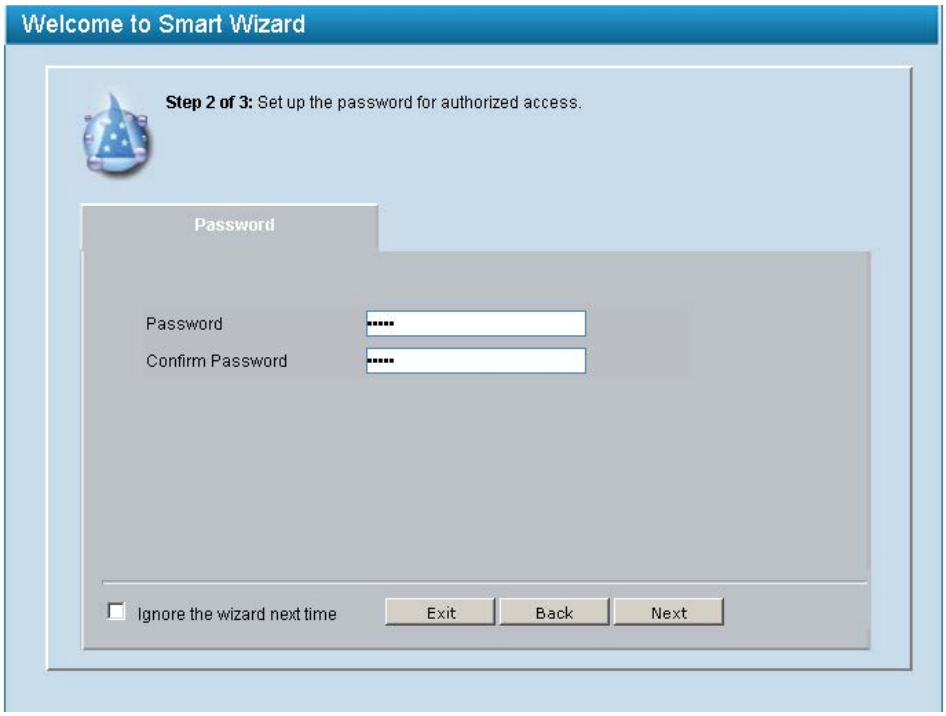


図 5-6　IP Information 設定画面

1. 「Password」欄に新しいパスワードを入力します。
2. 「Confirm Password」欄に確認のため再度同じパスワードを入力ます。
3. 「Next」をクリックします。

3. SNMP の設定を行います

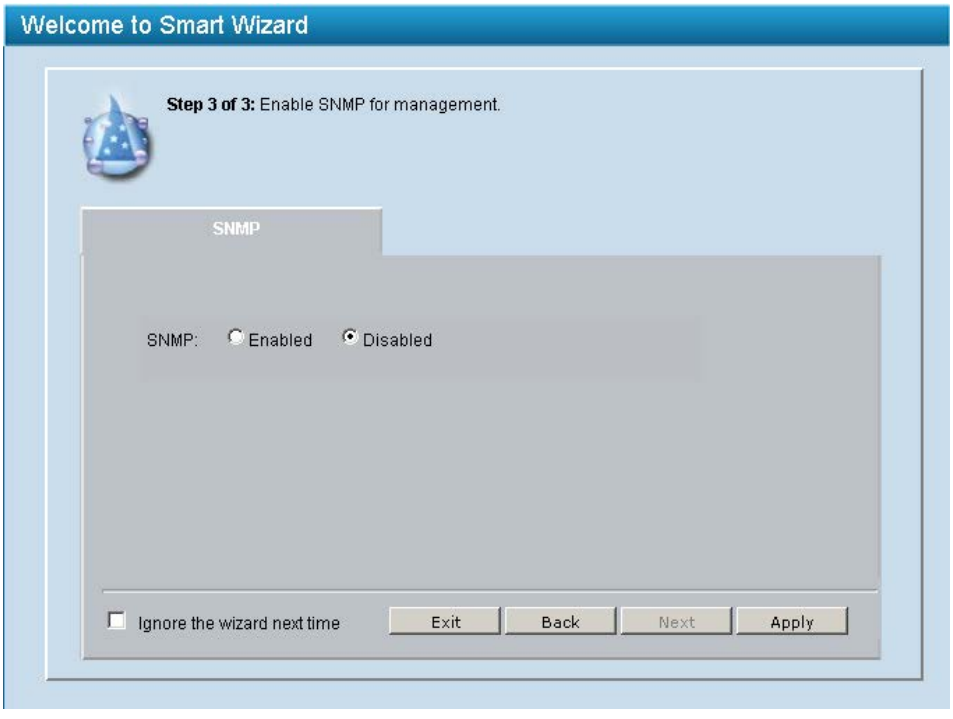


図 5-7　IP Information 設定画面

1. 「Enabled」(有効) または「Disabled」(無効) を選択します。
2. 「Apply」をクリックします。

Web マネージャ画面が表示されます。

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を行ったり、パフォーマンス状況やシステム状況を参照することができます。

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 5-8　　初期画面

エリア 1（機能一覧）：表示するメニューを選択します。メニューアイコンを開いて、サブメニューを表示します。
エリア 2（ツールバー）：スイッチの再起動や設定の初期化・保存、ファームウェアアップデートなどを行います。
エリア 3（デバイス情報）：IP アドレスなど、スイッチ設定情報が表示されます。「Device Status and Quick Configurations」の「Settings」から、設定を変更することも可能です。

注意　ハードウェアリミテーションによりユーザートラフィックもしくは装置の高負荷時に WebGUI の表示が遅延または表示できない場合、Ping、SNMP に応答できない場合があります。

Web マネージャのメニュー構成

Web マネージャで設定可能な機能は以下の通りです。スイッチのすべての設定オプションは画面左側の機能フォルダの各項目をクリックして、設定画面にアクセスします。ここでは各オプションに関する機能や設定の詳細を説明します。

メインメニュー	サブメニュー	説明
ツールバー		
Save	Save Configuration	スイッチにコンフィグレーションの設定を保存します。
	Save Log	ログエントリをローカルドライブに保存します。 ログはテキストファイル形式で保存され、閲覧、編集が可能です。
Tools	Reset	スイッチのリセットを行います。IP アドレス以外の設定が初期値にリセットされます。
	Reset System	スイッチの完全リセットを行います。全ての設定値が初期値にリセットされ、再起動します。
	Reboot Device	システムを再起動します。
	Configuration Backup & Restore	コンフィグレーションをファイルに保存し、またはスイッチへ復元します。復元方法は「HTTP」「TFTP」から選択します。
	Firmware Backup & Upload	ファームウェアのバックアップとアップロードを行います。「HTTP」「TFTP」から選択します。
Wizard		「Smart Wizard」画面へ移動します。「Smart Wizard」で設定をする場合に使用します。
Help		以下の 2 種類のウェブサイトへ接続します。 • D-Link Support Site： 英語版のサポートサイトです。日本用のファームウェアやマニュアルのダウンロードについては、http://www.dlink-jp.com/ の「製品情報」をご参照ください。 • User Guide： 英語版のオンラインマニュアルです。
Logout		Web マネージャ画面からログオフします。
機能一覧		
System	System Settings	IP 情報およびシステム情報の設定を行います。
	IPv6 System Settings	IPv6 情報およびシステム情報の設定を行います。
	IPv6 Route Settings	IPv6 Route の設定を行います。
	IPv6 Neighbor Settings	IPv6 Neighbor の設定を行います。
	Password	パスワードの設定を行います。
	Port Settings	ポートの設定と状態モニタを行います。
	Port Description	ポート概要を設定、表示します。
	DHCP Auto Configuration	DHCP の設定を行います。
	DHCP Relay	DHCP リレーの設定を行います。
	DHCP Local Relay Settings	DHCP ローカルリレーの設定を行います。
	DHCPv6 Relay Settings	DHCPv6 ローカルリレーの設定を行います。
	Syslog Host	システムログの範囲、記録方法、有効 / 無効について設定します。
	Time Profile	時間の設定を行います。
	Power Saving	省電力の設定を行います。
	IEEE802.3az EEE settings	IEEE802.3az EEE の設定を行います。
	D-Link Discover Protocol Settings	D-Link Discover Protocol の設定を行います。

メイン メニュー	サブメニュー	説明
VLAN	802.1Q VLAN	802.1Q VLAN の設定、および Asymmetric VLAN の設定を行います。
	802.1Q VLAN PVID	各ポートの 802.1Q VLAN PVID の設定を行います。
	802.1Q Management VLAN	スイッチの設定した VLAN に変更します。
	Voice VLAN	音声 VLAN 機能を設定します。
	Auto Surveillance VLAN	デバイスから割り当てられた VLAN まで、自動的にビデオトラフィックの送信を行います。
L2 Functions	Jumbo Frame	ジャンボフレームを有効にします。
	Port Mirroring	ポートミラーリングの設定を行います。
	Loopback Detection	ループ検知機能を設定します。
	MAC Address Table	スタティック / ダイナミック MAC アドレステーブルの設定をします。
	Spanning Tree	802.1D スパニングツリーの設定を行います。
	Link Aggregation	Link Aggregation 機能を設定します。
	Multicast	マルチキャストフォワーディング、マルチキャストフィルタリングの設定を行います。
	SNTP	時刻、タイムゾーンの設定をします。
	LLDP	LLDP ポート設定、802.1 /802.3 Extension TLV ポート情報の表示、LLDP 管理アドレス / 管理アドレステーブルの設定、LLDP リモートテーブルの表示を行います。
QoS	Bandwidth Control	帯域幅の設定を行います。
	802.1p/DSCP/ToS	QoS プライオリティレベルの設定を行います。
Security	Trusted Host	トラストホストを設定します。
	Port Security	ポートセキュリティの設定を行います。
	Traffic Segmentation	ポートのトラフィックフローを制限します。
	Safeguard Engine	セーブガードエンジン機能を設定します。
	Storm Control	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を制限します。
	ARP Spoofing Prevention	パケットコンテンツ ACL を使用して、ARP スプーフィング攻撃を防止します。
	DHCP Server Screening	不正な DHCP サーバへのアクセスを拒否します。
	SSL	証明書の設定、暗号スイートの設定を行います
	DoS Prevention Settings	DoS 攻撃防御の設定を行います。
	SSH	SSH の設定を行います。
	Smart Binding	「Smart Binding」（MAC と IP のバインドによるクライアントのアクセス制限）の設定を行います。
AAA	RADIUS Server	RADIUS Server を設定します。
	802.1X	802.1X 認証を設定します。
ACL	ACL Wizard	ACL 設定ウィザード（ACL Configuration Wizard）で ACL の設定を行います。
	ACL Access List	ACL アクセスリストを表示、編集します。
	ACL Access Group	ACL アクセスグループを表示、編集します。
	ACL Hardware Resource Status	ハードウェアにおける ACL アクセスリストのリソース状況を表示します。
PoE	PoE Global Settings	システムの給電可能電力を設定し、PoE ステータスを表示します。（DGS-1210-10P/28P のみ）
	PoE Port Settings	PoE の有効 / 無効などポートにおける PoE 機能の設定を行います。（DGS-1210-10P/28P のみ）
SNMP	SNMP	SNMP 設定を行います。
	RMON	SNMP 機能に対するリモートモニタリング (RMON) 設定を行います。
Monitoring	Port Statistics	ポートのパケットカウント統計情報を表示します。
	Cable Diagnostics	スイッチに接続しているケーブルの診断をします。
	System Log	システムログを表示します。

Web マネージャの初期画面

Web マネージャが表示された場合、または画面左側部「機能一覧」の機種名が選択されている場合、メイン画面には「Device Information」（デバイス情報）が表示されます。本画面から現在のデバイスの状態を確認し、設定の変更を行います。

Device Information（デバイス情報）

ハードウェア情報や IP アドレス、ファームウェア情報、などスイッチについて重要な情報が表示されます。
「Settings」から、設定を変更することも可能です。

図 5-9　Device Information 画面

■ 画面に表示される項目

項目	説明
Device Information	
Device Type	機種名を表示します。
System Name	ユーザが定義したシステム名を表示します。
Boot Version	デバイスのブートバージョンを表示します。
System Location	システムが位置している場所を表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
System Time	システムの日付を表示します。日 / 月 / 年 / 時刻で表示します。
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
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ナンバーを表示します。
Login Timeout (minutes)	ユーザが Web マネージャで操作をしなかった場合に、デバイスがタイムアウトするまでの時間を表示します。（単位：分） 初期値：5 (分） 設定可能範囲：3-30 (分)
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 Information	
IPv4 Address	IPv4 アドレスを表示します。
Subnet Mask	サブネットマスクを表示します。
Default Gateway	デフォルトゲートウェイを表示します。
IPv6 Global Unicast Address	IPv6 グローバルユニキャストアドレスを表示します。
IPv6 Link-Local Address	IPv6 リンクローカルアドレスを表示します。

項目	説明
Device Status and Quick Configurations	
RSTP	「Setting」をクリックすると L2 Functions > Spanning Tree > STP Global Settings にリンクします。 初期値：「Disabled」
Port Mirroring	「Setting」をクリックすると L2 Functions > Port Mirroring にリンクします。 初期値：「Disabled」
Storm Control	「Setting」をクリックすると Security > Storm Control にリンクします。 初期値：「Disabled」
DHCP Client	「Setting」をクリックすると System > System Settings にリンクします。 初期値：「Disabled」
Jumbo Frame	「Setting」をクリックすると L2 Functions > Jumbo Frame にリンクします。 初期値：「Disabled」
SNMP Status	「Setting」をクリックすると SNMP > SNMP > SNMP Global Setting にリンクします。 初期値：「Disabled」
802.1X Status	「Setting」をクリックすると AAA > 802.1X > 802.1X Settings にリンクします。 初期値：「Disabled」
Safeguard Engine	「Setting」をクリックすると Security > Safeguard Engine にリンクします。 初期値：「Enabled」
IGMP Snooping	「Setting」をクリックすると L2 Functions > Multicast > IGMP Snooping にリンクします。 初期値：「Disabled」
Power Saving	「Setting」をクリックすると System > Power Saving Settings にリンクします。 初期値：「Enabled」

Save メニュー

コンフィグレーションおよびログを保存します。

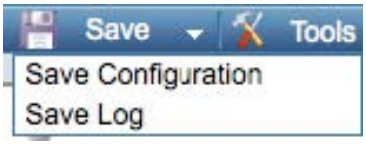


図 5-10　Save メニュー

Save Configuration（コンフィグレーションの保存）

設定したコンフィグレーションを保存します。

1. 「Save」>「Save Configuration」の順にメニューをクリックします。
2. 「Save Config」をクリックします。

図 5-11　Save Configration 画面

3. 「Continue」をクリックします。

図 5-12　Save Configration 画面

警告　「Save Config」をクリックしたあと、30 秒間以上経過するまで電源を切らないでください。
30 秒以上経過する前に電源を切ると、設定が正しく保存されないか、設定が工場出荷時状態に戻ります。

Save Log（ログ保存）

ログををファイルに保存します。

1. 「Save」>「Save Log」の順にメニューをクリックします。
2. 「Backup Log」をクリックします。

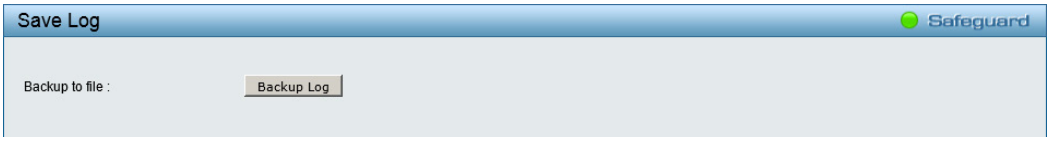


図 5-13　Save Log 画面

ログファイルがダウンロードできます。

Tools メニュー

リセット、システムリセット、コンフィグレーションのバックアップとリストア、ファームウェアのバックアップとアップグレード、システムの再起動などのシステムに関する機能を提供します。

図 5-14　Tools メニュー

Reset（リセット）

スイッチのリセットを行います。
IP アドレスをのぞき、すべての設定が工場出荷時の状態にリセットされます。

1. 「Tools」>「Reset」の順にメニューをクリックします。
2. 「Apply」をクリックします。

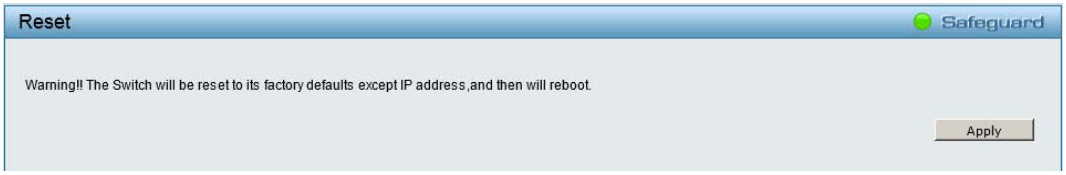


図 5-15　Reset 画面

3. 「OK」をクリックします。

図 5-16　Reset 確認画面

設定がリセットされ、デバイスが再起動します。

Reset System（システムリセット）

スイッチのリセットを行います。すべてのコンフィグレーションは工場出荷時設定にリセットされます。

1. 「Tools」>「System Reset」の順にメニューをクリックします。
2. 「Apply」をクリックします。

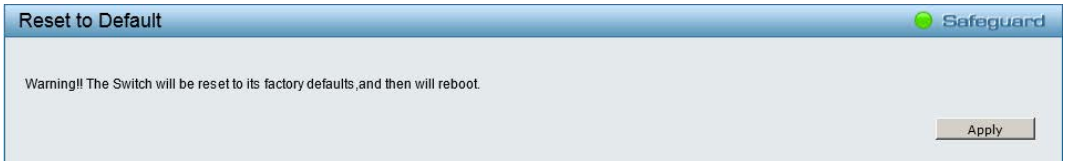


図 5-17　System Reset 画面

3. 「OK」をクリックします。

図 5-18　System Reset 確認画面

設定がリセットされ、デバイスが再起動します。

Reboot Device（デバイスの再起動）

スイッチの再起動を行います。保存していない設定は失われます。

1. 「Tools」>「Reboot Device」の順にメニューをクリックします。
2. 「Apply」をクリックします。

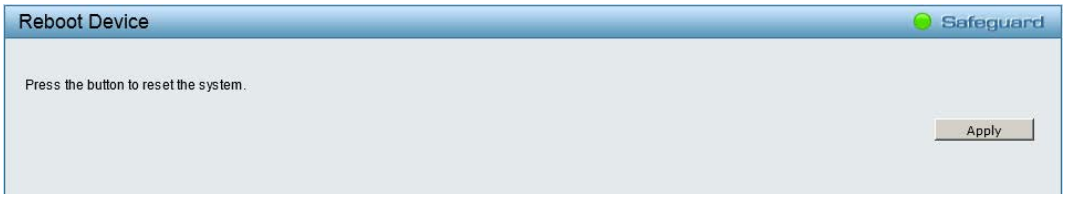


図 5-19　Reboot Device 画面

3. 「OK」をクリックします。

図 5-20　Reboot Device 確認画面

デバイスが再起動します。

Configuration Backup & Restore（コンフィグレーションのバックアップとリストア）

現在のコンフィグレーション（パスワードは除く）をファイルに保存します。
必要時にはバックアップファイルを使用した復元も可能です。ファイルの転送方法は「HTTP」または「TFTP」から選択できます。

1. 「Tools」>「Configuration Backup & Restore」の順にメニューをクリックします。
2. 「HTTP」または「TFTP」を選択します。

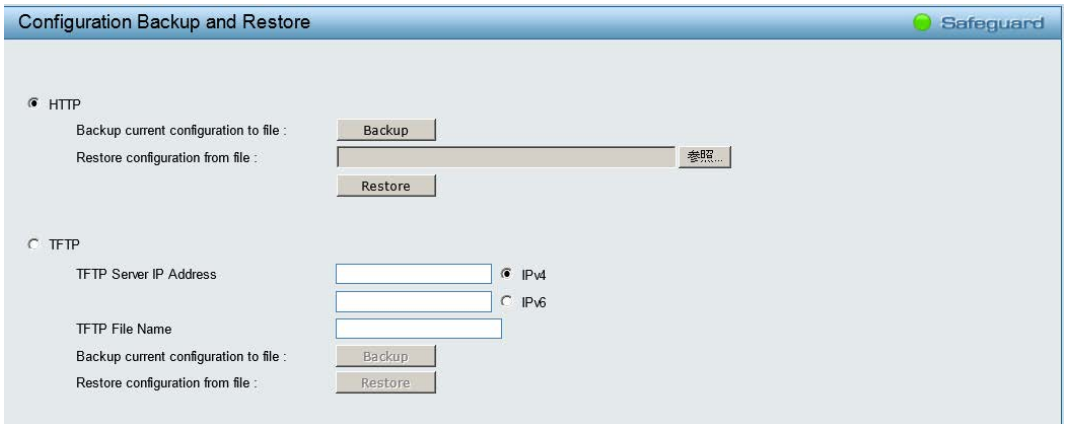


図 5-21　Configuration Backup and Restore 画面

3. 設定したい内容に応じて、以下の項目から操作を選択します。

■ 画面に表示される項目

プロトコル	説明
HTTP	**バックアップ方法** • 「Backup」をクリックし、現在のコンフィグレーションをローカルデスクに保存します。 **リストア方法** • 「Restore configuration from file :」横の「参照 / ファイルを選択 /Browse」をクリックし、保存したコンフィグレーションファイルを参照します。 • 保存済みのコンフィグレーションファイルを指定後に「Restore」をクリックし、設定の復元を開始します。
TFTP	**バックアップ方法** • 対応する TFTP サーバの IP アドレスを「IPv4」/「IPv6」から選択します。 • TFTP サーバの IP アドレスを「TFTP Server IP Adress」に入力し、「TFTP File Name」にファイル名を入力します • 「Backup」をクリックし、現在のコンフィグレーションを指定した TFTP サーバに保存します。 **リストア方法** • 対応する TFTP サーバの IP アドレスを「IPv4」/「IPv6」から選択します。 • TFTP サーバの IP アドレスを「TFTP Server IP Adress」に入力し、「TFTP File Name」にファイル名を入力します。 • 「Restore」をクリックし、TFTP サーバから 設定の復元を開始します。

注意　コンフィグレーションを復元するためにはスイッチの再起動が必要です。
また、コンフィグレーションを復元すると、現在のすべての設定が失われます。

Firmware Backup & Upgrade（ファームウェアの保存とアップグレード）

ファームウェアのバックアップ、またはファームウェアのアップグレードを行います。
ファームウェアの転送方法は、「HTTP」または「TFTP」から選択できます。

1. 「Tools」>「Firmware Backup & Upgrade」の順にメニューをクリックします。
2. 「HTTP」または「TFTP」を選択します。

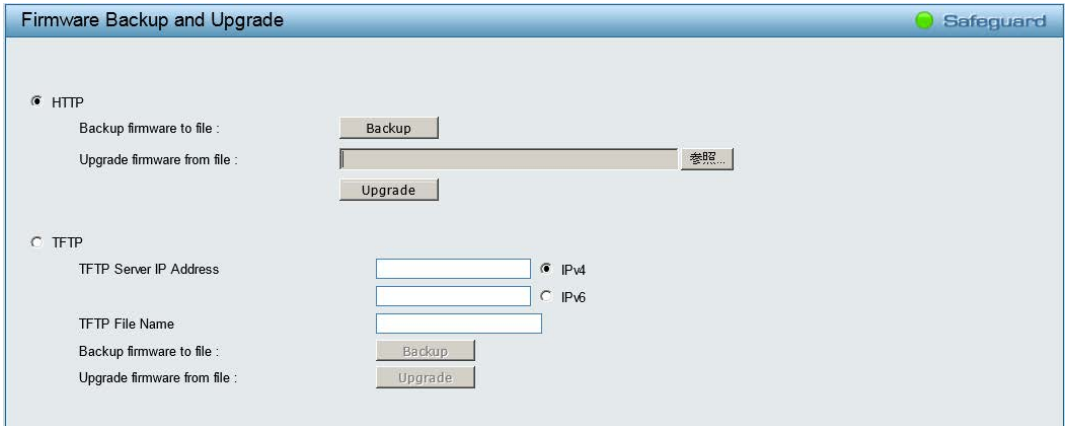


図 5-22　Firmware Backup and Upgrade 画面

3. 設定したい内容に応じて、以下の項目から操作を選択します。

■ 画面に表示される項目

プロトコル	説明
HTTP	**バックアップ方法** • 「Backup」をクリックし、現在のコンフィグレーションをローカルデスクに保存します。 **アップグレード方法** • 「Upgrade firmware from file : 」横の「参照 / ファイルを選択 /Browse」をクリックし、ファームウェアファイルを参照します。 • ファイルを指定後に「Upgrade」をクリックし、アップグレードを開始します。
TFTP	**バックアップ方法** • 対応する TFTP サーバの IP アドレスを「IPv4」/「IPv6」から選択します。 • TFTP サーバの IP アドレスを「TFTP Server IP Adress」に入力し、「TFTP File Name」にファイル名を入力します • 「Backup」をクリックし、現在のコンフィグレーションを指定した TFTP サーバに保存します。 **アップグレード方法** • 対応する TFTP サーバの IP アドレスを「IPv4」/「IPv6」から選択します。 • TFTP サーバの IP アドレスを「TFTP Server IP Adress」に入力し、「TFTP File Name」にファイル名を入力します • 「Upgrade」をクリックし、TFTP サーバから スイッチのアップグレードを開始します。

注意　ファイルの更新が完全に終了する前に PC との接続を切断したり、電源コードを外したりしないでください。
ファームウェアの更新が終了しないと、スイッチが破損する可能性があります。

Smart Wizard メニュー（スマートウィザード）

「Smart Wizard」をクリックして、「Smart Wizard」画面へ移動します。
Smart Wizard については、Smart Wizard 設定を参照してください。

Help メニュー（オンラインヘルプ）

オンラインヘルプを表示します。
「D-Link Support Site」と「User Guide」の 2 種類があります。

D-Link Support Site（D-Link サポートサイトへの参照）

D-Link のサポートサイトを参照します。
本サイトは英語版です。ファームウェアのダウンロードなどについては、ディーリンクジャパンのウェブサイトを参照してください。

User Guide（ユーザガイドへの参照）

「User Guide」をクリックします。以下の画面を表示します。

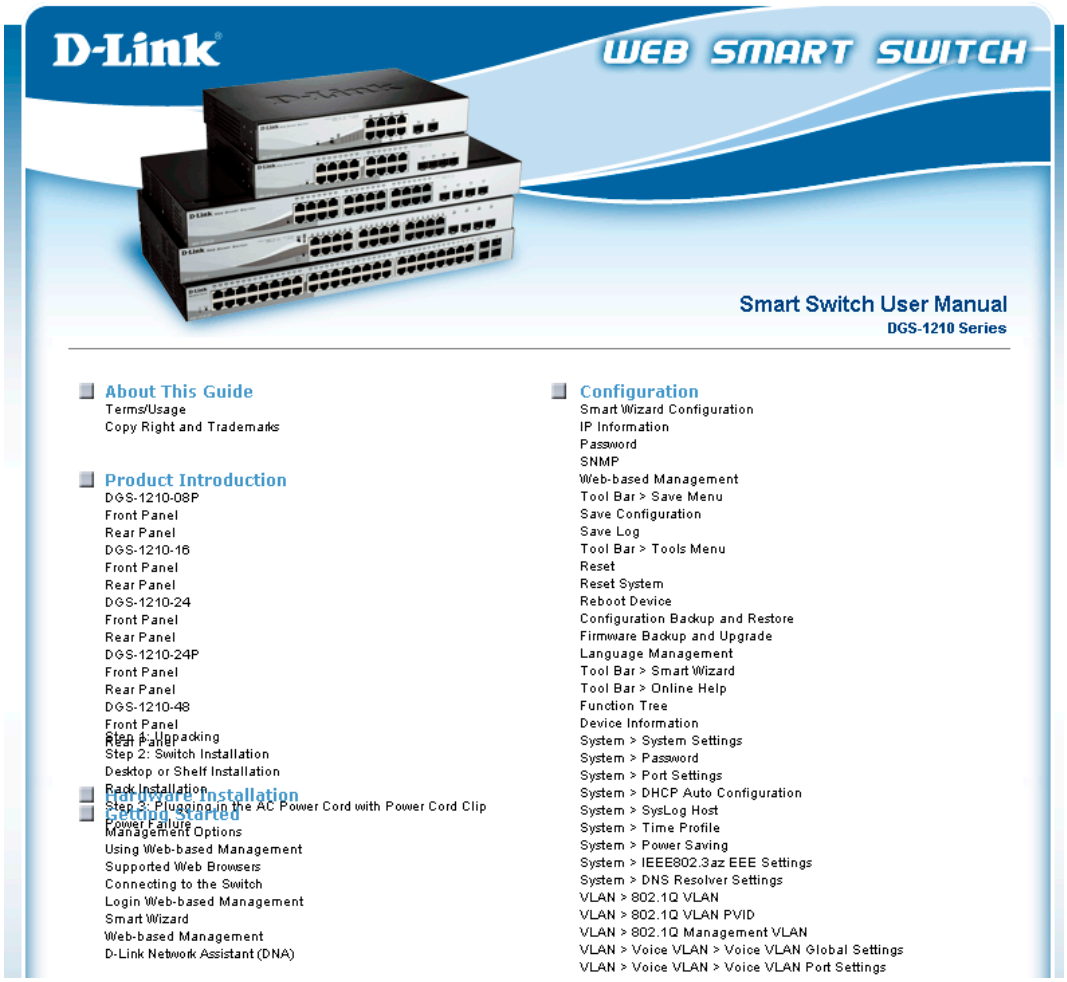


図 5-23　User Guide 画面

System（システム設定）

■ System(システム設定) の設定項目

- System Settings（スイッチの基本機能の設定）
- IPv6 System Settings（IPv6 システム設定）
- IPv6 Route Settings（IPv6 Route 設定）
- IPv6 Neighbor Settings（IPv6 Neighbor 設定）
- Password（パスワード設定）
- Port Settings（ポート設定）
- DHCP Auto Configuration（DHCP 自動設定）
- DHCP Relay（DHCP リレー設定）
- DHCP Local Relay Settings（DHCP ローカルリレー設定）
- DHCPv6 Relay Settings（DHCPv6 リレー設定）
- SysLog Host（SysLog Host 設定）
- Time Profile（タイムプロファイル設定）
- Power Saving（省電力設定）
- IEEE802.3az EEE Settings（IEEE 802.3az EEE 設定）
- D-Link Discover Protocol Settings（D-Link Discover Protocol 設定）

System Settings（スイッチの基本機能の設定）

スイッチの IP アドレスおよび基本的なシステム情報の設定を行います。

1. 「System」>「System Settings」の順にメニューをクリックします。

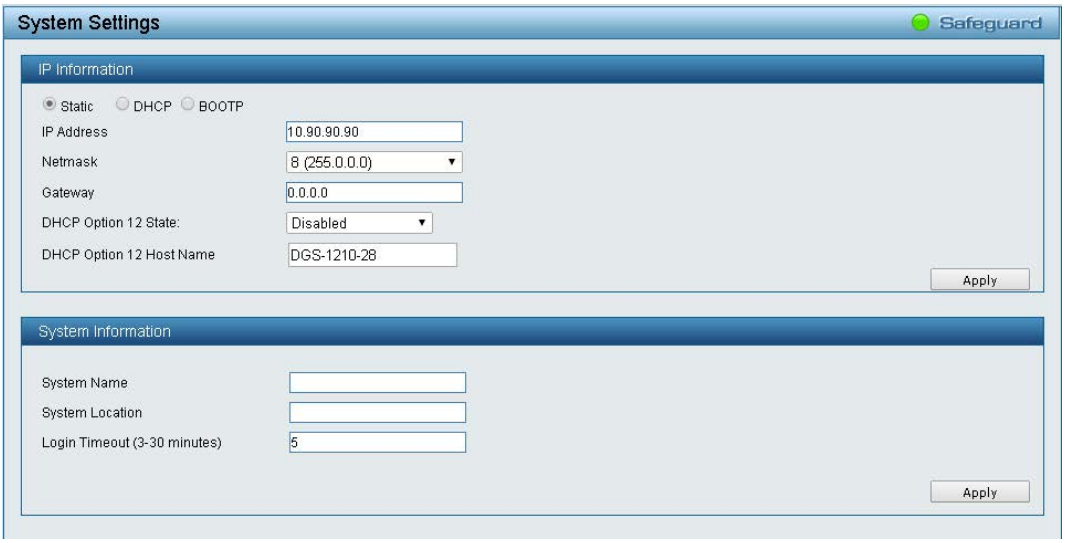


図 5-24　System Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
IP Information	
Static/DHCP/BOOTP	IP アドレスを取得するモードを選択します。 初期値：「Static」 選択肢：「Static 」「DHCP」「BOOTP」 • Static 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します。本モードを選択した場合には、「IP Address」、「Subnet Mask」および「Gateway」を入力します。初期値は IP アドレスは「10.90.90.90」、サブネットマスクは「255.0.0.0」です。 • DHCP DHCP を使用して 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割り当てます。 • BOOTP BOOTP を使用して 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割り当てます。
IP Address	「Static」を選択した場合、IP アドレスを設定します。
Netmask	「Static」を選択した場合、上記 IP アドレスのサブネットマスクを設定します。
Gateway	「Static」を選択した場合、上記 IP アドレスのゲートウェイを設定します。
DHCP Option 12 State	DHCP Option 12 を有効 / 無効にします。
DHCP Option 12 Host Name	DHCP Option 12 のホスト名を指定します。
System Information	
System Name	ネットワーク上でスイッチを識別する名前を設定します。 名前を登録することにより、DNA（D-Link Network Assistant）を使用する際に LAN 上の他の Web スマートデバイスの中から特定のデバイスを認識しやすくなります。
System Location	ネットワーク上のスイッチの場所を入力します。 登録することにより、DNA（D-Link Network Assistant）を使用する際に LAN 上の他の Web スマートデバイスの中から特定のデバイスを認識しやすくなります。
Login Timeout (3-30 minutes)	Web マネージャ上で操作が行われない場合に、自動的にログインする時間を指定します。(単位：分) 指定した時間が経過すると、再ログインが要求されます。 初期値：5（分） 選択可能範囲：3-30（分）

3. 「Apply」をクリックし、設定を有効にします。

IPv6 System Settings（IPv6 システム設定）

スイッチの IPv6 情報およびシステム情報の設定を行います。

1. 「System」>「IPv6 System Settings」の順にメニューをクリックします。

図 5-25　IPv6 System Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
IPv6 System Settings	
Interface Name	インターフェース名を表示します。
IPv6 State	IPv6 を「Enabled」(有効) または「Disabled」無効にします。 初期値：「Enabled」
DHCPv6 Client	DHCPv6 クライアントを「Enabled」(有効) または「Disabled」無効にします。 初期値：「Disabled」
IPv6 Network Address	IPv6 ネットワークアドレスを設定します。
NS Retransmit Time Settings	
NS Retransmit Time (1-3600)	Neighbor Solicitation の再送タイマ (秒) を入力します。 初期値：1（秒） 入力可能範囲：1-3600（秒）
Automatic Link Local State Settings:	
Automatic Link Local Address	自動リンクローカルアドレスを有効または無効にします。

3. 「Apply」をクリックし、設定を有効にします。

IPv6 Route Settings（IPv6 Route 設定）

IPv6 Route の設定を行います。

1. 「System」>「IPv6 Route Settings」の順にメニューをクリックします。

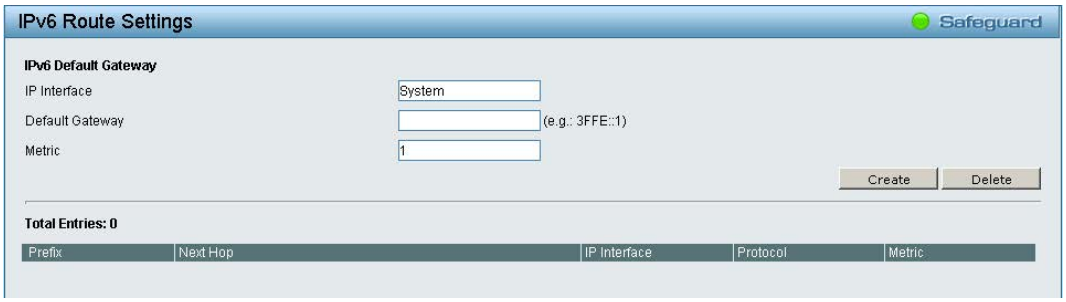


図 5-26　IPv6 Route Settings 画面

2. 設定したい内容に応じて、以下の項目から操作を選択します。

■ 画面に表示される項目

項目	説明
IPv6 Default Gateway	
IP Interface	インタフェース名を指定します。
Default Gateway	IPv6 形式におけるネクストホップゲートウェイアドレスに対応する IPv6 アドレスを指定します。
Metric	IPv6 インタフェースのメトリック値を指定します。 入力可能範囲：1-65535

3. 「Create」をクリックし、設定を保存します。

設定を削除する場合は、「Delete」をクリックします。

IPv6 Neighbor Settings（IPv6 Neighbor 設定）

IPv6 Neighbor の設定を行います。

1. 「System」>「IPv6 Neighbor Settings」の順にメニューをクリックします。

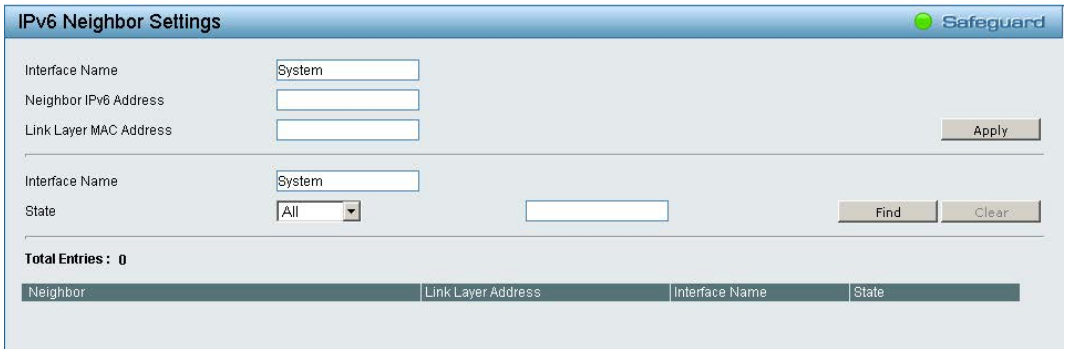


図 5-27　IPv6 Neighbot Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

IPv6 Neighbor の新規登録：
「Neighbor IPv6 Address」および「Link Layer MAC Address」を入力 →「Apply」をクリックします。

エントリの検索：
画面中央の「State」で「All」、「Address」、「Static」または「Dynamic」を選択 →「Find」クリックします。

エントリの削除：
「Clear」をクリックします。

■ 画面に表示される項目

項目	説明
Interface Name	インターフェース名が表示されます。
Neighbor IPv6 Address	Neighbor の IPv6 アドレスを入力します。
Link Layer MAC Address	リンクレイヤの MAC アドレスを入力します。
State	「All」、「Address」、「Static」または「Dynamic」を指定します。 「Address」を選択すると、「State」オプション横にあるスペースに IP アドレスを入力できるようになります。

Password（パスワード設定）

デバイスにログインするパスワードを設定します。

1. 「System」>「Password」の順にメニューをクリックします。

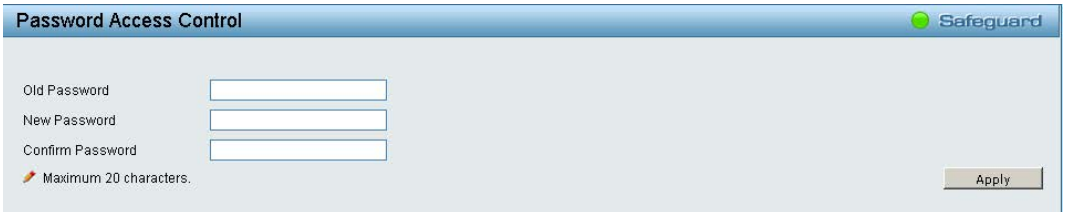


図 5-28　Password Access Control 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Old Password	登録済みのパスワードを入力します。 初期値：Admin
New Password	新しいパスワードを入力します。 入力可能文字：20 文字までの半角英数字
Confirm Password	新しい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。

3. 「Apply」をクリックし、設定を有効にします。

Port Settings（ポート設定）

各ポートについて、スピード、MDI/MDIX、Flow Control の設定を行います。

1. 「System」>「Port Settings」の順にメニューをクリックします。

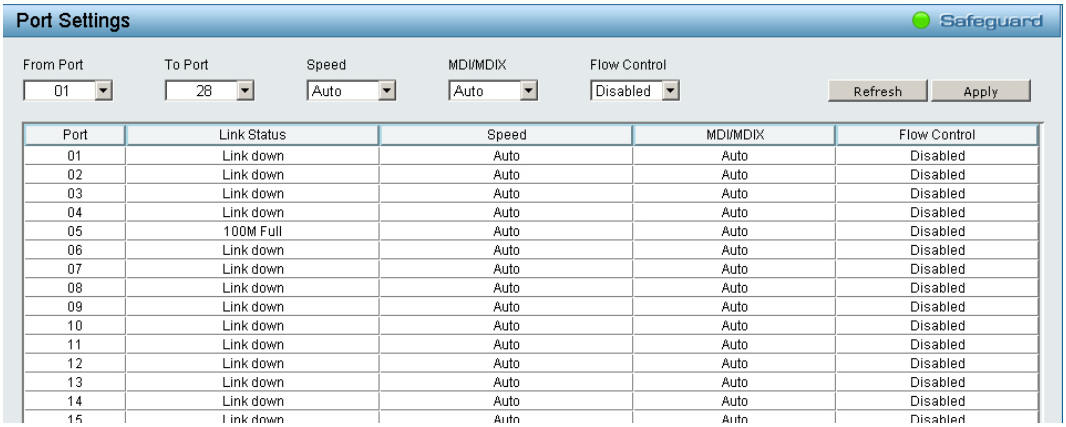


図 5-29　Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
Speed	ポートスピードを指定します。 選択肢：「1000M Full」、「100M Full」、「100M Half」、「10M Full」、「10M Half」、「Auto」、「Disable」 初期値：「Auto」 注意 接続ケーブルのメディアタイプを変更した場合、適切なポート速度の設定を行ってください。 注意 100M 光ファイバ接続では「100 M Full」、「100 M Half」または「Disable」を指定します。

項目	説明
MDI/MDIX	MDI/MDIX 機能の設定を選択します。 選択肢：「Auto」「MDI」「MDIX」 初期値：「Auto」 • MDIX 通常の接続の場合に選択します。 • MDI スイッチがクロスケーブルを使用せずに他のスイッチやハブに接続する場合に選択します。 • Auto ポートや接続の状態に合わせて、自動的に「MDI」または「MDIX」を選択します。
Flow Control	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、Half-Duplex ではバックプレッシャーによる制御を行います。 選択肢：「Enabled」「Disabled」 初期値：「Disabled」

3. 「Apply」をクリックし、設定を有効にします。

表示を最新の状態にするには、「Refresh」をクリックします。

Port Description（ポート概要）

各ポート概要の設定を行います。

1. 「System」>「Port Description」の順にメニューをクリックします。

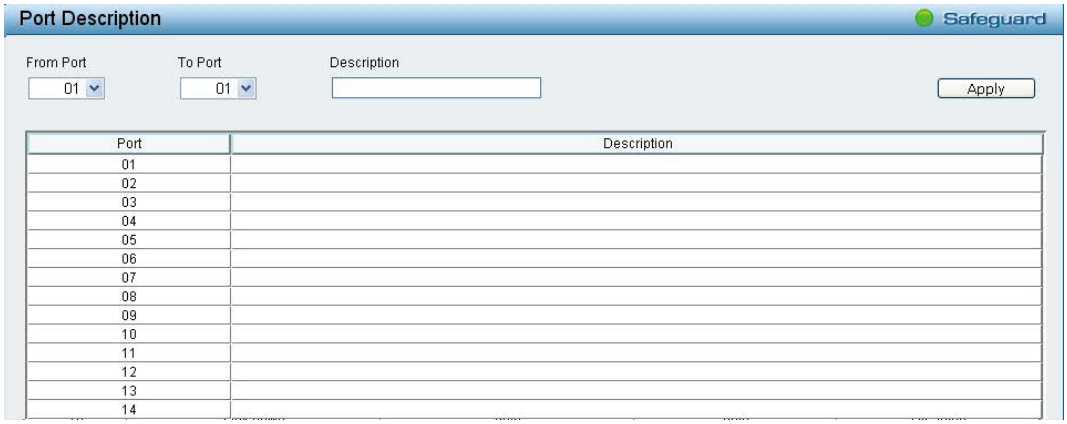


図 5-30　Port Description 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
Description	指定したポートの概要を入力します。

3. 「Apply」をクリックし、設定を有効にします。

DHCP Auto Configuration（DHCP 自動設定）

DHCP 自動設定機能を有効 / 無効にします。

有効にした場合、スイッチは起動時に自動で TFTP サーバからコンフィグレーションファイルを取得します。
スイッチが TFTP サーバからコンフィグレーションファイルを取得できない場合は、スイッチのフラッシュメモリに保存された最新のコンフィグレーションファイルが読み込まれます。

1. 「System」>「DHCP Auto Configuration」の順にメニューをクリックします。

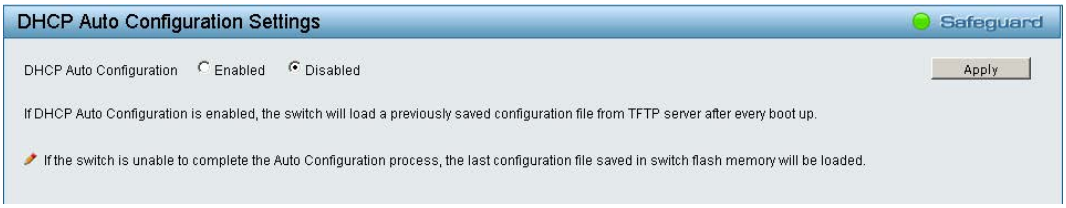


図 5-31　DHCP Auto Configuration Settings 画面

2. 「Enable」(有効) または「Disabled」（無効）を選択します。

3. 「Apply」をクリックし、設定を有効にします。

DHCP Relay（DHCP リレー設定）

DHCP リレーの設定を行います。「System」>「DHCP Relay」をクリックし、フォルダから設定項目を選択します。

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

DHCP リレーのグローバル設定を行います。

1. 「System」>「DHCP Relay」>「DHCP Relay Global Settings」の順にメニューをクリックします。

図 5-32　DHCP Relay Global Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
DHCP Relay State	プルダウンメニューから「Enabled」または「Disabled」を選択し、スイッチ上で DHCP リレーを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
DHCP Relay Hops Count Limit (1-16)	DHCP メッセージが中継されるルータホップの最大数（1-16）を設定します。初期値は 4 です。
DHCP Relay Time Threshold (0-65535)	DHCP パケットのルーティングを行うタイムリミットを設定します。0 が指定されると、スイッチは DHCP パケットの「Seconds」内の値のプロセスを行いません。0 以外の値を指定すると、スイッチはその値を使用し、ホップカウントと併用しながら DHCP パケットの送出を決定します。初期値は 0 です。

項目	説明
DHCP Relay Agent Information Option 82 State	DHCP Agent Information Option 82 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。 • Enabled - リレーエージェントは DHCP サーバとクライアント間で交わすメッセージに DHCP Relay Information（「Option 82」欄）を挿入 / 削除します。リレーエージェントが DHCP リクエストを受信すると、Option 82 情報と（設定があれば）リレーエージェントの IP アドレスをパケットに付加します。Option 82 情報が付加されたパケットは DHCP サーバに送信されます。Option 82 をサポートする DHCP サーバがパケットを受信すると、そのサーバは remote ID、circuit ID、またはそれらの両方を使用して IP アドレスを割り当て、単一の remote ID または circuit ID に割り当て可能な IP アドレス制限などのポリシーを適用できます。それから、DHCP サーバは「Option-82」欄の値を DHCP reply の中にそのまま残します。DHCP サーバはスイッチが DHCP request を中継していた場合には、ユニキャストで reply を返します。スイッチは remote ID や circuit ID 欄を調べて、本来の Option-82 情報が insert されていたかを確認します。スイッチは「Option-82」欄を削除してからそのパケットを DHCP クライアントに接続されているスイッチポートに転送します。 • Disabled - リレーエージェントは DHCP サーバとクライアント間で交換するメッセージへの DHCP Relay Information（「Option 82」欄）の挿入 / 削除を行いません。また、以下の Option 82 のチェックとポリシーの項目は無効になります。
DHCP Relay Agent Information Option 82 Check	スイッチのパケットの Option 82 項目の妥当性のチェックを行う機能を「Enabled」（有効）/「Disabled」（無効）にします。 • Enabled - リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行います。スイッチが DHCP クライアントから Option 82 項目を含むパケットを受信すると、スイッチはこれらのパケットは不正だとしてパケットを廃棄します。リレーエージェントは DHCP サーバから受信したパケットから不正なメッセージを削除します。 • Disabled - リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行いません。
DHCP Relay Agent Information Option 82 Policy	プルダウンメニューから「Replace」、「Drop」または「Keep」を選択します。初期値は「Replace」です。 • Replace - DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。 • Drop - DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。 • Keep - DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。
DHCP Relay Agent Information Option 82 Remote ID	「Default」または手動でリモート ID を設定できます。

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。

3. 「Apply」をクリックし、設定を有効にします。

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

DHCP 情報をスイッチにリレーするために、DHCP サーバの登録を行います。以下の画面から、DHCP サーバに直接接続する既存の IP インタフェースを設定します。正しく入力を行い「Apply」ボタンをクリックすると、以下の画面の下部に位置する「DHCP Relay Interface Table」にリスト表示されます。スイッチの 1 つの IP インタフェースに対して 4 件までのサーバ IP アドレスを登録できます。

1. 「System」>「DHCP Relay」>「DHCP Relay Interface Settings」の順にメニューをクリックします。

図 5-33　DHCP Relay Interface Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

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

3. 「Apply」をクリックし、設定を有効にします。

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

DHCP ローカルリレーの設定を行います。
DHCP ブロードキャストはスイッチ CPU にトラップされ、代わりのブロードキャストが Option82 とともに転送されるようになります。
DHCP サーバからの代替はスイッチ CPU にトラップされ Option82 も除去されて DHCP クライアントに返信されます。

1. 「System」>「DHCP Local Relay Settings」の順にメニューをクリックします。

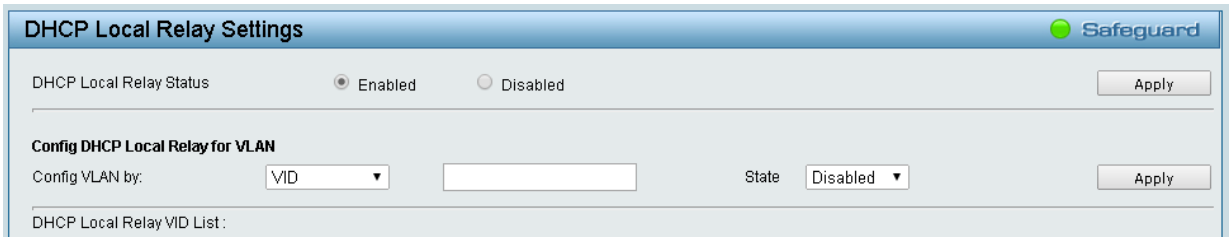


図 5-34　DHCP Local Relay Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
DHCP Local Relay Status	ローカルリレーのグローバルステート機能を「Enable」(有効) または「Disable」(無効) にします。 初期値は「Disabled」です。 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。
Config VLAN by	ユーザが DHCP ローカルリレーに適用する VLAN または VID をドロップダウンメニューから選択し、入力します。
State	DHCP ローカルリレー設定を「Enable」(有効) または「Disable」(無効) にします。設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
DHCP Local Relay VID List	DHCP ローカルリレーが設定された VLAN のリストを表示します。

3. 「Apply」をクリックし、設定を有効にします。

DHCPv6 Relay Settings（DHCPv6 リレー設定）

スイッチの DHCPv6 リレー機能を設定します。

1. 「System」>「DHCPv6 Relay Settings」の順にメニューをクリックします。

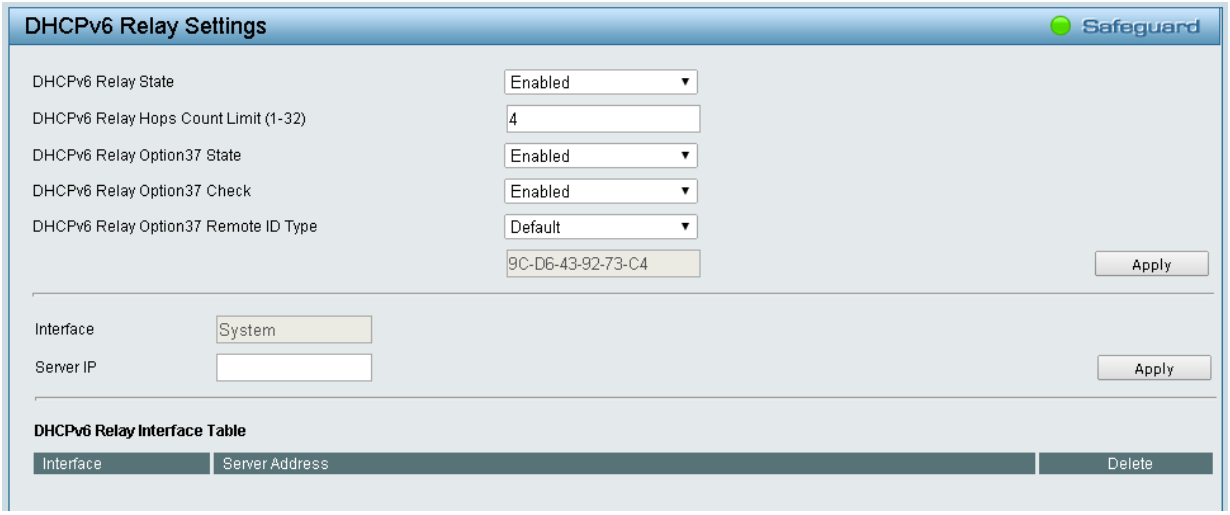


図 5-35　DHCPv6 Relay Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
DHCPv6 Relay State	DHCPv6 リレー機能を「Enabled」(有効)/「Disabled」(無効) にします。
DHCPv6 Relay Hops Count Limit (1-32)	DHCPv6 メッセージが転送されるルータホップの最大数（1-32）を定義します。初期値は 4 です。
DHCPv6 Relay Option37 State	「DHCPv6 Relay Option37 State」を有効 / 無効にします。
DHCPv6 Relay Option37 Check	「DHCPv6 Relay Option37 Check」を有効 / 無効にします。
DHCPv6 Relay Option37 Remote ID Type	リモート ID のタイプを指定します。 タイプには「Default」「CID With User Defined」「User Defined」があります。
Interface	インタフェース名を入力します。
Server IP	サーバの IP アドレスを入力します。

3. 「Apply」をクリックし、設定を有効にします。

SysLog Host（SysLog Host 設定）

SysLog Host 設定を有効にすると、システムログサーバを使用して指定したホストに Syslog メッセージを送信します。
システムログは、情報メッセージやエラー報告など、発生するイベントの管理・記録を行います。
「Severity」でイベントの重大性を設定することにより、メッセージを送信する対象のイベントが決まります。

1. 「System」>「Syslog Host」の順にメニューをクリックします。

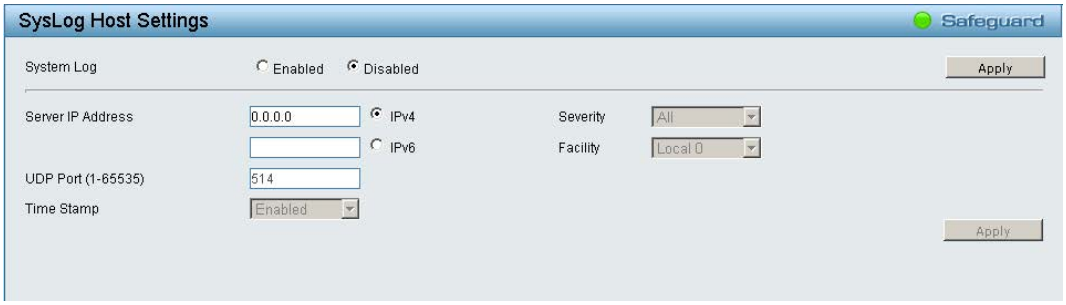


図 5-36　SysLog Host Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
System Log	システムログの出力を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
Server IP Address	IPv4 または IPv6 を選択し、システムログサーバの IP アドレスを入力します。
UDP Port (1-65535)	ログが送信される UDP ポートを指定します。 設定可能範囲 : 1-65535 初期値：514
Time Stamp	「Enabled」を選択すると、ログメッセージに時刻情報を設定します。
Severity	サーバに対して警告メッセージ送信が必要なイベントの重要性を設定します。 重要レベルは 3 種類あります。ひとつの重要性を選択すると、選択した重要性以下のレベルは全て選択されたことになります。 • Warning 最も低いレベルの警告です。デバイスは機能していますが、操作上の問題が発生しています。 • Informational デバイス情報を提供します。 • All 全てのレベルのシステムログが表示されます。
Facility	システム ログがリモート サーバに送信されるファシリティ値を選択します。 サーバに割り当てられるファシリティ値は 1 つのみです。 設定可能範囲 : Local 0 ～ Local 7

3. 「Apply」をクリックし、設定を有効にします。

Time Profile（タイムプロファイル設定）

デバイスのタイムプロファイルを設定します。

1. 「System」>「Time Profile」の順にメニューをクリックします。

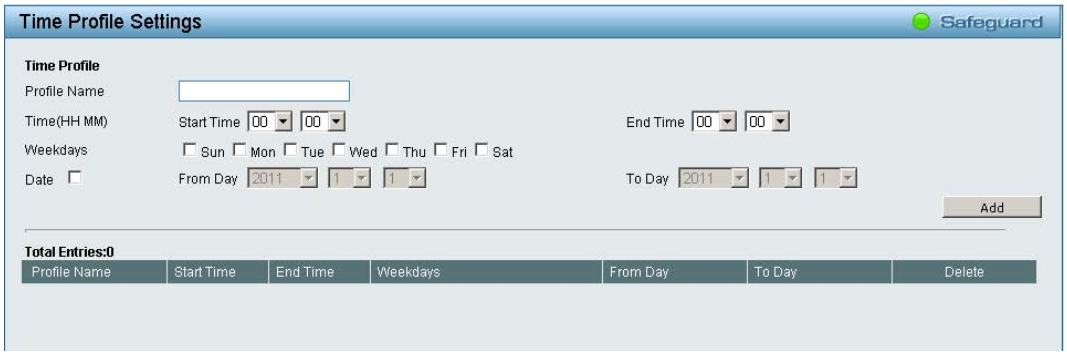


図 5-37　Time Profile Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Profile Name	プロファイル名を指定します。
Time(HH MM)	開始時刻と終了時間を指定します。 「Start Time」および「End Time」のプルダウンメニューから時間範囲を選択します。
Weekdays	稼働日を指定します。 チェックボックスを使用して、タイムプロファイルを使用する曜日をチェックします。
Date	プロファイルを使用する日付を選択します。 「From Day」および「To Day」プルダウンメニューから指定する期間を選択します。

3. 「Add」をクリックして、タイムプロファイルを追加します。

作成したプロファイルを削除するには、「Delete」をクリックします。

Power Saving（省電力設定）

省電力機能を使用すると、RJ-45 ポートがリンクダウンしている場合や、接続しているデバイスの電源が入っていない場合に、自動的に電力の消費量を削減することができます。

消費電力を削減すると、発熱量が少なくなります。

1. 「System」>「Power Saving」の順にメニューをクリックします。

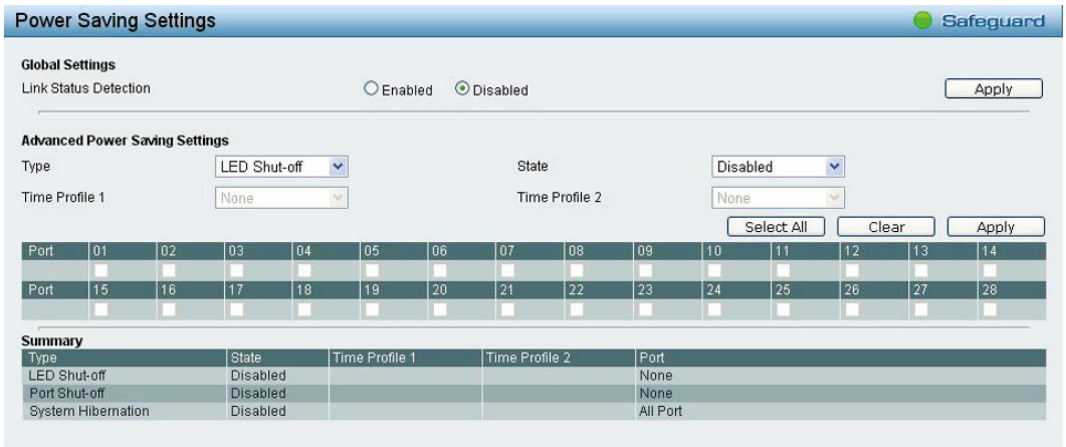


図 5-38　Power Saving Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Global Settings	
Link Status Detection	リンクの状態を検知する機能を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Enabled」
Advanced Power Saving Settings	
Type	省電力タイプを指定します。 選択肢：「LED Shut-off」「Port Shut-off」「Port Standby」「System Hibernation」 • LED Shut-off 優先度：高 「LED Shut-off」が「Disabled」になっている場合、プロファイル機能は適用されません。 • Port Shut-off 優先度：高 「Port Shut-off」が「Disabled」になっている場合、プロファイル機能は適用されません。 • System Hibernation メインチップセット（MAC と PHY の両方）がすべてのポートで無効となり、CPU を動作させるのに必要とされるエネルギーを最小の状態にします。
State	省電力機能を「Enabled」（有効）または「Disabled」（無効）にします。
Time Profile 1	タイムプロファイルまたは「None」を選択します。
Time Profile 2	タイムプロファイルまたは「None」を選択します。
Port	省電力設定を行うポートにチェックをいれます。 「Select All」をクリックするとすべてのポートが選択されます。 「Clear」をクリックすると選択が解除されます。

3. 「Apply」をクリックし、設定を有効にします。

IEEE802.3az EEE Settings（IEEE 802.3az EEE 設定）

IEEE 802.3az EEE は、省電力技術の規格です。ネットワークの使用率が低い場合に、機器を省電力状態に移行させ、電力消費を抑えます。その際、ネットワークの接続状態に影響を与えることはありません。送信側 / 受信側ともに IEEE 802.3az EEE に準拠している必要があります。

1. 「System」>「IEEE802.3az EEE Settings」の順にメニューをクリックします。

図 5-39　IEEE802.3az EEE settings 画面

2. 「From Port」「To Port」で、設定を行うポートを指定します。
3. 「State」で「Enabled」(有効) または「Disabled」(無効) を選択します。
4. 「Apply」をクリックし、設定を適用します。

補足　接続スピードが 1000M から 100M に落ちた場合、または最初のリンクアップまでに長い時間がかかるようになった場合は、以下の手順を実行後、再度状況を確認してください。

1：　イーサネットアダプターまたはホスト PC 用の LAN コントローラのドライバをアップグレードしてください。

2：　スイッチのポートの EEE 機能を無効にしてください。

D-Link Discover Protocol Settings（D-Link Discover Protocol 設定）

D-Link Discovery Protocol (DDP) サポートしている機器に対し、本機器の DDP の有効 / 無効や DDP パケットリポートタイマの設定を行います。

1. 「System」>「D-Link Discover Protocol Settings」の順にメニューをクリックします。

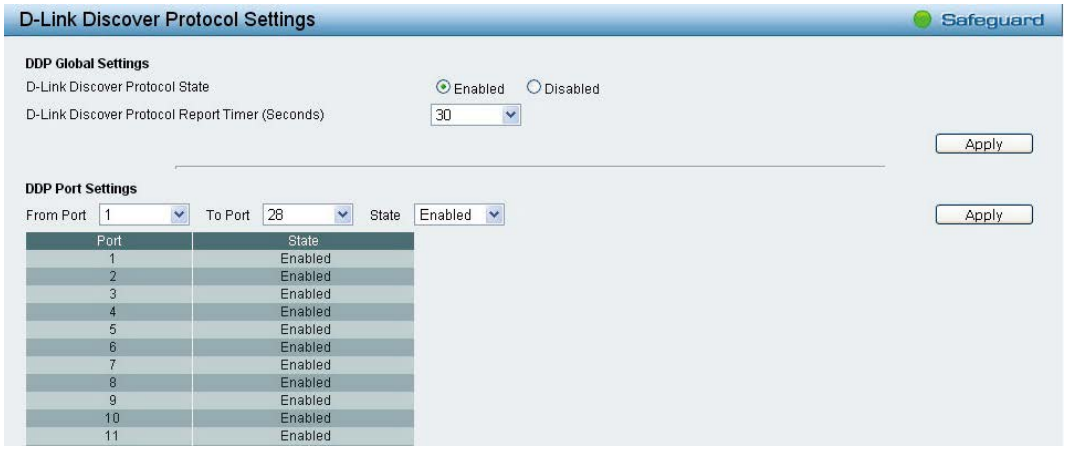


図 5-40　D-Link Discover Protocol Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
D-Link Discover Protocol State:	D-Link Discovery Protocol (DDP) の有効 / 無効を設定します。初期値：「Enabled」
D-Link Discover Protocol Report Timer (Seconds)	D-Link Discovery Protocol (DDP) のリポートタイマの設定を行います。 「30」「60」「90」「120」（秒）または「Never」から選択します。

3. 「Apply」をクリックし、設定を有効にします。

VLAN（VLAN 設定）

■ VLAN(VLAN 設定) の設定項目

802.1Q VLAN（802.1Q VLAN 設定）

VLAN とは、ポートをグループ化したものです。VLAN 内では実際のネットワーク内での場所にかかわらず、同じエリア内に位置しているかのような通信ができます。

VLAN は、部署別（開発研究（R&D）またはマーケティングなど）、使用用途別（E-mail など）、あるいはマルチキャストグループ別（ビデオ会議などのマルチメディアアプリケーション）などの単位で簡単に編成することができます。VLAN の再編成を行う際にも、ユーザは物理的な接続を変更せずに新しい VLAN に参加することができるため、ネットワーク管理の簡素化が実現できます。
「IEEE 802.1Q VLAN」の設定画面では VID 管理機能を設定することが可能です。初期設定では VID は「1」、初期名はなし、すべてのポートは “Untagged” に指定されています。

1. 「VLAN」>「802.1Q VLAN」の順にメニューをクリックします。

図 5-41　802.1Q VLAN Settings 画面

■ 画面に表示される項目

項目	説明
Asymmetric VLAN	「Asymmetric VLAN」を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」(無効)
Delete	VLAN グループを削除します。
Add	新しい VID グループを作成します。

VLAN を有効 / 無効にする場合：

1. 「Asymmetric VLAN」の「Enabled」（有効）または「Disabled」（無効）を選択します。

図 5-42　802.1Q VLAN Settings 画面

補足　「Example」をクリックすると、設定例が表示されます。

2. 「Apply」をクリックし、設定を有効にします。

新しい VID グループを作成する場合：

1. 「Add」をクリックします。

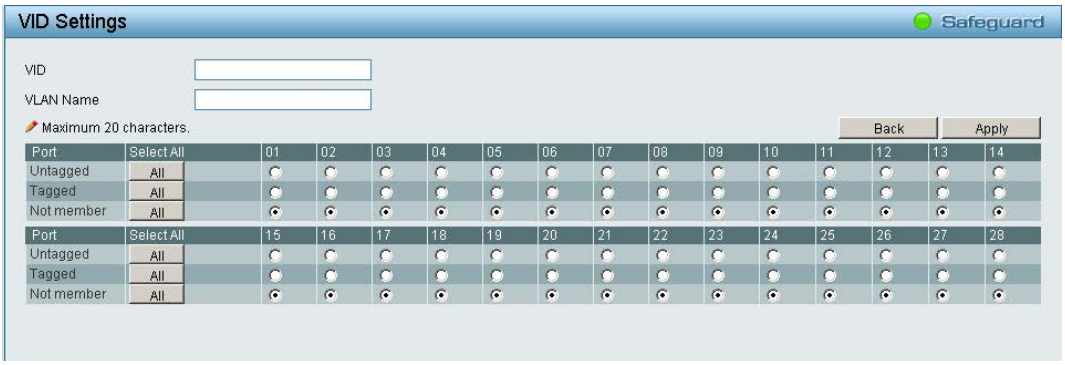


図 5-43　VID Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
VID	VLAN ID を設定します。
VLAN Name	VLAN 名を設定します。 VLAN 名は、Accounting、Marketing などのように、グループの特性に合わせて設定できます。
Port	各ポートを VLAN のメンバとして定義します。 • Untagged ポートを 802.1Q タグなしとして定義します。タグなしとするポートのボックスをチェックします。 • 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。 • 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」をクリックし、すべてのポートを選択します。

3. 「Apply」をクリックし、設定を有効にします。

補足　「Back」をクリックすると、802.1Q VLAN Settings 画面に戻ります。

VID グループを削除する場合：

1. 削除する VID グループの「Delete」をクリックします。

図 5-44　802.1Q VLAN Settings 画面

802.1Q VLAN PVID（802.1Q VLAN PVID 設定）

802.1Q VLAN PVID 設定では各ポートに PVID（Port VLAN ID）を設定します。

1. 「VLAN」>「802.1Q VLAN PVID」の順にメニューをクリックします。

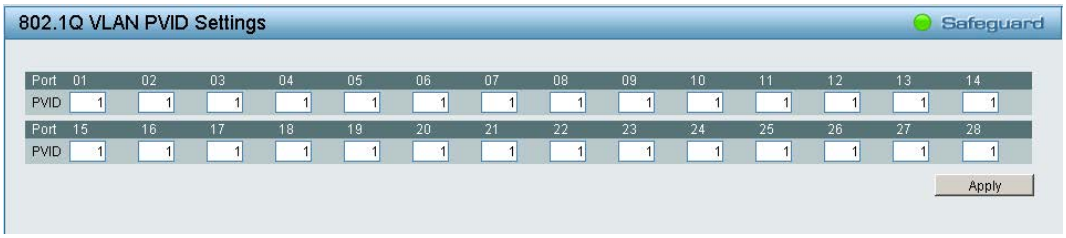


図 5-45　802.1Q VLAN PVID Settings 画面

2. 各ポートに「PVID」を設定します。

3. 「Apply」をクリックし、設定を有効にします。

802.1Q Management VLAN Configuration (802.1Q マネジメント VLAN 設定)

本設定を有効にした場合、スイッチの権限をデフォルトの VLAN からユーザが設定した VLAN に変更することができます。
これにより、ネットワーク全体をより柔軟に管理することができます。

1. 「VLAN」>「802.1Q Management VLAN Configuration」の順にメニューをクリックします。

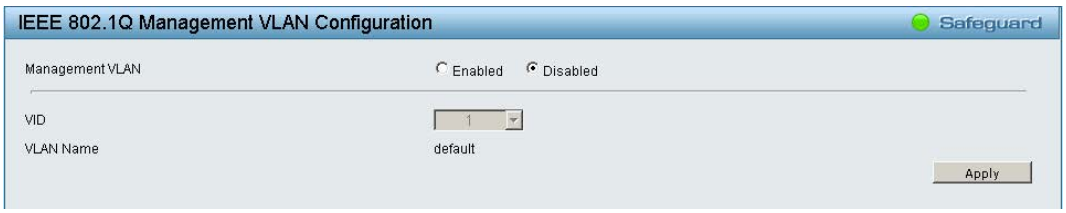


図 5-46　IEEE802.1Q Management VLAN Configuration 画面

2. 「Enabled」または「Disabled」を選択します。（初期値：「Disabled」）

3. 「Enabled」を選択した場合は、「VID」を指定します。

4. 「Apply」をクリックし、設定を有効にします。

Voice VLAN（音声 VLAN 設定）

音声 VLAN は、VoIP サービスを強化するために、IP 電話からの音声トラフィックに対し VLAN を自動的にアサインする機能です。
高い優先度と個別の VLAN を使用することで、VoIP トラフィックの品質とセキュリティを保証します。
VLAN タグを持つ VoIP パケットが来ると、音声 VLAN 機能はオリジナルの VLAN タグを置き換えません。

注意 Voice VLAN 機能は、他の機能（QoS を含む）より優先順位が高くなっています。そのため、音声トラフィックは QoS 機能には影響されずに Voice VLAN 機能設定に従って処理されます。

注意 VoIP トラフィックの品質を保証するためには、音声 VLAN に最も高い優先度を設定することをお勧めします。

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

1. 「VLAN」>「Voice VLAN」>「Voice VLAN Global Settings」の順にメニューをクリックします。

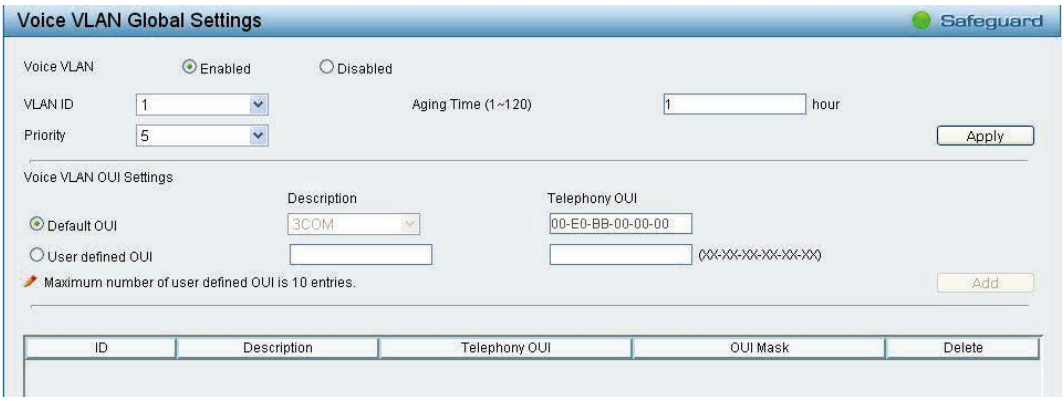


図 5-47　Voice VLAN Global Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Voice VLAN	音声 VLAN を「Enabled」（有効）または「Disabled」（無効）に設定します。 初期値 :「Disabled」(無効) **補足** 本設定を有効にすると「Voice VLAN Global Setting」の設定が可能になります。
VLAN ID	音声 VLAN の VLAN ID を選択します。 **補足** 事前に「802.1Q VLAN」画面にて VLAN を作成する必要があります。 「802.1Q VLAN」で設定されたメンバポートが、音声 VLAN のスタティックメンバポートになります。 自動的に音声 VLAN にポートを追加する場合、「Auto Detection」機能を有効にします
Priority	音声 VLAN における 音声 VLAN のトラフィックの 802.1p プライオリティレベルを設定します。 選択肢：「Highest」「High」「Medium」「Low」
Aging Time（1-120）	ポートが自動 VLAN の一部の場合、音声 VLAN からポートを削除するまでの時間を設定します。 初期値：1（時間） 選択可能範囲：1-120（時間） **補足** 後の音声機器がトラフィックを送信しなくなり、音声機器の MAC アドレスが期限切れになると、音声 VLAN タイマは開始されます。ポートは音声 VLAN タイマの時間切れの後、音声 VLAN から削除されます。
Voice VLAN OUI Settings	
Default OUI	既存の OUI 値を選択します。 選択肢：「3COM」「Cisco」「Veritel」「Pingtel」「Siemens」「NEC/Philips」「Huawei3COM」「Avaya」
User defined OUI	手動でテレフォニー OUI の定義を作成します。 **補足** 作成可能な OUI の数は 10 です。 手動で設定された OUI が選択されている場合、ACL ルールが 1 つ使用され、設定するともう 1 つ ACL ルールが使用されます。システムは ACL プロファイル（ Profile ID:51）を全ての音声 VLAN ルールのために生成します。 **注意** OUI 設定を行う際の注意事項については、OUI 設定についてを参照してください。

OUI 設定について

いくつかの定義済みの OUI があり、ユーザが新たに OUI を設定する場合は、これらの定義済み OUI を避ける必要があります。
以下は、定義済みの音声トラフィックの OUI です。

OUI	支給元	簡略名
00:E0:BB	3COM	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

3. 「Voice VLAN」の設定を行った場合、「Apply」をクリックして設定を有効にします。
「Voice VLAN OUI Settings」の設定を行った場合、「 Add」をクリックして設定内容を保存します。

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

ポートの音声 VLAN 情報を設定および表示します。
IP 電話からの音声トラフィックを、アサインした VLAN へ自動的に配置し、VoIP のサービスを向上させることができます。
優先度が高いこと、また個別の VLAN を使用することで、VoIP トラフィックの品質とセキュリティを保証します。

1. 「VLAN」>「Voice VLAN」>「Voice VLAN Port Settings」の順にメニューをクリックします。

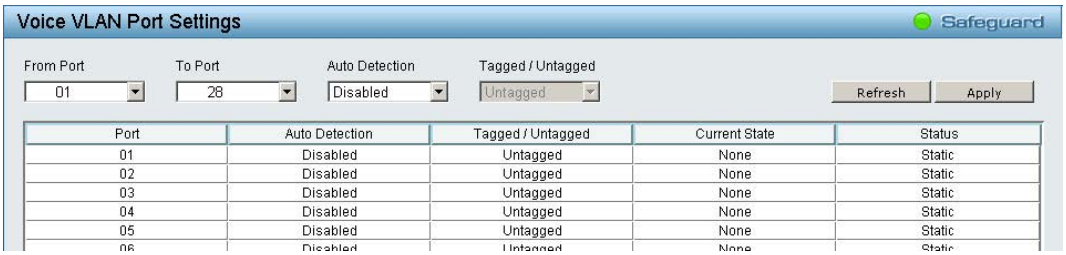


図 5-48　Voice VLAN Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port / To Port	設定対象のポート範囲を指定します。
Auto Detection	OUI 自動検出機能を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」 補足　デバイス OUI が「Voice VLAN OUI Setting」画面で設定した「Telephony OUI」に一致することを検出すると、スイッチは自動的に音声 VLAN にポートを追加します。
Tagged / Untagged	「Tagged」（ポートにタグ付けをする）または「Untagged」（ポートからタグを削除する）を選択します。

3. 「Apply」をクリックし、設定を有効にします。

補足　「Refresh」をクリックすると、表示を最新のものに更新できます。

Voice Device List（音声 VLAN のポート設定）

ポートに接続する音声デバイスに関する情報を表示します。

1. 「VLAN」>「Voice VLAN」>「Voice Device List」の順にメニューをクリックします。

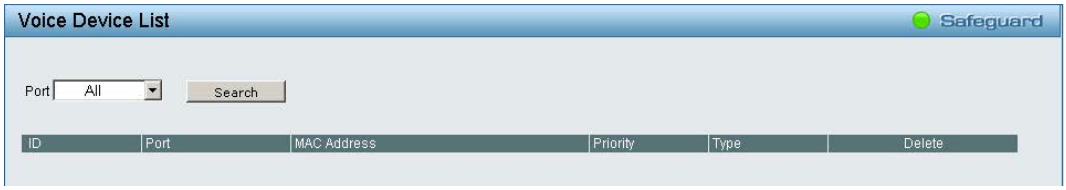


図 5-49　Voice Device List 画面

2. 「Port」で音声デバイスを表示するポートを指定します。

3. 「Search」をクリックします。

   テーブルに音声デバイスの情報が表示されます。

Auto Surveillance VLAN（自動サーベイランス VLAN）

自動サーベイランス VLAN は、IP サーベイランスサービスを強化するための機能です。音声 VLAN と同様、D-Link IP カメラからのビデオトラフィックに対して自動的に VLAN をアサインします。優先度が高いこと、また個別の VLAN を使用することで、サーベイトラフィックの品質とセキュリティを保証します。

自動サーベイ VLAN 機能は、入力パケットのソース MAC アドレス /VLAN ID をチェックします。特定の MAC アドレス /VLAN ID に一致すると、パケットはユーザが設定した優先度でスイッチを通過します。

1. 「VLAN」>「Auto Surveillance VLAN」の順にメニューをクリックします。

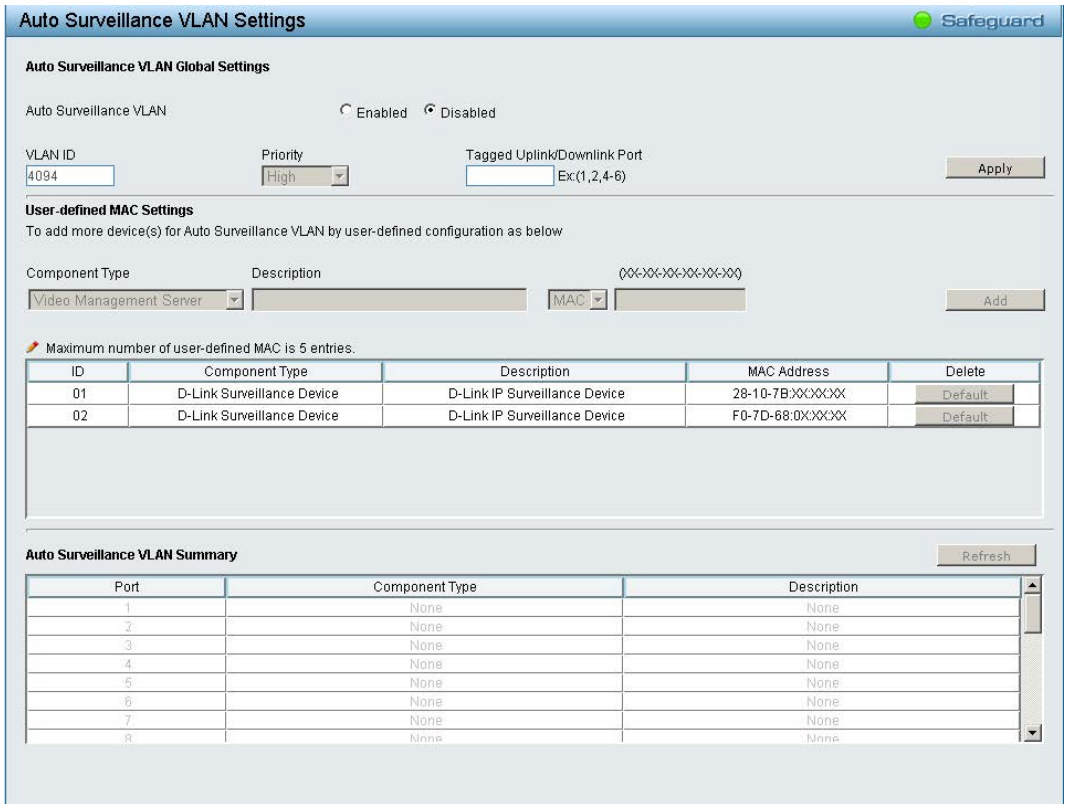


図 5-50　Auto Surveillance VLAN 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Auto Surveillance VLAN Global Settings	
Auto Surveillance VLAN	本機能を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
VLAN ID	自動サーベイ VLAN を作成します。 初期値：4094 補足 「802.1Q VLAN」画面にて作成済みの VLAN ID を選択することで別の自動サーベイ VLAN を作成することもできます。 「802.1Q VLAN」で設定されたメンバポートが、自動サーベイランス VLAN のスタティックメンバポートになります。
Priority	自動サーベイ VLAN の優先度を指定します。 初期値：「High」 選択肢：「Highest」「High」「Medium 」「Low」
Tagged Uplink/ Downlink Port	自動サーベイ VLAN に対してタグ付けされた、アップリンクポートまたはダウンリンクポートを指定します。
User-defined MAC Settings	
Component Type	コンポーネントタイプを選択します。 選択肢： 「Video Management Server 」「VMS Client/Remote viewer」「Video Encoder」「Network Storage」「Other IP Surveillance Devices」 補足 初期値では、自動サーベイ VLAN は自動的に D-Link サーベイデバイスを検出します。
Description	コンポーネントタイプに説明文を指定します。
MAC/OUI	サーベイコンポーネントの MAC または OUI アドレスを手動で作成します。 補足 作成可能な MAC アドレス数は 5 です。 システムは ACL プロファイル (Profile ID:56) を全ての自動サーベイ VLAN ルールのために自動的に生成します

自動サーベイ VLAN グローバル設定を行う場合

1. 「Auto Surveillance VLAN Global Settings」セクションを指定します。
2. 「Apply」をクリックして、自動サーベイ VLAN グローバル設定の変更を適用します。

サーベイコンポーネントの作成を行う場合

1. 「User-defined MAC Settings」セクションを指定します。
2. 「Add」をクリックして、新しいサーベイコンポーネントを作成します。
3. 「Refresh」をクリックして、自動サーベイ VLAN サマリテーブルを更新します。

サーベイコンポーネントの削除を行う場合

1. 削除するエントリの「Delete」をクリックします。

補足 「Refresh」をクリックすると、「Auto Surveillance VLAN Summary」の表示内容を更新できます。

L2 Functions（L2 機能の設定）

■ L2 Functions (L2 機能の設定) の設定項目

Jumbo Frame (ジャンボフレーム)

本スイッチはジャンボフレームをサポートしています。
ジャンボフレームとは、1536 bytes のイーサネットフレームよりも大きいサイズのフレームです。最大サイズは 9,216 bytes（タグ付き）になります。

1. 「L2 Functions」>「Jumbo Frame」の順にメニューをクリックします。

図 5-51　Jumbo Frame Settings 画面

2. 「Enabled」(有効) または「Disabled」(無効) を選択します。（初期値：「Disabled」）

3. 「Apply」をクリックし、設定を有効にします。

Port Mirroring（ポートミラーリング）

ポートミラーリングとは、スイッチのあるポートに入出力するパケットのコピーを他のポートに送信して、そこでパケットを監視することにより、ネットワークトラフィックのモニタリングを行う方法です。
本機能により、ネットワーク管理者は効率よくネットワークパフォーマンスを監視できるようになります。

1. 「L2 Functions」>「Port Mirroring」の順にメニューをクリックします。

図 5-52　Port Mirroring Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Port Mirroring	ポートミラーリング機能を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
Target Port	ターゲットポートを選択します。
TX	ソースポートが送信したデータをコピーしてターゲットポートに送信します。 「All」をクリックすると、すべてのポートが選択されます。（送信）
RX	ソースポートが受信したデータをコピーしてターゲットポートに送信します。 「All」をクリックすると、すべてのポートが選択されます。（受信）
TX / RX	ソースポートが送受信したデータをターゲットポートに送信します。 「All」をクリックすると、すべてのポートが選択されます。（送受信）
None	ポートミラーリングを行いません。 「All」をクリックすると、すべてのポートが選択されます。

3. 「Apply」をクリックし、設定を有効にします。

Loopback Detection（ループバック検知）

ループバック検知機能は、ネットワークでスパニングツリー（STP）が無効な場合に、『ハブやアンマネージドスイッチ等の特定ポートにより生成されるループ』や、『自筐体内のポート間ループ』を検出するために使用されます。
本機能は、スイッチのポートを自動的にシャットダウンし、管理者にログを送信します。ループバック検知の「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開放されます。ループバック検知機能は、設定したポート範囲に対して同時に実行されます。

1. 「L2 Functions」>「Loopback Detection」の順にメニューをクリックします。

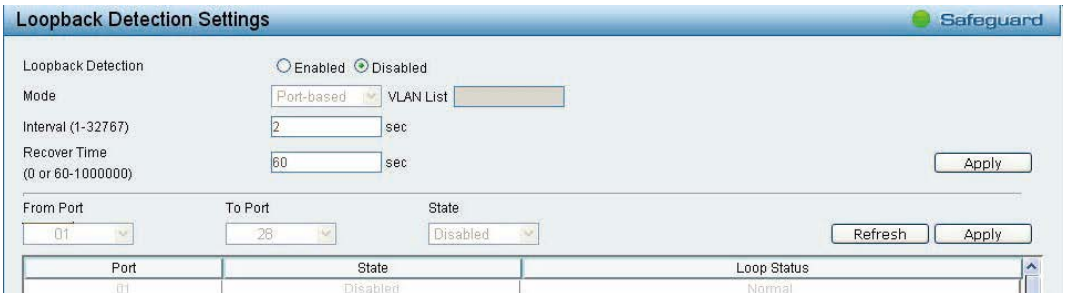


図 5-53　Loopback Detection Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Loopback Detection	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：「Disabled」
Mode	モードを「Port-based」または「VLAN-based」から選択します。「Port-based」を選択するとループが発生しているポートがシャットダウンされ、すべてのメンバ VLAN に影響が及びます。「VLAN-based」を選択するとループが発生してる VLAN のメンバポートのみシャットダウンされます。 初期値：「Port-based」
VLAN List	VLAN のリスト（VID）を指定します。
Interval (1-32767)	ループ検知間隔を設定します。 初期値：2（秒） 選択可能範囲：1-32767（秒）
Recover Time (0 or 60-1000000)	ループバックが検知された場合にリカバリする時間（秒）を指定します。 初期値：60 秒 選択可能範囲：0 または 60-1000000（秒） 補足　0 を指定すると、Recover Time は無効になります。
From Port/To Port	設定対象のポート範囲を指定します。
State	「Enabled」（有効）または「Disabled」（無効）を指定します。

3. 「Apply」をクリックし、設定を有効にします。

MAC Address Table（MAC アドレステーブル）

Static MAC Settings（スタティック MAC 設定）

本設定では二つに分かれた機能の設定を行います。「MAC Address Learning」テーブルではポートがアップリンクポートとして設定し荒れていない場合（DHCP サーバやゲートウェイなどへの接続）に、MAC アドレスの自動取得の無効を設定します。初期値では本設定は無効です。

1. 「L2 Functions」>「MAC Address Table」>「Static MAC Settings」の順にメニューをクリックします。

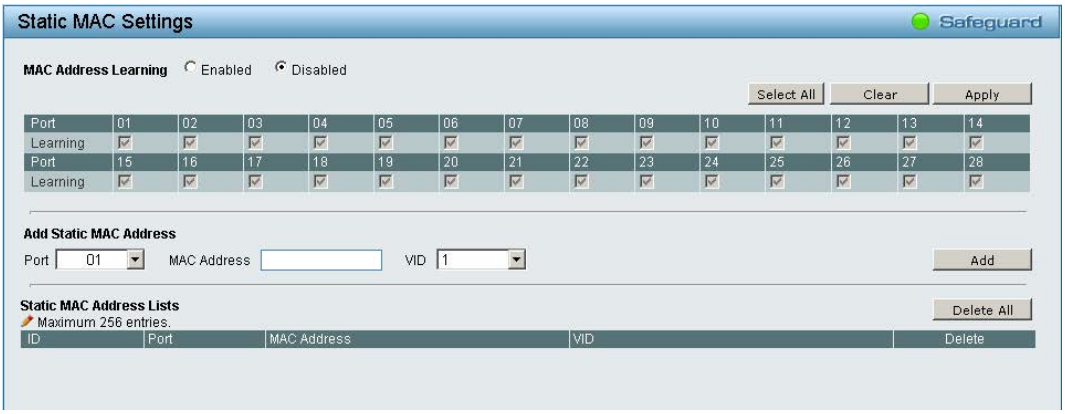


図 5-54　Static MAC Settings 画面

2. 設定する内容に応じて、以下から操作を選択します。

MAC Address Learning の設定を行う場合

1. 「MAC Address Learning」を「Enabled」(有効) または「Disabled」(無効) にします。
2. 「Enabled」(有効) にした場合、適用するポートを選択します。
   ※「Select All」をクリックすると、すべてのポートが選択されます。
   ※「Clear」をクリックすると、ポートの選択を解除できます。
3. 「Apply」をクリックします。

スタティック MAC アドレスの追加を行う場合

1. 「User-defined MAC Settings」で割り当てるポートを選択します。
2. 「MAC Address」に MAC アドレスを入力します。
3. 「VID」を選択します。
4. 「Add」をクリックします。

スタティック MAC アドレスの削除を行う場合

1. 「Static MAC Address Lists」で、削除するアドレスの「Delete」をクリックします。

補足　MAC アドレスの自動学習機能を無効にし、スタティック MAC アドレスを指定することによって、スイッチは不正な MAC アドレスからのトラフィックを転送しなくなり、ネットワークはハッカーなどの潜在的な脅威から保護されます。

Dynamic Forwarding Table（ダイナミックフォワーディングテーブル）

スイッチが学習した MAC アドレスを各ポートごとに表示します。

1. 「L2 Functions」>「MAC Address Table」>「Dynamic Forwarding Table」の順にメニューをクリックします。

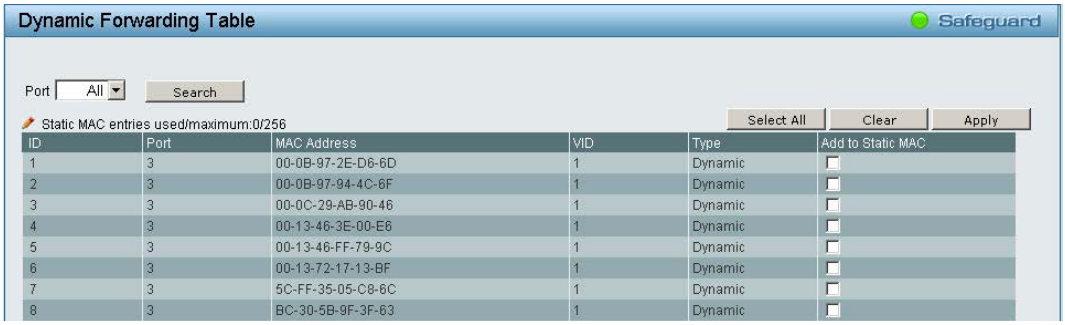


図 5-55　Dynamic Forwarding Table 画面

2. 設定する内容に応じて、以下から操作を選択します。

ポートに学習された MAC アドレスの検索を行う場合

1. 「Port」で検索するポートを選択します。
2. 「Search」をクリックします。

スタティック MAC アドレスリストへ MAC アドレスの追加を行う場合

1. 追加を行うアドレスの「Add to Static MAC」にチェックをいれます。
   ※「Select All」をクリックすると、すべてのポートが選択されます。
   ※「Clear」をクリックすると、ポートの選択を解除できます。
2. 「Apply」をクリックします。

補足　ダイナミックフォワーディングテーブルが複数ページにわたっている場合は、画面右下の「Page」「Back」「Next」でページを選択します。

Spanning Tree（スパニングツリー設定）

本スイッチは 2 つのバージョンのスパニングツリーを搭載しています。
1 つは 802.1W「Rapid Spanning Tree Protocol」（RSTP）、もう 1 つは 802.1D「Spanning Tree Protocol」（STP）です。
RSTP は 802.1D STP 対応のレガシー機器にも対応可能ですが、この場合 RSTP の利点は失われます。

IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) は、802.1D STP を改善したものです。 RSTP は最近のスイッチ技術の最新機能を妨げる STP の制限事項を克服するために開発されました。基本的な機能と用語は STP と同様で、STP 用の設定の大部分は RSTP にも使用できます。本項目ではいくつかの新しいスパニングツリーのコンセプトと、この二つのプロトコルについての違いを説明します。

初期値では RSTP は無効です。有効にすると、スイッチは BPDU パケットとそれに付随する Hello パケットをリッスンします。BPDU パケットは受信しない相手にも送信されます。それによりブリッジ間の各リンクはリンクの状態を感知します。最終的にはこの違いにより障害が発生したリンクの検出が速やかに行われ、迅速なトポロジの再構成へと繋がります。

STP Global Settings（スパニングツリーグローバル設定）

1. 「L2 Functions」>「Spanning Tree」>「STP Global Settings」の順にメニューをクリックします。

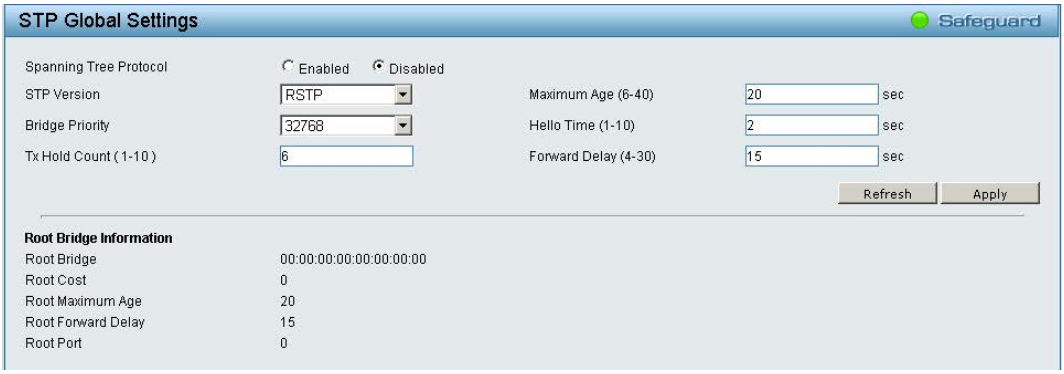


図 5-56　STP Global Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Spanning Tree Protocol	スパニングツリー機能を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
STP Version	「RSTP」または「STP」を選択します。 初期値：「RSTP」
Bridge Priority	パケット送信を行う優先度を設定します。値が小さいほど優先度は高くなります。 初期値：32768 設定可能範囲：0 - 61440
Tx Hold Count (1-10)	各送信間隔に送信される Hello パケット の最大数を設定します。 初期値：6 設定可能範囲：1 - 10
Maximum Age (6-40)	最大経過時間を設定します。 初期値：20 (秒) 設定可能範囲：6 - 40 (秒) 補足　最大経過時間は、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。 この値は、ルートブリッジにより設定され、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します。 本値が経過した時にルートブリッジからの BPDU パケットを受信していないと、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。
Hello Time (1-10)	ルートデバイスにより、スイッチが機能している旨を通知するために送信されるコンフィグレーションメッセージの送信間隔を指定します。 初期値：2 (秒) 設定可能範囲：1 - 10 (秒) 補足　「Maximum Age」の値は「Hello Time」の値より大きい必要があります。

項目	説明
Forward Delay (4-30)	ルートデバイスが状態を変更するまでの最大待ち時間を設定します。 初期値：15（秒） 設定可能範囲：4-30（秒）
Root Bridge Information	
Root Bridge	ルートブリッジの MAC アドレスを表示します。
Root Cost	ルートブリッジのコストを表示します。
Root Maximum Age	ルートブリッジの 最大経過時間を表示します。
Root Forward Delay	ルートブリッジの 状態を変更するまでの最大待ち時間 を表示します。
Root Port	ルートポートを表示します。

3. 「Apply」をクリックし、設定を有効にします。

STP Port Settings（スパニングツリーポート設定）

STP は、ポートごとに設定することができます。スイッチレベルでのスパニングツリー設定のほかに、ポートをグループ分けして、各ポートグループに対してスパニングツリーの設定を行うことも可能です。

STP グループのスパニングツリーは、スイッチレベルのスパニングツリーと同様の働きをしますが、ルートブリッジの概念はルートポートに置き換えられて考えることができます。グループ内のルートポートは、ポートプライオリティとポートコストに基づいて選出され、ネットワークとグループを接続する役割を果たします。スイッチレベルの場合と同様に、冗長リンクはブロックされます。

スイッチレベルの STP は、スイッチ間（または同様のネットワークデバイス）の冗長リンクをブロックし、ポートレベルの STP は STP グループ内の冗長リンクをブロックします。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。

1. 「L2 Functions」>「Spanning Tree」>「STP Port Settings」の順にメニューをクリックします。

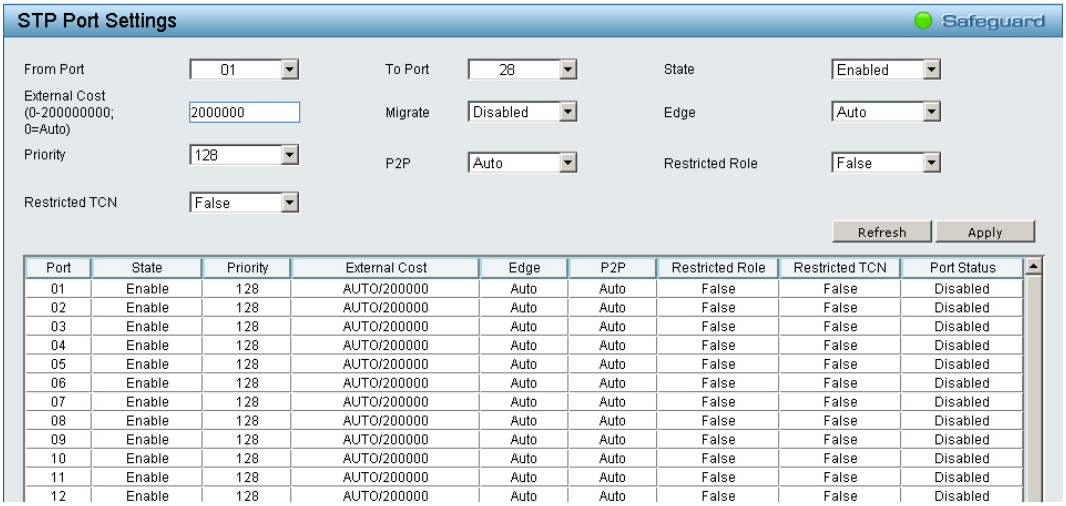


図 5-57　STP Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
State	ポートの STP を「Enabled」（有効）または「Disabled」（無効）に設定します。 初期値：「Enabled」

項目	説明
External Cost （1-2000000000; 0 = Auto）	設定対象のポートに対し、パケット送信のためのコストを表すメトリックを定義します。 ポートコストには、自動設定、または手動でメトリック値を指定できます。 初期値：　100Mbps ポートの場合：200000、ギガビットポートの場合：20000 **手動設定の場合：** • 1-200000000 の範囲から指定します。 小さい数字を指定すると、パケット送出ポートとして選出される確率が上がります。 **自動設定の場合：** • 0 を指定します。 指定したポートに対して、最適なパケット送信速度を自動的に設定します。
Migrate	「Enabled」（有効）または「Disabled」（無効）に設定します。 初期値：「Disabled」 補足　RSTP モードで動作中に、「Enabled」を選択すると、選択されたポートは RSTP BPDU を送信します。
Edge	エッジポートの設定を行います。 初期値：「Auto」 選択肢：「True」「False」「Auto」 • True 選択されたポートはエッジポートとして指定されます。 エッジポートはループを構成しませんが、トポロジの変更によってループ発生の可能性が生じると、エッジポートはエッジポートではなくなります。エッジポートは通常 BPDU パケットを受信しませんが、BPDU パケットを受信すると、そのポートはエッジポートではなくなります。 • False そのポートがエッジポートとして指定されていないことを示しています。 • Auto ポートが自動的にエッジポートステータスを持つかどうかを示します。
Priority	各ポートのプライオリティ（0-240）を指定します。 初期値：128 選択可能範囲：0-240 補足　指定した数字が小さいほど、ポートがルートポートとして選択される可能性が高くなります。
P2P	P2P ポートの設定を行います。 初期値：「Auto」 選択肢：「Force True」「Force False」「Auto」 • Force True 選択ポートは P2P ポートとして指定されます。 P2P ポートはエッジポートと似ていますが、P2P ポートは全二重モードでのみ稼動する点で異なります。RSTP の特長として、エッジポート同様、P2P ポートは迅速に Forwarding 状態に遷移します。 • Force False そのポートが P2P ポートとして指定されていないことを示しています。 • Auto ポートはいつでも可能な時に（「Force True」を指定した時と同様に）P2P ポートとして稼動します。P2P ポートではなくなる時（例 : 半二重モードを指定された時など）、自動的に「Force False」を指定した時と同様になります。
Restricted Role	「True」または「False」を選択します。 初期値：「False」 補足　「True」に設定した場合、ポートはルートポートとして識別されません。
Restricted TCN	「True」または「False」を選択します。 初期値：「False」 補足　Topology Change Notification (TCN) はブリッジがルートポートにトポロジの変更を送信する BPDU です。 「True」に設定すると、受信した TCN を他のポートへ伝搬することを停止します。

3. 「Apply」をクリックし、設定を有効にします。

Link Aggregation（リンクアグリゲーション設定）

Port Trunking（ポートトランキング設定）

トランキング機能を使用すると、複数のポートを束ねて帯域幅を増加させることができます。各トランキンググループは最大 8 個のポートから構成されます。
作成できるトランキンググループ数は以下のとおりです。

作成できるトランキンググループ数：
- DGS-1210-10P: 最大 5 グループ
- DGS-1210-20: 最大 10 グループ
- DGS-1210-28/28P : 最大 14 グループ
- DGS-1210-52 : 最大 26 グループ

1. 「L2 Functions」>「Link Aggregation」>「Port Trunking」の順にメニューをクリックします。

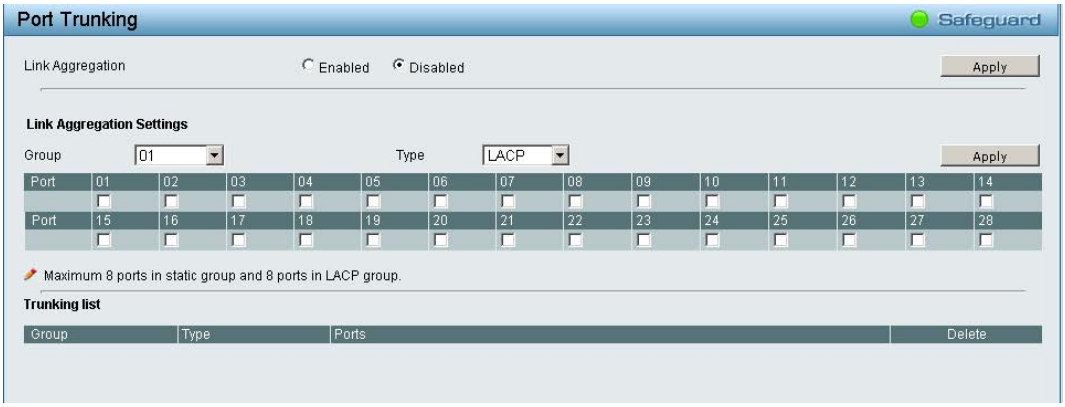


図 5-58　Port Trunking 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Link Aggregation State	本機能を「Enabled」（有効）/「Disabled」（無効）にします。 初期値：「Disabled」 補足　無効にすると、トランキンググループ内のすべてのメンバを削除します。
Group	トランキンググループの番号を選択します。
Port	グループ化するポートを選択します。 補足　グループ化できるポートは、1 グループあたり最大 8 個までです。
Type	トランキンググループの種類を設定します。 初期値：「LACP」 選択肢：「LACP」「Static」 • Static スタティックなリンクアグリゲーションです。手動でリンクアグリゲーションの設定をします。 • LACP LACP (Link Aggregation Control Protocol) をデバイスに有効とします。 LACP では、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。

注意　まとめられる各トランクポートは、同じ VLAN グループ内のデバイスに接続する必要があります。

3. 「Apply」をクリックし、設定を有効にします。

作成したトランキンググループを削除するには、「Trunking List」で削除したいグループの「Delete」をクリックします。

LACP Port Settings（LACP ポート設定）

LACP ポート設定は、スイッチのポートトランキンググループの作成に使用します。
LACP 制御フレームを送受信した際の、各ポートの動作を設定します。

1. 「L2 Functions」>「Link Aggregation」>「LACP Port Settings」の順にメニューをクリックします。

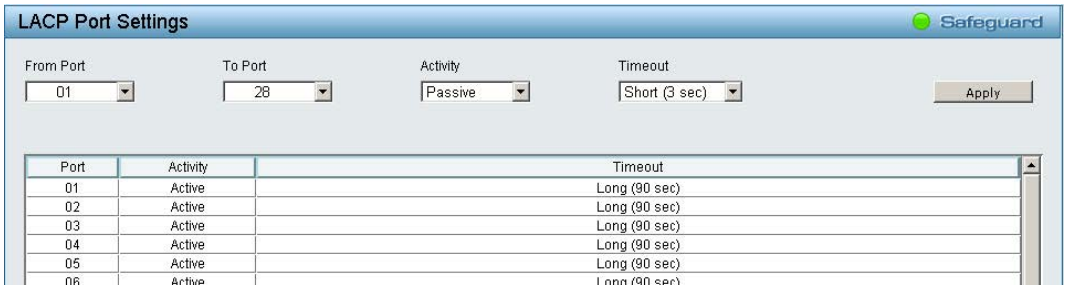


図 5-59　LACP Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
Activity	LACP ポートの動作を選択します。 初期値：「Passive」 選択肢：「Active」「Passive」 • Active 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 ポートをアクティブ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 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アクティブな LACP ポートである必要があります。
Timeout	管理用の LACP タイムアウトを指定します。 初期値：「Long (90 sec)」 選択肢：「Long (90 sec)」「Short (3 sec)」 • Short (3 sec) - LACP タイムアウトを 3 秒に定義します。 • Long (90 sec) -LACP タイムアウトを 90 秒に定義します。

3. 「Apply」をクリックし、設定を有効にします。

Multicast（マルチキャスト）

IGMP Snooping（IGMP Snooping 設定）

IGMP（Internet Group Management Protocol）Snooping 機能を利用して、各フレームのレイヤ 2 MAC ヘッダの内容を確認し、高度なマルチキャストフォワーディングを行うことができます。
IGMP Snooping 機能は、LAN 上に散乱したトラフィックの削減に貢献します。本機能を有効にすると、Web スマートスイッチは、マルチキャストトラフィックをそのマルチキャストグループのメンバのみに転送します。

IGMP Snooping の設定は、各 VLAN ごとに個別で行います。

1. 「L2 Functions」>「Multicast」>「IGMP Snooping」の順にメニューをクリックします。

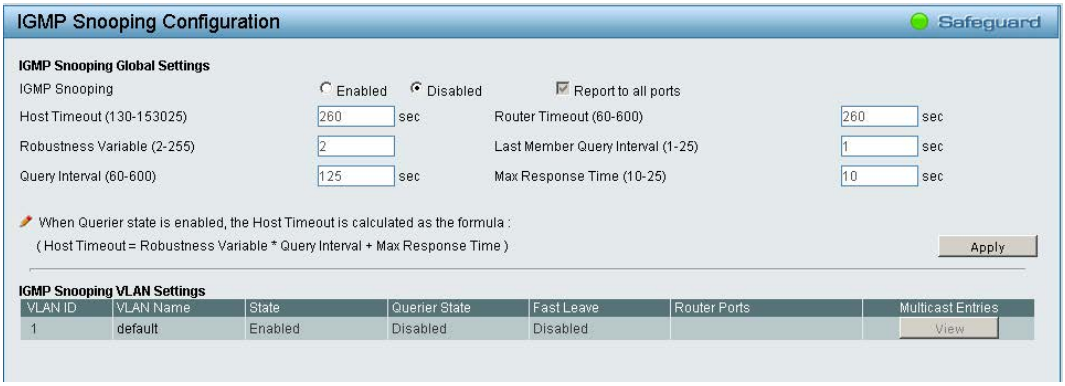


図 5-60　IGMP Snooping Configuration 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
IGMP Snooping	IGMP Snooping を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
Host Timeout (130-153025)	学習されたホストポートエントリが削除されるまでの時間を設定します。 初期値：260（秒） 選択可能範囲：130-153025（秒） 補足 学習された各ホストポートに対し、「Host Port Purge Interval」に使用する「Port Purge Timer」が起動されます。本タイマはそのポートにてホストからの Report メッセージを受信する度に開始されます。「Host Port Purge Interval」の間に Report メッセージを受信しない場合、そのホストエントリはマルチキャストグループから除外されます。
Robustness Variable (2-255)	予想されるパケット損失率に合わせて本値を調整します。 パケット損失率が高ければ、大きい値を指定します。「0」には設定できません。「1」は非推奨です。 初期値：2（秒） 選択可能範囲：2-255（秒）
Query Interval (60-600)	General Query の送信間隔を設定します。 初期値：125（秒） 選択可能範囲：60-600（秒） 補足 クエリインターバルの値を調整することで、送信する IGMP メッセージ数を増減できます。 大きい値を指定すると IGMP クエリの送信頻度は少なくなります。
Router Timeout (60-600)	学習されたルータポートエントリが削除されるまでの時間を設定します。 初期値：260 秒 選択可能範囲：60-600 秒 補足 学習された各ルータポートに対し、「Router Port Purge Interval」に使用する「Router Port Purge Timer」が起動されます。本タイマはそのポートから Router control メッセージを受信する度に開始されます。「Router Port Purge Interval」の間に Router control メッセージを受信しない場合、そのルータポートエントリは除外されます。
Last Member Query Interval (1-25)	Leave Group メッセージを受け取った時に送信する、Group-Specific Membership Query の Max Response Time フィールドに設定する値（Last Member Query Interval）を設定します。また、同 Query の送信間隔でもあります。 初期値：1 秒 選択可能範囲：1-25 秒 補足 本値はネットワークでの「Leave Latency」を変更する目的でも使用できます。 小さい値を設定するとグループの最後のメンバの不在を検知する時間が短く設定されます。

項目	説明
Max Response Time (10-25)	IGMP Response report を送信するまでの最大時間（秒）を設定します。 初期値：10 秒 選択可能範囲：10-25 秒 補足 本値を調整すると、「Leave Latency」、または「最後のホストがグループを抜けた瞬間からマルチキャストサーバがメンバが存在していないことに気付くまでの時間差」が変更されます。また、サブネット上の IGMP トラフィックの頻度を制御することも可能です。

3. 「Apply」をクリックし、設定を有効にします。

特定の VLAN に対する IGMP Snooping の有効化を行う場合

既存の VLAN に IGMP スヌーピングを有効にするには、「Enable」を選択し「Apply」をクリックします。それから Then press the Edit button under「Router Port Setting」の下の「Edit」を押し、VLAN の IGMP スヌーピングのルータポートに指定するポートを選択します。「Apply」をクリックすると設定が有効になります。手動で指定したルータポートは「Static Router Port」になり、「Dynamic Router Port」はクエリコントロールメッセージ受信時にスイッチにより自動的に設定されます。

1. 「IGMP Snooping VLAN Settings」の「VLAN ID」欄のリンクをクリックします。

補足 「IGMP Snooping Global Settings」で、「IGMP Snooping」を「Enabled」（有効）にした場合のみ選択可能です。

補足 VLAN のリストが複数ページにわたっている場合は、画面右下の「Page」「Back」「Next」でページを選択します。

2. 設定したい内容に応じて、以下から操作を選択します。

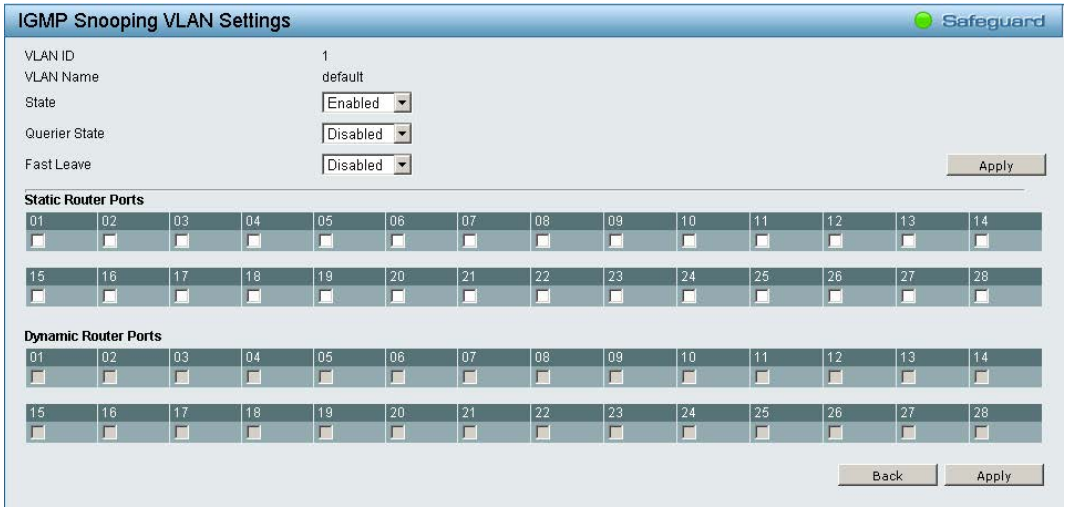


図 5-61　IGMP Snooping VLAN Settings 画面

■ 画面に表示される項目

項目	説明
VLAN ID	VLAN ID を表示します。 VLAN 名と共に、IGMP Snooping 設定の対象となる VLAN を識別するために使用します。
VLAN Name	IGMP Snooping クエリアを設定する VLAN 名を表示します。 VLAN ID と共に、IGMP Snooping 設定を行う対象の VLAN を識別します。
State	指定した VLAN への IGMP Snooping 機能を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Enabled」
Querier State	クエリア状態を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
Fast Leave	IGMP Snooping の Fast Leave 機能を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」 補足 本機能を有効にすると、システムが IGMP Leave メッセージを受信した場合、メンバはすぐにグループから削除されます。

項目	説明
Static Router Port	手動でルーターポートを指定します。
Dynamic Router Port	ダイナミックに設定されたルータポートを表示します。

3. 「Apply」をクリックし、設定を有効にします。

補足 「Static Router Port」の設定を行った場合は画面下部の「Apply」を、それ以外の変更を行った場合は上部の「Apply」をクリックしてください。

「Back」をクリックすると、IGMP Snooping（IGMP Snooping 設定）画面に戻ります。

MLD Snooping（MLD Snooping 設定）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じように使用される IPv6 機能です。マルチキャストデータを要求する VLAN に接続しているポートを検出するために使用されます。選択した VLAN 上のすべてのポートにマルチキャストトラフィックが流れる替わりに、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。

1. 「L2 Functions」>「Multicast」>「MLD Snooping」の順にメニューをクリックします。

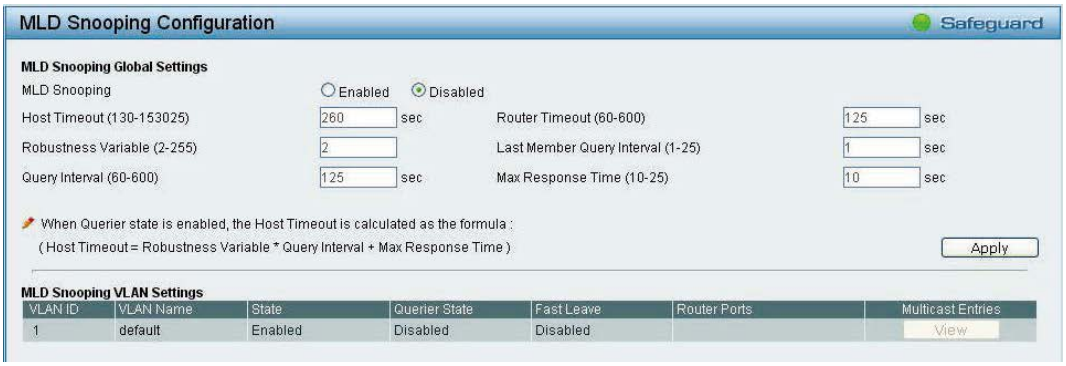


図 5-62　MLD Snooping Configuration 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

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：「Disabled」
Host Timeout (130-153025)	学習されたホストポートエントリが削除されるまでの時間を設定します。 ここで設定した時間をこえて MLD リポートが受信されなかった場合、ポートはマルチキャストグループから除外されます。 初期値：260（秒） 選択可能範囲：130-153025（秒）
Router Timeout (60-600)	学習されたルータポートエントリが削除されるまでの時間を設定します。 初期値：125 秒 選択可能範囲：60-600 秒
Robustness Variable (2-255)	予想されるパケット損失率に合わせて本値を調整します。 パケット損失率が高ければ、大きい値を指定します。「0」には設定できません。「1」は非推奨です。 初期値：2（秒） 選択可能範囲：2-255（秒）

項目	説明
Last Member Query Interval (1-25)	Leave Group メッセージを受け取った時に送信する、Group-Specific Membership Query の Max Response Time フィールドに設定する値（Last Member Query Interval）を設定します。また、同 Query の送信間隔でもあります。 この値はネットワークの "leave latency" を調整するのにも使用される場合があります。本数値の減少はグループメンバ損失の検出時間の削減になります。 初期値：1 秒 選択可能範囲：1-25 秒
Query Interval (60-600)	General Query の送信間隔を設定します。「Query Interval」の増減により MLD メッセージの増減にもつながります。値が大きいと MLD クエリの送信の減少につながります。 初期値：125（秒） 選択可能範囲：60-600（秒）
Max Response Time (10-25)	MLD Response report を送信するまでの最大時間（秒）を設定します。ポートが「Done」メッセージを送信するとポートはマルチキャストメンバから除外されます。 初期値：10 秒 選択可能範囲：10-25 秒

3. 「Apply」をクリックし、設定を有効にします。

特定の VLAN に対する MLD Snooping の有効化を行う場合

1. 「MLD Snooping VLAN Settings」の「VLAN ID」欄のリンクをクリックします。
2. 設定したい内容に応じて、以下から操作を選択します。

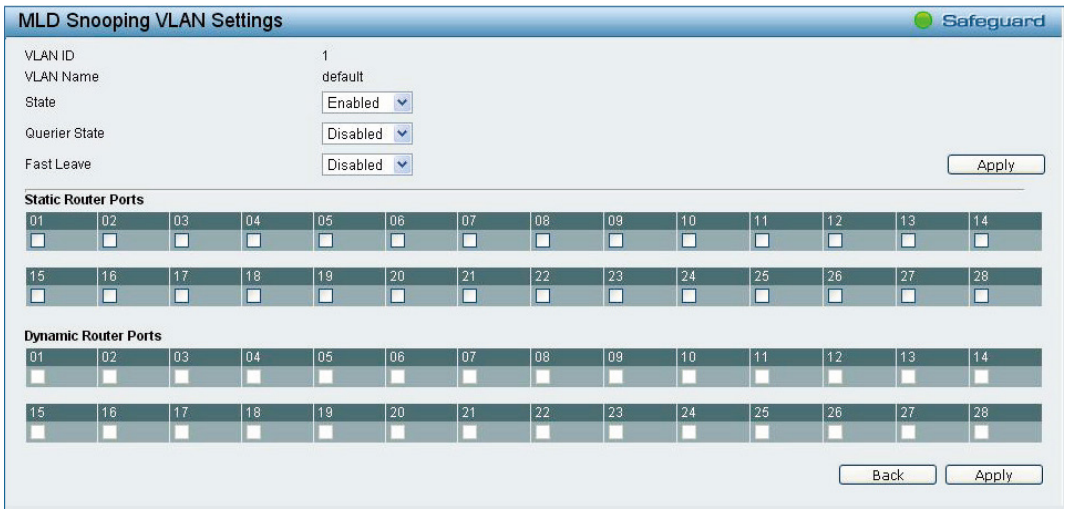


図 5-63　MLD Snooping VLAN Settings 画面

■ 画面に表示される項目

項目	説明
VLAN ID	VLAN ID を表示します。 VLAN 名と共に、IGMP Snooping 設定の対象となる VLAN を識別するために使用します。
VLAN Name	MLD Snooping クエリアを設定する VLAN 名を表示します。 VLAN ID と共に、MLD Snooping 設定を行う対象の VLAN を識別します。
State	指定した VLAN への MLD Snooping 機能を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Enabled」
Querier State	クエリア状態を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
Fast Leave	MLD Snooping の Fast Leave 機能を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
Static Router Port	手動でルーターポートを指定します。
Dynamic Router Port	ダイナミックに設定されたルータポートを表示します。

3. 「Apply」をクリックし、設定を有効にします。

補足　「Static Router Port」の設定を行った場合は画面下部の「Apply」を、それ以外の変更を行った場合は上部の「Apply」をクリックしてください。

「Back」をクリックすると、MLD Snooping（MLD Snooping 設定）画面に戻ります。

Multicast Forwarding（マルチキャストフォワーディング）

スイッチにスタティックなマルチキャストフォワーディングを設定します。
スタティックマルチキャストフォワーディングテーブルには、登録したすべてのエントリが表示されます。

1. 「L2 Functions」>「Multicast」>「Multicast Forwarding」の順にメニューをクリックします。

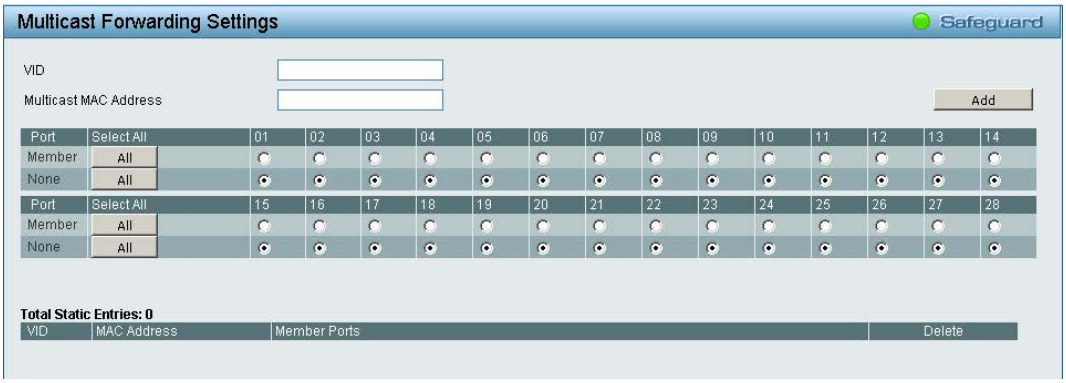


図 5-64　Multicast Forwarding Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
VID	指定の Multicast MAC アドレスが属する VLAN の VLAN ID を指定します。
Multicast MAC Address	マルチキャスト MAC アドレスを指定します。
Port	各ポートを「Member」または「None」に設定します。 初期値：「None」 • Member 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。 • None ダイナミックにマルチキャスト参加を行います。 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。 補足　「All」をクリックすると、すべてのポートを選択できます。

3. 「Add」をクリックし、設定内容を登録します。

登録した設定内容を削除するには、「Delete」をクリックします。

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

マルチキャストフィルタリング機能により、VLAN ごとに IGMP グループのフィルタリングモードを選択します。

1. 「L2 Functions」>「Multicast」>「Multicast Filtering Mode」の順にメニューをクリックします。

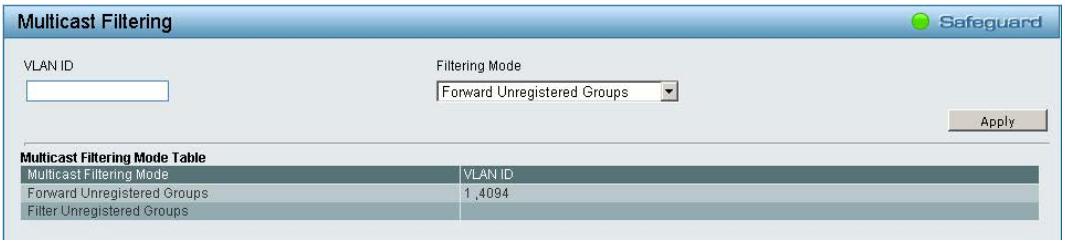


図 5-65　Multicast Filtering 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
VLAN ID	VLAN ID を指定します。
Filtering Mode	フィルタリングモードを「Forward Unregistered Groups」「Filter Unregistered Groups」から選択します。 初期値：「Forward Unregistered Groups 」 • Forward Unregistered Groups マルチキャストグループに登録されていないポートに対しても、マルチキャストパケットを転送します。 • Filter Unregistered Groups マルチキャストグループに登録されているポートに対してのみ、マルチキャストパケットを転送します。

3. 「Apply」をクリックし、設定を有効にします。

SNTP（SNTP 設定）

SNTP（Simple Network Time Protocol）は、コンピュータのクロックにスイッチを同期させるために使用されます。
SNTP 設定には 、「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。

1. 「L2 Functions」>「SNTP」>「Time Settings」の順にメニューをクリックします。

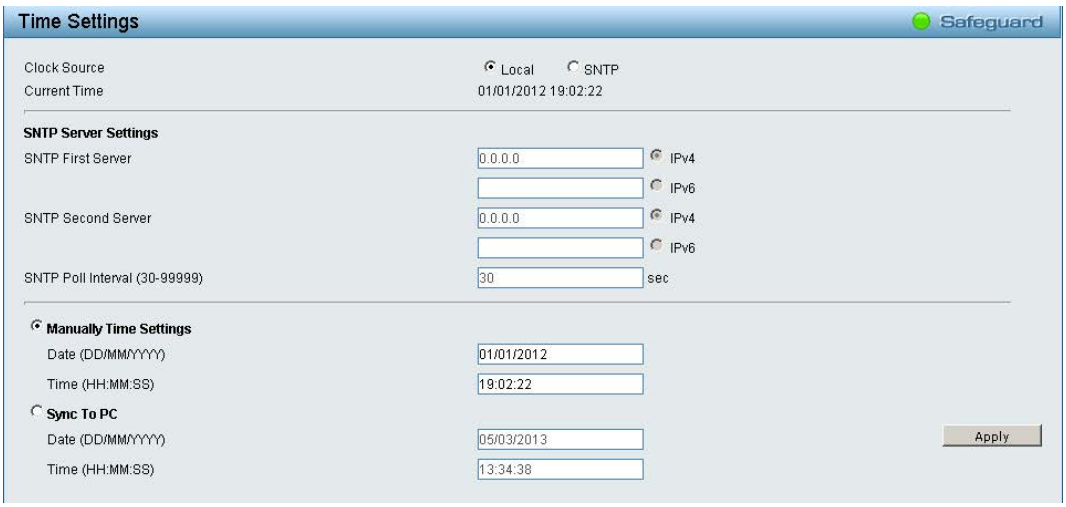


図 5-66　Time Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Clock Source	システム時刻を設定するタイムソースを設定します。 初期値：「Local」 • 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。 • Local システム時刻をデバイスに対して直接設定します。
Current Time	現在の時間を表示します。
SNTP Server Settings	
SNTP First Server	IPv4 または IPv6 を選択し、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	IPv4 または IPv6 を選択し、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を設定します。 初期値 : 30（秒） 選択可能範囲：30-99999（秒）
Manually Time Settings / Sync To PC	
• Manually Time Settings - 手動で時刻の設定をします。 • Sync To PC - PC の時刻設定を同期させます。	
Date（DD/MM/YYYY）	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：午後 9 時であれば 21:00:00 と指定します。

3. 「Apply」をクリックし、設定を有効にします。

TimeZone Settings（時刻設定）

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。

1. 「L2 Functions」>「SNTP 」>「TimeZone Settings」の順にメニューをクリックします。

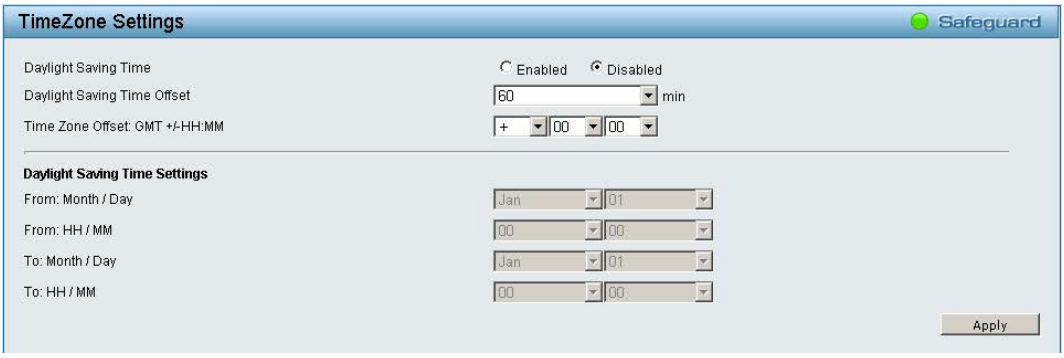


図 5-67　TimeZone Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Daylight Saving Time State	サマータイム設定を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
Daylight Saving Time Offset	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選択します。 初期値：60（分） 選択肢：30、60、90、120（分）
Time Zone Offset: from GMT +/ - 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。
Daylight Saving Time Settings	
From: Month / Day	サマータイムが開始する月および日を指定します。
From: HH MM	サマータイムが開始する時間を指定します。
To: Month / Day	サマータイムが終了する月および日を指定します。
To: HH MM	サマータイムが終了する時間を指定します。

3. 「Apply」をクリックし、設定を有効にします。

LLDP（LLDP 設定）

LLDP Global Settings（LLDP グローバル設定）

本スイッチは、IEEE 802.1AB に準拠した LLDP（Link Layer Discovery Protocol）に準拠しています。
本機能では、LLDP 対応デバイス同士が、隣接する LLDP デバイスに自分自身についての情報を通知し合い、お互いを認識します。
これらの情報を MIB（Management Information Base）に保存し、SNMP ユーティリティが各 LLDP デバイスの MIB 情報を取得することでネットワークトポロジを把握します。

1. 「L2 Functions」>「L2 Functions」>「LLDP」>「LLDP Global Settings」の順にメニューをクリックします。

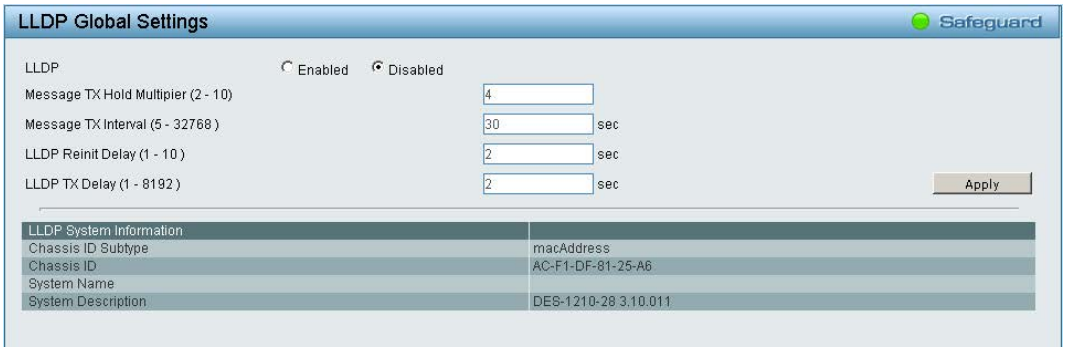


図 5-68　LLDP Global Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
LLDP	LLDP 機能を「Enabled」(有効) または「Disabled」(無効) にします。 有効にすると、スイッチは LLDP パケットの送信、受信、プロセスを開始します。LLDP パケットの周知のためにスイッチはポートを通してネイ場に LLDP の情報を展開します。LLDP パケットの受信にはネイバテーブル上のネイバから周知された LLDP パケット情報を取得します。「Apply」をクリックして設定の変更を有効にします。 初期値：「Disabled」
Message TX Hold Multiplier (2-10)	LLDP で送信する情報の TTL 値を設定します。 初期値：4 選択可能範囲：2-10 補足　TTL 値を超過すると、隣接するスイッチの MIB から、送信した情報は削除されます。
Message TX Interval (5-32768)	LLDP で情報を送信する間隔を設定します。 初期値：30（秒） 選択可能範囲：5-32768（秒）
LLDP Reinit Delay (1-10)	LLDP を初期化するときの遅延時間（秒）を指定します。 初期値：2（秒） 選択可能範囲：1-10（秒）
LLDP TX Delay (1-8192)	連続した LLDP フレーム伝送間の遅延（LLDP TX Delay）の値を設定します。 初期値：2（秒） 選択可能範囲：1-8192（秒） 補足　LLDP TX Delay には、以下の公式を満たす数値を設定する必要があります。 『　LLDP TX Delay の値 < (0.25×(Message TX Interval の値))　』

3. 「Apply」をクリックし、設定を有効にします。

LLDP MED Settings（LLDP MED 設定）

補足　LLDP MED 設定は DGS-1210-10P/28P でのみ使用可能です。

LLDP-MED（Link Layer Discovery Protocol-Media Endpoint Discovery）は LLDP の機能を増強しており、IP 電話や AP などといったエンドポイントの危機の LLDP 機能が改善されています。LLDP-MED は LAN ポリシーや機器の自動検出などが強化されています。現在は DGS-1210-10P/28P のみが PoE エンドポイントの自動電源管理を 802.3at ポート（10P: 全ポート /28P: 1 ～ 4 ポート) で対応しています。

This page allows user to configure the 本ページでは 802.3at ポートの設定と「Power PSE TLV (Type-length-value)」、「From Port/ To Port」（ポート範囲）、「Enable / Disable」（有効 / 無効）などを設定し、「Apply」を押下することで「Power PSE TLV」通信の有効も功を設定することができます。

1. 「L2 Functions」>「LLDP」>「LLDP MED」の順にメニューをクリックします。

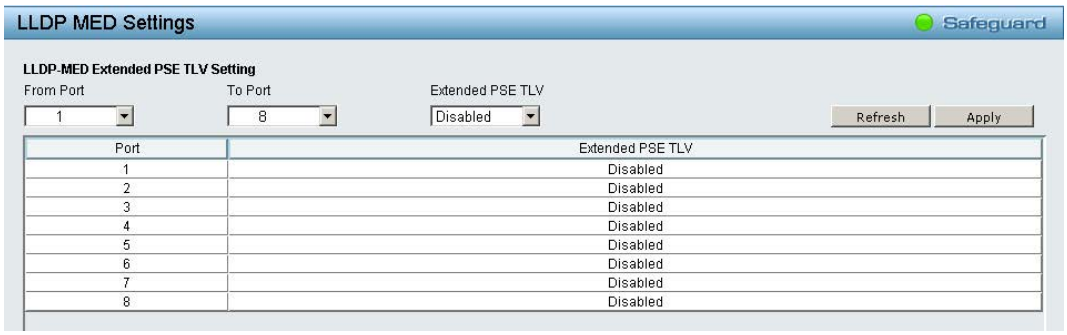


図 5-69　LLDP MED Settings 画面

2. 「From Port」「To Port」で設定対象のポート範囲を指定します。
3. 「Extended PSE TLV」を「Enabled」（有効）または「Disabled」(無効) にします。
4. 「Apply」をクリックし、設定を有効にします。

   「Refresh」をクリックすると、表示を最新のものに更新できます。

LLDP Port Settings（LLDP ポート設定）

LLDP ポート設定のためのパラメータを含む LLDP ポート情報を表示または設定します。

1. 「L2 Functions」>「LLDP」>「LLDP Port Settings」の順にメニューをクリックします。

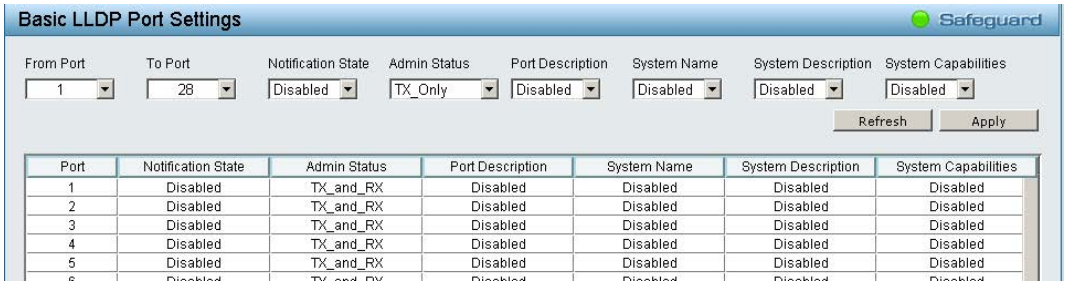


図 5-70　Basic LLDP Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
Notification State	LLDP トポロジ変化がポートに発生した場合に、通知を送信するかどうかを指定します。 初期値：「Disabled」 • Enabled - ポートの LLDP 通知を有効にします。 • Disabled - ポートの LLDP 通知を無効にします。

項目	説明
Admin Status	ポートの LLDP 転送モードを定義します。 初期値：「TX_Only」 選択肢：「TX_Only」「RX_Only 」「TX_and_RX 」「Disabled」 • TX_Only - LLDP パケットを送信します。 • RX_Only - LLDP パケットを受信します。 • TX_and_RX - LLDP パケットを送受信します。 • Disabled - ポートの LLDP を無効にします。
Port Description	ポート説明の TLV を、ポートで「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
System Name	システム名の TLV を、ポートで「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
System Description	システム説明の TLV を、ポートで「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
System Capabilities	システムケイパビリティの TLV を、ポートで「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」

3. 「Apply」をクリックし、設定を有効にします。

「Refresh」をクリックすると、表示を最新のものに更新できます。

802.1 Extension TLV（802.1 Extension TLV 設定）

802.1 Extension LLDP ポートの設定を行います。

1. 「L2 Functions」>「LLDP」>「802.1 Extension TLV」の順にメニューをクリックします。

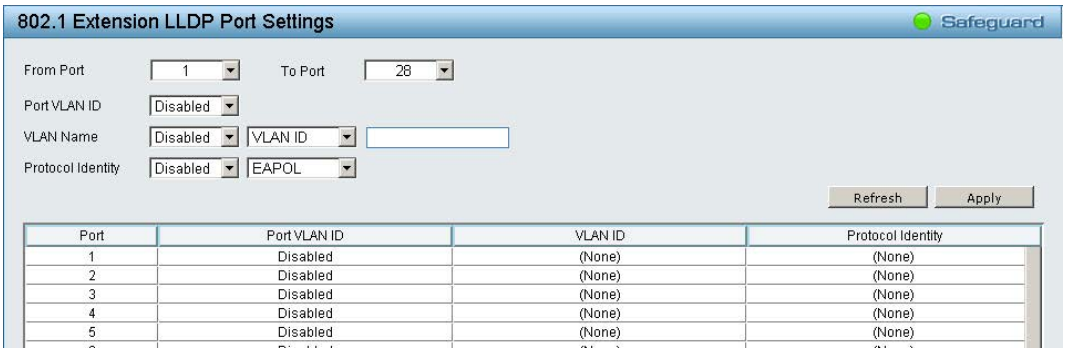


図 5-71　802.1 Extension LLDP Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
Port VLAN ID	ポート VLAN ID を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
VLAN Name	VLAN 名を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」 「Enabled」を選択した場合は、「VLAN ID」「VLAN Name」「All」を選択します。 「VLAN ID」または「VLAN Name」を選択した場合は、右の欄にそれぞれ VLAN ID、VLAN 名を入力します。
Protocol Identity	プロトコル識別子を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」 「Enabled」を選択した場合、「EAPOL」「LACP」「GVRP」「STP」または「All」を指定します。

3. 「Apply」をクリックし、設定を有効にします。

「Refresh」をクリックすると、表示を最新のものに更新できます。

802.3 Extension TLV（802.3 Extension TLV 設定）

802.3 Extension LLDP ポートの設定を行います。

1. 「L2 Functions」>「LLDP」>「802.3 Extension TLV」の順にメニューをクリックします。

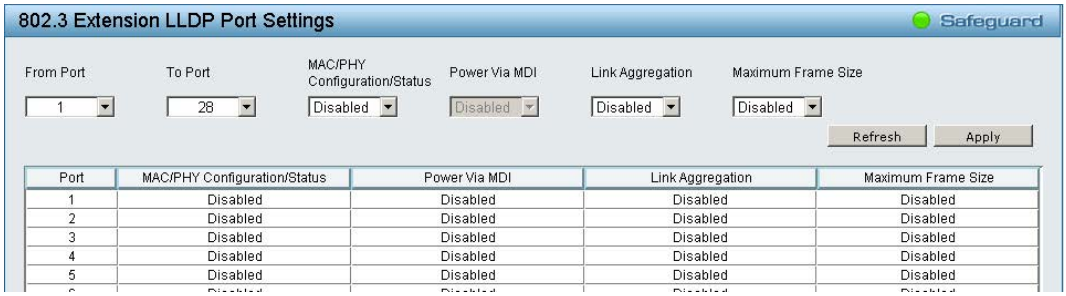


図 5-72　802.3 Extension LLDP Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
MAC/PHY Configuration/ Status	MAC/PHY 設定ステータスをポートで「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
Power via MDI	ポートにサポートされる Power via MDI を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
Link Aggregation	リンクアグリゲーション「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
Maximum Frame Size	最大フレームサイズを「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」

3. 「Apply」をクリックし、設定を有効にします。

「Refresh」をクリックすると、表示内容を更新できます。

LLDP Management Address Settings（LLDP 管理アドレス設定）

転送される LLDP 情報に含める管理アドレスを設定します。

1. 「L2 Functions」>「LLDP」>「LLDP Management Address Settings」の順にメニューをクリックします。

図 5-73　LLDP Management Address Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
Address Type	ポートにおける LLDP アドレスタイプを指定します。本設定は IPv4 のみ設定可能です。
Address	アドレスを入力します。
Port State	ポート状態を「Enabled」(有効) または「Disabled」(無効) にします。

3. 「Apply」をクリックし、設定を有効にします。

LLDP Management Address Table（LLDP 管理アドレステーブル）

管理アドレス情報の詳細を表示します。

1. 「L2 Functions」>「LLDP」>「LLDP Management Address Table」の順にメニューをクリックします。

図 5-74　LLDP Management Address Table 画面

2. 「Management Address」で「IPv4」または「IPv6」を選択します。

3. IP アドレスを入力し、「Search」をクリックします。

4. 管理アドレスの情報が以下のように表示されます。

- Subtype：管理アドレスのサブタイプを表示します。
- Management Address：IP アドレスを表示します。
- IF Type：IF タイプを表示します。
- OID：SNMP OID を表示します。
- Advertising Ports：通知するポートを表示します。

LLDP Local Port Table（LLDP ローカルポートテーブル）

LLDP ローカルポート情報を表示します。

1. 「L2 Functions」>「LLDP」>「LLDP Local Port Table」の順にメニューをクリックします。

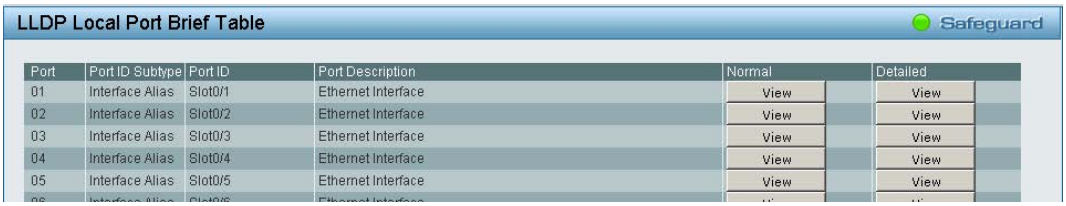


図 5-75　LLDP Local Port Brief Table 画面

2. 以下の内容が表示されます。

■ 画面に表示される項目

項目	説明
Port	ポート番号を表示します。
Port ID Subtype	ポート ID サブタイプを表示します。
Port ID	ポート ID（ユニット番号 / ポート番号）を表示します。
Port Description	ポート説明文を表示します。
Normal	「View」をクリックすると、LLDP ローカルポートノーマル情報が表示されます。
Detailed	「View」をクリックすると、LLDP ローカルポート詳細情報が表示されます。

「Normal」の「View」をクリックした場合：

以下の LLDP ローカルポートノーマル情報画面が表示されます。

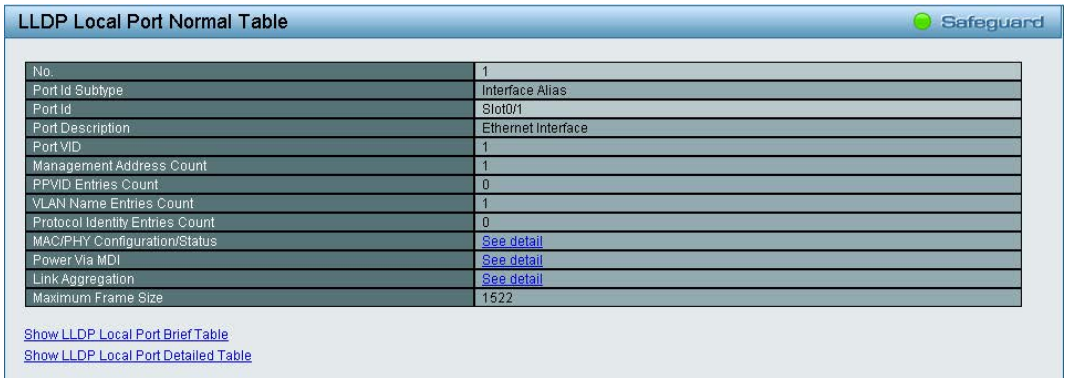


図 5-76　LLDP Local Port Normal Table 画面

「Detailed」の「View」をクリックした場合：

以下の LLDP ローカルポート詳細情報画面が表示されます。

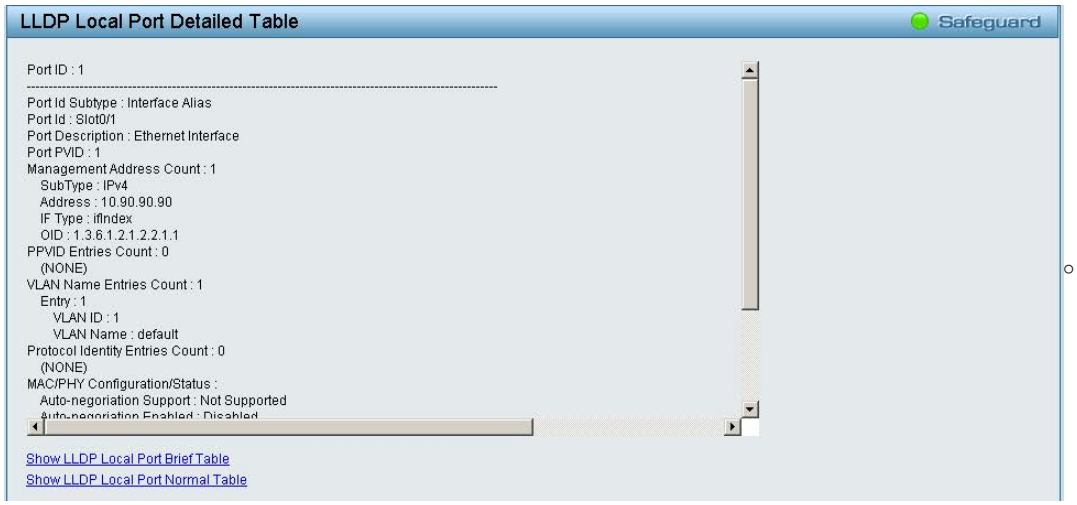


図 5-77　LLDP Local Port Detailed Table 画面

補足　画面左下のリンクをクリックすると、以下の画面に移動します。
「Show LLDP Local Port Brief Table」：手順 1 の画面に戻ります。
「Show LLDP Local Port Normal Table」：LLDP リモートポートノーマル情報画面が表示されます。
「Show LLDP Local Port Detailed Table」をクリックすると、LLDP リモートポート詳細情報画面が表示されます。

LLDP Remote Port Table（LLDP リモートポートテーブル）

LLDP リモートポートテーブルを表示します。

1. 「L2 Functions」>「LLDP」>「LLDP Remote Port Table」の順にメニューをクリックします。

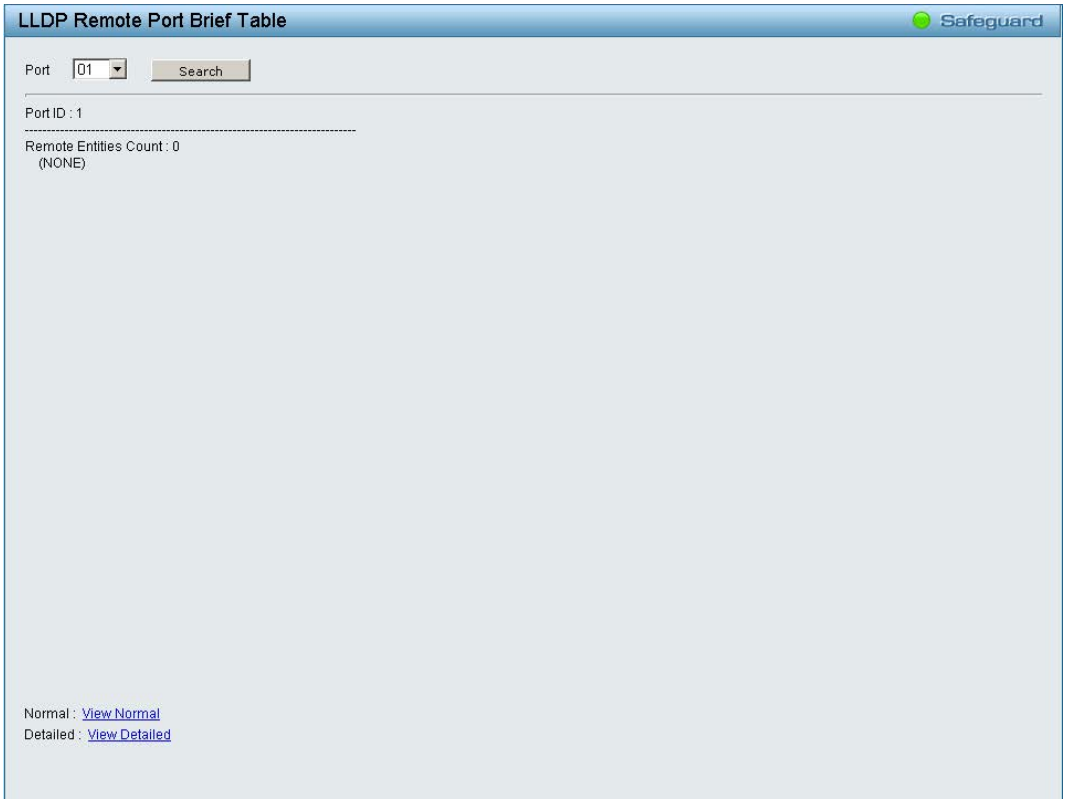


図 5-78　LLDP Remote Port Brief Table 画面

2. 「Port」でポートを選択し、「Search」をクリックします。

3. 「View Normal」または「View Detailed」をクリックします。

「View Normal」をクリックした場合：
以下の LLDP リモートポートノーマル情報画面が表示されます。

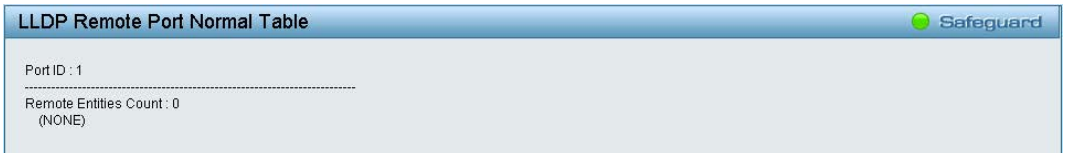


図 5-79　LLDP Remote Port Normal Table 画面

「Normal」の「View」をクリックした場合：
以下の LLDP リモートポート詳細情報画面が表示されます。

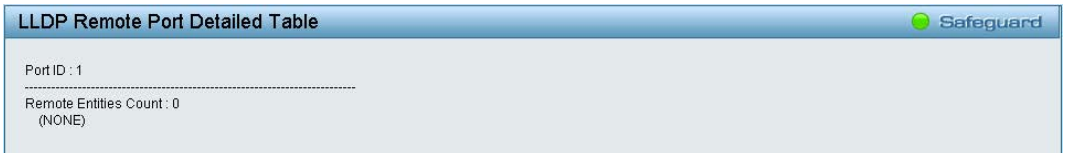


図 5-80　LLDP Remote Port Detailed Table 画面

補足　画面左下のリンクをクリックすると、以下の画面に移動します。
「Show LLDP Remote Port Brief Table」：手順 1 の画面に戻ります。
「Show LLDP Remote Port Normal Table」：LLDP リモートポートノーマル情報画面が表示されます。
「Show LLDP Remote Port Detailed Table」をクリックすると、LLDP リモートポート詳細情報画面が表示されます。

LLDP Statistics（LLDP 統計情報）

LLDP トラフィックに関する概要を表示します。

1. 「L2 Functions」>「LLDP」>「LLDP Statistics」の順にメニューをクリックします。

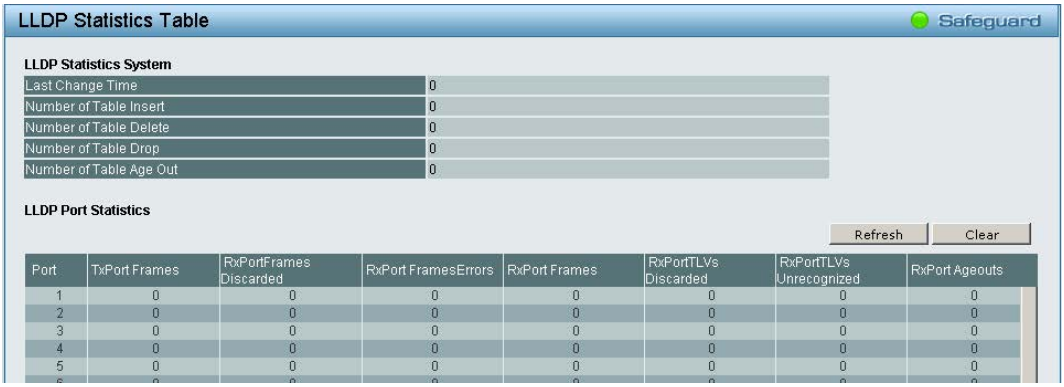


図 5-81　LLDP Statistics Table 画面

2. 以下の内容が表示されます。

■ 画面に表示される項目

項目	説明
LLDP Statistics System	
スイッチ全体についてカウンタを表示します。	
Last Change Time	最後に変更したエントリが最後に削除または追加された時間を表示します。 最後の変更が検出されてからの経過時間も表示します。
Number of Table Insert	スイッチの再起動後に追加された新しいエントリの数を表示します。
Number of Table Delete	スイッチの再起動後に削除された新しいエントリの数を表示します。
Number of Table Drop	テーブルがいっぱいになったため、破棄された LLDP フレーム数を表示します。
Number of Table Age Out	Time-To-Live の期限が切れたために削除されたエントリ数を表示します。
LLDP Port Statistics	
ポートについてカウンタを表示します。	
Port	ポート番号を表示します。
TxPort Frames Total	ポートに LLDP エージェントが転送した LLDP フレームの合計数を表示します。
RxPort Frames Discarded	ポートに受信した LLDP フレームのうち破棄されたフレームの合計数を表示します。
RxPort Frames Errors	ポートに受信した LLDP フレームのうちのエラーフレーム数を表示します。
RxPort Frames	ポートが受信した LLDP フレームの合計数を表示します。
RxPortTLVs Discarded	破棄された TLV 数を表示します。 補足　各 LLDP フレームには、TLV として知られる複数の情報があります。TLV が不正な形式であると破棄されます。
RxPortTLVs Unrecognized	整形式の TLV 数（既知のタイプ値を持つ）を表示します。
RxPort Ageouts	各 LLDP フレームには LLDP 情報が有効である時間情報があります。 エージング時間内に新しい LLDP フレームを受信しないと、LLDP 情報は削除されて、Age-Out カウンタがカウントアップされます。

「Refresh」をクリックすると、表示が更新されます。
「Clear」をクリックすると、カウンタが削除されます。

QoS（QoS 機能の設定）

■ QoS の設定項目

- Bandwidth Control（帯域幅の設定）
- 802.1p/DSCP/ToS (802.1p/DSCP/ToS 設定)

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。

1. 「QoS」>「Bandwidth Control」の順にメニューをクリックします。

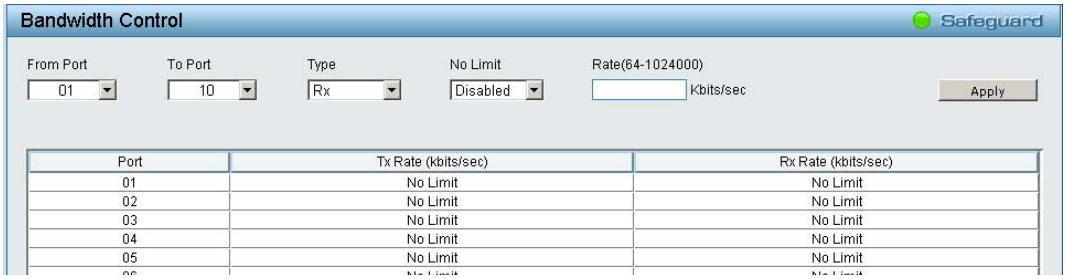


図 5-82　Bandwidth Control 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
Type	タイプを選択し、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。 選択肢：「Rx」「Tx」「Both」 • Rx - 帯域上限を受信に適用します。 • Tx - 帯域上限を送信に適用します。 • Both - 帯域上限を送受信両方に適用します。
No Limit	ポートに対する帯域制限を設定します。 初期値：「Disabled」 • 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。
Rate(64-1024000)	指定したポートでのデータ速度の上限値（Kbit/ 秒）を設定します。 設定可能範囲：64-1024000

3. 「Apply」をクリックし、設定を有効にします。

802.1p/DSCP/ToS (802.1p/DSCP/ToS 設定)

QoS は IEEE 802.1p 標準で規定される技術です。ネットワーク管理者は、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、およびビデオ会議などのような広帯域を必要とする、またはより高い優先順位を持つ重要なサービスのために、帯域を確保することができます。

優先度が高いポートからのトラフィックがスイッチで優先されます。タグ付けされていないパケットに関しては、スイッチはユーザの設定に従って優先順位を割り当てます。

QoS の設定は「802.1p」「DSCP」「ToS」から行います。

1. 「QoS」>「802.1p/DSCP/ToS」の順にメニューをクリックします。

2. 「Select QoS Mode」で、「802.1p」「DSCP」「ToS」のいずれかを選択します。
   上部の「Apply」をクリックすると、「802.1p」「DSCP」「ToS」の画面に移動します。

802.1p Prioriy Setting 画面

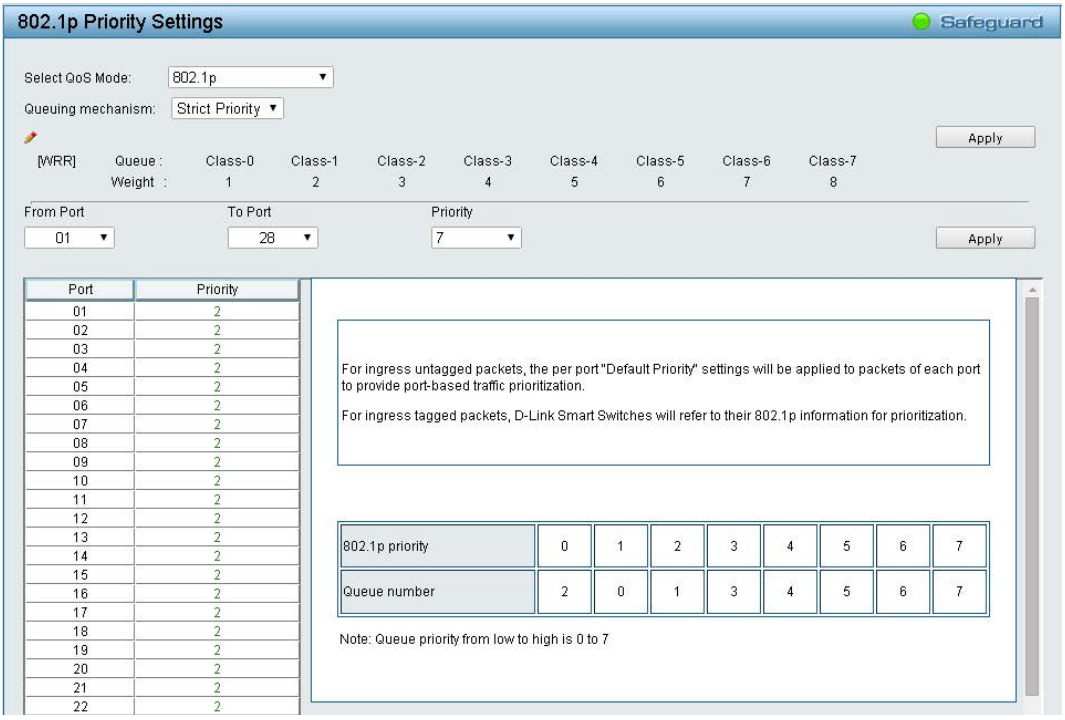


図 5-83　802.1p Priority Settings 画面

DSCP Prioriy Setting 画面

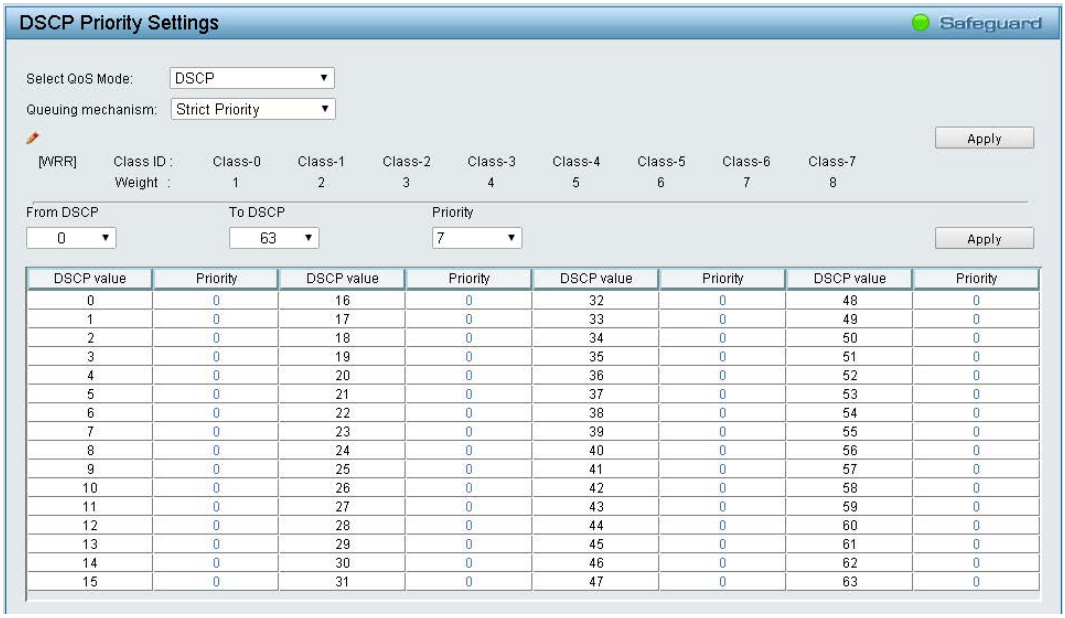


図 5-84　DSCP Priority Settings 画面

ToS Prioriy Setting 画面

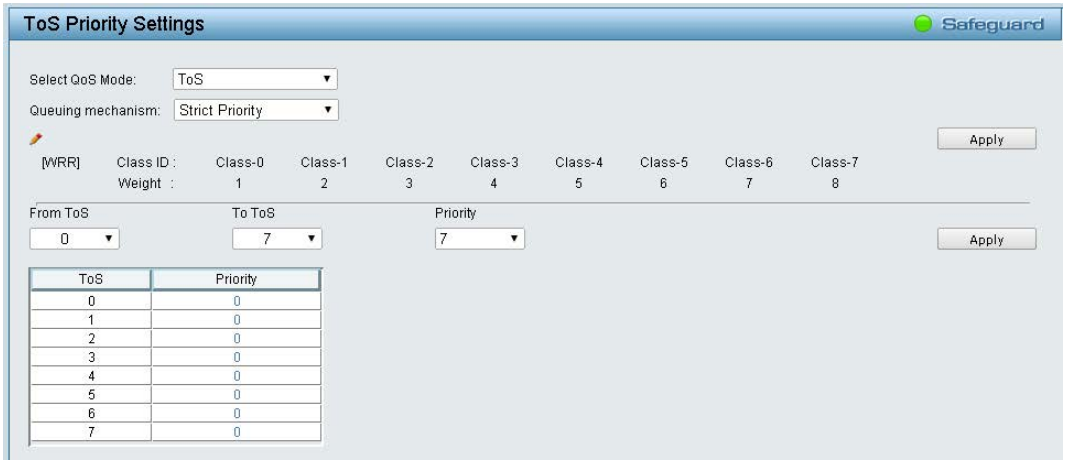


図 5-85　ToS Priority Settings 画面

3. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Select QoS Mode	QoS モードを選択します。 初期値：「802.1p」 選択肢：「802.1p」「DSCP」「ToS」 • 802.1p VLAN タグの 802.1p プライオリティベースとします。 • DSCP IP ヘッダの DSCP プライオリティベースとします。 • ToS IP ヘッダの ToS プライオリティベースとします。
Queuing mechanism	キューイングの方法を選択します。 初期値 :「Strict Priority」 選択肢：「WRR」 • Strict Priority Strict スケジューリングでは優先値の高いキューが最優先となり、続く級は WRR スケジュールに従います。 • WRR WRR (Weighted Round-Robin) のアルゴリズムを使用してパケットを取り扱います。
From Port/ To Port	設定対象のポート範囲を指定します。 802.1p Prioriy Setting 画面でのみ表示されます。
From DSCP/ To DSCP	設定対象の DSCP 範囲を指定します。 DSCP Prioriy Setting 画面でのみ表示されます。
From ToS/ To ToS	設定対象の ToS 範囲を指定します。 ToS Prioriy Setting 画面でのみ表示されます。
Priority	優先度を選択します。 ポートへの優先値を指定します。0 から 7 までの間で指定できます。 0 が最小の優先値となり、7 が最大の優先値となります。初期値は 7 です。

4. 「Apply」をクリックし、設定を有効にします。

Security（セキュリティ機能の設定）

■ Security の設定項目

Trusted Host（トラストホスト）

トラストホスト機能を使用して、リモートステーションからスイッチを管理します。
IPv4 アドレス /Netmask または IPv6 アドレス /Prefix を定義したホストを最大 10 個まで登録することができます。
機能を有効にしたあと、トラストホストとしてローカルホスト IP アドレスを追加します。そうしないと接続を失います。

1. 「Security」>「Trusted Hostl」の順にメニューをクリックします。

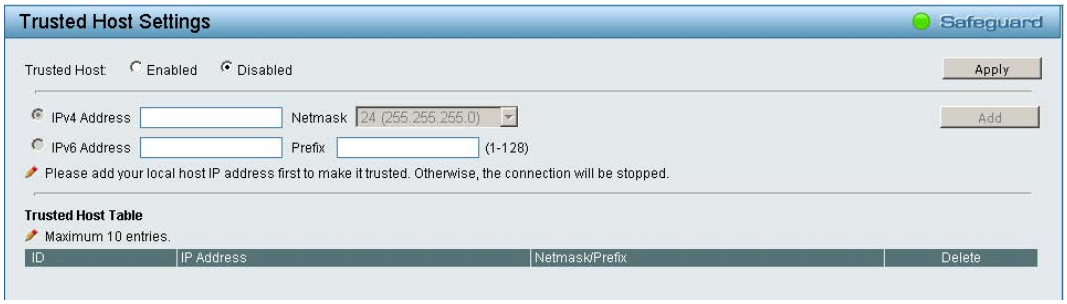


図 5-86　Trusted Host Settings 面

2. 「Trusted Host」を「Enabled」（有効）または「Disabled」（無効）にします。

3. 「Apply」をクリックします。

4. 「Trusted Host」を「Enabled」（有効）にした場合は、「IPv4 Address」または「IPv6 Address」を選択します。

5. IPv4 アドレス /Netmask または IPv6 アドレス /Prefix を入力します。

6. 「Add」をクリックしてトラストホストを作成します。

   作成したトラストホストを削除する場合は、「Delete」をクリックします。

   異なる IP マスク設定ごとに IP アドレスまたは IP アドレス範囲を入力します。
   入力形式は、192.168.1.1/255.255.255.0 または 192.168.0.1/24 です。
   入力可能な IP 範囲の例は以下の通りです。

IP Address	IP Mask	Permitted IP
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255
172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

Port Security（ポートセキュリティ）

ポートセキュリティは、ポートのロックを行う前にソース 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。

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。

1. 「Security」>「Port Security」の順にメニューをクリックします。

図 5-87　Port Security 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Admin State	ポートのロックを「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
Max Learning Address (0-64)	ポートが学習できる最大の MAC アドレス数を指定します。 初期値：0 設定可能範囲：0-64

3. 「Apply」をクリックし、設定を有効にします。

設定した内容は、「Port Security」に表示されます。

Traffic Segmentation（トラフィックセグメンテーション）

スイッチの 1 つのポートから、ポートグループへのトラフィックフローを制限します。
トラフィックフローの分割方法は VLAN を使用したトラフィック制限に類似していますが、より限定的です。

1. 「Security」>「Traffic Segmentation」の順にメニューをクリックします。

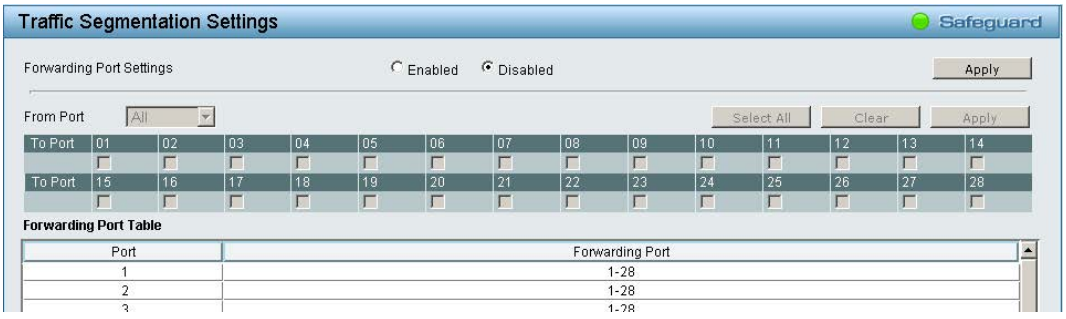


図 5-88　Traffic Segmentation 画面

2. 「Forwarding Port Settings」を「Enabled」（有効）または「Disabled」（無効）にします。（初期値：無効）

3. 画面上部の「Apply」をクリックします。

4. 「Forwarding Port Settings」を「Enabled」（有効）にした場合は、「From Port」/「To Port」でポートを選択します。
「Select All」をクリックすると、すべてのポートを選択できます。
「Clear」をクリックすると、選択したポートを解除できます。

5. 画面下部の「Apply」をクリックします。

Safeguard Engine（セーフガードエンジン）

セーフガードエンジンは、パケットフラッディングによるスイッチの CPU への影響を自動的に抑制する機能です。
悪意のあるウィルスやワームによる攻撃が Web スマートプロスイッチの動作に影響を与えないように保護を行います。

1. 「Security」>「Safeguard Engine」の順にメニューをクリックします。

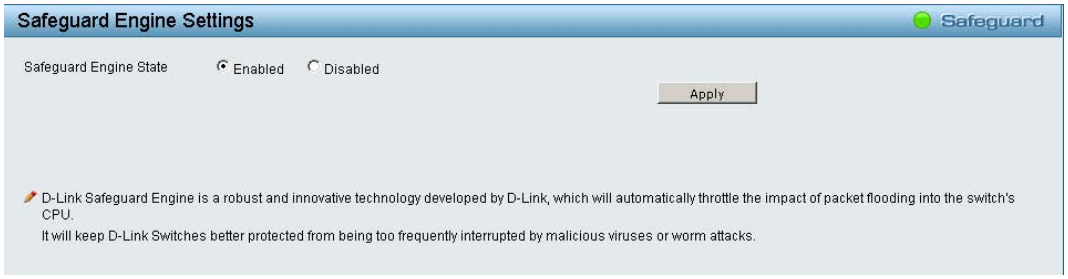


図 5-89　Safeguard Engine 画面

2. 「Safeguard Engine State」を「Enabled」(有効) または「Disabled」(無効) にします。
   初期値：「Enabled」

3. 「Apply」をクリックし、設定を有効にします。

Storm Control（ストームコントロール）

ストームコントロール機能は、ブロードキャスト、マルチキャスト、未知のユニキャストパケットを制限する機能です。
一度パケットストームが検出されると、ストームがおさまるまでスイッチはパケットの廃棄を継続します。

1. 「Security」>「Storm Control」の順にメニューをクリックします。

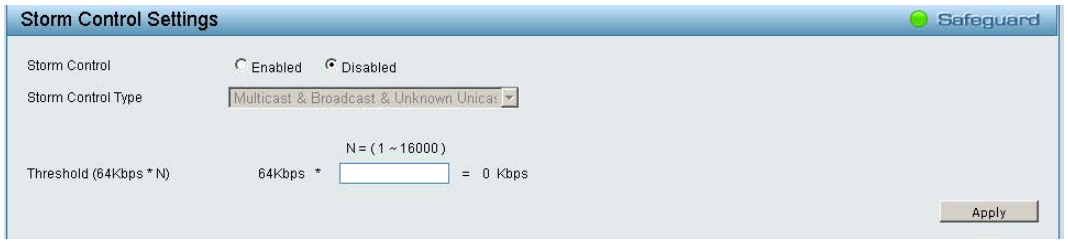


図 5-90　Storm Control Settings 画面

2. 「Storm Control」を「Enabled」(有効) または「Disabled」(無効) にします。
   初期値：「Disabled」

3. 「Storm Control」を「Enabled」(有効) にした場合、「StormControl Type」を選択します。
   初期値：「Multicast & Broadcast & Unknown Unicast」
   選択肢：「Broadcast Only」「Multicast & Broadcast」「Multicast & Broadcast & Unknown Unicast」

4. 「Threshold(64Kbps*N)」で、しきい値を設定します。

   補足　しきい値は毎秒 64 - 1024000Kbps で設定可能です。
   「N」には 1- 16000 の間の数値を設定し、64Kbps との倍数を指定します。

5. 「Apply」をクリックし、設定を有効にします。

ARP Spoofing Prevention（ARP スプーフィング防止）

ARP スプーフィングは、ARP ポイゾニングとしても知られています。
LAN 上のデータフレームを盗み見たり、トラフィックを改竄したり、トラフィックを止める（DoS 攻撃として知れられている）といったことをすることで、イーサネットネットワークを攻撃する方法です。

ARP スプーフィングの主な方法は、イーサネットネットワークに偽造または改竄した ARP メッセージを送信することです。
この ARP メッセージによって、デフォルトゲートウェイなど別ノードの IP アドレスに、攻撃者の MAC アドレスやでたらめな MAC アドレスを割り当ててしまいます。これにより、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しまいます。

一般的な DoS 攻撃は、実在しない MAC アドレスや指定 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。攻撃者は、1 つの Gratuitous ARP をゲートウェイとするネットワークに対してブロードキャストし、間違ったノードにインターネットへの全パケットを向けるため、すべてのネットワーク操作がダウンさせられてしまいます。

ARP スプーフィング防止機能は、Gratuitous ARP パケットをチェックして、不正な IP または MAC アドレスを持つものをフィルタすることで、ネットワークにおける ARP スプーフィング攻撃を破棄します。

1. 「Security」>「ARP Spoofing Prevention」の順にメニューをクリックします。

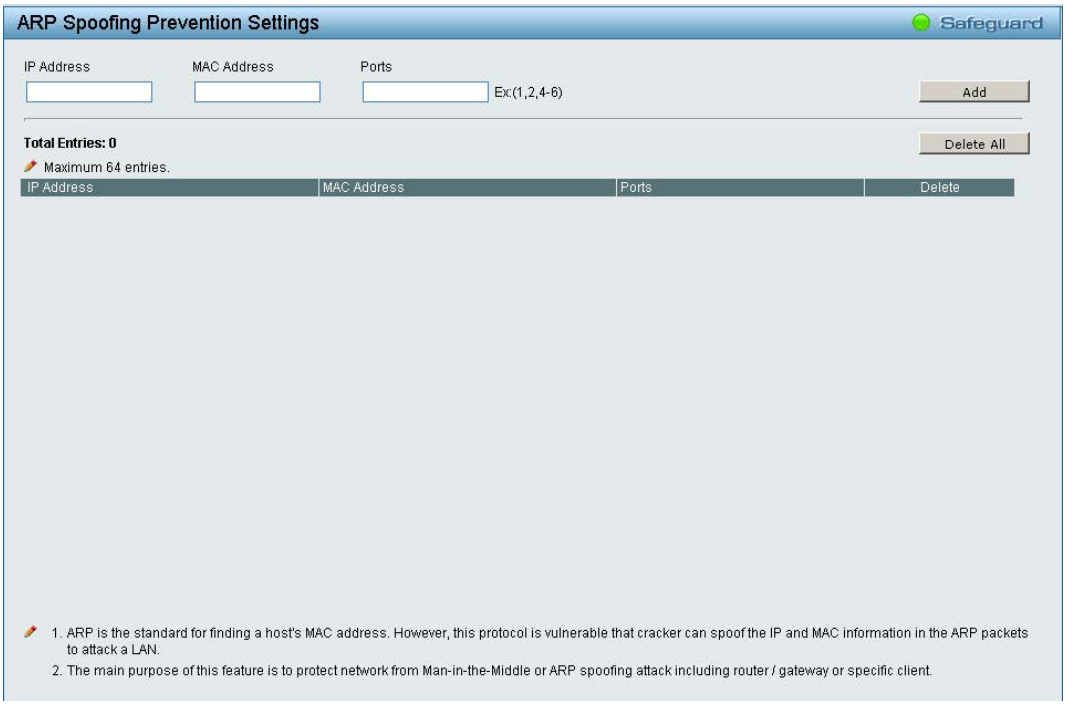


図 5-91　ARP Spoofing Prevention Settings 画面

2. ARP スプーフィングを適用する「IP Address」「MAC Address」「Ports」を設定します。

3. 「Add」をクリックします。

作成したエントリを削除する場合は、「Delete」をクリックしてください。
作成したエントリをすべて削除する場合は、「Delete All」をクリックしてください。

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

DHCP サーバスクリーニングは、疑わしいポートから DHCP サービスを破棄することによって、不正な DHCP サーバを制限する機能です。各ポートに DHCP サーバスクリーニングの有効 / 無効を設定し、信頼する DHCP サーバの IP アドレスを指定することができます。

1. 「Security」>「DHCP Server Screening」の順にメニューをクリックします。

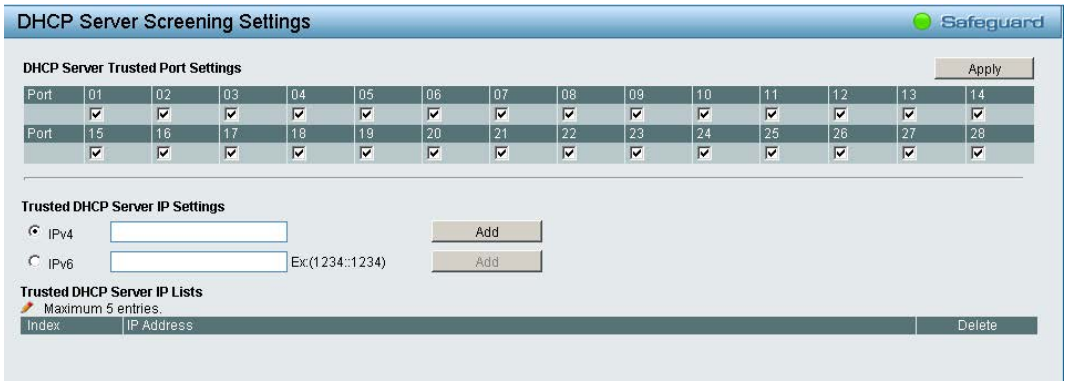


図 5-92　DHCP Server Screening Settings 画面

2. 「DHCP Server Trusted Port Settings」で、DHCP サーバスクリーニングを適用するポートを選択します。

3. 「Apply」をクリックし、設定を有効にします。

4. 「Trusted DHCP Server IP Settings」で、信頼する DHCP サーバの IP アドレスの種類を「IPv4」/「IPv6」から選択します。

5. 信頼する DHCP サーバの IP アドレスを入力します。

6. 「Add」をクリックします。
   作成したエントリを削除する場合は、「Delete」をクリックしてください。

SSL（SSL 設定）

SSL(Secure Sockets Layer) とは、認証、デジタル署名および暗号化を使用して、Web 管理ホストとスイッチの Web UI 間に安全な通信パスを提供するセキュリティ機能です。これらのセキュリティ機能は、暗号のパラメータ・暗号化アルゴリズム・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されます。

1. 「Security」>「SSL」の順にメニューをクリックします。

図 5-93　SSL Settings 画面

2. 「SSL State」で、「Enabled」（有効）または「Disabled」（無効）を選択します。（初期値：「Disabled」）

補足　SSL が有効である場合、暗号化により Web を開く際に以前より長い時間がかかります。コンフィグレーションの保存後、システムのサマリページの表示まで 10 秒ほどお待ちください。

3. 上部の「Apply」をクリックし、設定を有効にします。

4. 「Enabled」（有効）を選択した場合は、「SSL Ciphersuite Settings」で、各暗号スイートの「Enabled」（有効）または「Disabled」（無効）を選択します。（初期値：「Enabled」）

5. 下部の「Apply」をクリックし、設定を有効にします。

DoS Prevention（DoS 攻撃防止設定）

DoS 攻撃防止設定を有効 / 無効にします。DoS 攻撃防止が有効な場合は、下記テーブルで設定した DoS 攻撃と見られるパケットをスイッチは破棄します。パケットの精査はハードウェアで行われます。

1. 「Security」>「DoS Prevention Settings」の順にメニューをクリックします。

図 5-94　DoS Prevention Settings 画面

2. 「State」で、「Enabled」（有効）または「Disabled」（無効）を選択します。（初期値：「Disabled」）
3. 「Apply」をクリックし、設定を有効にします。

SSH（SSH 設定）

SSH は、Secure Shell の略語です。安全性の低いネットワーク上においても、安全なリモートログインおよびネットワークサービスを実現します。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。

SSH Settings（SSH 設定）

1. 「Security」>「SSH」>「SSH Settings」の順にメニューをクリックします。

図 5-95　SSH Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
SSH State	「Enabled 」（有効）または「Disabled」（無効）を選択します。
Max Session (1-4)	同時にスイッチに接続できる数を 1 から 4 の数字を設定します。 初期値：4
Connection Timeout (120-600)	接続のタイムアウト時間を指定します。120 から 600（秒）が指定できます。初期値は（秒）です。 初期値：120（秒） 選択可能範囲：120-600（秒）
Authfail Attempts (2-20)	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。　初期値：2 選択可能範囲：2-20 補足　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。
Rekey Timeout	スイッチが SSH 鍵の再交換を行う間隔をプルダウンメニューから選択します 選択肢：「Never」、「10 min」、「30 min」、「60 min」 初期値：「60 min」

3. 「Apply」をクリックし、設定を有効にします。

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

SSH 認証モードの設定と、認証および暗号化に使用する SSH アルゴリズムの設定を行います。
アルゴリズムは 3 つのカテゴリ（「Encryption Algorithm」「Encryption Algorithm」「Public Key Algorithm」）ごとに分けて表示されています。
チェックボックスを使用して有効、無効に設定できます。

1. 「Security」>「SSH」>「SSH Authmode and Algorithm Settings」の順にメニューをクリックします。

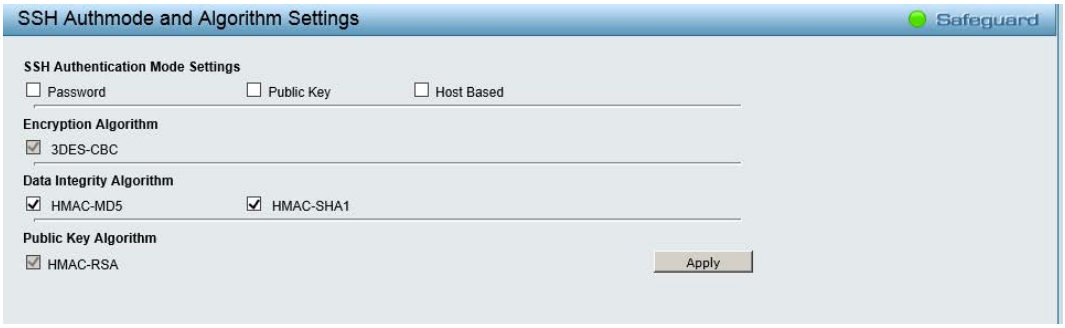


図 5-96　SSH Authmode and Algorithm Settings 画面

■ 画面に表示される項目

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

2. 有効にしたい項目にチェックをいれます。

3. 「Apply」をクリックし、設定を有効にします。

SSH User Authentication Lists（SSH ユーザ認証設定）

SSH を使用してスイッチにアクセスを行うユーザリストの設定を行います。

1. 「Security」>「SSH」>「SSH User Authentication Lists」の順にメニューをクリックします。

図 5-97　SSH User Authentication Lists 画面

2. 「Edit」をクリックします。

3. 以下の画面で SSH ユーザ認証の設定を行います。

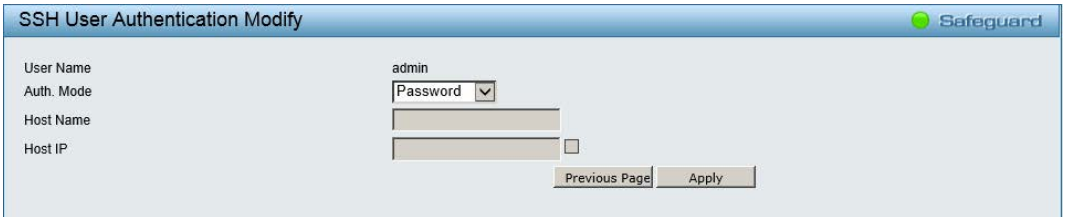


図 5-98　SSH User Authentication Modify 画面

■ 画面に表示される項目

項目	説明
User Name	ユーザ名が表示されます。
Auth.mode	認証モードを選択します。 選択肢：「Password」「Public Key」「Host Based」 • 「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。選択、設定すると管理者定義のパスワードの入力を求められます。 • 「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 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。
Host Name	リモート SSH ユーザを識別する 32 文字までの半角英数字を入力します。本項目は「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。

4. 「Apply」をクリックし、設定を有効にします。
「Previous Page」をクリックすると「SSH User Authentication Lists」画面に戻ります。

Smart Binding（スマートバインディング）

スマートバインディングは、認証されたユーザのみがスイッチにアクセスできるよう制限する機能です。
IP アドレスと MAC アドレスのペアを事前に設定したデータベースと比較して認証を行います。また、DHCP スヌーピングが有効になっている場合は、スイッチが自動的に DHCP パケットをスヌーピングして IP アドレスと MAC アドレスのペアを学習し、スマートバインディングのホワイトリストに登録することもできます。
未認証ユーザがスマートバインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。

Smart Binding Settings（スマートバインディング設定）

1. 「Security」>「Smart Binding」>「Smart Binding Settings」の順にメニューをクリックします。

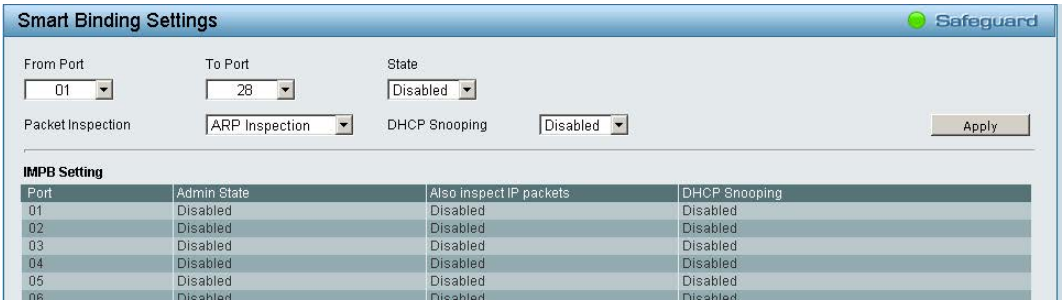


図 5-99　Smart Binding Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port / To Port	設定するポート範囲を指定します。
State	スマートバインディングを「Enabled」(有効) または「Disabled」(無効) に設定します。 初期値：「Disabled」
Packet Inspection	IP パケット検知機能を選択します。 初期値：「ARP Inspection」 選択肢：「ARP Inspection」「IP+ARP Inspection」 • ARP Inspection 認証済みの ARP パケットは転送され、未認証の ARP パケットは破棄されます。受信した ARP パケットは審査されスマートバインディングホワイトリストと照合されます。ARP パケットと IP-MAC ペアがリストにない場合、スイッチはその MAC アドレスをブロックします。この機能の主な利点は CPU リソースを多用しないことですが、しかしユニキャスト IP パケットのみを使う不正ユーザはブロックできません。例として手動で設定された ARP テーブルのある PC からの DoS 攻撃に対し、ARP パケットを送信しない PC からの攻撃をスイッチはブロックできません。 • IP+ARP Inspection 認証済みの IP パケットは転送され、未認証の IP パケットは破棄されます。受信した ARP パケットと IP パケットは審査され IMPB ホワイトリストと照合されます。IP-MAC ペアがリストとマッチすると、スイッチはその MAC アドレスをブロックしません。もしマッチしないと MAC アドレスはブロックしたままになります。すべての ARP、IP パケットを精査するためより強固なセキュリティを実現できます。
DHCP Snooping	DHCP スヌーピングを「Enabled」(有効) または「Disabled」(無効) に設定します。 初期値：「Disabled」 補足　「DHCP Snooping」を有効にすると、DHCP サーバ / クライアントからのパケットを詮索し、ホワイトリストの情報を更新します。

3. 「Apply」をクリックし、設定を有効にします。

設定した内容は、画面下部のテーブルに表示されます。

Smart Binding（スマートバインディング）

「Manual Binding」では、IP アドレス、MAC アドレス、ポート番号を入力し、IP-MAC バインディングエントリを作成します。
「Auto Scan」から、接続している機器を検出してバインディングを行うことも可能です。

1. 「Security」>「Smart Binding」>「Smart Binding」の順にメニューをクリックします。

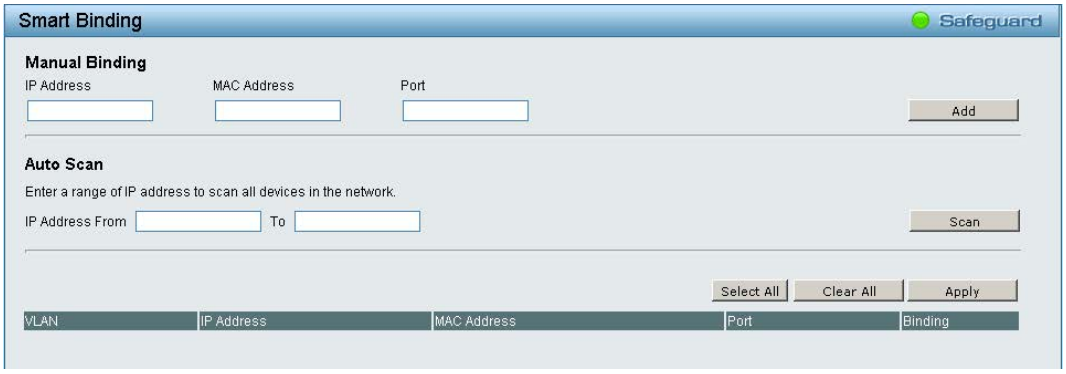


図 5-100　Smart Binding 画面

Manual Binding で設定を行う場合

1. 「IP Address」「MAC Address」「Port」を指定します。
   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。
   Port : 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。
2. 「Add」をクリックします。

登録が成功すると、「Complete!」とメッセージが表示されるので、「OK」をクリックします。
登録内容は「Security」>「White List」に表示されます。

Auto Scan で設定を行う場合

1. 「IP Address From/To」でスキャンする機器の IP アドレス範囲を指定します。
2. 「Scan」をクリックし、スキャンを実行します。
3. スキャン結果が表示されるので、バインディングさせるエントリの「Binding」にチェックをいれます。
   「Select All」をクリックすると、すべてのエントリが選択されます。
   「Clear All」をクリックすると、すべてのエントリのチェックが解除されます。
4. 「Apply」をクリックします。

登録が成功すると、「Complete!」とメッセージが表示されるので、「OK」をクリックします。
登録内容は「Security」>「White List」に表示されます。

White List（ホワイトリスト）

認証されたデバイスのリストが表示されます。

1. 「Security」>「Smart Binding」>「White List」の順にメニューをクリックします。

図 5-101　White List 画面

エントリを削除する場合は、エントリの「Delete」欄にチェックをいれ、「Delete」をクリックします。
すべての「Delete」欄にチェックをいれる場合は、「Select All」をクリックします。
チェックを解除するには、「Clean」をクリックします。

Black List（ブラックリスト）

認証されていないデバイスのリストが表示されます。「ARP Inspection」が選択されていて、対象機器がマッチしない IP-MAC-Port 情報を含む ARP パケットを送信している場合、その機器はブロックされここにリストされます。

1. 「Security」>「Smart Binding」>「Black List」の順にメニューをクリックします。

図 5-102　Black List 画面

認証されていないデバイスの検索を行う場合

1. デバイスの「VID」「IP Address」「MAC Address」「Port」を入力します
2. 「Find」をクリックします。

認証されていないデバイスの削除を行う場合

1. エントリの「Delete」欄にチェックをいれ、「Delete」をクリックします。

すべての「Delete」欄にチェックをいれる場合は、「Select All」をクリックします。
チェックを解除するには、「Clean」をクリックします。

AAA（AAA 機能の設定）

■ AAA の設定項目

- RADIUS Server（RADIUS サーバ設定）
- 802.1X（802.1X 機能の設定）

RADIUS Server（RADIUS サーバ設定）

RADIUS サーバは、中央集中型のユーザ管理を容易にし、またスニッフィングやハッカーからの攻撃から保護します。

1. 「AAA」>「RADIUS Server」の順にメニューをクリックします。

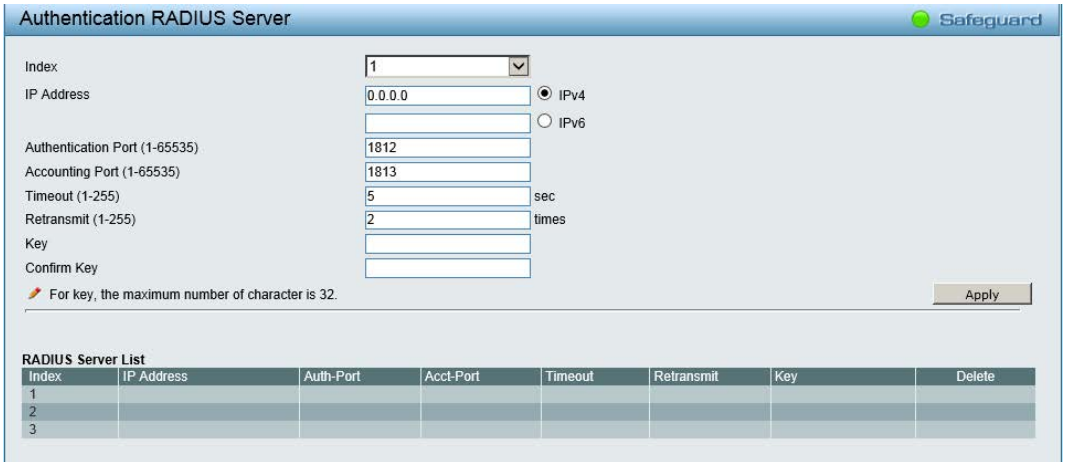


図 5-103　Authentication RADIUS Server 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Index	「1」、「2」、「3」から設定を行う RADIUS サーバを指定します。
IP Address	RADIUS サーバの IP アドレスを入力します。
Authentication Port (1-65535)	RADIUS 認証サーバの UDP ポートを指定します。 初期値：1812 設定可能範囲：1-65535
Accounting Port (1-65535)	RADIUS アカウントサーバの UDP ポートを指定します。 初期値：1813 設定可能範囲：1-65535
Timeout (1-255)	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。 初期値：5（秒） 設定可能範囲：1-255
Retransmit (1-255)	ユーザが認証を試みることができる最大回数を指定します。指定した回数を超えて認証に失敗すると、そのユーザはスイッチへのアクセスを拒否され、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：2 設定可能範囲：1-255
Key	RADIUS サーバと同じキーを入力します。
Confirm Key	RADIUS サーバと同じキーを確認のために再度入力します。

3. 「Apply」をクリックし、設定を有効にします。

設定した内容は、画面下部のテーブルに表示されます。

802.1X（802.1X 機能の設定）

ネットワークスイッチを利用することにより、クライアント PC は、接続するだけで簡単にリソースへアクセスできるようになります。しかし、このような自動コンフィグレーション機能は、不正なユーザが簡単に侵入して重要なデータへのアクセスを行う危険性があります。

IEEE 802.1X はネットワークへのアクセス制御に関するセキュリティ標準規格で、特に Wi-Fi 無線ネットワークにおけるユーザ認証仕様として知られています。IEEE 802.1X では、ユーザの認証が完了するまでネットワークポートを切断状態にします。スイッチは EAPOL（Extensible Authentication Protocol over LANs）と呼ばれるプロトコルを使用し、ユーザとの間でユーザ名などのクライアント認証データを交換し、それをリモートの RADIUS 認証サーバに転送してアクセスのための認証を受けます。クライアントは認証方法を拒否し、クライアントのソフトウェアと RADIUS サーバのコンフィグレーションに応じた他の認証方法を要求することができます。認証結果に応じて、そのポートをユーザに開放するか、ユーザのネットワークへのアクセスを拒否するかを決定します。

管理者は、RADIUS サーバを利用したユーザリストの収集・記録を行うことで、ネットワーク管理を簡素化できます。

802.1X Global Settings（802.1X グローバル設定）

802.1X 設定の有効・無効と EAPOL PDU の転送設定、および認証プロトコルの設定を行います。

1. 「AAA」>「802.1X」>「802.1X Global Settings」の順にメニューをクリックします。

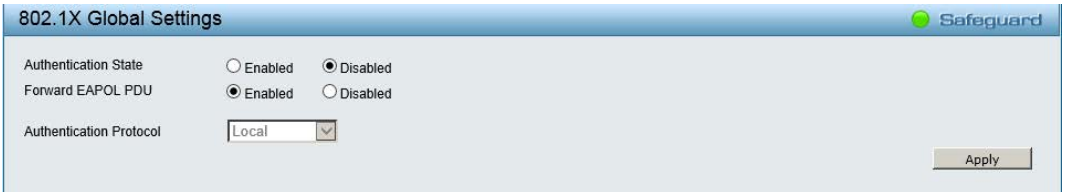


図 5-104　802.1X Global Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Authentication State	802.1X を「Enabled」(有効) または「Disabled」(無効) にします。 初期値：「Disabled」
Forward EAPOL PDU	EAPOL PDU の転送を制御するグローバル設定を「Enabled」(有効) または「Disabled」(無効) にします。 「Authentication State」が「Enabled」(有効) の場合は、本機能は使用できません。 初期値：「Enabled」
Authentication Protocol	認証プロトコルを「Local」または「RADIUS」から選択します。

3. 「Apply」をクリックし、設定を有効にします。

802.1X Port Settings（802.1X ポート設定）

802.1X ポートを設定します。

1. 「AAA」>「802.1X」>「802.1X Port Settings」の順にメニューをクリックします。

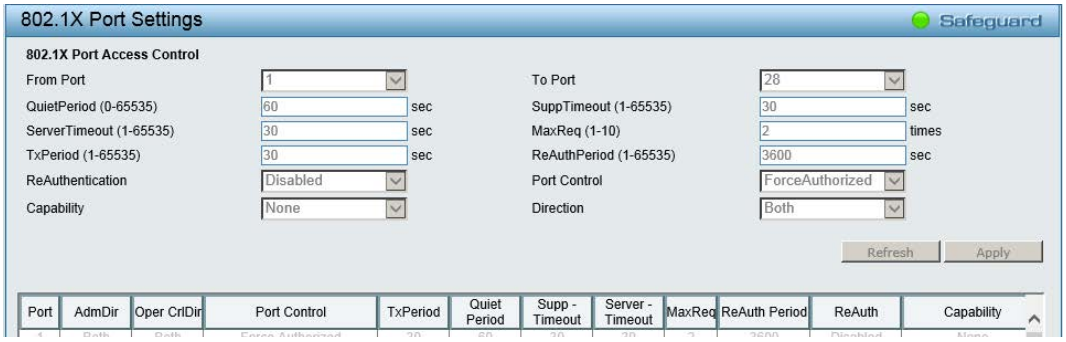


図 5-105　802.1X Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port / To Port	設定するポート範囲を指定します。
QuietPeriod (0-65535)	クライアントとの間での認証が失敗した場合、非認証状態（認証処理を行わない状態）を保持する時間 を設定します。 初期値：60（秒） 設定可能範囲：0-65535（秒）
SuppTimeout (1-65535)	クライアントとの間で認証処理を行う時間を設定します。 初期値：30（秒） 設定可能範囲：1-65535（秒）
ServerTimeout (1-65535)	認証サーバに応答を再送するまえに、スイッチがクライアントからの応答を待つ時間を設定します。 初期値：30（秒） 設定可能範囲：1-65535（秒）
MaxReq (1-10)	スイッチが EAP-request パケットをクライアントに送出する最大回数を設定します。 初期値：2 設定可能範囲：1-10
TxPeriod (1-65535)	オーセンティケータ PAE 状態の機器の TxPeriod を設定します。本値がクライアントへの EAP Request/ Identity パケットの送信間隔となります。 初期値：30（秒）
ReAuthPeriod (1-65535 sec)	認証成功後、クライアントの再認証を行う周期を設定します。 クライアントの周期的な再認証（ReAuthEnabled）が有効とされた場合のみ使用されます。 初期値：3600（秒） 設定可能範囲：1-65535（秒）
Port Control	ポート認証制御の方法を設定します。 初期値：「Auto」 選択肢：「Force Authorized」「Force Unauthorized 」「Auto」 • Force Authorized 802.1X を無効にし、認証情報の交換を要求せずにポートを Authorized 状態にします。この時ポートではクライアントの 802.1X ベースの認証を行うことなく、通常のトラフィックの送受信が可能になります。 • Force Unauthorized 対象ポートは Unauthorized 状態を保ち、すべてのクライアントからの認証要求を無視します。スイッチはインタフェースを通したクライアントの認証サービスを行いません。 • Auto 802.1X を有効にし、Unauthorized 状態を開始し、ポートにおいて EAPOL フレームのみの送受信を許可します。認証プロセスは、ポートのリンク状態が Down から Up に遷移した時、または EAPOL-start フレームが受信された時に開始されます。スイッチはクライアントの ID を要求し、クライアントと認証サーバとの間で認証メッセージの中継を開始します。
Capability	802.1X のケイパビリティを指定します。 • Authenticator - 各ポートに適用する 802.1X オーセンティケータの設定を指定します。 • None - ポートの 802.1X 認証機能を無効にします。
Direction	ポートにおける管理制御する方向を設定します。 • Both - 最初の欄で選択した制御ポートを経由する内向き、外向きトラフィックの両方に制御が行われます。 • In - 現在のファームウェアリリースではサポートしていません。

3. 「Apply」をクリックし、設定を有効にします。

802.1X User（802.1X ユーザ設定）

本画面では、802.1X ユーザの追加を行うことができます。

1. 「AAA」>「802.1X」>「802.1X User」の順にメニューをクリックします。

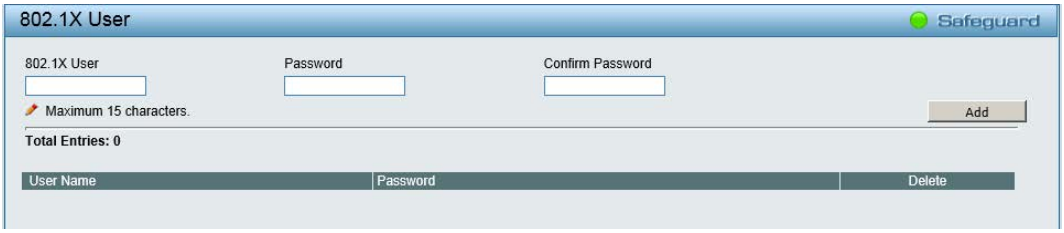


図 5-106　802.1X User 画面

2. 「802.1X User」(802.1X ユーザ名)、「Password」(パスワード) および「Confirm Password」(パスワードの確認) を入力します。

3. 「Add」をクリックし、ユーザを追加します。

   ユーザを削除するには「Delete」をクリックします。

ACL（ACL 機能の設定）

■ ACL の設定項目

- ACL Wizard（ACL 設定ウィザード）
- ACL Access List (ACL アクセスリスト)
- ACL Access List (ACL アクセスリスト)
- ACL Hardware Resource Status（ACL ハードウェアリソースステータス）

ACL Wizard（ACL 設定ウィザード）

アクセスコントロールリスト（ACL）により、パケットヘッダの中の情報に従って、スイッチがパケット送信を決定するための基準を設定できるようになります。この基準は MAC アドレスや IP アドレスをベースに設定することができます。

ACL 設定ウィザードでは、アクセスプロファイルと ACL ルールの新規作成を行います。スイッチで使用可能なプロファイル数は 50/200 ルールになります。

1. 「ACL」>「ACL Wizard」の順にメニューをクリックします。
2. 新しいアクセスルールを作成する場合は、「Create」を選択し「Access-List Name」にアクセスリストの名前を設定して「Next」をクリックします。

図 5-107　ACL Configuration Wizard 画面

3. パケットの種類を「MAC」「IPv4」「IPv6」から選択し「Next」をクリックします。

図 5-108　ACL Configuration Wizard - Packet Type 画面

■ 画面に表示される項目

項目	説明
MAC	MAC アドレスから送信されたパケットを対象に ACL を適用します。
IPv4	IPv4 アドレスから送信されたパケットを対象に ACL を適用します。
IPv6	IPv6 アドレスから送信されたパケットを対象に ACL を適用します。

選択したパケットの種類により次に表示される画面が違います。プロファイルの種類に合わせた設定方法に従い設定を行います。

MAC ACL Rule の設定

MAC ACL Rule を設定します。「MAC」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

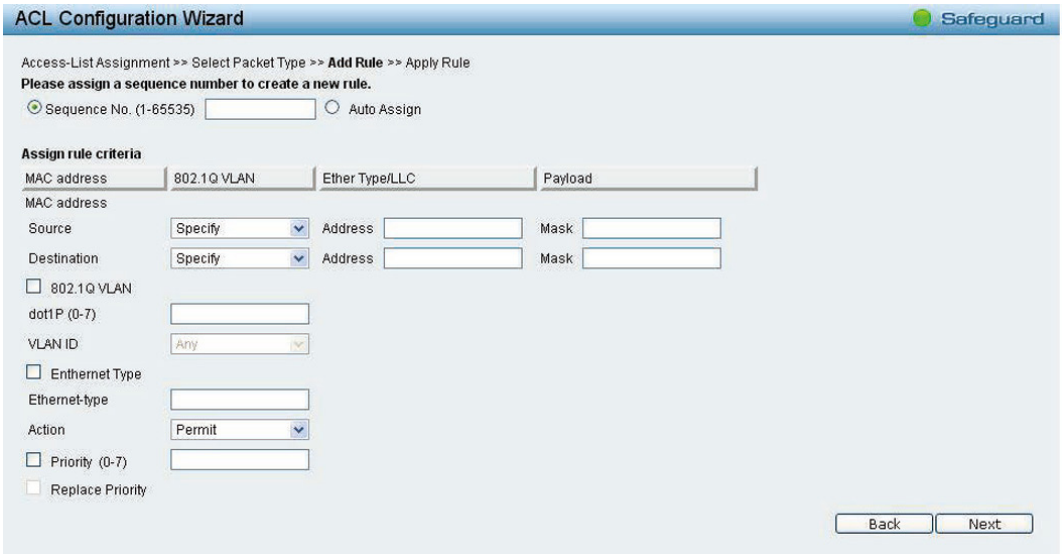


図 5-109　ACL Configuration Wizard - MAC ACL Rule 画面

■ 画面に表示される項目

項目	説明
Assign sequence number:（シークエンス番号の指定）	
Sequence No. (1-65535):	シークエンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign:	新規ルール用のシークエンス番号を自動でアサインします。
Assign Rule Criteria:（MAC アドレスの設定）	
Source:	送信元の MAC アドレスを指定、または「Any」に指定します。 MAC アドレスと MAC アドレスマスクを入力します。例）「FF-FF-FF-FF-FF-FF.」
Destination:	宛先の MAC アドレスを指定、または「Any」に指定します。 MAC アドレスと MAC アドレスマスクを入力します。例）「FF-FF-FF-FF-FF-FF.」

「802.1Q VLAN」を選択した場合、「dot1p」と「VLAN ID」を設定する必要があります。

項目	説明
Dot1p (0-7):	優先値を指定します。
VLAN ID:	転送の基準としてスイッチによるパケットヘッダの 802.1p 優先値を確認するオプションになります。

「Ethernet Type」を選択した場合、「Ethernet Type」の設定と「Action」を選択する必要があります。

項目	説明
Ethernet Type:	転送の基準としてスイッチによる各フレームヘッダのヘッダのイーサネット種類を確認するオプションになります。
Action:	ルールに合致した場合の ACL 転送動作を指定します。 • 「Permit」- パケットを転送します。 • 「Deny」- パケットを破棄します。

項目	説明
Priority (0-7):	MAC ACL の優先値を 0 から 7 の間で指定します。
Replace Priority:	チェックを入れ「Replace Priority」機能を有効にします。

「Next」をクリックし、設定した ACL プロファイルを追加します。

IPv4 ACL Rule の設定

IPv4 ACL Rule を設定します。
「IPv4」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

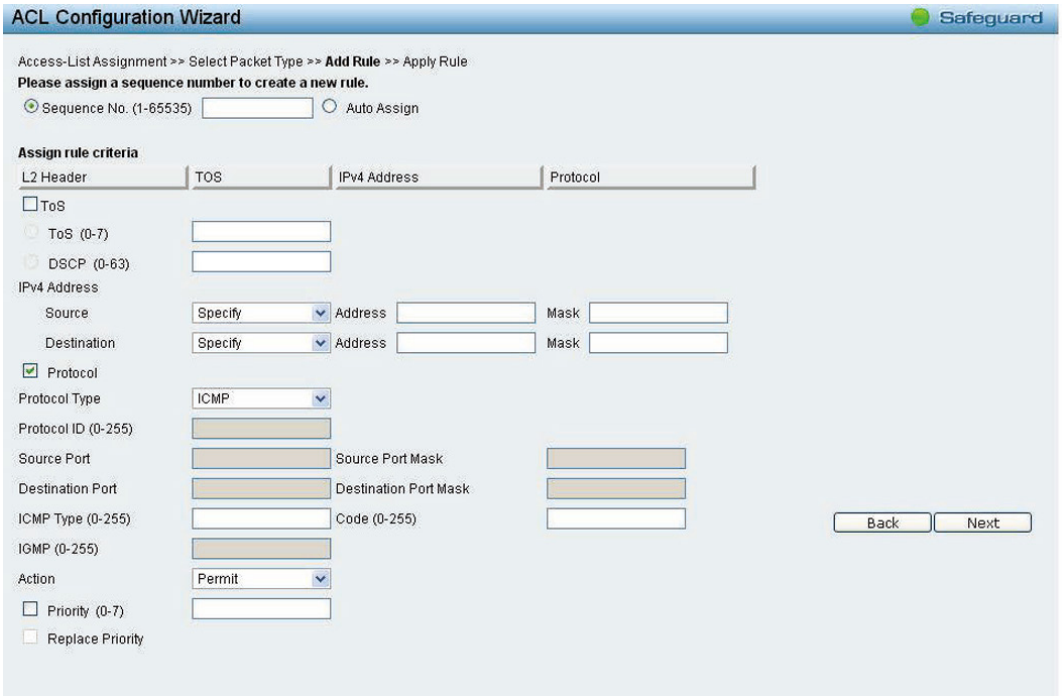


図 5-110　ACL Configuration Wizard -IPv4 画面

■ 画面に表示される項目

項目	説明
Assign sequence number:（シークエンス番号の指定）	
Sequence No. (1-65535):	シークエンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign:	新規ルール用のシークエンス番号を自動でアサインします。
Assign Rule Criteria:（IPv4 ACL の設定）	
ToS:	チェックを入れ ToS 優先値と DSCP 値の設定をします。
ToS (0-7):	ToS の値を入力します。
DSCP (0-63):	DSCP の値を入力します。
IPv4 Address（IPv4 宛先 / 送信元アドレスの指定）	
Source:	送信元 IPv4 アドレスを指定します。 Specify -「Specify」を選択し送信元 IPv4 アドレス / マスクを指定します。 Any - ACL ルールに沿った送信元 IPv4 アドレス / マスクが指定されます。
Destination:	宛先 IPv4 アドレスを指定します。 Specify -「Specify」を選択し宛先 IPv4 アドレス / マスクを指定します。 Any - ACL ルールに沿った宛先 IPv4 アドレス / マスクが指定されます。
Protocol（チェックを入れプロトコルの設定を行います。）	
Protocol Type	IPv4 のプロトコル種類を選択します。「ICMP」「IGMP」「TCP」「UDP」「Protocol ID」から選択可能です。

ICMP 選択時

ICMP Type (0-255)	ICMP Type を入力します。
Code (0-255)	ICMP code を入力します。

IGMP 選択時

IGMP Type (0-255)	IGMP Type を入力します。

TCP/UDP 選択時

Source Port	ACL ルールに関連した送信元ポートの範囲を指定します。

項目	説明
Source Port Mask	ACL ルールに関連した送信元ポートマスクを指定します。
Destination Port	ACL ルールに関連した宛先ポートの範囲を指定します。
Destination Port Mask	ACL ルールに関連した宛先ポートマスクを指定します。

Protocol ID 選択時

Protocol ID	プロトコル ID を指定します。
項目	説明
Priority (0-7):	優先値を 0 から 7 の間で指定します。
Replace Priority:	チェックを入れ「Replace Priority」機能を有効にします。

「Next」をクリックし、設定した ACL プロファイルを追加します。

注意　一つまたは複数のフィルタリングマスクは同時に設定可能です。

IPv6 ACL Rule の設定

IPv6 ACL Rule を設定します。
「IPv6」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

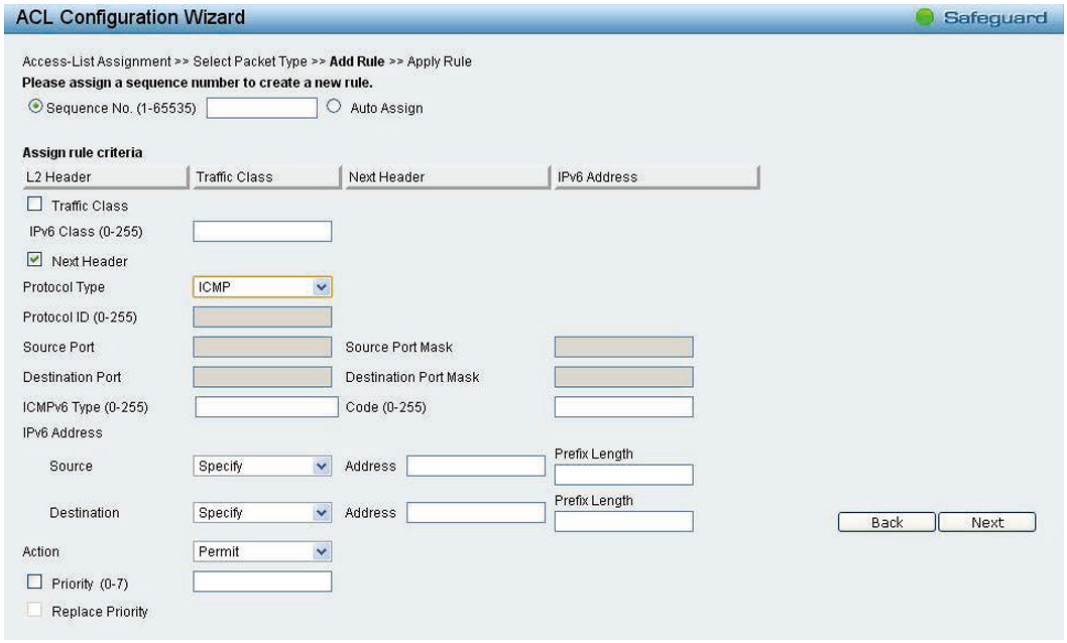


図 5-111　ACL Configuration Wizard -IPv6 画面

■ 画面に表示される項目

項目	説明
Assign sequence number:（シークエンス番号の指定）	
Sequence No. (1-65535):	シークエンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign:	新規ルール用のシークエンス番号を自動でアサインします。
Traffic Class	チェックを入れ Traffic Class の設定をします。
IPv6 Class	アクセスルールのクラスを指定します。範囲は 0 から 255 です。
Protocol（プロトコルの設定を行います。）	
Next Header	チェックを入れプロトコルタイプの指定を行います。
Protocol Type	IPv4 のプロトコル種類を選択します。「ICMP」「TCP」「UDP」「Protocol ID」から選択可能です。

ICMP 選択時

ICMPv6 Type (0-255)	ICMPv6 Type を入力します。
Code (0-255)	ICMP code を入力します。

項目	説明
TCP/UDP 選択時	
Source Port	ACL ルールに関連した送信元ポートの範囲を指定します。
Source Port Mask	ACL ルールに関連した送信元ポートマスクを指定します。
Destination Port	ACL ルールに関連した宛先ポートの範囲を指定します。
Destination Port Mask	ACL ルールに関連した宛先ポートマスクを指定します。
Protocol ID 選択時	
Protocol ID	プロトコル ID を指定します。
項目	説明
Priority (0-7):	優先値を 0 から 7 の間で指定します。
Replace Priority:	チェックを入れ「Replace Priority」機能を有効にします。
IPv6 Address（IPv6 宛先 / 送信元アドレスの指定）	
Source:	送信元 IPv6 アドレスを指定します。 Specify -「Specify」を選択し送信元 IPv6 アドレス / マスクを指定します。 Any - ACL ルールに沿った送信元 IPv6 アドレス / マスクが指定されます。 Prefix Length -「Specify」を選択時にプレフィクス長を入力します。
Destination:	宛先 IPv6 アドレスを指定します。 Specify -「Specify」を選択し宛先 IPv6 アドレス / マスクを指定します。 Any - ACL ルールに沿った宛先 IPv6 アドレス / マスクが指定されます。 Prefix Length -「Specify」を選択時にプレフィクス長を入力します。
Action:	ルールに合致した場合の ACL 転送動作を指定します。 • 「Permit」- パケットを転送します。 • 「Deny」- パケットを破棄します。
項目	説明
Priority (0-7):	優先値を 0 から 7 の間で指定します。

「Next」をクリックし、設定した ACL プロファイルを追加します。

4. アクセスリストを適用するポートを選択します。

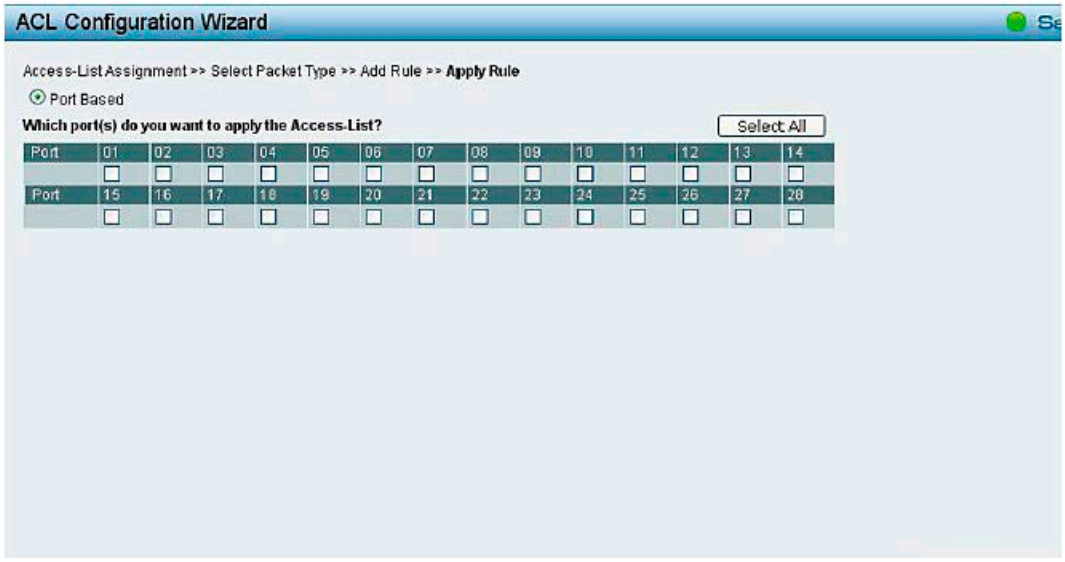


図 5-112　Add Access Rule – Ports 画面

「Next」をクリックし、設定した ACL プロファイルを追加します。

5. 既存のルールを編集する場合は、「Update」と「Access-List Name」を選択し「Next」をクリックします。

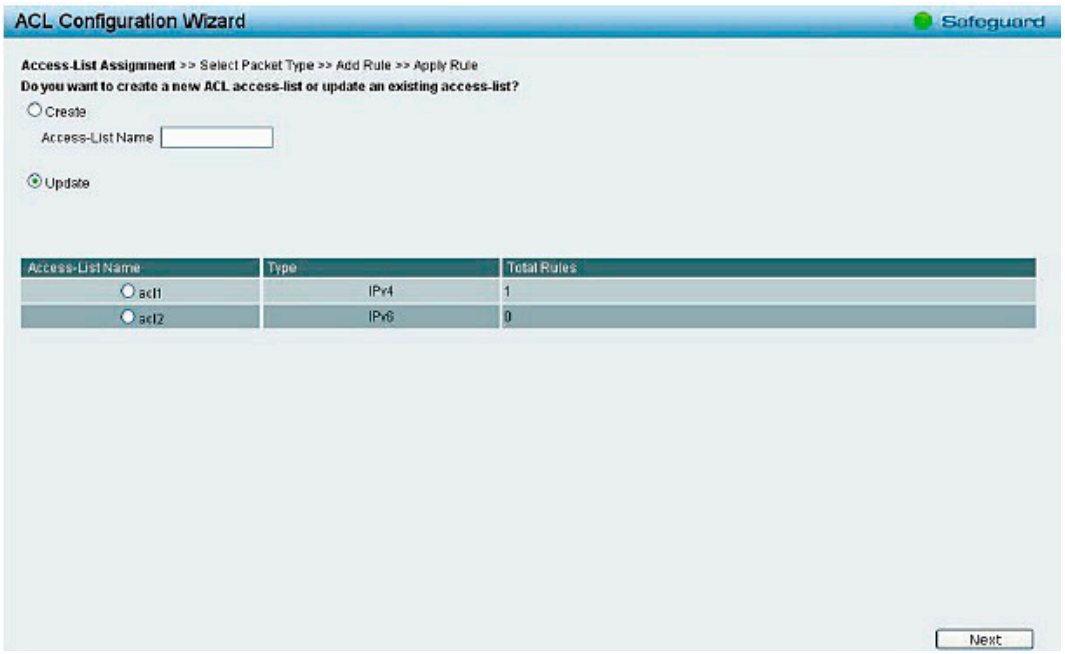


図 5-113　ACL Wizard – Update ACL List 画面

ACL Access List (ACL アクセスリスト)

ACL Access List (ACL アクセスリスト) は手動で ACL アクセスを設定します。

1. 「ACL」>「ACL Access List」の順にメニューをクリックします。

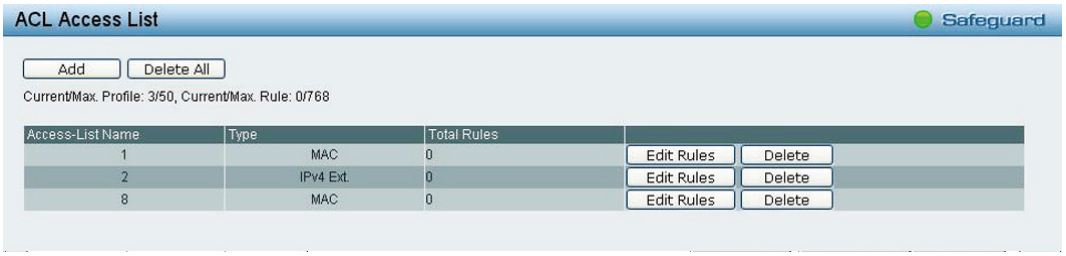


図 5-114　ACL Access List 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Add	ACL プロファイルのルールを追加します。
Delete All	すべての ACL プロファイルを削除します。
Edit Rules	ACL プロファイルのルールを編集します。
Delete	ACL プロファイルを削除します。

3. 新しいプロファイルを追加する場合、「Add」をクリックして以下の画面を表示します。

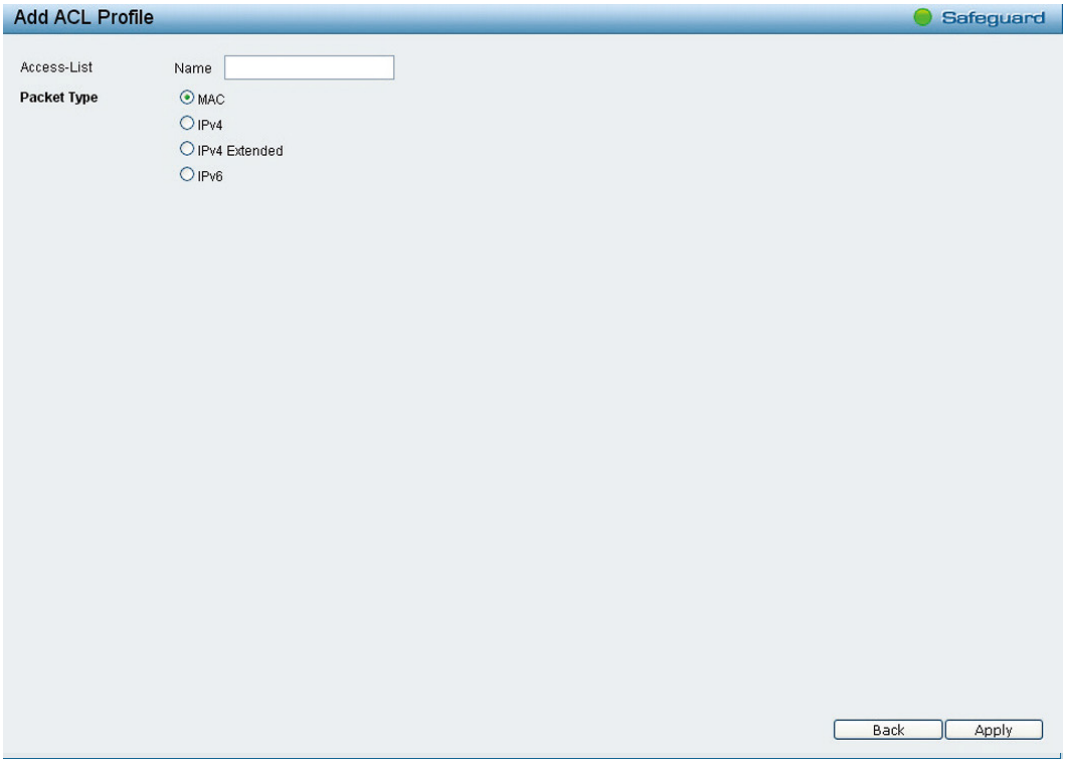


図 5-115　Add ACL Profile 画面

■ 画面に表示される項目

項目	説明
Access-List:	ACL プロファイルに追加するアクセスリストの名前を指定します。
Packet Type:	パケットの種類を「MAC」「IPv4」「IPv4 Exdended」「IPv6」から選択し「Apply」をクリックします。

4. 既存のルールを編集する場合はシークエンス番号のハイパーリンクをクリックします。

図 5-116　ACL Access List – Update ACL Profile 画面

ACL Access Group（ACL アクセスグループ）

ACL アクセスグループの設定を行います。

1. 「ACL」>「ACL Access Group」の順にメニューをクリックします。

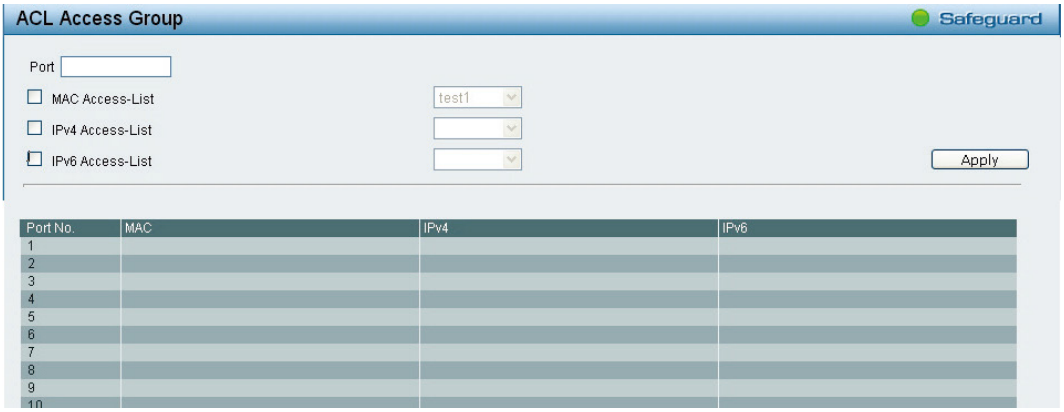


図 5-117　ACL Access Group 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Port	アクセスリストグループに追加するポートを指定します。
MAC Access-List	MAC アクセスリストグループに指定のポートを追加します。
IPv4 Access-List	IPv4 アクセスリストグループに指定のポートを追加します。
IPv6 Access-List	IPv6 アクセスリストグループに指定のポートを追加します。

3. 「Apply」をクリックし、設定を有効にします。

ACL Hardware Resource Status（ACL ハードウェアリソースステータス）

ACL Hardware Resource Status（ACL ハードウェアリソースステータス）では ACL ハードウェアリソース状態を表示します。

図 5-118　ACL Hardware Resource Status 画面

PoE（PoE の設定）（DGS-1210-10P/28P のみ）

■ PoE の設定項目

- PoE Global Settings（PoE グローバル設定）
- PoE Port Settings（PoE ポート設定）

PoE Global Settings（PoE グローバル設定）

PoE の 設定を行います。
また、RPS ステータス、システム総供給可能電力、使用電力、残電力およびシステム電力供給率を含む PoE ステータスを表示します。

1. 「PoE」>「PoE Global Settings」の順にメニューをクリックします。

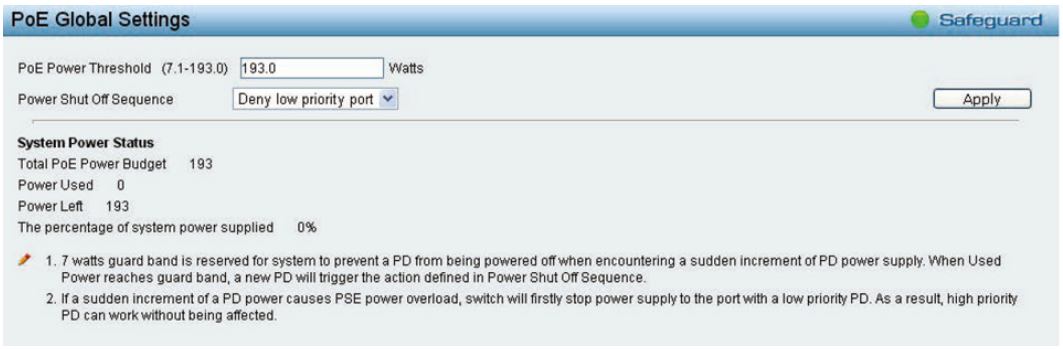


図 5-119　PoE Global Settings 画面（DGS-1210-28P）

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
PoE Power Threshold	システムの給電可能電力を設定します。 7.1 ~ 78.0W（DGS-1210-10P）、7.1 ~ 193.0W（DGS-1210-28P）の間で設定可能です。
Power Shut Off Sequence	最大電力に達した場合に、ポートへの電力停止を行う方法を定義します。 選択肢：「Deny next port」「Deny low priority port」 • Deny next port 最大電力に達した場合、ポートの優先度に関わらず次のポートには給電されません。 • Deny low priority port 低い優先度を持つポートはシャットダウンされ、高い優先度を持つポートに給電されます。
System Power Status	
Total PoE Power Budget	本スイッチの総 PoE 給電可能電力を表示します。
Power Used	本スイッチの現在の使用電力を表示します。
Power Left	本スイッチの残電力を表示します。
The percentage of system power supplied	スイッチにおけるシステムの供給電力 (%) を表示します。

3. 「Apply」をクリックし、設定を有効にします。

PoE Port Settings（PoE ポート設定）

DGS-1210-10P/28P は、IEEE で定義される PoE（Power over Ethernet）をサポートしています。
EEE 802.3af および 802.3at 標準規格に準拠する PD デバイスに対して電源を供給します。
EEE 802.3at では、PSE（給電機器）が以下の電力クラスに応じた給電を行うことを定義しています。

クラス	用途	PSE の最大出力電力
0	初期値	15.4W
1	オプション	4.0W
2	オプション	7.0W
3	オプション	15.4W
4	リザーブ	30.0W

各機種のポートの供給可能電力は以下のとおりです。
DGS-1210-10P：全ポート：最大 30W
DGS-1210-28P：1 ～ 4 ポート：最大 30W、5 ～ 24 ポート：最大 15.4 W

1. 「PoE」>「PoE Port Settings」の順にメニューをクリックします。

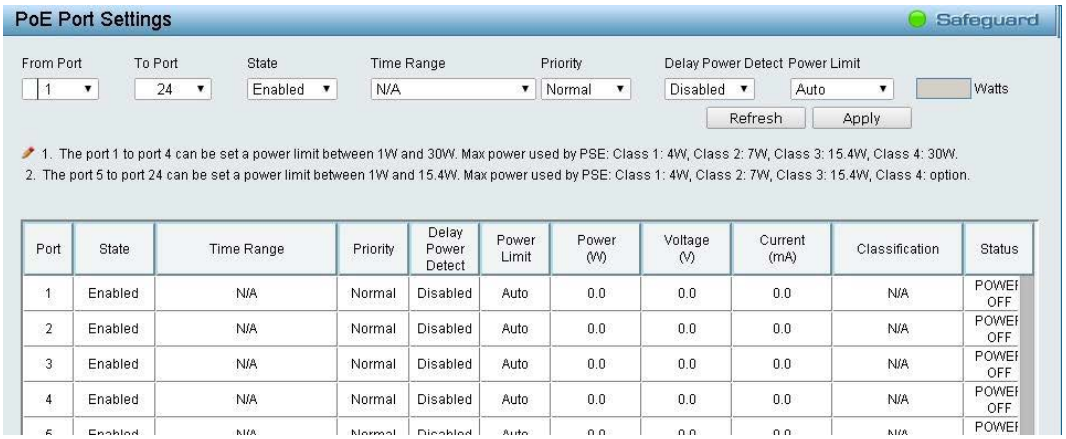


図 5-120　PoE Port Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port / To Port	設定を行うポートの範囲を指定します。
State	PoE を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Enabled」
Time Range	指定したポートに、PoE 機能を自動で有効 / 無効にする時間範囲を設定します。 初期値：「N/A」
Priority	指定ポートの電力供給の優先度を指定します。 選択肢：「Low」、「Normal」、「High」 初期値：「Normal」
Delay Power Detect	電力供給遅延の検出を「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
Power limit	接続する PD デバイスに適用する給電量の制限を設定します。 本機能により、過負荷発生時にはそのポートの PoE 機能が無効になり、本製品と接続する PD デバイスを保護します。 選択肢：「Class 1」、「Class 2」、「Class 3」、「Class 4」、「Auto」、「User Define」 • Auto 接続デバイスとネゴシエーションを行い、IEEE 802.3af に基づいたクラス分けが行われます。 • Class 1、Class 2、Class 3、Class4 「Class 1」（4W）、「Class 2」（7W）、「Class 3」（15.4W）、「Class 4」（30W）が適用されます。 • User Define 手動でポートの電力の上限値を割り当てます。

3. 「Apply」をクリックし、設定を有効にします。

「Refresh」をクリックすると、表示内容を更新できます。

SNMP（SNMP の設定）

■ SNMP の設定項目

- SNMP（SNMP 設定）
- RMON（RMON 設定）

SNMP（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）のプロトコルです。
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やルータなどのネットワークデバイスの設定状態の確認・変更をします。SNMP を利用して、スイッチまたは LAN に対し、適切な操作のための設定、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。

注意 ハードウェアリミテーションによりユーザートラフィックもしくは装置の高負荷時に WebGUI の表示が遅延または表示できない場合、Ping、SNMP に応答できない場合があります。

SNMP Global Settings（SNMP グローバル設定）

SNMP グローバル設定を行います。

1. 「SNMP」>「SNMP」>「SNMP Global Settings」の順にメニューをクリックします。

図 5-121　SNMP Global Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
SNMP Global Settings	
Enabled / Disabled	トラップを「Enabled」（有効）または「Disabled」（無効）にします。 初期値：「Disabled」
Trap Settings	
デバイスが SNMP 通知を送信するかどうかを指定します。	

項目	説明
Event	トラップするイベントを選択します。 • SNMP Authentication Traps 認証エラー通知を送信します。 • Device Bootup 起動通知を送信します。 • Port Link Up/Link Down ポートのリンクアップまたはリンクダウンの際に通知を送信します。 • RSTP Port State Change RSTP ポートの状態が変更する場合に、通知を送信します。 • Firmware Upgrade State ファームウェアの更新時に通知を送信します。 • PoE Power On / Off* PoE の状態を有効 / 無効にした場合に、通知を送信します。 • PoE Power Error * 以下の PoE 電源エラーが発生した場合に、通知を送信します。 - 電力が過負荷になったとき - 漏電がおきたとき - サーマルシャットダウンがおきたとき - 電力供給の拒否がおきたとき （電力供給量が最大に達しているときに新しい受電装置が接続された場合、拒否が実行されます。） • PoE over max power budget * 受電装置に給電をしていて最大供給可能電力に達したときに、通知を送信します。 • Loopback Detection occuring / recovery ループバックが発生 / 復旧した場合に通知を送信します。

*DGS-1210-10P/28P でのみ表示されます。

3. 「Apply」をクリックし、設定を有効にします。

SNMP User（SNMP ユーザ設定）

SNMPv3 で使用する SNMP ユーザテーブルを保持します。
SNMPv3 は MIB OID を使用してユーザの許可または制限を行い、ユーザとスイッチ間で送出される SNMP メッセージを暗号化します。

1. 「SNMP」>「SNMP」>「SNMP User」の順にメニューをクリックします。

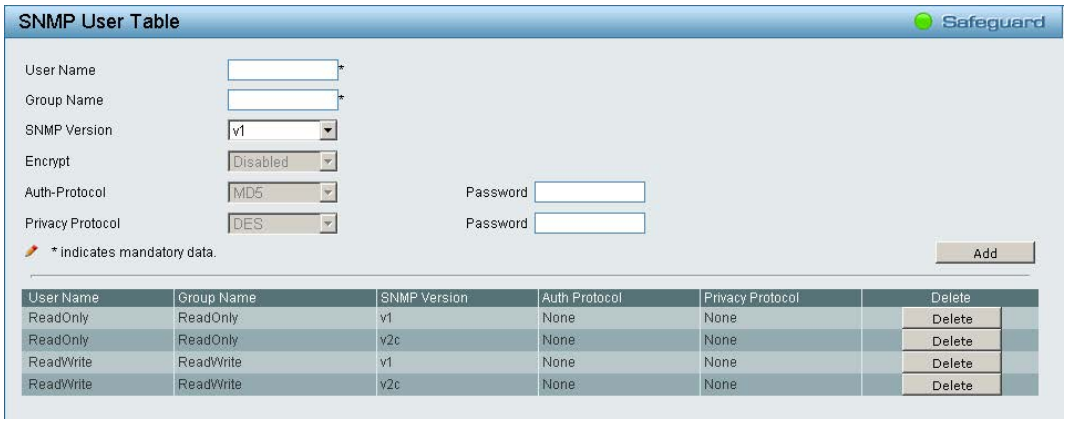


図 5-122　SNMP User Table 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
User Name	SNMP ユーザ名（最大 32 文字）を入力します。
Group Name	SNMP ユーザの SNMP グループを指定します。
SNMP Version	ユーザの SNMP バージョン（v1、v2c、v3）を指定します。SNMPv3 のみがメッセージを暗号化します。
Encrypt	暗号化を「Enabled」(有効) または「Disabled」(無効) にします。

項目	説明
Auth-Protocol/ Password	認証プロトコルとして、「MD5」または「SHA」を指定します。 • 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。 補足 本項目は「SNMP Version」で「v3」を選択し、「Encrypt」を「Enabled」に設定した場合に有効になります。 本項目を選択後、右の欄には SNMPv3 暗号化のためのパスワードを入力します。
Privacy Protocol/ Password	「none」または「DES」暗号化を指定します。 • 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。 補足 本項目は「SNMP Version」で「v3」を選択し、「Encrypt」を「Enabled」に設定した場合に有効になります。 本項目を選択後、右の欄には SNMPv3 暗号化のためのパスワードを入力します。

エントリの登録を行う場合

1. 設定項目を入力します
2. 「Add」をクリックします。

エントリの削除を行う場合

1. エントリの「Delete」をクリックします。

SNMP Group（SNMP グループ設定）

「SNMP User Table」内のユーザに関連する「SNMP Group Table」を保持します。
SNMPv3 は、ユーザグループの MIB アクセスポリシー、セキュリティポリシーを直接制御できます。

1. 「SNMP」>「SNMP」>「SNMP Group」の順にメニューをクリックします。

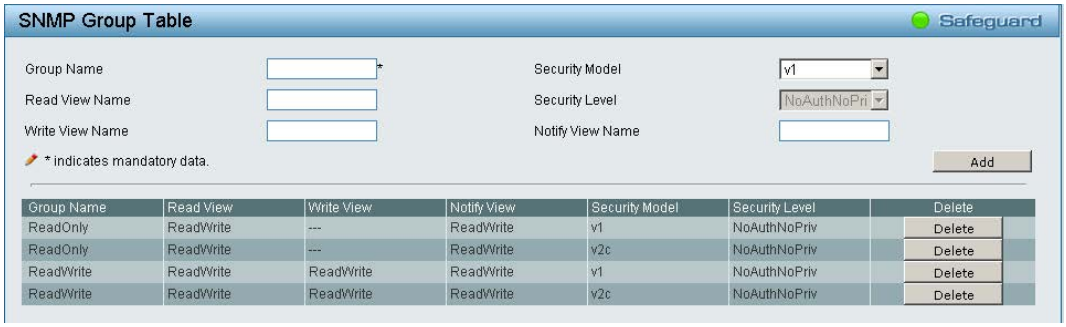


図 5-123　SNMP Group Table 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Group Name	SNMP ユーザグループ（最大 32 文字）を指定します。
Read View Name	スイッチの SNMP エージェントに読み取り権限を与えるユーザの SNMP グループ名を入力します。
Write View Name	SNMP エージェントに書き込み権限を与える SNMP グループ名を入力します。
Security Model	SNMP セキュリティモデルを選択します。 選択肢：「v1」「v2c」「v3」 • v1 SNMPv1 はセキュリティ機能をサポートしません。 • v2c SNMPv2c は、集中型、分散型どちらのネットワーク管理方法にも対応します。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。 • v3 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	本機能は、SNMPv3 セキュリティレベルを選択する場合にのみ利用可能です。 選択肢：「NoAuthNoPriv」「AuthNoPriv」「AuthPriv」 • NoAuthNoPriv スイッチと SNMP マネージャ間で送信されるパケットには認証または暗号化はありません。 • AuthNoPriv スイッチとリモート SNMP マネージャ間で送信されるパケットに対して認証は要求されますが、暗号化はありません。 • AuthPriv スイッチとリモート SNMP マネージャ間で送信されるパケットに対して認証および暗号化が要求されます。
Notify View Name	SNMP エージェントによるトラップメッセージを送信する SNMP グループ名を入力します。

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

1. エントリの「Delete」をクリックします。

SNMP View（SNMP ビュー設定）

SNMP ビューでは、MIB ツリーのどの部分をリモート SNMP マネージャからアクセスできるようにするかを指定することができます。

1. 「SNMP」>「SNMP」>「SNMP View」の順にメニューをクリックします。

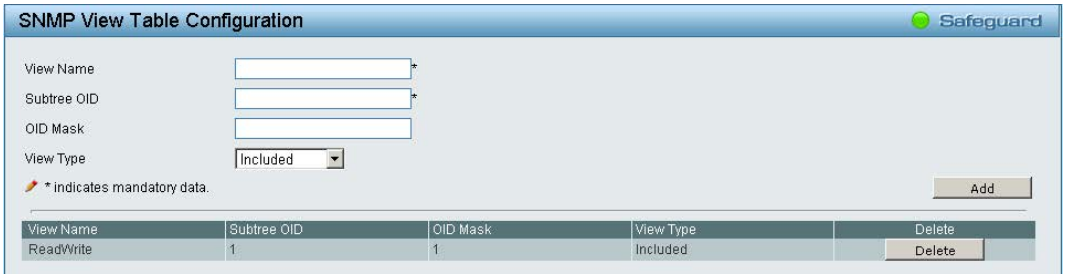


図 5-124　SNMP View Table Configuration 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
View Name	ビュー名 (32 文字以内) を設定します。
Subtree OID	ビューの OID (Object Identifier) サブツリーを指定します。 「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。
OID Mask	Subtree OID のマスクを設定します。 1 はこのオブジェクト番号は関連することを意味し、0 は関連しないことを意味します。 例：マスク 1.1.1.1.1.1 を持つ .0 1.3.6.1.2.1.1 は 1.3.6.1.2.1.X を意味します。
View Type	ビュータイプを設定します。 選択肢：「Included」「Excluded」 • Included 設定した OID を SNMP マネージャからのアクセスに含めます。 • Excluded 設定した OID を SNMP マネージャからのアクセスから除外します。

SNMP ビューの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

SNMP ビューの削除を行う場合

1. 「Delete」をクリックします。

SNMP Community（SNMP コミュニティ設定）

スイッチの SNMP コミュニティ名を設定します。
同じコミュニティ名を使用している SNMP マネージャは、スイッチの SNMP エージェントへのアクセスを許可されます。

1. 「SNMP」>「SNMP」>「SNMP Community」の順にメニューをクリックします。

図 5-125　SNMP Community Table 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Community Name	コミュニティ名を入力します。
User Name (View Policy)	SNMP コミュニティにアクセス可能な MIB オブジェクトに対して、レベルの権限を指定します。 初期値：「ReadOnly」 選択肢：「ReadWrite」（読み込み / 書き込み）、「ReadOnly」（読み込みのみ）

SNMP コミュニティの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

SNMP コミュニティの削除を行う場合

1. 「Delete」をクリックします。

SNMP Host（SNMP ホスト）

SNMP トラップの受信者を設定します。

1. 「SNMP」>「SNMP」>「SNMP Host」の順にメニューをクリックします。

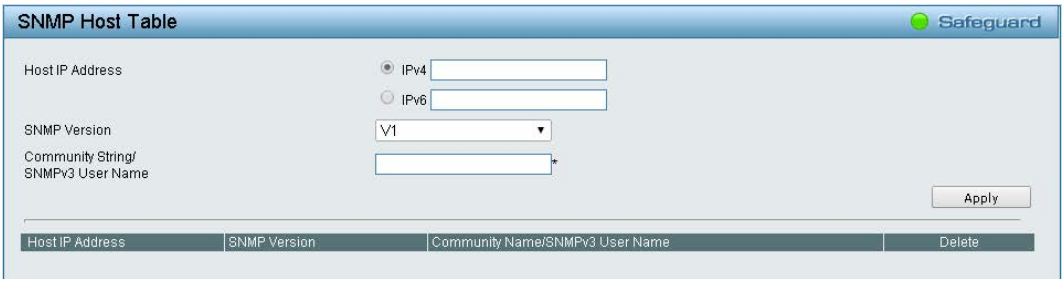


図 5-126　SNMP Host Table 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Host IP Address	IPv4 または IPv6 を選択し、SNMP 管理ホストの IP アドレスを指定します。
SNMP Version	管理ホストに使用する SNMP バージョンを指定します。 選択肢：「V1」「V2c」「V3-NoAuthNoPriv」「V3-AuthNoPriv」「V3-AuthPriv」
Community String/SNMPv3 User Name	管理ホストのコミュニティストリング、または SNMPv3 ユーザ名を指定します。

3. 「Apply」をクリックし、設定を有効にします。

SNMP Engine ID（SNMP エンジン ID）

SNMP エンジン ID を設定します。エンジン ID は、スイッチの SNMPv3 を確認するのに使用される固有の識別子です。

1. 「SNMP」>「SNMP」>「SNMP Engine ID」の順にメニューをクリックします。

図 5-127　SNMP Engine ID 画面

2. 「Engine ID」を入力します。

補足 「Engine ID」には、0 ～ 9 の数字と a ～ f の英字が入力できます。入力可能な長さは 10 ～ 64 以内です。

3. 「Apply」をクリックし、設定を有効にします。

設定を初期値に戻す場合は、「Default」をクリックします。

RMON（RMON 設定）

RMON Global Settings（RMON グローバル設定）

スイッチの SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効または無効にします。

1. 「SNMP」>「RMON」>「RMON Global Settings」の順にメニューをクリックします。

図 5-128　RMON Global Settings 画面

2. 「Enabled」(有効) または「Disabled」(無効) を選択します。
3. 「Apply」をクリックし、設定を有効にします。

RMON Statistics（RMON 統計情報）

RMON イーサネット統計情報を表示して、設定を許可します。

1. 「SNMP」>「RMON」>「RMON Statistics」の順にメニューをクリックします。

図 5-129　RMON Ethernet Statistics Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Index (1 - 65535)	RMON イーサネット統計情報エントリの番号を指定します。
Port	RMON 情報を取得したポートを指定します。
Owner	RMON 情報を要求した RMON ステーションまたはユーザを表示します。

統計情報の登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。
   登録した内容は下の表に表示されます。

統計情報の削除を行う場合

1. 「Delete」をクリックします。

統計情報の更新を行う場合

1. 「Refresh」をクリックします。

RMON History（RMON ヒストリ）

ポートから RMON のヒストリ（履歴）情報を取得するための制御設定を行います。

1. 「SNMP」>「RMON」>「RMON History」の順にメニューをクリックします。

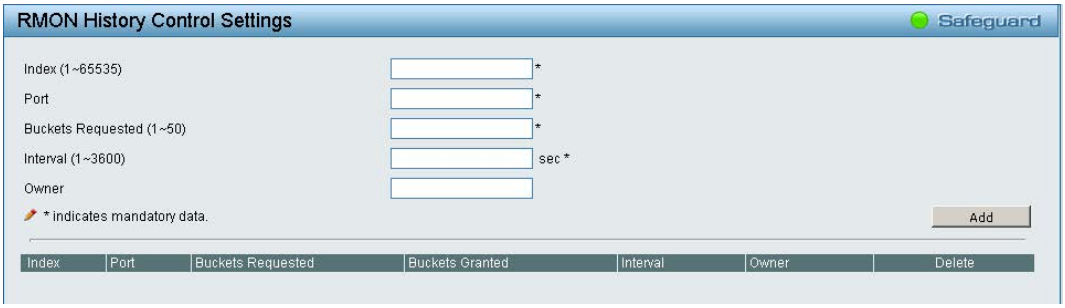


図 5-130　RMON History Control Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Index (1 - 65535)	ヒストリ制御エントリ番号を指定します。
Port	RMON 情報を取得したポートを指定します。
Buckets Requested (1~50)	デバイスが保存するバケット数を指定します。
Interval (1~3600)	ポートからサンプリングする間隔（秒）を設定します。 初期値：1800 (秒) 入力可能範囲：1-3600 (秒)
Owner	RMON 情報を要求した RMON ステーションまたはユーザを表示します。

登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。
   登録した内容は下の表に表示されます。

削除を行う場合

1. 「Delete」をクリックします。

RMON Alarm Settings（RMON アラーム設定）

ネットワークアラームを設定します。ネットワークの問題またはイベントが検出されると、ネットワークアラームが発生します。

1. 「SNMP」>「RMON」>「RMON Alarm」の順にメニューをクリックします。

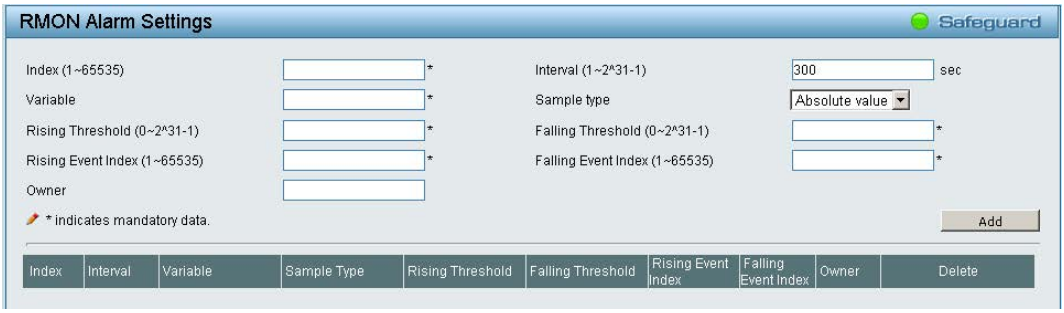


図 5-131　RMON Alarm Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Index (1-65535)	特定のアラームを指定します。
Variable	選択した MIB 変数の値を指定します。
Rising Threshold (0~2^31-1)	上昇しきい値を設定します。
Rising Event Index (1~65535)	上昇しきい値を超えたときに始動するイベントを設定します。 設定可能な項目は、ユーザ定義の RMON イベントです。
Owner	アラームを定義したデバイスまたはユーザを表示します。
Interval (1~2^31-1)	アラームの間隔（秒）を定義します。
Sample type	選択した変数に対するサンプリング方式としきい値と比較する値を定義します。 選択肢：「Delta value」「Absolute value」 • Delta value 現在の値から最後にサンプリングされた値を引きます。値の差がしきい値と比較されます。 • Absolute value サンプリング間隔の終わりで値を直接しきい値と比較します。
Falling Threshold (0 ~ 2^31-1)	下降しきい値を設定します。
Falling Event Index (1 ~ 65535)	下降しきい値を超えたときに始動するイベントを設定します。 設定可能な項目は、ユーザ定義の RMON イベントです。

アラームの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。
   登録した内容は下の表に表示されます。

アラームの削除を行う場合

1. 「Delete」をクリックします。

RMON Event（RMON イベント）

RMON イベント統計情報の定義、編集、および参照を行います。

1. 「SNMP」>「RMON」>「RMON Event」の順にメニューをクリックします。

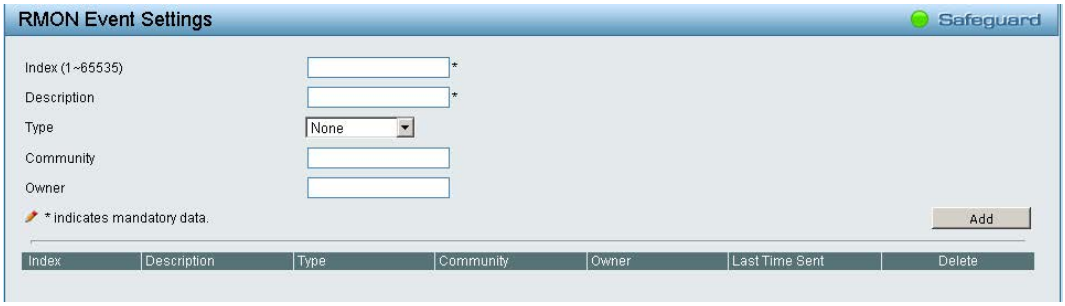


図 5-132　RMON Event Settings 画面

2. 設定したい内容に応じて、以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Index (1~65535)	イベントを指定します。
Description	ユーザ定義のイベントの記述を指定します。
Type	イベントタイプを指定します。 選択肢：「None」「Log」「SNMP Trap」「Log and Trap」 • None イベントが発生しなかったことを示します。 • Log イベントがログエントリであることを示します。 • SNMP Trap イベントがトラップであることを示します。 • Log and Trap イベントがログエントリとトラップの両方であることを示します。
Community	イベントが所属するコミュニティを指定ます。
Owner	イベントが発生した時間を指定します。

3. 「Add」をクリックし、設定内容を保存します。

設定内容を削除する場合は、「Delete」をクリックします。

アラームの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。
登録した内容は下の表に表示されます。

アラームの削除を行う場合

1. 「Delete」をクリックします。

Monitoring（スイッチのモニタリング）

■ Monitoring の設定項目

- Port Statistics（ポート統計情報）
- Cable Diagnostics（ケーブル診断）
- System Log（システムログ）

Port Statistics（ポート統計情報）

各ポートのパケットカウント統計情報を表示します。

1. 「Monitoring」>「Port Statistics」の順にメニューをクリックします。

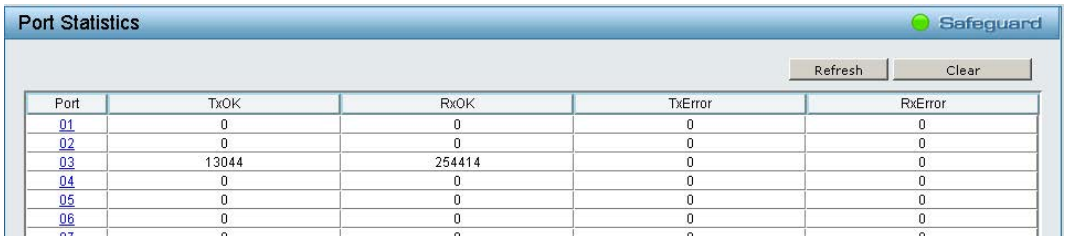


図 5-133　Port Statistics 画面

■ 画面に表示される項目

項目	説明
Port	ポート数が表示されます。
TxOK	正常に送信されたパケット数が表示されます。
RxOK	正常に受信されたパケット数が表示されます。
TxError	エラーが発生した送信パケット数が表示されます。
RxError	エラーが発生した受信パケット数が表示されます。

2. 「Port」欄のリンクをクリックすると、以下の画面で各ポートの詳細情報を表示できます。

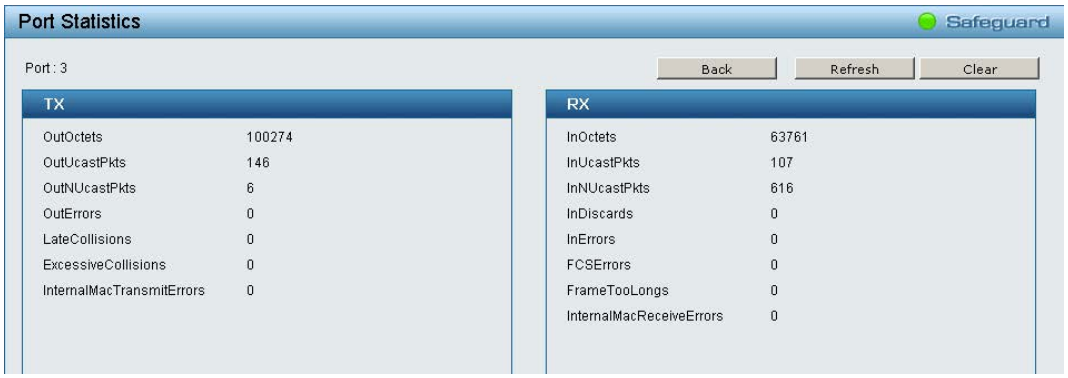


図 5-134　Port Statistics 画面

「Back」をクリックすると、手順 1 の画面に戻ります。

3. 表示を更新する場合は「Refresh」をクリックします。
表示をリセットする場合は「Clear」をクリックします。

Cable Diagnostics（ケーブル診断）

スイッチに接続しているケーブルの状態を診断します。
イーサネットケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。

1. 「Monitoring」>「Cable Diagnostics」の順にメニューをクリックします。

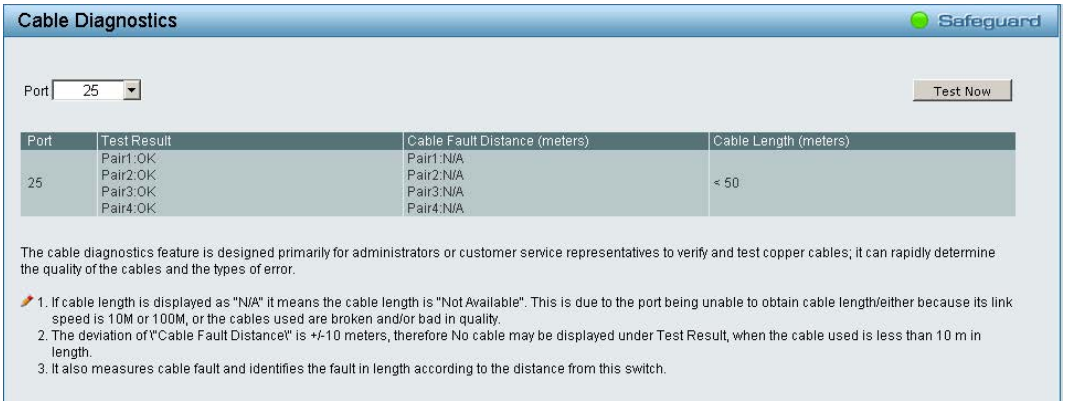


図 5-135　Cable Diagnostics 画面

2. 「Port 」でケーブル診断を行うポートを選択します。

3. 「Test Now」をクリックし、ケーブル診断を実行します。

4. ケーブル診断の結果を確認します。

■ 画面に表示される項目

項目	説明
Test Result	ケーブル診断の結果が表示されます。 • OK ケーブルの状態に問題はありません。 • Open in Cable UTP ケーブルが断線しているか、接続が外れています。 • Short in Cable UTP ケーブルが接触しています。 • Test Failed ケーブル診断中に他のエラーが発生しました。 再度同じポートを選択して診断を行ってください。
Cable Fault Distance (meters)	スイッチポートからケーブル故障点までの距離を示します。 ケーブルが 2 メートル未満の場合は「No Cable」と表示されます。
Cable Length (meter)	診断結果でケーブルが「OK」の場合、ケーブルの全長を示します。 ケーブルの長さは以下の 4 つに分類されます。 • 50 メートル未満 • 50 ～ 80 メートル • 80 ～ 100 メートル • 100 メートル以上

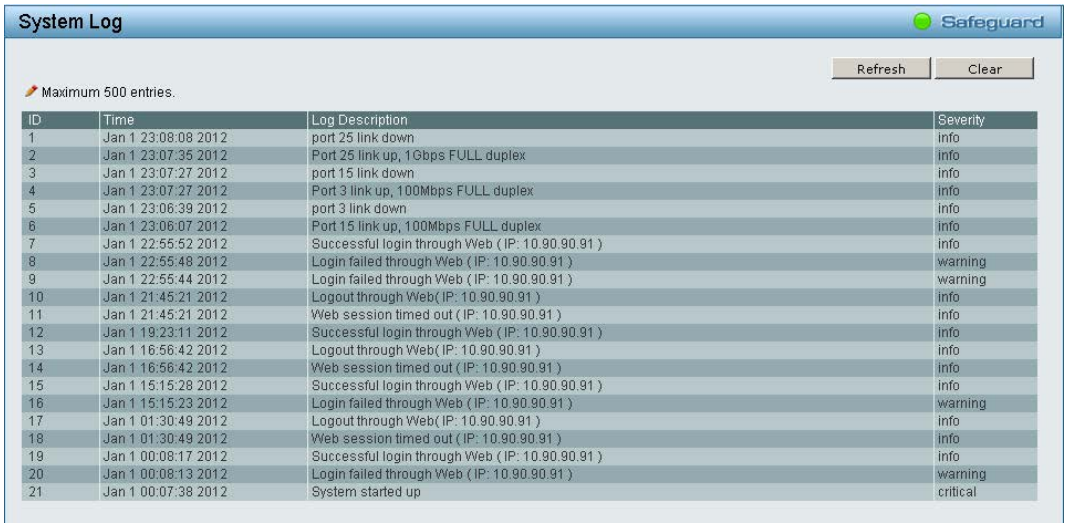
注意　ケーブル長の検出機能をサポートしているのはギガビットポートのみです。

注意　ケーブル診断機能を使用する場合は、事前に Power Saving（省電力設定）機能を無効にしてください。

System Log（システムログ）

デバイスの起動、ポートの動作方法、ユーザのログインした時間、セッションがタイムアウトした時間などのログを表示します。

1. 「Monitoring」>「System Log」の順にメニューをクリックします。



ID	Time	Log Description	Severity
1	Jan 1 23:08:08 2012	port 25 link down	info
2	Jan 1 23:07:35 2012	Port 25 link up, 1Gbps FULL duplex	info
3	Jan 1 23:07:27 2012	port 15 link down	info
4	Jan 1 23:07:27 2012	Port 3 link up, 100Mbps FULL duplex	info
5	Jan 1 23:06:39 2012	port 3 link down	info
6	Jan 1 23:06:07 2012	Port 15 link up, 100Mbps FULL duplex	info
7	Jan 1 22:55:52 2012	Successful login through Web (IP: 10.90.90.91)	info
8	Jan 1 22:55:48 2012	Login failed through Web (IP: 10.90.90.91)	warning
9	Jan 1 22:55:44 2012	Login failed through Web (IP: 10.90.90.91)	warning
10	Jan 1 21:45:21 2012	Logout through Web(IP: 10.90.90.91)	info
11	Jan 1 21:45:21 2012	Web session timed out (IP: 10.90.90.91)	info
12	Jan 1 19:23:11 2012	Successful login through Web (IP: 10.90.90.91)	info
13	Jan 1 16:56:42 2012	Logout through Web(IP: 10.90.90.91)	info
14	Jan 1 16:56:42 2012	Web session timed out (IP: 10.90.90.91)	info
15	Jan 1 15:15:28 2012	Successful login through Web (IP: 10.90.90.91)	info
16	Jan 1 15:15:23 2012	Login failed through Web (IP: 10.90.90.91)	warning
17	Jan 1 01:30:49 2012	Logout through Web(IP: 10.90.90.91)	info
18	Jan 1 01:30:49 2012	Web session timed out (IP: 10.90.90.91)	info
19	Jan 1 00:08:17 2012	Successful login through Web (IP: 10.90.90.91)	info
20	Jan 1 00:08:13 2012	Login failed through Web (IP: 10.90.90.91)	warning
21	Jan 1 00:07:38 2012	System started up	critical

図 5-136　Cable Diagnostics 画面

2. ログを確認します。

■ 画面に表示される項目

項目	説明
ID	記録されたシステムログエントリの番号です。最大数は 500 です。
Time	スイッチに発生したイベントの日時を表示します。
Log Description	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。
Severity	ヒストリログエントリの重要性レベルを表示します。

3. 表示を更新する場合は「Refresh」をクリックします。
表示をリセットする場合は「Clear」をクリックします。

第 6 章　コマンドラインインタフェース

スイッチはコマンドラインインタフェース（CLI）をサポートしており、ネットワーク上で Telnet プロトコルを使用して、基本的な管理やモニタリングを行うことができます。

接続とログイン

Telnet 経由でスイッチに接続する

1. スイッチとコンピュータがネットワークで接続していることを確認します。
2. 接続にはターミナルソフトウェア（例 : Windows OS に搭載のハイパーターミナル）、またはコマンドプロンプトを使用して「telnet」コマンドを入力し、スイッチの IP アドレスを続けて 入力します。（例：telnet 10.90.90.90）
3. ログインプロンプトが表示されます。

コマンドラインインタフェースにログインする

ユーザ名とパスワードを使ってログインします。ユーザ名とパスワードの初期値は「admin」です。ユーザ名とパスワードは大文字と小文字を区別します。ユーザ名とパスワードの両項目で「Enter」を押します。コマンドプロンプトが以下のように表示されます。

```
DGS-1210-52 login: admin
Password:

DGS-1210-52>
```

ログインタイムアウト時間が過ぎると自動的にログアウトします。ログインタイムアウト時間の初期値は 5 分です。ログインタイムアウト時間の変更は System Settings（スイッチの基本機能の設定）を参照してください。

コマンド

CLI コマンドについて

コマンドラインインタフェース (CLI) における基本的なスイッチコマンドとそのパラメータは以下の通りです。

コマンド	パラメータ
?	
download	{ firmware_fromTFTP | cfg_fromTFTP } {<ipaddr> | <ipv6addr>} <path_filename>
upload	{ firmware_fromTFTP | cfg_fromTFTP } {<ipaddr> | <ipv6addr>} <path_filename>
config ipif system	{ ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp | bootp}
config ipif system	{ ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client [enable | disable] }
logout	
ping	<ip_addr>
ping6	<ipv6_addr>
create iproute	default <ipaddr>
delete iproute	{default}
show iproute	{ <ipaddr> | static }
reboot	
reset config	
show ipif	[ipif_name<string>]
show switch	
config account admin password	<passwd>
save	
debug info	

各コマンドの詳細は以下の通りです。

?

目的

コマンドのリストを表示します。

構文

?

説明

スイッチのコマンドリストを表示します。

パラメータ

なし

使用例

```
DGS-1210-52> ?
USEREXEC commands :
  config account admin password <passwd>
  config ipif System { ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp | bootp}
  debug info
  download { firmware_fromTFTP tftp://ip-address/filename | cfg_fromTFTP tftp://ip-address/filename }
  logout
  ping <ip_addr>
  reboot
  reset config
  save
  show ipif [ipif_name<string>]
  show switch
  upload { firmware_toTFTP tftp://ip-address/filename | cfg_toTFTP tftp://ip-address/filename }
DGS-1210-52>
```

download

目的

TFTP サーバから新しいファームウェア、ブートまたは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してインストールします。

構文

download { firmware_fromTFTP | cfg_fromTFTP } {<ipaddr> | <ipv6addr>} <path_filename>

説明

TFTP サーバから新しいファームウェア、ブートまたは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します。

パラメータ

パラメータ	説明
firmware_fromTFTP	新しいファームウェアを TFTP サーバからスイッチにダウンロードしてインストールします。
cfg_fromTFTP	新しいコンフィグレーションファイルを TFTP サーバからスイッチにダウンロードしてインストールします。
<ipaddr>	TFTP サーバの IPv4 アドレスを指定します。
<ipv6addr>	TFTP サーバの IPv6 アドレスを指定します。
<path_filename>	ファームウェアファイルのパスとファイル名を指定します。ファイルが TFTP サーバにのルートディレクトリにない場合、DOS パスを指定する必要があります。

制限事項

なし

使用例

ファームウェアファイルをダウンロードします。

```
DGS-1210-52> download firmware_fromTFTP 10.90.90.100 DGS-1210-52-B1-3-10-013.hex

Device will reboot after firmware upgraded successfully

Image Updated Successful
DGS-1210-52>
```

注意　スイッチはリストア後に再起動し、現在のすべてのコンフィグレーションが失われます。

upload

目的

スイッチのファームウェアファイル / コンフィグレーションファイルを TFTP サーバにアップロードします。

構文

upload {firmware_fromTFTP | cfg_fromTFTP } {<ipaddr> | <ipv6addr>} <path_filename>

説明

TFTP サーバにコンフィグレーションファイルまたはファームウェアファイルをアップロードします。

パラメータ

パラメータ	説明
firmware_toTFTP	ファームウェアを TFTP サーバにアップロードします。
cfg_toTFTP	コンフィグレーションファイルを TFTP サーバにアップロードします。
<ipaddr>	TFTP サーバの IPv4 アドレスを指定します。
<ipv6addr>	TFTP サーバの IPv6 アドレスを指定します。
<path_filename>	ファームウェアファイルのパスとファイル名を指定します。ファイルが TFTP サーバにのルートディレクトリにない場合、DOS パスを指定する必要があります。

制限事項

なし

使用例

ファームウェアファイルをアップロードします。

```
DGS-1210-52> upload firmware_fromTFTP 10.90.90.100 DGS-1210-52-B1-3-10-013.hex


Image Upload Successfully.
DGS-1210-52>
```

config ipif system

目的

スイッチの IPv4 アドレスを設定します。

構文

config ipif system { ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp | bootp }

説明

スイッチの System IP インタフェースを設定します。

パラメータ

パラメータ	説明
ipaddress <ip-address> <subnet-mask>	作成するインタフェースの IP アドレスとサブネットマスク。従来のフォーマット（例 :10.1.2.3/255.0.0.0）を使用して IP アドレスとマスク情報を指定します。
gateway <gw-address>	ルータまたはゲートウェイの IP アドレスを入力します。
dhcp	スイッチの SystemIP インタフェースに IP アドレスを割り当てるために、DHCP プロトコルを選択します。
bootp	スイッチの BOOTP を選択します。

制限事項

なし

使用例

IP インタフェース「System」を設定します。

```
DGS-1210-52> config ipif System ipaddress 192.168.1.10 255.255.255.0 gateway 192.168.1.1
%   Note : If succeeded (please reconnect), the IP setting mode will cause CLI
disconnect.
DGS-1210-52>
```

config ipif system

目的

スイッチの IPv6 アドレスを設定します。

構文

config ipif system { ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client [enable | disable] }

説明

スイッチの System IP インタフェースを設定します。

パラメータ

パラメータ	説明
ipv6 ipv6address <ipv6networkaddr>	固定の IPv6 アドレスを割り当てるパラメータです。 ホストアドレスとネットワークプレフィックス長を定義する必要があります。 例：Ex: 3ffe:501:ffff:100::1/64 「/64」がプレフィックス長を表します。
dhcpv6_client [enable | disable]	DHCPv6 プロトコルの有効 / 無効を選択します。

制限事項

なし

使用例

IPv6 インタフェース「System」を設定します。

```
DGS-1210-52> config ipif System ipv6 ipv6address 3ffe:501:ffff:100::1/64

Success.
DGS-1210-52>
```

logout

目的

接続を終了して、ログアウトします。

構文

logout

説明

接続を終了して、ログアウトします。ログアウトの前にスイッチの設定を保存しておくことをお勧めします。

パラメータ

なし

使用例

現在のユーザコンソールセッションを終了します。

```
DGS-1210-52> logout
```

注意　ログアウトする前に設定変更を保存してください。

ping

目的

ネットワークデバイス間の接続性をテストします。

構文

ping <ipaddr>

説明

別の IP アドレスがネットワークに到達するかどうかをチェックします。スイッチとターゲットの IP デバイス間の物理的パスがある場合、管理 VLAN（初期値では VLAN1）を通じて接続する IP アドレスに ping します。初期値では、ターゲットの IP アドレスに 5 回 ping を送信します。

パラメータ

パラメータ	説明
<ipaddr>	ホストの IP アドレスを指定します。

制限事項

なし

使用例

IP アドレス 192.168.1.10 に ping します。

```
DGS-1210-52> ping 192.168.1.10
Reply Received From :192.168.1.10, TimeTaken : <1 msecs
Reply Received From :192.168.1.10, TimeTaken : <1 msecs
Reply Received From :192.168.1.10, TimeTaken : <1 msecs
Reply Received From :192.168.1.10, TimeTaken : <1 msecs
Reply Received From :192.168.1.10, TimeTaken : 10 msecs

--- 192.168.1.10 Ping Statistics ---
5 Packets Transmitted, 5 Packets Received, 0% Packets Loss
DGS-1210-52>
```

ping6

目的

ネットワークデバイス間の接続性をテストします。

構文

ping6 <ipv6addr>

説明

別の IP アドレスがネットワークに到達するかどうかをチェックします。スイッチとターゲットの IP デバイス間の物理的パスがある場合、管理 VLAN（初期値では VLAN1）を通じて接続する IP アドレスに ping します。初期値では、ターゲットの IP アドレスに 5 回 ping を送信します。

パラメータ

パラメータ	説明
<ipv6addr>	ホストの IPv6 アドレスを指定します。

制限事項

なし

使用例

IP アドレス 3000::1 に ping します。

```
DGS-1210-52> ping6 3000 ::1
Reply Received From : 3000 ::1, TimeTaken : 20 msecs
Reply Received From : 3000 ::1, TimeTaken : 20 msecs
Reply Received From : 3000 ::1, TimeTaken : 20 msecs

--- 192.168.1.10 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
DGS-1210-52>
```

create iproute

目的

スイッチの IP ルーティングテーブルに IP ルートエントリを作成します。

構文

create iproute default <ipaddr>

説明

スイッチの IP ルーティングテーブルに IP ルートエントリを作成します。

パラメータ

パラメータ	説明
default <ipaddr>	ルーティングテーブルを作成する IP アドレスを指定します。 • default - IP デフォルトルートを作成します。 • <ipaddr> - ネクストホップルータのゲートウェイ IP アドレス。

制限事項

管理者レベル、オペレータレベル、およびパワーユーザレベルユーザが本コマンドを実行できます。

使用例

ルーティングテーブルにデフォルトスタティックアドレス（10.90.90.92）を作成します。

```
DGS-1210-28> create iproute default 10.90.90.92
Command: create iproute default 10.90.90.92

Success.
DGS-1210-28>
```

delete iproute

目的

スイッチの IP ルーティングテーブルの IP ルートエントリを削除します。

構文

delete iproute {default}

説明

スイッチの IP ルーティングテーブルから IP ルートエントリを削除します。

パラメータ

パラメータ	説明
{default}	• default - IP デフォルトルートエントリを削除します。

制限事項

管理者レベル、オペレータレベル、およびパワーユーザレベルユーザが本コマンドを実行できます。

使用例

IP デフォルトルートを削除します。

```
DGS-1210-28> delete iproute
Command: delete iproute

Success.
DGS-1210-28>
```

show iproute

目的

スイッチの現在の IP ルーティングテーブルを表示します。

構文

show iproute {<ipaddr> | static}

説明

スイッチの現在の IP ルーティングテーブルを表示します。

パラメータ

パラメータ	説明
{<ipaddr> | static}	• <ipaddr> - ルーティングテーブルを表示する IP アドレスを指定します。 • static - すべてのスタティックルートを表示します。

制限事項

なし

使用例

IP ルーティングテーブルの内容を表示します。

```
DGS-1210-28> show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway  Interface  Hops  Protocol
------------------  -------  ---------  ----  ---------

Total Entries :0
DGS-1210-28>
```

reboot

目的

スイッチを再起動します。スイッチがスタックのメンバである場合、スタックの他のメンバに影響せず、個別に再起動されます。

構文

reboot

説明

システムを再起動します。すべてのネットワーク接続が終了し、ブートコードを実行します。

制限事項

なし

使用例

スイッチを再起動します

```
DGS-1210-52> reboot
% Device will reboot, please wait a few minutes to re-login.
DGS-1210-52>
```

reset config

目的

スイッチを工場出荷時設定に戻します。

構文

reset config

説明

すべてのコンフィグレーションは工場出荷時設定にリセットされます。

パラメータ

パラメータ	説明
config	IP アドレス、ユーザアカウントなどのパラメータが工場出荷時設定にリストアされます。スイッチは保存または再起動しません。

制限事項

なし

使用例

スイッチのすべてのパラメータを初期値に戻します

```
DGS-1210-52> reset config
% Device will reboot after reset configuration successfully.
DGS-1210-52>
```

show ipif

目的

スイッチの現在の IP アドレスを表示します。

構文

show ipif [ipif_name<string>]

説明

スイッチの現在の IP モード /IP アドレス / サブネットマスク / ゲートウェイを表示します。

パラメータ

パラメータ	説明
<string>	表示するインタフェース名を指定します。

制限事項

なし

使用例

IP インタフェースを表示します。

```
DGS-1210-52> show ipif
IP Setting Mode                  : Static
Interface Name                   : System
Interface VLAN Name              : default
IP Address                       : 192.168.1.10
Subnet Mask                      : 255.255.255.0
Default Gateway                  : 192.168.1.1

DGS-1210-52>
```

show switch

目的

スイッチに関する情報を表示します。

構文

show switch

説明

スイッチの現在の状態を表示します。

制限事項

なし

使用例

スイッチの現在の状態を表示します。

```
DGS-1210-52> show switch
System name                       :
System Contact                    :
System Location                   :
System up time                    : 0 days, 0 hrs, 1 min, 44 secs
System Time                       : 01/01/2009 22:57:59
System hardware version           : A1
System firmware version           : 1.00.015
System boot version               : 1.00.009
System Protocol version           : 2.001.004
System serial number              : QBI21B8000004
MAC Address                       : 1C-7E-E5-29-F8-17

DGS-1210-52>
```

config account admin password

目的

管理者パスワードを設定します。

構文

config account admin password <passwd>

説明

スイッチの管理者パスワードを設定します。

パラメータ

パラメータ	説明
<passwd>	新しい管理者パスワードを指定します。

制限事項

なし

使用例

アカウント admin のパスワードを設定します。

```
DGS-1210-52> config account admin password dlink
DGS-1210-52>
```

save

目的

NV-RAM にスイッチ設定内の変更を保存します。

構文

save

説明

メモリに設定の変更を保存します。

制限事項

なし

使用例

NV-RAM に現在のスイッチ設定を入力します

```
DGS-1210-52> save
Building configuration ...
[OK]
DGS-1210-52>
```

debug info

目的

スイッチの ARP テーブルと MAC FDB 情報を表示します。

構文

debug info

説明

スイッチの ARP テーブルと MAC FDB を表示します。

パラメータ

なし

制限事項

なし

使用例

スイッチの ARP テーブルと MAC FDB 情報を表示します。

```
DGS-1210-52> debug info
% sgementation fault log file :

File doesn't exist !!!
% ARP table :

Address          Hardware Address   Type  Interface  Mapping
-------          ----------------   ----  ---------  -------
192.168.1.0      ff:ff:ff:ff:ff:ff  ARPA  vlan1      Static
192.168.1.10     1c:7e:e5:29:f8:17  ARPA  vlan1      Static
192.168.1.12     00:13:72:0f:28:a4  ARPA  vlan1      Dynamic
192.168.1.255    ff:ff:ff:ff:ff:ff  ARPA  vlan1      Static

% MAC table :

Vlan    Mac Address         Type     Ports
----    -----------         ----     -----
1       00:13:72:0f:28:a4   Learnt   Gi0/3
1       00:24:a5:4e:c9:c2   Learnt   Gi0/3
1       00:a0:b0:a3:6c:ba   Learnt   Gi0/3
1       14:fe:b5:e6:8a:b4   Learnt   Gi0/3

Total Mac Addresses displayed: 4

DGS-1210-52>
```

第 7 章　スイッチのメンテナンス

工場出荷時設定に戻す

リセットボタンを押下することで本製品の設定を工場出荷状態に戻します。

1. 必要に応じて設定ファイルのバックアップを行い、本製品からログアウトします。

2. 前面のリセットボタンを 5 秒間押下します。
この間の前面パネルの LED ステータスは以下の通りです。

LED	状態
PWR	点灯
Link/Act（リンクしている場合）	点灯

3. リセットボタンを放すと本製品は再起動します。

4. 初期化が完了すると前面パネルの LED 表示は以下の通りになります。

LED	状態
PWR	点灯
Link/Act（リンクしている場合）	消灯後に点灯

注意 リセットボタンを押下する前に必ずご使用の製品の設定を保存してください。
リセットボタンを押下すると、すべての設定が消去されます。

【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。

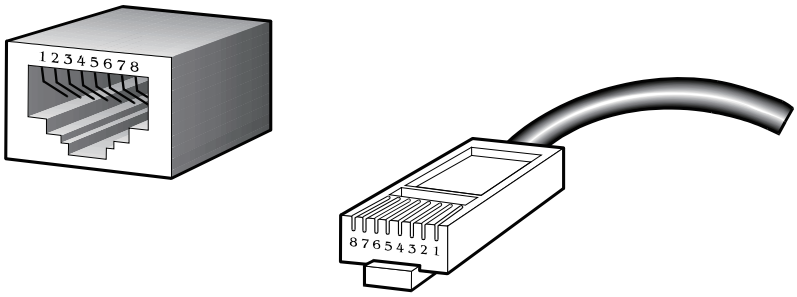


図 A-1　標準的な RJ-45 プラグとコネクタ

表 A-1　標準的な RJ-45 ピンアサイン

RJ-45 ピンアサイン		
コンタクト（ピン番号）	MDI-X 信号	MDI-II 信号
1	RD+（受信）	TD+（送信）
2	RD-（受信）	TD-（送信）
3	TD+（送信）	RD+（受信）
4	未使用	未使用
5	未使用	未使用
6	TD-（送信）	RD-（受信）
7	未使用	未使用
8	未使用	未使用

【付録 B】 ケーブル長

以下の表は各規格に対応するケーブル長 (最大) です。

表 B-1　ケーブル長

規格	メディアタイプ	最大伝送距離
SFP	1000BASE-LX、シングルモードファイバモジュール 1000BASE-SX、マルチモードファイバモジュール 1000BASE-LH、シングルモードファイバモジュール 1000BASE-ZX、シングルモードファイバモジュール	10km 550m 40km 80km
1000BASE-T	エンハンスドカテゴリ 5 UTP ケーブル カテゴリ 5 UTP ケーブル（1000Mbps）	100m
100BASE-TX	カテゴリ 5 UTP ケーブル（100Mbps）	100m
10BASE-T	カテゴリ 3 UTP ケーブル（10Mbps）	100m

【付録 C】　用語解説

用語	説明
1000BASE-LX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。長い光波長で長距離伝送用に使用されます。伝送距離 (最大) はシングルモード光ファイバを使用した場合で 10km。
1000BASE-SX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。短い光波長でマルチモード光ファイバを使用した場合伝送距離 (最大) は 550km。
100BASE-FX	光ファイバを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
100BASE-TX	カテゴリ 5 以上の UTP ケーブルを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
10BASE-T	IEEE 802.3 準拠でカテゴリ 3 以上の UTP ケーブルを使用する最大伝送速度 10Mbps の Ethernet の規格のひとつ。
エージング	タイムアウトし、無効のスイッチのダイナミックデータベースを自動的に消去します。
ATM	非同期転送モード。セルと呼ばれる固定長のセル (パケット) ベースで転送するプロトコル。ATM は音声、データおよびビデオ信号を含むユーザトラフィックの完全な列を転送するために開発されたものです。
オートネゴシエーション	スピード、デュプレックスおよびフローコントロールを自動的に認識する機能。オートネゴシエーションをサポートする端末と接続すると、リンクは自動的に最適なリンク条件に設定されます。
バックボーンポート	デバイスのアドレスを学習せず不明なアドレスを持つすべてのフレームを受信するポート。バックボーンポートは通常ご使用のネットワークのバックボーンにスイッチを接続するために使用されるポートです。バックボーンポートは以前はダウンリンクポートとして知られていました。
バックボーン	ネットワークセグメント間でトラフィックが転送される場合に優先パスとして使用されるネットワークの一部分。
帯域	1 秒あたりのビット数で計算される 1 チャンネルが転送できる情報量。イーサネットの帯域は 10Mbps、ファーストイーサネットは 100Mbps。
ボーレート	ラインのスイッチングスピード。ネットワークセグメント間のラインスピードとして知られています。
BOOTP	BOOTP プロトコルはデバイスが起動するたびに IP アドレスを MAC アドレスに自動マッピングします。さらにデバイスにサブネットマスク、デフォルトゲートウェイを割り当てます。
ブリッジ	たとえ高いレベルのプロトコルが関連してもローカルまたはリモートネットワークを相互接続するデバイス。ブリッジはネットワーク管理を中央に集めて 1 個の論理ネットワークを形成します。
ブロードキャスト	ネットワーク上のすべての終点デバイスに送信されるメッセージ。
ブロードキャストストーム	が主として可能なネットワーク帯域を奪い、ネットワークエラーを引き起こす Multiple simultaneous ブロードキャスト。
コンソールポート	端末またはモデムコネクタと接続可能なスイッチ上のポート。コンピュータ内でパラレル配列のデータをデータ転送リンクで使用されるシリアル形式に変換します。このポートはほとんどの場合ローカル管理のために使用されます。
CSMA/CD	イーサネットと IEEE 802.3 標準によって使用されるチャンネルアクセス方法で検索したデータチャンネルが一定期間後クリアされた後にだけデバイスに転送します。2 つのデバイスが同時に転送する場合、コリジョンが発生し、コリジョンを発生したデバイスは任意の時間再転送を遅らせます。
データセンタースイッチング	スイッチがサーバファームへの高パフォーマンスアクセス、高速バックボーン接続、およびネットワーク管理とセキュリティのためのコントロールポイントを提供するコーポレートネットワーク内のアグリゲーションポイント
イーサネット	Xerox、Intel および DEC が共同で開発した LAN 仕様。イーサネットネットワークは CSMA/CD を使用して 10Mbps で処理を行います。
ファーストイーサネット	Ethernet/CD ネットワークアクセス方法をベースにした 100Mbps 技術。
フローコントロール	(IEEE 802.3z) 端末に接続した転送ポートへのパケットを抑止します。受信バッファがあふれそうになった場合にパケットロスを防ぎます。
フォワーディング	中間のネットワークデバイスによりパケットを到達点に向けて送信するプロセス。
フルデュプレックス	同時にパケットの送受信を可能とし、スループットを 2 倍にするシステム。
ハーフデュプレックス	パケットの送受信を行うが、同時には行えないシステム。
IP アドレス	Internet Protocol アドレス。TCP/IP を使用するネットワークに付属するデバイスの固有な識別子。IPv4 アドレスは 8 ビットずつピリオドで区切られ、ネットワークセクション、サブネットセクション、ホストセクションで構成されます。
IPX（Internetwork Packet Exchange）	ネットワーク通信で使用するプロトコル。
LAN – ローカルエリアネットワーク	通常フロアもしくはビルのような規模の小さいエリアで PC、プリンタ、サーバのようなコンピュータリソースを接続するネットワーク。高速で低エラー率が特長です。
レイテンシ	デバイスがパケットを受信する時間とパケットが到達点ポートに転送される時間の遅延。
ラインスピード	ボーレートを参照。
メインポート	通常の操作条件でデータトラフィックを送信する Resilient リンク内のポート。
MDI（Medium Dependent Interface）	1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。
MDI-X（Medium Dependent InterfaceCross-over）	接続送受信のラインが交差しているイーサネットポート接続。
MIB（Management Information Base）	デバイスの管理特性とパラメータを保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。
マルチキャスト	シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。
プロトコル	ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。
Resilient link	他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。
RJ-45	10BASE-T や 100BASE-TX などで使用する標準 8 線コネクタ

用語	説明
RMON	リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。
RPS （リダンダント電源システム）	スイッチに接続されて、バックアップ電源を供給するデバイス。
サーバファーム	大量のユーザにサービスを提供する中央に位置するサーバグループ。
SLIP （Serial Line Internet Protocol）	IP がシリアルライン接続を経由して動作することが可能なプロトコル。
SNMP （Simple Network Management Protocol）	当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。
スパニングツリープロトコル (STP)	ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。
スタック	1 個の論理的なデバイスの形をとするために統合されたネットワークデバイスのグループ。
スタンバイポート	リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。
スイッチ	パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。
TCP/IP	Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。
telnet	仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。
TFTP （Trivial File Transfer Protocol）	スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する (ソフトウェアアップグレードなど) ことができます。
UDP （User Datagram Protocol）	インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。
VLAN（Virtual LAN）	物理的に接続した LAN のように通信する位置やトポロジが独立しているデバイスのグループ。
VLT（Virtual LAN Trunk）	各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。
VT100	ASCII コードを使用するターミナルタイプ。VT100 画面はテキストベースの表示をします。

【付録 D】　機能設定例

本項では、一般によく使う機能についての設定例を記載します。実際に設定を行う際の参考にしてください。

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DGS-1210

Traffic Segmentation（トラフィックセグメンテーション）

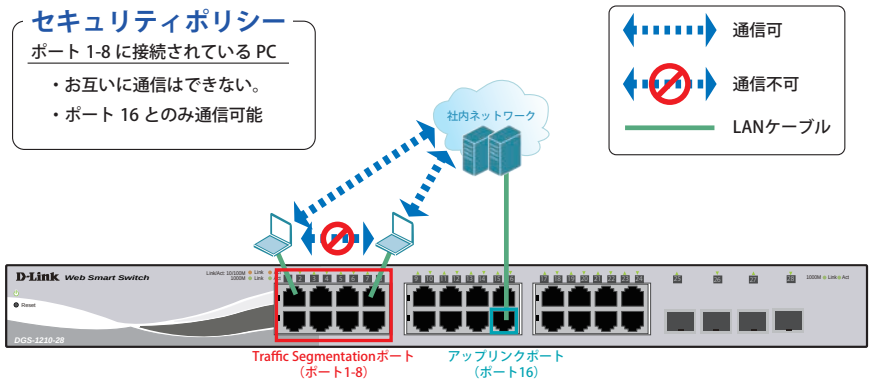


図 8-1　Traffic Segmentation（DGS-1210-28）

概要

ポート 1 ～ 8 に対し、トラフィックセグメンテーションを設定します。1 ～ 8 のポート間ではお互いに通信ができないようにし、ポート 1 ～ 8 は、アップリンクポートとして使用するポート 16 とのみ通信ができるようにします。

設定手順

1. 「Traffic Segmentation」の適応ポート範囲を設定します。通信するポートにのみチェックを入れます。

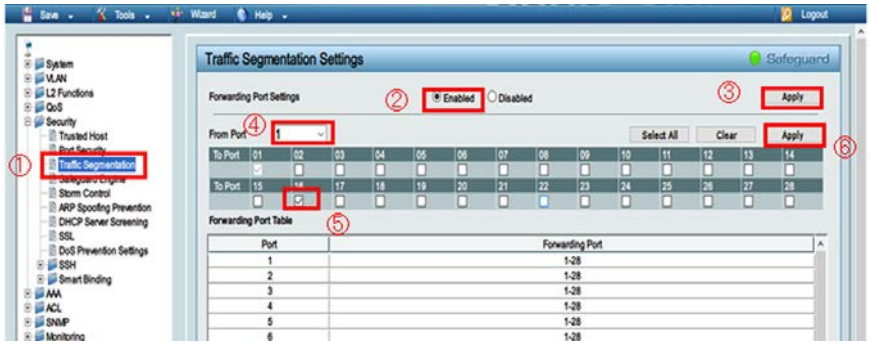


図 8-2　Traffic Segmentation（DGS-1210-28）

2. 「1. 」の手順をポート 1~8 について同様に繰り返します。またポート 16 については、「To Port」の 1~8 にチェックを入れて「Apply」を適用します。設定終了後、以下のようになっていることを確認します。

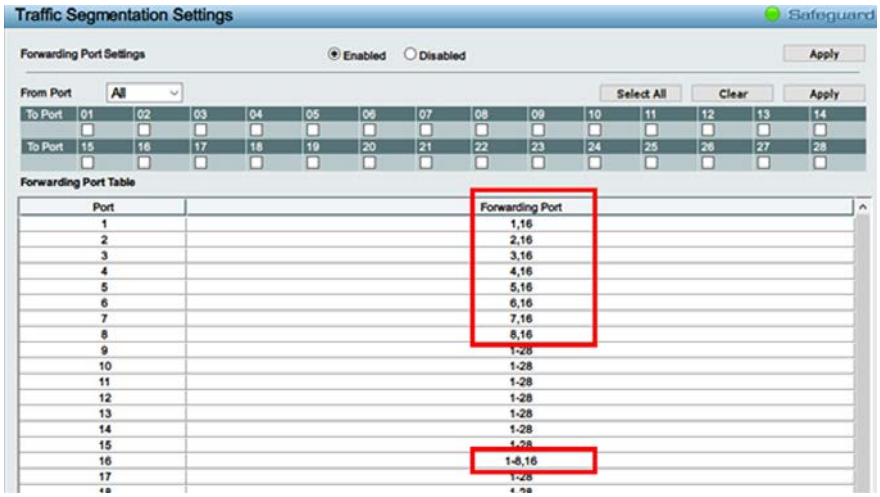


図 8-3　Traffic Segmentation Settings（DGS-1210-28）

注意　本機能を利用する場合、Unknown ユニキャストについては全ポートにブロードキャストされます。

3. **Save > Save Configuration** で設定を保存します。「Save Config」をクリックします。

図 8-4　Save Configuration（DGS-1210-28）

VLAN

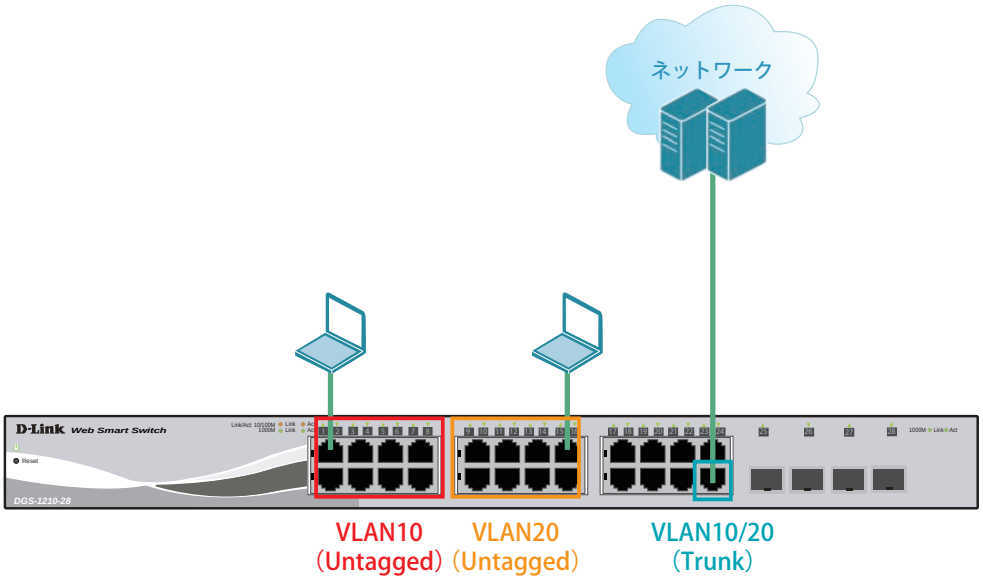


図 8-5　VLAN（DGS-1210-28）

概要

VLAN を設定します。ポート 1 ～ 8 に VLAN10 を「Untagged」で割り当て、ポート 9 ～ 16 に VLAN20 を「Untagged」で割り当て、ポート 24 において、VLAN10 と VLAN20 を「Tagged」（Trunk）で割り当てます。

設定手順

1. VLAN10 と 20 をアサインするポートのデフォルト VLAN のアサインを削除します。**VLAN > 802.1Q VLAN** で VLAN を指定します。

図 8-6　デフォルト VLAN 指定（DGS-1210-28）

2. ポート 1 ～ 16 のデフォルト VLAN のアサインを削除します。

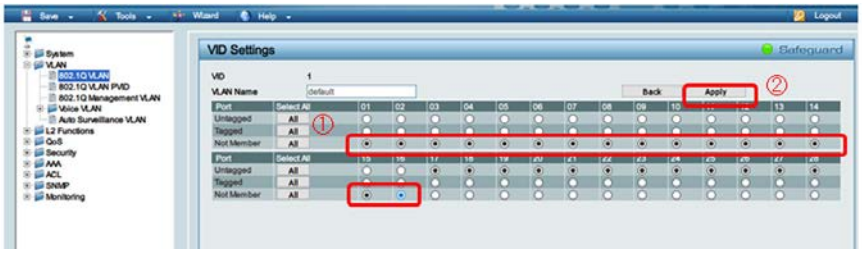


図 8-7　デフォルト VLAN アサイン削除（DGS-1210-28）

注意 WebUI にアクセスしている PC を接続しているポートは Management VLAN に属したポートに接続している必要があります（デフォルトでは VLAN1）。ポート 1~16 に接続している場合、WebUI へのアクセスが失われますので、Management VLAN に所属しているポートに差し替えてください。

3. **VLAN > 802.1Q VLAN** で VLAN10 を作成します。

図 8-8　　VLAN10 作成（DGS-1210-28）

4. ポート 1 ～ 8 に Untagged、ポート 24 に Tagged でアサインします。

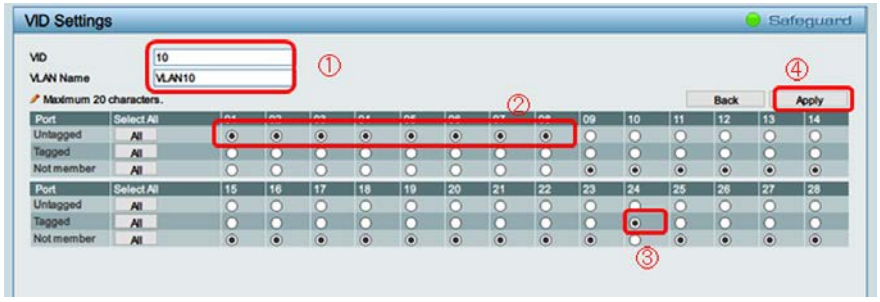


図 8-9　　ポートアサイン（DGS-1210-28）

5. 同様に VLAN20 を作成し、ポート 9 ～ 16 に Untagged、ポート 24 に Tagged でアサインします。
図 8-1
6. **Save > Save Configuration** で設定を保存します。「Save Config」をクリックします。

図 8-10　　Save Configuration（DGS-1210-28）

Link Aggregation（リンクアグリゲーション）

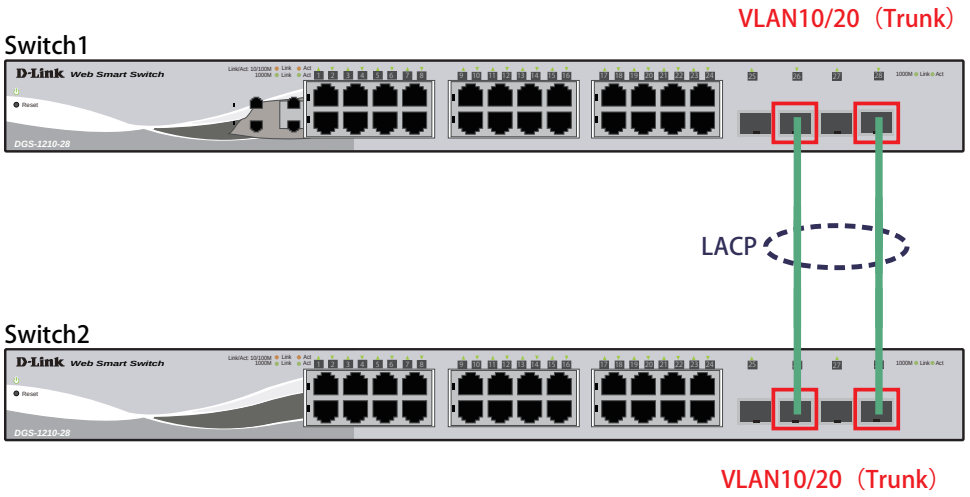


図 8-11　Link Aggregation（DGS-1210-28）

概要

VLAN10 と 20 の Tagged VLAN を設定したポートにリンクアグリゲーションを設定します。ポート 26 と 28 に VLAN10 と VLAN20 を Tagged で割当て、ポート 26 と 28 をグループとして LACP によるリンクアグリゲーションに設定します。

設定手順

1. **VLAN > 802.1Q VLAN** で VLAN10 を作成します。

図 8-12　VLAN10 作成（DGS-1210-28）

2. ポート 26、28 に Tagged でアサインします。

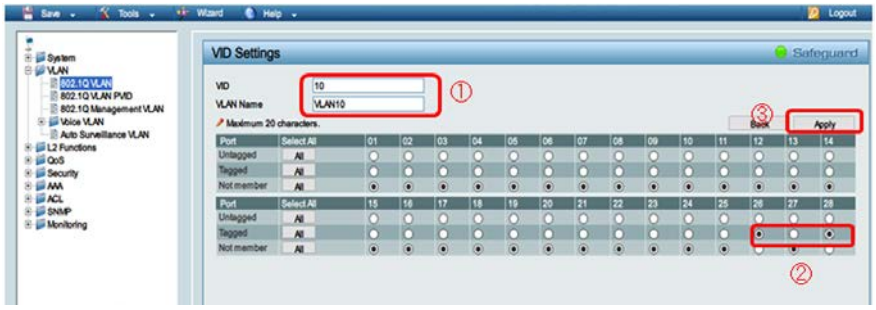


図 8-13　ポートアサイン（DGS-1210-28）

3. **L2 Functions > Link Aggregation > Port Trunking** でポート 26、28 に LACP を設定します。
④⑤の項目で「Group」「Type」「対象ポート」を下図のように設定します。「Apply」をクリックします。

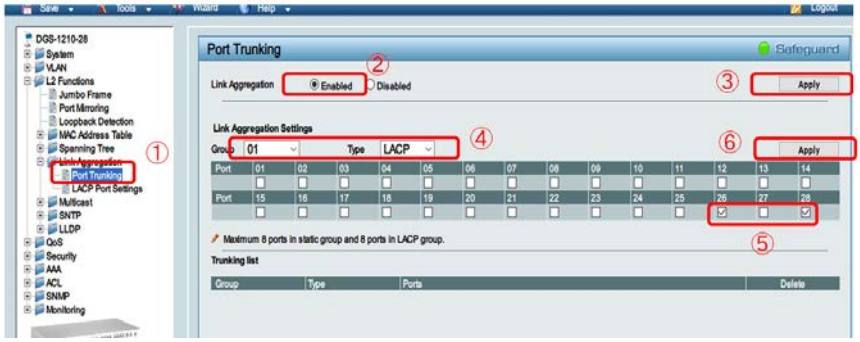


図 8-14　LACP 設定（DGS-1210-28）

4. **L2 Functions > Link Aggregation > LACP Port Settings** でポート 26 の LACP モードを「Active」にします。

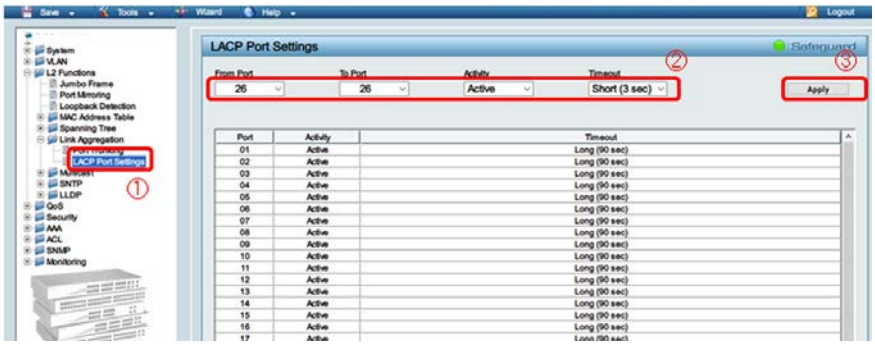


図 8-15　LACP（Active）（DGS-1210-28）

注意　「Timeout」は環境により変更してください。

5. 同様にポート 28 の LACP モードを「Active」にします。

6. **Save > Save Configuration** で設定を保存します。「Save Config」をクリックします。

図 8-16　Save Configuration（DGS-1210-28）

Access List（アクセスリスト）

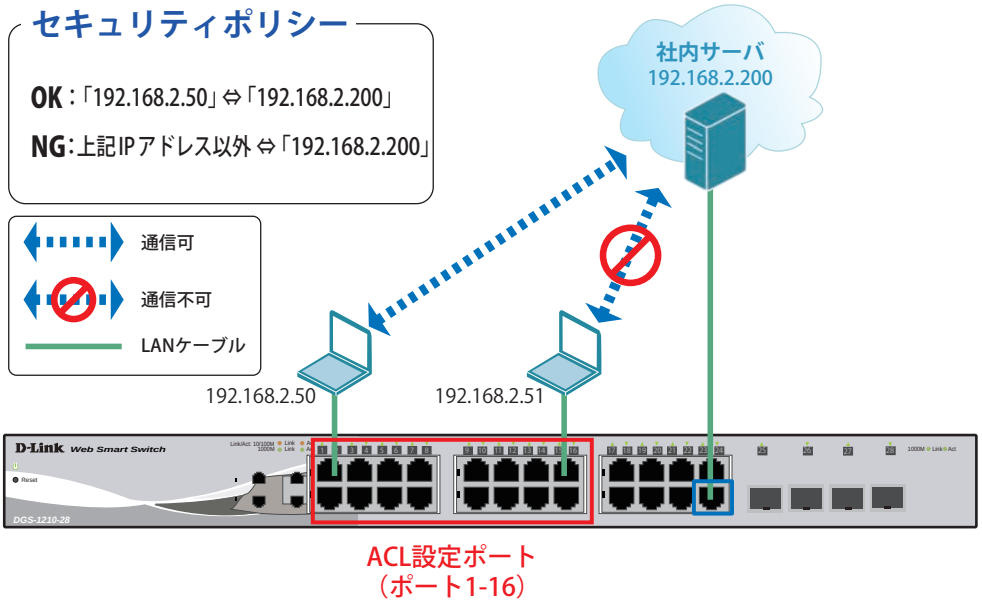


図 8-17　Access List

概要

ポート 1~16 に対し、アクセスリストを設定します。ポート 1~16 に接続される端末の IP の中から ,192.168.2.50 の端末から社内サーバ（192.168.2.200）へのアクセスは許可し、それ以外の端末から社内サーバへのアクセスは禁止するように設定します。

設定手順

1. **ACL > ACL Access List** で IPv4 プロファイルを作成します。

図 8-18　IP プロファイル作成（DGS-1210-28）

2. 「Name」を入力、「Packet Type」を「IPv4」に指定し「Apply」をクリックし、表示されるダイアログで「Continue」をクリックします。

図 8-19　IPv4 プロファイル作成（DGS-1210-28）

3. 次に「Edit Rules」、「Add」をクリックしルールの作成、追加を行います。

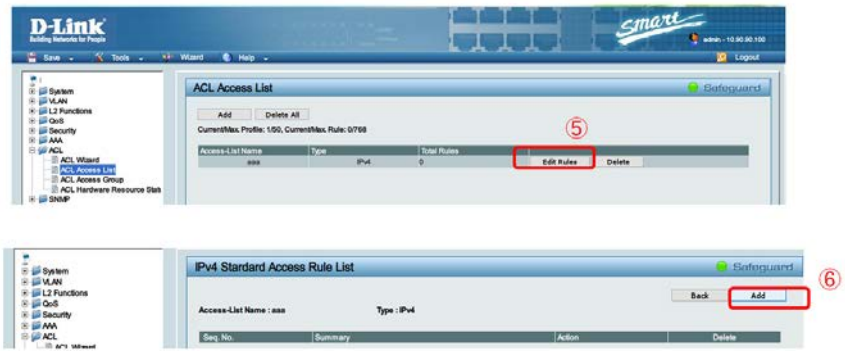


図 8-20　IPv4 プロファイルルール設定（DGS-1210-28）
図 8-2

4. 作成した IPv4 プロファイルに 192.168.2.50 から 192.168.2.200 への通信を拒否するルールを追加します。

図 8-21　IPv4 プロファイルルール設定（DGS-1210-28）

5. 作成したアクセスプロファイルをポート 1 ～ 16 に適用します。

図 8-22　IPv4 プロファイルルール設定（DGS-1210-28）

6. **Save > Save Configuration** で設定を保存します。「Save Config」をクリックします。

図 8-23　Save Configuration（DGS-1210-28）