D-Link DGS-1210 シリーズ
（DGS-1210-10/10MP/20/28/28MP/52）
Gigabit Layer2 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

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

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

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

この装置は、クラスA機器です。この装置を住宅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。

VCCI - A

ご使用上の注意

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

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。また、計画停電などが予定されている場合には、事前に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器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器具に固定すると、ケーブルの抜けを防止することができます。

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。

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。

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、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

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

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。
- 弊社は、予告なく本書の全体または一部を修正・改訂することがあります。
- 弊社は改良のため製品の仕様を予告なく変更することがあります。

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

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 F1/F2/F3 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　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 5 章　サーベイランスモードの設定
  - サーベイランスモードによる管理、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)#`
< >	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*}]

製品名 / 品番一覧

製品名	H/W バージョン	品番
DGS-1210-10	F1	DGS-1210-10/F1
DGS-1210-10MP	F1	DGS-1210-10MP/F1
DGS-1210-20	F1	DGS-1210-20/F1
DGS-1210-28	F1	DGS-1210-28/F1
	F2	DGS-1210-28/F2
	F3	DGS-1210-28/F3
DGS-1210-28MP	F1	DGS-1210-28MP/F1
	F2	DGS-1210-28MP/F2
	F3	DGS-1210-28MP/F3
DGS-1210-52	F1	DGS-1210-52/F1
	F2	DGS-1210-52/F2
	F3	DGS-1210-52/F3

第 1 章　本製品のご利用にあたって

スイッチ概要

柔軟なポート設定
DGS-1210 シリーズはスマートスイッチシリーズの新世代スイッチです。8、20、28、52 ポートの 10/100/1000Mbps ポート（DGS-1210-10MP/28MP では PoE 対応ポート）に加えて、SFP スロットを 2 つまたは SFP コンボスロットを 4 つ搭載したラインナップを揃えています。本スイッチに備わっている SFP アップリンクポートにより、リング型やツリー型、混合型など柔軟なネットワークトポロジを構成することが可能です。

セキュアで快適なネットワーク環境
D-Link Green 技術は、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-1210-10MP/28MP 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、802.1p プライオリティキューをサポートしており、マルチメディアのストリーミング配信のような多くの帯域を使用するアプリケーションについて、ネットワーク上のトラフィックの優先順位付けを行います。これらの機能により、ネットワーク上のトラフィックのシームレスな通信が可能となります。
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。Asymmetric VLAN 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、外部の RADIUS サーバを利用してネットワークの制御を行うことができます。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 スマートスイッチは、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。
Web ベースの GUI での製品の設定および管理が可能です。また、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のみコマンドライン（telnet）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 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 がサポートされているため、SNMP 環境の管理において、サードパーティ製のデバイスと本スイッチを統合化することができます。

サポートする機能

- IIEEE 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 802.1s Multiple 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-1210-10MP/28MP のみ）、IEEE 802.3at PoE Plus（DGS-1210-10MP/28MP のみ）

- L2 機能
  - IGMP スヌーピング：v1/v2
    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グループ数：256
    VLAN 毎の IGMP、IGMP スヌーピングクエリア
  - MLD スヌーピング：v1
    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グループ数：64
  - スパニングツリー：IEEE 802.1D STP、IEEE 802.1w RSTP、802.1s MSTP
  - 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-1210-10/10MP：4 グループ / デバイス、8 ポート / グループ
    DGS-1210-20/28/28MP：8 グループ / デバイス、8 ポート / グループ
    DGS-1210-52：16 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：10,000 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

- L3 機能
  - スタティックルーティングエントリ（IPv4：最大 124、IPv6：最大 50）
  - デフォルトルート（IPv4/IPv6）、IP インタフェース数：4[※1]
  - ARP エントリ：最大 1000（スタティック：384）
  - IPv6 Neighbor Discovery

  ※1　複数の IP インタフェースを設定した場合、ハードウェアリミテーションにより、DHCP リレーが適切に動作しません。

- 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、MAC アドレス、Ether タイプ、IP アドレス、プロトコルタイプ、ToS/IP Preference、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
  - SSHv2（IPv4/IPv6）、TLSv1.3
  - 管理アクセス認証用：ローカル、ユーザ認証用：RADIUS/ ローカル
  - IEEE 802.1X 認証：ポートベース認証
  - 802.1X ゲスト VLAN
  - ポートセキュリティ：64MAC アドレス / ポート
  - ブロードキャスト / マルチキャストストームコントロール、トラフィックセグメンテーション
  - IP-MAC ポートバインディング：ARP インスペクション、DHCP スヌーピング（IPv4/IPv6）
  - DHCP サーバスクリーニング、ARP スプーフィング防止、DoS アタック防止
  - D-Link セーフガードエンジン
  - トラストホスト（IPv4/IPv6）

- マネジメント
  - ユーザ種別：1 種類
  - Web GUI（IPv4/IPv6）、簡易 CLI
  - Telnet サーバ（IPv4/IPv6）、SNMPv1/v2c/v3、SNMP over IPv6、SNMP トラップ
  - TFTP クライアント（IPv4/IPv6）、SNTP クライアント（IPv4/IPv6）、SYSLOG（IPv4/IPv6）
  - RMONv1：4 グループ、LLDP、LLDP-MED（DGS-1210-10MP/28MP のみ）
  - DHCP 自動設定、DHCP/BOOTP クライアント、DHCPv6 クライアント、DHCP リレー：オプション 82
  - 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 / アップグレード
  - ケーブル診断、複数設定ファイル、複数イメージ
  - タイムベース PoE（DGS-1210-10MP/28MP のみ）、PD アライブ（DGS-1210-10MP/28MP のみ）
  - Perpetual PoE（DGS-1210-28MP のみ）

- 以下の MIB のサポート
  - MIB II（RFC1213）
  - MIB Traps Convention（RFC1215）、
  - SNMP MIB（RFC1157, RFC2573, RFC2575, RFC2576）
  - SNMPv2 MIB（RFC1442, RFC1901-1908, RFC2578, RFC3418）、
  - RMON MIB（RFC271, RFC1757, RFC2819）
  - RMONv2 MIB（RFC2021）、
  - Ether-like MIB（RFC1398, RFC1643, RFC1650, RFC2358, RFC2665）
  - 802.1p MIB（RFC2674, RFC4363）、
  - Interface Group MIB
  - RADIUS Authentication Client MIB（RFC2618）、
  - MIB for TCP（RFC4022）
  - MIB for UDP（RFC4113）
  - RADIUS Accounting Client MIB (RFC2620)、
  - Private MIB
  - PoE MIB
  - DDP MIB
  - LLDP-MED MIB

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-1210-10

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

DGS-1210-10MP

- 10BASE-T/100BASE-TX/1000BASE-T ポート x　8（PoE 給電：8）
- SFP スロット　x　2

DGS-1210-20

- 10BASE-T/100BASE-TX/1000BASE-T ポート x　20
- SFP コンボスロット　x　4

DGS-1210-28

- 10BASE-T/100BASE-TX/1000BASE-T ポート x　28
- SFP コンボスロット　x　4

DGS-1210-28MP

- 10BASE-T/100BASE-TX/1000BASE-T ポート x　28（PoE 給電：24）
- SFP コンボスロット　x　4

DGS-1210-52

- 10BASE-T/100BASE-TX/1000BASE-T ポート x　52
- SFP コンボスロット　x　4

SFP（コンボ）スロットで使用可能な SFP モジュールは以下のとおりです。

種別	製品名
2 芯 SFP モジュール (100M)	DEM-211
2 芯 SFP モジュール (1Giga)	DEM-310GT
	DEM-311GT
	DEM-312GT2
	DEM-314GT
	DEM-315GT
WDM 対応 1 芯 SFP モジュール	DEM-330T
	DEM-330R
	DEM-331T
	DEM-331R
Copper SFP (1Giga)	DGS-712※

※：SFP スロットのみの対応になります。

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。

参照 リセットボタン押下時の動作については、「リセットボタン押下時の動作」を参照してください。

参照 SFP ポートに使用するオプションモジュールについては、「搭載ポート」を参照してください。

補足 DGS-1210-10MP/28MP 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。

補足 SFP コンボポートは、対応する 1000BASE-T ポートと同時に使用することはできません。

注意 DGS-1210-10MP/28MP の PoE ネットワークへの接続時には、屋外設備への配線を行わないでください。

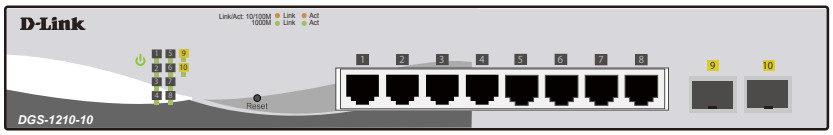


図 1-1　DGS-1210-10 の前面パネル図

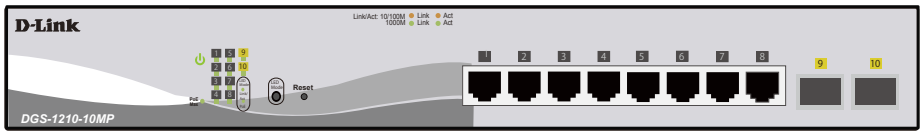


図 1-2　DGS-1210-10MP の前面パネル図

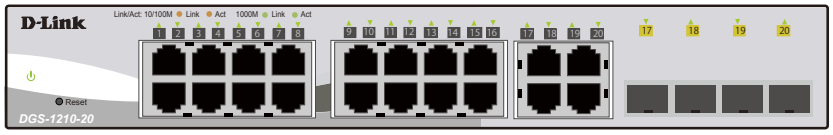


図 1-3　DGS-1210-20 の前面パネル図

図 1-4　DGS-1210-28 の前面パネル図

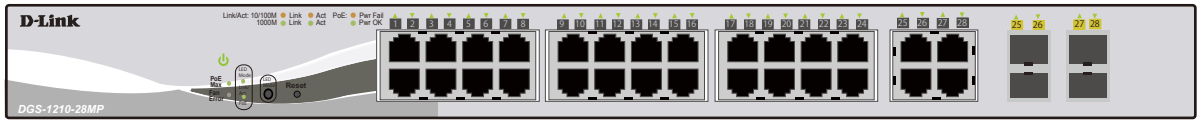


図 1-5　DGS-1210-28MP の前面パネル図

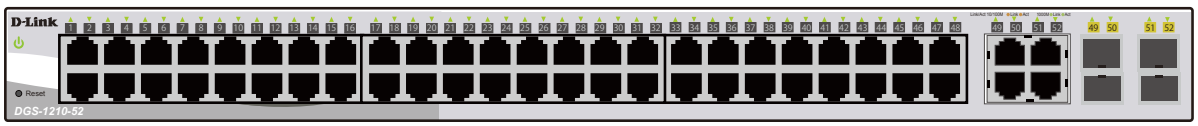


図 1-6　DGS-1210-52 の前面パネル図

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-1210-10

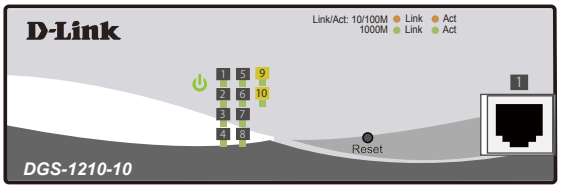


図 1-7　DGS-1210-10 の前面パネルの LED 配置図

DGS-1210-20

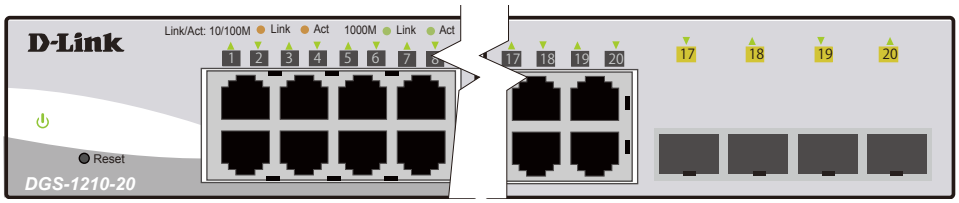


図 1-8　DGS-1210-20 の前面パネルの LED 配置図

DGS-1210-28

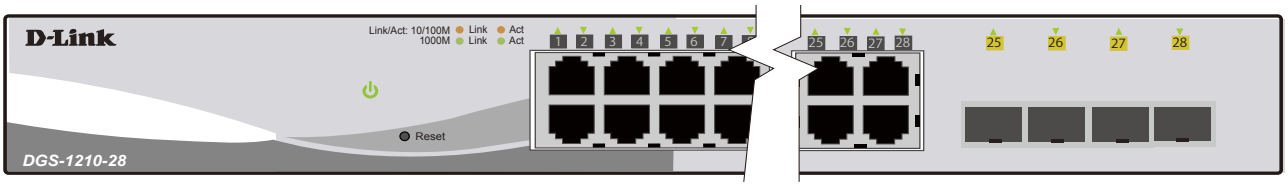


図 1-9　DGS-1210-28 の前面パネルの LED 配置図

DGS-1210-52

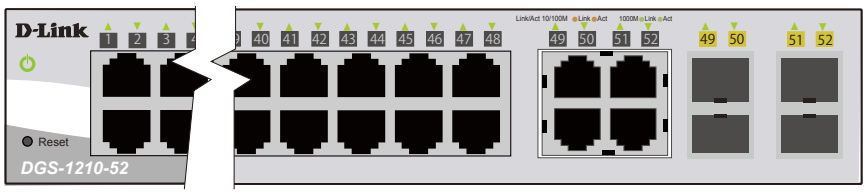


図 1-10　DGS-1210-52 の前面パネル LED 配置図

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	―	電源が供給されていません。
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	10/100Mbps でリンクが確立しています。
	点滅	橙	10/100Mbps でデータを送受信しています。
	消灯	―	リンクが確立していません。
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。
	点灯	橙	100Mbps でリンクが確立しています。
	点滅	橙	100Mbps でデータを送受信しています。
	消灯	―	リンクが確立していません。

DGS-1210-10MP

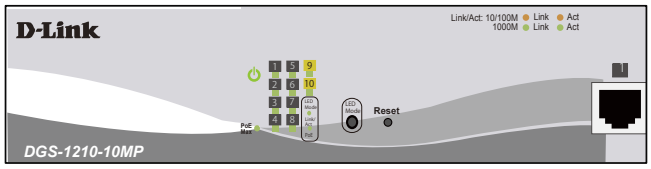


図 1-11　DGS-1210-10MP の前面パネルの LED 配置図

DGS-1210-28MP

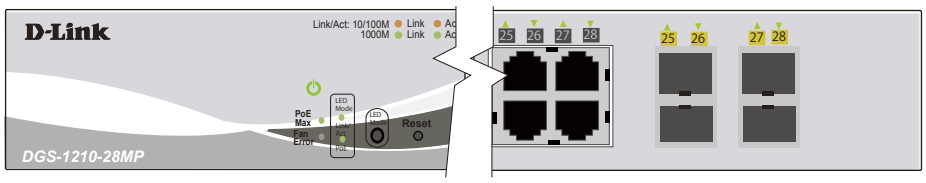


図 1-12　DGS-1210-28MP の前面パネルの LED 配置図

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-1210-28MP のみ）		消灯	―	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-1210-10MP/28MP）		点灯	橙	PoE デバイスが接続されましたが、Power Guard Band（電力保護帯域）、または最大 PoE 供給電力に達しています。 補足 Power Guard Band（電力保護帯域）は、最大供給電力の内 7W 確保されています。 補足 最大 PoE 供給電力は、130W（DGS-1210-10MP）/370W（DGS-1210-28MP）です。
		消灯	―	使用電力は帯域保護モードのしきい値に到達していません。
Link/Act（DGS-1210-10MP/28MP）		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 (DGS-1210-10MP/28MP)		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	10/100Mbps でリンクが確立しています。
		点滅	橙	10/100Mbps でデータを送受信しています。
		消灯	―	リンクが確立していません。
	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 コンボスロット 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。
		点灯	橙	100Mbps でリンクが確立しています。
		点滅	橙	100Mbps でデータを送受信しています。
		消灯	―	リンクが確立していません。

補足 PoE モードに設定されている場合、PoE 供給ポートのみ LED が点灯します。（DGS-1210-10MP では 1 ～ 8 ポート、DGS-1210-28MP では 1 ～ 24 ポート）

リセットボタン押下時の動作

各機種のリセットボタン押下時の動作は、以下の表のとおりです。

リセットボタン押下秒数	LED 状態	動作
1~5 秒	橙色に点滅	デバイスが再起動します。
6~10 秒	橙色に 2 秒間点灯	すべての設定が工場出荷時の状態にリセットされます。
11 秒以上	緑色に 2 秒間点灯	ローダーモードに移行します。

補足　イメージファイルが破損している場合、スイッチはローダーモードで起動します。

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-1210-10

図 1-13　DGS-1210-10 背面パネル図

DGS-1210-10MP

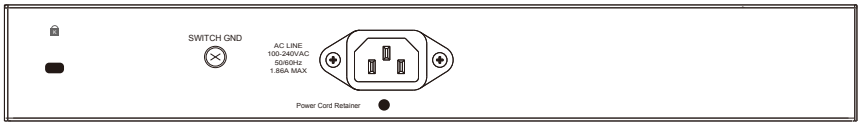


図 1-14　DGS-1210-10MP 背面パネル図

DGS-1210-20

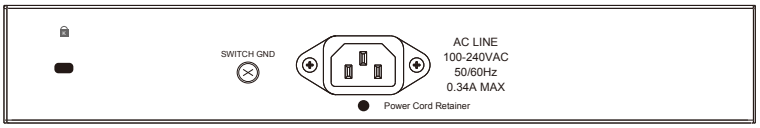


図 1-15　DGS-1210-20 背面パネル図

DGS-1210-28

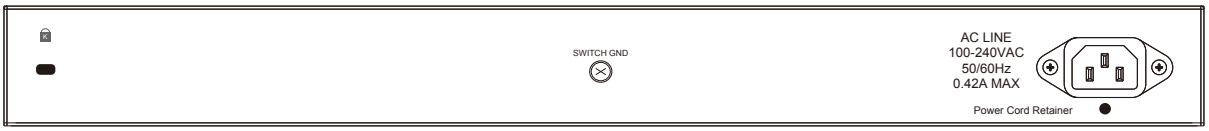


図 1-16　DGS-1210-28 背面パネル図

DGS-1210-28MP

図 1-17　DGS-1210-28MP 背面パネル図

DGS-1210-52

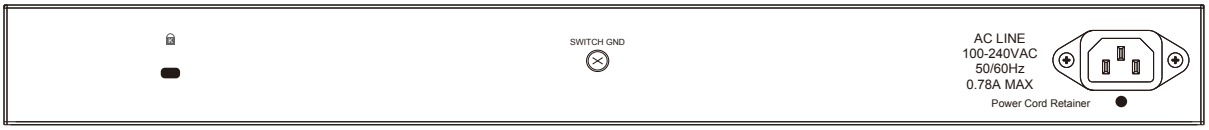


図 1-18　DGS-1210-52 背面パネル図

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。

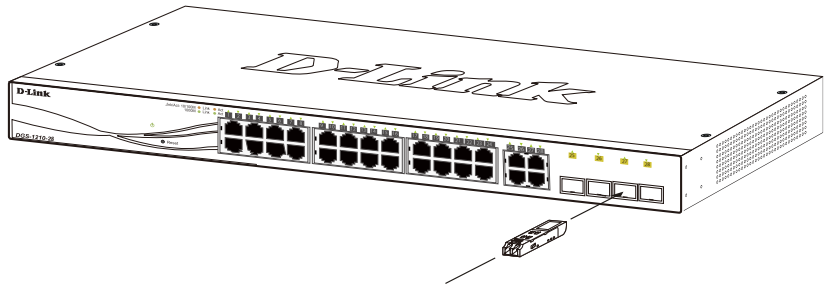


図 1-19　スイッチに光トランシーバを取り付ける

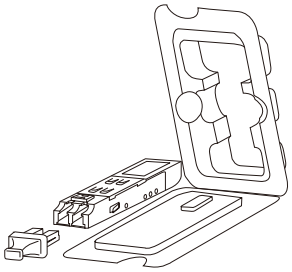


図 1-20　SFP モジュール図

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
- 電源抜け防止器具
- ゴム足
- マニュアル
- 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、ご購入いただきました代理店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 / 電源アダプタ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。

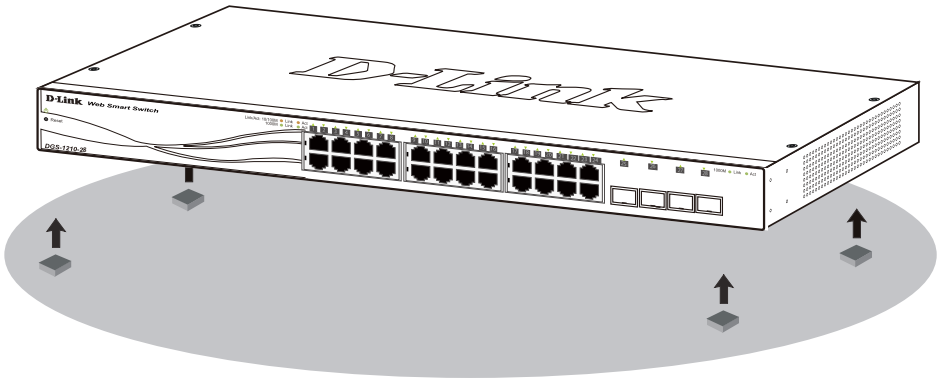


図 2-1　ゴム足の取り付け

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。

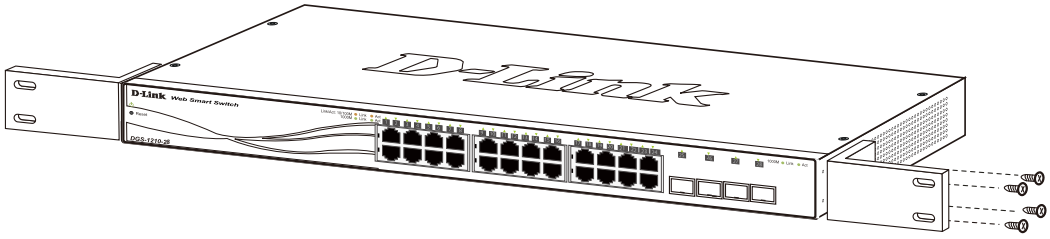


図 2-2　スイッチへのブラケットの取り付け

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。

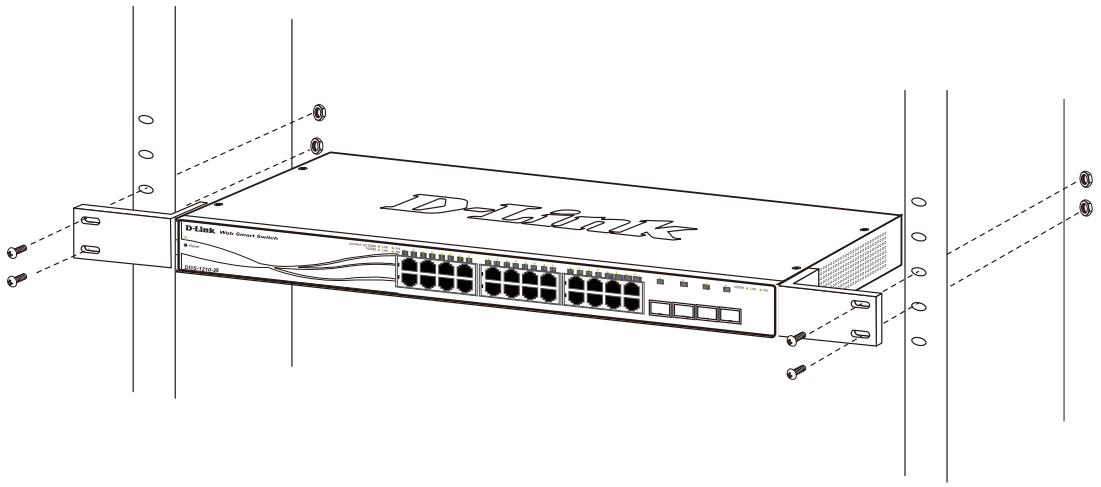


図 2-3　スイッチのラックへの設置

電源抜け防止器具の装着

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器具を装着します。
以下の手順に従って電源抜け防止器具を装着します。

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器具のタイラップ（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。

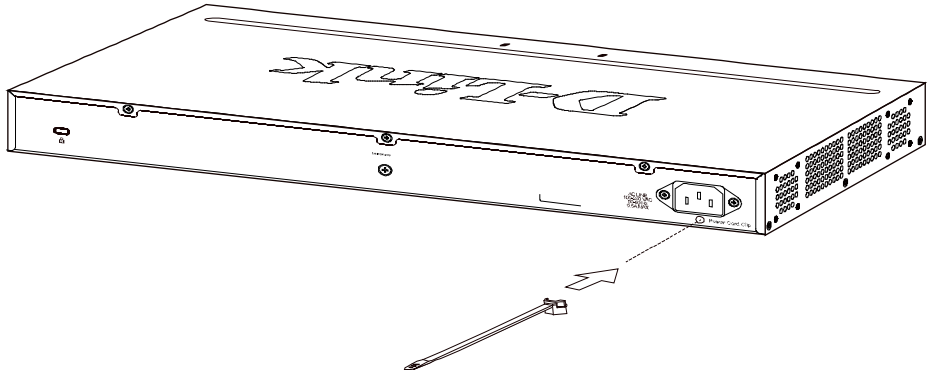


図 2-4　タイラップの挿し込み

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。

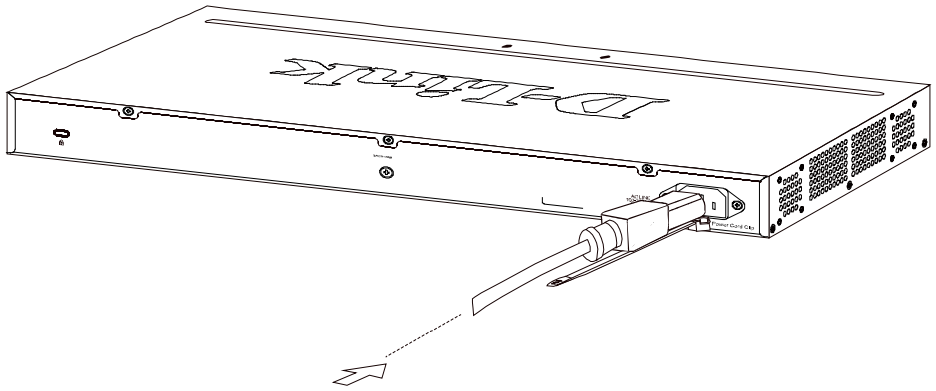


図 2-5　電源コード挿し込み

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。

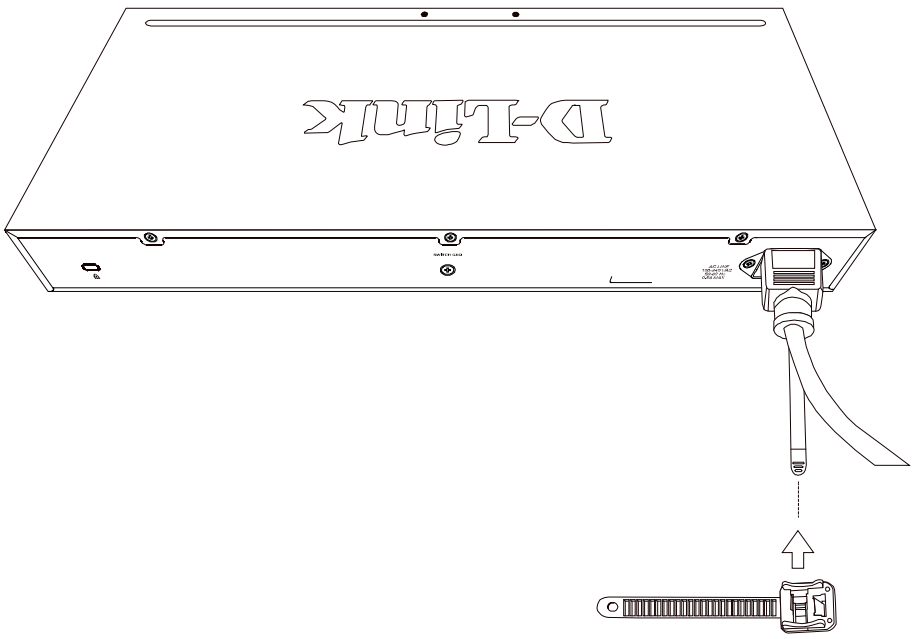


図 2-6　リテイナー（固定具）のスライド

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。

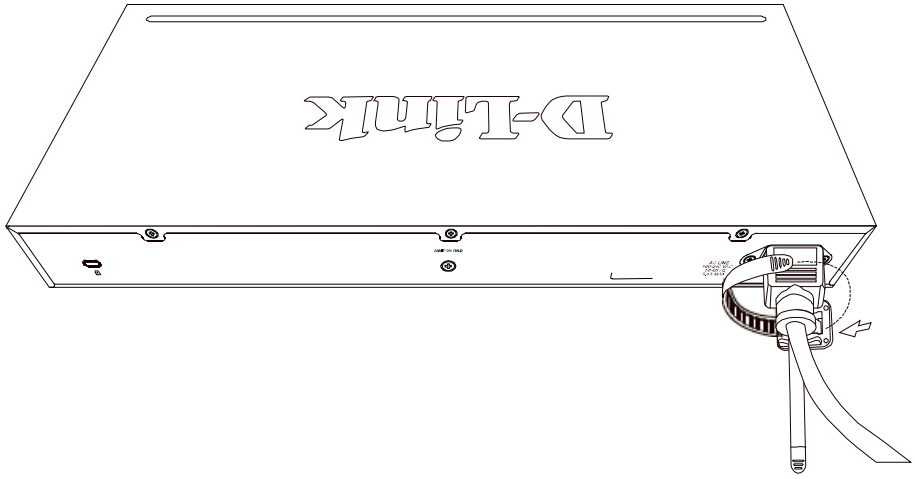


図 2-7　　リテイナーの巻き付け、固定

5. 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。

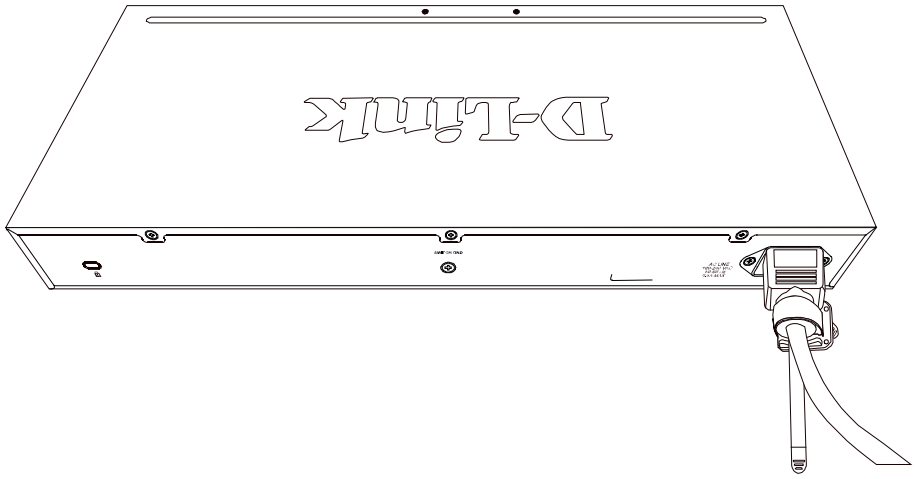


図 2-8　　電源抜け防止器具の固定確認

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
- リング型ラグ端子付接地線（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 - 12 AWG の範囲から適した接地線の使用をお勧めします。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。

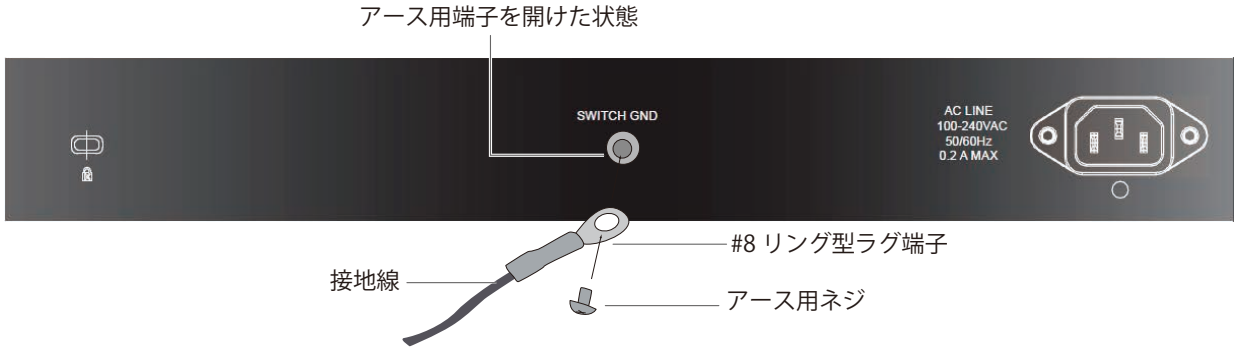


図 2-9　　スイッチへのラグ端子の接続

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。

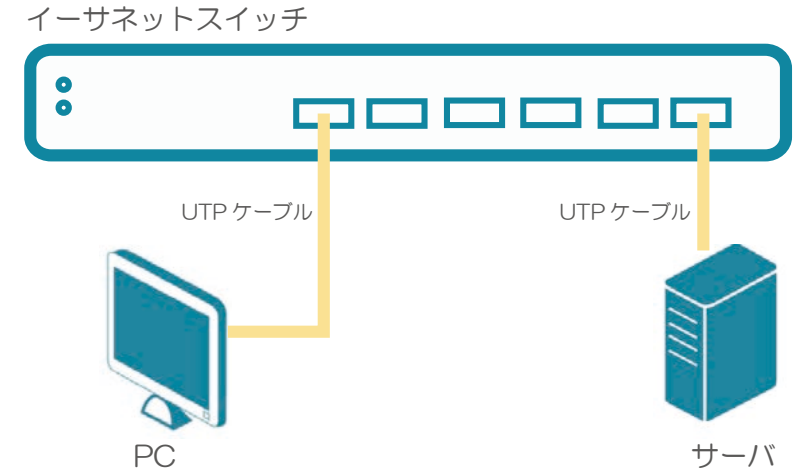


図 3-1　エンドノードと接続した図

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-1210-10MP/28MP 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。

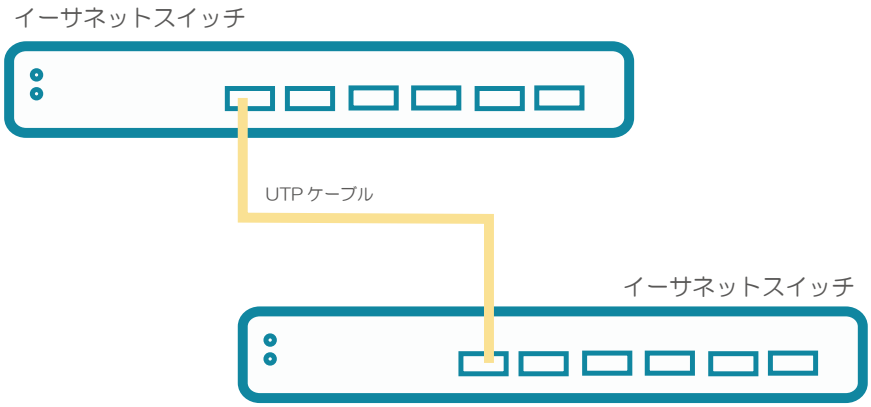


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

2 つまたは 4 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。

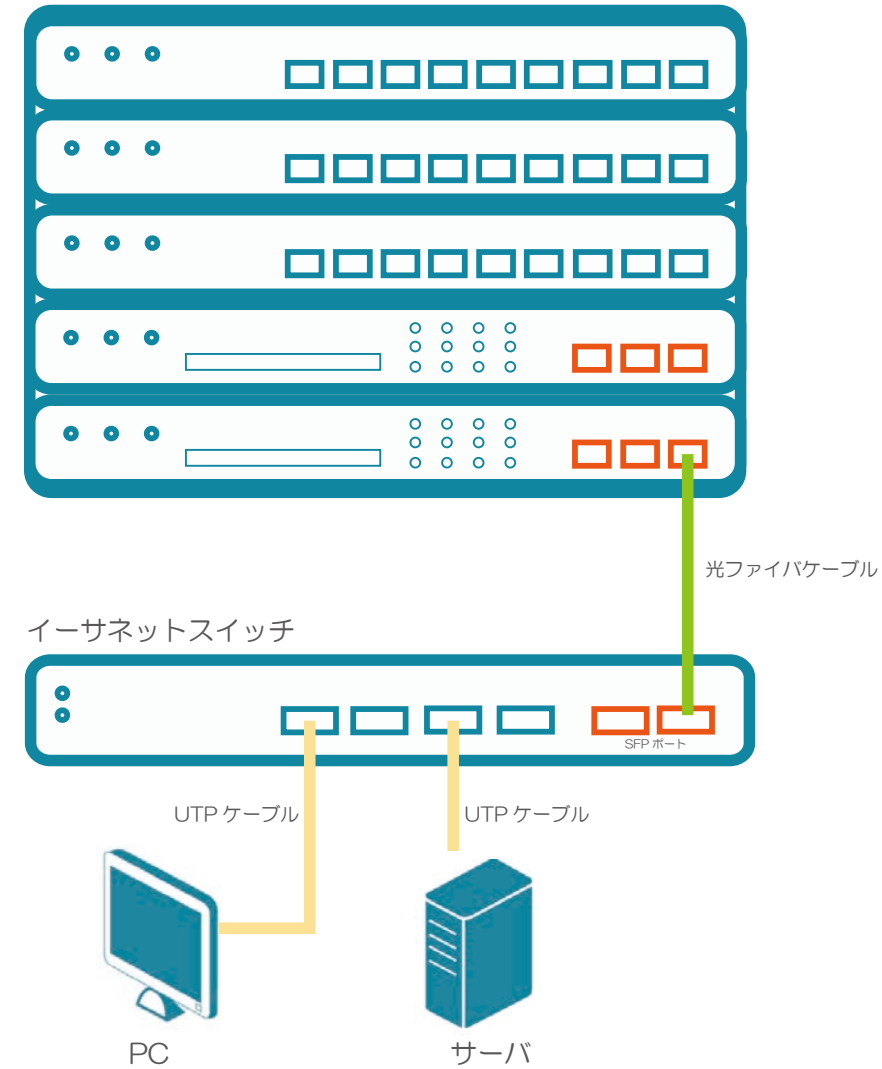


図 3-3　サーバ、PC、スイッチスタックとのアップリンク接続図

第 4 章　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

- Internet Explorer 11 以降
- Mozilla Firefox
- Chrome
- Safari

ブラウザの仕様により互換性が確保されない場合があります。

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。

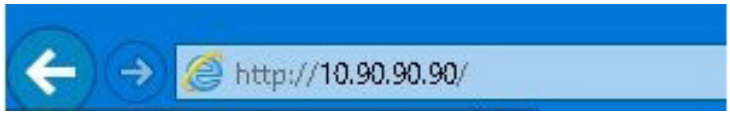


図 4-1　URL の入力

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 4-2　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。

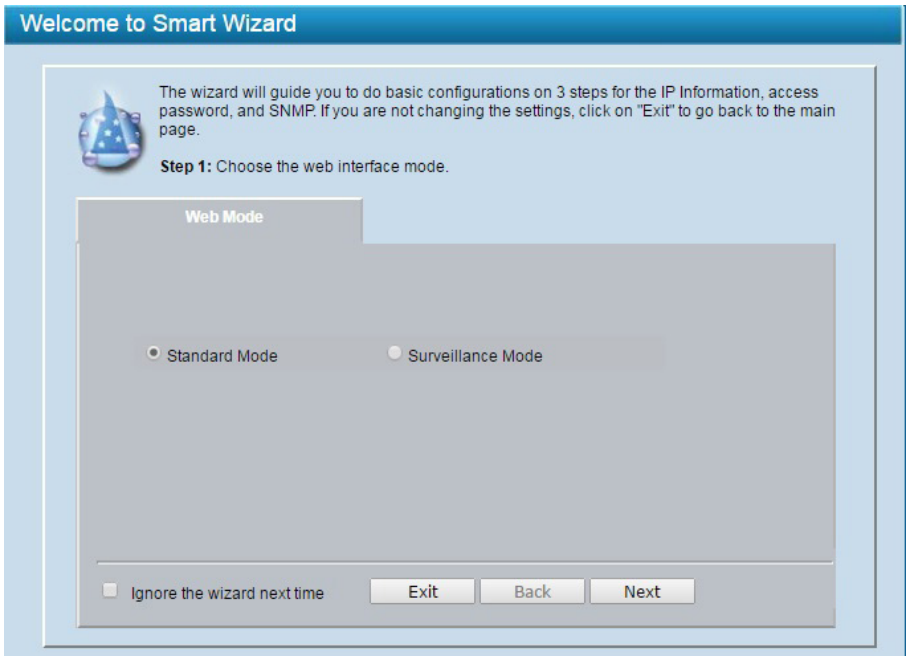


図 4-3　Smart Wizard 画面

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. Web マネージャのメイン画面が表示されます。

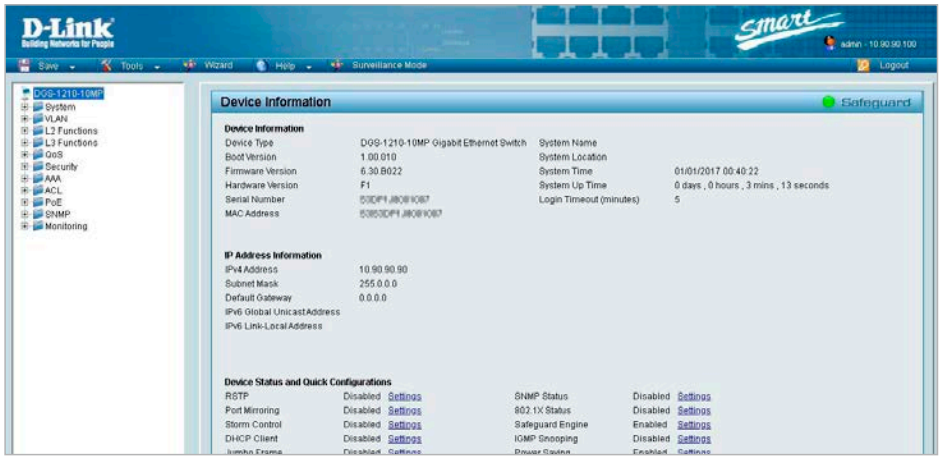


図 4-4　Web マネージャメイン画面

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。
ウィザードの初期ページではまずスイッチの Web モードを「Standard Mode」（スタンダードモード）または「Surveillance Mode」（サーベイランスモード）から指定します。この設定は「Smart Wizard」で再度変更することが可能です。「Surveillance Mode」（サーベイランスモード）の詳細については「第 5 章　サーベイランスモードの設定」を参照ください。

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「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。

補足 「Surveillance Mode」（サーベイランスモード）は IP カメラ機器の管理に特化したモードです。Web マネージャによるシステムの設定に関しては通常「Standard Mode」（スタンダードモード）で行い、本項目以降もスタンダードモードでの設定を基本として説明を行います。

1. WEB モードを選択します。

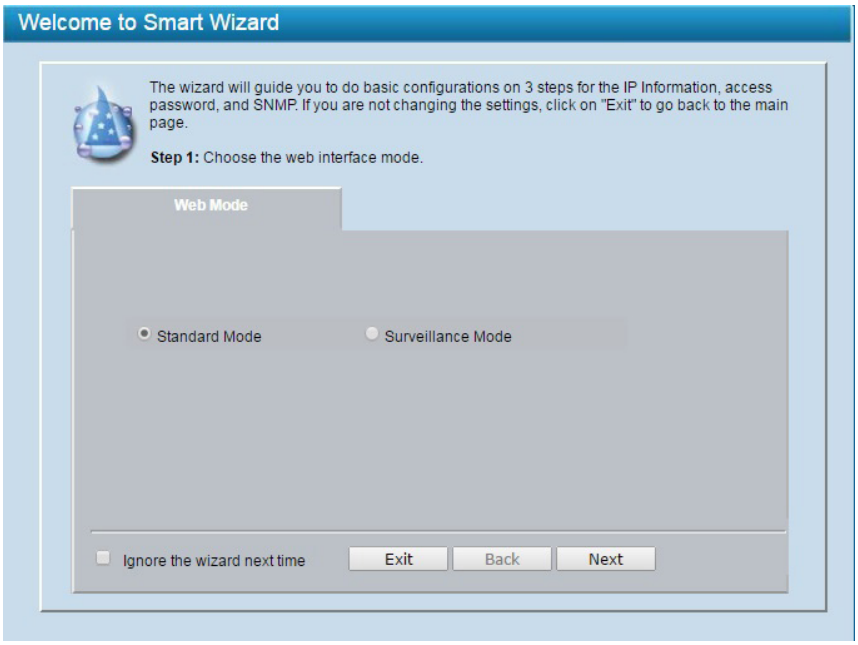


図 4-5　Web Mode 設定画面

- 「Standard Mode」「Surveillance Mode」のいずれかをクリックします。
  - 「Standard Mode」：通常の Web GUI での設定を行います。
  - 「Surveillance Mode」：スイッチを「Surveillance Mode」（サーベイランスモード）として使用します。

- 「Next」をクリックします。

2. IP アドレスの設定を行います。

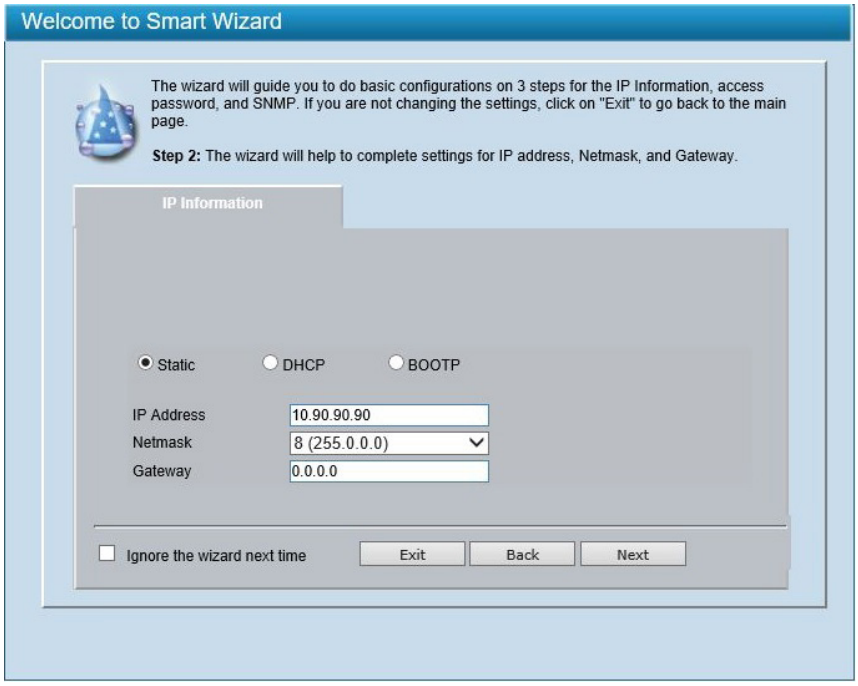


図 4-6　IP Information 設定画面

- 「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

- 「Static」を選択した場合は、「IP Address」「Netmask」「Gateway」を入力します。

- 「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、ウィザード終了時に現在の PC とスイッチの接続が切断されます。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。

3. パスワードの設定を行います。

図 4-7　Password 設定画面

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

4. SNMP の設定を行います。（「Standard Mode」選択時のみ表示されます。）

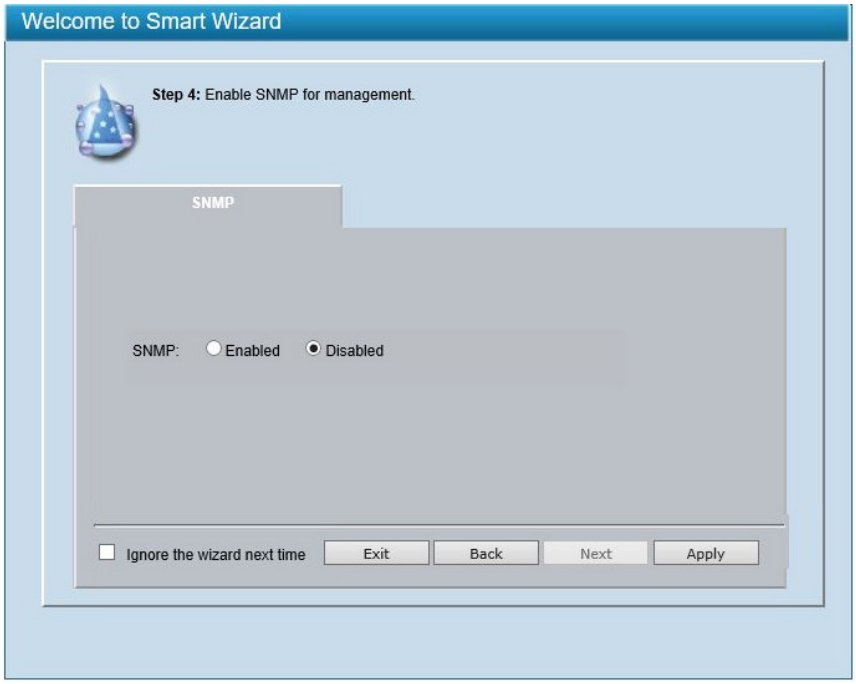


図 4-8　SNMP 設定画面

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

5. Web マネージャ画面が表示されます。

補足 Web UI の各モード（Standard Mode と Surveillance Mode）は、同じコンフィグファイルを共有しています。どちらか一方のインタフェースで有効化された機能は、もう片方のインタフェースでも有効となります。

補足 IP アドレスを変更し「Apply」をクリックした場合は以下の画面が表示されます。「OK」をクリックすると、現在の PC とスイッチの接続が切断されます。再度ログインする際は、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の上、Web ブラウザに新しい IP アドレスを入力してください。

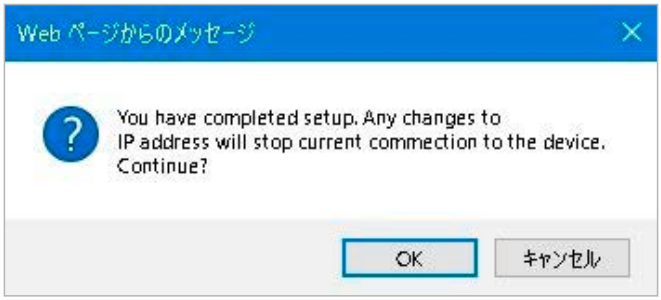


図 4-9　確認画面

補足　サーベイランスモードを選択した場合、以下のインストラクション画面が表示されます。画面下部の「OK」をクリックします。

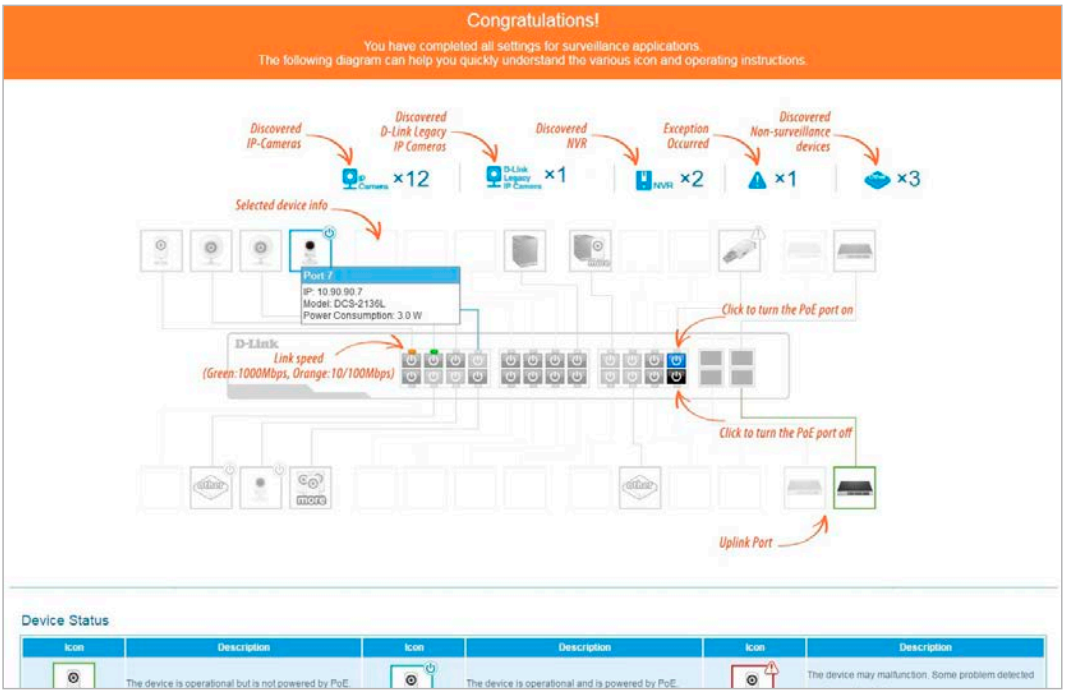


図 4-10　Surveillance Mode クイックスタート画面

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。

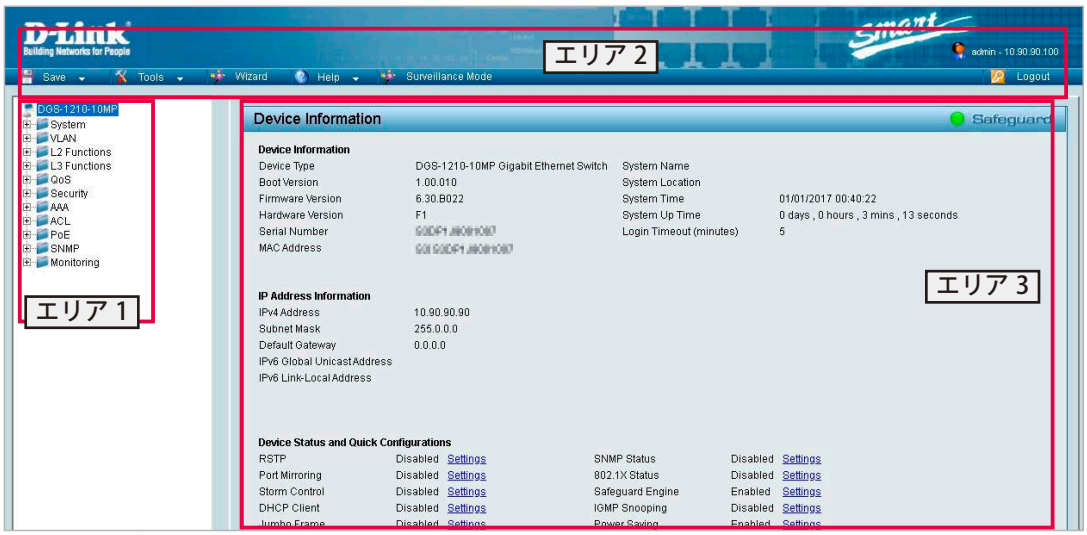


図 4-11　初期画面

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。

画面右上にはユーザ名と現在の IP アドレスが表示されます。ユーザ名の下の「Logout」をクリックし、セッションを終了することができます。

注意　ログアウトボタンを押下せずにブラウザを閉じた場合、セッションは残ったままとなります。

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。

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 & Upgrade	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。
	Flash Information	フラッシュメモリの情報を表示します。
	Nuclias Connect Setting	Nuclias Connect の設定を行います。Nuclias Connect による管理は未サポートです。
	Upload Nuclias Connect File	Nuclias Connect のネットワークファイルをアップロードします。Nuclias Connect による管理は未サポートです。
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、https://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。
Surveillance Mode/Standard Mode		Web 画面モード（Surveillance Mode/Standard Mode）の切り替えを行います。
Logout		Web マネージャ画面からログアウトします。
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。
	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。
	DNS Resolver	DNS リゾルバの設定を行います。
	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。
	System Log Configuration	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	D-Link Discover Protocol の設定を行います。
	Firmware Information	ファームウェア情報の表示、ブートアップイメージの設定を行います。
	Configuration Information	コンフィグ情報の表示、ブートアップコンフィグの設定を行います。
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。
	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。

メイン メニュー	サブメニュー	説明
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行います。
	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行います。
	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。
L3 Functions	IP Interface	IPv6 インタフェースの設定を行います。
	IPv6 Neighbor Settings	IPv6 Neighbor 設定を行います。
	IPv4 Static Route	IPv4 スタティックルートの設定を行います。
	IPv4 Routing Table Finder	IPv4 スタティックルートのテーブルを表示します。
	IPv6 Static Route	IPv6 スタティックルートの設定を行います。
	IPv6 Routing Table Finder	IPv6 スタティックルートのテーブルを表示します。
	ARP	ARP エントリを表示します。
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/TLS	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-1210-10MP/28MP 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-1210-10MP/28MP のみ）
	PD Alive	PD アライブの表示、設定を行います。（DGS-1210-10MP/28MP のみ）
SNMP	System	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。
	Ping Test	Ping テストを行います。

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 4-12　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。 • 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。
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」

項目	説明
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 Settings 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 Global 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。

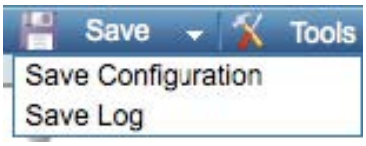


図 4-13　Save メニュー

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. 「config_id 1」または「config_id 2」を選択し、「Save Config」をクリックします。

図 4-14　Save Configuration 画面

3. 「Continue」をクリックします。

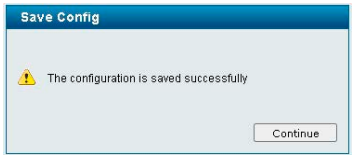


図 4-15　Save Config 画面

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）

ログファイルをローカルドライブに保存します。ログファイルはテキストエディタで閲覧・編集することが可能です。

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、ログファイルを保存します。

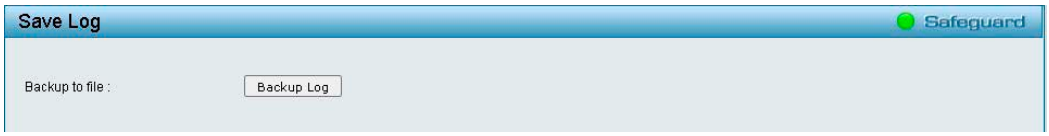


図 4-16　Save Log 画面

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。

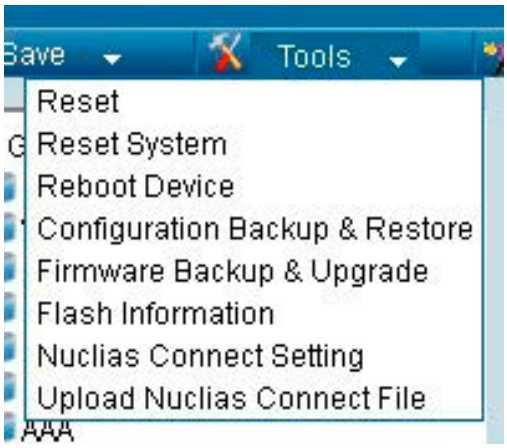


図 4-17　Tools メニュー

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 System」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 4-18　Reset 画面

3. 確認画面で「OK」をクリックします。

図 4-19　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」>「Reset System」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 4-20　Reset System 画面

3. 「OK」をクリックします。

図 4-21　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. 現在の設定を保存する場合は「YES」、保存しない場合は「NO」を選択します。
3. 「Reboot」をクリックします。

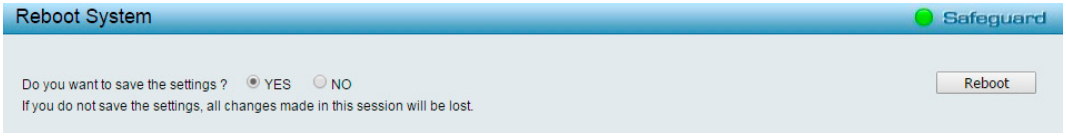


図 4-22　Reboot Device 画面

4. 「OK」をクリックします。

図 4-23　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 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 4-24　Configuration Backup and Restore 画面

3. 以下の項目を設定します。

項目	説明
HTTP	**バックアップ方法** • バックアップ対象のコンフィグ ID を「config_id 1」または「config_id 2」から指定します。 • 「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** • リストア対象のコンフィグ ID を「config_id 1」または「config_id 2」から指定します。 • 「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** • バックアップ対象のコンフィグ ID を「config_id 1」または「config_id 2」から指定します。 • 「TFTP Server IP Address」で「IPv4」「IPv6」「Domain Name」のいずれかを選択し、TFTP サーバの IP アドレスまたはドメイン名を入力します。 • 「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** • リストア対象のコンフィグ ID を「config_id 1」または「config_id 2」から指定します。 • 「TFTP Server IP Address」で「IPv4」「IPv6」「Domain Name」のいずれかを選択し、TFTP サーバの IP アドレスまたはドメイン名を入力します。 • 「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。

4. 「Restore」をクリックした場合、リストア完了の画面が表示されます。画面上の「Continue」をクリックします。

注意　現在のコンフィグとは別の ID を指定して適用した場合、Configuration Information 画面でブート ID を指定してください。

注意　コンフィグレーションの復元後、以下の手順でスイッチを再起動します。
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。

手順

1. 「Tools」>「Reboot Device」の順にメニューをクリックします。
2. 「Do you want to save the settings」の項目で「NO」を選択します。
3. 「Reboot」をクリックします。
4. 「Are you sure you want to reboot device?」メッセージのポップアップウィンドウにおいて、「OK」をクリックします。

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。

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。

注意 アップグレードを行う前に、ご利用の H/W および F/W バージョンを必ずご確認ください。
バージョンの互換性に関する注意事項についてはリリースノートをご確認ください。

注意 V6.30 では新しいイメージファイル（.con）で暗号化に対応しています。
V6.20 以前のバージョンからアップグレードする場合、以下の手順でファームウェアファイルを適用し、アップグレードを実施する必要があります。

① V6.20 以前のバージョンから v6.30.016（.hex）にアップグレード
② もう片方のイメージに v6.30.B022（.con）を適用

※ダウングレードの際は、.con ファイルのイメージから V6.20 以前のバージョンへ直接ダウングレードしていただけます。
※ダウングレードが可能なハードウェアには制限があります。
手順の詳細はリリースノートをご確認ください。

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 4-25　Firmware Backup and Upgrade 画面

3. 以下の項目を設定します。

項目	説明
HTTP	**バックアップ方法** • バックアップ対象のイメージ ID を「image_id 1」または「image_id 2」から指定します。 • 「Backup」をクリックし、現在のイメージファイル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 /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** • 「TFTP Server IP Address」で「IPv4」「IPv6」「Domain Name」のいずれかを選択し、TFTP サーバの IP アドレスまたはドメイン名を入力します。 • 「TFTP File Name」にファイル名を入力します。 • バックアップ対象のイメージ ID を「image_id 1」または「image_id 2」から指定します。 • 「Backup」をクリックし、現在のイメージファイルを指定した TFTP サーバに保存します。 **アップグレード方法** • 「TFTP Server IP Address」で「IPv4」「IPv6」「Domain Name」のいずれかを選択し、TFTP サーバの IP アドレスまたはドメイン名を入力します。 • 「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 ファームウェアのアップグレードを行う際に TFTP を使用する場合は、セーフガードエンジン機能を無効にする必要がありますのでご注意ください。

注意 リンクアグリゲーション（LAG）、スパニングツリー（STP）を使用している場合は、ファームウェアアップグレードの操作中、DGS-1210 の動作が不安定になる可能性があるため、ネットワークから切り離して実施してください。

注意 HTTPS 経由でのファームウェアアップグレードには対応していません。

Flash Information（フラッシュメモリ情報）

フラッシュメモリの詳細情報を表示します。

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

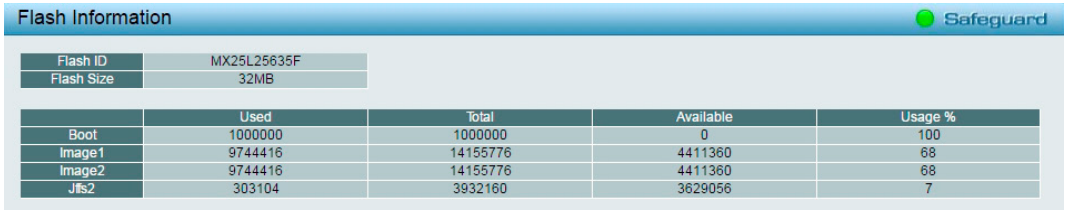


図 4-26　Flash Information 画面

Nuclias Connect Setting（Nuclias Connect 設定）

スイッチの Nuclias Connect 設定を行います。
Nuclias Connect は、ネットワーク機器をソフトウェアまたはアプライアンス機器から集中管理することが可能な Web クライアントベースの日本語 UI 対応の管理ツールです。簡単かつ直感的な操作でネットワークの構築や拡張をサポートすることができます。

注意　Nuclias Connect による管理は未サポートです。

1. 「Tools」>「Nuclias Connect Setting」の順にメニューをクリックします。

図 4-27　Nuclias Connect Setting 画面

2. 「Nuclias Connect State」を「Enabled」（有効）または「Disabled」（無効）に設定します。
「Nuclias Connect Status」には、Nuclias Connect のステータスが表示されます。
3. 「Apply」をクリックし、設定を保存します。

Upload Nuclias Connect File（Nuclias Connect ファイルのアップロード）

Nuclias Connect ファイルのアップロードを行います。

注意　Nuclias Connect による管理は未サポートです。

1. 「Tools」>「Upload Nuclias Connect File」の順にメニューをクリックします。

図 4-28　Upload Nuclias Connect File 画面

2. 「ファイルを選択」でファイルを選択し「Upload」（アップロード）をクリックします。

Smart Wizard メニュー（スマートウィザード）

「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 4-29　User Guide 画面

Surveillance Mode（サーベイランスモード）

Web 管理画面を Surveillance Mode（サーベイランスモード）に切り替えます。

1. 「Surveillance Mode」メニューをクリックします。
2. 以下の確認メッセージが表示されるので、「OK」をクリックします。

図 4-30　確認画面

補足　サーベイランスモードに移行すると、ASV2.0、LBD、SNMP、SNMP トラップがグローバルで有効になります。また、VLAN メンバポートはアップリンクポートを除いてタグなしポートになります。

3. 「OK」をクリックします。

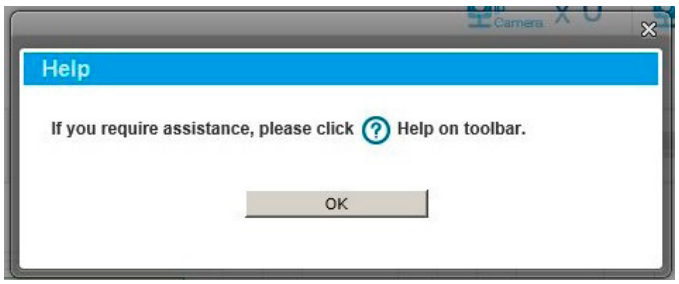


図 4-31　確認画面

4. 以下の画面が表示されます。

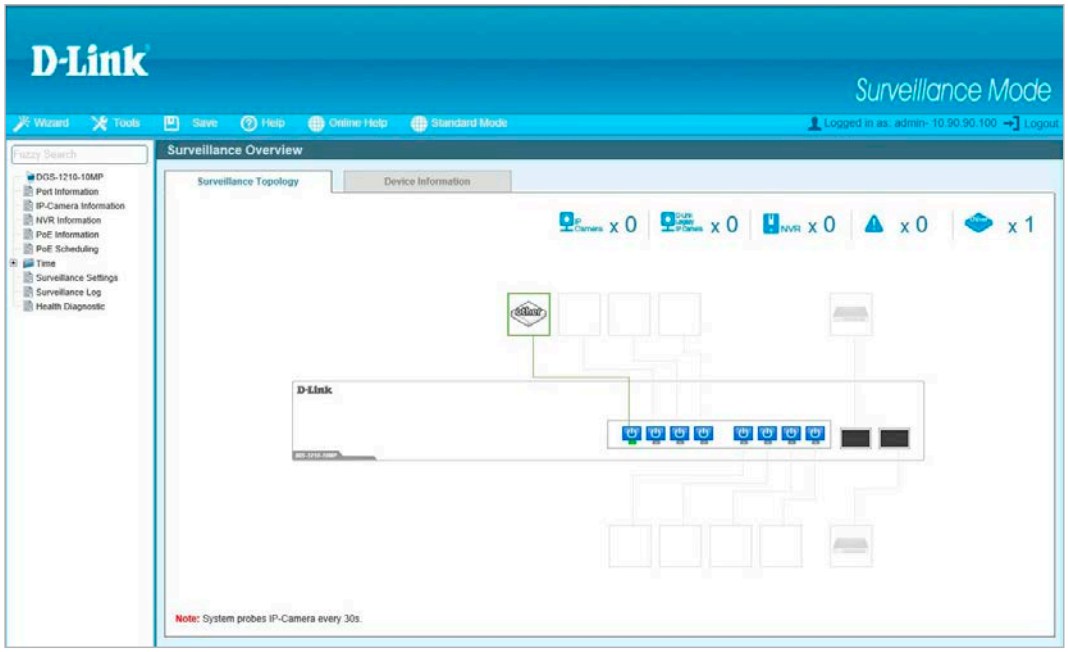


図 4-32　Surveillance Mode 画面

補足　サーベイランスモード画面でツールバーの「Standard Mode」をクリックすると、スタンダードモード画面に切り替わります。

補足　サーベイランスモード画面の詳細については「第 5 章　サーベイランスモードの設定」を参照してください。

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）

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。

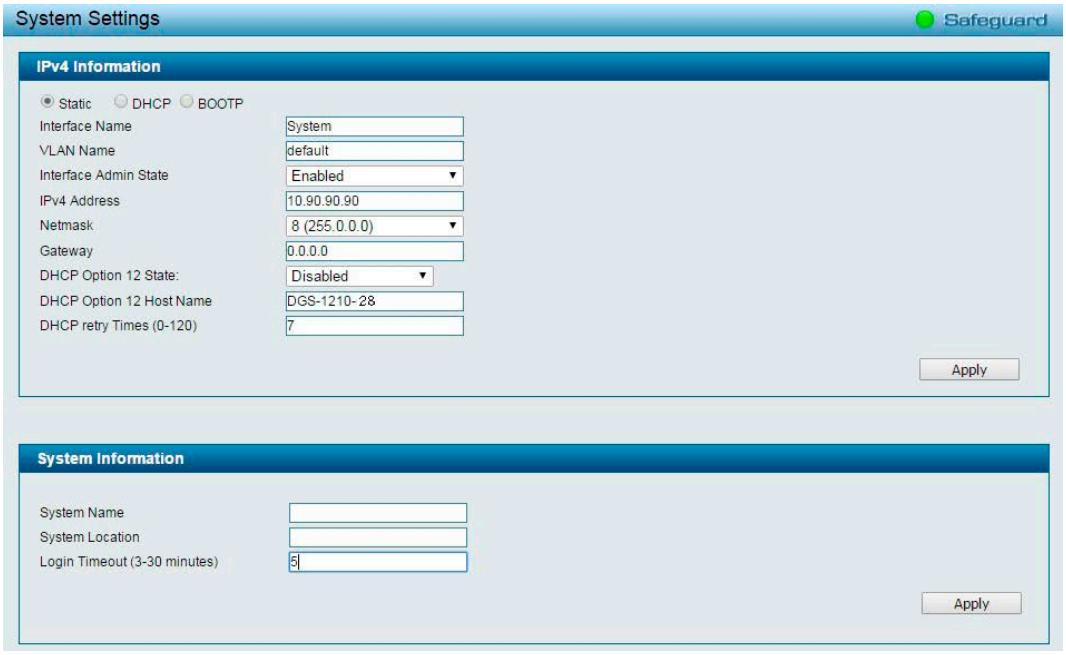


図 4-33　System Settings 画面

2. 以下の項目を設定します。

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。 • 「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。
Interface Name	「Static」を選択した場合、IP インタフェース名を設定します。
VLAN NAME	「Static」を選択した場合、IP VLAN 名を設定します。
Interface Admin State	IP インタフェースの管理を「Enabled」（有効）/「Disabled」（無効）にします。
IPv4 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。
DHCP Retry Times	DHCP リトライ回数を指定します。 • 設定可能範囲：0-120（回）
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。
System Location	ネットワーク上のスイッチの場所を入力します。
Login Timeout	Web GUI 上で操作が行われない場合に、自動的にログアウトする時間を指定します。 指定した時間が経過するとログアウトし、再ログインが要求されます。 • 初期値：5（分） • 設定可能範囲：3-30（分）

3. 「Apply」をクリックし、設定を有効にします。

補足 「IP Information」の設定を行った場合は画面上部の「Apply」を、「System Information」の設定を行った場合は画面下部の「Apply」をクリックしてください。

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。

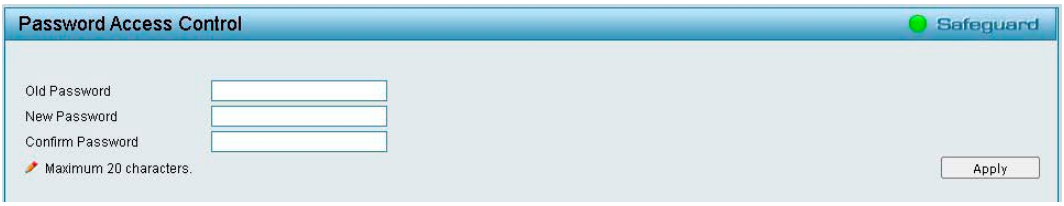


図 4-34　Password Access Control 画面

2. 以下の項目を設定します。

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。

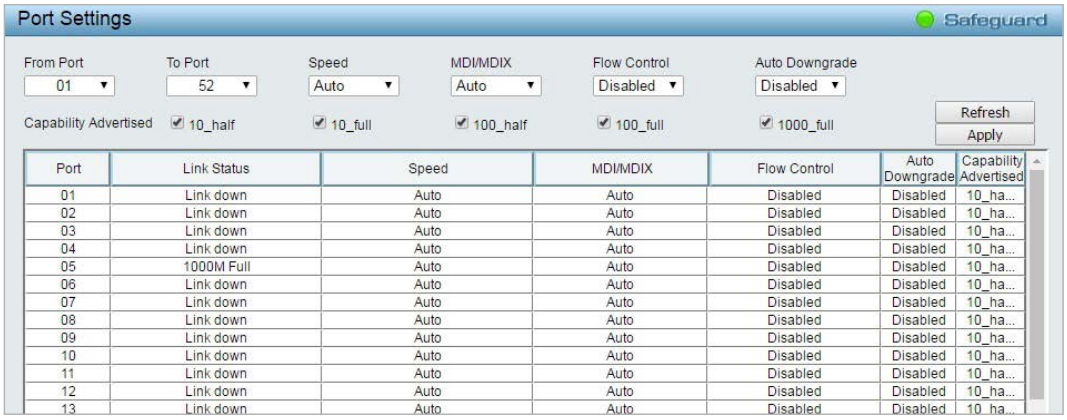


図 4-35　Port Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
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「100M Full」、「100M Half」または「Disable」を指定します。
MDI/MDIX	MDI/MDIX 機能の設定を選択します。 • 「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」（初期値）- 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」
Auto Downgrade	アドバタイズ速度を自動的に低下させる機能を「Enabled」（有効）/「Disabled」（無効）にします。 「Speed」が「Auto」に設定されている場合に有効です。 • 初期値：「Disabled」
Capability Advertised	「Speed」が「Auto」に設定されている場合、オートネゴシエーション時に、選択したケイパビリティがアドバタイズされます。

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）

各ポートの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。

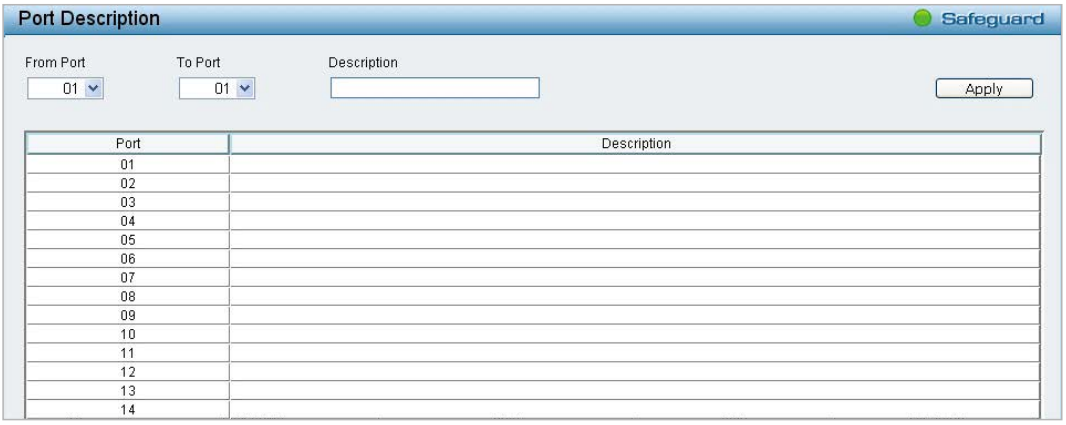


図 4-36　Port Description 画面

2. 以下の項目を設定します。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
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。

DNS Resolver（DNS リゾルバ設定）

DNS リゾルバは、ドメイン名を照会して IP アドレスを割り出す機能です。

DNS Resolver Global Setting（DNS リゾルバグローバル設定）

DNS リゾルバのグローバル設定を行います。

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

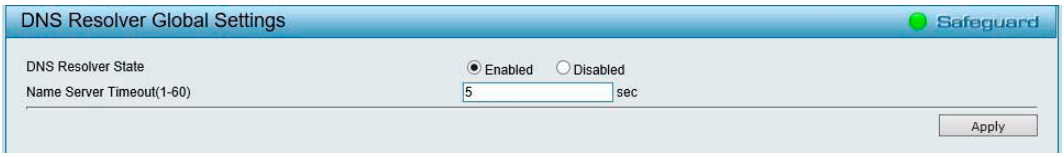


図 4-37　DNS Resolver Global Settings 画面

2. 以下の項目を設定します。

項目	説明
DNS Resolver State	DNS リゾルバを「Enabled」（有効）/「Disabled」（無効）に設定します。 • 初期値：「Enabled」
Name Server Timeout	指定のネームサーバからの応答を待つ最大時間を設定します。 • 設定可能範囲：1-60（秒） • 初期値：5（秒）

3. 「Apply」をクリックし、設定を有効にします。

DNS Resolver Static Name Server Settings（DNS リゾルバスタティックネームサーバ設定）

DNS リゾルバのネームサーバを作成します。

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

図 4-38　DNS Resolver Static Name Server Settings 画面

2. 以下の項目を設定します。

項目	説明
Server IP Address	DNS リゾルバのネームサーバ IP アドレスを入力します。最大 3 つのネームサーバを登録できます。
Primary	プライマリネームサーバとして設定します。
Secondary	セカンダリネームサーバとして設定します。
Third	サードネームサーバとして設定します。

3. 「Add」をクリックし、設定を有効にします。

エントリを削除する場合は「Delete」をクリックします。

DNS Resolver Dynamic Name Server Table（DNS リゾルバダイナミックネームサーバテーブル）

ダイナミック DNS ネームサーバの情報を表示します。

1. 「System」>「DNS Resolver」>「DNS Resolver Dynamic Name Server Table」の順にメニューをクリックします。

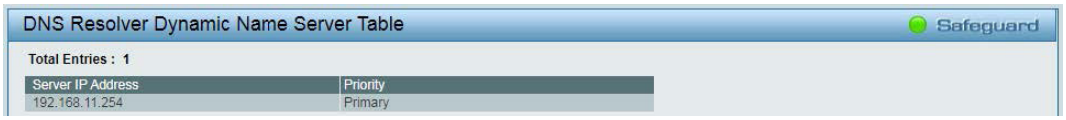


図 4-39　DNS Resolver Dynamic Name Server Table 画面

DNS Resolver Static Host Name Settings（DNS リゾルバスタティックホストネーム設定）

ユーザが手動で DNS エントリを追加できます。
本製品は最大 16 のスタティックエントリをサポートしています。

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

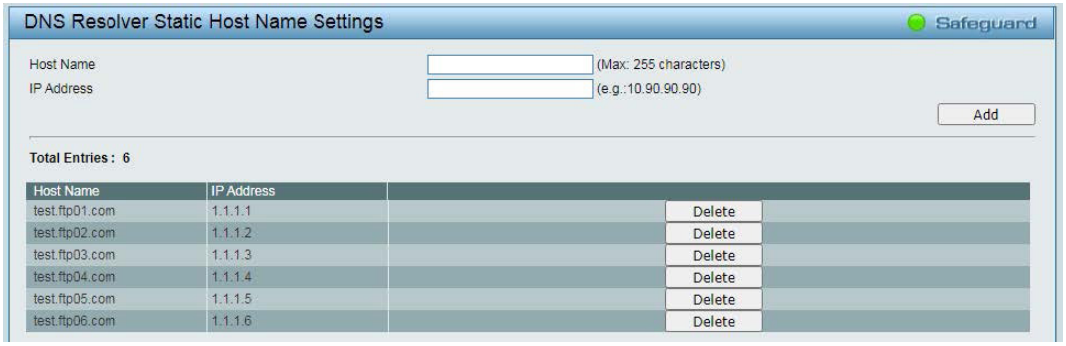


図 4-40　DNS Resolver Static Host Name Settings 画面

2. 以下の項目を設定します。

項目	説明
Host Name	ホスト名を入力します。
IP Address	IP アドレスを入力します。

3. 「Add」をクリックし、設定を有効にします。

エントリを削除する場合は「Delete」をクリックします。

DNS Resolver Dynamic Host Name Table（DNS リゾルバスダイナミックホストネームテーブル）

ダイナミックに学習した DNS エントリを表示します。表示できる最大エントリ数は 10 です。

1. 「System」>「DNS Resolver」>「DNS Resolver Dynamic Host Name Table」の順にメニューをクリックします。

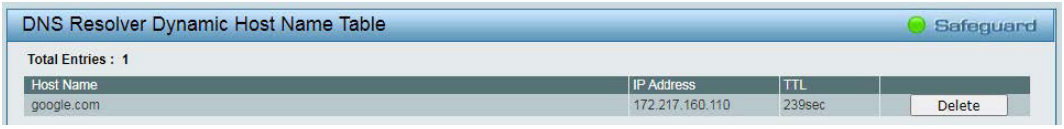


図 4-41　DNS Resolver Dynamic Host Name Table 画面

エントリを削除する場合は「Delete」をクリックします。

DHCP Auto Configuration（DHCP 自動設定）

DHCP 自動設定機能は、TFTP サーバから自動的にコンフィグレーションファイルを取得する機能です。

本機能を有効にすると、スイッチは DHCP クライアントになり、次回起動時に 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。これを実現するには、DHCP サーバが DHCP オプションにより TFTP サーバの IP アドレスとコンフィグレーションファイル名情報を配信する必要があります。スイッチからリクエストを受信したときに、実行中の TFTP サーバのベースディレクトリに必要な設定ファイルを保存しておく必要があります。

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

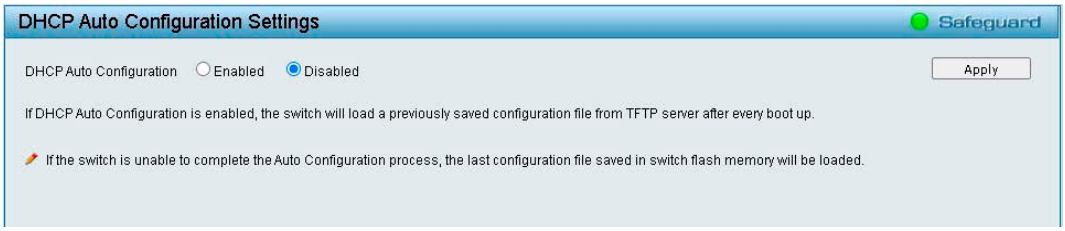


図 4-42　DHCP Auto Configuration Settings 画面

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。

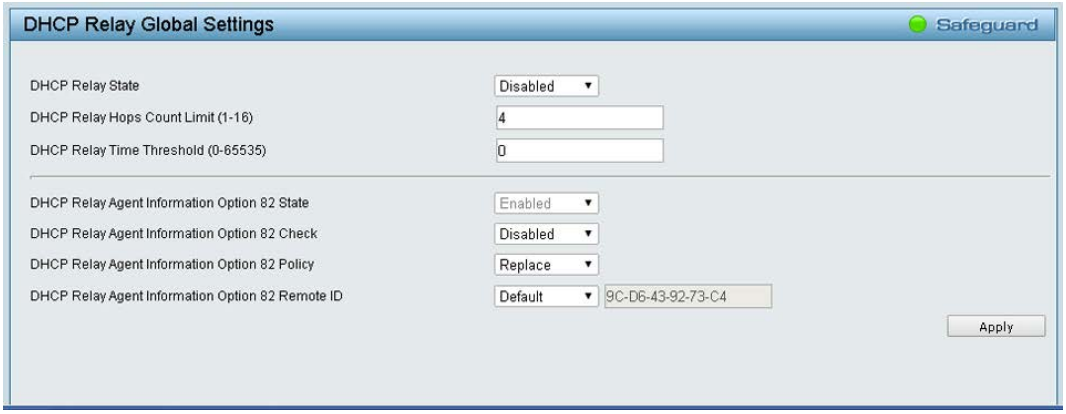


図 4-43　DHCP Relay Global Settings 画面

2. 以下の項目を設定します。

項目	説明
DHCP Relay State	スイッチ上で DHCP リレーを「Enabled」（有効）/「Disabled」（無効）にします。 • 初期値：「Disabled」
DHCP Relay Hops Count Limit	DHCP メッセージが中継されるルータホップの最大数を設定します。 • 設定可能範囲：1-16 • 初期値：4
DHCP Relay Time Threshold	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 を指定すると、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。 • 設定可能範囲：0-65535 • 初期値：0
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。 • 「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 request がスイッチにより中継されている場合には、DHCP サーバはユニキャストで 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 情報が挿入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」（初期値）- リレーエージェントは DHCP サーバとクライアント間で交換するメッセージへの DHCP Relay Information（「Option 82」欄）の挿入 / 削除を行いません。また、以下の Option 82 のチェックとポリシーの項目は無効になります。
DHCP Relay Agent Information Option 82 Check	スイッチのパケットの Option 82 項目の妥当性のチェックを行う機能を「Enabled」（有効）/「Disabled」（無効）にします。 • 「Enabled」- リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行います。スイッチが DHCP クライアントから Option 82 項目を含むパケットを受信すると、スイッチはこれらのパケットは不正だとしてパケットを廃棄します。リレーエージェントは DHCP サーバから受信したパケットから不正なメッセージを削除します。 • 「Disabled」- リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行いません。
DHCP Relay Agent Information Option 82 Policy	DHCP エージェント情報オプション 82 のチェック機能が無効の場合の処理を指定します。 • 「Replace」（初期値）- 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「User Define」（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 IP アドレスを登録します。
リレーエージェントのインタフェースは「System」に固定されます。

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

図 4-44　DHCP Relay Interface Settings 画面

2. 以下の項目を設定します。

項目	説明
Interface	DHCP サーバに直接接続するスイッチの IP インタフェースを選択します。
Server IP	DHCP サーバの IP アドレスを入力します。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。

注意 複数の IPv4 Interface を設定した際に、DHCP Relay は適切に機能しません。

注意 DHCP Relay において指定する Server IP は、DGS-1210 に設定された IP Interface と同一 IP Segment である必要があります。

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 ローカルリレーが有効化されると、スイッチは LAN（VLAN）内で DHCP リレーエージェントとして動作します。DHCP ブロードキャストはスイッチによりトラップされ、置き換えられます。また、DHCP オプション 82 がホスト発信元 DHCP パケットに挿入されます。

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

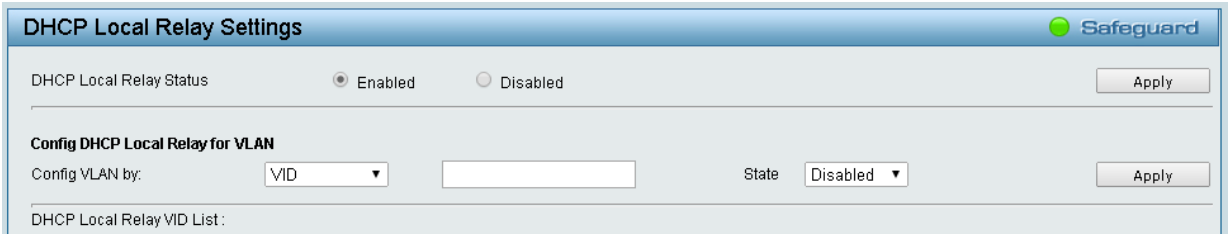


図 4-45　DHCP Local Relay Settings 画面

2. 以下の項目を設定します。

項目	説明
DHCP Local Relay Status	ローカルリレーのグローバルステート機能を「Enable」（有効）または「Disable」（無効）にします。 • 初期値：「Disabled」
Config DHCP Local Relay for VLAN	
Config VLAN by	「VLAN Name」または「VID」をドロップダウンメニューから選択し、ユーザが DHCP ローカルリレーに適用する VLAN 名または VID を入力します。
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。
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。

補足　「DHCP Local Relay Status」の有効化 / 無効化の設定を行った場合は画面上部の「Apply」を、「Config DHCP Local Relay for VLAN」の設定を行った場合は画面下部の「Apply」をクリックしてください。

注意　複数の IPv4 Interface を設定した際、DHCP Relay は適切に機能しません。

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。

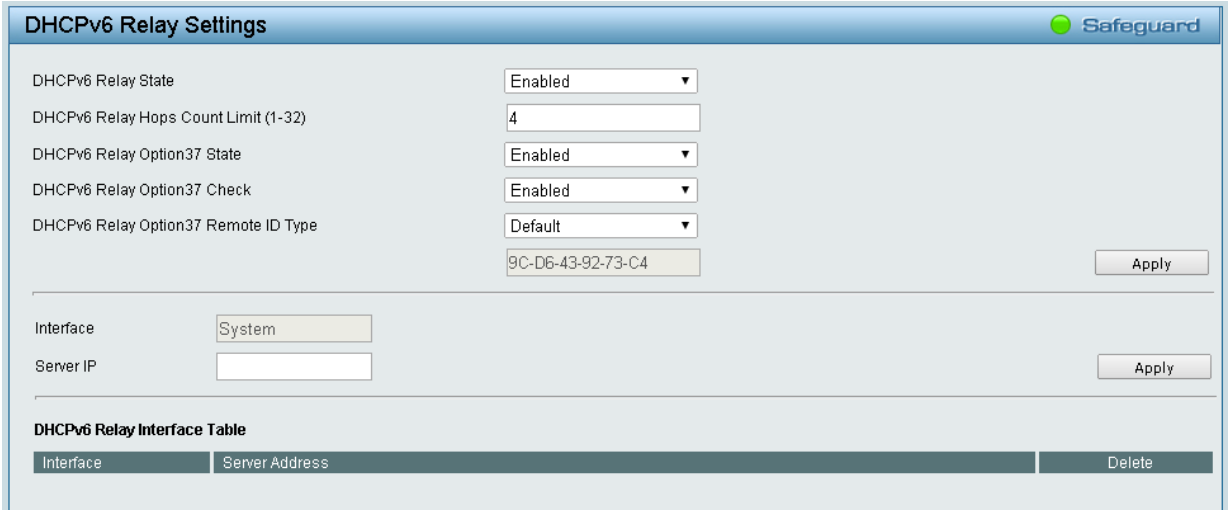


図 4-46　DHCPv6 Relay Settings 画面

2. 以下の項目を設定します。

項目	説明
DHCPv6 Relay State	DHCPv6 リレー機能を「Enabled」（有効）/「Disabled」（無効）にします。
DHCPv6 Relay Hops Count Limit	DHCPv6 メッセージが転送されるルータホップの最大数を定義します。 • 設定可能範囲：1-32 • 初期値：4
DHCPv6 Relay Option37 State	「DHCPv6 Relay Option37 State」を「Enabled」（有効）/「Disabled」（無効）にします。
DHCPv6 Relay Option37 Check	「DHCPv6 Relay Option37 Check」を「Enabled」（有効）/「Disabled」（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。 • 選択肢：「Default」「CID With User Defined」「User Defined」
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。

補足　設定を変更したセクション毎に「Apply」をクリックしてください。

注意　RA に関する機能実装がないため、複数の IPv6 Interface を設定した際、DHCPv6 Relay は適切に機能しません。

System Log Configuration（システムログ設定）

システムログの設定を行います。「System」>「System Log Configuration」をクリックし、フォルダから設定項目を選択します。

System Log Settings（システムログ設定）

システムログを有効化し、フラッシュメモリにログの保存を行う間隔やトリガを設定します。

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

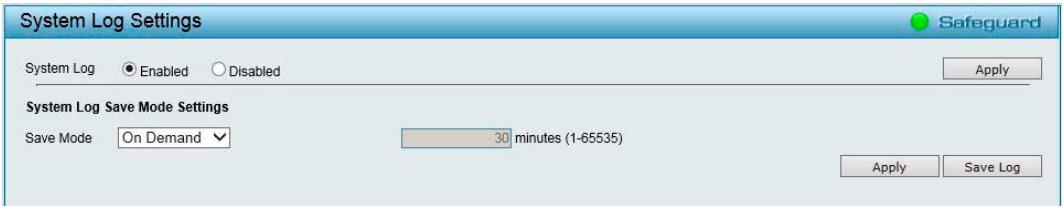


図 4-47　System Log Settings 画面

2. 以下の項目を設定します。

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」
System Log Save Mode Settings	
Save Mode	ログの保存方法を選択します。 • 「On Demand」-「Save Log」機能などによりユーザが手動で保存操作を実施した場合のみ、ログを保存します。 • 「Time Interval」- ログファイルを定期的に保存します。 • 「Log Trigger」- ログイベントの発生毎にログを保存します。
minutes (1-65535)	「Save Mode」で「Time Interval」を選択した場合に、ログが保存される間隔を設定します。 • 設定可能範囲 : 1-65535（分）

3. 「Apply」をクリックし、設定を有効にします。

補足　「System Log」の有効化 / 無効化の設定を行った場合は画面上部の「Apply」を、「System Log Save Mode Settings」の設定を行った場合は画面下部の「Apply」をクリックしてください。

補足　スイッチのフラッシュメモリにログを保存するには、「Save Log」をクリックしてください。

Syslog Host（Syslog ホスト設定）

ログを受信するシスログホストの設定を行います。
ログが送信される対象となるイベントは、「Severity」で設定される重要度によって決まります。

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

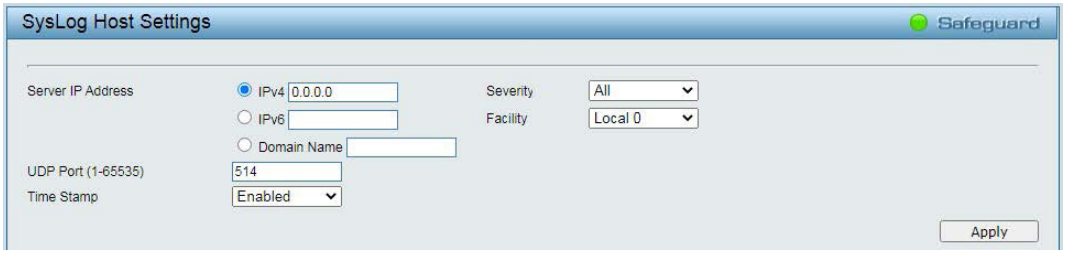


図 4-48　Syslog Host Settings 画面

2. 以下の項目を設定します。

項目	説明
Server IP Address	「IPv4」「IPv6」「Domain Name」のいずれかを選択し、システムログサーバの IP アドレスまたはドメイン名を入力します。
UDP Port	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	指定した重要度以上のイベントが発生した場合に、サーバに対してメッセージが送信されます。 重要度レベルは 3 種類あります。 • 「Warning」- 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る場合にシステムログが送信されます。 • 「Informational」- デバイス情報が送信されます。 • 「All」（初期値）- すべての重要度レベルのシステムログが送信されます。
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。

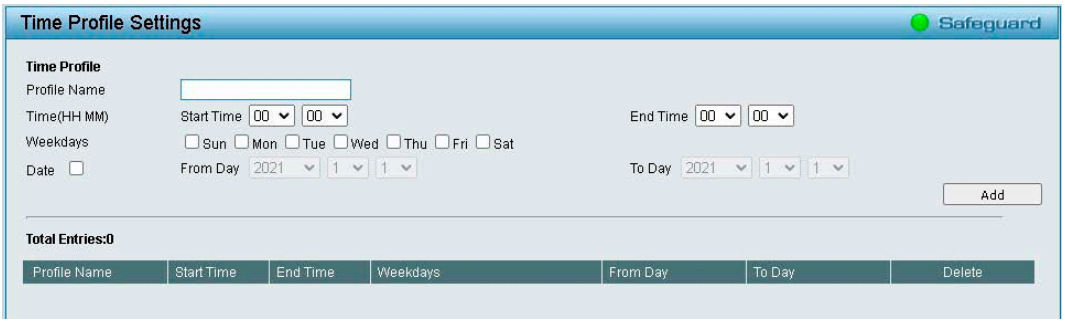


図 4-49　Time Profile Settings 画面

2. 以下の項目を設定します。

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	曜日を指定します。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。

注意　「Date」と「Weekdays」の両方を指定した場合、「指定した期間」内の「指定した曜日」がタイムプロファイルの設定になります。

Power Saving（省電力設定）

スケジュールによる各種省電力機能が利用可能です。電力を抑えることで、発熱量を抑えて製品寿命を延ばし、稼働コストを抑えることができます。

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

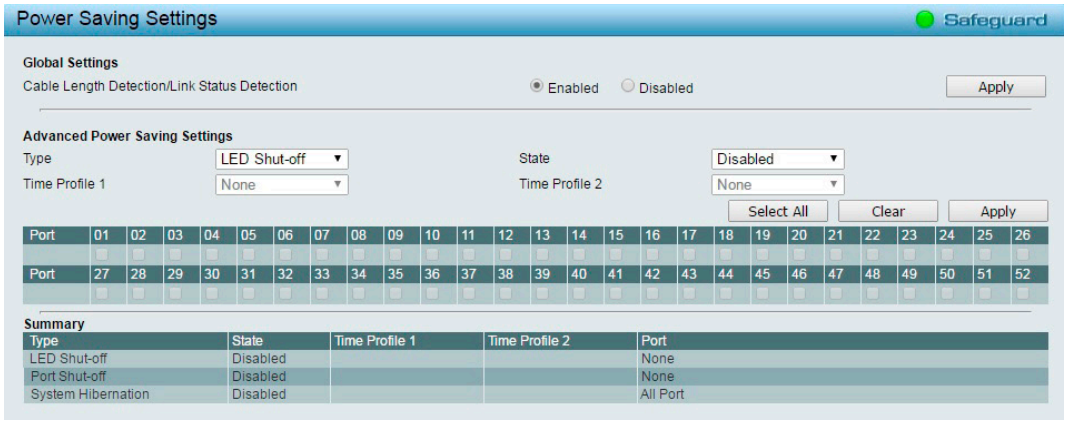


図 4-50　Power Saving Settings 画面

2. 以下の項目を設定します。

項目	説明
Global Settings	
Cable Length Detection/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。 • 「LED Shut-off」　優先度：高 「LED Shut-off」が選択され、「Status」が無効の場合、タイムプロファイル機能は適用されません。つまり、ステータスが無効の場合、タイムプロファイルが終了時刻になっても LED は点灯しません。有効の場合、タイムプロファイルに従って動作します。 • 「Port Shut-off」　優先度：高 「Port Shut-off」が選択され、「Status」が無効の場合、タイムプロファイル機能は適用されません。優先度のルールは「LED Shut-off」と同様です。 • 「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。

補足　「Global Settings」の有効化 / 無効化の設定を行った場合は画面上部の「Apply」を、「Advanced Power Saving Settings」の設定を行った場合は画面下部の「Apply」をクリックしてください。

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 4-51　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。

注意　EEE の有効化 / 無効化により、インタフェースがリンクアップ / リンクダウンします。

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

DNA などの D-Link 管理ユーティリティで使用する D-Link Discovery Protocol (DDP) を設定します。

注意　D-Link Network Assistant（DNA）のサポートは終了しております。

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

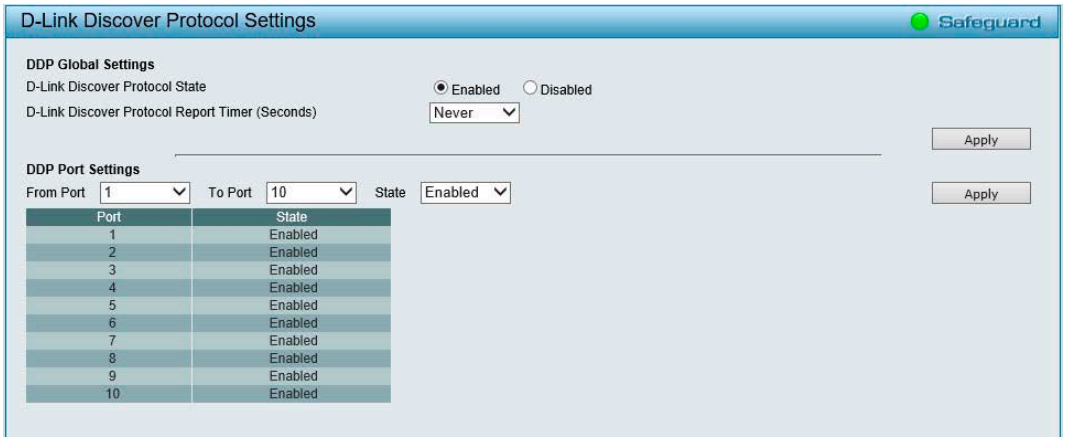


図 4-52　D-Link Discover Protocol Settings 画面

2. 以下の項目を設定します。

項目	説明
DDP Global Settings	
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。 • 選択肢：「30」「60」「90」「120」（秒）、「Never」
DDP Port Setting	
From Port / To Port	設定を行うポートを指定します。
State	「Enabled」（有効）または「Disabled」（無効）を選択します。

3. 「Apply」をクリックし、設定を適用します。

Firmware Information（ファームウェア情報）

ファームウェアの情報を表示します。
また、次回スイッチが起動した際にブートアップを行うイメージファイルを選択することができます。

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

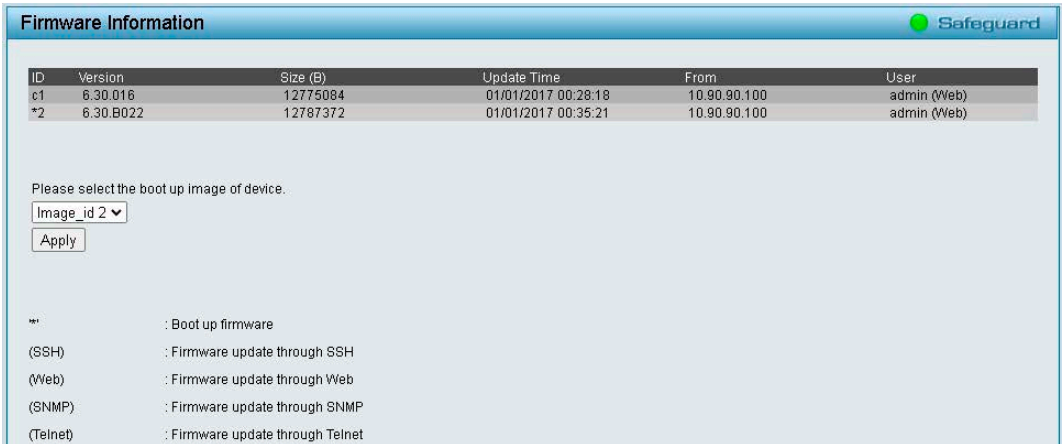


図 4-53　Firmware Information 画面

2. 次回スイッチが起動した際にブートアップを行うイメージファイルの ID を選択します。
3. 「Apply」をクリックし、設定を有効にします。

Configuration Information（コンフィグレーション情報）

コンフィグレーションの情報を表示します。次回スイッチが起動した際にブートアップを行うコンフィグファイルを選択することができます。

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

図 4-54　Configuration Information 画面

2. コンフィグ ID を選択します。
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。

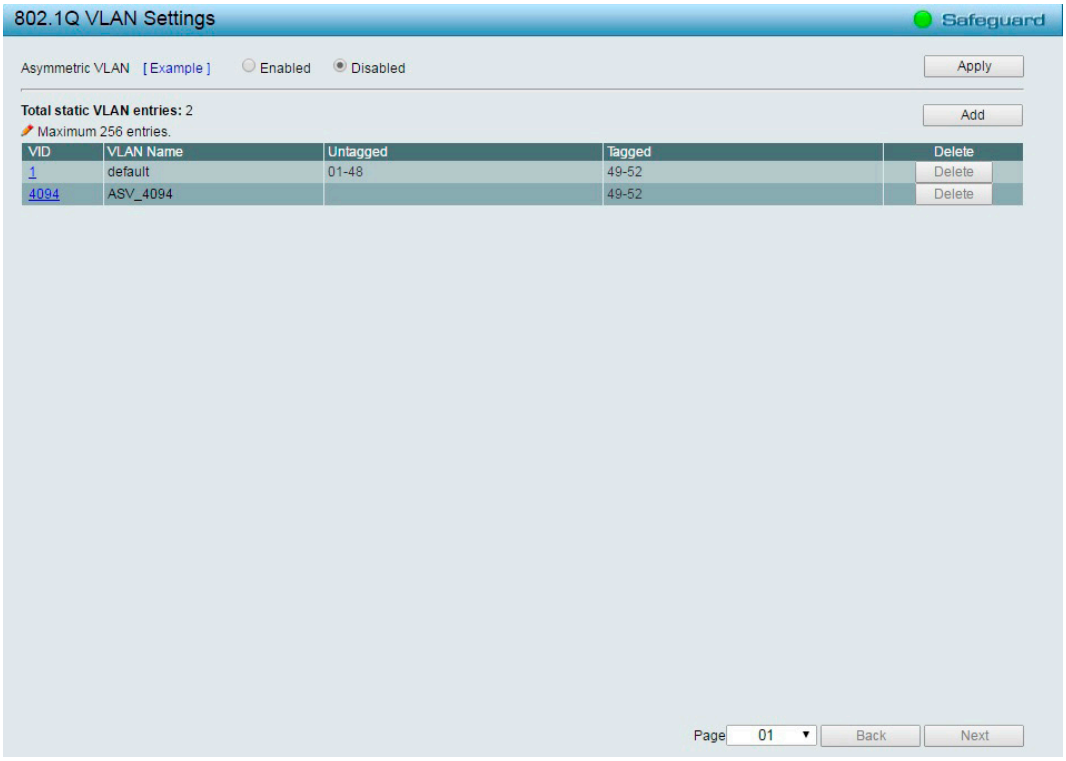


図 4-55　802.1Q VLAN Settings 画面

2. 以下の項目を設定します。

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。

注意　Asymmetric VLAN、Traffic Segmentation は Unknown ユニキャストのフィルタはできません。

注意　Asymmetric VLAN の機能は、複数の IP Interface を作成している状態では有効にできません。

■ **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 4-56　802.1Q 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、以下の画面を表示します。

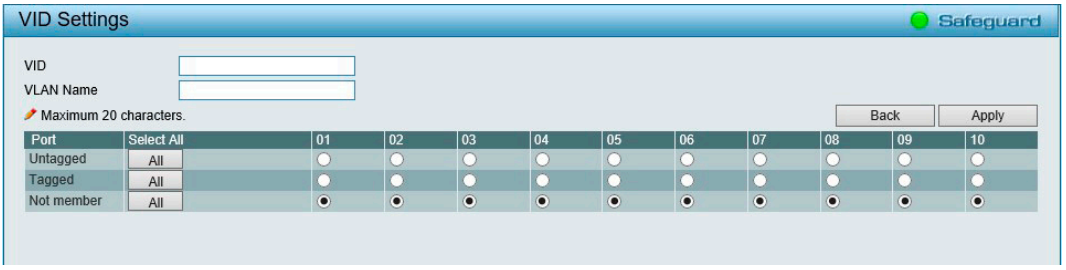


図 4-57　VID Settings 画面

2. 以下の項目を設定します。

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。

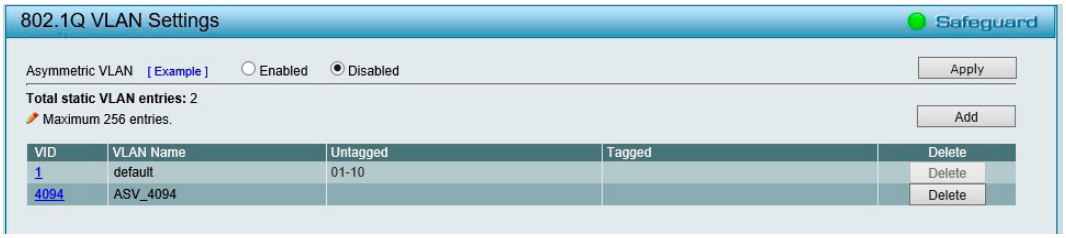


図 4-58　802.1Q VLAN Settings 画面

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 4-59　802.1Q 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。

Voice VLAN（音声 VLAN 設定）

音声ネットワークの品質を保つには、低遅延（高優先度）でリアルタイムにトラフィック転送を行う必要があります。
音声 VLAN 機能を利用すると、音声トラフィックを高い優先度を持つ VLAN グループで処理することができます。

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。

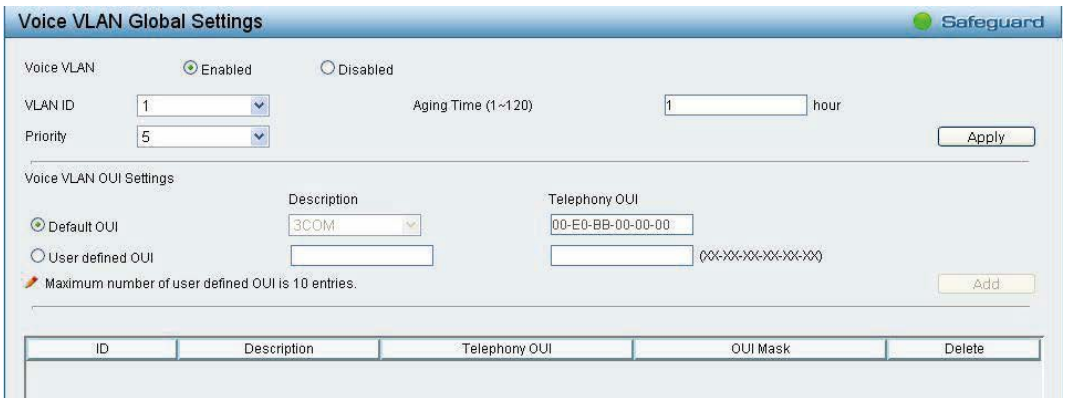


図 4-60　Voice VLAN Global Settings 画面

2. 以下の項目を設定します。

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：0-7
Aging Time	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。 • 設定可能範囲：1-120（時間） • 初期値：1（時間） 補足 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。 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

スイッチには定義済みの 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自動的に割り当て VLAN へ所属させ、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。

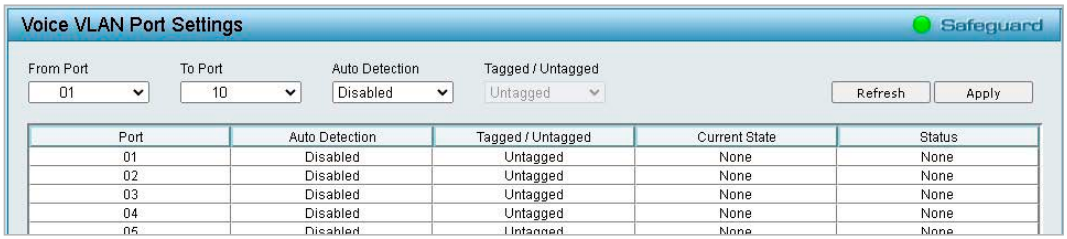


図 4-61　Voice VLAN Port Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port / To Port	設定対象のポート範囲を指定します。
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、表示を最新の状態に更新できます。

Voice Device List（音声デバイスリスト）

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 4-62　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」をクリックすると、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）

サーベイランス機器の音声・映像トラフィックの品質を保つには、低遅延（高優先度）でリアルタイムにトラフィック転送を行う必要があります。自動サーベイランス VLAN 機能を利用すると、これらのトラフィックを高い優先度を持つ VLAN グループで処理することができます。

Auto Surveillance Properties（自動サーベイランスプロパティ設定）

自動サーベイランス VLAN の設定や表示を行います。

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

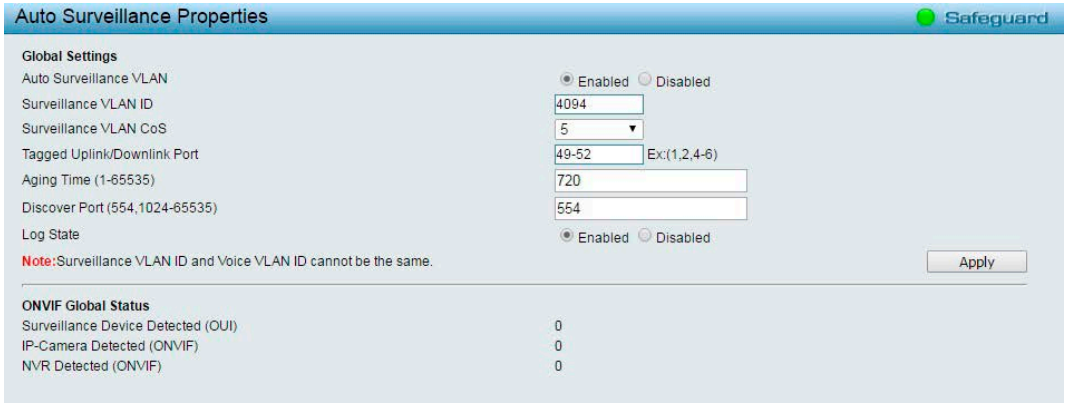


図 4-63　Auto Surveillance Properties 画面

2. 以下の項目を設定します。

項目	説明
Auto Surveillance VLAN	自動サーベイランス VLAN 機能を「Enabled」（有効）または「Disabled」（無効）にします。 • 初期値：「Disabled」
Surveillance VLAN ID	サーベイランス VLAN ID を設定します。 • 初期値：4094
Surveillance VLAN CoS	サーベイランス VLAN のプライオリティを設定します。 • 設定可能範囲：0-7 • 初期値：5
Tagged Uplink/ Downlink Port	自動サーベイランス 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。
Aging Time	サーベイランス VLAN のエージングタイムを設定します。 • 設定可能範囲：1-65535（分） • 初期値：720（分） 補足 自動サーベイランス VLAN のメンバポートについて、サーベイランス VLAN から削除されるまでの時間を設定します。最後のサーベイデバイスがトラフィックの送信を停止し、MAC アドレスがエージングアウトした場合、サーベイランス VLAN エージングタイマが開始されます。サーベイランス VLAN エージングタイマが期限切れになると、サーベイランス VLAN からポートが削除されます。エージングタイムの間にサーベイランストラフィックが再開されると、エージングタイマはリセットされ、停止します。
Discover Port	サーベイランス VLAN の TCP/UDP ポート番号を設定します。 • 設定可能範囲：554, 1024-65535 • 初期値：554 補足 RTSP ストリームスヌーピングの TCP/UDP ポート番号の構成に使用されます。ONVIF 対応 IPC と ONVIF 対応 NVR は、WS-Discovery を使用して他のデバイスを検出します。IPC が検出されると、スイッチは IPC・NVR 間の RTSP、HTTP、HTTPS パケットをスヌーピングして、NVR を検出することができます。TCP/UDP ポート番号が RTSP ポート番号と異なる場合、これらのパケットをスヌーピングすることはできません。
Log State	自動サーベイランス VLAN のログを「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。

MAC Settings and Surveillance Device（MAC 設定およびサーベイデバイス）

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。優先度の高い個別の VLAN を使用することで、サーベイランス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」>「MAC Settings and Surveillance Device」の順にメニューをクリックします。

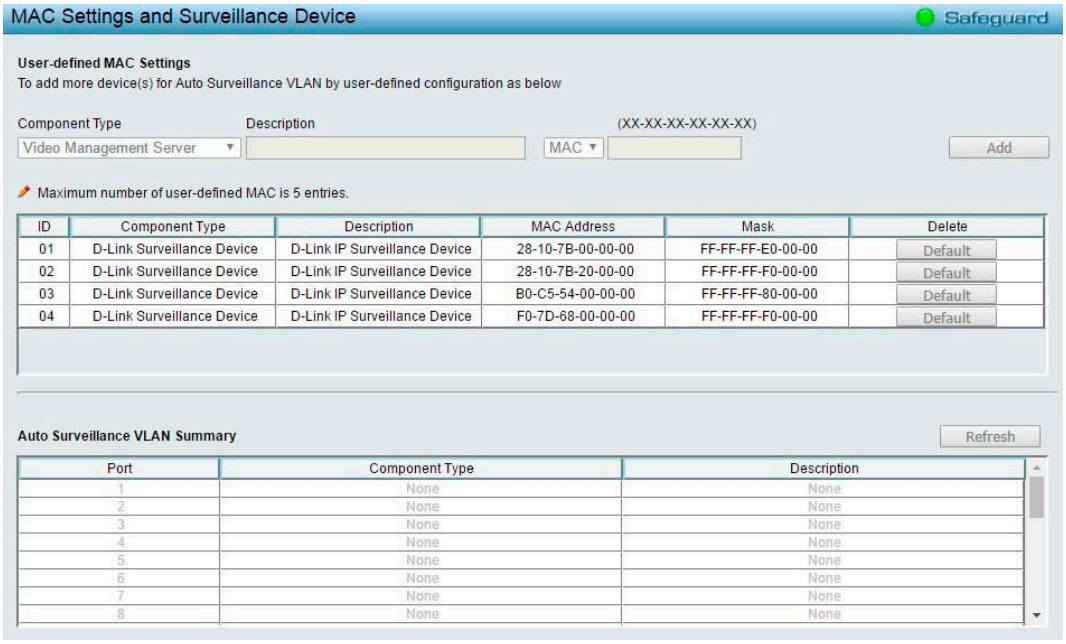


図 4-64　MAC Settings and Surveillance Device 画面

2. 以下の項目を設定します。

項目	説明
Component Type	自動サーベイランス VLAN は、デフォルトで D-Link サーベイデバイスを検出します。その他、以下 5 種類のコンポーネントタイプについて、自動で検出を行うように設定することが可能です。 • 選択肢： 「Video Management Server (VMS)」「VMS Client/Remote viewer」「Video Encoder」「Network Storage」 「Other IP Surveillance Devices」
Description	サーベイランスコンポーネントに対し、MAC や OUI アドレスを設定することができます。 設定可能な MAC アドレス数は 5 つです。
MAC Address	自動サーベイランス VLAN の優先度を指定します。
Mask	MAC または OUI アドレスのマスクアドレスを指定します。

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、「Auto Surveillance VLAN Summary」の表示内容を更新できます。

ONVIF IPC Information（ONVIF IPC 情報）

ONVIF IPC 情報 では、スイッチに接続された各 IP カメラの情報を表示します。ポート番号、IP アドレス、MAC アドレス、スループット、ポート概要、モデル名などが表示されます。

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

図 4-65　ONVIF IPC Information 画面

ONVIF NVR Information（ONVIF NVR 情報）

ONVIF NVR 情報 では、スイッチに接続された各 NVR の情報を表示します。
ポート番号、IP アドレス、MAC アドレス、IP カメラ番号、スループット、NVR に接続されたカメラに関する説明（グループ名、接続カメラの台数、ポート、IP アドレス）などが表示されます。

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

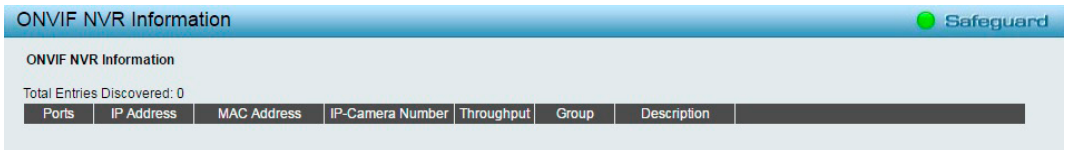


図 4-66　ONVIF NVR Information 画面

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 10,000 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 4-67　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。

注意　CPU インタフェースではジャンボフレームがサポートされません。

注意　ジャンボフレーム無効時の最大フレームサイズはタグ付きフレームで 1518 bytes までとなります。

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。

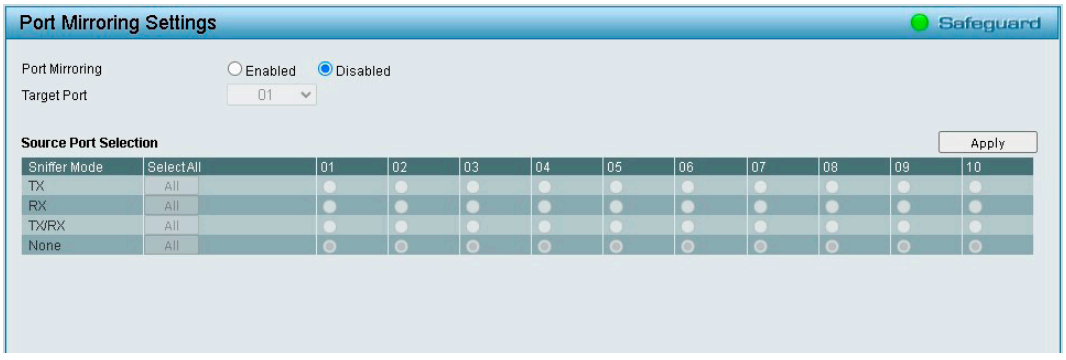


図 4-68　Port Mirroring Settings 画面

2. 以下の項目を設定します。

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。（送信モード） 「All」をクリックすると、すべてのポートが選択されます。
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。（受信モード） 「All」をクリックすると、すべてのポートが選択されます。
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。（送受信モード） 「All」をクリックすると、すべてのポートが選択されます。
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。

注意　Port Mirroring の機能において、複数の Source Port を指定した場合に、重複する パケットは Mirror されません。

注意　Port Mirroring の機能において、Source Port Selection に TX/RX を指定した場合、Switching 対象の パケットは Mirror されません。

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。

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

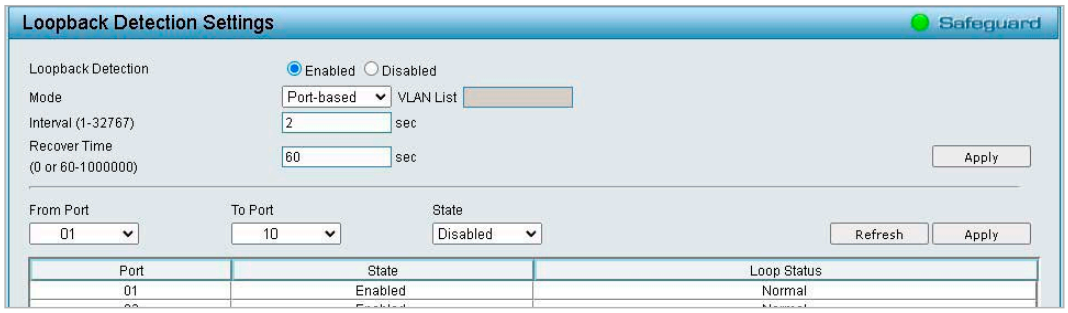


図 4-69　Loopback Detection Settings 画面

2. 以下の項目を設定します。

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いる 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	ループ検知間隔を設定します。 • 設定可能範囲：1-32767（秒） • 初期値：2（秒）
Recover Time	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。 • 設定可能範囲：0 または 60-1000000（秒） • 初期値：60（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。

補足　ポート毎のステータス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。

注意　LBD を VLAN-based mode でご利用の場合に、同時に検出可能な VLAN 数は検出順に 8 までに制限されます。

注意　CTP（Configuration Testing Protocol）の送信元 MAC アドレスとして、ポート MAC アドレスではなく、システム MAC アドレスを使用します。

注意　LBD と Link Aggregation の併用はできません。

MAC Address Table（MAC アドレステーブル）

Static MAC Settings（スタティック MAC 設定）

フォワーディングテーブルに MAC アドレスエントリを作成します。通常、ネットワークで固定で使用されるデバイス（DHCP サーバ、シスログサーバ、ゲートウェイなど）が接続されているポートに設定されます。

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

図 4-70　Static MAC Settings 画面

2. 以下の項目を設定します。

■ 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. 「Port」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。

注意　スタティック MAC の機能について、LAG ポートへの登録は出来ません。

注意　MAC アドレス学習において最大テーブル数の 1% 以上のロスが発生します。

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。

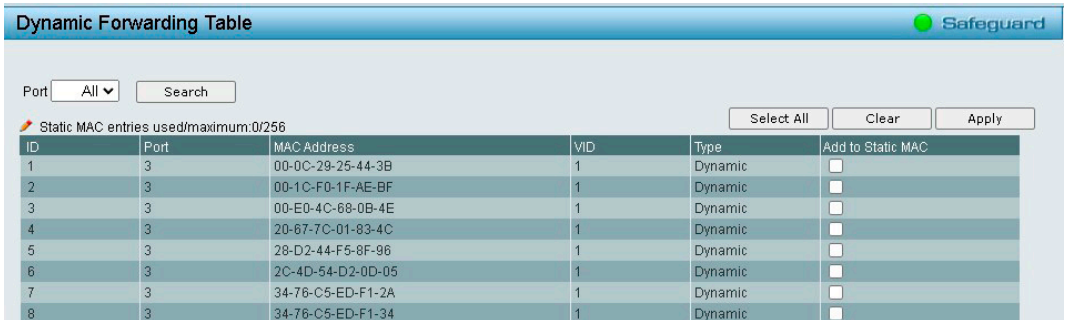


図 4-71　Dynamic Forwarding Table 画面

2. 以下の項目を設定します。

■ 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。

注意　Asymmetric VLAN を有効にした場合、Dynamic Forwarding Table の VID は「N/A」と表示されます。

Forwarding Table Aging Time Settings（フォワーディングテーブルエージングタイム設定）

フォワーディングテーブルのエージングタイムを設定します。

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

図 4-72　Forwarding Table Aging Time Settings 画面

2. 「Forwarding Table Aging Time」の値を編集します。
3. 「Apply」をクリックし、設定を変更します。

注意　実際のエージングタイムは、「設定した値」から「設定した値の 2 倍」の間になります。

Spanning Tree（スパニングツリー設定）

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

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

MSTP（Multiple STP Protocol）は IEEE 委員会により定義された標準規格で、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングし、ネットワーク上に複数の経路を提供します。ロードバランシングが可能となるため、 1 つのインスタンスに障害が発生した場合でも、広い範囲に影響を与えないようにすることができます。障害発生時には、障害が発生したインスタンスに代わって新しいトポロジが素早く収束されます。

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。RSTP/MSTP では、ルートブリッジから BPDU を受信しなくても BPDU パケットが Hello パケット送信毎に送信されます。ブリッジ間の各リンクはリンクの状態を素早く検知することができるため、リンク断絶時の素早い検出とトポロジの調整が可能となります。

初期値では MST が有効です。受信デバイスへの BPDU パケットにタグ付けを行い、スパニングツリーインスタンス、スパニングツリーリージョン、それらに紐づく VLAN を識別します。

STP Bridge Global Settings（スパニングツリーグローバル設定）

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

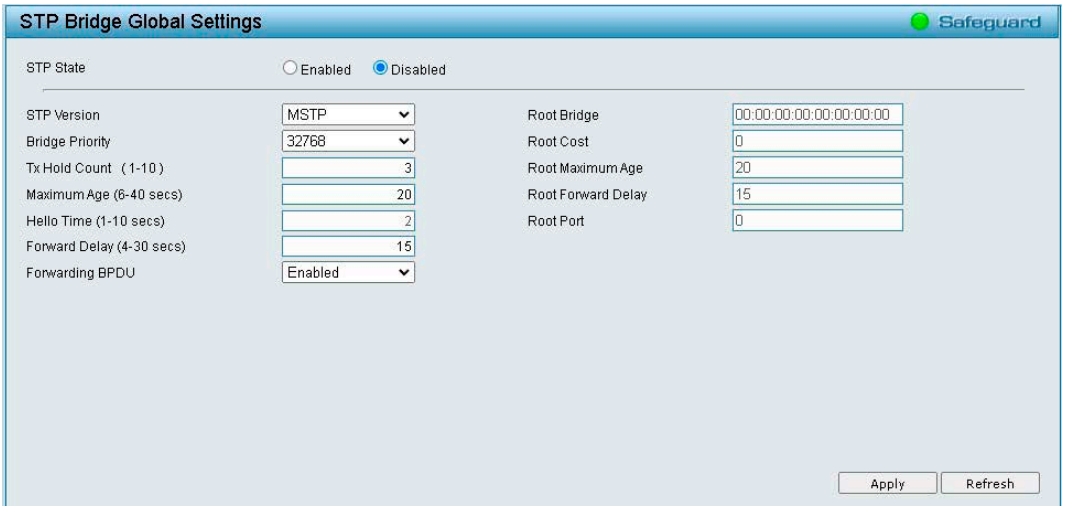


図 4-73　STP Bridge Global Settings 画面

2. 以下の項目を設定します。

項目	説明
STP State	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	STP のバージョンを選択します。 • 選択肢：「RSTP」「STP」「MSTP」 • 初期値：「MSTP」
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。 • 設定可能範囲：0-61440 • 初期値：32768
Tx Hold Count	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。 • 設定可能範囲：1-10 • 初期値：3

項目	説明
Maximum Age	最大経過時間を設定します。 • 設定可能範囲：6 - 40（秒） • 初期値：20（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	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。 • 設定可能範囲：1 - 10（秒） • 初期値：2（秒） 補足 「Maximum Age」の値は以下の公式を満たす数値を設定する必要があります。 『　Maximum Age の値 >= (2 × (Hello Time" + 1.0))　』
Forward Delay	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。 • 設定可能範囲：4-30（秒） • 初期値：15（秒）
Forwarding BPDU	BPDU フォワーディング機能を「Enabled」（有効）または「Disabled」（無効）にします。
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。

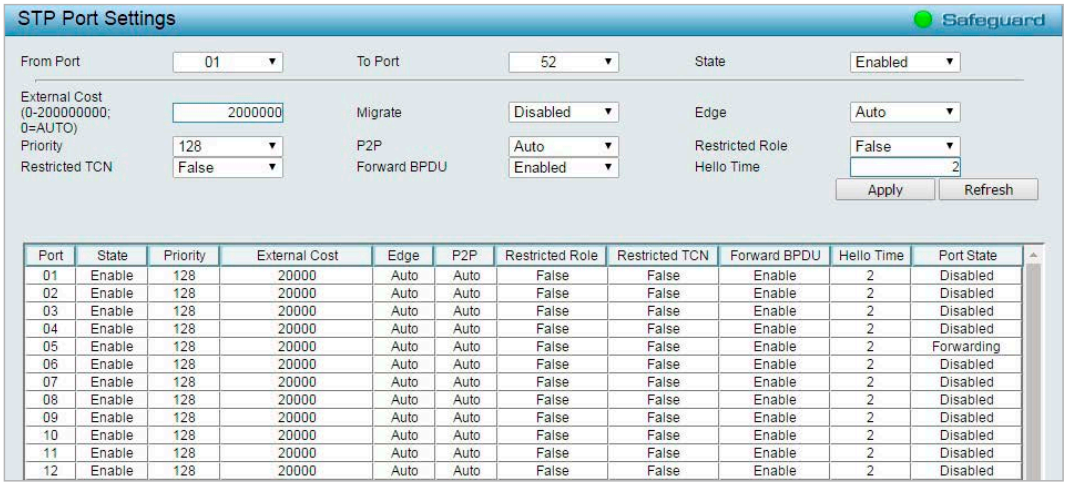


図 4-74　STP Port Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
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」
External Cost	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。 • 「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。 エッジポートではループは発生しませんが、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」- ポートをエッジポートとして指定しません。 • 「Auto」（初期値）- ポートのエッジポートステータスは自動的に決定されます。
Priority	各ポートのプライオリティを指定します。 • 設定可能範囲：0-240 • 初期値：128 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。

項目	説明
P2P	P2P ポートの設定を行います。 • 「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」- ポートを P2P ポートとして指定しません。 • 「Auto」（初期値）- 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。
Forward BPDU	BPDU フォワーディング機能を「Enabled」（有効）または「Disabled」（無効）にします。 補足 本機能は、ブリッジが 2 つのリージョンを接続し、それぞれで異なる STP 構成を必要とする場合に役に立ちます。BPDU フィルタリングは、STP がグローバルもしくはインタフェースで無効化されている時のみ動作します。 • 「Disabled」- 指定したポート上で BPDU フィルタリングが有効になります。 • 「Enabled」- STP が無効の場合、指定したポート上で PBDU フォワーディングが有効になります。
Hello Time	ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために送信します。本値は、BPDU パケットの送信間隔となります。 • 初期値：2（秒）

3. 「Apply」をクリックし、設定を有効にします。

MST Configuration Identification（MST の設定）

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

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

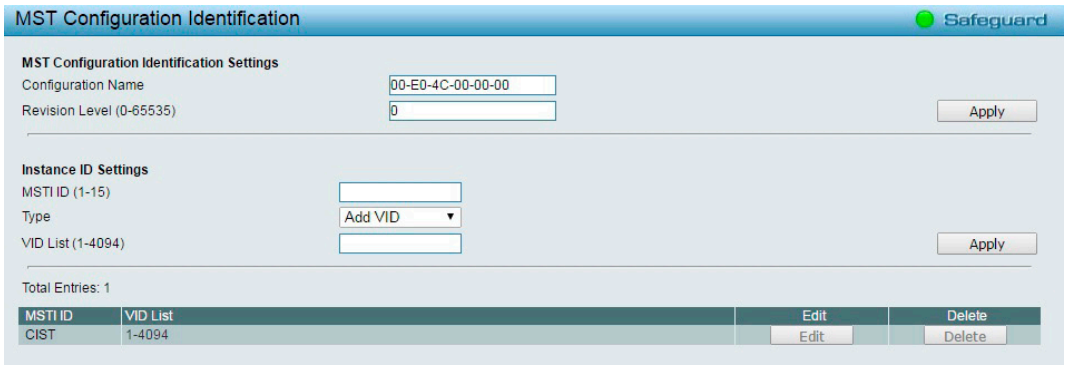


図 4-75　MST Configuration Identification 画面

2. 以下の項目を設定します。

項目	説明
MST Configuration Identification Settings	
Configuration Name	各 MSTI（Multiple Spanning Tree Instance）を識別するためにスイッチに名前を設定します。名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level	コンフィグレーション名と同様に、MSTP リージョンを識別するための値を設定します。 • 設定可能範囲：0-65535 • 初期値：0
Instance ID Settings	
MSTI ID	スイッチに新規の MSTI を設定します。「Edit」をクリックした場合、更新対象の MSTI ID が表示されます。 • 設定可能範囲：1-15
Type	MSTI 設定の変更内容を指定します。 •「Add VID」- MSTI ID に「VID List」で指定する VID を追加します。 •「Remove VID」- MSTI ID から「VID List」で指定する VID を削除します。
VID List	MSTI に紐づく VLAN ID を入力します。「Edit」をクリックした場合、更新対象の MSTI ID に紐づく VLAN ID が表示されます。 • 設定可能範囲：1-4094

3. 「Apply」をクリックし、設定を有効にします。

補足 「MST Configuration Identification Settings」の設定を行った場合は画面上部の「Apply」を、「Instance ID Settings」の設定を行った場合は画面下部の「Apply」をクリックしてください。

「Edit」をクリックすると、「Instance ID Settings」で該当の MSTI を編集できます。
エントリを削除するには、「Delete」をクリックします。

STP Instance Settings（STP インスタンス設定）

MSTI の設定内容を表示します。また、MSTP のプライオリティ値を変更することが可能です。

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

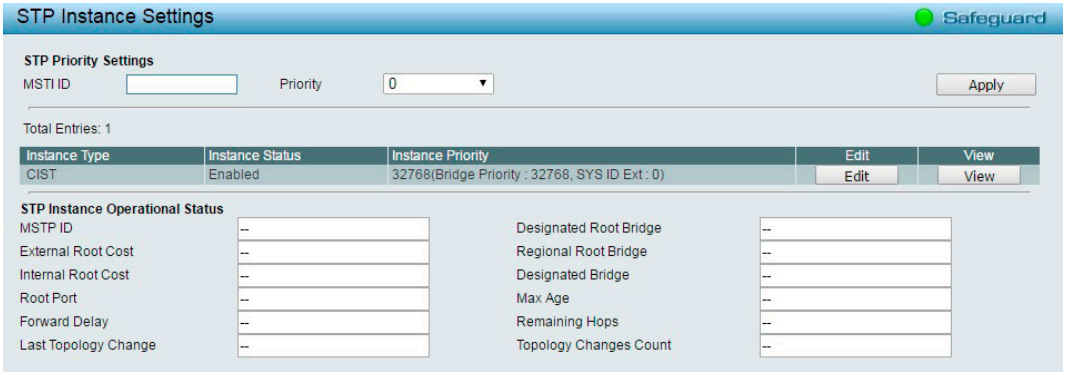


図 4-76　STP Instance Settings 画面

2. 以下の項目を設定します。

項目	説明
MST ID	更新対象の MSTI ID が表示されます。0 は CIST を意味し、デフォルトの MSTI となります。
Priority	新しいプライオリティ値を選択します。 • 設定可能範囲：0-61440

3. 「Apply」をクリックし、設定を有効にします。

エントリの編集
更新対象のエントリ欄で「Edit」をクリックします。

エントリの表示
対象のエントリ欄で「View」をクリックします。

MSTP Port Information（MSTP ポート情報）

本画面では現在の MSTP ポート情報が表示され、MSTI ID 単位でポート構成の更新を行います。ループが発生した場合に MSTP 機能はポートプライオリティを使用して、Forwarding 状態に遷移させるインタフェースを選択します。最初に転送されるインタフェースには、高いプライオリティを設定します。プライオリティ値が同じインスタンスの場合、最も小さい MAC アドレスを持つインタフェースを Forwarding 状態に移行し、他のインタフェースをブロックします。低いプライオリティ値ほど転送パケットに対して高いプライオリティを意味することにご注意ください。

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

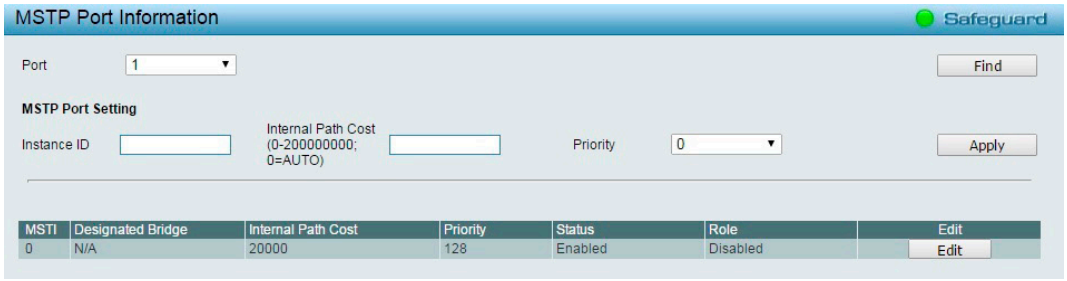


図 4-77　MSTP Port Information 画面

■ 指定ポートの MSTI インスタンス設定の編集

1. 特定の MSTI インスタンス設定を編集する場合は、編集する MSTI の「Edit」をクリックします。
2. 以下の項目を設定します。

項目	説明
Port	適用するポート番号を選択します。
Instance ID	更新対象の MSTI ID が表示されます。0 は CIST を意味し、デフォルトの MSTI となります。
Internal Path Cost	STP インスタンスでインタフェースを選択する場合、指定ポートにパケットを転送する相対的なコストを設定します。 • 設定可能範囲：0-200000000 　• 0 (Auto) 　　インタフェースに自動的で最適な最速のルートを設定します。 　　初期値はインタフェースのメディアスピードに基づいて設定されます。 　• 0-200000000 　　ループが発生した場合、指定した値の範囲で最短のルートを設定します。 　　コストが小さいほど高速で伝送されます。
Priority	ポートインタフェースのプライオリティを設定します。高いプライオリティほど、パケットの転送は優先されます。値が低いほどプライオリティは高くなります。 • 設定可能範囲：0-240

3. 「Apply」をクリックし、設定を有効にします。

特定のポートに関する MSTI 設定を表示するには、ポート番号を選択して「Find」をクリックします。

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、複数のポートを論理的に束ねることで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-1210-10/10MP: 最大 4 グループ
- DGS-1210-20/28/28MP: 最大 8 グループ
- DGS-1210-52 : 最大 16 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。

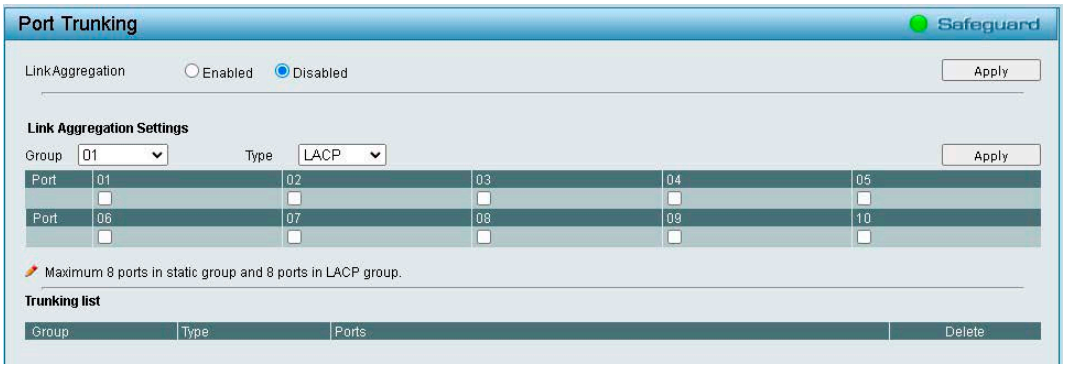


図 4-78　Port Trunking 画面

2. 以下の項目を設定します。

項目	説明
Link Aggregation	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。
Link Aggregation Settings	
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。 •「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行います。 •「LACP」（初期値）- 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　グループ化さ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。

補足　「Link Aggregation State」の有効化 / 無効化の設定を行った場合は画面上部の「Apply」を、「Link Aggregation Settings」の設定を行った場合は画面下部の「Apply」をクリックしてください。

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。

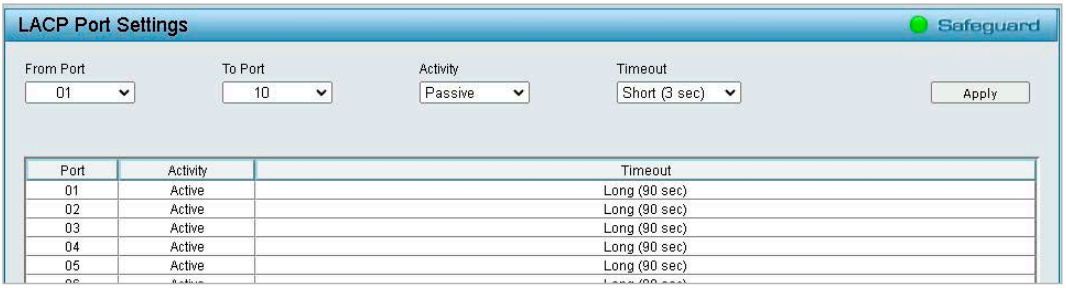


図 4-79　LACP Port Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
Activity	LACP ポートの動作を選択します。 • 「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」（初期値）- 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。 • 「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。

DGS-1210 シリーズは「IGMP v1/v2/v3 awareness」をサポートしています。
IGMP v1/v2/v3 awareness は、IGMPv3 スヌーピングについては限定的に対応しており、IGMPv3 プロトコルの認識が可能です。
なお、RFC の観点では、IGMPv3 のフルサポートとしてソースフィルタ機能が含まれますが、当該機能は本製品ではサポートされません。

IGMP Snooping の設定は、各 VLAN ごとに個別で行います。

注意 IGMP Snooping 機能において、IGMPv3 は一部の機能のみをサポートします。

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

図 4-80　IGMP Snooping Configuration 画面

2. 以下の項目を設定します。

項目	説明
IGMP Snooping	IGMP Snooping を「Enabled」（有効）または「Disabled」（無効）にします。「Report to all ports」にチェックを入れると、Join/Leave レポートをルータポートとホストポートを含むすべてのポートに転送します。チェックを外した場合、ルータポートのみに転送されます。 • 初期値：「Disabled」
Host Timeout	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。 • 設定可能範囲：130-153025（秒） • 初期値：260（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	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」および「1」には設定できません。 • 設定可能範囲：2-255（秒） • 初期値：2（秒）
Query Interval	General Query の送信間隔を設定します。 • 設定可能範囲：60-600（秒） • 初期値：125（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	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。 • 設定可能範囲：60-600（秒） • 初期値：125（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。

項目	説明
Last Member Query Interval	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。 • 設定可能範囲：1-25（秒） • 初期値：1（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。
Max Response Time	IGMP Response report を送信するまでの最大時間を設定します。 • 設定可能範囲：10-25（秒） • 初期値：10（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、以下の手順を実施します。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」で「Enable」を選択し「Apply」をクリックします。

2. 「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。

3. 以下の項目を設定します。

図 4-81　IGMP Snooping VLAN Settings 画面

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」

項目	説明
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。
Static Router Port	手動で VLAN の IGMP スヌーピングのルータ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。

4. 「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。
マルチキャストエントリテーブルを表示するには、「View」をクリックします。

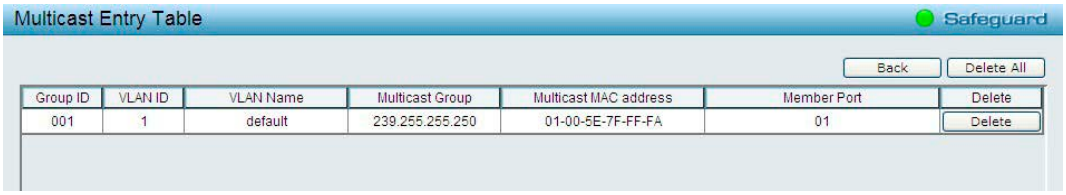


図 4-82　Multicast Entry Table 画面

特定のエントリを削除するには、「Delete」をクリックします。すべてのエントリを削除するには「Delete All」をクリックします。

注意 IGMP 有効化時に、マルチキャストグループメンバ以外のパケットをブロックする設定の場合、マルチキャストパケットはルータポートに送信されません。

注意 IGMP/MLD Snooping の機能において、Non-Querier、または Fast Leave が Disable の場合、IGMP Leave、MLD Done、または SQ の受信による M/C entries の削除を行いません。

注意 IGMP/MLD Snooping の機能において、Querier State が 有効の場合、バージョンは IGMPv2、MLDv1 です。MLDv1 の Done は認識しません。

注意 IGMP/MLD Snooping の機能において、Querier State が 有効の場合、Src IP は System の IP が使用されます。

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のみを行います。

注意　MLD Snooping は、Link Aggregation ポートでは動作しません。

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

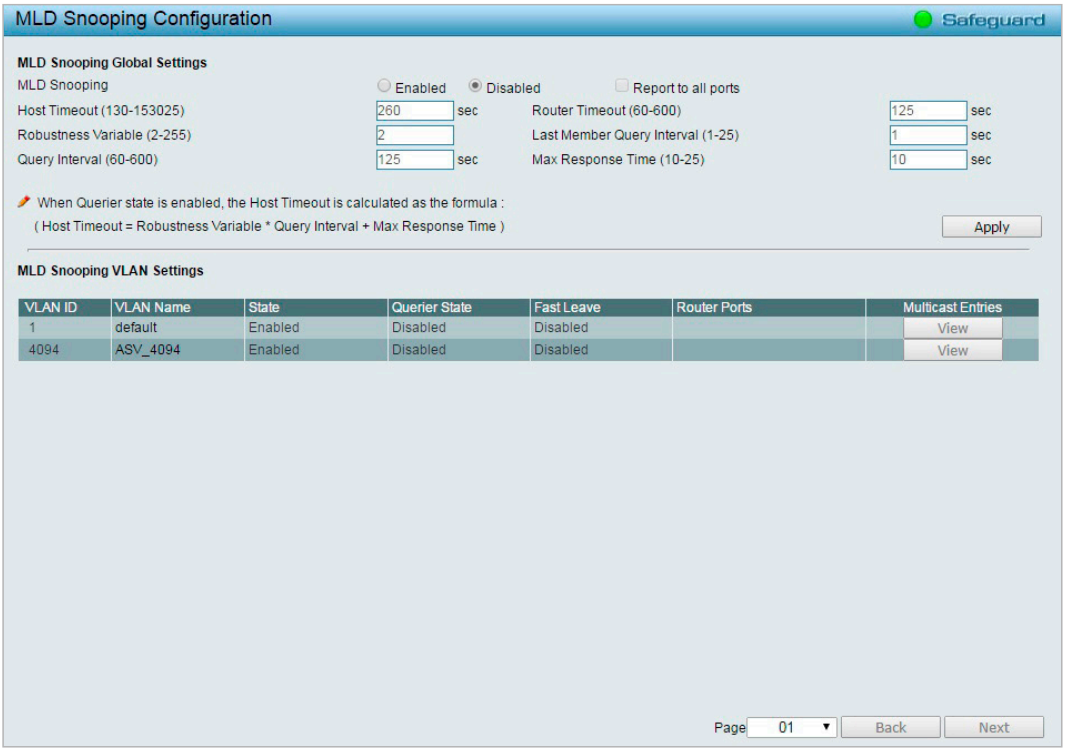


図 4-83　MLD Snooping Configuration 画面

2. 以下の項目を設定します。

項目	説明
MLD Snooping	MLD Snooping を「Enabled」（有効）または「Disabled」（無効）にします。「Report to all ports」にチェックを入れると、Join/Leave レポートをルータポートとホストポートを含むすべてのポートに転送します。チェックを外した場合、ルータポートのみに転送されます。 • 初期値：「Disabled」
Host Timeout	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以内に 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。 • 設定可能範囲：130-153025（秒） • 初期値：260（秒）
Router Timeout	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。 • 設定可能範囲：60-600（秒） • 初期値：125（秒）
Robustness Variable	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」および「1」には設定できません。 • 設定可能範囲：2-255（秒） • 初期値：2（秒）

項目	説明
Last Member Query Interval	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。 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。 • 設定可能範囲：1-25（秒） • 初期値：1（秒）
Query Interval	General Query の送信間隔を設定します。「Query Interval」の設定値により、MLD メッセージ量を調整することができます。値が大きいと MLD クエリの送信の減少につながります。 • 設定可能範囲：60-600（秒） • 初期値：125（秒）
Max Response Time	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。 • 設定可能範囲：10-25（秒） • 初期値：10（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。

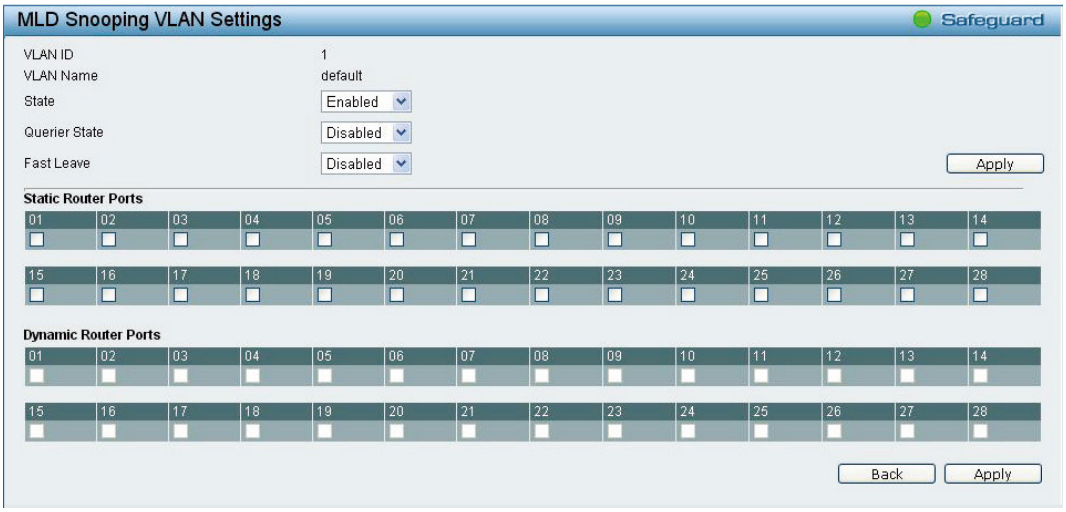


図 4-84　MLD Snooping VLAN Settings 画面

2. 以下の項目を設定します。

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。

注意　IGMP/MLD Snooping の機能において、Non-Querier、または Fast Leave が Disable の場合、IGMP Leave、MLD Done、または SQ の受信による M/C entries の削除を行いません。

注意　MLD Snooping の Querier Emulation、Fast Leave は、MLDv1 の Done を認識しません。

注意　IGMP/MLD Snooping の機能において、Querier State が 有効の場合、バージョンは IGMPv2、MLDv1 です。MLDv1 の Done は認識しません。

注意　IGMP/MLD Snooping の機能において、Querier State が 有効の場合、Src IP は System の IP が使用されます。

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。

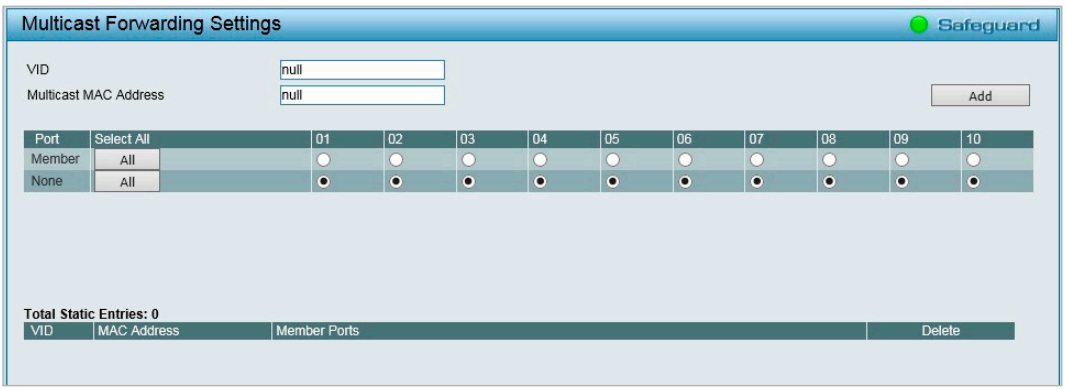


図 4-85　Multicast Forwarding Settings 画面

2. 以下の項目を設定します。

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。 • 「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」（初期値）- 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）

ポートインターフェイスベースでマルチキャストパケットをフィルタリングします。

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

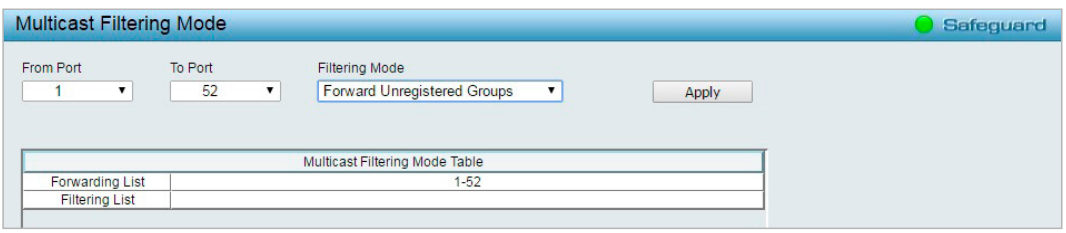


図 4-86　Multicast Filtering Mode 画面

2. 以下の項目を設定します。

項目	説明
From Port/To Port	設定対象のポート範囲を指定します。
Filtering Mode	フィルタリングモードを選択します。 • 「Forward Unregistered Groups」- 登録されたマルチキャストパケットはフォワーディングテーブルに基づいて転送され、登録されていないマルチキャストパケットは VLAN ドメインにフラッドします。 • 「Filter Unregistered Groups」- 登録されたマルチキャストパケットはフォワーディングテーブルに基づき転送され、登録されていないマルチキャストパケットはフィルタされます。

3. 「Apply」をクリックし、設定を有効にします。

注意　IGMP 有効化時に、マルチキャストグループメンバ以外のパケットをブロックする設定の場合、マルチキャストパケットはルータポートに送信されません。

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。

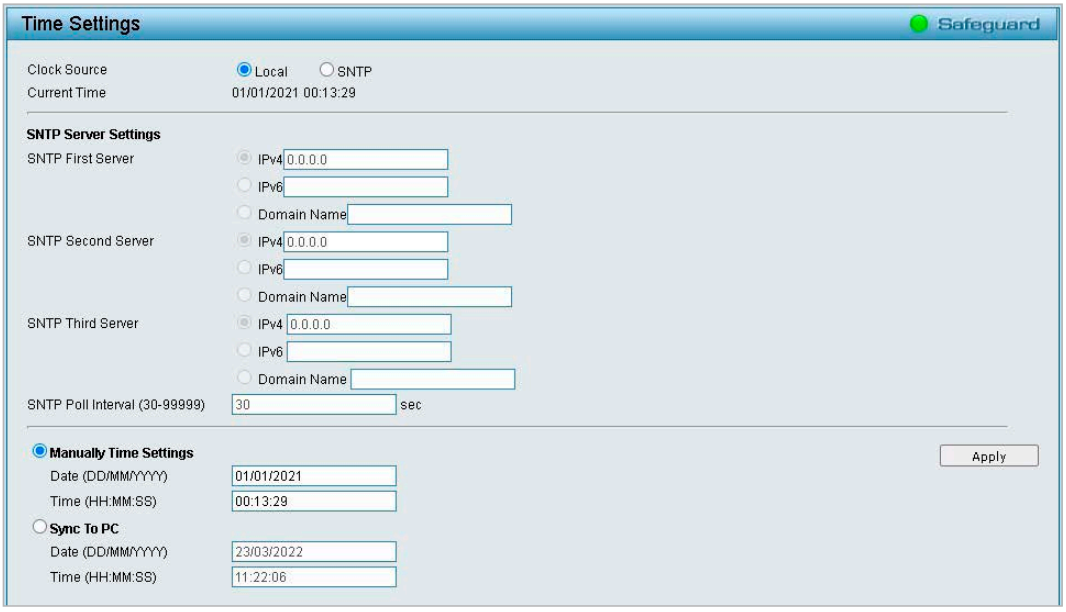


図 4-87　Time Settings 画面

2. 以下の項目を設定します。

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。 • 「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」（初期値）- 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」「IPv6」「Domain Name」のいずれかを選択し、システム時刻を受け取るプライマリ SNTP サーバの IP アドレスまたはドメイン名を設定します。
SNTP Second Server	「IPv4」「IPv6」「Domain Name」のいずれかを選択し、システム時刻を受け取るセカンダリ SNTP サーバの IP アドレスまたはドメイン名を設定します。
SNTP Third Server	「IPv4」「IPv6」「Domain Name」のいずれかを選択し、システム時刻を受け取るターシャリ SNTP サーバの IP アドレスまたはドメイン名を設定します。
SNTP Poll Interval In Seconds	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。 • 設定可能範囲：30-99999（秒） • 初期値 : 30（秒）

項目	説明
Manually Time Settings / Sync To PC	
• 「Manually Time Settings」- 手動で時刻の設定を行います。 • 「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。

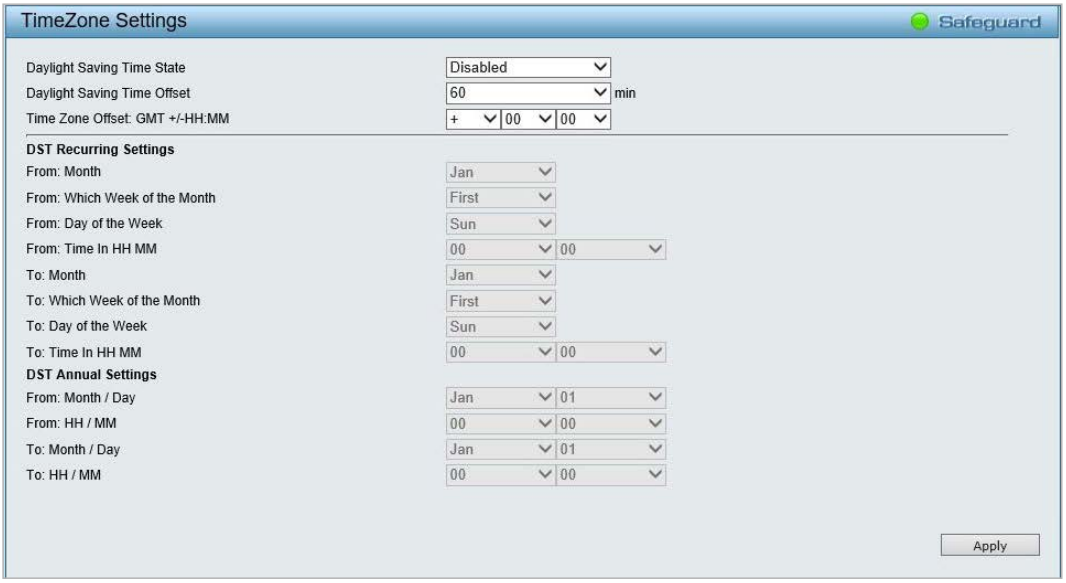


図 4-88　TimeZone Settings 画面

2. 以下の項目を設定します。

項目	説明
Daylight Saving Time State	デバイスに設定するサマータイムの種類を設定します。 • 「Disabled」- サマータイムを無効にします。（初期値） • 「Annual」- サマータイムを日付指定で有効にします。このオプションでは、指定年月日にサマータイムが開始 / 終了します。 • 「Recurring Setting」- サマータイムを周期的に有効にします。このオプションでは、指定月の指定曜日にサマータイムが開始 / 終了します。
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。 • 選択肢：30、60、90、120（分） • 初期値：60（分）
Time Zone Offset: 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。
DST Recurring Settings	
From: Month	サマータイムが開始する月を指定します。
From: Which Week of the Month	月の第何週からサマータイムが始まるかを設定します。 • 「First」- 月の最初の週に設定します。 • 「Second」- 月の 2 番目の週に設定します。 • 「Third」- 月の 3 番目の週に設定します。 • 「Fourth」- 月の 4 番目の週に設定します。

項目	説明
From: Day of the Week	サマータイムが開始する曜日を指定します。
From: Time In HH MM	サマータイムが開始する時間を指定します。
To: Month	サマータイムが終了する月を指定します。
To: Which Week of the Month	月の第何週でサマータイムが終わるかを設定します。 • 「First」- 月の最初の週に設定します。 • 「Second」- 月の 2 番目の週に設定します。 • 「Third」- 月の 3 番目の週に設定します。 • 「Fourth」- 月の 4 番目の週に設定します。
To: Day of the Week	サマータイムが終了する曜日を指定します。
To: Time In HH MM	サマータイムが終了する時間を指定します。
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。

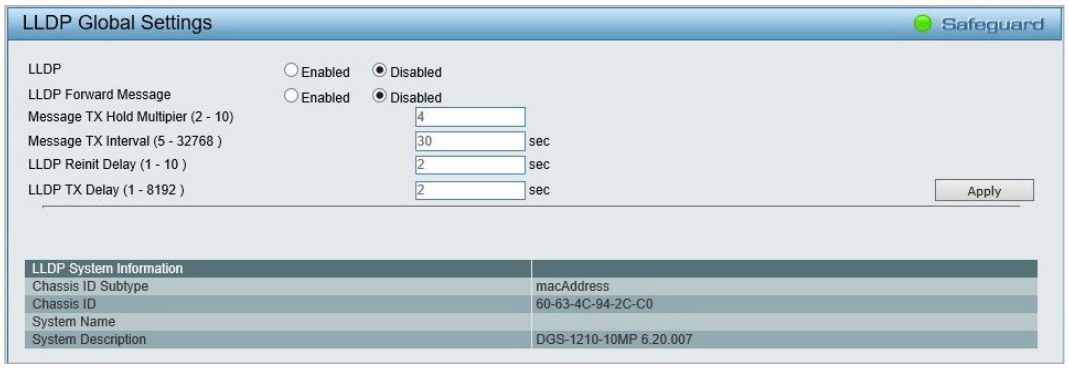


図 4-89　LLDP Global Settings 画面

2. 以下の項目を設定します。

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、処理を開始します。LLDP パケット通知では、スイッチはポートを通してネイバに LLDP の情報を展開します。LLDP パケットの受信では、スイッチは、ネイバテーブルのネイバから通知された LLDP パケットの情報を学習します。 • 初期値：「Disabled」
LLDP Forward Message	LLDP パケットの転送を許可します。 • 初期値：「Disabled」
Message TX Hold Multiplier	LLDPDU で使用される TTL 値を決定するために使用される乗数を指定します。 • 設定可能範囲：2-10 • 初期値：4
Message TX Interval	LLDP で情報を送信する間隔を設定します。 • 設定可能範囲：5-32768（秒） • 初期値：30（秒）
LLDP Reinit Delay	LLDP を初期化するときの遅延時間を指定します。 • 設定可能範囲：1-10（秒） • 初期値：2（秒）
LLDP TX Delay	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。 • 設定可能範囲：1-8192（秒） • 初期値：2（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-1210-10MP/28MP 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機器の 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。PoE エンドポイントの自動電源管理について、現在は DGS-1210-10MP/28MP のみが 802.3at ポート（10MP: 1 ～ 8 ポート /28MP: 1 ～ 24 ポート) で対応しています。

本画面では、802.3at ポートの「Power PSE TLV (Type-length-value)」ステートの設定を行います。「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 / 無効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。

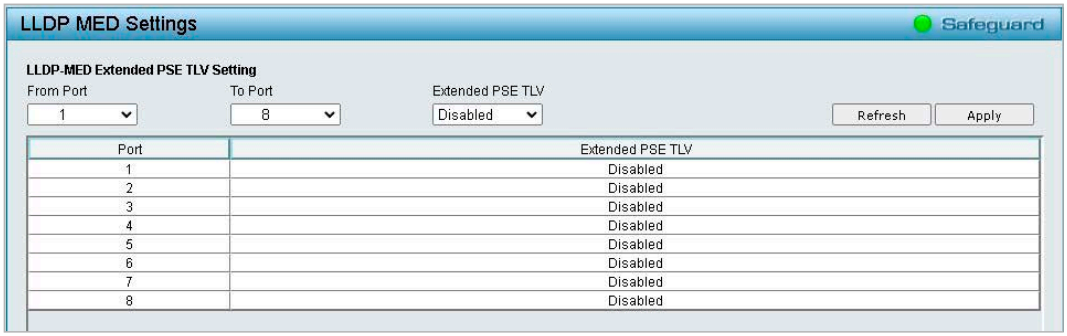


図 4-90　LLDP MED Settings 画面

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、表示を最新の状態に更新できます。

Basic LLDP Port Settings（ベーシック LLDP ポート設定）

LLDP ポートの設定、表示を行います。

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

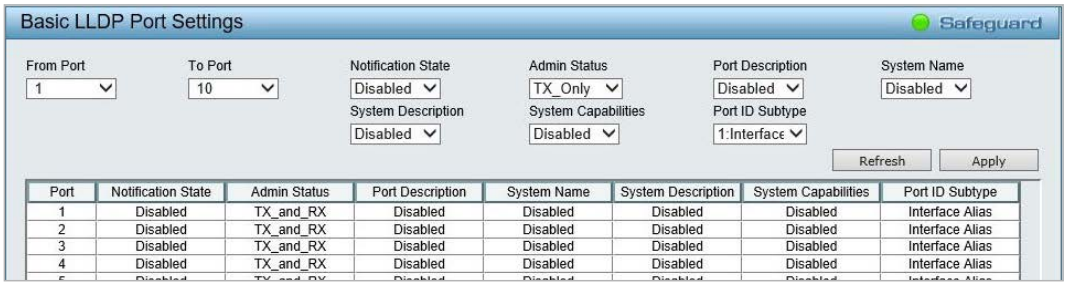


図 4-91　Basic LLDP Port Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
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。 ・「Enabled」- ポートの LLDP 通知を有効にします。 ・「Disabled」（初期値）- 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。 • 「TX_Only」（初期値）- LLDP パケットの送信のみを行います。 • 「RX_Only」- LLDP パケットの受信のみを行います。 • 「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」
Port ID Subtype	ポート ID サブタイプを指定します。 • 選択肢：「1: Interface alias」「3: MAC address」「5: Interface name」「7: Locally assigned」

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、表示を最新の状態に更新できます。

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。

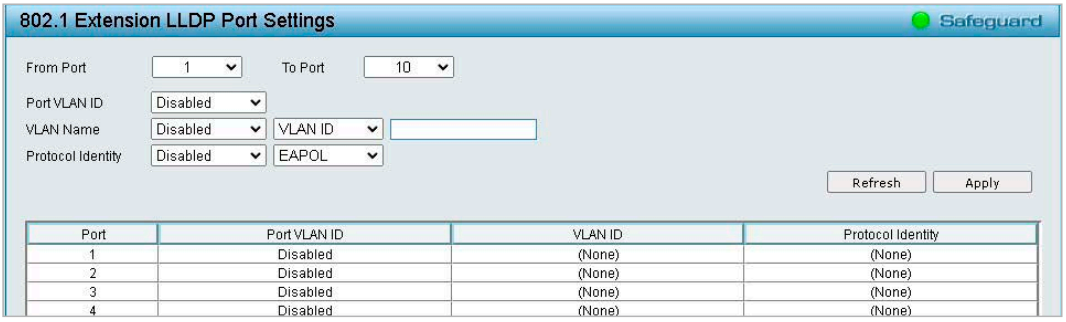


図 4-92　802.1 Extension LLDP Port Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
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」「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、表示を最新の状態に更新できます。

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。

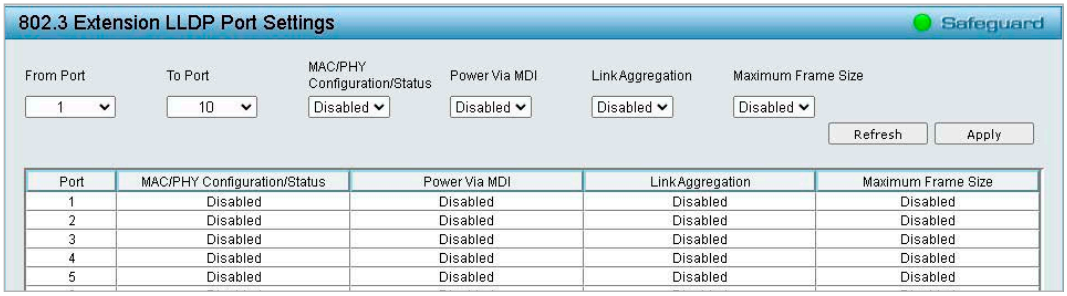


図 4-93　802.3 Extension LLDP Port Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
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。

注意　「Power Via MDI」を有効に設定しても、Power Class 及び PSE Allocated power Value は設定されません。

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。

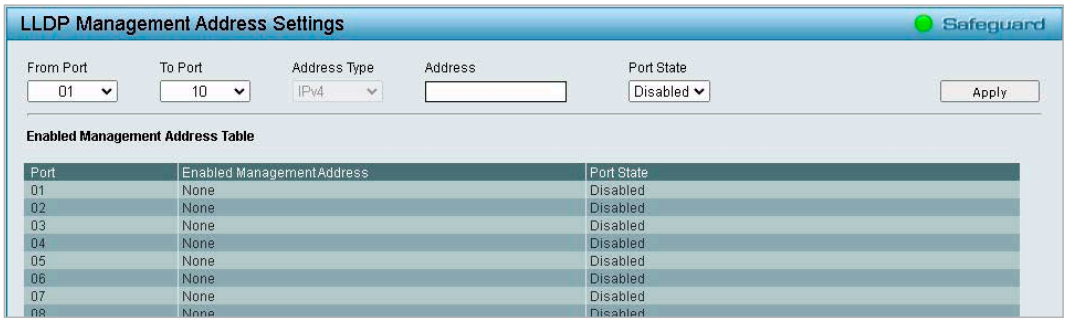


図 4-94　LLDP Management Address Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
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 4-95　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。

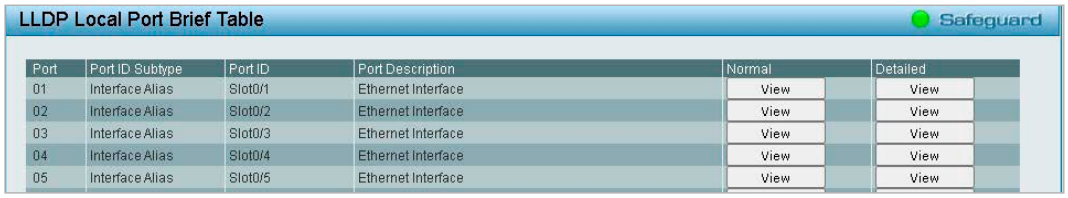


図 4-96　LLDP Local Port Brief Table 画面

2. 以下の内容が表示されます。

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。

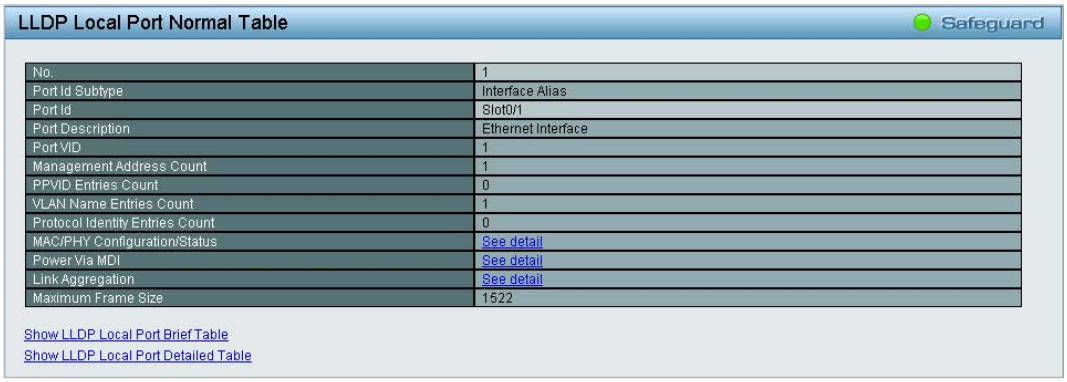


図 4-97　LLDP Local Port Normal Table 画面

■ 「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。

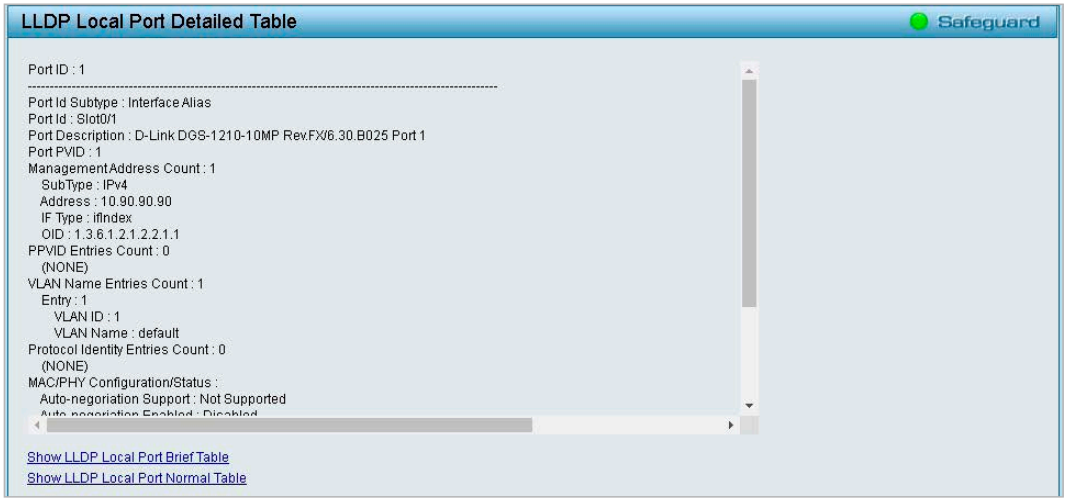


図 4-98　LLDP Local Port Detailed Table 画面

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。

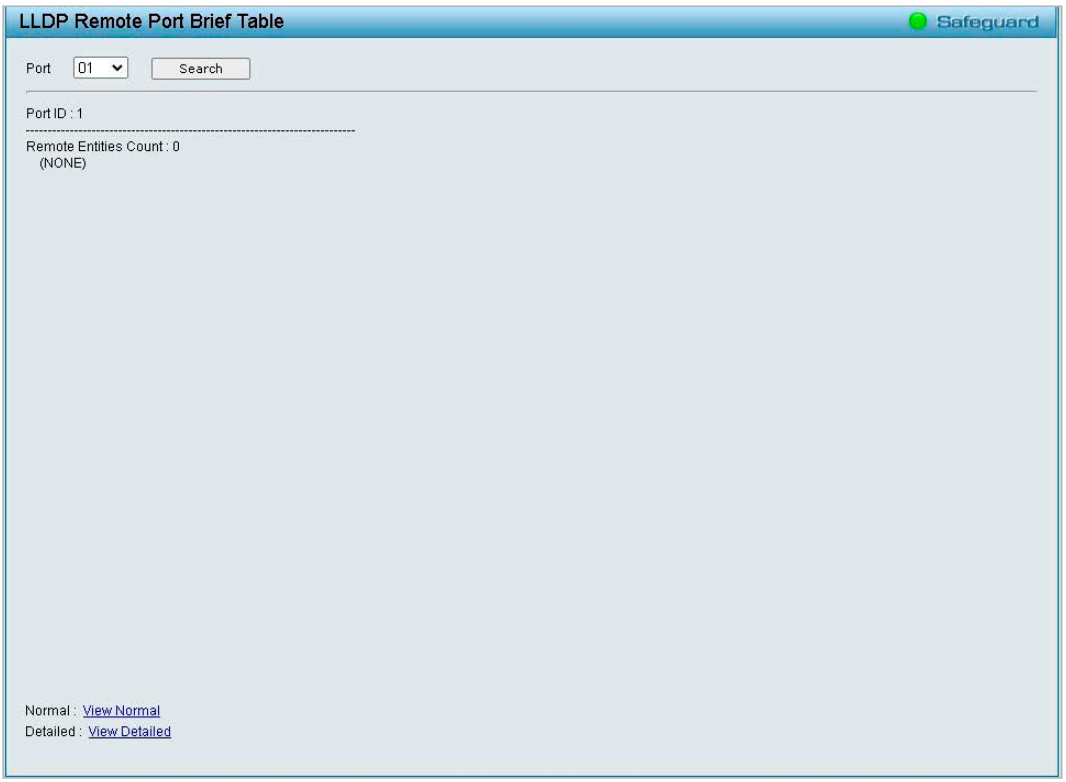


図 4-99　LLDP Remote Port Brief Table 画面

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。

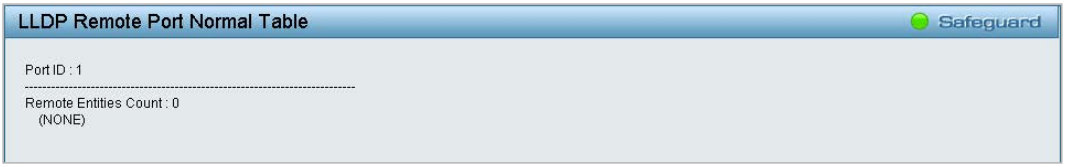


図 4-100　LLDP Remote Port Normal Table 画面

■「View Detailed」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。

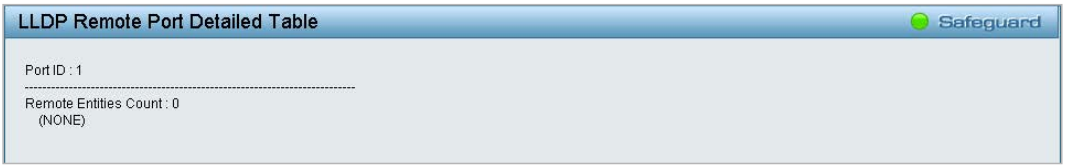


図 4-101　LLDP Remote Port Detailed Table 画面

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。

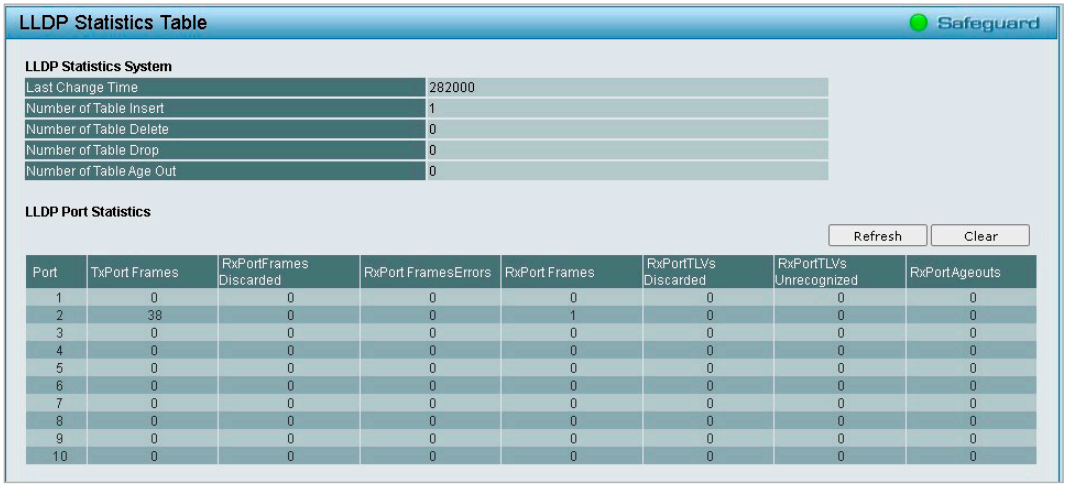


図 4-102　LLDP Statistics Table 画面

2. 以下の内容が表示されます。

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。

L3 Functions（L3 機能）

L3 機能の設定項目

IP Interface（IP インタフェース設定）

スイッチの IP インタフェース管理の設定を行います。

1. 「L3 Functions」>「IP Interface」の順にメニューをクリックします。

図 4-103　IP Interface Settings 画面

2. 以下の項目を設定します。

項目	説明
Interface Name	IP インタフェース名を指定します。
VLAN Name	IP インタフェースの VLAN 名を指定します。
IPv4 Address	インタフェースの IPv4 アドレスを指定します。
Netmask	IP アドレスのネットマスクを選択します。
Interface Admin State	IP インタフェースの管理を「Enabled」（有効）または「Disabled」（無効）にします。

3. 「Add」をクリックし、設定を有効にします。

設定を削除する場合は、「Delete」をクリックします。
設定を変更するには「Edit」をクリックし、変更後に「Apply」をクリックします。

注意　複数の IPv4 Interface を設定した際に、DHCP Relay は適切に機能しません。

注意　IPv4 Interface 設定において、/3 より短い サブネットマスクは指定できません。

■ IPv6 インタフェース設定

1. IPv6 インタフェースを設定するには「IPv6」をクリックします。以下の画面が表示されます。

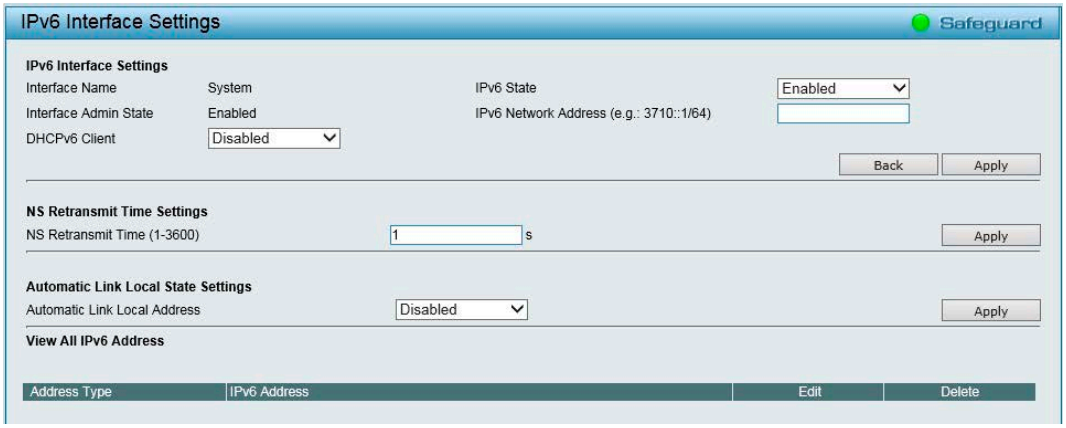


図 4-104　IPv6 Interface Settings 画面

2. 以下の項目を設定します。

項目	説明
IPv6 Interface Settings	
Interface Name	IPv6 IP インタ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。
Interface Admin State	IP インタフェースの管理を「Enabled」（有効）または「Disabled」（無効）にします。
DHCPv6 Client	DHCPv6 クライアントを「Enabled」（有効）または「Disabled」（無効）にします。
IPv6 Network Address	IPv6 ネットワークアドレスを指定します。
NS Retransmit Time Settings	
NS Retransmit Time	Neighbor Solicitation の再送信タイマ（秒）を入力します。 • 設定可能範囲：1-3600（秒） • 初期値：1（秒）
Automatic Link Local State Settings	
Automatic Link Local Address	リンクローカルアドレスの自動設定を「Enabled」（有効）または「Disabled」（無効）にします。

3. セクション毎に「Apply」をクリックし、設定を有効にします。

設定を削除する場合は、「Delete」をクリックします。
設定を変更するには「Edit」をクリックし、変更後に「Apply」をクリックします。
「Back」をクリックすると「IP Interface Settings」画面に戻ります。

注意　RA に関する機能実装がないため、複数 IPv6 Interface を設定した際に、DHCPv6 Relay が適切に機能しません。

IPv6 Neighbor Settings（IPv6 Neighbor 設定）

IPv6 Neighbor の設定を行います。現在の IPv6 Neighbor 設定が画面下部のテーブルに表示されます。

1. 「L3 Functions」>「IPv6 Neighbor Settings」の順にメニューをクリックします。

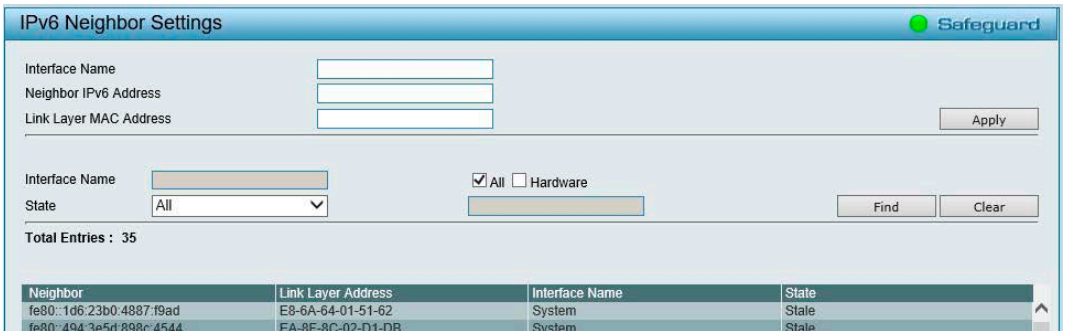


図 4-105　IPv6 Neighbor Settings 画面

2. 以下の項目を設定します。

項目	説明
Interface Name	Neighbor デバイスのインタフェース名を入力します。
Neighbor IPv6 Address	Neighbor デバイスの 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。

■ IPv6 Neighbor の新規登録

1. 「Interface Name」「Neighbor IPv6 Address」および「Link Layer MAC Address」を入力します。
2. 「Apply」をクリックします。

■ エントリの検索

1. 画面中央の「State」で「All」、「Address」、「Static」または「Dynamic」を選択します。
2. 「Find」クリックします。

画面中央の「Interface Name」の横の「All」にチェックを入れると、全てのインタフェースについて検索します。
特定のインタフェースを指定する場合は、「All」のチェックを外します。
「Hardware」にチェックを入れると、ハードウェアテーブルに書き込まれた全ての Neighbor キャッシュエントリが表示されます。

■ エントリの削除

1. エントリを検索して、削除対象のエントリを表示します。
2. 「Clear」をクリックします。

IPv4 Static Route（IPv4 スタティックルート設定）

本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。
IPv4 には最大 124 個のスタティックルートエントリを作成することできます。

スタティックルートが設定されると、スイッチは設定されたネクストホップルータに対し ARP リクエストパケットを送信します。ネクストホップから ARP 応答を受け取ると、ルートが有効になります。ただし、既に ARP エントリが存在する場合、ARP 要求は送信されません。

また、スイッチはフローティングスタティックルートをサポートしています。これは、同じネットワークにある異なるネクストホップデバイスに代替のスタティックルートを作成できるものです。この セカンダリネクストホップデバイスのルートは、プライマリスタティックルートがダウンした場合のバックアップ用スタティックルートとなります。プライマリスタティックルートが失われた場合、バックアップルートがリンクアップし、アクティブな状態になります。IP アドレスサブネットマスクとゲートウェイを使用してフォワーディングテーブルにエントリを作成することが可能です。

IPv4 スタティックルート画面では、IPv4 ルート設定を有効化し、構成を行うことができます。

1. 「L3 Functions」>「IPv4 Static Route」の順にメニューをクリックします。

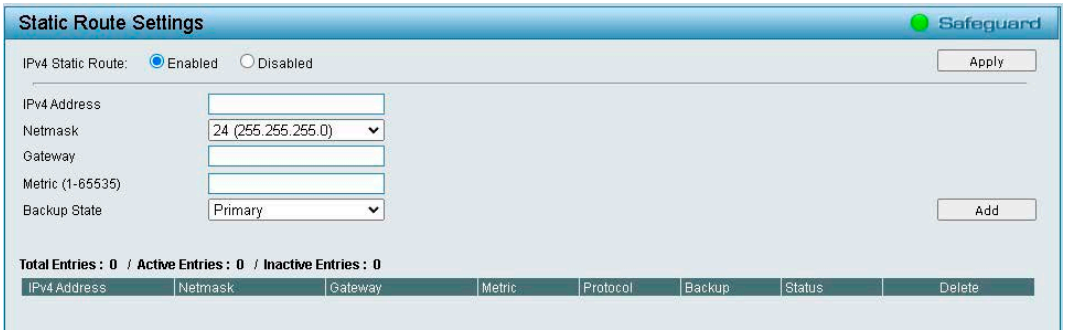


図 4-106　Static Route Settings 画面

2. 以下の項目を設定します。

■ IPv4 スタティックルートの有効化 / 無効化

1. 「IPv4 Static Route」で IPv4 スタティックルート機能を「Enabled」（有効）または「Disabled」（無効）にします。（初期値：「Disabled」）
2. 「Apply」をクリックし、設定を保存します。

■ ルーティングエントリの追加

1. 以下の項目を設定します。

項目	説明
IPv4 Address	スタティックルートに割り当てる IPv4 アドレスを指定します。
Netmask	IPv4 アドレスに対応するサブネットマスクを選択します。
Gateway	IPv4 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 IPv4 アドレスを指定します。
Metric	IP インタフェースのメトリック値を指定します。 • 設定可能範囲：1-65535
Backup State	Primary または Backup を選択します。プライマリルートに障害が発生した場合、バックアップルートが使用されます。プライマリルートとバックアップルートには同じゲートウェイを指定できません。

2. 「Add」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。

注意　Static Route Settings の機能ついて、Longest Match による経路選択は設定出来ません。

注意　同一経路に対し、「Metric」より「Backup State」の設定が優先されます。

IPv4 Routing Table Finder（IPv4 ルーティングテーブル検索）

現在の IPv4 ルーティングテーブルを表示します。

1. 「L3 Functions」>「IPv4 Routing Table Finder」の順にメニューをクリックします。

図 4-107　Routing Table Finder 画面

2. 「Network Address」に IPv4 アドレスを入力し、「Search」をクリックします。

IPv6 Static Route（IPv6 スタティックルート設定）

IPv6 スタティックルートを設定します。

1. 「L3 Functions」>「IPv6 Static Route」の順にメニューをクリックします。

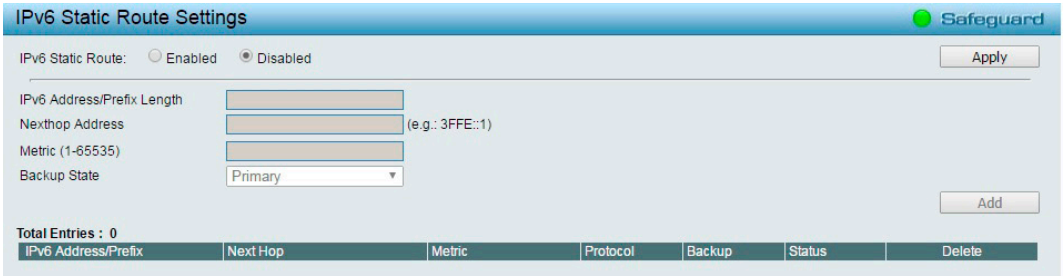


図 4-108　IPv6 Static Route Settings 画面

2. 「IPv6 Static Route」で IPv6 スタティックルート機能を「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、設定を保存します。

■ ルーティングエントリの追加

1. 以下の項目を設定します。

項目	説明
IPv6 Address/ Prefix Length	スタティックルートに割り当てる IPv6 アドレスを指定します。
Nexthop Address	IPv6 形式におけるネクストホップゲートウェイアドレスに対応する IPv6 アドレスを指定します。
Metric	IPv6 インタフェースのメトリック値を指定します。スイッチと上記 IP アドレス間のルータの数を表します。 • 設定可能範囲：1-65535
Backup State	プライマリルートに障害が発生した場合、バックアップルートが使用されます。プライマリルートとバックアップルートには同じゲートウェイを指定できません。

2. 「Add」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 Routing Table Finder（IPv6 ルーティングテーブル検索）

現在の IPv6 ルーティングテーブルを表示します。

1. 「L3 Functions」>「IPv6 Routing Table Finder」の順にメニューをクリックします。

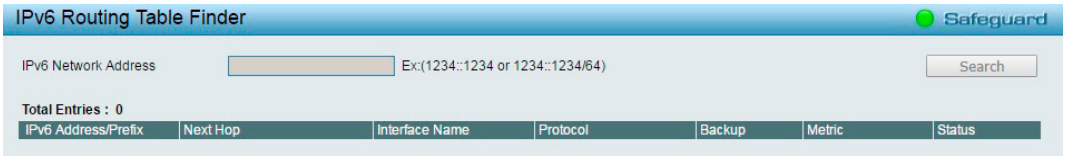


図 4-109　IPv6 Routing Table Finder 画面

2. 「IPv6 Network Address」に IPv6 アドレスを入力し、「Search」をクリックします。

ARP（ARP 設定）

ARP Table Global Settings（ARP テーブルグローバル設定）

現在の ARP エントリを表示します。また、本画面では、ARP のグローバル設定を更新することができます。スタティックエントリは ARP テーブル内で定義することができます。スタティックエントリが定義されると、永続的なエントリが登録され IP アドレスから MAC アドレスへの変換に使用されます。

1. 「L3 Functions」>「ARP」>「ARP Table Global Settings」の順にメニューをクリックします。

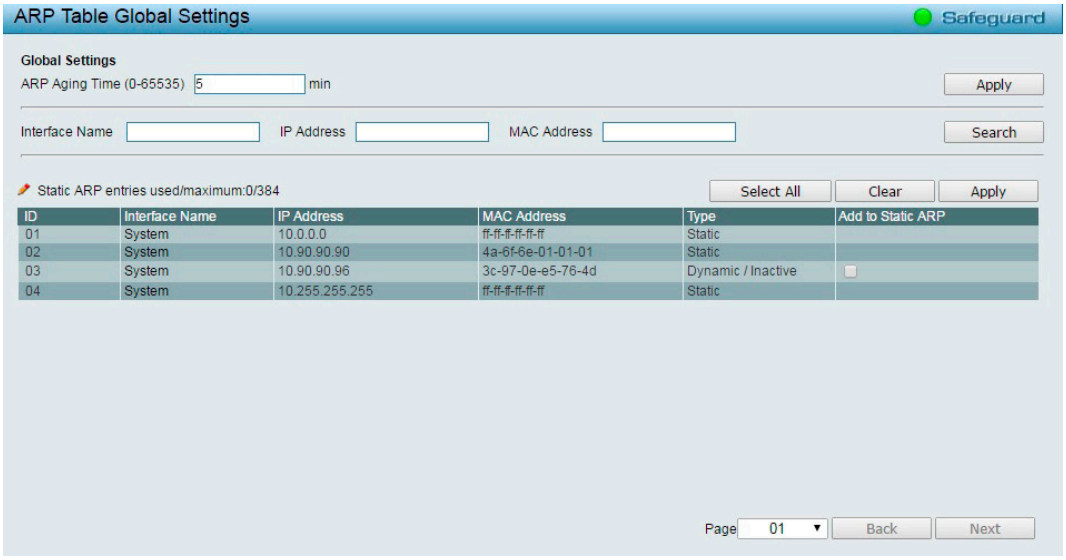


図 4-110　ARP Table Global Settings 画面

2. 以下の項目を設定します。

■ ARP エージングタイム設定

1. 「ARP Aging Time (0-65535)」でエージングタイムの時間（分）を設定します。（初期値：5 分）
2. 「Apply」をクリックし、設定を保存します。

■ ARP エントリ検索

1. 検索条件として「Interface Name」「IP Address」「MAC Address」を入力します。
2. 「Search」をクリックし、検索結果を表示します。

■ スタティック ARP への追加

1. 設定対象のエントリにおいて、「Add to Static ARP」のチェックボックスにチェックを入れます。
   Select All」をクリックすると、適用可能な全てのエントリが選択されます。選択を解除するには「Clear」をクリックします。
2. 「Apply」をクリックします。

注意　Gratuitous ARP による ARP テーブルの更新に対応していません。（ARP Request/Reply いずれも非対応）

Static ARP Settings（スタティック ARP 設定）

アドレス解決プロトコルは、IP アドレスを物理アドレスに変換する TCP/IP プロトコルです。本画面では、ARP の情報を表示・定義・更新・削除することができます。スタティックエントリは ARP テーブル内で定義することができます。スタティックエントリが定義されると、永続的なエントリが登録され IP アドレスと MAC アドレスの変換に使用されます。

1. 「L3 Functions」>「ARP」>「Static ARP Settings」の順にメニューをクリックします。

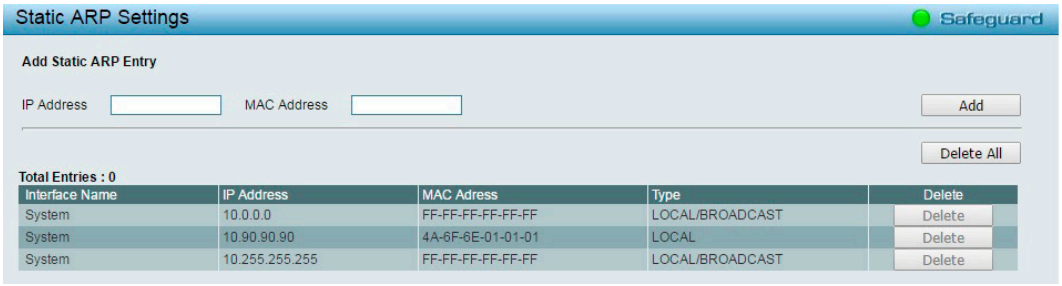


図 4-111　Static ARP Settings 画面

2. 以下の項目を設定します。

項目	説明
IP Address	IP アドレスを入力します。
MAC Address	MAC アドレスを入力します。

3. 「Add」をクリックし、Static ARP エントリを追加します。

■ スタティック ARP エントリの削除

1. 特定のエントリを削除するには、エントリ横の「Delete」をクリックします
「Delete All」をクリックすると、全てのスタティック ARP エントリが削除されます。

注意　Static ARP エントリの最大数は 384 です。

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。

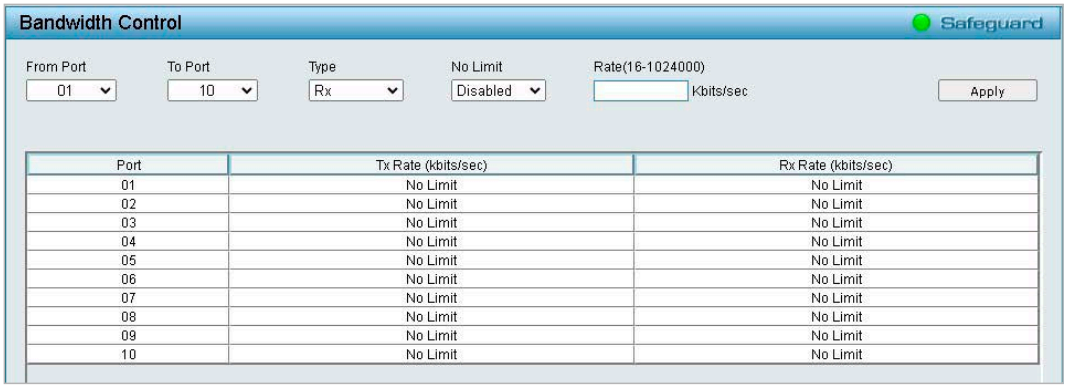


図 4-112　Bandwidth Control 画面

2. 以下の項目を設定します。

項目	説明
From Port/ To Port	設定対象のポート範囲を指定します。
Type	帯域上限を「受信」「送信」「送受信の両方」のいずれかに適用します。 • 「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。 • 「Enabled」- ポートで帯域制限を行いません。 • 「Disabled」（初期値）- ポートで帯域制限を行います。
Rate	指定したポートでのデータ速度の上限値を設定します。 • 設定可能範囲：16-1024000（Kbit/ 秒）

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的に処理されます。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 Priority Settings 画面

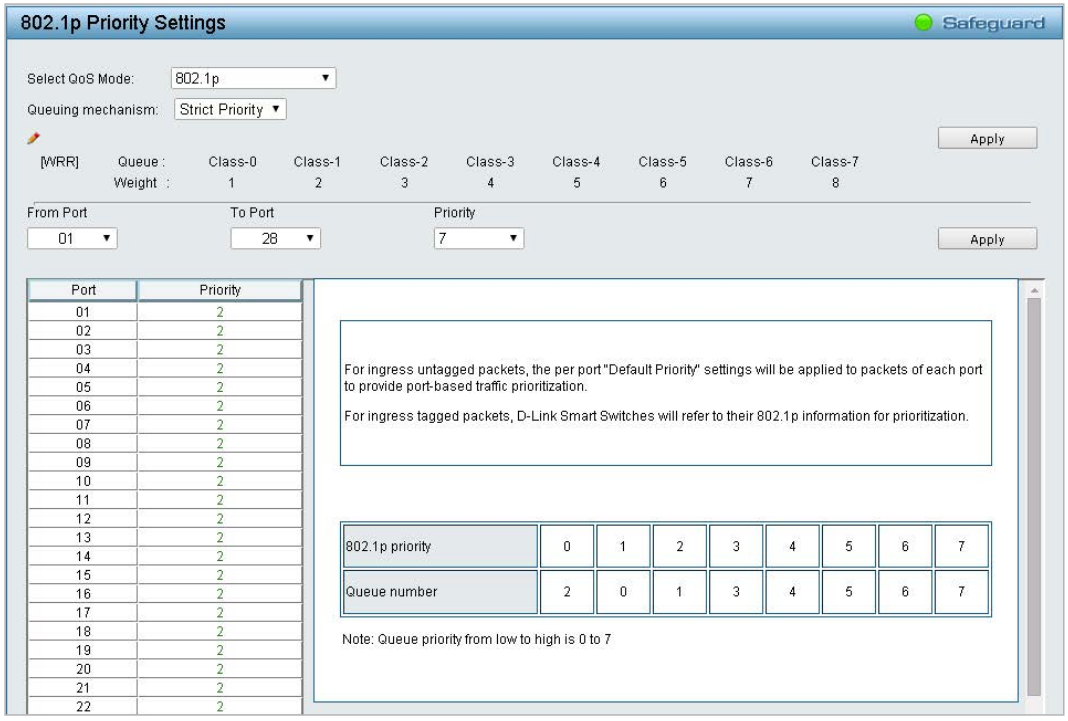


図 4-113　802.1p Priority Settings 画面

■ DSCP Priority Settings 画面

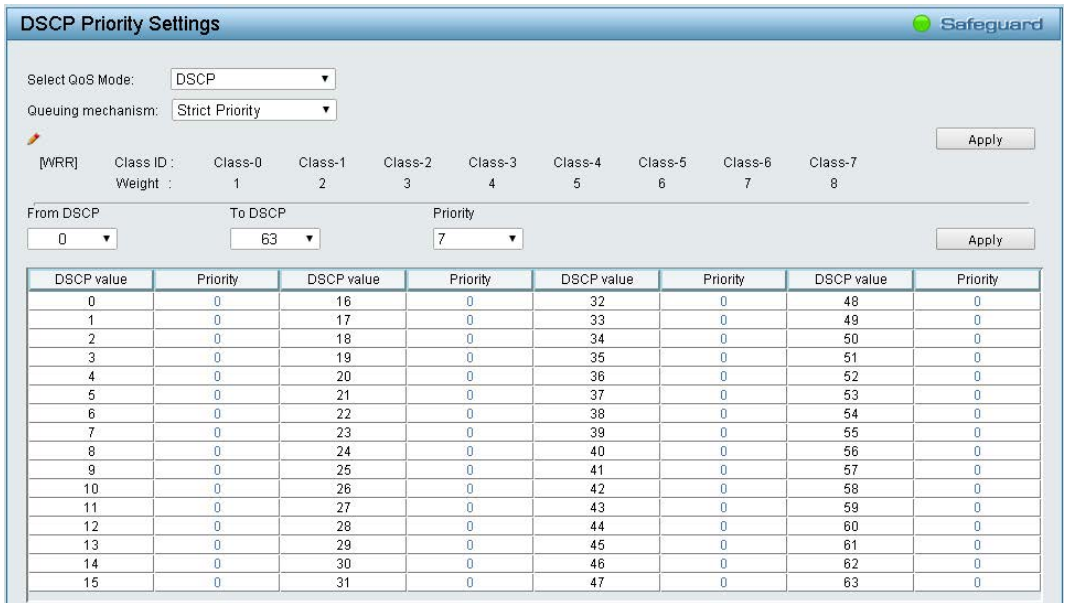


図 4-114　DSCP Priority Settings 画面

■ ToS Priority Settings 画面

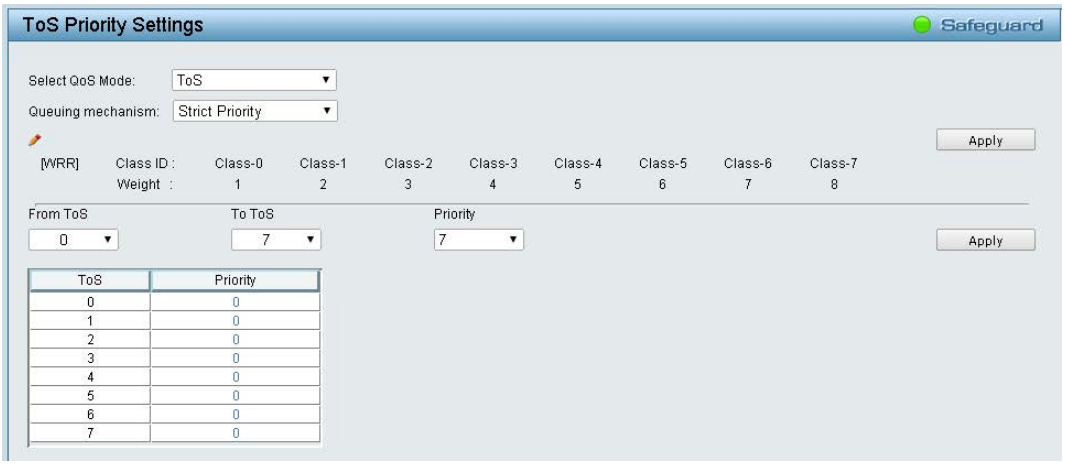


図 4-115　ToS Priority Settings 画面

3. 以下の項目を設定します。

項目	説明
Select QoS Mode	QoS モードを選択します。 • 「802.1p」（初期値）- 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。 • 「Strict Priority」（初期値）- 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、続くキューは 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 Priority 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 Priority 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 Priority Setting 画面でのみ表示されます。
Priority	ポートに割り当てる優先度を選択します。0 が最小の優先値となり、7 が最大の優先値となります。 • 選択肢：0-7 • 初期値：7

4. 「Apply」をクリックし、設定を有効にします。

補足　「Select QoS Mode」および「Queuing mechanism」の設定を行った場合は画面上部の「Apply」を、それ以外の変更を行った場合は画面下部の「Apply」をクリックしてください。

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。

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

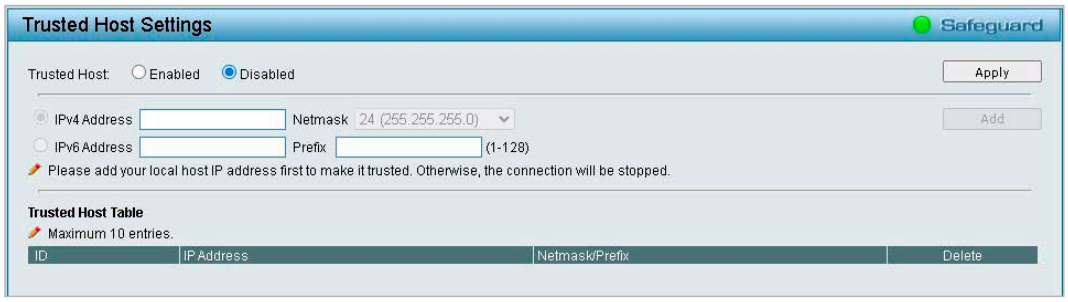


図 4-116　Trusted Host Settings 画面

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。

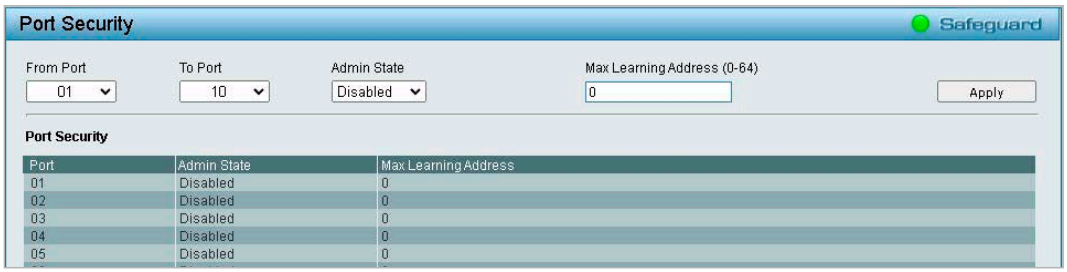


図 4-117　Port Security 画面

2. 以下の項目を設定します。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Admin State	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	ポートが学習できる最大の MAC アドレス数を指定します。 • 設定可能範囲：0-64 • 初期値：0

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）

レイヤ 2 メカニズムにより、トラフィックフローをセグメント内に制限します。ただし、このセグメントは VLAN グループを越えることはできません。

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

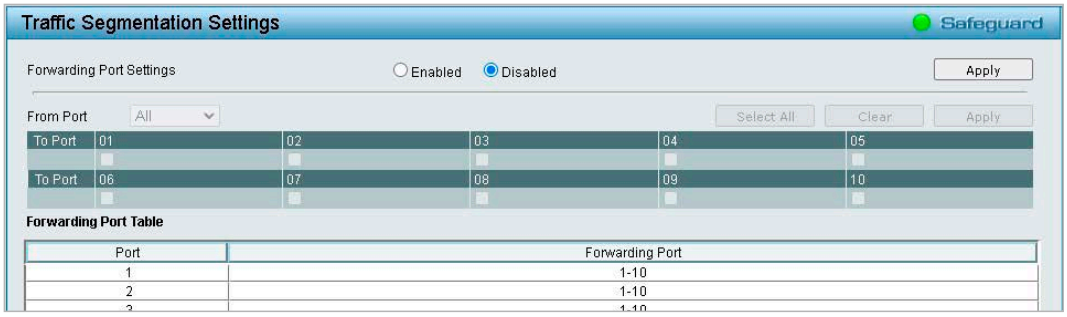


図 4-118　Traffic Segmentation Settings 画面

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。

注意　Asymmetric VLAN、Traffic Segmentation は Unknown ユニキャストの フィルタはできません。

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。

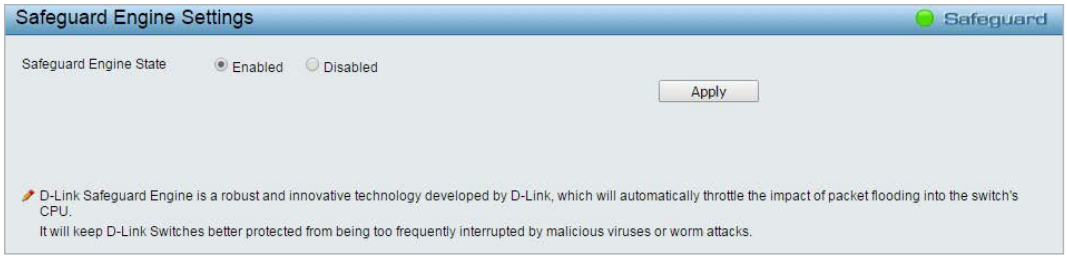


図 4-119　Safeguard Engine Settings 画面

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。
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しきい値を超えた分のパケットが廃棄されます。

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

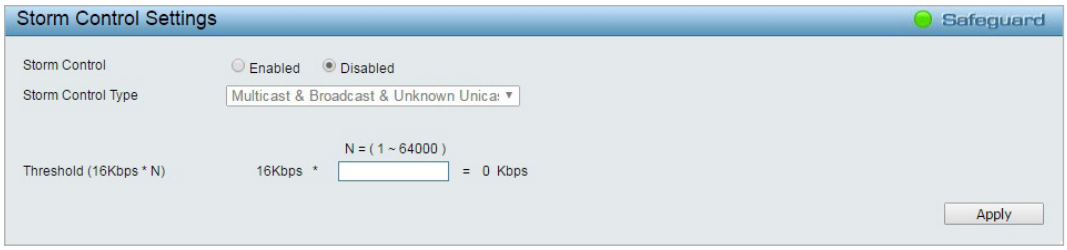


図 4-120　Storm Control Settings 画面

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、「Storm Control 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(16Kbps*N)」で、しきい値を設定します。

補足　しきい値は毎秒 16-1024000Kbps で設定可能です。
「N」には 1-64000 の間の数値を設定し、16Kbps 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。

注意　ストームコントロール設定において、Unknown Unicast の設定が含まれる場合、CPU 宛ての トラフィックも対象となります。

注意　ストームコントロールは、OSPF などの予約 MAC アドレス宛てのマルチキャストも対象とします。

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ます）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 4-121　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。

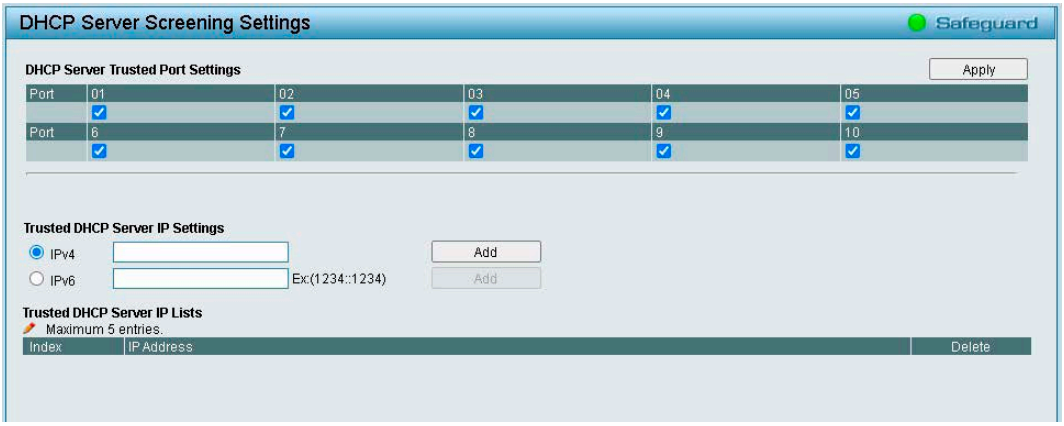


図 4-122　DHCP Server Screening Settings 画面

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/TLS（SSL/TLS 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（Ciphersuite）と呼ばれるセキュリティ文字列により実現されます。

DGS-1210 シリーズは、セキュリティに対する需要に応えた最新の TLS1.3 をサポートしています。
本画面では、SSL のグローバル設定と暗号スイート（Ciphersuite）の設定を行います。初期値では SSL は無効です。

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。

補足　SSL プロトコルには古い順から「SSL v2.0」「SSL v3.0」「TLS v1.0」「TLS v1.1」「TLS v1.2」「TLS v1.3」の種類があります。
本製品は「TLS v1.0」「TLS v1.1」「TLS v1.2」「TLS v1.3」をサポートしています。SSL v3.0 はサポートしていません。

SSL（Secure Sockets Layer）は、インターネットコミュニティの大部分で選択されている安全な通信プロトコルです。 SSL は、TCP を介した送信を保護できるため、多くのアプリケーションが存在します。
TLS（Transport Layer Security）は、SSL の後継であり提供する機能はほぼ同じです。通信するアプリケーションとインターネット上のユーザとの間のプライバシーを確保します。サーバとクライアントが通信する際、TLS は第三者によるメッセージの盗聴や改ざんを防止します。
HTTPS は、機密性の高い情報を保護し、暗号化と認証を強化し、SSL/TLS 上で実行するために使用される HTTP のセキュアバージョンです。 HTTPS は、ブラウザと Web サーバ間の Web ブラウジングサービスを保護するために使用されます。HTTPS（Hyper Text Transfer Protocol Secure）による Web の閲覧を行う場合は「SSL State」を有効に設定します。有効に設定した場合、HTTP は無効になります。

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

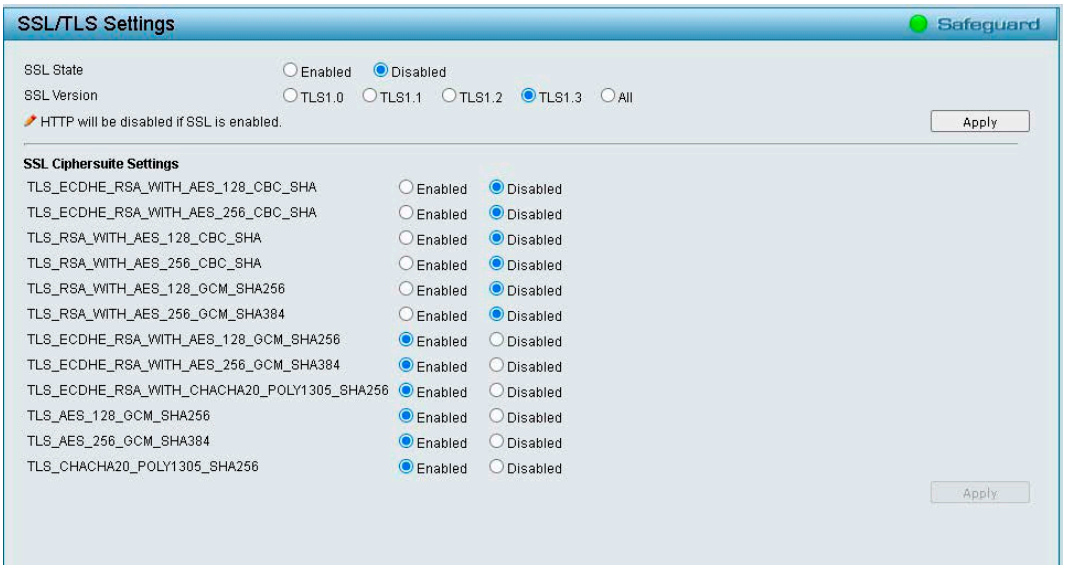


図 4-123　SSL/TLS Settings 画面

2. 「SSL State」で、「Enabled」（有効）または「Disabled」（無効）を選択します。（初期値：「Disabled」）
3. 「SSL Version」で SSL バージョンを指定します。
4. 上部の「Apply」をクリックし、設定を有効にします。
5. 「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。
6. 下部の「Apply」をクリックし、設定を有効にします。

補足　SSL 設定を有効化した後は、ブラウザにセキュア URL を入力し、再度ログインしてください。（例：https://10.90.90.90）

注意　HTTPS を使用した Web GUI 設定はサポートしていません。

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。

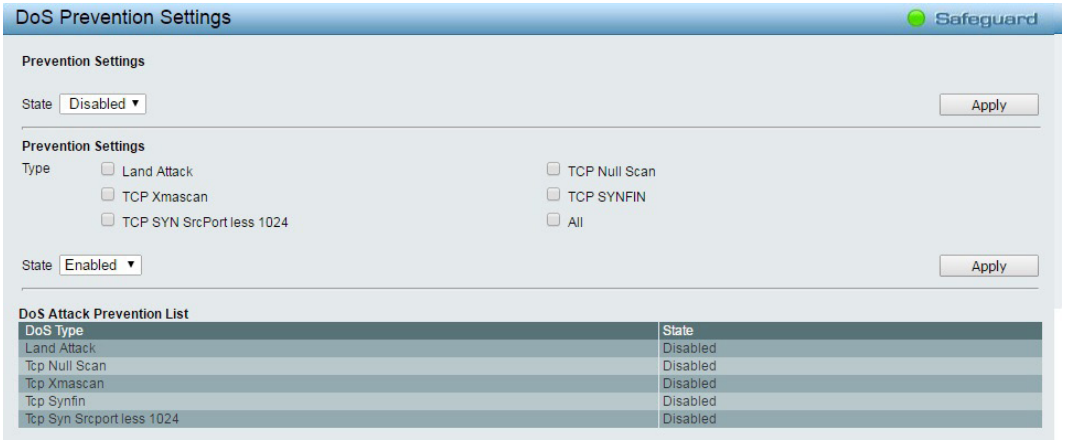


図 4-124　DoS Prevention Settings 画面

2. 「Prevention Settings」セクションの「State」で、「Enabled」（有効）または「Disabled」（無効）を選択します。

3. 上部の「Apply」をクリックし、設定を有効にします。

4. 以下の項目を設定します。

項目	説明
Prevention Settings	
Type	攻撃防止設定を有効にする攻撃の種類を選択します。 • 選択肢：「Land Attack」「TCP Null Scan」「TCP Xmascan」「TCP SYNFIN」「TCP SYN SrcPortless 1024」「All」
State	指定した攻撃タイプの攻撃防止設定を「Enabled」（有効）または「Disabled」（無効）に設定します。

5. 下部の「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。エンドポイント間で、安全性の高い、暗号化されたリモート通信を実現します。
SSH は、平文の通信（Telnet）に比べてより安全な通信です。

注意　Telnet のセッション数は最大 4、SSH のセッション数は最大 4 です。

注意　SSH のセッションタイムアウトは「Security」>「SSH」>「SSH Settings」の「Connection Timeout」で設定します。
Telnet のセッションタイムアウトは「System」>「System Settings」の「Login Timeout」で設定した値で実行されます。

注意　Telnet と SSH は同時に有効化できません。

注意　SSH の場合、ログインプロンプト画面が表示されるまでの時間が Telnet よりも長くなります。

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 4-125　SSH Settings 画面

2. 以下の項目を設定します。

項目	説明
SSH State	「Enabled」（有効）または「Disabled」（無効）を選択します。
Max Session	同時にスイッチに接続できる数を指定します。 • 設定可能範囲：1-4 • 初期値：4
Connection Timeout	接続のタイムアウト時間を指定します。 • 設定可能範囲：120-600（秒） • 初期値：120（秒）
Authfail Attempts	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。 • 設定可能範囲：2-20（回） • 初期値：2（回） 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。
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」「Data Integrity 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。

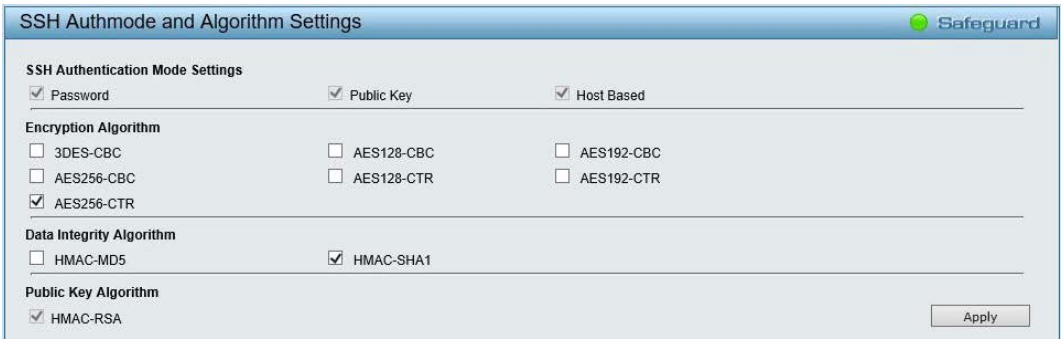


図 4-126　SSH Authmode and Algorithm Settings 画面

2. 有効にする項目にチェックをいれます。

項目	説明
SSH Authentication Mode Settings	
Password	スイッチにおける認証にローカルに設定したパスワードを使用する場合、有効にします。初期値 :「Enabled」（有効）
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 :「Enabled」（有効）
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 :「Enabled」（有効）
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。
AES128-CBC	CBC 方式で AES128 暗号化アルゴリズムを有効または無効にします。
AES192-CBC	CBC 方式で AES192 暗号化アルゴリズムを有効または無効にします。
AES256-CBC	CBC 方式で AES256 暗号化アルゴリズムを有効または無効にします。
AES128-CTR	CTR 方式で AES128 暗号化アルゴリズムを有効または無効にします。
AES192-CTR	CTR 方式で AES192 暗号化アルゴリズムを有効または無効にします。
AES256-CTR	CTR 方式で AES256 暗号化アルゴリズムを有効または無効にします。
Data Integrity Algorithm	
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。
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。
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 :「Enabled」（有効）

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 4-127　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 4-128　SSH User Authentication Modify 画面

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。 • 「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 IPv4 address	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。
Host IPv6 address	SSH ユーザの IP v6 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。
Download Host Based Public Key	
File Name	認証モードが「Host Based」の場合、ファイルを指定して「Download」をクリックすると、スイッチにファイルがダウンロードされます。

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。

SSH Public Key Settings（SSH 公開鍵設定）

SSH 公開鍵ファイルをスイッチにダウンロードします。

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

図 4-129　SSH Public Key Settings 画面

2. 「参照」をクリックして SSH 公開鍵ファイルを選択します。
3. 「Download」をクリックしてファイルをダウンロードします。

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、パケットを破棄します。

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。

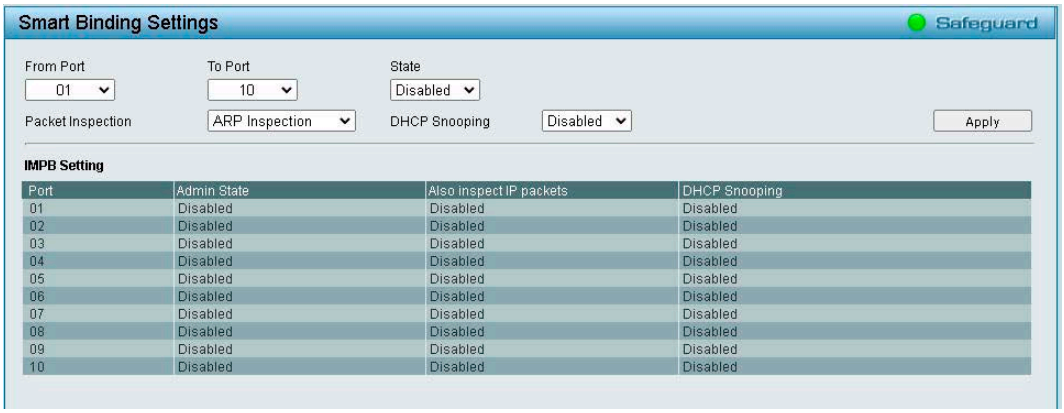


図 4-130　Smart Binding Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
State	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。 • 「ARP Inspection」（初期値）- 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、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 テーブルを持つ PC からの DoS 攻撃では ARP パケットが送信されないため、スイッチはこの PC からの攻撃を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 ペアがリストで一致すると、スイッチはその MAC アドレスをブロックしません。一致しない場合、MAC アドレスはブロックされたままになります。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スヌーピングし、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。

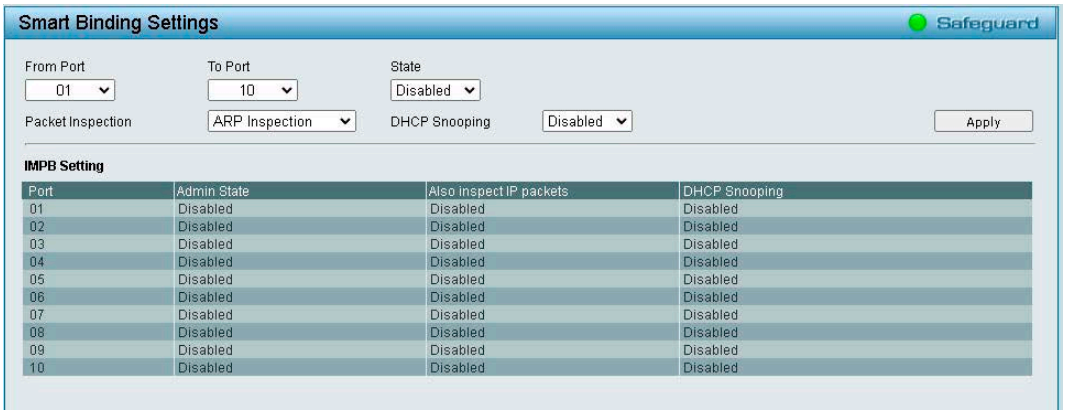


図 4-131　Smart Binding Settings 画面

■ Manual Binding で設定を行う場合

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

 登録が成功すると「Complete!」の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。

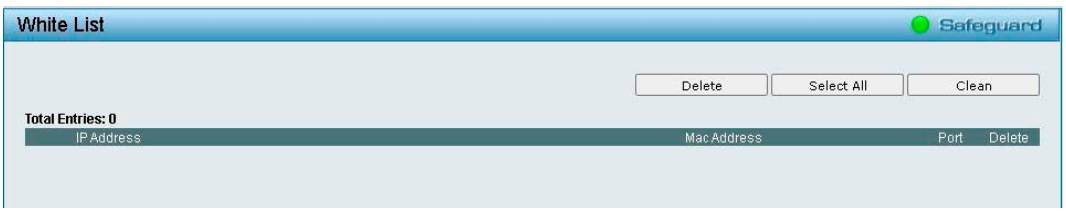


図 4-132　White List 画面

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、リストに一致しない IP-MAC-Port 情報を含む ARP パケットをデバイスが送信している場合、その機器はブロックされ、このテーブルに表示されます。

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

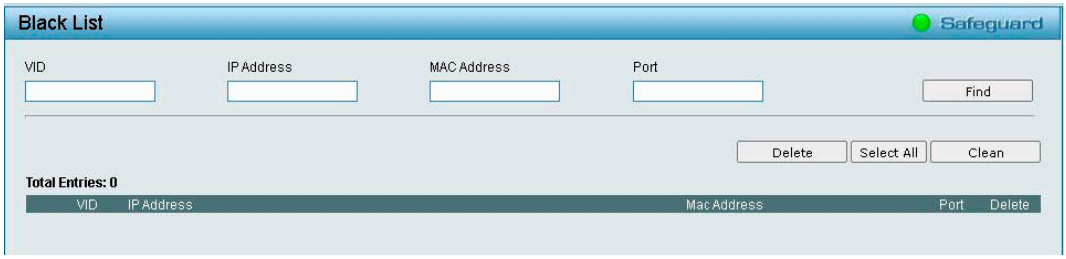


図 4-133　Black List 画面

■ 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。

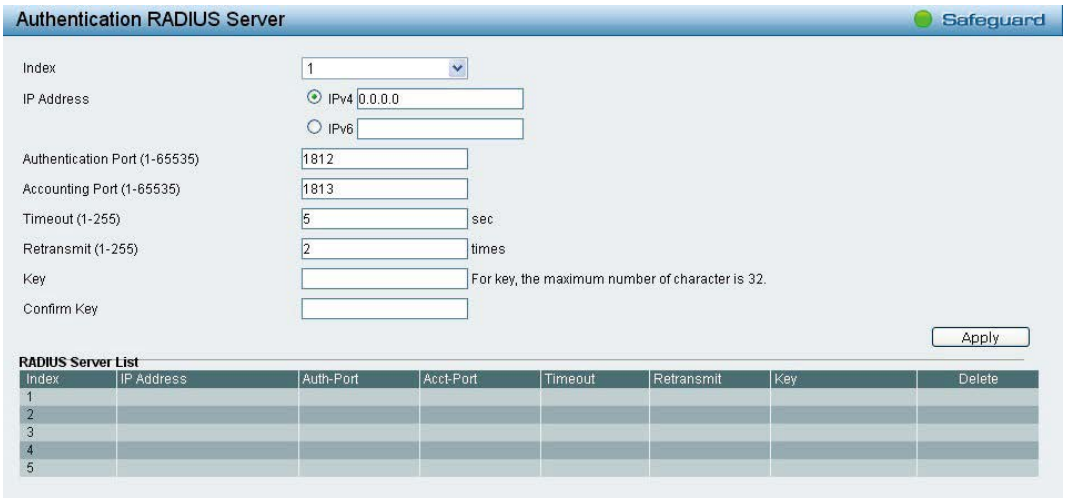


図 4-134　Authentication RADIUS Server 画面

2. 以下の項目を設定します。

項目	説明
Index	設定を行う RADIUS サーバを指定します。 • 選択肢 :「1」「2」「3」「4」「5」
IP Address	RADIUS サーバの IP アドレスを入力します。
Authentication Port	RADIUS 認証サーバの UDP ポートを指定します。 • 設定可能範囲：1-65535 • 初期値：1812
Accounting Port	RADIUS アカウントサーバの UDP ポートを指定します。 • 設定可能範囲：1-65535 • 初期値：1813
Timeout	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。 • 設定可能範囲：1-255（秒） • 初期値：5（秒）
Retransmit	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。 • 設定可能範囲：1-255（回） • 初期値：2（回）
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。

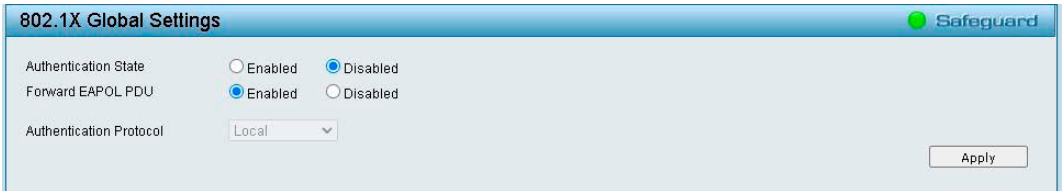


図 4-135　802.1X Global Settings 画面

2. 以下の項目を設定します。

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」 補足　802.1X 機能をグローバルまたはポートで無効とした場合に、EAPOL PDU をグローバルおよびポートに対して送信するように 802.1X を設定すると、同じ VLAN 内で（グローバルまたはそのポートに対して）802.1X forward PDU が有効で 802.1X が無効であるポートに、ポートで受信した EAPOL パケットをフラッドします。 注意　IGMP スヌーピング有効時には EAP は透過できません。
Authentication Protocol	認証プロトコルを選択します。 ・ 選択肢：「Local」「RADIUS」

3. 「Apply」をクリックし、設定を有効にします。

注意　802.1X の機能において、Local DB を指定した場合、EAP-MD5 のみをサポートします。

注意　802.1X の機能は、Port Based のみサポートします。

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。

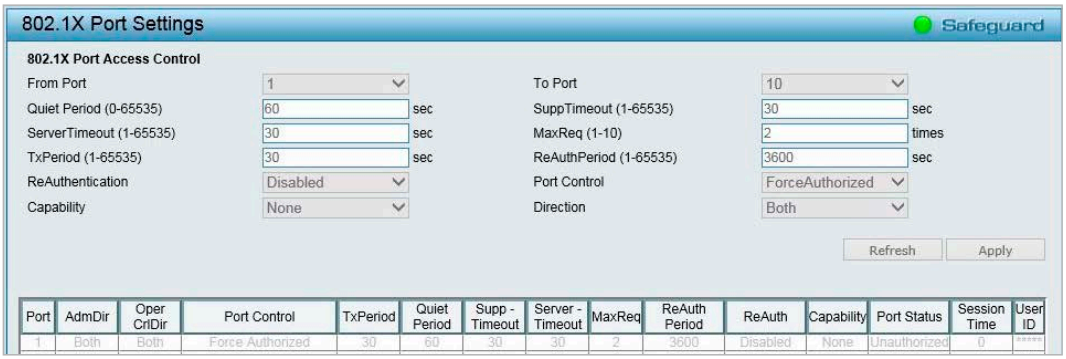


図 4-136　802.1X Port Settings 画面

2. 以下の項目を設定します。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
QuietPeriod	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。 • 設定可能範囲：0-65535（秒） • 初期値：60（秒）
SuppTimeout	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。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
ServerTimeout	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。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
MaxReq	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。 • 設定可能範囲：1-10（回） • 初期値：2（回）
TxPeriod	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。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
ReAuthPeriod	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。 • 設定可能範囲：1-65535（秒） • 初期値：3600（秒）
Port Control	ポート認証制御の方法を設定します。本項目は「Capability」を「Authenticator」に設定した場合のみ設定できます。 • 「ForceAuthorized」- 802.1X を無効にし、認証情報の交換を要求せずにポートを Authorized 状態にします。この時ポートではクライアントの 802.1X ベースの認証を行うことなく、通常のトラフィックの送受信が可能になります。 • 「ForceUnauthorized」- 対象ポートは Unauthorized 状態を保ち、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」（初期値）- 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。

注意　「Direction」で「Both」を指定しても、Tagged の Egress は抑止されません。

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 4-137　802.1X 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。

802.1X Guest VLAN（802.1X ゲスト VLAN 設定）

802.1X ゲスト VLAN は、802.1X 経由で認証に失敗したポートをゲスト VLAN グループに割り当てます。
本画面では、802.1X ゲスト VLAN をオンにするポートを指定できます。

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

図 4-138　Guest VLAN 画面

2. 802.1X ゲスト VLAN をオンにするポートにチェックを入れます。
3. 「Apply」をクリックし、設定を有効にします。

設定を削除する場合は「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 Group（ACL アクセスグループ）
- 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 プロファイル（768 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→「Access-List Name」にアクセスリストの名前を設定し、「Next」をクリックします。

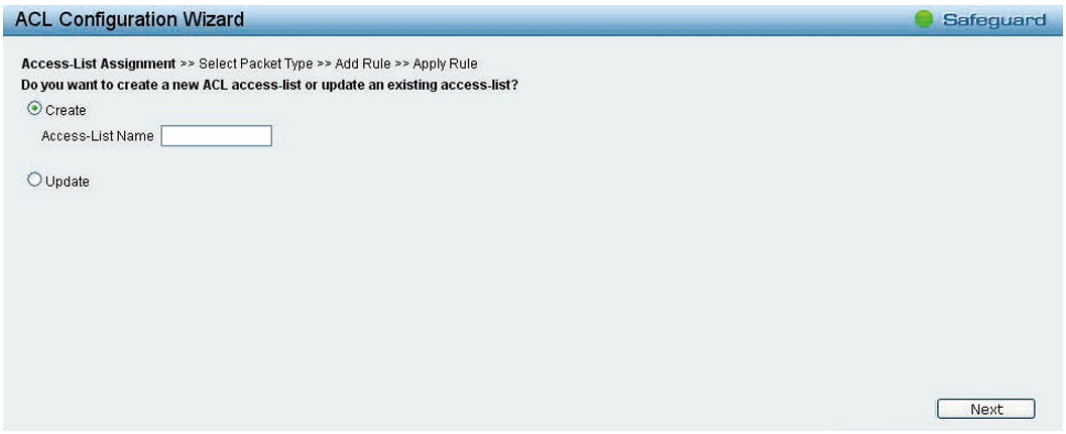


図 4-139　ACL Configuration Wizard 画面

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 4-140　ACL Configuration Wizard - Packet Type 画面

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異なります。
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 →「Next」をクリックし、以下の画面で設定を行います。

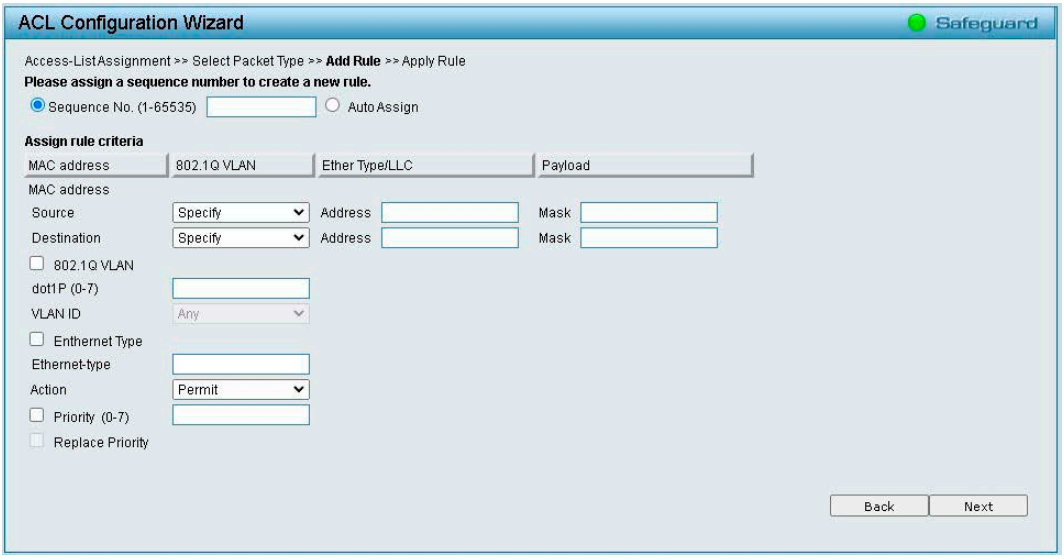


図 4-141　ACL Configuration Wizard - MAC ACL Rule 画面

項目	説明
Assign sequence number（シークエンス番号の指定）	
Sequence No.	シークエンス番号を指定します。 • 設定可能範囲：1-65535
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 ACL の設定）	
MAC Address	
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	
802.1Q VLAN	チェックを入れ 802.1Q VLAN の設定を行います。
dot1P	優先値を指定します。 • 設定可能範囲：0-7
VLAN ID	パケットヘッダの 802.1p プライオリティ値を検査し、転送の基準として本値を確認するオプションになります。 • 選択肢：「Any」、既存の VLAN ID
Ethernet Type	
Ethernet Type	チェックを入れイーサネットタイプの設定を行います。
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	
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。
Priority	
Priority	チェックを入れ、プライオリティ値を指定します。 • 設定可能範囲：0-7
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→「Next」をクリックし、以下の画面で設定を行います。

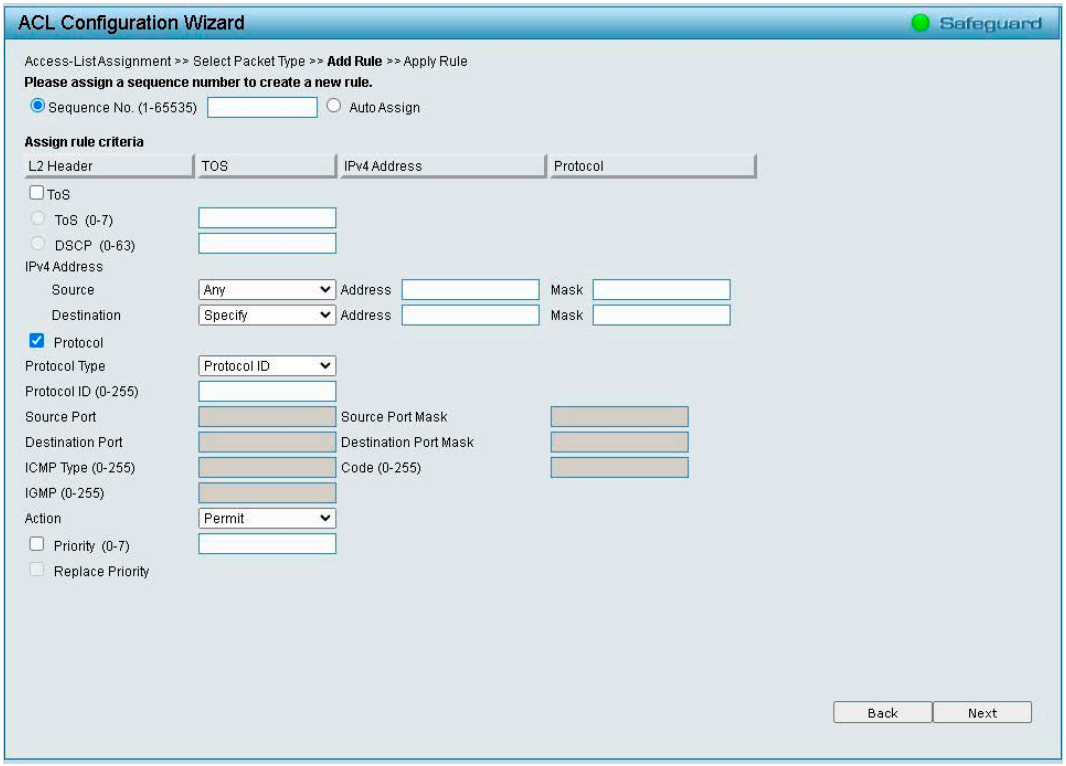


図 4-142　ACL Configuration Wizard -IPv4 画面

項目	説明
Assign sequence number（シークエンス番号の指定）	
Sequence No.	シークエンス番号を指定します。 • 設定可能範囲：1-65535
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	
ToS	チェックを入れ ToS 優先値と DSCP 値の設定を行います。
ToS	ToS の値を入力します。 • 設定可能範囲：0-7
DSCP	DSCP の値を入力します。 • 設定可能範囲：0-63
IPv4 Address	
Source	送信元 IPv4 アドレスを指定します。 •「Specify」- ACL ルールで照合する送信元 IPv4 アドレス / マスクを指定します。 •「Any」- 全ての送信元 IP アドレスが ACL ルールで照合されます。
Destination	宛先 IPv4 アドレスを指定します。 •「Specify」- ACL ルールで照合する宛先 IPv4 アドレス / マスクを指定します。 •「Any」- 全ての宛先 IP アドレスが ACL ルールで照合されます。
Protocol	
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。 • 選択肢：「ICMP」「IGMP」「TCP」「UDP」「Protocol ID」
ICMP 選択時	
ICMP Type	ICMP Type を入力します。 • 設定可能範囲：0-255
Code	ICMP code を入力します。 • 設定可能範囲：0-255

項目	説明
IGMP 選択時	
IGMP	IGMP Type を入力します。 • 設定可能範囲：0-255
TCP/UDP 選択時	
Source Port	ACL ルールで照合する送信元ポートの範囲を指定します。
Source Port Mask	ACL ルールで照合する送信元ポートマスクを指定します。
Destination Port	ACL ルールで照合する宛先ポートの範囲を指定します。
Destination Port Mask	ACL ルールで照合する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。 • 設定可能範囲：0-255
Action	
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。
Priority	
Priority	チェックを入れ、プライオリティ値を指定します。 • 設定可能範囲：0-7
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を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 →「Next」をクリックし、以下の画面で設定を行います。

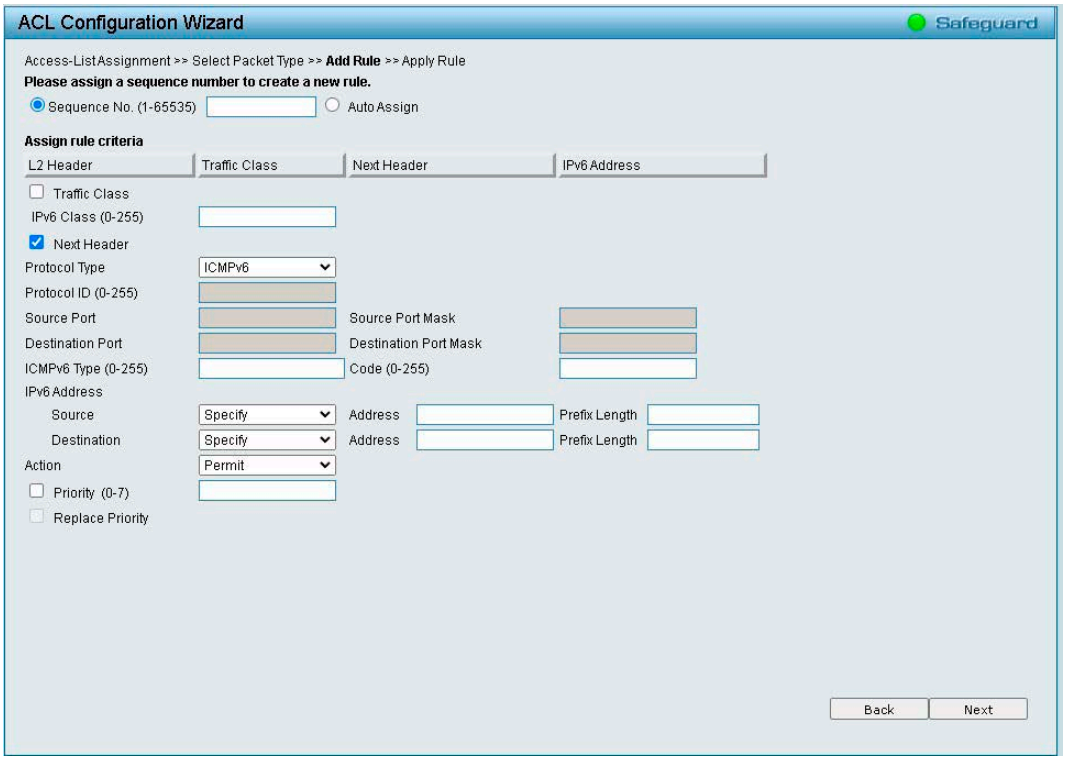


図 4-143　ACL Configuration Wizard -IPv6 画面

項目	説明
Assign sequence number（シークエンス番号の指定）	
Sequence No.	シークエンス番号を指定します。 • 設定可能範囲：1-65535
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（IPv6 ACL の設定）	
ToS	
Traffic Class	チェックを入れ Traffic Class の設定を行います。
IPv6 Class	アクセスルールのクラスを指定します。 • 設定可能範囲：0-255
Protocol	
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	IPv6 のプロトコル種類を選択します。 • 選択肢：「ICMPv6」「TCP」「UDP」「Protocol ID」
ICMP 選択時	
ICMPv6 Type	ICMPv6 Type を入力します。 • 設定可能範囲：0-255
Code	ICMP code を入力します。 • 設定可能範囲：0-255
TCP/UDP 選択時	
Source Port	ACL ルールで照合する送信元ポートの範囲を指定します。
Source Port Mask	ACL ルールで照合する送信元ポートマスクを指定します。
Destination Port	ACL ルールで照合する宛先ポートの範囲を指定します。
Destination Port Mask	ACL ルールで照合する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。
IPv6 Address	
Source	送信元 IPv6 アドレスを指定します。 •「Specify」- ACL ルールで照合する送信元 IPv6 アドレス / マスクを指定します。 •「Any」- 全ての送信元 IPv6 アドレスが ACL ルールで照合されます。 •「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」- ACL ルールで照合する宛先 IPv6 アドレス / マスクを指定します。 •「Any」- 全ての宛先 IPv6 アドレスが ACL ルールで照合されます。 •「Prefix Length」-「Specify」を選択時にプレフィクス長を入力します。
Action	
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。
Priority	
Priority	チェックを入れ、プライオリティ値を指定します。 • 設定可能範囲：0-7
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。

4. アクセスリストを適用するポートを選択します。

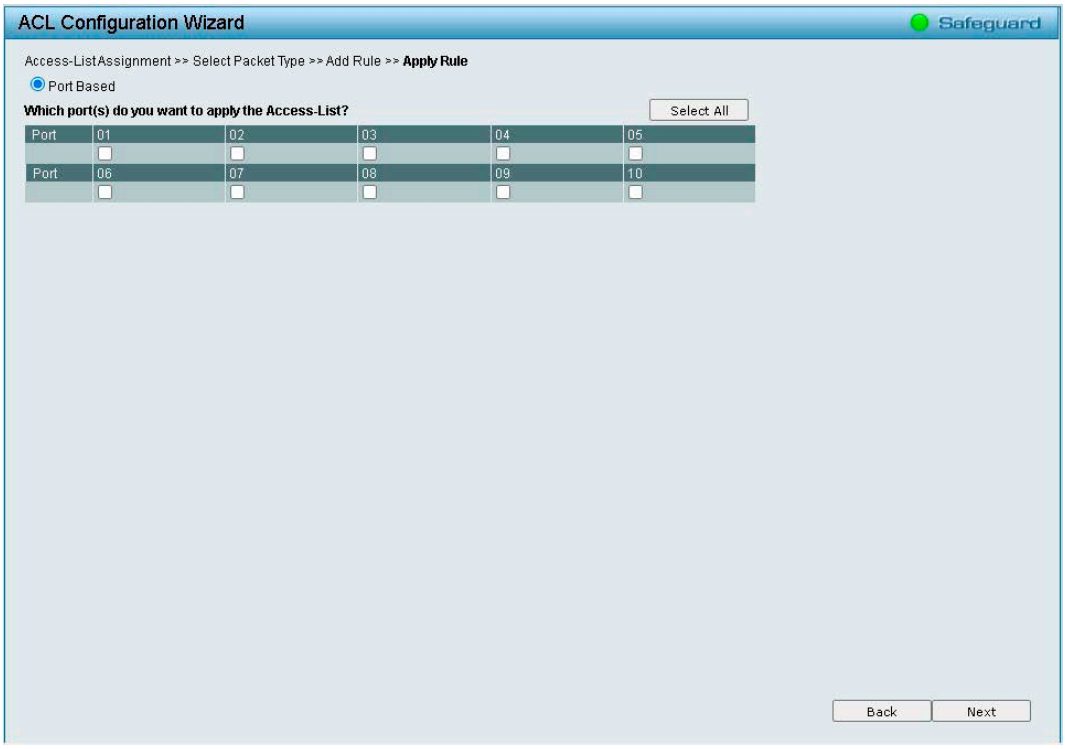


図 4-144　Add Access Rule – Ports 画面

「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。

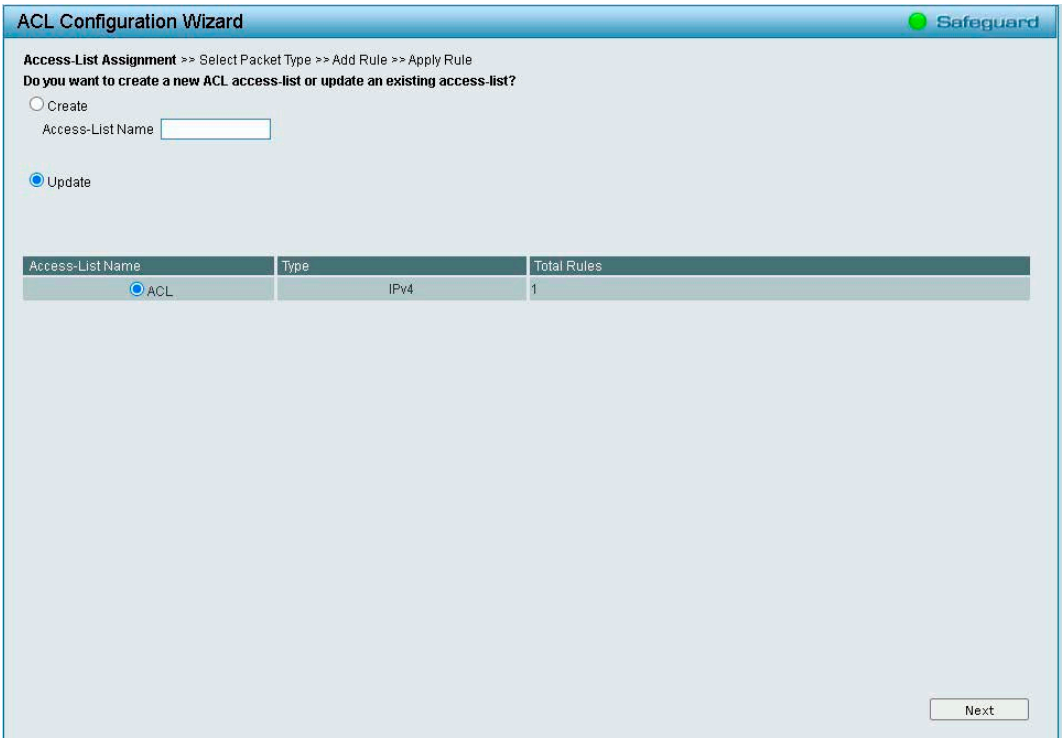


図 4-145　ACL Wizard – Update ACL List 画面

ACL Access List (ACL アクセスリスト)

ACL Access List（ACL アクセスリスト）では、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。

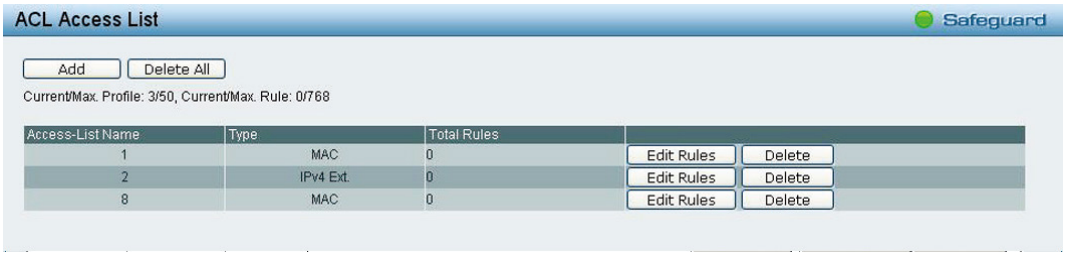


図 4-146　ACL Access List 画面

2. 以下の項目を設定します。

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。

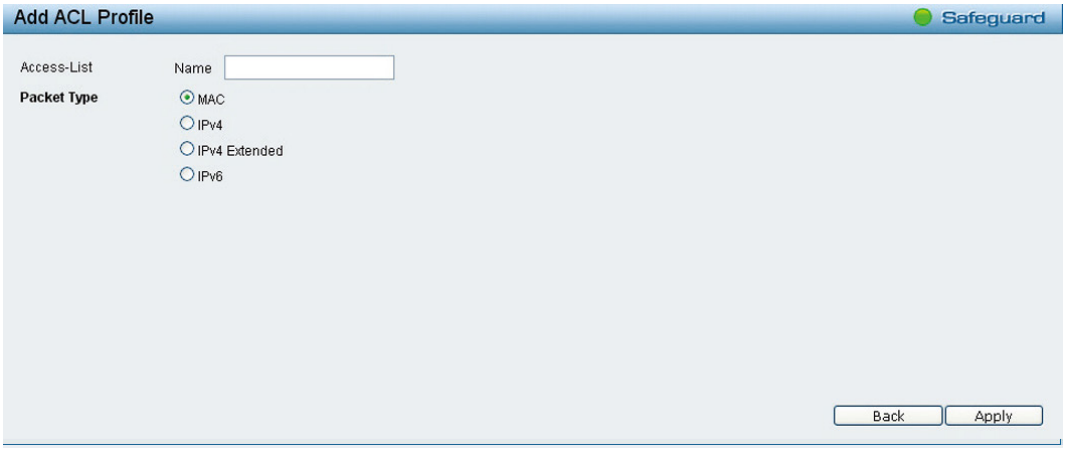


図 4-147　Add ACL Profile 画面

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 Extended」「IPv6」から選択します。

4. 「Apply」をクリックします。

5. 既存のルールを編集する場合は「Edit Rules」をクリックし、表示されるルールリスト画面で「Seq. No」（シークエンス番号）のハイパーリンクをクリックします。

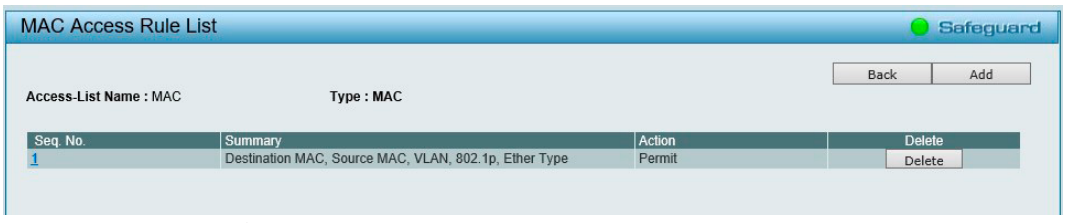


図 4-148　MAC Access Rule List 画面

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 4-149　ACL Access Group 画面

2. 以下の項目を設定します。

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 4-150　ACL Hardware Resource Status 画面

PoE の設定（DGS-1210-10MP/28MP 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）
- PD Alive（PD アライブ設定）

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。

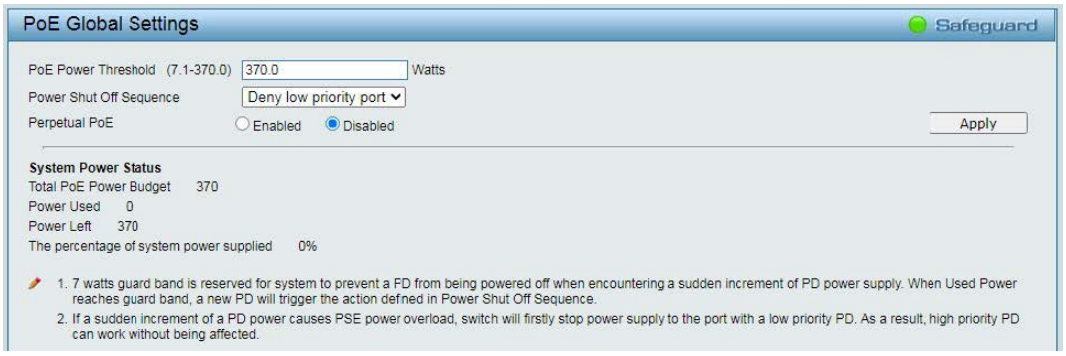


図 4-151　PoE Global Settings 画面

2. 以下の項目を設定します。

項目	説明
PoE Power Threshold	システムの給電可能電力を設定します。 • 設定可能範囲：7.1 - 130W（DGS-1210-10MP）、7.1 - 370W（DGS-1210-28MP）
Power Shut Off Sequence	Power Guard Band（電力保護帯域）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。 •「Deny next port」- Power Guard Band 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。 補足 Power Guard Band（電力保護帯域）は、最大供給電力の内 7W 確保されています。
Perpetual PoE	有効にした場合、スイッチがブートプロセス中でも受電機器に給電を継続できます。 補足 Perpetual PoE は、DGS-1210-10MP ではサポートされていません。
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。

注意　ハードウェア制限により、「Power Shut Off Sequence」を「Deny next port（既定）」に設定している場合でも、給電余力電力が Guard band を下回らない限り、「Deny low priority port」として動作します。

PoE Port Settings（PoE ポート設定）

DGS-1210-10MP/28MP 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-1210-10MP：1 ～ 8 ポート：最大 30W
DGS-1210-28MP：1 ～ 24 ポート：最大 30W

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

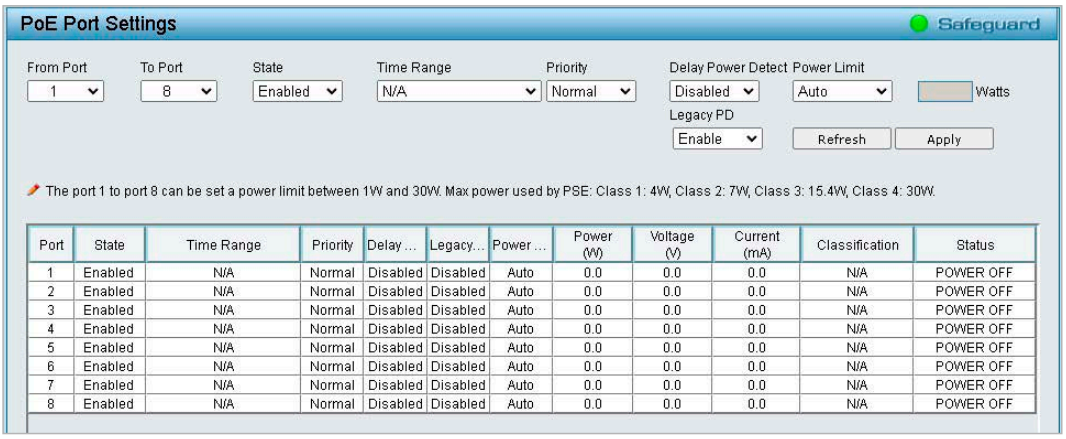


図 4-152　PoE Port Settings 画面

2. 以下の項目を設定します。

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」 補足 本スイッチは IEEE「802.3af」と「802.3at」規格に準拠しています。「IEEE」の PoE 規格は、ポートにおける「400ms（ミリ秒）」間隔で 10mA 以下となる電力使用の場合の、ポート遮断を義務付けています。規格に準拠していない機器が、より長い間隔を必要とする場合、本機能を有効化して「500ms（ミリ秒）」間隔まで延長することが可能です。有効化した場合でも PoE 受電機器が起動しない場合、その機器のサポートにご確認ください。
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。 • 「Auto」- 接続デバイスとネゴシエーションを行い、IEEE 802.3at に基づいたクラス分けが行われます。 • 「Class 1-4」-「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。
Legacy PD	レガシー PD シグナルの検出を「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。

注意　「Priority」、「Legacy PD」、「Power Limit」を変更すると、PoE による給電が一度停止します。

注意　スイッチを再起動すると、PoE 接続されている IP カメラが検出されません。再起動完了後に PoE を有効化する必要があります。

PD Alive（PD アライブ設定）

PoE ポートに接続された受電デバイス（PD）に対する PD アライブ設定を行います。PD の状態について「Ping」を使用して確認します。
PD が動作していない場合、リセット、通知などを行います。

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

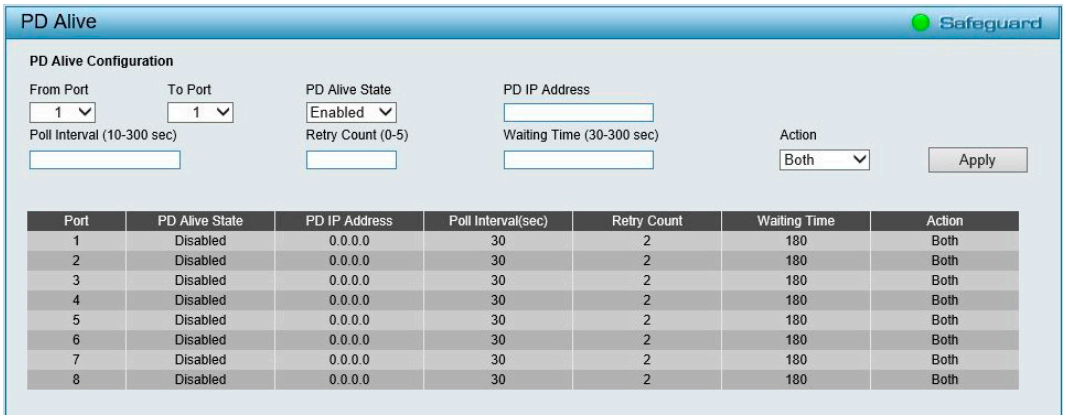


図 4-153　PD Alive 画面

2. 以下の項目を設定します。

項目	説明
From Port/To Port	本設定を適用するポート範囲を設定します。
PD Alive State	指定ポートの PD アライブの有効 / 無効を指定します。
PD IP Address	PD の IP アドレスを指定します。
Poll Interval	ポールインターバルを指定します。システムから PD に「Ping」を送信する間隔を指定します。 • 設定可能範囲：10-300（秒）
Retry Count	リトライカウントを指定します。PD に無反応の場合に再度「Ping」を送信する回数を指定します。 • 設定可能範囲：0-5（回）
Waiting Time	待機時間を指定します。リセット後にシステムから PD に「Ping」を送信するまでの待機時間を指定します。 • 設定可能範囲：30-300（秒）
Action	動作を指定します。 • 「Reboot」- PoE ポートをリブートします。（PoE ポートのオフ / オン） • 「Notify」- 管理者へログとトラップを送信します。 • 「Both」- PoE ポートをリブート（PoE ポートのオフ / オン）し、管理者へログとトラップを送信します。

3. 「Apply」をクリックし、設定を有効にします。

SNMP（SNMP の設定）

SNMP の設定項目

System（システム設定）

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

図 4-154　SNMP Global Settings 画面

2. 以下の項目を設定します。

項目	説明
SNMP Global State	SNMP を「Enabled」（有効）または「Disabled」（無効）にします。 • 初期値：「Disabled」
Trap Settings	SNMP 通知を送信する内容にチェックをいれます。 • 「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-1210-10MP/28MP 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。

注意 SNMP のウォームスタートトラップはサポートされません。

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

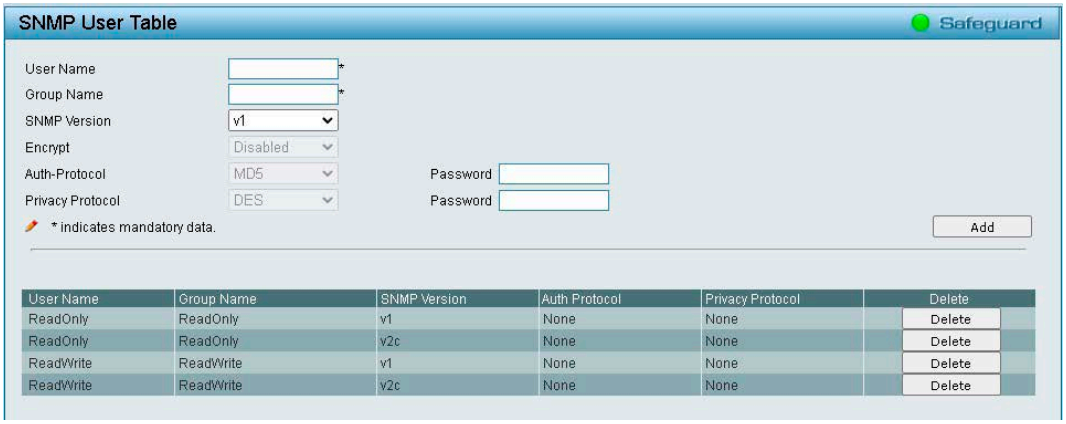


図 4-155　SNMP User Table 画面

2. 以下の項目を設定します。

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 バージョンを指定します。SNMPv3 のみがメッセージを暗号化します。 • 選択肢：「v1」「v2c」「v3」
Encrypt	暗号化を「Enabled」（有効）または「Disabled」（無効）にします。
Auth-Protocol/ Password	認証プロトコルを指定します。 • 「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	暗号化方式を指定します。 • 「none」- 認証プロトコルは使用されません。 • 「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
設定項目を入力し、「Add」をクリックします。

エントリの削除を行う場合
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」>「System」>「SNMP Group」の順にメニューをクリックします。

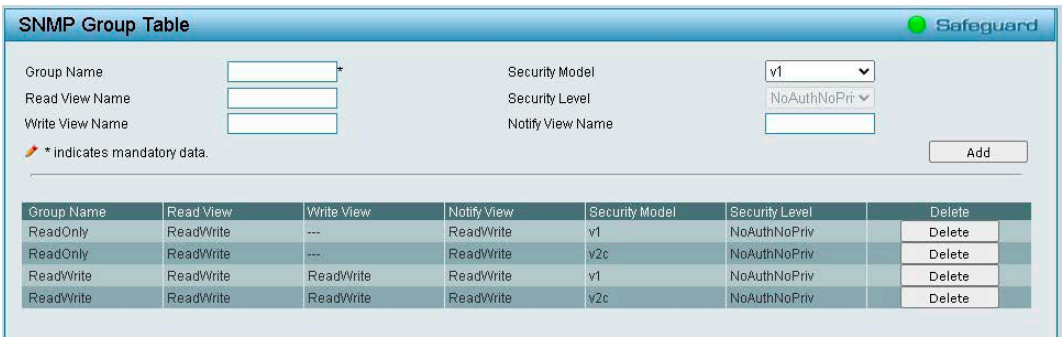


図 4-156　SNMP Group Table 画面

2. 以下の項目を設定します。

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。 • 「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。 • 「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
設定項目を入力し、「Add」をクリックします。

エントリの削除を行う場合
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可能にするかを指定します。

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

図 4-157　SNMP View Table Configuration 画面

2.　以下の項目を設定します。

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 に指定した箇所はオブジェクト番号が一致している必要があり、0 に指定した箇所はマスクされます。 例：マスク 1.1.1.1.1.1.0 を持つ 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。 • 「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
設定項目を入力し、「Add」をクリックします。

SNMP ビューの削除を行う場合
「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」>「System」>「SNMP Community」の順にメニューをクリックします。

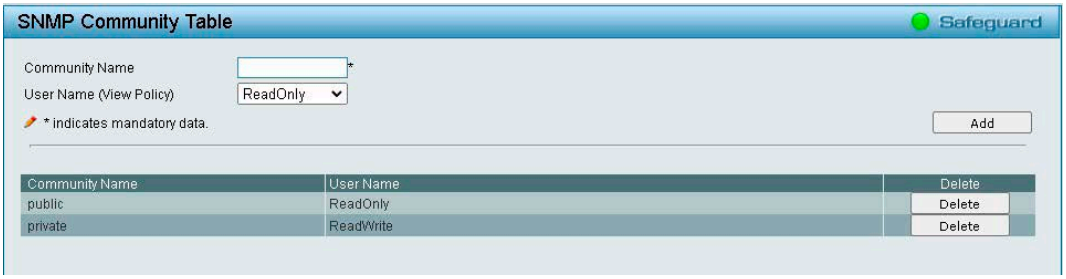


図 4-158　SNMP Community Table 画面

2.　以下の項目を設定します。

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。 • 選択肢：「ReadWrite」（読み込み / 書き込み）、「ReadOnly」（読み込みのみ） • 初期値：「ReadOnly」

SNMP コミュニティの登録を行う場合
設定項目を入力し、「Add」をクリックします。

SNMP コミュニティの削除を行う場合
「Delete」をクリックします。

SNMP Host（SNMP ホスト）

SNMP トラップの受信ホストを設定します。

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

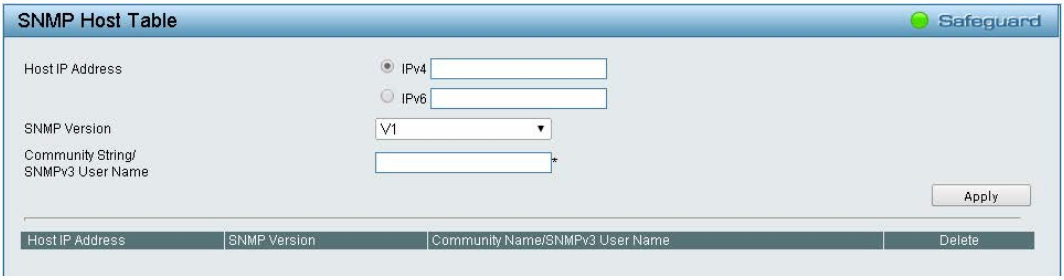


図 4-159　SNMP Host Table 画面

2. 以下の項目を設定します。

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 エンジンを識別するために使用される固有の識別子です。

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

図 4-160　SNMP Engine 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 4-161　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、設定します。

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

図 4-162　RMON Ethernet Statistics Settings 画面

2. 以下の項目を設定します。

項目	説明
Index	RMON イーサネット統計情報エントリの番号を指定します。 • 設定可能範囲：1-65535
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
設定項目を入力し、「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
エントリの「Delete」をクリックします。

統計情報の更新を行う場合
「Refresh」をクリックします。

RMON History Control Settings（RMON ヒストリ管理設定）

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。

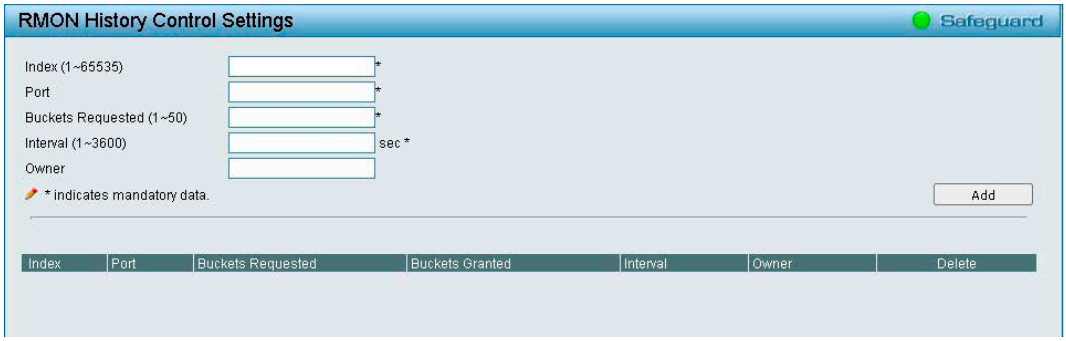


図 4-163　RMON History Control Settings 画面

2. 以下の項目を設定します。

項目	説明
Index	ヒストリ制御エントリ番号を指定します。 • 設定可能範囲：1-65535
Port	RMON 情報を取得したポートを指定します。
Buckets Requested	デバイスが保存するバケット数を指定します。 • 設定可能範囲：1-50
Interval	ポートからサンプリングする間隔（秒）を設定します。 • 設定可能範囲：1-3600（秒） • 初期値：1800（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

設定項目を入力し、「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

「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 4-164　RMON Alarm Settings 画面

2. 以下の項目を設定します。

項目	説明
Index	特定のアラームを指定します。 • 設定可能範囲：1-65535
Variable	選択した MIB 変数の値を指定します。
Rising Threshold	上昇しきい値を設定します。 • 設定可能範囲：0-2^31-1
Rising Event Index	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。 • 設定可能範囲：1-65535
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	アラームの間隔を定義します。 設定可能範囲：1-2^31-1（秒）
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。 •「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	下降しきい値を設定します。 • 設定可能範囲：0 -2^31-1
Falling Event Index	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。 • 設定可能範囲：1-65535

アラームの登録を行う場合

設定項目を入力し、「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

「Delete」をクリックします。

RMON Event Settings（RMON イベント設定）

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 4-165　RMON EventSettings 画面

2. 以下の項目を設定します。

項目	説明
Index	イベントを指定します。 • 設定可能範囲：1-65535
Description	ユーザ定義のイベントの説明を指定します。
Type	イベントタイプを指定します。 • 「None」- イベントは発生しません。 • 「Log」- イベントにログエントリを指定します。 • 「SNMP Trap」- イベントにトラップを指定します。 • 「Log and Trap」- イベントにログエントリとトラップの両方を指定します。
Community	イベントが所属するコミュニティを指定します。
Owner	イベントの所有者を指定します。

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
設定項目を入力し、「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
「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。

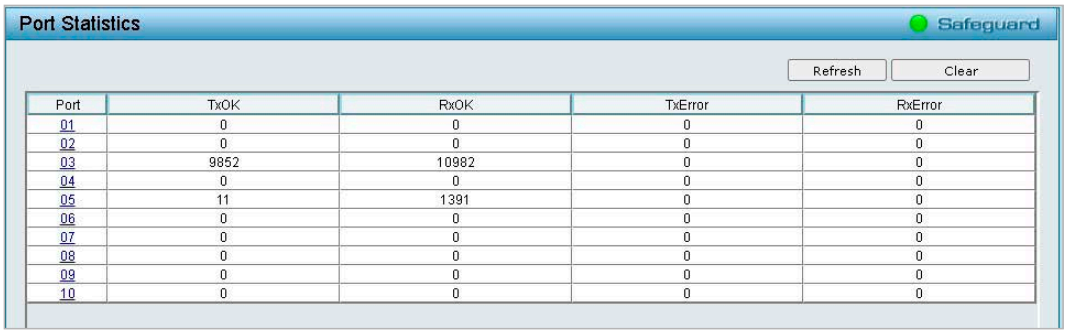


図 4-166　Port Statistics 画面

2. 以下の項目が表示されます。

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。

3. 「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 4-167　Port Statistics 画面

「Back」をクリックすると、手順 1 の画面に戻ります。

4. 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。

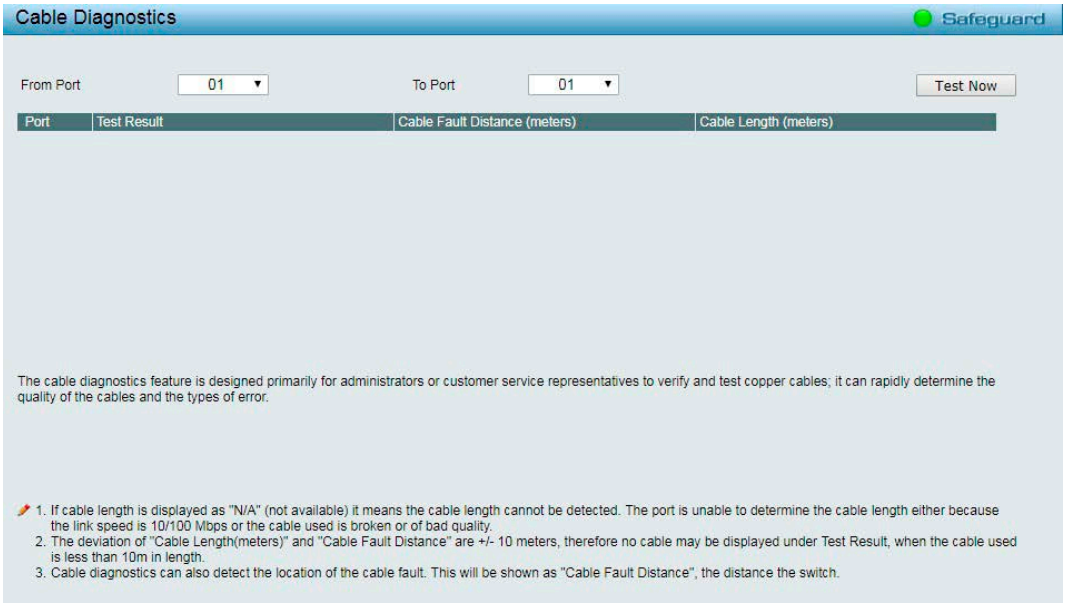


図 4-168　Cable Diagnostics 画面

2. 「From Port / To 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。

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。 • 「Mismatched」- 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。 • 「Line Driver in Cable」- ハイ・インピーダンス状態を検出しました。電源オフ状態のリンクパートナーに接続している場合などが考えられます。
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 10 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 5 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 ～ 140 メートル • 140 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。

注意　「Cable Length (meters)」及び「Cable Fault Distance」の結果は、実際のケーブル長に対して +/- 10 メートル程度の誤差が発生する可能性があります。そのため、ケーブル長が 10 メートル未満の場合は検出結果に表示されない可能性があります。

注意　ケーブル診断の機能において、2 Paris の UTP を使用した場合でも、4 Pairs で "Open in Cable"、"OK" の表示となります。

注意　ケーブル診断では Crosstalk の検出はできません。

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。

図 4-169　System Log 画面

2. ログを確認します。

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。

注意　スイッチを再起動すると、システムログはリセットされます。

Ping Test（Ping テスト）

Ping を送信し、接続の確認を行います。

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

図 4-170　Ping Test 画面

2. 以下の項目を設定します。

項目	説明
Target IP Address	Ping を送信する宛先を「IPv4」「IPv6」「Domain Name」から選択し、IP アドレスまたはドメイン名を入力します。
Repeat Pinging for	Ping を送信する回数を設定します。 ・ 設定可能範囲：1-255（回） 「Infinite times」にチェックを入れた場合、Ping の送信回数は無制限になります。
Timeout	Ping のタイムアウト値を設定します。 ・ 設定可能範囲：1-99（秒）

3. 「Start」をクリックし、Ping テストを実行します。

4. ログを確認します。

注意　CLI の場合、Domain Name を指定して Ping コマンドを実行することはできません。

第 5 章　サーベイランスモードの設定

本製品シリーズには「Standard Mode（スタンダードモード）」と「Surveillance Mode（サーベイランスモード）」の 2 種類の Web GUI が用意されています。「サーベイランスモード」はネットワーク上の監視デバイス（IP カメラ等）や IP セキュリティデバイスの確認と管理のために特化したインタフェースです。この二つのモード切替は「Smart Wizard」により行うことが可能です。

サーベイランスモードの開始

サーベイランスモードを開始するには、スマートウィザードで「Surveillance mode」を選択するか、通常の Web 画面のツールバーから「Surveillance mode」をクリックし、Web 画面のモードを切り替えます。

■ 初期セットアップ時にサーベイランスモードを選択した場合

スマートウィザードの初期セットアップでサーベイランスモードを選択した場合、最初に以下のクイックスタート画面が表示されます。
画面下部の「OK」をクリックします。

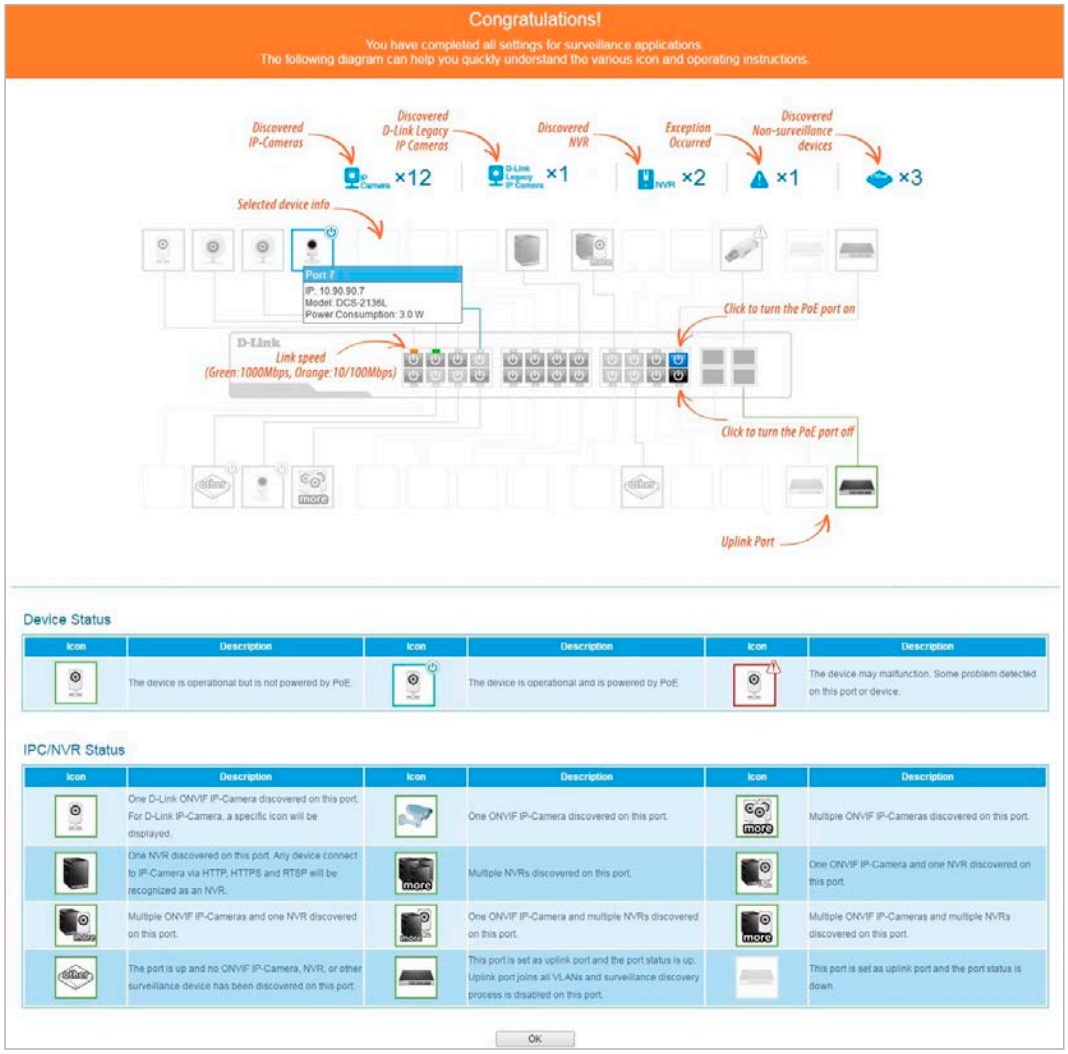


図 5-1　Surveillance Mode クイックスタート画面

■ Standard Mode 画面から切り替えた場合

1. Standard Mode（通常の Web 画面）のツールバーで「Surveillance Mode」をクリックした場合、以下の確認画面が表示されます。「OK」をクリックします。

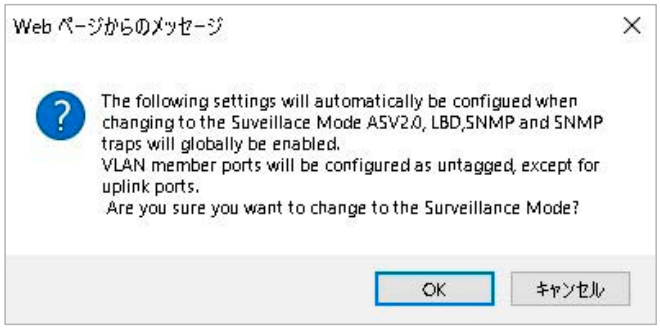


図 5-2　確認画面

補足　サーベイランスモードに移行すると、ASV2.0、LBD、SNMP、SNMP トラップがグローバルで有効になります。また、VLAN メンバポートはアップリンクポートを除いてタグなしポートになります。

補足　Web UI の各モード（Standard Mode と Surveillance Mode）は、同じコンフィグファイルを共有しています。どちらか一方のインタフェースで有効化された機能は、もう片方のインタフェースでも有効となります。

2. Web ユーザインタフェースに接続する前に、以下のポップアップ画面が表示されます。「OK」をクリックします。

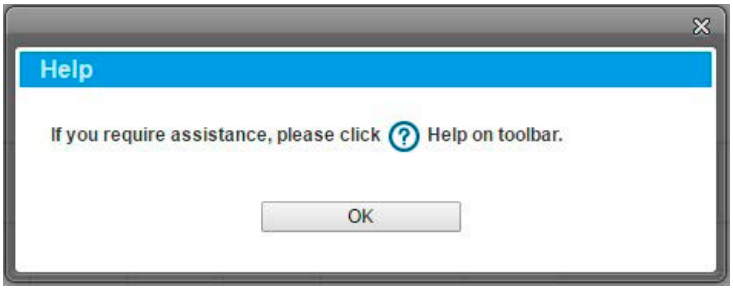


図 5-3　Help 案内画面

サーベイランスモードの画面構成

Web ユーザインタフェースではスイッチの設定、管理画面にアクセスし、パフォーマンス状況やシステム状態をグラフィック表示で参照できます。

注意 本項目では Web モードを「Surveillance Mode」にした場合についての設定方法を説明します。「Standard Mode」について詳しくは「第 4 章　Web マネージャによる詳細設定」を参照ください。

サーベイランスモードのメイン画面について

Web マネージャでスイッチの設定または管理画面にアクセスしたり、パフォーマンス状況やシステム状況を参照できます。
ログインに成功すると、デバイスの状態表示を行う画面が開きます。画面右上の角にユーザ名（初期値では「admin」）とスイッチの IP アドレスが表示されます。その下にはセッション終了時に使用する「Logout」ボタンがあります。

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。

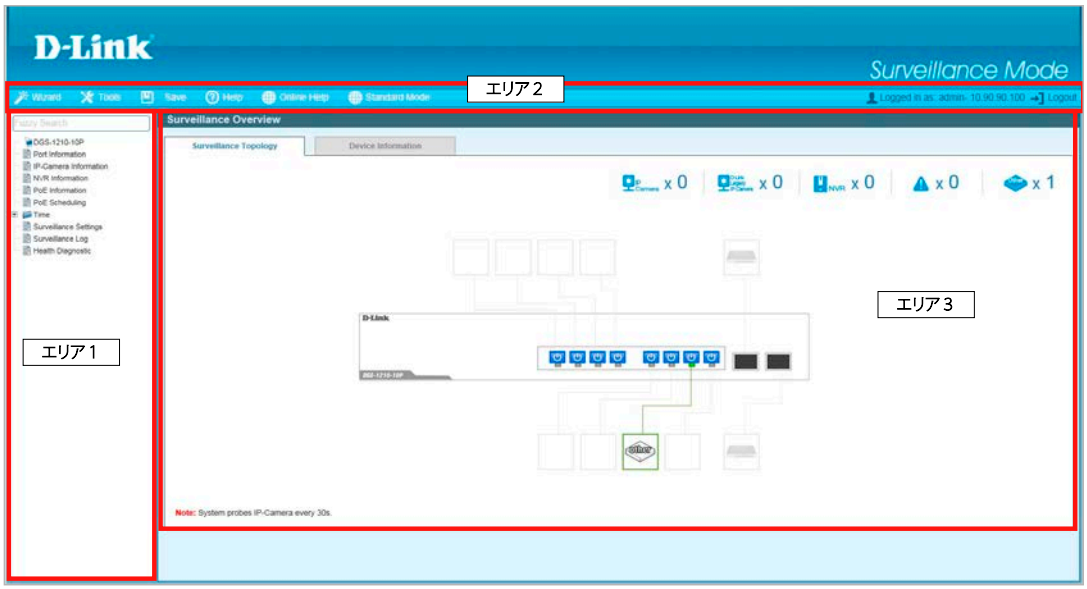


図 5-4　サーベイランスモードのメイン画面

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）：設定情報や構成オプションを表示します。

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。

サーベイランスモード Overview（サーベイランス概要）

サーベイランスモード画面が表示された場合、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「Surveillance Overview（サーベイランスの概要）」が表示されます。本画面には、「Surveillance Topology」（サーベイランストポロジ）」タブと「Device Information（デバイス情報）」タブが存在します。

Surveillance Topology（サーベイランストポロジ）

「Surveillance Topology」タブでは、スイッチに接続されたデバイスの情報など、サーベイランストポロジ（図）が表示されます。他の画面を開いている場合、「機能一覧」の機種名をクリックし、本画面を表示することが可能です。

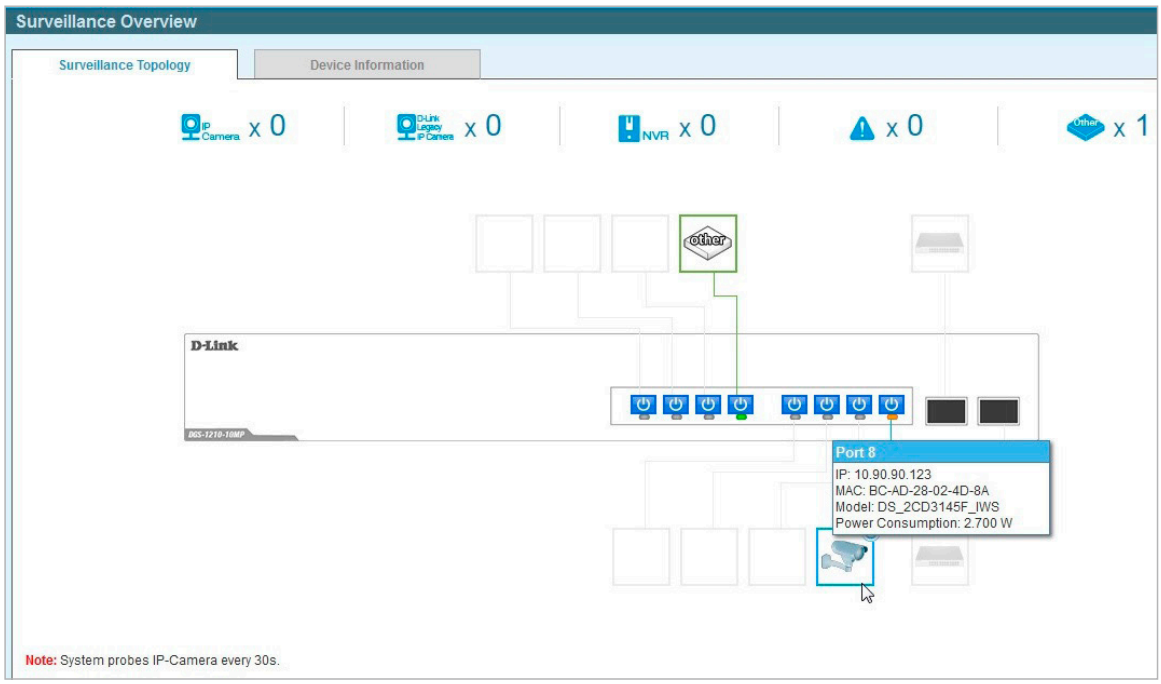


図 5-5　Surveillance Topology 画面

ページ上部に IP カメラ、NVR やその他の接続機器の数が表示されます。

補足　サーベイランストポロジでは、各ポートに接続されているデバイスに関する詳細情報が表示されます。識別されたデバイスのアイコンにマウスカーソルを合わせると、デバイスの数、デバイスの種類、IP アドレス、電力消費、リンクスピード、エラーなどの情報が表示されます。

補足　PoE 対応製品（DGS-1210-10MP/28MP）の場合、各ポートの電源マークをクリックすることで、PoE 給電のオン / オフを切り替えることもできます。

注意　スイッチを再起動すると、PoE 接続されている IP カメラが検出されません。再起動完了後に PoE を有効化する必要があります。

以下の項目が表示されます。

アイコン	説明
上部機器アイコン	
IP Camera	検出された IP カメラ数です。
D-Link Legacy IP Camera	検出された D-Link レガシー IP カメラ数です。
NVR	検出された NVR 数です。
	システムで発生している警告の数です。「Surveillance Log」（サーベイランスログ）と「Health Diagnostic」（正常性診断）で詳細な情報について確認できます。

アイコン	説明
	スイッチに接続している ONVIF をサポートしていない不明機器の数です。
接続機器アイコン	
	ONVIF をサポートしている IP カメラです。
	ONVIF をサポートしていない IP カメラ、NVR、その他のサーベイランス機器です。
	ONVIF をサポートしている IP カメラ（複数）です。
	ONVIF をサポートしている NVR です。 IP カメラからのサーベイランスストリーム上に接続している機器は全て NVR と認識されます。
	ONVIF をサポートしている NVR（複数）です。
	ONVIF をサポートしている NVR と IP カメラです。
	ONVIF をサポートしている NVR と IP カメラ（複数）です。
	ONVIF をサポートしている NVR（複数）と IP カメラです。
	ポートがアップリンクポートとして設定されており、リンクアップしています。
	ポートがアップリンクポートとして設定されていますが、リンクアップしていません。

各機器アイコンの PoE 電力需給状況について以下のように表示されます。

アイコン	説明
	機器は操作可能ですが PoE 電力供給は行われていません。
	機器は操作可能で PoE 電力供給が行われています。「PD Alive」機能が使用可能です。
	ポート、または機器にエラーが発生しており使用できなくなっています。

ポート状況とリンクステータスについて以下のように表示されます。

アイコン	説明
	ポートがダウンしています。
	ポートが 1 G でリンクアップしています。
	ポートが 10/100M でリンクアップしています。

各ポートの PoE 有効 / 無効状況について以下のように表示されます。

アイコン	説明
	ポートの PoE が有効です。
	ポートの PoE が無効です。

■ PoE の設定について

各ポートの PoE 電力の有効 / 無効についてはアイコンをクリックすることで切り替えることが可能です。初期値では有効です。以下のダイアログが表示されるので、「Apply」をクリックします。

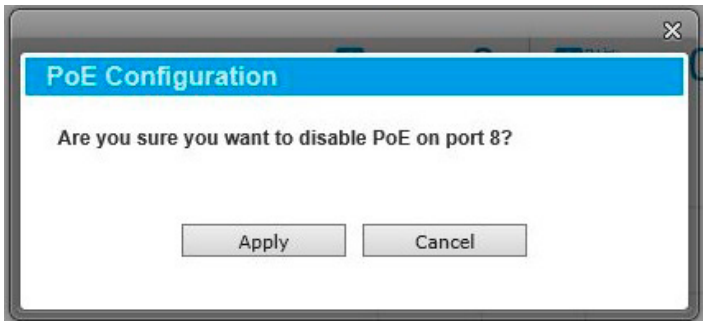


図 5-6　　PoE 設定画面

補足　ツールバーの「Help」画面を開き、アイコンの説明を確認することができます。

補足　システムは 30 秒毎に IP カメラの探索を実施します。

トポロジに表示されているデバイスのアイコンにカーソルを置くと、デバイスについての情報が表示されます。

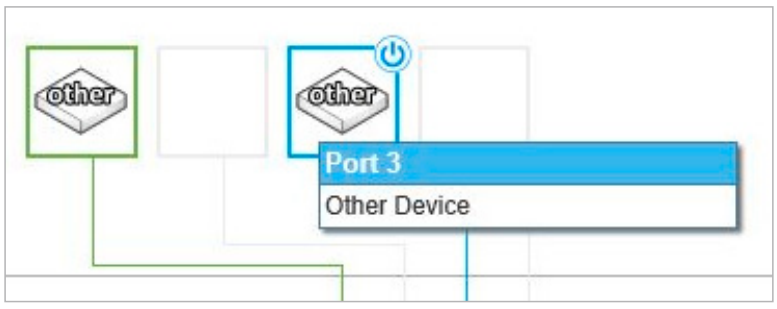


図 5-7　　機器情報画面

さらにデバイスアイコンをクリックすると、「PD Alive」について次の画面が表示されます。

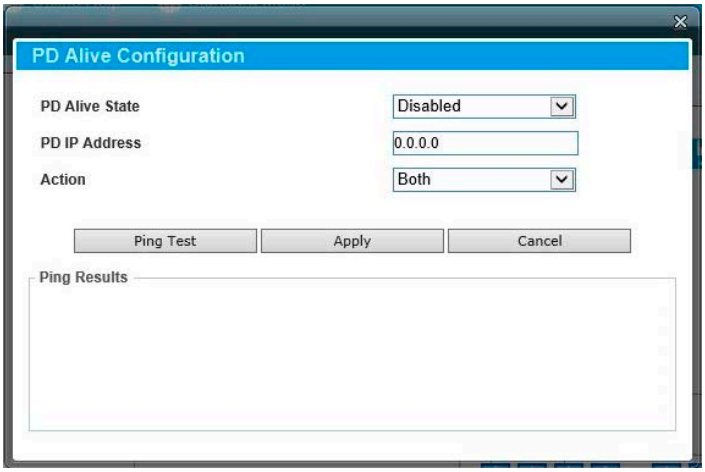


図 5-8　PD Alive Configuration 画面

以下の項目が表示されます。

項目	説明
PD Alive State	「PD Alive」を有効 / 無効に指定します。
PD IP Address	PD（PoE 機器）の IP アドレスを指定します。
Action	実行する動作を指定します。 • 「Reboot」- PoE ポートのリセット（PoE のオフ / オン）を実行します。 • 「Notify」- ログとトラップを管理者へ送信します。 • 「Both」- ログとトラップを管理者へ送信し、PoE ポートのリセット（PoE のオフ / オン）を実行します。

「Apply」をクリックし、設定を適用します。
「Cancel」をクリックすると、設定は適用されず破棄されます。

「Ping Test」をクリックし、Ping を実行して PD の有効性を確認します。次の画面が表示されます。

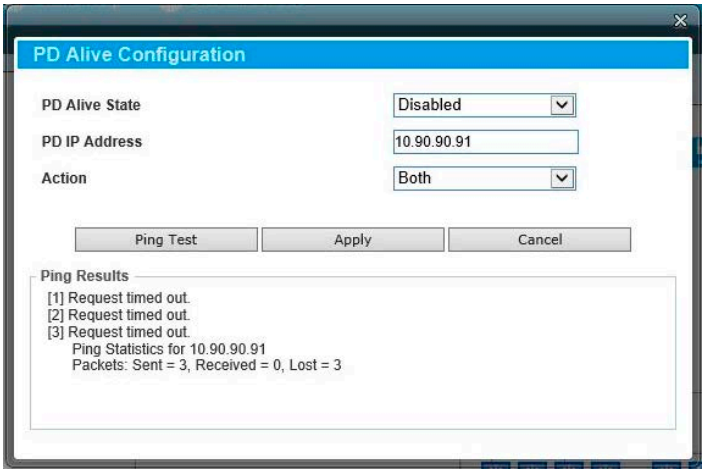


図 5-9　PD Alive Configuration (Ping Result) 画面

注意　スイッチは ONVIF トラフィックをサーベイランス機器のステータスのモニタに使用しますが、他社製機器だと ONVIF 基準を準拠していない場合があります。「検出されない」など問題が発生した場合、サーベイランス機器の ONVIF 準拠の有無を確認してください。

Device Information（デバイス情報）

「Device Information」タブでは、3 つのセクション（デバイス情報、PoE 使用情報、帯域使用情報）が表示されます。
他の画面を開いている場合、「機能一覧」の機種名をクリックし、「Device Information」タブを選択して本画面を表示することが可能です。

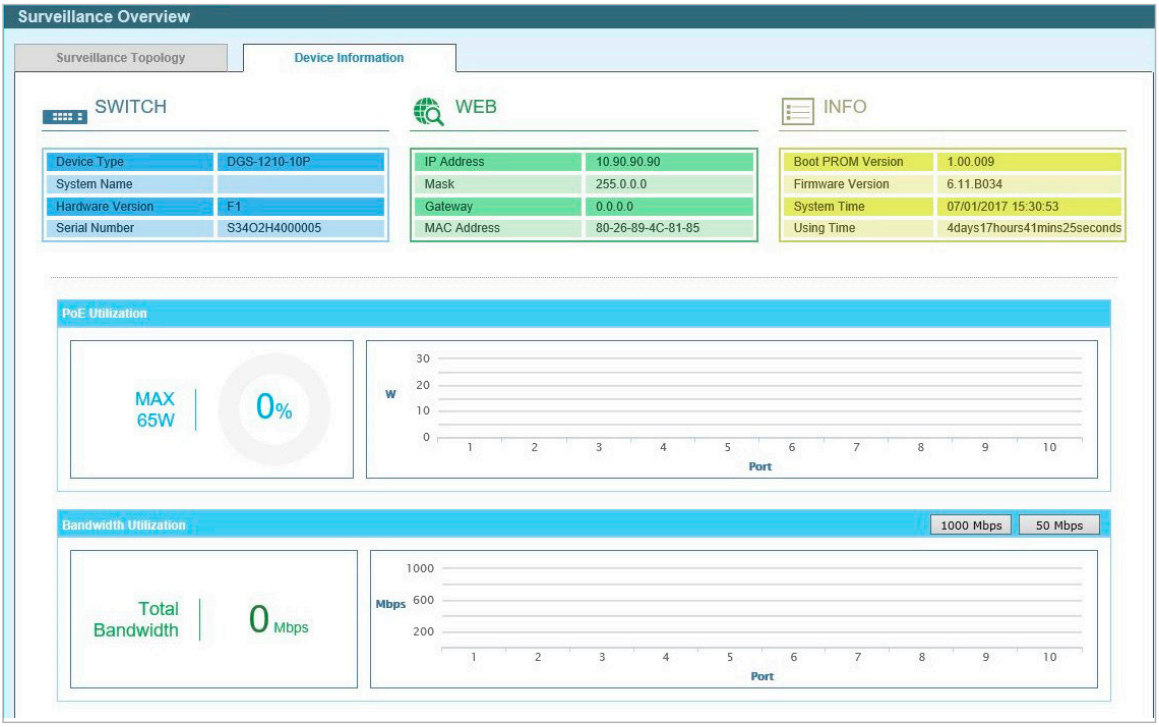


図 5-10　Device Information 画面

以下の項目が表示されます。

表示項目	説明
SWITCH	
Device Type	機種名を表示します。
System Name	システム名を表示します。
Hardware Version	デバイスのハードウェアバージョンを表示します。
Serial Number	デバイスのシリアル番号を表示します。
WEB	
IP Address	デバイスに割り当てられた IP アドレスを表示します。
Mask	デバイスに割り当てられたサブネットマスクを表示します。
Gateway	デバイスに割り当てられたデフォルトゲートウェイを表示します。
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。
INFO	
Boot PROM Version	デバイスのブートバージョンを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
System Time	最後のデバイスリセットからの経過時間を表示します。日、時、分、秒の形式で表示します。
Using Time	使用している時間を表示します。日、時、分、秒の形式で表示します。
PoE Utilization（DGS-1210-10MP/28MP のみ）	
PoE の使用状況を表示します。 左側には PoE 最大供給電力と現在の合計使用率が表示され、右側にはポート毎の使用量がグラフで表示されます。	
Bandwidth Utilization	
帯域（速度）使用状況を表示します。 左側には全ポートにおける受信トラフィックの合計量が表示されます。右側にはポート毎の受信トラフィック帯域使用量がグラフで表示されます。 グラフのスケールは「1000Mbps」「50Mbps」をクリックして変更することができます。 補足 「1000Mbps」をクリックすると、「Bandwidth Utilization」に表示される最大帯域が 1Gbps となります。「50Mbps」をクリックすると、「Bandwidth Utilization」に表示される最大帯域が 50Mbps となります。	

Port Information（ポート情報）

各ポートのステータスを表示します。スループット、PoE ステータス、ループ検知ステータス、ケーブル長、電力消費、IP カメラ /NVR/ その他のデバイスの接続台数などが表示されます。各アイコンにマウスカーソルを合わせると、項目名が表示されます。

1. 機能一覧から「Port Information」をクリックします。

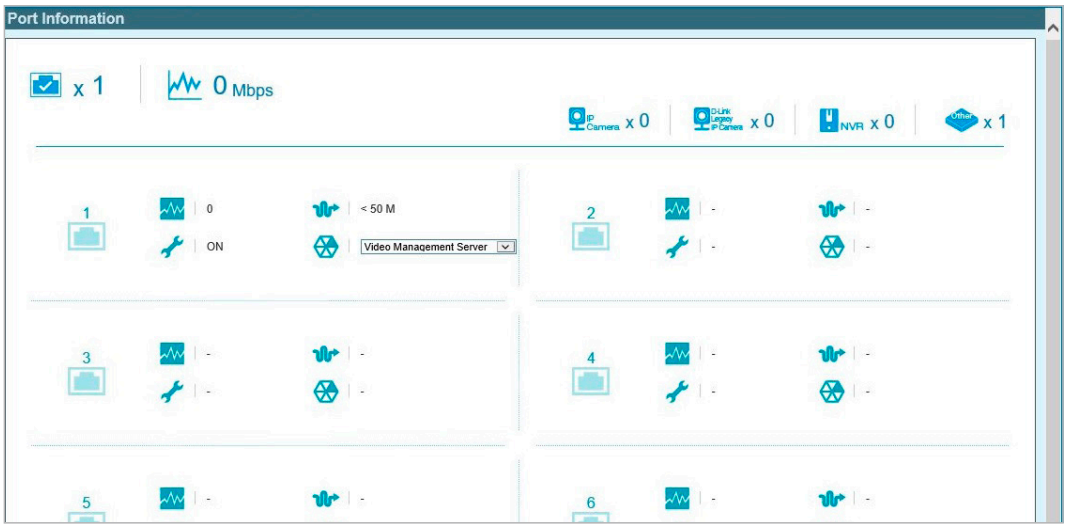


図 5-11　Port Information 画面

以下のアイコン、項目が表示されます。

アイコン	説明
上部機器アイコン	
	現在アクティブなポート数です。
	全ポートの総インバウンドスループットです。
	検出された IP カメラ数です。
	検出された D-Link レガシー IP カメラ数です。
	検出された NVR 数です。
	スイッチに接続している ONVIF をサポートしていない不明機器の数です。
各ポート情報	
	ポート番号です。
	対象ポートの総インバウンドスループット（Mbps）です。
	接続しているケーブルのケーブル長です。
	ポートのループバック検出状況について表示します。ループが検出されると、アイコンは「Health Diagnostics」ページへのリンクアイコンへと変化します。
	「Group Details」（グループ詳細）についてのページです。ONVIF 対応機器が対象ポートに検出された場合、アイコンは「Group Details」へのリンクアイコンへと変化します。ONVIF 非対応機器の場合、ドロップダウンが表示され、機器の種類を選択することが可能です。

IP-Camera Information（IP-Camera 情報）

スイッチに接続されているカメラの情報を表示します。ポート番号、デバイスの種類、スループット、IP アドレス、その他の情報（ポートの説明など）、電力消費量、位置情報が表示されます。各アイコンにマウスカーソルを合わせると、項目名が表示されます。

1. 機能一覧から「IP-Camera Information」をクリックします。

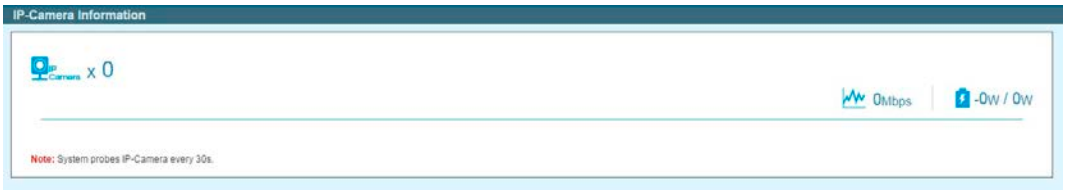


図 5-12　IP-Camera Information 画面

以下のアイコン、項目が表示されます。

アイコン	説明
上部アイコン	
	検出された IP カメラ数です。
	全ポートの総インバウンドスループットです。
	ポートの PoE 電力消費量を表示します。
各機器情報	
	ポート番号です。
	機器のアイコンまたは画像が表示されます。D-Link 以外の ONVIF 対応カメラでは、一般的な画像が表示されます。D-Link の ONVIF 対応カメラの場合、対象機器の画像が表示されます。
	対象ポートの総インバウンドスループット（Mbps）です。
	IP カメラの設置場所です。
	IP カメラの IP アドレスです。
	ポートの PoE 電力消費量を表示します。
	機器の概要を表示します。アイコンをクリックして概要を編集します。入力完了後、アイコンをクリックして設定を保存します。

NVR Information（NVR 情報）

スイッチに接続された NVR の情報を表示します。ポート番号、スループット、IP アドレス、NVR に接続しているカメラの情報（グループ名、カメラの合計数、ポート番号、IP アドレス）が表示されます。各アイコンにマウスカーソルを合わせると、項目名が表示されます。

1. 機能一覧から「NVR Information」をクリックします。

図 5-13　NVR Information 画面

以下のアイコン、項目が表示されます。

アイコン	説明
上部アイコン	
	検出された NVR 数です。
	全ポートの総インバウンドスループットです。
各機器情報	
	ポート番号です。
	機器のアイコンまたは画像が表示されます。D-Link の ONVIF 対応機器の場合、対象機器の画像が表示されます。
	対象ポートの総インバウンドスループット（Mbps）です。
	NVR の IP アドレスです。
	機器の概要を表示します。  アイコンをクリックして概要を編集します。入力完了後、  アイコンをクリックして設定を保存します。
	機器が所属しているグループ番号です。同じ NVR によって管理されている機器は同じグループ番号になります。番号は連番で指定されます。NVR「1」はグループ番号「1」になります。NVR が削除されると、グループ番号は自動的に変更されます。（NVR1 が削除されるとグループ番号「2」は自動的にグループ「1」になります。）
	NVR に管理されている ONVIF 対応の IP カメラの数です。
	グループに属する IP カメラの情報です。ポート番号や IP アドレスなどが表示されます。

PoE Information（PoE 情報）（DGS-1210-10MP/28MP のみ）

各ポートの Power-over-Ethernet（PoE）使用情報を表示します。ポート番号、PoE ステータス、正常性ステータス、PoE 給電可能電力量、消費電力量が表示されます。各アイコンにマウスカーソルを合わせると、項目名が表示されます。

1. 機能一覧から「PoE Information」をクリックします。

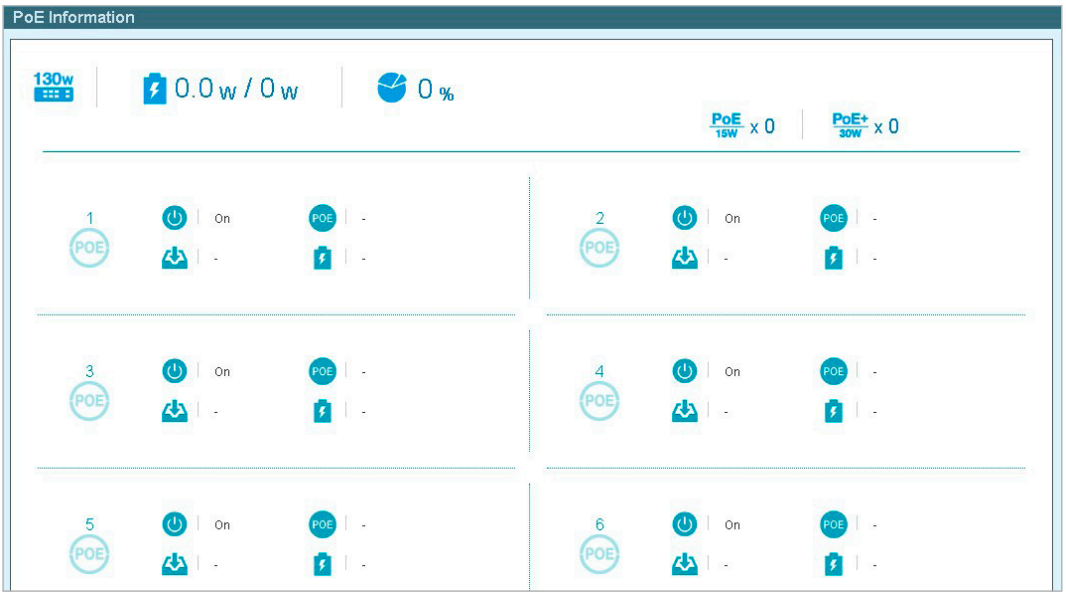


図 5-14　PoE Information 画面

以下のアイコン、項目が表示されます。

アイコン	説明
上部アイコン	
130w	PoE の給電可能電力です。
	PoE 電力消費量を表示します。
	PoE 給電の使用率について表示します。
PoE 15W	15w の PoE 給電を受ける機器数です。
PoE+ 30W	30w の PoE 給電を受ける機器数です。
各機器情報	
POE	ポート番号です。
	ポートの PoE ステータス（PoE の有効 / 無効）です。
POE	ポートの最大 PoE 供給電力です。
	PoE の状態です。正常に供給されている場合は「Delivering」と表示されます。何らかのエラーを検出すると、問題の概要表示と「Health Diagnostic」へのリンクになります。
	ポートの PoE 電力消費量（使用電力 / 供給可能電力）を表示します。

PoE Scheduling（PoE スケジューリング）（DGS-1210-10MP/28MP のみ）

PoE ポートに電力が供給される時間を設定します。これにより、デバイス未使用時の電力を抑制したり、セキュリティ面の強化として、ビジネス時間外の無線アクセスを遮断したりすることが可能です。スケジュール名、開始時間、終了時間、適用ポートを指定することができます。

1. 機能一覧から「PoE Scheduling」をクリックします。

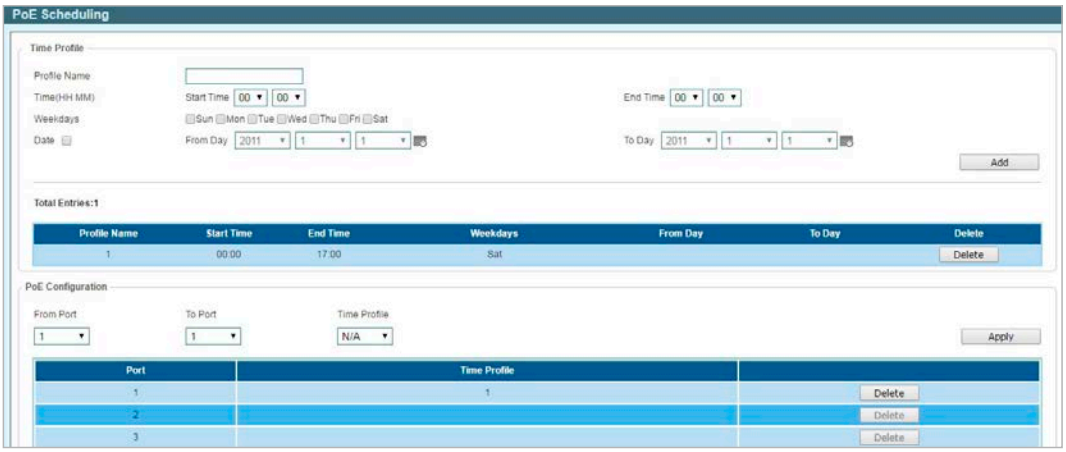


図 5-15　PoE Scheduling 画面

■ 新しいタイムプロファイルの作成

1. 「Time Profile」セクションで、以下の項目を設定します。

項目	説明
Profile Name	スケジュール名を設定します。
Time (HH MM)	開始時間と終了時間を指定します。
Weekdays	曜日を指定します。
Date	チェックボックスにチェックを入れ、「From Day」（開始日）/「To Day」（終了日）を指定します。

2. 「Add」をクリックしてタイムプロファイルを作成します。

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。

■ タイムプロファイルの適用

1. 「PoE Configuration」セクションで、以下の項目を設定します。

項目	説明
From Port / To Port	設定対象のポート範囲を指定します。
Time Profile	適用するタイムプロファイルを指定します。

2. 「Apply」をクリックして設定を有効にします。

設定内容を削除するには、「Delete」をクリックします。

Time（時刻設定）

スイッチの時刻や SNTP サーバの設定を行います。

Clock Settings（時刻設定）

スイッチの時刻を設定します。

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

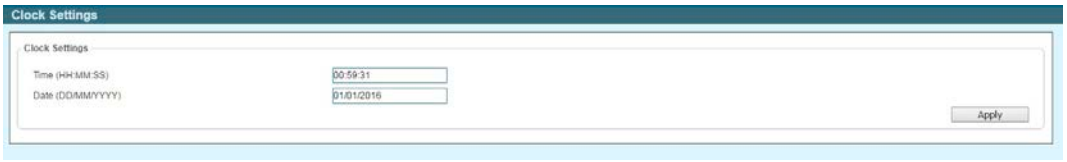


図 5-16　Clock Settings 画面

2. 以下の項目を設定します。

項目	説明
Time (HH:MM:SS)	システムの時刻を「HH:MM:SS」のフォーマットで設定します。
Date (DD/MM/YYYY)	システムの日付を「DD:MM:YYYY」のフォーマットで設定します。

3. 「Apply」をクリックして設定を有効にします。

SNTP Settings（SNTP 設定）

外部の時刻サーバを設定します。Simple Network Time Protocol（SNTP）は NTP プロトコルの簡易版であり、ネットワーク上の時刻サーバと同期してシステムの時刻を調整します。

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

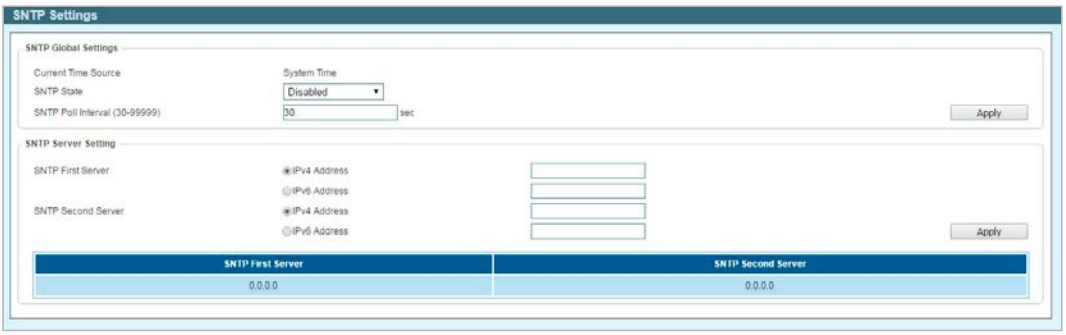


図 5-17　SNTP Settings 画面

2. 「SNTP Global Settings」セクションで、以下の項目を設定します。

項目	説明
SNTP State	SNTP 機能を「Enabled」（有効）または「Disabled」（無効）にします。
SNTP Poll Interval	ポーリング間隔を指定します。 • 選択可能範囲：30-99999（秒） • 初期値：30（秒）

3. 「Apply」をクリックして設定を有効にします。

■ SNTP サーバを設定する場合

1. 「SNTP Server Settings」セクションで、以下の項目を設定します。

項目	説明
SNTP First Server	SNTP サーバの IPv4/IPv6 アドレスを設定します。
SNTP Second Server	セカンダリ SNTP サーバの IPv4/IPv6 アドレスを設定します。

2. 「 Apply」をクリックして設定を有効にします。

Surveillance Settings（サーベイランス設定）

サーベイランス VLAN の設定を行います。本設定は IP カメラ（IPC）、Network Video Recorder（NVR）用の VLAN であり、ネットワーク上のサーベイデバイスを管理するためにも使用されます。

1. 機能一覧から「Surveillance Settings」をクリックします。

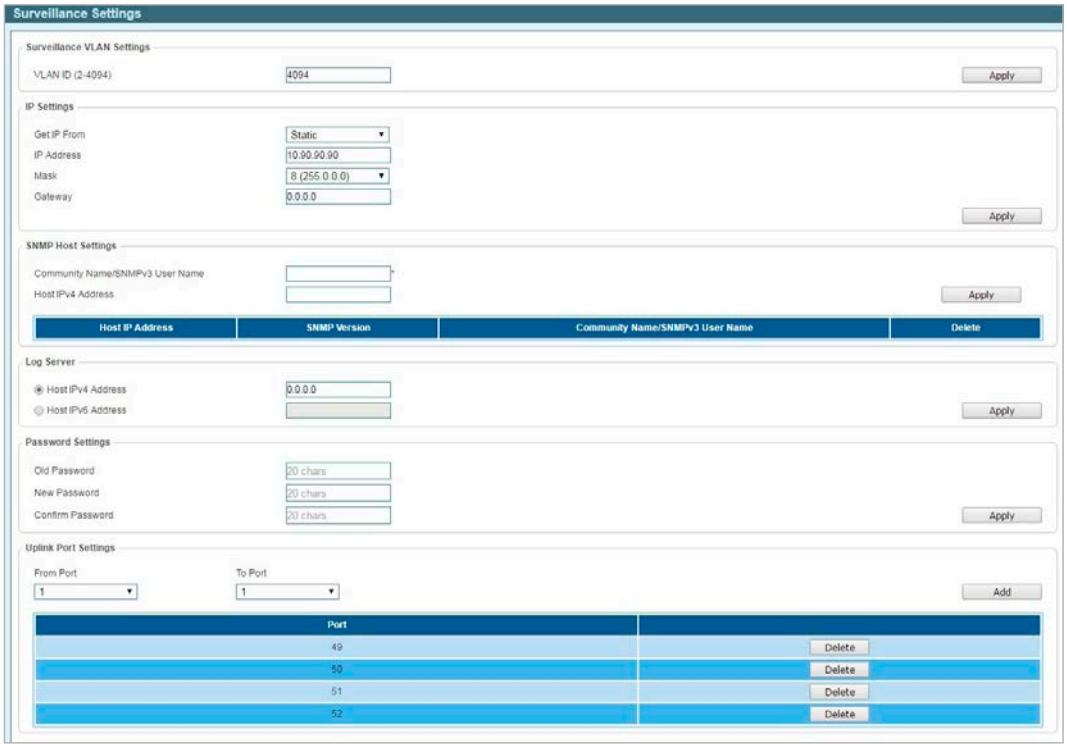


図 5-18　Surveillance Settings 画面

以下の項目が表示されます。

項目	説明
Surveillance VLAN Settings	
VLAN ID	サーベイランス VLAN の ID を指定します。 • 選択可能範囲：2-4094（秒）
IP Settings	
Get IP From	サーベイランス VLAN の管理 IP の種類を指定します。 • 選択肢：「Static」「DHCP」「BOOTP」 「Static」を指定した場合、以下の項目の指定を行います。
IP Address	サーベイランス VLAN の管理 IP アドレスを手動で指定します。
Mask	サーベイランス VLAN の管理 IP アドレスのマスクを指定します。
Gateway	サーベイランス VLAN のゲートウェイを指定します。
SNMP Host Settings	
Community Name/SNMPv3 User Name	コミュニティ名または SNMPv3 のユーザ名を入力します。
Host Ipv4 Address	スイッチから SNMP トラップを受信する SNP Network Management Server（NMS）の IPv4 アドレスを指定します。 補足　設定を削除するには「Delete」をクリックします。
Log Server	
Host IPv4 Address	スイッチから Syslog メッセージを受信する Syslog NMS の IPv4 アドレスを指定します。
Host IPv6 Address	スイッチから Syslog メッセージを受信する Syslog NMS の IPv6 アドレスを指定します。
Password Settings	
Old Password	スイッチに Web UI 経由でアクセスする際に使用する現在のパスワード（最大 20 文字）を入力します。
New Password	スイッチに Web UI 経由でアクセスする際に使用する新しいパスワード（最大 20 文字）を入力します。
Confirm Password	確認のため、新しいパスワードをもう一度入力します。
Uplink Port Settings	
From Port / To Port	アップリンクポートの範囲を指定します。ほかのスイッチでサーベイランス VLAN に接続する際に使用します。 「From Port」で開始ポート、「To Port」で終了ポートを指定します。「Delete」で指定ポートを解除することが可能です。

各項目で「Apply」をクリックして設定を有効にします。

Surveillance Log（サーベイランスログ）

スイッチで生成された Syslog メッセージの一覧を表示します。「Surveillance Setting」セクションの Syslog サーバ設定に基づき、ローカルに保存または外部ログサーバに送信されます。メッセージ一覧は最新のメッセージから順に表示されます。

1. 機能一覧から「Surveillance Log」をクリックします。

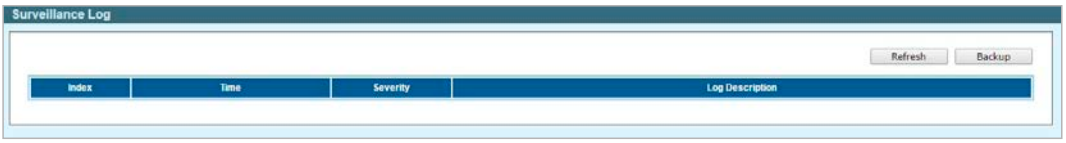


図 5-19　Surveillance Log 画面

テーブルの情報を更新するには「Refresh」をクリックします。
「Backup」をクリックすると、Syslog メッセージをテキスト形式ファイルとして保存します。

Health Diagnostic（正常性診断）

ポートステータスの概要を表示します。ポート番号、ループ検知ステータス、ケーブルリンクステータス、PoE ステータス、Tx/Rx エラーカウンタ、検出されたサーベイランスデバイスの台数が表示されます。サーベイデバイスの台数をクリックすると、「Group Details」画面に遷移します。画面の情報は 30 秒毎に自動で更新されます。

1. 機能一覧から「Health Diagnostic」をクリックします。

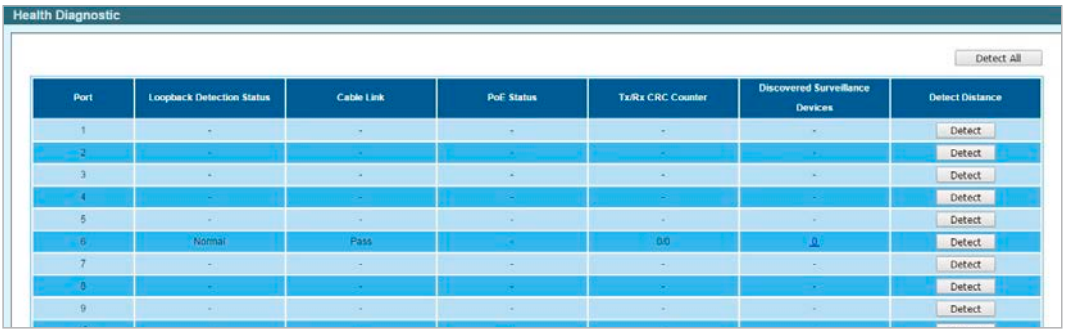


図 5-20　Health Diagnostic 画面

■ ケーブル長の検出

スイッチの全ポートでケーブル長を検出するには「Detect All」をクリックします。
スイッチの特定のポートでケーブル長を検出するには、該当ポートの「Detect」をクリックします。

■ ポートで検出されたデバイスの情報

ポートに接続されたデバイスの情報を確認するには、「Discovered Surveillance Devices」項目のリンクをクリックします。
以下の画面が表示されます。

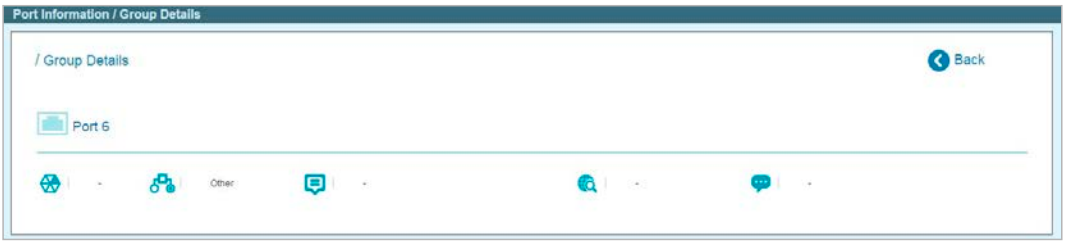


図 5-21　Group Details 画面

前の画面に戻るには「Back」をクリックします。

Wizard（ウィザード）

ツールバーの「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。

Tools（ツール）

Tools(ツール) の設定項目

Reset System（システムリセット）

サーベイランス VLAN の安全な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」>「Reset System」の順にメニューをクリックします。
2. 以下のオプションを選択します。
   ・Warning!! The Switch will be reset to its factory defaults, and then will reboot. - スイッチのコンフィグを工場出荷時の設定に戻します。
   ・Warning!! The Switch will be reset to its factory defaults except IP address, and then will reboot. - スイッチのコンフィグを IP アドレスを除いて工場出荷時の設定に戻します。

図 5-22　Reset System 画面

3. 「Apply」をクリックします。
4. 「OK」をクリックします。

図 5-23　Reset System 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. 現在の設定を保存する場合は「YES」、保存しない場合は「NO」を選択します。
3. 「Reboot」をクリックします。

図 5-24　Reboot Device 画面

4. 「OK」をクリックすると、デバイスが再起動します。

図 5-25　Reboot Device 確認画面

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。

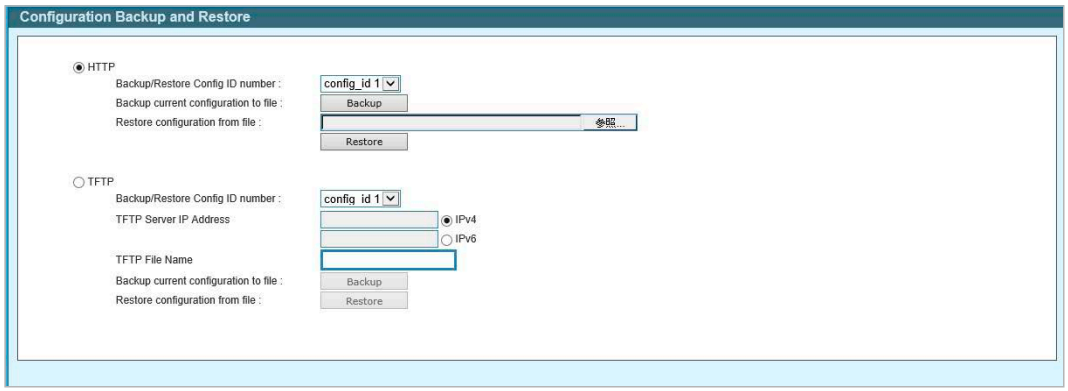


図 5-26　Configuration Backup and Restore 画面

3. 以下の項目を設定します。

プロトコル	説明
HTTP	**バックアップ方法** • バックアップ対象のコンフィグ ID を「config_id 1」または「config_id 2」から指定します。 • 「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** • リストア対象のコンフィグ ID を「config_id 1」または「config_id 2」から指定します。 • 「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** • バックアップ対象のコンフィグ ID を「config_id 1」または「config_id 2」から指定します。 • 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 Address」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** • リストア対象のコンフィグ ID を「config_id 1」または「config_id 2」から指定します。 • 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 Address」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。

「Restore」をクリックした場合、以下の画面が表示されます。「Continue」をクリックします。

図 5-27　Restore 確認画面

注意 現在のコンフィグとは別の ID を指定して適用した場合、Configuration Information 画面でブート ID を指定してください。

注意 コンフィグレーションの復元後、以下の手順でスイッチを再起動します。
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。

手順

1. 「Tools」>「Reboot Device」の順にメニューをクリックします。
2. 「Do you want to save the settings」の項目で「NO」を選択します。
3. 「Reboot」をクリックします。
4. 「Are you sure you want to reboot device?」メッセージのポップアップウィンドウにおいて、「OK」をクリックします。

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。

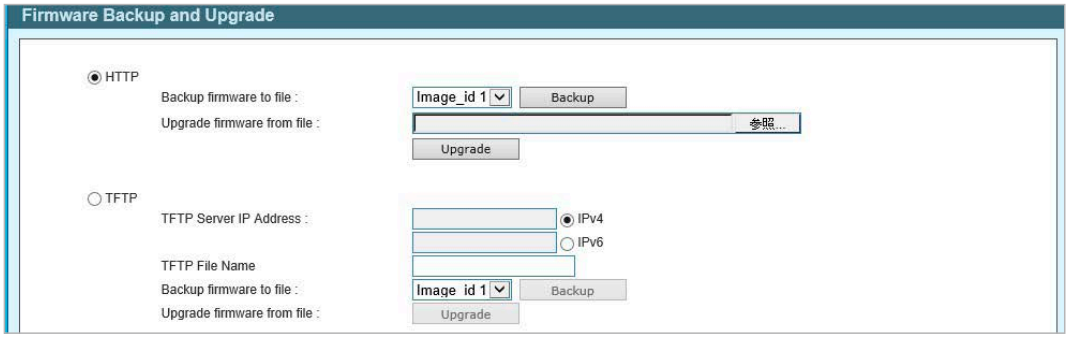


図 5-28　Firmware Backup & Upgrade 画面

3. 以下の項目を設定します。

プロトコル	説明
HTTP	**バックアップ方法** • バックアップ対象のイメージ ID を「image_id 1」または「image_id 2」から指定します。 • 「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** • バックアップ対象のイメージ ID を「image_id 1」または「image_id 2」から指定します。 • 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 Address」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 Address」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。

注意 R6.10.B010 以降のバージョンでは、アップグレード時にイメージ ID を指定できません。新しいイメージファイルは現在のイメージ ID とは別の ID に適用されます。

Firmware Information（ファームウェア情報）

ファームウェアの情報を表示します。
次回スイッチが起動した際にブートアップを行うコンフィグファイルとイメージファイルを選択することができます。

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

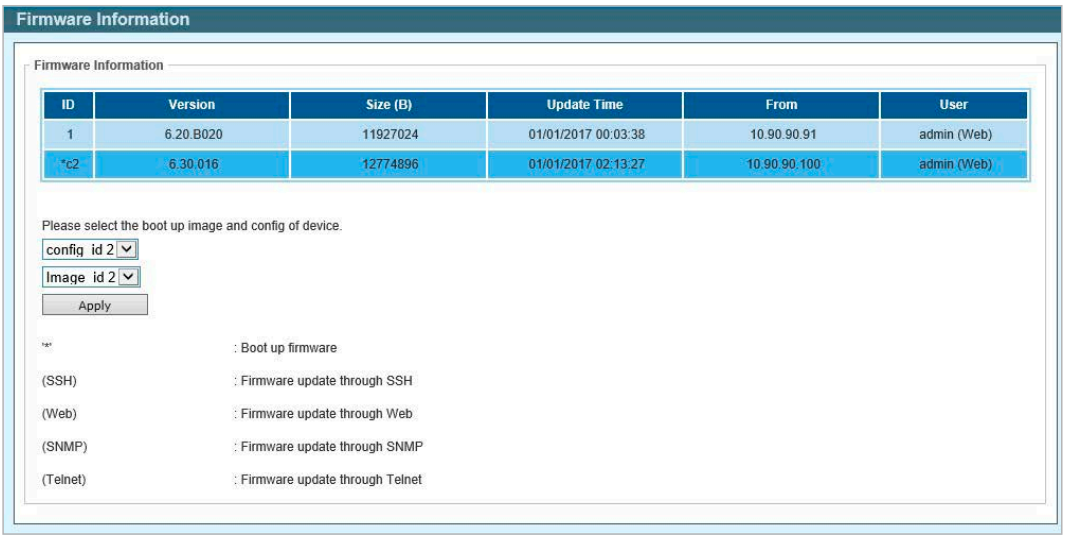


図 5-29　Firmware Information 画面

2. コンフィグ ID とイメージ ID を選択します。
3. 「Apply」をクリックし、設定を有効にします。

Flash Information（フラッシュメモリ情報）

フラッシュメモリの詳細情報を表示します。

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

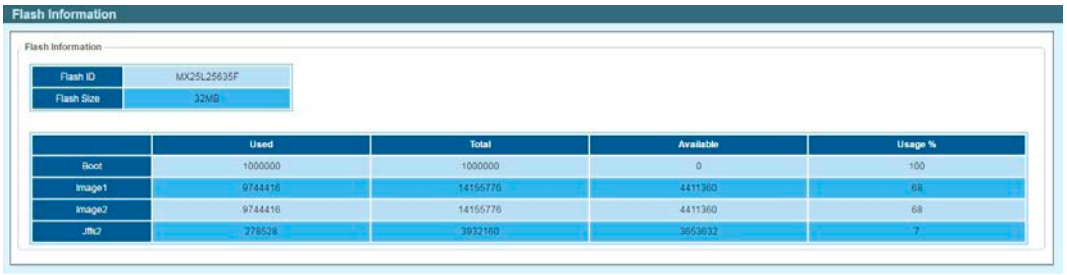


図 5-30　Flash Information 画面

Save（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 Configuration ID 1 または Configuration ID 2 に保存します。また、ログエントリをローカルドライブに保存することも可能です。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。

1. ツールバーの「Save」をクリックします。
2. 「config_id_1」または「config_id_2」を選択し、「Save Config」をクリックします。

図 5-31　Save Configuration 画面

3. 「Continue」をクリックします。

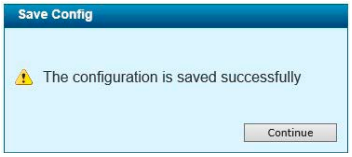


図 5-32　Save Configuration 画面

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。

現在の設定をローカルディスクに保存するには、「Backup Log」をクリックします。

Help（ヘルプ画面）

ツールバーの「Help」をクリックすると、以下のヘルプ画面が表示されます。

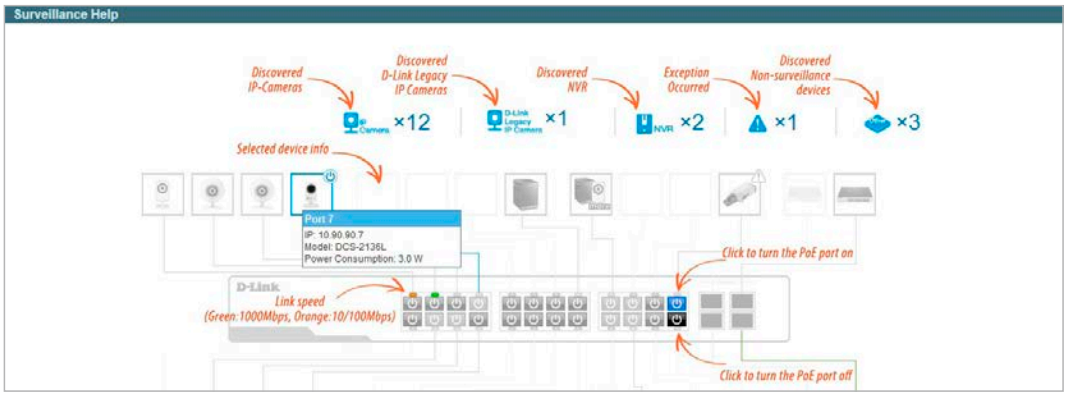


図 5-33　Surveillance Help - Diagram 画面

図 5-34　Surveillance Help - Table 画面

Online Help（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 5-35　User Guide 画面

Standard Mode（スタンダードモード）

ツールバーの「Standard Mode」をクリックすると、スタンダードモードの Web UI 表示に切り替わります。

補足　複数のセッションが存在する場合、スタンダードモードへの切り替えを行うことはできません。

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 {<ipaddr>| <ipv6addr>} <path_filename (64)> | cfg_fromTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> config_id <integer (1-2)>}
download profile_fromTFTP	{<ip_addr>| <ipv6_addr>} <string>
upload	{firmware_toTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> image_id <integer 1-2> | cfg_toTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> config_id <integer (1-2)>}
config firmware	image_id <integer (1-2)> boot_up
config configuration	config_id <integer (1-2)> {delete | boot_up}
config ipif	<ipif_name> { ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp | bootp }
config ipif	<ipif_name> { ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client [enable | disable] }
logout	
ping	<ip_addr>
ping6	<ipv6_addr>
reboot	
reset config	
show boot_file	
show firmware information	
show flash information	
show ipif	[ipif_name]
show switch	
show route	{ipv4 | ipv6}
show switch	
show ddpClient	
show nmsManaged	
enable ddpClient	
enable nmsManaged	
disable ddpClient	
disable nmsManaged	
config account admin password	<passwd>
save	[config config_id <integer (1-2)>]
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-1210-20> ?
USEREXEC commands :
  config account admin password <passwd>
  config configuration config_id <integer (1-2)> {delete | boot_up }
  config firmware image_id <integer (1-2)> boot_up
  config ipif <ipif_name> { ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp |
bootp }
  config ipif <ipif_name> { ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client {enable | disable}}
  debug info
  disable ddpClient
  disable nmsManaged
  download profile_fromTFTP {<ip_addr>| <ipv6_addr>} <string>
  download {firmware_fromTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> | cfg_fromTFTP {<ipaddr>|
<ipv6addr>} <p
ath_filename (64)> config_id <integer (1-2)>}
  enable ddpClient
  enable nmsManaged
  logout
  ping <ip_addr>
  ping6 <ipv6addr>
  reboot
  reset config
  save [config config_id <integer (1-2)> ]
  show boot_file
  show ddpClient
  show firmware information
  show flash information
  show ipif [<ipif_name>]
  show nmsManaged
  show route { ipv4 | ipv6 }
  show switch
  upload {firmware_toTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> image_id <integer 1-2> | cfg_
toTFTP {<ipaddr
>| <ipv6addr>} <path_filename (64)> config_id <integer (1-2)>}
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 {<ipaddr>| <ipv6addr>} <path_filename (64)> | cfg_fromTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> config_id <integer (1-2)>}

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 64>	ファームウェアファイルまたはコンフィグレーション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。
config_id <integer 1-2>	コンフィグレーションをインストールする場合、設定対象のコンフィグ ID を指定します。

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 firmware.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。

download profile_fromTFTP

注意　Nuclias Connect による管理は未サポートです。

目的

TFTP サーバから Nuclias Connect のネットワークファイルをダウンロードします。

構文

download profile_fromTFTP {<ip_addr>| <ipv6_addr>} <string>

説明

TFTP サーバから Nuclias Connect のネットワーク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。
<ip_addr>	TFTP サーバの IPv4 アドレスを指定します。
<ipv6_addr>	TFTP サーバの IPv6 アドレスを指定します。
<string>	ネットワークファイルを指定します。

制限事項

なし

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_toTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> image_id <integer 1-2> | cfg_toTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> config_id <integer (1-2)>}

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 64>	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。
image_id <integer 1-2>	アップロード対象のイメージ ID を指定します。
config_id <integer 1-2>	アップロード対象のコンフィグ ID を指定します。

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_toTFTP 10.90.90.100 runtime image_id 1

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

config firmware

目的

ファームウェアを削除またはブートアップに指定します。

構文

config firmware image_id <integer (1-2)> {delete | boot_up}

説明

ファームウェアを削除またはブートアップに指定します。

パラメータ

パラメータ	説明
<integer (1-2)>	設定対象のイメージ ID を指定します。
{delete | boot_up}	指定したイメージファイルを削除する場合は「delete」、ブートアップファイルとして指定する場合は「boot_up」を指定します。

制限事項

なし

使用例

スイッチのブートアップイメージファイルとしてイメージ ID「1」を指定します。

```
DGS-1210-52> config firmware image_id 1 boot_up
DGS-1210-52>
```

config configuration

目的

コンフィグファイルを設定します。

構文

config configuration config_id <integer (1-2)> {delete | boot_up}

説明

コンフィグファイルを削除またはブートアップファイルとして指定します。

パラメータ

パラメータ	説明
config_id <integer (1-2)>	設定対象のコンフィグ ID を指定します。
{delete | boot_up}	指定したコンフィグファイルを削除する場合は「delete」、ブートアップファイルとして指定する場合は「boot_up」を指定します。

制限事項

なし

使用例

スイッチのブートアップコンフィグファイルとしてコンフィグ ID「1」を指定します。

```
DGS-1210-52> config configuration config_id 1 boot_up
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 <ipif_name> { 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
<ipif_name>	設定対象の IP インタフェース名を指定します。
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 d
isconnect.
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 <ipif_name> { 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
<ipif_name>	設定対象の IP インタフェース名を指定します。
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。一つの IP インタフェースに対して複数の IPv6 アドレスを設定することが可能です。 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

ネットワーク上の他の IP アドレスに到達可能かどうかをチェックします。スイッチとターゲットの IP デバイス間に物理パスが存在する場合、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

ネットワーク上の他の IP アドレスに到達可能かどうかをチェックします。スイッチとターゲットの IP デバイス間に物理パスが存在する場合、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>
```

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。

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 boot_file

目的

スイッチのブートファイル情報を表示します。

構文

show boot_file

説明

スイッチのブートファイル情報を表示します。

制限事項

なし

使用例

スイッチのブートファイル情報を表示します。

```
DGS-1210-52> show boot_file
Bootup Firmware : image_1
Bootup Configuration : config_1
DGS-1210-52>
```

show firmware information

目的

スイッチのファームウェア情報を表示します。

構文

show firmware information

説明

スイッチのファームウェア情報を表示します。

制限事項

なし

使用例

スイッチのファームウェア情報を表示します。

```
DGS-1210-52> show firmware information
IMAGE ONE:
Version      : 6.10.B010
Size         : 12288000 Bytes
Updated Time : 01/01/2017 00:06:15
From         : 10.90.90.90
User         : Anonymous (unknown)

IMAGE TWO:
Version      : 6.00.011
Size         : 12288000 Bytes
Updated Time : 01/01/1970 00:00:00
From         : 10.90.90.90
User         : Anonymous (unknown)

DGS-1210-52>
```

show flash information

目的

スイッチのフラッシュメモリ情報を表示します。

構文

show flash information

説明

スイッチのフラッシュメモリ情報を表示します。

制限事項

なし

使用例

スイッチのフラッシュメモリ情報を表示します。

```
DGS-1210-52> show flash information
Flash ID    : MX25L25635F
Flash size  : 32MB

Partition      Used           Available      Use%
Boot           1000000        0              100
Image1         10051616       4104160        71
Image2         10051616       4104160        71
FileSystem     286720         3645440        7

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]

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
<ipif_name>	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                       : 10.90.90.90
Subnet Mask                      : 255.0.0.0
Default Gateway                  : 0.0.0.0
DHCPv6 Client State              : Disabled

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, 1 hrs, 0 min, 10 secs
System Time                      : 01/01/2017 01:09:37
System hardware version          : F1
System firmware version          : 6.10.B010
System boot version              : 1.00.009
System serial number             : QBI21B8000004
MAC Address                      : 1C-7E-E5-29-F8-17

DGS-1210-52>
```

show route

目的

スイッチの IPv4 または IPv6 のルーティングステータスを表示します。

構文

show route {ipv4 | ipv6}

説明

スイッチの IPv4 または IPv6 のルーティングステータスを表示します。

制限事項

なし

使用例

IPv4 と IPv6 のルーティングステータスを表示します。

```
DGS-1210-28> show route ipv4

IPv4 Static Route State : Disable

DGS-1210-28>show route ipv6

IPv6 Static Route State : Disable

DGS-1210-28>
```

show ddpClient

目的

スイッチの DDP クライアントのステータスを表示します。

構文

show ddpClient

説明

スイッチの DDP クライアントのステータスを表示します。

制限事項

なし

使用例

DDP クライアントのステータスを表示します。

```
DGS-1210-28> show ddpClient

Enable

DGS-1210-28>
```

show nmsManaged

注意　Nuclias Connect による管理は未サポートです。

目的

スイッチの Nuclias Connect による管理のステータスを表示します。

構文

show nmsManaged

説明

スイッチの Nuclias Connect による管理のステータスを表示します。

制限事項

なし

使用例

NMS 管理のステータスを表示します。

```
DGS-1210-28> show nmsManaged

Status                          :Disable
Connection Status               :Disconnected
Management status               :Not managed
D-Link NMS URL                  :
Network UUID                    :
Periodic Message Interval       :0

DGS-1210-28>
```

enable ddpClient

目的

スイッチの DDP クライアントを有効にします。

構文

enable ddpClient

説明

スイッチの DDP クライアントを有効にします。

制限事項

なし

使用例

DDP クライアントを有効にします。

```
DGS-1210-28> enable ddpClient

DGS-1210-28>
```

enable nmsManaged

注意　Nuclias Connect による管理は未サポートです。

目的

Nuclias Connect による管理を有効にします。

構文

enable nmsManaged

説明

Nuclias Connect による管理を有効にします。

制限事項

なし

使用例

Nuclias Connect による管理を有効にします。

```
DGS-1210-28> enable nmsManaged

Device will reboot and connect to Nuclias Connect automatically.
Current running config will be reset to default automatically.
Do you want to continue?[Y/n]

DGS-1210-28>
```

注意　スイッチは再起動し、自動的に Nuclias Connect に接続します。現在のコンフィグは初期値にリセットされます。

disable ddpClient

目的

スイッチの DDP クライアントを無効にします。

構文

disable ddpClient

説明

スイッチの DDP クライアントを無効にします。

制限事項

なし

使用例

DDP クライアントを無効にします。

```
DGS-1210-28> disable ddpClient

DGS-1210-28>
```

disable nmsManaged

注意　Nuclias Connect による管理は未サポートです。

目的

Nuclias Connect による管理を有効にします。

構文

disable nmsManaged

説明

Nuclias Connect による管理を有効にします。

制限事項

なし

使用例

Nuclias Connect による管理を有効にします。

```
DGS-1210-28> disable nmsManaged

DGS-1210-28>
```

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（最大 20 文字）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 [config config_id <integer (1-2)>]

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 config config_id 2
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 6 ～ 10 秒間押下します。
   リセットボタンを 6 秒以上押下すると、前面パネルの LED ステータスが以下の状態となります。

LED	状態
PWR	点灯（変化なし）
Link/Act（全てのポート LED）	橙色に 2 秒間点灯

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のバックアップを取得し保存してください。
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。

補足 リセットボタンを 1 ～ 5 秒間押下するとスイッチが再起動します。

補足 リセットボタンを 11 秒以上押下すると再起動後にローダーモード※1 となり、LED が緑色に 2 秒間点灯します。

※ 1 : イメージファイルが破損している場合、スイッチはローダーモードで起動します。

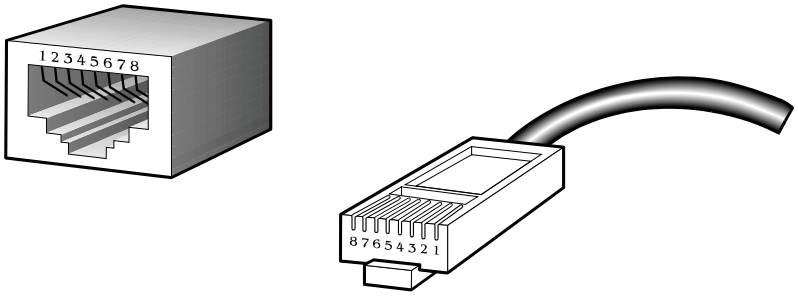
※ 1 : ローダーモードにおいて SFP インタフェースはサポートされません。

※ 1 : ローダーモードになった場合、IP アドレスは 10.90.90.90 になります。設定内容は保持されます。

※ 1 : ローダーモードではファームウェアアップグレードを実行できません。

【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。



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。

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	ループ状のネットワークにおいてブロードキャストフレームがネットワーク帯域を消費し、ネットワークエラーを引き起こす現象。
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。

- Traffic Segmentation（トラフィックセグメンテーション）
- VLAN
- Link Aggregation（リンクアグリゲーション）
- Access List（アクセスリスト）

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DGS-1210

Traffic Segmentation（トラフィックセグメンテーション）

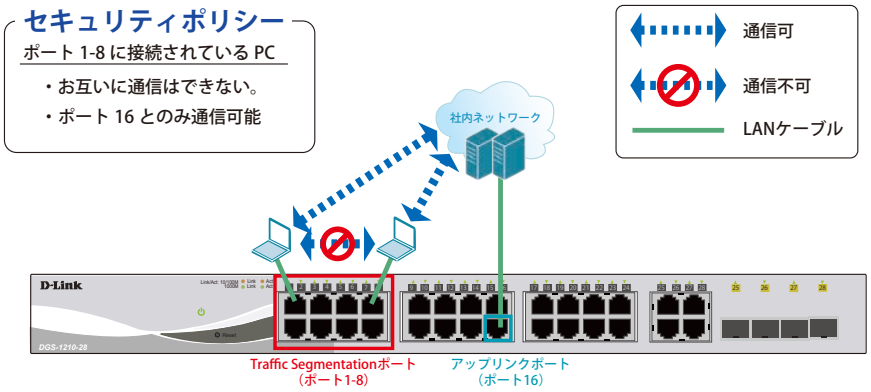


図 8-1　Traffic Segmentation（DGS-1210-28）

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. **Security > Traffic Segmentation** で「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。

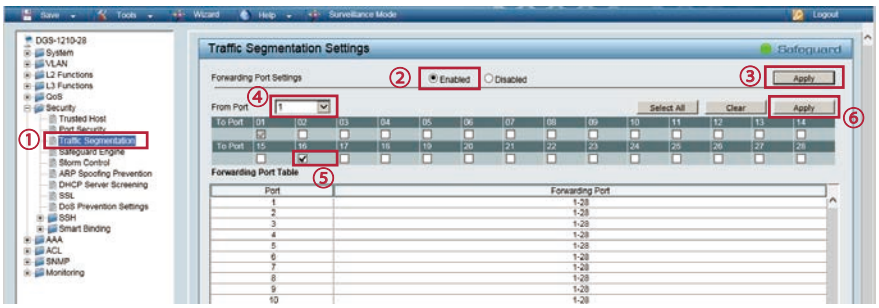


図 8-2　Traffic Segmentation（DGS-1210-28）

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。

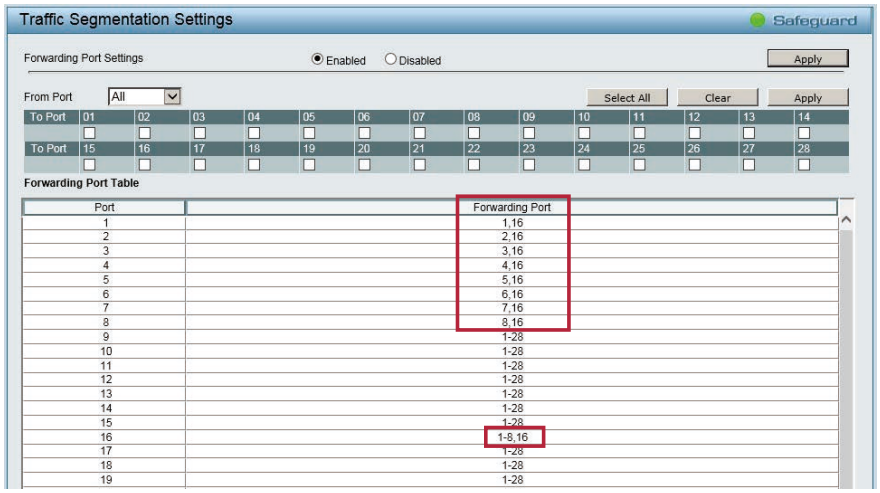


図 8-3　Traffic Segmentation Settings（DGS-1210-28）

補足　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。

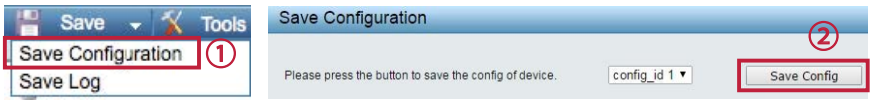


図 8-4　Save Configuration（DGS-1210-28）

VLAN

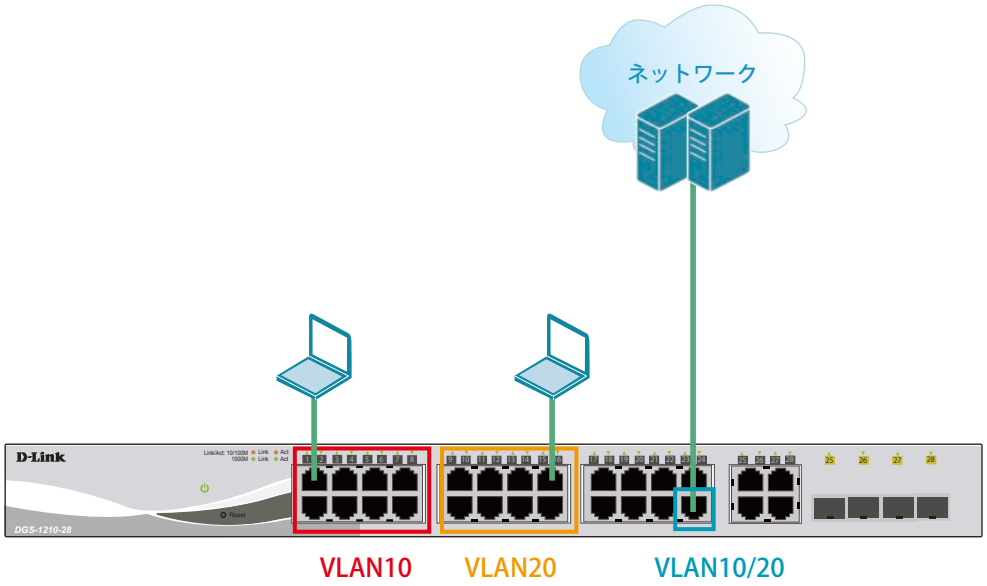


図 8-5　VLAN（DGS-1210-28）

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。

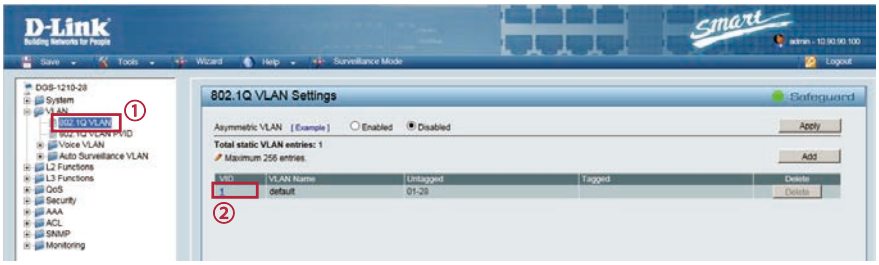


図 8-6　デフォルト VLAN 指定（DGS-1210-28）

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

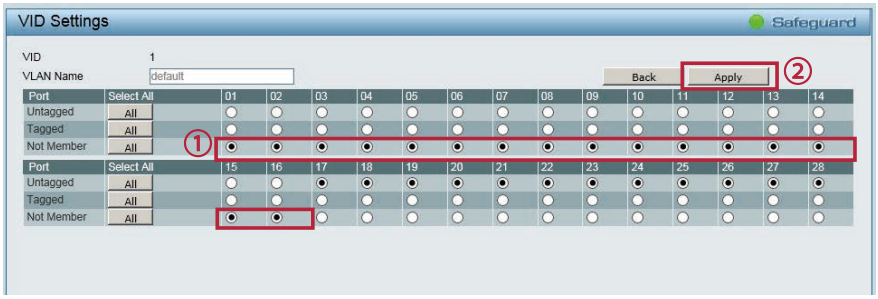


図 8-7　デフォルト VLAN アサイン削除（DGS-1210-28）

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。

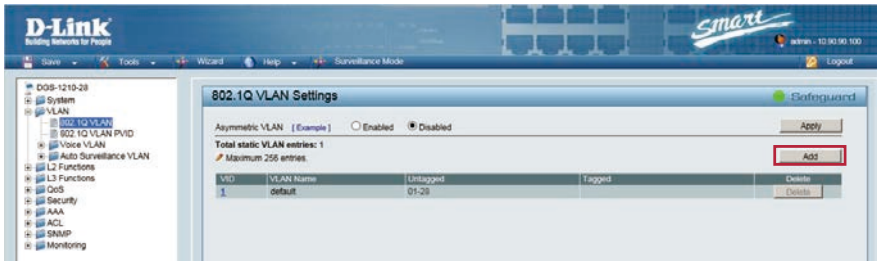


図 8-8　VLAN10 作成（DGS-1210-28）

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

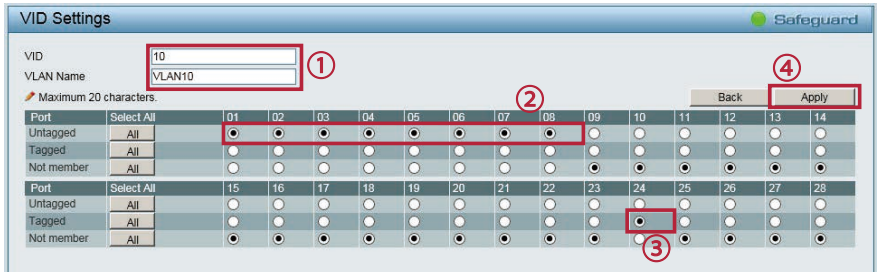


図 8-9　ポートアサイン（DGS-1210-28）

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。

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

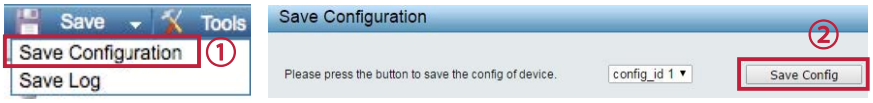


図 8-10　Save Configuration（DGS-1210-28）

Link Aggregation（リンクアグリゲーション）

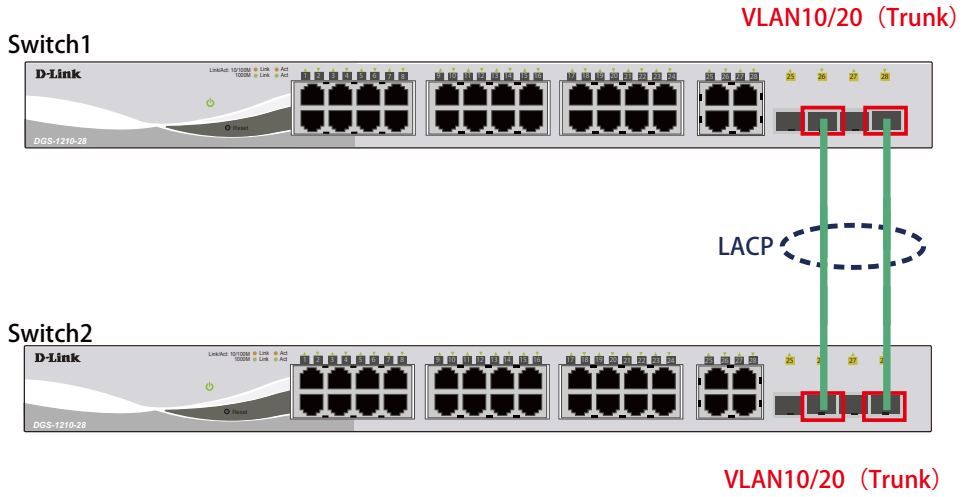


図 8-11　Link Aggregation（DGS-1210-28）

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。VLAN20 も同様に作成し、ポート 26、28 に Tagged でアサインします。

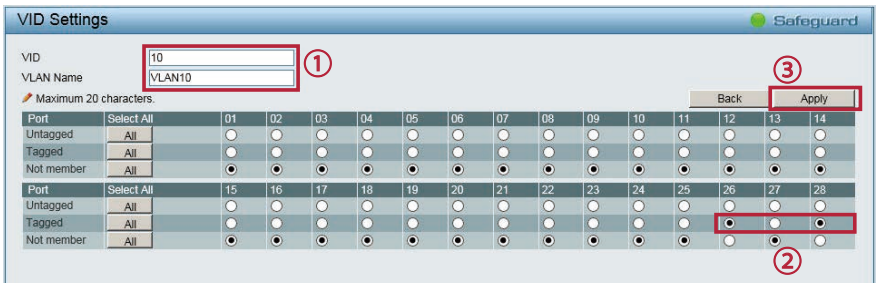


図 8-13　ポートアサイン（DGS-1210-28）

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。

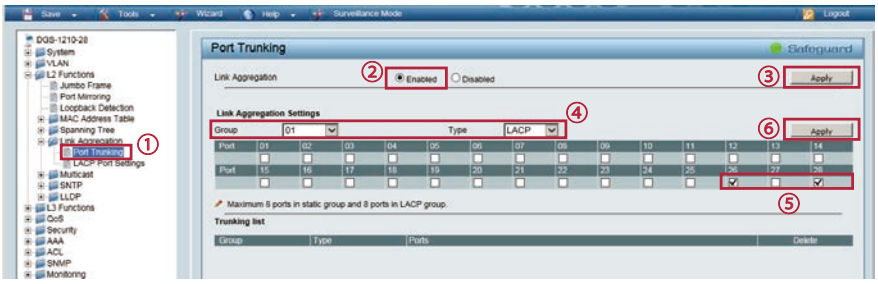


図 8-14　LACP 設定（DGS-1210-28）

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

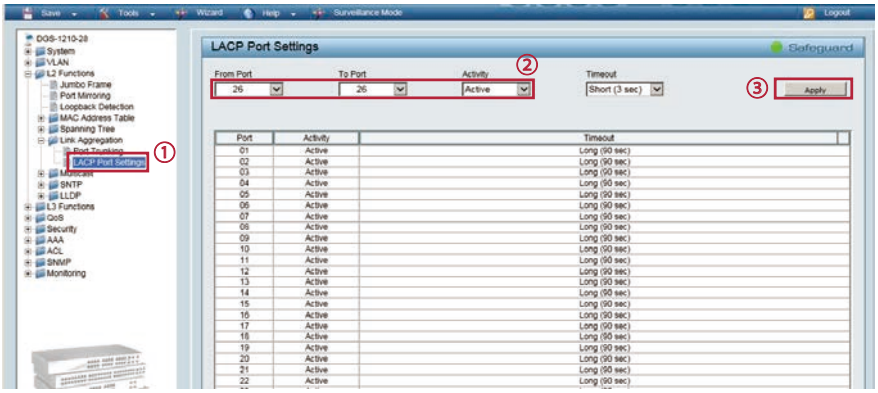


図 8-15　LACP（Active）（DGS-1210-28）

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。

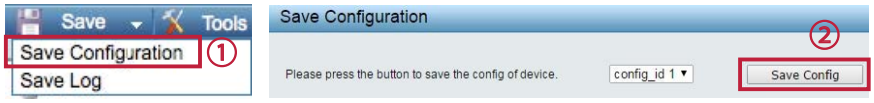


図 8-16　Save Configuration（DGS-1210-28）

Access List（アクセスリスト）

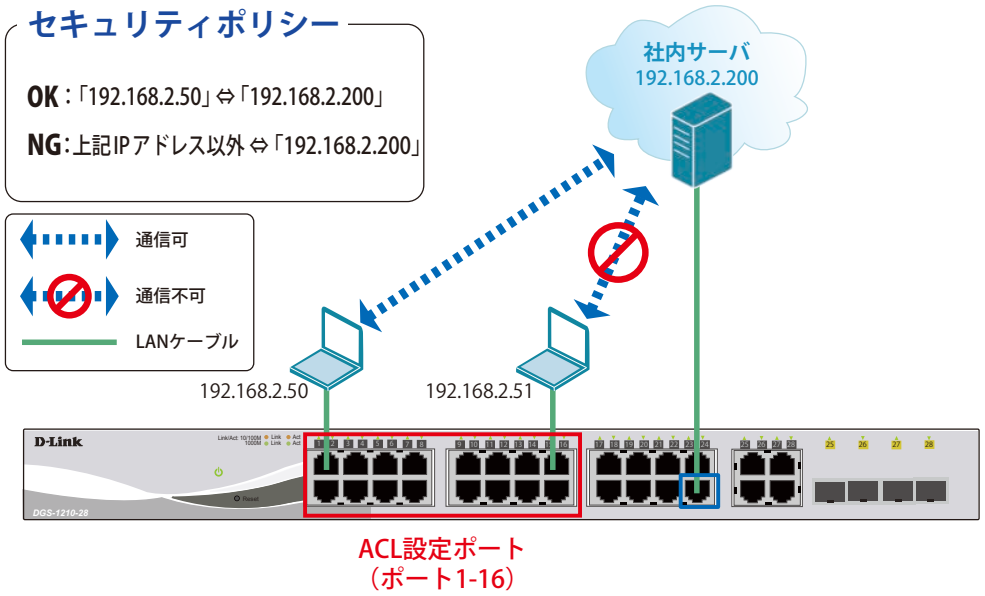


図 8-17　Access List

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。

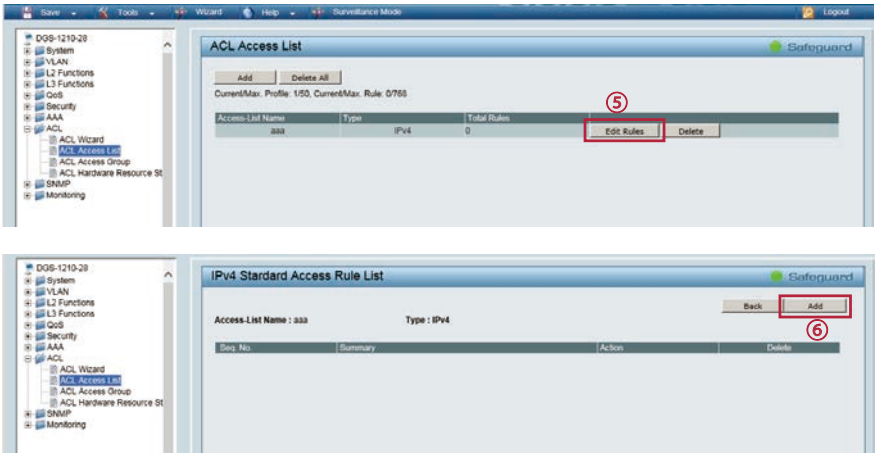


図 8-20　IPv4 プロファイルルール設定（DGS-1210-28）

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。

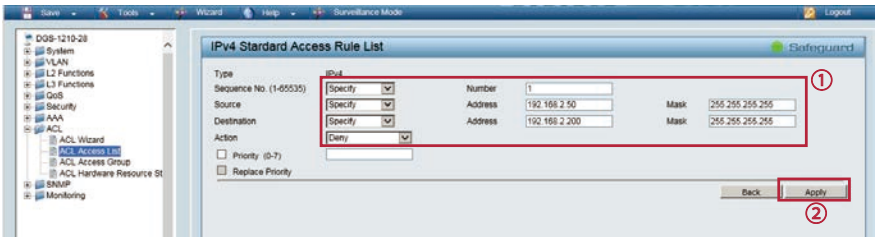


図 8-21　IPv4 プロファイルルール設定（DGS-1210-28）

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。

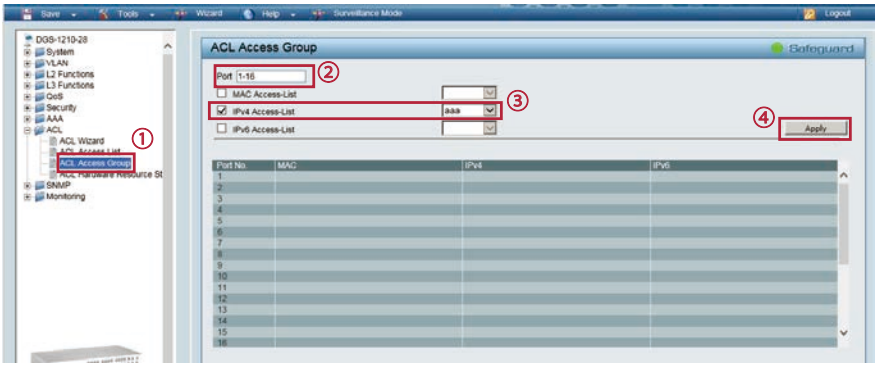


図 8-22　IPv4 プロファイルルール設定（DGS-1210-28）

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）