D-Link DMS-1100 シリーズ

Multi Gigabit Layer2 Easy Smart Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

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

禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI - A

ご使用上の注意

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

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

  ※当社出荷時に「Warranty Void Sticker」（シール）が貼られていない製品もあります。

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。

ラック搭載型製品に関する一般的な注意事項

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

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

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

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

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

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

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

バッテリの取り扱いについて

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

安全にお使いいただくために

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

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

注意 製品に貼られているラベルや「Warranty Void Sticker」(シール) 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。

※当社出荷時に「Warranty Void Sticker」（シール）が貼られていない製品もあります。

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

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

警告 本書の内容の一部、または全部を無断で転載したり、複写することは固くお断りします。

目次

安全にお使いいただくために 2
ご使用上の注意 4
静電気障害を防止するために 4
電源の異常 4
ラック搭載型製品に関する一般的な注意事項 5
バッテリの取り扱いについて 5

はじめに 10

本マニュアルの対象者 11
表記規則について 11
製品名 / 品番一覧 11

第 1 章　本製品のご使用にあたって 12

スイッチ概要 12
サポートする機能 12
搭載ポート 14
前面パネル 14
　LED 表示 15
背面パネル 15
SFP スロット 16

第 2 章　スイッチの設置 17

パッケージの内容 17
ネットワーク接続前の準備 17
ゴム足の取り付け（19 インチラックに設置しない場合） 17
19 インチラックへの取り付け 18
　ブラケットの取り付け 18
　19 インチラックにスイッチを取り付ける 18
電源抜け防止器具の装着 19
スイッチの接地 21
　接地に必要なツールと機器 21
電源の投入 22

第 3 章　スイッチの接続 23

エンドノードと接続する 23
ハブまたはスイッチと接続する 23
バックボーンまたはサーバと接続する 24

第 4 章　Web ベースのスイッチ管理 25

Web ベースの管理について 25
Web マネージャへのログイン 25
Smart Wizard 設定 27
Web マネージャの画面構成 29
　Web マネージャのメイン画面について 29
Web マネージャのメニュー構成 30
Device Information（デバイス情報） 31
　Device Information（デバイス情報） 31
Save（Save メニュー） 32
　Save Configuration（コンフィグレーションの保存） 32
Tools（Tools メニュー） 33
　Firmware Information（ファームウェア情報） 33
　Configuration Information（コンフィグレーション情報） 33
　Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ） 33
　Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ） 35
　Log Backup（ログファイルのバックアップ） 37
　Ping（Ping 送信） 37
　Reset（リセット） 38
　Reboot System（システム再起動） 39

第 5 章　System（システム設定） 40

System Information（システム情報 ） 40
Port Configuration（ポート設定） 40
　Port Settings（スイッチのポート設定） 40
　Port Status（ポートステータス） 41
　Error Disable Settings（エラーによるポートの無効） 41
　Jumbo Frame（ジャンボフレーム設定） 42

PoE（PoE の管理）（DMS-1100-10TP）....43
PoE System（PoE システム設定）....43
PoE Status（PoE ステータス）....43
PoE Configuration（PoE ポート設定）....44
PoE Measurement（PoE 測定）....44
PD Alive（PD アライブ設定）....45
System Log（システムログ構成）....46
System Log Settings（システムログ設定）....46
System Log Server Settings（システムログサーバの設定）....47
System Log（Syslog ログ）....47
Time and SNTP（時刻設定）....48
Clock Settings（時間設定）v....48
Time Zone Settings（タイムゾーン設定）....48
SNTP Settings（SNTP 設定）....50
Time Range（タイムレンジ設定）....51

第 6 章　Management（スイッチの管理）　52

User Accounts Settings（ユーザアカウント設定）....52
Password Encryption（パスワード暗号化）....53
SNMP Settings（SNMP 設定）....53
SNMP Global Settings（SNMP グローバル設定）....54
SNMP View Table Settings（SNMP ビューテーブル）....55
SNMP Community Table Settings（SNMP コミュニティテーブル設定）....55
SNMP Group Table Settings（SNMP グループテーブル）....56
SNMP Engine ID Local Settings（SNMP エンジン ID ローカル設定）....57
SNMP User Table Settings（SNMP ユーザテーブル設定）....57
SNMP Host Table Settings（SNMP ホストテーブル設定）....58
Web（Web 設定）....59
Session Timeout（セッションタイムアウト）....59
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）....59

第 7 章　L2 Features（L2 機能の設定）　61

FDB（FDB 設定）....61
Static FDB（スタティック FDB の設定）....61
MAC Address Table Settings（MAC アドレステーブル設定）....62
MAC Address Table（MAC アドレステーブル）....63
VLAN（VLAN 設定）....64
802.1Q VLAN（802.1Q VLAN）....65
Asymmetric VLAN（Asymmetric VLAN 設定）....65
VLAN Interface（VLAN インタフェース設定）....66
Auto Surveillance VLAN（自動サーベイランス VLAN）....69
Voice VLAN（音声 VLAN）....71
STP（スパニングツリー設定）....74
STP Global Settings（STP グローバル設定）....74
STP Port Settings（STP ポートの設定）....76
MST Configuration Identification（MST の設定）....77
STP Instance（STP インタンス設定）....78
MSTP Port Information（MSTP ポート情報）....78
ERPS (G.8032)（イーサネットリングプロテクション設定）....79
ERPS....79
ERPS Profile（ERPS プロファイル）....80
Loopback Detection（ループバック検知設定）....82
Link Aggregation（リンクアグリゲーション）....83
L2 Multicast Control（L2 マルチキャストコントロール）....84
IGMP Snooping（IGMP Snooping の設定）....84
MLD Snooping（MLD Snooping 設定）....89
LLDP....94
LLDP Global Settings（LLDP グローバル設定）....94
LLDP Port Settings（LLDP ポート設定）....95
LLDP Management Address List（LLDP 管理アドレスリスト）....96
LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）....96
LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）....97
LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）....97
LLDP-MED Port Settings（LLDP-MED ポート設定）....98
LLDP Statistics Information（LLDP 統計情報）....98
LLDP Local Port Information（LLDP ローカルポート情報）....99
LLDP Neighbor Port Information（LLDP ネイバポート情報）....100

第 8 章　L3 Features（L3 機能の設定） 101

IPv4 Interface（IPv4 インタフェース） 101
IPv4 Default Gateway（IPv4 デフォルトゲートウェイ） 102
IPv6 Interface（IPv6 インタフェース） 102
IPv6 Default Gateway（IPv6 デフォルトゲートウェイ） 104

第 9 章　QoS（QoS 機能の設定） 105

Port Default CoS（ポートデフォルト CoS 設定） 105
Port Scheduler Method（ポートスケジューラーメソッド設定） 105
Queue Settings（QoS 設定） 106
CoS to Queue Mapping（CoS キューマッピング設定） 106
Port Rate Limiting（ポートレート制限設定） 107

第 10 章　Security（セキュリティ機能の設定） 108

Safeguard Engine（セーフガードエンジン） 108
Trusted Host（トラストホスト） 108
Traffic Segmentation Settings（トラフィックセグメンテーション） 109
Storm Control Settings（ストームコントロール） 109
DoS Attack Prevention Settings（DoS 攻撃防止設定） 110
SSL（Secure Socket Layer） 111
SSL Global Settings（SSL グローバル設定） 111
SSL Service Policy（SSL サービスポリシー） 111

第 11 章　OAM (Operations, Administration, Maintenance：運用・管理・保守) 113

Cable Diagnostics（ケーブル診断機能） 113

第 12 章　Monitoring（スイッチのモニタリング） 114

Statistics（統計情報） 114
Port（ポート統計情報） 114
Port Counters（ポートカウンタ） 115
Counters（カウンタ） 116
Mirror Settings（ミラー設定） 117

第 13 章　Green（省電力機能） 118

Power Saving（省電力） 118
EEE（Energy Efficient Ethernet/ 省電力イーサネット） 118

第 14 章　スイッチのメンテナンス 119

スイッチを工場出荷時設定に戻す 119
スイッチを再起動させる 119

【付録 A】　ケーブルとコネクタ 120

【付録 B】　ケーブル長 120

【付録 C】　用語解説 121

【付録 D】　機能設定例 123

対象機器について 123
Traffic Segmentation（トラフィックセグメンテーション） 123
VLAN 125
Link Aggregation（リンクアグリゲーション） 129

はじめに

DMS-1100 シリーズユーザマニュアルは、本スイッチのインストールおよび操作方法を例題と共に記述しています。

第 1 章　本製品のご使用にあたって

- 本スイッチの概要とその機能について説明します。また、前面、背面、側面の各パネルと LED 表示について説明します。

第 2 章　スイッチの設置

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

第 3 章　スイッチの接続

- スイッチをご使用のネットワークに接続する方法を説明します。

第 4 章　Web ベースのスイッチ管理

- Web ベースの管理機能への接続方法および使用方法について説明します。

第 5 章　System（システム設定）

- デバイス情報、ポート設定、PoE 設定、システムログ設定、時刻設定などの基本機能の設定について説明します。

第 6 章　Management（スイッチの管理）

- ユーザアカウント設定、SNMP 設定、Web 設定などの管理機能について説明します。

第 7 章　L2 Features（L2 機能の設定）

- VLAN、ポートトランキング、スパニングツリー、LLDP などのレイヤ 2 機能について説明します。

第 8 章　L3 Features（L3 機能の設定）

- インタフェース設定、デフォルトゲートウェイ設定などのレイヤ 3 機能について説明します。

第 9 章　QoS（QoS 機能の設定）

- QoS 機能について説明します。帯域制御、QoS スケジューリング、802.1p プライオリティなどの機能を含みます。

第 10 章　Security（セキュリティ機能の設定）

- トラストホスト、トラフィックセグメンテーション、SSL、セーフガードエンジンなどのセキュリティ機能について説明します。

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

- ケーブル診断機能機能について説明します。

第 12 章　Monitoring（スイッチのモニタリング）

- パケット統計情報、エラー、パケットサイズ、ミラーリングなどのモニタ機能について説明します。

第 13 章　Green（省電力機能）

- Power Saving（省電力）、EEE（Energy Efficient Ethernet/ 省電力イーサネット）について説明します。

第 14 章　スイッチのメンテナンス

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

【付録 A】　ケーブルとコネクタ

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

【付録 B】　ケーブル長

- 各規格に対応するケーブル長について説明します。

【付録 C】　用語解説

- 一般用語について説明します。

【付録 D】　機能設定例

- 一般によく使う機能についての設定例を記載します。

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	コマンドパラメータ（可変または固定）。	*value*
< >	可変パラメータ。< > にあたる箇所に値または文字を入力します。	<*value*>
[ ]	任意の固定パラメータ。	[*value*]
[< >]	任意の可変パラメータ。	[<*value*>]
{ }	{ } 内の選択肢から 1 つ選択して入力するパラメータ。	{*choice1* | *choice2*}
|（垂直線）	相互排他的なパラメータ。	*choice1* | *choice2*
[{ }]	任意のパラメータで、指定する場合はどちらかを選択します。	[{*choice1* | *choice2*}]

製品名 / 品番一覧

製品名	品番
DMS-1100-10TS	DMS-1100-10TS/A1
DMS-1100-10TP	DMS-1100-10TP/A1

第 1 章　本製品のご使用にあたって

- スイッチ概要
- サポートする機能
- 搭載ポート
- 前面パネル
- 背面パネル
- SFP スロット

スイッチ概要

D-Link の最新 L2 スイッチである 2.5 ギガビットイーサネットスイッチシリーズは、プラグアンドプレイの簡易性と中小規模（SMB）ネットワーク向けの信頼性を兼ね備えたスイッチです。すべてのモデルは、前面パネルの見やすい診断用 LED を搭載するメタルケースに収納されており、ネットワークセキュリティ、トラフィックセグメンテーション、QoS 及び多様な管理機能を搭載しています。

柔軟なポート設定

DMS-1100 シリーズは D-Link の新世代 2.5G スイッチです。8 ポートの 10/100/1000Mbps/2.5Gbps ポート（DMS-1100-10TP では PoE 対応ポート）に加えて、SFP+ スロットを 2 つ搭載しています。DMS-1100 シリーズのスイッチは、多機能で直感的なソフトウェア構成とシンプルで見やすい WebGUI を備え、リモートからブラウザを使用して設定を行うことができます。2.5GBASE-T は既存の規格と上位互換性があるため、Cat 5e ケーブル（シールド付き・シールドなしのツイストペアケーブル）を使用して、10/100/1000Mbps のネットワーク環境から 2.5Gbps ネットワーク環境へ、透過的にアップグレードすることができます。また、10G SFP+ に対応しており、消費電力の抑制、長距離への対応、レイテンシのパフォーマンス向上を図ることができます。隣接したスイッチの 10Gbps 通信には、ダイレクトアタッチケーブル（DAC）を使用してコストを抑えることも可能です。

D-Link グリーンテクノロジー

D-Link グリーン製品は、高性能で環境に優しい製品を提供します。DMS-1100 シリーズにおける D-Link Green 技術には、EEE、LED オフによる電力調整のような消費電力を削減するイノベーションが盛り込まれています。

レイヤ 2 機能

本スイッチは、IGMP Snooping、MLD Snooping、ポートミラーリング、スパニングツリー、802.3ad LACP、LLDP およびループバック検知などの L2 機能を搭載しており、性能とネットワークの柔軟性を強化しています。

QoS

本スイッチは帯域制御と 802.1p プライオリティキューに対応しており、音声や映像といった帯域幅の影響を受けやすいアプリケーションを適切に処理することができます。これらの機能は、802.1p トラフィックと一緒に動作して優先順位をつけることが可能です。

ネットワークセキュリティ

セーフガードエンジン機能は、ウィルス攻撃により引き起こされるトラフィックのフラッドからスイッチを保護します。また、ストームコントロールでは、異常なトラフィックによるフラッドからネットワークを保護します。ポートセキュリティはネットワークデバイスの安全を保つことのできる、シンプルですが有効な認証方法です。

多様な管理

D-Link の新世代スイッチである 2.5 ギガビットイーサネットスイッチは、管理者によるリモートでのネットワーク制御が可能であるため、ネットワークをシンプルかつ簡単に管理することを可能にし、ビジネスの成長を助けます。

さらに、スイッチステータスに関する情報のために、実装されている MIB を使用してスイッチへのポーリングや異常なイベントのトラップ送信が可能です。MIB がサポートされているため、SNMP 環境の管理において、サードパーティ製のデバイスと本スイッチを統合化することができます。本スイッチはまた「D-View 7.0」に対応しており、視覚的なインタフェースによる効果的な操作、管理が可能です。

サポートする機能

- IEEE 802.3 10BASE-T、IEEE 802.3u 100BASE-TX、IEEE 802.3ab 1000BASE-T、IEEE 802.3z 1000BASE-X、IEEE 802.3bz 2.5GBASE-T、IEEE802.3ae 10GBASE-SR/LR/ER/ZR、IEEE 802.3x Flow Control
  IEEE 802.1D Spanning Tree、IEEE 802.1w Rapid Spanning Tree、IEEE 802.1s Multiple Spanning Tree、IEEE 802.3ad Link Aggregation、IEEE 802.1Q VLAN Tagging
  IEEE 802.1p Class of Service、IEEE 802.3az Energy Efficient Ethernet
  IEEE 802.3af Power over Ethernet（DMS-1100-10TP のみ）、IEEE 802.3at PoE Plus（DMS-1100-10TP のみ）
- L2 機能
  - IGMP スヌーピング：v1/v2
  - MLD スヌーピング：v1
  - スパニングツリー：IEEE 802.1D STP、IEEE 802.1w RSTP、802.1s MSTP
  - E-RPS（ITU-T G.8032 イーサネットリング）
  - ループバック検知（STP 無し）

  - ポートトランキング：IEEE 802.3ad/ スタティック
    DMS-1100-10TS/10TP：8 グループ / デバイス、8 ポート / グループ
  - ポートミラーリング：1 ポート対 1 ポート / 多対 1 ポート
  - ジャンボフレーム：9KBytes
- VLAN
  - IEEE 802.1Q タグ VLAN、ポートベース VLAN、VLAN グループ数：4094（スタティック）
    VLAN ID レンジ：1-4094、Voice VLAN、Asymmetric VLAN、自動サーベイランス VLAN
- QoS
  - 帯域制御、キュー：8 レベル / ポート
  - キューのスケジューリング：Strict/WRR
  - CoS：IEEE 802.1p プライオリティ
- セキュリティ
  - SSLv3/TLS1.2（IPv4/IPv6）
  - ブロードキャスト / マルチキャストストームコントロール
  - D-Link セーフガードエンジン
  - DoS 攻撃防御
  - トラフィックセグメンテーション
  - 管理アクセス認証用：ローカル
- マネジメント
  - LLDP、LLDP-MED、Web ベース GUI（IPv4/IPv6）
  - SNMPv1/v2c/v3、SNMP over IPv6、SNMP トラップ
  - トラストホスト、DHCP/BOOTP クライアント、Syslog、TFTP クライアント（IPv4/IPv6）、SNTP クライアント
  - 設定バックアップ / リストア、ファームウェアバックアップ / リストア
  - ケーブル診断、EEE（802.3az）、デュアル設定ファイル、デュアルイメージ、PD アライブ（DMS-1100-10TP）
- 以下の MIB のサポート
  - MIB II（ RFC1213）
  - MIB Traps Convention（RFC1215）
  - Bridge MIB（RFC1493, RFC4188）
  - SNMP MIB（RFC1157, RFC2571-2576）
  - SNMPv2 MIB（RFC1442, RFC1901-1908, RFC2578, RFC3418, RFC3636）
  - Ether-like MIB（RFC1398, RFC1643, RFC1650, RFC2358, RFC2665, RFC3635）
  - 802.1p MIB（RFC2674, RFC4363）
  - Interface Group MIB
  - Private MIB
  - PoE MIB
  - DDP MIB
  - LLDP-MED MIB

※ IGMP スヌーピンググループと MLD グループは共通のテーブルを使用しています。

搭載ポート

DMS-1100 シリーズスイッチは以下のポートを搭載しています。

DMS-1100-10TS

- 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T ポート x　8
- SFP+ スロット　x　2

DMS-1100-10TP

- 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T ポート x　8（PoE 給電：8）
- SFP+ スロット　x　2

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

種別	製品名
2 芯 SFP モジュール (1Giga)	DEM-310GT
	DEM-311GT
Copper SFP（1Giga）	DGS-712
WDM 対応 1 芯 SFP モジュール	DEM-330T
	DEM-330R
2 芯 SFP+(10Giga) モジュール	DEM-431XT
	DEM-432XT

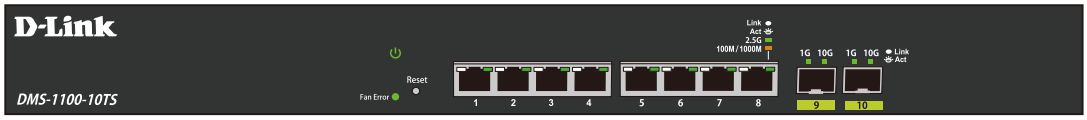
※ スイッチ /SFP モジュールの H/W バージョンの組み合わせによっては、接続できない場合があります。サポートされる SFP モジュールの H/W バージョンについては、弊社 Web ページで公開されている「光トランシーバ対応製品一覧」をご確認ください。

前面パネル

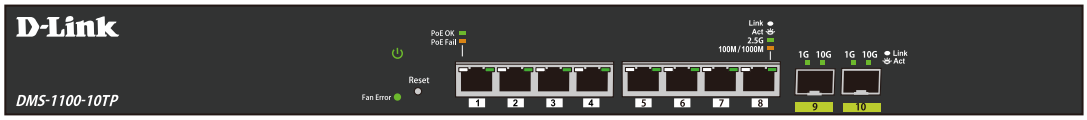
前面パネルには、Power、リセットボタン、オプションモジュール用の SFP スロット、ポートの Link/Act の状態を表示する LED を搭載しています。

参照 LED 表示については、「LED 表示」を参照してください。

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



DMS-1100-10TS の前面パネル図

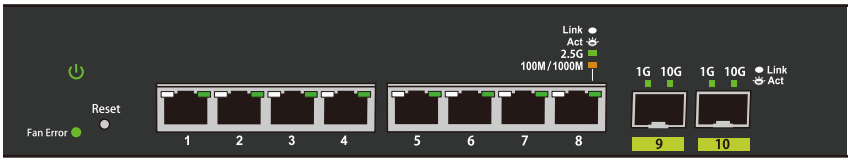


DMS-1100-10TP の前面パネル図

LED 表示

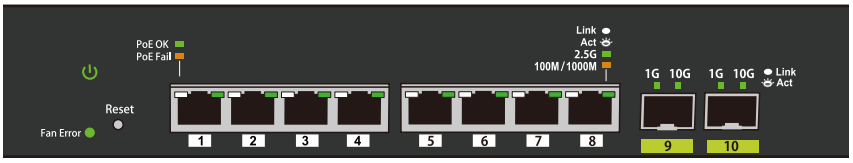
各機種の LED 表示は、以下のイラストと表のとおりです。

DMS-1100-10TS



DMS-1100-10TS の前面パネルの LED 配置図

DMS-1100-10TP



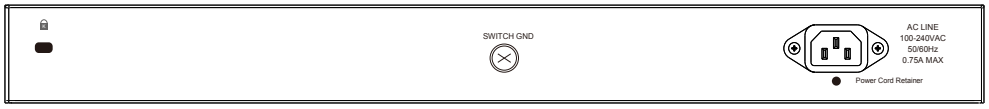
DMS-1100-10TP の前面パネルの LED 配置図

LED	状態	色	内容
システム LED			
Power	点灯	緑	電源が供給されています。
	消灯	―	電源が供給されていません。
Fan Error	点灯	赤	ファンが正常に動作していません。
	消灯	―	ファンは正常に動作しています。
ポート LED			
10/100/1000 Mbps/2.5Gbps ポート LED	点灯	緑	2.5Gbps でリンクが確立しています。
	点滅	緑	2.5Gbps でデータを送受信しています。
	点灯	橙	10/100/1000Mbps でリンクが確立しています。
	点滅	橙	10/100/1000Mbps でデータを送受信しています。
	消灯	―	リンクが確立していません。
SFP+ スロット LED	点灯	緑	10Gbps でリンクが確立しています。
	点滅	緑	10Gbps でデータを送受信しています。
	点灯	橙	1000Mbps でリンクが確立しています。
	点滅	橙	1000Mbps でデータを送受信しています。
	消灯	―	リンクが確立していません。
PoE LED（DMS-1100-10TP）	点灯	緑	接続中の PoE 受電機器に給電中です。
	点灯	橙	PoE 受電機器が接続されていますが不具合が発生しています。 （PD 側のエラーもしくは給電容量の不足により供給できません。）
	消灯	―	給電をしていません。（受電機器が未検出または未接続）

背面パネル

背面パネルには電源コネクタ、接地コネクタ、電源抜け防止器具挿入口、およびセキュリティロックがあります。電源コネクタは標準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ～ 240VAC 内の電圧に調整されます。

DMS-1100-10TS



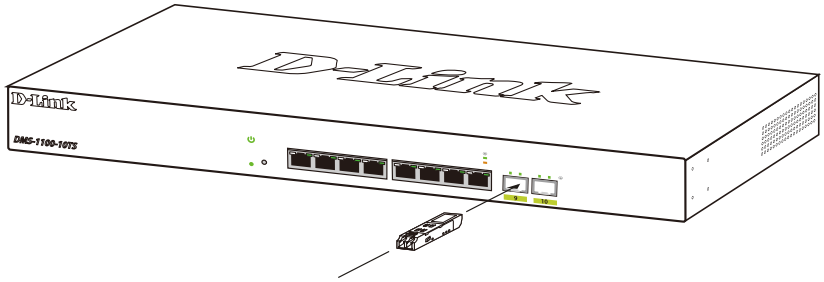
DMS-1100-10TS 背面パネル図

DMS-1100-10TP

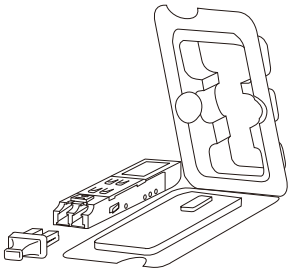
DMS-1100-10TP 背面パネル図

SFP スロット

DMS-1100 シリーズスイッチは、スイッチの前面パネルに SFP モジュール用スロットを装備しています。



スイッチに光トランシーバを取り付ける



SFP モジュール図

第 2 章　スイッチの設置

- パッケージの内容
- ネットワーク接続前の準備
- ゴム足の取り付け（19 インチラックに設置しない場合）
- 19 インチラックへの取り付け
- 電源抜け防止器具の装着
- スイッチの接地
- 電源の投入

パッケージの内容

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

- 本体
- AC 電源ケーブル（100V 用）
- 19 インチラックマウントキット
- 電源抜け防止器具
- ゴム足
- CD-ROM（DMS-1100-10TS のみ）※
- マニュアル
- PL シート

※出荷のタイミングによっては、CD-ROM は同梱されません。

万一、不足しているものや損傷を受けているものがありましたら、ご購入いただきました代理店までご連絡ください。

ネットワーク接続前の準備

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

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

ゴム足の取り付け（19 インチラックに設置しない場合）

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

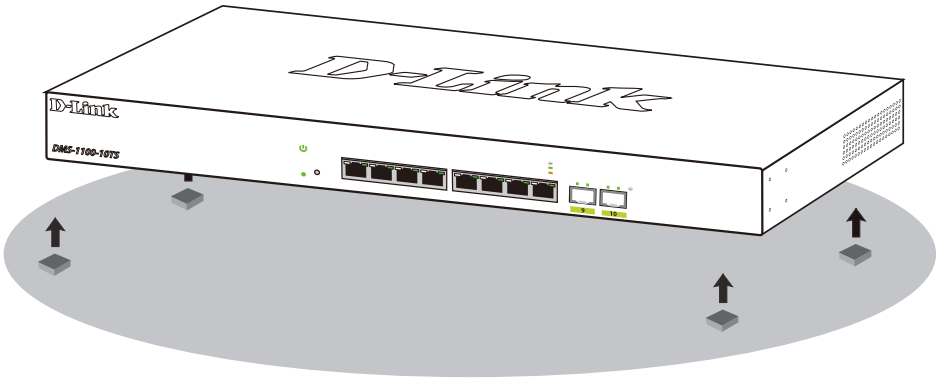


図 2-1　ゴム足の取り付け

19 インチラックへの取り付け

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

ブラケットの取り付け

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

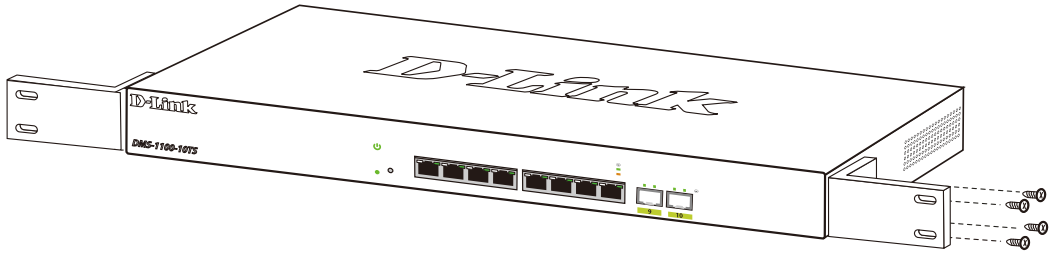


図 2-2　スイッチへのブラケットの取り付け

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

19 インチラックにスイッチを取り付ける

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

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

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

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

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

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

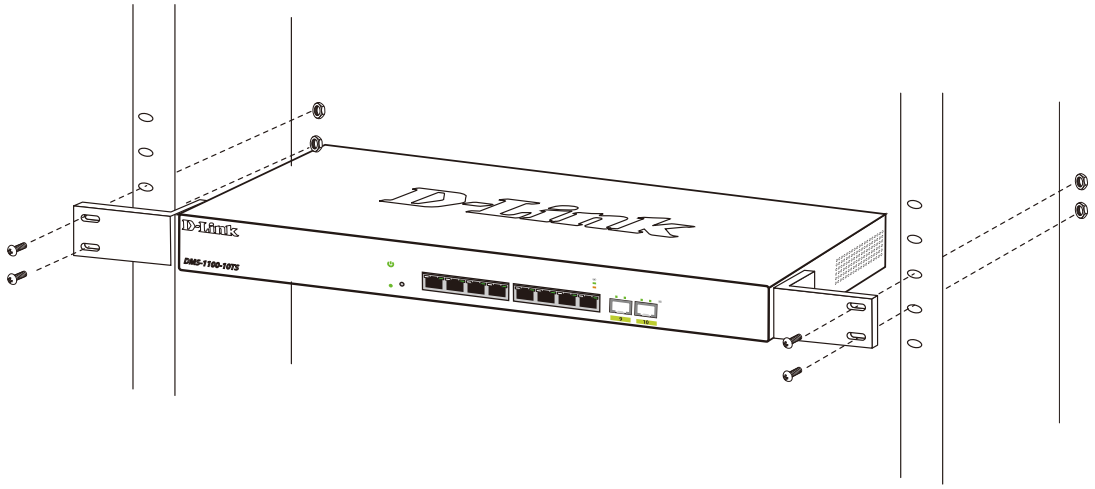


図 2-3　スイッチのラックへの設置

電源抜け防止器具の装着

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

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

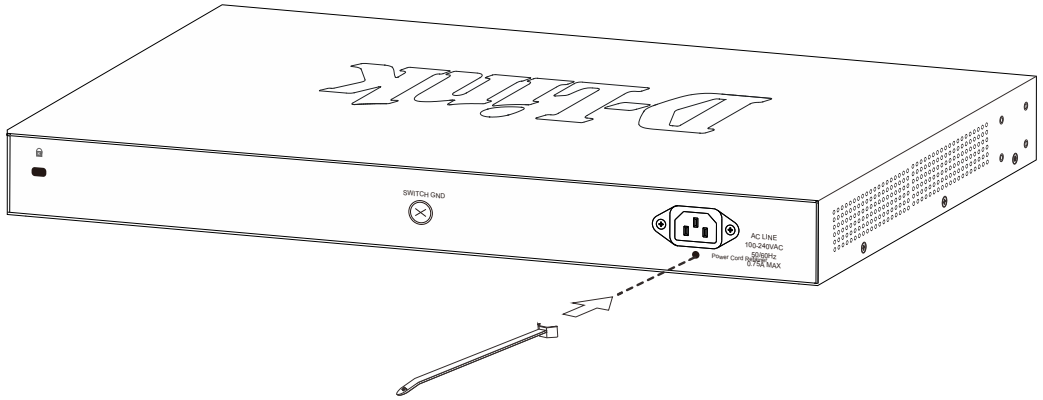


図 2-4　タイラップの挿し込み

2. AC 電源コードをスイッチの電源プラグに挿し込みます。

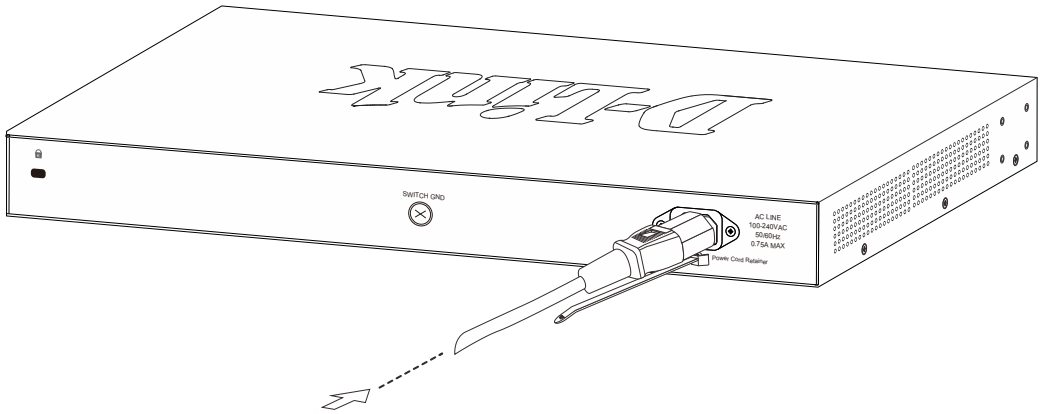


図 2-5　電源コード挿し込み

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

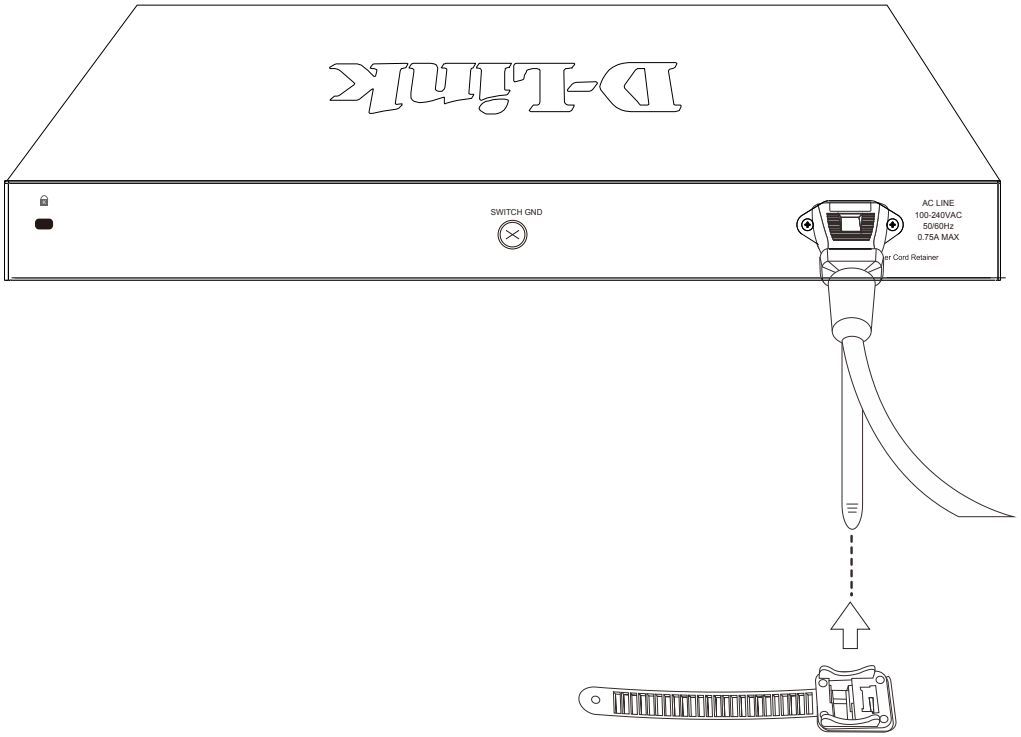


図 2-6　リテイナー（固定具）のスライド

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

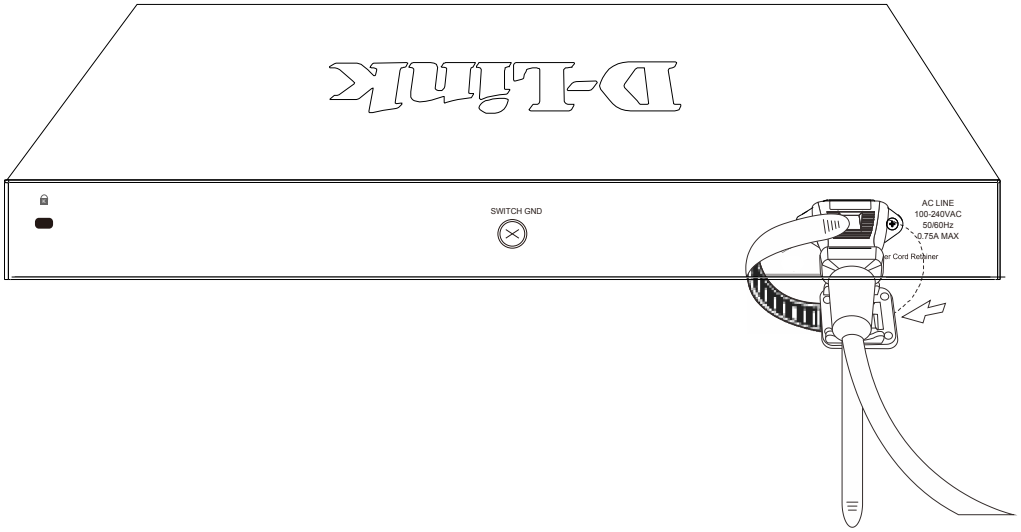


図 2-7　リテイナーの巻き付け、固定

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

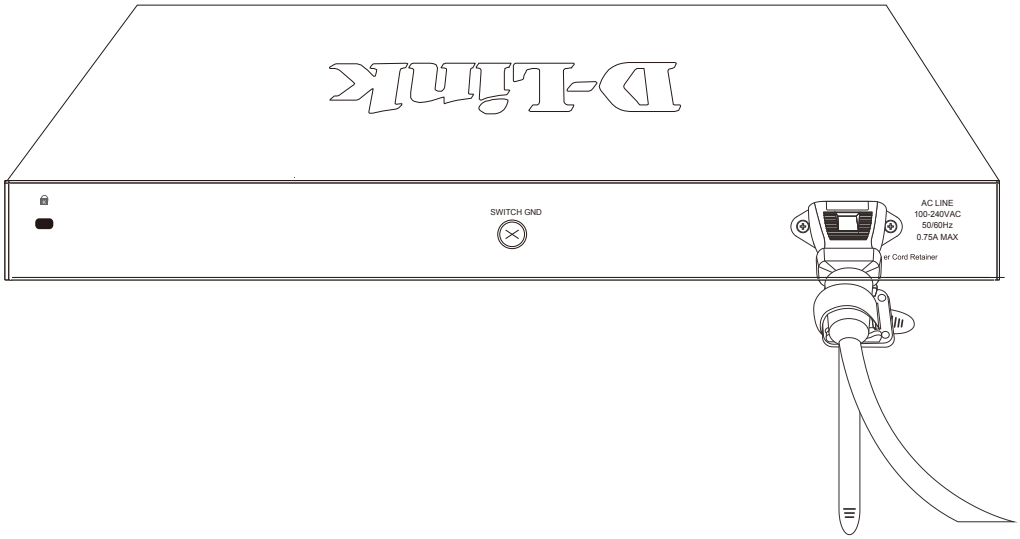


図 2-8　電源抜け防止器具の固定確認

スイッチの接地

本スイッチを接地する方法について説明します。

注意 スイッチの電源をオンにする前に、本手順を完了する必要があります。

接地に必要なツールと機器

- 接地ネジ（M4x6mm のパンヘッドネジ）1 個
- リング型ラグ端子付接地線（同梱されていません）
- スクリュードライバ（同梱されていません）

注意 接地線は国の設置必要条件に従ったサイズにする必要があります。商用に利用可能な 6 ～ 12AWG の範囲から適した接地線の使用をお勧めします。また、ケーブル長は適切な接地設備にスイッチの距離に従います。

以下の手順でスイッチを保安用接地に接続します。

1. システムの電源がオフであることを確認します。

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

3. 接地ネジ穴に接地端子を挿入します。

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

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

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

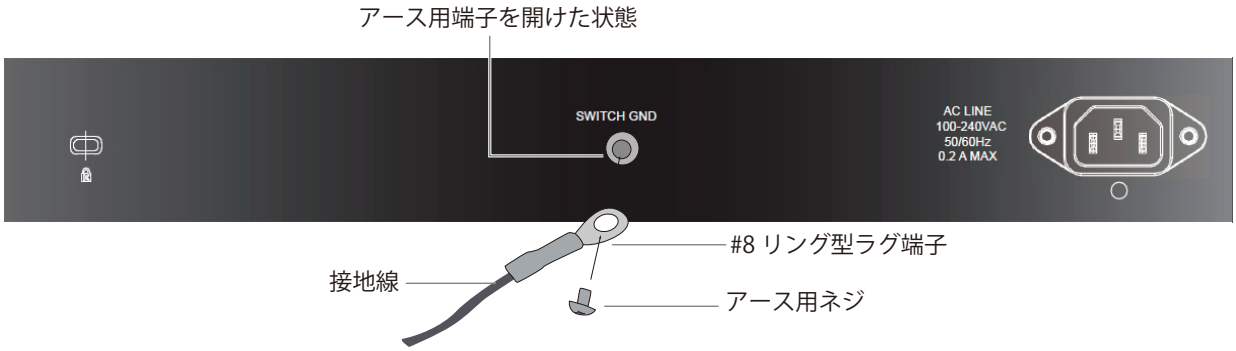


図 2-9　スイッチへのラグ端子の接続

電源の投入

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

第 3 章　スイッチの接続

- エンドノードと接続する
- ハブまたはスイッチと接続する
- バックボーンまたはサーバと接続する

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

「エンドノード」とは本スイッチと接続するネットワーク機器の一般的な呼称です。パソコン、ノート PC、アクセスポイント、プリントサーバ、VoIP 電話機などが該当します。各エンドノードは「10/100/1000Mbps/2.5Gbps」RJ45 ネットワークポートを有している必要があります。通常エンドノードはスタンダードなツイストペア UTP/STP ネットワークケーブルを使ってスイッチと接続されます。接続が成功すると、対応ポートの LED がポートでのネットワーク動作に従い点灯 / 点滅します。

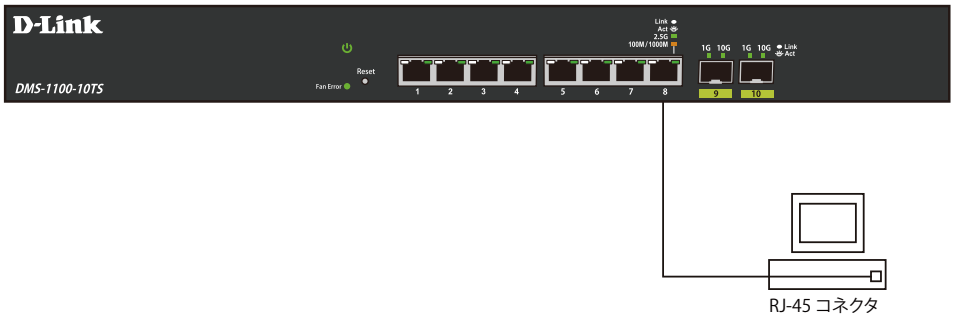


図 3-1　エンドノードと接続した図

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 は緑または橙に点灯します。データの送受信中は点滅します。

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- カテゴリ 3 以上の UTP/STP 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/STP ケーブル：100BASE-TX ハブまたはスイッチと接続する。
- エンハンスドカテゴリ 5 以上の UTP ケーブル：1000/2.5GBASE-T スイッチと接続する。
- 光ファイバケーブル : SFP+ ポート経由で光ファイバをサポートするスイッチにアップリンクする。

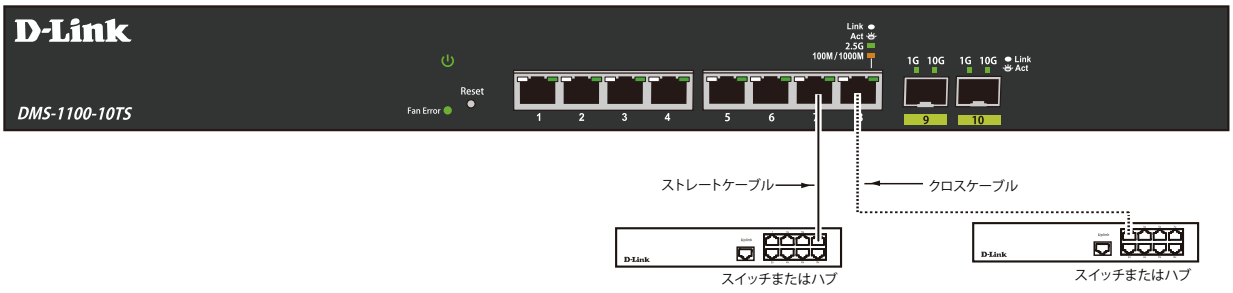


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

SFP+ ポートと 1000BASE-T ポートは、ネットワークバックボーンやサーバとのアップリンク接続に適しています。RJ-45 ポートは、全二重モード時において 10/100/1000Mbps/2.5Gbps の速度を提供し、SFP+ ポートは、全二重モード時において 1000Mbps または 10Gbps の速度を提供します。

ギガビットイーサネットポートとの接続はポートのタイプによって光ファイバケーブルまたはエンハンスドカテゴリ 5 ケーブルを使用します。正しくリンクが確立すると Link LED が点灯します。

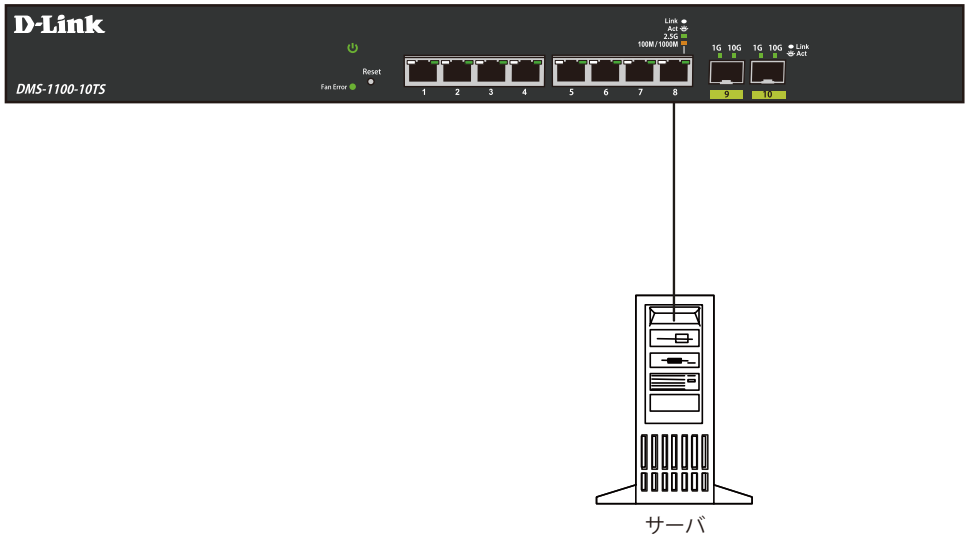


図 3-3　サーバ、PC、スイッチとのアップリンク接続図

第 4 章　Web ベースのスイッチ管理

- Web ベースの管理について
- Web マネージャへのログイン
- Smart Wizard 設定
- Web マネージャの画面構成
- Web マネージャのメニュー構成
- Device Information（デバイス情報）
- Save（Save メニュー）
- Tools（Tools メニュー）

Web ベースの管理について

DMS-1100 シリーズでは、スイッチの前面パネル上のいずれかのポートと PC のイーサネットポートを接続することで、Web ベースの管理が可能です。

スイッチ固有の IP アドレスを使用して、Web ベース管理や SNMP ネットワークマネージャによる通信を行います。管理 PC はスイッチと同じサブネット内に配置される必要があります。スイッチの同時ログインユーザ数は最大 1 ユーザ（異なるブラウザを使用した場合は最大 4 ユーザ）です。

サポートされるブラウザ

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

ブラウザの仕様により互換性が確保されない場合があります。

Web マネージャへのログイン

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

図 4-1　URL の入力

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

【例】スイッチの IP アドレスが 10.90.90.90 の場合：

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

3. ユーザ認証画面で、パスワードを入力し、「OK」をクリックします。

図 4-2　パスワード入力画面

補足　パスワードの初期値は「admin」です。

補足 「Language」で表示言語を選択することができます。

4. スマートウィザード画面が表示されます。

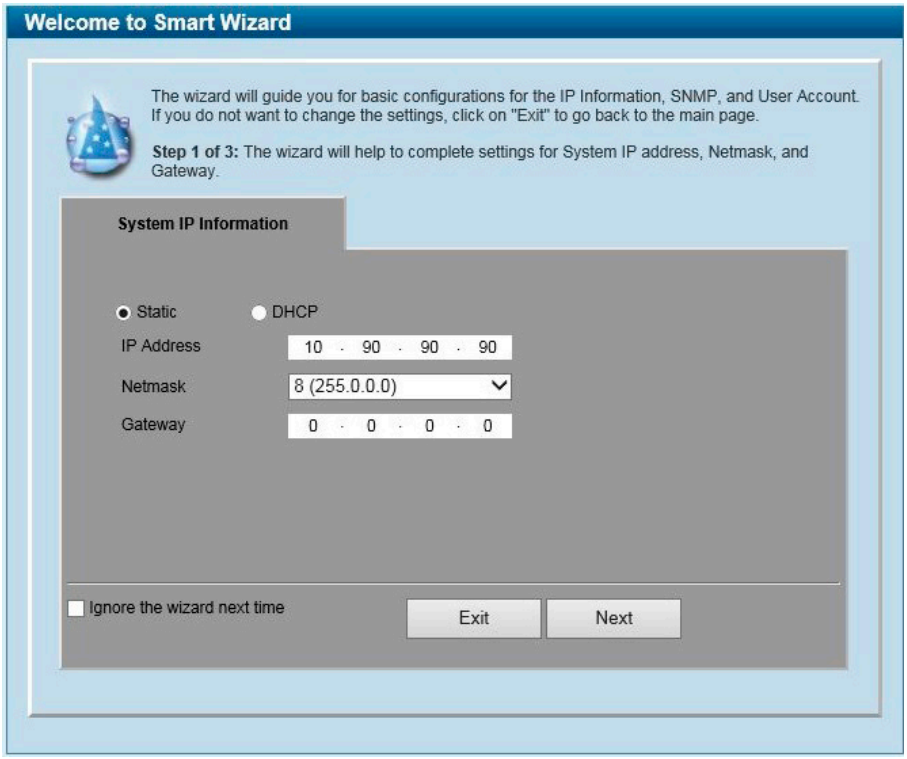


図 4-3　Smart Wizard 画面

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

5. ウィザードを使用しない場合は、「Exit」をクリックします。また、次回ログイン以降ウィザードをスキップする場合は「Ignore the wizard next time.」にチェックを入れてください。

6. 以下の Web マネージャのメイン画面が表示されます。

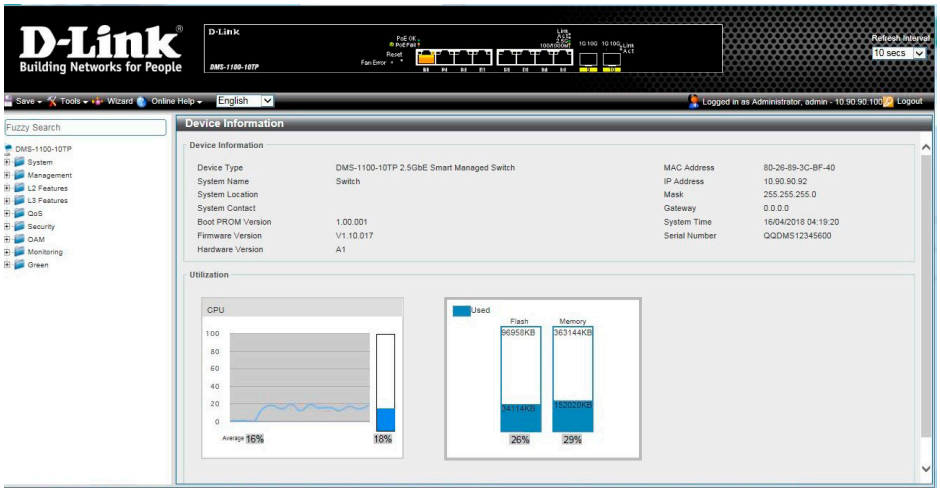


図 4-4　Web マネージャメイン画面

Smart Wizard 設定

「Smart Wizard」で、基本的なシステム構成 (IP アドレス、パスワード、SNMP) を設定します。

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

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

1. IP アドレスの設定を行います。

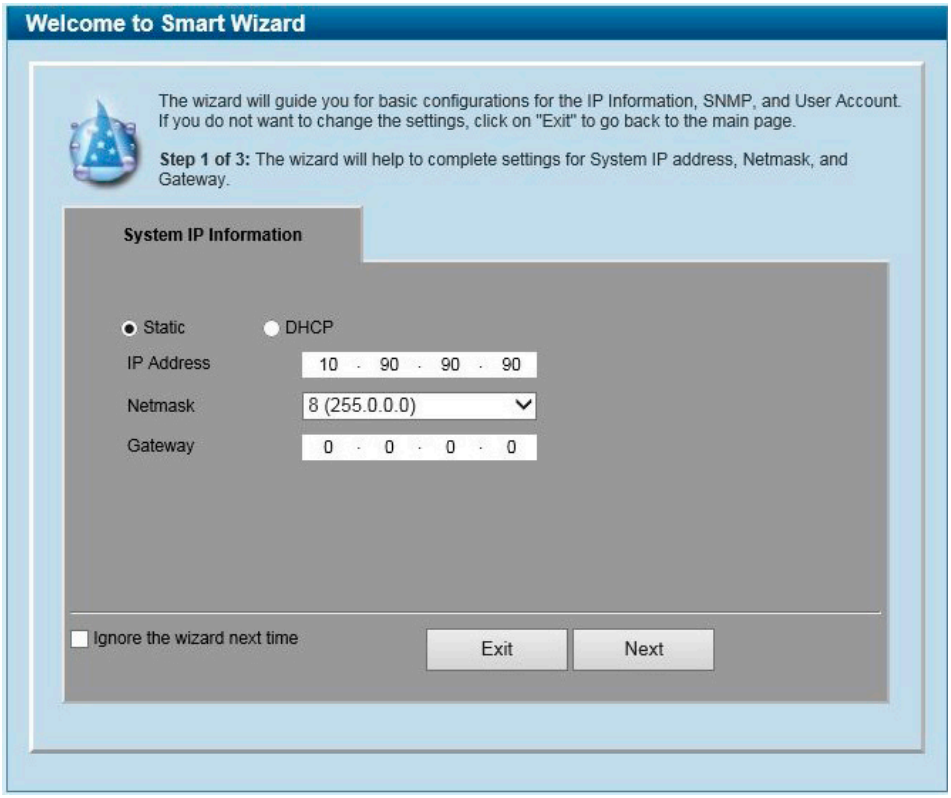


図 4-5　IP Information 設定画面

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

補足 Smart Wizard では、IPv4 アドレスのみ設定可能です。

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

2. SNMP の設定を行います。

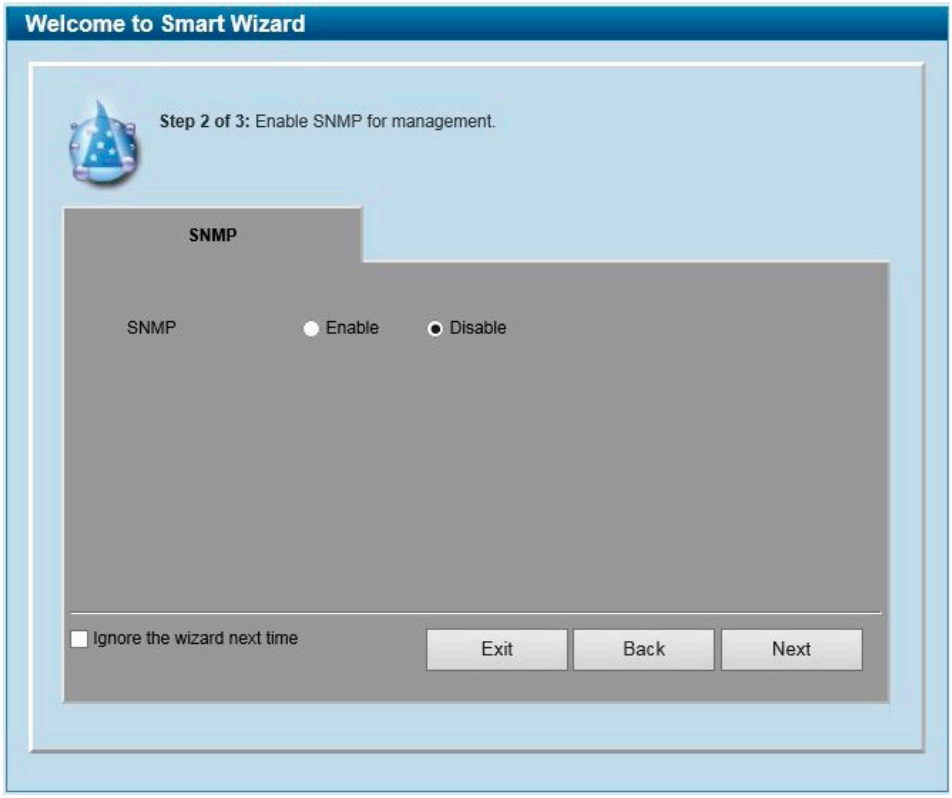


図 4-6　SNMP 設定画面

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

3. アカウントを追加します。

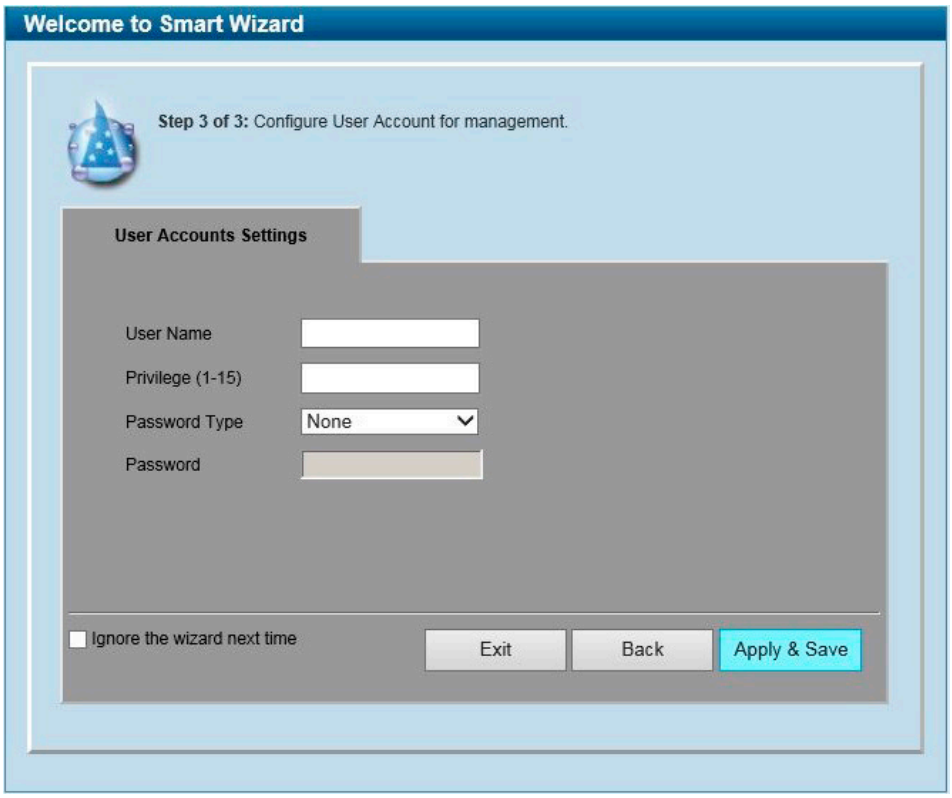


図 4-7　Password 設定画面

1. 「User Name」欄に新しいユーザ名を入力します。
2. 「Privilege 」欄でアクセス権限を指定します。詳細は第 6 章の「User Accounts Settings（ユーザアカウント設定）」をご確認ください。
3. 「Password Type」欄でパスワードの種類を選択し、「Plain Text」または「Encrypted」を選択した場合は「Password」欄にパスワードを入力します。

4. 「Apply & Save」をクリックします。

   Web マネージャ画面が表示されます。

補足 IP アドレスを変更し「Apply & Save」をクリックした場合は、以下のメッセージが表示されます。「OK」をクリックすると、現在の PC とスイッチの接続が切断されます。再度ログインする際は、ご使用のコンピュータをスイッチと同じサブネットに設定の上、Web ブラウザに新しい IP アドレスを入力して接続してください。

図 4-8　確認画面

Web マネージャの画面構成

Web マネージャでは、スイッチの設定を行ったり、パフォーマンス状況やシステム状況を参照することができます。

Web マネージャのメイン画面について

Web マネージャのメイン画面は 4 つのエリアで構成されています。

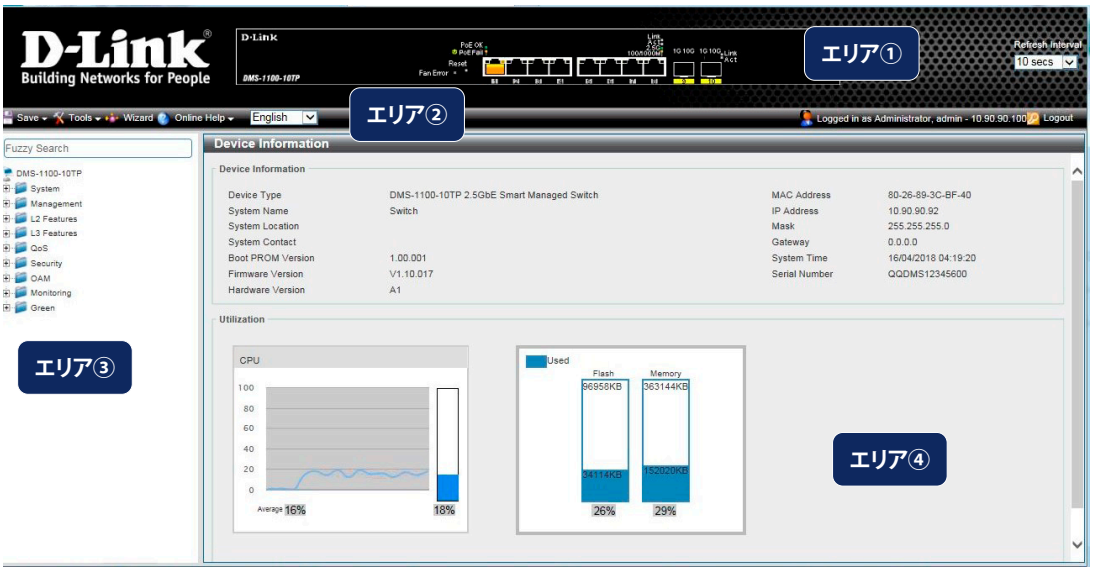


図 4-9　Web マネージャのメインページ

エリア	機能
エリア①	本エリアではスイッチの前面パネルの現在の状態がグラフィカル表示されます。スイッチのポート、拡張モジュールが表示されます。「D-Link」ロゴをクリックすると D-Link Web サイト（英語）へ移動します。
エリア②	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、設定の初期化などを行う「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	設定項目のメニューツリーを表示します。サブフォルダには上位フォルダに関連するカテゴリの詳細情報や設定項目が表示されます。
エリア④	選択したスイッチ情報の表示と設定を行うことができます。

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

注意 「Logout」ボタンをクリックせずにブラウザを閉じた場合、セッションは残ったままとなります。

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

Web マネージャのメニュー構成

Web マネージャで設定可能な機能を以下に説明します。

メインメニュー	サブメニュー	説明
Device Information（デバイス情報）		スイッチの基本的な情報を表示します。
Save	Save Configuration （コンフィグレーションの保存）	スイッチのコンフィグレーションを保存します。
Tools	Firmware Information （ファームウェア情報）	ファームウェアの情報を表示します。
	Configuration Information （コンフィグレーション情報）	コンフィグレーションの情報を表示します。
	Firmware Upgrade & Backup （ファームウェアアップグレード&バックアップ）	HTTP/TFTP プロトコルを使用してファームウェアアップグレード / バックアップを行います。
	Configuration Restore & Backup （コンフィグレーションリストア&バックアップ）	HTTP/TFTP プロトコルを使用してコンフィグレーションリストア / バックアップを行います。
	Log Backup （ログファイルのバックアップ）	HTTP/TFTP プロトコルを使用してログファイルのバックアップを行います。
	Ping	ICMP Echo パケットを送信し、特定の IP アドレスに対して疎通確認を行います。
	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。
	Reboot System（システム再起動）	スイッチの再起動を行います。
System	System Information（システム情報）	システム情報の設定を行います。
	Port Configuration（ポート設定）	スイッチポートの詳細設定などを行います。
	PoE（PoE の管理）（DMS-1100-10TP）	PoE 機能の設定を行います。（DMS-1100-10TP のみ）
	System Log（ システムログ構成）	システムログの設定及び表示を行います。
	Time and SNTP（時刻設定）	スイッチの時刻を設定します。
	Time Range（タイムレンジ設定）	スイッチの PD アライブ機能などで使用するスケジュールを定義します。
Management	User Accounts Settings（ユーザアカウント設定）	ユーザパスワードとアクセス権限を含むユーザアカウント設定を行います。
	Password Encryption（パスワード暗号化）	コンフィグレーションのパスワード暗号化の設定を行います。
	SNMP Settings（SNMP 設定）	SNMP の設定を行います。本スイッチシリーズは、SNMP v1、v2c、および v3 をサポートしています。
	Web（Web 設定）	スイッチの Web ポート番号の設定を行います。
	Session Timeout （セッションタイムアウト）	Web セッションのタイムアウトの設定を行います。
	D-Link Discovery Protocol Settings （D-Link ディスカバリプロトコル設定）	D-Link ディスカバリプロトコル（DDP）の設定を行います。
L2 Features	FDB（FDB 設定）	FDB（Forwarding DataBase）フォワーディングデータベースの設定を行います。
	VLAN（VLAN 設定）	802.1Q VLAN、Asymmetric VLAN、VLAN インタフェース、自動サーベイランス VLAN、音声 VLAN の設定を行います。
	STP（スパニングツリー設定）	スパニングツリープロトコル（STP）設定を行います。3 つのバージョンの STP（8802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。
	ERPS (G.8032) （イーサネットリングプロテクション設定）	「Ethernet Ring Protection Switching」(ERPS) 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（LBD）機能の設定を行います。
	Link Aggregation （リンクアグリゲーション）	Link Aggregation（リンクアグリゲーション / ポートトランキング）の設定を行います。
	L2 Multicast Control （L2 マルチキャストコントロール）	IGMP Snooping 及び MLD Snooping の設定を行います。
	LLDP	Link Layer Discovery Protocol（LLDP）の設定を行います。
L3 Features	IPv4 Interface	IPv4 アドレスのインタフェースの設定を行います。
	IPv4 Default Gateway	IPv4 デフォルトゲートウェイの設定を行います。
	IPv6 Interface	IPv6 アドレスのインタフェースの設定を行います。
	IPv6 Default Gateway	IPv6 デフォルトゲートウェイの設定を行います。

メインメニュー	サブメニュー	説明
QoS	Port Default CoS（ポートデフォルト CoS）	ポートのデフォルト CoS の設定を行います。
	Port Scheduler Method（ポートスケジューリング方式）	ポートのスケジューリング方式の設定を行います。
	Queue Settings（キュー設定）	キューの設定を行います。
	CoS to Queue Mapping（CoS/ キューマッピング）	CoS とキューのマッピング設定を行います。
	Port Rate Limiting（ポートレート制限）	ポートレート制限の設定を行います。
Security	Safeguard Engine（セーフガードエンジン）	セーフガードエンジンは、攻撃中に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。
	Trusted Host（トラストホスト）	トラストホストの設定を行います。
	Traffic Segmentation Settings（トラフィックセグメンテーション設定）	ポート間のトラフィック制御の設定を行います。
	Storm Control Settings（ストームコントロール設定）	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）	各 DoS 攻撃に対して防御設定を行います。
	SSL（Secure Socket Layer）	Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。
OAM	Cable Diagnostics（ケーブル診断機能）	スイッチに接続する UTP ケーブルの詳細について表示します。
Monitoring	Statistics（統計情報）	スイッチの統計情報を表示します。
	Mirror Settings（ミラー設定）	ミラーリング機能の設定を行います。特定ポートの送受信フレームを、他のポートにコピーすることができます。
Green	Power Saving（省電力）	スイッチの省電力機能を設定します。
	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おり、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。

Device Information（デバイス情報）

本画面は、ログインを行うと自動的に表示される画面で、スイッチの主な設定情報を確認できます。本画面に戻るためには「DMS-1100-10TS/10TP」フォルダをクリックします。

Device Information（デバイス情報）

ハードウェア情報や IP アドレス、ファームウェア情報など、スイッチの基本的な情報が表示されます。

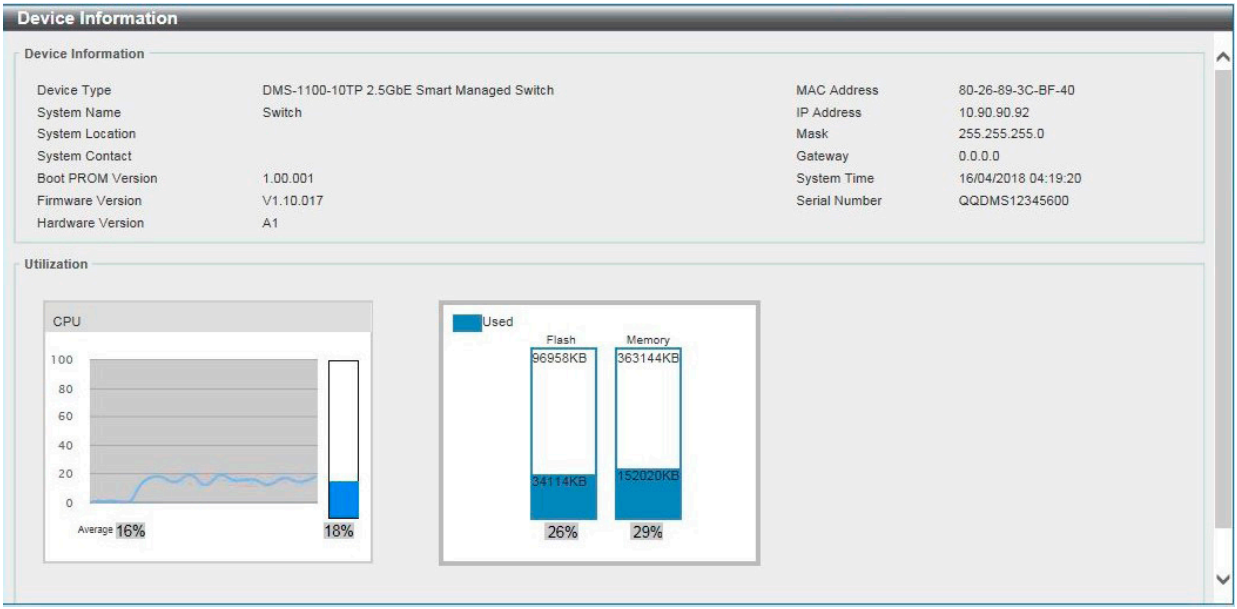


図 4-1　Device Information 画面

本画面には以下の項目があります。

項目	説明
Device Information	
Device Type	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	ユーザが定義したシステムの設置場所を表示します。
System Contact	ユーザが定義した担当者名を表示します。
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	システム時刻を表示します。
Serial Number	デバイスのシリアル番号を表示します。
Utilization	
CPU	CPU の使用率を表示します。
Flash	Flash の使用率を表示します。
Memory	Memory の使用率を表示します。

Save（Save メニュー）

Save メニューではコンフィグレーションの保存を行います。

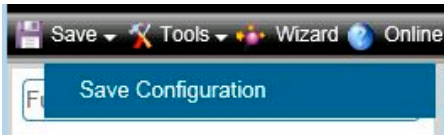


図 4-1　Save Configuration メニュー

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。

図 4-1　Save Configuration 画面

本画面には以下の項目があります。

項目	説明
Destination	コンフィグレーションを保存する宛先を指定します。
startup-config	本項目にチェックを入れると、現在のコンフィグレーションファイルに設定が保存されます。

「Apply」ボタンをクリックし、コンフィグレーションを保存します。

重要 : 設定保存後に電源を切る場合の注意

UI での設定保存を実行後、スイッチ内部での書き込み処理に時間がかかる場合があります。UI での設定保存実行後、必ず 1 分以上待ってから、電源を抜くようにしてください。

Tools（Tools メニュー）

ツールメニューでは、リセットや再起動、コンフィグレーションのバックアップ＆リストア、ファームウェアバックアップ＆アップグレードといった、システムのグローバル機能を提供します。

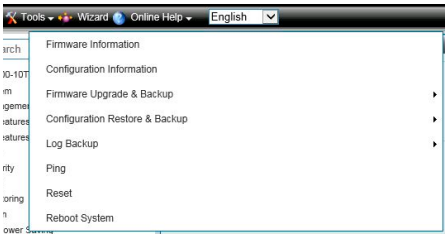


図 4-1　Tools メニュー

Firmware Information（ファームウェア情報）

ファームウェアイメージの情報を表示します。現在のブートアップイメージと、次回起動時のブートアップイメージを確認することができます。

Tools > Firmware Information をクリックし、設定画面を表示します。

図 4-2　Firmware Information 画面

「Boot UP」をクリックして、次回起動時のブートアップイメージを指定します。

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

コンフィグレーションの情報を表示します。現在のコンフィグレーションと、次回起動時のコンフィグレーションを確認することができます。

Tools > Configuration Information をクリックし、設定画面を表示します。

図 4-3　Configration Information 画面

「Boot UP」をクリックして、次回起動時のブートアップコンフィグレーションを指定します。

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

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 を使用してスイッチの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 4-4　Firmware Upgrade from HTTP 画面

本画面には以下の項目があります。

項目	説明
Source URL	「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を指定します。
Destination URL	アップグレード先のイメージ ID 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 新しいファームウェアで起動するには、**Tools > Firmware Information** で新しいイメージファイルをブートイメージとして指定し、システムを再起動する必要があります。

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 を使用してスイッチの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 4-5　Firmware Upgrade from TFTP 画面

本画面には以下の項目があります。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source URL	ファームウェアファイルが保存されている TFTP サーバの場所（パス / ファイル名）を指定します。
Destination URL	アップグレード先のイメージ ID 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 新しいファームウェアで起動するには、**Tools > Firmware Information** で新しいイメージファイルをブートイメージとして指定し、システムを再起動する必要があります。

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

HTTP サーバを使用して、スイッチからローカル PC 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 HTTP をクリックし、設定画面を表示します。

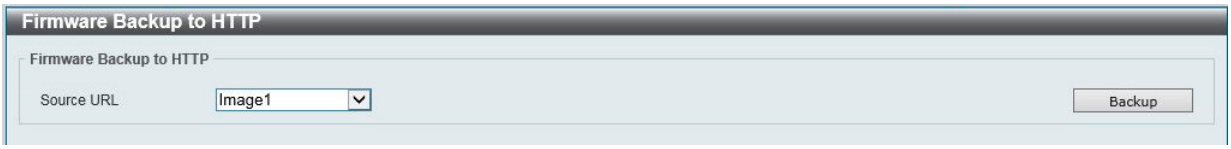


図 4-6　Firmware Backup to HTTP 画面

本画面には以下の項目があります。

項目	説明
Source File	バックアップ対象のイメージファイルを選択します。 選択肢：「image 1」「image 2」

「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）

スイッチから 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 4-7　Firmware Backup to TFTP 画面

本画面には以下の項目があります。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	バックアップ対象のイメージファイルを選択します。 選択肢：「image 1」「image 2」
Destination File	TFTP サーバ上のファームウェアファイル保存先（パス / ファイル名）を指定します。64 文字までで指定できます。

「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 4-8　Configuration Restore from HTTP 画面

本画面には以下の項目があります。

項目	説明
Source URL	「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を指定します。
Destination	コンフィグレーションファイルのリストア先を指定します。 選択肢：「Config 1」「Config 2」
startup-config	本項目にチェックを入れると、現在のコンフィグ ID の startup-config がリストアされます。

「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。リストアは startup-config に適用されます。

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。

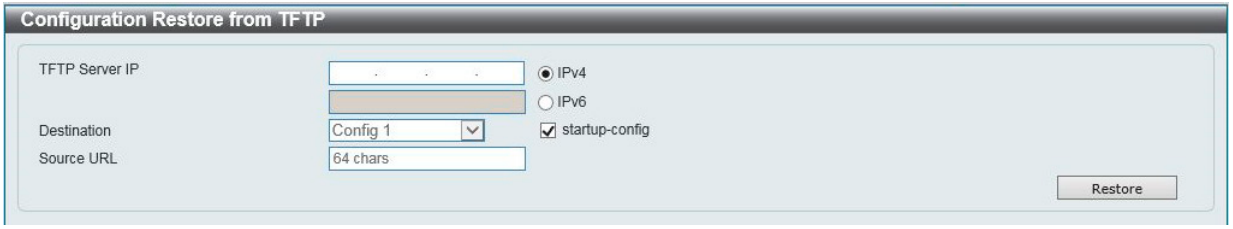


図 4-9　Configuration Restore from TFTP 画面

本画面には以下の項目があります。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Destination	コンフィグレーションファイルのリストア先を指定します。 選択肢：「Config 1」「Config 2」
startup-config	本項目にチェックを入れると、現在のコンフィグ ID の startup-config がリストアされます。
Source URL	TFTP サーバ上のコンフィグレーションファイル保存場所（パス / ファイル名）を指定します。64 文字まで指定します。

「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。リストアは startup-config に適用されます。

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 サーバを使用してスイッチからローカル PC に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 4-10　Configuration Backup to HTTP 画面

本画面には以下の項目があります。

項目	説明
Source	バックアップ対象のコンフィグレーションファイルを指定します。 選択肢：「Config 1」「Config 2」
startup-config	本項目にチェックを入れると、現在のコンフィグレーションがバックアップされます。

「Backup」ボタンをクリックして、バックアップを開始します。

Configuration 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）

スイッチから TFTP サーバ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 TFTP をクリックし、設定画面を表示します。

図 4-11　Configuration Backup to TFTP 画面

本画面には以下の項目があります。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source	バックアップ対象のコンフィグレーションファイルを指定します。 選択肢：「Config 1」「Config 2」
startup-config	本項目にチェックを入れると、現在のコンフィグレーションがバックアップされます。
Destination URL	TFTP サーバ上のコンフィグレーションファイル保存先（パス / ファイル名）を指定します。64 文字まで指定します。

「Backup」ボタンをクリックして、バックアップを開始します。

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 サーバを使用してスイッチからローカル 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 4-12　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）

スイッチから 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 4-13　Log Backup to TFTP 画面

本画面には以下の項目があります。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Destination URL	TFTP サーバ上のログファイル保存先を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックして、バックアップを開始します。

Ping（Ping 送信）

コンピュータやデバイスに対して Ping を送信し、疎通確認を行います。

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

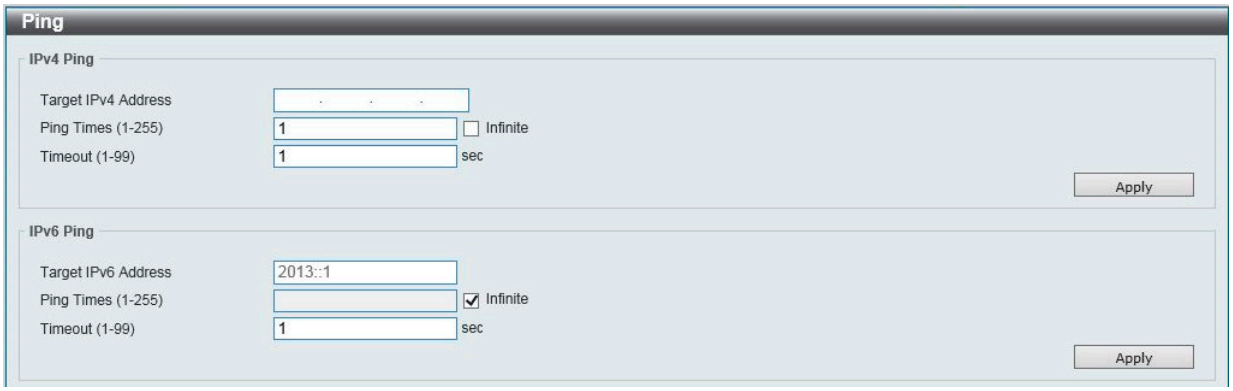


図 4-14　Ping 画面

本画面には以下の項目があります。

IPv4 Ping（IPv4 Ping 送信）

項目	説明
Target IPv4 Address	Ping 送信先の IPv4 アドレスを入力します。

項目	説明
Ping Times (1-255)	Ping の送信回数を指定します。「Infinite」にチェックを入れると、「Stop」ボタンをクリックするまで送信し続けます。 設定可能範囲：1-255
Timeout (1-99)	リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。 設定可能範囲：1-99（秒）

「Start」ボタンをクリックし、Traceroute プログラムを開始します。

IPv6 Ping（IPv6 Ping 送信）

項目	説明
Target IPv6 Address	Ping 送信先の IPv6 アドレスを入力します。
Ping Times (1-255)	Ping の送信回数を指定します。「Infinite」にチェックを入れると、「Stop」ボタンをクリックするまで送信し続けます。 設定可能範囲：1-255
Timeout (1-99)	リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。 設定可能範囲：1-99（秒）

「Apply」ボタンをクリックし、Ping 送信を開始します。

以下の結果画面が表示されます。

図 4-15　Ping Result（IPv4）画面

Ping 送信を停止するには、「Stop」ボタンをクリックします。
前の画面に戻るには、「Back」ボタンをクリックします。

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 4-16　Reset 画面

本画面には以下の項目があります。

項目	説明
The Switch will be reset to its factory defaults except IP address,and then will save,reboot.	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。 （IP アドレスを除く）
The Switch will be reset to its factory defaults including IP address.	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。 （IP アドレスを含む）

「Apply」ボタンをクリックして、リセット処理を開始します。

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 4-17　Reboot System 画面

本画面には以下の項目があります。

項目	説明
Do you want to save the settings ?	• Yes - スイッチは再起動する前に現在の設定を保存します。 • No - スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使用されます。
Destination	設定保存先のコンフィグレーションファイルを選択します。 選択肢：「Config 1」「Config 2」
startup-config	本項目にチェックを入れると、再起動時の startup-config ファイルに設定が保存されます。

「Reboot」をクリックして、再起動を開始します。

第 5 章　System（システム設定）

本メニューでは、ポートやシステムログ、時刻設定などのシステムに関する設定を行います。

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
System Information（システム情報 ）	システム情報の設定を行います。
Port Configuration（ポート設定）	スイッチポートの詳細設定などを行います。
PoE（PoE の管理）（DMS-1100-10TP）	PoE 機能の設定を行います。（DMS-1100-10TP のみ）
System Log（システムログ構成）	システムログの設定及び表示を行います。
Time and SNTP（時刻設定）	スイッチの時刻を設定します。
Time Range（タイムレンジ設定）	スイッチの PD アライブ機能などで使用するスケジュールを定義します。

System Information（システム情報 ）

スイッチのシステム情報の設定を行います。

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

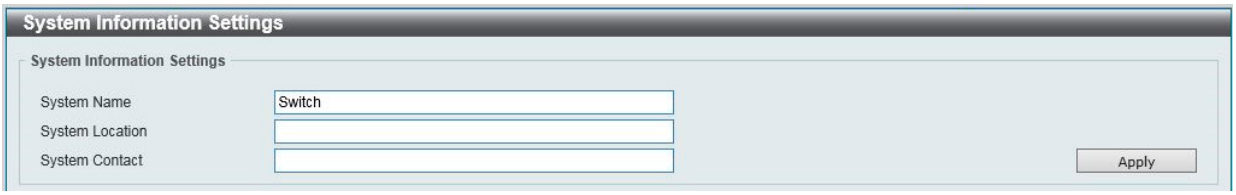


図 5-18　System Information 画面

本画面には次の項目があります。

項目	説明
System Information Settings	
System Name	システム名を設定します。
System Location	システムが現在動作している場所を定義します。（半角英数字 160 文字以内）
System Contact	スイッチの管理者情報を入力します。

「Apply」ボタンをクリックし、設定を適用します。

Port Configuration（ポート設定）

Port Settings（スイッチのポート設定）

スイッチポートの詳細を設定します。

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

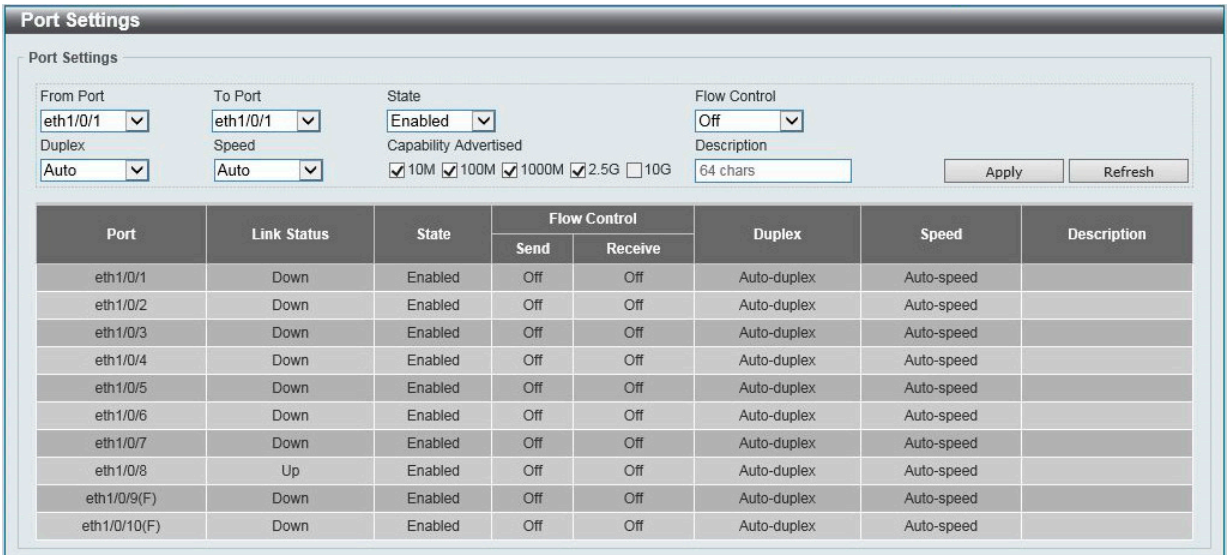


図 5-19　Port Settings 画面

本画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート / ポート範囲を指定します。
State	物理ポートを「Enabled」（有効）/「Disabled」（無効）に設定します。
Flow Control	フロー制御を「Enabled」（有効）/「Disabled」（無効）に設定します。Full-Duplex では 802.3x フローコントロールを、Half-Duplex ではバックプレッシャーによる制御を自動で行います。
Duplex	接続モードの選択を行います。 選択肢：「Auto（自動）」「Full（全二重通信）」
Speed	ポートの速度を選択します。これ以外の設定の場合、両端のポートでリンクダウン状態となります。 選択肢：「Auto（自動）」「10M」「100M」「1000M」「2.5G」「10G」
Capability Advertised	「Speed」が「Auto」に設定されている場合、オートネゴシエーションの間、これらの Capability を通知します。ポート 1-8 を指定した場合、「10G」は選択できません。ポート 9-10 を指定した場合、「1000M」「10G」が選択できます。
Description	指定したポートの説明を入力します。（最大 64 文字）

「Apply」ボタンをクリックし、設定を適用します。
「Refresh」ボタンをクリックして、本画面を更新します。

Port Status（ポートステータス）

ポートの状態、設定について表示します。各ポートの状態、MAC アドレス、VLAN、フローコントロール設定、Duplex 設定、速度を確認することができます。

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

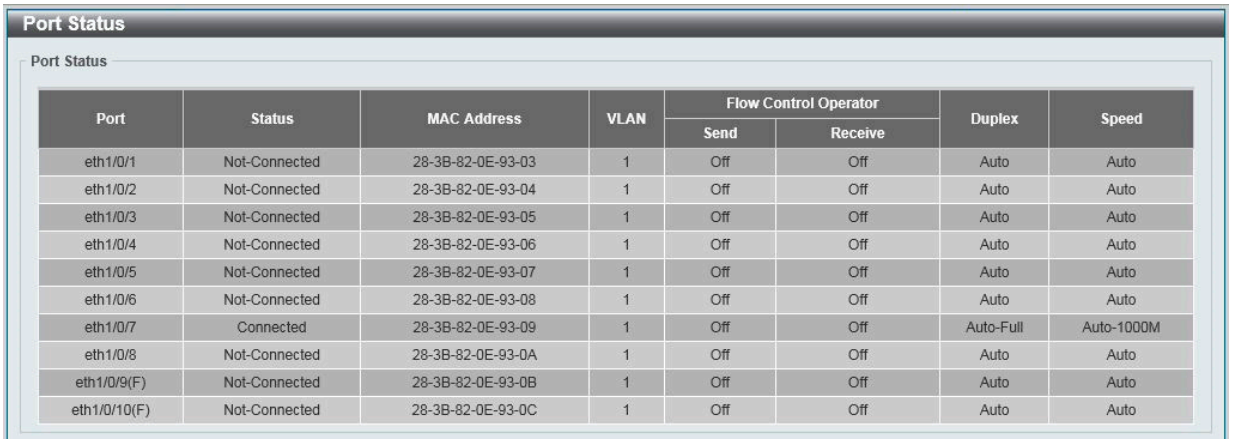


図 5-20　Port Status 画面

Error Disable Settings（エラーによるポートの無効）

ポートのエラー状態により Error Disable 状態になった場合に SNMP 通信を送信するかどうかを設定します。

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

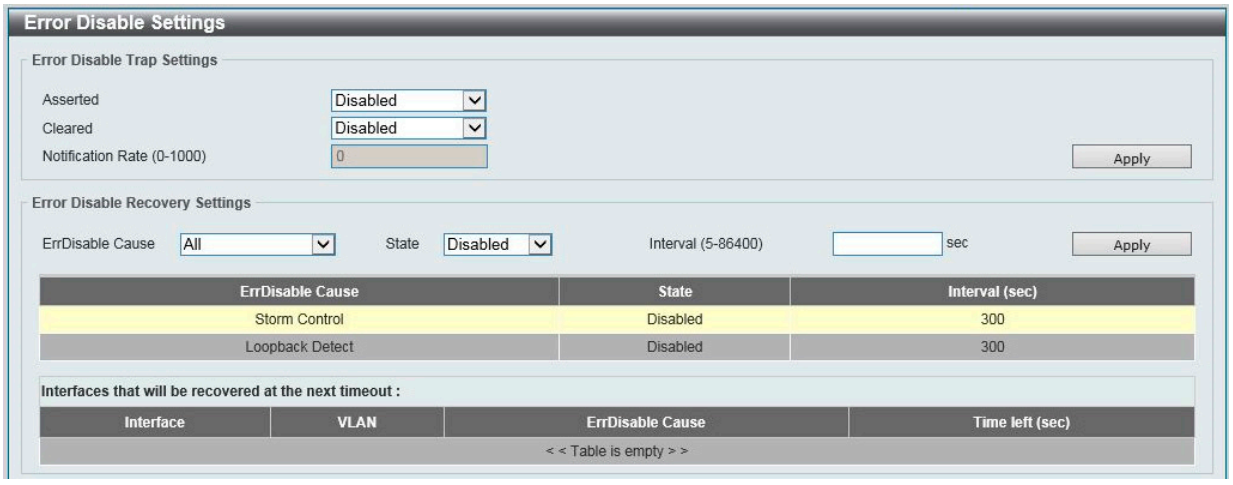


図 5-21　Error Disable Settings 画面

本画面には以下の項目があります。

Error Disable Trap Settings（エラー Disable トラップ設定）

項目	説明
Asserted	エラー Disable 状態になった際の通知送信を「Enabled」（有効）/「Disabled」（無効）に設定します。
Cleared	エラー Disable 状態から回復した際の通知送信を「Enabled」（有効）/「Disabled」（無効）に設定します。
Notification Rate	1 分あたりのトラップ数を入力します。指定したしきい値超えたパケットは破棄されます。 設定可能範囲：0-1000

「Apply」ボタンをクリックし、設定を適用します。

Error Disable Recovery Settings（エラー Disable リカバリ設定）

項目	説明
ErrDisable Cause	エラー Disable の原因を選択します。 選択肢：「All」「Storm」「Loopback Detect」
State	指定した原因によるエラー Disable ポートの自動リカバリ機能を「Enabled」（有効）/「Disabled」（無効）に設定します。
Interval	ポートリカバリ実行の間隔を指定します。 設定可能範囲：5-86400（秒）

「Apply」ボタンをクリックし、設定を適用します。

Jumbo Frame（ジャンボフレーム設定）

ジャンボフレームの設定と表示を行います。

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 5-22　Jumbo Frame 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	本設定を適用するポート / ポート範囲を指定します。
Maximum Receive Frame Size	スイッチのジャンボフレーム機能の最大値を指定します。 初期値：1536（バイト） 設定可能範囲：1518-9216（バイト）

「Apply」ボタンをクリックし、設定を適用します。

PoE（PoE の管理）（DMS-1100-10TP）

DMS-1100-10TP は IEEE の 802.3af と IEEE802.3at 規格の PoE 機能をサポートしています。ポート 1-8 は PoE 受電機器に 30W までの電力を供給することができます。DMS-1100-10TP は全ての D-Link 802.3af/at 対応デバイスと接続できます。アクセスポイントや IP カメラ、IP フォンなどへの電力供給が可能です。

IEEE 802.3af 定義による PSE 電力供給量：

クラス	用途	給電機器の出力電力	受電機器の最大電力
0	デフォルト	15.4W	0.44 ～ 12.95W
1	オプション	4.0W	0.44 ～ 3.84W
2	オプション	7.0W	3.84 ～ 6.49W
3	オプション	15.4W	6.49 ～ 12.95W
4	オプション	クラス 0 として処理	予備

IEEE 802.3at 定義による PSE 電力供給量：

クラス	用途	受電機器のクラス	給電機器の出力電力	受電機器の最大電力
0	デフォルト	デフォルト、Type1	15.4W	0.44 ～ 12.95W
1	オプション	Type1	4.0W	0.44 ～ 3.84W
2	オプション	Type1	7.0W	3.84 ～ 6.49W
3	オプション	Type1	15.4W	6.49 ～ 12.95W
4	オプション	Type2	30W	12.95 ～ 25.5W

PoE System（PoE システム設定）

現在の電力消費の表示と、レガシー PD 検出の設定を行います。

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

図 5-23　PoE System 画面

本画面には以下の項目があります。

項目	説明
Power Budget (W)	デバイスの最大電力供給量（ワット）を表示します。
Delivered (W)	現在の電力供給量（ワット）を表示します。
Legacy Support	レガシー PD シグナルの検出を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）

「Apply」ボタンをクリックし、設定を適用します。

注意　DMS-1100-10TP の PoE ネットワークへの接続時には、屋外設備への配線を行わないでください。

PoE Status（PoE ステータス）

各ポートの PoE ステータスを表示します。

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

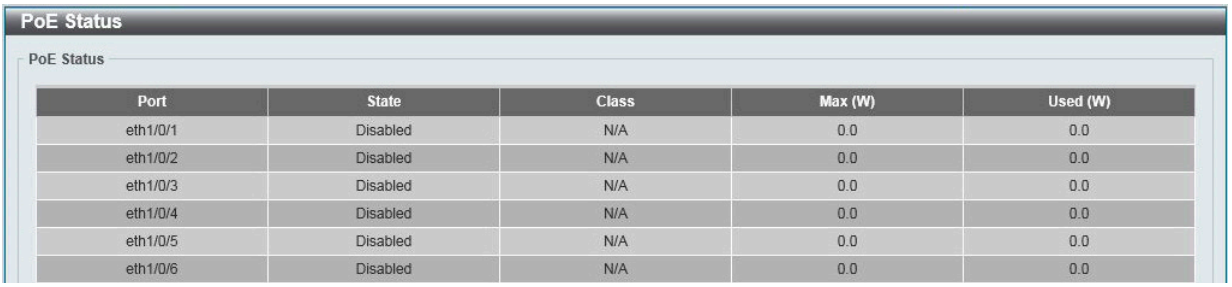


図 5-24　PoE Status 画面

注意　Class が「Legacy PD」と表示されている場合、802.3af 非対応のデバイス、レガシー PD として分類されます。

PoE Configuration（PoE ポート設定）

各ポートの PoE 設定を行います。

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

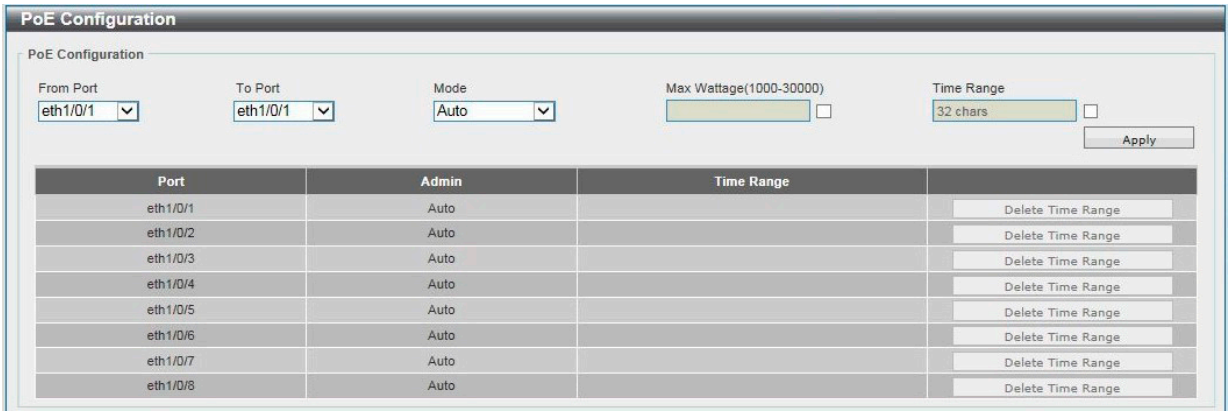


図 5-25　PoE Configuration 画面

本画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート / ポート範囲を指定します。
Mode	PoE ポートの電力管理モードを選択します。 選択肢：「Auto（自動）」「Never（無効）」
Max Wattage	「Mode」で「Auto」を選択した場合、本オプションを設定することができます。チェックボックスにチェックを入れ、自動検出 PD へ供給する最大電力数（W）を指定します。数値を指定しない場合、PD のクラスは供給可能な最大の電力で指定されます。 設定可能範囲：1000-30000（mW）
Time Range	タイムレンジ名を指定し、ポートの PoE 機能を有効にする時間を設定します。ポートは設定した時間内のみ給電を行います。

「Apply」ボタンをクリックすると設定が更新されます。
「Delete Time Range」ボタンをクリックし、指定したタイムレンジを削除します。

注意　DMS-1100-10TP では、ポート 1 ～ポート 8 までが IEEE 802.3at に準拠しています。PoE 供給可能合計値は 240W です。

PoE Measurement（PoE 測定）

PoE の測定情報を表示します。

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

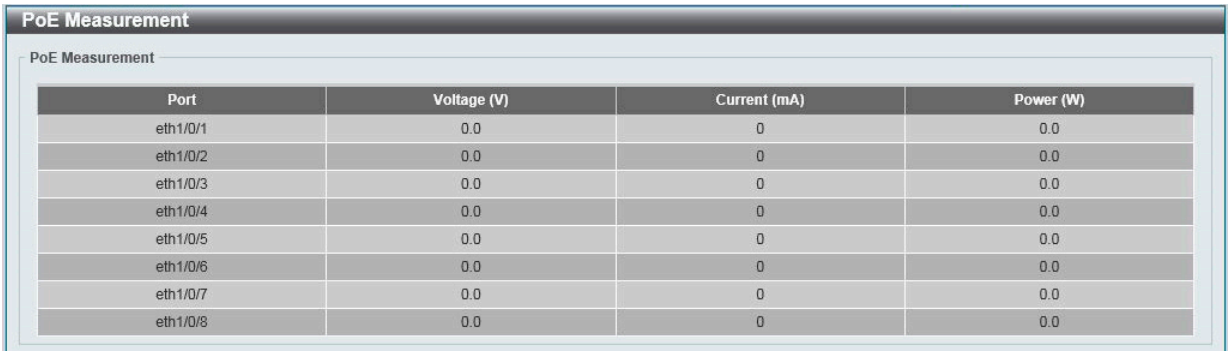


図 5-26　PoE Measurement 画面

PD Alive（PD アライブ設定）

PD アライブの表示、設定を行います。「PD アライブ」機能は Ping メカニズムを使用して、応答のない PD（受電機器）や停止した PD に対して解決を図ります。

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

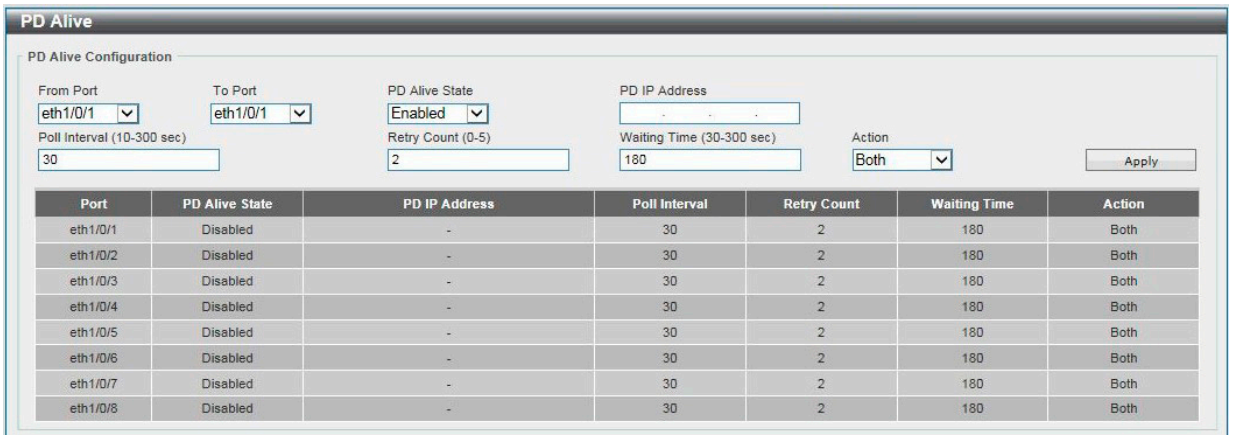


図 5-27　PD Alive 画面

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	PoE アライブ機能を有効 / 無効にします。
PD IP Address	PD の IPv4 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。指定の PD の状況を確認する Ping 送信間隔になります。 設定可能範囲：10-300（秒）
Retry Count	リトライカウント（再試行回数）を指定します。指定の PD からの応答がなかった際に Ping を再送信する回数を指定します。 設定可能範囲：0-5（回）
Waiting Time	待機時間を指定します。指定の PD が再起動から回復するまでスイッチが待つ時間を指定します。 設定可能範囲：30-300（秒）
Action	実行する動作を指定します。 • Reset - PoE ポートをリセットします。 • Notify - 管理者に通知するログとトラップを送信します。 • Both - 管理者に通知するログとトラップを送信し、PoE ポートをリセットします。

「Apply」ボタンをクリックし、設定を適用します。

System Log（システムログ構成）

System Log Settings（システムログ設定）

システムログ機能の設定を行います。

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。

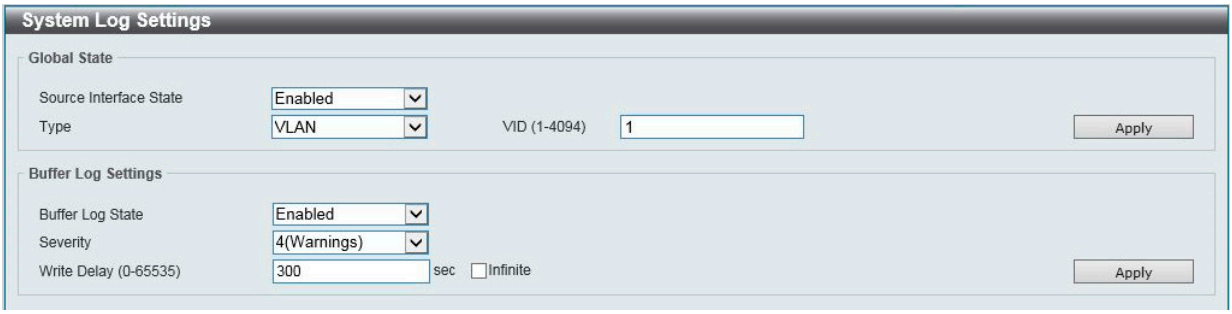


図 5-28　System Log Settings 画面

本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
Source Interface State	ソースインタフェースを「Enabled」（有効）/「Disabled」（無効）に設定します。
Type	インタフェースの種類を選択します。 初期値：VLAN
VID	VLAN ID を指定します。 設定可能範囲：1-4094

「Apply」ボタンをクリックし、設定を適用します。

Buffer Log Settings（バッファログ設定）

項目	説明
Buffer Log State	バッファログを「Enabled」（有効）/「Disabled」（無効）に設定します。
Severity	ログ出力される情報のレベルを選択します。 選択肢：「1：Emergencies」（緊急）、「2：Alerts」（警告）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（注意）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Write Delay	バッファログをフラッシュに書き込む間隔を設定します。 「Infinite」オプションにチェックを入れると、Write Delay（書き込み遅延）機能を無効にします。 初期値：300 設定可能範囲：0-65535（秒）

「Apply」ボタンをクリックし、設定を適用します。

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

システムログサーバの設定を行います。

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

図 5-29　System Log Server Settings 画面

本画面には次の項目があります。

項目	説明
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：514 設定可能範囲：514、1024-65535
Severity	ログされる情報のレベルを選択します。 選択肢：「1：Emergencies」（緊急）、「2：Alerts」（警告）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（注意）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Facility	ファシリティ値を選択します。 設定可能範囲：0-23

「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のエントリを削除します。

System Log（Syslog ログ）

Syslog 画面では、スイッチ上のシステムログを閲覧することができます。

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

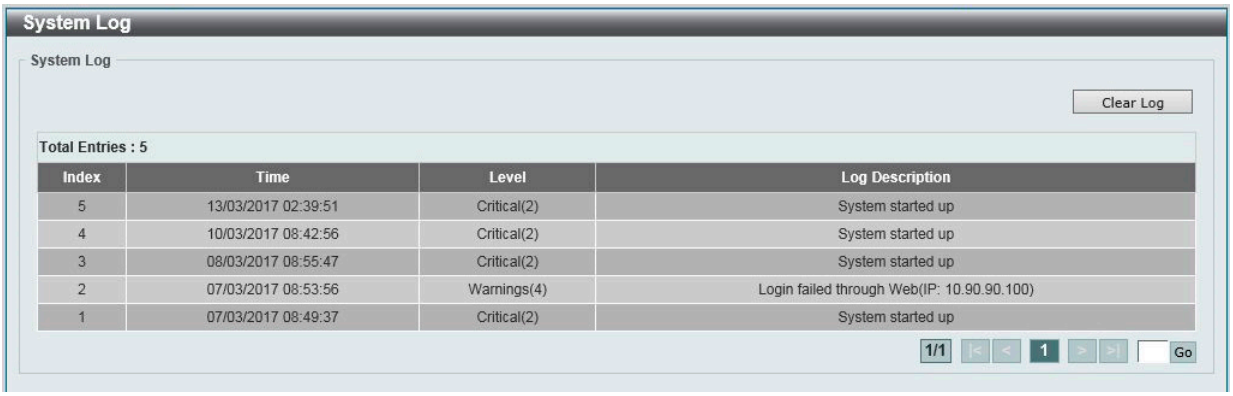


図 5-30　System Log 画面

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ページへ移動します。
すべてのエントリをクリアするには、「Clear Log」ボタンをクリックします。

Time and SNTP（時刻設定）

Clock Settings（時間設定）v

スイッチの時刻を設定します。

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

図 5-31　Clock Settings 画面

本画面には次の項目があります。

項目	説明
Time（HH:MM:SS）	システムの時刻を「HH:MM:SS」のフォーマットで設定します。（例：21:00:00）
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。（例：26/04/2018）

「Apply」ボタンをクリックし、設定を適用します。

Time Zone Settings（タイムゾーン設定）

以下の画面では、SNTP 用のタイムゾーンとサマータイム（Daylight Saving Time）の設定を行います。

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

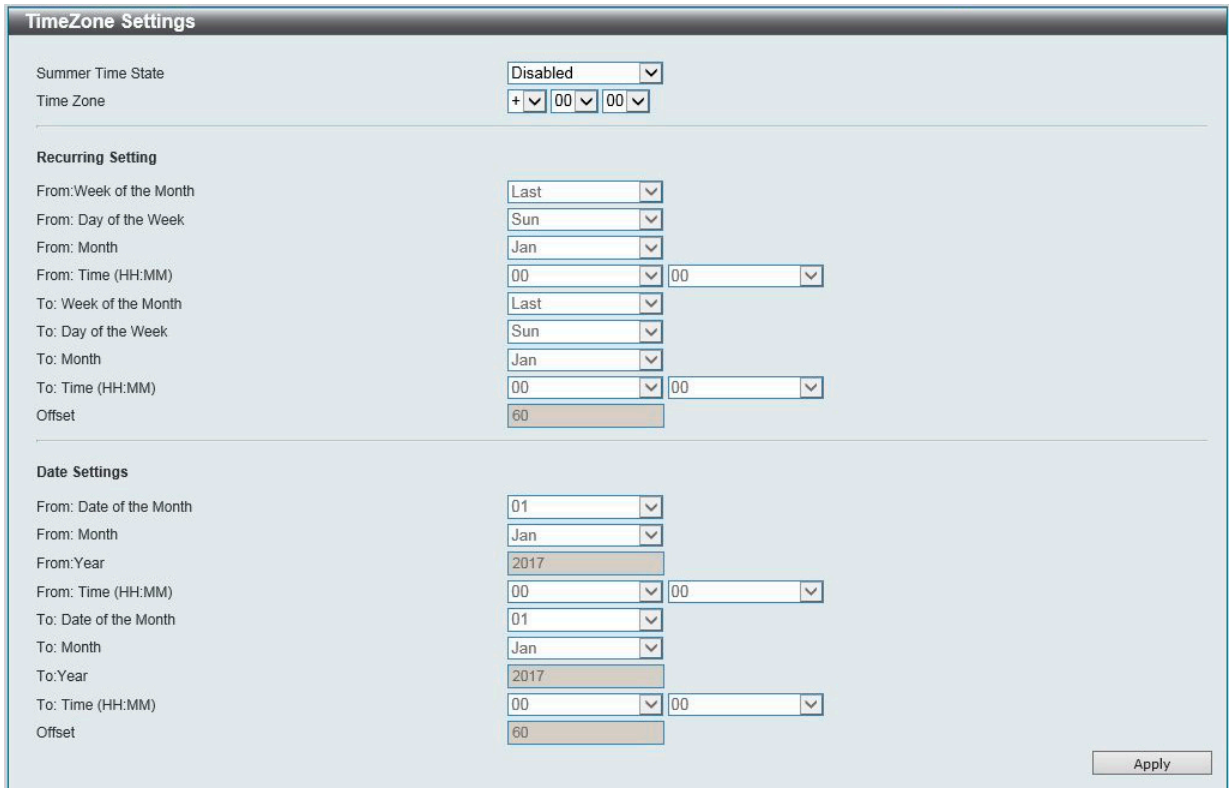


図 5-32　TimeZone Settings 画面

本画面には次の項目があります。

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 - サマータイムを周期的に有効にします。このオプションでは開始と終了のタイミングを指定月の指定週で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	タイムゾーンを設定します。UTC を基準として、現地時間のオフセットを指定します。

項目	説明
Recurring Setting	
From: Week Of The Month	月の第何週からサマータイムが始まるかを設定します。 • Last - 月の最後の週に設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
From: Day Of Week	サマータイムが開始する曜日を指定します。 選択肢：「Sun」「Mon」「Tue」「Web」「Tues」「Fri」「Sat」
From: Month	サマータイムが開始する月を指定します。 選択肢：「Jan」「Feb」「Mar」「Apr」「May」「Jun」「Jul」「Aug」「Sep」「Oct」「Nov」「Dec」
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	月の第何週でサマータイムが終わるかを設定します。 • Last - 月の最後の週に設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
To: Day Of Week	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	サマータイム期間中に追加される時間を指定します。 初期値：60（分）
Date Setting	
From: Date of the Month	サマータイムが開始する日を指定します。（毎年）
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。
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）
To: Date of the Month	サマータイムが終了する日を指定します。（毎年）
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。
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	サマータイム期間中に追加される時間を指定します。 初期値：60（分）

「Apply」ボタンをクリックし、設定を適用します。

SNTP Settings（SNTP 設定）

SNTP（Simple Network Time Protocol ）はインターネット経由で SNTP サーバのクロックに同期するプロトコルです。

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

図 5-33　SNTP Settings 画面

本画面には次の項目があります。

SNTP Global Settings（SNTP グローバル設定）

項目	説明
Current Time Source	現在の日付と時刻の提供元を表示します。
SNTP State	SNTP を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）
Poll Interval	同期する間隔を指定します。 初期値：720（秒） 設定可能範囲：30-99999（秒）

「Apply」ボタンをクリックし、設定を適用します。

SNTP Server Settings（SNTP サーバ設定）

項目	説明
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。

「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のエントリを削除します。

Time Range（タイムレンジ設定）

スイッチの PD アライブ機能などで使用するスケジュールを定義します。

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

図 5-34　Time Range 画面

以下の項目が表示されます。

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入力します。（半角英数字 32 文字以内）
From Week / To Week	タイムレンジとして使用する期間を指定します。「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。 • 「From: Week」- タイムレンジに使用する「始まり」の曜日を指定します。 • 「To: Week」- タイムレンジに使用する「終わり」の曜日を指定します。「End Weekday」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。

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

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ページへ移動します。

第 6 章　Management（スイッチの管理）

本メニューでは、ユーザアカウントや SNMP、セッションなどのスイッチ管理に関する設定を行います。

以下は、Management 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
User Accounts Settings（ユーザアカウント設定）	ユーザパスワードとアクセス権限を含むユーザアカウント設定を行います。
Password Encryption（パスワード暗号化）	コンフィグレーションのパスワード暗号化の設定を行います。
SNMP Settings（SNMP 設定）	SNMP の設定を行います。本スイッチシリーズは、SNMP v1、v2c、および v3 をサポートしています。
Web（Web 設定）	スイッチの Web ポート番号の設定を行います。
Session Timeout（セッションタイムアウト）	Web セッションのタイムアウトの設定を行います。
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）の設定を行います。

User Accounts Settings（ユーザアカウント設定）

スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。

注意　初期値ではユーザアカウントは設定されていません。

本スイッチでは、事前定義済みのユーザアカウント権限レベルとして以下の 3 種類が用意されています。

アカウントの種類	説明
Basic User（基本ユーザ）	権限レベル 1。ユーザアカウントの中でも一番低い優先値になります。このアカウントの目的は基本的なシステムのチェックになります。
Operator（オペレータ）	権限レベル 12。システム設定の変更や確認が可能です。SNMP アカウントやユーザアカウントなどのセキュリティ関連情報への権限はありません。
Administrator（管理者）	権限レベル 15。システム情報を含むすべての設定に関する閲覧、変更の権限があります。

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

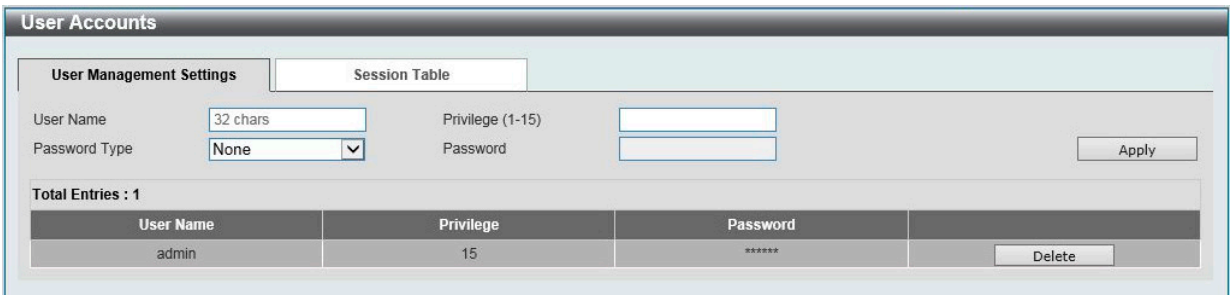


図 6-1　User Accounts Settings - User Management Settings 画面

本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。 設定可能範囲：1-15
Password Type	アカウントで使用する暗号化の方式を選択します。 選択肢：「None」「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」
Password	「Plain Text」もしくは「Encrypted-SHA1/MD5」を指定した場合、アカウントで使用するパスワードを入力します。

「Apply」ボタンをクリックし、設定を適用します。
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ページへ移動します。

注意　アカウントの権限レベルとして、定義済みの権限レベル（1、12、15）以外を指定した場合は以下のように設定されます。

- 2 ～ 11 を指定した場合は権限レベル 1 とみなされます。
- 13 ～ 14 を指定した場合は権限レベル 12 とみなされます。

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

Session Table

「Session Table」タブをクリックするとユーザアカウントの現在の状況が表示されます。

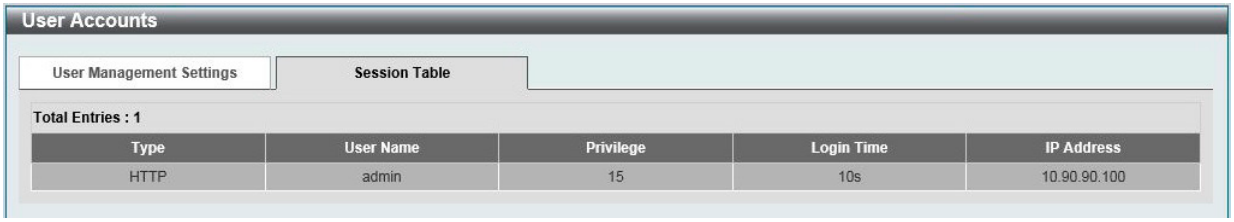


図 6-2　User Accounts Settings - Session Table 画面

Password Encryption（パスワード暗号化）

コンフィグレーションファイルのパスワードを暗号化します。

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

図 6-3　Password Encryption 画面

画面には次の項目があります。

項目	説明
Password Encryption State	コンフィグレーションファイルのパスワード暗号化を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）
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 - パスワード暗号化タイプを「SHA-1」に指定します。 • Encrypted-MD5 - パスワード暗号化タイプを「MD-5」に指定します。

「Apply」ボタンをクリックし、設定を適用します。

SNMP Settings（SNMP 設定）

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルで、ネットワークデバイスの管理や監視を行います。ネットワーク管理デバイスは、SNMP を利用してゲートウェイ、ルータ、およびその他のネットワークデバイスの設定状態を確認または変更します。また、SNMP を利用して、ローカルネットワーク上のスイッチに対し、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、管理側のデバイスに対し、デバイス上の SNMP エージェントによる標準的な情報提供が行われます。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。

SNMP Global Settings（SNMP グローバル設定）

SNMP グローバルステート設定を有効または無効にします。

初期状態では、SNMP グローバル設定は無効化されています。SNMP 機能を利用するには、「Enabled」にチェックを入れ、トラップ設定を行い、「Apply」をクリックしてください。

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。

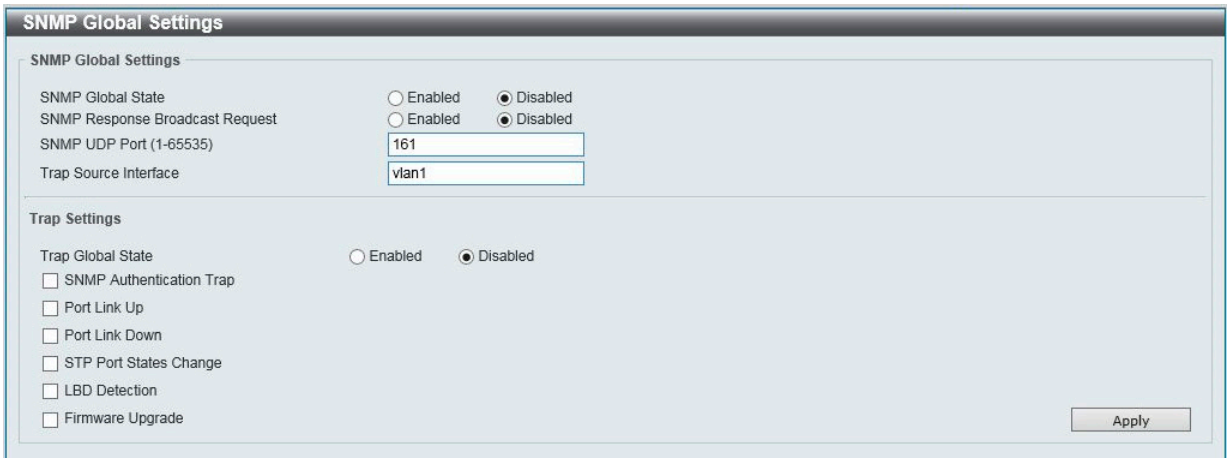


図 6-4　SNMP Global Settings 画面

本画面には次の項目があります。

項目	説明
SNMP Global Settings	
SNMP Global State	「SNMP」機能を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）
SNMP Response Broadcast Request	「SNMP GetRequest」パケットのブロードキャストに対応するサーバを「Enabled」（有効）/「Disabled」（無効）に設定します。
SNMP UDP Port	SNMP UDP ポート番号を指定します。 設定可能範囲：1-65535
Trap Source Interface	SNMP トラップパケットを送信する際に送信元アドレスとして使用する IP アドレスのインタフェースを入力します。
Trap Settings	
Trap Global State	「SNMP」トラップを「Enabled」（有効）/「Disabled」（無効）に設定します。無効に設定した場合、トラップ信号は送信されません。有効に設定した場合、SNMP トラップの種類を選択します。
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、使用している SNMP のバージョンによって異なります。SNMPv1 または SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。SNMPv3 の場合、不正な SHA/MD5 鍵によってパケットが構成されている時に認証に失敗します。
Port Link Up	リンクアップ通知を有効にします。リンクダウン状態からリンクアップ状態に変わったときに、「Link Up」トラップが管理デバイスに対して送信されます。
Port Link Down	リンクダウン通知を有効にします。リンクアップ状態からリンクダウン状態に変わったときに、「Link Down」トラップが管理デバイスに対して送信されます。
STP Port Status Change	STP ポートステータス変更通知を有効にします。STP ポートステータスで状態の変更があったときに、「STP Port Status Change」トラップが管理デバイスに対して送信されます。
LBD Detection	LBD 検知通知を有効にします。LBD を検知したときに、「LBD Detection」トラップが管理デバイスに対して送信されます。
Firmware Upgrade	ファームウェアアップグレード通知を有効にします。ファームウェアアップグレードが実施されたときに、「Firmware Upgrade」トラップが管理デバイスに対して送信されます。

「Apply」ボタンをクリックし、設定を適用します。

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

SNMP ビューでは、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できるようにするかを定義することができます。

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。

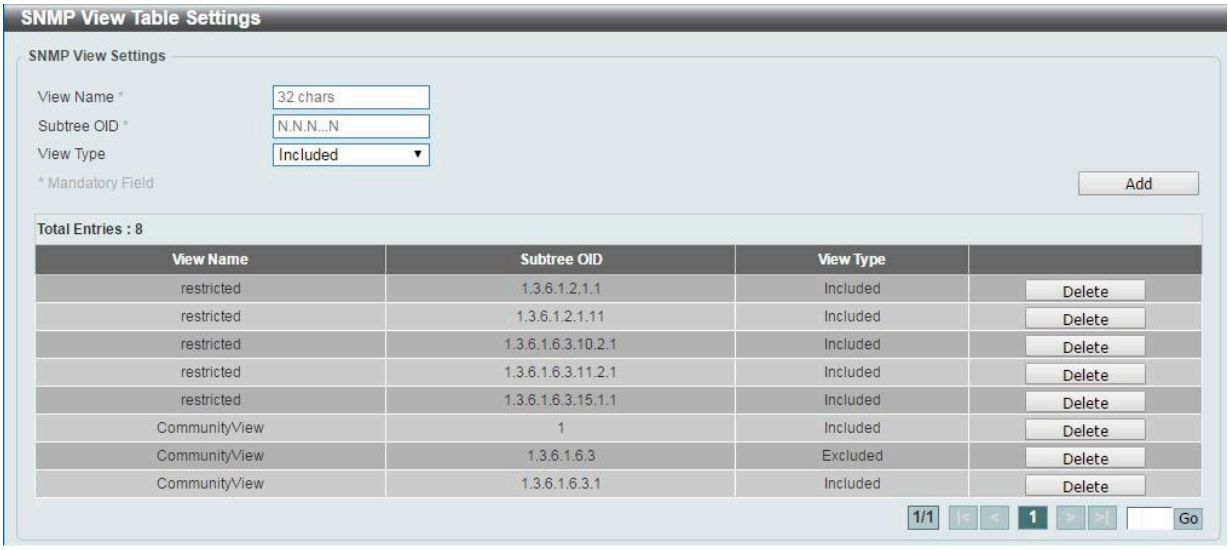


図 6-5　SNMP View Table Settings 画面

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。

エントリの新規作成

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

本画面には次の項目があります。

項目	説明
View Name	SNMP ビュー名を、32 文字までの半角英数字を入力します。
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）の識別に使用され、SNMP マネージャによってアクセス可能な範囲に含まれるかどうかが指定されます。
View Type	「Subtree OID」で指定した OID が、SNMP マネージャがアクセス可能な範囲であるかを指定します。 • Included - アクセス可能になります。 • Excluded - アクセス不可になります。

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

スイッチの SNMP コミュニティ名を設定します。コミュニティ名は、スイッチのエージェントへのアクセスを行う際のパスワードの役割をします。本スイッチと同じコミュニティ名を使用する SNMP マネージャが、スイッチの SNMP エージェントにアクセスすることができます。

エントリの設定

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

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。

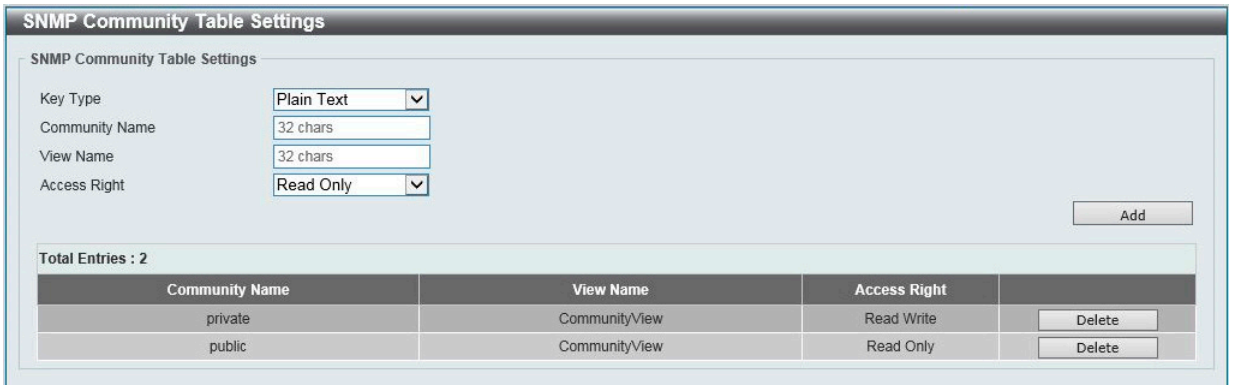


図 6-6　SNMP Community Table Settings 画面

本画面には次の項目があります。

項目	説明
Key Type	SNMP コミュニティのキーの種類を選択します。 選択肢：「Plain Text」「Encrypted」
Community Name	SNMP コミュニティメンバを識別するためのコミュニティ名を、32 文字までの半角英数字で入力します。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されます。
View Name	SNMP ビュー名を、32 文字までの半角英数字で入力します。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 グループを識別するために使用します。View Name は SNMP View Table 画面で定義済みである必要があります。
Access Right	プルダウンメニューからユーザのアクセス権限を選択します。 • Read Only - 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 - 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「Delete」ボタンをクリックし、エントリを削除します。

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

SNMP グループを登録します。SNMP の OID とセキュリティポリシーへのアクセスは、グループ単位で制御することができます。

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 6-7　SNMP Group Table Settings 画面

本画面には次の項目があります。

項目	説明
Group Name	SNMP グループ名を、32 文字までの半角英数字で入力します。
User-based Security Model	SNMP セキュリティモデルを選択します。 • 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）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に対し、認証と暗号化は行われません。 • AuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットに対して認証が行われます。暗号化は行われません。 • AuthPriv - スイッチとリモート SNMP マネージャ間のパケットに対して認証と暗号化が要求されます。
Read View Name	読み取り可能な SNMP ビュー名を入力します。
Write View Name	書き込み可能な SNMP ビュー名を入力します。
Notify View Name	トラップメッセージの送信を許可する SNMP ビュー名を入力します。

「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。

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

エンジン ID は、スイッチの SNMP v3 エンジンを識別するための固有の識別名です。

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

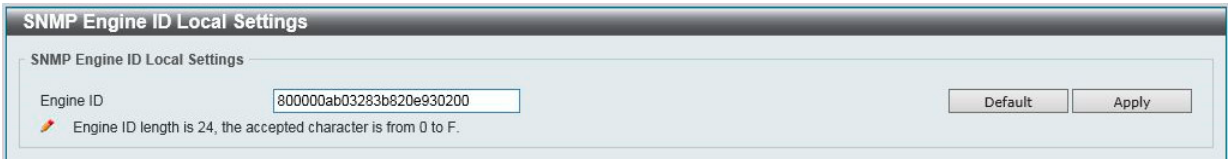


図 6-8　SNMP Engine ID Settings 画面

本画面には次の項目があります。

項目	説明
Engine ID	スイッチの SNMP エンジンの識別子を指定します。24 文字内で指定可能です。

新しいエンジン ID 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）

SNMP ユーザテーブル設定では、スイッチにアクセス可能な SNMP ユーザを管理します。ユーザ毎に、グループ、SNMP バージョン、認証や暗号化について設定が可能です。

Management > SNMP > SNMP User 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。

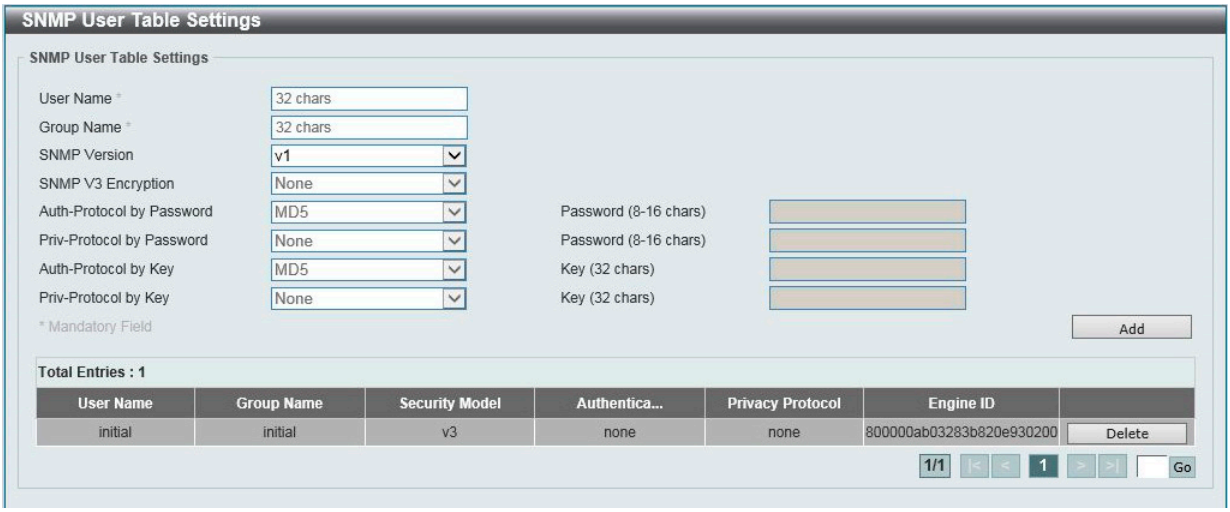


図 6-9　SNMP User Table Settings 画面

本画面には次の項目があります。

項目	説明
User Name	SNMP ユーザ名を、32 文字までの半角英数字で入力します。
Group Name	SNMP ユーザの SNMP グループ名を入力します。
SNMP Version	ユーザの SNMP バージョンを選択します。 選択肢：「v1」「v2c」「v3」
SNMP V3 Encryption	SNMP V3 に対して暗号化を有効にします。本項目は「SNMP Version」で「v3」を選択した場合に有効になります。 • None - ユーザ認証は使用しません。 • Key - HMAC-MD5 アルゴリズムまたは HMAC-SHA-96 アルゴリズムレベルのユーザ認証を行います。 • Password - HMAC-MD5-96 パスワードまたは HMAC-SHA-96 パスワードによる認証を行います。
Auth-Protocol by Password/ Auth-Protocol by Key	本項目は「SNMP Version」で「v3」を選択し、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。本項目を選択後、「Password」/「Key」にパスワードを入力します。 • MD5 - HMAC-MD5-96 認証レベルが使用されます。（Password：半角英数字 8-16 文字 /Key：半角英数字 32 文字） • SHA - HMAC-SHA 認証プロトコルが使用されます。（Password：半角英数字 8-20 文字 /Key：半角英数字 40 文字）
Priv-Protocol by Password/ Priv-Protocol by Key	本項目は「SNMP Version」で「v3」を選択し、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 • None - 認証プロトコルは使用されません。 • DES56 - CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されます。本項目を選択後、「Password」/「Key」にパスワード（半角英数字 8-16 文字）、または Key（半角英数字 32 文字）を入力します。

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。

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

SNMP トラップの送信先を設定します。

Management > SNMP > SNMP Host 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。

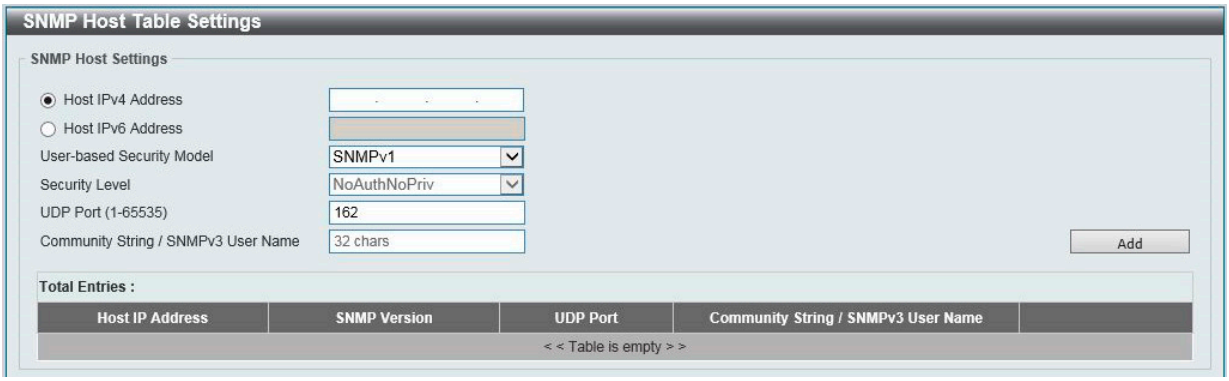


図 6-10　SNMP Host Table Settings 画面

本画面には次の項目があります。

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。
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv6 アドレスを入力します。
User-based Security Model	管理ホストに対して使用される SNMP バージョンを指定します。 選択肢：「SNMPV1」「SNMPV2c」「SNMPV3」
Security Level	SNMP バージョン 3 を選択した場合のみ、セキュリティレベルの設定を行います。 • NoAuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットに対し、認証と暗号化は行われません。 • AuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットに対して認証が行われます。暗号化は行われません。 • AuthPriv - スイッチとリモート SNMP マネージャ間のパケットに対して認証と暗号化が要求されます。
UDP Port	トラップ UDP ポート番号を入力します。 初期値：162 設定可能範囲：1-65535
Community String/ SNMPv3 User Name	通知パケットと一緒に送信される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。

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、「Add」ボタンをクリックします。

Web（Web 設定）

スイッチの Web 設定を行います。

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

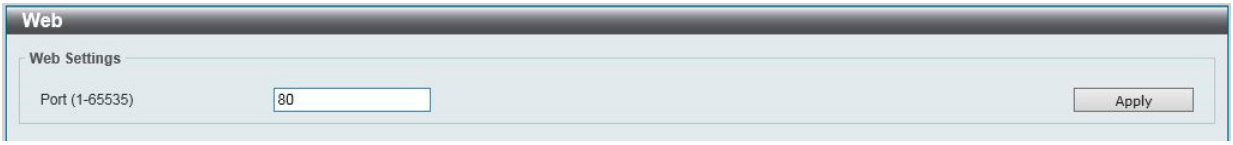


図 6-11　Web 画面

本画面には次の項目があります。

項目	説明
Port (1-65535)	スイッチの Web ベースマネジメントに使用される TCP ポート番号を指定します。HTTP プロトコルに通常使用される TCP ポートは 80 です。 設定可能範囲：1-65535

「Apply」ボタンをクリックし、設定を適用します。

Session Timeout（セッションタイムアウト）

セッションタイムアウトの設定を行います。

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

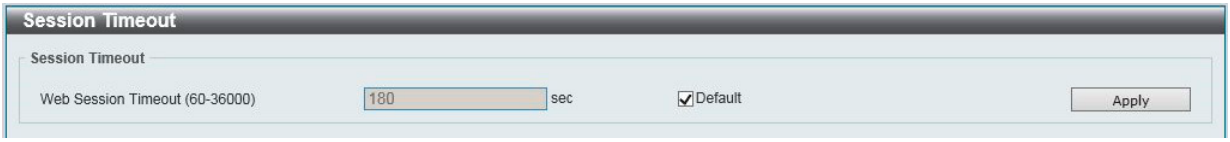


図 6-12　Session Timeout 画面

本画面には次の項目があります。

項目	説明
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。「Default」にチェックを入れると初期値に戻ります。 初期値：180（秒） 設定可能範囲：60-36000（秒）

「Apply」ボタンをクリックし、設定を適用します。

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。

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。

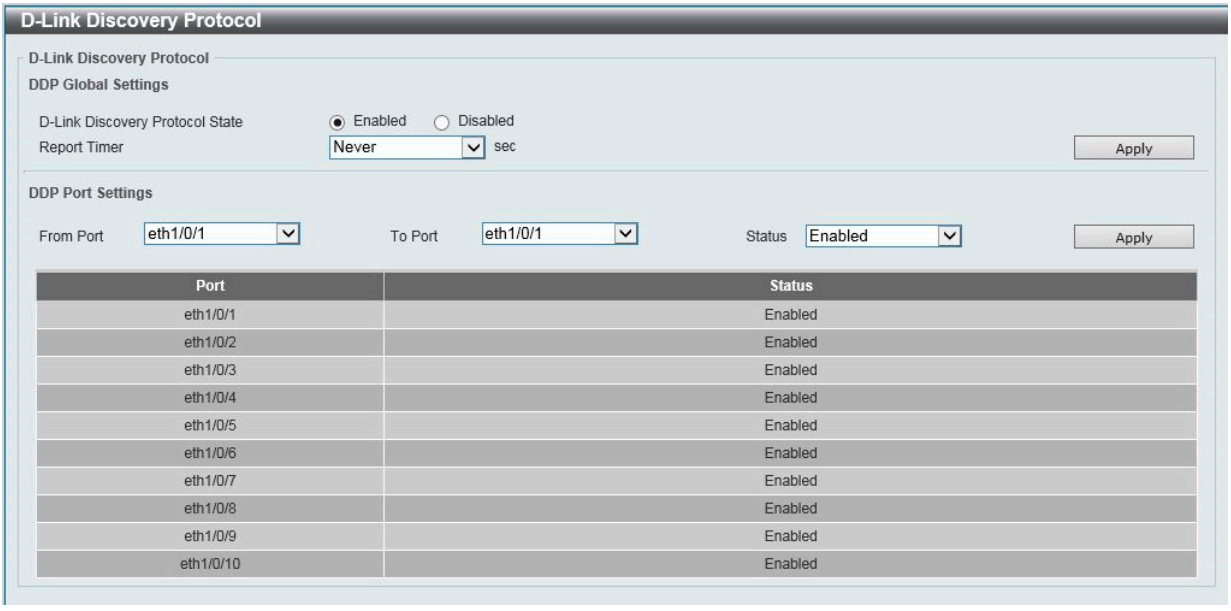


図 6-13　D-Link Discovery Protocol 画面

本画面には次の項目があります。

D-Link Discovery Protocol（D-Link Discovery プロトコル）

項目	説明
D-Link Discovery Protocol State	DDP を「Enabled」（有効）/「Disabled」（無効）に設定します。
Report Timer	DDP レポートメッセージの送信間隔（秒）を指定します。 選択肢：「30」「60」「90」「120」「Never」

「Apply」ボタンをクリックし、設定を適用します。

DDP Port Settings（DDP ポート設定）

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
Status	DDP ポートを「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

第 7 章　L2 Features（L2 機能の設定）

本メニューでは、レイヤ 2 機能に関する設定を行います。

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）	FDB（Forwarding DataBase）フォワーディングデータベースの設定を行います。
VLAN（VLAN 設定）	802.1Q VLAN、Asymmetric VLAN、VLAN インタフェース、自動サーベイランス VLAN、音声 VLAN の設定を行います。
STP（スパニングツリー設定）	スパニングツリープロトコル（STP）設定を行います。3 つのバージョンの STP（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。
ERPS (G.8032)（イーサネットリングプロテクション設定）	「Ethernet Ring Protection Switching」(ERPS) 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（LBD）機能の設定を行います。
Link Aggregation（リンクアグリゲーション）	Link Aggregation（リンクアグリゲーション / ポートトランキング）の設定を行います。
L2 Multicast Control（L2 マルチキャストコントロール）	IGMP Snooping 及び MLD Snooping の設定を行います。
LLDP	Link Layer Discovery Protocol（LLDP）の設定を行います。

FDB（FDB 設定）

Static FDB（スタティック FDB の設定）

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

スイッチにスタティックなユニキャストフォワーディングを設定します。

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

図 7-1　Unicast Static FDB 画面

本画面には次の項目があります。

項目	説明
Port/Drop	• Port - 指定した MAC アドレスが属するポート番号を指定します。 • drop - ユニキャストのスタティック FDB から MAC アドレスを破棄します。
Port Number	「Port」を選択した場合、ポート番号を選択します。
VID	関連するユニキャスト MAC アドレスが属する VLAN ID を入力します。
MAC Address	パケットがスタティックに送信または破棄される宛先の MAC アドレス。ユニキャスト MAC アドレスを指定します。

「Apply」ボタンをクリックし、設定を適用します。
「Delete」ボタンをクリックすると指定のエントリを削除します。
「Delete All」ボタンをクリックするとすべてのエントリを削除します。
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。

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

スイッチにスタティックなマルチキャストフォワーディングを設定します。

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

図 7-2　Multicast Static FDB 画面

本画面には次の項目があります。

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
VID	指定の MAC アドレスが属する VLAN の VLAN ID。
MAC Address	マルチキャストパケットのスタティックな送信先 MAC アドレスを指定します。宛先 MAC アドレスの形式は「01-xx-xx-xxxxxx」です。

「Apply」ボタンをクリックし、設定を適用します。
「Delete」ボタンをクリックすると指定のエントリを削除します。
「Delete All」ボタンをクリックするとすべてのエントリを削除します。
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。

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

スイッチの MAC アドレスフォワーディングテーブルを参照または設定します。

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 7-3　MAC Address Table Settings 画面（Global Settings）

本画面には次の項目があります。

項目	説明
Aging Time (10-410)	MAC アドレスのエージングタイム値を入力します。エージングタイム内に同じ送信元 MAC アドレスからのフレームを受信しなかった場合、MAC アドレスはテーブルから破棄されます。 初期値：300（秒） 設定可能範囲：10-410（秒）
Aging Destination Hit	Aging Destination Hit 機能を「Enabled」（有効）/「Disabled」（無効）に設定します。 通常、MAC アドレスフォワーディングテーブルは送信元 MAC アドレスにより更新されます。本項目を有効化すると、宛先 MAC アドレスまたは送信元 MAC アドレスによる更新を有効にします。エントリの更新頻度を高めることで、MAC アドレスエントリのエージングがタイムアウトした際のトラフィックフラッディングを軽減します。

「Apply」ボタンをクリックし、設定を適用します。

MAC Address Port Learning Settings（MAC アドレスポートラーニング設定タブ）

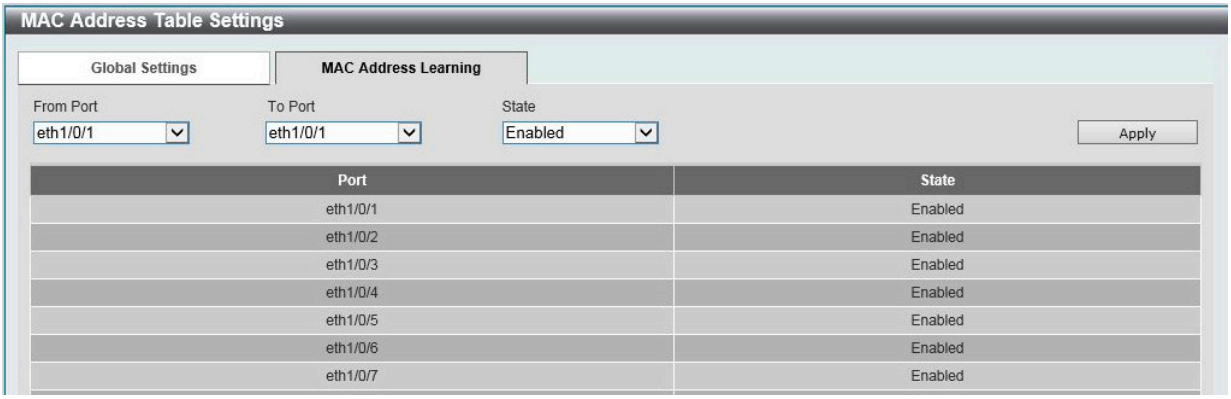


図 7-4　MAC Address Table Settings (MAC Address Port Learning) 画面

本画面には次の項目があります。

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
State	MAC アドレスラーニングを「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

MAC Address Table（MAC アドレステーブル）

スイッチの MAC アドレステーブルを参照します。

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 7-5　MAC Address Table 画面

本画面には次の項目があります。

項目	説明
Port	設定対象のポートを選択します。
VID	設定対象の VLAN ID を入力します。
MAC Address	設定対象の MAC アドレスを入力します。

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

エントリの検索

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

ダイナミックエントリの削除

「Clear Dynamic Entries（by Port/VLAN/MAC）」ボタンをクリックして、アドレステーブルのダイナミックエントリを削除します。

エントリの表示

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

全エントリの削除

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

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 を設定します。

1. **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 7-6　VLAN Configuration Wizard 画面

以下の項目が表示されます。

項目	内容
Create VLAN VID	VLAN ID を新しく作成します。
Configure VLAN ID	既存の VLAN ID を編集します。

2. 「Next」ボタンをクリックして次に進みます。VLAN の編集画面が表示されます。

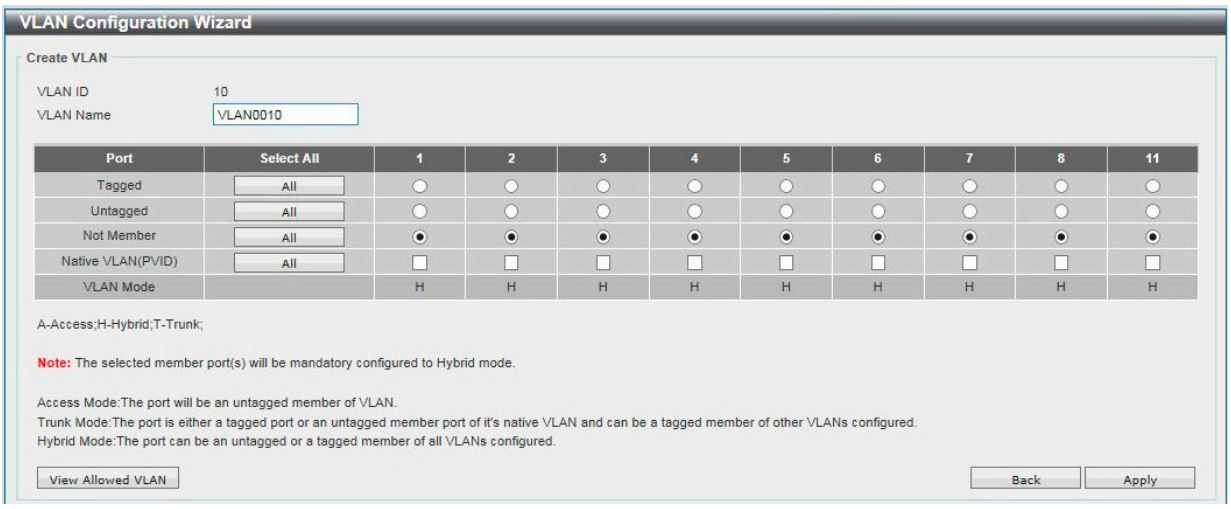


図 7-7　VLAN Configuration Wizard 画面（Create VLAN）

以下の項目が表示されます。

項目	内容
VLAN VID	VLAN ID が表示されます。
VLAN Name	VLAN グループ名を設定します。
Port	各ポートを VLAN のメンバとして定義します。「All」をクリックすると、すべてのポートを選択します。 • Untagged - ポートを 802.1Q タグなしとして定義します。 • Tagged - ポートを 802.1Q タグ付きとして定義します。 • Not Member - ポートが VLAN メンバでないことを定義します。 • Native VLAN (PVID) - Native VLAN を有効にします。

3. 「Apply」ボタンをクリックし設定内容を適用してください。

VLAN 設定を確認するには、「View Allowed VLAN」をクリックします。

802.1Q VLAN（802.1Q VLAN）

802.1Q VLAN を設定します。

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

図 7-8　802.1Q VLAN 画面

本画面には次の項目があります。

802.1Q VLAN（802.1Q VLAN）

項目	内容
VID List	VID の範囲を指定します。 設定可能範囲：1-4094

「Apply」ボタンをクリックし、設定を適用します。
「Delete」ボタンをクリックすると指定のエントリを削除します。

Find VLAN（VLAN 検索）

項目	内容
VID	表示する VLAN ID を指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「View All」をクリックして、すべてのエントリを表示します。
「Edit」をクリックして、指定エントリの編集を行います。
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。

Asymmetric VLAN（Asymmetric VLAN 設定）

Asymmetric VLAN を設定します。

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

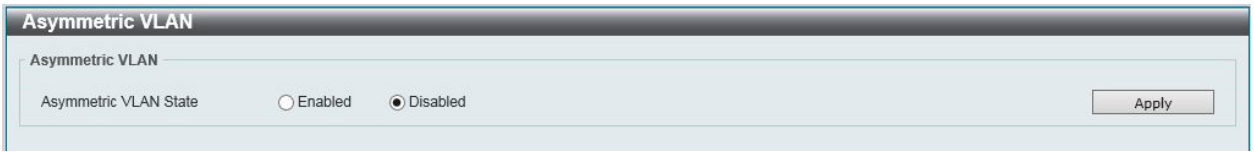


図 7-9　Asymmetric VLAN 画面

本画面には次の項目があります。

項目	内容
Asymmetric VLAN State	Asymmetric VLAN 機能を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

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。

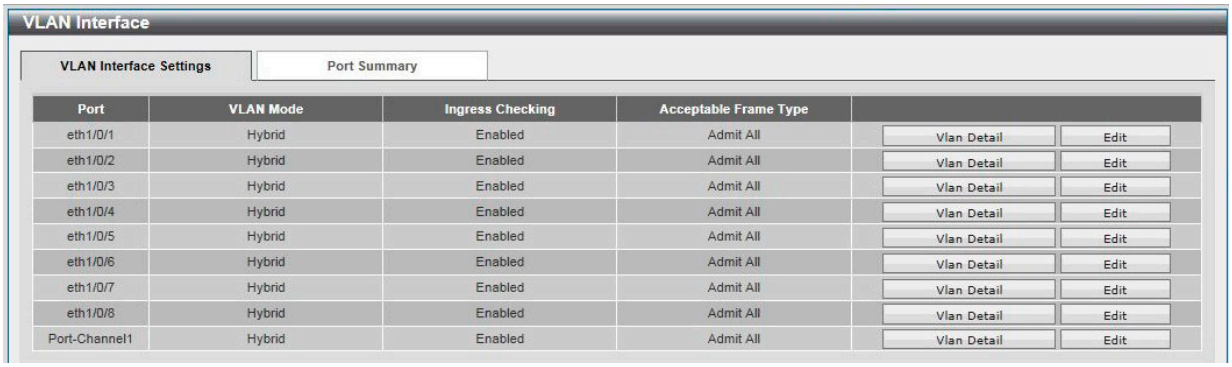


図 7-10　VLAN Interface（VLAN Interface Settings）画面

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 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。

VLAN Detail（VLAN 詳細情報の表示）

「Vlan Detail」ボタンをクリックすると、以下の画面が表示されます。

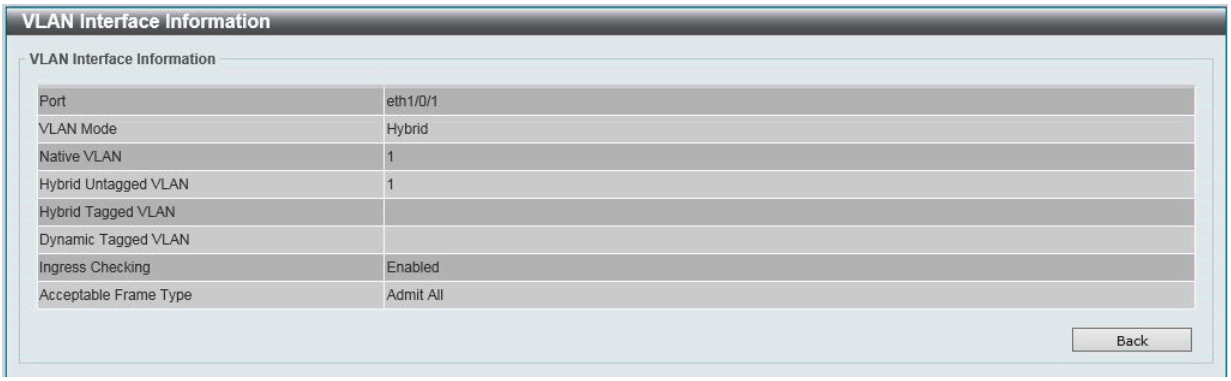


図 7-11　VLAN Interface (VLAN Detail) 画面

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」ボタンをクリックすると前画面に戻ります。

Port Summary（ポートのサマリ情報の表示）

「Port Summary」タブをクリックすると、以下の画面が表示されます。

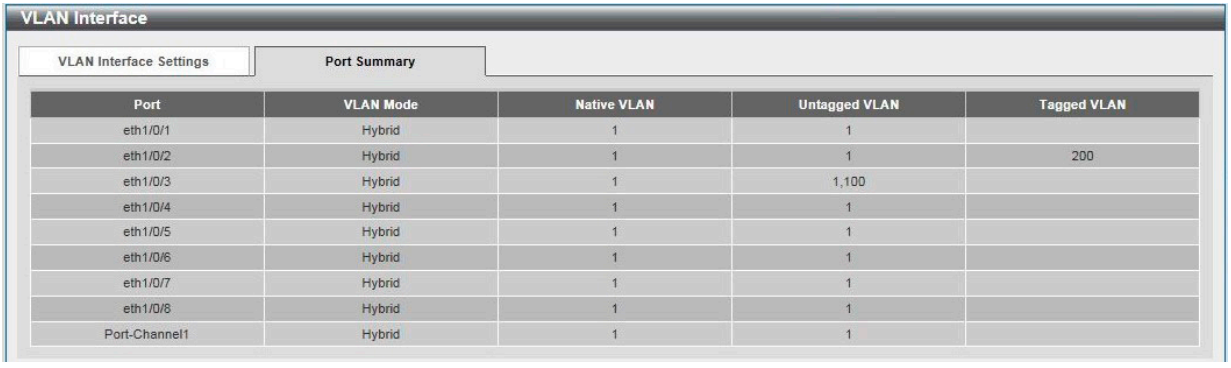


図 7-12　VLAN Interface (Port Summaryl) 画面

VLAN 設定の概要が表示されます。

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

「**L2 Features > VLAN > VLAN Interface**」画面で「Edit」をクリックします。「Access」を選択すると本画面には次の項目があります。

図 7-13　Configure VLAN Interface - Access 画面

画面には次の項目があります。

項目	説明
Port	設定対象の VLAN ポート番号が表示されます。
VLAN Mode	VLAN モードを選択します。 選択肢：「Access」「Hybrid」「Trunk」
Acceptable Frame Type	許可するフレームの種類を 選択します。 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を「Enabled」（有効）/「Disabled」（無効）に設定します。
VID	設定する「VLAN ID」を指定します。 設定可能範囲：1 -4094
Clone	本設定を特定のポートにコピーします。
From Port / To Port	コピー先のポートの始点 / 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のページに戻ります。

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。

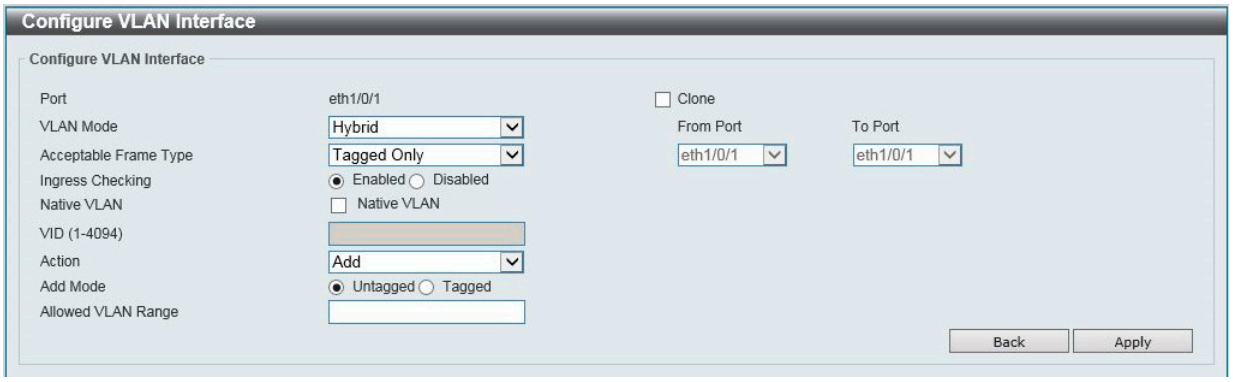


図 7-14　Configure VLAN Interface - Hybrid 画面

本画面には次の項目があります。

項目	説明
Port	設定対象の VLAN ポート番号が表示されます。
VLAN Mode	VLAN モードを選択します。 選択肢：「Access」「Hybrid」「Trunk」
Acceptable Frame Type	許可するフレームの種類を 選択します。 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を「Enabled」（有効）/「Disabled」（無効）に設定します。
Native VLAN	「Native VLAN」を有効にします。
VID	「Native VLAN」を有効にした後、「Native VLAN」に設定する「VLAN ID」を指定します。 設定可能範囲：1 -4094
Action	実行する動作を選択します。「Add」を選択した場合、「Add Mode」を指定します。 選択肢：「Add（追加）」「Remove（削除）」「Tagged」「Untagged」
Add Mode	「Untagged」または「Tagged」パラメータを追加します。

項目	説明
Allowed VLAN Range	Hybrid モードで追加または削除する VLAN 範囲を指定します。
Clone	本設定を特定のポートにコピーします。
From Port / To Port	コピー先のポートの始点 / 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。

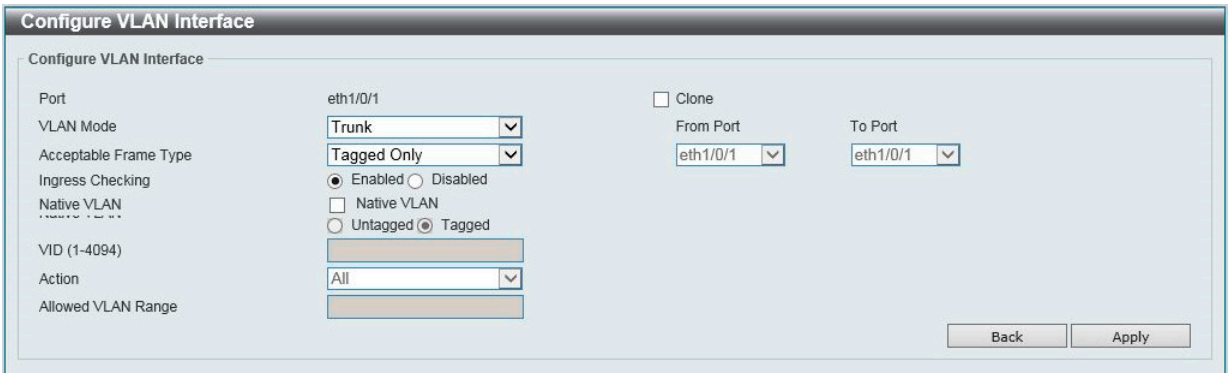


図 7-15　Configure VLAN Interface - Trunk 画面

画面には次の項目があります。

項目	説明
Port	設定対象の VLAN ポート番号が表示されます。
VLAN Mode	VLAN モードを選択します。 選択肢：「Access」「Hybrid」「Trunk」
Acceptable Frame Type	許可するフレームの種類を 選択します。 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を「Enabled」（有効）/「Disabled」（無効）に設定します。
Native VLAN	「Native VLAN」を有効にします。また、「Untagged」「Tagged」を選択します。
VID	「Native VLAN」を有効にした後、「Native VLAN」に設定する「VLAN ID」を指定します。 設定可能範囲：1 -4094
Action	実行する動作を選択します。「Add」を選択した場合、「Add Mode」を指定します。 選択肢：「All（すべて追加）」「Add（追加）」「Remove（削除）」「Except（除外）」「Replace（置き換え）」 補足　本設定を行うには、「Trunk」モードを選択し、一旦「Apply」をクリックする必要があります。初期値では「All」が指定され、全ての VLAN が許可されます。
Allowed VLAN Range	Trunk モードで追加または削除する VLAN 範囲を指定します。 補足　本設定を行うには、「Trunk」モードを選択し、一旦「Apply」をクリックする必要があります。
Clone	本設定を特定のポートにコピーします。
From Port / To Port	コピー先のポートの始点 / 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 の設定と表示を行います。

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。

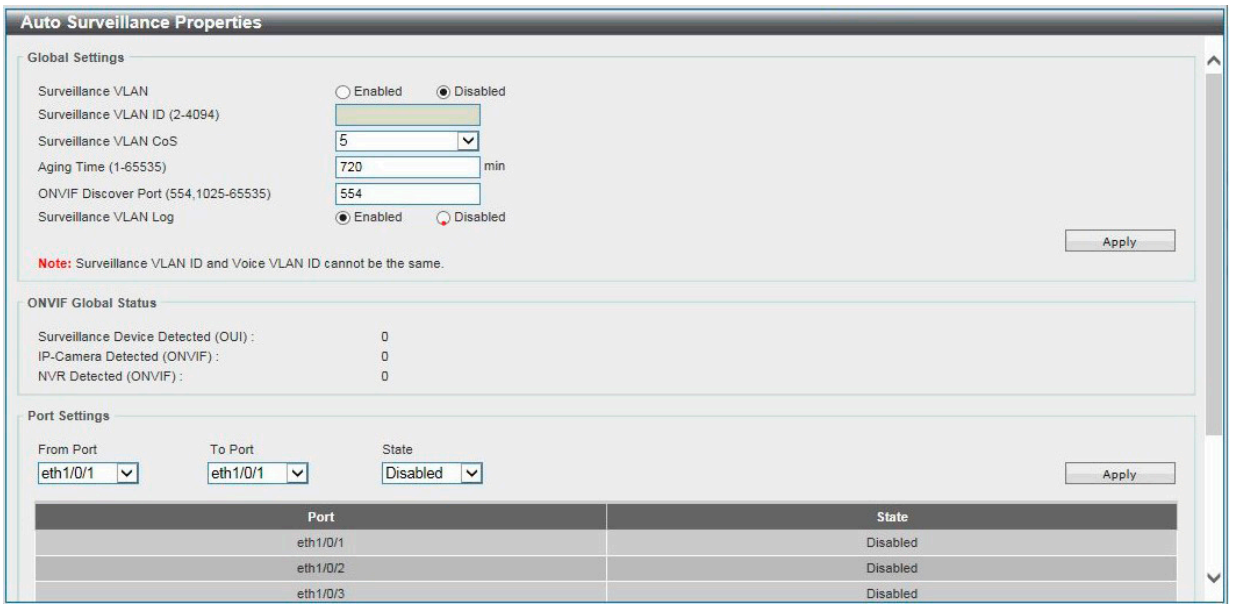


図 7-16　Auto Surveillance Properties 画面

本画面には次の項目があります。

Global Settings（グローバル設定）

項目	説明
Surveillance VLAN	サーベイランス VLAN を「Enabled」（有効）/「Disabled」（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。 設定可能範囲：2-4094
Surveillance VLAN CoS	サーベイランス VLAN の優先値を指定します。 設定可能範囲：0-7
Aging Time	サーベイランス VLAN のエージングタイム 。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。サーベイランスデバイスによるトラフィック送信が停止し、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。 サーベイランストラフィックがエージングタイム内に再開すると、エージングカウンタがリセットされ、エージングタイマは停止します。 初期値：720（分） 設定可能範囲：1-65535（分）
ONVIF Discover Port	「TCP/UDP」ポート番号を指定します。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。 設定可能範囲：554、1025 -65535
Surveillance VLAN Log	Surveillance VLAN ログを「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

Port Settings（ポート設定）

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
State	ポートの状態を「Enabled」（有効）/「Disabled」（無効）に設定します。

「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トラフィックの 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。

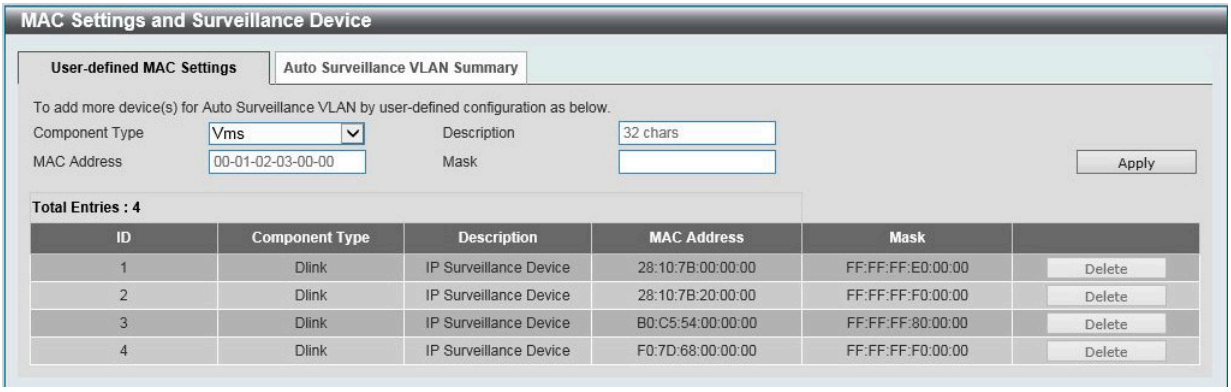


図 7-17　User -defined MAC Settings 画面

本画面には次の項目があります。

項目	説明
Component Type	プルダウンメニューから、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。 選択肢：「Video Management Server」「VmsClient」「VideoEncoder」「NetworkStorage」「Other IP Surveillance Device」
Description	ユーザ定義 OUI に関する説明文を入力します。（最大 32 文字）
MAC Address	ユーザ定義の OUI MAC アドレスを入力します。
Mask	ユーザ定義の OUI MAC アドレスマスクを入力します。

「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 7-18　Auto Surveillance VLAN Summary 画面

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

ONVIF VLAN で検出された IP カメラのリストを表示します。

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 7-19　ONVIF IP-Camera Information 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。

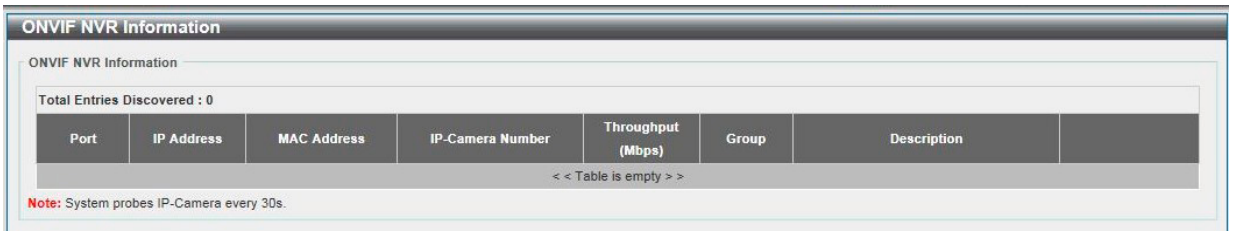


図 7-20　ONVIF NVR Information 画面

Voice VLAN（音声 VLAN）

Voice VLAN Global（音声 VLAN グローバル設定）

音声 VLAN は、IP 電話からの音声トラフィックを送信する際に使用される VLAN です。VoIP（Voice over IP）における音声品質は遅延の影響を受けやすいため、音声トラフィックが優先的に処理されるように Quality of service（QoS）の設定を行います。

スイッチは、送信元 MAC アドレスをチェックすることで受信パケットが音声パケットであるかどうか判断します。パケットの送信元 MAC アドレスが、システムによって定義される OUI（Organizationally Unique Identifier：組織で一意な識別子）アドレスに適合している場合、パケットは音声パケットと判断されて音声 VLAN に送信されます。

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 7-21　Voice VLAN Global 画面

本画面には次の項目があります。

Voice VLAN Global（音声 VLAN グローバル設定）

項目	説明
Voice VLAN State	音声 VLAN 機能を「Enabled」（有効）/「Disabled」（無効）に設定します。
Voice VID (2-4094)	音声 VLAN の 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。

Voice VLAN CoS（音声 VLAN CoS 設定）

項目	説明
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。 設定可能範囲：0-7
Aging Time (1-65535)	音声 VLAN のエージングタイムを設定します。エージングタイムは、ポートが自動 VLAN メンバである場合に、音声 VLAN からポートを削除するまでの時間です。音声機器がトラフィックを送信しなくなり、当該機器の 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。音声 VLAN タイマの時間切れの後、音声 VLAN からポートが削除されます。エージングタイム期間内に音声トラフィックが再開すると、エージングカウンタはリセットされ、タイマは停止します。 初期値：720（分） 設定可能範囲：1-65535（分）

「Apply」ボタンをクリックし、設定を適用します。

Voice VLAN Port（音声 VLAN のポート設定）

ポートの音声 VLAN 情報を表示します。

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。

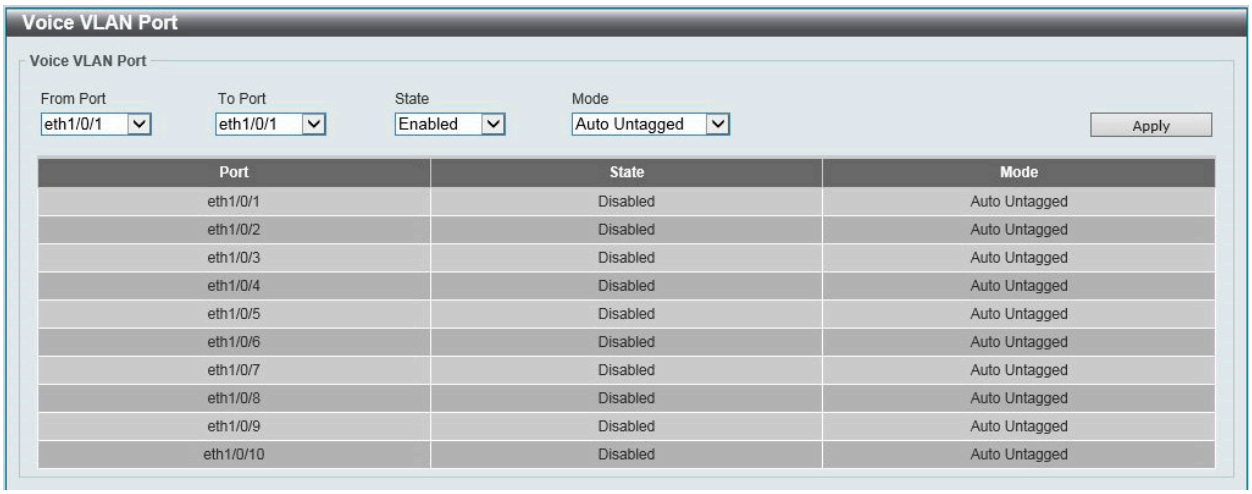


図 7-22　Voice VLAN Port 画面

本画面には次の項目があります。

項目	説明
From Port / To Port	表示するポート範囲を選択します。
State	ポートの状態を「Enabled」（有効）/「Disabled」（無効）に設定します。
Mode	ポートのモードを選択します。 選択肢：「Auto Untagged」「Auto Tagged」「Manual」

「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）

ユーザ定義の音声トラフィックの OUI を設定します。
OUI は音声トラフィックを識別するために使用されます。多くの定義済み OUI があり、必要に応じて追加のユーザ定義の OUI を設定できます。
ユーザ定義 OUI は、定義済みの OUI と同じものには設定できません。

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。

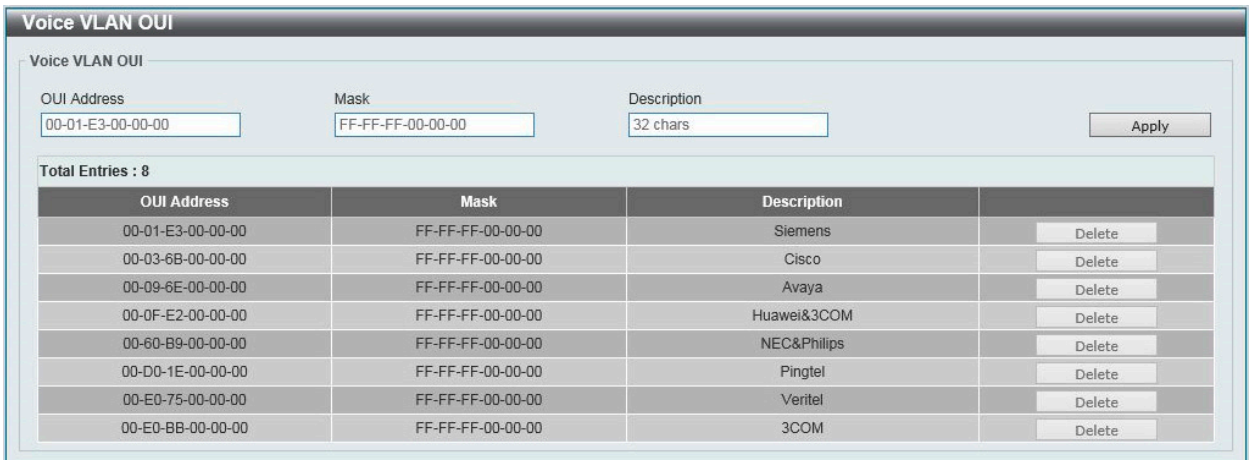


図 7-23　Voice VLAN OUI 画面

本画面には次の項目があります。

項目	説明
OUI 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。
Description	ユーザ定義 OUI に関する説明文を入力します。（半角英数字 32 文字以内）

「Apply」ボタンをクリックし、設定を適用します。

エントリの削除

「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 デバイス）

ポートに接続された音声デバイスを表示します。「Start Time」はデバイスがポートで検出された時間です。また、「Status」は、ポート上の音声 VLAN ステータスを示します。

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

図 7-24　Voice VLAN Device 画面

Voice VLAN LLDP-MED Device（音声 VLAN LLDP-MED 音声デバイス）

スイッチに接続された音声 VLAN LLDP-MED 音声デバイスを表示します。

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

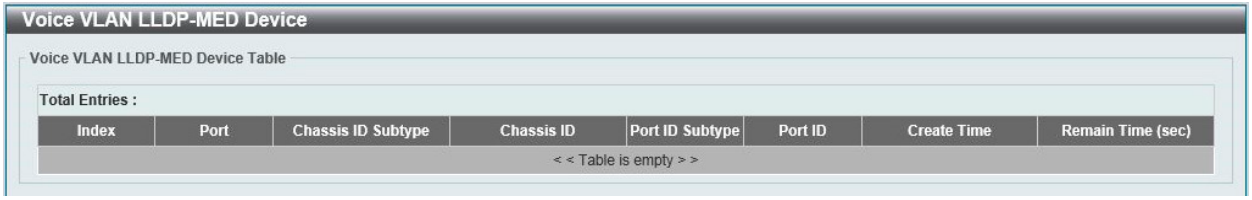


図 7-25　Voice VLAN LLDP-MED Device 画面

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

STP（スパニングツリー設定）

L2 Features > STP

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

802.1D-2004 Rapid STP

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 と同じであり、STP 用の設定項目の多くも RSTP で同じように使用されます。本項では、スパニングツリーの新しいコンセプトと、これらの 2 つのプロトコル間の主な違いについて記述します。

802.1Q-2005 MSTP

MSTP（Multiple STP Protocol）は IEEE 委員会により定義された標準規格で、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングし、ネットワーク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。

初期値では RSTP は無効です。RSTP を有効にすると、スイッチは BPDU パケットとそれに付随する Hello パケットをリッスンします。RTSP では、BPDU パケットを受信しない場合でも BPDU が送信されます。これにより、ブリッジ間の各リンクはリンクの状態をすばやく感知します。このような特性により、障害が発生したリンクの検出が速やかに行われ、迅速なトポロジの再構成へと繋がります。

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

STP Global Settings（STP グローバル設定）

STP をグローバルに設定します。STP 有効化後に STP グローバル設定を行います。

L2 Features > Spanning Tree > STP 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。

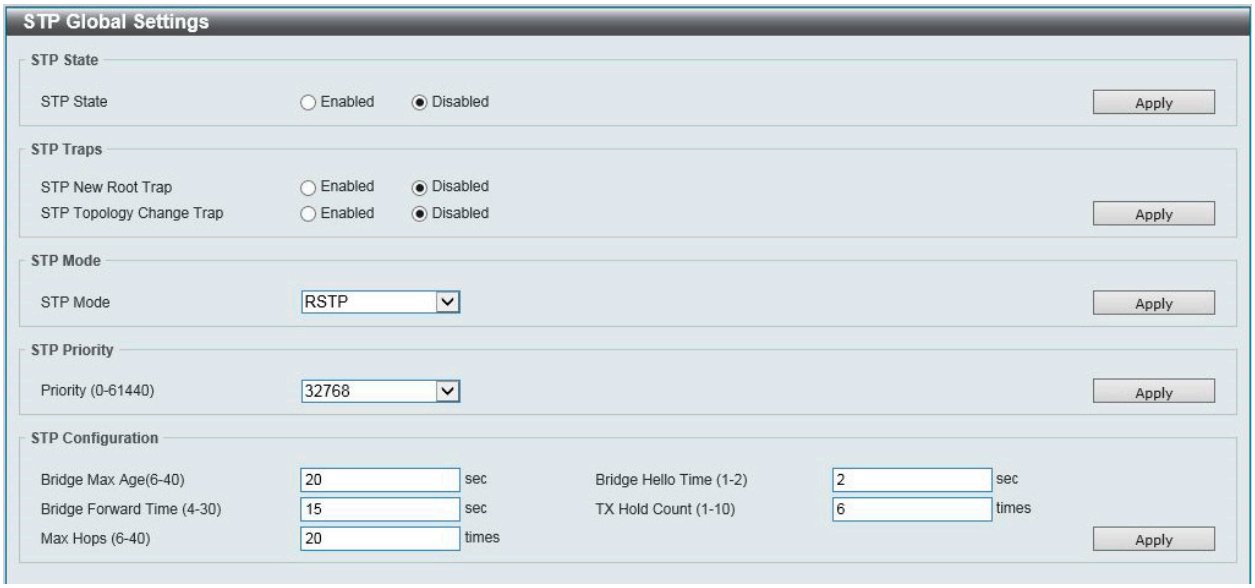


図 7-26　STP Global Settings 画面

本画面には次の項目があります。

STP State（STP ステート）

項目	説明
STP State	スパニングツリー機能を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

STP Traps（STP トラップ）

項目	説明
STP New Root Trap	新しいルートトラップ送信を「Enabled」（有効）/「Disabled」（無効）に設定します。
STP Topology Change Trap	トポロジ変更トラップ送信を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

STP Mode（STP モード）

項目	説明
STP 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。

「Apply」ボタンをクリックし、設定を適用します。

STP Priority（STP プライオリティ）

項目	説明
Priority	STP 優先値を指定します。低い値の方が、優先値は高くなります。 初期値：32768 設定可能範囲：0-61440

「Apply」ボタンをクリックし、設定を適用します。

STP Configuration（STP 設定）

項目	説明
Bridge Max Age (6-40)	最大経過時間を入力します。本項目は、古い情報がネットワーク内の冗長パスを延々と循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。 初期値：20（秒） 設定可能範囲：6-40（秒）
Bridge Forward Time (4-30)	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間、本値で指定した時間 Listening 状態を保ちます。 初期値：15（秒） 設定可能範囲：4-30（秒）
Max Hops (6-40)	スイッチが送信した BPDU パケットが破棄されるまでのスパニングツリー範囲内のデバイス間のホップ数を設定します。値が0に到達するまで、各スイッチは1つずつホップカウントを減らしていきます。スイッチは、その後BPDUパケットを破棄し、ポートに保持していた情報を解放します。 初期値：20 設定可能範囲：6-40
Bridge Hello Time (1-2)	ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために BPDU パケットを 2 回送信します。本値は、1 回目の送信と 2 回目の送信との間の時間です。「STP Version」として STP または RSTP を選択した場合のみ本項目は設定可能です。MSTP に対しては、Hello Time はポートごとに設定される必要があります。詳しくは「STP ポートの設定」セクションを参照してください。 初期値：2（秒） 設定可能範囲：1-2 (秒)
Tx Hold Count (1-10)	Hello パケットの最大送信回数を指定します。 初期値：6 設定可能範囲：1-10

「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）

スパニングツリーのパラメータをグローバル（スイッチレベル）で設定する以外に、ポートレベルのグループに対して STP の設定を行うことができます。それぞれのグループには固有のスパニングツリーインスタンス及び設定が含まれます。

ポートレベルのスパニングツリーの動作はスイッチレベルのものと同様ですが、ルートブリッジはルートポートに置き換えられます。ルートポートはポートの優先度とコストに基づいて選出され、グループのネットワークへのコネクションとなります。冗長リンクは、スイッチレベルでの冗長リンクと同様にブロックされます。

スイッチレベルの STP では、スイッチ間（及び同等のネットワークデバイス間）で冗長リンクがブロックされます。ポートレベルの STP では STP グループ内で冗長リンクがブロックされます。

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

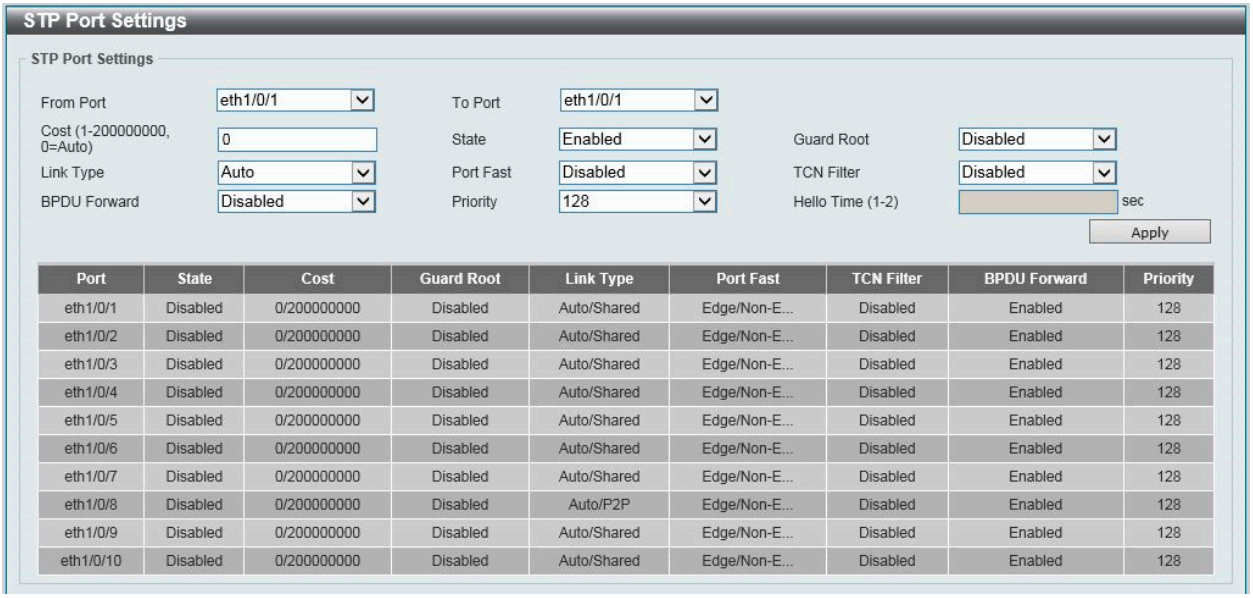


図 7-27　STP Port Settings 画面

本画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート / ポート範囲を指定します。
Cost (1-200000000, 0=Auto)	スパニングツリートポロジの計算に使用される STP ポートコストを指定します。コスト値はインタフェース帯域と相対関係があり、リンクの望ましさを表しています。ポートのコストは自動か、メトリックの値で設定します。 • 0（Auto）- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。 ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。 • 値 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほどパケット転送は頻繁に行われるようになります。 初期値：0（Auto）
State	ポートグループでの STP を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Enabled（有効）」
Guard Root	Guard Root を「Enabled」（有効）/「Disabled」（無効）に設定します。
Link Type	リンクの種類を設定します。全二重ポートは P2P 接続、半二重ポートは Shared 接続として認識されます。「Shared」に設定された場合、ポートはすぐにフォワーディング状態とはなりません。 選択肢：「P2P」「Auto」「Shared」 初期値：「Auto」
Port Fast	ポートファストオプションを指定します。 • 「Disable」モード - 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へ変化するまで転送遅延時間の経過を待ちます。 • 「Edge」モード - ポートは転送遅延時間の経過を待たずに直接 STP フォワーディングステートに変化します。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。
TCN Filter	TCN（Topology Change Notification/ トポロジ変更通知）フィルタを「Enabled」（有効）/「Disabled」（無効）に設定します。管理者の完全な制御下にはない外部ネットワークへ接続する場合、TCN フィルタリング機能が役に立ちます。TCN フィルタモードに設定されると、ポートで受信したトポロジ変更イベントは無視されます。 初期値：「Disabled」（無効）

項目	説明
BPDU Forward	ブリッジではスパニングツリーの処理において BPDU（Bridge Protocol Data Units）を使用します。 ブリッジで接続された 2 つのリージョンでそれぞれ固有のスパニングツリーを構成する場合、フォワーディング機能が役に立ちます。BPDU フィルタ機能は、STP がグローバルまたはインタフェース上で無効な場合に動作します。 • 「Disabled」（無効）- ポート上で BPDU フィルタが有効（転送が無効）になります。 • 「Enabled」（有効）- ポート上で BPDU 転送が有効になります。（STP が無効化されている必要があります。）
Priority	優先値を指定します。値が小さい方が優先度は高くなります。 初期値：128 設定可能範囲：0-240
Hello Time	BPDU パケットの送信間隔を指定します。BPDU パケットは、ルートブリッジが他の全てのスイッチに対して自身がルートブリッジであることを示すために送信されます。 初期値：2（秒） 設定可能範囲：1- 2（秒）

「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）

Multiple Spanning Tree（MSTP）は、マルチプル VLAN を 1 つのスパニングツリーインスタンスに紐付けることで負荷分散を行い、ネットワークに複数経路を提供します。例えば、ポート A が STP インスタンスによってブロックされた場合、このポートは他のインスタンスでフォワーディング状態に移行することができます。

MST Configuration Identifiaction 画面では、リージョン名、MSTP リビジョンレベルなどの MSTP のグローバル設定を行います。

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

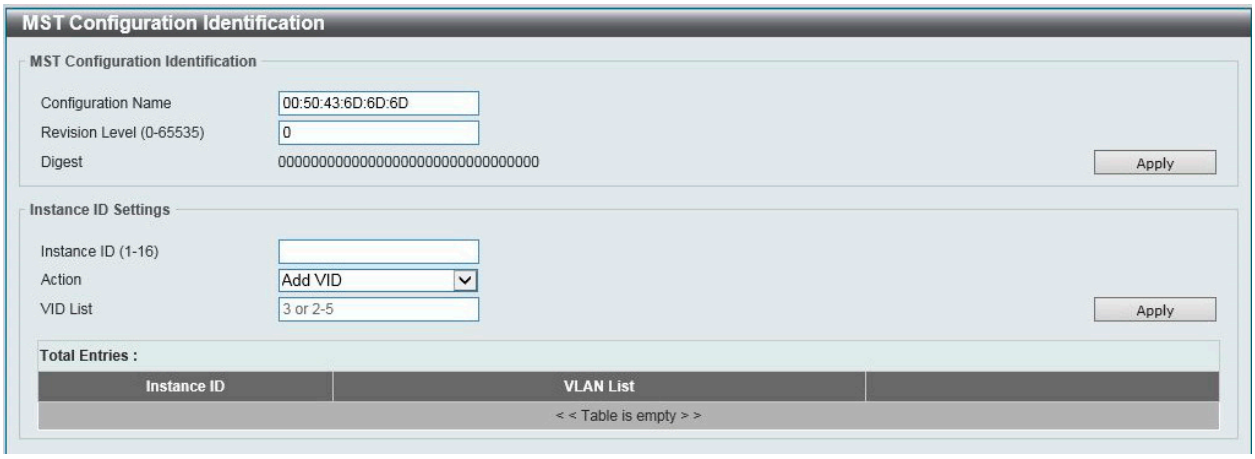


図 7-28　MST Configuration Identification 画面

上記画面には以下の項目が含まれます。

項目	説明
Configuration Name	各 MSTI（Multiple Spanning Tree Instance）を識別するためにスイッチに名前を設定します。 名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level (0-65535)	コンフィグレーション名及び STP インスタンス ID にマッピングされた識別可能な VLAN と同様に、スイッチ上に設定された MST リージョンの値を設定します。 初期値：0
Instance ID	VID リストに紐づく MSTI ID を入力します。 設定可能範囲：1-16
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 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。
「Delete」ボタンをクリックすると指定のエントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。
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。

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

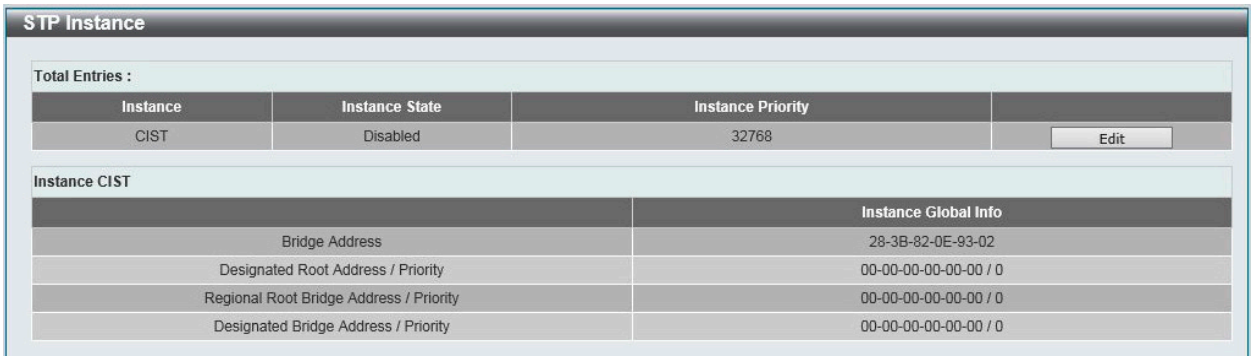


図 7-29　STP Instance 画面

本画面には以下の情報があります。

項目	説明
Edit	「Edit」をクリックして、指定エントリの編集を行います。
Instance Priority	「Edit」をクリック後、指定したインスタンスのプライオリティを設定します。 設定可能範囲：0-61440

「Apply」ボタンをクリックし、設定を適用します。
「Edit」をクリックして、指定エントリの編集を行います。
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。

MSTP Port Information（MSTP ポート情報）

本画面では、MSTP インタフェース設定を行います。

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

図 7-30　MSTP Port Information 画面

以下の項目を設定または参照できます。

項目	説明
Port	適用するポートを選択します。
Edit	「Edit」をクリックして、指定エントリの編集を行います。
Cost	「Edit」をクリック後、指定エントリのコストを設定します。
Priority	「Edit」をクリック後、指定エントリのプライオリティを設定します。

「Apply」ボタンをクリックし、設定を適用します。
「Edit」をクリックして、指定エントリの編集を行います。
「Clear Detected Protocol」ボタンをクリックし、選択したポートの検出したプロトコル設定をクリアします。
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。
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。

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、イーサネットの操作、管理、およびメンテナンス機能（OAM）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現します。

リング内の 1 つのリンク（RPL : Ring Protection Link）が、ループ 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

本項目では「Ethernet Ring Protection Switching」(ERPS) の表示、設定を行います。

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 7-31　ERPS 画面

上記画面には以下の項目が含まれます。

項目	説明
Ethernet Ring G.8032	
Instance ID（1-16）	作成するインスタンス ID を指定します。 設定可能範囲：1-16

「Apply」をクリックして設定を保存します。

注意　ERPS を有効化する前に、STP と LBD はリングポートで無効化する必要があります。

Ring の編集

1. 「Edit Instance」をクリックします。

図 7-32　ERPS 画面

2. 以下の設定画面が表示されます。

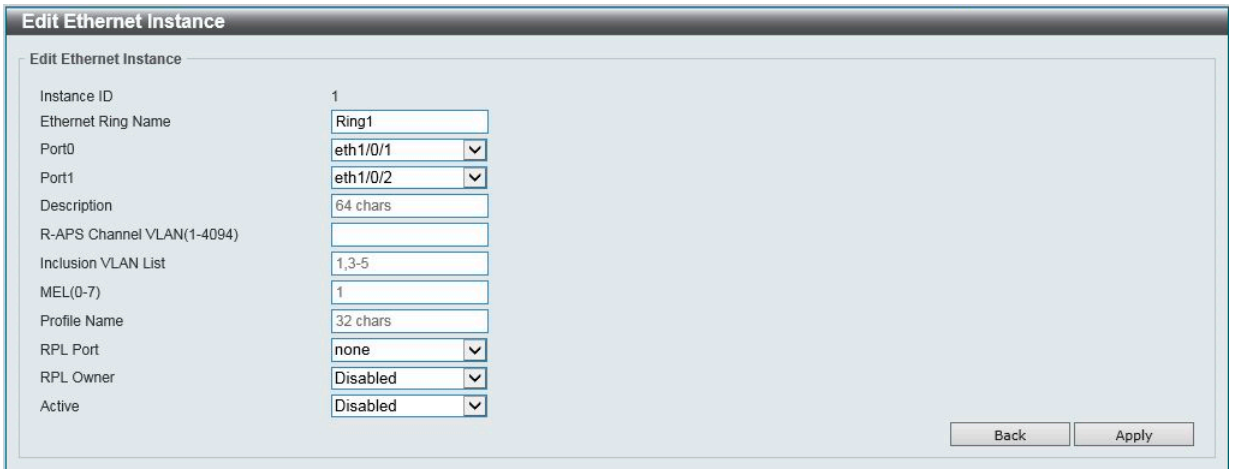


図 7-33　Edit Ethernet Instance 画面

設定対象となる項目は以下の通りです。

項目	説明
Ethernet Ring Name	インスタンスのイーサネットリング名を入力します。
Port0	初期リングポートとして、物理ポートまたは仮想ポートチャンネルを指定します。
Port1	2 番目のリングポートとして、物理ポートまたは仮想ポートチャンネルを指定します。
Description	インスタンスの概要を入力します。
R-APS Channel VLAN	ERP インスタンスの R-APS チャネルを指定します。 設定可能範囲：1-4094
Inclusion VLAN List	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。
MEL	R-APS 機能のリング MEL を指定します。 初期値：1
Profile Name	イーサネットインスタンスのプロファイル名を指定します。
RPL Port	使用する RPL ポートを指定します。選択されたオプションは RPL ポートとして設定されます。 選択肢：「Port0」「Port1」「None」
RPL Owner	RPL オーナーノードを「Enabled」（有効）/「Disabled」（無効）に設定します。
Active	ERP インスタンスを「Enabled」（有効）/「Disabled」（無効）に設定します。

「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」ボタンをクリックし、設定を適用します。

「Show Status」をクリックすると、ERPS Status 画面が表示されます。

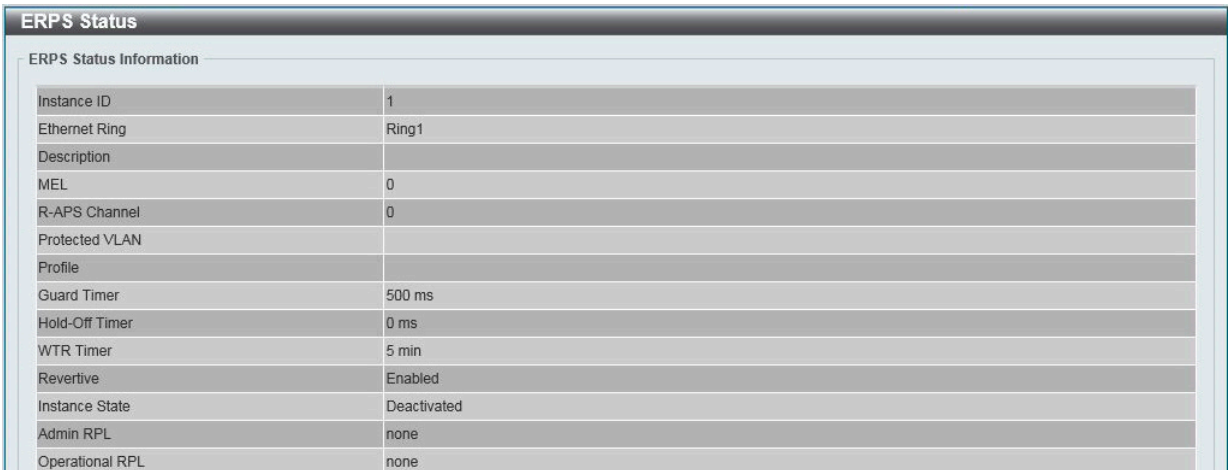


図 7-34　ERPS Status 画面

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 7-35　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」プロファイル名を指定します。32 文字まで指定可能です。

「Apply」をクリックして「G.8032」プロファイルを作成します。
「Delete」ボタンをクリックして指定の「G.8032」プロファイルを削除します。
「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

1. 「Edit Instance」をクリックします。

図 7-36　ERPS Profile 画面

2. 以下の設定画面が表示されます。

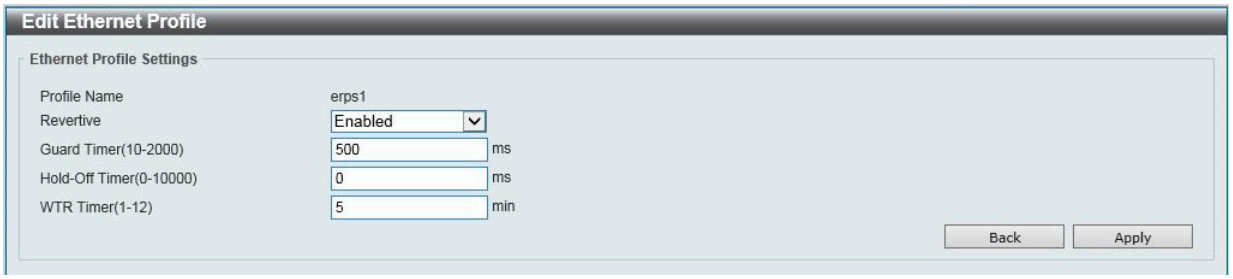


図 7-37　Edit Ethernet Profile 画面

設定対象となる項目は以下の通りです。

項目	説明
Revertive	「Revertive（切り戻し）」機能を「Enabled」（有効）/「Disabled」（無効）に設定します。RPL がブロックされた場合などの障害発生時の状態から、元の状態に戻ることを有効にします。
Guard Time	R-APS 機能の Guard Time の設定を行います。 初期値：500（ミリ秒） 設定可能範囲：10-2000（ミリ秒）
Hold-Off Timer	R-APS 機能の Hold-Off Timer の設定を行います。 初期値：0（ミリ秒） 設定可能範囲：0-10000（ミリ秒）
WTR Timer	R-APS 機能の WTR Timer の設定を行います。 初期値：5（分） 設定可能範囲：1-12（分）

「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」ボタンをクリックし、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（LBD）機能は、Spanning Tree Protocol（STP）が有効化されていない場合、特にダウンリンクがハブやアンマネスイッチである場合に、特定のポートに生成されるループを検出するために使用されます。ループが検出されると、スイッチは自動的にポートまたは VLAN をシャットダウンし、管理者にトラップを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートのロックが解除されます。ループバック検知機能は、指定のポート範囲に対してまとめて有効 / 無効に指定できます。

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。

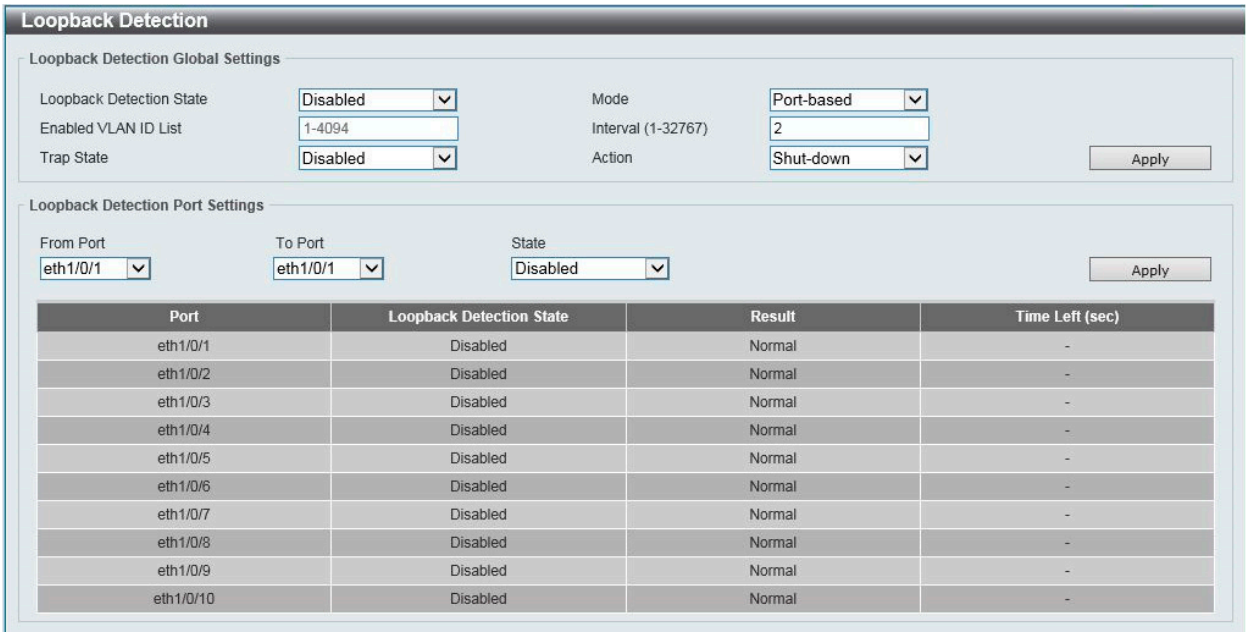


図 7-38　Loopback Detection 画面

本画面には次の項目があります。

Loopback Detection Global Settings（ループバック検出グローバル設定）

項目	説明
Loopback Detection State	ループバック検知機能を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）
Mode	検出モードを選択します。 選択肢：「Port Based」「VLAN Based」
Enable VLAN ID List	「Mode」で「VLAN ID」を選択した場合 VLAN ID のリストを入力します。
Interval (1-32767)	ループ検知間隔を設定します。 初期値：10（秒） 設定可能範囲：1-32767（秒）
Traps State	ループバック検知のトラップを「Enabled」（有効）/「Disabled」（無効）に設定します。
Action	動作モードを指定します。 • Shut-down - ループ検出時にポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックします。 • None - ループ検出時でもポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックしません。

「Apply」ボタンをクリックし、設定を適用します。

Loopback Detection Port Settings（ループバック検出ポート設定）

項目	説明
From Port/To Port	本設定を適用するポート / ポート範囲を指定します。
State	指定ポートに対し、ループバック検知機能を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）

「Apply」ボタンをクリックし、設定を適用します。

Link Aggregation（リンクアグリゲーション）

リンクアグリゲーションの設定を行います。

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

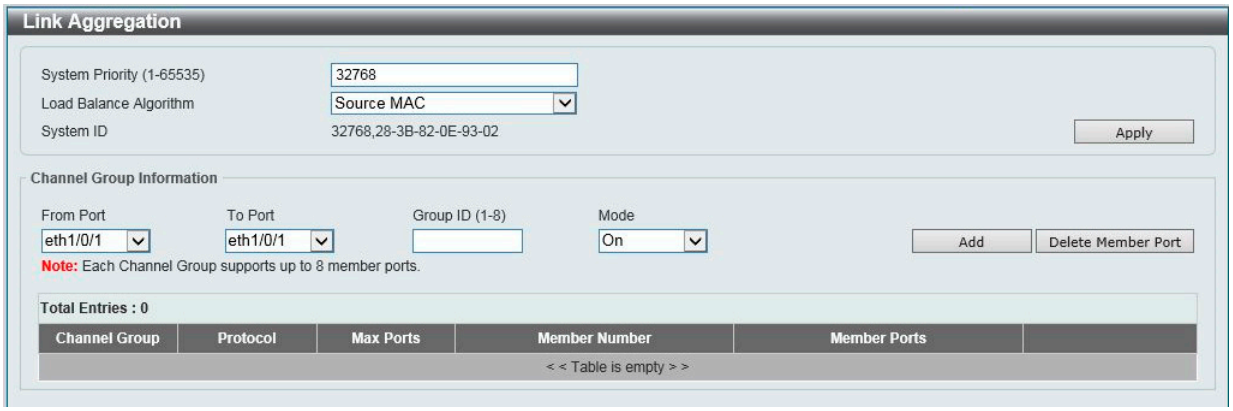


図 7-39　Link Aggregation 画面

本画面には次の項目があります。

Link Aggregation Settings（リンクアグリゲーション設定）

項目	説明
System Priority	システム優先値を指定します。システム優先値はどのポートがポートチャネルに属するか、そしてどのポートがスタンドアロンモードに入るかを決定します。低い値の方が高い優先値を示します。二つ以上のポートで同じ優先値を与えられた場合、ポート番号で優先値が決まります。 初期値：32768 設定可能範囲：1-65535
Load Balance Algorithm	ロードバランスに使用するアルゴリズムを選択します。 選択肢：「Source MAC」、「Destination MAC」、「Source Destination MAC」、「Source IP」、「Destination IP」、「Source Destination IP」 初期値：「Source MAC」
System ID	System ID 情報を表示します。

「Apply」ボタンをクリックし、設定を適用します。

Channel Group Information（チャンネルグループ設定）

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
Group ID (1-8)	チャンネルグループの ID 番号を設定します。物理ポートが初めてチャンネルグループに参加すると、ポートチャンネルが自動的に作成されます。各インタフェースは 1 つのチャンネルグループのみに参加することができます。 設定可能範囲：1-8
Mode	モードを指定します。「On」を選択した場合、チャンネルグループタイプは固定です。「Active」または「Passive」を選択した場合、チャンネルグループタイプは LACP です。チャンネルグループは固定グループか LACP グループのどちらかになります。チャンネルグループタイプが決定すると、他のタイプのインタフェースはチャンネルグループに参加することができません。 選択肢：「On」「Active」「Passive」

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。

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」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。

「Detail」をクリックすると、Port Channel 画面が表示されます。ポートチャンネルの詳細情報を確認することができます。

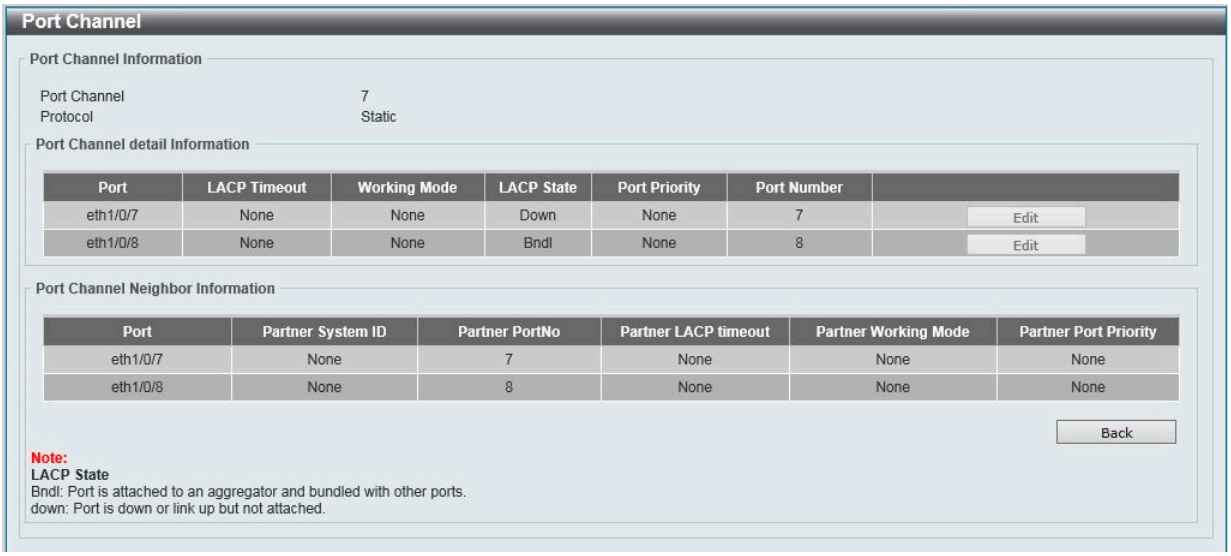


図 7-40　Port Channel 画面

編集するエントリの「Edit」ボタンをクリックします。
「Back」ボタンをクリックし前の画面に戻ります。

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

IGMP Snooping（IGMP Snooping の設定）

IGMP（Internet Group Management Protocol）Snooping 機能を利用すると、各フレームのレイヤ 2 MAC ヘッダコンテンツを検査して、インテリジェントなマルチキャスト転送を行うことができます。IGMP スヌーピング機能により、LAN 上の無駄なトラフィックを削減することが可能です。本機能をグローバルに有効化すると、マルチキャストトラフィックはグループメンバの所属するポートのみに転送されます。
IGMP スヌーピングは VLAN 毎に設定することができます。

IGMP Snooping Settings（IGMP Snooping 設定）

IGMP Snooping 設定をグローバルに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、画面上にある「IGMP Snooping Global Settings」でスイッチ全体を有効にする必要があります。その後、対応する「Edit」ボタンをクリックして、各 VLAN に詳細な設定を行います。

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 7-41　IGMP Snooping Settings 画面

本画面には以下の項目があります。

Global Setting（グローバル設定）

項目	説明
Global State	IGMP Snooping を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）

「Apply」ボタンをクリックし、設定を適用します。

VLAN Status Settings（VLAN ステータス設定）

項目	説明
VID	VLAN ID を入力し、IGMP Snooping を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）

「Apply」ボタンをクリックし、設定を適用します。

IGMP Snooping Table（IGMP スヌーピング設定）

項目	説明
VID	IGMP Snooping Table 上で表示する VLAN の VLAN ID を指定します。 設定可能範囲：1-4094

「Find」をクリックして、指定した VLAN ID のエントリを表示します。
「Find All」をクリックして IGMP Snooping Table 上のすべてのエントリを表示します。

IGMP Snooping VLAN の詳細情報表示

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

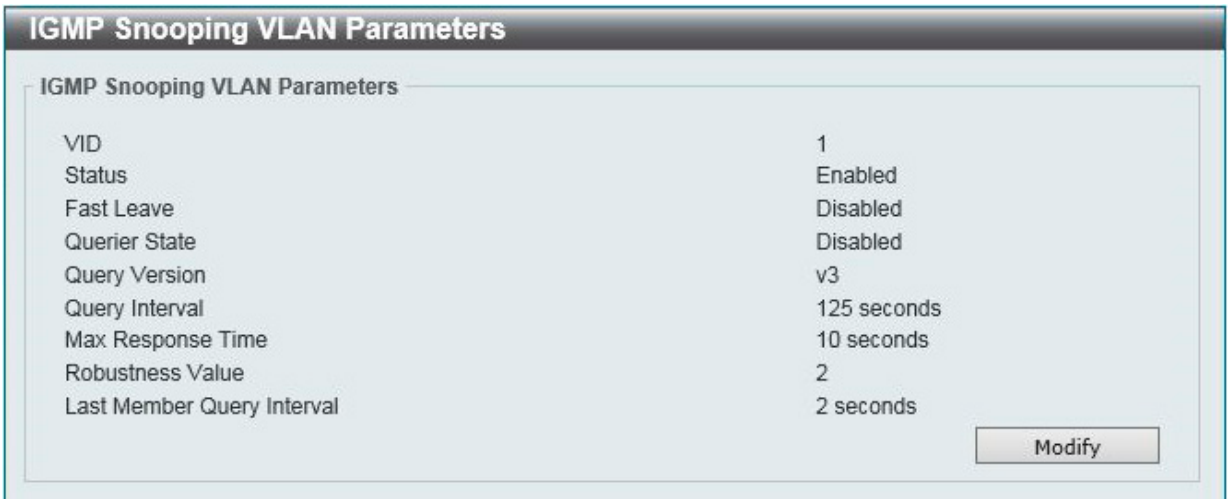


図 7-42　IGMP Snooping VLAN Parameters 画面

本画面の「Modify」をクリックすると「IGMP Snooping VLAN Settings」画面へ移動し、IGMP Snooping の VLAN 設定を行うことができます。

IGMP Snooping 機能の詳細設定

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

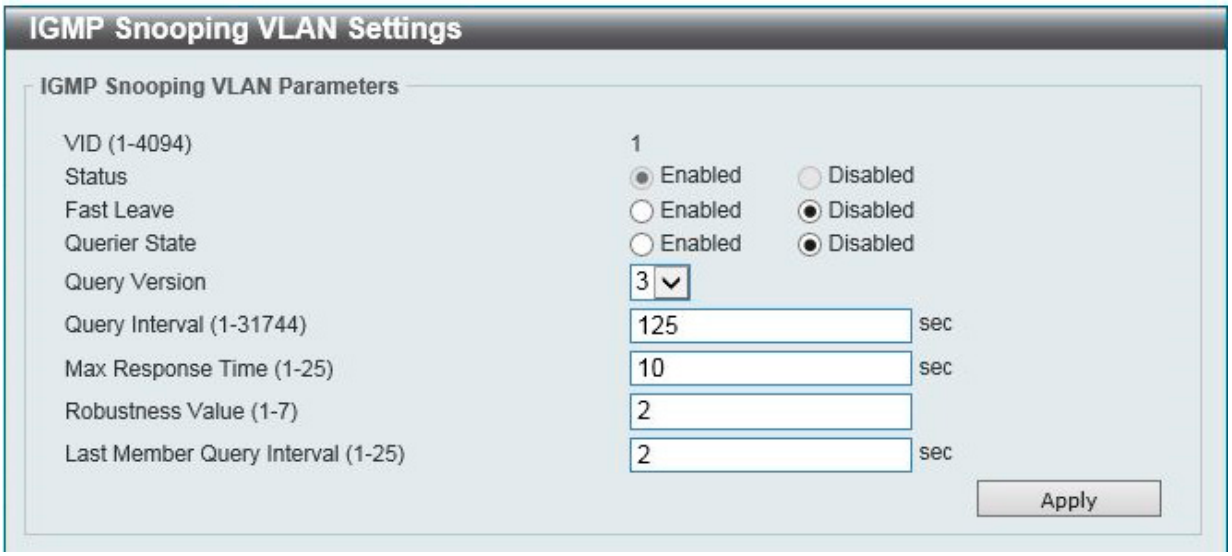


図 7-43 IGMP Snooping VLAN Settings 画面

本画面には次の項目があります。

項目	説明
VID	設定対象の VLAN ID を表示します。
Status	IGMP Snooping 機能のステータスを表示します。
Fast Leave	Fast Leave 機能を「Enabled」（有効）/「Disabled」（無効）にします。

項目	説明
Querier State	IGMP クエリア機能を「Enabled」（有効）/「Disabled」（無効）にします。 初期値：「Disabled」（無効）
Query Version	IGMP スヌーピングクエリアに送信されるクエリパケットのバージョンを選択します。 選択肢：「1」「2」「3」
Query Interval	IGMP query 送信間隔を指定します。IGMP Snooping クエリアが IGMP General Query メッセージを定期的に送る間隔を示します。 初期値：125（秒） 設定可能範囲：1-31744（秒）
Max Response Time (1-25)	IGMP Snooping クエリアが IGMP General Query メッセージを送信するまでの最大時間を指定します。 初期値：10（秒） 設定可能範囲：1-25（秒）
Robustness Value (1-7)	IGMP Snooping の Robustness Variable を指定します。本値は、パケットロスへの抵抗力を示します。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。 初期値：2 設定可能範囲：1-7
Last Member Query Interval (1-25)	IGMP Snooping クエリアが、Group-Specific または Group-Source-Specific クエリメッセージを送る間隔を指定します。

「Apply」ボタンをクリックし、設定を適用します。

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

IGMP Snooping スタティックグループの設定と表示を行います。

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

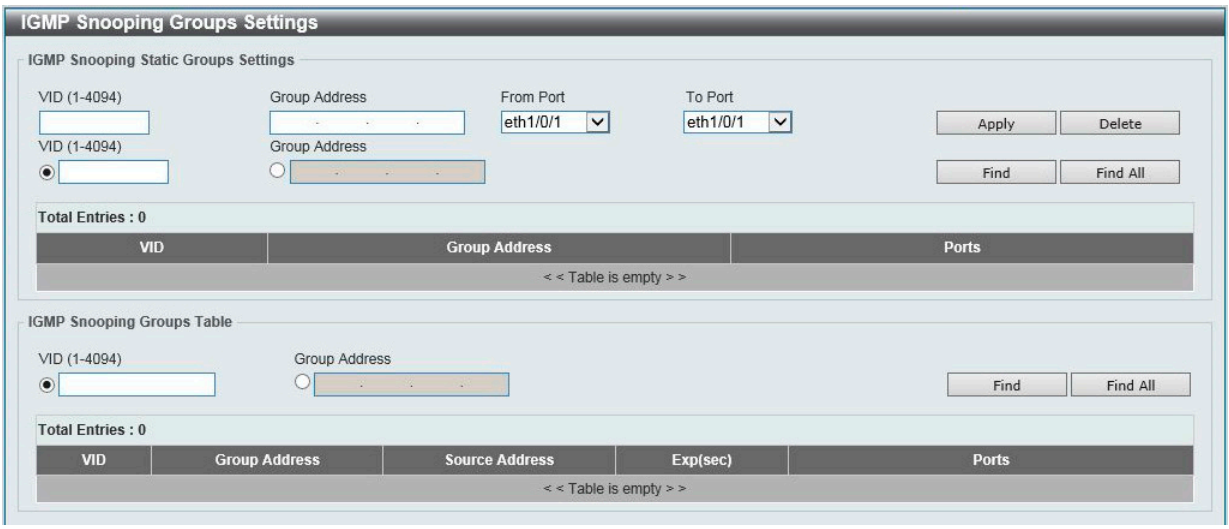


図 7-44　IGMP Snooping Groups Settings 画面

本画面には次の項目があります。

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
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	本設定を適用するポート / ポート範囲を指定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。

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

IGMP Snooping Groups Table（IGMP スヌーピンググループテーブル）

項目	説明
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。

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

IGMP Snooping Mrouter Settings（IGMP Snooping マルチキャストルータ設定）

指定インタフェースをマルチキャストルータポートへの移行、もしくはマルチキャストルータポートへの移行禁止に設定します。

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

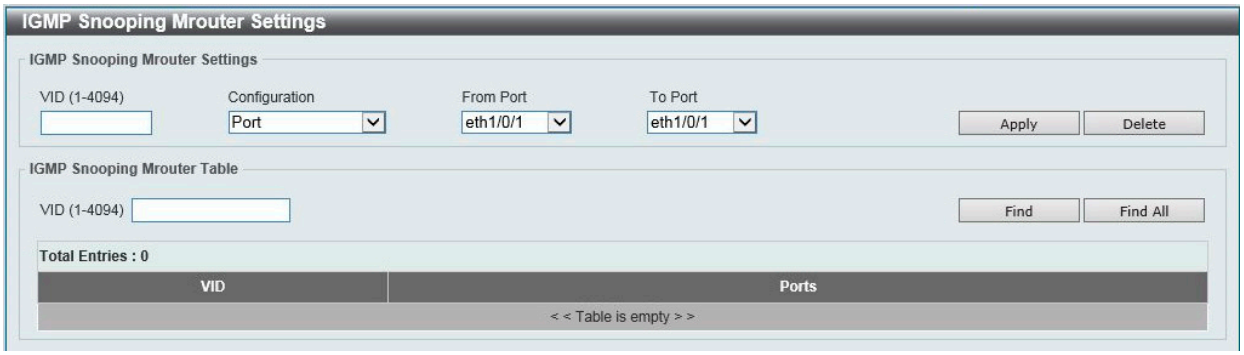


図 7-45　IGMP Snooping Mrouter Settings 画面

画面には以下の項目があります。

IGMP Snooping Mrouter Settings（IGMP スヌーピングマルチキャストルータ設定）

項目	説明
VID	VLAN ID を入力します。 設定可能範囲：1-4094
Configuration	ポートの設定を行います。「Port」「Forbidden Port」から選択します。 • Port - スタティックなマルチキャストルータポートとして指定します。 • Forbidden Port - スタティックなマルチキャストルータポートとして指定しません。
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。

「Apply」ボタンをクリックし、設定を適用します。
「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。
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。

IGMP Snooping Mrouter Table（IGMP スヌーピングマルチキャストルータテーブル）

項目	説明
VID	VLAN ID を入力します。

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

IGMP Snooping Statistics Settings（IGMP Snooping 統計設定）

現在の IGMP Snooping の統計情報を表示します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics 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。

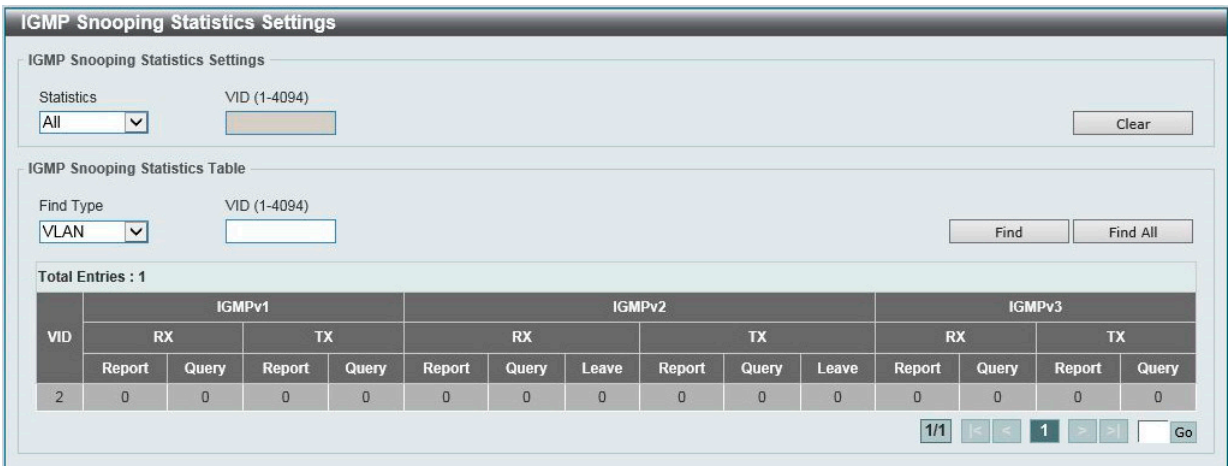


図 7-46　IGMP Snooping Statistics Settings 画面

本画面には次の項目があります。

IGMP Snooping Statistics Settings（IGMP スヌーピング統計設定）

項目	説明
Statistics	インタフェースの種類を選択します。 選択肢：「All」「VLAN」
VID	VLAN ID を指定します。「Statistics」で「VLAN」を選択すると指定可能になります。 設定可能範囲：1-4094

「Clear」をクリックすると、指定されたエントリの統計情報がクリアされます。

IGMP Snooping Statistics Table（IGMP スヌーピング統計テーブル）

項目	説明
Find Type	インタフェースの種類を選択します。 選択肢：「VLAN」
VID	VLAN ID を指定します。「Find Type」で「VLAN」を選択すると設定可能になります。 設定可能範囲：1-4094

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

MLD Snooping（MLD Snooping 設定）

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。

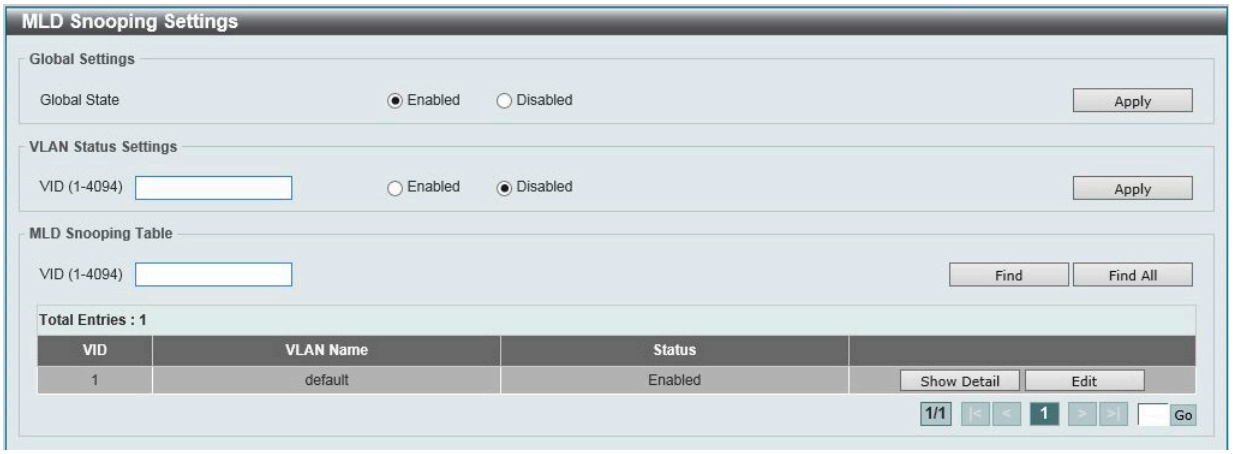


図 7-47　MLD Snooping Settings 画面

本画面には以下の項目があります。

Global Setting（グローバル設定）

項目	説明
Global State	MLD Snooping を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）

「Apply」ボタンをクリックし、設定を適用します。

VLAN Status Settings（VLAN ステータス設定）

項目	説明
VID	VLAN ID を指定し、この VLAN 上の MLD Snooping を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

MLD Snooping Table（MLD スヌーピングテーブル）

項目	説明
VID	MLD Snooping Table 上に表示する VLAN の VLAN ID を指定します。 設定可能範囲：1-4094

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。
「Find All」をクリックして MLD Snooping Table 上のすべてのエントリを表示します。

MLD Snooping VLAN の詳細情報表示

関連する VLAN エントリの「Show Detail」ボタンをクリックし、指定 VLAN の詳細情報を表示します。

図 7-48　MLD Snooping VLAN Parameters 画面

本画面の「Modify」をクリックすると「MLD Snooping VLAN Settings」画面へ移動し、MLD Snooping の VLAN 設定を行うことができます。

MLD Snooping 機能の詳細設定

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

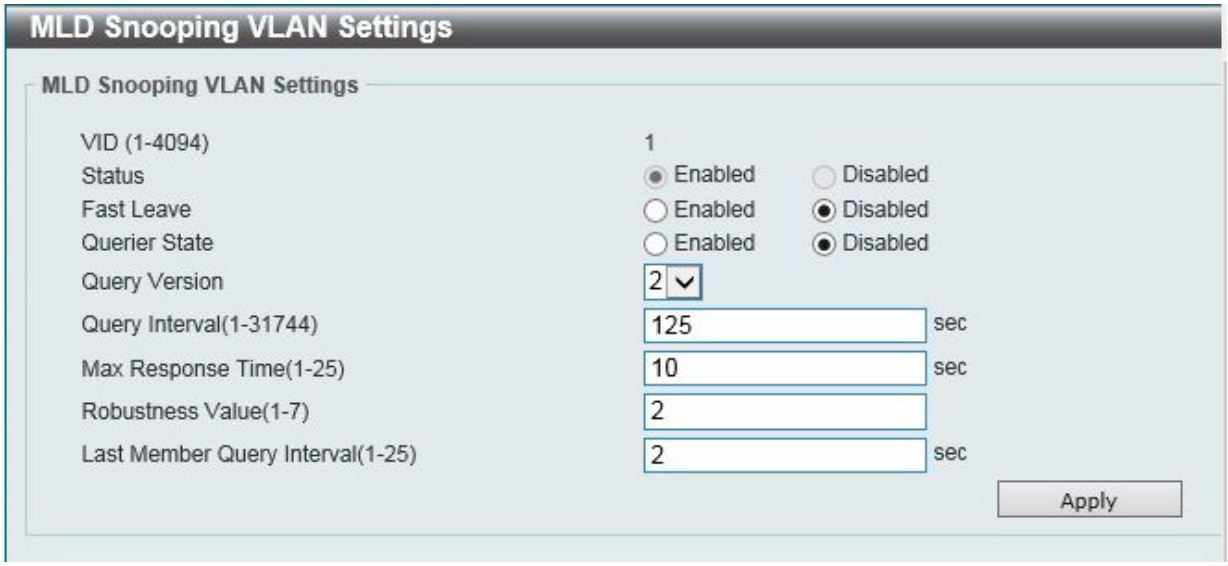


図 7-49 MLD Snooping VLAN Settings 画面

本画面には次の項目があります。

項目	説明
VID	MLD Snooping 設定を変更する VLAN の VLAN ID が表示されます。
Status	指定した VLAN の MLD Snooping 機能の有効 / 無効状態が表示されます。
Fast Leave	Fast Leave 機能を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）
Querier State	MLD Query パケットの送信を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）
Query Version	MLD スヌーピングクエリアに送信されるクエリパケットのバージョンを選択します。 選択肢：「1」「2」
Query Interval	MLD query 送信間隔を指定します。 初期値：125（秒） 設定可能範囲：1-31744（秒）
Max Response Time (1-25)	MLD スヌーピングクエリでアドバタイズされる最大応答時間を指定します。 初期値：10（秒） 設定可能範囲：1-25（秒）
Robustness Value (1-7)	MLD スヌーピングで使用される Robust Variable 値を指定します。予想されるパケット損失率が高い場合、大きい値を取ります。 初期値：2 設定可能範囲：1-7
Last Member Query Interval	MLD Snooping クエリアが MLD Group-Specific Query メッセージまたは Group-Source-Specific (Channel) Query メッセージを送信する間隔を指定します。 初期値：2

「Apply」ボタンをクリックし、設定を適用します。

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

MLD Snooping スタティックグループの設定・表示を行います。

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

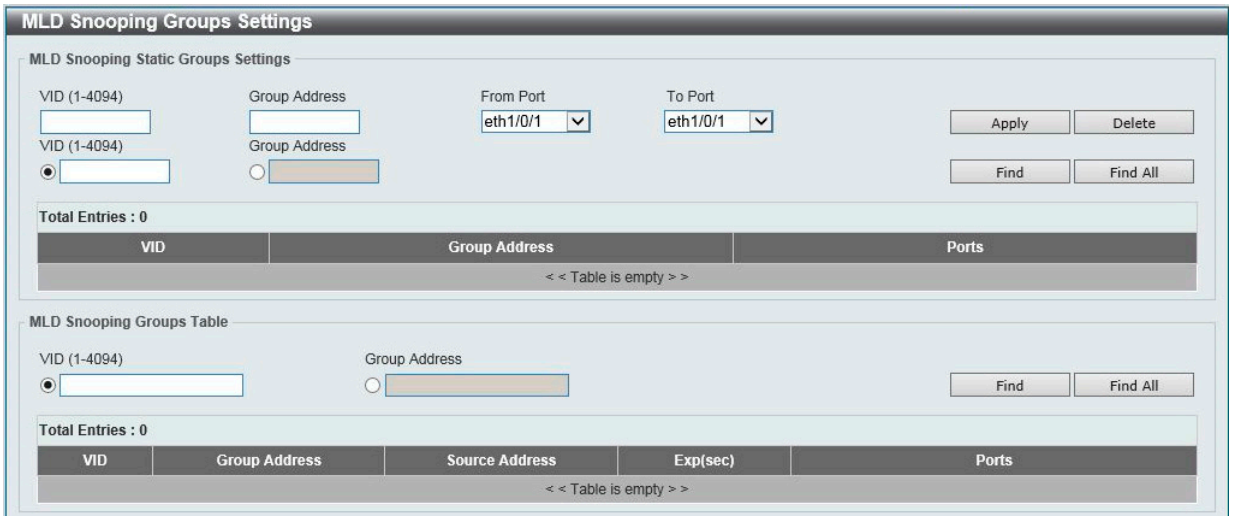


図 7-50　MLD Snooping Groups Settings 画面

本画面には次の項目があります。

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
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 を指定します。
Group Address	登録または削除する IPv6 マルチキャストグループの IPv6 アドレスを指定します。
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。

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

MLD Snooping Groups Table（MLD スヌーピンググループテーブル）

項目	説明
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 設定可能範囲：1-4094
Group Address	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。

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

MLD Snooping Mrouter Settings（MLD Snooping マルチキャストルータ設定）

指定インタフェースをマルチキャストルータポートへの移行、もしくはマルチキャストルータポートへの移行禁止に設定します。

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

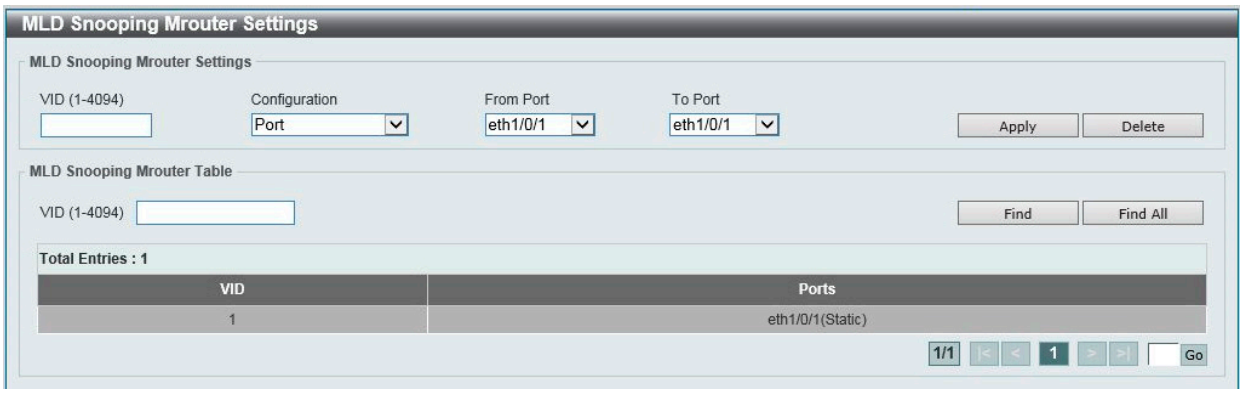


図 7-51　MLD Snooping Mrouter Settings 画面

画面には以下の項目があります。

MLD Snooping Mrouter Settings（MLD スヌーピングマルチキャストルータ設定）

項目	説明
VID	VLAN ID を入力します。
Configuration	ポートの設定を行います。「Port」「Forbidden Port」から選択します。 • Port - マルチキャストが有効なルータと接続するポート範囲を設定します。 • Forbidden Port - マルチキャストが有効なルータと接続しないポート範囲を設定します。
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。

「Apply」ボタンをクリックし、設定を適用します。
「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 Mrouter Table（MLD スヌーピングマルチキャストルータテーブル）

項目	説明
VID	VLAN ID を入力します。 設定可能範囲：1-4094

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

MLD Snooping Statistics Settings（MLD Snooping 統計設定）

現在の MLD Snooping の統計情報を表示します。

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

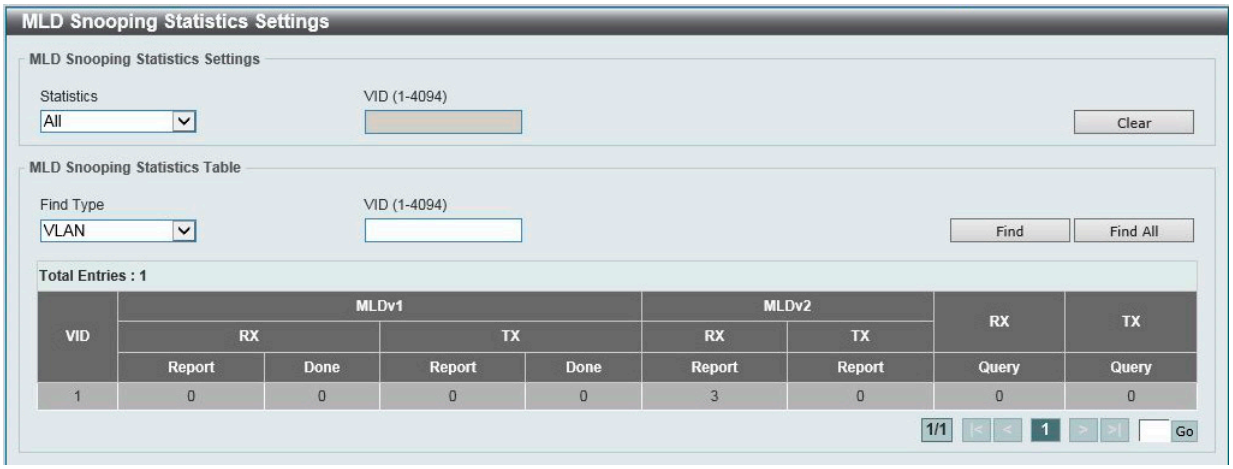


図 7-52　MLD Snooping Statistics Settings 画面

本画面には次の項目があります。

MLD Snooping Statistics Settings（MLD スヌーピング統計設定）

項目	説明
Statistics	インタフェースを選択します。 選択肢：「All」「VLAN」
VID	VLAN ID を指定します。「Statistics」で「VLAN」を選択すると設定可能になります。 設定可能範囲：1-4094

「Clear」をクリックすると表示された統計情報がクリアされます。

MLD Snooping Statistics Table（MLD スヌーピング統計テーブル）

項目	説明
Find Type	インタフェースを選択します。 選択肢：「VLAN」
VID	VLAN ID を指定します。「Find Type」で「VLAN」を選択すると設定可能になります。 設定可能範囲：1-4094

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

LLDP

Link Layer Discovery Protocol（LLDP）は、IEEE 802.1AB 標準規格に準拠した、隣接するデバイス同士で通知を行う機能です。
SNMP ユーティリティが各 LLDP 対応デバイスの MIB 情報を取得し、ネットワークトポロジを学習することができます。LLDP 機能はデフォルトで有効化されています。

LLDP Global Settings（LLDP グローバル設定）

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。

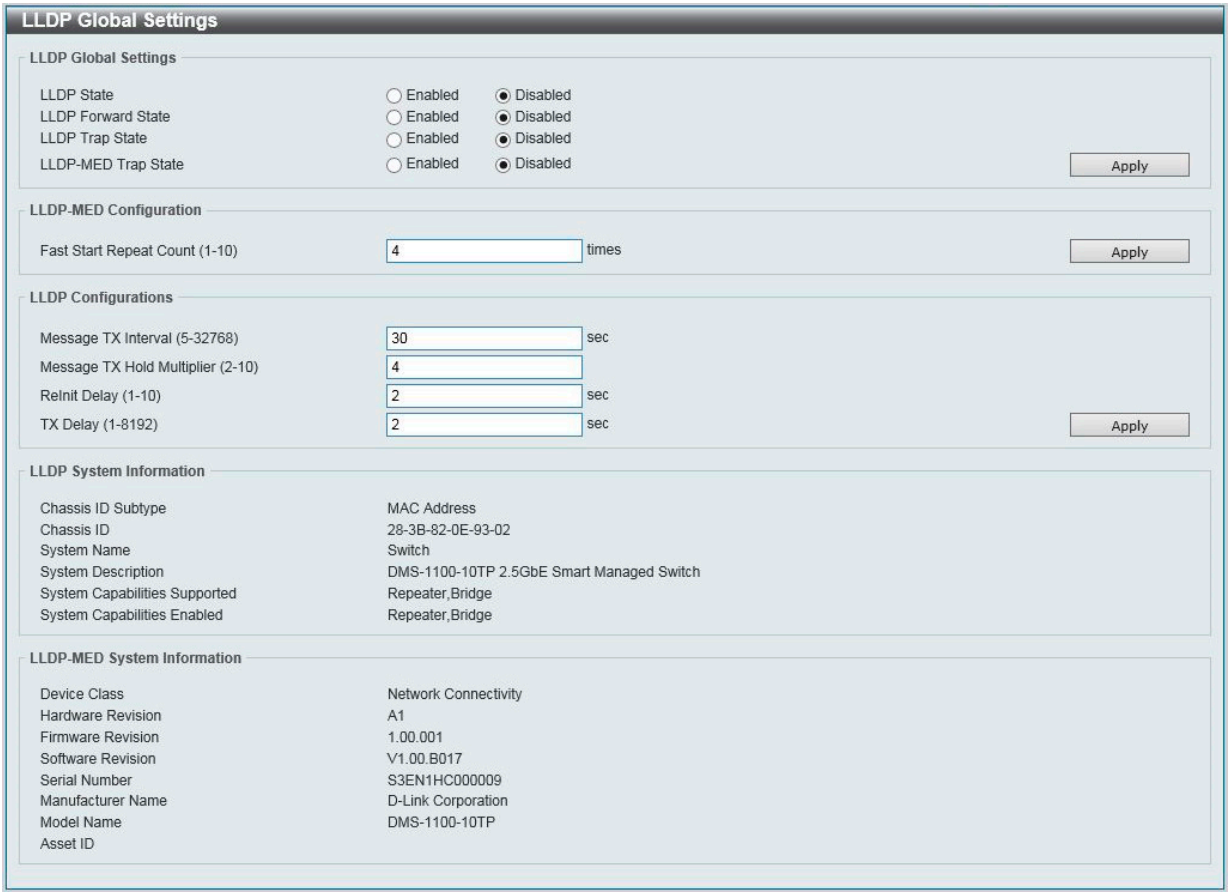


図 7-53　LLDP Global Settings 画面

本画面には以下の項目があります。

LLDP Global Settings（LLDP グローバル設定）

項目	説明
LLDP State	スイッチにおける LLDP 機能を「Enabled」（有効）/「Disabled」（無効）に設定します。
LLDP Forward State	同じ IEEE 802 ネットワークに割り当てられた他のステーションに通知するために LLDP 機能のメッセージ転送を「Enabled」（有効）/「Disabled」（無効）に設定します。 「LLDP」が 無効で「LLDP Forward State」が有効の場合、受信した「LLDPDU」パケットは転送されます。
LLDP Trap State	LLDP Trap を「Enabled」（有効）/「Disabled」（無効）に設定します。
LLDP-MED Trap State	LLDP-MED Trap を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

LLDP-MED Configration（LLDP-MED 設定）

項目	説明
Fast Start Repeat Count	「LLDP-MED」ファストスタートリピートカウント値を指定します。 設定可能範囲：1-10

「Apply」ボタンをクリックし、設定を適用します。

LLDP Configurations（LLDP 設定）

項目	説明
Message TX Interval (5-32768)	LLDP フレームが送信される間隔を指定します。 初期値：30（秒） 設定可能範囲：5-32768（秒）

項目	説明
Message TX Hold Multiplier (2-10)	LLDPDU で使用される TTL 値を決定するための乗数を指定します。 初期値：4
Relnit Delay (1-10)	adminStatus が無効となってから再初期化が行われるまでの遅延時間を指定します。 初期値：2（秒） 設定可能範囲：1-10（秒）
TX Delay (1-8192)	LLDP ローカルシステム MIB の値やステータス変更によって送信される、連続した LLDP フレームの遅延時間を設定します。 初期値：2（秒） txDelay の値は以下の計算式による範囲に設定されます。 1 < txDelay < (0.25 × msgTxInterval)

「Apply」ボタンをクリックし、設定を適用します。

LLDP Port Settings（LLDP ポート設定）

LLDP ポートパラメータを設定します。

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

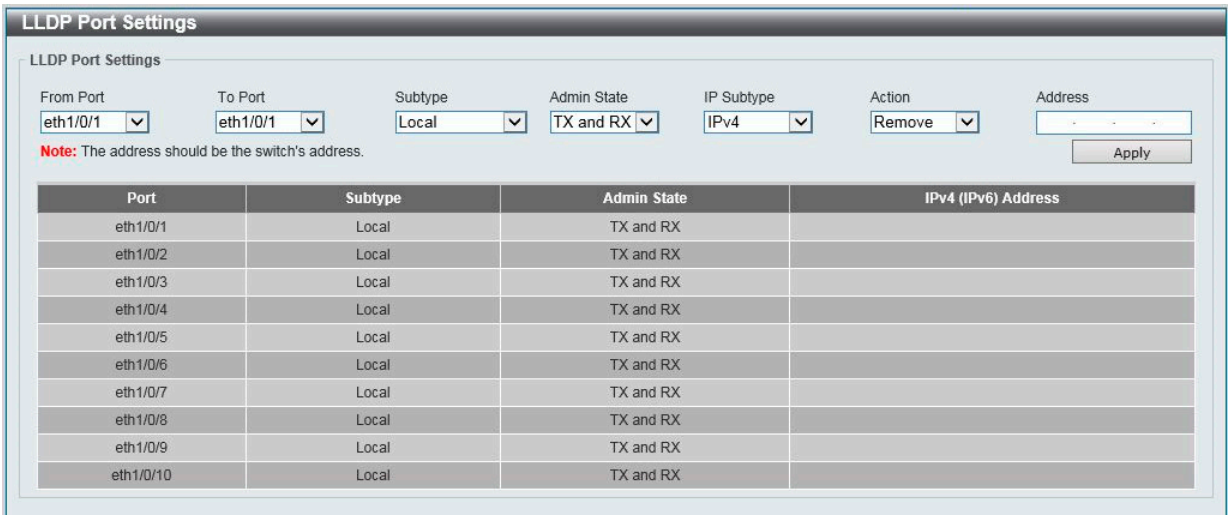


図 7-54　LLDP Port Settings 画面

本画面には次の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート / ポート範囲を指定します。
Subtype	プルダウンメニューから LLDP TLV(s) のサブタイプを選択します。 選択肢：「Local」「MAC Address」
Admin State	プルダウンメニューから通知のステータスを選択します。 • TX - LLDP フレームの送信のみ有効にします。 • RX - LLDP フレームの受信のみ有効にします。 • TX and RX - LLDP フレームの送受信を有効にします。 • Disabled - LLDP フレームの送受信を無効にします。 初期値：「TX and RX」
IP Subtype	送信する IP アドレスの種類を選択します。 選択肢：「IPv4」「IPv6」
Action	以下の設定を行います。 • Remove - 指定したアドレスを削除します。 • Add - 指定したアドレスを追加します。
Address	送信される IP アドレスを入力します。

「Apply」ボタンをクリックし、変更を有効にします。

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

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

図 7-55　LLDP Management Address List 画面

本画面には次の項目があります。

項目	説明
Management Address	表示する LLDP 管理 IP アドレスのサブタイプを選択します。 選択肢：「IPv4」「IPv6」「All」
Subtype	管理アドレスのサブタイプを表示します。（例：MAC、IPv4）
Address	IP アドレスを表示します。
IF Type	IF Type を表示します。
OID	SNMP OID を表示します。
Advertising Ports	アドバタイズポートを表示します。

「Find」ボタンをクリックし、LLDP 管理情報を検索します。

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

LLDP ベーシック TLV の設定を行います。

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

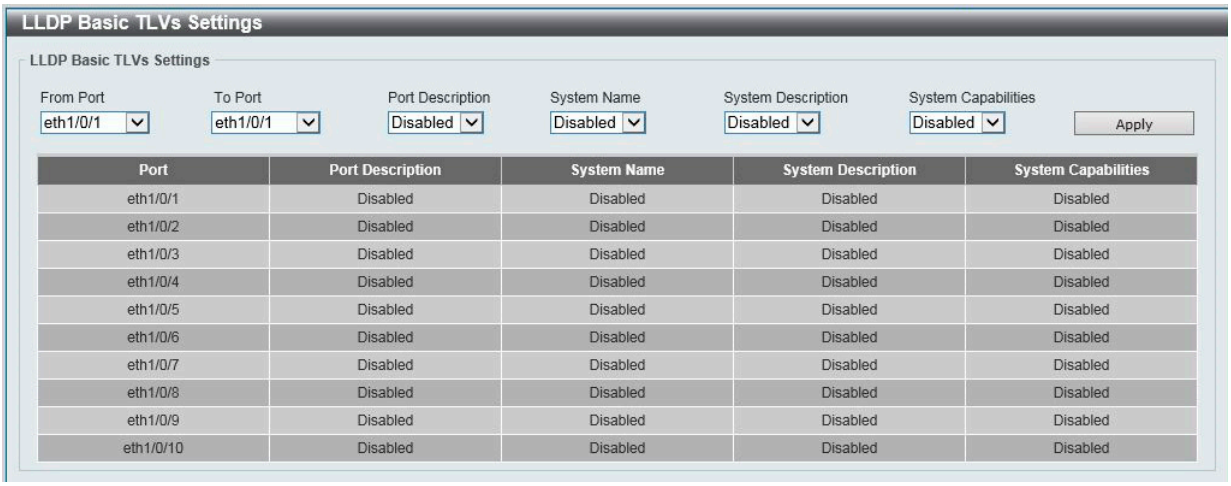


図 7-56　LLDP Basic TLVs Settings 画面

本画面には次の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート / ポート範囲を指定します。
Port Description	ポート説明 TLV を「Enabled」（有効）/「Disabled」（無効）に設定します。
System Name	システム名 TLV を「Enabled」（有効）/「Disabled」（無効）に設定します。
System Description	システム説明 TLV を「Enabled」（有効）/「Disabled」（無効）に設定します。
System Capabilities	システム機能 TLV を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

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

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

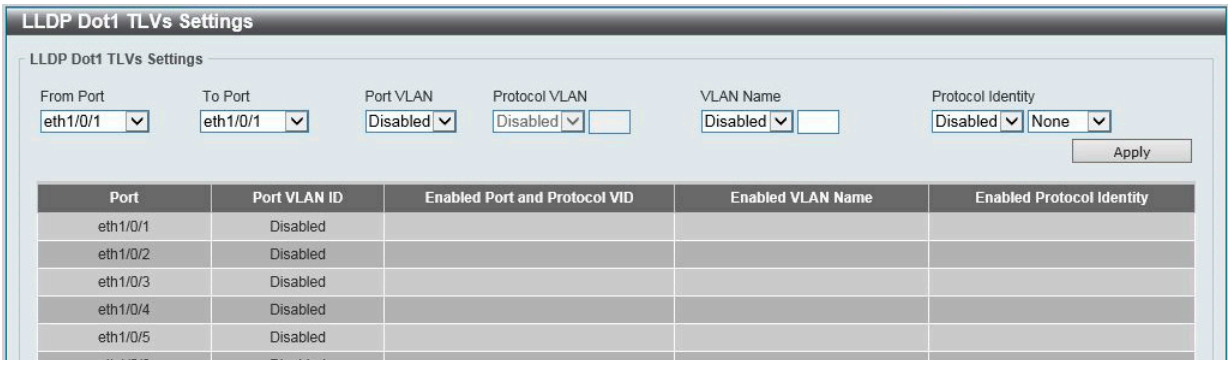


図 7-57　LLDP Dot1 TLVs Settings 画面

本画面には次の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート / ポート範囲を指定します。
Port VLAN	ポート VLAN ID TLV の通知を「Enabled」（有効）/「Disabled」（無効）に設定します。 「ポート VLAN ID TLV」は VLAN ブリッジポートにタグなし・タグ付きフレームの PVID の通知を許可するオプションのフィックス長 TLV です。
Protocol VLAN	本製品ではサポートされていません。
VLAN Name	VLAN 名の通知を「Enabled」（有効）/「Disabled」（無効）に設定します。右の欄で対象となるプロトコル VLAN ID（PVID）を指定します。
Protocol Identity	プロトコル識別子の通知を「Enabled」（有効）/「Disabled」（無効）に設定し、対象とするプロトコルを選択します。 選択肢：「None」「EAPOL」「LACP」「GVRP」「STP」「All」

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

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

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

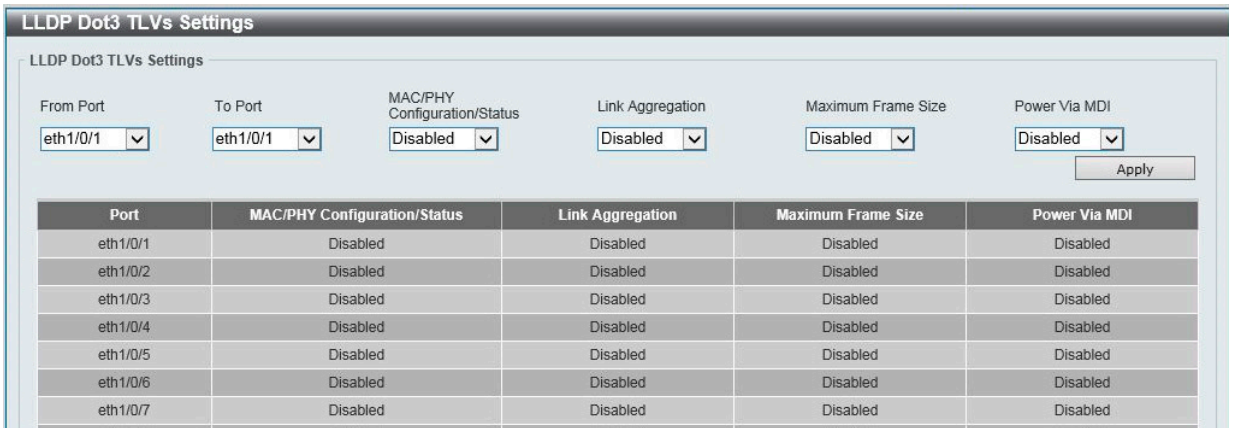


図 7-58　LLDP Dot3 TLVs Settings 画面

本画面には次の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート / ポート範囲を指定します。
MAC/PHY Configuration Status	スイッチの MAC または PHY 状態の通知を「Enabled」（有効）/「Disabled」（無効）に設定します。
Link Aggregation	スイッチのリンクアグリゲーション状態の通知を「Enabled」（有効）/「Disabled」（無効）に設定します。
Maximum Frame Size	最大フレームサイズの通知を「Enabled」（有効）/「Disabled」（無効）に設定します。
Power Via MDI	Power Via MDI 実装の通知を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP-MED Port Settings（LLDP-MED ポート設定）

LLDP-MED TLV の送信を有効または無効にします。

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

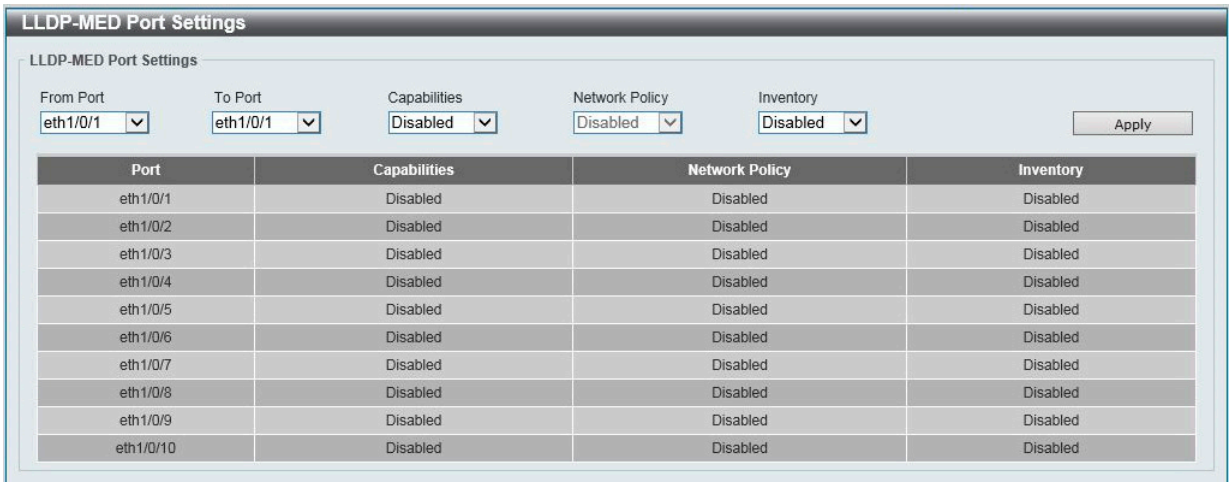


図 7-59　LLDP-MED Port Settings 画面

本画面には次の項目があります。

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
Capabilities	「LLDP-MED capabilities TLV」の送信を「Enabled」（有効）/「Disabled」（無効）に設定します。
Network Policy	「LDP-MED network policy TLV」の送信を「Enabled」（有効）/「Disabled」（無効）に設定します。
Inventory	「LLDP-MED inventory management TLV」の送信を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックして変更を適用します。

LLDP Statistics Information（LLDP 統計情報）

LLDP 統計情報を表示します。

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

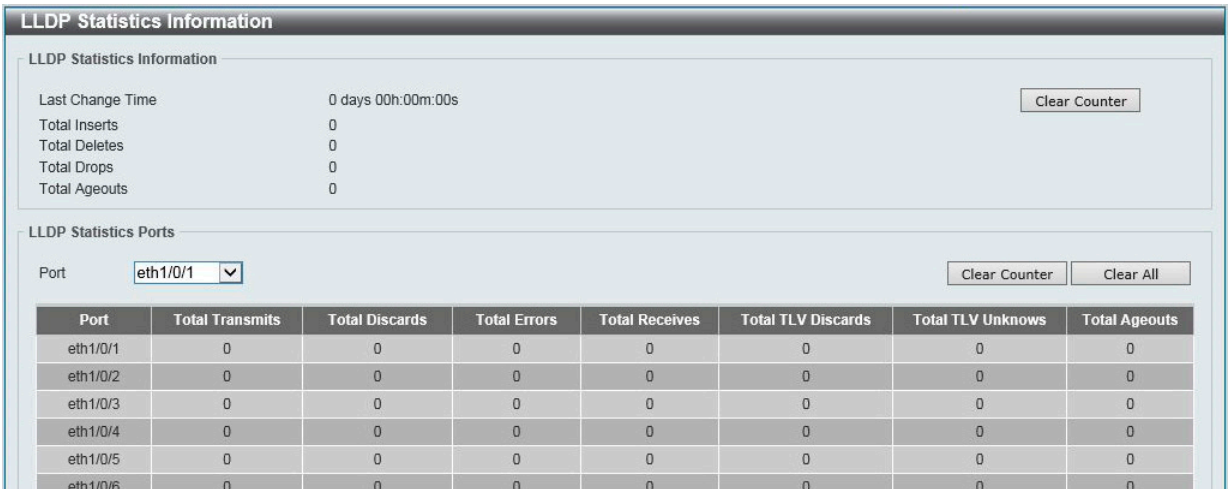


図 7-60　LLDP Statistics Information 画面

本画面には次の項目があります。

LLDP Statistics Information（LLDP 統計情報）

項目	説明
Last Change Time	変更が検出されてから経過した時間を表示します。
Total Inserts	スイッチ起動後の新しいエントリ数を表示します。
Total Deletes	スイッチ起動後の削除エントリを表示します。
Total Drops	テーブルが一杯になったことで廃棄された LLDP フレーム数を表示します。
Total Ageouts	TTL 超過により削除されたエントリ数を表示します。

「Clear Counter」をクリックして統計情報のカウンタ数をクリアします。

LLDP port Statistics（LLDP ポート統計）

項目	説明
Port	表示するポートを指定します。
Total Transmits	ポート上で送信された LLDP フレーム合計数を表示します。
Total Discards	ポート上で受信された LLDP フレーム合計廃棄数を表示します。
Total Errors	ポート上で受信された LLDP エラーフレーム数を表示します。
Total Receives	ポート上で受信された LLDP フレーム合計数を表示します。
Total TLV Discards	各 LLDP には TLV と呼ばれる情報が含まれます。TLV が不正な場合、カウントされ廃棄されます。
Total TLV Unknowns	正しいフォーマットかつ不明な Type 値の TLV 数を表示します。
Total Ageouts	LLDP には、保持する情報の有効期間があります。エージアウト時間内に新しい LLDP フレームを受信しないと、LLDP 情報は削除され、Age-Out カウンタが増加します。

「Clear Counter」をクリックして統計情報のカウンタ数をクリアします。
「Clear All」をクリックしてすべてのカウンタ数をクリアします。

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

LLDP ローカルポート情報を表示します。

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

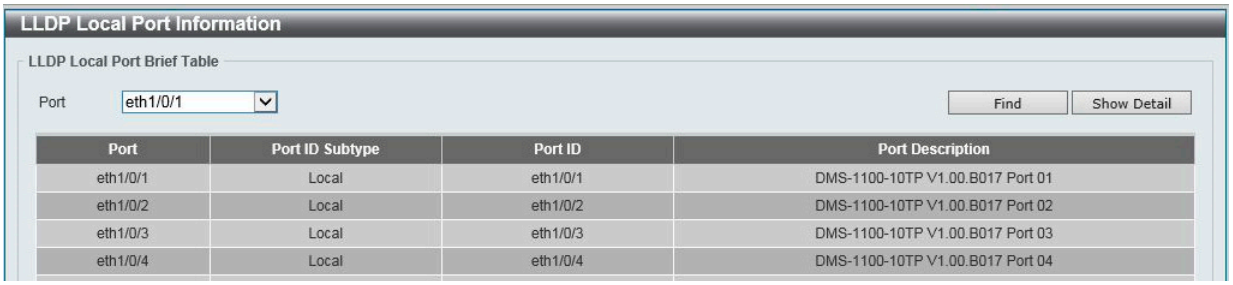


図 7-61　LLDP Local Port Information 画面

画面上部の「Port」で表示するポートを指定し、「Find」ボタンをクリックします。

本画面には次の項目があります。

項目	説明
Port	ポート番号を表示します。
Port ID Subtype	ポート ID サブタイプを表示します。
Port ID	ポート ID を表示します。（ポート番号）
Port Description	ポートの説明を表示します。

各パラメータの詳細の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。

図 7-62　LLDP Local Port Information（Show Detail）画面

各項目の情報の参照

各項目のリンクをクリックすると、画面下部に詳細が表示されます。

図 7-63　LLDP Local Port Information - MAC/PHY Configuration/Status 画面

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

送信する LLDP アドバタイズ情報を格納するための、ポート毎の基本情報を表示します。

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 7-64　LLDP Neighbor Port Information 画面

本画面には次の項目があります。

項目	説明
Port	表示するポートを指定します。

ポートを選択し、「Find」ボタンをクリックします。情報が画面下半分に表示されます。

「Clear」をクリックして特定の LLDP ネイバポート情報をクリアします。

「Clear All」をクリックして全ての LLDP ネイバポート情報をクリアします。

第 8 章　L3 Features（L3 機能の設定）

本メニューでは、レイヤ 3 機能に関する設定を行います。

以下は L3 Features サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
IPv4 Interface（IPv4 インタフェース）	IPv4 アドレスのインタフェースの設定を行います。
IPv4 Default Gateway（IPv4 デフォルトゲートウェイ）	IPv4 デフォルトゲートウェイの設定を行います。
IPv6 Interface（IPv6 インタフェース）	IPv6 アドレスのインタフェースの設定を行います。
IPv6 Default Gateway（IPv6 デフォルトゲートウェイ）	IPv6 デフォルトゲートウェイの設定を行います。

IPv4 Interface（IPv4 インタフェース）

スイッチの IPv4 インタフェース設定を行います。

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

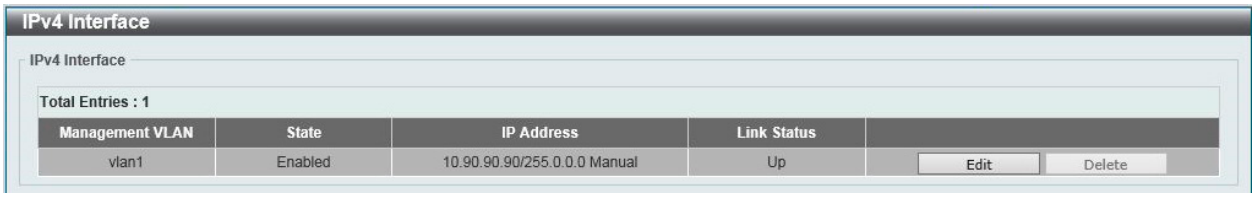


図 8-65　IPv4 Interface 画面

「Edit」ボタンをクリックすると、「IPv4 Interface Configuration」画面でインタフェースの編集を行うことができます。

IPv4 インタフェースの編集（IPv4 Interface Settings）

「IPv4 Interface Configuration」画面で「IPv4 Interface Settings」タブをクリックして以下の画面を表示します。

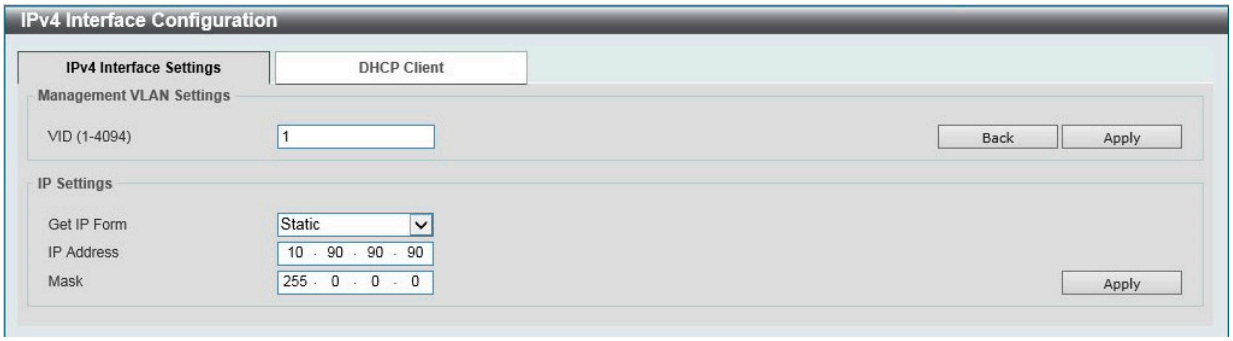


図 8-66　IPv4 Interface (Edit) 画面

本画面には次の項目があります。

Management VLAN Settings（管理 VLAN 設定）

項目	説明
VID (1-4094)	管理 VLAN ID に紐づく 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。
入力 / 指定した変更を破棄し前のページに戻る場合は「Back」をクリックします。

IP Settings（IP 設定）

項目	説明
Get IP From	IP アドレスの割当て方法を選択します。 • 「Static」- 手動で IPv4 アドレスを入力します。 • 「DHCP」- ローカルネットワーク上の DHCP サーバから IPv4 アドレスを取得します。
IP Address	IPv4 インタフェースに割り当てる IPv4 アドレスを入力します。
Mask	IPv4 インタフェースに割り当てるサブネットマスクを入力します。

「Apply」ボタンをクリックし、設定を適用します。

IPv4 インタフェースの編集（DHCP Client）

「IPv4 Interface Configuration」画面で「DHCP Client」タブをクリックして以下の画面を表示します。

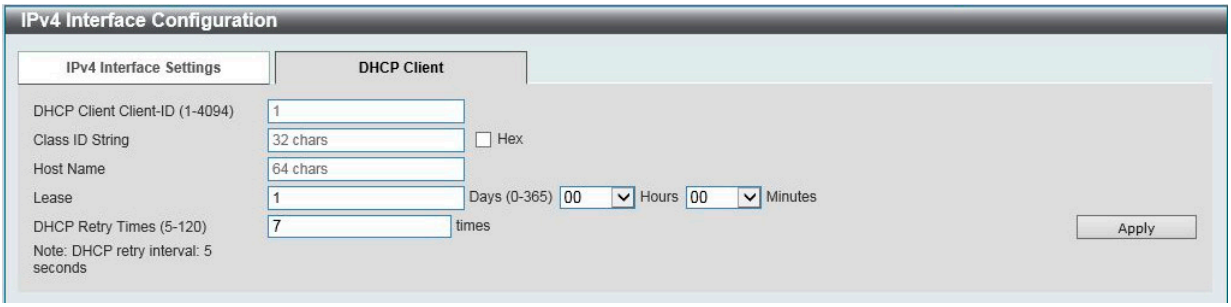


図 8-67　DHCP Client 画面

本画面には次の項目があります。

項目	説明
DHCP Client Client-ID (1-4094)	VLAN インタフェースを入力します。この 16 進数 MAC アドレスはディスカバメッセージを送信するクライアント ID として使用されます。
Class ID String	最大 32 文字を使用してベンダクラス識別名を入力します。「Hex」にチェックを入れると 16 進数方式になります。
Host Name	ホスト名を入力します。最大 64 文字で入力可能です。
Lease	DHCP サーバに要求する IP アドレスのリース時間を指定します。リース期間を、日または時間・分で指定します。
DHCP Retry Times (5-120)	DHCP 試行回数を指定します。 初期値：7（回） 設定可能範囲：5-120（回）

「Apply」ボタンをクリックし、設定を適用します。

IPv4 Default Gateway（IPv4 デフォルトゲートウェイ）

スイッチの IPv4 デフォルトゲートウェイ設定を行います。

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

図 8-68　IPv4 Default Gateway 画面

本画面には次の項目があります。

項目	説明
Gateway	IPv4 ルートのゲートウェイを入力します。

「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。

IPv6 Interface（IPv6 インタフェース）

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

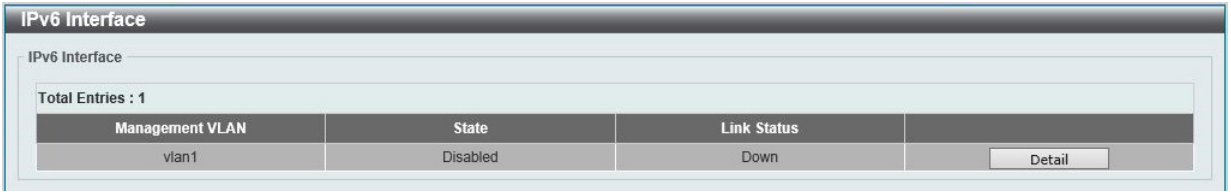


図 8-69　IPv6 Interface 画面

「Detail」ボタンをクリックすると、「IPv6 Interface」画面でインタフェースの編集を行うことができます。

IPv6 インタフェースの編集（IPv6 Interface Settings タブ）

「IPv6 Interface」画面で「IPv6 Interface Settings」タブをクリックして以下の画面を表示します。

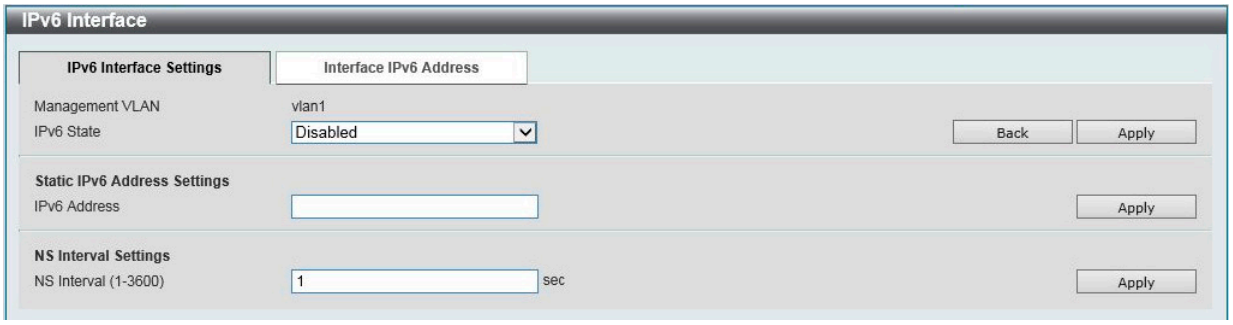


図 8-70　IPv6 Interface（IPv6 Interface Settings）画面

本画面には次の項目があります。

Interface（インタフェース）

項目	説明
IPv6 State	IPv6 インタフェースを「Enabled」（有効）/「Disabled」（無効）に設定します。

「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。

Static IPv6 Address Settings（固定 IPv6 アドレス設定）

項目	説明
IPv6 Address	IPv6 インタフェースに割り当てる IPv6 アドレスを入力します。

「Apply」ボタンをクリックし、設定を適用します。

NS Interval Settings（NS インターバル設定）

項目	説明
NS Interval (1-3600)	NS Interval を設定します。 設定可能範囲：1-3600（ミリ秒）

「Apply」ボタンをクリックし、設定を適用します。

IPv6 インタフェースの表示（ Interface IPv6 Address タブ）

「IPv6 Interface」画面で「Interface IPv6 Address」タブをクリックして以下の画面を表示します。

図 8-71　IPv6 Interface（Interface IPv6 Address ）画面

「Delete」をクリックすると指定のエントリを削除します。

IPv6 Default Gateway（IPv6 デフォルトゲートウェイ）

スイッチの IPv6 デフォルトゲートウェイ設定を行います。

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

図 8-72　IPv6 Default Gateway 画面

本画面には次の項目があります。

項目	説明
Interface VLAN (1-4094)	このルートに紐づくインタフェース VLAN ID を入力します。
Next Hop IPv6 Address	ルータのネクストホップ IPv6 アドレスを入力します。

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

第 9 章　QoS（QoS 機能の設定）

本メニューでは、QoS 機能に関する設定を行います。

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
Port Default CoS（ポートデフォルト CoS 設定）	ポートのデフォルト CoS の設定を行います。
Port Scheduler Method（ポートスケジューラーメソッド設定）	ポートのスケジューリング方式の設定を行います。
Queue Settings（QoS 設定）	キューの設定を行います。
CoS to Queue Mapping（CoS キューマッピング設定）	CoS とキューのマッピング設定を行います。
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 Default CoS（ポートデフォルト CoS 設定）

各ポートにデフォルト CoS の設定を行います。

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

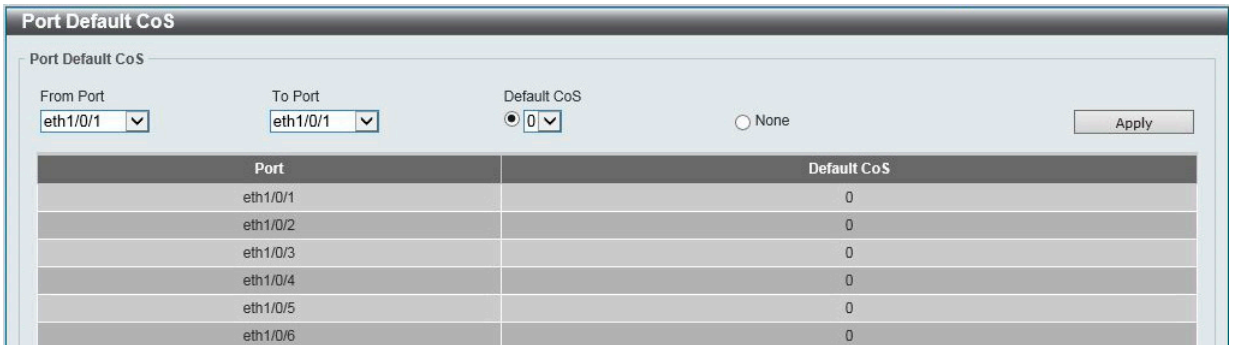


図 9-1　Port Default CoS 画面

本画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート / 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。「None」を選択すると、初期設定を使用します。 設定可能範囲：0-7

「Apply」ボタンをクリックし、設定を適用します。

Port Scheduler Method（ポートスケジューラーメソッド設定）

ポートスケジューラーメソッドを設定します。

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

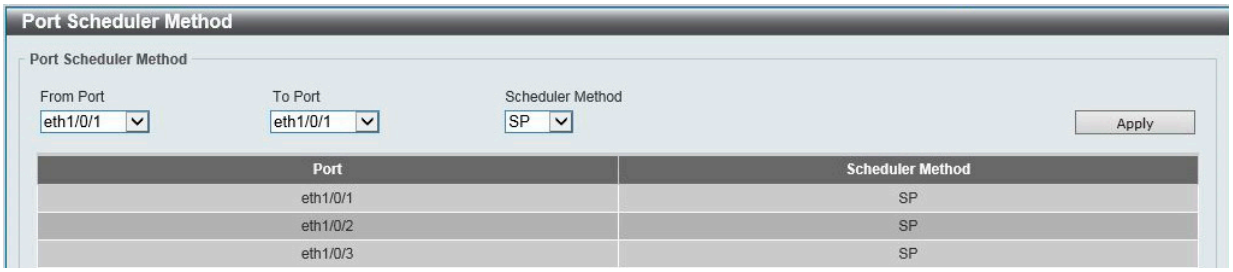


図 9-2　Port Scheduler Method 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
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。 選択肢：「SP（Strict Priority）」「WRR（Weighted Round-Robin）」 初期値：「SP」

「Apply」ボタンをクリックし、設定を適用します。

Queue Settings（QoS 設定）

キューを設定します。

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

図 9-3　Queue 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	本設定を適用するポート / ポート範囲を指定します。
Queue ID	キュー ID を指定します。 設定可能範囲：0-7
WRR Weight	WRR の値を入力します。 設定可能範囲：1-127

「Apply」ボタンをクリックし、設定を適用します。

CoS to Queue Mapping（CoS キューマッピング設定）

CoS-to-Queue マッピングの表示、設定を行います。

QoS > CoS to Queue Mapping の順にクリックし、以下の画面を表示します。

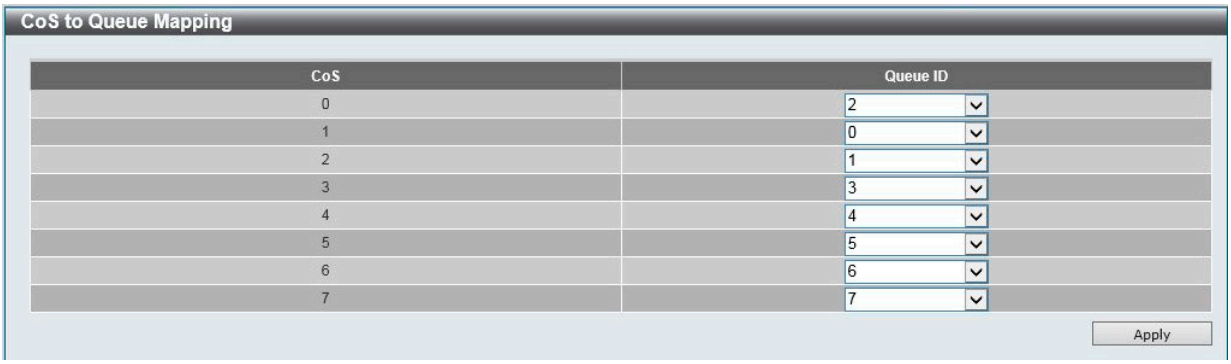


図 9-4　CoS to Queue Mapping 画面

本画面には以下の項目があります。

項目	説明
Queue ID	対応する CoS 値にマッピングするキュー ID を選択します。 設定可能範囲：0-7

「Apply」ボタンをクリックし、設定を適用します。

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。

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。

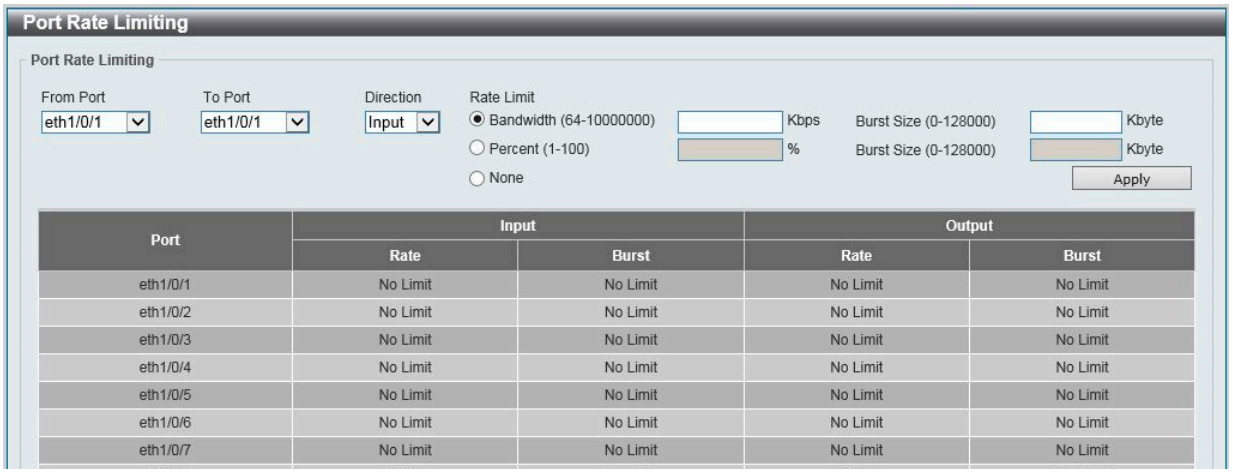


図 9-5　Port Rate Limiting 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
Direction	レート制限の対象を Input（イングレス）、Output（イーグレス）から選択します。 • 「Input」- イングレスパケットのレート制限を行います。 • 「Output」- イーグレスパケットのレート制限を行います。
Rate Limit	レート制限の値を指定します。 • 「Bandwidth」-「Bandwidth」を選択し、受信 / 送信の帯域値を入力欄に入力します。この値は 64 から 10000000 Kbps で指定できます。また「Burst Size」の値も 0 から 128000Kbytes で指定可能です。 • 「Percent」-「Percent」を選択し、受信 / 送信の帯域パーセントを入力欄に入力します。この値は 1 から 100%で指定できます。また「Burst Size」の値も 0 から 128000 Kbytes で指定可能です。 • 「None」-「None」を選択すると指定ポートのレート制限を削除します。 指定する制限は、インタフェースの最大スピードを超えることはできません。イングレスの帯域制限において、受信トラフィックが制限を超えた場合、PAUSE フレームまたはフローコントロールフレームをトリガします。

「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）

本メニューでは、デバイスのセキュリティに関する設定を行います。

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
Safeguard Engine（セーフガードエンジン）	セーフガードエンジンは、攻撃中に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。
Trusted Host（トラストホスト）	トラストホストの設定を行います。
Traffic Segmentation Settings（トラフィックセグメンテーション）	ポート間のトラフィック制御の設定を行います。
Storm Control Settings（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）	各 DoS 攻撃に対して防御設定を行います。
SSL（Secure Socket Layer）	Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。

Safeguard Engine（セーフガードエンジン）

D-Link のセーフガードエンジン機能は、パケットのフラッディングによるスイッチの CPU への影響を自動的に抑制する、強力で革新的な技術です。本機能により、不正なウイルスやウォーム攻撃によってスイッチが中断されないようにします。本機能はデフォルトで有効化されています。

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** の順にクリックし、以下の画面を表示します。

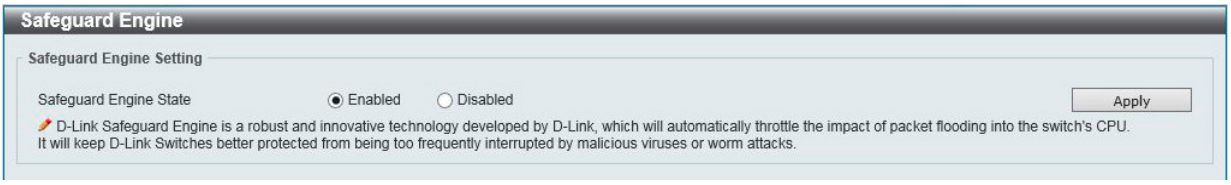


図 10-6　Safeguard Engine 画面

本画面には以下の項目があります。

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）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

Trusted Host（トラストホスト）

トラストホストの設定、表示を行います。

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

図 10-7　Trusted Host 画面

本画面には以下の項目があります。

項目	説明
IPv4 Host	IPv4 アドレスを指定します。
Type	トラストホストの種類を指定します。 選択肢：「Ping」「HTTP」「HTTPS」

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

Traffic Segmentation Settings（トラフィックセグメンテーション）

トラフィックセグメンテーション機能は、（単一 / 複数）ポート間のトラフィックの流れを制限するために使用します。「トラフィックフローの分割」という方法は「VLAN によるトラフィック制限」に似ていますが、さらに制限的です。

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。

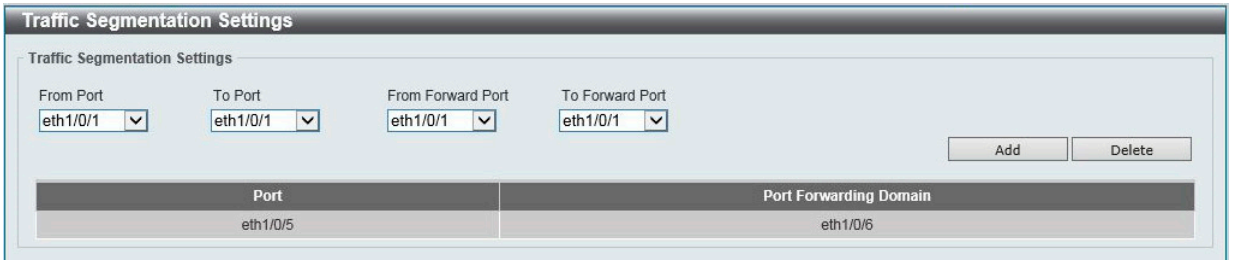


図 10-8　Traffic Segmentation Settings 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	パケットを受信するポート範囲を指定します。
From Forward Port / To Forward Port	上記のポートで受信したパケットを転送するポートの範囲を指定します。

「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 Settings（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。

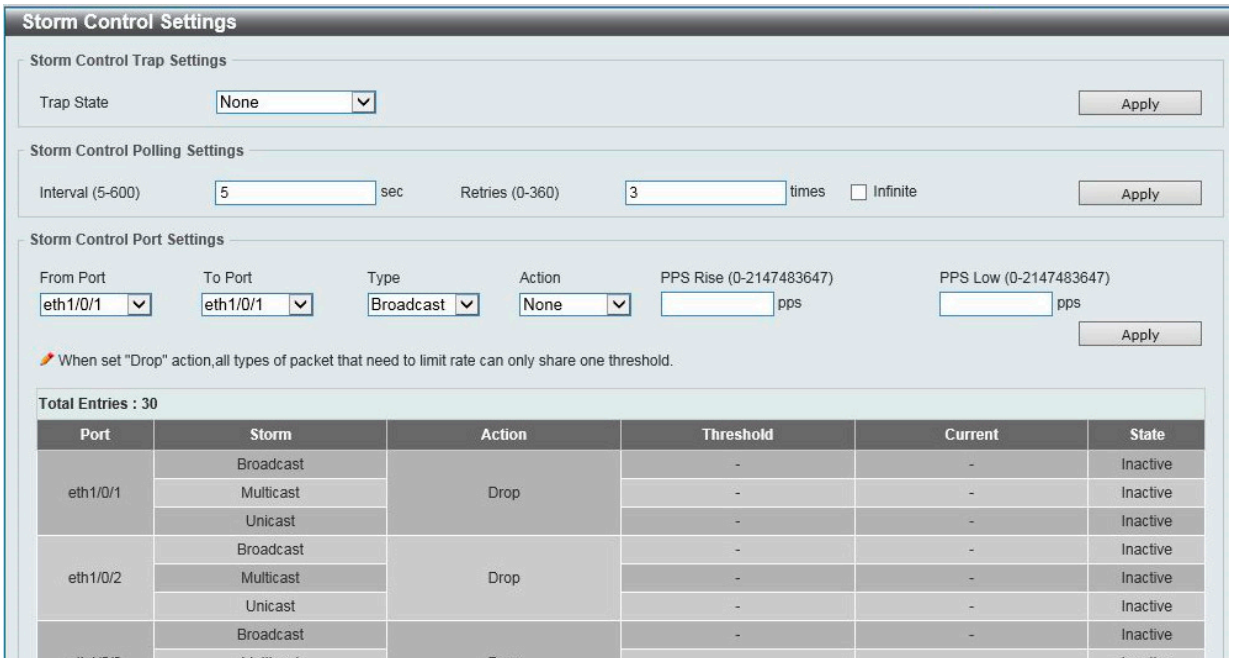


図 10-9　Storm Control Settings 画面

本画面には以下の項目があります。

Storm Control Trap Settings（ストームコントロールトラップ設定）

項目	説明
Trap State	ストームコントロールトラップのオプションを指定します。 • 「None」- トラップは送信されません。 • 「Storm Occur」- ストームの発生を検出した時点でトラップが通知されます。 • 「Storm Clear」- ストームが解消された時点でトラップが通知されます。 • 「Both」- ストームの発生時と解消時にトラップが通知されます。

「Apply」ボタンをクリックし、設定を適用します。

Storm Control Polling Settings（ストームコントロールポーリング設定）

項目	説明
Interval (5-600)	ストームの発生を判定する時間間隔を指定します。 初期値：5（秒） 設定可能範囲：5-600（秒）
Retries (0-360)	ポートがシャットダウンモードの場合、ストームの検出が本値で設定された回数に到達すると、エラー無効状態になります。「Infinite」にチェックを入れると、ストームが検出されてもシャットダウンモードのポートはエラー無効状態になりません。 初期値：3 設定可能範囲：0-360

「Apply」ボタンをクリックし、設定を適用します。

Storm Control Port Settings（ストームコントロールポート設定）

項目	説明
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
Type	コントロールするストームの種類を選択します。シャットダウンモードの場合、「Unicast」は「Known」「Unknown」ユニキャストパケット両方を意味します。これらのユニキャストパケットがしきい値に達した場合にポートがシャットダウンされます。破棄モードの場合は、「Unicast」は「Unknown」ユニキャストパケットにのみ対応します。 選択肢：「Broadcast」「Multicast」「Unicast」
Action	ポートに対するアクションを指定します。 • 「None」- ストームパケットをフィルタしません。 • 「Shutdown」- 指定したしきい値に達するとポートはシャットダウンされます。 • 「Drop」- 指定したしきい値に達するとパケットは破棄されます。
PPS Rise (0-2147483647)	毎秒のパケット増加の上限値について指定します。 設定可能範囲：0-2147483647（パケット毎秒）
PPS Low (0-2147483647)	毎秒のパケット減少の下限値について指定します。 設定可能範囲：0-2147483647（パケット毎秒）

「Apply」ボタンをクリックし、設定を適用します。

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

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。

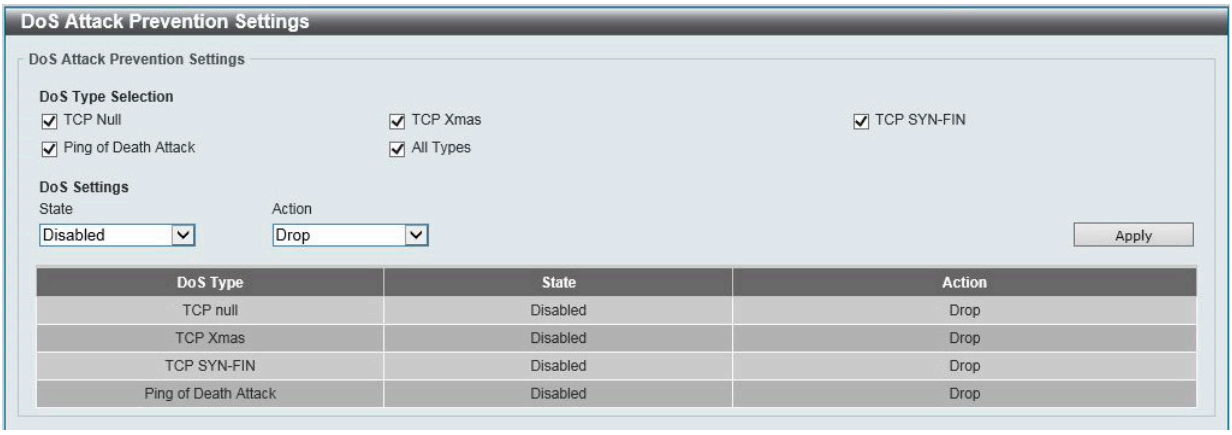


図 10-10　DoS Attack Prevention Settings 画面

本画面には以下の項目があります。

項目	説明
DoS Attack Prevention Settings	
DoS Type Selection	DoS 攻撃防御のタイプを選択します。 • TCP Null - DoS 攻撃防止タイプに TCP Null Scan 攻撃を指定します。 • TCP Xmas - DoS 攻撃防止タイプに TCP Xmascan 攻撃を指定します。 • TCP SYN-FIN - DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。 • Ping of Death Attack - DoS 攻撃防止タイプに Ping Death Attack 攻撃を指定します。 • 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。

項目	説明
Action	DoS 攻撃防止機能により行われる操作を無効にします。 • Drop - 一致する DoS 攻撃パケットをすべて破棄します。

「Apply」ボタンをクリックし、設定を適用します。

SSL（Secure Socket Layer）

Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、サーバ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暗号パラメータ / 暗号化アルゴリズム / キー長を決定する、暗号スイートと呼ばれるセキュリティ文字列により実現しています。

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 > 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 10-11　SSL Global Settings 画面

本画面には以下の項目があります。

項目	説明
SSL Global Settings	
SSL Status	SSL を「Enabled」（有効）/「Disabled」（無効）に設定します。 初期値：「Disabled」（無効）
Service Policy	SSL ポリシー名を入力します。

「Apply」ボタンをクリックし、設定を適用します。

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

SSL Service Policy（SSL サービスポリシー）

SSL サービスポリシーの表示、設定を行います。

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

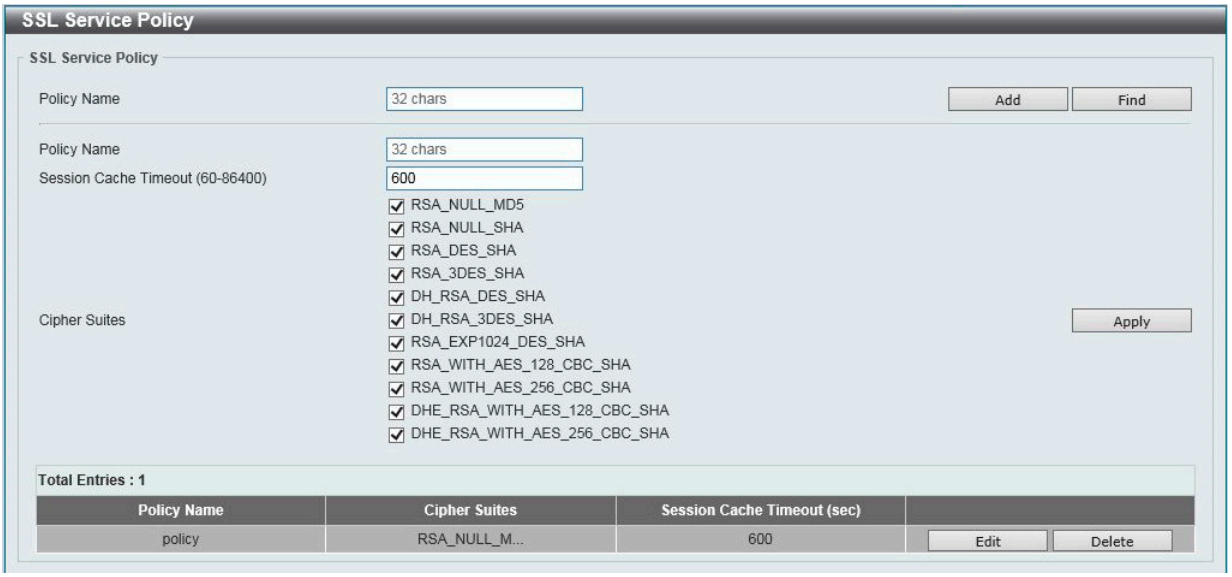


図 10-12　SSL Service Policy 画面

ポリシーを作成するには、画面上部のセクションでポリシー名を入力し、「Apply」をクリックします。
ポリシーを編集するには、画面真ん中のセクションで作成済みのポリシー名を入力し、設定の変更を行った上で「Apply」をクリックします。

本画面には以下の項目があります。

項目	説明
Policy Name	SSL サービスポリシー名を入力します。32 文字まで指定可能です。
Session Cache Timeout (60-86400)	セッションキャッシュタイムアウトの時間を指定します。 初期値：600（秒）
Cipher Suites	本プロファイルの暗号スイートを選択します。

「Apply」ボタンをクリックし、設定を適用します。
「Find」ボタンをクリックして、入力した情報に基づいて指定エントリを検出します。
「Edit」ボタンをクリックして、指定エントリを編集します。
「Delete」ボタンをクリックして、指定エントリを削除します。

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

本メニューでは、ケーブル診断機能を提供します。

以下は OAM 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
Cable Diagnostics（ケーブル診断機能）	スイッチに接続する UTP ケーブルの詳細について表示します。

Cable Diagnostics（ケーブル診断機能）

ケーブル診断機能は、使用している UTP の状態を簡単に確認するための簡易機能です。検査結果を目安に実施ケーブルの状態を確認してください。

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。

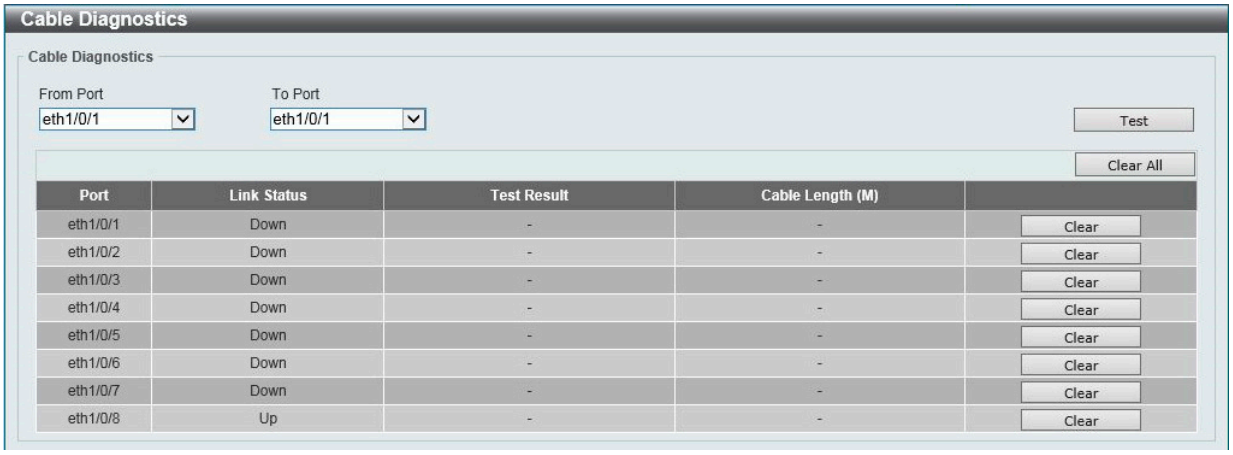


図 11-13　Cable Diagnostics 画面

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、「From Port/To Port」項目で検査対象のポートを選択し、「Test」ボタンをクリックします。
結果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　ケーブル長の検出機能をサポートしているのは Copper ポート（10/100/1000Mbps/2.5Gbps ）のみです。

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

第 12 章　Monitoring（スイッチのモニタリング）

本メニューでは、ポートのトラフィックやエラー、サイズ等の統計情報を表示します。

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）	スイッチの統計情報を表示します。
Mirror Settings（ミラー設定）	ミラーリング機能の設定を行います。特定ポートの送受信フレームを、他のポートにコピーすることができます。

Statistics（統計情報）

Port（ポート統計情報）

ポートのトラフィック統計情報を表示します。

Monitoring > Statistics > 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。

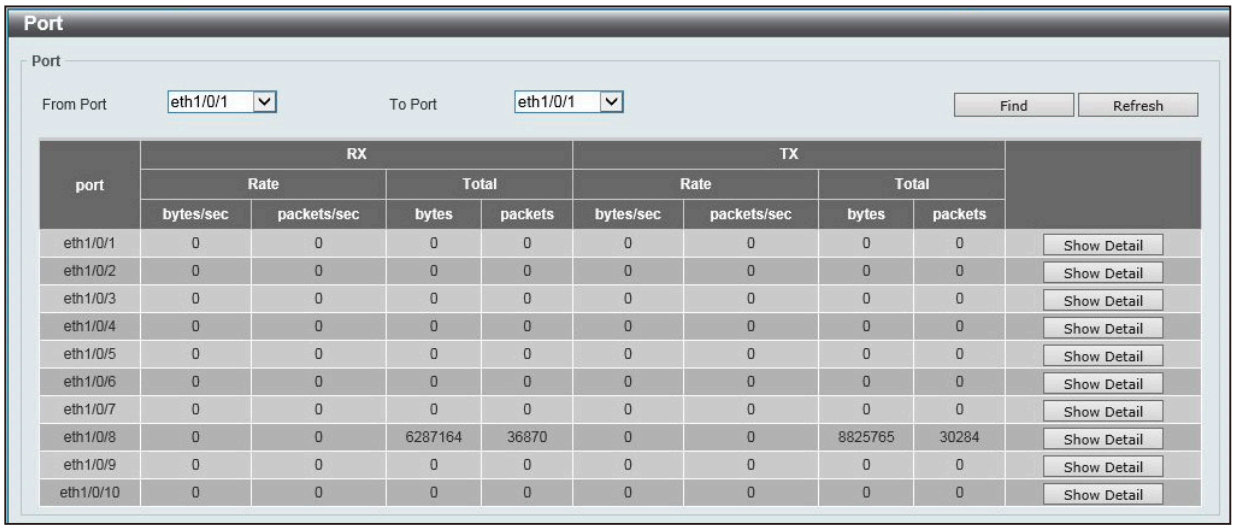


図 12-14　Port 画面

本画面には以下の項目があります。

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

「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、テーブルを更新します。
「Show Detail」ボタンをクリックし、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

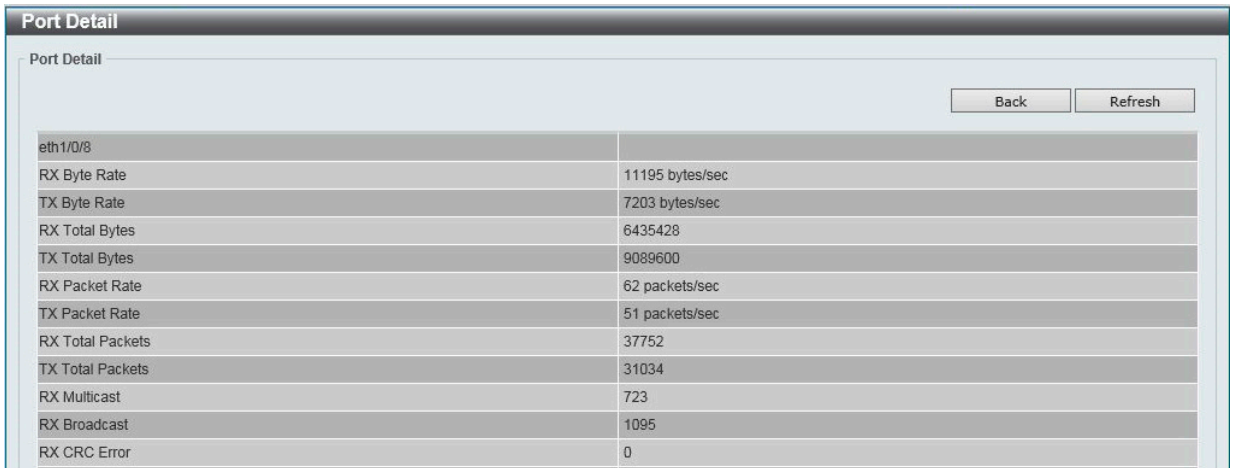


図 12-15　Port Statistics - Show Detail 画面

「Refresh」ボタンをクリックし、テーブルを再起動します。
「Back」ボタンをクリックし、前の画面に戻ります。

Port Counters（ポートカウンタ）

ポートカウンタ情報について表示します。

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。

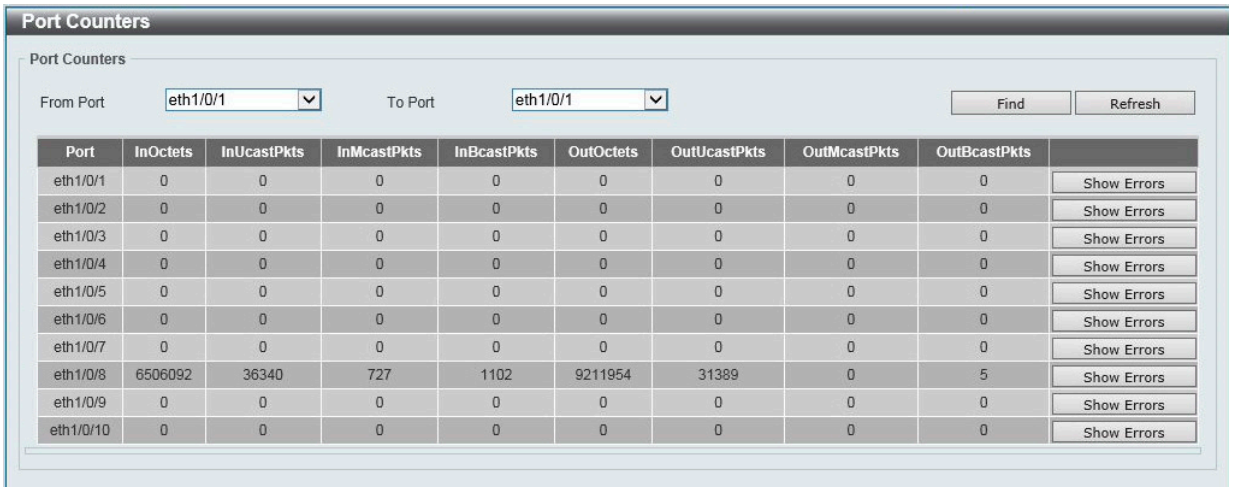


図 12-16　Port Counters 画面

本画面には以下の項目があります。

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

「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。
「Show Errors」ボタンをクリックすると、指定ポートのエラー情報について表示します。

「Show Errors」ボタンをクリックすると、次の画面が表示されます。

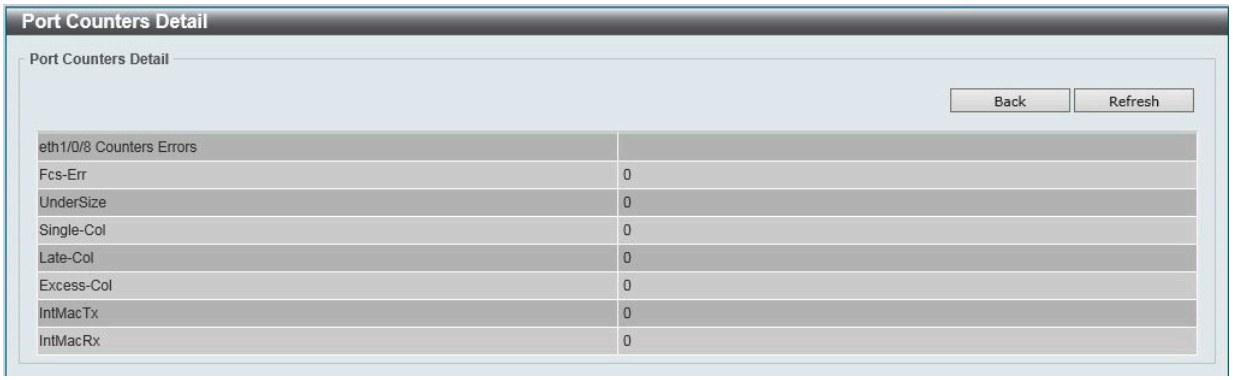


図 12-17　Port Counters (Show Errors) 画面

「Back」をクリックすると前のページに戻ります。
「Refresh」ボタンをクリックし、テーブルを更新します。

Counters（カウンタ）

すべてのポートのカウンタ情報を表示、消去します。

Monitoring > Statistics > 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。

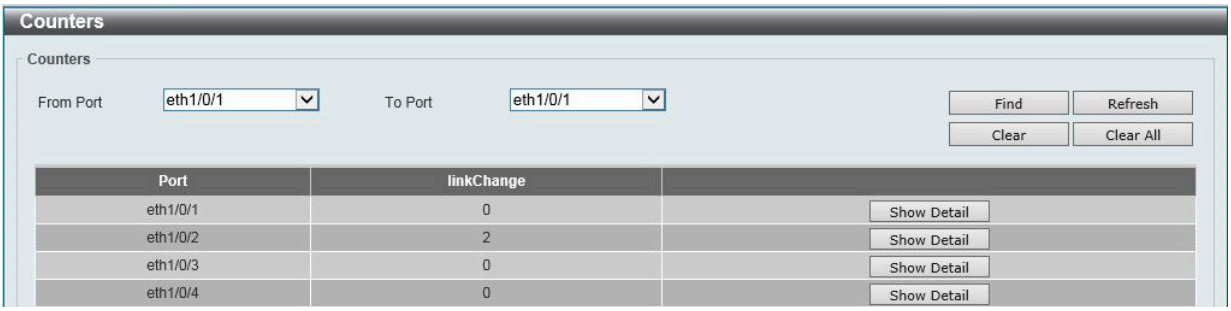


図 12-18　Counters 画面

本画面には以下の項目があります。

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

「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、テーブルを更新します。
「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。
「Show Detail」ボタンをクリックし、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

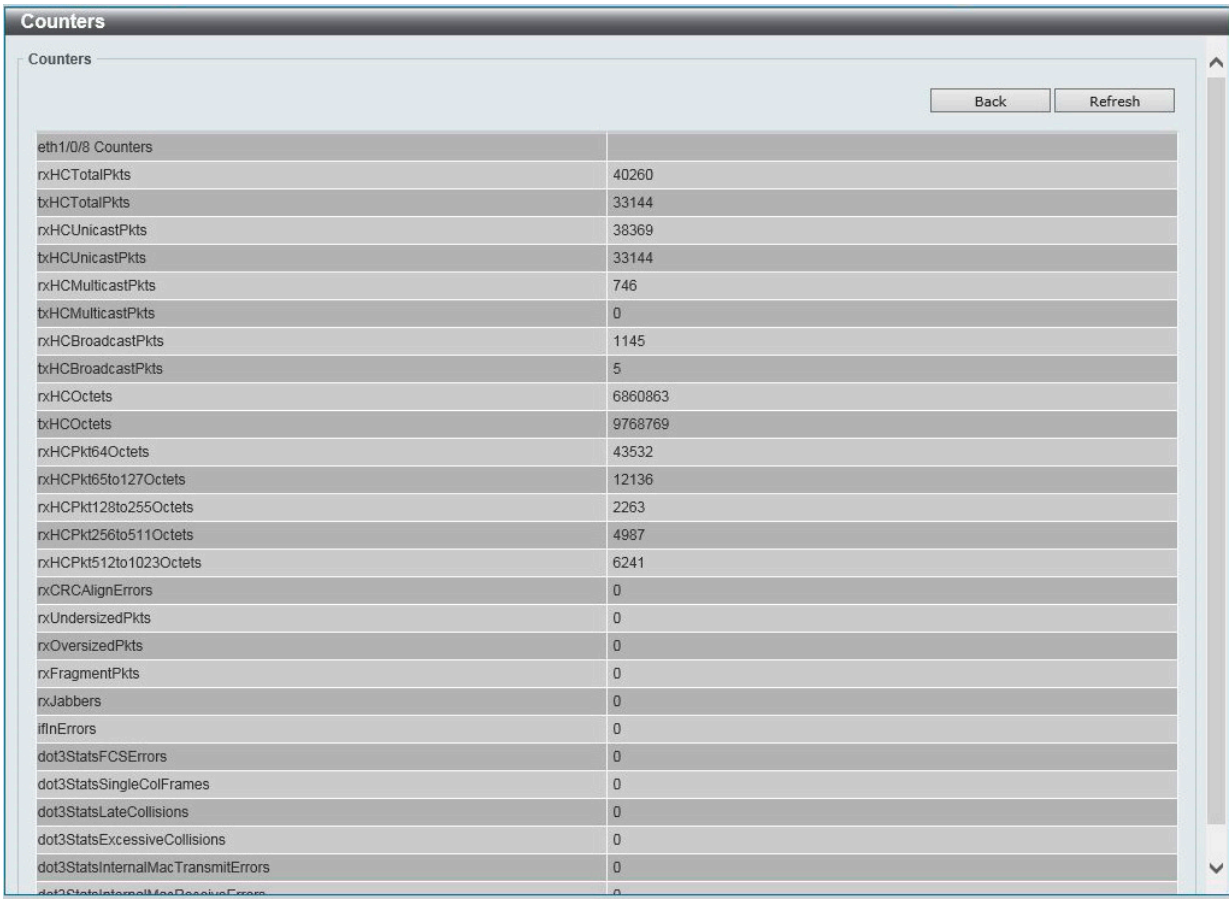


図 12-19　Counters - Show Detail 画面

「Refresh」ボタンをクリックし、テーブルを再起動します。
「Back」ボタンをクリックし、前の画面に戻ります。

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。

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

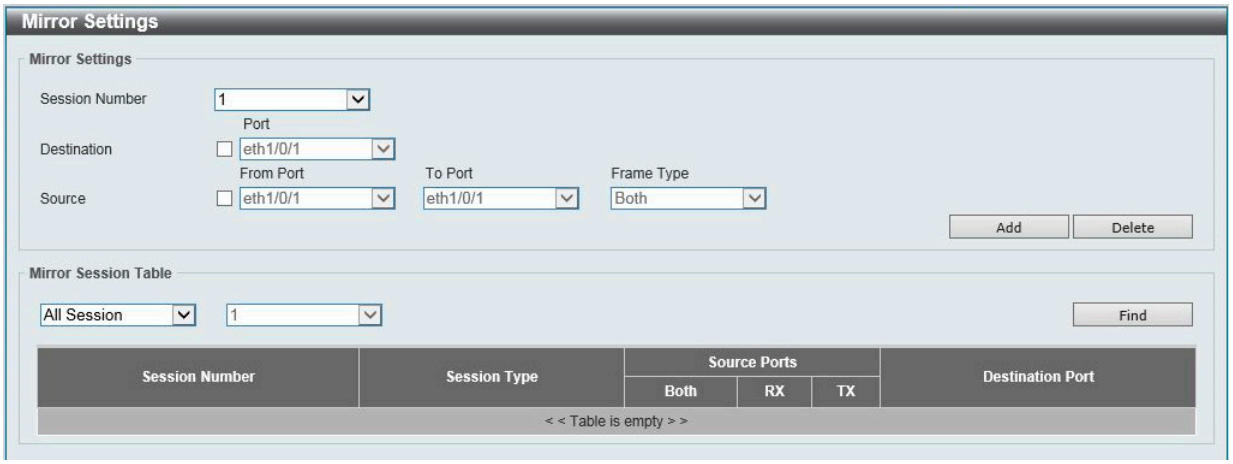


図 12-20　Mirror Settings 画面

本画面には以下の項目があります。

Mirror Settings（ミラー設定）

項目	説明
Session Number	該当エントリのセッション番号を指定します。 設定可能範囲：1-2
Destination	チェックボックスにチェックを入れ、ポートミラーエントリの宛先を設定します。
Source	チェックボックスにチェックを入れ、ポートミラーエントリの送信元を設定します。
Frame Type	「Source」として送信元を指定した場合、ミラーリングを行うトラフィックを選択します。 選択肢：「Both（両方）」「RX（受信）」「TX（送信）」「TX Forwarding」

「Add」ボタンをクリックして、入力した情報に基づいた新規のミラーエントリを追加します。
「Delete」ボタンをクリックして、入力した情報に基づいた既存のミラーエントリを削除します。

Mirror Session Table（ミラーセッションテーブル）

項目	説明
Mirror Session Type	テーブルに表示するミラーセッションの種類を選択します。「Session Number」を選択した場合、セッション番号として「1」または「2」を選択します。 選択肢：「All Session」「Session Number」

「Find」ボタンをクリックして、入力した情報に基づいたエントリを検出します。

第 13 章　Green（省電力機能）

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）	スイッチの省電力機能を設定します。
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おり、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。

Power Saving（省電力）

スイッチの省電力機能を設定します。

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

図 13-1　Power Saving 画面

本画面には以下の項目があります。

項目	説明
Administrative Dim-LED	ポート LED オフを「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

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 13-2　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
EEE Settings	
From Port / To Port	本設定を適用するポート / ポート範囲を指定します。
State	本機能を「Enabled」（有効）/「Disabled」（無効）に設定します。

「Apply」ボタンをクリックし、設定を適用します。

注意　本機能を使用するには、接続する対向の機器も EEE に対応している必要があります。

第 14 章　スイッチのメンテナンス

スイッチを工場出荷時設定に戻す

リセットボタンを押下することで本製品の設定を工場出荷状態に戻します。

1. 必要に応じて設定ファイルのバックアップを行い、本製品からログアウトします。
2. 前面のリセットボタンを 5 秒以上押して離します。
3. 本製品は工場出荷時の状態に戻って再起動します。

注意 工場出荷時の状態に戻るとすべての設定が消去されます。
リセットボタンを押下する前に、必要に応じて「Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）」でご使用の製品の設定をバックアップしてください。

スイッチを再起動させる

リセットボタンを押下することで本製品を再起動させます。

1. 前面のリセットボタンを 5 秒未満押して離します。
2. 本製品は再起動します。

注意 スイッチを再起動させると、保存（Save）していないすべての設定が消去されます。
リセットボタンを押下する前に、必要に応じて「Save Configuration（コンフィグレーションの保存）」でご使用の製品の設定を保存してください。

【付録 A】 ケーブルとコネクタ

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。
以下の図と表は標準の RJ-45 プラグ / コネクタとピンアサインです。

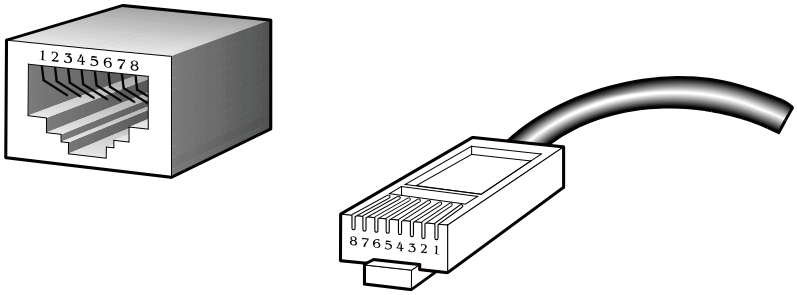


図 A-1 標準的な RJ-45 プラグとコネクタ

表 A-1 標準的な RJ-45 ピンアサイン

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

【付録 B】 ケーブル長

以下の表は各規格に対応するケーブル長 (最大) です。

表 B-1 ケーブル長

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

【付録 C】 用語解説

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

用語	説明
MDI（Medium Dependent Interface）	1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。
MDI-X（Medium Dependent Interface Cross-over）	接続送受信のラインが交差しているイーサネットポート接続。
MIB（Management Information Base）	デバイスの管理特性とパラメータを保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。
マルチキャスト	シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。
プロトコル	ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。
Resilient link	他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。
RJ-45	10BASE-T や 100BASE-TX などで使用する標準 8 線コネクタ。
RMON	リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。
RPS（リダンダント電源システム）	スイッチに接続されて、バックアップ電源を供給するデバイス。
サーバファーム	大量のユーザにサービスを提供する中央に位置するサーバグループ。
SLIP（Serial Line Internet Protocol）	IP がシリアルライン接続を経由して動作することが可能なプロトコル。
SNMP（Simple Network Management Protocol）	当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。
スパニングツリープロトコル (STP)	ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。
スタック	1 個の論理的なデバイスの形とするために統合されたネットワークデバイスのグループ。
スタンバイポート	リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。
スイッチ	パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。
TCP/IP	Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。
telnet	仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。
TFTP（Trivial File Transfer Protocol）	スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する (ソフトウェアアップグレードなど) ことができます。
UDP（User Datagram Protocol）	インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。
VLAN（Virtual LAN）	物理的に接続した LAN のように通信する位置やトポロジが独立しているデバイスのグループ。
VLT（Virtual LAN Trunk）	各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。
VT100	ASCII コードを使用するターミナルタイプ。VT100 画面はテキストベースの表示をします。

【付録 D】 機能設定例

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

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

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。

- DMS-1100

Traffic Segmentation（トラフィックセグメンテーション）

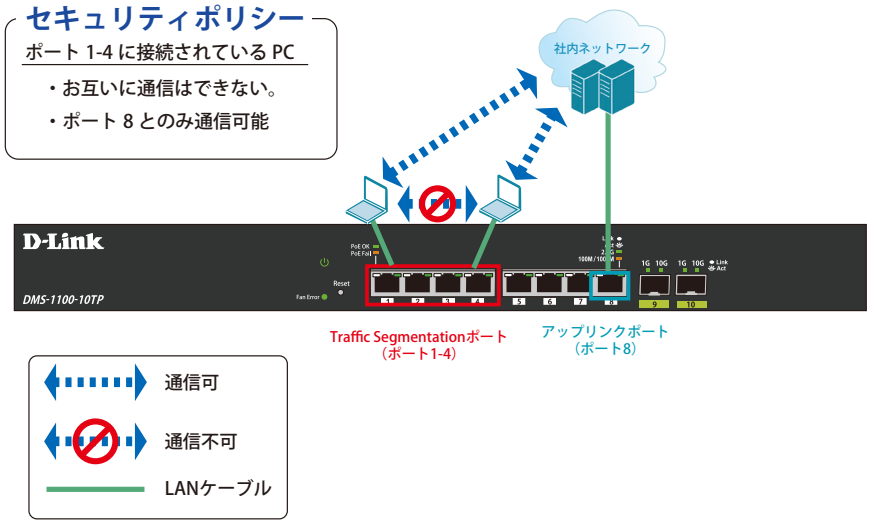


図 16-1 Traffic Segmentation（DMS-1100-10TP）

概要

ポート 1 ～ 4 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 ～ 4 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 ～ 4 は、アップリンクポートとして使用するポート 8 とのみ通信ができるようにします。

設定手順

1. **Security > Traffic Segmentation Settings** での「From/To Port」で適応ポート範囲（1-4）を指定します。
「From/To Forward Port」で指定するポート（8）が通信可能（転送）なポートとなります。

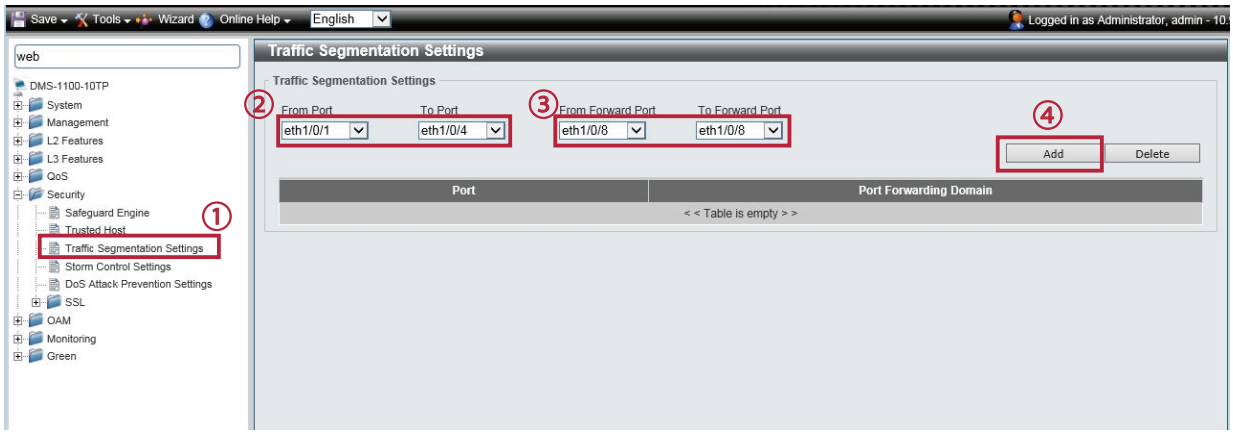


図 16-2　Traffic Segmentation Settings 画面（DMS-1100-10TP）

2. 以下の設定になっていることを確認します。

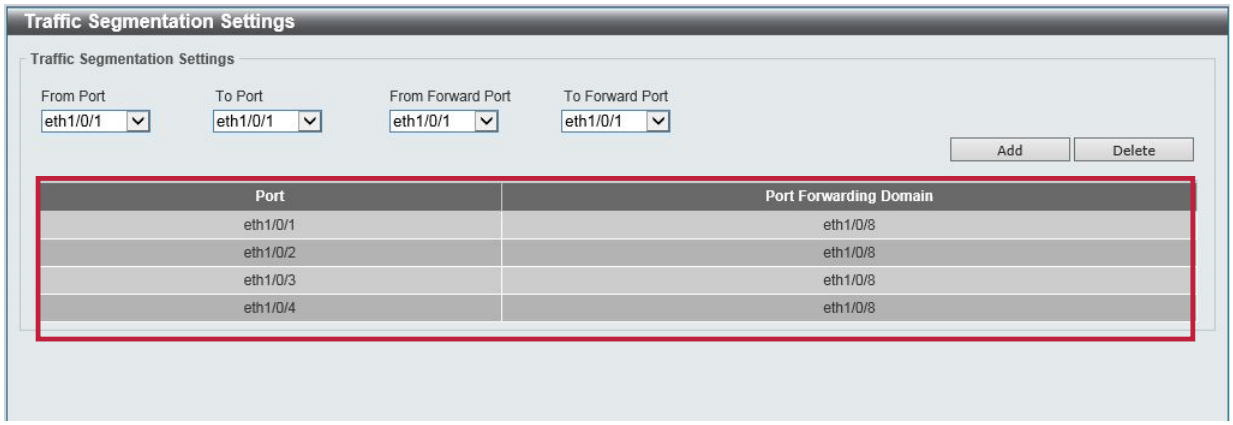


図 16-3　Traffic Segmentation Settings 画面（DMS-1100-10TP）

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

図 16-4　Save Configuration 画面（DMS-1100-10TP）

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。

VLAN

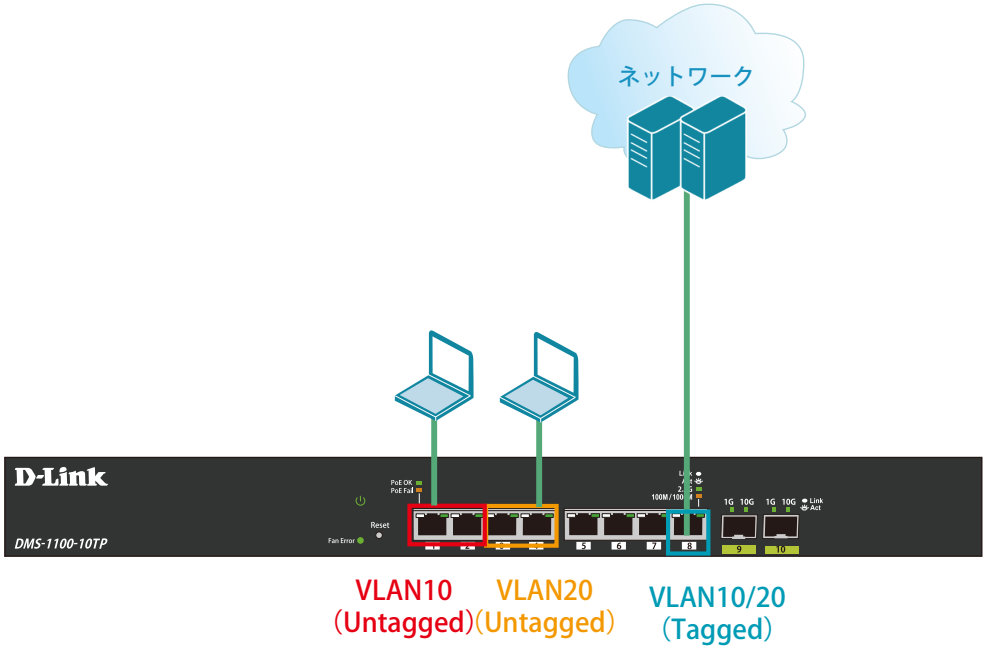


図 16-5 VLAN（DMS-1100-10TP）

概要

VLAN を設定します。ポート 1 ～ 2 に VLAN10 を「Untagged」で割り当て、ポート 3 ～ 4 に VLAN20 を「Untagged」で割り当て、ポート 8 において、VLAN10 と VLAN20 を「Tagged」で割り当てます。

設定手順

注意 WebUI にアクセスしている PC を接続しているポートは Management VLAN に属したポートに接続している必要があります（デフォルトでは VLAN1）。ポート 1~4 に接続している場合、以下の手順により Untagged VLAN へ設定した後、WebUI へのアクセスが失われますので、Management VLAN に所属しているポートに差し替えてください。

1. **L2 Functions > 802.1Q VLAN** で VLAN10、20 を作成します。
   以下の設定を行い、「Apply」をクリックします。

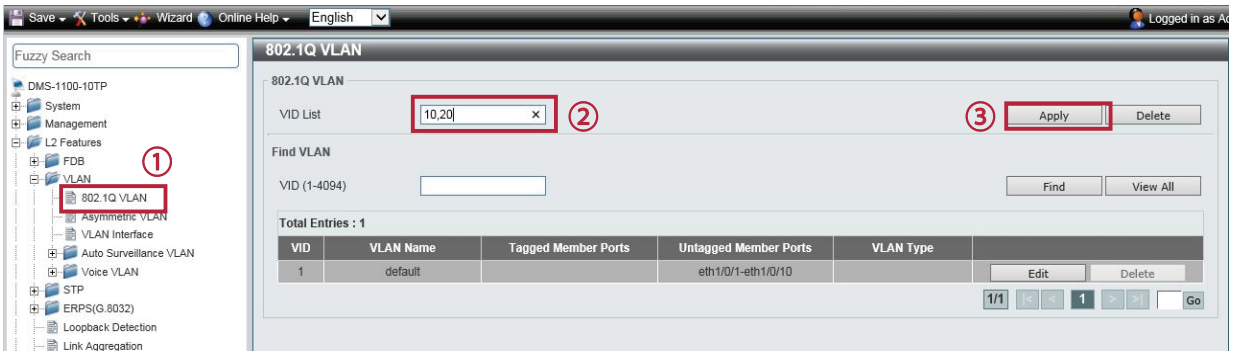


図 16-6 802.1Q VLAN（DMS-1100-10TP）

項目	値
VID List	10,20

2. **L2 Features > VLAN > VLAN Interface** でポート「eth1/0/1」の「Edit」をクリックします。

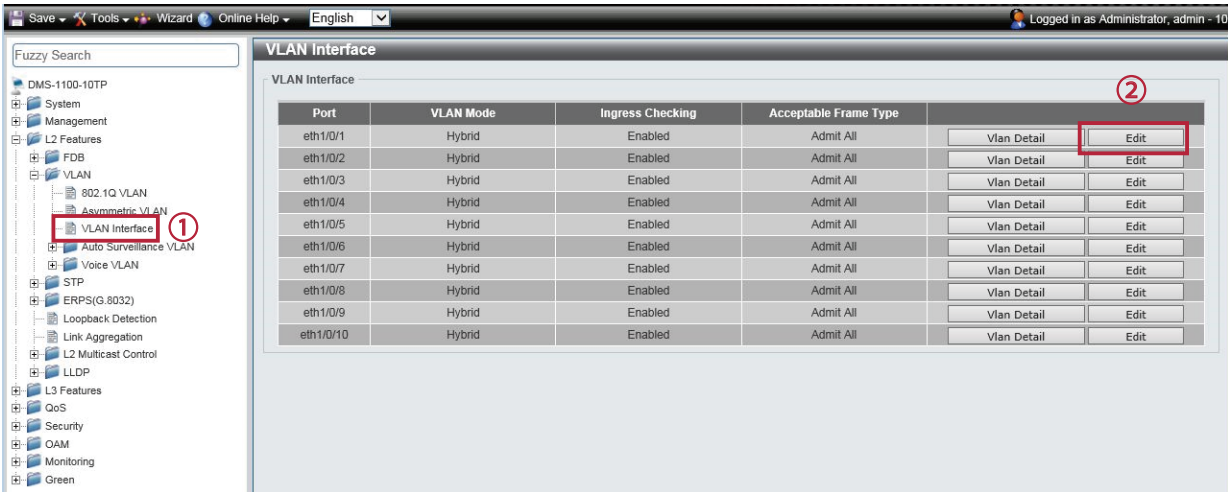


図 16-7　VLAN Interface 画面（DMS-1100-10TP）

3. ポート 1-2 に VLAN10 を割り当てます。以下の設定を行い、「Apply」をクリックします。

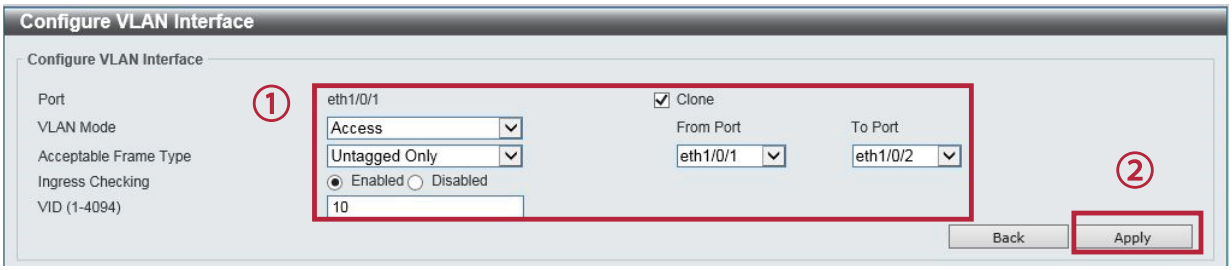


図 16-8　Configure VLAN Interface 画面（DMS-1100-10TP）

項目	値
Port	eth1/0/1
VLAN Mode	Access
Acceptable Frame Type	Untagged Only
Ingress Checking	Enabled
VID (1-4094)	10
Clone	チェック
From Port	eth1/0/1
To Port	eth1/0/2

4. VLAN Interface 画面に戻り、ポート「eth1/0/3」の「Edit」をクリックします。

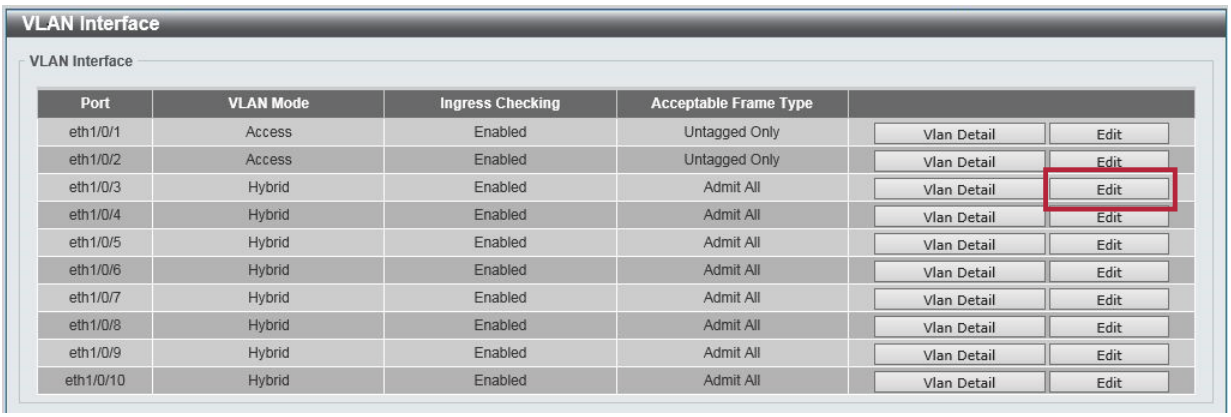


図 16-9　LAN Interface 画面（DMS-1100-10TP）

5. ポート 3-4 に VLAN20 を割り当てます。以下の設定を行い、「Apply」をクリックします。

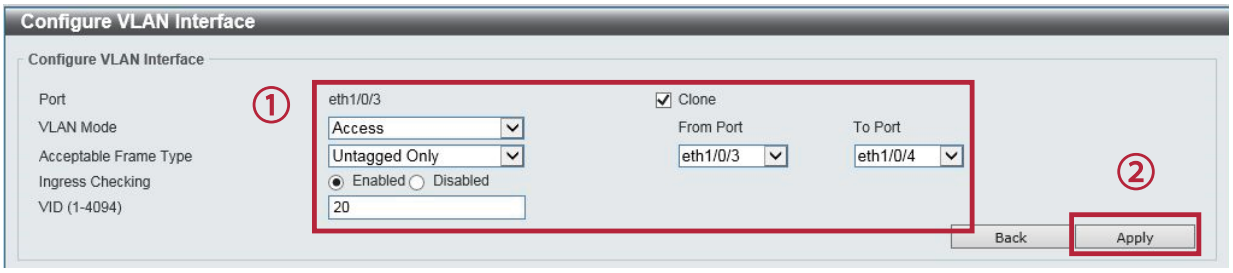


図 16-10　Configure VLAN Interface 画面（DMS-1100-10TP）

項目	値
Port	eth1/0/3
VLAN Mode	Access
Acceptable Frame Type	Untagged Only
Ingress Checking	Enabled
VID (1-4094)	20
Clone	チェック
From Port	eth1/0/3
To Port	eth1/0/4

6. VLAN Interface 画面に戻り、ポート「eth1/0/8」の「Edit」をクリックします。

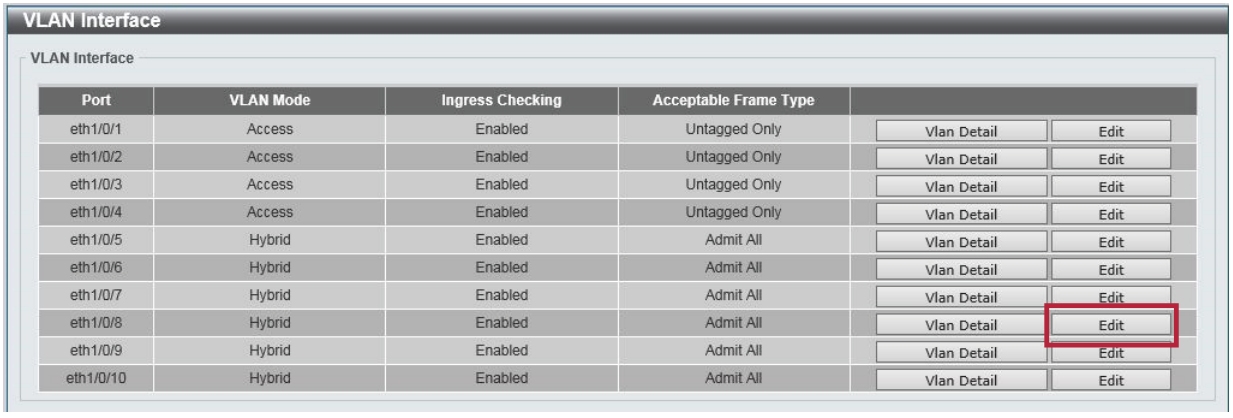


図 16-11　VLAN Interface 画面（DMS-1100-10TP）

7. 上位のネットワークへ接続されているポート 8 に VLAN10、20 の通信を転送することができるように、VLAN を設定します。以下の設定を行い、「Apply」をクリックします。

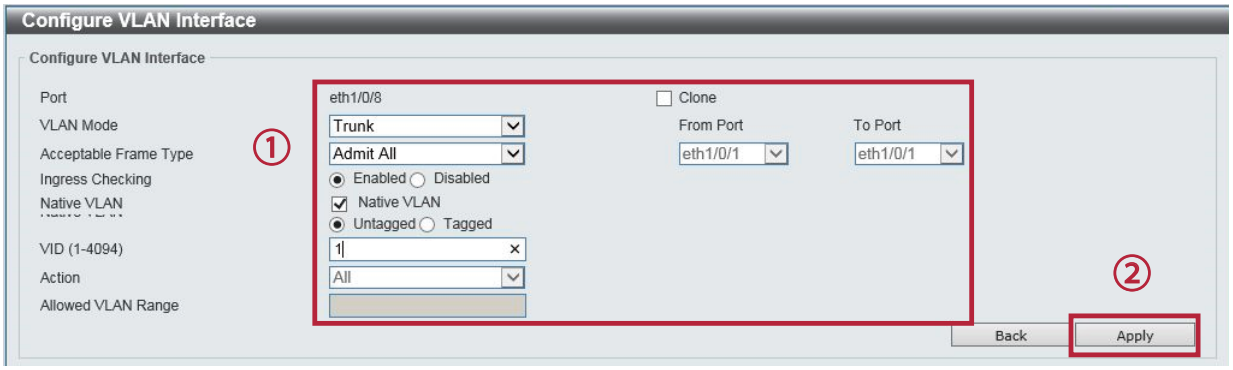


図 16-12　Configure VLAN Interface 画面（DMS-1100-10TP）

項目	値
Port	eth1/0/8
VLAN Mode	Trunk
Acceptable Frame Type	Admit All
Ingress Checking	Enabled
Native VLAN	チェックあり
VID (1-4094)	1
Action	All（デフォルト）
Allowed VLAN Range	入力なし
Clone	チェックなし

注意 トランクモードに設定すると、全ての VLAN が自動的に Tagged VLAN メンバとして当該ポートに登録されます。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。（Trunk モードに設定後、編集できるようになります。）

8. **L2 Features > VLAN > 802.1Q VLAN** で以下の設定になっていることを確認します。

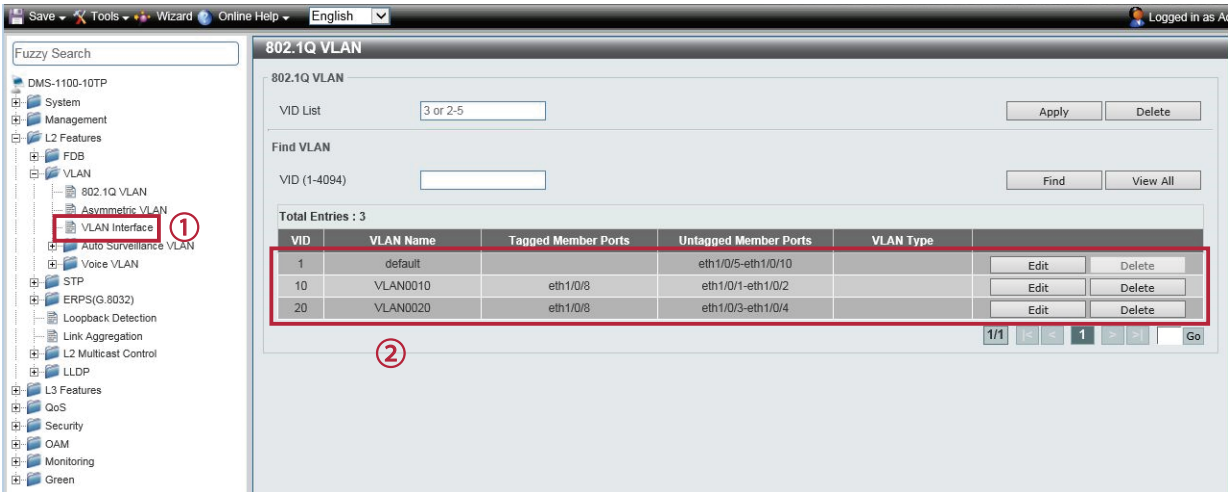


図 16-13　802.1Q VLAN 画面（DMS-1100-10TP）

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

図 16-14　Save Configuration 画面（DMS-1100-10TP）

Link Aggregation（リンクアグリゲーション）

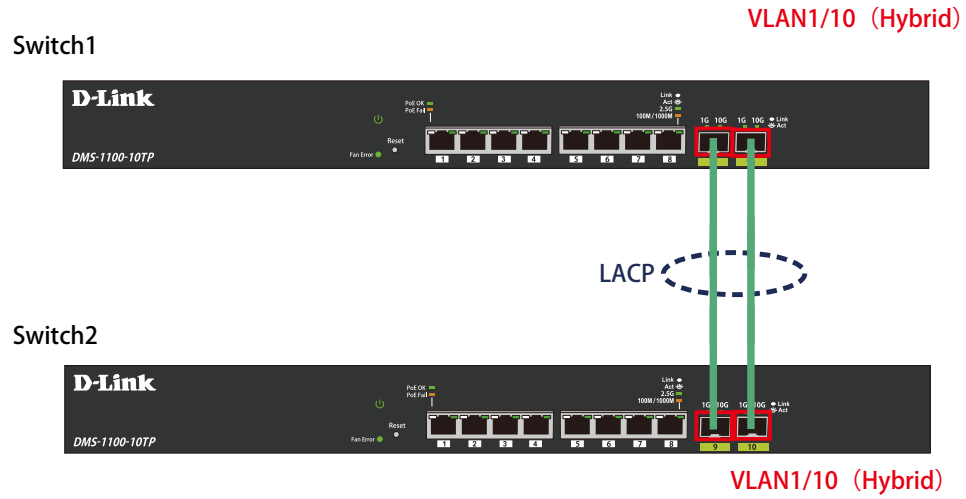


図 16-15　Link Aggregation（DMS-1100-10TP）

概要

VLAN1 と 10 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 VLAN1 と VLAN10 を Tagged で割当て、ポート 9 と 10 をグループとして LACP によるリンクアグリゲーションに設定します。

設定手順

1. **L2 Functions > 802.1Q VLAN** で VLAN10 を作成します。
   以下の設定を行い、「Apply」をクリックします。

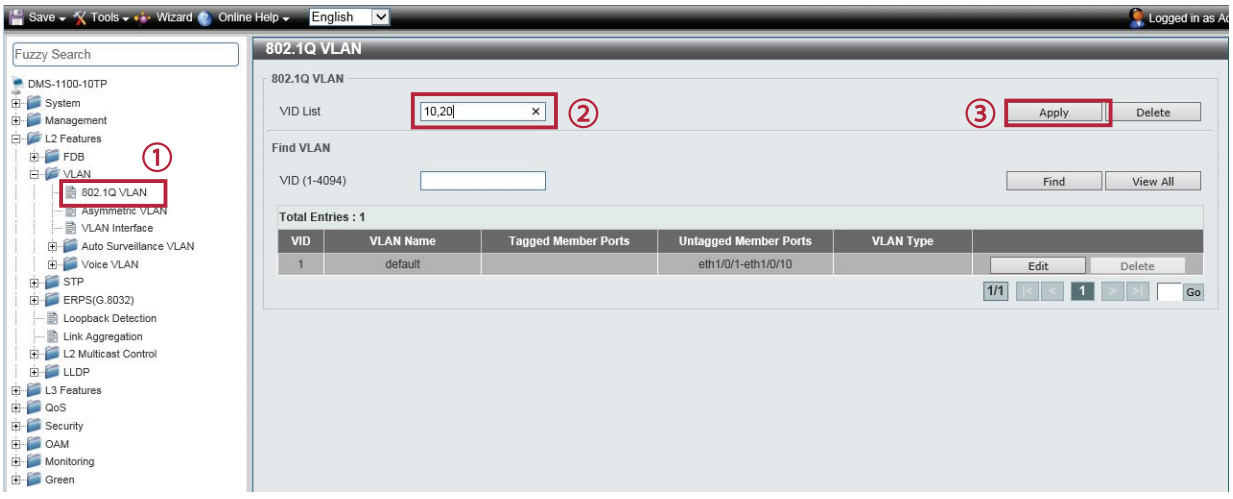


図 16-16　802.1Q VLAN 画面（DMS-1100-10TP）

項目	値
VID List	10

2. **L2 Functions > Link Aggregation** でポート 9、10 に LACP を設定します。
以下の設定を行い、「Add」をクリックします。

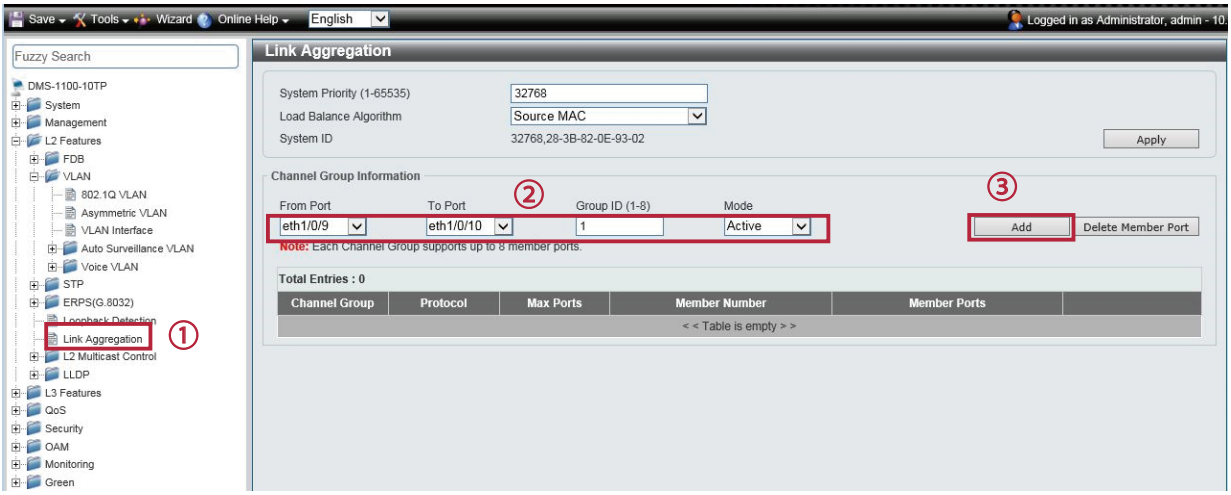


図 16-17　Link Aggregation 画面（DMS-1100-10TP）

項目	値
From Port	eth1/0/9
To Port	eth1/0/10
Group ID	1
Mode	Active

3. VLAN10、VLAN20 を割り当てます。**L2 Features > VLAN > VLAN Interface** でポート「Port-Channel1」の「Edit」をクリックします。

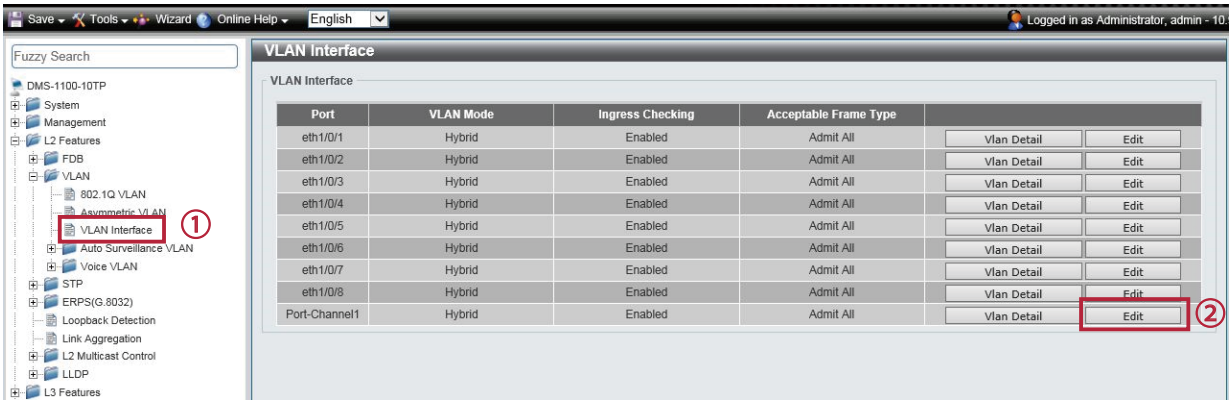


図 16-18　VLAN Interface 画面（DMS-1100-10TP）

4. Port-Channel1 に VLAN1、10 を割り当てます。「VLAN Mode」に「Trunk」を設定し、一旦「Apply」をクリックします。

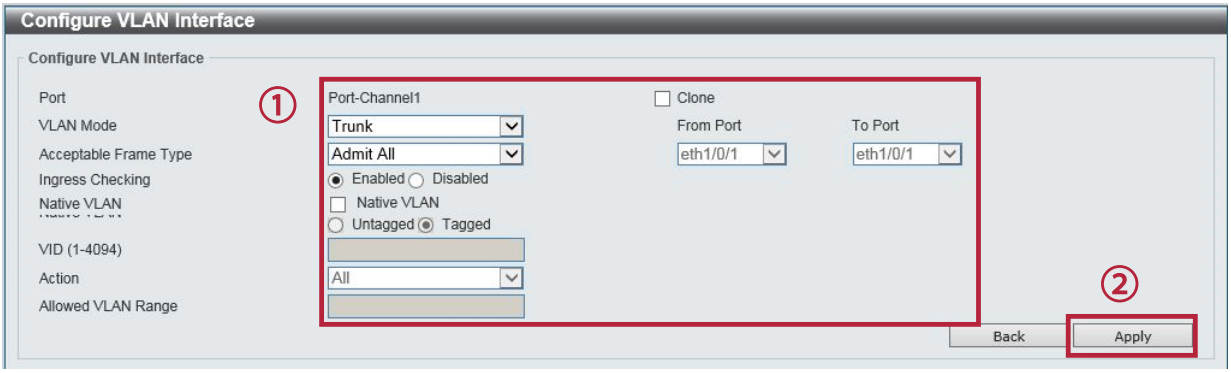


図 16-19　Configure VLAN Interface 画面（DMS-1100-10TP）

5. Trunk モードに設定後、VLAN 範囲の設定ができるようになります。続けて以下の設定を行い、「Apply」をクリックします。

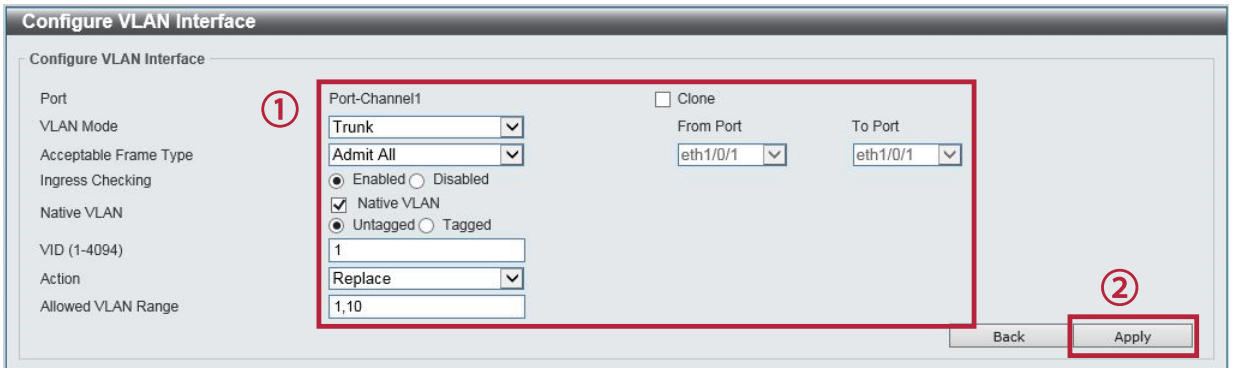


図 16-20　Configure VLAN Interface 画面（DMS-1100-10TP）

項目	値
Port	Port-Channel1
VLAN Mode	Trunk
Acceptable Frame Type	Admit All
Ingress Checking	Enabled
Native VLAN	チェックあり
VID (1-4094)	1
Action	Replace
VID (1-4094)	1,10
Clone	チェックなし

6. **L2 Features > VLAN > 802.1Q VLAN** で以下の設定になっていることを確認します。

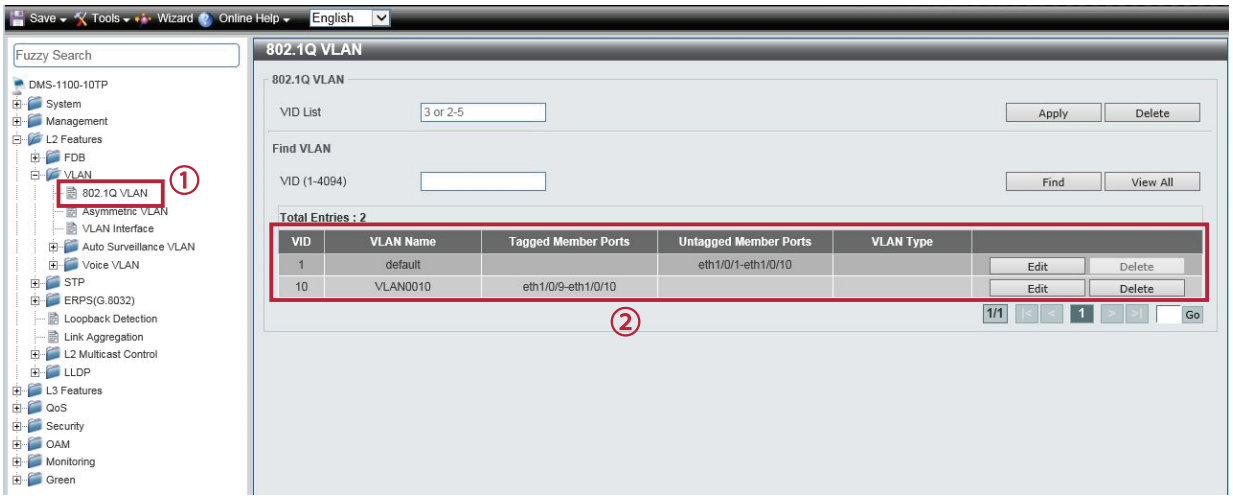


図 16-21　802.1Q VLAN 画面（DMS-1100-10TP）

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

図 16-22　Save Configuration 画面（DMS-1100-10TP）