D-Link DGS-1530 シリーズ

Gigabit Layer2 Stackable Smart Managed 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 / する場合は、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。

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

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

はじめに 14

本マニュアルの対象者 16
表記規則について 16
製品名 / 品番一覧 16

第 1 章　本製品のご使用にあたって 17

スイッチ概要 17
搭載ポート 18
オプションモジュール（光トランシーバ / ダイレクトアタッチケーブル） 18
前面パネル 19
　LED 表示 21
背面パネル 24
側面パネル 25
　スマートファンについて 26

第 2 章　スイッチの設置 28

パッケージの内容 28
ネットワーク接続前の準備 28
ゴム足の取り付け (19 インチラックに設置しない場合) 28
19 インチラックへの取り付け 29
SFP/SFP+ スロットへのモジュールの取り付け 30
電源抜け防止器具の装着 31
リダンダント電源システムの設置 33
　DPS-500A 33
　DPS-700 34
電源の投入 35
　電源の異常 35

第 3 章　スイッチの接続 36

エンドノードと接続する 36
ハブまたはスイッチと接続する 36
バックボーンまたはサーバと接続する 37

第 4 章　スイッチ管理について 38

Web GUI による管理 38
SNMP による管理 38
CLI による管理 38
　端末をコンソールポートに接続する 38
　初回ログイン後のパスワードの設定 39
　IP アドレスの割り当て 40

第 5 章　Web ベースのスイッチ管理 41

Web ベースの管理について 41
Web マネージャへのログイン 41
スマートウィザード設定 42
Web マネージャの画面構成 44
　Web マネージャのメイン画面について 44
Web マネージャのメニュー構成 45

第 6 章　System（スイッチの主な設定） 49

Device Information（デバイス情報） 50
System Information Settings（システム情報設定 ） 51
Peripheral Settings（環境設定） 51
Port Configuration（ポート設定） 52
　Port Settings（スイッチのポート設定） 52
　Port Status（ポートステータス） 53
　Port GBIC 54
　Port Auto Negotiation（オートネゴシエーション） 54
　Error Disable Settings（エラーによるポートの無効） 55

Jumbo Frame（ジャンボフレームの有効化）....56
Interface Description（インタフェース概要）....56
Loopback Test（ループバックテスト）....57
PoE（DGS-1530-28P/52P）....58
PoE System（PoE システム設定）....58
PoE Status（PoE ステータス）....59
PoE Configuration（PoE 設定）....60
PD Alive（PD アライブ）....61
PoE Statistics（PoE 統計）....62
PoE Measurement（PoE 計測）....62
PoE LLDP Classification（PoE LLDP 分類表示）....63
System Log（システムログ構成）....64
System Log Settings（システムログ設定）....64
System Log Discriminator Settings（システムログディスクリミネータ設定）....65
System Log Server Settings（システムログサーバの設定）....66
System Log（Syslog ログ）....67
System Attack Log（システムアタックログ）....67
Time and SNTP（時刻設定）....68
Clock Settings（時間設定）....68
Time Zone Settings（タイムゾーン設定）....68
SNTP Settings（SNTP 設定）....70
Time Range（タイムレンジ設定）....71
PTP（PTP 設定）....72
PTP Global Settings（PTP グローバル設定）....72
PTP Port Global Settings（PTP ポートグローバル設定）....73
Reset Button Settings（リセットボタンの設定）....73
Archive Settings（アーカイブ設定）....74

第 7 章　Management（スイッチの管理）　75

Command Logging（コマンドログ設定）....76
User Accounts Settings（ユーザアカウント設定）....76
Password Encryption（パスワード暗号化）....78
Password Recovery（パスワードリカバリ）....78
Login Method（ログイン方法）....79
Web Login Lock Settings（Web ログインロック設定）....80
SNMP（SNMP 設定）....81
トラップ....81
MIB....81
SNMP Global Settings（SNMP グローバル設定）....82
SNMP Linkchange Trap Settings（SNMP リンクチェンジトラップ設定）....83
SNMP View Table Settings（SNMP ビューテーブル設定）....83
SNMP Community Table Settings（SNMP コミュニティテーブル設定）....84
SNMP Group Table Settings（SNMP グループテーブル）....85
SNMP Engine ID Local Settings（SNMP エンジン ID ローカル設定）....86
SNMP User Table Settings（SNMP ユーザテーブル設定）....86
SNMP Host Table Settings（SNMP ホストテーブル設定）....87
RMON（RMON 設定）....88
RMON Global Settings（RMON グローバル設定）....88
RMON Statistics Settings（RMON 統計情報）....88
RMON History Settings（RMON ヒストリ設定）....89
RMON Alarm Settings（RMON アラーム設定）....90
RMON Event Settings（RMON イベント設定）....91
Telnet/Web（Telnet/Web 設定）....92
Session Timeout（セッションタイムアウト）....92
DHCP（DHCP 設定）....93
Service DHCP（DHCP サービス）....93
DHCP Class Settings（DHCP クラス設定）....93
DHCP Pool Settings（DHCP プール設定）....94
DHCP Server（DHCP サーバ）....95
DHCPv6 Server（DHCPv6 サーバ設定）....101
DHCP Relay（DHCP リレー）....105
DHCPv6 Relay（DHCPv6 リレー）....109
DHCP Auto Configuration（DHCP 自動コンフィグ設定）....115
DHCP Auto Image Settings（DHCP 自動イメージ設定）....116
DNS（ドメインネームシステム）....117
DNS Global Settings（DNS グローバル設定）....117

DNS Name Server Settings（DNS ネームサーバ設定）....117
DNS Host Settings（DNS ホスト名設定）....118
NTP（NTP 設定）....118
NTP Global Settings（NTP グローバル設定）....118
NTP Server Settings（NTP サーバ設定）....119
NTP Peer Settings（NTP ピア設定）....120
NTP Access Group Settings（NTP アクセスグループ設定）....120
NTP Key Settings（NTP キー設定）....121
NTP Interface Settings（NTP インタフェース設定）....122
NTP Associations（NTP アソシエーション）....122
NTP Status（NTP ステータス）....123
File System（ファイルシステム設定）....124
Stacking（スタッキング設定）....126
Physical Stacking（物理スタッキング）....130
Stacking Bandwidth（スタッキング帯域）....131
シングル IP マネジメント（SIM）設定....132
シングル IP マネジメント（SIM）の概要....132
シングル IP マネジメント（SIM）のルールと動作....132
バージョン 1.61 へのアップグレード....133
Single IP Settings（シングル IP 設定）....134
Topology（トポロジ）....135
Firmware Upgrade（ファームウェア更新）....138
Configuration File Backup/ Restore（コンフィグレーションファイルのバックアップ / リストア）....138
Upload Log File（ログファイルのアップロード）....139
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）....139
DDP Settings....139
DDP Neighbors（DDP 隣接機器）....140
SMTP Settings（SMTP 設定）....141
Reboot Schedule Settings（再起動スケジュール設定）....142
NLB FDB Settings（NLB FDB 設定）....143
PPPoE Circuit ID Insertion Settings（PPPoE 回線 ID 挿入設定）....144
TCP Path MTU Discovery（TCP パス MTU 検出）....144
TCP Selective ACK（TCP 選択的確認応答）....145
TWAMP（TWAMP 設定）....145
TWAMP Settings（TWAMP 設定）....145
TWAMP Server Connections（TWAMP サーバ接続）....146
TWAMP Server Sessions....146

第 8 章　L2 Features（L2 機能の設定）　147

FDB（FDB 設定）....148
Static FDB（スタティック FDB の設定）....148
MAC Address Table Settings（MAC アドレステーブル設定）....149
MAC Address Table（MAC アドレステーブル）....150
MAC Notification（MAC 通知）....151
VLAN について....152
IEEE 802.1p プライオリティについて....152
VLAN とは....152
IEEE 802.1Q VLAN....152
VLAN（VLAN 設定）....157
VLAN Configuration Wizard（VLAN 設定ウィザード）....157
802.1Q VLAN（802.1Q VLAN）....159
VLAN Interface（VLAN インタフェース）....159
802.1v Protocol VLAN（802.1v プロトコル VLAN）....164
GVRP（GVRP の設定）....165
Asymmetric VLAN（Asymmetric VLAN 設定）....168
MAC VLAN（MAC VLAN 設定）....168
L2VLAN Interface Description（L2VLAN インタフェース概要）....169
Auto Surveillance VLAN（自動サーベイランス VLAN）....170
Voice VLAN（音声 VLAN）....172
Private VLAN（プライベート VLAN 設定）....175
VLAN Tunnel（VLAN トンネル）....176
Dot1q Tunnel（Dot1q トンネル）....176
VLAN Mapping（VLAN マッピング）....177
VLAN Mapping Profile（VLAN マッピングプロファイル）....178
STP（スパニングツリー設定）....182
802.1Q-2005 MSTP....182

802.1D-2004 Rapid STP 182
ポートの状態遷移 182
STP Global Settings（STP グローバル設定） 184
STP Port Settings（STP ポートの設定） 185
MST Configuration Identification（MST の設定） 186
STP Instance（STP インタンス設定） 187
MSTP Port Information（MSTP ポート情報） 187
ERPS (G.8032)（イーサネットリングプロテクション設定） 188
ERPS 188
ERPS Profile（ERPS プロファイル） 192
Loopback Detection（ループバック検知設定） 193
Link Aggregation（リンクアグリゲーション） 194
ポートトランクグループについて 194
Flex Links（フレックスリンク） 197
L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル） 197
L2 Multicast Control（L2 マルチキャストコントロール） 199
IGMP Snooping（IGMP Snooping の設定） 199
MLD Snooping（MLD スヌーピング） 207
Multicast VLAN（マルチキャスト VLAN） 214
Multicast Filtering Mode（マルチキャストフィルタリングモード） 217
LLDP 218
LLDP Global Settings（LLDP グローバル設定） 218
LLDP Port Settings（LLDP ポート設定） 219
LLDP Management Address List（LLDP 管理アドレスリスト） 220
LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定） 220
LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定） 221
LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定） 221
LLDP-MED Port Settings（LLDP-MED ポート設定） 222
LLDP Statistics Information（LLDP 統計情報） 223
LLDP Local Port Information（LLDP ローカルポート情報） 223
LLDP Neighbor Port Information（LLDP ネイバポート情報） 225

第 9 章　L3 Features（レイヤ 3 機能の設定） 227

ARP（ARP 設定） 228
ARP Aging Time（ARP エージングタイム設定） 228
Static ARP（スタティック ARP 設定） 228
Proxy ARP（プロキシ ARP） 229
ARP Table（ARP テーブルの参照） 229
Gratuitous ARP（Gratuitous ARP 設定） 230
IPv6 Neighbor（IPv6 ネイバ設定） 231
Interface（インタフェース設定） 232
IPv4 Interface（IPv4 インタフェース） 232
IPv6 Interface（IPv6 インタフェース） 234
Loopback Interface（ループバックインタフェース設定） 237
Null Interface（Null インタフェース） 238
UDP Helper（UDP ヘルパー） 238
IP Forward Protocol（IP 転送プロトコル） 238
IP Helper Address（IP ヘルパーアドレス） 239
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定） 240
IPv4 Route Table（IPv4 ルートテーブル） 241
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定） 241
IPv6 Route Table（IPv6 ルートテーブル） 242
IPv6 General Prefix（IPv6 汎用プレフィックス） 242
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル） 243
IPMC（IP マルチキャスト設定） 243
IPv6MC（IPv6 マルチキャスト設定） 244

第 10 章　QoS（QoS 機能の設定） 246

QoS の長所 247
QoS について 247
Basic Settings（基本設定） 248
Port Default CoS（ポートデフォルト CoS 設定） 248
Port Scheduler Method（ポートスケジューラ方式設定） 248
Queue Settings（QoS 設定） 249
CoS to Queue Mapping（CoS キューマッピング設定） 250
Port Rate Limiting（ポートレート制限設定） 250

Queue Rate Limiting（キューレート制限設定）.....251
Advanced Settings（アドバンス設定）.....252
DSCP Mutation Map（DSCP 変更マップ設定）.....252
Port Trust State（ポートトラスト設定）.....253
DSCP CoS Mapping（DSCP CoS マップ設定）.....253
CoS Color Mapping（CoS カラーマップ設定）.....254
DSCP Color Mapping（DSCP カラーマップ設定）.....254
Class Map（クラスマップ設定）.....254
Aggregate Policer（集約ポリサー設定）.....256
Policy Map（ポリシーマップ設定）.....258
Policy Binding（ポリシーバインディング設定）.....260

第 11 章　ACL（ACL 機能の設定）　262

ACL Configuration Wizard（ACL 設定ウィザード）.....263
手順 1：アクセスリストのアサイン（ACL 設定ウィザード）.....263
手順 2：パケットタイプ選択（ACL 設定ウィザード）.....264
手順 3：ルール追加（ACL 設定ウィザード）.....264
手順 4：ポート設定（ACL 設定ウィザード）.....274
ACL Access List（ACL アクセスリスト）.....275
Add Rule（ACL ルールの追加）.....277
ACL Interface Access Group（ACL インタフェースアクセスグループ）.....288
ACL VLAN Access Map（ACL VLAN アクセスマップ）.....289
Match Access-List（照合アクセスリスト設定）.....290
ACL VLAN Filter（ACL VLAN フィルタ設定）.....291
CPU ACL（CPU ACL 設定）.....291

第 12 章　Security（セキュリティ機能の設定）　294

Port Security（ポートセキュリティ）.....295
Port Security Global Settings（ポートセキュリティグローバル設定）.....295
Port Security Port Settings（ポートセキュリティポート設定）.....296
Port Security Address Entries（ポートセキュリティアドレスエントリ設定）.....297
802.1X（802.1X 設定）.....298
802.1X Global Settings（802.1X グローバル設定）.....302
802.1X Port Settings（802.1X ポート設定）.....302
Authentication Session Information（認証セッションの状態）.....303
Authenticator Statistics（オーセンティケータ統計情報）.....303
Authenticator Session Statistics（オーセンティケータセッション統計情報）.....304
Authenticator Diagnostics（オーセンティケータ診断）.....304
AAA（AAA 設定）.....305
AAA Global Settings（AAA グローバル設定）.....305
Application Authentication Settings（アプリケーションの認証設定）.....305
Application Accounting Settings（アプリケーションアカウンティング設定）.....306
Authentication Settings（認証設定）.....307
Accounting Settings（アカウンティング設定）.....309
Server RADIUS Dynamic Author Settings（RADIUS サーバダイナミックオーサー設定）.....310
RADIUS（RADIUS 設定）.....311
RADIUS Global Settings（RADIUS グローバル設定）.....311
RADIUS Server Settings（RADIUS サーバの設定）.....311
RADIUS Group Server Settings（RADIUS グループサーバの設定）.....312
RADIUS Statistic（RADIUS 統計情報）.....313
TACACS+（TACACS+ 設定）.....314
TACACS+ Server Settings（TACACS+ サーバの設定）.....314
TACACS+ Group Server Settings（TACACS+ グループサーバの設定）.....314
TACACS+ Statistic（TACACS+ 統計情報）.....315
IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）.....316
IPv4.....316
IPv6.....326
DHCP Server Screening（DHCP サーバスクリーニング設定）.....333
DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）.....333
DHCP Server Screening Port Settings（DHCP サーバスクリーニングポート設定）.....334
ARP Spoofing Prevention（ARP スプーフィング防止設定）.....335
BPDU Attack Protection（BPDU アタック防止設定）.....336
NetBIOS Filtering（NetBIOS フィルタリング設定）.....337
MAC Authentication（MAC 認証）.....338
Web-based Access Control（Web 認証）.....339
Web Authentication（Web 認証設定）.....341

WAC Port Settings（Web 認証ポート設定）.....341
WAC Customize Page（WAC カスタマイズページ設定）.....342
Network Access Authentication（ネットワークアクセス認証）.....343
Guest VLAN（ゲスト VLAN 設定）.....343
Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）.....343
Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）.....345
Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）.....346
Safeguard Engine（セーフガードエンジン）.....347
Safeguard Engine Settings（セーフガードエンジン設定）.....348
CPU Protect Counters（CPU プロテクトカウンタ）.....348
CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）.....349
CPU Protect Type（CPU プロテクトタイプ）.....349
Trusted Host（トラストホスト）.....350
Traffic Segmentation（トラフィックセグメンテーション）.....350
Storm Control Settings（ストームコントロール設定）.....351
DoS Attack Prevention Settings（DoS 攻撃防止設定）.....353
SSH（Secure Shell）.....354
SSH Global Settings（SSH グローバル設定）.....354
SSH Algorithm Settings（SSH アルゴリズム設定）.....355
Host Key（Host Key 設定）.....356
SSH Server Connection（SSH サーバ接続）.....356
SSH User Settings（SSH ユーザ設定）.....357
SSH Client Settings（SSH クライアント設定）.....357
SSL（Secure Socket Layer）.....358
SSL Global Settings（SSL グローバル設定）.....359
Crypto PKI Trustpoint（暗号 PKI トラストポイント）.....360
SSL Service Policy（SSL サービスポリシー）.....361
Network Protocol Port Protect Settings（ネットワークプロトコルポート保護設定）.....362

第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)　364

CFM（Connectivity Fault Management : 接続性障害管理）.....365
CFM Settings（CFM 設定）.....365
CFM Port Settings（CFM ポート設定）.....372
CFM Loopback Test（CFM ループバックテスト）.....373
CFM Linktrace Settings（CFM リンクトレース設定）.....374
CFM Packet Counter（CFM パケットカウンタ）.....375
CFM Counter CCM（CFM カウンタ CCM）.....375
CFM MIP CCM Table（CFM MIP CCM テーブル）.....376
CFM MEP Fault Table（CFM MEP 障害テーブル）.....376
Cable Diagnostics（ケーブル診断機能）.....377
Ethernet OAM（イーサネット OAM）.....378
Ethernet OAM Settings（イーサネット OAM 設定）.....378
Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）.....379
Ethernet OAM Event Log Table（イーサネット OAM イベントログテーブル）.....380
Ethernet OAM Statistics Table（イーサネット OAM 統計情報テーブル）.....381
Ethernet OAM DULD Settings（イーサネット OAM DULD 設定）.....382
DDM（DDM 設定）.....383
DDM Settings（DDM 設定）.....383
DDM Temperature Threshold Settings（DDM 温度しきい値設定）.....384
DDM Voltage Threshold Settings（DDM 電圧しきい値設定）.....384
DDM Bias Current Threshold Settings（DDM バイアス電流しきい値設定）.....385
DDM TX Power Threshold Settings（DDM 送信電力しきい値設定）.....385
DDM RX Power Threshold Settings（DDM 受信電力しきい値設定）.....386
DDM Status Table（DDM ステータステーブル）.....386

第 14 章　Monitoring（スイッチのモニタリング）　387

VLAN Counter（VLAN カウンタ）.....388
Utilization（利用分析）.....389
Port Utilization（ポート使用率）.....389
History Utilization（使用率履歴）.....389
Statistics（統計情報）.....390
Port（ポート統計情報）.....390
CPU Port（CPU ポート）.....392
Interface Counters（インタフェースカウンタ）.....392
Interface History Counters（インタフェースカウンタ履歴）.....394
Counters（カウンタ）.....395

Mirror Settings（ミラー設定）.....397
sFlow（sFlow 設定）.....399
sFlow Agent Information（sFlow エージェント情報）.....399
sFlow Receiver Settings（sFlow レシーバ設定）.....399
sFlow Sampler Settings（sFlow サンプラ設定）.....400
sFlow Poller Settings（sFlow ポーラー設定）.....400
Device Environment（機器環境確認）.....401

第 15 章　Green（省電力機能）　402

Power Saving（省電力）.....403
EEE（Energy Efficient Ethernet/ 省電力イーサネット）.....404

第 16 章　Save and Tools（Save メニュー /Tools メニュー）　405

Save（Save メニュー）.....406
Save Configuration（コンフィグレーションの保存）.....406
Tools（Tools メニュー）.....406
Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）.....406
Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）.....411
Certificate & Key Restore & Backup（証明書 / 鍵リストア＆バックアップ）.....417
Log Backup（ログファイルのバックアップ）.....422
Ping.....424
Trace Route（トレースルート）.....426
Language Management（言語管理）.....428
Reset（リセット）.....428
Reboot System（システム再起動）.....428
Wizard（ウィザード）.....429
Online Help（オンラインヘルプ）.....429
D-Link Support Site（D-Link サポート Web サイト（英語））.....429
User Guide（ユーザガイド（英語版））.....429
言語.....429
Logout（ログアウト）.....429

付録　430

付録 A パスワードリカバリ手順.....430
付録 B システムログエントリ.....431
付録 C トラップログエントリ.....456
付録 D RADIUS 属性割り当て.....465
付録 E IETF RADIUS 属性サポート.....468
付録 F 機能設定例.....470
対象機器について.....470
Traffic Segmentation（トラフィックセグメンテーション）.....470
VLAN.....471
Link Aggregation（リンクアグリゲーション）.....472
Access List（アクセスリスト）.....473
Loopback Detection（LBD）（ループ検知）.....474

はじめに

DGS-1530 シリーズユーザマニュアルは、シリーズの設置方法および操作方法について記載しています。

- 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
  - スイッチの設置方法、電源接続の方法について説明します。
- 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　スイッチ管理について
  - パスワード設定、SNMP 設定、および各種インタフェース経由での本スイッチへの接続など基本的なスイッチの管理について説明します。
- 第 5 章　Web ベースのスイッチ管理
  - Web ベースの管理機能への接続方法および使用方法について説明します。
- 第 6 章　System（スイッチの主な設定）
  - デバイス情報、ポート設定、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 7 章　Management（スイッチの管理）
  - ユーザアカウント、シングル IP マネジメント設定、SNMP 設定、Telnet 設定、Web 設定などの管理機能について説明します。
- 第 8 章　L2 Features（L2 機能の設定）
  - VLAN、リンクアグリゲーション、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 9 章　L3 Features（レイヤ 3 機能の設定）
  - ARP 設定、インタフェース設定、スタティックルート設定などのレイヤ 3 機能について説明します。
- 第 10 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 デフォルトプライオリティなどの機能を含みます。
- 第 11 章　ACL（ACL 機能の設定）
  - ACL アクセスリスト、ACL VLAN アクセスマップ、CPU ACL などの ACL（アクセスコントロールリスト）機能について説明します。
- 第 12 章　Security（セキュリティ機能の設定）
  - 802.1X、Web ベース認証、MAC ベース認証、トラストホスト、ポートセキュリティ、トラフィックセグメンテーション、SSL、SSH、IP-MAC- ポートバインディング、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 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)
  - CFM（接続性障害管理）、イーサネット OAM、DDM、ケーブル診断機能について説明します。
- 第 14 章　Monitoring（スイッチのモニタリング）
  - CPU 使用率、パケットのエラーやパケットサイズなどの統計情報、ミラーリング、sFlow などのモニタ機能について説明します。
- 第 15 章　Green（省電力機能）
  - 省電力設定、EEE（Energy Efficient Ethernet/ 省電力イーサネット）設定について説明します。
- 第 16 章　Save and Tools（Save メニュー /Tools メニュー）
  - コンフィグレーションの保存、ファームウェアアップグレード＆バックアップ、コンフィグレーションリストア＆バックアップ、ログファイルのバックアップ、Ping、トレースルート、リセット、システム再起動などのツール機能について説明します。

- 付録 A パスワードリカバリ手順
  - パスワードのリセット、リカバリについて説明します。
- 付録 B システムログエントリ
  - スイッチのシステムログに出力されるログエントリについて説明します。
- 付録 C トラップログエントリ
  - トラップログエントリついて説明します。
- 付録 D RADIUS 属性割り当て
  - スイッチの RADIUS 属性割り当てについて説明します。
- 付録 E IETF RADIUS 属性サポート
  - スイッチによりサポートされる IETF RADIUS 属性一覧です。
- 付録 F 機能設定例
  - スイッチの機能設定例です。

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	HW バージョン	品番
DGS-1530-10	A1	DGS-1530-10/A1
DGS-1530-20	A1	DGS-1530-20/A1
DGS-1530-28	A1	DGS-1530-28/A1
DGS-1530-28P	A1	DGS-1530-28P/A1
DGS-1530-28S	A1	DGS-1530-28S/A1
DGS-1530-28SC	A1	DGS-1530-28SC/A1
DGS-1530-52	A1	DGS-1530-52/A1
DGS-1530-52P	A1	DGS-1530-52P/A1

第 1 章　本製品のご使用にあたって

- スイッチ概要
- 搭載ポート
- オプションモジュール（光トランシーバ / ダイレクトアタッチケーブル）
- 前面パネル
- 背面パネル
- 側面パネル

スイッチ概要

DGS-1530 シリーズは、多様なポート数、ポート構成をラインナップしたギガビット L2 スマートマネージドスイッチです。比較的小さなネットワークのディストリビューションスイッチや、大きなネットワークのエッジスイッチとしての利用に適しています。
802.1X/MAC アドレス認証 /WEB 認証の標準装備に加えて、Compound 認証や中間者攻撃対策等により強固なセキュリティを実現できます。イーサネットリングや OAM 機能、CFM 機能といったメトロイーサネットの機能が充実していることも特長です。また、50℃の環境で動作可能、リダンダント電源※をサポートしているなど、様々な環境で安定したネットワーク環境を提供することができます。

マルチキャスト制御に対応
IGMP/MLD スヌーピングなど、豊富な L2 マルチキャスト機能を搭載しています。ホストベース IGMP/ MLD スヌーピングでは物理インターフェイスごとに複数の利用者にサービスを提供し、ISM VLAN ではマルチキャスト VLAN 内でマルチキャストストリームを登録してネットワークバックボーン上の帯域幅を節約することができます。また、本製品は QoS 機能をサポートしており、高品質なマルチキャストサービスを提供します。

強固なセキュリティと高可用性
IEEE802.1X 認証 /MAC アドレス認証 /Web 認証 /Compound 認証をはじめとする充実したエンドポイントセキュリティ機能に加えて、ARP スプーフィング防止や DHCP サーバスクリーニングなどの中間者攻撃対策機能も実装し、強固なセキュリティを実現することが可能です。また、これらの機能に加え、不正な攻撃とウイルス / ワームによるスイッチのオーバロードを防止するために D-Link セーフガードエンジンによりスイッチの信頼性と可用性を向上させます。

信頼性の高いネットワーク
最大 9 台までの物理スタックに対応し、筐体の障害時にもダウンタイムを最小限にした機器の交換や運用が可能です。また、物理スタックにリンクアグリゲーションやリングプロトコルを組み合わせて使用することで、経路の冗長性も確保することができるため、より信頼性の高いネットワークを構築できます。リダンダント電源※にも対応しているため、主電源にトラブルがあった場合でも電源を供給することが可能です。また、本製品は OAM 機能、CFM 機能、ケーブル診断機能などを搭載しており、メンテナンスとトラブルシューティングをより効率よく行うことができます。

高い耐環境性能を装備
省エネに対応するだけでなく、動作環境温度を最大 50℃まで対応可能です。また、イーサネット（RJ-45）ポートでは 6KV サージプロテクションを実装し、落雷や電気配線の不具合による電力サージからスイッチを保護する耐環境性能を実装しています。

※ DGS-1530-28P を除く

搭載ポート

本シリーズは以下のポートを搭載しています。

製品名	10/100/1000BASE-T ポート（PoE 給電）	SFP スロット	10G SFP+ スロット
DGS-1530-10	8	—	2
DGS-1530-20	16	—	4
DGS-1530-28	24	—	4
DGS-1530-28P	24（24）	—	4
DGS-1530-28S	—	24	4
DGS-1530-28SC	4 （SFP 4 スロットとのコンボ）	24	4
DGS-1530-52	48	—	4
DGS-1530-52P	48（48）	—	4

オプションモジュール（光トランシーバ / ダイレクトアタッチケーブル）

本シリーズには SFP/ SFP + スロットが搭載されており、以下のモジュールを使用することができます。

■ 光トランシーバ

種別	製品名
SFP+(10Giga)	DEM-431XT
	DEM-432XT
Copper SFP+（10Giga）	DEM-410T※1※2
2 芯 SFP(1Giga)	DEM-310GT
	DEM-311GT
Copper SFP(1Giga)	DGS-712※3※4

※ 1：DGS-1520-10 および DGS-1530-20 で使用可能な数はスイッチ 1 台に対し最大 1 個までとなります。その他のモデルはスイッチ 1 台に対し最大 4 個までとなります。
※ 2：DEM-410T を使用する場合、環境温度（室温）が 40℃までの環境での利用のみをサポートしています。そのため、この場合のスイッチの動作温度範囲も 0 ～ 40℃までとなりますので、十分にご注意ください。
※ 3：SFP スロットでのみ使用可能です。Combo スロットでは使用できません。
※ 4：DGS-1530-10/28SC を除く
※ 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。

■ リダンダント電源

種別	製品名
リダンダント電源システム	DPS-500A※1
	DPS-700※2※3

※ 1：DGS-1530 シリーズで DPS-500A を使用するには、DPS-CB150-2PS の B1 バージョンが必要です。PoE モデルではサポートされていません。
※ 2：DGS-1530-52P のみ使用できます。
※ 3：DPS-700 のハードウェアバージョン：B1 のみサポートされます。

■ ダイレクトアタッチケーブル

種別	製品名
SFP+ ダイレクトアタッチケーブル	DEM-CB100S
	DEM-CB300S

注意 光トランシーバを使用する場合、使用する対向のスイッチの機種により、双方向で受光しないとリンクアップしない場合と、片方向でもリンクアップする場合がありますのでご注意ください。

注意 リダンダント電源はホットスワップには対応していません。

前面パネル

スイッチの前面パネルは、以下のコンポーネントで構成されています。

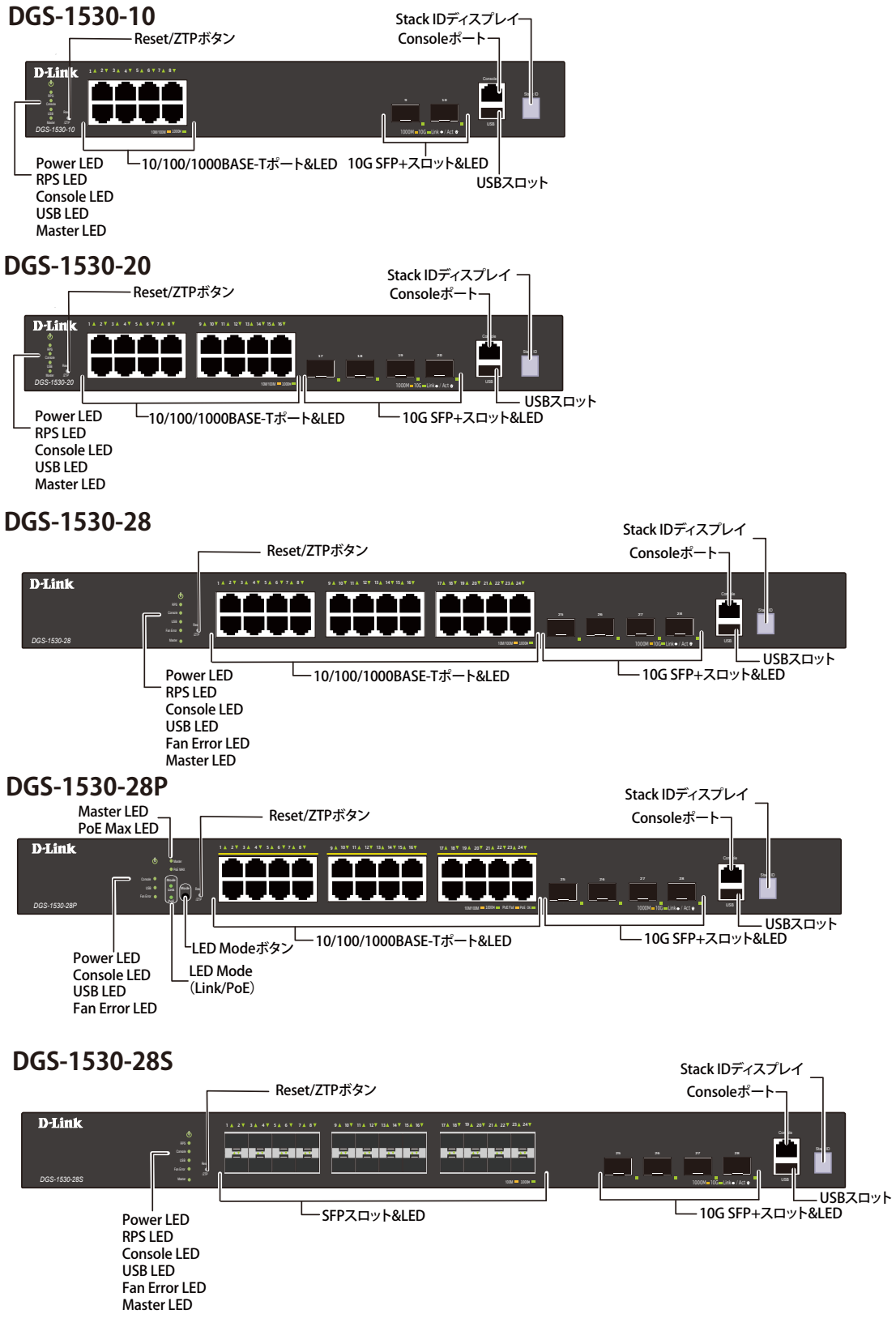


図 3-1　　DGS-1530 の前面パネル

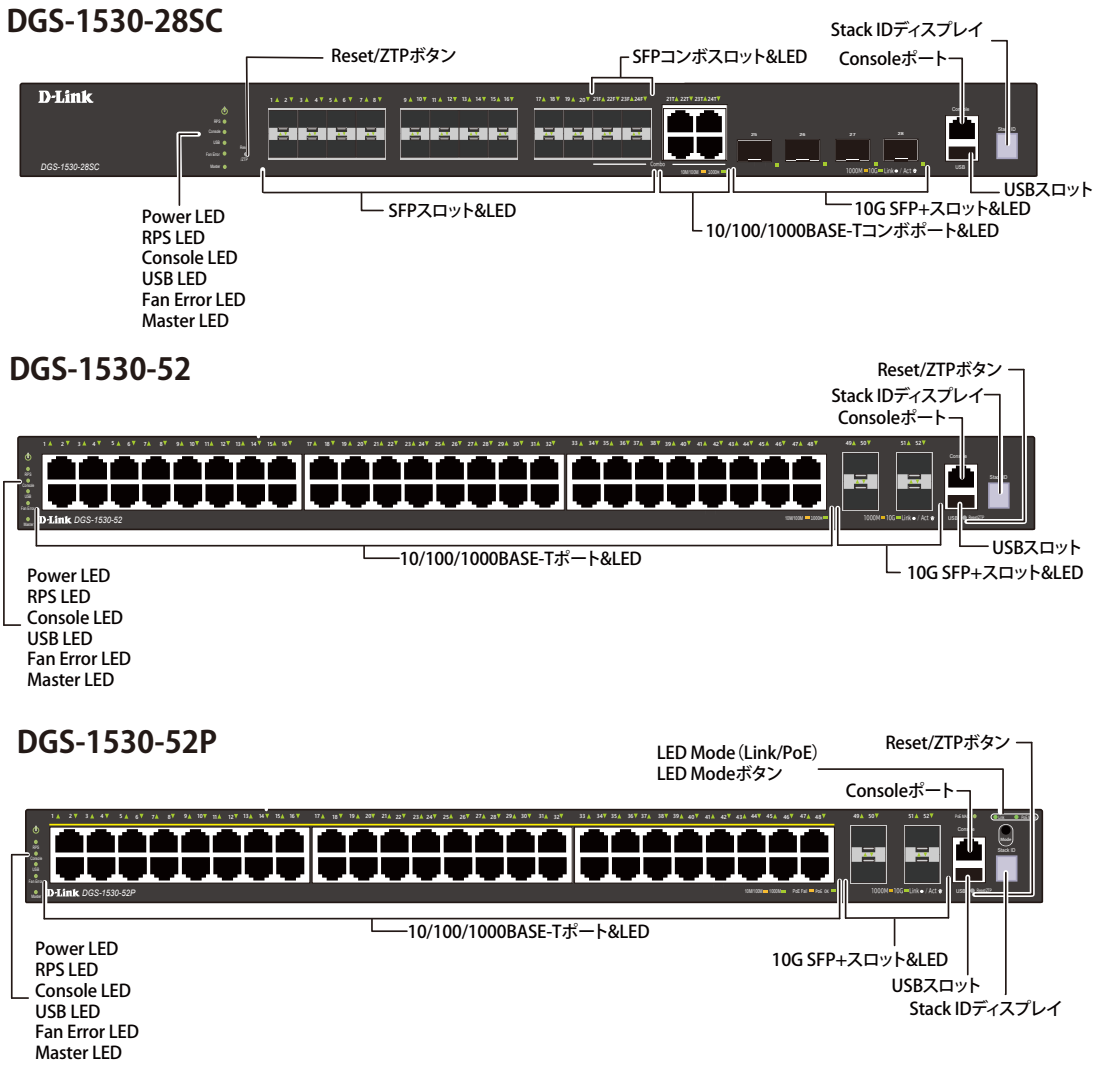


図 3-2　　DGS-1530 の前面パネル

ポート	説明
10/100/1000BASE-T ポート	10Mbps、100Mbps、1000Mbps の速度で通信を行う RJ-45 イーサネットポートです。 ※ DGS-1530-28P/52P の 10/100/1000BASE-T ポートは PoE 給電に対応しています。 ※ DGS-1530-28SC は、SFP スロット × 4 とのコンボポートとなります。ポート 21-24 の 10/100/1000BASE-T ポートと SFP スロットは同時に利用することはできません。
SFP スロット （DGS-1530-28S/28SC のみ）	1000Mbps の速度で通信を行う SFP スロットです。
10 G SFP+ スロット	1000Mbps または 10Gbps の速度で通信を行う SFP+ スロットです。
RJ-45 コンソールポート	コマンドラインインタフェース（CLI）に接続してスイッチの管理を行う RJ45 コンソールポートです。 同梱のコンソールケーブルを使用し、管理 PC のシリアルポートと接続します。
USB ポート	USB フラッシュドライブを挿入し、ファームウェアイメージやコンフィグレーションファイルを保存するなど、スイッチのファイル管理に利用することができます。
Reset/ZTP ボタン	Reset/ZTP ボタンでは、ボタンを押下する秒数により、以下の処理を実行することができます。 **スイッチの再起動（5 秒未満）** スイッチは再起動します。 **ZTP 機能の開始（5-10 秒）** スイッチは ZTP 機能を開始します。 ボタン押下後に緑色 LED が点灯し、ボタンを離すと点滅します。その後、ZTP 機能を開始してシステムは再起動します。 **工場出荷時の設定へのリセット（10 秒以上）** スイッチの設定内容を工場出荷時の状態へリセットします。 ボタン押下後に橙色 LED が点灯します。ボタンを離した後、システムの再起動とリセットが行われます。

ポート	説明
	ゼロタッチプロビジョニング（ZTP）は、デバイスの設定を自動化する機能です。
Mode ボタン （DGS-1530-28P/52P のみ）	ポート LED の表示モードを変更します。 表示モードには、**(1) Link/Act/Speed モード、(2) PoE モード**の 2 種類のモードがあります。 各モードにより、LED の点灯状態が異なります。詳細は「LED 表示」の説明をご確認ください。
各種 LED	電源、RPS、コンソール、USB、ファン、PoE、Link/Act/Speed、スタックの動作状態を表示します。

LED 表示

LED 表示により、スイッチとネットワークの状態を確認することができます。

DGS-1530-10

図 3-3　DGS-1530-10 の前面パネル LED 配置図

DGS-1530-20

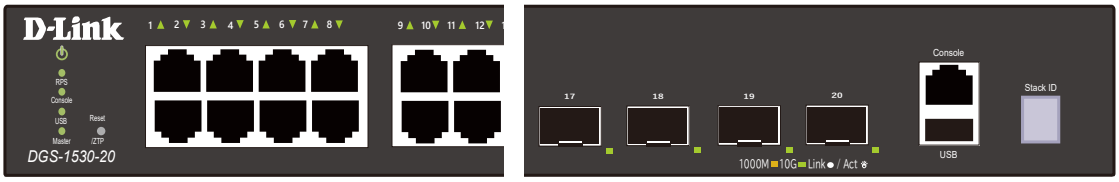


図 3-4　DGS-1530-20 の前面パネル LED 配置図

DGS-1530-28

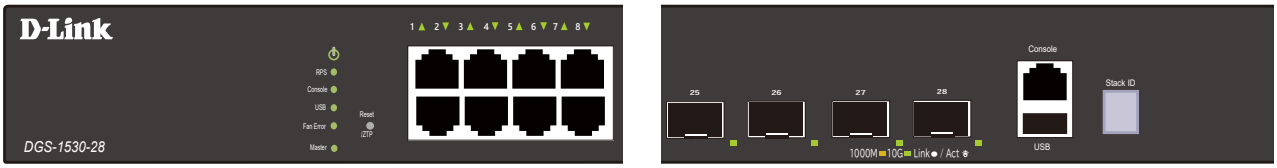


図 3-5　DGS-1530-28 の前面パネル LED 配置図

DGS-1530-28P

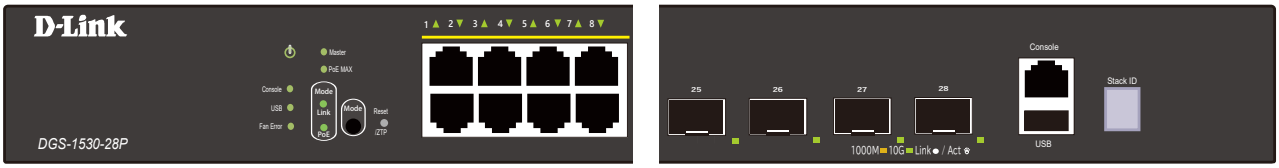


図 3-6　DGS-1530-28P の前面パネル LED 配置図

DGS-1530-28S

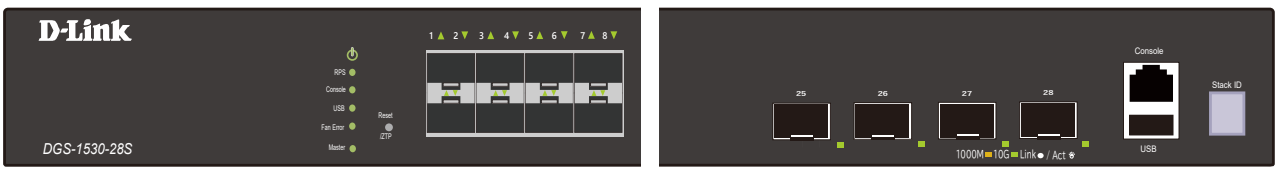


図 3-7　DGS-1530-28S の前面パネル LED 配置図

DGS-1530-28SC

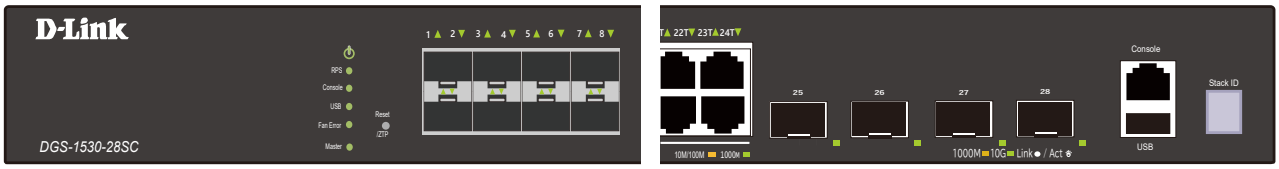


図 3-8　DGS-1530-28SC の前面パネル LED 配置図

DGS-1530-52

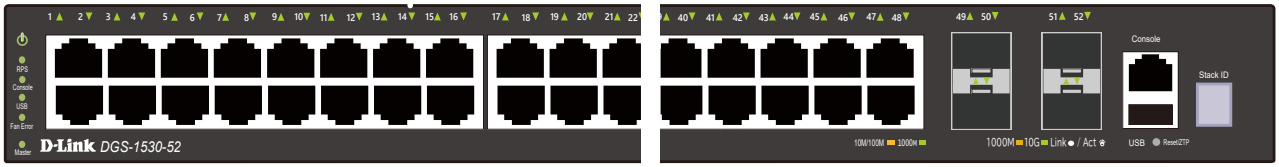


図 3-9　DGS-1530-52 の前面パネル LED 配置図

DGS-1530-52P

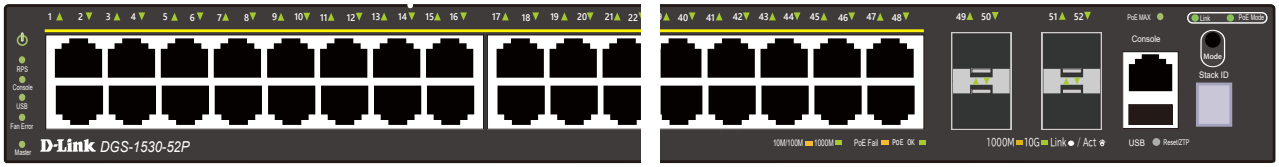


図 3-10　DGS-1530-52P の前面パネル LED 配置図

前面パネルの LED 表示について説明します。

通常動作時の LED 表示

LED		色	状態	状態説明
システム LED				
Power		緑	点灯	スイッチに電源が供給され正常に動作しています。
		ー	消灯	スイッチに電源が供給されていません。
RPS		緑	点灯	リダンダント電源ユニットが動作しています。
		ー	消灯	リダンダント電源ユニットは動作していません。
Console		緑	点灯	RJ-45 コンソールポートのリンクが確立しています。
		ー	消灯	リンクが確立していません。
USB		緑	点灯	USB ディスクが挿入されています。
			点滅	USB でデータを転送中です。
		ー	消灯	USB ディスクは挿入されていません。
Fan Error		緑	点灯	ファンが正常に動作しています。
		赤	点灯	ファンに不具合が発生しています。
PoE MAX （DGS-1530-28P/52P）		橙	点灯	接続された受電デバイスに供給している電力が、Power Guard Band（電力保護帯域）のしきい値を超えています。ポートの優先度または PoE ルールに基づき、受電デバイスへの電力供給を停止します。
			点滅	受電デバイスに供給している合計電力が Power Guard Band（電力保護帯域）を下回り、追加の受電デバイスを接続可能になると、LED は 5 秒間点滅します。 補足 Power Guard Band（電力保護帯域）は、最大供給電力のうち、7W 確保されています。
		ー	消灯	PoE 供給電力が十分あり、Power Guard Band（電力保護帯域）を下回っています。
Mode （DGS-1530-28P/52P）	Link	緑	点灯	ポート LED は Link/Act/Speed モードで表示されています。
	PoE	緑	点灯	ポート LED は PoE モードで表示されています。
Master		緑	点灯	本スイッチはスタックマスタです。（スタック機能が有効化されている場合）
			消灯	本スイッチはスタックメンバです。（スタック機能が有効化されている場合）

LED	色	状態	状態説明
Stack ID	緑	点灯（1-9）	スイッチスタックにおけるスイッチのボックス番号が表示されます。
		点灯（H）	スイッチがスイッチスタックのプライマリマスタである場合、大文字の「H」の文字が表示されます。
		点灯（h）	スイッチがスイッチスタックのバックアップマスタの場合は、小文字の「h」が表示されます。
		点灯（E）	システムによるセルフテストエラーです。
		点灯（G）	セーフガードエンジンが「exhausted」モードに入っています。
ポート LED（Link/Act/Speed モード）			
10/100/1000 ポート LED	緑	点灯	1Gbps でリンクが確立しています。
		点滅	1Gbps でデータを送受信しています。
	橙	点灯	10/100Mbps でリンクが確立しています。
		点滅	10/100Mbps でデータを送受信しています。
	ー	消灯	リンクが確立されていない、もしくはポートが無効化されています。
SFP スロット LED	緑	点灯	1Gbps でリンクが確立しています。
		点滅	1Gbps でデータを送受信しています。
	橙	点灯	100Mbps でリンクが確立しています。
		点滅	100Mbps でデータを送受信しています。
	ー	消灯	リンクが確立されていない、もしくはポートが無効化されています。
10G SFP+ スロット LED	緑	点灯	10Gbps でリンクが確立しています。
		点滅	10Gbps でデータを送受信しています。
	橙	点灯	1Gbps でリンクが確立しています。
		点滅	1Gbps でデータを送受信しています。
	ー	消灯	リンクが確立されていない、もしくはポートが無効化されています。
ポート LED（PoE モード）			
10/100/1000 ポート LED（DGS-1530-28P/52P）	緑	点灯	PoE 受電機器が接続され、電力が供給されています。
		点滅	PoE 受電機器が接続されていますが、電力を供給できません。（PD 側のエラー、過電流、給電容量の不足といった理由が考えられます。）
	ー	消灯	PoE ポートが無効状態、または PoE 受電機器が接続されていません。

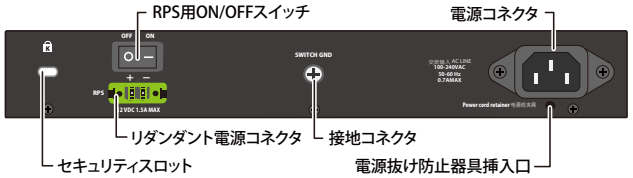
システム起動時の LED 表示

1. Power LED が緑色に点灯します。
2. ポート LED（Link/Act）が緑色 / 橙色で同時に点灯した後、交互に点灯します。その後、システムの起動が完了するまで消灯します。
3. システム起動中、7 セグメント LED（Stack ID）はすべてのセグメントが点灯します。

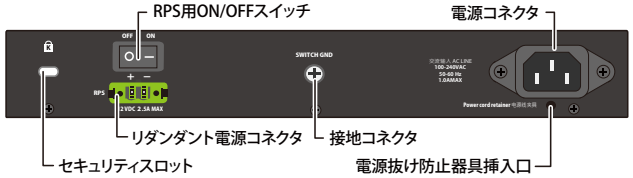
背面パネル

スイッチの背面パネルは、以下のコンポーネントで構成されています。

DGS-1530-10

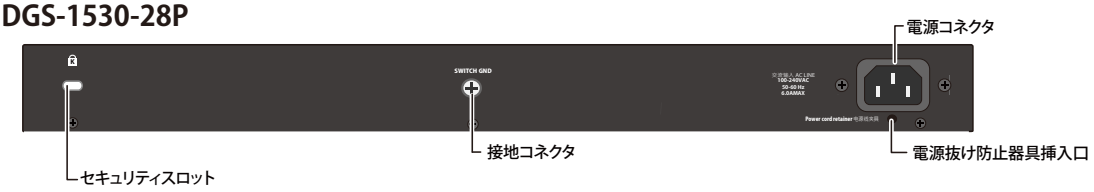


DGS-1530-20

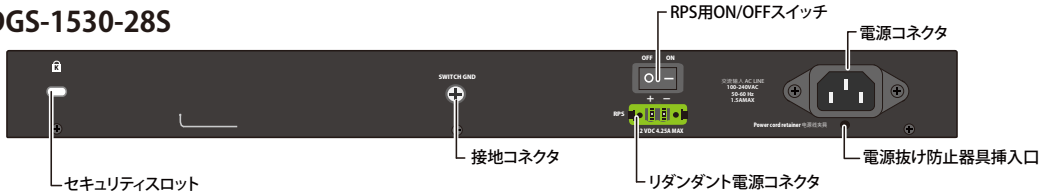


DGS-1530-28

DGS-1530-28P

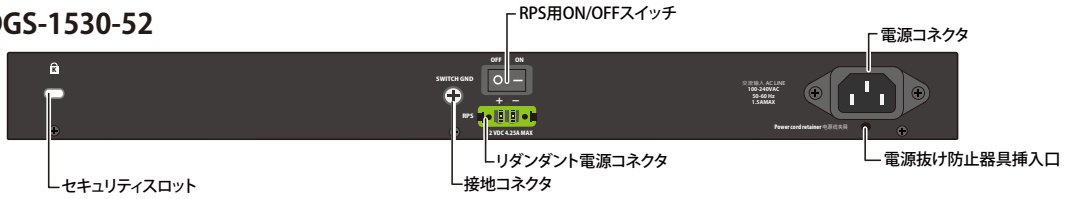


DGS-1530-28S



DGS-1530-28SC

DGS-1530-52



DGS-1530-52P

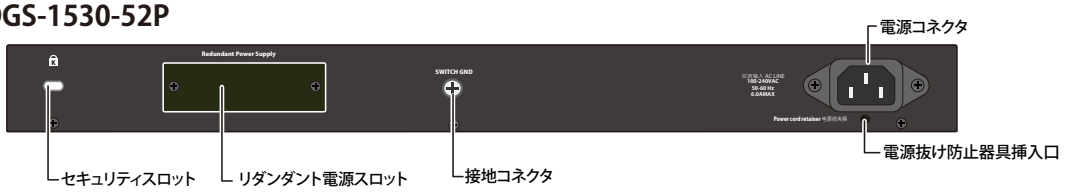


図 3-11　DGS-1530 の背面パネル

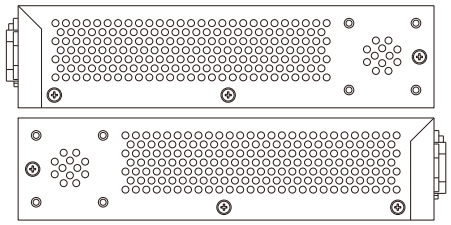
コンポーネント	説明
セキュリティスロット	Kensington セキュリティロックを使用し、本製品をロックします。Kensington セキュリティロックは同梱されていません。
リダンダント電源コネクタ	オプションの RPS（外部リダンダント電源ユニット）をリダンダント電源用コネクタに接続します。 内蔵電源ユニットに異常が発生した場合に、RPS が自動的にスイッチに電源を供給できるようにします。
接地コネクタ	接地用ケーブルの片側を接地コネクタ（スイッチ GND）に接続し、もう一方をラックなどの接地ポイントに接続します。
AC 電源コネクタ	AC 電源コネクタは標準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。 スイッチは自動的に 50/60Hz、100 ～ 240VAC 内の電圧に調整されます。
電源抜け防止器具挿入口	同梱の電源抜け防止器具を挿入し、電源ケーブルを固定します。

側面パネル

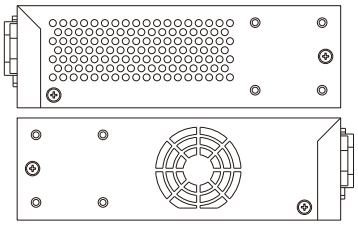
スイッチの側面パネルには、通気口、ファン、ラックマウント用のネジ穴およびネジが配置されています。

警告 側面パネルにある通気口には、スイッチが持つ熱を放出する役割があります。通気口をふさがないようにご注意ください。最適な熱放出、空気の循環をしないとシステム障害や部品の激しい損傷を引き起こす場合がありますのでご注意ください。

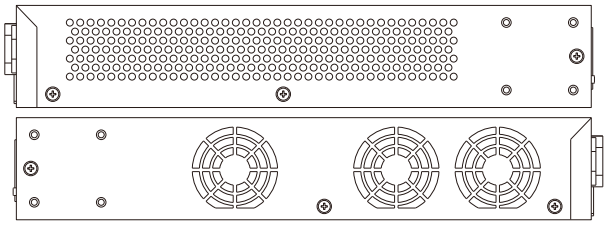
DGS-1530-10/20



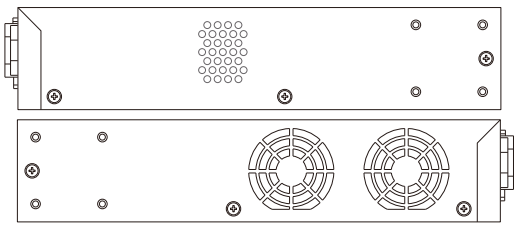
DGS-1530-28



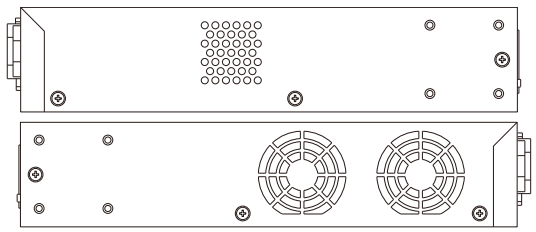
DGS-1530-28P



DGS-1530-28S/28SC



DGS-1530-52



DGS-1530-52P

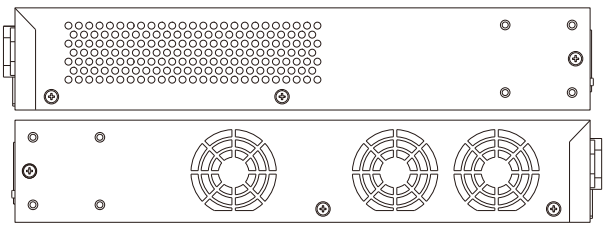


図 3-12　DGS-1530 側面パネル

スマートファンについて

本製品は「スマートファン」を搭載しています。
ハードウェアに内蔵されたセンサによってスイッチ内部の温度を検出し、自動的にファンのスピードを細かく調整することができます。

各機種のスマートファンによるスピード調整基準は以下のとおりです。

ファンモード	ファン状態		DGS-1530-28	DGS-1530-52
「Normal（ノーマル）」モード	低速 ↕ 高速	Ultra Low	• 17℃未満	• 17℃未満
		Very Low	• 15℃を超えたとき（「Ultra Low」⇒「Very Low」） • 27℃を下回ったとき（「Low」⇒「Very Low」）	• 15℃を超えたとき（「Ultra Low」⇒「Very Low」） • 27℃を下回ったとき（「Low」⇒「Very Low」）
		Low	• 30℃を超えたとき（「Very Low」⇒「Low」） • 34℃を下回ったとき（「Medium」⇒「Low」）	• 30℃を超えたとき（「Very Low」⇒「Low」） • 34℃を下回ったとき（「Medium」⇒「Low」）
		Medium	• 37℃を超えたとき（「Low」⇒「Medium」） • 40℃を下回ったとき（「High」⇒「Medium」）	• 37℃を超えたとき（「Low」⇒「Medium」） • 40℃を下回ったとき（「High」⇒「Medium」）
		High	• 43℃を超えたとき	• 43℃を超えたとき
「Quiet（静音）」モード	低速	Ultra Low	以下の条件を満たす場合、「Quiet（静音）」モードを有効化することができます。 • 30℃未満 • DEM-410T 未使用 以下のいずれかの状態になると、自動的に「Normal（ノーマル）」モードに戻ります。 • 30℃超過 • DEM-410T 使用 ※「Normal」モードに変更された後、「Quiet」モードには自動的には戻りません。	

ファンモード	ファン状態		DGS-1530-28P	DGS-1530-52P
「Normal（ノーマル）」モード	低速 ↕ 高速	Ultra Low	• 22℃未満	• 22℃未満
		Very Low	• 25℃を超えたとき（「Ultra Low」⇒「Very Low」） • 27℃を下回ったとき（「Low」⇒「Very Low」）	• 25℃を超えたとき（「Ultra Low」⇒「Very Low」） • 27℃を下回ったとき（「Low」⇒「Very Low」）
		Low	• 30℃を超えたとき（「Very Low」⇒「Low」） • 33℃を下回ったとき（「Medium」⇒「Low」）	• 30℃を超えたとき（「Very Low」⇒「Low」） • 33℃を下回ったとき（「Medium」⇒「Low」）
		Medium	• 36℃を超えたとき（「Low」⇒「Medium」） • 40℃を下回ったとき（「High」⇒「Medium」）	• 37℃を超えたとき（「Low」⇒「Medium」） • 40℃を下回ったとき（「High」⇒「Medium」）
		High	• 43℃を超えたとき	• 44℃を超えたとき
「Quiet（静音）」モード	低速	Ultra Low	以下の条件を満たす場合、「Quiet（静音）」モードを有効化することができます。 • 30℃未満 • DEM-410T 未使用 • PoE 使用量 ≤ 120W 以下のいずれかの状態になると、「Normal（ノーマル）」モードに戻ります。 • 30℃超過 • DEM-410T 使用 • PoE 使用量 ≥ 120W ※「Normal」モードに変更された後、「Quiet」モードには自動的には戻りません。	

ファンモード	ファン状態		DGS-1530-28S	DGS-1530-28SC
「Normal（ノーマル）」モード	低速 ↕ 高速	Ultra Low	• 17℃未満	• 17℃未満
		Very Low	• 20℃を超えたとき（「Ultra Low」⇒「Very Low」） • 27℃を下回ったとき（「Low」⇒「Very Low」）	• 20℃を超えたとき（「Ultra Low」⇒「Very Low」） • 27℃を下回ったとき（「Low」⇒「Very Low」）
		Low	• 30℃を超えたとき（「Very Low」⇒「Low」） • 33℃を下回ったとき（「Medium」⇒「Low」）	• 30℃を超えたとき（「Very Low」⇒「Low」） • 33℃を下回ったとき（「Medium」⇒「Low」）
		Medium	• 36℃を超えたとき（「Low」⇒「Medium」） • 40℃を下回ったとき（「High」⇒「Medium」）	• 36℃を超えたとき（「Low」⇒「Medium」） • 40℃を下回ったとき（「High」⇒「Medium」）
		High	• 43℃を超えたとき	• 43℃を超えたとき
「Quiet（静音）」モード	低速	Ultra Low	以下の条件を満たす場合、「Quiet（静音）」モードを有効化することができます。 • 30℃未満 • DEM-410T 未使用 以下のいずれかの状態になると、「Normal（ノーマル）」モードに戻ります。 • 30℃超過 • DEM-410T 使用 ※「Normal」モードに変更された後、「Quiet」モードには自動的には戻りません。	

補足 DGS-1530-10/20 はファンレススイッチです。

注意 ファンの速度は、DGS-712 の使用や PoE 供給可能電力の変更により調整される場合があります。

参照 ファンの動作モードは WebUI や CLI で設定することが可能です。詳細は「Peripheral Settings（環境設定）」の説明をご確認ください

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
- SFP/SFP+ スロットへのモジュールの取り付け
- 電源抜け防止器具の装着
- リダンダント電源システムの設置
- 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　x　1
- AC 電源ケーブル（100V 用）　x　1
- RJ-45/RS232C コンソールケーブル　x　1
- 19 インチラックマウントキット（ブラケット、ネジ）　x　1
- ゴム足　x　4
- DC 電源コネクタ（28P/52P を除く）　x　1
- 電源抜け防止器具　x　1
- マニュアル　x　1
- PL シート　x　1

万一、不足しているものや損傷などがありましたら、ご購入頂いた販売代理店までご連絡ください。

ネットワーク接続前の準備

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

- スイッチは、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。また、スイッチの上に重いものを置かないでください。
- 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本スイッチの周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後 10 cm 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製足をスイッチの裏面の四隅に取り付けます。スイッチの周囲に十分な通気を確保するようにしてください。

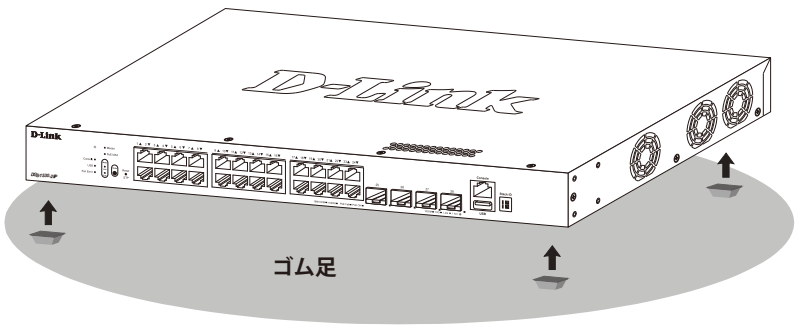


図 2-1　ゴム足の取り付け

19 インチラックへの取り付け

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

1. 電源ケーブルおよびケーブル類が本体に接続していないことを確認します。
2. 付属のネジで、スイッチの正面側の側面に、ブラケットを取り付けます。

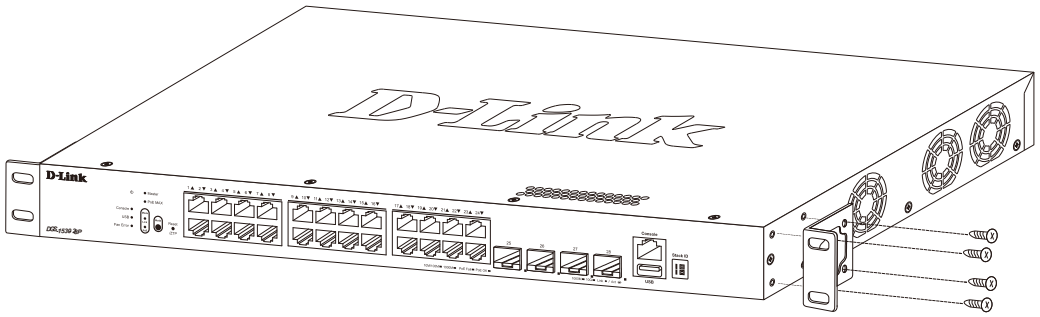


図 2-2　ブラケットの取り付け

3. 19 インチラックに付属のネジを使用し、スイッチをラックに固定します。

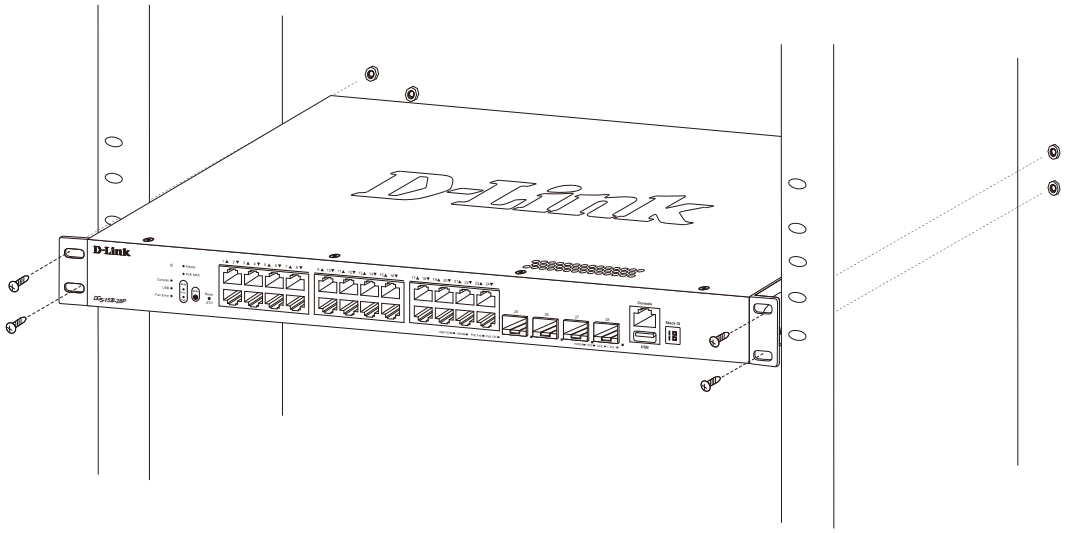


図 2-3　19 インチラックへの取り付け

注意 スイッチのエアフロー、換気、熱放出を考慮し、スイッチの周りに適切なスペースを確保してください。

SFP/SFP+ スロットへのモジュールの取り付け

本シリーズには SFP/SFP+ ロットが搭載されています。 これらスロットを使用して、標準の RJ45 接続をサポートしないさまざまなネットワークデバイスをスイッチに接続することができます。

これらのスロットは通常、光ファイバ通信に接続するために使用され、長距離接続に対応することができます。 RJ45 接続の最大到達距離は 100 メートル、光ファイバ接続は最大数キロメートルとなります。

以下に、スイッチの SFP+ スロットに光トランシーバを挿入した例を図に示します。

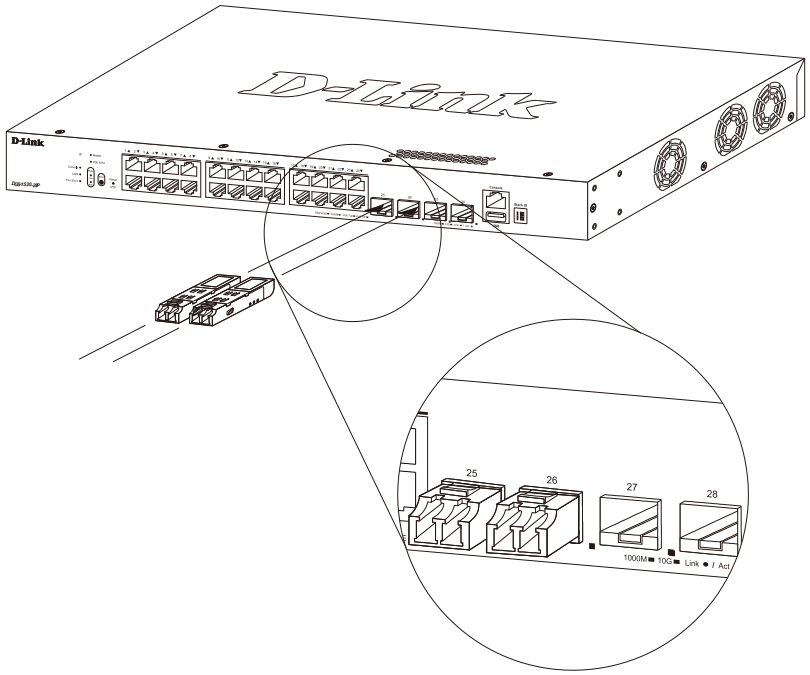


図 2-4　　SFP+ スロットへのトランシーバの挿入

参照 サポートしている光トランシーバの一覧は「オプションモジュール（光トランシーバ / ダイレクトアタッチケーブル）」を参照してください。

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。

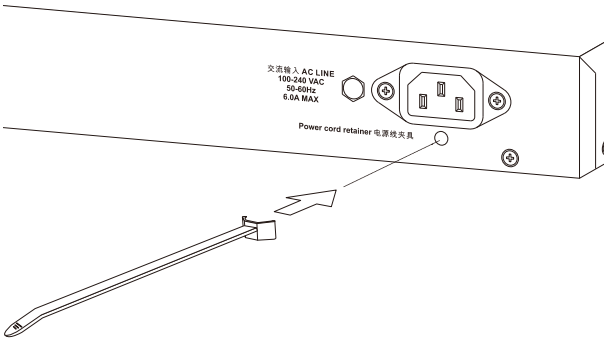


図 2-5　　タイラップの挿し込み

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。

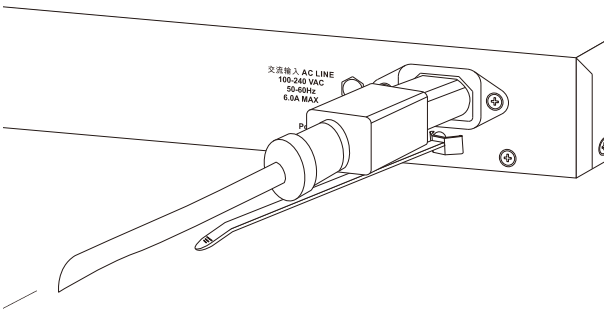


図 2-6　　電源コード挿し込み

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。

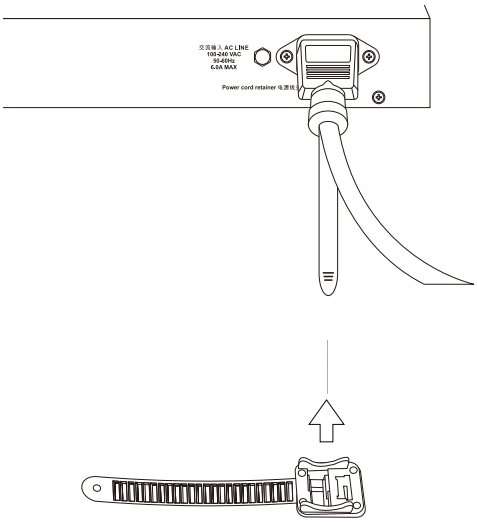


図 2-7　　リテイナー（固定具）のスライド

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。

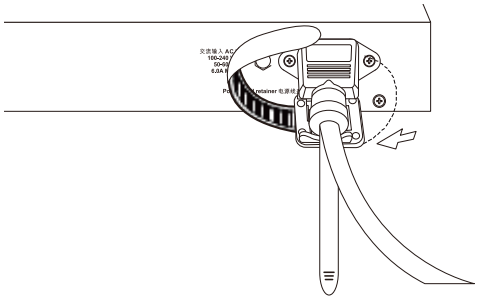


図 2-8　　リテイナーの巻き付け、固定

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

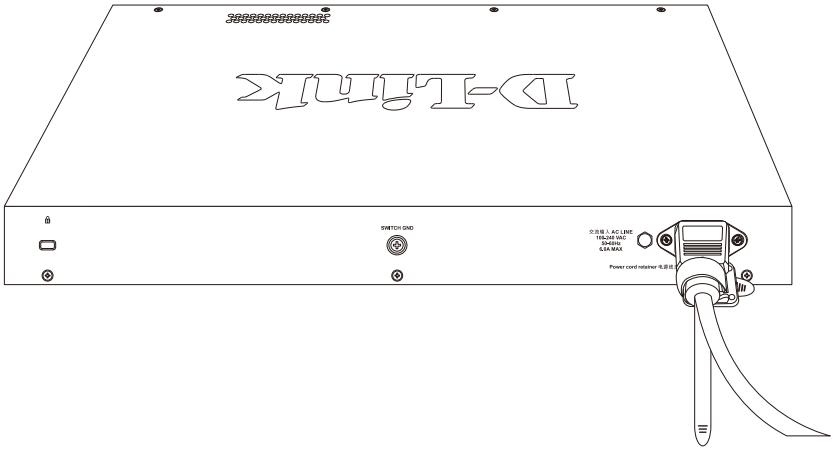


図 2-9　　電源抜け防止器具の固定確認

リダンダント電源システムの設置

本シリーズは、外付けのリダンダント電源システム（RPS）である DPS-500A、DPS-700 をサポートしています。

RPS は緊急時に必要な電力を供給するリダンダント電源ユニットであり、スイッチの電源不具合によるシャットダウンなどのリスクを回避し、安定した電源供給を提供します。DPS-700 は PoE スイッチに対応しているため、スイッチの PoE 給電可能電力を倍にすることができます。

補足 DPS-500A は DGS-1530-10/20/28/28S/28SC/52 で使用することができます。

補足 DPS-700 は DGS-1530-52P で使用することができます。

本スイッチへリダンダント電源ユニットを接続する手順は以下の通りです。

DPS-500A

DPS シリーズのスイッチへの接続は、専用の DC 電源ケーブル「DPS-CB150-2PS」を使用して行います。DPS-500A は 2 台までのスイッチに同時に電力を供給することが可能です。

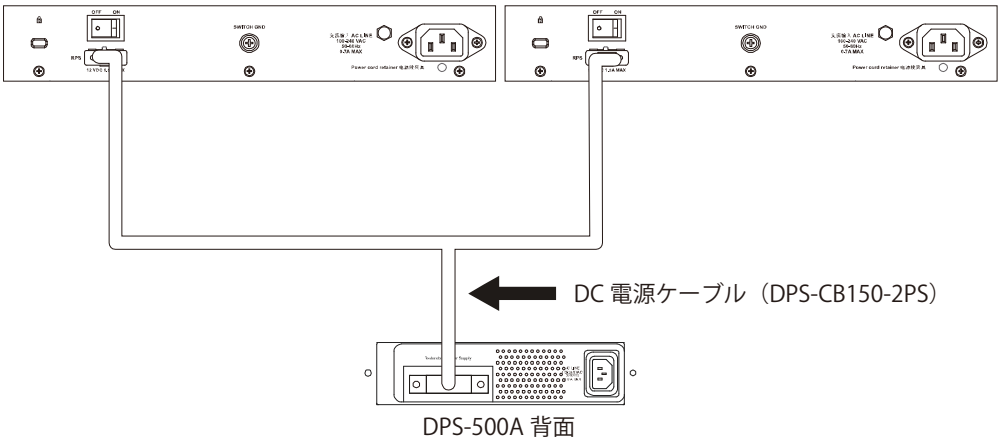


図 2-10　スイッチと DPS-500A の接続

警告 DC 電源ケーブルを接続する前に、DPS-500A を AC 電源に接続しないでください。内蔵電源が破損するおそれがあります。

警告 ケーブルの損傷を防ぐため、DPS-500A を取り付ける場合はスイッチの後ろに 15cm 以上のスペースを確保してください。

1. DPS-500A はホットスワップに対応していないため、スイッチの AC 電源コネクタから AC 電源ケーブルを取り外します。
2. 14 ピン DC 電源ケーブル（DPS-CB150-2PS）の一端をスイッチ背面のソケットに挿入し、もう一端をリダンダント電源装置に挿入します。
3. 標準の AC 電源ケーブルでリダンダント電源装置と電源コンセントを接続します。
4. スイッチ背面にある「RPS 用 ON/OFF スイッチ」を「ON」にします。
   リダンダント電源装置の前面にある緑の LED 点灯により、正しく接続が行われたことが確認できます。
5. スイッチを再び AC 電源に接続します。
   スイッチの RPS LED が点灯し、リダンダント電源が動作していることを確認できます。ソフトウェアの設定変更は必要ありません。

補足 DPS-500A は DPS-800 に取り付けることができます。

補足 DGS-1530 と DPS-500A の接続には「DPS-CB150-2PS」のハードウェアバージョン B1 が必要です。

補足 DPS-500A は DGS-1530-10/20/28/28S/28SC/52 でサポートされます。

DPS-700

DPS-700 は 22 ピンの DC 電源ケーブルを使用したスイッチに接続します。

注意 DC 電源ケーブルを接続する前に、DPS-700 を AC 電源に接続しないでください。内蔵電源が破損するおそれがあります。

警告 ケーブルの損傷を防ぐため、DPS-700 を取り付ける場合はスイッチの後ろに 15cm 以上のスペースを確保してください。

1. DPS-700 はホットスワップに対応していないため、スイッチの AC 電源コネクタから AC 電源ケーブルを取り外します。
2. プラスドライバーを使用し、RPS ポートのカバーを固定しているネジ 2 つを取り外します。

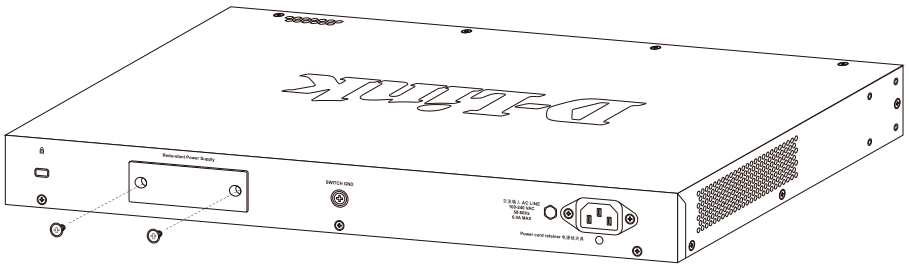
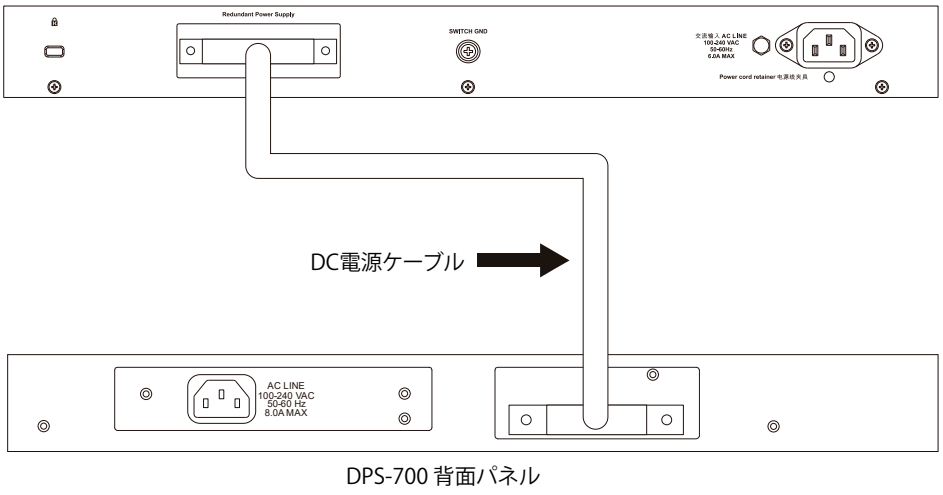


図 2-11　RPS ポートカバーの取り外し

3. 22 ピンの DC 電源ケーブルの一端をスイッチ背面の RPS ポートに挿入し、もう一端をリダンダント電源装置に挿入します。



DPS-700 背面パネル

図 2-12　スイッチと DPS-700 の接続

4. DPS-700 を AC 電源に接続します。接続に成功すると、DPS-700 の前面パネルにある緑色の LED が点灯します。
5. スイッチを再び AC 電源に接続します。
   スイッチの RPS LED が点灯し、リダンダント電源が動作していることを確認できます。ソフトウェアの設定変更は必要ありません。

補足 DPS-700 は DGS-1530-52P でサポートされます。

DGS-1530-52P に DPS-700 を接続しない場合は、RPS ポートのカバーを取り付けたままにしてください。

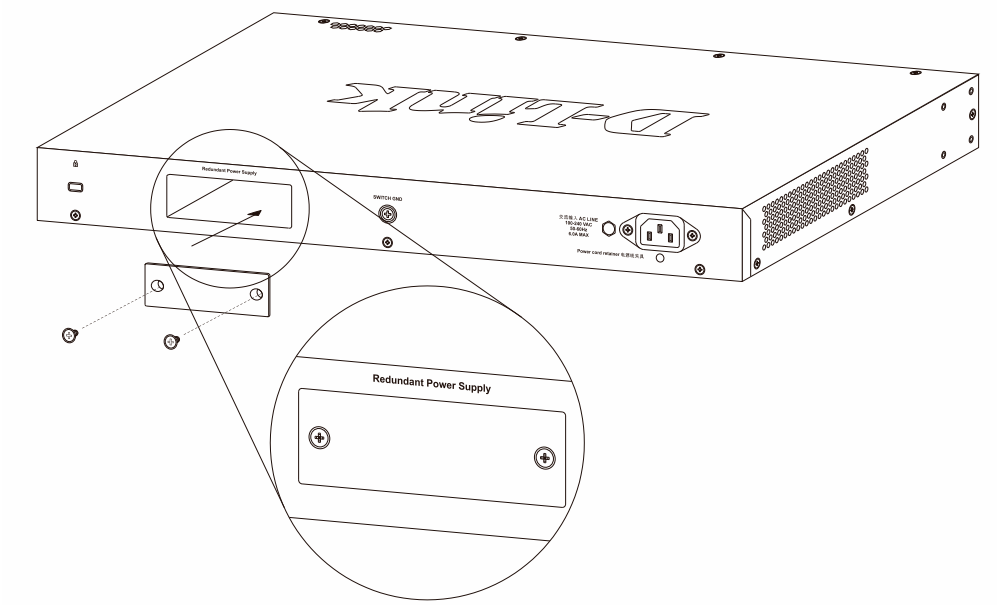


図 2-13　RPS ポートカバーの装着

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。システムのリセット中、LED は点滅します。

電源の異常

計画停電前や電源設備に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。

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

エンドノードと接続する

UTP/STP ケーブルを使用して本スイッチとエンドノードを接続します。エンドノードとは、RJ45 ネットワークポートを装備した PC やルータの総称です。接続が正常に確立されると、対応するポートの LED が点灯・点滅し、そのポートでデータの送受信が行われていることを示します。

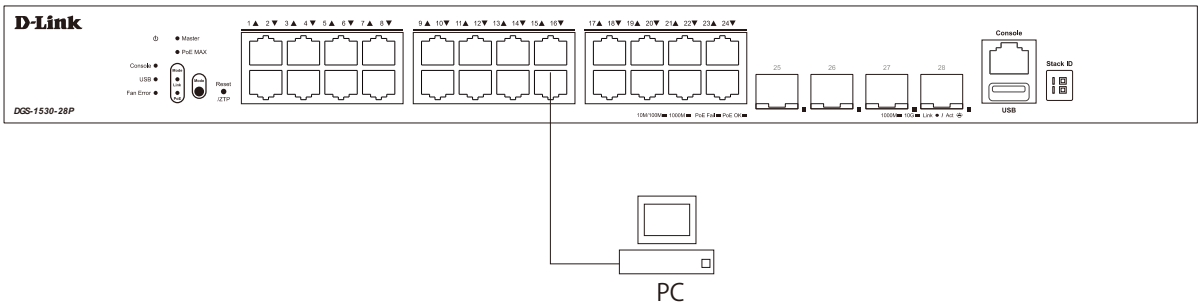


図 3-1　エンドノードと接続した図

ハブまたはスイッチと接続する

本スイッチは、ネットワーク内の他のスイッチやハブに接続することができます。
このネットワークトポロジは、ネットワーク内のすべてのエンドノードに対応するのに十分なポートがスイッチにない場合に使用されます。

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 ハブスイッチポートと接続します。
- カテゴリ 5 以上の UTP/STP ケーブル：100BASE-TX スイッチポートと接続します。
- エンハンスドカテゴリ 5 以上の UTP ケーブル：1000BASE-T スイッチポートと接続します。
- 光ファイバケーブル：SFP/SFP+ スロッ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します。

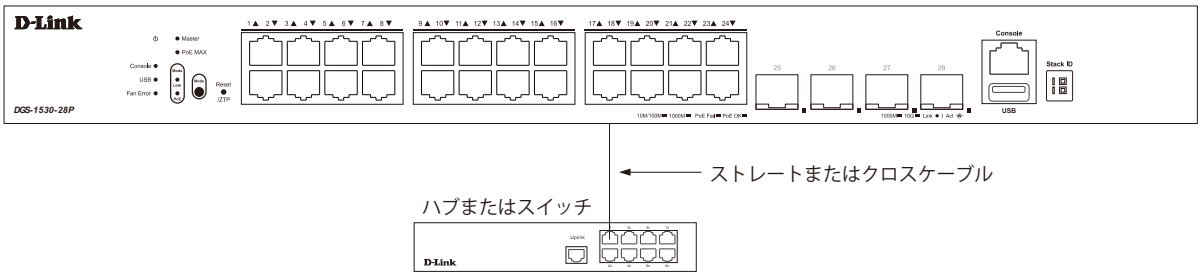


図 3-2　ハブまたはスイッチと接続した図

バックボーンまたはサーバと接続する

本スイッチは、ネットワークバックボーン、サーバ、サーバファームへ接続できます。

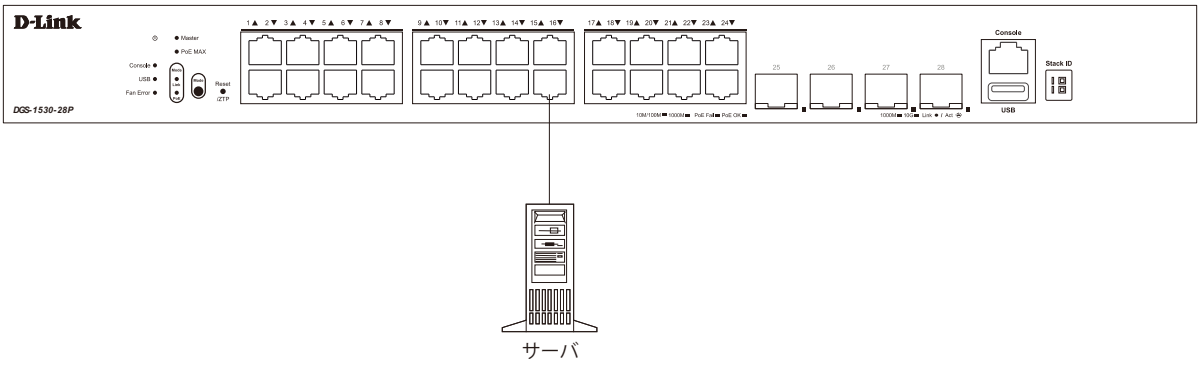


図 3-3　サーバと接続した図

第 4 章　スイッチ管理について

- Web GUI による管理
- SNMP による管理
- CLI による管理

Web GUI による管理

標準的な Web ブラウザを使用して、本製品の設定をグラフィカルに表示し、管理することができます。

Web GUI の詳細については「第 5 章　Web ベースのスイッチ管理」を参照してください。

SNMP による管理

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルです。ネットワークに接続された通信機器の管理や監視を行います。

SNMP の詳細については「SNMP（SNMP 設定）」を参照してください。

CLI による管理

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

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

端末をコンソールポートに接続する

ケーブルの接続

1. RJ-45/RS-232C 変換ケーブルの RS-232C コネクタを、シリアルポート搭載の端末またはコンピュータに接続します。
2. RJ-45/RS-232C 変換ケーブルの RJ-45 コネクタを、本製品のコンソールポートに接続します。

ターミナルソフトの設定

1. VT100 のエミュレーションが可能なターミナルソフトを起動します。
2. 適切なシリアルポート（COM 1 など）を選択します。
3. ターミナルソフトの設定をスイッチのシリアルポートの設定に合わせます。
   スイッチのシリアルポートの設定は以下の通りです。
   - スピード：「115200」
   - データ：「8bit」
   - パリティ：「なし（none）」
   - ストップビット：「1bit」
   - フロー制御：「なし（none）」

ログインとログアウト

1. 本製品と管理 PC をケーブルで接続後、本製品の電源をいれます。
2. 管理 PC とスイッチが正しく接続されると、画面に「Press any key to login...」というメッセージが表示されます。
   キーボード上のいずれかのキーを押します。
3. 設定済みのユーザ名とパスワードがある場合は、設定したユーザ名とパスワードを入力し「Enter」を押します。
   初期値のアカウントおよびパスワードは「admin」です。

注意 パスワードの大文字と小文字は区別されます。

4. コマンドを入力し、必要な設定を行います。

   コマンドの多くは管理者レベルのアクセス権が必要です。
   管理者レベルのアカウント作成については「User Accounts Settings（ユーザアカウント設定）」を参照してください。
   CLI の詳細及びコマンドリストについては、CLI マニュアルを参照してください。
5. ログアウトする場合は、logout コマンド使用するか、ターミナルソフトを終了します。

初回ログイン後のパスワードの設定

CLI に最初に接続した後、ログインパスワードの変更が求められます。
プロンプトメッセージに従い、パスワードを変更します。

注意 初期値のアカウントおよびパスワードは「admin」です。変更後のパスワードは忘れないように記録しておいてください。

```
                DGS-1530-28P Gigabit Ethernet Smart Managed Switch

                              Command Line Interface
                             Firmware: Build 1.00.0xx
           Copyright(C) 2025 D-Link Corporation. All rights reserved.

User Access Verification

Username:admin
Password:*****


Please modify the password of default user 'admin' for security.
Enter Old Password:*****
Enter New Password:*********
Confirm New Password:*********
Password has been changed successfully!
Login again using new password.

Username:admin
Password:*********

Switch#
```

補足 パスワードの入力ルールは以下の通りです。

- 8 - 30 文字以内の UTF-8 文字（Unicode Hex 範囲 0x0021 - 0x007e）
- アルファベットの大文字小文字、数字、記号をそれぞれ 1 つ以上含める必要があります。
- 非連続文字でなければなりません。
- ユーザ名と同じにすることはできません。
- デフォルトのログインアカウントとデフォルトの IP アドレスを含めることはできません。

注意 CLI の設定コマンドは実行中の設定ファイルの編集でありスイッチが再起動した場合、設定は保存されません。

設定内容変更を保存するには、「copy running-config startup-config」コマンドを使用して実行中の設定ファイルをスタート時の設定ファイルとしてコピーする必要があります。

IP アドレスの割り当て

CLI を使用してスイッチの IP アドレスを設定する方法について説明します。

- IP アドレスの初期値：10.90.90.90/8

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
Switch(config-if)#
```

1. 「configure terminal」コマンドを入力し、Global Configuration モードになります。
2. 「interface vlan 1」コマンドを入力し、デフォルト VLAN の VLAN Configuration モードに入り「VLAN 1」を指定します。
3. 「ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy」を入力し、IP アドレスを変更します。
   xxx.xxx.xxx.xxx　：　IP アドレス
   yyy.yyy.yyy.yyy　：　IP アドレスに対応するサブネットマスク
4. 「end」コマンドを入力し、Privilege EXEC モードに戻ります。

注意 CLI の設定コマンドは実行中の設定ファイルの編集でありスイッチが再起動した場合、設定は保存されません。

設定内容変更を保存するには、「copy running-config startup-config」コマンドを使用して実行中の設定ファイルをスタート時の設定ファイルとしてコピーする必要があります。

第 5 章　Web ベースのスイッチ管理

- Web ベースの管理について
- Web マネージャへのログイン
- スマートウィザード設定
- Web マネージャの画面構成
- Web マネージャのメニュー構成

Web ベースの管理について

本スイッチのすべてのソフトウェア機能は、実装されている Web ベース (HTML) インタフェース経由で管理、設定およびモニタできます。標準的な Web ブラウザを使用して、HTTP または HTTPS（SSL）プロトコル経由で Web ベースの管理画面にアクセスします。

Web マネージャへのログイン

初期値では、Secure HTTP（https）で接続が可能です。
スイッチの管理を行うには、はじめにコンピュータで Web ブラウザを起動し、本スイッチに定義されている IP アドレスを入力します。

1. Web ブラウザを開きます。
2. アドレスバーに本スイッチの IP アドレスを入力し、「Enter」キーを押下します（例 : https://10.90.90.90）

図 5-1　URL の入力

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

3. 以下のユーザ認証画面が表示されます。

図 5-2　ログイン画面

4. ユーザ名とパスワードを入力してログインします。
   工場出荷時設定ではユーザ名「admin」、パスワード「admin」が設定されています。

注意 セキュリティのため、ユーザ名とパスワードを設定することを強くお勧めします。

5. スマートウィザード画面が表示されます。

   ウィザード画面では、Web モードの選択や IP アドレス・パスワード・SNMP の設定を行うことができます。
   ウィザードを使用して設定する場合は、「スマートウィザード設定」を参照してください。

スマートウィザード設定

スマートウィザードで Web モードの選択や、基本的なシステム設定（IP アドレス、パスワード、SNMP）を行います。

補足 Web マネージャメイン画面の「Wizard」から、スマートウィザード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、次回のログイン時にスマートウィザード 画面が表示されません。

1. IP アドレスの設定を行い、「Next」をクリックします。

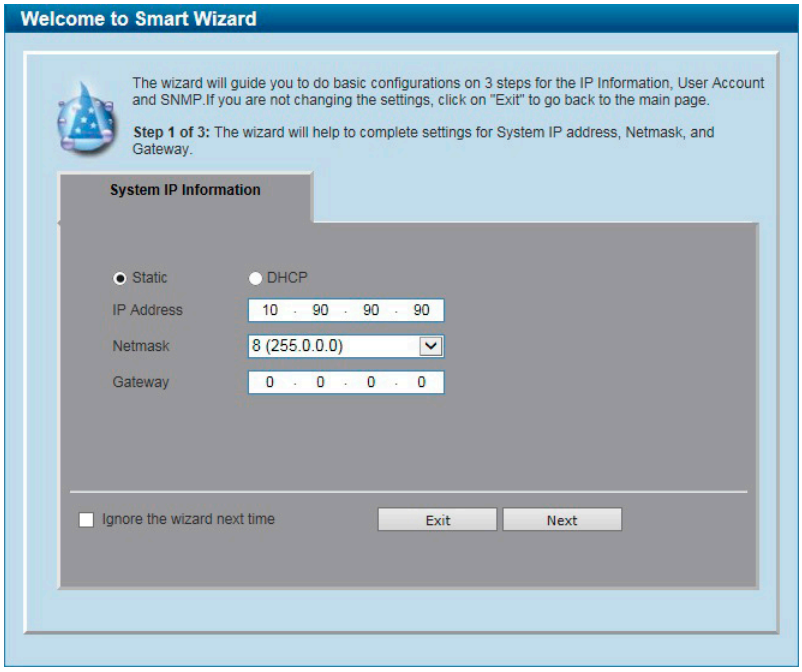


図 5-3　System IP Information 画面

- 「Static」：固定 IP アドレスを手動で設定します。
- 「DHCP」：DHCP から IPv4 アドレスを自動的に取得します。

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

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

2. ユーザアカウントの設定を行い、「Next」をクリックします。

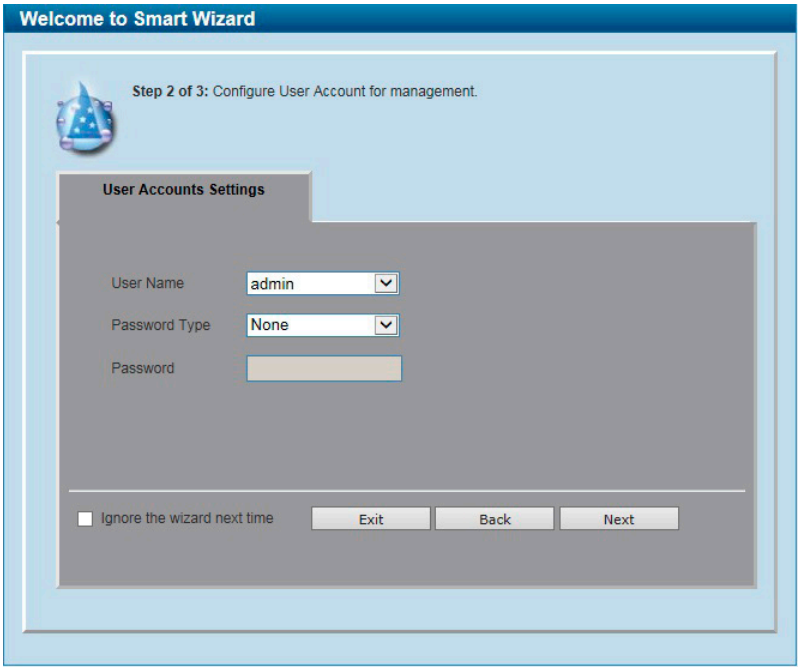


図 5-4　User Account Settings 画面

画面に表示される項目：

項目	説明
User Name	設定を行うユーザアカウントを選択します。
Password Type	パスワードの種類を指定します。 • 「None」- ユーザアカウントにパスワードを指定しません。 • 「Plain Text 」- プレーンテキストでパスワードを指定します。 • 「Encrypted-SHA1」-「SHA-1」を使用してパスワードを暗号化します。 • 「Encrypted-MD5」-「MD5」を使用してパスワードを暗号化します。
Password	パスワードの種類で「None」以外を選択した場合、ユーザアカウントのパスワードを入力します。

3. SNMP の有効 / 無効を設定し、「Apply & Save」をクリックします。

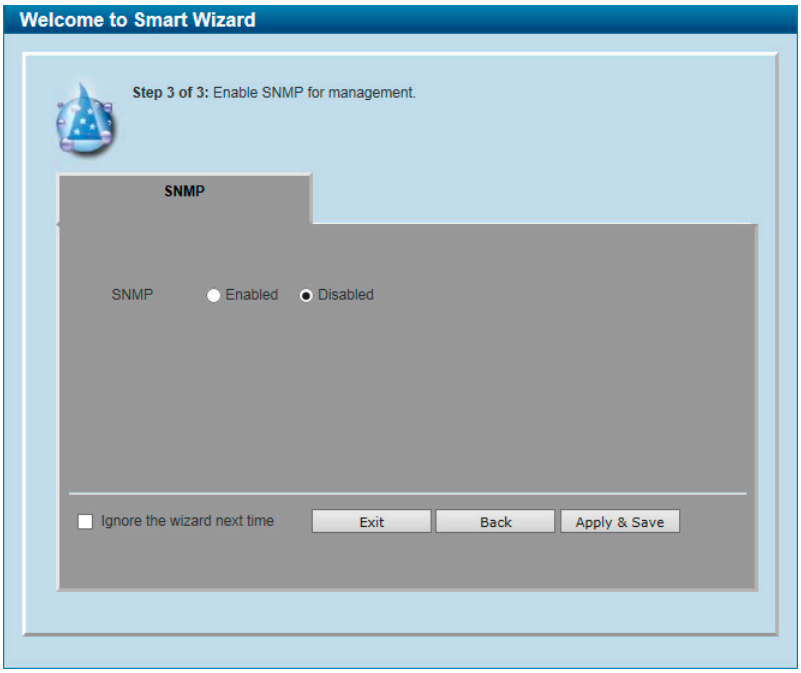


図 5-5　SNMP 画面

Web マネージャの画面構成

Web マネージャでスイッチの設定または管理画面にアクセスしたり、パフォーマンス状況やシステム状況を参照できます。
ログインに成功すると、デバイスの状態が表示されます。

Web マネージャのメイン画面について

Web マネージャのメイン画面は 3 つのエリアで構成されています。

図 5-6　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状態がほぼリアルタイムに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。 ツールバーの右側には、現在接続中のユーザ名とスイッチの IP アドレス、ログアウトボタンが表示されます。
エリア③	WebUI を使用して設定可能な機能のツリービューが表示されます。ツリー項目をクリックして各機能の設定画面に移動します。 製品名をクリックすると、デバイス情報画面が表示されます。 また、メニュー項目をキーワードで検索するための検索フィールドも用意されています。
エリア④	ツリービューで選択した各機能の設定画面が表示されます。

補足　Web UI を表示する最適の解像度は「1280 x 1024」ピクセルです。

注意　スイッチ設定を変更した場合、Web ブラウザの「Save Configuration」メニューまたはコマンドラインインタフェース（CLI）の「copy」コマンドにて保存する必要があります。

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一覧は以下の通りです。

メインメニュー	サブメニュー	説明
System	Device Information（デバイス情報）	スイッチの主な設定情報を表示します。
	System Information Settings（システム情報設定 ）	スイッチの基本情報を表示します。
	Peripheral Settings（環境設定）	システムの警告温度や環境トラップの設定を行います。
	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。
	Interface Description（インタフェース概要）	スイッチの各ポートの概要、管理ステータスなどについて表示します。
	Loopback Test（ループバックテスト）	物理ポートインタフェースのループバック設定とループバックテストを行います。
	PoE（PoE 設定）	PoE 設定を行います。
	System Log（ システムログ構成）	スイッチのフラッシュメモリにスイッチログを保存する方法を設定します。
	Time and SNTP（時刻設定）	スイッチに時刻を設定します。
	Time Range（タイムレンジ設定）	スイッチで使用されるタイムレンジを設定します。ACL などに使用されます。
	PTP (Precision Time Protocol)（PTP 設定）	PTP（Precision Time Protocol : 高精度時刻同期方式）システムは、イーサネットネットワークを通して時刻を同期します。
	Reset Button Settings（リセットボタン設定）	リセット /ZTP ボタンの設定を行います。
	Archive Settings（アーカイブ設定）	コンフィグレーションのアーカイブ設定を行います。
Management	Command Logging（コマンドログ設定）	コマンドログ設定を有効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
	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。
	Password Encryption（パスワード暗号化）	パスワードを暗号化し設定ファイルに保存します。
	Password Recovery（パスワードリカバリ）	パスワードリカバリを行います。例えば管理者がパスワードを忘れた場合に有効です。
	Login Method（ログイン方法）	各管理インタフェースでのログイン方法について設定します。
	Web Login Lock Settings（Web ログインロック設定）	Web ログイン失敗時のロック設定を行います。
	SNMP（SNMP 設定）	SNMP 設定を有効にします。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。
	RMON（RMON 設定）	SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効にします。
	Telnet/Web（Telnet/Web 設定）	スイッチの Telnet/Web 設定を有効にします。
	Session Timeout（セッションタイムアウト）	各セッション（Web やコンソールなど）のタイムアウトの設定をします。
	DHCP（DHCP 設定）	スイッチの DHCP について設定します。
	DHCP Auto Configuration（DHCP 自動コンフィグ設定）	DHCP 自動コンフィグ機能の設定を行います。
	DHCP Auto Image Settings（DHCP 自動イメージ設定）	DHCP 自動イメージ設定を行います。スタートアップ時に、外部サーバからイメージファイルを取得する機能です。
	DNS（ドメインネームシステム）	DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。
	NTP（NTP 設定）	スイッチの時刻を同期するための NTP プロトコルの設定を行います。
	File System（ファイルシステム設定）	フラッシュファイルシステムにより、ファームウェア、コンフィグレーション情報、および Syslog 情報はフラッシュ内のファイルに保存されます。
	Stacking（スタッキング設定）	物理スタッキングの設定を行います。
	Virtual Stacking（SIM）設定	仮想（SIM）スタッキングの設定を行います。
	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。
	SMTP Settings（SMTP 設定）	Simple Mail Transfer Protocol (SMTP) の設定を行います。
	Reboot Schedule Settings（再起動スケジュール設定）	スイッチの再起動スケジュール設定を行います。
	NLB FDB Settings（NLB FDB 設定）	ネットワークロードバランシング (NLB) の設定を行います。
	PPPoE Circuit ID Insertion Settings（PPPoE 回線 ID 挿入設定）	PPPoE 回線 ID 挿入機能の設定を行います。
	TCP Path MTU Discovery（TCP パス MTU 検出）	IP TCP パス MTU 変換の設定を行います。

メインメニュー	サブメニュー	説明
	TCP Selective ACK（TCP 選択的確認応答）	TCP 選択的確認応答の設定を行います。
	TWAMP（TWAMP 設定）	Two-Way Active Measurement Protocol（TWAMP）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 スタティック VLAN の設定を行います。
	VLAN Tunnel（VLAN トンネル）	802.1Q VLAN トンネルの設定を行います。
	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) の表示、設定を行います。 ERPS 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。
	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機能）の設定を行います。
	Flex Links（フレックスリンク）	フレックスリンク機能の設定を行います。
	L2 Protocol Tunnel （レイヤ 2 プロトコルトンネル）	L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）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（Internet Group Management Protocol）Snooping 機能を始めとした L2 Multicast Control（L2 マルチキャストコントロール）の設定を行います。
	LLDP	Link Layer Discovery Protocol（LLDP）の設定を行います。
L3 Features	ARP（ARP 設定）	ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
	Gratuitous ARP（Gratuitous ARP 設定）	Gratuitous ARP の設定を行います。
	IPv6 Neighbor（IPv6 ネイバ設定）	IPv6 ネイバ設定を行います。
	Interface（インタフェース設定）	IP インタフェース設定を行います。
	UDP Helper（UDP ヘルパー）	IP 転送プロトコルの設定を行います。本機能は指定の UDP サービスタイプのパケットの転送を有効にします。また UDP ブロードキャストパケットを転送するターゲットアドレスを指定します。
	IPv4 Static/Default Route （IPv4 スタティック / デフォルトルート設定）	IPv4 スタティックルーティング機能を設定します。
	IPv4 Route Table（IPv4 ルートテーブル）	IPv4 ルートテーブルを表示します。
	IPv6 Static/Default Route （IPv6 スタティック / デフォルトルート設定）	IPv6 スタティックルーティング機能を設定します。
	IPv6 Route Table（IPv6 ルートテーブル）	IPv6 ルートテーブルを表示します。
	IPv6 General Prefix （IPv6 汎用プレフィックス）	VLAN インタフェース IPv6 汎用プレフィックスの設定を行います。
	IP Multicast Routing Protocol （IP マルチキャストルーティングプロトコル）	IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）の設定を行います。
QoS	Basic Settings（基本設定）	QoS の Basic Settings（基本設定）を行います。
	Advanced Settings（アドバンス設定）	QoS の Advanced Settings（アドバンス設定）を行います。
ACL	ACL Configuration Wizard （ACL 設定ウィザード）	ACL 設定ウィザードを使用して、アクセスプロファイルと ACL ルールの新規作成・更新を行います。
	ACL Access List（ACL アクセスリスト）	ACL アクセスリストの設定を行います。
	ACL Interface Access Group （ACL インタフェースアクセスグループ）	ACL インタフェースアクセスグループの設定を行います。
	ACL VLAN Access Map （ACL VLAN アクセスマップ）	ACL VLAN アクセスマップの設定を行います。
	ACL VLAN Filter（ACL VLAN フィルタ設定）	ACL VLAN フィルタの設定を行います。
	CPU ACL（CPU ACL 設定）	CPU インタフェースフィルタリング機能の設定を行います。
Security	Port Security（ポートセキュリティ）	ポートセキュリティ機能では、ソース MAC アドレスが未認証であるコンピュータについて、指定ポートからネットワークへアクセスすることを防ぐことができます。
	802.1X（802.1X 設定）	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。
	AAA（AAA 設定）	AAA（Authentication、Authorization、Accounting）の設定を行います。
	RADIUS（RADIUS 設定）	RADIUS の設定を行います。
	TACACS+（TACACS+ 設定）	TACACS+ の設定を行います。

メインメニュー	サブメニュー	説明
	IMPB（IP-MAC-Port Binding/IP-MAC- ポートバインディング）	IP-MAC バインディングにより、スイッチにアクセスするユーザを制限します。
	DHCP Server Screening（DHCP サーバスクリーニング設定）	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
	ARP Spoofing Prevention（ARP スプーフィング防止設定）	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスと一致しなかった IP アドレスの ARP パケットをバイパスします。
	BPDU Attack Protection（BPDU アタック防止設定）	スイッチのポートに BPDU アタック防止機能を設定します。
	NetBIOS Filtering（NetBIOS フィルタリング設定）	NetBIOS フィルタリングの設定を行います。
	MAC Authentication（MAC 認証）	MAC 認証機能は、MAC アドレスを使用してネットワークの認証を行う機能です。
	Web-based Access Control（Web 認証）	Web ベース認証はスイッチ経由で HTTP/HTTPS を使用してインターネットにアクセスする場合、ユーザを認証する機能です。
	Network Access Authentication（ネットワークアクセス認証）	Network Access Authentication（ネットワークアクセス認証）の設定を行います。
	Safeguard Engine（セーフガードエンジン）	セーフガードエンジンは、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）	トラフィックセグメンテーション機能はポート間のトラフィックの流れの制限を行います。
	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。
	SSH（Secure Shell）	SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。
	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。
	Network Protocol Port Protection Settings（ネットワークプロトコルポート保護設定）	ネットワークプロトコルポート保護設定を行います。
OAM	CFM（Connectivity Fault Management : 接続性障害管理）	CFM 機能を設定します。
	Cable Diagnostics（ケーブル診断機能）	スイッチのポートに接続するケーブルの診断を行います。
	Ethernet OAM（イーサネット OAM）	ポートにイーサネット OAM モード、イベント、ログを設定します。
	DDM（DDM 設定）	Digital Diagnostic Monitoring（DDM）機能を実行します。スイッチに挿入した SFP/SFP+ モジュールの DDM 状態の参照、各種設定（アラーム / 警告設定、温度 / 電圧 / バイアス電流 /Tx（送信）電力 /Rx（受信）電力しきい値設定）を行うことができます。
Monitoring	VLAN Counter（VLAN カウンタ）	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを作成します。
	Utilization（利用分析）	スイッチの Utilization（利用分析）を表示します。
	Statistics（統計情報）	スイッチの Statistics（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。対象ポートで送受信するフレームをコピーし、フレームの出力先を他のポートに変更する機能（ポートミラーリング）です。
	sFlow（sFlow 設定）	sFlow は、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチ内蔵）と「sFlow レシーバ」によって構成されます。
	Device Environment（機器環境確認）	スイッチの内部温度、ファン、電源状態を表示します。
Green	Power Saving（省電力）	スイッチの省電力機能を設定、表示します。
	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。

メインメニュー	サブメニュー	説明
Toolbar	Save Configuration （コンフィグレーションの保存）	「Save Configuration」ではスイッチのコンフィグレーションを保存します。
	Tools（ツール）	ファームウェアアップグレードやバックアップ、コンフィグレーションのリストア、バックアップなどを行います。
	Wizard（ウィザード）	スマートウィザードを開始します。
	Online Help（オンラインヘルプ）	D-Link のサポート Web サイト（英語）/ またはユーザガイド（英語版）を表示します。インターネット接続が必要です。
	Language（言語）	Web GUI の表示言語を選択します。
	Logout（ログアウト）	Web GUI からログアウトします。

第 6 章　System（スイッチの主な設定）

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

サブメニュー	説明
Device Information（デバイス情報）	スイッチの主な設定情報を表示します。
System Information Settings（システム情報設定 ）	スイッチの基本情報を表示します。
Peripheral Settings（環境設定）	システムの警告温度や環境トラップの設定を行います。
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。
Interface Description（インタフェース概要）	スイッチの各ポートの概要、管理ステータスなどについて表示します。
Loopback Test（ループバックテスト）	物理ポートインタフェースのループバック設定とループバックテストを行います。
PoE（DGS-1530-28P/52P）	PoE の設定を行います。（DGS-1530-28P/52P）
System Log（システムログ構成）	スイッチのフラッシュメモリにスイッチログを保存する方法を設定します。
Time and SNTP（時刻設定）	スイッチに時刻を設定します。
Time Range（タイムレンジ設定）	スイッチのタイムレンジを設定します。ACL などに使用されます。
PTP（PTP 設定）	PTP（Precision Time Protocol : 高精度時刻同期方式）システムは、イーサネットネットワークを通して時刻を同期します。
Reset Button Settings（リセットボタンの設定）	リセット /ZTP ボタンの設定を行います。
Archive Settings（アーカイブ設定）	コンフィグレーションのアーカイブ設定を行います。

Device Information（デバイス情報）

本画面にはスイッチの基本情報が一覧で表示されます。スイッチへのログイン後に自動的に表示される画面です。別の画面から本画面に戻るためには、メニューツリーの一番上にある製品名のリンクをクリックします。

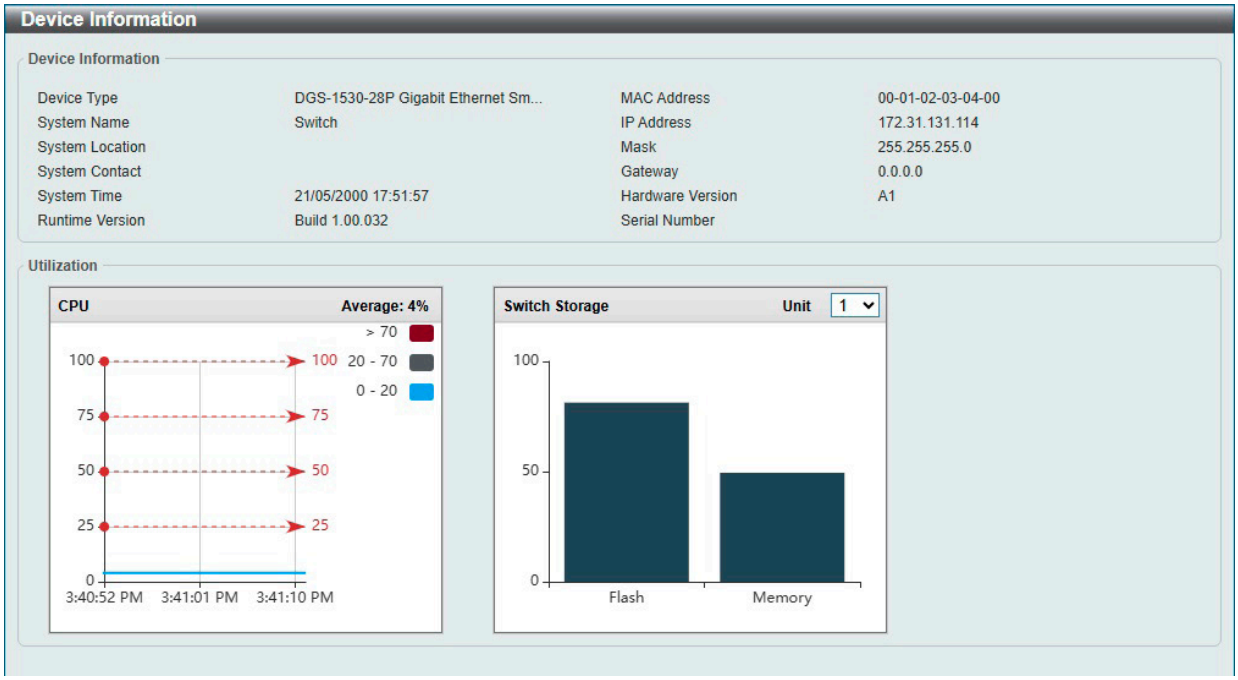


図 6-1　Device Information 画面

画面に表示される項目：

項目	説明
Device Information	
Device Type	機種名を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。
System Contact	担当者名を表示します。
System Time	システム時刻を表示します。
Runtime Version	デバイスのファーム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。
Hardware Version	デバイスのハードウェアバージョンを表示します。
Serial Number	デバイスのシリアル番号を表示します。
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。

System Information Settings（システム情報設定 ）

スイッチのシステム情報の設定を行います。

System > System Information 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 6-2　System Information Settings 画面

画面に表示される項目：

項目	説明
System Information Settings	
System Name	必要に応じて、スイッチのシステム名を変更します。ネットワーク内での識別名となります。
System Location	必要に応じて、システムが稼働している場所を定義します。
System Contact	必要に応じて、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て、設定内容を適用します。

Peripheral Settings（環境設定）

システムの警告温度や環境トラップの設定を行います。

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

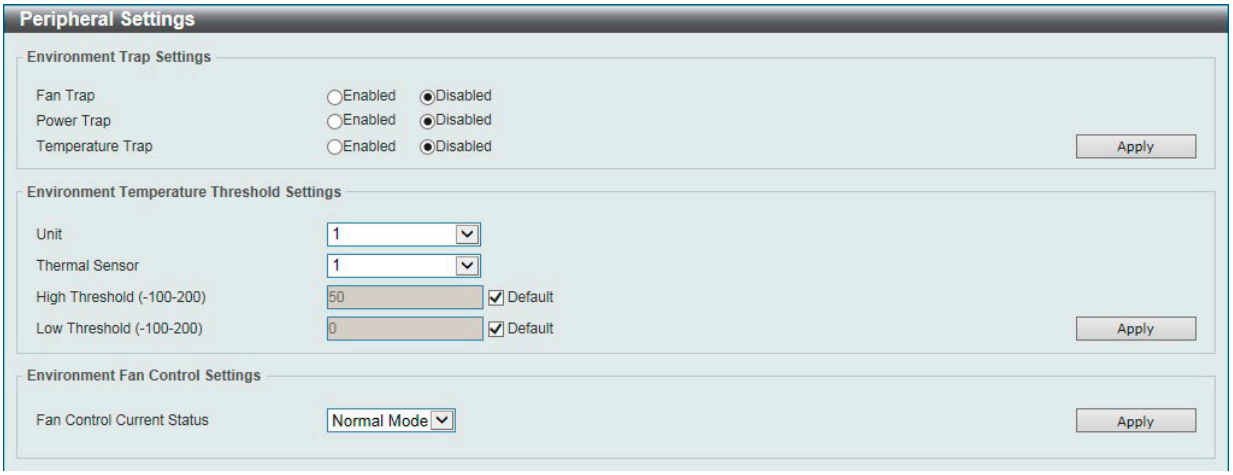


図 6-3　Peripheral Settings 画面

画面に表示される項目：

項目	説明
Environment Trap Settings	
Fan Trap	ファン警告イベント（ファンエラーまたは回復）のトラップを有効 / 無効に設定します。
Power Trap	電源警告イベント（電源エラーまたは回復）のトラップを有効 / 無効に設定します。
Temperature Trap	温度警告イベント（温度しきい値の超過または回復）のトラップを有効 / 無効に設定します。
Environment Temperature Threshold Settings	
Unit	本設定を適用するユニットを選択します。
Thermal Sensor	温度センサ ID を選択します。
High Threshold	高温警告しきい値を指定します。 • 設定可能範囲：「-100℃」-「200℃」 「Default」にチェックを入れると初期値に戻ります。
Low Threshold	低温警告しきい値を指定します。 • 設定可能範囲：「-100℃」-「200℃」 「Default」にチェックを入れると初期値に戻ります。

項目	説明
Environment Fan Current Status	
Fan Control Current State	ファンの制御モードを選択します。 • 選択肢：「Normal Mode（ノーマルモード）」「Quiet Mode（静音モード）」

「Apply」ボタンをクリックして、設定内容を適用します。

注意　ファンの制御モードはコンフィグレーションに保存されません。システムを再起動した場合、設定し直す必要があります。

Port Configuration（ポート設定）

各ポートの設定を行います。

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。

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

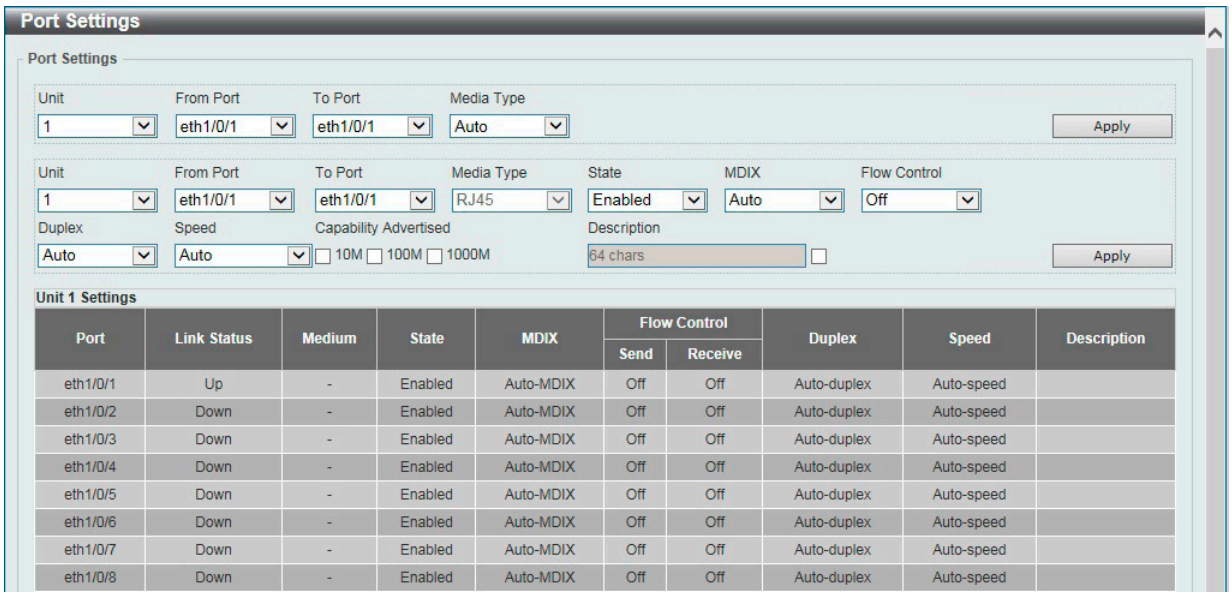


図 6-4　Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Media	コンボポートで使用するポートの種類を選択します。 • 選択肢：「Auto」「RJ45」「SFP」
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Media	ポートの種類を選択します。 • 選択肢：「RJ45」「SFP」
State	物理ポートのステータスを有効 / 無効に設定します。
MDIX	MDIX オプションを選択します。 • 「Auto」- 最適なケーブル接続を自動的に設定します。 • 「Normal」- 通常のケーブル接続の場合は、このオプションを選択します。このオプションを選択すると、ポートは MDIX モードになり、ストレートケーブルを使用して PC の NIC に接続するか、クロスケーブルを介して別のスイッチのポート（MDI モード）に接続できます。 • 「Cross」- ポートは MDI モードとなり、ストレートケーブルで別のスイッチのポート (MDIX モード) に接続することができます。
Flow Control	「On」（フロー制御あり）または「Off」（フロー制御なし）を選択します。物理スタックのスイッチはサポートしていません。
Duplex	Duplex モードの選択を行います。 • 選択肢：「Auto」「Half」「Full」

項目	説明
Speed	ポートの速度を選択します。速度を指定すると、指定のポートで接続速度が固定となります。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 • **「Auto」** - copper ポートの場合、オートネゴシエーションを開始してリンクパートナーと速度、フローコントロールの調整を行います。光ファイバポートの場合、オートネゴシエーションを開始してリンクパートナーとクロック、フローコントロールの調整を行います。 • **「10M」** - ポート速度を 10Mbps に固定します。 • **「100M」** - ポート速度を 100Mbps に固定します。 • **「1000M」** - ポート速度を 1Gbps に固定します。 • **「1000M Master」** - ポート速度を 1Gbps に固定し、送受信のタイミング制御におけるマスタとして指定します。 • **「1000M Slave」** - ポート速度を 1Gbps に固定し、送受信のタイミング制御におけるスレーブとして指定します。 • **「10G」** - ポート速度を 10Gbps に固定します。 補足　製品およびインタフェースによりサポートされる速度が異なります。 • マスタ設定 (1000M Master/10G Master) - 該当ポートは Duplex、速度、物理レイヤタイプについてアドバタイズを行います。また、接続された物理レイヤ間のマスタ・スレーブ関係を決定します。これらの関係は、2 つの物理レイヤ間のタイミング制御を確立するために必要です。タイミング制御は、ローカルソースによってマスタの物理層にセットされます。 • スレーブ設定 (1000M Slave/10G Slave) - ループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わせます。一方の接続にマスタを設定した場合、他方の接続はスレーブとする必要があります。それ以外の設定を行うと、両ポートのリンクダウンを引き起こします。
Capability Advertised	上記「Speed」が「Auto」に設定されている場合、指定した項目がオートネゴシエーションの間にアドバタイズされます。
Description	チェックボックスにチェックを入れ、ポートの説明を入力します。（64 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

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。

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。

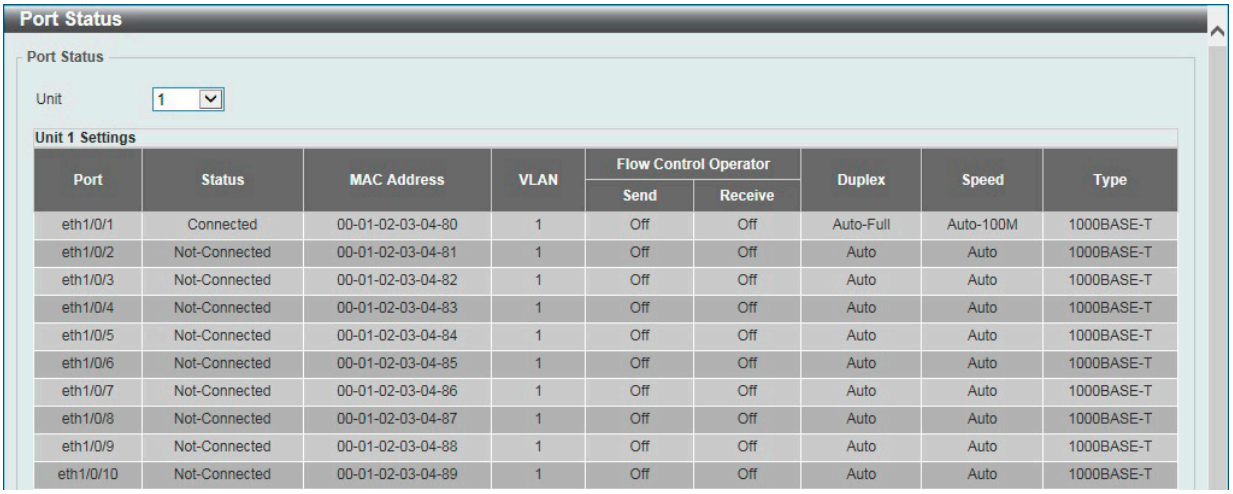


図 6-5　Port Status 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

Port GBIC

各物理ポートの GBIC 情報について表示します。

System > Port Configuration > Port GBIC 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 6-6　Port GBIC 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

Port Auto Negotiation（オートネゴシエーション）

オートネゴシエーションの詳細情報を表示します。

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

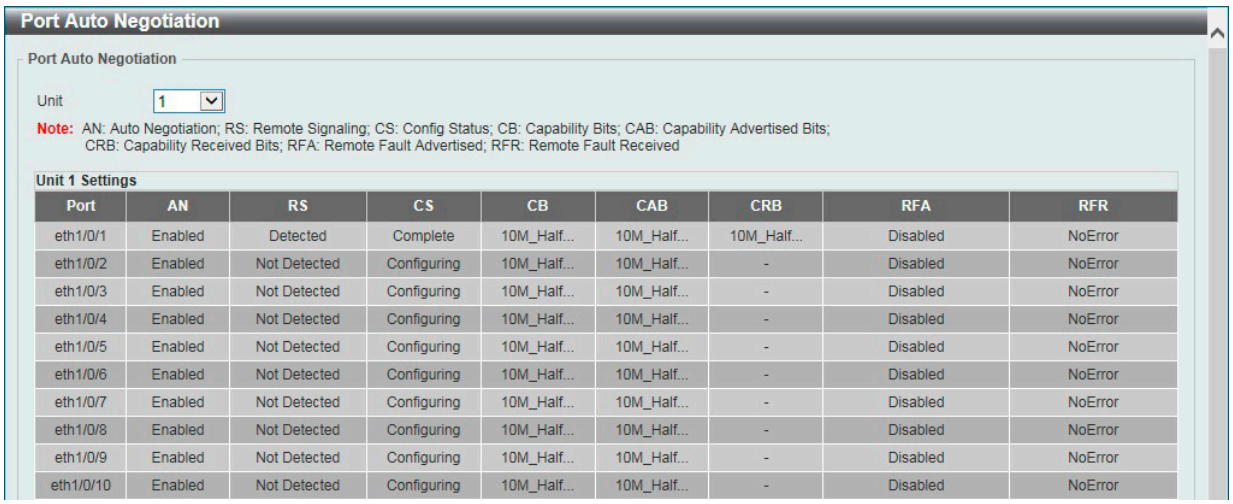


図 6-7　Port Auto Negotiation 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

Error Disable Settings（エラーによるポートの無効）

パケットストームの発生やループバックの検出などの理由により切断されたポート（エラー無効状態）に関する情報を表示、設定します。

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

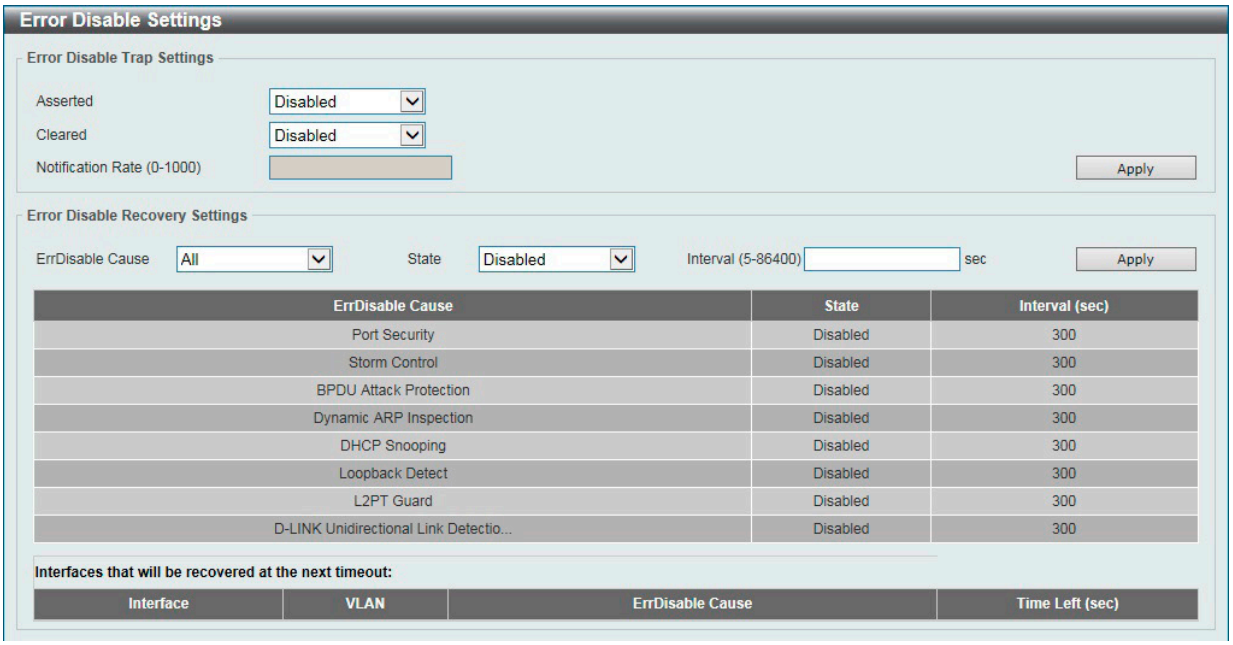


図 6-8　Error Disable Settings 画面

画面に表示される項目：

項目	説明
Error Disable Trap Settings	
Asserted	エラー無効状態になったときの通知送信の有効 / 無効を指定します。
Cleared	エラー無効状態から回復したときの通知送信の有効 / 無効を指定します。
Notification Rate	1 分あたりのトラップ数を入力します。指定したしきい値を超えたパケットは破棄されます。 • 設定可能範囲：0-1000 • 初期値：0 初期値の「0」は、無効状態が変更されるたびに SNMP トラップが生成されることを示します。
Error Disable Recovery Settings	
ErrDisable Cause	エラー無効の原因を選択します。 • 選択肢：「All」「Port Security」「Storm Control」「BPDU Attack Protection」「Dynamic ARP Inspection」「DHCP Snooping」「Loopback Detect」「L2PT Guard」「DULD」
State	指定した原因によるエラー無効ポートの自動リカバリ機能を有効 / 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） • 初期値：300（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

Jumbo Frame（ジャンボフレームの有効化）

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。ジャンボフレームは、1518 バイト以上のペイロードを持つイーサネットフレームです。本スイッチは最大 1 0232 バイトまでのジャンボフレームをサポートします。本機能を設定することにより、オーバヘッド、処理時間、割り込みを減らすことができます。

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

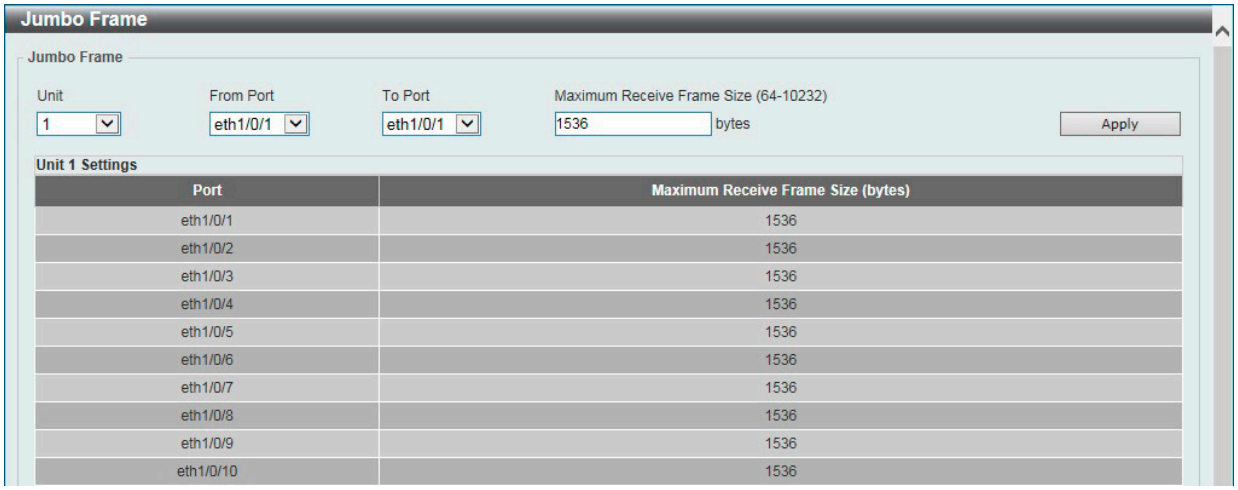


図 6-9　Jumbo Frame 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Maximum Receive Frame Size	受信フレームサイズの最大値を入力します。 • 設定可能範囲：64 - 10232（bytes） • 初期値：1536（bytes）

「Apply」ボタンをクリックして、設定内容を適用します。

Interface Description（インタフェース概要）

スイッチの各ポートのリンク状態、管理ステータス、概要を表示します。

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

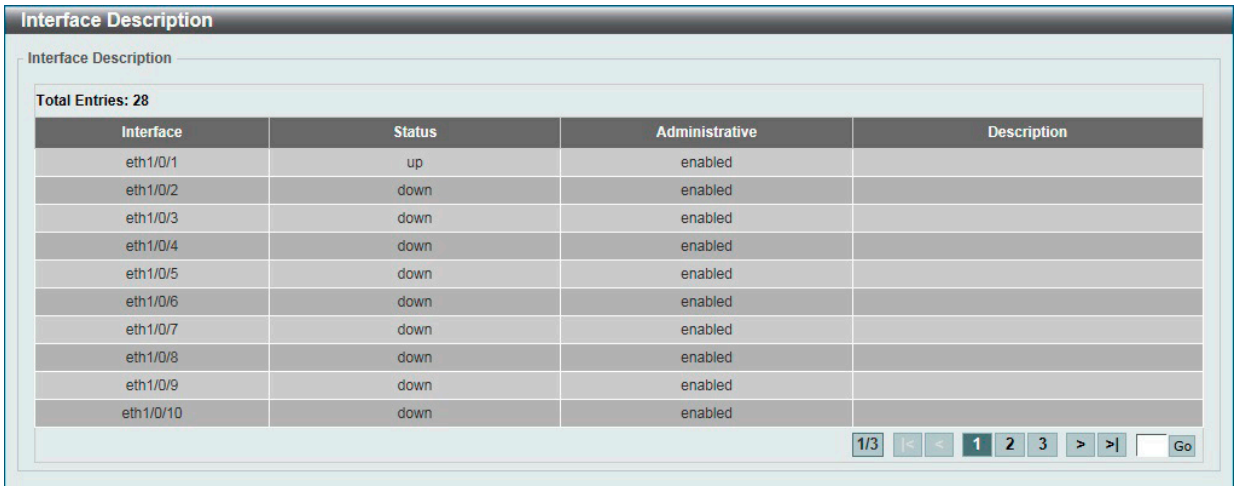


図 6-10　Interface Description 画面

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

Loopback Test（ループバックテスト）

物理ポートインタフェースのループバック設定とループバックテストを行います。

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

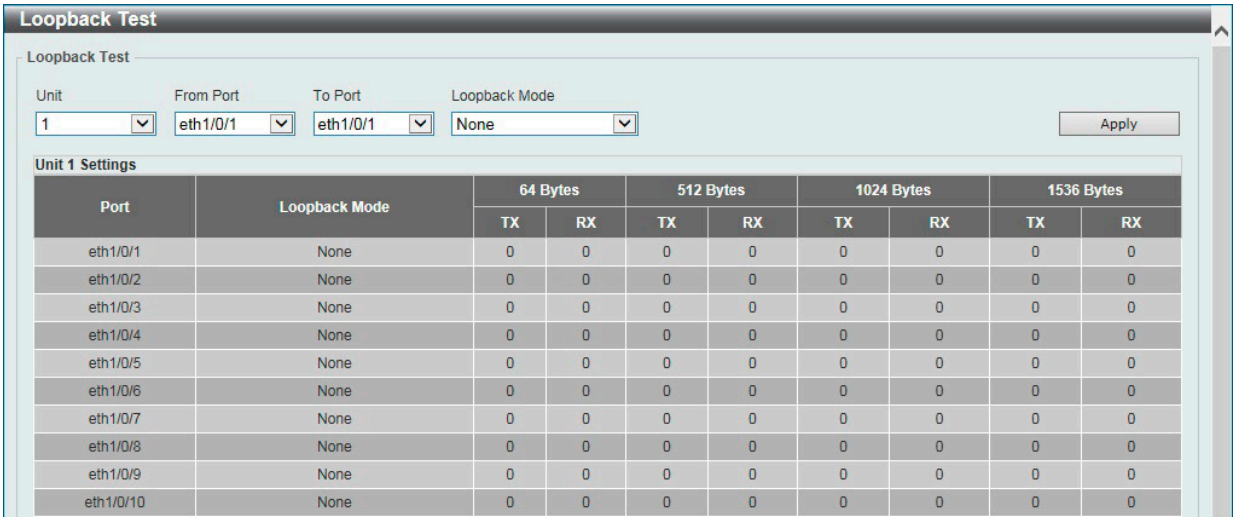


図 6-11　Loopback Test 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Loopback Mode	ループバックモードを指定します。 • 「None」- ループバックモードを有効にしません。 • 「Internal MAC」- MAC レイヤでの内部ループバックモードを指定します。 • 「Internal PHY Default」- PHY レイヤでの内部ループバックモードを指定します。デフォルトメディアに対してテストを実行します。 • 「Internal PHY Copper」- PHY レイヤでの内部ループバックモードを指定します。カッパーメディアに対してテストを実行します。 • 「Internal PHY Fiber」- PHY レイヤでの内部ループバックモードを指定します。ファイバメディアに対してテストを実行します。 • 「External MAC」- MAC レイヤでの外部ループバックモードを指定します。 • 「External PHY Default」- PHY レイヤでの外部ループバックモードを指定します。デフォルトメディアに対してテストを実行します。 • 「External PHY Copper」- PHY レイヤでの外部ループバックモードを指定します。カッパーメディアに対してテストを実行します。 • 「External PHY Fiber」- PHY レイヤでの外部ループバックモードを指定します。ファイバメディアに対してテストを実行します。

「Apply」ボタンをクリックして、設定内容を適用します。

PoE（DGS-1530-28P/52P）

DGS-1530-28P/52P は、IEEE802.3af 規格および IEEE802.3at 規格の PoE 機能をサポートしています。

本スイッチでは以下の PoE 機能を使用できます。
- Auto-discovery 機能で PD（受電機器）の接続を自動的に認識し、電力を供給します。
- ポートの電流が 600mA を超えた場合に、自動的にポートを無効にします。他のポートはアクティブなままとなります。
- Active circuit protection 機能は、電力の短絡が生じた場合に自動的にポートを無効にする機能です。他のポートはアクティブなままとなります。

802.3af/at 準拠の受電機器の最大受信電力一覧

クラス	用途	PSE の供給電力	受電機器の受電電力
0	デフォルト	15.4W	0.44 W - 12.95 W
1	オプション	4.0W	0.44 W - 3.84 W
2	オプション	7.0W	3.84 W - 6.49 W
3	オプション	15.4W	6.49 W - 12.95 W
4	オプション（802.3at のみ）	30W	12.95 W - 25.5 W

PoE System（PoE システム設定）

デバイスの PoE 情報を参照および変更します。

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

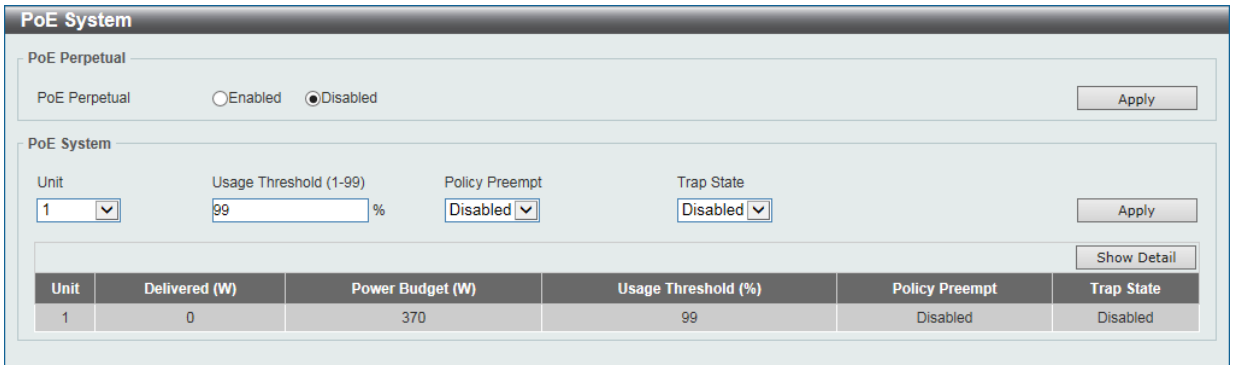


図 6-12　PoE System 画面

画面に表示される項目：

項目	説明
PoE Perpetual	Perpetual PoE 機能を有効または無効に設定します。本機能を有効にすると、スイッチの再起動時にも受電デバイスへの PoE 供給が中断されません。
Unit	本設定を適用するユニットを選択します。
Usage Threshold	使用電力のしきい値を指定します。設定したしきい値を超えた場合、ログや通知を生成します。 • 設定可能範囲：1 - 99（%）
Policy Preempt	ポリシープリエンプトを有効 / 無効にします。 ポリシープリエンプトは、電力が不足している状態で新しくデバイスを接続した場合に、優先度の低いデバイスを切断して、新規の優先度の高いデバイスに供給する電力を確保する機能です。
Trap State	PoE イベントの通知送信を有効 / 無効にします。

「Apply」をクリックして、設定内容を適用します。

補足　本スイッチは Fast PoE と Perpetual PoE をサポートしています。Fast PoE はデフォルトで有効、設定を変更することはできません。

- Fast PoE は、スイッチの OS 起動完了を待たずに起動途中から PD への給電を開始する機能です。
- Perpetual PoE は、スイッチが再起動している間も PD への給電を継続する機能です。

「Show Detail」をクリックすると、画面下部に追加の情報が表示されます。

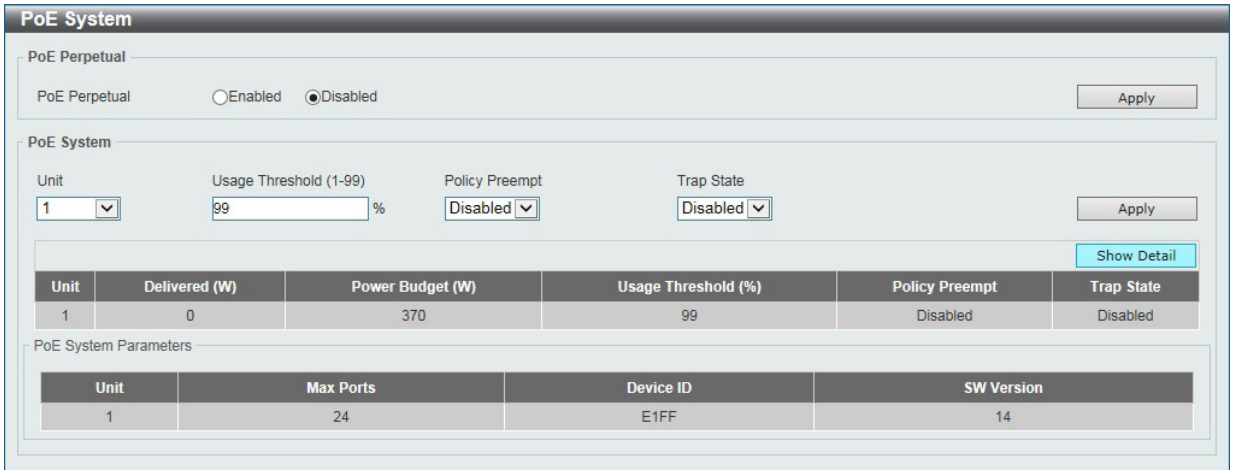


図 6-13　PoE System（Show Detail）画面

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。

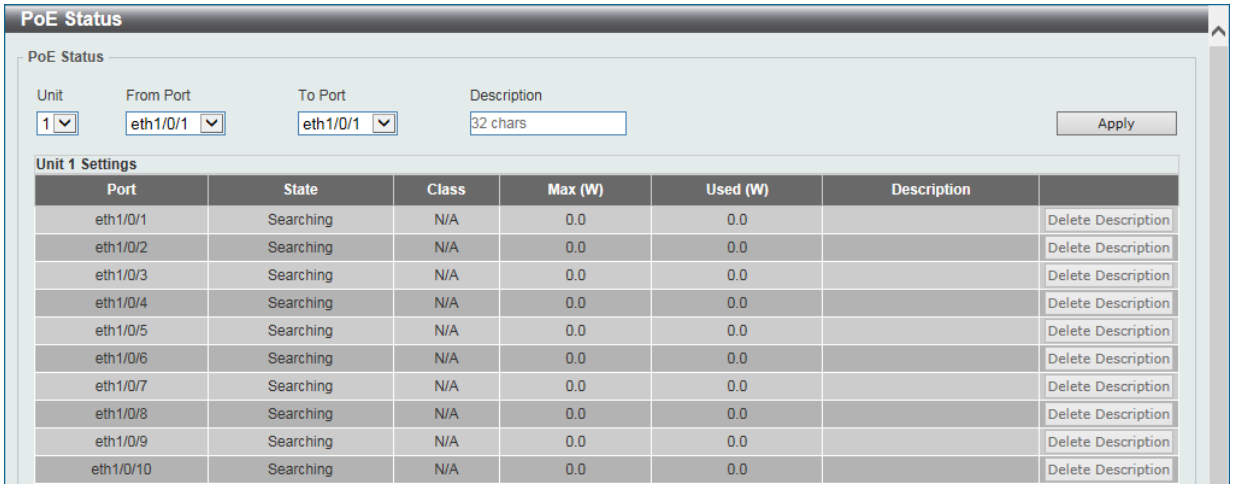


図 6-14　PoE Status 画面

以下の項目を設定します。

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Description	PoE インタフェースに接続されている PD（受電デバイス）についての説明を入力します。（32 文字以内）

「Apply」をクリックして、設定内容を適用します。
「Delete Description」をクリックして、説明を削除します。

注意　接続する PD デバイスにより、"faulty[6] - Startup Failure" エラーにより給電が開始できない場合があります。

PoE Configuration（PoE 設定）

PoE ポートの優先度、電力量、タイムレンジなど、PoE の設定を行います。

補足　IEEE802.3at PD への給電に失敗する場合は、以下の点について確認してください。

- 対象の PD デバイスが IEEE802.3at に準拠していることを確認
- 対象のポートを 30W に手動設定

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

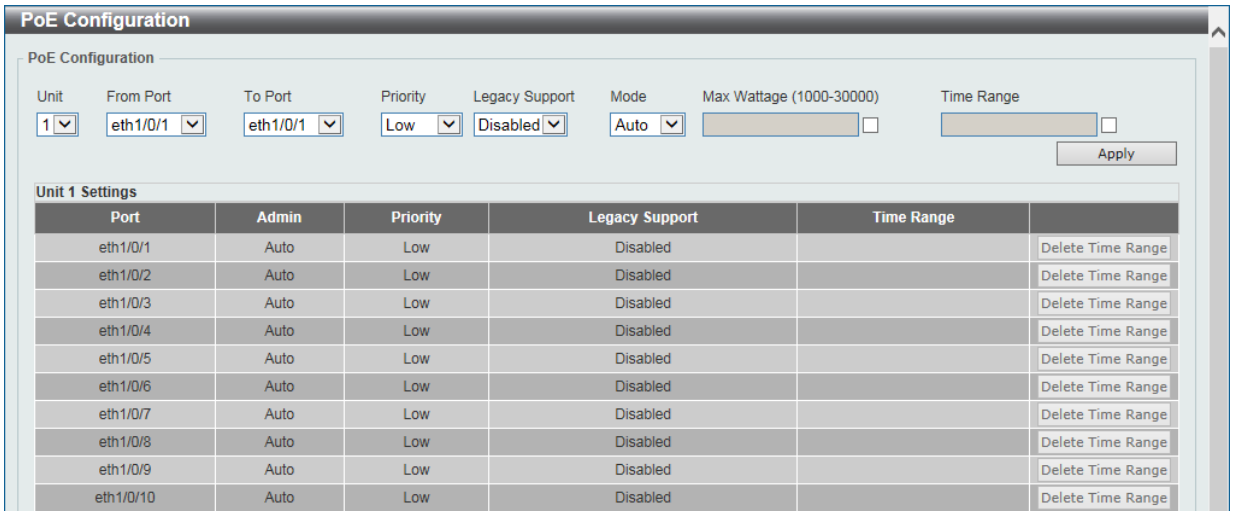


図 6-15　PoE Configuration 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Priority	ポートの優先度を指定します。ポート優先度はシステムがどのポートに優先的に電力供給を行うかを設定します。 • 選択肢：「Critical」「High」「Low」
Legacy Support	レガシー PD（受電機器）のサポートを有効 / 無効にします。
Mode	PoE ポートの電力管理モードを選択します。 • 選択肢：「Auto」「Never」
Max Wattage	本項目は「Mode」で「Auto」を選択した場合に表示されます。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を指定します。数値を設定しない場合、PD のクラスによって、供給可能な電力が自動的に決定されます。 • 設定可能範囲：1000 - 30000（mW）
Time Range	本項目は「Mode」で「Auto」を選択した場合に表示されます。チェックボックスにチェックを入れ、定義済みのタイムレンジ名を入力します。タイムレンジにより、ポートの PoE 機能を有効にする時間を指定します。

「Apply」をクリックして、設定内容を適用します。
「Delete Time Range」をクリックするとタイムレンジが削除されます。

PD Alive（PD アライブ）

PD アライブ機能の設定を行います。PoE ポートに接続している PD（受電機器）の状態を「Ping」を使用して確認します。PD が動作していない場合、PoE ポートのリセット、通知などを行います。

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

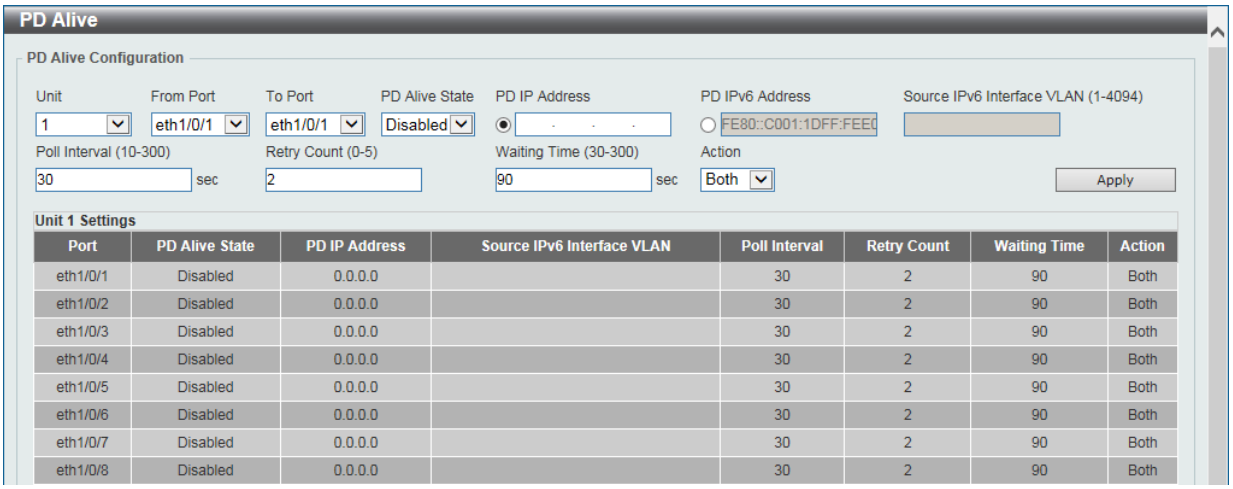


図 6-16　PD Alive 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
PD Alive State	PD 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。
PD IPv6 Address	PD の IPv6 アドレスを指定します。
Source IPv6 Interface VLAN	Ping パケットで使用する送信元 IPv6 インタフェース VLAN を指定します。
Poll Interval	ポーリング間隔を指定します。ポーリング間隔は、指定の PD の状況を確認するために Ping を送信する間隔です。 • 設定可能範囲：10 - 300（秒）
Retry Count	リトライ回数を指定します。リトライ回数は、指定の PD から応答がなかった際に Ping を再送信する回数です。 • 設定可能範囲：0 - 5
Waiting Time	待機時間を指定します。待機時間は、リセットアクションが実行された後、その PD に ping メッセージを送信する前にシステムが待機する時間です。 • 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。（一旦 PoE をオフにし、再度オンにします。） • 「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。（一旦 PoE をオフにし、再度オンにします。）

「Apply」をクリックして、設定内容を適用します。

注意　タイムレンジを PD Alive と併用した場合、PD Alive は機能しません。

PoE Statistics（PoE 統計）

PoE の統計情報を表示します。

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

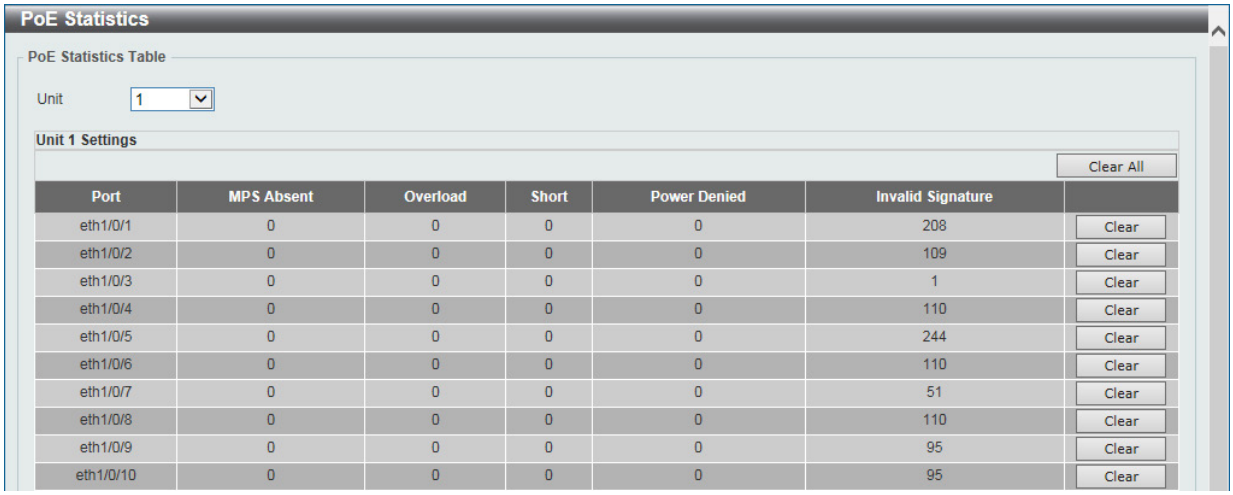


図 6-17　PoE Statistics 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

「Clear All」をクリックすると全ポートの PoE 統計情報が消去されます。
「Clear」をクリックすると対象ポートの PoE 統計情報が消去されます。

注意　未給電のポートでは、「Invalid Signature」のカウンタが上昇しますが、異常ではありません。

PoE Measurement（PoE 計測）

PoE の計測情報を表示します。

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

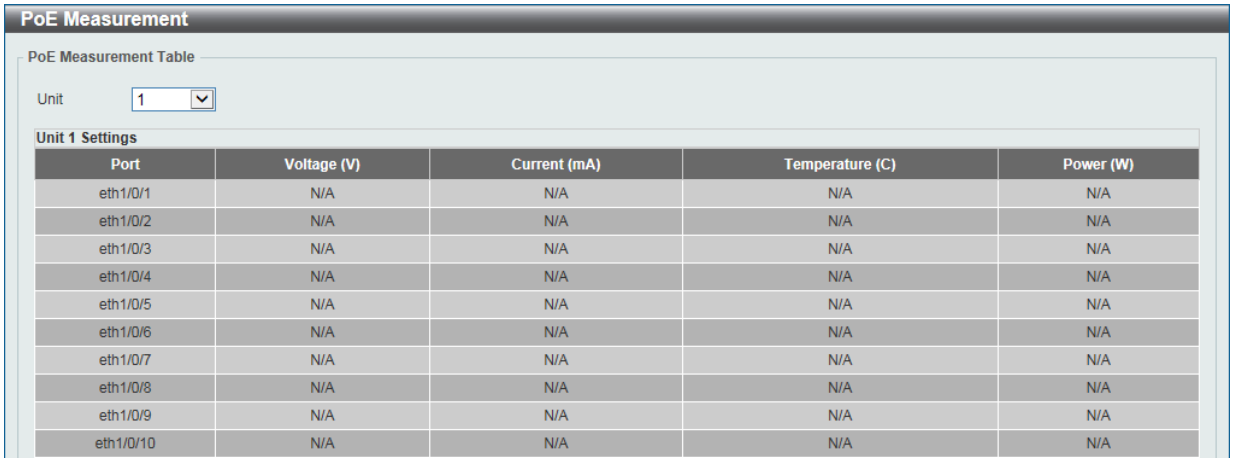


図 6-18　PoE Measurement 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

PoE LLDP Classification（PoE LLDP 分類表示）

PoE の LLDP 分類情報を表示します。

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

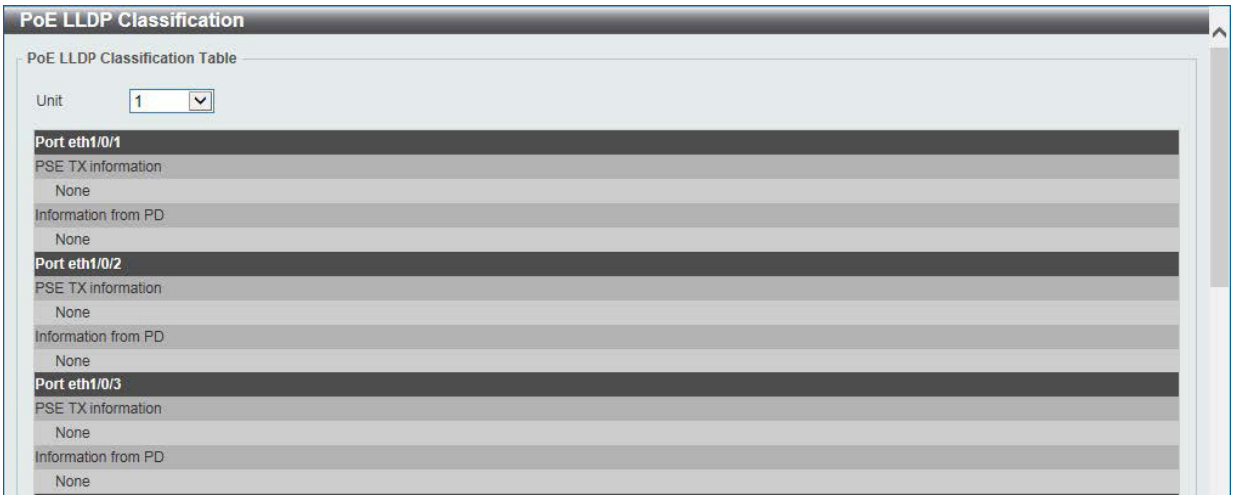


図 6-19　PoE LLDP Classification 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

System Log（システムログ構成）

システムログの設定を行います。

System Log Settings（システムログ設定）

システムログ機能のステータスや、ログの保存方法などを設定します。

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

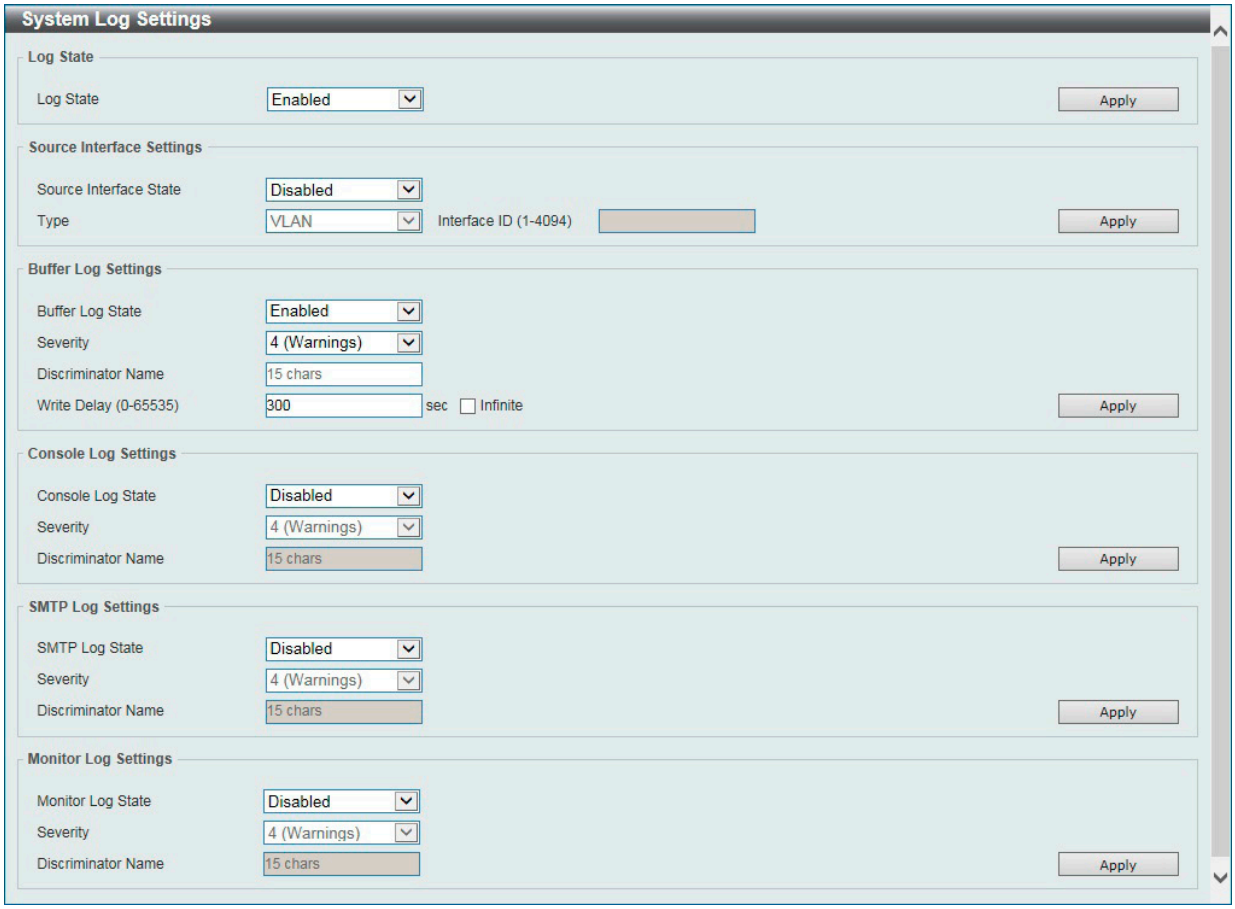


図 6-20　System Log Settings 画面

画面に表示される項目：

項目	説明
Log State	
Log State	シスログのグローバルステータスを有効 / 無効に指定します。
Source Interface Settings	
Source Interface State	ソースインタフェースのグローバルステータスを有効 / 無効に指定します。
Type	インタフェースの種類を選択します。 • 選択肢：「Loopback」「VLAN」
Interface ID	インタフェース ID を指定します。 • 設定可能範囲：1-8（Loopback 選択時）、1-4094（VLAN 選択時）
Buffer Log Settings	
Buffer Log State	バッファログのグローバルステータスを有効 / 無効に指定します。 • 選択肢：「Enable」「Disabled」「Default」 「Default」を選択すると、バッファログのグローバルステータスは初期設定に従います。
Severity	ログ出力される情報のレベルを選択します。 • 選択肢：「0：Emergencies」（緊急）、「1：Alerts」（アラート）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Discriminator Name	ディスクリミネータの名前を入力します。（15 文字以内）このディスクリミネータプロファイルで指定されたフィルタリング条件に基づき、バッファログメッセージがフィルタされます。

項目	説明
Write Delay	フラッシュにロギングバッファを書き込む間隔を指定します。 • 設定可能範囲：0-65535（秒） • 初期値：300（秒） 「Infinite」にチェックを入れると本機能は無効になります。
Console Log Settings	
Console Log State	コンソールログのグローバルステータスを有効 / 無効に指定します。
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」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Discriminator Name	ディスクリミネータの名前を入力します。（15 文字以内）このディスクリミネータプロファイルで指定されたフィルタリング条件に基づき、コンソールログメッセージがフィルタされます。
SMTP Log Settings	
SMTP Log State	SMTP ログのグローバルステータスを有効 / 無効に指定します。
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」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Discriminator Name	ディスクリミネータの名前を入力します。（15 文字以内）このディスクリミネータプロファイルで指定されたフィルタリング条件に基づき、SMTP ログメッセージがフィルタされます。
Monitor Log Settings	
Monitor Log State	モニタログのグローバルステータスを有効 / 無効に指定します。
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」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Discriminator Name	ディスクリミネータの名前を入力します。（15 文字以内）このディスクリミネータプロファイルで指定されたフィルタリング条件に基づき、モニタログメッセージがフィルタされます。

「Apply」ボタンをクリックして、設定内容を適用します。

System Log Discriminator Settings（システムログディスクリミネータ設定）

システムログディスクリミネータの設定、設定内容の表示を行います。

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

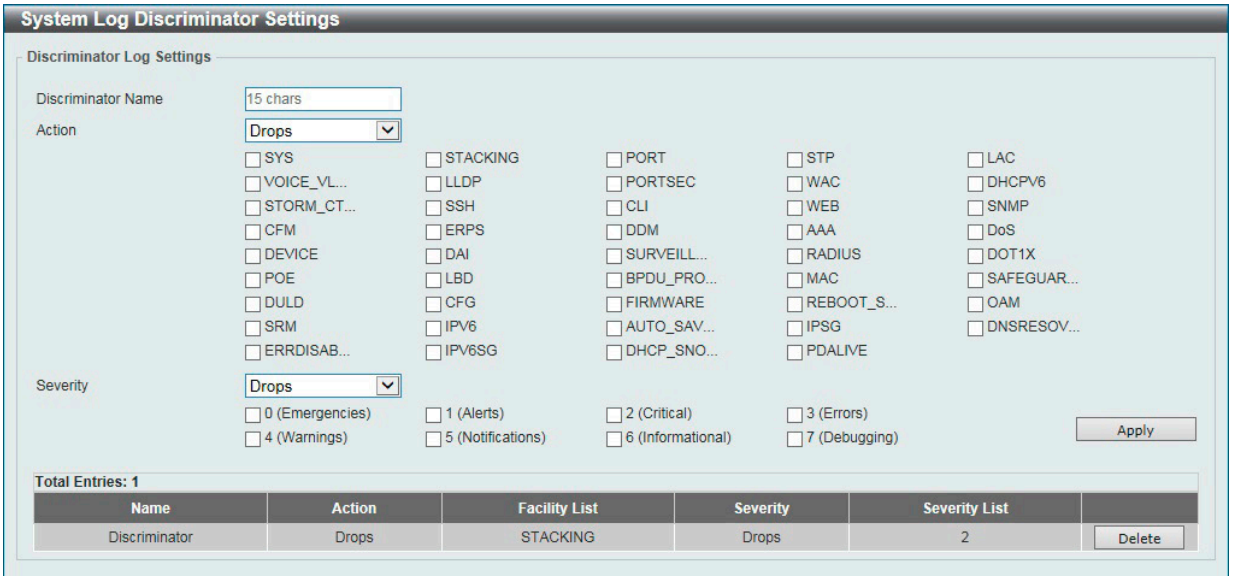


図 6-21　System Log Discriminator Settings 画面

画面に表示される項目：

項目	説明
Discriminator	ディスクリミネータの名前を入力します。（15 文字以内）
Action	ログファシリティに対する動作を「Drops（破棄）」「Includes（含める）」から選択し、対象とするファシリティの種類のチェックボックスにチェックを入れます。

項目	説明
Severity	ログセベリティに対する動作を「Drops（破棄）」「Includes（含める）」から選択し、ログ出力される情報のレベルのチェックボックスにチェックを入れます。セベリティは以下の種類から選択します。 • 選択肢：「1：Emergencies」（緊急）、「2：Alerts」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）

「Apply」ボタンをクリックして、設定内容を適用します。
「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 Server Settings（システムログサーバの設定）

シスログサーバを設定します。

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 6-22　System Log Server Settings 画面

画面に表示される項目：

項目	説明
Host IPv4 Address	システムログサーバの IPv4 アドレスを設定します。
Host IPv6 Address	システムログサーバの IPv6 アドレスを設定します。
UDP Port	システムログサーバの UDP ポートを設定します。 • 設定可能範囲：514、1024-65535 • 初期値：514
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」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Facility	ログ出力されるファシリティの番号を選択します。 • 選択可能範囲：0-23

Facility 値	Facility 名	Facility 概要
0	kern	カーネルメッセージ
1	user	ユーザレベルメッセージ
2	mail	メールシステム
3	daemon	システム daemon
4	auth1	セキュリティ / 権限メッセージ 1
5	syslog	Syslog により内部生成されたメッセージ
6	lpr	ラインプリンタサブシステム
7	news	ネットワークニュースサブシステム
8	uucp	UUCP サブシステム
9	clock1	クロック daemon 1
10	auth2	セキュリティ / 権限メッセージ 2
11	ftp	FTP daemon
12	ntp	NTP サブシステム
13	logaudit	ログ検査
14	logalert	ログ警告
15	clock2	クロック daemon 2
16	local0	ローカル使用 0（local0）
17	local1	ローカル使用 1（local1）
18	local2	ローカル使用 2（local2）
19	local3	ローカル使用 3（local3）
20	local4	ローカル使用 4（local4）
21	local5	ローカル使用 5（local5）
22	local6	ローカル使用 6（local6）
23	local7	ローカル使用 7（local7）

項目	説明
Discriminator	ディスクリミネータの名前を入力します。（15 文字以内）ログサーバへ送信されるログメッセージのフィルタリングで使用されます。

「Apply」ボタンをクリックして、設定内容を適用します。
「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）

システムログの閲覧 / 消去を行います。

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。

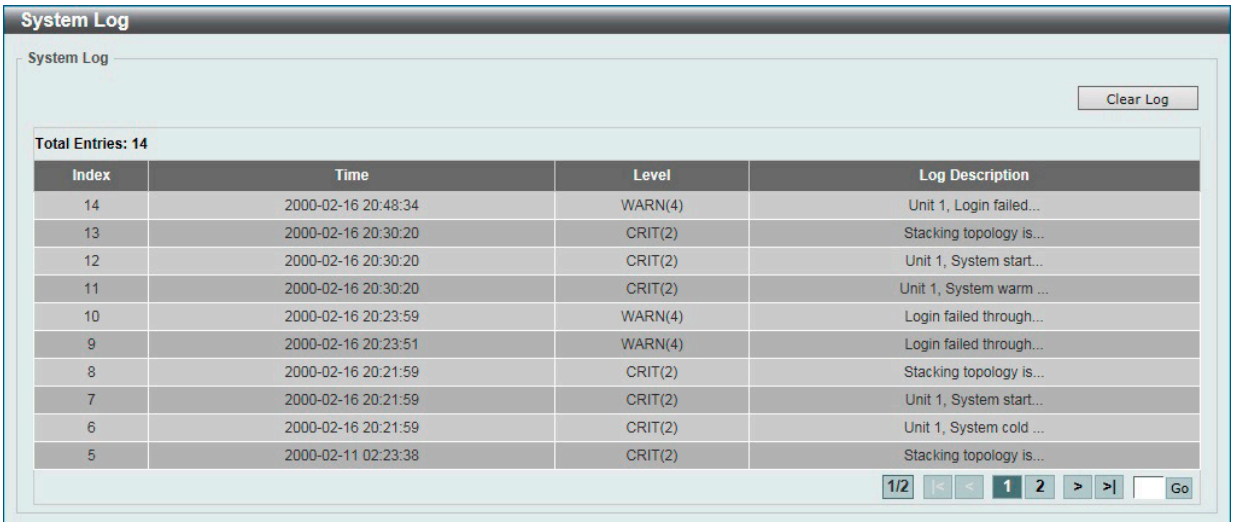


図 6-23　System Log 画面

「Clear Log」ボタンをクリックして、テーブル上のすべてのエントリを削除します。
複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

System Attack Log（システムアタックログ）

システム攻撃ログの閲覧 / 消去を行います。

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

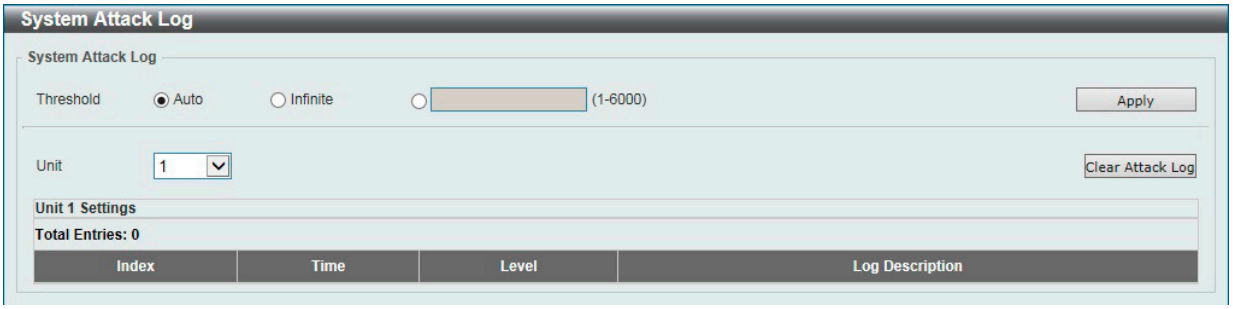


図 6-24　System Attack Log 画面

画面に表示される項目：

項目	説明
Threshold	攻撃ログのしきい値を設定します。 対象となるログ（DOS、ポートセキュリティなど）は、多数のメッセージを生成する場合があります。本項目でしきい値を設定すると、しきい値までのログはシステムログに保存され、残りのログは攻撃ログテーブルに保存されます。 • 「Auto」- 各種類のログに対し、初期値を使用します。 • 「Infinite」- 制限を設定しません。 • 「1 - 6000」- 1 分あたりのログの数を指定します。
Unit	表示するユニットを選択します。

「Clear Attack Log」ボタンをクリックして、テーブル上のすべてのエントリを削除します。

Time and SNTP（時刻設定）

System > Time and SNTP
スイッチの時刻設定を行います。手動または SNTP サーバにより時刻を設定することができます。

Clock Settings（時間設定）

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 6-25　Clock Settings 画面

画面に表示される項目：

項目	説明
Time（HH:MM:SS）	現在時刻を入力します。フォーマットは「時 : 分 : 秒」です。（例：「18:30:30」）
Date（DD/MM/YYYY）	現在の日付を入力します。フォーマットは「日 / 月 / 年」です。（例：「30/04/2015」

「Apply」ボタンをクリックして、設定内容を適用します。

Time Zone Settings（タイムゾーン設定）

SNTP のタイムゾーンとサマータイム（Daylight Saving Time）の設定を行います。

System > Time 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。

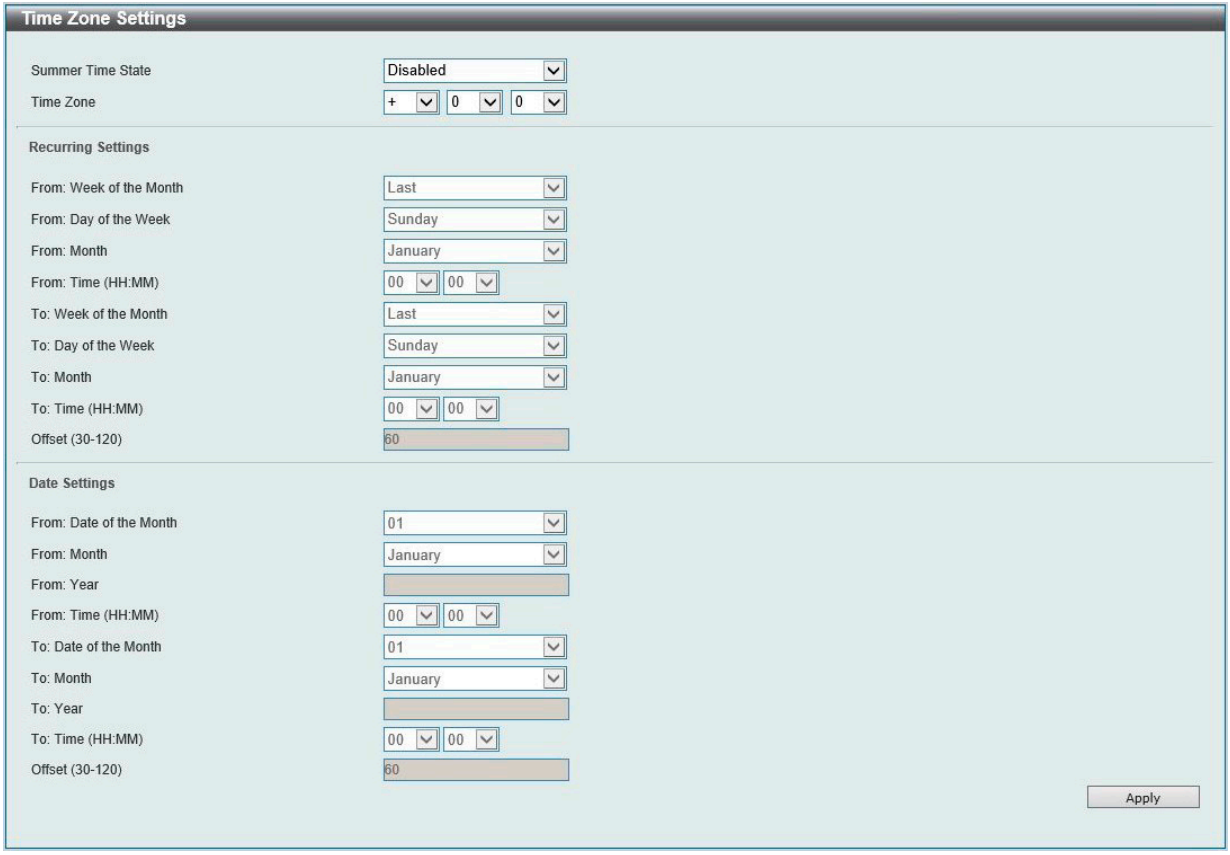


図 6-26　Time Zone Settings 画面

表示される項目：

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 Settings」- サマータイムを周期的に有効にします。このオプションでは、指定月の指定曜日にサマータイムが開始 / 終了します。 • 「Date Settings」- サマータイムを日付指定で有効にします。このオプションでは、指定年月日にサマータイムが開始 / 終了します。
Time Zone	ローカルタイムゾーンの UTC からのオフセットを指定します。
Recurring Settings	
Recurring Setting モードを使用すると、サマータイムの設定を指定した期間で自動的に調整できるようになります。例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。	
From: 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 the Week	サマータイムが開始する曜日を指定します。 • 選択肢：「Sunday」「Monday」「Tuesday」「Wednesday」「Thursday」「Friday」「Saturday」
From: Month	サマータイムが開始する月を指定します。 • 選択肢:「January」「February」「March」「April」「May」「June」「July」「August」「September」「October」「November」「December」
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 the Week	サマータイムが終了する曜日を指定します。
To: Month	サマータイムが終了する月を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。 • 設定可能範囲：30-120 • 初期値：60（分）
Date Settings	
From: Date of the Month	サマータイムが開始する日にちを指定します。
From: Month	サマータイムが開始する月を指定します。
From: Year	サマータイムが開始する年を指定します。
From: Time (HH:MM)	サマータイムが開始する時間を指定します。
To: Date of the Month	サマータイムが終了する日にちを指定します。
To: Month	サマータイムが終了する月を指定します。
To: Year	サマータイムが終了する年を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。 • 設定可能範囲：30-120 • 初期値：60（分）

「Apply」ボタンをクリックして、設定内容を適用します。

SNTP Settings（SNTP 設定）

SNTP（Simple Network Time Protocol ）はインターネット経由でコンピュータのクロックを同期するプロトコルです。標準時と周波数標準サービスへのアクセス、サーバとクライアントの SNTP サブネットの体系付け、および各関連機器のシステムクロックの調整を行う包括的なメカニズムを提供します。

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。

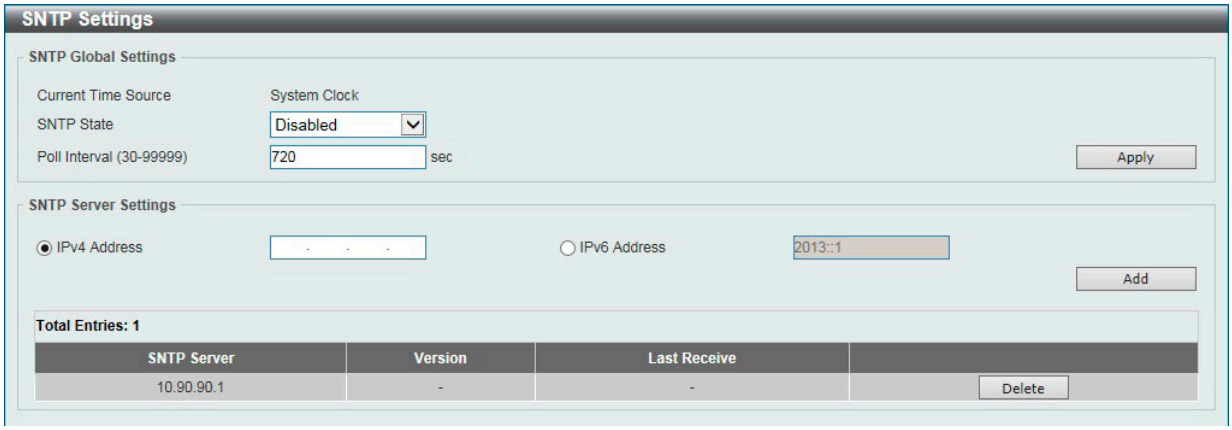


図 6-27　SNTP Settings 画面

画面に表示される項目：

項目	説明
SNTP Global Settings	
Current Time Source	現在の日付と時刻の提供元を表示します。
SNTP State	SNTP ステータス を有効 / 無効に設定します。
Poll Interval	同期する間隔を指定します。 • 設定可能範囲：30-99999（秒） • 初期値：720（秒）
SNTP Server Settings	
IPv4 Address	SNTP 情報の取得元であるサーバの IPv4 アドレスを設定します。
IPv6 Address	SNTP 情報の取得元であるサーバの IPv6 アドレスを設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Add」ボタンをクリックして、SNTP サーバを追加します。
「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 ACL 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。

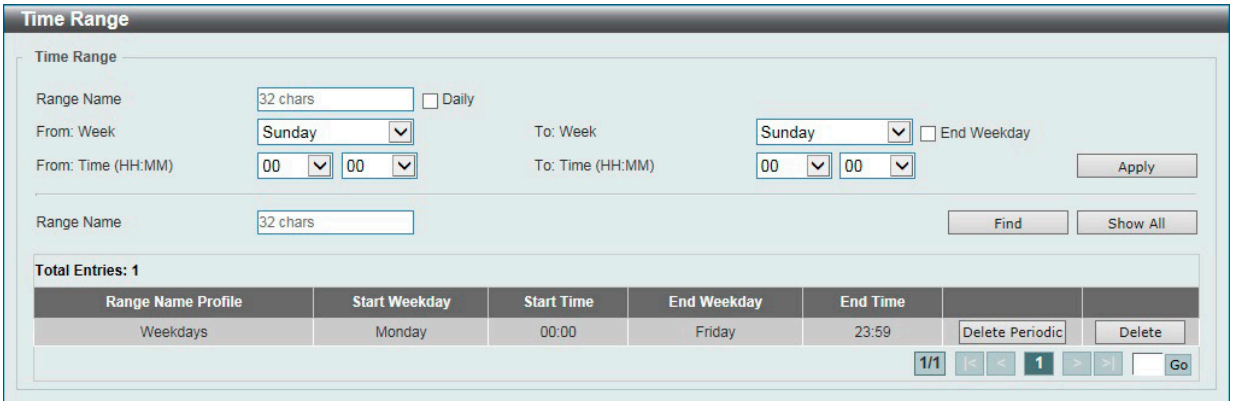


図 6-28　Time Range 画面

画面に表示される項目：

項目	説明
Range Name	タイムレンジのプロファイル名を入力します。（32 文字以内）
From Week / To Week	タイムレンジに使用する「始まり」と「終わり」の曜日を指定します。 「Daily」にチェックを入れると「毎日」がタイムレンジとして指定されます。 「End 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て、設定内容を適用します。
「Find」ボタンをクリックして、指定のエントリを検索します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

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て、該当エントリを削除します。
削除するエントリ横の「Delete Periodic」ボタンをクリックして、定期エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

PTP（PTP 設定）

System > PTP

PTP（Precision Time Protocol : 高精度時刻同期方式）システムは、イーサネットネットワークを通して 1 マイクロ秒未満の精度で分散クロックを同期させることができます。

PTP は、ネットワークシステムにおける正確なクロックの同期を可能にする技術です。イーサネットや UDP を含むマルチキャストメッセージ送信をサポートするローカルエリアネットワークで通信するシステムに適しています。PTP により、異なる固有の精度、分解能、安定性を持つ様々なシステムをグランドマスタクロックに同期させることが可能となります。

同期プロセスは 2 つの処理に分かれます。

- ベストマスタクロック（BMC : Best Master Clock）アルゴリズム - すべてのローカルポートの PTP 状態（マスタ / スレーブ）を決定します。
- 同期アルゴリズム - マスタクロックとスレーブクロック間のクロックオフセットを計算します。イベントメッセージの伝搬時間を計算するために、2 つのメカニズム（Delay Request-response Mechanism および Peer Delay Mechanism）を使用します。

PTP システムには、3 つ PTP デバイスタイプ（境界クロック、エンドツーエンド透過クロック、およびピアツーピア透過クロック）があります。境界クロックのみベストマスタクロックの選択に参加できます。

スタックモードが有効で、トランクグループのメンバポートが複数のスタックユニットに存在する場合、PTP 機能は次の動作となります。

- 同じスタックユニットのメンバポートへの PTP メッセージの送受信時に通常通り動作します。
- 異なるスタックユニットのメンバポートへの PTP メッセージの送受信時には正常に動作しません。

PTP Global Settings（PTP グローバル設定）

PTP 機能のグローバルステータスを設定します。

System > PTP (Precise Time Protocol) > PTP 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 6-29　PTP Global Settings 画面

画面に表示される項目：

項目	説明
PTP Global Settings	
PTP State	PTP 機能を有効 / 無効に設定します。 PTP 機能が有効になっている場合、スイッチポートはフィールドを修正するために滞留時間を追加します。PTP 機能が無効の場合、すべてのポートはマルチキャストフィルタリングの設定に従って PTP パケットを転送します。
PTP Mode	「E2E Transparent」に指定されます。

「Apply」ボタンをクリックして、設定内容を適用します。

スタックモードが有効で、トランクグループのメンバポートが異なるスタックユニットに存在する場合、PTP 機能が正しく機能しない場合があります。

- 同じスタックユニットのメンバポートへの PTP メッセージの送受信時に通常通り動作します。
- 異なるスタックユニットのメンバポートへの PTP メッセージの送受信時には正常に動作しません。

注意　PTP 機能は、単体利用の場合のみサポートしている機能です。スタック構成時にはご使用になれませんのでご注意ください。

PTP Port Global Settings（PTP ポートグローバル設定）

ポート毎の PTP ステータスを設定します。

System > PTP (Precise Time Protocol) > PTP Port 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。

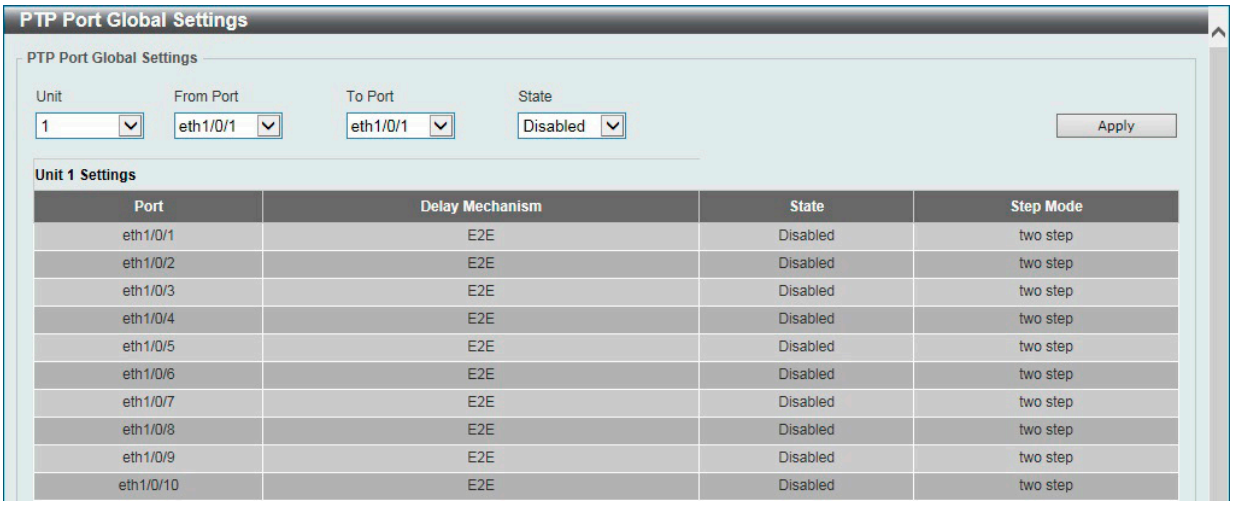


図 6-30　PTP Port Global Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートの PTP ステータスを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

Reset Button Settings（リセットボタンの設定）

リセット /ZTP ボタンの動作を設定します。

System > Reset Button 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 6-31　Reset Button Settings 画面

画面に表示される項目：

項目	説明
Reboot	リセット /ZTP ボタンのリブート機能を有効または無効にします。 有効にした場合、スイッチのリセット /ZTP ボタンを 0 - 5 秒間押すと、スイッチが再起動します。
Zero Touch Provision	リセット /ZTP ボタンの ZTP（Zero Touch Provisioning）機能を有効または無効にします。 有効にした場合、スイッチのリセット /ZTP ボタンを 5 - 10 秒間押すと、ZTP が開始されます。
Factory Default	リセット /ZTP ボタンのリセット機能を有効または無効にします。 有効にした場合、スイッチのリセット /ZTP ボタンを 10 秒以上押すと、スイッチの再起動と工場出荷時設定へのリセットが実行されます。

「Apply」ボタンをクリックして、設定内容を適用します。

Archive Settings（アーカイブ設定）

コンフィグレーションのアーカイブ設定を行います。現在実行中のコンフィグレーションファイルを指定サーバに自動で保存することができます。

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

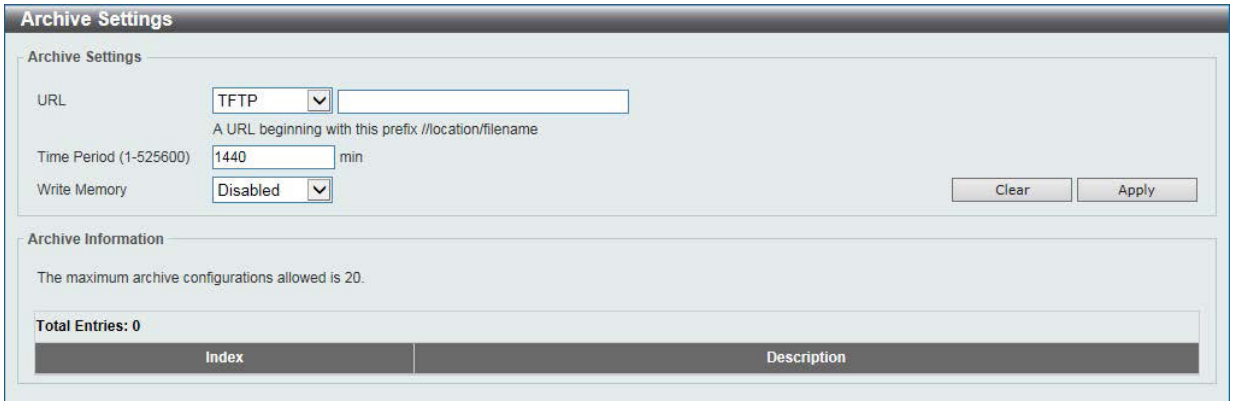


図 6-32　Archive Settings 画面

画面に表示される項目：

項目	説明
URL	サーバの種類を選択し、IPv4/IPv6 アドレスを入力します。 • 選択肢：「TFTP」「FTP」「RCP」
Time Period	実行中のコンフィグレーションを保存する間隔を指定します。 • 設定範囲：1 - 525600（分） • 初期値：1440（分）
Write Memory	本機能を有効にすると、コンフィグレーションの保存を実施した際に、指定サーバへのアーカイブ保存も実行されます。

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、アーカイブ情報エントリを削除します。

注意　archive コマンドで FTP 指定時にエラーが発生する場合、no network-protocol-port protect tcp コマンドを実行してください。

注意　アーカイブ保存においてファイルに自動付与される "_<timestamp>" の形式は、"_dd-mm-yy_HH-MM"（イギリス式）です。

注意　Archive Information セクションの "The maximum archive configurations allowed is 20." というメッセージは、表示される履歴の最大が 20 であることを意味しています。Index が 20 を超える場合に、テーブル表示から古い履歴が削除されます。

※アーカイブ先のサーバにおいては、古い設定ファイルが保持されたままになりますので、容量にご注意ください。

第 7 章　Management（スイッチの管理）

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
Command Logging（コマンドログ設定）	コマンドログ設定を有効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
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。
Password Encryption（パスワード暗号化）	パスワードを暗号化し設定ファイルに保存します。
Password Recovery（パスワードリカバリ）	パスワードリカバリを行います。例えば管理者がパスワードを忘れた場合に有効です。
Login Method（ログイン方法）	各管理インタフェースでのログイン方法について設定します。
Web Login Lock Settings（Web ログインロック設定）	Web ログイン失敗時のロック設定を行います。
SNMP（SNMP 設定）	SNMP 設定を有効にします。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。
RMON（RMON 設定）	SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効にします。
Telnet/Web（Telnet/Web 設定）	スイッチの Telnet/Web 設定を有効にします。
Session Timeout（セッションタイムアウト）	各セッション（Web やコンソールなど）のタイムアウトの設定をします。
DHCP（DHCP 設定）	スイッチの DHCP について設定します。
DHCP Auto Configuration（DHCP 自動コンフィグ設定）	DHCP 自動コンフィグ機能の設定を行います。
DHCP Auto Image Settings（DHCP 自動イメージ設定）	DHCP 自動イメージ設定を行います。スタートアップ時に、外部サーバからイメージファイルを取得する機能です。
DNS（ドメインネームシステム）	DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。
File System（ファイルシステム設定）	フラッシュファイルシステムにより、ファームウェア、コンフィグレーション情報、および Syslog 情報はフラッシュ内のファイルに保存されます。
Stacking（スタッキング設定）	物理スタッキングの設定を行います。
シングル IP マネジメント（SIM）設定	仮想（SIM）スタッキングの設定を行います。
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。
SMTP Settings（SMTP 設定）	Simple Mail Transfer Protocol (SMTP) の設定を行います。
Reboot Schedule Settings（再起動スケジュール設定）	スイッチの再起動スケジュール設定を行います。
NLB FDB Settings（NLB FDB 設定）	ネットワークロードバランシング (NLB) の設定を行います。
PPPoE Circuit ID Insertion Settings（PPPoE 回線 ID 挿入設定）	PPPoE 回線 ID 挿入機能の設定を行います。
TCP Path MTU Discovery（TCP パス MTU 検出）	IP TCP パス MTU 変換の設定を行います。
TCP Selective ACK（TCP 選択的確認応答）	TCP 選択的確認応答の設定を行います。
TWAMP（TWAMP 設定）	Two-Way Active Measurement Protocol（TWAMP）の設定を行います。

Command Logging（コマンドログ設定）

コマンドログ設定を有効または無効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。システムログには、コマンド及びコマンドを入力したユーザ情報が含まれます。スイッチの設定や処理に変更が発生しないコマンド（例 : show）はログに出力されません。

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

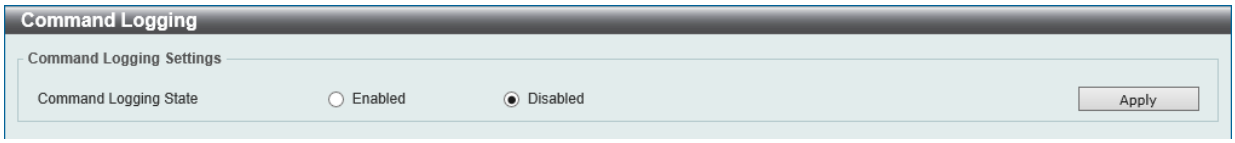


図 7-1　Command Logging 画面

画面に表示される項目：

項目	説明
Command Logging State	コマンドログ機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

User Accounts Settings（ユーザアカウント設定）

ユーザアカウントの作成と更新を行います。アクティブなユーザのセッションを確認することもできます。Web UI で利用可能な設定オプションは、アカウントの権限レベルによって異なります。

User Management Settings タブ

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

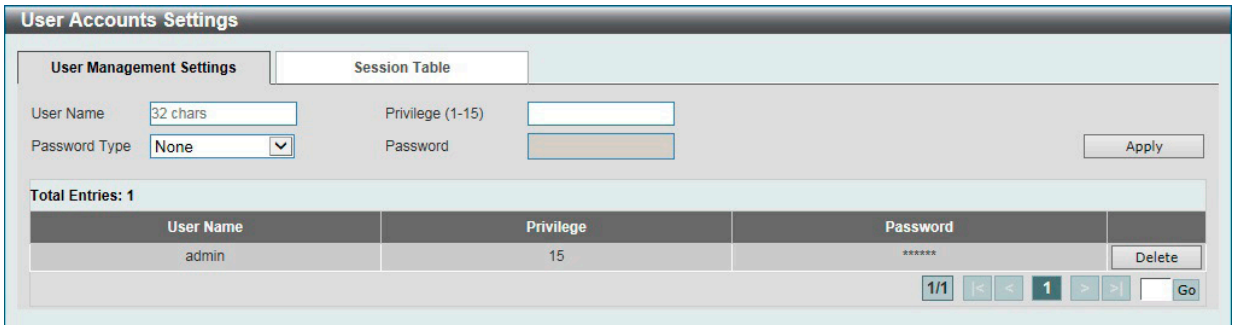


図 7-2　User Accounts Settings 画面 - User Management Settings タブ

画面に表示される項目：

項目	説明
User Name	ユーザ名を定義します。（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パスワードの種類を選択します。 • 選択肢：「None」「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」
Password	ユーザアカウントのパスワードを入力します。 パスワードの入力ルールは以下の通りです。 • 8 - 30 文字以内の UTF-8 文字（Unicode Hex 範囲 0x0021 - 0x007e） • アルファベットの大文字小文字、数字、記号をそれぞれ 1 つ以上含める必要があります。 • 非連続文字でなければなりません。 • ユーザ名と同じにすることはできません。 • デフォルトのログインアカウントとデフォルトの IP アドレスを含めることはできません。

「Apply」ボタンをクリックして、設定内容を適用します。
複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

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

Session Table タブ

「Session Table」タブをクリックすると、現在のアクティブなユーザアカウントの情報が表示されます。

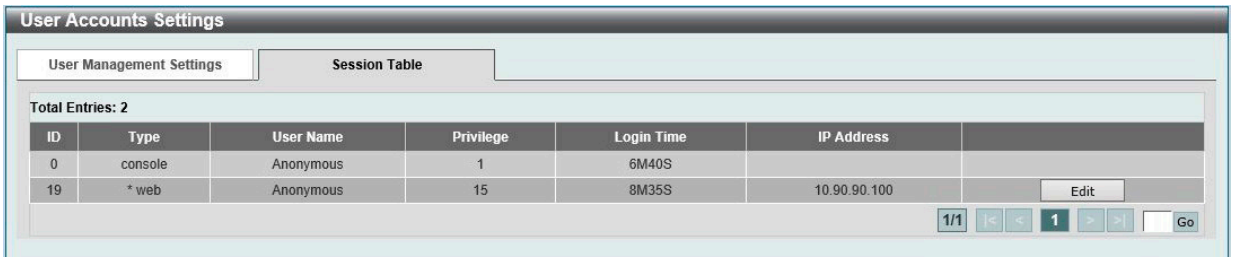


図 7-3　User Accounts Settings 画面 - Session Table タブ

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。
「Edit」ボタンをクリックすると、ユーザ権限の設定画面へ移動します。

■ User Privilege（ユーザ権限）

「Session Table」タブで「Edit」をクリックするとユーザ権限設定画面が表示されます。

図 7-4　User Accounts Settings（Edit）- User Privilege 画面

画面に表示される項目：

項目	説明
Action	ユーザレベルのセキュリティ設定を有効 / 無効に設定します。
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	パスワードを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Password Encryption（パスワード暗号化）

パスワードを暗号化して設定ファイルに保存します。

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

図 7-5　Password Encryption 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

Password Recovery（パスワードリカバリ）

パスワードリカバリの設定を行います。管理者がパスワードを忘れた場合などにアカウントの更新が必要になります。

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

図 7-6　Password Recovery 画面

画面に表示される項目：

項目	説明
Password Recovery State	パスワードリカバリ機能を有効 / 無効に設定します。本機能を有効にすると、CLI でのリセットコンフィグレーションモードへのアクセスが可能になります。リセットコンフィグモードでは以下の内容を実行できます。 - ユーザアカウントの更新 - 管理者権限レベルの enable password 機能の更新 - AAA 機能を無効にしてローカル認証を許可 その後、実行中のコンフィグレーションをブートコンフィグとして保存することが可能です。再起動が必要です。

「Apply」ボタンをクリックして、設定内容を適用します。

Login Method（ログイン方法）

各管理インタフェースへのログイン方法について表示、設定します。

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

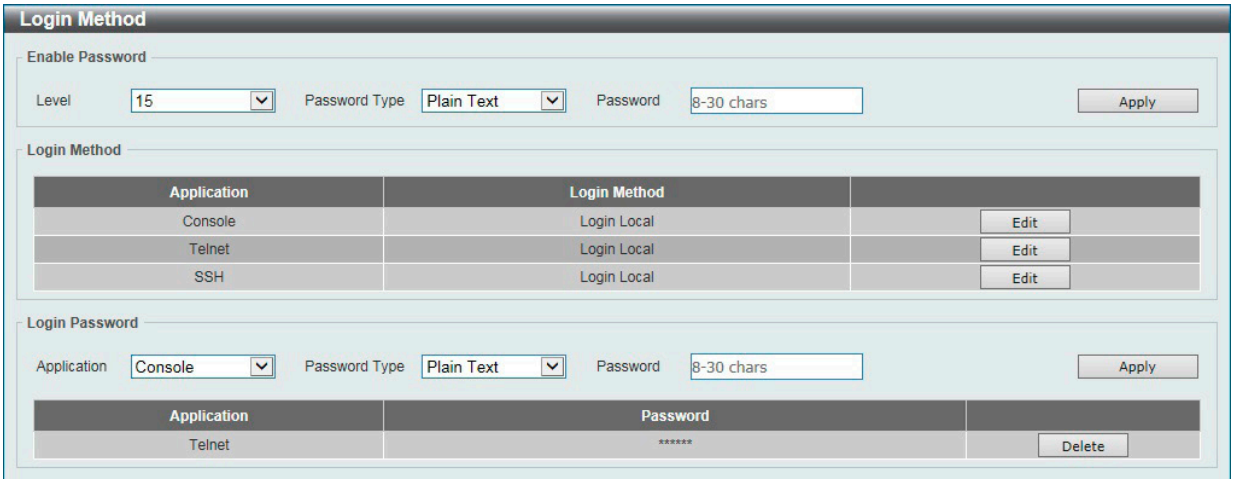


図 7-7　Login Method 画面

画面に表示される項目：

項目	説明
Enable Password	
Level	ユーザの権限レベルを指定します。 • 設定可能範囲：1-15
Password Type	暗号化の方法を選択します。 •「Plain Text」- パスワードは平文形式となります。（初期値） •「Encrypted-SHA1」- パスワードは SHA1 形式で暗号化されます。 •「Encrypted-MD5」- スワードは MD5 形式で暗号化されます。
Password	ユーザアカウントのパスワードを入力します。 •「Plain Text」選択時：入力ルールは以下の通りです。 - 8 - 30 文字以内の UTF-8 文字（Unicode Hex 範囲 0x0021 - 0x007e） - アルファベットの大文字小文字、数字、記号をそれぞれ 1 つ以上含める必要があります。 - 非連続文字でなければなりません。 - ユーザ名と同じにすることはできません。 - デフォルトのログインアカウントとデフォルトの IP アドレスを含めることはできません。 •「Encrypted-SHA1」選択時：35 バイト（大文字と小文字を区別） •「Encrypted-MD5」選択時：31 バイト（大文字と小文字を区別）
Login Method	
Login Method	「Edit」ボタンをクリックしてパラメータの設定を行います。指定のアプリケーションへのログイン方法を選択します。 •「No Login」- 指定アプリケーションへアクセスするためのログイン認証は不要です。 •「Login」- 指定アプリケーションへアクセスするにはパスワードを入力する必要があります。 •「Login Local」- 指定アプリケーションへアクセスするにはユーザ名とパスワードの入力が必要になります。
Login Password	
Application	設定するアプリケーションを選択します。 • 選択肢：「Console」「Telnet」「SSH」
Password Type	パスワード暗号化の方法を選択します。 • 選択肢：「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」
Password	選択したアプリケーションで使用するパスワードを入力します。 指定のアプリケーションのログイン方法が「Login」に設定されている時のパスワードになります。 •「Plain Text」選択時：入力ルールは以下の通りです。 - 8 - 30 文字以内の UTF-8 文字（Unicode Hex 範囲 0x0021 - 0x007e） - アルファベットの大文字小文字、数字、記号をそれぞれ 1 つ以上含める必要があります。 - 非連続文字でなければなりません。 - ユーザ名と同じにすることはできません。 - デフォルトのログインアカウントとデフォルトの IP アドレスを含めることはできません。 •「Encrypted-SHA1」選択時：35 バイト（大文字と小文字を区別） •「Encrypted-MD5」選択時：31 バイト（大文字と小文字を区別）

「Apply」ボタンをクリックして、設定内容を適用します。

「Edit」ボタンをクリックすると、設定内容を編集できます。

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

Web Login Lock Settings（Web ログインロック設定）

Web ログイン失敗時のロック設定を行います。

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

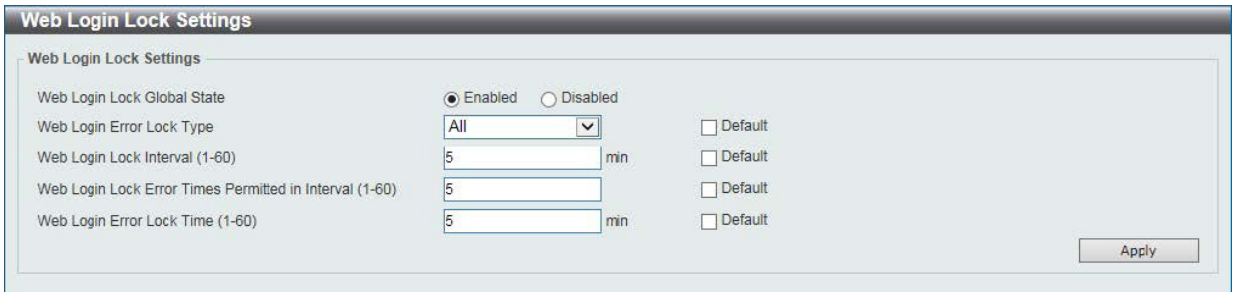


図 7-8　Web Login Lock Settings 画面

画面に表示される項目：

項目	説明
Web Login Lock Global State	Web ログインのロック機能を有効 / 無効に設定します。
Web Login Error Lock Type	ロックの種類を選択します。 • 「All」- IPv4/IPv6 アドレスによる Web ログインのロックを指定します。（初期値） • 「IP」- IPv4 アドレスによる Web ログインのロックを指定します。 • 「IPv6」- IPv6 アドレスによる Web ログインのロックを指定します。 • 「Web Session ID」- Web セッション ID による Web ログインのロックを指定します。
Web Login Lock Interval	Web ログインのエラーをチェックする間隔を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1 - 60（分） • 初期値：5（分）
Web Login Lock Error Times Permitted in Interval	指定間隔における Web ログインのエラー回数を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1 - 60（回） • 初期値：5（回）
Web Login Error Lock Time	ログインエラー検出時に Web インタフェースをロックする時間を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1 - 60（分） • 初期値：5（分）

「Apply」ボタンをクリックして、設定内容を適用します。

注意　Web ログインロック機能は、ソース IP アドレス毎に判定されます。

SNMP（SNMP 設定）

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルです。ネットワークに接続された通信機器の管理や監視を行います。

SNMP によって、ネットワーク管理ステーションはゲートウェイやルータなどのネットワークデバイスの設定状態の確認・変更をすることができます。適切な動作のためにシステム機能を設定、パフォーマンスを監視し、スイッチやスイッチグループおよびネットワークの潜在的な問題を検出します。

SNMP をサポートするデバイスは、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。
定義された変数（管理対象オブジェクト）が SNMP エージェントに保持され、デバイスの管理に使用されます。これらの管理オブジェクトは MIB（Management Information Base）内に定義され、SNMP エージェントにより管理される情報表示の基準を管理ステーションに伝えます。
SNMP は、MIB の仕様フォーマット、およびネットワーク経由で情報にアクセスするために使用するプロトコルの両方を定義しています。

■ SNMP のバージョンについて
SNMP には、「SNMPv1」「SNMPv2c」「SNMPv3」の 3 つのバージョンがあります。
これらの 3 つのバージョンでは、ネットワーク管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルが異なります。

注意　本製品がサポートしている SNMP のバージョンは v1、v2c、v3 です。

● SNMPv1 と SNMPv2c
SNMPv1 と SNMPv2c では、SNMP のコミュニティ名を使用して認証を行います。
リモートユーザの SNMP アプリケーションとスイッチの SNMP は同じコミュニティ名を使用する必要があります。認証が行われていない SNMP パケットを受信した場合、そのパケットは破棄されます。
SNMPv1 と SNMP v2c を使用する場合、初期値のコミュニティ名は以下のとおりです。

- public：管理ステーションは、MIB オブジェクトの読み取りができます。
- private： 管理ステーションは、MIB オブジェクトの読み取りと書き込みができます。

● SNMPv3
SNMPv3 では、2 つのパートで構成される、より高度な認証を行います。
最初のパートは SNMP マネージャとして動作することのできるユーザとその属性を掲載したリストを保持しています。次のパートではリスト上のユーザの SNMP マネージャとしての権限を記載しています。

ユーザのグループをリストにまとめ、権限を設定できます。また、リスト上の SNMP マネージャのグループに対して、SNMP バージョン情報を登録可能です。「SNMPv1 を使用して読み取り専用の情報とトラップの受信のみを可能にするグループ」や、「SNMPv3 を使用して高いセキュリティレベルを与え、読み書き可能にするグループ」など、グループごとに異なる設定を登録することができます。

個別のユーザや SNMP マネージャグループに SNMPv3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。
管理機能の可否は各 MIB に関連付けられる OID（Object Identifier）を使用して定義します。SNMPv3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。

トラップ

トラップは、スイッチ上で発生したイベントをネットワーク管理者に警告するためのメッセージです。

イベントには、再起動（誤ってスイッチの電源を切ってしまった）などの重大なものから、ポートの状態変化を知らせる軽微なものまで幅広い種類があります。スイッチはトラップを生成し、事前に設定された IP アドレスに送信します。トラップの例には、認証の失敗、トポロジの変化などがあります。

MIB

MIB（Management Information Base）には、管理情報およびカウンタ情報が格納されています。

本製品は標準 MIB-II モジュールを使用し、MIB オブジェクトの値を SNMP ベースのネットワーク管理ソフトウェアにより取得します。本製品は、標準 MIB-II に加えて、拡張 MIB としてベンダ固有の MIB もサポートしています。MIB OID の指定によってもベンダ固有の MIB を取得することができます。
MIB の値には「読み取り専用」「読み書き可能」があります。

SNMP Global Settings（SNMP グローバル設定）

SNMP およびトラップのグローバル設定を行います。

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

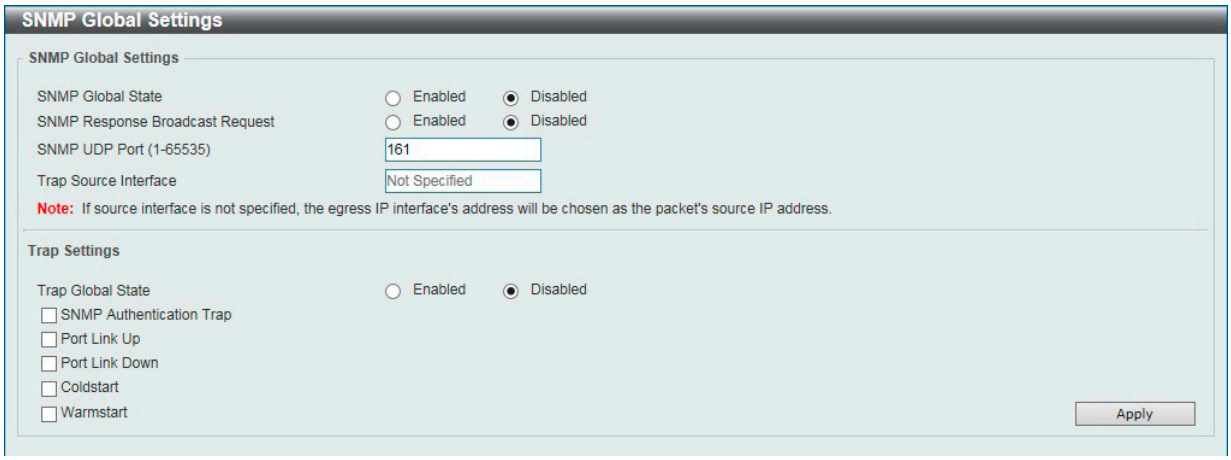


図 7-9　SNMP Global Settings 画面

画面に表示される項目：

項目	説明
SNMP Global Settings	
SNMP Global State	SNMP 機能を有効 / 無効に設定します。
SNMP Response Broadcast Request	ブロードキャスト SNMP GetRequest パケットに対するサーバの応答を有効 / 無効に設定します。
SNMP UDP Port	SNMP UDP ポート番号を指定します。
Trap Source Interface	SNMP トラップパケットを送信する送信元アドレスとして使用される 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 トラップを有効 / 無効に設定します。
SNMP Authentication Trap	SNMP 認証失敗の通知を有効にするには、本オプションにチェックを入れます。機器が正しく認証されていない SNMP メッセージを受信すると、authenticationFailuretrap トラップが生成されます。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。
Port Link Up	ポートリンクアップ通知を有効にするには、本オプションにチェックを入れます。通信リンクのいずれかが起動すると、linkUp トラップが生成されます。
Port Link Down	ポートリンクダウン通知を有効にするには、本オプションにチェックを入れます。通信リンクのいずれかがダウンすると、linkDown トラップが生成されます。
Coldstart	coldStart 通知を有効にするには、本オプションにチェックを入れます。
Warmstart	warmStart 通知を有効にするには、本オプションにチェックを入れます。

「Apply」ボタンをクリックして、設定内容を適用します。

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

SNMP リンクチェンジトラップを設定します。

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

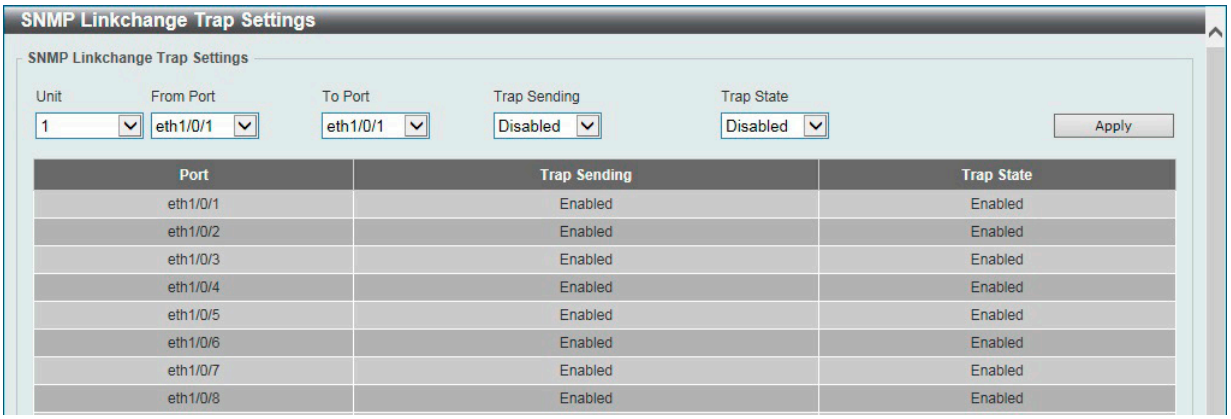


図 7-10　SNMP Linkchange Trap Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Trap Sending	SNMP 通知トラップ送信を有効 / 無効に設定します。
Trap State	linkChange トラップを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

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

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

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

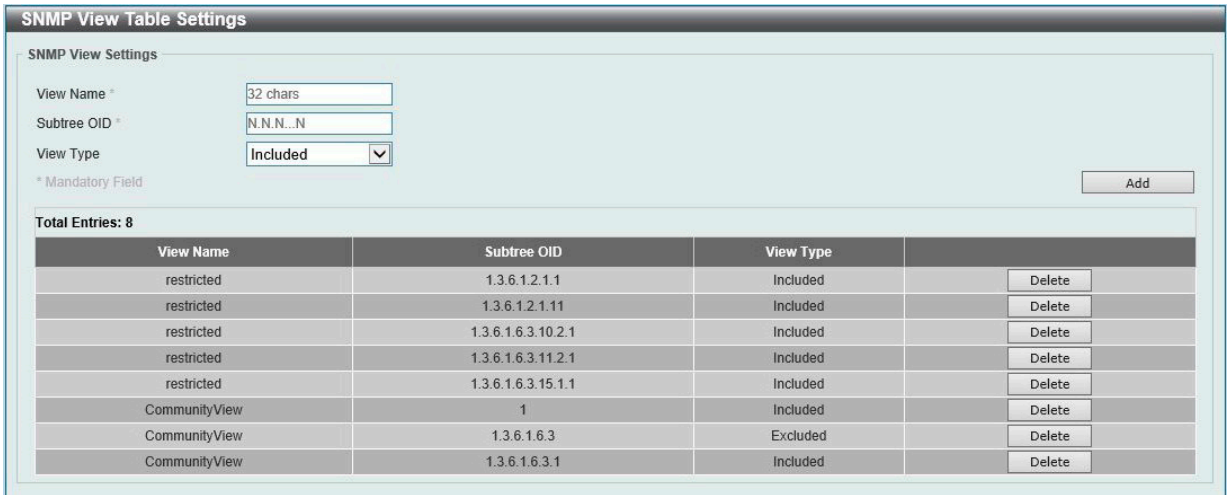


図 7-11　SNMP View Table Settings 画面

画面に表示される項目：

項目	説明
View Name	ビュー名を入力します。（半角英数字 32 文字以内）SNMP ビューを識別する際に使用します。
Subtree OID	ビューの OID（Object Identifier）サブツリーを入力します。OID は、オブジェクトツリー（MIB ツリー）が SNMP マネージャによってアクセス可能な範囲かどうかを識別します。
View Type	「Subtree OID」で指定した OID について、ビューのタイプを指定します。 • 「Included」- SNMP マネージャがアクセス可能なオブジェクトリストに含めます。 • 「Excluded」- SNMP マネージャがアクセス可能なオブジェクトのリストから除外します。

「Add」ボタンをクリックして、SNMP ビューを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

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

SNMP マネージャとエージェントの関係を定義する SNMP コミュニティ名の登録を行います。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。コミュニティ名に関連するアクセス制限は以下の通りです。

- アクセスリストには、コミュニティ名を使用してスイッチの SNMP エージェントにアクセスを行う SNMP マネージャの IP アドレスが含まれます。
- SNMP コミュニティは、MIB オブジェクトのサブセットを定義する MIB ビューにアクセスできます。
- コミュニティ名に対し、MIB オブジェクトへの Read/Write または Read-only レベルのアクセス権限が付与されます。

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 7-12　SNMP Community Table Settings 画面

画面に表示される項目：

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入力します。（半角英数字 32 文字以内）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	ビュー名を入力します。（半角英数字 32 文字以内）リモート SNMP マネージャがアクセスすることのできる MIB グループの識別に使用します。「View Name」が「SNMP View Table」で定義されている必要があります。
Access Right	アクセス権限の種類を設定します。 •「Read Only」- 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りのみ可能となります。 •「Read Write」- 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取り、および書き込みが可能です。
IP Access-List Name	ユーザを制限するために使用するアクセスリストの名前を入力します。許可されるユーザは、コミュニティ文字列を使用して SNMP にアクセスすることができます。

「Add」ボタンをクリックして、新しいエントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

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

SNMP グループを作成し、SNMP ユーザと「SNMP View Table Settings」画面で定義されているビューをマッピングします。

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

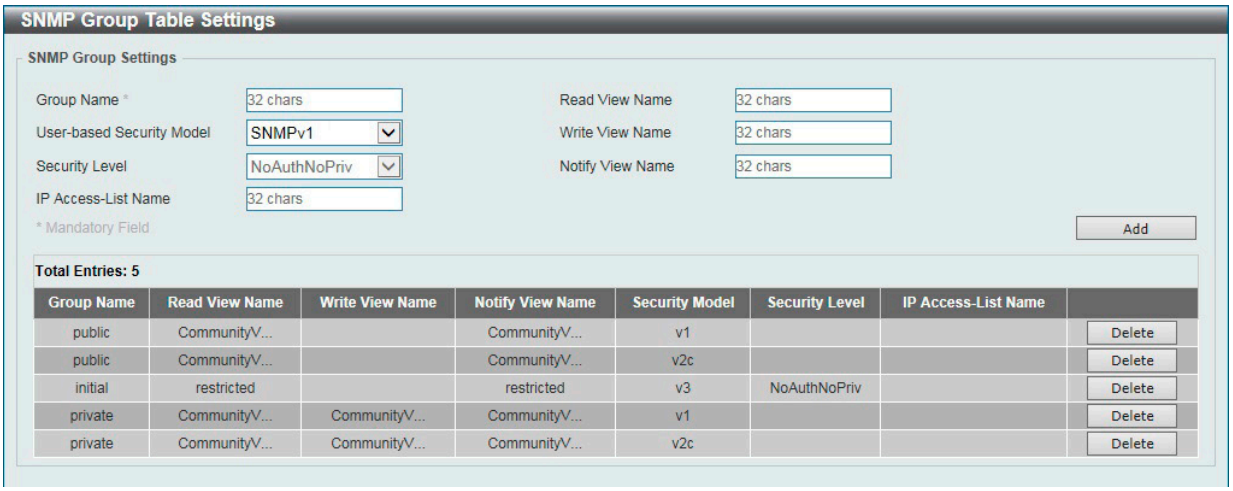


図 7-13　SNMP Group Table Settings 画面

画面に表示される項目：

項目	説明
Group Name	グループ名を入力します。（半角英数字 32 文字以内、スペース使用不可）
User-based Security Model	セキュリティモデルを選択します。 • 「SNMPv1」- SNMP バージョン 1 を使用します。 • 「SNMPv2c」- SNMP バージョン 2c を使用します。 • 「SNMPv3」- SNMP バージョン 3 を使用します。
Security Level	「SNMPv3」を選択した場合、セキュリティレベルを設定します。 • 「NoAuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証も暗号化も行われません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証は行われますが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ついて、認証 / 暗号化が行われます。
Read View Name	グループのユーザがアクセス可能な Read View 名を入力します。
Write View Name	グループのユーザがアクセス可能な Write View 名を入力します。
Notify View Name	グループのユーザがアクセス可能な Notify View 名を入力します。グループユーザに対しトラップパケット経由でステータスの通知が可能なオブジェクトです。
IP Access-List Name	アクセスするための IP アクセスコントロールリスト（ACL）の名前を入力します。

「Add」ボタンをクリックして、新しいエントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

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

エンジン ID は、SNMP バージョン 3 で使用される固有の識別名です。

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。

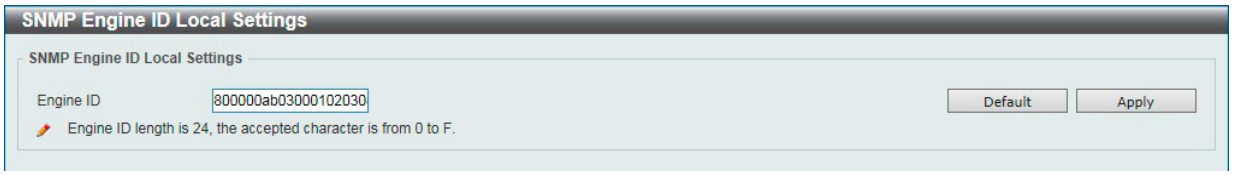


図 7-14　SNMP Engine ID Local Settings 画面

画面に表示される項目：

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 文字以内）

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」ボタンをクリックすると、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 ユーザの登録、表示を行います。

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 7-15　SNMP User Table Settings 画面

画面に表示される項目：

項目	説明
User Name	SNMP ユーザ名を入力します。（32 文字以内）
Group Name	ユーザが属する SNMP グループ名を入力します。（32 文字以内 / スペース使用不可）
SNMP Version	SNMP v3 が使用されます。
SNMP V3 Encryption	SNMP v3 に対して暗号化を有効にします。 • 選択肢：「None「Password」「Key」
Auth-Protocol by Password	「SNMP V3 Encryption」で「Password」を選択した場合に有効になります。本項目を選択後、「Password」にパスワードを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。（Password：半角英数字 8-16 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）
Priv-Protocol by Password	「SNMP V3 Encryption」で「Password」を選択した場合に有効になります。本項目を選択後、「Password」にパスワードを入力します。 • 「None」- 認証プロトコルは使用されていません。 • 「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ています。（Password：半角英数字 8-16 文字） • 「AES128」- AES 暗号が使用されます。（Password：半角英数字 8-16 文字）
Auth-Protocol by Key	「SNMP V3 Encryption」で「Key」を選択した場合に有効になります。本項目を選択後、「Key」に暗号キーを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。（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。（Key：半角英数字 40 文字）

項目	説明
Priv-Protocol by Key	「SNMP V3 Encryption」で「Key」を選択した場合に有効になります。本項目を選択後、「Key」に暗号キーを入力します。 • 「None」- 認証プロトコルは使用されていません。 • 「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ています。（Key：半角英数字 32 文字） • 「AES128」- AES 暗号が使用されます。（Key：半角英数字 32 文字）
IP Access-List Name	ユーザに関連付ける標準 IP アクセスコントロールリストの名前を入力します。

「Add」ボタンをクリックして、SNMP ユーザを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

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。

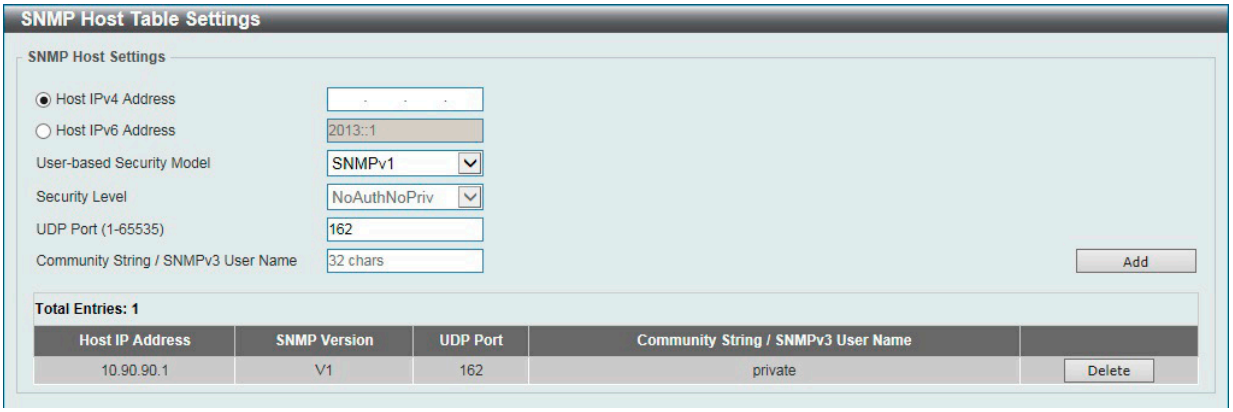


図 7-16　SNMP Host Table Settings 画面

画面に表示される項目：

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	SNMP バージョンを選択します。 • 「SNMPV1」- SNMP バージョン 1 を使用します。 • 「SNMPV2c」- SNMP バージョン 2c を使用します。 • 「SNMPV3」- SNMP バージョン 3 を使用します。
Security Level	「SNMPv3」を選択した場合、セキュリティレベルを設定します。 • 「NoAuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証も暗号化も行われません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証は行われますが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ついて、認証 / 暗号化が行われます。
UDP Port	UDP ポート番号を入力します。ポート番号によっては他のプロトコルと競合する可能性があります。 • 設定可能範囲：1-65535 • 初期値：162
Community String / SNMPv3 User Name	コミュニティ名または SNMP V3 ユーザ名を入力します。

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

RMON（RMON 設定）

スイッチの SNMP 機能に対する上昇 / 下降しきい値トラップのリモートモニタリング (RMON) ステータスを有効または無効にします。

RMON Global Settings（RMON グローバル設定）

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

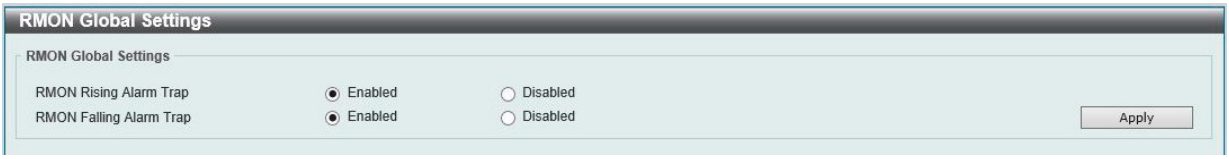


図 7-17　RMON Global Settings 画面

画面に表示される項目：

項目	説明
RMON Rising Alarm Trap	「RMON Rising Alarm Trap」を有効 / 無効に設定します。
RMON Falling Alarm Trap	「RMON Falling Alarm Trap」を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

RMON Statistics Settings（RMON 統計情報）

RMON 統計情報を表示、設定します。

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

図 7-18　RMON Statistics Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポートを指定します。
Index	RMON テーブルインデックスを入力します。 • 設定可能範囲：1-65535
Owner	オーナの文字列を入力します。（127 文字以内）

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Show Detail」ボタンをクリックして、特定のポートの詳細情報を表示します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

指定ポートの統計情報を表示する場合

「Show Detail」をクリックすると、以下の画面が表示されます。

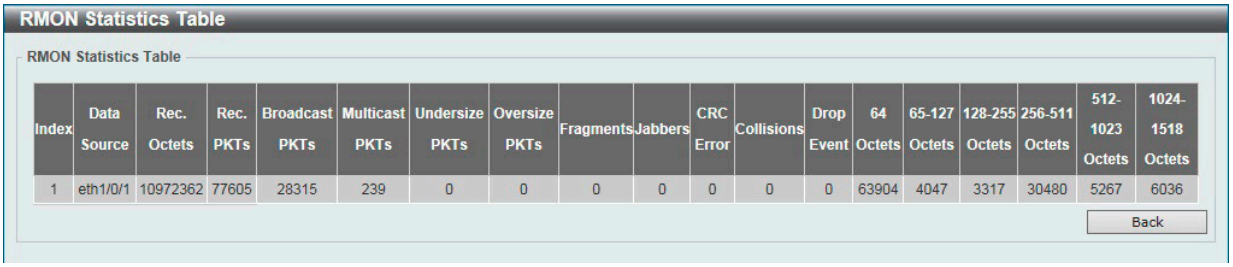


図 7-19　RMON Statistics Settings（Show Detail）- RMON Statistics Table 画面

前の画面に戻るには、「Back」ボタンをクリックします。

RMON History Settings（RMON ヒストリ設定）

ポートで収集された RMON MIB のヒストリ（履歴）統計を表示、設定します。

Management > RMON > RMON History 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。

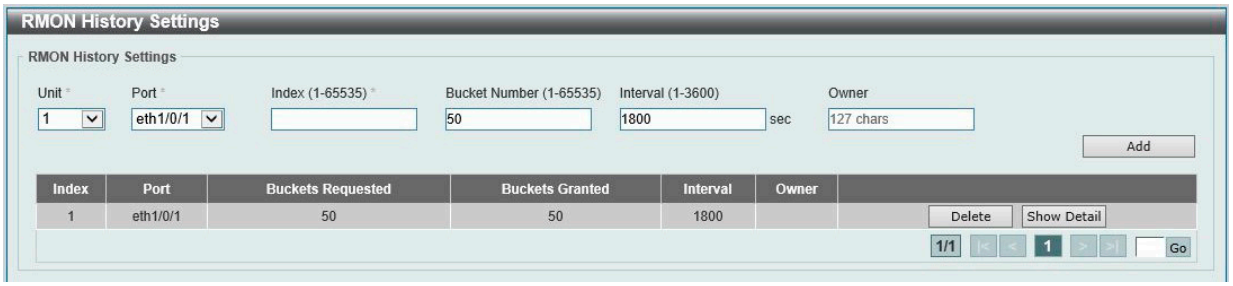


図 7-20　RMON History Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポートを指定します。
Index	ヒストリグループテーブルのインデックス番号を指定します。 • 設定可能範囲：1-65535
Bucket Number	統計における RMON 収集ヒストリグループのバケット数を指定します。 • 設定可能範囲：1-65535 • 初期値：50
Interval	ポーリング間隔を設定します。 • 設定可能範囲：1-3600（秒）
Owner	オーナの文字列を入力します。（127 文字以内）

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Show Detail」ボタンをクリックして、特定のポートの詳細情報を表示します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

指定ポートの履歴情報を表示する場合

「Show Detail」をクリックすると、以下の画面が表示されます。

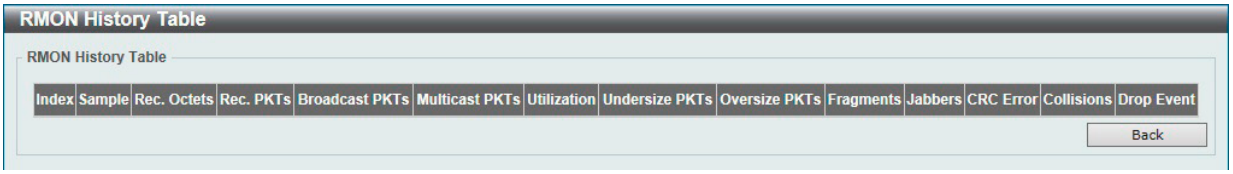


図 7-21　RMON History Settings（Show Detail）- RMON History Table 画面

前の画面に戻るには、「Back」ボタンをクリックします。

RMON Alarm Settings（RMON アラーム設定）

RMON のアラームを設定します。

Management > RMON > RMON Alarm 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。

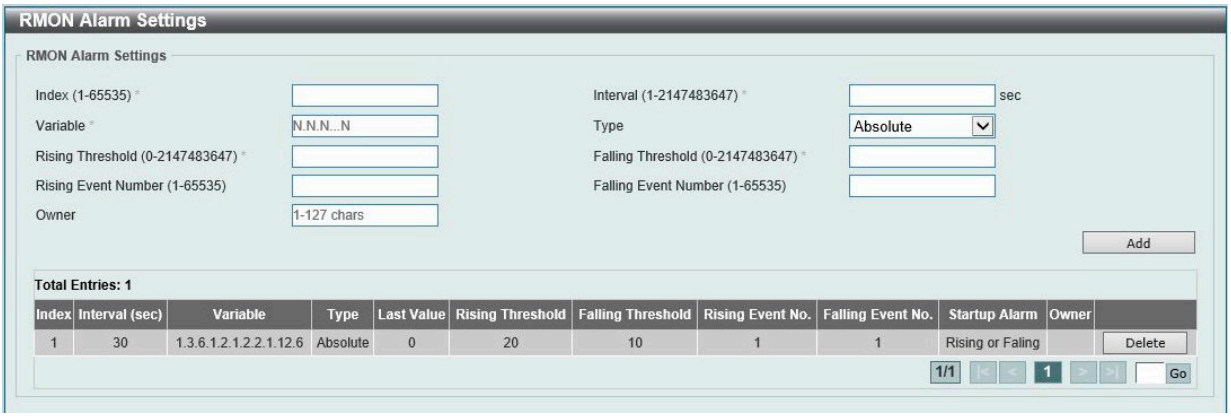


図 7-22　RMON Alarm Settings 画面

画面に表示される項目：

項目	説明
Index	アラームのインデックス番号を指定します。 • 設定可能範囲：1-65535
Interval	変数のサンプリングおよびしきい値に対するチェックの間隔を定義します。 • 設定可能範囲：1-2147483647（秒）
Variable	サンプリング対象の MIB 変数の値を指定します。
Type	監視タイプを選択します。 •「Delta」- 2 つの連続したサンプル値の差分がしきい値と比較されます。 •「Absolute」- サンプリング値がしきい値と直接比較されます。
Rising Threshold	上昇しきい値を設定します。 • 設定可能範囲：0-2147483647
Falling Threshold	下降しきい値を設定します。 • 設定可能範囲：0-2147483647
Rising Event Number	上昇しきい値を超えたときに開始するイベントのインデックス番号を指定します。 • 設定可能範囲：1-65535 指定しない場合、しきい値を超えてもアクションは実行されません。
Falling Event Number	下降しきい値を超えたときに開始するイベントのインデックス番号を指定します。 • 設定可能範囲：1-65535 指定しない場合、しきい値を超えてもアクションは実行されません。
Owner	オーナの文字列を入力します。（127 文字以内）

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

RMON Event Settings（RMON イベント設定）

RMON イベントエントリの設定を行います。

Management > RMON > RMON Event 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。

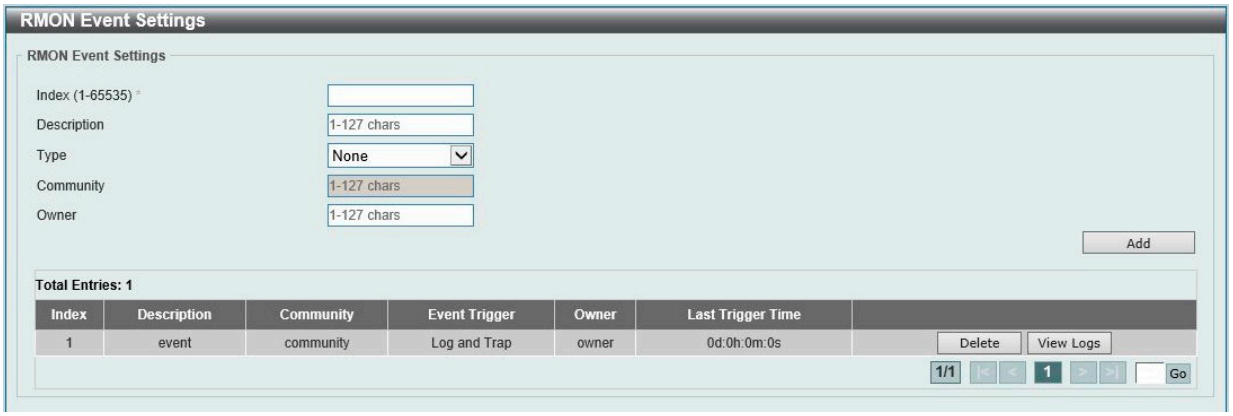


図 7-23　RMON Event Settings 画面

画面に表示される項目：

項目	説明
Index	アラームエントリのインデックス番号を指定します。 • 設定可能範囲：1-65535
Description	RMON イベントエントリの説明を入力します。（127 文字以内）
Type	イベントの種類を指定します。 • 「None」- イベントは発生しません。 • 「Log」- ログを出力します。 • 「Trap」- トラップを送信します。 • 「Log and Trap」- ログを出力し、トラップを送信します。
Community	コミュニティ文字列を指定します。（127 文字以内）
Owner	オーナの文字列を入力します。（127 文字以内）

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「View Logs」ボタンをクリックして、特定のポートの詳細情報を表示します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

指定エントリのログ情報を表示する場合

「View Logs」をクリックすると、以下の画面が表示されます。

図 7-24　RMON Event Settings（View Logs）- Event Logs Table 画面

前の画面に戻るには、「Back」ボタンをクリックします。

Telnet/Web（Telnet/Web 設定）

スイッチの Telnet/Web 設定を行います。

Management > Telnet/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 7-25　Telnet/Web 画面

画面に表示される項目：

項目	説明
Telnet Settings	
Telnet State	Telnet サーバ機能を有効 / 無効に設定します。
Port	スイッチの Telnet 管理に使用する TCP ポート番号を入力します。Telnet プロトコルに通常使用される TCP ポートは 23 です。 • 設定可能範囲：1-65535
Web Settings	
Web State	Web ベース管理を有効 / 無効に設定します。
Port	スイッチの Web ベース管理に使用される TCP ポート番号を入力します。Web 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て、設定内容を適用します。

Session Timeout（セッションタイムアウト）

各セッション（Web やコンソールなど）のタイムアウトの設定をします。

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。

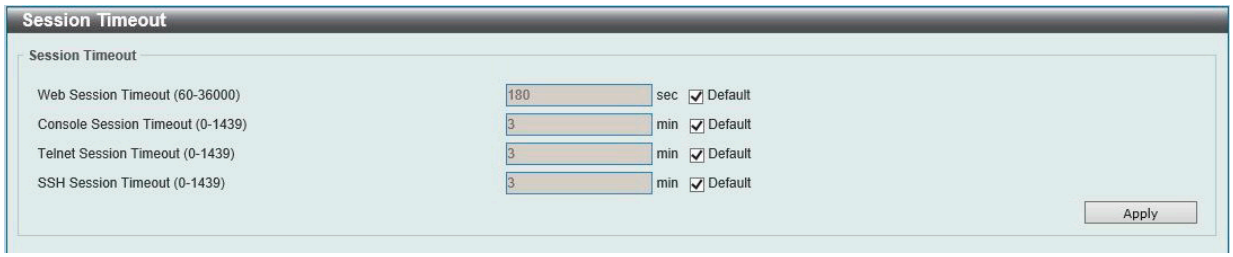


図 7-26　Session Timeout 画面

画面に表示される項目：

項目	説明
Web Session Timeout	Web セッションのタイムアウト時間を設定します。 • 設定可能範囲：60-36000（秒） • 初期値：180（秒） 「Default」にチェックを入れると初期値を使用します。
Console Session Timeout	コンソールセッションのタイムアウト時間を設定します。 • 設定可能範囲：0-1439（分） • 初期値：3（分） 「Default」にチェックを入れると初期値を使用します。0 に指定するとタイムアウトしません。
Telnet Session Timeout	Telnet セッションのタイムアウト時間を設定します。 • 設定可能範囲：0-1439（分） • 初期値：3（分） 「Default」にチェックを入れると初期値を使用します。0 に指定するとタイムアウトしません。

項目	説明
SSH Session Timeout	SSH セッションのタイムアウト時間を設定します。 • 設定可能範囲：0-1439（分） • 初期値：3（分） 「Default」にチェックを入れると初期値を使用します。0 に指定するとタイムアウトしません。

「Apply」ボタンをクリックして、設定内容を適用します。

DHCP（DHCP 設定）

スイッチの DHCP 機能に関する設定を行います。

Service DHCP（DHCP サービス）

スイッチの DHCP サービスについて設定します。

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

図 7-27　Service DHCP 画面

画面に表示される項目：

項目	説明
Service DHCP	
Service DHCP State	DHCP サービスを有効 / 無効に設定します。
Service IPv6 DHCP	
Service IPv6 DHCP State	IPv6 DHCP サービスを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

DHCP Class Settings（DHCP クラス設定）

DHCP クラスと、クラスに対する DHCP オプションのマッチングパターンについて表示、設定します。

Management > DHCP > DHCP Class 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 7-28　DHCP Class Settings 画面

画面に表示される項目：

項目	説明
Class Name	DHCP クラス名を指定します。（32 文字以内）

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

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

指定エントリの編集を行う場合

「DHCP Class Settings」画面で DHCP クラスエントリの「Edit」をクリックします。以下の画面が表示されます。

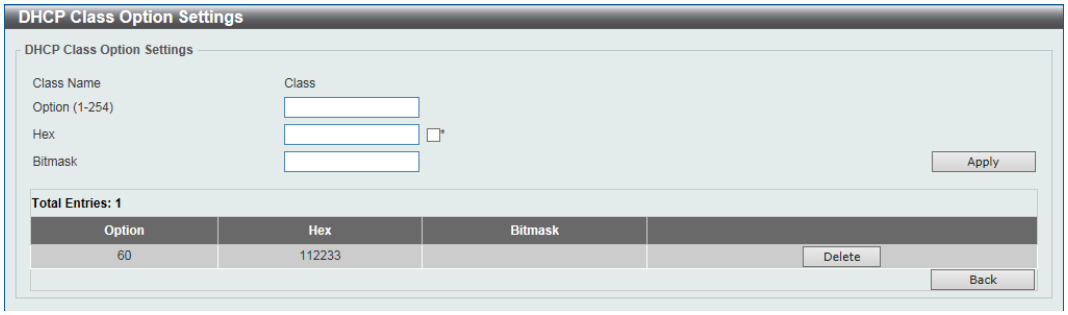


図 7-29　DHCP Class Settings（Edit）- DHCP Class Option Settings 画面

画面に表示される項目：

項目	説明
Option	DHCP オプション番号を指定します。 • 設定可能範囲：1-254
Hex	指定した DHCP オプションの 16 進数方式を入力します。 「*」にチェックを入れると残りのオプションのビットは照合されません。
Bitmask	16 進数ビットマスクを入力します。 マスクされたパターンのビットが照合されます。指定しない場合、16 進数のすべてのビットがチェックされます。

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

前の画面に戻るには、「Back」ボタンをクリックします。

DHCP Pool Settings（DHCP プール設定）

DHCP プールの設定を行います。

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

図 7-30　DHCP Pool Settings 画面

画面に表示される項目：

項目	説明
DHCP Pool Name	DHCP プール名を指定します。（32 文字以内）

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

エントリの検索・表示

「Find」ボタンをクリックして、指定のエントリを検索します。
「Show All」ボタンをクリックして、テーブル上のすべての DHCP プールを表示します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

DHCP Server（DHCP サーバ）

Management > DHCP > DHCP Server

DHCP（Dynamic Host Configuration Protocol）を使用すると、IP アドレス、サブネットマスク、デフォルトゲートウェイ、および他の IP パラメータについて、これらの情報を要求するデバイスに発行することができます。この処理は、DHCP が有効化されたデバイスが起動またはローカルなネットワークに接続された際に実行されます。ネットワーク情報を受信するデバイスは DHCP クライアントと呼ばれ、DHCP クライアントステータスが有効な場合、IP パラメータが設定される前にネットワークにクエリメッセージを送信します。DHCP サーバがこのリクエストを受信すると、クライアントに対して IP アドレスを割り当てます。その後、DHCP クライアントは割り当てられた IP アドレスをローカル構成として使用します。

自動 IP 設定が適用されるクライアントに対して、ローカル接続ネットワークで利用するための DHCP に関連する多くのパラメータ（割り当て IP アドレスのリース時間、DHCP プールで許可される IP アドレス範囲、除外 IP アドレス）を設定することができます。また、DNS サーバやデフォルトルートの IP アドレスなど重要なデバイスに対して IP アドレスを設定することもできます。

さらに、DHCP プール内の IP アドレスを特定の MAC アドレスに割り当てることで、重要なデバイスの IP アドレスを固定することができます。

注意　DHCP サーバ機能の設定変更を行った際は、設定変更後に必ず DHCP サーバサービスの再起動を行ってください。

注意　スタック構成において、DHCP/DHCPv6 サーバの機能をご利用の場合、スタックマスタの交代に伴い、リース情報（バインディング情報など）の状態の保持、同期は行われません。

DHCP Server Global Settings（DHCP サーバグローバル設定）

DHCP サーバのグローバル設定を行います。

Management > DHCP > DHCP Server > DHCP Server 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。

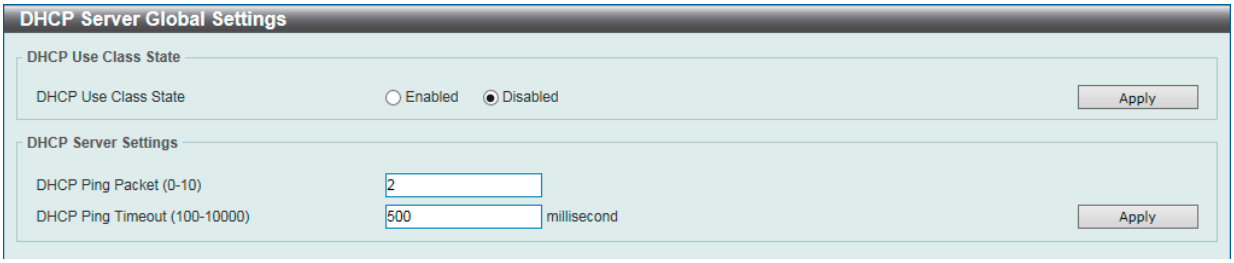


図 7-31　DHCP Server Global Settings 画面

画面に表示される項目：

項目	説明
DHCP Use Class State	
DHCP Use Class State	DHCP Use Class ステータスを有効 / 無効に設定します。有効にした場合、DHCP サーバはアドレス割り当てに DHCP クラスを使用します。
DHCP Server Settings	
DHCP Ping Packets	割り当てる IP アドレスを含むネットワークにスイッチが送信する Ping パケットの数を指定します。Ping リクエストが返ってこない場合、その IP アドレスはローカルネットワークに対して固有であると見なされ、要求側クライアントに割り当てられます。0 は Ping テストを行わないことを意味します。 • 設定可能範囲：0-10（パケット） • 初期値：2（パケット）
DHCP Ping Timeout	Ping パケットがタイムアウトになるまでの DHCP サーバの待機時間を指定します。 • 設定可能範囲：100-10000（ミリ秒） • 初期値：500（ミリ秒）

「Apply」ボタンをクリックして、各セクションで行った変更を適用します。

DHCP Server Pool Settings（DHCP サーバプール設定）

DHCP サーバプールの設定を行います。

Management > DHCP > DHCP Server > DHCP Server Pool 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 7-32　DHCP Server Pool Settings 画面

画面に表示される項目：

項目	説明
DHCP Pool Name	DHCP サーバプール名を入力します。（32 文字以内）

「Find」ボタンをクリックして、指定のエントリを検索します。
「Show All」ボタンをクリックして、テーブル上のすべての DHCP プールを表示します。
作成されたプールは、「Edit Class」「Edit Option」「Configure」ボタンをクリックして、設定内容を編集することができます。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

エントリの編集（Edit Class）

「DHCP Server Pool Settings」画面で DHCP サーバプールエントリの「Edit Class」ボタンをクリックすると、以下の画面が表示されます。

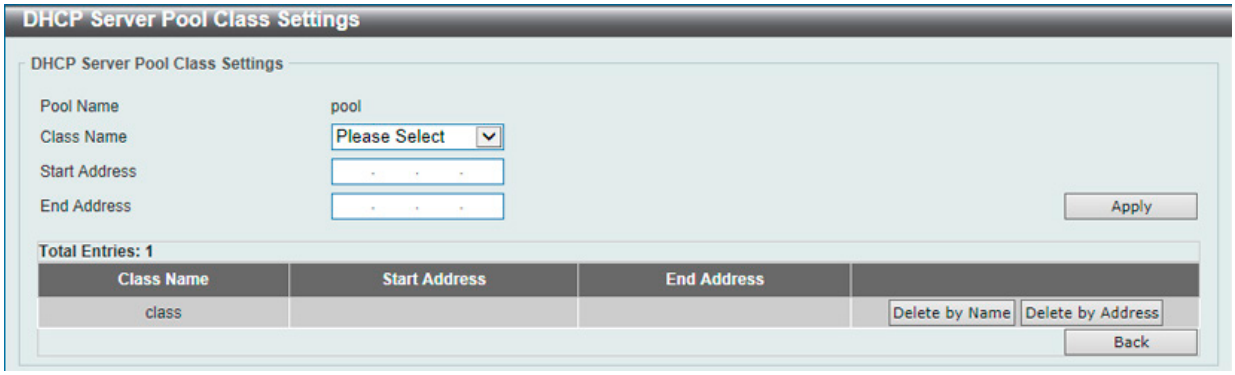


図 7-33　DHCP Server Pool Settings（Edit Class）- DHCP Server Pool Class Settings 画面

画面に表示される項目：

項目	説明
Pool Name	編集する DHCP プール名が表示されます。
Class Name	DHCP プールに紐づける DHCP クラス名を指定します。
Start Address	DHCP クラスに紐づける開始 IPv4 アドレスを指定します。
End Address	DHCP クラスに紐づける終了 IPv4 アドレスを指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete by Name」ボタンをクリックして、DHCP クラスの割り当てを削除します。
「Delete by Address」ボタンをクリックして、アドレスの割り当てを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

エントリの編集（Edit Option）

「DHCP Server Pool Settings」画面で DHCP サーバプールエントリの「Edit Option」ボタンをクリックすると、以下の画面が表示されます。

図 7-34　DHCP Server Pool Settings（Edit Option）- DHCP Server Pool Option Settings 画面

画面に表示される項目：

項目	説明
Pool Name	編集する DHCP プール名が表示されます。
Option	DHCP オプション番号を指定します。 • 設定可能範囲：1-254
Type	DHCP オプションタイプを「ASCII」「Hex」「IP」から選択し、値を入力します。 • 「ASCII」- ASCII 文字列で入力します。（255 文字以内） • 「HEX」- 16 進数文字列で入力します。（254 文字以内） • 「IP」- IPv4 アドレスを入力します。最大 8 個のアドレスを入力することが可能です。 「Hex」を選択した場合に、長さ 0 の Hex 文字列を指定する場合は、「None」オプションにチェックを入れます。

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

前の画面に戻るには、「Back」ボタンをクリックします。

エントリの編集（Configure）

「DHCP Server Pool Settings」画面で DHCP サーバプールエントリの「Configure」ボタンをクリックすると、以下の画面が表示されます。

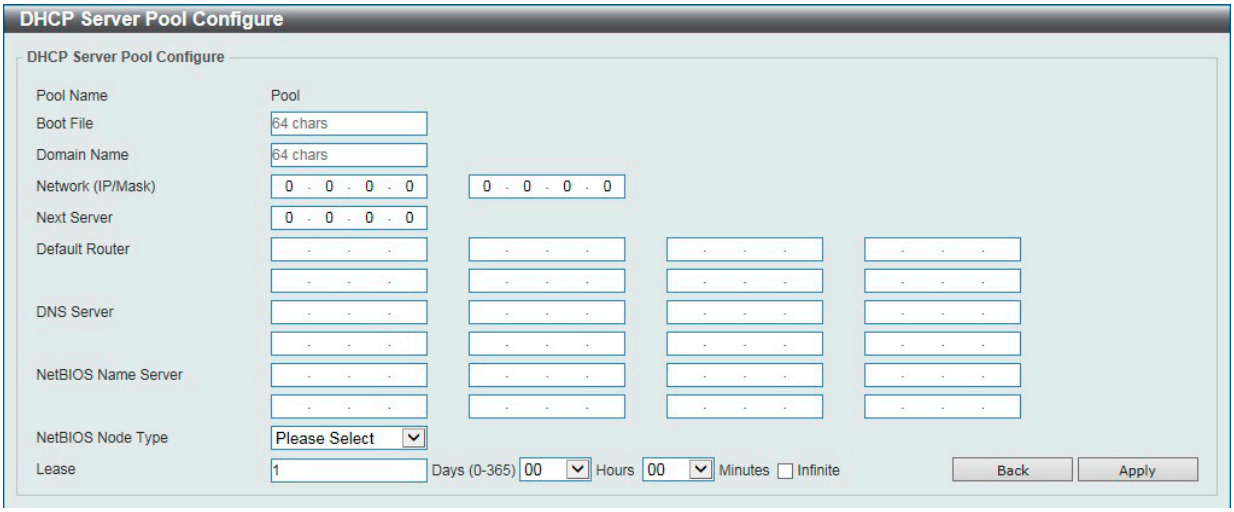


図 7-35　DHCP Server Pool Settings（Configure) - DHCP Server Pool Configure 画面

画面に表示される項目：

項目	説明
Pool Name	編集する DHCP プール名が表示されます。
Boot File	ブートイメージのファイル名を指定します。（64 文字以内）
Domain Name	クライアントのドメイン名を入力します。（64 文字以内）
Network (IP/Mask)	DHCP プールのネットワークアドレスとサブネットマスクを入力します。
Next Server	ネクストサーバの IP アドレスを指定します。このサーバに格納されているブートイメージファイルが DHCP クライアントによって検索されます。一般的に TFTP サーバが使用されます。ネクストサーバの IP アドレスは 1 つのみ指定できます。

項目	説明
Default Router	DHCP クライアントのデフォルトルータの IP アドレスを入力します。 ここでは最大 8 つの IP アドレスを指定できます。このルータの IP アドレスはクライアントのサブネットと同じサブネットである必要があります。ルータは優先度の高い順に並んでいます。デフォルトルータが既に設定済みの場合、後から設定されたデフォルトルータはデフォルトルータリストに追加されます。
DNS Server	DHCP クライアントが使用する DNS サーバの IP アドレスを入力します。 ここでは最大 8 つの IP アドレスを指定できます。DNS サーバは優先度の高い順に並んでいます。DNS サーバが既に設定済みの場合、後から設定された DNS サーバは DNS サーバリストに追加されます。
NetBIOS Name Server	DHCP クライアントが使用する WINS サーバの IP アドレスを指定します。 ここでは最大 8 つの IP アドレスを指定できます。サーバは優先度の高い順に並んでいます。ネームサーバが既に設定済みの場合、後から設定されたネームサーバはネームサーバリストに追加されます。
NetBIOS Node Type	マイクロソフト DHCP クライアントの NetBIOS ノードタイプを指定します。このオプションでは、NetBIOS において登録および名前解決に使用する方法を選択します。 • 「Broadcast」- システムはブロードキャストを使用します。 • 「Peer-to-Peer」（p-node）- ネームサーバ（WINS）に対して Peer to Peer による名前クエリのみを使用します。 • 「Mixed」（m-node）- まずブロードキャストを使用し、その後ネームサーバへの問い合わせを行います。 • 「Hybrid」（h-node）- まずネームサーバへの問い合せを行い、その後ブロードキャストを使用します。 「Hybrid」を使用することを推奨します。
Lease	アドレスプールから割り当てるアドレスのリース期間を指定します。 • 「Days」- リースする日数（0-365） • 「Hours」- リースする時間（時） • 「Minutes」- リースする時間（分） • 「Infinite」- リース期間が無制限

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

DHCP Server Exclude Address（DHCP サーバ除外アドレス）

DHCP サーバがクライアントへの IP 割り当てを行う際に除外する IP アドレスを指定します。
DHCP サーバは自動的に DHCP アドレスプールから DHCP クライアントに IP アドレスを割り当てますが、ルータのインタフェース IP アドレスと除外リストのアドレス以外が割り当て範囲となります。複数の IP アドレス範囲を指定することができます。

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

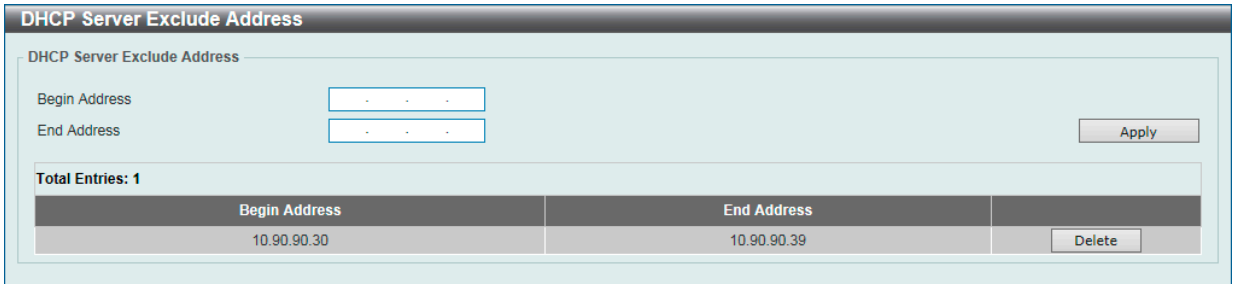


図 7-36　DHCP Server Exclude Address 画面

画面に表示される項目：

項目	説明
Begin Address	除外する IP アドレス範囲の開始 IP アドレスを指定します。
End Address	除外する IP アドレス範囲の終了 IP アドレスを指定します。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

DHCP Server Manual Binding（DHCP サーバマニュアルバインディング）

DHCP サーバの手動バインディング設定を行います。
IP アドレスとクライアント識別子や、IP アドレスと MAC アドレスの組み合わせで固定の割り当てを設定することができます。

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

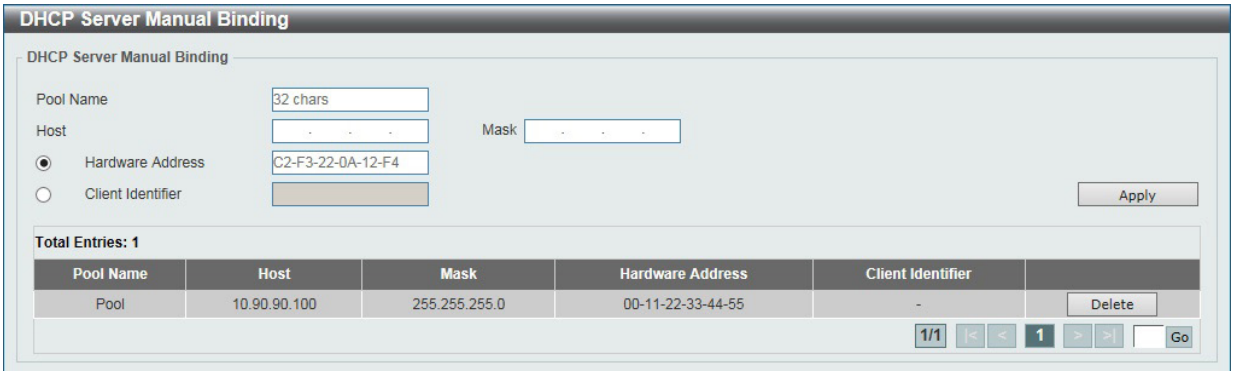


図 7-37　DHCP Server Manual Binding 画面

画面に表示される項目：

項目	説明
Pool Name	DHCP サーバプール名を入力します。（32 文字以内）
Host	DHCP ホストの IPv4 アドレスを入力します。
Mask	DHCP ホストのネットワークのサブネットマスクを入力します。
Hardware Address	DHCP ホストの MAC アドレスを入力します。
Client Identifier	DHCP ホスト識別子を 16 進数表記で指定します。 クライアント識別子はメディアタイプと MAC アドレスによって構成されています。

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

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

DHCP Server Dynamic Binding（DHCP サーバダイナミックバインディング）

DHCP サーバダイナミックバインディングテーブルの表示とエントリの削除を行います。

Management > DHCP > DHCP Server > DHCP Server Dynamic Binding 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　DHCP Server Dynamic Binding 画面

画面に表示される項目：

項目	説明
IP Address	バインディングエントリの IPv4 アドレスを入力します。
Pool Name	DHCP サーバプール名を入力します。（32 文字以内） 「All」オプションにチェックを入れると、全てのプールのバインディングエントリを削除します。
Binding IP Address	バインディング 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エントリを検出します。
「Clear」ボタンをクリックして、入力した情報に基づくエントリをクリアします。

DHCP Server IP Conflict（DHCP サーバ IP 重複）

DHCP サーバデータベースの DHCP 重複エントリを表示、クリアします。

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

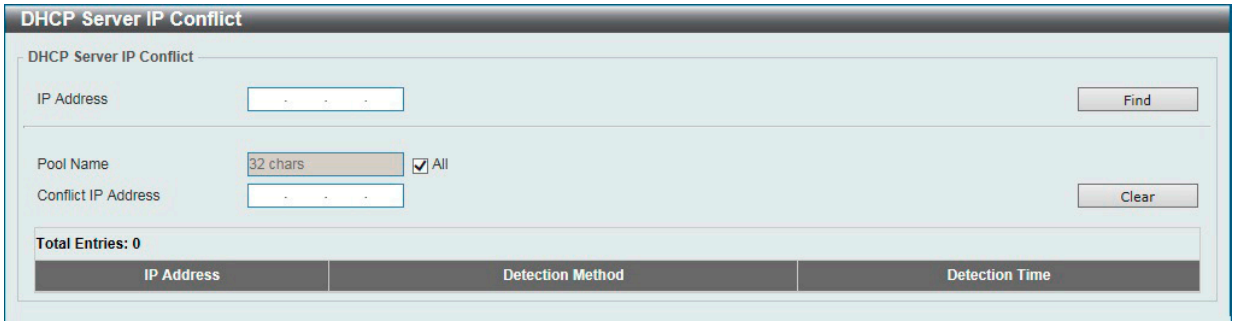


図 7-39　DHCP Server IP Conflict 画面

画面に表示される項目：

項目	説明
IP Address	検出する重複エントリの IPv4 アドレスを入力します。
Pool Name	DHCP サーバプール名を入力します。（32 文字以内） 「All」オプションにチェックを入れると、全てのプールの重複エントリを削除します。
Conflict IP Address	クリアする重複エントリの IPv4 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エントリを検出します。
「Clear」ボタンをクリックして、入力した情報に基づくエントリをクリアします。

DHCP Server Statistics（DHCP サーバ統計）

DHCP サーバの統計情報を表示します。

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

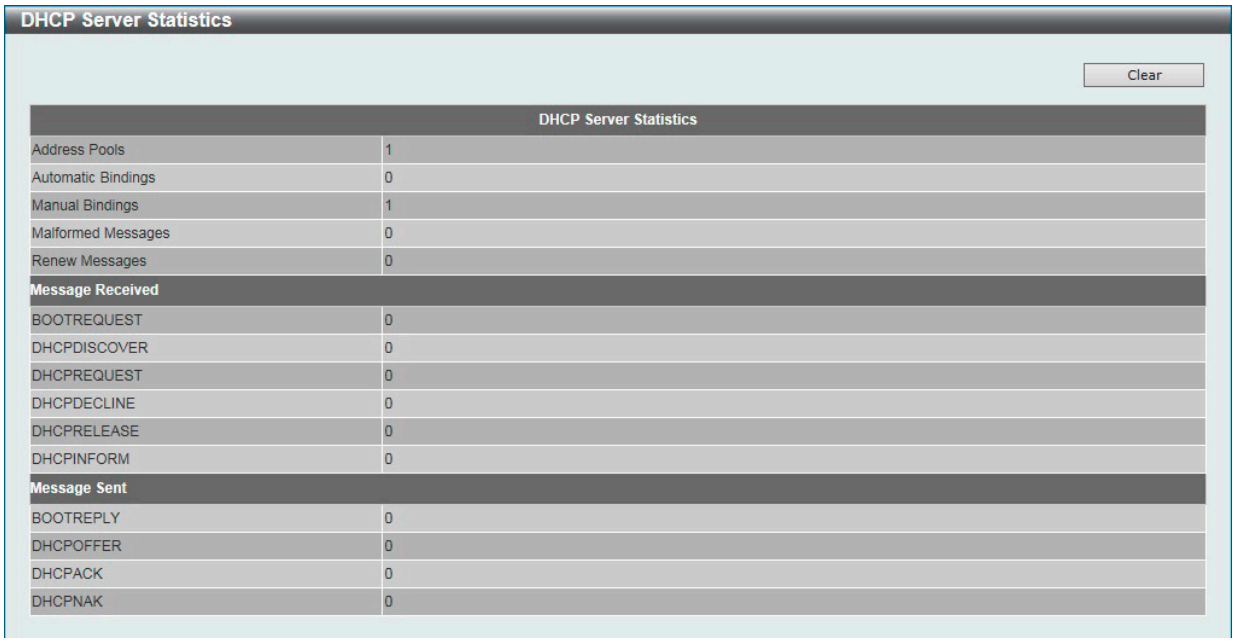


図 7-40　DHCP Server Statistics 画面

「Clear」ボタンをクリックして、統計情報をクリアします。

DHCPv6 Server（DHCPv6 サーバ設定）

Management > DHCP > DHCPv6 Server

注意 DHCPv6 サーバでは、接続済の IPv6 プリフィクス以外へのリースは機能しません。

注意 スタック構成において、DHCP/DHCPv6 サーバの機能をご利用の場合、スタックマスタの交代に伴い、リース情報（バインディング情報など）の状態の保持、同期は行われません。

DHCPv6 Server Pool Settings（DHCP サーバプール設定）

DHCPv6 プールの作成および設定を行います。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Pool 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 7-41　DHCPv6 Server Pool Settings 画面

画面に表示される項目：

項目	説明
Pool Name	DHCPv6 サーバプール名を入力します。（12 文字以内）

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Configure」ボタンをクリックして、該当エントリの編集を行います。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

エントリの編集（Configure）

「DHCPv6 Server Pool Settings 」画面で DHCPv6 サーバプールエントリの「Configure」ボタンをクリックすると、以下の画面が表示されます。

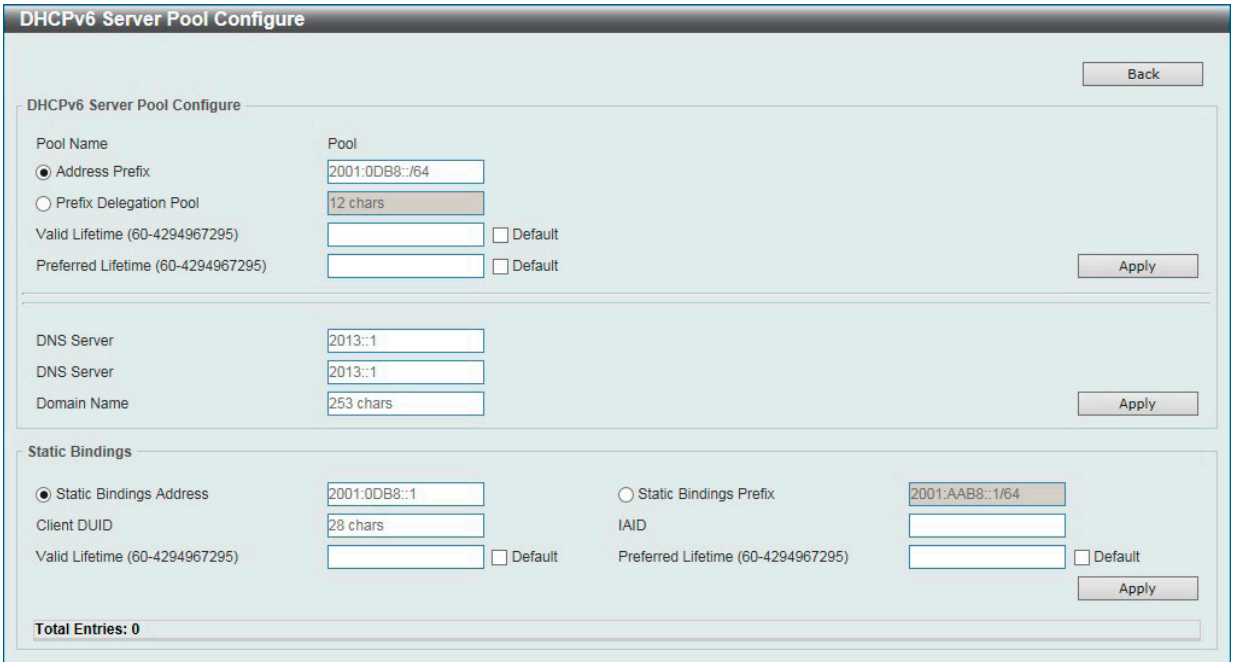


図 7-42　DHCPv6 Server Pool Settings (Configure) - DHCPv6 Server Pool Configure 画面

画面に表示される項目：

項目	説明
DHCPv6 Server Pool Configure	
Address Prefix	DHCPv6 サーバプールの IPv6 ネットワークアドレスとプレフィックス長を入力します。（例：2015::0/64）

項目	説明
Prefix Delegation Pool	DHCPv6 サーバプールのプレフィックス委任名を入力します。（12 文字以内）
Valid Lifetime	IPv6 アドレスが有効な状態を維持する時間を入力します。「Preferred Lifetime」よりも大きい値である必要があります。 • 設定可能範囲：60-4294967295（秒） • 初期値：2592000（秒）（30 日） 「Default」にチェックを入れると、初期値が使用されます。
Preferred Lifetime	preferred-lifetime（推奨有効期限）を入力します。 • 設定可能範囲：60-4294967295（秒） • 初期値は 604800（秒）（7 日） 「Default」にチェックを入れると、初期値が使用されます。
DNS Server	DHCPv6 クライアントに割り当てる DNS サーバの IPv6 アドレスを入力します。2 台の DNS サーバまで設定できます。
Domain Name	DHCPv6 クライアントに割り当てるドメイン名を指定します。
Static Bindings	
Static Bindings Address	指定クライアントに割り当てるスタティックバインディング IPv6 アドレスを入力します。
Static Bindings Prefix	スタティックバインディング IPv6 ネットワークアドレスとプレフィックスを入力します。
Client DUID	デバイスの DHCP 固有識別子（DUID）を入力します。（28 文字以内）
IAID	「Identity Association Identifier」(IAID/IA 識別子) を入力します。 これは、クライアントに割り当てられる一時的ではないアドレス（IANA）の集合体を識別します。
Valid Lifetime	IPv6 アドレスが有効な状態を維持する時間を入力します。「Preferred Lifetime」よりも大きい値である必要があります。 • 設定可能範囲：60-4294967295（秒） • 初期値：2592000（秒）（30 日） 「Default」にチェックを入れると、初期値が使用されます。
Preferred Lifetime	preferred-lifetime（推奨有効期限）を入力します。 • 設定可能範囲：60-4294967295（秒） • 初期値：604800（秒）（7 日） 「Default」にチェックを入れると、初期値が使用されます。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

DHCPv6 Server Local Pool Settings（DHCPv6 サーバローカルプール設定）

DHCPv6 サーバローカルプールの表示および設定を行います。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Local Pool 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。

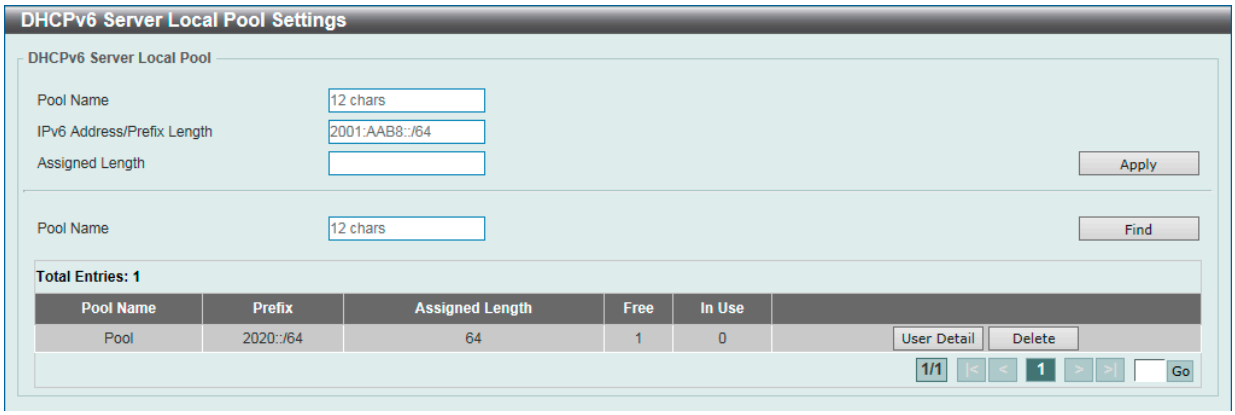


図 7-43　DHCPv6 Server Local Pool Settings 画面

画面に表示される項目：

項目	説明
Pool Name	DHCPv6 サーバプール名を入力します。（12 文字以内）
IPv6 Address / Prefix Length	ローカルプールの IPv6 プレフィックスアドレスとプレフィックス長を入力します。
Assigned Length	プール内からユーザに委任されるプレフィックス長を入力します。「Assigned Length」の値はプレフィックス長の値より長い必要があります。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「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。
「User Detail」ボタンをクリックすると、ユーザについての詳細が画面下部に表示されます。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

「User Detail」ボタンをクリックすると、画面下部に以下のように情報が表示されます。

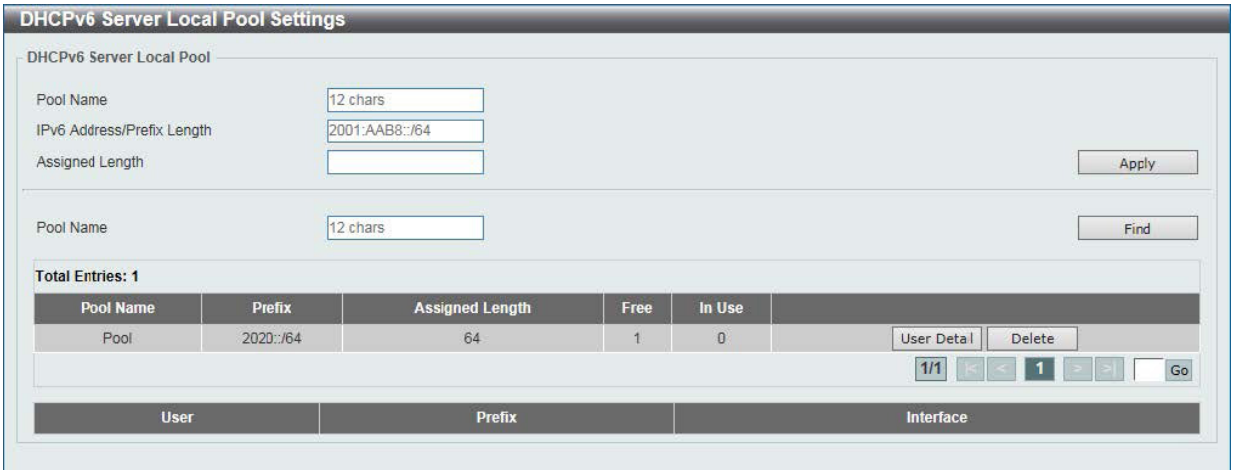


図 7-44　DHCPv6 Server Local Pool Settings（User Detail）画面

DHCPv6 Server Exclude Address（DHCPv6 サーバ除外アドレス）

DHCPv6 クライアントへの割り当てから除外する IPv6 アドレスの範囲を設定します。DHCPv6 サーバは全てのアドレス（スイッチ自身の IPv6 を除く）をクライアントへ割り当てることが可能です。本画面では、割り当て範囲から IPv6 アドレス / アドレス範囲を除外する設定を行うことができます。除外アドレスはアドレス割り当てプールにのみ適用されます。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Exclude Address の順にメニューをクリックし、以下の画面を表示します。

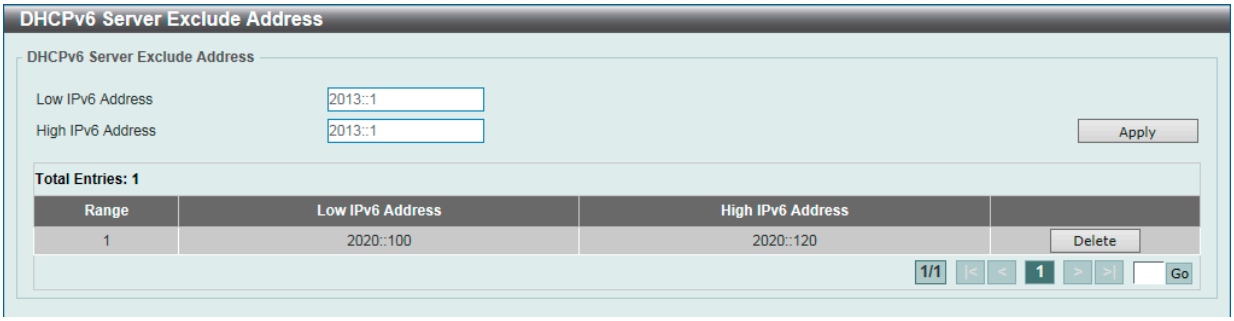


図 7-45　DHCPv6 Server Exclude Address 画面

画面に表示される項目：

項目	説明
Low IPv6 Address	除外する IPv6 アドレス（単体）、または除外 IPv6 アドレス範囲の開始 IPv6 アドレスを指定します。
High IPv6 Address	除外 IPv6 アドレス範囲の終了 IPv6 アドレスを指定します。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

DHCPv6 Server Binding（DHCPv6 サーババインディング）

DHCPv6 バインディング情報を参照、クリアします。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Binding の順にメニューをクリックし、以下の画面を表示します。

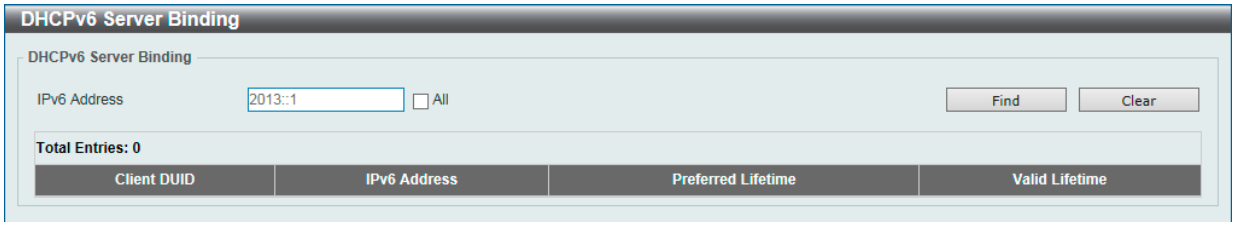


図 7-46　DHCPv6 Server Binding 画面

画面に表示される項目：

項目	説明
IPv6 Address	表示、クリアするバインディングエントリの IPv6 アドレスを入力します。 「All」を選択するとバインディングテーブルの全ての DHCPv6 クライアントプレフィックスバインディングが対象になります。

「Find」ボタンをクリックして、指定した情報に基づくエントリを検出します。
「Clear」ボタンをクリックして、指定した情報に基づくエントリをクリアします。

DHCPv6 Server Interface Settings（DHCPv6 サーバインタフェース設定）

インタフェースごとに DHCPv6 サーバ状態を表示および設定します。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Interface Settings の順にメニューをクリックし、以下の画面を表示します。

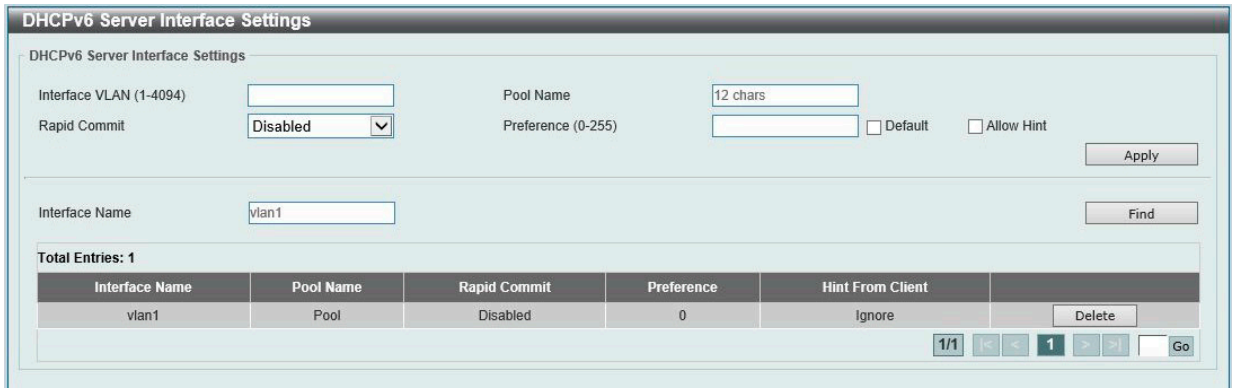


図 7-47　DHCPv6 Server Interface Settings 画面

画面に表示される項目：

項目	説明
Interface VLAN	インタフェース VLAN を指定します。 • 設定可能範囲：1-4094
Pool Name	DHCPv6 サーバプール名を入力します。（12 文字以内）
Rapid Commit	2 メッセージ交換を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
Preference	Preference 値を指定します。 - 「Default」- 本オプションにチェックを入れると、初期値が使用されます。 - 「Allow Hint」- 本オプションにチェックを入れると、ヒントを利用します。
Interface Name	インタフェース名を入力します。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づくエントリを検出します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

DHCPv6 Server Operational Information（DHCPv6 サーバ操作情報）

DHCPv6 サーバ状態を表示します。

Management > DHCP > DHCPv6 Server > DHCPv6 Server Operational Information の順にメニューをクリックし、以下の画面を表示します。

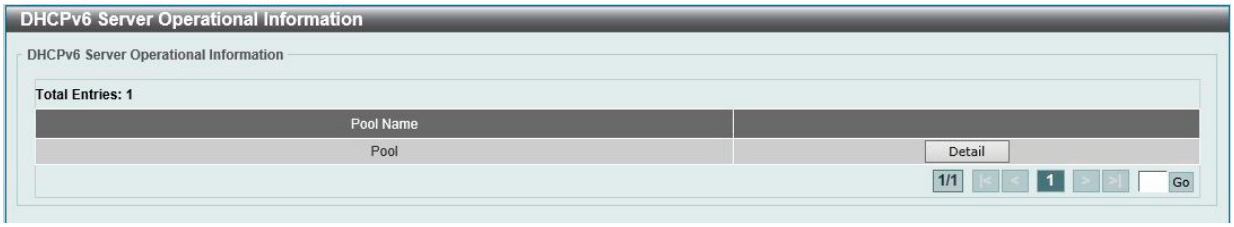


図 7-48　DHCPv6 Server Operational Information 画面

「Detail」ボタンを選択すると、以下の画面が表示されます。

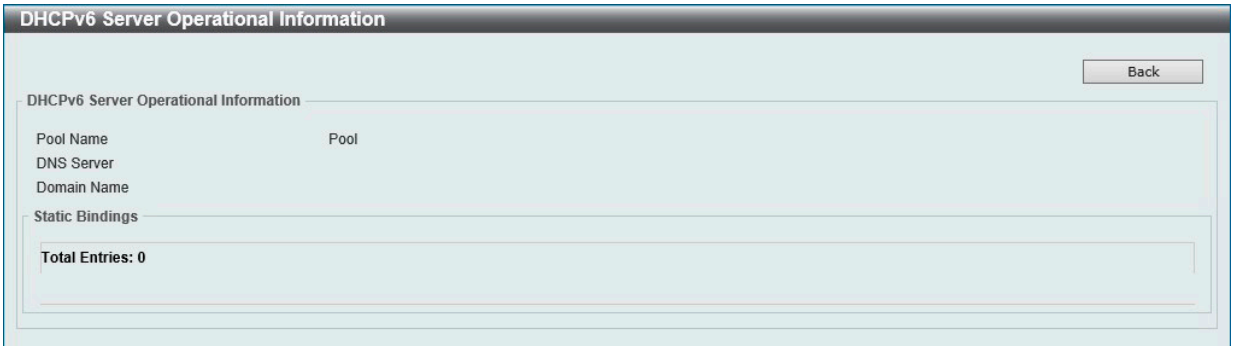


図 7-49　DHCPv6 Server Operational Information（Detail）画面

前の画面に戻るには、「Back」ボタンをクリックします。

DHCP Relay（DHCP リレー）

Management > DHCP > DHCP Relay

注意　DHCP リレーが有効の場合、Discover パケットが対象 VLAN 内にフラッディングされません。

DHCP Relay Pool Settings（DHCP リレープール設定）

DHCP リレーエージェントの DHCP リレープールの表示、設定を行います。

Management > DHCP > DHCP Relay > DHCP Relay Pool 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 7-50　DHCP Relay Pool Settings 画面

画面に表示される項目：

項目	説明
DHCP Pool Name	プール名を指定します。（32 文字以内）

「Find」ボタンをクリックして、指定した DHCP リレープールを表示します。
「Show All」ボタンをクリックして、すべての DHCP リレープールを表示します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

各プールエントリの編集を行う（Edit）

各エントリの「Source」「Destination」「Class」下にある「Edit」をクリックして、それぞれの内容を編集します。

■「Source」の編集を行う場合

「DHCP Relay Pool Settings」画面の DHCP リレープールエントリについて、「Source」欄の「Edit」をクリックすると、以下の画面が表示されます。

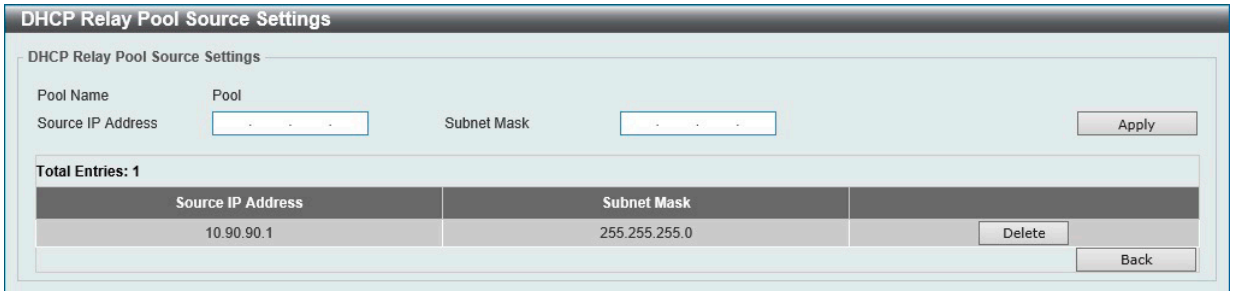


図 7-51　DHCP Relay Pool Settings（Source/Edit）- DHCP Relay Pool Source Settings 画面

画面に表示される項目：

項目	説明
Source IP Address	クライアントパケットのソースサブネットを入力します。
Subnet Mask	ソースサブネットのネットマスクを入力します。

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

前の画面に戻るには、「Back」ボタンをクリックします。

■「Destination」の編集を行う場合

「DHCP Relay Pool Settings」画面の DHCP リレープールエントリについて、「Destination」欄の「Edit」をクリックすると、以下の画面が表示されます。

図 7-52　DHCP Relay Pool Settings（Destination/Edit）- DHCP Relay Pool Destination Settings 画面

以下の項目が使用されます。

項目	説明
Relay Destination	リレー宛先 DHCP サーバの IP アドレスを入力します。

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

前の画面に戻るには、「Back」ボタンをクリックします。

■「Class」の編集を行う場合

「DHCP Relay Pool Settings」画面の DHCP リレープールエントリについて、「Class」欄の「Edit」をクリックすると、以下の画面が表示されます。

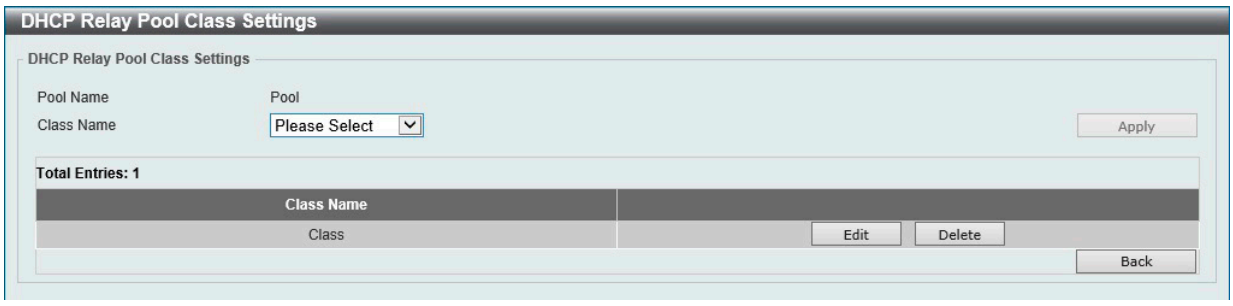


図 7-53　DHCP Relay Pool Settings（Class/Edit）- DHCP Relay Pool Class Settings 画面

画面に表示される項目：

項目	説明
Class Name	DHCP クラスの名前を選択します。

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

前の画面に戻るには、「Back」ボタンをクリックします。

クラスエントリの横の「Edit」をクリックすると、以下の画面が表示されます。

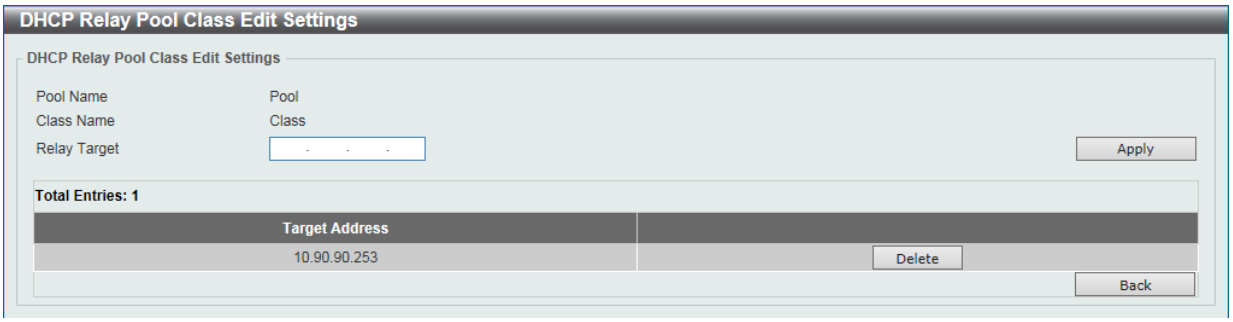


図 7-54　DHCP Relay Pool Settings（Class/Edit）- DHCP Relay Pool Class Settings（Edit）- DHCP Relay Pool Class Edit Settings 画面

画面に表示される項目：

項目	説明
Relay Target	DHCP クラスで設定したオプションの値パターンと一致するパケットをリレーする DHCP リレーターゲットを入力します。

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

前の画面に戻るには、「Back」ボタンをクリックします。

DHCP Relay Information Settings（DHCP リレーインフォメーション設定）

DHCP リレー情報の設定を行います。

Management > DHCP > DHCP Relay > DHCP Relay Information 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。

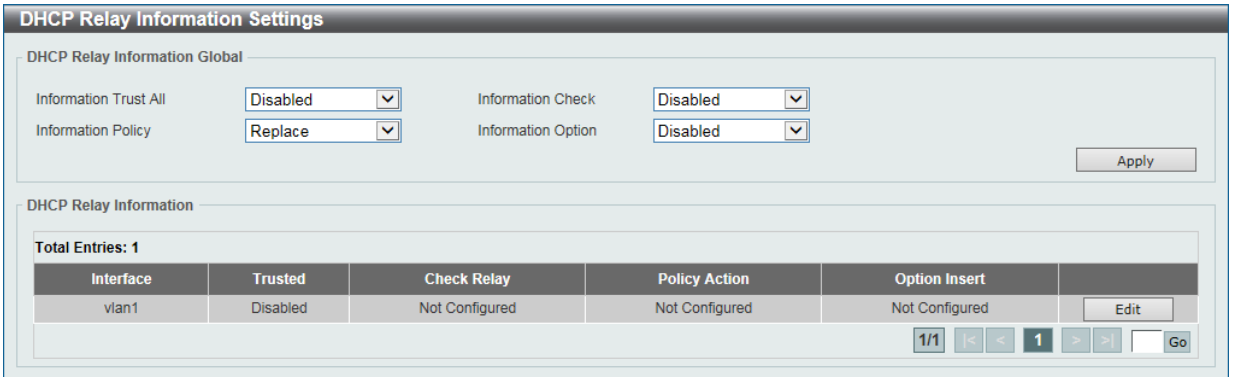


図 7-55　DHCP Relay Information Settings 画面

画面に表示される項目：

項目	説明
Information Trust All	すべてのインタフェースで DHCP リレーエージェントによる IP DHCP リレーインフォメーションへの信頼を有効 / 無効に設定します。
Information Check	DHCP リレーエージェントによる、受信した DHCP リレーパケットに含まれるリレーエージェントインフォメーションの検証と破棄を有効 / 無効に設定します。
Information Policy	DHCP リレーエージェントのオプション 82 再転送ポリシーを選択します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。 • 「Replace」- DHCP クライアントから受信したパケット内の既存のリレー情報を新しいオプションで置き換えます。
Information Option	DHCP リクエストパケットがリレーされる間のリレーエージェント情報（Option82）の挿入を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Edit」ボタンをクリックして、対応するインタフェースの設定を編集することができます。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

DHCP Relay Information Option Format Settings（DHCP リレーインフォメーションオプションフォーマット設定）

DHCP 情報フォーマットの設定を行います。

Management > DHCP > DHCP Relay > DHCP Relay Information Option Format 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。

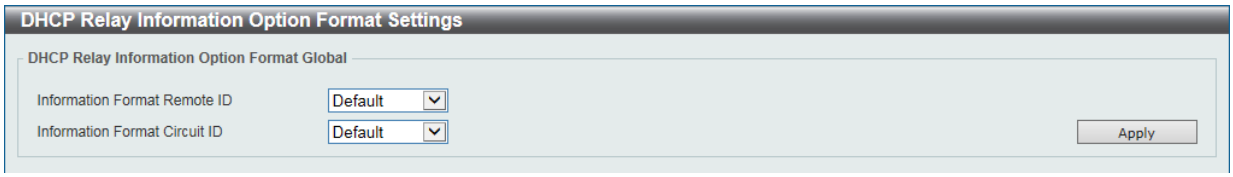


図 7-56　DHCP Relay Information Option Format Settings 画面

画面に表示される項目：

項目	説明
DHCP Relay Information Option Format Global	
Information Format Remote ID	「DHCP information remote ID」のサブオプションを選択します。 • 「Default」- リモート ID としてシステムの MAC アドレスを使用します。 • 「User Define」- ユーザ定義のリモート ID を使用します。（32 文字以内） • 「Vendor 2」- リモート ID としてベンダ 2 を使用します。
Information Format Circuit ID	「DHCP information circuit ID」のサブオプションを選択します。 • 「Default」- 初期値のサーキット ID サブオプションを使用します。 • 「User Define」- ユーザ定義のサーキット ID を使用します。（32 文字以内） • 「Vendor 1」- サーキット ID としてベンダ 1 を使用します。

「Apply」ボタンをクリックして、設定内容を適用します。

DHCP Relay Port Settings（DHCP リレーポート設定）

DHCP リレーポートの設定、表示を行います。

Management > DHCP > DHCP Relay > DHCP Relay 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。

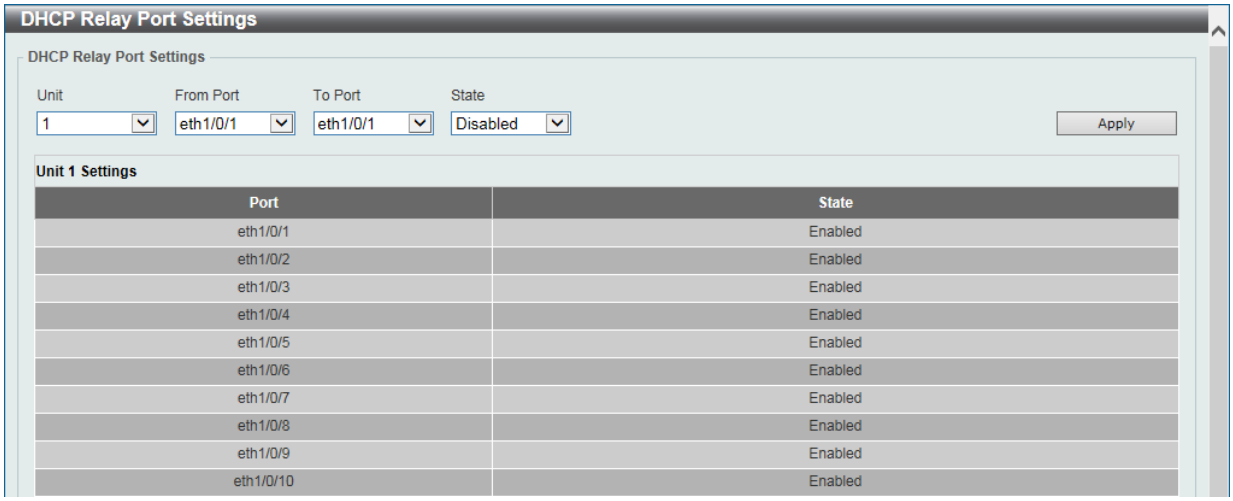


図 7-57　DHCP Relay Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定のポートの DHCP リレーを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

DHCP Local Relay VLAN（DHCP ローカルリレー VLAN）

VLAN、またはグループ VLAN のリレー設定を行います。

Management > DHCP > DHCP Relay > DHCP Local Relay 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。

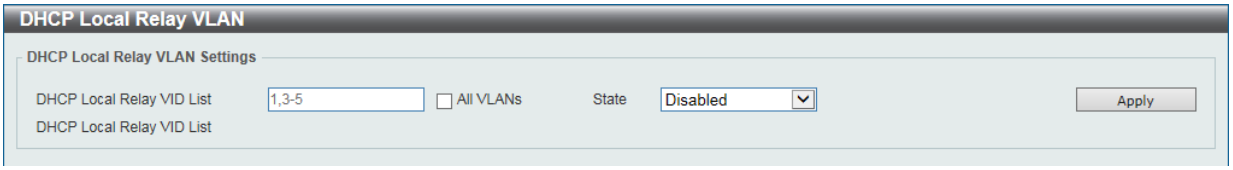


図 7-58　DHCP Local Relay VLAN 画面

画面に表示される項目：

項目	説明
DHCP Local Relay VID List	DHCPv6 ローカルリレーの VLAN ID を入力します。 「ALL VLANs」オプションを指定すると、すべての VLAN が対象になります。
State	指定 VLAN の DHCPv6 ローカルリレー機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　DHCP リレーポートが無効の場合、ポートは受信 DHCP パケットのリレー / ローカルリレーを行いません。

DHCPv6 Relay（DHCPv6 リレー）

DHCPv6 Relay Global Settings（DHCPv6 リレーグローバル設定）

スイッチの DHCPv6 リレー機能を設定します。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings の順にメニューをクリックし、以下の画面を表示します。

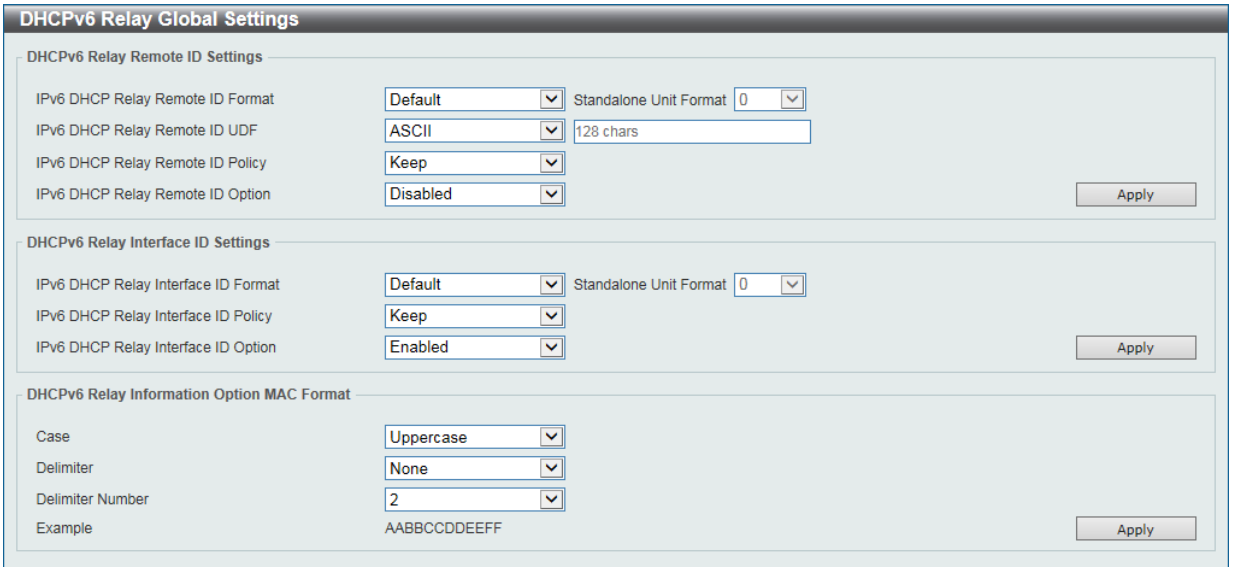


図 7-59　DHCPv6 Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCPv6 Relay Remote ID Settings	
IPv6 DHCP Relay Remote ID Format	IPv6 DHCP リレーのリモート ID フォーマットを選択します。 • 選択肢：「Default」「CID With User Define」「User Define」「Expert UDF」
Standalone Unit Format	「Expert UDF」を選択した場合、スタンドアロンユニットのフォーマットを選択します。 • 選択肢：「0」「1」
IPv6 DHCP Relay Remote ID UDF	リモート ID のユーザ定義項目 (UDF) の入力形式 を選択します。 • 「None」- リモート ID の UDF を空のままにします。 • 「ASCII」- ASCII 文字列で入力します。（128 文字以内） • 「HEX」- 16 進数文字列で入力します。（256 文字以内）

項目	説明
IPv6 DHCP Relay Remote ID Policy	DHCPv6 リレーエージェントのオプション 37 転送ポリシーを選択します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプション 37 リレー情報を保持します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にオプション 37 リレー情報があった場合はそのパケットを破棄します。
IPv6 DHCP Relay Remote ID Option	DHCP IPv6 リクエストパケットのリレーの間のリレーエージェント情報（Option37）の挿入を有効 / 無効に設定します。
DHCPv6 Relay Interface ID Settings	
IPv6 DHCP Relay Interface ID Format	インタフェース ID のフォーマットを指定します。 • 選択肢：「Default」「CID」「Vendor 1」「Expert UDF」
Standalone Unit Format	「Expert UDF」を選択した場合、スタンドアロンユニットのフォーマットを選択します。 • 選択肢：「0」「1」
IPv6 DHCP Relay Interface ID Policy	DHCPv6 リレーエージェントのオプション 18 転送ポリシーを選択します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプション 18 リレー情報を保持します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にオプション 18 リレー情報があった場合はそのパケットを破棄します。
IPv6 DHCP Relay Interface ID Option	DHCP IPv6 リクエストパケットのリレーの間のリレーエージェント情報（Option18）の挿入を有効 / 無効に設定します。
DHCPv6 Relay Information Option MAC Format	
Case	MAC アドレスの形式を選択します。 • 「Lowercase」- 小文字を使用します。（例：aa-bb-cc-dd-ee-ff） • 「Uppercase」- 大文字を使用します。（例：AA-BB-CC-DD-EE-FF）
Delimiter	MAC アドレスを入力する際の区切りを選択します。 • 「Hyphen」（ハイフン）-（例）「AA-BB-CC-DD-EE-FF」 • 「Colon」（コロン）-（例）「AA:BB:CC:DD:EE:FF」 • 「Dot」（ ドット）-（例）「AA.BB.CC.DD.EE.FF」 • 「None」（区切りなし）-（例）「AABBCCDDEEFF」
Delimiter Number	MAC アドレスにおける区切り数を選択します。 • 「1」-（例）「AABBCC.DDEEFF」 • 「2」-（例）「AABB.CCDD.EEFF」 • 「5」-（例）「AA.BB.CC.DD.EE.FF」

「Apply」ボタンをクリックして、設定を適用します。

DHCPv6 Relay Interface Settings（DHCPv6 リレーインタフェース設定）

DHCPv6 リレーインタフェース設定の表示と設定を行います。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface Settings の順にメニューをクリックし、以下の画面を表示します。

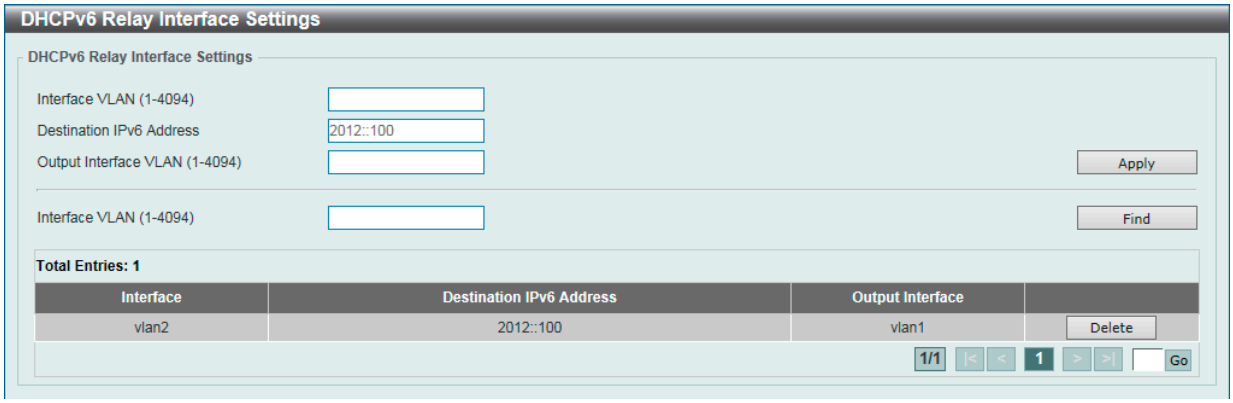


図 7-60　DHCPv6 Relay Interface Settings 画面

画面に表示される項目：

項目	説明
Interface VLAN	DHCPv6 リレーの VLAN ID を指定します。 • 設定可能範囲：1-4094
Destination IPv6 Address	DHCPv6 リレーの宛先アドレスを入力します。
Output Interface VLAN	リレー宛先の送信インタフェース 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て、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く特定のエントリを検出します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

DHCPv6 Relay Remote ID Profile Settings（DHCPv6 リレーリモート ID プロファイル設定）

DHCPv6 リレーリモート ID プロファイル設定を行います。DHCPv6 リレーオプション 37 のプロファイルの作成に使用されます。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Remote ID Profile Settings の順にメニューをクリックし、以下の画面を表示します。

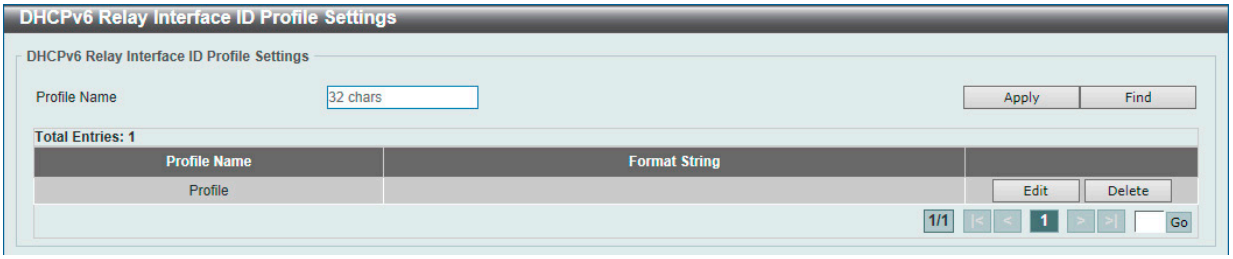


図 7-61　DHCPv6 Relay Remote ID Profile Settings 画面

画面に表示される項目：

項目	説明
Profile Name	オプション 37 のプロファイル名を入力します。（32 文字以内）
Format String	「Edit」をクリックし、ユーザ定義のオプション 37 フォーマット文字列を指定します。（251 文字以内） ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた形式（例："Ethernet"）とします。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列と 16 進数の両方を含むことができます。 • 「%」の後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。（オプション）フォーマットキー文字列において文字長オプションの指定文字数（バイト数）を満たすために使用されます。 - 「$」は先頭をスペース（0x20）で埋めます。 - 「0」は先頭を 0 で埋めます。（初期値） • 「1-32」は文字長オプションです。（オプション）変換されたキー文字列の文字数 / バイト数を指定します。変換されたキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字列がそのまま採用されます。 • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。 - 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。 - 「sysname」はスイッチのシステム名を意味します。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。 - 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列または 16 進数値になります。ASCII 文字列フォーマットの場合、MAC アドレスの形式をカスタマイズすることができます。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列または 16 進数値になります。ASCII 文字列フォーマットの場合、MAC アドレスの形式をカスタマイズすることができます。116 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「unit」はユニット ID を意味します。ASCII 文字列または 16 進数値になります。スタンドアロンのデバイスの場合、ユニット ID は 0 です。 - 「module」はモジュール ID 番号を意味します。ASCII 文字列または 16 進数値になります。 - 「port」はローカルポート番号を意味します。ASCII 文字列または 16 進数値になります。 - 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列または 16 進数値になります。 - 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列または 16 進数値になります。

項目	説明
	• 「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合、この最後の文字（":"）は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットキー文字列のいかなる組み合わせも可能です。「\」はエスケープ文字であり、「\」の後の特殊文字はそのままになります。例えば「\%」は「%」を意味し、フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列に含まれないスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「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。
「Edit」ボタンをクリックして、指定エントリの編集を行います。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

DHCPv6 Relay Interface ID Profile Settings（DHCPv6 リレーインタフェース ID プロファイル設定）

DHCPv6 リレーインタフェース ID プロファイル設定の表示と設定を行います。DHCPv6 リレーオプション 18 のプロファイルを作成に使用されます。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface ID Profile Settings の順にメニューをクリックし、以下の画面を表示します。

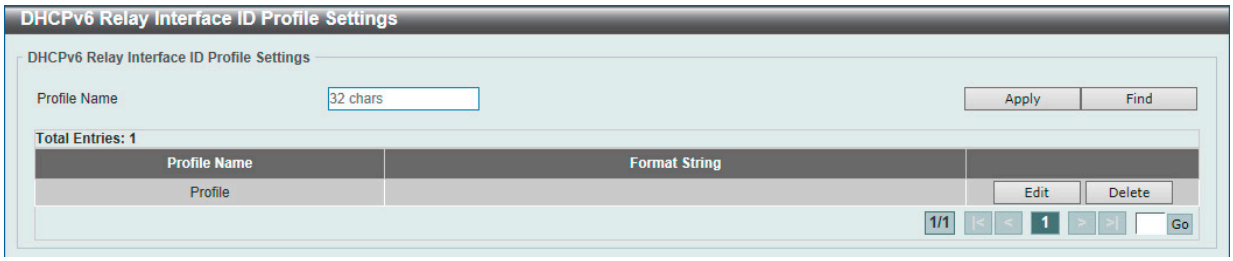


図 7-62　DHCPv6 Relay Interface ID Profile Settings 画面

画面に表示される項目：

項目	説明
Profile Name	オプション 18 のプロファイル名を入力します。（32 文字以内）
Format String	「Edit」をクリックし、ユーザ定義のオプション 18 フォーマット文字列を指定します。（251 文字以内）ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた形式（例："Ethernet"）とします。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列と 16 進数の両方を含むことができます。 • 「%」の後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。（オプション）フォーマットキー文字列において文字長オプションの指定文字数（バイト数）を満たすために使用されます。 - 「$」は先頭をスペース（0x20）で埋めます。 - 「0」は先頭を 0 で埋めます。（初期値） • 「1-32」は文字長オプションです。（オプション）変換されたキー文字列の文字数 / バイト数を指定します。変換されたキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字列がそのまま採用されます。 • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。 - 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。 - 「sysname」はスイッチのシステム名を意味します。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。 - 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列または 16 進数値になります。ASCII 文字列フォーマットの場合、MAC アドレスの形式をカスタマイズすることができます。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。

項目	説明
	- 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列または 16 進数値になります。ASCII 文字列フォーマットの場合、MAC アドレスの形式をカスタマイズすることができます。116 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「unit」はユニット ID を意味します。ASCII 文字列または 16 進数値になります。スタンドアロンのデバイスの場合、ユニット ID は 0 です。 - 「module」はモジュール ID 番号を意味します。ASCII 文字列または 16 進数値になります。 - 「port」はローカルポート番号を意味します。ASCII 文字列または 16 進数値になります。 - 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列または 16 進数値になります。 - 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列または 16 進数値になります。 • 「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合、この最後の文字（":"）は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットキー文字列のいかなる組み合わせも可能です。「\」はエスケープ文字であり、「\」の後の特殊文字はそのままになります。例えば「\%」は「%」を意味し、フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列に含まれないスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「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。
「Edit」ボタンをクリックして、指定エントリの編集を行います。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

DHCPv6 Relay Format Type Settings（DHCPv6 リレーフォーマットタイプ設定）

DHCPv6 リレーフォーマットタイプ設定の表示と設定を行います。各ポートの「expert UDF」文字列の DHCPv6 オプション 37 とオプション 18 を設定します。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Format Type 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。

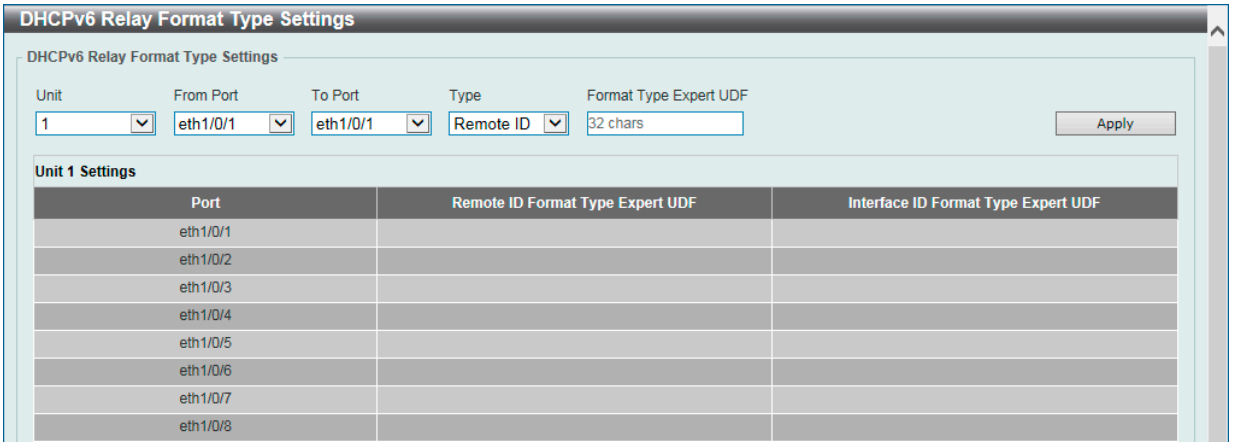


図 7-63　DHCPv6 Relay Format Type Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Type	以下のタイプから指定します。 • 「Remote ID」-「Expert UDF」フォーマットタイプ文字列を DHCPv6 オプション 37 で指定します。 • 「Interface ID」-「Expert UDF」フォーマットタイプ文字列を DHCPv6 オプション 18 で指定します。
Format Type Expert UDF	指定ポートで使用する「expert UDF」文字列を入力します。

「Apply」ボタンをクリックして、設定を適用します。

DHCPv6 Relay Port Settings（DHCPv6 リレーポート設定）

DHCPv6 リレーポート設定を行います。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay 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。

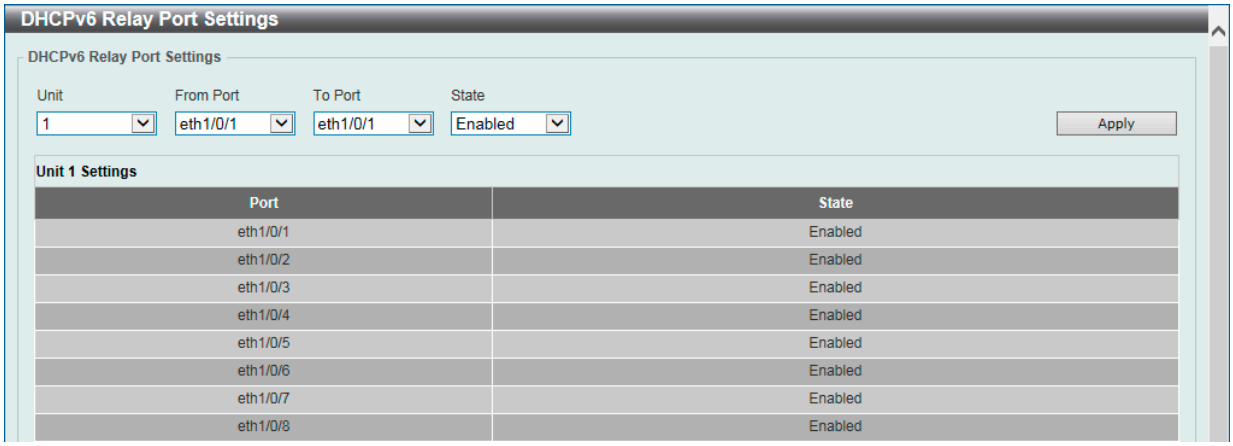


図 7-64　DHCPv6 Relay Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートの DHCPv6 リレーポート機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定を適用します。

DHCPv6 Local Relay VLAN（DHCPv6 ローカルリレー VLAN 設定）

DHCPv6 ローカルリレー VLAN 設定を行います。
DHCPv6 ローカルリレーが有効の場合、クライアントからのリクエストパケットに Option 37 と 18 を追加します。Option 37 のチェックステートが有効の場合、クライアントからのリクエストパケットをチェックし、DHCPv6 リレー機能による Option 37 が含まれる場合、パケットを破棄します。無効の場合、ローカルリレー機能は、Option 37 の有効 / 無効にかかわらず、常に Option 37 をリクエストパケットに追加します。DHCPv6 ローカルリレー機能はサーバからのパケットを直接クライアントに転送します。

Management > DHCP > DHCPv6 Relay > DHCPv6 Local Relay 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。

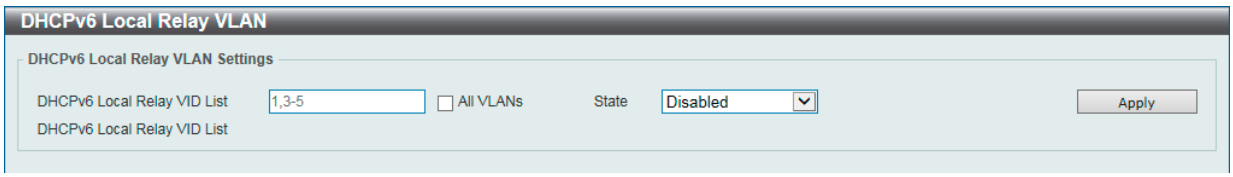


図 7-65　DHCPv6 Local Relay VLAN 画面

画面に表示される項目：

項目	説明
DHCPv6 Local Relay VID List	DHCPv6 ローカルリレー VLAN ID を入力します。一つ以上の VLAN ID が入力可能です。 「ALL VLANs」オプションを指定すると、すべての VLAN が対象になります。
State	指定 VLAN の DHCPv6 ローカルリレー機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定を適用します。

注意　「DHCPv6 リレーポート」が無効の場合、ポートは受信した DHCPv6 パケットをリレー / ローカルにリレーしません。

DHCPv6 Local Relay Port Settings（DHCPv6 ローカルリレーポート設定）

DHCPv6 ローカルリレーポートの再転送ポリシーを設定します。

Management > DHCP > DHCPv6 Relay > DHCPv6 Local Relay 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。

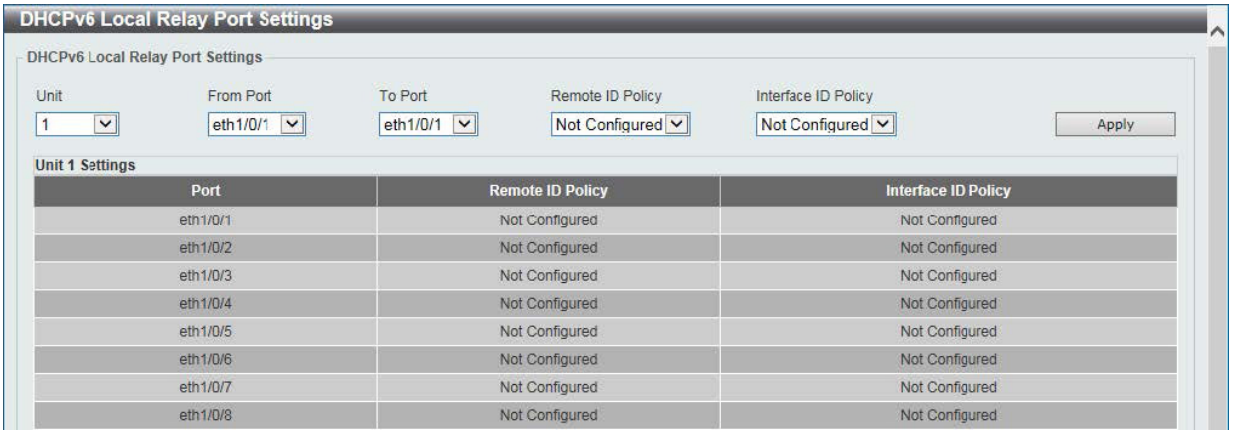


図 7-66　DHCPv6 Local Relay Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Remote ID Policy	DHCPv6 リレーのオプション 37 再転送ポリシーを選択します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にオプション 37 リレー情報があった場合はそのパケットを破棄します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプション 37 リレー情報を保持します。 • 「Replace」- DHCP クライアントから受信したパケット内の既存のオプション 37 リレー情報を新しいオプションで置き換えます。
Interface ID Policy	DHCPv6 リレーのオプション 18 再転送ポリシーを選択します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にオプション 18 リレー情報があった場合はそのパケットを破棄します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプション 18 リレー情報を保持します。 • 「Replace」- DHCP クライアントから受信したパケット内の既存のオプション 18 リレー情報を新しいオプションで置き換えます。

「Apply」ボタンをクリックして、設定内容を適用します。

DHCP Auto Configuration（DHCP 自動コンフィグ設定）

DHCP 自動コンフィグ機能の設定を行います。

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

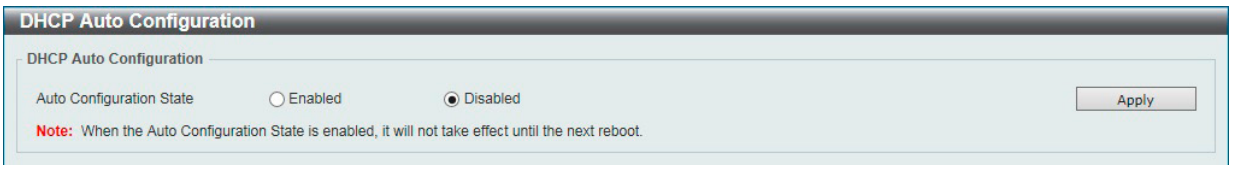


図 7-67　DHCP Auto Configuration 画面

画面に表示される項目：

項目	説明
Auto Configuration State	自動設定機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定を適用します。

DHCP Auto Image Settings（DHCP 自動イメージ設定）

ここでは DHCP 自動イメージ設定を行います。本機能は、スイッチの起動時に外部 TFTP サーバからイメージファイルを取得する機能です。
この TFTP サーバの IP アドレスとファイル名は、DHCP サーバからの「DHCP OFFER」メッセージに含まれています。システムはこのイメージファイルを起動イメージとして使用します。システムが起動し、自動イメージ機能が有効である場合、本スイッチは自動的に DHCP クライアントになります。

DHCP クライアントがアクティブになると、DHCP サーバからネットワーク設定を取得します。DHCP サーバからのメッセージには、TFTP サーバの IP アドレスとイメージファイル名が含まれています。スイッチがこの情報を受信した後、指定した TFTP サーバからの TFTP ダウンロード機能を起動します。このタイミングで、ダウンロード設定パラメータがコンソールに表示されます。レイアウトは download firmware コマンドを使用した場合と同じです。ファームウェアのダウンロードが完了すると、スイッチはすぐに再起動します。

自動コンフィグ機能（auto-configuration）と自動イメージ（auto-image）機能の両方が有効な場合、イメージファイルが先にダウンロードされ、次にコンフィグがダウンロードされます。その後、スイッチはコンフィグレーションを保存して再起動します。

スイッチはダウンロードされたファームウェアを常にチェックします。バージョンが現在実行中のファームウェアと同じ場合、本スイッチは自動イメージ処理を終了します。ただし、自動コンフィギュレーション機能も有効になっている場合は、ダウンロードしたコンフィギュレーションは引き続き実行されます。

本機能は自動コンフィグ機能に似ています。DHCP オプションフィールドは自動イメージ機能だけでなく、自動設定機能でも使用されるため、イメージファイルと設定ファイルの両方を同じ TFTP サーバ配置する必要があります。TFTP サーバの IP アドレスは、引き続き Option 66 または Option 150 の DHCP siaddr フィールドに配置されます。Option 66、Option 150、および siaddr フィールドが同時に DHCP 応答メッセージに存在する場合、Option 150 が最初に解決されます。システムが TFTP サーバへの接続に失敗した場合、システムは Option 66 を解決します。それでもシステムが TFTP サーバへの接続に失敗した場合は、siaddr フィールドが最後の選択肢になります。

本スイッチは、Option 66 を使用して TFTP サーバ名を取得すると、最初に Option6 を解決して DNS サーバの IP アドレスを取得します。
スイッチが DNS サーバへの接続に失敗した場合、または応答メッセージにオプション 6 が存在しない場合、スイッチシステム内に定義されている DNS サーバに接続しようとします。

Option 67 は、DHCP ヘッダの「file」フィールドが DHCP オプションに使用されている場合に、ブートファイルを識別するために使用されます。
これは、DHCP 自動コンフィギュレーションモードでのみ使用でき、DHCP 自動イメージモードでは使用できません。詳細については、RFC 2132 を参照してください。イメージファイル名を指定する場合は、DHCP Option 125（RFC 3925）を使用する必要があります。
本スイッチでは enterprise-number1 フィールドを確認する必要があります。値が D-Link ベンダ ID（171）でない場合、プロセスが停止します。オプションが複数のフィールドを含む場合、最初のエントリ enterprise-number1 のみが使用されます。

Management > DHCP Auto Image 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。

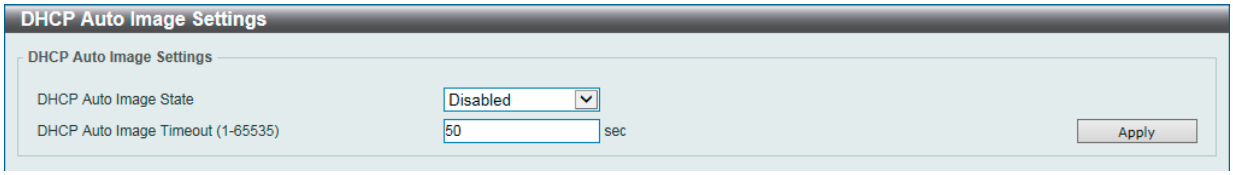


図 7-68　DHCP Auto Image Settings 画面

画面に表示される項目：

項目	説明
DHCP Auto Image State	DHCP 自動イメージ機能を有効 / 無効に設定します。
DHCP Auto Image Timeout	DHCP 自動イメージ機能のタイムアウト時間を指定します。 • 設定可能範囲：1-65535（秒）

「Apply」ボタンをクリックして、設定を適用します。

DNS（ドメインネームシステム）

DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けを行うシステムです。DNS サーバがドメイン名と IP アドレスの変換を実行し、必要に応じて他のネームサーバ問い合わせを行います。ドメインネームサービスを行うデバイスのアドレスは、DHCP または BOOTP サーバから取得する場合と、初期設定時に手動で OS に設定する場合があります。

DNS Global Settings（DNS グローバル設定）

DNS のグローバル設定を行います。

Management > DNS > DNS 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。

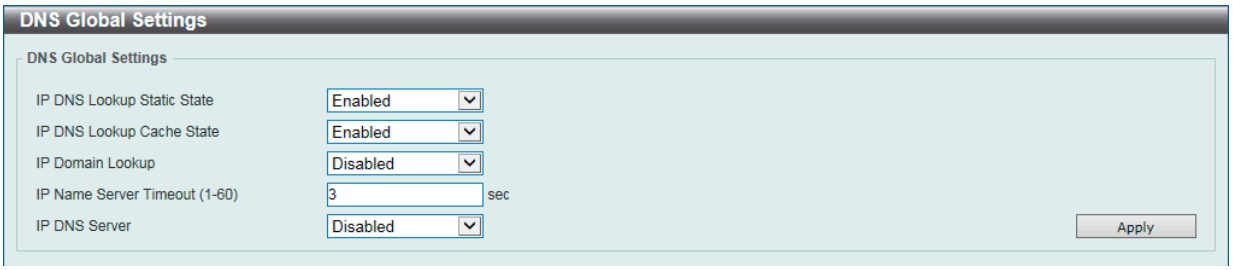


図 7-69　DNS Global Settings 画面

画面に表示される項目：

項目	説明
DNS Global Settings	
IP DNS Lookup Static State	IP DNS ルックアップのスタティックステータスを有効 / 無効に設定します。
IP DNS Lookup Cache State	IP DNS ルックアップのキャッシュを有効 / 無効に設定します。
IP Domain Lookup	IP ドメインルックアップを有効 / 無効に設定します。
IP Name Server Timeout	指定ネームサーバからの回答を待つ待機時間を指定します。 • 設定可能範囲：1-60（秒）
IP DNS Server	DNS サーバを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定を適用します。

注意　IP DNS Server 機能は TCP 未対応です。

DNS Name Server Settings（DNS ネームサーバ設定）

スイッチに DNS サーバの IP アドレスを設定します。

Management > DNS > DNS Name Server 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。

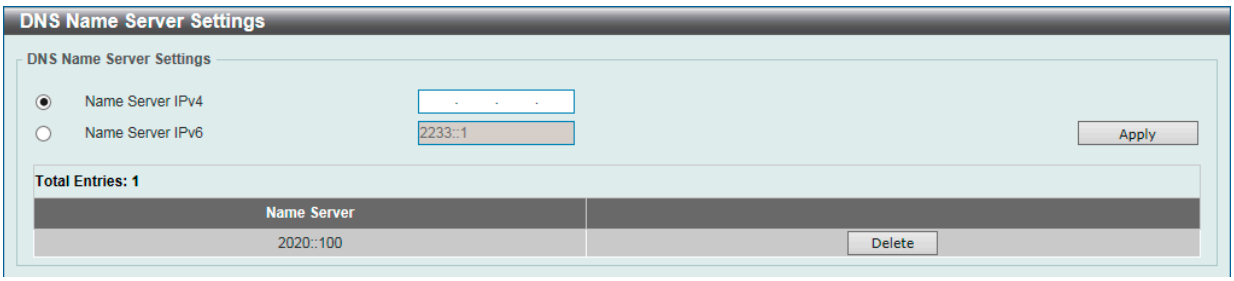


図 7-70　DNS Name Server Settings 画面

画面に表示される項目：

項目	説明
Name Server IPv4	本項目を選択し、DNS サーバの IPv4 アドレスを入力します。
Name Server IPv6	本項目を選択し、DNS サーバの IPv6 アドレスを入力します。

「Apply」ボタンをクリックして、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。

DNS Host Settings（DNS ホスト名設定）

ホストテーブルのホスト名 /IP アドレスのスタティックマッピングを表示、設定します。

Management > DNS > DNS Host 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。

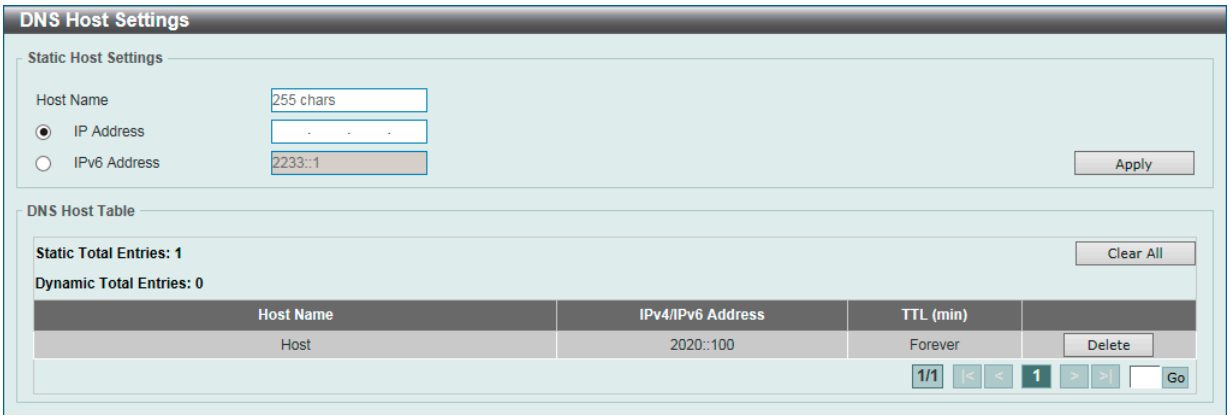


図 7-71　DNS Host Settings 画面

画面に表示される項目：

項目	説明
Host Name	ホスト名を入力します。
IP Address	ホストの IPv4 アドレスを入力します。
IPv6 Address	ホストの IPv6 アドレスを入力します。

「Apply」ボタンをクリックして、設定を適用します。
「Clear All」ボタンをクリックして、入力したエントリを全てクリアします。
「Delete」ボタンをクリックして、指定エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

NTP（NTP 設定）

スイッチの時刻を同期するための通信プロトコル（NTP/Network Time Protocol）の設定を行います。

NTP Global Settings（NTP グローバル設定）

NTP のグローバル設定を行います。

Management > NTP > NTP 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。

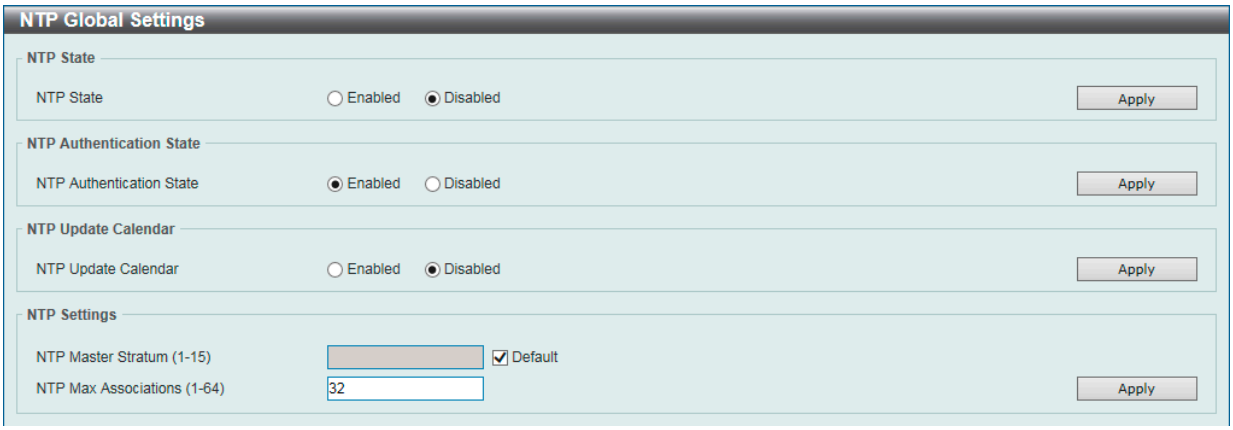


図 7-72　NTP Global Settings 定画面

画面に表示される項目：

項目	説明
NTP State	
NTP State	NTP 機能をグローバルに有効 / 無効にします。

項目	説明
NTP Authentication State	
NTP Authentication State	NTP の認証を有効 / 無効にします。 この機能を有効にすると、ネットワークノードは、認証キーの 1 つを持っていない限り、スイッチと同期しません。
NTP Update Calendar	
NTP Update Calendar	NTP のアップデートカレンダーを有効 / 無効にします。 この機能は、NTP ソースからハードウェアクロックを定期的に更新するために使用されます。
NTP Settings	
NTP Master Stratum	NTP マスタの階層値を指定します。 外部 NTP が使用できない場合に、Real-Time Clock（RTC）を NTP マスタクロックとして設定するために使用されます。 「Default」を指定すると初期値を使用します。 • 設定可能範囲：1 - 15
NTP Max Associations	NTP への接続最大値を指定します。 スイッチ上の NTP ピアとクライアントの最大数を設定するために使用します。 • 設定可能範囲：1 - 64

「Apply」をクリックして、設定内容を適用します。

NTP Server Settings（NTP サーバ設定）

NTP サーバの設定を行います。

Management > NTP > NTP Server 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。

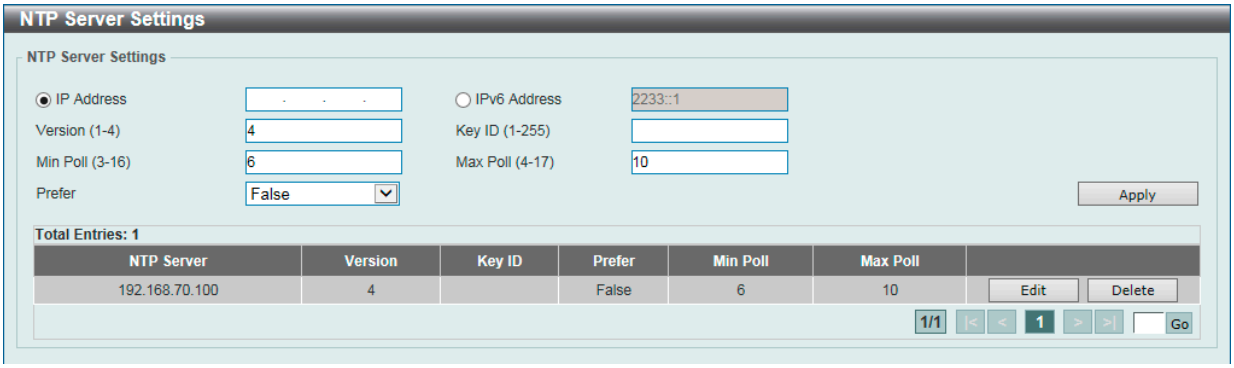


図 7-73　NTP Server Settings 設定画面

画面に表示される項目：

項目	説明
IP Address	NTP サーバの IPv4 アドレスを指定します。
IPv6 Address	NTP サーバの IPv6 アドレスを指定します。
Version	NTP サーバのバージョンを指定します。 • 設定可能範囲：1 - 4
Key ID	認証鍵 ID を指定します。 • 設定可能範囲：1 - 255
Min Poll	NTP メッセージ送信の最小ポーリング間隔を指定します。 指定された「Min Poll」値の 2 乗が、最小ポーリング間隔となります。例えば、ここで指定された値が 6 の場合、使用される最小ポーリング間隔は 64 秒（$2^6 = 64$）です。 • 設定可能範囲：3-16
Max Poll	NTP メッセージ送信の最大ポーリング間隔を指定します。 指定された「Max Poll」値の 2 乗が、最大ポーリング間隔となります。例えば、ここで指定された値が 6 の場合、使用される最大ポーリング間隔は 64 秒（$2^6 = 64$）です。 • 設定可能範囲：4-17
Prefer	このエントリを同期するサーバとして優先するかどうかを選択します。 • 選択肢：「True」「False」

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、指定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。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

注意　NTP サーバの機能において、経路に従って送信元の IP が決定されるため、構成によりクライアントは同期に失敗する場合があります。

NTP Peer Settings（NTP ピア設定）

NTP のピア設定を行います。

Management > NTP > NTP Peer 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。

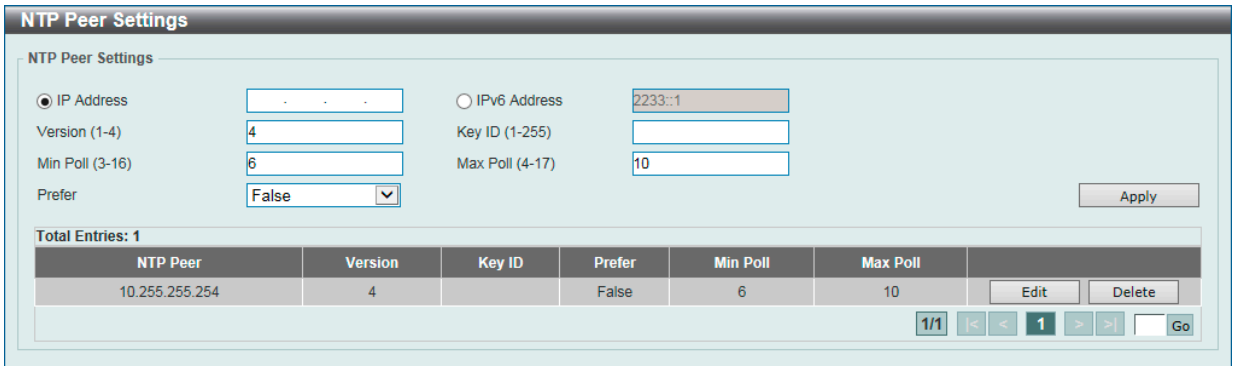


図 7-74　NTP Peer Settings 設定画面

画面に表示される項目：

項目	説明
IP Address	NTP ピアの IPv4 アドレスを指定します。
IPv6 Address	NTP ピアの IPv6 アドレスを指定します。
Version	NTP バージョンを指定します。 • 設定可能範囲：1 - 4
Key ID	認証鍵 ID を指定します。 • 設定可能範囲：1 - 255
Min Poll	NTP メッセージ送信の最小ポーリング間隔を指定します。 指定された「Min Poll」値の 2 乗が、最小ポーリング間隔となります。例えば、ここで指定された値が 6 の場合、使用される最小ポーリング間隔は 64 秒（$2^6 = 64$）です。 • 設定可能範囲：3-16
Max Poll	NTP メッセージ送信の最大ポーリング間隔を指定します。 指定された「Max Poll」値の 2 乗が、最大ポーリング間隔となります。例えば、ここで指定された値が 6 の場合、使用される最大ポーリング間隔は 64 秒（$2^6 = 64$）です。 • 設定可能範囲：4-17
Prefer	対象のピアを同期するピアとして優先するか否かを選択します。 • 選択肢：「True」「False」

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、指定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。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

NTP Access Group Settings（NTP アクセスグループ設定）

NTP アクセスグループの設定を行います。
IPv4 アドレス /IPv6 アドレスとマスクを設定し、アクセスコントロールリストを作成します。

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

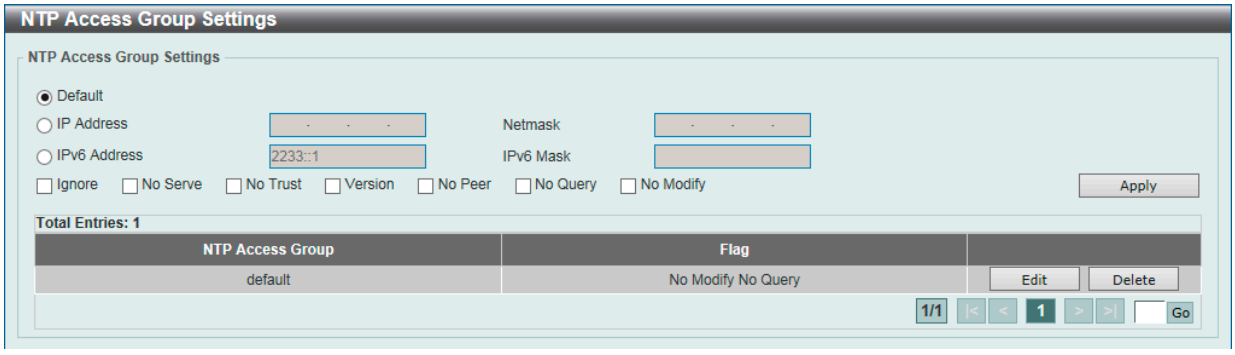


図 7-75　NTP Access Group Settings 画面

画面に表示される項目：

項目	説明
Default	初期値の IPv4 アドレス（0.0.0.0/0.0.0.0）または IPv6 アドレス（::/::）を使用します。 初期値の IP アドレスは、リスト内で常に一番低い優先度となります。
IP Address	ホスト IPv4 アドレスを指定します。
Netmask	ホストネットワークの IPv4 ネットマスクを指定します。
IPv6 Address	ホスト IPv6 アドレスを指定します。
IPv6 Mask	ホストネットワークの IPv6 プレフィックス長を指定します。
Ignore	NTP コントロールクエリを含むすべてのパケットを拒否します。
No Serve	NTP コントロールクエリを除く、すべてのパケットを拒否します。
No Trust	暗号認証されていないパケットを拒否します。
Version	現在の NTP バージョンと一致しないパケットを拒否します。
No Peer	認証されない限り、アソシエーションを形成する可能性のあるパケットを拒否します。 設定されたアソシエーションが存在しない場合、パケットには Broadcast、Symmetric Active、Many Cast Server パケットが含まれます。「No Peer」は、アソシエーションを形成しようとしないパケットには適用されません。
No Query	すべての NTP コントロールクエリを拒否します。
No Modify	サーバの状態を変更しようとする NTP コントロールクエリを拒否します。

「Apply」をクリックして、設定内容を適用します。
「Edit」をクリックして、エントリを編集します。
「Delete」をクリックして、指定エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

NTP Key Settings（NTP キー設定）

NTP キーの設定を行います。

Management > NTP > NTP Key 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。

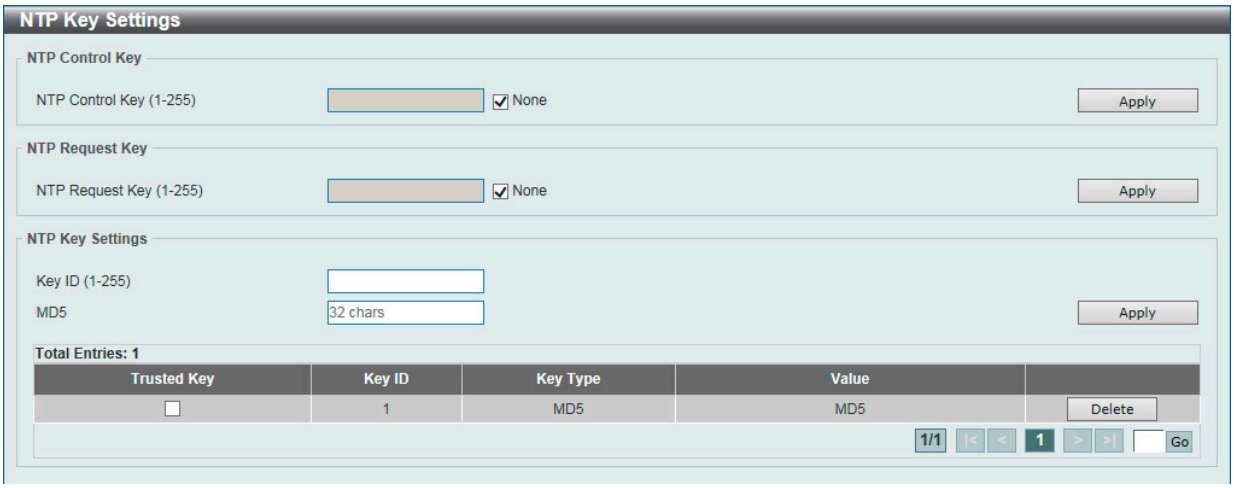


図 7-76　NTP Key Settings 画面

画面に表示される項目：

項目	説明
NTP Control Key	
NTP Control Key	NTP コントロールキー（制御鍵）を指定します。本項目は、NTP コントロールメッセージのキー ID を定義するために使用されます。「None」にチェックを入れると NTP コントロールキーを使用しません。 • 設定可能範囲：1-255
NTP Request Key	
NTP Request Key	NTP リクエストキー（要求鍵）を指定します。 ntpdc ユーティリティプログラムによって使用される NTP モード 7 パケットのキー ID を定義するために使用されます。 「None」にチェックを入れると NTP リクエストキーを使用しません。 • 設定可能範囲：1-255
NTP Key Settings	
Key ID	NTP キー ID を指定します。 • 設定可能範囲：1-255
MD5	MD5 認証キーを指定します。（32 文字以内）

項目	説明
Trusted Key	設定済みエントリの本項目にチェックを入れて、ピア NTP システムのキーが認証で信頼されることを指定します。

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、指定エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

NTP Interface Settings（NTP インタフェース設定）

NTP のインタフェース設定を行います。インタフェースの NTP パケット受信を許可 / 拒否します。

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

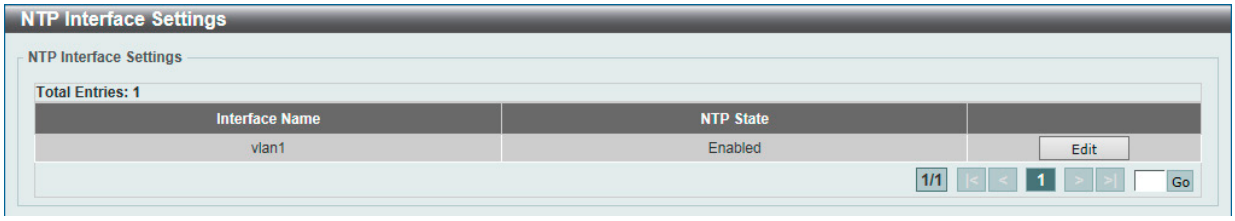


図 7-77　NTP Interface Settings 画面

画面に表示される項目：

項目	説明
NTP State	「Edit」をクリックして、VLAN インタフェース上の NTP 機能を有効 / 無効にします。

「Apply」をクリックして、設定内容を適用します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

NTP Associations（NTP アソシエーション）

NTP アソシエーションを表示します。

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

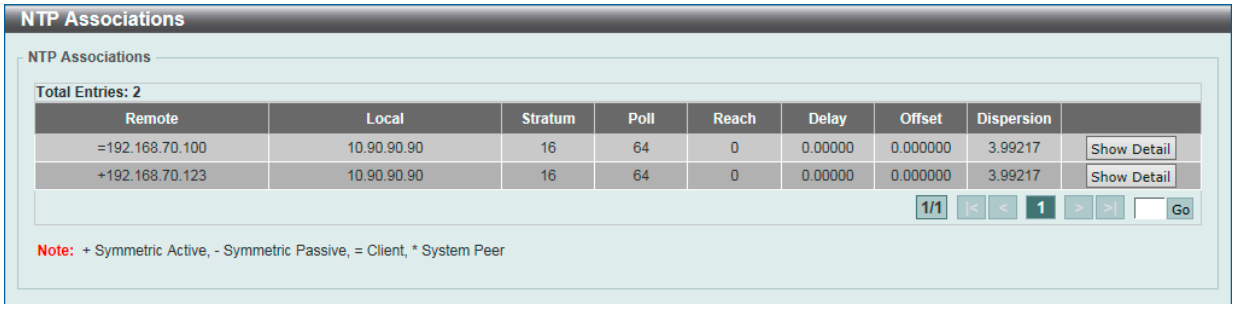


図 7-78　NTP Associations 画面

エントリ横の「Show Detail」をクリックし、該当 NTP アソシエーションの詳細を表示します。

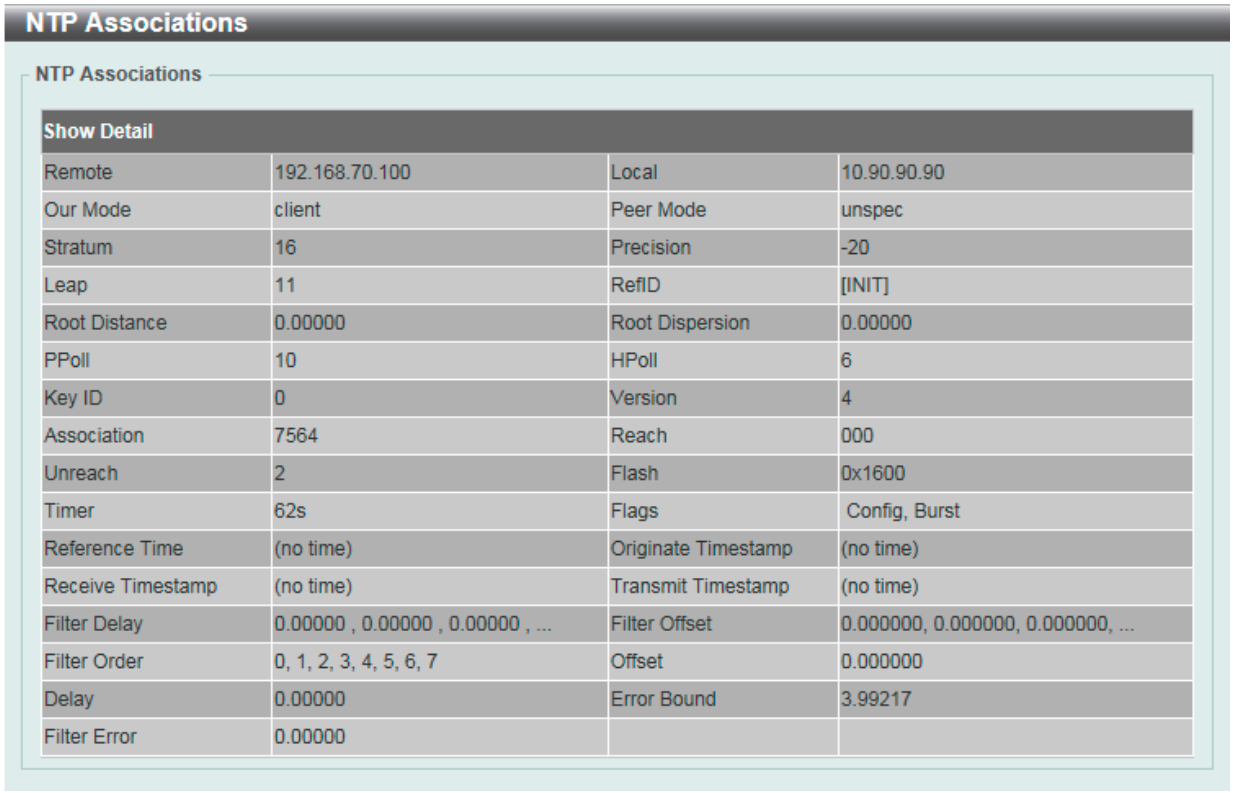


図 7-79　NTP Associations（Show Detail）画面

NTP Status（NTP ステータス）

NTP ステータスを表示します。

Management > **NTP** > **NTP 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。

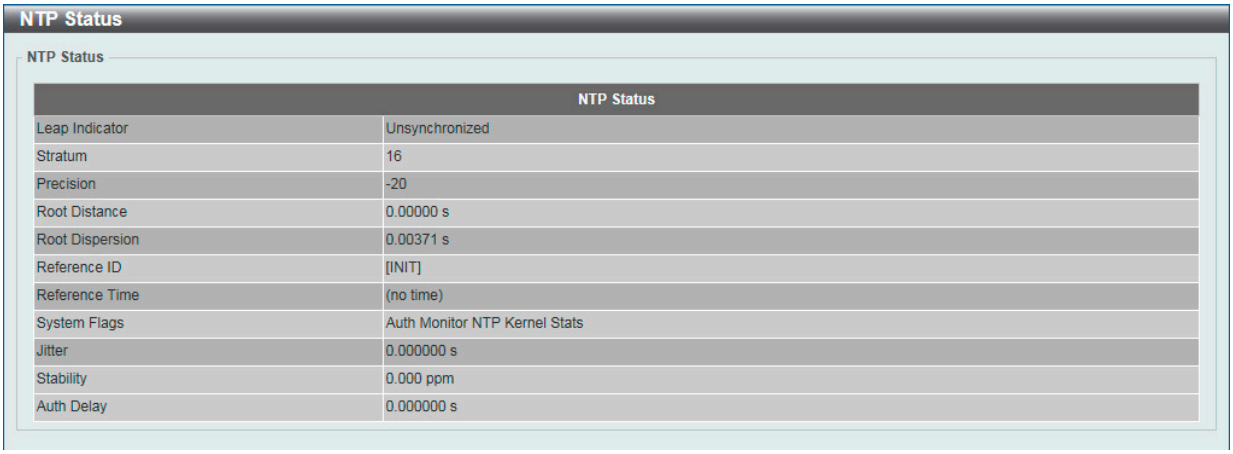


図 7-80　NTP Status 画面

File System（ファイルシステム設定）

スイッチのファイルシステムを閲覧、管理および設定します。

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

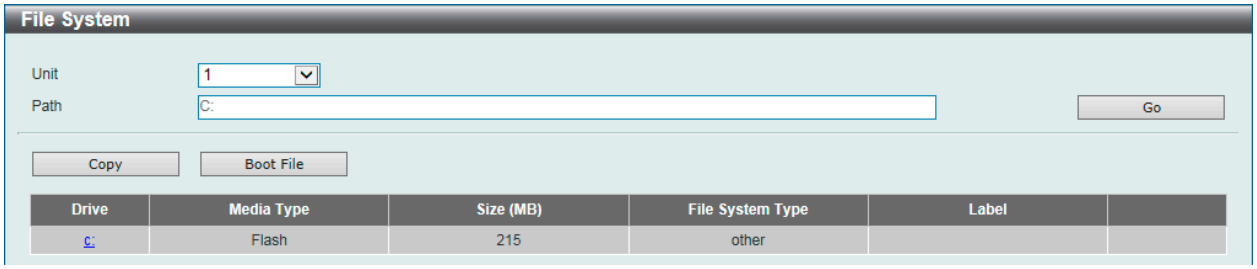


図 7-81　File System 画面

画面に表示される項目：

項目	説明
Unit	設定を行うユニットを指定します。
Path	パスの文字列を入力します。

「Go」ボタンをクリックして、入力したパスに遷移します。
「Copy」ボタンをクリックして、指定のファイルをスイッチへコピーします。
「Boot File」ボタンをクリックして、ブートイメージおよびブートコンフィグの指定を行います。
「C:」リンクをクリックして、「C:」ドライブに遷移します。

「C:」リンクをクリックすると、以下の画面が表示されます。

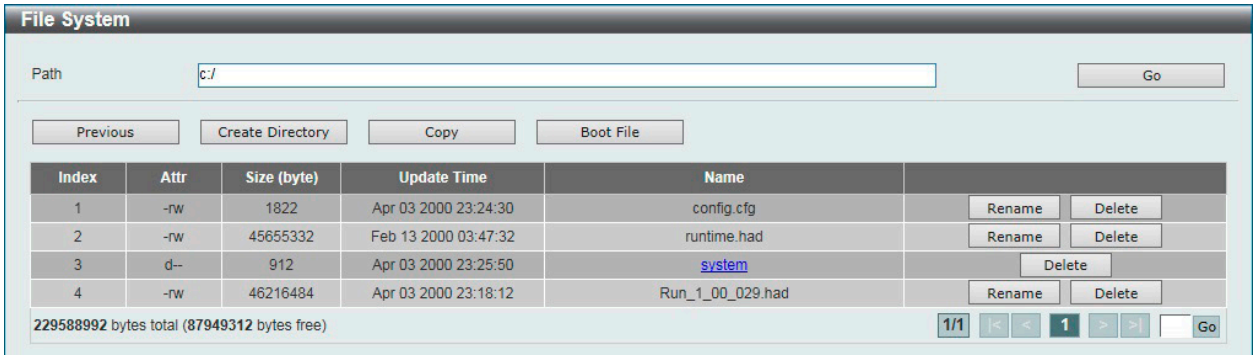


図 7-82　File System (Drive) 画面

画面に表示される項目：

項目	説明
Go	入力したパスに移動します。
Previous	前のページに戻ります。
Create Directory	スイッチのファイルシステムに新しいディレクトリを作成します。
Copy	指定ファイルをスイッチにコピーします。
Boot File	起動用のブートアップイメージとコンフィグレーションを指定します。
Rename	ファイル名を変更します。
Delete	ファイルシステムから指定ファイルを削除します。

ファイルのコピー

「Copy」ボタンをクリックすると、以下の画面が表示されます。

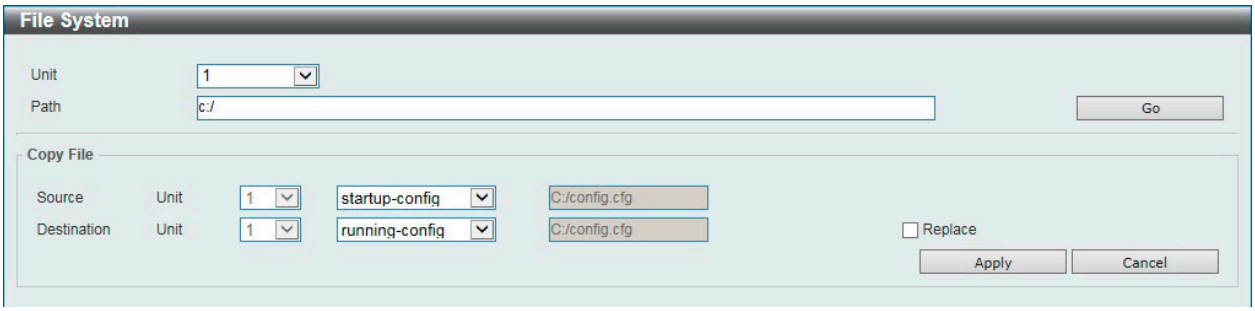


図 7-83　File System (Copy) 画面

画面に表示される項目：

項目	説明
Source	コピー元のファイルが保存されているスイッチのユニット ID と、コピー元のファイルの種類を選択します。 • 選択肢：「startup-config」「Source File」 「Source File」選択時には、ファイルパスを入力します。
Destination	コピー先のスイッチのユニット ID と、コピー先のファイルの種類を選択します。 • 選択肢：「startup-config」「running-config」「Destination File」 「Destination File」選択時には、ファイルパスを入力します。「Replace」にチェックを入れると、現在実行中のコンフィグファイルを指定のコンフィグファイルと差し替えます。

「Apply」ボタンをクリックして、コピーを開始します。
「Cancel」ボタンをクリックすると処理は破棄されます。

起動ファイルの指定

「Boot File」ボタンをクリックすると、以下の画面が表示されます。

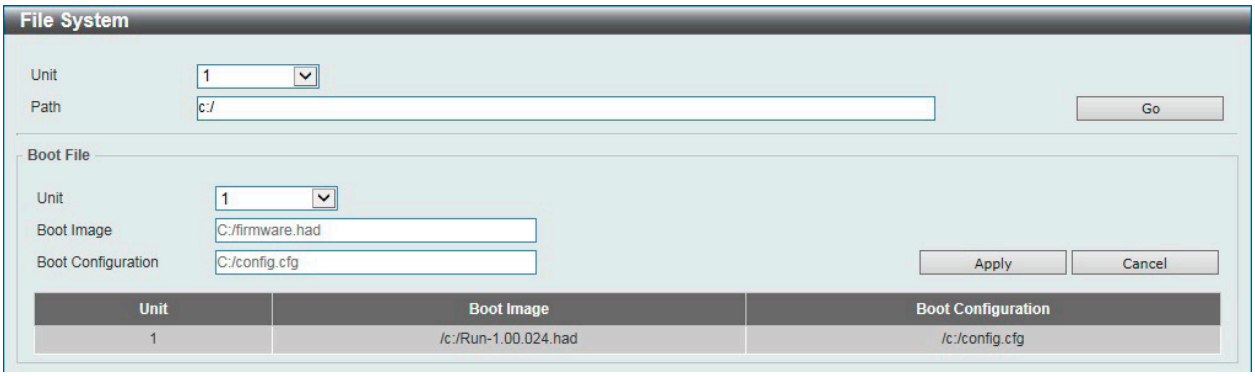


図 7-84　File System (Boot File) 画面

画面に表示される項目：

項目	説明
Unit	設定を行うユニットを指定します。
Boot Image	ブートイメージファイルのパスを入力します。
Boot Configuration	ブートコンフィグファイルのパスを入力します。

「Apply」ボタンをクリックして、設定を適用します。
「Cancel」ボタンをクリックすると入力内容は破棄されます。

Stacking（スタッキング設定）

本スイッチは、スイッチの物理スタックをサポートしています。Telnet、GUI インタフェース（Web）、SNMP を介して 1 つの IP アドレスで管理することができます。物理スタックによりお使いのネットワークの信頼性、サービス性、そして可用性が向上します。本シリーズの各スイッチは、前面に 2/4 個のスタック用スロットを搭載しスタッキング可能なデバイスを接続することができます。スタックポートを設定した後、SFP+ ダイレクトアタッチケーブル（DAC）もしくは光ファイバーケーブルを使用して、スタックポート間を接続し、2 つのトポロジのうちいずれかを形成することができます。

- Duplex Chain - Duplex Chain トポロジはチェーン・リンク形式でスイッチをスタックします。この方法を使用すると、一方向のデータ転送だけが可能となります。1 カ所中断が発生すると、データ転送は影響を受けます。

- Duplex Ring - Duplex Ring は、データが双方向に転送できるようにリングまたはサークルの形式でスイッチをスタックします。このトポロジは、リングに 1 カ所中断が発生しても、データはスタック内のスイッチ間の代替えパスのスタックケーブル経由で転送されるため高い冗長性を実現できます。

本シリーズのスイッチは、SFP+ モジュールに接続された光ファイバケーブル、または SFP+ スロットに接続された SFP+ ダイレクトアタッチケーブルを使用して、物理的にスタックすることが可能です。最後の 2/4 つの SFP+ スロットのみ物理スタックに使用できます。

注意　スタッキングが有効になっている場合、最後の SFP+ スロット 2/4 つは他のデバイスやスイッチなどへのアップリンクとして使用できません。これらのスロットはスタッキング専用スロットとなります。

以下は、SFP+ モジュールに接続された光ファイバケーブル、または SFP+ ダイレクトアタッチケーブルを使用した「Duplex Chain」構成での物理スタック図です。「4 ポート」スタッキング設定を使用しています。

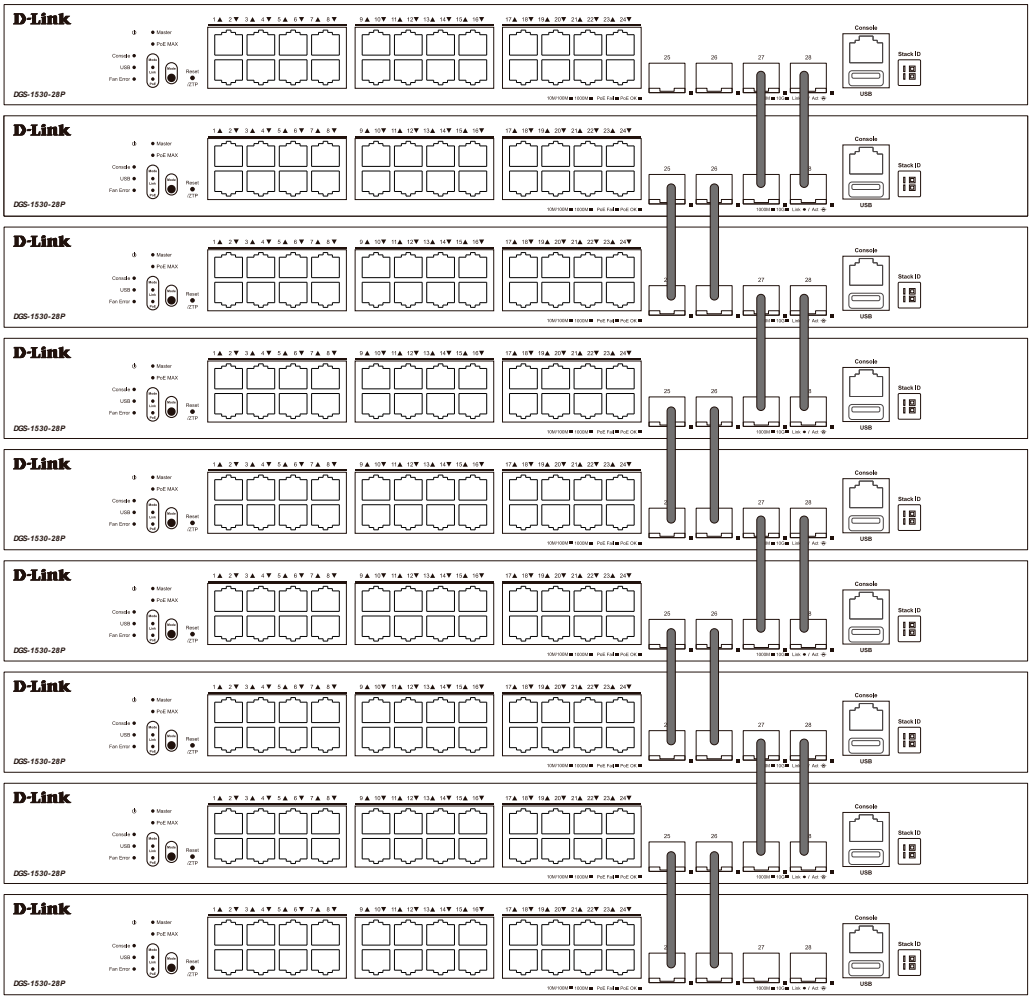


図 7-85　Duplex Chain でスタックされているスイッチ（SFP+）

以下は、SFP+ モジュールに接続された光ファイバケーブル、または SFP+ ダイレクトアタッチケーブルを使用した「Duplex Ring」構成での物理スタック図です。「4 ポート」スタッキング設定を使用しています。

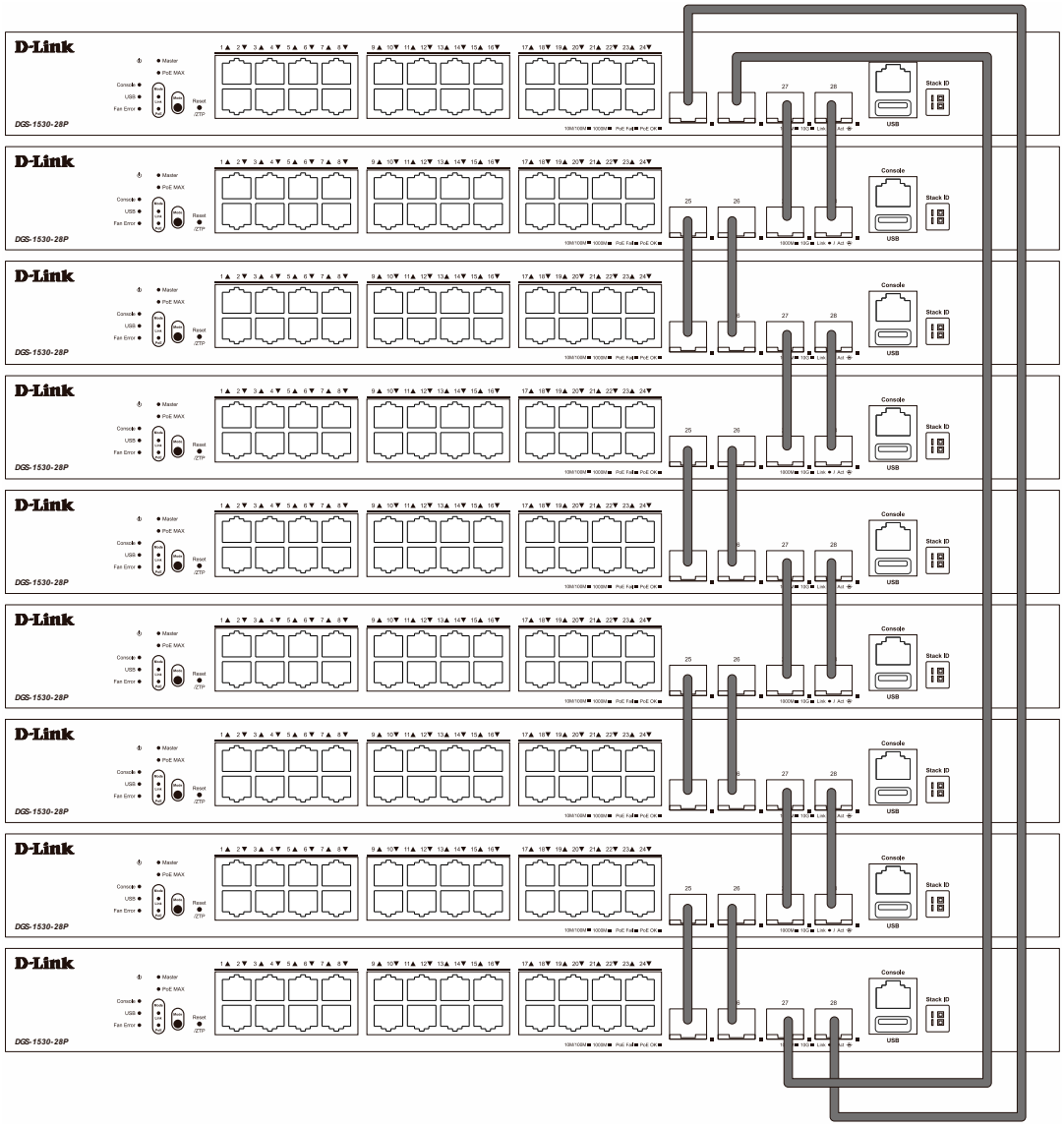


図 7-86　Duplex Ring でスタックされているスイッチ（SFP+）

物理スタックでは「2 ポート」「4 ポート」スタッキングコンフィグレーションを設定することができます。

- 「2 ポート」スタッキング設定時にはスイッチ間のフルデュプレックススピードで、最大 40Gbps が使用可能です。
- 「4 ポート」スタッキング設定時にはスイッチ間のフルデュプレックススピードで、最大 80Gbps が使用可能です。

スタッキングポートの設定と、それに対応する SIO ポートペアは以下の通りです。

製品名	2 ポートスタッキング		4 ポートスタッキング	
	SIO1	SIO2	SIO1	SIO2
DGS-1530-10	ポート 9	ポート 10	—	—
DGS-1530-20	ポート 19	ポート 20	ポート 17、18	ポート 19、20
DGS-1530-28	ポート 27	ポート 28	ポート 25、26	ポート 27、28
DGS-1530-28P	ポート 27	ポート 28	ポート 25、26	ポート 27、28
DGS-1530-28S	ポート 27	ポート 28	ポート 25、26	ポート 27、28
DGS-1530-28SC	ポート 27	ポート 28	ポート 25、26	ポート 27、28
DGS-1530-52	ポート 51	ポート 52	ポート 49、50	ポート 51、52
DGS-1530-52P	ポート 51	ポート 52	ポート 49、50	ポート 51、52

スタッキングポートは、SIO1、SIO2 と呼ばれる 2 つの論理スタッキングポートにグループ化されます。（SIO：Stacking Input/Output）論理スタッキングポートのグループは、常にグループとしてスタック内の別のスイッチに接続する必要があります。

以下の図は、4 ポートスタッキングにおける適切な接続例です。

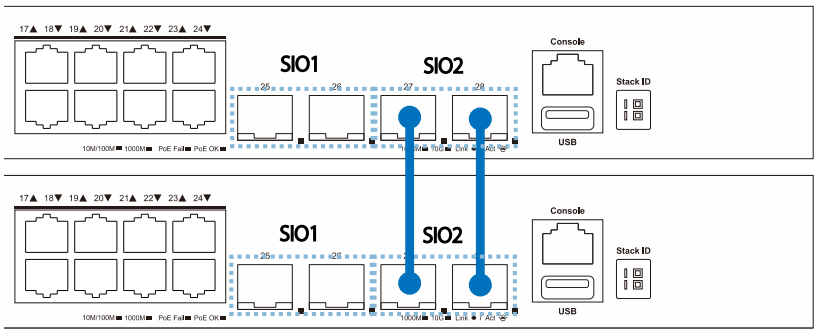


図 7-87　スイッチ間のケーブル接続①

以下の図では、異なる SIO に接続されているため、安定したスタッキング接続を保証できません。

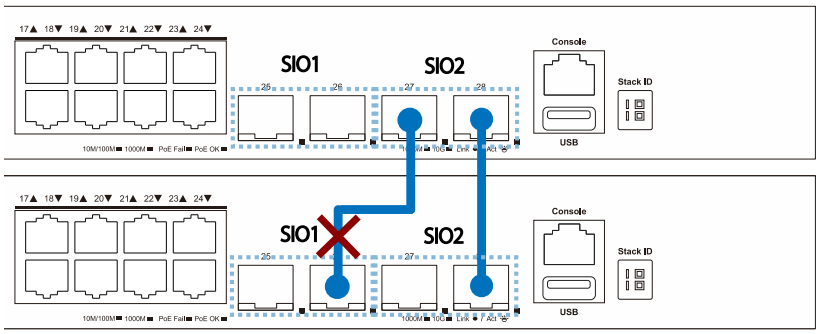


図 7-88　スイッチ間のケーブル接続②

スタック内のスイッチ役割

トポロジ内で、各スイッチはスイッチスタックにおける役割を果たします。各スイッチには役割を設定でき、スイッチスタック機能により自動的に決定することもできます。スイッチをスタックする場合、次の 3 つの役割があります。

- プライマリマスタ
  プライマリマスタは、スタックのリーダです。スタックの通常操作、モニタ操作、およびトポロジの実行をメンテナンスします。このスイッチは、スイッチスタック内にあるスイッチへのスタックユニット番号の割り当て、コンフィグレーションの同期、コマンドの送信を行います。物理的にスタックを構成する前に、スイッチに最も高いプライオリティ（より小さい番号がより高いプライオリティを示します）を割り当てることによって、プライマリマスタを手動で設定することができます。または、すべてのプライオリティが同じ場合、最も値の小さい MAC アドレスを持つスイッチをプライマリマスタとして割り当てる選択プロセスによって、スタック機能により自動的に決定されます。プライマリマスタに設定されている場合、スイッチの前面パネルの一番右にある LED により、Box ID と「H」が表示されます。

- バックアップマスタ
  バックアップマスタは、プライマリマスタに対するバックアップであり、プライマリマスタが故障、またはスタックから取り外される場合に、プライマリマスタの機能を引き継ぎます。また、スタック内で隣接するスイッチの状態をモニタし、プライマリマスタによって割り当てられたコマンドを実行して、プライマリマスタの動作状態をモニタします。物理的にスタックを構成する前に、スイッチに 2 番目に高いプライオリティを割り当てることによって、バックアップマスタを手動で設定することができます。または、すべてのプライオリティが同じ場合、2 番目に値の小さい MAC アドレスを持つスイッチをバックアップマスタとして割り当てる選択プロセスによって、スタック機能により自動的に決定されます。バックアップマスタに設定されている場合、スイッチの前面パネルの一番右にある LED により、Box ID と「h」が表示されます。

- スレーブ
  スレーブスイッチは、プライマリマスタまたはバックアップマスタではないスイッチスタックの残りのスイッチです。プライマリマスタおよびバックアップマスタが故障、またはスタックから取り外される場合に、それらの機能を引き継ぎます。スレーブスイッチは、マスタに要求された操作を実行して、スタックとスタックトポロジにある近接スイッチの状態をモニタします。さらに、バックアップマスタがプライマリマスタになるとバックアップマスタのコマンドに従います。スレーブスイッチは、バックアップマスタがプライマリマスタに移行する場合や、バックアップマスタが故障、またはスイッチから取り外される場合に、セルフチェックを行い、自身がバックアップマスタになるかどうかを決定します。プライマリマスタとバックアップマスタの両方が故障、またはスイッチから取り外される場合、プライマリマスタになるかどうかを決定します。これらの役割はプライオリティによって決定され、プライオリティが同じである場合は、最も値の小さい MAC アドレスによって決定されます。

適切なトポロジでスイッチが構成された後、3 つのプロセスを経てスタックが動作状態になります。

- 初期化状態 - スタックの最初の状態です。ランタイムコードがセットおよび初期化され、周辺機器を診断することによって各スイッチが適切に機能していることを検証します。
- マスタ選出状態 - ランタイムコードがロードおよび初期化されると、スタックはマスタ選出状態になり、使用されるトポロジのタイプを検出し、プライマリマスタ、バックアップマスタの順に選出します。
- 同期状態 - プライマリマスタとバックアップマスタが確立すると、プライマリマスタはスタック内のスイッチにスタックユニット番号を割り当て、

すべてのスイッチに構成を同期させ、プライマリマスタの構成に基づいて残りのスイッチにコマンドを送信します。

これらの処理が完了すると、スイッチスタックは通常の操作モードに入ります。

スタックスイッチのスワップ

スイッチのスタック機能は、スタック内のスイッチのホットスワップをサポートしています。いくつかの基本的な条件に従うことにより、電源オフやスタック内のスイッチ間のデータ転送に大きな影響を与えずに、スタックからスイッチを削除または追加することができます。

スイッチが動作中のスタックに「ホットインサート」される場合、新たに追加されたスイッチのコンフィグレーション（プライオリティや MAC アドレスなど）に基づいて、新しいスイッチがプライマリマスタ、バックアップマスタまたはスレーブとなる可能性があります。また、既に選択プロセスを経てプライマリマスタとバックアップマスタをそれぞれ持った 2 つのスタックを統合する場合、プライオリティまたは MAC アドレスに基づいて、どちらかのプライマリマスタが新しいプライマリマスタとして選出されます。このプライマリマスタは、ホットインサートされた新しいスイッチすべてのプライマリマスタの全役割を引き継ぎます。このプロセスはディスカバリパケットを使用して行われ、パケットはディスカバリプロセスが完了するまで 1.5 秒ごとにスイッチスタックを循環します。

「ホットリムーブ」の動作は、スタックの動作中にスタックからデバイスが削除されたことを意味します。ホットリムーブは、指定した間隔でデバイスからハートビートパケットを受信しない場合、またはスタックポートのいずれかがリンクがダウンした場合に、スタックによって検出されます。デバイスが取り外されると、残りのスイッチはスタックトポロジデータベースを更新し、変更を反映します。これらの 3 つの役割（プライマリマスタ、バックアップマスタ、またはスレーブ）は、いずれもスタックから削除される可能性がありますが、それぞれの削除毎に異なる処理が発生します。

スレーブデバイスが取り外される場合、プライマリマスタは unit leave メッセージを使用して、このデバイスのホットリムーブを他のスイッチに通知します。スタック内のスイッチは、取り外されたユニットのコンフィグレーションおよび ARP などのダイナミックに学習されたデータベースをクリアします。

バックアップマスタがホットリムーブされると、前述の選出プロセスにより新しくバックアップマスタが選ばれます。スタック内のスイッチは、取り外されたユニットのコンフィグレーションおよび ARP などのダイナミックに学習されたデータベースをクリアします。その後、スタックによるデータベースの同期が完了した後に、バックアップマスタがプライマリマスタのバックアップを開始します。

プライマリマスタが取り外されると、バックアップマスタがプライマリマスタの役割を引継ぎ、選出プロセスにより新しいバックアップマスタが選ばれます。スタック内のスイッチは、取り外されたユニットのコンフィグレーションおよび ARP などのダイナミックに学習されたデータベースをクリアします。スタックとネットワークの間での競合を避けるために、新しいプライマリマスタは、前のプライマスタの MAC と IP アドレスを引き継ぎます。

プライマリマスタとバックアップマスタの両方が取り外される場合、選出プロセスが即時に実行され、新しいプライマリマスタとバックアップマスタが決定します。スタック内のスイッチは、取り外されたユニットのコンフィグレーションおよび ARP などのダイナミックに学習されたデータベースをクリアします。スタティックなスイッチ設定は、スタック内の残りのスイッチのデータベース内に残ったままとなり、それらの機能は影響を受けません。

注意 スタックの検出プロセス実行中に Box ID の競合が見つかると、そのデバイスは特別なスタンドアロントポロジモードに入ります。ユーザはデバイス情報の取得、Box ID の設定、保存、および再起動だけ行うことができます。すべてのスタックポートが無効となり、スタック内の各デバイスのローカルコンソールポートに対してエラーメッセージが生成されます。ユーザは、Box ID を再設定し、スタックを再起動する必要があります。

Physical Stacking（物理スタッキング）

物理スタッキングの設定を行います。

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

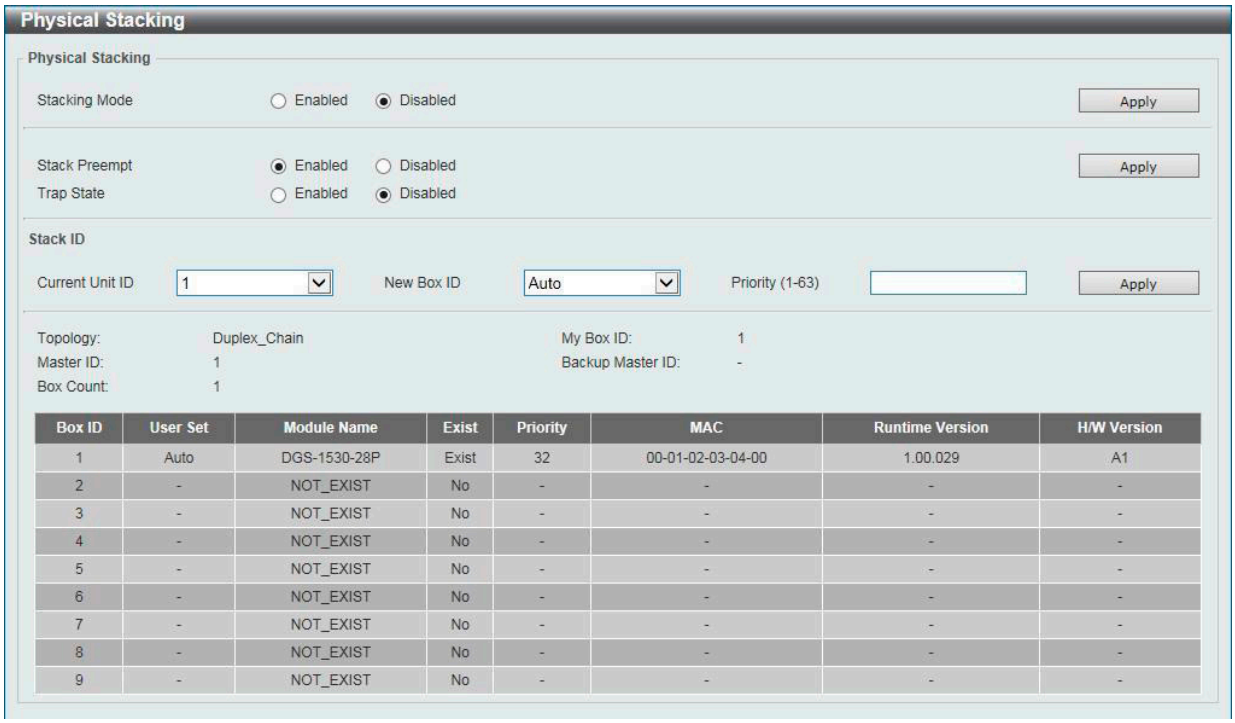


図 7-89　Physical Stacking 画面

画面に表示される項目：

項目	説明
Physical Stacking	
Stacking Mode	スタッキングモードを有効 / 無効に設定します。
Stack Preempt	Stack Preempt 機能の有効 / 無効を設定します。「Disabled」（無効）に設定した場合、現在のマスタスイッチの優先度が 0 に変更され、新しいデバイスを現在のスタックトポロジに追加した場合でも、マスターとなるスイッチが変更されません。
Trap State	スタック関連の SNMP トラップの送信を有効 / 無効に設定します。
Stack ID	
Current Unit ID	スタックにおけるスイッチの現在のユニット番号を選択します。
New Box ID	「Current Unit ID」で選択したスタック内のスイッチに、新しくボックス番号を指定します。「Auto」を選択すると、自動的にボックス番号を割り当てます。 • 設定可能範囲：1-9
Priority	スイッチの優先度番号を指定します。低い値ほど高いプライオリティを示します。スタック内で最も低い優先度番号を持つボックス（スイッチ）が、プライマリマスタです。プライマリマスタスイッチは、スイッチスタックにおけるアプリケーションを設定するために使用されます。 • 設定可能範囲：1-63

「Apply」ボタンをクリックして、設定内容を適用します。

Stacking Bandwidth（スタッキング帯域）

スタッキング帯域の設定、表示を行います。

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

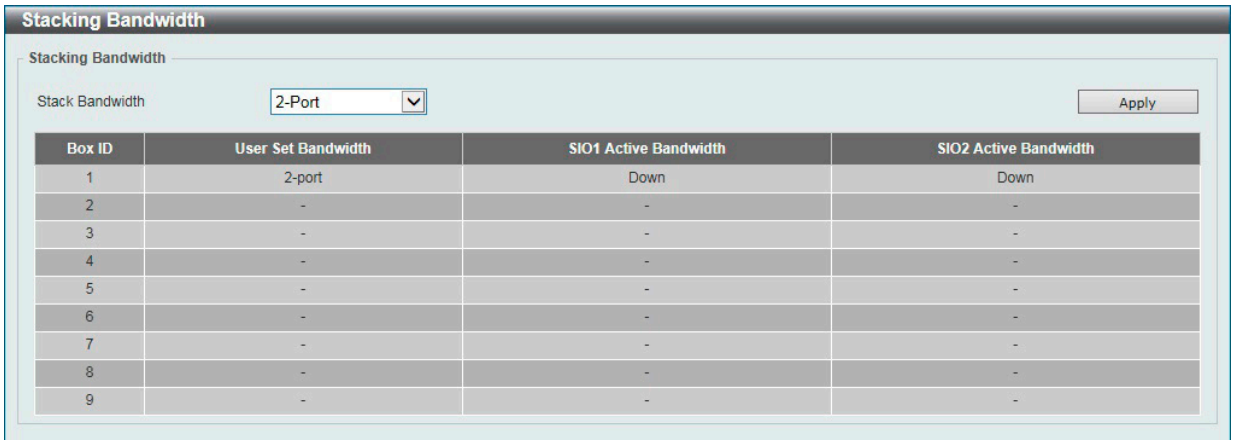


図 7-90　Stacking Bandwidth 画面

画面に表示される項目：

項目	説明
Stack Bandwidth	スタッキング帯域を指定します。 • 「2-Port」- スタックに 2 つのポートを使用します。 • 「4-Port」- スタックに 4 つのポートを使用します。

「Apply」ボタンをクリックして、設定内容を適用します。

シングル IP マネジメント（SIM）設定

シングル IP マネジメント（SIM）の設定を行います。

シングル IP マネジメント（SIM）の概要

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

- 帯域幅の需要の増加に対応するためにネットワークを拡張しつつ、小規模なワークグループや配線の管理を簡素化できます。
- ネットワークで必要な IP アドレスの数を減らすことができます。
- スタック接続のための特別なケーブル配線を必要としません。また、他のスタック技術ではトポロジ上の制限となり得る、距離的な問題を取り除きます。

シングル IP マネジメント（SIM）のルールと動作

D-Link シングル IP マネジメント（以下、SIM）機能を搭載するスイッチは、次のルールに従います。

- SIM はスイッチのオプション機能であり、CLI または Web インタフェース経由で簡単に有効 / 無効に設定することができます。また、SIM グループはネットワーク内のスイッチの通常動作に影響を与えることはありません。
- スイッチは 3 つの役割に分類されます。
  - **Commander Switch（CS）-** グループのマスタスイッチ
  - **Member Switch（MS）**- CS によって SIM グループのメンバとして認識されるスイッチ
  - **Candidate Switch（CaS）**- SIM グループに物理的にリンクはしているが、SIM グループのメンバとして認識されていないスイッチ
- SIM グループの Commander Switch（CS）は 1 台のみです。
- SIM グループには、最大 32 台のスイッチ（番号：1-32）が所属できます。（Commander Switch（番号：0）を除く）
- SIM グループ内のすべてのスイッチは、同じ IP サブネット内にある必要があります。
- 同じ IP サブネット内の SIM グループ数に制限はありませんが、各スイッチは 1 つの SIM グループにしか所属することができません。
- 複数の VLAN が設定されている場合、SIM グループはスイッチ上のデフォルト VLAN だけを使用します。
- SIM は SIM をサポートしていないデバイスを経由することができます。そのため CS から 1 ホップ以上離れたスイッチを管理することができます。

SIM グループは、1 つのエンティティとして管理されるスイッチのグループです。SIM スイッチは次の 3 つのいずれかの役割を持ちます。

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

2. **Member Switch（MS）**- SIM グループに所属し、CS からアクセスが可能なスイッチです。MS は以下の特徴を持っています。
   - 他の SIM グループの CS や MS ではない。
   - CS のマネジメント VLAN 経由で CS に接続する。

3. **Candidate Switch（CaS）**- SIM グループに参加する準備が整っているが、まだ MS ではないスイッチです。手動により SIM グループの MS として設定することで、SIM グループに参加させることができます。CaS として登録されたスイッチは、SIM グループには所属せず、以下の特長を持っています。
   - 他の SIM グループの CS や MS ではない。
   - CS のマネジメント VLAN 経由で CS に接続する。

これらの役割には、さらに以下のルールが適用されます。

- 各デバイスは、まず CaS の状態から始まります。
- CaS から CS への遷移
  - ユーザは、手動により CaS を CS に設定することができます。
- CS が SIM グループの MS になるには、CS → CaS → MS の順で遷移する必要があります。CS から MS へ直接遷移することはできません。
- CS から CaS への遷移
  - ユーザは、手動により CS を CaS に設定することができます。
- CaS から MS への遷移
  - ユーザは、CS を介して、手動により CaS を MS に設定することができます。
- MS から CaS への遷移
  - ユーザは、CS を介して、手動により MS を CaS に設定することができます。
  - CS から MS への Report パケットがタイムアウトになると、MS から CaS に遷移します。

SIM グループの CS として 1 台のスイッチを設定した後、追加のスイッチをグループの MS として登録することができます。設定後、CS は MS へのアクセス用インバンドエントリポイントとして動作します。CS の IP アドレスがグループのすべての MS への経路になり、CS の管理パスワードや認証によって、SIM グループのすべての MS へのアクセスが制御されます。

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

CS が MS に遷移すると、自動的に CS が所属する最初の SNMP コミュニティ（read/write 権限、read only 権限を含む）のメンバになります。MS が IP アドレスを持っている場合は、グループ内の他のスイッチ（CS を含む）が所属していない SNMP コミュニティに加入することができます。

バージョン 1.61 へのアップグレード

SIM 管理機能強化の目的で、本スイッチはバージョン 1.61 にアップグレードされています。本バージョンでは以下の改善点が加わりました。

1. CS は、再起動または Web の誤動作によって SIM グループから抜けたメンバスイッチを自動的に再検出する機能が搭載しました。この機能は、以前設定された SIM メンバが再起動の後に送受信する Discovery パケットと Maintain パケットを利用します。MS の MAC アドレスとパスワードが CS のデータベースに記録された状態で MS が再起動を行うと、CS はこの MS の情報をデータベースに保持し、MS が再検出された場合、この MS を SIM ツリーに自動的に戻します。これらのスイッチを再検出するために設定を行う必要はありません。

   保存済みの MS を再検出ができないケースもあります。例えば、スイッチの電源がオンになっていない場合、他のグループのメンバとなっている場合、または CS スイッチとして設定された場合は、再検出プロセスを実行することができません。

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

3. 本バージョンでは、以下のファームウェア / コンフィグレーションファイル / ログファイルのアップロードやダウンロードをサポートしました。

   - ファームウェア : TFTP サーバからの MS に対するファームウェアダウンロードがサポートされました。
   - コンフィグレーションファイル : TFTP サーバ経由の MS からのコンフィグレーションのダウンロード（バックアップ）/TFTP サーバ経由の MS へのコンフィグレーションのアップロード（リストア）が可能になりました。
   - ログ : MS のログファイルを TFTP サーバにアップロード可能になりました。

4. トポロジ画面を拡大、縮小して、より詳細に構成を確認することができます。

補足　SIM 状態が有効で、スイッチの役割状態がコマンダの場合、トポロジ、ファームウェアアップグレード、設定ファイルのバックアップ / 復元、およびログファイルのアップロード画面が使用可能になります。

Single IP Settings（シングル IP 設定）

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

Management > Virtual Stacking (SIM) >Single IP Settings の順にメニューをクリックし、以下の画面を表示します。

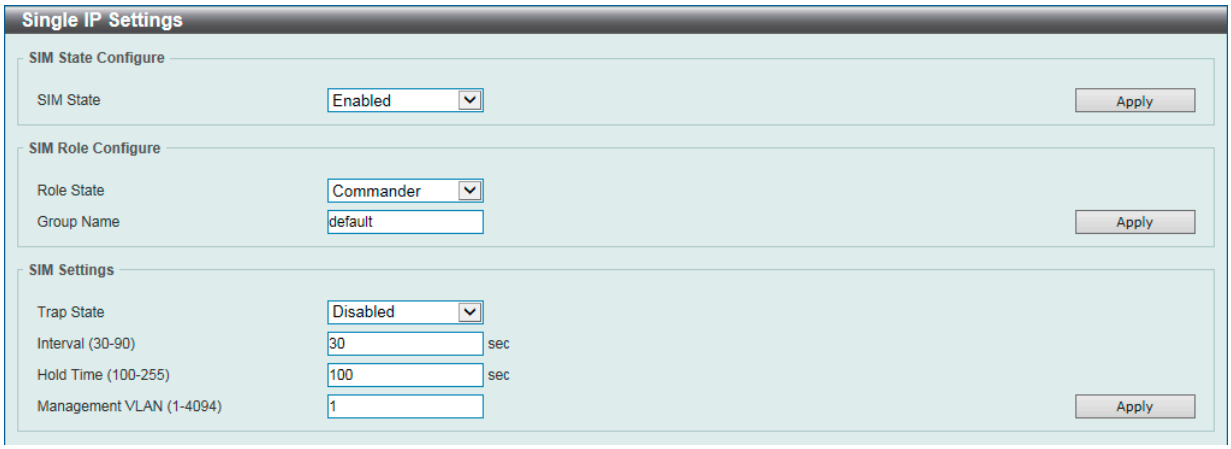


図 7-91　Single IP Settings 画面

画面に表示される項目：

項目	説明
SIM State Configure	
SIM State	SIM 機能を有効 / 無効に設定します。
SIM Role Configure	
Role State	スイッチの SIM での役割を選択します。 • 「Candidate」- Candidate Switch（CaS）は SIM グループメンバではありませんが、Commander スイッチに接続しています。（初期値） • 「Commander」- Commander Switch（CS）。他のスイッチを CS に参加させて SIM グループを作成することができます。また、このオプションを選択すると、本スイッチで SIM の設定が可能になります。
Group Name	SIM グループ名を入力します。複数の SIM グループでスイッチを管理する場合のオプションです。
SIM Settings	
Trap State	SIM トラップを有効 / 無効に設定します。
Interval	SIM 管理プロトコルのメッセージ送信間隔を設定します。 • 選択可能範囲：30-90（秒）
Hold Time	ホールド時間を指定します。 SIM メッセージを受信せずに指定時間経過すると、コマンダまたはメンバスイッチは他のスイッチの情報を消去します。 • 選択可能範囲：100-255（秒）
Management VLAN	シングル IP マネージメントメッセージの VLAN ID を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

SIM 機能を有効化し、スイッチを CS（「コマンダ」スイッチ）として登録すると、「Single IP Management」メニュー配下には 4 つのリンクが追加され、Web を使用した SIM 設定ができるようになります。

CS スイッチで設定可能なメニューリンク：

- 「Topology」
- 「Firmware Upgrade」
- 「Configuration File Backup/Restore」
- 「Upload Log File」

Topology（トポロジ）

SIM グループ内のスイッチの設定および管理を行います。本画面を表示するためには、ご使用のコンピュータに Java の実行環境が必要です。

Management > Virtual Stacking (SIM) > Topology の順にメニューをクリックします。以下の画面が表示されます。

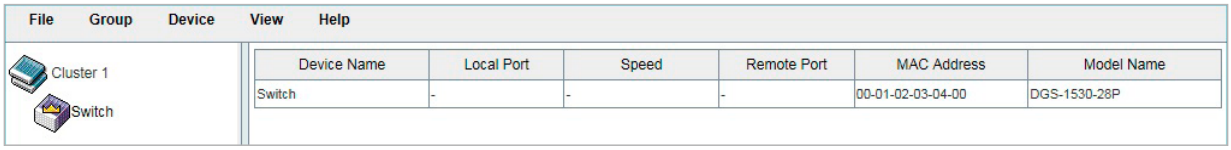


図 7-92　トポロジ画面

トポロジ画面には、デバイスの設定のために以下のようなメニューバーが配置されています。

図 7-93　トポロジメニューバー

「File」メニュー

■ Print Topology（トポロジの印刷）

トポロジマップを印刷します。

■ Preference（優先度）

ポーリング間隔（interval）などの表示プロパティを設定します。

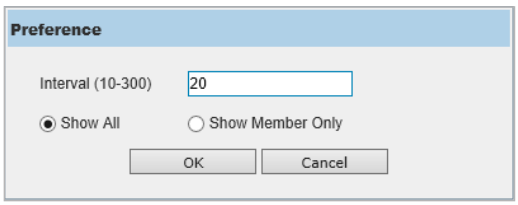


図 7-94　Preference 画面

以下の項目が使用できます。

項目	説明
Interval	SIM トポロジ表示の更新間隔を指定します。 • 設定可能範囲：10-300
Show All	トポロジ内の全ての有効な SIM デバイスを表示します。
Show Member Only	トポロジ内の SIM メンバデバイスのみを表示します。

「OK」ボタンをクリックして、設定を適用します。
「Cancel」ボタンをクリックすると、変更した設定内容は破棄されます。

「Group」メニュー

■ Add to Group（グループに追加）

リストからキャンディデートスイッチ（CaS）を選択し、本項目（**Group > Add to Group**）を選択します。

CaS を SIM グループに追加するには、当該スイッチのパスワード認証を行う必要があります。
パスワードを入力して「Apply」をクリックするか、「キャンセル」をクリックして画面を閉じます。

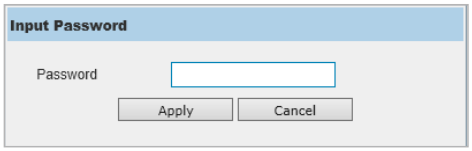


図 7-95　Input password 画面

■ Remove from Group（グループから削除）

リストからメンバスイッチ（MS）を選択し、本項目（**Group > Remove from Group**）を選択します。MS をグループから削除します。

「Device」メニュー

■ Configure（設定）

リストからデバイスを選択し、本項目（**Device > Configure**）を選択します。指定したデバイスの Web マネージャを開きます。

「View」メニュー

■ Refresh（更新）

表示されている情報を最新の状態に更新します。

■ Topology（トポロジ）

トポロジビューを表示します。

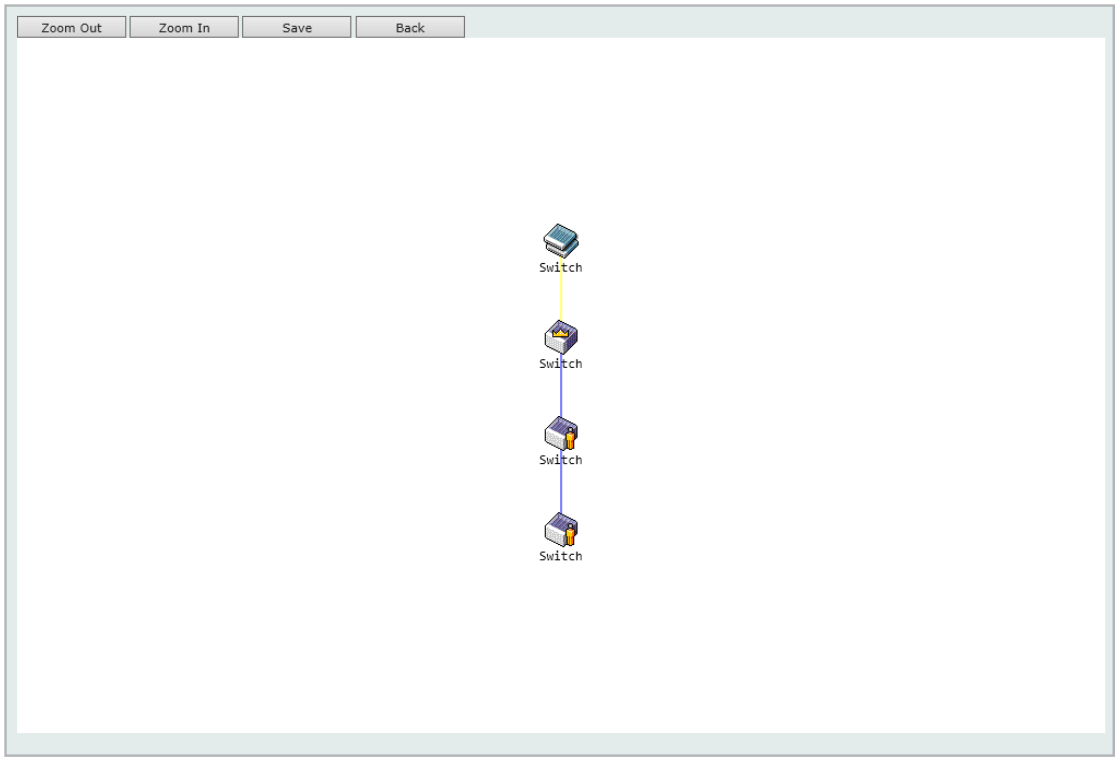


図 7-96　View >Topology 画面

「Zoom In」をクリックすると表示アイテムが拡大します。
「Zoom Out」をクリックすると表示アイテムが縮小します。
「Save」をクリックすると表示が保存されます。
「Back」をクリックすると前画面に戻ります。

本画面は、SIM グループ内のデバイスが他のグループやデバイスとどのように接続しているかを表示します。

本画面で表示されるアイコンは以下の通りです。

アイコン	説明
	グループ
	レイヤ 2 Commander スイッチ
	レイヤ 3 Commander スイッチ
	他のグループの Commander スイッチ
	レイヤ 2 Member スイッチ
	レイヤ 3 Member スイッチ

アイコン	説明
	他のグループの Member スイッチ
	レイヤ 2 Candidate スイッチ
	レイヤ 3 Candidate スイッチ
	不明なデバイス
	SIM 非対応のデバイス

ツールヒント

トポロジビュー画面では、マウスはデバイス情報の確認と設定のために重要な役割を果たします。トポロジ画面の特定のデバイス上にマウスポインタを置くと、ツリービューと同様にデバイス情報（ツールヒント）を表示します。以下にその例を示します。

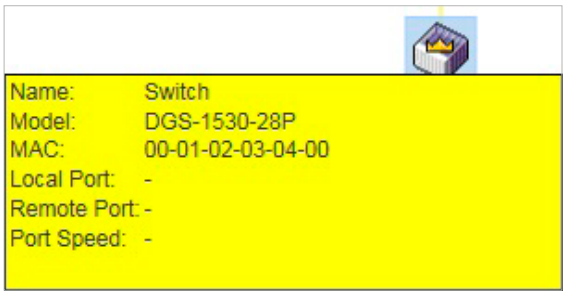


図 7-97　ツールヒントを利用したデバイス情報の表示

2 つのデバイスの間のライン上でマウスポインタを静止させると、以下の図のようにデバイス間の接続速度を表示します。

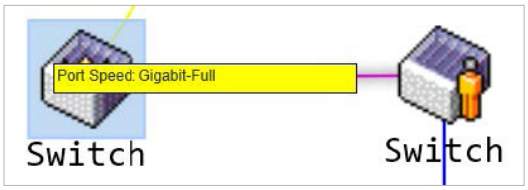


図 7-98　ツールヒントを利用したポート速度の表示

右クリックメニュー

デバイスのアイコン上で右クリックすると、スイッチのプロパティの表示や機能の設定、グループへの追加 / 削除を実行できます。

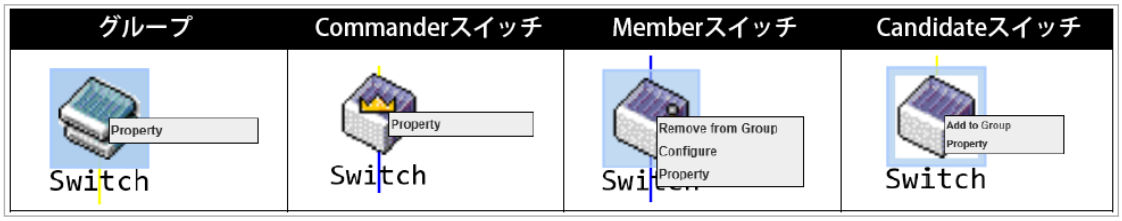


図 7-99　各アイコン上での右クリック

画面に表示される項目：

項目	説明
Property	ポップアップ画面が開き、デバイスの情報を表示します。
Configure	（Member スイッチのみ） Web 管理機能を起動して、スイッチの設定を行うことができます。
Add to group	（Candidate スイッチのみ） CaS をグループに追加します。CaS スイッチを SIM グループに追加するには、パスワード認証を行う必要があります。
Remove from Group	（Member スイッチのみ） メンバをグループから削除します。

■ 「Property」

図 7-100　Property 画面

画面に表示される項目：

項目	説明
Name	SIM グループ内のスイッチのデバイス名を表示します。
Model	スイッチのモデル名を表示します。
MAC Address	スイッチの MAC アドレスを表示します。

項目	説明
Local Port	MS または CaS が接続している CS の物理ポートの番号を表示します。CS の場合は何も表示されません。
Remote Port	CS が接続している MS または CaS の物理ポートの番号を表示します。CS の場合は何も表示されません。
Port Speed	CS と MS/CaS 間の接続スピードを表示します。

「Help」メニュー

- **About（概要）**

SIM の Copyright 情報とリリース日を表示します。

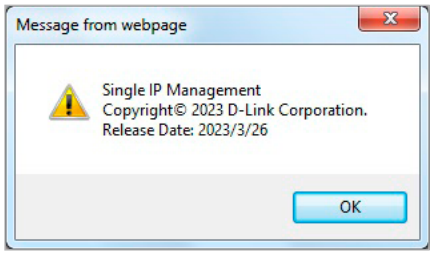


図 7-101　About 画面

Firmware Upgrade（ファームウェア更新）

CS から MS へのファームウェアの更新を行います。

Management > Virtual Stacking (SIM) >Firmware Upgrade の順にメニューをクリックし、以下の画面を表示します。

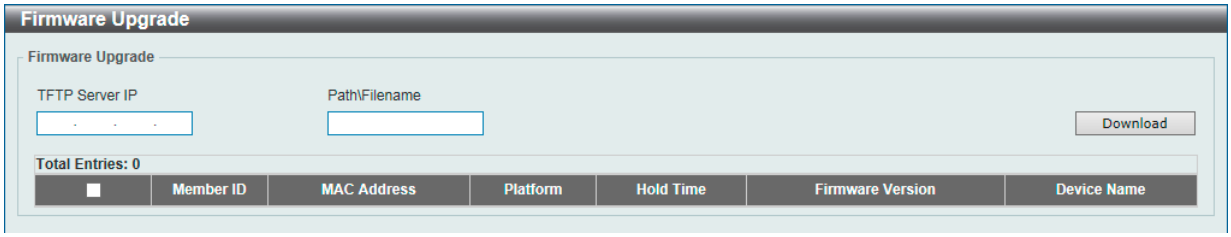


図 7-102　Firmware Upgrade 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。
Path\Filename	パスとファイル名を入力します。

「Download」ボタンをクリックして、ファームウェアを更新します。
特定のスイッチをファームウェア更新対象として指定するには、対応するチェックボックスをオンにします。

Configuration File Backup/ Restore（コンフィグレーションファイルのバックアップ / リストア）

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

Management > Virtual Stacking (SIM) >Configuration File Backup/Restore の順にメニューをクリックし、以下の画面を表示します。

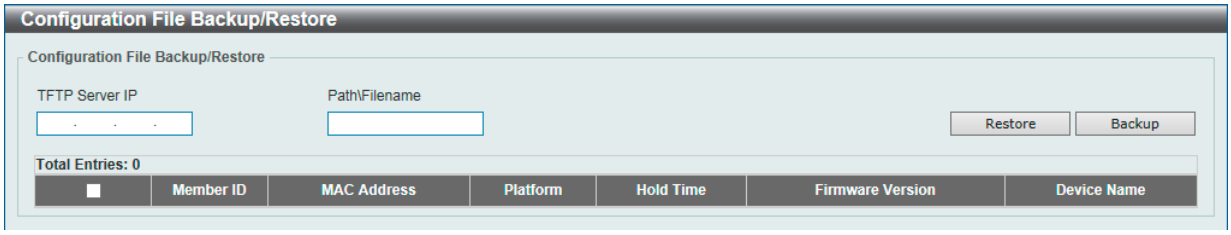


図 7-103　Configuration File Backup/Restore 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。
Path\Filename	パスとファイル名を入力します。

「Restore」ボタンをクリックして、TFTP サーバからメンバスイッチへのコンフィグレーションのリストアを実行します。
「Backup」ボタンをクリックして、TFTP サーバへバックアップファイルを保存します。

Upload Log File（ログファイルのアップロード）

SIM メンバスイッチから指定した PC へログファイルのアップロードを行います。

Management > Virtual Stacking (SIM) >Upload Log File の順にメニューをクリックし、以下の画面を表示します。

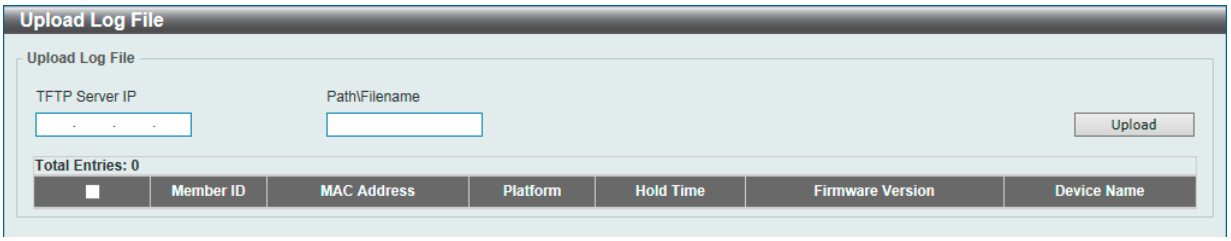


図 7-104　Upload Log File 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。
Path\Filename	パスとファイル名を入力します。

「Upload」ボタンをクリックして、TFTP サーバへログファイルをアップロードします。

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

DDP Settings

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 > DDP 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。

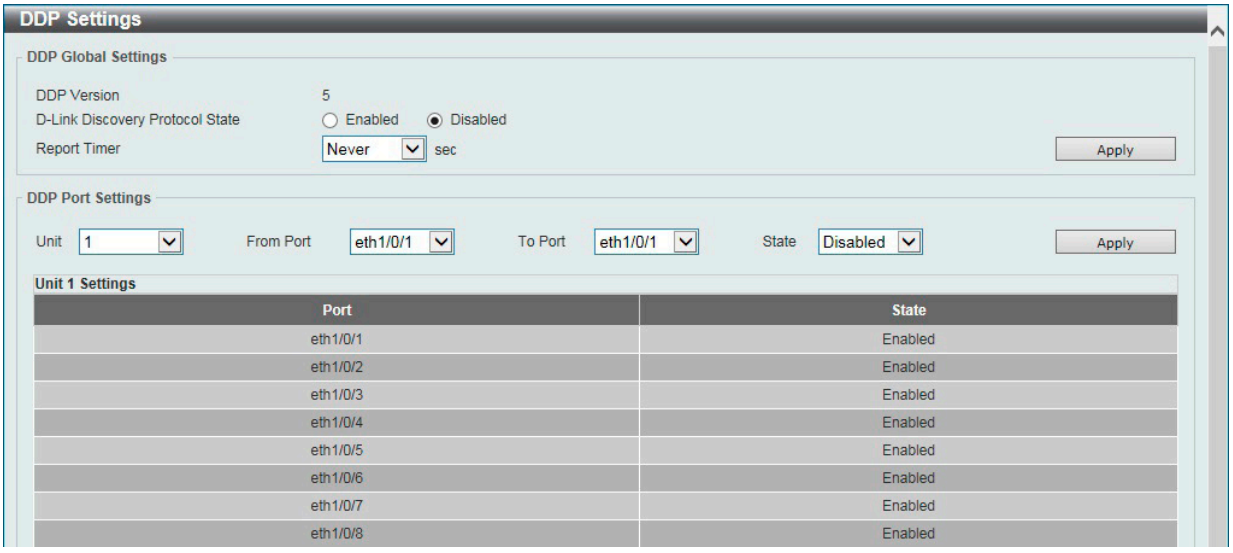


図 7-105　DDP Settings 画面

画面に表示される項目：

項目	説明
D-Link Global Settings	
D-Link Discovery Protocol State	DDP のグローバルステータスを有効 / 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を以下から指定します。 ・「30」「60」「90」「120」「Never」（秒） 「Never」を選択した場合、レポートメッセージの送信は停止されます。
DDP Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートの DDP 機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

DDP Neighbors（DDP 隣接機器）

DDP 隣接機器の表示を行います。

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

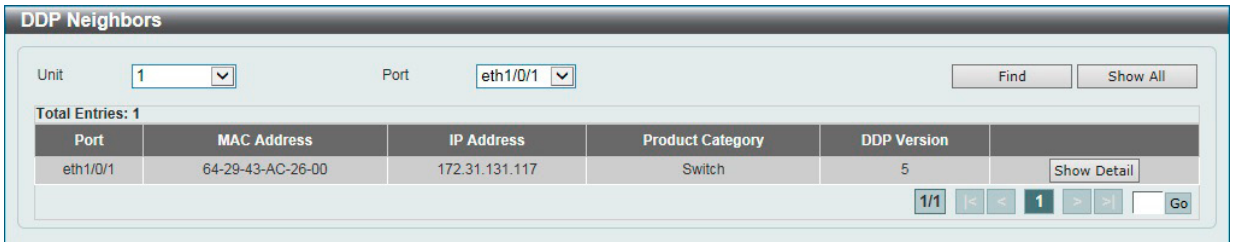


図 7-106　DDP Neighbors 画面

画面に表示される項目：

項目	説明
Unit	検出対象のユニットを選択します。
Port	検出対象のポートを選択します。

「Find」ボタンをクリックして、指定したポートを介して接続している DDP 隣接機器を表示します。
「Show All」ボタンをクリックして、本スイッチに接続しているすべての DDP 隣接機器を表示します。
「Show Detail」ボタンをクリックして、エントリの詳細情報を表示します。

「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。

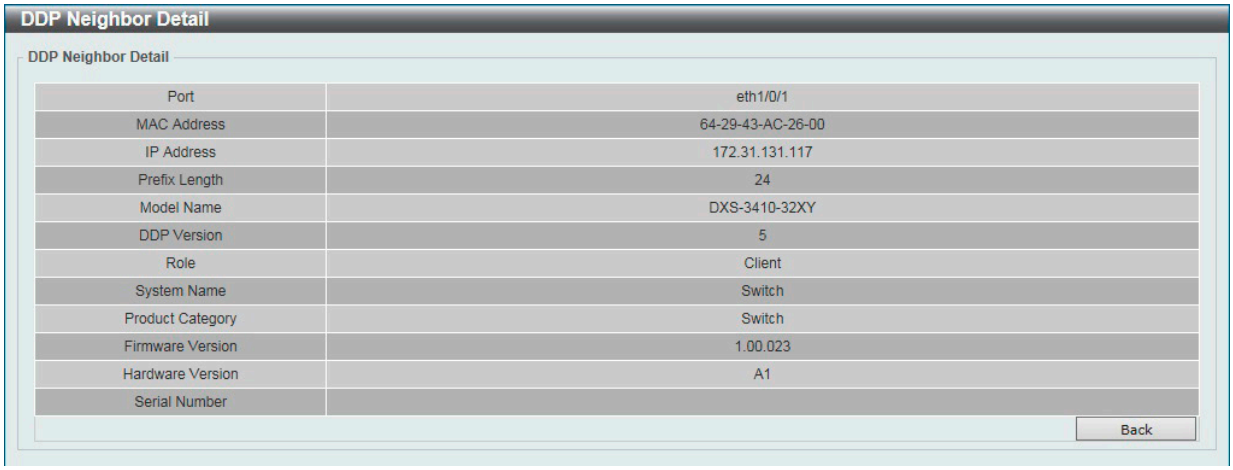


図 7-107　DDP Neighbors (Show Detail) - DDP Neighbor Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

SMTP Settings（SMTP 設定）

Simple Mail Transfer Protocol (SMTP) 設定の表示、構成を行います。

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

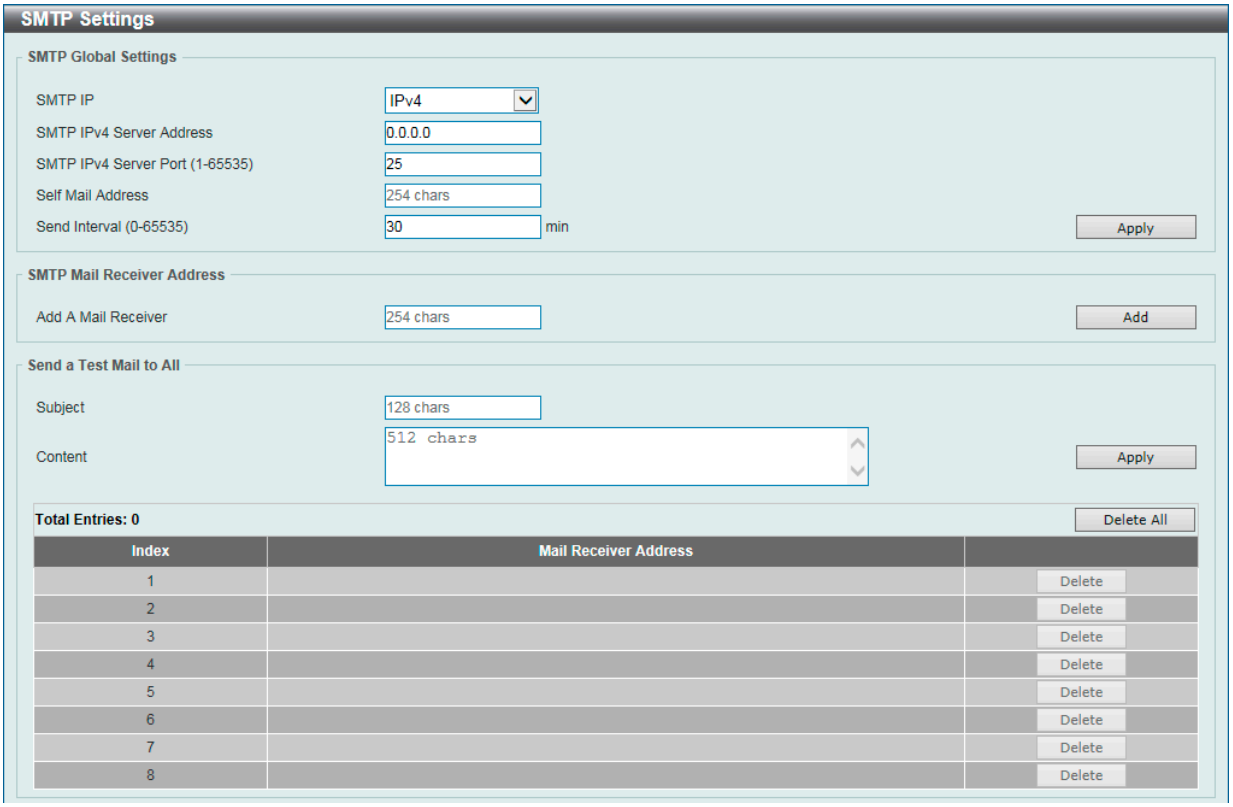


図 7-108　SMTP Settings 画面

画面に表示される項目：

SMTP Global Settings

項目	説明
SMTP IP	SMTP サーバ IP アドレスタイプを指定します。 • 選択肢：「IPv4」「IPv6」
SMTP IPv4 Server Address	IP アドレスタイプで「IPv4」を選択した場合、SMTP サーバの IPv4 アドレスを指定します。
SMTP IPv6 Server Address	IP アドレスタイプで「IPv6」を選択した場合、SMTP サーバの IPv6 アドレスを指定します。
SMTP IPv4 Server Port	IP アドレスタイプで「IPv4」を選択した場合、SMTP IPv4 サーバポート番号を指定します。 • 設定可能範囲：1-65535 • 初期値：25
SMTP IPv6 Server Port	IP アドレスタイプで「IPv6」を選択した場合、SMTP IPv6 サーバポート番号を指定します。 • 設定可能範囲：1-65535 • 初期値：25
Self Mail Address	スイッチの E メールアドレスを指定します。（254 文字以内）
Send Interval	送信間隔を指定します。 • 設定可能範囲：0-65535（分） • 初期値：30（分）

「Apply」ボタンをクリックして、設定内容を適用します。

SMTP Mail Receiver Address

項目	説明
Add A Mail Receiver	受信者の E メールアドレスを指定します。（254 文字以内）

「Add」ボタンをクリックして、エントリを追加します。
画面下部のテーブル上で、該当エントリの「Delete」ボタンをクリックして、エントリを削除します。
「Delete All」ボタンをクリックして、画面下部のテーブル上のすべてのエントリを削除します。

Send a Test Mail to All

項目	説明
Subject	E メールの件名を指定します。（128 文字以内）
Content	E メールの内容を指定します。（512 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

Reboot Schedule Settings（再起動スケジュール設定）

スイッチの再起動スケジュール設定を行います。

Management > Reboot Schedule 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。

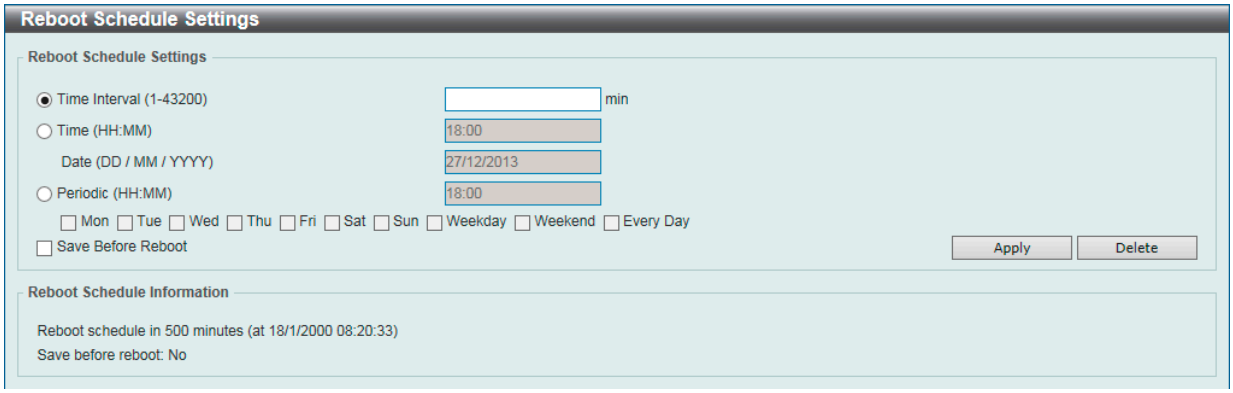


図 7-109　Reboot Schedule Settings 画面

画面に表示される項目：

項目	説明
Time Interval	本項目を選択した場合、指定の時間経過後にスイッチの再起動が実行されます。 • 設定可能範囲：1 - 43200（分）（30 日）
Time/Date	本項目を選択した場合、再起動スケジュールを日時で指定します。 スイッチが再起動する時刻を「HH:MM」形式（例：21:30）で指定します。 • 「Date」- スイッチが再起動する日付を指定します。入力形式は「DD/MM/YYYY」（例：23/12/2015）です。 日付が指定されていない場合、次の 24 時間以内の指定時間に再起動が実行されます。
Periodic	本項目を選択した場合、再起動スケジュールを定期スケジュールで指定します。 スイッチが再起動する時刻を「HH:MM」形式（例：21:30）で指定し、再起動を繰り返し実行する曜日を指定します。
Save Before Reboot	本オプションにチェックを入れた場合、再起動実行前に、変更されたすべての設定内容を保存します。

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

NLB FDB Settings（NLB FDB 設定）

本スイッチはネットワークロードバランシング (NLB) をサポートしています。本機能は、複数のサーバが同じ IP アドレスと MAC アドレスを共有する Microsoft サーバロードバランシングアプリケーションをサポートするために使用されます。クライアントからの要求はすべてのサーバに転送されますが、そのうちの 1 つによってのみ処理されます。サーバは、2 つの異なるモードで動作可能です。

- ユニキャストモード：クライアントはユニキャスト MAC アドレスをサーバへの宛先 MAC として使用します。
- マルチキャストモード：クライアントはマルチキャスト MAC アドレスをサーバへの宛先 MAC として使用します。

この宛先 MAC アドレスは、共有 MAC アドレスと呼ばれます。ただし、サーバは応答パケットの送信元 MAC アドレスとして（共有 MAC アドレスではなく）自身の MAC アドレスを使用します。つまり、NLB ユニキャストアドレスは通常、パケットの送信元 MAC アドレスではありません。

受信したパケットに、設定されたユニキャスト MAC アドレスと一致する宛先 MAC アドレスが含まれている場合、VLAN メンバシップ設定に関係なく、指定のポートに転送されます。

管理者は、MAC アドレステーブルのスタティックアドレスを NLB アドレスとして設定することはできません。ただし、MAC アドレスが NLB MAC アドレスエントリとして作成されている場合、同じ MAC アドレスをレイヤ 2 MAC アドレステーブルで動的に学習できます。この場合、NLB の方が優先順位が高くなり、動的に学習された FDB エントリは有効になりません。

注意 物理スタックしているスイッチにおいて、L3 の NLB を行っているサーバを筐体またぎの LAG（リンクアグリゲーショングループ）では接続できません。物理スタックとの併用は、しないでください。

Management > NLB FDB 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。

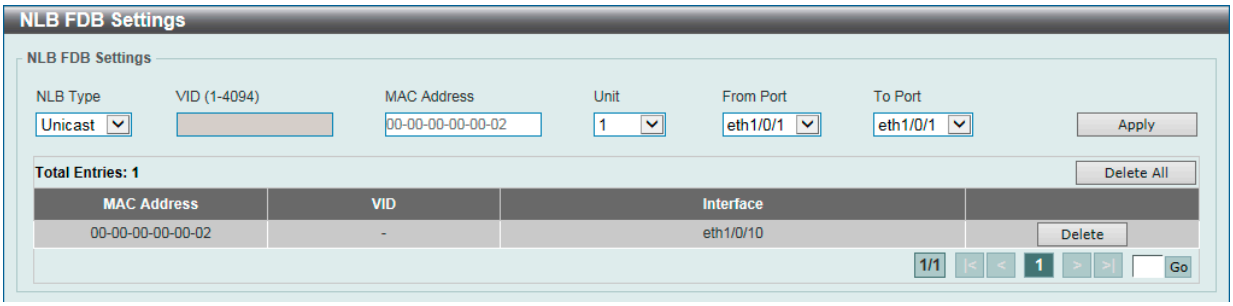


図 7-110　NLB FDB Settings 画面

画面に表示される項目：

項目	説明
NLB Type	NLB タイプを指定します。 • 選択肢：「Unicast」「Multicast」
VID	「Multicast」を選択した場合、この設定で使用される VLAN ID を入力します。
MAC Address	エントリのユニキャストまたはマルチキャスト MAC アドレスを入力します。受信したパケットに、指定された MAC アドレスと一致する宛先 MAC アドレスが含まれている場合、指定されたインタフェースに転送されます。
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Delete All」ボタンをクリックして、すべてのエントリを削除します。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

PPPoE Circuit ID Insertion Settings（PPPoE 回線 ID 挿入設定）

PPPoE 回線 ID 挿入機能の設定を行います。

Management > PPPoE Circuit ID Insertion 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。

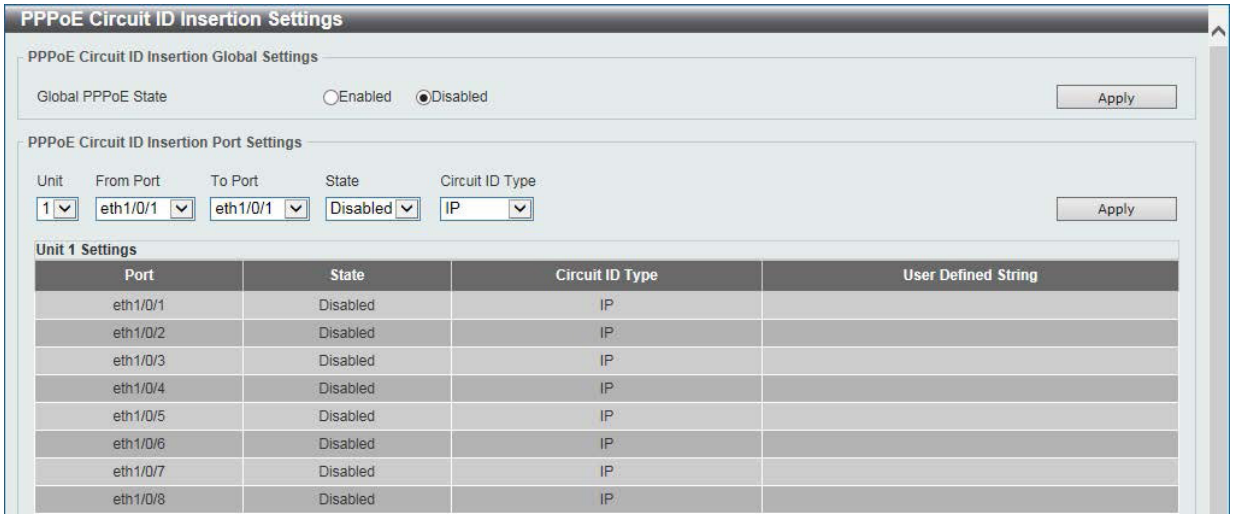


図 7-111　Reboot Schedule Settings 画面

画面に表示される項目：

項目	説明
PPPoE Circuit ID Insertion Global Settings	
Global PPPoE State	PPPoE 回線 ID 挿入をスイッチで有効 / 無効に設定します。
PPPoE Circuit ID Insertion Ports Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートの PPPoE 回線 ID 挿入を有効 / 無効に設定します。
Circuit ID Type	回線 ID オプションのエンコーディングで使用するデバイス ID を選択します。「UDF」を選択した場合、ユーザ定義文字列を指定します。（32 文字以内） • 選択肢：「IP」「MAC」「UDF」「Vendor5」

「Apply」ボタンをクリックして、設定内容を適用します。

TCP Path MTU Discovery（TCP パス MTU 検出）

IP TCP パス MTU 変換の設定を行います。

Management > TCP Path MTU Discovery 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 7-112　TCP Path MTU Discovery 画面

画面に表示される項目：

項目	説明
TCP Path MTU Discovery State	TCP パス MTU の変換を有効 / 無効に設定します。
Age Time	エージングタイムを設定します。「Infinite」にチェックを入れると本機能を無効にします。 • 設定可能範囲：1 - 30（分） • 初期値：10（分）

「Apply」ボタンをクリックして、設定内容を適用します。

TCP Selective ACK（TCP 選択的確認応答）

TCP 選択的確認応答の設定を行います。

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

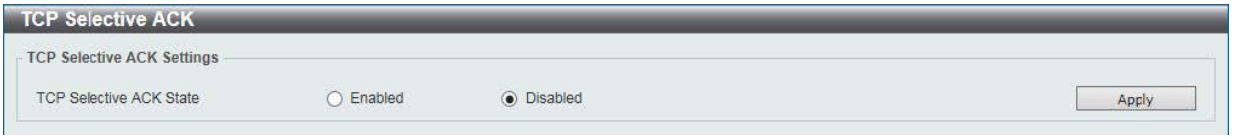


図 7-113　TCP Selective ACK 画面

画面に表示される項目：

項目	説明
TCP Selective ACK State	TCP 選択的確認応答をスイッチで有効 / 無効にします。

「Apply」ボタンをクリックして、設定内容を適用します。

TWAMP（TWAMP 設定）

TWAMP Settings（TWAMP 設定）

Two-Way Active Measurement Protocol（TWAMP）の設定を行います。

Management > TWAMP > TWAMP 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。

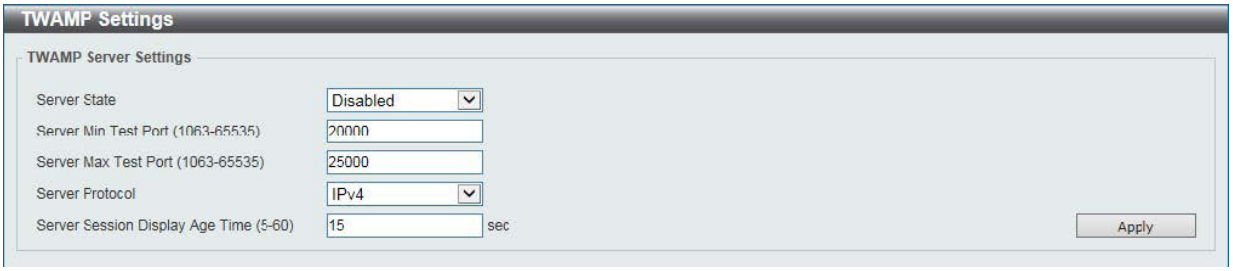


図 7-114　TWAMP Settings 画面

画面に表示される項目：

項目	説明
Server State	TWAMP サーバを有効 / 無効に設定します。
Server Min Test Port	テストポート番号の最小値を指定します。 • 設定可能範囲：1063 - 65535 • 初期値：20000
Server Max Test Port	テストポート番号の最大値を指定します。 • 設定可能範囲：1063 - 65535 • 初期値：25000
Server Protocol	TWAMP サーバのプロトコルタイプを選択します。 • 選択肢：「IPv4」「IPv6」
Server Session Display Age Time	TWAMP クライアントセッションの表示エージングタイムを設定します。 • 設定可能範囲：5 - 60（秒） • 初期値：15（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

TWAMP Server Connections（TWAMP サーバ接続）

TWAMP サーバの接続について表示します。

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

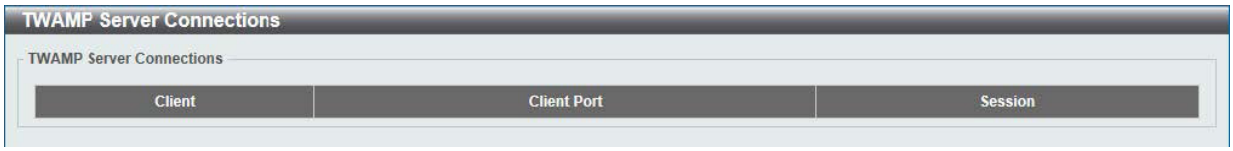


図 7-115　TWAMP Server Connections 画面

TWAMP Server Sessions

TWAMP サーバのセッションについて表示します。

Management > TWAMP > TWAMP Server Sessions 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 7-116　TWAMP Server Sessions 画面

画面に表示される項目：

項目	説明
IP Address	宛先ホストの IPv4 アドレスを入力します。
IPv6 Address	宛先ホストの 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エントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。
「Clear All」ボタンをクリックして、テーブル上のすべてのエントリをクリアします。

複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

第 8 章　L2 Features（L2 機能の設定）

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

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

サブメニュー	説明
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 スタティック VLAN の設定を行います。
VLAN Tunnel（VLAN トンネル）	802.1Q VLAN トンネルの設定を行います。
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) の表示、設定を行います。 ERPS 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。
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機能）の設定を行います。
Flex Links（フレックスリンク）	フレックスリンク機能の設定を行います。
L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）	L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）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（Internet Group Management Protocol）Snooping 機能始めとした L2 Multicast Control（L2 マルチキャストコントロール）の設定を行います。
LLDP	Link Layer Discovery Protocol（LLDP）の設定を行います。

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。

補足　FDB で登録可能な MAC アドレス数は 16K です。（スタティック：1K）

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。

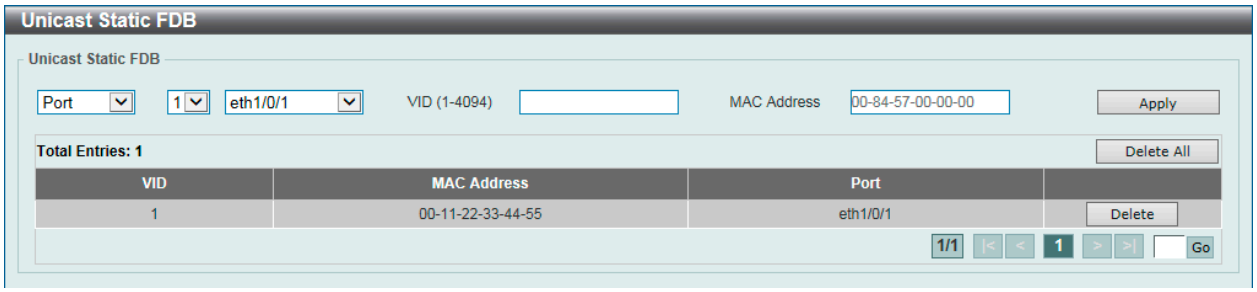


図 8-1　Unicast Static FDB 画面

画面に表示される項目：

項目	説明
Port/Drop	指定 MAC アドレスのあるポート番号を指定します。 また、本オプションはユニキャストのスタティック FDB から MAC アドレスを削除することもできます。 • 「Port」- 指定 MAC アドレスのあるユニット / 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。
Unit	「Port」を選択した場合、本設定を適用するユニットを選択します。
Port Number	「Port」を選択した場合、本設定を適用するポート番号を入力します。
VID	指定のユニキャスト MAC アドレスが所属する VLAN ID を入力します。
MAC Address	ユニキャストパケットが送信される宛先の MAC アドレスを入力します。または、破棄する MAC アドレスを入力します。 ユニキャスト MAC アドレスを指定する必要があります。

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

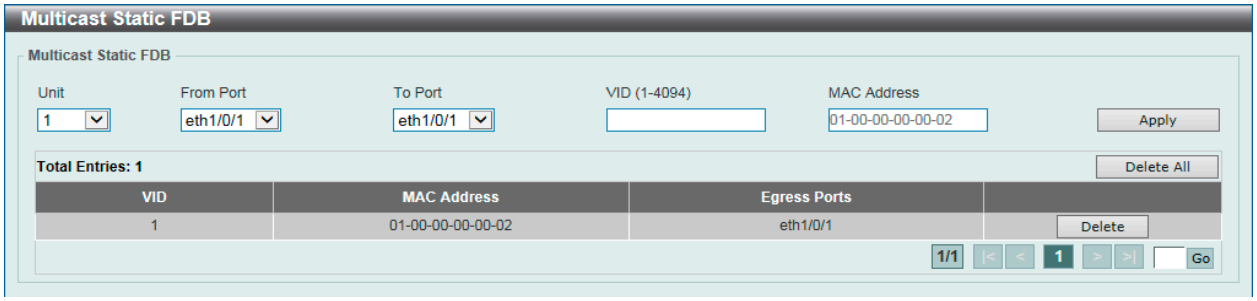


図 8-2　Multicast Static FDB 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。

項目	説明
VID	指定のマルチキャスト MAC アドレスが所属する VLAN の VLAN ID を入力します。
MAC Address	マルチキャストパケットが送信される宛先の MAC アドレスを入力します。マルチキャスト MAC アドレスを指定する必要があります。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Delete All」ボタンをクリックすして、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 アドレステーブルの設定を行います。

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

Global Settings（グローバル設定タブ）

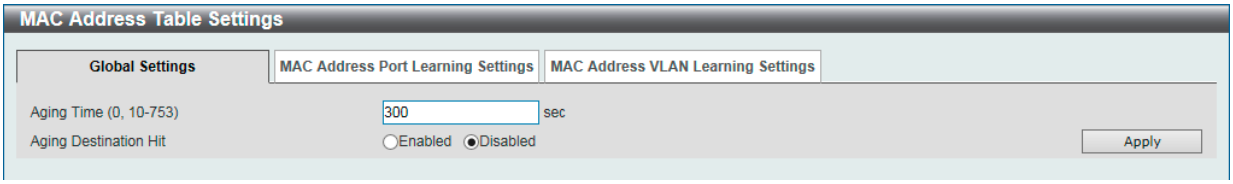


図 8-3　MAC Address Table Settings 画面 - Global Settings タブ

画面に表示される項目：

項目	説明
Aging Time	MAC アドレステーブルのエージングタイムを入力します。 設定した時間内にアクセスのない端末について、学習した MAC アドレスを MAC アドレステーブルから削除します。 • 設定可能範囲：0，10-753（秒） • 初期値：300（秒） 0 に設定した場合、学習した MAC アドレスは削除されません。
Aging Destination Hit	送信元 MAC アドレスだけでなく、宛先 MAC アドレスによる MAC アドレステーブルの更新を有効 / 無効に設定します。MAC アドレスのエージングタイムアウトによるフラッディングを抑えることができます。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　Vlan インタフェース毎に異なる MAC アドレスを使用します。

MAC Address Port Learning Settings（MAC アドレスポート学習設定タブ）

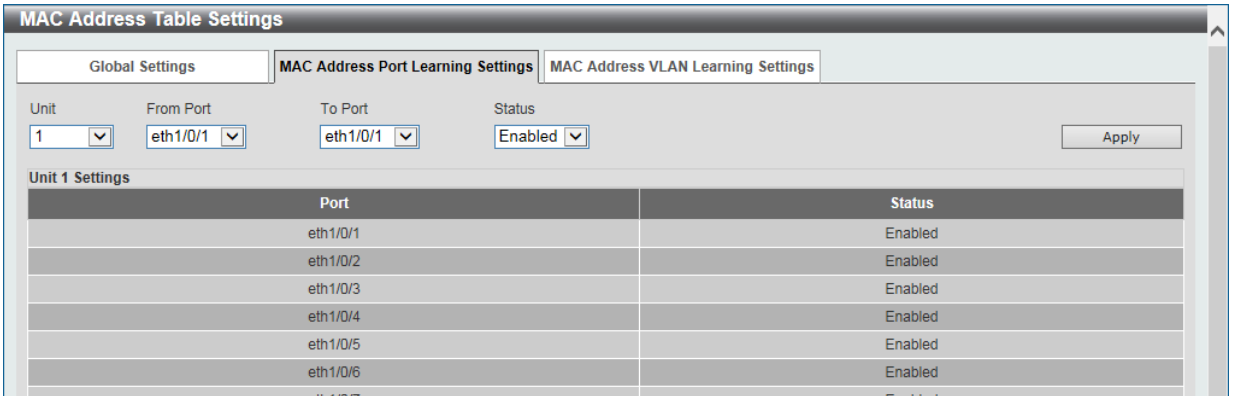


図 8-4　MAC Address Table Settings 画面 - MAC Address Port Learning Settings タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Status	指定したポートの MAC アドレス学習を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

MAC Address VLAN Learning Settings（MAC アドレス VLAN 学習設定タブ）

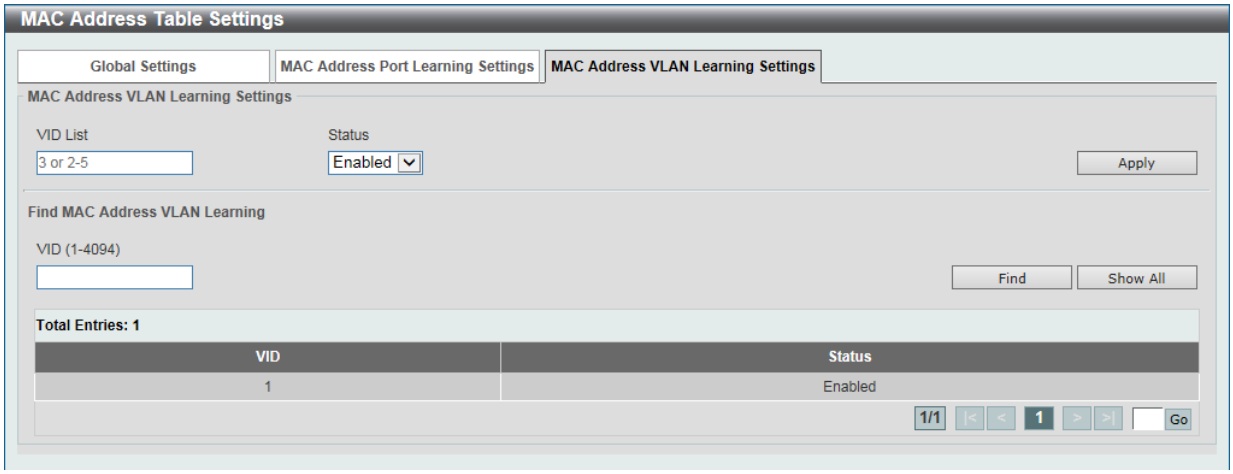


図 8-5　MAC Address Table Settings 画面 - MAC Address VLAN Learning Settings タブ

画面に表示される項目：

項目	説明
MAC Address VLAN Learning Settings	
VID List	本設定を適用する VLAN ID を入力します。 複数の VLAN ID をカンマで区切って入力、または VLAN ID の範囲をハイフンで区切って入力することも可能です。
Status	指定した VLAN の MAC アドレス学習を有効 / 無効に設定します。
Find MAC Address VLAN Learning	
VID	VLAN ID を入力してエントリを表示します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての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。

MAC Address Table（MAC アドレステーブル）

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。

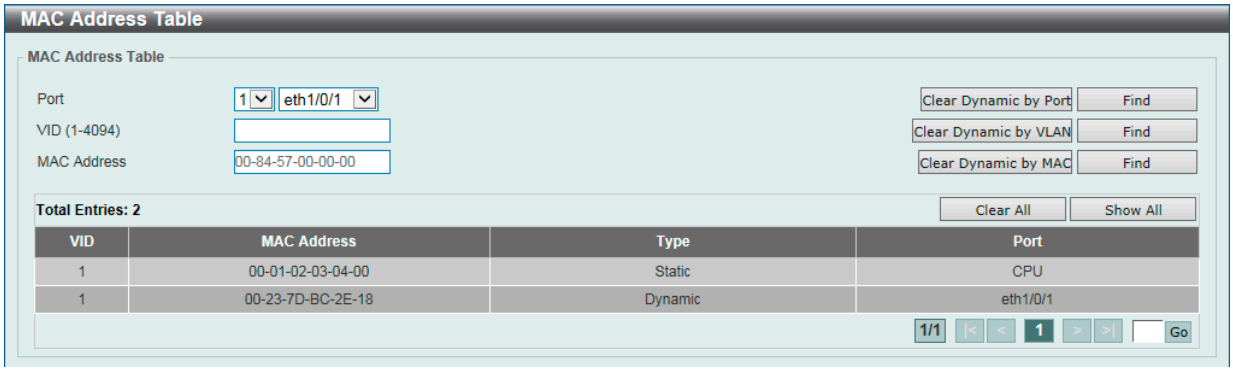


図 8-6　MAC Address Table 画面

画面に表示される項目：

項目	説明
Port	削除 / 表示するエントリのユニット ID およびポート番号を指定します。
VID	削除 / 表示するエントリの VLAN ID を入力します。
MAC Address	削除 / 表示するエントリの MAC アドレスを入力します。

エントリの検索 / 表示

「Find」ボタンをクリックして、指定した条件を基にエントリを検索します。
「Show 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。

ダイナミックエントリの削除

「Clear Dynamic Entries（by Port/by VLAN/by MAC）」ボタンをクリックして、指定した条件を基に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。
「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ダイナミックエントリを削除します。

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。

MAC Notification（MAC 通知）

MAC 通知のグローバル設定を行います。また、スイッチの各ポートに MAC 通知を設定します。

MAC Notification Settings タブ

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

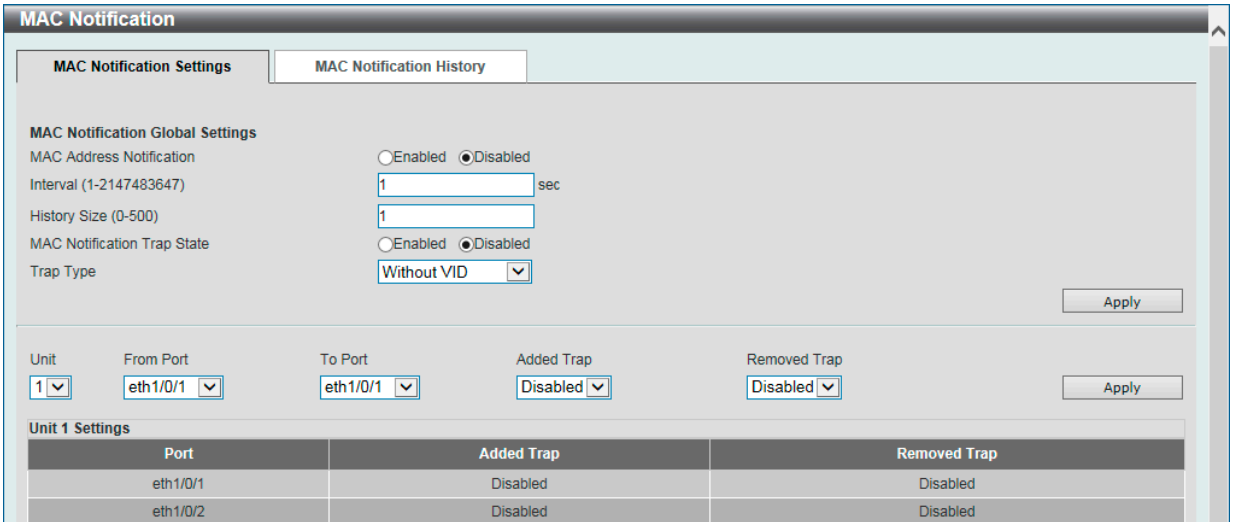


図 8-7　MAC Notification 画面 - MAC Notification Settings タブ

画面に表示される項目：

項目	説明
MAC Notification Global Settings	
MAC Address Notification	MAC 通知のグローバルステータスを有効 / 無効に設定します。
Interval	通知を行う間隔を指定します。 • 設定可能範囲：1-2147483647（秒） • 初期値 : 1（秒）
History Size	通知用に使用するヒストリログの最大エントリ数を指定します。 • 設定可能範囲：0-500 • 初期値 : 1
MAC Notification Trap State	MAC 通知トラップを有効 / 無効に設定します。
Trap Type	トラップタイプを選択します。 • 「Without VID」- トラップ情報に VLAN ID を含めません。 • 「With VID」- トラップ情報に VLAN ID を含めます。
ポート設定	
Unit	本設定を適用するユニットを選択します。
From Port /To Port	本設定を適用するポートを指定します。
Added Trap	選択したポートの追加トラップを有効 / 無効に設定します。
Removed Trap	選択したポートの削除トラップを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

MAC Notification History タブ

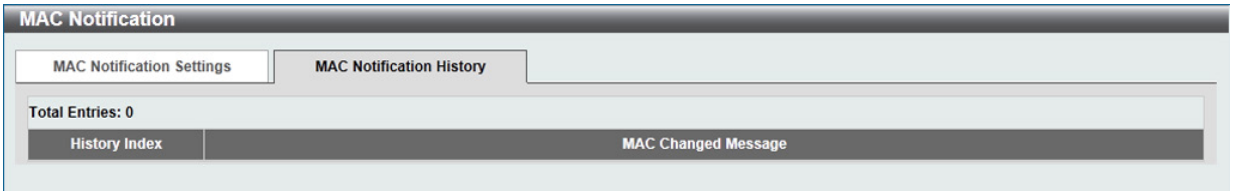


図 8-8　MAC Notification 画面 - MAC Notification History タブ

MAC 通知メッセージの履歴が表示されます。

VLAN について

IEEE 802.1p プライオリティについて

IEEE 802.1p 標準規格で定義されるプライオリティタグ機能では、多くの異なる種類のデータが同時に送受信されるようなネットワークにおいてトラフィックを制御することができます。本機能は、混雑したネットワーク上でのタイムクリティカルなデータの伝送時に発生する問題を解決するために開発されました。例えばビデオ会議のような、タイムクリティカルなデータに依存するタイプのアプリケーションの品質は、わずかな伝送遅延にも多大な影響を受けてしまいます。

IEEE 802.1p 標準規格に準拠するネットワークデバイスは、データパケットのプライオリティレベル（優先度）を認識することができます。また、これらのデバイスでは、パケットに対してプライオリティレベルやタグを割り当てたり、パケットからタグを取り外したりすることも可能です。このプライオリティタグ（優先タグ）により、パケットの緊急度および送信キューが決定します。

プライオリティタグは 0 から 7 までの値で設定され、0 が最も低い優先度、7 が最も高い優先度を表します。一般的にプライオリティ値「7」は、伝送遅延に影響を受けやすい音声・映像に関連するデータや、データ転送速度が保証されているような特別なユーザに対して使用されます。

本スイッチでは、プライオリティタグ付きのパケットをどのように扱うかを細かく調整することができます。キューを利用してプライオリティタグ付きのデータを管理することにより、ご使用のネットワークのニーズに合わせてデータの優先度を設定できます。複数の異なるタグ付きパケットを同じキューにグループ化することで効果を発揮するケースもありますが、通常は、優先度の最も高いキュー（キュー 7）をプライオリティレベル 7 のパケットに割り当てることをお勧めします。プライオリティレベルが設定されていないパケットは、キュー 0 に割り当てられ、最も低い送信優先度となります。

本スイッチは、優先制御方式として Strict モードと WRR（重み付けラウンドロビン）モードをサポートしています。WRR モードではキューからパケットが送信される比率が決定します。キュー 0 とキュー 7 の送信比率が 4 : 1 の場合、キュー 0 から 1 つのパケットが送信される毎に、キュー 7 から 4 つのパケットが送信されます。

プライオリティキューはスイッチ上のすべてのポートに対して設定されるため、スイッチに接続されるすべてのデバイスがこの設定による影響を受けることに注意してください。ご利用のネットワーク上のスイッチがプライオリティタグ割り当て機能をサポートしている場合、プライオリティキューイング機能は特に効果を発揮します。

VLAN とは

VLAN（Virtual Local Area Network : 仮想 LAN）とは、物理的なレイアウトではなく、論理的なスキームに従って構成されるネットワークトポロジです。VLAN を使用することで、LAN セグメントの集まりを自律的なユーザグループへと結合し、1 つの LAN のように見せることができます。また、ネットワークを異なるブロードキャストドメインに論理的に分割し、パケットが特定 VLAN 内のポート間にのみ送信されるように設定することが可能です。一般的に、VLAN とサブネットは 1 対 1 で対応付けられますが、必ずしもそうである必要はありません。

VLAN では、ネットワーク帯域の消費を抑えることでパフォーマンスを改善し、トラフィックを特定のドメイン内に制限することでセキュリティを強化します。

VLAN は、物理的位置ではなく論理的にエンドノードを束ねた集合体です。頻繁に通信を行うエンドノード同士に対しては、ネットワーク上の物理的位置に関わらず、同じ VLAN を割り当てます。ブロードキャストパケットは送信元と同じ VLAN メンバに対してのみ送信されるため、VLAN は論理的にはブロードキャストドメインと同等と言えます。

本スイッチシリーズにおける VLAN について

エンドノードの識別方法や VLAN メンバシップ割り当て方法に関わらず、VLAN 間にルーティング機能を持つネットワークデバイスが存在しない限り、パケットが VLAN をまたいで送信されることはありません。

本スイッチは、IEEE 802.1Q VLAN とポートベース VLAN をサポートします。タグなし機能では、パケットヘッダから 802.1Q タグを取り外すことにより、タグを認識しないデバイスとの互換性を保ちます。

スイッチの初期状態では、すべてのポートに「default」と名付けられた 802.1Q VLAN が割り当てられています。
「default」VLAN の VID は 1 です。ポートベース VLAN のメンバポートは重複して設定することが可能です。

IEEE 802.1Q VLAN

用語の説明

- タグ付け - パケットのヘッダに 802.1Q VLAN 情報を挿入すること。
- タグなし - パケットのヘッダから 802.1Q VLAN 情報を削除すること。
- イングレスポート（Ingress Port）- スイッチ上のパケットを受信するポート。VLAN の照合が行われます。
- イーグレスポート（Egress Port）- スイッチ上のパケットを送信するポート。タグ付けの決定が行われます。

本スイッチには、IEEE 802.1Q（タグ付き）VLAN が実装されています。802.1Q VLAN で行われるタグ付けによってネットワーク全体で 802.1Q VLAN が有効になります（ネットワーク上のすべてのスイッチが IEEE 802.1Q 準拠である場合）。

VLAN によりネットワークを分割することで、ブロードキャストドメインの範囲を小さくすることができます。パケットは、（IEEE 802.1Q をサポートするスイッチを経由して）受信 VLAN と同じ VLAN メンバのステーションのみに送信されます。このパケットには、送信元の不明なブロードキャスト、マルチキャスト、ユニキャストパケットも含まれます。

このほか、VLAN はネットワークにおけるセキュリティ機能を提供します。IEEE 802.1Q VLAN では、VLAN メンバであるステーションにのみパケットが送信されます。

各ポートに対して、タグ付けまたはタグなしに設定することが可能です。IEEE 802.1Q VLAN のタグなし機能により、パケットヘッダ中の VLAN タグを認識しない旧式のスイッチと連携することができます。タグ付け機能では、802.1Q 準拠の複数のスイッチを 1 つの物理接続により結びつけ、すべてのポート上でスパニングツリーを有効にして正常に動作させることができます。

IEEE 802.1Q 標準では、受信ポートが所属する VLAN へのタグなしパケットの送信を禁じています。

IEEE 802.1Q 標準規格の主な特徴は以下の通りです。
- フィルタリングによりパケットを VLAN に割り当てます。
- 全体で 1 つのスパニングツリーが構成されていると仮定します。
- 1 レベルのタグ付けにより明示的なタグ付けスキームを使用します。
- 802.1Q VLAN のパケット転送
- パケットの転送は以下の 3 種類のルールに基づいて決定されます。
  イングレスルール - VLAN に所属する受信フレームの分類に関するルール。
  ポート間のフォワーディングルール - 転送するかしないかを決定します。
  イーグレスルール - パケットが送信される時にタグ付きかタグなしかを決定します。

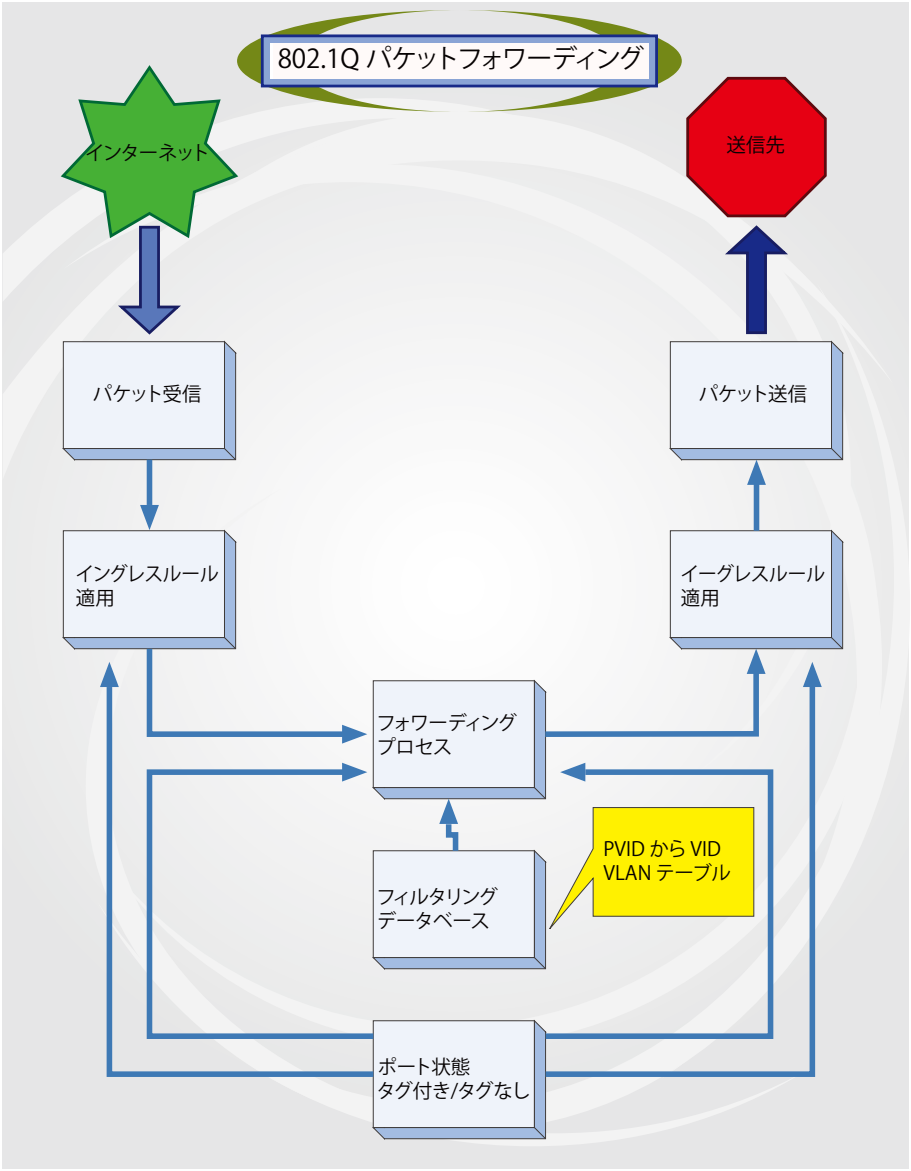


図 8-1　IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

次の図は 802.1Q VLAN のタグについて表しています。ソース MAC アドレスの後に 4 オクテットのフィールドが挿入されており、EtherType フィールドに設定された 0x8100 という値により、パケットに IEEE 802.1Q/802.1p タグが含まれていることが示されています。タグはその後に続く 2 オクテットに含まれており、ユーザプライオリティの 3 ビット、CFI(Canonical Format Identifier: イーサネットバックボーンを介して転送できるようにトークンリングパケットをカプセル化するために使用される) の 1 ビット、および VID(VLAN ID) の 12 ビットによって構成されています。ユーザプライオリティの 3 ビットは 802.1p によって使用されます。VID は VLAN を識別するためのもので、802.1Q 規格によって使用されます。VID は長さが 12 ビットであるため、4094 個の一意の VLAN を構成することができます。

タグはパケットヘッダに埋め込まれ、パケット全体は 4 オクテット分長くなります。元々のパケットに含まれていた情報はすべて保持されます。

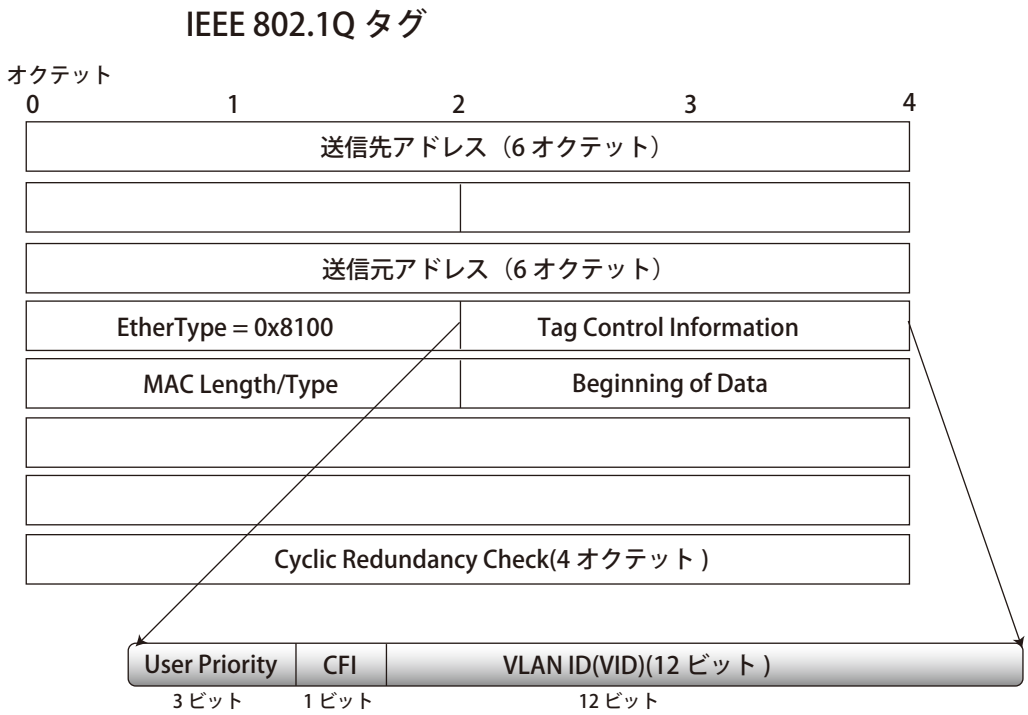


図 8-2　IEEE 802.1Q タグ

EtherType と VLAN ID は、ソース MAC アドレスと元の Length/EtherType または Logical Link Control の間に挿入されます。パケットは元のものよりも少し長くなるため、CRC は再計算されます。

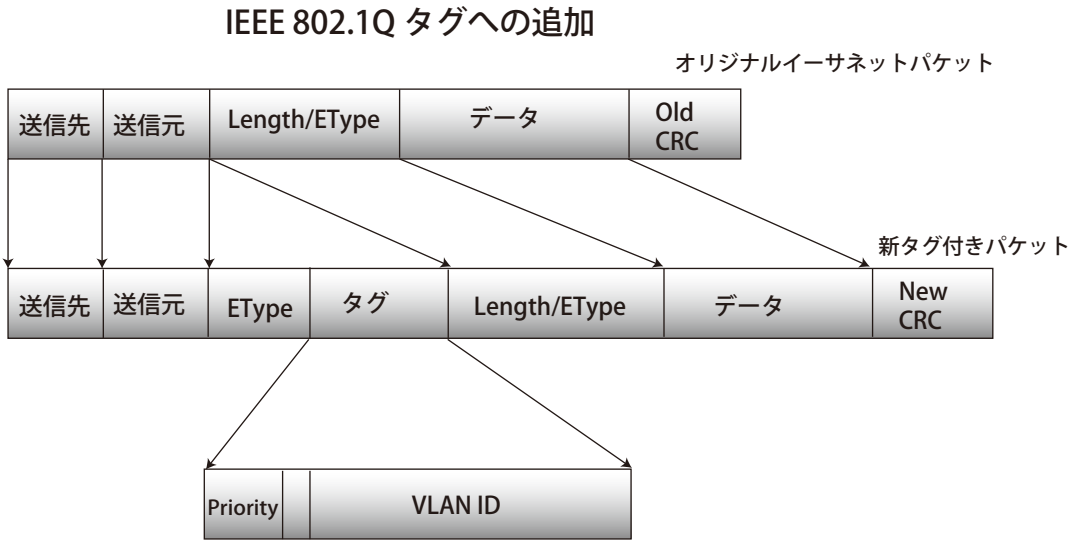


図 8-3　IEEE 802.1Q タグの挿入

ポート VLAN ID

802.1Q VID 情報が含まれるタグ付きパケットは、802.1Q に対応したネットワークデバイスから他のデバイスまで、VLAN 情報を完全に保持したまま転送されます。従って、すべてのネットワークデバイスが 802.1Q に準拠している場合、ネットワーク全体をまるごと 802.1Q VLAN によって結ぶことができます。

しかしながら、すべてのネットワークデバイスが 802.1Q に準拠しているわけではありません。これらの 802.1Q 非準拠のデバイスを tag-unaware（タグ認識不可）、802.1Q 準拠のデバイスを tag-aware（タグ認識可能）と呼ぶことにします。

802.1Q VLAN が採用される以前は、ポートベースや MAC ベースの VLAN が主流でした。これら VLAN のパケット送信は、ポート VLAN ID（PVID）を元に行われます。あるポートでタグなしパケットを受信した場合、パケットにはその受信ポートの PVID が割り当てられ、パケットの宛先アドレスに対応するポート（スイッチのフォワーディングテーブルで検出）へと送信されます。パケットを受信したポートの PVID が送信先ポートの PVID と異なる場合、パケットは破棄されます。

スイッチ内では、PVID が異なるということは VLAN が異なることを意味します（2 つの VLAN は外部ルータを経由しないと通信ができません）。そのため、PVID をベースにした VLAN の識別の場合、スイッチ（またはスイッチスタック）の外部へ VLAN を拡張することができません。

スイッチの各物理ポートには PVID が割り当てられています。802.1Q ポートにも PVID が割り当てられており、スイッチ内で使用されます。スイッチ上で VLAN が定義されていない場合、すべてのポートは PVID 1 のデフォルト VLAN が割り当てられます。タグなしのパケットは、パケットの受信ポートの PVID が割り当てられます。フォワーディングはこの PVID を元に決定されます。タグ付きのパケットにも PVID が割り当てられますが、フォワーディング処理はタグ中に含まれる VID に従います。

tag-aware（タグ認識可能）スイッチは、スイッチ内の PVID とネットワークの VID を対応付けるテーブルを保持している必要があります。スイッチは送信されるパケットの VID と、パケット送信を行うポートの VID を比較します。これらの VID が一致しない場合、パケットは廃棄されます。タグなしパケットには PVID、タグ付きパケットには VID が存在するため、タグを認識するネットワークデバイスも認識しないデバイスも、同じネットワーク内に共存が可能になります。

PVID は 1 ポートあたり 1 つしか持つことはできませんが、VID はスイッチの VLAN テーブルのメモリ上限まで持つことができます。

ネットワーク上にはタグを認識しないデバイスが存在するため、送信するパケットにタグを付けるかどうかの判断を、タグを認識できるデバイスの各ポートで行わなければなりません。送信するポートがタグを認識しないデバイスと接続していれば、タグなしのパケットを送信し、逆にタグを認識するデバイスと接続していれば、タグ付きのパケットを送信します。

タグ付きとタグなし

802.1Q に対応するスイッチのすべてのポートは、タグ付きかタグなしに設定できます。
タグ付きのポートは、送受信するすべてのパケットのヘッダに VID、プライオリティ、その他の VLAN 情報を埋め込みます。パケットが既にタグ付けされている場合、パケットは変更されず VLAN 情報は完全に保たれます。これにより、ネットワーク上の他の 802.1Q 対応デバイスは、タグの VLAN 情報を使用してパケットの転送処理を決定することができます。
タグなしとして設定されているポートは、送受信するすべてのパケットから 802.1Q タグを削除します。パケットに 802.1Q VLAN タグがない場合、ポートはパケットを変更しません。従って、タグなしのポートで受信、転送されたすべてのパケットは 802.1Q VLAN 情報を持っていません。PVID はスイッチの内部のみで使用されます。タグの削除は、802.1Q 対応のデバイスから非対応のデバイスにパケットを送信する場合に使用されます。

イングレスフィルタリング

スイッチ上のポートの内、スイッチへのパケットの入り口となり、VLAN を照合するポートをイングレスポートと呼びます。イングレスフィルタリングがポート上で有効に設定されていれば、スイッチはパケットヘッダ内の VLAN 情報を参照し、パケットの送信を行うかどうかを決定します。

パケットに VLAN 情報のタグが付加されている場合、イングレスポートはまず、自分自身がその VLAN のメンバであるかどうかを確認します。メンバでない場合、そのパケットは廃棄されます。イングレスポートが 802.1Q VLAN のメンバであれば、スイッチは送信先ポートが 802.1Q VLAN のメンバであるかどうかを確認します。802.1Q VLAN メンバでない場合は、そのパケットは廃棄されます。送信先ポートが 802.1Q VLAN のメンバであれば、そのパケットは送信され、送信先ポートはそのパケットを接続するネットワークセグメントに転送します。

パケットに VLAN 情報のタグが付加されていない場合は、イングレスポートはそのパケットに VID として自分の PVID を付加します。するとスイッチは、送信先ポートはイングレスポートと同じ VLAN のメンバであるか（同じ VID を持っているか）を確認します。同じ VLAN メンバでない場合、パケットは廃棄されます。同じ VLAN メンバである場合、パケットは送信され、送信先ポートはそのパケットを接続するネットワークセグメントに転送します。

本プロセスは、イングレスフィルタリングと呼ばれ、イングレスポートとの VLAN とは異なるパケットを受信時に廃棄することにより、スイッチ内での帯域を有効利用するために使用されます。これにより、送信先ポートに届いてから廃棄されるパケットを事前に処理することができます。

デフォルト VLAN

スイッチには、初期設定で「default」という名前で VID が 1 の VLAN が設定されています。本製品の初期設定ではスイッチ上のすべてのポートが「default」に割り当てられています。新しい VLAN がポートベースモードで設定される時、そのポートは自動的に「default」VLAN から削除されます。

パケットは VLAN 間を通過できません。ある VLAN のメンバが他の VLAN と接続を行うためには、そのリンクは外部ルータを経由する必要があります。

注意　スイッチ上に VLAN が設定されていない場合、各パケットは任意の送信先ポートへと転送されます。宛先アドレスが不明なパケットやブロードキャストパケット、マルチキャストパケットはすべてのポートに送信されます。

VLAN の設定例を以下に示します。

VLAN 名	VID	ポート番号
System (default)	1	5、6、7
Engineering	2	9、10
Sales	5	1、2、3、4

ポートベース VLAN

ポートベース VLAN は、スイッチポート単位で送受信するトラフィックを制限します。そのため、スイッチのポートに 1 台のコンピュータが直接接続されていようと、部門全体が接続されていようと、そのポートに接続されたすべてのデバイスは、そのポートが所属している VLAN のメンバになります。

ポートベース VLAN では、NIC はパケットヘッダ内の 802.1Q タグを識別できる必要はありません。NIC は通常のイーサネットパケットを送受信します。パケットの送信先が同じセグメント上にある場合、通常のイーサネットプロトコルを使用して通信が行われます。パケットの送信先が別のスイッチポートである場合、スイッチによってパケットが破棄されるか転送を行うかは VLAN の照会によって決定されます。

VLAN セグメンテーション

VLAN 2 に所属するポート 1 から送信されるパケットを例に説明します。宛先が別のポートである場合（通常のフォワーディングテーブル検索により判定）、スイッチはそのポート（ポート 10）が VLAN 2 に所属しているか（つまり VLAN 2 パケットを受け取れるか）どうかを確認します。ポート 10 が VLAN 2 のメンバでない場合は、スイッチはそのパケットを廃棄します。メンバである場合、パケットは送信されます。ポート 1 が VLAN2 にのみ送信を行うという点が重要です。このように VLAN の仕組みに基づいて選択的にフォワーディング処理が行われることで、ネットワークの分割を実現します。

VLAN（VLAN 設定）

スイッチの VLAN 設定を行います。

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

ウィザードを使用して VLAN の作成と設定を行います。

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

図 8-4　VLAN Configuration Wizard 画面

画面に表示される項目：

項目	内容
Create VLAN	新しく VLAN を作成する場合に選択します。 • 設定可能範囲：1-4094
Configure VLAN	作成済みの VLAN を編集する場合に選択します。 • 設定可能範囲：1-4094

「Next」をクリックし、以下の画面で設定を行います。

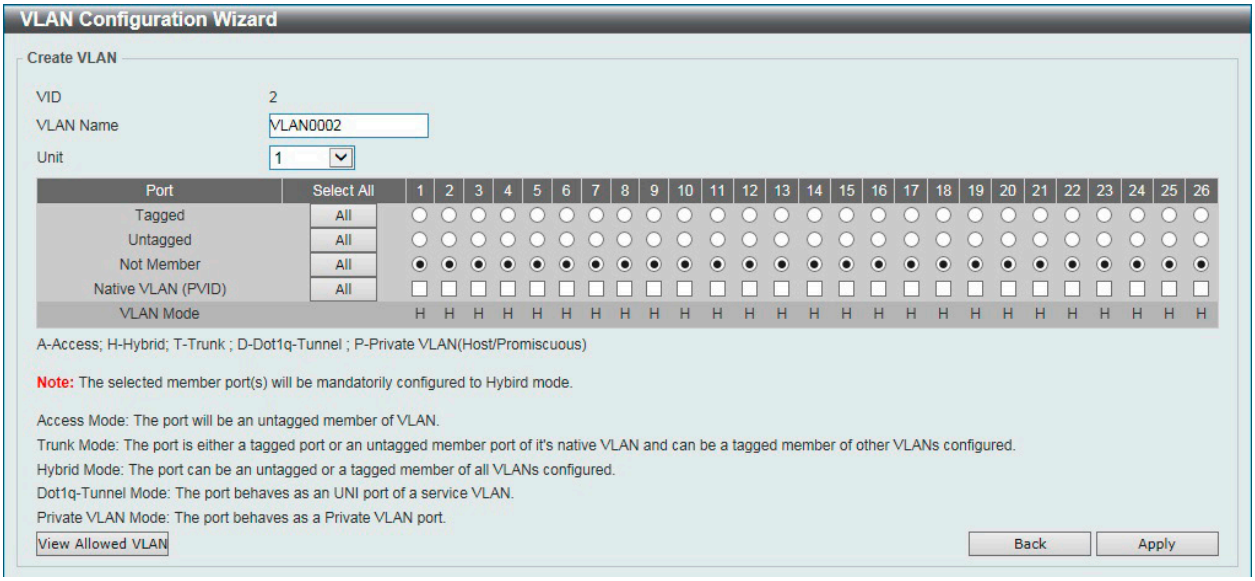


図 8-5　VLAN Configuration Wizard 画面

画面に表示される項目：

項目	内容
VID	選択した VID が表示されます。
VLAN Name	VLAN 名を入力します。
Unit	本設定を適用するユニットを選択します。
Port	各ポートを以下の通り VLAN のメンバとして定義します。 • 「Tagged」- ポートを 802.1Q タグ付きとして定義します。 • 「Untagged」- ポートを 802.1Q タグなしとして定義します。 • 「Not Member」- 各ポートが VLAN メンバでないことを定義します。 • 「Native VLAN (PVID)」- ポートをネイティブ VLAN として定義します。 「All」ボタンをクリックすると、すべてのポートが選択されます。

項目	内容
VLAN Mode	各ポートの VLAN モードが表示されます。 アルファベットの表示は以下のモードを表します。 • A：Access モード ポートは VLAN のタグなしメンバになります。 • H：Hybrid モード ポートは設定されているすべての VLAN のタグなしまたはタグ付きメンバにすることができます。 • T：Trunk モード ポートはネイティブ VLAN のタグ付きポートまたはタグなしメンバポートのいずれかであり、設定されている他の VLAN のタグ付きメンバにすることができます。 • D：Dot1q トンネルモード ポートはサービス VLAN の UNI（User Network Interface）ポートとして動作します。 • P：Private VLAN（Host/Promiscuous）モード ポートはプライベート VLAN ポートとして動作します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

許可 VLAN の表示

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

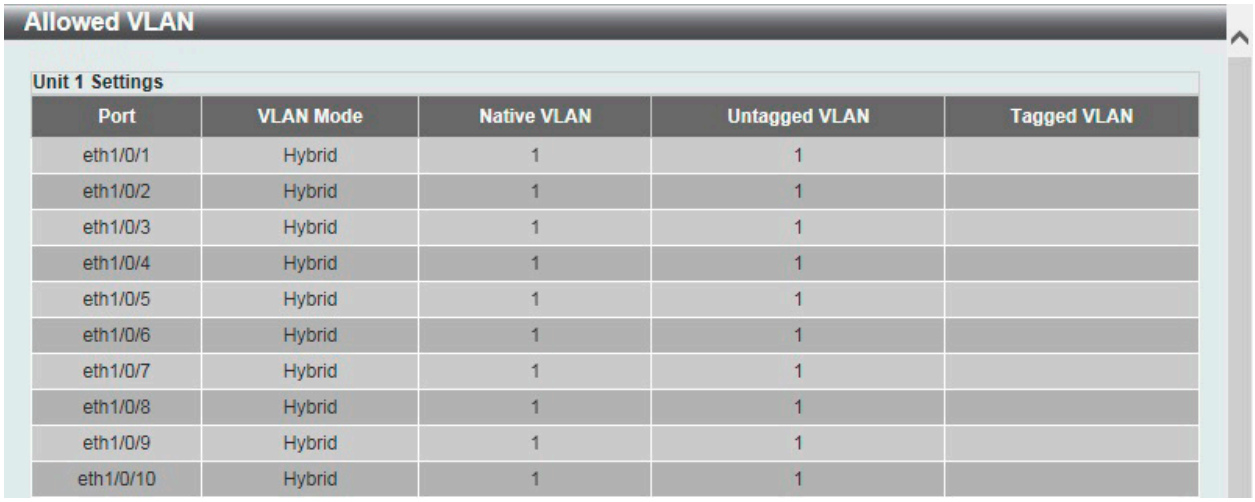


図 8-6　Allowed VLAN 画面

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。

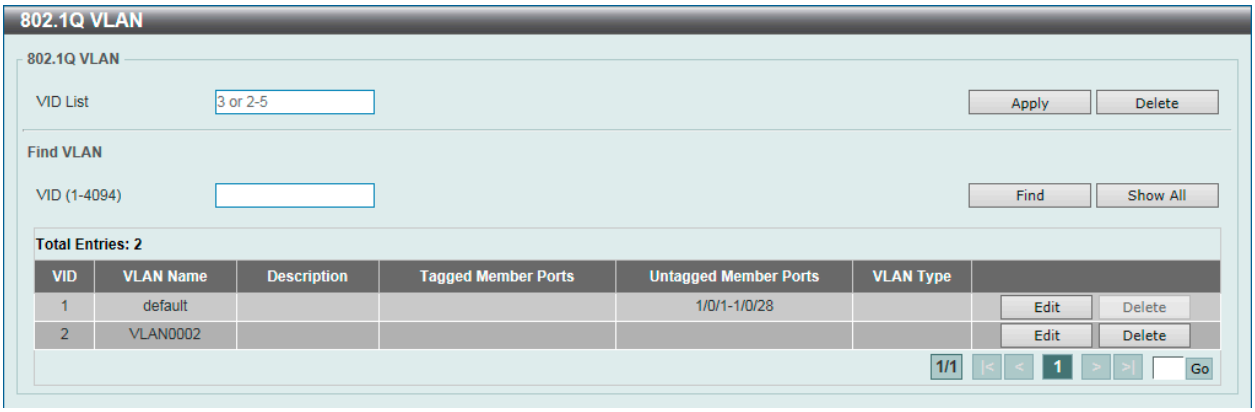


図 8-7　802.1Q VLAN 画面

画面に表示される項目：

項目	内容
802.1Q VLAN	
VID List	作成 / 削除する VLAN ID または VLAN ID の範囲を指定します。
Find VLAN	
VID	表示する VLAN ID を指定します。
VLAN Name	既存エントリの「Edit」ボタンをクリックした後、VLAN 名を編集することができます。

「Apply」ボタンをクリックし、VLAN エントリを作成します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「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。
「Show All」ボタンをクリックして、すべての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。

VLAN Interface（VLAN インタフェース）

VLAN インタフェースの設定を行います。

L2 Features > VLAN > VLAN Interface の順にメニューをクリックします。
本画面には、「VLAN Interface Settings」タブと「Port Summary」タブがあります。

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

「VLAN Interface Settings」タブでは、各ポートの VLAN インタフェース設定の確認、および編集を行うことができます。

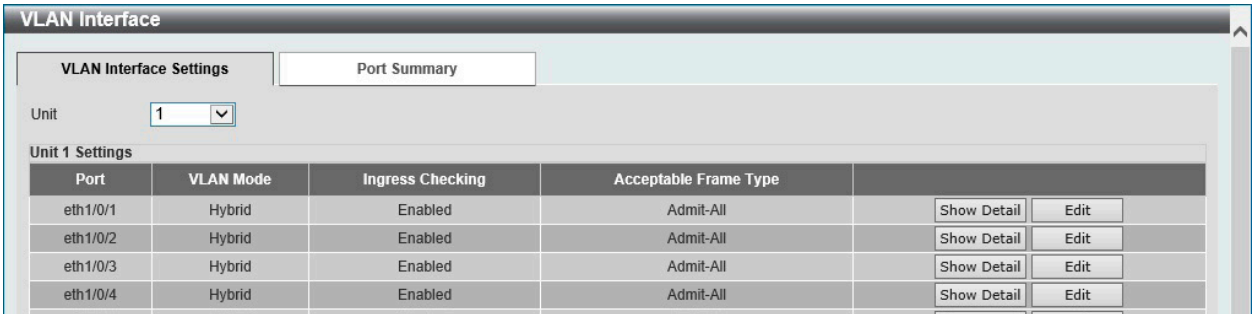


図 8-8　VLAN Interface 画面 - VLAN Interface Settings タブ

画面に表示される項目：

項目	説明
Unit	表示 / 設定を行うユニットを選択します。

エントリの編集
「Edit」ボタンをクリックして、指定エントリの編集を行います。

VLAN 詳細情報の表示

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

■ Show Detail（VLAN 詳細情報の表示）

「Show Detail」をクリックすると、以下の画面で各ポートの VLAN インタフェース設定を確認できます。

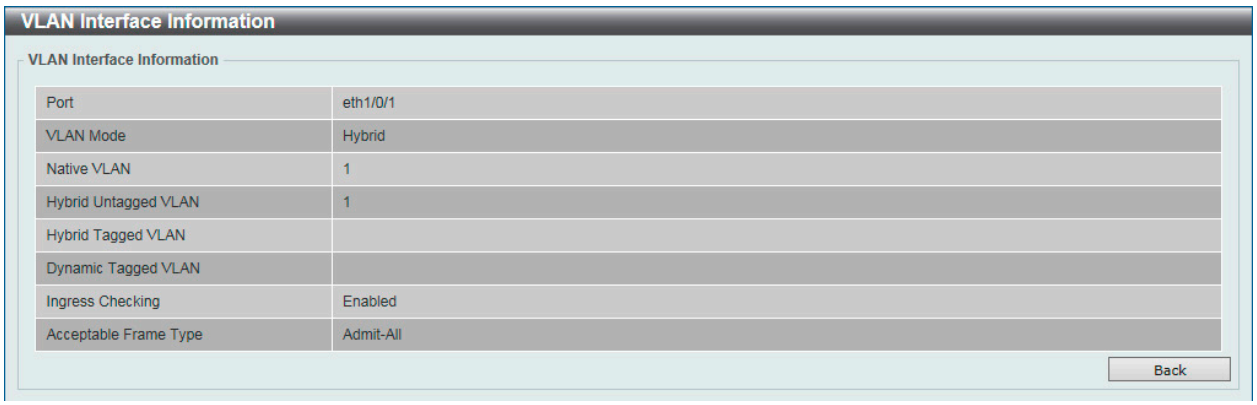


図 8-9　VLAN Interface（Show Detail）- VLAN Interface Information 画面

前の画面に戻るには、「Back」ボタンをクリックします。

■ Edit（VLAN インタフェース設定の編集）

「Edit」をクリックすると、各ポートの VLAN インタフェース設定を編集できます。

画面に表示される項目は、「VLAN Mode」で設定した VLAN モードによって異なります。
選択できる VLAN モードは以下の通りです。

「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」

● VLAN モード「Access」を選択した場合：

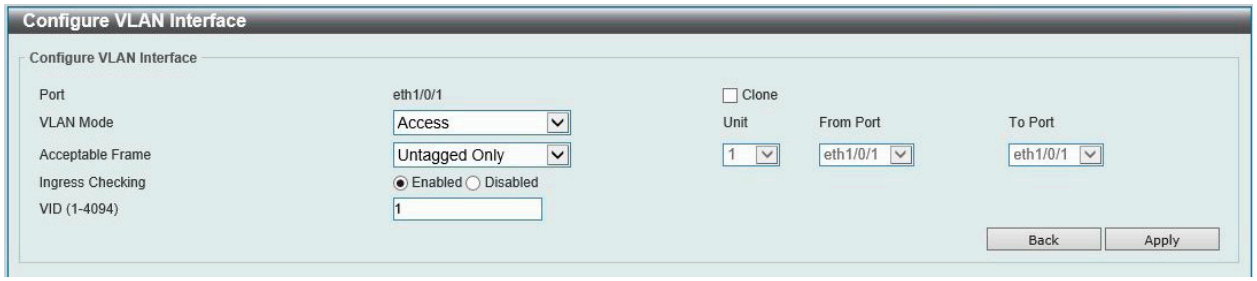


図 8-10　VLAN Interface（Edit）- Configure VLAN Interface 画面（Access 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを選択します。ここでは「Access」を選択します。
Acceptable Frame	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有効 / 無効に設定します。
VID	VLAN ID を指定します。 • 設定可能範囲：1 -4094
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

● **VLAN モード「Hybrid」を選択した場合：**

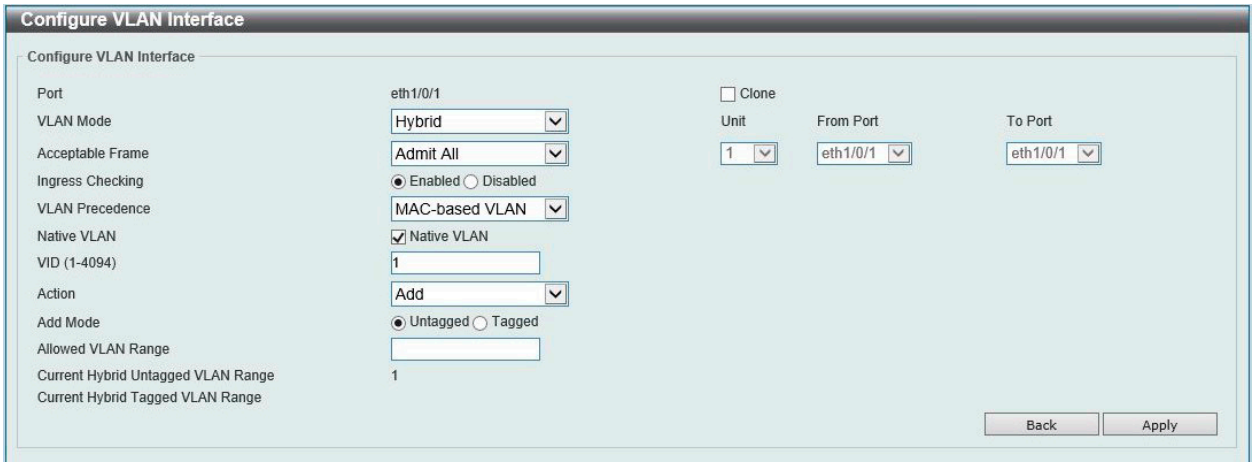


図 8-11　VLAN Interface（Edit）- Configure VLAN Interface 画面（Hybrid 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを選択します。ここでは「Hybrid」を選択します。
Acceptable Frame	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有効 / 無効に設定します。
VLAN Precedence	優先 VLAN を選択します。 • 「Mac-based VLAN」「Subnet-based VLAN」
Native VLAN	Native VLAN を有効にします。
VID	Native VLAN を有効にした場合は、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。 • 選択肢：「Add」「Remove」「Tagged」「Untagged」
Add Mode	「Add Mode」のパラメータとして、タグ付きまたはタグなしを指定します。 • 選択肢：「Untagged」「Tagged」
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

● **VLAN モード「Trunk」を選択した場合：**

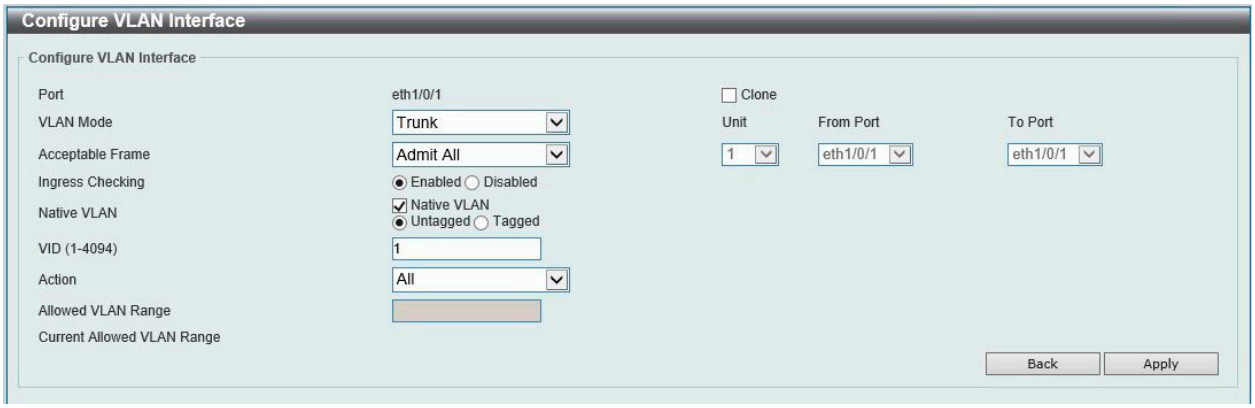


図 8-12　VLAN Interface（Edit）- Configure VLAN Interface 画面（Trunk 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。

項目	内容
VLAN Mode	VLAN モードを選択します。ここでは「Trunk」を選択します。
Acceptable Frame	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有効 / 無効に設定します。
Native VLAN	Native VLAN を有効にします。「Untagged」または「Tagged」フレームを選択します。
VID	Native VLAN を有効にした場合は、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。 • 選択肢：「None」「All」「Add」「Remove」「Except」「Replace」
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

● **VLAN モード「Dot1q-Tunnel」を選択した場合：**

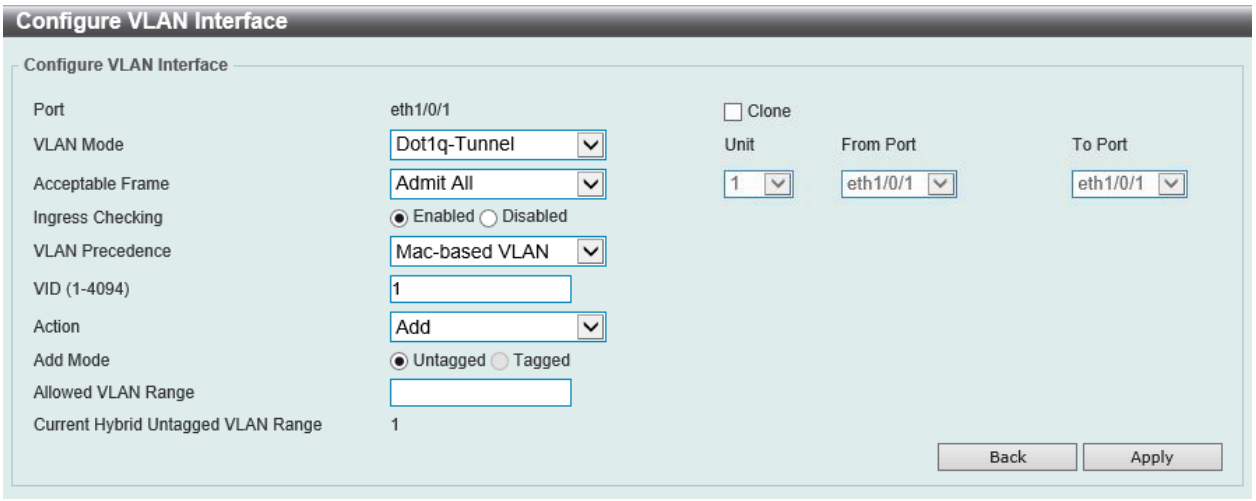


図 8-13　VLAN Interface（Edit）- Configure VLAN Interface 画面（Dot1q-Tunnel 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを選択します。ここでは「Dot1q-Tunnel」を選択します。
Acceptable Frame	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有効 / 無効に設定します。
VID	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。 • 選択肢：「Add」「Remove」
Add Mode	「Add Mode」のパラメータとして「Untagged」が指定されます。
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

● **VLAN モード「Promiscuous」を選択した場合：**

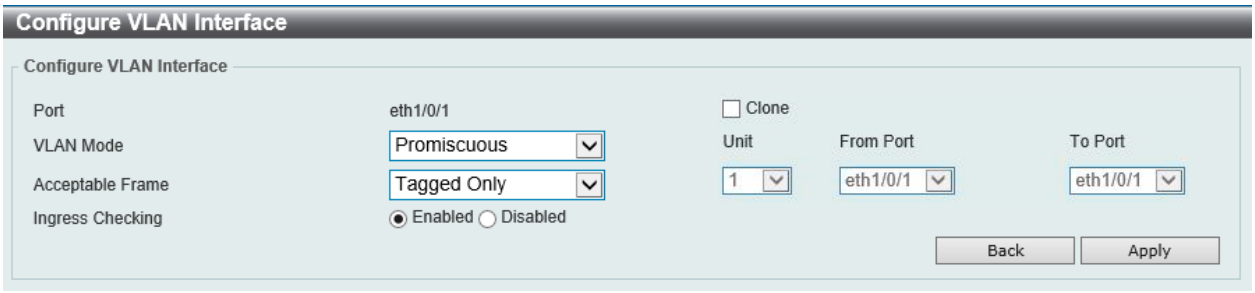


図 8-14　VLAN Interface（Edit）- Configure VLAN Interface 画面（Promiscuous 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Promiscuous」を選択します。
Acceptable Frame	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有効 / 無効に設定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

● **VLAN モード「Host」を選択した場合：**

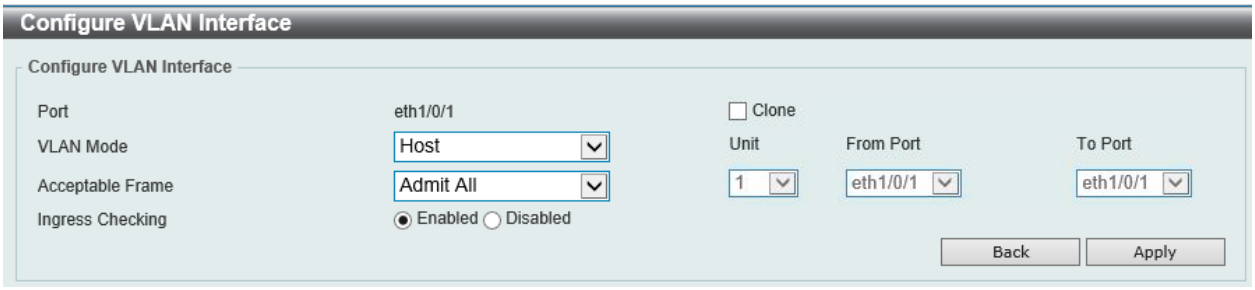


図 8-15　VLAN Interface（Edit）- Configure VLAN Interface 画面（Host 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを選択します。ここでは「Host」を選択します。
Acceptable Frame	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有効 / 無効に設定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Port Summary（ポートサマリー）タブ

「Port Summary」タブでは、各ポートの VLAN インタフェース設定を確認できます。

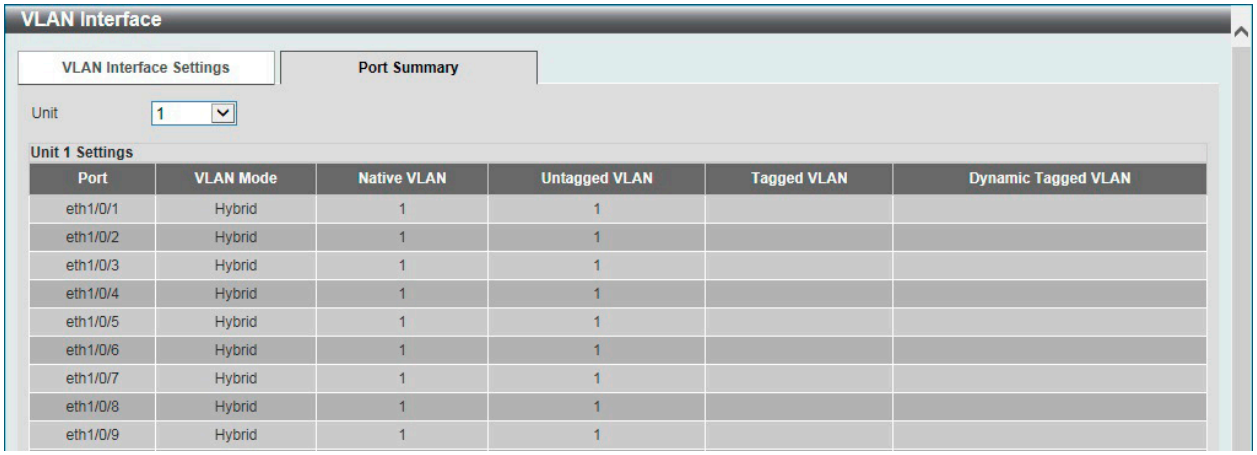


図 8-16　VLAN Interface 画面 - Port Summary タブ

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

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

802.1v プロトコル VLAN の設定を行います。

Protocol VLAN Profile（プロトコル VLAN プロファイル設定）

802.1v プロトコル VLAN プロファイルを作成します。
802.1v プロトコル VLAN グループ設定は、各プロトコルに対して複数の VLAN をサポートし、同じ物理ポート上に異なるプロトコルを持つアンタグポートを設定することができます。たとえば、同じ物理ポートで 802.1Q および 802.1v のアンタグポートを設定できます。

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

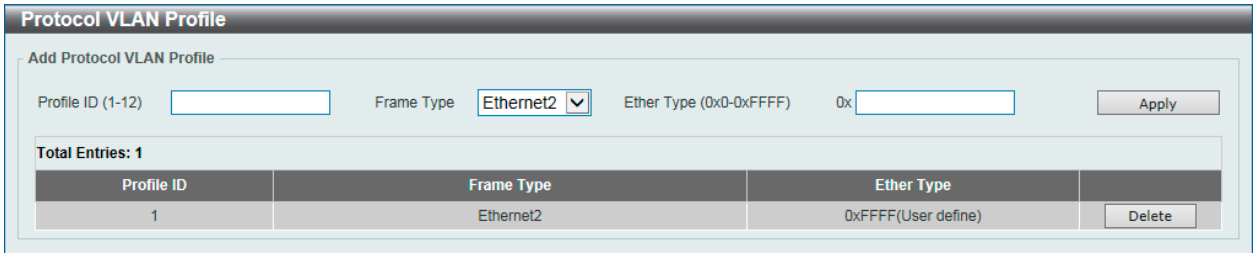


図 8-17　Protocol VLAN Profile 画面

画面に表示される項目：

項目	説明
Profile ID	802.1v プロトコル VLAN のプロファイル ID を指定します。 • 設定可能範囲：1-12
Frame Type	フレームタイプを選択します。 本機能は、パケットヘッダ内のタイプオクテットを検証し、関連するプロトコルのタイプを検出することにより、パケットをプロトコル定義 VLAN にマッピングします。 • 選択肢：「Ethernet2」「SNAP」「LLC」
Ether Type	グループに対してイーサネットタイプを指定します。 プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。入力形式は 0x0 から 0xFFFF です。オクテット文字列は、フレームタイプに応じて以下のいずれかになります。 • 「Ethernet 2」- 16 ビット (2 オクテット) の 16 進数です。例えば、IPv4 は 0800、IPv6 は 86DD、ARP は 0806 です。 • 「SNAP」- 16 ビット (2 オクテット) の 16 進数です。 • 「LLC」- 2 オクテットの IEEE 802.2 Link Service Access Point（LSAP）ペアです。最初のオクテットは Destination Service Access Point（DSAP）用で、2 番目のオクテットは送信元用の値です。

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

Protocol VLAN Profile Interface（プロトコル VLAN プロファイルインタフェース）

プロトコル VLAN ポートの設定を行います。

L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile 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。

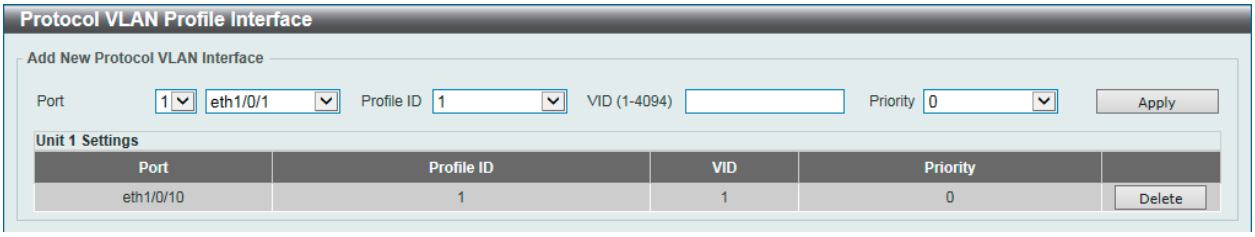


図 8-18　Protocol VLAN Profile Interface 画面

画面に表示される項目：

項目	説明
Port	設定するスタッキングユニット ID とポート番号を指定します。
Profile ID	定義済みの 802.1v プロトコル VLAN プロファイル ID を選択します。
VID	VLAN ID を入力します。
Priority	プライオリティ値を選択します。 このパラメータは、スイッチに定義済みの 802.1p のデフォルトプライオリティを書き換えるために指定し、パケットが転送される CoS キューを決定するために使用されます。本項目が指定されると、このプライオリティに一致する受信パケットは、指定した CoS キューに転送されます。 • 設定可能範囲：0-7

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

GVRP（GVRP の設定）

GVRP Global（GVRP グローバル設定）

GVRP（GARP VLAN Registration Protocol）の設定を行います。

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

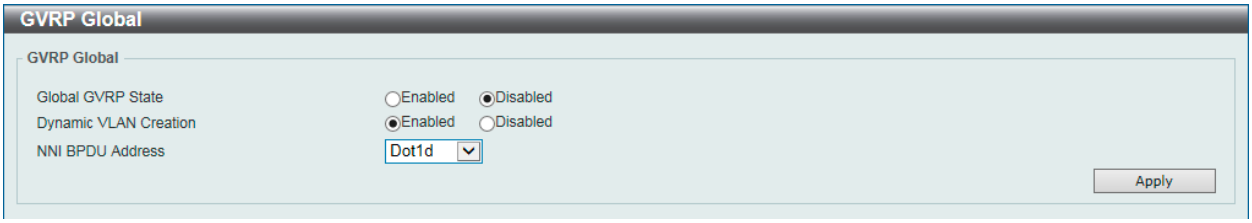


図 8-19　GVRP Global 画面

画面に表示される項目：

項目	説明
Global GVRP State	GVRP のグローバルステータスを有効 / 無効に設定します。
Dynamic VLAN Creation	ダイナミック VLAN クリエーション機能を有効 / 無効に設定します。
NNI BPDU Address	NNI BPDU アドレスオプションを選択します。 カスタマネットワークにおける GVRP の BPDU プロトコルアドレスを決定するために使用されます。802.1d GVRP アドレスまたは 802.1ad サービスプロバイダ GVRP アドレスを使用することができます。 • 選択肢：「Dot1d」「Dot1ad」

「Apply」ボタンをクリックして、設定内容を適用します。

GVRP Port（GVRP ポート設定）

ポート毎に GVRP のパラメータを設定します。

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

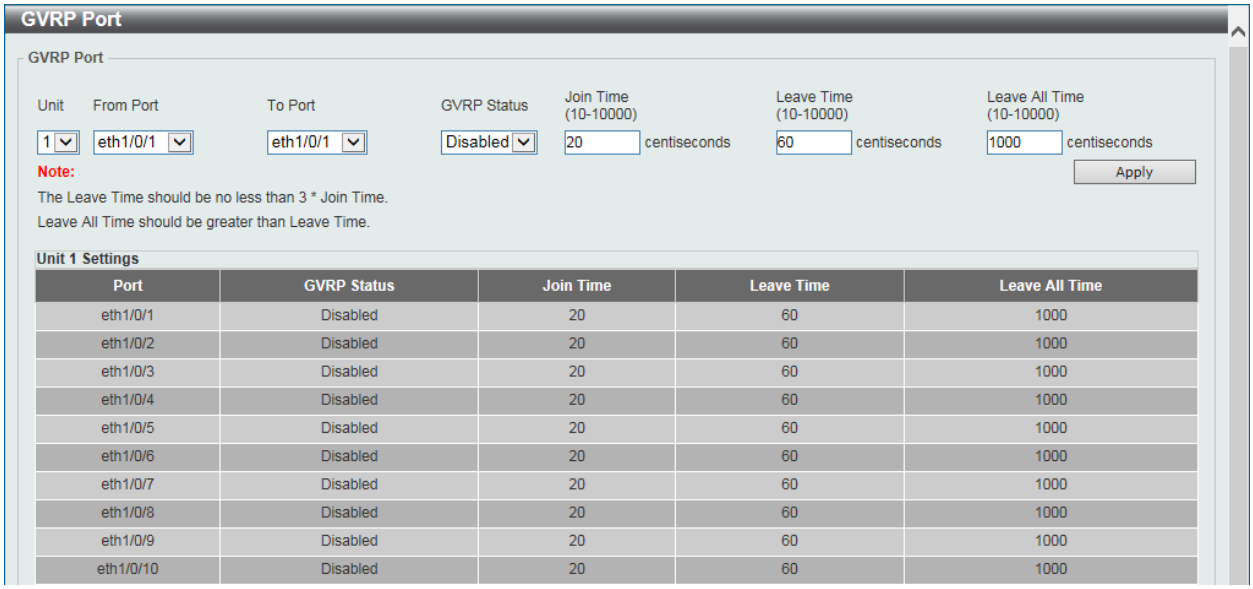


図 8-20　GVRP Port 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
GVRP Status	各ポートの GVRP ステータスを有効 / 無効に設定します。有効にするとポートが自動的に VLAN のメンバになります。 • 初期値：「Disabled（無効）」
Join Time	開始時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 初期値：20
Leave Time	終了時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 初期値：60
Leave All Time	全終了時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 初期値：1000

「Apply」ボタンをクリックして、設定内容を適用します。

GVRP Advertise VLAN（GVRP アドバタイズ VLAN 設定）

GVRP アドバタイズ VLAN の設定、表示を行います。

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

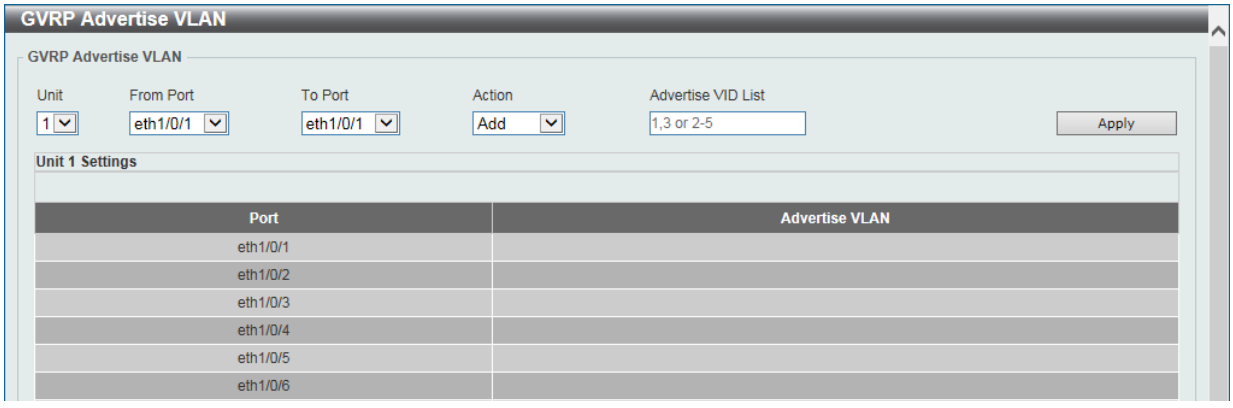


図 8-21　GVRP Advertise VLAN 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Action	指定した VLAN に対し、アドバタイズ VLAN として指定、削除、置き換えを行います。 「All」を選択するとすべての VLAN がアドバタイズ VLAN として指定されます。 • 選択肢：「All」「Add」「Remove」「Replace」
Advertise VID List	アドバタイズ VLAN ID を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

GVRP Forbidden VLAN（GVRP Forbidden VLAN 設定）

GVRP Forbidden VLAN の設定、表示を行います。

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

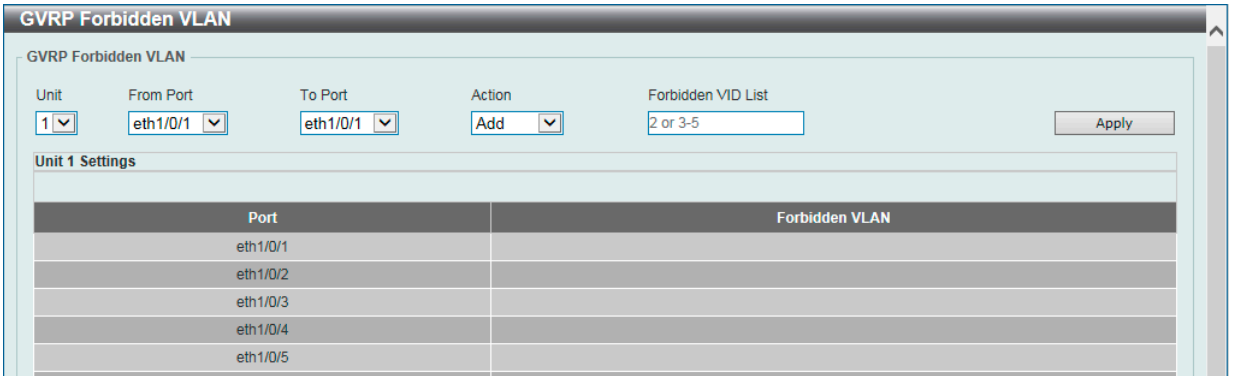


図 8-22　GVRP Forbidden VLAN 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Action	指定した VLAN に対し、禁止 VLAN として指定、削除、置き換えを行います。 「All」を選択するとすべての VLAN が禁止 VLAN として指定されます。 • 選択肢：「All」「Add」「Remove」「Replace」
Forbidden VID List	禁止 VLAN ID を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

GVRP Statistics Table（GVRP 統計テーブル）

GVRP の統計情報を表示します。

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

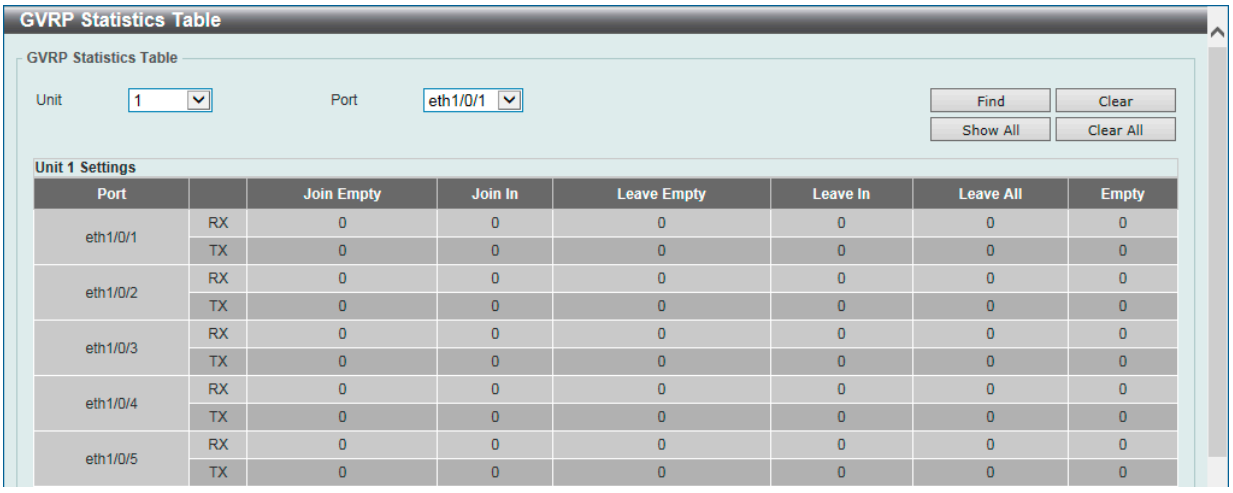


図 8-23　GVRP Statistics Table 画面

画面に表示される項目：

項目	説明
Unit	統計情報を表示 / 削除するユニットを指定します。
Port	統計情報を表示 / 削除するポートを指定します。

エントリの検索
「Find」ボタンをクリックして、指定ポートのエントリを検索します。
「Show All 」ボタンをクリックして、すべてのエントリを表示します。

エントリの削除
「Clear」ボタンをクリックして、指定ポートの統計情報を削除します。
「Clear All 」ボタンをクリックして、すべての統計情報を削除します。

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。

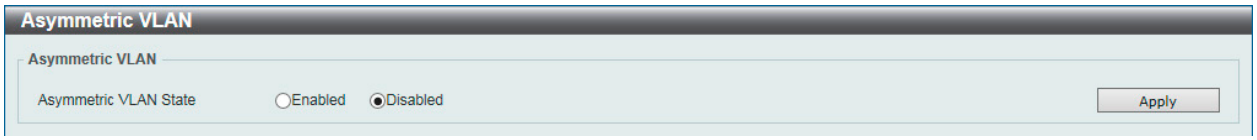


図 8-24　Asymmetric VLAN 画面

画面に表示される項目：

項目	説明
Asymmetric VLAN State	Asymmetric VLAN を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　Asymmetric VLAN は、重複する全 VLAN に学習した MAC アドレスを乗せる事により異なるネイティブ VLAN 間のフラッディングを抑止します。

MAC VLAN（MAC VLAN 設定）

MAC ベース VLAN を設定、表示します。
スタティック MAC ベース VLAN エントリが設定されている場合、接続するデバイスによりポートの VLAN が変わります。

L2 Features > VLAN > MAC 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。

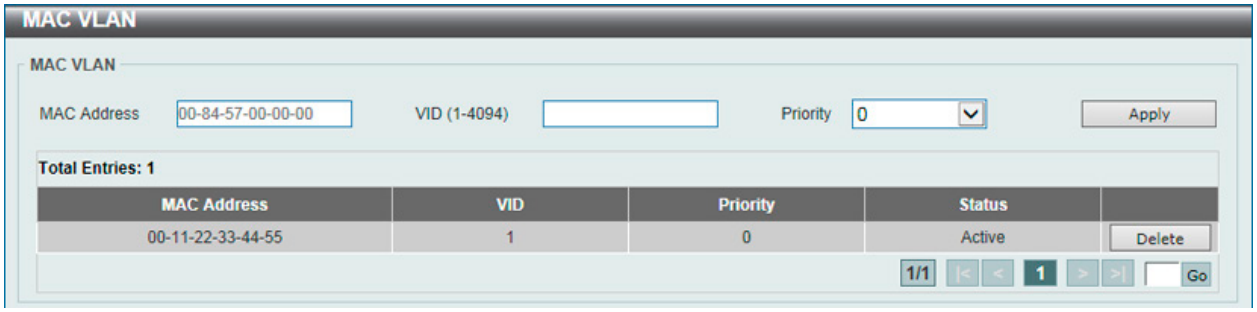


図 8-25　MAC VLAN 画面

画面に表示される項目：

項目	説明
MAC Address	ユニキャスト MAC アドレスを入力します。
VID	VLAN ID を入力します。
Priority	タグなしパケットに割り当てる優先度を選択します。 • 設定可能範囲：0-7

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

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。

L2VLAN Interface Description（L2VLAN インタフェース概要）

L2 VLAN インタフェースについて表示、設定を行います。

L2 Features > VLAN > L2VLAN Interface Description をクリックします。次の画面が表示されます。

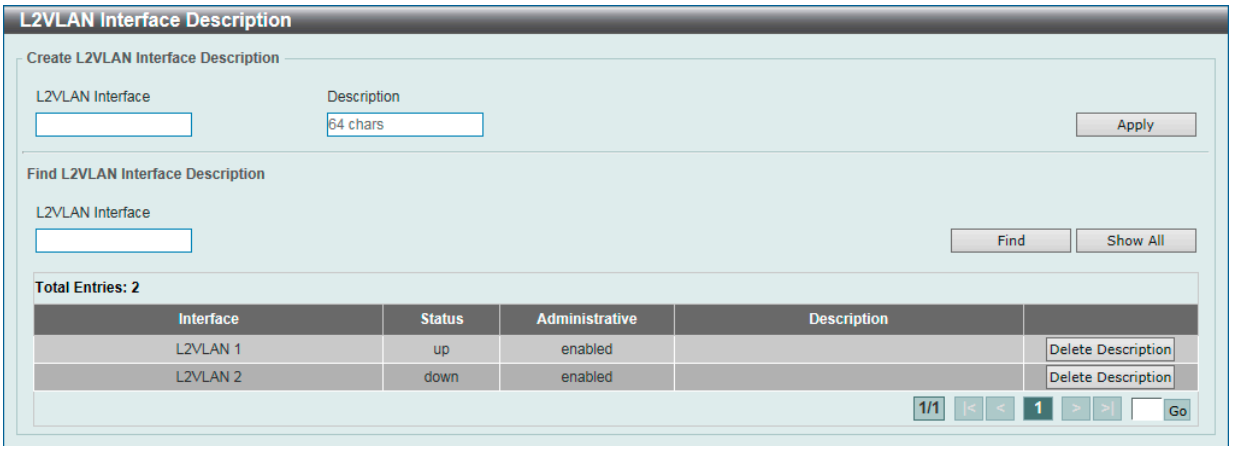


図 8-26　L2VLAN Interface Description 画面

画面に表示される項目：

項目	説明
L2VLAN Interface	L2 VLAN インタフェースの ID を指定します。
Description	L2 VLAN インタフェースの説明を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。
「Delete Description」ボタンをクリックして、指定の L2 VLAN の説明を削除します。

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。

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

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

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

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

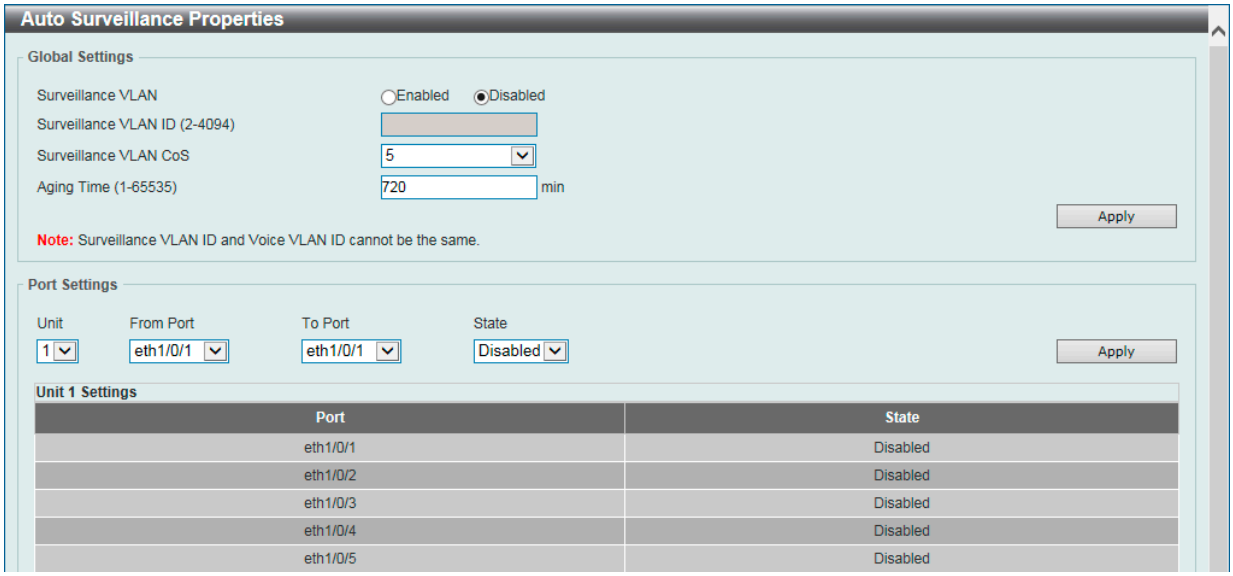


図 8-27　Auto Surveillance Properties 画面

画面に表示される項目：

項目	説明
Global Settings	
Surveillance VLAN	サーベイランス VLAN を有効 / 無効に設定します。
Surveillance VLAN ID	サーベイランス VLAN の VLAN ID を指定します。 VLAN をサーベイランス VLAN に割り当てる前に、通常の VLAN として作成する必要があります。 • 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。 サーベイランス VLAN が有効化されたポートで受信したサーベイランスパケットは、この CoS 値でマークされます。CoS のリマーキングにより、サーベイランス VLAN トラフィックをデータトラフィックと区別することができます。 • 設定可能範囲：0-7
Aging Time	エージングタイムを設定します。 本機能は、サーベイランス VLAN ダイナミックメンバポートのエージングタイムを設定するために使用されます。ポートに接続されたサーベイランスデバイスがトラフィックの送信を停止し、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、エージングタイマはキャンセルされます。 • 設定可能範囲：1-65535（分）
Port Settings	
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
State	指定したポートでサーベイランス VLAN を有効 / 無効に設定します。 サーベイランス VLAN が有効な場合、ポートはアンタグのサーベイランス VLAN メンバとして自動的に学習され、受信したアンタグのサーベイランスパケットはサーベイランス VLAN に転送されます。受信したパケットの送信元 MAC アドレスが OUI（Organizationally Unique Identifier）アドレスに一致している場合、そのパケットはサーベイランスパケットとして認識されます。

「Apply」ボタンをクリックして、設定内容を適用します。

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

サーベイランスデバイスの表示と MAC アドレスの設定を行います。

■ User-Defined MAC Settings（ユーザ定義 MAC 設定）タブ

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。

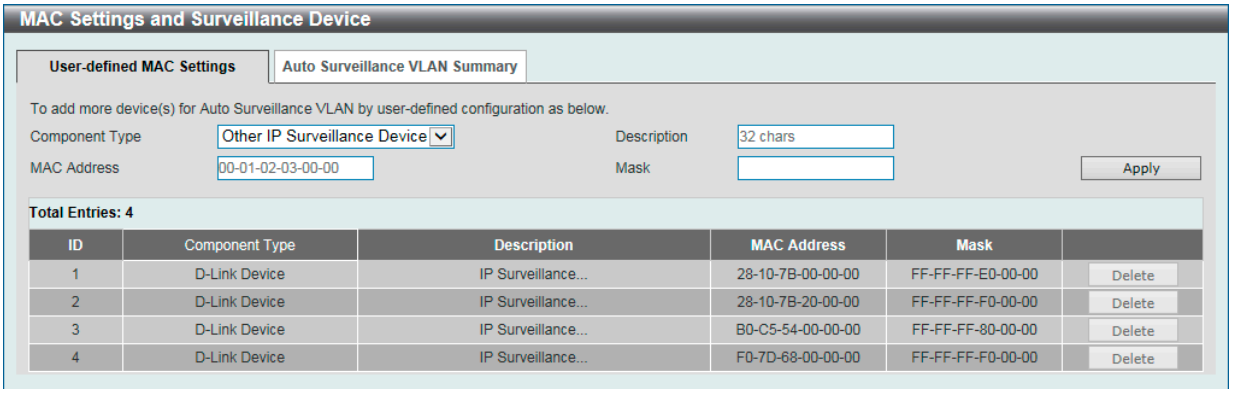


図 8-28　MAC Settings and Surveillance Device 画面 - User-defined MAC Settings タブ

画面に表示される項目：

項目	説明
Component Type	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の種類を選択します。 • 選択肢：「Video Management Server」「VMS Client/Remote Viewer」「Video Encoder」「Network Storage」「Other IP Surveillance Device」
Description	ユーザ定義の OUI に関する説明を入力します。（32 文字以内）
MAC Address	ユーザ定義の OUI MAC アドレスを入力します。受信パケットの MAC アドレスが OUI パターンにいずれかと一致すると、そのパケットはサーベイランスパケットとして識別されます。
Mask	ユーザ定義 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て、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

■ Auto Surveillance VLAN Summary（自動サーベイランス VLAN サマリ）タブ

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

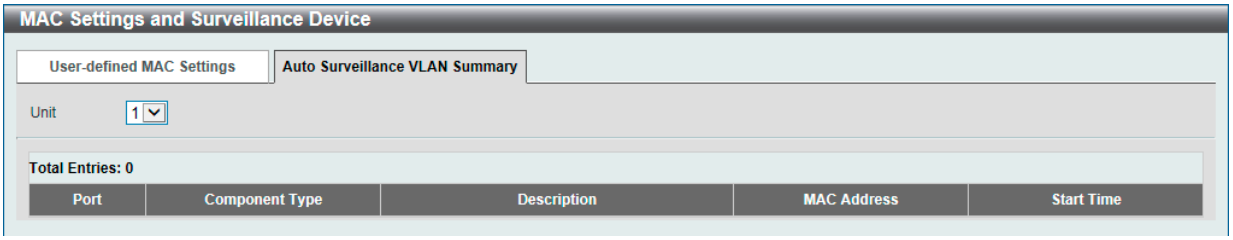


図 8-29　MAC Settings and Surveillance Device 画面 - Auto Surveillance VLAN Summary タブ

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

Voice VLAN（音声 VLAN）

Voice VLAN Global（音声 VLAN グローバル設定）

音声 VLAN の設定を行います。本スイッチの音声 VLAN は 1 つのみです。

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

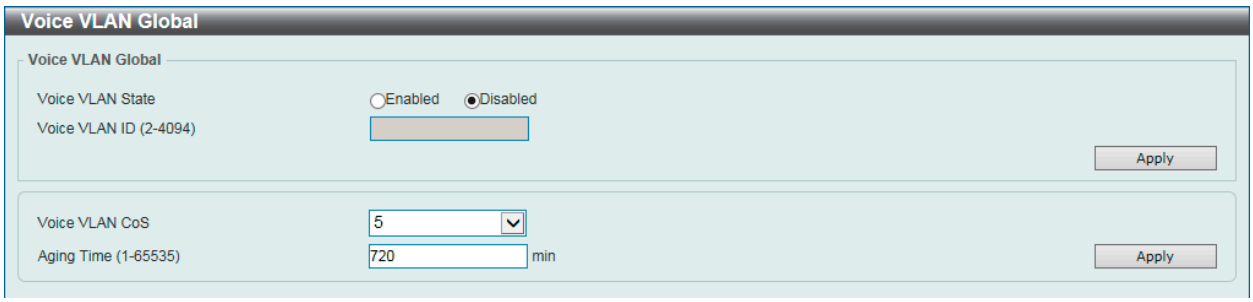


図 8-30　Voice VLAN Global Settings 画面

画面に表示される項目：

項目	説明
Voice VLAN State	音声 VLAN 機能を有効 / 無効に設定します。
Voice VLAN ID	音声 VLAN の VLAN ID を入力します。指定する VLAN は事前に作成しておく必要があります。 • 設定可能範囲：2-4094
Voice VLAN CoS	音声 VLAN の優先値を設定します。音声 VLAN が有効化されたポートで受信した音声パケットは、この CoS 値でマークされます。CoS のリマーキングにより、音声 VLAN トラフィックをデータトラフィックと区別することができます。 • 設定可能範囲：0-7
Aging Time	自動学習された音声デバイスと音声 VLAN 情報のエージングタイム を設定します。 音声デバイスがトラフィックの送信を停止し、この音声デバイスの MAC アドレスが FDB のエージングタイムに到達すると、音声 VLAN エージングタイマが開始されます。 ポートは音声 VLAN のエージングタイム経過後に音声 VLAN から削除されます。 音声トラフィックがエージングタイム内に再開すると、エージングタイマはキャンセルされます。 • 設定可能範囲：1-65535（分）

「Apply」ボタンをクリックして、設定内容を適用します。

Voice VLAN Port（音声 VLAN のポート設定）

ポートの音声 VLAN を設定、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。

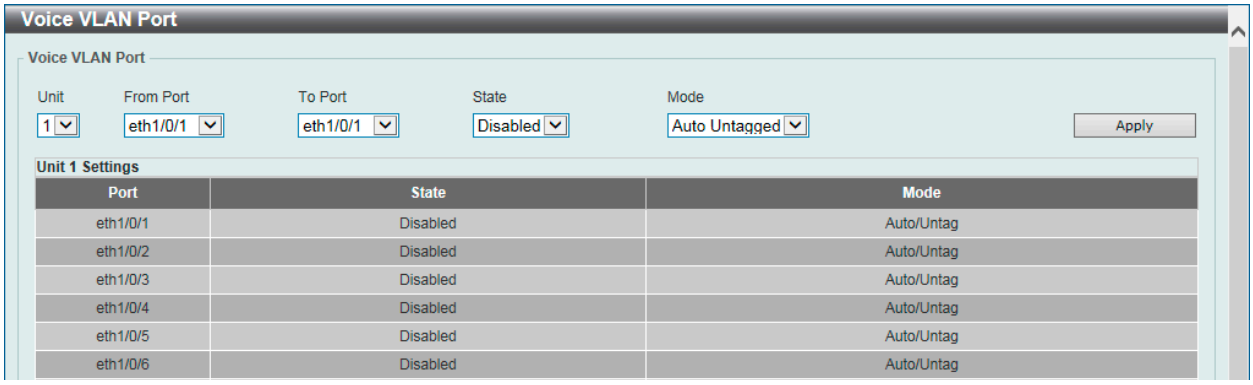


図 8-31　Voice VLAN Port 画面

画面に表示される項目：

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を選択します。
State	指定ポートの音声 VLAN 機能を有効 / 無効に設定します。 音声 VLAN が有効になると、受信した音声パケットは音声 VLAN として送信されます。受信した音声 VLAN パケットの送信元 MAC アドレスが OUI アドレスに一致すると、音声 VLAN と認識されます。

項目	説明
Mode	モードを選択します。 • 「Auto Untagged」- タグなしの音声 VLAN メンバシップが自動的に学習されます。 • 「Auto Tagged」- タグ付きの音声 VLAN メンバシップが自動的に学習されます。 • 「Manual」- 音声 VLAN メンバシップを手動で設定します。 指定ポートで自動学習が有効化されている場合、音声 VLAN メンバは自動的に学習され、エージアウトします。 「Auto Tagged」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、ポートはタグ付きメンバとして音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなしパケットは Port VLAN ID（PVID）で転送されます。 「Auto Untagged」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、ポートはタグなしメンバとして音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなしパケットは音声 VLAN で転送されます。 スイッチが LLDP-MED パケットを受信した場合、VLAN ID、Tagged フラグ、優先度フラグがチェックされます。スイッチは Tagged フラグ、優先度フラグに従います。

「Apply」ボタンをクリックして、設定内容を適用します。

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。受信パケットのソース MAC アドレスが OUI パターンのいずれかと一致した場合、受信パケットは音声パケットとして識別されます。定義済み OUI に加えて、ユーザ定義の OUI を追加することができます。
ユーザ定義 OUI は定義済みの OUI と同じにすることはできません。また、システム定義 OUI は削除できません。

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。

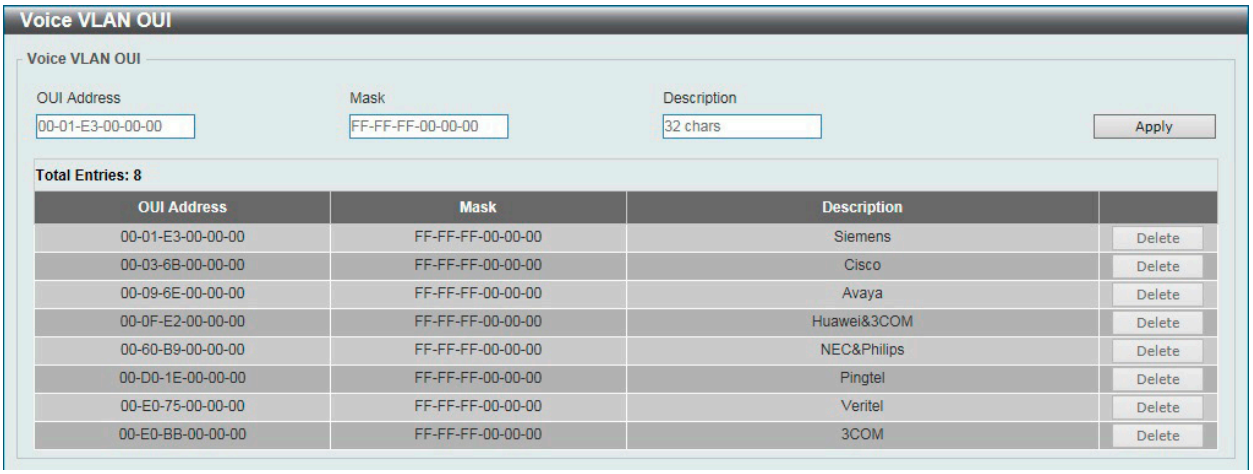


図 8-32　Voice VLAN OUI 画面

画面に表示される項目：

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

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

Voice VLAN Device（音声 VLAN 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。

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

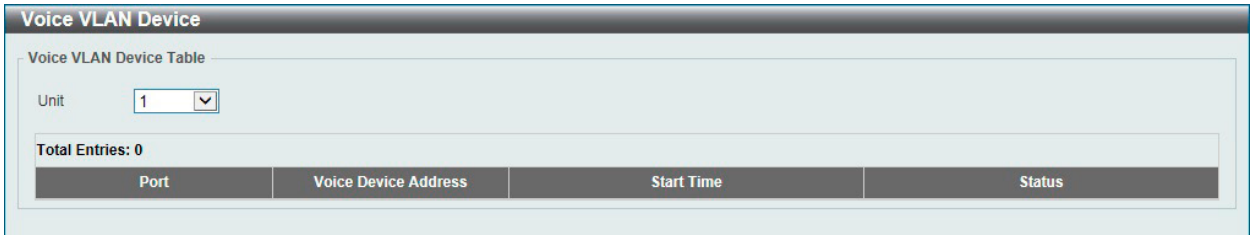


図 8-33　Voice VLAN Device 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

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

スイッチに接続された音声 VLAN LLDP-MED 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。

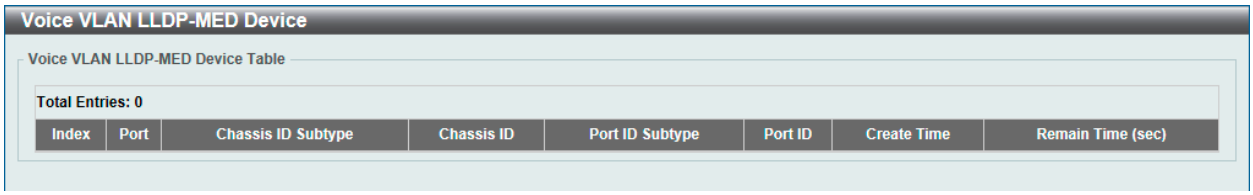


図 8-34　Voice VLAN LLDP-MED Device 画面

Private VLAN（プライベート VLAN 設定）

プライベート VLAN の設定を行います。

L2 Features > VLAN > Private 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。

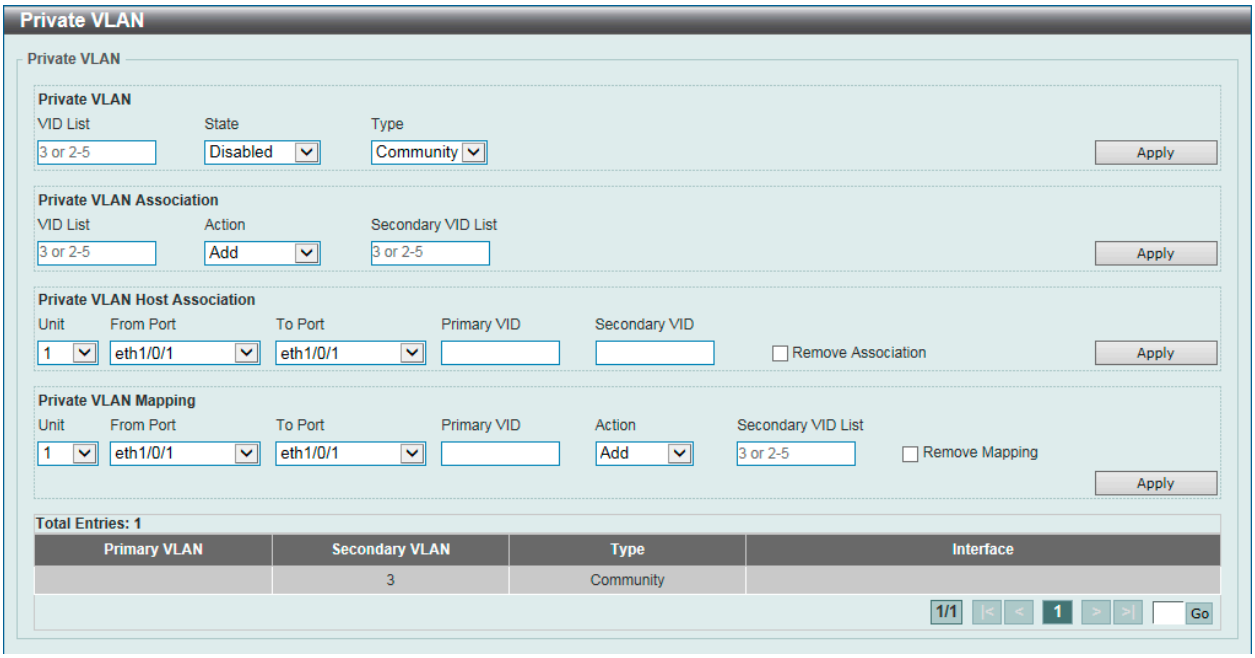


図 8-35　Private VLAN 画面

画面に表示される項目：

項目	説明
Private VLAN	
VID List	プライベート VLAN の VLAN ID を指定します。
State	プライベート VLAN を有効 / 無効に設定します。
Type	プライベート VLAN の種類を指定します。 • 選択肢：「Community」「Isolated」「Primary」
Private VLAN Association	
VID List	プライベート VLAN の VLAN ID を指定します。
Action	指定したプライベート VLAN に対し、セカンダリ VLAN の関連付けを設定します。 • 選択肢：「Add（追加）」「Remove（削除）」「Disabled（無効）」
Secondary VID List	セカンダリプライベート VLAN の VLAN ID を入力します。
Private VLAN Host Association	
Unit	設定を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。 指定したプライベート VLAN ポート（Host ポート）に対し、プライベート VLAN の関連付けを設定します。
Primary VID	プライマリプライベート VLAN の VLAN ID を入力します。 「Remove Association」にチェックを入れると対象ポートとの関連付けは削除されます。
Secondary VID	セカンダリプライベート VLAN の VLAN ID を入力します。 「Remove Association」にチェックを入れると対象ポートとの関連付けは削除されます。
Private VLAN Mapping	
Unit	設定を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。 指定したプライベート VLAN ポート（Promiscuous ポート）に対し、プライベート VLAN の関連付けを設定します。
Primary VID	プライマリプライベート VLAN の VLAN ID を入力します。
Action	• 「Add」- 入力した情報に基づき関連付けを設定します。 • 「Remove」- 入力した情報に基づき関連付けを削除します。
Secondary VID	セカンダリプライベート VLAN の VLAN ID を入力します。 「Remove Association」にチェックを入れると対象ポートとの関連付けは削除されます。

「Apply」ボタンをクリックして、設定内容を適用します。

VLAN Tunnel（VLAN トンネル）

L2 Features > VLAN Tunnel
VLAN トンネルの設定を行います。

Dot1q Tunnel（Dot1q トンネル）

802.1Q VLAN トンネルの設定、表示を行います。

802.1Q トンネルポートはサービス VLAN において「User Network Interface」(UNI) ポートとして動作します。サービス VLAN のタグ付きメンバであるトランクポートは、サービス VLAN の「Network Node Interface」(NNI) ポートとして動作します。
サービス VLAN タグ付きフレームを送受信するプロバイダブリッジネットワークに接続するポートに対し、802.1Q トンネリングイーサネットタイプを設定します。トンネルイーサネットタイプが設定されると、この値はポートの送信フレームの出力 VLAN タグ内の「Tag Protocol ID」(TPID) に指定されます。また、指定 TPID は当該ポートの受信フレームのサービス VLAN タグの識別にも使用されます。

TPID Settings タブ

L2 Features > VLAN Tunnel > Dot1q Tunnel の順にメニューをクリックし、以下の画面を表示します。

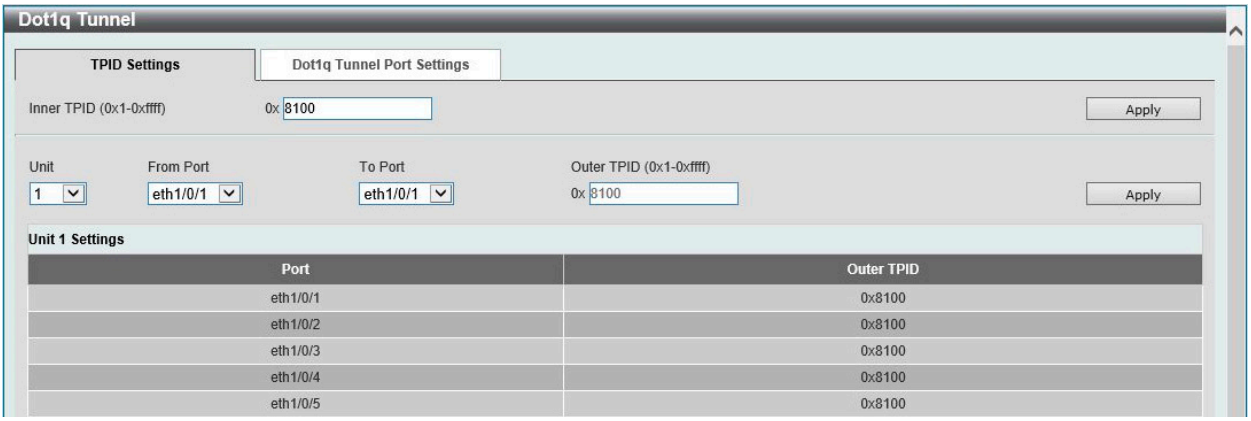


図 8-36　Dot1q Tunnel 画面 - TPID Settings タブ

画面に表示される項目：

項目	説明
Inner TPID	インナー TPID 値を指定します。インナー TPID は、イングレスパケットが「C タグ付き」であるかどうかを判別するために使用されます。このインナー TPID はシステム毎に設定することができます。 • 設定可能範囲：0x1-0xFFFF（16 進数方式）
Unit	設定を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Outer TPID	アウター TPID 値を指定します。 • 設定可能範囲：0x1-0xFFFF（16 進数方式）

「Apply」ボタンをクリックして、設定内容を適用します。

Dot1q Tunnel Port Settings タブ

Dot1q Tunnel Port Settings タブをクリックすると以下の画面が表示されます。

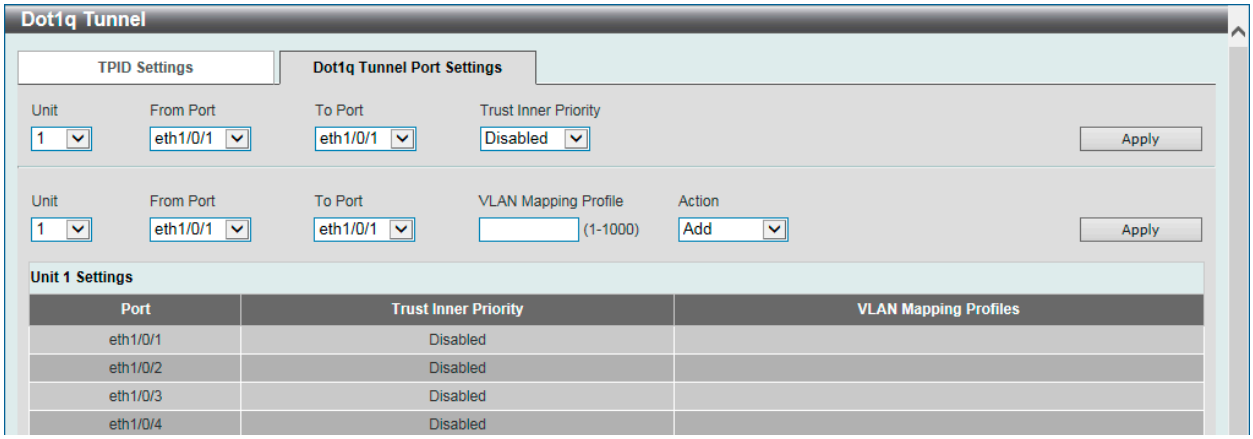


図 8-37　Dot1q Tunnel 画面 - Dot1q Tunnel Port Settings タブ

画面に表示される項目：

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Trust Inner Priority	802.1Q Inner Trust Priority機能を有効/無効に設定します。802.1Q トンネルポートで Trust Priorityオプションが有効な場合、受信パケットの VLAN タグの優先値はサービス VLAN タグにコピーされます。
VLAN Mapping Profile	VLAN マッピングプロファイル ID を指定します。各プロファイルにおいて、値の小さい方が優先度が高くなります。 • 設定可能範囲：1-1000
Action	• 「Add」- 入力した情報に基づきエントリを追加します。 • 「Remove」- 入力した情報に基づきエントリを削除します。

「Apply」ボタンをクリックして、設定内容を適用します。

VLAN Mapping（VLAN マッピング）

VLAN マッピングの設定、表示を行います。

プロファイルが適用されたインタフェースでは、プロファイルルールに従い受信パケットの照合が行われます。パケットがルールに合致すると、ルールに設定されたアクションが実行されます。このアクションには、outer VID の追加や置換、新しい outer タグの優先値設定、またはパケットの新しい inner VID の設定などがあります。
照合の順序はプロファイル内のルールのシーケンス番号に依存しており、合致するエントリが見つかると照合は停止します。シーケンス番号が設定されていない場合、番号は自動的に付与されます。シーケンス番号は、10 から始まり 10 ずつ増加します。1 つのインタフェースに対し、複数の異なるタイプのプロファイルを設定することができます。

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

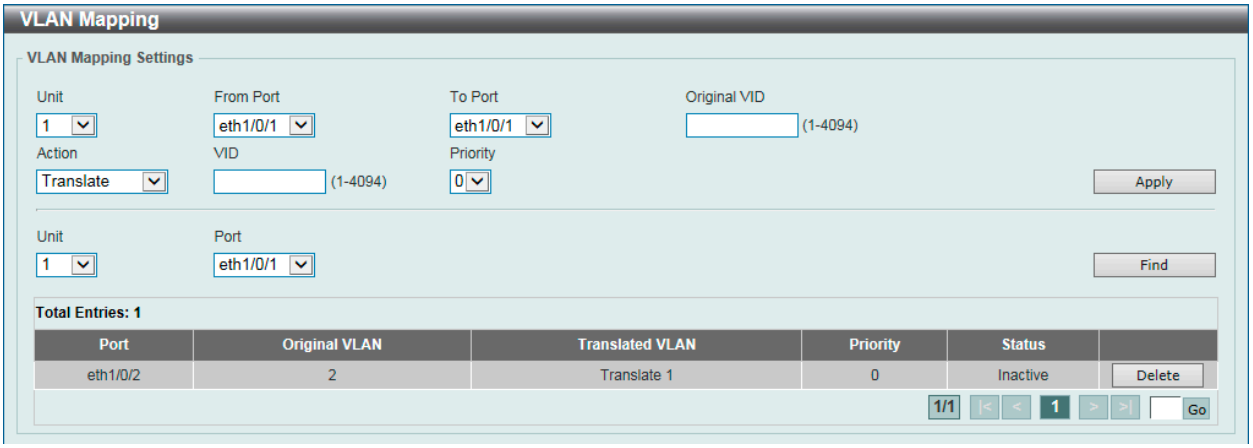


図 8-38　VLAN Mapping 画面

画面に表示される項目：

項目	説明
Unit	設定 / 検索を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Port	検索するポートを指定します。
Original VID	オリジナルの VID を指定します。 • 設定可能範囲：1-4094
Action	実行する動作を指定します。 • 「Translate」- VID が一致したパケットのアウター VID と交換する VID を指定します。 • 「Dot1q-Tunnel」- VID が一致したパケットにアウター VID を追加します。
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094
Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、指定ポートのエントリを検出します。

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。

VLAN Mapping Profile（VLAN マッピングプロファイル）

本項目では VLAN マッピングプロファイルの設定、表示を行います。

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

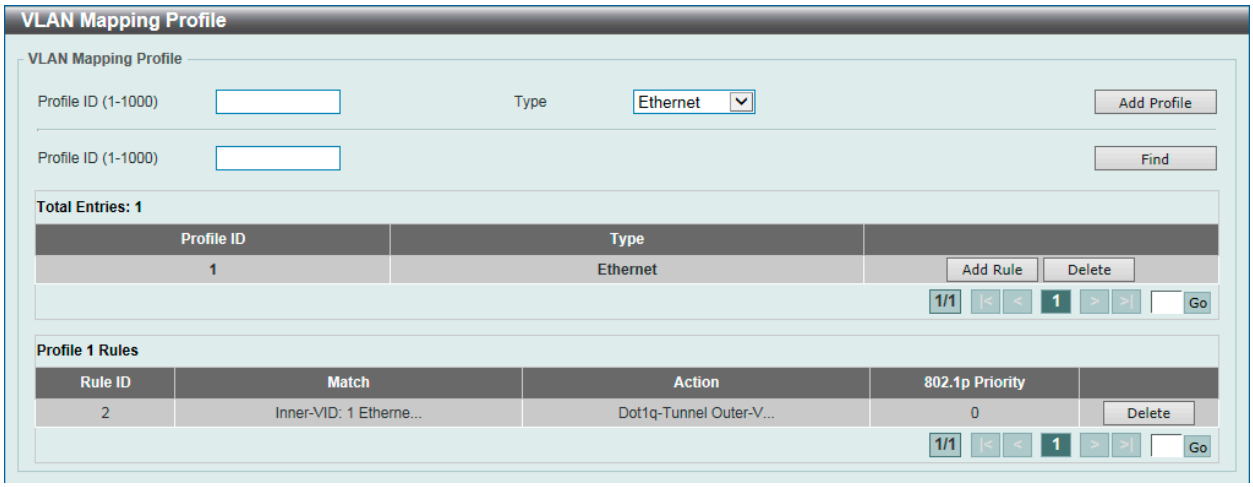


図 8-39　VLAN Mapping Profile 画面

画面に表示される項目：

項目	説明
Profile ID	VLANマッピングプロファイルのIDを入力します。各プロファイルタイプにおいて、値の小さい方が優先度が高くなります。 • 設定可能範囲：1-1000
Type	プロファイルタイプを指定します。プロファイル毎に異なるフィールドの照合を行うことができます。 •「Ethernet」- プロファイルは L2 項目を照合します。 •「IP」- プロファイルは L3 IP 項目を照合します。 •「IPv6」- プロファイルは IPv6 宛先 / 送信元アドレス項目を照合します。 •「Ethernet-IP」- プロファイルは L2/L3 IP 項目を照合します。

「Add Profile」ボタンをクリックして、新しい VLAN マッピングプロファイルを追加します。
「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。
「Add Rule」ボタンをクリックして、新しいルールを追加します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

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。

Add VLAN Mapping Rule（Ethernet）（VLAN マッピングルールの追加 /Ethernet）

「Ethernet」タイプの VLAN マッピング プロファイルを作成した後、該当プロファイルで「Add Rule」をクリックし、新しいルールを追加します。

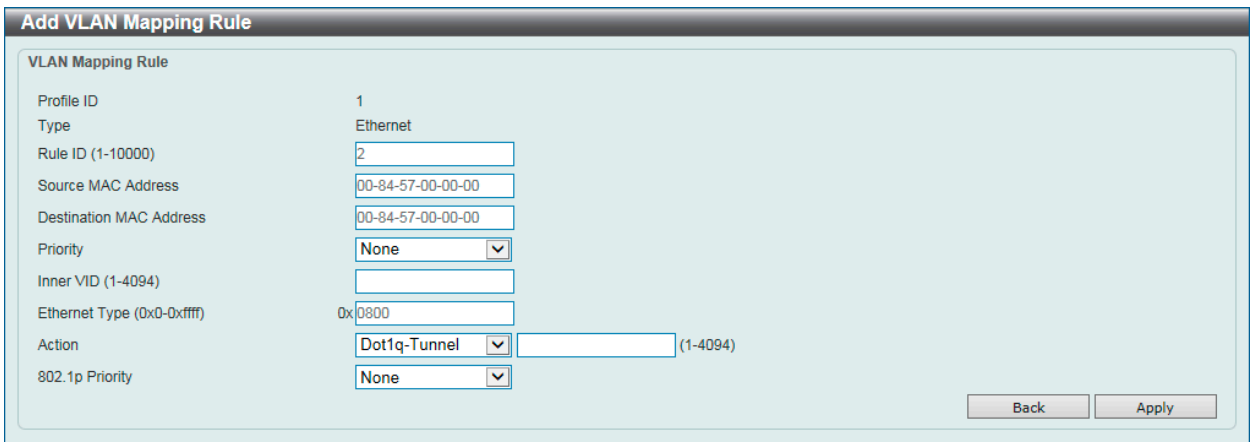


図 8-40　Add VLAN Mapping Rule（Ethernet）画面

画面に表示される項目：

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。 指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000

項目	説明
Source MAC Address	送信元 MAC アドレスを指定します。
Destination MAC Address	宛先 MAC アドレスを指定します。
Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
Inner VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
Ethernet Type	イーサネットタイプを指定します。 • 設定可能範囲：0x0-0xFFFF
Action	実行する動作を指定します。 •「Dot1q-Tunnel」- 一致したパケットにアウター VID を追加します。
802.1P Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Add VLAN Mapping Rule（IP）（VLAN マッピングルールの追加 /IP）

「IP」タイプの VLAN マッピング プロファイルを作成した後、該当プロファイルで「Add Rule」をクリックし、新しいルールを追加します。

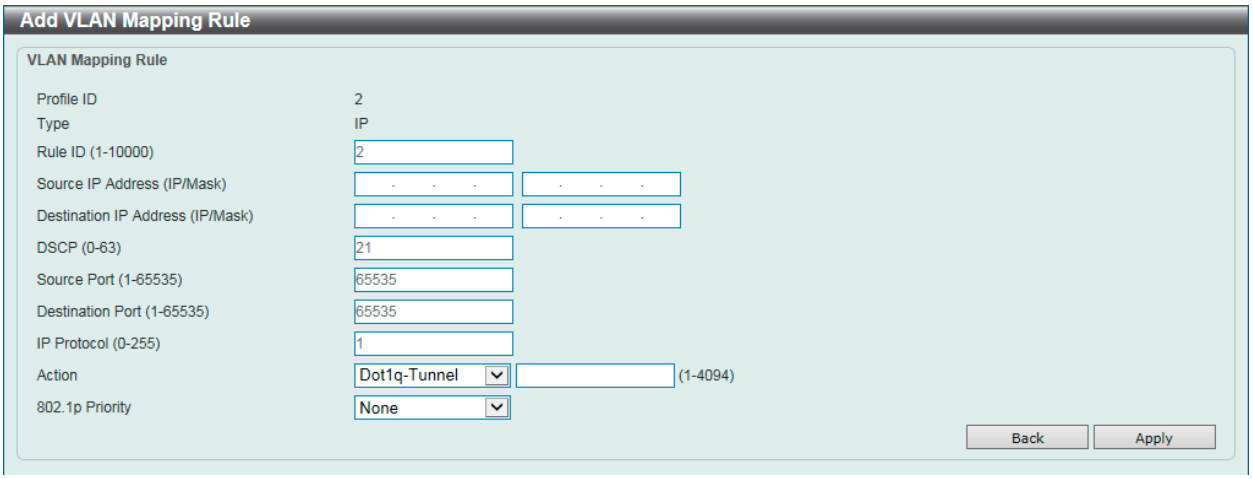


図 8-41　Add VLAN Mapping Rule（IP）画面

画面に表示される項目：

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。 指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
Source IP Address (IP/Mask)	送信元 IP アドレスとサブネットマスクを指定します。
Destination IP Address (IP/Mask)	宛先 IP アドレスとサブネットマスクを指定します。
DSCP	DSCP 値を指定します。 • 設定可能範囲：0-63
Source Port	送信元 TCP/UDP ポートを指定します。 • 設定可能範囲：1-65535
Destination Port	宛先 TCP/UDP ポートを指定します。 • 設定可能範囲：1-65535
IP Protocol	L3 IP プロトコル値を指定します。 • 設定可能範囲：0-255
Action	実行する動作を指定します。 •「Dot1q-Tunnel」- 一致したパケットにアウター VID を追加します。
802.1P Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Add VLAN Mapping Rule（IPv6）（VLAN マッピングルールの追加 /IPv6）

「IPv6」タイプの VLAN マッピング プロファイルを作成した後、該当プロファイルで「Add Rule」をクリックし、新しいルールを追加します。

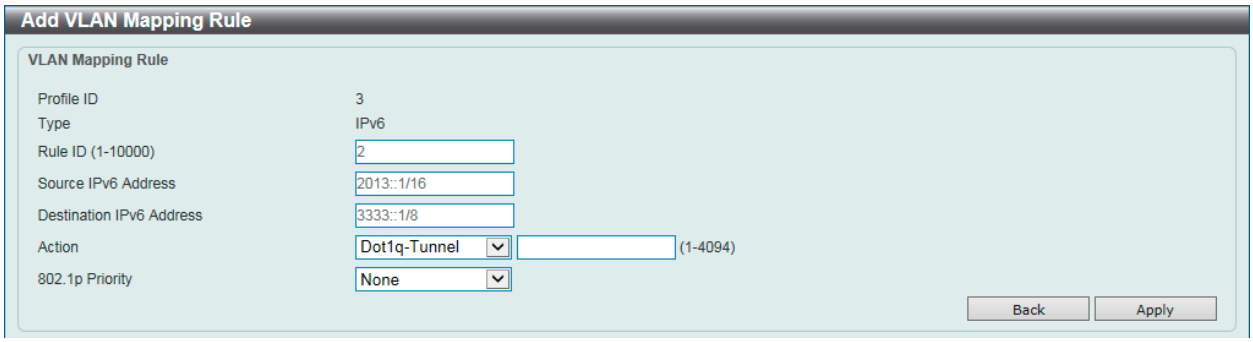


図 8-42　Add VLAN Mapping Rule（IPv6）画面

画面に表示される項目：

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。 指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
Source IPv6 Address	送信元 IPv6 アドレスとプレフィックス長を指定します。
Destination IPv6 Address	宛先 IPv6 アドレスとプレフィックス長を指定します。
Action	実行する動作を指定します。 •「Dot1q-Tunnel」- 一致したパケットにアウター VID を追加します。
802.1P Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Add VLAN Mapping Rule（Ethernet-IP）（VLAN マッピングルールの追加 /Ethernet-IP）

「Ethernet-IP」タイプの VLAN マッピング プロファイルを作成した後、該当プロファイルで「Add Rule」をクリックし、新しいルールを追加します。

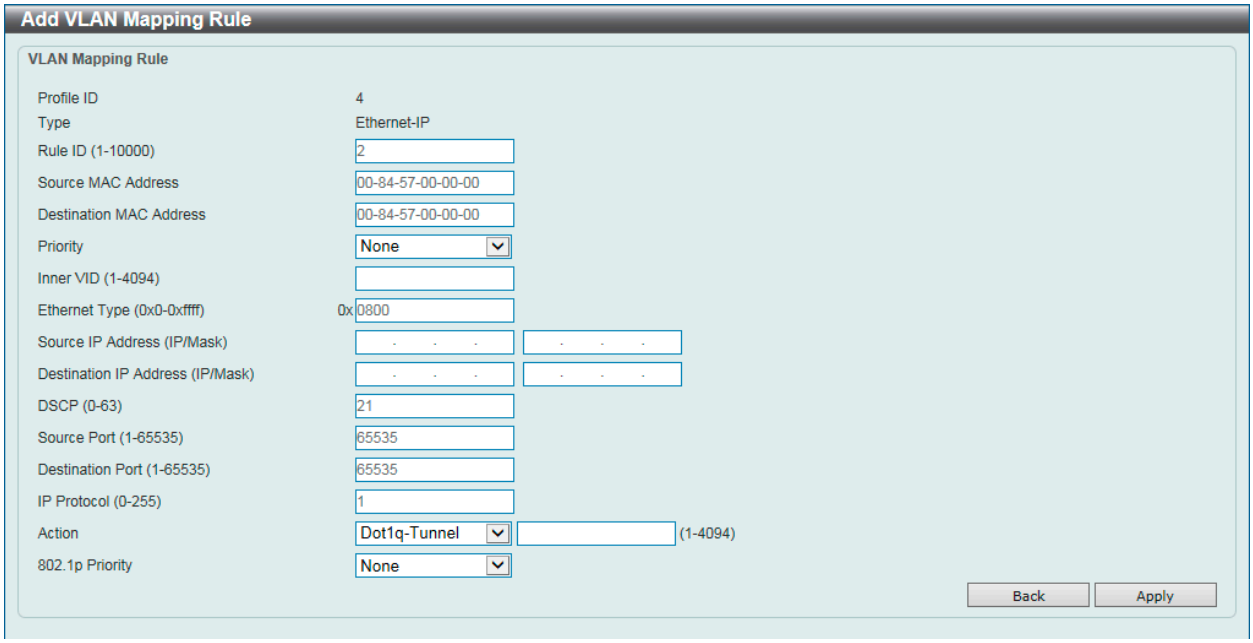


図 8-43　Add VLAN Mapping Rule（Ethernet-IP）画面

画面に表示される項目：

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。 指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
Source MAC Address	送信元 MAC アドレスを指定します。
Destination MAC Address	宛先 MAC アドレスを指定します。

項目	説明
Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
Inner VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
Ethernet Type	イーサネットタイプを指定します。 • 設定可能範囲：0x0-0xFFFF
Source IP Address (IP/Mask)	送信元 IP アドレスとサブネットマスクを指定します。
Source IP Address (IP/Mask)	宛先 IP アドレスとサブネットマスクを指定します。
DSCP	DSCP 値を指定します。 • 設定可能範囲：0-63
Source Port	送信元 TCP/UDP ポートを指定します。 • 設定可能範囲：1-65535
Destination Port	宛先 TCP/UDP ポートを指定します。 • 設定可能範囲：1-65535
IP Protocol	L3 IP プロトコル値を指定します。 • 設定可能範囲：0-255
Action	実行する動作を指定します。 •「Dot1q-Tunnel」- 一致したパケットにアウター VID を追加します。
802.1P Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

STP（スパニングツリー設定）

L2 Features > STP

本スイッチは 3 つのバージョンのスパニングツリープロトコル（IEEE 802.1D-1998 STP、IEEE 802.1D-2004 Rapid STP、および IEEE 802.1Q-2005 MSTP）をサポートしています。ネットワーク管理者の間では IEEE 802.1D-1998 STP が最も一般的なプロトコルとして認識されていますが、D-Link のマネジメントスイッチには IEEE 802.1D-2004 RSTP と IEEE 802.1Q-2005 MSTP も導入されています。これらの技術について、以下に概要を紹介します。また、802.1D-1998 STP、802.1D-2004 RSTP および 802.1Q-2005 MSTP の設定方法についても説明します。

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、ネットワーク上に複数の経路を提供します。ロードバランシングが可能となるため、 1 つのインスタンスに障害が発生した場合でも、広い範囲に影響を与えないようにすることができます。障害発生時には、障害が発生したインスタンスに代わって新しいトポロジが素早く収束されます。

VLAN が指定されたフレームは、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、相互接続されたブリッジを介して素早く適切に処理されます。

MSTI ID（MST インスタンス ID）は、これらのインスタンスをクラス分けする ID です。MSTP では、複数のスパニングツリーを CIST（Common and Internal STP）で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を判定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジのように見せかけます。そのため、VLAN が割り当てられた各フレームは、定義 VLAN の誤りや対応するスパニングツリーに関係なくシンプルで完全なフレーム処理が保持されたまま、ネットワーク上で管理用に設定されたリージョン内において異なるデータ経路を通ることができます。

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

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

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

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

802.1D-2004 Rapid STP

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

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

ポートの状態遷移

3 つのプロトコル間の根本的な相違点は、ポートがどのように Forwarding 状態に遷移するかという点と、この状態遷移がトポロジ内でのポートの役割（Forwarding/Not Forwarding）にどのように対応するかという点にあります。802.1D-1998 規格で使用されていた 3 つの状態「Disabled」「Blocking」「Listening」が、MSTP 及び RSTP では「Discarding」という 1 つの状態に統合されました。いずれの場合も、ポートはパケットの送信を行わない状態です。STP の「Disabled」「Blocking」「Listening」であっても、RSTP/MSTP の「Discarding」であっても、ネットワークトポロジ内では「非アクティブ状態」であり、機能の差はありません。以下の表では、3 つのプロトコルにおけるポートの状態遷移の違いを示しています。

トポロジの計算については、3 つのすべてのプロトコルにおいて同様に行われます。各セグメントにはルートブリッジへのパスが 1 つ存在し、すべてのブリッジで BPDU パケットをリッスンします。RSTP/MSTP では、ルートブリッジから BPDU を受信しなくても BPDU パケットが Hello パケット送信毎に送信されます。ブリッジ間の各リンクはリンクの状態を素早く検知することができるため、リンク断絶時の素早い検出とトポロジの調整が可能となります。802.1D-1998 規格では、隣接するブリッジ間においてこのような素早い状態検知が行われません。

ポート状態の比較

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

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

RSTP では、タイマ設定への依存がなくなり、Forwarding 状態への高速な遷移が可能になりました。RSTP 準拠のブリッジは、他の RSTP に準拠するブリッジリンクのフィードバックを素早く検知します。ポートはトポロジの安定を待たずに Forwarding 状態へ遷移することができます。こうした高速な状態遷移を実現するために、RSTP プロトコルでは以下の 2 つの新しい変数（Edge Port と P2P Port）が使用されています。

Edge Port

エッジポートは、ループが発生しないセグメントに直接接続しているポートに対して設定することができます。例えば、1 台のワークステーションに接続しているポートがこれに該当します。エッジポートとして指定されたポートは、Listening 及び Learning の段階を経ずに、直接 Forwarding 状態に遷移します。エッジポートは BPDU パケットを受け取った時点でそのステータスを失い、通常のスパニングツリーポートに変わります。

P2P Port

P2P ポートにおいても高速な状態遷移が可能です。P2P ポートは他のブリッジとの接続に使用されます。RSTP と MSTP では、手動で設定の変更が行われていない限り、全二重モードで動作しているすべてのポートは P2P ポートと見なされます。

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

RSTP や MSTP はレガシー機器と相互運用が可能で、必要に応じて BPDU パケットを 802.1D-1998 形式に自動的に変換することができます。ただし、802.1D-1998 STP を使用しているセグメントでは、MSTP や RSTP の利点である高速な状態遷移やトポロジ変更の検出を享受することはできません。また、これらのプロトコルでは、セグメント上でレガシー機器の更新により RSTP や MSTP を使用する場合に必要となる変数が用意されており、マイグレーションの際に使用されます。

2 つのレベルで動作するスパニングツリープロトコル

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

STP Global Settings（STP グローバル設定）

STP をグローバルに設定します。

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

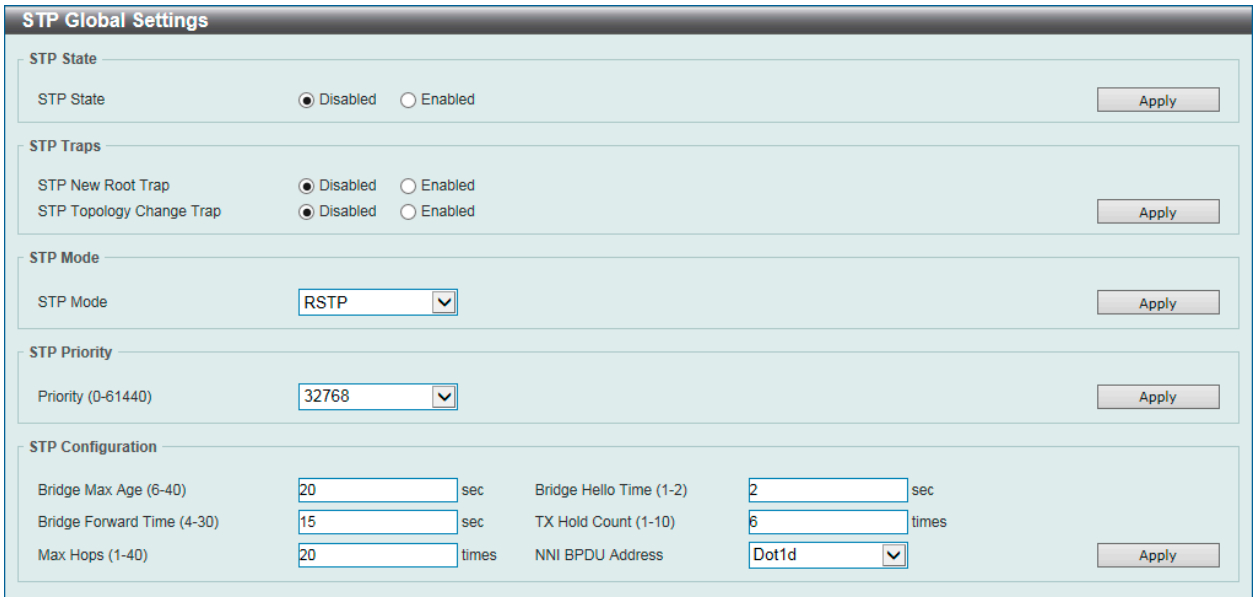


図 8-44　STP Global Settings 画面

画面に表示される項目：

項目	説明
STP State	
STP State	STP のグローバルステータスを有効 / 無効に設定します。
STP Traps	
STP New Root Trap	新しいルートトラップ送信を有効 / 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有効 / 無効に設定します。
STP Mode	
STP Mode	スイッチで使用する STP のバージョンを選択します。 • 「MSTP」- スイッチ上で MSTP 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。 • 「STP」- スイッチ上で STP がグローバルに使用されます。
STP Priority	
Priority	STP 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。 • 設定可能範囲：0-61440 • 初期値：32768
STP Configuration	
Bridge Max Age	ブリッジの最大エージタイマを設定します。 本項目は、古い情報がネットワーク内の冗長パスを無限に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。この値はルートブリッジによりセットされ、ブリッジで相互接続された LAN 内のデバイスと本スイッチの STP 設定値が整合性を持っていることを確認するために使用されます。 • 設定可能範囲：6-40（秒） • 初期値：20（秒）
Bridge Hello Time	Bridge Hello タイムを入力します。 ルートブリッジは、他のスイッチに自身がルートブリッジであることを示すために BPDU パケットを送信します。本値は、BPDU パケットの送信間隔です。「STP Mode」で STP または RSTP が選択された場合にのみ本項目が表示されます。MSTP については、Hello Time はポートごとに設定される必要があります。 • 設定可能範囲：1-2（秒） • 初期値：2（秒）
Bridge Forward Time	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。 • 設定可能範囲：4-30（秒） • 初期値：15（秒）

項目	説明
Tx Hold Count	Hello パケットの最大送信回数を指定します。 • 設定可能範囲：1-10（回） • 初期値：6（回）
Max Hops	スパニングツリー範囲のデバイス間で、スイッチが送信した BPDU パケットが破棄されるまで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。0 に到達すると、BPDU パケットが破棄され、ポートに保持していた情報は解放されます。 • 設定可能範囲：1-40 • 初期値：20
NNI BPDU Address	NNI BPDU アドレスを指定します。このパラメータはサービスプロバイダネットワークの STP の BPDU プロトコルアドレスを決定するために使用されます。「802.1d STP アドレス」と「802.1ad サービスプロバイダ STP アドレス」を使用することができます。 • 選択肢：「Dot1d」「Dot1ad」

「Apply」ボタンをクリックして、設定内容を適用します。

STP Port Settings（STP ポートの設定）

STP をポートごとに設定します。

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

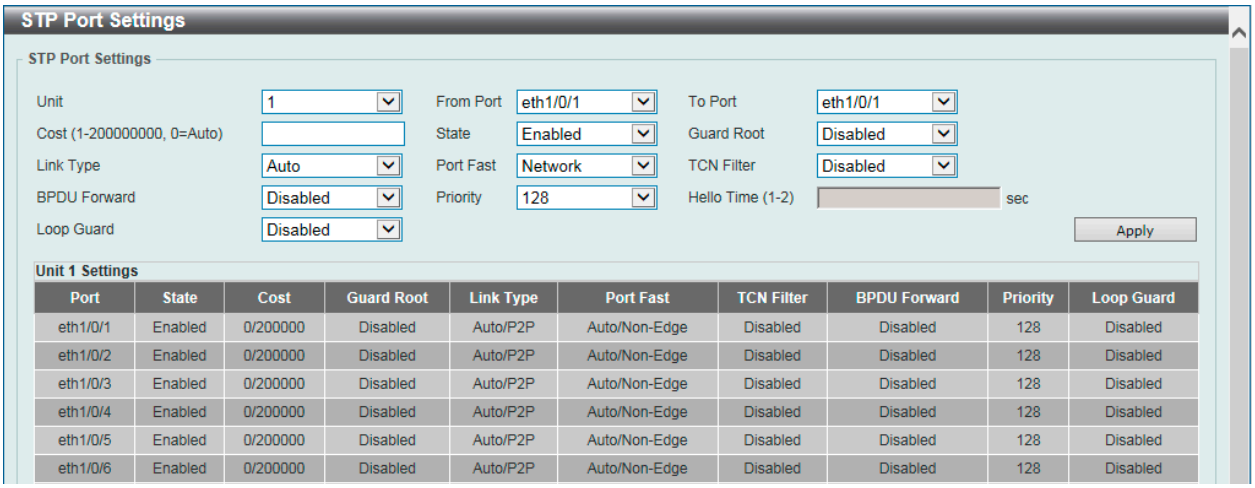


図 8-45　STP Port Settings 画面

画面に表示される項目：

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Cost	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。ポートのコストは自動か、メトリックの値で設定します。 • 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。（初期値） • 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。数字が小さいほどパケット転送は頻繁に行われるようになります。 ポートコストの初期値は以下の通りです。 • 10Mbps：2000000、100Mbps：200000、1Gbps：20000、10Gbps：2000
State	指定ポートに対し、STP の有効 / 無効を設定します。
Guard Root	Guard Root を有効 / 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 ポートとして判別されます。Shared 設定の場合、ポートは即時に Forwarding 状態にはなりません。 • 選択肢：「Auto」「P2P」「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。 • 「Network」- ポートは 3 秒だけ非ポートファスト状態に残ります。BPDU が受信されない場合、ポートファスト状態に移行し、その後転送状態に移行します。その後、BPDU を受信すると非ポートファスト状態へ戻ります。 • 「Disabled」- ポートは常に非ポートファスト状態です。常に「forward-time delay」の時間待機し、転送状態へ移行します。 • 「Edge」- リンクアップ発生時、ポートは「forward-time delay」の時間を待たずに直接 STP 転送状態に移行します。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。

項目	説明
TCN Filter	TCN（Topology Change Notification）フィルタを有効 / 無効に設定します。 本オプションが有効な場合、ポートで受信した TC イベントは無視されます。 • 初期値：「Disabled」（無効）
BPDU Forward	BPDU パケットの転送を有効 / 無効に設定します。 本オプションが有効な場合、受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。 • 初期値：「Disabled」（無効）
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。 • 設定可能範囲：0-240 • 初期値：128
Hello Time	ハロータイムの値を指定します。この設定は指定ポートによる各設定メッセージの定期的な送信の間隔となります。 • 設定可能範囲：1- 2（秒）
Loop Guard	指定ポートでのループガードを有効 / 無効に設定します。 本機能は、L2 フォワーディングループ（STP ループ）に対する追加の防御機能です。STP ループは、冗長トポロジ内の STP ブロッキングポートが、誤ってフォワーディングステートへ移行する際に発生します。これは通常、物理冗長トポロジ内のポートの一つ（必ずしも STP ブロッキングポートではない）が、STP BPDU を受信しなくなることにより発生します。このような状況において、BPDU の送受信はポートに割り当てられた役割に依存することになります。つまり、指定ポート（Designated Port）は BPDU を送信し、非指定ポート（Non Designated Port）は BPDU を受信します。 物理冗長ポロジのポートの一つが BPDU を受信しなくなると、STP はトポロジをループ解除状態と認識します。これにより、ブロッキング / バックアップポートであった代替ポートが、指定ポート（Designated Port）となりフォワーディングステートに移行します。この結果ループが発生します。

「Apply」ボタンをクリックして、設定内容を適用します。

MST Configuration Identification（MST の設定）

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

L2 Features > 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。

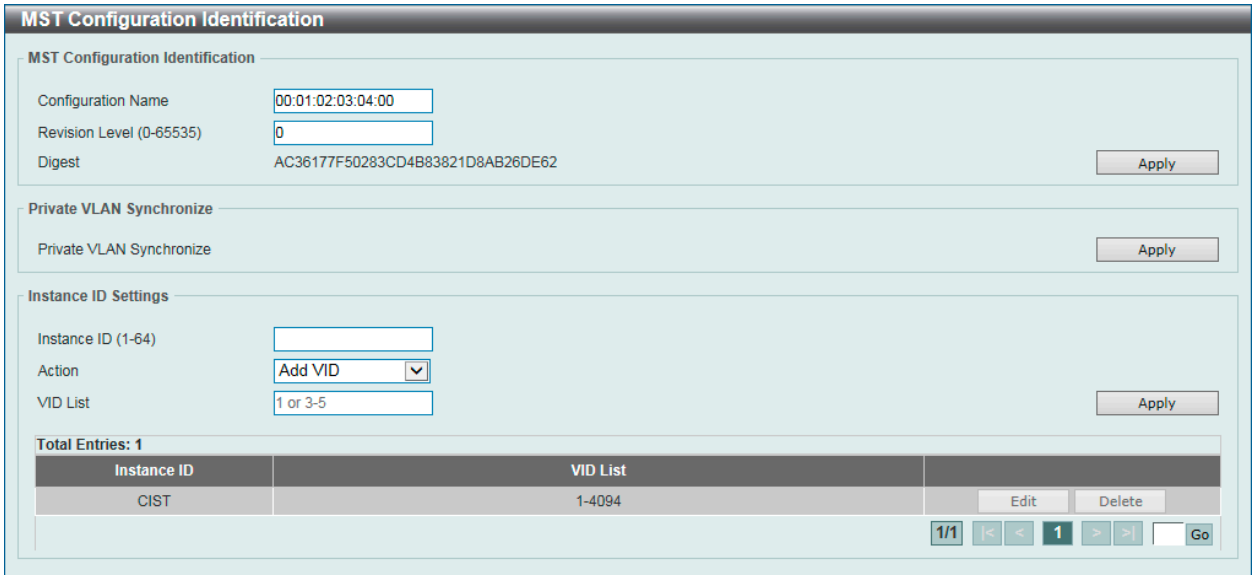


図 8-46　MST Configuration Identification 画面

画面に表示される項目：

項目	説明
MST Configuration Identification	
Configuration Name	MSTI（Multiple Spanning Tree Instance）を識別するための名前を設定します。 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	MST リビジョンの値を設定します。 Configuration Name とともに、スイッチ上の MSTP リビジョンを識別するために使用します。 • 設定可能範囲：0-65535 • 初期値：0
Private VLAN Synchronize	
Private VLAN Synchronize	「Apply」ボタンをクリックし、プライベート VLAN の同期を行います。

項目	説明
Instance ID Settings	
Instance ID	スイッチにインスタンス ID を設定します。 • 設定可能範囲：1-64
Action	MSTI に行う変更を選択します。 • 「Add VID」- VID List 項目で指定された VID を MSTI ID に追加します。 • 「Remove VID」- VID List 項目で指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

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

STP インスタンスの設定を行います。

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

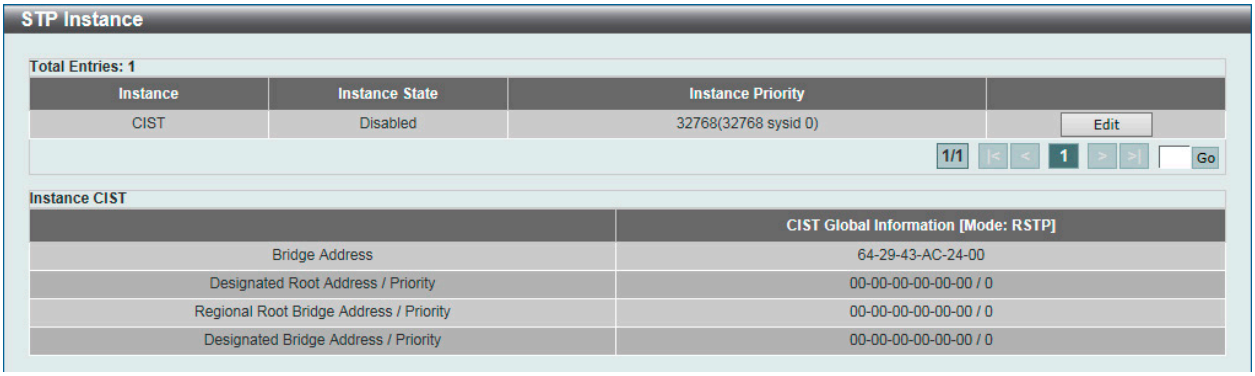


図 8-47　STP Instance 画面

画面に表示される項目：

項目	説明
Instance Priority	「Edit」をクリック後、当該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

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

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のページへ移動します。

MSTP Port Information（MSTP ポート情報）

MSTP（Multiple Spanning Tree Protocol）ポート情報を表示、編集します。

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。

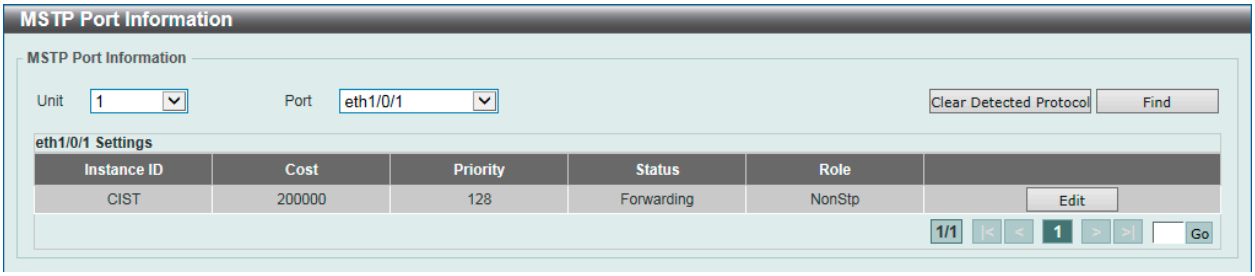


図 8-48　MSTP Port Information 画面

画面に表示される項目：

項目	説明
Unit	エントリを表示 / 削除するユニットを指定します。
Port	エントリを表示 / 削除するポートを選択します。

項目	説明
Cost	「Edit」をクリックした後、パケットを転送するコストを設定します。 • 設定可能範囲：1-200000000
Priority	「Edit」をクリックした後、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。 • 設定可能範囲：0-240 • 初期値：128

「Clear Detected Protocol」ボタンをクリックして、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。
「Find」ボタンをクリックして、指定ポートの MSTP 設定を参照します。
「Edit」ボタンを選択して、指定エントリのパラメータを編集します。「適用」をクリックし、設定内容を適用します。

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。発達したイーサネット OAM（Operations, Administration, Maintenance）とシンプルな APS（automatic protection switching）プロトコルの統合により、リングトポロジ内でイーサネットトラフィックを保護します。これにより、イーサネットレイヤにループが形成されないようにします。

リング内の 1 つのリンクが、ループを回避するためにブロックされます（RPL : Ring Protection Link）。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。ERPS を有効化する前に、STP とループバック検知 (LBD) をリングポートで無効にする必要があります。ERPS は「R-APS VLAN」リングポート、RPL ポート、RPL オーナが設定されていない状態では、有効にできません。

注意　ERPS バージョンを変更するとプロトコルが再起動します。

ERPS Status タブ

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

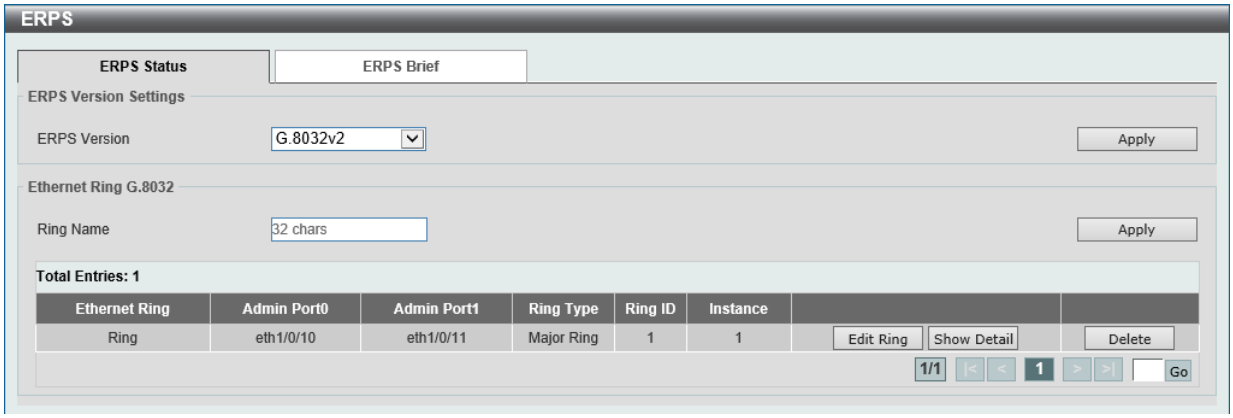


図 8-49　ERPS 画面 - ERPS Status タブ

画面に表示される項目：

項目	説明
ERPS Version Settings	
ERPS Version	ERPS バージョンを選択します。 • 選択肢：「G.8032v1」「G.8032v2」 「G.8032v2」では以下の機能をサポートしています。 - 物理リング内のマルチインスタンス - 「manual」「force」「clear」などの操作コマンド - 物理リングの RING-ID を持つ R-APS PDU 宛先アドレスの送信の設定

項目	説明
	「G.8032v2」を実行している機器に対し「G.8032v1」を設定する前に、「G.8032v1」がサポートしない全ての ERPS 設定を削除する必要があります。そうでない場合バージョンの変更は行えません。ERPS バージョンを変更すると、実行中のプロトコルは再起動します。 「G.8032v2」から「G.8032v1」へ変更する前に、次の設定であることをチェックする必要があります。 • 手動（Manual）または強制（force）スイッチコマンドの消去 • 相互接続のメジャーリングインスタンスとサブリングインスタンス機器が、それぞれ異なる「R-APS VLAN ID」を保持していること • 物理リング内で一つのインスタンスのみをサポート イーサネットリングで「ITU-T G.8032v1」と「ITU-T G.8032v2」のイーサネットリングノードが同時に存在している場合、「G.8032v2」機器に対して次の設定を行う必要があります。 • 全ての物理リング ID は初期値の 1 であること • 相互接続ノードのメジャーリングインスタンスとサブリングインスタンス機器が、それぞれ異なる「R-APS VLAN ID」を保持していること • Manual Switch または Force Switch コマンドが削除されていること • 物理リング内で一つのインスタンスのみをサポート
Ethernet Ring G.8032	
Ring Name	ERP インスタンス名を入力します。（32 文字以内）

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

■ Ring の編集

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

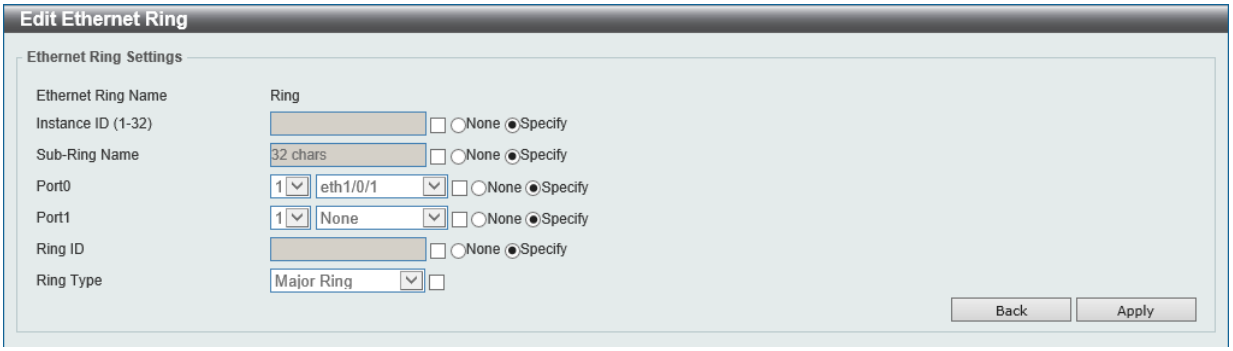


図 8-50　ERPS（Edit Ring）- Edit Ethernet Ring 画面

画面に表示される項目：

項目	説明
Instance ID	チェックボックスにチェックを入れ、「ERP インスタンス」の番号を指定します。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-32
Sub-Ring Name	チェックボックスにチェックを入れ、「サブリング名」を指定します。（32 文字以内） 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Port0	チェックボックスにチェックを入れ、初期リングになるユニット ID とポート番号を指定します。 ドロップダウンメニューから「None」を選択すると、相互接続されたノードがオープンリングのローカルノードエンドポイントとして指定されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Port1	チェックボックスにチェックを入れ、2 番目のリングになるユニット ID とポート番号を指定します。 ドロップダウンメニューから「None」を選択すると、相互接続されたノードがオープンリングのローカルノードエンドポイントとして指定されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Ring ID	チェックボックスにチェックを入れ、リング ID を指定します。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-239
Ring Type	チェックボックスにチェックを入れ、リングタイプを指定します。 • 選択肢：「Major Ring」「Sub Ring」

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ERP リング詳細情報の表示
「Show Detail」ボタンをクリックすると、以下の詳細画面が表示されます。

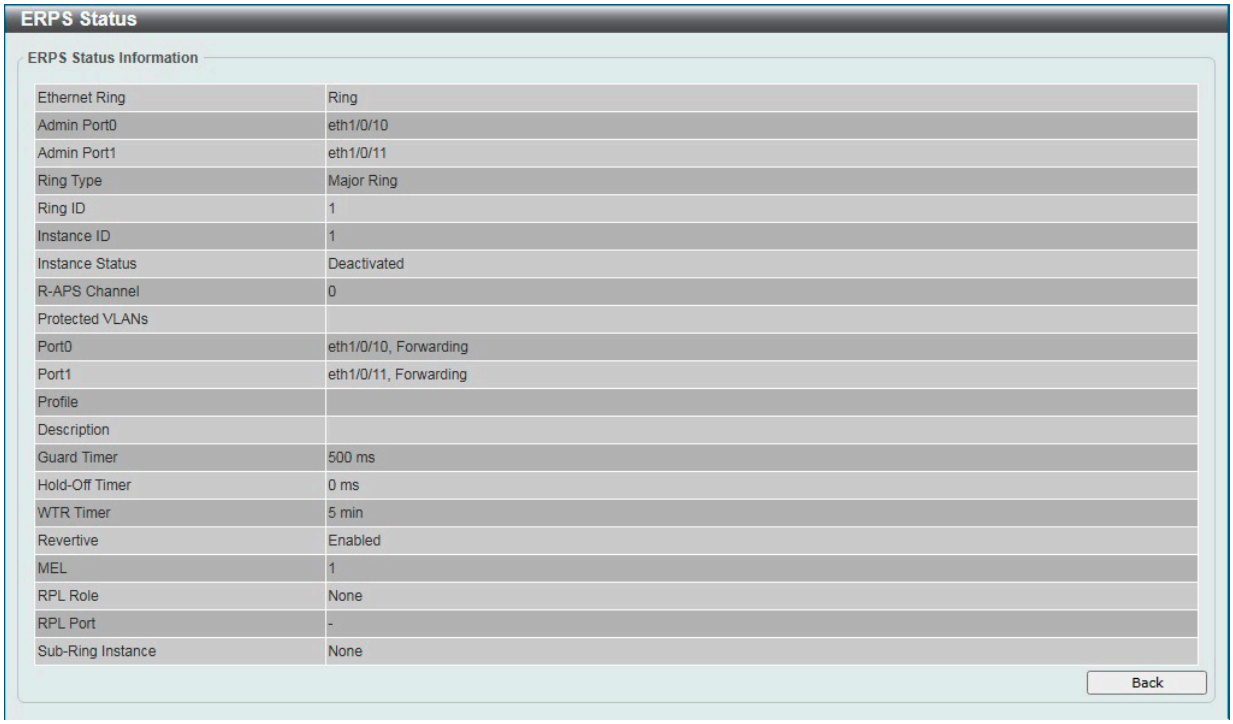


図 8-51　ERPS（Show Detali）- ERPS Status 画面

前の画面に戻るには、「Back」ボタンをクリックします。

「ERPS Brief」タブの表示

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

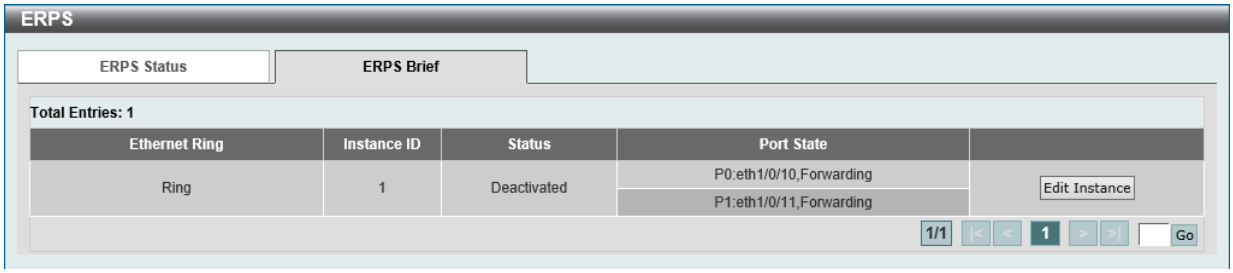


図 8-52　ERPS 画面 - ERPS Brief タブ

「Edit Instance」ボタンをクリックして、ERP インスタンスを設定します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

■ Instance の編集（Edit Instance）

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

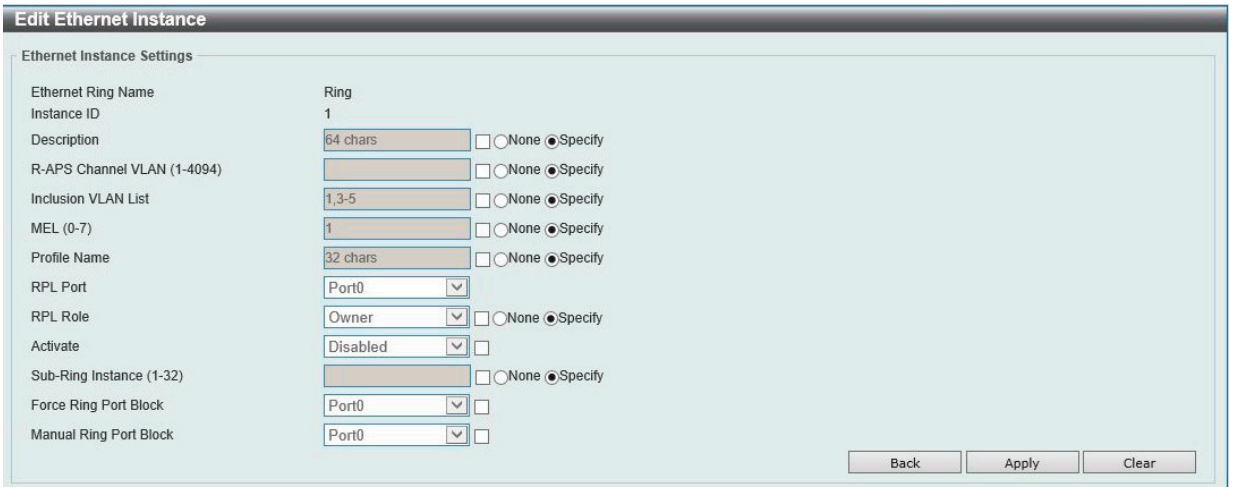


図 8-53　ERPS（ERPS Brief, Edit Instance）- Edit Ethernet Instance 画面

画面に表示される項目：

項目	説明
Description	チェックボックスにチェックを入れ、「ERP インスタンス」の説明を入力します。（64 文字以内） 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
R-APS Channel VLAN	チェックボックスにチェックを入れ、「ERP インスタンス」の「R-APS Channel VLAN ID」を指定します。サブインスタンスの「APS channel VLAN」はサブリングの仮想チャネルでもあります。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-4094
Inclusion VLAN List	チェックボックスにチェックを入れ、インスタンスに含まれる VLAN リストを指定します。 VLAN 範囲や個別の指定が可能です（例：「VLAN1 から 5」は「1-5」、「VLAN1 と 3 と 5」は「1,3,5」）。指定された VLAN は ERP のメカニズムで保護されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
MEL	チェックボックスにチェックを入れ、ERP インスタンスの「MEL」を指定します。 同じ ERP インスタンスに所属する全てのリングノードの MEL 値は同じ値である必要があります。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：0-7
Profile Name	チェックボックスにチェックを入れ、ERP インスタンスに関連付ける「G.8032」のプロファイルを指定します（32 文字以内）。同じ G.8032 プロファイルに複数の ERP インスタンスを含めることも可能です。同じプロファイルに含まれる各インスタンスは、同じ VLAN セットを保護します。つまり、この場合 VLAN セットは複数の異なるインスタンスに保護されることになります。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
RPL Port	「RPL Role」右横のチェックボックスにチェックを入れ、RPL ポートオプションを選択します。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」
RPL Role	チェックボックスにチェックを入れ、ノードの種類を選択します。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 選択肢：「Owner」「Neighbor」
Activate	チェックボックスにチェックを入れ、ERP インスタンスをアクティブにするかどうかを選択します。「Enabled」の場合、ERP インスタンスはアクティブになります。 • 選択肢：「Enabled」「Disabled」
Sub-Ring Instance	チェックボックスにチェックを入れ、ERP インスタンスの識別子を指定します。物理リングインスタンスのサブリングインスタンスを指定する場合に使用されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-32
Force Ring Port Block	チェックボックスにチェックを入れ、ブロックされる ERP インスタンスポートを選択します。リンク不具合などの発生有無にかかわらず、本設定が有効になると即時にインスタンスポートがブロックされます。 • 選択肢：「Port0」「Port1」
Manual Ring Port Block	チェックボックスにチェックを入れ、ブロックされる ERP インスタンスポートを選択します。リンク不具合や FS（強制切替）がない場合、MS が設定されたポートがブロックされます。 • 選択肢：「Port0」「Port1」

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、このエントリに関連付けられた強制 / 手動の設定をクリアします。
前の画面に戻るには、「Back」ボタンをクリックします。

ERPS Profile（ERPS プロファイル）

ERPS プロファイル設定を行います。

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

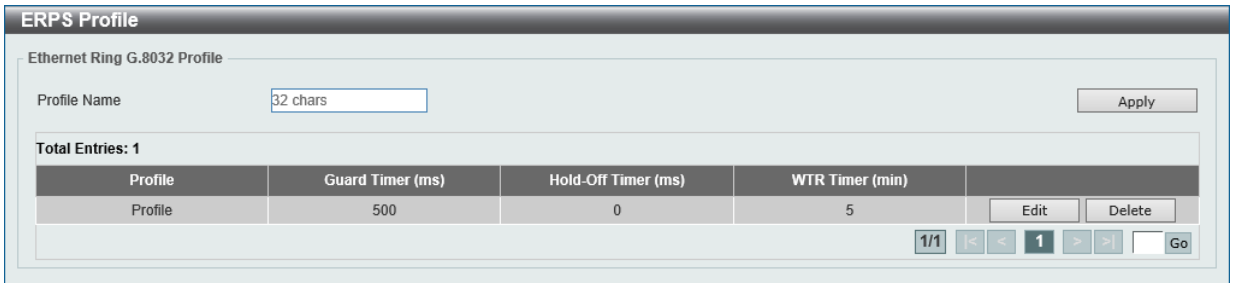


図 8-54　ERPS Profile 画面

画面に表示される項目：

項目	説明
Profile Name	「G.8032」のプロファイル名を指定します（32 文字以内）。 複数の ERP インスタンスを同じ「G.8032」プロファイルに関連づけることができます。同じプロファイルに含まれる各インスタンスは、同じ VLAN セットを保護します。つまり、この場合 VLAN セットは複数の異なるインスタンスに保護されることになります。

「Apply」ボタンをクリックして、「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」ボタンをクリックして、「G.8032」プロファイルを編集します。

■「G.8032」プロファイルの編集

「Edit 」ボタンをクリックすると、以下の設定画面が表示されます。

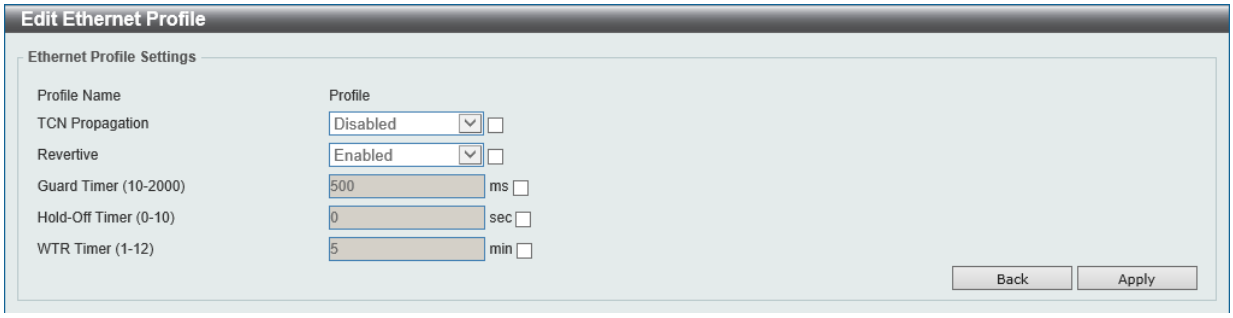


図 8-55　ERPS Profile（Edit）- Edit Ethernet Profile 画面

画面に表示される項目：

項目	説明
TCN Propagation	チェックボックスにチェックを入れ、「TCN Propagation」の設定を行います。 本機能はサブ ERP インスタンスからメジャーインスタンスへのトポロジ変更の通知の伝播を有効にします。 • 選択肢：「Enabled（有効）」「Disabled（無効）」
Revertive	チェックボックスにチェックを入れ、「Revertive」ステータスの設定を行います。 RPL がブロックされた場合などに、稼働中の送信エンティティに戻すために使用されます。 • 選択肢：「Enabled（有効）」「Disabled（無効）」
Guard Timer	チェックボックスにチェックを入れ、Guard Timer の設定を行います。 • 設定可能範囲：10-2000（ミリ秒） • 初期値：500（ミリ秒）
Hold-Off Timer	チェックボックスにチェックを入れ、Hold-Off Timer の設定を行います。 • 設定可能範囲：0-10（秒） • 初期値：0（秒）
WTR Timer	チェックボックスにチェックを入れ、Wait To Restore（WTR）Timer の設定を行います。 • 設定可能範囲：1-12（分） • 初期値：5（分）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Loopback Detection（ループバック検知設定）

ループバック検知（LBD）機能は、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。本機能は、CTP(Configuration Testing Protocol) パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN で受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートは再起動 (Normal 状態へ遷移) を行います。

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

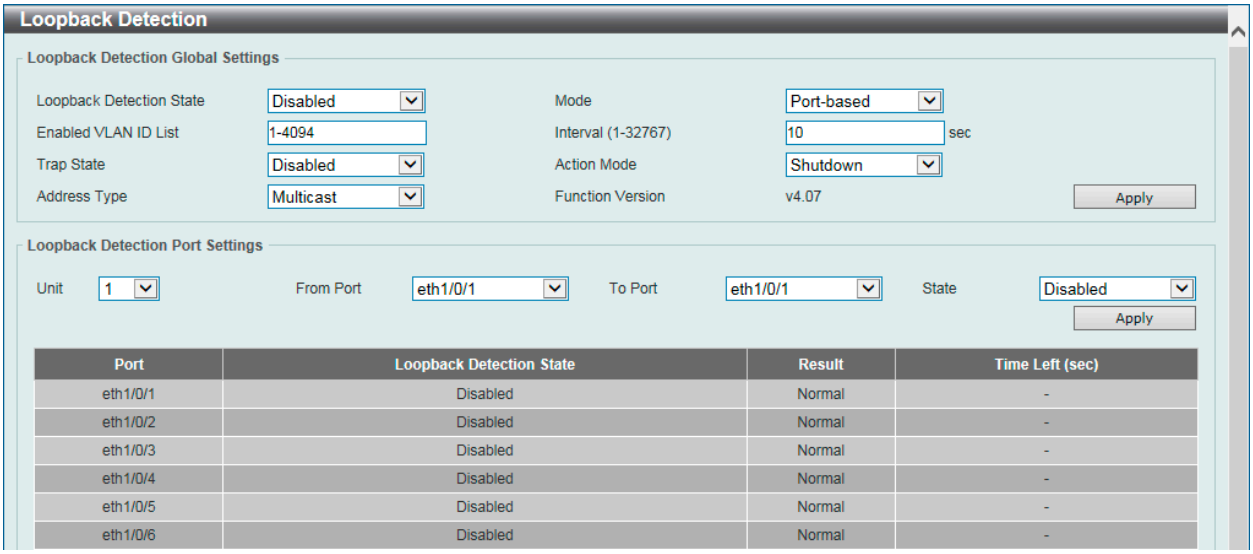


図 8-56　Loopback Detection 画面

画面に表示される項目：

項目	説明
Loopback Detection Global Settings	
Loopback Detection State	ループバック検知機能を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
Mode	ループ検知のモードを選択します。 • 選択肢：「Port-based」「VLAN-based」
Enabled 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	ループ検知間隔を設定します。 本設定の間隔で Configuration Test Protocol（CTP）パケットが送信され、ループバックイベントを検知します。 • 設定可能範囲：1-32767（秒） • 初期値：10（秒）
Traps State	ループバック検出トラップを有効 / 無効に設定します。
Action Mode	動作モードを指定します。 • 「Shutdown」- 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。
Address Type	アドレスタイプを選択します。 • 選択肢：「Multicast」「Broadcast」
Loopback Detection Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	ポートのループバック検知ステータスを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　VLAN モードで使用した場合、CTP パケットは 100VLANs/Port/Interval ずつ送信されます。CTP は 100VLANs を検出後、該当の VLAN のみに送出されます。

Link Aggregation（リンクアグリゲーション）

ポートトランクグループについて

ポートトランクグループは、複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。トランクグループは最大 32 個まで作成可能であり、各グループには 8 個までの物理ポートを割り当てることができます。

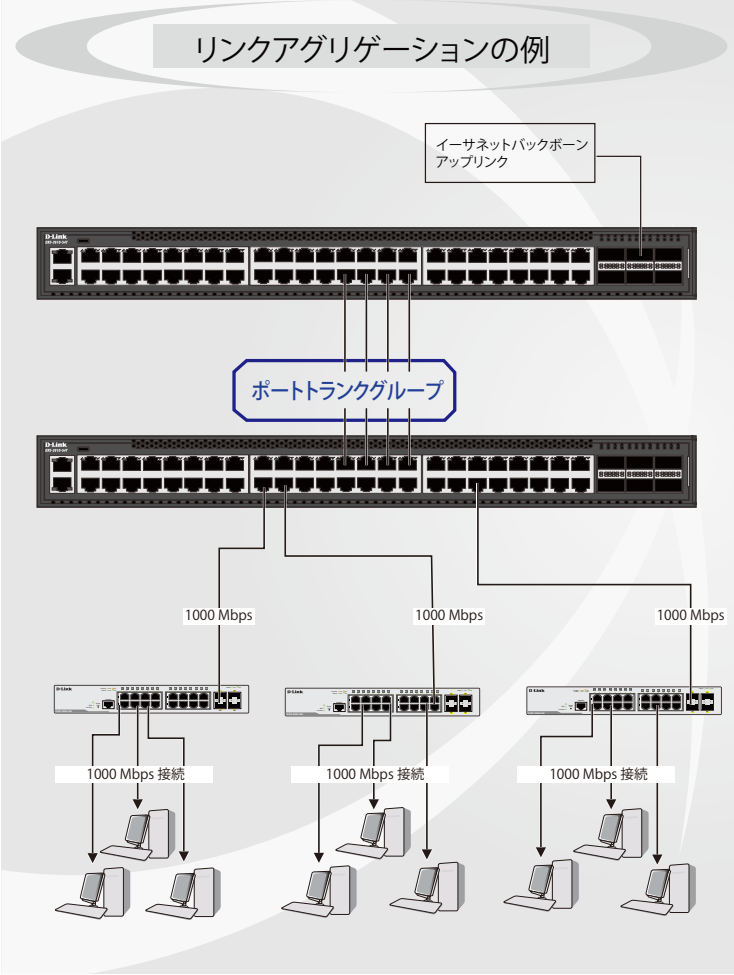


図 8-57　ポートトランクグループの例

トランクグループ内のすべてのポートは 1 つのポートと見なされます。あるホスト（宛先アドレス）へデータ転送が行われる際には、常にトランクグループ内の特定のポートが使用されるため、データは送信された順で宛先ホスト側に到着します。

リンクアグリゲーション機能により複数のポートが 1 つのグループとして束ねられ、1 つのリンクとして動作します。この時、1 つのリンクの帯域は束ねられたポート分拡張されます。リンクアグリゲーションは、サーバなどの広帯域を必要とするネットワークデバイスをバックボーンネットワークに接続する際に広く利用されています。

本スイッチでは、2 ～ 8 個のリンク（ポート）から構成される最大 32 個のリンクアグリゲーショングループの構築が可能です。各ポートは 1 つのリンクアグリゲーショングループにのみ所属することができます。グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断が発生した場合、ネットワークトラフィックはグループ内の他のリンクに振り分けられます。

スパニングツリープロトコル（STP）は、リンクアグリゲーショングループを 1 つのリンクとして扱います。スイッチに冗長化された 2 つのリンクアグリゲーショングループが設定されている場合、STP において片方のグループ全体がブロックされます。（冗長リンクを持つ 1 つのポートがブロックされるケースと同様）。

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

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

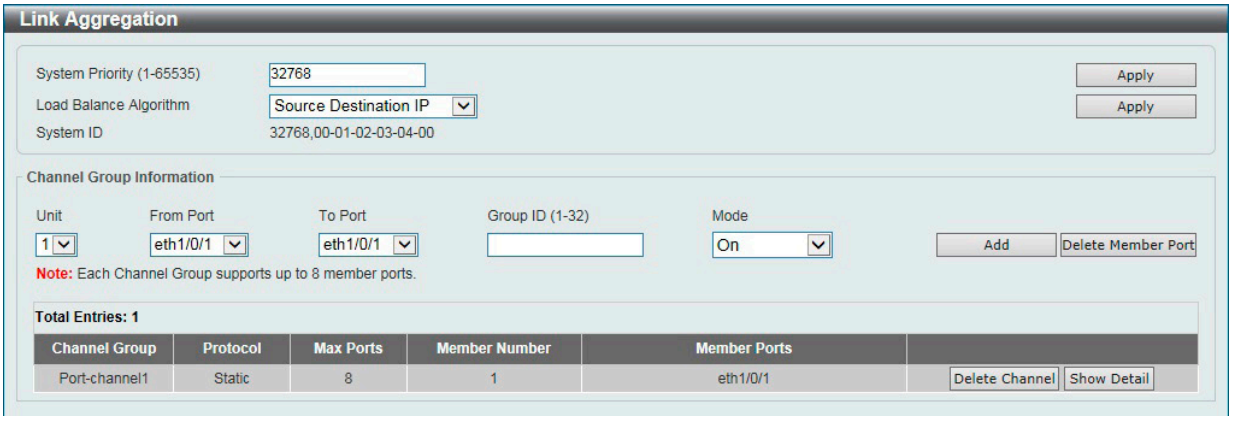


図 8-58　Link Aggregation 画面

画面に表示される項目：

項目	説明
System Priority	システムプライオリティを指定します。 本値により、接続するスイッチ間で「Actor」となるシステムが決定され、そのシステムのポートプライオリティが使用されます。値の小さい方が高い優先度を示します。システムプライオリティが同じ値の場合、MAC ID の小さいシステムが選出されます。その後、「Actor」スイッチのポートプライオリティの値により、ポートチャネルに属するかスタンドアロンモードになるかが決定します。ポートプライオリティが同じ値の場合、ポート番号で優先値が決まります。 • 設定可能範囲：1-65535 • 初期値：32768
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 Destination IP」

「Apply」ボタンをクリックして、設定内容を適用します。

Channel Group Information

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
Group ID	グループの ID 番号を設定します。 チャネルグループに物理ポートを初めて追加した際に、システムにより自動的にポートチャネルが作成されます。各インタフェースは複数のチャネルグループに参加することはできません。 • 設定可能範囲：1-32
Mode	動作モードを指定します。チャネルグループは、固定もしくは LACP メンバのどちらかのみで構成されます。チャネルグループが決定すると、他のタイプのインタフェースはそのチャネルグループに参加できません。 • 「On」- チャネルグループタイプは固定です。 • 「Active」- チャネルグループは LACP になります。LACP パケットを送信してネゴシエーションを開始します。 • 「Passive」- チャネルグループは LACP になります。LACP パケットへの応答のみ行います。

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作成します。
「Delete Channel」ボタンをクリックして、チャネルを削除します。
「Delete Member Port」ボタンをクリックして、特定グループのメンバポートを削除します。

ポートトランキンググループの設定

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

■ ポートトランキンググループの編集

「Show Detail」をクリックして、チャネルの詳細情報を表示します。以下の画面が表示されます。

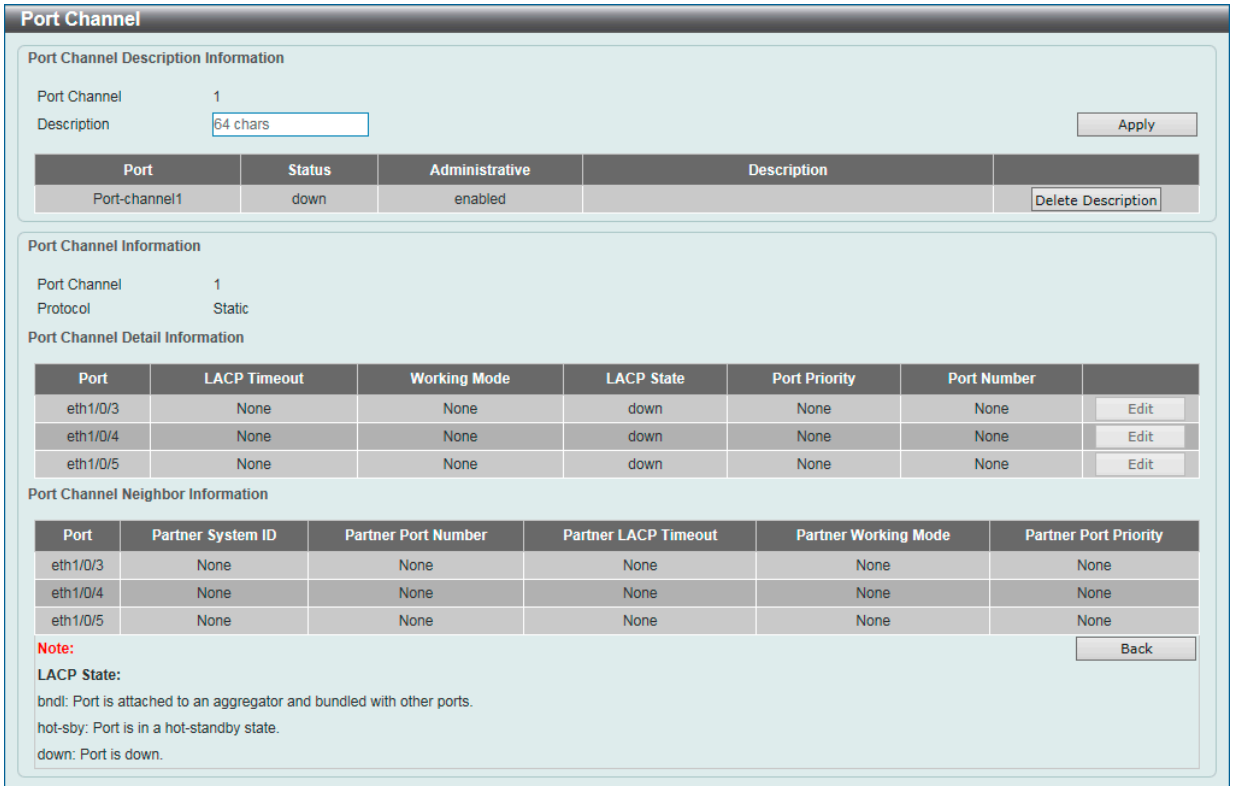


図 8-59　Link Aggregation（Show Detail）- Port Channel 画面

以下の項目が表示されます。

Port Channel Description Information

項目	説明
Description	ポートチャネルの説明を入力します。（64 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
設定内容を編集するには、「Edit」ボタンをクリックしてパラメータを設定後、「Apply」ボタンをクリックして設定内容を適用します。
「Delete Description」ボタンをクリックして、ポートチャネルの説明を削除します。

Port Channel Information

項目	説明
Port Channel Detail Information	
LACP Timeout	LACP タイムアウトを設定します。 • 選択肢：「Short」「Long」
Working Mode	動作モードを指定します。 • 「Active」- LACP パケットを送信してネゴシエーションを開始します。 • 「Passive」- LACP パケットへの応答のみ行います。
Port Priority	ポートプライオリティを設定します。値の小さい方が高い優先度を示します。

「Edit」ボタンをクリックしてパラメータを設定後、「Apply」ボタンをクリックして設定内容を適用します。

前の画面に戻るには、「Back」ボタンをクリックします。

Flex Links（フレックスリンク）

フレックスリンク機能を設定します。本機能では、レイヤ 2 インタフェースのペアを作成しインタフェースのバックアップを設定します。STP や LBD の代替機能として、リンクレベルでの冗長性を提供します。

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

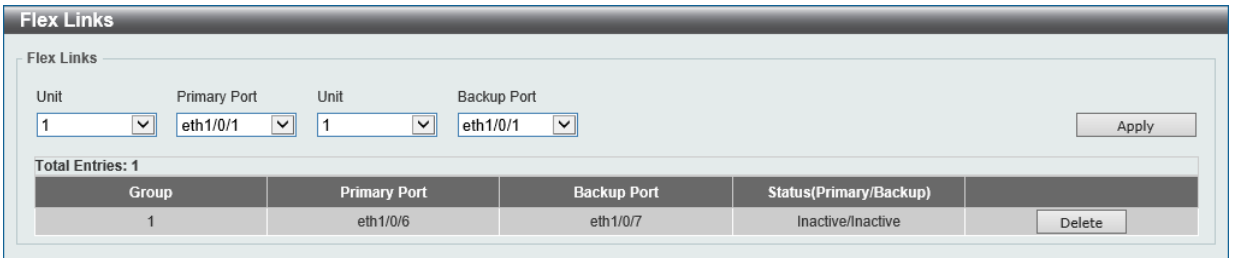


図 8-60　Flex Links 画面

画面に表示される項目：

項目	説明
Unit	プライマリポートのユニットを指定します。
Primary Port	プライマリポートを指定します。
Unit	バックアップポートのユニットを指定します。
Backup Port	バックアップポートを指定します。

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

注意　フレックスリンクは、STP、ERPS、LBD 機能と相互排他になります。

注意　フレックスリンクでは、Preemption には対応していません。

L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）

レイヤ 2 プロトコルトンネルの設定を行います。

L2 Protocol Tunnel Global Settings タブ

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

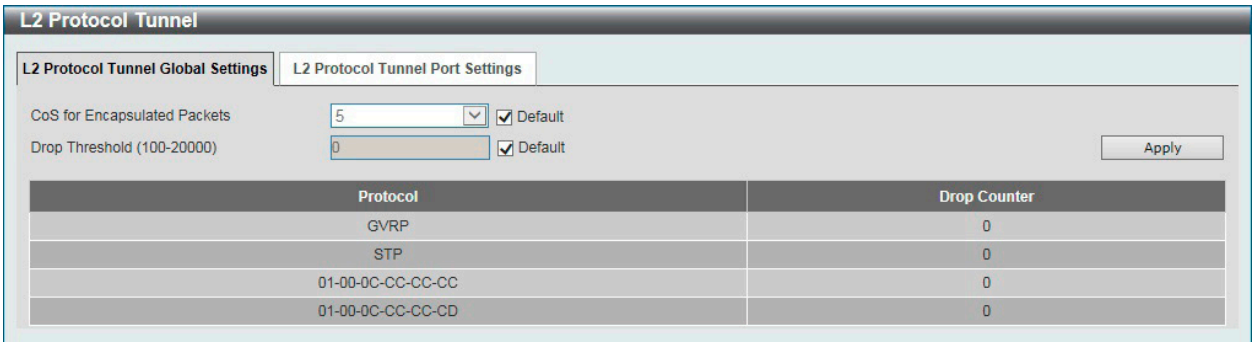


図 8-61　L2 Protocol Tunnel 画面 - L2 Protocol Tunnel Global Settings タブ

画面に表示される項目：

項目	説明
CoS for Encapsulated Packets	カプセル化されたパケットの CoS 値を指定します。「Default」を指定すると初期値を使用します。 • 設定可能範囲：0-7
Drop Threshold	破棄しきい値を指定します。 L2 プロトコルパケットのトンネリングは、パケットのカプセル化、非カプセル化、フォワーディングに CPU 処理容量を消費します。本オプションを使用することにより、システムにより処理される全 L2 プロトコルパケットの数にしきい値を設け、消費される CPU プロセス帯域を制限します。パケットの最大値がしきい値を超えた場合、超えた分のパケットは破棄されます。「Default」を指定すると初期値を使用します。 • 設定可能範囲：100-20000 • 初期値：0

「Apply」ボタンをクリックして、設定内容を適用します。

L2 Protocol Tunnel Port Settings タブ

L2 Protocol Tunnel Port Setting タブをクリックし、次の画面を表示します。

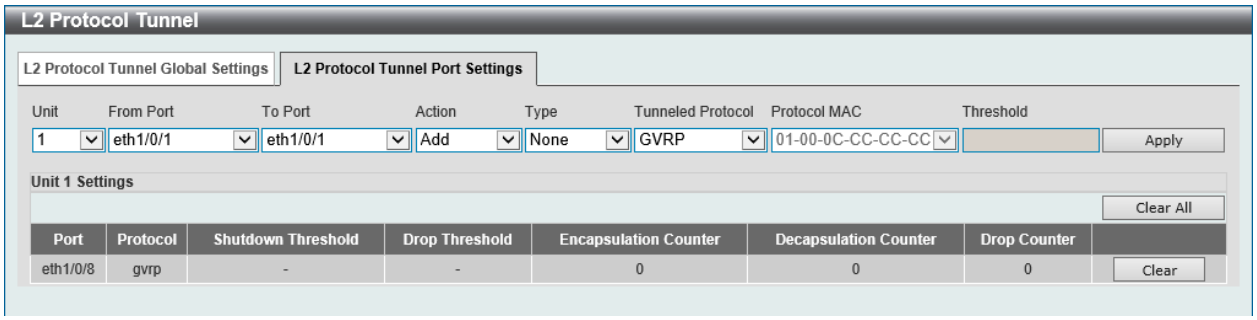


図 8-62　L 2 Protocol Tunnel 画面 - L2 Protocol Tunnel Port Settings タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Action	実行する動作を指定します。 • 「Add」- 入力した情報に基づいてエントリを追加します。 • 「Delete」- 入力した情報に基づいてエントリを削除します。
Type	指定しきい値を超えた際に実行されるアクションを指定します。 • 選択肢：「None（なし）」「Shutdown（シャットダウン）」「Drop（破棄）」
Tunneled Protocol	トンネルされるプロトコルを選択します。 • 選択肢：「GVRP」「STP」「Protocol MAC」「All」
Protocol MAC	トンネルプロトコルに「Protocol MAC」を選択した場合、プロトコル MAC オプションを指定します。 • 選択肢：「01-00-0C-CC-CC-CC 」「01-00-0C-CC-CC-CD」
Threshold	ポートタイプで「Shutdown」「Drop」を指定した場合、しきい値を入力します。 • 設定可能範囲：1-4096

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、指定エントリのカウンタ情報をクリアします。
「Clear All」ボタンをクリックして、すべてのカウンタ情報をクリアします。

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

IGMP（Internet Group Management Protocol）Snooping 機能を始めとした L2 Multicast Control（L2 マルチキャストコントロール）の設定を行います。

IGMP Snooping（IGMP Snooping の設定）

IGMP（Internet Group Management Protocol）Snooping 機能を利用すると、スイッチはネットワークステーションまたはデバイスと IGMP ホスト間で送信される IGMP クエリと IGMP レポートを認識するようになります。IGMP スヌーピングが有効な場合、スイッチを通過する IGMP メッセージの情報に基づいて、特定のマルチキャストグループメンバに対してポートをオープン / クローズできるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストが存在しなくなった場合、マルチキャストパケットの送信を停止します。
適切にマルチキャストパケットを転送することにより、無駄なトラフィックの発生を抑えることができます。

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、まず本機能をスイッチ全体で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 で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。

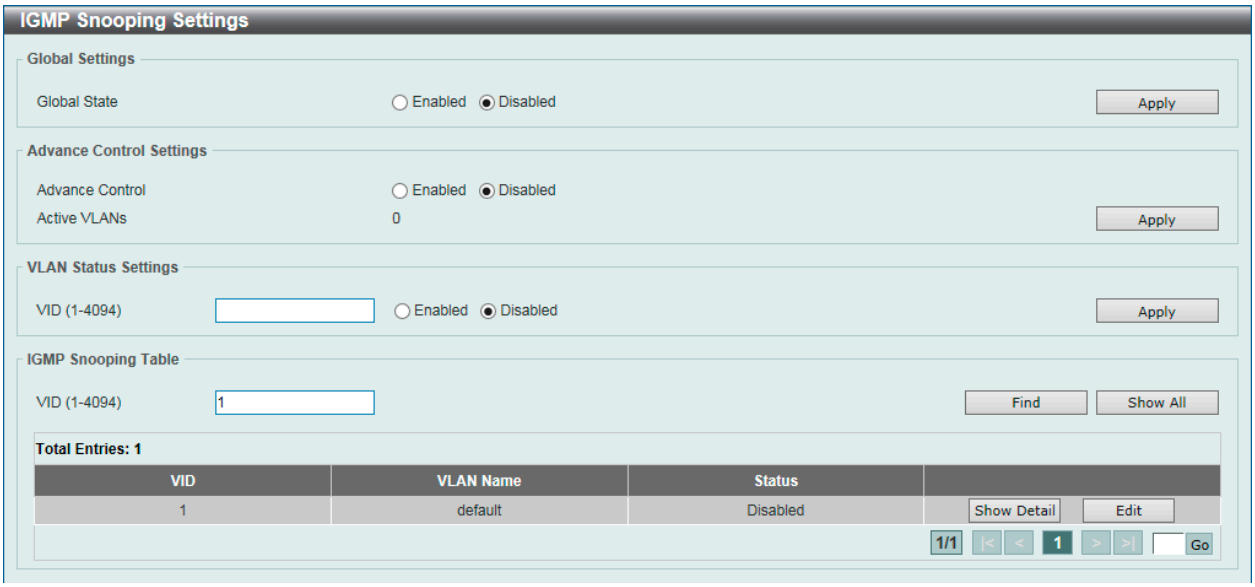


図 8-63　IGMP Snooping Settings 画面

画面に表示される項目：

項目	説明
Global Setting	
Global State	IGMP スヌーピングのグローバルステータスを有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
Advance Control Settings	
Advance Control	IGMP スヌーピングのアドバンスコントロール機能を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
VLAN Status Settings	
VID	VLAN を識別する VLAN ID を入力し、指定 VLAN 上の IGMP スヌーピングを有効 / 無効に設定します。 • 設定可能範囲：1-4094
IGMP Snooping Table	
VID	IGMP スヌーピングテーブルに表示する VLAN の 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て、設定内容を適用します。
「Find」ボタンをクリックして、指定した VLAN ID のエントリを表示します。
「Show All」ボタンをクリックして、IGMP スヌーピングテーブル上のすべてのエントリを表示します。

注意　IGMP/MLD スヌーピング機能において、マルチキャストエントリは Leave/Done + SQ の組み合わせにより削除されます。

■ 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 8-64　IGMP Snooping Settings（Show Detail）- IGMP Snooping VLAN Parameters 画面

本画面の「Modify」ボタンをクリックすると「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」画面で 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。

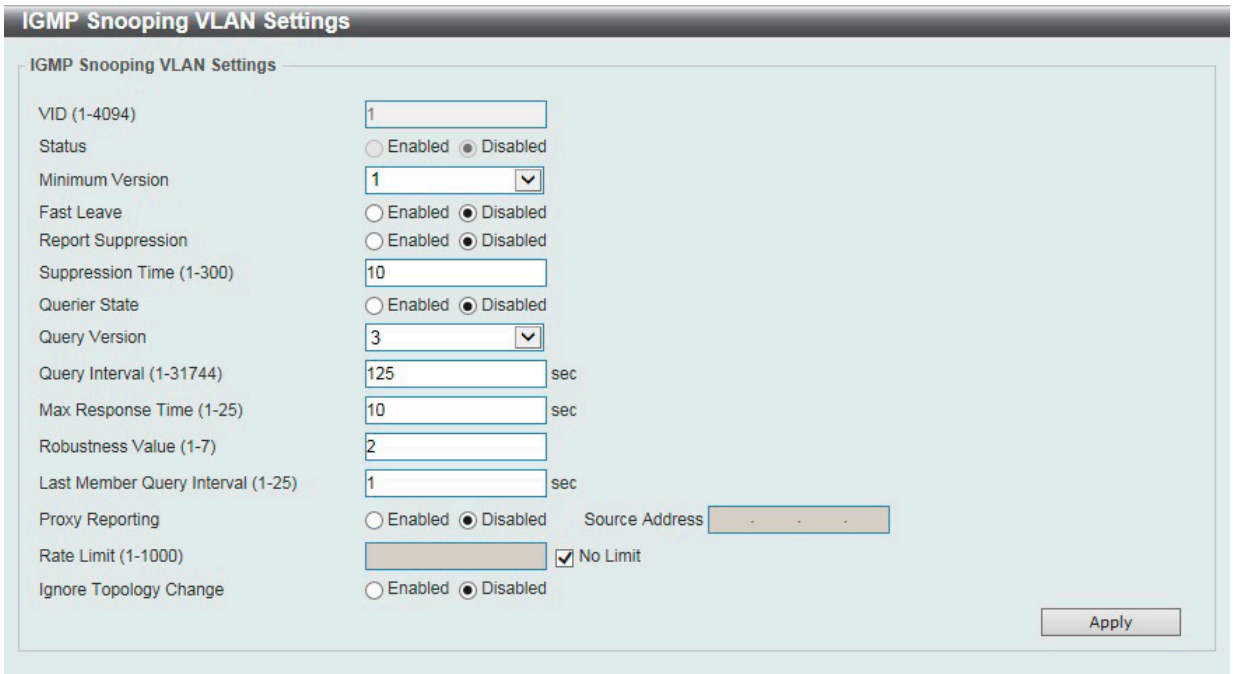


図 8-65 IGMP Snooping Settings（Edit）- IGMP Snooping VLAN Settings 画面

画面に表示される項目：

項目	説明
VID	IGMP Snooping 設定を変更する VLAN を識別する VLAN ID が表示されます。
Status	VLAN の IGMP Snooping 機能の有効 / 無効ステータスが表示されます。
Minimum Version	VLAN に対して許可される IGMP ホストの最小バージョンを選択します。 • 選択肢：「1」「2」「3」
Fast Leave	Fast Leave 機能を有効 / 無効に設定します。 本機能が有効な場合、システムが IGMP Leave メッセージを受信すると、本スイッチは Group-Specific クエリを生成せずに、メンバシップがすぐに削除されます。

項目	説明
Report Suppression	特定の VLAN への IGMP スヌーピングレポートの抑制を有効 / 無効に設定します。 レポートサスペンション機能は「IGMPv1」「IGMPv2」トラフィックでのみ機能します。 本機能が有効になると、ホストによるレポートの重複した送信が抑制されます。同じグループの Report/Leave メッセージの抑制は抑制時間（Suppression Time）を経過するまで継続されます。 同じグループの Report/Leave メッセージは、1 つのメッセージのみが送信され、残りのメッセージは抑制されます。
Suppression Time	重複する Report/Leave メッセージの抑制時間を設定します。 • 設定可能範囲：1-300（秒）
Querier State	クエリア機能を有効 / 無効に設定します。
Query Version	IGMP スヌーピングクエリアで送信される General 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 スヌーピングクエリアが General クエリを送信する間隔を指定します。 • 設定可能範囲：1-31744（秒）
Max Response Time	IGMP 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。 • 設定可能範囲：1-25（秒）
Robustness Value	パケットロスに対するロバストネス変数を指定します。 • 設定可能範囲：1-7
Last Member Query Interval	IGMP スヌーピングクエリアが IGMP Group-Specific クエリまたは Group-Source-Specific (Channel) クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1-25（秒）
Proxy Reporting	プロキシレポーティング機能を有効 / 無効に設定します。
Source Address	プロキシレポートを有効にした場合、プロキシレポーティングの送信元 IP アドレスを指定します。
Rate Limit	レートリミットを指定します。「No Limit」を指定すると、プロファイルにレート制限が適用されません。 • 設定可能範囲：1-1000
Ignore Topology Change	「Ignore Topology Change」機能を有効 / 無効にします。有効にするとトポロジの変更は無視されます。

「Apply」ボタンをクリックして、設定内容を適用します。

注意 IGMP Snooping について、Fast Leave は IGMPv2 のみサポートします。

IGMP Snooping AAA Settings（IGMP Snooping AAA 設定）

IGMP スヌーピング AAA 設定を指定、表示します。

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

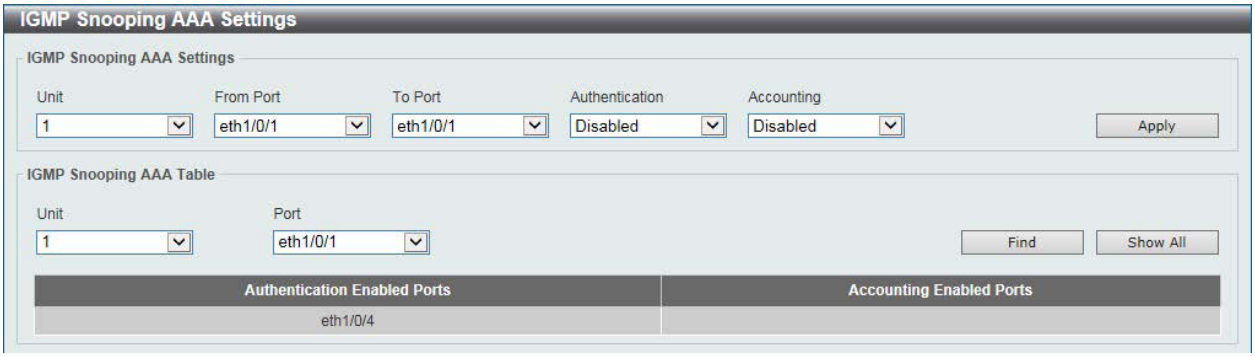


図 8-66　IGMP Snooping AAA Settings 画面

画面に表示される項目：

項目	説明
IGMP Snooping AAA Settings	
Unit	設定するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Authentication	IGMP join メッセージの認証機能を有効 / 無効に設定します。
Accounting	リスナーが IGMP グループに参加する際のアカウンティングを有効 / 無効に設定します。
IGMP Snooping AAA Table	
Unit	表示するユニットを指定します。
Port	表示するポートを指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」をクリックして、指定のエントリを表示します。
「Show All」をクリックして、IGMP スヌーピングテーブル上のすべてのエントリを表示します。

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

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

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

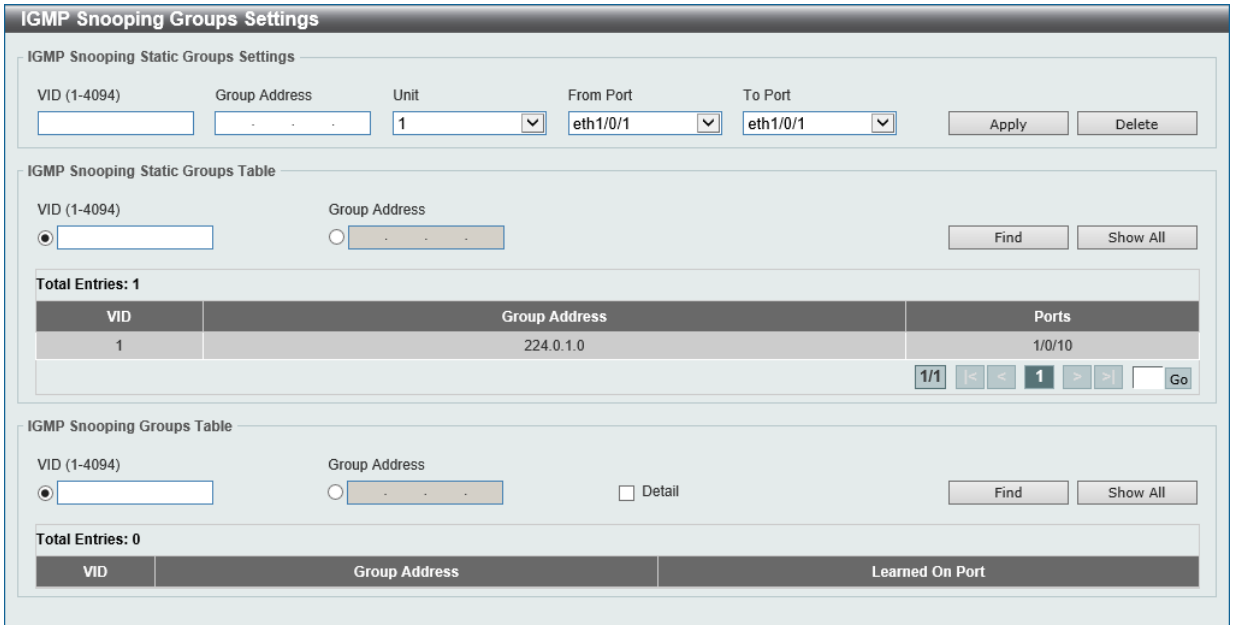


図 8-67　IGMP Snooping Groups Settings 画面

以下の項目を使用して、設定します。

IGMP Snooping Static Groups Settings/Table（IGMP スヌーピングスタティックグループ設定 / テーブル）

項目	説明
IGMP Snooping Static Groups Settings	
VID	登録または削除するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	登録または削除するマルチキャストグループの IP アドレスを入力します。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
IGMP Snooping Static Groups Table	
VID	ラジオボタンを選択し、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	ラジオボタンを選択し、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て、設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて特定の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。
「Show 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	ラジオボタンを選択し、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	ラジオボタンを選択し、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。
Detail	IGMP グループの詳細情報を表示します。

「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。
「Show All」ボタンをクリックして、すべての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 Filter Settings（IGMP Snooping フィルタ 設定）

IGMP Snooping フィルタの設定を行います。

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

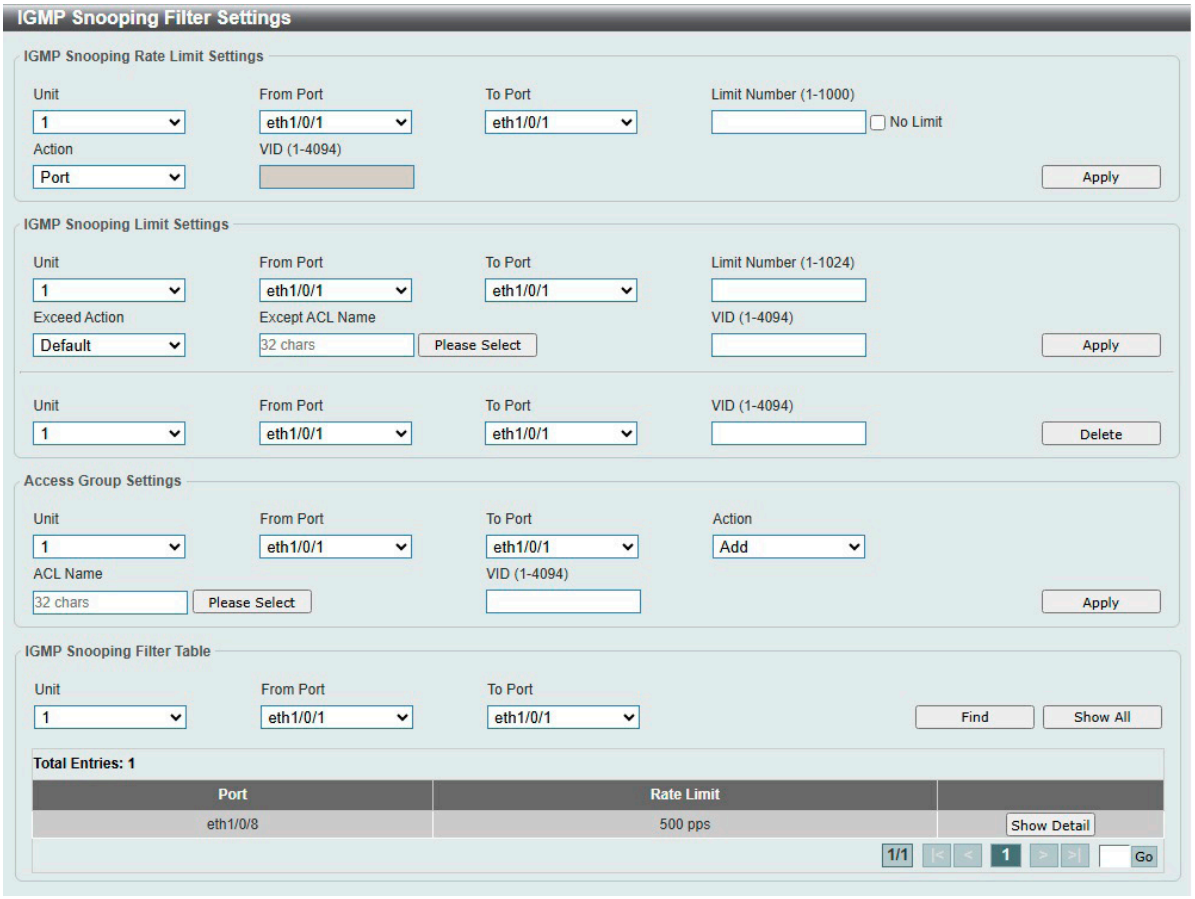


図 8-68　IGMP Snooping Filter Settings 画面

以下の項目を使用して、設定します。

IGMP Snooping Rate Limit Settings（IGMP スヌーピングレートリミット設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Limit Number	スイッチが指定のインタフェースで処理可能な IGMP コントロールパケットのレートを指定します。「No Limit」を指定すると、制限を行いません。 • 設定可能範囲：1-1000（パケット / 秒）
Action	対象のインタフェースのタイプを指定します。 • 選択肢：「Port」「VLAN」
VID	「Action」で「VLAN」を選択した場合、VLAN を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。

IGMP Snooping Limit Settings（IGMP スヌーピングリミット設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Limit Number	生成される IGMP キャッシュエントリ数の上限値を指定します。 • 設定可能範囲：1-1024
Exceed Action	しきい値を超過した場合の動作について指定します。制限を超えた場合、新しく学習したグループに対して以下の処理を実行します。 • 「Default」- デフォルトのアクションを実行します。 • 「Drop」- 新規グループは破棄されます。 • 「Replace」- 古いグループは新規グループにより置き換わります。

項目	説明
Except ACL Name	標準 IP アクセスリストを指定します（32 文字以内）。 アクセスリストに許可されたグループ (*,G) は制限から外れます。グループ (*,G) を許可するにはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「Please Select」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	フィルタを適用する 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て、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

Access Group Settings（アクセスグループ設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Action	• 「Add」- 入力した情報に基づき新しいエントリを追加します。 • 「Delete」- 入力した情報に基づき既存エントリを削除します。
ACL Name	標準 IP アクセスリストを指定します（32 文字以内）。 グループ (*,G) への参加をユーザに許可する場合に使用します。アクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「Please Select」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	設定する VLAN を指定します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。

IGMP Snooping Filter Table（IGMP スヌーピングフィルタテーブル）

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

「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
「Show 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。
「Show Detail」ボタンをクリックして、エントリの詳細情報を表示します。

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。

「Please Select」をクリックすると次の画面が表示されます。

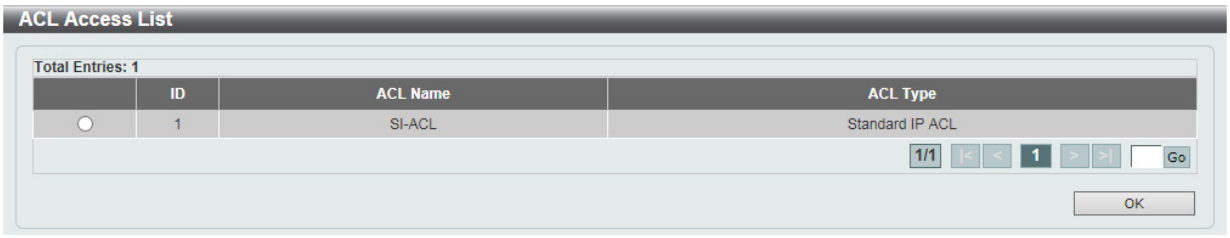


図 8-69　ACL Access List 画面

ACL を選択し「OK」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。

「**Show Detail**」をクリックすると次の画面が表示されます。

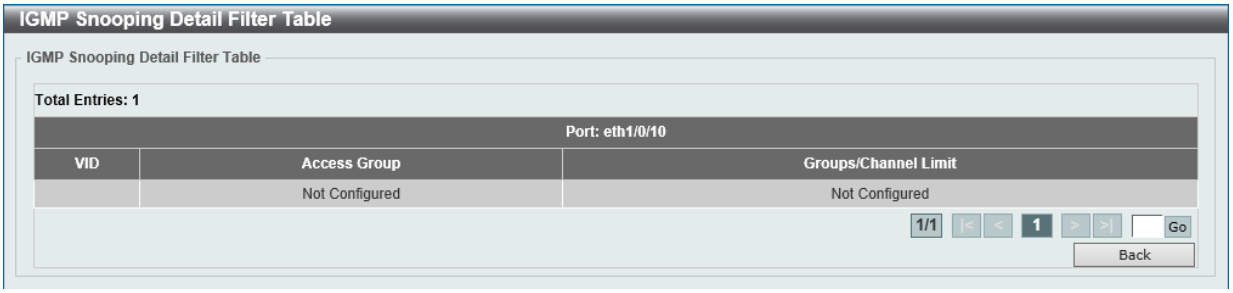


図 8-70　IGMP Snooping Filter Settings（Show Detail）- IGMP Snooping Detail Filter table 画面

前の画面に戻るには、「Back」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。

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

IGMP スヌーピングマルチキャストルータの設定を行います。

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

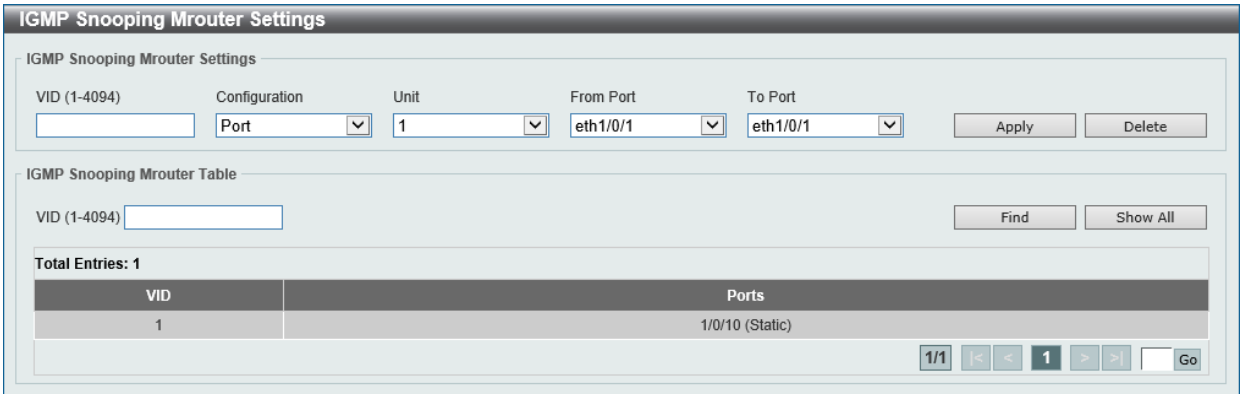


図 8-71　IGMP Snooping Mrouter Settings 画面

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
IGMP Snooping Mrouter Settings	
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」- ポートをマルチキャストルータポートに指定します。 •「Forbidden Router Port」- ポートを非マルチキャストポートに指定します。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。

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

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
IGMP Snooping Mrouter Table	
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。
「Show 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）

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。

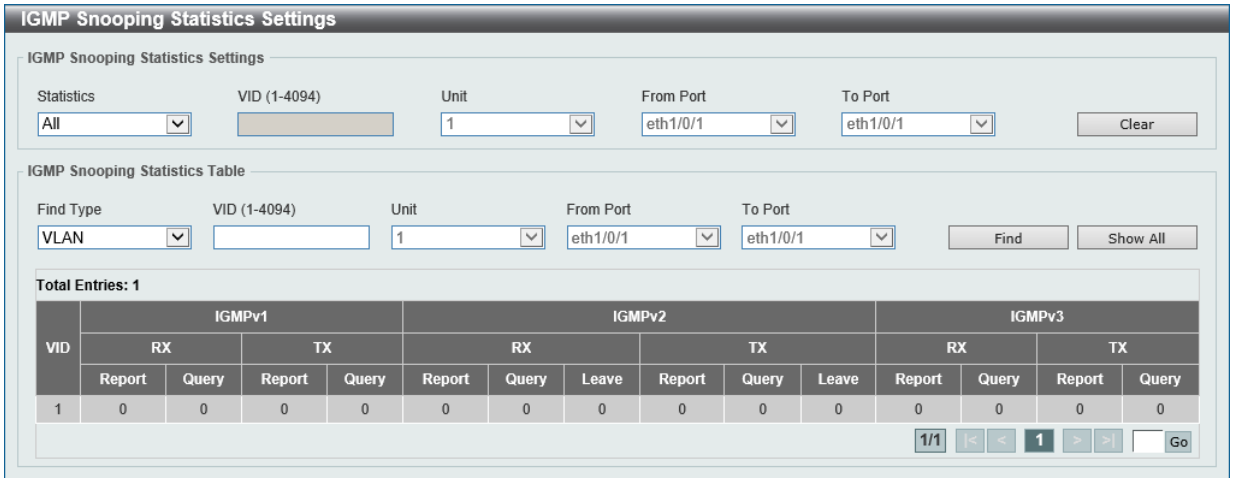


図 8-72　IGMP Snooping Statistics Settings 画面

以下の項目が表示されます。

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

項目	説明
Statistics	インタフェースを選択します。 • 選択肢：「All」「VLAN」「Port」
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
Unit	統計情報をクリアするユニットを選択します。「Statistics」で「Port」を選択すると指定可能になります。
From Port / To Port	統計情報をクリアするポートの範囲を設定します。「Statistics」で「Port」を選択すると指定可能になります。

「Clear」ボタンをクリックして、IGMP スヌーピング関連の統計情報をクリアします。

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

項目	説明
Find Type	インタフェースを選択します。 • 選択肢：「VLAN」「Port」
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
Unit	表示するユニットを選択します。「Find Type」で「Port」を選択すると設定可能になります。
From Port / To Port	表示するポートの範囲を設定します。「Find Type」で「Port」を選択すると設定可能になります。

「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。
「Show All」ボタンをクリックして、すべての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。

MLD Snooping（MLD スヌーピング）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じ機能を持つ、IPv6 用のマルチキャストトラフィック制御機能です。VLAN 上でマルチキャストデータを要求するポートを検出するために使用されます。MLD Snooping では、所定の VLAN 上のすべてのポートにマルチキャストトラフィックを流すのではなく、要求元ポートとマルチキャストの送信元によって生成される MLD クエリと MLD レポートを使用して、データを受信したいポートに対してのみ、マルチキャストデータを転送します。
MLD Snooping は、エンドノードと MLD ルータとの間で交換される MLD 制御パケットのレイヤ 3 部分を調べることでパケットを処理します。スイッチは、ルートがマルチキャストトラフィックをリクエストしていることを検出すると、そのルートに直接接続されているポートを IPv6 マルチキャストテーブルに追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のエントリには、該当ポートや VLAN ID、関連する IPv6 マルチキャストグループアドレスが記録され、このポートはアクティブな Listening ポートと見なされます。アクティブな Listening ポートのみがマルチキャストグループデータを受信します。

MLD コントロールメッセージ

MLD Snooping を使用するデバイス間で以下の MLD コントロールメッセージが交換されます。これらのメッセージは、130、131、132 および 143 でラベル付けされた 4 つの ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query – IPv4 の IGMPv2 Host Membership Query（HMQ）に相当するメッセージです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query はリンク上のすべての Listening ポートに対し送信され、Multicast Specific Query は、特定のマルチキャストアドレスに対して送信されます。この 2 種類のメッセージは、IPv6 ヘッダ内のマルチキャスト宛先アドレス及び Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別されます。
2. Multicast Listener Report – IGMPv2 の Host Membership Report（HMR）に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。
3. Multicast Listener Done – IGMPv2 の Leave Group Message に相当するメッセージです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからのマルチキャストデータの受信を停止すること、つまり、このアドレスからのマルチキャストデータが "done"（完了）となった旨を伝えます。スイッチが本メッセージを受信すると、この Listening ホストには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しなくなります。
4. Multicast Listener Report Version2 – IGMPv3 の Host Membership Report（HMR）に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

MLD Snooping Settings（MLD スヌーピング設定）

MLD Snooping 設定を有効または無効にします。

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

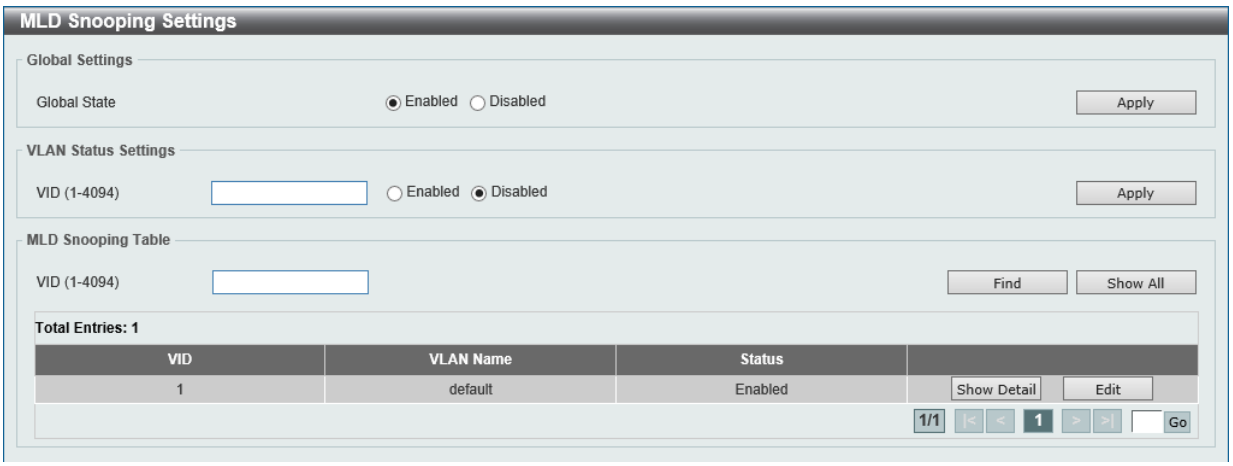


図 8-73　MLD Snooping Settings 画面

画面に表示される項目：

項目	説明
Global Setting	
Global State	MLD Snooping のグローバルステータスを有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
VLAN Status Settings	
VID	VLAN を識別する VLAN ID を入力し、指定 VLAN 上の MLD Snooping を有効 / 無効に設定します。 • 設定可能範囲：1-4094

項目	説明
MLD Snooping Table	
VID	MLD Snooping テーブルで表示する VLAN の 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て、設定内容を適用します。
「Find」ボタンをクリックして、指定した VLAN ID のエントリを表示します。
「Show All」ボタンをクリックして、MLD Snooping Table 上のすべてのエントリを表示します。

注意　IGMP/MLD スヌーピング機能において、マルチキャストエントリは Leave/Done + SQ の組み合わせにより削除されます。

MLD 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。

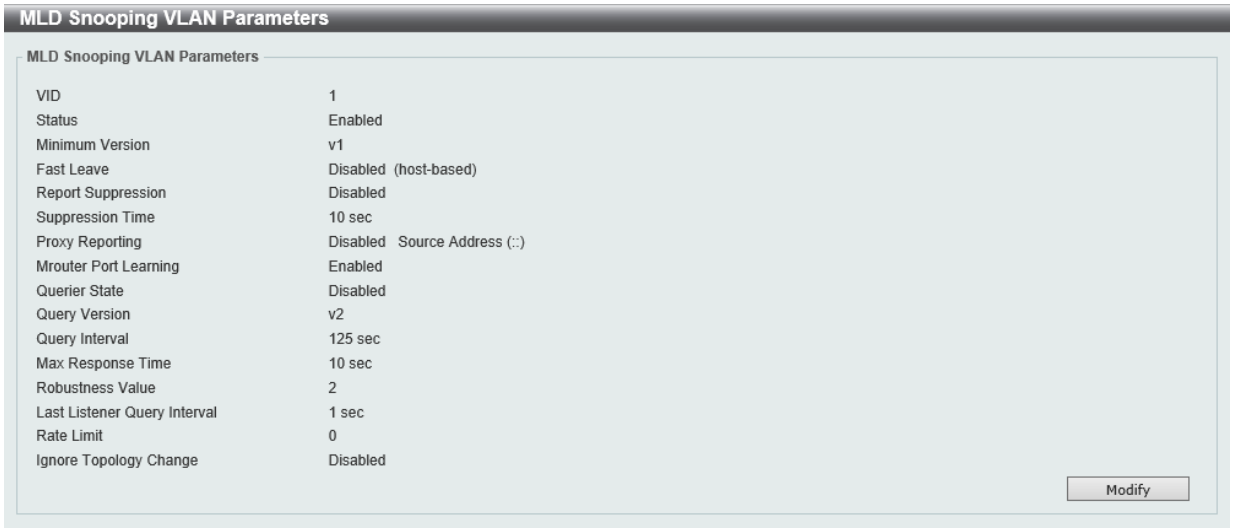


図 8-74　MLD Snooping VLAN Parameters 画面

本画面の「Modify」ボタンをクリックすると「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。

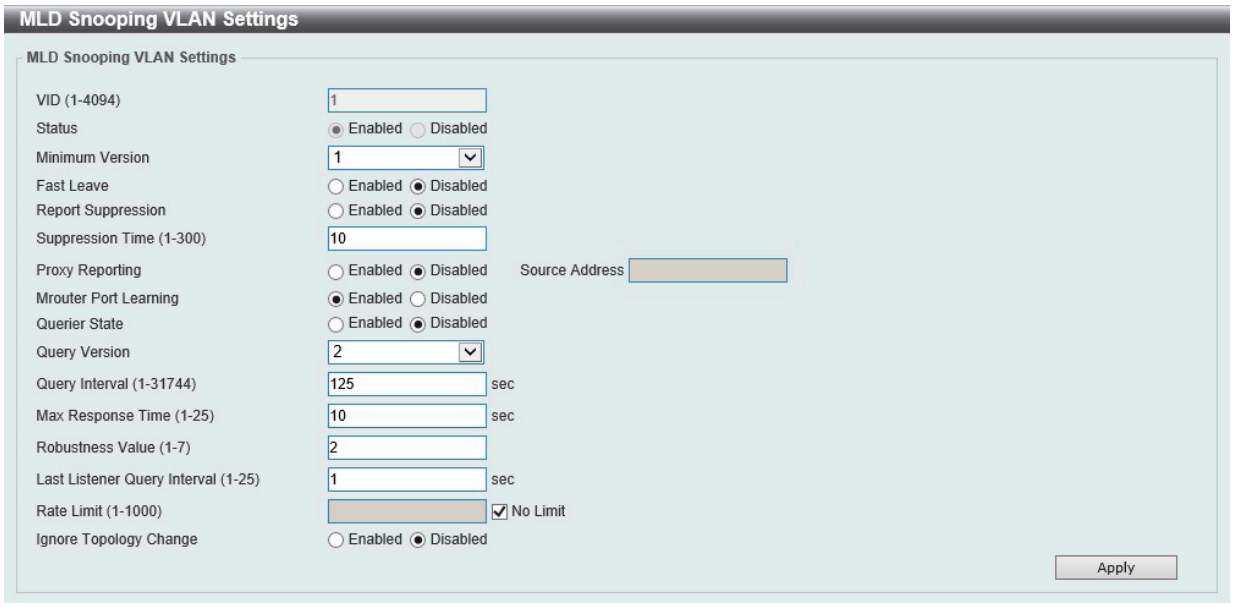


図 8-75 MLD Snooping Settings（Edit）- MLD Snooping VLAN Settings 画面

画面に表示される項目：

項目	説明
VID	MLD Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
Status	VLAN の MLD Snooping 機能を有効 / 無効ステータスを表示します。

項目	説明
Minimum Version	VLAN に許可された MLD ホストの最小バージョンを選択します。 • 選択肢：「1」「2」
Fast Leave	Fast Leave 機能の有効 / 無効を設定します。本機能が有効の場合、スイッチが MLD Done メッセージを受信すると、マルチキャストグループのメンバシップは削除されます。
Report Suppression	MLD スヌーピングレポートの抑制を有効 / 無効に設定します。
Suppression Time	重複するスヌーピングレポートの抑制時間を設定します。 • 設定可能範囲：1-300（秒）
Proxy Reporting	プロキシレポーティング機能を有効 / 無効に設定します。
Source Address	プロキシレポートが有効な場合、プロキシレポーティングの送信元 IP アドレスを指定します。
Mrouter Port Learning	Mrouter ポート学習機能を有効 / 無効に設定します。
Querier State	MLD クエリア機能を有効 / 無効に設定します。
Query Version	MLD スヌーピングクエリアによって送信される General 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 スヌーピングクエリアが MLD General クエリメッセージを送信する間隔を入力します。 • 設定可能範囲：1-31744（秒）
Max Response Time	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。 • 設定可能範囲：1-25（秒）
Robustness Value	パケットロスに対するロバストネス変数を指定します。 • 設定可能範囲：1-7
Last Listener Query Interval	MLD スヌーピングクエリアが MLD Group-Specific クエリまたは Group-Source-Specific (Channel) クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1-25
Rate Limit	レートリミットを指定します。「No Limit」を指定すると本プロファイルでは制限がなしになります。 • 設定可能範囲：1-1000
Ignore Topology Change	「Ignore Topology Change」を有効 / 無効に設定します。有効にするとトポロジの変更は無視されます。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　MLD Snooping について、Fast Leave は MLDv1 のみサポートします。

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

MLD スヌーピングスタティックグループの表示と設定、および MLD スヌーピンググループの表示を行います。

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

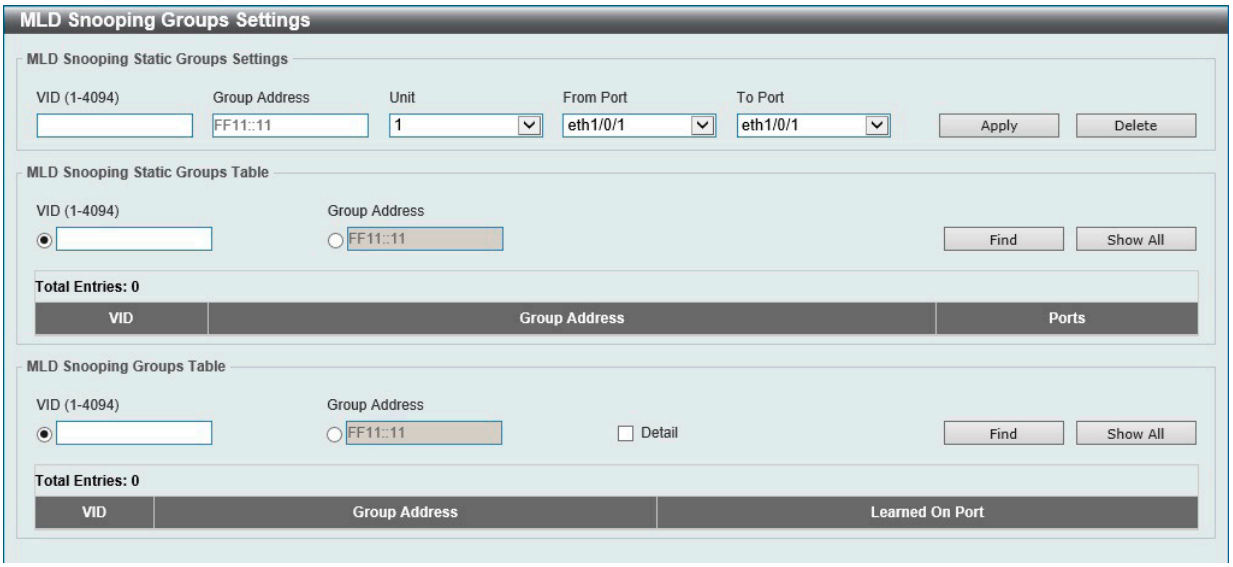


図 8-76　MLD Snooping Groups Settings 画面

以下の項目を使用して、設定します。

■ MLD Snooping Static Groups Settings/Table（MLD スヌーピングスタティックグループ設定 / テーブル）

項目	説明
MLD Snooping Static Groups Settings	
VID	登録または削除する IPv6 マルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
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 アドレスを入力します。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
MLD Snooping Static Groups Table	
VID	ラジオボタンを選択し、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	ラジオボタンを選択し、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て、設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「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。
「Show 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
MLD Snooping Groups Table	
VID	ラジオボタンを選択し、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	ラジオボタンを選択し、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。
Detail	MLD グループの詳細について表示します。

「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。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

MLD Snooping Filter Settings（MLD Snooping フィルタ設定）

MLD Snooping フィルタの設定を行います。

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

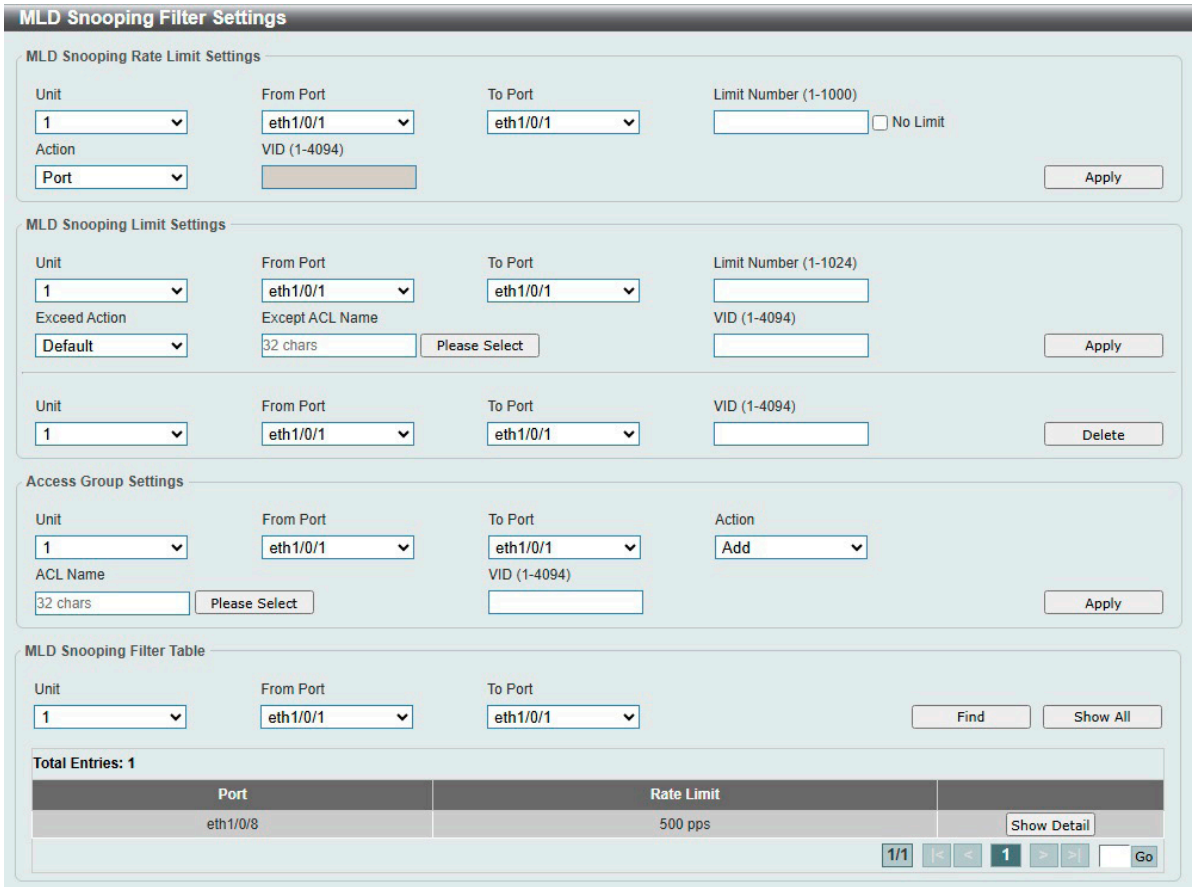


図 8-77　MLD Snooping Filter Settings 画面

以下の項目を使用して、設定します。

■ MLD Snooping Rate Limit Settings（MLD スヌーピングレートリミット設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
Limit Number	スイッチが指定のインタフェースで処理可能な MLD コントロールパケットのレートを指定します。「No Limit」にチェックを入れると制限を設定しません。 • 設定可能範囲：1-1000（パケット / 秒）
Action	対象のインタフェースのタイプを指定します。 • 選択肢：「Port」「VLAN」
VID	「Action」で「VLAN」を選択した場合、VLAN ID を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。

■ MLD Snooping Limit Settings（MLD スヌーピングリミット設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
Limit Number	生成される MLD キャッシュエントリ数の上限値を指定します。 • 設定可能範囲：1-1024
Exceed Action	制限を超えた場合、新しく学習したグループに対して以下の処理を実行します。 •「Default」- デフォルトのアクションを実行します。 •「Drop」- 新規グループは破棄されます。 •「Replace」- 古いグループは新規グループにより置き換わります。
Except ACL Name	標準 IP アクセスリストを指定します（32 文字以内）。 アクセスリストに許可されたグループ (*,G) は制限から除外されます。グループ (*,G) を許可するにはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「Please Select」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	フィルタを適用する 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て、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

■ Access Group Settings（アクセスグループ設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
Action	•「Add」- 入力した情報に基づき新しいエントリを追加します。 •「Delete」- 入力した情報に基づき既存エントリを削除します。
ACL Name	標準 IP アクセスリストを指定します（32 文字以内）。 グループ (*,G) への参加をユーザに許可する場合に使用します。アクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「Please Select」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	設定する VLAN を指定します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。

■ MLD Snooping Filter Table（MLD スヌーピングフィルタテーブル）

項目	説明
Unit	表示するユニットを選択します。
From Port / To Port	表示するポートの範囲を設定します。

「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
「Show 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。
「Show Detail」ボタンをクリックして、エントリの詳細情報を表示します。

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。

「Please Select」をクリックすると次の画面が表示されます。

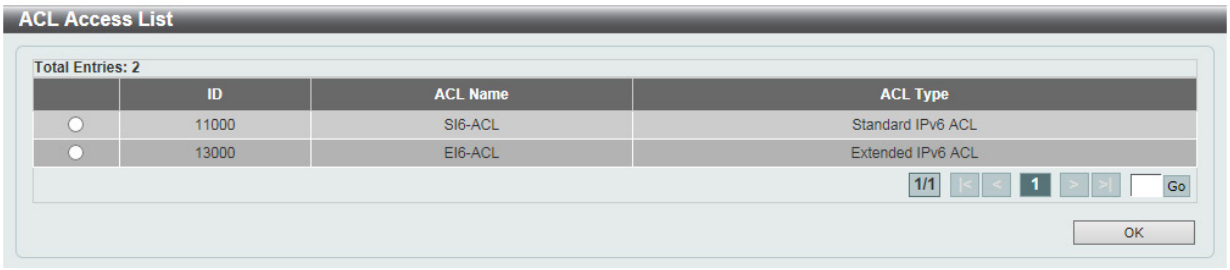


図 8-78　ACL Access List 画面

ACL を選択し「OK」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。

「Show Detail」をクリックすると次の画面が表示されます。

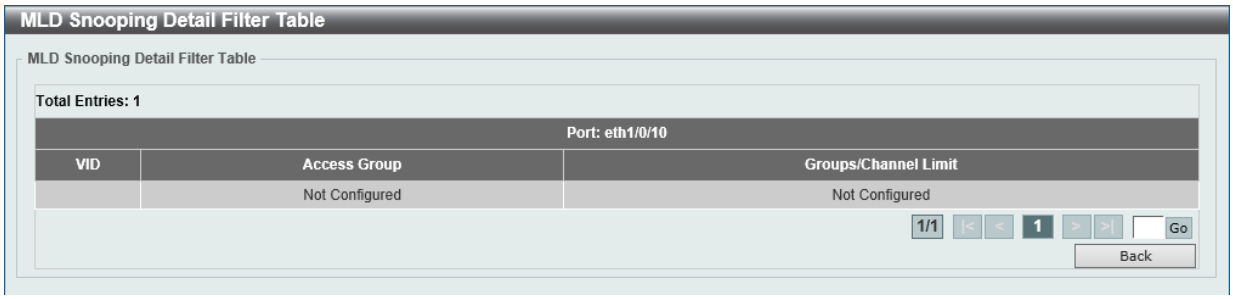


図 8-79　MLD Snooping Filter Settings（Show Detail）- MLD Snooping Detail Filter Table 画面

前の画面に戻るには、「Back」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。

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

VLAN インタフェースで、マルチキャストルータポートを指定します。

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

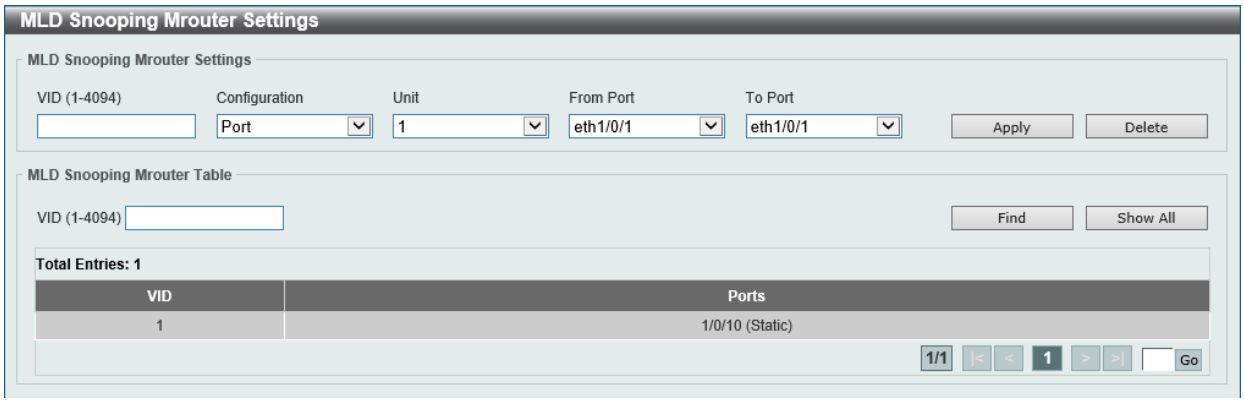


図 8-80　MLD Snooping Mrouter Settings 画面

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
MLD Snooping Mrouter Settings	
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」- 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。 •「Learn pimv6」- マルチキャストルータポートの自動学習を有効にします。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。

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

MLD Snooping 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
MLD Snooping Mrouter Table	
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。
「Show 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。

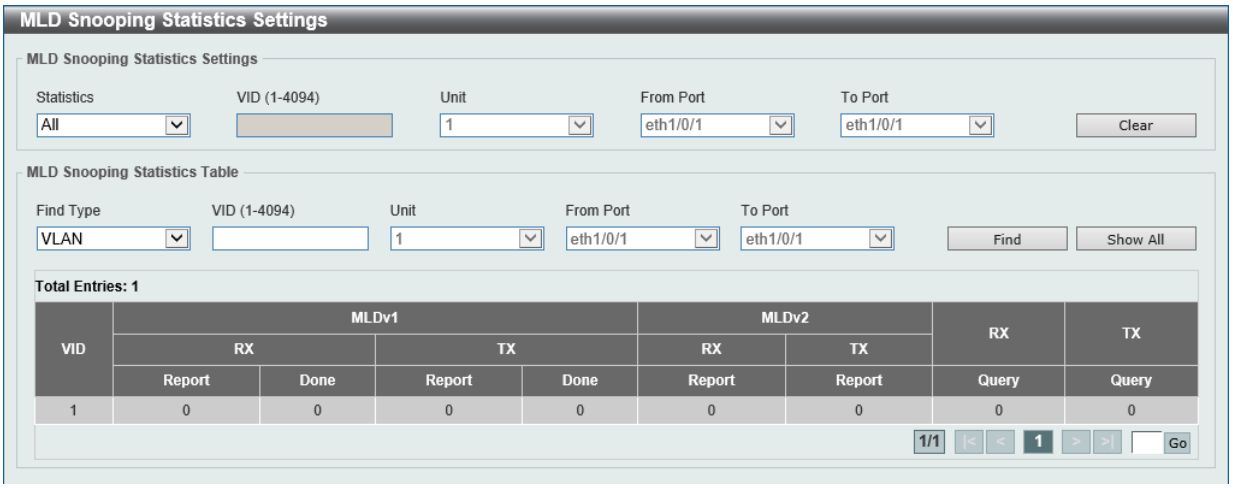


図 8-81　MLD Snooping Statistics Settings 画面

以下の項目が表示されます。

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

項目	説明
Statistics	インタフェースの種類を選択します。 • 選択肢：「All」「VLAN」「Port」
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
Unit	統計情報をクリアするユニットを選択します。「Statistics」で「Port」を選択すると指定可能になります。
From Port / To Port	統計情報をクリアするポートの範囲を設定します。「Statistics」で「Port」を選択すると指定可能になります。

「Clear」ボタンをクリックして、MLD スヌーピング関連の統計情報をクリアします。

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

項目	説明
Find Type	インタフェースの種類を選択します。 • 選択肢：「VLAN」「Port」
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
Unit	表示するユニットを選択します。「Find Type」で「Port」を選択すると指定可能になります。
From Port / To Port	表示するポートの範囲を設定します。「Find Type」で「Port」を選択すると指定可能になります。

「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。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

Multicast VLAN（マルチキャスト VLAN）

L2 Features > L2 Multicast Control > Multicast VLAN

Multicast VLAN Settings（マルチキャスト VLAN 設定）

マルチキャスト VLAN の設定を行います。

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

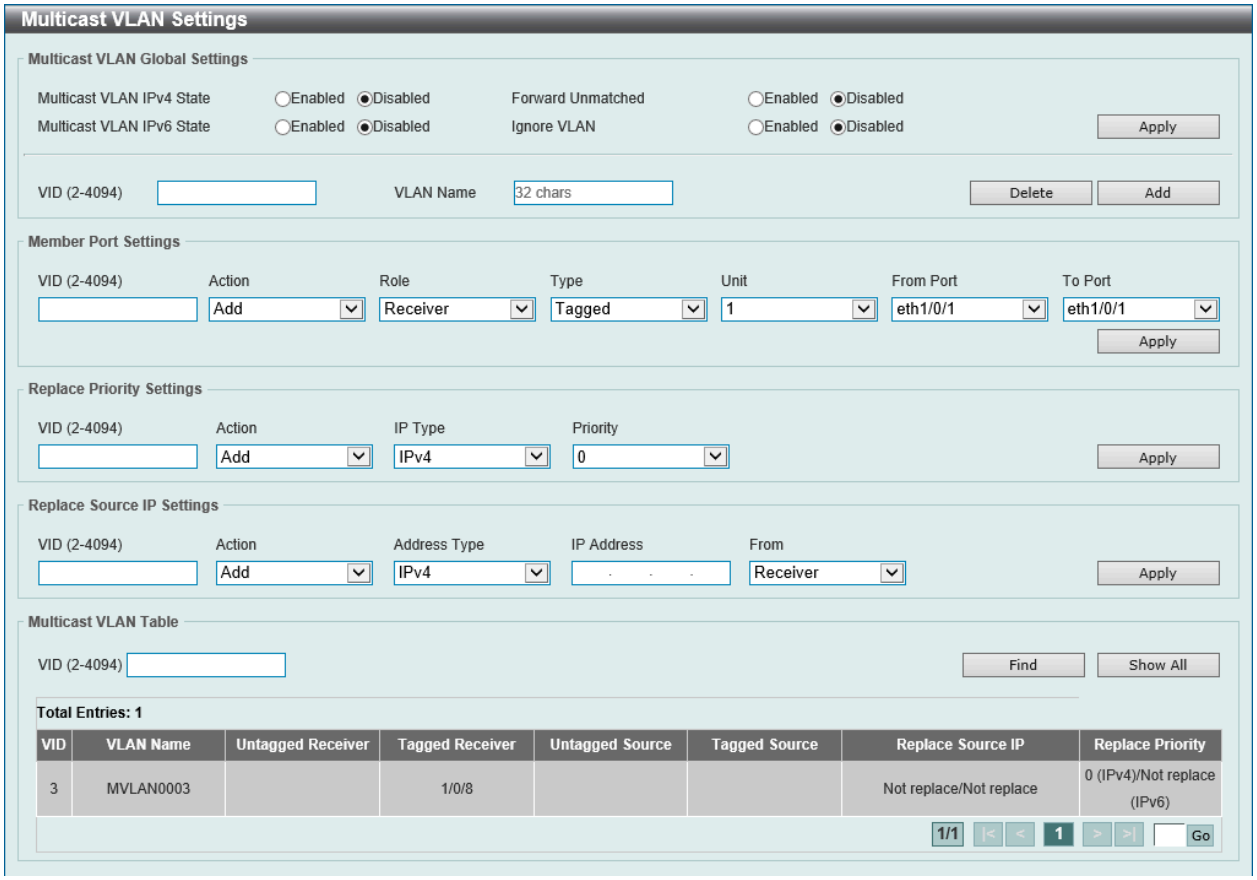


図 8-82　Multicast VLAN Settings 画面

画面に表示される項目：

項目	説明
Multicast VLAN Global Settings	
Multicast VLAN IPv4 State	マルチキャスト VLAN における IPv4 IGMP コントロールパケット処理を有効 / 無効に設定します。
Forward Unmatched	「Forward Unmatched」を有効 / 無効に設定します。 以下のいずれかの場合に、本設定に応じて転送または破棄されます。 - 受信 IGMP/MLD コントロールパケットがアンタグパケットであり、プロファイルに一致しない、かつ関連するデフォルト VLAN がマルチキャスト VLAN の場合 - 受信 IGMP/MLD コントロールパケットがマルチキャスト VLAN のタグ付きパケットであり、プロファイルに一致しない場合 • 初期値（Disabled）：ではパケットは破棄されます。
Multicast VLAN IPv6 State	マルチキャスト VLAN における IPv6 MLD コントロールパケット処理を有効 / 無効に設定します。
Ignore VLAN	タグ付き IGMP/MLD コントロールパケットに対する「Ignore VLAN」を有効/無効に設定します。本設定を有効にすると、受信 IGMP/MLD コントロールパケットの VLAN は無視され、プロファイルの照合を行います。
VID	作成 / 削除するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
VLAN Name	作成 / 削除するマルチキャスト VLAN の VLAN 名を指定します。
Member Port Settings	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
Action	実行するアクションを指定します。 • 「Add」- 入力した情報に基づきエントリを追加します。 • 「Delete」- 入力した情報に基づきエントリを削除します。

項目	説明
Role	メンバポートの役割を指定します。 • 「Receiver」- マルチキャスト VLAN のマルチキャストデータ受信のみを行うサブスクライバポートとして設定します。 • 「Source」- マルチキャスト VLAN のマルチキャストデータ送信を行うことができるアップリンクポートとして設定します。
Type	メンバポートの種類を指定します。 • 「Tagged」- ポートがタグ付きメンバに指定されると、当該ポートから送信されるパケットはマルチキャスト VLAN ID でタグ付けされます。 • 「Untagged」- ポートがタグなしメンバに指定されると、当該ポートから送信されるパケットはタグ無しフォームで転送されます。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Replace Priority Settings	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
Action	実行するアクションを指定します。 • 「Add」- 入力した情報に基づきエントリを追加します。 • 「Delete」- 入力した情報に基づきエントリを削除します。
IP Type	アドレスの種類を指定します。 • 「IPv4」- マルチキャスト VLAN で送信する IPv4 マルチキャストパケットにプライオリティを再マッピングします。 • 「IPv6」- マルチキャスト VLAN で送信する IPv6 マルチキャストパケットにプライオリティを再マッピングします。
Priority	優先値を指定します。 • 設定可能範囲：0-7
Replace Source IP Settings	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
Action	実行するアクションを指定します。 • 「Add」- 入力した情報に基づきエントリを追加します。 • 「Delete」- 入力した情報に基づきエントリを削除します。
Address Type	アドレスの種類を指定します。 • 「IPv4」- ルータに送信される IGMP コントロールパケットの送信元 IPv4 アドレスを指定します。 • 「IPv6」- ルータに送信される MLD コントロールパケットの送信元 IPv6 アドレスを指定します。
IP Address	IPv4/IPv6 アドレスを指定します。
From	送信元オプションを指定します。 • 「Receiver」- マルチキャスト VLAN Receiver ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。 • 「Source」- マルチキャスト VLAN Source ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。 • 「Both」- 全てのマルチキャスト VLAN ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。
Multicast VLAN Table	
VID	表示するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Add」をボタンクリックして、指定のエントリを作成します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「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。
「Show All」ボタンをクリックして、すべての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。

Multicast VLAN Group Settings（マルチキャスト VLAN グループ設定）

マルチキャスト VLAN グループの設定、表示を行います。

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

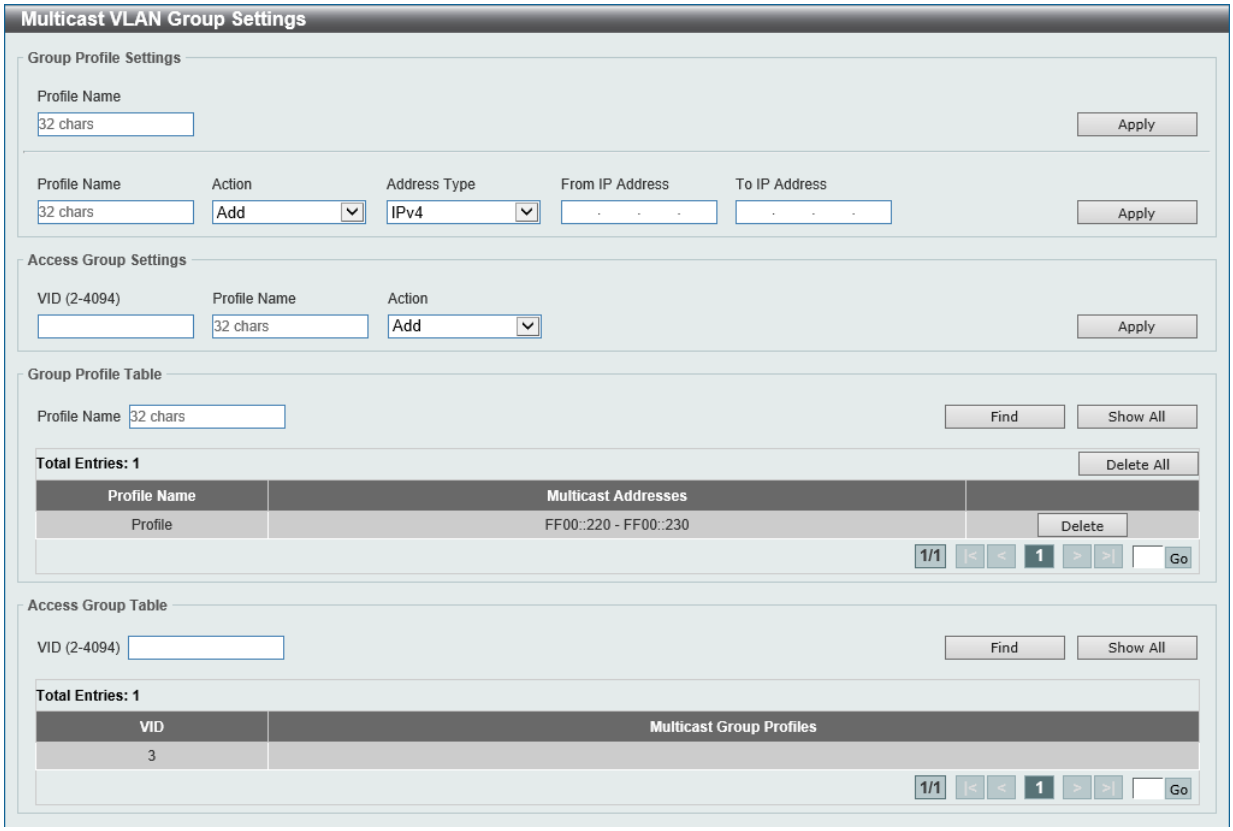


図 8-83　Multicast VLAN Group Settings 画面

画面に表示される項目：

項目	説明
Groups Profile Settings	
Profile Name	マルチキャスト VLAN のグループプロファイル名を指定します。（32 文字以内）
Action	実行する動作を指定します。マルチキャスト VLAN プロファイルには複数の範囲を追加することができます。同じプロファイルに対して指定される IP アドレス範囲は同じアドレスファミリである必要があります。 • 選択肢：「Add（追加）」「Delete（削除）」
Address Type	アドレスタイプを指定します。 • 「IPv4」- IPv4 マルチキャストアドレスを使用します。 • 「IPv6」- IPv6 マルチキャストアドレスを使用します。
From IP Address	IPv4/IPv6 アドレス範囲の開始アドレスを指定します。
To IP Address	IPv4/IPv6 アドレス範囲の終了アドレスを指定します。
Access Group Settings	
VID	VLAN ID を指定します。 • 設定可能範囲：2-4094
Profile Name	マルチキャスト VLAN のグループプロファイル名を指定します。（32 文字以内）
Action	実行する動作を指定します。 • 「Add」- マルチキャストグループを追加します。 • 「Delete」- マルチキャストグループを削除します。
Group Profile Table	
Profile Name	マルチキャスト VLAN のグループプロファイル名を指定します。（32 文字以内）
Access Group Table	
VID	VLAN ID を指定します。 • 設定可能範囲：2-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Delete All」ボタンをクリックすして、すべての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。

「Show 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。

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

L2 マルチキャストフィルタリング設定を行います。

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

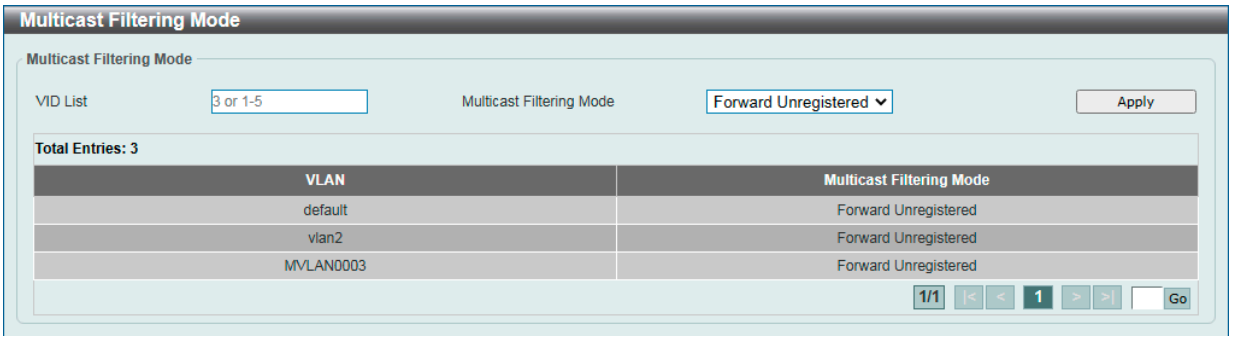


図 8-84　Multicast Filtering Mode 画面

画面に表示される項目：

項目	説明
VID List	設定する VLAN ID を入力します。
Multicast Filter Mode	マルチキャストフィルタモードを選択します。 • 「Forward Unregistered」- 登録されたマルチキャストパケットはフォワーディングテーブルに基づいて転送され、登録されていないマルチキャストパケットは VLAN ドメインにフラッドします。 • 「Filter Unregistered」- 登録されたマルチキャストパケットはフォワーディングテーブルに基づき転送され、登録されていないマルチキャストパケットはフィルタされます。

「Apply」ボタンをクリックして、設定内容を適用します。
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のページへ移動します。

LLDP

L2 Features > LLDP
LLDP（Link Layer Discovery Protocol）は、隣接する機器の情報を収集するためのプロトコルです。
IEEE 802 ネットワークに接続している他の機器に対し、自分の機器情報をアドバタイズします。

LLDP Global Settings（LLDP グローバル設定）

LLDP のグローバル設定を行います。

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

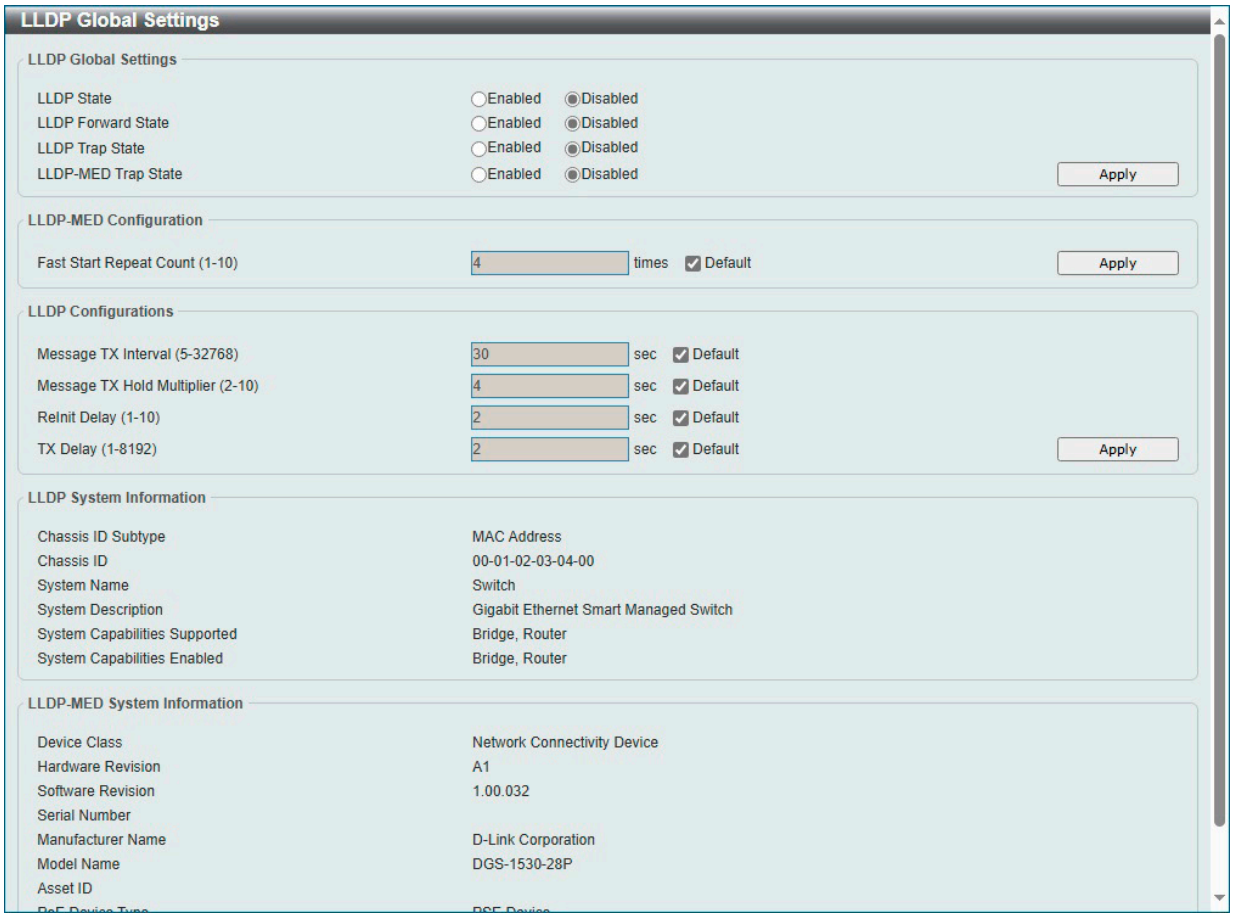


図 8-85　LLDP Global Settings 画面

画面に表示される項目：

項目	説明
LLDP Global Settings	
LLDP State	LLDP 機能を有効 / 無効に設定します。
LLDP Forward State	LLDP 転送ステータスを有効 / 無効に設定します。「LLDP Status」が 無効で「LLDP Forward Sate」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 トラップを有効 / 無効に設定します。
LLDP-MED Trap State	LLDP-MED トラップを有効 / 無効に設定します。
LLDP-MED Configuration	
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。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-10
LLDP Configurations	
Message TX Interval	物理インタフェースの LLDP アドバタイズメント送信間隔を設定します。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：5-32768（秒）
Message TX Hold Multiplier	LLDPDU の TTL 値を計算するために使用される、LLDPDU 転送間隔に対する乗数を指定します。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：2-10

項目	説明
Relnit Delay	LLDP ポートが再初期化を行うまでの待機時間を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-10（秒）
TX Delay	インタフェースで LLDPDU を送信するまでの待機時間を指定します。送信間隔の数値の 1/4 より大きくすることはできません。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-8192（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

LLDP Port Settings（LLDP ポート設定）

LLDP ポートの設定を行います。

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。

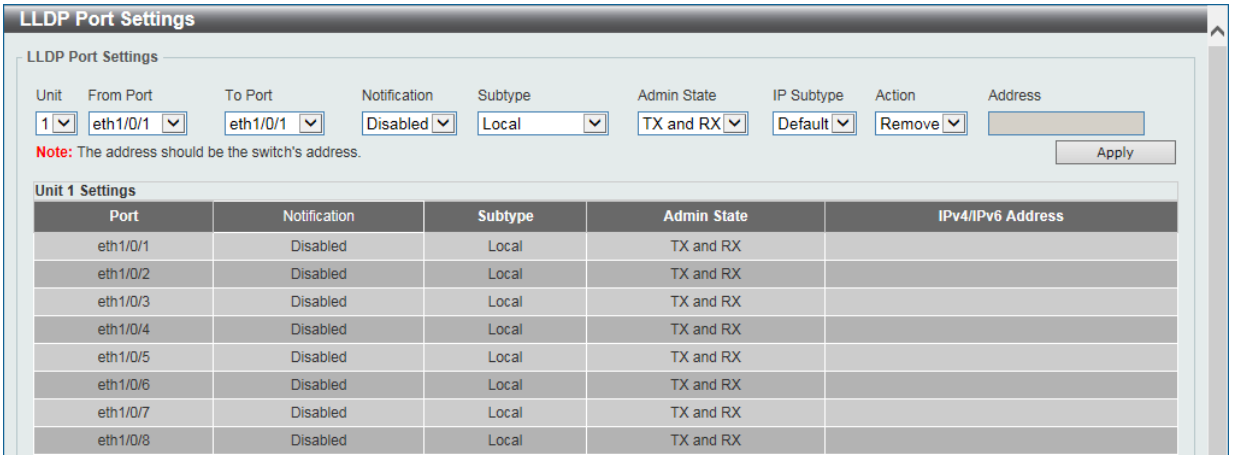


図 8-86　LLDP Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Notification	LLDP 通知を有効 / 無効に設定します。
Subtype	LLDP TLV のサブタイプを選択します。 • 選択肢：「MAC Address」「Local」
Admin State	LLDP フレームの送受信オプションを選択します。 • 「TX」- ローカル LLDP エージェントは LLDP フレーム送信のみを行います。 • 「RX」- ローカル LLDP エージェントは LLDP フレーム受信のみを行います。 • 「TX and RX」- ローカル LLDP エージェントは LLDP フレームの送受信を行います。（初期値） • 「Disabled」- ローカル LLDP エージェントは LLDP フレームの送受信を行いません。
IP Subtype	送信する IP アドレスの種類を選択します。 • 選択肢：「Default」「IPv4」「IPv6」
Action	実行する動作を選択します。 • 選択肢：「Remove（削除）」「Add（追加）」
Address	送信する IP アドレスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　入力する IPv4/IPv6 アドレスは既存の LLDP 管理 IP アドレスである必要があります。

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

LLDP 管理アドレスリストを表示します。

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。

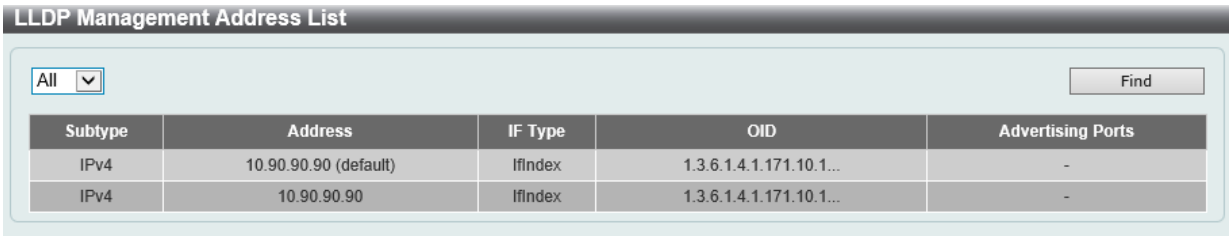


図 8-87　LLDP Management Address List 画面

画面に表示される項目：

項目	説明
Subtype	表示する LLDP 管理アドレスのサブタイプを選択します。 • 「All」- すべてのエントリを表示します。 • 「IPv4」- 表示されるフィールドに IPv4 アドレスを入力します。 • 「IPv6」- 表示されるフィールドに IPv6 アドレスを入力します。

「Find」ボタンをクリックして、指定した内容を基に 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 の Type-Length-Value（TLV）設定を行います。TLV により、LLDP パケット内で特定の情報を送信できます。
スイッチのアクティブな LLDP ポートには、通常、その外向き通知に必須データが含まれています。

必須のデータタイプには、以下の 4 タイプの TLV が含まれます。必須のデータタイプを無効にすることはできません。

- end of LLDPDU TLV
- chassis ID TLV
- port ID TLV
- TTL TLV

さらに、オプションで選択可能な 4 つのデータタイプがあります。

- ポート説明（Port Description）
- システム名（System Name）
- システム説明（System Description）
- システム機能（System Capability）

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。

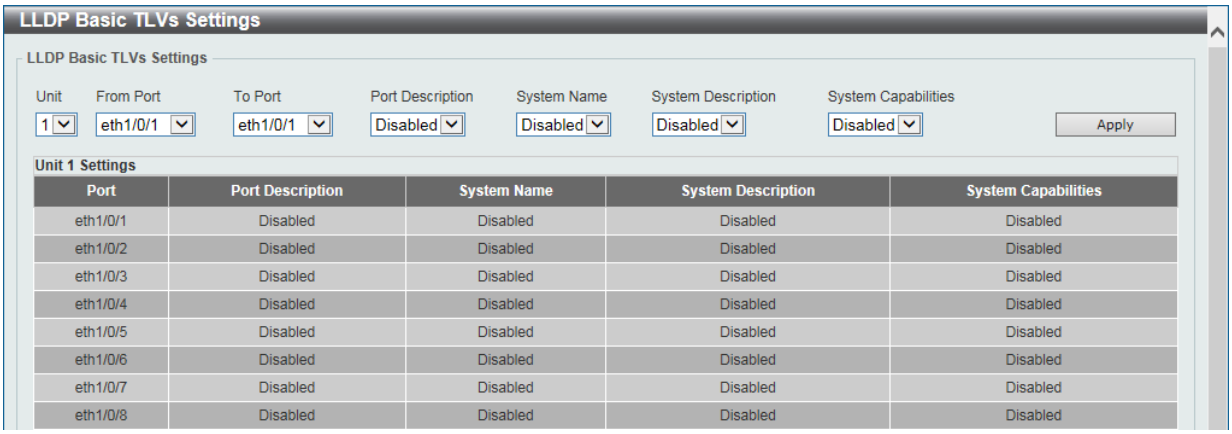


図 8-88　LLDP Basic TLVs Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Port Description	ポート説明オプションを有効 / 無効に設定します。
System Name	システム名オプションを有効 / 無効に設定します。

項目	説明
System Description	システム説明オプションを有効 / 無効に設定します。
System Capabilities	システム能力オプションを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

VLAN 関連の TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

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。

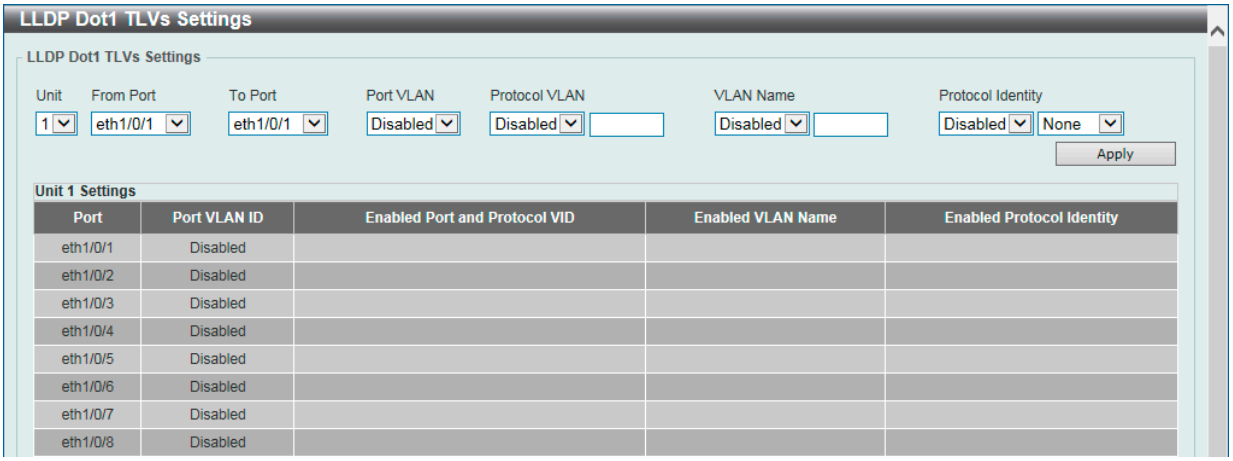


図 8-89　LLDP Dot1 TLVs Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Port VLAN	ポート VLAN ID TLV の通知を有効 / 無効に設定します。 ポート VLANID TLV はオプションの固定長 TLV であり、VLAN ブリッジポートにおいて、アンタグまたはプライオリティタグ付きのフレームに紐づくポート VLAN ID（PVID）を通知することが可能です。
Protocol VLAN	Port and Protocol VLAN ID（PPVID）TLV の通知を有効 / 無効に設定します。右の欄に VLAN ID を入力します。
VLAN Name	VLAN 名 TLV の通知を有効 / 無効に設定します。右の欄に VLAN 名 TLV の VLAN ID を入力します。
Protocol Identity	Protocol Identity TLV およびプロトコル名の通知を有効 / 無効に設定します。対象とするプロトコルを「None」「EAPOL」「LACP」「GVRP」「STP」「All」から選択します。

「Apply」ボタンをクリックして、設定内容を適用します。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

イーサネット関連の TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

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。

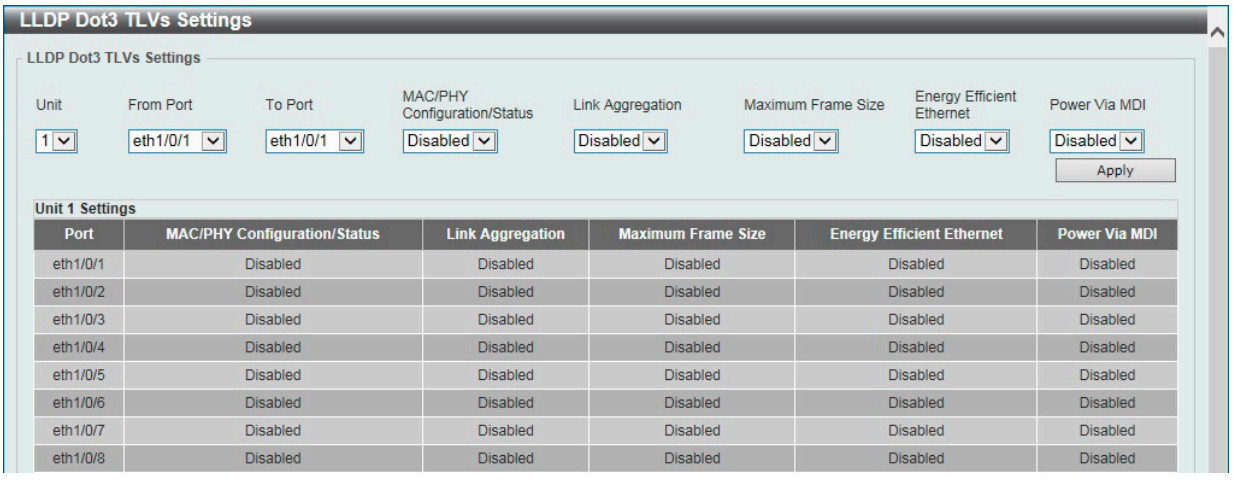


図 8-90　LLDP Dot3 TLVs Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
MAC/PHY Configuration/Status	MAC/PHY Configuration/Status TLV の通知を有効 / 無効に設定します。 （1）送信 IEEE 802.3 LAN ノードの Duplex およびビットレートの Capability （2）送信 IEEE 802.3 LAN ノードの現在の Duplex およびビットレート設定 を判別するオプションの TLV です。
Link Aggregation	Link Aggregation TLV の通知を有効 / 無効に設定します。Link Aggregation TLV には以下の情報が含まれます。 - リンクはリンクアグリゲーション可能かどうか - リンクは現在リンクアグリゲーションに設定されているか / 集約ポートのチャンネル ID ポートがリンクアグリゲーションで集約されていない場合、ID は 0 となります。
Maximum Frame Size	Maximum Frame Size TLV の通知を有効 / 無効に設定します。 この TLV は、実装された MAC/PHY の最大フレームサイズ性能を示します。
Energy Efficient Ethernet	Energy Efficient Ethernet TLV の通知を有効 / 無効に設定します。Energy Efficient Ethernet TLV は、パケットが送信されていないときのリンクのエネルギー省電力機能を示します。
Power Via MDI （PoE モデルのみ）	Power Via MDI 機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

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

LLDP-MED TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

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。

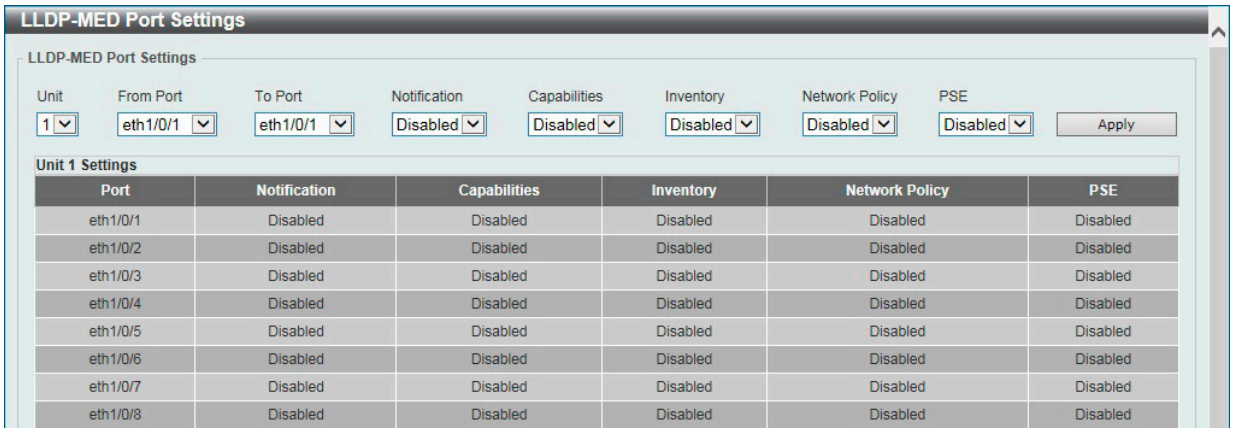


図 8-91　LLDP-MED Port Settings 画面

以下の項目が使用できます。

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Notification	LLDP-MED notification TLV の送信を有効 / 無効に設定します。
Capabilities	LLDP-MED capabilities TLV の送信を有効 / 無効に設定します。
Inventory	LLDP-MED inventory TLV の送信を有効 / 無効に設定します。
Network Policy	LDP-MED network policy TLV の送信を有効 / 無効に設定します。
PSE （PoE モデルのみ）	ローカルデバイスが PSE（給電デバイス）または PD（受電デバイス）の場合の LLDP-MED Extended Power-via MDI TLV の送信を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

LLDP Statistics Information（LLDP 統計情報）

スイッチにおける LLDP 統計情報を参照します。

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。

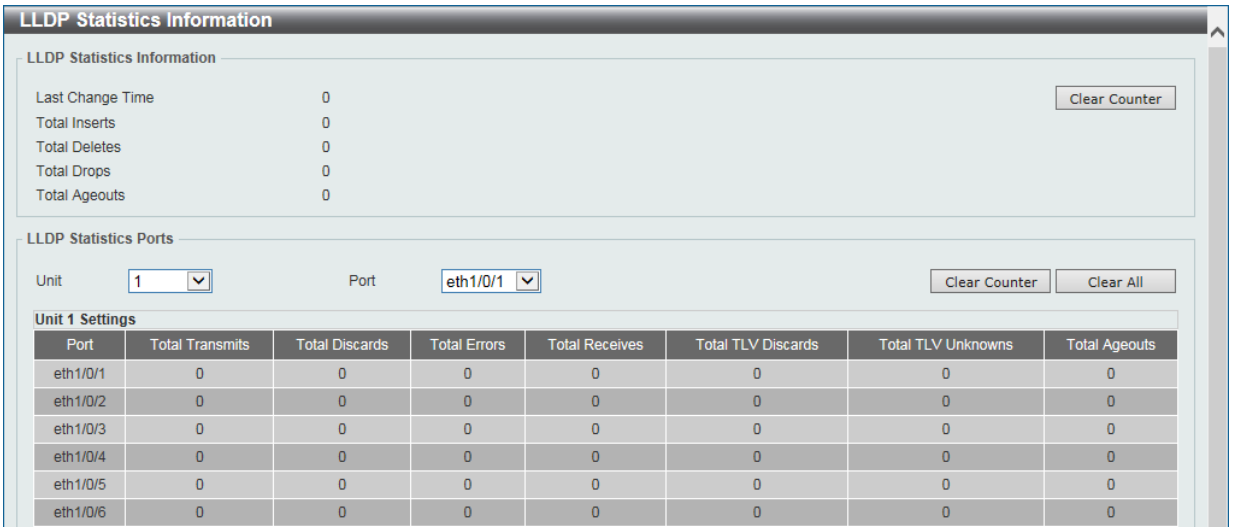


図 8-92　LLDP Statistics Information 画面

以下の項目が使用できます。

項目	説明
Unit	統計情報をクリアするユニットを選択します。
Port	統計情報をクリアするポートを指定します。

「Clear Counter」ボタンをクリックして、指定ポートの統計情報のカウンタ数をクリアします。
「Clear All」ボタンをクリックして、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）

外向きの LLDP 通知に含まれる情報を表示します。

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。

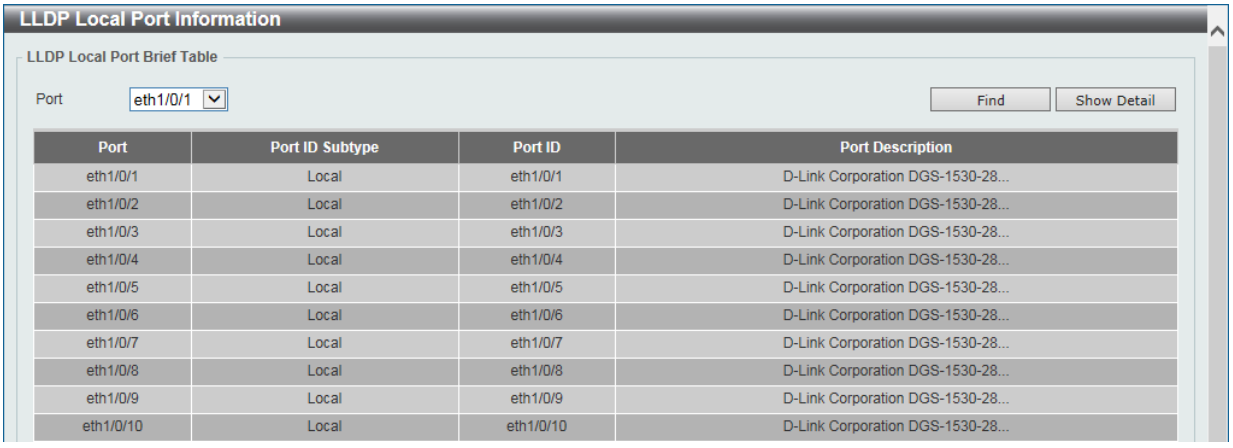


図 8-93　LLDP Local Port Information 画面

画面に表示される項目：

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

「Find」ボタンをクリックして、指定ポートのエントリを表示します。
「Show Detail」ボタンをクリックして、指定ポートの詳細情報を表示します。

詳細情報の参照

「Show Detail」ボタンをクリックし、以下の画面を表示します。

図 8-94　LLDP Local Port Information（Show Detail）画面

各パラメータの詳細の参照

各項目の「Show Detail」リンクをクリックすると、画面下部に情報が表示されます。

図 8-95　LLDP Local Port Information - MAC/PHY Configuration/Status 画面

前の画面に戻るには、「Back」ボタンをクリックします。

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

隣接（ネイバ）から学習した LLDP 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。

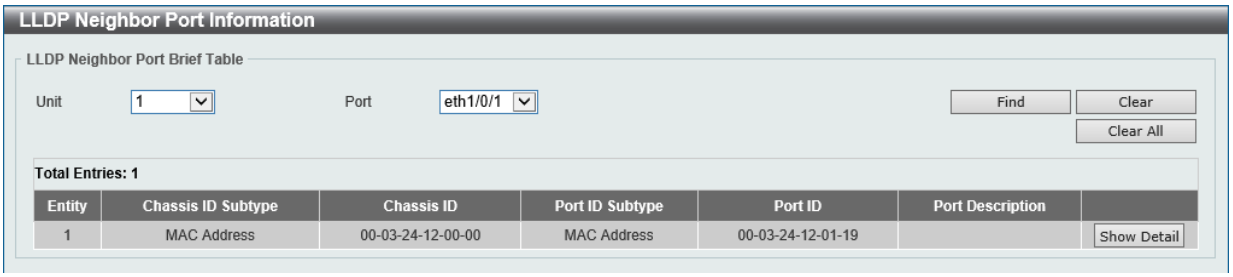


図 8-96　LLDP Neighbor Port Information 画面

画面に表示される項目：

項目	説明
Unit	ネイバ情報を表示 / クリアするユニットを選択します。
Port	ネイバ情報を表示 / クリアするポートを指定します。

「Find」ボタンをクリックして、指定ポートのネイバ情報を表示します。
「Clear」ボタンをクリックして、指定ポートのネイバ情報をクリアします。
「Clear All」ボタンをクリックして、全てのポートのネイバ情報をクリアします。

「Show Detail」をクリックして指定ポートの詳細情報を表示します。

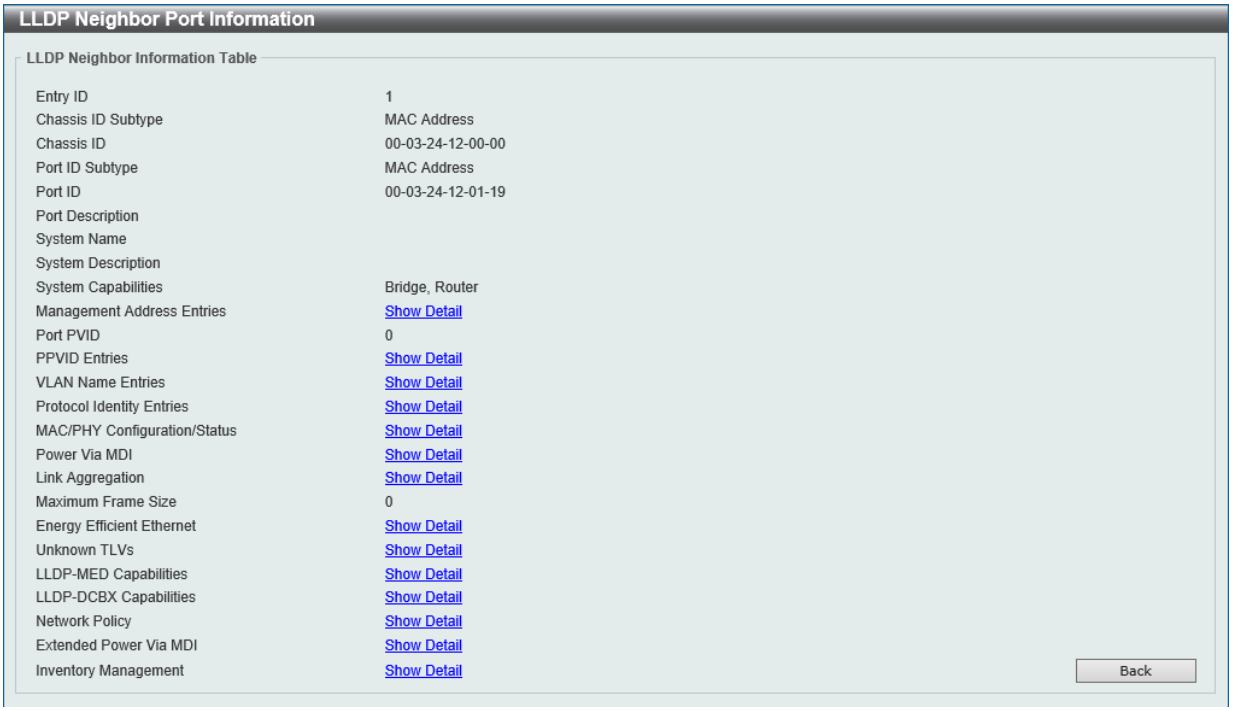


図 8-97　LLDP Neighbor Port Information（Show Detail）画面

各項目の「Show Detail」リンクをクリックすると、画面下部に情報が表示されます。（例 :MAC/PHY Configuration/Status）

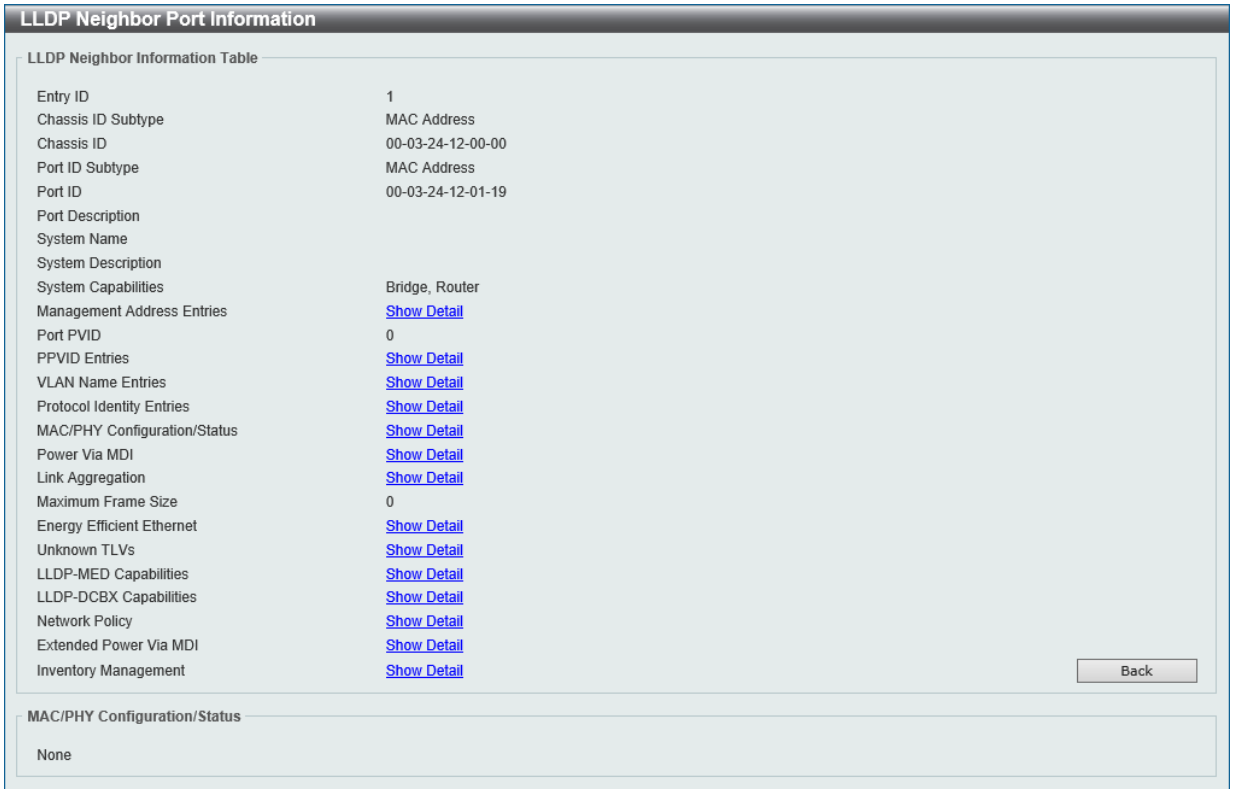


図 8-98　LLDP Neighbor Port Information（Show Detail - MAC/PHY Configuration/Status）画面

前の画面に戻るには、「Back」ボタンをクリックします。

第 9 章　L3 Features（レイヤ 3 機能の設定）

L3 Features メニューを使用し、本スイッチにレイヤ 3 機能を設定することができます。

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
ARP（ARP 設定）	ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
Gratuitous ARP（Gratuitous ARP 設定）	Gratuitous ARP の設定を行います。
IPv6 Neighbor（IPv6 ネイバ設定）	IPv6 ネイバ設定を行います。
Interface（インタフェース設定）	IP インタフェース設定を行います。
UDP Helper（UDP ヘルパー）	IP 転送プロトコルの設定を行います。本機能は指定の UDP サービスタイプのパケットの転送を有効にします。また UDP ブロードキャストパケットを転送するターゲットアドレスを指定します。
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定）	本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。
IPv4 Route Table（IPv4 ルートテーブル）	IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定）	IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。
IPv6 Route Table（IPv6 ルートテーブル）	IPv6 ルーティングテーブルを表示します。
IPv6 General Prefix（IPv6 汎用プレフィックス）	VLAN インタフェース IPv6 汎用プレフィックスの設定を行います。
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）	IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）の設定を行います。

ARP（ARP 設定）

L3 Features > ARP

ARP（Address Resolution Protocol）は、IP アドレスによってネットワーク上のホストの MAC アドレスを得るためのアドレス解決プロトコルです。
特定のデバイスに対する ARP 情報を参照、編集および削除することができます。

補足　ARP エントリ数は最大 1K です。（スタティック：256）

ARP Aging Time（ARP エージングタイム設定）

ARP エージングタイムの設定を行います。

L3 Features > ARP > ARP Aging Time の順にクリックし、以下の画面を表示します。

図 9-99　ARP Aging Time 画面

画面に表示される項目：

項目	説明
Interface VLAN	インタフェース VLAN ID を入力します。 • 設定可能範囲：1-4094
Timeout	「Edit」をクリックし、ARP エージングタイムアウト値（分）を入力します。 この時間が経過すると、エントリはテーブルから削除されます。

「Find」ボタンをクリックして、指定 VLAN に基づいてエントリを検索します。
「Show All」ボタンをクリックして、すべての ARP エージングタイムエントリを表示します。

ARP エージングタイムの編集

編集するエントリの「Edit」ボタンをクリックし、タイムアウト値を設定します。「Apply」ボタンをクリックして、設定内容を適用します。

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のページへ移動します。

Static ARP（スタティック ARP 設定）

スタティックエントリを ARP テーブルに定義します。

L3 Features > ARP > Static ARP の順にクリックし、以下の画面を表示します。

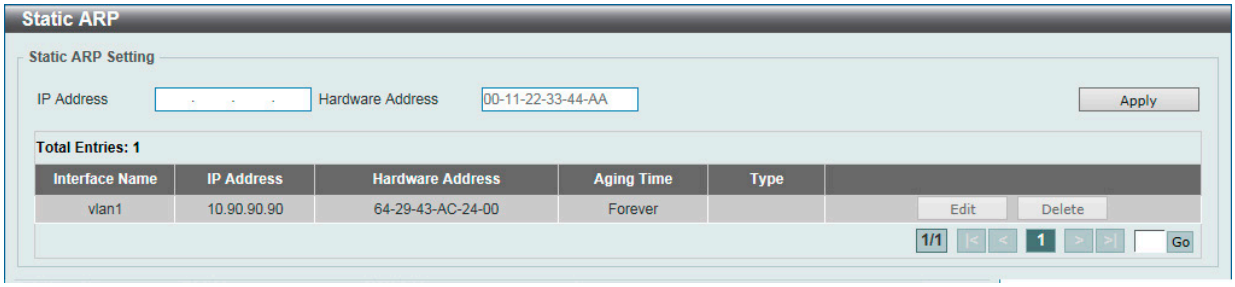


図 9-100　Static ARP 画面

画面に表示される項目：

項目	説明
IP Address	MAC アドレスに紐づける IP アドレスを設定します。
Hardware Address	IP アドレスに紐づける MAC アドレスを設定します。

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

Proxy ARP（プロキシ ARP）

プロキシ ARP の設定を参照および編集します。

プロキシ ARP は、他のデバイス当ての ARP リクエストに対して、L3 スイッチやルータが代理で ARP 応答を行う機能です。これにより、スタティックのルーティングやデフォルトゲートウェイを設定せずに、目的の宛先にパケットをルートすることが可能です。ホスト（通常レイヤ 3 スイッチ）は別の機器宛てのパケットに応答します。

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

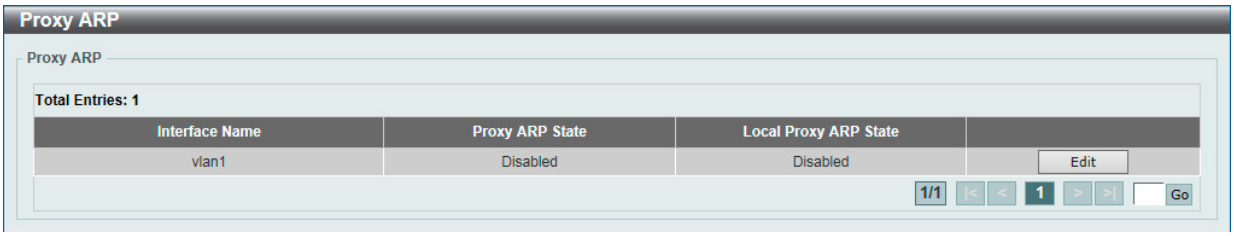


図 9-101　Proxy ARP 画面

画面に表示される項目：

項目	説明
Proxy ARP State	「Edit」をクリックし、プロキシ ARP を有効 / 無効に設定します。
Local Proxy ARP State	「Edit」をクリックし、ローカルプロキシ ARP を有効 / 無効に設定します。 ローカルプロキシ ARP 機能により、送信元 IP と宛先 IP が同じインタフェースにある場合に、スイッチがプロキシ ARP に返答できます。

「Edit」ボタンを選択して、特定エントリの設定を編集します。
「Apply」ボタンをクリックして、設定内容を適用します。

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のページへ移動します。

ARP Table（ARP テーブルの参照）

ARP テーブルの表示と設定を行います。

L3 Features > ARP > ARP Table メニューをクリックし、以下の画面を表示します。

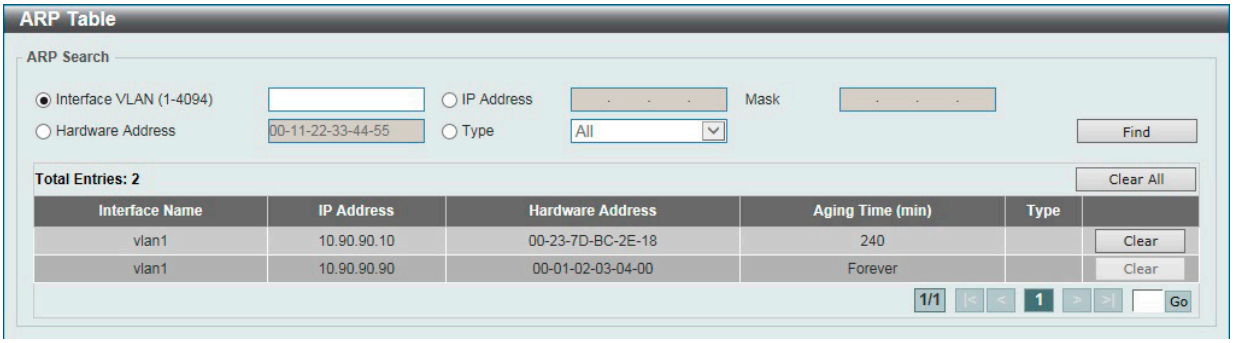


図 9-102　ARP Table 画面

画面に表示される項目：

項目	説明
Interface VLAN	表示するインタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094
IP Address	表示する IP アドレスを入力します。
Mask	上記 IP アドレスのマスクを指定します。
Hardware Address	表示する MAC アドレスを入力します。
Type	表示する ARP の種類を指定します。 • 選択肢：「All」「Dynamic」

「Find」ボタンをクリックして、入力した情報に基づくエントリを検索します。
「Clear」をクリックして、特定エントリのダイナミック ARP キャッシュを消去します。
「Clear All」ボタンをクリックして、すべてのダイナミック ARP キャッシュを消去します。

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。

Gratuitous ARP（Gratuitous ARP 設定）

Gratuitous ARP の設定を行います。
Gratuitous ARP リクエストパケットは、送信元 / 宛先 IP アドレスが送信元デバイスのアドレスに設定され、宛先 MAC アドレスがブロードキャストアドレスとなっている ARP リクエストパケットです。通常、Gratuitous ARP リクエストパケットを使用して、IP アドレスが他のデバイスと競合していないかどうかを検出したり、インタフェースに接続されたホストの ARP キャッシュエントリを事前ロードまたは再構成したりします。

Gratuitous ARP のグローバル設定を行います。

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

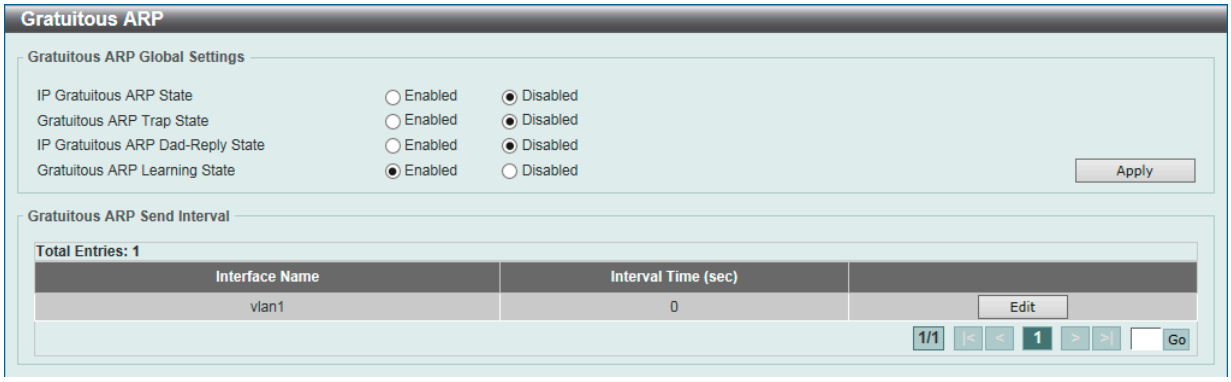


図 9-103　Gratuitous ARP 画面

画面に表示される項目：

項目	説明
IP Gratuitous ARP State	ARP キャッシュテーブルの Gratuitous ARP パケットの学習を有効 / 無効に設定します。
Gratuitous ARP Trap State	Gratuitous ARP トラップ を有効 / 無効に設定します。
IP Gratuitous ARP Dad-Reply State	IP Gratuitous ARP Dad-reply を有効 / 無効に設定します。
Gratuitous ARP Learning State	Gratuitous ARP 学習を有効 / 無効に設定します。 システムは通常、ARP 応答パケットや、スイッチの IP アドレスに対応する MAC アドレスを問い合せるための通常の ARP リクエストパケットからのみ ARP エントリを学習します。このオプションを使用すると、受信した Gratuitous ARP パケットに基づく ARP エントリの学習を有効 / 無効に設定できます。Gratuitous ARP パケットは、送信元アドレスと問合せ IP アドレスが同一のパケットです。

「Apply」ボタンをクリックして、設定内容を適用します。

「Edit」をクリックして指定エントリを編集します。以下の項目を使用して設定します。

項目	説明
Gratuitous ARP Send Interval	
Interval Time(sec)	Gratuitous ARP を送信する間隔（秒）を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

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のページへ移動します。

IPv6 Neighbor（IPv6 ネイバ設定）

スイッチの IPv6 ネイバ（隣接）設定を行います。

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

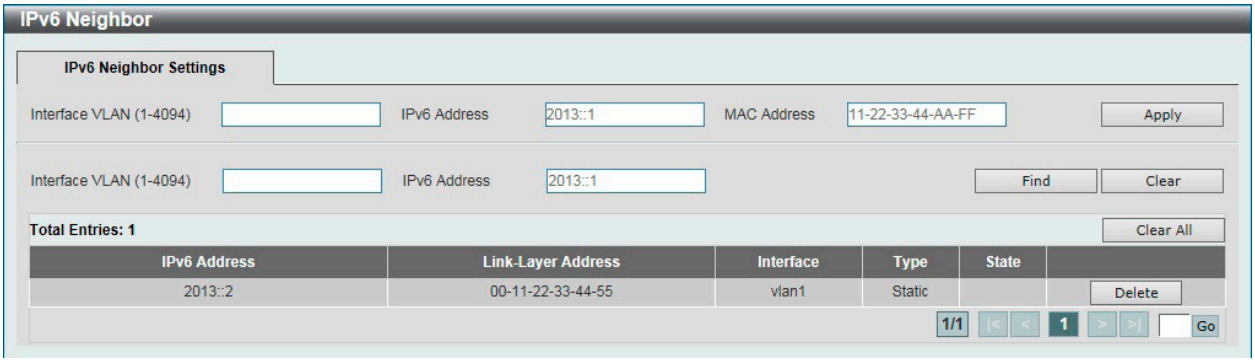


図 9-104　IPv6 Neighbor 画面

画面に表示される項目：

項目	説明
Interface VLAN	IPv6 Neighbor のインタフェース VLAN を指定します。 • 設定可能範囲：1-4094
IPv6 Address	IPv6 アドレスを入力します。
MAC Address	MAC アドレスを指定します。

IPv6 Neighbor の新規登録
画面上段の「Interface VLAN」「IPv6 Address」「MAC Address」を入力し、「Apply」ボタンをクリックします。

エントリの検索
画面中央の「Interface VLAN」「IPv6 Address」を入力し「Find」ボタンをクリックします。

ダイナミック IPv6 ネイバ情報の削除
指定インタフェースのダイナミック IPv6 ネイバ情報を削除するには、「Clear」ボタンをクリックします。
すべてのダイナミック IPv6 ネイバ情報を削除するには、「Clear All」ボタンをクリックします。

エントリの削除
該当エントリの「Delete」ボタンをクリックします。

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。

Interface（インタフェース設定）

スイッチの IP インタフェース設定を行います。

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。

補足　設定可能な IPv4 インタフェースは最大 64 です。

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。

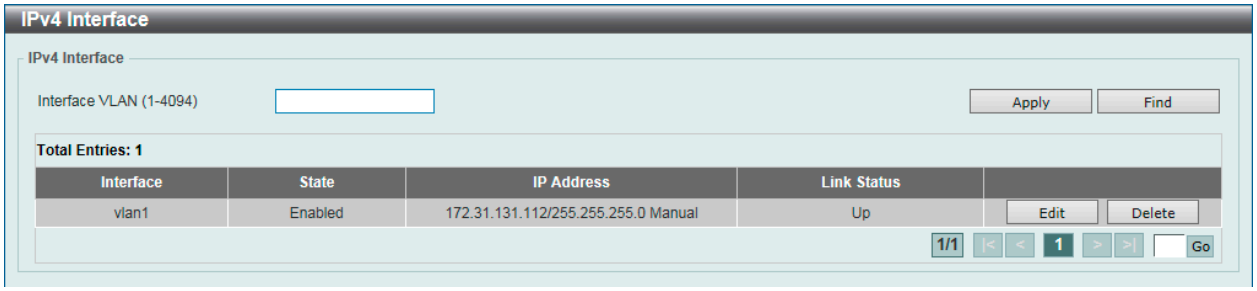


図 9-105　IPv4 Interface 画面

画面に表示される項目：

項目	説明
Interface VLAN	設定、表示するインタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」ボタンをクリックして、指定エントリを削除します。

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

「IPv4 Interface」画面で IPv4 インタフェースエントリの「Edit」ボタンをクリックして以下の画面を表示します。

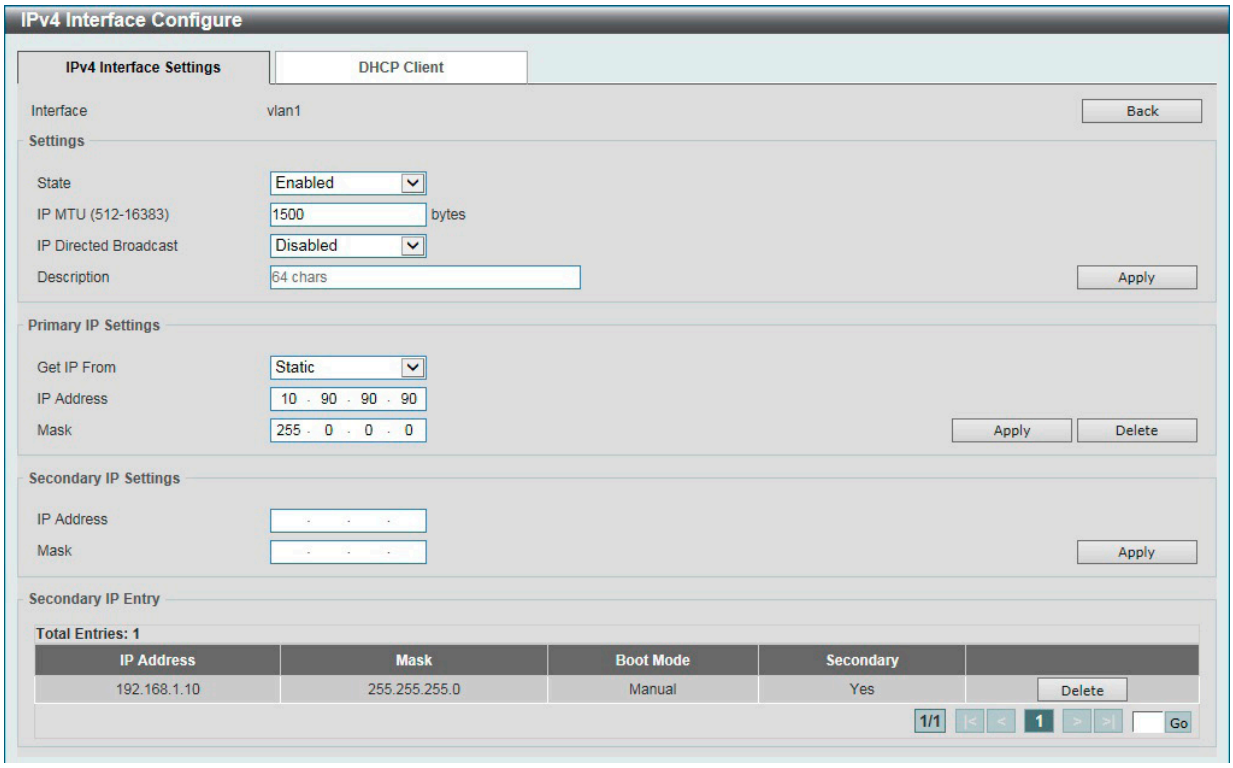


図 9-106　IPv4 Interface Configure 画面 - IPv4 Interface Settings タブ

画面に表示される項目：

項目	説明
Settings	
State	該当エントリの IPv4 インタフェースをグローバルに有効 / 無効に設定します。
IP MTU	MTU 値を入力します。 • 設定可能範囲：512-16383（bytes） • 初期値：1500（bytes）
IP Directed Broadcast	IP インタフェースの IP ディレクティッドブロードキャストの状態を有効 / 無効に設定します。 受信した IP ディレクティッドブロードキャストパケットについて、宛先ネットワークが直接スイッチに接続されている場合、そのパケットを転送するように設定します。
Description	エントリの説明を入力します。（64 文字以内）
Primary IP Settings	
Get IP From	IP アドレスの設定方法を選択します。 • 「Static」- インタフェースに設定する IPv4 アドレスを手動で設定します。 • 「DHCP」- ローカルネットワーク上の DHCP サーバから自動的に IPv4 情報を取得します。
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。
Secondary IP Settings	
IP Address	セカンダリインタフェースの IPv4 アドレスを設定します。
Mask	セカンダリインタフェースのサブネットマスクを設定します。

前の画面に戻るには、「Back」ボタンをクリックします。
「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
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。

注意 Secondary IP Address も IP インタフェース数を消費します。ただし、MAC アドレスは消費しません。

IPv4 インタフェースの編集（DHCP Client）

「IPv4 Interface」画面で IPv4 インタフェースエントリの「Edit」ボタンをクリック→「IPv4 Interface Configure」画面の「DHCP Client」タブをクリックして以下の画面を表示します。

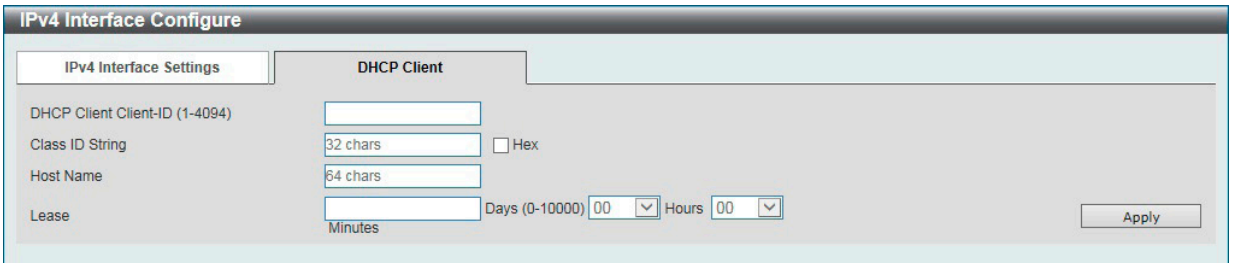


図 9-107　IPv4 Interface Configure 画面 - DHCP Client タブ

画面に表示される項目：

項目	説明
DHCP Client Client-ID	DHCP クライアント ID を入力します。この ID は VLAN インタフェースを指定します。該当インタフェースの 16 進数 MAC アドレスは、DISCOVER メッセージと一緒に送信されるクライアント ID として使用されます。 • 設定可能範囲：1-4094
Class ID String	クラス識別名を入力します（32 文字以内）。「Hex」にチェックを入れると 16 進数方式（64 文字以内）になります。 DHCP DISCOVER メッセージに含まれるオプション 60（ベンダークラス識別子）を指定するための設定値です。
Host Name	ホスト名を入力します。（64 文字以内）DHCP DISCOVER メッセージと一緒に送信されるホスト名オプションの値です。
Lease	DHCP クライアントに対し DHCP サーバから割り振られる IP アドレスのリース時間を指定します。オプションで時間と分を指定することもできます。 • 設定可能範囲：0-10000（日）

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6 Interface（IPv6 インタフェース）

スイッチの IPv6 インタフェース設定を行います。

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。

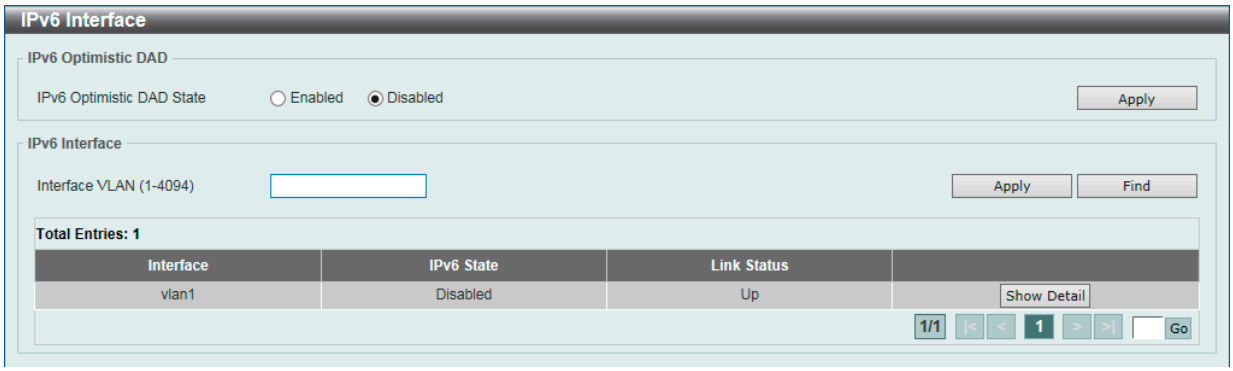


図 9-108　IPv6 Interface 画面

画面に表示される項目：

項目	説明
IPv6 Optimistic DAD	
IPv6 Optimistic DAD State	IPv6 Optimistic Duplicate Address Detection（DAD）を有効 / 無効に設定します。
IPv6 Interface	
Interface VLAN	設定、表示する IPv6 インタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show Detail」ボタンをクリックして、IPv6 インタフェースエントリの詳細を表示、設定します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

「IPv6 Interface」画面で IPv6 インタフェースエントリの「Show Detail」ボタンをクリックして以下の画面を表示します。

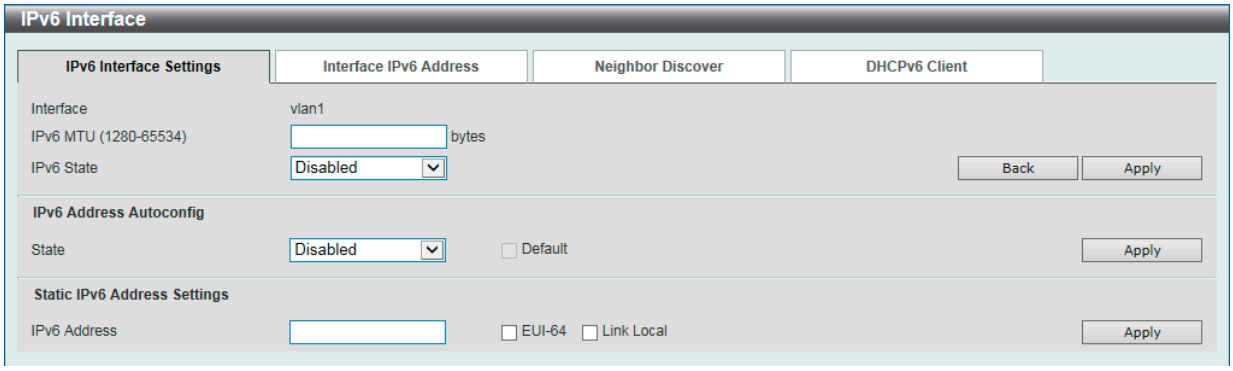


図 9-109　IPv6 Interface 画面 - IPv6 Interface Settings タブ

画面に表示される項目：

項目	説明
Interface	
IPv6 MTU	IPv6 MTU 値を入力します。RA メッセージ内でアドバタイズされる MTU の値です。 • 設定可能範囲：1280 - 65534（Bytes） • 初期値：1500（Bytes）
IPv6 State	設定エントリの IPv6 インタフェースをグローバルに有効 / 無効にします。
IPv6 Address Autoconfig	
State	ステートレス自動設定を使用した IPv6 アドレスの自動設定を有効 / 無効に設定します。 「Default」に指定すると、このインタフェースでデフォルトルータが選択されている場合、そのデフォルトルータを使用してデフォルトルートがインストールされます。このオプションは 1 つのインタフェースのみで指定可能です。

項目	説明
Static IPv6 Address Settings	
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。 • 「EUI-64」- EUI-64 インタフェース ID を使用してインタフェースの IPv6 アドレスを設定します。 • 「Link Local」- IPv6 インタフェースにリンクローカルアドレスを使用します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

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

「IPv6 Interface」画面で IPv6 インタフェースエントリの「Show Detail」ボタンをクリック→「Interface IPv6 Address」タブを選択して以下の画面を表示します。

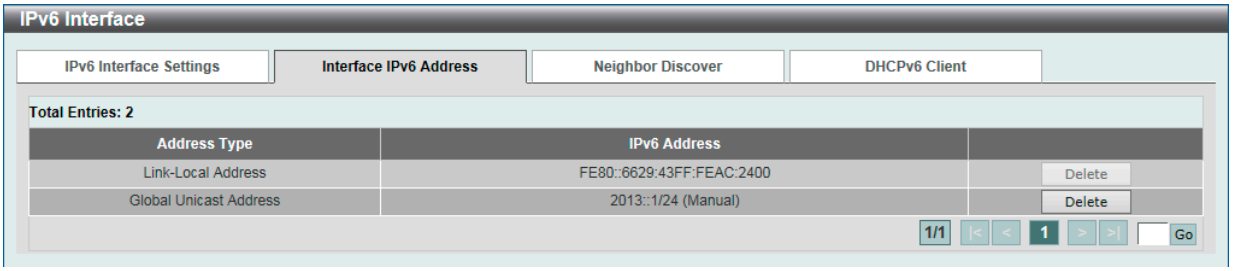


図 9-110　IPv6 Interface 画面 - Interface IPv6 Address タブ

エントリの削除
対象のエントリの「Delete」ボタンをクリックします。

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。

IPv6 インタフェースの編集（ Neighbor Discover タブ）

「IPv6 Interface」画面で IPv6 インタフェースエントリの「Show Detail」ボタンをクリック→「Neighbor Discover」タブを選択して以下の画面を表示します。

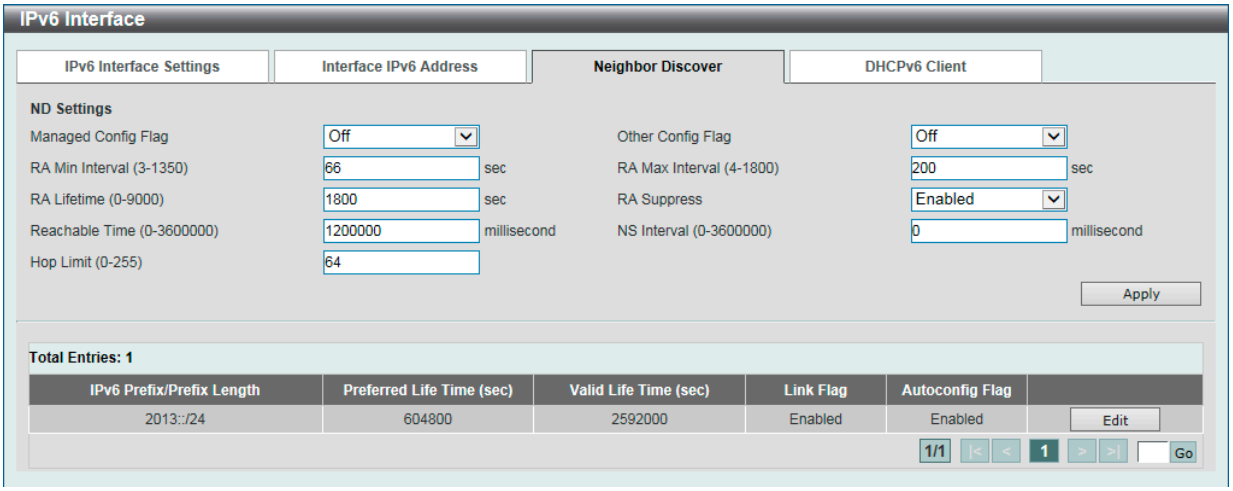


図 9-111　IPv6 Interface 画面 - Neighbor Discover タブ

画面に表示される項目：

項目	説明
Managed Config Flag	Managed Config Flag オプションを有効 / 無効に設定します。このフラグが有効な RA を受信すると、ネイバホストはステートフル設定プロトコルを使用して IPv6 アドレスを取得します。
Other Config Flag	Other Config Flag オプションを有効 / 無効に設定します。本設定を有効にすると、接続ホストはステートフル設定プロトコルを使用して、IPv6 アドレス以外の自動設定情報を取得します。
RA Min Interval	RA 通知の送信間隔の最小時間を入力します。最大値の 3/4 より大きくしないでください。 • 設定可能範囲：3-1350（秒）
RA Max Interval	RA 通知の送信間隔の最大時間を入力します。 • 設定可能範囲：4-1800（秒）
RA Lifetime	RA の有効期間を指定します。ホストは受信した RA に含まれる有効期間の値に基づき、送信元ルータをデフォルトルータとして使用します。 • 設定可能範囲：0-9000（秒）

項目	説明
RA Suppress	RA 抑制機能を有効 / 無効に設定します。
Reachable Time	Reachable Time 値を指定します。IPv6 ノードが、隣接しているノードの到達性を有効とみなす時間です。 「0」に指定された場合、1200 秒となり、RA メッセージでは 0（未指定）の値がアドバタイズされます。 • 設定可能範囲：0-3600000（ミリ秒）
NS Interval	Neighbor Solicitation（NS）間隔を指定します。 0 に指定された場合、1 秒間隔となり、RA メッセージには 0（未指定）の値がアドバタイズされます。 • 設定可能範囲：0-3600000（ミリ秒）（1000 の倍数）
Hop Limit	ホップリミットを指定します。システムから送信される IPv6 パケットも、最初のホップリミット値としてこの値を使用します。 • 設定可能範囲：0-255

「Apply」ボタンをクリックして、設定内容を適用します。

「Edit」をクリックすると、以下のように各パラメータを編集することができます。

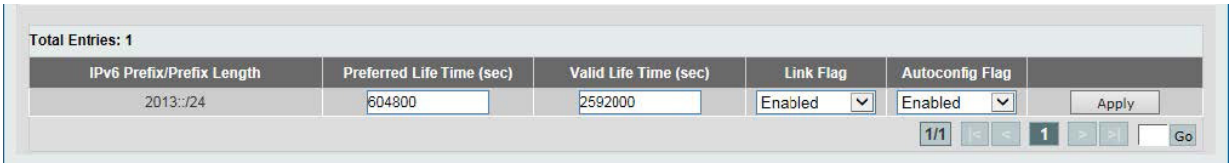


図 9-112　IPv6 Interface 画面 - Neighbor Discover タブ（Edit）

画面に表示される項目：

項目	説明
Preferred Life Time	推奨有効期間を入力します。 • 設定可能範囲：0-4294967295（秒）
Valid Life Time	有効期間を入力します。 • 設定可能範囲：0-4294967295（秒）
Link Flag	リンクフラグ機能の有効 / 無効を選択します。
Autoconfig Flag	自動設定フラグ機能の有効 / 無効を選択します。

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6 インタフェースの編集（DHCPv6 Client タブ）

「IPv6 Interface」画面で IPv6 インタフェースエントリの「Show Detail」ボタンをクリック→「DHCPv6 Client」タブを選択して以下の画面を表示します。

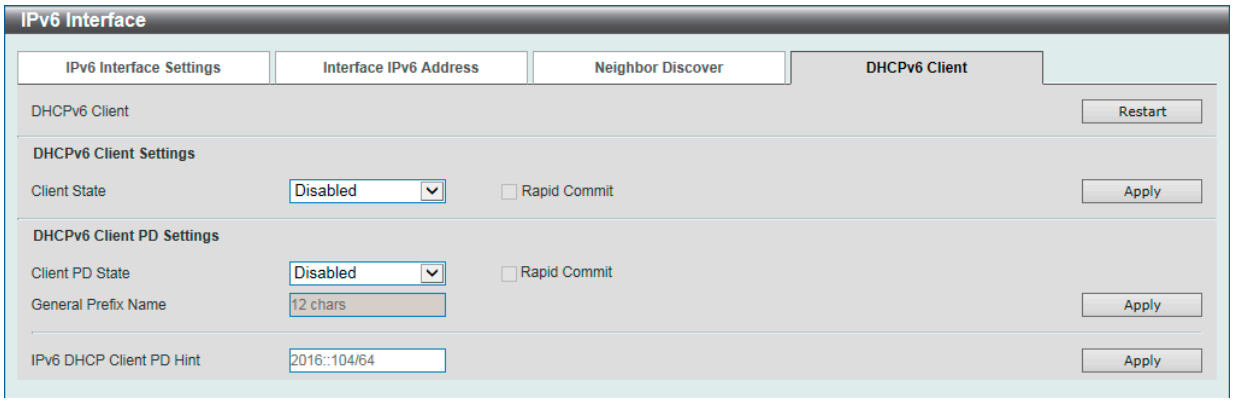


図 9-113　IPv6 Interface 画面 - DHCPv6 Client タブ

画面に表示される項目：

項目	説明
DHCPv6 Client	
DHCPv6 Client	「Restart」をクリックすると、DHCPv6 クライアントサービスを再始動します。
DHCPv6 Client Settings	
Client State	DHCPv6 クライアントを有効 / 無効に設定します。 アドレス配布では通常 4 個のメッセージ交換を行いますが、「Rapid Commit」にチェックを入れると、2 個のメッセージ交換を実行します。2 個のメッセージ交換を行うための「Rapid-Commit」オプションが Solicit メッセージに含まれます。

項目	説明
DHCPv6 Client PD Settings	
Client PD State	指定インタフェースを介して Prefix Delegation (PD) をリクエストする DHCPv6 クライアントプロセスを有効 / 無効に設定します。アドレス配布では通常 4 個のメッセージ交換を行いますが、「Rapid Commit」にチェックを入れると、2 個のメッセージ交換を実行します。2 個のメッセージ交換を行うための「Rapid-Commit」オプションが Solicit メッセージに含まれます。
General Prefix Name	IPv6 汎用プレフィックス名（12 文字以内）を指定します。
IPv6 DHCP Client PD Hint	ヒントとしてメッセージで送信される IPv6 プレフィックスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

Loopback Interface（ループバックインタフェース設定）

ループバックインタフェースを設定します。ループバックインタフェースは論理インタフェースであり、常に UP 状態となります。

L3 Features > Interface > Loopback 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。

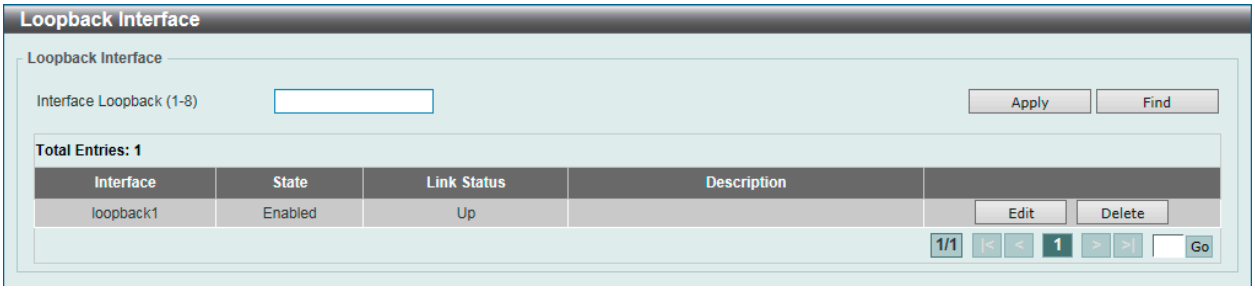


図 9-114　Loopback Interface 画面

画面に表示される項目：

項目	説明
Interface Loopback	ループバックインタフェース ID を入力します。 • 設定可能範囲：1-8

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

ループバックインタフェースの編集（Edit）

「Edit」（編集）ボタンをクリックして、以下の画面を表示します。

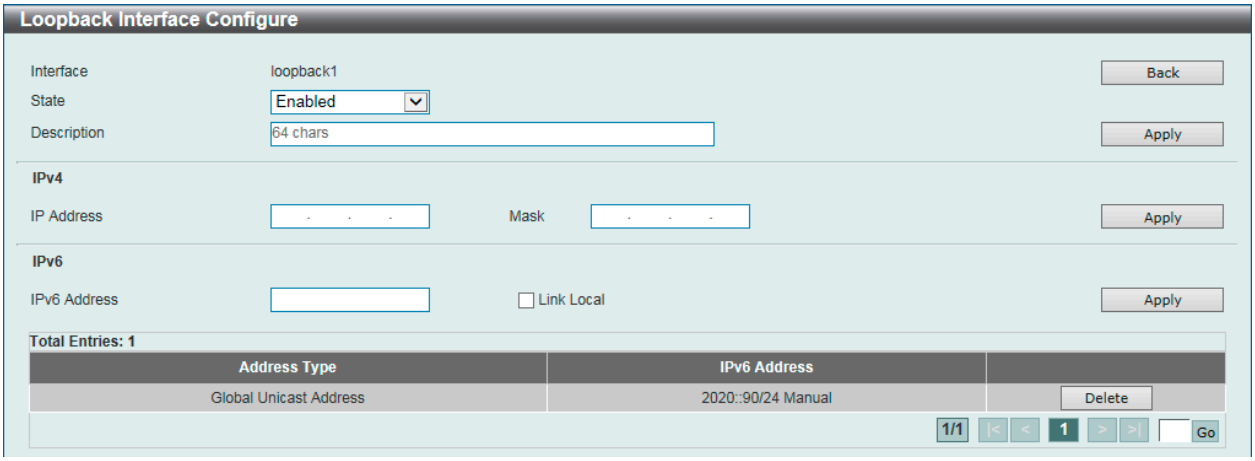


図 9-115　Loopback Interface（Edit）- Loopback Interface Configure 画面

画面に表示される項目：

項目	説明
State	ループバックインタフェースを有効 / 無効に設定します。
Description	ループバックインタフェースの説明（64 文字以内）を指定します。
IPv4	
IP Address	ループバックインタフェースの IPv4 アドレスを入力します。

項目	説明
Mask	ループバック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。
IPv6	
IPv6 Address	ループバックインタフェースの IPv6 アドレスを入力します。
Link Local	入力した IPv6 アドレスをリンクローカル IPv6 アドレスとして指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

インタフェースの削除
「Delete」ボタンをクリックして、指定エントリを削除します。

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。

Null Interface（Null インタフェース）

Null インタフェースを設定します。

L3 Features > Interface > Null 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 9-116　Null Interface 画面

画面に表示される項目：

項目	説明
Interface Null	Null インタフェース ID（0）を指定します。「0」のみ指定可能です。
Description	「Edit」をクリックして、Null インタフェースの説明を入力します。（64 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Delete」ボタンをクリックして、指定エントリを削除します。

UDP Helper（UDP ヘルパー）

L3 Features > UDP Helper
IP 転送プロトコルの設定を行います。

IP Forward Protocol（IP 転送プロトコル）

IP 転送プロトコルの設定、表示を行います。本機能では、特定の UDP サービスタイプのパケットの転送を有効にします。

L3 Features > UDP Helper > IP Forward 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。

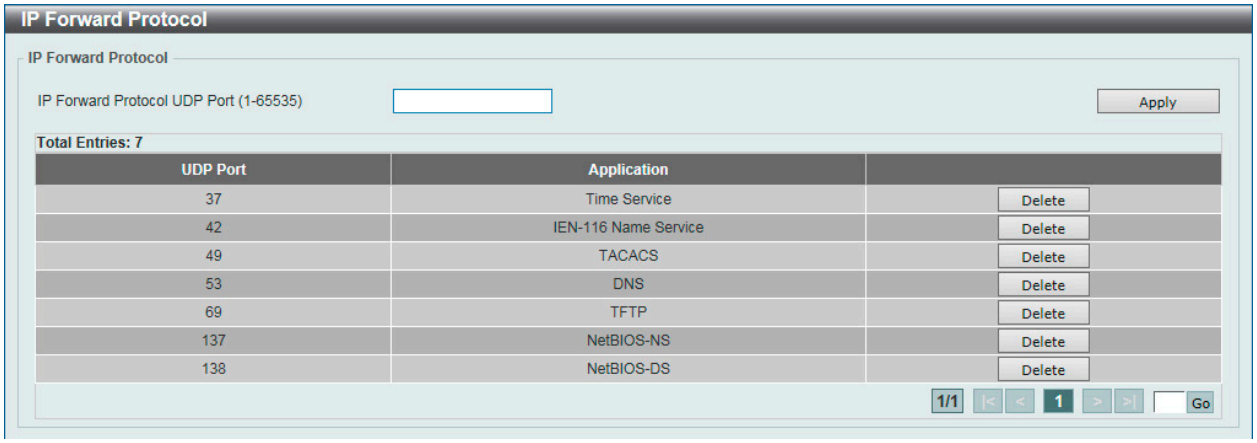


図 9-117　IP Forward Protocol 画面

画面に表示される項目：

項目	説明
IP Forward Protocol UDP Port	転送する UDP サービスの宛先ポートを指定します。 • 設定可能範囲：1-65535

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

IP Helper Address（IP ヘルパーアドレス）

本項目では UDP ブロードキャストパケットを転送するターゲットアドレスの追加 / 削除を指定します。
本機能は IP アドレスがアサインされた受信インタフェースのみ有効です。システムは以下の条件を満たす場合のみパケットを転送します。

- 宛先 MAC アドレスがブロードキャストアドレスである。
- 宛先 IP アドレスがオールワンブロードキャストである。
- パケットが IPv4 UDP パケットである。
- 「IP TTL 値」が「2」以上である。

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

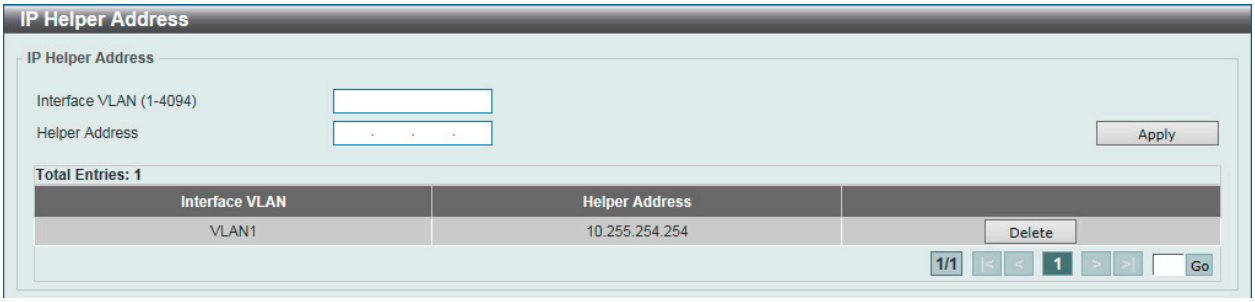


図 9-118　IP Helper Address 画面

画面に表示される項目：

項目	説明
Interface VLAN	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Helper Address	UDP ブロードキャストパケットの転送先 IPv4 アドレスを指定します。

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

IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定）

IPv4 スタティック / デフォルトルートの設定を行います。

IPv4 スタティックルートが設定されている場合、スイッチがネクストホップルータに対し ARP リクエストパケットを送信します。ネクストホップからスイッチに対し ARP 応答が返されると、ルートが有効になります。ただし、ARP エントリが既に存在している場合には、ARP 要求は送信されません。

スイッチはフローティングスタティックルートをサポートしています。ユーザは、異なるネクストホップを持つ代替のスタティックルートを作成することができます。この 2 個目のネクストホップデバイスのルートは、プライマリスタティックルートがダウンした場合のバックアップ用スタティックルートであると見なされます。プライマリルートが失われた場合、バックアップルートがアクティブになり、トラフィックの転送を開始します。

本スイッチのフォワーディングテーブル内のエントリは、IP アドレス、サブネットマスクおよびゲートウェイを使用して作成します。

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

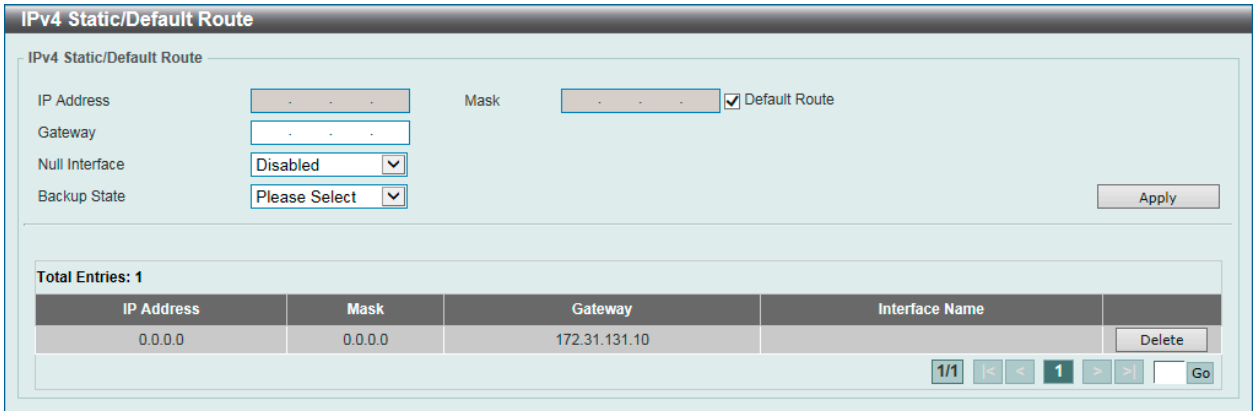


図 9-119　IPv4 Static/Default Route 画面

画面に表示される項目：

項目	説明
IP Address	スタティックルートに割り当てる IPv4 アドレスを入力します。 「Default Route」にチェックを入れると、IPv4 デフォルトルートを使用します。
Mask	このルートのサブネットマスクを入力します。
Default Route	このルートのゲートウェイ IP アドレスを入力します。
Gateway	このルートのゲートウェイ IP アドレスを入力します。
Null Interface	Null インタフェースを有効 / 無効に設定します。
Backup State	バックアップオプションを選択します。 • 「Primary」- 宛先へのプライマリルートとしてルートを指定します。 • 「Backup」- 宛先へのバックアップルートとしてルートを指定します。

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

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。

IPv4 Route Table（IPv4 ルートテーブル）

IPv4 ルートテーブルを表示します。

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

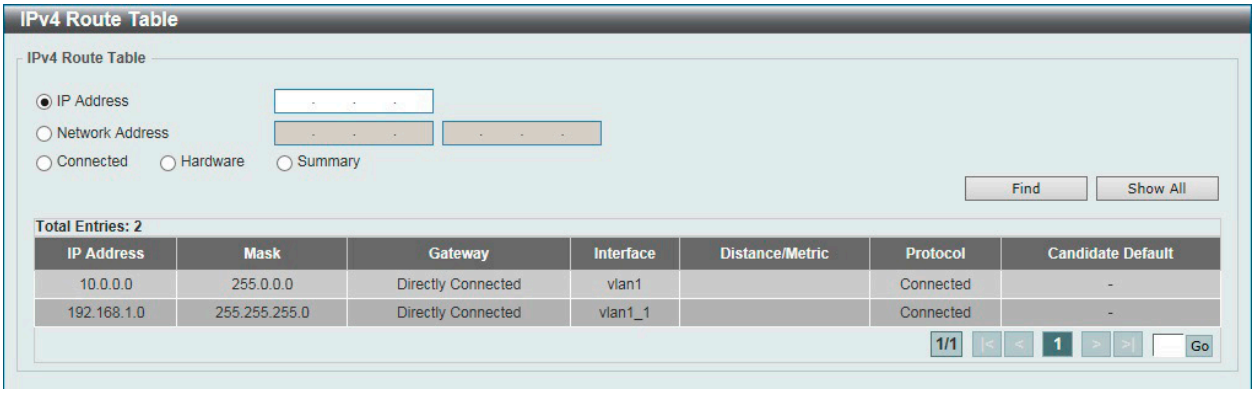


図 9-120　IPv4 Route Table 画面

画面に表示される項目：

項目	説明
IP Address	表示するルートの宛先 IP アドレスを指定します。
Network Address	表示するルートの宛先ネットワークアドレスを指定します。 1 つ目の入力欄にネットワークプレフィックス、2 つ目の入力欄にネットワークマスクを入力します。
Connected	接続されたルートのみを表示します。
Hardware	ハードウェアチップに記録されたルートのみ表示されます。
Summary	スイッチのルートエントリの概要が表示されます。

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

IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定）

IPv6 スタティックルート / デフォルトルートの設定を行います。

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

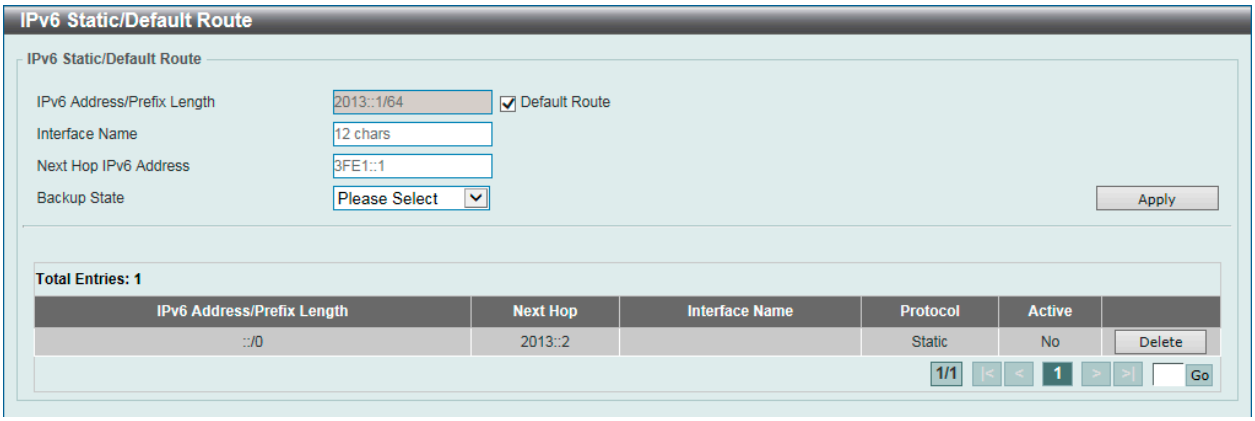


図 9-121　IPv6 Static/Default Route 画面

画面に表示される項目：

項目	説明
IPv6 Address/Prefix Length	スタティックルートに割り当てる IPv6 アドレスおよびプレフィックス長を入力します。 「Default Route」にチェックを入れると、IPv6 デフォルトルートを使用します。
Interface Name	このルートを関連づけるインタフェースの名前を入力します。
Next Hop IPv6 Address	ネクストホップ IPv6 アドレスを指定します。
Backup State	バックアップオプションを選択します。 • 「Primary」- 宛先へのプライマリルートとしてルートを指定します。 • 「Backup」- 宛先へのバックアップルートとしてルートを指定します。

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

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。

IPv6 Route Table（IPv6 ルートテーブル）

IPv6 ルートテーブルを表示します。

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

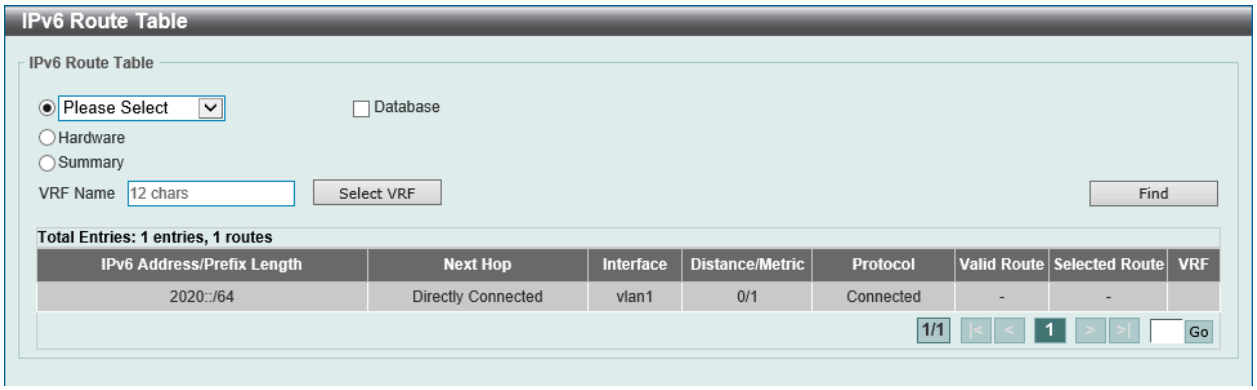


図 9-122　IPv6 Route Table 画面

画面に表示される項目：

項目	説明
IPv6 Address	プルダウンメニューから本項目を選択し、IPv6 アドレスを入力します。
IPv6 Address/Prefix Length	プルダウンメニューから本項目を選択し、ルートの IPv6 アドレスとプレフィックス長を指定します。 「Longer Prefixes」を指定した場合、プレフィックス長と同等、もしくはそれよりも長いプレフィックスの IPv6 ルートを表示します。
Interface Name	プルダウンメニューから本項目を選択し、表示するインタフェース名を指定します。
Connected	接続されたルートのみ表示します。
Database	ベストルートだけでなく、ルーティングデータベース内のすべての関連エントリを表示します。
Hardware	ハードウェアチップに記録されたルートのみ表示します。
Summary	スイッチのルートエントリの概要を表示します。

「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
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。

IPv6 General Prefix（IPv6 汎用プレフィックス）

本項目では、VLAN インタフェース IPv6 汎用プレフィックスの設定、表示を行います。

L3 Features > IPv6 General Prefix をクリックし、以下の画面を表示します。

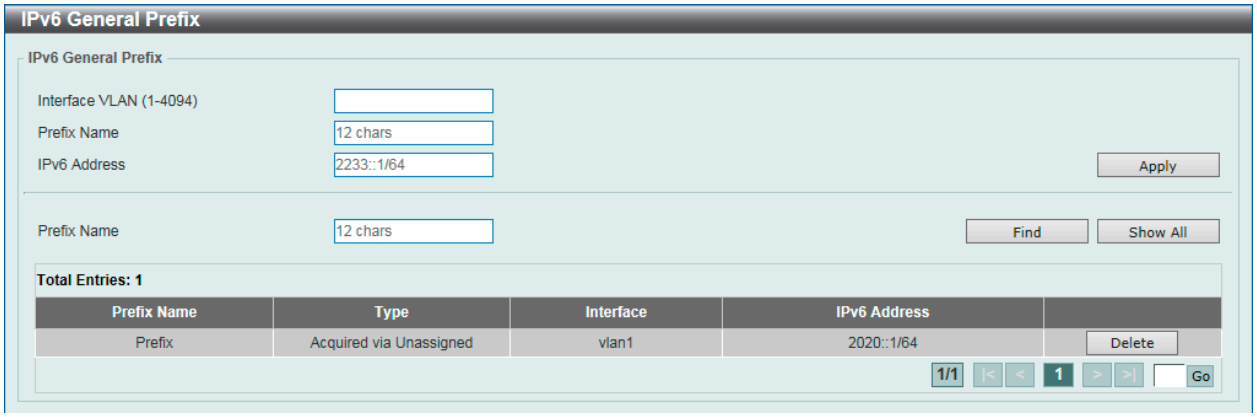


図 9-123　IPv6 General Prefix 画面

画面に表示される項目：

項目	説明
Interface VLAN	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Prefix Name	IPv6 汎用プレフィックスエントリ名を指定します。（12 文字以内）
IPv6 Address	IPv6 アドレスとプレフィックス長を指定します。 IPv6 アドレスのプレフィックス長は VLAN インタフェースのローカルサブネットでもあります。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

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。

IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）

L3 Features > IP Multicast Routing Protocol
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）の設定を行います。

IPMC（IP マルチキャスト設定）

L3 Features > IP Multicast Routing Protocol > IPMC

IP Multicast Global Settings（IP マルチキャストグローバル設定）

IP Multicast（IPMC）のグローバル設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Global Settings の順にメニューをクリックして、以下の画面を表示します。

図 9-124　IP Multicast Global Settings 画面

画面に表示される項目：

項目	説明
Table Lookup Mode	IP マルチキャストフォワーディングのルックアップモードを指定します。 • 「IP」- IP アドレスに基づいてマルチキャストフォワーディングルックアップを行います。 • 「MAC」- MAC アドレスに基づいてマルチキャストフォワーディングルックアップを行います。

「Apply」ボタンをクリックして、設定内容を適用します。

IP Multicast Routing Forwarding Cache（IP マルチキャストルーティングフォワーディングキャッシュ）

IP Multicast Routing Forwarding Cache（IP マルチキャストルーティングフォワーディングキャッシュ）データベースの表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Routing Forwarding Cache Table の順にメニューをクリックして、以下の画面を表示します。

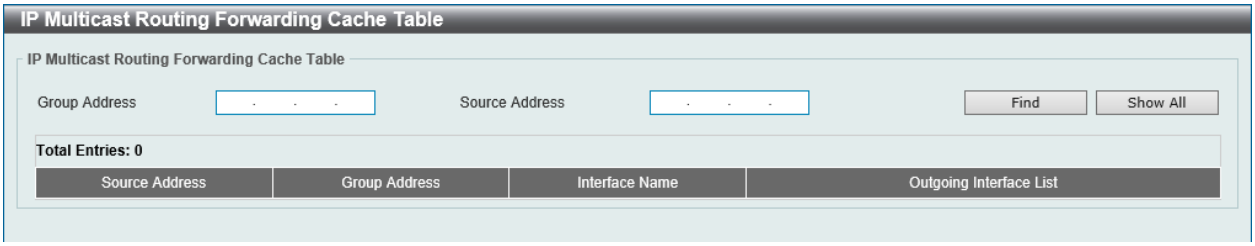


図 9-125　IP Multicast Routing Forwarding Cache Table 画面

画面に表示される項目：

項目	説明
Group Address	マルチキャストグループ IP アドレスを指定します。
Source Address	ソース IP アドレスを指定します。

「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。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

Control Packet CPU Filtering（コントロールパケット CPU フィルタリング）

コントロールパケット CPU フィルタリングの表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > Control Packet CPU Filtering の順にメニューをクリックして、以下の画面を表示します。

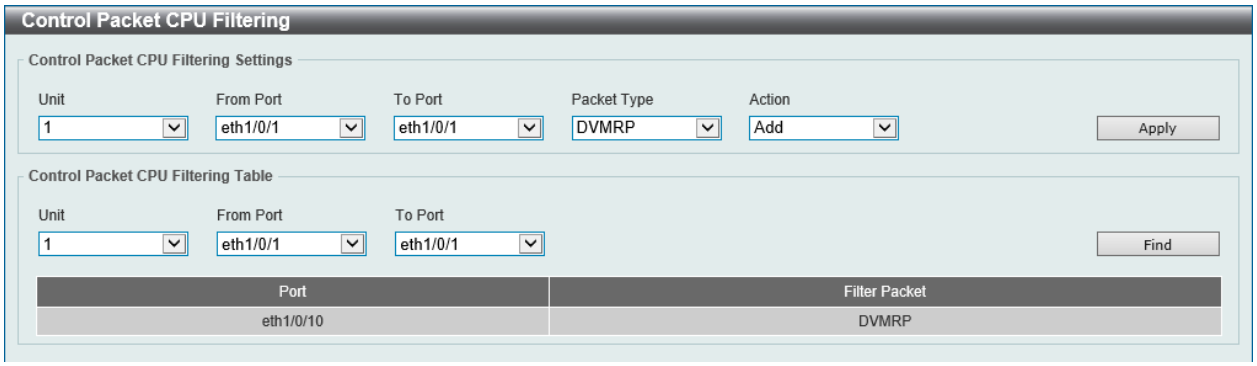


図 9-126　Control Packet CPU Filtering 画面

画面に表示される項目：

項目	説明
Control Packet CPU Filtering Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Packet Type	パケットの種類を指定します。 • 「DVMRP」- CPU に対して送信された「DVMRP L3 コントロールパケット」を破棄します。 • 「PIM」- CPU に対して送信された「PIM L3 コントロールパケット」を破棄します。 • 「IGMP Query」- CPU に対して送信された「IGMP Query L3 コントロールパケット」を破棄します。 • 「OSPF」- CPU に対して送信された「OSPF L3 コントロールパケット」を破棄します。 • 「RIP」- CPU に対して送信された「RIP L3 コントロールパケット」を破棄します。 • 「VRRP」- CPU に対して送信された「VRRP L3 コントロールパケット」を破棄します。
Action	実行するアクションを指定します。 • 「Add」- 指定した情報に基づきエントリを追加します。 • 「Remove」- 指定した情報に基づきエントリを削除します。
Control Packet CPU Filtering Table	
Unit	表示するユニットを指定します。
From Port / To Port	表示するポート範囲を設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。

IPv6MC（IPv6 マルチキャスト設定）

L3 Features > IP Multicast Routing Protocol > IPv6MC

IPv6 Multicast Routing Forwarding Cache Table（IPv6 マルチキャストルーティングフォワーディングキャッシュテーブル）

IPv6 Multicast Routing Forwarding Cache（IPv6 マルチキャストルーティングフォワーディングキャッシュ）データベースを表示します。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Forwarding Cache Table の順にメニューをクリックして、以下の画面を表示します。

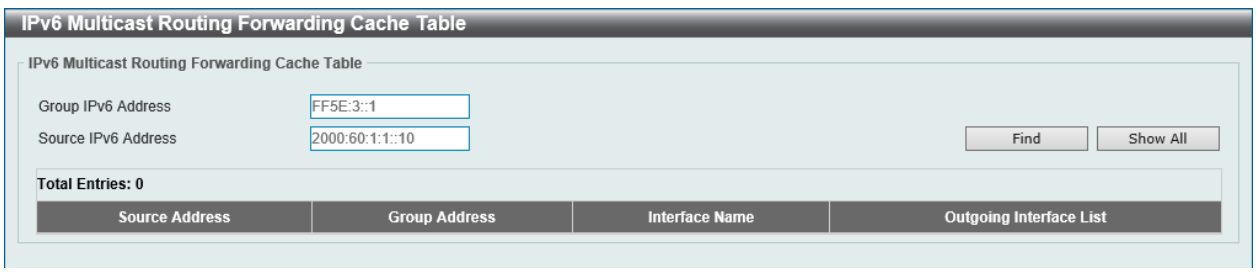


図 9-127　IPv6 Multicast Routing Forwarding Cache Table 画面

画面に表示される項目：

項目	説明
Group IPv6 Address	マルチキャストグループ IPv6 アドレスを指定します。
Source IPv6 Address	ソース IPv6 アドレスを指定します。

「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。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

第 10 章　QoS（QoS 機能の設定）

本スイッチは、802.1p プライオリティキューイングの QoS（Quality of Service）機能をサポートしています。

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
Basic Settings（基本設定）	QoS の Basic Settings（基本設定）を行います。
Advanced Settings（アドバンス設定）	QoS の Advanced Settings（アドバンス設定）を行います。

QoS の長所

QoS は IEEE 802.1p 標準で規定される技術であり、VoIP（Voice-over Internet Protocol）、Web 閲覧用アプリケーション、ファイルサーバアプリケーション、ビデオ会議など、広帯域を必要としたり高い優先順位を持つ重要なサービスのために、帯域を確保することができます。ネットワーク帯域を拡張するだけでなく、重要度の低いトラフィックに対して制限を行うことで、ネットワークが必要以上の帯域を使用しないようにします。スイッチの各物理ポートには個別のハードウェアキューがあり、様々なアプリケーションからのパケットがマッピングされ、優先順位が付けられます。
以下の図に、802.1p プライオリティキューイングがどのように本スイッチに実装されているかを示します。

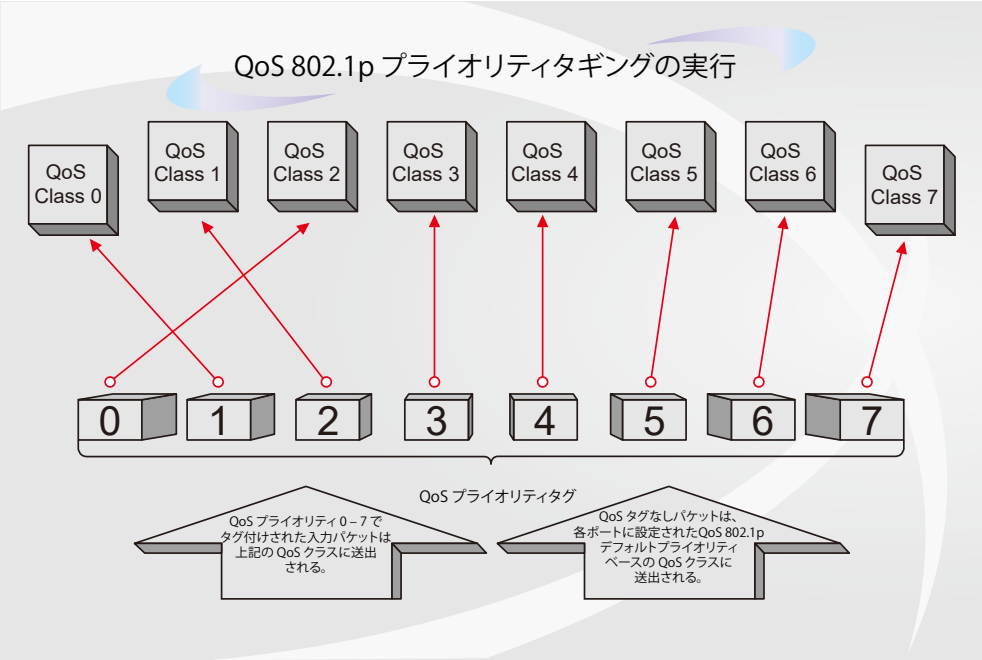


図 10-1　スイッチ上での QoS マッピングの例

上の図は本スイッチのプライオリティの初期設定です。クラス 7 はスイッチにおける 7 つのプライオリティクラスの中で、最も高い優先度を持っています。QoS を実行するためには、パケットのヘッダを調べて適切な識別タグがあるかどうかを確認するようにスイッチに指示する必要があります。そして、ユーザはそれらのタグ付きパケットをスイッチ上の指定されたキューに送り、優先順序に従って送出するようにします。

例えば、遠隔地に設置した 2 台のコンピュータ間でビデオ会議を行うとします。管理者は Access プロファイルコマンドを使用して、送信するビデオパケットにプライオリティタグを追加することができます。そして、受信側ではそのタグを検査するように設定し、受信したタグ付きパケットをスイッチのクラスキューに関連付けるようにします。また、管理者はこのキューに優先順位を与え、他のパケットよりも先に送信されるように設定を行います。この結果、このサービス用のパケットはできる限り早く送信されます。キューが優先されることにより、パケットは中断せずに送信されるため、このビデオ会議用に帯域を最適化することが可能になります。

QoS について

本スイッチは、802.1p プライオリティキューをサポートしており、8 個のプライオリティキューがあります。プライオリティキューには、最高レベルの 7 番キュー（クラス 7）から最低レベルの 0 番キュー（クラス 0）までがあります。IEEE 802.1p（p0 から p7）に規定される 8 つのプライオリティタグは、以下のようにスイッチのプライオリティキューにマッピングされます。

- プライオリティ 0 は、スイッチの Q2 キューに割り当てられます。
- プライオリティ 1 は、スイッチの Q0 キューに割り当てられます。
- プライオリティ 2 は、スイッチの Q1 キューに割り当てられます。
- プライオリティ 3 は、スイッチの Q3 キューに割り当てられます。
- プライオリティ 4 は、スイッチの Q4 キューに割り当てられます。
- プライオリティ 5 は、スイッチの Q5 キューに割り当てられます。
- プライオリティ 6 は、スイッチの Q6 キューに割り当てられます。
- プライオリティ 7 は、スイッチの Q7 キューに割り当てられます。

Strict（絶対優先）のプライオリティベースのスケジューリングでは、優先度の高いキューに属するパケットから送信されます。Strict 方式のキューが複数ある場合、プライオリティタグに従って順番に送信されます。優先度の高いキューが空になると、次の優先度を持つパケットが送信されます。

重み付けラウンドロビンキューイングでは、各プライオリティキューから送信されるパケットの数は、指定された重み付けによって決定されます。8 つの CoS（Class of Service）キュー、A ～ H に 8 から 1 までの重み付けを設定したとすると、パケットは以下の順に送信されます。
A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1

重み付けラウンドロビンキューイングにおいて各 CoS キューが同じ重み付けを持つ場合、ラウンドロビンキューイングのように、各 CoS キューのパケットは同じ割合で送信されます。また、ある CoS キューの重み付けとして 0 を設定すると、そのキューから送信するパケットがなくなるまでパケットを処理します。0 以外の値を持つ他のキューでは、重み付けラウンドロビンの規則により、重みに従って送信を行います。

Basic Settings（基本設定）

QoS の Basic Settings（基本設定）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 > Basic Settings > 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。

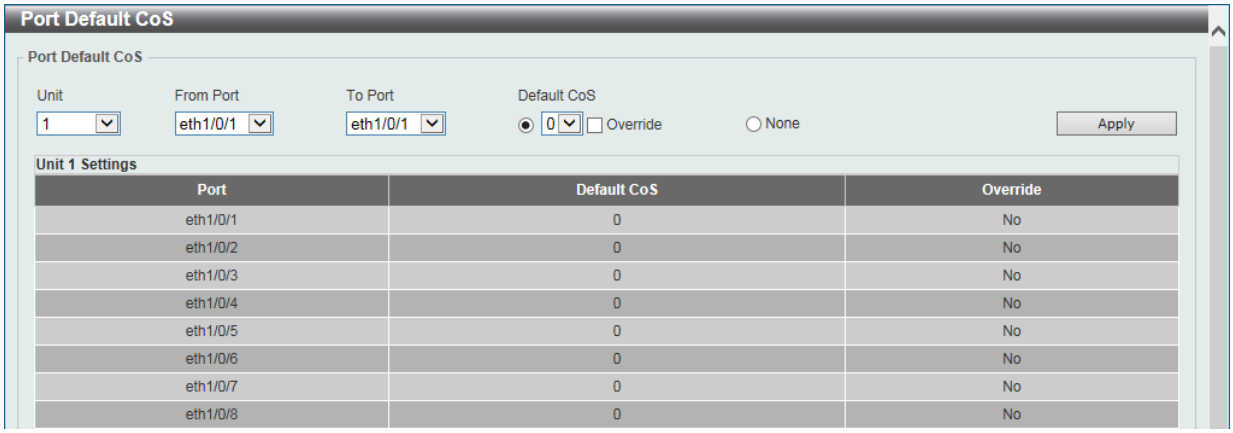


図 10-1　Port Default CoS 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Default CoS	ポートのデフォルト CoS を指定します。 「Override」にチェックを入れると、パケットの CoS を上書きします。デフォルト CoS は、ポートで受信した全てのパケット（タグ付き / タグなしの両方）に適用されます。「None」を選択すると、タグ付きパケットの場合はパケットの CoS を使用し、タグなしパケットの場合はポートデフォルト CoS となります。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。

Port Scheduler Method（ポートスケジューラ方式設定）

ポートスケジューラ方式を設定します。

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

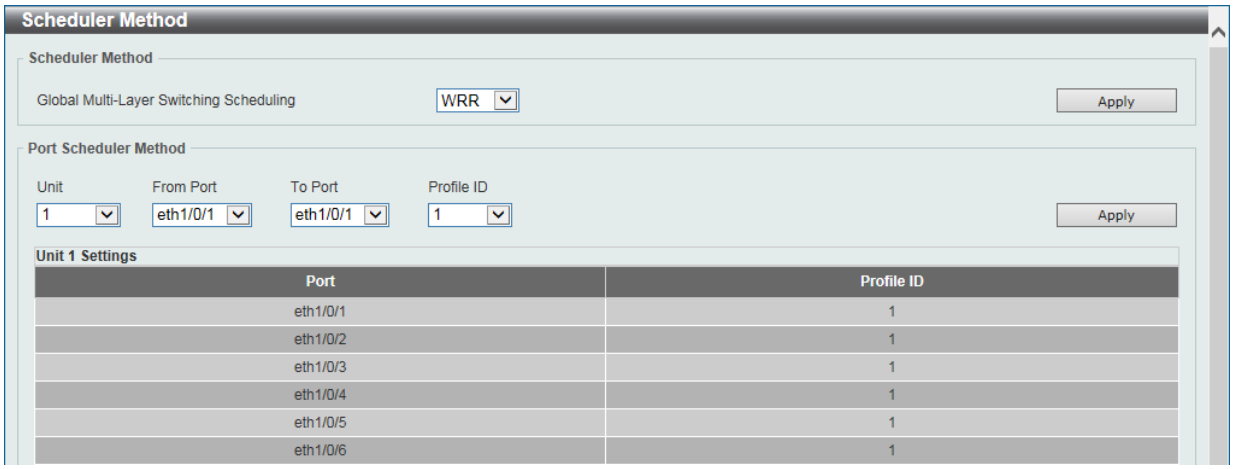


図 10-2　Port Scheduler Method 画面

画面に表示される項目：

項目	説明
Scheduler Method	
Global Multi-Layer Switching Scheduling	指定ポートに対するスケジューリング方式を以下から設定します。 • **「SP」（Strict Priority）**： すべてのキューは Strict Priority（絶対優先）スケジューリングを使用します。最も高い CoS 優先度のキューから絶対優先で送信されます。 • **「WRR」（Weighted Round-Robin）**： Round-Robin 方式でパケットをキューに送出します。最初に、各キューは可変の重みをセットします。高い優先度の CoS キューからパケットが送信される度に、重み（Weight）の値から「1」が差し引かれ、次の CoS 優先度キューが処理されます。重みが「0」になると、重みが補充されるまでそのキューの処理は停止します。すべての CoS キューの重みが「0」に到達すると、キューの重みが補充されます。（初期値） • **「WDRR」（Weighted Deficit Round Robin）**： Round-Robin 方式で送信キューに蓄積された未処理のクレジットを処理します。最初に、各キューはクレジットカウンタを可変のクオンタム値にセットします。CoS キューからパケットが送信される度に、クレジットカウンタからパケットサイズが差し引かれ、次の CoS 優先度キューが処理されます。クレジットカウンタが「0」になると、クレジットが補充されるまでそのキューの処理は停止します。すべての CoS キューのクレジットカウンタが「0」に到達すると、クレジットカウンタが補充されます。クレジットカウンタが 0 またはマイナスになり、最後のパケット送信が完了するまで処理が行われます。その後、クレジットは補充されます。クレジットが補充されると、各 CoS キューのクレジットカウンタにクレジットのクオンタムが補充されます。各キューのクオンタムはユーザ定義により異なる場合があります。 特定の CoS キューを SP モードに設定する場合、それより優先度の高い CoS キューについても SP モードである必要があります。
Port Scheduler Method	
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Profile ID	スケジューリングプロファイル ID を選択します。 • 選択可能範囲：1-8

「Apply」ボタンをクリックして、設定内容を適用します。

Queue Settings（QoS 設定）

キューを設定、表示します。

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

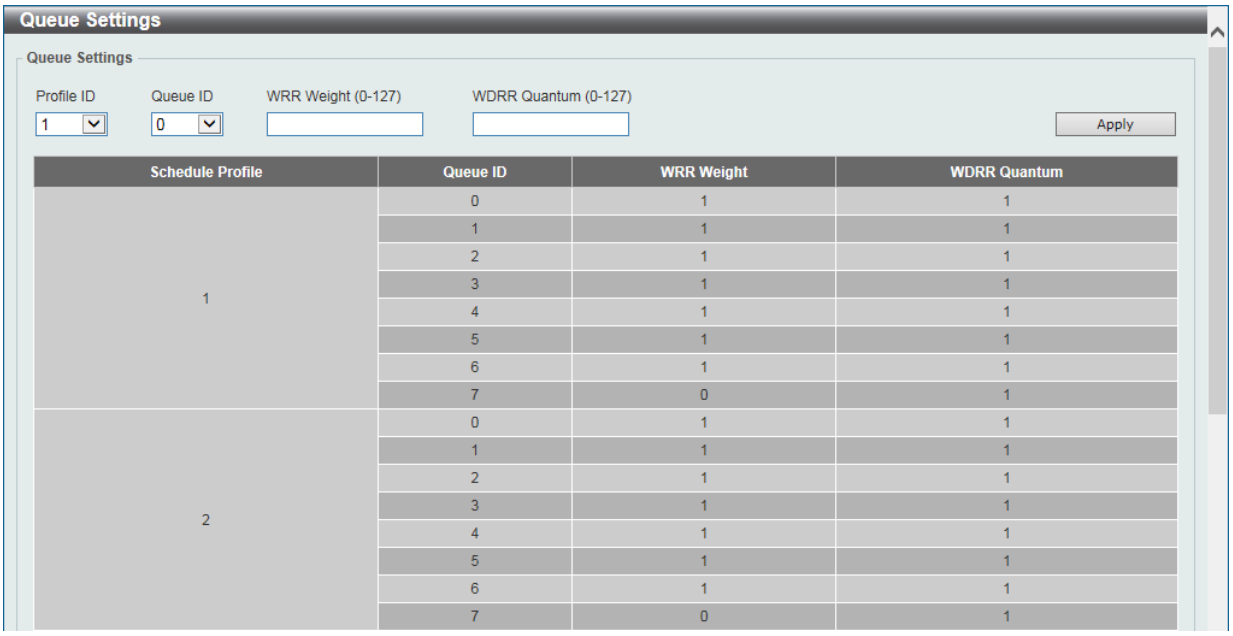


図 10-3　Queue Settings 画面

画面に表示される項目：

項目	説明
Profile ID	スケジューリングプロファイル ID を選択します。 • 設定可能範囲：1-8

項目	説明
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。「Expedited Forwarding」(EF) の動作要件を満たすには、最も優先度の高いキューが常に「Per-hop Behavior」(PHB) により選択され、キューのスケジュールモードが Strict プライオリティである必要があります。そのため、「Differentiate Service」がサポートされている場合、最後のキューの重みは 0 に設定する必要があります。 • 設定可能範囲：0-127
WDRR Quantum	「WDRR Quantum」の値を入力します。 • 設定可能範囲：0-127

「Apply」ボタンをクリックして、設定内容を適用します。

CoS to Queue Mapping（CoS キューマッピング設定）

CoS キューマッピングの表示、設定を行います。

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

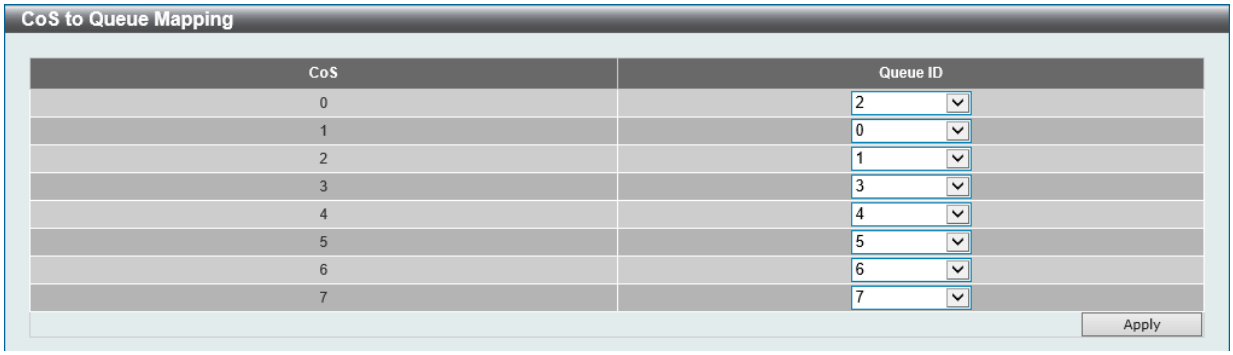


図 10-4　CoS to Queue Mapping 画面

画面に表示される項目：

項目	説明
Queue ID	各 CoS 値にマッピングされるキュー ID を指定します。 • 選択肢：0-7

「Apply」ボタンをクリックして、設定内容を適用します。

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 > Basic Settings > 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。

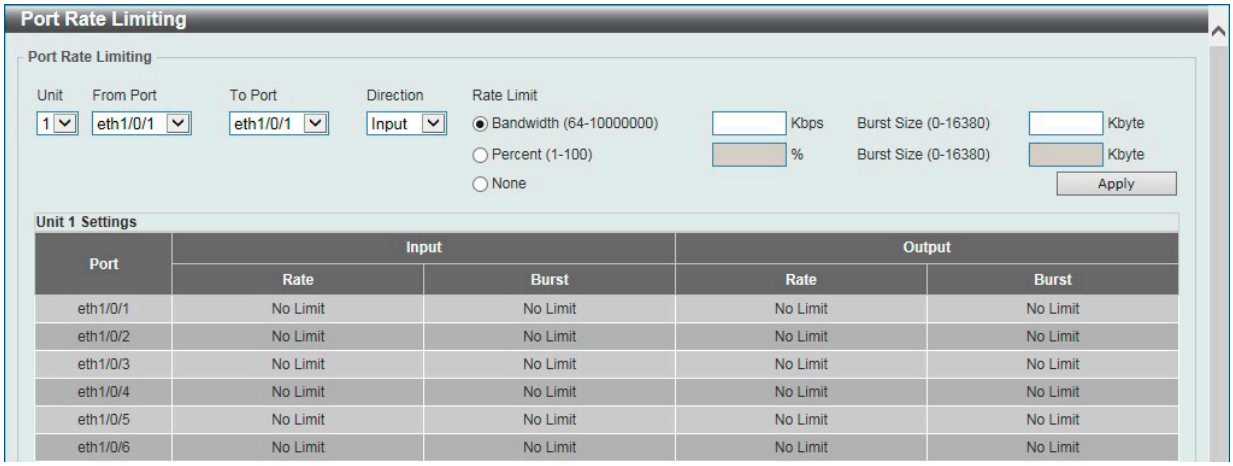


図 10-5　Port Rate Limiting 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。

項目	説明
Direction	レート制限の対象を指定します。 • 「Input」- 入力パケットのレート制限が設定されます。 • 「Output」- 出力パケットのレート制限が設定されます。
Rate Limit	レート制限の値を指定します。 指定された制限は、指定インタフェースの最大速度を超えることはできません。受信帯域幅制限については、受信トラフィックが制限を超えたときに、受信側は PAUSE フレームまたはフロー制御フレームを送信します。 • 「Bandwidth」- 受信 / 送信の帯域幅のレート制限値を入力欄に入力します。「Burst Size」に 0 を指定した場合、インタフェース上でレート制限は無効（制限なし）となります。 - 設定可能範囲：64-10000000（Kbps） - 「Burst Size」：0-16380（Kbytes） • 「Percent」- 受信 / 送信の帯域幅のレート制限パーセンテージを入力欄に入力します。 - 設定可能範囲：1-100（%） - 「Burst Size」：0-16380（Kbytes） • 「None」- 指定ポートのレート制限を削除します。初期値では、すべてのポートの送受信に対し、このオプションが使用されます。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　バーストサイズに 0 を指定した場合、レート制限は機能しません。

Queue Rate Limiting（キューレート制限設定）

キューレートの制限設定をします。

QoS > Basic Settings > Queue 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。

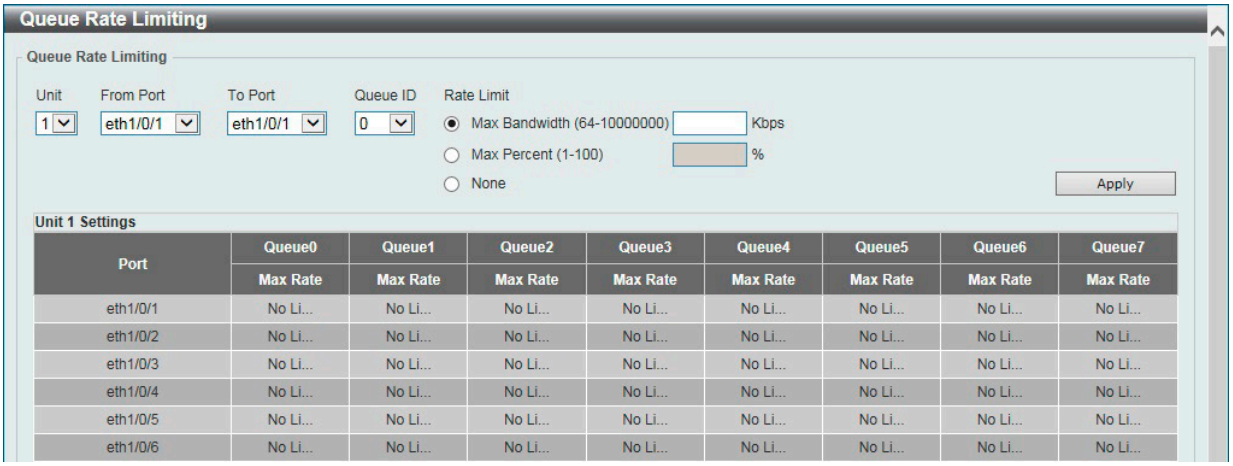


図 10-6　Queue Rate Limiting 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Queue ID	キュー ID を指定します。 • 選択肢：0-7
Rate Limit	キューレート制限の設定を行います。 • 「Max Bandwidth」- 帯域幅の最大レート制限値を入力します。 - 設定可能範囲：64-10000000（Kbps） • 「Max Percent」- 最大レート制限パーセンテージを入力します。 - 設定可能範囲：1-100（%） • 「None」- 指定ポートのレート制限を「なし」に設定します。初期値では、すべてのポートのすべてのキューに対し、このオプションが使用されます。 帯域幅に余裕がある場合でも、キューからの送信パケットは設定された最大帯域幅を超えることはありません。 本設定は物理ポートにのみ設定可能であり、ポートチャネルに対しては設定できません。

「Apply」ボタンをクリックして、設定内容を適用します。

Advanced Settings（アドバンス設定）

QoS の Advanced Settings（アドバンス設定）を行います。

DSCP Mutation Map（DSCP 変更マップ設定）

Differentiated Services Code Point (DSCP) 変更マップ設定を行います。
インタフェースでパケットを受信すると、QoS 関連の処理の前に、DSCP 変更マップに基づき受信 DSCP が他の DSCP に変更されます。DSCP 変更機能は、異なる DSCP 割り当てを持つドメインを統合する場合に役に立ちます。後続のすべての処理は変更 DSCP に基づいて行われます。

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

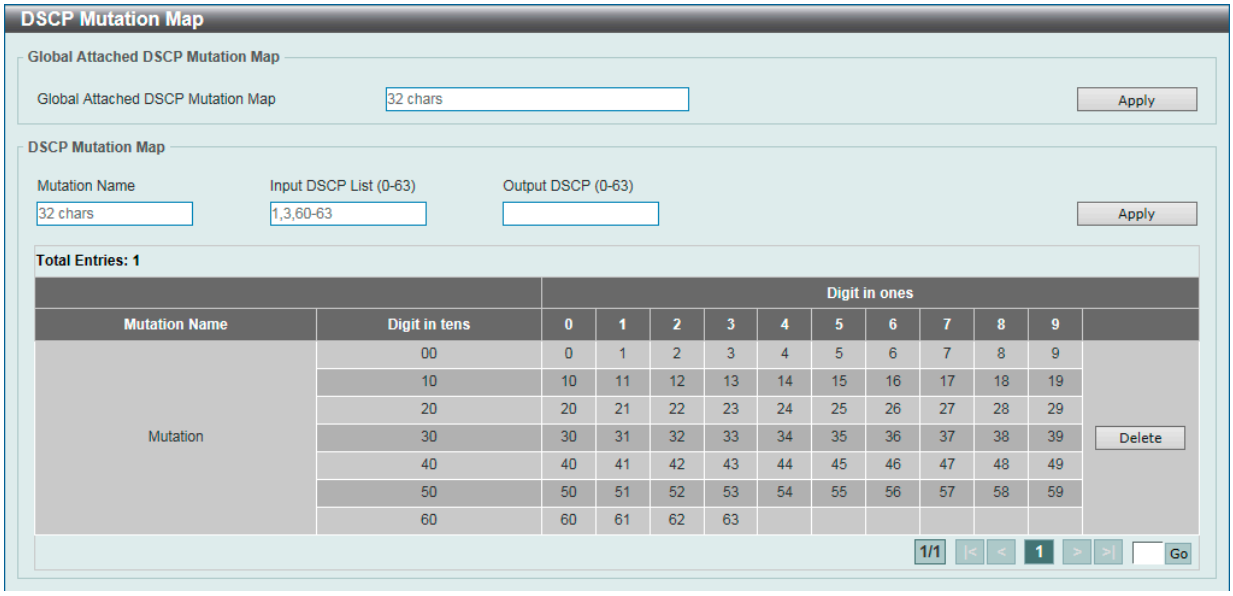


図 10-7　DSCP Mutation Map 画面

画面に表示される項目：

項目	説明
Global Attached DSCP Mutation Map	
Global Attached DSCP Mutation Map	グローバル DSCP 変更マップ名を指定します。（32 文字以内）
DSCP Mutation Map	
Mutation Name	DSCP 変更マップ名を指定します。（32 文字以内）
Input DSCP List	インプット DSCP リストの値を入力します。 • 設定可能範囲：0-63
Output DSCP	アウトプット DSCP リストの値を入力します。 • 設定可能範囲：0-63

「Apply」ボタンをクリックし、各項目の変更を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
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。

Port Trust State（ポートトラスト設定）

ポートトラスト設定を行います。

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

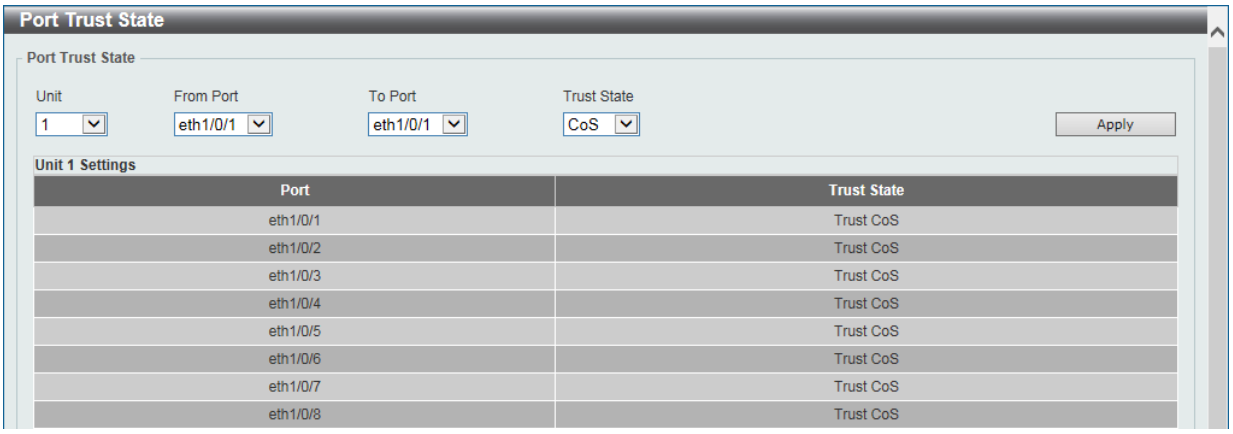


図 10-8　Port Trust State 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Trust State	ポートトラストのオプションを指定します。 • 選択肢：「CoS」「DSCP」

「Apply」ボタンをクリックして、設定内容を適用します。

DSCP CoS Mapping（DSCP CoS マップ設定）

DSCP CoS マップの設定と表示を行います。

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

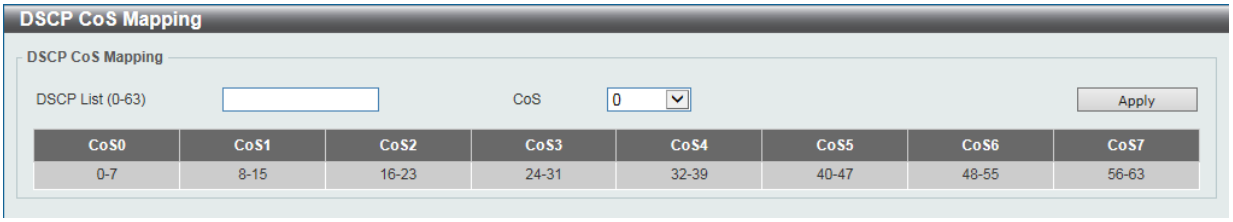


図 10-9　DSCP CoS Mapping 画面

画面に表示される項目：

項目	説明
DSCP List	CoS 値にマッピングする DSCP リストの値を入力します。 • 設定可能範囲：0-63
CoS	DSCP リストにマッピングする CoS 値を指定します。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。

CoS Color Mapping（CoS カラーマップ設定）

CoS カラーマップの設定と表示を行います。

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

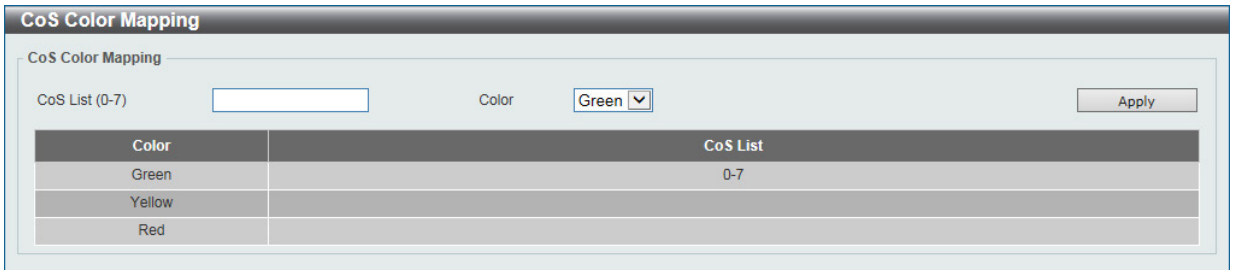


図 10-10　CoS Color Mapping 画面

画面に表示される項目：

項目	説明
CoS List	カラーにマッピングされる CoS 値を指定します。 • 設定可能範囲：0-7
Color	CoS 値にマッピングされるカラーを指定します。 • 選択肢：「Green」「Yellow」「Red」

「Apply」ボタンをクリックして、設定内容を適用します。

DSCP Color Mapping（DSCP カラーマップ設定）

DSCP カラーマップの設定と表示を行います。

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

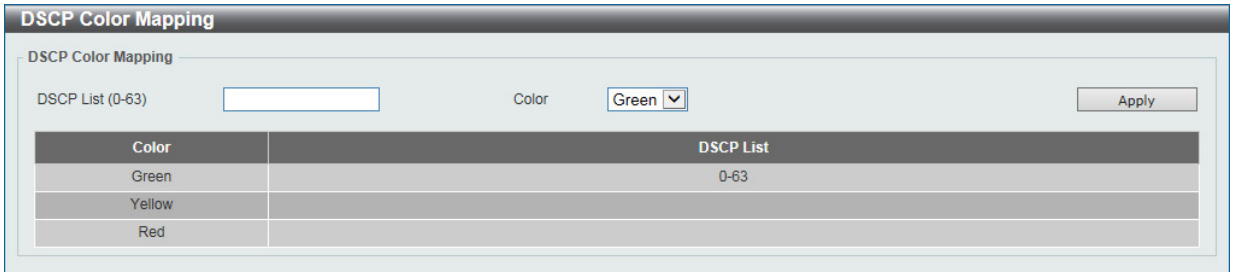


図 10-11　DSCP Color Mapping 画面

画面に表示される項目：

項目	説明
DSCP List	カラーにマッピングされる DSCP リストを指定します。 • 設定可能範囲：0-63
Color	DSCP 値にマッピングされるカラーを指定します。 • 選択肢：「Green」「Yellow」「Red」

「Apply」ボタンをクリックして、設定内容を適用します。

Class Map（クラスマップ設定）

クラスマップの設定と表示を行います。

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

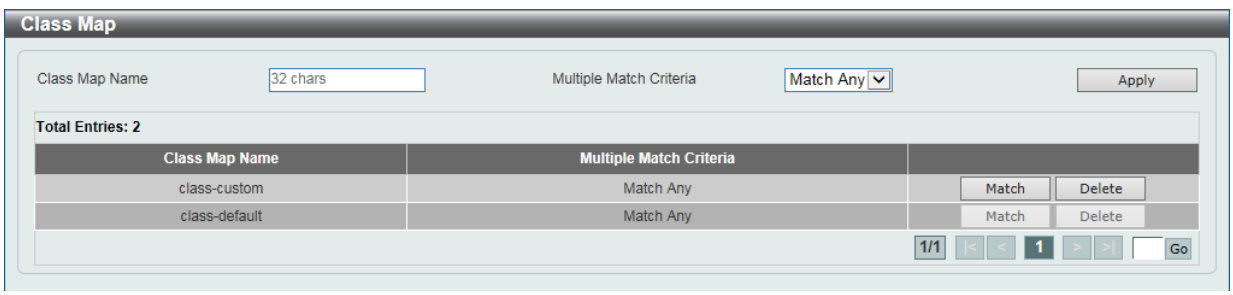


図 10-12　Class Map 画面

画面に表示される項目：

項目	説明
Class Map Name	クラスマップ名を指定します。（32 文字以内）
Multiple Match Criteria	一致条件の種類を指定します。 • 選択肢：「Match All（すべて一致）」「Match Any（いずれかに一致）」

「Apply」ボタンをクリックして、設定内容を適用します。
「Match」ボタンをクリックして、指定のエントリを設定します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

「Match」ボタンをクリックすると、以下の画面が表示されます。

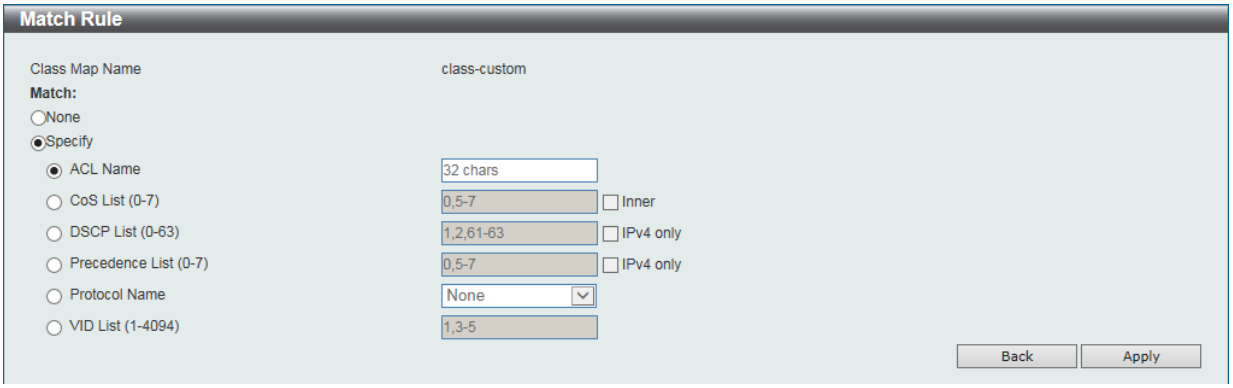


図 10-13　Class Map（Match）- Match Rule 画面

画面に表示される項目：

項目	説明
None	このクラスマップでは照合を行いません。
Specify	このクラスマップでは下記のいずれかのオプションで照合を行います。 • 「ACL Name」- クラスマップで照合するアクセスリスト名を指定します。（32 文字以内） • 「CoS List」- クラスマップで照合する CoS リスト値を指定します。「Inner」を指定すると、レイヤ 2 CoS マーキングの QinQ パケット内のインナーモースト CoS を照合します。 - 設定可能範囲：0-7 • 「DSCP List」- クラスマップで照合する DSCP リスト値を指定します。「IPv4 only」にチェックを入れると、IPv4 パケットのみ照合します。チェックを入れない場合、IPv4/v6 両方のパケットを照合します。 - 設定可能範囲：0-63 • 「Precedence List」- クラスマップで照合する Precedence リスト値を指定します。「IPv4 only」にチェックを入れると、IPv4 パケットのみ照合します。チェックを入れない場合、IPv4/v6 両方のパケットを照合します。IPv6 パケットの場合、IPv6 ヘッダに含まれるトラフィッククラスの上位 3 ビットが Precedence になります。 - 設定可能範囲：0-7 • 「Protocol Name」- クラスマップで照合するプロトコル名を指定します。 - 選択肢：「None」「ARP」「BGP」「DHCP」「DNS」「EGP」「FTP」「IPv4」「IPv6」「NetBIOS」「NFS」「NTP」「OSPF」「PPPOE」「RIP」「RTSP」「SSH」「Telnet」「TFTP」 • 「VID List」- クラスマップで照合する VLAN リスト値を指定します。 - 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Aggregate Policer（集約ポリサー設定）

集約ポリサーの設定と表示を行います。

Single Rate Settings タブ

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

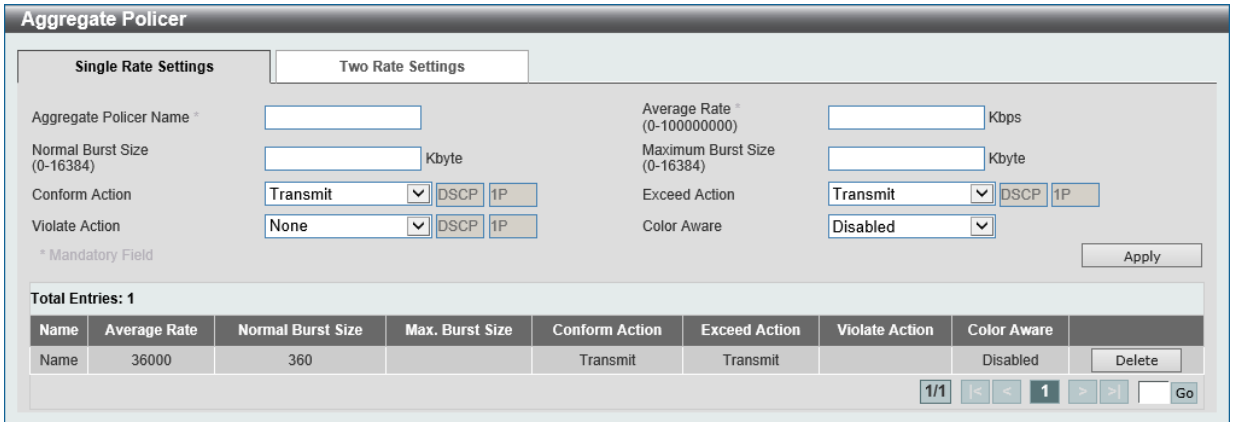


図 10-14　Aggregate Policer 画面 - Single Rate Settings タブ

画面に表示される項目：

項目	説明
Aggregate Policer Name	集約ポリサー名を入力します。
Average Rate	平均レート値を入力します。 • 設定可能範囲：0-10000000（kbps）
Normal Burst Size	ノーマルバーストサイズを入力します。 • 設定可能範囲：0-16384（Kbytes）
Maximum Burst Size	最大バーストサイズを入力します。 • 設定可能範囲：0-16384（Kbytes）
Confirm Action	緑色パケットに対するアクションを指定します。 •「Drop」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p 値でパケットを送信します。 •「Transmit」- パケットはそのまま送信されます。（初期値） •「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Exceed Action	レート制限を超えたパケットに対するアクションを指定します。 •「Drop」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p 値でパケットを送信します。 •「Transmit」- パケットはそのまま送信されます。 •「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Violate Action	シングルレートポリシングでは、ノーマルおよび最大バーストサイズを超えたパケットに対するアクションを指定します。 2 レートポリシングでは、「CIR」や「PIR」を順守しないパケットの動作を指定します。 •「None」- アクションは実行されません。 •「Drop」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（ DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p 値でパケットを送信します。 •「Transmit」- パケットはそのまま送信されます。 •「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。 シングルレートのポリサーの場合、初期値ではシングルレート 2 色ポリサーが作成されます。 2 レートポリサーの場合、初期値では「破棄」オプションが適用され、パケットは破棄されます。
Color Aware	Color Aware オプションを有効 / 無効に指定します。 •「Enabled」- ポリサーは Color-Aware モードで動作します。 •「Disabled」- ポリサーは Color-Blind モードで動作します。

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

Two Rate Settings タブ

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

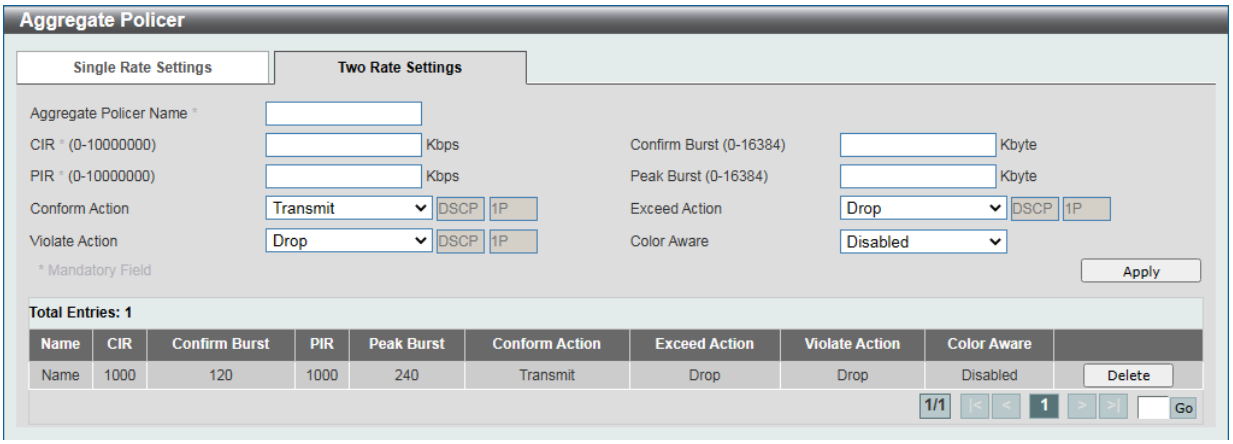


図 10-15　Aggregate Policer 画面 - Two Rate Settings タブ

画面に表示される項目：

項目	説明
Aggregate Policer Name	集約ポリサー名を入力します。
CIR	CIR（Committed Information Rate）値を入力します。 • 設定可能範囲：0-10000000（ kbps） この保証パケットレートは、２レートメータリングにおける最初のトークンバケットになります。
Confirm Burst	バーストサイズを入力します。 • 設定可能範囲：0-16384（Kbytes） Confirm Burst は、最初のトークンバケットのバーストサイズ（kbps）になります。
PIR	PIR（Peak Information Rate）値を入力します。 • 設定可能範囲：0-10000000（kbps） PIR は、２レートメータリングにおける二つ目のトークンバケットになります。
Peak Burst	ピークバースト値を入力します。 • 設定可能範囲：0-16384（Kbytes） ピークバーストサイズは、二つ目のトークンバケットのバーストサイズになります。
Confirm Action	緑色パケットに対するアクションを指定します。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。（初期値） • 「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Exceed Action	レート制限を超えたパケットに対するアクションを指定します。 • 「Drop」- パケットを破棄します。（初期値） • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。 ２レートポリサーの場合、初期値では「破棄」オプションが適用され、パケットは破棄されます。
Violate Action	シングルレートポリシングでは、ノーマルおよび最大バーストサイズを超えたパケットに対するアクションを指定します。 2 レートポリシングでは、「CIR」や「PIR」を順守しないパケットの動作を指定します。 • 「Drop」- パケットを破棄します。（初期値） • 「Set-DSCP-Transmit」- IP differentiated services code points（ DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。 シングルレートのポリサーの場合、初期値ではシングルレート２色ポリサーが作成されます。 ２レートポリサーの場合、初期値では「破棄」オプションが適用され、パケットは破棄されます。

項目	説明
Color Aware	Color Aware オプションを有効 / 無効に指定します。 • 「Enabled」- ポリサーは Color-Aware モードで動作します。 • 「Disabled」- ポリサーは Color-Blind モードで動作します。

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

Policy Map（ポリシーマップ設定）

ポリシーマップの設定と表示を行います。

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

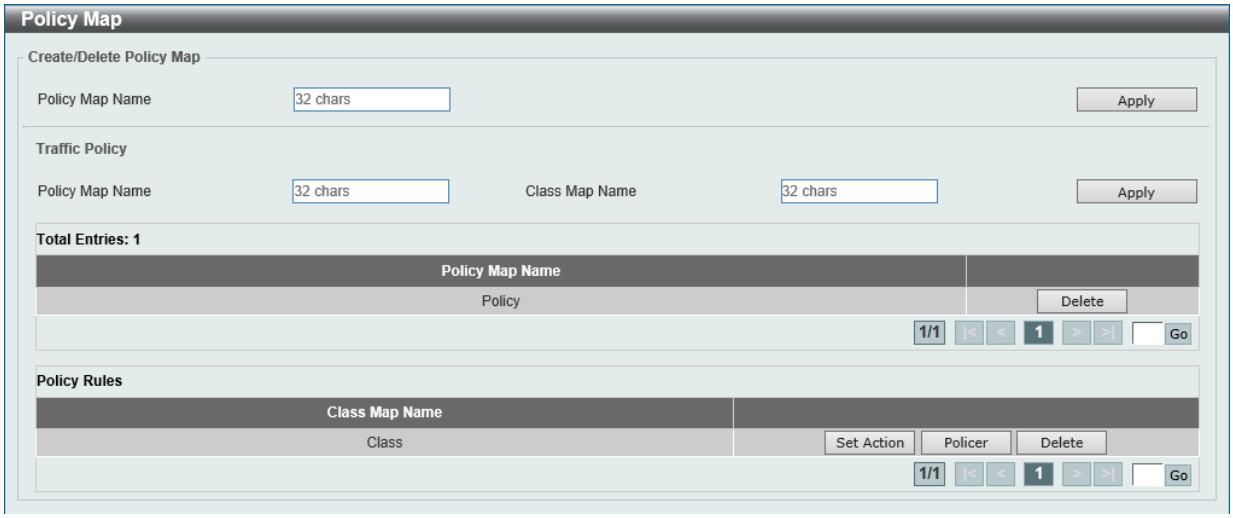


図 10-16　Policy Map 画面

画面に表示される項目：

項目	説明
Create/Delete Policy Map	
Policy Map Name	作成 / 削除するポリシーマップ名を指定します。（32 文字以内）
Traffic Policy	
Policy Map Name	ポリシーマップ名を指定します。（32 文字以内）
Class Map Name	クラスマップ名を指定します。（32 文字以内）

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

Class Map の編集

テーブル上のエントリを選択後、「Set Action」ボタンをクリックして、アクション設定を行います。
テーブル上のエントリを選択後、「Policer」ボタンをクリックして、ポリサー設定を行います。

ポリシーマップのエントリをクリックし、画面下部に表示されるクラスマップの「Set Action」ボタンをクリックします。以下の画面が表示されます。

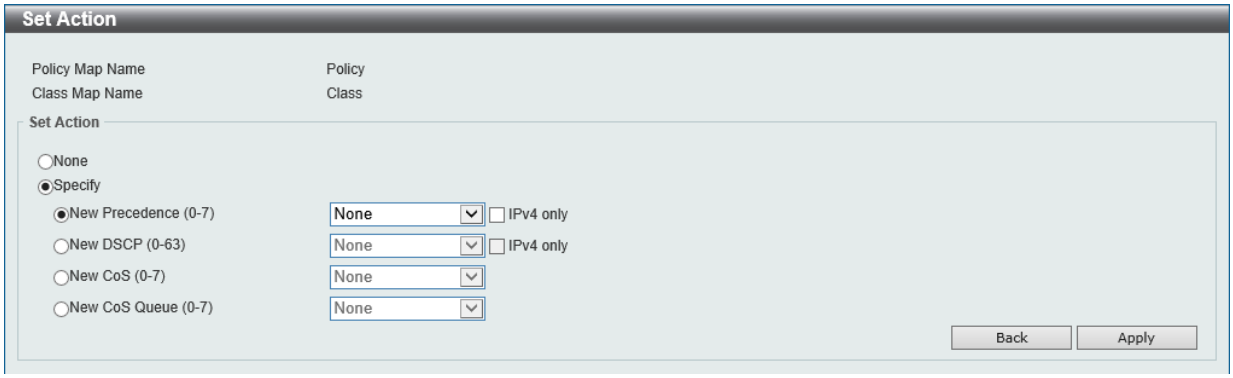


図 10-17　Policy Map（Set Action）- Set Action 画面

画面に表示される項目：

項目	説明	
None	アクションを実行しません。	
Specify	設定に基づきアクションを実行します。	
	New Precedence	新しい Precedence 値を選択します。 「IPv4 only」にチェックを入れると、IPv4 Precedence のみマークされます。チェックを入れない場合、IPv4/v6 両方の Precedence がマークされます。IPv6 パケットの場合、IPv6 ヘッダに含まれるトラフィッククラスの上位 3 ビットが Precedence になります。Precedence の設定は CoS キュー選択には影響しません。 • 選択肢：0-7
	New DSCP	パケットの新しい DSCP 値を指定します。 「IPv4 only」にチェックを入れると、IPv4 DSCP のみマークされます。チェックを入れない場合、IPv4/v6 両方の DSCP がマークされます。DSCP の設定は CoS キュー選択には影響しません。 • 選択肢：0-63
	New CoS	パケットの新しい CoS 値を指定します。入力インタフェースにポリシーマップが適用されている場合、CoS 値の設定は CoS キュー選択に影響します。 • 選択肢：0-7
	New CoS Queue	パケットの新しい CoS キュー値を指定します。元の CoS キュー選択は上書きされます。インタフェースの出力フローにポリシーマップが適用されている場合、CoS 値の設定は影響しません。 • 選択肢：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ポリシーマップのエントリをクリックし、画面下部に表示されるクラスマップの「Policer」ボタンをクリックします。以下の画面が表示されます。

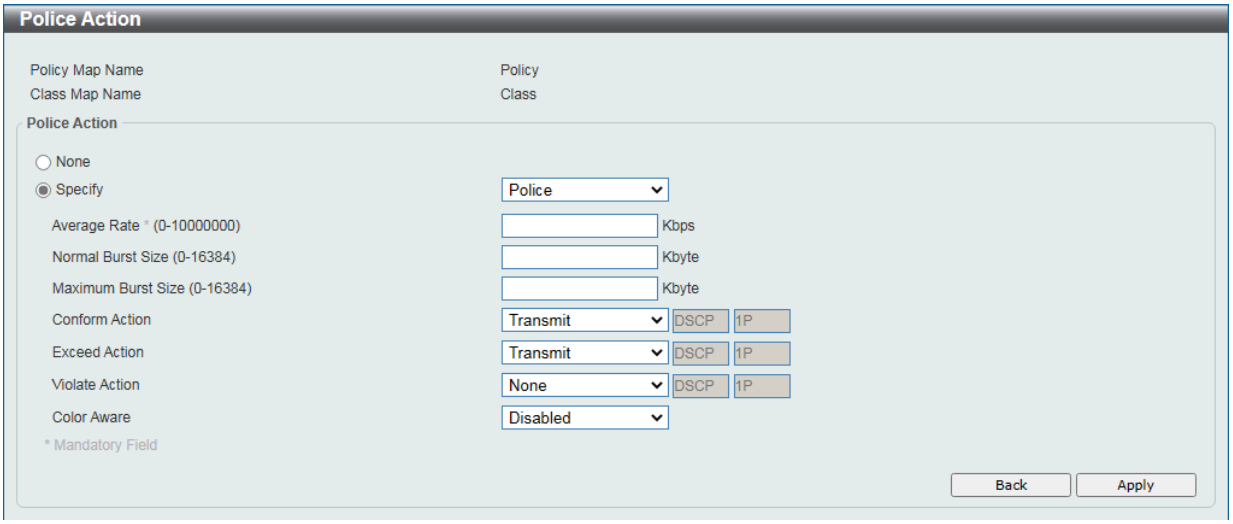


図 10-18　Policy Map（Policer）- Police Action 画面

画面に表示される項目：

項目	説明	
None	このエントリにポリサー設定を指定しない場合に選択します。	
Specify	このエントリにポリサー設定を指定する場合に選択します。 • 選択肢：「Police」「Police CIR」「Police Aggregate」	
	「Police」を選択した場合にのみ表示される項目	
	Average Rate	平均レート値を入力します。 • 設定可能範囲：0-10000000（Kbps）
	Normal Burst Size	ノーマルバーストサイズを入力します。 • 設定可能範囲：0-16384（Kbyte）
	Maximum Burst Size	最大バーストサイズを入力します。 • 設定可能範囲：0-16384（Kbyte）
	「Police CIR」を選択した場合にのみ表示される項目	
	CIR	CIR 値を入力します。
	Confirm Burst	バーストサイズを入力します。
	PIR	PIR 値を入力します。
	Peak Burst	ピークバーストサイズを入力します。

項目	説明	
	「Police」「Police CIR」を選択した場合に表示される項目	
	Confirm Action	適合パケットに対するアクションを指定します。緑色パケットに対してアクションが実行されます。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値 を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- DSCP と 802.1p 値を設定して、新しい DSCP と 802.1p 値でパケットを送信します。
	Exceed Action	超過パケットに対するアクションを指定します。黄色パケットに対してアクションが実行されます。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値 を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- DSCP と 802.1p 値を設定して、新しい DSCP と 802.1p 値でパケットを送信します。
	Violate Action	違反パケットに対するアクションを指定します。赤色パケットに対してアクションが実行されます。 • 「None」- アクションを実行しません。（「Police」選択時のみ指定可能） • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値 を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- DSCP と 802.1p 値を設定して、新しい DSCP と 802.1p 値でパケットを送信します。
	Color Aware	Color Aware オプションを有効 / 無効に指定します。 • 「Enabled」- ポリサーは Color-Aware モードで動作します。 • 「Disabled」- ポリサーは Color-Blind モードで動作します。
	「Police Aggregate」を選択した場合にのみ表示される項目	
	Aggregate Policer Name	集約ポリサー名を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

Policy Binding（ポリシーバインディング設定）

ポリシーバインディング設定を行います。

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

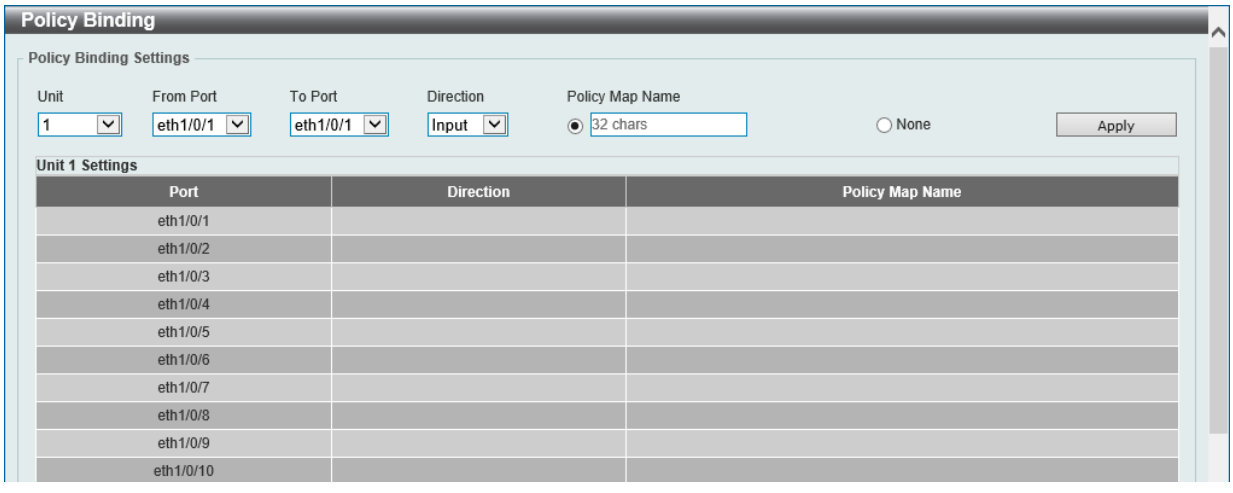


図 10-19　Policy Binding 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。

項目	説明
Direction	トラフィックの方向を指定します。 ・ 選択肢「Input（イングレス）」「Output（イーグレス）」
Policy Map Name	ポリシーマップ名を指定します。（32 文字以内）「None」を選択すると本エントリにポリシーマップは関連付けられません。

「Apply」ボタンをクリックして、設定内容を適用します。

第 11 章　ACL（ACL 機能の設定）

ACL メニューを使用し、本スイッチにアクセスプロファイルおよびルールの設定を行うことができます。

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

サブメニュー	説明
ACL Configuration Wizard（ACL 設定ウィザード）	ACL 設定ウィザードを使用して、アクセスプロファイルと ACL ルールの新規作成・更新を行います。
ACL Access List（ACL アクセスリスト）	ACL アクセスリストの設定を行います。
ACL Interface Access Group（ACL インタフェースアクセスグループ）	ACL インタフェースアクセスグループの設定を行います。
ACL VLAN Access Map（ACL VLAN アクセスマップ）	ACL VLAN アクセスマップの設定を行います。
ACL VLAN Filter（ACL VLAN フィルタ設定）	ACL VLAN フィルタの設定を行います。
CPU ACL（CPU ACL 設定）	CPU インタフェースフィルタリング機能の設定を行います。

ACL の利用可能なエントリ数は以下の通りです。
実際に作成可能な ACL ルール数は、消費する HW エントリや他の機能の利用状況に依存します。

- Ingress ACL：2048 HW エントリ
  - システムで使用：256 HW エントリ
  - ユーザ作成可能分および他の機能で使用：1792 HW エントリ（共有プール）

■ ユーザ作成可能な ACL

ACL の種類	1ACL あたりの消費 HW エントリ数
MAC ACL	2
IP ACL	2
IPv6 ACL	4
Expert ACL	2
UDF ACL	2

■ IPSG/IPv6SG 機能

機能	IPSG あたりの消費 HW エントリ数
IPSG	2
IPv6SG	2

■ 802.1X/WAC/MAC/Compound 認証

機能	消費 HW エントリ数
認証のみ	認証のみの場合、ACL エントリは消費されません。
ホストベース認証を使用し、異なる VLAN への割り当てが設定されている場合	認証ごとに 6 エントリ消費されます。
ホストベース認証を使用し、ACL 割り当てが設定されている場合	割り当て ACL に基づき HW エントリが消費されます。

ACL Configuration Wizard（ACL 設定ウィザード）

ウィザードを使用してアクセスプロファイルとルールを作成・更新します。

手順 1：アクセスリストのアサイン（ACL 設定ウィザード）

アクセスプロファイルと ACL ルールの新規作成または更新を行います。

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

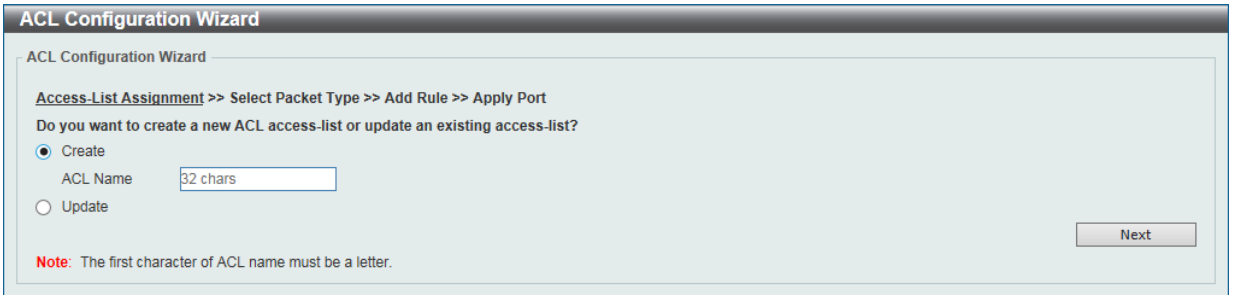


図 11-1　ACL Configuration Wizard（Access-List Assignment - Create) 画面

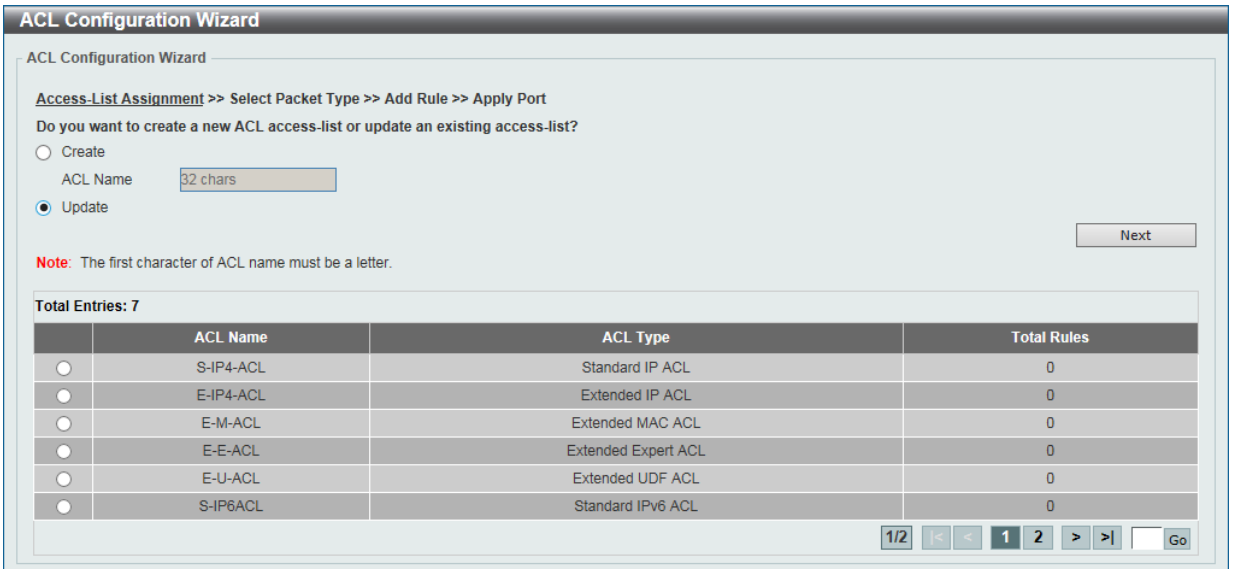


図 11-2　ACL Configuration Wizard（Access-List Assignment - Update) 画面

画面に表示される項目：

項目	説明
Create	新しいアクセスリストを作成する場合は、「Create」を選択します。
ACL Name	作成する ACL 名を指定します。（32 文字以内）
Update	既存の ACL アクセスリストを表示し、エントリを再設定する場合に選択します。

「Next」ボタンをクリックし、パケットタイプの選択を行います。

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。

手順 2：パケットタイプ選択（ACL 設定ウィザード）

「ACL Configuration Wizard」にて新規アクセスリストを作成する場合、以下の画面でパケットタイプを指定します。

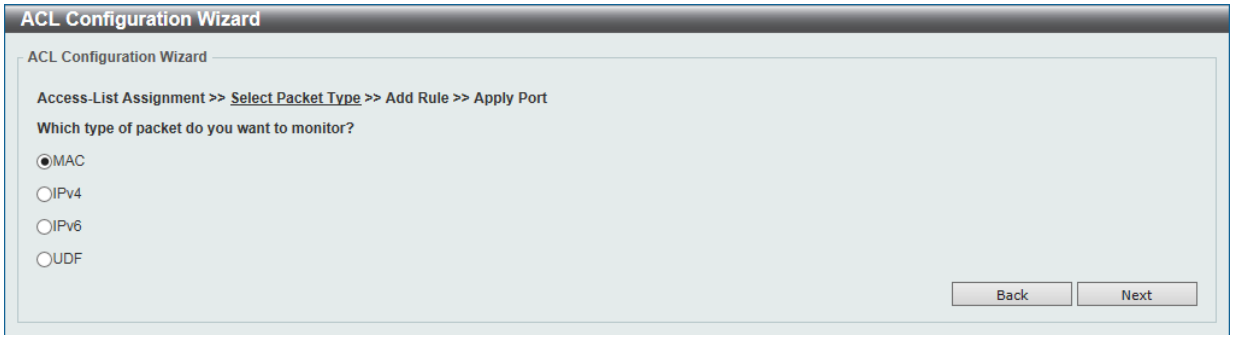


図 11-3　ACL Configuration Wizard（Select Packet Type) 画面

画面に表示される項目：

項目	説明
MAC	MAC ACL を作成します。
IPv4	IPv4 ACL を作成します。
IPv6	IPv6 ACL を作成します。
UDF	UDF ACL を作成します。

「Next」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。

手順 3：ルール追加（ACL 設定ウィザード）

選択したパケットの種類に応じて、ACL エントリにおける ACL ルールの追加設定を行います。

- MAC ACL ルールの設定内容については「MAC ACL の設定」を参照してください。
- IPv4 ACL ルールの設定内容については「Extended/Standard IPv4 ACL の設定」を参照してください。
- IPv6 ACL ルールの設定内容については「Extended/Standard IPv6 ACL の設定」を参照してください。
- UDF ACL ルールの設定内容については「Extended UDF ACL の設定」を参照してください。
- Expert ACL ルールの設定内容については「Extended Expert ACL の設定」を参照してください。

MAC ACL の設定

「ACL Configuration Wizard」にて MAC ACL ルールを作成・更新する場合、以下の画面が表示されます。

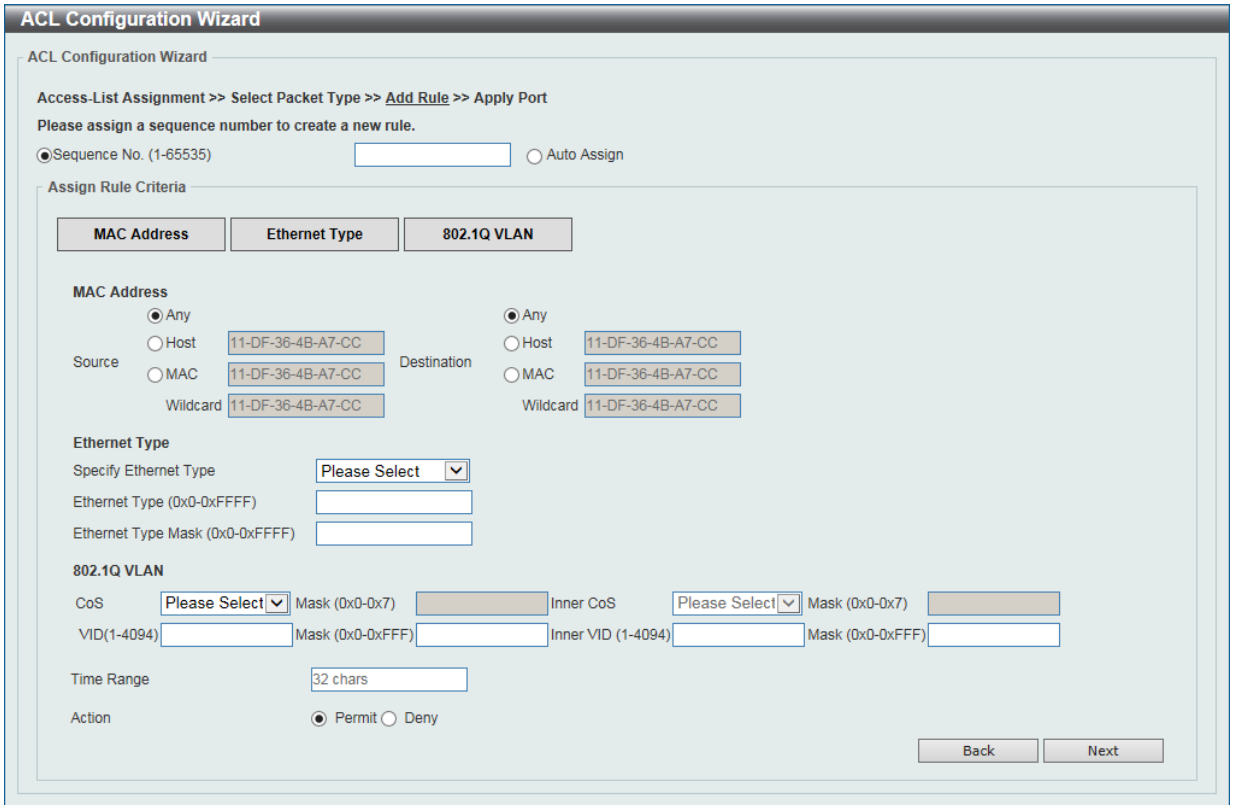


図 11-4　ACL Configuration Wizard 画面（Extended MAC ACL）

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	ACL ルールのシーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Assign Rule Criteria（ルール条件の割り当て）	
MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力することができます。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
Ethernet Type	
Specify Ethernet Type	イーサネットタイプを選択します。 • 選択肢:「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
Ethernet Type	イーサネットタイプの 16 進数値を指定します。 「Specify Ethernet Type」で指定したイーサネットタイプに基づき、自動的に適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。 「Specify Ethernet Type」で指定したイーサネットタイプに基づき、自動的に適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
802.1Q VLAN	
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 •「Mask」：CoS マスクを入力します。（0x0-0x7）
Inner CoS	CoS 値を指定後、Inner CoS の値を入力します。 • 設定可能範囲：0-7 •「Mask」：Inner CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 •「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）
Inner VID	ACL ルールに紐づける Inner VLAN ID を入力します。 • 設定可能範囲：1-4094 •「Mask」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」

「Next」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。

Extended/Standard IPv4 ACL の設定

「ACL Configuration Wizard」にて Extended/Standard IPv4 ACL ルールを作成・更新する場合、以下の画面が表示されます。

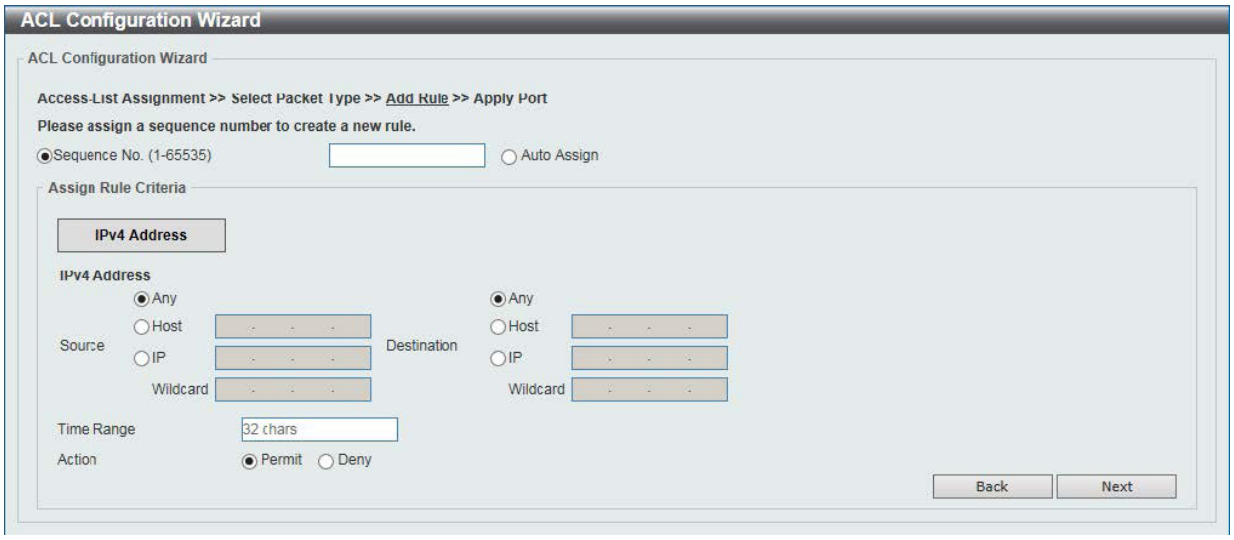


図 11-5　ACL Configuration Wizard 画面（Standard IP ACL/ 更新時）

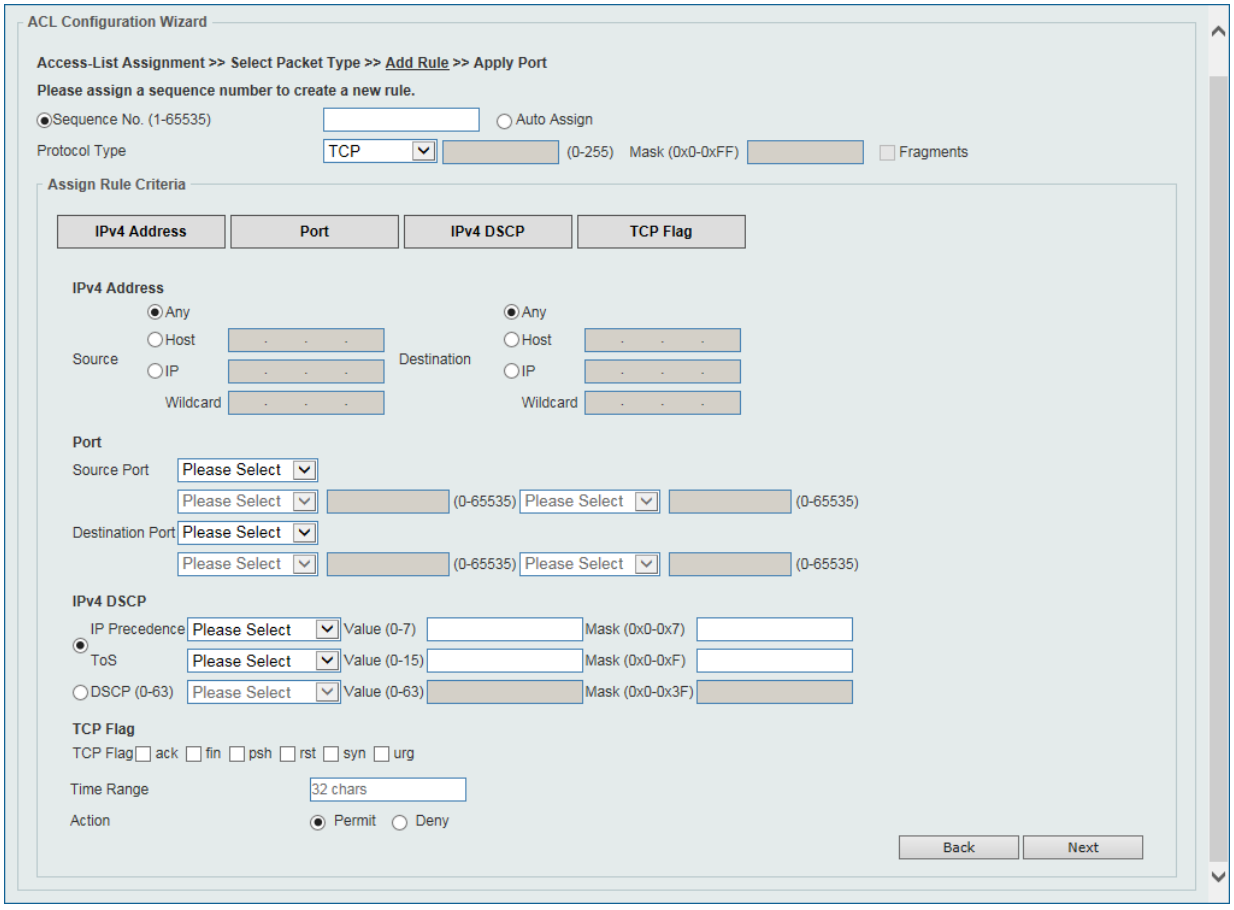


図 11-6　ACL Configuration Wizard 画面（Extended IP ACL）

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	ACL ルールのシーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Protocol Type（プロトコルタイプ）	
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

項目	説明
IPv4 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Port	
Source Port	【TCP/UDP を選択時に表示】 送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】 宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「routine（0）」「priority（1）」「immediate（2）」「flash（3）」「flash-override（4）」「critical（5）」「internet（6）」「network（7）」 - 「Value」：IP 優先値を入力します。（0-7） - 「Mask」：IP 優先値マスクを入力します。（0x0-0x7）

項目	説明
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢:「normal（0）」「min-monetary-cost（1）」「max-reliability（2）」「max-throughput（4）」「min-delay（8）」 - 「Value」：ToS 値を入力します。（0-15） - 「Mask」：ToS マスクを入力します。（0x0-0xF）
DSCP	使用する DSCP 値を選択します。 • 選択肢:「default（0）」「af11（10）」「af12（12）」「af13（14）」「af21（18）」「af22（20）」「af23（22）」「af31（26）」「af32（28）」「af33（30）」「af41（34）」「af42（36）」「af43（38）」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。（0-63） - 「Mask」：DSCP マスクを入力します。（0x0-0x3F）
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」

「Next」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。

Extended/Standard IPv6 ACL の設定

「ACL Configuration Wizard」にて Extended/Standard IPv6 ACL ルールを作成・更新する場合、以下の画面が表示されます。

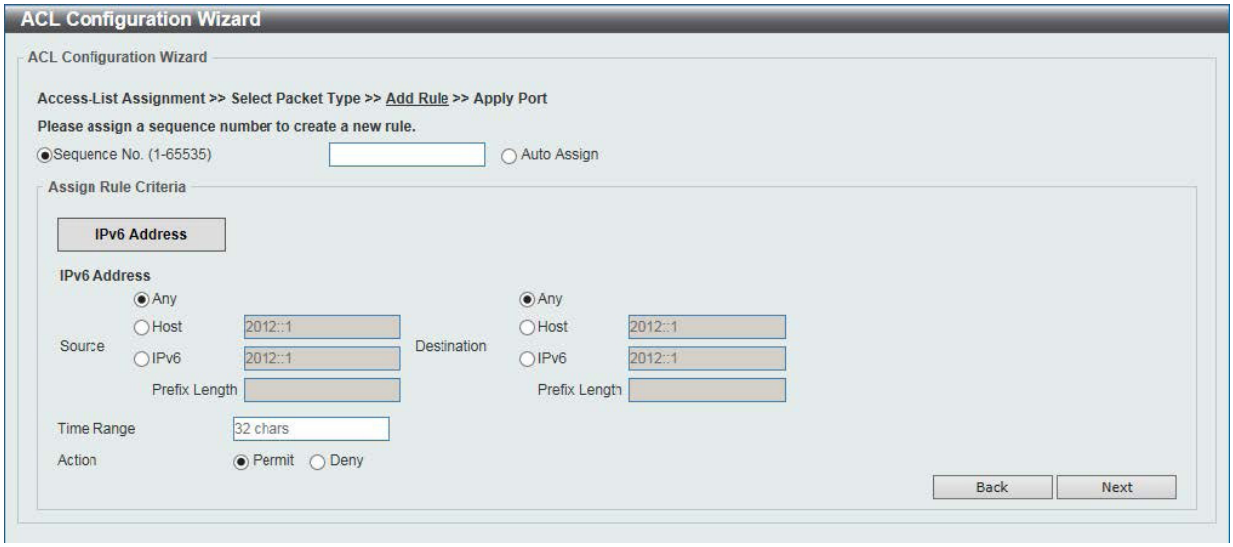


図 11-7　ACL Configuration Wizard 画面（Standard IPv6 ACL/ 更新時）

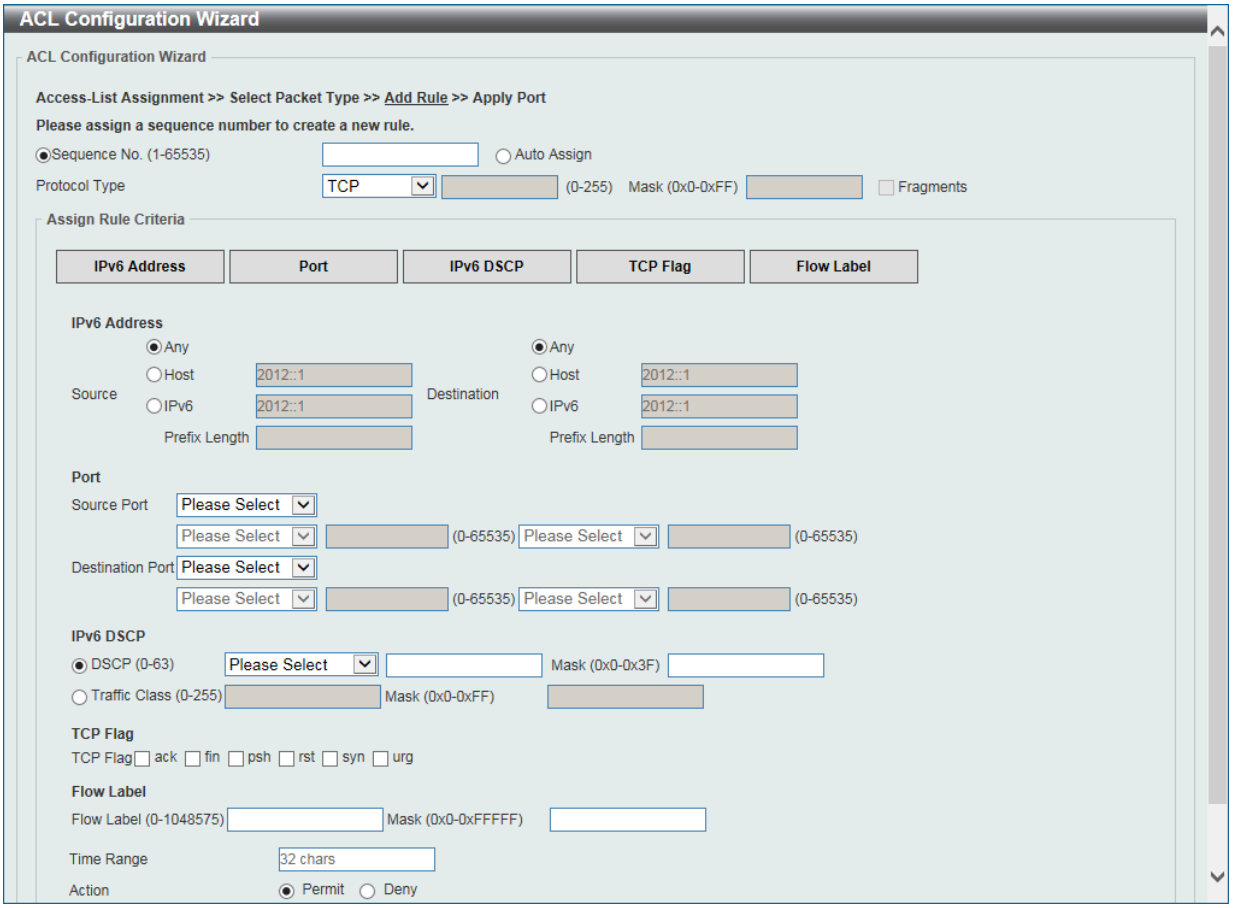


図 11-8　ACL Configuration Wizard 画面（Extended IPv6 ACL）

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Protocol Type（プロトコルタイプ）	
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「Protocol ID」「ESP」「RCP」「SCTP」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

項目	説明
IPv6 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。

項目	説明
Port	
Source Port	【TCP/UDP を選択時に表示】 送信元ポートの値を指定します。 ・「=」- 指定のポート番号が使用されます。 ・「>」- 指定ポートよりも大きいポートが使用されます。 ・「<」- 指定ポートより小さいポートが使用されます。 ・「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 ・「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】 宛先ポートの値を指定します。 ・「=」- 指定のポート番号が使用されます。 ・「>」- 指定ポートよりも大きいポートが使用されます。 ・「<」- 指定ポートより小さいポートが使用されます。 ・「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 ・「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 ・ 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 ・ 設定可能範囲：0-255
IPv6 DSCP	
DSCP	使用する DSCP 値を選択します。 ・ 選択肢：「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。（0-63） - 「Mask」：DSCP マスクを入力します。（0x0-0x3F）
Traffic Class	トラフィッククラス値とトラフィッククラスのマスク値を入力します。 ・ 設定可能範囲：0-255 ・「Mask」：トラフィッククラスのマスクを入力します。（0x0-0xFF）
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 ・ 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Flow Label	
Flow Label	フローラベルの値を入力します。 ・ 設定可能範囲：0-1048575 ・「Mask」：フローラベルマスクを入力します。（0x0-0xFFFFF）
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 ・ 選択肢：「Permit（許可）」「Deny（拒否）」

「Next」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。

Extended UDF ACL の設定

「ACL Configuration Wizard」にて Extended UDF ACL ルールを作成・更新する場合、以下の画面が表示されます。

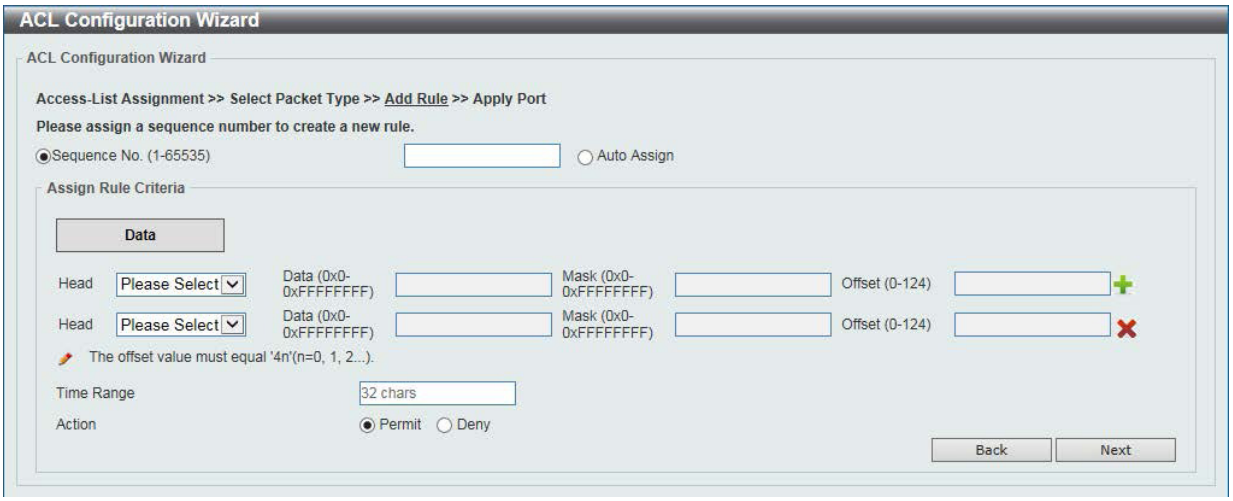


図 11-9　ACL Configuration Wizard（Extended UDF）画面

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
ルール基準を割り当て	
データ	
Head	ヘッダで設定されるオフセット値を選択します。 • 選択肢：「L2」「L3」「L4」
Data	パケットのコンテンツに一致する UDF フィールドを入力します。 •「Mask」：データマスクを入力します。ビットは 0 の値が無視され、1 が認識されます。（0x0-0xFFFFFFFF）
Offset	ヘッダで設定されるオフセット値を指定します。 •「L2」の場合、L2 ヘッダから開始されるオフセットを指定します。 •「L3」の場合、L3 ヘッダのマイナス 2Bytes から開始されるオフセットを指定します。 •「L4」の場合、L4 ヘッダから開始されるオフセットを指定します。
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」

「＋」ボタンをクリックして、データエントリを追加します。
「×」ボタンをクリックして、データエントリを削除します。
「Next」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。

Extended Expert ACL の設定

「ACL Configuration Wizard」にて Extended Expert ACL ルールを更新する場合、以下の画面が表示されます。

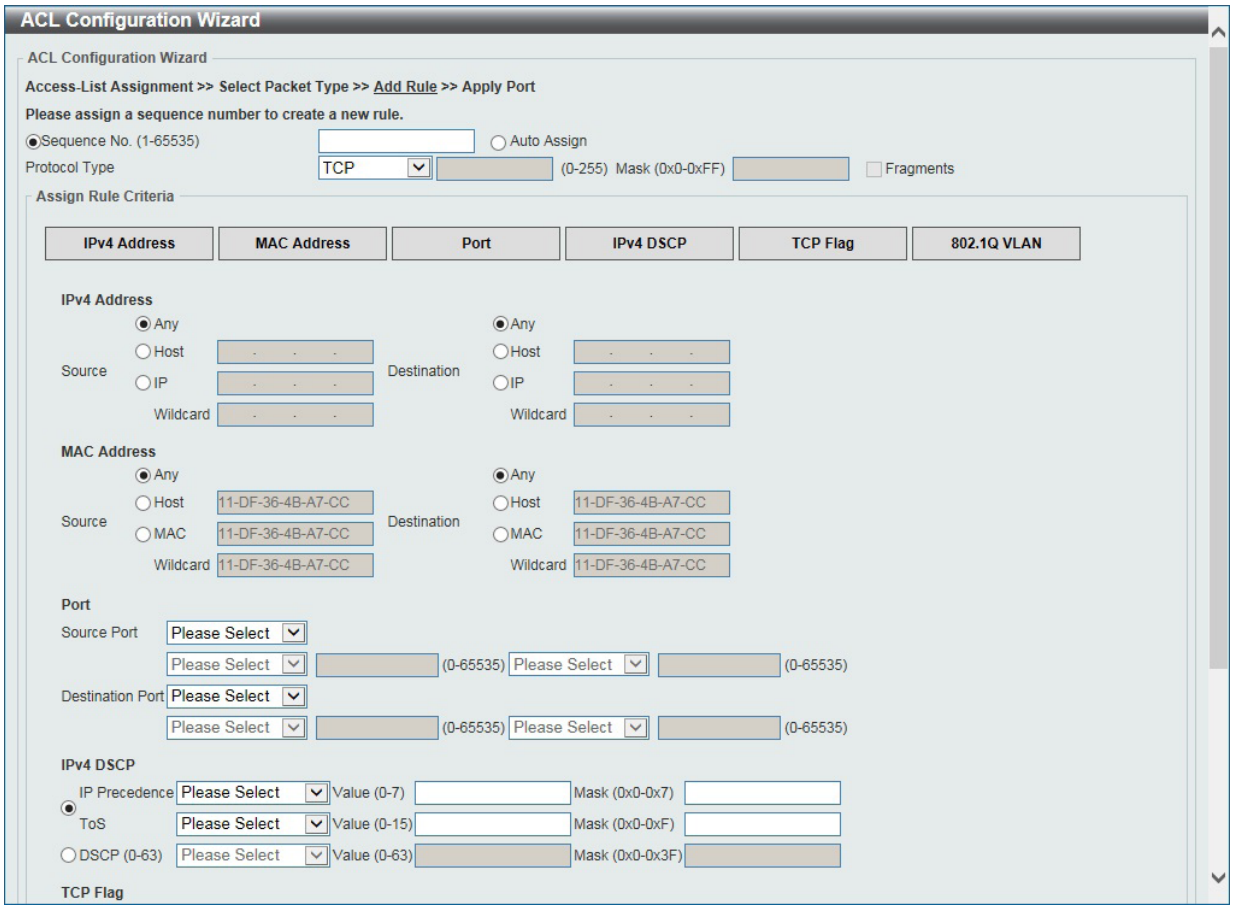


図 11-10　ACL Configuration Wizard（Extended Expert ACL/ 更新時）画面

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Protocol Type（プロトコルタイプ）	
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「 Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

項目	説明
IPv4 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。

項目	説明
MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「ホスト」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「ワイルドカード」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力できます。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「ホスト」- 宛先ホストの MAC アドレスを入力します。 • 「MAC」-「ワイルドカード」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力できます。
Port	
Source Port	【TCP/UDP を選択時に表示】 送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】 宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「routine（0）」「priority（1）」「immediate（2）」「flash（3）」「flash-override（4）」「critical（5）」「internet（6）」「network（7）」 - 「Value」：IP 優先値を入力します。（0-7） - 「Mask」：IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「normal（0）」「min-monetary-cost（1）」「max-reliability（2）」「max-throughput（4）」「min-delay（8）」 - 「Value」：ToS 値を入力します。（0-15） - 「Mask」：ToS マスクを入力します。（0x0-0xF）
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default（0）」「af11（10）」「af12（12）」「af13（14）」「af21（18）」「af22（20）」「af23（22）」「af31（26）」「af32（28）」「af33（30）」「af41（34）」「af42（36）」「af43（38）」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。（0-63） - 「Mask」：DSCP マスクを入力します。（0x0-0x3F）
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

項目	説明
802.1Q VLAN	
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 •「Mask」：CoS マスクを入力します。（0x0-0x7）
Inner CoS	CoS 値を指定後、Inner CoS の値を入力します。 • 設定可能範囲：0-7 •「Mask」：Inner CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 •「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）
Inner VID	ACL ルールに紐づける Inner VLAN ID を入力します。 • 設定可能範囲：1-4094 •「Mask」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」

「Next」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。

手順 4：ポート設定（ACL 設定ウィザード）

「ACL Configuration Wizard」にて適用するポートの設定を行います。

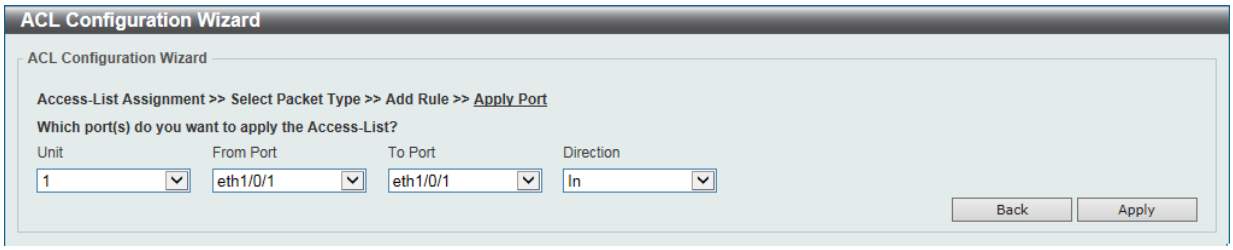


図 11-11　ACL Configuration Wizard (Apply Port) 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Direction	方向を指定します。 • 選択肢：「In」「Out」

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL Access List（ACL アクセスリスト）

アクセスコントロールリスト、ACL ルールの設定、表示を行います。

ACL > ACL Access 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。

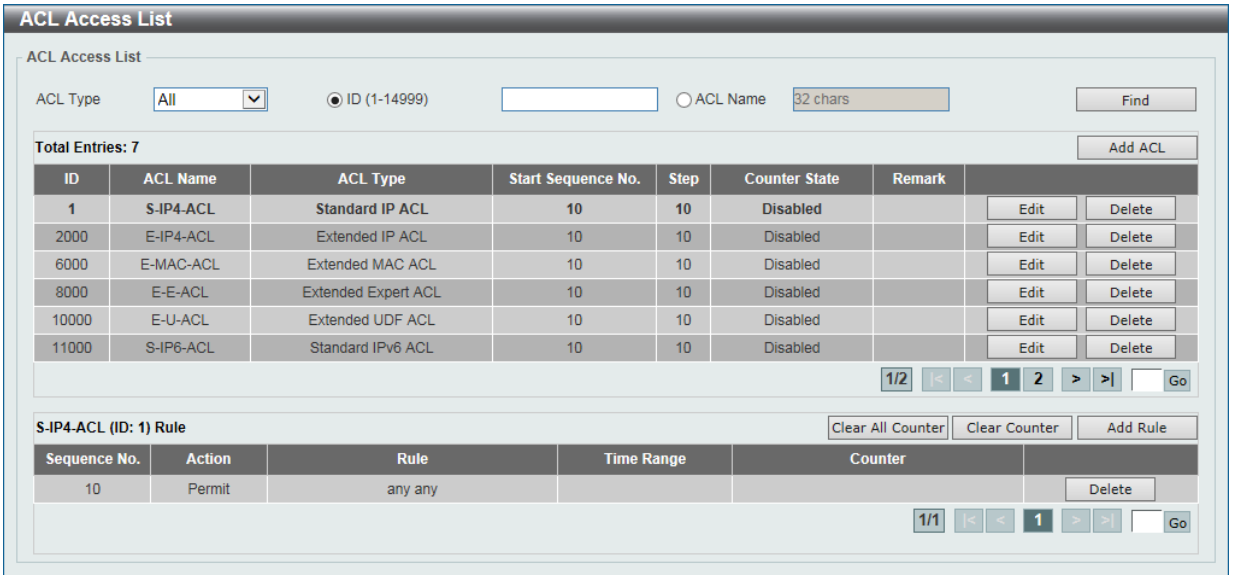


図 11-12　ACL Access List 画面

画面に表示される項目：

項目	説明
ACL Type	ACL プロファイルの種類を選択します。 • 選択肢：「All」「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」「UDF ACL」
ID	ACL ID を入力します。 • 設定可能範囲：1-14999
ACL Name	ACL 名を入力します。（32 文字以内）

「Find」ボタンをクリックし、入力した情報を基にエントリを検索します。
「Add ACL」ボタンをクリックして、新しい ACL プロファイルを作成します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Delete」ボタンをクリックして、指定のエントリを削除します。

ACL ルールの作成・カウンタ情報の削除

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後、「Add Rule」ボタンをクリックします。
「Clear All Counter」ボタンをクリックして、表示されたすべてのカウンタ情報を消去します。
「Clear Counter」ボタンをクリックして、表示されたルールのカウンタ情報を消去します。

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。

「Edit」ボタンをクリックすると、以下のようにパラメータを編集できます。

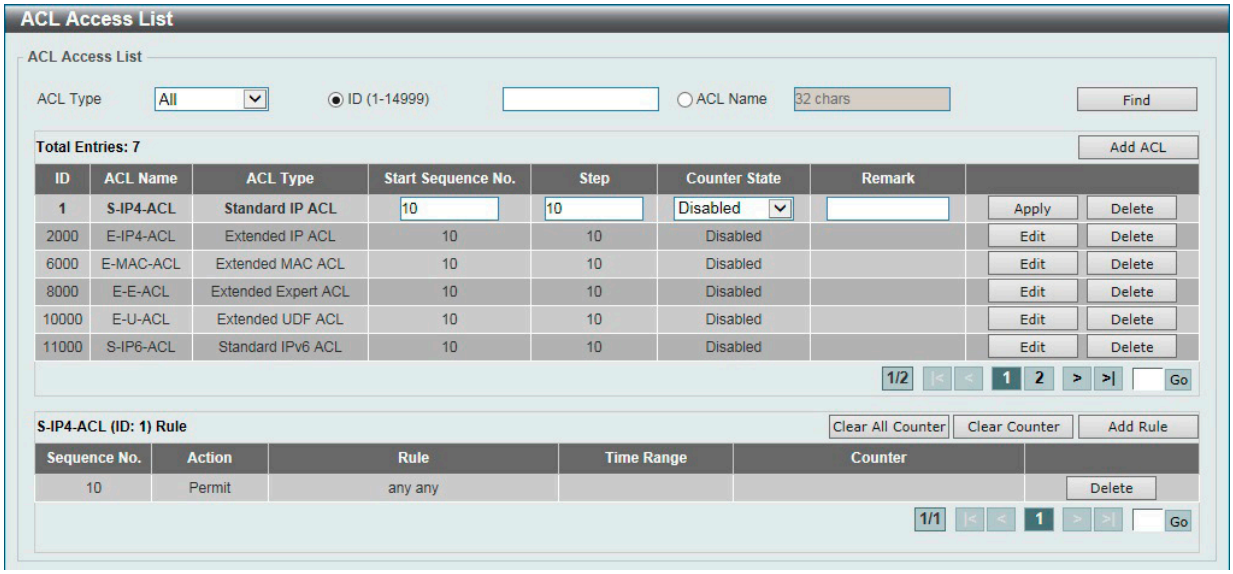


図 11-13　ACL Access List（Edit）画面

画面に表示される項目：

項目	説明
Start Sequence No.	シーケンスの開始番号を入力します。
Step	シーケンス番号のステップ（インクリメント）数を入力します。 たとえば、シーケンスの開始番号が 20、ステップ値が 5 の場合、後続のシーケンス番号は 25、30、35、40 となります。 • 設定可能範囲：1-32 • 初期値：10
Counter State	カウンタ状態オプションを有効 / 無効に設定します。
Remark	ACL のオプション注釈を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

ACL プロファイルの作成

「Add ACL」ボタンをクリックすると、以下の画面が表示されます。

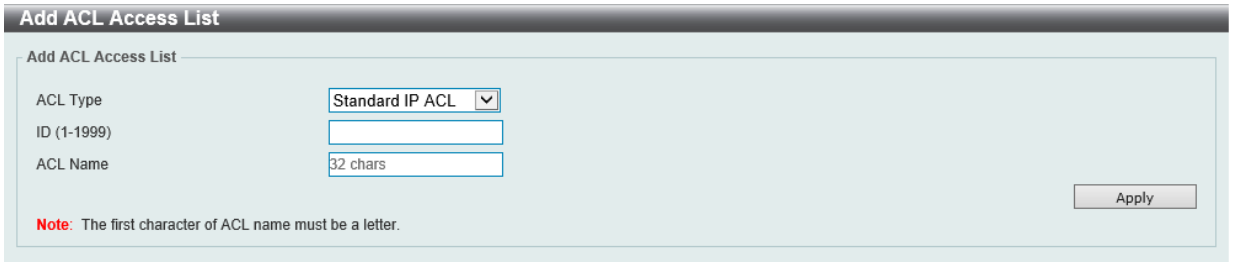


図 11-14　ACL Access List（Add ACL）- Add ACL Access List 画面

画面に表示される項目：

項目	説明
ACL Type	ACL プロファイルの種類を選択します。 • 選択肢:「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」「Extended UDF ACL」
ID	ACL ID を入力します。 • 設定可能範囲：（Standard IP ACL）1-1999 （Extended IP ACL）2000-3999 （Standard IPv6 ACL）11000-12999 （Extended IPv6 ACL）13000-14999 （Extended MAC ACL）6000-7999 （Extended Expert ACL）8000-9999 （Extended UDF ACL）10000-10999
ACL Name	ACL 名を入力します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

Add Rule（ACL ルールの追加）

ACL プロファイルにルールを追加します。
プロファイルの種類に応じて、以下の説明を参照してください。

- 「ACL ルールの追加（Add Rule）（Standard IP ACL）」
- 「ACL ルールの追加（Add Rule）（Extended IP ACL）」
- 「ACL ルールの追加（Add Rule）（Standard IPv6 ACL）」
- 「ACL ルールの追加（Add Rule）（Extended IPv6 ACL）」
- 「ACL ルールの追加（Add Rule）（Extended MAC ACL）」
- 「ACL ルールの追加（Add Rule）（Extended Expert ACL）」
- 「ACL ルールの追加（Add Rule）（Extended UDF ACL）」

ACL ルールの追加（Add Rule）（Standard IP ACL）

「ACL Access List」画面で「Standard IP ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

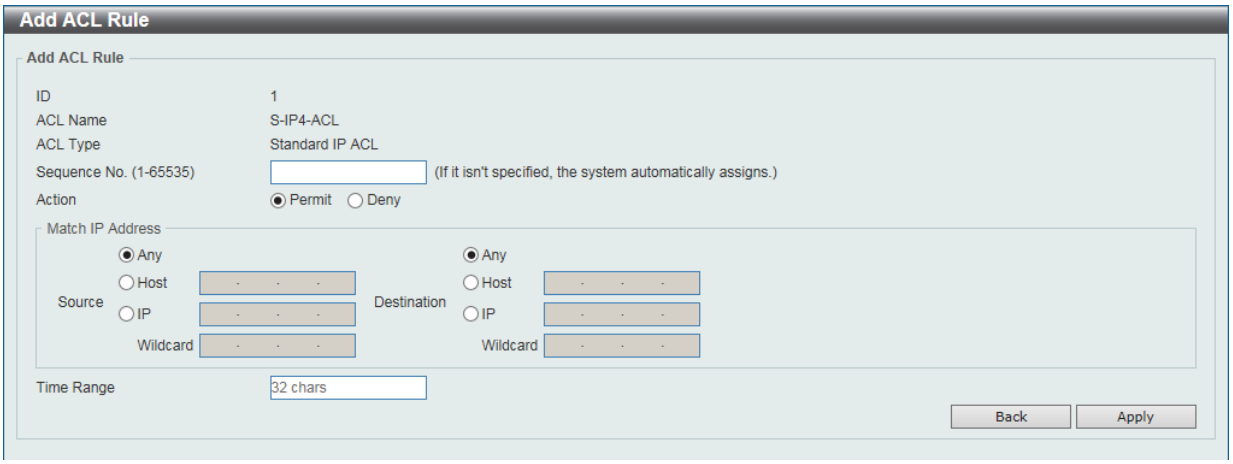


図 11-15　ACL Access List（Standard IP ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Match IP Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended IP ACL）

「ACL Access List」画面で「Extended IP ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

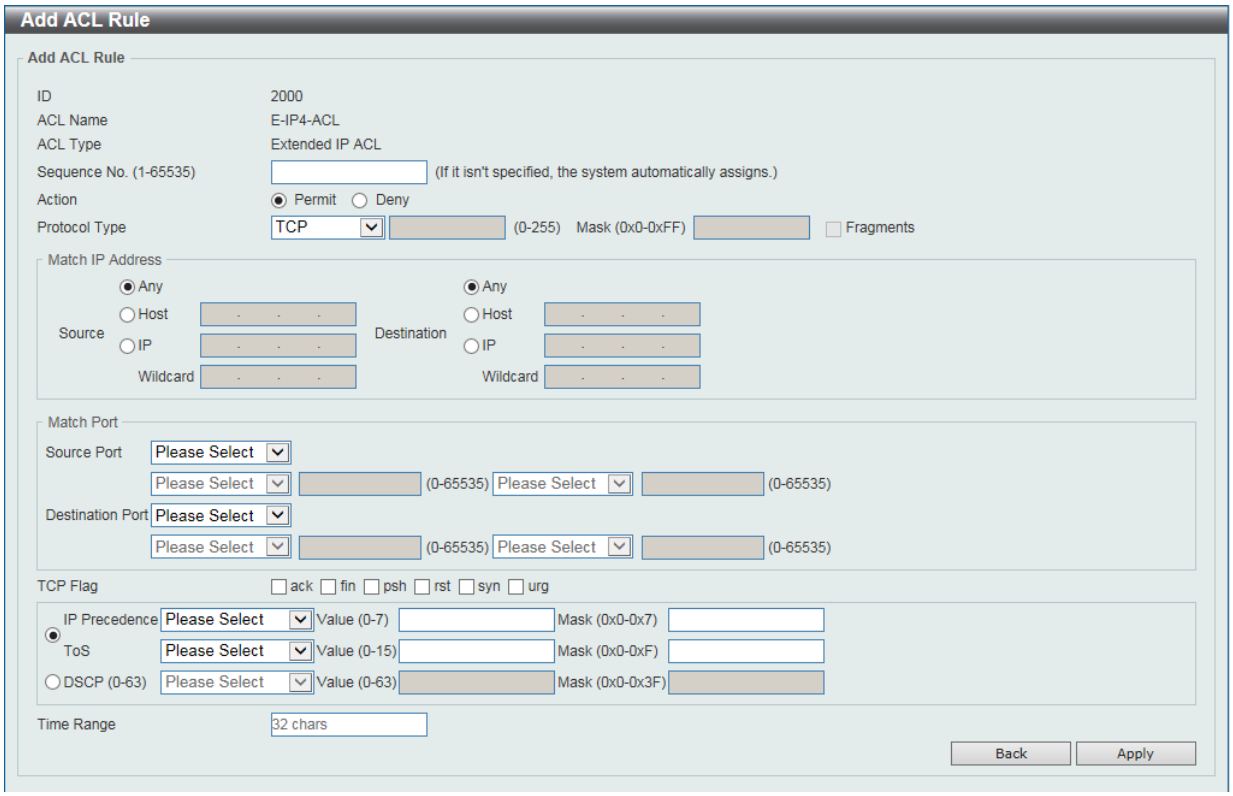


図 11-16　ACL Access List（Extended IP ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Protocol Type	プロトコルの種類を選択します。 • 選択肢:「TCP」「UDP」「ICMP」「EIGRP (88)」「 ESP (50)」「 GRE (47)」「 IGMP (2)」「 OSPF (89)」「 PIM (103)」「 VRRP (112)」「 IP-in-IP (94)」「 PCP (108) 」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

項目	説明
Match IPv4 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。

項目	説明
Match Port	
Source Port	【TCP/UDP を選択時に表示】 送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】 宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Match ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「routine（0）」「priority（1）」「immediate（2）」「flash（3）」「flash-override（4）」「critical（5）」「internet（6）」「network（7）」 - 「Value」：IP 優先値を入力します。（0-7） - 「Mask」：IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「normal（0）」「min-monetary-cost（1）」「max-reliability（2）」「max-throughput（4）」「min-delay（8）」 - 「Value」：ToS 値を入力します。（0-15） - 「Mask」：ToS マスクを入力します。（0x0-0xF）
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default（0）」「af11（10）」「af12（12）」「af13（14）」「af21（18）」「af22（20）」「af23（22）」「af31（26）」「af32（28）」「af33（30）」「af41（34）」「af42（36）」「af43（38）」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。（0-63） - 「Mask」：DSCP マスクを入力します。（0x0-0x3F）
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Standard IPv6 ACL）

「ACL Access List」画面で「Standard IPv6 ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

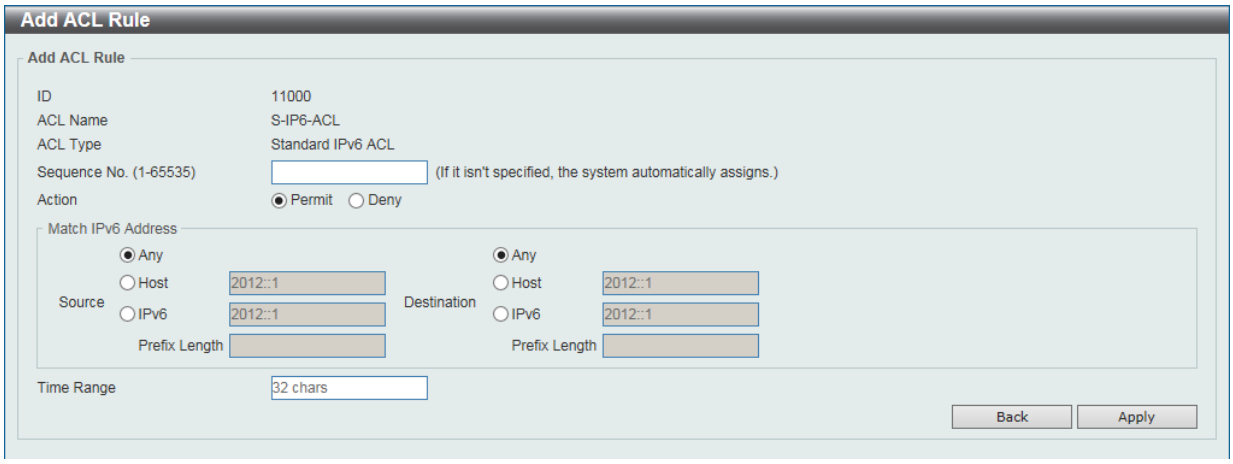


図 11-17　ACL Access List（Standard IPv6 ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Match IPv6 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended IPv6 ACL）

「ACL Access List」画面で「Extended IPv6 ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

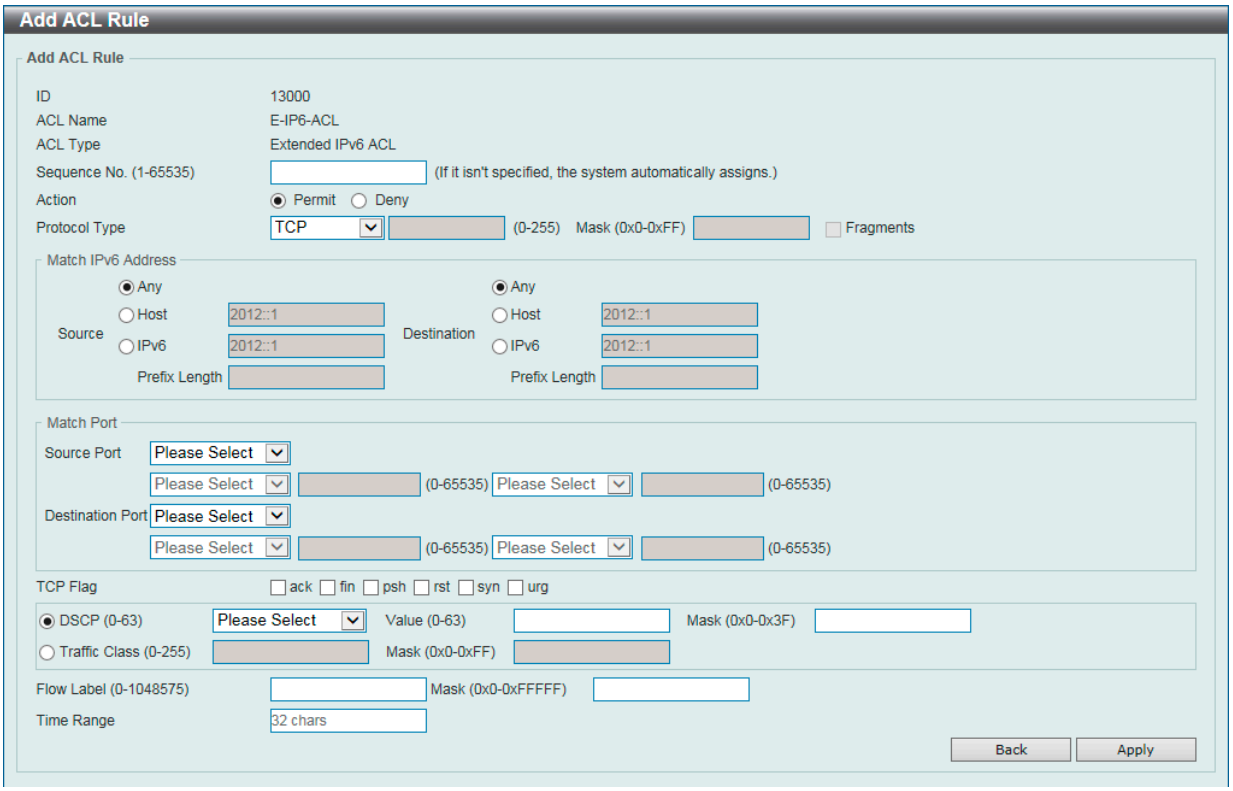


図 11-18　ACL Access List（Extended IPv6 ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「Protocol ID」「ESP」「PCP」「SCTP」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

項目	説明
Match IPv6 Address	
Source	送信元のアドレスを指定します。 •「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 •「Host」- 送信元ホストの IPv6 アドレスを入力します。 •「IPv6」-「Prefix Length」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先のアドレスを指定します。 •「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 •「Host」- 宛先ホストの IPv6 アドレスを入力します。 •「IPv6」-「Prefix Length」が選択可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
Match Port	
Source Port	【TCP/UDP を選択時に表示】 送信元ポートの値を指定します。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

項目	説明
Destination Port	【TCP/UDP を選択時に表示】 宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Match ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
IPv6 DSCP	
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。（0-63） - 「Mask」：DSCP マスクを入力します。（0x0-0x3F）
Traffic Class	トラフィッククラス値とトラフィッククラスのマスク値を入力します。 • 設定可能範囲：0-255 • 「Mask」：トラフィッククラスのマスクを入力します。（0x0-0xFF）
Flow Label	
Flow Label	フローラベルの値を入力します。 • 設定可能範囲：0-1048575 • 「Mask」：フローラベルマスクを入力します。（0x0-0xFFFFF）
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended MAC ACL）

「ACL Access List」画面で「Extended MAC ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

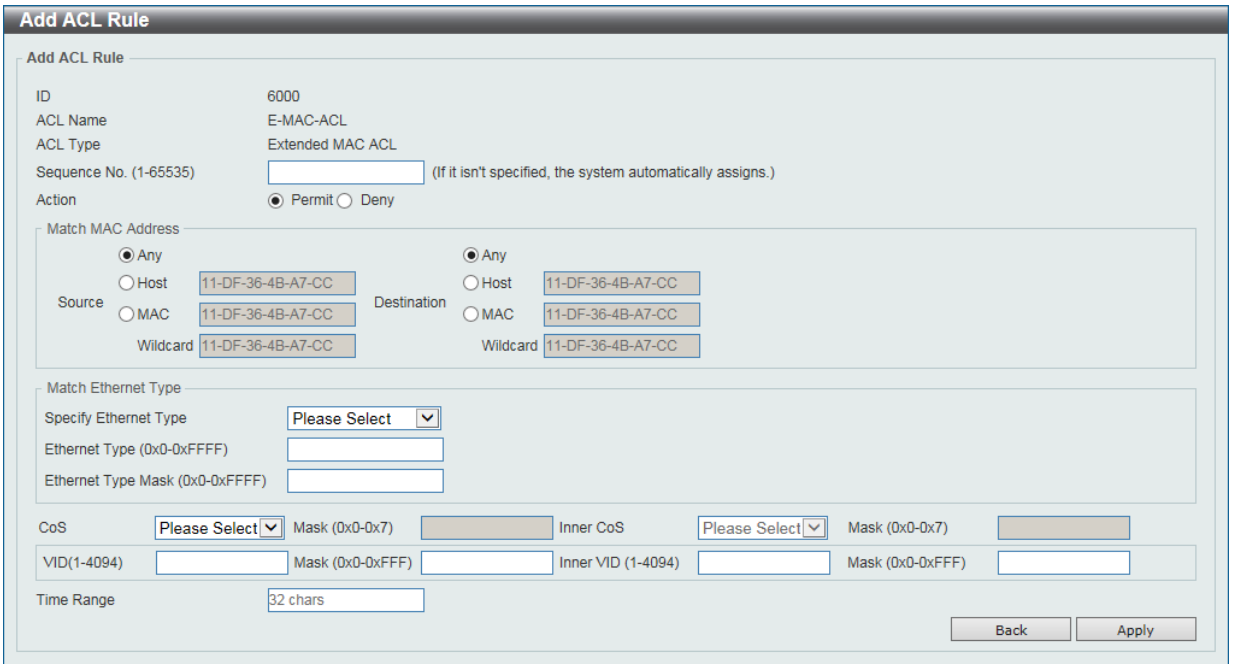


図 11-19　ACL Access List（Extended MAC ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Match MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。送信元 MAC アドレスとワイルドカードを指定します。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの MAC アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。宛先 MAC アドレスとワイルドカードを指定します。
Match Ethernet Type	
Specify Ethernet Type	イーサネットタイプを選択します。 • 設定可能範囲：「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
Ethernet Type	イーサネットタイプの 16 進数値を指定します。「Specify Ethernet Type」で指定したイーサネットタイプに基づき自動的に適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。「Specify Ethernet Type」で指定したイーサネットタイプに基づき自動的に適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
802.1Q VLAN	
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：CoS マスクを入力します。
Inner CoS	CoS 値を指定後、Inner CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：Inner CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに適用する VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）

項目	説明
Inner VID	ACL ルールに適用する Inner VID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended Expert ACL）

「ACL Access List」画面で「Extended Expert ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

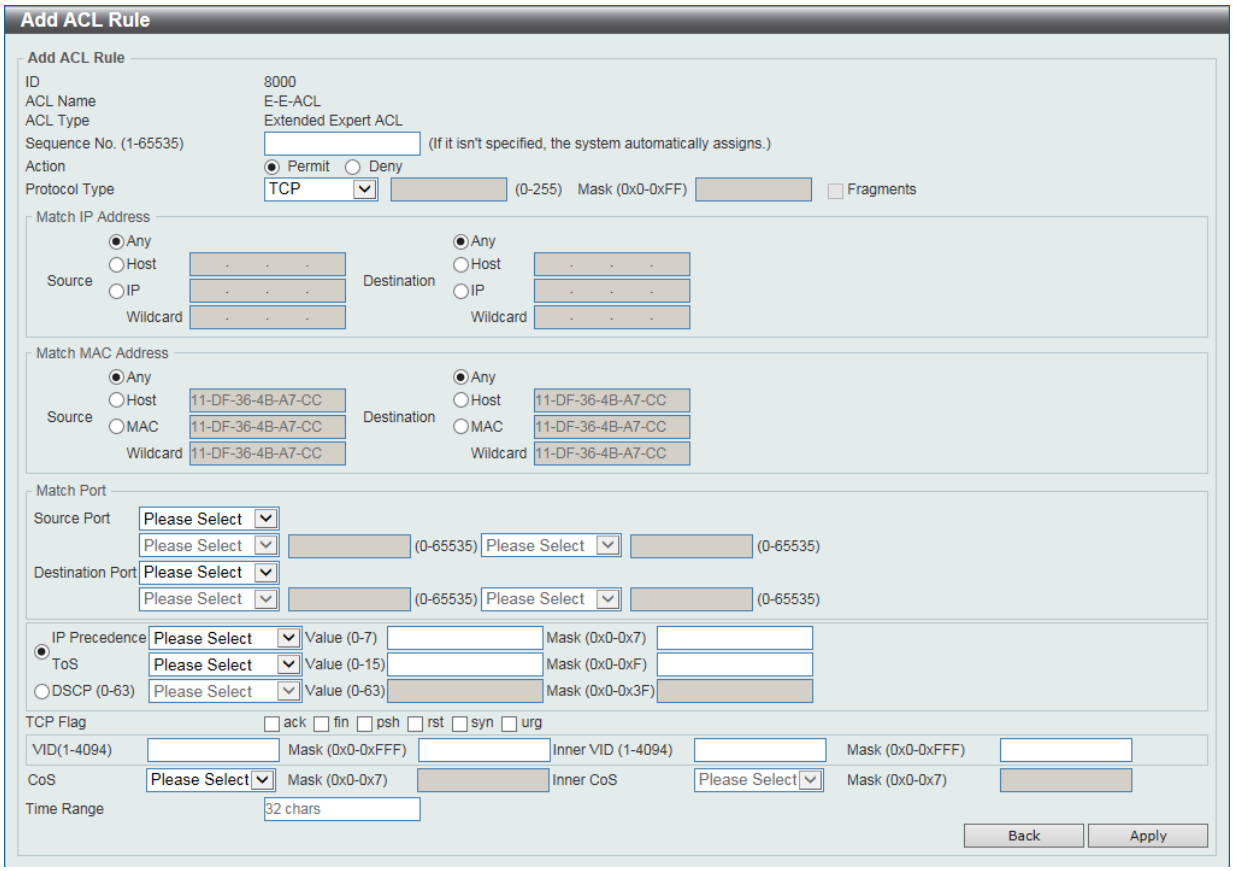


図 11-20　ACL Access List（Extended Expert ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Protocol Type	プロトコルの種類を選択します。 • 選択肢:「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「 Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

項目	説明
Match IP Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Match MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力することができます。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
Match Port	
Source Port	【TCP/UDP を選択時に表示】 送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】 宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「routine（0）」「priority（1）」「immediate（2）」「flash（3）」「flash-override（4）」「critical（5）」「internet（6）」「network（7）」 - 「Value」：IP 優先値を入力します。（0-7） - 「Mask」：IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「normal（0）」「min-monetary-cost（1）」「max-reliability（2）」「max-throughput（4）」「min-delay（8）」 - 「Value」：ToS 値を入力します。（0-15） - 「Mask」：ToS マスクを入力します。（0x0-0xF）

項目	説明
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。（0-63） - 「Mask」：DSCP マスクを入力します。（0x0-0x3F）
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
802.1Q VLAN	
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）
Inner VID	ACL ルールに紐づける Inner VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：CoS マスクを入力します。（0x0-0x7）
Inner CoS	CoS 値を指定後、Inner CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：Inner CoS マスクを入力します。（0x0-0x7）
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended UDF ACL）

「ACL Access List」画面で「Extended UDF ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

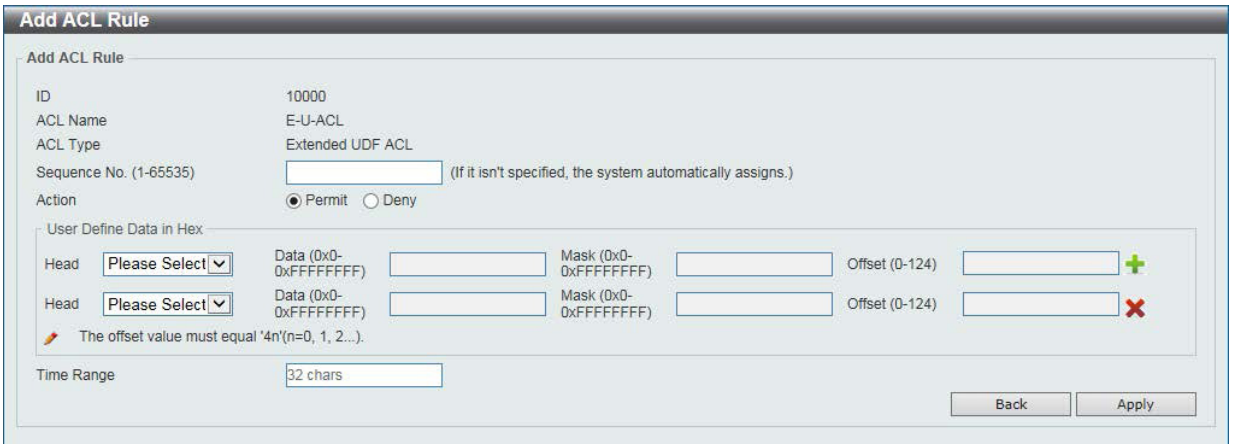


図 11-21　ACL Access List（Extended UDF ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
User Define Data in Hex	
Head	ヘッダで設定されるオフセット値を選択します。 • 選択肢：「L2」「L3」「L4」
Data	パケットのコンテンツに一致する UDF フィールドを入力します。 •「Mask」：データマスクを入力します。ビットは 0 の値が無視され、1 が認識されます。（0x0-0xFFFFFFFF）
Offset	ヘッダで設定されるオフセット値を指定します。 •「L2」の場合、L2 ヘッダから開始されるオフセットを指定します。 •「L3」の場合、L3 ヘッダのマイナス 2Bytes から開始されるオフセットを指定します。 •「L4」の場合、L4 ヘッダから開始されるオフセットを指定します。
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「＋」ボタンをクリックして、データエントリを追加します。
「×」ボタンをクリックして、データエントリを削除します。
「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL Interface Access Group（ACL インタフェースアクセスグループ）

ACL インタフェースアクセスグループの設定、表示を行います。

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

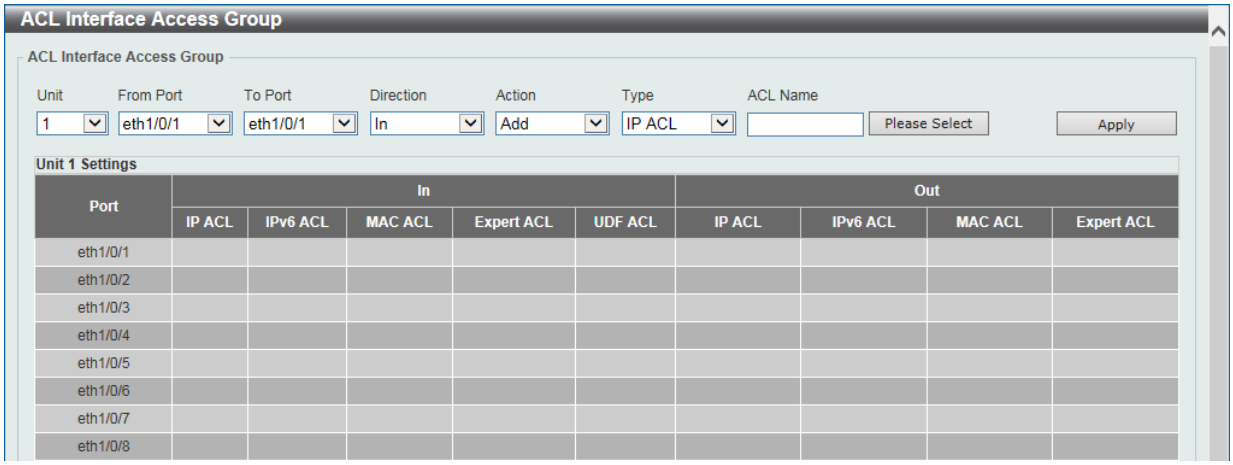


図 11-22　ACL Interface Access Group 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Direction	方向を指定します。 • 選択肢：「In」「Out」
Action	ACL インタフェースアクセスグループを追加 / 削除します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	ACL の種類を選択します。 • 選択肢：「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」「UDF ACL」
ACL Name	アクセスコントロールリスト名を入力します。 「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定することも可能です。

「Apply」ボタンをクリックして、設定内容を適用します。

「Please Select」ボタンをクリックすると次の画面が表示されます。

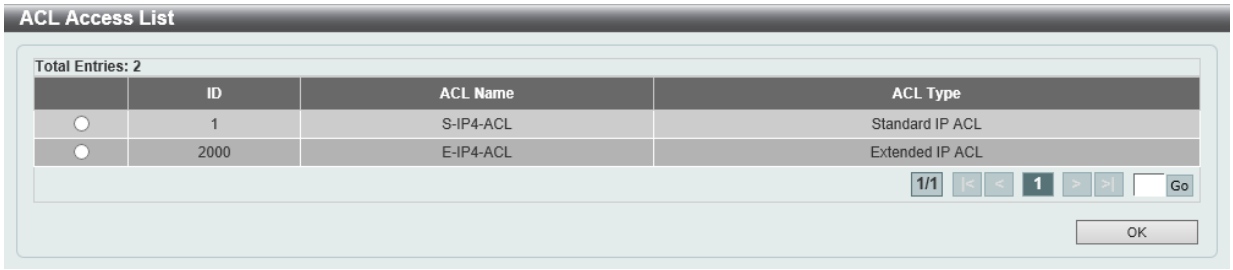


図 11-23　ACL Interface Access Group（Please Select ）- ACL Access List 画面

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。
設定するエントリを選択し「OK」ボタンをクリックします。

ACL VLAN Access Map（ACL VLAN アクセスマップ）

ACL VLAN アクセスマップの設定、表示を行います。

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

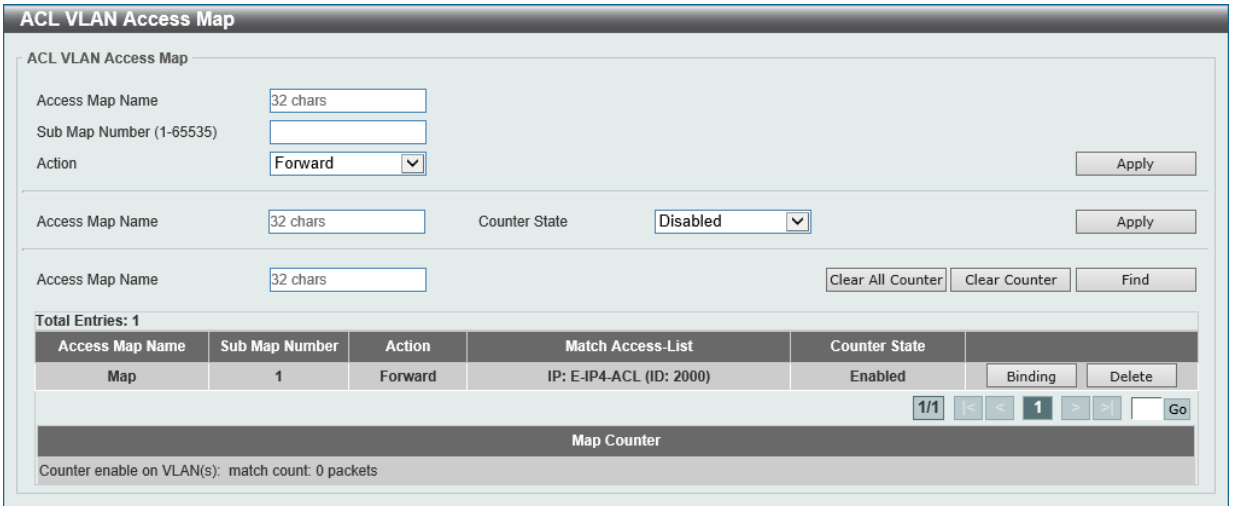


図 11-24　ACL VLAN Access Map 画面

画面に表示される項目：

項目	説明
Access Map Name	アクセスマップ名を入力します。（32 文字以内）
Sub Map Number	サブマップ番号を入力します。 • 設定可能範囲：1-65535
Action	実行するアクションを選択します。 • 選択肢：「Forward」「Drop」「Redirect」 「Redirect」を選択した場合、ドロップダウンリストからリダイレクトされるインタフェースを選択できます。
Counter State	カウンタの有効 / 無効を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

カウンタの検索・削除

「Clear All Counter」ボタンをクリックして、すべてのアクセスマップのカウンタ情報を消去します。
「Clear Counter」ボタンをクリックして、指定アクセスマップのカウンタ情報を消去します。
「Find」ボタンをクリックして、入力した情報を基に特定のエントリを検索します。

アクセスリストのバインディング・エントリの削除

「Binding」ボタンをクリックして、エントリにアクセスリストをバインディングします。
「Delete」ボタンをクリックして、指定エントリを削除します。

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。

アクセスマップエントリをクリックすると、画面下部に Map Counter テーブルが表示されます。

Match Access-List（照合アクセスリスト設定）

アクセスマップエントリの「Binding」ボタンをクリックすると、以下の画面が表示されます。

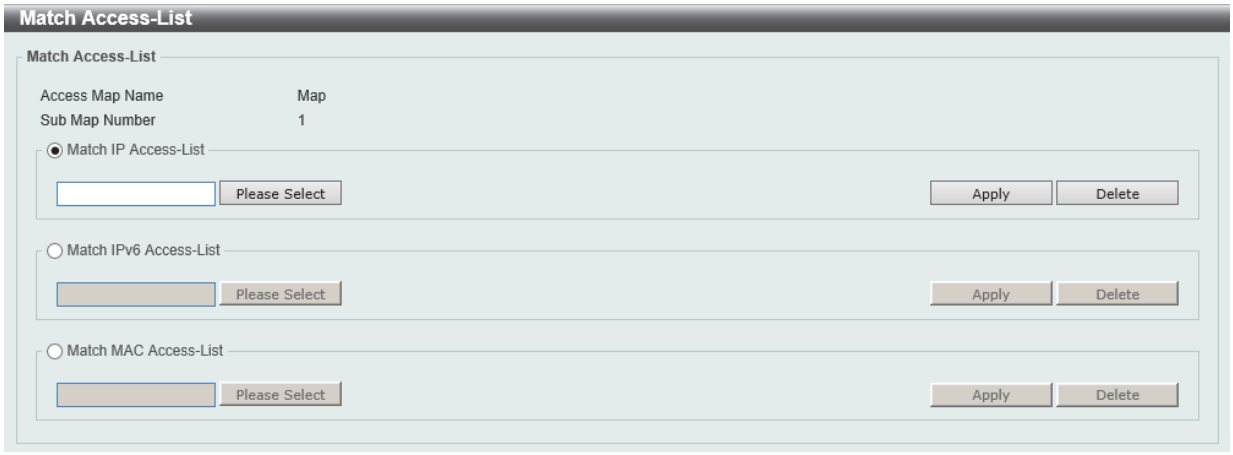


図 11-25　ACL VLAN Access Map（Binding）- Match Access-List 画面

画面に表示される項目：

項目	説明
Match IP Access-List	照合する IP アクセスリストを指定します。 「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定することも可能です。
Match IPv6 Access-List	照合する IPv6 アクセスリストを指定します。 「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定することも可能です。
Match MAC Access-List	照合する MAC アクセスリストを指定します。 「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定することも可能です。

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

ACL の指定画面

「Please Select」ボタンをクリックすると次の画面が表示されます。

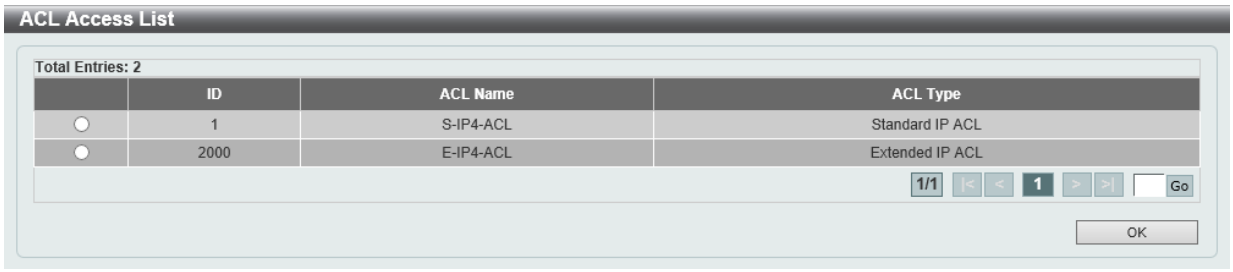


図 11-26　Match Access-List（Please Select）- ACL Access List 画面

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。
設定するエントリを選択し「OK」ボタンをクリックします。

ACL VLAN Filter（ACL VLAN フィルタ設定）

ACL VLAN フィルタの設定、表示を行います。

ACL > ACL VLAN Filter 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 11-27　ACL VLAN Filter 画面

画面に表示される項目：

項目	説明
Access Map Name	アクセスマップ名を入力します。（32 文字以内）
Action	ACL VLAN フィルタを追加 / 削除します。 • 選択肢：「Add（追加）」「Delete（削除）」
VID List	使用する VLAN ID リストを入力します。 「All VLANs」オプションにチェックを入れると、すべての VLAN に本設定を適用します。

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

CPU ACL（CPU ACL 設定）

CPU ACL 機能の設定を行います。

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

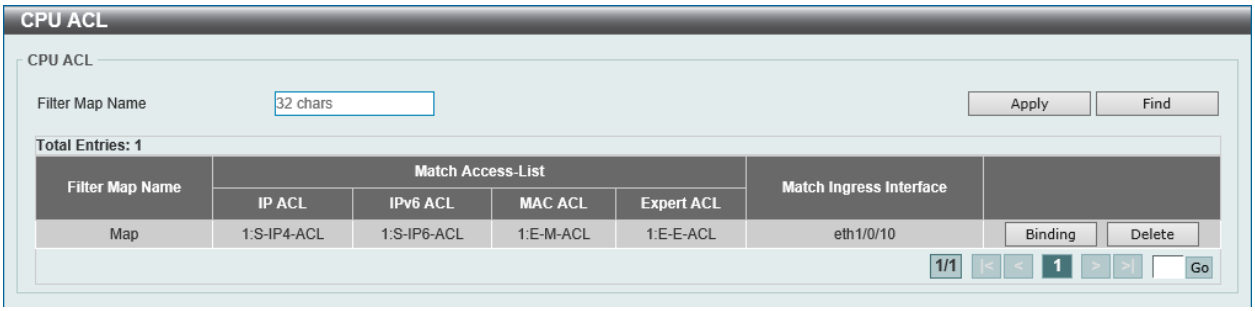


図 11-28　CPU ACL 画面

画面に表示される項目：

項目	説明
Filter Map Name	CPU ACL フィルタマップ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックし、入力した情報を基に特定のエントリを検索します。
「Binding」ボタンをクリックし、エントリにアクセスリストをバインディングします。
「Delete」ボタンをクリックして、指定エントリを削除します。

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。

「Binding」ボタンをクリックすると以下の画面が表示されます。

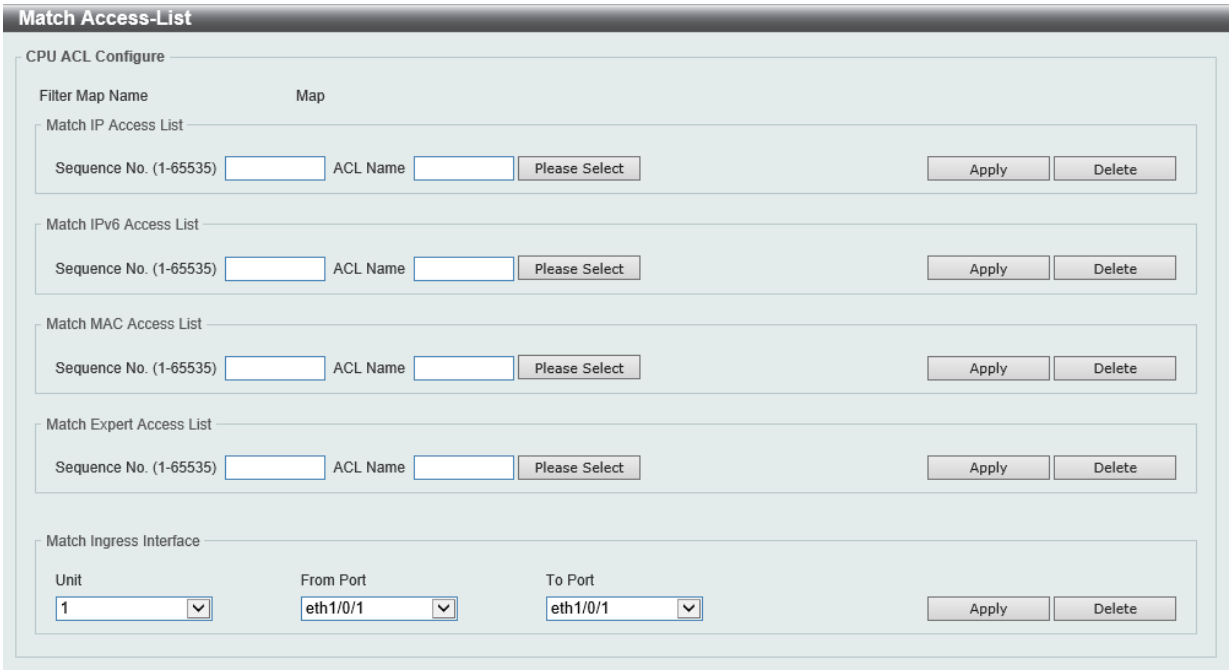


図 11-29　CPU ACL（Binding）- Match Access-List 画面

画面に表示される項目：

項目	説明
Match IP Access List	
Sequence No.	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL Name	照合する Standard または Extended IP アクセスリスト名を指定します。（32 文字以内） 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match IPv6 Access List	
Sequence No.	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL Name	照合する Standard または Extended IPv6 アクセスリスト名を指定します。（32 文字以内） 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match MAC Access List	
Sequence No.	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL Name	照合する Extended MAC アクセスリスト名を指定します。（32 文字以内） 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match Expert Access List	
Sequence No.	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL Name	照合する Extended Expert アクセスリスト名を指定します。（32 文字以内） 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match Ingress Interface	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。

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

ACL 選択画面

「Please Select」ボタンをクリックすると次の画面が表示されます。

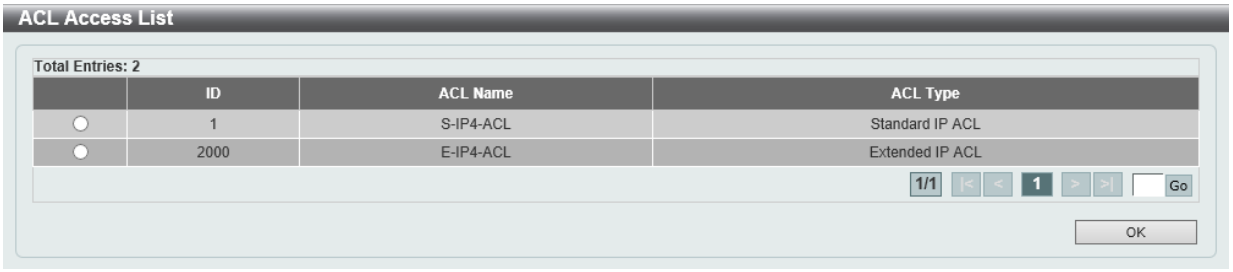


図 11-30　Match Access-List（Please Select）- ACL Access List 画面

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。
設定するエントリを選択し「OK」ボタンをクリックします。

第 12 章　Security（セキュリティ機能の設定）

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

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

サブメニュー	説明
Port Security（ポートセキュリティ）	ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。
802.1X（802.1X 設定）	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。
AAA（AAA 設定）	AAA（Authentication、Authorization、Accounting）の設定を行います。
RADIUS（RADIUS 設定）	RADIUS の設定を行います。
TACACS+（TACACS+ 設定）	TACACS+ の設定を行います。
IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）	IP-MAC バインディングにより、スイッチにアクセスするユーザ数を制限します。
DHCP Server Screening（DHCP サーバスクリーニング設定）	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
ARP Spoofing Prevention（ARP スプーフィング防止設定）	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスと一致しなかった IP アドレスの ARP パケットをバイパスします。
BPDU Attack Protection（BPDU アタック防止設定）	スイッチのポートに BPDU 防止機能を設定します。
NetBIOS Filtering（NetBIOS フィルタリング設定）	NetBIOS フィルタリングの設定を行います。
MAC Authentication（MAC 認証）	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
Web-based Access Control（Web 認証）	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認証する機能です。
Network Access Authentication（ネットワークアクセス認証）	Network Access Authentication（ネットワークアクセス認証）の設定を行います。
Safeguard Engine（セーフガードエンジン）	セーフガードエンジンは、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（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ポート間のトラフィックの流れの制限を行います。
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。
SSH（Secure Shell）	SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。
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。
Network Protocol Port Protect Settings（ネットワークプロトコルポート保護設定）	ネットワークプロトコルポートプロテクションの設定、表示を行います。

Port Security（ポートセキュリティ）

ポートセキュリティの設定を行います。ポートセキュリティ機能では、ソース MAC アドレスが未認証であるコンピュータについて、指定ポートからネットワークへアクセスすることを防ぐことができます。

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

ポートセキュリティのグローバル設定を行います。

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

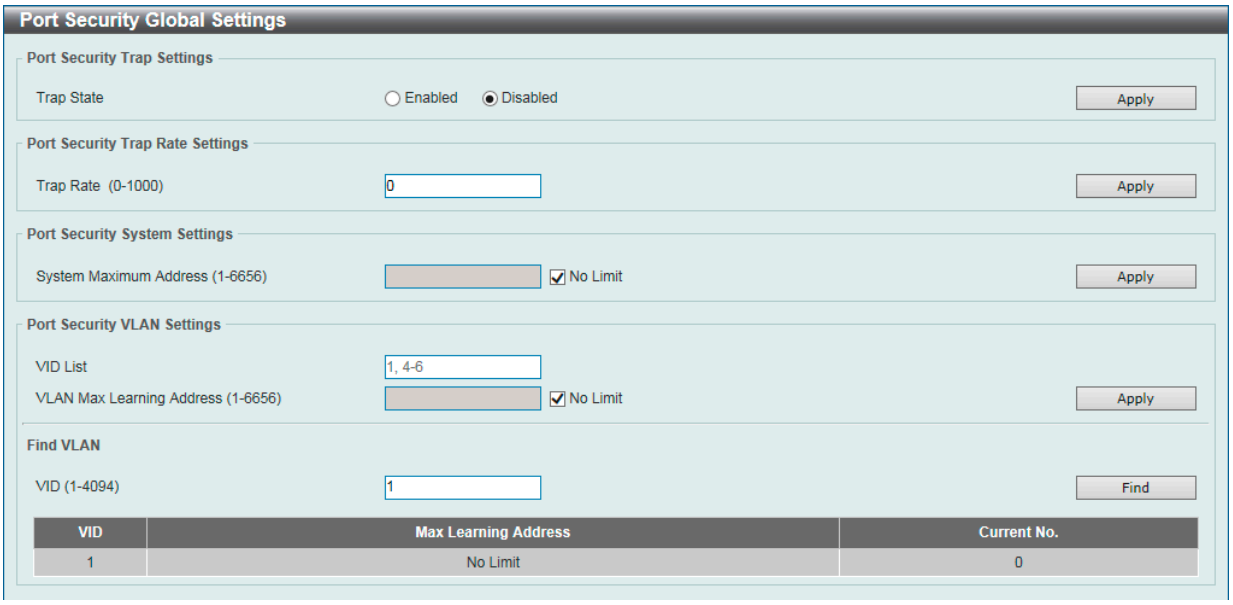


図 12-1　Port Security Global Settings 画面

画面に表示される項目：

項目	説明
Port Security Trap Settings	
Trap State	ポートセキュリティのトラップを有効 / 無効に設定します。
Port Security Trap Rate Settings	
Trap Rate	1 秒あたりのトラップ数を指定します。 初期値の 0 では、すべてのセキュリティ違反に対して SNMP トラップが生成されます。 • 設定可能範囲：0-1000 • 初期値：0
Port Security System Settings	
System Maximum Address	許可される最大 MAC アドレス数を入力します。初期値では制限なしになります。 「No Limit」オプションにチェックを入れると、セキュアな MAC アドレスの最大数が適用されます。 • 設定可能範囲：1-6656
Port Security VLAN Settings	
VID List	VLAN ID を指定します。
VLAN Max Learning Address	指定の VLAN が学習可能な MAC アドレスの最大数を指定します。 「No Limit」オプションにチェックを入れると、セキュアな MAC アドレスの最大数が適用されます。 • 設定可能範囲：1-6656
Find VLAN	
VID	表示する VLAN ID を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「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。

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

ポートセキュリティのポート設定と設定内容の表示を行います。

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

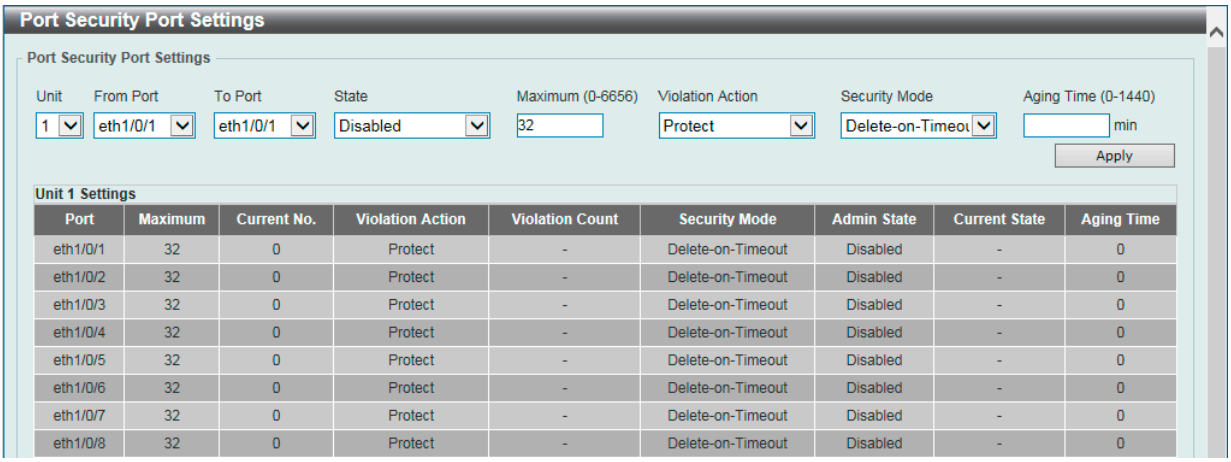


図 12-2　Port Security Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
State	指定ポートにおけるポートセキュリティ機能を有効 / 無効に設定します。
Maximum	指定ポートで許可されるセキュアな MAC アドレスの最大数を指定します。 • 設定可能範囲：0-6656 • 初期値：32
Violation Action	違反に対して実行するアクションを指定します。 • 「Protect」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反としてはカウントされません。 • 「Restrict」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントしてシステムログに記録します。 • 「Shutdown」- セキュリティ違反がある場合にポートをシャットダウンし、システムログに記録します。
Security Mode	セキュリティモードを選択します。 • 「Permanent」- すべての学習した MAC アドレスは、手動でエントリを削除しない限り削除されません。 • 「Delete-on-Timeout」- すべての学習した MAC アドレスは、タイムアウトにより自動的に削除されるか、手動により削除されます。
Aging Time	指定ポートで自動学習された安全なアドレスに使用するエージングタイムを入力します。 • 設定可能範囲：0-1440（分）

「Apply」ボタンをクリックして、設定内容を適用します。

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

ポートセキュリティアドレスエントリの設定、表示を行います。

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

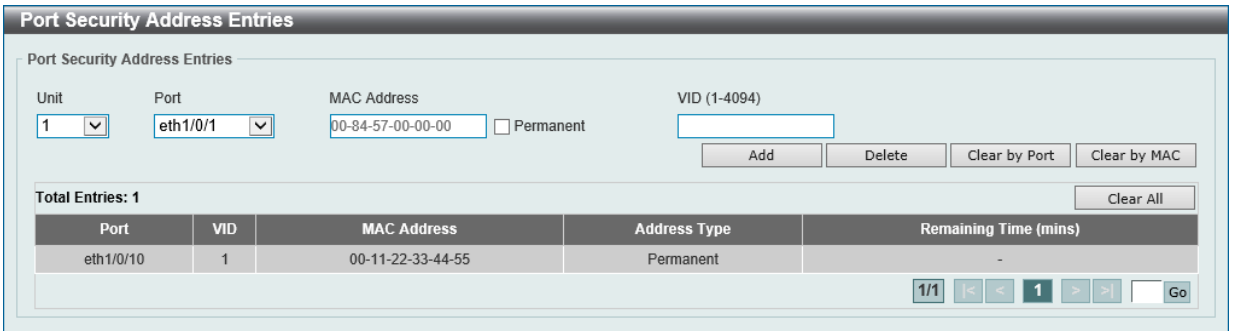


図 12-3　Port Security Address Entries 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
MAC Address	MAC アドレスを入力します。 「Permanent」オプションにチェックを入れると、すべての学習した MAC アドレスは、手動でエントリを削除しない限り削除されません。
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094

「Add」ボタンをクリックして、入力した情報に基づく新しいエントリを追加します。
「Delete」ボタンをクリックし、入力した情報に基づくエントリを削除します。
「Clear by Port」ボタンをクリックして、指定したポートに基づき情報を消去します。
「Clear by MAC」ボタンをクリックして、指定した MAC アドレスに基づき情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。

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。

802.1X（802.1X 設定）

802.1X（ポートベースおよびホストベースのアクセスコントロール）

IEEE 802.1X は、ユーザ認証を行うセキュリティの規格です。

クライアント / サーバベースのアクセスコントロールモデルを使用し、特定のローカルエリアネットワーク上の有線 / 無線デバイスへのアクセスを許可および認証するために使用します。この認証方法は、ネットワークへアクセスするユーザの認証に RADIUS サーバを使用し、EAPOL（Extensible Authentication Protocol over LAN）と呼ばれるパケットをクライアント / サーバ間でリレーして実現します。

以下の図は、基本的な EAPOL パケットの構成です。

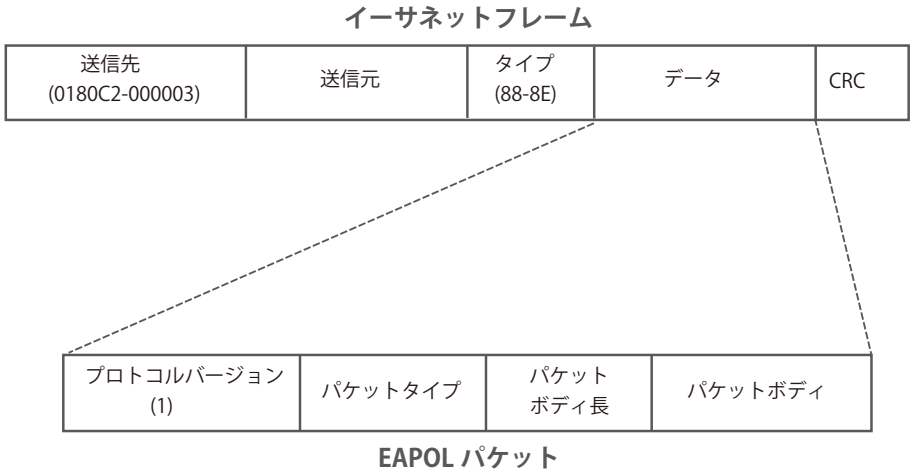


図 12-4　EAPOL パケット

IEEE 802.1X を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。
EAPOL パケットは、承認完了前でも指定ポート経由で送受信できる唯一のトラフィックです。

802.1X アクセスコントロールには認証サーバ、オーセンティケータ、クライアントの 3 つの役割があります。
それぞれがアクセスコントロールセキュリティの作成、状態の維持、動作のために重要です。

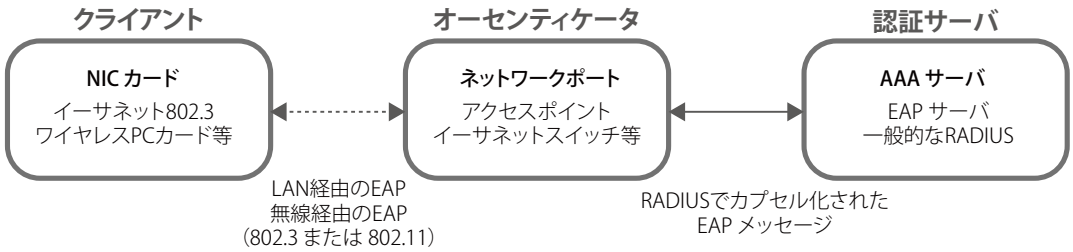


図 12-5　802.1X の 3 つの役割

以降の項目では、認証サーバ、オーセンティケータ、クライアントのそれぞれの役割について説明します。

認証サーバ

認証サーバは、クライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。

認証サーバ上で RADIUS サーバプログラムが実行され、認証サーバのデータがオーセンティケータ（スイッチ）に正しく登録されている必要があります。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを使用する前に、認証サーバ（RADIUS）によって認証される必要があります。

認証サーバの役割は、ネットワークにアクセスするクライアントの身元を証明することです。認証サーバ（RADIUS）とクライアントの間で EAPOL パケットによるセキュアな情報交換を行い、クライアントが「LAN やスイッチのサービスに対するアクセス許可があるか」をスイッチに通知します。

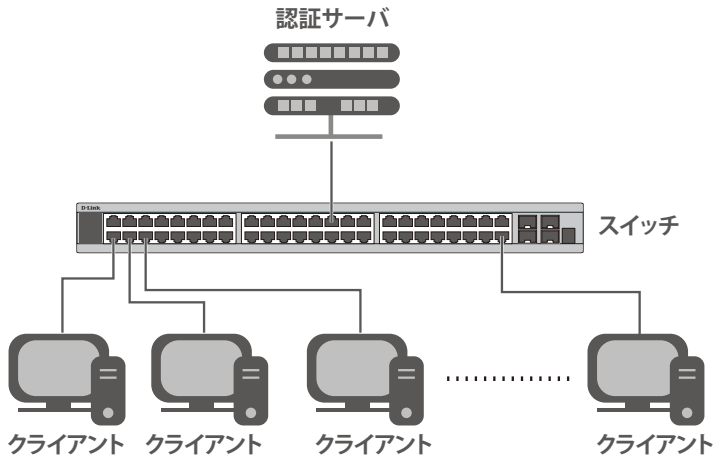


図 12-6　認証サーバ

オーセンティケータ

オーセンティケータ（スイッチ）は、認証サーバとクライアントの間を仲介します。

802.1X を使用する場合、オーセンティケータには 2 つの役割があります。

- 1 つ目の役割：
  クライアントに EAPOL パケットを通して認証情報を提出するよう要求することです。
  EAPOL パケットはクライアントにアクセスが許可される前にオーセンティケータを通過することのできる唯一の情報です。
- 2 つ目の役割：
  クライアントから収集した情報を認証サーバに確認してもらい、その結果をクライアントに伝達することです。

スイッチをオーセンティケータとして設定するには、以下の手順を実行します。

1. スイッチの 802.1X 機能を有効にします。（**Security > 802.1X > 802.1X Global Settings**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Port Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > RADIUS > RADIUS Server Settings**）

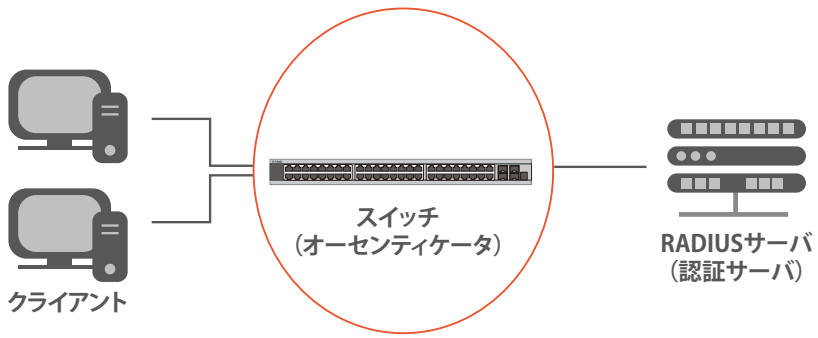


図 12-7　オーセンティケータ

クライアント

クライアントとは、LAN やスイッチが提供するサービスへアクセスしようとする端末です。

クライアントとなる端末では、802.1X プロトコルに準拠したソフトウェアが起動している必要があります。一部の Windows OS のように、OS 内に既にそのソフトウェアが組み込まれている場合がありますが、それ以外の OS をお使いの場合は、802.1X クライアントソフトウェアを別途用意する必要があります。

クライアントは EAPOL パケットを使用して LAN へのアクセスを要求し、スイッチからの要求に応答します。

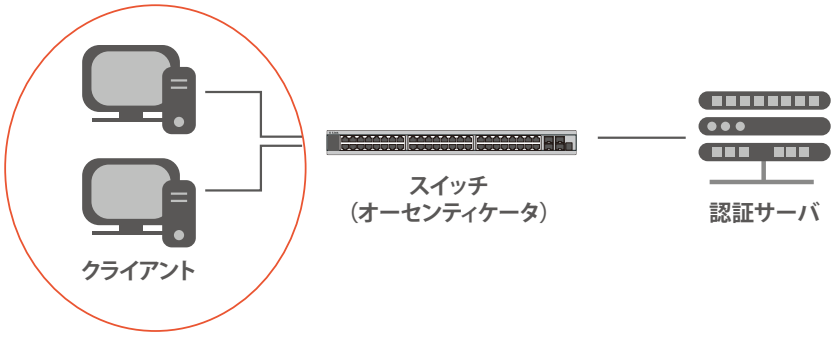


図 12-8　クライアント

認証プロセスについて

前述の「認証サーバ」「オーセンティケータ」「クライアント」により、802.1X プロトコルはネットワークへアクセスするユーザの認証を安定的かつ安全に行います。

認証完了前には EAPOL トラフィックのみが特定のポートの通過を許可されます。このポートは、有効なユーザ名とパスワード（802.1X の設定によっては MAC アドレスも）を持つクライアントがアクセス権を取得してポートのロックが解除されるまで、ロック状態を保ちます。ロックが解除されると、通常のトラフィックがポートを通過できるようになります。

本製品の 802.1X では、以下の 2 種類のアクセスコントロールが選択できます。

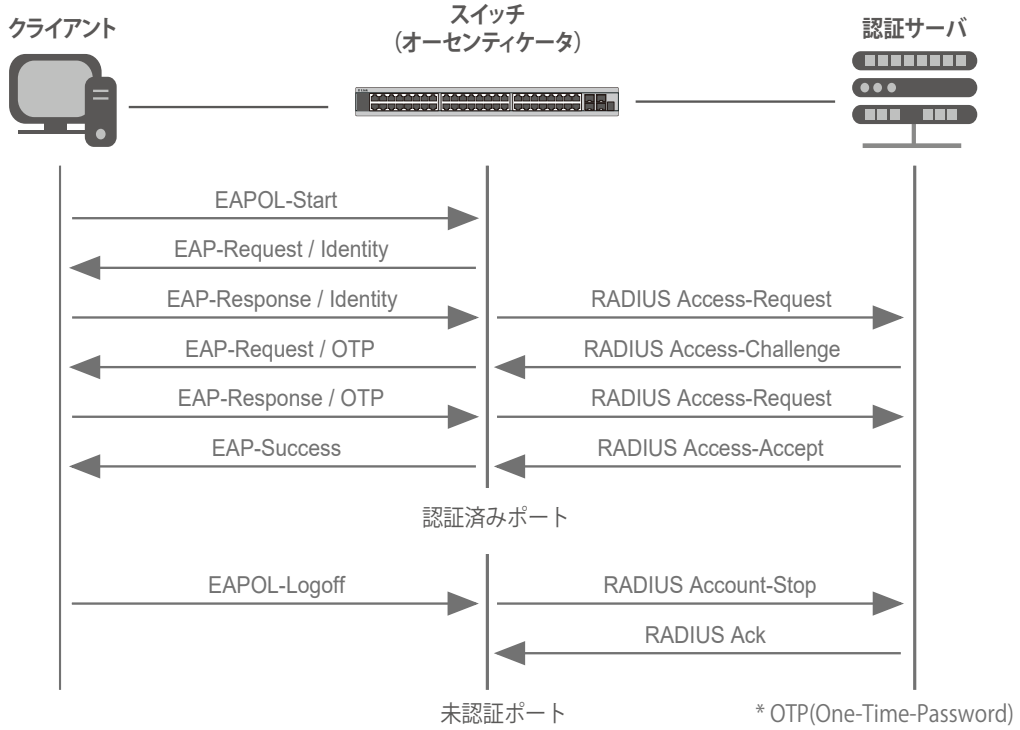


図 12-9　802.1X 認証プロセス

本製品の 802.1X 機能では、以下の 2 つのタイプのアクセスコントロールから選択することができます。

1. **ポートベースのアクセスコントロール**
   本方式では、リモート RADIUS サーバが、ポートごとに 1 人のユーザのみを認証することで、同じポート上の残りのユーザがネットワークにアクセスできるようにします。
2. **ホストベースのアクセスコントロール**
   本方式では、スイッチはポートで最大 448 件までの MAC アドレスを自動的に学習してリストに追加します。
   スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に MAC アドレスごと（ユーザごと）の認証を行います。

802.X ポートベース / ホストベースのネットワークアクセスコントロールについて

802.1X は、元々は LAN 上で Point to Point プロトコルの特長を活用するために開発されました。

単一の LAN セグメントが 2 台より多くのデバイスを持たない場合、デバイスのどちらかがブリッジポートとなります。
ブリッジポートは、「リンクのリモートエンドにアクティブなデバイスが接続された」「アクティブなデバイスが非アクティブ状態になった」などのイベントを検知します。これらのイベントをポートの認証状態の制御に利用し、ポートの許可がされていない接続デバイスの認証プロセスを開始します。これをポートベースのアクセスコントロールと呼びます。

■ ポートベースネットワークアクセスコントロール

接続デバイスが認証に成功すると、ポートは「Authorized」（認証済み）の状態になります。ポートが未認証になるようなイベントが発生するまで、ポート上のすべてのトラフィックはアクセスコントロール制限の対象になりません。

そのため、ポートが複数のデバイスが所属する共有 LAN セグメントに接続される場合、接続デバイスの 1 つが認証に成功すると共有セグメント上のすべての LAN に対してアクセスを許可することになります。このような場合、ポートベースネットワークアクセスコントロールは脆弱であるといえます。

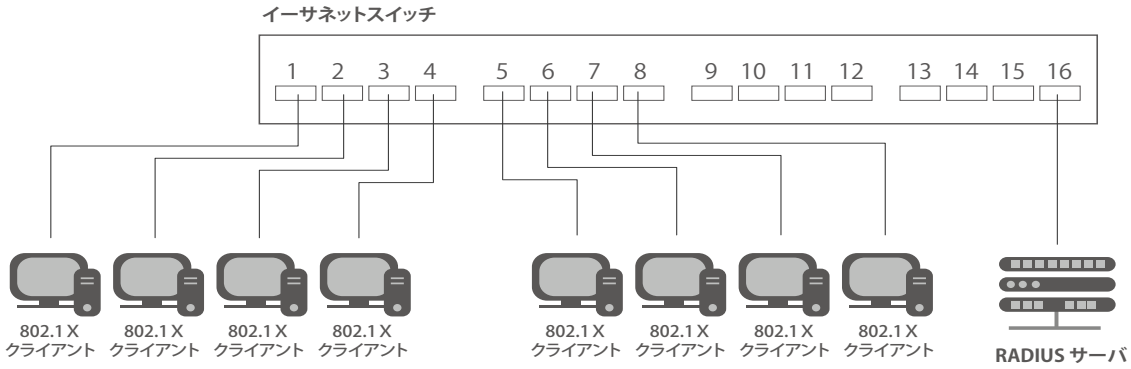


図 12-10　ポートベースアクセスコントロールのネットワーク構成例

■ ホストベースネットワークアクセスコントロール

共有 LAN セグメント内で 802.1X を活用するには、LAN へのアクセスを希望する各デバイスに論理ポートを定義する必要があります。

スイッチは、共有 LAN セグメントに接続する 1 つの物理ポートを異なる論理ポートの集まりであると認識し、それら論理ポートを EAPOL パケット交換と認証状態に基づいて別々に制御します。スイッチは接続する各デバイスの MAC アドレスを学習し、それらのデバイスがスイッチ経由で LAN と通信するための論理ポートを確立します。

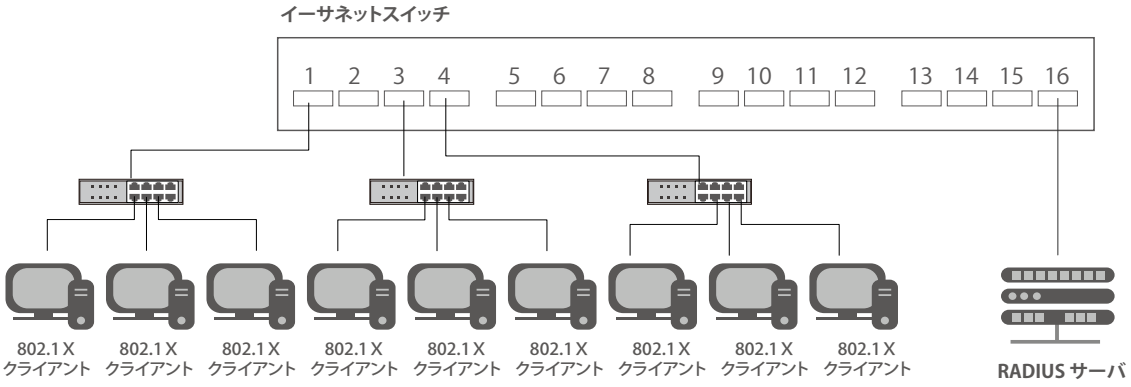


図 12-11　ホストベースアクセスコントロールのネットワーク構成例

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

本画面では 802.1X グローバル設定を行います。

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

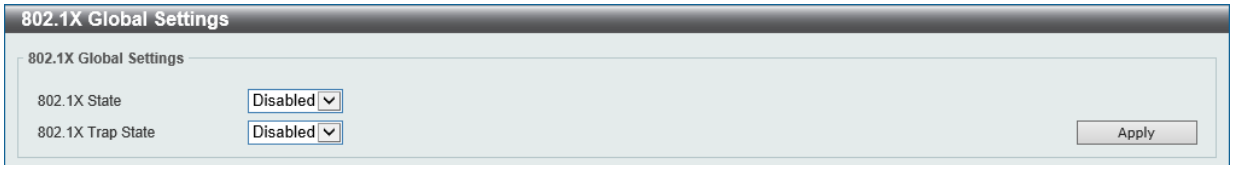


図 12-12　802.1X Global Settings 画面

画面に表示される項目：

項目	説明
802.1X State	802.1X 認証を有効 / 無効に設定します。
802.1X Trap State	802.1X トラップを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

802.1X Port Settings（802.1X ポート設定）

802.1X 認証ポートを設定します。

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

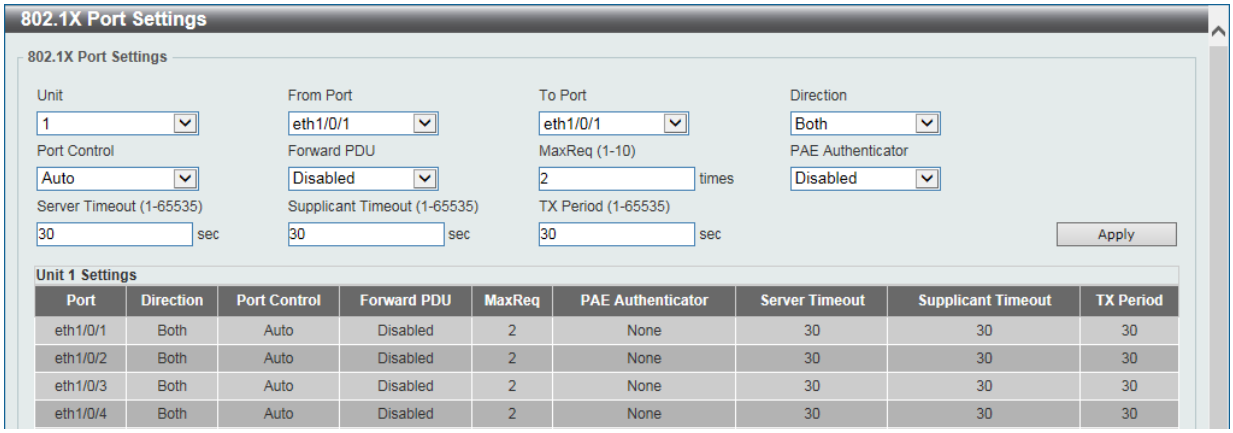


図 12-13　802.1X Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Direction	制御するトラフィックの方向を指定します。 • 「Both」- ポートが受信送信する両方向のトラフィックについて制御します。 • 「In」- 指定したポートへの入力トラフィックのみ制御対象となります。
Port Control	ポートの認証状態を指定します。 • 「ForceAuthorized（強制許可）」- 両方向の通信でポートは制御されません。 • 「Auto（自動）」- 制御対象の方向のポートへのアクセスは認証が必要になります。 • 「ForceUnauthorized（強制未認証）」- 制御対象の方向のポートへのアクセスはブロックされます。
Forward PDU	PDU 転送機能を有効 / 無効に設定します。
MaxReq	認バックエンドの認証ステートマシンがクライアントに対して Extensible Authentication Protocol（EAP）リクエストフレームを再送する最大回数を指定します。本指定回数後、認証プロセスが再開されます。 • 設定可能範囲：1-10 • 初期値：2
PAE Authenticator	PAE Authenticator を有効 / 無効に設定します。 本設定により、特定ポートを IEEE 802.1X Port Access Entity（PAE）オーセンティケータとして指定します。
Server Timeout	サーバのタイムアウト時間を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
Supplicant Timeout	サプリカント（クライアント）のタイムアウト状態となる時間を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）

項目	説明
Tx Period	送信間隔を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

注意　定期的に EAP Request/Identity を送信する機能はありません。

Authentication Session Information（認証セッションの状態）

認証セッションの情報を表示します。

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

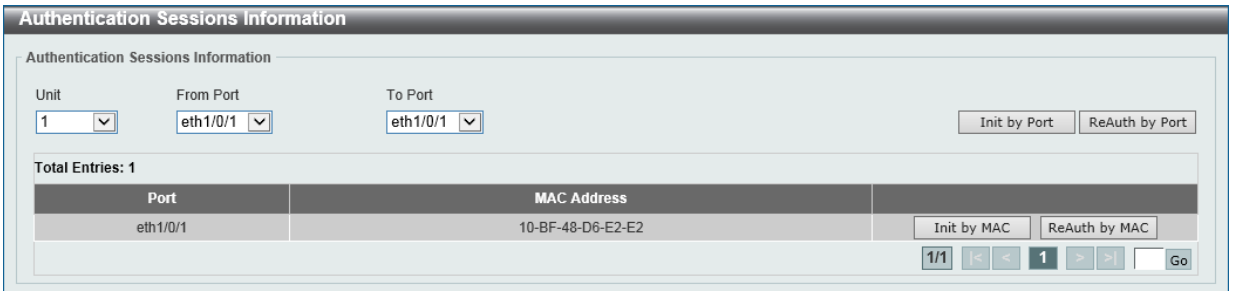


図 12-14　Authentication Session Information 画面

画面に表示される項目：

項目	説明
Unit	セッション情報の初期化 / 再認証を行うユニットを選択します。
From Port/To Port	セッション情報の初期化 / 再認証を行うポート範囲を指定します。

「Init by Port」ボタンをクリックして、指定ポートのセッション情報の初期化を実行します。
「ReAuth by Port」ボタンをクリックして、指定ポートのセッション情報の再認証（Re-Authenticate）を実行します。
「Init by MAC」ボタンをクリックして、指定 MAC アドレスのセッション情報の初期化を実行します。
「ReAuth by MAC」ボタンをクリックして、指定 MAC アドレスのセッション情報の再認証（Re-Authenticate）を実行します。
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。

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

オーセンティケータの統計情報を表示します。

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

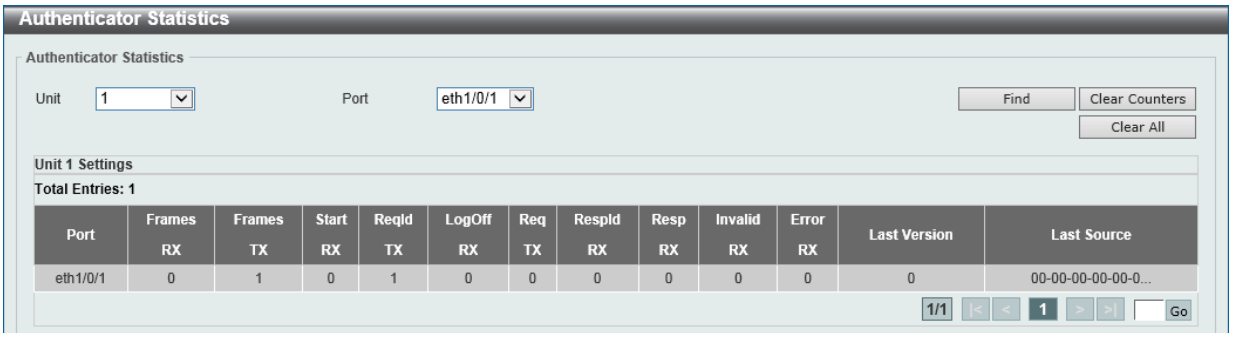


図 12-15　Authenticator Statics 画面

画面に表示される項目：

項目	説明
Unit	統計情報を表示 / クリアするユニットを選択します。
Port	統計情報を表示 / クリアするポート範囲を指定します。

「Find」ボタンをクリックし、指定ポートのエントリを検出します。
「Clear Counters」ボタンをクリックして、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て、テーブル上のすべての情報を消去します。
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。

Authenticator Session Statistics（オーセンティケータセッション統計情報）

オーセンティケータセッションの統計情報を表示します。

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

図 12-16　Authenticator Session Statistics 画面

画面に表示される項目：

項目	説明
Unit	統計情報を表示 / クリアするユニットを選択します。
Port	統計情報を表示 / クリアするポート範囲を指定します。

「Find」ボタンをクリックして、指定ポートのエントリを検出します。
「Clear Counters」ボタンをクリックして、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て、テーブル上のすべての情報を消去します。

Authenticator Diagnostics（オーセンティケータ診断）

オーセンティケータ診断情報を表示します。

Security > 802.1X > Authenticator 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。

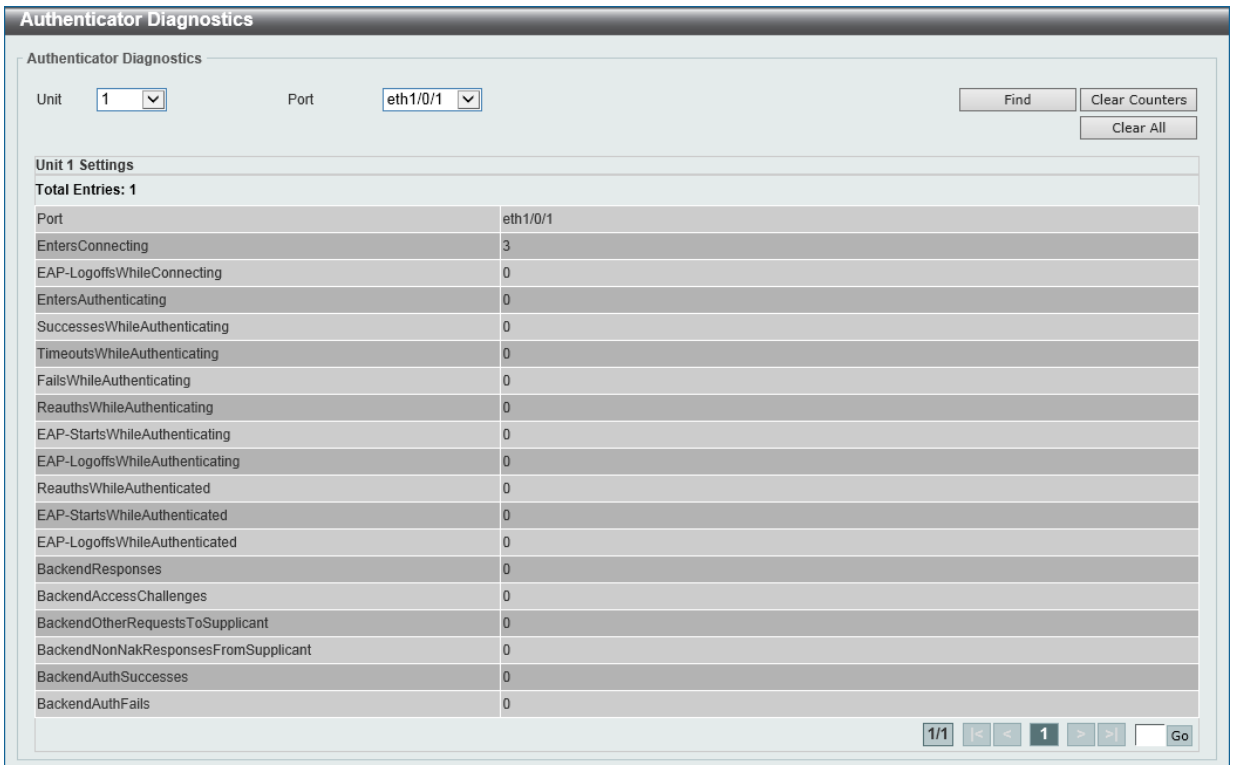


図 12-17　Authenticator Diagnostics 画面

画面に表示される項目：

項目	説明
Unit	診断情報を表示 / クリアするユニットを選択します。
Port	診断情報を表示 / クリアするポート範囲を指定します。

「Find」ボタンをクリックして、指定ポートのエントリを検出します。
「Clear Counters」ボタンをクリックして、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て、テーブル上のすべての情報を消去します。
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。

AAA（AAA 設定）

Security > AAA
本項目では AAA（Authentication、Authorization、Accounting）の設定を行います。

AAA Global Settings（AAA グローバル設定）

本項目では AAA（Authentication、Authorization、Accounting）のグローバル設定を行います。

Security > AAA > AAA 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。

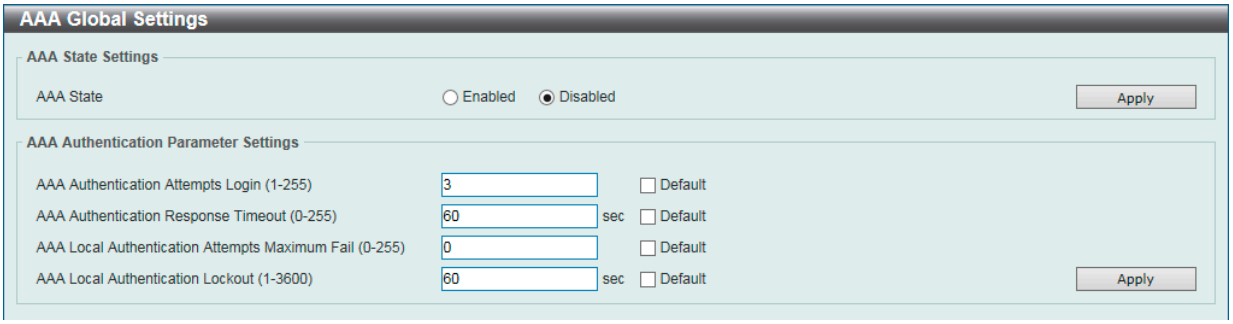


図 12-18　AAA Global Settings 画面

画面に表示される項目：

項目	説明
AAA State Settings	
AAA State	AAA のグローバルステータスを有効 / 無効に設定します。
AAA Authentication Parameter Settings	
AAA Authentication Attempts Login	許可される AAA 認証ログイン試行回数を入力します。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：1-255 • 初期値：3
AAA Authentication Response Timeout	AAA 認証応答のタイムアウト値を入力します。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：0-255（秒） • 初期値：60（秒）
AAA Local Authentication Attempts Maximum Fail	ローカル AAA 認証で許可される失敗の最大回数を入力します。この値が「0」の場合、本機能は無効となります。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：0-255 • 初期値：0
AAA Local Authentication Lockout	ローカル AAA 認証のロックアウト時間を入力します。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：1-3600（秒） • 初期値：60（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

Application Authentication Settings（アプリケーションの認証設定）

ログインする際に使用するスイッチの設定用アプリケーション（コンソール、Telnet、SSH、HTTP）を設定します。

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

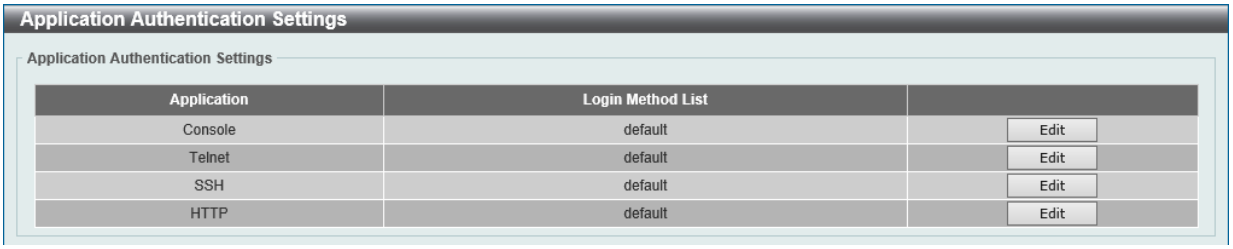


図 12-19　Application Authentication Settings 画面

指定エントリの「Edit」ボタンをクリックし編集を行います。

補足　Telnet/SSH のセッション数は、それぞれ最大 8 となります。

「Edit」をクリックすると、以下の画面が表示されます。

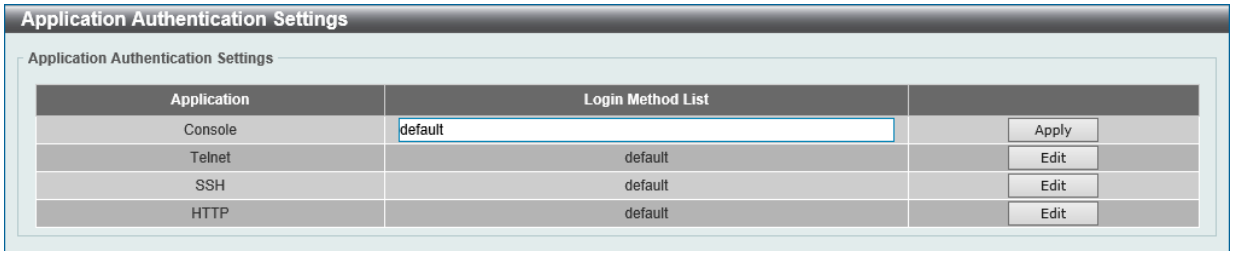


図 12-20　Application Authentication Settings (Edit) 画面

画面に表示される項目：

項目	説明
Login Method List	指定エントリの「Edit」ボタンをクリックし編集を行います。使用するログインメソッドリスト名を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

Application Accounting Settings（アプリケーションアカウンティング設定）

アプリケーションアカウンティングを設定します。

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

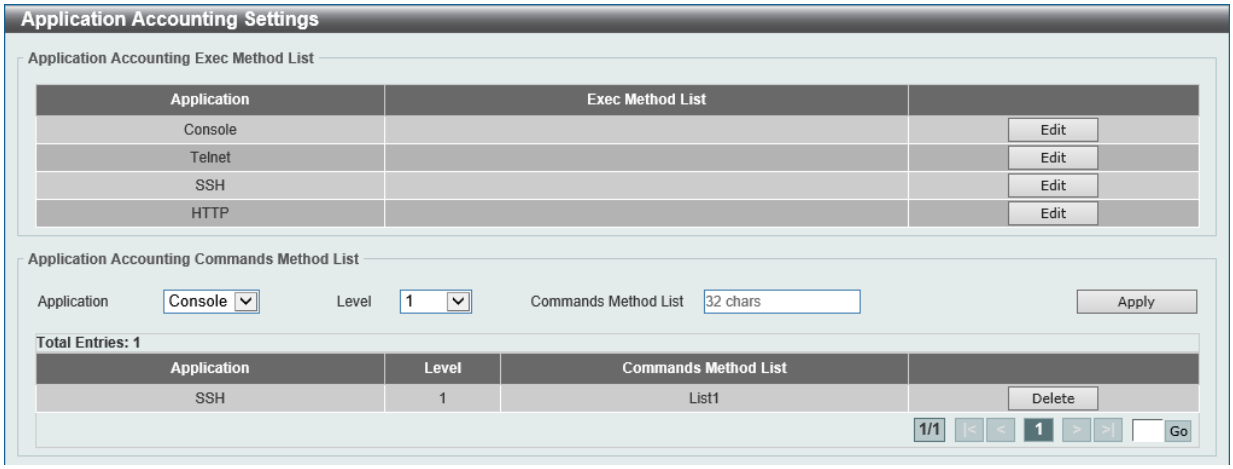


図 12-21　Application Accounting Settings 画面

「Edit」をクリックし、以下の画面で指定エントリの設定を行います。

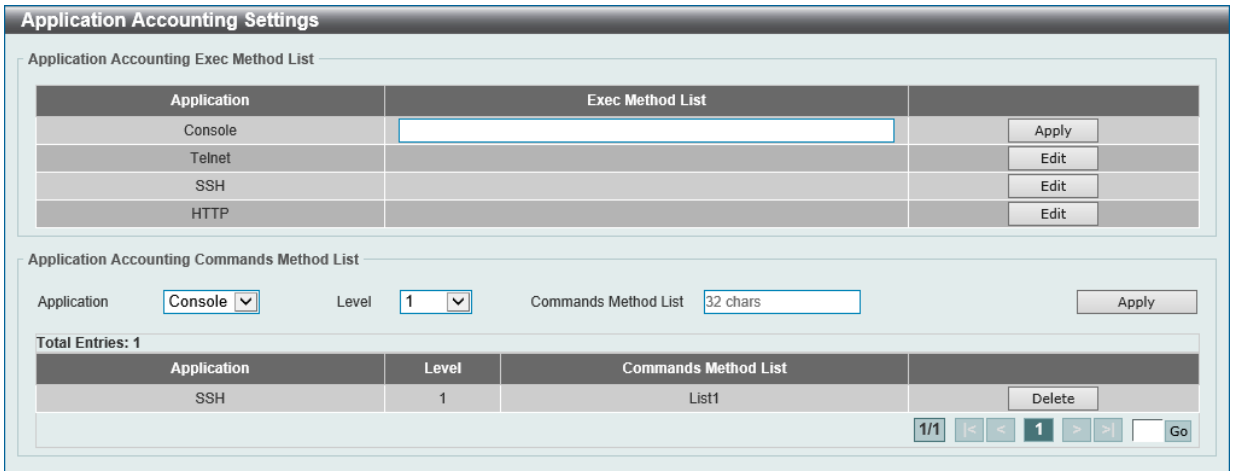


図 12-22　Application Accounting Settings (Edit) 画面

画面に表示される項目：

項目	説明
Application Accounting Exec Method List	
Exec Method List	「Edit」をクリックし、使用する EXEC メソッドリスト名を入力します。

項目	説明
Application Accounting Commands Method List	
Application	使用するアプリケーションを選択します。 • 選択肢：「Console」「Telnet」「SSH」
Level	権限レベルを指定します。 • 設定可能範囲：1-15
Commands Method List	使用するコマンドメソッドリスト名を入力します。

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

Authentication Settings（認証設定）

AAA ネットワークと EXEC 認証設定を行います。

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

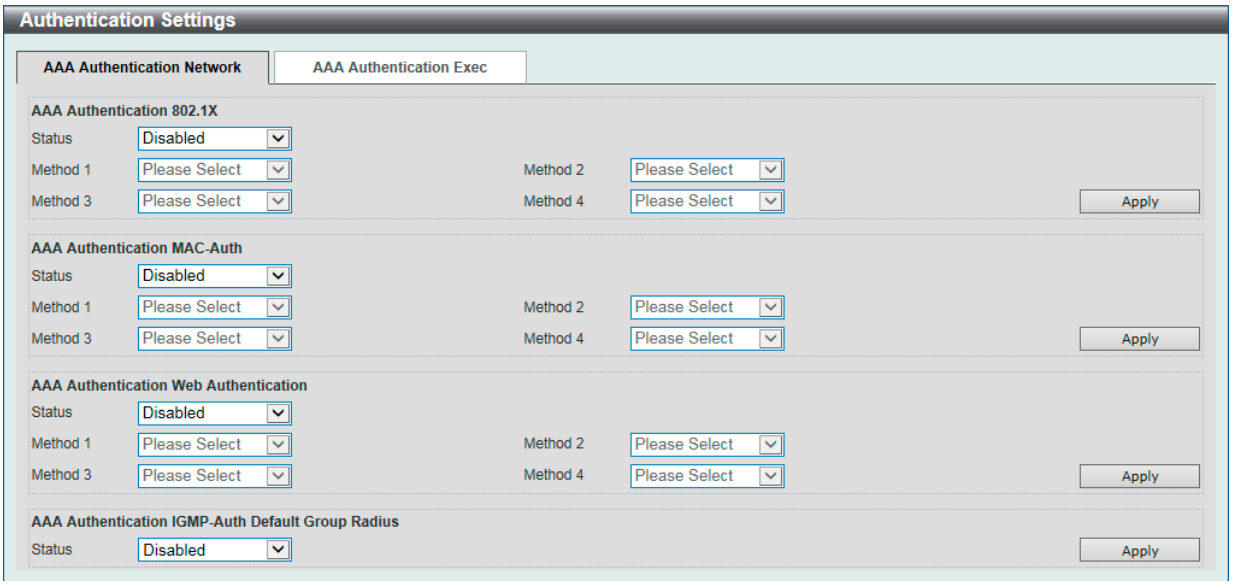


図 12-23　Authentication Settings 画面 -AAA Authentication Network タブ

「AAA Authentication Network」タブ

「AAA Authentication Network」タブ内の設定を行います。

画面に表示される項目：

項目	説明
AAA Authentication 802.1X	
Status	AAA 802.1X 認証ステータスを有効 / 無効に設定します。
Method 1 ～ 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- 認証にローカルデータベースを使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- 定義済みの RADIUS サーバを使用します。
AAA Authentication MAC-Auth	
Status	AAA MAC 認証ステータスを有効 / 無効に設定します。
Method 1 ～ 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- 認証にローカルデータベースを使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- 定義済みの RADIUS サーバを使用します。

項目	説明
AAA Authentication Web Authentication	
Status	AAA Web 認証ステータスを有効 / 無効に設定します。
Method 1 ～ 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- 認証にローカルデータベースを使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- 定義済みの RADIUS サーバを使用します。
AAA Authentication IGMP-Auth Default Group Radius	
Status	IGMP 認証のデフォルトメソッドリストを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

「AAA Authentication Exec」タブ

「AAA Authentication Exec」タブをクリックして、タブ内の設定を行います。

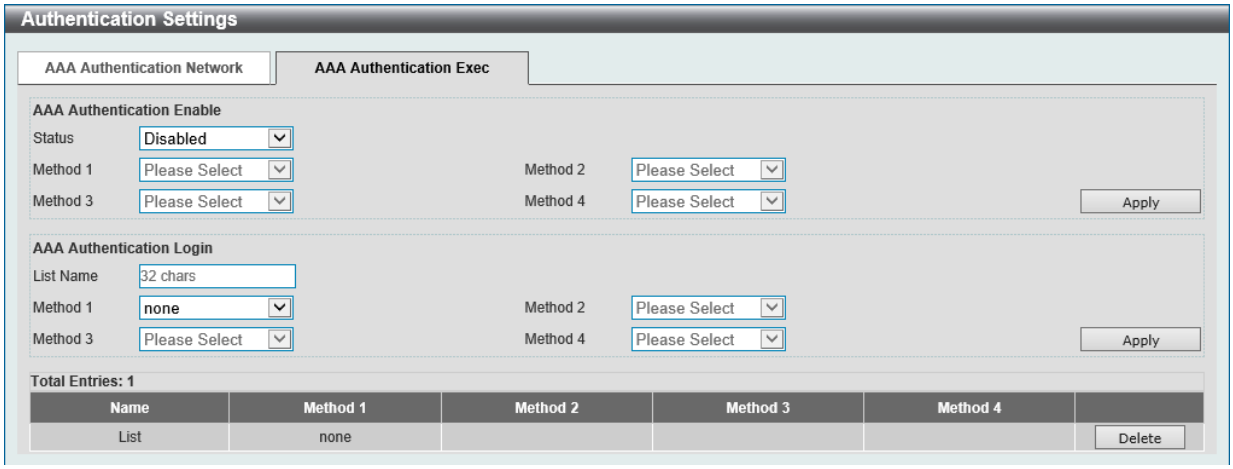


図 12-24　Authentication Settings 画面 -AAA Authentication Exec タブ

画面に表示される項目：

項目	説明
AAA Authentication Enable	
Status	AAA 認証 Enable ステータスを有効 / 無効に設定します。
Method 1 ～ 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「enable」- ローカル Enable パスワードを認証に使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- 定義済みの RADIUS サーバを使用します。 • 「tacacs+」- 定義済みの TACACS+ サーバを使用します。
AAA Authentication Login（AAA 認証ログイン）	
List Name	AAA 認証ログインオプションで使用するメソッドリスト名を入力します。
Method 1 ～ 4	使用するメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- ローカルデータベースを認証に使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- 定義済みの RADIUS サーバを使用します。 • 「tacacs+」- 定義済みの TACACS+ サーバを使用します。

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

Accounting Settings（アカウンティング設定）

AAA アカウンティングの設定を行います。

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

「AAA Accounting Network」タブ

「AAA Accounting Network」タブをクリックして、以下の画面を表示します。

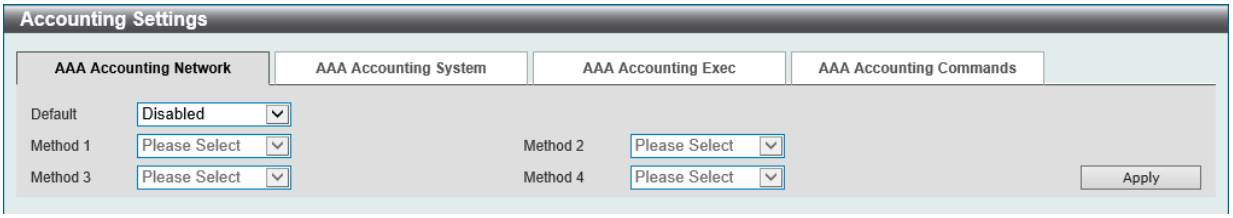


図 12-25　Accounting Settings 画面 - AAA Accounting Network タブ

画面に表示される項目：

項目	説明
Default	デフォルトのメソッドリストの使用を有効 / 無効に指定します。
Method 1 ～ 4	使用するメソッドリストを選択します。「None」オプションは「Method1」のみで設定可能です。 • 選択肢：「None」「Group」「RADIUS」「TACACS+」

「Apply」ボタンをクリックして、設定内容を適用します。

「AAA Accounting System」タブ

「AAA Accounting System」タブをクリックして、以下の画面を表示します。

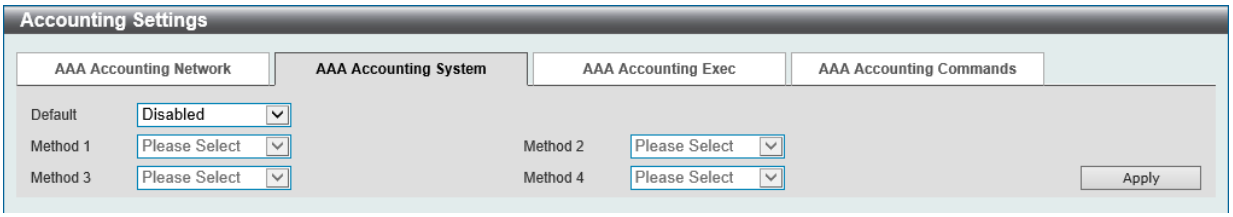


図 12-26　Accounting Settings 画面 - AAA Accounting System タブ

画面に表示される項目：

項目	説明
Default	デフォルトのメソッドリストの使用を有効 / 無効に指定します。
Method 1 ～ 4	使用するメソッドリストを選択します。「None」オプションは「Method1」のみで設定可能です。 • 選択肢：「None」「Group」「RADIUS」「TACACS+」

「Apply」ボタンをクリックして、設定内容を適用します。

「AAA Accounting Exec」タブ

「AAA Accounting Exec」タブをクリックして、以下の画面を表示します。

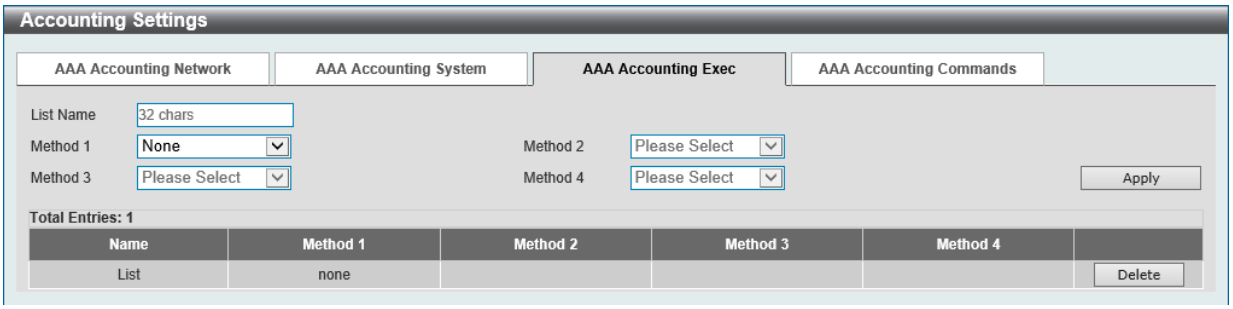


図 12-27　Accounting Settings 画面 - AAA Accounting Exec タブ

画面に表示される項目：

項目	説明
List Name	AAA アカウンティング EXEC オプションで使用するメソッドリスト名を入力します。
Method 1 ～ 4	使用するメソッドリストを選択します。「None」オプションは「Method1」のみで設定可能です。 • 選択肢：「None」「Group」「RADIUS」「TACACS+」

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

「AAA Accounting Commands」タブ

「AAA Accounting Commands」タブをクリックして、以下の画面を表示します。

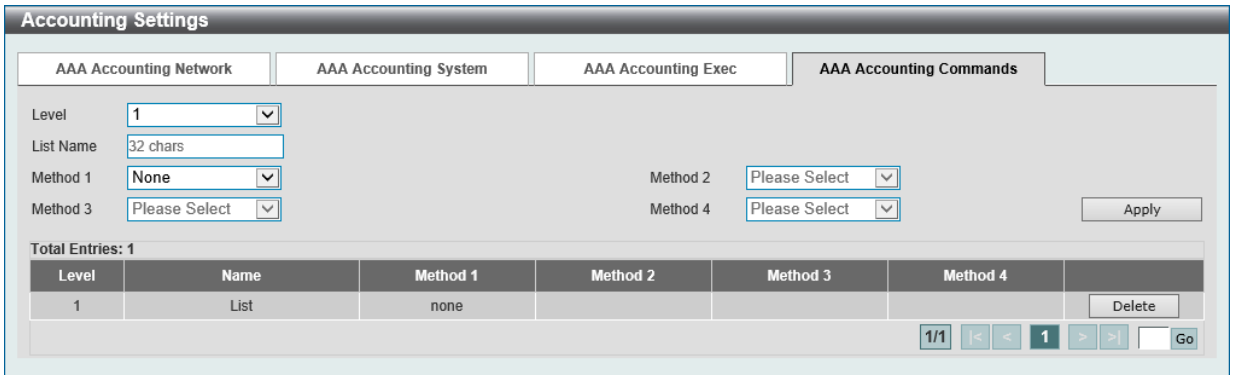


図 12-28　Accounting Settings 画面 - AAA Accounting Commands タブ

画面に表示される項目：

項目	説明
Level	権限レベルを指定します。 • 設定可能範囲：1-15
List Name	AAA アカウンティングコマンドオプションで使用するメソッドリスト名を入力します。
Method 1 ～ 4	使用するメソッドリストを選択します。「None」オプションは「Method1」のみで設定可能です。 • 選択肢：「None」「Group」「TACACS+」

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

Server RADIUS Dynamic Author Settings（RADIUS サーバダイナミックオーサー設定）

外部ポリシーサーバとの相互通信を行うために、スイッチを AAA サーバとして設定します。

Security > AAA > Server RADIUS Dynamic Author Settings の順にクリックし、以下の画面を表示します。

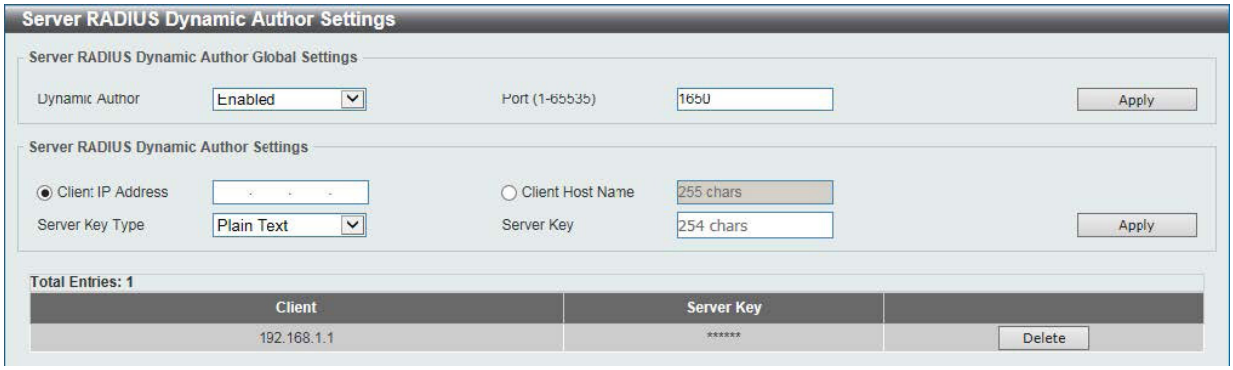


図 12-29　Server RADIUS Dynamic Author Settings 画面

画面に表示される項目：

項目	説明
Server RADIUS Dynamic Author Global Settings	
Dynamic Author	ダイナミック認証機能を有効 / 無効に設定します。
Port	RADIUS クライアントからの RADIUS リクエストをリッスンするポート番号を入力します。 • 設定可能範囲：1-65535
Server RADIUS Dynamic Author Settings	
Client IP Address	RADIUS クライアントの IP アドレスを入力します。
Client Host Name	RADIUS クライアントのホスト名を入力します。
Server Key Type	RADIUS キータイプを以下から選択します。 • 選択肢：「Plain Text」「Encrypted」
Server Key	RADIUS サーバとの通信で使用するキーを入力します。（254 文字以内）

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

RADIUS（RADIUS 設定）

RADIUS サーバの設定を行います。

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

RADIUS サーバのグローバルステータスを設定します。

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

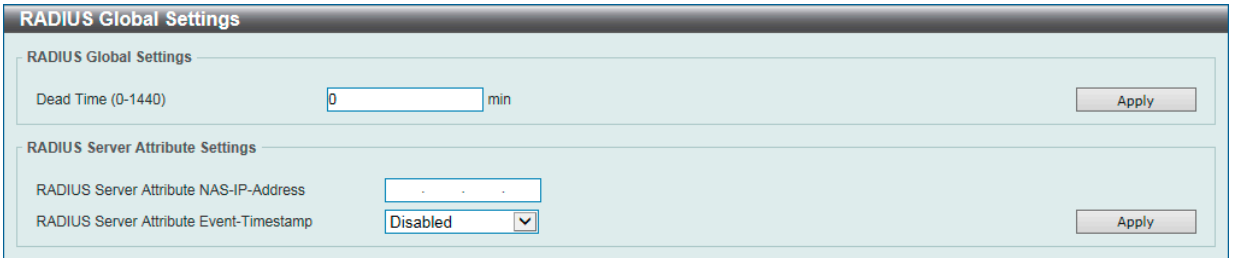


図 12-30　RADIUS Global Settings 画面

画面に表示される項目：

項目	説明
RADIUS Global Settings	
Dead Time	デッドタイムの設定を行います。 0 に設定されている場合、応答しないサーバは「Dead」として認識されることはありません。本設定により、応答しないサーバホストのエントリはスキップされ、認証プロセス時間が改善されます。 システムが認証サーバへ認証を行う際、一度に一台のサーバへの認証が試みられます。接続を試みたサーバが応答しない場合、システムは次のサーバに対して接続を試行します。応答しないサーバが検出されると、当該サーバはダウン状態として認識され、「デッドタイム」タイマが開始されます。それ以降のリクエスト認証はデッドタイム時間が経過するまでスキップされます。 • 設定可能範囲：0-1440（分） • 初期値：0（分）
RADIUS Server Attribute Settings	
RADIUS Server Attribute NAS-IP-Address	RADIUS パケットに含まれる RADIUS サーバ属性 4（NAS-IP アドレス）を指定します。
RADIUS Server Attribute Event-Timestamp	RADIUS サーバ属性のイベントタイムスタンプ機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

RADIUS Server Settings（RADIUS サーバの設定）

RADIUS サーバ設定を行います。

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

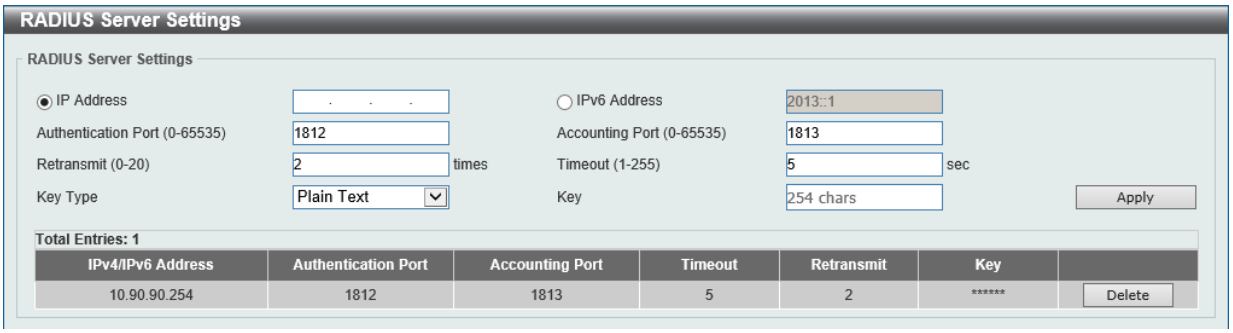


図 12-31　RADIUS Server Settings 画面

画面に表示される項目：

項目	説明
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。

項目	説明
Authentication Port	認証ポート番号を入力します。認証を使用しない場合は「0」を指定します。 • 設定可能範囲：0-65535 • 初期値：1812
Accounting Port	アカウンティングポート番号を入力します。アカウンティングを使用しない場合は「0」を指定します。 • 設定可能範囲：0-65535 • 初期値：1813
Retransmit	再送回数を設定します。このオプションを無効にする場合、「0」を指定します。 • 設定可能範囲：0-20（回） • 初期値：2（回）
Timeout	タイムアウト時間を設定します。 • 設定可能範囲：1-255（秒） • 初期値：5（秒）
Key Type	使用する鍵の種類を選択します。 • 選択肢：「Plain Text（平文）」「Encrypted（暗号化）」
Key	RADIUS サーバとの通信で使用する鍵を指定します。（254 文字以内）

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

RADIUS Group Server Settings（RADIUS グループサーバの設定）

RADIUS グループサーバの表示、設定を行います。

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

図 12-32　RADIUS Group Server Settings 画面

画面に表示される項目：

項目	説明
Group Server Name	RADIUS グループサーバ名を入力します。（32 文字以内）
IPv4 Address	RADIUS グループサーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS グループサーバの IPv6 アドレスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Show Detail」ボタンをクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

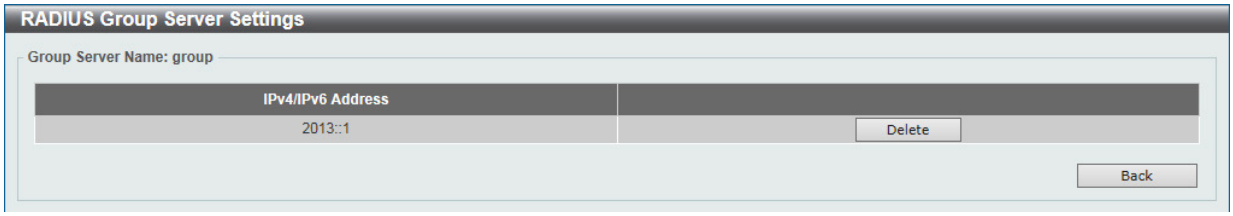


図 12-33　RADIUS Group Server Settings (Detail) 画面

「Delete」ボタンをクリックして、指定エントリを削除します。
前の画面に戻るには、「Back」ボタンをクリックします。

RADIUS Statistic（RADIUS 統計情報）

RADIUS 統計情報を表示、削除します。

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

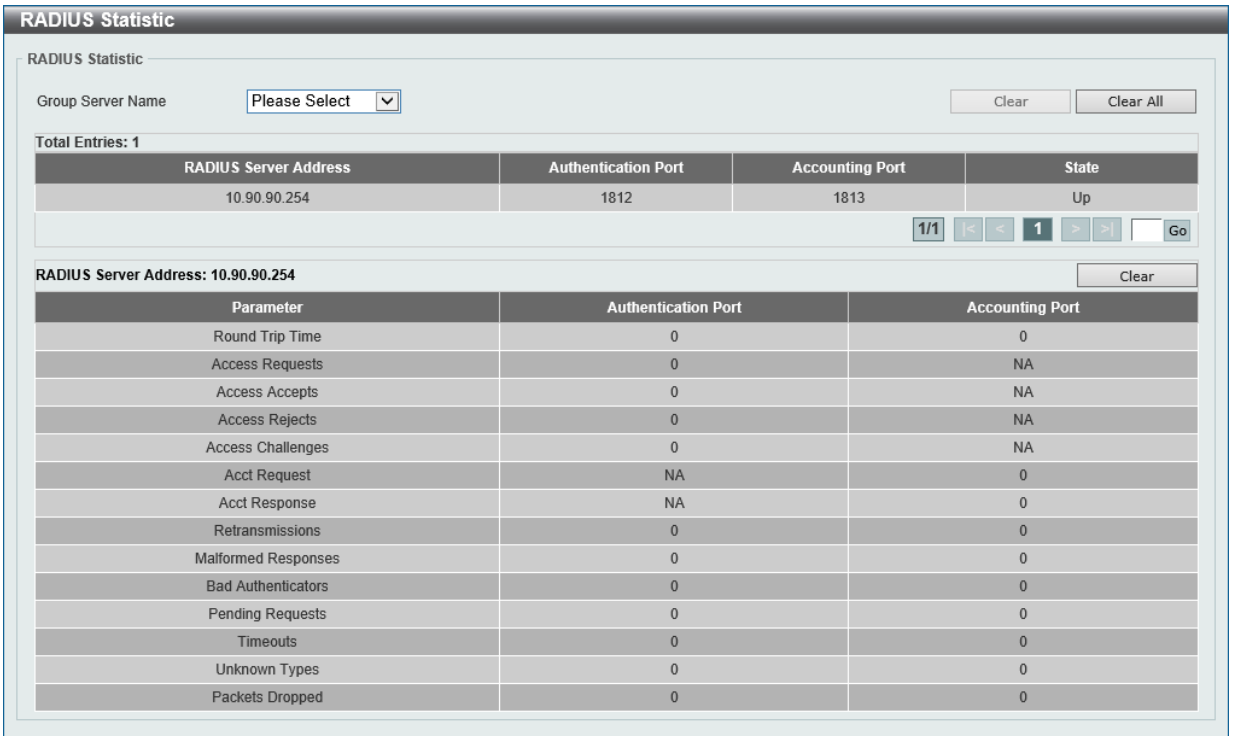


図 12-34　RADIUS Statistic 画面

画面に表示される項目：

項目	説明
Group Server Name	統計情報をクリアする RADIUS グループサーバ名を選択します。

「Clear」ボタンをクリックして、指定エントリの情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。
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。

TACACS+（TACACS+ 設定）

TACACS+ サーバの設定を行います。

TACACS+ Server Settings（TACACS+ サーバの設定）

TACACS+ サーバの表示、設定を行います。

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

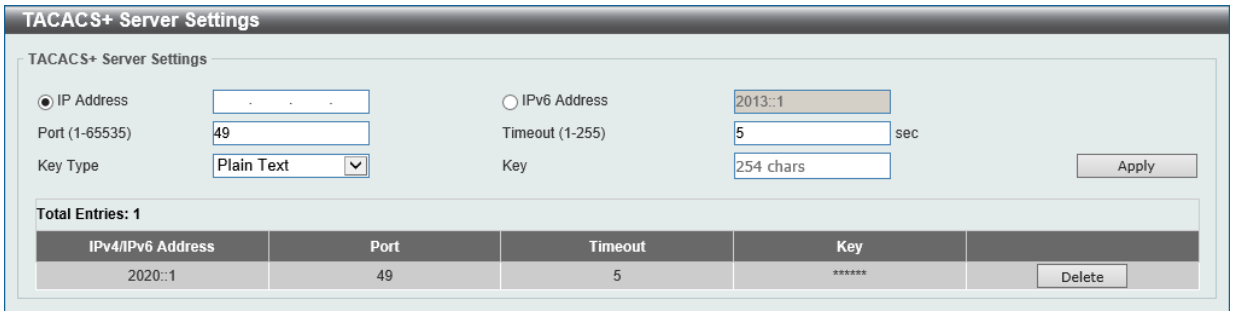


図 12-35　TACACS+ Server Settings 画面

画面に表示される項目：

項目	説明
IP Address	TACACS+ サーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ サーバの IPv6 アドレスを入力します。
Port	TACACS+ サーバのポート番号を入力します。 • 設定可能範囲：1-65535 • 初期値：49
Timeout	タイムアウト時間を設定します。 • 設定可能範囲：1-255（秒） • 初期値：5（秒）
Key Type	使用する鍵の種類を選択します。 • 選択肢：「Plain Text（平文）」「Encrypted（暗号化）」
Key	TACACS+ サーバとの通信で使用する鍵を指定します。（254 文字以内）

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

TACACS+ Group Server Settings（TACACS+ グループサーバの設定）

TACACS+ グループサーバの表示、設定を行います。

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

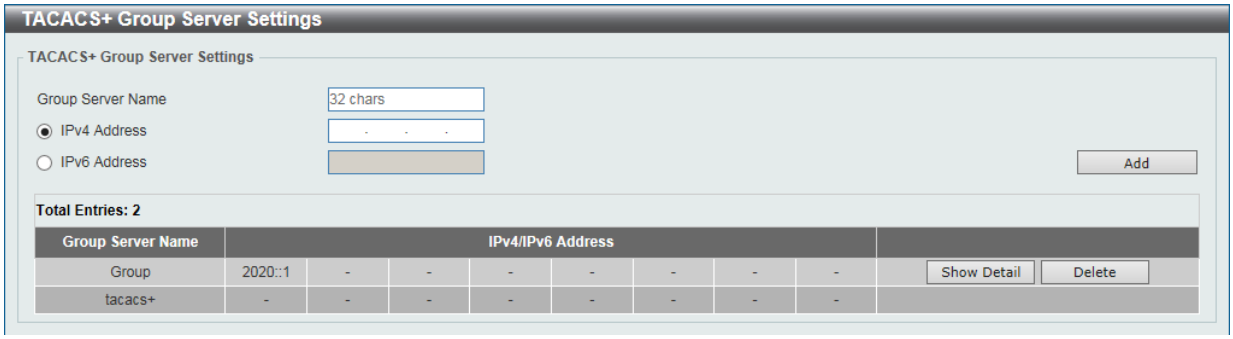


図 12-36　TACACS+ Group Server Settings 画面

画面に表示される項目：

項目	説明
Group Server Name	TACACS+ グループサーバ名を入力します。（32 文字以内）
IPv4 Address	TACACS+ グループサーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ グループサーバの IPv6 アドレスを入力します。

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

「Show Detail」ボタンをクリックして、TACACS+ グループサーバの詳細情報について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

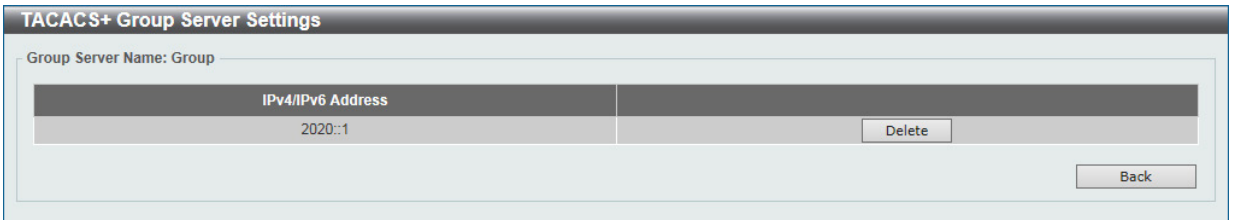


図 12-37　TACACS+ Group Server Settings（Show Detail）画面

「Delete」ボタンをクリックして、指定エントリを削除します。
前の画面に戻るには、「Back」ボタンをクリックします。

TACACS+ Statistic（TACACS+ 統計情報）

TACACS+ 統計情報を表示します。

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

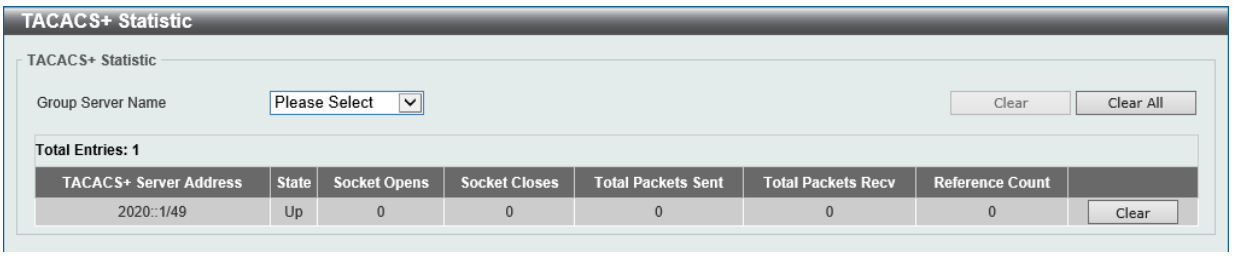


図 12-38　TACACS+ Statistic 画面

画面に表示される項目：

項目	説明
Group Server Name	統計情報を削除する TACACS+ グループサーバ名を選択します。

「Clear」ボタンをクリックして、指定エントリの情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。
テーブル内の「Clear」ボタンをクリックして、特定エントリの情報を消去します。

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

IMPB（IP-MAC-Port Binding) の設定を行います。

IP ネットワークレイヤ（IP レベル）では 4 バイトのアドレスを使用し、イーサネットリンクレイヤ（データリンクレベル）では 6 バイトの MAC アドレスを使用します。これらの 2 つのアドレスタイプを結びつけることにより、レイヤ間のデータ転送が可能になります。

IP-MAC バインディングの主な目的は、スイッチにアクセスするユーザを制限することです。IP アドレスと MAC アドレスのペアについて、事前に設定したデータベースと比較を行い、認証クライアントのみがスイッチのポートアクセスできるようにします。もしくは DHCP スヌーピングが有効な場合において、スイッチがスヌーピング DHCP パケットから自動的に IP/MAC ペアを学習し、IMPB ホワイトリストに保存することで、認証クライアントのポートアクセスが可能になります。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。本機能はポートベースであるため、ポートごとに本機能を有効 / 無効にすることができます。

IPv4

DHCPv4 Snooping（DHCPv4 スヌーピング）

■ DHCP Snooping Global Settings（DHCP スヌーピンググローバル設定）

DHCP スヌーピングのグローバル設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings の順にクリックして、以下の画面を表示します。

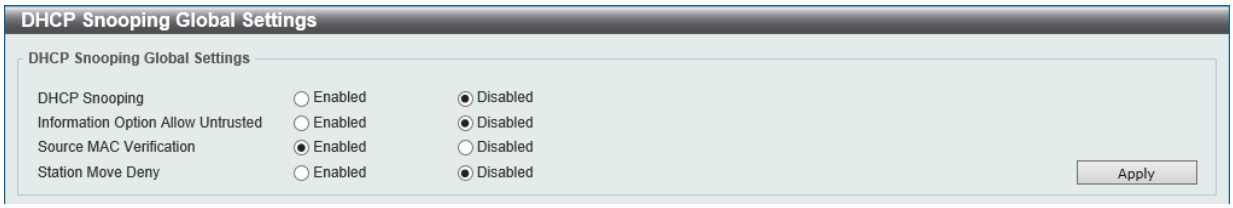


図 12-39　DHCP Snooping Global Settings 画面

画面に表示される項目：

項目	説明
DHCP Snooping	DHCP スヌーピングのグローバルステータスを有効 / 無効に設定します。
Information Option Allow Untrusted	信頼されていないインタフェースにおけるリレーオプション 82 付き DHCP パケットの許可を有効 / 無効に設定します。
Source MAC Verification	クライアントのハードウェアアドレスと DHCP パケットの送信元 MAC アドレスが一致しているかどうかの検証を有効 / 無効に設定します。
Station Move Deny	DHCP スヌーピングの端末移動拒否（Station Move Deny）を有効 / 無効に設定します。 端末移動を有効（本機能を無効）にすると、指定ポート上で同じ VLAN ID と MAC アドレスを持つダイナミック DHCP バインディングエントリは、同じ VLAN ID と MAC アドレスに属する新しい DHCP プロセスが検出された場合、他のポートへ移動することが可能です。

「Apply」ボタンをクリックして、設定内容を適用します。

■ DHCP Snooping Port Settings（DHCP スヌーピングポート設定）

DHCP スヌーピングポートの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings の順にクリックして、以下の画面を表示します。

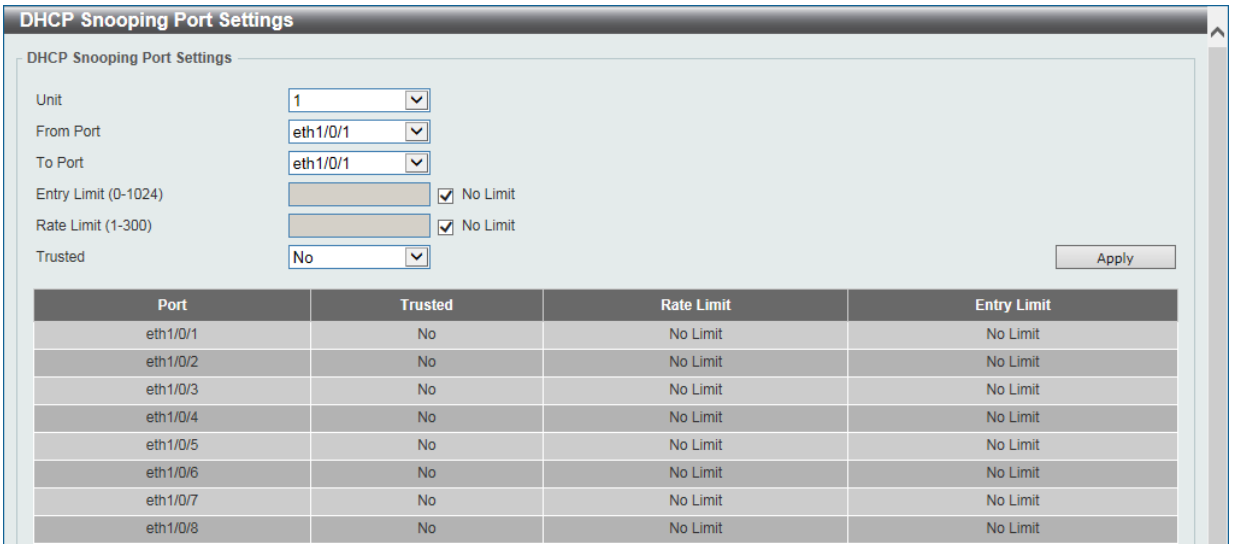


図 12-40　DHCP Snooping Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Entry Limit	エントリリミットの値を入力します。「No Limit」にチェックを入れると、本機能は無効になります。 • 設定可能範囲：0-1024
Rate Limit	レートリミットの値を入力します。「No Limit」にチェックを入れると、本機能は無効になります。 • 設定可能範囲：1-300
Trusted	信頼済みオプションを選択します。DHCP サーバや他のスイッチなどに接続しているポートは信頼済みインタフェースとして設定される必要があります。DHCP クライアントに接続しているポートは信頼されていないポートとして設定します。DHCP スヌーピングは DHCP サーバと信頼されていないインタフェースの間でファイアウォールとして動作します。 • 選択肢：「No」「Yes」

「Apply」ボタンをクリックして、設定内容を適用します。

■ DHCP Snooping VLAN Settings（DHCP スヌーピング VLAN 設定）

DHCP スヌーピング VLAN の設定、表示を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings の順にクリックして、以下の画面を表示します。

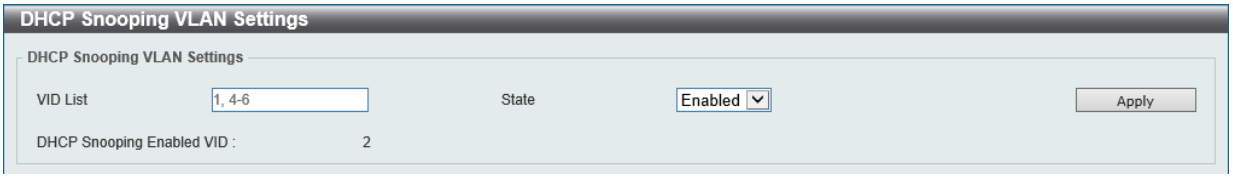


図 12-41　DHCP Snooping VLAN Settings 画面

画面に表示される項目：

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	DHCP スヌーピング VLAN を有効 / 無効に指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

■ DHCP Snooping Database（DHCP スヌーピングデータベース）

DHCP スヌーピングデータベースの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database の順にクリックして、以下の画面を表示します。

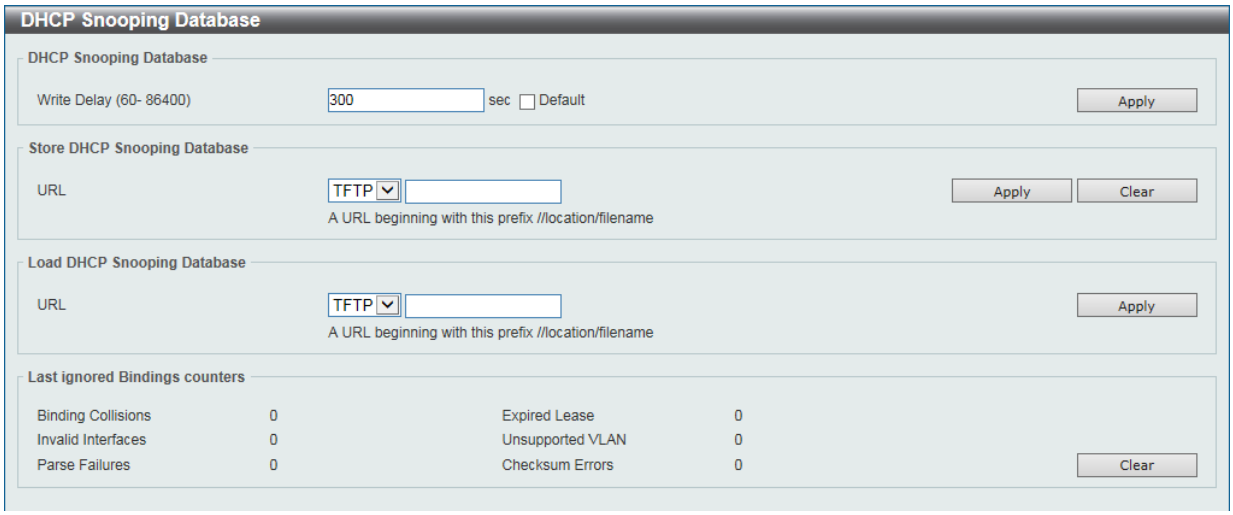


図 12-42　DHCP Snooping Database 画面

画面に表示される項目：

項目	説明
DHCP Snooping Database	
Write Delay	書き込み遅延時間の値を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：60-86400（秒） • 初期値：300（秒）
Store DHCP Snooping Database	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースの保存先 URL を入力します。 • 選択肢：「TFTP」「FTP」「Flash」
Load DHCP Snooping Database	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースの読み込み元 URL を入力します。 • 選択肢：「TFTP」「FTP」「Flash」

「Apply」ボタンをクリックして、設定内容を適用します。
「Store DHCP Snooping Database」セクションで「Clear」をクリックして、設定値をリセットします。
「Last ignored Bindings counters」セクションで「Clear」ボタンをクリックして、カウンタ情報を消去します。

■ DHCP Snooping Binding Entry（DHCP スヌーピングバインディングエントリ設定）

DHCP スヌーピングバインディングエントリの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry の順にクリックして、以下の画面を表示します。

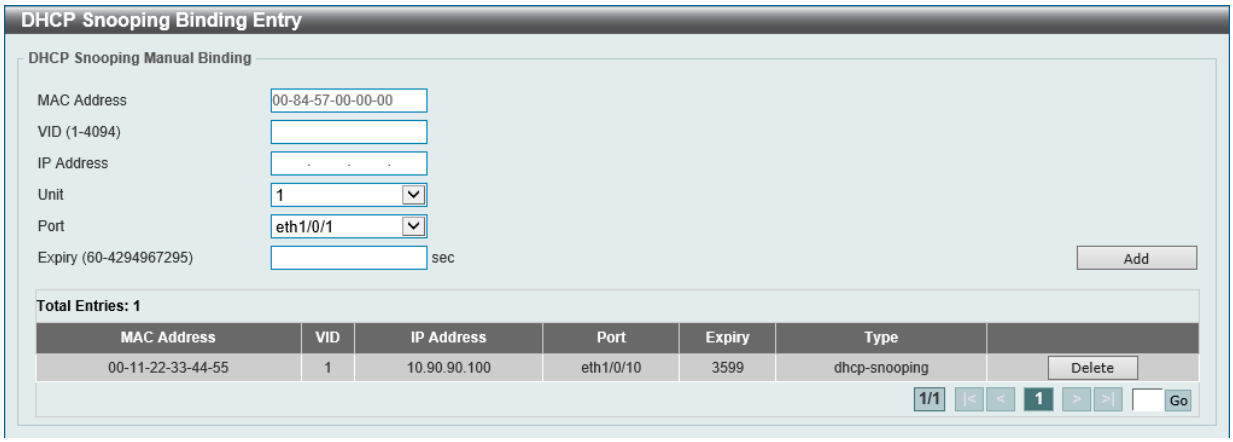


図 12-43　DHCP Snooping Binding Entry 画面

画面に表示される項目：

項目	説明
MAC Address	DHCP スヌーピングバインディングエントリの MAC アドレスを入力します。

項目	説明
VID	DHCP スヌーピングバインディングエントリの VLAN ID を入力します。 • 設定可能範囲：1-4094
IP Address	DHCP スヌーピングバインディングエントリの IP アドレスを入力します。
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポートを指定します。
Expiry	有効期限を入力します。 • 設定可能範囲：60-4294967295（秒）

「Add」ボタンをクリックして、入力した情報を基に新しいエントリを追加します。
「Delete」ボタンをクリックして、指定エントリを削除します。
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。

Dynamic ARP Inspection（ダイナミック ARP インスペクション）

■ ARP Access List（ARP アクセスリスト）

ARP アクセスリストの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List の順にクリックして、以下の画面を表示します。

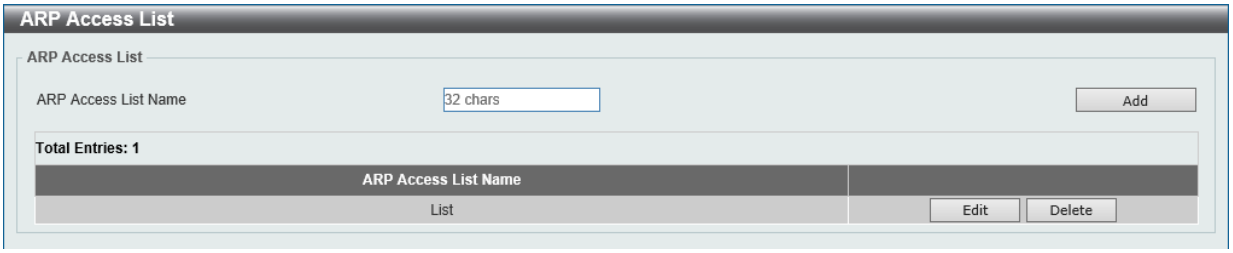


図 12-44　ARP Access List 画面

画面に表示される項目：

項目	説明
ARP Access List Name	ARP アクセスリスト名を入力します。（32 文字以内）

「Add」ボタンをクリックして、入力した情報を基に新しいエントリを追加します。
「Delete」ボタンをクリックして、指定エントリを削除します。

エントリの編集

「Edit」ボタンをクリックして指定のエントリを編集します。以下の画面が表示されます。

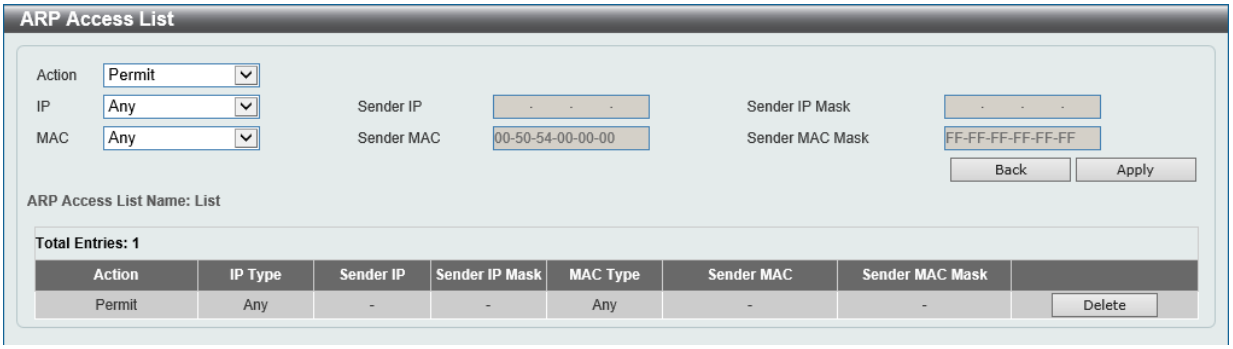


図 12-45　ARP Access List（Edit）画面

画面に表示される項目：

項目	説明
Action	実行するアクションを指定します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
IP	送信元 IP アドレスの種類を指定します。 • 選択肢：「Any」「Host」「IP with Mask」
Sender IP	IP アドレスの種類として「Host」「IP with Mask」を選択した場合、使用する送信元 IP アドレスを入力します。
Sender IP Mask	IP アドレスの種類として「IP with Mask」を選択した場合、使用する送信元 IP マスクを入力します。
MAC	送信元 MAC アドレスの種類を指定します。 • 選択肢：「Any」「Host」「MAC with Mask」
Sender MAC	MAC アドレスの種類として「Host」「MAC with Mask」を選択した場合、使用する送信元 MAC アドレスを入力します。
Sender MAC Mask	MAC アドレスの種類として「MAC with Mask」を選択した場合、使用する送信元 MAC マスクを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

「Delete」ボタンをクリックして、指定エントリを削除します。

■ ARP Inspection Settings（ARP インスペクション設定）

ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings の順にクリックして、以下の画面を表示します。

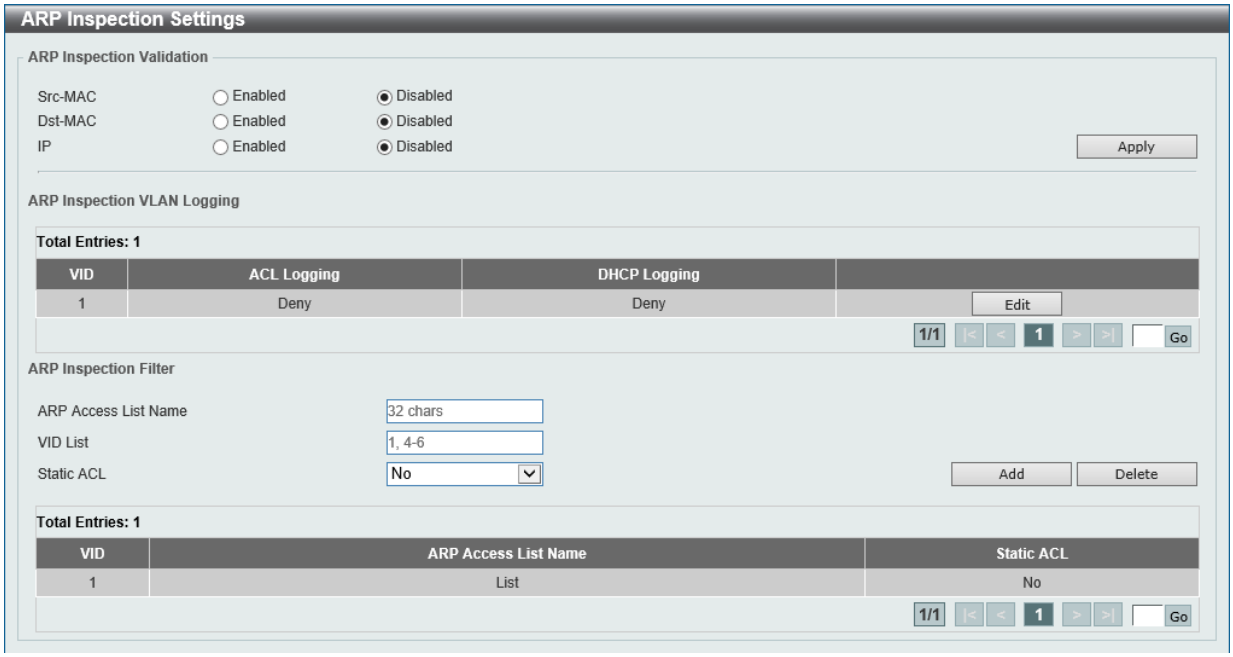


図 12-46　ARP Inspection Settings 画面

本画面の「ARP Inspection Validation」には以下の項目があります。

項目	説明
ARP Inspection Validation	
Src-MAC	送信元 MAC オプションについて有効 / 無効に設定します。 本オプションを有効にすると、ARP リクエストおよび応答パケットをチェックし、ARP ペイロードに含まれる送信元 MAC アドレスに対してイーサネットヘッダ内の送信元 MAC アドレスの整合性を検証します。
Dst-MAC	宛先 MAC オプションについて有効 / 無効に設定します。 本オプションを有効にすると、ARP 応答パケットをチェックし、ARP ペイロードに含まれる宛先 MAC アドレスに対してイーサネットヘッダ内の宛先 MAC アドレスの整合性を検証します。
IP	IP オプションについて有効 / 無効に設定します。 本オプションを有効にすると、不正な IP アドレスや予期せぬ IP アドレスがないか ARP の body をチェックします。また、ARP ペイロードにおける IP アドレスの妥当性もチェックします。ARP リクエストとレスポンスの両方の送信元 IP、および ARP レスポンスのターゲット IP が検証されます。IP アドレス「0.0.0.0」「255.255.255.255」宛のパケットとすべての IP マルチキャストは破棄されます。送信元 IP アドレスはすべての ARP リクエストとレスポンスにおいてチェックされ、宛先 IP アドレスは ARP レスポンス内のみでチェックされます。
ARP Inspection VLAN Logging	
ACL Logging	「Edit」をクリックして、ACL ロギングアクションを選択します。 • 選択肢：「Deny（拒否）」「Permit（許可）」「All（全て）」「None（なし）」
DHCP Logging	「Edit」をクリックして、ACL ロギングアクションを選択します。 • 選択肢：「Deny（拒否）」「Permit（許可）」「All（全て）」「None（なし）」
ARP Inspection Filter	
ARP Access List Name	ARP アクセスリスト名を入力します。（32 文字以内）
VID List	使用する VLAN ID リストを指定します。
Static ACL	スタティック ACL を使用するか否かを選択します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Edit」ボタンをクリックして、ACL/DHCP ロギングアクションを設定します。
「Add」ボタンをクリックして、入力した情報を基に新しいエントリを追加します。
「Delete」ボタンをクリックして、指定エントリを削除します。
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。

■ ARP Inspection Port Settings（ARP インスペクションポート設定）

ポートでの ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings の順にクリックして、以下の画面を表示します。

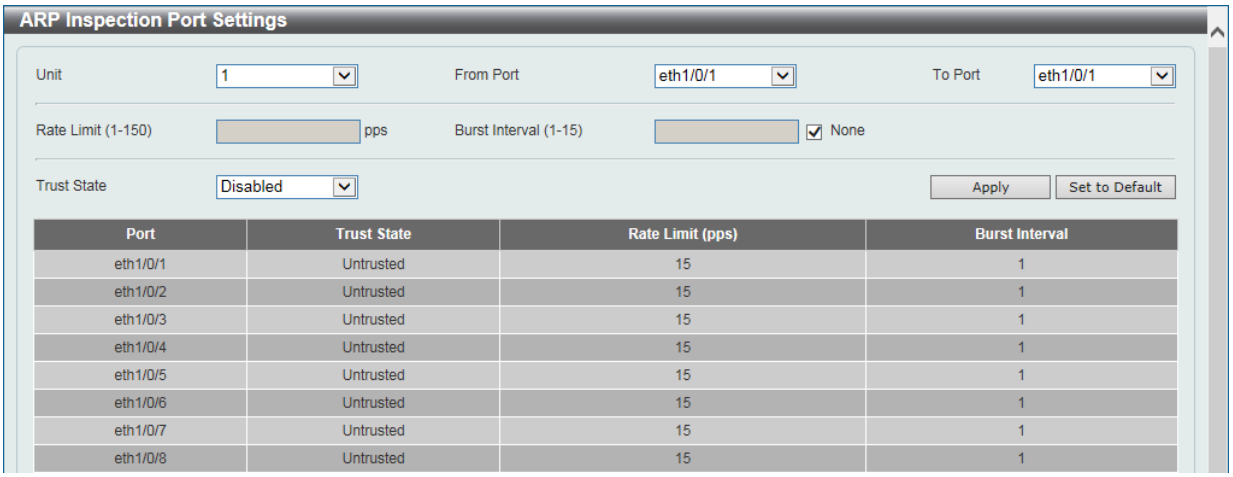


図 12-47　ARP Inspection Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Rate Limit	レート制限の値を入力します。「Burst Interval」横の「None」にチェックを入れるとオプションは無効になります。 • 設定可能範囲：1- 150（パケット / 秒）
Burst Interval	バーストインターバルの値を入力します。「None」にチェックを入れるとオプションは無効になります。 • 設定可能範囲：1-15
Trust State	トラストステータスを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Set to Default」ボタンをクリックすると、設定内容は初期値に変更されます。

■ ARP Inspection VLAN（ARP インスペクション VLAN 設定）

VLAN での ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN の順にクリックして、以下の画面を表示します。

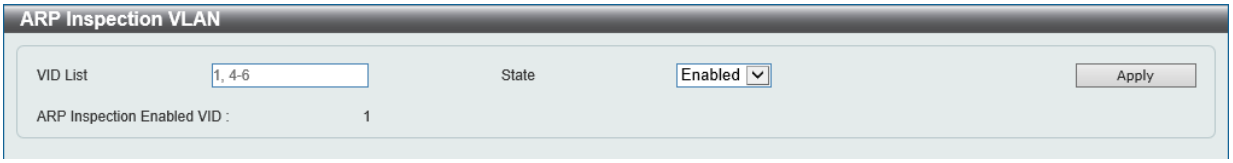


図 12-48　ARP Inspection VLAN 画面

画面に表示される項目：

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	指定 VLAN の ARP インスペクションについて有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

■ ARP Inspection Statistics（ARP インスペクション統計）

ARP インスペクションの統計情報の表示、消去を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics の順にクリックして、以下の画面を表示します。

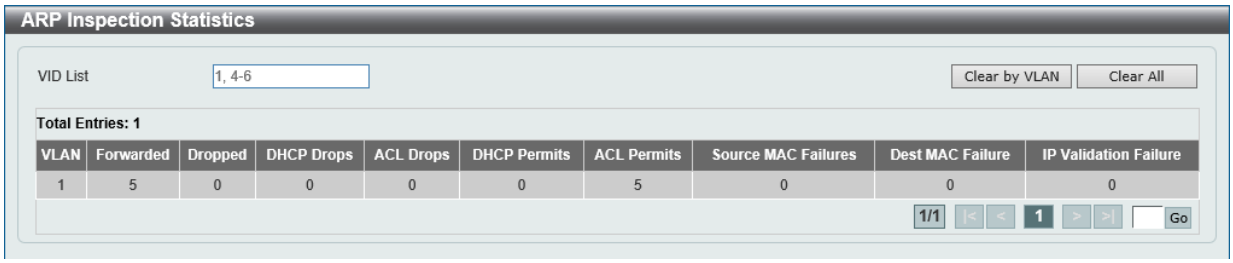


図 12-49　ARP Inspection Statistics 画面

画面に表示される項目：

項目	説明
VID List	統計情報を削除する VLAN ID リストを入力します。

「Clear by VLAN」ボタンをクリックして、入力した VLAN ID に基づき情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。
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。

■ ARP Inspection Log（ARP インスペクションログ）

ARP インスペクションログ情報の表示、消去、設定を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log の順にクリックして、以下の画面を表示します。

図 12-50　ARP Inspection Log 画面

画面に表示される項目：

項目	説明
Log Buffer	使用するログバッファの値を入力します。「Default」にチェックを入れると初期値を使用します。 • 設定可能範囲：1-1024 • 初期値：32

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear Log」ボタンをクリックして、ログを消去します。

IP Source Guard（IP ソースガード）

■ IP Source Guard Port Settings（IP ソースガードポート設定）

IP ソースガード（IPSG）の表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings の順にクリックして、以下の画面を表示します。

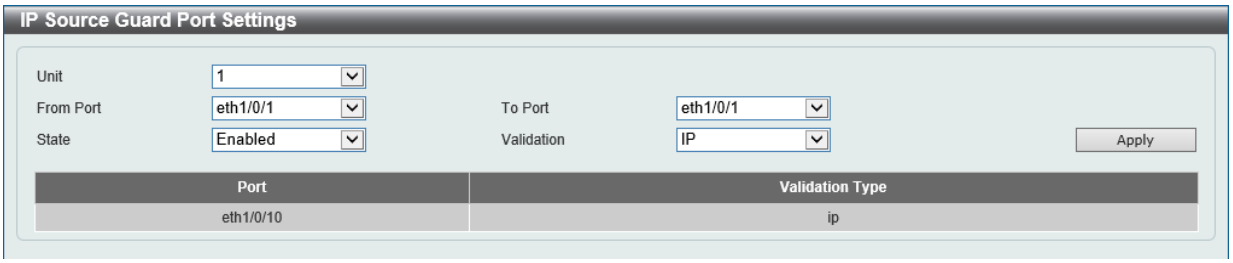


図 12-51　IP Source Guard Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポートを指定します。
State	指定ポートの IP ソースガードを有効 / 無効に設定します。
Validation	検証方法について選択します。 • 「IP」- 受信パケットの IP アドレスがチェックされます。 • 「IP-MAC」- 受信パケットの IP アドレスと MAC アドレスがチェックされます。

「Apply」ボタンをクリックして、設定内容を適用します。

■ IP Source Guard Binding（IP ソースガードバインディング）

IP ソースガードバインディングの表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding の順にクリックして、以下の画面を表示します。

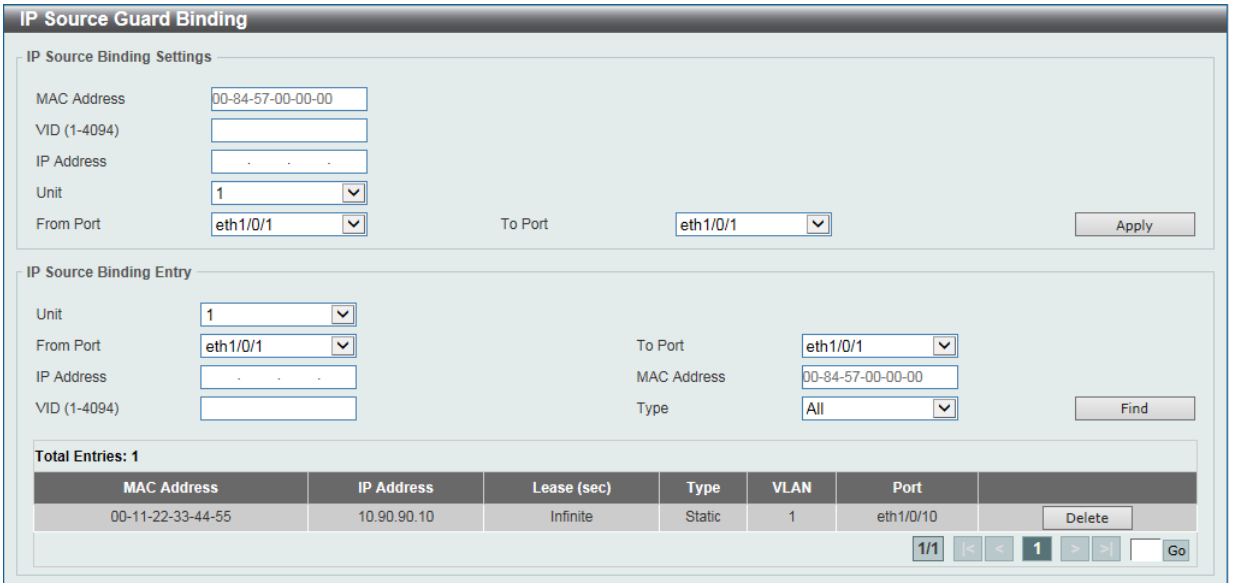


図 12-52　IP Source Guard Binding 画面

画面に表示される項目：

項目	説明
IP Source Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
IP Address	バインディングエントリの IP アドレスを入力します。
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

項目	説明
IP Source Binding Entry	
Unit	バインディングエントリを検索するユニットを指定します。
From Port/To Port	バインディングエントリを検索するポートの範囲を指定します。
IP Address	バインディングエントリの IP アドレスを入力します。
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
Type	バインディングエントリの種類を選択します。 • 「All」- すべての DHCP バインディングエントリが表示されます。 • 「DHCP Snooping」- DHCP バインディングスヌーピングによって学習された IP ソースガードバインディングエントリが表示されます。 • 「Static」- 手動で設定した IP ソースガードバインディングエントリが表示されます。

「Find」ボタンをクリックして、入力した情報を基に指定のエントリを表示します。
「Delete」ボタンをクリックして、指定エントリを削除します。
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。

■ IP Source Guard HW Entry（IP ソースガードハードウェアエントリ）

IP ソースガードハードウェアエントリの表示を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry の順にクリックして、以下の画面を表示します。

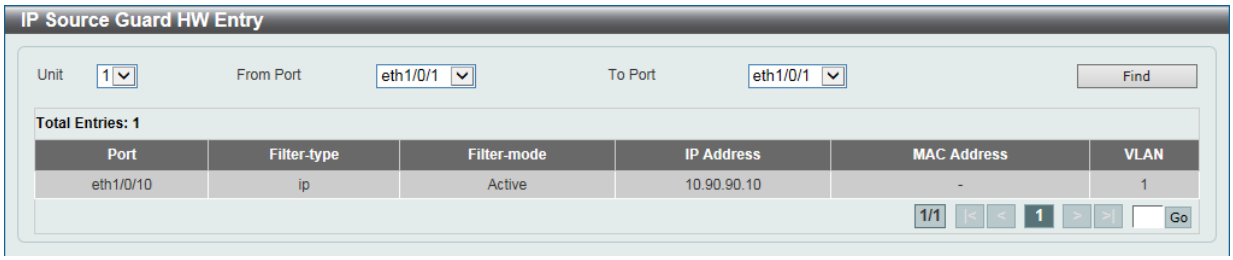


図 12-53　IP Source Guard HW Entry 画面

画面に表示される項目：

項目	説明
Unit	検索対象のユニットを指定します。
From Port/To Port	検索対象のポート範囲を指定します。

「Find」ボタンをクリックして、指定した情報を基にエントリを表示します。
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。

Advanced Settings（詳細設定）

■ IP-MAC-Port Binding Settings（IP-MAC ポートバインディング設定）

IP-MAC ポートバインディングの設定、表示を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings の順にクリックして、以下の画面を表示します。

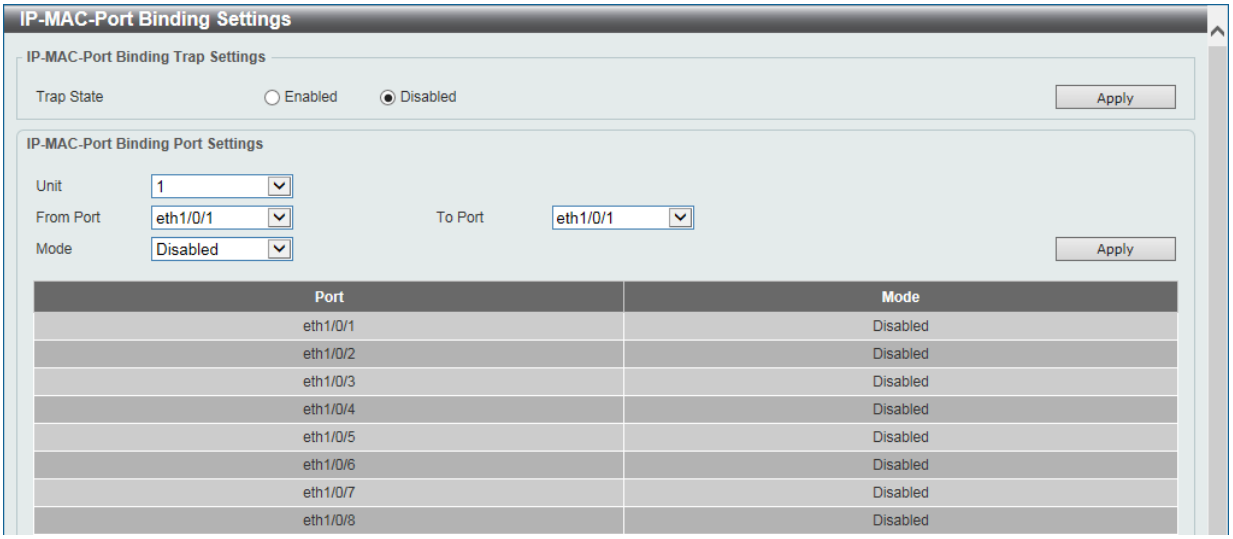


図 12-54　IP-MAC-Port Binding Settings 画面

画面に表示される項目：

項目	説明
IP-MAC-Port Binding Trap Settings	
Trap State	IP-MAC ポートバインディングのトラップ設定を有効 / 無効に指定します。
IP-MAC-Port Binding Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Mode	アクセスコントロールのモードを選択します。 • 「Disabled」- 指定ポートで IP-MAC ポートバインディング機能が無効になります。 • 「Strict」- ホストが ARP/IP パケット送信後、それらのパケットがバインディングチェックを通過した後のみ、ポートへアクセスできます。 • 「Loose」- ホストが ARP/IP パケット送信後、それらのパケットがバインディングチェックを通過しなかった場合にポートへのアクセスが拒否されます。 バインディングチェックを通過するには、送信元 IP アドレス / 送信元 MAC アドレス /VLAN ID/ 受信ポート番号が、IP ソースガードのスタティックバインディングエントリ、または DHCP スヌーピングによって学習されたダイナミックバインディングエントリのいずれかのエントリに一致する必要があります。

「Apply」ボタンをクリックして、設定内容を適用します。

■ IP-MAC-Port Binding Blocked Entry（IP-MAC ポートバインディングブロックエントリ）

IP-MAC ポートバインディングブロックエントリの表示、消去を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry の順にクリックして、以下の画面を表示します。

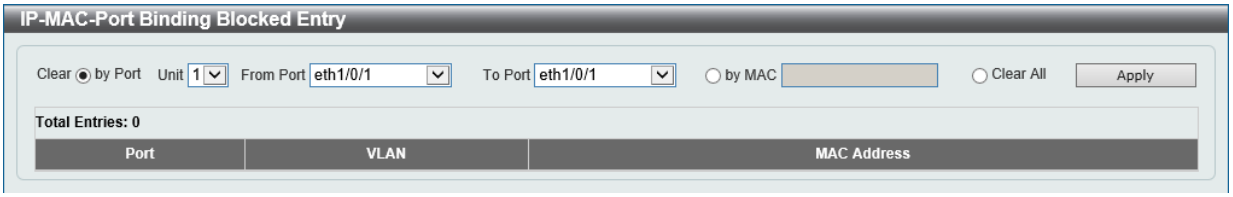


図 12-55　IP-MAC-Port Binding Blocked Entry 画面

画面に表示される項目：

項目	説明
Clear by Port	選択ポートに基づきエントリをクリアします。 • 「Unit」- エントリを削除するユニットを指定します。 • 「From Port/To Port」- エントリを削除するポート範囲を指定します。

項目	説明
Clear by MAC	指定した MAC アドレスに基づきエントリを消去します。入力欄に MAC アドレスを入力します。
Clear All	すべてのエントリを消去します。

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6

IPv6 Snooping（IPv6 スヌーピング）

IPv6 スヌーピングについて表示、設定します。

Security > IMPB > IPv6 > IPv6 Snooping の順にクリックして、以下の画面を表示します。

■ **IPv6 Snooping Policy Settings タブ**

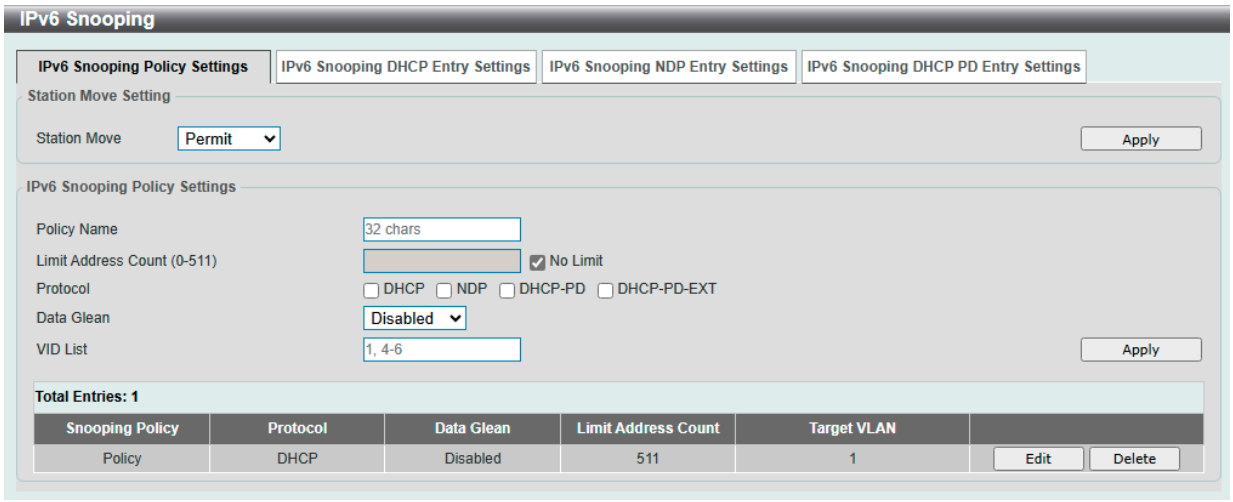


図 12-56　IPv6 Snooping 画面 - IPv6 Snooping Policy Settings タブ

画面に表示される項目：

項目	説明
	Station Move Setting
Station Move	ステーション移動について設定します。 • 「Permit（許可）」「Deny（拒否）」
	IPv6 Snooping Policy Settings
Policy Name	IPv6 スヌーピングポリシー名を入力します。（32 文字以内）
Limit Address Count	アドレスカウント制限の値を指定します。「No Limit」を指定するとアドレスカウント制限は無効になります。 • 設定可能範囲：0-511
Protocol	プロトコルステートを有効 / 無効に設定し、本ポリシーに対応するプロトコルを選択します。 • 「DHCP」- DHCPv6 パケットのアドレスがスヌーピングされます。 • 「NDP」- NDP パケットのアドレスがスヌーピングされます。 • 「DHCP-PD」- DHCPv6 PD パケットの IPv6 プレフィックスがスヌーピングされます。 • 「DHCP-PD-EXT」- DHCPv6 PD パケットの IPv6 プレフィックスがスヌーピングされます。PD スヌーピングは extension モードで動作します。 DHCPv6 スヌーピング： アドレス割り当ての際に DHCPv6 クライアントとサーバ間の DHCPv6 パケットをスヌーピングします。DHCPv6 クライアントが有効な IPv6 アドレスを取得すると、DHCPv6 スヌーピングによってバインディングデータベースが作成されます。 ND スヌーピング： ステートレス自動設定による IPv6 アドレスと手動設定による IPv6 アドレスのための機能です。IPv6 アドレスを割り当てる前に、ホストは「Duplicate Address Detection」（DAD：重複アドレス検出）を実行する必要があります。ND スヌーピングは DAD メッセージ（DAD NS と DAD NA）を受信しバインディングデータベースを構築します。NDP パケット (NS と NA) は、ホストが到達可能かを判断しバインディングを削除するかどうかを決定するためにも使用されます。 DHCP-PD スヌーピング： Prefix Delegation（PD）の DHCPv6 スヌーピングを実行して、（IPv6 プレフィックスを割り当てられた）委任ルータと、対応する要求ルータの間のバインディングを設定します。このバインディングはパケット内の送信元プレフィックスを検証するために使用されます。

項目	説明
Data Glean	データ収集機能を有効 / 無効に設定します。 DAD-NS パケット損失時やスイッチ再起動時など、バインディングテーブルで一部デバイスに対し有効な IPv6 アドレスが見つからない場合があります。このような場合、これらのデバイスとの間のトラフィックが IPv6 ソースガードによって拒否されます。データ収集機能を有効にすると、IPv6 重複アドレス検出（DAD）を使用して失われた IPv6 アドレスを回復することができます。
VID List	使用する VLAN ID リストを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」ボタンをクリックして、指定エントリを編集します。

■ IPv6 Snooping DHCP Entry Settings タブ

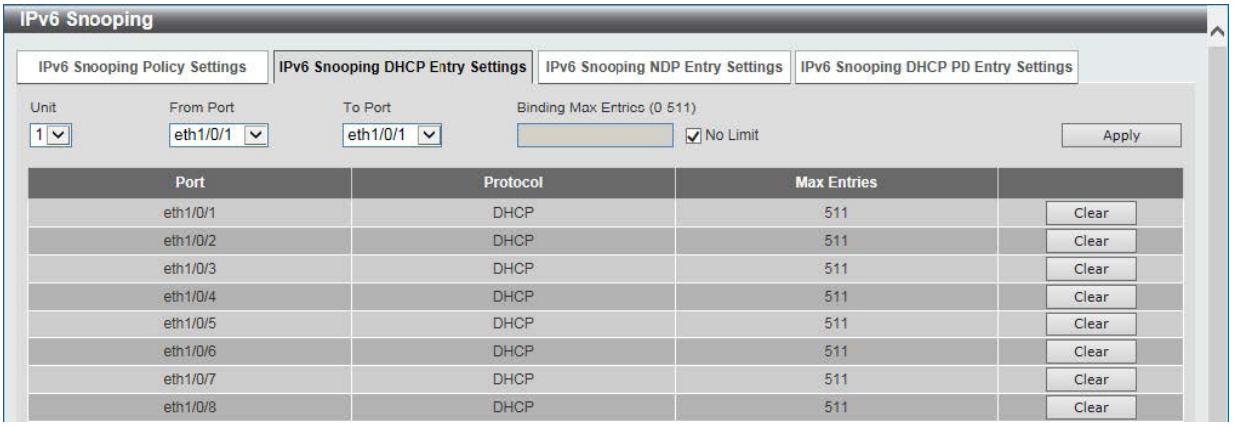


図 12-57　IPv6 Snooping 画面 - IPv6 Snooping DHCP Entry Settings タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Binding Max Entries	IPv6 スヌーピングバインディングエントリの最大数を指定します。「No Limit」にチェックを入れると、初期値を使用します。 設定可能範囲：0-511

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、指定ポートの DHCPv6 スヌーピングエントリを削除します。

■ IPv6 Snooping NDP Entry Settings タブ

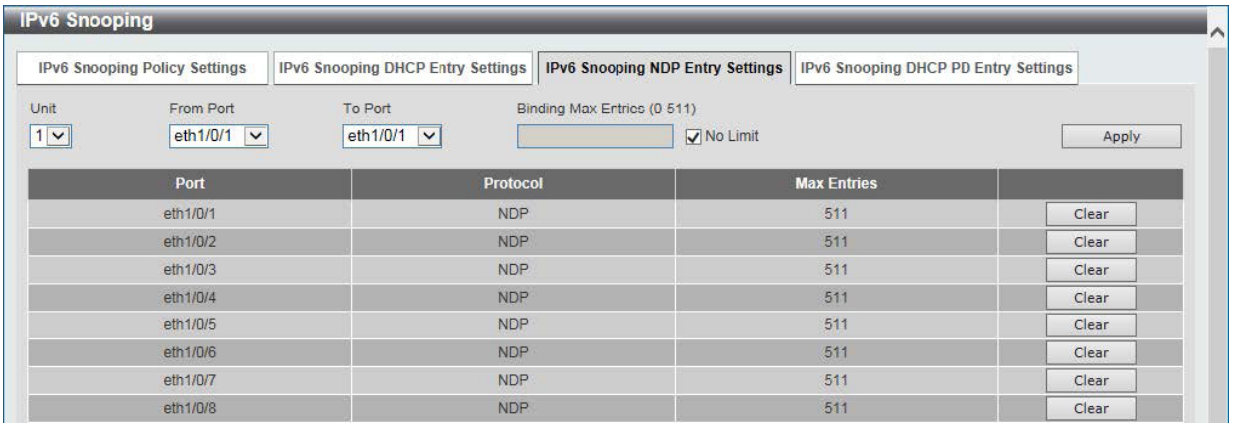


図 12-58　IPv6 Snooping 画面 - IPv6 Snooping NDP Entry Settings タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Binding Max Entries	IPv6 スヌーピングバインディングエントリの最大数を指定します。「No Limit」にチェックを入れると、初期値を使用します。 設定可能範囲：0-511

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、指定ポートの NDP スヌーピングエントリを削除します。

■ **IPv6 Snooping PD Entry Settings タブ**

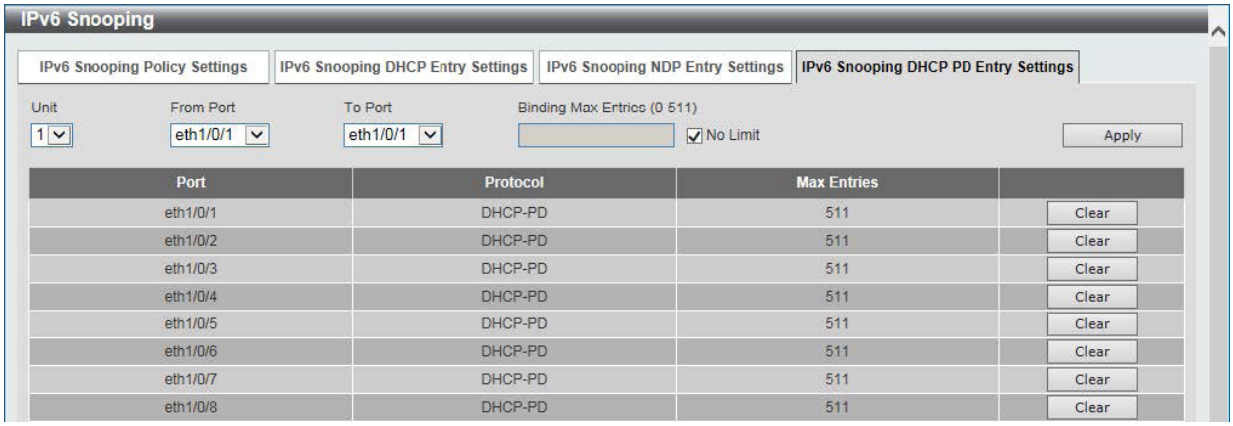


図 12-59　IPv6 Snooping 画面 - IPv6 Snooping DHCP Entry PD Settings タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Binding Max Entries	IPv6 スヌーピングバインディングエントリの最大数を指定します。「No Limit」にチェックを入れると、初期値を使用します。 設定可能範囲：0-511

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、指定ポートの PD スヌーピングエントリを削除します。

IPv6 ND Inspection（IPv6 ND インスペクション）

IPv6 ND インスペクションについて表示、設定します。

Security > IMPB > IPv6 > IPv6 ND Inspection の順にクリックして、以下の画面を表示します。

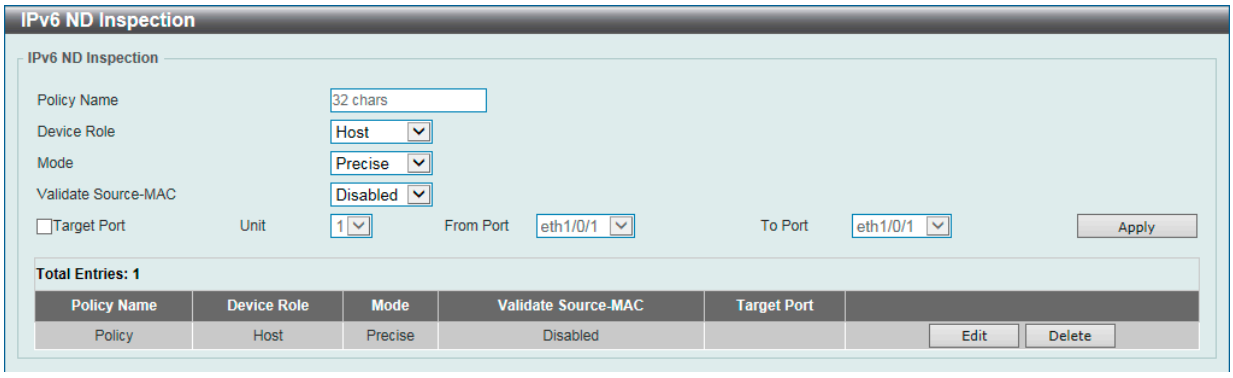


図 12-60　IPv6 ND Inspection 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 • 「Host」- デバイスの役割をホストに設定します。NS/NA メッセージに対するインスペクションが実行されます。（初期値） • 「Router」- デバイスの役割をルータに設定します。NS/NA に対するインスペクションは実行されません。 NS/NA インスペクションが実行されると、DHCP もしくは ND プロトコルから学習したダイナミックバインディングテーブルに対してメッセージの検証が行われます。
Mode	ND インスペクションのモードを選択します。 • 選択肢：「Precise」「Fuzzy」
Validate Source-MAC	送信元 MAC アドレスオプションの検証を有効 / 無効に設定します。 リンクレイヤアドレスを含む ND メッセージを受信した時に、リンクレイヤアドレスに対して送信元 MAC アドレスがチェックされます。リンクレイヤアドレスと MAC アドレスが異なる場合、パケットは破棄されます。
Target Port	本項目にチェックを入れ、ターゲットポートを指定します。
Unit	本設定を適用するユニットを選択します。

項目	説明
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」ボタンをクリックして、指定エントリを編集します。

IPv6 RA Guard（IPv6 RA ガード）

IPv6 RA ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 RA Guard の順にクリックして、以下の画面を表示します。

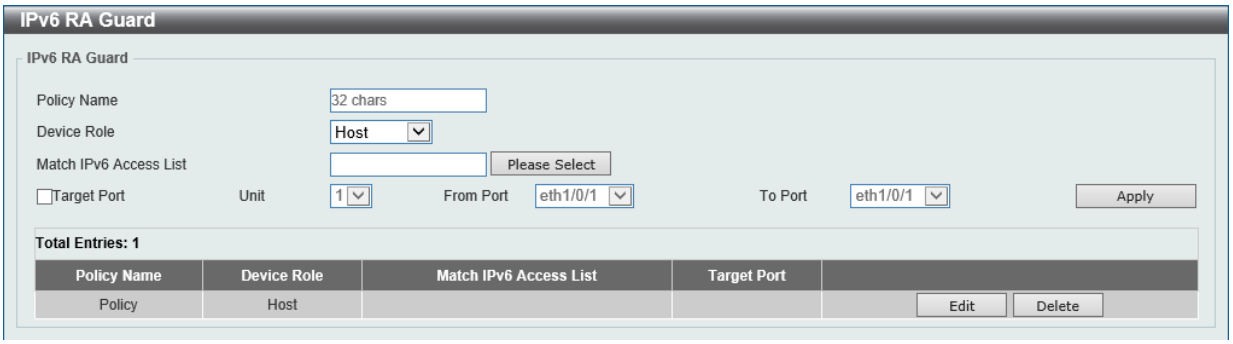


図 12-61　IPv6 RA Guard 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 ・「Host」- デバイスの役割をホストに設定します。RA パケットはすべてブロックされます。（初期値） ・「Router」- デバイスの役割をルータに設定します。RA パケットは、ポートに設定された ACL に従い転送されます。
Match IPv6 Access List	照合を行う IPv6 アクセスリストを入力します。 「Please Select」をクリックすると、既存の ACL を選択することができます。
Target Port	本項目にチェックを入れ、ターゲットポートを指定します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」ボタンをクリックして、指定エントリを編集します。

ACL 選択画面

「Please Select」をクリックすると次の画面が表示されます。

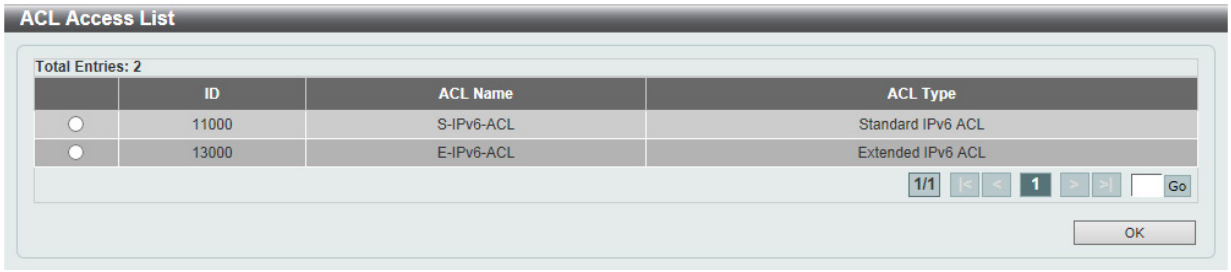


図 12-62　IPv6 RA Guard (Please Select) - ACL Access List 画面

設定するエントリを選択し、「OK」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。

IPv6 DHCP Guard（IPv6 DHCP ガード）

IPv6 DHCP ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 DHCP Guard の順にクリックして、以下の画面を表示します。

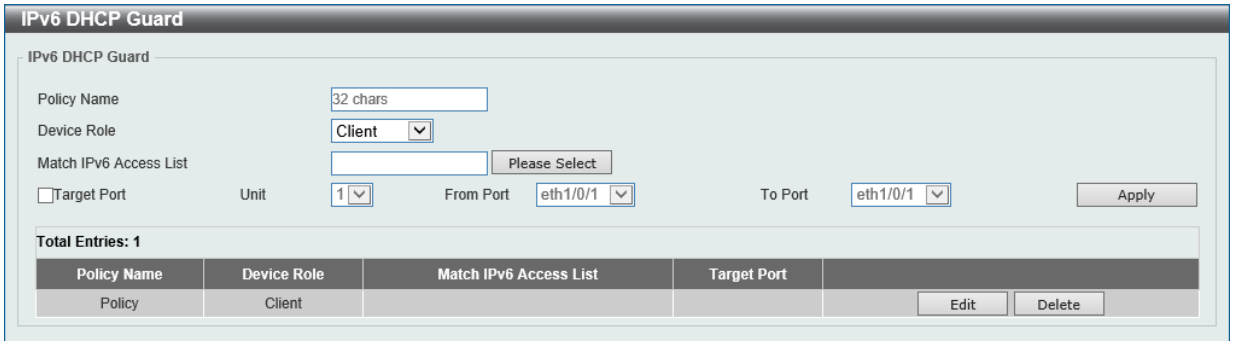


図 12-63　IPv6 DHCP Guard 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 • 「Client」- DHCPv6 サーバからの DHCPv6 パケットはすべてブロックされます。（初期値） • 「Server」- DHCPv6 サーバパケットはポートに設定された ACL に従い転送されます。
Match IPv6 Access List	照合する IPv6 アクセスリストを入力します。 「Please Select」をクリックすると、既存のエントリから選択することができます。
Target Port	本項目にチェックを入れ、ターゲットポートを指定します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」ボタンをクリックして、指定エントリを編集します。

ACL 選択画面

「Please Select」をクリックすると次の画面が表示されます。

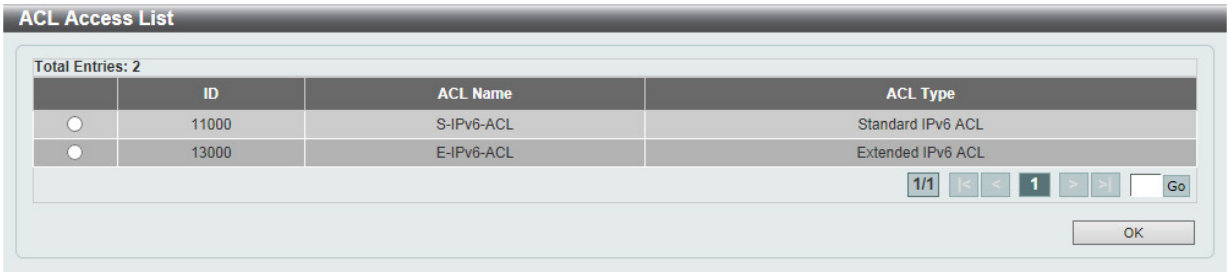


図 12-64　IPv6 DHCP Guard (Please Select) - ACL Access List 画面

設定するエントリを選択し、「OK」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。

IPv6 Source Guard（IPv6 ソースガード）

■ IPv6 Source Guard Settings（IPv6 ソースガード設定）

IPv6 ソースガードの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings の順にクリックして、以下の画面を表示します。

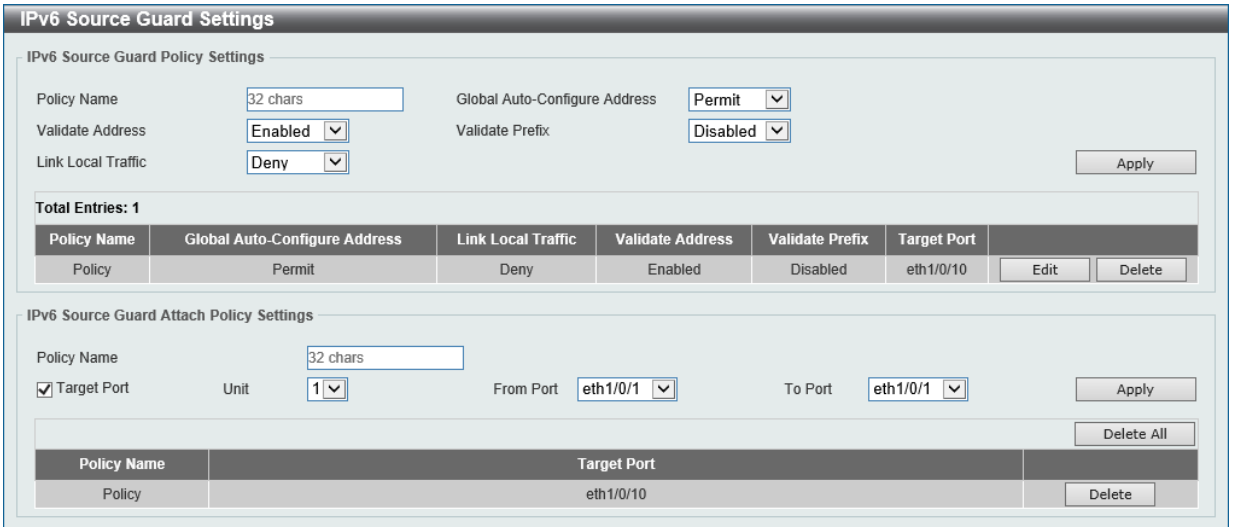


図 12-65　IPv6 Source Guard Settings 画面

画面に表示される項目：

項目	説明
IPv6 Source Guard Policy Settings	
Policy Name	ポリシー名を入力します。（32 文字以内）
Global Auto-Configure Address	自動設定グローバルアドレスからのデータトラフィックの許可 / 拒否を選択します。 リンク上のすべてのグローバルアドレスが DHCP によって割り当てられていて、ホスト自身による設定アドレスからのトラフィック送信をブロックしたい場合に役に立ちます。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Validate Address	アドレス検証機能を有効 / 無効に指定します。IPv6 ソースガードでアドレス検証機能を実行します。
Validate Prefix	プレフィックス検証機能を有効 / 無効に指定します。IPv6 ソースガードで IPv6 プレフィックスガード機能を実行します。
Link Local Traffic	ハードウェアによって許可された、リンクローカルアドレスからのデータトラフィックを許可 / 拒否します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
IPv6 Source Guard Attach Policy Settings	
Policy Name	ポリシー名を入力します。（32 文字以内）
Target Port	本項目にチェックを入れ、ターゲットポートを指定します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Delete All」ボタンをクリックして、すべてのエントリを削除します。

■ IPv6 Neighbor Binding（IPv6 隣接バインディング）

IPv6 隣接（ネイバ）バインディングの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding の順にクリックして、以下の画面を表示します。

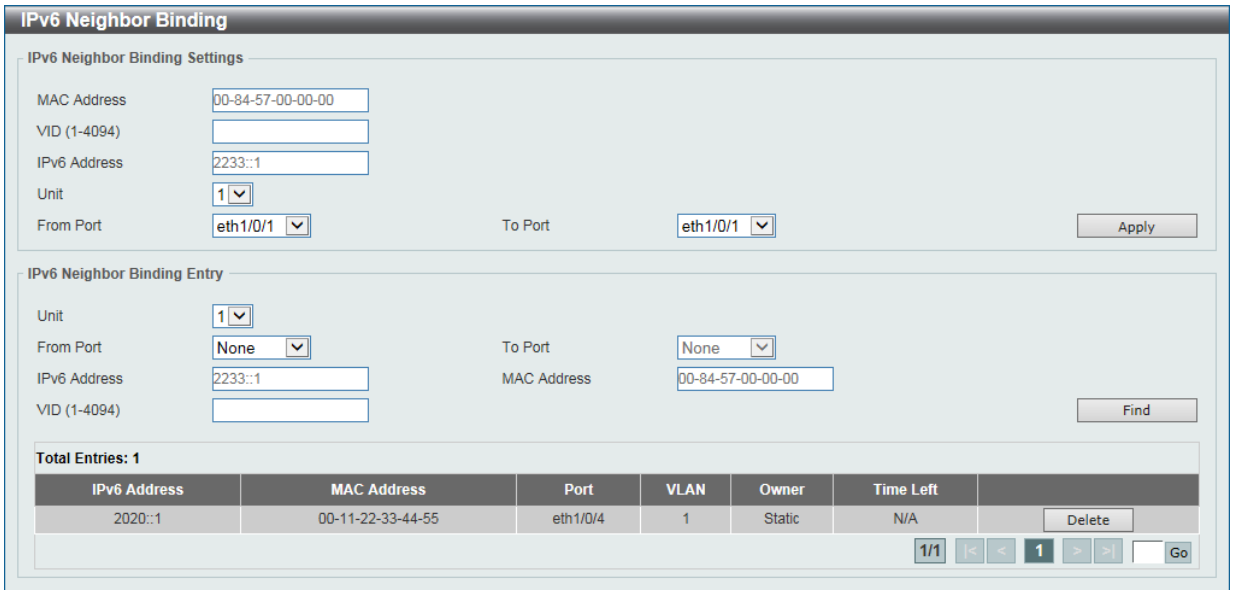


図 12-66　IPv6 Neighbor Binding 画面

画面に表示される項目：

項目	説明
IPv6 Neighbor Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。 • 設定可能範囲：1-4094
IPv6 Address	バインディングエントリの IPv6 アドレスを入力します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
IPv6 Neighbor Binding Entry	
Unit	バインディングエントリを表示するユニットを指定します。
From Port/To Port	バインディングエントリを表示するポート範囲を指定します。
IPv6 Address	検索する IPv6 アドレスを入力します。
MAC Address	検索する MAC アドレスを入力します。
VID	検索する VLAN ID を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Find」ボタンをクリックして、入力した情報を基に指定の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。

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

DHCP サーバパケットの制限や、DHCP クライアントが指定の DHCP サーバパケットを受信するように設定します。複数の DHCP サーバがネットワーク上に存在し、それぞれ異なる個別のクライアントグループに DHCP サービスを提供する場合に役立ちます。

ポートで DHCP サーバスクリーニング機能が有効になっている場合、このポートで受信したすべての DHCP サーバパケットは、ソフトウェアベースのチェックのために CPU にリダイレクトされます。 正当な DHCP サーバパケットは転送され、不正な DHCP サーバパケットは破棄されます。
DHCP サーバスクリーニング機能を有効にすると、すべての DHCP サーバパケットが特定のポートでフィルタリングされます。

DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）

DHCP サーバスクリーニングのグローバル設定を行います。

Security > DHCP Server Screening > DHCP Server Screening Global Settings 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。

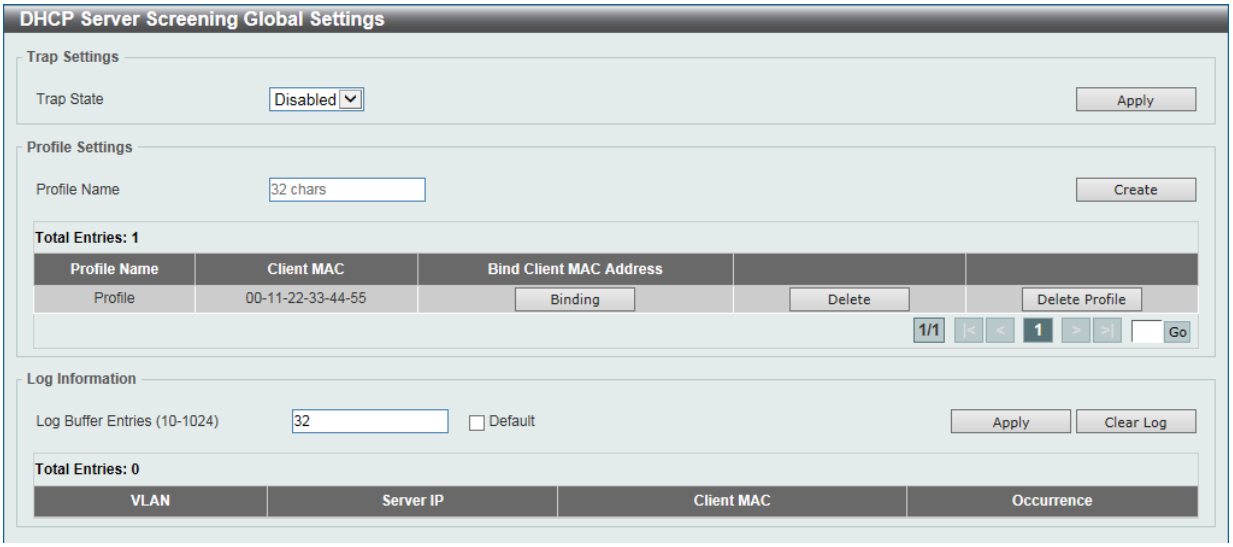


図 12-67　DHCP Server Screening Global Settings 画面

画面に表示される項目：

Trap Settings

項目	説明
Trap State	DHCP サーバスクリーニングのトラップ機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

Profile Settings

項目	説明
Profile Name	DHCP サーバスクリーニングのプロファイル名を入力します。（32 文字以内）

「Create」をクリックし、プロファイルを作成します。
「Binding」ボタンをクリックして、プロファイルでクライアント MAC アドレスを設定します。
「Delete」ボタンをクリックして、プロファイルから MAC アドレスの設定を削除します。
「Delete Profile」ボタンをクリックして、プロファイルを削除します。

Log Information

項目	説明
Log Buffer Entries	ログバッファエントリ数を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：10-1024 • 初期値：32

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear Log」ボタンをクリックして、ログを削除します。

「Binding」ボタンをクリックすると以下の画面が表示されます。

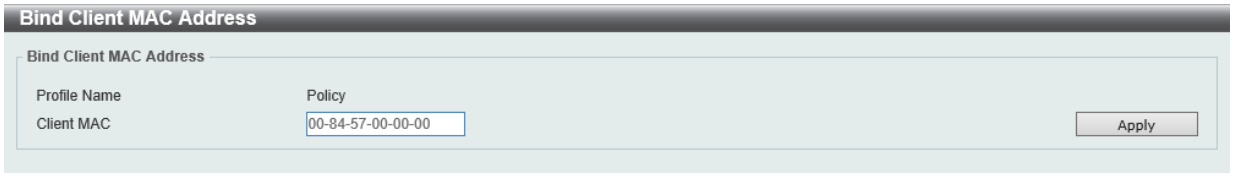


図 12-68　DHCP Server Screening Global Settings（Binding）- Bind Client MAC Address 画面

画面に表示される項目：

項目	説明
Client MAC	使用する MAC アドレスを指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

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

DHCP サーバスクリーニングポートの表示、設定を行います。

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

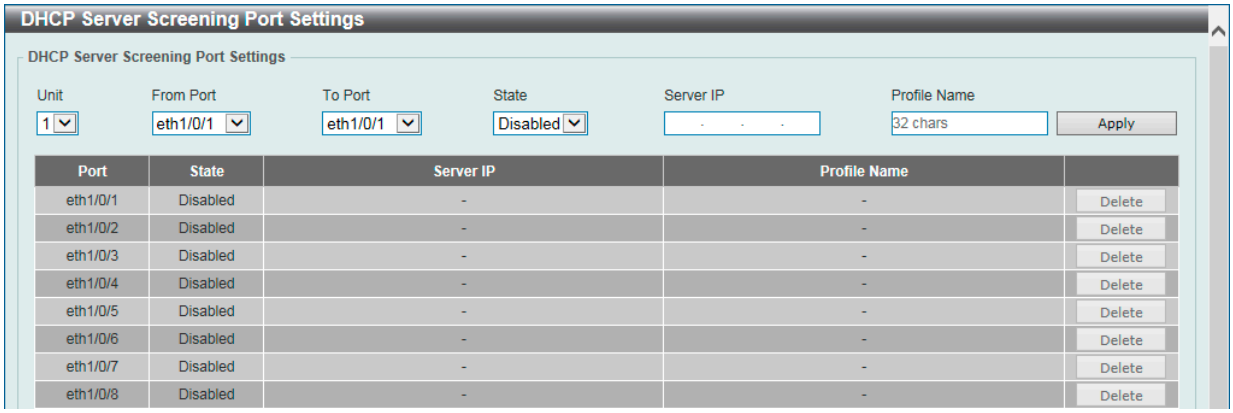


図 12-69　DHCP Server Screening Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
State	指定ポートでの DHCP サーバスクリーニング機能を有効 / 無効に設定します。
Server IP	DHCP サーバの IP アドレスを入力します。
Profile Name	ポートに設定する DHCP サーバスクリーニングプロファイル名を入力します。

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

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

ARP スプーフィング防止設定を表示および設定します。

ARP パケットの送信元 IP アドレスが指定のゲートウェイ IP アドレスと一致し、送信元 MAC アドレスが指定のゲートウェイ MAC アドレスと一致しない場合、パケットはシステムによって破棄されます。 ARP パケットの送信元 IP アドレスが指定のゲートウェイ IP アドレスと一致しない場合、ARP スプーフィング防止機能によりバイパスされます。

ARP アドレスが指定のゲートウェイの IP アドレス、MAC アドレス、およびポートリストと一致する場合、受信ポートが ARP により信頼済みか否かにかかわらず、ダイナミック ARP インスペクション（DAI）チェックをバイパスします。

Security > ARP Spoofing Prevention 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 12-70　ARP Spoofing Prevention 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Gateway IP	ゲートウェイの IP アドレスを入力します。
Gateway MAC	ゲートウェイの MAC アドレスを入力します。

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

BPDU Attack Protection（BPDU アタック防止設定）

スイッチのポートに BPDU 防止機能を設定します。
通常、BPDU 防止機能には 2 つの状態があります。1 つは正常な状態で、もう 1 つはアタック保護状態（Under attack）です。アタック保護状態には、3 つのモード（破棄、ブロックおよびシャットダウン）があります。BPDU 防止が有効なポートは、STP BPDU パケットを受信するとアタック保護状態に入ります。そして、設定に基づいてアクションを実行します。

BPDU 防止は、STP 機能における BPDU Forward 設定よりも高い優先度を持っています。つまり、ポートで BPDU Forward 設定が有効になっていても、BPDU 防止が有効である場合には、ポートは STP BPDU を転送しません。

また、BPDU 防止は BPDU トンネルポート設定よりも高い優先度を持っています。つまり、ポートが STP において BPDU トンネルポートとして設定されている場合、通常 STP BPDU を転送しますが、ポートで BPDU 防止が有効である場合には STP BPDU を転送しません。

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

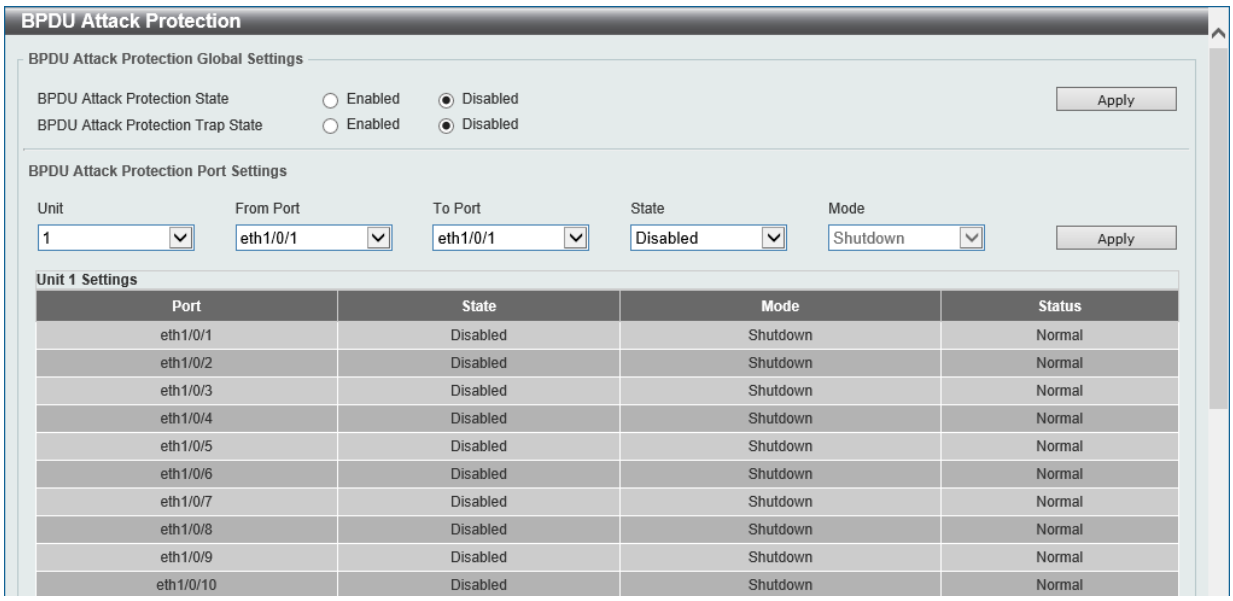


図 12-71　BPDU Attack Protection 画面

画面に表示される項目：

項目	説明
BPDU Attack Protection Global Settings	
BPDU Attack Protection State	BPDU アタック防止機能を有効 / 無効に設定します。
BPDU Attack Protection Trap State	BPDU アタック防止トラップの状態を有効 / 無効に設定します。
BPDU Attack Protection Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートに対して BPDU アタック防止機能を有効 / 無効に設定します。
Mode	BPDU 防止モードを指定します。 • 「Drop」- ポートがアタック保護状態に入ると、受信したすべての BPDU パケットを破棄します。 • 「Block」- ポートがアタック保護状態に入ると、すべてのパケット（BPDU と正常なパケットを含む）を破棄します。 • 「Shutdown」- ポートがアタック保護状態に入るとポートをシャットダウンします。

「Apply」ボタンをクリックして、設定内容を適用します。

NetBIOS Filtering（NetBIOS フィルタリング設定）

本項目では NetBIOS フィルタリングの設定、表示を行います。

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

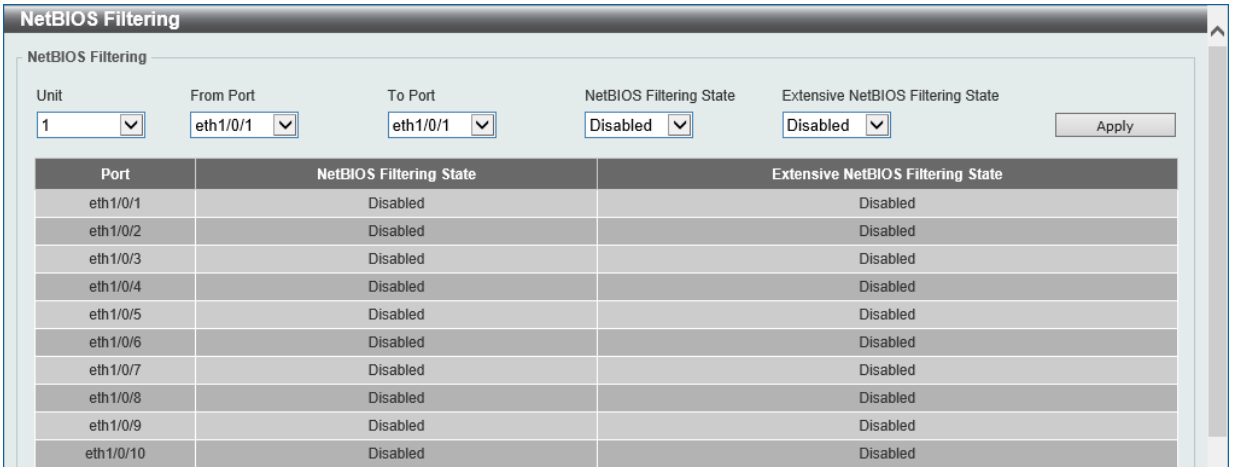


図 12-72　NetBIOS Filtering 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
NetBIOS Filtering State	指定ポートでの NetBIOS フィルタリングを有効 / 無効に設定します。 これにより物理ポートでの NetBIOS パケットが許可 / 拒否されます。
Extensive NetBIOS Filtering State	指定ポートでの Extensive NetBIOS フィルタリングを有効 / 無効に設定します。 これにより物理ポートでの 802.3 フレーム上の NetBIOS パケットが許可 / 拒否されます。

「Apply」ボタンをクリックして、設定内容を適用します。

MAC Authentication（MAC 認証）

MAC 認証機能は、MAC アドレスを使用してネットワークの認証を行う機能です。
本スイッチでは、ローカル認証方式、RADIUS サーバ認証方式の両方をサポートしています。
スイッチのローカルデータベースに基づいて認証を実行、またはスイッチが RADIUS クライアントとしてリモート RADIUS サーバとの間で RADIUS プロトコルを介して認証プロセスを実行します。

補足　RADIUS サーバを使った場合の MAC 認証の最大ユーザ数は 1,000 となります。

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

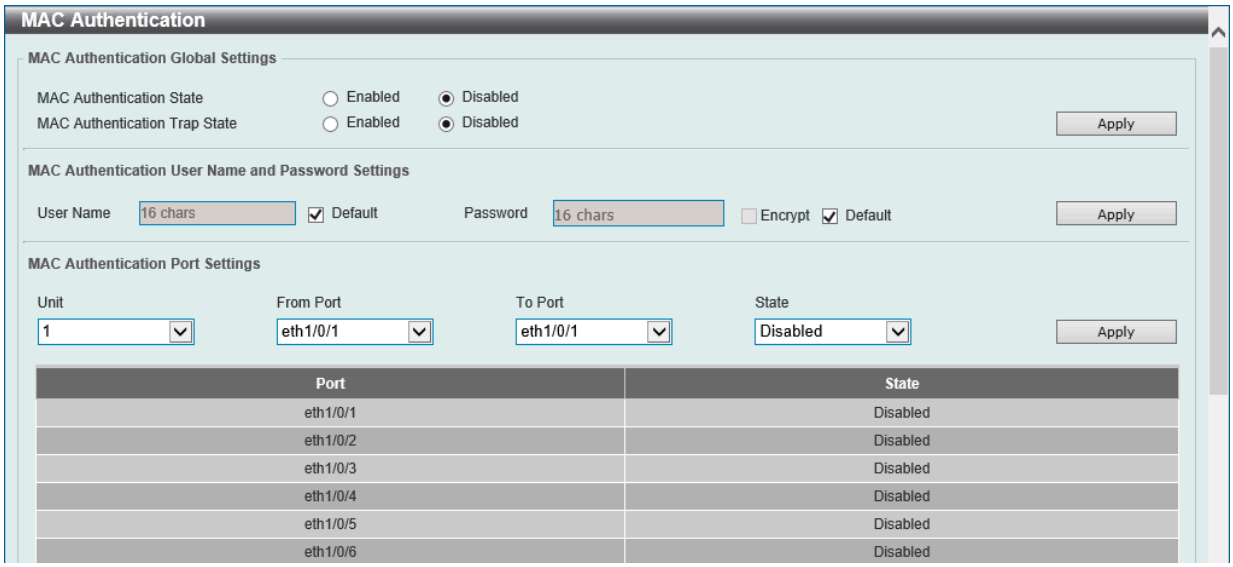


図 12-73　MAC Authentication 画面

画面に表示される項目：

項目	説明
MAC Authentication Global Settings	
MAC Authentication State	MAC 認証のグローバルステータスを有効 / 無効に設定します。
MAC Authentication Trap State	MAC 認証のトラップのステータスを有効 / 無効に設定します。
MAC Authentication User Name and Password Settings	
User Name	MAC 認証のユーザ名を入力します。（16 文字以内） 「Default」にチェックを入れると、クライアントの MAC アドレスがユーザ名として指定されます。
Password	MAC 認証のパスワードを入力します。 「Encrypt」にチェックを入れると、パスワードを暗号化します。 「Default」にチェックを入れると、クライアントの MAC アドレスがパスワードとして指定されます。
MAC Authentication Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定のポートに対し、MAC 認証を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

Web-based Access Control（Web 認証）

Web-based Access Control（WAC）は、ユーザがスイッチを経由してインターネットにアクセスを試みる際に、ユーザを認証する機能です。認証処理にはHTTP/HTTPS プロトコルが使用されます。ユーザがWeb ブラウザ経由でWebページ(例 : http://www.dlink.com) を閲覧しようとすると、スイッチは認証段階に進みます。スイッチにより HTTP/HTTPS パケットが検出され、ポートが未認証である場合、ユーザは認証ページにリダイレクトされます。認証処理が完了するまで、ユーザはインターネットにアクセスすることはできません。

スイッチは、認証サーバとしてローカルデータベースに基づく認証を行うか、RADIUS クライアントとしてリモート RADIUS サーバ経由による RADIUS プロトコルを利用した認証処理を実行します。クライアントユーザが Web へのアクセスを試みると、WAC の認証処理が開始されます。

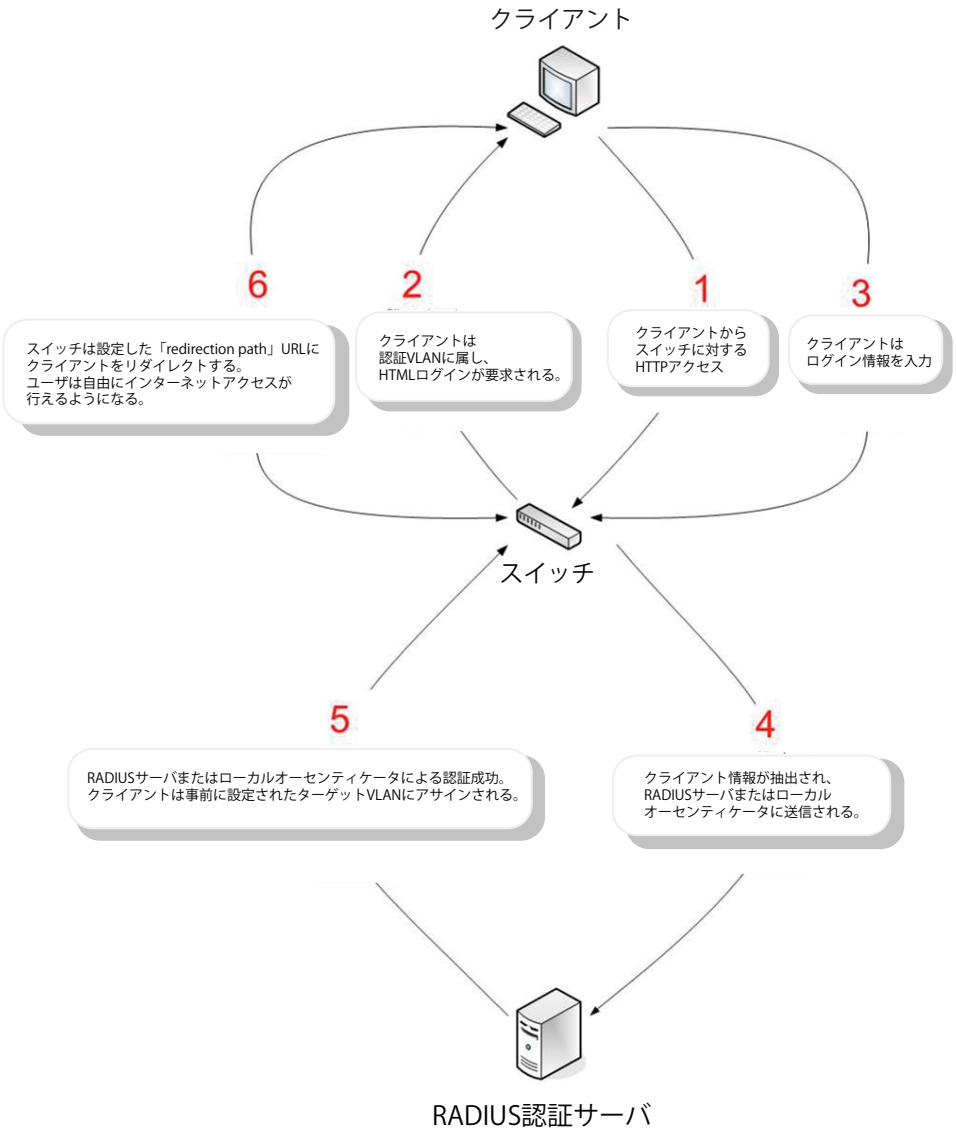
D-Link の WAC の実行には、WAC 機能が排他的に使用している仮想 IP が使用されます。この IP アドレスは、スイッチの他のモジュールには認識されません。スイッチの他の機能への影響を避けるため、WAC は仮想 IP アドレスのみを使用してホストとの通信を行います。従って、すべての認証要求は、スイッチの物理インタフェースの IP アドレスではなく仮想 IP アドレスに送信される必要があります。

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

認証された / 認証中のホストからの仮想 IP へのすべてのパケットは、スイッチの CPU で処理されます。そのため、仮想 IP が他のサーバや PC の IP アドレスと同じ場合、WAC が有効なポートに接続するホストは、その IP アドレスを実際に使用しているサーバや PC とは通信ができません。ホストがそれらのサーバや PC にアクセスする必要がある場合、仮想 IP をサーバや PC のアドレスと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、認証が適切に実行されるように、PC のユーザはプロキシの例外設定に仮想 IP を追加する必要があります。

スイッチの WAC 機能では、HTTP または HTTPS プロトコルに対し、ユーザ定義の TCP ポート番号を設定することができます。HTTP または HTTPS 用の TCP ポートは、認証処理において CPU で処理される HTTP /HTTPS パケットを識別したり、ログインページにアクセスしたりするために使用されます。ポート番号を指定しない場合、HTTP のポート番号の初期値は 80、HTTPS のポート番号の初期値は 443 となります。

次の図は、Web ベースのアクセスコントロールにおいて、各ノードで行われる認証プロセスの基本の 6 つのステップを例示しています。



条件および制限

1. クライアントが IP アドレスの取得に DHCP を使用している場合、IP アドレスを取得できるように、認証 VLAN に DHCP サーバまたは DHCP リレー機能を設定する必要があります。
2. アクセスプロファイル機能などの一部のスイッチ機能では、HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
3. 認証に RADIUS サーバを使用する場合、スイッチで Web 認証を有効にする前に、RADIUS サーバに対して適切な構成（ユーザ情報やターゲット VLAN など）を行ってください。

Web Authentication（Web 認証設定）

スイッチの Web 認証設定を行います。

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

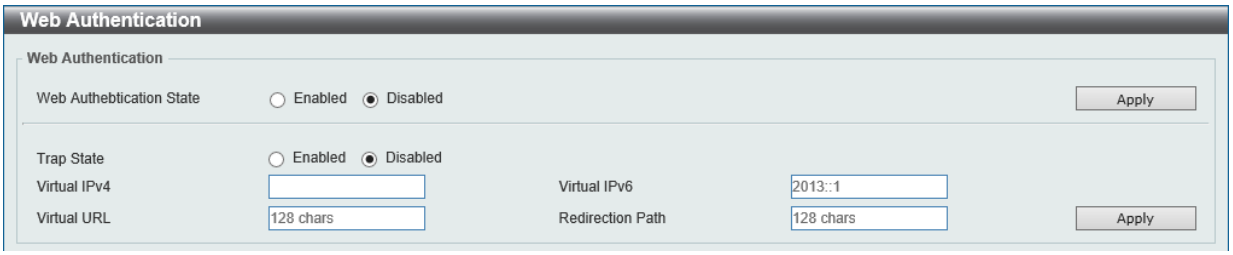


図 12-74　Web Authentication 画面

画面に表示される項目：

項目	説明
Web Authentication State	Web 認証機能のグローバルステータスを有効 / 無効に設定します。
Trap State	Web 認証のトラップの状態を有効 / 無効に設定します。
Virtual IPv4	仮想 IPv4 アドレスを入力します。 このアドレスは WAC 機能のみで使用されます。すべての Web 認証のプロセスはこの IPv4 アドレスを使用して行われますが、仮想 IP は ICMP パケットや ARP リクエストには応答しません。そのため、仮想 IP はスイッチやホスト PC のインタフェースと同じサブネットに設定することはできません。同じサブネットに設定した場合、Web 認証は正しく動作しません。定義した URL は、仮想 IP アドレスが設定されている場合にのみ有効になります。ユーザは、DNS サーバに保存された FQDN URL を取得して、仮想 IP アドレスを取得します。取得した IP アドレスは本項目で指定した仮想 IP アドレスと一致する必要があります。仮想 IPv4 アドレスが設定されていない場合、IPv4 接続で Web 認証を開始することができません。
Virtual IPv6	仮想 IPv6 アドレスを入力します。 仮想 IPv6 アドレスが設定されていない場合、IPv6 接続で Web 認証を開始することができません。
Virtual URL	仮想 URL を指定します。（128 文字以内）
Redirection Path	リダイレクトパスを入力します。（128 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

注意　仮想 IP が設定されていないと WAC が正しく機能しないため、WAC を有効にする前に WAC 仮想 IP アドレスを設定する必要があります。

注意　WAC 未認証時、DNS Over TCP はブロックされます。

WAC Port Settings（Web 認証ポート設定）

ポート毎に WAC 機能のステータスを設定します。

Security > Web-based Access Control > WAC Port Settings をクリックし、以下の設定用画面を表示します。

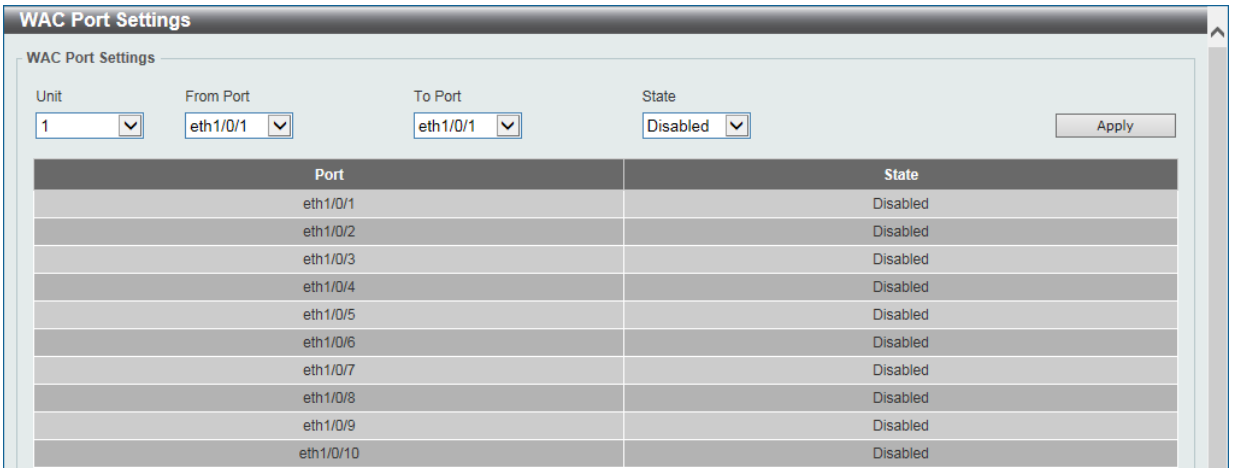


図 12-75　WAC Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。

項目	説明
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートで WAC 機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

WAC Customize Page（WAC カスタマイズページ設定）

認証ページの項目をカスタマイズします。

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

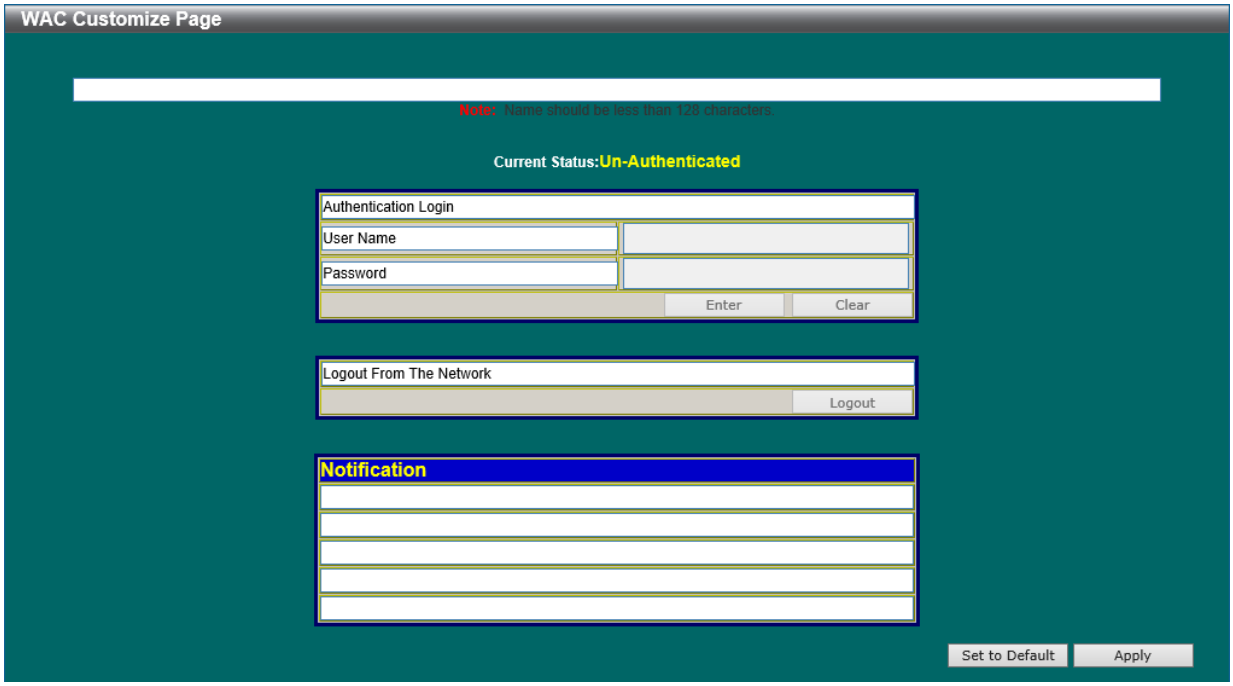


図 12-76　WAC Customize Page 画面

画面に表示される項目：

項目	説明
Page Title	ページのタイトルとなるメッセージを入力します。（128 文字以内）
Login window Title	ログイン画面のタイトルを入力します。（64 文字以内）
User Name Title	ユーザ名項目のタイトルを入力します。（32 文字以内）
Password Title	パスワード項目のタイトルを入力します。（32 文字以内）
Logout window Title	ログアウト画面のタイトルを入力します。（64 文字以内）
Notification	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。

「Apply」ボタンをクリックして、設定内容を適用します。
「Set to Default」ボタンをクリックして、全項目を初期設定に戻します。

注意　WAC カスタマイズページは日本語の入力はできません。

Network Access Authentication（ネットワークアクセス認証）

Network Access Authentication（ネットワークアクセス認証）の設定を行います。

Guest VLAN（ゲスト VLAN 設定）

ネットワークアクセス認証のゲスト VLAN の表示、設定を行います。

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

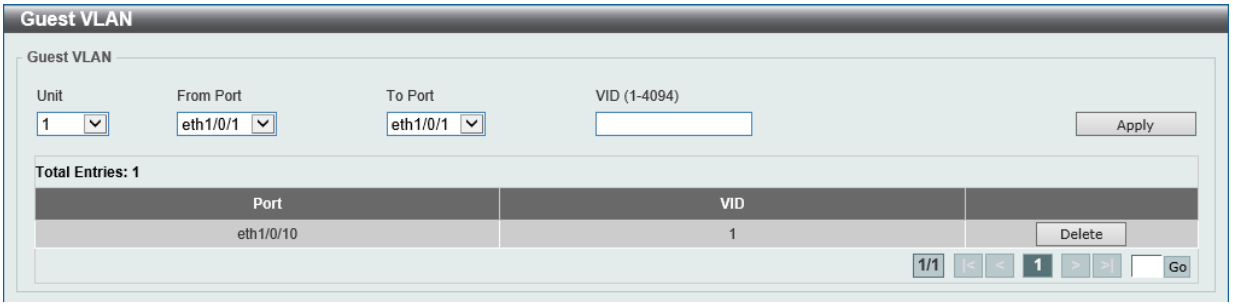


図 12-77　Guest VLAN 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
VID	設定する VLAN ID を入力します。 • 設定可能範囲：1-4094

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

Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）

ネットワークアクセス認証のグローバルステータスを設定します。

Security > Network Access Authentication > Network Access Authentication 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。

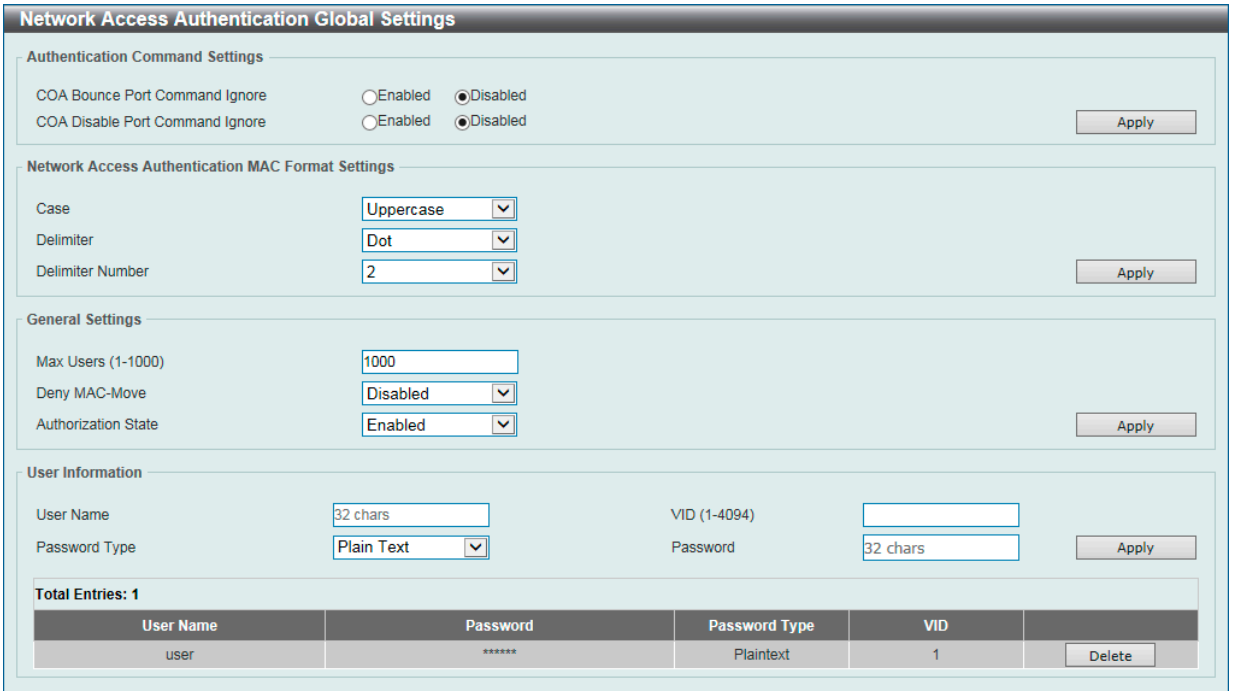


図 12-78　Network Access Authentication Global Settings 画面

画面に表示される項目：

項目	説明
Authentication Command Settings	
COA Bounce Port Command Ignore	RADIUS CoA バウンスポートコマンドを無視（本機能を有効）または許可（本機能を無効）に設定します。
COA Disable Port Command Ignore	RADIUS CoA 無効ポートコマンドを無視（本機能を有効）または許可（本機能を無効）に設定します
Network Access Authentication MAC Format Settings	
Case	ネットワークアクセス認証に使用する MAC アドレスの形式を選択します。 • 選択肢：「Uppercase（大文字）」「Lowercase（小文字）」
Delimiter	MAC アドレスを入力する際の区切りを選択します。 • 選択肢：「Hyphen（ハイフン）」「Colon（コロン）」「Dot（ドット）」「None（区切り文字なし）」
Delimiter Number	MAC アドレスにおける区切り数を選択します。 • 選択肢：「1」「2」「5」
General Settings	
Max Users	許可するユーザの最大数を指定します。 • 設定可能範囲：1-1000 • 初期値：1000
Deny MAC-Move	MAC 移動拒否機能の拒否を有効 / 無効に設定します。マルチ認証モードのポートで認証されたホストについて、別のポートへの移動を許可するかどうかを制御します。 ホストによる認証ポート間の移動には二つの状況が考えられます。次のルールに基づき、再認証が必要となるか、再認証を行うことなく新しいポートに直接移動します。 - 新しいポートの認証設定が元のポートと同じ場合、再認証は必要ありません。ホストは新しいポートに同じ承認属性を引き継ぎます。認証されたホストは、ポート 1 からポート 2 へのローミングを実行でき、再認証なしで承認属性を継承します。 - 新しいポートの認証設定が元のポートと異なる場合は、再認証が必要です。ポート 1 の認証済みホストは、ポート 2 に移動して再認証を行うことが可能です。新しいポートで認証方式が有効になっていない場合は、ステーションは新しいポートに直接移動します。元のポートとのセッションは削除されます。ポート 1 の認証済みホストは、ポート 2 に移動できます。 MAC 移動が無効（本機能が有効）になっていて、認証されたホストが別のポートに移動した場合、違反エラーとして認識されます。
Authorization State	承認について有効 / 無効に指定します。本オプションは、認証された設定を承認するかどうかを指定します。 認証への承認が有効になると、RADIUS サーバにより付与される権限属性（VLAN、802.1p default priority、bandwidth、ACL など）が許容されます。「Bandwidth」「ACL」はポートベースでアサインされます。マルチ認証モードの場合、「VLAN」と「802.1p」は各ホストベースでアサインされます。それ以外の場合、「Bandwidth」「ACL」は各ポートベースでアサインされます。
User Information	
User Name	ユーザ名を入力します。（32 文字以内）
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094
Password Type	パスワードの種類を選択します。 • 選択肢：「Plain Text（平文）」「Encrypted（暗号化）」
Password	パスワードを入力します。

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

注意 MAC 認証において、Guest VLAN 使用時、ARP などの CPU 処理対象パケット契機を除く、認証済みの MAC アドレスはポート間の移動不可となります。

Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）

ネットワークアクセス認証のポート設定を行います。

Security > Network Access Authentication > Network Access Authentication 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。

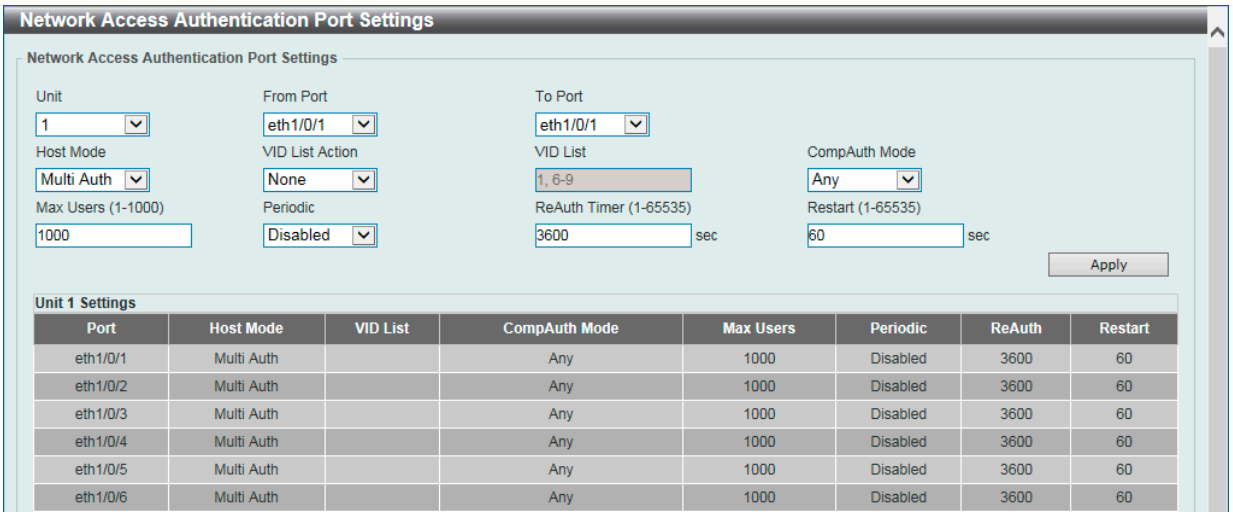


図 12-79　Network Access Authentication Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Host Mode	選択ポートに適用するホストモードを選択します。 • 「Multi Host」- ポートがマルチホストモードで動作している場合、一台のホストが認証されると、他のすべてのホストについてもポートへのアクセスが許可されます。802.1X 認証に従い、再認証失敗や認証ユーザのログオフなどが発生した場合、ポートはしばらくの間ブロックされます。一定の時間が過ぎると、EAPOL パケットの処理を元に戻します。 • 「Multi Auth」- ポートがマルチ認証モードで動作している場合、各ホストに対し、ポートへのアクセスに認証が必要になります。ホストは MAC アドレスによって識別され、認証されたホストのみポートへのアクセスが可能になります。
VID List Action	VLAN リストに対するアクションを設定します。 • 選択肢：「None（なし）」「Add（追加）」「Delete（削除）」
VID List	ホストモードでマルチ認証オプションを選択すると、パラメータが有効になります。使用する VLAN ID を入力します。この設定は、スイッチ上の各 VLAN に対して異なる認証要件が求められる場合に便利です。クライアントが認証された後、クライアントは他の VLAN から受信しても再認証は必要とされません。このオプションは、トランクポートが VLAN ごとの認証制御を行う場合に便利です。ポートの認証モードがマルチホストに変更された場合、ポート上の以前の認証 VLAN はクリアされます。
CompAuth Mode	コンパウンド認証モードのオプションを選択します。 • 「Any」- いずれかの認証方式（802.1X、MAC、WAC）でパスした場合、認証をパスします。 • 「MAC-WAC」-MAC ベースの認証を最初に検証します。クライアントが MAC 認証をパスをすると、次に WAC が検証され、最終的には両方の認証をパスする必要があります。
Max Users	最大ユーザ数を指定します。 • 設定可能範囲：1-1000
Periodic	選択ポートにおける定期的な再認証を有効 / 無効に設定します。
ReAuth Timer	再認証タイマを指定します。 • 設定可能範囲：1-65535（秒） • 初期値：3600（秒）
Restart	リスタート時間を入力します。 • 設定可能範囲：1-65535（秒） • 初期値：60（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）

ネットワークアクセス認証セッション情報の表示、消去を行います。

Security > Network Access Authentication > Network Access Authentication Sessions 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。

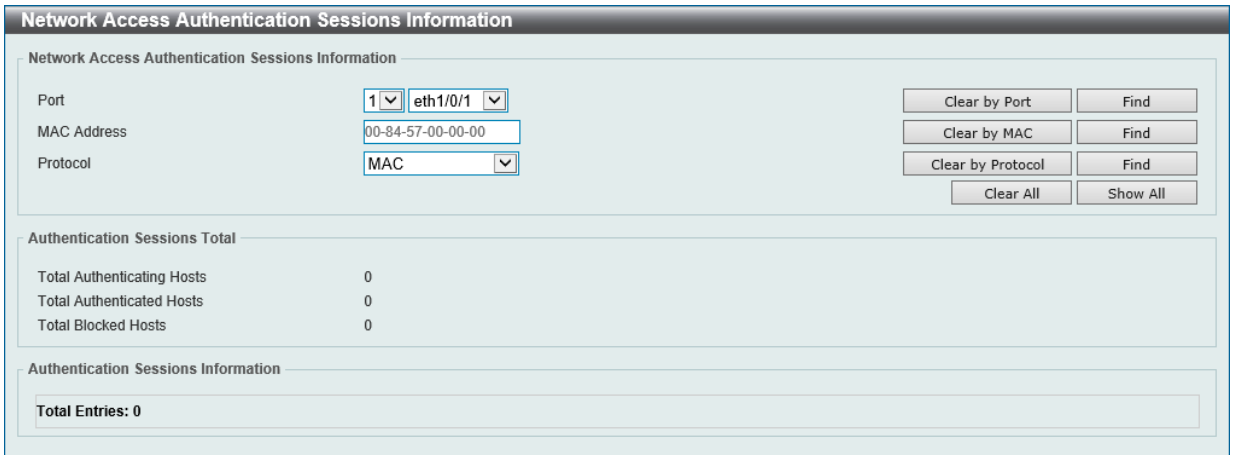


図 12-80　Network Access Authentication Sessions Information 画面

画面に表示される項目：

項目	説明
Port	表示 / クリアするユニットとポートを指定します。
MAC Address	表示 / クリアする MAC アドレスを指定します。
Protocol	プロトコルオプションを選択します。 • 選択肢：「MAC」「WAC」「DOT1X」

情報の消去

「Clear by Port」ボタンをクリックして、指定したポートに基づき情報を消去します。
「Clear by MAC」ボタンをクリックして、指定した MAC アドレスに基づき情報を消去します。
「Clear by Protocol」ボタンをクリックして、指定したプロトコルに基づき情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。

エントリの検出 / 表示

「Find」ボタンをクリックして、指定した情報を基に指定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

注意　Compound 認証時、認証プロトコルを指定して認証情報を表示した場合、他の認証モジュールによって認証された対象ホストについて、指定の認証においてタイムアウトするまでカウントして表示する場合があります。

Safeguard Engine（セーフガードエンジン）

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃により、スイッチの CPU 負荷は対応可能なキャパシティを超えて増大してしまう可能性があります。このような問題を軽減するために、本スイッチにはセーフガードエンジン機能が実装されています。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化してスイッチ全体の操作性を保ち、限られたリソース内で重要なパケットの送受信を可能にします。

CPU 負荷が上昇しきい値を超えると、セーフガードエンジン機能が作動し、スイッチは「Exhausted」モードに入ります。Exhausted モードでは、スイッチは ARP とブロードキャスト IP パケットで使用可能な帯域を制限します。CPU 負荷がしきい値を下回った場合、セーフガードエンジンは動作を停止し、スイッチは Exhausted モードを脱却して通常モードへ移行します。

CPU 宛に送信されるパケットは 3 つのグループに分類されます。サブインタフェースとしても知られるこれらのグループは、CPU が特定の種類のトラフィックを識別するために使用する論理的なインタフェースです。この 3 つのグループは「プロトコル」「管理」「ルート」に分類されています。通常、スイッチの CPU が受信パケットを処理する際、「プロトコル」グループが最も高い優先度でパケットを受信し、（スイッチの CPU は基本的にルーティングパケットの処理を行うため）「ルート」グループは最も低い優先度でパケットを受信します。「プロトコル」グループで処理されるパケットは、ルータによって識別されるプロトコルコントロールパケットです。「管理」グループで処理されるパケットは、Telnet や SSH などの対話型アクセスプロトコルを使用して、ルータやシステムネットワーク管理インタフェースへ送信されます。「ルート」グループで処理されるパケットは、一般にルータ CPU によって処理される通過ルーティングパケットとして認識されます。

以下の表は、プロトコルと対応するサブインタフェースの一覧です。

プロトコル名	サブインタフェース（グループ）	概要
802.1X	Protocol	Port-based Network Access Control（ポートベースアクセスコントロール）
ARP	Protocol	Address resolution Protocol (ARP)
DHCP	Protocol	Dynamic Host Configuration Protocol（DHCP）
DNS	Protocol	Domain Name System（DNS）
GVRP	Protocol	GARP VLAN Registration Protocol（GVRP）
ICMPv4	Protocol	Internet Control Message Protocol（ICMP）
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol（NS/NA/RS/RA) 以外
IGMP	Protocol	Internet Group Management Protocol（IGMP）
LACP	Protocol	Link Aggregation Control Protocol（LACP）
NTP	Protocol	Network Time Protocol（NTP）
PPPoE	Protocol	Point-to-point protocol over Ethernet（PPPoE）
SNMP	Manage	Simple Network Management Protocol（SNMP）
SSH	Manage	Secure Shell（SSH）
STP	Protocol	Spanning Tree Protocol（STP）
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol（TFTP）
Web	Manage	Hypertext Transfer Protocol (HTTP) Hypertext Transfer Protocol Secure (HTTPS)

カスタマイズされたレートリミット（パケット / 毎秒）をセーフガードエンジンのサブインタフェースに対してまとめて割り当て、または管理インタフェースで指定した個々のプロトコルに対して割り当てることが可能です。本機能を使用して個々のプロトコルのレート制限をカスタマイズする場合、不適切なレート制限を設定すると、パケットの処理に異常が発生する可能性がありますのでご注意ください。

注意 エンジンガードが有効になっている場合、スイッチは FFP（高速フィルタプロセッサ）メータリングテーブルを使用して、様々なトラフィックフロー（ARP、IP）に帯域幅を割り当て、CPU 使用率とトラフィック制限を制御します。これにより、ネットワーク経由のトラフィックルーティング速度が制限される場合があります。

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

スイッチにセーフガードエンジンの設定を行います。

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

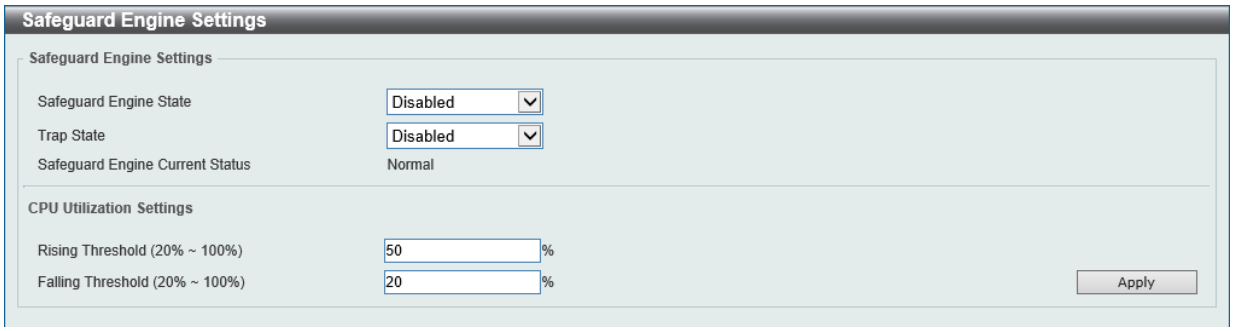


図 12-81　Safeguard Engine Settings 画面

画面に表示される項目：

項目	説明
Safeguard Engine Settings	
Safeguard Engine State	セーフガードエンジン機能を有効 / 無効に設定します。
Trap State	セーフガードエンジンのトラップを有効 / 無効に設定します。
Safeguard Engine Current Status	現在のセーフガードエンジンのステータスを表示します。
CPU Utilization Settings	
Rising Threshold	CPU 使用率の上限しきい値を設定します。 CPU 使用率がこのしきい値に到達すると、スイッチは Exhausted モードに入ります。 • 設定可能範囲：20-100（%）
Falling Threshold	CPU 使用率の下限しきい値を設定します。 CPU 使用率がこのしきい値を下回ると、スイッチは Safeguard Engine 状態から Normal モードに戻ります。 • 設定可能範囲：20-100（%）

「Apply」ボタンをクリックして、設定内容を適用します。

注意　CPU 使用率の上限 / 下限しきい値設定は、2 Core の平均値に対して適用されます。

CPU Protect Counters（CPU プロテクトカウンタ）

CPU プロテクションのカウンタ情報を表示、消去します。

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

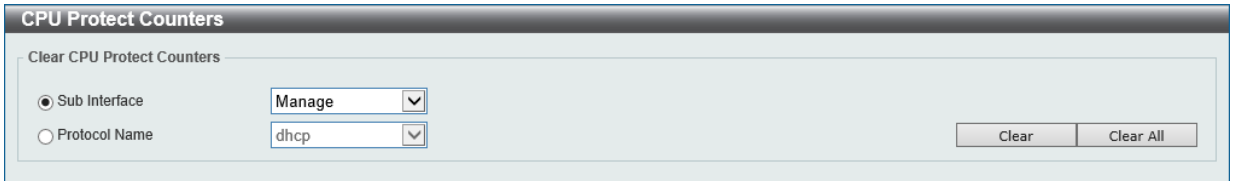


図 12-82　CPU Protect Counters 画面

画面に表示される項目：

項目	説明
Sub Interface	サブインタフェースのオプションを選択します。指定したサブインタフェースの CPU プロテクトカウンタをクリアします。 • 選択肢：「Manage」「Protocol」「Route」「All」
Protocol Name	プロトコル名のオプションを選択します。

「Clear」ボタンをクリックして、指定した内容に基づいて情報を消去します。
「Clear All」ボタンをクリックして、すべての情報を消去します。

CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）

CPU プロテクションのサブインタフェースを設定、表示します。

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

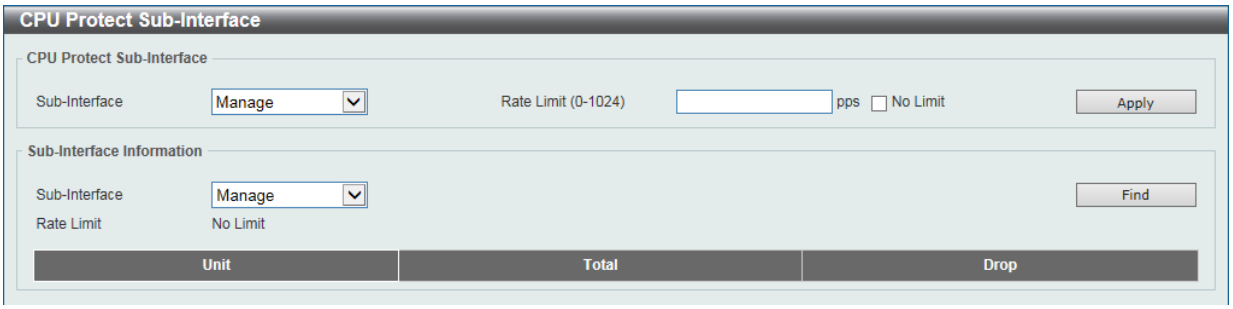


図 12-83　CPU Protect Sub-Interface 画面

画面に表示される項目：

項目	説明
CPU Protect Sub-Interface	
Sub-Interface	サブインタフェースのオプションを選択します。 • 選択肢：「Manage」「Protocol」「Route」
Rate Limit	レート制限の値を入力します。「No Limit」を指定するとレート制限を無効にします。 • 設定可能範囲：0-1024（パケット / 秒）
Sub-Interface Information	
Sub-Interface	検索するサブインタフェースのオプションを選択します。サブインタフェースを選択して「Find」をクリックすると、レート制限の設定値とカウンタ情報が表示されます。 • 選択肢：「Manage」「Protocol」「Route」

「Apply」ボタンをクリックして、設定内容を適用します。
「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出します。

CPU Protect Type（CPU プロテクトタイプ）

CPU プロテクションの種類の設定、表示します。

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

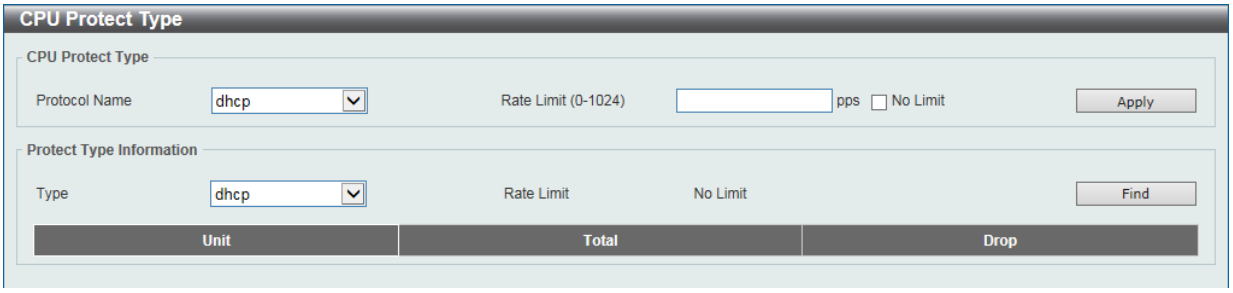


図 12-84　CPU Protect Type 画面

画面に表示される項目：

項目	説明
CPU Protect Type	
Protocol Name	プロトコル名のオプションを選択します。
Rate Limit	レート制限の値を入力します。「No Limit」を指定するとレート制限を無効にします。 • 設定可能範囲：0-1024（パケット / 秒）
Protect Type Information	
Type	プロトコルタイプを選択します。プロトコルタイプを選択して「Find」をクリックすると、レート制限の設定値とカウンタ情報が表示されます。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報を基にエントリを検出します。

注意　CPU Protect Type に関する設定は、Safeguard Engine の有効 / 無効とは独立して動作します。

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。

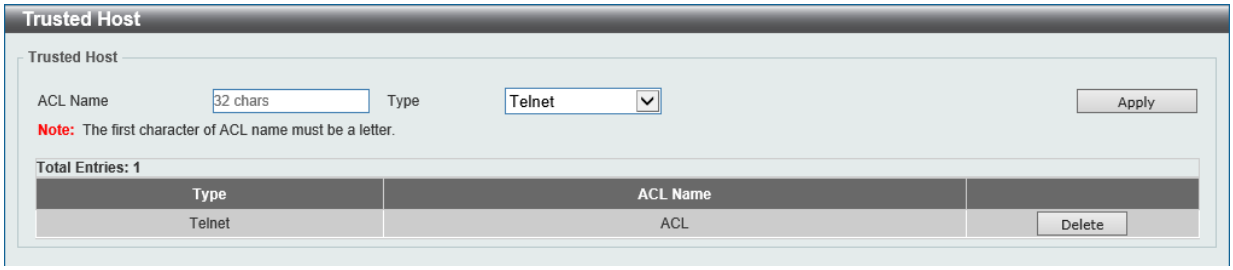


図 12-85　Trusted Host 画面

画面に表示される項目：

項目	説明
ACL Name	使用する ACL 名を入力します。（32 文字以内）
Type	トラストホストの種類を指定します。 ・ 選択肢：「Telnet」「SSH」「Ping」「HTTP」「HTTPS」

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

Traffic Segmentation（トラフィックセグメンテーション）

トラフィックセグメンテーションを設定します。
トラフィックセグメンテーション転送ドメインが指定されると、ポートで受信するパケットは、レイヤ 2 パケット転送においてドメイン内のインタフェースに制限されます。 ポートの転送ドメインが空の場合、ポートで受信したパケットのレイヤ 2 転送は制限されません。
トラフィックセグメンテーションのメンバリストは、同じ転送ドメインのポートとポートチャネルなど、異なるインタフェースタイプで構成できます。指定されたインタフェースにポートチャネルが含まれている場合、このポートチャネルのすべてのメンバポートが転送ドメインに含まれます。

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。

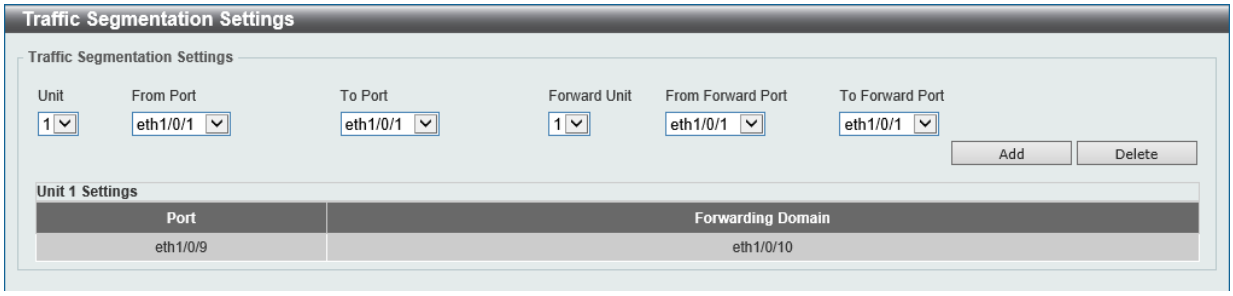


図 12-86　Traffic Segmentation 画面

画面に表示される項目：

項目	説明
Unit	設定する受信スイッチユニットを選択します。
From Port / To Port	設定する受信ポート範囲を指定します。
Forward Unit	設定する転送スイッチユニットを指定します。
From Forward Port / To Forward Port	設定する転送ポート範囲を指定します。

「Add」ボタンをクリックして、指定した情報を基に新しいエントリを追加します。
「Delete」ボタンをクリックして、指定した情報を基にエントリを削除します。

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、表示を行います。

Security > Storm Control Settings の順にクリックします。

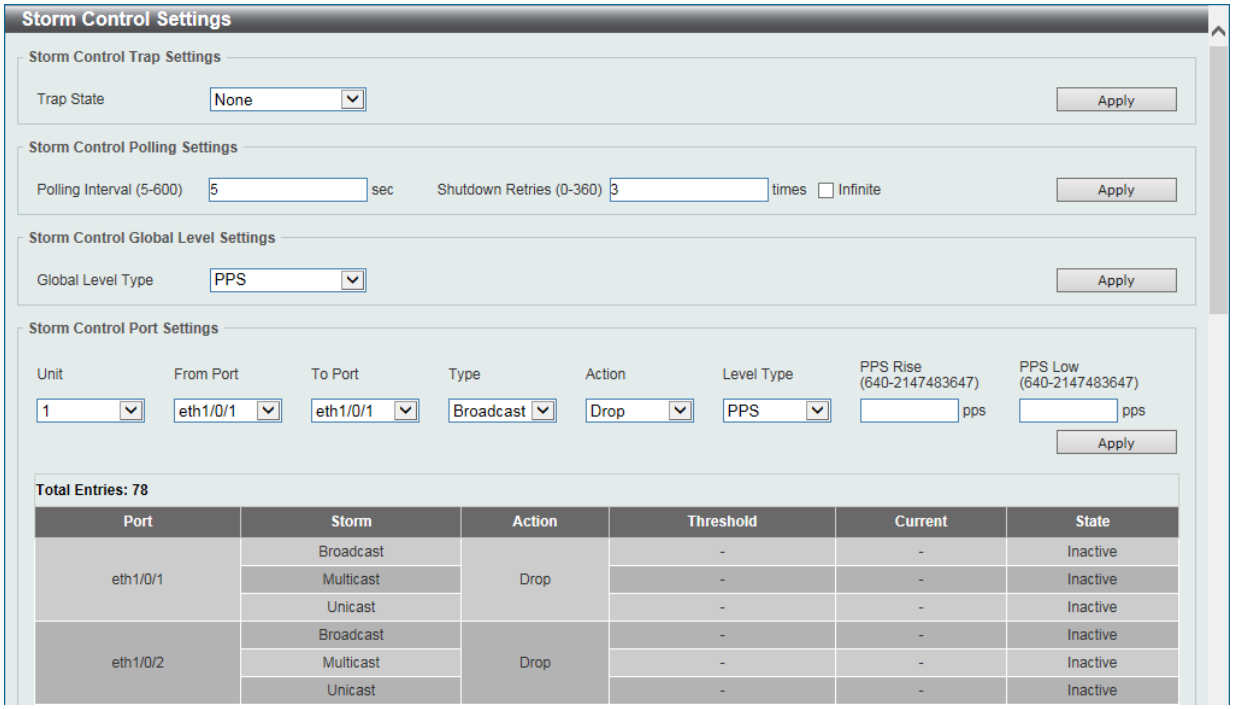


図 12-87　Storm Control Settings 画面

画面に表示される項目：

項目	説明
Storm Control Trap Settings	
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」- ストームの発生を検出、またはストームが解消された時点でトラップが通知されます。
Storm Control Polling Settings	
Polling Interval	ポーリング間隔の値を指定します。 • 設定可能範囲：5-600（秒） • 初期値：5（秒）
Shutdown Retries	アクションが「Shutdown」に設定されている場合、指定回数ストームを検知すると、エラー無効状態に移行します。 「0」を指定した場合、ストームを検出するとすぐにエラー無効状態に移行します。 「Infinite」にチェックを入れると、ストームを検知してもエラー無効状態に移行しません。 • 設定可能範囲：0-360（回） • 初期値：3（回）
Storm Control Global Level Settings	
Global Level Type	ストームコントロールの測定単位をグローバルで指定します。 • 「PPS」- 1 秒あたりのパケット数で指定します。 • 「Kbps」- 1 秒あたりのビットレートで指定します。 • 「Percentage」- 総帯域のパーセンテージで指定します。
Storm Control Port Setting	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用する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。 • 選択肢：「Broadcast」「Multicast」「Unicast」 シャットダウンモードに設定されている場合、ユニキャストは「Known」「Unknown」両方を参照します。つまり、既知または不明なユニキャストパケットが指定のしきい値に達すると、ポートはシャットダウンします。それ以外の設定では、ユニキャストは「Unknown」パケットのみを参照します。

項目	説明	
Action	実行するアクション指定します。 • 「None」- ストームパケットをフィルタしません。 • 「Shutdown」- 指定した上限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」- 指定した上限しきい値に達するとパケットは破棄されます。	
Level Type	ストームコントロールの測定単位を指定します。 • 選択肢：「PPS」「Kbps」「Level」	
	レベルタイプで「PPS」を選択した場合	
	PPS Rise	1 秒あたりのパケット量について上限しきい値を指定します。 • 設定可能範囲：640-2147483647（パケット / 秒）
	PPS Low	1 秒あたりのパケット量について下限しきい値を指定します。 • 設定可能範囲：640-2147483647（パケット / 秒） • 初期値：PPS Rise 値の 80%
	レベルタイプで「KBPS」を選択した場合	
	KBPS Rise	ポートで受信するトラフィックの上限しきい値をキロビット / 秒で指定します。 • 設定可能範囲：512-2147483647（Kbps）
	KBPS Low	ポートで受信するトラフィックの下限しきい値をキロビット / 秒で指定します。 • 設定可能範囲：512-2147483647（Kbps） • 初期値：KBPS Rise 値の 80%
	レベルタイプで「Level」を選択した場合	
	Level Rise	ポートで受信するトラフィックの総帯域の上限しきい値をパーセンテージで指定します。 • 設定可能範囲：1-100（%）
	Level Low	ポートで受信するトラフィックの総帯域の下限しきい値をパーセンテージで指定します。 • 設定可能範囲：1-100（%） • 初期値：Level Rise 値の 80%

「Apply」ボタンをクリックして、設定内容を適用します。

注意　ストームコントロールのしきい値を 0 に指定することはできません。

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。次のような既知の DoS 攻撃をスイッチで検出することができます。

項目	説明
TCP-Null	TCP NULL スキャンを検出・防御します。このスキャンでは、攻撃者は TCP フラグを持たないパケットを送信します。
TCP-Xmas	TCP Xmas スキャンを検出・防御します。このスキャンでは、攻撃者は様々な TCP フラグを持つ（クリスマスツリーのように飾られる）パケットを送信します。
TCP SYN-FIN	TCP SYN/FIN キャンを検出･防御します。このスキャンでは､SYN および FIN フラグを含む TCP パケットが送信されます。
ARP MAC SA Mismatch	ARP 不一致攻撃を検出・防御します。ARP 不一致攻撃には、攻撃者の MAC アドレスと別のネットワークノードの IP アドレスを紐づけるための偽の ARP パケットが含まれます。
TCP Flag SYNRST	TCP SYN/RST スキャンを検出・防御します。このスキャンでは、SYN および RST フラグを含む TCP パケットが送信されます。
TCP Over MAC MC/BC	TCP packets over MAC MCBC（multicast MAC addresses）を検出・防御します。マルチキャストトラフィックが増幅攻撃に使用されるのを防ぎます。
TCP SYN With Data	TCP SYN/Data スキャンを検出・防御します。このスキャンでは、SYN とデータペイロードを持つ TCP パケットが送信されます。
TCP UDP Port Zero	ポート 0 の TCP/UDP パケットを検出・防御します。ポート 0 は攻撃または偵察で使用される可能性があります。
All Types	上記のすべてのタイプ

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。

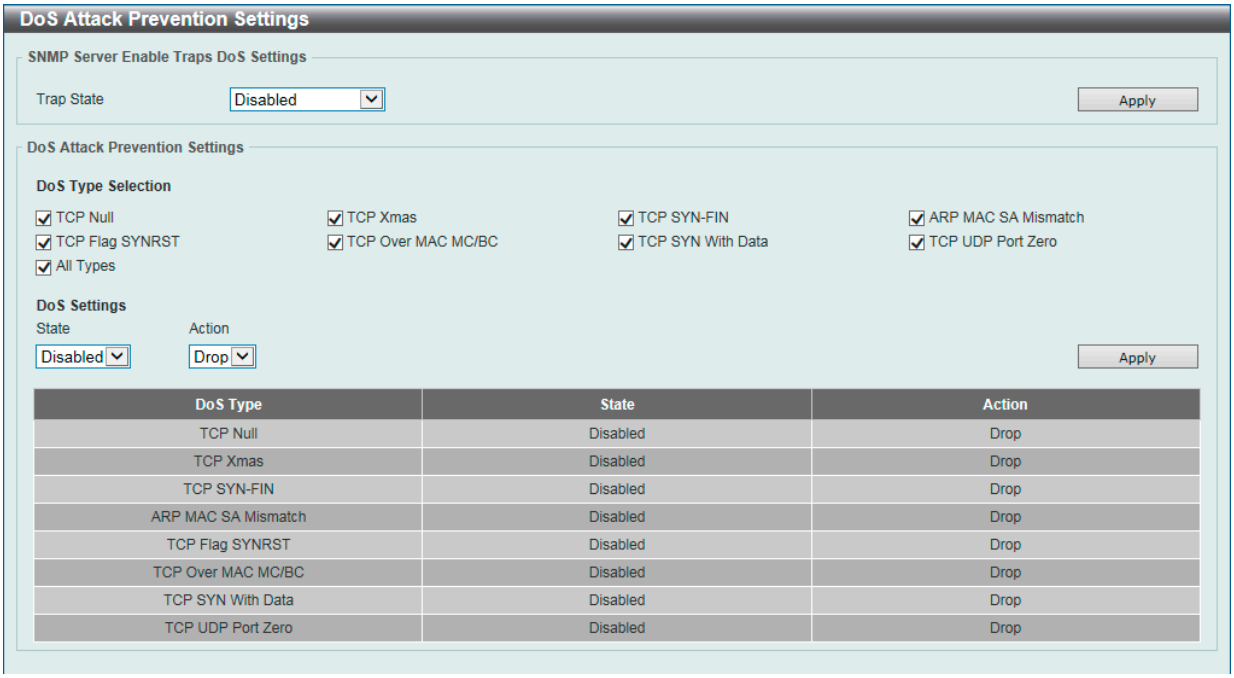


図 12-88　DoS Attack Prevention Settings 画面

画面に表示される項目：

項目	説明
SNMP Server Enable Traps DoS Settings	
Trap State	DoS 攻撃防止のトラップ状態を有効 / 無効に設定します。
DoS Attack Prevention Settings	
DoS Type Selection	DoS 攻撃防御のタイプを選択します。
State	DoS 攻撃防止の状態を有効 / 無効に指定します。
Action	DoS 攻撃を検出したときに実行されるアクションを指定します。 ・「Drop」- 一致する DoS 攻撃パケットをすべて破棄します。

「Apply」ボタンをクリックして、設定内容を適用します。

SSH（Secure Shell）

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

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

1. 「User Accounts Settings」で管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに他の管理者レベルのユーザアカウントを作成する方法と同じであり、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
2. 「SSH User Settings」画面を使用して、ユーザアカウントを設定します。ここでは、スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「Host Based」、「Password」、「Public Key」の 3 つがあります。
3. 「SSH Algorithm Settings」画面を使用して、SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。
4. 最後に「SSH Global Settings」画面で、SSH を有効にします。

これらの手順が完了後、安全な帯域内の接続でスイッチの管理を行うために、リモート PC 上の SSH クライアントの設定を行います。

SSH Global Settings（SSH グローバル設定）

SSH グローバル設定および表示を行います。

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

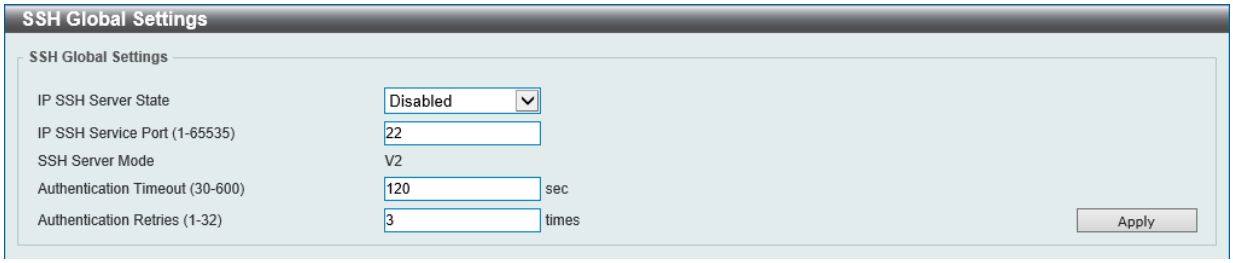


図 12-89　SSH Global Settings 画面

画面に表示される項目：

項目	説明
IP SSH Server State	SSH 機能のグローバルステータスを有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
IP SSH Service Port	SSH サービスポート番号を設定します。 • 設定可能範囲：1-65535 • 初期値：22
Authentication Timeout	認証のタイムアウト時間を指定します。 • 設定可能範囲：30-600（秒） • 初期値：120（秒）
Authentication Retries	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。 指定した回数を超えると接続が切断され、ユーザは再度スイッチに接続する必要があります。 • 設定可能範囲：1-32 • 初期値：3

「Apply」ボタンをクリックして、設定内容を適用します。

SSH Algorithm Settings（SSH アルゴリズム設定）

SSH アルゴリズムの設定、表示を行います。

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

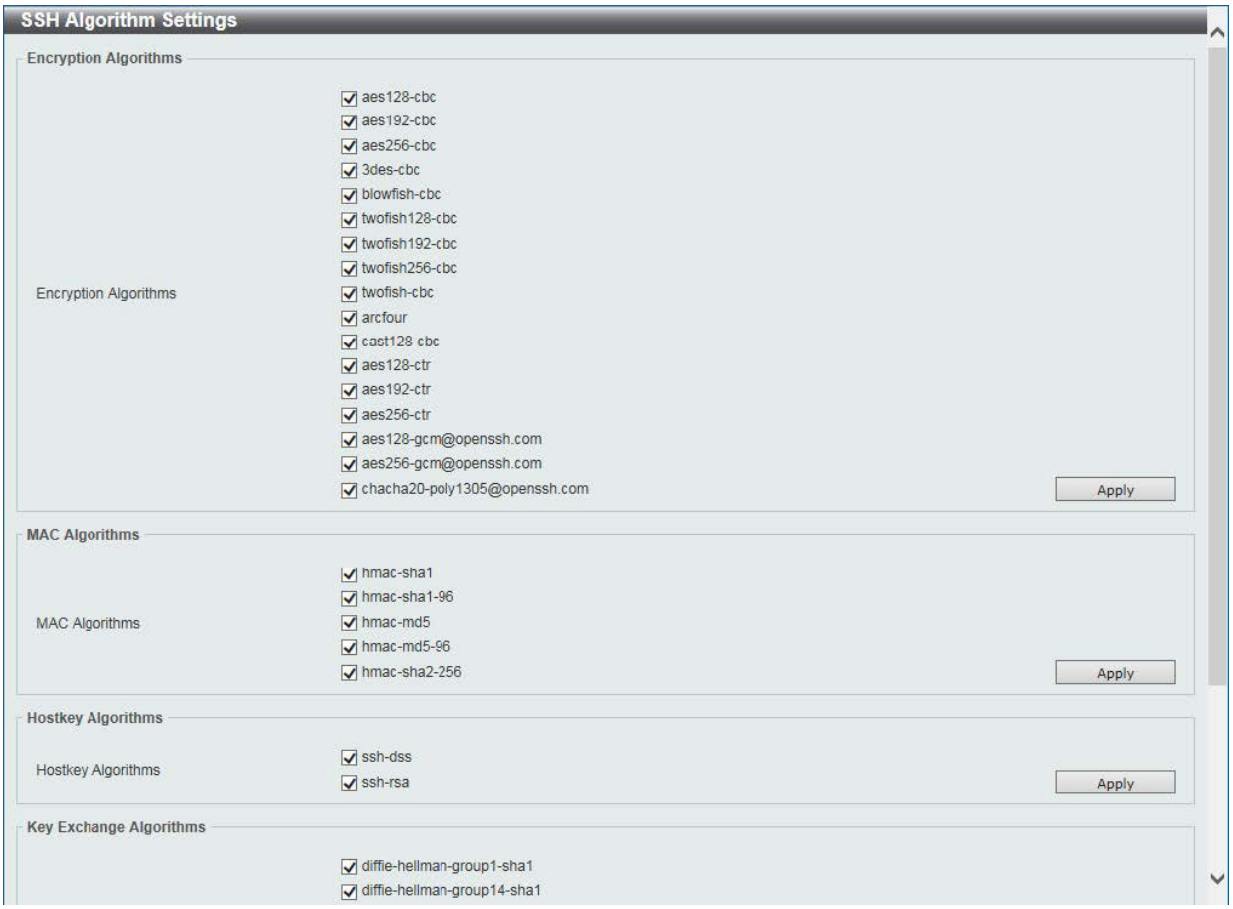


図 12-90　SSH Algorithm Settings 画面

画面に表示される項目：

項目	説明
Encryption Algorithms	
Encryption Algorithms	SSH サーバで許可される暗号化アルゴリズムを選択します。
MAC Algorithms	
MAC Algorithms	SSH サーバで許可される Message Authentication Code（MAC）アルゴリズムを選択します
Hostkey Algorithms	
Hostkey Algorithms	SSH サーバで許可されるホスト鍵アルゴリズムを選択します。
Key Exchange Algorithms	
Key Exchange Algorithms	SSH サーバで許可される鍵交換アルゴリズムを選択します。

「Apply」ボタンをクリックして、設定内容を適用します。

Host Key（Host Key 設定）

SSH ホスト鍵の生成、表示を行います。

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

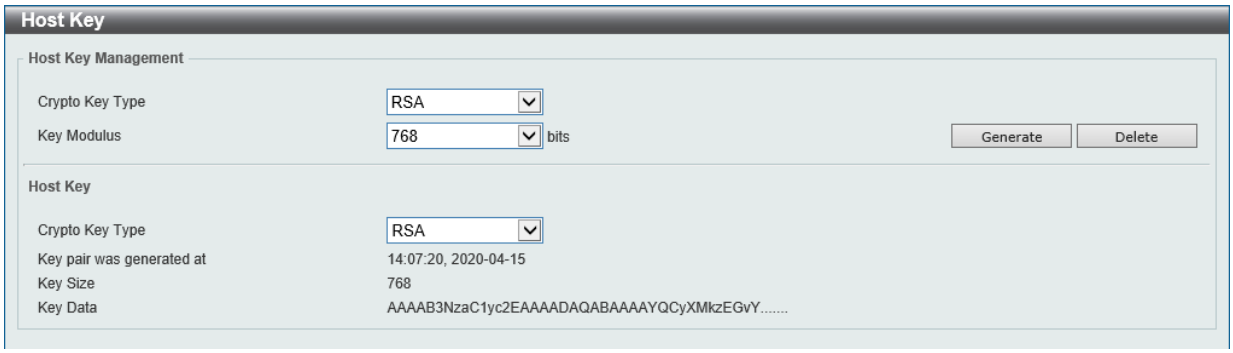


図 12-91　Host Key 画面

画面に表示される項目：

項目	説明
Host Key Management	
Crypto Key Type	暗号鍵の種類を選択します。 • 選択肢：「RSA（Rivest Shamir Adleman）」「DSA（Digital Signature Algorithm）」
Key Modulus	鍵長を選択します。 • 選択肢：「512」「768」「1024」「2048」（ビット）
Host Key	
Crypto Key Type	表示する暗号鍵の種類を選択します。 • 選択肢：「RSA（Rivest Shamir Adleman）」「DSA（Digital Signature Algorithm）」

「Generate」ボタンをクリックして、指定したホスト鍵を生成します。
「Delete」ボタンをクリックして、指定したホスト鍵を削除します。

「Generate」ボタンをクリックすると次の画面が表示されます。

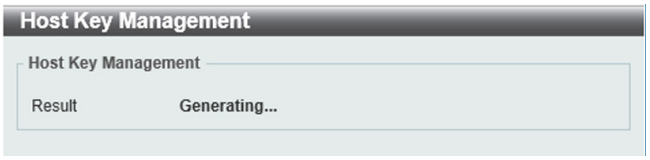


図 12-92　Host Key (Generating) 画面

鍵の生成が完了すると「Success.」メッセージが表示されます。

SSH Server Connection（SSH サーバ接続）

SSH サーバ接続テーブルの内容を確認します。

Security > SSH > SSH Server Connection 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 12-93　SSH Server Connection 画面

SSH User Settings（SSH ユーザ設定）

SSH ユーザの設定を行います。

Security > SSH > SSH User 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 12-94　SSH User Settings 画面

画面に表示される項目：

項目	説明
User Name	SSH ユーザ名を入力します。（32 文字以内）
Authentication Method	SSH ユーザの認証モードを指定します。 • 選択肢：「Password」「Public Key」「Host-based」
Key File	認証モードで「Public Key」または「Host-based」を選択した場合、公開鍵（Public Key）を入力します。
Host Name	認証モードで「Host-based」を選択した場合、ホスト名を入力します。
IPv4 Address	認証モードで「Host-based」を選択した場合、IPv4 アドレスを入力します。
IPv6 Address	認証モードで「Host-based」を選択した場合、IPv6 アドレスを入力します。

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

SSH Client Settings（SSH クライアント設定）

SSH クライアントの設定を行います。

Security > SSH > SSH Client 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。

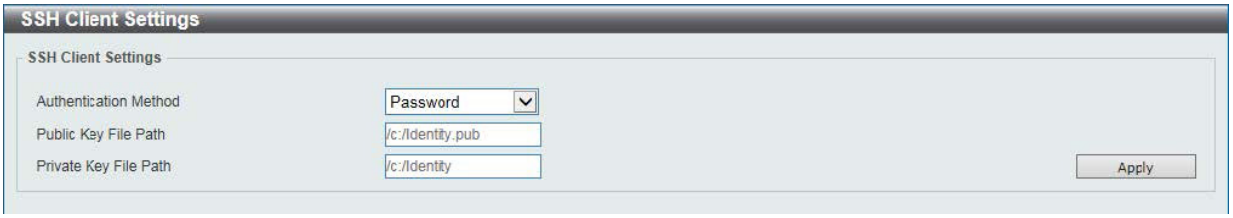


図 12-95　SSH Client Settings 画面

画面に表示される項目：

項目	説明
Authentication Method	SSH クライアントの認証モードを指定します。 • 「Password」- パスワード認証を使用します。（初期値） • 「Public Key」- 公開鍵認証を使用します。
Public Key File Path	公開鍵として使用するローカルファイルのファイルパスを入力します。
Private Key File Path	プライベート鍵として使用するローカルファイルのファイルパスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

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、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、暗号スイートを使用して実現されます。暗号スイートは、認証セッションに使用される厳密な暗号化パラメータ、特定の暗号化アルゴリズムおよびキー長を決定するセキュリティ文字列であり、以下の 3 つの段階で構成されます。

1. 鍵交換（Key Exchange）
   暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DSA、ここでは DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。これはクライアントとホスト間の最初の認証プロセスであり、「鍵交換」を行って一致した場合、認証が受諾され、次のレベルで暗号化のネゴシエーションが行われます。
2. 暗号化（Encryption）
   暗号スイートの次の部分は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
   - ストリーム暗号（Stream Ciphers）– スイッチは 2 種類のストリーム暗号（40 ビット鍵での RC4 と、128 ビット鍵での RC4）に対応しています。これらの鍵はメッセージの暗号化に使用され、最適に利用するためにはクライアントとホスト間で一致させる必要があります。
   - CBC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、1 つ前の暗号化テキストのブロックを使用して、現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義される 3 DES EDE 暗号化コードと高度な暗号化規格（AES）をサポートし、暗号化されたテキストを生成します。
3. ハッシュアルゴリズム（Hash Algorithm）
   暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージと共に暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）、SHA-256 の 3 つのハッシュアルゴリズムをサポートします。

サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成するために、これら 3 つのパラメータの一意の組み合わせである 13 種類の暗号化スイートについてスイッチ上で設定が可能です。それぞれの暗号化スイートに対して有効 / 無効の設定を行うことが可能ですが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号化スイートに含まれる情報はスイッチには実装されていないため、サードソースから証明書ファイルをダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバやスイッチのファイルシステムを使用してスイッチにダウンロードできます。また、本スイッチは、TLSv1.0/1.1/1.2 をサポートしています。それ以外のバージョンは本スイッチとは互換性がない恐れがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する可能性があります。

SSL 機能が有効化されると、通常の HTTP 接続はできなくなります。SSL 機能を使用した Web ベースの管理を行うには、SSL 暗号化がサポートされた Web ブラウザにおいて、https:// で始まる URL を使用する必要があります（例 : https://10.90.90.90）。これらの条件を満たさない場合、エラーが発生し、Web ベースの管理機能への接続認証が行われません。

SSL 機能で使用する証明書ファイルは TFTP サーバからスイッチへダウンロードすることができます。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者や認証のための鍵、デジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバ側とクライアント側で整合性のある証明書ファイルを保持している必要があります。スイッチには初期状態で証明書がインストールされていますが、ユーザ環境に応じて追加のダウンロードが必要になる場合があるかもしれません。

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。

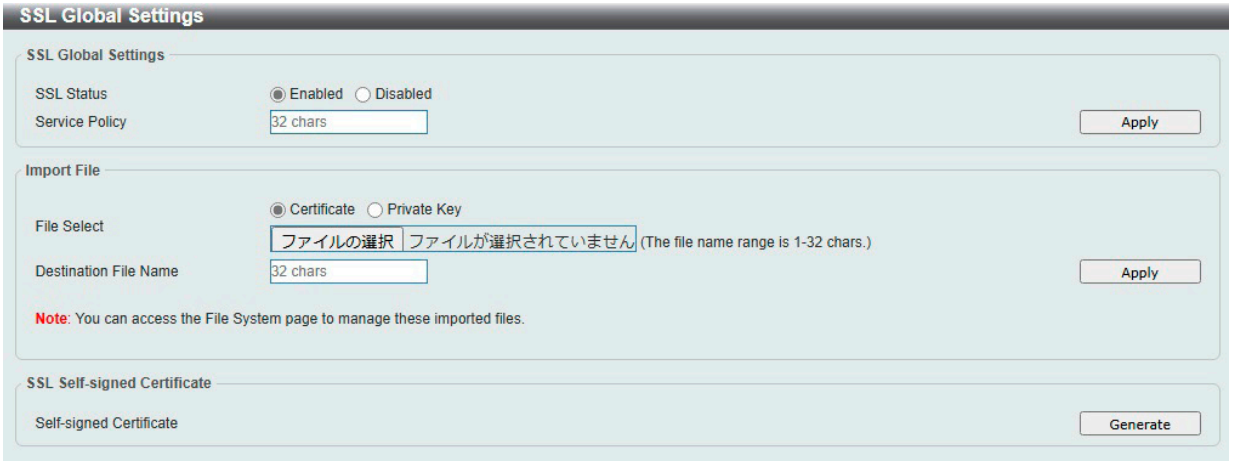


図 12-96　SSL Global Settings 画面

画面に表示される項目：

項目	説明
SSL Global Settings	
SSL Status	SSL のグローバルステータスを有効 / 無効に設定します。
Service Policy	SSL ポリシー名を入力します。（32 文字以内）
Import File	
File Select	ロードされるファイルの種類を指定します。 • 選択肢：「Certificate」「Private Key」 ファイル種類を選択した後、「ファイルの選択 / 参照」ボタンをクリックし、適切なファイルを選択してローカルコンピュータからロードします。
Destination File Name	宛先ファイル名を指定します。（32 文字以内）
SSL Self-signed Certificate	
Self-signed Certificate	「Generate」ボタンを選択すると、組み込みの自己署名証明書があるかどうかに関係なく、新しい自己署名証明書が生成されます。生成された証明書は、ユーザが所有する証明書には影響しません。

「Apply」ボタンをクリックして、設定内容を適用します。

補足　SSL 自己署名証明書は、キー長が 2048 ビットの自己署名 RSA 証明書のみをサポートします。

Crypto PKI Trustpoint（暗号 PKI トラストポイント）

暗号 PKI トラストポイントの表示、設定を行います。

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

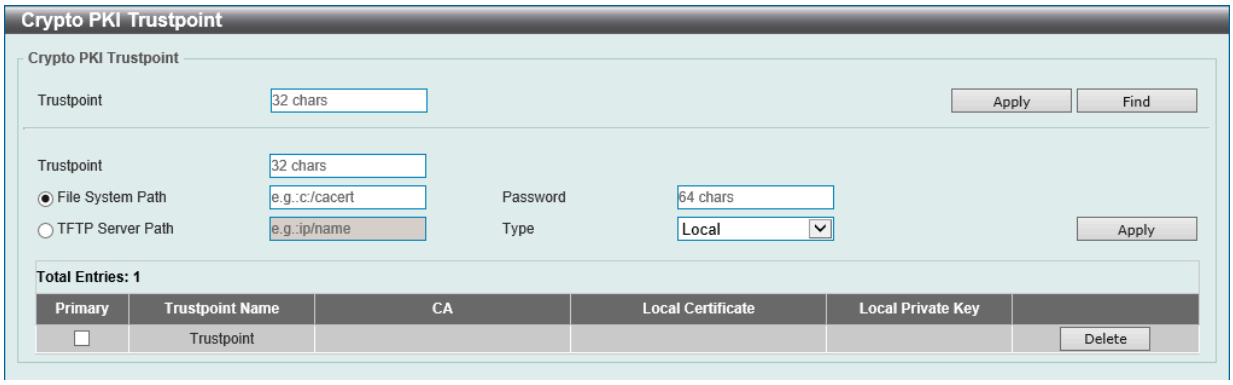


図 12-97　Crypto PKI Trustpoint 画面

画面に表示される項目：

項目	説明
Trustpoint	インポートした証明書と鍵ペアに対応するトラストポイント名を入力します。（32 文字以内）
File System Path	証明書と鍵ペアのファイルシステムパスを入力します。
Password	インポートしたプライベート鍵の暗号を解除する暗号パスフレーズを入力します。（64 文字以内） パスフレーズが指定されない場合、「NULL」文字列が使用されます。
TFTP Server Path	TFTP サーバのパスを指定します。
Type	インポートされる証明書の種類を指定します。 • 「Both」-「CA 証明書」「ローカル証明書」「鍵ペア」をインポートします。 • 「CA」-「CA 証明書」のみインポートします。 • 「Local」-「ローカル証明書」「鍵ペア」のみインポートします。

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

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。

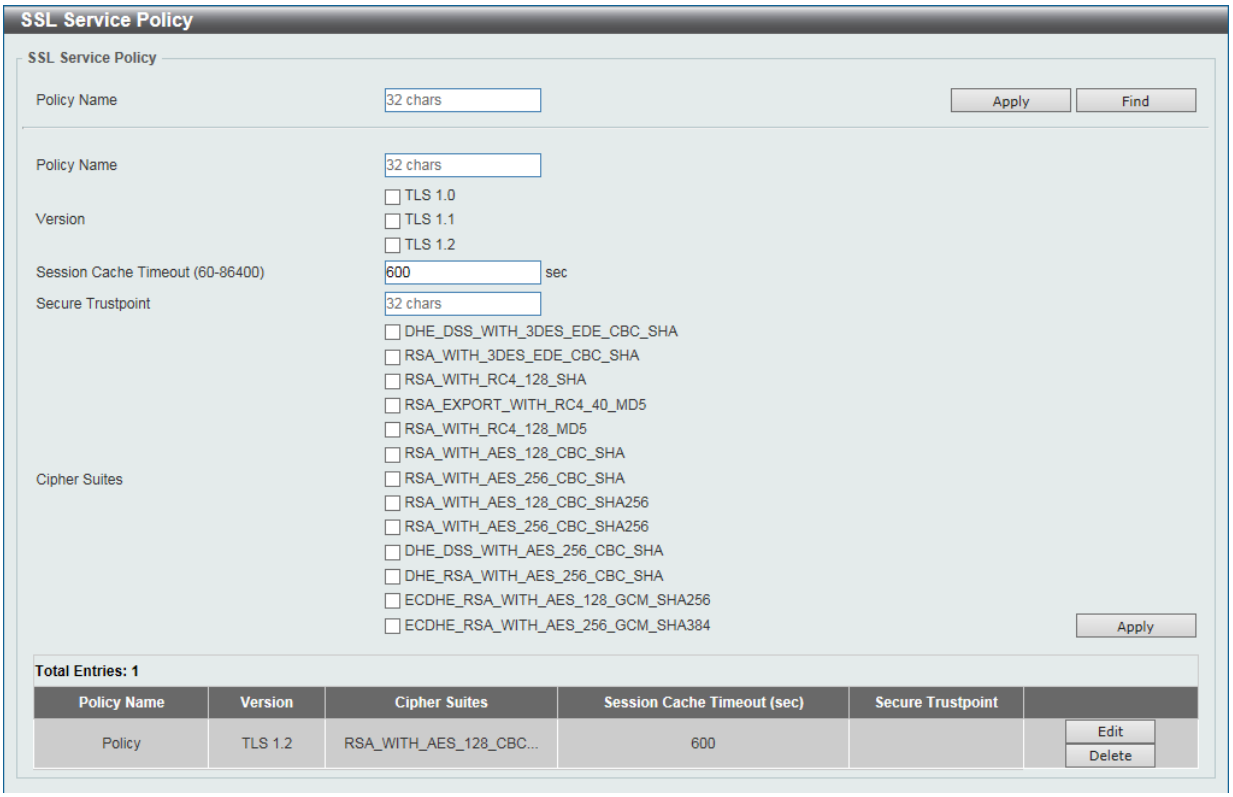


図 12-98　SSL Service Policy 画面

画面に表示される項目：

項目	説明
Policy Name	SSL サービスポリシー名を入力します。（32 文字以内）
Version	「Transport Layer Security」(TLS) のバージョンを指定します。 • 選択肢：「TLS 1.0」「TLS 1.1」「TLS 1.2」
Session Cache Timeout	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。 • 設定可能範囲：60-86400（秒） • 初期値：600（秒）
Secure Trustpoint	セキュアなトラストポイントの名前を入力します。（32 文字以内）
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て、設定内容を適用します。
「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。

Network Protocol Port Protect Settings（ネットワークプロトコルポート保護設定）

ネットワークプロトコルポート保護の設定、表示を行います。

Security > Network Protocol Port Protect 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。

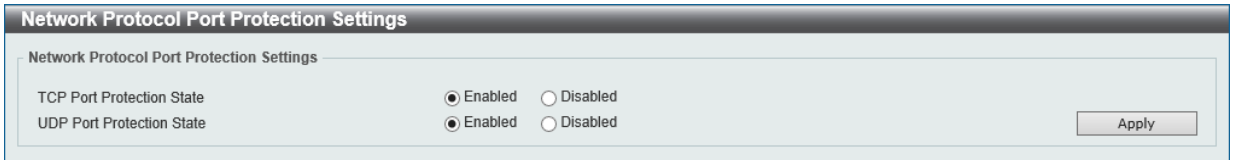


図 12-99　Network Protocol Port Protect Settings 画面

画面に表示される項目：

項目	説明
TCP Port Protection State	TCP ポート保護ステータスを有効 / 無効に指定します。
UDP Port Protection State	UDP ポート保護ステータスを有効 / 無効に指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)

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
CFM（Connectivity Fault Management : 接続性障害管理）	CFM 機能を設定します。
Cable Diagnostics（ケーブル診断機能）	スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。
Ethernet OAM（イーサネット OAM）	ポートにイーサネット OAM モード、イベント、ログを設定します。
DDM（DDM 設定）	Digital Diagnostic Monitoring（DDM）機能を実行します。スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定（アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx（送信）電力しきい値設定、および Rx（受信）電力しきい値設定）を行うことができます。

CFM（Connectivity Fault Management：接続性障害管理）

CFM は IEEE 802.1ag に定義されており、ネットワークにおける接続性故障の検出、隔離、およびレポートを行う標準規格です。

CFM Settings（CFM 設定）

CFM 機能を設定します。

OAM > CFM > CFM 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。

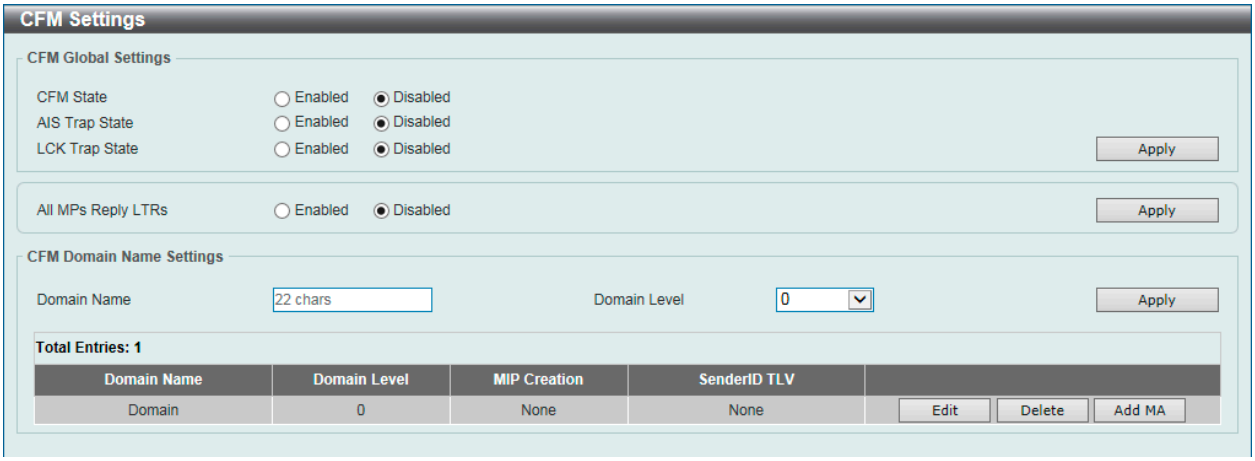


図 13-1　CFM Settings 画面

画面に表示される項目：

項目	説明
CFM Global Settings	
CFM State	CFM 機能を有効 / 無効に設定します。
AIS Trap State	「Alarm Indication Signal」(AIS) トラップ機能を有効 / 無効に設定します。本機能を有効にすると「ETH-AIS」イベント発生 / 解消時にトラップが送信されます。
LCK Trap State	「Locked Signal」(LCK) トラップ機能を有効 / 無効に設定します。本機能を有効にすると「ETH-LCK」イベント発生 / 解消時にトラップが送信されます。
All MPs Reply LTRs	すべての MP について、Link-Trace Reply（LTR）機能を有効 / 無効に設定します。IEEE 802.1ag 標準では、ブリッジは Link-Trace Message（LTM）への応答として LTR を返します。本機能を有効にすると、LTM のフォワーディングパス上のすべての MP が、ブリッジ上に存在するかどうかについて LTR で応答します。
CFM Domain Name Settings	
Domain Name	メンテナンスドメイン（MD）の名称を入力します。（22 文字以内）スペースを含めることはできません。サービスプロバイダまたはオペレータで使用される MD はそれぞれ固有の名前を持ちます。これにより、各メンテナンスドメインを管理する上で識別が容易になります。
Domain Level	メンテナンスドメインのレベルを選択します。MD レベルを割り当てることで、ドメイン間の階層関係を定義することができます。広い範囲のドメインには大きな値を設定します。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、各セクションで行った変更を適用します。
「Edit」をクリックして、特定エントリの設定を編集します。
「Delete」をクリックして、指定エントリを削除します。
「Add MA」をクリックして、Maintenance Association（MA）ルールを追加します。

エントリの編集

編集するエントリの「Edit」ボタンをクリックすると、以下のパラメータを編集できます。

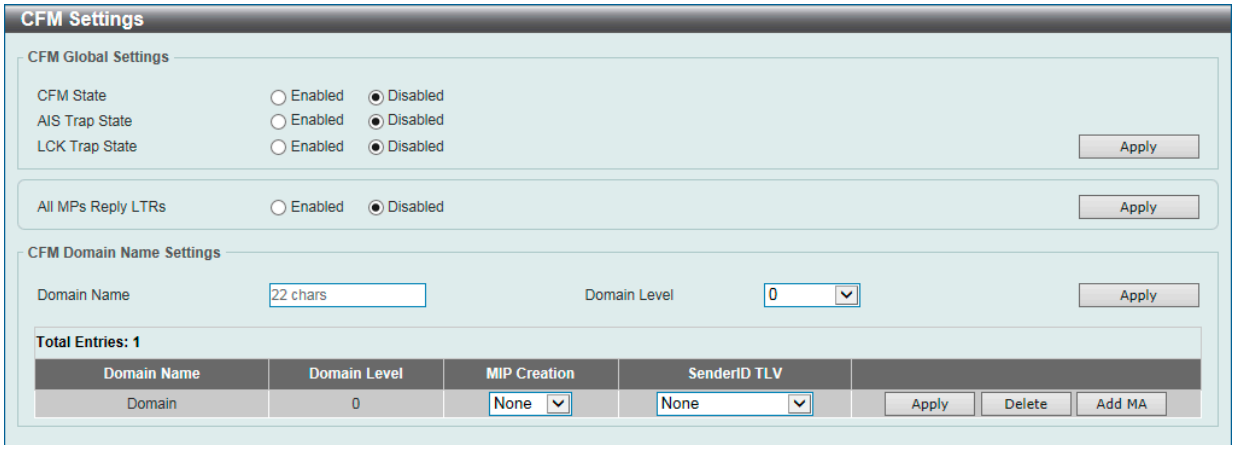


図 13-2　CFM Settings（Edit）画面

画面に表示される項目：

項目	説明
MIP Creation	Maintenance domain Intermediate Point（MIP）オプションを選択します。メンテナンスドメインにおける MIP の作成は、MIP 毎にリンクを追跡する上で役に立ちます。また、本設定により、ユーザは MEP から MIP へのループバックを実行することもできます。列挙値に基づき、管理エンティティがメンテナンスドメインの MIP Half Functions（MHF）を作成できます。 • 「None」- メンテナンスドメインに MIP を作成しません。 • 「Auto」- 次の場合にこの MD のポートで MIP が作成されます。 - 本 MD レベル以上のアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されていない場合、かつ本レベルの次に低いレベルのアクティブな MD において同じ VID を持つ MA のポートで MEP が設定されている場合、または本 MD レベルより低いアクティブな MD レベルにおいて同じ VID を持つ MA が存在しない場合 • 「Explicit」- 次の場合にこの MD の MA のポートで MIP が作成されます。 - 本 MD レベル以上のアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されていない場合、かつ本レベルの次に低いレベルのアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されている場合 MA 内の中間スイッチには「Auto」を指定してデバイス上に MIP が作成されるようにします。
Sender ID TLV	MD 内の MP による SenderID TLV のデフォルト送信を設定します。 • 「None」- SenderID TLV を送信しません。 • 「Chassis」- シャーシ ID 情報を持つ SenderID TLV を送信します。 • 「Manage」- 管理アドレス情報を持つ SenderID TLV を送信します。 • 「Chassis_Manage」- シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を送信します。

「Apply」ボタンをクリックして、設定内容を適用します。

Add MA（CFM MA Settings）

メンテナンスアソシエーションを設定します。

OAM > CFM > CFM Settings 画面で定義済みエントリの「Add MA」ボタンをクリックし、以下の画面を表示します。

図 13-3　CFM Settings（Add MA）- CFM MA Settings 画面

画面に表示される項目：

項目	説明
MA Name	メンテナンスアソシエーション（MA）のエントリ名（22 文字以内）を入力します。同一 MD 内の MA は、それぞれ異なる MA 名を持つ必要があります。別の MD に設定される MA には同じ MA 識別子が設定されていても問題ありません。MA エントリが削除されると設定も削除されます。

項目	説明
MA VID	メンテナンスアソシエーション（MA）エントリの VLAN ID を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。
「Edit」をクリックして、特定エントリの設定を編集します。
「Delete」ボタンをクリックして、エントリを削除します。
「Add MEP」ボタンをクリックして、MEP（Maintenance End Point）エントリを追加します。

エントリの編集
CFM MA エントリの「Edit」ボタンをクリックすると、以下のパラメータを編集できます。

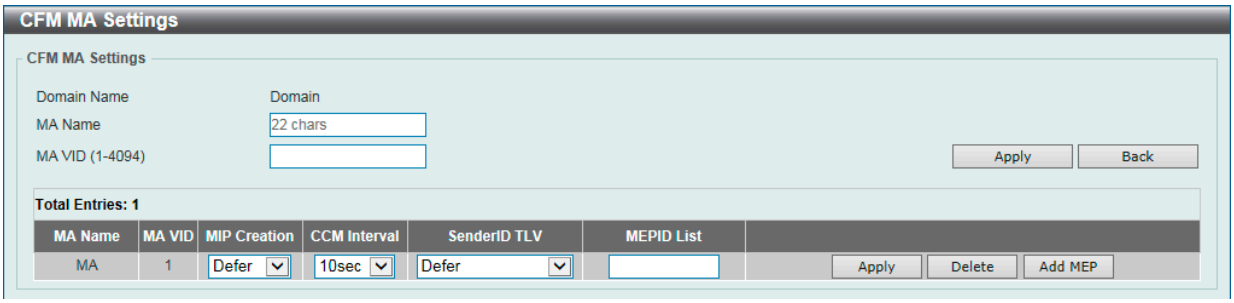


図 13-4　CFM Settings（Add MA）- CFM MA Settings 画面（Edit）

画面に表示される項目：

項目	説明
MIP Creation	MA に対する MIP の作成について設定します。 • 「None」- MA に MIP を作成しません。 • 「Auto」- 次のいずれかの場合にこの MA のポートで MIP が作成されます。 - 本 MD レベル以上のアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されていない場合、かつ本レベルの次に低いレベルのアクティブな MD において同じ VID を持つ MA のポートで MEP が設定されている場合、または本 MD レベルより低いアクティブな MD レベルにおいて同じ VID を持つ MA が存在しない場合 • 「Explicit」- 次の場合にこの MA のポートで MIP が作成されます。 - 本 MD レベル以上のアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されていない場合、かつ本レベルの次に低いレベルのアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されている場合 • 「Defer」- この MA が関連付けられているメンテナンスドメインの設定を継承します。（初期値） MA 内の中間スイッチには「Auto」を指定してデバイス上に MIP が作成されるようにします。
CCM Interval	Continuity Check Message（CCM）送信間隔を選択します。MEP が MA 内で定期的に CCM パケットを送信する間隔となります。 • 「100ms」- 100 ミリ秒 • 「1sec」- 1 秒 • 「10sec」- 10 秒 • 「1min」- 1 分 • 「10min」- 10 分
SenderID TLV	MA 内の MP による SenderID TLV の送信を制御します。 • 「None」- SenderID TLV を送信しません。CFM ハードウェアモードでは、「None」に設定されます。 • 「Chassis」- シャーシ ID 情報を持つ SenderID TLV を送信します。 • 「Manage」- 管理アドレス情報を持つ SenderID TLV を送信します。 • 「Chassis_Manage」- シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を送信します。 • 「Defer」- この MA が関連付けられているメンテナンスドメインの設定を継承します。（初期値）
MEPID List	MA に含まれる Maintenance association End Point（MEP）ID を指定します。 • 設定可能範囲：1-8191

「Apply」ボタンをクリックして、設定内容を適用します。

Add MEP（CFM Settings）

MEP を追加します。

「CFM MA Settings」画面で「Add MEP」ボタンをクリックし、以下の画面を表示します。

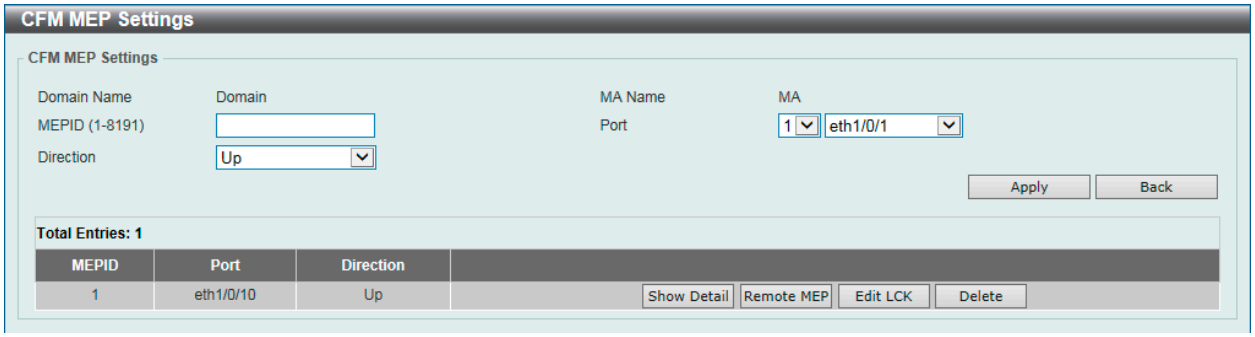


図 13-5　CFM Settings（Add MA, Add MEP）- CFM MEP Settings 画面

画面に表示される項目：

項目	説明
MEP ID	MEP ID を入力します。同一 MA 内に存在する MEP には、それぞれ固有の MEP ID を設定する必要があります。別の MA に設定される MEP には同じ MEP ID が設定されていても問題ありません。MEP を作成する前に、MA の MEP ID リストに MEP ID を設定しておく必要があります。 • 設定可能範囲：1-8191
Port	設定を適用するユニットとポートを指定します。
Direction	MEP の方向を指定します。 • 「Up」- 内向き（アップ）MEP を作成します。 • 「Down」- 外向き（ダウン）MEP を作成します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。
「Show Detail」ボタンをクリックして、指定 MEP の詳細情報を表示します。
「Remote MEP」ボタンをクリックして、Remote MEP テーブルを表示します。
「Edit LCK」ボタンを選択して、指定エントリの LCK 設定を変更します。
「Delete」ボタンを選択して、指定エントリを削除します。

詳細情報の参照（Show Detail）

「CFM MEP Settings」画面で「Show Detail」ボタンをクリックし、以下の画面を表示します。

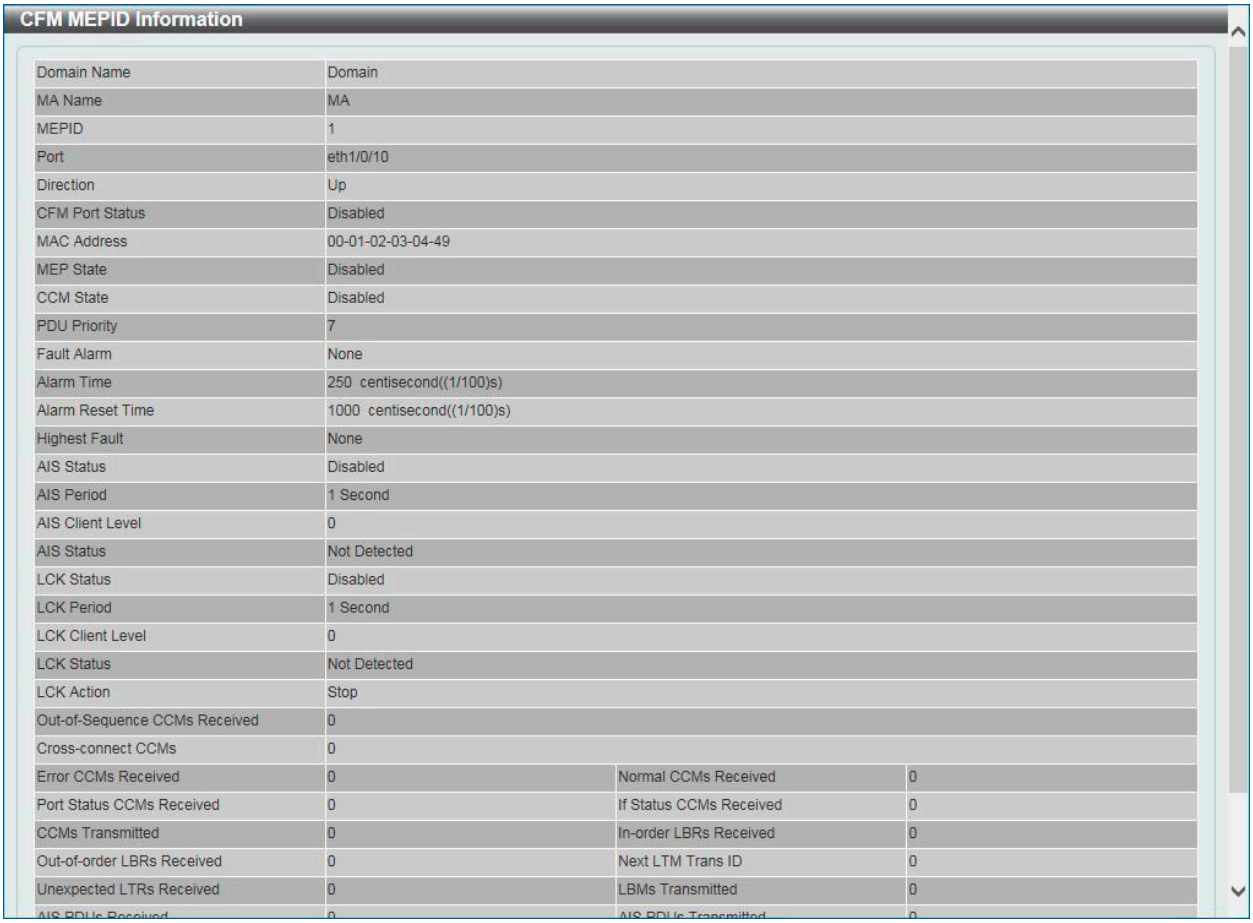


図 13-6　CFM Settings（Add MA, Add MEP, Show Detail）- CFM MEPID Information 画面

「Edit」ボタンを選択して、指定エントリを変更します。
前の画面に戻るには、「Back」ボタンをクリックします。

MEP の編集

「CFM MEPID Information」画面で「Edit」ボタンをクリックすると、以下のパラメータを編集できます。

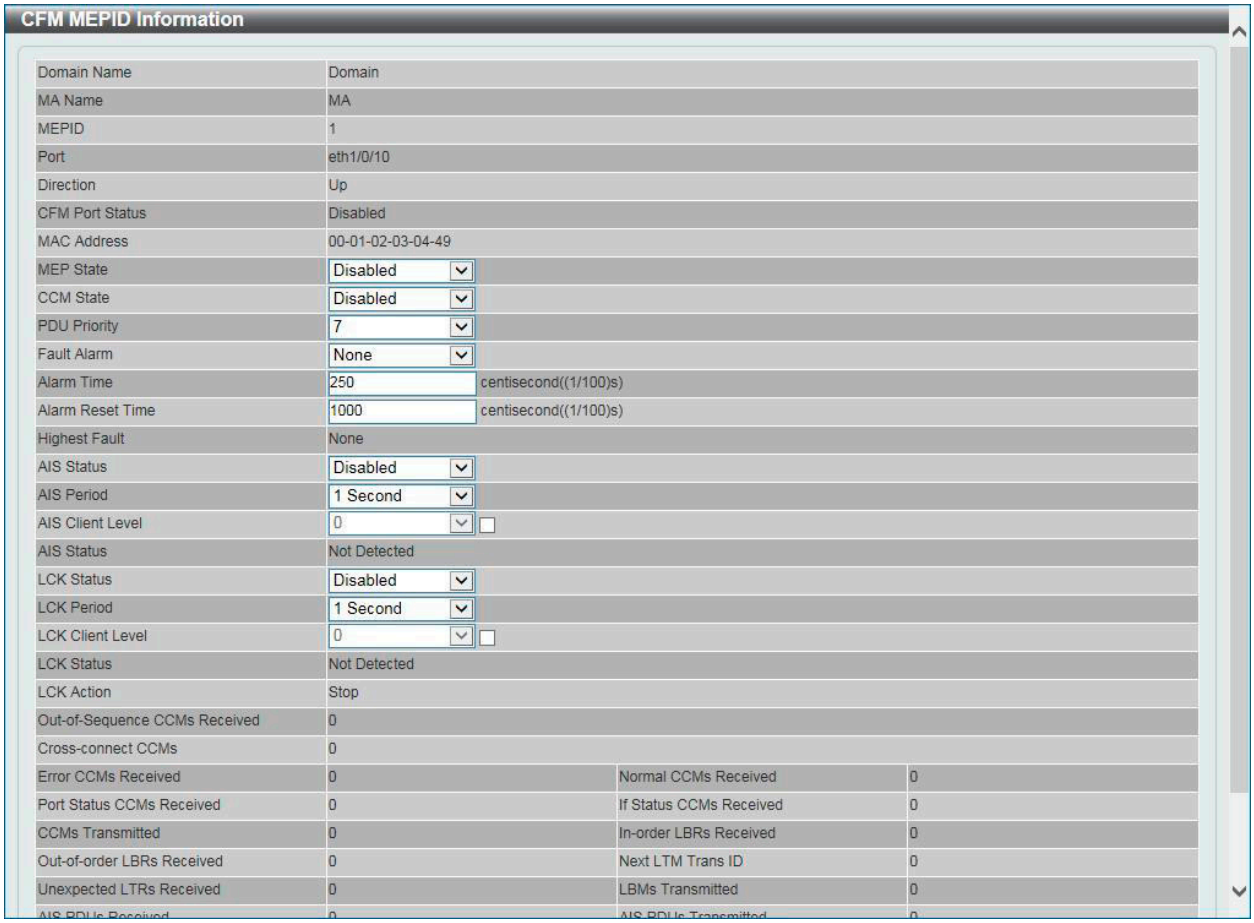


図 13-7　CFM Settings（Add MA, Add MEP, Show Detail）- CFM MEP ID Information 画面（Edit）

画面に表示される項目：

項目	説明
MEP State	インタフェースの MEP ステータスを有効 / 無効に設定します。
CCM State	CCM ステータスを有効 / 無効に設定します。
PDU Priority	PDU 優先度の値を設定します。MEP によって送信される CCM およびその他の CFM PDU にセットされる 802.1p プライオリティ値を定義します。 • 設定可能範囲：0-7
Fault Alarm	MEP によって送信される障害アラームのタイプを指定します。 • 「None」- 障害アラームは送信されません。 • 「All」- すべての障害アラームのタイプが送信されます。 • 「MAC-Status」- 優先度が「DefMACstatus」以上である障害アラームのみが送信されます。 • 「Remote-CCM」- 優先度が「DefRemoteCCM」以上である障害アラームのみが送信されます。 • 「Error-CCM」- 優先度が「DefErrorCCM」以上である障害アラームのみが送信されます。 • 「Xcon-CCM」- 優先度が「DefXconCCM」以上である障害アラームのみが送信されます。
Alarm Time	MEP で障害が検出された後、障害アラームが送信されるまでの時間を設定します。 • 設定可能範囲：250-1000（センチ秒） • 初期値：250（センチ秒）
Alarm Reset Time	MEP で検出されたすべての障害が取り除かれてから障害アラームがリセットされるまでの時間を設定します。 • 設定可能範囲：250-1000（センチ秒） • 初期値：1000（センチ秒）
AIS State	インタフェースにおける AIS 機能を有効 / 無効に設定します。
AIS Period	AIS PDU 送信間隔を選択します。 • 選択肢：「1 Second（1 秒）」「1 Minute（1 分）」 • 初期値：「1 Second（1 秒）」
AIS Client Level	MEP が AIS PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は、MIP と MEP が存在する最も近いクライアントレイヤの MD レベルです。 • 設定可能範囲：0-7
LCK State	インタフェースにおける LCK 機能を有効 / 無効に設定します。

項目	説明
LCK Period	LCK PDU 送信間隔を選択します。 • 選択肢：「1 Second（1 秒）」「1 Minute（1 分）」 • 初期値：「1 Second（1 秒）」
LCK Client Level	MEP が LCK PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は、MIP と MEP が存在する最も近いクライアントレイヤの MD レベルです。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

■ Remote MEP（CFM Settings）

Remote MEP を参照します。

「CFM MEP Settings」画面で「Remote MEP」ボタンをクリックし、以下の画面を表示します。

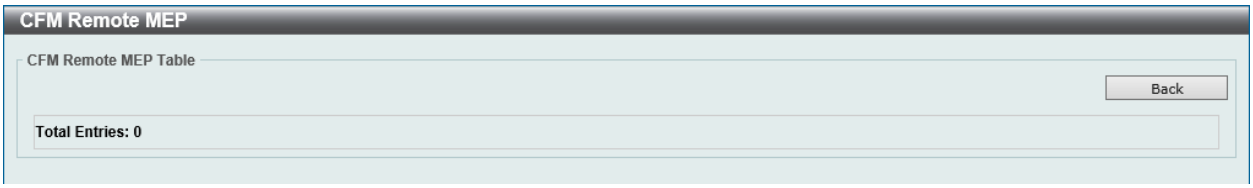


図 13-8　CFM Settings（Add MA, Add MEP, Remote MEP）- CFM Remote MEP 画面

前の画面に戻るには、「Back」ボタンをクリックします。

■ Edit LCK（CFM Settings）

LCK を編集します。

「CFM MEP Settings」画面で「Edit LCK」ボタンをクリックし、以下の画面を表示します。

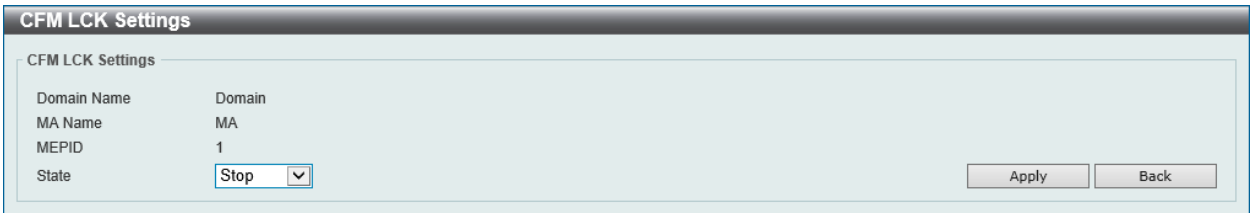


図 13-9　CFM Settings（Add MA, Add MEP, Edit LCK）- CFM LCK Settings 画面

画面に表示される項目：

項目	説明
State	管理ロック動作を指定します。MEP からクライアントレベル MEP に LCK PDU を送信します。 • 選択肢：「Start（開始）」「Stop（停止）」

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

CFM Port Settings（CFM ポート設定）

CFM ポート状態を有効または無効にします。

OAM > CFM > CFM 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。

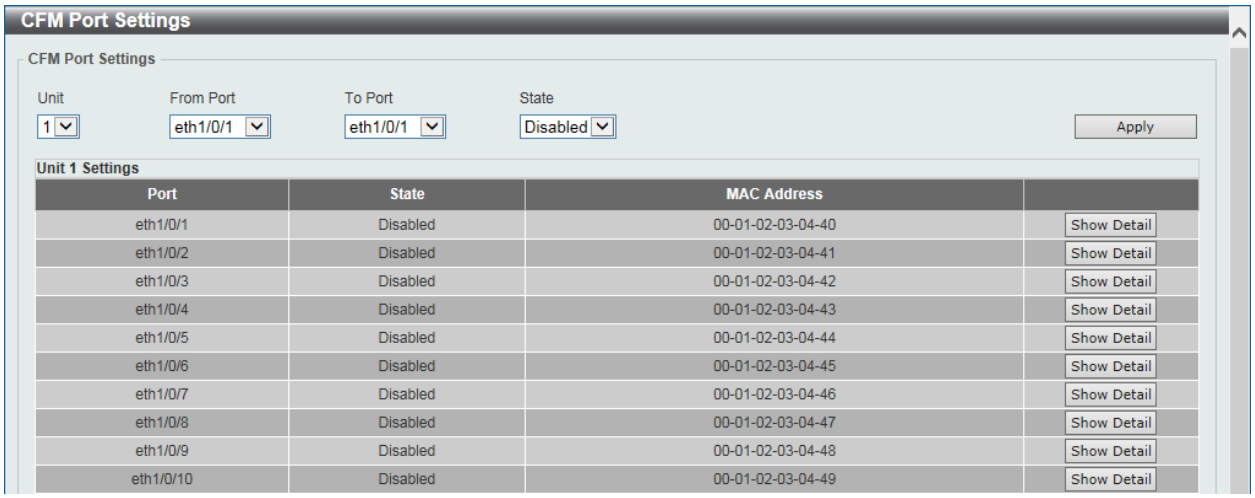


図 13-10　CFM Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
State	特定ポートの CFM 設定を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Show Detail」ボタンをクリックして、指定ポートの CFM 設定の詳細情報を表示します。

詳細情報の表示

「Show Detail」ボタンをクリックし、以下の画面を表示します。

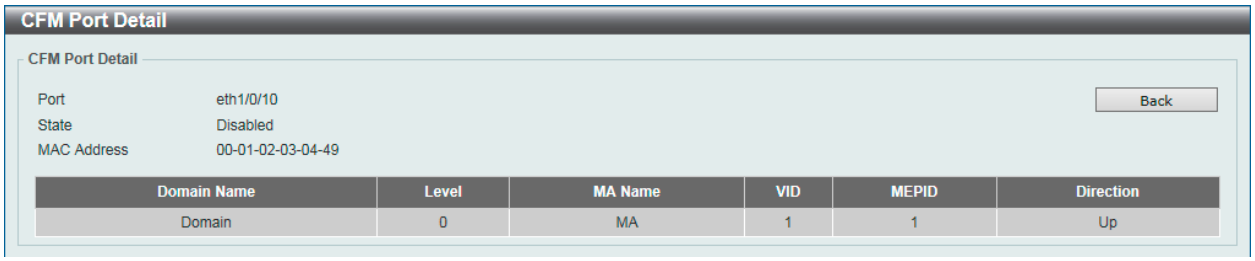


図 13-11　CFM Port Settings（Show Detail）- CFM Port Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

CFM Loopback Test（CFM ループバックテスト）

CFM ループバックテストを設定します。

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

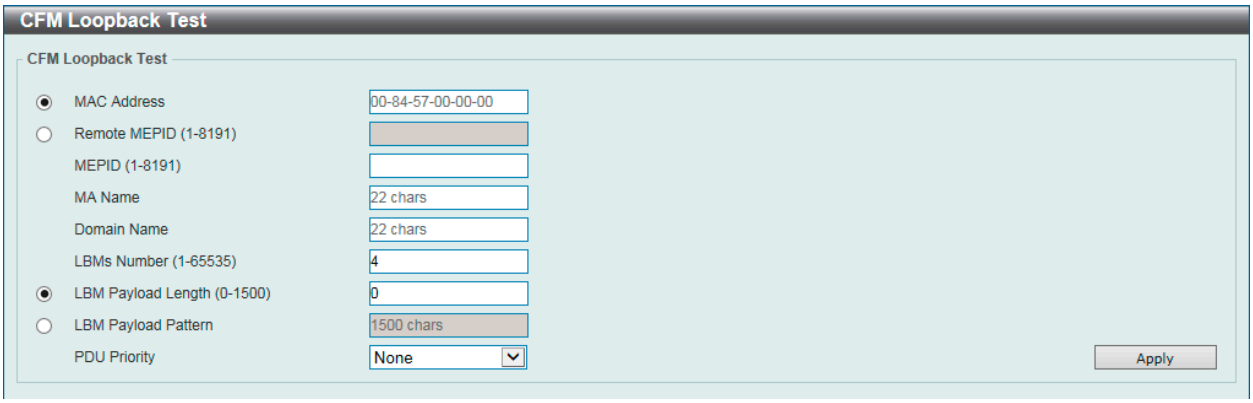


図 13-12　CFM Loopback Test 画面

画面に表示される項目：

項目	説明
MAC Address	宛先 MAC アドレスを入力します。
Remote MEPID	リモート MEP ID を入力します。 • 設定可能範囲：1-8191
MEP ID	ループバックテストを開始する MEP ID を入力します。 • 設定可能範囲：1-8191
MA Name	使用するメンテナンスアソシエーション名を指定します。（22 文字以内）
Domain Name	使用するメンテナンスドメイン名を指定します。（22 文字以内）
LBMs Number	送信する LBM 数を指定します。 • 設定可能範囲：1-65535 • 初期値：4
LBM Payload Length	送信される LBM のペイロード長を指定します。 • 設定可能範囲：0-1500 • 初期値：0
LBM Payload Pattern	LBM のペイロードパターンを指定します。Data TLV が含まれるかどうかの指定と、Data TLV に含まれる任意の数のデータを指定します。（1500 文字以内）スペースを含めることはできません。
PDU Priority	送信される LBM に設定される 802.1p プライオリティを指定します。「None」を指定した場合、MEP により送信される CCM と同じ優先度を使用します。 • 選択肢：0-7、「None（なし）」

「Apply」ボタンをクリックして、設定内容を適用します。

「Apply」をクリックすると、CFM ループバックテストテスト結果が表示されます

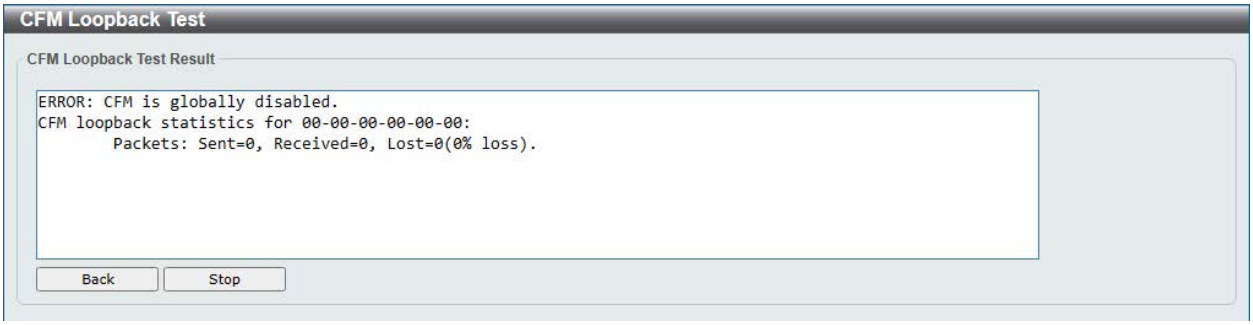


図 13-13　CFM Loopback Test Result 画面

「Stop」をクリックして、CFM ループバックテストを停止します。
前の画面に戻るには、「Back」をクリックします。

CFM Linktrace Settings（CFM リンクトレース設定）

CFM リンクトレースの設定を行います。

OAM > CFM > CFM Linktrace 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。

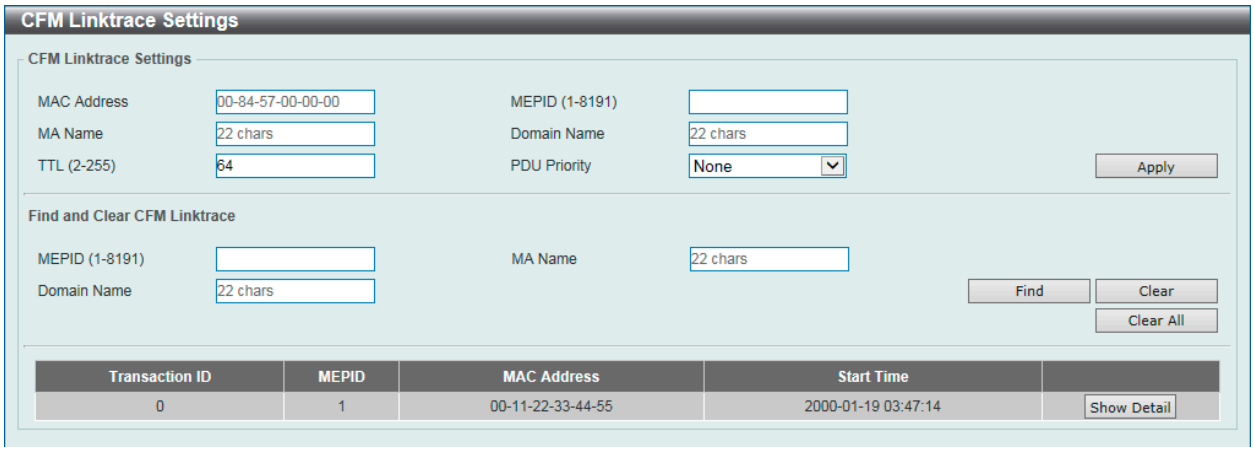


図 13-14　CFM Linktrace Settings 画面

画面に表示される項目：

項目	説明
CFM Linktrace Settings	
MAC Address	宛先 MAC アドレスを入力します。
MEP ID	リンクトレース機能を開始する MEP ID を指定します。 • 設定可能範囲：1-8191
MA Name	使用するメンテナンスアソシエーション名を指定します。（22 文字以内）
Domain Name	使用するメンテナンスドメイン名を指定します。（22 文字以内）
TTL	リンクトレースメッセージの TTL 値を指定します。 • 設定可能範囲：2-255 • 初期値：64
PDU Priority	送信される LTM に設定される 802.1p プライオリティを選択します。「None」を指定した場合、MEP によって送信される CCM と同じ優先度を使用します。 • 選択肢：：0-7、「None（なし）」
Find and Clear CFM Linktrace	
MEPID	MEP ID を入力します。 • 設定可能範囲：1-8191
MA Name	使用するメンテナンスアソシエーション名を指定します。（22 文字以内）
Domain Name	使用するメンテナンスドメイン名を指定します。（22 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、入力した情報を基にエントリをクリアします。
「Clear All」ボタンをクリックして、すべてのエントリに紐づく情報をクリアします。

エントリの参照

「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。

「Show Detail」リンクをクリックすると、CFM リンクトレースの詳細情報が表示されます。

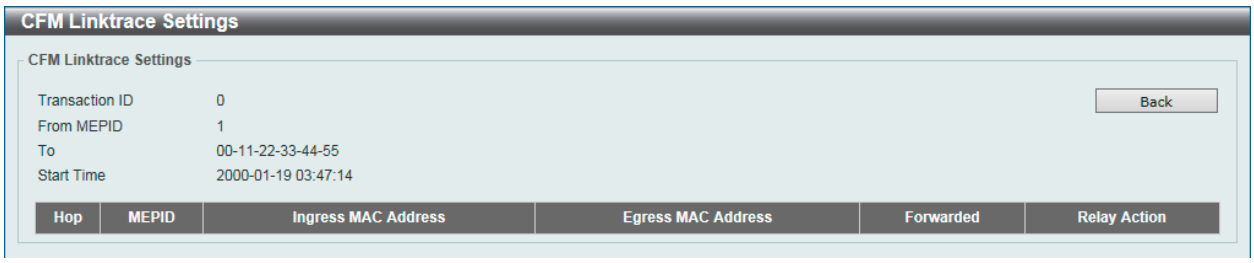


図 13-15　CFM Linktrace Settings（Show Detail）- CFM Linktrace Settings 画面

前の画面に戻るには、「Back」ボタンをクリックします。

CFM Packet Counter（CFM パケットカウンタ）

CFM パケットカウンタ情報を表示します。

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

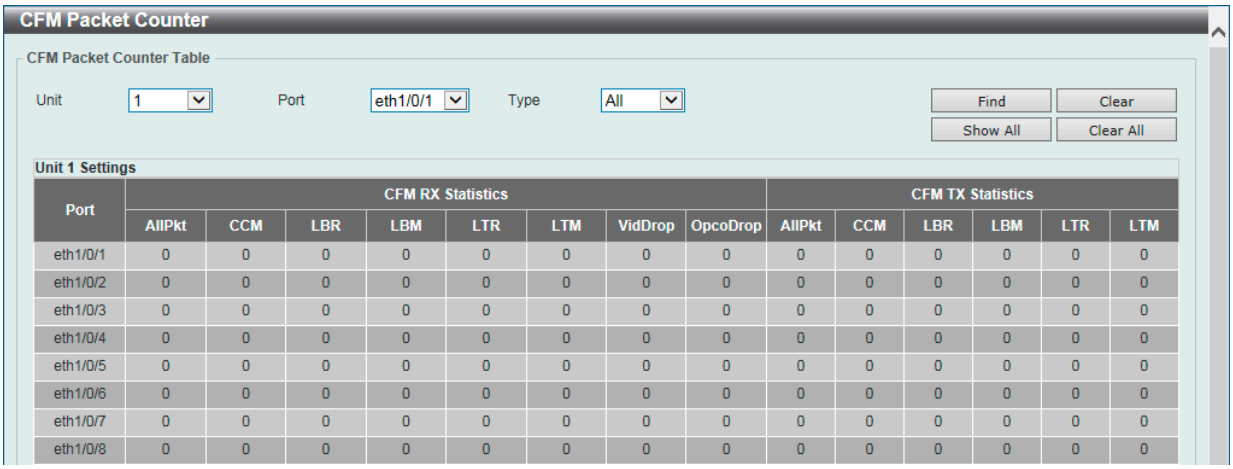


図 13-16　CFM Packet Counter 画面

画面に表示される項目：

項目	説明
Unit	カウンタを参照 / 削除するユニットを指定します。
Port	カウンタを参照 / 削除するポートを選択します。
Type	パケットの種類を選択します。 • 「RX」- 受信したすべての CFM パケットのカウンタ情報を表示 / 削除します。 • 「TX」- 送信したすべての CFM パケットのカウンタ情報を表示 / 削除します。 • 「All」- 送受信したすべての CFM パケットのカウンタ情報を表示 / 削除します。

「Find」ボタンをクリックして、指定条件に基づくカウンタ情報を検索 / 表示します。
「Show All」ボタンをクリックして、すべてのカウンタ情報を表示します。
「Clear」ボタンをクリックして、指定条件に基づいてカウンタ情報をクリアします。
「Clear All」ボタンをクリックして、すべてのカウンタ情報をクリアします。

CFM Counter CCM（CFM カウンタ CCM）

CFM カウンタ CCM 情報を表示します。

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

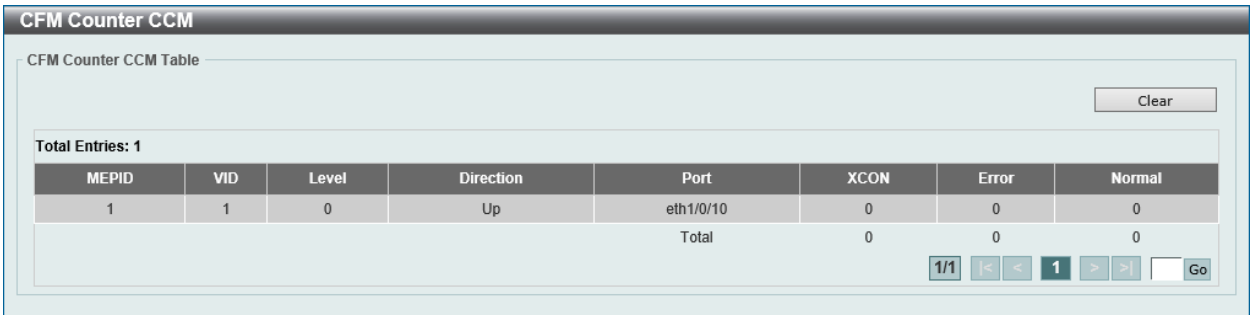


図 13-17　CFM Counter CCM 画面

「Clear」ボタンをクリックして、すべてのエントリに紐づくカウンタ情報をクリアします。
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。

CFM MIP CCM Table（CFM MIP CCM テーブル）

MIP CCM データベースエントリを表示します。

OAM > CFM > CFM MIP CCM 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。

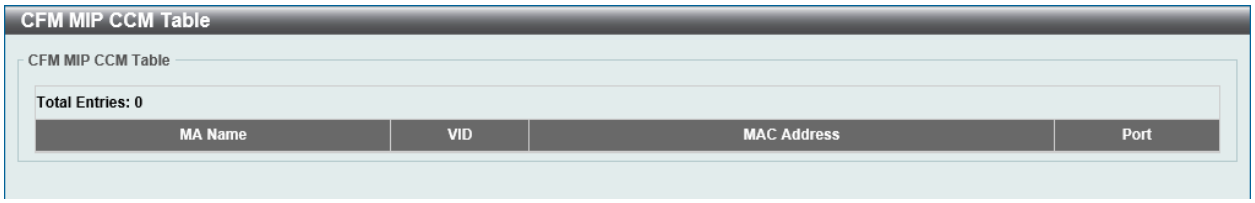


図 13-18　CFM MIP CCM Table 画面

CFM MEP Fault Table（CFM MEP 障害テーブル）

障害の発生している MEP を表示します。

OAM > CFM > CFM MEP Fault 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。

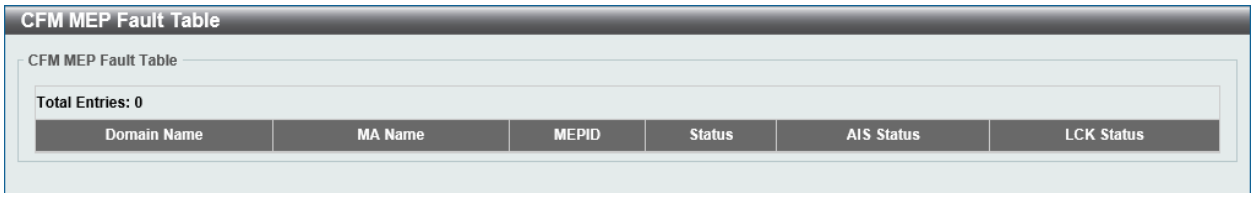


図 13-19　CFM MEP Fault Table 画面

Cable Diagnostics（ケーブル診断機能）

スイッチのポートに接続する Copper ケーブルの品質やエラーの種類を診断します。ケーブル診断機能はケーブルを簡易的に確認するために設計されています。

注意 ケーブル診断機能は簡易機能であり、参考としてご利用ください。正確な検査やテストのためには専用のテスタを使用して行ってください。

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。

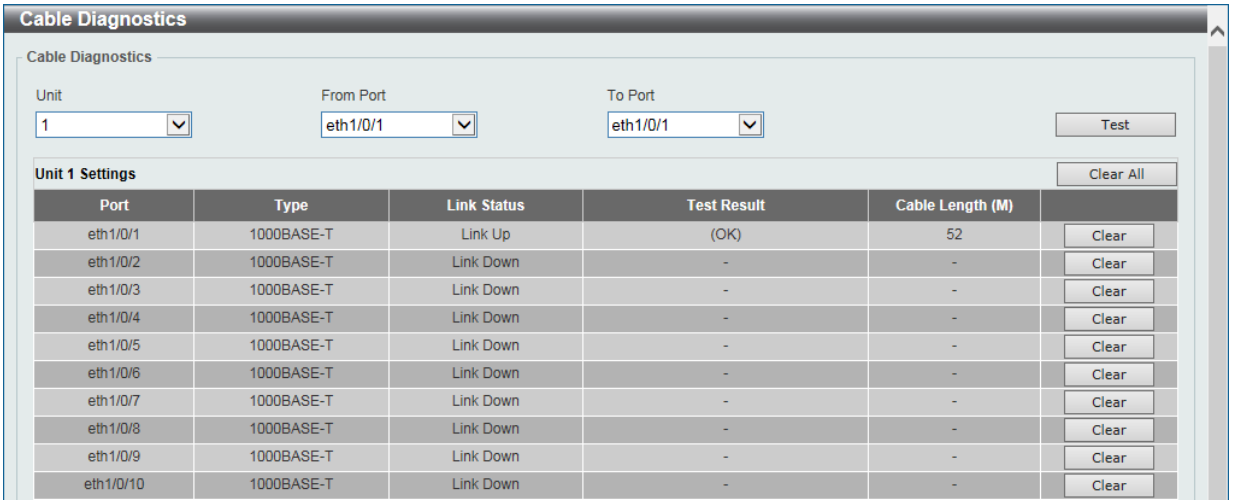


図 13-20　Cable Diagnostics 画面

画面に表示される項目：

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

「Test」ボタンをクリックして、指定ポートのケーブル診断を実行します。
「Clear」ボタンをクリックして、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て、テーブル上のすべての情報を消去します。

診断結果のメッセージは以下の通りです。

項目	説明
Test Result	ケーブル診断の結果が表示されます。 • OK - ケーブルの状態に問題はありません。 • Open - ケーブルが断線しているか、接続が外れています。 • Short - ケーブルでショート（短絡）が発生しています。 • Open or Short - ケーブルにオープン（断線）またはショート（短絡）の問題がありますが、PHY にはそれらを区別する機能がありません。 • Shutdown - リモートパートナーの電源がオフです。 • No cable - ポートには、リモートパートナーへのケーブル接続がありません。

注意 ケーブル診断機能は Copper ポートのみでサポートされます。

注意 より正確なテスト結果を得るには、RJ45 コネクタの TIA/EIA-568B ピン割り当てを使用します。

注意 10/100Mbps でリンクアップしている場合、正しい距離が表示されません。

Ethernet OAM（イーサネット OAM）

Ethernet OAM（Operations, Administration, and Maintenance）の設定を行います。
ポートに対するイーサネット OAM モード、イベントの設定や、ログの参照を行います。

Ethernet OAM Settings（イーサネット OAM 設定）

ポートにイーサネット OAM モードを設定します。

OAM > Ethernet OAM > Ethernet OAM 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。

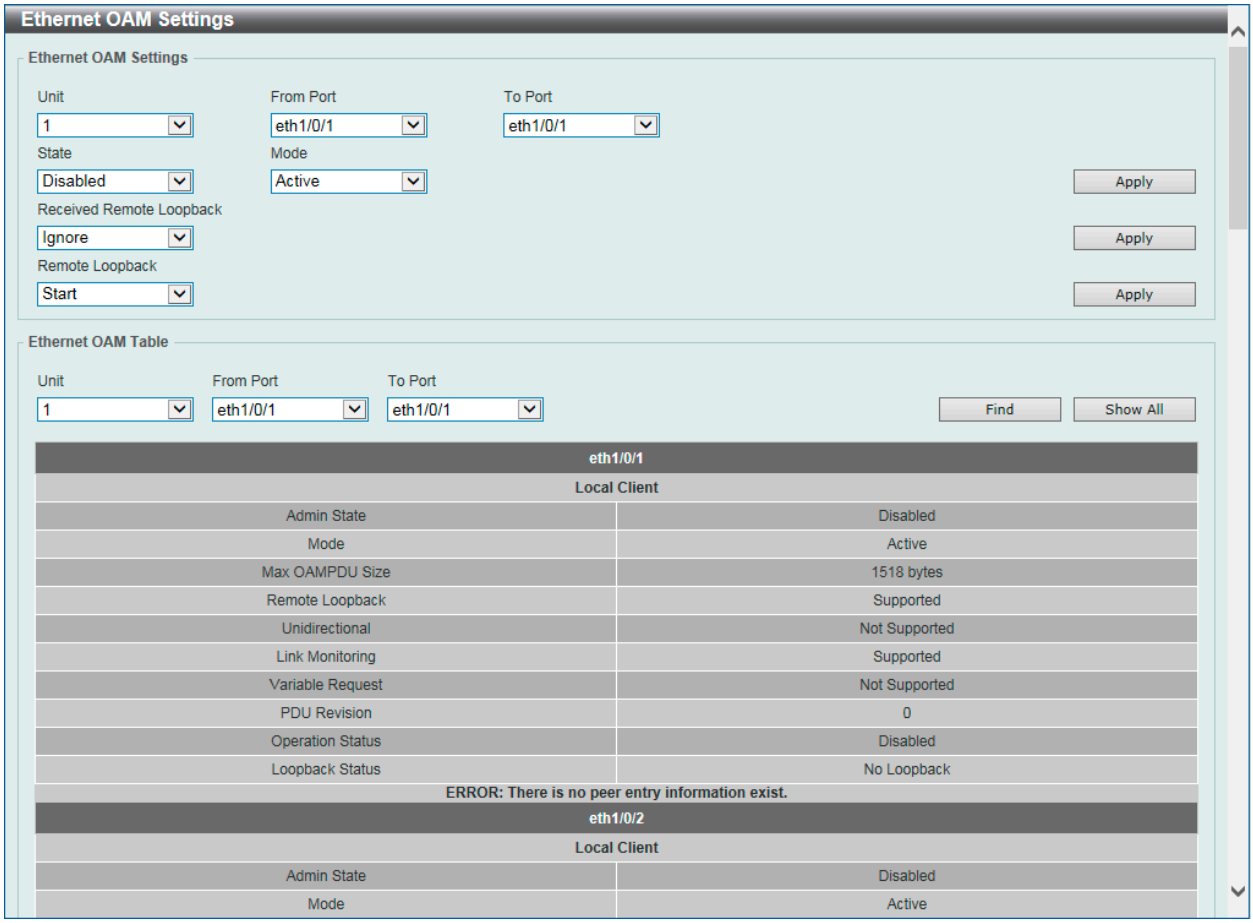


図 13-21　Ethernet OAM Settings 画面

画面に表示される項目：

項目	説明
Ethernet OAM Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートで OAM 機能を有効 / 無効に設定します。 本機能を有効化すると、インタフェースで OAM ディスカバリが開始されます。OAM モードが「Active」の場合、ディスカバリが開始され、「Passive」の場合、ピアから受信したディスカバリに応答します。
Mode	イーサネット OAM モードを指定します。 • 選択肢：「Active」「Passive」 Active モードでは、次の 2 つのアクションが許可されます。Passive モードでは許可されません。 （1）OAM ディスカバリの開始 （2）リモートループバックの開始 / 停止
Received Remote Loopback	ピアからのイーサネット OAM リモートループバック要求に対する指定ポート上での動作を指定します。 • 「Ignore」- ピアからのリモートループバック要求を無視します。 • 「Process」- ピアからのリモートループバック要求を処理します。 リモートループバックモードでは、全てのユーザトラフィックは処理されません。受信したリモートループバックを無視することで、ポートがリモートループバックモードに移行することを回避することができます。

項目	説明
Remote Loopback	リモートループバックのアクションを選択します。 ・「Start」- リモートループバックモードに変更するようにピアに要求します。 ・「Stop」- 通常の操作モードに変更するようにピアに要求します。 リモートピアがリモートループバック要求を無視するように設定されている場合、要求を受信しても、リモートピアはリモートループバックモードへの移行や離脱を行いません。リモートピアがリモートループバックモードへ移行するには、ローカルクライアントが Active モードかつ OAM 接続が確立されている必要があります。ローカルクライアントが既にリモートループバックモードの場合、本機能は適用されません。
Ethernet OAM Table	
Unit	表示するユニットを指定します。
From Port / To Port	表示するポート範囲を設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）

ポートにイーサネット OAM のイベントを設定します。

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

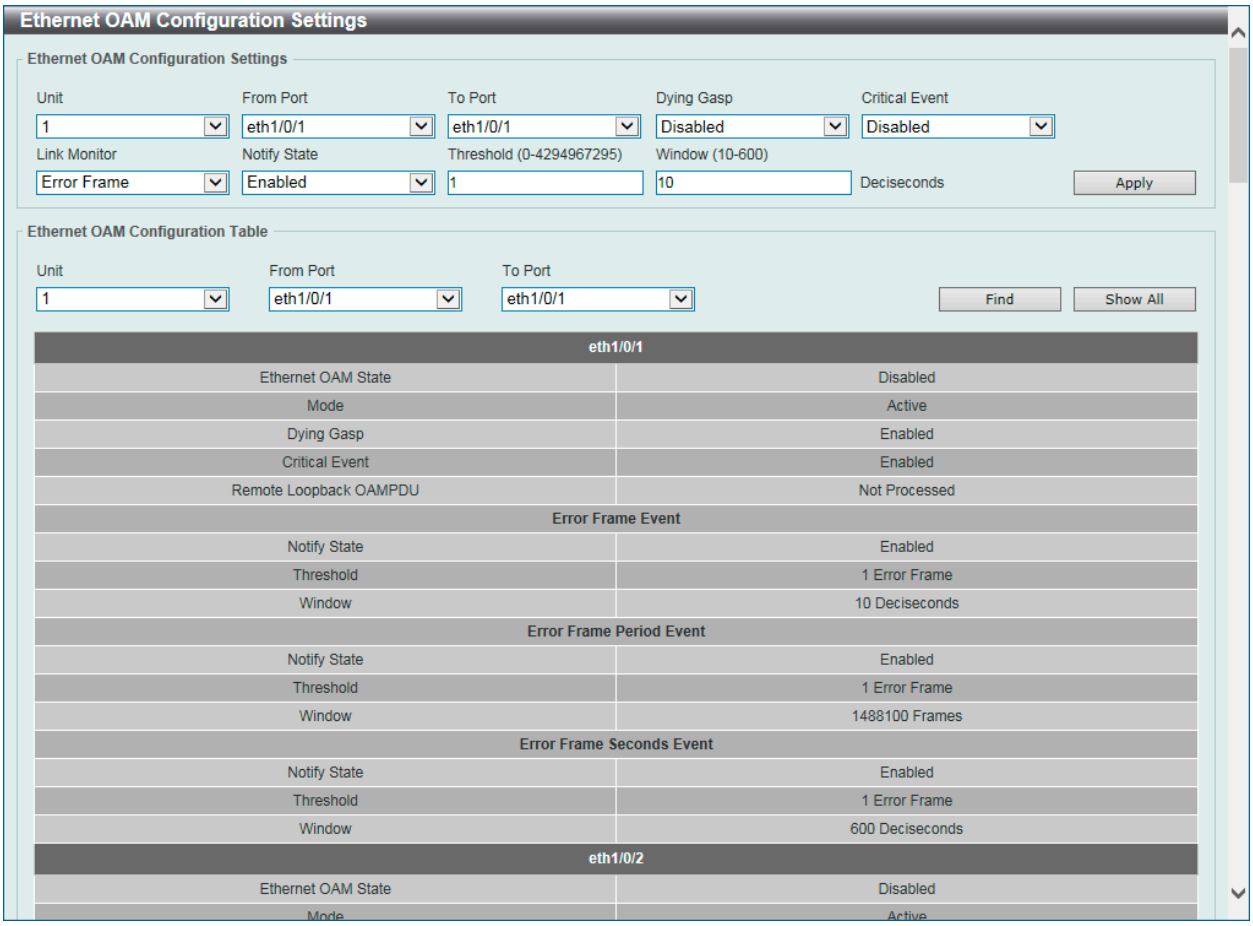


図 13-22　Ethernet OAM Configuration Settings 画面

画面に表示される項目：

項目	説明
Ethernet OAM Configuration Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Dying Gasp	「Dying Gasp」を有効 / 無効に設定します。電源障害など回復不可能なイベントの発生の検出について指定します。本機能が無効化されている場合、回復不可能なローカル障害が発生した際に、Dying Grasp イベントのビットを含む OAM PDU がポートから送信されません。
Critical Event	イーサネット OAM の重大イベント機能を有効 / 無効に設定します。本機能が無効化されている場合、指定されていない重大イベントが発生した際に、クリティカルイベントのビットを含む OAM PDU がポートから送信されません。

項目	説明
Link Monitor	リンクモニタ機能を設定します。 • 「Error Frame」- イーサネット OAM エラーフレームのイベント通知を有効化し、モニタリングのしきい値とウィンドウを設定します。 • 「Error Frame Seconds」- イーサネット OAM エラーフレーム秒のイベント通知を有効化し、モニタリングのしきい値とウィンドウを設定します。 • 「Error Frame Period」- イーサネット OAM エラーフレーム期間のイベント通知を有効化し、モニタリングのしきい値とウィンドウを設定します。
Notify State	イベント通知を有効 / 無効に設定します。
Threshold	「Error Frame」選択時：エラーフレームの数を入力します。指定期間（Window）におけるエラーフレームの数がしきい値を超えた場合、イベントが生成されます。 • 選択可能範囲：0-4294967295 「Error Frame Seconds」選択時：エラーフレームの秒数を入力します。指定期間（Window）におけるエラーフレームの秒数がしきい値を超えた場合、イベントが生成されます。 • 選択可能範囲：1-900（秒） 「Error Frame Period」選択時：エラーフレームの数を入力します。指定フレーム数（Window）におけるエラーフレームの数がしきい値を超えた場合、イベントが生成されます。 • 選択可能範囲：0-4294967295
Window	「Error Frame」選択時：この期間内でエラーフレームの発生数がしきい値を超えた場合、イベント通知の OAM PDU が生成されます。これには、しきい値を超過したことを示すエラーフレームイベント TLV が含まれます。 • 選択可能範囲：10-600（デシ秒） 「Error Frame Seconds」選択時：この期間内でエラーフレームの秒数がしきい値を超えた場合、イベント通知の OAM PDU が生成されます。これには、しきい値を超過したことを示すエラーフレーム秒サマリイベント TLV が含まれます。 • 選択可能範囲：100-9000（デシ秒） 「Error Frame Period」選択時：この指定フレーム数で発生したエラーフレームの数がしきい値を超えた場合、イベント通知の OAM PDU が生成されます。これには、しきい値を超過したことを示すエラーフレーム期間イベント TLV が含まれます。下限値は、物理レイヤにおいて 100ms 内で受信可能な最小フレームサイズのフレーム数です。上限値は、物理レイヤにおいて 1 分内で受信可能な最小フレームサイズのフレーム数です。 • 選択可能範囲：148810-892860000
Ethernet OAM Configuration Table	
Unit	設定を表示するユニットを選択します。
From Port / To Port	設定を表示するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

Ethernet OAM Event Log Table（イーサネット OAM イベントログテーブル）

ポートのイーサネット OAM イベントログ情報を表示します。

OAM > Ethernet OAM > Ethernet OAM Event Log 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。

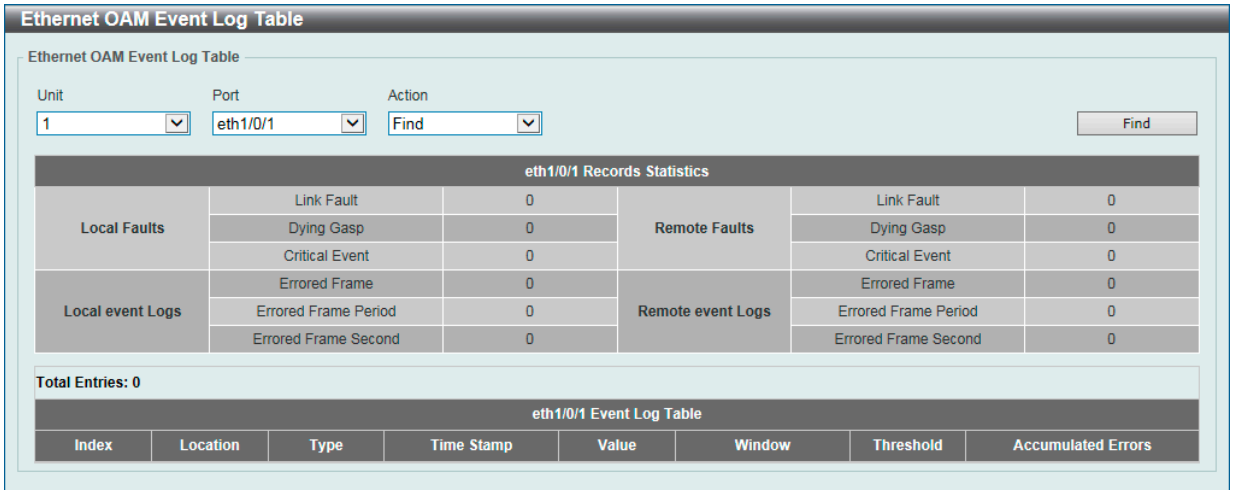


図 13-23　Ethernet OAM Event Log Table 画面

画面に表示される項目：

項目	説明
Unit	ログを参照 / 削除するユニットを指定します。
Port	ログを参照 / 削除するポート範囲を選択します。
Action	実行する動作を指定します。 • 「Find」- 指定ポートのログエントリを表示します。 • 「Clear」- 指定ポートのログエントリを削除します。

「Action」で「Find」を指定した場合の動作
「Find」ボタンをクリックして、指定ポートのログエントリを表示します。

「Action」で「Clear」を指定した場合の動作
「Clear」ボタンをクリックして、指定条件に基づくエントリを削除します。
「Clear All」ボタンをクリックして、すべてのエントリを削除します。

Ethernet OAM Statistics Table（イーサネット OAM 統計情報テーブル）

ポートのイーサネット OAM 統計情報を表示します。

OAM > Ethernet OAM > Ethernet OAM Statistics 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。

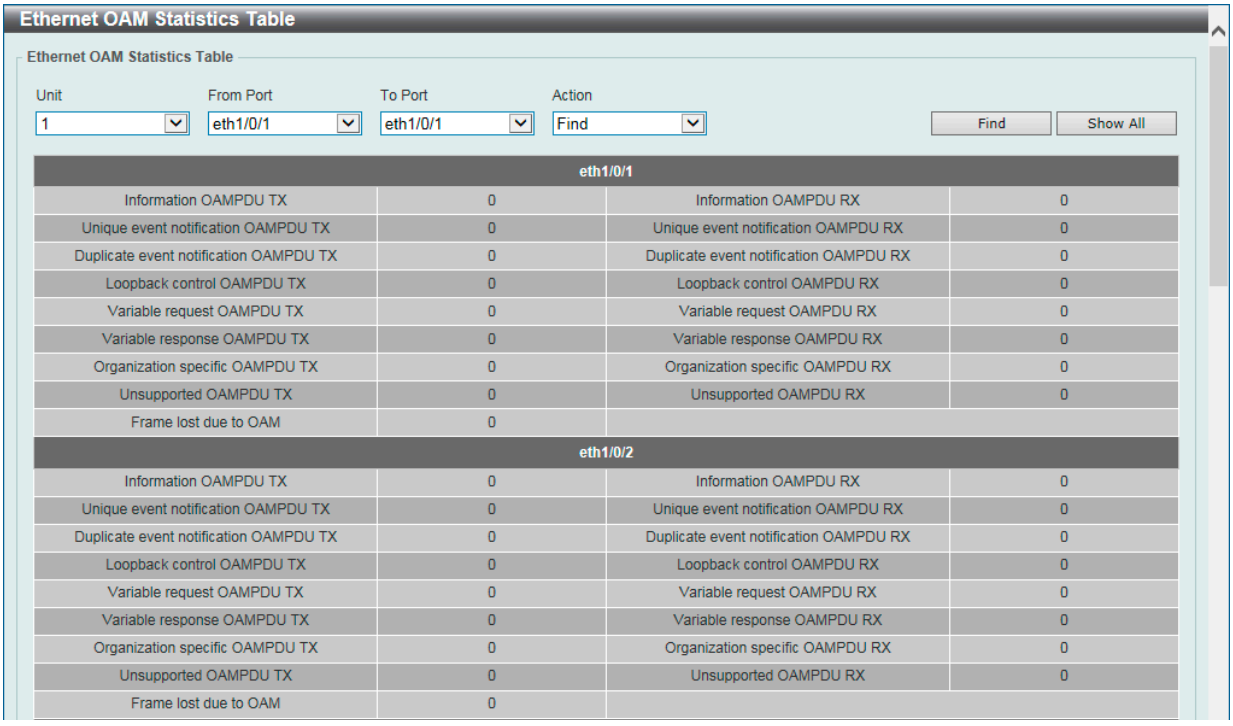


図 13-24　Ethernet OAM Statistics Table 画面

画面に表示される項目：

項目	説明
Unit	統計情報を参照 / 削除するユニットを指定します。
From Port / To Port	統計情報を参照 / 削除するポート範囲を選択します。
Action	実行する動作を指定します。 • 「Find」- 指定ポートの統計情報を表示します。 • 「Clear」- 指定ポートの統計情報を削除します。

「Action」で「Find」を指定した場合の動作
「Find」ボタンをクリックして、指定条件に基づく統計情報を表示します。
「Show All」ボタンをクリックして、すべての統計情報を表示します。

「Action」で「Clear」を指定した場合の動作
「Clear」ボタンをクリックして、指定条件に基づく統計情報を削除します。
「Clear All」ボタンをクリックして、テーブル上のすべての統計情報を削除します。

Ethernet OAM DULD Settings（イーサネット OAM DULD 設定）

イーサネット OAM「D-Link Unidirectional Link Detection」(DULD) の設定、表示を行います。
DULD は、802.3ah イーサネット OAM の拡張機能です。PHY サポート外の単方向ポイントツーポイントイーサネットリンクの検出を行います。
OAM ベンダ固有のメッセージが検出に使用されます。OAM ディスカバリの開始後に検出プロセスが開始されますが、ネゴシエーションは設定された検出時間内には完了しません。

OAM > Ethernet OAM > Ethernet OAM DULD 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。

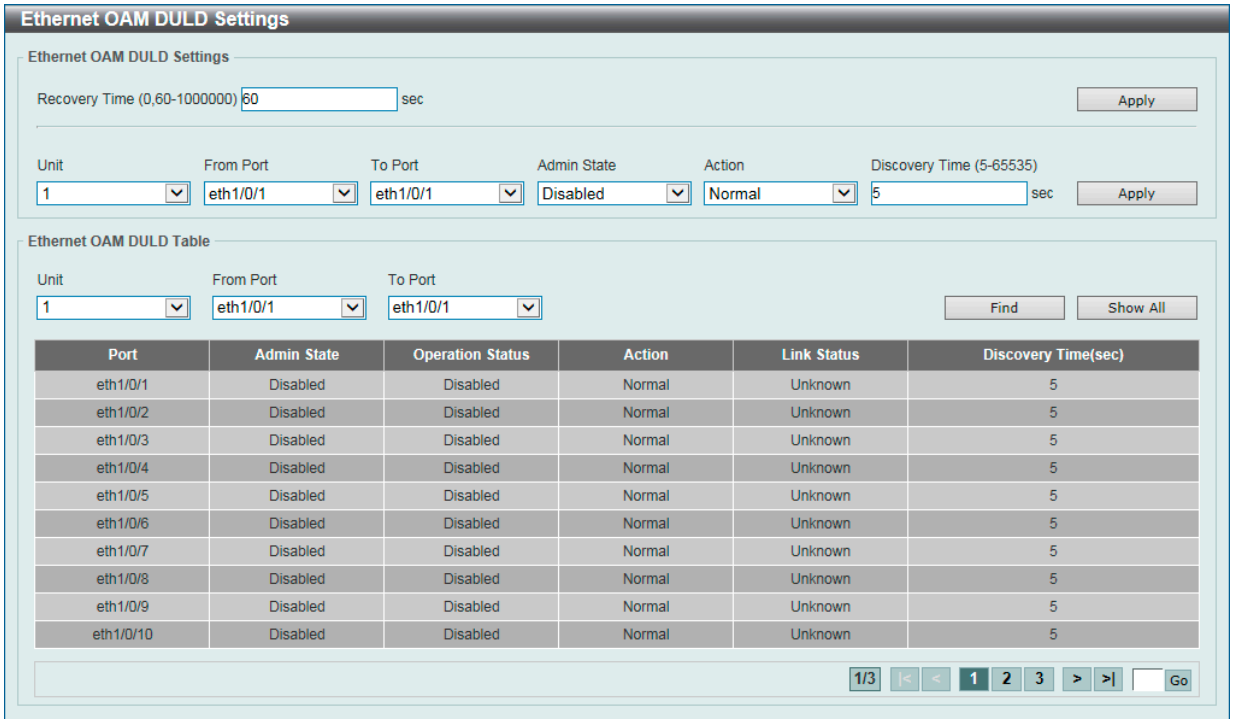


図 13-25　Ethernet OAM DULD Settings 画面

画面に表示される項目：

項目	説明
Ethernet OAM DULD Settings	
Recovery Time	イーサネット OAM の単方向リンク検出の自動リカバリ時間を入力します。 • 設定可能範囲：0, 60 - 1000000（秒） • 初期値：60（秒）
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Admin State	管理ステータスを有効 / 無効に設定します。指定ポートの単方向リンク検出状態を有効にするために使用されます。
Action	実行するアクションを選択します。 • 選択肢：「Normal」「Shutdown」
Discovery Time	検出時間を入力します。OAM ディスカバリによるネゴシエーションが正常に完了しないまま検出時間がタイムアウトになると、単方向リンク検出が開始します。 • 設定可能範囲：5-65535（秒） • 初期値：5（秒）
Ethernet OAM DULD Table	
Unit	設定を表示するユニットを指定します。
From Port / To Port	設定を表示するポート範囲を設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

DDM（DDM 設定）

Digital Diagnostic Monitoring（DDM）機能の設定を行います。スイッチに挿入した SFP/SFP+ モジュールの DDM 状態の参照、各種設定（アラーム / 警告設定、温度 / 電圧 / バイアス電流 /Tx（送信）電力 /Rx（受信）電力しきい値設定）を行うことができます。

DDM Settings（DDM 設定）

アラームしきい値や警告しきい値を超過するイベントが発生した際に、指定ポートで実行するアクションを設定します。

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

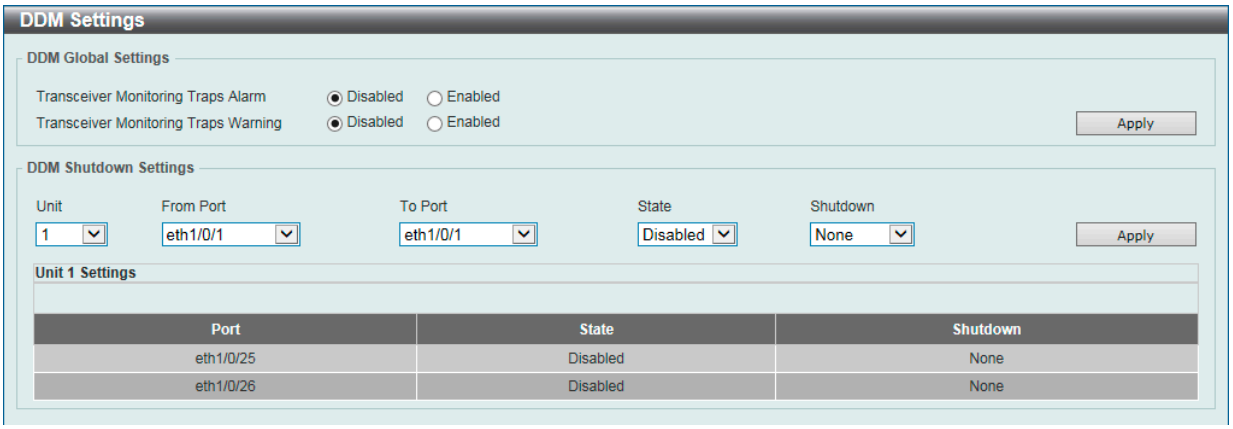


図 13-26　DDM Settings 画面

画面に表示される項目：

項目	説明
DDM Global Settings	
Transceiver Monitoring Traps Alarm	トランシーバモニタリングにおいて、アラームしきい値を超過した際にトラップを送信するか否かを指定します。
Transceiver Monitoring Traps Warning	トランシーバモニタリングにおいて、警告しきい値を超過した際にトラップを送信するか否かを指定します。
DDM Shutdown Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	DDM の状態を有効 / 無効に設定します。
Shutdown	稼働パラメータがアラームまたは 警告しきい値を超過した際に、ポートをシャットダウンするかどうかを指定します。 • 「Alarm」- アラーム（Alarm）しきい値を超過した場合にポートをシャットダウンします。 • 「Warning」- 警告（Warning）しきい値を超過した場合にポートをシャットダウンします。 • 「None」- しきい値の超過に関わらずシャットダウンは実行されません。（初期値）

「Apply」ボタンをクリックして、設定内容を適用します。

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

スイッチの特定ポートに DDM 温度しきい値設定を行います。

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

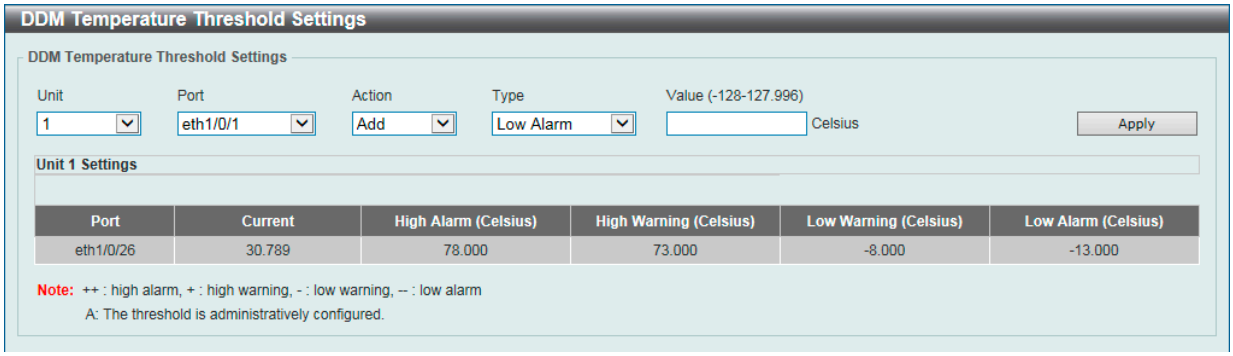


図 13-27　DDM Temperature Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	温度しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	温度しきい値の値について指定します。 • 設定可能範囲：-128 ～ 127.996（℃）

「Apply」ボタンをクリックして、設定内容を適用します。

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

スイッチの特定ポートに電圧しきい値を設定します。

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

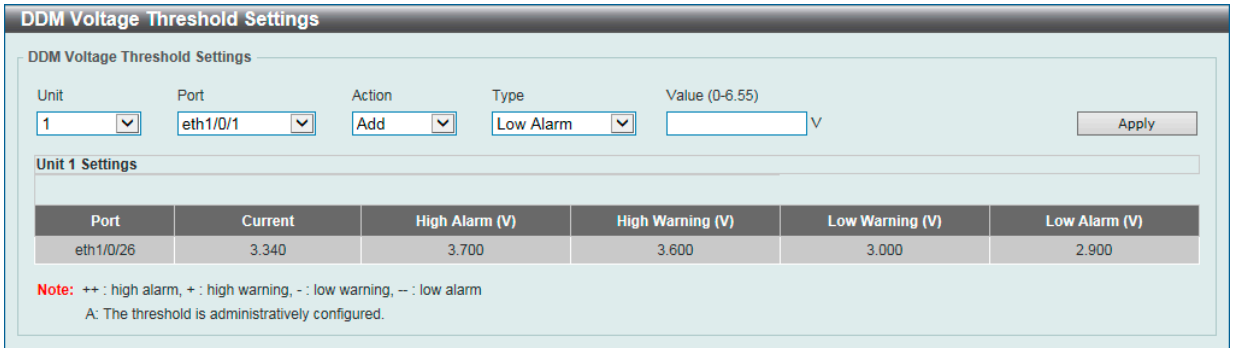


図 13-28　DDM Voltage Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	電圧しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	電圧しきい値の値について指定します。 • 設定可能範囲：0-6.55（V）

「Apply」ボタンをクリックして、設定内容を適用します。

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

スイッチの特定ポートにバイアス電流しきい値を設定します。

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

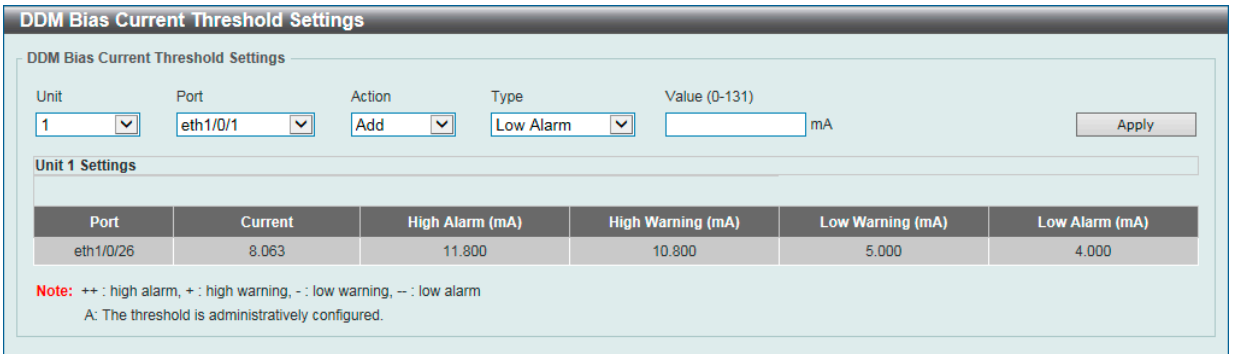


図 13-29　DDM Bias Current Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポートを指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	バイアス電流しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	バイアス電流しきい値の値について指定します。 • 設定可能範囲：0-131（mA）

「Apply」ボタンをクリックして、設定内容を適用します。

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

スイッチの特定ポートに送信電力しきい値を設定します。

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

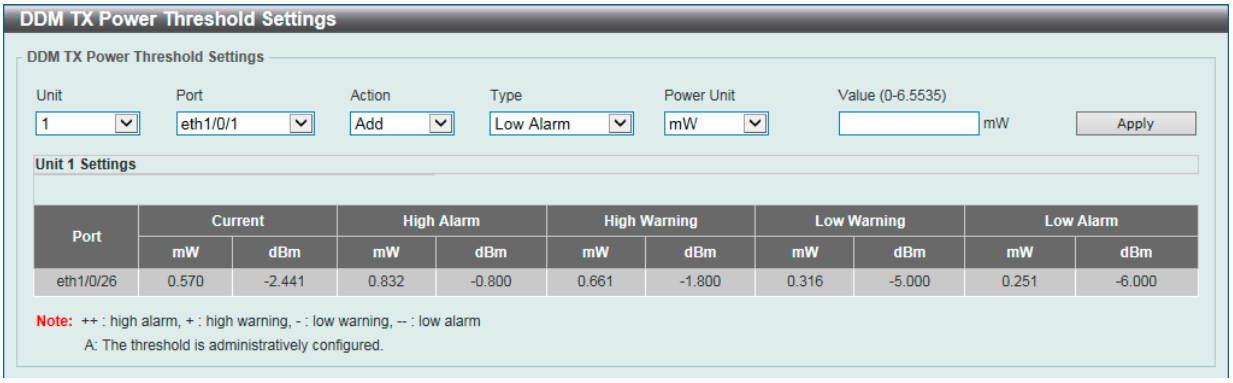


図 13-30　DDM TX Power Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	送信電力しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Power Unit	送信電力単位について指定します。 • 選択肢：「mW」「dBm」

項目	説明
Value	送信電力しきい値の値について指定します。 • 設定可能範囲：0-6.5535（mW） -40 ～ 8.1647（dBm）

「Apply」ボタンをクリックして、設定内容を適用します。

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

スイッチの特定ポートに受信電力しきい値を設定します。

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

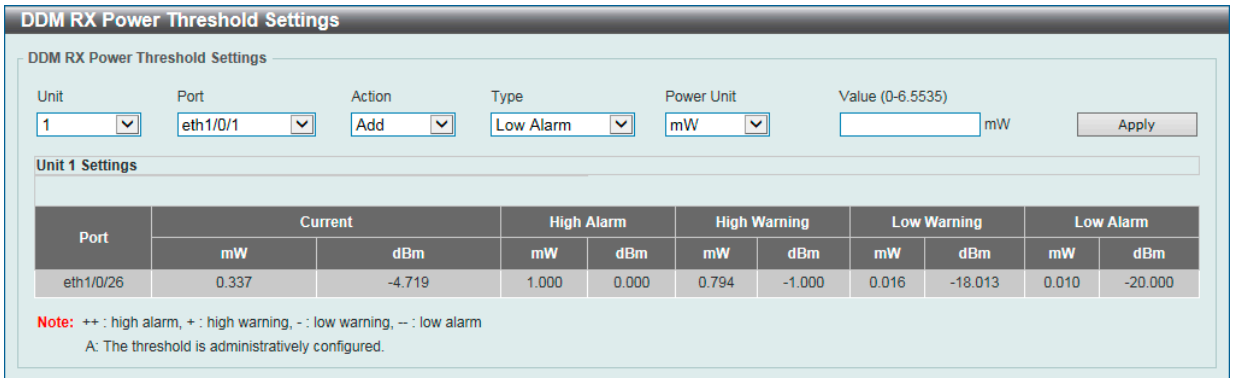


図 13-31　DDM RX Power Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	受信電力しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Power Unit	受信電力単位について指定します。 • 選択肢：「mW」「dBm」
Value	受信電力しきい値の値について指定します。 • 設定可能範囲：0-6.5535（mW） -40 ～ 8.1647（dBm）

「Apply」ボタンをクリックして、設定内容を適用します。

DDM Status Table（DDM ステータステーブル）

指定ポートで現在動作中の DDM パラメータと SFP モジュールにおける値を表示します。

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

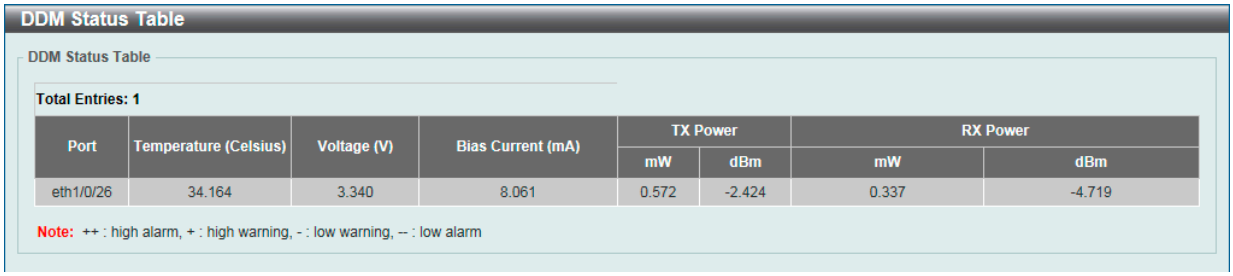


図 13-32図 13-8　　DDM Status Table 画面

第 14 章　Monitoring（スイッチのモニタリング）

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

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

サブメニュー	説明
VLAN Counter（VLAN カウンタ）	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを作成します。
Utilization（利用分析）	スイッチの Utilization（利用分析）を表示します。
Statistics（統計情報）	スイッチの Statistics（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。対象ポートで送受信するフレームをコピーし、フレームの出力先を他のポートに変更する機能（ポートミラーリング）です。
sFlow（sFlow 設定）	sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。
Device Environment（機器環境確認）	Device Environment（機器環境確認）ではスイッチの内部の温度状態を表示します。

VLAN Counter（VLAN カウンタ）

本画面では、VLAN カウンタの設定、表示を行います。
指定の L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを作成します。

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

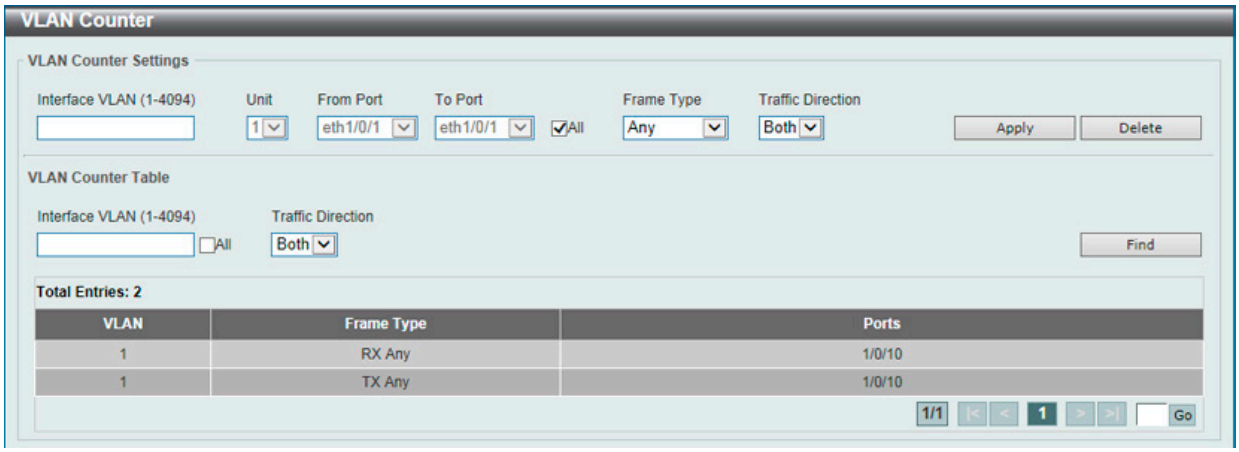


図 14-1　VLAN Counter 画面

画面に表示される項目：

項目	説明
VLAN Counter Settings	
Interface VLAN	インタフェース VLAN を指定します。 • 設定可能範囲：1-4094
Unit	本設定を適用するユニットを指定します。 「All」オプションにチェックを入れている場合、すべてのユニット / ポートが対象となります。
From Port / To Port	本設定を適用するポート範囲を指定します。 「All」オプションにチェックを入れている場合、すべてのユニット / ポートが対象となります。
Frame Type	フレームタイプを指定します。 • 「Broadcast」- ブロードキャストフレームのみをカウントします。 • 「Multicast」- マルチキャストフレームのみをカウントします。 • 「Unicast」- ユニキャストフレームのみをカウントします。 • 「Any」- フレームタイプに関係なく全てのフレームをカウントします。 • 「All」- 上記全てのフレームをカウントします。
Traffic Direction	トラフィックの向きを指定します。 • 「RX」- イングレストラフィックをカウントします。 • 「TX」- イーグレストラフィックをカウントします。 • 「Both」- イングレス / イーグレス両方のトラフィックをカウントします。
VLAN Counter Table	
Interface VLAN	検索するインタフェース VLAN を指定します。「All」にチェックを入れるとすべての VLAN が対象になります。 • 設定可能範囲：1-4094
Traffic Direction	トラフィックの向きを指定します。 • 「RX」- イングレストラフィックカウンタの設定を表示します。 • 「TX」- イーグレストラフィックカウンタの設定を表示します。 • 「Both」- 両方のトラフィックカウンタの設定を表示します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報を基に特定のエントリを検出します。
「Delete」ボタンをクリックして、指定した情報を基に特定のエントリを削除します。

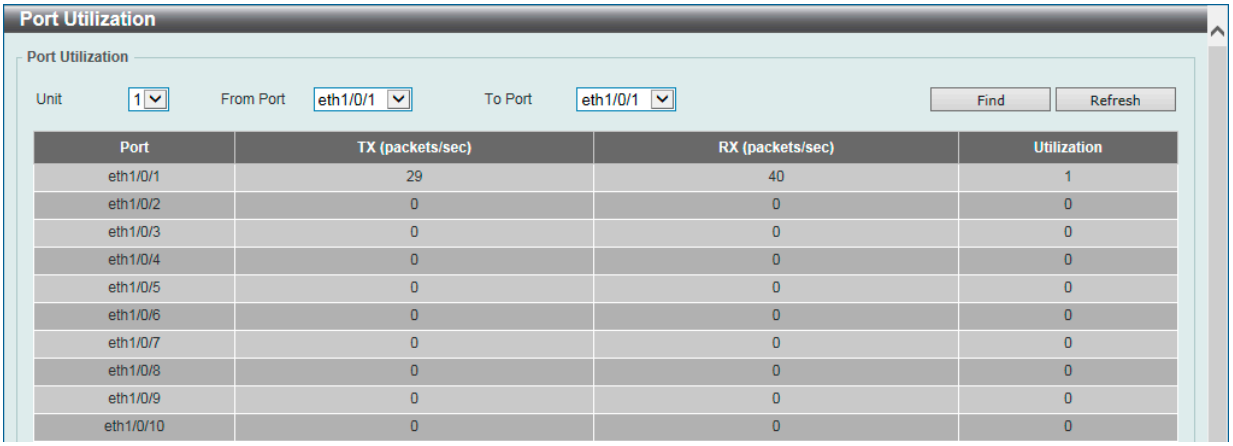
Utilization（利用分析）

CPU 使用率、ポートの帯域使用率などを表示します。

Port Utilization（ポート使用率）

本画面では、ポートの帯域使用率を表示します。

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



Port	TX (packets/sec)	RX (packets/sec)	Utilization
eth1/0/1	29	40	1
eth1/0/2	0	0	0
eth1/0/3	0	0	0
eth1/0/4	0	0	0
eth1/0/5	0	0	0
eth1/0/6	0	0	0
eth1/0/7	0	0	0
eth1/0/8	0	0	0
eth1/0/9	0	0	0
eth1/0/10	0	0	0

図 14-2　Port Utilization 画面

画面に表示される項目：

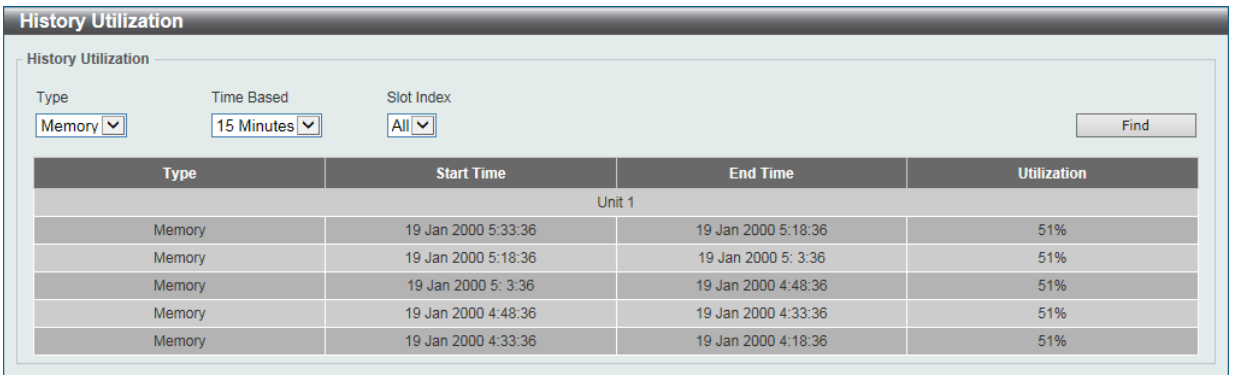
項目	説明
Unit	ポート使用率を表示するユニットを指定します。
From Port / To Port	ポート使用率を表示するポート範囲を指定します。

「Find」ボタンをクリックして、指定ポートのエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。

History Utilization（使用率履歴）

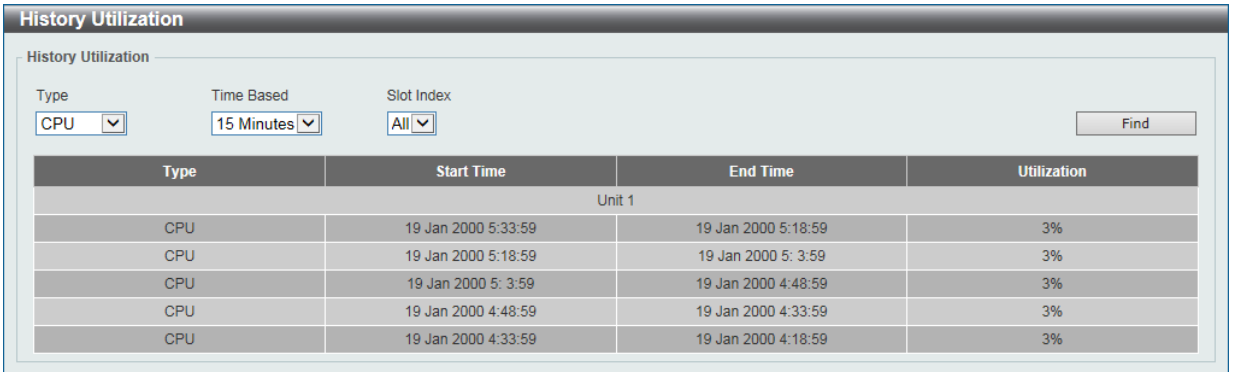
本項目ではメモリ、CPU およびポートの使用率履歴について表示します。

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



Type	Start Time	End Time	Utilization
Unit 1			
Memory	19 Jan 2000 5:33:36	19 Jan 2000 5:18:36	51%
Memory	19 Jan 2000 5:18:36	19 Jan 2000 5: 3:36	51%
Memory	19 Jan 2000 5: 3:36	19 Jan 2000 4:48:36	51%
Memory	19 Jan 2000 4:48:36	19 Jan 2000 4:33:36	51%
Memory	19 Jan 2000 4:33:36	19 Jan 2000 4:18:36	51%

図 14-3　History Utilization (Memory) 画面



Type	Start Time	End Time	Utilization
Unit 1			
CPU	19 Jan 2000 5:33:59	19 Jan 2000 5:18:59	3%
CPU	19 Jan 2000 5:18:59	19 Jan 2000 5: 3:59	3%
CPU	19 Jan 2000 5: 3:59	19 Jan 2000 4:48:59	3%
CPU	19 Jan 2000 4:48:59	19 Jan 2000 4:33:59	3%
CPU	19 Jan 2000 4:33:59	19 Jan 2000 4:18:59	3%

図 14-4　History Utilization (CPU) 画面

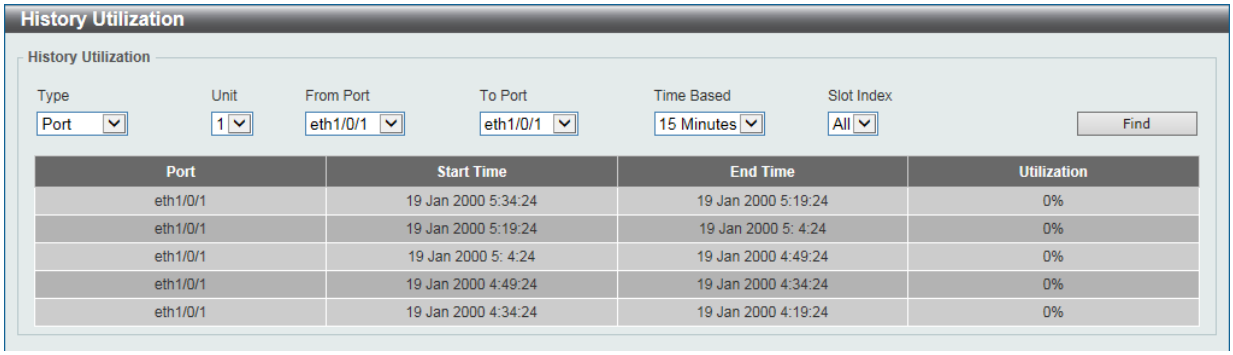


図 14-5　History Utilization (Port) 画面

画面に表示される項目：

項目	説明
Type	表示する使用率履歴の種類を指定します。 • 「Memory」- メモリの使用率履歴を表示します。 • 「CPU」- CPU の使用率履歴を表示します。 • 「Port」- ポートの使用率履歴を表示します。
Unit	「Port」を選択した場合、使用率履歴を表示するユニットを指定します。
From Port / To Port	「Port」を選択した場合、使用率履歴を表示するポート範囲を指定します。
Time Based	表示する統計情報の期間を指定します。 • 「15 Minutes」- 15 分間単位の使用率情報を表示します。 • 「1 Day」- 1 日単位の使用率情報を表示します。 「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1Day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。
Slot Index	スロットのインデックスを指定します。 • 選択肢：All、1- 5（「15 Minutes」選択時）、1-2（「1 Day」選択時）

「Find」ボタンをクリックして、指定した情報を基に特定のエントリを検出します。

注意　show cpu utilization コマンドでは、2 Core のそれぞれの状態が表示されます。

Statistics（統計情報）

スイッチの統計情報を表示します。

Port（ポート統計情報）

ポートのパケット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。

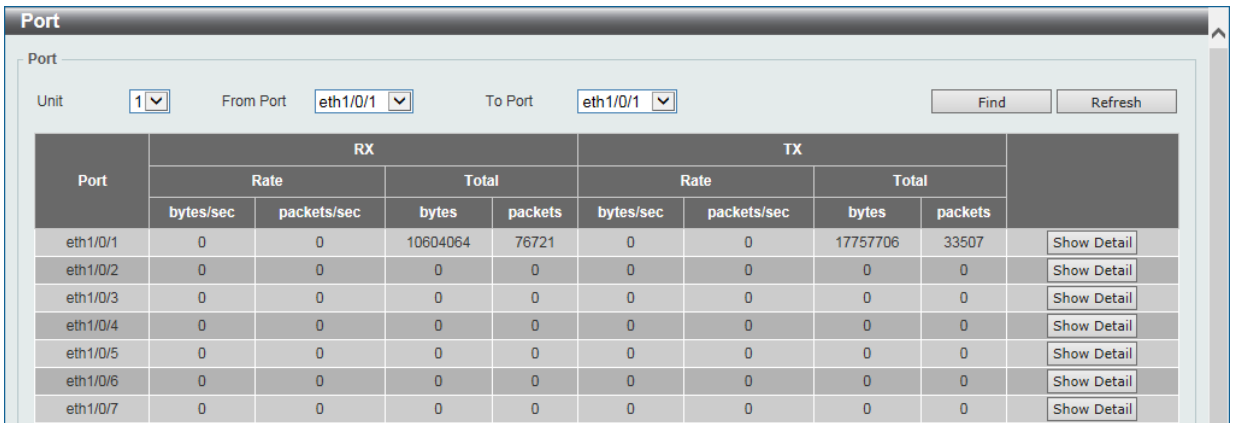


図 14-6　Port 画面

画面に表示される項目：

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

「Find」ボタンをクリックして、指定ポートのエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Show Detail」ボタンをクリックして、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。

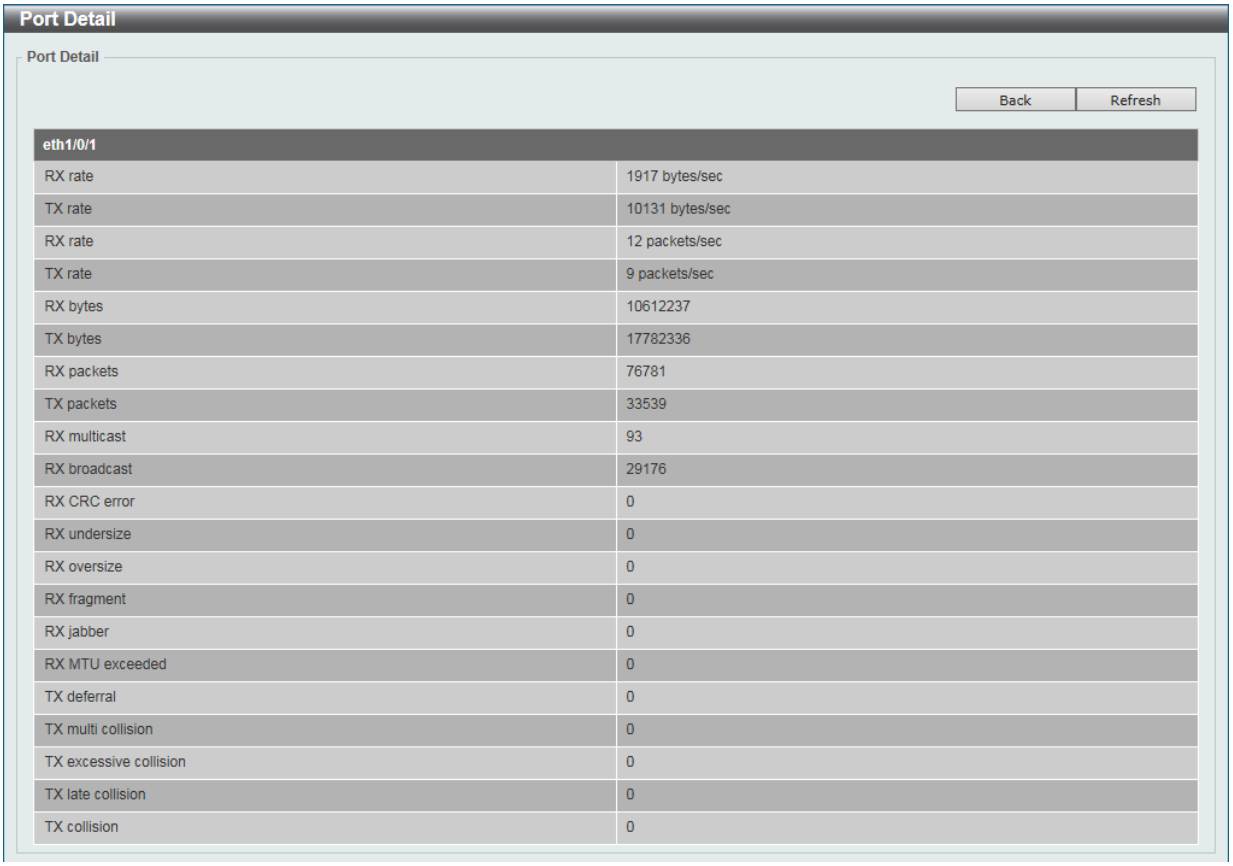


図 14-7　Port（Show Detail）- Port Detail 画面

「Refresh」ボタンをクリックし、テーブルの情報を更新します。
前の画面に戻るには、「Back」ボタンをクリックします。

CPU Port（CPU ポート）

CPU の統計情報について表示します。

Monitoring > Statistics > CPU 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。

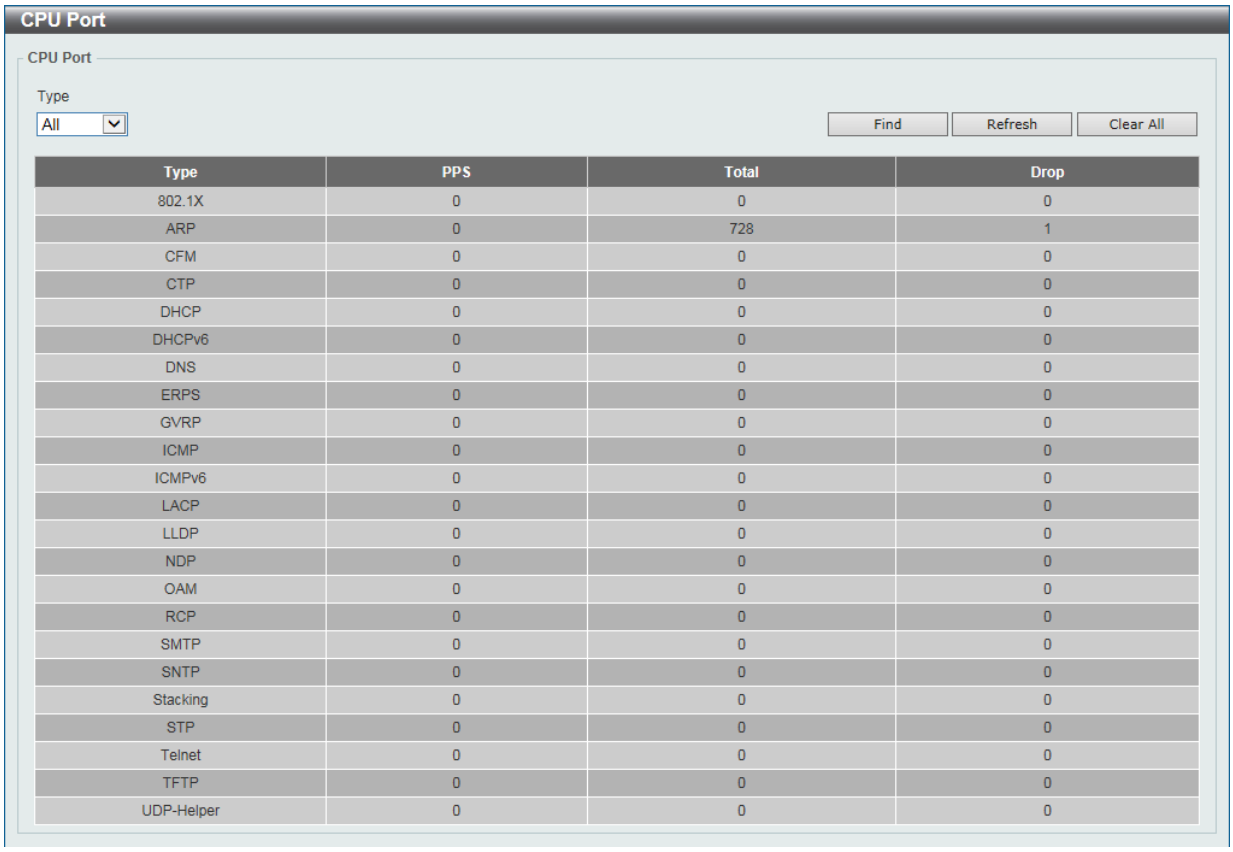


図 14-8　CPU Port 画面

画面に表示される項目：

項目	説明
Type	表示する情報のタイプを指定します。「Protocol」を指定した場合、表示される入力欄にプロトコル名を入力します。 • 選択肢：「All」「L2」「L3」「Protocol」

「Find」ボタンをクリックして、指定した情報を基に特定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。

Interface Counters（インタフェースカウンタ）

インタフェースカウンタ情報について表示します。

Monitoring > Statistics > Interface 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。

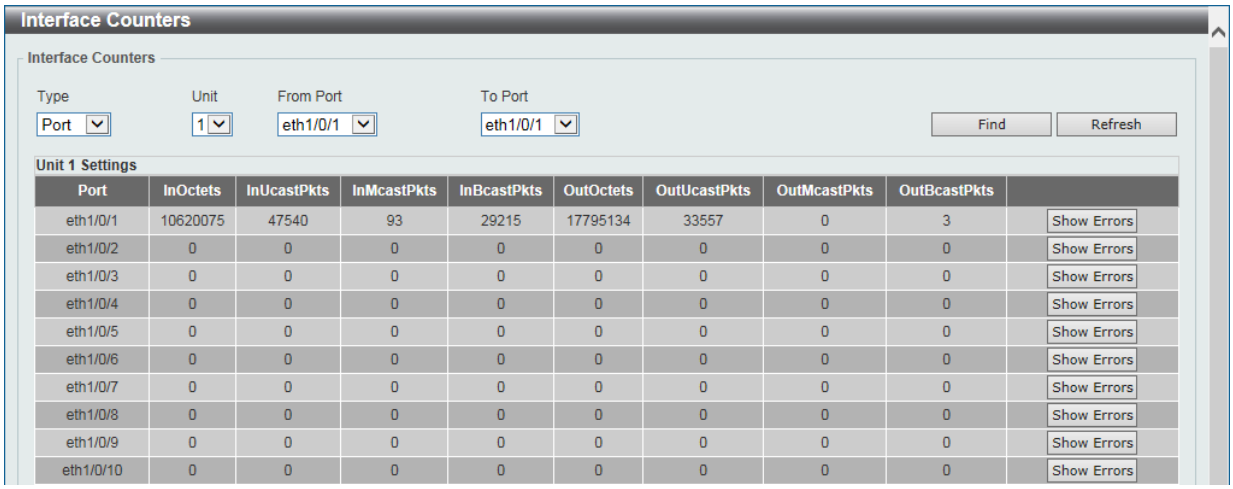


図 14-9　Interface Counters 画面（Port 選択時）

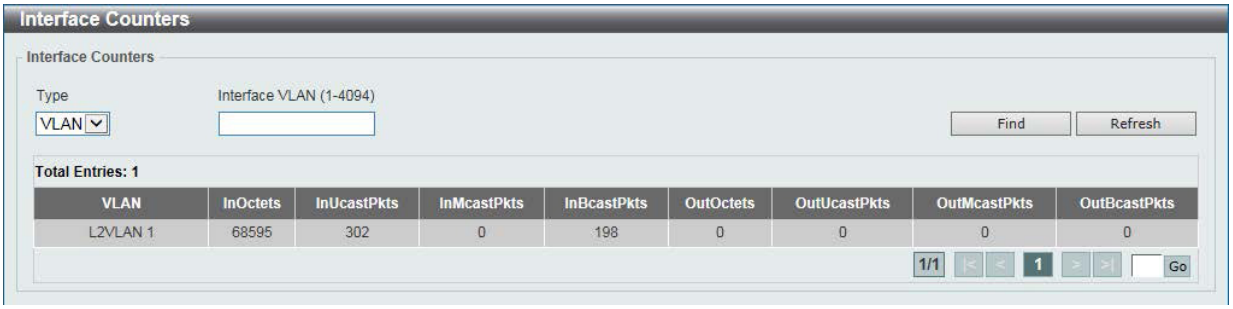


図 14-10　Interface Counters 画面（VLAN 選択時）

画面に表示される項目：

項目	説明
Type	表示する情報のタイプを指定します。 • 選択肢：「Port」「VLAN」
Unit	「Port」を選択した場合、インタフェースカウンタを表示するユニットを指定します。
From Port / To Port	「Port」を選択した場合、インタフェースカウンタを表示するポート範囲を指定します。
Interface VLAN	「VLAN」を選択した場合、表示する VLAN インタフェースの ID を指定します。 • 設定可能範囲：1-4094

「Find」ボタンをクリックして、指定した情報を基に指定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Show Errors」ボタンをクリックして、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。

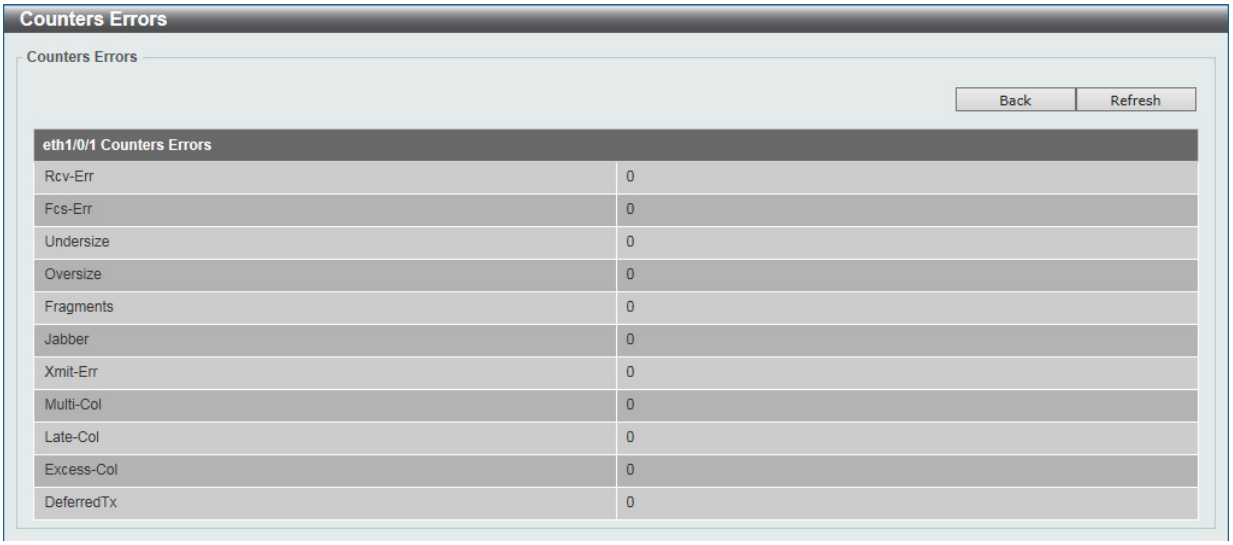


図 14-11　Interface Counters (Show Errors) 画面

前の画面に戻るには、「Back」ボタンをクリックします。
「Refresh」ボタンをクリックし、テーブルの情報を更新します。

Interface History Counters（インタフェースカウンタ履歴）

本項目ではインタフェースにおけるカウンタの履歴を表示します。

Monitoring > Statistics > Interface History 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。

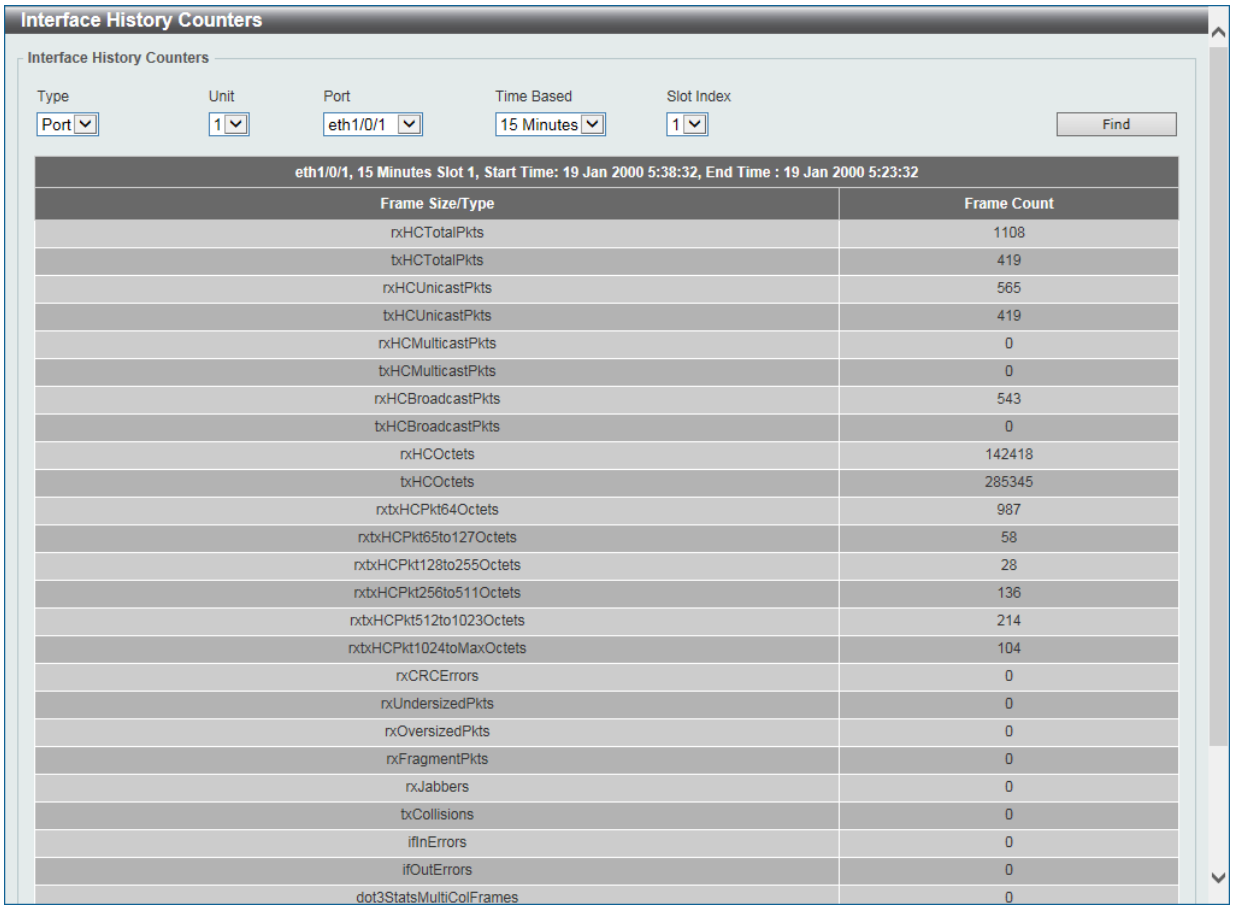


図 14-12　Interface History Counters 画面

画面に表示される項目：

項目	説明
Type	表示する情報のタイプを指定します。 • 選択肢：「Port」
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。
Time Based	表示する統計情報の期間を指定します。 • 「15 Minutes」- 15 分間単位の使用情報を表示します。 • 「1 Day」- 1 日単位の使用情報を表示します。 「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1Day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。
Slot Index	スロットのインデックスを指定します。 • 選択肢：1-5（「15 Minutes」選択時）、1-2（「1 Day」選択時）

「Find」ボタンをクリックして、指定した情報を基に特定のエントリを検出します。

補足　受信パケットサイズが 1536Bytes を超える場合、dot3StatsFrameTooLongs の数値が増加します。

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。

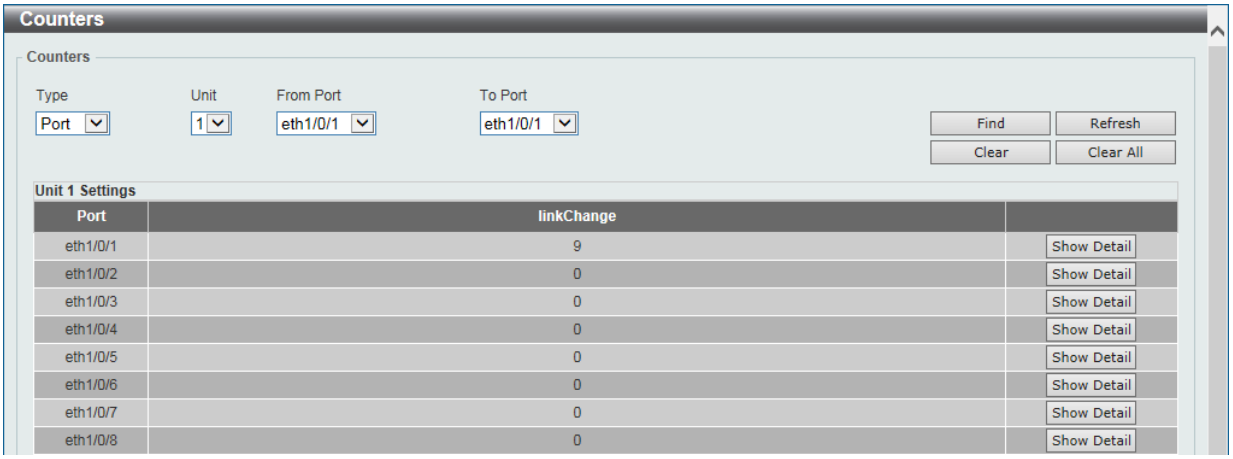


図 14-13　Counters 画面（Port 選択時）

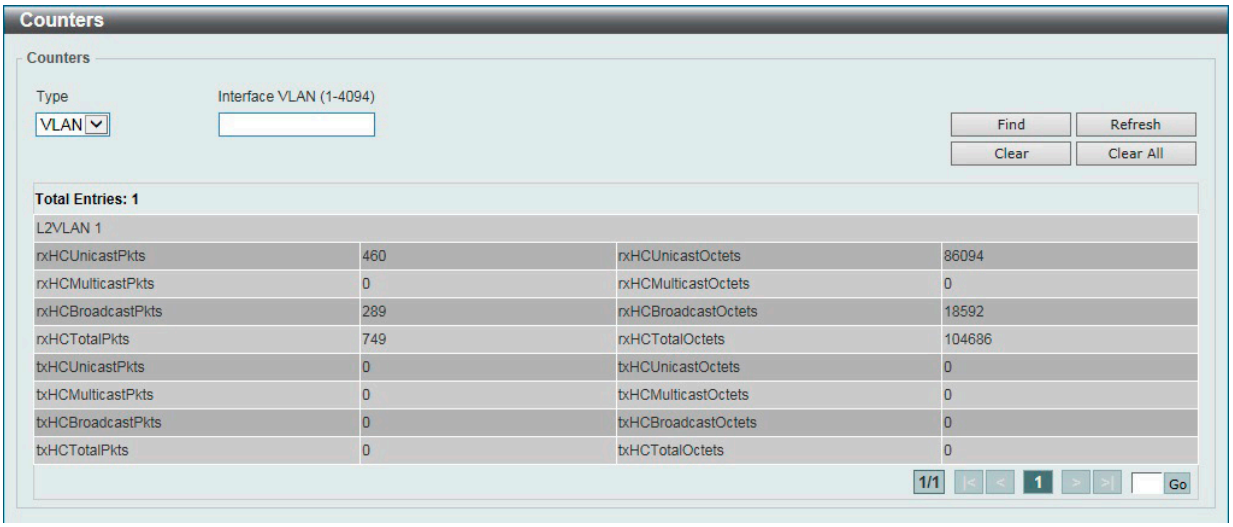


図 14-14　Counters 画面（VLAN 選択時）

画面に表示される項目：

項目	説明
Type	表示するタイプを指定します。 • 「Port」- ポート毎のカウンタを表示します。 • 「VLAN」- VLAN 毎のカウンタを表示します。
Unit	「Port」を選択した場合、表示するユニットを選択します。
From Port / To Port	「Port」を選択した場合、表示するポート範囲を指定します。
Interface VLAN	「VLAN」を選択した場合、表示するインタフェース VLAN ID を指定します。

「Find」ボタンをクリックして、指定 / 入力した情報を基に特定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Clear」ボタンをクリックして、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て、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て、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。

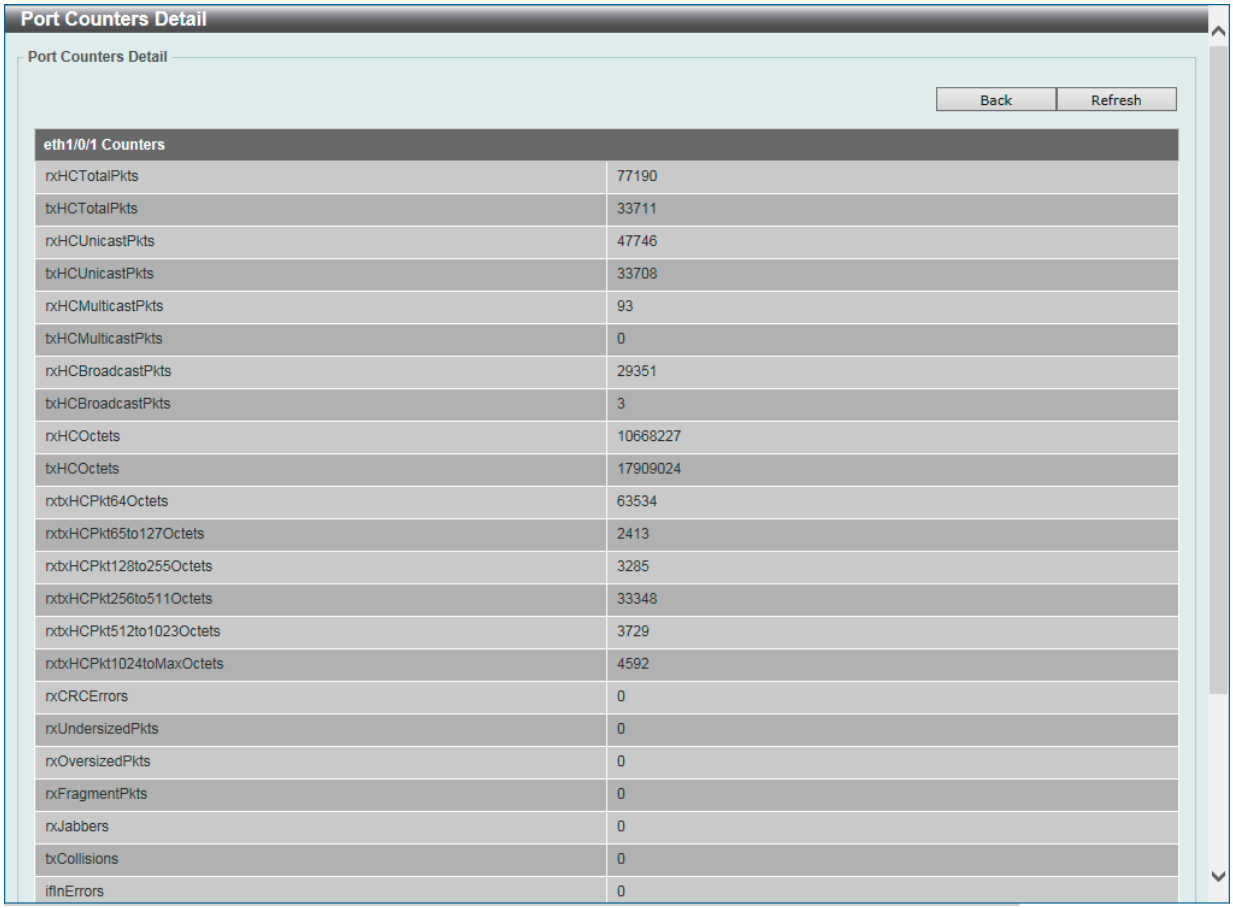


図 14-15　Counters（Show Detail）- Port Counters Detail 画面

「Refresh」ボタンをクリックし、テーブルの情報を更新します。
前の画面に戻るには、「Back」ボタンをクリックします。

補足　受信パケットサイズが 1536Bytes を超える場合、rxOversizedPkts の数値が増加します。

Mirror Settings（ミラー設定）

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

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

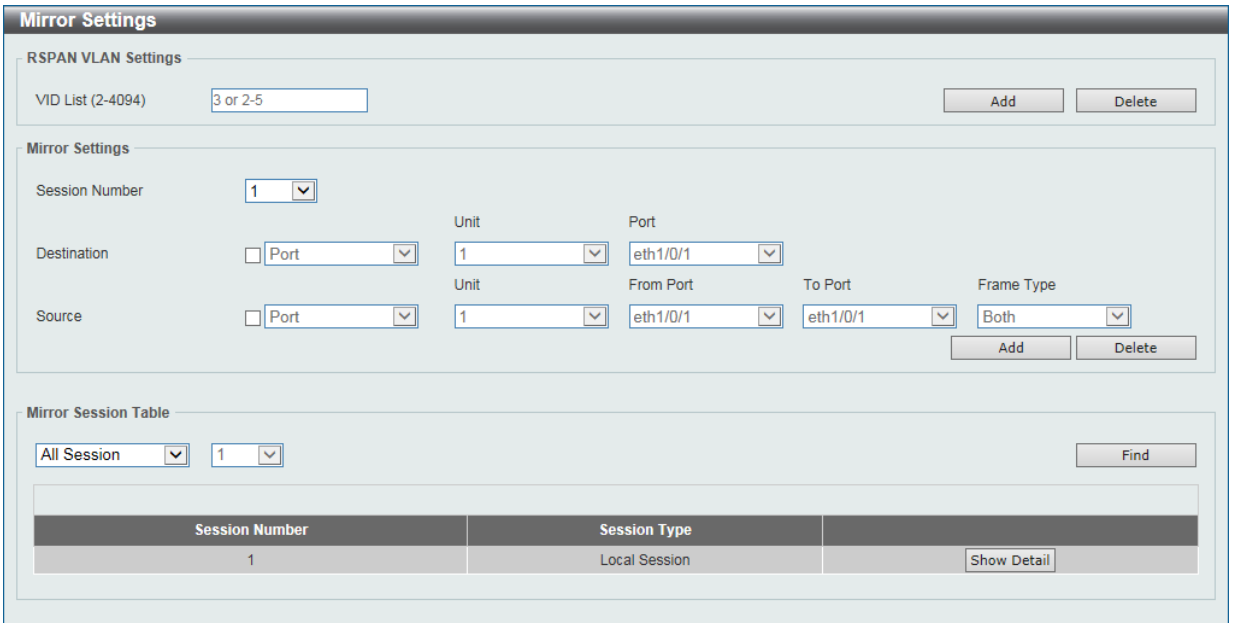


図 14-16　Mirror Settings 画面

画面に表示される項目：

項目	説明
RSPAN VLAN Settings	
VID List	VLAN ID のリストを指定します。
Mirror Settings	
Session Number	このエントリのセッション番号を指定します。 • 設定可能範囲：1-4
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タイプを設定します。 • 宛先タイプオプションの選択肢：「Port」「Remote VLAN」 - 「Unit」ユニット ID を指定します。 - 「Port」- ポート番号を指定します。 - 「Remote VLAN」-「Remote VLAN」を選択した場合、「VID」（2-4094）を指定します。
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タイプを設定します。 • 送信元タイプオプションの選択肢：「Port」「ACL」「VLAN」「Remote VLAN」 • 「Port」を選択した場合、以下の設定を行います。 - 「Unit」：ユニット ID を指定します。 - 「From Port / To Port」：ポート範囲を指定します。 - 「Frame Type」：ミラーリングされるフレームの種類を「Both」（両方）、「RX」（受信データ）、「TX」（送信データ）から指定します。 • 「ACL」を選択した場合、以下の設定を行います。 - 「ACL」：ACL 名を入力します。 • 「VLAN」を選択した場合、以下の設定を行います。 - 「VID List」：VID リストを入力します。 - 「Frame Type」：ミラーリングされるフレームの種類は「RX」（受信データ）のみサポートされます。 • 「Remote VLAN」を選択した場合、以下の設定を行います。 - 「VID」：VLAN ID（2-4094）を指定します。

項目	説明
Mirror Session Table	
Mirror Session Type	表示する情報のミラーセッションタイプを選択します。 • 選択肢：「All Session」「Session Number」「Remote Session」「Local Session」 「Session Number」を選択した場合、ドロップダウンメニューからセッション番号（1-4）を選択します。

「Add」ボタンをクリックして、指定 / 入力した情報に基づき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、指定 / 入力した情報に基づき既存のミラーエントリを削除します。
「Find」ボタンをクリックして、指定した情報に基づいたエントリを検出します。

「Show Detail」リンクをクリックし、以下の画面を表示します。

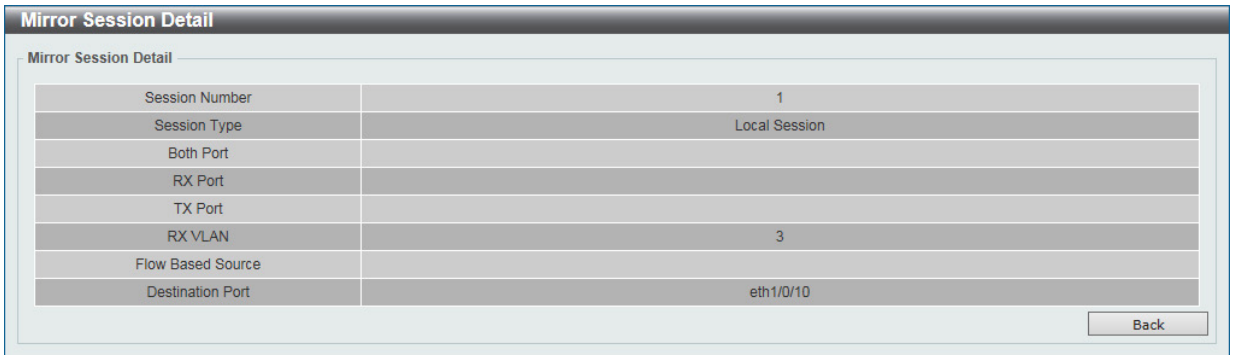


図 14-17　Mirror Settings（Show Detail）- Mirror Session Detail 画面

「Back」をクリックして、前の画面に戻ります。

sFlow（sFlow 設定）

sFlow は、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。

sFlow Agent Information（sFlow エージェント情報）

sFlow エージェント情報を表示します。

Monitoring > sFlow > sFlow Agent 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。

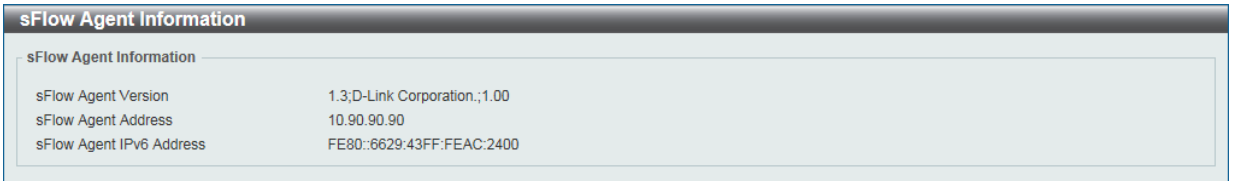


図 14-18　sFlow Agent Information 画面

sFlow Receiver Settings（sFlow レシーバ設定）

sFlow エージェントのレシーバについて設定、表示を行います。レシーバは sFlow エージェントから追加または削除することはできません。

Monitoring > sFlow > sFlow Receiver 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。

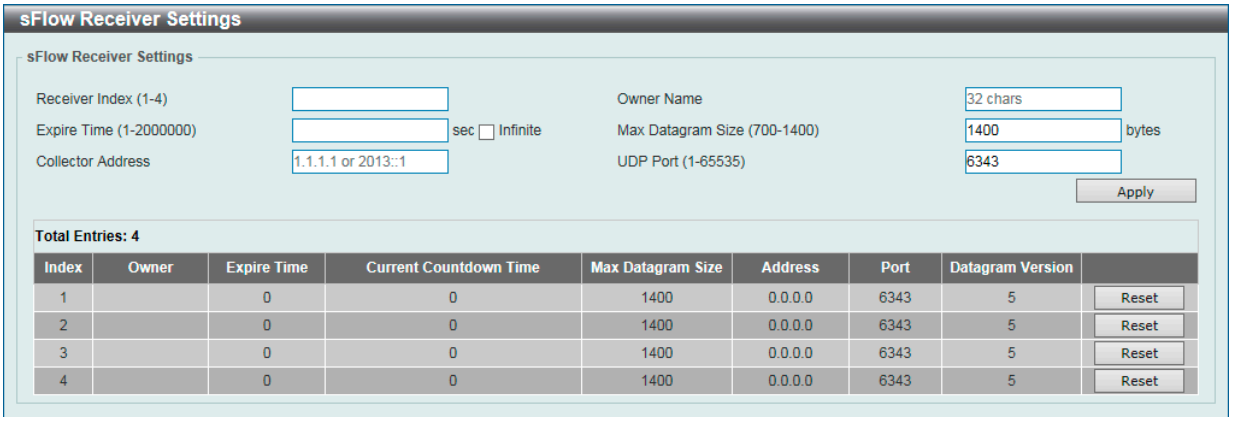


図 14-19　sFlow Receiver Settings 画面

画面に表示される項目：

項目	説明
Receiver Index	sFlow レシーバの識別子を指定します。 • 設定可能範囲：1-4
Owner Name	sFlow レシーバのオーナ名を指定します。（32 文字以内）
Expire Time	エントリの有効期限を指定します。期限になるとエントリのパラメータはリセットされます。 「Infinite」を設定するとエントリはタイムアウトしません。 • 設定可能範囲：1-2000000（秒）
Max Datagram Size	sFlow データグラム 1 つあたりの最大データバイト数を指定します。 • 設定可能範囲：700-1400（Bytes） • 初期値：1400（Bytes）
Collector Address	リモート sFlow コレクタの IPv4/IPv6 アドレスを指定します。
UDP Port	リモート sFlow コレクタの UDP ポート番号を指定します。 • 設定可能範囲：1-65535 • 初期値：6343

「Apply」ボタンをクリックして、設定内容を適用します。
「Reset」ボタンをクリックして、指定エントリの設定を初期値に戻します。

sFlow Sampler Settings（sFlow サンプラ設定）

sFlow サンプラの設定を行います。

Monitoring > sFlow > sFlow Sampler 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。

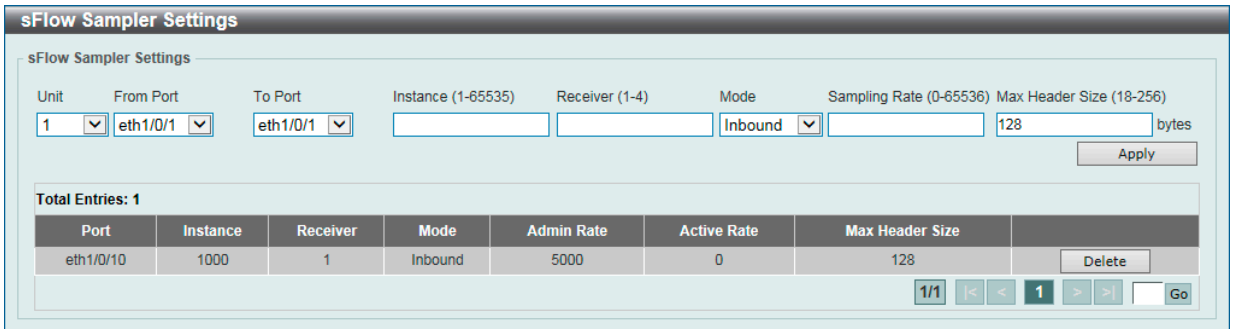


図 14-20　sFlow Sampler Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Instance	インタフェースに複数のサンプラを設定する場合、インスタンスのインデックス番号を指定します。 • 設定可能範囲：1-65535
Receiver	レシーバの識別番号を指定します。何も指定しない場合、値は「0」になります。 • 設定可能範囲：1-4
Mode	モードを指定します。 •「Inbound」- 受信パケットをサンプリングします。（初期値） •「Outbound」- 送信パケットをサンプリングします。
Sampling Rate	パケットサンプリングのレートを設定します。 • 設定可能範囲：0-65536 • 初期値：0（サンプリング無効）
MAX Header Size	サンプリングパケットからコピーすることができる最大バイト数を設定します。 • 設定可能範囲：18-256（Bytes） • 初期値：128（Bytes）

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

sFlow Poller Settings（sFlow ポーラー設定）

スイッチのポーラー設定を行います。

Configuration > sFlow > sFlow Poller 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。

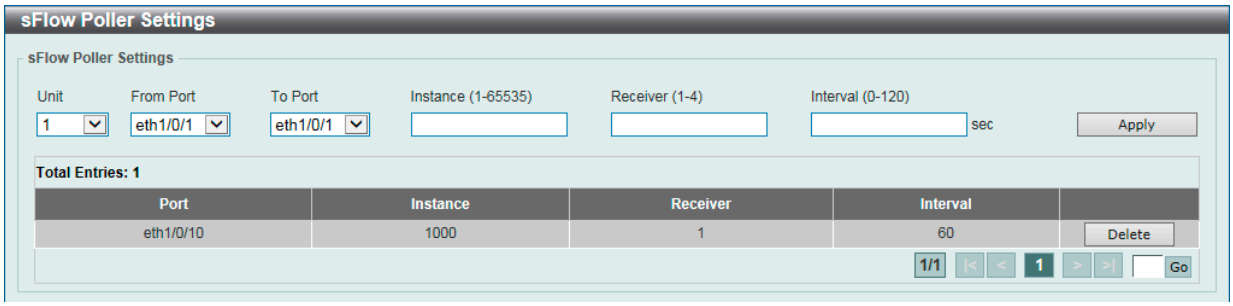


図 14-21　sFlow Poller Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Instance	インタフェースで複数のサンプラを設定する場合、インスタンスの識別番号を指定します。 • 設定可能範囲：1-65535

項目	説明
Receiver	レシーバの識別番号を指定します。 • 設定可能範囲：1-4
Interval	サンプリングのポーリング間隔を設定します。「0」を入力すると機能は無効になります。 • 設定可能範囲：0-120（秒） • 初期値：0

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

Device Environment（機器環境確認）

本画面ではスイッチの内部温度、ファン、電源の状態を表示します。

Monitoring > Device Environment をクリックして次の画面を表示します。

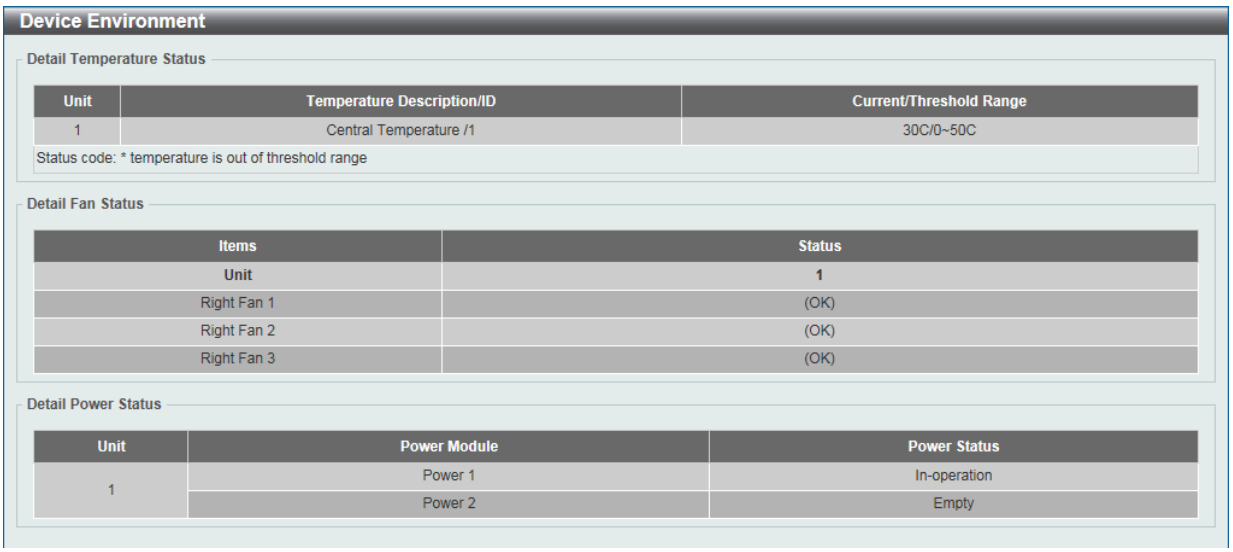


図 14-22　Device Environment 画面

第 15 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、表示します。
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、表示します。

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

Power Saving Global Settings タブ

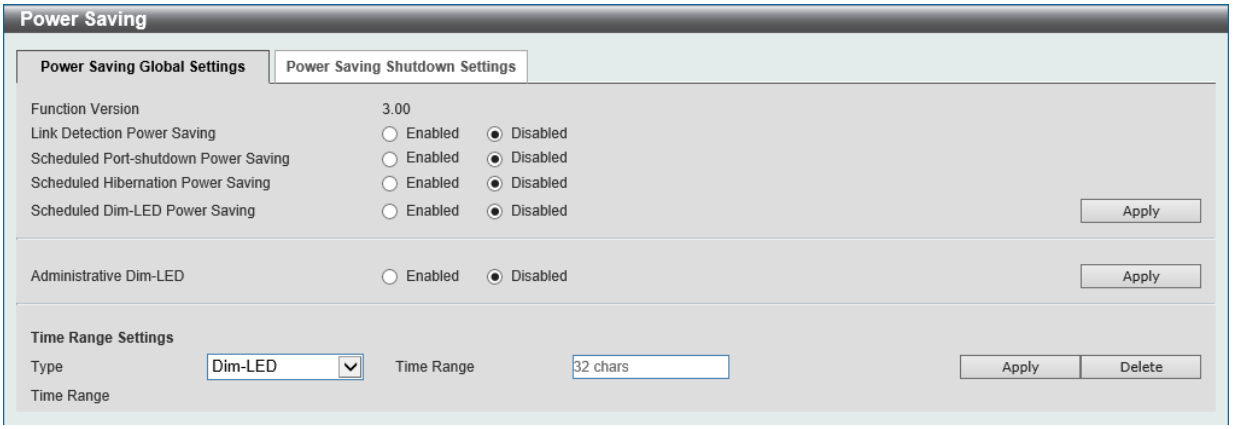


図 15-1　Power Saving 画面 - Power Saving Global Settings タブ

画面に表示される項目：

項目	説明
Link Detection Power Saving	リンク検知による省電力を有効 / 無効に指定します。 本設定を有効にすると、リンクダウンしているポートへの電力供給が停止し、スイッチの消費電力を抑えます。 リンクアップしているポートへの影響はありません。
Scheduled Port-shutdown Power Saving	スケジュールによるポートシャットダウン機能の有効 / 無効を指定します。
Scheduled Hibernation Power Saving	スケジュールによるシステム休止の有効 / 無効を指定します。 この機能は、物理スタッキングが有効になっている場合は使用できません。
Scheduled Dim-LED Power Saving	スケジュールによる減光 LED の有効 / 無効を指定します。
Administrative Dim-LED	ポート LED 機能の有効 / 無効を指定します。
Time Range Settings	
Type	省電力モードの種類を指定します。 • 選択肢：「Dim-LED」「Hibernation」
Time Range	上記省電力機能に適用するスケジュールを指定します。

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

Power Saving Shutdown Settings タブ

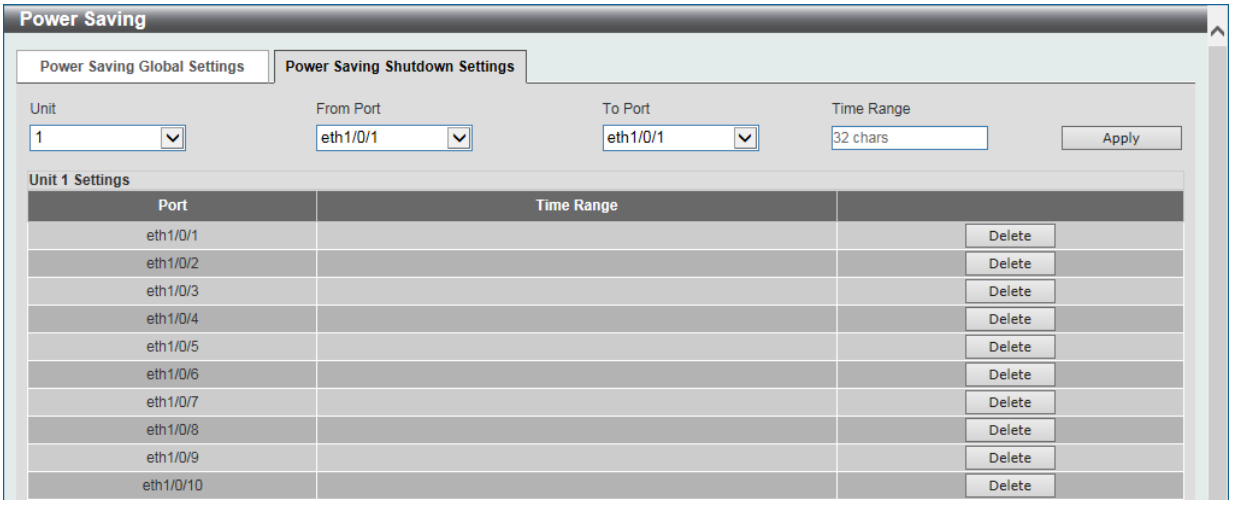


図 15-2　Power Saving 画面 - Power Saving Shutdown Settings タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Time Range	ポートに適用するスケジュール名を指定します。

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

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。
リンク上でパケットの送受信が発生していない場合、電力消費を抑えることができます。

Green > EEE メニューをクリックし、以下の画面を表示します。

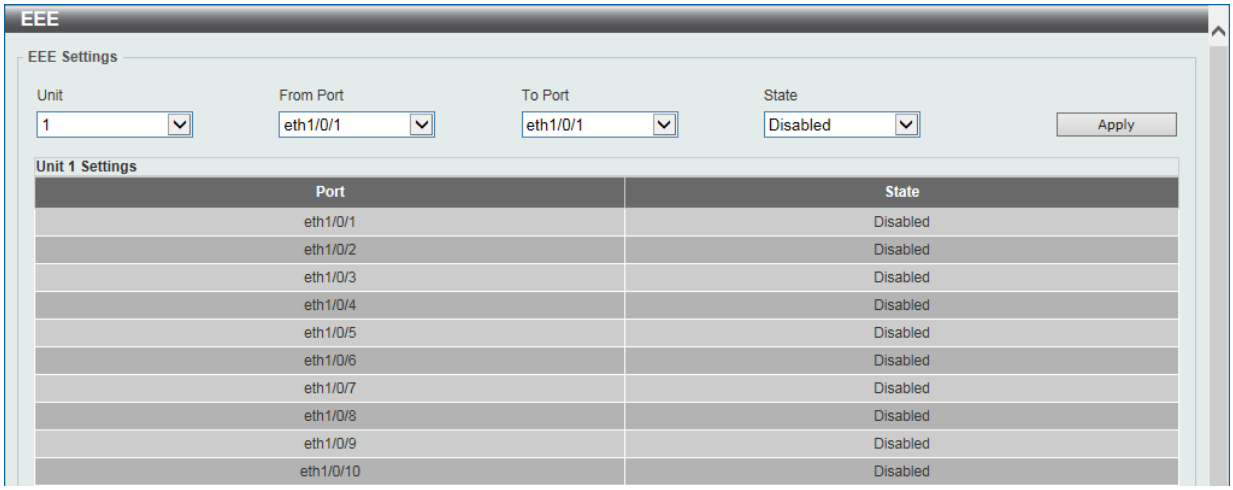


図 15-3　EEE 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	本機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

第 16 章　Save and Tools（Save メニュー /Tools メニュー）

メンテナンス用のメニューを使用し、本スイッチのリセットおよび再起動等を行うことができます。

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

サブメニュー	説明
Save（Save メニュー）	
Save Configuration（コンフィグレーションの保存）	コンフィグレーションをスイッチに保存します。
Tools メニュー	
Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）	様々なプロトコルを使用してファームウェアアップグレード / バックアップを実行します。
Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）	様々なプロトコルを使用してコンフィグレーションリストア / バックアップを実行します。
Certificate & Key Restore & Backup（証明書 / 鍵リストア＆バックアップ）	様々なプロトコルを使用して証明書と鍵のリストア / バックアップを実行します。
Log Backup（ログファイルのバックアップ）	様々なプロトコルを使用してログファイルのバックアップを実行します。
Ping	「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。
Trace Route（トレースルート）	パケットの経路をスイッチに到着する前に遡ってトレースすることができます。
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。

Save（Save メニュー）

現在のコンフィグレーションを保存します。

Save Configuration（コンフィグレーションの保存）

現在実行中のコンフィグレーションをブートコンフィグとしてスイッチに保存します。
電源が落ちた場合にコンフィグレーションが失われることを防ぎます。

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

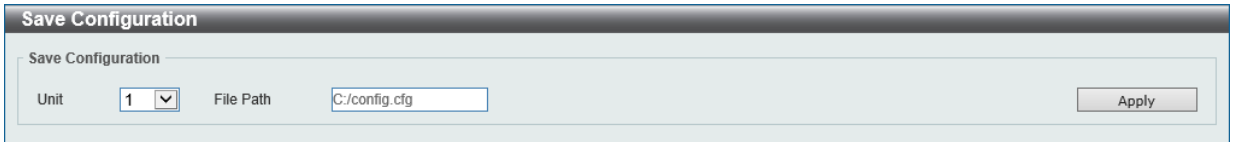


図 16-1　Save - Configuration 画面

以下の項目が表示されます。

項目	説明
Unit	保存先のユニットを選択します。
File Path	保存先のファイルパスおよびファイル名を指定します。

「Apply」ボタンをクリックして、コンフィグレーションを保存します。

Tools（Tools メニュー）

ファームウェアアップグレード＆バックアップ、コンフィグレーションリストア＆バックアップ、ログファイルのバックアップ、Ping、トレースルート、リセット、システム再起動などを行います。

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

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

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

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

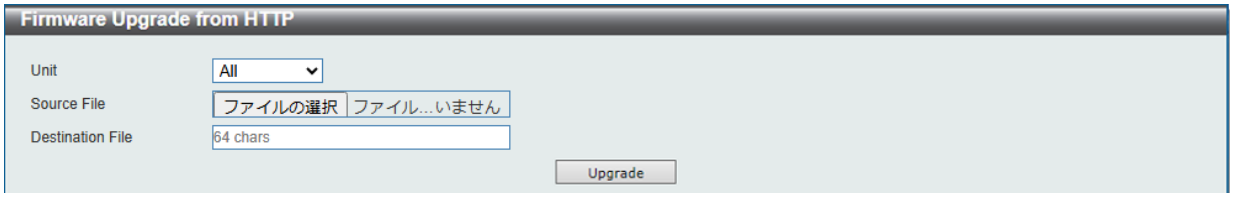


図 16-2　Firmware Upgrade from HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	「ファイルの選択 / 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選択します。
Destination File	ファームウェアが保存されるスイッチ上のファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Upgrade」ボタンをクリックして、アップグレードを開始します。

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

TFTP を使用してファームウェアアップグレードを実行します。

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

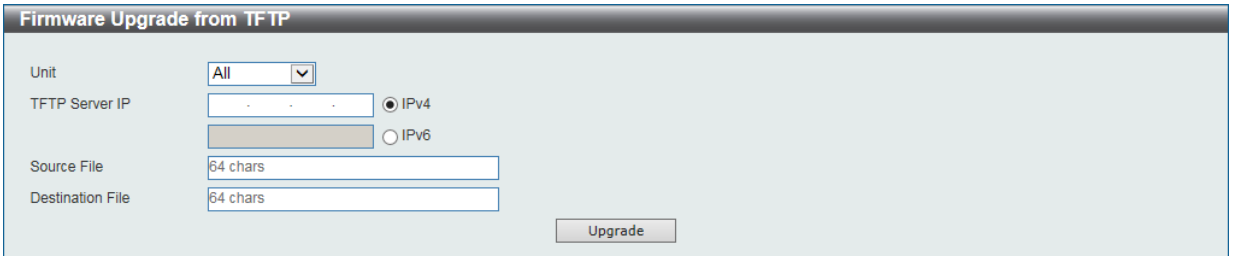


図 16-3　Firmware Upgrade from TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内） 例：DGS1530_A1_FW1_00.had
Destination File	ファームウェアが保存されるスイッチ上のファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Upgrade」ボタンをクリックして、アップグレードを開始します。

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

FTP を使用してファームウェアアップグレードを実行します。

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

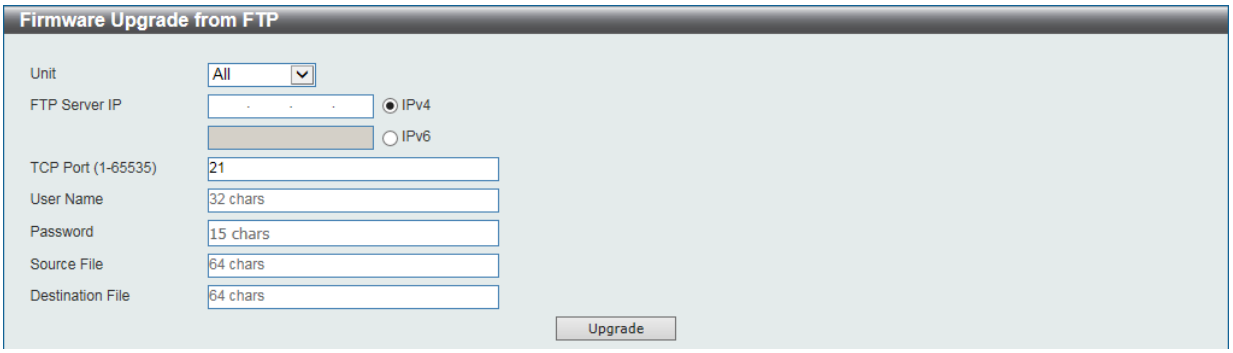


図 16-4　Firmware Upgrade from FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
Source File	FTP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内） 例：DGS1530_A1_FW1_00.had
Destination File	ファームウェアが保存されるスイッチ上のファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Upgrade」ボタンをクリックして、アップグレードを開始します。

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

RCP を使用してファームウェアアップグレードを実行します。

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

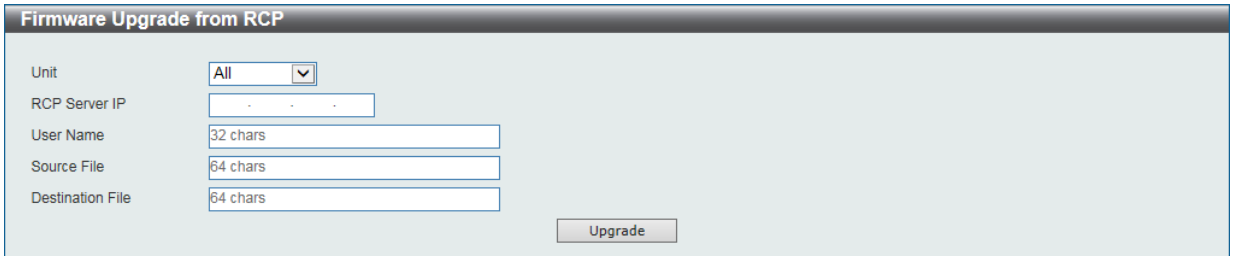


図 16-5　Firmware Upgrade from RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（32 文字以内）を指定します。
Source File	RCP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内） 例：DGS1530_A1_FW1_00.had
Destination File	ファームウェアが保存されるスイッチ上のファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Upgrade」ボタンをクリックして、アップグレードを開始します。

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

SFTP を使用してファームウェアアップグレードを実行します。

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

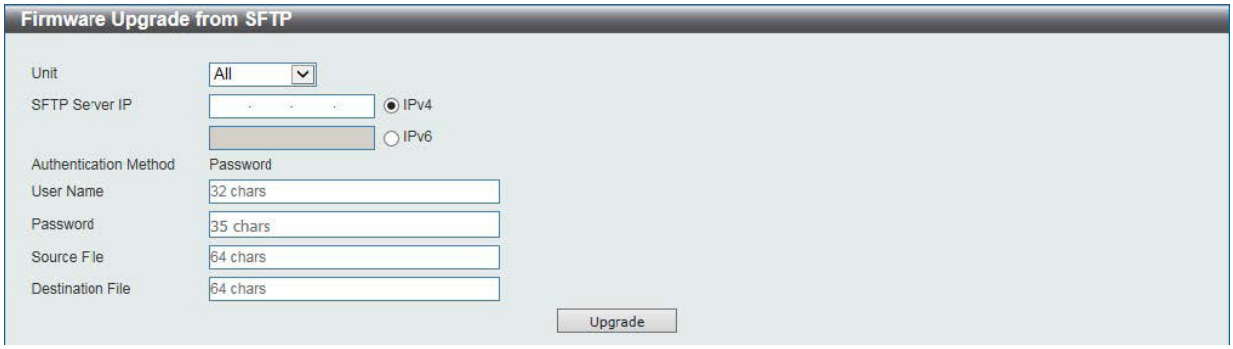


図 16-6　Firmware Upgrade from SFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	SFTP 接続に使用するパスワード（35 文字以内）を指定します。
Source File	SFTP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内） 例：DGS1530_A1_FW1_00.had
Destination File	ファームウェアが保存されるスイッチ上のファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Upgrade」ボタンをクリックして、アップグレードを開始します。

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

HTTP を使用して、ローカル PC へ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。

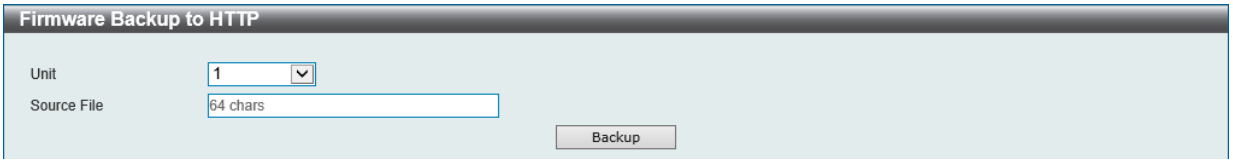


図 16-7　Firmware Backup to HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	スイッチ上でファームウェアが保存されている送信元ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。

「Backup」ボタンをクリックして、バックアップを開始します。

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

TFTP サーバに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。

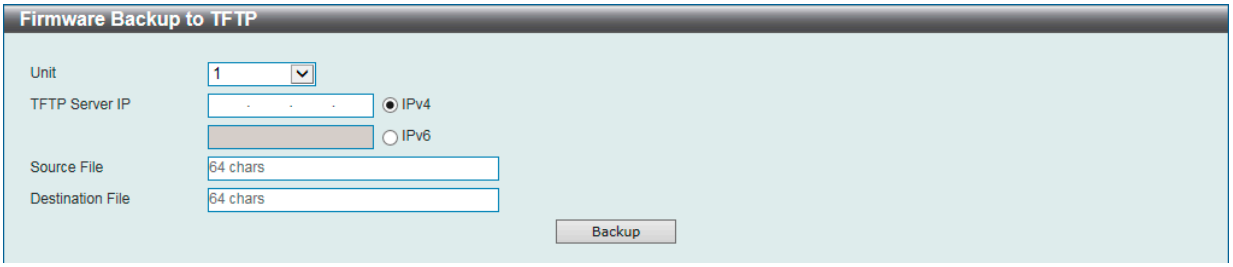


図 16-8　Firmware Backup to TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	スイッチ上でファームウェアが保存されている送信元ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。
Destination File	TFTP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had

「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 FTP（FTP を使用したファームウェアバックアップ）

FTP サーバにファームウェアバックアップを行います。

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

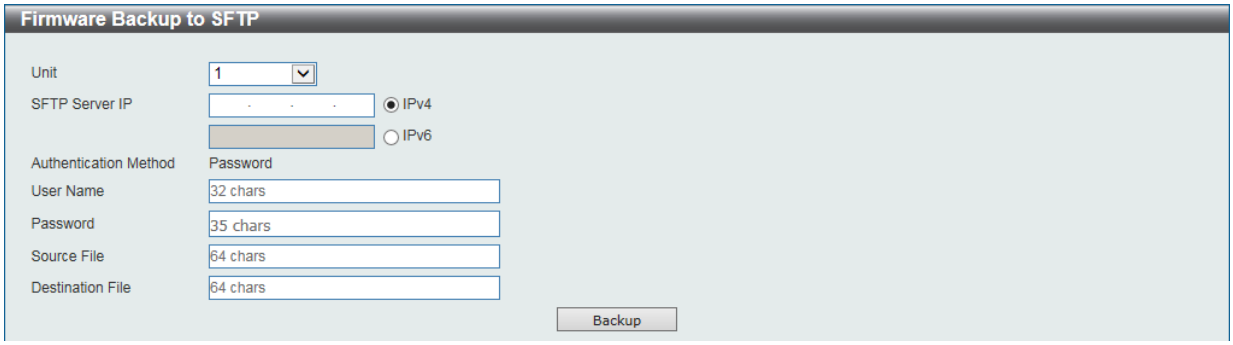


図 16-9　Firmware Backup to FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
Source File	スイッチ上でファームウェアが保存されている送信元ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。
Destination File	FTP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had

「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 RCP（RCP を使用したファームウェアバックアップ）

RCP サーバへファームウェアバックアップを行います。

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

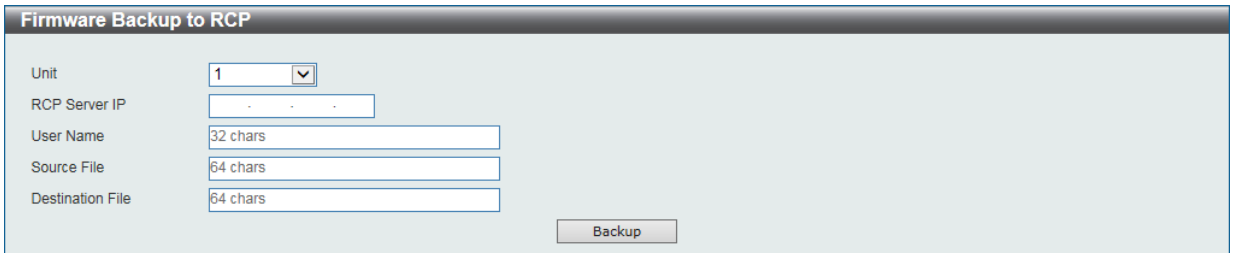


図 16-10　Firmware Backup to RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（32 文字以内）を指定します。
Source File	スイッチ上でファームウェアが保存されている送信元ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。
Destination File	RCP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had

「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 SFTP（SFTP を使用したファームウェアバックアップ）

SFTP サーバにファームウェアバックアップを行います。

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

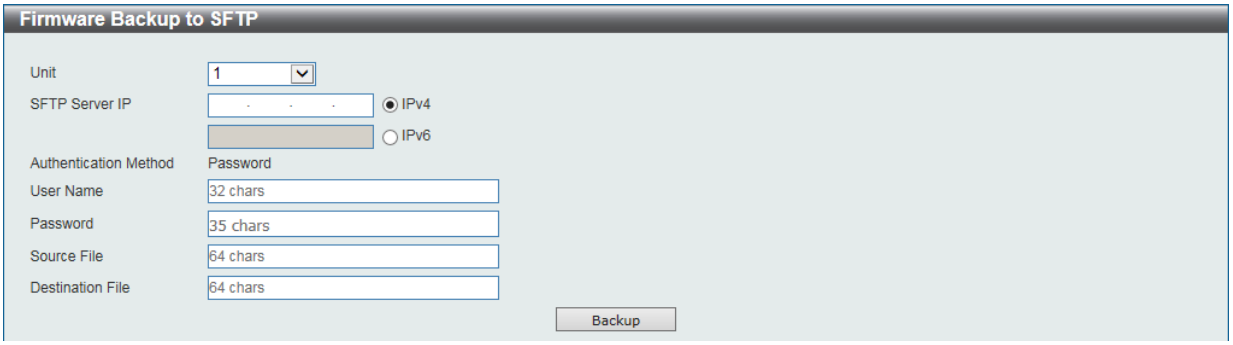


図 16-11　Firmware Backup to SFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	SFTP 接続に使用するパスワード（35 文字以内）を指定します。
Source File	スイッチ上でファームウェアが保存されている送信元ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。
Destination File	SFTP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：DGS1530_A1_FW1_00.had

「Backup」ボタンをクリックして、バックアップを開始します。

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

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

HTTP を使用してローカル PC から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 16-12　Configuration Restore from HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	「ファイルを選択 / 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選択します。
Destination File	新しいコンフィグレーションファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストアされます。「Replace」オプションの指定により処理が異なります。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルが上書きされます。

項目	説明
Replace	「running-config」を選択した場合、本オプションが利用可能です。 「Replace」にチェックを入れると、ランニングコンフィグレーションが削除され、新しいコンフィグレーションに置き換えられます。チェックを入れない場合、現在のランニングファイルは消去されずに指定ファイルの設定がマージされます。

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

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

TFTP サーバから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。

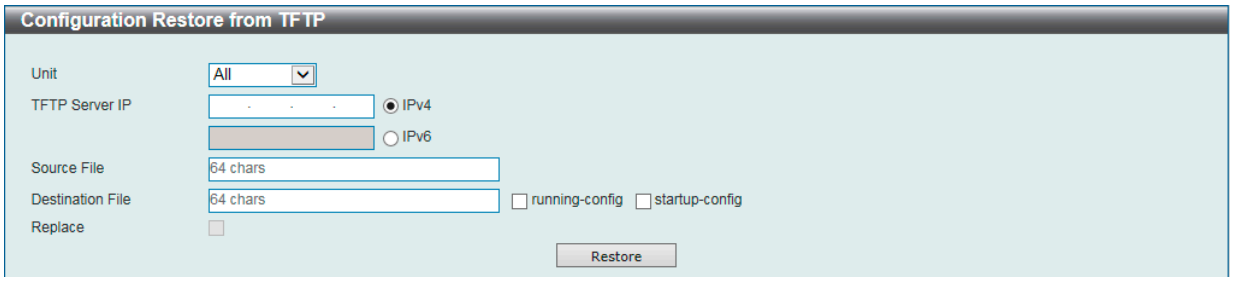


図 16-13　Configuration Restore from TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。（64 文字以内） 例：config.cfg
Destination File	新しいコンフィグレーションファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストアされます。「Replace」オプションの指定により処理が異なります。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルが上書きされます。
Replace	「running-config」を選択した場合、本オプションが利用可能です。 「Replace」にチェックを入れると、ランニングコンフィグレーションが削除され、新しいコンフィグレーションに置き換えられます。チェックを入れない場合、現在のランニングファイルは消去されずに指定ファイルの設定がマージされます。

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

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

FTP サーバから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 FTP をクリックし、設定画面を表示します。

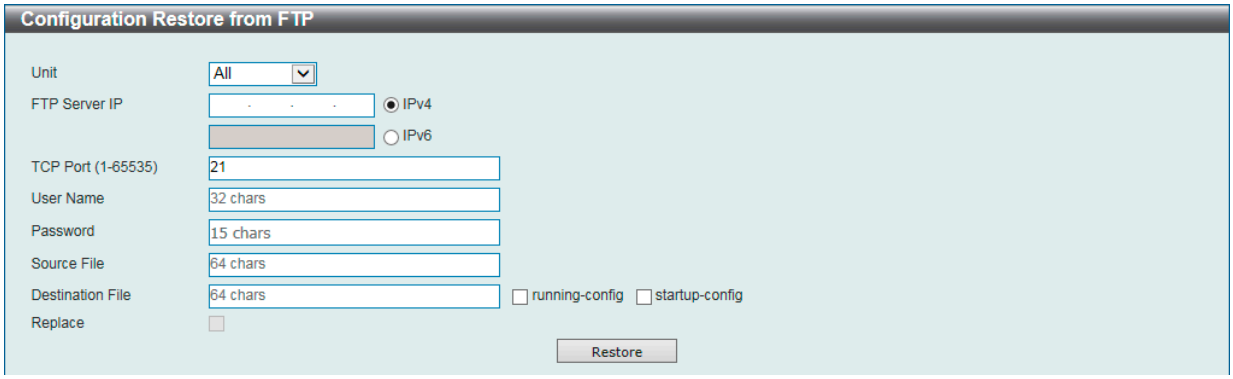


図 16-14　Configuration Restore from FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
Source File	FTP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。（64 文字以内） 例：config.cfg
Destination File	新しいコンフィグレーションファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストアされます。「Replace」オプションの指定により処理が異なります。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルが上書きされます。
Replace	「running-config」を選択した場合、本オプションが利用可能です。 「Replace」にチェックを入れると、ランニングコンフィグレーションが削除され、新しいコンフィグレーションに置き換えられます。チェックを入れない場合、現在のランニングファイルは消去されずに指定ファイルの設定がマージされます。

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

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

RCP サーバから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 RCP をクリックし、設定画面を表示します。

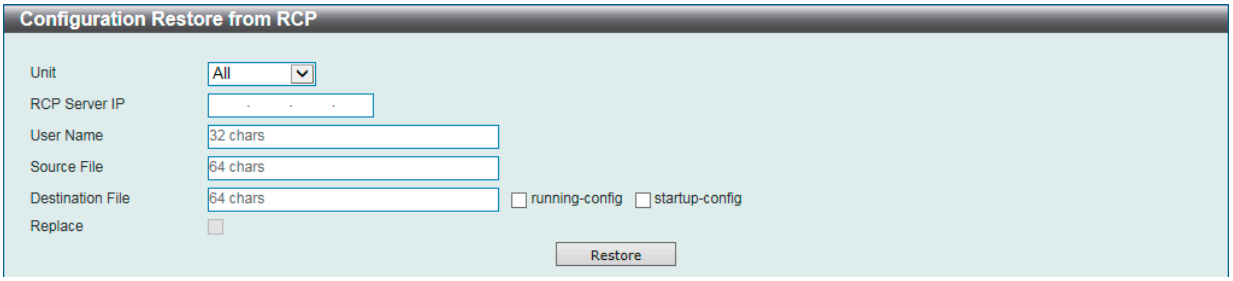


図 16-15　Configuration Restore from RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。 • 「IPv4」- RCP サーバの IPv4 アドレスを入力します。 • 「IPv6」- RCP サーバの IPv6 アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（32 文字以内）を指定します。
Source File	RCP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。（64 文字以内） 例：config.cfg
Destination File	新しいコンフィグレーションファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストアされます。「Replace」オプションの指定により処理が異なります。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルが上書きされます。
Replace	「running-config」を選択した場合、本オプションが利用可能です。 「Replace」にチェックを入れると、ランニングコンフィグレーションが削除され、新しいコンフィグレーションに置き換えられます。チェックを入れない場合、現在のランニングファイルは消去されずに指定ファイルの設定がマージされます。

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

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

SFTP サーバから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 SFTP をクリックし、設定画面を表示します。

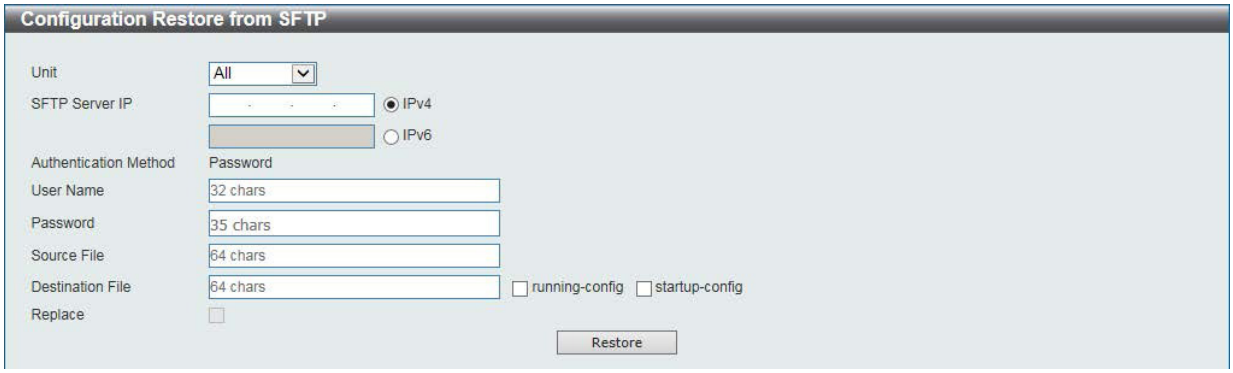


図 16-16　Configuration Restore from SFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	SFTP 接続に使用するパスワード（35 文字以内）を指定します。
Source File	SFTP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。（64 文字以内） 例：config.cfg
Destination File	新しいコンフィグレーションファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストアされます。「Replace」オプションの指定により処理が異なります。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルが上書きされます。
Replace	「running-config」を選択した場合、本オプションが利用可能です。 「Replace」にチェックを入れると、ランニングコンフィグレーションが削除され、新しいコンフィグレーションに置き換えられます。チェックを入れない場合、現在のランニングファイルは消去されずに指定ファイルの設定がマージされます。

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

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

HTTP を使用してローカル 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。

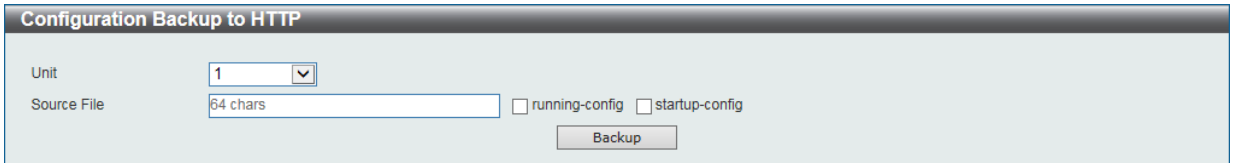


図 16-17　Configuration Backup to HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	スイッチ上でコンフィグレーションファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルのバックアップを行います。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルのバックアップを行います。

「Backup」ボタンをクリックして、バックアップを開始します。

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

TFTP サーバにコンフィグレーション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。

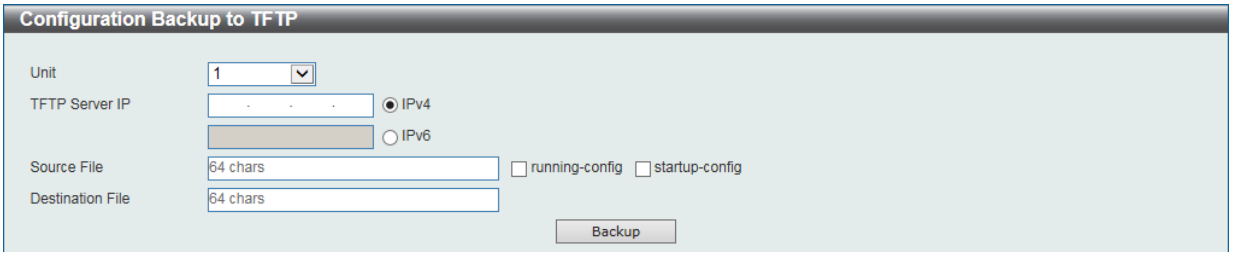


図 16-18　Configuration Backup to TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	スイッチ上でコンフィグレーションファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルのバックアップを行います。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルのバックアップを行います。
Destination File	TFTP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：config.cfg

「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 FTP（FTP を使用したコンフィグレーションバックアップ）

FTP サーバ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 FTP をクリックし、設定画面を表示します。

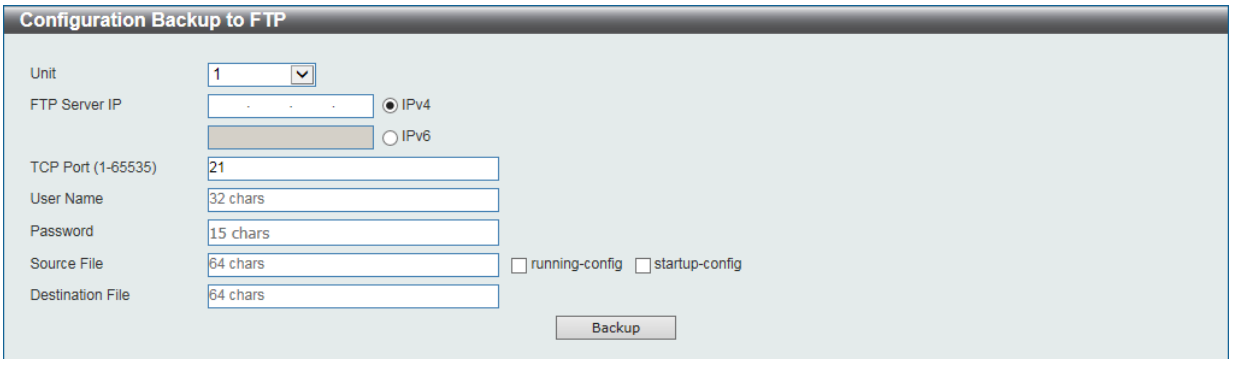


図 16-19　Configuration Backup to FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。

項目	説明
Source File	スイッチ上でコンフィグレーションファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルのバックアップを行います。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルのバックアップを行います。
Destination File	FTP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：config.cfg

「Backup」ボタンをクリックして、バックアップを開始します。

注意　copy running-config ftp: コマンドでエラーが発生する場合、no network-protocol-port protect tcp コマンドを実行してください。

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

RCP サーバ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 RCP をクリックし、設定画面を表示します。

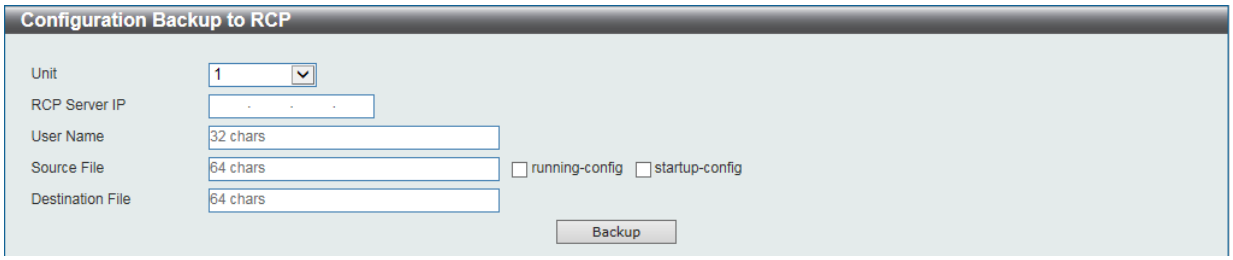


図 16-20　Configuration Backup to RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（32 文字以内）を指定します。
Source File	スイッチ上でコンフィグレーションファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルのバックアップを行います。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルのバックアップを行います。
Destination File	RCP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：config.cfg

「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 SFTP（SFTP を使用したコンフィグレーションバックアップ）

SFTP サーバ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 SFTP をクリックし、設定画面を表示します。

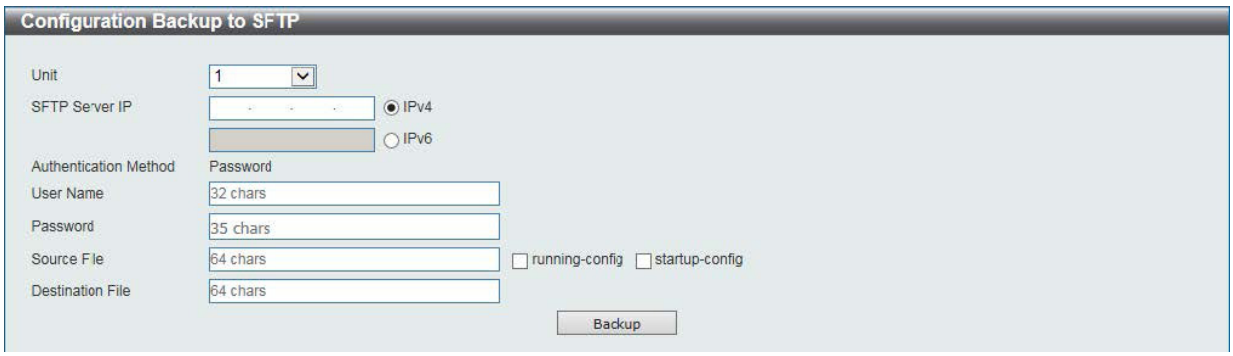


図 16-21　Configuration Backup to SFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	SFTP 接続に使用するパスワード（35 文字以内）を指定します。
Source File	スイッチ上でコンフィグレーションファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） 例：config.cfg スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルのバックアップを行います。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルのバックアップを行います。
Destination File	SFTP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：config.cfg

「Backup」ボタンをクリックして、バックアップを開始します。

Certificate & Key Restore & Backup（証明書 / 鍵リストア＆バックアップ）

Certificate & Key Restore from HTTP（HTTP を使用した証明書 / 鍵リストア）

HTTP を使用してローカル PC から証明書 / 鍵のリストアを実行します。

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

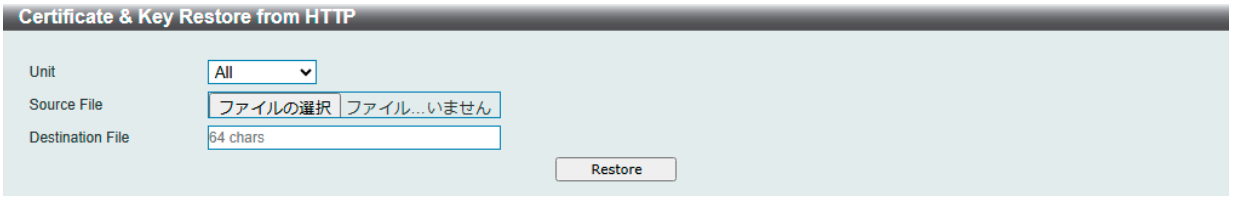


図 16-22　Certificate & Key Restore from HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	「ファイルの選択 / 参照」ボタンをクリックして、ローカル PC 上の証明書 / 鍵ファイルを選択します。
Destination File	新しいファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Restore」ボタンをクリックして、リストアを開始します。

Certificate & Key Restore from TFTP（TFTP を使用した証明書 / 鍵リストア）

TFTP サーバからの証明書 / 鍵リストアを実行します。

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

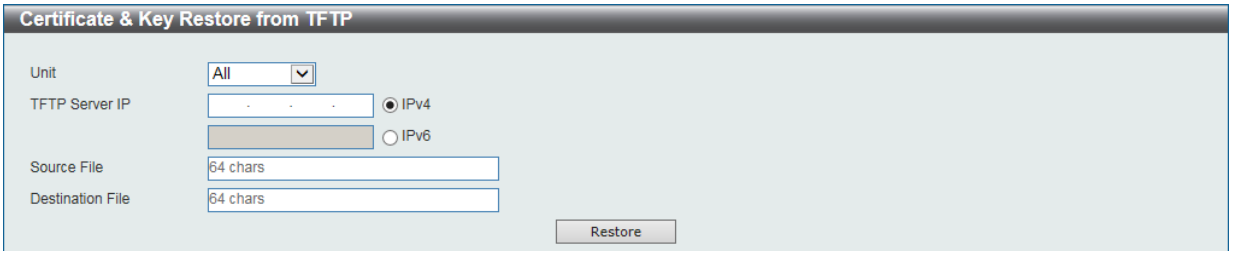


図 16-23　Certificate & Key Restore from TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバ上に保存されている証明書 / 鍵のファイルパスを入力します。（64 文字以内）
Destination File	新しいファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Restore」ボタンをクリックして、リストアを開始します。

Certificate & Key Restore from FTP（FTP を使用した証明書 / 鍵リストア）

FTP サーバからの証明書 / 鍵リストアを実行します。

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

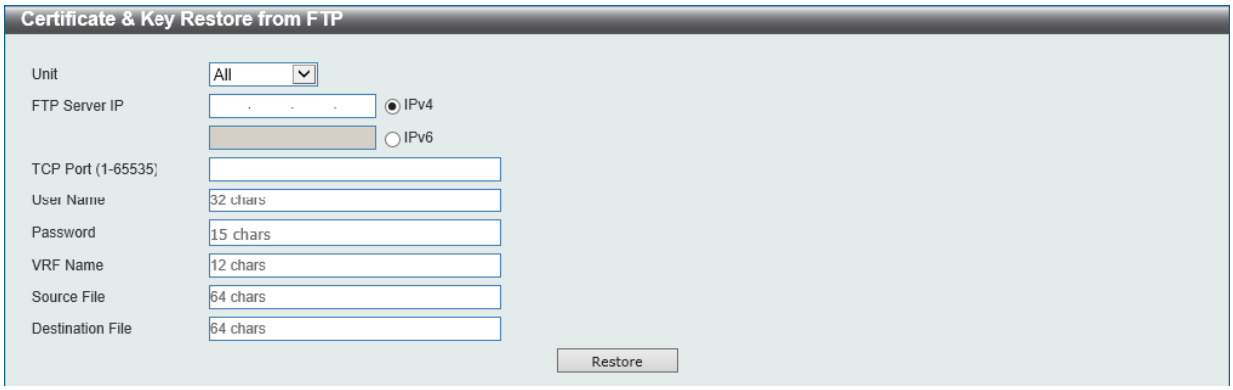


図 16-24　Certificate & Key Restore from FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
Source File	FTP サーバ上に保存されている証明書 / 鍵のファイルパスを入力します。（64 文字以内）
Destination File	新しいファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Restore」ボタンをクリックして、リストアを開始します。

Certificate & Key Restore from RCP（RCP を使用した証明書 / 鍵リストア）

RCP サーバからの証明書 / 鍵リストアを実行します。

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

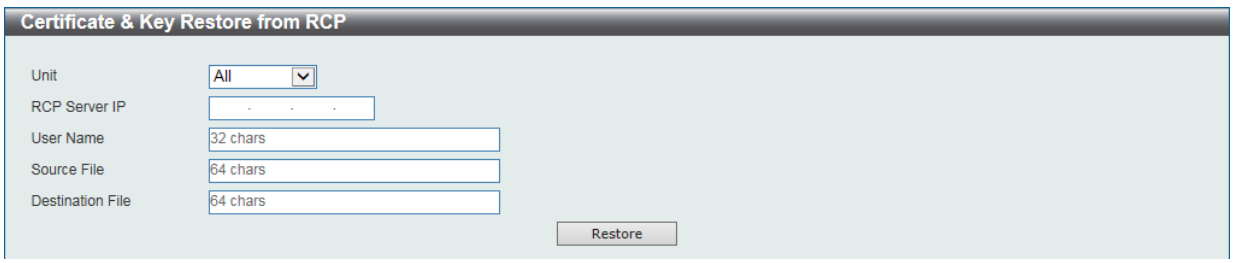


図 16-25　Certificate & Key Restore from RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（32 文字以内）を指定します。
Source File	RCP サーバ上に保存されている証明書 / 鍵のファイルパスを入力します。（64 文字以内）
Destination File	新しいファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Restore」ボタンをクリックして、リストアを開始します。

Certificate & Key Restore from SFTP（SFTP を使用した証明書 / 鍵リストア）

SFTP サーバからの証明書 / 鍵リストアを実行します。

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

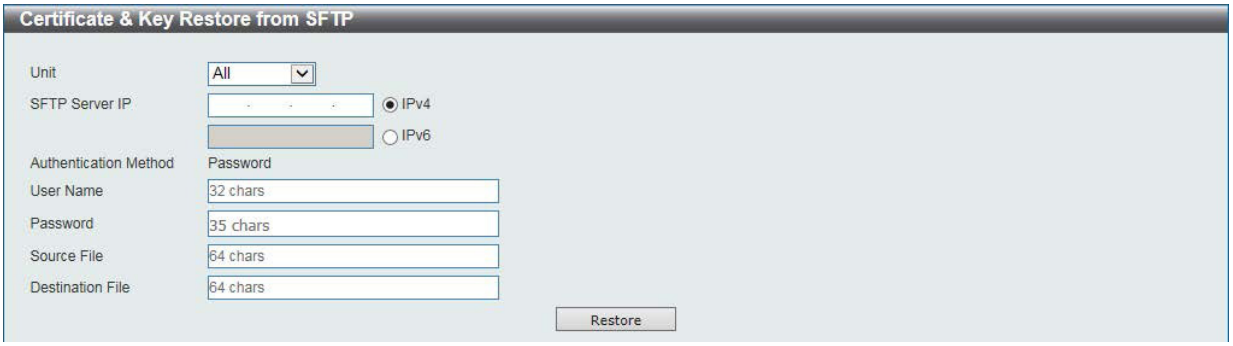


図 16-26　Certificate & Key Restore from SFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	SFTP 接続に使用するパスワード（35 文字以内）を指定します。
Source File	SFTP サーバ上に保存されている証明書 / 鍵のファイルパスを入力します。（64 文字以内）
Destination File	新しいファイルを保存するスイッチ上の送信先ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「Restore」ボタンをクリックして、リストアを開始します。

Public Key Backup to HTTP（HTTP を使用した公開鍵バックアップ）

HTTP を使用してローカル PC へ証明書 / 鍵をバックアップします。

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

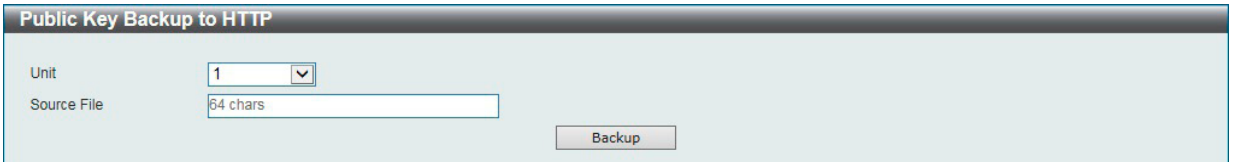


図 16-27　Public Key Backup to HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	スイッチに保存されている証明書 / 鍵ファイルのファイルパスを入力します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Public Key Backup to TFTP（TFTP を使用した公開鍵バックアップ）

TFTP サーバへの証明書 / 鍵バックアップを行います。

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

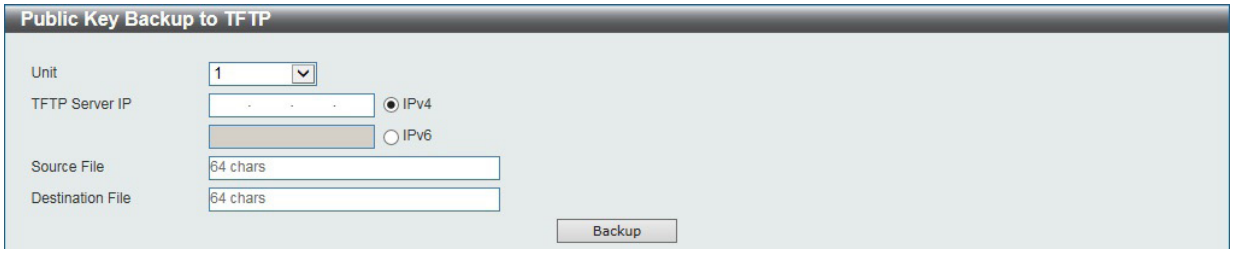


図 16-28　Public Key Backup to TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	スイッチ上で証明書および公開鍵ファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。
Destination File	TFTP サーバ上の保存先ファイルパスを指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Public Backup to FTP（FTP を使用した公開鍵バックアップ）

FTP サーバへの証明書 / 鍵バックアップを行います。

Tools > Certificate & Key Restore & Backup > Public Key Backup to FTP をクリックし、設定画面を表示します。

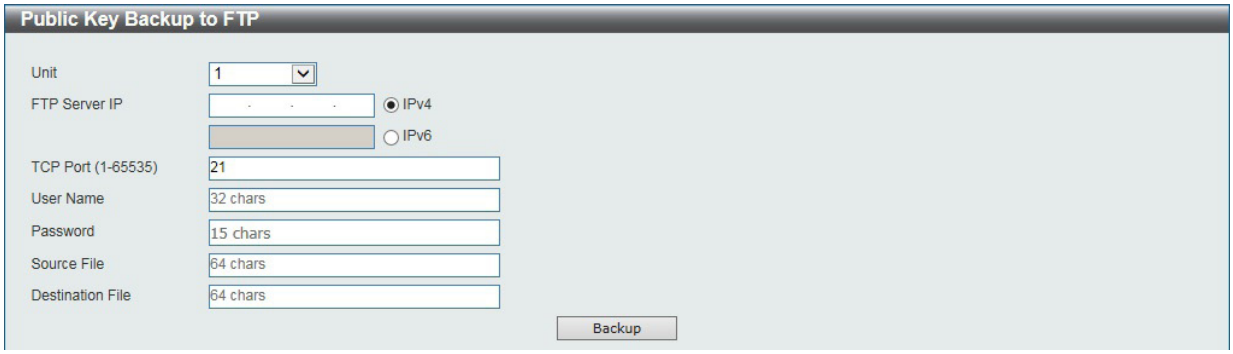


図 16-29　Public Key Backup to FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
Source File	スイッチ上で証明書および公開鍵ファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。
Destination File	FTP サーバ上の保存先ファイルパスを指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Public Key Backup to RCP（RCP を使用した公開鍵バックアップ）

RCP サーバへの証明書 / 鍵バックアップを行います。

Tools > Certificate & Key Restore & Backup > Public Key Backup to RCP をクリックし、設定画面を表示します。

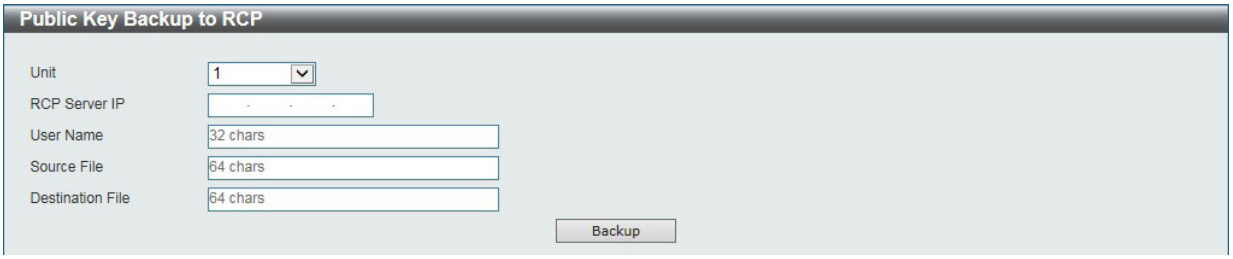


図 16-30　Public Key Backup to RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（32 文字以内）を指定します。
Source File	スイッチ上で証明書および公開鍵ファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。
Destination File	RCP サーバ上の保存先ファイルパスを指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Public Backup to SFTP（SFTP を使用した公開鍵バックアップ）

SFTP サーバへの証明書 / 鍵バックアップを行います。

Tools > Certificate & Key Restore & Backup > Public Key Backup to SFTP をクリックし、設定画面を表示します。

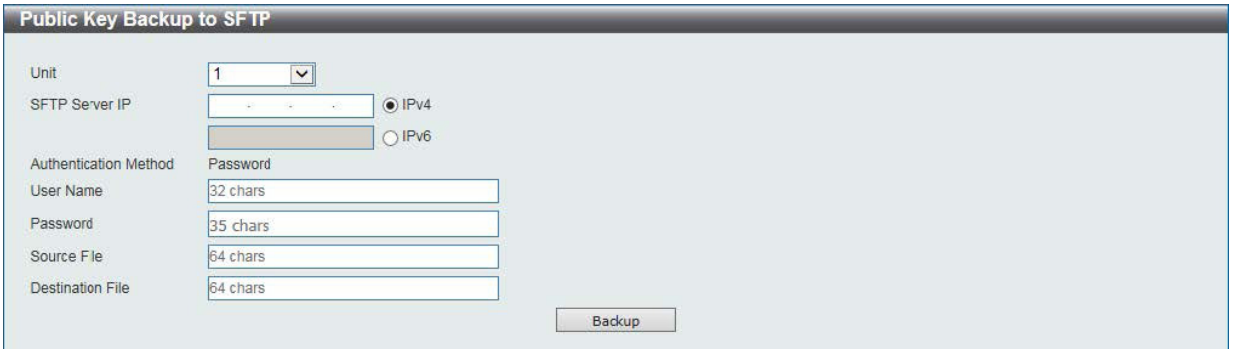


図 16-31　Public Key Backup to SFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	SFTP 接続に使用するパスワード（35 文字以内）を指定します。
Source File	スイッチ上で証明書および公開鍵ファイルが保存されている送信元ファイルパスを入力します。（64 文字以内） スイッチのルートディレクトリに保存されている場合はフォルダパス（c:/）を省略できます。
Destination File	SFTP サーバ上の保存先ファイルパスを指定します。（64 文字以内）

「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。

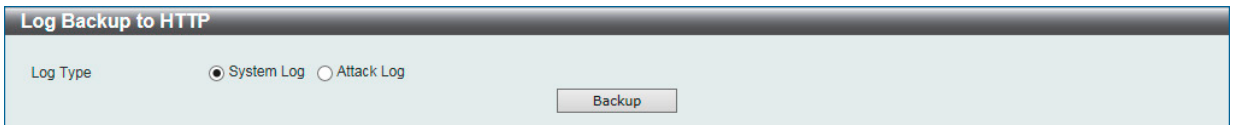


図 16-32　Log Backup to HTTP 画面

画面に表示される項目：

項目	説明
Log Type	HTTP を使用してローカル PC にバックアップするログの種類を選択します。 • 「System Log」- システムログをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「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 to TFTP（TFTP サーバを使用したログファイルのバックアップ）

TFTP サーバへのシステムログのバックアップを行います。

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

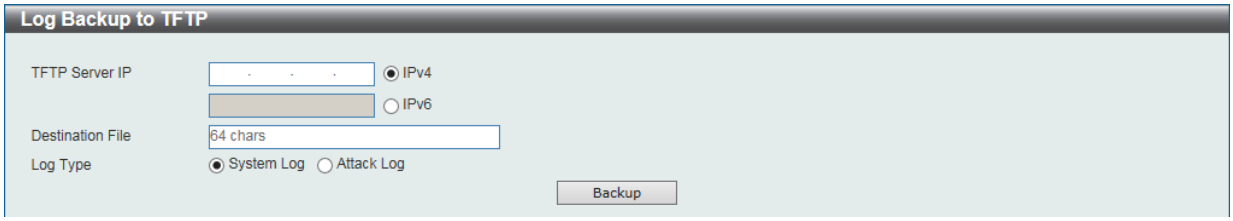


図 16-33　Log Backup to TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Destination File	TFTP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：Syslog.log
Log Type	バックアップするログの種類を選択します。 • 「System Log」- システムログエントリをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「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 to RCP（RCP サーバを使用したログファイルのバックアップ）

RCP 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 RCP をクリックし、設定画面を表示します。

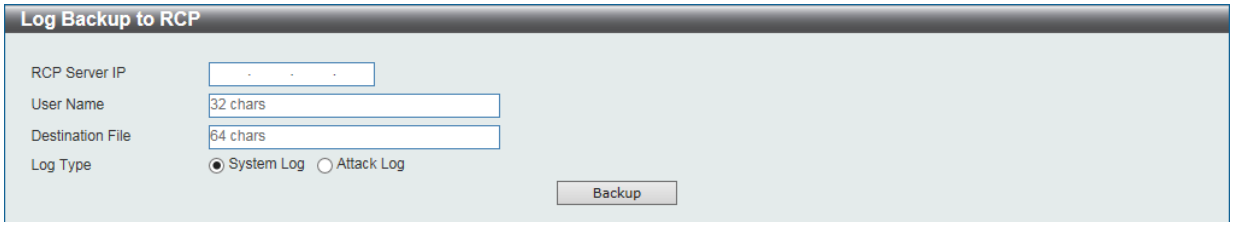


図 16-34　Log Backup to RCP 画面

画面に表示される項目：

項目	説明
RCP Server IP	RCP サーバの IP アドレスを入力します。

項目	説明
User Name	RCP 接続に使用するユーザ名（32 文字以内）を指定します。
Destination File	RCP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：Syslog.log
Log Type	バックアップするログの種類を選択します。 • 「System Log」- システムログエントリをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「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 to SFTP（SFTP サーバを使用したログファイルのバックアップ）

SFTP 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 SFTP をクリックし、設定画面を表示します。

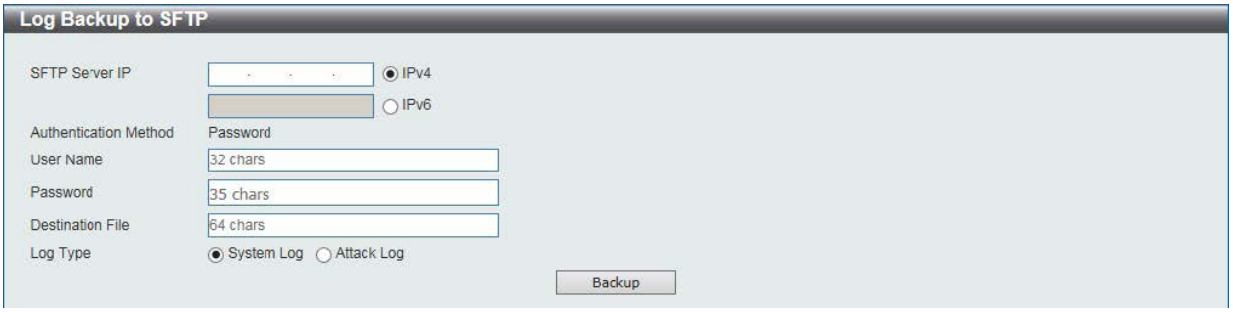


図 16-35　Log Backup to SFTP 画面

画面に表示される項目：

項目	説明
SFTP Server IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	SFTP 接続に使用するパスワード（35 文字以内）を指定します。
Destination File	SFTP サーバ上の保存先ファイルパスを指定します。（64 文字以内） 例：Syslog.log
Log Type	バックアップするログの種類を選択します。 • 「System Log」- システムログエントリをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「Backup」ボタンをクリックして、バックアップを開始します。

Ping

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

Tools > Ping をクリックし、設定画面を表示します。

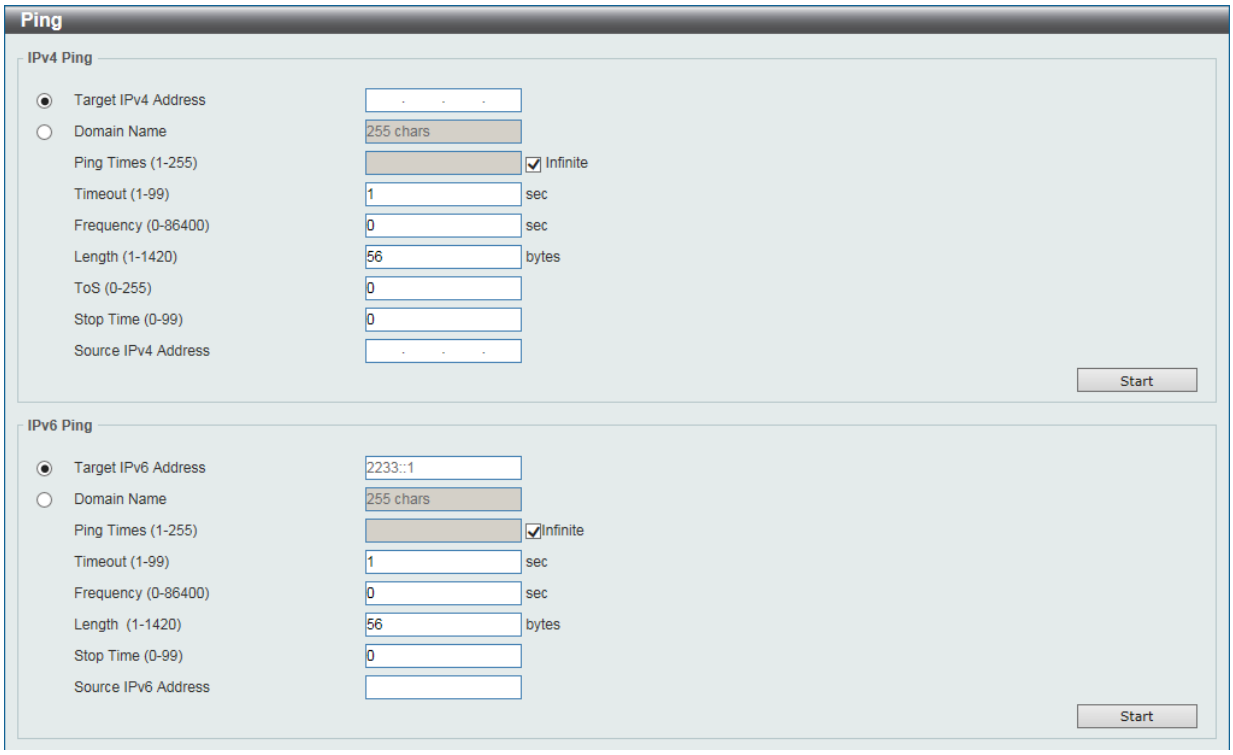


図 16-36　Ping 画面

画面に表示される項目：

項目	説明
IPv4 Ping	
Target IPv4 Address	Ping の送信先となる IPv4 アドレスを入力します。
Domain Name	検出するシステムのドメイン名を入力します。
Ping Times	Ping の試行回数を入力します。 「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。 • 設定可能範囲：1-255
Timeout	Ping メッセージが宛先に到達するまでのタイムアウトの時間を指定します。 指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。 • 設定可能範囲：1-99（秒）
Frequency	Ping 頻度を指定します。 • 設定可能範囲：0-86400（秒）
Length	送信データバイト数を指定します。VLAN（IEEE 802.1Q）タグ長は含まれません。 • 設定可能範囲：1-1420（Bytes）
ToS	送信データグラムの IP ヘッダに含まれる ToS 値を指定します。 • 設定可能範囲：0-255
Stop Time	停止回数を指定します。指定の Ping 回数を過ぎると Ping が停止します。「0」に指定した場合、「Stop」をクリックするまで Ping が実行されます。自動的には停止しません。 • 設定可能範囲：0-99
Source IPv4 Address	送信元 IPv4 アドレスを入力します。 スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。入力した IPv4 アドレスは、リモートホストに送信されるパケットの送信元 IP アドレスまたはプライマリ IP アドレスとして使用されます。
IPv6 Ping	
Target IPv6 Address	Ping する IPv6 アドレスを入力します。
Domain Name	検出するシステムのドメイン名を入力します。
Ping Times	Ping の試行回数を入力します。 「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。 • 設定可能範囲：1-255

項目	説明
Timeout	Ping メッセージが宛先に到達するまでのタイムアウトの時間を指定します。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。 • 設定可能範囲：1-99（秒）
Frequency	Ping 頻度を指定します。 • 設定可能範囲：0-86400
Length	送信データバイト数を指定します。VLAN（IEEE 802.1Q）タグ長は含まれません。 • 設定可能範囲：1-1420（Bytes）
Stop Time	停止回数を指定します。指定の Ping 回数を過ぎると Ping が停止します。「0」に指定した場合、「Stop」をクリックするまで Ping が実行されます。自動的には停止しません。 • 設定可能範囲：0-99
Source IPv6 Address	送信元 IPv6 アドレスを入力します。 スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。入力した IPv6 アドレスは、リモートホストに送信されるパケットの送信元 IP アドレスまたはプライマリ IP アドレスとして使用されます。

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

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

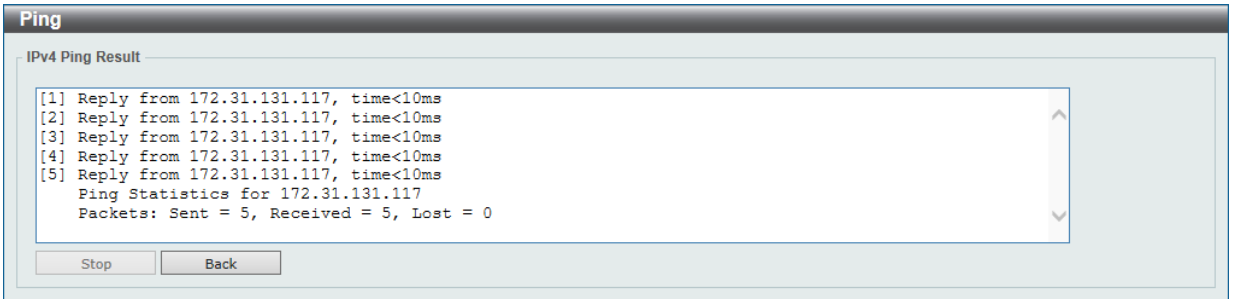


図 16-37　IPv4 Ping Result 画面

「IPv6 Ping」セクションで「Start」ボタンをクリックすると、以下の「IPv6 Ping Result」画面が表示されます。

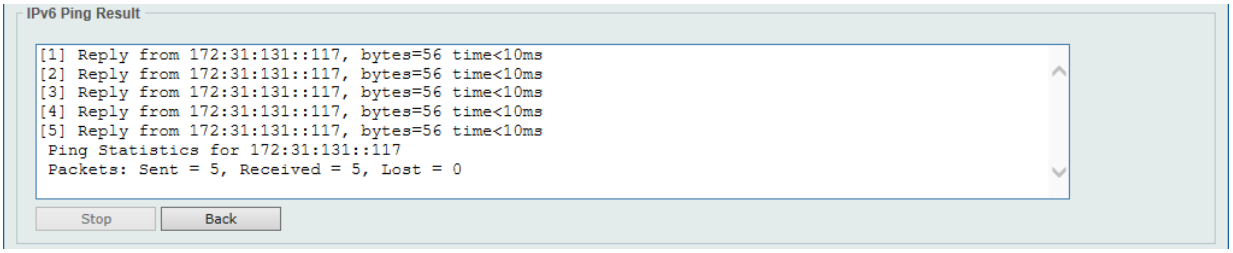


図 16-38　IPv6 Ping Result 画面

「Stop」ボタンをクリックして、Ping テストを停止します。
「Back」ボタンをクリックして、前の画面に戻ります。

Trace Route（トレースルート）

ネットワークとホスト間のルートをトレースします。

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

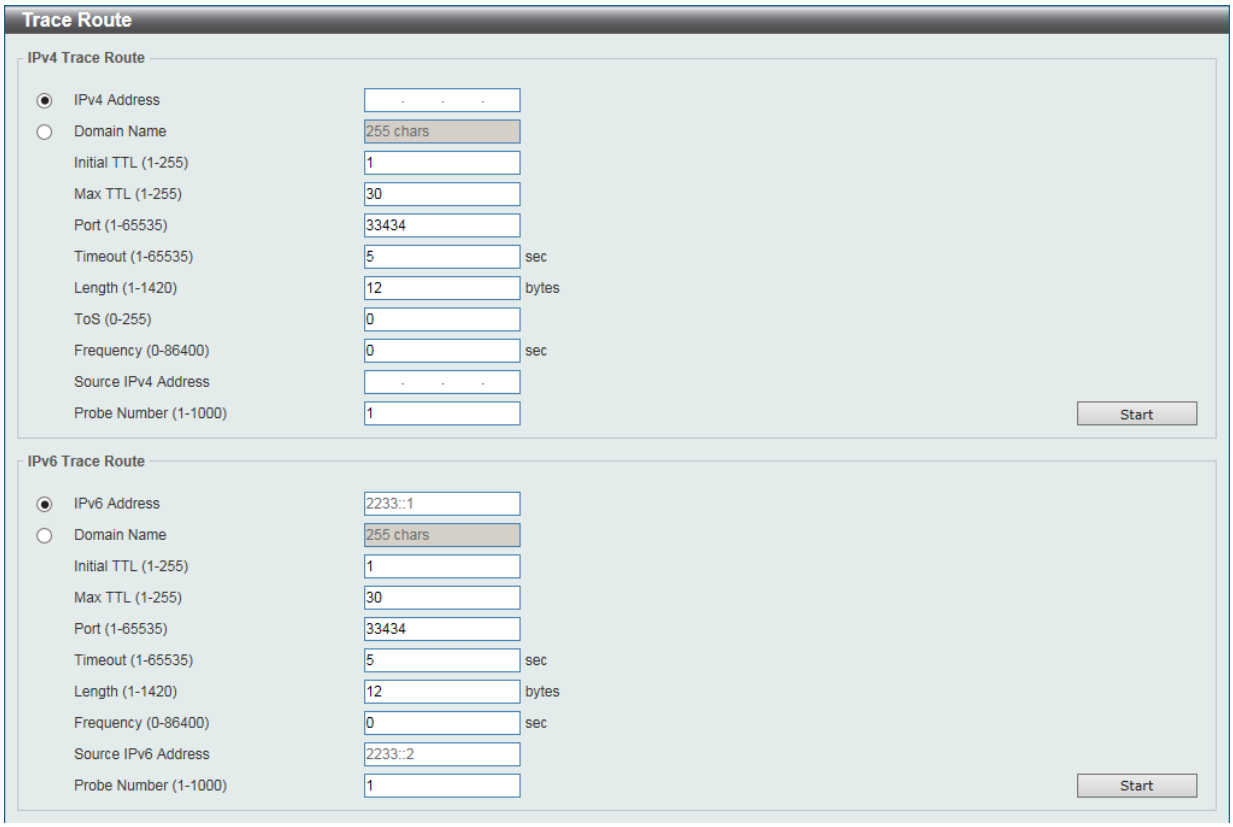


図 16-39　Trace Route 画面

画面に表示される項目：

項目	説明
IPv4 Trace Route	
IPv4 Address	宛先 IPv4 アドレスを入力します。
Domain Name	宛先のドメイン名を入力します。
Initial TTL	初期 TTL（Time-To-Live）値を入力します。UDP データグラムは指定した TTL 値で送信されます。 • 設定可能範囲：1-255
Max TTL	トレースルートリクエストの Time-To-Live (TTL) 値を入力します。トレースルートパケットが通過できるルータの最大数となります。2 台のデバイス間でネットワークパスを検出する際に、このトレースルートオプションを使用します。 • 設定可能範囲：1-255
Port	ポート番号を指定します。 • 設定可能範囲：1-65535
Timeout	リモートデバイスからのレスポンスを待機する時間を指定します。この時間を過ぎるとタイムアウトになります。 • 設定可能範囲：1-65535（秒） • 初期値：5（秒）
Length	送信データグラムのバイト数を指定します。 • 設定可能範囲：1-1420（Bytes）
ToS	送信データグラムの IP ヘッダにセットされる ToS 値を指定します。 • 設定可能範囲：0-255
Frequency	トレースルートの頻度を指定します。 • 設定可能範囲：0-86400（秒）
Source IPv4 Address	トレースルートパケットの送信元 IPv4 アドレスを入力します。
Probe Number	プローブ数を指定します。 • 設定可能範囲：1-1000 • 初期値：1
IPv6 Trace Route	
IPv6 Address	宛先 IPv6 アドレスを入力します。
Domain Name	宛先のドメイン名を入力します。

項目	説明
Initial TTL	初期 TTL（Time-To-Live）値を入力します。UDP データグラムは指定した TTL 値で送信されます。 • 設定可能範囲：1-255
Max TTL	トレースルートリクエストの Time-To-Live (TTL) 値を入力します。トレースルートパケットが通過できるルータの最大数となります。2 台のデバイス間でネットワークパスを検出する際に、このトレースルートオプションを使用します。 • 設定可能範囲：1-255
Port	ポート番号を指定します。 • 設定可能範囲：1-65535
Timeout	リモートデバイスからのレスポンスを待機する時間を指定します。この時間を過ぎるとタイムアウトになります。 • 設定可能範囲：1-65535（秒）
Length	送信データグラムのバイト数を指定します。 • 設定可能範囲：1-1420（Bytes）
Frequency	トレースルートの頻度を指定します。 • 設定可能範囲：0-86400
Source IPv6 Address	トレースルートパケットの送信元 IPv6 アドレスを入力します。
Probe Number	プローブ数を指定します。 • 設定可能範囲：1-1000 • 初期値：1

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

「IPv4 Trace Route」セクションで「Start」ボタンをクリックすると、以下の「IPv4 Trace Route Result」画面が表示されます。

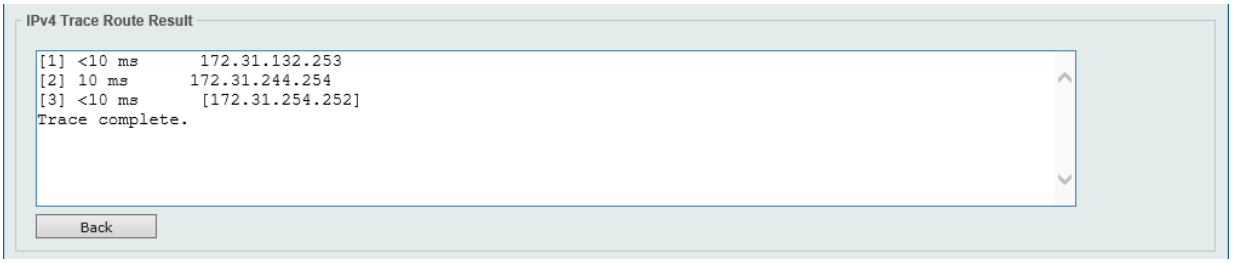


図 16-40　IPv4 Trace Route Result 画面

「IPv6 Trace Route」セクションで「Start」ボタンをクリックすると、以下の「IPv6 Trace Route Result」画面が表示されます。

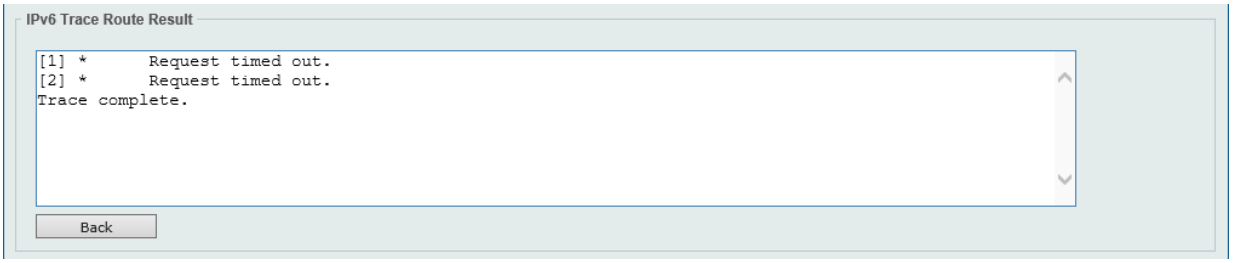


図 16-41　IPv6 Trace Route Result 画面

「Back」ボタンをクリックして、前の画面に戻ります。

Language Management（言語管理）

言語ファイルのインストールを行います。

Tools > Language をクリックし、次の設定画面を表示します。

図 16-42　Language Management 画面

画面に表示される項目：

項目	説明
Language File	「ファイルの選択 / 参照」をクリックして、ローカル PC 上の言語ファイルを選択します。

「Apply」をクリックし、言語ファイルをインストールします。

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。

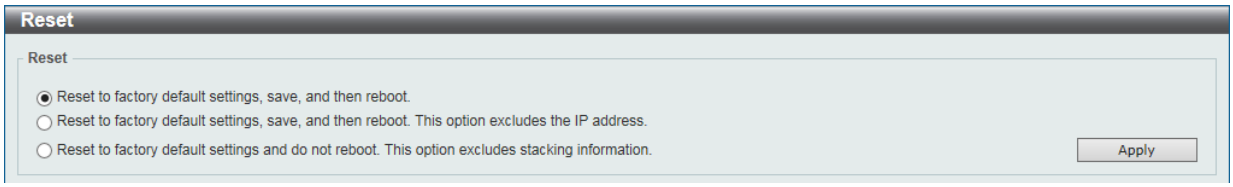


図 16-43　Reset 画面

画面に表示される項目：

項目	説明
Reset to factory default settings, save, and then 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、スタック情報を含む）
Reset to factory default settings, save, and then reboot. This option excludes the 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 アドレスは除く）
Reset to factory default settings and do not reboot. This option excludes stacking information.	スイッチを工場出荷時設定にリセットしますが、再起動は行いません。 （スタック情報は除く）

「Apply」ボタンをクリックして、リセットを開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

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

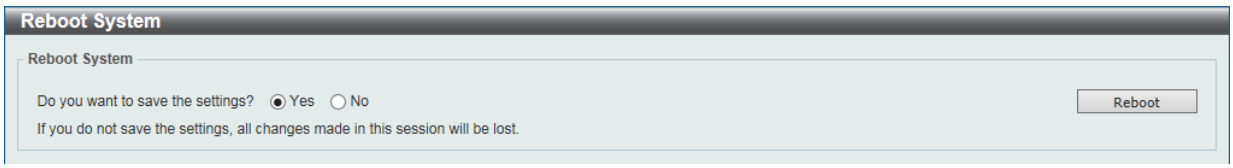


図 16-44　Reboot System 画面

画面に表示される項目：

項目	説明
Do you want to save the settings?	再起動オプションを指定します。 • 「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。

「Reboot」ボタンをクリックして、再起動を開始します。

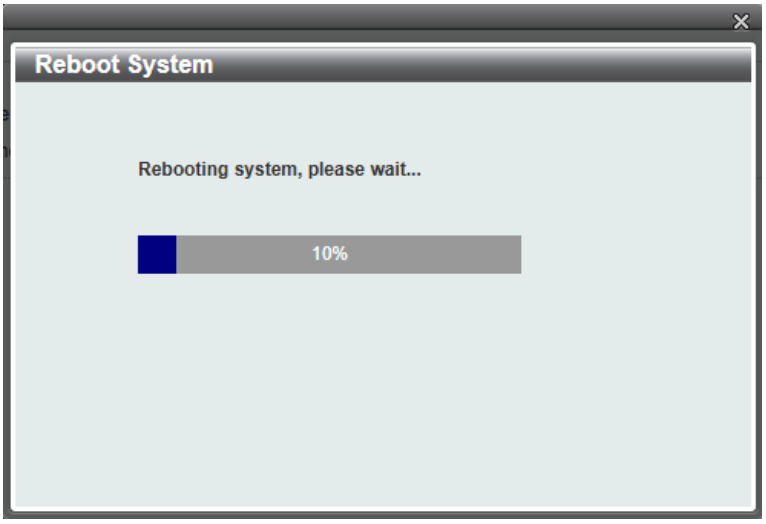


図 16-45　Reboot System 画面（再起動時）

Wizard（ウィザード）

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

Online Help（オンラインヘルプ）

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

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

User Guide（ユーザガイド（英語版））

ユーザガイド（英語版）を表示します。インターネット接続が必要です。

言語

WebUI で表示される言語をドロップダウンメニューから選択します。

Logout（ログアウト）

クリックすると Web GUI からログアウトします。

付録

付録 A パスワードリカバリ手順

本スイッチシリーズのパスワードのリセット手順について説明します。

ネットワークにアクセスを試みるすべてのユーザに対し、認証を行うことが必要かつ重要です。権限のあるユーザを受け入れるために使用される基本的な認証方法は、ユーザ名とパスワードを使用したローカルログイン認証です。ネットワーク管理者は、パスワードを忘れた場合や破棄された場合などに、パスワードのリセットを行う必要があります。

本セクションでは、スイッチのパスワードリカバリ機能を使用して、パスワードを簡単に復旧する方法について説明します。
パスワードをリセットするには、次の手順を実行します。

1. セキュリティの理由により、パスワードリカバリ機能を実行するには物理的にコンソールポートへ接続する必要があります。
   本スイッチのコンソールポートに、端末または端末エミュレーションを搭載した PC を接続します。
2. スイッチの電源をオンにします。パスワードリカバリモードに入るためには、「UART init」が 100% までロードされた後 2 秒以内に、ホットキー「 ^ 」を押します。「Password Recovery Mode」に入ると、スイッチのすべてのポートが無効になります。

```
Loader Procedure
--------------------------------------------------------------------------------
 Please Wait, Loading 1.00.032 Runtime Image ..............  100 %
 UART init ..................................................  100 %
 Starting runtime image
```

```
Password Recovery Mode

Switch(reset-config)#
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
no enable password	全アカウントレベルのパスワードを削除します。
no login console	コンソールのログイン方法をクリアします。
no username	全ローカルユーザアカウントを削除します。
password-recovery	パスワードリカバリ手順を開始します。
reload	スイッチを再起動します。
reload clear running-config	実行中の設定を工場出荷時の設定に戻し、スイッチを再起動します。
show running-config	実行中の設定を表示します。
show username	ローカルユーザアカウント情報を表示します。

付録 B システムログエントリ

スイッチのシステムログに出力されるログイベントとそれらの意味を以下に示します。

Alert（アラート）、Critical（重大）、Warning（警告）、Notice（通知）、Informational（情報）

ログの内容		緊急度	イベントの説明
802.1X			
1	802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) **パラメータ説明：** • reason: 認証失敗の理由 (1) 認証失敗 (2) サーバ応答なし (3) サーバ設定なし (4) リソース不足 (5) タイムアウト • username：認証ユーザ名 • interface-id：インタフェース番号 • mac-address：認証デバイスの MAC アドレス	Critical	802.1X 認証に失敗しました。
2	802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) **パラメータ説明：** • username：認証ユーザ名 • interface-id：インタフェース番号 • mac-address：認証デバイスの MAC アドレス	Informational	802.1X 認証に成功しました。
3	802.1X cannot work correctly because ACL rule resource is not available	Alert	ACL ハードウェアの枯渇により 802.1X 認証を実行できません。
AAA			
1	AAA is <status> **パラメータ説明：** status：AAA が有効または無効	Informational	AAA グローバルステートが有効または無効です。
2	Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ（例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式（例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証ユーザ名	Informational	ログインに成功しました。
3	Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ（例：Console、Telnet、SSH、Web、Web(SSL) • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式（例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証ユーザ名	Warning	ログインに失敗しました。
4	RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • vid：RADIUS サーバから割り当てられた VLAN ID • interface–id：認証クライアントのポート番号 • username：認証ユーザ名	Informational	RADIUS が有効な VLAN ID 属性を割り当てました。

ログの内容		緊急度	イベントの説明
5	RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port <interface-id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • direction:：帯域幅制御の方向（例：ingress または egress.） • threshold: サーバから割り当てられた帯域幅のしきい値 • interface–id：認証クライアントのポート番号 • username：認証ユーザ名	Informational	RADIUS が有効な帯域幅属性を割り当てました。
6	RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port <interface-id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • priority：RADIUS サーバから割り当てられた優先度 • interface–id：認証クライアントのポート番号 • username：認証ユーザ名	Informational	RADIUS が有効な優先度属性を割り当てました。
7	RADIUS server <server-ip> assigns <username> ACL failure at port <interface-id> (<acl-script>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • username：認証ユーザ名 • interface–id：認証クライアントのポート番号 • acl-script：RADIUS サーバから割り当てられた ACL スクリプト	Warning	RADIUS が ACL スクリプトを割り当てましたが、リソース不足のためシステムへの適用に失敗しました。
8	Login failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ（例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • server-ip：AAA サーバ IP アドレス • username：認証ユーザ名	Warning	リモートサーバが認証リクエストに応答しません。
9	Successful enable privilege through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ（例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式（例：local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証ユーザ名	Informational	特権の有効化に成功しました。
10	Enable privilege failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type：EXEC タイプ（例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式（例：local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証ユーザ名	Warning	特権の有効化に失敗しました。
11	Enable privilege failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ（例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • server-ip：AAA サーバ IP アドレス • username：認証されるユーザ名	Warning	リモートサーバが enable パスワードの認証リクエストに応答しません。

ログの内容		緊急度	イベントの説明
12	User <username> locked out on authentication failure **パラメータ説明：** • username：ロックアウトされたユーザ名	Notice	ローカルユーザがロックアウトされました。
13	User <username> unlocked **パラメータ説明：** • username：ロックが解除されたユーザ名	Notice	ローカルユーザのロックが解除されました。
14	server <server-ip> assigns <username> ACL success at port <interface-id> (<acl-script>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • username：認証ユーザ名 • interface–id：認証クライアントのポート番号 • acl-script：RADIUS サーバから認証された ACL スクリプト	Warning	RADIUS が ACL スクリプトの割り当てに成功しました。
ARP			
1	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <port-num>, Interface: <ipif-name>) **パラメータ説明：** • ipaddr：重複する IP アドレス • macaddr：重複する IP アドレスを持つデバイスの MAC アドレス • portNum：デバイスのポート番号 • ipif-name：重複する IP アドレスを持つスイッチの IP インタフェース名	Warning	Gratuitous ARP は重複した IP を検出しました。
Auto image			
1	The downloaded firmware was successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：TFTP サーバの IP アドレス	Informational	DHCP 自動イメージによるファームウェア適用が成功しました。
2	The downloaded firmware was not successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：TFTP サーバの IP アドレス	Informational	DHCP 自動イメージによるファームウェア適用が失敗しました。
Auto Save Config			
1	CONFIG-6-DDPSAVECONFIG: Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	DDP の設定情報が自動で保存されました。
Auto Surveillance VLAN			
1	New surveillance device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface–id：インタフェース名 • mac-address：監視デバイスの MAC アドレス	Informational	インタフェースで新しい監視デバイスが検出されました。
2	<interface-id> add into surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名 • vid：VLAN ID	Informational	サーベイランス VLAN が有効のインタフェースが自動的にサーベイランス VLAN に追加されました。
3	<interface-id> remove from surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名 • vid：VLAN ID	Informational	インタフェースがサーベイランス VLAN から離脱し、エージング期間内に当該インタフェースに監視デバイスが検出されませんでした。

ログの内容		緊急度	イベントの説明
BPDU Protection			
1	<interface-id> enter STP BPDU under protection state (mode: <mode>) **パラメータ説明：** • interface–id：STP BPDU アタックが検出されたインタフェース • mode：インタフェースの BPDU 保護モード（drop、block、shutdown）	Informational	BPDU アタックが発生しました。
2	<interface-id> recover from BPDU under protection state. **パラメータ説明：** • interface–id：STP BPDU アタックが検出されたインタフェース	Informational	STP BPDU 攻撃から回復しました。
CFM			
1	CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward） • mepid：MEP の MEPID。「0」は不明な MEIPD を意味します。 • macaddr：MEP の MAC アドレス。すべて「0」となっている場合は、不明な MAC アドレスです。	Critical	クロス接続が検出されました。
2	CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward） • mepid：MEP の MEPID。「0」は不明な MEIPD を意味します。 • macaddr：MEP の MAC アドレス。すべて「0」となっている場合は、不明な MAC アドレスです。	Warning	エラー CFM CCM パケットが検出されました。
3	CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward）	Warning	リモート MEP の CCM パケットを受信できません。
4	CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward）	Warning	リモート MEP の MAC がエラー状態です。
5	CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward）	Informational	リモート MEP による CFM 不良の検出

ログの内容		緊急度	イベントの説明
CFM Extension			
1	AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward） • mepid：MEP の MEPID	Notice	AIS コンディションの検出
2	AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>,Local(Interface:<interface-id>,Direction:<mepdirection>, MEPID:<mepid>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward） • mepid：MEP の MEPID	Notice	AIS コンディションの解消
3	LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward） • mepid：MEP の MEPID	Notice	LCK コンディションの検出
4	LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース番号 • mepdirection：MEP の方向（inward、outward） • mepid：MEP の MEPID	Notice	LCK コンディションの解消
Configuration/Firmware			
1	[Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Informational	ファームウェアのアップグレードに成功しました。

ログの内容		緊急度	イベントの説明
2	[Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Warning	ファームウェアのアップグレードに失敗しました。
3	[Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Informational	ファームウェアのアップロードに成功しました。
4	[Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Warning	ファームウェアのアップロードに失敗しました。
5	[Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Informational	コンフィグレーションのダウンロードに成功しました。
6	[Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Warning	コンフィグレーションのダウンロードに失敗しました。

ログの内容		緊急度	イベントの説明
7	[Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Informational	コンフィグレーションのアップロードに成功しました。
8	[Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Warning	コンフィグレーションのアップロードに失敗しました。
9	[Unit <unitID>,]Configuration saved to flash by console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • username：現在のログインユーザ名	Informational	コンソール経由でコンフィグレーションがフラッシュに保存されました。
10	[Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	リモートでコンフィグレーションがフラッシュに保存されました。
11	Log message uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Informational	ログメッセージのアップロードが成功しました。
12	Log message uploaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Warning	ログメッセージのアップロードが失敗しました。

ログの内容		緊急度	イベントの説明
13	[Unit <unitID>,]Downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • unitID：ユニット ID。スタンドアロンの場合は出力されません。 • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバ上のパスとファイル名	Warning	不明な種類のファイルのダウンロードに失敗しました。
• ユーザのセッションは Console、Web、SNMP、Telnet、SSH のいずれかです。 • コンソール経由でのコンフィグレーション / ファームウェアの更新では、IP や MAC 情報はログ出力されません。			
DAD			
1	Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages **パラメータ説明：** • ipv6address：NS メッセージの IPv6 アドレス • interface-id：インタフェース ID	Warning	DAD の間に、重複アドレスを含む「Neighbor Solicitation」(NS) メッセージを受信しました。
2	Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages **パラメータ説明：** • ipv6address：NA メッセージの IPv6 アドレス • interface-id：インタフェース ID	Warning	DAD の間に、重複アドレスを含む「Neighbor Advertisement」(NA) メッセージを受信しました。
DAI			
1	Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) **パラメータ説明：** • type：ARP パケットのタイプ（ARP パケット要求または応答） • ip-address：IP アドレス • mac-addr：MAC アドレス • vlan-id：VLAN ID • interface-id：インタフェース ID	Warning	DAI で不正な ARP パケットを検出しました。
2	Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) **パラメータ説明：** • type：ARP パケットのタイプ（ARP パケット要求または応答） • ip-address：IP アドレス • mac-addr：MAC アドレス • vlan-id：VLAN ID • interface-id：インタフェース ID	Informational	DAI で有効な ARP パケットを検出しました。
DDM			
1	Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded **パラメータ説明：** • interface-id：ポートインタフェース ID • component：DDM のしきい値タイプ。しきい値タイプは以下のいずれかです。 - temperature - supply voltage - bias current - TX power - RX power • high-low：High または Low しきい値	Warning	SFP パラメータのいずれが警告しきい値を超えました。

ログの内容		緊急度	イベントの説明
2	Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded **パラメータ説明：** • interface-id：ポートインタフェース ID • component：DDM のしきい値タイプ。しきい値タイプは以下のいずれかです。 - temperature - supply voltage - bias current - TX power - RX power • high-low：High または Low しきい値	Critical	SFP パラメータのいずれかがアラームしきい値を超えました。
3	Optical transceiver <interface-id> <component> back to normal **パラメータ説明：** • interface-id：ポートインタフェース ID • component：DDM のしきい値タイプ。しきい値タイプは以下のいずれかです。 - temperature - supply voltage - bias current - TX power - RX power	Warning	SFP パラメータのいずれかが警告しきい値から回復しました。（アラームしきい値から回復した後、まだ警告しきい値内にある場合はログは送信されません。）
DHCP Snooping			
1	DHCP snooping entry reload failure (URL: <url-string>) **パラメータ説明：** • url-string：URL 文字列	Informational	外部ストレージからの DHCP スヌーピングエントリのリロードに失敗しました。
DHCPv6 Client			
1	DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] **パラメータ説明：** • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 クライアントインタフェース管理者ステートが変更されました。
2	DHCPv6 client obtains an IPv6 address <ipv6address> on interface <ipif-name> **パラメータ説明：** • ipv6address：DHCPv6 クライアントが取得した IPv6 アドレス • ipif-name：DHCPv6 クライアントが IPv6 アドレスを取得したインタフェース名	Informational	DHCPv6 クライアントが IPv6 アドレスを取得しました。
3	The IPv6 address <ipv6address> on interface <ipif-name> starts renewing **パラメータ説明：** • ipv6address：更新処理を開始した IPv6 アドレス • ipif-name：IPv6 アドレスが存在するインタフェース名	Informational	IPv6 アドレスの更新を開始します。
4	The IPv6 address <ipv6address> on interface <ipif-name> renews success **パラメータ説明：** • ipv6address：更新処理が完了した IPv6 アドレス • ipif-name：IPv6 アドレスが存在するインタフェース名	Informational	IPv6 アドレスの更新に成功しました。
5	The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding **パラメータ説明：** • ipv6address：リバインド処理を開始した IPv6 アドレス • ipif-name：IPv6 アドレスが存在するインタフェース名	Informational	IPv6 アドレスのリバインドを開始します。
6	The IPv6 address <ipv6address> on interface <ipif-name> rebinds success **パラメータ説明：** • ipv6address：リバインド処理が完了した IPv6 アドレス • ipif-name：IPv6 アドレスが存在するインタフェース名	Informational	IPv6 アドレスのリバインドに成功しました。

ログの内容		緊急度	イベントの説明
7	The IPv6 address <ipv6address> on interface <ipif-name> was deleted **パラメータ説明：** • ipv6address：削除された IPv6 アドレス • ipif-name：IPv6 アドレスが削除されたインタフェース名	Informational	IPv6 アドレスが削除されました。
8	DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> **パラメータ説明：** • intf-name：ステートが変更された DHCPv6 クライアント PD インタフェース名	Informational	DHCPv6 クライアント PD のインタフェース管理者ステートが変更されました。
9	DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> **パラメータ説明：** • ipv6networkaddr：DHCPv6 クライアント PD により取得された IPv6 プリフィックス • intf-name：DHCPv6 クライアント PD が IPv6 プリフィックスを取得したインタフェース名	Informational	DHCPv6 クライアント PD が IPv6 プリフィックスを取得しました。
10	The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing **パラメータ説明：** • ipv6networkaddr：更新処理を開始した IPv6 プリフィックス • intf-name：IPv6 プリフィックスが存在するインタフェース名	Informational	IPv6 プリフィックスの更新を開始します。
11	The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success **パラメータ説明：** • ipv6networkaddr：更新処理が完了した IPv6 プリフィックス • intf-name：IPv6 プリフィックスが存在するインタフェース名	Informational	IPv6 プリフィックスの更新に成功しました。
12	The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding **パラメータ説明：** • ipv6networkaddr：リバインド処理を開始した IPv6 プリフィックス • intf-name：IPv6 プリフィックスが存在するインタフェース名	Informational	IPv6 プリフィックスのリバインドを開始します。
13	The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success **パラメータ説明：** • ipv6networkaddr：リバインド処理が完了した IPv6 プリフィックス • intf-name：IPv6 プリフィックスが存在するインタフェース名	Informational	IPv6 プリフィックスのリバインドに成功しました。
14	The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted **パラメータ説明：** • ipv6networkaddr：削除された IPv6 プリフィックス • intf-name：IPv6 プリフィックスが削除されたインタフェース名	Informational	IPv6 プリフィックスが削除されました。
DHCPv6 Relay			
1	DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] **パラメータ説明：** • ipif-name：DHCPv6 リレーエージェントインタフェース名	Informational	特定インタフェースの DHCPv6 リレーの管理者ステートが変更されました。
DHCPv6 Server			
1	The address of the DHCPv6 Server pool <pool-name> is used up **パラメータ説明：** • pool-name：DHCPv6 サーバプール名	Informational	DHCPv6 サーバプールのアドレスが枯渇しました。
2	The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 256	Informational	割り当てられた IPv6 アドレス数が 256 に達しました。

ログの内容		緊急度	イベントの説明
	DNS Resolver		
1	Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr> **パラメータ説明：** • domain-name：ドメイン名文字列 • ipaddr：スタティック / ダイナミック IP アドレス	Informational	重複するドメイン名キャッシュが追加され、ダイナミックドメイン名キャッシュが削除されました。
	DoS Prevention		
1	<dos-type> is dropped from (Port <interface-id>) **パラメータ説明：** • dos-type：DoS 攻撃タイプ • interface-id:：インタフェース名	Notice	DoS 攻撃を検出しました。
	DULD		
1	DULD <INTERFACE-ID> is detected as unidirectional link **パラメータ説明：** • INTERFACE-ID：インタフェース名	Warning	ポートで単一方向リンクを検出しました。
	ERPS		
1	Manual switch is issued on node (MAC: < macaddr >, instance < InstanceID >) **パラメータ説明：** • macaddr：MAC アドレス • InstanceID：インスタンス ID	Warning	「Manual Switch」が発行されました。
2	Signal fail detected on node (MAC: < macaddr >, instance < InstanceID >) **パラメータ説明：** • macaddr：MAC アドレス • InstanceID：インスタンス ID	Warning	シグナル失敗が検出されました。
3	Signal fail cleared on node(MAC: < macaddr >, instance < InstanceID >) **パラメータ説明：** • macaddr：MAC アドレス • InstanceID：インスタンス ID	Warning	シグナル失敗が解消されました。
4	Force switch is issued on node (MAC: < macaddr >, instance < InstanceID >) **パラメータ説明：** • macaddr：MAC アドレス • InstanceID：インスタンス ID	Warning	「Force Switch」が発行されました。
5	Clear command is issued on node (MAC: < macaddr >, instance < InstanceID >) **パラメータ説明：** • macaddr：MAC アドレス • InstanceID：インスタンス ID	Warning	「Clear」コマンドが発行されました。
6	RPL owner conflicted on the node (MAC: < macaddr >, instance < InstanceID >) **パラメータ説明：** • macaddr：MAC アドレス • InstanceID：インスタンス ID	Warning	RPL オーナが競合しています。
	ErrDisable		
1	Port <interface-id> enters error disable state due to <reason-id> **パラメータ説明：** • interface-id：ポート番号 • reason-id：「Loopback Detection」「Port Security Violation」「Storm Control」「BPDU Protect」「ARP Rate Limit」「DHCP Rate Limit」「L2 Protocol Tunneling」「Scheduled Port-shutdown by Power Saving」「Scheduled Hibernation by Power Saving」	Warning	ポートがエラーディセーブル状態に移行しました。

ログの内容		緊急度	イベントの説明
2	Port <interface-id> leaves the error disable state which is previously caused by <reason-id> **パラメータ説明：** • interface-id：ポート番号 • reason-id：「Loopback Detection」「Port Security Violation」「Storm Control」「BPDU Protect」「ARP Rate Limit」「DHCP Rate Limit」「L2 Protocol Tunneling」「Scheduled Port-shutdown by Power Saving」「Scheduled Hibernation by Power Saving」	Warning	ポートがエラーディセーブル状態から元の状態に戻りました。
3	Port <interface-id> VLAN <vid> enters error disable state due to <reason-id> **パラメータ説明：** • interface-id：ポート番号 • reason-id：「Loopback Detection」「Port Security Violation」「Storm Control」「Scheduled Port-shutdown by Power Saving」「Scheduled Hibernation by Power Saving」 • vid：VLAN ID	Warning	ポートがエラーディセーブル状態に移行しました。
4	Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id> **パラメータ説明：** • interface-id：ポート番号 • reason-id：「Loopback Detection」「Port Security Violation」「Storm Control」「Scheduled Port-shutdown by Power Saving」「Scheduled Hibernation by Power Saving」 • vid：VLAN ID	Warning	ポートがエラーディセーブル状態から元の状態に戻りました。
Ethernet OAM			
1	OAM dying gasp event received (Port<interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートで「Dying gasp」イベントが発生しました。
2	Device encountered an OAM dying gasp event	Warning	ローカルで「Dying gasp」イベントが発生しました。
3	OAM critical event received (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでクリティカルなイベントが発生しました。
4	Device encountered an OAM critical event (Port <interface-id>, <condition>) **パラメータ説明：** • interface-id：インタフェース ID • condition：クリティカルなリンクイベントの発生状況について表示します。（例；OAM disable、Port shutdown、Port link down、Packet overload など）	Warning	ローカルでクリティカルなイベントが発生しました。
5	Errored frame event received (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでエラーフレームイベントが発生しました。
6	Errored frame period event received (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでエラーフレーム期間イベントが発生しました。
7	Errored frame seconds summary event received (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでエラーフレーム秒サマリイベントが発生しました。
8	OAM Remote loopback started (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートループバックが開始しました。

ログの内容		緊急度	イベントの説明
9	OAM Remote loopback stopped (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートループバックが停止しました。
10	Device encountered an errored frame event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	ローカルでエラーフレームイベントが発生しました。
11	Device encountered an errored frame period event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	ローカルでエラーフレーム期間イベントが発生しました。
12	Device encountered an errored frame seconds summary event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	ローカルでエラーフレーム秒サマリイベントが発生しました。
Interface			
1	Port <port-type><interface-id> link down **パラメータ説明：** • port-type：ポートタイプ • interface-id：インタフェース ID	Informational	ポートがリンクダウンしました。
2	Port <port-type><interface-id> link up, <link-speed> **パラメータ説明：** • port-type：ポートタイプ • interface-id：インタフェース ID • link-speed：ポートリンク速度	Informational	ポートがリンクアップしました。
IP Source Guard（IPSG）			
1	Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>) **パラメータ説明：** • ipaddr：IP アドレス • macaddr：MAC アドレス • vlanid：VLAN ID • interface-id：インタフェース ID	Warning	ハードウェアルールのリソースが枯渇しているため、DHCP スヌーピングエントリを ISPG テーブルにセットできません。
IPv6 Source Guard			
1	Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlan-id>, Interface <interface-id>) **パラメータ説明：** • ipaddr：IPv6 スヌーピングエントリの IPv6 アドレス • macaddr：IPv6 スヌーピングエントリの MAC アドレス • vlanid：IPv6 スヌーピングエントリの VLAN ID • interface-id：IPv6 スヌーピングエントリのインタフェース ID	Warning	ハードウェアルールのリソースが枯渇しているため、IPv6 スヌーピングエントリを ISPG テーブルにセットできません。
IPv6 Snooping			
1	Failed to glean (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) **パラメータ説明：** • IPADDR：IPv6 スヌーピングエントリの IP アドレス • MACADDR：IPv6 スヌーピングエントリの MAC アドレス • VLANID：IPv6 スヌーピングエントリの VLAN ID • NTERFACE-ID：IPv6 スヌーピングエントリのインタフェース ID	Notice	IPv6 Data Glean に失敗しました。

ログの内容		緊急度	イベントの説明
2	Glean to recover (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) **パラメータ説明：** • IPADDR：IPv6 スヌーピングエントリの IP アドレス • MACADDR：IPv6 スヌーピングエントリの MAC アドレス • VLANID：IPv6 スヌーピングエントリの VLAN ID • NTERFACE-ID：IPv6 スヌーピングエントリのインタフェース ID	Notice	IPv6 Data Glean に成功しました。
LACP			
1	Link Aggregation Group <group-id> link up **パラメータ説明：** • group-id：リンクアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクアップしました。
2	Link Aggregation Group <group-id> link down **パラメータ説明：** • group-id：リンクアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクダウンしました。
3	<ifname> attach to Link Aggregation Group <group-id> **パラメータ説明：** • ifname：アグリゲーショングループにアタッチされたポートのインタフェース名 • group-id：ポートがアタッチされたアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループにアタッチされました。
4	<ifname> detach from Link Aggregation Group <group-id> **パラメータ説明：** • ifname：アグリゲーショングループからデタッチされたポートのインタフェース名 • group-id：ポートがデタッチされたアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループからデタッチされました。
LBD（ループバック検知）			
1	<interface-id> LBD loop occurred **パラメータ説明：** • interface-id：ループが検出されたインタフェース	Critical	ポートベースモードでループバックが検出されました。
2	<interface-id> VLAN <vlan-id> LBD loop occurred **パラメータ説明：** • interface-id：ループが検出されたインタフェース • vlan-id：ループが検出された VLAN ID	Critical	VLAN ベースモードでループバックが検出されました。
3	<interface-id> LBD loop recovered **パラメータ説明：** • interface-id：ループから回復したインタフェース	Critical	ポートベースモードでループバックから回復しました。
4	<interface-id> VLAN <vlan-id> LBD loop recovered **パラメータ説明：** • interface-id：ループから回復したインタフェース • vlan-id：ループから回復した VLAN ID	Critical	VLAN ベースモードでループバックからポートが回復しました。
5	Loop VLAN numbers overflow	Critical	ループバックが発生した VLAN の数が予約数に達しました。

ログの内容		緊急度	イベントの説明
LLDP-MED			
1	LLDP-MED topology change detected (on port <portNum>. chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent (1) 2. interfaceAlias (2) 3. portComponent (3) 4. macAddress (4) 5. networkAddress (5) 6. interfaceName (6) 7. local (7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias (1) 2. portComponent (2) 3. macAddress (3) 4. networkAddress (4) 5. interfaceName (5) 6. agentCircuitId (6) 7. local (7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notice	LLDP-MED トポロジの変更が検出されました。
2	Conflict LLDP-MED device type detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent (1) 2. interfaceAlias (2) 3. portComponent (3) 4. macAddress (4) 5. networkAddress (5) 6. interfaceName (6) 7. local (7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias (1) 2. portComponent (2) 3. macAddress (3) 4. networkAddress (4) 5. interfaceName (5) 6. agentCircuitId (6) 7. local (7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notice	LLDP-MED デバイスタイプの重複が検出されました。

ログの内容		緊急度	イベントの説明
3	Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent (1) 2. interfaceAlias (2) 3. portComponent (3) 4. macAddress (4) 5. networkAddress (5) 6. interfaceName (6) 7. local (7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias (1) 2. portComponent (2) 3. macAddress (3) 4. networkAddress (4) 5. interfaceName (5) 6. agentCircuitId (6) 7. local (7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notice	LLDP-MED TLV セットの非互換性が検出されました。
Login/Logout CLI			
1	Successful login through Console (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ名	Informational	コンソール経由のログインに成功しました。
2	Login failed through Console (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ名	Warning	コンソール経由のログインに失敗しました。
3	Console session timed out (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ名	Informational	コンソールのセッションがタイムアウトしました。
4	Logout through Console (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ名	Informational	コンソール経由でログアウトしました。
5	Successful login through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由のログインに成功しました。
6	Login failed through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Warning	Telnet 経由のログインに失敗しました。
7	Telnet session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	Telnet のセッションがタイムアウトしました。

ログの内容		緊急度	イベントの説明
8	Logout through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由でログアウトしました。
9	Successful login through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	SSH 経由のログインに成功しました。
10	Login failed through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Critical	SSH 経由のログインに失敗しました。
11	SSH session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	SSH のセッションがタイムアウトしました。
12	Logout through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	SSH 経由でログアウトしました。
MAC-based Access Control（MAC 認証）			
1	MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) **パラメータ説明：** • mac-address：ホストの MAC アドレス • interface-id：ホストが認証されたインタフェース • vlan-id：認証後にホストが所属する VLAN ID	Informational	ホストは MAC 認証にパスしました。
2	MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) **パラメータ説明：** • mac-address：ホストの MAC アドレス • interface-id：ホストが認証されたインタフェース • vlan-id：エージアウト前にホストが所属する VLAN ID	Informational	ホストはエージアウトしました。
3	based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) **パラメータ説明：** • mac-address：ホストの MAC アドレス • interface-id：ホストが認証を試みたインタフェース • vlan-id：ホストが所属する VLAN ID	Critical	ホストは MAC 認証に失敗しました。
4	MAC-based Access Control enters stop learning state	Warning	デバイス全体で認証されたユーザ数が上限数に達しました。
5	MAC-based Access Control recovers from stop learning state	Warning	デバイス全体で認証されたユーザ数が一定期間、上限数を下回りました。
6	<interface-id> enters MAC-based Access Control stop learning state **パラメータ説明：** • interface-id：ホストが認証されたインタフェース	Warning	インタフェースで認証されたユーザ数が上限数に達しました。
7	<interface-id> recovers from MAC-based Access Control stop learning state **パラメータ説明：** • interface-id：ホストが認証されたインタフェース	Warning	インタフェースの認証されたユーザ数が一定期間、上限数を下回りました。

ログの内容		緊急度	イベントの説明
MSTP Debug			
1	Spanning Tree Protocol is enabled	Informational	スパニングツリープロトコル有効化
2	Spanning Tree Protocol is disabled	Informational	スパニングツリープロトコル無効化
3	Topology changed (Instance: <instance-id>,<interface-id>, MAC:<macaddr>) **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号 • macaddr：ブリッジの MAC アドレス	Notice	MSTP インスタンストポロジに変更がありました。
4	[CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority:<priority>) **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。 • macaddr：ブリッジの MAC アドレス • value：ブリッジの優先値。4096 で割り切れる数値です。	Informational	新しい MSTP インスタンスルートブリッジが選定されました。
5	New root port selected (Instance:<instance-id>, <interface-id>) **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号	Notice	新しい MSTP インスタンスルートポートが選定されました。
6	Spanning Tree port status change (Instance:<instance-id>, <interface-id>) <old-status> -> <new-status> **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号 • old-status：ポートの前のステータス • new-status：ポートの新しいステータス - Disable、Discarding、Learning、Forwarding	Notice	MSTP インスタンスポートのステートが変更されました。
7	Spanning Tree port role change (Instance:<instance-id>, <interface-id>) <old-role> -> <new-role> **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号 • old-role：STP ロールの前のステータス • new-role：STP ロールの新しいステータス - DisablePort、AlternatePort、BackupPort、RootPort、DesignatedPort、NonstpPort、MasterPort	Informational	MSTP インスタンスポートのロールが変更されました。
8	Spanning Tree instance created (Instance:<instance-id>) **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。	Informational	MST インスタンスが作成されました。
9	Spanning Tree instance deleted (Instance:<instance-id>) **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。	Informational	MST インスタンスが削除されました。

ログの内容		緊急度	イベントの説明
10	Spanning Tree version change (new version:<new-version>) **パラメータ説明：** • new-version：アクティブなスパニングツリーのバージョン	Informational	スパニングツリーのバージョンが変更されました。
11	Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision-level>) **パラメータ説明：** • name：MST リージョンの名前 • revision-level：リビジョンレベル。同じ名前 / 異なるリビジョンレベルの場合、異なる MST リージョンのメンバと認識されます。	Informational	MST 設定でコンフィグレーション ID 名とリビジョンレベルが変更されました。
12	Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> add vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。 • startvlanid：追加される VLAN 範囲の開始 VLAN ID • endvlanid：追加される VLAN 範囲の終了 VLAN ID	Informational	MST インスタンスに VLAN がマッピングされました。
13	Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> delete vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。 • startvlanid：削除される VLAN 範囲の開始 VLAN ID • endvlanid：削除される VLAN 範囲の終了 VLAN ID	Informational	MST インスタンスから VLAN が削除されました。
14	Spanning Tree port role change (Instance:<instance-id>, <interface-id>) to alternate port due to the guard root **パラメータ説明：** • interface-id：MST インスタンス ID。0 は、デフォルトのインスタンス（CIST）を表します。 • interface-id：イベントを検出したポート番号	Informational	ガードルートによりポートロールが変更されます。
Peripheral			
1	Unit <unit-id> <fan-descr> back to normal **パラメータ説明：** • unit-id：ユニット ID • fan-descr：ファン ID と位置	Critical	ファンが回復しました。
2	Unit <unit-id> <fan-descr> failed **パラメータ説明：** • unit-id：ユニット ID • fan-descr：ファン ID と位置	Critical	ファンの不具合
3	Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> **パラメータ説明：** • unit-id：ユニット ID • thermal-sensor-descr：センサ ID と位置 • degree：現在の温度	Critical	温度センサがアラーム状態に移行しました。
4	Unit <unit-id> <thermal-sensor-descr> temperature back to normal **パラメータ説明：** • unit-id：ユニット ID • thermal-sensor-descr：センサ ID と位置	Critical	温度が通常に戻りました。

ログの内容		緊急度	イベントの説明
5	Unit <unit-id> <power-descr> failed **パラメータ説明：** • unit-id：ユニット ID • power-descr：電源の説明	Critical	電源の不具合
6	Unit <unit-id> <power-descr> back to normal **パラメータ説明：** • unit-id：ユニット ID • power-descr：電源の説明	Critical	電源回復
7	Unit <unit-id> Fan control mode changed from <mode> to <mode> **パラメータ説明：** • unit-id：ユニット ID • mode：ファン制御モード	Informational	手動でファン制御モードを変更しました。
8	Unit <unit-id> Fan control mode returns to normal mode **パラメータ説明：** • unit-id：ユニット ID	Warning	ファン制御モードが「Normal」に戻りました。
PoE			
1	Unit <unit-id> usage threshold <percentage> is exceeded **パラメータ説明：** • unit-id：ユニット ID • percentage：使用率しきい値	Warning	総電力の使用率がしきい値を超えました。
2	Unit <unit-id> usage threshold <percentage> is recovered **パラメータ説明：** • unit-id：ユニット ID • percentage：使用率しきい値	Warning	総電力の使用率がしきい値を下回りました。
3	PD alive check failed. (Port: <portNum>, PD: <ipaddr>) **パラメータ説明：** • portNum：ポート番号 • ipaddr：PD の IP アドレス	Warning	PD が Ping リクエストに応答しません。
Port Security			
1	MAC address <macaddr> causes port security violation on <interface-id> **パラメータ説明：** • macaddr：違反 MAC アドレス • interface-id：インタフェース名	Warning	MAC アドレスによりポートセキュリティ違反が発生しました。
2	Limit on system entry number has been exceeded	Warning	システムのアドレステーブルが一杯です。
Reboot Schedule			
1	Display “Reboot scheduled in 5 minutes” when the countdown equals 5 minutes	Warning	指定時間内にスイッチの再起動が行われます。
2	Display Reboot scheduled in 1 minute” when the countdown equals 1 minute	Critical	指定時間内にスイッチの再起動が行われます。
3	System was restarted by schedule in an interval time	Informational	指定時間後のスケジュール再起動が実行されました。
4	System was restarted by schedule at specific time	Informational	指定時刻のスケジュール再起動が実行されました。
5	System was restarted by periodic schedule at specific time	Informational	指定時刻の定期スケジュールされた再起動が実行されました。
6	Configuration was saved by schedule	Informational	「Save Before Reboot」オプションが設定されたスケジュール再起動が実行されました。

ログの内容		緊急度	イベントの説明
Safeguard			
1	Safeguard Engine enters EXHAUSTED mode	Warning	スイッチは「exhausted」モードに移行します。
2	Safeguard Engine enters NORMAL mode	Informational	スイッチはノーマルモードに移行します。
SIM			
1	Firmware upgraded by <session-name> successfully (Username: <username>) **パラメータ説明：** • session-name：ファームウェアアップグレード中のセッション名 • username：ファームウェアアップグレードを開始したユーザ（GMUSER）	Informational	ファームウェアのダウンロードに成功しました。
2	Firmware upgrade by <session-name> was unsuccessful! (Username: <username>) **パラメータ説明：** • session-name：ファームウェアアップグレード中のセッション名 • username：ファームウェアアップグレードを試みたユーザ（GMUSER）	Warning	ファームウェアのダウンロードに失敗しました。
3	Firmware upgraded to SLAVE successfully (Username: <username>) **パラメータ説明：** • username：スレーブへのファームウェアアップグレードを開始したユーザ（GMUSER）	Informational	スレーブへのファームウェアのダウンロードに成功しました。
4	Firmware upgraded to SLAVE unsuccessfully! (Username: <username>) **パラメータ説明：** • username：スレーブへのファームウェアアップグレードを試みたユーザ（GMUSER）	Warning	スレーブへのファームウェアのダウンロードに失敗しました。
5	Configuration successfully downloaded by <session-name> (Username: <username>) **パラメータ説明：** • session-name：コンフィグレーションダウンロード中のセッション名 • username：コンフィグレーションダウンロードを開始したユーザ（GMUSER）	Informational	コンフィグレーションのダウンロードに成功しました。
6	Configuration download by <session-name> was unsuccessful! (Username: <username>) **パラメータ説明：** • session-name：コンフィグレーションダウンロード中のセッション名 • username：コンフィグレーションダウンロードを試みたユーザ（GMUSER）	Warning	コンフィグレーションのダウンロードに失敗しました。
7	Configuration successfully uploaded by <session-name> (Username: <username>) **パラメータ説明：** • session-name：コンフィグレーションアップロード中のセッション名 • username：コンフィグレーションアップロードを開始したユーザ（GMUSER）	Informational	コンフィグレーションのアップロードに成功しました。
8	Configuration upload by <session-name> was unsuccessful! (Username: <username>) **パラメータ説明：** • session-name：コンフィグレーションアップロード中のセッション名 • username：コンフィグレーションアップロードを試みたユーザ（GMUSER）	Warning	コンフィグレーションのアップロードに失敗しました。
9	Log message successfully uploaded by <session-name> (Username: <username>) **パラメータ説明：** • session-name：ログアップロード中のセッション名 • username：ログアップロードを開始したユーザ（GMUSER）	Informational	ログのアップロードに成功しました。
10	Log message upload by <session-name> was unsuccessful! (Username: <username>) **パラメータ説明：** • session-name：ログアップロード中のセッション名 • username：ログアップロードを試みたユーザ（GMUSER）	Warning	ログのアップロードに失敗しました。

ログの内容		緊急度	イベントの説明
SNMP			
1	SNMP request received from <ipaddr> with invalid community string **パラメータ説明：** • ipaddr：IP アドレス	Informational	受信した SNMP リクエストに無効なコミュニティ文字列が含まれています。
SSH			
1	SSH server is enabled	Informational	SSH サーバは有効です。
2	SSH server is disabled	Informational	SSH サーバは無効です。
Stacking			
1	Unit: <unitID>, MAC: <macaddr> Hot insertion **パラメータ説明：** • unitID：ボックス ID • macaddr：MAC アドレス	Informational	デバイスが挿入されました。
2	Unit: <unitID>, MAC: <macaddr> Hot removal **パラメータ説明：** • unitID：ボックス ID • macaddr：MAC アドレス	Informational	デバイスが削除されました。
3	Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>) **パラメータ説明：** • Stack-TP-TYPE：スタッキングトポロジタイプ（Ring、Chain） • unitID：ボックス ID • macaddr：MAC アドレス	Critical	スタッキングトポロジが変更されました。
4	Backup master changed to master. Master (Unit: <unitID>) **パラメータ説明：** • unitID：ボックス ID	Informational	バックアップマスタがマスタに変更されました。
5	Slave changed to master. Master (Unit: <unitID>) **パラメータ説明：** • unitID：ボックス ID	Informational	スレーブがマスタに変更されました。
6	Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>) **パラメータ説明：** • unitID：ボックス ID • macaddr：重複するボックスの MAC アドレス	Critical	ボックス ID が重複しています。
7	Stacking port <port> link up **パラメータ説明：** • port：SIO ポート番号	Critical	スタックポートがリンクアップ
8	Stacking port <port> link down **パラメータ説明：** • port：SIO ポート番号	Critical	スタックポートがリンクダウン
9	SIO interface Unit <unitID> <SIOn > link up **パラメータ説明：** • unitID：ボックス ID • SIOn：SIO インタフェース番号（SIO1、SIO2）	Critical	SIO がリンクアップ
10	SIO interface Unit <unitID> <SIOn > link down **パラメータ説明：** • unitID：ボックス ID • SIOn：SIO インタフェース番号（SIO1、SIO2）	Critical	SIO がリンクダウン

	ログの内容	緊急度	イベントの説明
	Storm Control		
1	<Broadcast | Multicast | Unicast> storm is occurring on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：マルチキャストパケットによるストーム（未知 / 既知の L2 マルチキャスト、未知 / 既知の IP マルチキャストを含む） • Unicast：ユニキャストパケットによるストーム（既知 / 未知のユニキャストパケットを含む） • interface-id：ストームが発生しているインタフェース ID	Warning	ストームが発生しました。
2	<Broadcast | Multicast | Unicast> storm is cleared on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストストーム解消 • Multicast：マルチキャストストーム解消 • Unicast：ユニキャストストーム解消（既知 / 未知のユニキャストパケットを含む） • interface-id：ストームが解消したインタフェース ID	Informational	ストームが解消しました。
3	<interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm **パラメータ説明：** • interface-id：ストームによりエラー無効状態になったインタフェース ID • Broadcast：ブロードキャストストームによるエラー無効状態 • Multicast：マルチキャストストームによるエラー無効状態 • Unicast：ユニキャストストーム（既知 / 未知のユニキャストパケットを含む）によるエラー無効状態	Warning	パケットストームによりポートがシャットダウンしました。
	System		
1	Unit <unit-id> System warm start **パラメータ説明：** • unitID：ユニット ID スイッチがスタンドアロンモードの場合、ユニット ID は含まれません。	Critical	システムがウォームスタートしました。
2	Unit <unit-id> System cold start **パラメータ説明：** • unitID：ユニット ID スイッチがスタンドアロンモードの場合、ユニット ID は含まれません。	Critical	システムがコールドスタートしました。
3	Unit <unit-id> System started up **パラメータ説明：** • unitID：ユニット ID スイッチがスタンドアロンモードの場合、ユニット ID は含まれません。	Critical	システムが起動しました。
	Telnet		
1	Successful login through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet クライアントのユーザ名 • ipaddr：Telnet クライアントの IP アドレス	Informational	Telnet 経由のログインに成功しました。
2	Login failed through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet クライアントのユーザ名 • ipaddr：Telnet クライアントの IP アドレス	Warning	Telnet 経由のログインに失敗しました。
3	Logout through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet クライアントのユーザ名 • ipaddr：Telnet クライアントの IP アドレス	Informational	Telnet からログアウトしました。

ログの内容		緊急度	イベントの説明
4	Telnet session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet クライアントのユーザ名 • ipaddr：Telnet クライアントの IP アドレス	Informational	Telnet セッションがタイムアウトしました。
Voice VLAN			
1	New voice device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface-id：インタフェース ID • mac-address：音声デバイスの MAC アドレス	Informational	インタフェースで音声デバイスが検出されました。
2	<interface-id> add into voice VLAN <vid> **パラメータ説明：** • interface-id：インタフェース ID • vid：VLAN ID	Informational	自動音声 VLAN モードのインタフェースが音声 VLAN に追加されました。
3	<interface-id> remove from voice VLAN <vid> **パラメータ説明：** • interface-id：インタフェース ID • vid：VLAN ID	Informational	インタフェースが音声 VLAN から離脱し、エージング期間内に音声デバイスがインタフェースで検出されませんでした。
WAC			
1	Web-Authentication host login fail(Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <portNum>, VID: <vlanid>) **パラメータ説明：** • string：クライアントがログインを試みたユーザ名 • ipaddr：クライアントの IPv4 アドレス • ipv6address：クライアントの IPv6 アドレス • mac-address：クライアントの MAC アドレス • interface-id：クライアントが接続しているポート番号 • vlan-id：クライアントの通信に関連付けられる VLAN ID	Critical	クライアントホストが認証に失敗しました。
2	Web-Authentication enters stop learning state	Warning	認証ユーザ数が最大値に達しました。
3	Web-Authentication recovered from stop learning state	Warning	認証ユーザ数が最大値を下回りました。
4	Web-Authentication host login success(Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <portNum>, VID: <vlanid>) **パラメータ説明：** • string：クライアントがログインに成功したユーザ名 • ipaddr：クライアントの IPv4 アドレス • ipv6address：クライアントの IPv6 アドレス • mac-address：クライアントの MAC アドレス • interface-id：クライアントが接続しているポート番号 • vlan-id：クライアントの通信に関連付けられる VLAN ID	Informational	クライアントホストが認証に成功しました。
5	Web-Authentication cannot work correctly because ACL rule resource is not available	Alert	ACL ハードウェアリソースが枯渇しています。
Web			
1	Successful login through Web (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：接続ユーザ名 • ipaddr：接続 IP アドレス	Informational	Web 経由でのログインに成功しました。
2	Login failed through Web (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：接続ユーザ名 • ipaddr：接続 IP アドレス	Warning	Web 経由でのログインに失敗しました。

ログの内容		緊急度	イベントの説明
3	Web session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：接続ユーザ名 • ipaddr：接続 IP アドレス	Informational	Web セッションがタイムアウトしました。
4	Logout through Web (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：接続ユーザ名 • ipaddr：接続 IP アドレス	Informational	Web 経由でログアウトしました。
5	Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：接続ユーザ名 • ipaddr：接続 IP アドレス	Informational	Web（SSL）経由でのログインに成功しました。
6	Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：接続ユーザ名 • ipaddr：接続 IP アドレス	Warning	Web（SSL）経由でのログインに失敗しました。
7	Web(SSL) session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：接続ユーザ名 • ipaddr：接続 IP アドレス	Informational	Web（SSL）セッションがタイムアウトしました。
8	Logout through Web(SSL) (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：接続ユーザ名 • ipaddr：接続 IP アドレス	Informational	Web（SSL）経由でログアウトしました。
ZTP			
1	Unit <UnitID> reset button pressed, trigger <Name> function. **パラメータ説明：** • UnitID：ユニット ID • Name：Reboot、ZTP、Factory Reset	Critical	リセット /ZTP ボタンが押下されました。
2	The downloaded firmware was successfully executed by ZTP update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：TFTP サーバの IP アドレス	Informational	ZTP によるファームウェア更新が正常に完了しました。
3	The downloaded firmware was not successfully executed by ZTP update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：TFTP サーバの IP アドレス	Warning	ZTP によるファームウェア更新が失敗しました。

付録 C トラップログエントリ

スイッチのトラップログエントリとその説明を以下に示します。

	トラップ名	説明	OID
802.1X			
1	dDot1xExtLoggedSuccess	ホストが 802.1X 認証に成功したときに送信されます。 （ログインに成功） 関連オブジェクト： • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan • dnaSessionAuthUserName	1.3.6.1.4.1.171.14.30.0.1
2	dDot1xExtLoggedFail	ホストが 802.1X 認証に失敗したときに送信されます。 （ログインに失敗） 関連オブジェクト： • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan • dnaSessionAuthUserName • dDot1xExtNotifyFailReason	1.3.6.1.4.1.171.14.30.0.2
802.3ah OAM			
1	dot3OamThresholdEvent	しきい値を超えるローカル / リモートイベントが検出されました。 関連オブジェクト： • dot3OamEventLogTimestamp • dot3OamEventLogOui • dot3OamEventLogType • dot3OamEventLogLocation • dot3OamEventLogWindowHi • dot3OamEventLogWindowLo • dot3OamEventLogThresholdHi • dot3OamEventLogThresholdLo • dot3OamEventLogValue • dot3OamEventLogRunningTotal • dot3OamEventLogEventTotal	1.3.6.1.2.1.158.0.1
2	dot3OamNonThresholdEvent	しきい値を超えないローカル / リモートイベントが検出されました。 関連オブジェクト： • dot3OamEventLogTimestamp • dot3OamEventLogOui • dot3OamEventLogType • dot3OamEventLogLocation • dot3OamEventLogEventTotal	1.3.6.1.2.1.158.0.2
認証失敗			
1	authenticationFailure	エージェントロールで動作する SNMPv2 エントリが、正しく認証されていないプロトコルメッセージを受信したことを示します。SNMPv2 の実装ではこのトラップを生成できることを規定していますが、このトラップが生成されるかどうかは snmpEnableAuthenTraps オブジェクトにより指定されます。	1.3.6.1.6.3.1.1.5.5
BPDU アタック防止			
1	dBpduProtectionAttackOccur	インタフェースで BPDU アタックが発生したときに送信されます。 関連オブジェクト： • ifIndex • dBpduProtectionIfCfgMode	1.3.6.1.4.1.171.14.47.0.1
2	dBpduProtectionAttackRecover	インタフェースで BPDU アタックが解消したときに送信されます。 関連オブジェクト： • ifIndex	1.3.6.1.4.1.171.14.47.0.2

	トラップ名	説明	OID
CFM			
1	dot1agCfmFaultAlarm	接続に不具合が生じた場合、生成されます。 関連オブジェクト： • dot1agCfmMepHighestPrDefect	1.3.111.2.802.1.1.8.0.1
2	dCfmAisOccurred	ローカル MEP が AIS ステータスになった場合、生成されます。 関連オブジェクト： • dCfmEventMdIndex • dCfmEventMaIndex • dCfmEventMepIdentifier	1.3.6.1.4.1.171.14.86.0.1
3	dCfmAisCleared	ローカル MEP が AIS ステータスから解除された場合、生成されます。 関連オブジェクト： • dCfmEventMdIndex • dCfmEventMaIndex • dCfmEventMepIdentifier	1.3.6.1.4.1.171.14.86.0.2
4	dCfmLockOccurred	ローカル MEP がロックステータスになった場合、生成されます。 関連オブジェクト： • dCfmEventMdIndex • dCfmEventMaIndex • dCfmEventMepIdentifier	1.3.6.1.4.1.171.14.86.0.3
5	dCfmLockCleared	ローカル MEP がロックステータスから解除された場合、生成されます。 関連オブジェクト： • dCfmEventMdIndex • dCfmEventMaIndex • dCfmEventMepIdentifier	1.3.6.1.4.1.171.14.86.0.4
DDM			
1	dDdmAlarmTrap	異常なアラームが発生、または正常な状態に回復した際に通知されます。現在の値 > low warning または現在の値 < high warning になったときにのみリカバトラップを送信します。 関連オブジェクト： • dDdmNotifyInfoIfIndex • dDdmNotifyInfoComponent • dDdmNotifyInfoAbnormalLevel • dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.1
2	dDdmWarningTrap	異常な警告が発生、または正常な状態に回復した際に通知されます。 関連オブジェクト： • dDdmNotifyInfoIfIndex • dDdmNotifyInfoComponent • dDdmNotifyInfoAbnormalLevel • dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.2
DHCP サーバスクリーニング			
1	dDhcpFilterAttackDetected	DHCP サーバスクリーンが有効なとき、スイッチが偽造 DHCP サーバパケットを受信すると、攻撃パケットを受信したイベントをトラップ送信します。 関連オブジェクト： • dDhcpFilterLogBufServerIpAddr • dDhcpFilterLogBufClientMacAddr • dDhcpFilterLogBufferVlanId • dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.171.14.133.0.1
DoS 攻撃防御			
1	dDosPreveAttackDetectedPacket2	DoS アタックを検出したときに送信されます。 関連オブジェクト： • dDoSPrevCtrlAttackType • dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171.14.133.0.1

	トラップ名	説明	OID
ERPS			
1	dErpsFailuredetectedNotif	シグナル不具合が検出された場合に送信されます。	1.3.6.1.4.1.171.14.78.0.1
2	dErpsFailureClearedNotif	シグナル不具合が解消された場合に送信されます。	1.3.6.1.4.1.171.14.78.0.2
3	dErpsRPLOwnerConflictNotif	RPL オーナの競合が検出された場合に送信されます。	1.3.6.1.4.1.171.14.78.0.3
エラー Disable			
1	dErrDisNotifyPortDisabledAssert	ポートがエラー無効状態になった時に送信されます。 関連オブジェクト : • dErrDisNotifyInfoPortIfIndex • dErrDisNotifyInfoLoopDetectedVID • dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.1
2	dErrDisNotifyPortDisabledClear	指定間隔の後、ポートループ再始動時に送信されます。 関連オブジェクト : • dErrDisNotifyInfoPortIfIndex • dErrDisNotifyInfoLoopDetectedVID • dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.2
一般管理			
1	dGenMgmtLoginFail	ユーザがスイッチへのログインに失敗した場合に送信されます。 関連オブジェクト : • dGenMgmtNotifyInfoLoginType • dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171.14.165.0.1
Gratuitous ARP			
1	agentGratuitousARPTrap	IP アドレスが重複していた場合に送信されます。 関連オブジェクト : • ipaddr • macaddr • portNumber • agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.14.75.0.1
IP-MAC ポートバインディング（IMPB）			
1	dImpbViolationTrap	IP-MAC ポートバインディングアドレス違反が検出された際に生成されます。 関連オブジェクト : • ifIndex • dImpbViolationIpAddrType • dImpbViolationIpAddress • dImpbViolationMacAddress • dImpbViolationVlan	1.3.6.1.4.1.171.14.22.0.1
LACP			
1	linkUp	「linkUp」トラップは、エージェントロールで動作している SNMP エンティティにより、コミュニケーションリンクの 1 つにおいて、ifOperStatus が「down」ステートから他のステート（「notPresent」以外）に移行したことを検出した場合に送信されます。移行後のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : • ifIndex • ifAdminStatus • ifOperStatus	1.3.6.1.6.3.1.1.5.4

	トラップ名	説明	OID
2	linkDown	「linkDown」トラップは、エージェントロールで動作している SNMP エンティティにより、コミュニケーションリンクの 1 つにおいて、ifOperStatus が他のステート（「notPresent」以外）から「down」ステートに移行しようとしていることを検出した場合に送信されます。移行前のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト： • ifIndex • ifAdminStatus • ifOperStatus	1.3.6.1.6.3.1.1.5.3
		LBD	
1	dLbdLoopOccurred	インタフェースにループが発生したときに送信されます。 関連オブジェクト： • dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.1
2	dLbdLoopRestart	指定時間後、インタフェースのループが再スタートしたときに送信されます。 関連オブジェクト： • dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.2
3	dLbdVlanLoopOccurred	インタフェースに VID ループが発生したときに送信されます。 関連オブジェクト： • dLbdNotifyInfoIfIndex • dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.3
4	dLbdVlanLoopRestart	指定時間後、VID のインタフェースループが再スタートしたときに送信されます。 関連オブジェクト： • dLbdNotifyInfoIfIndex • dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.4
		LLDP/LLDP-MED	
1	lldpRemTablesChange	「lldpStatsRemTableLastChangeTime」の値が変更された時に送信されます。 関連オブジェクト： • lldpStatsRemTablesInserts • lldpStatsRemTablesDeletes • lldpStatsRemTablesDrops • lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2	lldpXMedTopologyChangeDetected	ローカルデバイスによってトポロジの変更が検知された時に送信されます。 （ローカルポートに新しいリモートデバイスがアタッチされた、またはリモートデバイスがポートから切断 / 移動した場合） 関連オブジェクト： • lldpRemChassisIdSubtype • lldpRemChassisId • lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1
		MAC 認証	
1	dMacAuthLoggedSuccess	MAC ベースのアクセスコントロールホストがログインに成功したときに送信されます。 関連オブジェクト： • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.1

	トラップ名	説明	OID
2	dMacAuthLoggedFail	MAC ベースのアクセスコントロールホストがログインに失敗したときに送信されます。 関連オブジェクト : • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.2
3	dMacAuthLoggedAgesOut	MAC ベースのアクセスコントロールホストがエージングアウトしたときに送信されます。 関連オブジェクト : • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.3
	MAC 通知		
1	swL2macNotification	本トラップはアドレステーブルの MAC アドレスに変更が生じたことを意味します。 関連オブジェクト : • swL2macNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
2	dL2FdbMacNotificationWithVID	本トラップはアドレステーブルの MAC アドレス（VLAN ID）に変更が生じたことを意味します。 関連オブジェクト : • dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.171.14.3.0.2
	MSTP		
1	newRoot	newRoot トラップは、送信側のエージェントがスパニングツリーの新しいルートになったことを示します。トラップは、新しいルートとして選出された後（Topology Change Timer の期限切れなどに伴い）すぐにブリッジによって送信されます。 本トラップの実装はオプションです。	1.3.6.1.2.1.17.0.1
2	topologyChange	topologyChange トラップは、いずれかの構成ポートが Learning 状態から Forwarding 状態に、または Forwarding 状態から Blocking 状態に遷移する場合にブリッジによって送信されます。同様の変更に対して newRoot トラップが送信される場合には、本トラップは送信されません。 本トラップの実装はオプションです。	1.3.6.1.2.1.17.0.2
	周辺機器		
1	dEntityExtFanStatusChg	ファン状態の変更通知 （ファンの不具合（「dEntityExtEnvFanStatus」が「fault」）または回復（「dEntityExtEnvFanStatus」が「ok」）） 関連オブジェクト : • dEntityExtEnvFanUnitId • dEntityExtEnvFanIndex • dEntityExtEnvFanStatus	1.3.6.1.4.1.171.14.5.0.1
2	dEntityExtThermalStatusChg	温度状態の変更通知 （温度警告（「dEntityExtEnvTempStatus」が「abnormal」）または回復（「dEntityExtEnvTempStatus」が「ok」）） 関連オブジェクト : • dEntityExtEnvTempUnitId • dEntityExtEnvTempIndex • dEntityExtEnvTempStatus	1.3.6.1.4.1.171.14.5.0.2
3	dEntityExtPowerStatusChg	電力状態の変更通知（電源モジュールの不具合、不具合からの回復、または取り外し） 関連オブジェクト : • dEntityExtEnvPowerUnitId • dEntityExtEnvPowerIndex • dEntityExtEnvPowerStatus	1.3.6.1.4.1.171.14.5.0.3

	トラップ名	説明	OID
PoE			
1	pethMainPowerUsageOnNotification	使用率が PSE しきい値に到達した事を示しています。同じオブジェクトインスタンスによって通知が発行されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : • pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
2	pethMainPowerUsageOffNotification	使用率が PSE しきい値を下回った事を示しています。同じオブジェクトインスタンスによって通知が発行されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : • pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
3	dPoeIfPowerDeniedNotification	PSE 状況ダイアグラムが POWER_DENIED になった事を示す通知です。同じオブジェクトインスタンスによって通知が発行されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : • pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171.14.24.0.1
4	dPoeIfPowerOverLoadNotification	PSE 状況ダイアグラムが ERROR_DELAY_OVER になった事を示すトラップです。同じオブジェクトインスタンスによって通知が発行されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : • pethPsePortOverLoadCounter	1.3.6.1.4.1.171.14.24.0.2
5	dPoeIfPowerShortCircuitNotification	PSE 状況ダイアグラムが ERROR_DELAY_SHORT になった事を示すトラップです。同じオブジェクトインスタンスによって通知が発行されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : • pethPsePortShortCounter	1.3.6.1.4.1.171.14.24.0.3
6	dPoeIfPdAliveFailOccurNotification	PD が動作を中止、回答不能になった事を示すトラップです。同じオブジェクトインスタンスによって通知が発行されるまで最低 500 ミリ秒が経過する必要があります。	1.3.6.1.4.1.171.14.24.0.4
ポート			
1	linkUp	ポートがリンクアップしたときに生成されます。 関連オブジェクト : • ifIndex • ifAdminStatus • ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	ポートがリンクダウンしたときに生成されます。 関連オブジェクト : • ifIndex • ifAdminStatus • ifOperStatus	1.3.6.1.6.3.1.1.5.3
ポートセキュリティ			
1	dPortSecMacAddrViolation	事前定義されたポートセキュリティ設定に違反する新しい MAC アドレスがトリガとなり送信されるトラップメッセージです。 関連オブジェクト : • ifIndex • dPortSecIfCurrentStatus • dPortSecIfLastMacAddress	1.3.6.1.4.1.171.14.8.0.1
再起動スケジュール			
1	agentRebootIn5Min	再起動までのカウントダウンが 5 分になると、本トラップが送信されます。	1.3.6.1.4.1.171.14.183.0.1
2	agentRebootIn1Min	再起動までのカウントダウンが 1 分になると、本トラップが送信されます。	1.3.6.1.4.1.171.14.183.0.2

	トラップ名	説明	OID
RMON			
1	risingAlarm	SNMP トラップは、アラームエントリが上昇しきい値超える時に生成され、SNMP トラップの送信に設定されたイベントを生成します。 関連オブジェクト : • alarmIndex • alarmVariable • alarmSampleType • alarmValue • alarmRisingThreshold	1.3.6.1.2.1.16.0.1
2	fallingAlarm	SNMP トラップは、アラームエントリが下降しきい値を下回るときに生成され、SNMP トラップの送信に設定されたイベントを生成します。 関連オブジェクト : • alarmIndex • alarmVariable • alarmSampleType • alarmValue • alarmFallingThreshold	1.3.6.1.2.1.16.0.2
セーフガードエンジン			
1	dSafeguardChgToExhausted	システムが動作モードをノーマルから exhausted に変更したことを示します。 関連オブジェクト : • dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.1
2	dSafeguardChgToNormal	システムが動作モードを exhausted からノーマルに変更したことを示します。 関連オブジェクト : • dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.2
SIM			
1	swSingleIPMSColdStart	コマンダースイッチはメンバが cold start 通知を生成するときにこの通知を送信します。 関連オブジェクト : • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.11
2	swSingleIPMSWarmStart	コマンダースイッチはメンバが warm start 通知を生成するときにこの通知を送信します。 関連オブジェクト : • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.12
3	swSingleIPMSLinkDown	コマンダースイッチはメンバがリンクダウン通知を生成するときにこの通知を送信します。 関連オブジェクト : • swSingleIPMSID • swSingleIPMSMacAddr • ifIndex	1.3.6.1.4.1.171.12.8.6.0.13
4	swSingleIPMSLinkUp	コマンダースイッチはメンバがリンクアップ通知を生成するときにこの通知を送信します。 関連オブジェクト : • swSingleIPMSID • swSingleIPMSMacAddr • ifIndex	1.3.6.1.4.1.171.12.8.6.0.14
5	swSingleIPMSAuthFail	コマンダースイッチはメンバが認証失敗の通知を生成するときにこの通知を送信します。 関連オブジェクト : • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.15

	トラップ名	説明	OID
6	swSingleIPMSnewRoot	コマンダースイッチはメンバが新しいルートの通知を生成するときにこの通知を送信します。 関連オブジェクト： • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.16
7	swSingleIPMSTopologyChange	コマンダースイッチはメンバがトポロジ変更の通知を生成するときにこの通知を送信します。 関連オブジェクト： • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.17
	スタック		
1	dStackInsertNotification	ユニットのホットインサート（活線挿入）の通知です。 関連オブジェクト： • dStackNotifyInfoBoxId • dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.1
2	dStackRemoveNotification	ユニットのホットリムーブ（活線抜出）の通知です。 関連オブジェクト： • dStackNotifyInfoBoxId • dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.2
3	dStackFailureNotification	ユニットのスタック失敗の通知です。 関連オブジェクト： • dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.3
4	dStackTPChangeNotification	スタックトポロジ変更の通知です。 関連オブジェクト： • dStackNotifyInfoTopologyType • dStackNotifyInfoBoxId • dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.4
5	dStackRoleChangeNotification	スタックユニットロール変更の通知です。 関連オブジェクト： • dStackNotifyInfoRoleChangeType • dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.5
	Start		
1	coldStart	coldStart トラップは、エージェントロールで動作する SNMPv2 エンティティが、自身を再初期化したことを示します。設定が変更された可能性があります。	1.3.6.1.6.3.1.1.5.1
2	warmStart	warmStart トラップは、エージェントロールで動作する SNMPv2 エンティティが、自身を再初期化したことを示します。設定は変更されません。	1.3.6.1.6.3.1.1.5.2
	ストーム制御		
1	dStormCtrlOccurred	「dStormCtrlNotifyEnable」が "stormOccurred" または "both" で、ストームが検出されたときに送信されます。 関連オブジェクト： • ifIndex • dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.1
2	dStormCtrlStormCleared	「dStormCtrlNotifyEnable」が "stormCleared" または "both" で、ストームがクリアされたときに送信されます。 関連オブジェクト： • ifIndex • dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.2
	システムファイル		
1	dsfUploadImage	イメージファイルのアップロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.1
2	dsfDownloadImage	イメージファイルのダウンロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.2
3	dsfUploadCfg	コンフィグレーションファイルのアップロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.3

	トラップ名	説明	OID
4	dsfDownloadCfg	コンフィグレーションファイルのダウンロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.4
5	dsfSaveCfg	コンフィグレーションファイルの保存に成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.5
		Web 認証	
1	dWebAuthLoggedSuccess	ホストが Web 認証でログインに成功した場合に送信されます。 関連オブジェクト : • ifIndex • dnaSessionAuthVlan • dnaSessionClientMacAddress • dnaSessionClientAddrType • dnaSessionClientAddress • dnaSessionAuthUserName	1.3.6.1.4.1.171.14.154.0.1
2	dWebAuthLoggedFail	ホストが Web 認証でログインに失敗した場合に送信されます。 関連オブジェクト : • ifIndex • dnaSessionAuthVlan • dnaSessionClientMacAddress • dnaSessionClientAddrType • dnaSessionClientAddress • dnaSessionAuthUserName	1.3.6.1.4.1.171.14.154.0.2
		ZTP	
1	swResetButtonPressedTrap	リセット /ZTP ボタンが押下されたときに送信されます。 関連オブジェクト : • Unit ID • swResetButtonMode	1.3.6.1.4.1.171.12.120.2.0.1

付録 D RADIUS 属性割り当て

本スイッチでは次のモジュールに対し、RADIUS 属性割り当てが使用されます。
- 「コンソール」「Telnet」「SSH」「Web」「802.1X」「MAC ベースアクセスコントロール」「WAC」

以下の RADIUS 属性割り当てタイプについて説明します。
- 特権レベル
- イングレス / イーグレス帯域幅
- 802.1p デフォルトプライオリティ
- VLAN
- ACL

■ 特権レベル

RADIUS サーバで特権レベルを割り当てるには、適切なパラメータが RADIUS サーバで設定されている必要があります。特権レベルのパラメータは以下の通りです。

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	1	必須
Attribute-Specific Field	スイッチを操作するユーザの特権レベルの割り当てに使用します。	範囲（1-15）	必須

ユーザが RADIUS サーバの特権レベル属性（例えば、レベル 15）を設定し、コンソール、Telnet、SSH、Web 認証が成功した場合、デバイスは、このアクセスユーザに（RADIUS サーバに基づく）特権レベルを割り当てます。ユーザが特権レベル属性を設定せず、認証に成功した場合、デバイスはアクセスユーザに特権レベルを割り当てません。特権レベルがサポートされる最小値よりも小さい場合、または最大値よりも大きい場合、特権レベルは無視されます。

■ イングレス / イーグレス帯域幅

RADIUS サーバにより Ingress/Egress 帯域を割り当てるには、適切なパラメータが RADIUS サーバに設定されている必要があります。帯域幅のパラメータは以下の通りです。

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	2（イングレス帯域幅） 3（イーグレス帯域幅）	必須
Attribute-Specific Field	ポートの帯域幅の割り当てに使用します。	単位 (Kbits)	必須

ユーザが RADIUS サーバの帯域属性（例えば、イングレス帯域 1000Kbps）を設定し、802.1X 認証に成功した場合、デバイスはポートへ（RADIUS サーバに基づく）帯域を割り当てます。ユーザが帯域属性を設定せず、認証に成功した場合、デバイスはポートに帯域を割り当てません。RADIUS サーバ上で帯域属性が "0" の値で設定されている場合、実効的な帯域は、"no_limited" に設定されます、また、帯域が "0" より小さい場合、またはサポートされる最大値よりも大きい場合、帯域は無視されます。

■ 802.1p デフォルトプライオリティ

RADIUS サーバにより 802.1p デフォルトプライオリティを割り当てるには、適切なパラメータが RADIUS サーバに設定されている必要があります。802.1p デフォルトプライオリティのパラメータは以下の通りです。

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	4	必須
Attribute-Specific Field	802.1p デフォルトプライオリティの割り当てに使用します。	0-7	必須

ユーザが RADIUS サーバの 802.1p プライオリティ属性（例えば、優先度 7）を設定し、802.1X 認証や MAC ベース認証に成功した場合、デバイスはポートに（RADIUS サーバに基づく）802.1p デフォルトプライオリティを割り当てます。ユーザがプライオリティ属性を設定せず、認証が成功した場合、デバイスはこのポートにプライオリティを割り当てません。RADIUS サーバで設定されたプライオリティ属性が、範囲外の値（7 よりも大きい値）である場合、デバイスに設定しません。

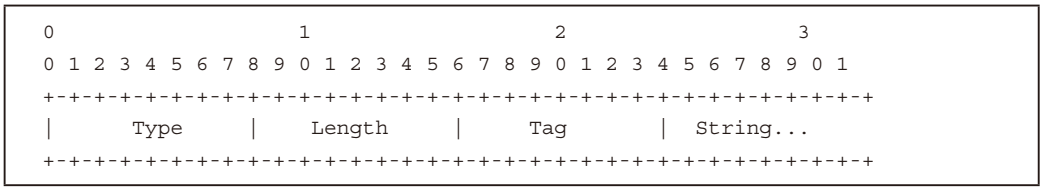
■ VLAN

RADIUS サーバにより VLAN を割り当てるには、適切なパラメータが RADIUS サーバに設定されている必要があります。VLAN 割り当てを使用するために、RADIUS パケット内の以下のトンネル属性が RFC3580 により定義されています。

VLAN のパラメータ

RADIUS トンネル属性	説明	値	使用法
Tunnel-Type	この属性は、（トンネルイニシエータの場合）使用されるトンネリングプロトコル、もしくは、（トンネルターミネータの場合）使用中のトンネリングプロトコルを示します。	13 (VLAN)	必須
Tunnel-Medium-Type	使用されるトランスポートミディアムタイプ	6（802）	必須
Tunnel-Private-Group-ID	特定のトンネルセッションのグループ ID	String 値（VID）	必須

トンネルプライベートグループ ID 属性形式の概要



タグフィールドの定義（RFC 2868 と異なる）

タグフィールド値	文字列のフィールド形式
0x01	VLAN 名（ASCII）
0x02	VLAN ID（ASCII）
その他 (0x00, 0x03 ~ 0x1F, >0x1F)	スイッチが VLAN 設定の文字列を受信すると、最初に VLAN ID と認識します。つまり、スイッチはすべての既存 VLAN ID を確認し、一致するものがあるかどうかを確認します。一致するものを検出できた場合はその VLAN に移動し、検出できなかった場合は VLAN 設定文字列を VLAN 名と判断し、一致する VLAN 名を検出します。

注意 0x1F より大きなタグフィールドは次に続くフィールドの初めのオクテットとして判断されます。

ユーザが RADIUS サーバの VLAN 属性（VID3 など）を設定し、802.1X、MAC ベースアクセスコントロール、または WAC 認証に成功した場合、ポートは VLAN3 が割り当てられます。ユーザが VLAN 属性を設定していない場合、ポートがゲスト VLAN メンバではないときは、現在の認証 VLAN にとどまり、ポートがゲスト VLAN メンバであるときは、元々の VLAN に割り当てられます。

■ ACL

RADIUS サーバで ACL を割り当てるには、2 種類の適切なパラメータが RADIUS サーバで設定されている必要があります。ACL のパラメータは以下の通りです。

● VSA14 ACL Script

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	14 (ACL スクリプト)	必須
Attribute-Specific Field	ACL スクリプトの割り当てに使用します。形式は Access Control List (ACL) コマンドに基づきます。	ACL スクリプト 例： ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;	必須

ユーザが RADIUS サーバの ACL 属性を設定（例：ACL スクリプト：ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;）し、802.1X、MAC ベースアクセスコントロール、または WAC に成功した場合、デバイスは RADIUS サーバによる ACL スクリプトを割り当てます。アクセスリストコンフィグモードへの移行 / 終了は対になっている必要があります。そのように設定されていない場合、ACL スクリプトは拒否されます。

● NAS-Filter-Rule (92)

NAS-Filter-Rule パラメータ

ベンダ指定属性	説明	値	使用法
NAS-Filter-Rule	この属性は、ユーザに適用されるフィルタ規則を示します。	文字列（個々のフィルタルールを連結し、NULL（0x00）オクテットで区切る）	必須

フィルタルールフォーマット

permit コマンドを使用して許可エントリを追加、deny コマンドを使用して拒否エントリを追加します。

```
{permit | deny} in tcp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR} [TCP-PORT-RANGE]
{permit | deny} in udp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR} [UDP-PORT-RANGE]
{permit | deny} in icmp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR} [ICMP-TYPE]
{permit | deny} in ip from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR}
{permit | deny} in IP-PROT-VALUE from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR}
```

パラメータ

パラメータ	説明
in	Ingress トラフィックを指定します。
tcp, udp, icmp, ip, IP-PROT-VALUE	TCP、UDP、ICMP、IP またはユーザ定義のプロトコル値のフィルタルールを指定します。 IP-PROT-VALUE は 0 ～ 255 の範囲で指定します。
any	送信元 IP アドレスまたは宛先 IP アドレスとして「すべて（any）」を指定します。
DST-IP-ADDR	宛先ホストの IP アドレスを指定します。
DST-IP-NET-ADDR	1.2.3.4/24 の形式で宛先 IP アドレスのグループを指定します。
DST-IPV6-ADDR	宛先ホストの IPv6 アドレスを指定します。
DST-IPV6-NET-ADDR	2000::1/64 の形式で宛先 IPv6 ネットワークのグループを指定します。
TCP-PORT-RANGE	（オプション）TCP ポートまたはポート範囲を指定します。（例：22-23、80）
UDP-PORT-RANGE	（オプション）UDP ポートまたはポート範囲を指定します。（例：22-23、80）
ICMP-TYPE	（オプション）ICMP メッセージタイプを指定します。メッセージタイプの有効な番号は 0 ～ 255 です。

例：

この例は、RADIUS サーバでホストの Telnet サービスを拒否する方法を示しています。

```
Nas-filter-Rule="deny in tcp from any to any 23"
Nas-filter-Rule+="permit in ip from any to any"
```

この例は、RADIUS サーバ上で、ホストからのアクセスを特定の IP アドレスのグループに制限する方法を示しています。

```
Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"
```

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダを定義します。	171 (DLINK)	必須
Vendor-Type	属性を定義します。	24	必須
Attribute-Specific Field	IPv6 フィルタルール。 IPv6 アドレス関連の入力を受け入れるために使用されます。	この属性は、NAS-Filter-Rule の次の IP モードのいずれかを示します。 1=IPv4 および IPv6 トラフィックを転送 2=IPv4 トラフィックのみ転送（IPv6 トラフィックは破棄） この属性が RADIUS サーバによって割り当てられていない場合、IPv4 トラフィックのみを転送し、IPv6 パケットは破棄されます。	必須

注意 ベンダ定義の ACL スクリプト（VSA14）と標準の NAS-Filter-Rule（92）の両方が同時に割り当てられている場合、NAS-Filter-Rule（92）が有効になり、VSA14 は無視されます。

付録 E IETF RADIUS 属性サポート

リモート認証ダイヤルインユーザサービス（RADIUS）属性を使用すると、リクエストや応答の中で認証、承認、情報、設定詳細などをやり取りすることができます。

本付録では、スイッチによりサポートされる RADIUS 属性一覧を記載しています。

RADIUS 属性は、IETF 規格やベンダ特定属性（VSA) によりサポートされます。VSA により、ベンダは固有の RADIUS 属性を定義することができます。D-Link VSA についての詳しい情報は、「付録 D RADIUS 属性割り当て」を参照してください。

IETF 規格 RADIUS 属性は、RFC 2865 リモート認証ダイヤルインユーザサービス（RADIUS)、RFC 2866 RADIUS アカウンティング、RFC 2868 トンネルプロトコルに対する RADIUS 属性、RFC 2869 RADIUS 拡張で定義されています。

以下のリストは、本スイッチでサポートされている IETF RADIUS 属性です。

RADIUS 認証属性

ナンバー	IETF 属性
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

RADIUS アカウンティング属性

ナンバー	IETF 属性
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

付録 F 機能設定例

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

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

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DGS-1530

Traffic Segmentation（トラフィックセグメンテーション）

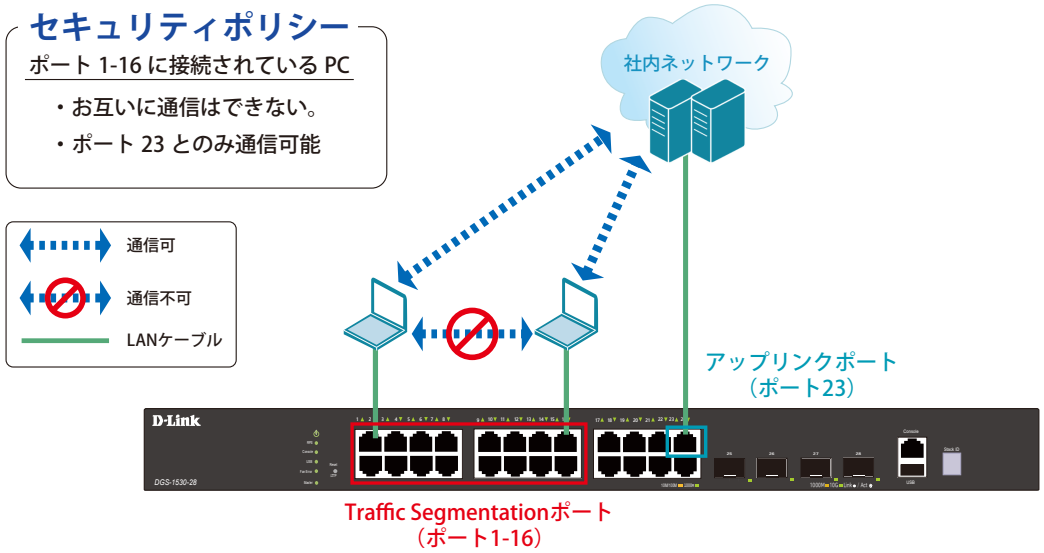


図 17-1　Traffic Segmentation（DGS-1530-28）

概要

ポート 1 ～ 16 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 ～ 16 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 ～ 16 は、アップリンクポートとして使用するポート 23 とのみ通信ができるようにします。

設定手順

1. ポート（1-16）のトラフィックセグメンテーション設定を行います。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#traffic-segmentation forward interface ethernet 1/0/23
Switch(config-if-range)#end
```

2. 情報確認

```
Switch#show traffic-segmentation forward
```

注意　本機能を利用する場合、送信先 MAC アドレスが不明な Unknown ユニキャストについて、スイッチの全ポートにフラッドされます。

3. 設定を保存します。

```
Switch#copy running-config startup-config
```

VLAN

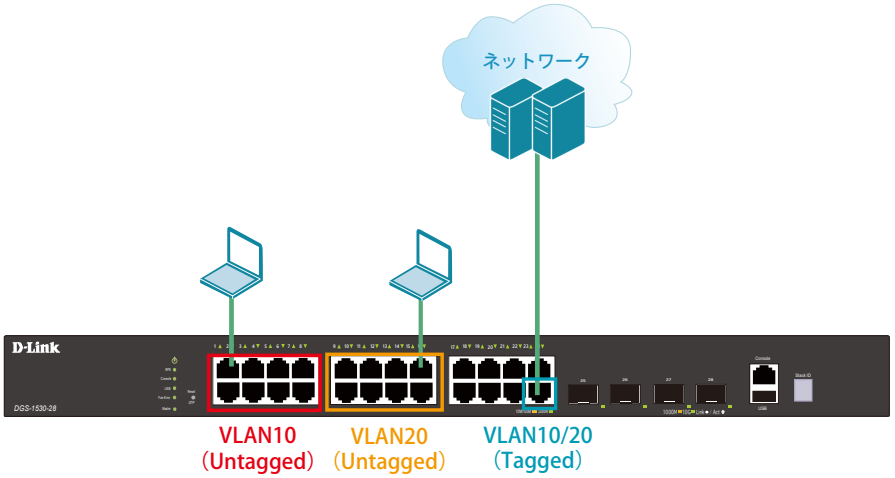


図 17-2　VLAN（DGS-1530-28）

概要

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

設定手順

1. VLAN10、VLAN20 を作成します。

```
Switch#configure terminal
Switch(config)#vlan 10,20
Switch(config-vlan)#exit
```

2. ポート 1-8 に VLAN10、ポート 9-16 に VLAN20 を 割り当てます。

```
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit

Switch(config)#interface range ethernet 1/0/9-16
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#end
```

3. 上位のネットワークへ接続されているポート 24 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。

■設定方法①（hybrid mode を設定する場合）

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add tagged 10,20
Switch(config-if)#end
```

■設定方法②（hybrid mode を使用せず、trunk にて同様の設定を行う場合）

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10,20
Switch(config-if)#end
```

4. 設定を保存します。

```
Switch#copy running-config startup-config
```

5. 情報確認

```
Switch#show vlan
```

（作成した VLAN と各ポートに割り当てられている VLAN が表示されます。）

```
Switch#show vlan int ethernet 1/0/xx
```

（ポートに紐づいている VLAN 情報が表示されます。）

Link Aggregation（リンクアグリゲーション）

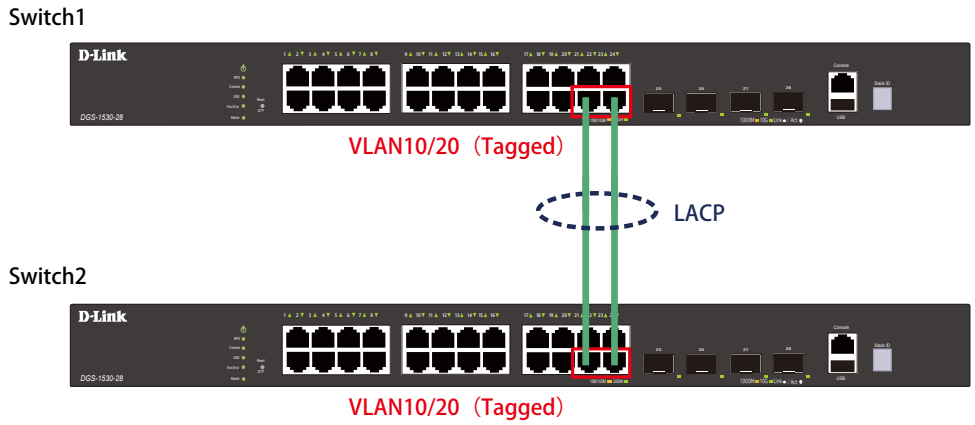


図 17-3　Link Aggregation（DGS-1530-28）

概要

VLAN10 と 20 の Tagged VLAN を設定したポートにリンクアグリゲーションを設定します。ポート 22 と 24 に VLAN10 と VLAN20 を「Tagged」で割り当て、ポート 22 と 24 をグループ 1 として LACP によるリンクアグリゲーションに設定します。

設定手順（Switch1、Switch2 共通）

1. VLAN10、VLAN20 を作成します。

```
Switch#configure terminal
Switch(config)#vlan 10,20
Switch(config-vlan)#exit
```

2. Link Aggregation（LACP）のグループを作成します。

```
Switch(config)#interface ethernet 1/0/22
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
```

3. 作成した port-channel に VLAN を設定します。
LAG ポートに設定する VLAN は、各物理インタフェース上では設定せず、Port-channel インタフェース上で VLAN の設定を行います。

```
Switch(config)#interface port-channel 1
Switch(config if)#switchport mode trunk
Switch(config if)#switchport trunk native vlan 1
Switch(config if)#switchport trunk allowed vlan 1,10,20
Switch(config if)#exit
Switch(config)#exit
```

4. 設定を保存します。

```
Switch#copy running-config startup-config
```

5. 情報確認
   - Port-channel に設定されている VLAN 情報を表示します。

```
Switch#show vlan interface port-channel 1
```

   - グループ番号とグループで使用されている Protocol を表示します。

```
Switch#show channel-group
```

   - 各グループに所属している Port 番号と、リンクアグリゲーションの状態を表示します。

```
Switch#show channel-group channel 1 detail
```

Access List（アクセスリスト）

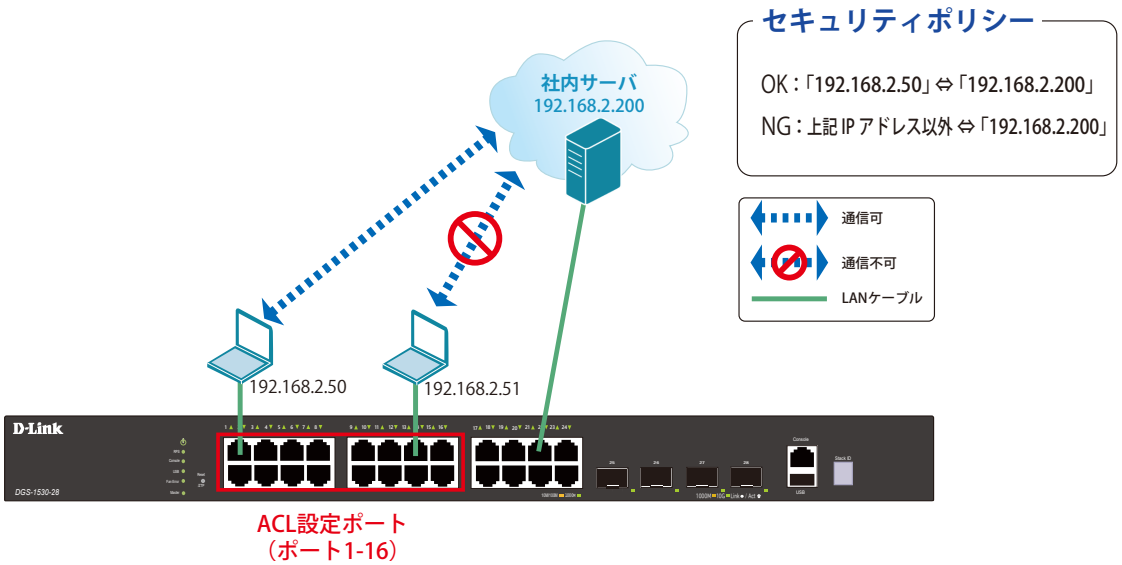


図 17-4　Access List（DGS-1530-28）

概要

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

設定手順

1. アクセスリストに名前（extended ACL）を付けて定義します。
「192.168.2.50 ⇔ 192.168.2.200」間の通信を許可するルールを追加します。
「192.168.2.200」へのすべての通信を拒否するルールを追加します。

```
Switch#configure terminal
Switch(config)#ip access-list extended ACL
Switch(config-ip-ext-acl)#permit 192.168.2.50 0.0.0.0 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#deny any 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#end
```

2. アクセスリストのルールを、適用対象ポート 1 ～ 16 へ設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#ip access-group ACL in
Switch(config-if-range)#end
```

3. 設定を保存します。

```
Switch#copy running-config startup-config
```

4. 情報確認

```
Switch#show access-list
Switch#show access-list ip
Switch#show access-group
```

Loopback Detection（LBD）（ループ検知）

ループを検知したPortをシャットダウンします。
（ポート1-8）

図 17-5　Loopback Detection（DGS-1530-28）

概要

ポート 1~8 に対しループバック検知を設定します。ポート 1~8 でループを検知した際、ポートをシャットダウンするように設定します。

設定手順

1. ポートベースでループ検知機能を動作させ、ループ検知後はポートをシャットダウンする設定をします。

```
Switch#configure terminal
Switch(config)#loopback-detection
Switch(config)#loopback-detection mode port-based
```

2. ループ発生を確認する間隔を 20 秒に設定します。

```
Switch(config)#loopback-detection interval 20
```

3. （必要に応じて）ループ発生後のループ解消確認間隔を 20 秒に設定し、ループ解消確認後、自動で Port 開放するように設定します。

```
Switch(config)#errdisable recovery cause loopback-detect interval 20
```

注意 この設定をしない場合、永続的にポートが「shutdown」状態となります。ポートを開放する場合、該当のポートに対し、インタフェースモードにて「no shutdown」コマンドを投入する必要があります。

4. ポート 1-8 でループバック検知機能を有効にします。

```
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#loopback-detection
Switch(config-if-range)#end
```

注意 「spanning-tree」が「enable」になっている場合、ループ検知機能を設定できないため、設定するインタフェースの「spanning-tree」の設定をまず「disable」にします。

5. show コマンドで「Spanning Tree」が無効になっているかを確認します。

```
Switch#show spanning-tree configuration interface ethernet 1/0/1-8
```

6. 「Spanning Tree」がポート単位で「disable」に設定されている場合、ステータスが Disabled と表示されます。

```
Spanning tree state : Disabled
```

7. 設定を保存します。

```
Switch#copy running-config startup-config
```

8. 情報確認

```
Switch#show loopback-detection
```

（ループ検知の有効 / 無効、各ポートのループ状態等を表示します。）

```
Switch#show errdisable recovery
```

（ループ解消後の自動ポート解放設定の有効 / 無効、確認間隔を表示します。）