D-Link DIS-200G シリーズ

Industrial Gigabit L2 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、傷害または物損損害が発生するおそれがあります。

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

⚠危険

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

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

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

ご使用上の注意

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

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

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

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

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

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

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

製品名 / 品番一覧

製品名	品番
DIS-200G-12SW	DIS-200G-12SW/A1
DIS-200G-12PSW	DIS-200G-12PSW/A1

目次

はじめに

DIS-200G シリーズユーザマニュアルは、本製品のインストールおよび操作方法を例題と共に記述しています。

第 1 章 本製品のご利用にあたって
- 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 機器の設置
- 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 スイッチ管理について
- スイッチの管理方法についての概要と DNA (D-Link Network Assistant) について説明します。

第 5 章 Web ベースのスイッチ管理
- Web ベースの管理機能への接続方法および使用方法、Smart Wizard 設定について説明します。

第 6 章 System（システム設定）
- デバイス情報の確認、システム情報設定、PoE 設定、Syslog 設定、システム時刻の設定について説明します。

第 7 章 Management（スイッチの管理）
- ユーザアカウント設定、SNMP 設定、HTTP/HTTPS 設定、D-Link Discovery Protocol 設定などについて説明します。

第 8 章 L2 Features（レイヤ 2 機能の設定）
- FDB 設定、VLAN 設定、スパニングツリーの設定、ループバック検知設定、リンクアグリゲーション、L2 マルチキャストコントロール、LLDP 設定など L2 機能について説明します。

第 9 章 QoS（QoS 機能の設定）
- 802.1p 設定、ポートレート設定について説明します。

第 10 章 Security（セキュリティ機能の設定）
- セーフガードエンジン、トラフィックセグメンテーション、ストームコントロール、DoS 攻撃防止設定、SSL などのセキュリティの設定について解説します。

第 11 章 OAM（Operations、Administration、Maintenance：運用・管理・保守）
- ケーブル診断機能について解説します。

第 12 章 Monitoring（スイッチのモニタリング）
- 本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報について表示します。

第 13 章 Green（省電力テクノロジー）
- 本スイッチの省電力、EEE について設定、表示します。

第 14 章 Save and Tools（Save と Tools メニュー）
- Web インタフェース画面左上部の「Save」「Tools」メニューを使用してスイッチの管理、設定を行います。

第 15 章 サーベイランスモード
- サーベイランスモードでのスイッチの管理、設定について説明します。

【付録 A】システムログエントリ
- スイッチのシステムログに表示されるシスログエントリとそれらの意味について説明します。

【付録 B】トラップログ
- トラップログとそれらの意味について説明します。

【付録 C】IETF RADIUS 属性のサポート
- 本製品がサポートする IETF RADIUS 属性について表示します。

【付録 D】機能設定例
- 主要な機能の設定例について表示します。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、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」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "（13 ページ）をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
courier 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
courier 斜体	コマンド項目（可変または固定）。	*value*
< >	可変項目。< > にあたる箇所に値または文字を入力します。	<*value*>
[ ]	任意の固定項目。	[*value*]
[< >]	任意の可変項目。	[<*value*>]
{ }	{ } 内の選択肢から 1 つ選択して入力する項目。	{*choice1* | *choice2*}
|（垂直線）	相互排他的な項目。	*choice1* | *choice2*
Menu Name > Menu Option	メニュー構造を示します。	Device > Port > Port Properties は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。

第 1 章　本製品のご利用にあたって

スイッチ概要

DIS-200G シリーズは、工場などで必要となる環境要件を備えた産業用ギガビット L2 スマートスイッチです。DIN レールや壁面への設置に対応しており、オプションで 19 インチラックマウントキットにも対応しています。また動作可能温度の範囲も - 40 ～ 75℃をカバーしているため、工場内等のエッジ環境での利用に最適です。全機種ギガビットポートを実装しており、SFP スロット × 2 も搭載、さらに DIS-200G-12PSW は 8 ポートが IEEE 802.3af/at 準拠の PoE+ 給電に対応しています。Web GUI や SNMP、CLI を使用した効率的な管理でシンプルなネットワークを構築できます。本スイッチは VLAN やループ検知、D-Link セーフガードエンジンなど最低限必要な機能を搭載、さらに IEEE 802.1p QoS、IEEE 802.3x フローコントロール、オートネゴシエーション、Auto MDI/MDI-X、ジャンボフレームにも対応しており、様々な環境で安定したネットワーク環境を提供することができます。

本製品は IP30 保護等級のメタル筐体を採用、動作温度 -40~75℃を達成するなど信頼性の高い設計になっています。また、ファンレス設計により、粉塵の吸い込みによる故障のリスクを軽減することができます。イーサネットポートは 6kV サージプロテクションに対応し、落雷による影響を最小限に抑えます。さらに、DC 電源の冗長化が可能で、片系等の電源に故障があった場合でも、ダウンタイムなしでもう冗長電源に切り替わりが可能です。

本製品は壁面への設置に加え、DIN レールへの簡単な設置が可能となっています。電源には冗長化可能な 2 系統の DC ターミナルブロックを搭載しています。さらにオプションで 19 インチラックマウントにも対応しています。

本製品は 802.1Q タグ / ポートベース VLAN に対応、帯域制御で各ポートのスループットを調整し、質の高いネットワーク状態を保ちます。ブロードキャスト / マルチキャストや不明なユニキャストトラフィックの発生をストームコントロールで検出し、ネットワークのフラッドを回避 / ブロック、充実した機能により安全なネットワーク環境を維持できます。

本製品はポートミラーリング、IGMP スヌーピングなどの L2 機能のほかに、ポート配下のスイッチや自筐体ポート間でループが発生したポートを検知するループバック検知機能など、充実したネットワークメンテナンス機能を搭載しています。

サポートする機能

- SNMP/CLI/Web-GUI による設定および管理
- IEEE 802.3af/at PoE/PoE+ 給電（DIS-200G-12PSW）
- 802.1p プライオリティキューと帯域制御
- ケーブル診断機能 / ループバック検知
- ポートベース VLAN/GVRP/Voice VLAN
- Auto Surveillance VLAN（ASV2.0）/Asymmetric VLAN
- IGMP スヌーピング
- IEEE802.1D STP/802.1w RSTP/802.1s MSTP
- ブロードキャストストームコントロール
- D-Link セーフガードエンジン
- D-Link Green 省電力機能対応
- DIN レール設置
- 安全規格（UL60950-1）/ 保護等級（IP30）準拠
- 19 インチラックマウントキット対応（オプション）
- RoHS 指令対応

搭載ポート

DIS-200G シリーズは以下のポートを搭載しています。

DIS-200G-12SW

- 10BASE-T/100BASE-TX/1000BASE-T ポート x　10
- コンソールポート x 1
- SFP スロット x 2

DIS-200G-12PSW

- 10BASE-T/100BASE-TX/1000BASE-T ポート（PoE）x　8
- 10BASE-T/100BASE-TX/1000BASE-T ポート x　2
- コンソールポート x 1
- SFP スロット x 2

前面パネル

前面パネルには、10/100/1000BASE-T ポート、SFP スロット、コンソールポート、リセットボタンと Power、システム、ポートの Link/Act、PoE（12PSW のみ）、アラームの状態を表示する LED を搭載しています。14 ページの「LED 表示」の項で詳細の動作について説明します。また、リセットボタンを押下すると、すべての設定を工場出荷時の状態にリセットします。

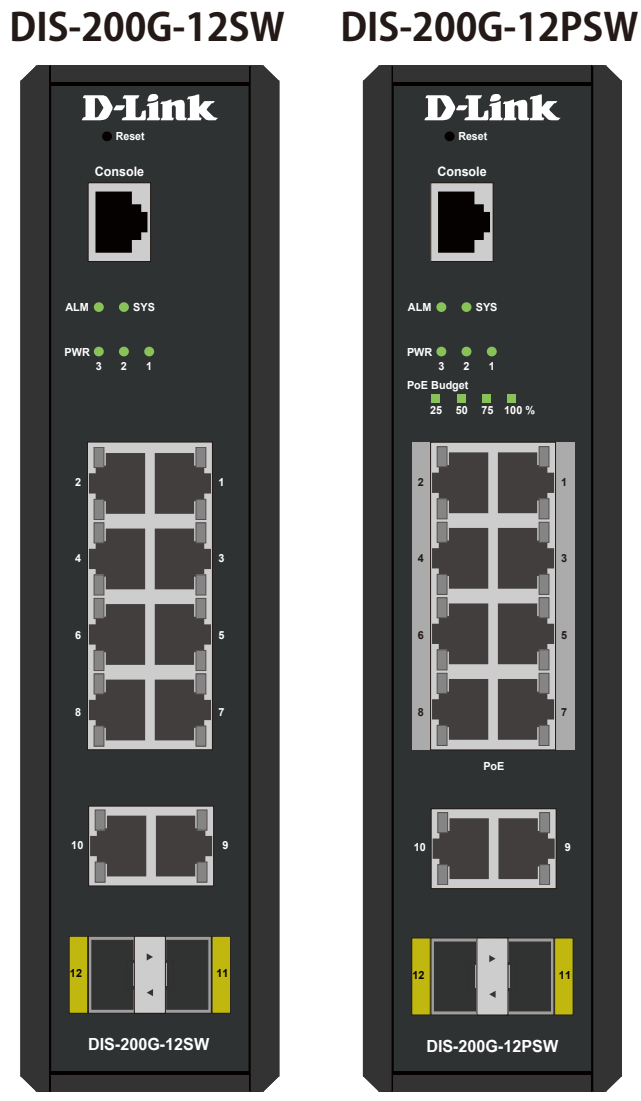


図 1-1　DIS-200G-12SW/12PSW 前面パネル図

LED 表示

Power、システム、ポートの Link/Act、PoE（12PSW のみ）、アラームの状態を表示する LED を搭載しています。

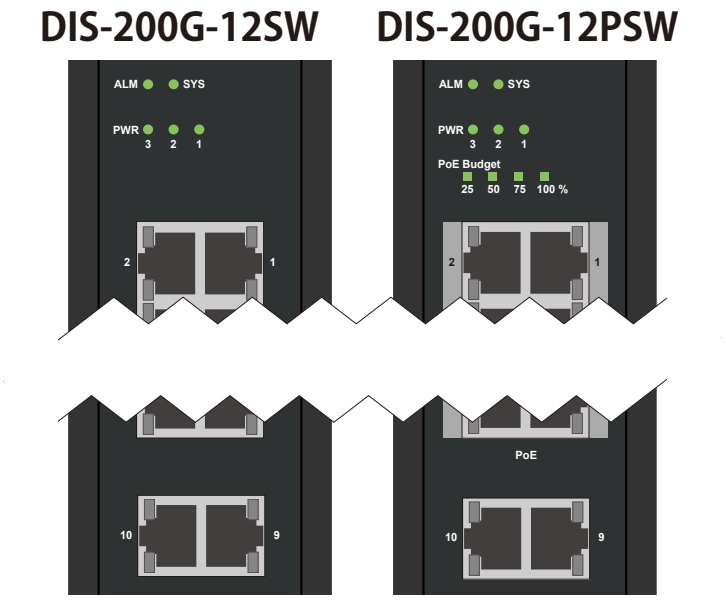


図 1-2　DIS-200G-12SW/12PSW 前面パネルの LED 配置図

以下の表にスイッチの LED の状態が意味するスイッチの状態を示します。

LED		色	状態	内容
SYS		緑	点灯	スイッチが起動し、ネットワークとの接続が確立しています。
		緑	点滅	ファームウェアの更新中です。
		橙	点灯	ネットワークとの接続準備中です。
		橙	点滅	スイッチが起動中です。または PoE に不具合が発生しています（12PSW のみ）
ALM		橙	点灯	スイッチへの電源供給に失敗しています。
PWR 1		緑	点灯	「P1」に電源が接続されています。
PWR 2		緑	点灯	「P2」に電源が接続されています。
PWR 3		緑	点灯	「P3」に電源が接続されています。
PoE Budget（12PSW のみ）	100	緑	点灯	PoE 給電可能電力が 100% です。現在 PoE 給電は行われていません。
	75	緑	点灯	現在の PoE 給電可能電力は 100% - 75% あります。
	50	緑	点灯	現在の PoE 給電可能電力は 75% - 50% あります。
	25	緑	点灯	現在の PoE 給電可能電力は 50% - 25% あります。
		橙	点灯	現在の PoE 給電可能電力は 25% - 0% です。15.4W 以上の電力が残されています。
		橙	点滅	現在の PoE 給電可能電力は 25% - 0% です。15.4W 以下の電力が残されています。
ポート LED 説明（本体上部を左に横にした状態での説明になります。）				
左 LED			右 LED	
ポート LED（DIS-200G-12PSW）				
ポート 1 - 10	左	緑	点灯	1Gbps でリンクが確立しています。
		緑	点滅	1Gbps でデータを送受信しています。
		橙	点灯	10/100Mbps でリンクが確立しています。
		橙	点滅	10/100Mbps でデータを送受信しています。
ポート 1 - 8	右	緑	点灯	PoE 給電が 15.4W 以下（IEEE 802.3af/at）で実行されています。
		橙	点灯	PoE 給電が 15.4 - 30W（IEEE 802.3at）で実行されています。
		橙	点滅	PoE 給電が 30W を超え、ポートはシャットダウンしています。
ポート LED（DIS-200G-12SW）				
ポート 1 - 8	左	緑	点灯	1Gbps でリンクが確立しています。
		緑	点滅	ケーブル診断が実行中です。
		橙	点灯	10/100Mbps でリンクが確立しています。

LED		色	状態	内容
ポート 1 - 8	右	緑	点滅	1Gbps でデータを送受信しています。
		橙	点滅	10/100Mbps でデータを送受信しています。
ポート 9 - 10	左	緑	点灯	1Gbps でリンクが確立しています。
		緑	点滅	1Gbps でデータを送受信しています。
		橙	点灯	10/100Mbps でリンクが確立しています。
		橙	点滅	10/100Mbps でデータを送受信しています。
ポート LED（DIS-200G-12SW/PSW 共通）				
ポート 11- 12		緑	点灯	1Gbps でリンクが確立しています。
		緑	点滅	1Gbps でデータを送受信しています。

背面パネル

背面パネルには壁面キット設置穴、AC アダプタ（オプション）コネクタ、DIN レールブラケット（設置済み）があります。

注意 AC アダプタは未サポートです。

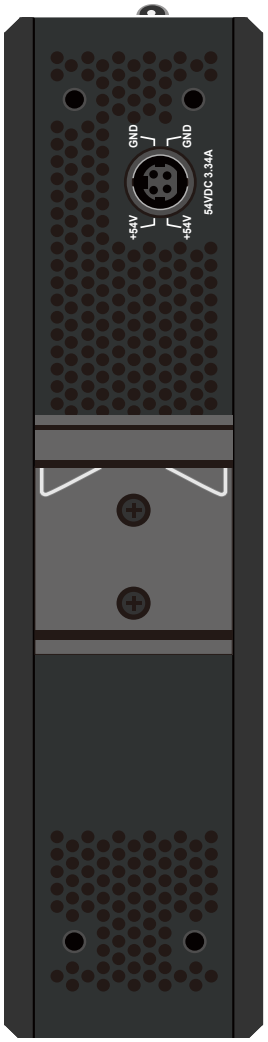


図 1-3　DIS-200G-12SW/12PSW の背面パネル図

上面パネル

本体上面には DC ターミナルブロックコネクタ（DC 電源コネクタ / アラームポート）と接地用端子があります。

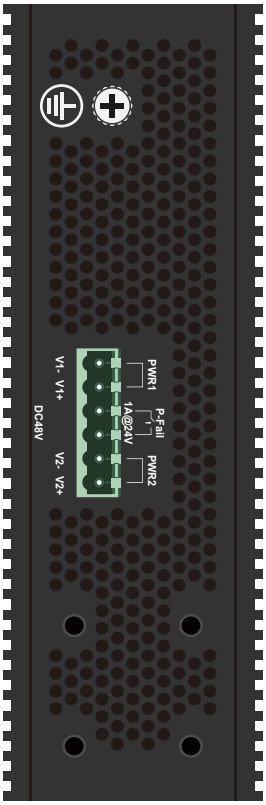


図 1-4　DIS-200G-12SW/12PSW の上面パネル図

第 2 章　機器の設置

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
- マニュアル
- シリアルラベル
- PL シート
- DC ターミナルブロック（取り付け済み）
- DIN レールブラケット（取り付け済み）
- 壁面取り付けキット
- RJ-45/RS232C コンソールケーブル
- CD-ROM

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、ご購入頂いた販売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。

- スイッチの上に重いものを置かないでください。
- 電源がしっかり差し込まれているか確認してください。
- 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。
- 本スイッチ上に他の機器を積み重ねて設置することは行わないで下さい。

DIN レールへの設置

DIS-200G シリーズは機器の背面に付属の DIN レールブラケットを使用することにより、DIN レールへの設置が可能です。DIN レールへの設置には以下の手順を参照してください。

警告　DIN レールへの設置や取り外しの際には力の加減に注意し、転倒や怪我、製品や DIN レールの落下、破損などに十分に注意してください。

注意　DIN レールブラケットは出荷時に取り付け済みです。

1. DIN レールに DIN レールブラケットを引っ掛け下に押し下げます（①）。次に製品下部を壁面に押し込むようにして設置します（②）。

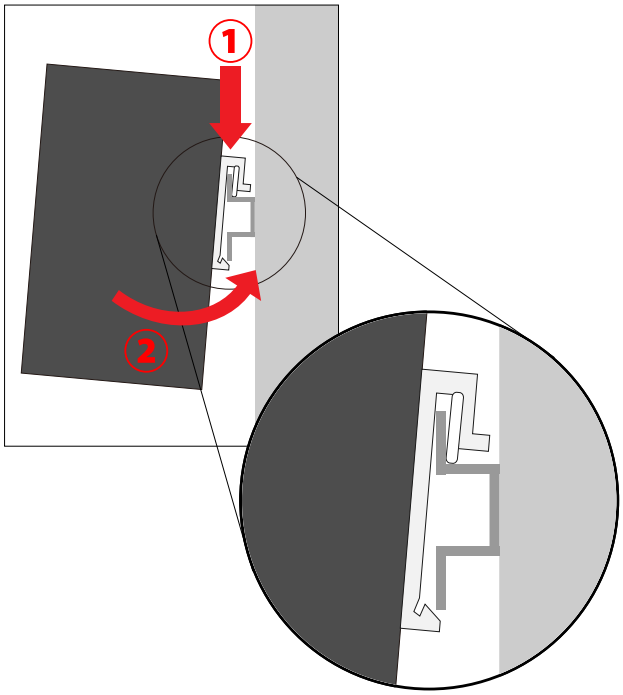


図 2-1　DIN レールへの設置

2. 製品が DIN レールにしっかり設置されていることを確認します。

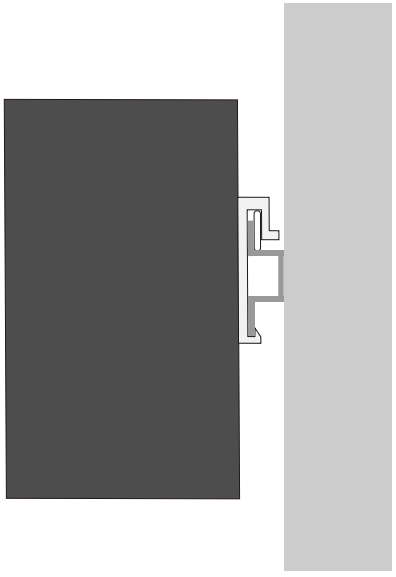


図 2-2　DIN レールへの設置確認

3. DIN レールから製品を外す際は、製品を上に押し上げ、製品下部を壁面から引き離すようにして取り外します。

壁面への設置

本製品は付属の壁面取り付けキットを利用して壁面に設置することも可能です。以下の手順で壁面に設置します。

警告　本製品を壁面に設置する際は、本製品の重さや壁面の強度、材質などを勘案し、落下などに十分注意した上で設置してください。

プレートを使用した壁面設置

1. DIN レールブラケットをドライバー（+）を使用して本製品から取り外します。
2. 壁面取り付けプレートを付属のネジで本製品に取り付けます。

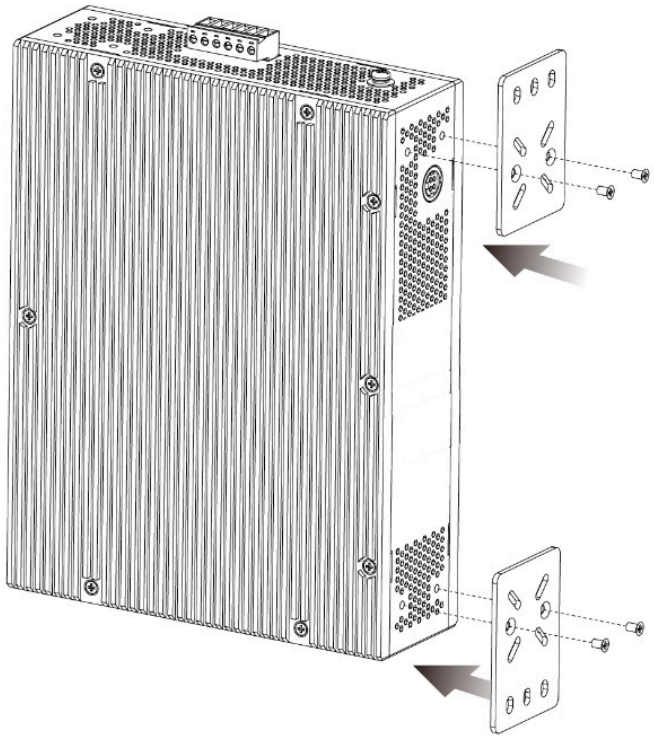


図 2-3　壁面取り付けプレートの取り付け

3. プレートを取り付けた製品背面を設置する壁面に合わせ、プレートのネジ穴を通して穴を開ける壁面の箇所を決定します。
4. ドリルなどで壁面に穴を開け、付属のアンカー（マウント）を挿し込みます。

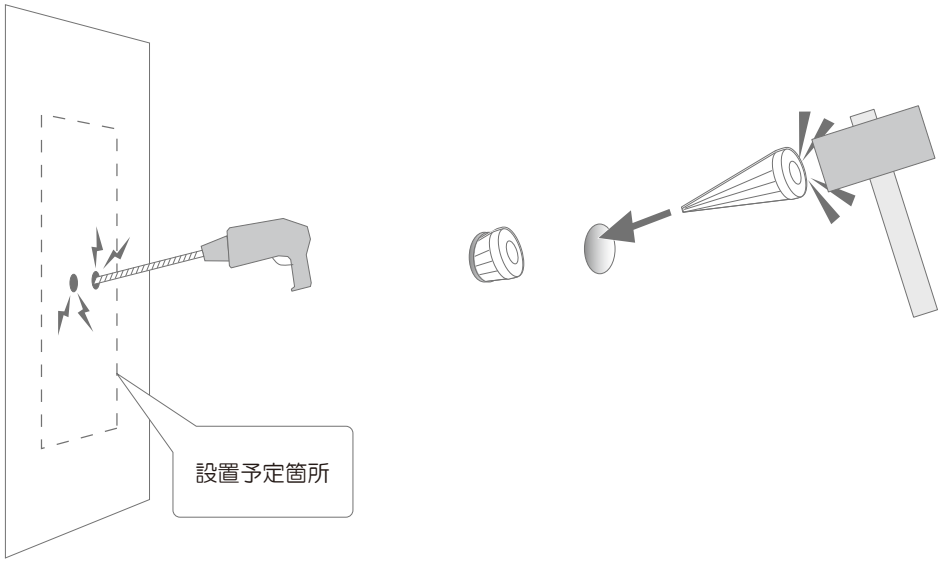


図 2-4　壁面への穴あけ、アンカー挿し込み

5. 再度、製品に取り付けたプレートの穴をアンカーに合わせ、付属のネジを使用して壁面に設置します。

ネジを使用した壁面設置

1. DIN レールブラケットをドライバー（＋）を使用して本製品から取り外します。
2. 穴を開ける壁面の箇所（× 2）を決定します。二つの穴には 60mm の間隔を設けます。

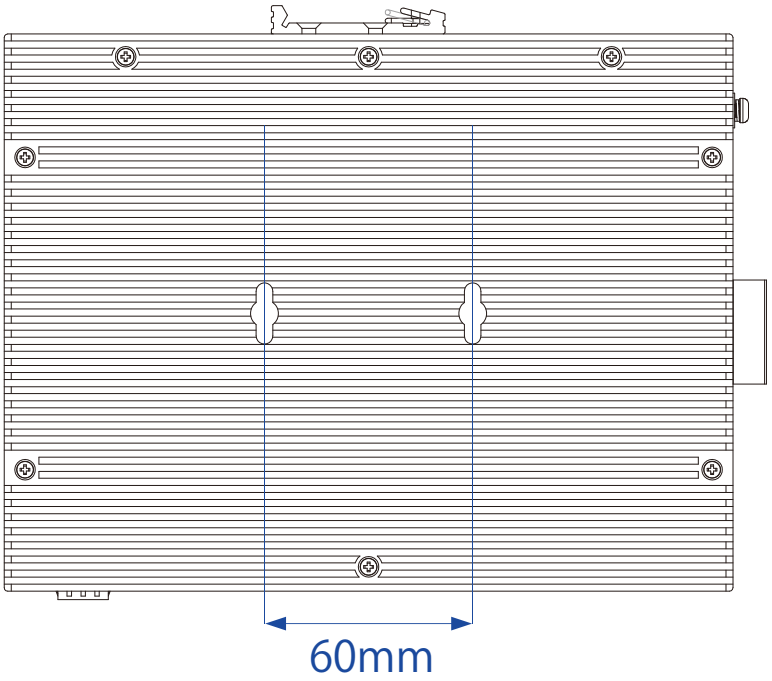


図 2-5　ネジ穴間隔

3. ドリルなどで壁面に穴を開け、付属のアンカー（マウント）を挿し込みます。

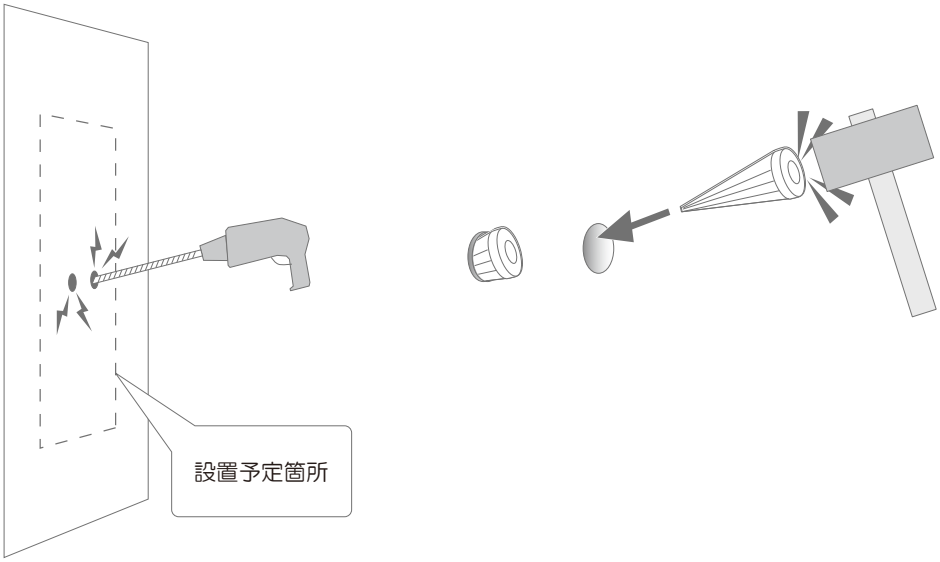


図 2-6　壁面への穴あけ、アンカー挿し込み

4. 付属のネジをアンカー（マウント）に挿し込みます。ネジは最後まで挿し込まず、壁面から 4.5mm の隙間を空けます。

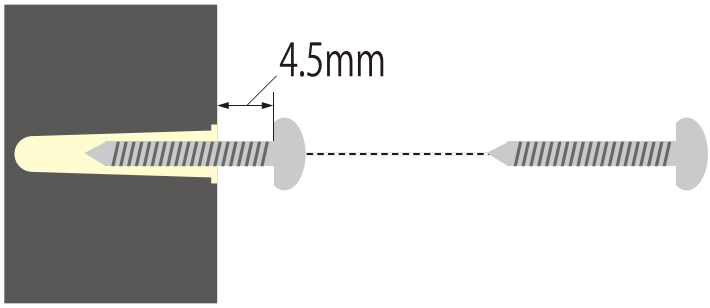


図 2-7　ネジの挿し込み

5. 壁面から出ているネジに製品側部の穴に引っ掛け、設置は完了です。

19 インチラックへの取り付け（オプション）

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。

注意　ラックマウントキットはオプションになります。弊社 Web サイトの製品情報をご確認ください。

ブラケットの取り付け

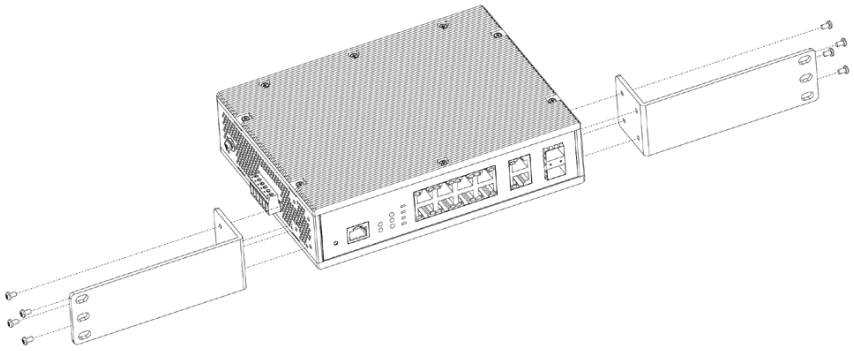


図 2-8　スイッチへのブラケットの取り付け

ラックマウントキット（オプション）に付属のネジを使用して、本スイッチにブラケットを取り付けます。完全にブラケットが固定されていることを確認し、本スイッチを以下の通り標準の 19 インチラックに固定します。

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。

D. 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。

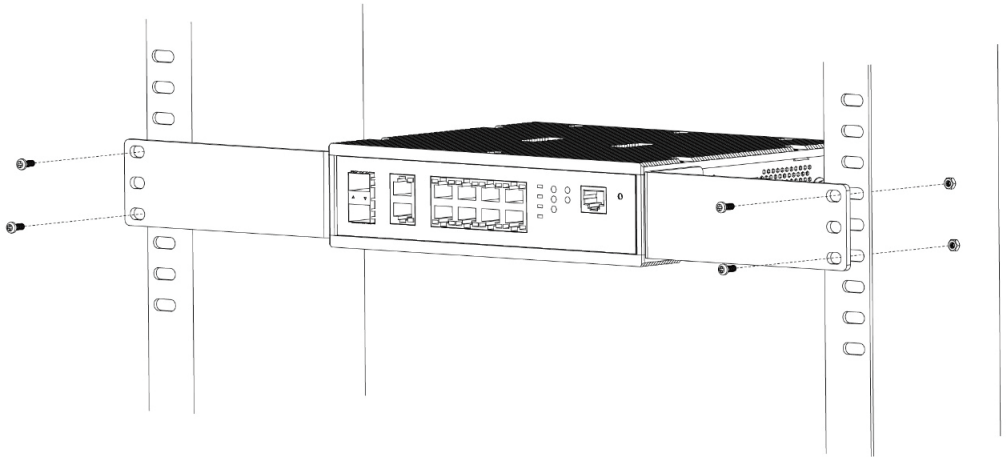


図 2-9　スイッチのラックへの設置

製品の接地

本製品を接地する方法について説明します。

注意　電源を投入する前に、本手順を完了する必要があります。

注意　本製品の接地は、接地抵抗についての専門的な知識と技能を有する資格保持者により実施してください。

接地に必要なツールと機器

- 接地用ネジ（製品に付属のネジ）
- 接地線（製品には付属されていません。）
- プラスドライバー（製品には付属されていません。ネジの大きさに合ったものをご使用ください。）

注意　接地線は国の各国の設置条件に従ったサイズ / 形状を選択します。また接地線の長さは接地環境（接地基準点とスイッチの距離など）を考慮し選択します。

以下の手順でスイッチを保安用接地に接続します。

1. スイッチの電源が投入されていないことを確認します。

2. プラスドライバを使用し、接地用ネジを取り外します。

3. 開いた状態の接地ネジ穴の上に、接地線（接地ケーブル）のリング型ラグ端子を置き、装着します。

4. 接地ネジ穴に接地用ネジを挿入します。

5. ドライバを使用して接地用ネジをしめて、スイッチに接地線（接地ケーブル）を固定します。

6. 適切な設置スタッドやボルトなどの電位基準点に、接地線のもう一端のリング型ラグ端子を取り付けます。

7. スイッチと接地線の接続がしっかりと行われていることを確認します。

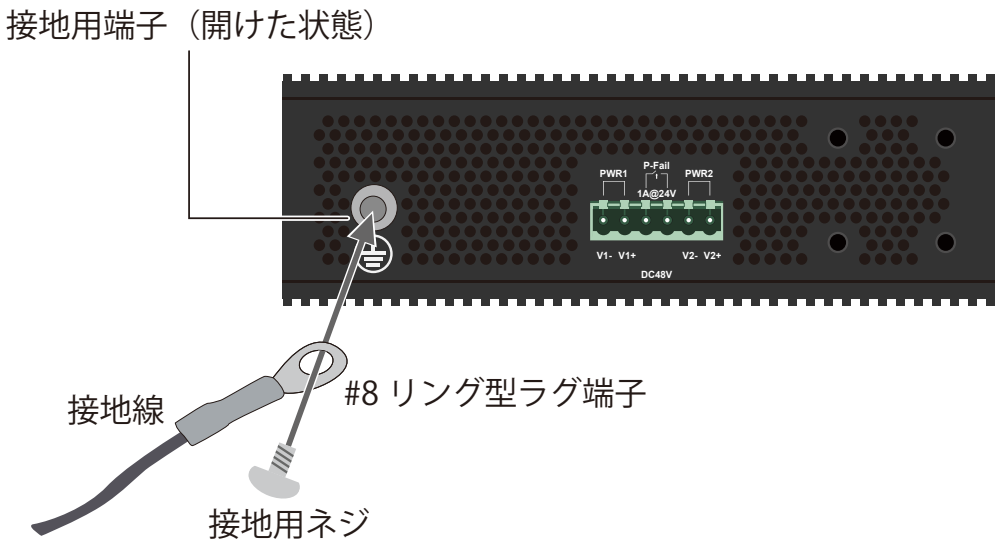


図 2-10　スイッチへのラグ端子の接地

SFP モジュールの取り付け

本製品は、前面パネルに SFP モジュール用スロットを装備しており、対応する SFP モジュールを取り付けることが可能です。

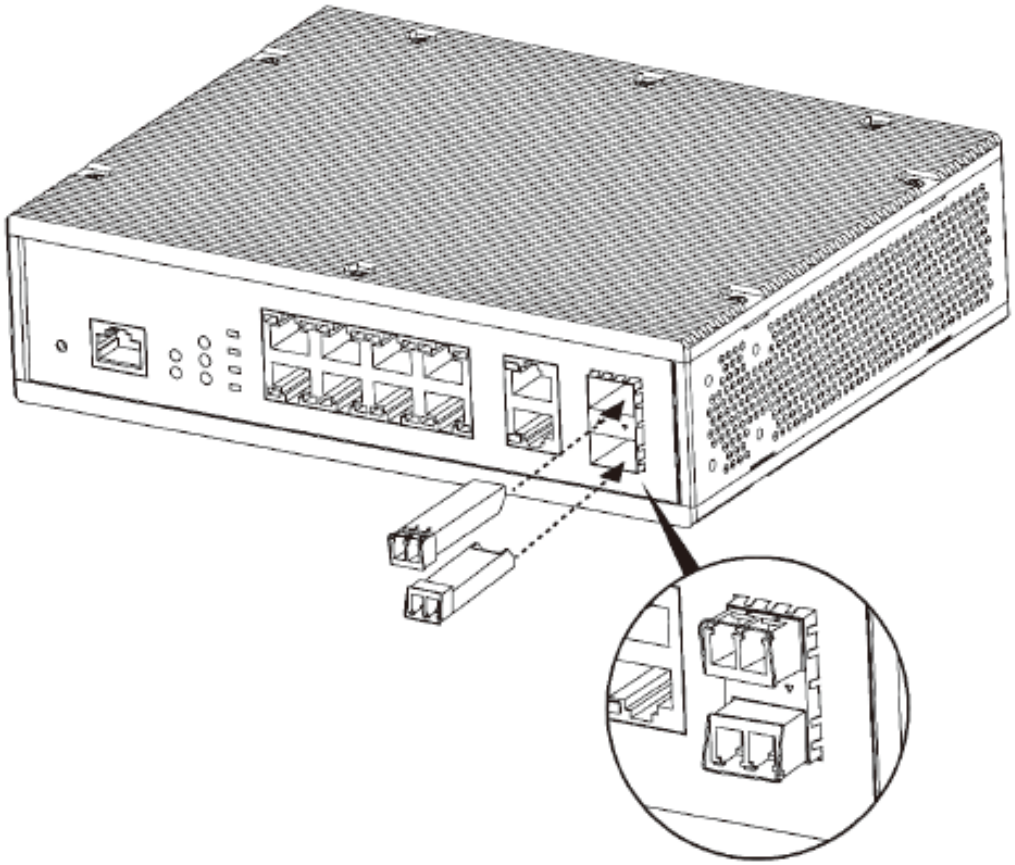


図 2-11　SFP モジュールの取り付け

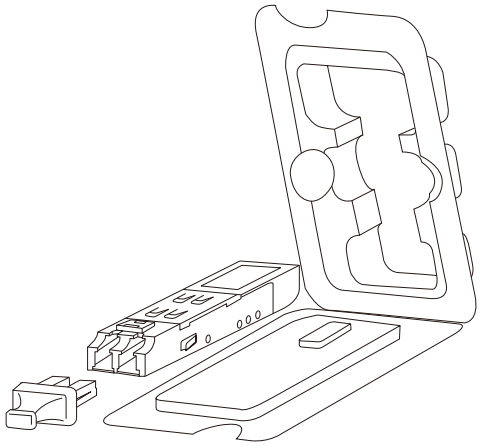


図 2-12　SFP モジュール図

注意　対応する SFP モジュールについては弊社 Web サイトの製品情報をご確認ください。

アラームの取り付け

本製品へのアラームの取り付けには DC ターミナルブロックを使用します。アラームを接続するアラームポート（アラームリレー）は DC 電源コネクタ（DC ターミナルブロック）の中央二つになります。

1. DC ターミナルブロック接続端子部分のネジを緩め、アラーム線接続部にアラームのリード線を挿入します。
2. ネジを締め直し、DC ターミナルブロックを製品の DC 電源コネクタに接続します。

アラームの作動が可能になるとリレー出力アラームは電源の不具合を検知して作動するようになります。

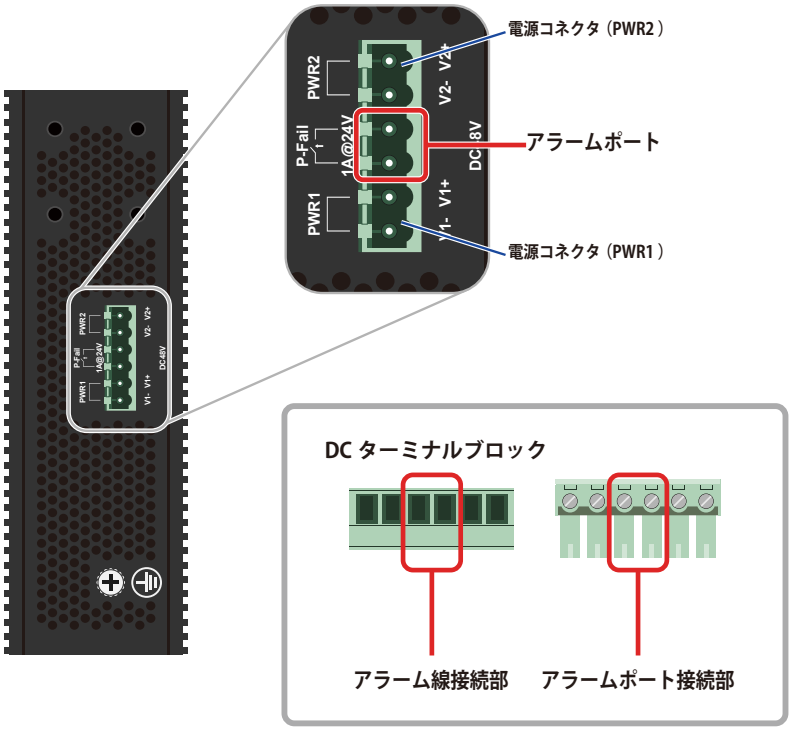


図 2-13　アラームポート

注意 DC ターミナルブロックを使用した電源の投入方法については「電源の投入」を参照ください。

注意 使用するアラームの詳しい設定方法についてはご購入のアラームの説明書をご確認ください。

電源の投入

本製品の電源の投入について説明します。

DC 電源の接続

本製品の DC 電源コネクタにはマイナス / プラス端子（PWR1/PWR2）とアラームポートがあります。付属する DC ターミナルブロックにはそれぞれの端子、ポートに対応する接続部があり、そこに DC 電源ケーブルを接続します。アラームの取り付けについては「アラームの取り付け」を参照ください。

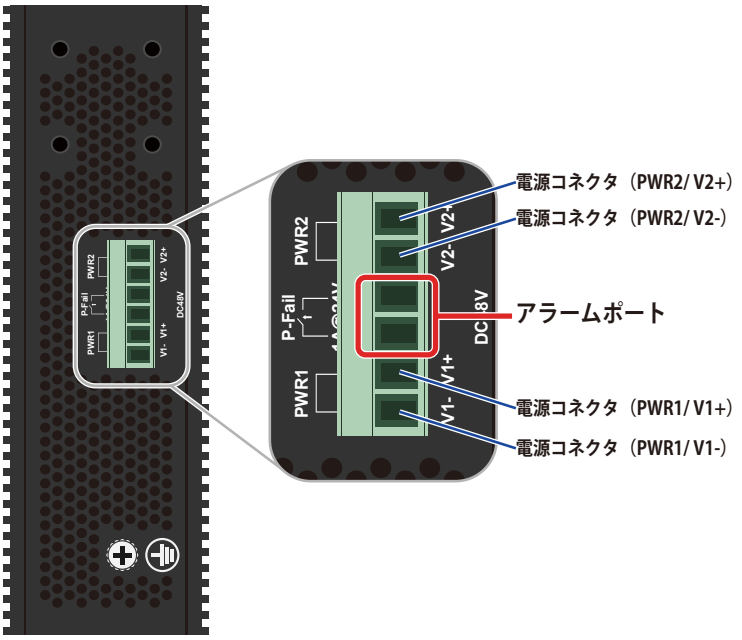


図 2-14　DC 電源コネクタ（DC ターミナルブロック接続時）

1. マイナスドライバーを使用して、DC ターミナルブロックの接続端子部分のネジを緩めます。

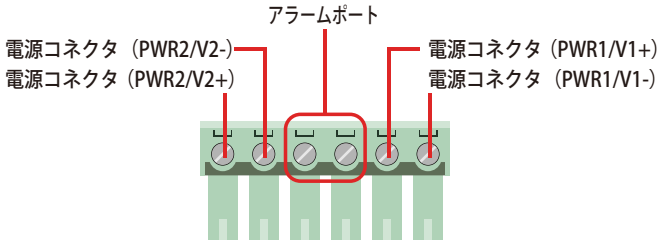


図 2-15　DC ターミナルブロックの接続端子部のネジと対応するコネクタ / ポート

2. DC ターミナルブロックのマイナス端子、プラス端子に接続する DC 電源ケーブルを挿し込み、再度ネジを締め直します。

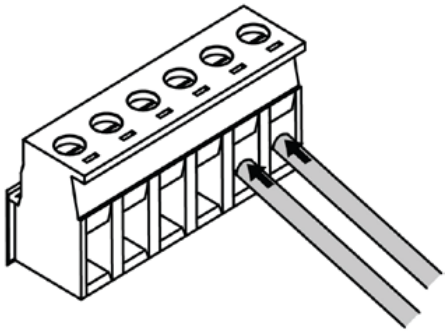


図 2-16　DC 電源ケーブル挿し込み

3. DC 電源ケーブル（アラーム線）を挿し込んだ DC ターミナルブロックを、本製品の DC 電源コネクタに取り付けます。

注意 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。

注意 資格を持つ電気工事士が、DC 電源への接続を行う必要があります。

注意 DC ターミナルブロック（DC 電源コネクタ）にはアラーム線の接続部（アラームポート）があります。DC 電源ケーブル / アラーム線の接続の際には接続箇所に注意してください。詳しくは「アラームの取り付け」を参照ください。

リダンダント電源について（冗長電源）

DC 電源は本製品付属の DC ターミナルブロックを通じて「PWR1」「PWR2」に同時に 2 つ接続することが可能です。その際、最初に接続された電源が自動的にメイン電源としてスイッチに識別されます。後から接続された電源はリダンダント電源（冗長電源）として識別されます。どちらかの電源に不具合が発生した場合、アラームポートのアラームリレーとアラーム LED（ALM LED）が作動します。本製品の DC 電源（PWR1/PWR2）において、最初からアクティブ / リダンダントを決定する順番や序列はありません。例えば、最初に「PWR 2」に電源が接続されメイン電源として識別されれば、その後「PWR 1」に接続された電源はバックアップとなります。

スイッチへの複数の電源の接続は可能ですが、同時にスイッチに電力供給を行うことはできません。120W の電源がそれぞれ「PWR1」「PWR2」に接続されていても、通常時にスイッチへの 120W の電力供給を行うのは最初に接続された電源のみになります。後から接続された電源はバックアップとなります。

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

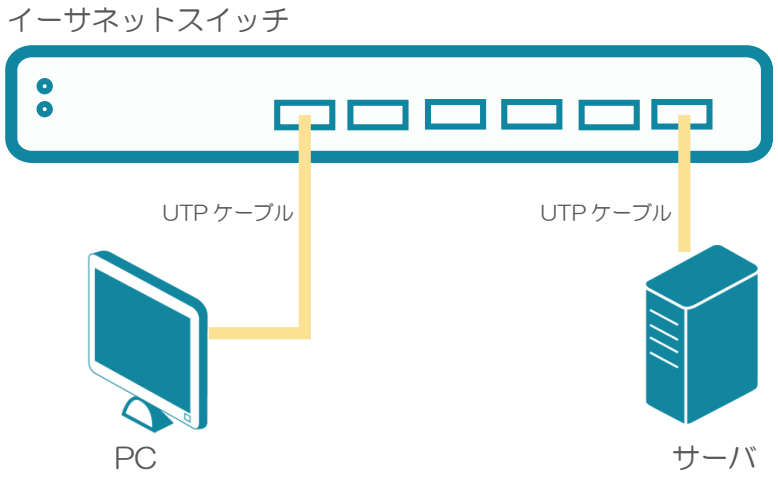


図 3-1　エンドノードと接続した図

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

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- カテゴリ 3 以上の UTP ケーブル：10BASE-T ハブまたはスイッチと接続する。
- カテゴリ 5 以上の UTP ケーブル：100BASE-TX/1000BASE-T ハブまたはスイッチと接続する。

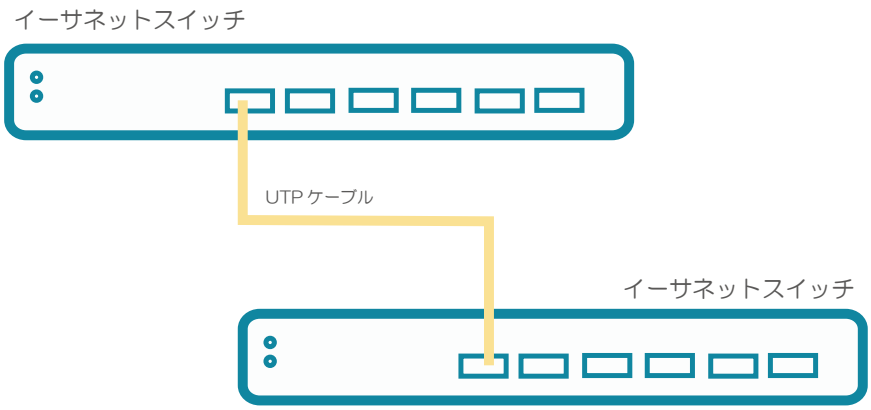


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

各イーサネットポートは、ネットワークバックボーンやサーバと接続することができます。エンハンスドカテゴリ 5 ケーブル以上の UTP ケーブルを使用します。正しくリンクが確立すると Link LED が点灯します。

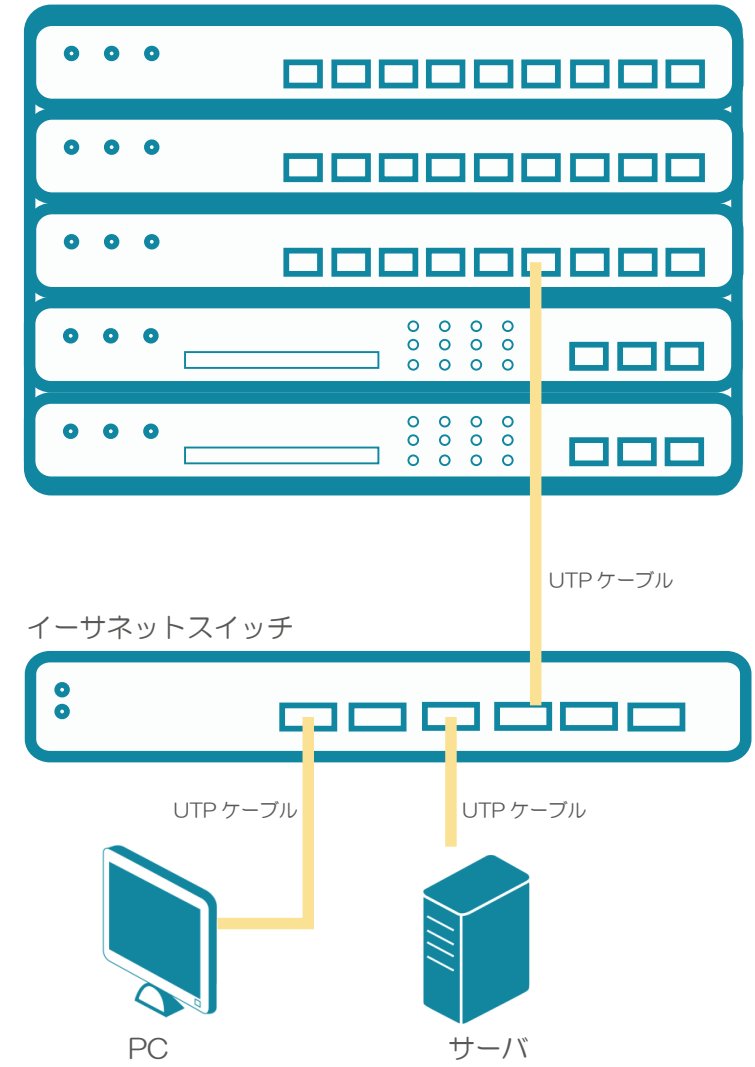


図 3-3　サーバ、PC、スイッチスタックとのアップリンク接続図

第 4 章　スイッチ管理について

管理オプション

本システムは Web インタフェース（Web ブラウザ）、DNA（D-Link Network Assistant）、コンソールポート（CLI）、Telnet や SNMP を使用し接続、管理することができます。

コマンドラインインタフェース（CLI）での管理

コンピュータやターミナルなどをコンソールポートに接続することにより、スイッチをアウトオブバンド方式で管理することが可能です。コマンドラインインタフェース（CLI）はすべてのスイッチの管理機能を提供します。LAN ポートで Telnet 接続をしている場合、インバンド方式でスイッチを管理することが可能です。CLI の詳細については CLI マニュアルを参照ください。

SNMP ベースでの管理

SNMP をサポートするコンソールプログラムでスイッチの管理をすることができます。本スイッチは、SNMP v1.0、v2c、および v3.0 をサポートしています。SNMP エージェントは、受信した SNMP メッセージを復号化し、マネージャからの要求に対してデータベースに保存された MIB オブジェクトを参照して応答を返します。SNMP エージェントは MIB オブジェクトを更新し、統計情報およびカウンタ情報を生成します。

Web ベースでの管理

本スイッチの設置完了後、Microsoft® Internet Explorer、Mozilla Firefox（最新バージョン）、Safari（最新バージョン）および Google Chrome（最新バージョン）によって本スイッチの設定、LED のモニタ、および統計情報をグラフィカルに表示することができます。

Web インタフェースでの管理

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/HTTPS（SSL）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。詳しくは「第 5 章　Web ベースのスイッチ管理」を参照ください。

DNA (D-Link Network Assistant) での管理

DNA（D-Link Network Assistant）は PC に接続している同じ L2 ネットワークセグメント内の Smart スイッチを検出、管理するためのプログラムです。DNA（D-Link Network Assistant）のダウンロード、インストールは手動で行います。詳しくは弊社製品ページの「DNA (ネットワーク簡易ツール) ユーザマニュアル」を参照ください。

コンソールポートの接続

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

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

端末をコンソールポートに接続する

1. 同梱の変換ケーブルのオス DB-9 コネクタを端末またはターミナルソフトが動作するコンピュータのシリアルコネクタに接続、次に RJ-45 コネクタをスイッチのコンソールポートに接続します。
2. 以下の手順でターミナルソフトを設定します。
3. 「接続の設定」画面の「接続方法」で、適切なシリアルポート（COM ポート）を選択します。
4. 選択したポートの「プロパティ」画面で「115200」ビット / 秒にデータ速度を設定します。
5. 「データビット」は「8」、「ストップビット」は「1」、「パリティ」は「なし」に設定します。
6. 「フロー制御」は「なし」に設定します。
7. 「エミュレーションモード」を「VT100」に設定します。
8. 「ファンクションキー」、「方向キー」、「Ctrl キー」の使い方で「ターミナルキー」を選択します。「ターミナルキー」（Windows キーではない）の選択を確認します。
9. 端末設定の完了後、本スイッチに電源ケーブルを接続し、電源プラグをコンセントに接続します。端末でブートシーケンスが始まります。

```
3 tests completed successfully
RedBoot> fis load -d managed
Image loaded from 0x80040000-0xB12d1d30
RedBoot> go

Press ENTER to get started
```

図 4-1　ブートシーケンス画面

10. ブートシーケンスが完了すると、コンソールのログイン画面が表示されます。
11. 購入後はじめてログインする場合は、ユーザ名（User Name）とパスワード（Password）プロンプトでそれぞれ「admin」を入力し、「Enter」キーを押します。既にユーザアカウントを作成している場合は、ユーザ名（User Name）とパスワード（Password）を入力してログインし、続けて本スイッチの設定をします。
12. コマンドを入力して設定を行います。コマンドの多くは管理者レベルのアクセス権が必要です。次のセクションでユーザアカウントの設定について説明します。CLI のすべてのコマンドリストおよび追加情報については、製品付属の CD-ROM に収録された「CLI Manual」を参照してください。
13. 管理プログラムを終了する場合は、logout コマンド使用するか、ターミナルソフトを終了します。
14. 接続する端末または PC が以上の通り設定されたことを確認してください。

端末上で接続に問題が発生した場合は、ターミナルソフトの設定で「エミュレーション」が「VT-100」となっていることを確認してください。「エミュレーション」は「ハイパーターミナル」画面の「ファイル」メニューから「プロパティ」をクリックし、「設定」タブにて設定します。何も表示されない場合はスイッチの電源を切り、再起動してください。コンソールに接続すると、コンソール画面が表示されます。ここでコマンドを入力し、管理機能を実行します。ユーザ名とパスワードの入力プロンプトが表示されます。

スイッチへの初回接続

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

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

スイッチに初めて接続すると、次の画面が表示されます。

```
                        DIS-200G-12PS/12PSW PoE GE Switch
                             Command Line Interface
                            Firmware: Build 1.20.B01
              Copyright © 2018 D-Link Corporation. All rights reserved.

User Access Verification

Username:
```

図 4-2　初回接続時の起動画面（ログイン画面）

初期値としてアカウント / パスワードはどちらも「admin」が設定されています。

注意　初期値のユーザアカウントは管理者レベルの権限が付与されています。少なくとも一つ以上の管理者権限ユーザが登録されている必要があります。

注意　セキュリティ上の理由から、スイッチ運用開始時には独自のアカウントとパスワードを設定してください。

ユーザアカウント作成 / パスワード設定

本スイッチは、初期値としてアカウント / パスワードは「admin」が設定されていて、その権限レベルは「15」です。ログイン後、新たにユーザアカウントの作成が可能になります。本スイッチに対する不正アクセスを防ぐためには、作成するアカウントに対して必ず固有のパスワードを定義し、このパスワードは忘れないように記録しておいてください。

管理者レベルのアカウントを作成するコマンド、手順は以下の通りです。

```
Switch>enable
Switch#configure terminal
Switch(config)#username user password pass1234
Switch(config)#
```

図 4-3　アカウント作成コマンド画面

1.「enable」コマンドを入力することで「Privileged EXEC」モードにアクセスします。「Enter」を押します。
2.「configure terminal」コマンドを入力することで「Global Configuration Mode」モードになります。「Enter」を押します。
3.「username User password 1234」コマンドを入力することで、ユーザ名 'User' を作成し、パスワード「1234」を指定します。「Enter」を押します。

注意　パスワードの大文字小文字は区別されます。ユーザ名、パスワードのどちらも 32 文字以内の半角英数字を指定してください。

4. CLI の設定コマンドは実行中の設定ファイルの編集でありスイッチが再起動した場合、設定は保存されません。設定内容変更の安全な保存については「copy running-config startup-config」コマンドを使用して実行中の設定ファイルをスタート時の設定ファイルとしてコピーする必要があります。

```
Switch# copy running-config startup-config
Building configuration…
% Saving 733 bytes to flash:startup-config
Switch#
```

図 4-4　「copy running-config startup-config」コマンド（スタート時の設定ファイルとしてコピー）画面

スイッチの再起動後、またはログアウト / ログイン後、新しく作成したユーザ名とパスワードが CLI インタフェースへのログインに必要になります。

```
DIS-200G Gigabit Ethernet Switch

Command Line Interface
Firmware: Build 1.20.001
Copyright (C) 2018 D-Link Corporation. All rights reserved.

User Access Verification

Username:user
Password:********

Switch#
```

図 4-5　CLI ログイン（ユーザ認証）画面

Telnet での接続

Telnet を使用した接続には「Telnet クライアント」が必要です。これは最初からオペレーションシステムに含まれているか、インターネットからダウンロードできます。スイッチへの接続前にお使いの PC がスイッチと同じネットワーク内の IP アドレスを設定されているか確認します。

1. Telnet ソフトウェアを使用し、スイッチの IP アドレスに接続します。
2. 初期値としてアカウント / パスワードはどちらも「admin」が設定されています。

SNMP での接続

本スイッチは「D-View」または他の SNMP 対応プログラムを使用しての管理が可能です。SNMP 機能は初期値で無効になっており、Web、DNA、CLI または Telnet などを使って有効にする必要があります。
D-View SNMP ネットワーク管理システムはネットワーク構築インフラストラクチャの中央管理に設計された、包括的な管理ツールです。D-View を使うことにより、障害対応、パフォーマンス、セキュリティなどに関する、効果的なデバイスの管理、設定を行うことが可能です。D-Link では 25 台までのデバイスを管理できる無料トライアル版を用意しています。詳しくは弊社 HP の製品情報をご確認ください。

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

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

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

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

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

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

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

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

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

トラップ

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

MIB

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

第 5 章　Web ベースのスイッチ管理

Web ベースの管理について

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

Web マネージャへのログイン

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

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

Web ベースユーザインタフェースに接続する :

1. Web ブラウザを開きます。

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

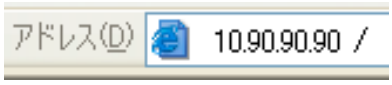


図 5-1　URL の入力

注意　工場出荷時設定では IP アドレス「10.90.90.90」、サブネットマスク「255.0.0.0」が設定されています。端末側の IP インタフェースを本スイッチに合わせるか、本スイッチを端末側の IP インタフェースに合わせてください。

3. ユーザ認証画面が表示されます。

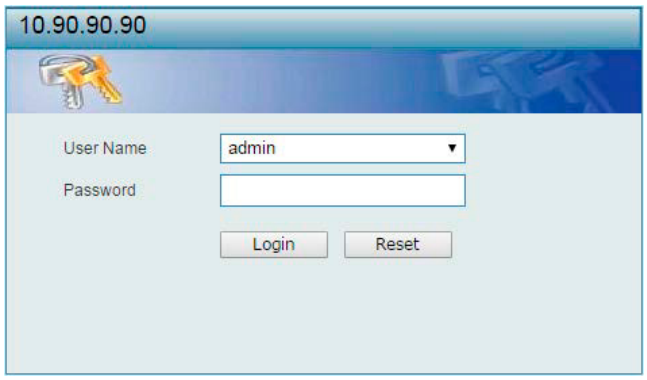


図 5-2　ユーザ認証画面

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

4. スマートウィザード画面が表示されます。

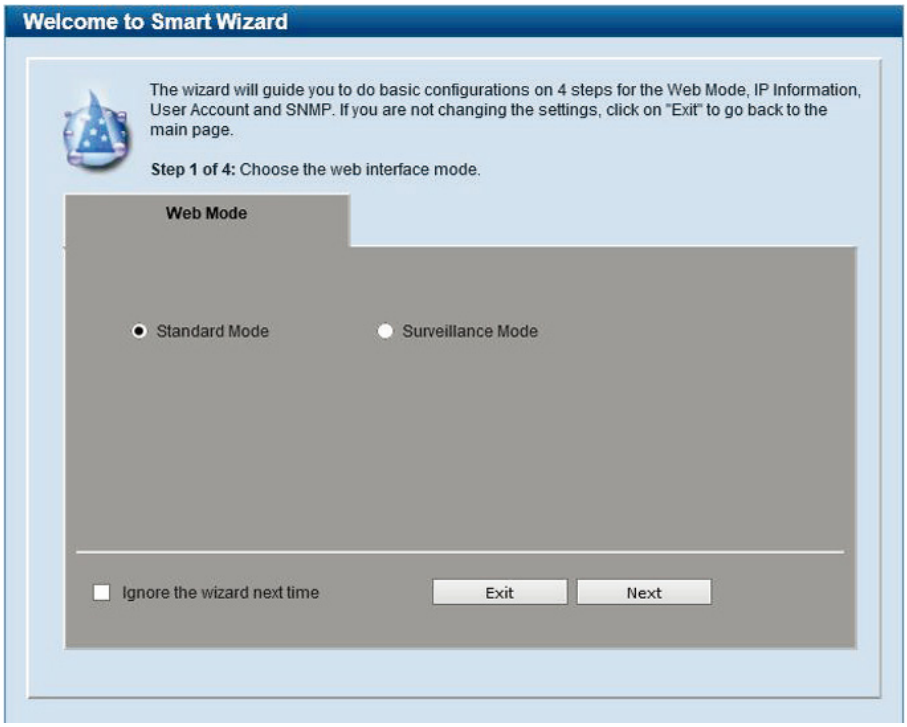


図 5-3　Smart Wizard 画面

ウィザード画面では、Web モードの選択や 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。

Smart Wizard 設定

「Smart Wizard」で Web モードの選択や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。

注意　Smart Wizard では、IPv4 アドレスのみ設定可能です。

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

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

Web モードの選択（Smart Wizard）

本スイッチは「Standard Mode（スタンダードモード）」と「Surveillance Mode（サーベイランスモード）」をサポートしています。スタンダードモードではソフトウェア機能の設定、管理、機能のモニタリングなどを行います。サーベイランスモードは本スイッチでサポートしている監視機能に関する設定に特化したモードです。

注意　Web モードの変更は Web UI へのログインが 1 ユーザの場合にのみ可能です。

1. Web モード「Standard Mode（スタンダードモード）」と「Surveillance Mode（サーベイランスモード）」から選択します。

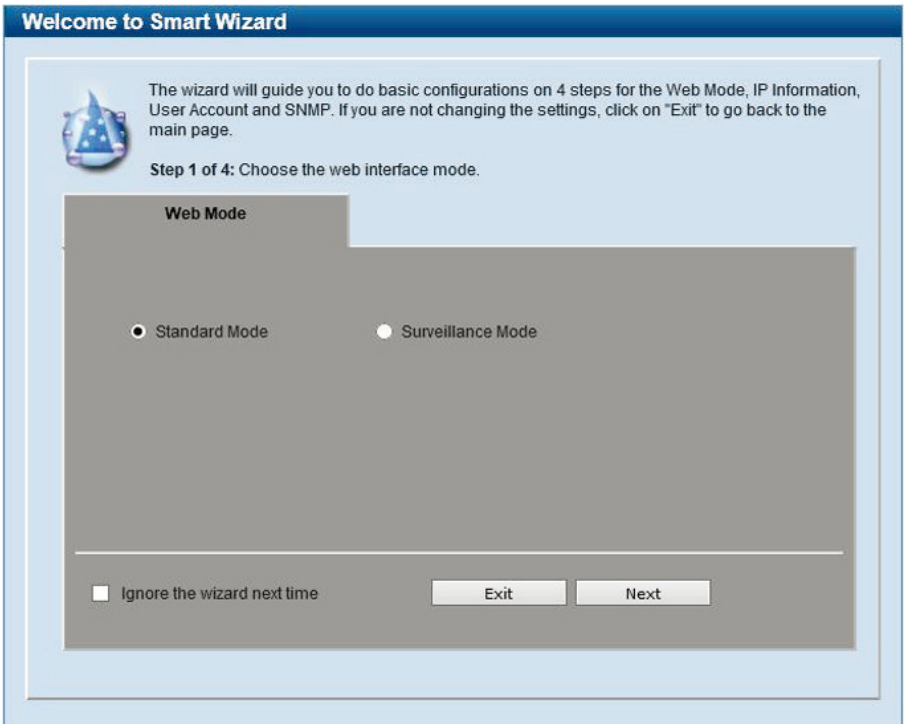


図 5-4　Web モード選択

1. 「Standard Mode（スタンダードモード）」と「Surveillance Mode（サーベイランスモード）」のいずれかをクリックします。
2. 「Next」をクリックします。

設定内容、変更を破棄し Web UI へ戻る場合は、「Exit」ボタンをクリックします。

IP アドレスの設定（Smart Wizard）

2. IP アドレスの設定を行います。

図 5-5　IP Information 設定画面

1. 「Static」「DHCP」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

   「Static」を選択した場合は、「IP Address」「Netmask」「Gateway」を入力します。
2. 「Next」をクリックします。

設定内容、変更を破棄し Web UI へ戻る場合は、「Exit」ボタンをクリックします。
前のページへ戻る場合は、「Back」ボタンをクリックします。

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

注意　スイッチはサーベイランスデバイスの確認を 30 秒毎で行います。サーベイランスデバイスがスイッチと同じサブネットにない場合、自動的に検出はされません。ONVIF カメラなどサーベイランス機器をサーベイランスモード WebUI に自動的に追加するためには、スイッチ管理 IP アドレスをそれらの機器と同様のサブネットにする必要があります。

ユーザアカウントの設定（Smart Wizard）

3. ユーザアカウント（admin）のパスワード設定を行います。

図 5-6　ユーザアカウント（admin）パスワード設定画面

以下の項目が表示されます。

項目	説明
Password	ユーザアカウントのパスワードを入力します。 「Confirm Password」で再度パスワードを入力します。

ユーザアカウント設定手順

1. 「Password」でパスワードを指定します。
2. 「Confirm Password」で再度パスワードを指定します。
3. 「Next」をクリックします。

設定内容、変更を破棄し Web UI へ戻る場合は、「Exit」ボタンをクリックします。
前のページへ戻る場合は、「Back」ボタンをクリックします。

SNMP の設定（Smart Wizard）

4. SNMP の設定を行います

図 5-7　SNMP 設定画面

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

設定内容、変更を破棄し Web UI へ戻る場合は、「Exit」ボタンをクリックします。
前のページへ戻る場合は、「Back」ボタンをクリックします。

Web ベースのユーザインタフェース

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

ユーザインタフェース内の各エリア（スタンダードモード）

Web ベースインタフェースの「Device Information」画面では以下の情報を参照することができます。Web マネージャのメイン画面は 3 つのエリアで構成されています。

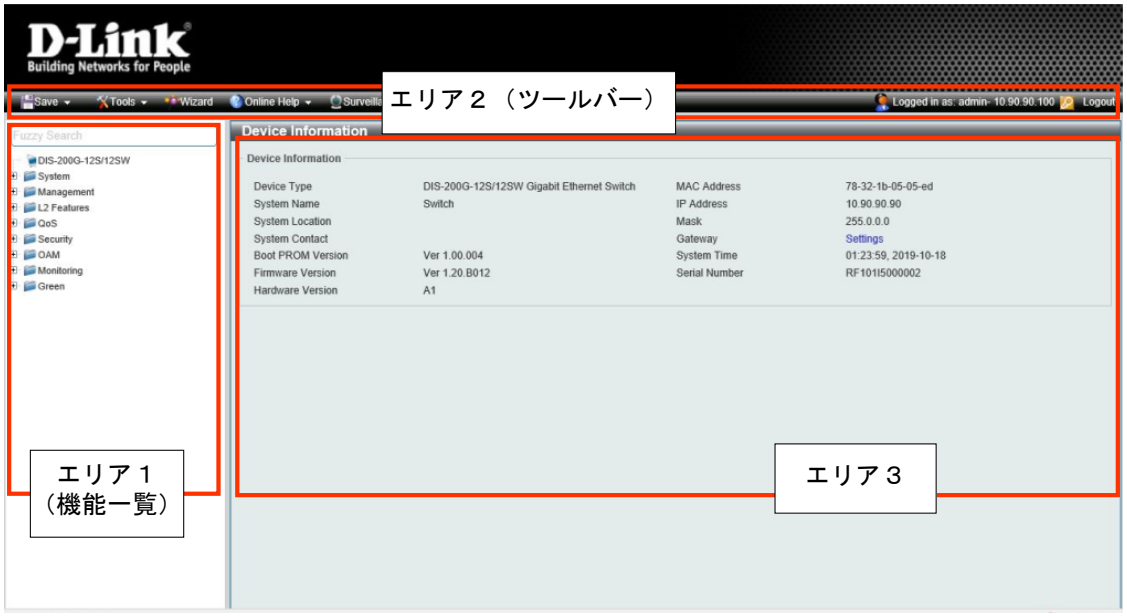


図 5-8　初期画面

エリア	機能
エリア 1 （機能一覧）	表示するメニューまたは画面を選択します。メニューアイコンを開いて、ハイパーリンクしたメニューボタンの表示やサブメニューを表示します。D-Link のロゴをクリックすると D-Link のホームページに接続します。
エリア 2 （ツールバー）	スイッチの再起動、コンフィグレーションのバックアップとリストア、ファームウェアの更新、設定の初期化を行う「Tools」メニューと設定の保存を行う「Save」メニューがあります。
エリア 3	選択したスイッチ情報の表示と設定データの入力を行います。

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

ユーザインタフェース内の各エリア（サーベイランスモード）

サーベイランスモードでの Web ベースインタフェースの初期画面では以下の情報を参照することができます。

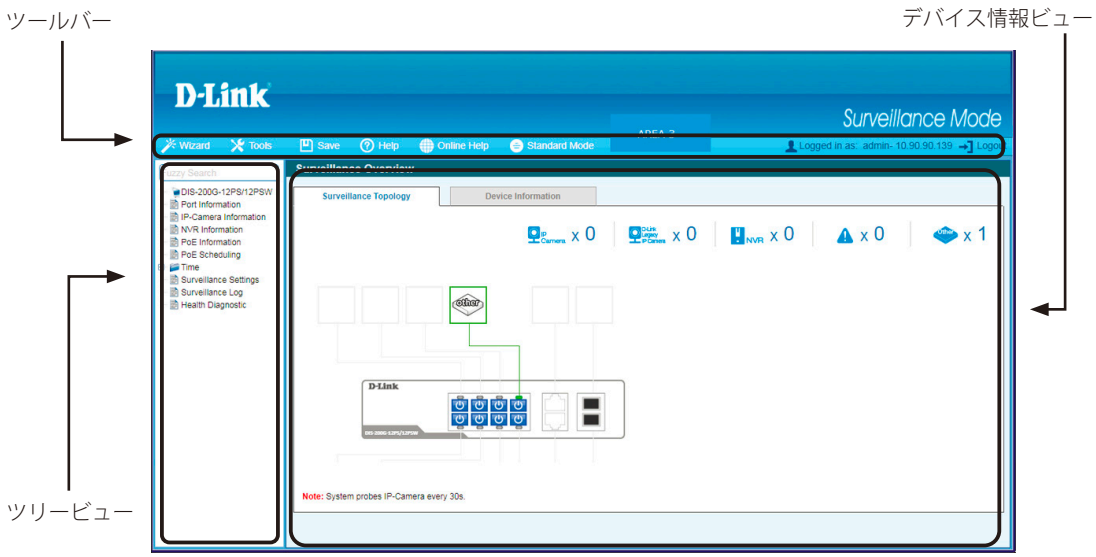


図 5-9　サーベイランスモード初期画面

次の表ではサーベイランスモード初期画面の主要な 3 つの領域について説明します。

ビュー	説明
ツールバー （メニュー情報ビュー）	「Save」、「Tools」メニューや、「Wizard」、「Help」「Online Help」、「Logout」ボタンを提供します。また、言語情報や IP 情報、ログインユーザ名も表示します。「Standard Mode」をクリックするとスタンダードモードへ移行します。
ツリービュー	システムの機能、設定オプションごとに分類して表示します。 表示されているフォルダか画面を選択します。フォルダアイコンを開くことにより、ハイパーリンクメニューボタンやさらにその下のサブフォルダを表示することができます。
デバイス情報ビュー	ツリービューで選択した項目が表示されます。デバイス情報ビューはスイッチの情報、テーブル、設定について表示します。

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。
Tools	Firmware Information	ファームウェアの情報を表示します。
	Firmware Upgrade & Backup	ファームウエアのアップグレードとバックアップをします。
	Configuration Restore & Backup	コンフィグレーションのリストアとバックアップをします。
	Log Backup	ログファイルのバックアップをします。
	Ping	Ping を実行します。
	Reset	機器をリセットします。
	Reboot System	システムの再起動を行います。
機能一覧		
製品名	Device Information	スイッチの主な設定情報を表示します。
System	System Information Settings	スイッチの基本情報を表示します。
	Port Configuration	ポート設定、ジャンボフレーム設定などを行います。
	PoE（DIS-200G-12PSW のみ）	PoE システムの設定を行います。
	System Log	スイッチのログを保存する方法、Syslog サーバの設定を行います。
	Time	スイッチに時刻を設定します。
	Time Profile	スイッチのタイムプロファイルを設定します。
Management	User Accounts Settings	ユーザアカウントの作成と設定を行います。
	Password Encryption	パスワードを暗号化し設定ファイルに保存します。
	SNMP Settings	SNMP を利用してゲートウェイ、ルータ、およびその他のネットワークデバイスの設定状態を確認または変更します。
	RMON	SNMP 機能に対するリモートモニタリング (RMON) の設定を行います。
	Telnet	スイッチの Telnet 接続について設定します。
	HTTP/HTTPS	スイッチの Web 設定を行います。
	D-Link Discovery Protocol	D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。
L2 Features	FDB	スタティック FDB、MAC アドレステーブルなどを設定します。
	VLAN	VLAN 表示、設定を行います。
	Spanning Tree	スパニングツリーの設定を行います。
	ERPS (G.8032)	ERPS（Ethernet Ring Protection Switching）の設定を行います。
	Loopback Detection	ループバック検知設定を行います。
	Link Aggregation	複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用します。
	L2 Multicast Control	L2 マルチキャストコントロールの設定を行います。
	LLDP	LLDP（Link Layer Discovery Protocol）の設定を行います。
QoS	802.1p Priority	802.1p Priority ではポートに default CoS 設定を行います。
	Port Rate Limiting	ポートレート制限の設定を行います。
	Port Trust State	ポートトラスト設定と表示を行います。
	DSCP CoS Mapping	DSCP CoS マップの設定と表示を行います。
Security	Port Security	ポートセキュリティ機能の設定と表示を行います。
	802.1X	IEEE 802.1X 認証の設定を行います。
	RADIUS	RADIUS の設定と表示を行います。
	Web-based Access Control	Web-based Access Control（Web 認証）の設定、表示を行います。
	Safeguard Engine Settings	セーフガードエンジン設定を行います。
	Traffic Segmentation	トラフィックセグメンテーション設定を行います。
	Storm Control	ストームコントロールの設定を行います。
	DoS Attack Prevention Settings	DoS 攻撃防止設定を行います。
	Zone Defense Settings	ゾーンディフェンスの設定を行います。
	SSH	SSH の設定を行います。
	SSL	SSL（Secure Socket Layer）の設定を行います。
OAM	Cable Diagnostics	ケーブル診断を行います。
	DDM	Digital Diagnostic Monitoring（DDM）機能の設定、表示を行います。

メインメニュー	サブメニュー	説明
Monitoring	Statistics	パケット統計情報とエラー統計情報を表示します。
	Mirror Settings	ポートミラーリングの設定を行います。
Green	Power Saving	機器の省電力設定を行います。
	EEE	Energy Efficient Ethernet/ 省電力イーサネットの設定を行います。

第 6 章　System（システム設定）

本章ではデバイス情報の確認、IP アドレスの設定、ポートパラメータの設定、システムログの設定と管理、システム時刻の設定について説明します。

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

サブメニュー	説明
Device Information（デバイス情報）	スイッチの主な設定情報を表示します。
System Information Settings（システム情報 ）	スイッチの基本情報を表示します。
Port Configuration（ポート設定）	ポート設定、ジャンボフレーム設定などを行います。
PoE（PoE の管理）（DIS-200G-12PSW のみ）	PoE システムの設定を行います。
System Log（システムログ）	スイッチのログを保存する方法、Syslog サーバの設定を行います。
Time（時間設定）	スイッチに時刻を設定します。
Time Profile（タイムプロファイル設定）	スイッチのタイムプロファイルを設定します。

Device Information（デバイス情報）

ログイン時に自動的に表示されるスイッチの主な機能の設定内容です。他の画面から「Device Information」画面に戻るためには、「DIS-200G-12PS/12PSW」をクリックします。
「Device Information」画面にはデバイスの一般的な情報として設定する項目があります。これには、システム名、場所、接続、システム MAC アドレス、システム稼働時間、IP アドレス、ファームウェア、ブート、およびハードウェアのバージョン情報などが含まれます。

ツリービューの製品名（例：DIS-200G-12PS/12PSW）をクリックし、以下の画面を表示します。

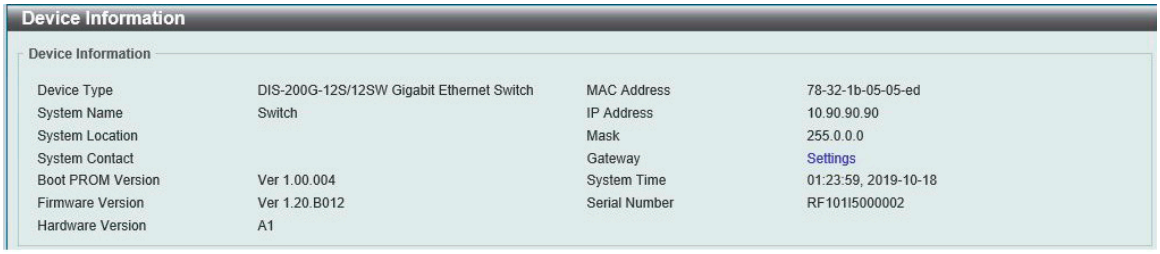


図 6-1　Device Information 画面

「Device Information」画面には以下の項目があります。

機能	設定方法
Device Information	
Device Type	工場にて定義した機種名と型式を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。
System Contact	システムコンタクトを表示します。
Boot PROM Version	デバイスのブートバージョンを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
Hardware Version	デバイスのハードウェアバージョンを表示します。
MAC Address	デバイスに割り当てられた MAC アドレスを表示します。
IP Address	デバイスに割り当てられた IP アドレスを表示します。
Mask	デバイスに割り当てられたサブネットマスクを表示します。
Gateway	デバイスに割り当てられたデフォルトゲートウェイを表示します。
System Time	デバイスに割り当てられた現在時刻を表示します。
Serial Number	デバイスのシリアル番号を表示します。

System Information Settings（システム情報

System Information

システム情報を提供します。

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

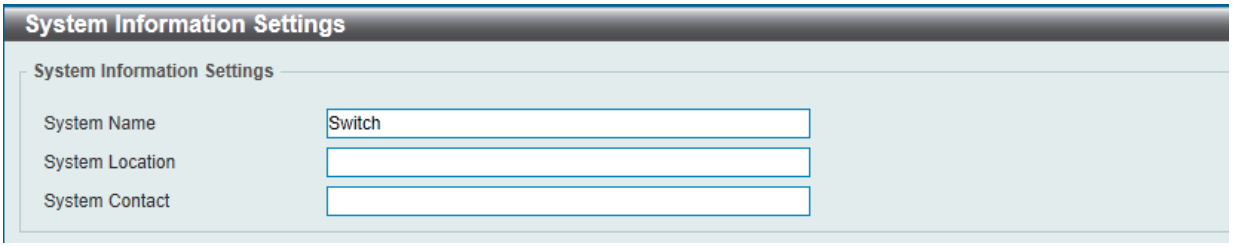


図 6-2　System Information Settings 画面

画面には以下の項目があります。

項目	説明
System Name	ユーザが定義するシステム名を設定します。
System Location	システムが現在動作している場所を定義します。（半角英数字 255 文字以内）
System Contact	担当者名を表示します。（半角英数字 255 文字以内）

「Apply」ボタンをクリックすると設定が更新されます。

IPv4 Interface（IPv4 インタフェース）

IPv4 インタフェースの設定をします。

System > System Information Settings > IPv4 Interface の順にクリックし、以下の画面を表示します。

図 6-3　IPv4 Interface 画面

画面には以下の項目があります。

項目	説明
Get IP From	IP アドレスの取得について指定します。 「DHCP」を選択すると自動的に IP アドレスを取得します。「Static」を選択すると手動で IP アドレスを指定します。
IP Address	「Static」を選択した場合、表示される空欄に IP アドレスを入力します。 「DHCP」を選択した場合、自動的に取得した IP アドレスが表示されます。
Mask	「Static」を選択した場合、表示される空欄にマスクを入力します。 「DHCP」を選択した場合、自動的に取得したマスクが表示されます。
Gateway	「Static」を選択した場合、表示される空欄にゲートウェイを入力します。 「DHCP」を選択した場合、自動的に取得したゲートウェイが表示されます。
DHCP retry Time (5 ～ 120)	「DHCP」を選択した場合、IP アドレスの取得までのリトライの回数を指定します。

「Apply」ボタンをクリックすると設定が更新されます。

IPv6 Interface（IPv6 インタフェース）

IPv6 インタフェースの設定をします。

System > System Information Settings > IPv6 Interface の順にクリックし、以下の画面を表示します。

図 6-4　IPv6 Interface 画面

画面には以下の項目があります。

項目	説明
IPv6 State	IPv6 を有効 / 無効にします。有効にした場合、IPv6 リンクローカルアドレスは管理 VLAN に自動的にアサインされます。 無効で固定 IPv6 アドレスを設定していない場合、スイッチの IPv6 関連機能は使用できません。
Static IPv6 Address	有効にした場合、表示される空欄に IPv6 アドレスを入力します。

「Apply」ボタンをクリックすると設定が更新されます。

Port Configuration（ポート設定）

各ポートの設定を行います。

Port Settings（ポート設定）

デバイスのポートの詳細説明を設定します。

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

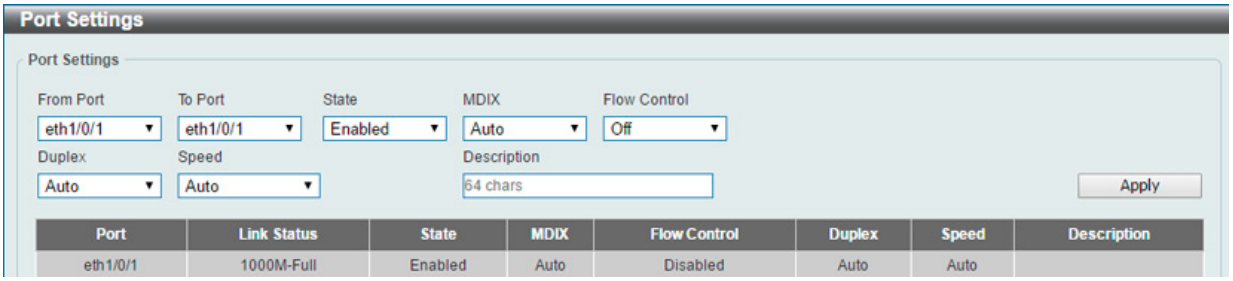


図 6-5　Port Settings 画面

画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート範囲を設定します。
State	物理ポートの有効 / 無効を指定します。 • Enabled - 選択した物理ポートが有効です。 • Disabled - 選択した物理ポートが無効です。
MDIX	• Auto - 最適なケーブル接続を自動的に設定します。 • Normal - ケーブル接続に Normal を選択します。 • Cross - ケーブル接続に Cross を選択します。 「Normal」を選択すると、MDI モードにあるポートはストレートケーブルを通して PC のネットワークボード、またはクロスケーブルで別のスイッチのポート（MDI モード）に接続することができます。「Cross」を選択すると、MDIX モードにあるポートはストレートケーブルで別のスイッチのポート (MDI モード) に接続することができます。
Flow Control	Full-Duplex では 802.3x フローコントロールを、Half-Duplex ではバックプレッシャーによる制御を自動で行います。「On」（フロー制御あり）または「Off」（フロー制御なし）を選択します。「Auto」は自動的にいずれかを使用します。
Duplex	全二重 / 半二重モードの選択を行います。「Auto」「Half」「Full」から選択します。
Speed	「Speed」欄でポートの速度を選択します。ここでは指定したポートを指定した速度のみで接続するように手動で設定します。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 オプションには「Auto」「10M」「100M」「1000M」があります。「Auto」以外のオプションのポート設定は固定となります。
Description	関連のポートについて 64 文字以内に概要を指定します。

「Apply」ボタンをクリックすると設定が更新されます。

Jumbo Frame（ジャンボフレーム設定）

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。ジャンボフレームは、1518 バイト以上のペイロードを持つイーサネットフレームです。本スイッチは最大 9600 バイトまでのジャンボフレームをサポートします。「Jumbo Frame」画面では、スイッチでジャンボフレームを扱うことを可能にします。これによりオーバヘッド、処理時間、割り込みを確実に減らすことができます。

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

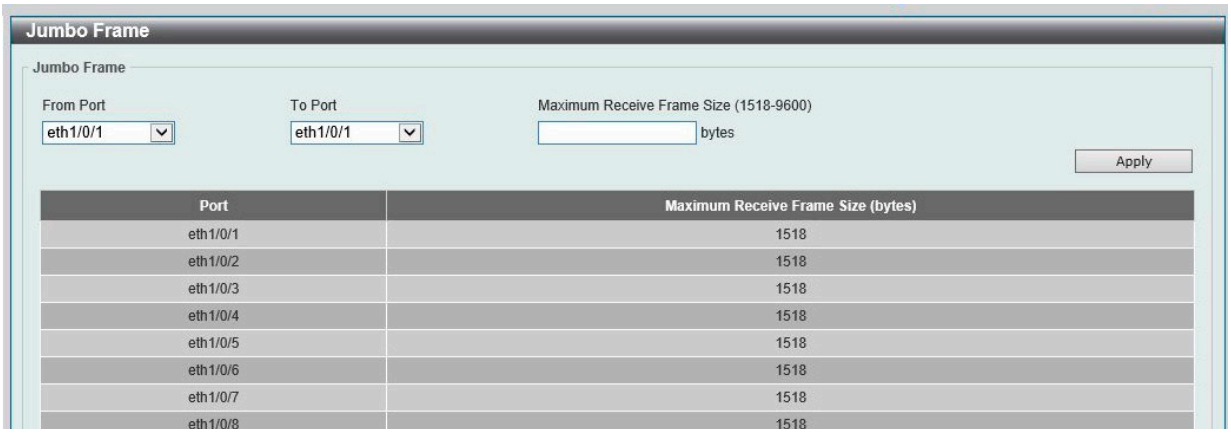


図 6-6　Jumbo Frame 画面

画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート範囲を設定します。
Maximum Receive Frame Size	受信する最大フレームサイズ（1518 - 9600/Byte）を指定します。初期値は 1518Bytes です。

「Apply」ボタンをクリックすると設定が更新されます。

PoE（PoE の管理）（DIS-200G-12PSW のみ）

DIS-200G-12PSW は IEEE の 802.3af と IEEE802.3at 規格の PoE 機能をサポートしています。対応ポートは 30W まで PoE をサポートしています。カテゴリ 5 以上の UTP イーサネットケーブル経由で PoE 受電機器に電力を供給できます。本スイッチは PSE pinout Alternative A に準拠しており、電力はピン 1、2、3、および 6 を通じて供給されます。本スイッチは全ての D-Link 802.3af/at 対応デバイスと接続できます。
本スイッチでは次の PoE 機能を使用することができます。

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

図 6-7802.3af/at 準拠の受電機器の最大受信電力一覧：

クラス	受電機器の最大受信電力
0	12.95W
1	3.84W
2	6.49W
3	12.95W
4	25.5W

図 6-8PSE により提供される最大電力一覧：

クラス	給電機器の最大提供電力
0	15.4W
1	4.0W
2	7.0W
3	15.4W
4	30W

PoE System（PoE システム設定）

デバイスの PoE 情報を参照および変更します。

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

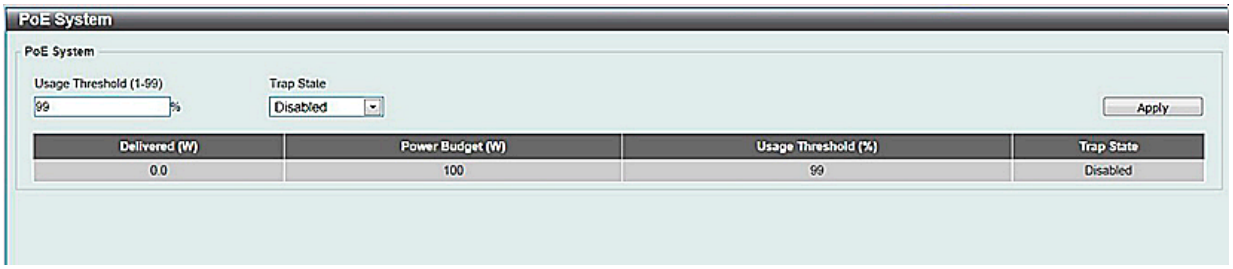


図 6-9　PoE System 画面

画面には以下の項目があります。

項目	説明
Usage Threshold	ログの記録や通常の通知送信を実行するしきい値を指定します。1 から 99（%）で指定できます。
Trap State	PoE の通知送信について有効 / 無効を指定します。

「Apply」ボタンをクリックすると設定が更新されます。

PoE Status（PoE ステータス）

各ポートの PoE ステータスの表示を行います。

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

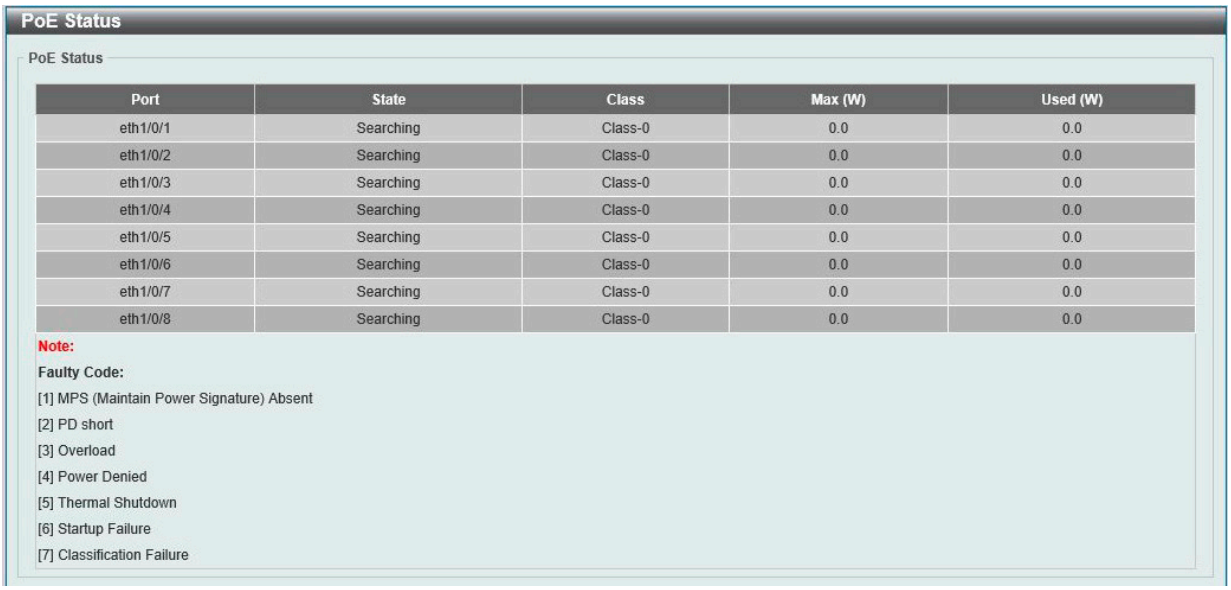


図 6-10　PoE Status 画面

PoE の状態が表示されます。

PoE Configuration（PoE ポート設定）

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

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

図 6-11　PoE Configuration 画面

画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート範囲を設定します。
Priority	プルダウンメニューを使ってポートの優先度（Critical、High、Low）を指定します。 ポート優先度はシステムがどのポートに優先的に電力供給を行うかを設定します。優先度には 3 段階あり「Critical」「High」「Low」で設定できます。
Power Limit	PoE ポートの電力管理モードを選択します。「Auto」「Never」から指定できます。
Time Profile	ポートの PoE 機能を有効にする時間設定を行います。名称と時間を指定します。ポートは設定した時間内のみ給電を行います。ドロップダウンに表示される「Time Profile」は事前に設定する必要があります。Time Profile の作成については「Time Profile（タイムプロファイル設定）」を参照ください。

「Delete Time Profile」ボタンをクリックすると指定の時間設定が削除されます。
「Apply」ボタンをクリックすると設定が更新されます。

PD Alive（PoE アライブ）

PoE ポートに接続した PD についての PD アライブ機能について説明します。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。

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

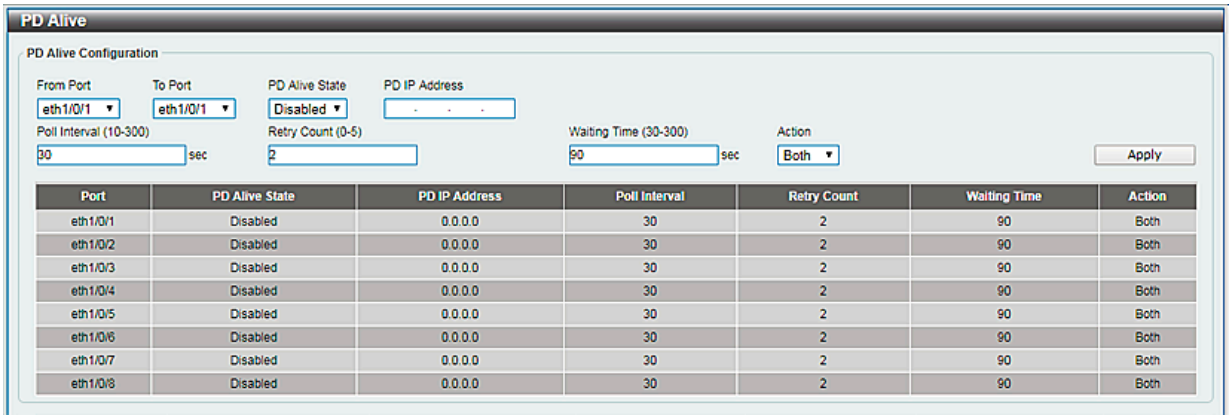


図 6-12　PD Alive 画面

画面には以下の項目があります。

項目	説明
From Port/To Port	本設定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。10-300（秒）になります。
Retry Count	リトライカウントを指定します。PD が無反応の場合に再度「Ping」を送信する回数を指定します。0 から 5 になります。
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。30-300（秒）になります。
Action	動作を指定します。「Reset」「Notify」「Both」から指定します。. • Reset - PoE ポートをリセットします。（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 ポートをリセット（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。

「Apply」ボタンをクリックすると設定が更新されます。

System Log（システムログ）

System Log Settings（システムログ設定）

スイッチのシステムログ設定を行います。

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

図 6-13　System Log Settings 画面

System Log Settings 画面には次の項目があります。

Global State（グローバルステート）

項目	説明
System Log	システムログ機能をグローバルに有効 / 無効に指定します。

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

Buffer Log Settings（バッファログ設定）

項目	説明
Buffer Log State	「Enabled」「Disabled」から選択します。

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

System Log Server Settings（システムログサーバ設定）

システムログサーバの表示、設定を行います。

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

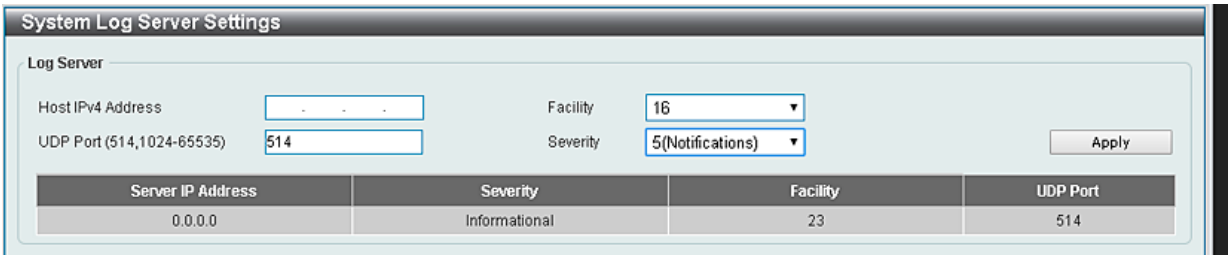


図 6-14　System Log Server 画面

本画面には次の項目があります。

項目	説明
Host IPv4 Address	ログを記録するサーバの IPv4 アドレスを設定します。
UDP Port	ログを送信するサーバの UDP ポートを設定します。初期値は 514 です。 値は「514」、または「1024」から「65535」で指定します。
Facility	ログ送信対象（Facility）をプルダウンメニューを使用して「16」から「23」までの間を選択します。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。 「3(Errors)」（エラー）、「4(Warnings)」（警告）、「5(Notification)」（通知）、「6(Informational)」（情報）から選択します。

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

System Log（システムログの設定）

システムログの閲覧 / 消去を行います。

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

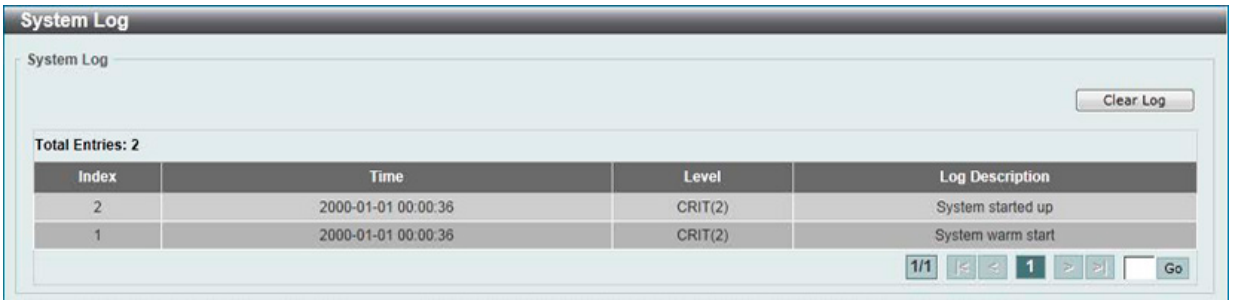


図 6-15　System Log 画面

「Clear Log」ボタンをクリックして、表示画面内のすべてのエントリをクリアします。

Time（時間設定）

SNTP（Simple Network Time Protocol）は、スイッチの時間をネットワークの時間と同期させるために使用されます。国 / 地域時刻へのアクセス、サーバ / クライアントの SNTP サブネットの設定、システム時刻の調整を行う包括的なメカニズムです。

Clock Settings（時間設定）

スイッチの時間設定を行います。

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

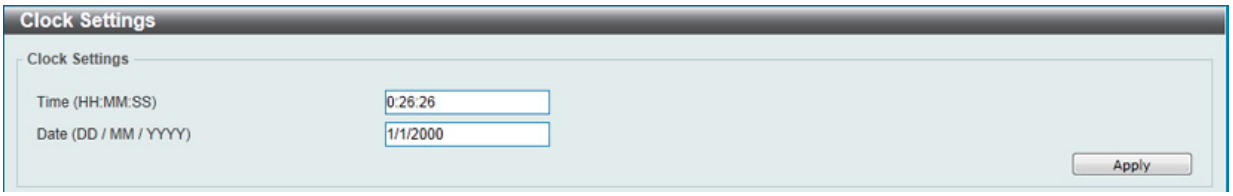


図 6-16　Clock Settings 画面

画面には以下の項目があります。

項目	説明
Time (HH:MM:SS)	現在時刻を入力します。（時 / 分 / 秒）
Date (DD / MM / YYYY)	現在の日付を入力します。（日 / 月 / 年）

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

TimeZone Settings（タイムゾーン設定）

SNTP 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。

System > Time > Time Zone Settings の順にメニューをクリックし、以下の設定画面を表示します。

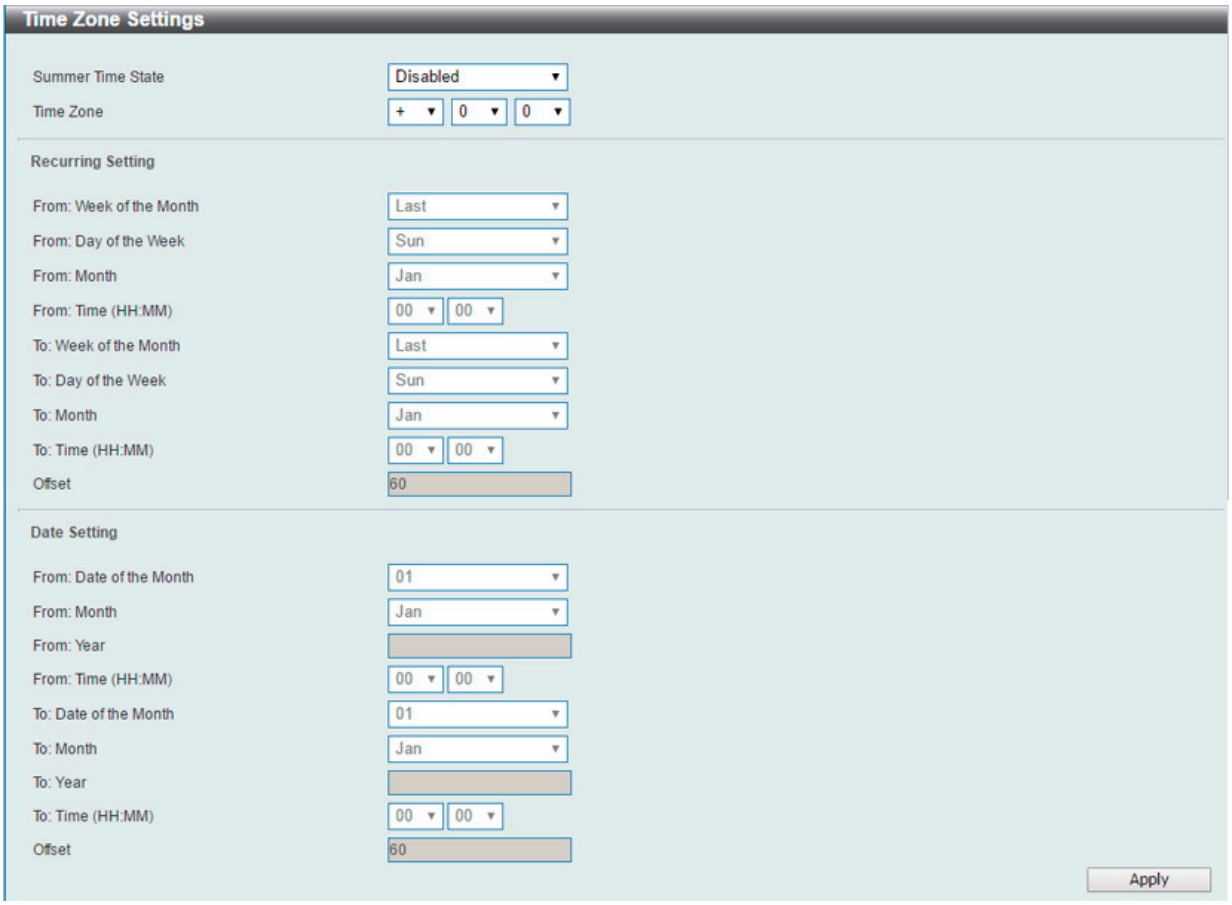


図 6-17　TimeZone Settings 画面

以下に、画面の各項目を示します。

項目	説明
Summer 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） • Recurring Setting - サマータイムを週指定で有効にします。このオプションでは開始と終了の月と曜日を設定する必要があります。 • Date Setting - サマータイムを日付指定で有効にします。このオプションでは開始と終了の日付を設定する必要があります。
Time Zone	UTC（ユニバーサル時間）からのタイムゾーンを選択します。
Recurring Setting	
From: Week of the Month	サマータイムが始まる週を指定します。
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: Month	サマータイムが開始する月を指定します。
From: Time (HH:MM)	サマータイムが開始する時間を指定します。
To: Week of the Month	サマータイムが終了する週を指定します。
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: Month	サマータイムが終了する月を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。初期値は 60（分）です。 オフセットの範囲は「30」「60」「90」「120」から選択可能です。
Date Setting	
From: Date of the Month	サマータイムが始まる日を指定します。
From: Month	サマータイムが開始する月を指定します。（毎年）
From: Year	サマータイムが開始する年を指定します。（毎年）
From: Time In HH MM	サマータイムが開始する時間を指定します。（毎年）

項目	説明
To: Date of the Month	サマータイムが修了する日を指定します。
To: Month	サマータイムが終了する月を指定します。（毎年）
To: Year	サマータイムが終了する年を指定します。（毎年）
To: Time In HH MM	サマータイムが終了する時間を指定します。（毎年）
Offset	サマータイムに追加する時間を指定します。初期値は 60（分）です。 オフセットの範囲は「30」「60」「90」「120」から選択可能です。

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

SNTP Settings（SNTP 設定）

スイッチに時刻を設定します。

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

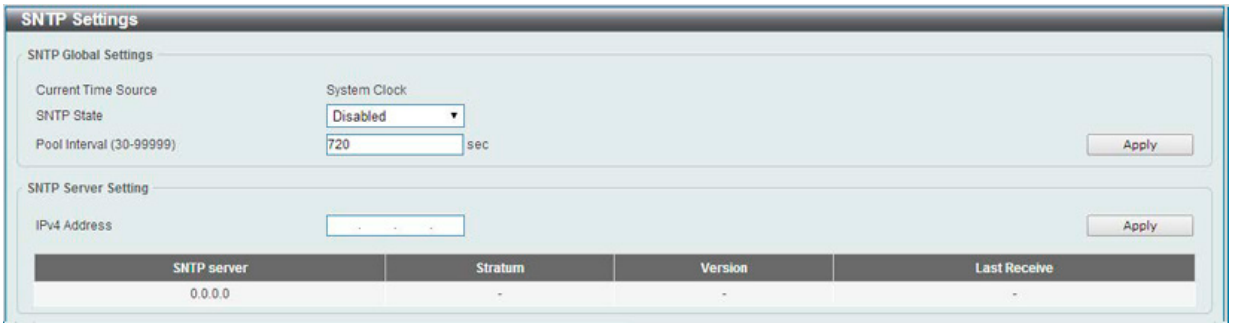


図 6-18　SNTP Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
SNTP Global Settings	
SNTP State	SNTP を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Pool Interval	同期する間隔（秒）を指定します。 「30」から「99999」（秒）で指定します。 初期値は「720 秒」です。
SNTP Server Settings	
IPv4 Address	SNTP 情報の取得元であるサーバの IP アドレスを設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Add」をクリックして SNTP サーバを追加します。
「Delete」をクリックして指定のエントリを削除します。

Time Profile（タイムプロファイル設定）

スイッチのタイムプロファイルを設定します。作成できるタイムプロファイルの数は 4 つです。

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

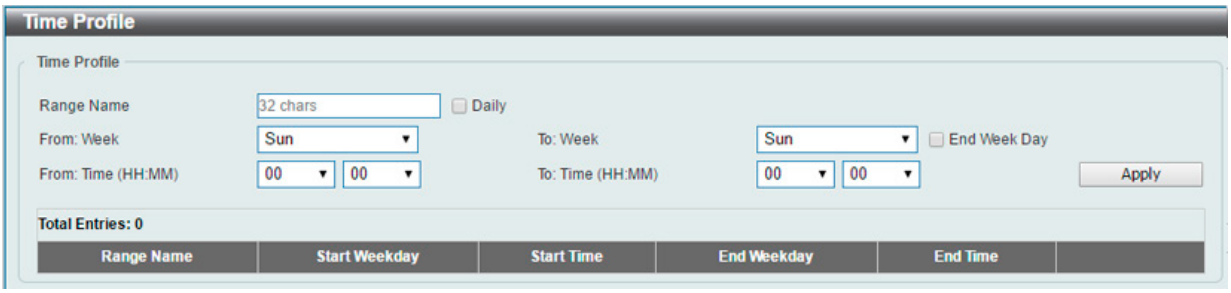


図 6-19　Time Range 画面

以下の項目を設定することができます。

項目	説明
Range Name	タイムレンジを識別するために使用する名前を半角英数字 32 文字以内で入力します。
From Week / To Week	タイムレンジに使用する「始まり」と「終わり」の曜日を指定します。 「Daily」にチェックを入れると「毎日」がタイムレンジとして指定されます。 「End Week Day」にチェックを入れると「始まり」に指定された日から週の最後（日曜日）までがタイムレンジになります。
From Time / To Time	タイムレンジに使用する「始まり」と「終わり」の時間を指定します。ドロップダウンメニューから時間と分を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
関連情報を入力して「Find」ボタンをクリックすると指定のエントリを検索できます。

エントリの削除
削除するエントリ横の「Delete」ボタンをクリックすると該当エントリは削除されます。

第 7 章　Management（スイッチの管理）

本章でスイッチの管理を行います。

以下は、Management サブメニューです。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
User Accounts Settings （ユーザアカウント設定）	ユーザアカウントの作成と設定を行います。有効なユーザアカウントを表示可能です。
Password Encryption（パスワード暗号化）	パスワードを暗号化し設定ファイルに保存します。
SNMP（SNMP 設定）	SNMP を利用してゲートウェイ、ルータ、およびその他のネットワークデバイスの設定状態を確認または変更するための設定を行います。
RMON（RMON 設定）	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。
Telnet（Telnet 設定）	スイッチの Telnet 接続について設定します。
HTTP/HTTPS（HTTP/HTTPS 設定）	スイッチの Web 設定を行います。
D-Link Discovery Protocol （D-Link ディスカバリプロトコル）	D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

User Account Settings（ユーザアカウント設定）

ユーザアカウントの設定を行います。有効なユーザアカウントが表示可能です。

注意　工場出荷時の設定では、「Read/Write」権限を持つ「admin」アカウントが用意されています。

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

図 7-1　User Accounts Settings 画面

画面には次の項目があります。

項目	説明
User Name	ユーザ名を定義します。（半角英数字 32 文字以内）
Privilege	アカウントの権限レベルを指定します。「Read-Only」「Read-Write」から選択します。
Password	アカウントで使用するパスワード（32 字以内）を入力します。

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

エントリの削除
削除するエントリ横の「Delete」ボタンをクリックすると該当エントリは削除されます。

Password Encryption（パスワード暗号化）

パスワードを暗号化して設定ファイルに保存します。

Management > Password Encryption の順にクリックし、次の画面を表示します。

図 7-2　Password Encryption 画面

画面には次の項目があります。

項目	説明
Password Encryption State	コンフィグファイル保存時のパスワード暗号化を有効 / 無効を設定します。
Password Type	パスワード暗号化を有効すると、次のオプションが選択可能です。 • Encrypted-SHA1 -「 SHA-1」を使用してパスワードを暗号化します。 • Encrypted-MD5 -「 MD-5」を使用してパスワードを暗号化します。

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

SNMP（SNMP 設定）

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

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

本スイッチは、SNMP バージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）をサポートしています。初期設定では SNMP 機能は無効になっているため、有効にする必要があります。SNMP 機能を有効にしたら、スイッチの監視と制御に使用する SNMP バージョンを選択します。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

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

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

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

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

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

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

トラップ

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

MIB

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

DIS-200G シリーズは、スイッチの環境に合わせた柔軟性のある SNMP 管理機能を採用しています。SNMP 管理機能は、ネットワークの要求やネットワーク管理者の好みに合わせてカスタマイズすることができます。SNMP バージョンの選択は、「SNMP Group Table」で行うことができます。

DIS-200G シリーズは、SNMP バージョン 1、2c、および 3 をサポートします。管理者は、スイッチの監視と制御にどの SNMP バージョンを使用するかを指定できます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

SNMP 設定は、Web マネージャの「SNMP」フォルダ下のメニューから行います。「Management Station IP Address」メニューを使用して、SNMP 権限を持ちスイッチへのアクセスを許されたワークステーションに制限を設けることも可能です。

SNMP Global Settings（SNMP グローバル設定）

SNMP グローバル設定とトラップ設定を行います。

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

図 7-3　SNMP Global Settings 画面

以下の項目が使用されます。

SNMP Global Settings（SNMP グローバル設定）

項目	説明
SNMP Global State	「SNMP」機能の有効 / 無効を選択します。

Trap Settings（トラップ設定）

項目	説明
Trap Global State	「SNMP」トラップを有効 / 無効にします。
SNMP Authentication Trap	SNMP 認証失敗の通知送信の設定を行います。認証失敗トラップ（authenticationFailuretrap）は、機器が正しく認証されていない SNMP メッセージを受信した時に実行されます。認証方法は SNMP のバージョンによって違います。SNMPv1 または SNMPv2c の場合、認証失敗はパケットが不正確なコミュニティ文字列で構成している場合に発生します。
Port Link Up	ポートリンクアップ通知送信の設定を行います。リンクアップトラップは機器がリンクアップを認識すると実行します。
Port Link Down	ポートリンクダウン通知送信の設定を行います。リンクダウントラップは機器がリンクダウンを認識すると実行します。
Coldstart	コールドスタート（coldStart）通知送信の設定を行います。
Warmstart	ウォームスタート（warmStart）通知送信の設定を行います。

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

SNMP View Table Settings（SNMP ビューテーブル）

コミュニティ名に対しビュー（アクセスできる MIB オブジェクトの集合）を割り当て、リモート SNMP マネージャがどの MIB オブジェクトにアクセスするかを定義するために使用します。

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

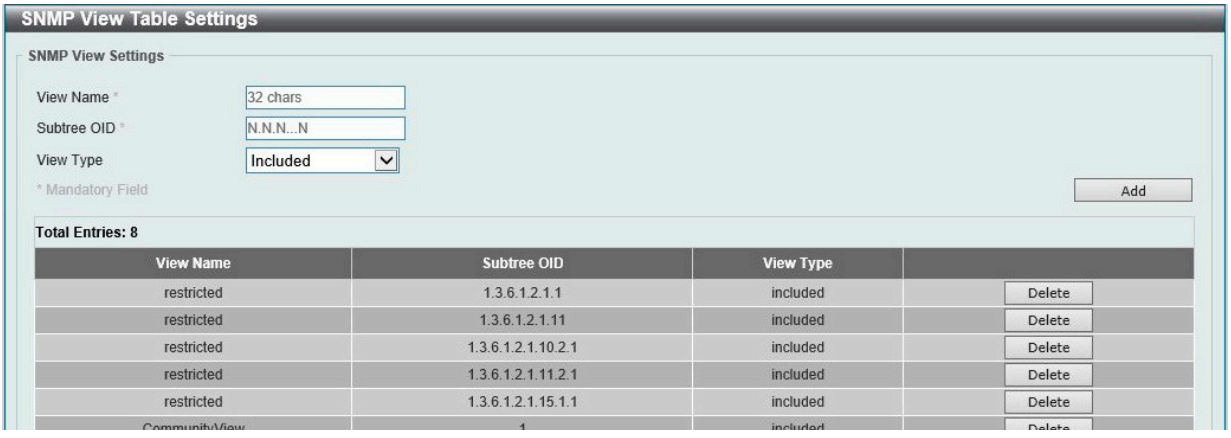


図 7-4　SNMP View Table 画面

エントリの削除

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

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

以下の項目が使用されます。

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

SNMP Community Table Settings（SNMP コミュニティテーブル設定）

「SNMP Community Table」は、SNMP コミュニティ名を登録し、SNMP マネージャとエージェントの関係を定義するために使用します。コミュニティ名は、スイッチ上のエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。

- SNMP コミュニティにアクセス可能な MIB オブジェクトが Read/Write または Read-only レベルである。

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

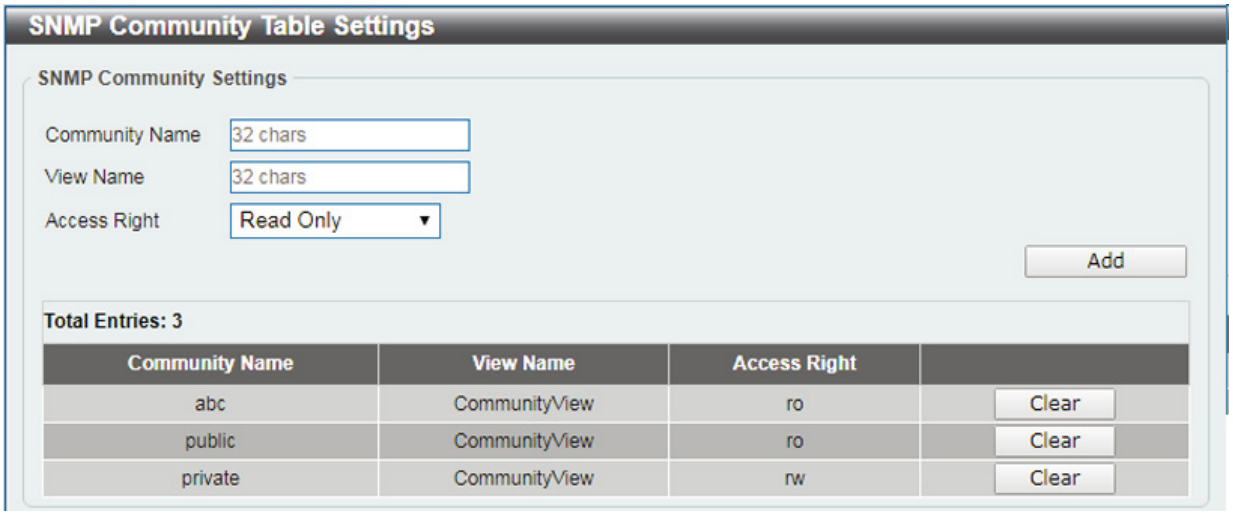


図 7-5　SNMP Community Table 画面

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

項目	説明
Community Name	32 文字までの半角英数字を入力し、SNMP コミュニティメンバを識別します。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
View Name	32 文字までの半角英数字を入力します。本値は、リモート SNMP マネージャがアクセスすることのできる MIB グループの定義に使用します。View Name は SNMP View Table に存在する必要があります。
Access Right	• Read Only - 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りのみ可能となります。 • Read Write - 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取り、および書き込みが可能です。

エントリの作成
新しいエントリを作成するためには、上記テーブルに情報を入力し、「Add」ボタンをクリックします。
エントリの削除
削除するエントリ横の「Clear」ボタンをクリックし、エントリを削除します。

SNMP Group Table Settings（SNMP グループテーブル設定）

SNMP グループを登録します。本グループは、SNMP ユーザ（「SNMP User Table」で設定）と「SNMP View Table」で設定するビューを関連付けます。

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

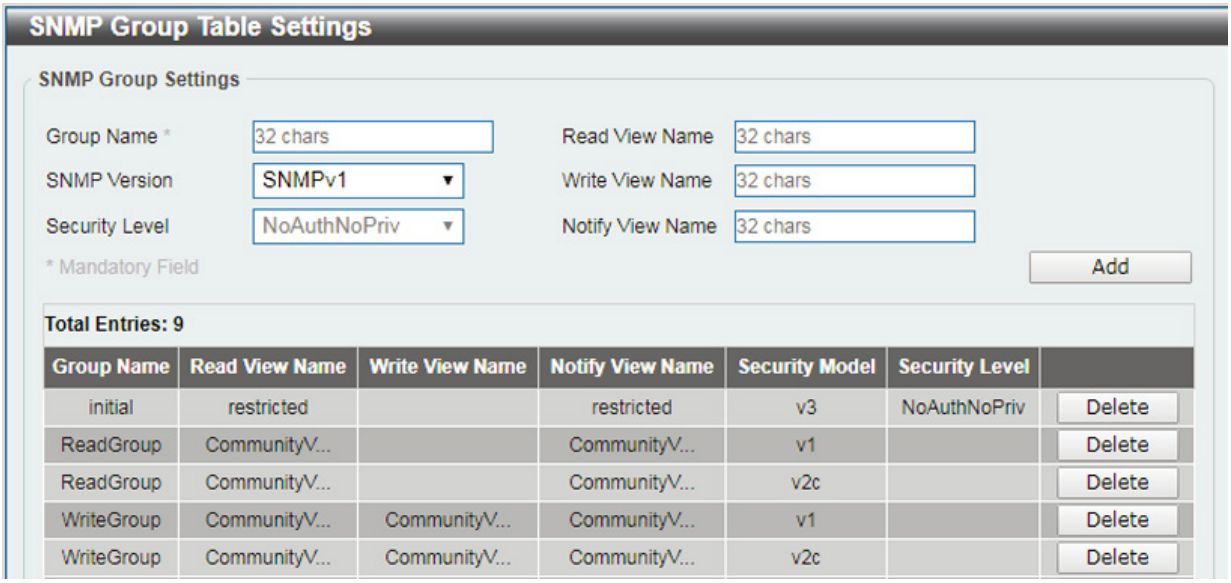


図 7-6　SNMP Group Table 画面

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

「SNMP Group Table」画面への新規エントリの追加
上記画面に情報を入力し、「Add」ボタンをクリックします。

以下の項目が使用されます。

項目	説明
Group Name	32 文字までの半角英数字を入力します。SNMP ユーザのグループの識別に使用します。
SNMP Version	• SNMPv1 - SNMP バージョン 1 が使用されます。 • SNMPv2c - SNMP バージョン 2c が使用されます。SNMP バージョン 2 は集中型、分散型どちらのネットワーク管理にも対応します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。 • SNMPv3 - SNMP バージョン 3 が使用されます。ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。
Security Level	セキュリティレベル設定は SNMP バージョン 3 にのみ適用されます。 • NoAuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットは認証も暗号化もされません。 • AuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化なしになります。 • AuthPriv - スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化ありになります。
Read View Name	グループユーザがアクセス可能な読み取りビュー名を入力します。
Write View Name	グループユーザがアクセス可能な書き込みビュー名を入力します。
Notify View Name	グループユーザがアクセス可能な通知ビュー名を入力します。 Notify View はトラップパケットを介してステータスをグループユーザにレポートすることができるオブジェクトです。

SNMP Engine ID Local Settings（SNMP エンジン ID ローカル設定）

エンジン ID は、SNMP バージョン 3 で使用される場合に定義される固有の識別名です。識別名は半角英数字の文字列で表記され、スイッチ上の SNMP エンジン（エージェント）を識別するために使用します。
スイッチの SNMP エンジン ID を表示します。

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

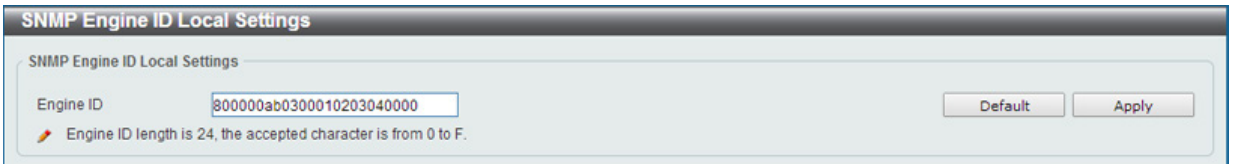


図 7-7　SNMP Engine ID 画面

エンジン ID を変更するためには、「Engine ID」に新しいエンジン ID（24 字以内）を入力し、「Apply」ボタンをクリックします。
「Default」をクリックするとエンジン ID は初期値に戻ります。

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

スイッチに現在設定されているすべての SNMP ユーザが表示されます。

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

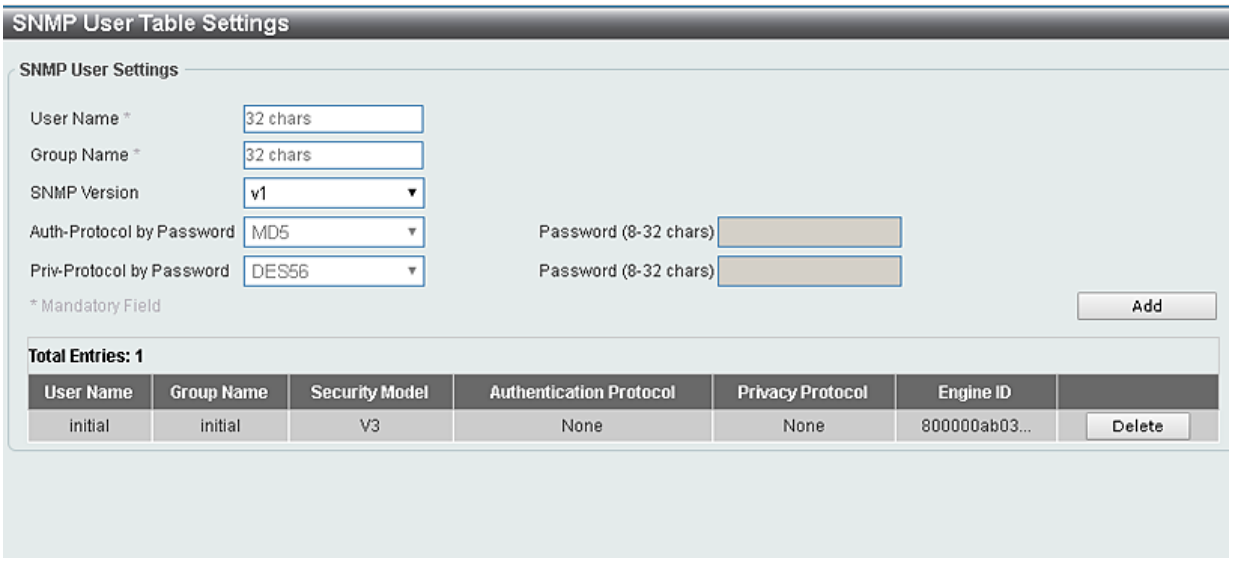


図 7-8　SNMP User Table 画面

エントリの削除
エントリの行の「Delete」ボタンをクリックします。

エントリの新規登録
新規エントリを追加するためには、上記画面に情報を入力し、「Add」ボタンをクリックします。

上記画面中の項目を以下に示します。

項目	説明
User Name	32 文字までの半角英数字で SNMP ユーザ名を指定します。
Group Name	作成した SNMP グループが SNMP メッセージを要求するために使用される名前です。
SNMP Version	• v1 - SNMP バージョン 1 が使用されます。 • v2c - SNMP バージョン 2 が使用されます。 • v3 - SNMP バージョン 3 が使用されます。
Auth-Protocol by Password	本項目は「SNMP Version」で「v3」を選択した場合に有効になります。本項目を選択後、「Password」にパスワードを入力します。 • MD5 - HMAC-MD5-96 認証レベルが使用されます。「Password (8-32 chars)」にパスワードを入力します。 • SHA - HMAC-SHA 認証プロトコルが使用されます。「Password (8-40 chars)」にパスワードを入力します。
Priv-Protocol by Password	本項目は「SNMP Version」で「v3」を選択した場合に有効になります。 • None - 認証プロトコルは使用されません。 • DES56 - CBC-DES（DES-56）標準に基づく DES56 ビット暗号化方式が使用されます。本項目を選択後、「Password (8-32 chars)」にパスワードを入力します。

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

SNMP トラップの送信先を登録します。

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

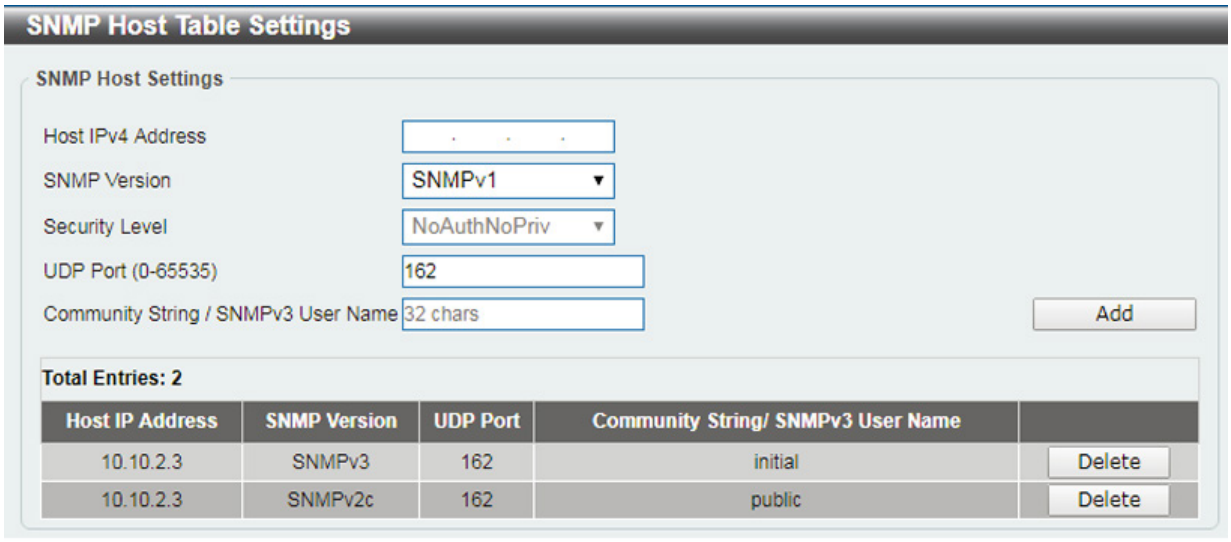


図 7-9　SNMP Host Table 画面

エントリの新規登録

スイッチの SNMP ホストテーブルに新しいエントリを追加するためには、上記画面に情報を入力し、「Apply」ボタンをクリックします。

以下の項目を設定します。

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
SNMP Version	• SNMPv1 : SNMP バージョン 1 が使用されます。 • SNMPv2c : SNMP バージョン 2c が使用されます。 • SNMPv3 : SNMP バージョン 3 が使用されます。
Security Level	「User-based Security Model」で「SNMPv3」を指定した場合、次のオプションを選択します。 • NoAuthNoPriv - リモート SNMP マネージャーとスイッチ間において認証 / パケット暗号化が適用されません。 • AuthNoPriv - リモート SNMP マネージャーとスイッチ間において認証が必要ですが、パケット暗号化は適用されません。 • AuthPriv - リモート SNMP マネージャーとスイッチ間において認証 / パケット暗号化は適用されます。
UDP Port	UDP ポート番号を入力します。UDP ポート番号の初期トラップは 162 です。UDP ポート範囲は 0 から 65535 です。いくつかのポート番号は他のプロトコルと衝突する可能性があります。
Community String/ SNMPv3 User Name	コミュニティ名または SNMP V3 ユーザ名を入力します。

エントリの削除

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

RMON（RMON 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。

RMON Global Settings（RMON グローバル設定）

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

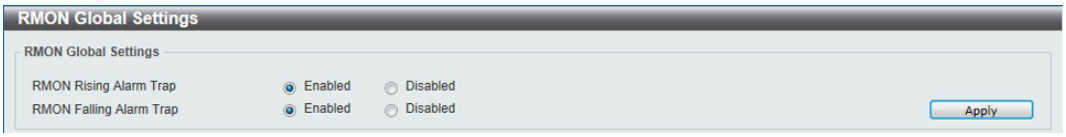


図 7-10　RMON Global Settings 画面

以下の項目が使用されます。

項目	説明
RMON Rising Alarm Trap	「RMON」における上昇しきい値警告トラップを有効にします。しきい値の設定は「RMON Alarm Settings（RMON アラーム設定）」で行います。
RMON Falling Alarm Trap	「RMON」における下降しきい値警告トラップを有効にします。しきい値の設定は「RMON Alarm Settings（RMON アラーム設定）」で行います。

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

RMON Statistics Settings（RMON 統計情報）

RMON 統計情報を表示、設定します。

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

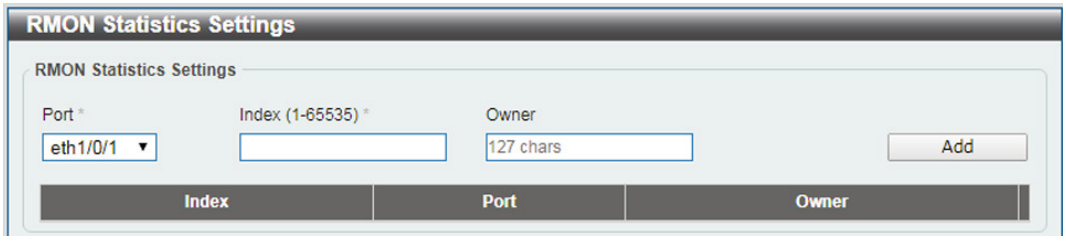


図 7-11　RMON Statistics Settings 画面

以下の項目が使用されます。

項目	説明
Port	RMON 情報を取得したポートを指定します。
Index (1 - 65535)	RMON イーサネット統計情報エントリの番号を指定します。
Owner	オーナ名（文字列）を 127 字までで指定します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

統計情報の削除を行う場合

「Delete」をクリックします。

指定ポートの統計情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

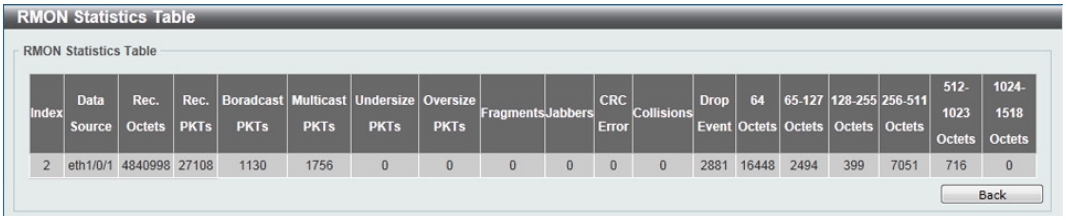


図 7-12　RMON Statistics Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

RMON History Settings（RMON ヒストリ設定）

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

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

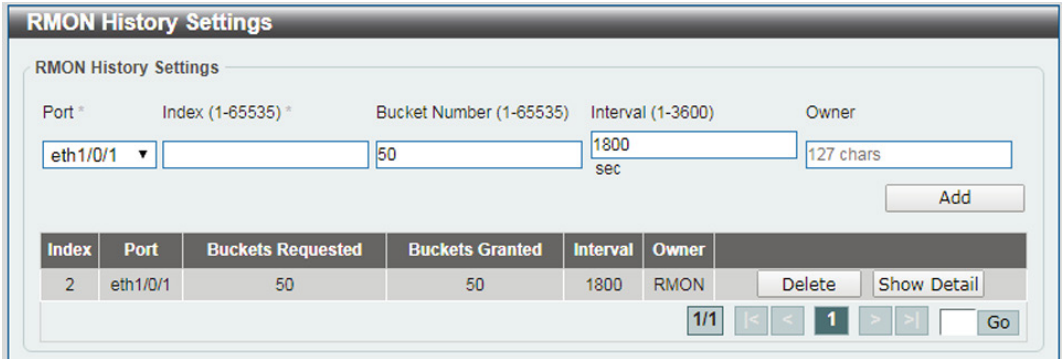


図 7-13　RMON History Settings 画面

以下の項目が使用されます。

項目	説明
Port	RMON ヒストリを取得するポートを指定します。
Index (1 - 65535)	インデックス番号を指定します。（1-65535）
Bucket Number	統計の RMON 取得履歴グループに指定するバケット数（1-65535）を指定します。初期値は 50 です。
Interval (1-3600)	ポーリング間隔（秒）を設定します。 初期値：1800 (秒) 入力可能範囲：1-3600 (秒)
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

履歴情報の登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

履歴情報の削除を行う場合

「Delete」をクリックします。

指定ポートの履歴情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

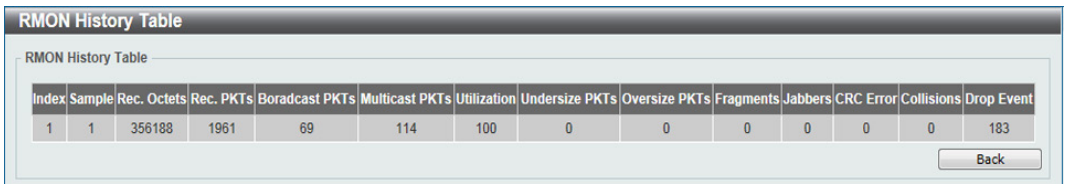


図 7-14　RMON History Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

RMON Alarm Settings（RMON アラーム設定）

インタフェースをモニタする設定を行います。

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

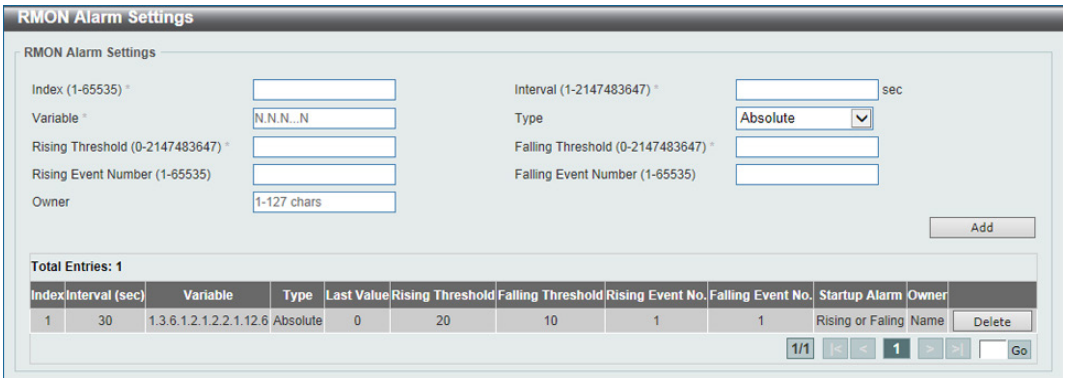


図 7-15　RMON Alarm Settings 画面

以下の項目が使用されます。

項目	説明
Index (1-65535)	アラームインデックスを入力します。（1-65535）
Interval	変数のサンプリングと閾値を確認する間隔を秒で指定します。1 から 2147483647（秒）の間で指定可能です。
Variable	サンプリングする変数のオブジェクト識別子を入力します。
Type	モニタリングタイプを選択します。
Rising Threshold	上昇しきい値を設定します。0 から 2147483647（秒）の間で指定可能です。
Falling Threshold	下降しきい値を設定します。0 から 2147483647（秒）の間で指定可能です。
Rising Event Number (1-65535)	上昇しきい値を超えたときに始動するイベントを設定します。 1 から 65535（秒）の間で指定可能です。指定しない場合は、上限閾値を上回ってもアクションをとりません。
Falling Event Number (1-65535)	下降しきい値を超えたときに始動するイベントのインデックスを入力します。 1 から 65535 から指定します。指定しない場合は、下限閾値を下回ってもアクションをとりません。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

「Delete」をクリックします。

RMON Event Settings（RMON イベント設定）

RMON イベントに関する設定と参照を行います。

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

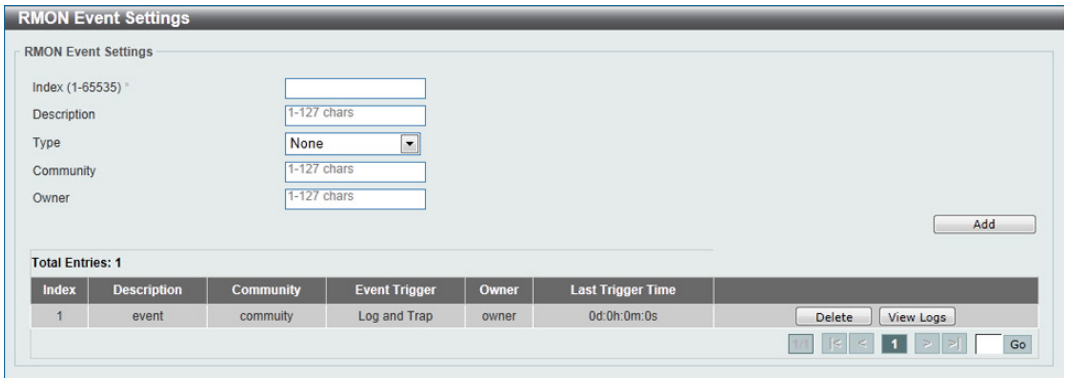


図 7-16　RMON Event Settings 画面

以下の項目が使用されます。

項目	説明
Index (1-65535)	イベントを指定します。
Description	RMON イベントエントリの説明を入力します。最大 127 文字までです。
Type	RMON イベントエントリタイプを選択します。 選択肢：「None」「Log」「Trap」「Log and Trap」 • None - イベントが発生しなかったことを示します。 • Log - イベントがログエントリであることを示します。 • Trap - イベントがトラップであることを示します。 • Log and Trap - イベントがログエントリとトラップの両方であることを示します。
Community	イベントが所属するコミュニティを指定します。127 文字まで入力可能です。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

「Delete」をクリックします。

指定エントリのログ情報を表示する場合

「View Logs」をクリックします。以下の画面が表示されます。

図 7-17　Event Logs Table 画面

「Back」をクリックすると前ページへ移動します。

Telnet（Telnet 設定）

スイッチの Telnet 設定を行います。

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

図 7-18　Telnet 画面

以下の項目が使用されます。

項目	説明
Telnet State	Telnet 機能の有効 / 無効を選択します。

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

補足　Telnet の最大セッション数は 4 となります。

HTTP/HTTPS（HTTP/HTTPS 設定）

スイッチに Web 設定をします。

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

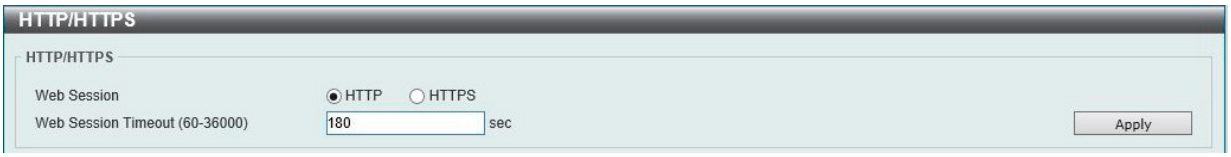


図 7-19　HTTP/HTTPS 画面

以下の項目が使用されます。

項目	説明
Web Session	HTTP または HTTPS 経由の Web ベースマネジメントを指定します。
Web Session Timeout	Web セッションのタイムアウト時間（秒）を設定します。60 から 36000（秒）で設定可能です。初期値は 180 秒です。

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

D-Link Discovery Protocol（D-Link ディスカバリプロトコル）

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

Management > D-Link Discovery Protocol の順にメニューをクリックし、以下の画面を表示します。

図 7-20　D-Link Discovery Protocol 画面

設定には以下の項目を使用します。

項目	説明
D-Link Discovery Protocol	
D-Link Discovery Protocol State	DDP をグローバルに有効にします。
Report Timer	DDP レポートメッセージの送信間隔（秒）を指定します。「30」「60」「90」「120」「Never」から指定できます。

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

第 8 章　L2 Features（レイヤ 2 機能の設定）

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

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

サブメニュー	説明
FDB（FDB 設定）	スタティック FDB、MAC アドレステーブルなどを設定します。
VLAN（VLAN 設定）	VLAN 表示、設定を行います。
Spanning Tree（スパニングツリーの設定）	スパニングツリーの設定を行います。
ERPS (G.8032)（イーサネットリングプロテクション設定）	ERPS (G.8032)（イーサネットリングプロテクション設定）の設定を行います。
Loopback Detection（ループバック検知設定）	ループバック検知設定を行います。
Link Aggregation（リンクアグリゲーション）	複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用します。
L2 Multicast Control（L2 マルチキャストコントロール）	L2 マルチキャストコントロールの設定を行います。
LLDP（LLDP 設定）	LLDP（Link Layer Discovery Protocol）の設定を行います。

FDB（FDB 設定）

Static FDB（スタティック FDB 設定）

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

スタティックユニキャスト転送の設定を行います。

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

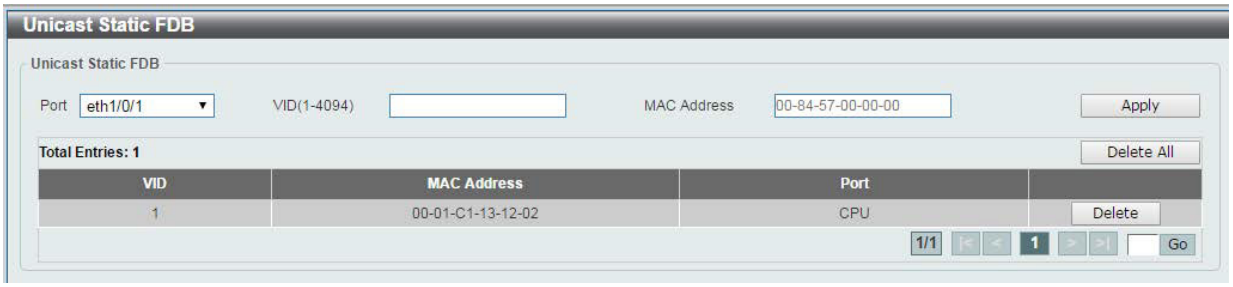


図 8-1　Unicast Static FDB 設定

画面には以下の項目があります。

項目	説明
Port	入力した MAC アドレスの存在するポートを指定します。
VID	ユニキャスト MAC アドレスのある VLAN リストを入力します。
MAC Address	パケットを手動で転送、または破棄するユニキャスト MAC アドレスを指定します。

項目を設定後、「Apply」ボタンをクリックし、デバイスに設定を適用します。
「Delete」をクリックすると指定のエントリを、「Delete All」ですべてのエントリを削除します。

Multicast Static FDB（マルチキャストスタティック FDB 設定）

スタティックマルチキャスト転送の設定を行います。

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

図 8-2　Multicast Static FDB 設定

画面には以下の項目があります。

項目	説明
From Port / To Port	ポートの始点 / 終点を設定します。
VID	関連の MAC アドレスが属する VLAN の VLAN ID です。
MAC Address	手動で転送（スタティックフォワーディング）するマルチキャストパケットの MAC アドレスを入力します。 MAC アドレスのフォーマットは 01-XX-XX-XX-XX-XX になります。

項目を設定後、「Apply」ボタンをクリックし、デバイスに設定を適用します。
「Delete」をクリックすると指定のエントリを、「Delete All」ですべてのエントリを削除します。

MAC Address Table Settings（MAC アドレステーブル設定）

スイッチに MAC アドレスエージングタイムを設定します。

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

Global Settings（グローバル設定タブ）

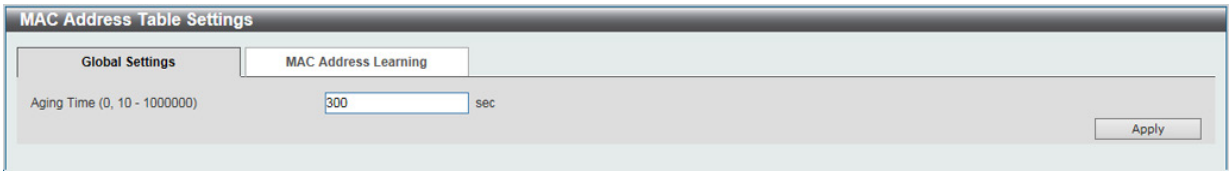


図 8-3　MAC Address Table Settings (Global Settings) 画面

以下の項目を使用して設定を行います。

項目	説明
Aging Time (0, 10-1000000)	MAC アドレステーブルのエージング時間を入力します。（10-1000000 秒）

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

MAC Address Learning（MAC アドレスラーニング設定タブ）

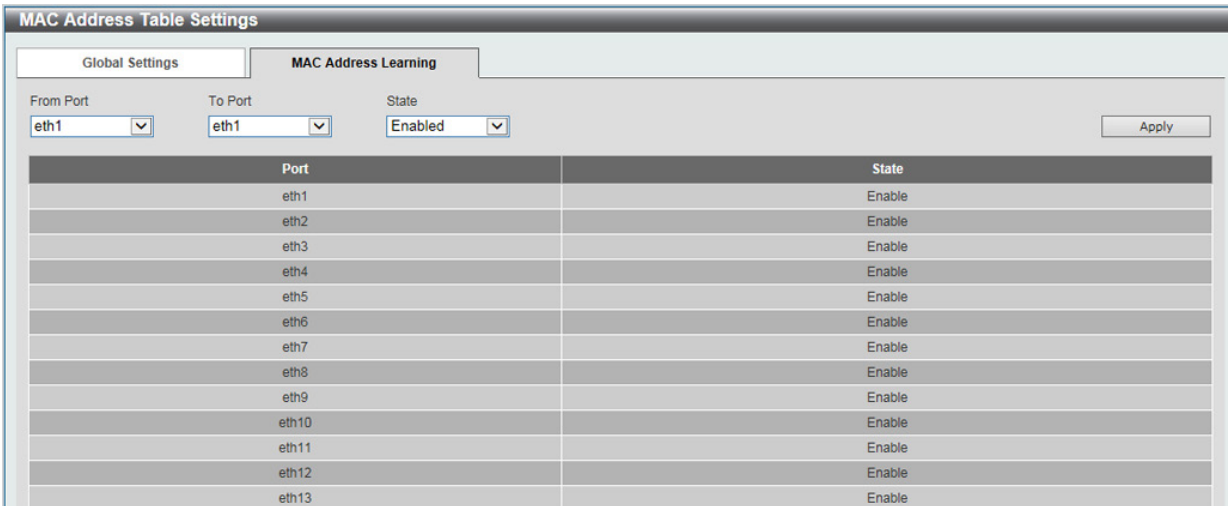


図 8-4　MAC Address Table Settings (MAC Address Learning) 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
From Port / To Port	ポートの始点 / 終点を設定します。
State	MAC アドレスラーニングを有効 / 無効にします。

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

MAC Address Table（MAC アドレステーブル）

MAC アドレステーブル内のエントリリストの表示を行います。

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

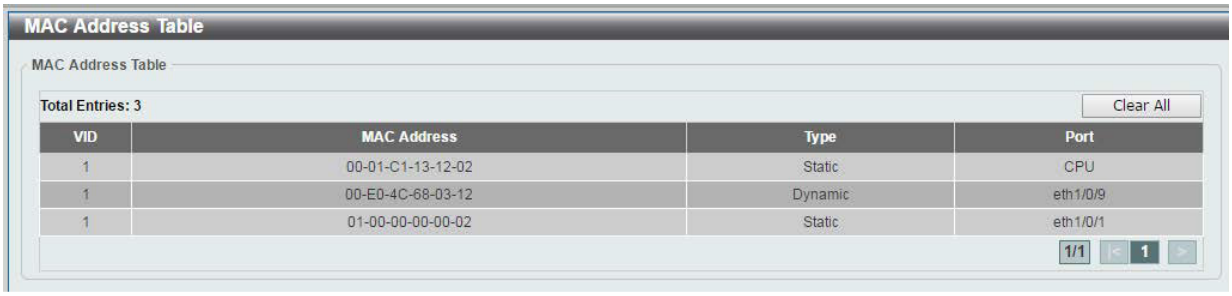


図 8-5　MAC Address Table 画面

「Clear All」ボタンをクリックすると、すべてのダイナミック MAC アドレスは消去されます。

VLAN（VLAN 設定）

VLAN Configuration Wizard（VLAN 設定ウィザード）

ウィザードを使用して、VLAN の作成と設定を行います。

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

図 8-6　VLAN Configuration Wizard 画面

以下の項目が含まれます。

項目	内容
Create VLAN	新しく VLAN を作成する場合に選択します。VID を 2-4094 の間で入力します。 VID 1 は default VLAN に設定されているため、本項目では入力できません。
Configure VLAN	作成済みの VLAN を設定する場合に選択します。設定する VID を入力します。

「Next」ボタンをクリックし、以下の画面で設定を行います。

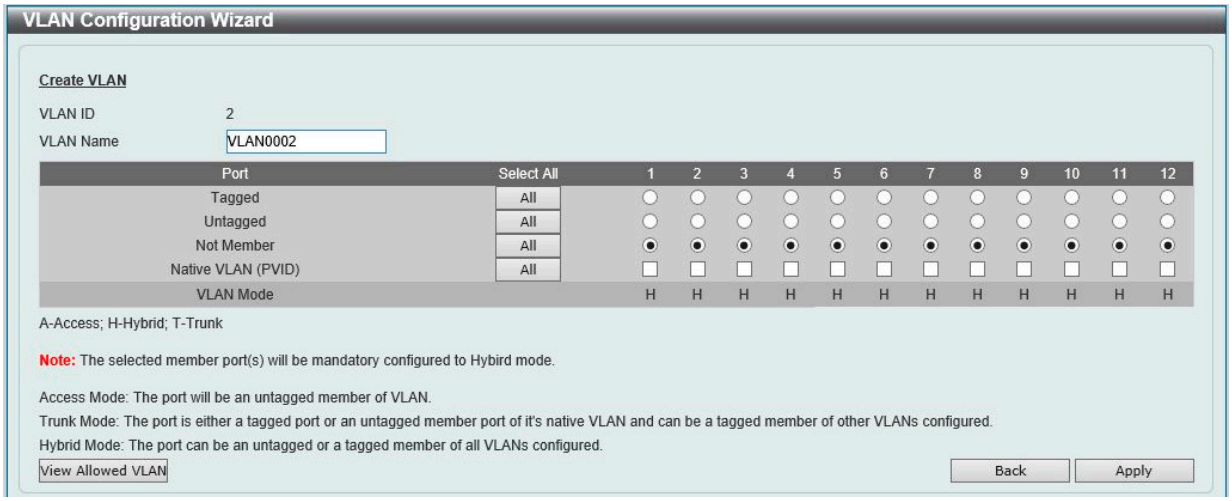


図 8-7　VLAN Configuration Wizard 画面

以下の項目が含まれます。

項目	内容
VLAN ID	選択した VID が表示されます。
VLAN Name	VLAN 名を入力します。
Port	各ポートを以下の通り VLAN のメンバとして定義します。 • Tagged - ポートを 802.1Q タグ付きとして定義します。タグ付きとするポートのボックスをチェックします。 • Untagged - ポートを 802.1Q タグなしとして定義します。タグなしとするポートのボックスをチェックします。 • Not Member - 各ポートが VLAN メンバでないことを定義します。 • Native VLAN (PVID) - ポートをネイティブ VLAN として定義します。 「All」ボタンをクリックすると、すべてのポートが選択されます。
	VLAN Mode 各ポートの VLAN モードが表示されます。 アルファベットの表示は以下のモードを表します。 • A：Access モード ポートは VLAN のタグなしメンバになります。 • H：Hybrid モード ポートは設定されているすべての VLAN のタグなしまたはタグ付きメンバにすることができます。 • T：Trunk モード ポートはネイティブ VLAN のタグ付きポートまたはタグなしメンバポートのいずれかであり、設定されている他の VLAN のタグ付きメンバにすることができます。

項目	内容
View Allowed VLAN	許可された VLAN の一覧が別ウィンドウで表示されます。

「Next」ボタンをクリックし、次へ進みます。

802.1Q VLAN（802.1Q VLAN 設定）

VLAN 表示、設定を行います。

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

図 8-8　802.1Q VLAN 画面

以下の項目が含まれます。

項目	内容
VID List	追加、削除する VLAN ID リストを入力します。

「Apply」ボタンをクリックし、設定を適用します。

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

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

VLAN の編集

該当エントリの横で「Edit」ボタンをクリックします。

Management VLAN (マネジメント VLAN 設定)

Management VLAN を設定します。

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

図 8-9　Management VLAN 画面

画面には次の項目があります。

項目	説明
Management VLAN State	マネジメント VLAN は有効です。
VID	VLAN の ID 番号を指定します。1 から 4094 の間で指定できます。

「Apply」ボタンをクリックし、設定を適用します。

GVRP（GVRP 設定）

GARP VLAN Registration Protocol（GVRP）グローバル設定を表示、設定します。

GVRP Global（GVRP グローバル設定）

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

図 8-10　GVRP Global 画面

画面には次の項目があります。

項目	説明
GVRP Global	
Global GVRP State	GVRP を有効にするかを設定します。 • Enabled - GVRP を有効にします。 • Disabled - GVRP を無効にします。（初期値）
Dynamic VLAN Creation	ダイナミック VLAN 作成機能を有効 / 無効にします。
GVRP Time Settings	
Join Time（1-20）	Join 時間を設定します。1-20（センチ秒）で指定します。初期値は 20（センチ秒）です。
Leave Time（60-300）	Leave 時間を設定します。60-300（センチ秒）で指定します。初期値は 60（センチ秒）です。
Leave All Time（1000-5000）	Leave All 時間を設定します。1000-5000（センチ秒）で指定します。初期値は 1000（センチ秒）です。

「Apply」ボタンをクリックし、設定を適用します。

GVRP Port（GVRP のポート設定）

GVRP のポート設定を行います。

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

図 8-11　GVRP Port 画面

画面には以下の項目があります。

項目	説明
From Port / To Port	ポートの始点 / 終点を設定します。

項目	説明
GVRP Status	GVRP が各ポートで有効かどうかを設定します。有効にするとポートが自動的に VLAN のメンバになります。 • Enabled - 選択したポートで GVRP を有効にします。 • Disabled - 選択したポートで GVRP を無効にします。（初期値）

「Apply」ボタンをクリックし、設定を適用します。

GVRP Advertise VLAN（GVRP Advertise VLAN 設定）

GVRP advertised VLAN の設定、表示を行います。

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

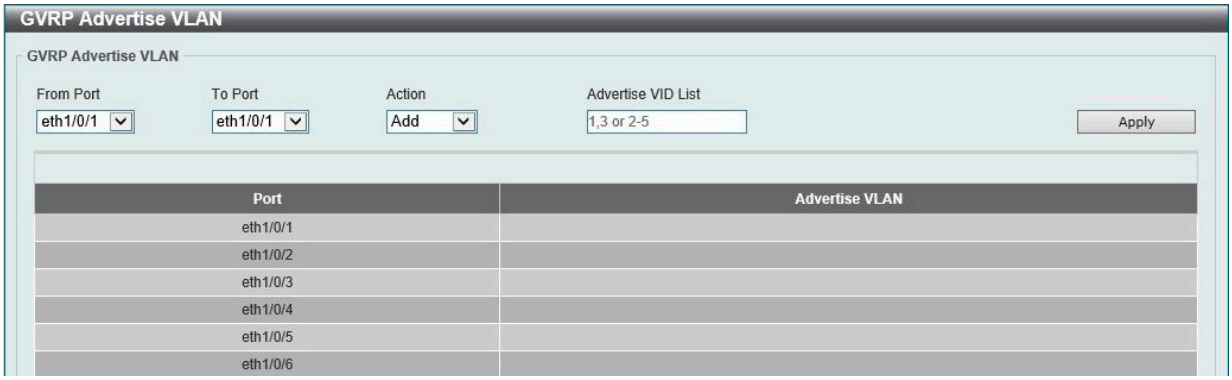


図 8-12　GVRP Advertise VLAN 画面

画面には次の項目があります。

項目	説明
From Port / To Port	ポートの始点 / 終点を設定します。
Action	アドバタイズ VLAN とポートのマッピング動作を選択します。「All」「Add」「Remove」「Replace」から選択可能です。「All」を選択するとすべてのアドバタイズ VLAN が使用されます。
Advertise VID List	アドバタイズ VLAN ID を入力します。

「Apply」ボタンをクリックし、設定を適用します。

GVRP Forbidden VLAN（GVRP Forbidden VLAN 設定）

GVRP Forbidden VLAN の設定、表示を行います。

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

図 8-13　GVRP Forbidden VLAN 画面

画面には次の項目があります。

項目	説明
From Port / To Port	ポートの始点 / 終点を設定します。
Action	禁止 VLAN とポートのマッピングの動作を選択します。「All」「Add」「Remove」「Replace」から選択可能です。「All」を選択するとすべての禁止 VLAN が使用されます。
Forbidden VID List	禁止 VLAN ID を入力します。

「Apply」ボタンをクリックし、設定を適用します。

Asymmetric VLAN（Asymmetric VLAN 設定）

Asymmetric VLAN の設定を行います。

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

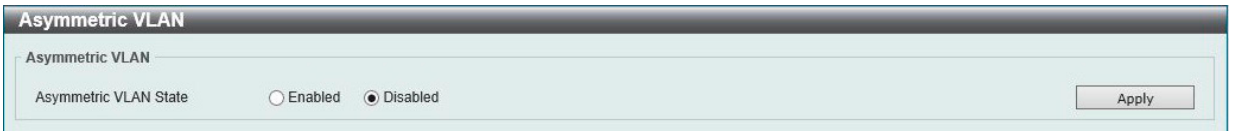


図 8-14　Asymmetric VLAN 画面

項目	説明
Asymmetric VLAN State	Asymmetric VLAN を有効にするかを設定します。 • Enabled - Asymmetric VLAN を有効にします。 • Disabled - Asymmetric VLAN を無効にします。（初期値）

「Apply」ボタンをクリックし、設定を適用します。

注意　Asymmetric VLAN 有効時、ハードウェア制限により FDB エントリが Static になります。

VLAN Interface（VLAN インタフェース設定）

VLAN インタフェースの設定を行います。

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

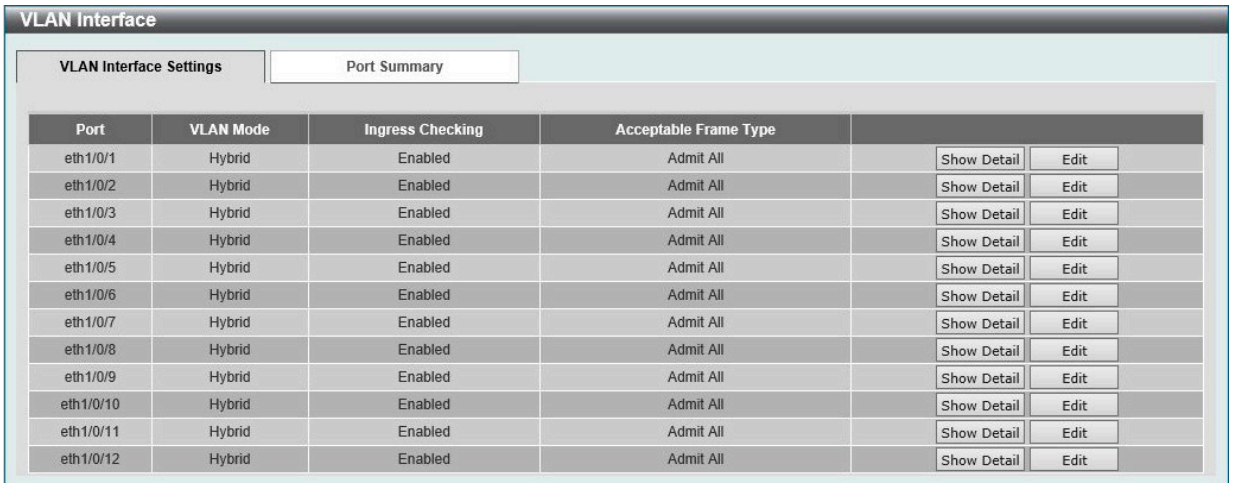


図 8-15　VLAN Interface 画面

VLAN 詳細情報の表示

「VLAN Detail」ボタンをクリックして、指定インタフェースの VLAN について詳細情報について表示します。

エントリの編集

「Edit」ボタンをクリックして、指定エントリの編集をします。

VLAN Deteil（VLAN 詳細情報の表示）

「VLAN Detail」ボタンをクリックして、指定 VLAN の詳細情報を表示します。

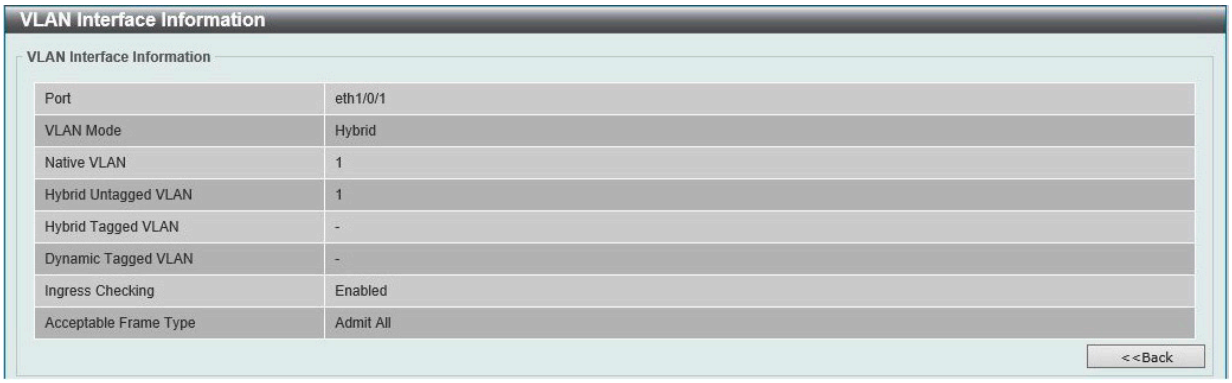


図 8-16　VLAN Interface Information 画面

指定インタフェースの VLAN についての詳細情報を表示します。
「Back」をクリックすると前画面に戻ります。

VLAN Mode - Access（VLAN モードが Access の場合）

「**L2 Features > VLAN > VLAN Interface**」画面で「Edit」をクリック、「VLAN Mode」として「Access」を選択すると次の画面が表示されます。

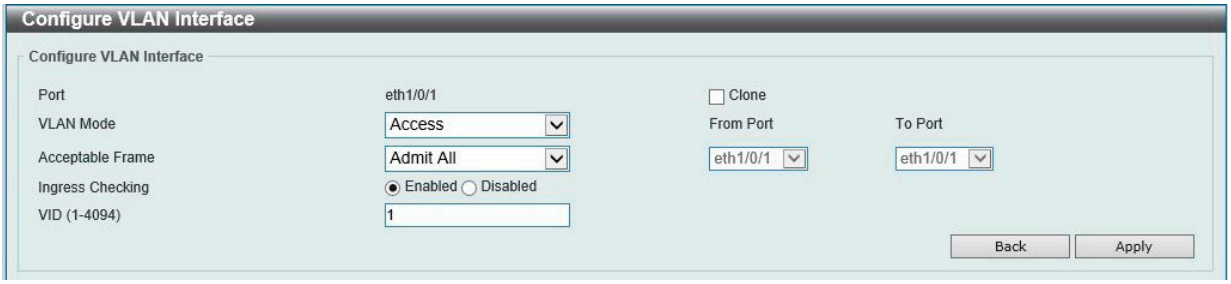


図 8-17　Configure VLAN Interface - Access 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
VID	設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」ボタンをクリックし、設定を適用します。
「Back」をクリックすると前画面に戻ります。

VLAN Mode - Hybrid（VLAN モードが Hybrid の場合）

「**L2 Features > VLAN > VLAN Interface**」画面で「Edit」をクリックします。「Hybrid」を選択すると次の画面が表示されます。

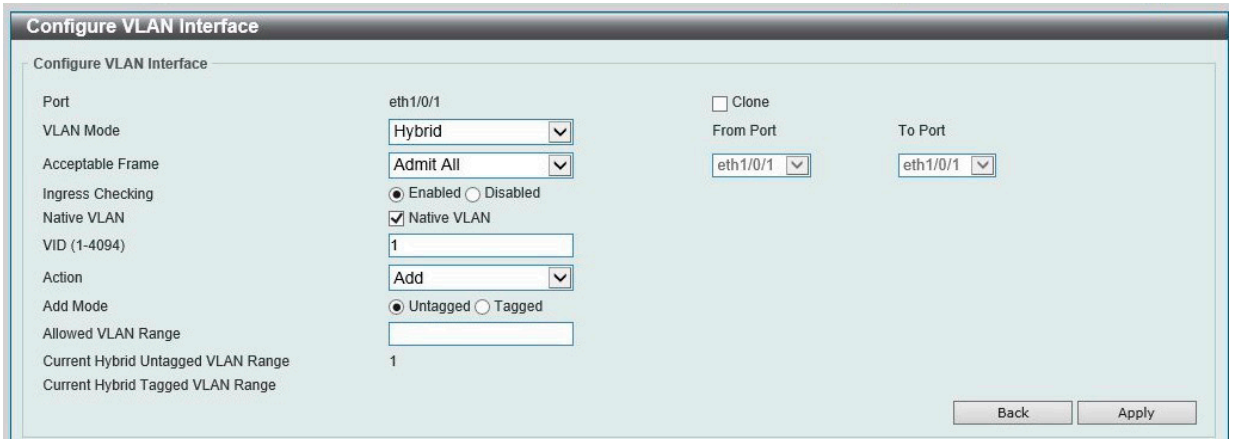


図 8-18　Configure VLAN Interface - Hybrid 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	ネイティブ VLAN を有効 / 無効に指定します。
VID	「Native VLAN」にチェックを入れると表示されます。「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「Add」（追加）、「Remove」（削除）、「Tagged」（タグ付き）、「Untagged」（タグ無し）から選択します。
Add Mode	「Tagged」（タグ付き）、「Untagged」（タグ無し）から選択します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Current Hybrid Untagged VLAN Range	現在の「Hybrid」モードでのタグ無し VLAN 範囲です。
Current Hybrid Tagged VLAN Range	現在の「Hybrid」モードでのタグ付き VLAN 範囲です。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」ボタンをクリックし、設定を適用します。
「Back」をクリックすると前画面に戻ります。

VLAN Mode - Trunk（VLAN モードが Trunk の場合）

「**L2 Features > VLAN > VLAN Interface**」画面で「Edit」をクリックします。「Trunk」を選択すると次の画面が表示されます。

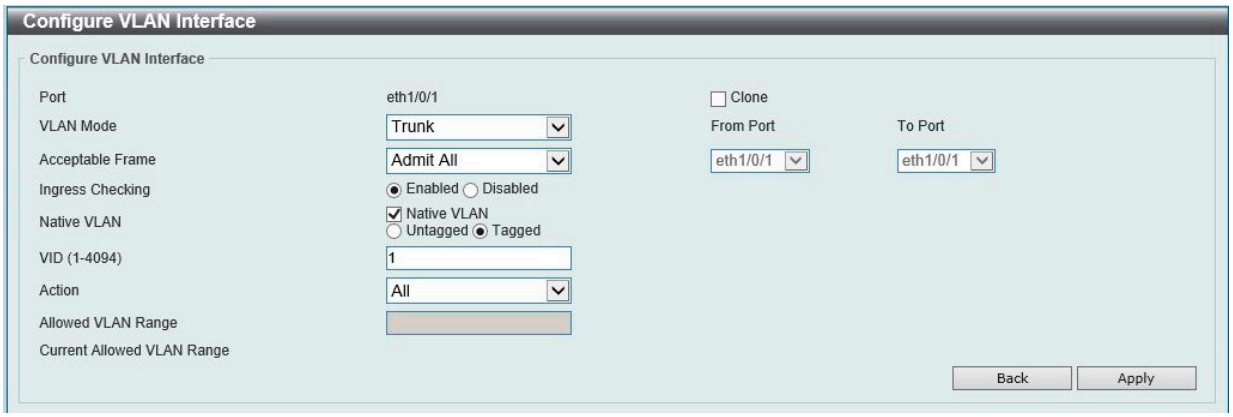


図 8-19　Configure VLAN Interface - Trunk 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。

項目	説明
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	ネイティブ VLAN を有効 / 無効に指定します。
VID	「Native VLAN」にチェックを入れると表示されます。「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「Add」、「All」、「Remove」、「Except」から選択します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Current Allowed VLAN Range	現在の許可されている VLAN 範囲です。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」ボタンをクリックし、設定を適用します。
「Back」をクリックすると前画面に戻ります。

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

自動サーベイランス VLAN のグローバル設定、各ポートのサーベイランス VLAN 情報の表示を行います。

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

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

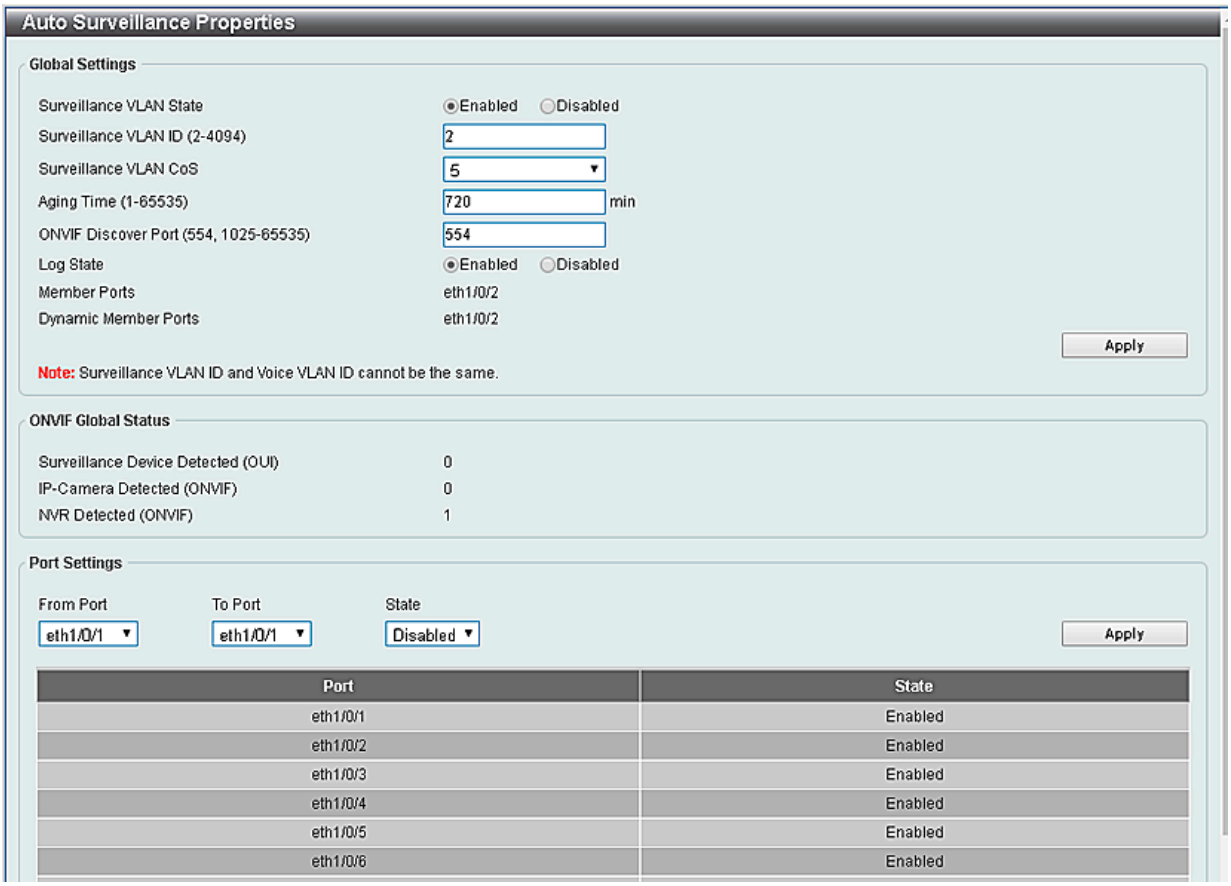


図 8-20　Auto Surveillance Properties 画面

画面には次の項目があります。

項目	説明
Global Settings	
Surveillance VLAN State	サーベイランス VLAN を有効 / 無効に設定します。
Surveillance VLAN ID	サーベイランス VLAN の VLAN ID を指定します。2 から 4094 で指定できます。
Surveillance VLAN CoS	サーベイランス VLAN の優先値を指定します。0 から 7 で指定できます。
Aging Time	エージングタイム（1-65535 分）。 初期値は 720（分）です。 エージングタイムは、ポートがオートサーベイランス VLAN メンバである場合にサーベイランス VLAN からポートを削除するために使用されます。最後のサーベイランスデバイスが、トラフィックの送信を止めて、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。 サーベイントラフィックがエージングタイム内に再開すると、エージングタイマは停止し、リセットされます。

項目	説明
ONVIF Discover Port	「TCP/UDP」ポート番号を指定します。範囲は「554」または「1025 から 65535」です。RSTP ストリームスヌーピングのポート番号になります。ONVIF IP カメラと ONVIF NVR が「WS-Discovery」を使用し他のデバイスを検出します。IP カメラが検出されるとスイッチは IP カメラと NVR 間のスヌーピング RSTP/HTTP/HTTPS パケットによってさらに NVR を検出します。これらのパケットは TCP/UDP ポートと RTSP ポート番号が同等でないとスヌーピングされません。
Log State	サーベイランス VLAN のログを有効 / 無効に指定します。
Port Settings	
From Port / To Port	ポート範囲を指定します。
State	ポートの状態を有効または無効にします。

「Apply」ボタンをクリックし、設定を適用します。

MAC Settings and Surveillance Device（MAC 設定 & サーベイランスデバイス設定）

ユーザ定義のサーベイランスデバイスの OUI を設定します。

L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device の順にメニューをクリックして以下の画面を表示します。
「User-defined MAC Setting」タブが表示されます。

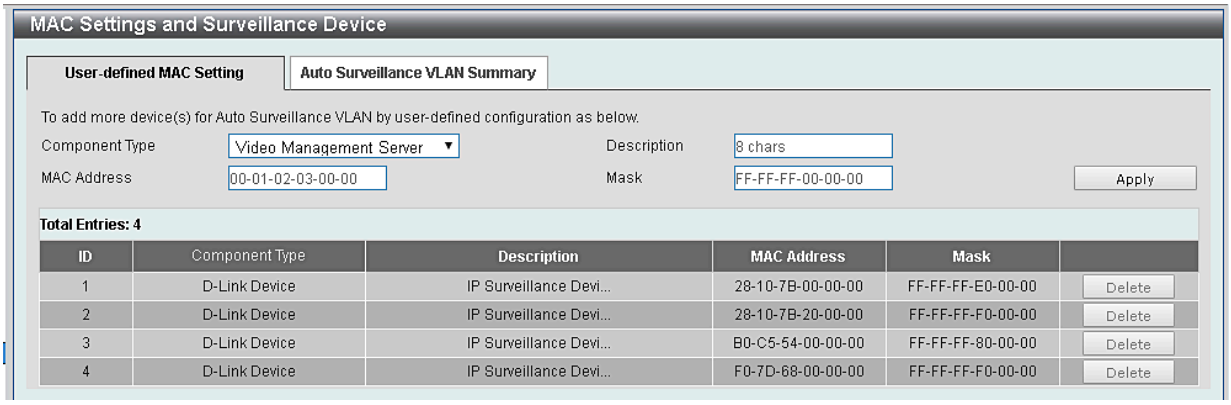


図 8-21　User -defined MAC Settings タブ画面

以下の項目を使用して設定します。

項目	説明
Component Type	プルダウンメニューを使用して、サーベイランス VLAN が自動検出可能なサーベイランスコンポーネントを選択します。選択可能項目は次の通りです。:「Video Management Server」「VMS Client/Remote Viewer」「Video Encoder」「Network Storage」「Other IP Surveillance Device」
Description	ユーザ定義 OUI の概要（8 字以内）を指定します。
MAC Address	ユーザ定義の OUI MAC アドレスを指定します。
Mask	ユーザ定義 OUI MAC アドレスマスクを指定します。

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

エントリの削除

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

自動サーベイランス VLAN サマリの表示

「Auto Surveillance VLAN Summary」タブをクリックして、以下の画面を表示します。

図 8-22　Auto Surveillance VLAN Summary 画面

ONVIF IP-Camera Information（ONVIF IP カメラ情報）

IP カメラ情報ページでは ONVIF を通して検出されたデバイスについて表示します。ここでは ONVIF 対応機器について表示されます。

L2 Features > VLAN > Auto Surveillance VLAN > ONVIF IP-Camera Information をクリックし、以下の画面を表示します。

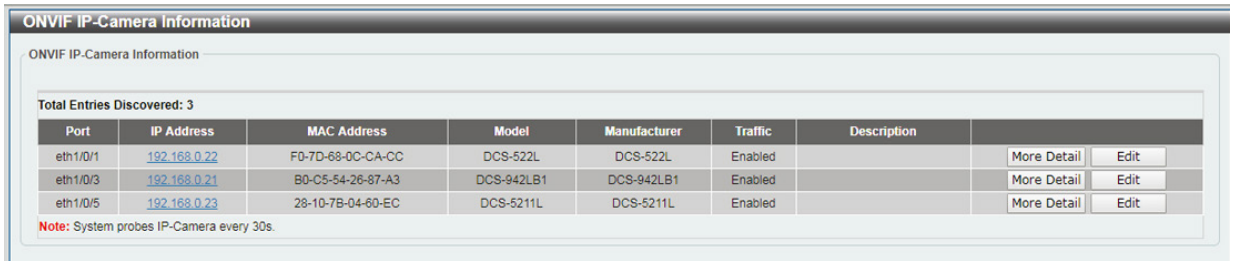


図 8-23　ONVIF IP-Camera Information 画面

「More Detail」をクリックすると接続している IP カメラについてより詳しい情報を表示します。
「Edit」をクリックすると該当の IP カメラについての設定を行います。

図 8-24　ONVIF IP-Camera Information_Edit 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
IP-Camera State	IP カメラを有効 / 無効に指定します。
Description	IP カメラの概要を入力します。

設定を変更する場合は、「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」ボタンをクリックし、前画面にもどります。

「More Detail」をクリックするとより詳細な情報が表示されます。

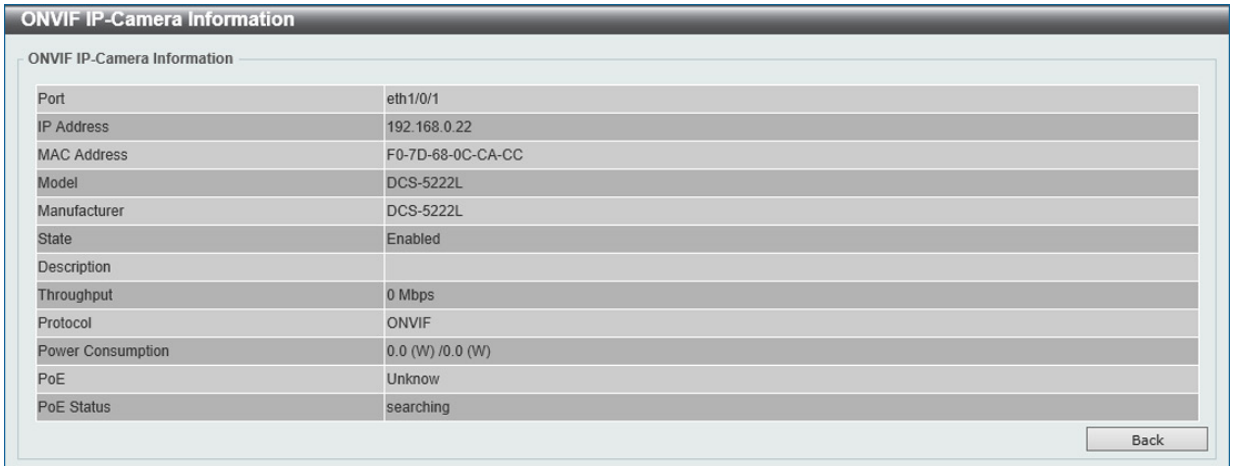


図 8-25　ONVIF IP-Camera Information_More Detail 画面

ONVIF NVR Information（ONVIF NVR 情報）

ONVIF VLAN で検出された NVR 機器のリストを表示します。

L2 Features > VLAN > Auto Surveillance VLAN > ONVIF NVR Information をクリックし、以下の画面を表示します。

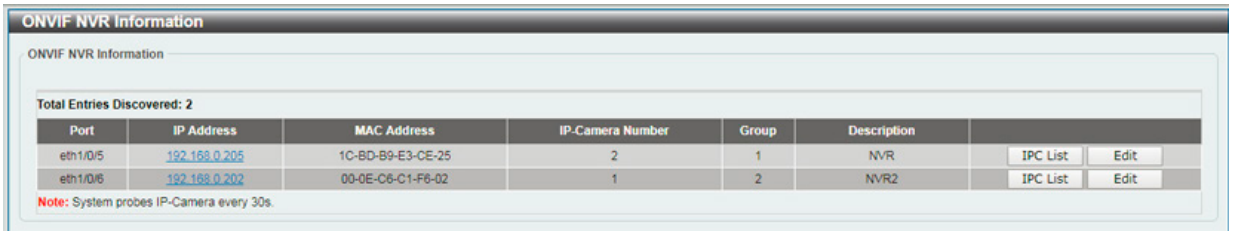


図 8-26　ONVIF NVR Information 画面

NVR の IP アドレスをクリックすると接続している NVR の Web インタフェースを表示します。
「IP-Camera List」をクリックすると NVR に接続している IP カメラのリストを表示します。

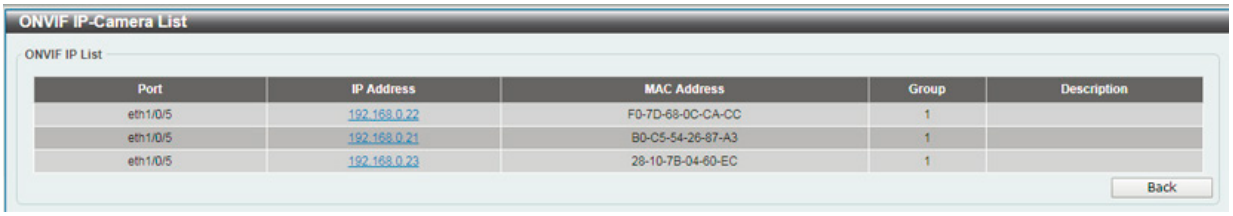


図 8-27　ONVIF NVR Information_IP-Camera List 画面

IP カメラの IP アドレスをクリックするとカメラの Web インタフェースを表示します。
「Back」ボタンをクリックし、前画面にもどります。

「Edit」をクリックすると該当の NVR についての設定を行います。

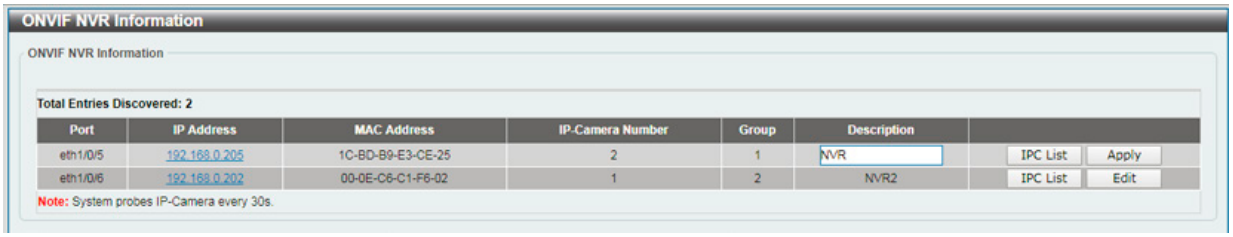


図 8-28　ONVIF NVR Information_Edit 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Description	NVR の概要を入力します。

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

Voice VLAN（音声 VLAN）

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

Voice VLAN Global（音声 VLAN グローバル設定）

音声 VLAN をグロバールに有効 / 無効にします。

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

図 8-29　Voice VLAN Global 画面

以下の項目を使用して、設定します。

項目	説明
Voice VLAN State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Voice VLAN ID (2-4094)	選択をして音声 VLAN の VLAN ID を入力します。
Voice VLAN CoS	プルダウンメニューを使用して音声 VLAN の優先度を設定します。音声 VLAN 優先度はデータトラフィック中の音声トラフィックの QoS を判別する上で使用されます。範囲は 0-7 の間で設定できます。初期値は 5 です。
Aging Time (1-65535)	サーベランス VLAN のエージングタイム（1-65535/min）を指定します。ポートが自動 VLAN の一部の場合、音声 VLAN からポートを削除するまでの時間を設定します。最新の音声機器がトラフィックを送信しなくなり、音声機器の MAC アドレスが期限切れになると、音声 VLAN タイマは開始されます。ポートは音声 VLAN タイマの時間切れのあと、音声 VLAN から削除されます。初期値は 720 分です。

「Apply」ボタンをクリックし、設定を適用します。

Voice VLAN Port（音声 VLAN ポート設定）

音声 VLAN のポート設定を行います。

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

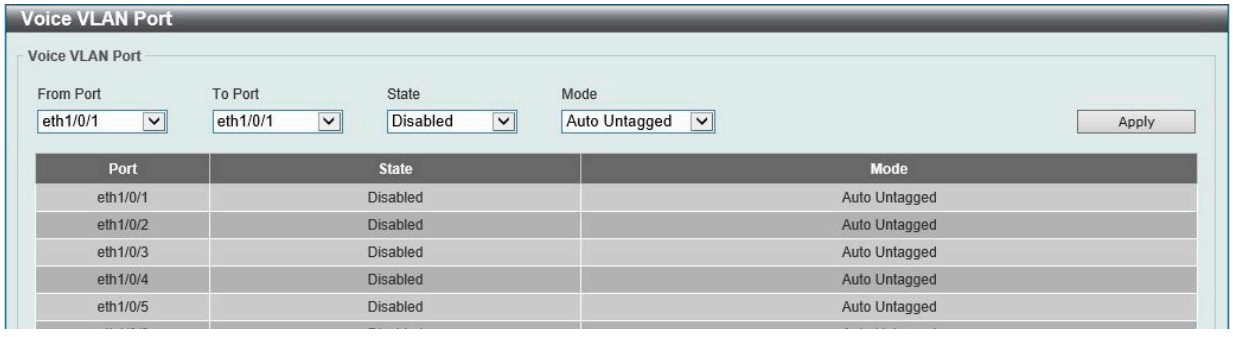


図 8-30　Voice VLAN Port 画面

以下の項目を使用して、設定します。

項目	説明
From Port / To Port	音声 VLAN を設定するポートの範囲を設定します。
State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Mode	「Auto Untagged」「Auto Tagged」「Manual」から設定します。

「Apply」ボタンをクリックし、設定を適用します。

Voice VLAN OUI（音声 VLAN OUI 設定）

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

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

図 8-31　Voice VLAN OUI 画面

以下の項目を使用して、設定します。

項目	説明
OUI Address	OUI MAC アドレスを入力します。
Mask	OUI MAC アドレスマスクを入力します。
Description	設定する OUI についての説明（32 字以内）を入力します。

「Apply」ボタンをクリックし、設定を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

Voice VLAN Device（音声 VLAN 機器）

各スイッチポートに接続中の音声 VLAN が使用可能なデバイスを表示します。「Voice Device Address」はデバイスのアドレス、「Start Time」はデバイスがポートで検出された時間を意味します。

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

図 8-32　Voice VLAN Device 画面

Spanning Tree（スパニングツリーの設定）

本スイッチは 3 つのバージョンのスパニングツリープロトコル（802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。ネットワーキング管理者間では 802.1D-1998 STP が最も一般的なプロトコルとして認識されていると思います。しかし、D-Link のマネジメントスイッチにも 802.1D-2004 RSTP と 802.1Q-2005 MSTP は導入されており、それらの技術について、以下に簡単に紹介します。また、802.1D-1998 STP、802.1D-2004 Rapid STP、802.1Q-2005 MSTP それぞれの設定方法についても、本章中に記述します。

802.1Q-2005 MSTP

MSTP（Multiple Spanning Tree Protocol）は IEEE 委員会により定義された標準規格で、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングし、ネットワーク中に複数の経路を提供します。また、ロードバランシングを可能にし、1 つのインスタンスに障害が発生した場合でも、広い範囲で影響を与えないようにすることができます。障害発生時には障害が発生したインスタンスに代わって新しいトポロジを素早く収束します。これら VLAN 用のフレームは、これらの 3 つのスパニングツリープロトコル（STP、RSTP、MSTP）のいずれかを使用して、素早く適切に相互接続されたブリッジを通して処理されます。

このプロトコルは BPDU パケットもまたタグ付けし、受信するデバイスはスパニングツリーのインスタンスやリージョン、それらに関連する VLAN を区別することも可能です。MSTI ID（MST インスタンス ID）はこれらのインスタンスをクラス分けします。MSTP は、複数のスパニングツリーを CIST（Common and Internal STP）で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を決定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジとして表示されます。そのため、異なる VLAN に割り当てられたフレームは、定義した VLAN や各スパニングツリー内の管理エラーに関係なく、フレームの単純で完全な処理を続けながら、ネットワーク上の管理用に構築されたリージョン中の異なるデータ経路を通ります。

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

1. 32 文字までの半角英数字で定義された「Configuration 名」。「MST Configuration Identification」画面中の「Configuration Name」で設定します。
2. 「Configuration Revision 番号」（「MST Configuration Identification」画面内の「Revision Level」）。
3. 4094 エレメントテーブル（「MST Configuration Identification」画面内の「VID List」）。スイッチがサポートする 4094 件までの VLAN とインスタンスとの関連付けです。

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

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

802.1D-2004 Rapid Spanning Tree

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

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

ポートの状態遷移

3 つのプロトコル間の根本的な相違は、ポートがフォワーディング状態に遷移する方法と、この遷移とトポロジの中でのポートの役割（Forwarding/Not Forwarding）の関連性にあります。MSTP と RSTP では、802.1D-1998 で使用されていた 3 つの状態、「Disabled」、「Blocking」、「Listening」が、「Discarding」という 1 つの状態に統合されました。どちらのケースにおいてもポートはパケットの送信を行わない状態です。STP の「Disabled」、「Blocking」、「Listening」であっても RSTP/MSTP の「Discarding」であっても、ネットワークトポロジ中では「アクティブではない状態」であり、機能の差はありません。以下の表にポートの状態遷移における 3 つのプロトコルの差を示しています。

トポロジの計算については 3 つのすべてのプロトコルにおいて同様に行われます。各セグメントにはルートブリッジへの 1 つのパスがあります。すべてのブリッジは BPDU パケットをリッスンします。しかし、BPDU パケットは、さらに Hello パケット送信ごと送信されます。
BPDU パケットは、受信されないことがあっても送信されます。そのため、ブリッジ間のリンクはリンクの状態に反応します。結果として、この違いがリンク断の素早い検出とトポロジの調整に繋がるのです。802.1D-1998 の欠点は隣接するブリッジからの即時のフィードバックがないことです。

ポート状態の比較

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

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

RSTP では、タイマの設定への依存をやめ、フォワーディング状態への急速な遷移が可能になりました。RSTP 準拠のブリッジは他の RSTP に準拠するブリッジリンクからのフィードバックに反応するようになりました。ポートは、フォワーディング状態の遷移の間トポロジが安定するまで待つ必要がなくなりました。この急速な遷移を実現するために、RSTP プロトコルでは以下の 2 つの新しい変数（Edge Port と P2P Port）が使用されます。

Edge Port

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

P2P Port

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

802.1D-1998/802.1D-2004/802.1Q-2005 間の互換性

RSTP や MSTP はレガシー機器と相互運用が可能で、必要に応じて BPDU パケットを 802.1D-1998 形式に自動的に変換することができます。しかし、802.1D-1998 STP を使用しているセグメントでは、MSTP や RSTP の利点である迅速な遷移やトポロジ変更の検出を享受することはできません。それらのプロトコルは、セグメント上でレガシー機器が RSTP や MSTP を使用するためにアップデートを行う場合などの、マイグレーションに使用する変数を用意しています。

2 つのレベルで動作するスパニングツリープロトコル

1. スイッチレベルでは、設定はグローバルに実行されます。
2. ポートレベルでは、設定はポートベースのユーザ定義のグループに対して実行されます。

STP Global Settings（STP グローバル設定）

STP をグローバルに設定します。

L2 Features > Spanning Tree > STP Global Settings の順にメニューをクリックし、以下に示す画面を表示します。

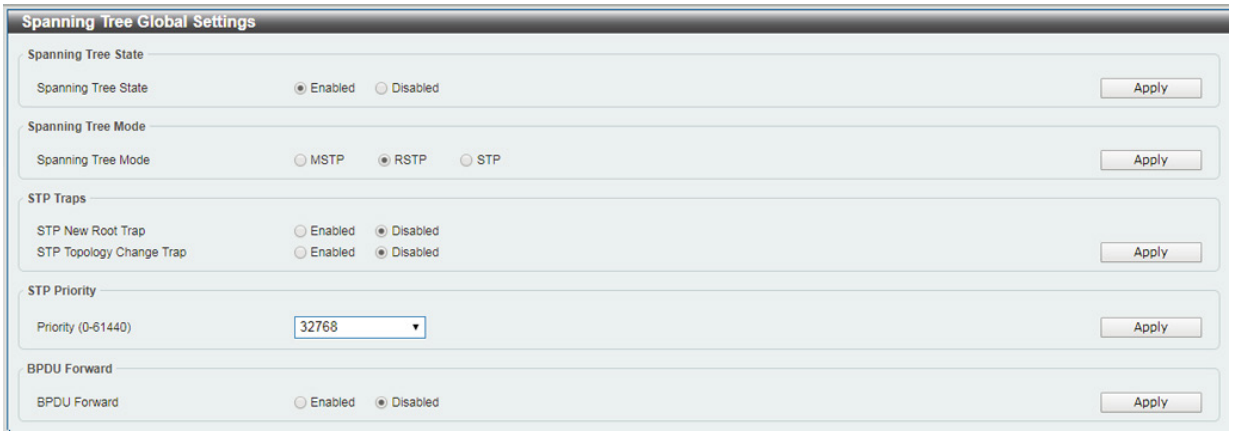


図 8-33　STP Global Settings 画面

設定には以下の項目が使用されます。

項目	説明
Spanning Tree State	
Spanning Tree State	STP をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
Spanning Tree Mode	
Spanning Tree Mode	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。 • MSTP - スイッチ上で MSTP がグローバルに使用されます。
STP Traps	
STP New Root Trap	新しいルートトラップ送信の有効 / 無効を設定します。
STP Topology Change Trap	トポロジ変更トラップ送信の有効 / 無効を設定します。

項目	説明
STP Priority	
Priority	STP 優先値を指定します。0から61440までで指定可能です。初期値は32768です。値が低いほうがプライオリティが高くなります。
BPDU Forward	
BPDU Forward	BPDU パケットの転送を「Enabled」（有効）または「Disabled」（無効）にします。 有効にすると受信したSTP BPDUはすべてのVLANメンバポートにタグなしフォームで転送されます。初期値は無効です。

「Apply」ボタンをクリックし、設定を適用します。

STP Port Settings（STP ポートの設定）

STP をポートごとに設定します。

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

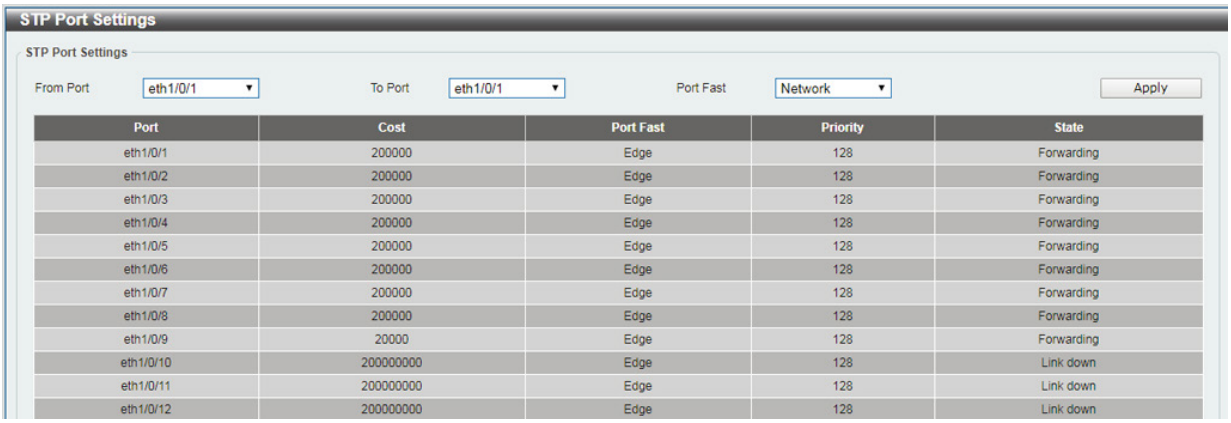


図 8-34　STP Port Setting 画面

本画面には以下の項目があります。

項目	説明
From Port	連続するポートグループの最初の番号を設定します。
To Port	連続するポートグループの最後の番号を設定します。
Port Fast	ポートファストオプションを指定します。 「Network」「Disabled」「Edge」から選択します。「Network」モードでは、ポートは 3 秒だけ非ポートファスト状態を保持します。ポートで BPDU が受信されず、フォワーディングステートに変更されない場合、ポートファスト状態に変更します。のちに BPDU を受信すると非ポートファストへ戻ります。「Disable」モードではポートは常に非ポートファスト状態です。フォワーディングステートに変更するまで転送時間遅延の間、常に待ちます。「Edge」モードではポートは転送時間遅延の間待たずに、直接 STP フォワーディングステートに変更されます。インタフェースが「BPDU」を受信すると非ポートファストへ移行します。初期値では「Network」になります。

「Apply」ボタンをクリックし、設定を適用します。

MST Configuration Identification（MST の設定）

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

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

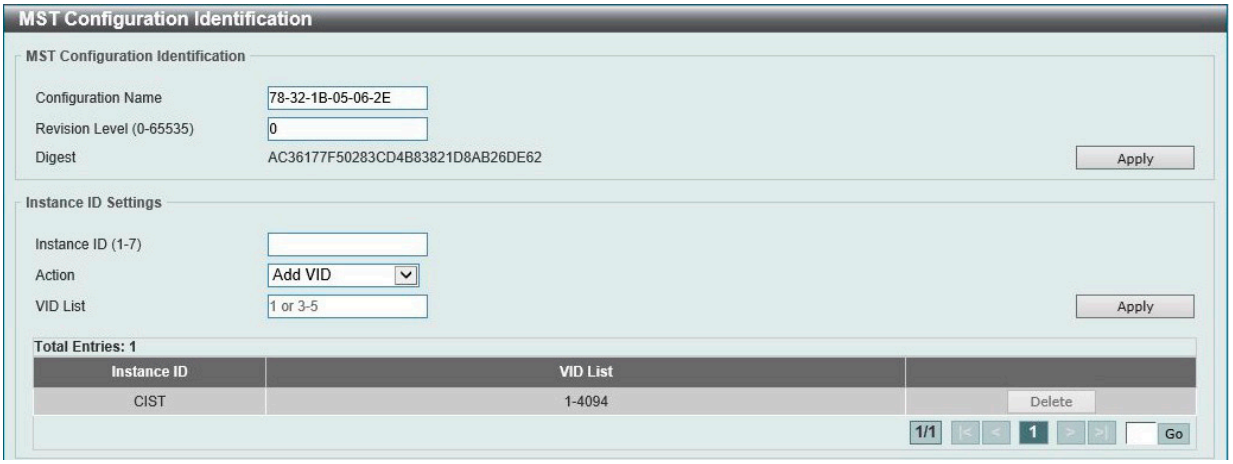


図 8-35　MST Configuration Identification 画面

上記画面には以下の項目が含まれます。

項目	説明
Configuration Name	各 MSTI（Multiple Spanning Tree Instance）を識別するためにスイッチに名前を設定します。 名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level	スイッチ上に設定された MST リージョンの値 (0-65535) を設定します。初期値は 0 です。「Configuration Name」とともに MSTP リージョンの識別に使用されます。
Instance ID	1-16 の番号を入力し、スイッチに Instance ID を設定します。
Action	MSTI に行う変更を選択します。 • Add VID - VID List 項目に指定された VID を MSTI ID に追加します。 • Remove VID - VID List 項目に指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

「Apply」ボタンをクリックし、設定を適用します。

エントリの編集

1. 編集するエントリ横の「Edit」ボタンをクリックします。
2. 「MST Configuration Identification」セクションに現在の設定が表示されます。設定変更後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックします。

STP Instance（STP インタンス設定）

スイッチの MSTI に関する現在の設定を表示し、MSTI のプライオリティを変更できます。

L2 Features > Spanning Tree > STP Instance をクリックし、以下の画面を表示します。

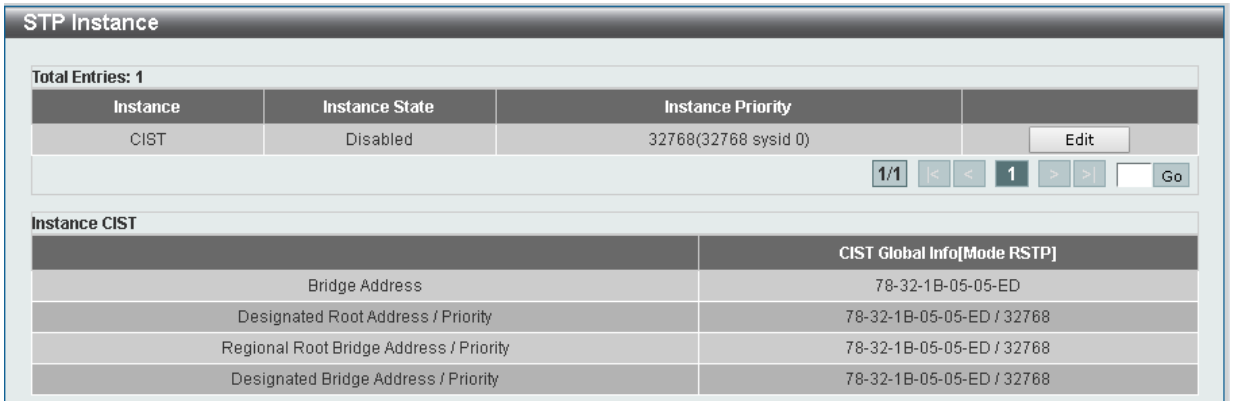


図 8-36　STP Instance 画面

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

MSTP Port Information（MSTP ポート情報）

現在の MSTP ポート情報の表示を行います。

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

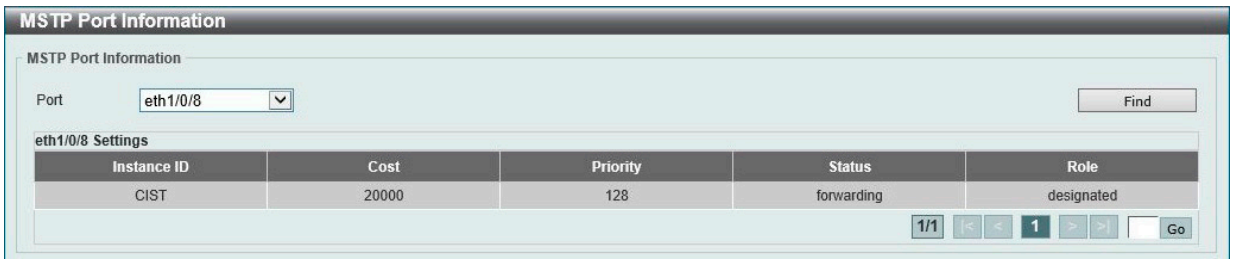


図 8-37　MSTP Port Information 画面

本画面には以下の情報があります。

項目	説明
Port	プルダウンメニューを使用して、ポートを選択します。

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

ERPS (G.8032)（イーサネットリングプロテクション設定）

ERPS（Ethernet Ring Protection Switching）はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。これは、イーサネットリングネットワークに対して十分に考慮されたイーサネット操作、管理、およびメンテナンス機能と簡単な APS（automatic protection switching）プロトコルを統合することによって実行されます。

リング内の 1 つのリンクが、ループ（RPL : Ring Protection Link）を回避するためにブロックされます。障害が発生すると、保護スイッチングは障害のあるリンクをブロックして RPL のブロックを解除します。障害が解決すると、保護スイッチングは再度 RPL をブロックして、障害が解決したリンクのブロックを解除します。

ERPS

スイッチの ERPS 機能を有効にします。

L2 Features > ERPS (G.8032) > ERPS の順にメニューをクリックし、以下の画面を表示します。

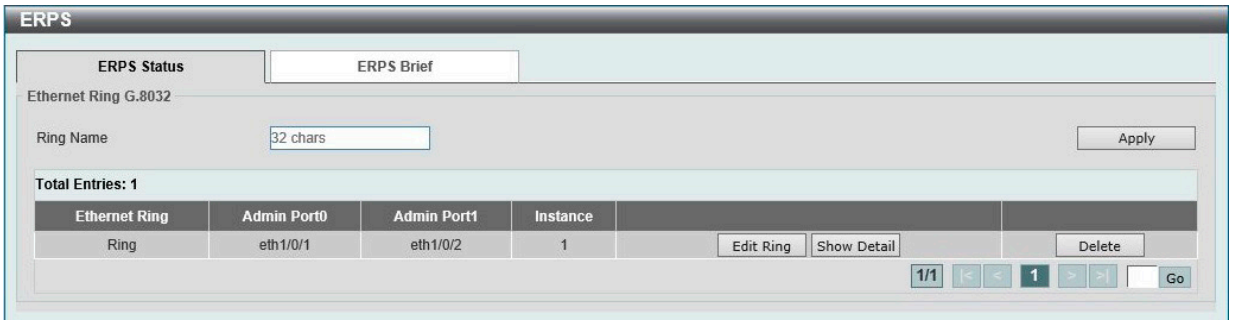


図 8-38　ERPS 画面

上記画面には以下の項目が含まれます。

項目	説明
ERPS Status タブ	
Ring Name	ERPS インスタンス名を入力します。32 文字までで指定可能です。

「Apply」をクリックして「ITU-T G.8032 ERP リング」を作成します。
「Edit Ring」をクリックして「ITU-T G.8032 ERP リング」を編集します。
「Show Detail」をクリックして「ITU-T G.8032 ERP リング」の情報について表示します。
「Delete」をクリックして指定の「ITU-T G.8032 ERP リング」を削除します。

Ring の編集

「Edit Ring」ボタンをクリックすると、以下の設定画面が表示されます。

図 8-39　ERPS 画面 - Edit

設定対象となる項目は以下の通りです。

項目	説明
Instance ID	チェックを入れ「ERP インスタンス」の番号を指定します。1-32 で指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Port0	チェックを入れユニット ID と初期リングになるポート番号を指定します。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Port1	チェックを入れユニット ID と 2 番目のリングになるポート番号を指定します。ドロップダウンメニューから「None」を選択すると内部接続されたノードはオープンリングのエンドポイントのローカルノードとして指定されます。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。

「Back」をクリックすると設定は破棄され前画面に戻ります。
「Apply」をクリックして設定を適用します。

「ERPS Brief」タブをクリックすると以下の画面が表示されます。

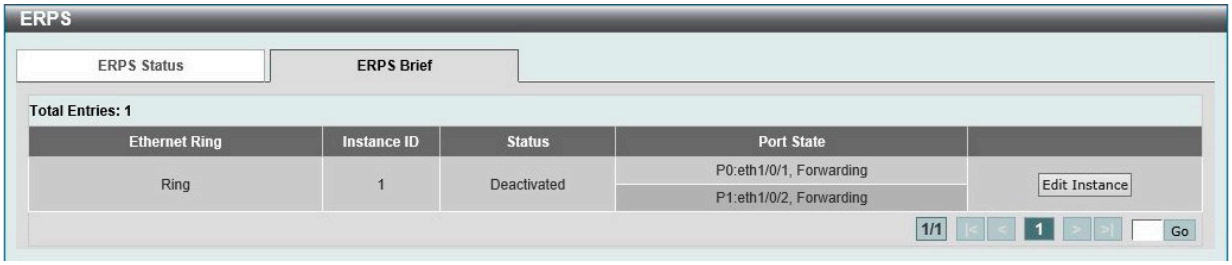


図 8-40　ERPS Brief タブ画面

「Edit Instance」ボタンをクリックしてインスタンスの編集を行います。

Instance の編集

「Edit Instance」ボタンをクリックすると、以下の設定画面が表示されます。

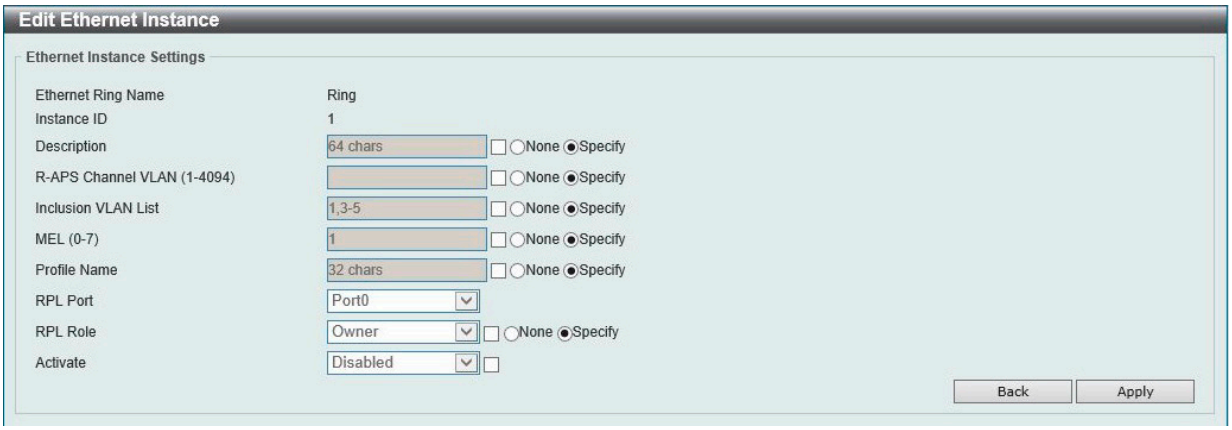


図 8-41　ERPS 画面 - Instance

設定対象となる項目は以下の通りです。

項目	説明
Description	チェックを入れ「ERP インスタンス」の概要を指定します。64 文字まで指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
R-APS Channel VLAN	チェックを入れ「ERP インスタンス」の「R-APS Channel VLAN ID」を指定します。サブインスタンスの「APS channel VLAN」はサブリングの仮想チャネルでもあります。1 から 4094 までの間で指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Inclusion VLAN List	チェックを入れインスタンスに含まれる VLAN リストを指定します。 「-」を使用すると範囲として指定され、「,」を使用すると個別に複数の VLAN を指定します（例;「VLAN1 から 5」は「1-5」、「VLAN1 と 3 と 5」は「1,3,5」）。指定された VLAN は ERP のメカニズムで保護されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
MEL	チェックを入れ ERP インスタンスの「MEL」を指定します。0 から 7 までの間で指定可能です。 同じ ERP インスタンスに参加するすべてのリングノードの MEL 値は同一である必要があります。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Profile Name	チェックを入れ ERP インスタンスに関連する「G.8032」のプロファイルを指定します。複数の ERP インスタンスを同じ G.8032 プロファイルに関連付けることも可能です。同じプロファイルに関連付けられたインスタンスは VLAN の同じセットを保護するか、もしくはあるインスタンスに保護される VLAN は、別のインスタンスに保護されている LAN のサブセットです。32 文字まで指定可能です。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
RPL Port	チェックを入れ RPL ポートオプションを選択します。オプションは「Port0」「Port1」から指定します。 選択されたオプションは RPL ポートとして設定されます。
RPL Role	チェックを入れノードが RPL オーナ（Owner）かネイバ（Neighbor）かを選択します。 「Enable」の場合、RPL は「オーナ」として設定されます。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Activate	チェックを入れ ERP インスタンスをアクティブにするか選択します。「Enable/Disable」から選択し、「Enable」の場合、ERP インスタンスはアクティブになります。

「Back」をクリックすると設定は破棄され前画面に戻ります。
「Apply」をクリックして設定を適用します。

Status の表示

「Show Status」ボタンをクリックすると、以下の設定画面が表示されます。

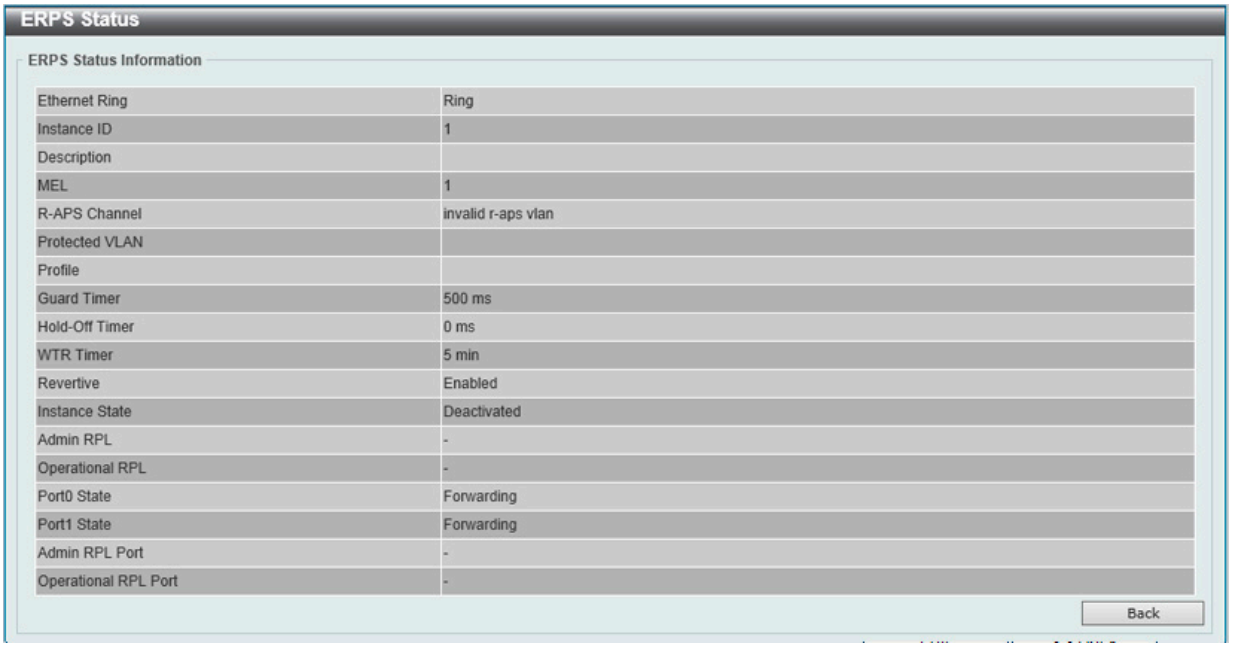


図 8-42　ERPS Staus 画面

「Back」をクリックすると前画面に戻ります。

ERPS Profile（ERPS プロファイル）

ERPS プロファイル設定を行います。

L2 Features > ERPS (G.8032) > ERPS Profile の順にメニューをクリックし、以下の画面を表示します。

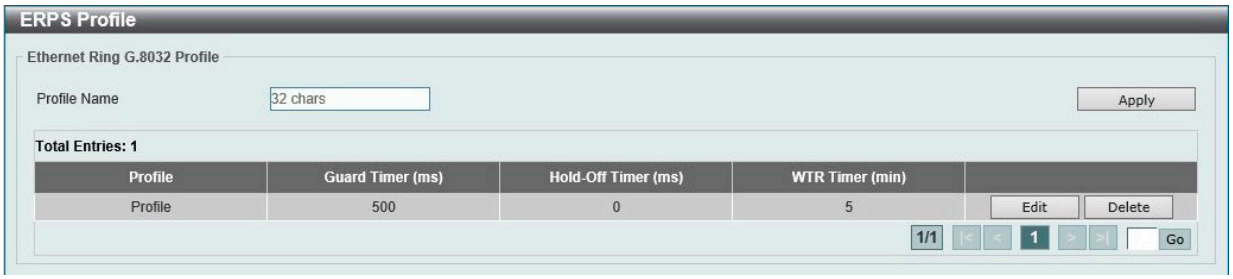


図 8-43　ERPS Profile 画面

設定対象となる項目は以下の通りです。

項目	説明
Profile Name	「G.8032」のプロファイル名を指定します。32 文字まで指定可能です。複数の ERP インスタンスが同じ「G.8032」プロファイルとして指定できます。同じプロファイルに含まれるインスタンスは同じセットの VLAN や一つのインスタンスに保護される VLAN、他のインスタンスに保護される LAN のサブセットを保護します。

「Apply」をクリックして「G.8032」プロファイルと ERP インスタンスを作成します。
「Delete」をクリックして指定の「G.8032」プロファイルと ERP インスタンスを削除します。
「Edit」をクリックして「G.8032」プロファイルを編集します。

「G.8032」プロファイルの編集

「Edit 」ボタンをクリックすると、以下の設定画面が表示されます。

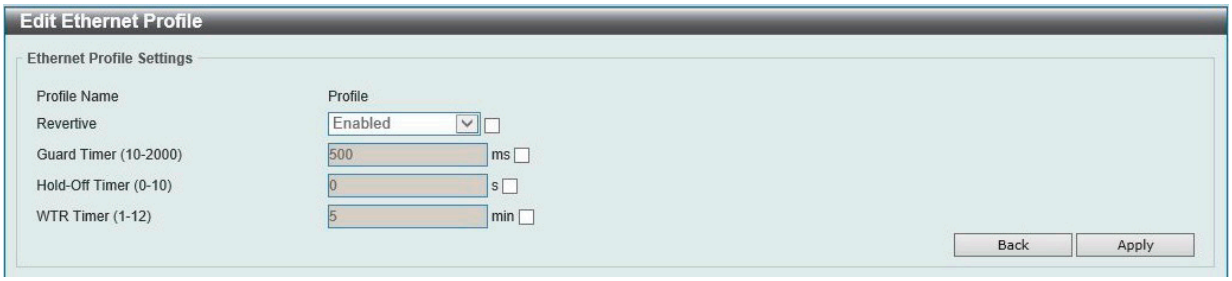


図 8-44　「G.8032」プロファイル画面 - Edit

設定対象となる項目は以下の通りです。

項目	説明
Revertive	チェックを入れ「Revertive」の設定を行います。「Enable/Disable」から選択します。本機能は運用系トランスポートエンティティに戻すために使用されます。例えば RPL がブロックされた場合などです。
Guard Timer	チェックを入れ Guard Timer の設定を行います。10 から 2000（ミリ秒）の間で指定可能です。初期値は 500（ミリ秒）です。
Hold-Off Timer	チェックを入れ Hold-Off Timer の設定を行います。0 から 10（秒）の間で指定可能です。初期値は 0（秒）です。
WTR Timer	チェックを入れ WTR Timer の設定を行います。1 から 12（分）の間で指定可能です。初期値は 5（分）です。

「Back」をクリックすると設定は破棄され前画面に戻ります。

「Apply」をクリックして設定を適用します。

Loopback Detection（ループバック検知設定）

ループバック検知機能は、特定のポートによって生成されるループを検出するために使用されます。

本機能は、CTP（Configuration Testing Protocol）パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートから受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートをブロックして管理者にアラートを送信します。ループバック検知機能はポート範囲に実行されます。プルダウンメニューを使用し、機能を「Enabled」（有効）/「Disabled」（無効）にします。

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

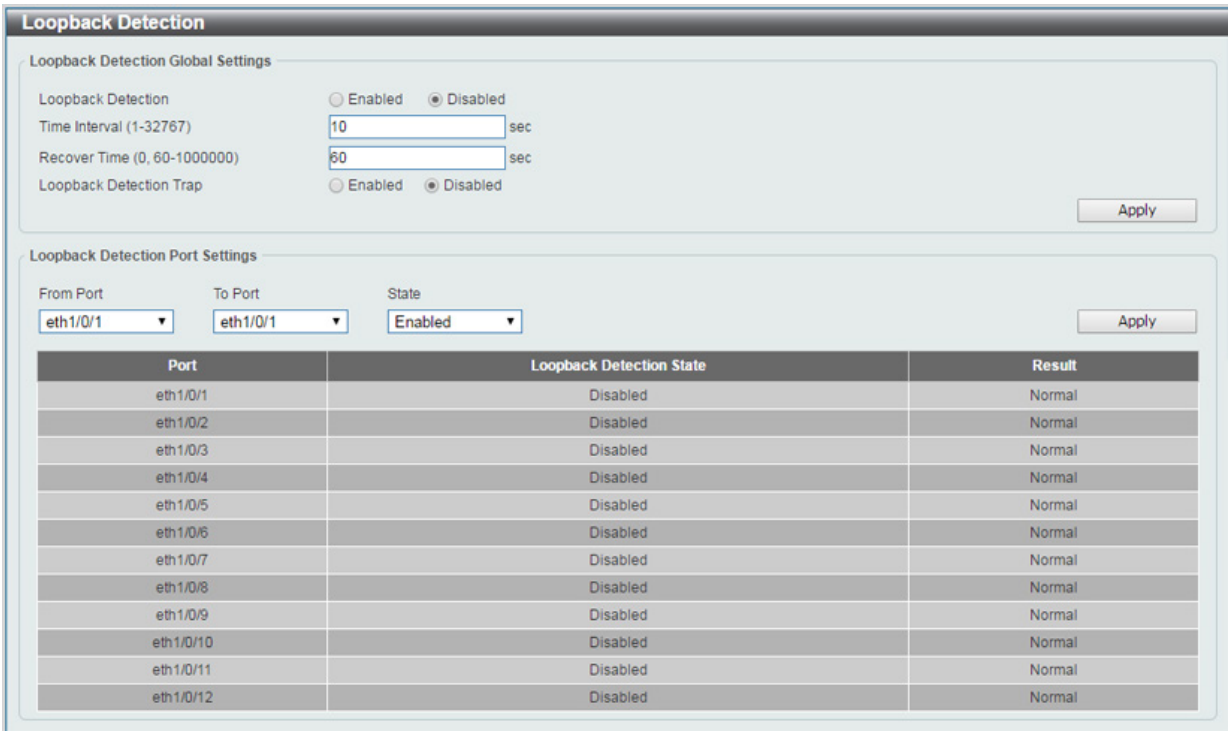


図 8-45　Loopback Detection Settings 画面

Loopback Detection Global Settings には以下の項目があります。

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。初期値は「Disabled」です。

項目	説明
Time Interval (1-32767)	ループバックを検知するための CTP（Configuration Testing Protocol）パケットを送信する間隔（1-32767 秒）を指定します。初期値は 10 秒です。
Recover Time	ループバック検出からリカバリにかかるまでの時間を指定します。0 または 60 から 1000000（秒）の間で指定できます。0 に指定するとスイッチを再起動するまでポートをブロックします。初期値は 60 です。
Loopback Detection Trap	トラップを有効 / 無効に設定します。

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

Loopback Detection Port Settings には以下の項目があります。

項目	説明
From Port / To Port	ループ検知を設定するポートの範囲を設定します。
State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。

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

注意　「スパニングツリー」と「ループバック検知」は排他的な仕様になっており、「スパニングツリー」が有効の場合、「ループバック検知」は無効になります。

注意　Link Aggregation を構成するポート上でループ検知機能を併用することができませんのでご注意ください。

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　VLAN Tag 付の CTP が ループした場合には、本機能はループを検知できません。

注意　VLAN Tag 無しの CTP を Untag VLAN 設定のない Port で受信した場合には、本機能はループを検知できません。

Link Aggregation（リンクアグリゲーション）

ポートトランクグループについて

ポートトランクグループは、複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。スイッチはポート 1-8 を束ねた 6 個までのトランクグループをサポートします。

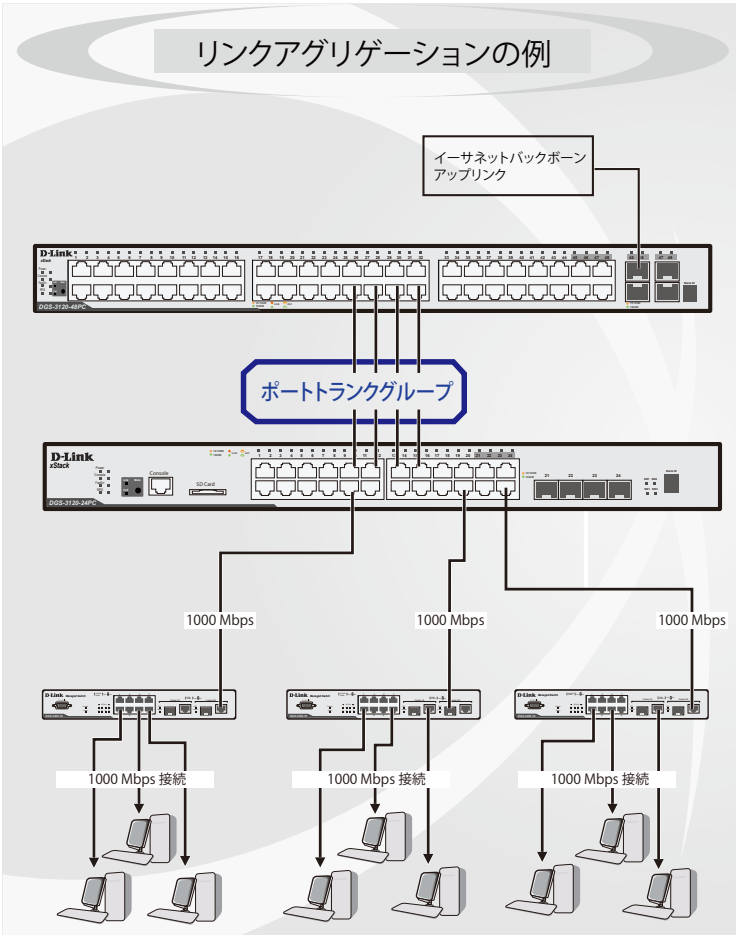


図 8-46　ポートトランクグループの例

スイッチはトランクグループ内のすべてのポートを 1 つのポートと見なします。あるホスト（宛先アドレス）へのデータ転送は、トランクグループ内のいつも同じポートから行われます。これにより、データが送信された順に受け取られるようになります。

注意 トランクグループ内のあるポートが接続不可になると、そのポートが処理するパケットは他のリンクアグリゲーション（集約）グループ内の他のポート間でロードシェアされます。

注意 Link Aggregation を構成するポート上でループ検知機能を併用することができませんのでご注意ください。

リンクアグリゲーション機能により、1 つのグループとして束ねられたポートは、1 つのリンクの働きをします。この時、1 つのリンクの帯域は、束ねられたポート分拡張されます。

リンクアグリゲーションは、サーバやバックボーンなど、広帯域を必要とするネットワークデバイスにおいて広く利用されています。

本スイッチでは、最大 8 個のリンク（ポート）で構成する最大 6 個のリンクアグリゲーショングループの構築が可能です。各ポートは、1 つのリンクアグリゲーショングループにのみ所属することが可能です。

1 つのグループ内のポートはすべて同じ VLAN に属し、それぞれのスパニングツリープロトコル（STP）ステータス、スタティックマルチキャスト、トラフィックコントロール、トラフィックセグメンテーション、および 802.1p デフォルトプライオリティの設定は同じである必要があります。さらに、集約する LACP リンクはすべて同じ速度で、全二重モードで設定されている必要があります。

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

スパニングツリープロトコル（STP）は、スイッチレベルにおいて、リンクアグリゲーショングループを 1 つのリンクとしてとらえます。ポートレベルでは STP はマスタポートのパラメータを使用してポートコストを計算し、リンクアグリゲーショングループの状態を決定します。スイッチ上に 2 つのリンクアグリゲーショングループが冗長して設定された場合、STP は冗長リンクを持つポートのブロックを行うのと同様に、1 つのポートをブロックします。

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

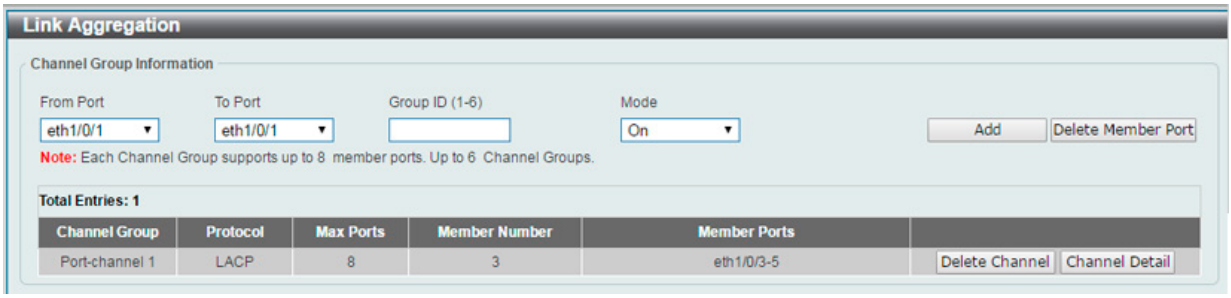


図 8-47　Link Aggregation 画面

本画面には次の項目があります。

項目	説明
Channel Group Information	
From Port / To Port	設定するポートの範囲を指定します。
Group ID	グループの ID 番号（1-6）を設定します。物理ポートがチャネルグループに属すと、システムによって自動的にポートチャネルが作成されます。一つのチャネルグループにつき一つのインタフェースのみ所属することができます。
Mode	モードを指定します。「On」「Active」「Passive」から指定できます。「On」にするとチャネルグループタイプは固定になります。「Active」「Passive」の場合、チャネルグループタイプは LACP になります。チャネルグループタイプは固定か LACP メンバのどちらかで構成されます。一度チャネルグループタイプが決定されると、他のタイプのインタフェースはチャネルグループに参加できなくなります。

指定のエントリを削除するためには、削除するグループの「Delete Channel」ボタンをクリックします。
指定のメンバポートを削除するためには、削除するグループの「Delete Member Port」ボタンをクリックします。

ポートトランキンググループの設定
各項目を入力後、「Add」ボタンをクリックし、ポートトランキンググループを設定します。

ポートトランクグループの編集

チャネルについてのより詳細な情報の確認には「Channel Detail」をクリックします。

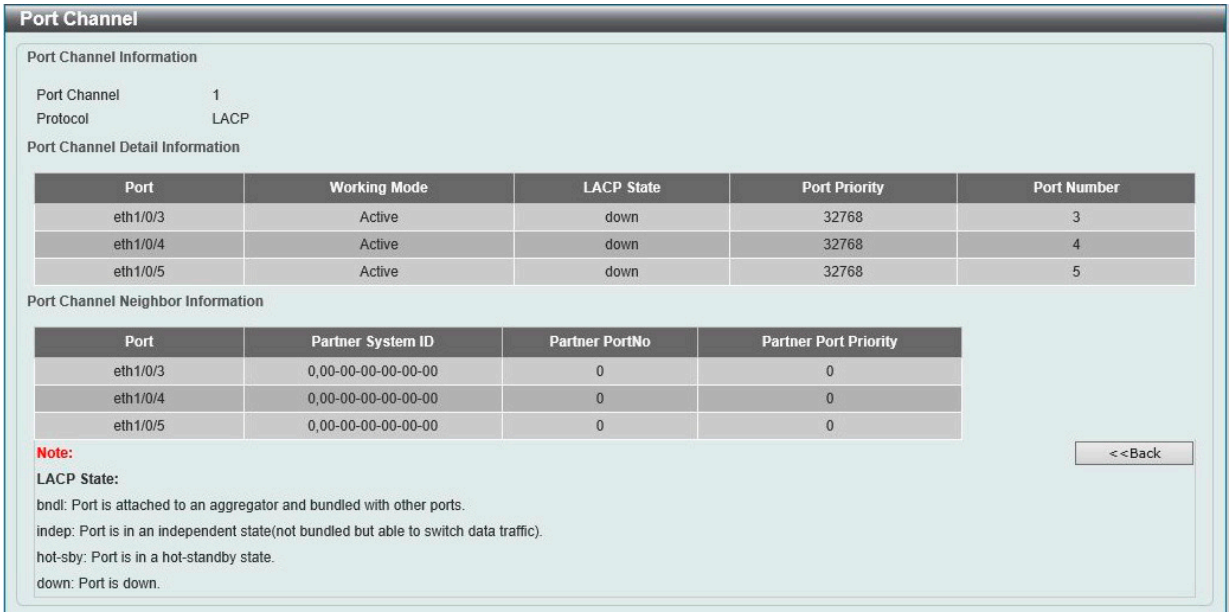


図 8-48　Port Channel 画面

「Back」ボタンをクリックし前の画面に戻ります。

注意　リンクアグリゲーションのアルゴリズムは Source MAC です。

注意　LACP は Short タイムアウトを使用します。

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

IGMP Snooping（IGMP スヌーピング）

IGMP（Internet Group Management Protocol）Snooping 機能を利用すると、スイッチはネットワークステーションまたはデバイスと IGMP ホスト間で送信される IGMP クエリと IGMP レポートを認識するようになります。

IGMP Snooping Settings（IGMP スヌーピング設定）

IGMP Snooping 設定を有効または無効にします。
IGMP Snooping 機能を利用するためには、まず、画面上部の IGMP の「Global Settings」セクションでスイッチ全体に機能を有効にします。「Edit」ボタンをクリックして、各 VLAN の設定を編集することができます。IGMP Snooping を有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバに対するポートを開閉できるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストがもう存在していないと判断すると、マルチキャストパケットの送信を停止します。

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

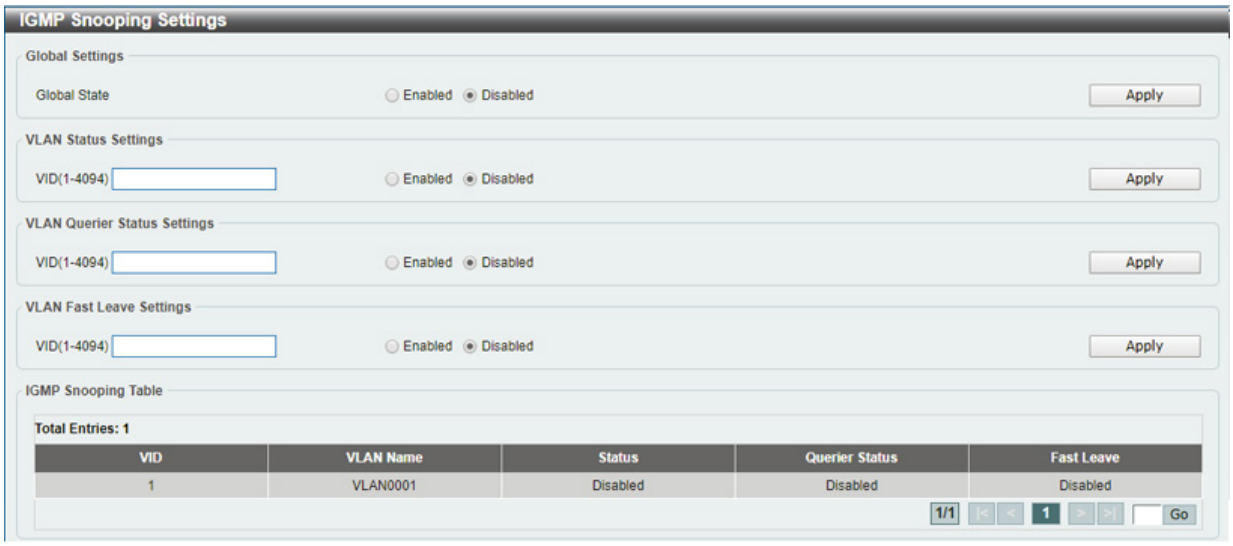


図 8-49　IGMP Snooping Settings 画面

画面には以下の項目があります。

項目	説明
Global Setting	
Global State	IGMP Snooping の有効 / 無効を設定します。 • Enabled - デバイスで IGMP Snooping を有効にします。 • Disabled - デバイスで IGMP Snooping を無効に設定します。（初期値）
VLAN Status Settings	
VID	VLAN 上の IGMP Snooping を有効 / 無効にし、VLAN を識別する VLAN ID（1-4094）を指定します。 • Enabled - VLAN 上での IGMP スヌーピングを有効にします。 • Disabled - VLAN 上での IGMP スヌーピングを無効にします。（初期値）
VLAN Querier Status Settings	
VID	IGMP Snooping Table 上の VLAN を表示させるための VLAN ID（1-4094）を指定します。 • Enable - VLAN 上の IGMP スヌーピングクエリアを有効にします。 • Disable - VLAN 上の IGMP スヌーピングクエリアを無効にします。(初期値）
VLAN Fast Leave Settings	
VID	VLAN 上の IGMP Snooping Fast Leave を有効 / 無効にし、VLAN を識別する VLAN ID（1-4094）を指定します。 • Enable - VLAN 上の IGMP Fast Leave を有効にします。 • Disable - VLAN 上の IGMP Fast Leave を無効にします。(初期値）

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

IGMP Snooping Group Settings（IGMP Snooping グループ設定）

IGMP スヌーピングスタティックグループの設定 / 表示、IGMP スヌーピンググループの表示を行います。

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

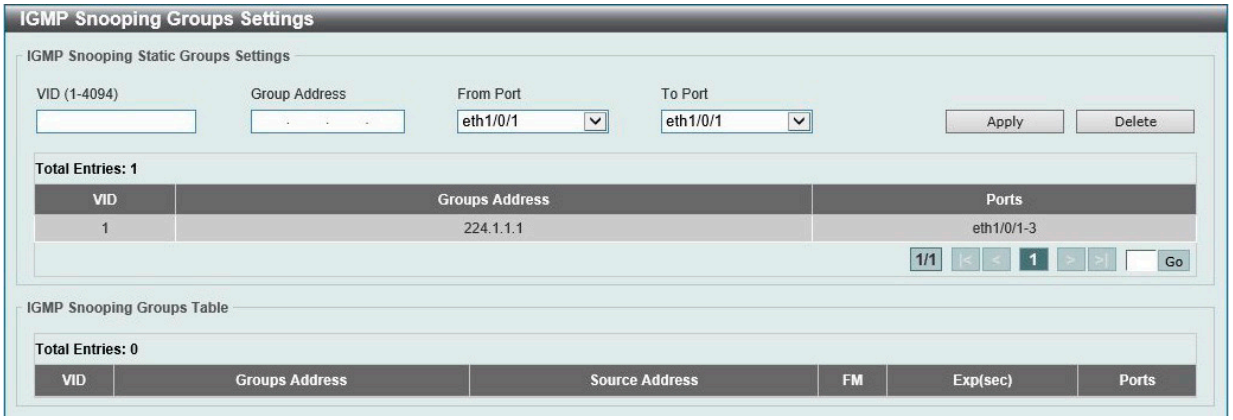


図 8-50　IGMP Snooping Group Settings 画面

以下の項目を使用して、設定します。

IGMP Snooping Static Group Settings（IGMP スヌーピングスタティックグループ設定）

項目	説明
IGMP Snooping Static Groups Settings	
VID	登録または削除するマルチキャストグループの VLAN ID。
Group Address	登録または削除するマルチキャストグループの IP アドレス。
From Port / To Port	設定するポートの範囲を設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

MLD Snooping（MLD スヌーピング）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じように使用される IPv6 機能です。マルチキャストデータを要求する VLAN に接続しているポートを検出するために使用されます。選択した VLAN 上のすべてのポートにマルチキャストトラフィックが流れる替わりに、MLD Snooping は、リクエストポートとマルチキャストの送信元によって生成する MLD クエリと MLD レポートを使用してデータを受信したいポートにのみマルチキャストデータを転送します。

MLD Snooping は、エンドノードと MLD ルータ間で交換される MLD コントロールパケットのレイヤ 3 部分を調査することで実行されます。ルータがマルチキャストトラフィックをリクエストしていることをスイッチが検出すると、該当ポートを IPv6 マルチキャストテーブルに直接追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のこのエントリは該当ポート、その VLAN ID、および関連する IPv6 マルチキャストグループアドレスを記録し、このポートをアクティブな Listening ポートと見なします。アクティブな Listening ポートはマルチキャストグループデータの受信だけをします。

MLD コントロールメッセージ

MLD Snooping を使用するデバイス間で 3 つのタイプのメッセージを交換します。これらのメッセージは、130、131、132 および 143 にラベル付けされた 4 つの ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query – IPv4 の IGMPv2 Host Membership Query（HMQ）と類似のものです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query は全マルチキャストアドレスに Listening ポートすべてにマルチキャストデータを送信する準備が整ったことを通知するために使用します。また、Multicast Specific query は特定のマルチキャストアドレスに送信準備が整ったことを通知するために使用します。 2 つのメッセージタイプは IPv6 ヘッダ内のマルチキャスト終点アドレス、および Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別します。
2. Multicast Listener Report Version1 – IGMPv2 の Host Membership Report（HMR）と類似のものです。Listening ホストは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。
3. Multicast Listener Done – IGMPv2 の Leave Group Message と類似のものです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからマルチキャストデータを受信せず、このアドレスからのマルチキャストデータとともに”done”（完了）した旨を伝えます。スイッチは本メッセージを受信すると、この Listening ホストには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しません。

MLD Snooping Settings（MLD スヌーピング設定）

MLD Snooping 設定を有効または無効にします。

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

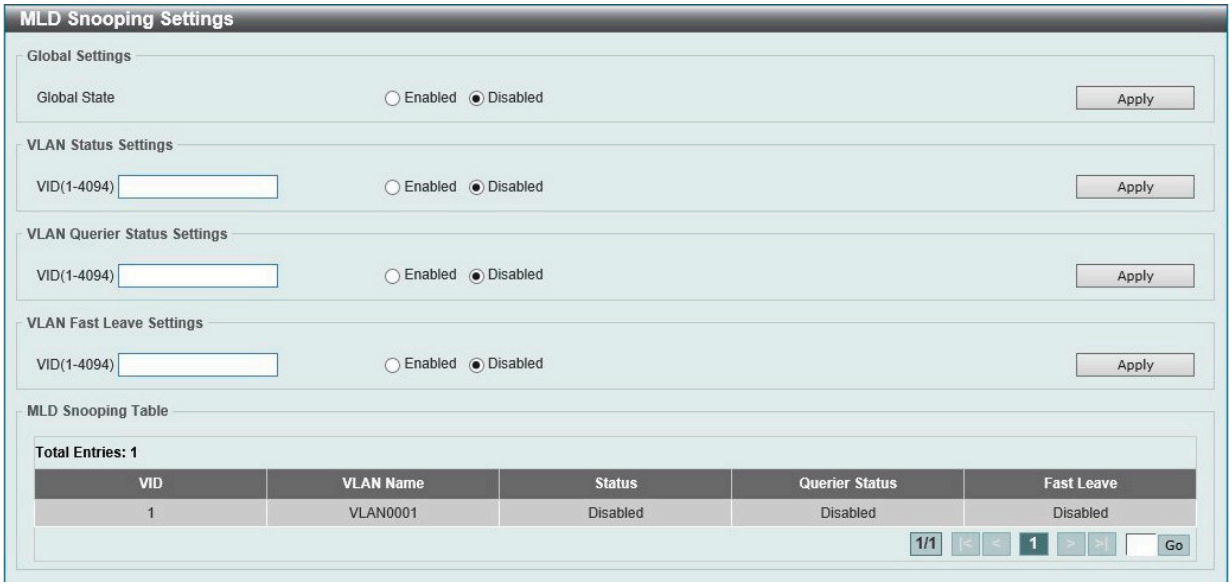


図 8-51　MLD Snooping Settings 画面

画面には以下の項目があります。

項目	説明
Global Setting	
Global State	MLD Snooping の有効 / 無効を設定します。 • Enabled - デバイスで MLD Snooping を有効にします。 • Disabled - デバイスで MLD Snooping を無効に設定します。（初期値）
VLAN Status Settings	
VID	VLAN 上の MLD Snooping を有効 / 無効にし、VLAN を識別する VLAN ID（1-4094）を指定します。 • Enabled - VLAN 上での MLD スヌーピングを有効にします。 • Disabled - VLAN での MLD スヌーピングを無効にします。（初期値）
VLAN Querier Status Settings	
VID	VLAN 上の MLD Snooping クエリアを有効 / 無効にし、VLAN を識別する VLAN ID（1-4094）を指定します。 • Enabled - VLAN 上での MLD スヌーピングクエリアを有効にします。 • Disabled - VLAN での MLD スヌーピングクエリアを無効にします。（初期値）
VLAN Fast Leave Settings	
VID	VLAN 上の MLD Snooping Fast Leave を有効 / 無効にし、VLAN を識別する VLAN ID（1-4094）を指定します。 • Enable - VLAN 上の MLD Fast Leave を有効にします。 • Disable - VLAN 上の MLD Fast Leave を無効にします。（初期値）

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

MLD Snooping Group Settings（MLD Snooping グループ設定）

MLD スヌーピングスタティックグループの設定と表示および MLD スヌーピンググループの表示に使用されます。

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

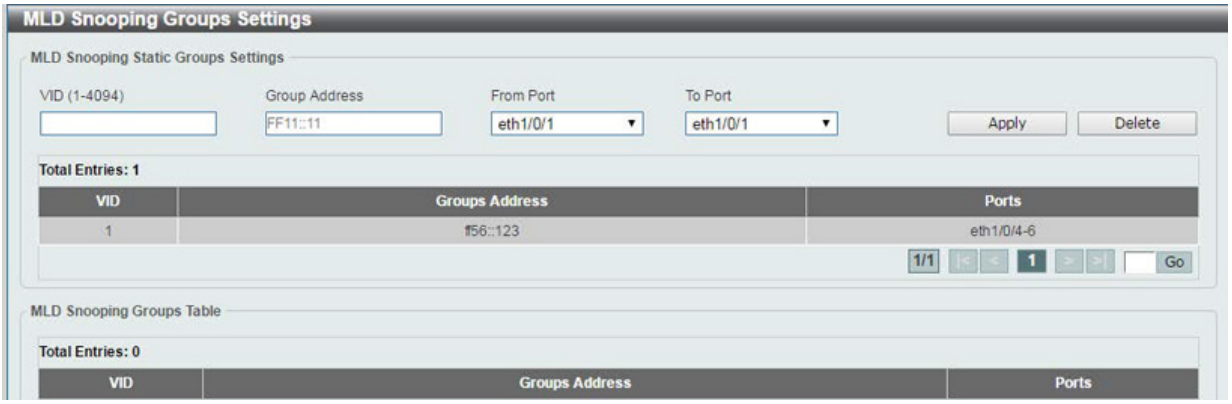


図 8-52　MLD Snooping Group Settings 画面

以下の項目を使用して、設定します。

MLD Snooping Static Group Settings（MLD スヌーピングスタティックグループ設定）

項目	説明
MLD Snooping Static Groups Settings	
VID	登録または削除する IPv6 マルチキャストグループの VLAN ID。
Group Address	登録または削除する IPv6 マルチキャストグループの IP アドレス。
From Port / To Port	設定するポートの範囲を設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

注意　既知の問題により、WebGUI で MLD スヌーピングのスタティックグループを追加することができません。グループを追加する場合は CLI をご利用ください。本問題は次のファームウェアで修正予定です。

Multicast Filtering（マルチキャストフィルタリング）

プロファイルを追加し、指定したスイッチポートに受信するマルチキャストアドレスレポートを設定します。

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

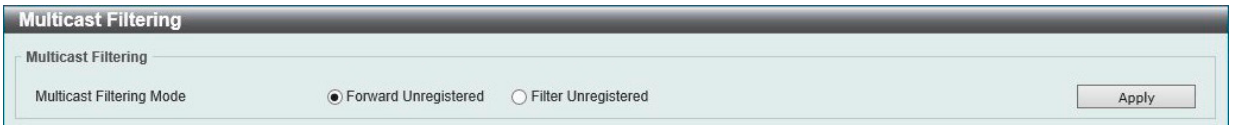


図 8-53　Multicast Filtering 画面

以下の項目を使用して、設定します。

項目	説明
Multicast Filter Mode	マルチキャストフィルタモードを選択します。「Forward Unregistered」「Filter Unregistered」から選択可能です。 • 「Forward Unregistered」- 選択すると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 ドメインに基づきフラッドします。 • 「Filter Unregistered」- 選択すると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。

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

注意　MLD Snooping 機能において、Multicast Filtering を Filter Unregistered に設定している場合、Listener Report と LLMNR はフラッディングされません。ただし、IPv6 マルチキャストルータが存在する場合はフラッディングします。

LLDP（LLDP 設定）

LLDP（Link Layer Discovery Protocol）の設定を行います。

LLDP Global Settings（LLDP グローバル設定）

LLDP（Link Layer Discovery Protocol）のグローバル設定を行います。

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

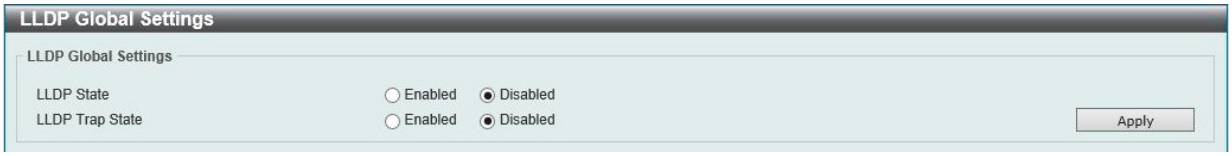


図 8-54　LLDP Global Settings 画面

以下の項目を設定できます。

項目	説明
LLDP State	スイッチにおける LLDP 機能を「Enabled」（有効）または「Disabled」（無効）にします。
LLDP Trap State	LLDP Trap を有効 / 無効に指定します。

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

LLDP Neighbor Port Information（LLDP ネイバポート情報）

Neighbor から学習したポート情報を表示します。スイッチはリモートステーションからパケットを受信しますが、情報はローカルに保存します。

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

図 8-55　LLDP Neighbor Port Information 画面

第 9 章　QoS（QoS 機能の設定）

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

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

サブメニュー	説明
802.1p Priority（802.1p プライオリティ）	802.1p Priority ではポートに default CoS 設定を行います。
Port Rate Limiting（ポートレート制限設定）	ポートレート制限の設定を行います。
Port Trust State（ポートトラスト設定）	ポートトラスト設定と表示を行います。
DSCP CoS Mapping（DSCP CoS マップ設定）	DSCP CoS マップの設定と表示を行います。

802.1p Priority（802.1p プライオリティ）

802.1p Priority ではポートに default CoS 設定を行います。

QoS > 802.1p Priority の順にメニューをクリックし、以下の画面を表示します。

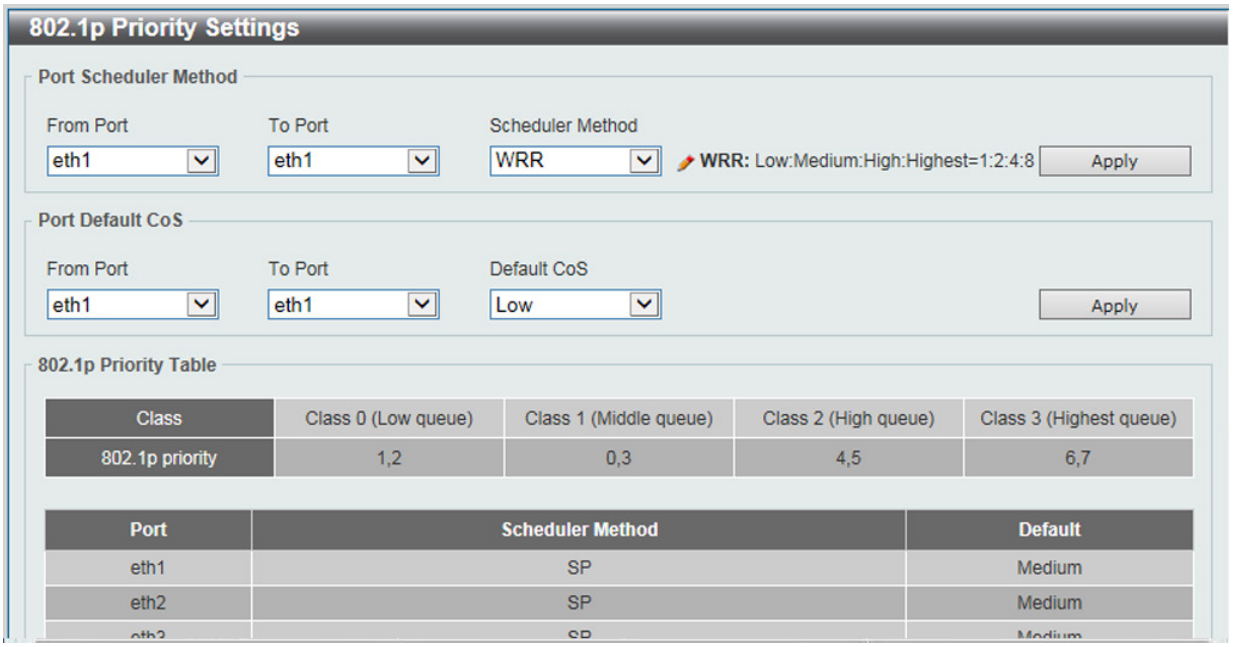


図 9-1　P802.1p Priority 画面

本画面には以下の項目があります。

項目	説明
Port Scheduler Method（ポートスケジューリング方法）	
From Port / To Port	設定するポート / ポート範囲を入力します。
Scheduler Method	指定ポートに対するスケジューリングの方法を設定します。「Strict Priority」(SP)、「Weighted Round-Robin」(WRR) から指定できます。初期値ではアウトプットキュースケジューリングアルゴリズムは「WRR」です。 SP モードでの CoS キューの設定はより優先値の高い CoS キューがストリクトプライオリティーモードで設定されている必要があります。WRR ではプライオリティのサービスクラスで配分されたパケットを重み付けされたラウンドロビン（WRR）アルゴリズムによって処理します。通常各キューの重みが設定の重みとなります。優先値の高い CoS キューからパケットが送信されると、関連した重みづけ（Weight）が 1 差し引かれ、次に低い CoS キューのパケットが実行されます。CoS キューの重みづけ（Weight）がゼロになると、補完されるまでキューは実行されません。すべての CoS キューの重みづけ（Weight）が 0 に到達すると同時にその重みづけ（Weight）は補完されます。
Port Default CoS（ポート初期 CoS）	
From Port/To Port	設定するポート範囲を指定します。
Default CoS	ポートに初期 CoS を指定します。「Highest」「High」「Medium」「Low」で指定可能です。

「Apply」ボタンをクリックして行った変更を適用します。

注意　WRR 使用時には、以下の重みづけとなります。

- Class0 (Low queue) : Class1 (Middle queue) : Class2 (High queue) : Class3 (Highest queue) = 1 : 2 : 4 : 8

Port Rate Limiting（ポートレート制限設定）

ポートレート制限の設定を行います。

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

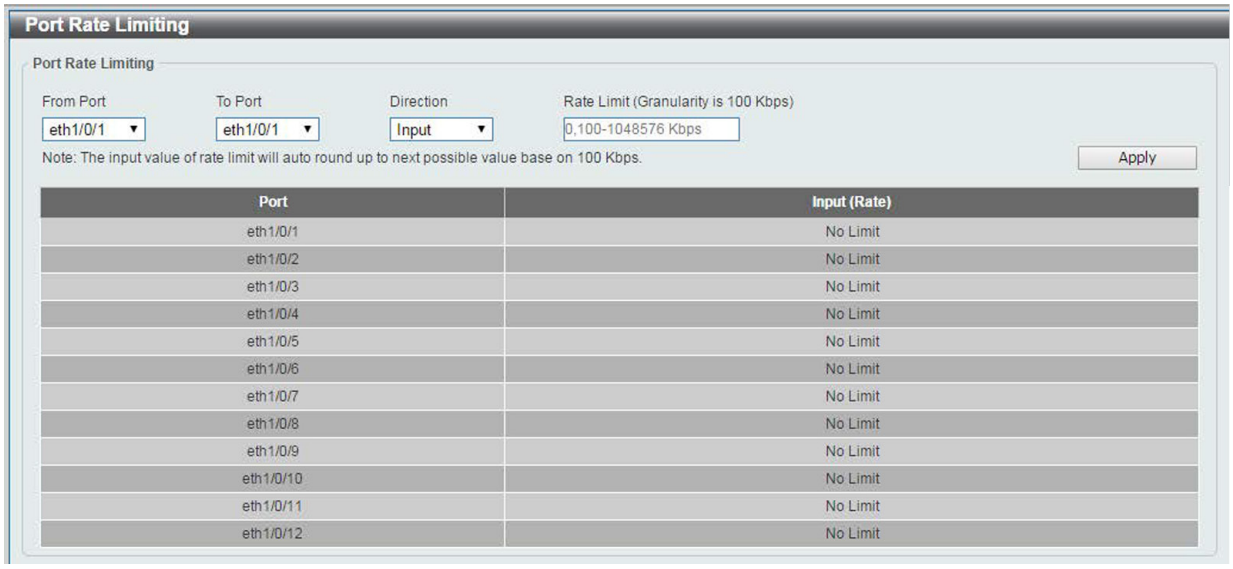


図 9-2　Port Rate Limiting 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	設定するポート / ポート範囲を入力します。
Direction	レート制限の対象を選択します。Input（イングレス）のみサポートしています。
Rate Limit	レート制限の値を指定します。「100Kbps」から「1048576Kbps」の値を選択可能です。

「Apply」ボタンをクリックして行った変更を適用します。

注意　ポートレート制限において、Egress（イーグレス）レート制限の設定はできません。

Port Trust State（ポートトラスト設定）

本スイッチにおけるポートトラスト設定と表示を行います。

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

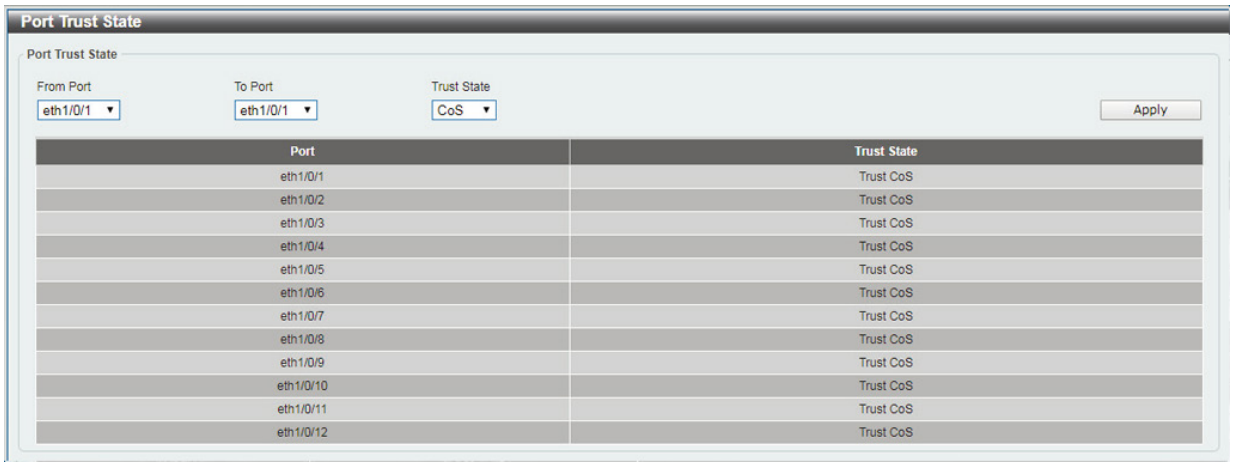


図 9-3　Port Trust State 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	設定するポート / ポート範囲を入力します。
Trust State	ポートトラストの設定をします。「CoS」「DSCP」から選択可能です。

「Apply」ボタンをクリックして行った変更を適用します。

DSCP CoS Mapping（DSCP CoS マップ設定）

本スイッチにおける DSCP CoS マップの設定と表示を行います。

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

図 9-4　DSCP CoS Mapping 画面

本画面には以下の項目があります。

項目	説明
CoS	CoS の値を指定します。0 から 7 の間で指定可能です。
DSCP List (0-63)	DSCP リストの値を入力します。0 から 63 の範囲で設定します。

「Apply」ボタンをクリックして行った変更を適用します。

第 10 章　Security（セキュリティ機能の設定）

本セクションではデバイスのセキュリティの設定について解説します。

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

サブメニュー	説明
Port Security（ポートセキュリティ）	ポートセキュリティ機能の設定 / 表示を行います。
802.1X（802.1X 設定）	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。
RADIUS（RADIUS 設定）	RADIUS の設定を行います。
Web-based Access Control（Web 認証）	Web 認証の設定を行います。
Safeguard Engine Settings（セーフガードエンジン設定）	セーフガードエンジン設定を行います。
Traffic Segmentation（トラフィックセグメンテーション）	トラフィックセグメンテーション設定を行います。
Storm Control（ストームコントロール）	ストームコントロールの設定を行います。
DoS Attack Prevention Settings（DoS 攻撃防止設定）	DoS 攻撃防止設定を行います。
Zone Defense Settings（ゾーンディフェンス設定）	ゾーンディフェンスの設定を行います。
SSH（Security Shell ）	SSH の設定を行います。
SSL（Secure Socket Layer）	SSL（Secure Socket Layer）の設定を行います。

Port Security（ポートセキュリティ）

Port Security Global Settings（ポートセキュリティグローバル設定）

本項目ではポートセキュリティ機能のグローバルでの設定 / 表示を行います。ポートセキュリティは、不正なホストからのポートへの接続とネットワークへのアクセスを防ぐセキュリティ機能です。

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

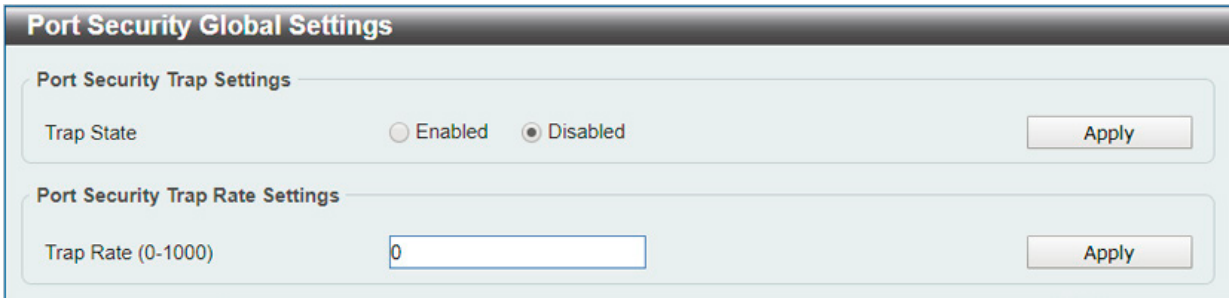


図 10-1　Port Security Global Settings 画面

本画面には以下の項目があります。

項目	説明
Trap State	ポートセキュリティトラップ設定を「Enabled」（有効）または「Disabled」（無効）にします。
Trap Rate	毎秒のトラップ数を指定します。0 から 1000 までの間で指定できます。初期値の 0 は SNMP トラップがあらゆるセキュリティ違反に対して動作することを意味します。

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

Port Security Port Settings（ポートセキュリティポート設定）

ポートセキュリティのポート設定と設定内容の表示を行います。

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

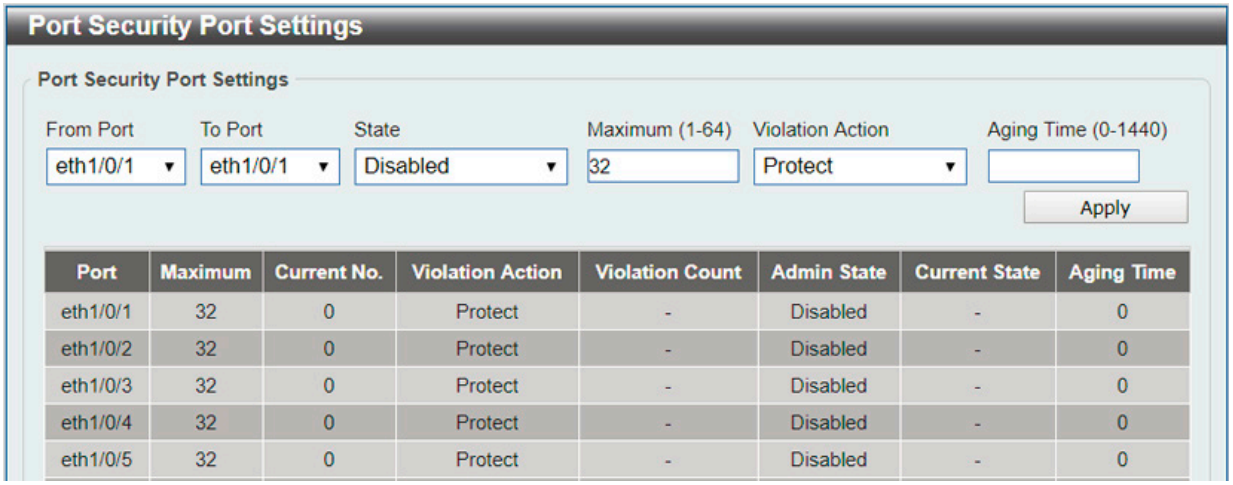


図 10-2　Port Security Port Settings 画面

本画面には以下の項目があります。

項目	説明
From Port/To Port	設定の対象となるポートを指定します。
State	指定ポートへのポートセキュリティ機能を有効 / 無効にします。
Maximum	指定ポートで許可される安全な MAC アドレスの最大数を指定します。0 から 64 まで指定可能で初期値は 32 です。
Violation Action	違反に対する動作を指定します。「Protect」「Restrict」「Shutdown」から指定可能です。 「Protect」を選択すると、ポートセキュリティレベルで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反カウントとしては数えられません。 「Restrict」を選択すると、ポートセキュリティレベルで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントされシステムログに記録されます。 「Shutdown」を選択すると、セキュリティ違反があるとポートをシャットダウンし、システムログに記録されます。
Aging Time	指定ポートの自動取得アドレスに使用するエージングタイムです。0 から 1440 分の間で指定可能です。

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

Port Security Address Entries（ポートセキュリティアドレスエントリ設定）

ポートセキュリティアドレスエントリの設定、表示を行います。

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

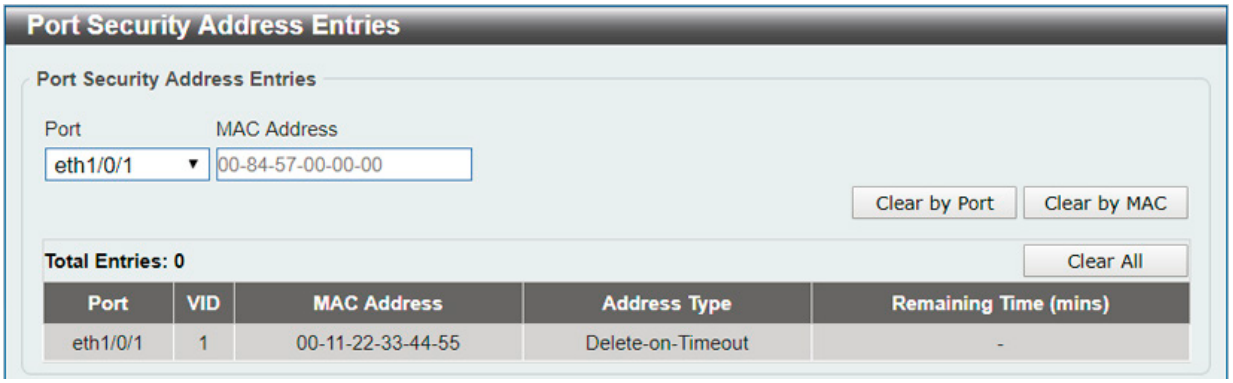


図 10-3　Port Security Address Entries 画面

本画面には以下の項目があります。

項目	説明
Port	設定の対象となるポートを指定します。
MAC Address	MAC アドレスを入力します。

「Clear by Port」ボタンをクリックし、選択したポートに基づく情報を消去します。
「Clear by MAC」ボタンをクリックし、選択した MAC アドレスに基づく情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

802.1X（802.1X 設定）

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

本画面では 802.1X グローバル設定を行います。

802.1X 認証設定をするには、**Security > 802.1X > 802.1X Global Settings** の順にメニューをクリックします。

図 10-4　802.1X Global Settings 画面

以下の項目が表示されます。

項目	説明
802.1X State	802.1X 認証を有効 / 無効に設定します。
Authentication Method	認証方式を「RADIUS」「Local User」から選択します。
Foward PDU	PDU 転送機能を有効 / 無効に設定します。
Re-authenticate	再認証を有効 / 無効に設定します。
Re-authenticate Period	再認証の間隔を指定します。
MaxReq	バックエンドの認証ステートマシンが、認証プロセスを再開する前に、クライアントに対して Extensible Authentication Protocol（EAP）リクエストフレームを再送する最大回数（1-10）を指定します。
Server Timeout	サーバのタイムアウト時間を指定します。1 から 65535 までの間で指定できます。
Supp Timeout	クライアントのタイムアウト時間を指定します。1 から 65535 までの間で指定できます。
TX Period	送信間隔を指定します。1 から 65535 までの間で指定できます。

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

注意　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。

802.1X Port Settings（802.1X ポート設定）

802.1X 認証ポートを設定します。

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

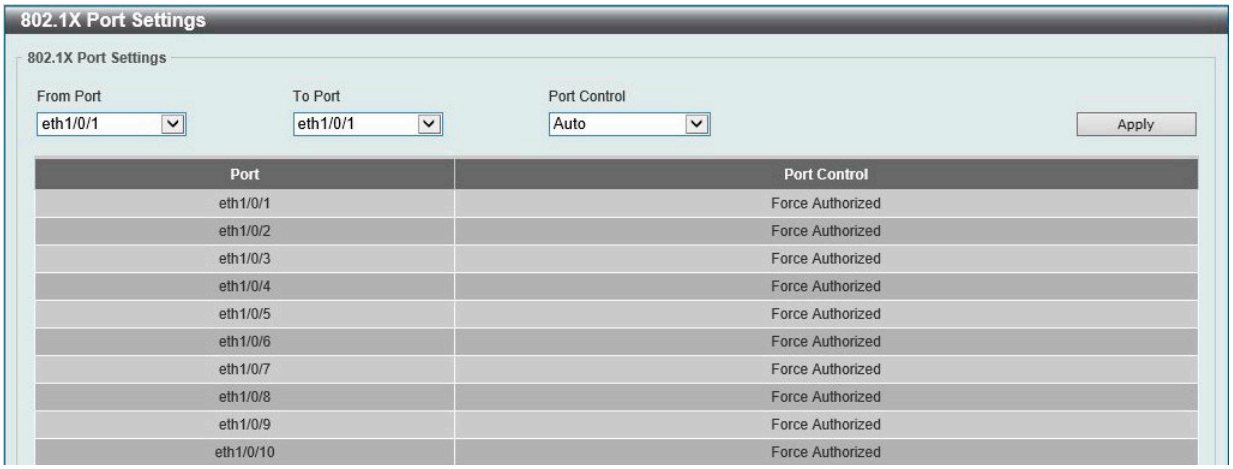


図 10-5　802.1X Settings 画面

以下の項目が表示されます。

項目	説明
From Port/To Port	本設定を適用するポート範囲を指定します。
Port Control	ポートの認証状態を指定します。 • 「ForceAuthorized（認証強制）」- 認証情報の交換を行わずに、ポートを「authorized」（認証）状態に変更します。 • 「Auto（自動）」- 802.1X 認証の結果に従って、ポートの状態（authorized または unauthorized）を決定します。 • 「ForceUnauthorized（未認証強制）」- クライアントからの認証要求を無視し、ポートを「unauthorized」（未認証）状態のままとします。ポートへのアクセスはブロックされます。

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

802.1X Local User（802.1X ローカルユーザ）

802.1X ローカルユーザを作成します。

Security > 802.1X > 802.1X Local User の順にメニューをクリックし、以下の画面を表示します。

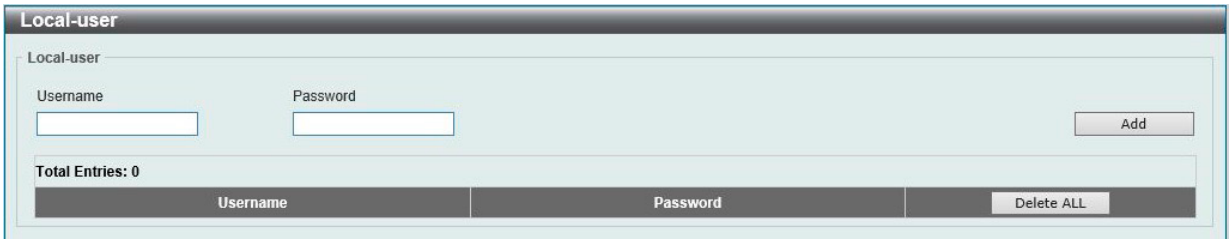


図 10-6　802.1X Local User 画面

以下の項目が表示されます。

項目	説明
User Name	ユーザ名を入力します。
Password	パスワードを入力します。

「Add」ボタンをクリックして、ユーザを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Delete ALL」ボタンをクリックして、テーブル上のすべてのユーザを削除します。

Authentication Session Information（認証セッション情報）

認証セッションの状態を表示します。

Security > 802.1X > Authentication Session Information の順にメニューをクリックし、以下の画面を表示します。

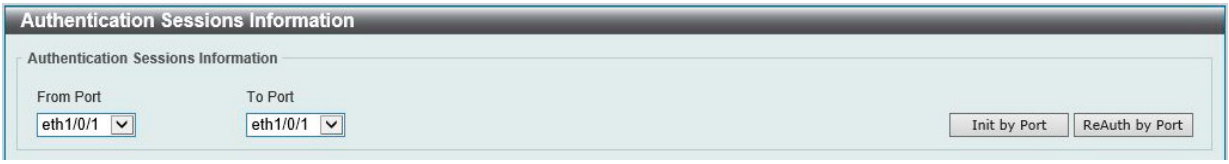


図 10-7　Authentication Session Information 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。
From Port/To Port	表示するポート範囲を指定します。

「Init by Port」ボタンをクリックして、指定ポートに基づくセッション情報を初期化します。
「ReAuth by Port」ボタンをクリックして、指定ポートに基づくセッション情報を再認証（Re-Authenticate）します。

Authenticator Statistics（オーセンティケータ統計情報）

オーセンティケータの統計情報を表示します。

Security > 802.1X > Authenticator Statistics の順にメニューをクリックし、以下の画面を表示します。

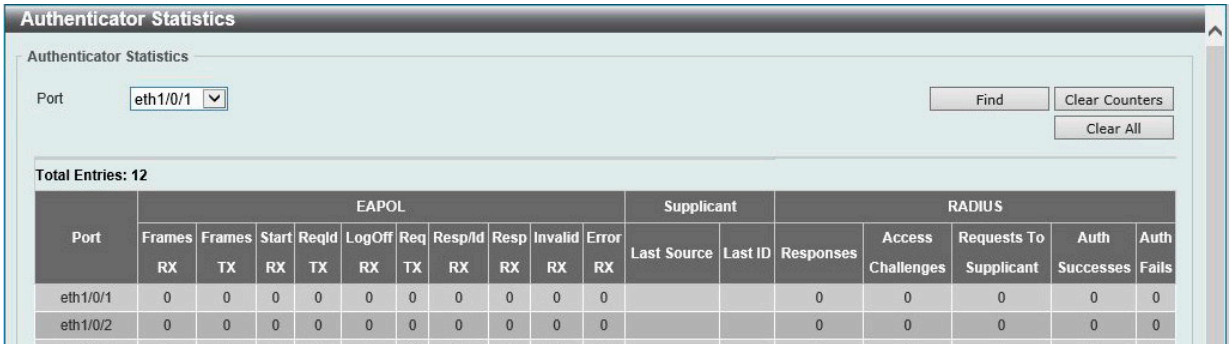


図 10-8　Authenticator Statics 画面

以下の項目が表示されます。

項目	説明
Port	表示するポート範囲を指定します。

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Clear Counters」ボタンをクリックして、指定条件に基づく情報を削除します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を削除します。

テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

RADIUS（RADIUS 設定）

RADIUS Global Settings（RADIUS グローバル設定）

RADIUS をグローバルに有効 / 無効にします。

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

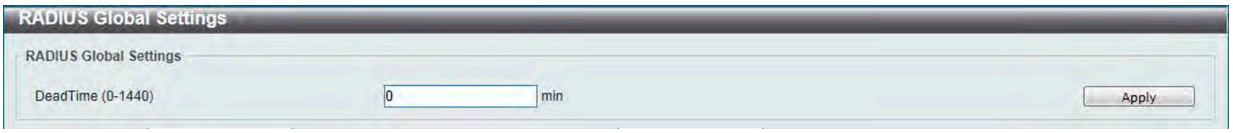


図 10-9　RADIUS Global Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
DeadTime (0-1440)	デッドタイムの設定を行います。1 から 1440（分）の間で指定できます。初期値は「0」です。0 に設定されている場合、応答しないサーバは「Dead」として認識されることはありません。この設定により、応答しないサーバホストエントリをスキップする「デッドタイム」が設定され認証プロセスは改善されます。システムが認証サーバと連携して動作する場合、一度に一つのサーバと連携します。もし連携しようとしたサーバが応答しない場合、システムは次のサーバとの連携を模索します。システムにより応答しないサーバが見つけられると、該当のサーバは「down」として認識され、「デッドタイム」タイマーが開始され、それ以後のリクエスト認証はデッドタイム時間が過ぎるまでスキップされます。

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

RADIUS Server Settings（RADIUS サーバの設定）

外部 RADIUS サーバの設定を行います。

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

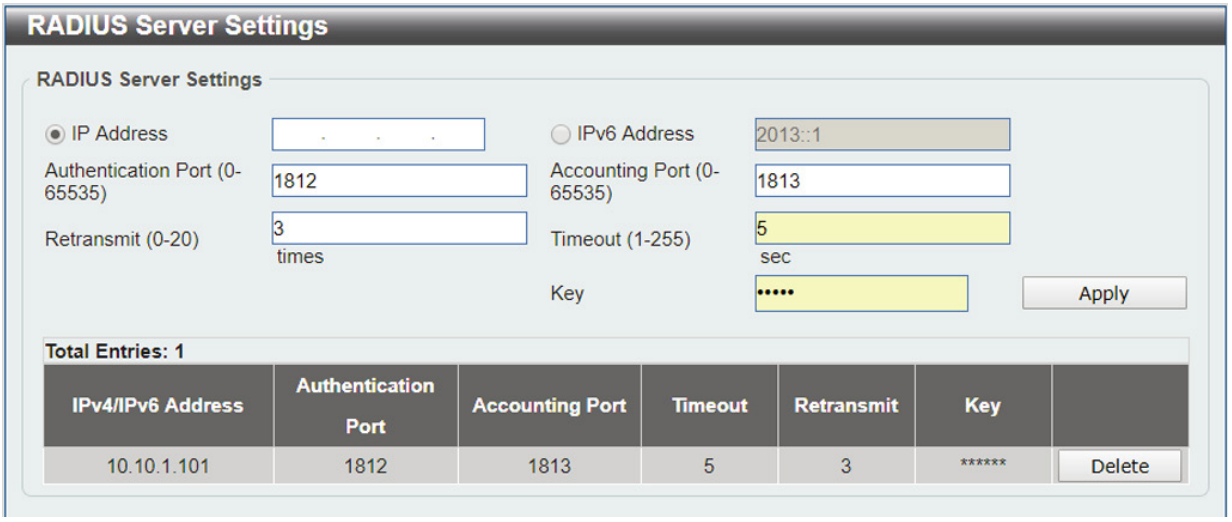


図 10-10　RADIUS Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。
Authentication Port (0-65535)	RADIUS 認証サーバの UDP ポートです。初期値は 1812 です。認証しない場合は、0 を使用します。
Accounting Port (0-65535)	RADIUS アカウントサーバのポートです。初期値は 1813 です。アカウンティングを使用しない場合は、0 を使用します。
Retransmit (0-20)	RADIUS サーバの再転送回数（0-20）を設定します。初期値は 3 です。このオプションを無効にするには、0 を設定します。
Timeout (1-255)	RADIUS サーバのタイムアウト時間（秒）を設定します。初期値は 5（秒）です。
Key	RADIUS サーバに設定したものと同一の鍵を指定します。32 文字以内で指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして指定エントリを削除します。

RADIUS Statistic（RADIUS 統計情報）

RADIUS 統計情報の表示、設定を行います。

Security > RADIUS > RADIUS Statistic Settings をクリックし、以下の画面を表示します。

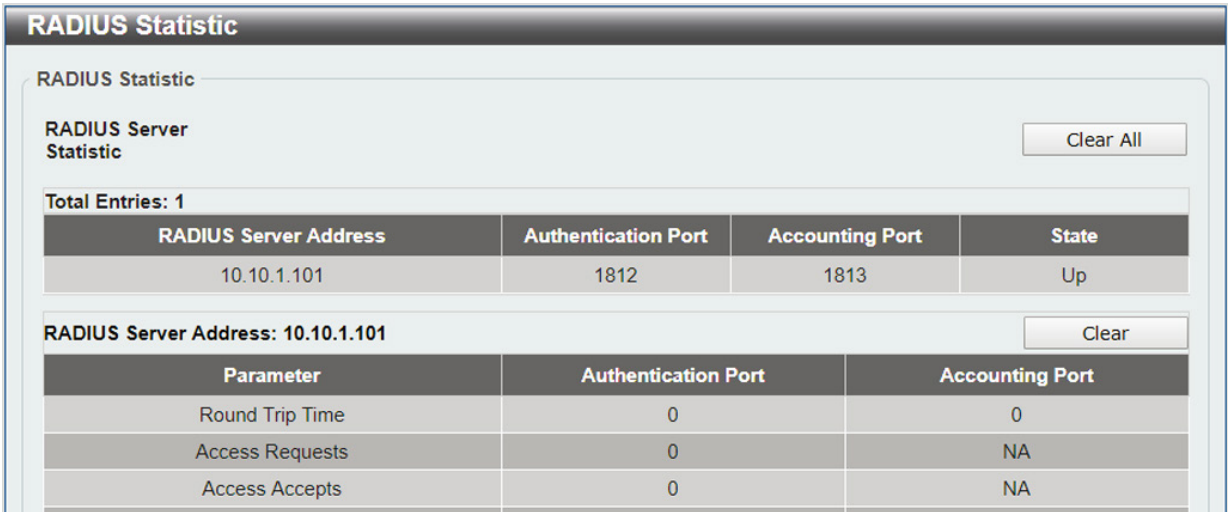


図 10-11　RADIUS Statistic 画面

「Clear」ボタンをクリックし、選択に基づいて表示した情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

Web-based Access Control（Web 認証）

Web ベース認証のログインは、スイッチを経由してインターネットにアクセスを試みる場合に、ユーザを認証するように設計された機能で、認証処理には HTTP/HTTPS プロトコルを使用します。

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

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

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

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

仮想 IP と PC が同じであると、WAC が有効なポートに接続するホストは、IP アドレスを実際に所有しているサーバまたは PC とは通信ができません。ホストがサーバまたは PC にアクセスする必要がある場合、仮想 IP をサーバまたは PC の 1 つと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、PC のユーザは、認証を適切に実行するために、プロキシ設定の例外として仮想 IP を加える必要があります。

認証 Web ページの初期プロトコルは HTTP になります。HTTPs での認証を行う場合、Web サーバ設定で HTTPs に変更します。

条件および制限

1. アクセスプロファイル機能のように、スイッチ上に存在する機能の中には HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
2. 認証に RADIUS サーバを使用する場合、Web 認証を有効にする前に、ターゲット VLAN を含む必要な項目を入力して RADIUS サーバの設定を行ってください。

Web Authentication（Web 認証設定）

スイッチの Web 認証設定をに行います。

Security > Web-based Access Control > Web Authentication をクリックして、以下の画面から設定します。

図 10-12　Web Authentication 画面

以下の項目を使用して、設定を行います。

項目	説明
Web Authentication State	Web 認証機能を「Enable」（有効）/「Disable」（無効）にします。
Trap State	Web 認証のトラップの状態を有効 / 無効にします。
Virtual IPv4	仮想 IP アドレスを入力します。Web 認証の仮想 IP は WAC にだけ使用され、スイッチの他のモジュールでは使用されません。すべての Web 認証のプロセスはこの IPv4 アドレスとの連携で行われますが、しかし仮想 IP はどの ICMP パケットや ARP リクエストにも応答しません。そのため仮想 IP はスイッチのインタフェースやホスト PC と同じサブネットに設定することはできません。でなければ Web 認証は正しく動作しません。設定した URL は仮想 IP アドレスが設定されている場合のみ有効です。DNS サーバに格納されている FQDN URL を取得して仮想 IP アドレスを取得します。取得した IP アドレスは本コマンドで指定した仮想 IP アドレスと一致する必要があります。もし仮想 IPv4 アドレスが設定されない場合、IPv4 アクセスは Web 認証を開始することができません。
Virtual IPv6	仮想 IPv6 アドレスを入力します。もし仮想 IPv6 アドレスが設定されない場合、IPv6 アクセスは Web 認証を開始することができません。
Redirection Path	認証に成功し、ターゲット VLAN に割り当てられたユーザを導く Web サイトの URL を入力します。128 文字以内で指定できます。

「Apply」ボタンをクリックし、設定を有効にします。

注意　仮想 IP アドレスを「0.0.0.0」もしくはスイッチの IPIF（IP インターフェイス）と同一のサブネットに設定した場合、WAC 機能は正常に動作しません。

WAC Port Settings（Web 認証ポート設定）

Web 認証用のユーザアカウントを登録するには、**Security > Web-based Access Control > WAC Port Settings** をクリックし、以下の設定用画面を表示します。

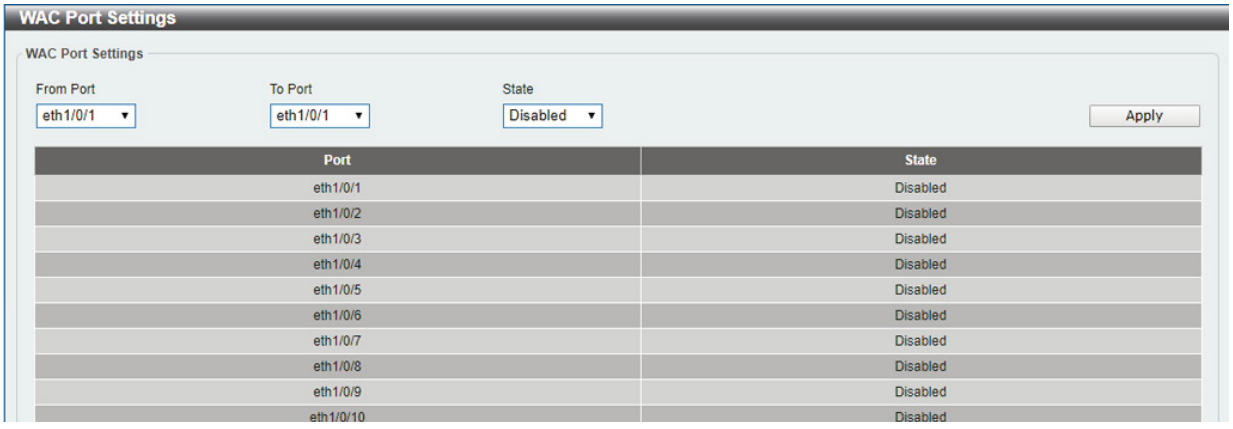


図 10-13　WAC Port Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
From Port / To Port	ポート範囲を設定します。
State	本機能を「Enabled」（有効）/「Disabled」（無効）にします。

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

WAC Customize Page（WAC カスタマイズページ設定）

Web 認証ページの項目をカスタマイズします。

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

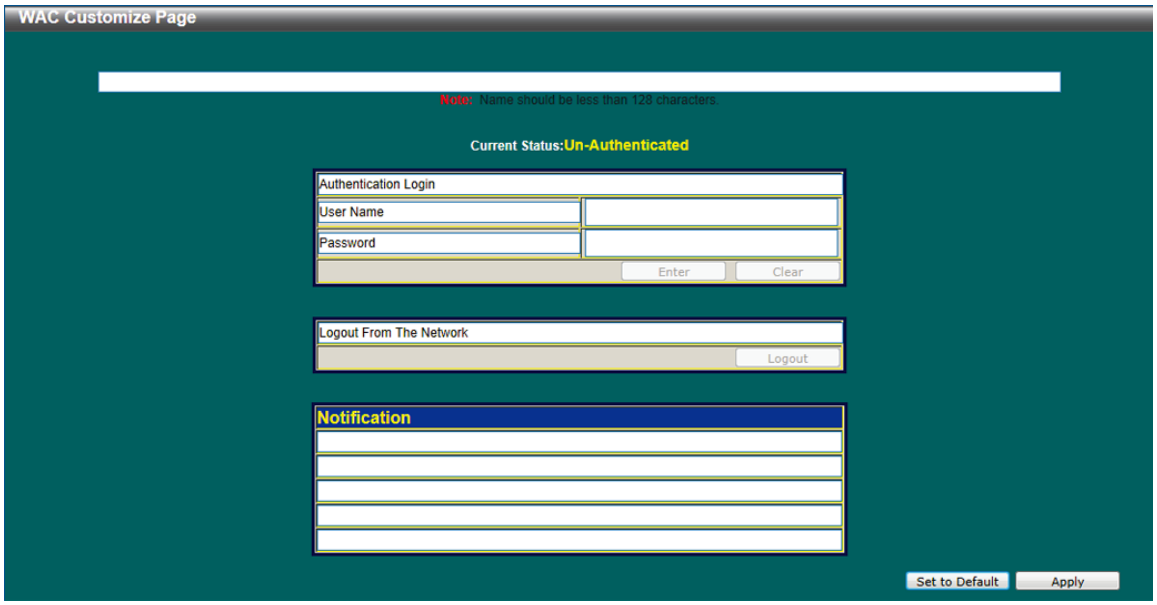


図 10-14　WAC Customize Page 画面

以下の項目を使用して、設定を行います。

項目	説明
Page Title	カスタムページタイトルとなるメッセージを入力します。128 文字まで入力可能です。
Login window Title	カスタムログインウィンドウタイトルを入力します。64 文字まで入力可能です。
User Name Title	カスタムユーザ名タイトルを入力します。32 文字まで入力可能です。
Password Title	カスタムパスワードタイトルを入力します。32 文字まで入力可能です。
Logout window Title	カスタムログアウトウィンドウタイトルを入力します。64 文字まで入力可能です。
Notification	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。

WAC ページの設定を行うためにはこの画面の WAC 認証情報をすべて入力して「Apply」ボタンをクリックして行った変更を適用します。
「Set to Default」ボタンをクリックして、全項目を初期設定に復元します。

注意　ASCII 文字のみ使用可能です。

Safeguard Engine Settings（セーフガードエンジン設定）

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃によりスイッチの CPU はその対応量を超えて増加してしまう可能性があります。このような問題を軽減するために、本スイッチのソフトウェアにセーフガードエンジン機能を付加しました。
セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。
もし CPU の稼働がしきい値を超えた場合、セーフガードエンジンは起動し、スイッチは省パワーモード（exhausted mode）へ移行します。省パワーモード（exhausted mode）の場合、スイッチは ARP と IP パケットのための帯域を制限します。もし CPU の稼働がしきい値以下に下がった場合、セーフガードエンジンは動作を停止しスイッチは省パワーモードを脱却し通常モードへ移行します。

スイッチにセーフガードエンジンの設定を行うためには、**Security > Safeguard Engine Settings** の順にクリックし、以下の画面を表示します。

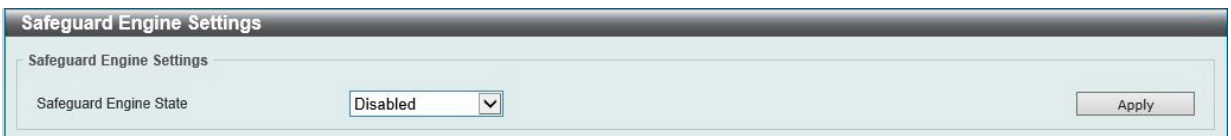


図 10-15　Safeguard Engine Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Safeguard Engine Settings	
Safeguard Engine State	セーフガードエンジン機能を「Enabled」（有効）/「Disabled」（無効）にします。

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

Traffic Segmentation（トラフィックセグメンテーション）

トラフィックセグメンテーション設定を行います。トラフィックセグメンテーション転送ドメインが指定されると、ポートに受信するパケットはドメイン内のインタフェースに転送される L2 パケットに制限されます。ポートの転送ドメインが空の場合、ポートに受信したパケットの L2 転送は制限されません。トラフィックセグメンテーションメンバリストは認証が有効でない場合、コマンドによってポートチャンネルを含めたインタフェースが指定されると、ポートチャネルのすべてのメンバポートは転送ドメインに含まれます。インタフェースの転送ドメインが空の場合、ポートに受信したパケットの L2 転送は制限されません。

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

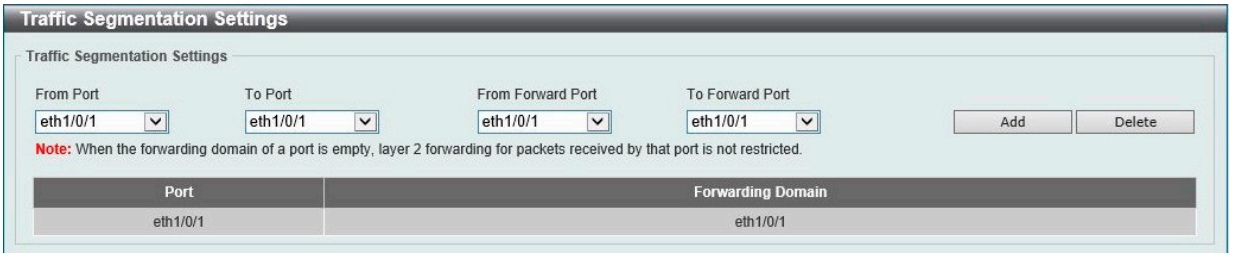


図 10-16　Traffic Segmentation 画面

以下の項目を使用して設定を行います。

項目	説明
From Port / To Port	設定する受信ポート範囲を指定します。
From Forward Port / To Forward Port	設定する転送ポート範囲を指定します。

「Add」ボタンをクリックすると、入力した情報を元に新しいエントリを追加します。
「Delete」ボタンをクリックすると、入力した情報を元にエントリを削除します。

Storm Control（ストームコントロール）

ストームコントロールの設定、表示を行います。

Security > Storm Control の順にクリックします。

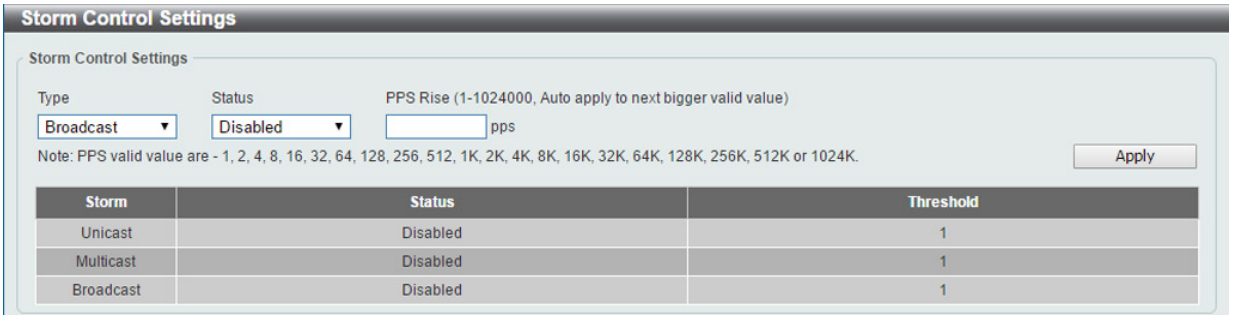


図 10-17　Storm Control 画面

以下の項目を使用して、設定を行います。

項目	説明
Type	コントロールするストームの種類を選択します。「Broadcast」「Multicast」「Unicast」から指定できます。シャットダウンモードで選択すると、ユニキャストは「Known」「Unknown」両方がしきい値に設定してある場合、どちらにも対応しポートはシャットダウンします。そうでない場合は「Unknown」にのみ対応します。
Status	指定したストームのタイプのストームコントロール機能を有効 / 無効に指定します。
PPS Rise	毎秒のパケット増加の上限値について指定します。毎秒増加するパケットの量について上限しきい値を指定します。1 から 1024000 パケット毎秒で指定します。

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

注意　OSPF など予約の Multicast は対象外となりますのでご注意ください。

DoS Attack Prevention Settings（DoS 攻撃防止設定）

各 Denial-of-Service（DoS）攻撃に対して防御設定を行います。

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

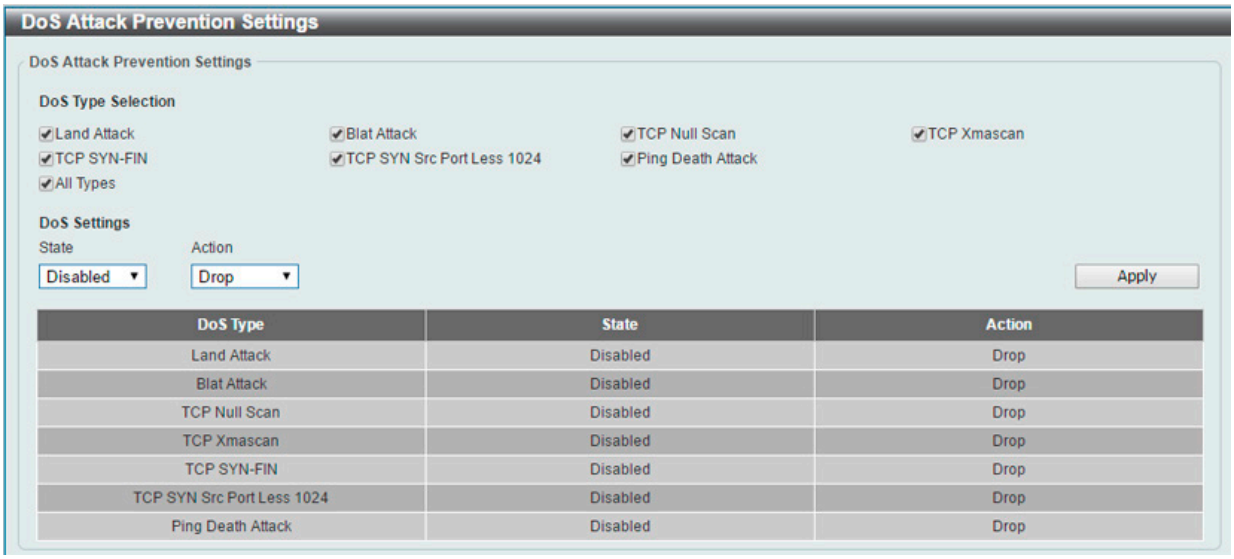


図 10-18　DoS Attack Prevention Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
DoS Attack Prevention Settings	
DoS Type Selection	適切な DoS 攻撃防御のタイプを選択します。 • Land Attack - DoS 攻撃防止タイプに LAND 攻撃を指定します。IP パケットの送信元 / 宛先アドレスがターゲットデバイスのアドレスとして設定されています。ターゲットデバイスに自身のアドレスへの継続的な返信を繰り返させる攻撃です。 • Blat Attack - DoS 攻撃防止タイプに BLAT 攻撃を指定します。ターゲットデバイスの宛先ポートと同様の TCP/UDP 送信元ポートを含むパケットを送信し、ターゲットデバイスに自身に対する回答を行わせる攻撃です。 • TCP Null - DoS 攻撃防止タイプに TCP Null Scan 攻撃を指定します。フラグ無し / シークエンス番号 0 のパケットを使用して、ポートスキャンを行う攻撃です。 • TCP Xmas - DoS 攻撃防止タイプに TCP Xmascan 攻撃を指定します。Urgent (URG)、Push (PSH)、FIN フラグ / シークエンス番号 0 のパケットを使用して、ポートスキャンを行う攻撃です。 • TCP SYN-FIN - DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。SYN / FIN フラグを使用して、ポートスキャンを行う攻撃です。 • TCP SYN SrcPort Less 1024 - DoS 攻撃防止タイプに TCP SYN Source Port Less 1024 攻撃を指定します。送信元ポート 0-1023 と SYN フラグ含むパケットを使用して、ポートスキャンを行う攻撃です。 • Ping Death Attack - DoS 攻撃防止タイプに Ping Death Attack 攻撃を指定します。「Ping Death Attack」はコンピュータに対し変形した、または悪意のある Ping を送信するタイプの攻撃です。Ping は通常 64 バイト（多くのコンピュータは最大 IP パケットサイズを超えた Ping を処理できない）ですが、「Death Ping」は 65535 バイトです。このサイズの Ping の送信は攻撃対象のコンピュータをクラッシュさせます。歴史的にこのバグは比較的安易に使用されてきました。通常 65536 バイトの Ping パケット送信はネットワーキングプロトコルにおいて不法ですが、分割されたものであれば送信できてしまいます。（コンピュータによるパケット結合作業はしばしばオーバーフローを発生させ、システムをクラッシュさせます。） • All Types - DoS 攻撃防止タイプにすべての攻撃を指定します。
State	DoS 攻撃防止の状態を指定します。 • Enabled - DoS 攻撃防止の状態を有効にします。 • Disabled - DoS 攻撃防止の状態を無効にします。
Action	DoS 攻撃防止機能により行われる操作を指定します。 • Drop - 一致する DoS 攻撃パケットをすべて破棄します。Drop のみ設定可能です。

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

Zone Defense Settings（ゾーンディフェンス設定）

ゾーンディフェンスの設定を行います。

Security > Zone Defence Settings の順にクリックします。

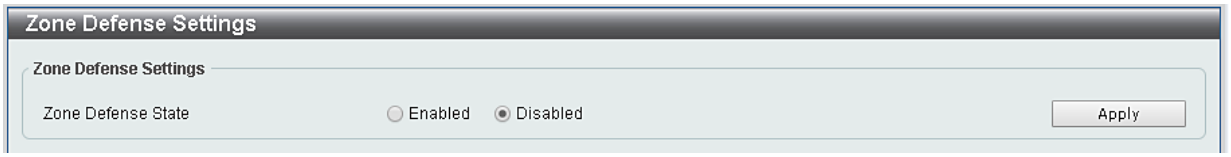


図 10-19　Zone Defense Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Zone Defense State	ゾーンディフェンスの有効 / 無効を設定します。

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

SSH（Secure Shell の設定）

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

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

1. **Management > User Account Settings** で管理者（admin）レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
2. 「SSH Global Settings」画面で、SSH を有効にします。

SSH Global Settings（SSH グローバル設定）

SSH をグローバルに設定します。

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

図 10-20　SSH Global Settings 画面

以下の項目を使用して、SSH サーバの設定を行います。

項目	説明
IP SSH Server State	IP SSH サーバを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
SSH Server Mode	SSH サーバのバージョンを表示します。

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

SSL（Secure Socket Layer）

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

1. 鍵交換（Key Exchange）
   暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。
2. 暗号化（Encryption）
   暗号スイートの次の段階は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
   - ストリーム暗号（Stream Ciphers）– スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとホスト間で一致させる必要があります。
   - CBC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義する 3 DES EDE 暗号化コードをサポートし、暗号化されたテキストと高度な暗号化規格（AES) を生成します。
3. ハッシュアルゴリズム（Hash Algorithm）
   暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）、SHA-256 の 3 つのハッシュアルゴリズムをサポートします。

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

「SSL Configuration Settings」画面では、ネットワークマネージャが SSL を有効にしてスイッチに暗号スイートを設定できます。暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

SSL 機能が有効になると、Web の使用はできなくなります。SSL 機能を使用しながら Web ベースの管理を行うためには、Web ブラウザが SSL 暗号化をサポートし、https:// で始まる URL を使用しなければなりません。（例 : https://10.90.90.90）これを守らないと、エラーが発生し、Web ベースの管理機能にアクセスできなくなります。

SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者の情報や認証のための鍵やデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバとクライアントが一致した証明書ファイルを持つ必要があります。現在のところ、ユーザ環境に応じて、ユーザはさらにダウンロードする必要がありますが、スイッチには事前にロードされた証明書が付属しています。

SSL Global Settings（SSL グローバル設定）

SSL グローバル設定を行います。

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

図 10-21　SSL Global Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
SSL Global Settings	
SSL State	SSL をグローバルに「Enabled」（有効）、「Disabled」（無効）に設定します。初期値は「Disabled」です。
Upgrade Certificate and Key	
Key	アップグレードする Key（鍵）を指定します。「Choose File」ボタンをクリックして、適切なファイルを選択しローカルコンピュータにロードします。
Certificate	アップグレードする Certificate を指定します。「Choose File」ボタンをクリックして、適切なファイルを選択しローカルコンピュータにロードします。

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

注意　筐体にインポートした SSL 用のサーバ証明書を削除する方法はありません。削除したい場合は、工場出荷時状態にリセットする必要がありますので、ご注意ください。

第 11 章　OAM（Operations、Administration、Maintenance：運用・管理・保守）

故障診断機能を設定します。

以下は、OAM のサブメニューです。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。
DDM（DDM 設定）	Digital Diagnostic Monitoring（DDM）機能の設定、表示を行います。

Cable Diagnostics（ケーブル診断機能）

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は主に管理者とカスタマサービス担当者が UTP ケーブルを検査、テストするために設計されています。ケーブルの品質やエラーの種類を即座に診断します。

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

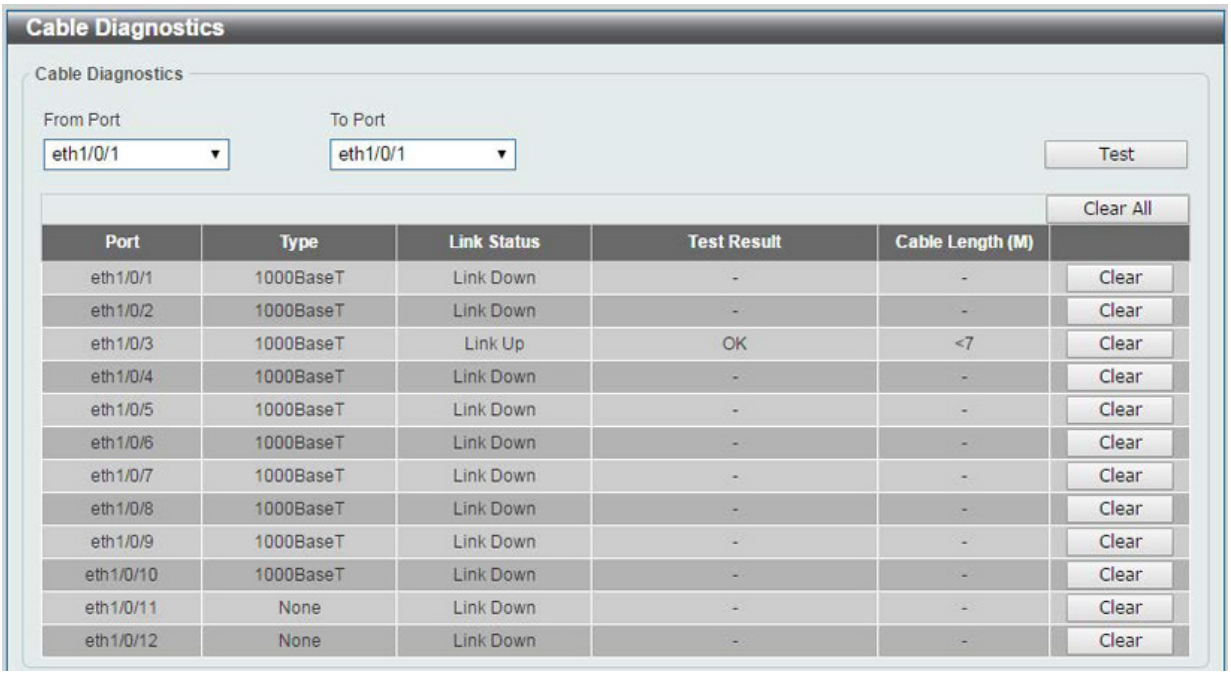


図 11-1　Cable Diagnostics 画面

特定のポートに対するケーブル診断を表示するためには、プルダウンメニューを使用して設定するポートを選択し、「Test」ボタンをクリックします。情報が画面に表示されます。
「Clear」ボタンをクリックし、指定ポートの情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

注意　10/100Mbps 通信ポートに対するケーブル診断実行中にリンクダウンが発生します。1GMbps 通信への影響はありません。

注意　10FastEther の PD を接続したポートにおいてケーブル診断を実行すると、Pair3、4 の結果が Unknown 表示となります。

ケーブル診断結果

項目	説明
OK	ケーブルの状態に問題はありません。
Short in Cable	UTP ケーブルのワイヤが接触している可能性があります。
Open in Cable	UTP ケーブルのワイヤが断線しているか、ケーブル接続が外れている可能性があります。
Crosstalk in Cable	UTP ケーブルのワイヤが対交差（クロスペア）の状態になっている可能性があります。
Unknow in Cable	ケーブル診断が開始されていないか、正しい結果を検出できません。

DDM（DDM 設定）

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

DDM Settings（DDM 設定）

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

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

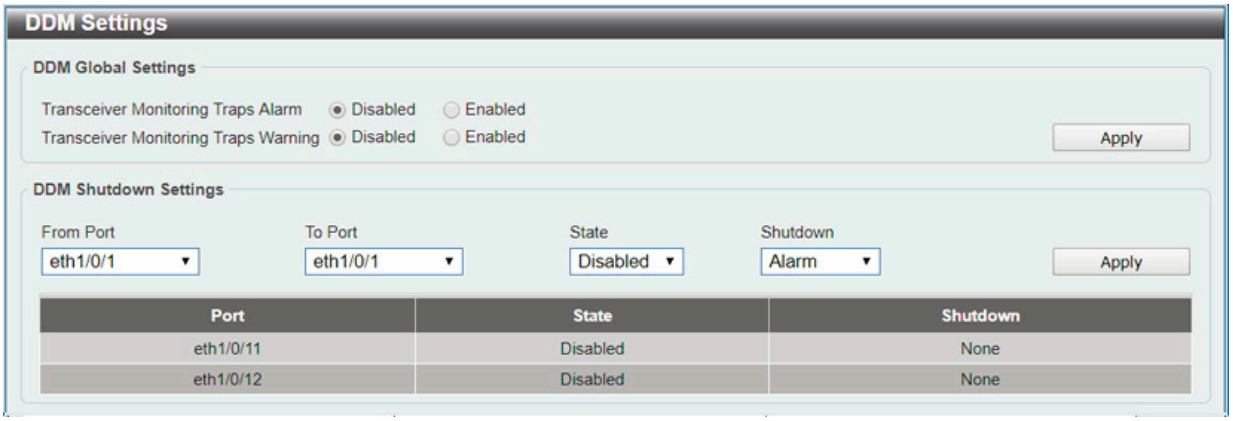


図 11-2　DDM Settings 画面

以下の項目を使用して設定します。

項目	説明
Transceiver Monitoring Traps Alarm	アラームしきい値を超過した際にトラップを送信するか否かを指定します。
Transceiver Monitoring Traps Warning	警告しきい値を超過した際にトラップを送信するか否かを指定します。
From Port / To Port	設定するポート範囲を指定します。
State	DDM の状態を有効または無効にします。
Shutdown	操作パラメータが「Alarm」または「Warning」のしきい値を超過した際に、ポートをシャットダウンするか否か指定します。「None」を選択するとしきい値の超過に関わらずシャットダウンは実行されません。初期値になります。

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

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

スイッチの特定ポートに DDM 温度しきい値設定を行います。

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

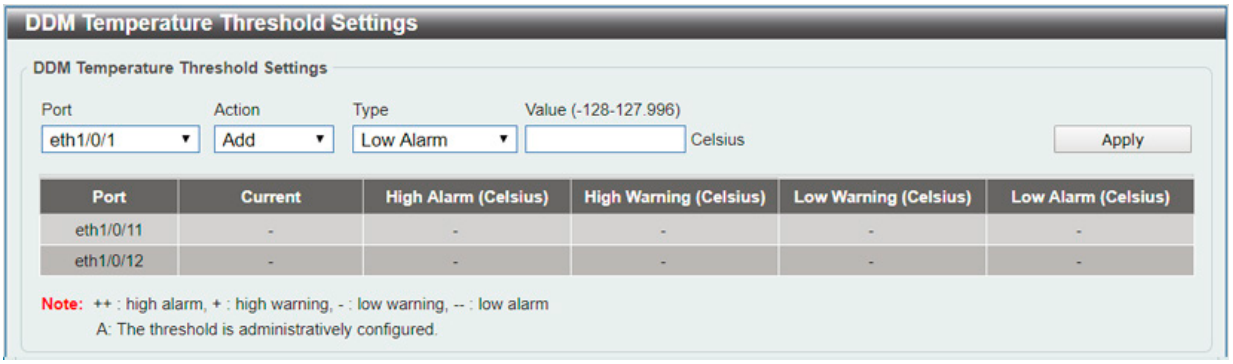


図 11-3　DDM Temperature Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	温度しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Value	温度しきい値の値について指定します。「-128」から「127.996」（℃）までの間で指定可能です。

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

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

スイッチの特定ポートに電圧しきい値を設定します。

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

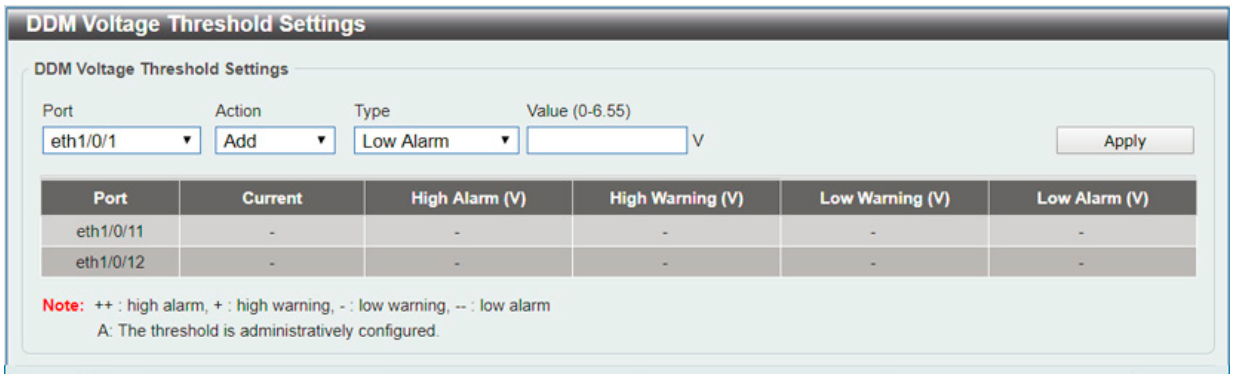


図 11-4　DDM Voltage Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	電圧しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Value	電圧しきい値の値について指定します。「0」から「6.55」（V）までの間で指定可能です。

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

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

スイッチの特定ポートにバイアス電流しきい値を設定します。

OAM > DDM > DDM Bias Current Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

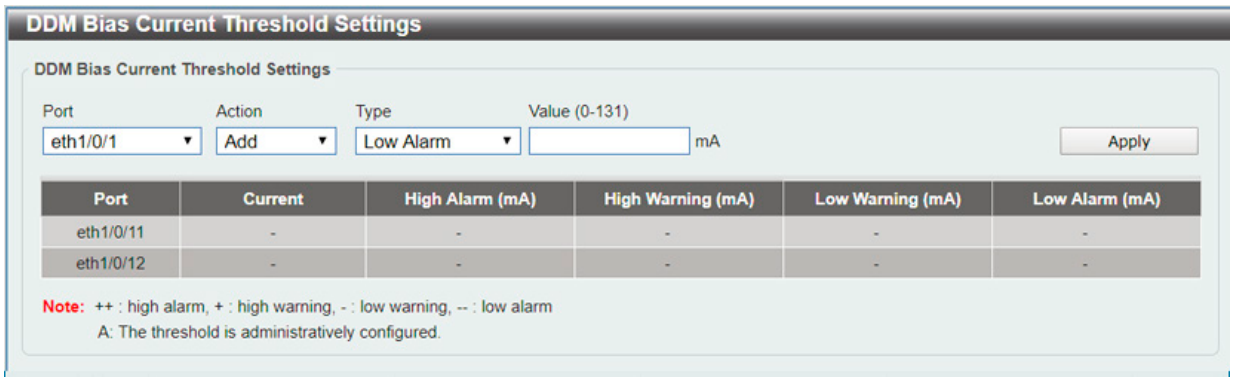


図 11-5　DDM Bias Current Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	電流しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Value	電流しきい値の値について指定します。「0」から「131」（mA）までの間で指定可能です。

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

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

スイッチの特定ポートに送信電力しきい値を設定します。

OAM > DDM > DDM TX Power Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

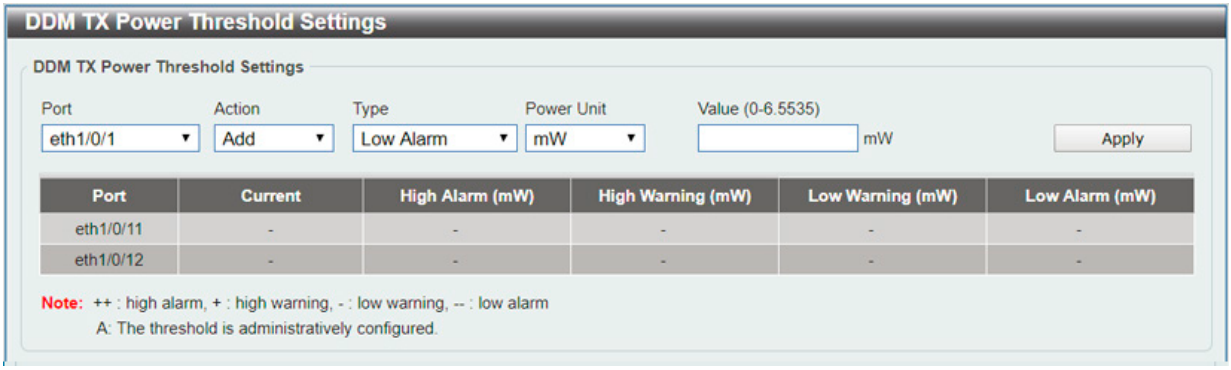


図 11-6　DDM TX Power Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	送信電力しきい値の種類について指定します。 「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Power Unit	送信電力単位について指定します。「mW」「dBm」から指定できます。
Value	送信電力しきい値の値について指定します。 「Power Unit」で「mW」を選択した場合、「0」から「6.5535」の間で指定します。「dBm」を選択した場合、「-40」から「8.1647」までの間で指定可能です。

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

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

スイッチの特定ポートに受信電力しきい値を設定します。

OAM > DDM > DDM RX Power Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

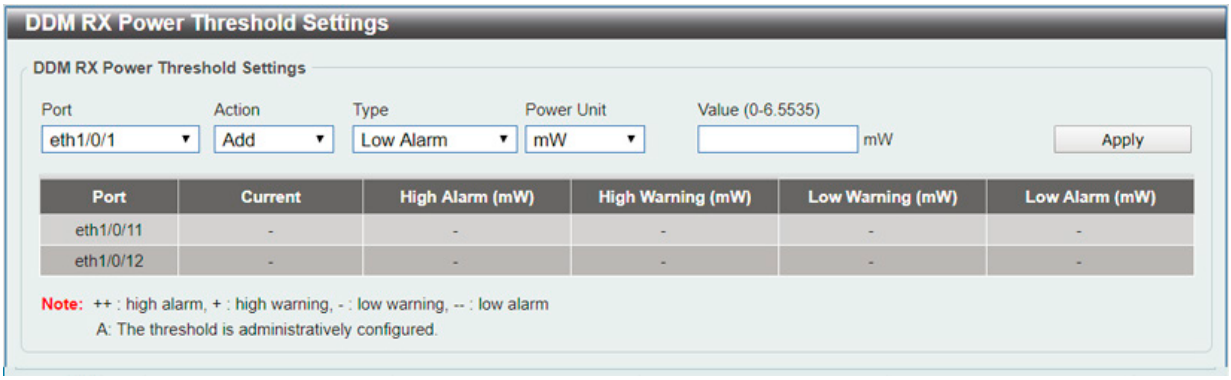


図 11-7　DDM RX Power Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	受信電力しきい値の種類について指定します。 「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Power Unit	受信電力単位について指定します。「mW」「dBm」から指定できます。
Value	受信電力しきい値の値について指定します。 「Power Unit」で「mW」を選択した場合、「0」から「6.5535」の間で指定します。「dBm」を選択した場合、「-40」から「8.1647」までの間で指定可能です。

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

DDM Status Table（DDM ステータステーブル）

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

OAM > DDM > DDM Status Table の順にメニューをクリックし、以下の画面を表示します。

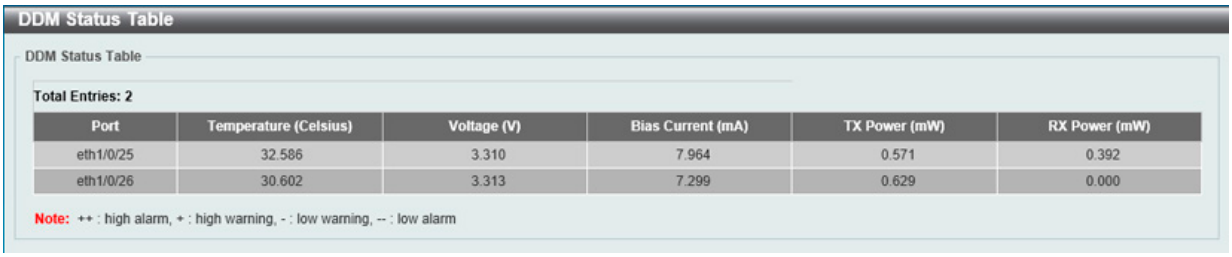


図 11-8　DDM Status Table 画面

以下の項目を表示します。

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

第 12 章　Monitoring（スイッチのモニタリング）

Monitoring メニューを使用し、本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報を提供することができます。

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

サブメニュー	説明
Statistics（統計情報）	パケット統計情報とエラー統計情報を表示します。
Mirror Settings（ミラー設定）	ポートミラーリングの設定を行います。

Statistics（統計情報）

Port Counters（ポートカウンタ）

ポートのカウンタ情報を表示します。

Monitoring > Statistics > Port Counters の順にメニューをクリックし、以下の画面を表示します。

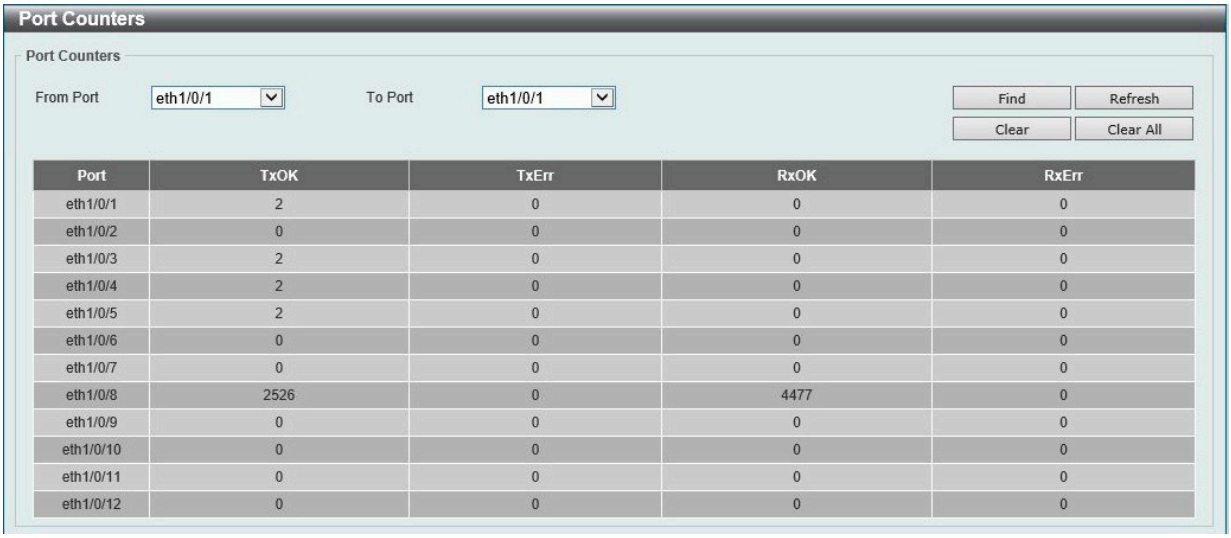


図 12-1　Port Counters 画面

以下の設定項目を使用して、設定および表示を行います。

項目	説明
From Port / To Port	表示するポート範囲を指定します。 • TxOK: パケットの送信に成功しました。 • RxOK: パケットの受信に成功しました。 • TxError: パケット送信にエラーが発生しました。 • RxError: パケット受信にエラーが発生しました。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。
「Clear」ボタンをクリックし、指定ポートの情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

Mirror Settings（ミラー設定）

ミラーリング機能についての設定、表示を行います。本スイッチは対象ポートで送受信するフレームをコピーして、そのコピーしたフレームの出力先を他のポートに変更する機能（ポートミラーリング）を持っています。ミラーリングポートに監視機器（スニファや RMON probe など）を接続し、最初のポートを通したパケットの詳細を確認することができます。トラブルシューティングやネットワーク監視の目的において適しています。

Monitoring > Mirror Settings をクリックします。

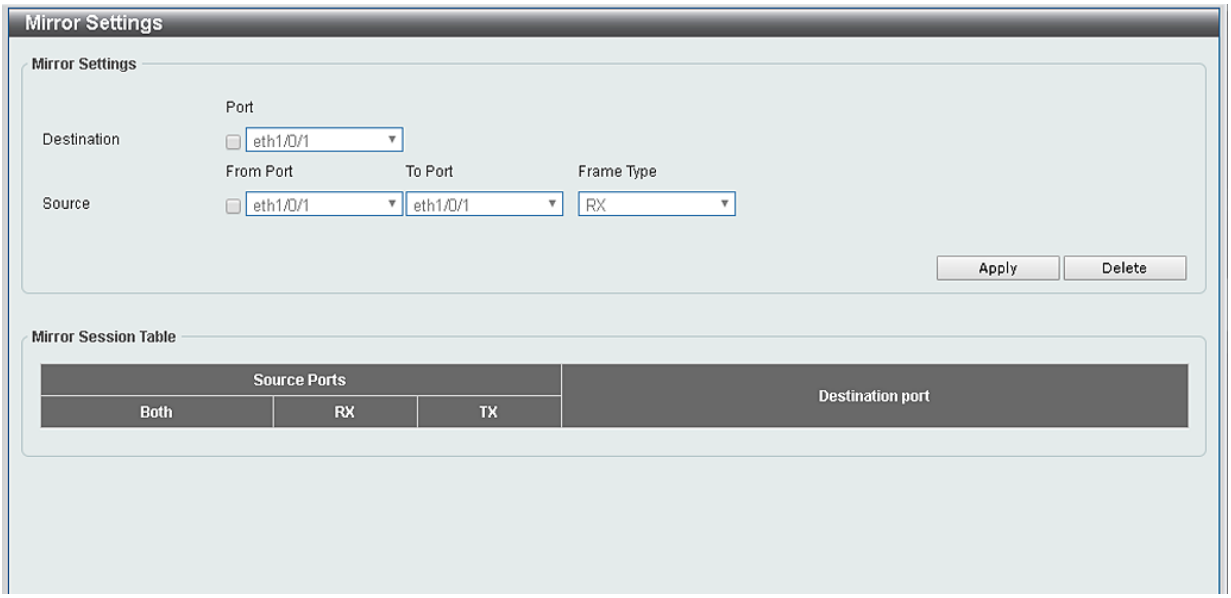


図 12-2　Mirror Settings 画面

以下の情報が表示されます。

項目	説明
Mirror Settings	
Destination	チェックを入れミラーエントリの宛先ポートについて指定します。
Source	チェックを入れミラーエントリの送信元について設定します。 送信元として「From Port」と「To Port」の番号を指定し、「Frame Type」オプションを指定します。「Frame Type」で指定可能なオプションは「Both」「RX」「TX」から指定可能です。「Both」を選択すると送信・受信どちらのトラフィックもミラーされます。「RX」の場合受信トラフィックのみミラーされ、「TX」は送信トラフィックのみミラーされます。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、入力した情報に基づいた既存のミラーエントリを削除します。

第 13 章　Green（省電力テクノロジー）

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

サブメニュー	説明
Power Saving（省電力）	機器の省電力設定を行います。
EEE（Energy Efficient Ethernet/ 省電力イーサネット）	Energy Efficient Ethernet/ 省電力イーサネットの設定を行います。

Power Saving（省電力）

スイッチの省電力機能を設定、表示します。

Green > Power Saving メニューをクリックし、以下の画面を表示します。

Power Saving Global Settings タブ

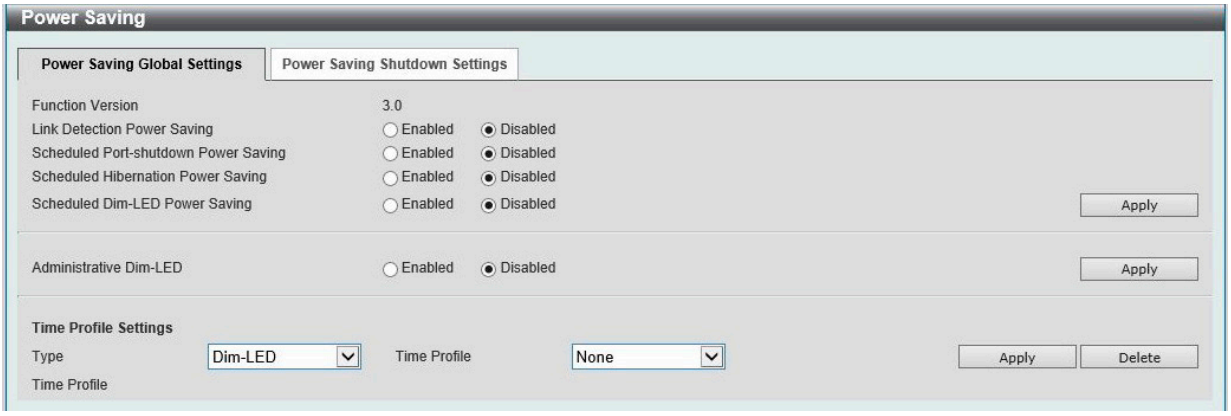


図 13-1　Power Saving - Power Saving Global Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Global Settings タブ	
Link Detection Power Saving	「リンク検出」を有効 / 無効に指定します。有効にするとリンクダウンしているポートへの電力供給は止められ、スイッチの消費電力を抑えます。これによりリンクアップしているポートへの影響はありません。
Scheduled Port-shutdown Power Saving	スケジュールによるポートシャットダウン機能の有効 / 無効を指定します。
Scheduled Hibernation Power Saving	スケジュールにより休止省電力機能を有効 / 無効に指定します。有効にすると、スイッチは設定期間休止状態（アイドル状態）になり電力消費を抑えます。
Scheduled Dim-LED Power Saving	スケジュールによりスイッチの LED 照明を消すことで、消費電力を抑えます。
Administrative Dim-LED	ポート LED 機能の有効 / 無効を指定します。
Type	省電力モードの種類を指定します。「Dim-LED」「Hibernation」から指定できます。
Time Profile	上記省電力機能に対応するスケジュールを指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。
「Delete」ボタンをクリックし指定のエントリを削除します。

Power Saving Shutdown Settings タブ

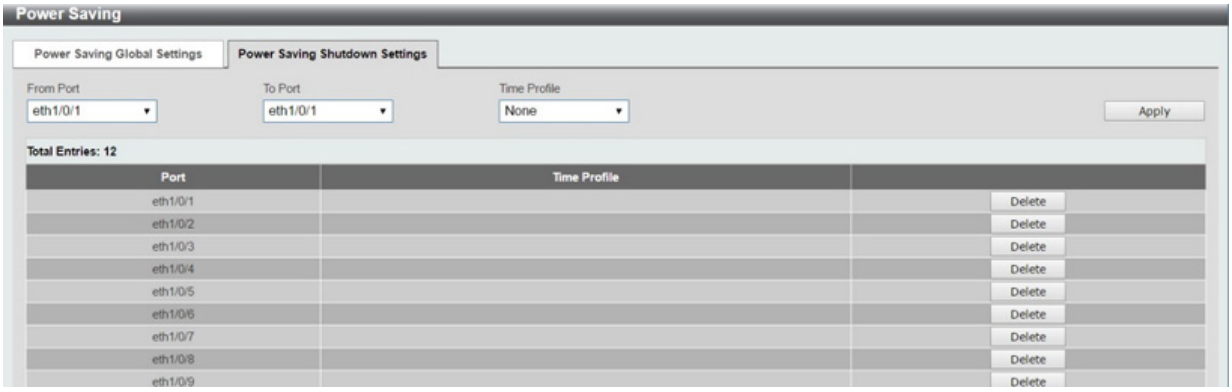


図 13-2　Power Saving - Power Saving Shutdown Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Shutdown Settings タブ	
From Port / To Port	設定するポート範囲を指定します。
Time Profile	ポートに対応するスケジュール名を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックし指定のエントリを削除します。

EEE（Energy Efficient Ethernet/ 省電力イーサネット）

「Energy Efficient Ethernet」(EEE/ 省電力イーサネット) は「IEEE 802.3az」によって定義されています。パケットの送受信がリンクに発生していない場合の電力消費を抑える目的で設計されています。

Green > EEE メニューをクリックし、以下の画面を表示します。

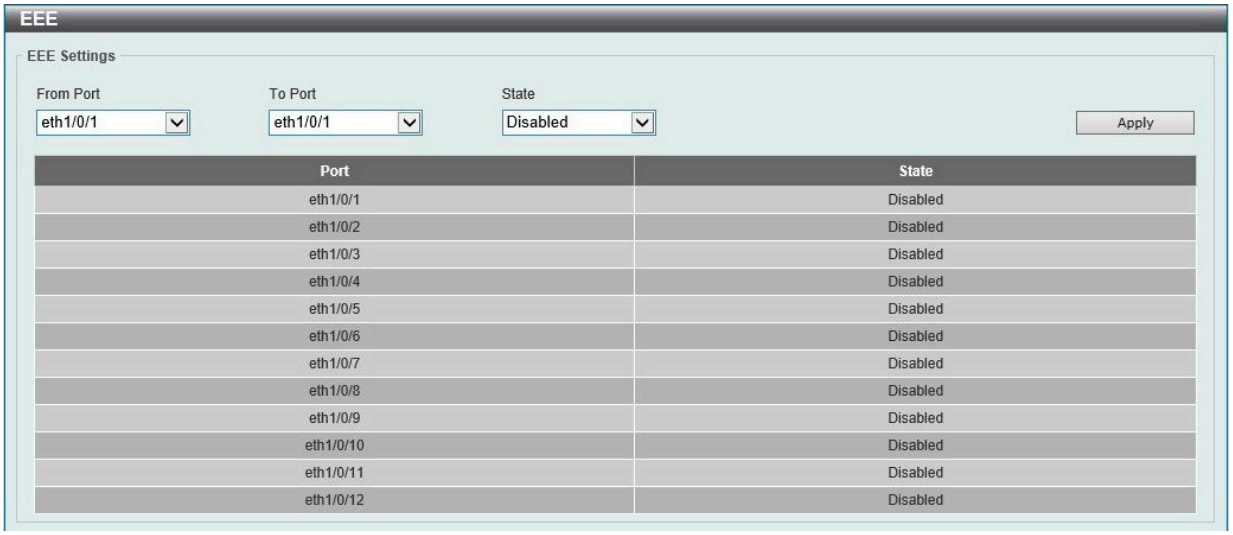


図 13-3　EEE 画面

以下の設定項目を使用して表示を変更します。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
State	本機能を有効 / 無効に指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。

第 14 章　Toolbar（ツールバー）

Web インタフェース画面上部のツールバーにある「Save」「Tools」「Wizard」「Online Help」「Surveillance Mode」「Logout」メニューを使用してスイッチの管理・設定を行います。

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

メニュー	サブメニュー	説明
Save（保存）	Save Configuration（コンフィグレーションの保存）	コンフィグレーションをスイッチに保存します。
Tools（ツール）	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、起動するイメージを指定します。
	Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）	ファームウエアのアップグレードとバックアップをします。
	Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）	コンフィグレーションのリストアとバックアップをします。
	Log Backup（ログファイルのバックアップ）	ログファイルのバックアップをします。
	Ping	Ping を実行します。
	Reset（リセット）	機器をリセットします。
	Reboot System（システム再起動）	システムの再起動を行います。
Wizard（ウィザード）	—	スマートウィザードを開始します。
Online Help（オンラインヘルプ）	D-Link Support Site（サポートサイト / 英語版）	D-Link サポートサイト（英語版）を表示します
	User Guide（ユーザガイド / 英語版）	ユーザガイド（英語版）を表示します。
Surveillance Mode（サーベイランスモード）	—	Web モードをサーベイランスモードに移行します。
Logout（ログアウト）	—	ログアウトします。

図 14-1　Toolbar

Save（保存）

Save Configuration（コンフィグレーションの保存）

「Save Configuration」では現在のコンフィグレーションを起動時のコンフィグレーションとして設定、またはスイッチに保存します。これにより、突然の電源の喪失によるコンフィグレーションの消失を防ぎます。

Save > Save Configuration をクリックし、以下の画面を表示します。

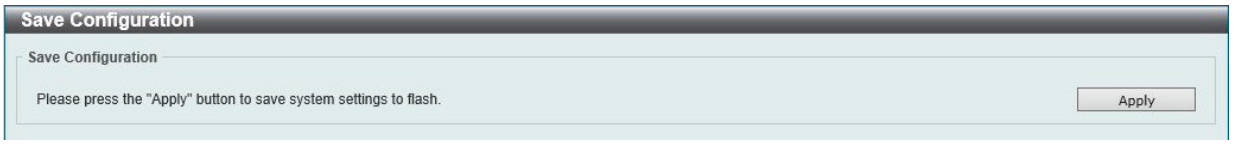


図 14-2　Save - Configuration 画面

「Apply」ボタンをクリックし、コンフィグレーションの保存を実行します。

注意　「Apply」をクリックし「The configuration has been saved.」と表示された後でも、30 秒程度経過するまでは電源を切らないでください。急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る場合があります。

Tools（ツール）

Firmware Information（ファームウェア情報）

起動ファームウェアイメージについての情報を表示、設定します。

Tools > Firmware Information をクリックし、以下の画面を表示します。

図 14-3　Firmware Information 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Boot Up	ファームウェアバージョンに対応する「Boot Up」ボタンをクリックすると、スイッチの次回起動時にそのファームウェアで起動します。

Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）

Firmware Upgrade from HTTP（HTTP を使用したファームウェアアップグレード）

HTTP を使用してローカル PC からファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP をクリックし、設定画面を表示します。

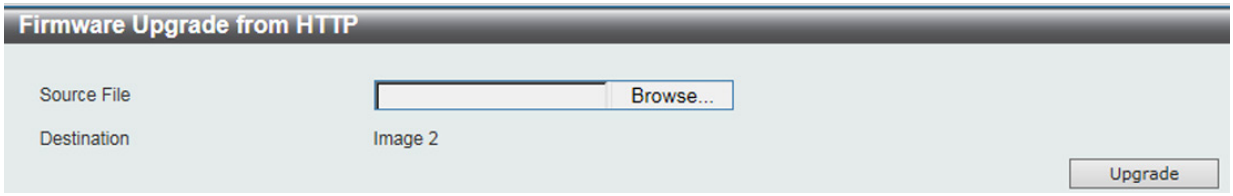


図 14-4　Firmware Upgrade from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source File	「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination	更新ファームウェアに自動的に割り振られれる宛先イメージ ID

「Upgrade」ボタンをクリックしてアップグレードを開始します。

Firmware Upgrade from TFTP（TFTP を使用したファームウェアアップグレード）

TFTP を使用してファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > firmware Upgrade from TFTP をクリックし、設定画面を表示します。

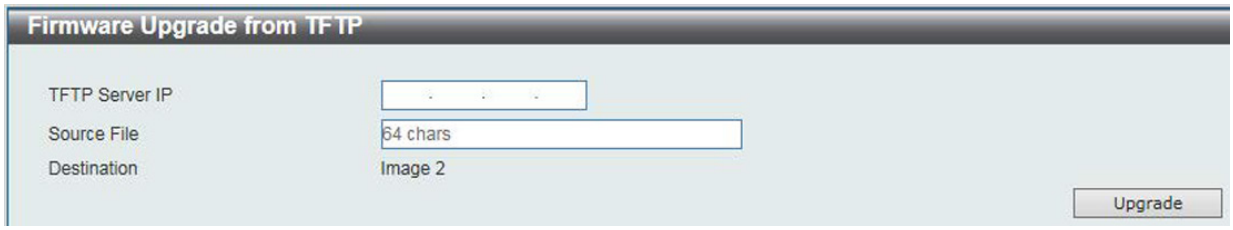


図 14-5　Firmware Upgrade from TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。
Source File	TFTP サーバにあるファームウェアファイル名を入力します。64 文字まで指定します。（例：DIS-200_Run_0_00_B000.had）
Destination	更新ファームウェアに自動的に割り振られれる宛先イメージ ID

「Upgrade」ボタンをクリックしてアップグレードを開始します。

Firmware Backup to HTTP（HTTP を使用したファームウェアバックアップ）

HTTP プロトコルを使用して、ローカル PC へのファームウェアのバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP をクリックし、設定画面を表示します。

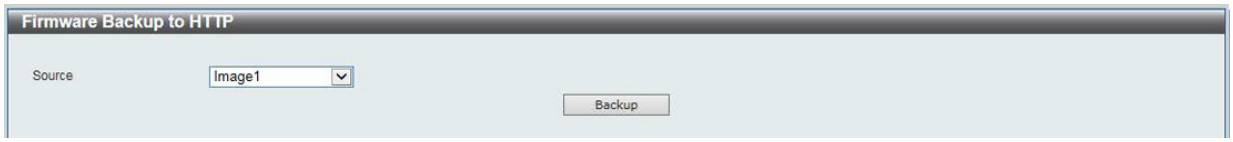


図 14-6　Firmware Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source	バックアップを行うファームウエアイメージを選択します。

「Backup」ボタンをクリックしてバックアップを開始します。

Firmware Backup to TFTP（TFTP を使用したファームウェアバックアップ）

TFTP サーバへのファームウェアバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP をクリックし、設定画面を表示します。

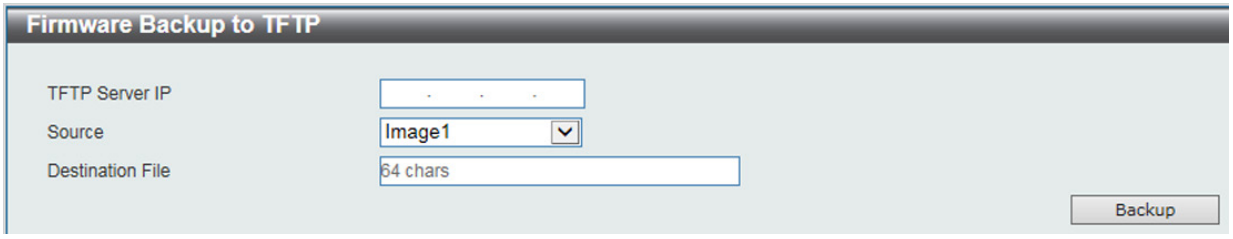


図 14-7　Firmware Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	ファームウェアファイルがバックアップされる TFTP サーバの IP アドレスを入力します。
Source	ファームウエアバックアップを行うイメージを選択します。
Destination File	TFTP サーバにバックアップされるファイル名を指定します。64 文字までで指定できます。 （例：DIS-200_Run_0_00_B000.had）

「Backup」ボタンをクリックしてバックアップを開始します。

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

Configuration Restore from HTTP（HTTP サーバからコンフィグレーションのリストア）

HTTP を使用してローカル PC からスイッチへコンフィグレーションをリストアします。

Tools > Configuration Restore & Backup > Configuration Restore from HTTP をクリックし、設定画面を表示します。

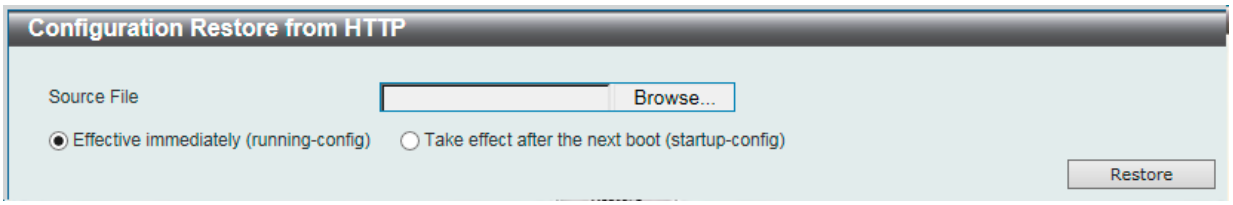


図 14-8　Configuration Restore from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source File	「Browse/ 参照」ボタンをクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定できます。 • 「Effective immediately（running-config）」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルが上書きされます。 • 「Take effect after the next boot（startup-config）」オプションを選択するとリストアと同時に起動時のコンフィグレーションファイルが上書きされます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

Configuration Restore from TFTP（TFTP サーバからコンフィグレーションのリストア）

TFTP サーバを使用してローカル PC からスイッチへコンフィグレーションをリストアします。

Tools > Configuration Restore & Backup > Configuration Restore from TFTP をクリックし、設定画面を表示します。

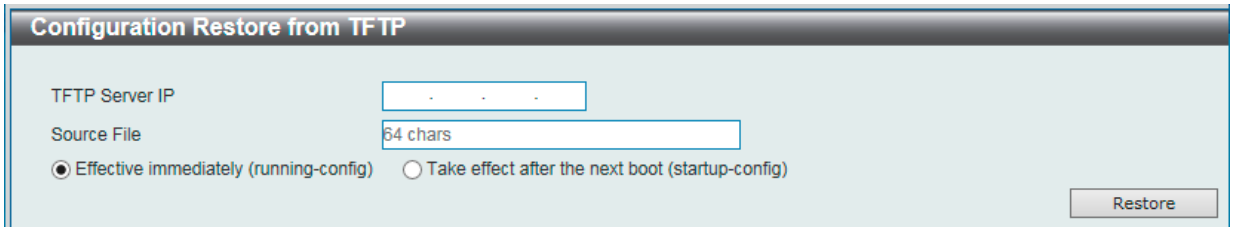


図 14-9　Configuration Restore from TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。
Source File	TFTP サーバにあるコンフィグレーションファイル名を入力します。64 文字までで指定します。 • 「Effective immediately（running-config）」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルが上書きされます。 • 「Take effect after the next boot（startup-config）」オプションを選択するとリストアと同時に起動時のコンフィグレーションファイルが上書きされます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

Configuration Backup to HTTP（HTTP を使用したコンフィグレーションバックアップ）

HTTP プロトコルを使用して、ローカル PC へコンフィグレーションファイルのバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to HTTP をクリックし、設定画面を表示します。

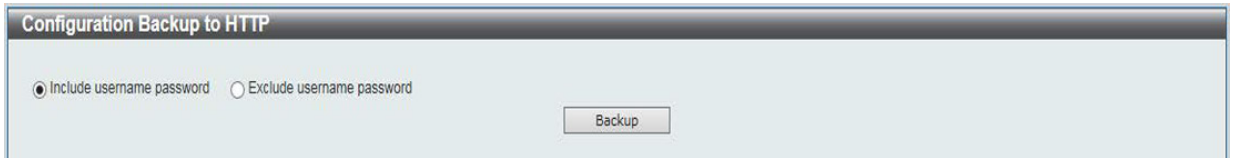


図 14-10　Configuration Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
「Include username password」を選択するとコンフィグレーションにユーザアカウントとパスワードも含めます。	
「Exclude username password」を選択するとコンフィグレーションにユーザアカウントとパスワードは含めません。	

「Backup」ボタンをクリックしてバックアップを開始します。

Configuration Backup to TFTP（TFTP を使用したコンフィグレーションバックアップ）

TFTP サーバにコンフィグレーションファイルのバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to TFTP をクリックし、設定画面を表示します。

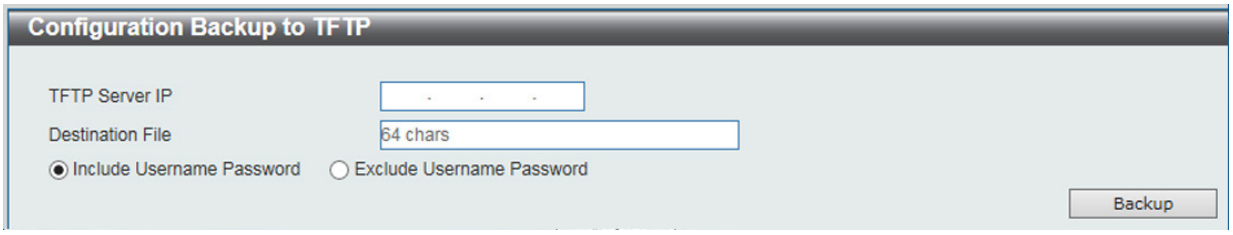


図 14-11　Configuration Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。
Destination File	TFTP サーバにストアされるコンフィグレーションファイル名を指定します。 • 「Include username password」を選択するとコンフィグレーションにユーザアカウントとパスワードを含めます。 • 「Exclude username password」を選択するとコンフィグレーションにユーザアカウントとパスワードは含めません。

「Backup」ボタンをクリックしてバックアップを開始します。

Log Backup（ログファイルのバックアップ）

Log Backup to HTTP（HTTP サーバを使用したログファイルのバックアップ）

HTTP プロトコルを使用して、ローカル PC へのシステムログのバックアップを行います。

Tools > Log Backup > Log Backup to HTTP をクリックし、設定画面を表示します。

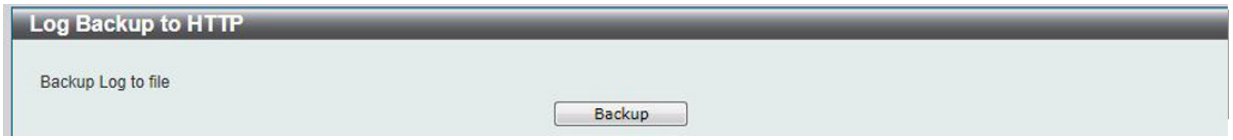


図 14-12　Log Backup to HTTP 画面

「Backup」ボタンをクリックしてバックアップを開始します。

Log Backup to TFTP（TFTP サーバを使用したログファイルのバックアップ）

TFTP サーバへのシステムログのバックアップを行います。

Tools > Log Backup > Log Backup to TFTP をクリックし、設定画面を表示します。

図 14-13　Log Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。
Destination File	TFTP サーバにストアされるログファイル名を指定します。64 文字までで指定できます。（例：log.txt）

「Backup」ボタンをクリックしてバックアップを開始します。

Ping

「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。宛先の機器はスイッチから送信された "echoes" に応答します。これはネットワーク上のスイッチと機器の接続状況を確認するうえで非常に有効です。

Tools > Ping をクリックし、設定画面を表示します。

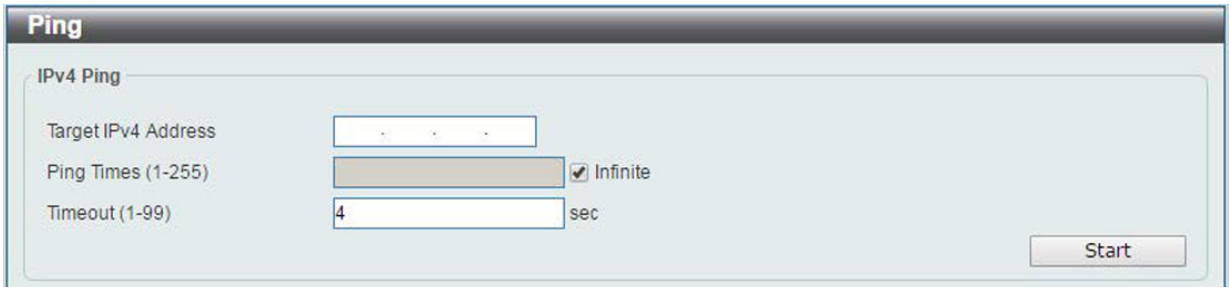


図 14-14　Ping 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
IPv4 Ping	
Target IPv4 Address	Ping する IPv4 アドレスを入力します。
Ping Times	繰り返し行う Ping の回数を入力します。1 から 255 の間で指定できます。「Infinite」にチェックを入れるとプログラムが停止されるまで「ICMP Echo」パケットを送信します。
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99（秒）までの間で指定できます。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。

「Start」ボタンをクリックして、各個別セクションでの Ping テストを実行します。

「IPv4 Ping」セクションで「Start」をクリックすると以下の「IPv4 Ping Result」画面が表示されます。

図 14-15　IPv4 Ping Result 画面

「New Ping」ボタンをクリックすると、Ping テストを停止して前の画面に戻ります。

Reset（リセット）

スイッチの設定内容を工場出荷時状態に戻します。

Tools > Reset をクリックし、次の設定画面を表示します。

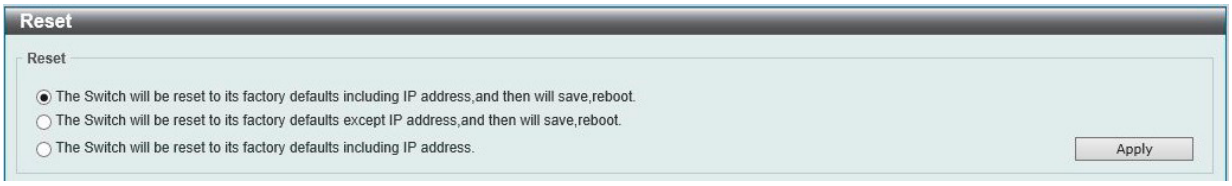


図 14-16　Reset System 画面

項目	説明
The Switch will be reset to its factory defaults including IP address, and then will save, reboot	IP アドレスを含むスイッチを工場出荷時設定にリセットして、保存、再起動を実行します。
The Switch will be reset to its factory default except IP address, and then will save, reboot	IP アドレスを除いてスイッチを工場出荷時の設定に戻し、保存、再起動を実行します。
The Switch will be reset to its factory defaults including IP address	IP アドレスを含むスイッチを工場出荷時設定にリセットしますが、再起動は行いません。

「Apply」ボタンをクリックして、リセット操作を開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。その際にコンフィグレーションの保存を行うことも可能です。

Tools > Reboot System をクリックし、以下の設定画面を表示します。

図 14-17　Reboot System 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Yes	スイッチは再起動する前に現在までに変更を行った設定が保存します。
No	スイッチは再起動する前に現在の設定を保存しません。変更した設定情報は破棄され、最後に保存した時の設定が使われます。
Reboot	スイッチは再起動します。

「Reboot」をクリックして再起動を開始します。

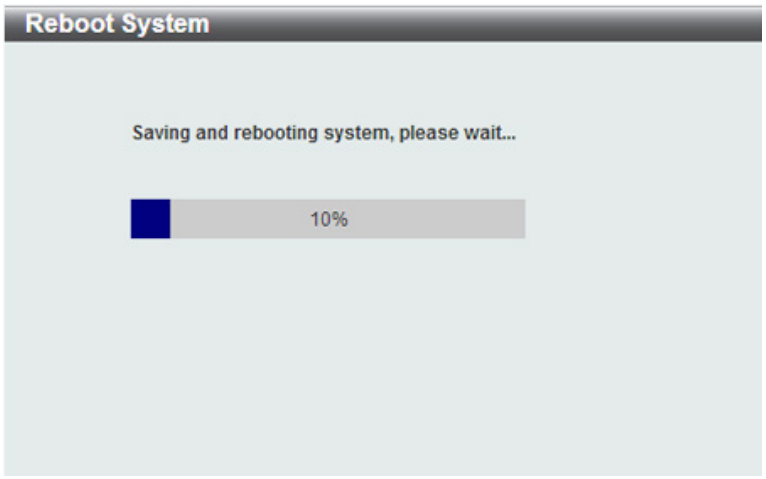


図 14-18　System Rebooting 画面

Wizard（ウィザード）

クリックするとスマートウィザードを開始します。詳しくは「Smart Wizard 設定」を参照ください。

Online Help（オンラインヘルプ）

D-Link Support Site（D-Link サポート Web サイト（英語））

クリックすると D-Link のサポート Web サイト（英語）へ接続します。インターネット接続が必要です。

User Guide（ユーザガイド（英語版））

ユーザガイド（英語版）を表示します。インターネット接続が必要です。

Surveillance Mode（サーベイランスモードへの変更）

クリックすると Web モードをスタンダードモードからサーベイランスモードに移行します。移行に失敗すると警告メッセージが表示されます。

注意 他のユーザセッションが同時にアクセスする場合、同じ Web UI モードの場合にのみアクセスが可能です。Web モードは実行中のユーザセッションが単一の場合において変更することができます。他のユーザセッションがある場合に、Web モードを変更することはできません。

「Surveillance Mode」をクリックすると次の画面が表示されます。複数の設定が自動的に変更される旨のメッセージです。

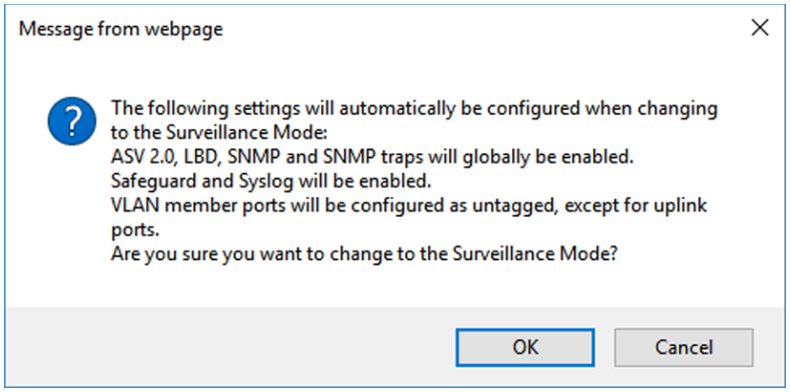


図 14-19　Surveillance Mode Confirmation Message 画面

「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。」という内容です。

サーベイランスモードへ変更する場合は「OK」をクリックします。「Cancel」をクリックするとスタンダードモードへ戻ります。

サーベイランスモードへの変更に成功すると、次のダイアログが表示されます。

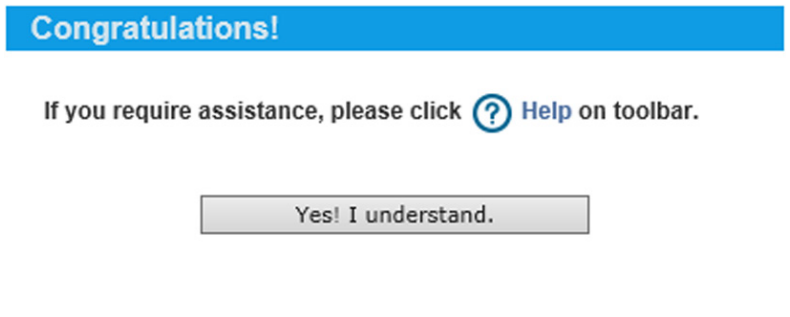


図 14-20　Surveillance Mode 'Congratulations' Message 画面

「Yes! I understand」をクリックしサーベイランスモードへ移行します。詳しくは「第 15 章　サーベイランスモード」を参照ください。

Logout（ログアウト）

クリックするとログアウトします。

第 15 章　サーベイランスモード

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。

Surveillance Overview（サーベイランスの概要）

サーベイランスモード画面が表示された場合、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。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。さらに「more」リンクをクリックするとポートに接続されているデバイスの詳細情報にアクセスします。

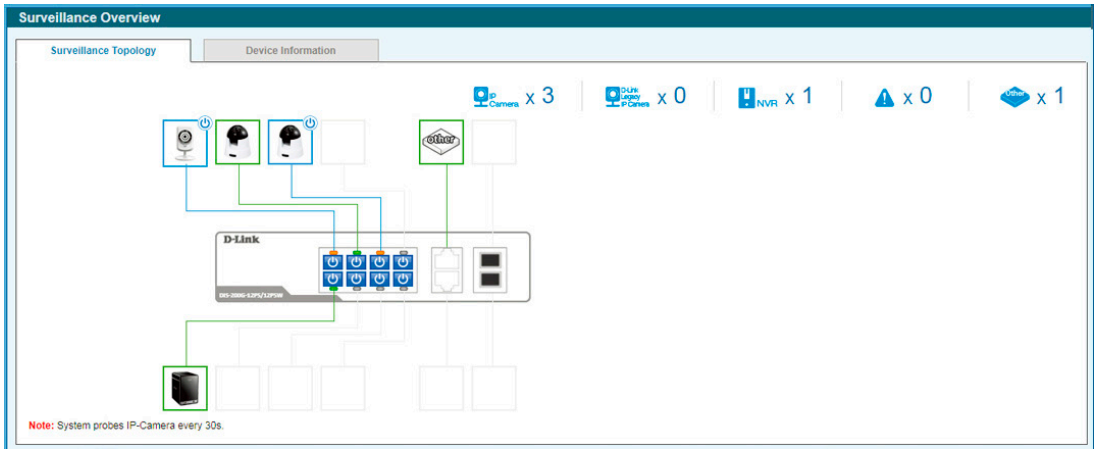


図 15-1　Surveillance Overview 画面

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 ONVIF 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。（ASV 1.0 により検出）
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。
Other	スイッチに接続している他の機器の数です。

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
	スイッチに接続している機器を表示します。緑枠で囲われている機器は PoE 受電機器ではありません。
	スイッチに接続している機器を表示します。青枠で囲われている機器は PoE 受電機器でスイッチから受電しています。「PD Alive」機能が使用可能です。

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。クリックすると無効になります。

アイコン	説明
	ポートの PoE が無効です。クリックすると有効になります。

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。  をクリックすると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。

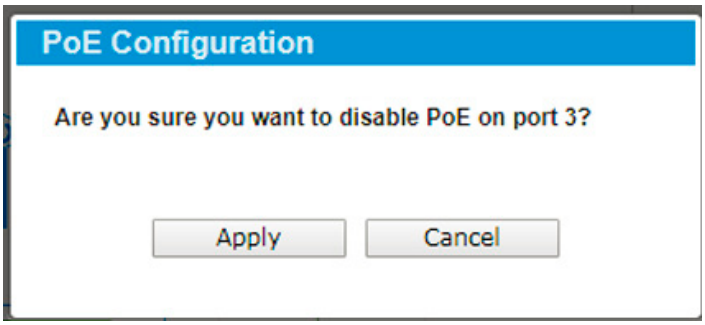


図 15-2　PoE 設定画面

「Apply」ボタンをクリックし、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。

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。

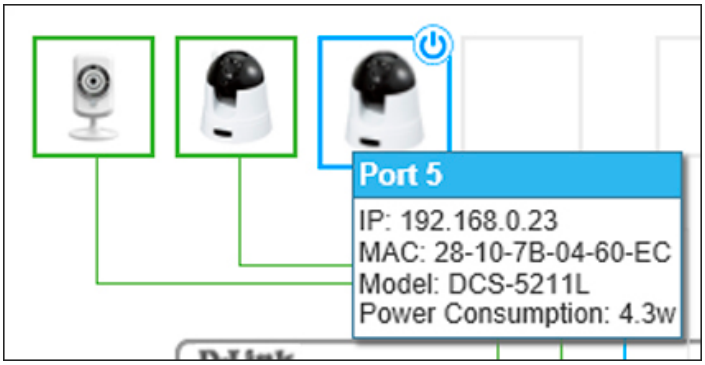


図 15-3　機器情報画面

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。

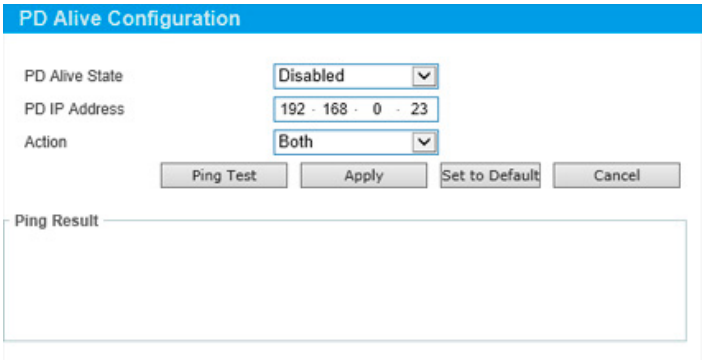


図 15-4　PD Alive Configuration 画面

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	「Reset」「Notify」「Both」から実行する動作を指定します。 • Reset - 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」ボタンをクリックし、設定を適用します。

「Set to Default」ボタンをクリックし、PD を初期設定に戻します。
「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」ボタンをクリックし、Ping を実行し PD の有効性を確認します。次の画面が表示されます。

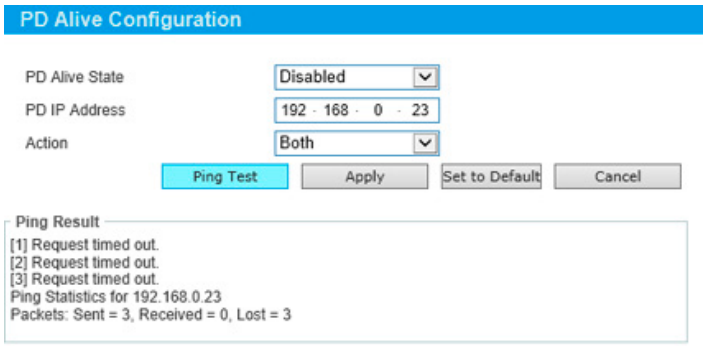


図 15-5　PD Alive Configuration (Ping Result) 画面

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、機器に関する情報が表示されます。

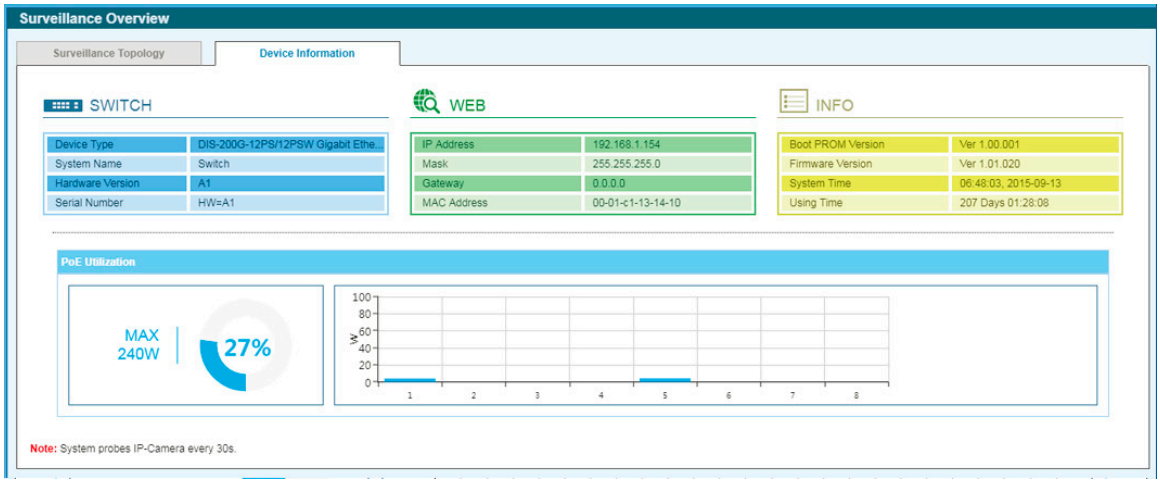


図 15-6　Device Information 画面

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	デバイスの現在時刻を表示します。
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（PoE モデルのみ）	

表示項目	説明
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。	

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。

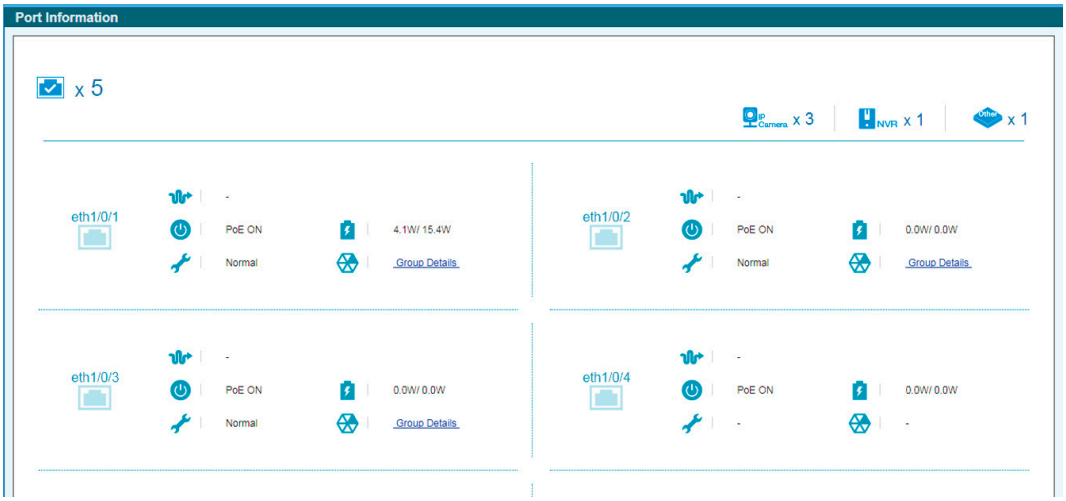


図 15-7　Port Information 画面

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	
	スイッチのイーサネットポートに接続したデバイス数です。
IP Camera	検出された ONVIF IP カメラ数です。
NVR	検出された NVR 数です。
Other	スイッチに接続している他の機器の数です。
各ポート情報	
	ポート番号です。
	接続しているケーブルのケーブル長です。
	ポートの PoE ステータス（PoE の有効 / 無効）です。
	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。
Normal Loop	ポートのループバック検出状況について表示します。 • Normal - ネットワークでのループは発生していません。 • Loop - ループが発生しています。ループが検出されると、「Normal」は「Loop」表記となり「Health Diagnostics」ページへのリンクになります。
Group Details	ONVIF 対応機器（IP カメラ /NVR）が対象ポートに検出された場合、アイコンは「Group Details」（グループ詳細）へのリンクアイコンへと変化します。

アイコン	説明
Video Management Server	ONVIF 非対応機器が検出された場合、ドロップダウンが表示され、下記から機器の種類を選択することが可能です。「Video Management Server（ビデオマネジメントサーバ）」、「VMS Client/Remote Viewer（VMS クライアント / リモートビューワ）」、「Video Encoder（ビデオエンコーダ）」、「Network Storage（ネットワークストレージ）」、「Other IP Surveillance Device（その他サーベイランス機器）」

Group Details（グループ詳細）をクリックすると次の画面が表示されます。

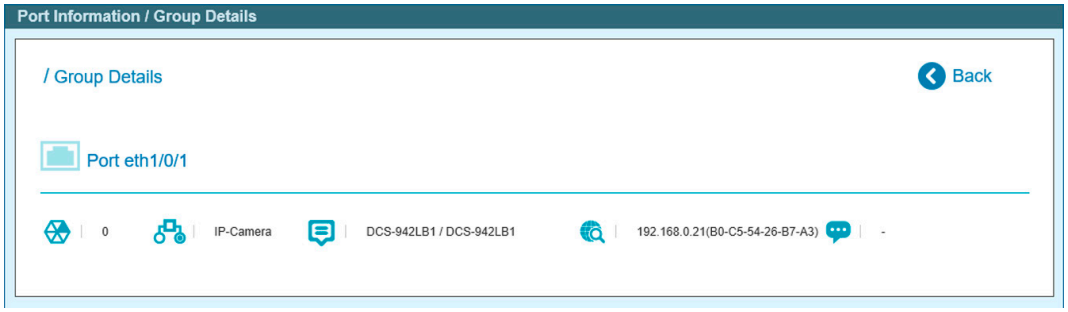


図 15-8　Port Information / Group Details 画面

以下のアイコン、項目が表示されます。

アイコン	説明
Port eth1/0/1	スイッチのポート番号です。
	スイッチのイーサネットポートに接続した IP カメラまたは NVR のグループ ID です。
	スイッチのイーサネットポートに接続した IP カメラまたは NVR の種類です。
	スイッチのイーサネットポートに接続した IP カメラの型番です。
	スイッチのイーサネットポートに接続した IP カメラまたは NVR の IP アドレスと MAC アドレスです。
	スイッチのイーサネットポートに接続したデバイスの概要です。

「Back」をクリックすると前の画面に戻ります。

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、帯域、IP アドレス、その他の情報（ポートの説明など）、電力消費量が表示されます。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。

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

図 15-9　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	
IP Camera	スイッチのイーサネットポートに接続した検出された ONVIF IP カメラ数です。
	スイッチのイーサネットポートに接続した ONVIF IP カメラの PoE 電力消費量と PD クラスを表示します。
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 カメラの場合、対象機器の画像が表示されます。
	ポートの PoE 電力消費量と IP カメラの PD クラスを表示します。
	IP カメラの IP/MAC 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。

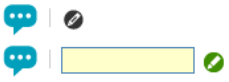
NVR Information（NVR 情報）

スイッチに接続された NVR の情報を表示します。

機能一覧から「NVR Information」をクリックします。

図 15-10　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	
	スイッチのイーサネットポートに接続した NVR 数です。
各機器情報	
	ポート番号です。
	NVR 機器のアイコンまたは画像が表示されます。
	NVR の IP/MAC アドレスです。
	NVR 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 のグループ ID です。
	NVR に管理されている ONVIF 対応の IP カメラの数です。
	NVR により管理されている ONVIF IP カメラについての情報が表示されます。

PoE Information（PoE 情報）（PoE モデルのみ）

各ポートの Power-over-Ethernet（PoE）使用情報を表示します。

機能一覧から「PoE Information」をクリックします。

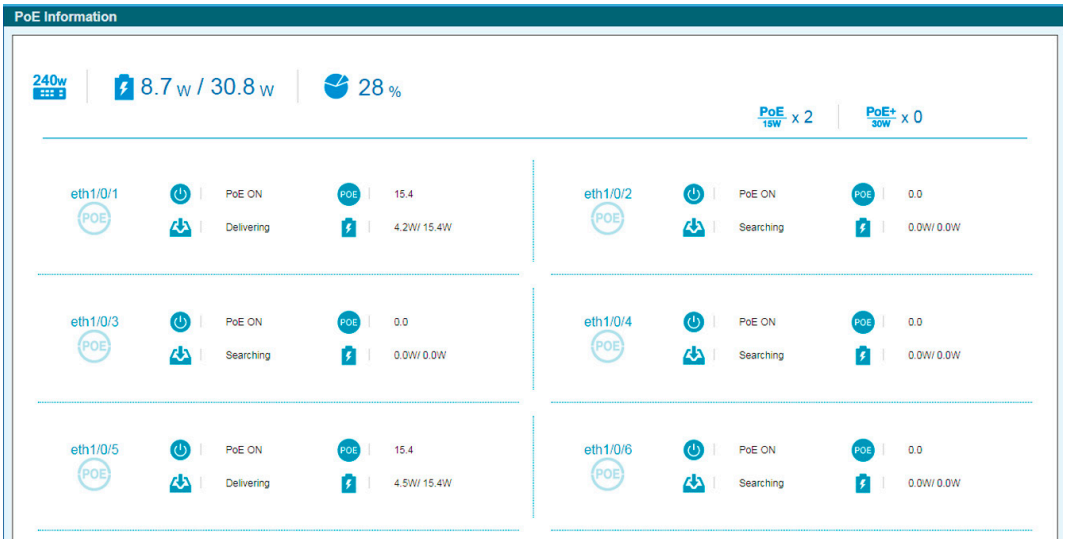


図 15-11　PoE Information 画面

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	
193w	PoE の給電可能電力です。
	PoE 電力消費量と PoE クラスを表示します。
	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 PoE 受電機器数です。
PoE+ 30W	30w の PoE 給電を受ける PoE 受電機器数です。
各機器情報	
POE	ポート番号です。
	ポートの PoE ステータス（PoE ON / OFF）です。
POE	ポートの最大 PoE 供給可能電力です。
Delivering Power Denied	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。「Searching」は検出中、「Power Denied」は給電不可（エラー発生）を意味します。「Power Denied」と表示された場合、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）（PoE モデルのみ）

PoE ポートに電力が供給される時間（PoE スケジューリング）を設定します。

機能一覧から「PoE Scheduling」をクリックします。

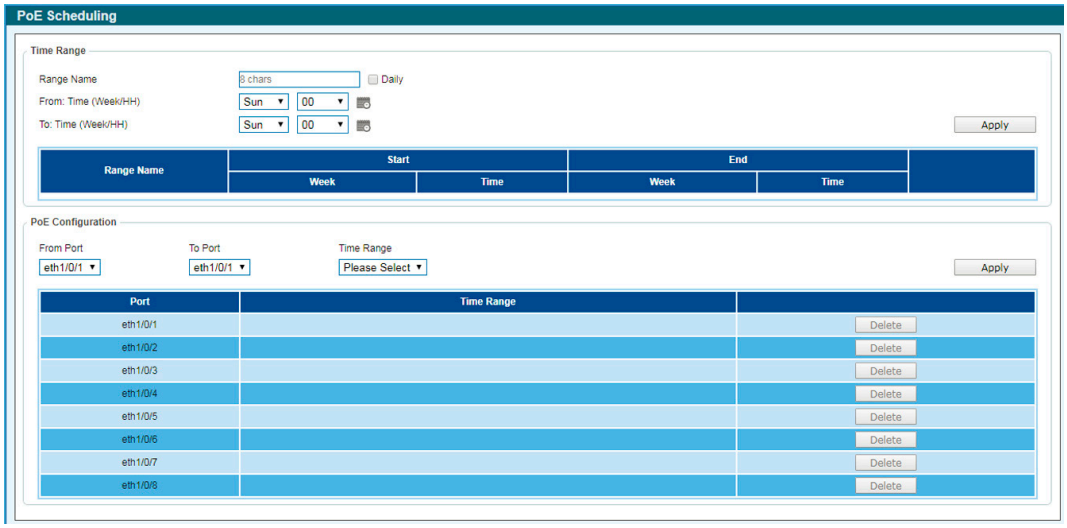


図 15-12　PoE Schedule 画面

新しいタイムレンジの作成：

1. 「Time Range」セクションで、設定したい内容に応じて以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Range Name	タイムレンジ名を設定します。
From/To: Time (Week/HH)	開始する曜日と時間、終了の曜日と時間を指定します。 「」をクリックするとカレンダー（下図）が表示され、視覚的に日時を指定することができます。  選択後「OK」をクリックします。
Daily	チェックボックスにチェックを入れると曜日設定が「毎日」に指定されます。

2. 「Apply」をクリックしてタイムレンジを作成します。

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、設定したい内容に応じて以下から操作を選択します。

■ 画面に表示される項目

項目	説明
From Port / To Port	設定対象のポート範囲を指定します。
Time Range	ポートに適用するタイムスケジュールを指定します。

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）

Clock Settings（時刻設定）

スイッチの時刻を設定します。

注意 本シリーズは RTC を持っていないため、再起動すると設定した時間は消去されます。

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

図 15-13　Clock Settings 画面

2. 設定したい内容に応じて以下から操作を選択します。

■ 画面に表示される項目

項目	説明
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」>「SNTP Settings」の順にメニューをクリックします。

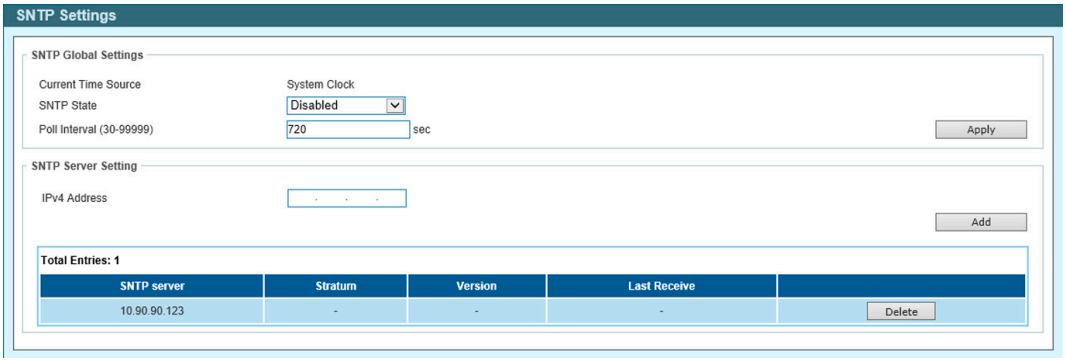


図 15-14　SNTP Settings 画面

2. 「SNTP Global Settings」セクションで、設定したい内容に応じて以下から操作を選択します。

■ 画面に表示される項目

項目	説明
SNTP State	SNTP 機能を「Enabled」（有効）または「Disabled」（無効）にします。
Poll Interval (30-99999)	ポーリング間隔を指定します。 初期値：720（秒） 選択可能範囲：30-99999（秒）

3. 「Apply」をクリックして設定を有効にします。

4.

SNTP サーバを設定する場合：

1. 「SNTP Server Settings」セクションで、設定したい内容に応じて以下から操作を選択します。

■ 画面に表示される項目

項目	説明
IPv4 Address	SNTP サーバの IPv4 アドレスを設定します。

2. 「 Add」をクリックして SNTP サーバを追加します。「Delete」をクリックすると SNTP サーバを削除します。

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。サーベイランス VLAN は 1 つのみです。本サーベイランス VLAN は、ONVIF プロトコルを使用して、IP カメラや NVR のようなサーベイランスデバイスを認識させることもサポートしています。

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

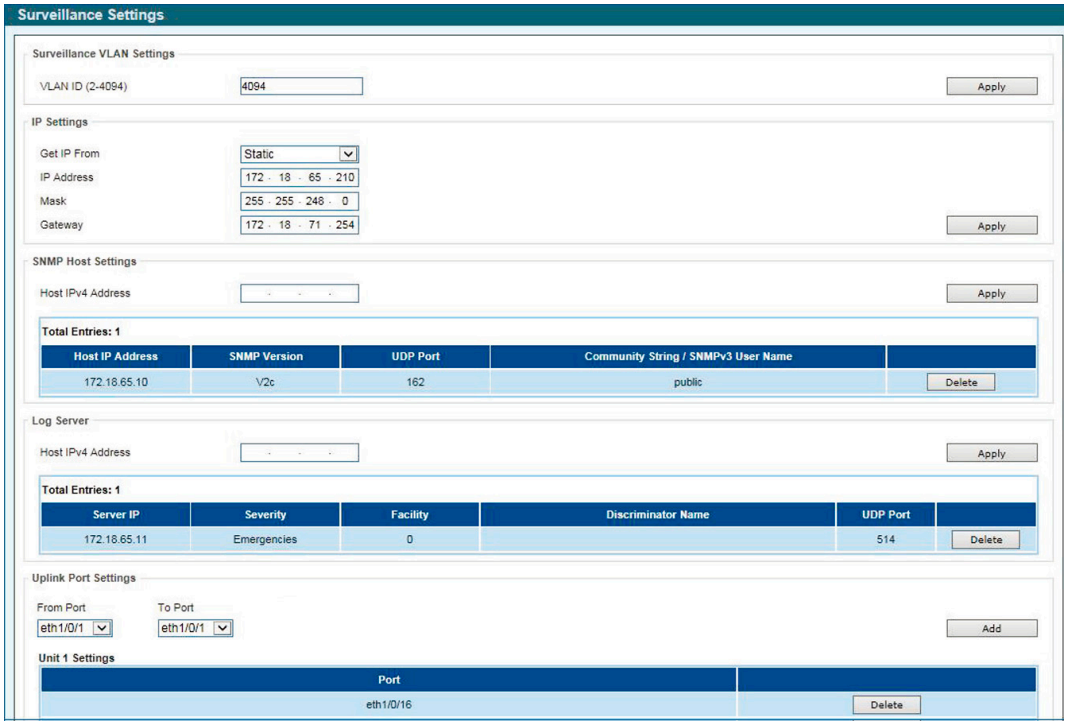


図 15-15　Surveillance Settings 画面

以下の項目が表示されます。

項目	説明
Surveillance VLAN Settings	
VLAN ID (2-4094)	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：「Statc」「DHCP」 「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	
Host IPv4 Address	SNMP ホストの IPv4 アドレスを指定します。
Log Server	
Host IPv4 Address	Syslog メッセージを受信する Syslog サーバの IPv4 アドレスを指定します。
Uplink Port Settings	

項目	説明
From Port / To Port	「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。設定を削除するには「Delete」をクリックします。

注意 他のスイッチへのサーベイランストラフィックの転送のために、アップリンクポートは全サーベイランス VLAN に所属します。これらのポートでは検出プロセスが無効になっているため、アップリンクポートを他のスイッチに接続することを推奨します。

注意 サーベイランスモードで接続中の IP カメラにアクセスしようとすると、Web GUI でのアクセスが切断される場合があります。その場合、コマンドを使用して「管理 PC が繋がっているポート」のサーベイランス VLAN を無効にするか、MAC アドレスのキャッシュを削除してから再度接続をしてください。

Surveillance Log（サーベイランスログ）

スイッチで生成されたサーベイランスログの一覧を表示します。

1. 機能一覧から「Surveillance Log」をクリックします。

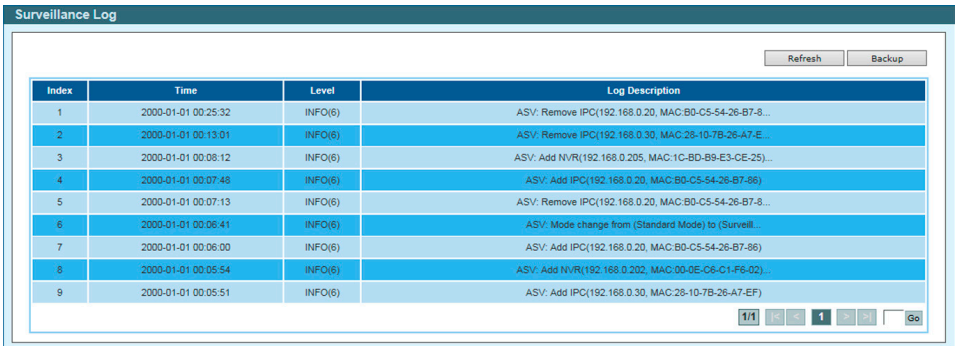


図 15-16　SNTP Settings 画面

2. **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、サーベイランスログを HTTP を使用して、PC へアップロードします。

Health Diagnostic（正常性診断）

ヘルス診断情報、検出された監視デバイス情報、およびスイッチ上のすべてのポートまたは選択されたポートのケーブル距離テストの開始に使用されます。 リンクアップポートごとに、システムはリンクステータス、PoE ステータス、およびエラーカウンタを定期的にチェックします。 このページは 30 秒ごとに更新されます。

機能一覧から「Health Diagnostic」をクリックします。

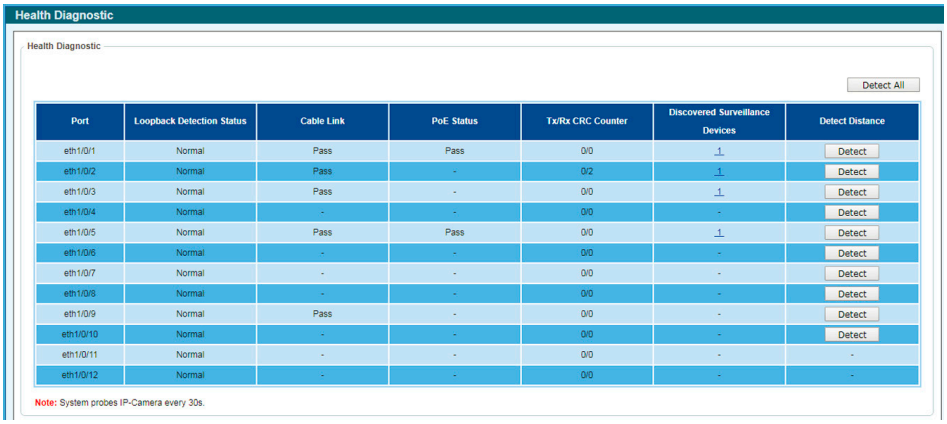


図 15-17　Health Diagnostic 画面

以下の項目が表示されます。

項目	説明
Port	表示のポート番号です。

項目	説明
Loopback Detection Status	ポートのループバック検出状況です。 • Normal - ループは検出されていません。 • Loop - ループが検出されています。
Cable Link	ケーブルリンクの状態です。 • PASS - 全二重モードでリンクアップしています。 • 10M Half - 10M/ 半二重モードでリンクアップしています。 • 100M Harf - 100M/ 半二重モードでリンクアップしています。
PoE Status	PoE 状況について下記の中から表示します。 「PASS」「PD Short」「Overload」「Power Denied」「Thermal Shutdown」「Classification Failure」
Tx/Rx CRC Counter	TX/RX CRC カウンタについて表示されます。
Discovered Surveillance Devices	検出された ONVIF IP カメラ /NVR の数を表示します。ハイパーリンク（1）をクリックするとポートに接続した IP カメラ /NVR のグループ詳細（Group Details）について表示します。
Detect Distance	「Detect」指定ポートのケーブル長テストを開始します。

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。

Toolbar（ツールバー）（サーベイランスモード）

Web インタフェース画面上部のツールバーにあるメニューを使用してスイッチの管理・設定を行います。

Wizard（ウィザード）

クリックするとスマートウィザードを開始します。詳しくは Smart Wizard 設定を参照ください。

Tools（ツール）

Firmware Information（ファームウェア情報）

起動するファームウェアの設定を行います。

Tools > Firmware Information をクリックし、設定画面を表示します。

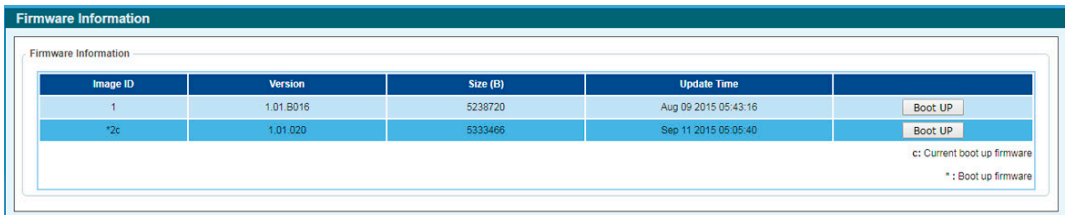


図 15-18　Firmware Information 画面

起動するイメージを「image1/2」から選択し「Boot UP」をクリックします。

Firmware Upgrade & Backup（ファームウェアのアップグレードと保存）

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。

Firmware Upgrade from HTTP（HTTP を使用したファームウェアアップグレード）

HTTP を使用してローカル PC からファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP をクリックし、設定画面を表示します。

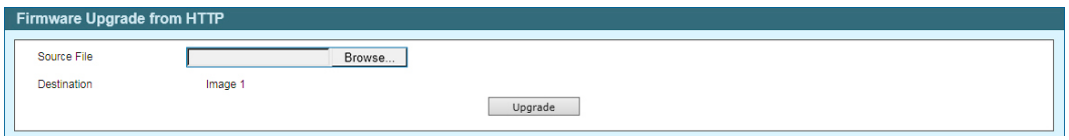


図 15-19　Firmware Upgrade from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source File	64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定します。
Destination	宛先（アップグレード先）イメージが表示されます。

「Upgrade」ボタンをクリックして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。

Firmware Backup to HTTP（HTTP を使用したファームウェアバックアップ）

HTTP プロトコルを使用して、ローカル PC へのファームウェアのバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP をクリックし、設定画面を表示します。

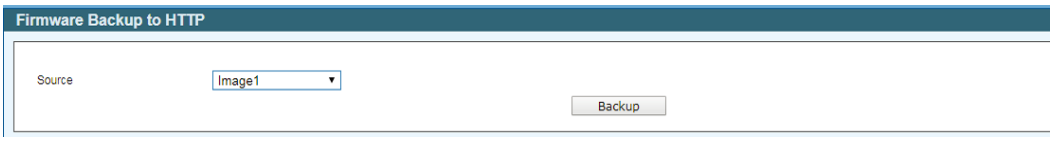


図 15-20　Firmware Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source	Source（バックアップするイメージ）を指定します。イメージについては「Tools > Firmware Information」にて確認できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

Configuration Restore from HTTP（HTTP サーバからコンフィグレーションのリストア）

HTTP サーバを使用してローカル PC からスイッチへコンフィグレーションをリストアします。

Tools > Configuration Restore & Backup > Configuration Restore from HTTP をクリックし、設定画面を表示します。

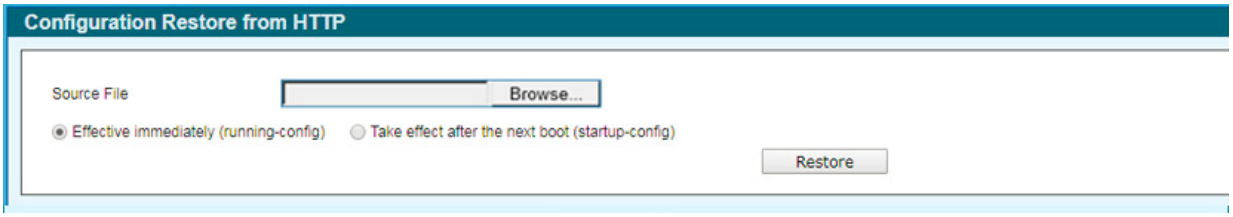


図 15-21　Configuration Restore from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source File	「Browse/ 参照」ボタンをクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定します。
Effective immediately (running-config)	選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。
Take effect after the next boot (startup-config)	選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

Configuration Backup to HTTP（HTTP を使用したコンフィグレーションバックアップ）

HTTP プロトコルを使用して、ローカル PC へコンフィグレーションバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to HTTP をクリックし、設定画面を表示します。

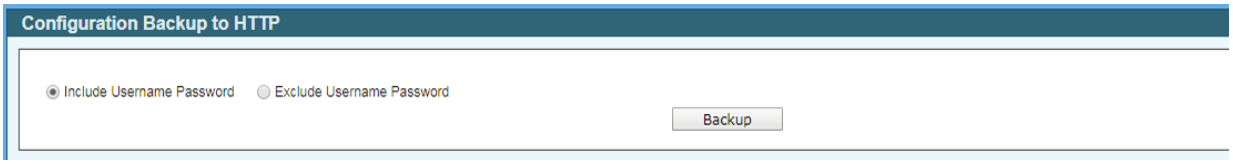


図 15-22　Configuration Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Include Username Password	選択するとバックアップするコンフィグレーションファイルにユーザ名とパスワードを含みます。
Exclude Username Password	選択するとバックアップするコンフィグレーションファイルにユーザ名とパスワードを含みません。

「Backup」ボタンをクリックしてバックアップを開始します。

Reset（リセット）

スイッチの設定内容を工場出荷時状態に戻します。

Tools > Reset をクリックし、次の設定画面を表示します。

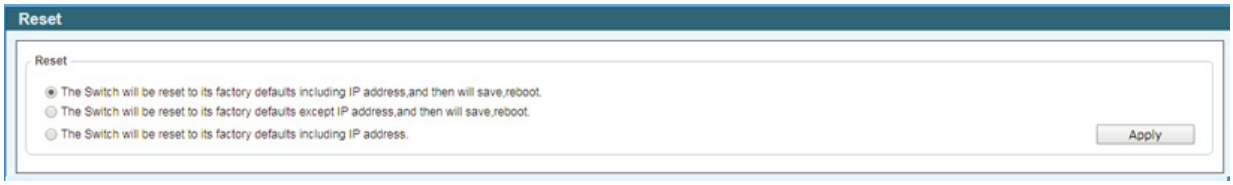


図 15-23　Reset System 画面

項目	説明
The Switch will be reset to its factory defaults including IP address, and then will save, reboot	IP アドレスを含むスイッチを工場出荷時設定にリセットして、保存、再起動を実行します。
The Switch will be reset to its factory default except IP address, and then will save, reboot	IP アドレスを除いてスイッチを工場出荷時の設定に戻し、保存、再起動を実行します。
The Switch will be reset to its factory defaults including IP address	IP アドレスを含むスイッチを工場出荷時設定にリセットしますが、再起動は行いません。

「Apply」ボタンをクリックして、リセット操作を開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

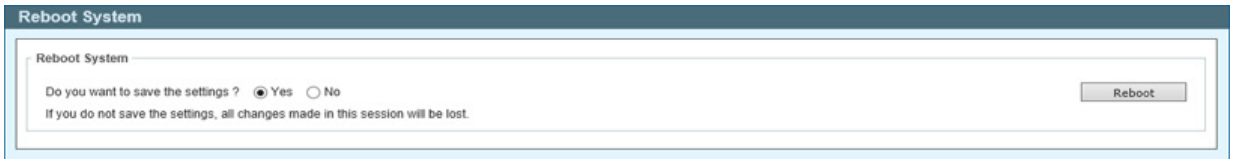


図 15-24　Reboot System 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Yes	スイッチは再起動する前に現在の設定を保存されます。
No	スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。
Reboot	スイッチは再起動します。

「Reboot」をクリックして再起動を開始します。

Save（保存）

Save Configuration（コンフィグレーションの保存）

Save > Save Configuration をクリックし、以下の画面を表示します。

コンフィグレーションの保存

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Apply」ボタンをクリックします。

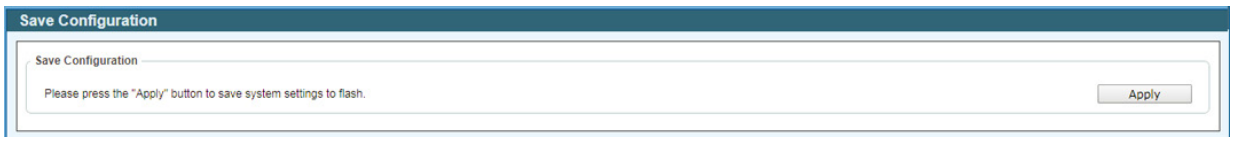


図 15-25　Save - Configuration 画面

警告　「Save Configuration」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。

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。

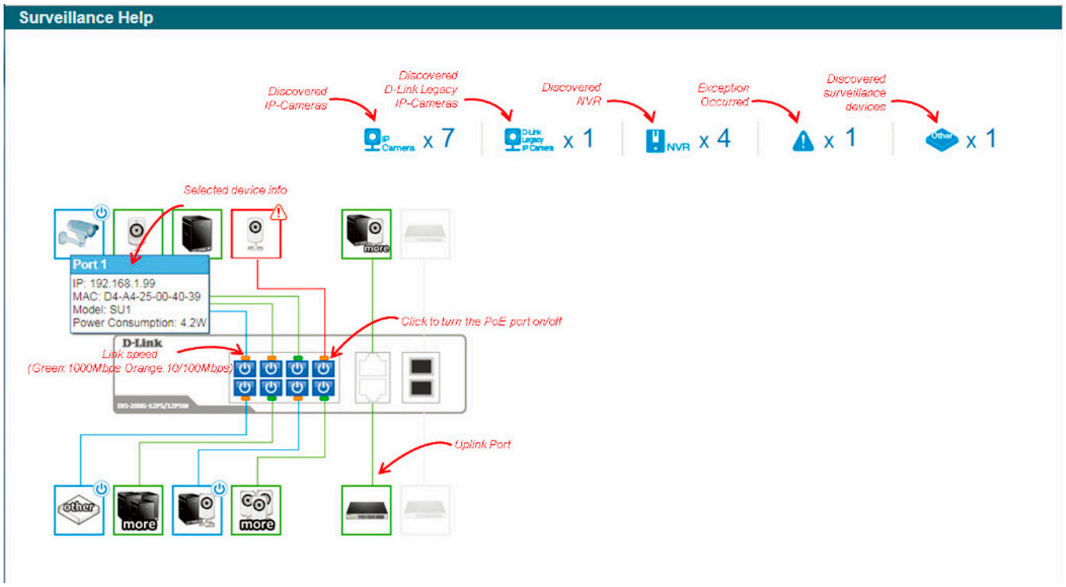


図 15-26　Surveillance Help - Diagram 画面

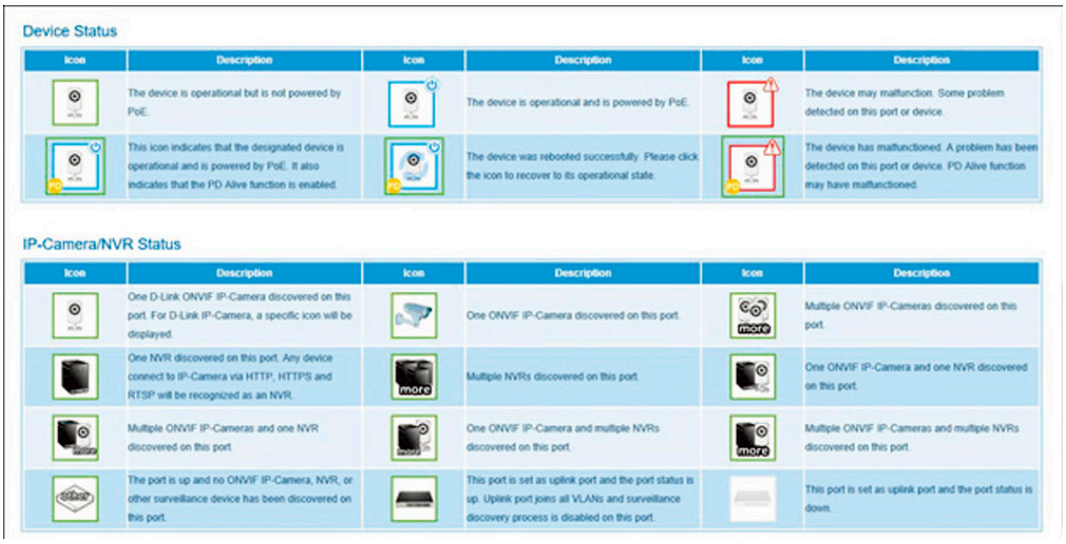


図 15-27　Surveillance Help - Table 画面

Online Help（オンラインヘルプ）

D-Link Support Site（D-Link サポート Web サイト（英語））

クリックすると D-Link のサポート Web サイト（英語）へ接続します。インターネット接続が必要です。

User Guide（ユーザガイド（英語版））

ユーザガイド（英語版）を表示します。インターネット接続が必要です。

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　セッションが複数接続されている場合、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。

Logout（ログアウト）

クリックするとログアウトします。

【付録 A】システムログエントリ

スイッチのシステムログに表示される可能性のあるログエントリとそれらの意味を以下に示します。

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
自動サーベイランス VLAN（Auto Surveillance VLAN）	ポートに新しくサーベイランス機器が検出されました。	New surveillance device detected (< インタフェース ID>, MAC: <MAC アドレス >)	Informational	
	ポートのサーベイランス VLAN が有効であると、サーベイランス VLAN に自動的に参加します。	< インタフェース ID> add into surveillance VLAN <VLAN ID>	Informational	
	ポートがサーベイランス VLAN から離脱し、同時にポートのエージングタイム内にサーベイランス VLAN が検出されない場合に、本ログメッセージが送信されます。	< インタフェース ID> remove from surveillance VLAN <VLAN ID>	Informational	
	IPC がサーベイランス VLAN に追加された場合、本ログメッセージが送信されます。	ASV: Add IPC(<IP アドレス > MAC:<MAC アドレス >)	Informational	
	IPC がサーベイランス VLAN から削除された場合、本ログメッセージが送信されます。	ASV: Remove IPC(<IP アドレス > MAC:<MAC アドレス >)	Informational	
	NVR がサーベイランス VLAN に追加された場合、本ログメッセージが送信されます。	ASV: Add NVR(<IP アドレス > MAC:<MAC アドレス >)	Informational	
	NVR がサーベイランス VLAN から削除された場合、本ログメッセージが送信されます。	ASV: Remove NVR(<IP アドレス > MAC:<MAC アドレス >)	Informational	
	Web GUI で ASV2.0 のモードが変更された場合、本ログメッセージが送信されます。	ASV: Mode change from < モード > to < モード >	Informational	
DDM	SFP の警告しきい値超過	Optical transceiver < インタフェース ID> < しきい値タイプ > < 上限 / 下限 > warning threshold exceeded.	Warning	
	SFP のアラームしきい値超過	Optical transceiver < インタフェース ID> < しきい値タイプ > < 上限 / 下限 > alarm threshold exceeded.	Warning	
	SFP の警告しきい値回復	Optical transceiver < インタフェース ID> < しきい値タイプ > < 上限 / 下限 > warning threshold exceeding back to normal.	Warning	
インタフェース（Interface）	ポートがダウン	Port < ポート種類 >< インタフェース ID> link down	Informational	
	ポートが回復	Port < ポート種類 >< インタフェース ID> link up, < リンク速度 >	Informational	
ループバック検知（LBD）	ループが発生	< インタフェース ID> LBD loop occurred.	Critical	
	ループが回復	< インタフェース ID> LBD loop recovered.	Critical	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
ログイン / ログアウト CLI	コンソール経由のログイン成功	Unit < ユニット ID>, Successful login through Console（Username: < ユーザ名 >）	Informational	
	コンソール経由のログイン失敗	Unit< ユニット ID>, Login failed through Console（Username: < ユーザ名 >）	Warning	
	コンソールセッション、タイムアウト	Unit< ユニット ID>, Console session timed out（Username: < ユーザ名 >）	Informational	
	コンソール経由でログアウト	Unit< ユニット ID>, Logout through Console（Username: < ユーザ名 >）	Informational	
	Telnet 経由のログイン成功	Successful login through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet 経由のログイン失敗	Login failed through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	Telnet セッションタイムアウト	Telnet session timed out（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet 経由でログアウト	Logout through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
PoE	使用電力のしきい値越え	Unit < ユニット ID> usage threshold < パーセンテージ > is exceeded	Warning	
	使用電力のしきい値回復	Unit < ユニット ID> usage threshold < パーセンテージ > is recovered	Warning	
	PD アライブチェック失敗	ASV: PD alive check failed. (Port: < インタフェース ID>, PD: <IP アドレス >)	Warning	
Port Security（ポートセキュリティ）	ポートセキュリティ侵犯が発生	MAC address <MAC アドレス > causes port security violation on < インタフェース ID>	Warning	
	アドレス数がシステムで上限値に到達	MAC address <MAC アドレス > causes port security violation on < インタフェース ID>	Warning	
Safeguard Engine（セーフガードエンジン）	セーフガードエンジン機能が省エネモードに遷移しました。	Limit on system entry number has been exceeded	Warning	
	セーフガードエンジン機能がノーマルモードに遷移しました。	Unit < ユニット ID>,SafeGuard Engine enters NORMAL mode	Informational	
SNMP	無効なコミュニティ名を含む SNMP request 受信	SNMP request received from <IP アドレス > with invalid community string!	Informational	
Telnet	Telnet 経由のログイン成功	Successful login through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet 経由のログイン失敗	Login failed through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	Telnet 経由でログアウト	Logout through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet セッションタイムアウト	Telnet session timed out（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
音声 VLAN	新しい音声機器を検出	New voice device detected (< インタフェース ID>, MAC: <MAC アドレス >)	Informational	
	自動音声 VLAN モードのインタフェースを音声 VLAN に追加しました。	< interface-id > add into voice VLAN <VLAN ID>	Informational	
	インタフェースが音声 VLAN から離脱し、同時にそのインタフェースのエージングタイム内に音声 VLAN が見つからないとログメッセージを送信します。	< interface-id > remove from voice VLAN <VLAN ID>	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
Web	Web 経由のログイン成功	Successful login through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Web 経由のログイン失敗	Login failed through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	Web セッションタイムアウト	Web session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web 経由でログアウト	Logout through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
Web 認証	ホストによる認証通過	Web-Authentication host login success (Username: < ユーザ名 >, IP: <IP アドレス | IPv6 アドレス >, MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>)	Informational	
	ホストによる認証失敗	Web-Authentication host login fail (Username: < ユーザ名 >, IP: <IP アドレス | IPv6 アドレス >, MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>).	Error	

【付録 B】トラップログ

本製品では、以下のトラップログが検出されます。

トラップ名	説明	OID
認証失敗		
authenticationFailure	管理者である SNMPv2 エンティティが正しく認証されなかった旨プロトコルメッセージを受信すると、送信されます。 SNMPv2 関連はすべて本トラップを送信可能です。「snmpEnableAuthenTraps」オブジェクトは本トラップが実行されたことを意味します。	1.3.6.1.6.3.1.1.5.5
DDM		
dDdmAlarmTrap	異常なアラーム状況の発生やアラーム状況からの回復時に送信されます。 関連オブジェクト : (1) dDdmNotifyInfoIfIndex (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.11.155.1000.72.0.1
dDdmWarningTrap	異常な警告状況の発生や警告状況からの回復時に送信されます。 関連オブジェクト : (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.11.155.1000.72.0.2
LBD		
isLbdLoopOccurred	インタフェースループ発生時に送信されます。 関連オブジェクト : (1) isLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.11.155.1000.46.0.1
isLbdLoopRestart	インタフェースループが時間をおいて再開した時に送信されます。 関連オブジェクト : (1) isLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.11.155.1000.46.0.2
LLDP		
lldpRemTablesChange	「lldpStatsRemTableLastChangeTime」の値が変更されたときに送信されます。NMS により LLDP リモートシステムテーブルメンテナンスポールのトリガとして使用されます。 関連オブジェクト : (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
STP		
newRoot	送信エージェントがスパニングツリーの新しいルートになった時に送信されます。新しいルートが決まり次第ブリッジによって送信されます。トポロジ変更タイマの期限切れに伴い、後続の決定後すぐに送信されます。	1.3.6.1.2.1.17.0.1
topologyChange	設定ポートがラーニング状態からフォワーディング状態へ変更した場合、またはフォワーディング状態からブロック状態に変更した場合にブリッジによって送信されます。「newRoot」トラップが同じ変更に伴い送信される場合、本トラップは送信されません。	1.3.6.1.2.1.17.0.2
PoE		
pethMainPowerUsageOnNotification	PSE しきい値が設定され使用電力がしきい値を超えた場合に送信されます。同じオブジェクトインスタンスの通知が送信されてから最小 500 ミリ秒経過している必要があります。 関連オブジェクト : (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
pethMainPowerUsageOffNotification	PSE しきい値が設定されず、使用電力がしきい値を超えていない場合に送信されます。同じオブジェクトインスタンスの通知が送信されてから最小 500 ミリ秒経過している必要があります。 関連オブジェクト : (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
isPoeIfPdAliveFailOccurNotification	PD 機器が動作を停止したか、回答をしていません。	1.3.6.1.4.1.171.11.155.1000.24.0.4

トラップ名	説明	OID
ポート		
linkUp	ポートリンクアップ時の通知 関連オブジェクト : (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
linkDown	ポートリンクダウン時の通知 関連オブジェクト : (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3
ポートセキュリティ		
dPortSecMacAddrViolation	ポートセキュリティトラップが有効時に、事前に設定したポートセキュリティ設定を侵害している新しい MAC アドレスがトリガとなり送信。 関連オブジェクト : (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.171.14.8.0.1
スタート		
coldStart	代理人としての SNMPv2 エンティティが再初期化され設定変更時の通知	1.3.6.1.6.3.1.1.5.1
warmStart	代理人としての SNMPv2 エンティティが再初期化され設定変更されない時の通知	1.3.6.1.6.3.1.1.5.2
Web 認証		
isWebAuthLoggedSuccess	ホストによるログイン成功時（Web 認証）の通知 関連オブジェクト : (1) ifIndex (2) isSessionAuthVlan (3) isSessionClientMacAddress (4) isSessionClientAddrType (5) isSessionClientAddress (6) isSessionAuthUserName	1.3.6.1.4.1.171.11.155.1000.154.0.1
isWebAuthLoggedFail	ホストによるログイン失敗時（Web 認証）の通知 関連オブジェクト : (1) ifIndex (2) isSessionAuthVlan (3) isSessionClientMacAddress (4) isSessionClientAddrType (5) isSessionClientAddress (6) isSessionAuthUserName	1.3.6.1.4.1.171.11.155.1000.154.0.2

【付録 C】IETF RADIUS 属性のサポート

RADIUS（Remote Authentication Dial-In User Service）属性は要求と応答用に特定の認証、許可、情報、および構成の詳細を運びます。この付録では現在スイッチがサポートする RADIUS 属性を示します。RADIUS 属性は IETF 標準と VSA（Vendor-Specific Attribute : ベンダー固有属性）によってサポートされています。

IETF 標準の RADIUS 属性は RFC 2865 Remote Authentication Dial-In User Service (RADIUS)、RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support、および RFC 2869 RADIUS Extensions で定義されています。

以下の表は D-Link スイッチがサポートする IETF RADIUS 属性を示しています。

1. RADIUS 認証属性

番号	IETF 属性
1	User-Name
2	User-Password

【付録 D】機能設定例

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

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DIS-200G-12SW、DIS-200G-12PSW

Traffic Segmentation（トラフィックセグメンテーション）

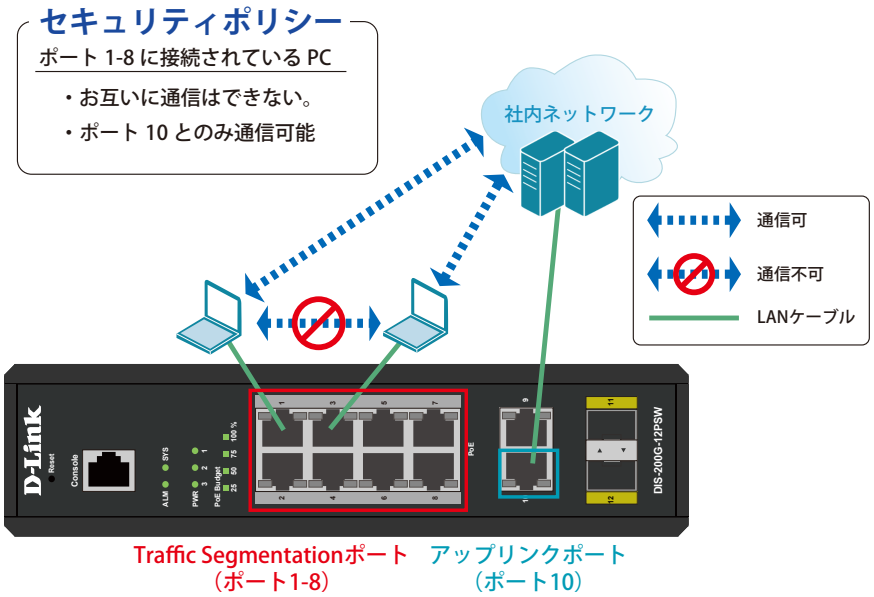


図 16-1　Traffic Segmentation（DIS-200G-12PSW）

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 10 とのみ通信ができるようにします。

設定手順

1. 「Traffic Segmentation」を有効にします。

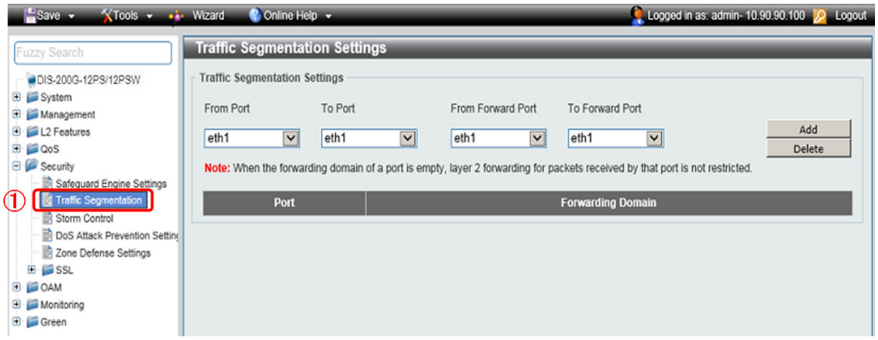


図 16-2　Traffic Segmentation（DIS-200G-12PSW）

2. 1～8番ポートを10番ポートとのみ通信する設定をします。

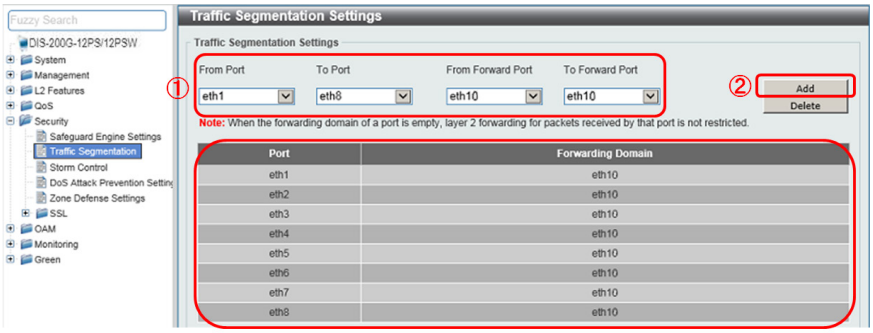


図 16-3　Traffic Segmentation Settings（DIS-200G-12PSW）

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

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

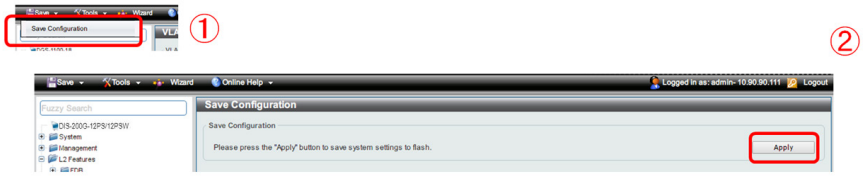


図 16-4　Save Configuration（DIS-200G-12PSW）

VLAN

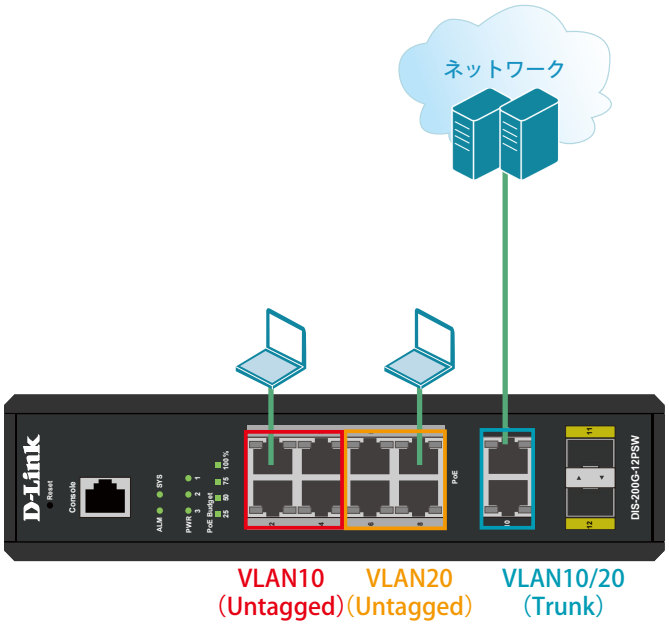


図 16-5　VLAN（DIS-200G-12PSW）

概要

VLAN を設定します。ポート 1 ～ 4 に VLAN10 を「Untagged」で割り当て、ポート 5 ～ 8 に VLAN20 を「Untagged」で割り当て、ポート 9、10 において、VLAN10 と VLAN20 を「Tagged」で割り当てます。

設定手順

1. VLAN10 と VLAN20 を作成します。**L2 Features > VLAN > 802.1Q VLAN** で VLAN10 を作成します。

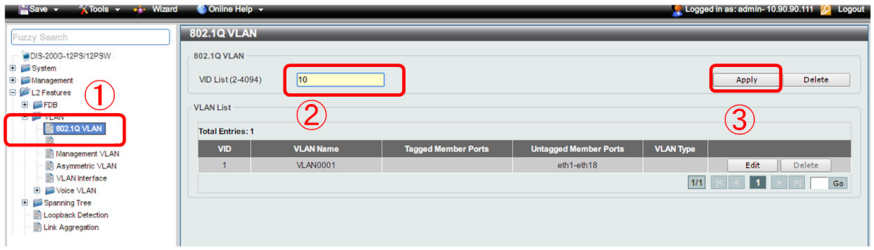


図 16-6　VLAN 作成（DIS-200G-12PSW）

2. 同様に VLAN20 を作成します。

3. ポート 1 ～ 4 に VLAN10、ポート 5 ～ 8 に VLAN20 を割り当て、ポート 9 ～ 10 に VLAN10、20 を「Tagged」で割当てします。
L2 Features > VLAN > VLAN Interface でポート 1 ～ 4 に VLAN10 を「Untagged」で割り当てます。まずポート 1 の「Edit」をクリックします。

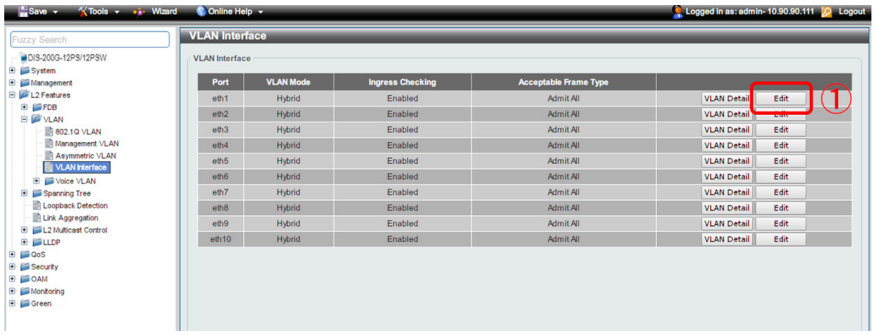


図 16-7　VLAN 編集（DIS-200G-12PSW）

4. ②の項目で下図のように設定し「Apply」をクリックします。

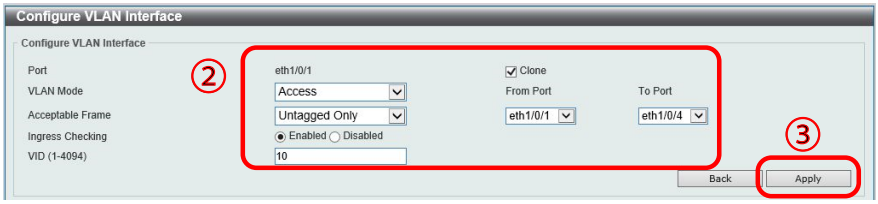


図 16-8　VLAN インタフェース設定（ポート 1-4）（DIS-200G-12PSW）

VLAN Mode	Access
Acceptable Frame	Untagged Only
VID	10
Clone	Check
From Port / To Port	1-4

5.「ポート 5 ～ 8」の設定では VID を 20（VLAN20）を上記の手順で割当てます。

6.「ポート 9 ～ 10」の設定では「VLAN10」と「VLAN20」を Trunk（トランク）で割当て「Apply」をクリックします。

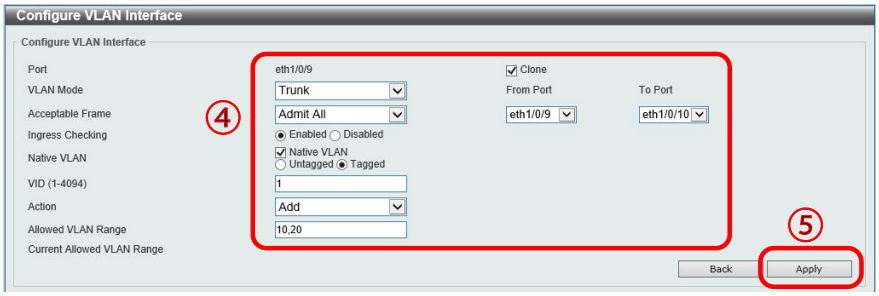


図 16-9　VLAN インタフェース設定（ポート 9-10）（DIS-200G-12PSW）

VLAN Mode	Trunk
Action	Add
Allowed VLAN Range	10、20
Clone	Check
From Port / To Port	9-10

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

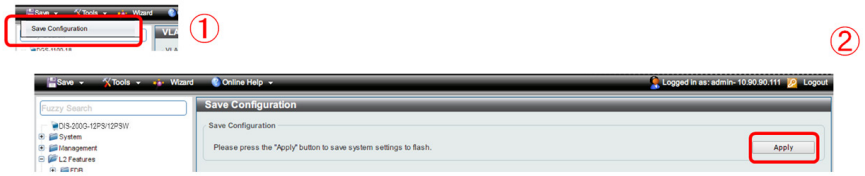


図 16-10　Save Configuration（DIS-200G-12PSW）

Link Aggregation（リンクアグリゲーション）

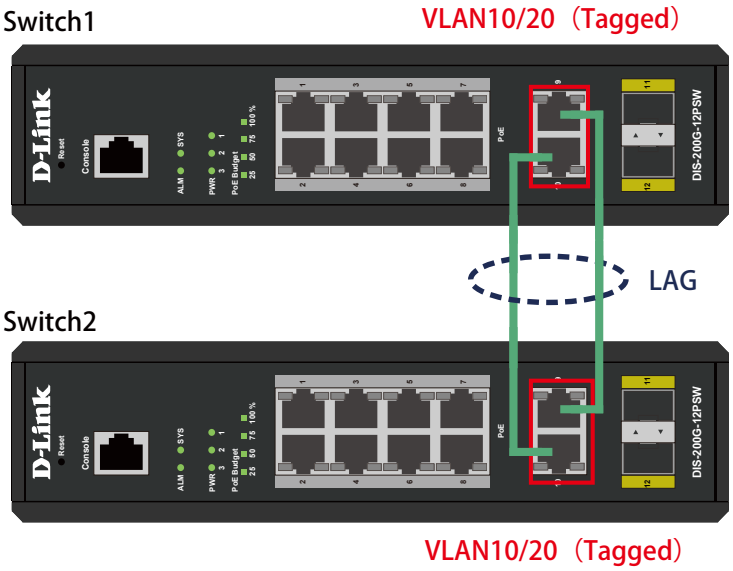


図 16-11　Link Aggregation（DIS-200G-12PSW）

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 9 と 10 に VLAN10 と VLAN20 を Tagged で割当て、ポート 9 と 10 をグループ 1 として LACP によるリンクアグリゲーションに設定します。

設定手順

1. VLAN10 と VLAN20 を作成します。**L2 Features > VLAN > 802.1Q VLAN** で VLAN10 を作成します。

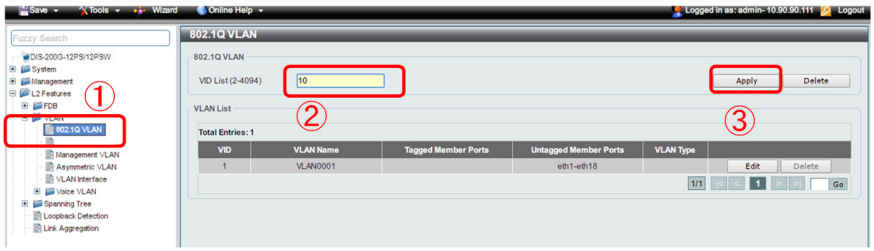


図 16-12　VLAN 作成（DIS-200G-12PSW）

2. 同様に VLAN20 を作成します。

3. ポート 9 ～ 10 に VLAN10、20 を「Tagged」で割当てします。

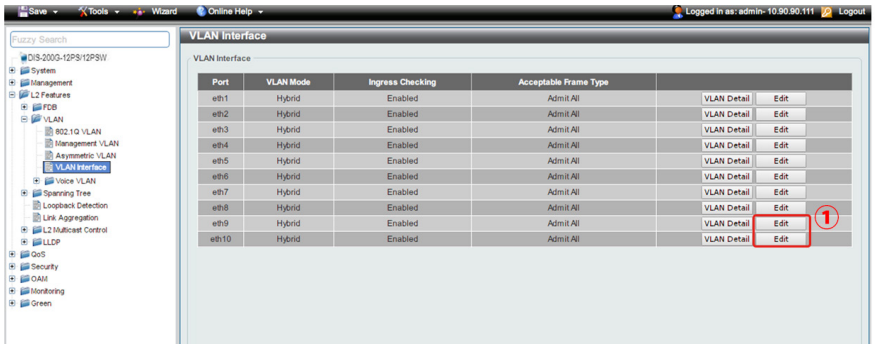


図 16-13　VLAN 編集（DIS-200G-12PSW）

4. 「ポート 9 ～ 10」の設定で「VLAN10」と「VLAN20」を Trunk（トランク）で割当て「Apply」をクリックします。

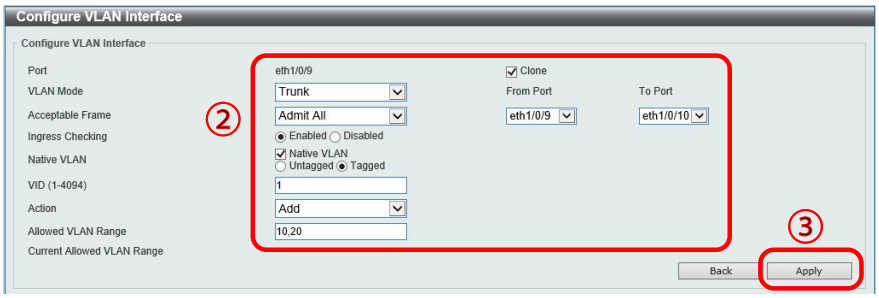


図 16-14　VLAN インタフェース設定（ポート 9-10）（DIS-200G-12PSW）

VLAN Mode	Trunk
Action	Add
Allowed VLAN Range	10、20
Clone	Check
From Port / To Port	9-10

5. 作成した VLAN でトランクしたくない VLAN は Remove を選択して削除してください。

6. **L2 Features > Link Aggregation** でポート 9 ～ 10 を LACP に設定します。
②の項目で対象ポートを「eth9 ～ 10」に指定し「Group ID」「Mode」を下図のように設定します。「Add」をクリックします。

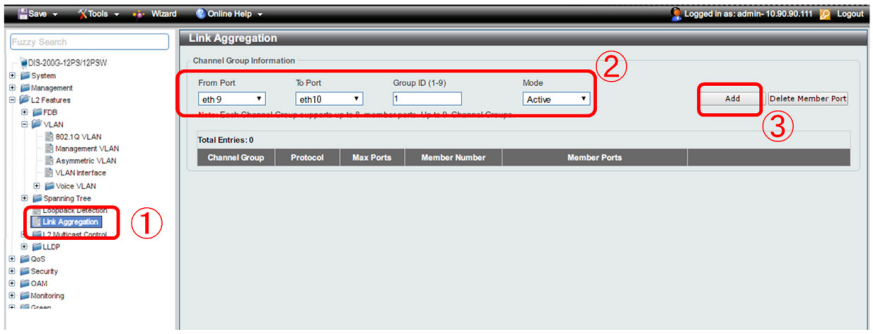


図 16-15　Link Aggregation 設定（ポート 9-10）（DIS-200G-12PSW）

Group ID	1
Mode	Active

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

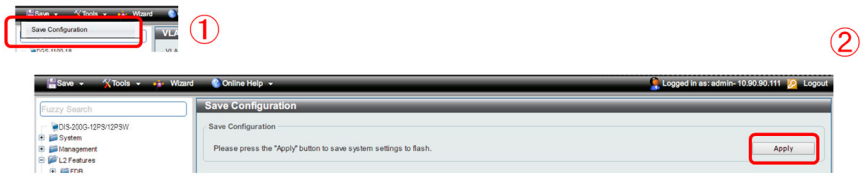


図 16-16　Save Configuration（DIS-200G-12PSW）

Firmware Upgrade（ファームウェアアップグレード）

概要

ファームウェアを HTTP 経由でアップグレードします。

設定手順

1. **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP** をクリックし HTTP でファームウェアをスイッチにダウンロードします。②で「Source File」を選択し、「Upgrade」をクリックします。

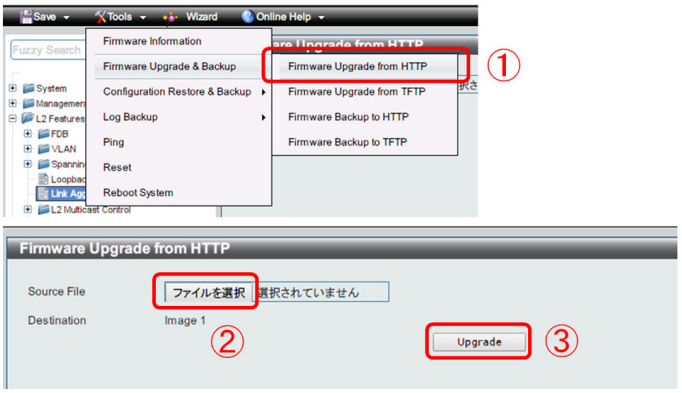


図 16-17　Firmware Upgrade from HTTP（DIS-200G-12PSW）

2. **Tools > Firmware Information** をクリックし、起動ファームウェアを切り替えます。

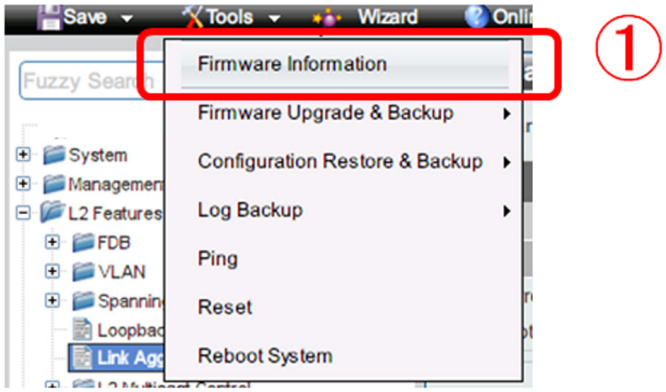


図 16-18　Firmware Information（DIS-200G-12PSW）

3. 表示の画面でダウンロードしたファームウェアの「Boot UP」ボタンを押下します。

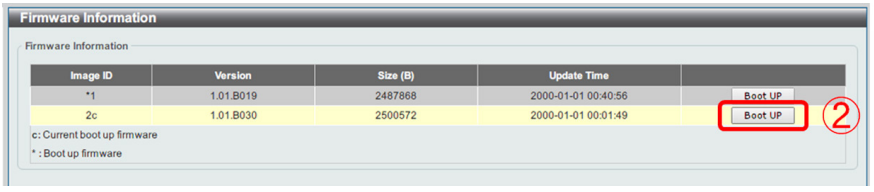


図 16-19　Firmware Information / Boot UP（DIS-200G-12PSW）

4. **Tools > Reboot** をクリックし、「Reboot」で再起動させます。

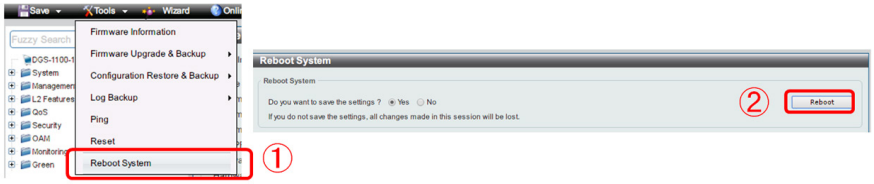


図 16-20　Reboot System（DIS-200G-12PSW）