D-Link DGS-3130 シリーズ

Gigabit Stackable Layer 2 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

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

ご使用上の注意

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

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

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

ラック搭載型製品に関する一般的な注意事項

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

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

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

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

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

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

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

バッテリの取り扱いについて

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

安全にお使いいただくために

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

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

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

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

目次

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

はじめに 14

本マニュアルの対象者 15
表記規則について 15
製品名 / 品番一覧 15

第 1 章　本製品のご使用にあたって 16

DGS-3130 シリーズについて 16
ポート 17
前面パネル 18
背面パネル 20
側面パネル 21
LED 表示 22

第 2 章　スイッチの設置 25

パッケージの内容 25
ネットワーク接続前の準備 25
ゴム足の取り付け (19 インチラックに設置しない場合) 26
19 インチラックへの取り付け 26
SFP/SFP+ ポートへのモジュールの取り付け 27
電源抜け防止クリップの装着 27
リダンダント電源システムの設置 30
DPS-500A 30
DPS-700 31
DPS-800 32
電源の投入 32
電源の異常 32

第 3 章　スイッチの接続 33

エンドノードと接続する 33
ハブまたはスイッチと接続する 33
バックボーンまたはサーバと接続する 34
スタック接続について 35
スタッキングコスト 35
Duplex Chain 構成例 36
Duplex Ring 構成例 38

第 4 章　スイッチの管理について 40

スイッチの管理方法 40
Web GUI による管理 40
SNMP による管理 40
CLI による管理 40
コンソールポートへの接続 41
端末をコンソールポートに接続する 41
ユーザアカウント / パスワードの設定 41
IP アドレスの設定 42
管理（MGMT）ポートへの接続 42
SNMP（SNMP 設定） 43
トラップ 43
MIB 43

第 5 章　Web ベースのスイッチ管理 44

Web ベースの管理について 44
Web GUI へのログイン 44
Web GUI の画面構成 45
Web GUI のメイン画面について 45
Web GUI のメニュー構成 46

第 6 章　System（スイッチの主な設定）　50

Device Information（デバイス情報）....51
System Information Settings（システム情報設定 ）....52
Peripheral Settings（環境設定）....52
Port Configuration（ポート設定）....53
Port Settings（スイッチのポート設定）....53
Port Status（ポートステータス）....55
Port GBIC....55
Port Auto Negotiation（オートネゴシエーション）....56
Error Disable Settings（エラーによるポートの無効）....56
Jumbo Frame（ジャンボフレームの有効化）....57
PoE（PoE の管理）（DGS-3130-30PS/54PS）....58
PoE System（PoE システム設定）....58
PoE Status（PoE ステータス）....59
PoE Configuration（PoE ポート設定）....60
PoE Statistics（PoE 統計）....61
PoE Measurement（PoE 測定）....61
PD Alive（PD アライブ設定）....62
System Log（システムログ構成）....63
System Log Settings（システムログ設定）....63
System Log Discriminator Settings（システムログディスクリミネータ設定）....64
System Log Server Settings（システムログサーバの設定）....65
System Log（Syslog ログ）....66
System Attack Log（システムアタックログ）....66
Time and SNTP（時刻設定）....67
Clock Settings（時間設定）....67
Time Zone Settings（タイムゾーン設定）....68
SNTP Settings（SNTP 設定）....69
Time Range（タイムレンジ設定）....70

第 7 章　Management（スイッチの管理）　71

Command Logging（コマンドログ設定）....72
User Accounts Settings（ユーザアカウント設定）....72
Password Encryption（パスワード暗号化）....73
Password Recovery（パスワードリカバリ）....74
Login Method（ログイン方法）....74
SNMP（SNMP 設定）....76
トラップ....76
MIB....76
SNMP Global Settings（SNMP グローバル設定）....77
SNMP Linkchange Traps Settings（SNMP リンクチェンジトラップ設定）....78
SNMP View Table Settings（SNMP ビューテーブル）....78
SNMP Community Table Settings（SNMP コミュニティテーブル設定）....79
SNMP Group Table Settings（SNMP グループテーブル）....80
SNMP Engine ID Local Settings（SNMP エンジン ID ローカル設定）....81
SNMP User Table Settings（SNMP ユーザテーブル設定）....81
SNMP Host Table Settings（SNMP ホストテーブル設定）....82
SNMP Context Mapping Settings（SNMP ホストテーブル設定）....83
RMON（RMON 設定）....83
RMON Global Settings（RMON グローバル設定）....83
RMON Statistics Settings（RMON 統計情報）....84
RMON History Settings（RMON ヒストリ設定）....84
RMON Alarm Settings（RMON アラーム設定）....85
RMON Event Settings（RMON イベント設定）....86
Telnet/Web（Telnet/Web 設定）....87
Session Timeout（セッションタイムアウト）....88
DHCP（DHCP 設定）....88
Service DHCP（DHCP サービス）....88
DHCP Class Settings（DHCP クラス設定）....89
DHCP Server（DHCP サーバ）....90
DHCPv6 Server（DHCPv6 サーバ設定）....96
DHCP Relay（DHCP リレー）....99
DHCPv6 Relay（DHCPv6 リレー）....104
DHCP Auto Configuration（DHCP 自動コンフィグ設定）....107

DNS（ドメインネームシステム）.....108
DNS Global Settings（DNS グローバル設定）.....108
DNS Name Server Settings（DNS ネームサーバ設定）.....108
DNS Host Settings（DNS ホスト名設定）.....109
IP Source Interface（IP ソースインタフェース）.....109
File System（ファイルシステム設定）.....110
Stacking（スタッキング設定）.....112
Physical Stacking（物理スタッキング）.....114
Stacking Bandwidth（スタッキング帯域）.....115
Virtual Stacking (SIM)（仮想スタック設定（SIM））.....116
シングル IP マネジメント（SIM）の概要.....116
Single IP Settings（シングル IP 設定）.....117
Topology（トポロジ）.....118
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）.....123
SMTP Settings（SMTP 設定）.....124
Reboot Schedule Settings（再起動スケジュール設定）.....125
PPPoE Circuit ID Insertion Global Settings（PPPoE Circuit ID 挿入設定）.....126
SD Card Management（SD カード管理）.....126
SD Card Backup Settings（SD カードへのバックアップ設定）.....126
SD Card Execute Settings（SD カード実行設定）.....127

第 8 章　L2 Features（L2 機能の設定）　128

FDB（FDB 設定）.....129
Static FDB（スタティック FDB の設定）.....129
MAC Address Table Settings（MAC アドレステーブル設定）.....130
MAC Address Table（MAC アドレステーブル）.....131
MAC Notification（MAC 通知）.....132
VLAN（VLAN 設定）.....133
802.1Q VLAN（802.1Q VLAN）.....133
802.1v Protocol VLAN（802.1v プロトコル VLAN）.....134
GVRP（GVRP の設定）.....135
Asymmetric VLAN（Asymmetric VLAN 設定）.....137
MAC VLAN（MAC VLAN 設定）.....138
VLAN Interface（VLAN インタフェース設定）.....138
Super VLAN（Super VLAN 設定）.....143
Auto Surveillance VLAN（自動サーベイランス VLAN）.....144
Voice VLAN（音声 VLAN）.....146
Private VLAN（プライベート VLAN 設定）.....149
VLAN Tunnel（VLAN トンネル）.....150
Dot1q Tunnel（Dot1q トンネル）.....150
VLAN Mapping（VLAN マッピング）.....152
VLAN Mapping Profile（VLAN マッピングプロファイル）.....153
STP（スパニングツリー設定）.....158
802.1Q-2005 MSTP.....158
802.1D-2004 Rapid STP.....158
ポートの状態遷移.....158
STP Global Settings（STP グローバル設定）.....159
STP Port Settings（STP ポートの設定）.....161
MST Configuration Identification（MST の設定）.....162
STP Instance（STP インタンス設定）.....163
MSTP Port Information（MSTP ポート情報）.....163
ERPS (G.8032)（イーサネットリングプロテクション設定）.....164
ERPS 164
ERPS Profile（ERPS プロファイル）.....168
Loopback Detection（ループバック検知設定）.....169
Link Aggregation（リンクアグリゲーション）.....170
ポートトランクグループについて.....170
L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）.....173
L2 Multicast Control（L2 マルチキャストコントロール）.....174
IGMP Snooping（IGMP Snooping の設定）.....174
MLD Snooping（MLD スヌーピング）.....180
Multicast VLAN（マルチキャスト VLAN）.....185
Multicast Filtering（マルチキャストフィルタリング）.....188

LLDP 189
LLDP Global Settings（LLDP グローバル設定） 189
LLDP Port Settings（LLDP ポート設定） 190
LLDP Management Address List（LLDP 管理アドレスリスト） 191
LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定） 191
LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定） 192
LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定） 192
LLDP-MED Port Settings（LLDP-MED ポート設定） 193
LLDP Statistics Information（LLDP 統計情報） 194
LLDP Local Port Information（LLDP ローカルポート情報） 194
LLDP Neighbor Port Information（LLDP ネイバポート情報） 196

第 9 章　L3 Features（レイヤ 3 機能の設定） 197

ARP（ARP 設定） 198
ARP Elevation（ARP エレベーション） 198
ARP Aging Time（ARP エージングタイム設定） 198
Static ARP（スタティック ARP 設定） 198
Proxy ARP（プロキシ ARP） 199
ARP Table（ARP テーブルの参照） 199
Gratuitous ARP（Gratuitous ARP 設定） 200
IPv6 Neighbor（IPv6 ネイバ設定） 201
Interface（インタフェース設定） 202
IPv4 Interface（IPv4 インタフェース） 202
IPv6 Interface（IPv6 インタフェース） 203
Loopback Interface（ループバックインタフェース設定） 206
Null Interface（Null インタフェース） 207
UDP Helper（UDP ヘルパー） 207
IP Forward Protocol（IP 転送プロトコル） 207
IP Helper Address（IP ヘルパーアドレス） 208
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定） 208
IPv4 Route Table（IPv4 ルートテーブル） 209
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定） 210
IPv6 Route Table（IPv6 ルートテーブル） 210
Route Preference（ルート優先度設定） 211
ECMP Settings（ECMP 設定） 211
RIP（Routing Information Protocol） 212
RIP Settings（RIP 設定） 212
RIP Distribute List（RIP ディストリビュートリスト） 213
RIP Interface Settings（RIP インタフェース設定） 213
RIP Database（RIP データベース） 214
RIPng（RIPng 設定） 215
RIPng Settings（RIPng 設定） 215
RIPng Interface Settings（RIPng インタフェース設定） 216
RIPng Database（RIPng データベース） 217
OSPF（OSPF 設定） 217
OSPFv2（OSPFv2 設定） 217
OSPFv3 229
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル） 238
IPMC（IP マルチキャスト設定） 238
IP Route Filter（IP ルートフィルタ） 239
Route Map（ルートマップ設定） 239
Policy Route（ポリシールート設定） 241
VRRP（VRRP 設定） 242
VRRPv3 Settings（VRRPv3 設定） 243

第 10 章　QoS（QoS 機能の設定） 245

Basic Settings（基本設定） 246
Port Default CoS（ポートデフォルト CoS 設定） 246
Port Scheduler Method（ポートスケジューラーメソッド設定） 246
Queue Settings（QoS 設定） 247
CoS to Queue Mapping（CoS キューマッピング設定） 248
Port Rate Limiting（ポートレート制限設定） 248
Queue Rate Limiting（キューレート制限設定） 249

Advanced Settings（アドバンス設定）.....250
DSCP Mutation Map（DSCP 変更マップ設定）.....250
Port Trust State and Mutation Binding（ポートトラスト設定）.....250
DSCP CoS Mapping（DSCP CoS マップ設定）.....251
CoS Color Mapping（CoS カラーマップ設定）.....252
DSCP Color Mapping（DSCP カラーマップ設定）.....252
Class Map（クラスマップ設定）.....253
Aggregate Policer（アグリゲートポリサー設定）.....254
Policy Map（ポリシーマップ設定）.....256
Policy Binding（ポリシーバインディング設定）.....258
WRED（WRED 設定）.....259
WRED Profile（WRED プロファイル設定）.....259
WRED Queue（WRED キュー設定）.....260

第 11 章　ACL（ACL 機能の設定）　261

ACL Configuration Wizard（ACL 設定ウィザード）.....262
ACL Configuration Wizard（ACL 設定ウィザードの開始）.....262
パケットタイプ選択（ACL 設定ウィザード）.....262
ルール追加（ACL 設定ウィザード）.....263
ポート設定（ACL 設定ウィザード）.....268
ACL Access List（ACL アクセスリスト）.....268
Standard IP ACL（通常 IP ACL）.....270
Extended IP ACL（拡張 IP ACL）.....271
Standard IPv6 ACL（通常 IPv6 ACL）.....273
Extended IPv6 ACL（拡張 IPv6 ACL）.....274
Extended MAC ACL（拡張 MAC ACL）.....276
Extended Expert ACL（拡張詳細 ACL）.....277
ACL Interface Access Group（ACL インタフェースアクセスグループ）.....279
ACL VLAN Access Map（ACL VLAN アクセスマップ）.....280
Match Access-List（照合アクセスリスト設定）.....281
ACL VLAN Filter（ACL VLAN フィルタ設定）.....282
CPU ACL（CPU ACL）.....282

第 12 章　Security（セキュリティ機能の設定）　285

Port Security（ポートセキュリティ）.....286
Port Security Global Settings（ポートセキュリティグローバル設定）.....286
Port Security Port Settings（ポートセキュリティポート設定）.....287
Port Security Address Entries（ポートセキュリティアドレスエントリ設定）.....288
802.1X（802.1X 設定）.....289
802.1X Global Settings（802.1X グローバル設定）.....293
802.1X Port Settings（802.1X ポート設定）.....293
Authentication Session Information（オーセンティケーションセッションの状態）.....294
Authenticator Statistics（オーセンティケータ統計情報）.....294
Authenticator Session Statistics（オーセンティケータセッション統計情報）.....295
Authenticator Diagnostics（オーセンティケータ診断）.....295
AAA（AAA 設定）.....296
AAA Global Settings（AAA グローバル設定）.....296
Application Authentication Settings（アプリケーションの認証設定）.....296
Application Accounting Settings（アプリケーションアカウント設定）.....297
Authentication Settings（認証設定）.....298
Accounting Settings（アカウンティング設定）.....299
RADIUS（RADIUS 設定）.....300
RADIUS Global Settings（RADIUS グローバル設定）.....300
RADIUS Server Settings（RADIUS サーバの設定）.....300
RADIUS Group Server Settings（RADIUS グループサーバの設定）.....301
RADIUS Statistic（RADIUS 統計情報）.....302
TACACS+（TACACS+ 設定）.....303
TACACS+ Global Settings（TACACS+ サーバグローバル設定）.....303
TACACS+ Server Settings（TACACS+ サーバの設定）.....303
TACACS+ Group Server Settings（TACACS+ グループサーバの設定）.....304
TACACS+ Statistic（TACACS+ 統計情報）.....305
IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）.....305
IPv4.....305
IPv6.....315

DHCP Server Screening（DHCP サーバスクリーニング設定）.....323
DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）.....323
DHCP Server Screening Port Settings（DHCP サーバスクリーニングポート設定）.....324
ARP Spoofing Prevention（ARP スプーフィング防止設定）.....324
BPDU Attack Protection（BPDU アタック防止設定）.....325
MAC Authentication（MAC 認証）.....326
Web-based Access Control（Web 認証）.....326
Web Authentication（Web 認証設定）.....328
WAC Port Settings（Web 認証ポート設定）.....329
WAC Customize Page（WAC カスタマイズページ設定）.....329
Network Access Authentication（ネットワークアクセス認証）.....330
Guest VLAN（ゲスト VLAN 設定）.....330
Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）.....331
Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）.....332
Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）.....333
Safeguard Engine（セーフガードエンジン）.....334
Safeguard Engine Settings（セーフガードエンジン設定）.....335
CPU Protect Counters（CPU プロテクトカウンタ）.....335
CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）.....336
CPU Protect Type（CPU プロテクトタイプ）.....336
Trusted Host（トラストホスト）.....337
Traffic Segmentation（トラフィックセグメンテーション）.....337
Storm Control Settings（ストームコントロール設定）.....338
DoS Attack Prevention Settings（DoS 攻撃防止設定）.....339
SSH（Secure Shell）.....341
SSH Global Settings（SSH グローバル設定）.....341
Host Key（Host Key 設定）.....342
SSH Server Connection（SSH サーバ接続）.....343
SSH User Settings（SSH ユーザ設定）.....343
SSL（Secure Socket Layer）.....344
SSL Global Settings（SSL グローバル設定）.....344
Crypto PKI Trustpoint（暗号 PKI トラストポイント）.....345
SSL Service Policy（SSL サービスポリシー）.....346
SFTP Server Settings（SFTP サーバ設定）.....347
Network Protocol Port Protect Settings（ネットワークプロトコルポート保護設定）.....347

第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)　348

CFM（Connectivity Fault Management : 接続性障害管理）.....349
CFM Settings（CFM 設定）.....349
CFM Port Settings（CFM ポート設定）.....358
CFM Loopback Test（CFM ループバックテスト）.....359
CFM Linktrace Settings（CFM リンクトレース設定）.....360
CFM Packet Counter（CFM パケットカウンタ）.....361
CFM Counter CCM（CFM カウンタ CCM）.....361
CFM MIP CCM Table（CFM MIPCCM テーブル）.....362
CFM MEP Fault Table（CFM MEP 障害テーブル）.....362
Cable Diagnostics（ケーブル診断機能）.....363
Ethernet OAM（イーサネット OAM）.....364
Ethernet OAM Settings（イーサネット OAM 設定）.....364
Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）.....365
Ethernet OAM Event Log Table（イーサネット OAM イベントログテーブル）.....367
Ethernet OAM Statistics Table（イーサネット OAM 統計情報テーブル）.....367
Ethernet OAM DULD Settings（イーサネット OAM DULD 設定）.....368
DDM（DDM 設定）.....369
DDM Settings（DDM 設定）.....369
DDM Temperature Threshold Settings（DDM 温度しきい値設定）.....370
DDM Voltage Threshold Settings（DDM 電圧しきい値設定）.....370
DDM Bias Current Threshold Settings（DDM バイアス電流しきい値設定）.....371
DDM TX Power Threshold Settings（DDM 送信電力しきい値設定）.....371
DDM RX Power Threshold Settings（DDM 受信電力しきい値設定）.....372
DDM Status Table（DDM ステータステーブル）.....372

第 14 章　Monitoring（スイッチのモニタリング）　373

Utilization（利用分析）....374
Port Utilization（ポート使用率）....374
Statistics（統計情報）....374
Port（ポート統計情報）....374
Interface Counters（インタフェースカウンタ）....375
Counters（カウンタ）....376
Mirror Settings（ミラー設定）....378
sFlow（sFlow 設定）....379
sFlow Agent Information（sFlow エージェント情報）....379
sFlow Receiver Settings（sFlow レシーバ設定）....379
sFlow Sampler Settings（sFlow サンプラ設定）....380
sFlow Poller Settings（sFlow ポーラ設定）....381
Device Environment（機器環境確認）....381

第 15 章　Green（省電力機能）　382

Power Saving（省電力）....383
EEE（Energy Efficient Ethernet/ 省電力イーサネット）....384

第 16 章　Save and Tools（Save メニュー /Tools メニュー）　385

Save（Save メニュー）....386
Save Configuration（コンフィグレーションの保存）....386
Tools（Tools メニュー）....386
Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）....386
Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）....388
Log Backup（ログファイルのバックアップ）....390
Ping....392
Trace Route（トレースルート）....394
Reset（リセット）....395
Reboot System（システム再起動）....396

付録 A パスワードリカバリ手順　397

付録 B システムログエントリ　398

付録 C トラップログエントリ　418

付録 D RADIUS 属性割り当て　428

付録 E IETF RADIUS 属性サポート　430

付録 F 機能設定例　432

対象機器について....432
Traffic Segmentation（トラフィックセグメンテーション）....432
VLAN....433
Link Aggregation（リンクアグリゲーション）....434
Access List（アクセスリスト）....436
Loopback Detection（LBD）（ループ検知）....437

はじめに

DGS-3130 シリーズユーザマニュアルは、スイッチの設置や操作方法など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
  - システムの基本的な設置方法について説明します。また、本スイッチの電源接続の方法についても紹介します。
- 第 3 章 スイッチの接続
  - スイッチをご使用のネットワークに接続する方法を説明します。
- 第 4 章 スイッチの管理について
  - スイッチの管理方法の概要と、コンソールポート / 管理ポートへの接続方法、SNMP 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、PoE 管理、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）
  - ユーザアカウント接地、SNMP 設定、Telnet/Web 設定、DHCP 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、スパニングツリー、ループバック検知、リンクアグリゲーション、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、ルート優先度設定、VRRP 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）
  - ポートセキュリティ、802.1X 認証、トラストホスト、トラフィックセグメンテーション、SSL、SSH 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 などの OAM 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）
  - パケット統計情報、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、EEE（Energy Efficient Ethernet/ 省電力イーサネット）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イベントについて説明します。
- 付録 C トラップログエントリ
  - トラップログについて説明します。
- 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
  - スイッチでサポートされる 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。

警告 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恐れがあります。

重要 使い方によっては、予期せぬ動作などを引き起こす可能性があります。

注意 設定の組み合わせ、イベントや手順により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があります。

補足 特徴や技術について、補足情報を説明します。

本マニュアル中での字体、・記号についての表記規則は以下の通りです。

字体・記号	解説	例
「」	WebGUI 上の UI 名を示します。	「OK」をクリックし、設定を適用します。
青字	参照先または URL を示します。	「Web GUI へのログイン」をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
courier 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
courier 斜体	コマンド項目（可変または固定）。	*value*
< >	可変項目。< > にあたる箇所に値または文字を入力します。	<*value*>
[ ]	任意の固定項目。	[*value*]
[< >]	任意の可変項目。	[<*value*>]
{ }	{ } 内の選択肢から 1 つ選択して入力する項目。	{*choice1* | *choice2*}
|（垂直線）	相互排他的な項目。	*choice1* | *choice2*
Menu Name > Menu Option	メニュー構造を示します。	**Device > Port > Port Properties** は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。

製品名 / 品番一覧

製品名	品番
DGS-3130-30TS	DGS-3130-30TS/A1
DGS-3130-30S	DGS-3130-30S/A1
DGS-3130-30PS	DGS-3130-30PS/A1
DGS-3130-54TS	DGS-3130-54TS/A1
DGS-3130-54S	DGS-3130-54S/A1
DGS-3130-54PS	DGS-3130-54PS/A1

第 1 章　本製品のご使用にあたって

- DGS-3130 シリーズについて
- ポート
- 前面パネル
- 背面パネル
- 側面パネル
- LED 表示

DGS-3130 シリーズについて

DGS-3130 シリーズは、SMB やエンタープライズ、メトロイーサネット向けのセキュアなネットワーク構築を実現するギガビットレイヤ 2+ スイッチです。充実した L2 機能に加えて、IP インタフェースや、スタティックルーティング機能などを提供します。本シリーズは、10/100/1000BASE-T ポートを 24/48 ポート備えた DGS-3130-30TS/54TS 、PoE/PoE+ に対応した DGS-3130-30PS/54PS、SFP 多ポートに対応した DGS-3130-30S/54S といった幅広いラインナップを用意しています。また、全てのモデルで 100/1000/10G BASE-T ポート× 2、10G SFP+ × 4 ポートを搭載し、10 ギガビットの高速ネットワーク環境を構築することができます。

信頼性の高いネットワーク

802.1D STP、802.1w RSTP、802.1s MSTP、ループバック検出、ブロードキャストストーム制御など、ネットワークの耐障害性を強化するための必須の信頼性機能が組み込まれています。そのほか、ERPS、リンクアグリゲーションなどの実装に加え、電力サージや落雷から保護する 6kV サージプロテクションを搭載し、信頼性の高いネットワークを構築することが可能です。

10G テクノロジー

本シリーズは、高速なバックボーンネットワークに対応するため、10G に対応した 100/1000/10G BASE-T ポートを 2 ポートと、SFP+ スロットを 4 スロット搭載しています。基幹ネットワークに 10G での接続が可能であり、高速ネットワークを構築することが可能となります。

強固なセキュリティと高い可用性

802.1X/MAC アドレス認証※ /WEB 認証※をはじめとして、DHCP スヌーピング※を利用した IP-MAC ポートバインディング※、ARP スプーフィング防止、Compound 認証※など様々なセキュリティ機能を利用できます。そのほか、ACL、ストーム制御などの多くのセキュリティ機能をユーザに提供します。

多様な管理機能

Web ベース GUI や CLI などによる管理が可能です。SNMP 機能ではステータス情報の確認や異常イベントに対するトラップ送信を行うことができます。また、802.3ah（リンク OAM）や CFM によるイーサネットレベルでの監視にも対応しており、充実したメンテナンス機能を提供します。

※将来のファームウェアでサポート予定

ポート

DGS-3130 シリーズは以下のポートを搭載しています。

製品名	DGS-3130-30TS	DGS-3130-30S	DGS-3130-30PS	DGS-3130-54TS	DGS-3130-54S	DGS-3130-54PS
10/100/1000BASE-T ポート (RJ-45) (PoE 給電)	24	—	24(24)	48	—	48(48)
100/1000/10G BASE-T ポート (RJ-45)	2					
SFP スロット	—	24	—	—	48	—
10 ギガ SFP+ スロット	4					
コンソールポート (RJ-45)	1					
管理ポート (MGMT) (RJ-45)	1					
USB ポート (USB2.0)	1					

DGS-3130 シリーズスイッチ対応オプションモジュール

種別	製品名
SFP+(10Giga) ※1	DEM-431XT
	DEM-432XT
	DEM-433XT
	DEM-434XT
WDM 対応 1 芯 SFP(1Giga)	DEM-330T
	DEM-330R
	DEM-331T
	DEM-331R
2 芯 SFP(1Giga)	DEM-310GT
	DEM-311GT
	DEM-312GT2
	DEM-314GT
	DEM-315GT
Copper SFP(1Giga)	DGS-712
100FX SFP ※2	DEM-211

※1 SFP+ スロットでのみ使用可能です。

※2 SFP スロットでのみ使用可能です。

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。

ポート	説明
10/100/1000BASE-T ポート	10Mbps、100Mbps または 1000Mbps の速度で通信を行う RJ-45 イーサネットポートです。
100/1000/10G BASE-T ポート	100Mbps、1000Mbps または 10Gbps の速度で通信を行う RJ-45 イーサネットポートです。
SFP スロット	100Mbps または 1Gbps の速度で通信を行う SFP スロットです。
10 ギガ SFP ＋スロット	1Gbps または 10Gbps の速度で通信を行う SFP+ スロットです。
Console ポート（RJ-45）	設定、管理、監視のために、スイッチのコマンドラインインターフェイス（CLI）に接続します。 DB9 インタフェースを備えた同梱のコンソールケーブルを使用して、スイッチを PC のシリアルポート（COM）に接続します。
MGMT ポート	RJ-45 管理（MGMT）ポートは、Telnet、Web、SNMP 管理用の IP ベースのアウトオブバンド（OOB）ポートです。このポートを使用すると、ネットワークに接続せずにスイッチを構成することができます。
USB ポート	USB 2.0 Type-A ポートにフラッシュドライブを挿入すると、追加のストレージスペースが提供されます。スイッチの NVRAM との間でファームウェアイメージおよび構成ファイルをコピーすることができます。
各種 LED	電源、RPS、ファンエラー、コンソール、USB、MGMT、Link/Act/Speed の動作状態を表示します。

補足　LED については「LED 表示」の項で詳細な動作について説明します。

DGS-3130-30TS

- 10/100/1000BASE-T ポート x 24
- 100/1000/10G BASE-T ポート x 2
- SFP+ スロット x 4
- RJ-45 コンソールポート x 1
- RJ-45 管理ポート x 1
- USB ポート x 1
- LED：Power、RPS、Fan Error、Console、USB、MGMT、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

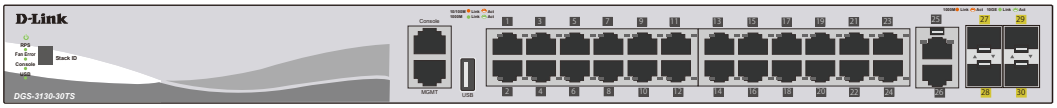


図 1-1　DGS-3130-30TS の前面パネル

DGS-3130-30S

- SFP スロット x 24
- 100/1000/10G BASE-T ポート x 2
- SFP+ スロット x 4
- RJ-45 コンソールポート x 1
- RJ-45 管理ポート x 1
- USB ポート x 1
- LED：Power、RPS、Fan Error、Console、USB、MGMT、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

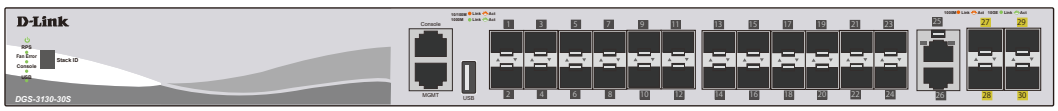


図 1-2　DGS-3130-30S の前面パネル

DGS-3130-30PS

- 10/100/1000BASE-T ポート（PoE 給電）x 24
- 100/1000/10G BASE-T ポート x 2
- SFP+ スロット x 4
- RJ-45 コンソールポート x 1
- RJ-45 管理ポート x 1
- USB ポート x 1
- LED：Power、RPS、Fan Error、Console、USB、MGMT、PoE（各ポート）、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

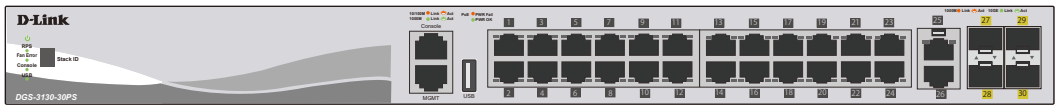


図 1-3　DGS-3130-30PS の前面パネル

DGS-3130-52TS

- 10/100/1000BASE-T ポート x 48
- 100/1000/10G BASE-T ポート x 2
- SFP+ スロット x 4
- LED：Power、RPS、Fan Error、Console、USB、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

補足　RJ-45 コンソールポート、RJ-45 管理ポート、USB ポートは背面に配置されています。

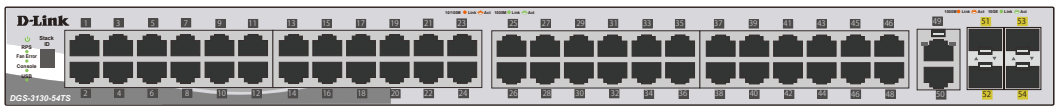


図 1-4　DGS-3130-54TS の前面パネル

DGS-3130-52S

- SFP スロット x 48
- 100/1000/10G BASE-T ポート x 2
- SFP+ スロット x 4
- LED：Power、RPS、Fan Error、Console、USB、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

補足　RJ-45 コンソールポート、RJ-45 管理ポート、USB ポートは背面に配置されています。

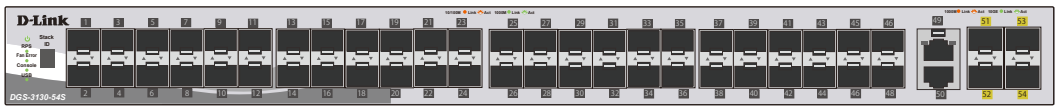


図 1-5　DGS-3130-54S の前面パネル

DGS-3130-52PS

- SFP スロット x 48（PoE 給電）
- 100/1000/10G BASE-T ポート x 2
- SFP+ スロット x 4
- LED：Power、RPS、Fan Error、Console、USB、PoE（各ポート）、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

補足　RJ-45 コンソールポート、RJ-45 管理ポート、USB ポートは背面に配置されています。

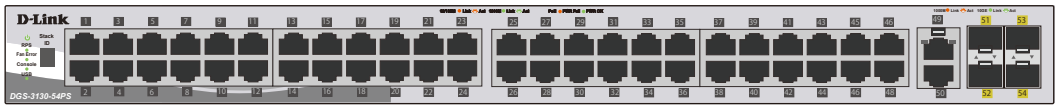


図 1-6　DGS-3130-54PS の前面パネル

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。

コンポーネント	説明
セキュリティロック	ケンジントンロックにより、デバイスを固定します。セキュリティワイヤは別途購入する必要があります。
MGMT	RJ-45 管理（MGMT）ポートは、Telnet、Web、SNMP 管理用の IP ベースのアウトオブバンド（OOB）ポートです。このポートを使用すると、ネットワークに接続せずにスイッチを構成することができます。
Console（RJ-45）	設定、管理、監視のために、スイッチのコマンドラインインターフェイス（CLI）に接続します。 DB9 インタフェースを備えた同梱のコンソールケーブルを使用して、スイッチを PC のシリアルポート（COM）に接続します。
USB	USB 2.0 Type-A ポートにフラッシュドライブを挿入すると、追加のストレージスペースが提供されます。スイッチの NVRAM との間でファームウェアイメージおよび構成ファイルをコピーすることができます。
接地コネクタ	アース線を使用して、ワイヤの一方の端をスイッチの GND に接続し、ワイヤのもう一方の端をご利用の環境のアース端子に接続します。
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。
電源抜け防止クリップ挿入口	電源抜け防止クリップを挿入して AC 電源コネクタが外れることを防止します。
リダンダント電源コネクタ	オプションのリダンダント電源ユニット用のコネクタです。内蔵電源ユニットに異常が発生した場合に外部リダンダント電源ユニット（オプション）が自動的にスイッチに電源を供給します。
MGMT LED	MGMT ポートの動作状態を表示します。

補足　LED については「LED 表示」の項で詳細な動作について説明します。

補足　RPS は将来のファームウェアでサポート予定です。

DGS-3130-30TS/DGS-3130-30S



図 1-7　DGS-3130-30TS/DGS-3130-30S 背面パネル図

DGS-3130-30PS



図 1-8　DGS-3130-30PS 背面パネル図

DGS-3130-54TS/DGS-3130-54S



図 1-9　DGS-3130-54TS/DGS-3130-54S 背面パネル図

DGS-3130-54PS

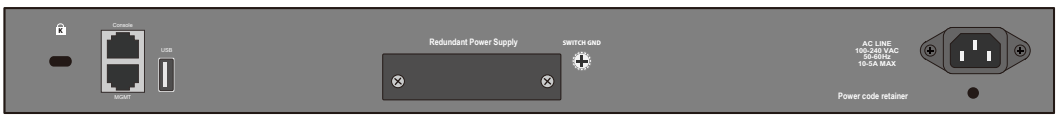


図 1-10　DGS-3130-54PS 背面パネル図

補足　DGS-3110-30TS/30S/30PS の RJ-45 コンソールポート、RJ-45 管理ポート、USB ポートは前面に配置されています。

側面パネル

スイッチの側面パネルには、通気口、ファン、およびラック取り付けネジ穴があります。 通気口は、内部熱を放散し、内部空気の循環を促進するために使用されます。 これらの開口部を塞がないようにご注意ください。 スイッチの適切な換気のためには、側面に少なくとも 4 インチ（10 cm）以上のスペースを確保してください。 適切な熱放出、空気の循環をしないと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-3130-30TS

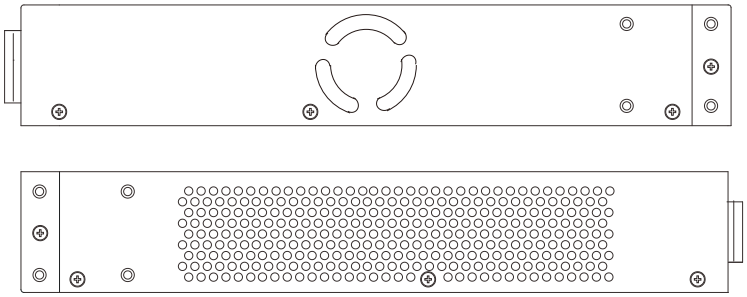


図 1-11　側面パネル図（DGS-3130-30TS）

DGS-3130-30S

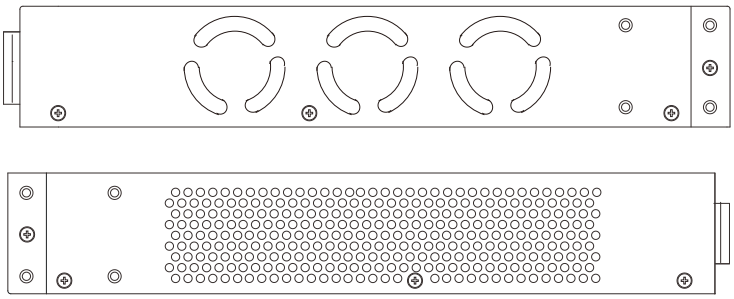


図 1-12　側面パネル図（DGS-3130-30S）

DGS-3130-30PS

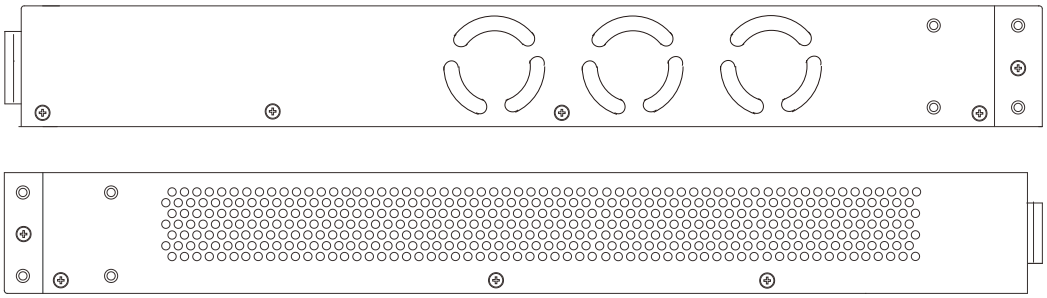


図 1-13　側面パネル図（DGS-3130-30PS）

DGS-3130-54TS

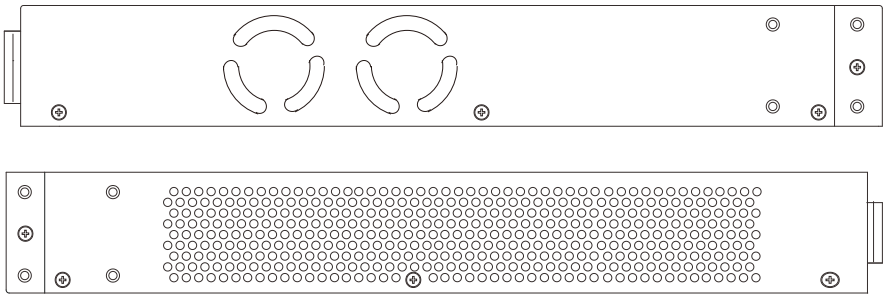


図 1-14　側面パネル図（DGS-3130-54TS）

DGS-3130-54S

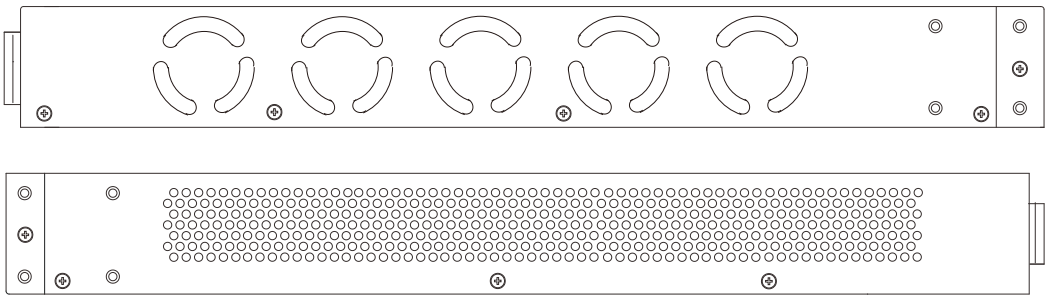


図 1-15　側面パネル図（DGS-3130-54S）

DGS-3130-54PS

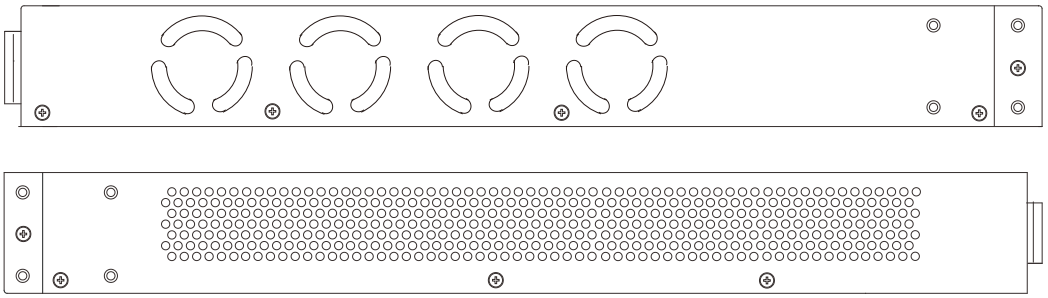


図 1-16　側面パネル図（DGS-3130-54PS）

LED 表示

LED はスイッチとネットワークの状態を表示します。Power、RPS、Fan Error、Console、USB、MGMT、PoE（各ポート）、Link/Act/Speed（各ポート / スロット）、スタック ID について確認することができます。以下に、スイッチ上の LED の配置と、各 LED の状態が表す意味を示します。

DGS-3130-30TS

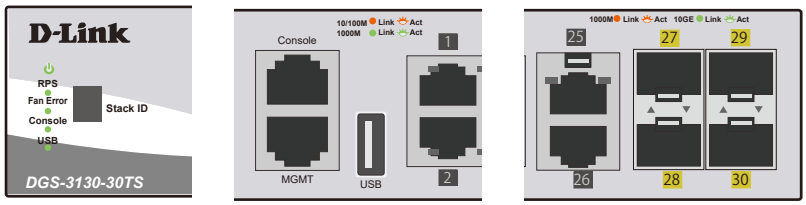


図 1-17　DGS-3130-30TS の前面パネル LED 配置図

DGS-3130-30S

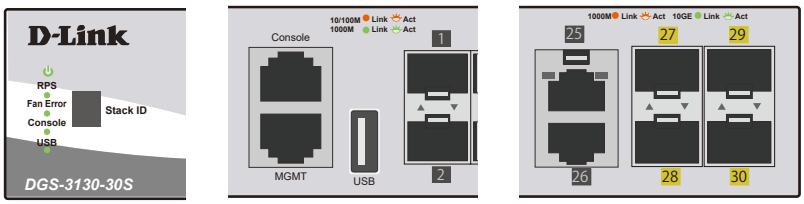


図 1-18　DGS-3130-30S の前面パネル LED 配置図

DGS-3130-30PS

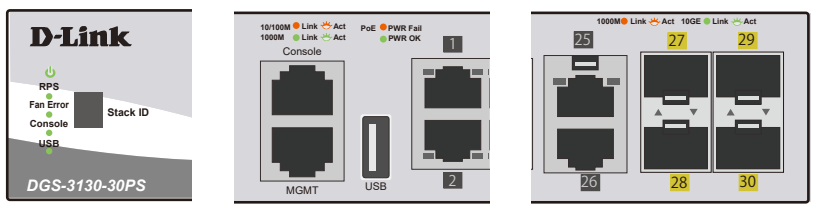


図 1-19　DGS-3130-30PS の前面パネル LED 配置図

DGS-3130-54TS

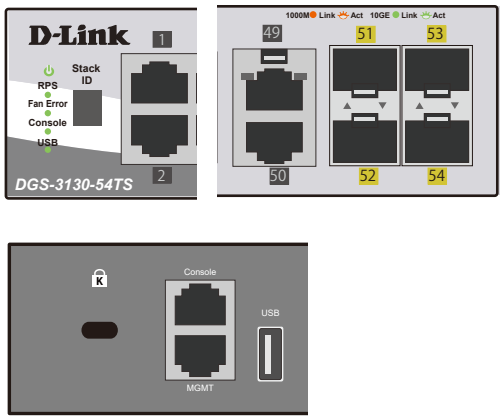


図 1-20　DGS-3130-54TS：前面パネル LED 配置図（上）、背面パネル LED 配置図（下）

DGS-3130-54S

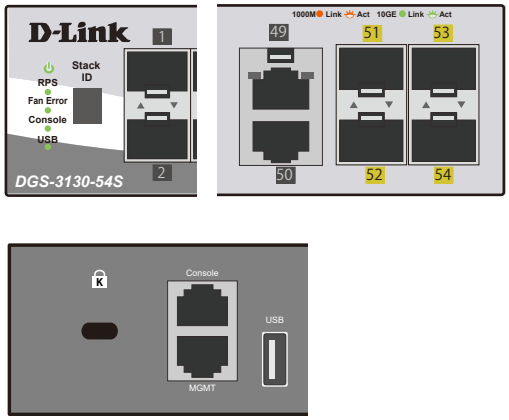


図 1-21　DGS-3130-54S：前面パネル LED 配置図（上）、背面パネル LED 配置図（下）

DGS-3130-54PS

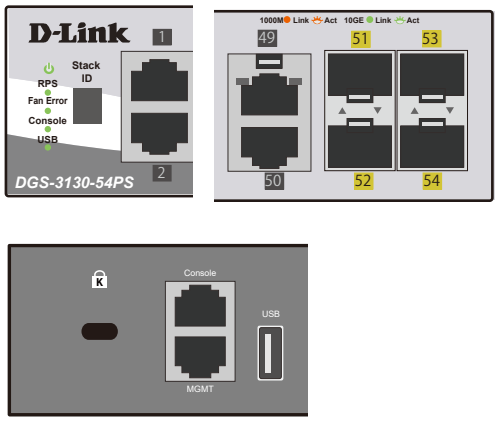


図 1-22　DGS-3130-54PS：前面パネル LED 配置図（上）、背面パネル LED 配置図（下）

LED が示すスイッチの状態は以下の通りです。

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。
Fan Error	赤	点灯	ファンに不具合が発生しています。
	ー	消灯	ファンは通常通り動作しています。
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。
	緑	点滅	ポートで通信が発生しています。
	ー	消灯	リンクが確立していません。
USB	緑	点灯	USB メモリが挿入されています。
		点滅	読み / 書きが実行されています。
	赤	点灯	USB メモリの不具合を検出しました。
	ー	消灯	USB メモリが挿入されていません。
スタック 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。
MGMT	緑 / 橙	点灯	管理ポートでリンクが確立されています。
		点滅	管理ポートで通信が発生しています。
	ー	消灯	リンクが確立されていない、もしくはインタフェースが管理者によりシャットダウンされています。
10/100/1000Mbps ポート LED			
Link/Act/Speed	緑	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps 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	リンクが確立していません。
PoE （DGS-3130-30PS/54PS： ポート LED 右側）	緑	点灯	接続中の PoE 受電機器に給電中です。
	橙	点灯	PoE ポートにエラーが発生しました。
	ー	消灯	給電をしていません。(受電機器が未検出または未接続)
100/1000/10G BASE-T ポート LED			
Link/ACT 左側 LED：10G ポート（上） 右側 LED：10G ポート（下）	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	100/1000Mbps でリンクが確立しています。
		点滅	100/1000Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
SFP ポート LED			
Link/ACT	緑	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps 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	リンクが確立していません。
SFP+ ポート LED			
Link/ACT	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	1000Mbps でリンクが確立しています。
		点滅	1000Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。

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+ ポートへのモジュールの取り付け
- 電源抜け防止クリップの装着
- 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 専用）　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
- マニュアル　x　1
- ゴム足　x　4
- CD-ROM　x　1
- 電源抜け防止クリップ　x　1
- PL シート　x　1

万一、不足しているもの損傷を受けているものがありましたら、ご購入頂いた販売代理店までご連絡ください。

ネットワーク接続前の準備

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

- スイッチは、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、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。

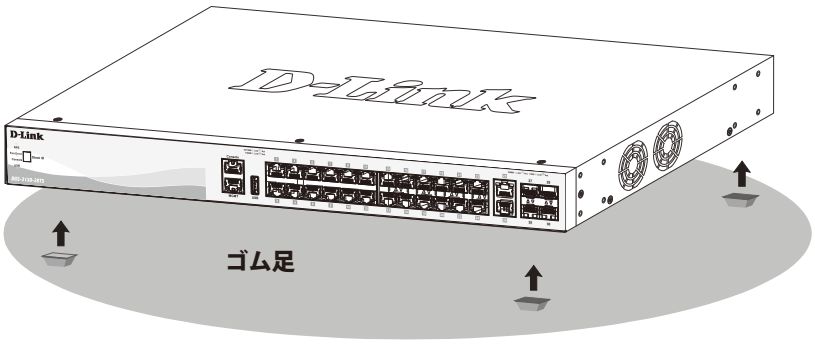


図 2-1　ゴム足の取り付け

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。

補足 スイッチをラックに固定するネジは付属品には含まれません。別途ご用意ください。

1. 電源ケーブルおよびケーブル類が本体、拡張モジュールに接続していないことを確認します。
2. 付属のネジで、スイッチの両側側面にブラケットを取り付けます。

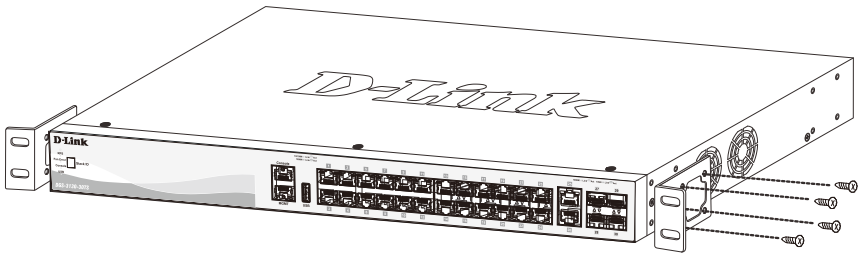


図 2-2　スイッチへのブラケットの取り付け図

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

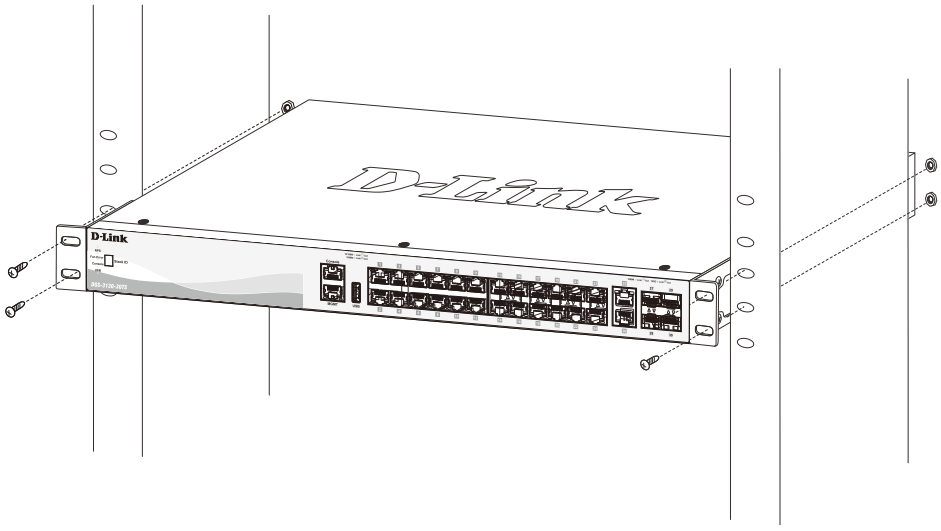


図 2-3　スイッチのラックへの設置図

SFP/SFP+ ポートへのモジュールの取り付け

本シリーズのスイッチは SFP と SFP+ ポートを搭載しており、通常の RJ-45 接続をサポートしないスイッチとネットワークを構成することが可能です。
以下に、スイッチに SFP ポートモジュールを挿入した例を図に示します。

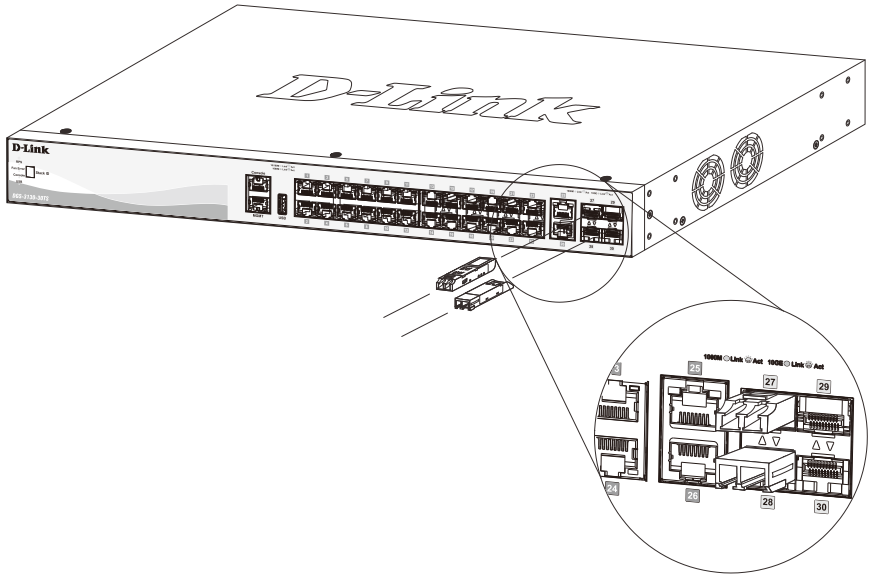


図 2-4　　前面パネルの SFP/SFP+ ポートへのモジュールの挿入

電源抜け防止クリップの装着

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

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

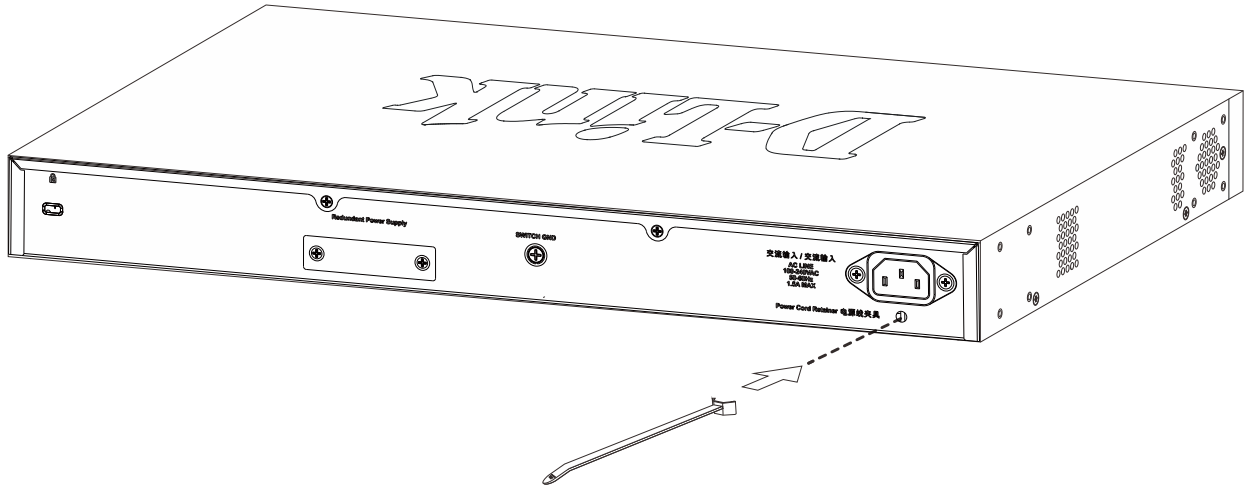


図 2-5　　タイラップの挿し込み

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。

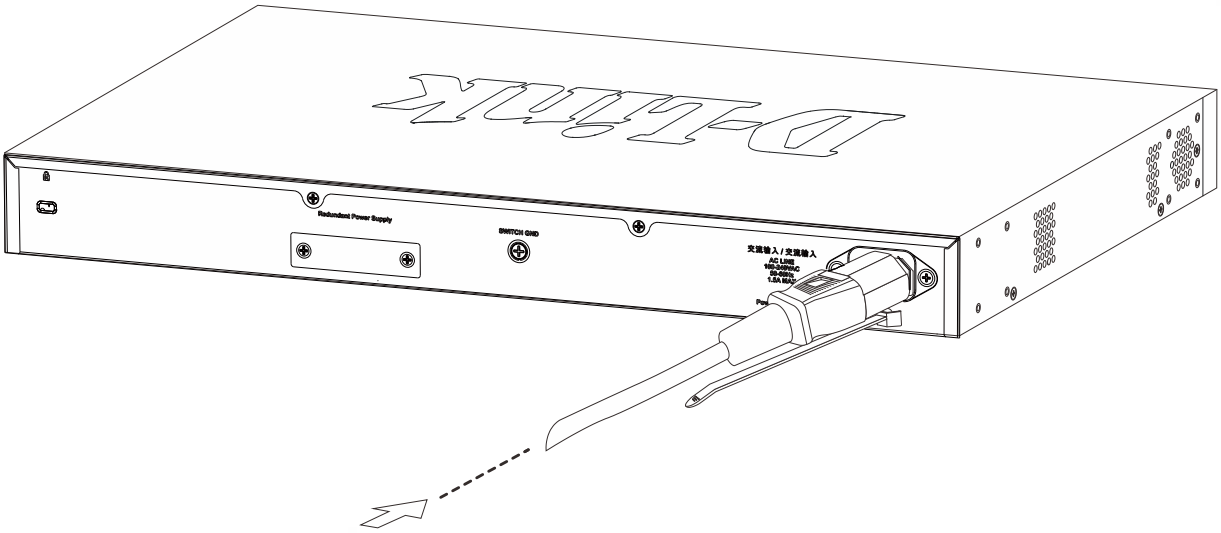


図 2-6　　電源コード挿し込み

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。

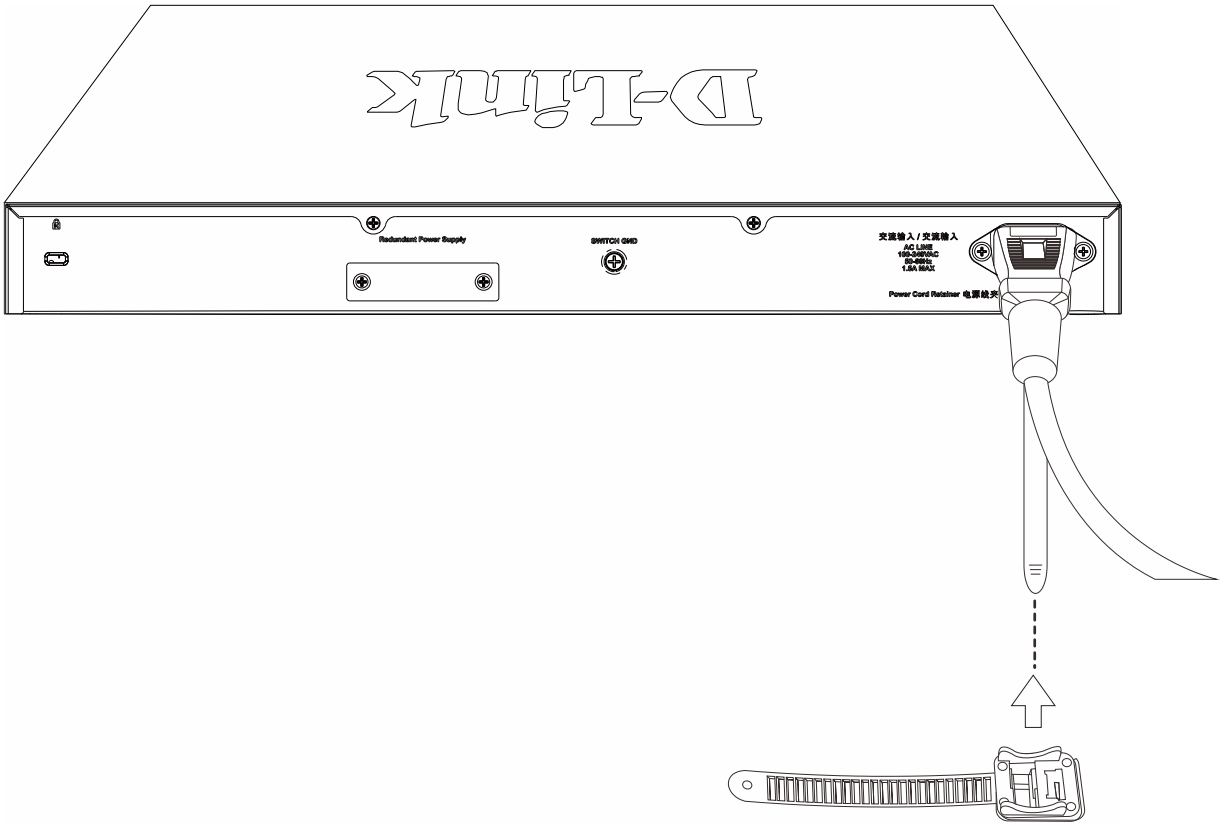


図 2-7　　リテイナー（固定具）のスライド

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。

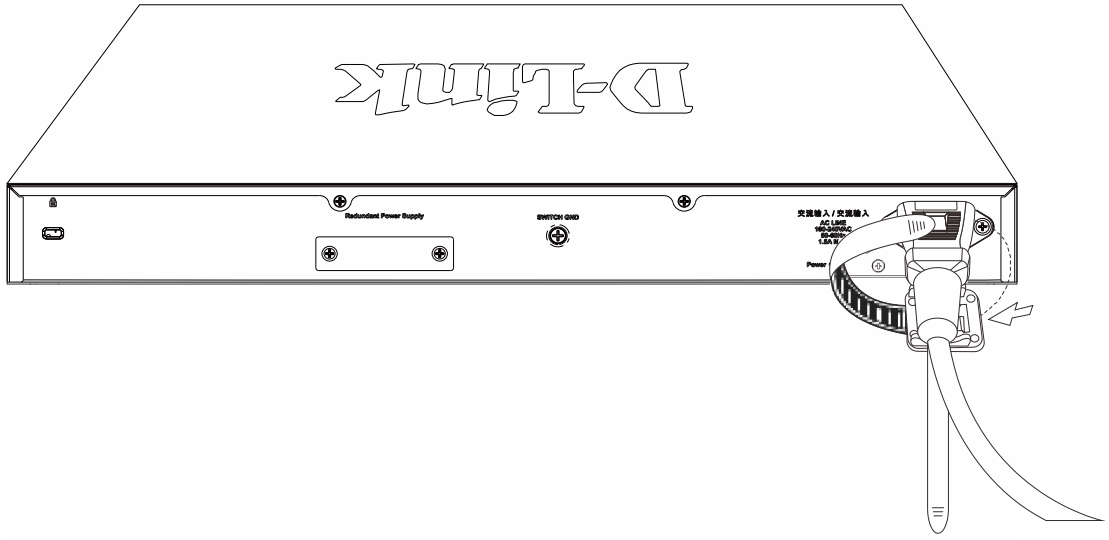


図 2-8　　リテイナーの巻き付け、固定

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。

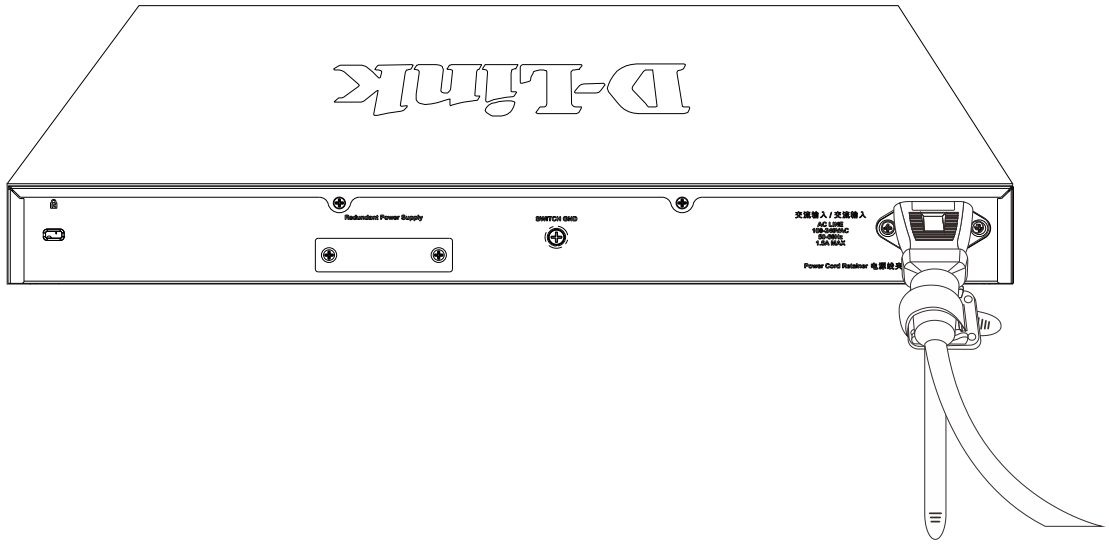


図 2-9　　電源抜け防止クリップの固定確認

リダンダント電源システムの設置

DGS-3130 シリーズは外付けのリダンダント電源システム（RPS）、DPS-500A（DGS-3130-30TS/30S/54TS/54S）、DPS-700（DGS-3130-30PS/54PS）をサポートしています。DPS-500A、DPS-700 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す。DPS-500A は DPS-800 に取り付けることができます。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　本機能は将来のファームウェアでサポート予定です。

警告　リダンダント電源ユニットの接続を行う前に、スイッチの AC 電源ケーブルを抜いておいてください。また、はじめに必ず電源ケーブルとコネクタの仕様書および設定手順をご確認ください。

警告　使用する「RPS」を DC 電源ケーブルに接続する前に AC 電源へ接続しないでください。RPS にダメージを与える場合があります。

警告　RPS を設置する場合、スイッチの背後に少なくとも 15cm（6 インチ）の空間を設けてください。ケーブルが損傷する場合があります。

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-500A は DGS-3130-30TS/30S/54TS/54S に対応しています。DPS-500A のマスタスイッチへの接続は、14 ピンの DC 電源ケーブルを使用して行います。標準の三極の AC 電源ケーブルでリダンダント電源装置とメイン電源を接続します。

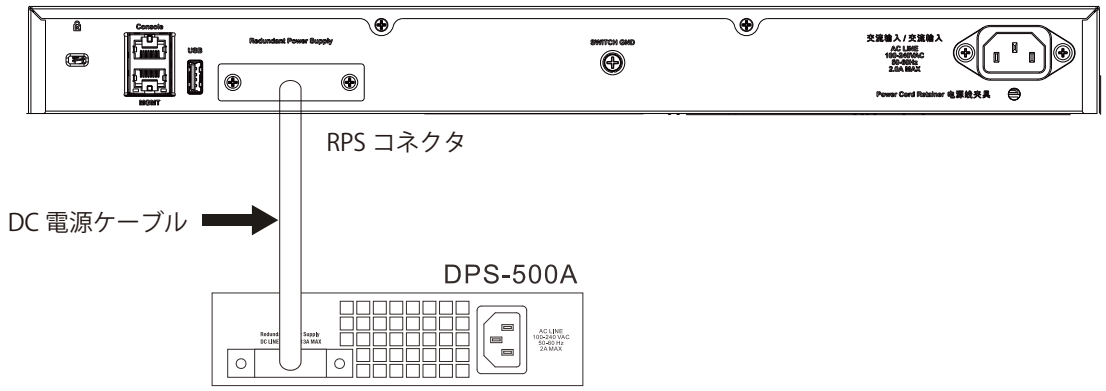


図 2-10　DGS-3130-54TS と DPS-500A の接続

1. 14 ピン DC 電源ケーブルの一端をスイッチ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。
2. 標準の AC 電源ケーブルでリダンダント電源装置とメインの AC 電源を接続します。DPS-500A 前面の緑の 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。
3. スイッチを再び AC 電源に接続します。RPS LED が点灯してリダンダント電源が動作していることを確認できます。
4. 本手順の実行による設定変更は必要ありません。

警告　本製品に対し DPS-500A 以外のリダンダント電源ユニットに使用しないでください。

補足　さらに詳細な情報については DPS-500A のマニュアルをご参照ください。

補足　PoE モデルの DGS-3130-30PS/54PS については、DPS-700 を使用してリダンダント電源または PoE 給電電力の拡張に対応することができます。

DPS-700

DPS-700 は DGS-3130-30PS/54PS に対応しています。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。標準の三極の AC 電源ケーブルでリダンダント電源装置とメイン電源を接続します。

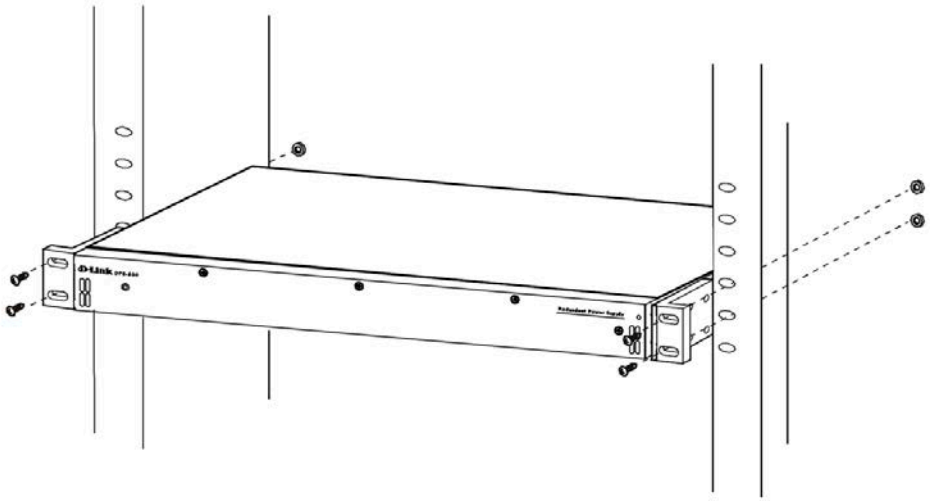


図 2-11　DPS-700 をラックに取り付ける

1. 22 ピン DC 電源ケーブルの一端をスイッチ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。
2. 標準の AC 電源ケーブルでリダンダント電源装置とメインの AC 電源を接続します。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。
3. スイッチを再び AC 電源に接続します。スイッチの 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。
4. 本手順の実行による設定変更は必要ありません。

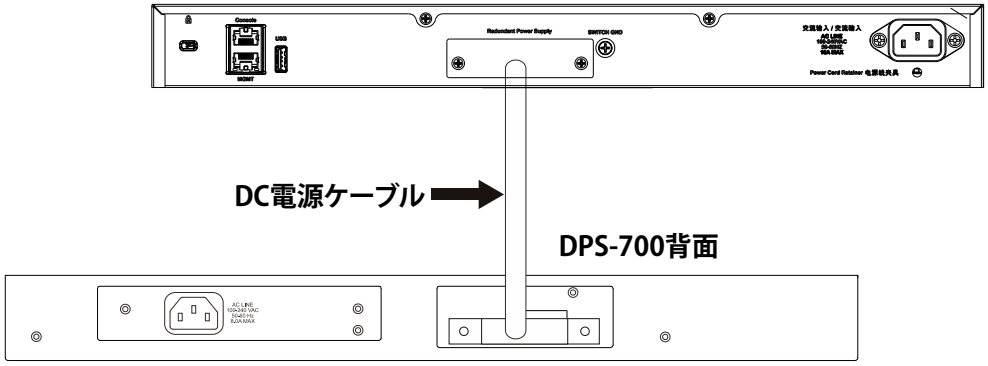


図 2-12　DGS-3130-54PS と DPS-700 の接続

警告　DGS-3130-30PS/54PS と DPS-700 の接続には 22 ピンの DC 電源ケーブル以外使用しないでください。

DPS-800

DPS-800 は標準サイズのラックマウント（1U サイズ）シャーシです。2 台までの DPS-500A を収容できます。

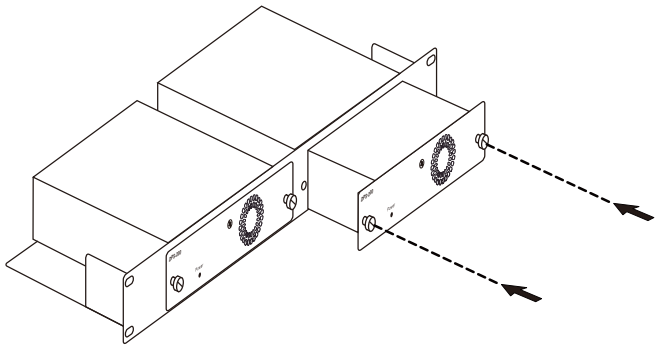


図 2-13　DPS-500A を DPS-800 に取り付ける

リダンダント電源システムは標準 19 インチラックにも取り付けることができます。以下の図を参照してください。

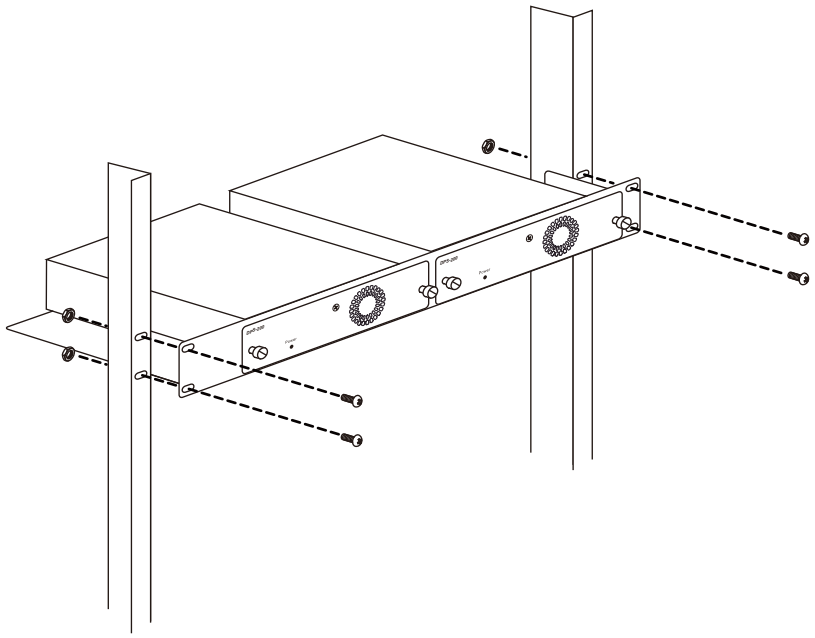


図 2-14　DPS-800 をラックに取り付ける

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。

電源の異常

万一停電などの電源異常が発生する / 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
- スタック接続について

補足　すべてのポートは Auto MDI/MDI-X 接続をサポートしています。

エンドノードと接続する

「エンドノード」とは本スイッチと接続するネットワーク機器の一般的な呼称です。パソコン、ノート PC、アクセスポイント、プリントサーバ、VoIP 電話機などが該当します。各エンドノードは「100/1000/10000Mbps」RJ45 ネットワークポートを有している必要があります。通常エンドノードはスタンダードなツイストペア UTP/STP ネットワークケーブルを使ってスイッチと接続されます。接続が成功すると、対応ポートの LED がポートでのネットワーク動作に従い点灯 / 点滅します。

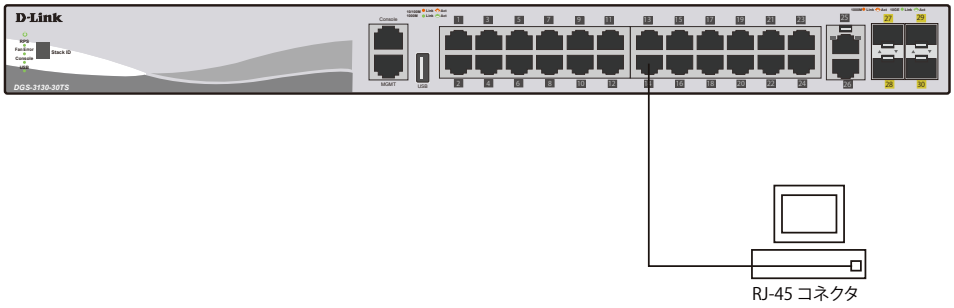


図 3-1　エンドノードと接続した図

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

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- カテゴリ 3 以上の UTP/STP ケーブル：10BASE-T ハブまたはスイッチと接続する。
- カテゴリ 5 以上の UTP/STP ケーブル：100BASE-TX ハブまたはスイッチと接続する。
- エンハンスドカテゴリ 5e 以上の UTP ケーブル：1000BASE-T スイッチと接続する。
- 光ファイバケーブル : SFP/SFP+ ポート経由で光ファイバをサポートするスイッチにアップリンクする。

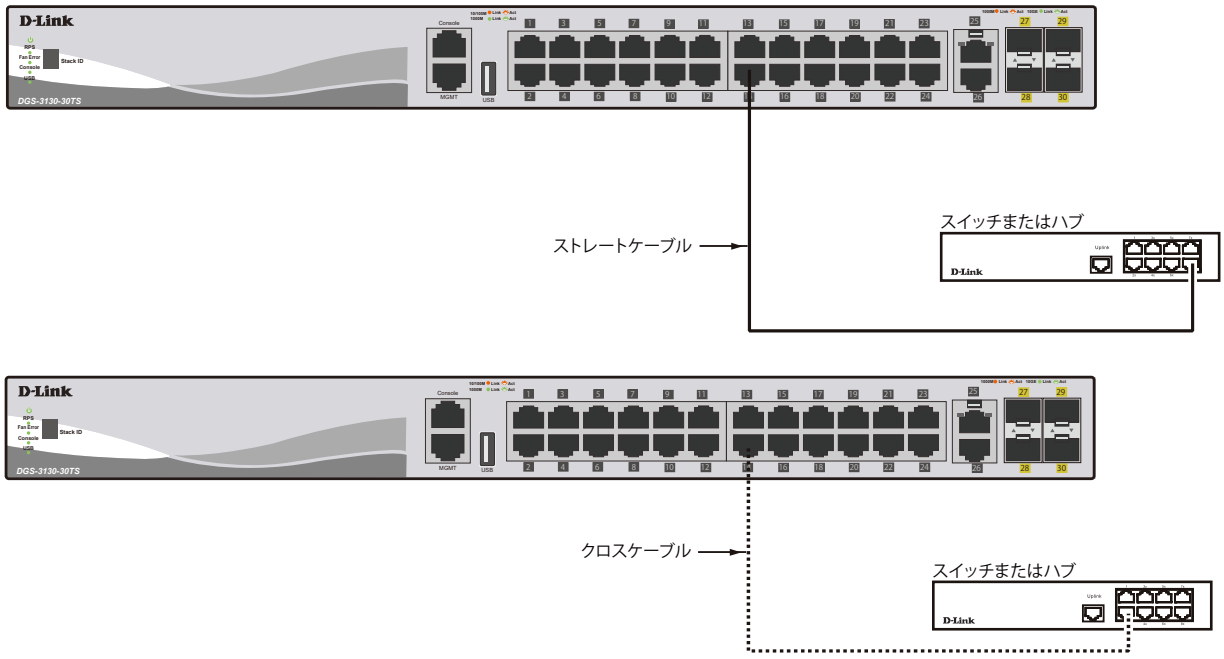


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

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

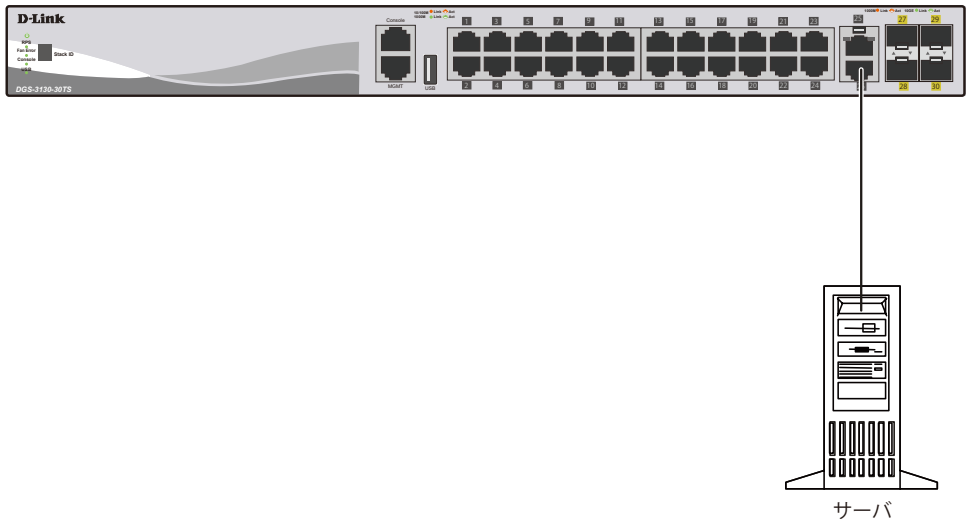


図 3-3　サーバ、PC、スイッチスタックとのアップリンク接続図

スタック接続について

補足　スタック機能は将来のファームウェアでサポート予定です。

本シリーズはスイッチのスタックをサポートしており、最大 9 台までのスタックが可能です。マススタースイッチ上で管理ポートを介して 1 つの IP アドレスで管理、または Telnet、GUI インタフェース（Web）、SNMP を介して複数の IP アドレスで管理することができます。
RJ-45/SFP+ ポートを使用したスイッチのスタックにより、ネットワークのアップグレードをリーズナブルでコストパフォーマンスの高い方法で実現します。これ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 6 個※のスタック用ポート / 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、RJ-45 ケーブルや SFP+ ダイレクトアタッチケーブル（DAC）、または光ファイバ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。
※ 10GBASE-T ポート× 2 と SFP+ × 4 スロットがスタック用に使用できます。実際に使用するのは、このうち 2 個または 4 個のポート / スロットです。

- 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円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、RJ-45 ケーブル、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 コネクタに接続された 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 6 ポートのみ物理スタックに使用できます。

補足　スタッキングが有効になっている場合、スタックに使用している 2/4 個のポート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。これらのポートはスタッキング専用ポートとなります。

物理スタックでは「2 ポート」または「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。

スタッキングコスト

スタック内の物理スタック台数は、スタックコストまたはスタック可能な最大デバイス数によって制限されます。DGS-3130 シリーズでは、合計スタッキングコストは 12 で、スタック可能な最大デバイス数は 9 です。

DGS-3130-30TS/30S/30PS モデルはスタッキングコストを「1」消費し、DGS-3130-54TS/54S/54PS はスタッキングコストを「2」消費します。したがって、スタックが DGS-3130-30TS/30S/30PS シリーズで構成されている場合、スタックあたりの最大デバイス数は 9 台です。スタックが DGS-3130-54TS/54S/54PS シリーズで構成されている場合、それぞれのスタッキングコストは「2」であるため、スタックあたりの最大デバイス数は 6 台となります。スタックが DGS-3130-30TS/30S/30PS および DGS-3130-54TS/54S/54PS シリーズで構成されている場合、スタック数は、スタッキングコストと最大スタック数 9 によって制限されます。
スタックの組み合わせ例については、以下の表を参照してください。

組み合わせパターン番号	DGS-3130-30TS/30S/30PS デバイス数	DGS-3130-54TS/54S/54PS デバイス数	デバイス数 / スタック	スタッキングコスト
1	9	0	9	9
2	8	1	9	10
3	7	2	9	11
4	6	3	9	12
5	5	3	8	11
6	4	4	8	12
7	3	4	7	11
8	2	5	7	12
9	1	5	6	11
10	0	6	6	12

Duplex Chain 構成例

以下は、RJ-45 ケーブル、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。「2 ポート」または「4 ポート」スタッキング設定を使用しています。

■ **Duplex Chain 構成例（2 ポートスタック、10GBASE-T ポート使用）**

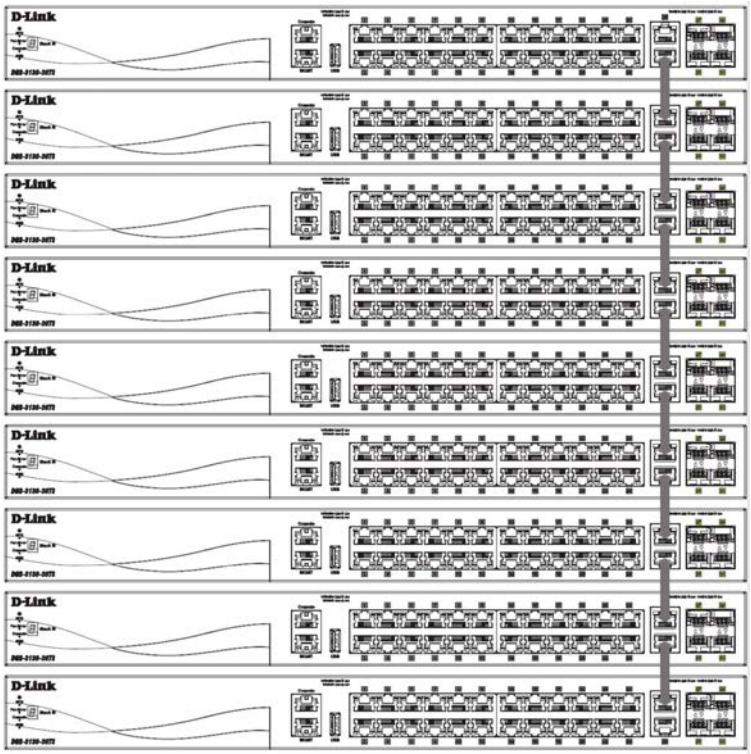


図 3-4　Duplex Chain でスタックされているスイッチ（2 ポートスタック /10GBASE-T）

■ **Duplex Chain 構成例（2 ポートスタック、SFP+ スロット使用）**

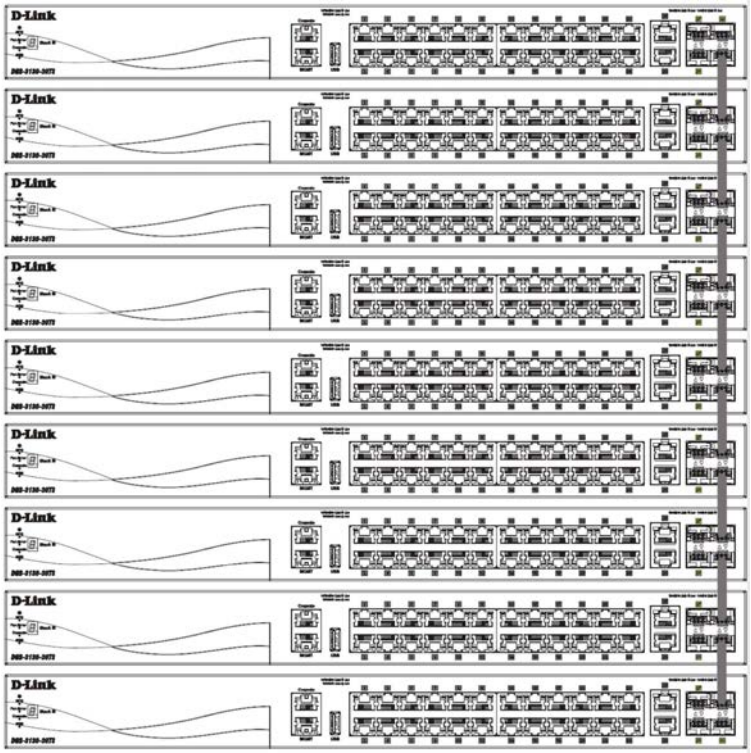


図 3-5　Duplex Chain でスタックされているスイッチ（2 ポートスタック /SFP+）

■ **Duplex Chain 構成例（4 ポートスタック、10GBASE-T ポートおよび SFP+ スロット使用）**

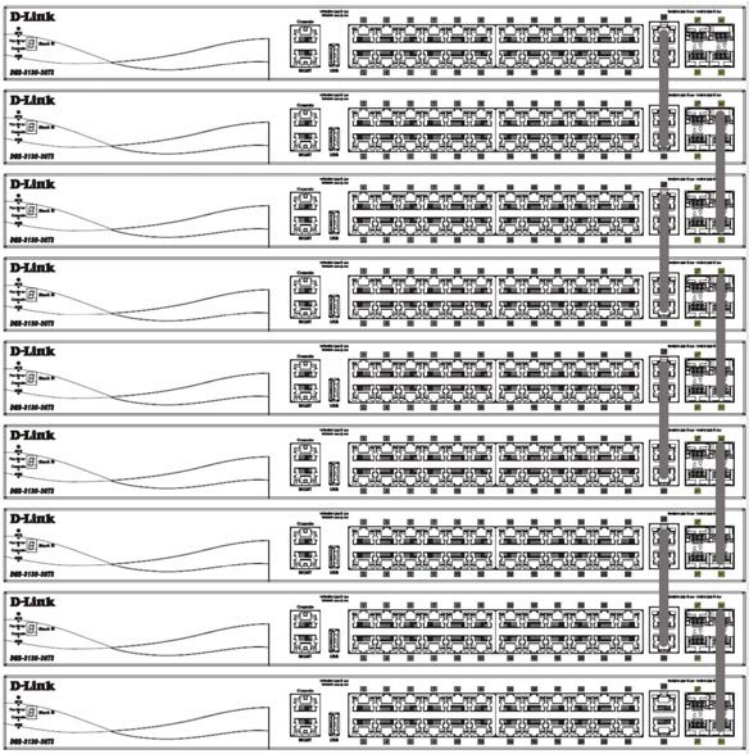


図 3-6　Duplex Chain でスタックされているスイッチ（4 ポートスタック /10GBASE-T および SFP+）

■ **Duplex Chain 構成例（4 ポートスタック、SFP+ スロット使用）**

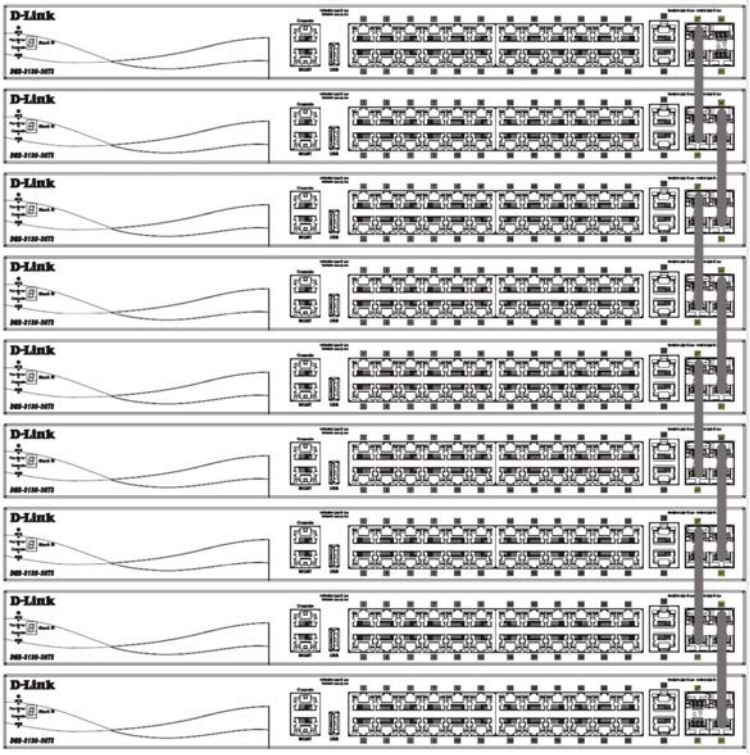


図 3-7　Duplex Chain でスタックされているスイッチ（4 ポートスタック /SFP+）

Duplex Ring 構成例

以下は、RJ-45 ケーブル、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。「2 ポート」または「4 ポート」スタッキング設定を使用しています。

■ **Duplex Ring 構成例（2 ポートスタック、10GBASE-T ポート使用）**

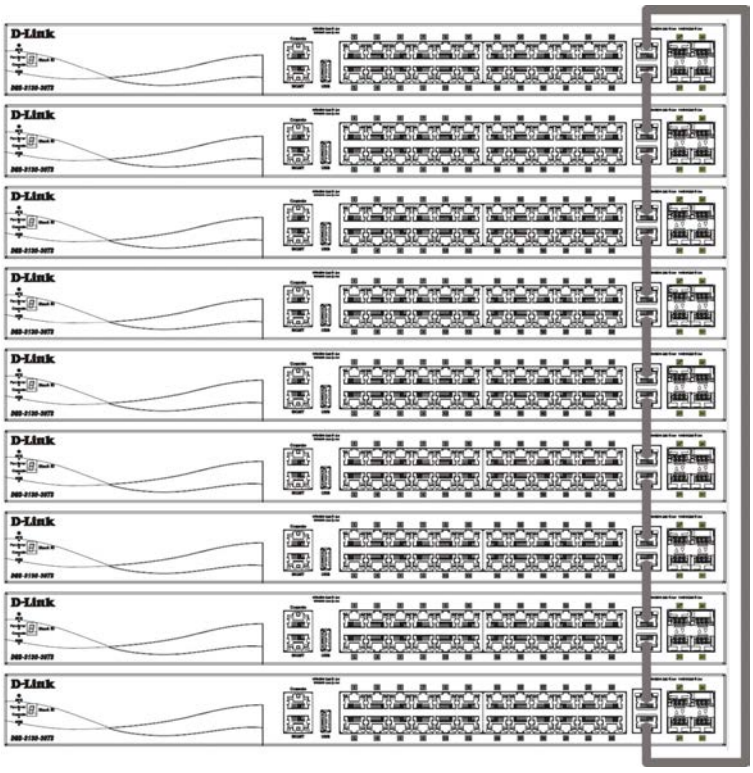


図 3-8　Duplex Ring でスタックされているスイッチ（2 ポートスタック /10GBASE-T）

■ **Duplex Ring 構成例（2 ポートスタック、SFP+ スロット使用）**

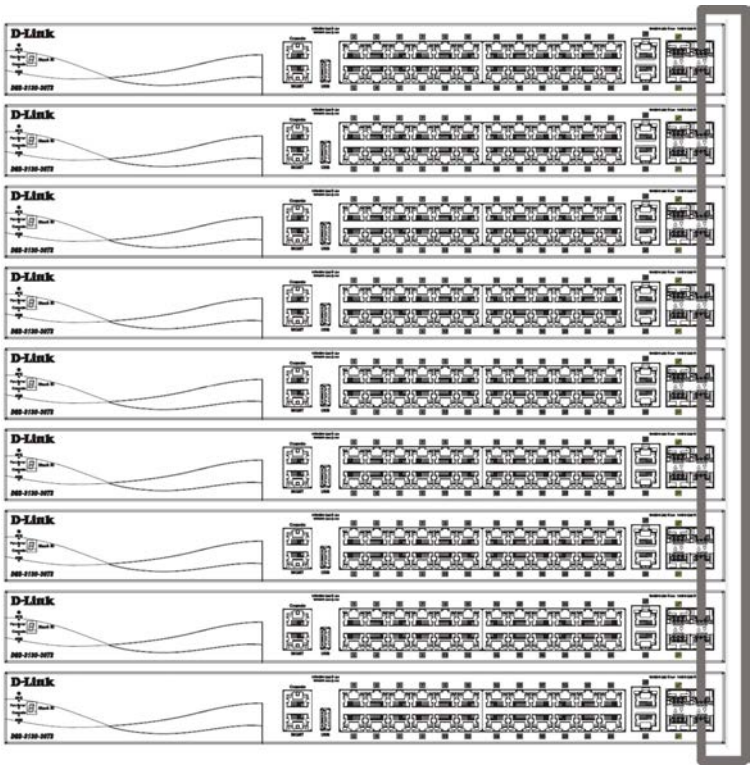


図 3-9　Duplex Ring でスタックされているスイッチ（2 ポートスタック /SFP+）

■ **Duplex Ring 構成例（4 ポートスタック、10GBASE-T ポートおよび SFP+ スロット使用）**

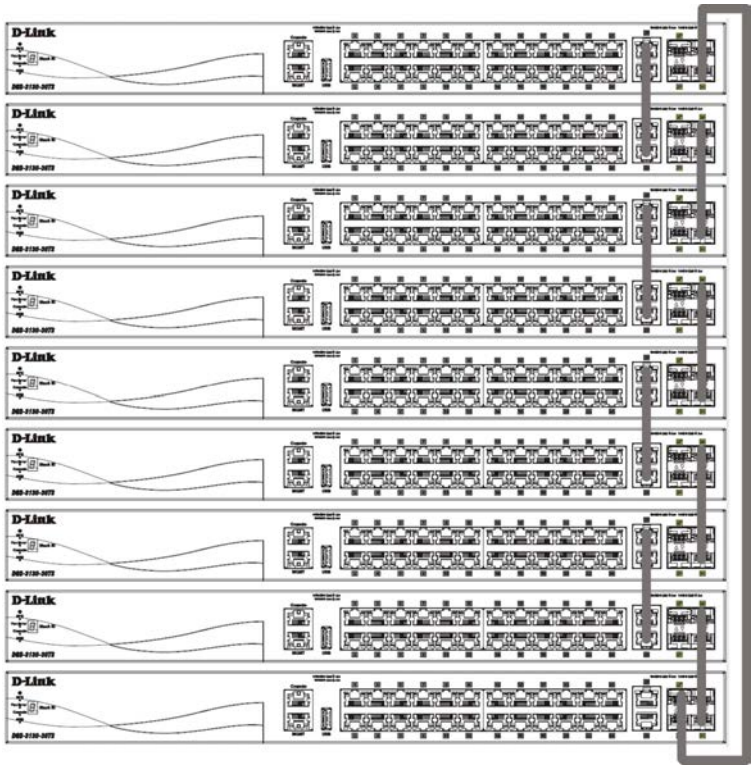


図 3-10　Duplex Ring でスタックされているスイッチ（4 ポートスタック /10GBASE-T および SFP+）

■ **Duplex Ring 構成例（4 ポートスタック、SFP+ スロット使用）**

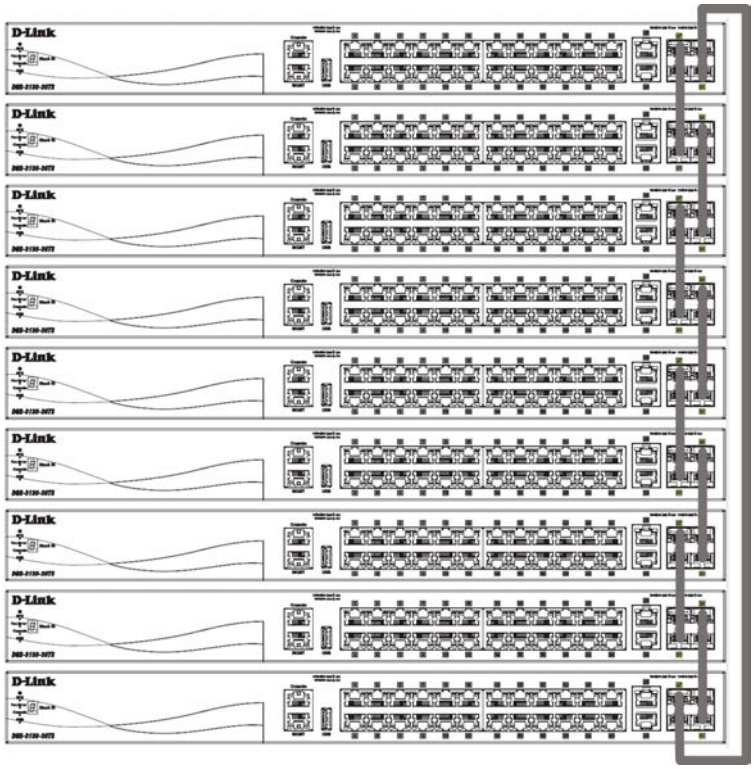


図 3-11　Duplex Ring でスタックされているスイッチ（4 ポートスタック /SFP+）

第 4 章　スイッチの管理について

- 「スイッチの管理方法」
- 「コンソールポートへの接続」
- 「管理（MGMT）ポートへの接続」
- 「コンソールポートへの接続」

スイッチの管理方法

Web GUI による管理

Microsoft® Internet Explorer などの Web ブラウザによって、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

■ アウトオブバンド管理

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、管理（MGMT）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

■ インバンド管理

スイッチ上の LAN ポートを使用して Telnet 接続によるインバンド管理を行うことも可能です。コマンドラインインタフェース（CLI）によりスイッチの全ての管理機能へのアクセスが可能です。コマンドについて詳しくは CLI マニュアルを参照ください。

コンソールポートへの接続

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」

コンソールへのログイン

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。
   初めてログインする場合は、なにも入力せず「Enter」を押します。

補足　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「ユーザアカウント / パスワードの設定」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。

ユーザアカウント / パスワードの設定

管理者レベルのユーザアカウントとパスワードを設定する方法について説明します。

注意　最初にログインしたユーザが自動的に管理者レベルの権限を取得します。スイッチに少なくとも 1 つの管理者レベルアカウントが作成されている必要があります。

注意　管理インタフェースへの不正なアクセスを防ぐために、ユーザ名とパスワードを持つユーザを作成することを強く推奨します。

```
Switch>enable
Switch#configure terminal
Switch(config)#username NewUser password 12345
Switch(config)#username NewUser privilege 15
Switch(config)#line console
Switch(config-line)#login local
Switch(config-line)#end
Switch#
```

1. 「`enable`」コマンドを入力し、Privileged EXEC モードにアクセスします。
2. 「`configure terminal`」コマンドを入力し、Global Configuration モードにアクセスします。
3. 「`username NewUser password 12345`」コマンドを入力し、ユーザ名「Administrator」、パスワード「12345」を指定します。
4. 「`username NewUser privilege 15`」コマンドを入力し、ユーザアカウントに権限レベル 15 を指定します。

権限レベルは 1 から 15 まで指定できます。「15」が最大、「1」が最小の権限レベルです。

5. 「line console」コマンドを入力し、LINE Configuration モードにアクセスします。
6. 管理インタフェースにアクセス可能なユーザアカウントが作成されました。
7. 「login local」コマンドを入力し、local line にログイン認証が必要となるように設定します。
8. 「end」コマンドを入力して、Privileged EXEC モードを終了します。

補足　パスワードの大文字と小文字は区別されます。
ユーザ名とパスワードは 32 文字以内の半角英数字で指定してください。

IP アドレスの設定

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> enable
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. 「enable」コマンドを入力し、Privileged EXEC モードにアクセスします。
2. 「configure terminal」コマンドを入力し、Global Configuration モードになります。
3. 「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。
「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

管理（MGMT）ポートへの接続

スイッチの前面または背面パネルには Out-of-Band（OOB）管理ポートがあります。このポートは、標準的なイーサネットケーブルを使用して PC に簡単に接続することが可能な RJ-45 ポートです。Web ブラウザもしくは Telnet クライアントを使用して、管理ポート経由でスイッチに接続します。

管理ポートを使用するには、イーサネットケーブルを使用して、スイッチ管理に使用するコンピュータのイーサネットインタフェースに接続します。IP アドレスの初期値は 192.168.0.1 で、サブネットマスクは 255.255.255.0 です。スイッチ管理に使用するコンピュータが、192.168.0.x サブネットで重複しない IP アドレスを持っていることを確認してください。

補足　Telnet 接続の場合、工場出荷時の設定ではパスワードの入力が必要となりますが、初期値ではパスワードが設定されていません。インバンド管理接続または管理ポートを使用して管理画面にアクセスし、Telnet のログイン方法および（または）パスワードを設定してください。

必要に応じてユーザ名とパスワードを入力し、「Enter」キーを押します。「Switch>」というコマンドプロンプトが表示されます。

以下のコマンドを実行し、管理ポートの IP 設定を参照します。

```
Switch#show ip interface mgmt 0

mgmt_ipif 0 is enabled, Link status is up
  IP address is 192.168.0.1/24
  Gateway is 0.0.0.0

Switch#
```

以下のコマンドを実行し、管理ポートの IP 設定を変更します。

```
Switch#configure terminal
Switch(config)#interface mgmt 0
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#
```

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。

補足　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。

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 GUI へのログイン
- Web GUI の画面構成
- Web GUI 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。

CLI を介して利用可能な多くの機能は、Web GUI からも利用することができます。 Internet Explorer、Mozilla Firefox、Google Chrome などの Web ブラウザを使用できます。

Web GUI へのログイン

スイッチの管理を行うには、はじめにコンピュータで Web ブラウザを起動し、本スイッチに定義した IP アドレスを入力します。ブラウザのアドレスバーに以下のように URL を入力します。例 : http://10.90.90.90（10.90.90.90 はスイッチの IP アドレス）



図 5-1　URL の入力

補足　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あわせるか、本スイッチを端末側の IP インタフェースにあわせてください。

補足　管理ポートを使用する場合は、工場出荷時の IP アドレス「192.168.0.1」を使用してアクセスすることができます。

以下のユーザ認証画面が表示されます。

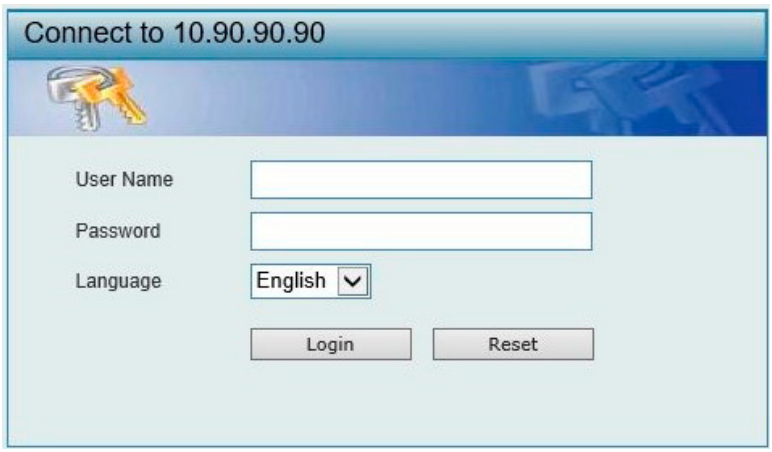


図 5-2　パスワード入力用画面

ユーザパスワードと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。

補足　スイッチとの「ログイン名 / パスワード」のやり取りには、不正アクセスを防止するために SSL/TLS が使用されます。

Web GUI の画面構成

Web GUI によるスイッチの設定または管理画面にアクセス、およびパフォーマンス状況やシステム状態をグラフィック表示で参照できます。

Web GUI のメイン画面について

Web GUI のメイン画面は 4 つのエリアで構成されています。

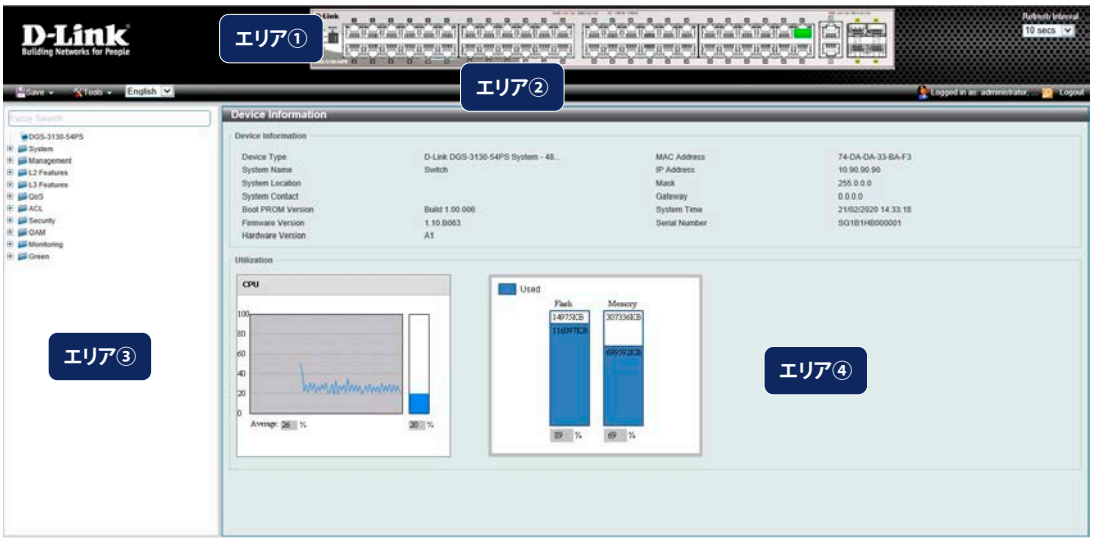


図 5-3　Web マネージャのメインページ

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。スイッチのポートや拡張モジュール、また、指定モードでのポートの動作も表示されます。ポートモニタなどの管理機能はここからアクセスする事も可能です。「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	「Save」メニュー /「Tools」メニューにアクセスするツールバーです。
エリア③	設定項目のメニューツリーが表示されます。フォルダを開き、ハイパーリンクのメニュー項目をクリックして該当カテゴリの詳細情報や設定項目を表示します。
エリア④	選択したスイッチ情報の表示と設定を行うことができます。

補足　「ASCII」文字のみサポートします。

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

Web GUI のメニュー構成

Web GUI で設定可能な機能は以下の通りです。

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設定します。
	Peripheral Settings（周辺機器設定）	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。
	PoE（PoE の管理）（DGS-3130-30PS/54PS）	DGS-3130-30PS/54PS の PoE 機能について設定を行います。
	System Log（ システムログ構成）	システムログの設定を行います。
	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 ACL 機能などで使用するスケジュールを定義します。
Management	Command Logging（コマンドログ設定）	コマンドログの出力設定を行います。
	User Accounts Settings（ユーザアカウント設定）	ユーザパスワードとアクセス権限を設定します。
	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の設定を行います。
	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。
	SNMP（SNMP 設定）	SNMP 設定を行います。
	RMON（RMON 設定）	SNMP 機能に対するリモートモニタリング (RMON) ステータスを設定します。
	Telnet/Web（Telnet/Web 設定）	スイッチの Telnet/Web 接続について設定します。
	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。
	IP Source Interface（IP ソースインタフェース）	IP ソースインタフェースの設定を行います。
	File System（ファイルシステム設定）	スイッチのファームウェア、コンフィグ、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)（仮想スタック設定（SIM））	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。
	PPPoE Circuit ID Insertion Global Settings（PPPoE Circuit ID 挿入設定）	PPPoE の Circuit ID 挿入を設定します。
	SD Card Management（SD カード管理）	USB ドライバストレージなどのリムーバブル機器の設定を行います。

※ サポート予定のため、使用できません。

メインメニュー	サブメニュー	説明
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（8802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。
	ERPS (G.8032) （イーサネットリングプロテクション設定）	「Ethernet Ring Protection Switching」(ERPS) の設定を行います。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。
	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 パケットの設定を行います。
	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 アドレス形式のスタティックルートを設定します。
	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。
	Route Preference（ ルート優先度設定）	ルート優先度を設定します。
	ECMP Settings（ECMP 設定）	Equal-Cost Multi-Path (ECMP) ルーティング設定を行います。ロードバランシングハッシュアルゴリズムの設定と、同じ宛先の複数パスエントリに対しネクストホップを決定する際に使用されます。
	IPv6 General Prefix （IPv6 汎用プリフィクス）	VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。
	RIP（Routing Information Protocol）※	RIP（Routing Information Protocol）は、距離ベクトル型のルーティングプロトコルです。
	RIPng（RIPng 設定）※	RIPng（Routing Information Protocol next generation）の設定を行います。RIPng は、ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルであり、IPv6 ベースのネットワーク用です。
	OSPF（OSPF 設定）※	OSPF 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。
	IP Route Filter（IP ルートフィルタ）	ルートマップの作成、更新を行います。
	Policy Route（ポリシールート設定）	ポリシーベースルーティングの設定、表示を行います。
	VRRP Settings（VRRP 設定）	VRRP（Virtual Routing Redundancy Protocol）は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です。
	VRRPv3 Settings（VRRPv3 設定）	VRRPv3 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。
	WRED（WRED 設定）	WRED（WRED 設定）の設定を行います。

メインメニュー	サブメニュー	説明
ACL	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。
	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 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 認証設定）	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 サーバの設定を行います。
	TACACS+（TACACS+ 設定）	TACACS+ サーバの設定を行います。
	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 アドレスとマッチしなかった 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。
	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）※（一部）	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を制限を行います。
	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。
	SFTP Server Settings（SFTP サーバ設定）	「Secure File Transfer Protocol」(SFTP) サーバの設定、表示を行います。
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）機能の設定を行います。

メインメニュー	サブメニュー	説明
Monitoring	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（RFC3176）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。
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。
Save	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	Firmware Upgrade & Backup （ファームウェアアップグレード＆バックアップ）	各種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）	各種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。
	Log Backup （ログファイルのバックアップ）	各種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。

※ サポート予定のため、使用できません。

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設定します。
Peripheral Settings（周辺機器設定）	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。
PoE（PoE の管理）（DGS-3130-30PS/54PS）	PoE 機能の設定、表示を行います。（DGS-3130-30PS/54PS のみ）
System Log（ システムログ構成）	システムログの設定を行います。
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 ACL 機能などで使用するスケジュールを定義します。

Device Information（デバイス情報）

本画面は、ログインを行うと自動的に表示される画面で、スイッチの主な設定情報を確認できます。本画面に戻るためには、メニューツリーの一番上にある製品名をクリックします。

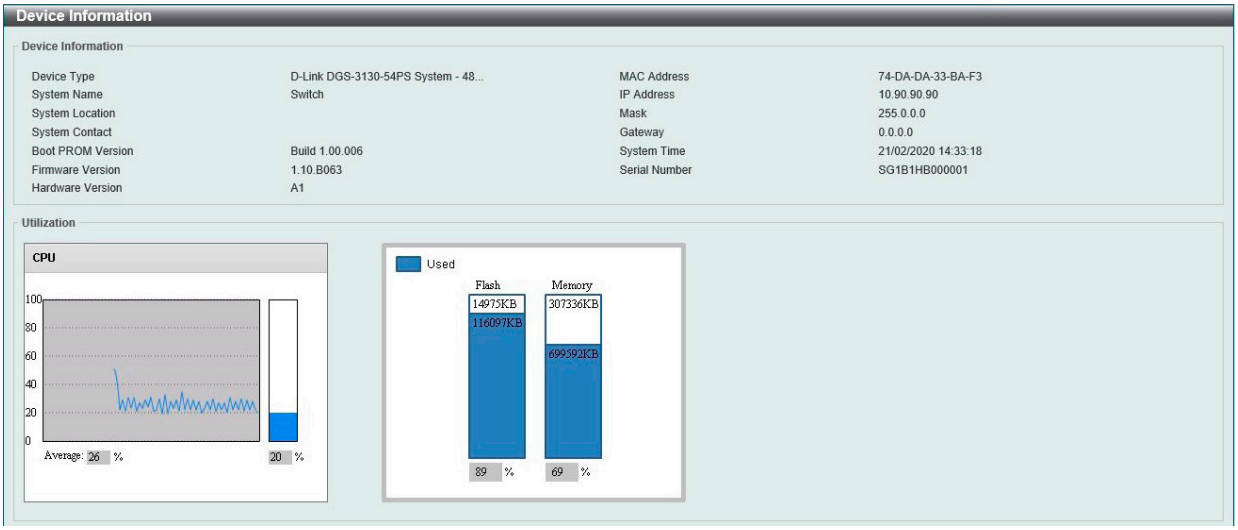


図 6-1　Device Information 画面

以下の項目が表示されます。

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

注意　本製品は、システム代表 MAC がラベルに記載されていて、Web UI には実際にマネージメントインターフェースが使用する MAC(システム代表 MAC+1) が表示されます。

System Information Settings（システム情報設定）

システム情報の設定と管理インタフェースの設定を表示します。

System > System Information 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。

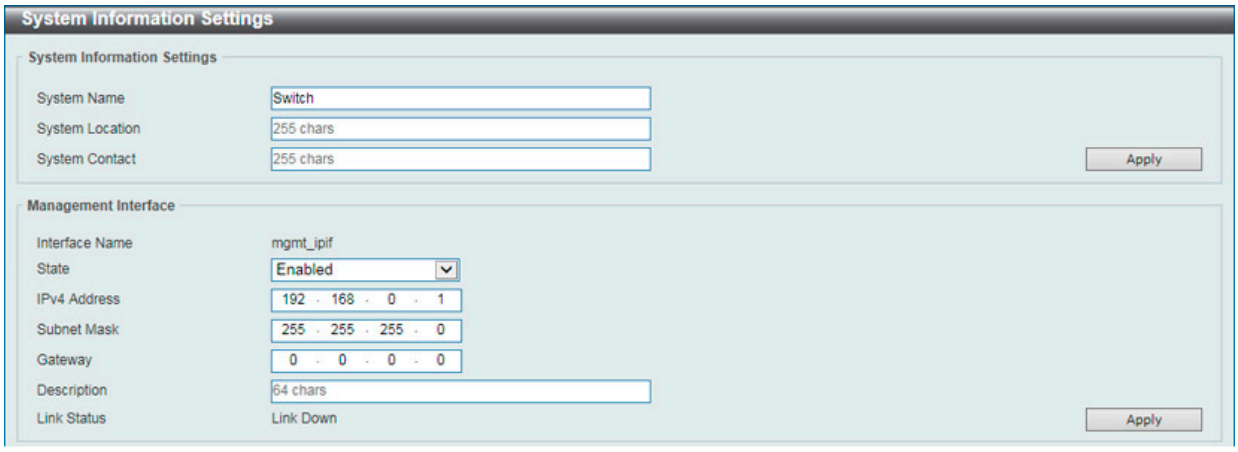


図 6-2　System Information Settings 画面

以下の項目が表示されます。

項目	説明
System Information Settings	
System Name	ユーザが定義するシステム名を設定します。
System Location	システムが現在動作している場所を定義します。
System Contact	スイッチの管理者情報を入力します。
Mangement Interface	
State	管理インタフェースを有効 / 無効に設定します。
IPv4 Address	管理インタフェースの IPv4 アドレスを指定します。
Subnet Mask	管理インタフェースのサブネットマスクを指定します。
Gateway	管理インタフェースのゲートウェイ IPv4 アドレスを指定します。
Description	管理インタフェースについての説明を指定します。（半角英数字 64 文字以内）

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

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 の順にメニューをクリックして、以下の画面を表示します。

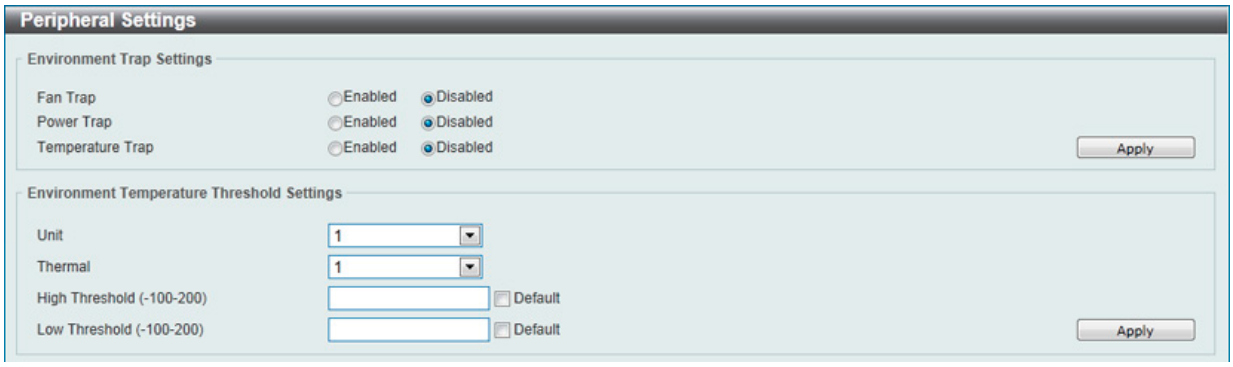


図 6-3　Peripheral Settings 画面

以下の項目が表示されます。

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。

項目	説明
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 Temperture Threshold Settings	
Unit	本設定を適用するユニットを選択します。
Thermal	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。

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

Port 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。

補足　「10M」は管理ポート（Mgmt 0）でのみ有効です。

System > Port Configuration > Port 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。

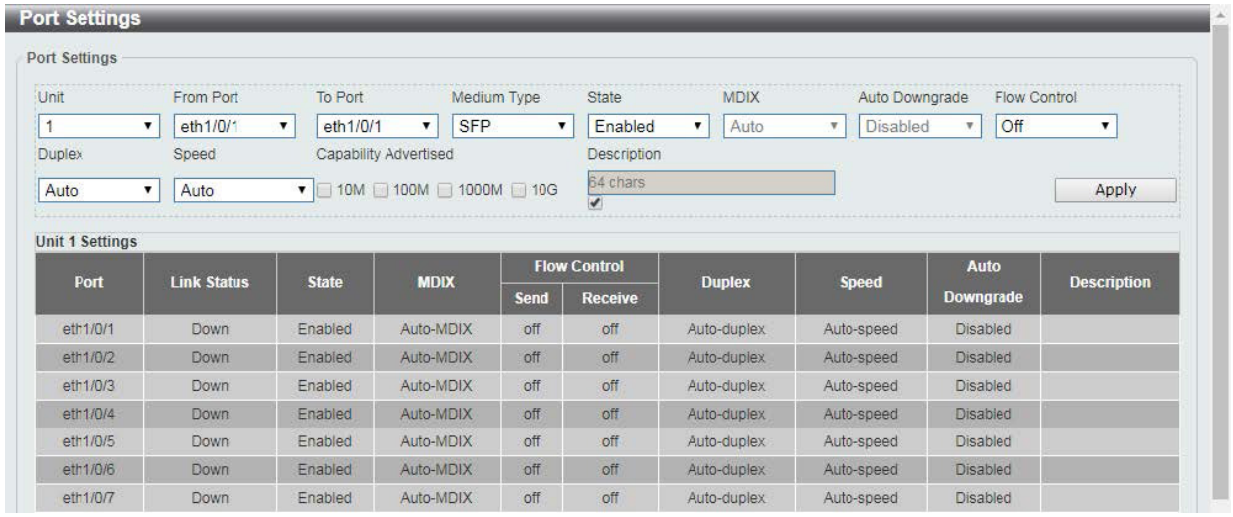


図 6-4　Port Settings 画面

以下の項目が表示されます。

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。
Medium Type	ポートメディアタイプを選択します。「SFP」オプションには SFP+ を使用する 10G 接続も含まれます。 • 選択肢：「RJ45」「SFP」
State	物理ポートの有効 / 無効を設定します。
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」- ケーブル接続に Normal を選択します。 •「Cross」- ケーブル接続に Cross を選択します。 「Normal」を選択すると、ポートは MDIX モードとなり、ストレートケーブルを通して PC のネットワークボードへ接続、またはクロスケーブルで別のスイッチのポート (MDI モード) に接続することができます。「Cross」を選択すると、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。
Auto Downgrade	リンクが有効なスピードを確立できなかった場合、アドバタイズスピードの自動的なダウングレードを有効 / 無効に設定します。
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。Full-Duplex のポートでは 802.3x フローコントロール、Half-Duplex のポートではバックプレッシャーによる制御を自動で行います。物理スタックのスイッチはサポートしていません。

項目	説明
Duplex	Duplex モードの選択を行います。半二重モードはサポートされていません。 • 選択肢：「Auto」「Full」
Speed	「Speed」欄でポートの速度を選択します。ここでは指定したポートを指定した速度のみで接続するように手動で設定します。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 • 選択肢：「Auto」「10M」「100M」「1000M」「1000M Master」「1000M Slave」「10G」「10G Master」「10G Slave」 「Auto」以外のオプションのポート設定は固定となります。 マスタ設定 (1000M Master) を行うと、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) は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「1000M Master」を設定すると、他方の接続は「1000M Slave」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。 • **「Auto」** - カッパーポートでは、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。光ファイバポートでは、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。10Mbps カッパー接続でのみ有効です。 • **「100M」** - ポート速度を 100Mbps に固定します。100Mbps カッパー接続でのみ有効です。 • **「1000M」** - ポート速度を 1Gbps に固定します。1Gbps 光ファイバ接続でのみ有効です。 • **「1000M Master」** - ポート速度を 1Gbps に固定し、マスタとして指定して送受信のタイミングについての動作を制御します。1Gbps カッパー接続でのみ有効です。 • **「1000M Slave」** - ポート速度を 1Gbps に固定し、スレーブとして指定して送受信のタイミングについての動作を制御します。1Gbps カッパー接続でのみ有効です。 • **「10G」** - ポート速度を 10Gbps に固定します。10Gbps 光ファイバ接続でのみ有効です。 • **「10G Master」** - ポート速度を 10Gbps に固定し、マスタとして指定して送受信のタイミングについての動作を制御します。10Gbps カッパー接続でのみ有効です。 • **「10G Slave」** - ポート速度を 10Gbps に固定し、スレーブとして指定して送受信のタイミングについての動作を制御します。10Gbps カッパー接続でのみ有効です。
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	ポートの説明を入力します。（64 文字以内）

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

注意 Duplex Half の指定はできません。

注意 ハードウェア制限により接続先の相手が「10M/Half」でネゴシエートする場合や、「10Mbps-Shared-HUB」である場合はリンクアップしません。

注意 speed auto-downgrade はサポートされません。

注意 ハードウェア制限により 10G での auto-negotiation 情報は表示できません。

注意 Interface の設定において、duplex 固定、speed auto (既定) の組み合わせでは Link Up しない場合があります。duplex を変更する場合は、speed についても適切な値を設定してください。

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。

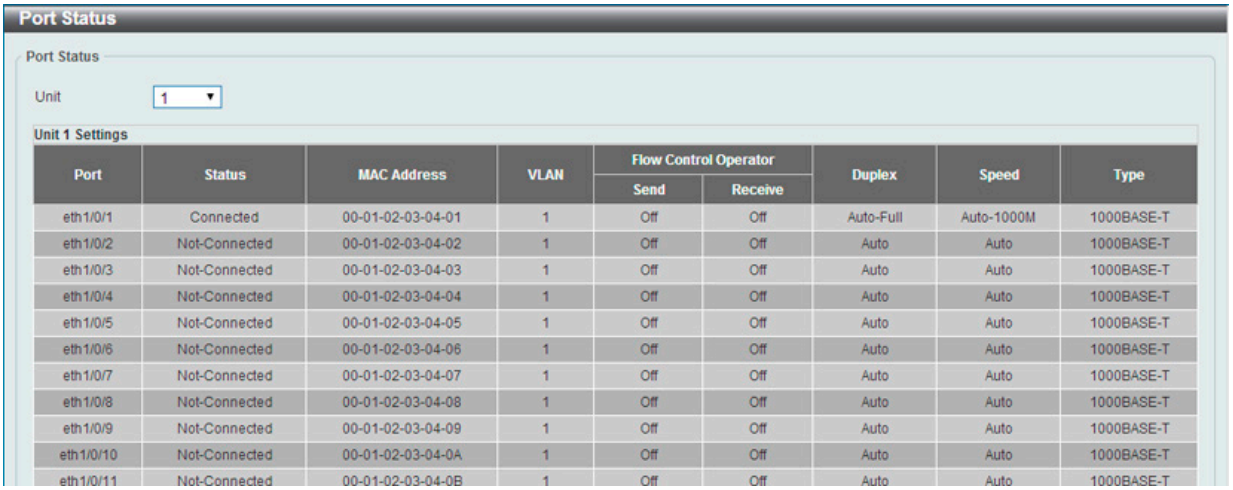


図 6-5　Port Status 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

Port GBIC

スイッチの各物理ポートの 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。

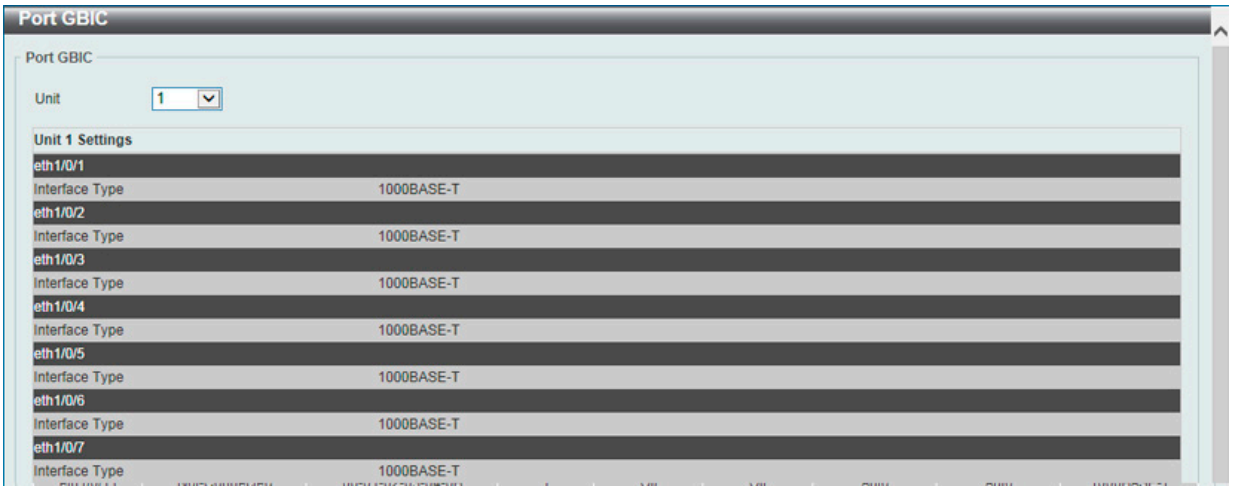


図 6-6　Port GBIC 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

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しい情報を表示します。

System > Port Configuration > Port Auto Negotiation 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。

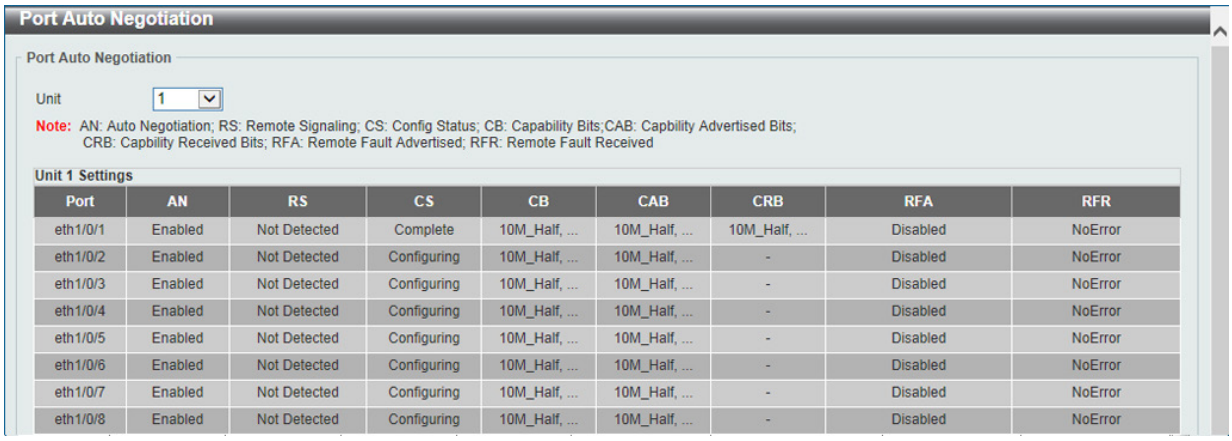


図 6-7　Port Auto Negotiation Information 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

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

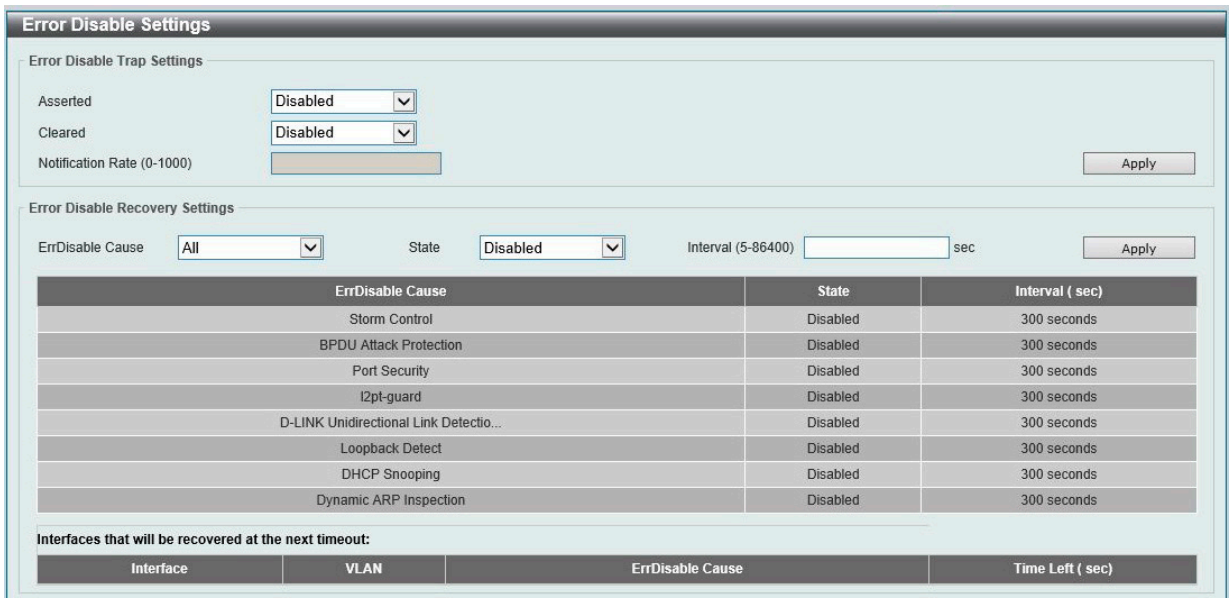


図 6-8　Port Error Disabled 画面

以下の項目が表示されます。

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

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

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

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

項目	説明
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」「D-LINK Unidirectional Link Detection」
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時間を指定します。 • 設定可能範囲：5-86400（秒）

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

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。有効にすると、最大 9,216 バイトを持つジャンボフレーム (1518 バイトの標準イーサネットフレームより大きいサイズのフレーム) の送信が可能になります。

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。

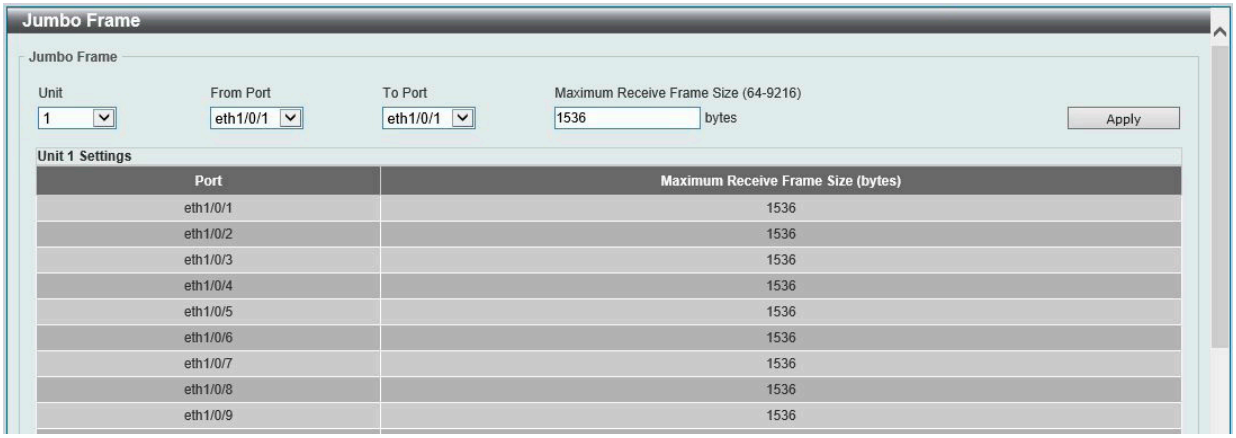


図 6-9　Jumbo Frame Settings 画面

以下の項目が表示されます。

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。
Maximum Receive Frame Size	スイッチのジャンボフレーム機能の最大値を指定します。 • 設定可能範囲：64 -9216（Bytes） • 初期値：1536（Bytes）

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

PoE（PoE の管理）（DGS-3130-30PS/54PS）

DGS-3130-30PS/54PS は IEEE の 802.3af と IEEE802.3at 規格の PoE 機能をサポートしています。対応ポートは 30W までの PoE をサポートしています。カテゴリ 5 以上の UTP イーサネットケーブル経由で PoE 受電機器に約 48VDC 電力を供給できます本スイッチは PSE pinout Alternative A に準拠しており、電力はピン 1、2、3、および 6 を通じて供給されます。本スイッチは全ての D-Link 802.3af 対応デバイスと接続できます。
本スイッチでは次の PoE 機能を使用することができます。

- Auto-discovery 機能は PD(受電機器) に自動的に電力を供給します。
- Auto-disable 機能は次のいずれかの状態となった場合に動作します。
  - システム合計の消費電力がシステム電力の上限を超えている
  - 各ポートの消費電力がポートの電力の上限を超えている
- Active circuit 防止機能は、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。

図 6-10　802.3af/at 準拠の受電 / 供給電力一覧

クラス	受電機器の最大受信電力	PSE によるの最大供給電力
0	12.95W	16.2W
1	3.84W	4.2W
2	6.49W	7.4W
3	12.95W	16.2W
4	25.5W	31.6W

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 6-11　PoE System 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Usage Threshold	ログの記録や通常の通知送信を実行するしきい値を指定します。 • 設定可能範囲：1-99（%）
Policy Preempt	電力供給不足となった場合に、優先度の低い既存の電力供給デバイス（PD）接続を解除して、優先度の高い新規接続のデバイスに電力を割り当てる機能を有効 / 無効に設定します。
Trap State	PoE のトラップ送信を有効 / 無効に設定します。

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

詳細情報の表示

「Show Detail」ボタンをクリックすると、画面下部に詳細情報が表示されます。

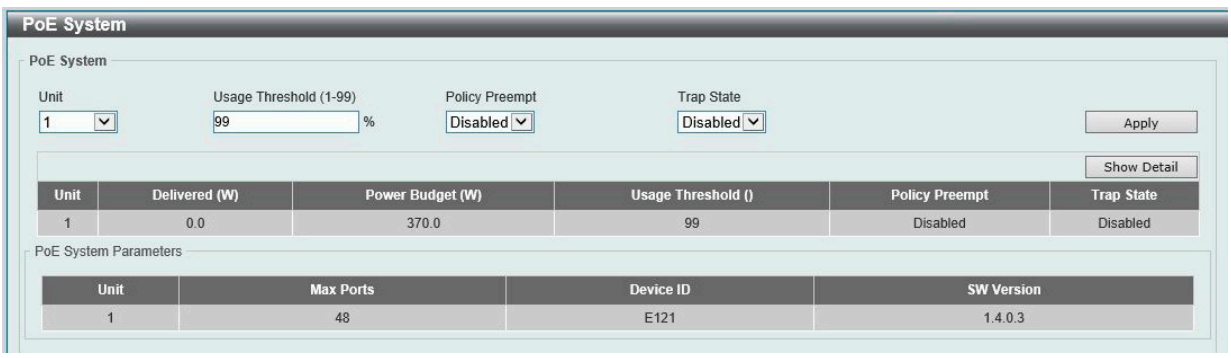


図 6-12　PoE System（Show Detail）画面

PoE Status（PoE ステータス）

各ポートの PoE ステータスの表示と概要の設定を行います。

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

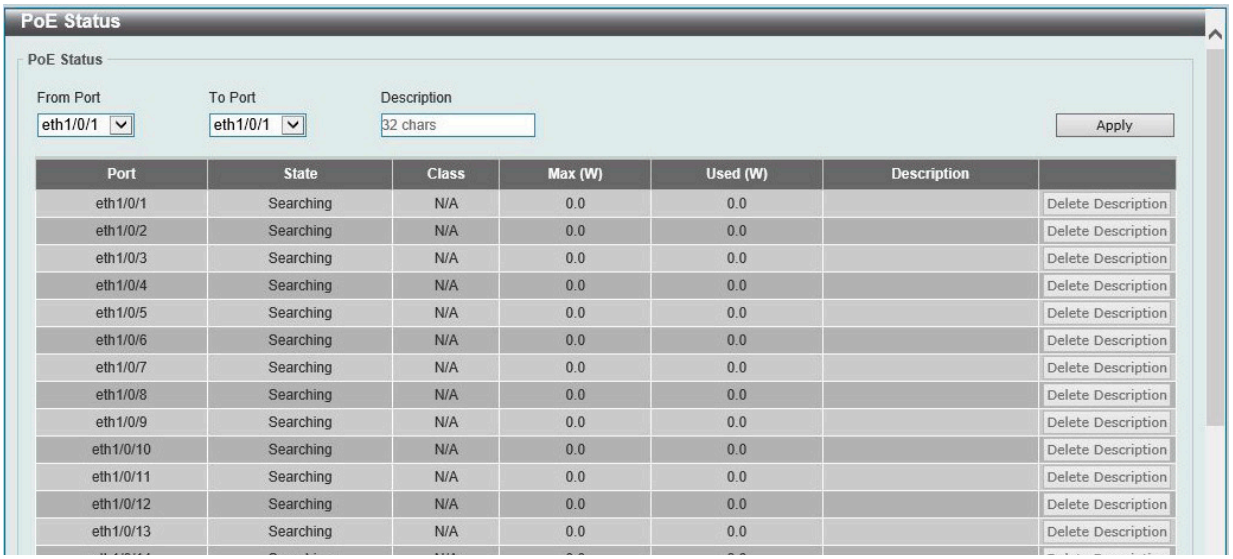


図 6-13　PoE Status 画面

以下の項目が表示されます。

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中の PD の概要について入力します。（32 文字以内）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete Description」ボタンをクリックして、概要を削除します。

PoE Configuration（PoE ポート設定）

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

補足　IEEE802.3at PD への給電に失敗する場合は、次の点を確認してください。

- 対象の PD デバイスが IEEE802.3at に準拠しているのかを確認する
- 対象のポートを 30W に手動設定する

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

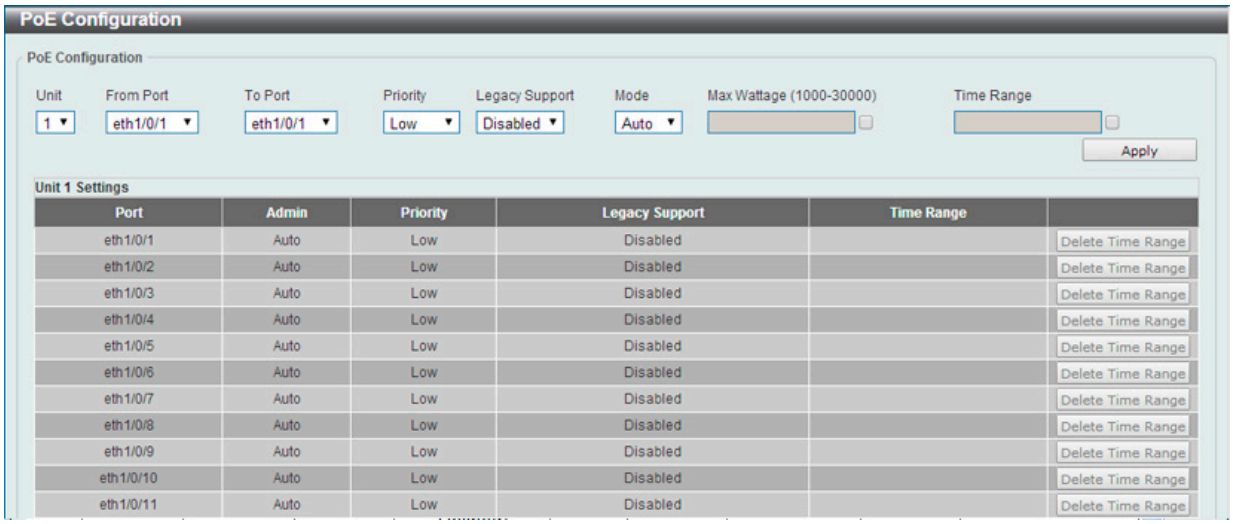


図 6-14　PoE Configuration 画面

以下の項目が表示されます。

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。
Priority	ポートの優先度を指定します。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することができます。 • 選択肢：「Critical（重大）」「High（高）」「Low（低）」
Legacy Support	レガシー PD へのサポートを有効 / 無効に設定します。
Mode	PoE ポートの電力管理モードを選択します。 • 「Auto」- PD の自動検出と電力供給を行います。 • 「Never」- PD に電力供給を行いません。
Max Wattage	上記「Mode」で「Auto」を選択した場合、本オプションが表示されます。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数（W）を指定します。数値を指定しない場合は PD のクラスは供給可能な最大の電力で指定されます。 • 設定可能範囲：1000-30000（mW）
Time Range	上記「Mode」で「Auto」を選択した場合、本オプションが表示されます。 ポートの PoE 機能を有効にする時間設定を行います。チェックボックスにチェックを入れ、タイムレンジの名前を指定します。 ポートは設定したタイムレンジの時間内のみ給電を行います。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete Time Range」ボタンをクリックして、該当ポートからタイムレンジを削除します。

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。

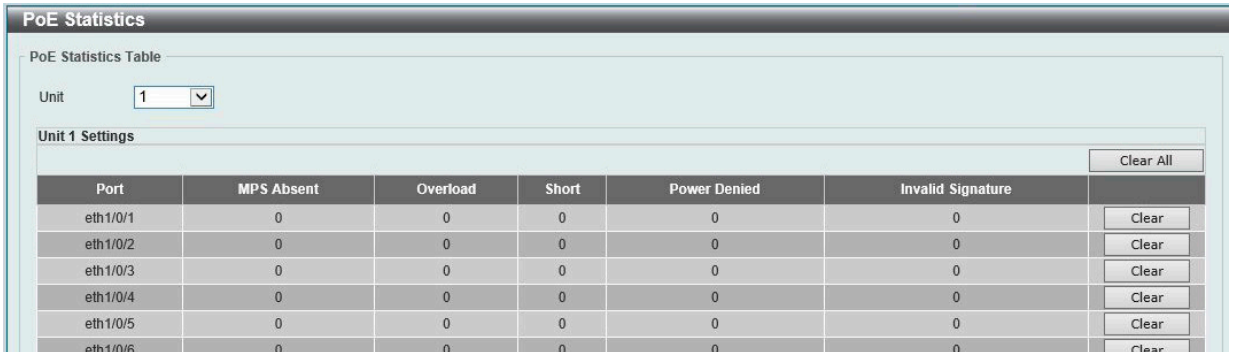


図 6-15　PoE Statistics 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

「Clear」ボタンをクリックして、該当ポートから PoE 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 PoE 統計情報を削除します。

PoE Measurement（PoE 測定）

PoE の測定情報を表示します。

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

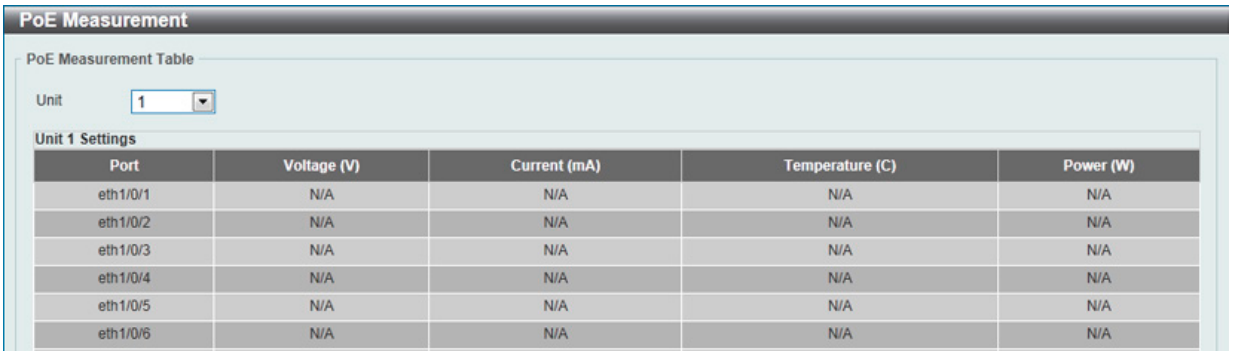


図 6-16　PoE Measurement 画面

以下の項目が表示されます。

項目	説明
Unit	表示を適用するユニットを選択します。

PD Alive（PD アライブ設定）

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

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

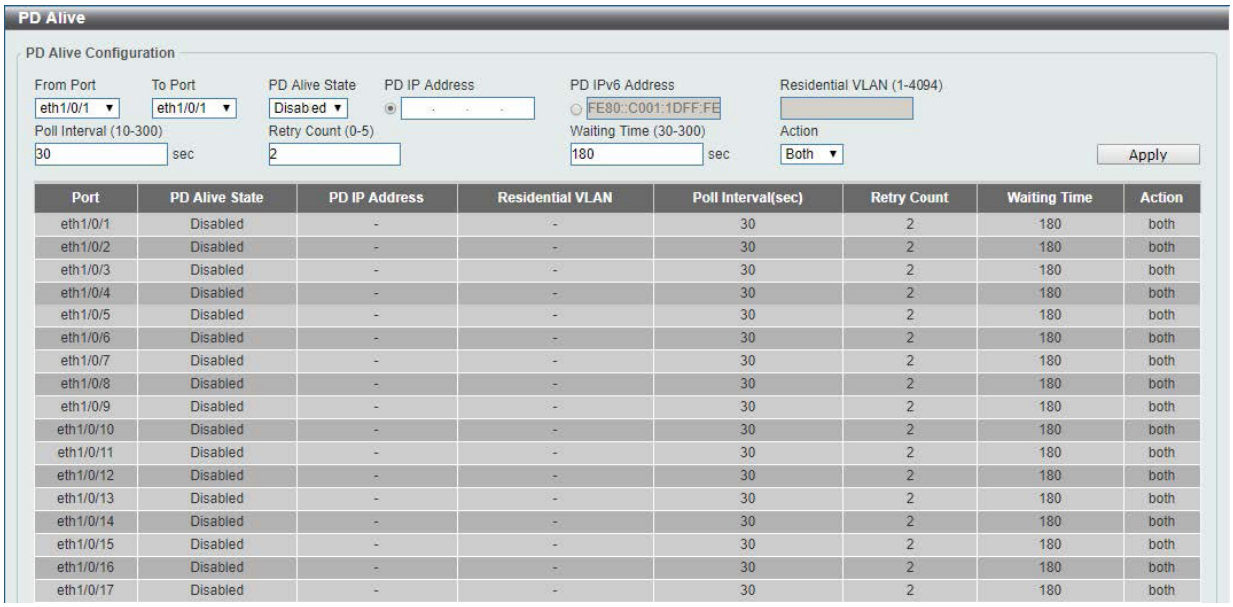


図 6-17　PD Alive 画面

以下の項目が表示されます。

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。
PD Alive State	PoE アライブ機能を有効 / 無効にします。
PD IP Address	PD の IPv4 アドレスを指定します。
PD IPv6 Address	PD の IPv6 アドレスを指定します。
Poll Interval	ポールインターバルを指定します。指定の PD の状況を確認する Ping 送信の間隔になります。 • 設定可能範囲：10-300（秒）
Retry Count	再試行回数を指定します。指定の PD からの応答がなかった際に Ping を再送信する回数になります。 • 設定可能範囲：0-5（回）
Waiting Time	待機時間を指定します。指定の PD が再起動から回復するまでスイッチが待つ時間になります。 設定可能範囲：30-300（秒）
Action	実行するアクションを指定します。 • 「Reset」- PoE ポートをリセットします。 • 「Notify」- 管理者に通知するログとトラップを送信します。 • 「Both」- 管理者に通知するログとトラップを送信し、PoE ポートをリセットします。

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

System Log（システムログ構成）

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）

システムログ機能を有効または無効にし、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選択します。

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。

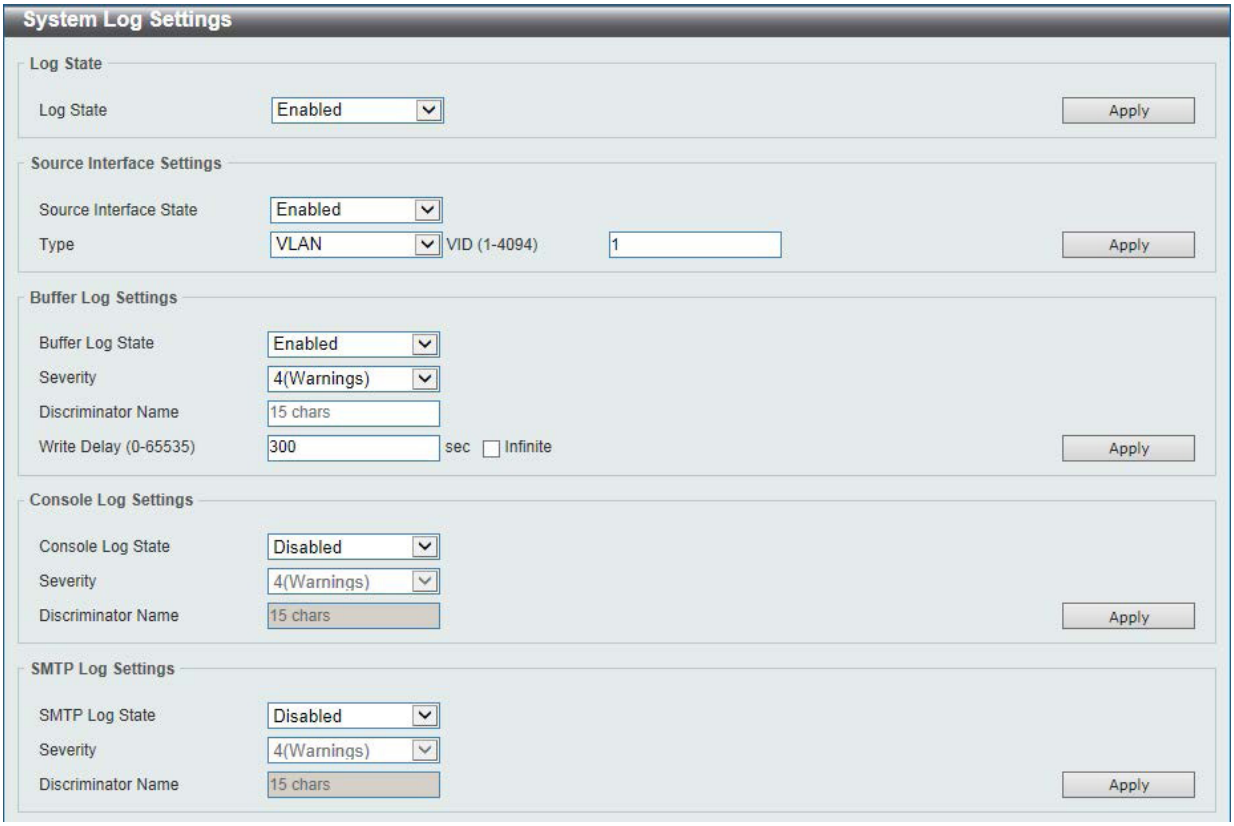


図 6-18　System Log Settings 画面

以下の項目が表示されます。

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 / 無効に設定します。
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 / 無効に設定します。
Type	インタフェースの種類を選択します。 • 選択肢：「Loopback」「Mgmt」「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）、0（Mgmt 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トは初期設定のまま動作します。
Severity	ログ出力される情報のレベルを選択します。 • 選択肢：「0：Emergencies」（緊急）、「1：Alerts」（警告）、「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）バッファログメッセージのフィルタリングで使用されます。
Write Delay	フラッシュにロギングバッファを定期的に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。

項目	説明
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：「0：Emergencies」（緊急）、「1：Alerts」（警告）、「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）コンソールログメッセージのフィルタリングで使用されます。
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：「0：Emergencies」（緊急）、「1：Alerts」（警告）、「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）SMTP ログメッセージのフィルタリングで使用されます。

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

System Log 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。

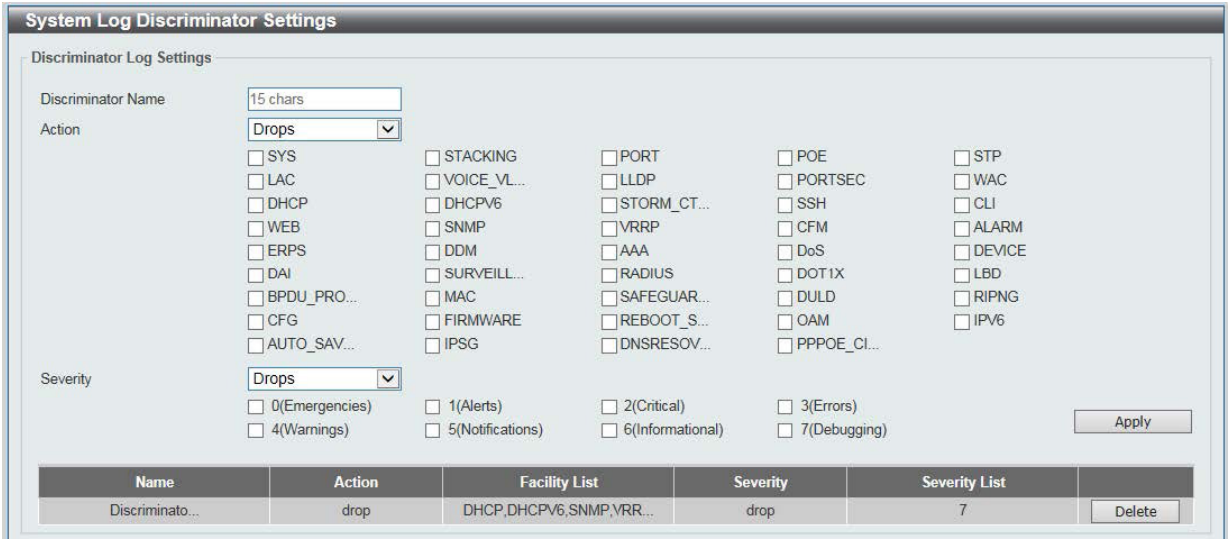


図 6-19　System Log Discriminator Settings 画面

以下の項目が表示されます。

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）
Facility	ファシリティに対する動作を選択し、ファシリティの種類にチェックを入れます。 • 選択肢：「Drops（破棄）」「Includes（含める）」
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」（警告）、「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）

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

システムログサーバの設定を表示、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。

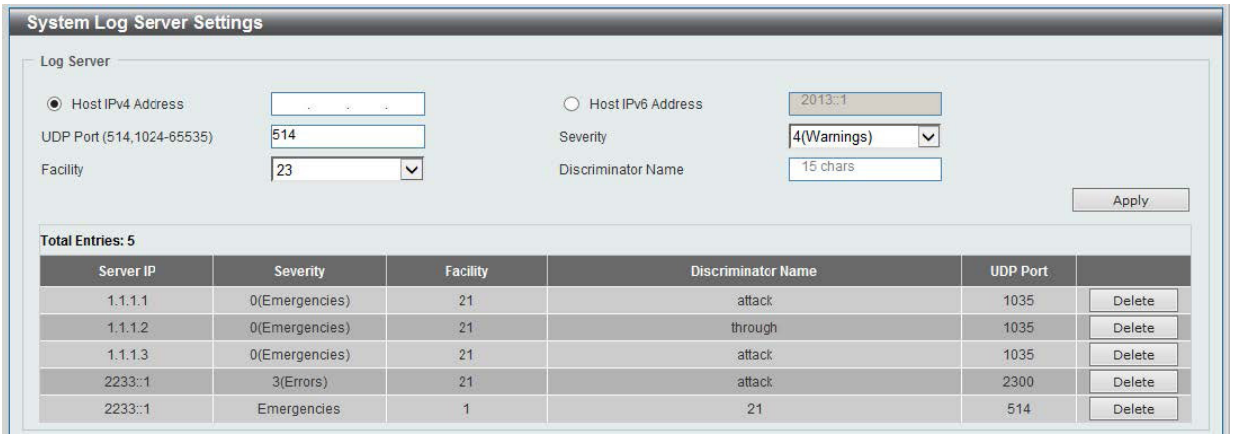


図 6-20　System Log Server Settings 画面

本画面には次の項目があります。

項目	説明
Host IPv4 Address	ログを記録するサーバの IPv4 アドレスを設定します。
Host IPv6 Address	ログを記録するサーバの IPv6 アドレスを設定します。
UDP Port	ログを送信するサーバの UDP ポートを設定します。 • 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:「0:Emergencies」（緊急）、「1:Alerts」（警告）、「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）
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
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。

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）

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

System Log（Syslog ログ）

システムログの表示および削除を行います。

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。

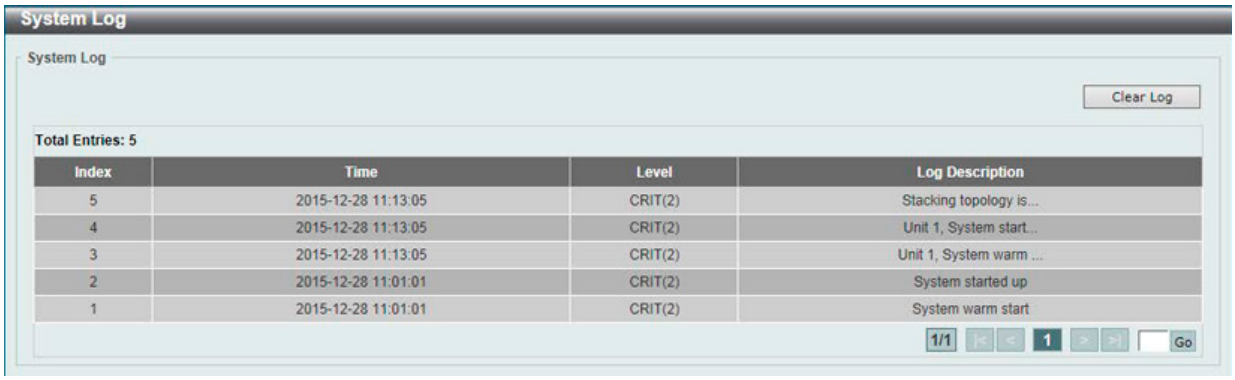


図 6-21　System Log 画面

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

System Attack Log（システムアタックログ）

システムの攻撃ログの閲覧 / 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。

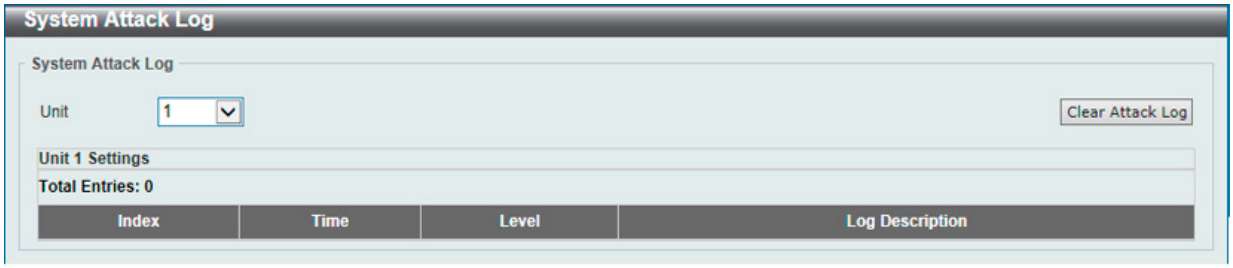


図 6-22　System Attack Log 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

「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）

SNTP（Simple Network Time Protocol）は、ネットワークを利用してスイッチの時刻を同期するために使用されます。

Clock Settings（時間設定）

スイッチに時刻を設定します。

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 6-23　Time Settings 画面

以下の項目が表示されます。

項目	説明
Time（HH:MM:SS）	現在のシステム時刻を時 : 分 : 秒（24 時間制）で設定します。例えば、午後 9 時であれば 21:00:00 と指定します。
Date（DD/MM/YYYY）	現在の年月日を入力します。項目のフォーマットは日 / 月 / 年です。

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

Time Zone Settings（タイムゾーン設定）

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

System > Time and SNTP > Time Zone 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。

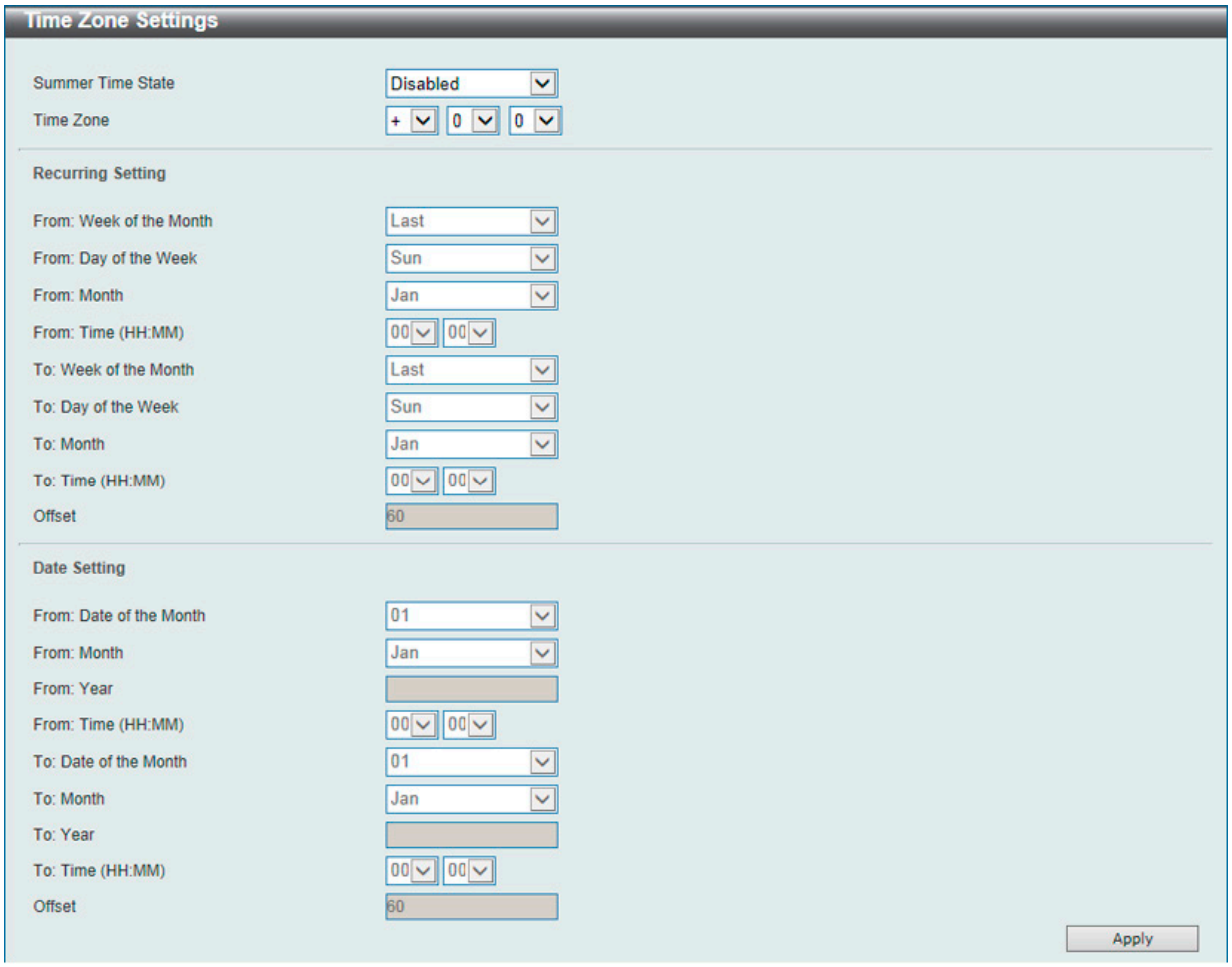


図 6-24　Time Zone Settings 画面

以下の項目が表示されます。

項目	説明
Summer Time State	デバイスに設定するサマータイムの種類を設定します。 • 「Disabled」- サマータイムを無効にします。（初期値） • 「Recurring Setting」- サマータイムを周期的に有効にします。このオプションでは、指定月の指定曜日にサマータイムが開始 / 終了します。 • 「Date Setting」- サマータイムを日付指定で有効にします。このオプションでは、指定年月日にサマータイムが開始 / 終了します。
Time Zone	UTC からのタイムゾーンを選択します。
Recurring Setting	
From: Week Of The Month	月の第何週から DST が始まるかを設定します。 • 「First」- 月の最初の週に設定します。 • 「Second」- 月の 2 番目の週に設定します。 • 「Third」- 月の 3 番目の週に設定します。 • 「Fourth」- 月の 4 番目の週に設定します。
From: Day Of Week	サマータイムが開始する曜日を指定します。 • 選択肢：「Sun」「Mon」「Tue」「Web」「Thurs」「Fri」「Sat」
From: Month	サマータイムが開始する月を指定します。 • 選択肢：「Jan」「Feb」「Mar」「Apr」「May」「Jun」「Jul」「Aug」「Sep」「Oct」「Nov」「Dec」
From: Time (HH:MM)	サマータイムが開始する時間を指定します。
To: Week Of The Month	月の第何週でサマータイムが終わるかを設定します。 • 「First」- 月の最初の週に設定します。 • 「Second」- 月の 2 番目の週に設定します。 • 「Third」- 月の 3 番目の週に設定します。 • 「Fourth」- 月の 4 番目の週に設定します。

項目	説明
To: Day Of Week	サマータイムが終了する曜日を指定します。
To: Month	サマータイムが終了する月を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間（オフセット）を指定します。 • 選択肢：「30」「60」「90」「120」 • 初期値：60（分）
Date Setting	
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。（毎年）
From: Month	サマータイムが開始する月を指定します。（毎年）
From: Year	サマータイムが開始する年を指定します。
From: Time (HH:MM)	サマータイムが開始する時間を指定します。（毎年）
To: Date of the Month	サマータイムが終了する日にちを指定します。（毎年）
To: Month	サマータイムが終了する月を指定します。（毎年）
To: Year	サマータイムが終了する年を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。（毎年）
Offset	サマータイムに追加する時間（オフセット）を指定します。 • 選択肢：「30」「60」「90」「120」 • 初期値：60（分）

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

SNTP Settings（SNTP 設定）

SNTP（Simple Network Time Protocol ）はインターネット経由でシステム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。

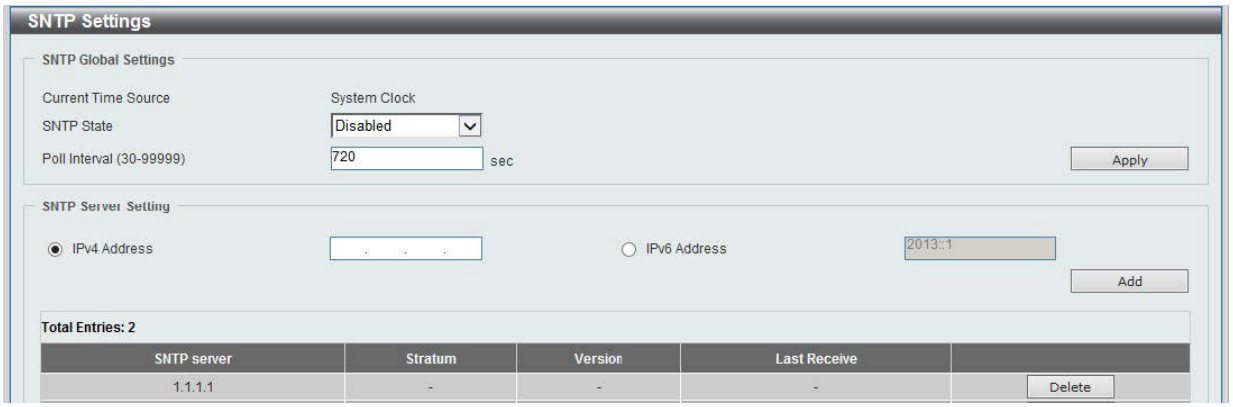


図 6-25　SNTP Settings 画面

以下の項目が表示されます。

SNTP Global Settings（SNTP グローバル設定）

項目	説明
Current Time Source	現在の日付と時刻の提供元を表示します。
SNTP State	SNTP を有効 / 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）

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

SNTP Server Settings（SNTP サーバ設定）

項目	説明
IPv4 Address	SNTP 情報の取得元であるサーバの 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。

「Add」ボタンをクリックして、設定内容に基づく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。

補足　SNTP 機能において、再起動した後、次回の Interval まで同期は行われません。

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。

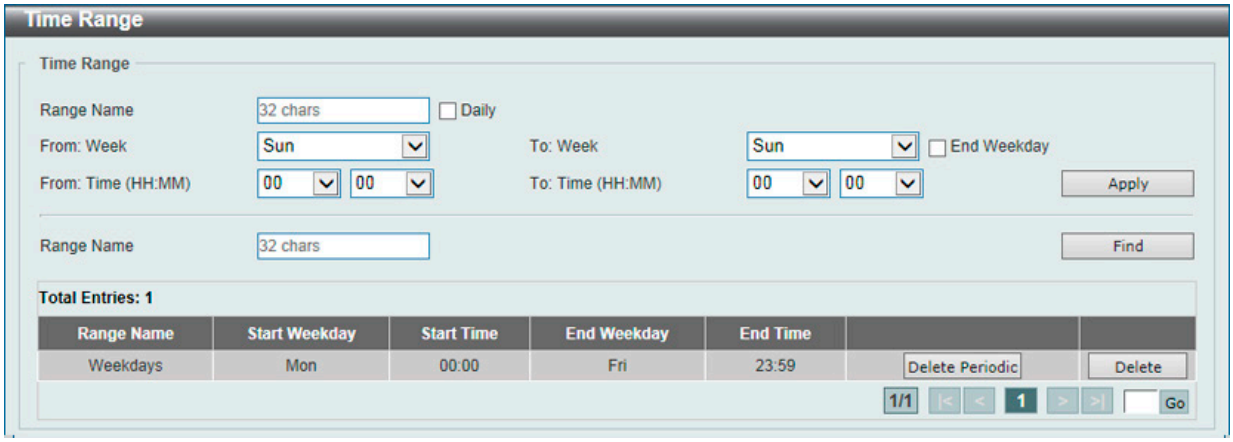


図 6-26　Time Range 画面

以下の項目が表示されます。

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

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。
「Delete Periodic」ボタンをクリックして、定期エントリを削除します。

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

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）	コマンドログの出力設定を行います。
User Accounts Settings（ユーザアカウント設定）	ユーザパスワードとアクセス権限を設定します。
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の設定を行います。
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。
SNMP（SNMP 設定）	SNMP 設定を行います。
RMON（RMON 設定）	SNMP 機能に対するリモートモニタリング (RMON) ステータスを設定します。
Telnet/Web（Telnet/Web 設定）	スイッチの Telnet/Web 接続について設定します。
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。
IP Source Interface（IP ソースインタフェース）	IP ソースインタフェースの設定を行います。
File System（ファイルシステム設定）	スイッチのファームウェア、コンフィグ、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）（仮想スタック設定（SIM））	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。
PPPoE Circuit ID Insertion Global Settings（PPPoE Circuit ID 挿入設定）	PPPoE の Circuit ID 挿入を設定します。
SD Card Management（SD カード管理）	USB ドライバストレージなどのリムーバブル機器の設定を行います。

※サポート予定のため、使用できません。

Command Logging（コマンドログ設定）

コマンドログ設定を表示および参照します。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。スイッチの設定または操作で変更を引き起こさないコマンド（例 : show）はログに出力されません。「save」コマンドは設定ファイルを変更するため、ログに出力されます。

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。

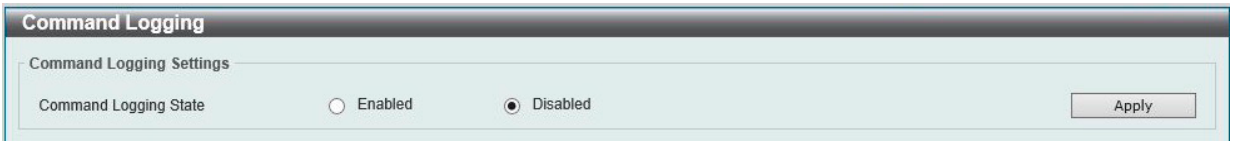


図 7-27　Command Logging 画面

以下の項目が表示されます。

項目	説明
Command Logging State	ラジオボタンを使用して機能を有効 / 無効に設定します。

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

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。

注意　初期値ではユーザアカウントは設定されていません。

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

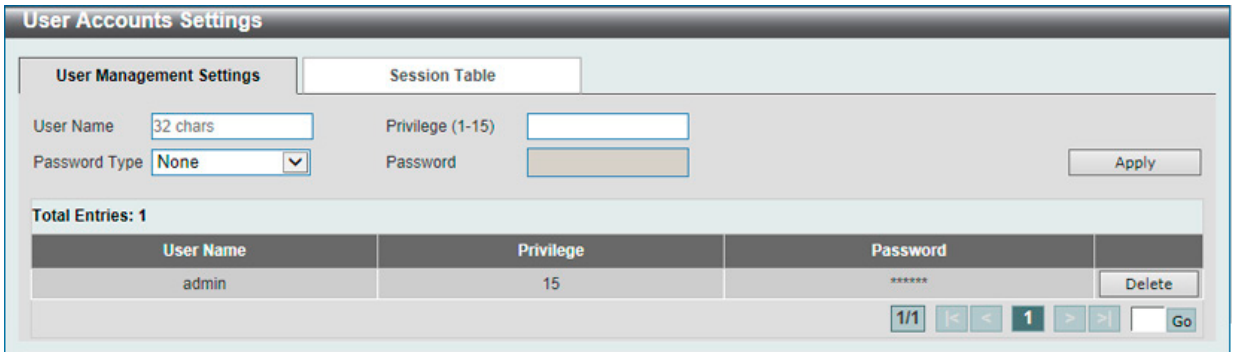


図 7-1　User Accounts Settings - User Management Settings 画面

以下の項目が表示されます。

項目	説明
User Name	ユーザ名を定義します。（半角英数字 32 文字以内）
Privilege	アカウントの権限レベルを指定します。 • 設定可能範囲：1-15
Password Type	アカウントで使用する暗号化の方法を選択します。 • 選択肢：「None」「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」
Password	アカウントで使用するパスワードを入力します。

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

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

Session Table

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

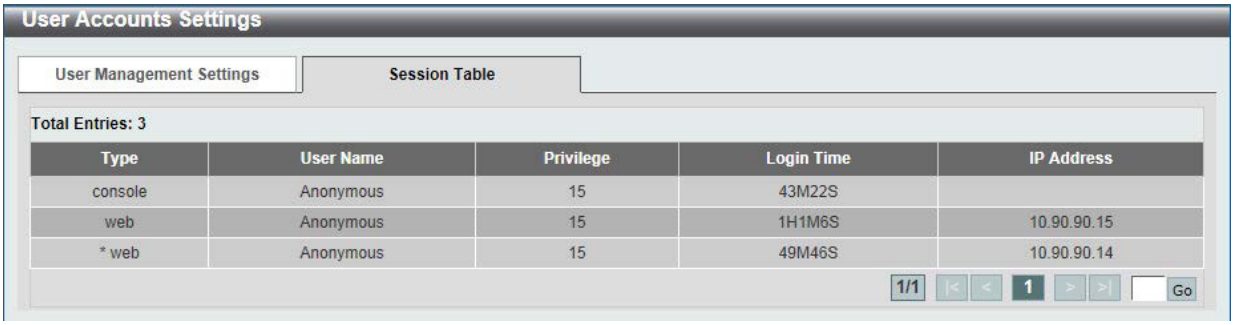


図 7-2　User Accounts Settings - Session Table 画面

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

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 7-3　Password Encryption 画面

以下の項目が表示されます。

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

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

Password Recovery（パスワードリカバリ）

本画面ではパスワードリカバリの設定を行います。例えば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。

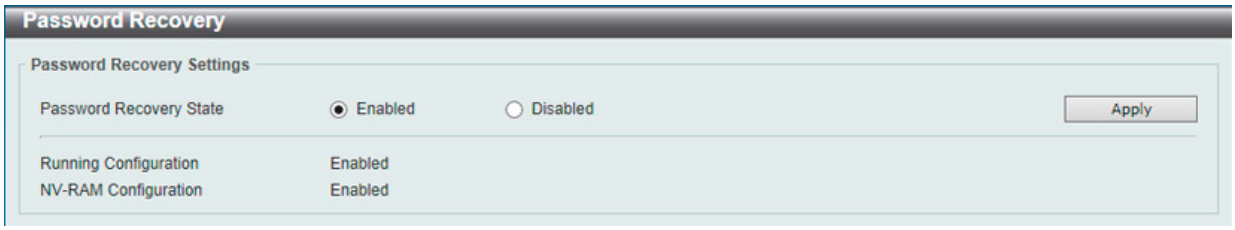


図 7-4　Password Recovery 画面

以下の項目が表示されます。

項目	説明
Password Recovery State	パスワードリカバリを有効 / 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 - 管理者権限レベルへの昇格の際に必要となる enable password 機能の更新 - ローカル認証を行うために AAA 機能を無効化 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。

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

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。

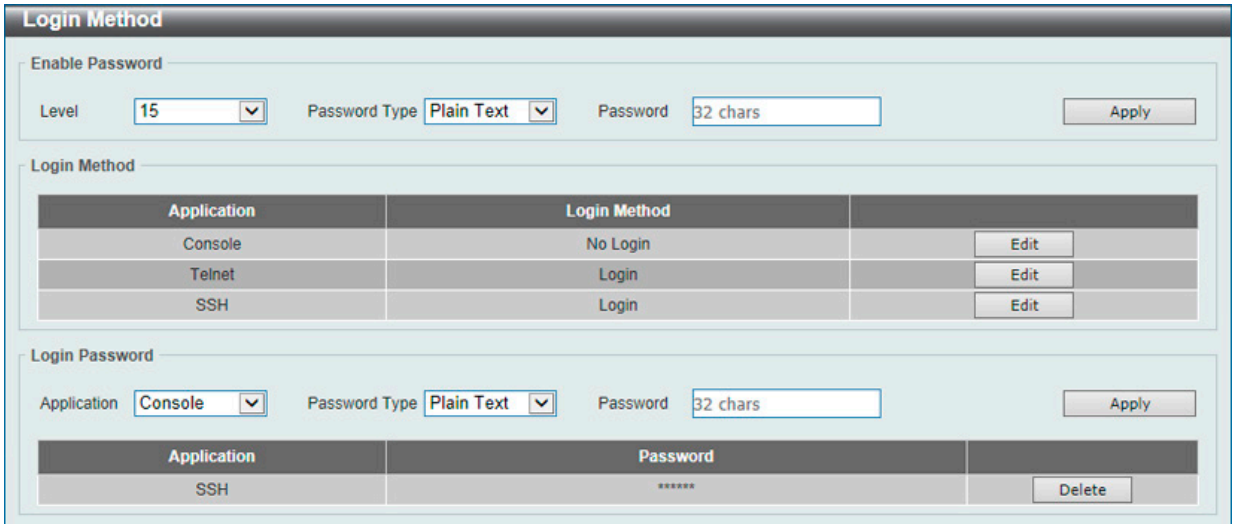


図 7-5　Login Method 画面

以下の項目が表示されます。

Enable Password（Enable パスワード）

項目	説明
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」- パスワードはプレーンテキストで保存されます。（初期値） • 「Encrypted」- パスワードは「SHA-1」を使用して暗号化されます。 • 「Encrypted-MD5」- パスワードは「MD-5」を使用して暗号化されます。

項目	説明
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。入力するパスワードのルールは、暗号化の方法によって異なります。 -「Plain Text」選択時：32 文字以内（大文字と小文字を区別、スペースを含める） -「Encrypted」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）

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

Login Method（ログインメソッド）

項目	説明
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」- 指定のアプリケーションへのアクセスに対してユーザ名入力などを必要としません。 • 「Login」- 指定のアプリケーションへのアクセスにパスワードを入力する必要があります。 • 「Login Local」- 指定のアプリケーションへのアクセスにユーザ名とパスワードの入力が必要になります。

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「Apply」ボタンをクリックして設定内容を適用します。

Login Password（ログインパスワード）

項目	説明
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	暗号化の方法を選択します。 • 選択肢：「Plain Text」「Encrypted」「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。入力するパスワードのルールは、暗号化の方法によって異なります。 -「Plain Text」選択時：32 文字以内（大文字と小文字を区別、スペースを含める） -「Encrypted」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）

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

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 とトラップのグローバル設定を構成、参照します。

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。

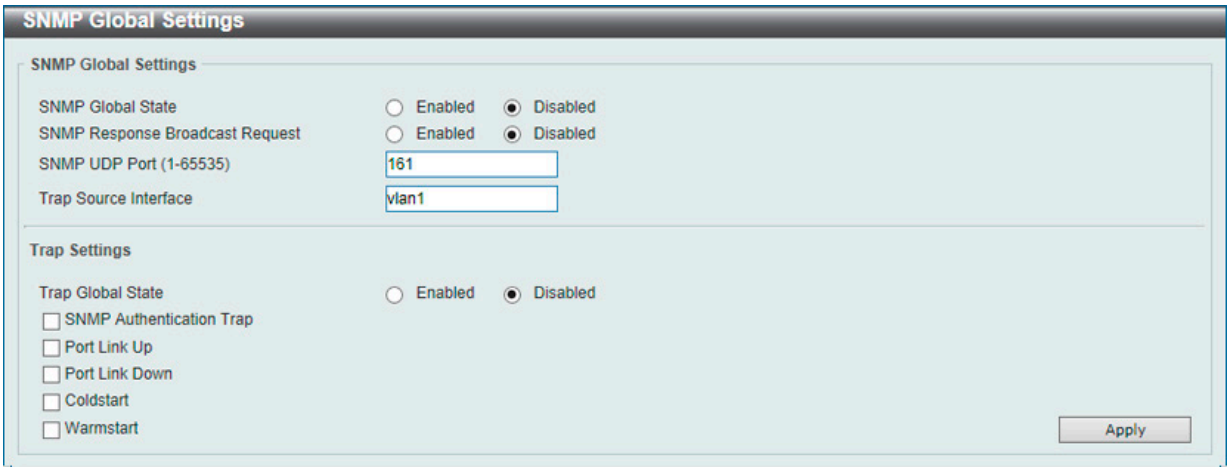


図 7-6　SNMP Global Settings 画面

以下の項目が表示されます。

SNMP Global Settings（SNMP グローバル設定）

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	SNMP GetRequest パケットのブロードキャストに対応するサーバを有効 / 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の 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 / 無効に設定します。認証失敗トラップは、機器が正しく認証されていない SNMP メッセージを受信した時に実行されます。認証方法は使用している SNMP のバージョンによって異なります。SNMPv1 または SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。SNMPv3 の場合、不正な SHA/MD5 認証キー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 / 無効に設定します。リンクアップトラップは機器がリンクアップを認識すると実行します。
Port Link Down	ポートリンクダウン通知を有効 / 無効に設定します。リンクダウントラップは機器がリンクダウンを認識すると実行します。
Coldstart	コールドスタート通知を有効 / 無効に設定します。
Warmstart	ウォームスタート通知を有効 / 無効に設定します。

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

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

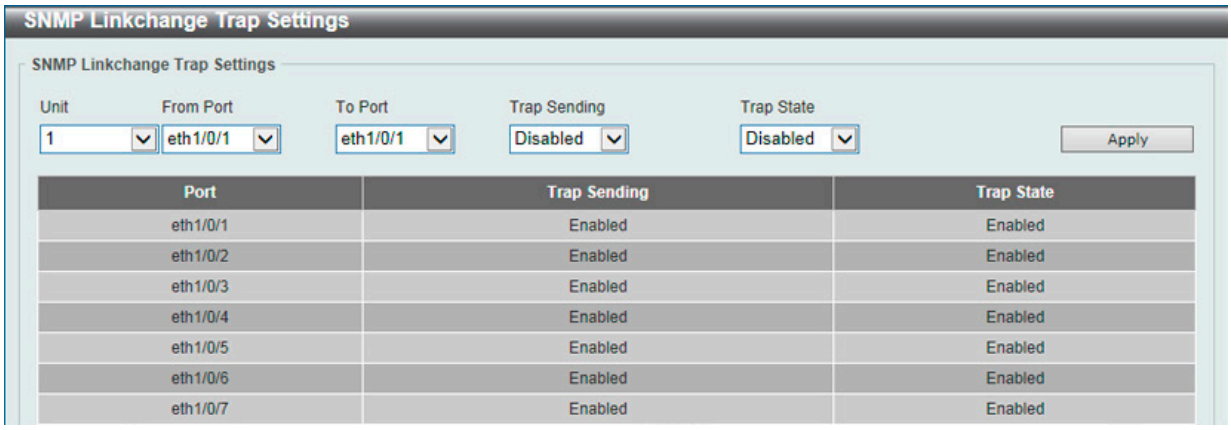


図 7-7　SNMP Linkchange Traps Settings 画面

以下の項目が表示されます。

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。
Trap Sending	SNMP 通知トラップ送信を有効 / 無効に設定します。
Trap State	SNMP リンクチェンジトラップを有効 / 無効に設定します。

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

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

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

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

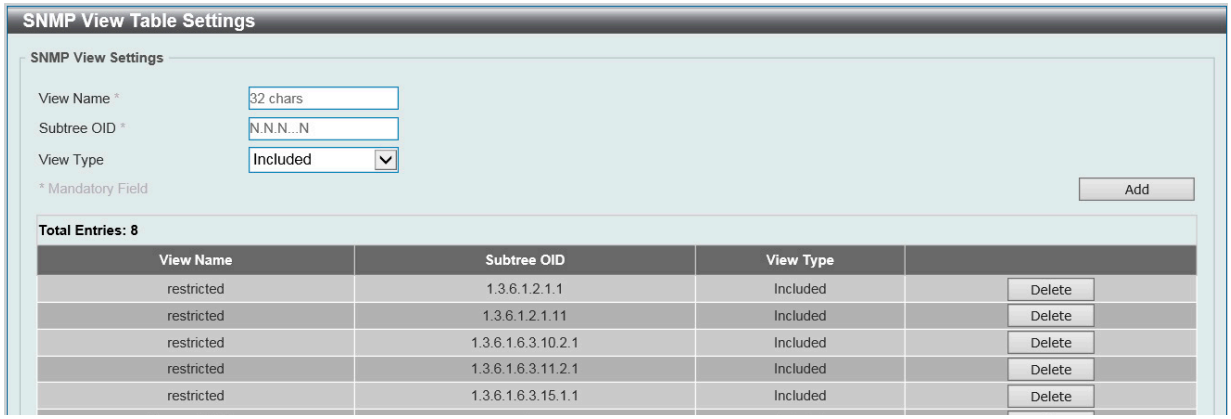


図 7-8　SNMP View Table Settings 画面

以下の項目が表示されます。

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）新しい SNMP ビューを登録し、識別する際に使用します。
Subtree OID	ビューの OID（Object Identifier）サブツリーを入力します。OID は、オブジェクトツリー（MIB ツリー）が SNMP マネージャによってアクセス可能な範囲かどうかを識別します。
View Type	「Subtree OID」で指定した OID に対し、ビューの種類を設定します。 ・「Included」- アクセス可能になります。 ・「Excluded」- アクセス不可になります。

「Add」ボタンをクリックして、設定内容に基づく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 ユーザ（「SNMP User Table」で設定）と本画面で登録するビューは、「SNMP Group Table」によって作成する SNMP グループによって関連付けます。

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

定義済みの SNMP コミュニティテーブルの参照、および、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 7-9　SNMP Community Table Settings 画面

以下の項目が表示されます。

項目	説明
Key Type	SNMP コミュニティのキーの種類を選択します。 • 選択肢：「Plain Text」「Encrypted」
Community Name	SNMP コミュニティメンバを識別するためのコミュニティ名を入力します。（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します。
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 グループの定義に使用します。View Name は SNMP View Table に存在する必要があります。
Access Right	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、設定内容に基づく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 グループを登録します。本グループは、SNMP ユーザ（「SNMP User Table」で設定）と「SNMP View Table」で設定するビューを関連付けるものです。

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。

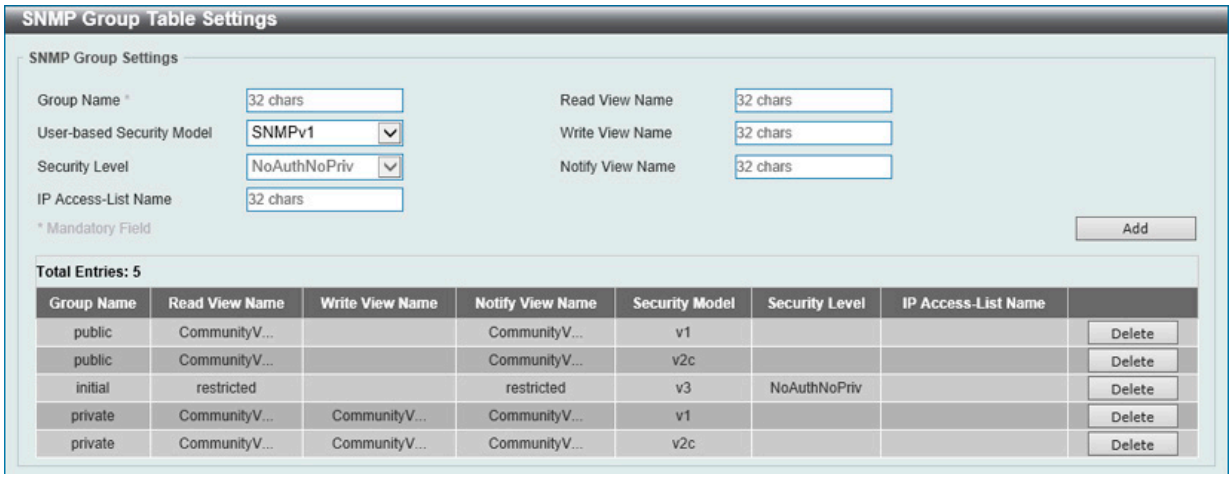


図 7-10　SNMP Group Table Settings 画面

以下の項目が表示されます。

項目	説明
Group Name	グループ名を指定します。（半角英数字 32 文字以内）SNMP ユーザのグループの識別に使用します。
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 が使用されます。 • 「SNMPv2c」- SNMP バージョン 2c が使用されます。SNMP バージョン 2 は集中型、分散型どちらのネットワーク管理にも対応します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。 • 「SNMPv3」- SNMP バージョン 3 が使用されます。ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。
Security Level	「SNMPv3」を選択した場合、セキュリティレベル設定を設定します。 • 「NoAuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットは認証も暗号化もされません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化なしになります。 • 「AuthPriv」- スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化ありになります。
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の名前を入力します。
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、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。

「Add」ボタンをクリックして、設定内容に基づく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 で使用される場合に定義される固有の識別名です。識別名は半角英数字の文字列で表記され、スイッチ上の SNMP エンジン（エージェント）を識別するために使用します。

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。

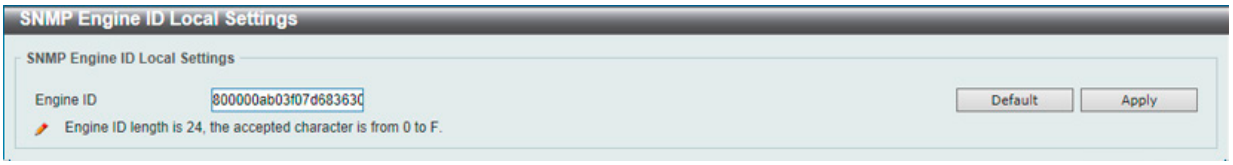


図 7-11　SNMP Engine ID Settings 画面

以下の項目が表示されます。

項目	説明
Engine ID	スイッチの SNMP エンジンの識別子を指定します。（24 文字内）

新しいエンジン ID を入力し、「Apply」ボタンをクリックして設定を適用します。
「Default」をクリックするとエンジン ID は初期値に戻ります。

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

SNMP ユーザを登録します。また、スイッチに現在設定されているすべての SNMP ユーザを表示します。

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。

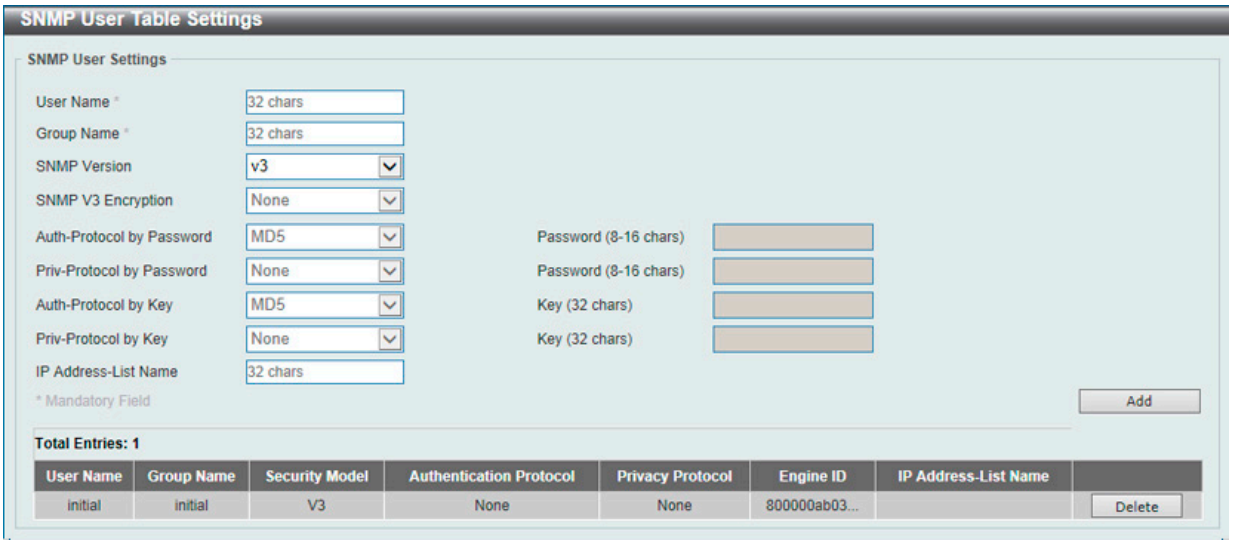


図 7-12　SNMP User Table Settings 画面

以下の項目が表示されます。

項目	説明
User Name	SNMP ユーザ名を入力します。（半角英数字 32 文以内）
Group Name	ユーザが属するグループ名を入力します。（半角英数字 32 文以内）
SNMP Version	SNMP バージョンを選択します。 • 「V1」- SNMP バージョン 1 を使用します。 • 「V2c」- SNMP バージョン 2 を使用します。 • 「V3」- SNMP バージョン 3 を使用します。
SNMP V3 Encryption	SNMP V3 に対して暗号化を有効にします。本項目は「SNMP Version」で「V3」を選択した場合に有効になります。 • 「None」- ユーザ認証は使用しません。 • 「Key」- HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムのキーによるのユーザ認証を行います。 • 「Password」- HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムのパスワードによるのユーザ認証を行います。
Auth-Protocol by Password	本項目は「SNMP Version」で「V3」を選択し、「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）

項目	説明
Priv-Protocol by Password	本項目は「SNMP Version」で「V3」を選択し、「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	本項目は「SNMP Version」で「V3」を選択し、「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。（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）
Priv-Protocol by Key	本項目は「SNMP Version」で「V3」を選択し、「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。（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	アクセスするための 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、設定内容に基づく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 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。

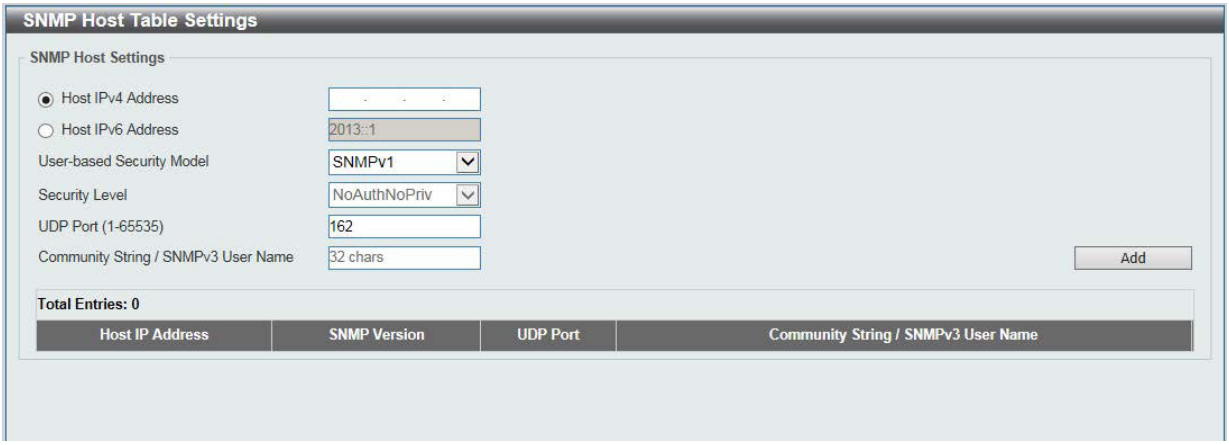


図 7-13　SNMP Host Table Settings 画面

以下の項目が表示されます。

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv6 アドレスを入力します。
User-based Security Model	SNMP バージョンを選択します。 • 「SNMPV1」: SNMP バージョン 1 が使用されます。 • 「SNMPV2c」: SNMP バージョン 2c が使用されます。 • 「SNMPV3」: SNMP バージョン 3 が使用されます。
Security Level	「SNMPv3」を選択した場合、セキュリティレベル設定を設定します。 • 「NoAuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットは認証も暗号化もされません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化なしになります。 • 「AuthPriv」- スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化ありになります。
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衝突する可能性があります。 • 設定可能範囲：0-65535 • 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、設定内容に基づく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 Context Mapping Settings（SNMP ホストテーブル設定）

SNMP コンテキストマッピングテーブルの表示、設定を行います。

Management > SNMP > SNMP Context Mapping 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。

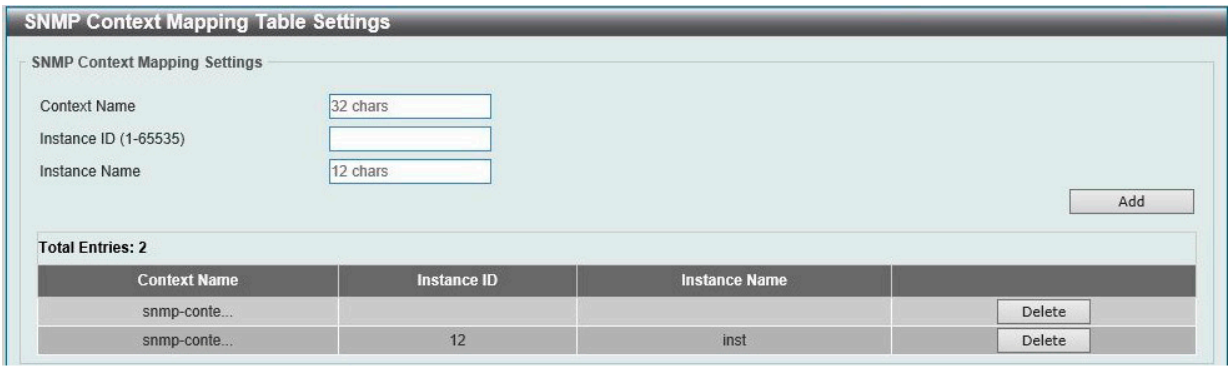


図 7-14　SNMP Host Table Settings 画面

以下の項目が表示されます。

項目	説明
Context Name	SNMP コンテキスト名を入力します。（32 文字以内）
Instance ID	インスタンス ID を入力します。
Instance Nmae	インスタンス名を入力します。

「Add」ボタンをクリックして、設定内容に基づく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 7-15　RMON Global Settings 画面

以下の項目が表示されます。

項目	説明
RMON Rising Alarm Trap	「RMON Rising Alarm Trap（上昇しきい値トラップ）」を有効 / 無効に設定します。
RMON Falling Alarm Trap	「RMON Falling Alarm Trap（下降しきい値トラップ）」を有効 / 無効に設定します。

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

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 7-16　RMON Statistics Settings 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポートを選択します。
Index	RMON 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
Owner	オーナー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、設定内容に基づく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。

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

詳細情報

「Show Detail」をクリックすると、以下の画面が表示されます。

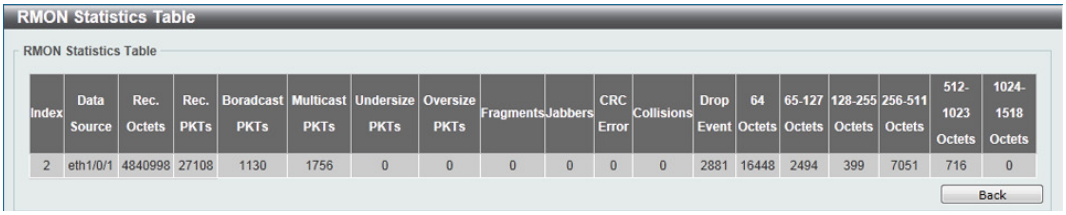


図 7-17　RMON Statistics Settings - Show Detail 画面

「Back」をクリックすると前ページへ戻ります。

RMON History Settings（RMON ヒストリ設定）

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

Management > RMON > RMON History 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。

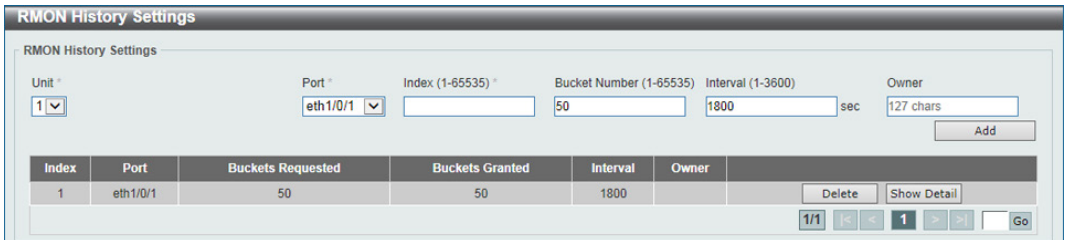


図 7-18　RMON History Settings 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポートを選択します。
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

項目	説明
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
Interval (1~3600)	ポートからサンプリングする間隔を設定します。 初期値：1800 (秒) 入力可能範囲：1-3600 (秒)
Owner	オーナーの文字列を入力します。（127 文字以内）

「Add」ボタンをクリックして、設定内容に基づく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。

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

詳細情報
「Show Detail」をクリックすると、以下の画面が表示されます。

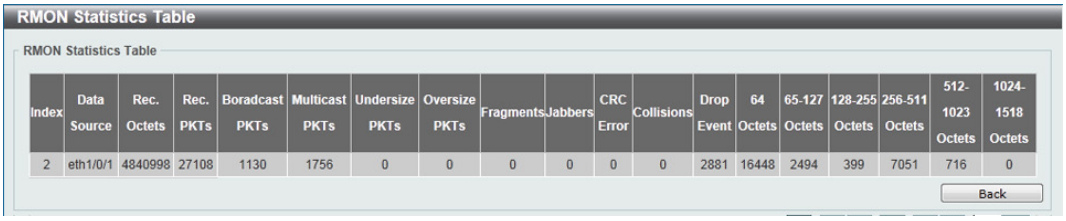


図 7-19　RMON History Settings - Show Detail 画面

「Back」をクリックすると前ページへ戻ります。

RMON Alarm Settings（RMON アラーム設定）

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

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。

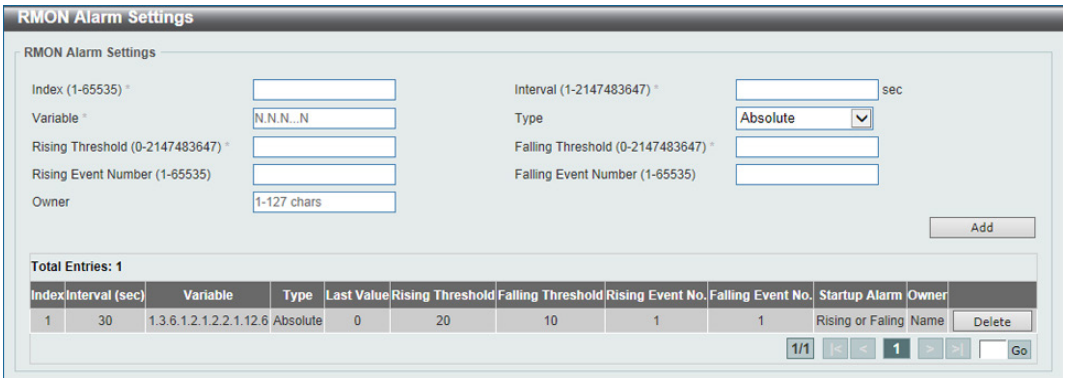


図 7-20　RMON Alarm Settings 画面

以下の項目が表示されます。

項目	説明
Index	アラームのインデックス番号を指定します。
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（秒）を定義します。 • 設定可能範囲：1-2147483648（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（秒）
Falling Threshold	下降しきい値を設定します。 • 設定可能範囲：0-2147483647（秒）
Rising Event Number	上昇しきい値を超えたときに開始するイベントを設定します。 • 設定可能範囲：1-65535（秒） 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。

項目	説明
Falling Event Number	下降しきい値を超えたときに開始するイベントを設定します。 • 設定可能範囲：1-65535（秒） 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	オーナー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、設定内容に基づく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。

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

RMON Event Settings（RMON イベント設定）

RMON イベントの定義、編集、および参照を行います。

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。

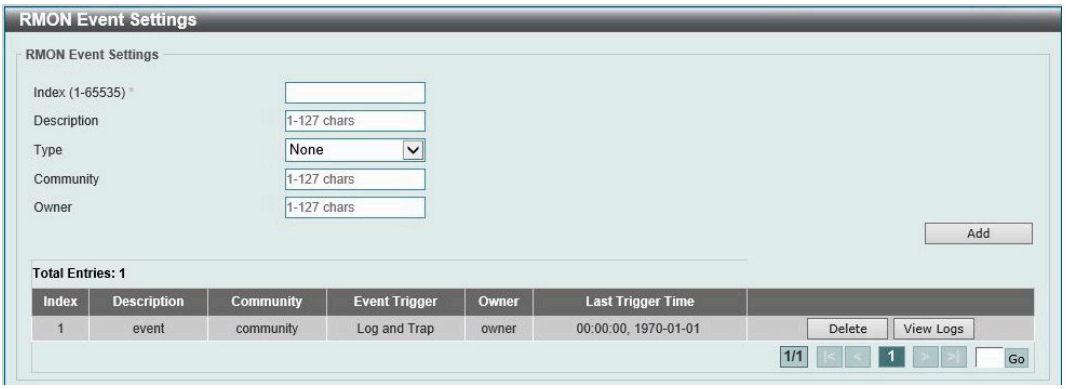


図 7-21　RMON Event Settings 画面

以下の項目が表示されます。

項目	説明
Index	イベントのインデックス番号を指定します。 • 設定可能範囲は 1-65535
Description	ユーザ定義のイベントの説明を入力します。（127 文字以内）
Type	イベントタイプを指定します。 •「None」- イベントは発生しません。 •「Log」- 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	イベントが所属するコミュニティを指定します。（127 文字以内）
Owner	オーナー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、設定内容に基づく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。

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

ログ情報の表示
「View Logs」をクリックすると、以下の画面が表示されます。

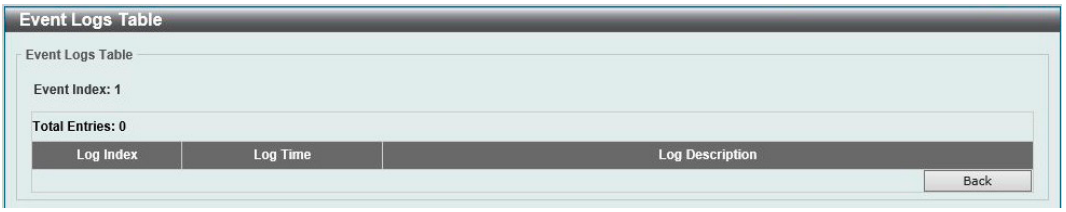


図 7-22　Event Logs Table 画面

「Back」をクリックすると前ページへ戻ります。

Telnet/Web（Telnet/Web 設定）

スイッチの Telnet/Web 設定を行います。

Management > Telnet/Web 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。

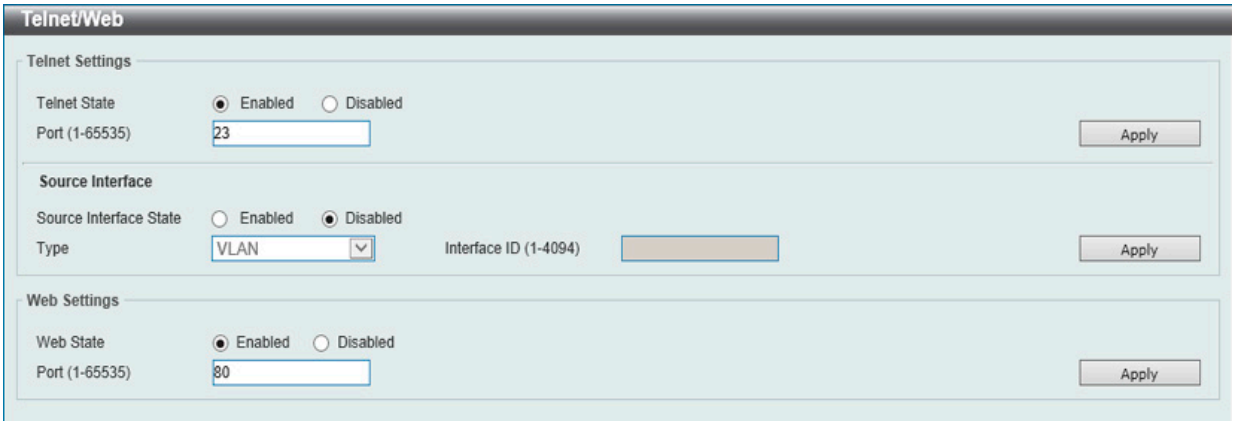


図 7-23　Telnet/Web Settings 画面

以下の項目が表示されます。

項目	説明
Telnet Settings	
Telnet State	Telnet 設定を有効 / 無効に設定します。Telnet 経由のシステム設定を許可しない場合は、「Disabled」（無効）を選択します。 • 初期値：「Enabled」（有効）
Port	スイッチの Telnet 管理に使用される 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
Source Interface	
Source Interface State	Source インタフェースの有効 / 無効を設定します。
Type	Source インタフェースの種類を指定します。 • 選択肢：「Loopback」「Mgmt」「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）、0（Mgmt 選択時）、1-4094（VLAN 選択時）
Source Interface	
Web State	Web ベースマネジメントの有効 / 無効を選択します。
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

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

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。

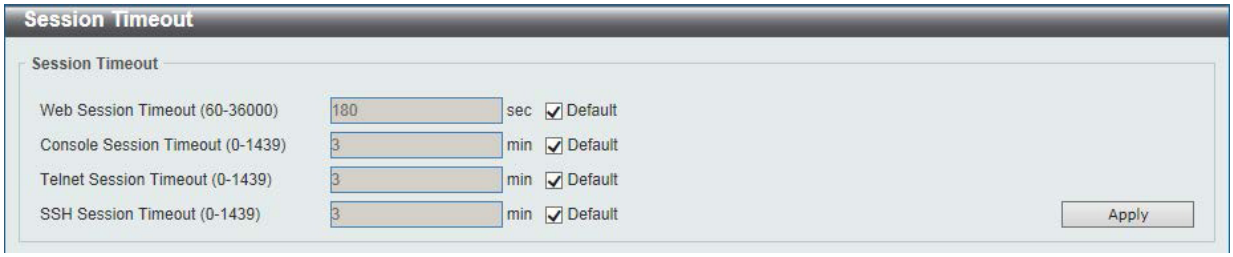


図 7-24　Session Timeout 画面

以下の項目が表示されます。

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に戻ります。
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に戻ります。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に戻ります。0 に指定するとタイムアウトしません。
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に戻ります。0 に指定するとタイムアウトしません。

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

DHCP（DHCP 設定）

スイッチの DHCP について設定します。

Service DHCP（DHCP サービス）

スイッチの DHCP リレー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 7-25　Service DHCP 画面

以下の項目が表示されます。

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

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

DHCP Class Settings（DHCP クラス設定）

DHCP クラスと、クラスに対する DHCP オプションのマッピ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 7-26　DHCP Class Settings 画面

以下の項目が表示されます。

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

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

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

エントリの編集

「Edit」をクリックすると、以下の画面が表示されます。

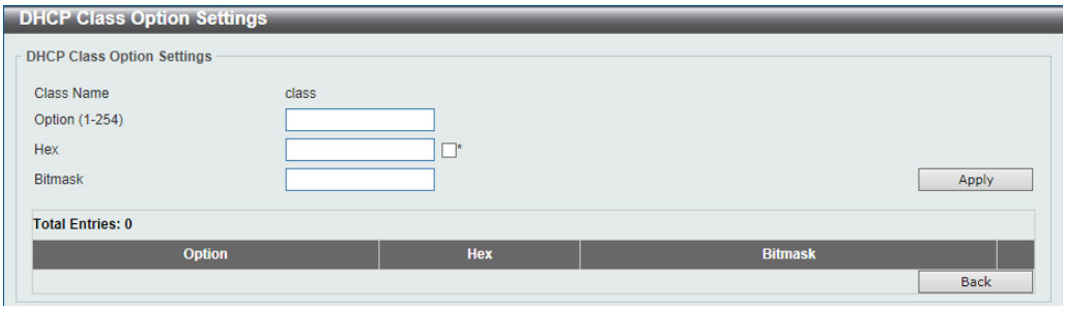


図 7-27　DHCP Class Option Settings（Edit）画面

以下の項目が表示されます。

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。マスクされたビット方式が照合されます。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。

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

「Back」をクリックすると前ページへ戻ります。

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。

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

DHCP サーバグローバルパラメータを設定します。

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。

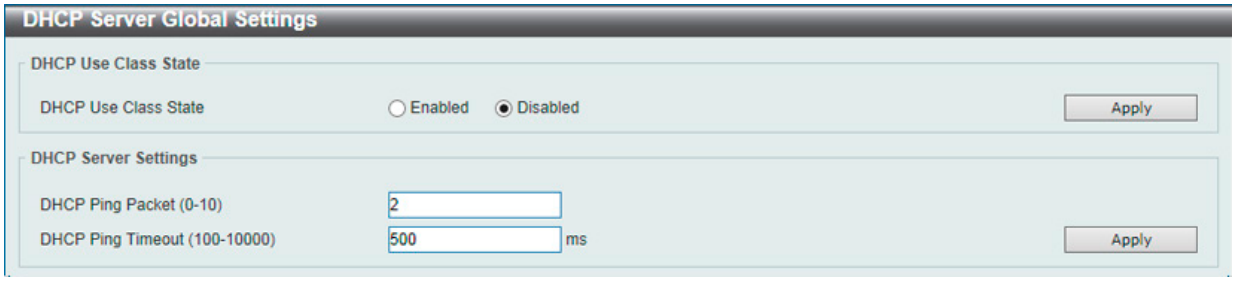


図 7-28　DHCP Server Global Settings 画面

以下の項目が表示されます。

DHCP User Class State

項目	説明
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。

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

Web Settings

項目	説明
Ping Packets	割り当て済みの 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 リクエストが戻らない場合、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て、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）
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：10-10000（ミリ秒） • 初期値：500（ミリ秒）

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

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

DHCP サーバプールの追加および削除を行います。

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 7-29　DHCP Server Pool Settings 画面

以下の項目が表示されます。

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）

「Apply」ボタンをクリックして、設定内容に基づくエントリを追加します。
作成されたプールは、「Edit Class」「Edit Option」「Configure」ボタンをクリックして、設定を編集することができます。
「Delete」ボタンをクリックして、指定エントリを削除します。

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

エントリの編集（クラス割り当て）

「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。

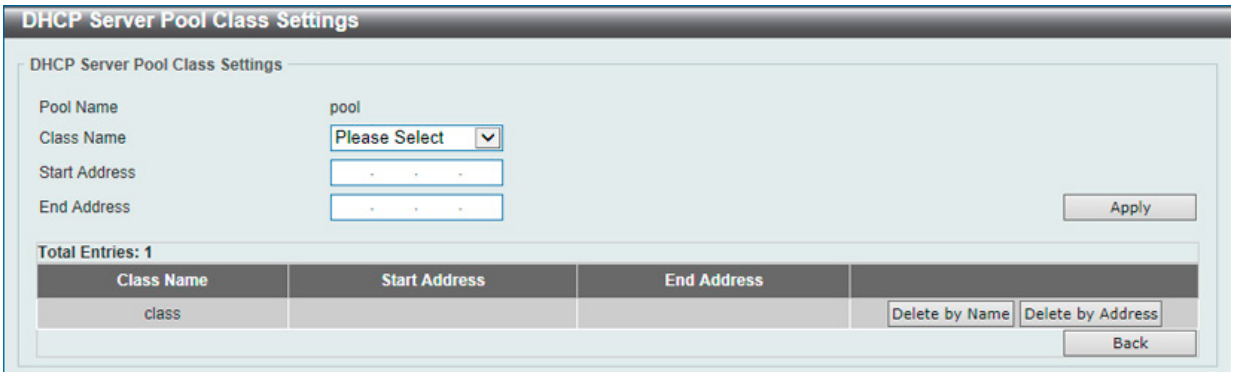


図 7-30　DHCP Server Pool Settings（Edit Class）画面

以下の項目が表示されます。

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。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete by Name」をクリックすると、名前に基づいて DHCP クラス割り当てを削除します。
「Delete by Address」をクリックすると、アドレスに基づいて DHCP クラス割り当てを削除します。

「Back」をボタンをクリックすると前のページに戻ります。

エントリの編集（DHCP オプション設定）

「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 7-31　DHCP Server Pool Settings（Edit Option）画面

以下の項目が表示されます。

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。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。

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

「Back」をボタンをクリックすると前のページに戻ります。

エントリの編集（サーバプール設定）

「Configure」ボタンをクリックすると、以下の画面が表示されます。

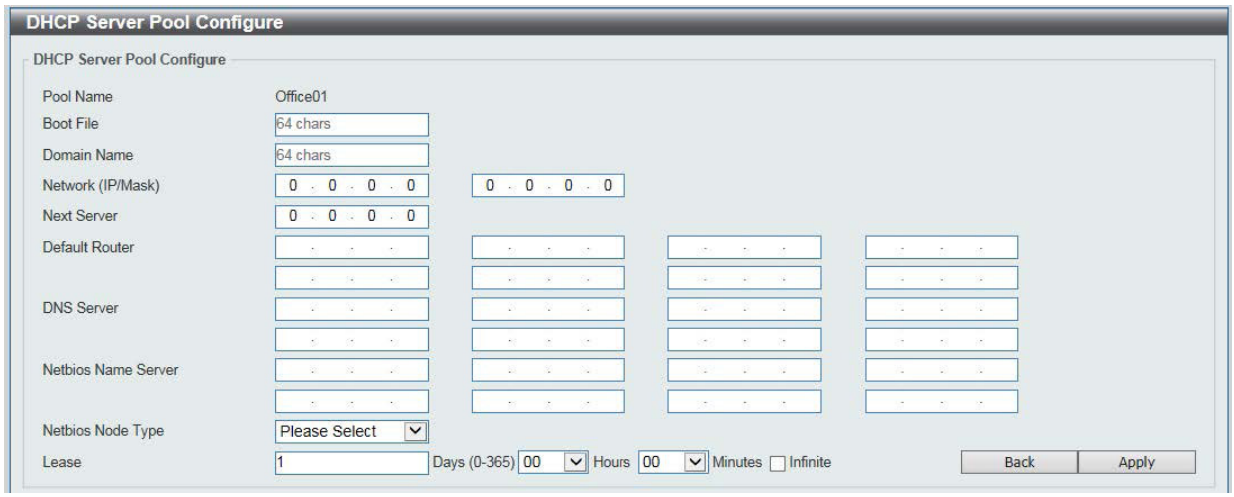


図 7-32　DHCP Server Pool Settings (Configure) 画面

以下の項目が表示されます。

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	DHCP 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)	プールのネットワークアドレスと対応する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。本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 アドレスはひと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。本ルータの 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インタフェース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。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デフォルトインテフェース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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をボタンをクリックすると前のページに戻ります。

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

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 プールからクライアントに 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 7-33　DHCP Server Exclude Address 画面

以下の項目が表示されます。

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。

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

アドレスバインディングは、クライアントの IP アドレスと MAC アドレスの間のマッピングです。手動のバインディングエントリによって、IP アドレスとクライアント識別子をバインディング、または IP アドレスと MAC アドレスをバインディング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。

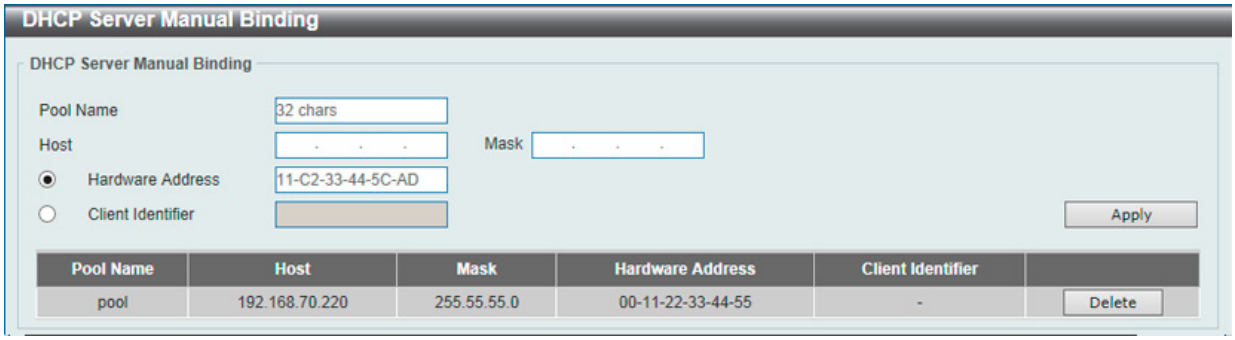


図 7-34　DHCP Server Manual Binding 画面

以下の項目が表示されます。

項目	説明
Pool Name	マニュアルバインディングエントリを作成する DHCP プール名を入力します。（32 文字以内）
Host	DHCP ホスト IP アドレスを入力します。
Mask	DHCP ホスト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 アドレスによってフォーマットされています。

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

「Back」をボタンをクリックすると前のページに戻ります。

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エントリの表示と削除を行います。

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。

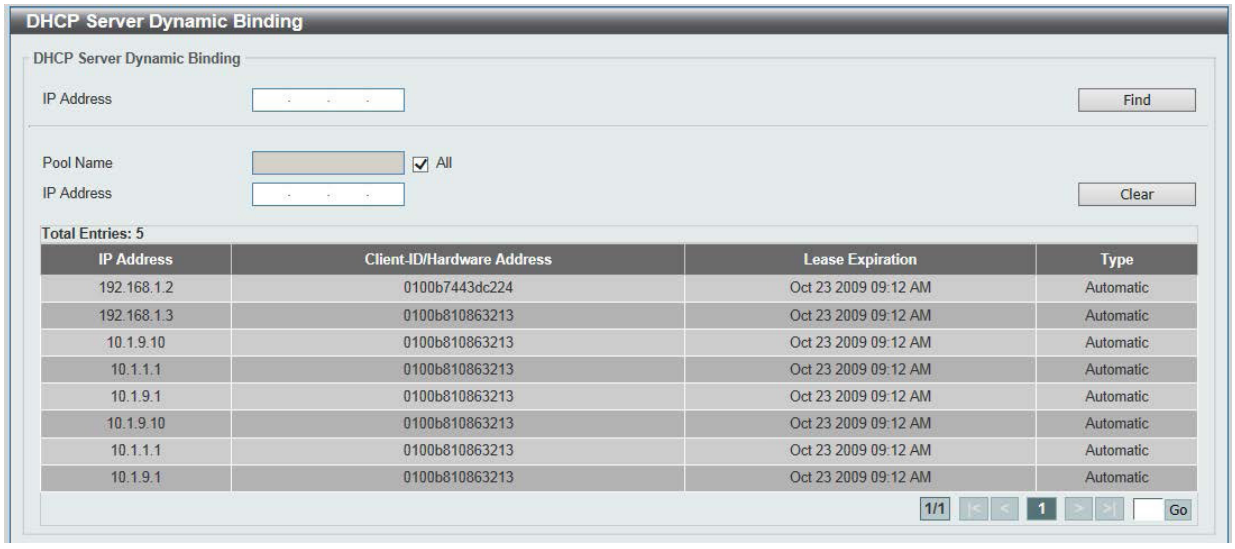


図 7-35　DHCP Server Dynamic Binding 画面

以下の項目が表示されます。

項目	説明
IP Address	バインディングエントリの IP アドレスを指定します。
Pool Name	ダイナミックにバインドされている DHCP エントリのプール名を指定します。「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。

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Clear」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。

DHCP Server IP Conflict（DHCP サーバ IP コンフリクト）

DHCP サーバデータベースの DHCP コンフリクトエントリを表示、クリアします。

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

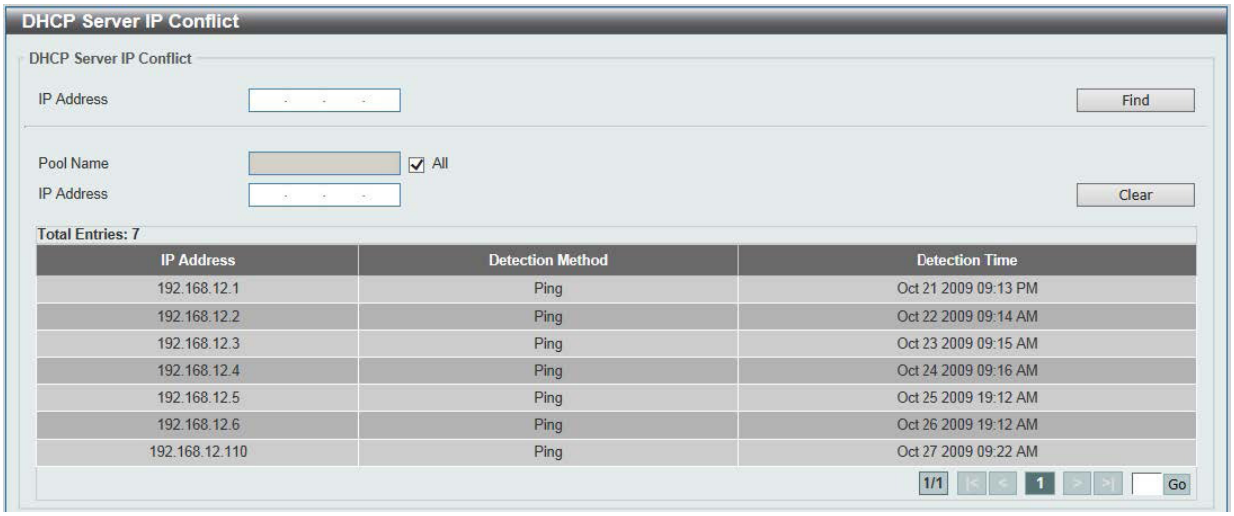


図 7-36　DHCP Server IP Conflict 画面

以下の項目が表示されます。

項目	説明
IP Address	コンフリクトエントリの IPv4 アドレスを入力します。
Pool Name	DHCP エントリのプール名を指定します。「All」オプションにチェックを入れると、全てのプールのコンフリクトエントリを削除します。

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Clear」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。

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

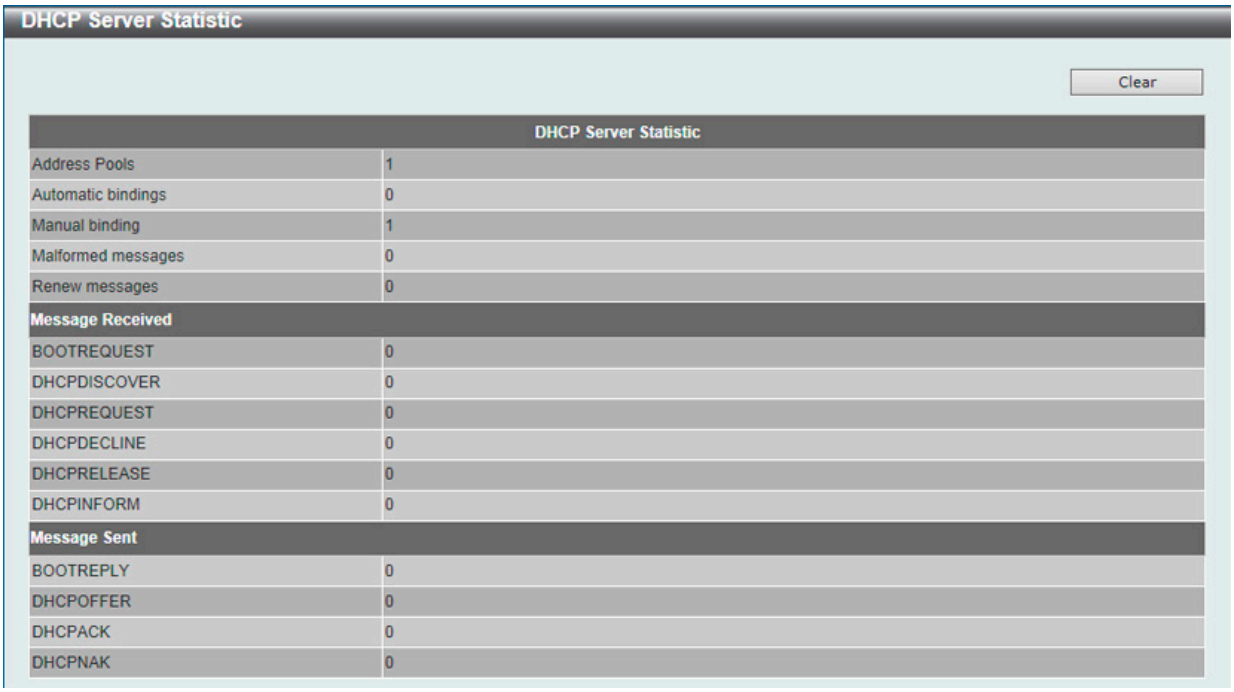


図 7-37　DHCP Server Statistic 画面

「Clear」ボタンをクリックして、エントリを削除します。

DHCPv6 Server（DHCPv6 サーバ設定）

Management > DHCP > DHCPv6 Server

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 7-38　DHCPv6 Server Pool Settings 画面

以下の項目が表示されます。

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、入力した情報に基づい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。

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

エントリの編集

「Configure」ボタンをクリックすると、以下の画面が表示されます。

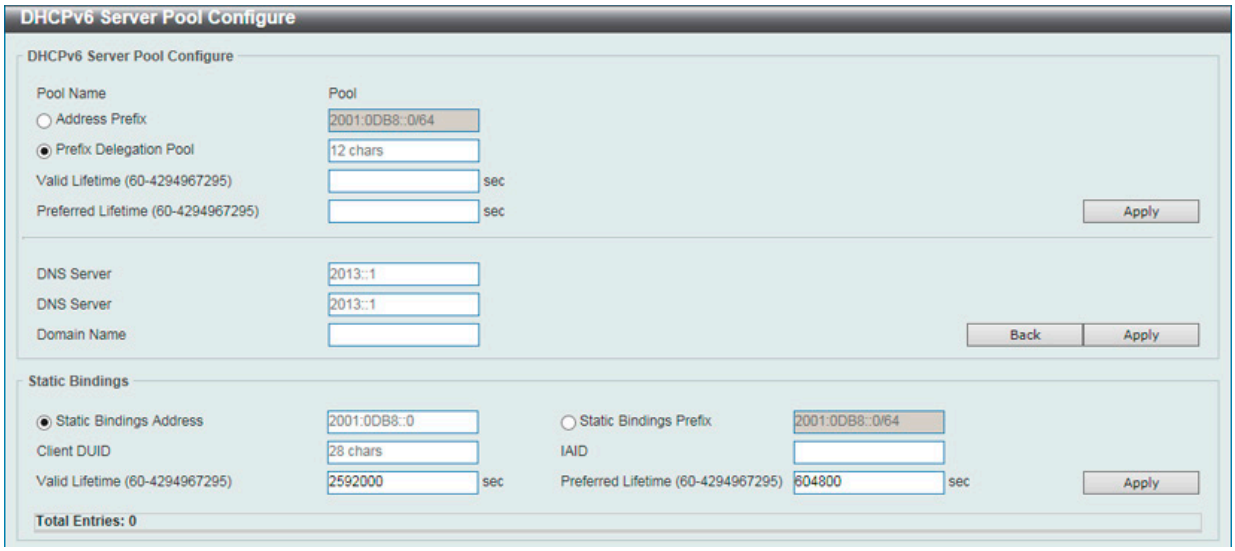


図 7-39　DHCPv6 Server Pool Settings (Configure) 画面

以下の項目が表示されます。

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

項目	説明
DHCPv6 Server Pool Configure	
Address Prefix	DHCPv6 サーバプール IPv6 ネットワークアドレスとプレフィクス長を入力します。（例：2015::0/64）
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）
Preferred Lifetime	IPv6 アドレスが preferred-lifetime（推奨有効期限）状態を維持する時間を入力します。 • 設定可能範囲：60-4294967295（秒） • 初期値は 604800（秒）（7 日）
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。

項目	説明
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クスを入力します。
Client DUID	デバイスの 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。 • 設定可能範囲：60-4294967295（秒） • 初期値：2592000（秒）（30 日）
Preferred Lifetime	IPv6 アドレスが preferred-lifetime（推奨有効期限）状態を維持する時間を入力します。 • 設定可能範囲：60-4294967295（秒） • 初期値：604800（秒）（7 日）

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

DHCPv6 Server Exclude Address（DHCPv6 サーバエクスクルードアドレス）

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 7-40　DHCPv6 Server Excluded Address Settings 画面

以下の項目が表示されます。

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。

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

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、削除します。

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。

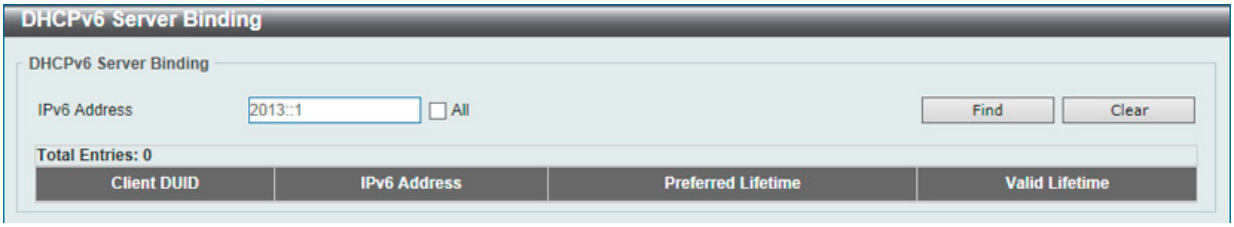


図 7-41　DHCPv6 Server Binding 画面

以下の項目が表示されます。

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 クライアントプリフィ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、指定条件に基づくエントリを検索 / 表示します。
「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。

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。

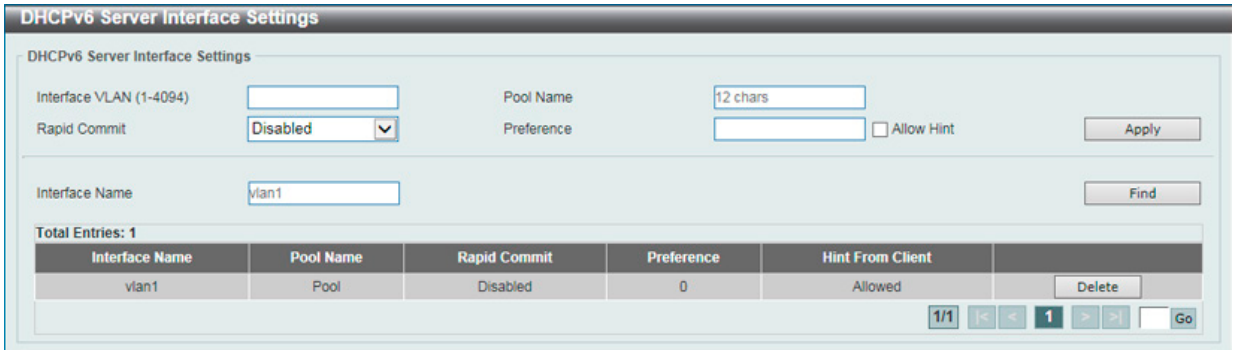


図 7-42　DHCPv6 Server Interface Settings 画面

以下の項目が表示されます。

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。「Allow Hint」を選択するとヒントが表示されます。
Interface Name	インタフェース名を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

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。

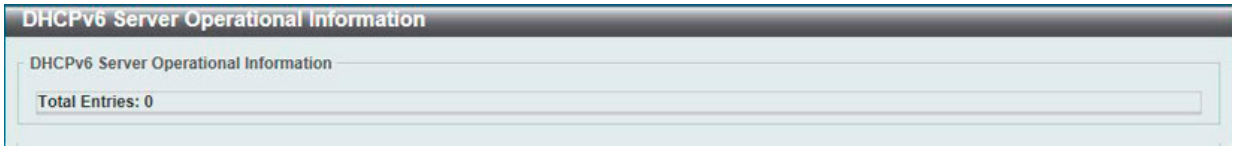


図 7-43　DHCPv6 Server Operational Information 画面

DHCP Relay（DHCP リレー）

Management > DHCP > DHCP Relay

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

DHCP リレーグローバル設定の有効化および設定を行うことができます。

Management > DHCP > DHCP Relay > DHCP 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。

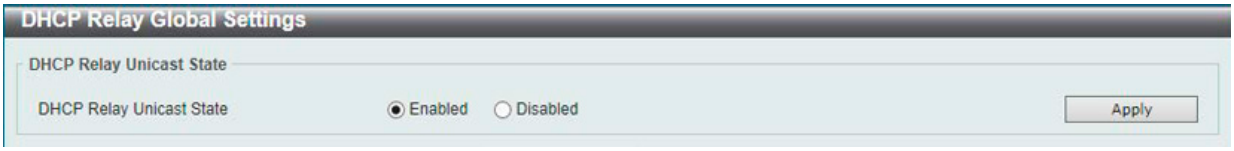


図 7-44　DHCP Relay Global Settings 画面

以下の項目が表示されます。

項目	説明
DHCP Relay Unicast State	DHCP リレーユニキャストのグローバルステータスを有効 / 無効に設定します。

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

注意　DHCP Relay 機能を有効にした VLAN において、Unicast Relay が初期設定で有効の為、Option 82 付きの DHCP Request は破棄されます。Unicast Relay 機能を無効にするか "ip dhcp relay information trust-all" を設定してください。

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。

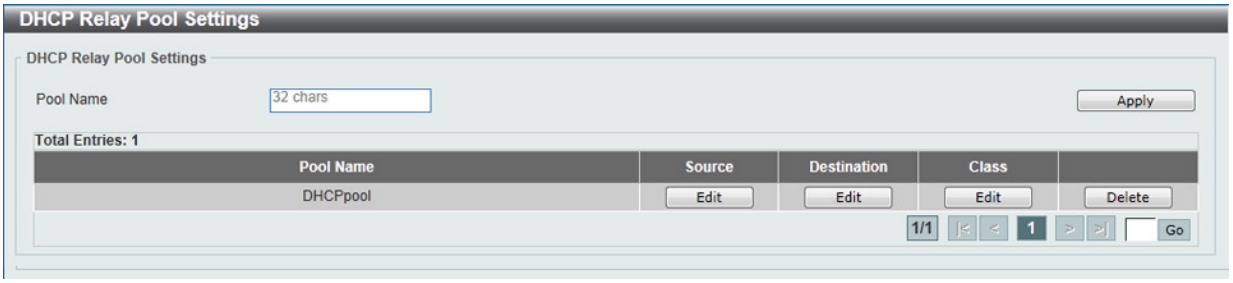


図 7-45　DHCP Relay Pool Settings 画面

以下の項目が表示されます。

項目	説明
Pool Name	プール名を指定します。（32 文字以内）

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

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

エントリの編集（Source）

「Source」下の「Edit」をクリックします。以下の画面が表示されます。

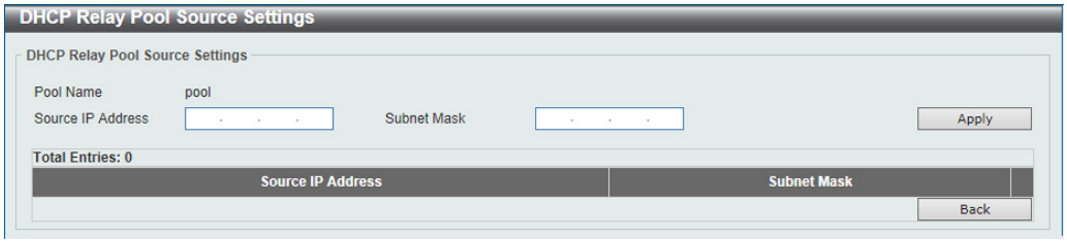


図 7-46　DHCP Relay Pool Source Settings 画面

以下の項目が表示されます。

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。

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

「Back」をクリックすると前の画面へ戻ります。

エントリの編集（Destination）

「Destination」下の「Edit」をクリックします。以下の画面が表示されます。

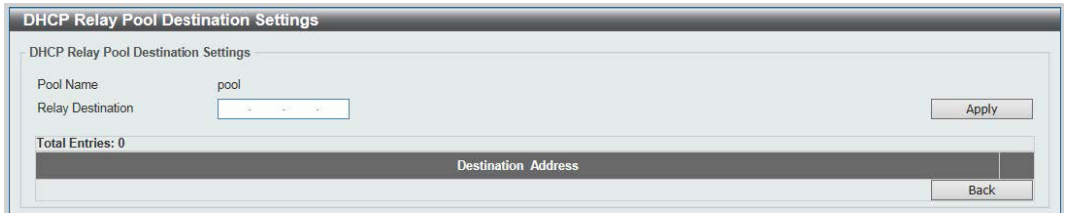


図 7-47　DHCP Relay Pool Destination Settings 画面

以下の項目が表示されます。

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

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

「Back」をクリックすると前の画面へ戻ります。

エントリの編集（Class）

「Class」下の「Edit」をクリックします。以下の画面が表示されます。

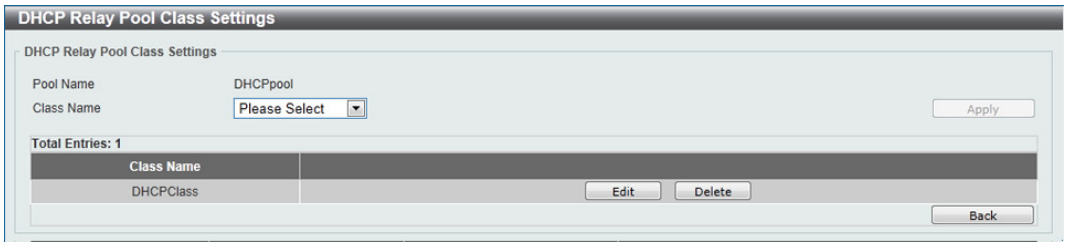


図 7-48　DHCP Relay Pool Class Settings 画面

以下の項目が表示されます。

項目	説明
Class Name	DHCP クラスの名前を選択します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。
「Back」をクリックすると前の画面へ戻ります。

クラスの編集

クラス名の横の「Edit」をクリックすると、以下の画面が表示されます。



図 7-49　DHCP Relay Pool Class Edit Settings 画面

以下の項目が表示されます。

項目	説明
Relay Target	DHCP クラスで設定したオプションの方式とマッチ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。

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

「Delete」ボタンをクリックして、エントリを削除します。

「Back」をクリックすると前の画面へ戻ります。

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

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。

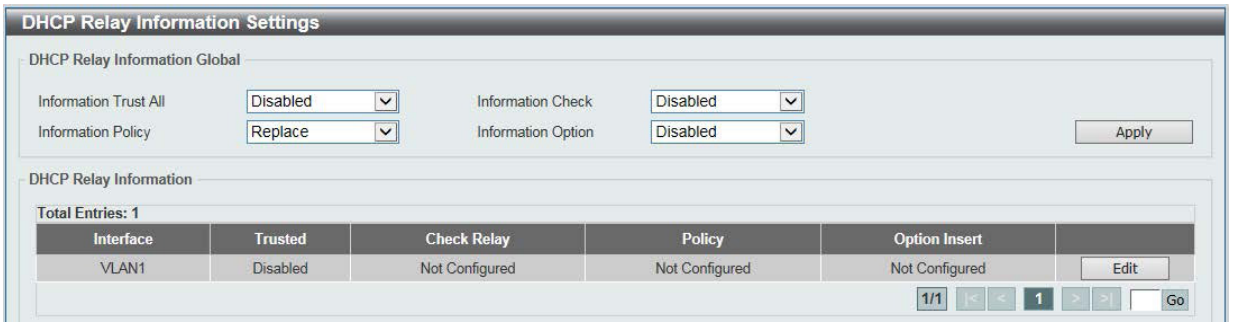


図 7-50　DHCP Relay Information Settings 画面

以下の項目が表示されます。

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。 • 「Replace」- DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。（初期値） • 「Drop」- DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。
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。

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

「Edit」をクリックすると、該当インタフェースの設定を編集することができます。

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

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表示、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。

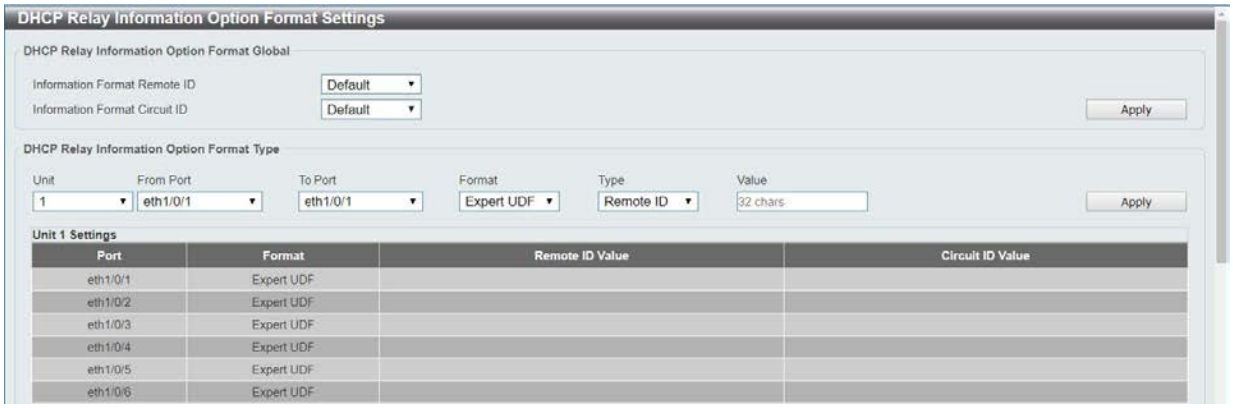


図 7-51　DHCP Relay Information Option Format Settings 画面

以下の項目が表示されます。

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 はシステムの MAC アドレスを使用します。 • 「User Define」- リモート ID はユーザ定義の文字列を使用します。（32 文字以内） • 「Vendor2」- リモート ID はベンダ 2 を使用します。 • 「Expert UDF」- Expert UDF リモート ID を使用します。スタンドアロンのユニットフォーマット選択します。
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 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） • 「Vendor1」- サーキット ID はベンダ 1 を使用します。 • 「Expert UDF」- Expert UDF サーキット ID を使用します。スタンドアロンのユニットフォーマット選択します。
DHCP Relay Information Option Format Type	
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。
Format	expert UDF のフォーマットを選択します。
Type	リレー情報オプションの種類を選択します。 • 選択肢：「Remote ID」「Circuit ID」
Value	オプション 82 情報として、リモート / サーキット ID サブオプションに含まれるベンダ定義の文字列を入力します。（32 文字以内）

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

DHCP Relay Information Profile Settings（DHCP リレー情報プロファイル設定）

DHCP リレー情報プロファイル設定を行います。

Management > DHCP > DHCP Relay > DHCP Relay Information 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。

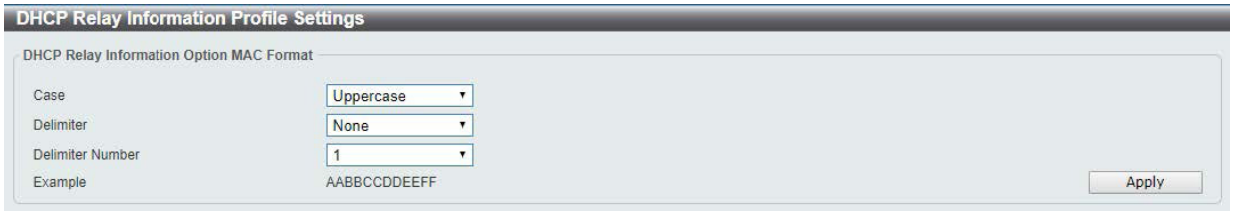


図 7-52　DHCP Relay Information Profile Settings 画面

以下の項目が表示されます。

項目	説明
Case	オプション 82 の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。 • 「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）

項目	説明
Delimiter	MAC アドレスを入力する際の区切りを選択します。区切り文字を持たない場合には「None」を選択します。各項目の例は次の通りです。 • 「Hyphen」（ハイフン）-「AA-BB-CC-DD-EE-FF」 • 「Colon」（コロン）-「AA:BB:CC:DD:EE:FF」 • 「Dot」（ドット）-「AA.BB.CC.DD.EE.FF」 • 「None」（なし）-「AABBCCDDEEFF」
Delimiter Number	MAC アドレスにおける区切り数を選択します。各項目の例は次の通りです。 • 「1」-「AABBCC.DDEEFF」 • 「2」-「AABB.CCDD.EEFF」 • 「5」-「AA.BB.CC.DD.EE.FF」

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

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

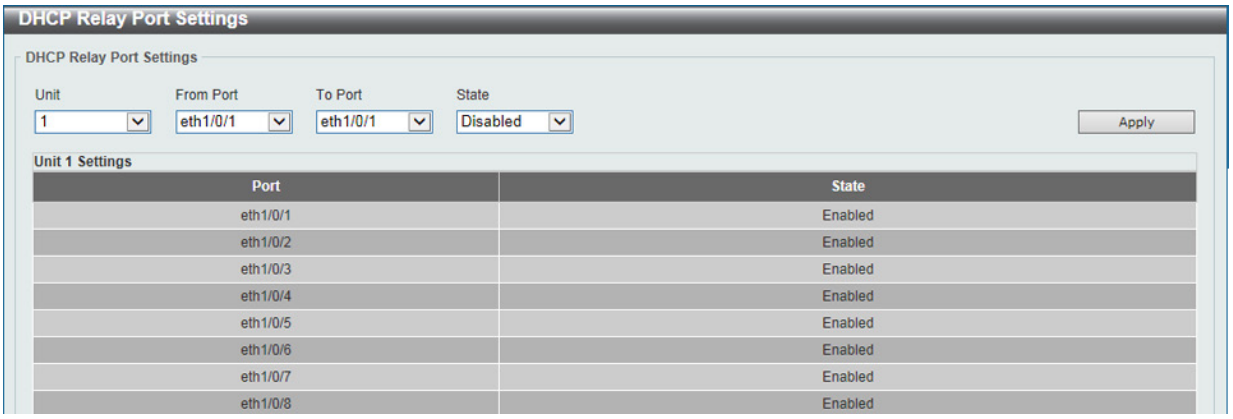


図 7-53　DHCP Relay Port Settings 画面

以下の項目が表示されます。

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。
State	指定のポートの DHCP リレーを有効 / 無効に設定します。

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

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。

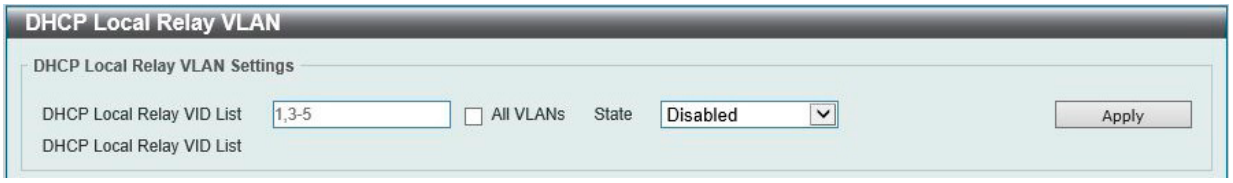


図 7-54　DHCP Local Relay VLAN 画面

以下の項目が表示されます。

項目	説明
DHCP Local Relay VID List	DHCP ローカルリレーを適用する VLAN ID を入力します。「All VLANs」にチェックを入れるとすべての VLAN を選択します。
State	指定の VLAN の DHCP ローカルリレーを有効 / 無効に設定します。

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

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。

注意　DHCP Relay 機能を有効にした VLAN において、Unicast Relay が初期設定で有効の為、Option 82 付きの DHCP Request は破棄されます。Unicast Relay 機能を無効にするか "ip dhcp relay information trust-all" を設定してください。

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。

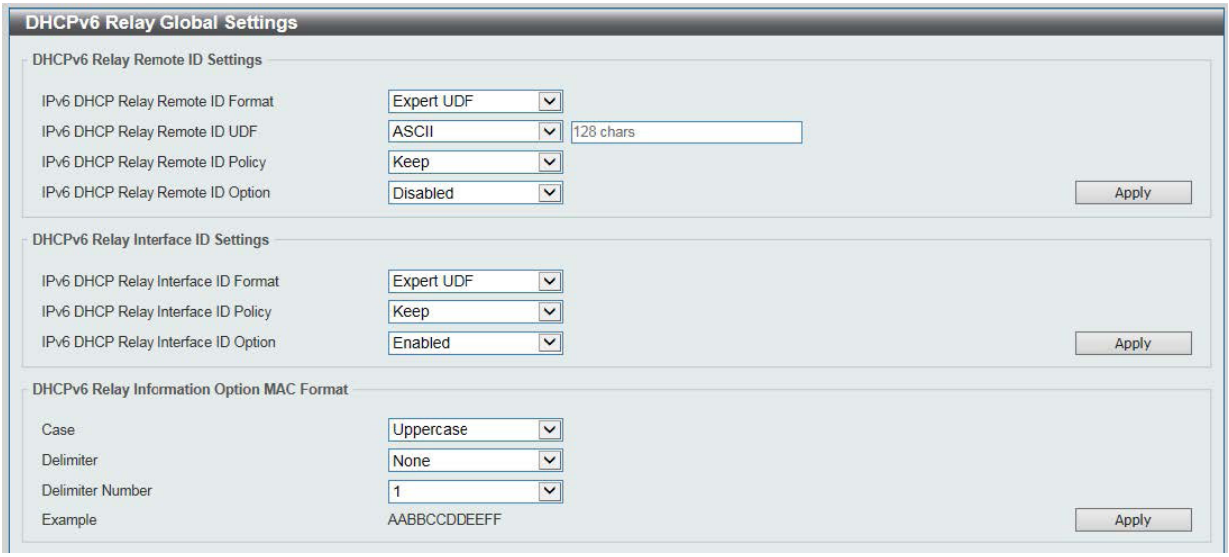


図 7-55　DHCPv6 Relay Global Settings 画面

以下の項目が表示されます。

DHCPv6 Relay Remote ID Settings

項目	説明
DHCPv6 Relay Remote ID Settings	
IPv6 DHCP Relay Remote ID Format	IPv6 DHCP リレーのリレー ID フォーマットを選択します。 「Default」「CID With User Define」「User Define」「Expert UDF」から選択します。
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。 • 「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）
IPv6 DHCP Relay Remote ID Policy	DHCPv6 リレーエージェントのオプション 37 フォワーディング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削除します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプション 37 リレー情報を保持します。
IPv6 DHCP Relay Remote ID Option	DHCP IPv6 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（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	DHCPv6 リレーインタフェース ID のフォーマットを指定します。 「Default」「CID」「User Define」「Vendor1」「Expert UDF」から選択します。
IPv6 DHCP Relay Interface ID Policy	DHCPv6 リレーエージェントのオプション 18 フォワーディングポリシーを選択します。 「Drop」「Keep」から選択します。 • 「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削除します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプショ 187 リレー情報を保持します。
IPv6 DHCP Relay Interface ID Option	DHCP IPv6 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（Option18）の挿入を有効 / 無効に設定します。
DHCPv6 Relay Information Option MAC Format	
Case	オプション 82 の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。 • 「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）

項目	説明
Delimiter	MAC アドレスを入力する際の区切りを選択します。区切り文字を持たない場合には「None」を選択します。 各項目の例は次の通りです。 • 「Hyphen」（ハイフン）-「AA-BB-CC-DD-EE-FF」 • 「Colon」（コロン）-「AA:BB:CC:DD:EE:FF」 • 「Dot」（ドット）-「AA.BB.CC.DD.EE.FF」 • 「None」（なし）-「AABBCCDDEEFF」
Delimiter Number	MAC アドレスにおける区切り数を選択します。各項目の例は次の通りです。 • 「1」-「AABBCC.DDEEFF」 • 「2」-「AABB.CCDD.EEFF」 • 「5」-「AA.BB.CC.DD.EE.FF」

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

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。

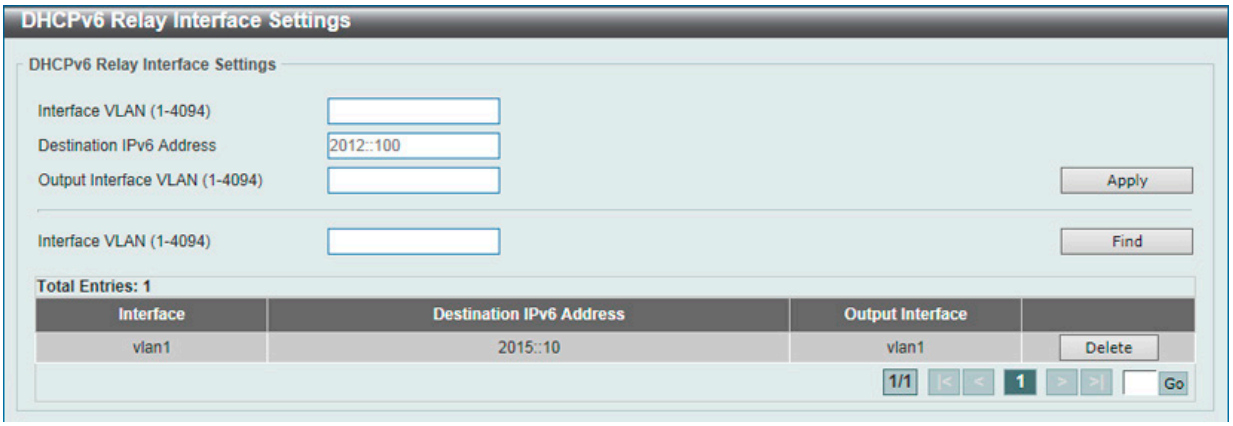


図 7-56　DHCPv6 Relay Interface Settings 画面

以下の項目が表示されます。

項目	説明
Interface VLAN	DHCPv6 リレーの VLAN 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を指定します。 • 設定可能範囲：1-4094

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

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。

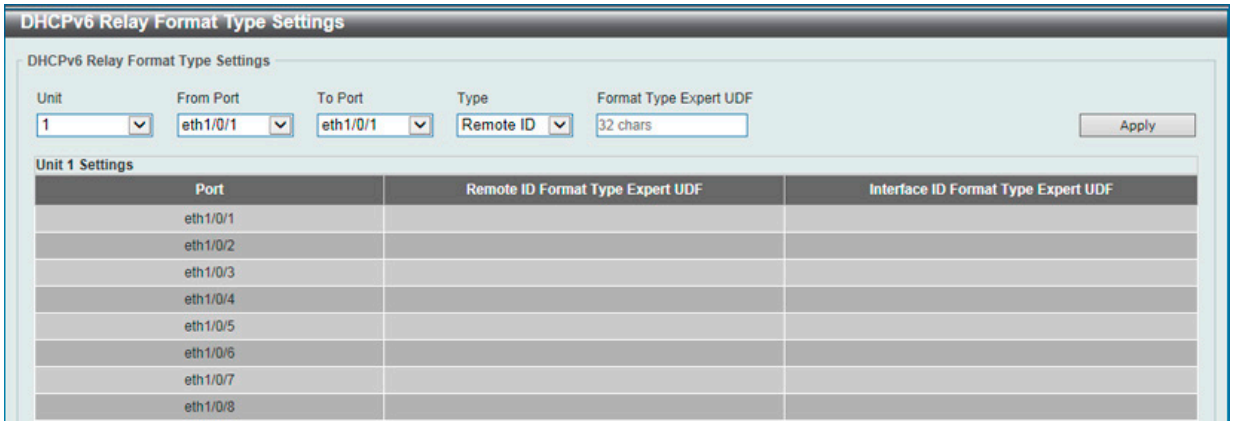


図 7-57　DHCPv6 Relay Format Type Settings 画面

以下の項目が表示されます。

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。
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」文字列のフォーマットを設定します。

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

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。

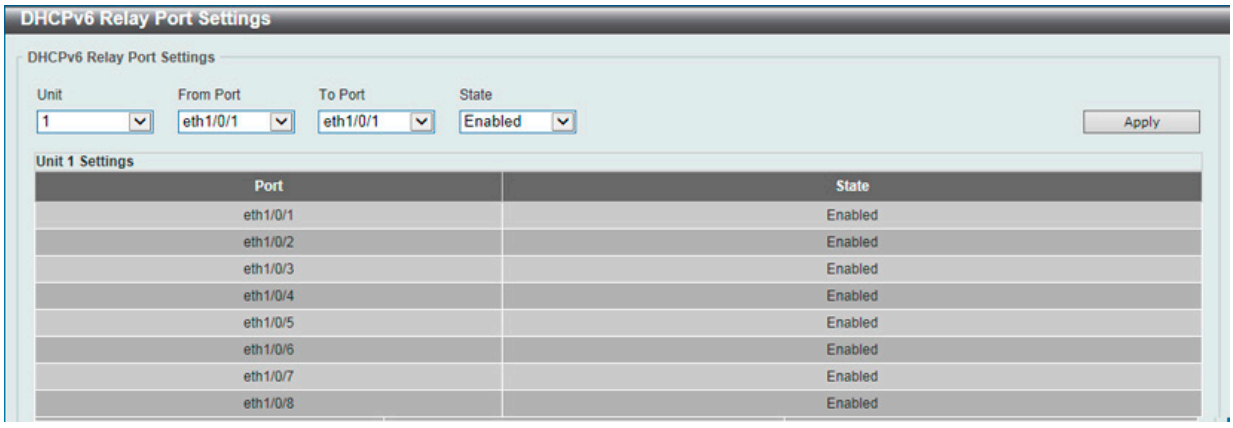


図 7-58　DHCPv6 Relay Port Settings 画面

以下の項目が表示されます。

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。
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。

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

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オプション 37 と 18 を追加します。オプション 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、オプション 37 の DHCPv6 リレー機能が含まれる場合、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、オプション 37 が有効であろうとなかろうと、常にオプション 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。

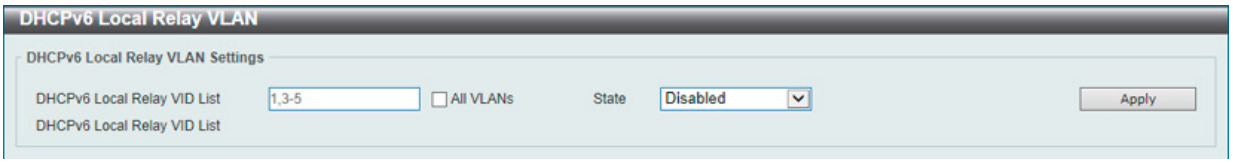


図 7-59　DHCPv6 Local Relay VLAN 画面

以下の項目が表示されます。

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。

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

注意　「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。

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 > 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。

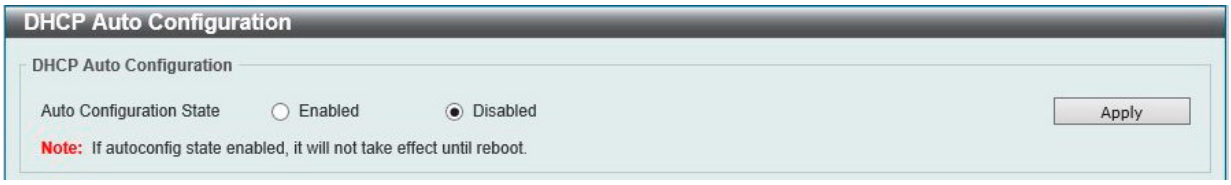


図 7-60　DHCP Auto Configuration 画面

以下の項目が表示されます。

項目	説明
Auto Configuration State	自動設定機能の有効 / 無効を設定します。

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

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。DNS サーバは「name-to-address」変換を実行し、ドメイン名とアドレスの変換を行うためにネームサーバと通信を行う必要があります。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、または初期設定時に手動で OS に設定することができます。

DNS Global Settings（DNS グローバル設定）

本項目ではグローバルに DNS を設定します。

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。

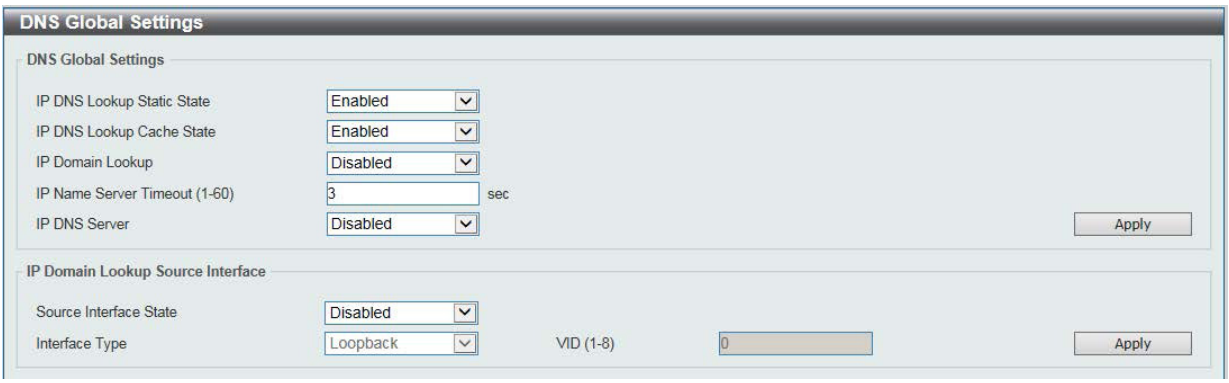


図 7-61　DNS Global Settings 画面

以下の項目が表示されます。

項目	説明
DNS Global Settings	
IP DNS Lookup Static State	IP DNS ルックアップスタティックを有効 / 無効に設定します。
IP DNS Lookup Cache State	IP DNS ルックアップキャッシュを有効 / 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。
IP Domain Lookup Source Interface	
Source Interface State	ソースインタフェースを指定します。
Interface Type	インタフェース種類を「Loopback」「Mgmt」「VLAN」から指定します。
VID	ソースインタフェースの VLAN ID を指定します。 • 設定可能範囲：1-8（Loopback 選択時）、0（Mgmt 選択時）、1-4094（VLAN 選択時）

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

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

DNS のネームサーバの IP アドレスを設定、表示します。

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。

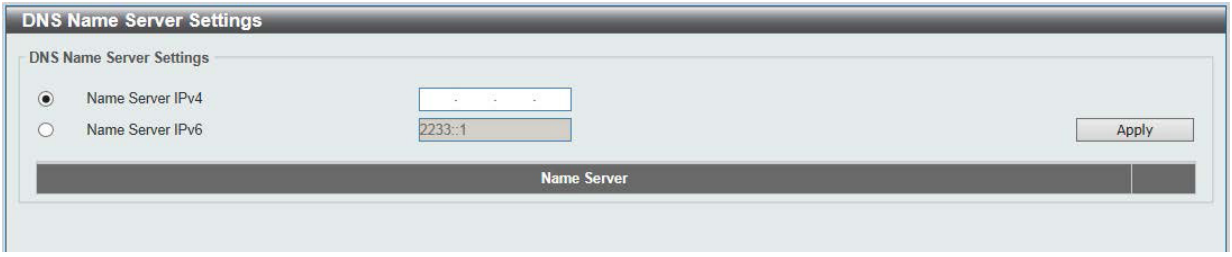


図 7-62　DNS Name Server Settings 画面

以下の項目が表示されます。

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

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

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

DNS Host Settings（DNS ホスト名設定）

ホスト名と IP アドレスのスタティックマッピング設定を行います。

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 7-63　DNS Host Settings 画面

以下の項目が表示されます。

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。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear All」ボタンをクリックして、入力した情報を削除します。
「Delete」ボタンをクリックして、エントリを削除します。

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

IP Source Interface（IP ソースインタフェース）

IP ソースインタフェースを設定します。

Management > IP Source 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。

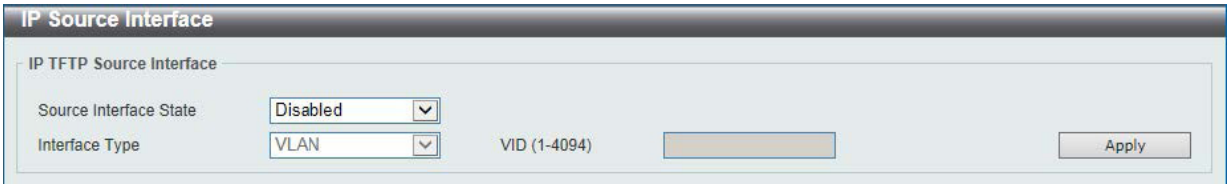


図 7-64　IP Source Interface 画面

以下の項目が表示されます。

項目	説明
IP TFTP Source Interface	
Source Interface State	IP TFTP ソースインタフェースを指定します。
Interface Type	インタフェース種類を「Loopback」「Mgmt」「VLAN」から指定します。
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）、0（Mgmt 選択時）、1-4094（VLAN 選択時）

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

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。

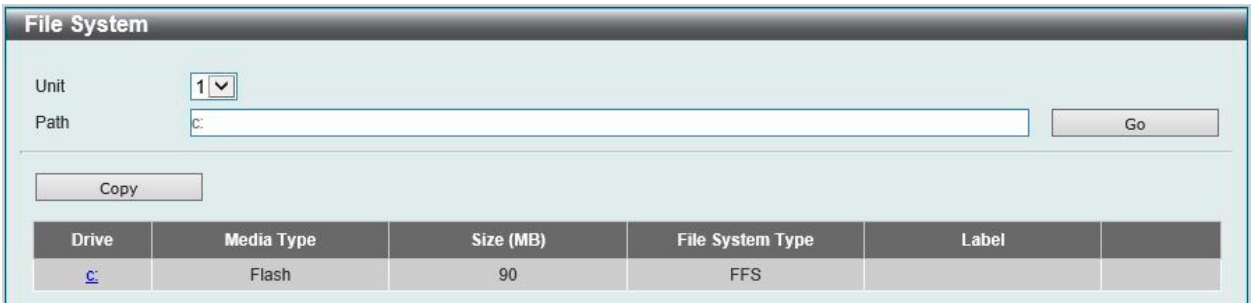


図 7-65　File System 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Path	パスの文字列を入力します。

「Path」に現在のパスを入力し、「Go」ボタンをクリックすると入力したパスに遷移します。
「Copy」をクリックすると指定のファイルをスイッチへコピーします。
「C:」リンクをクリックすると、「C:」ドライブに遷移します。

ディレクトリの表示

「C:」リンクをクリックすると、以下の画面が表示されます。

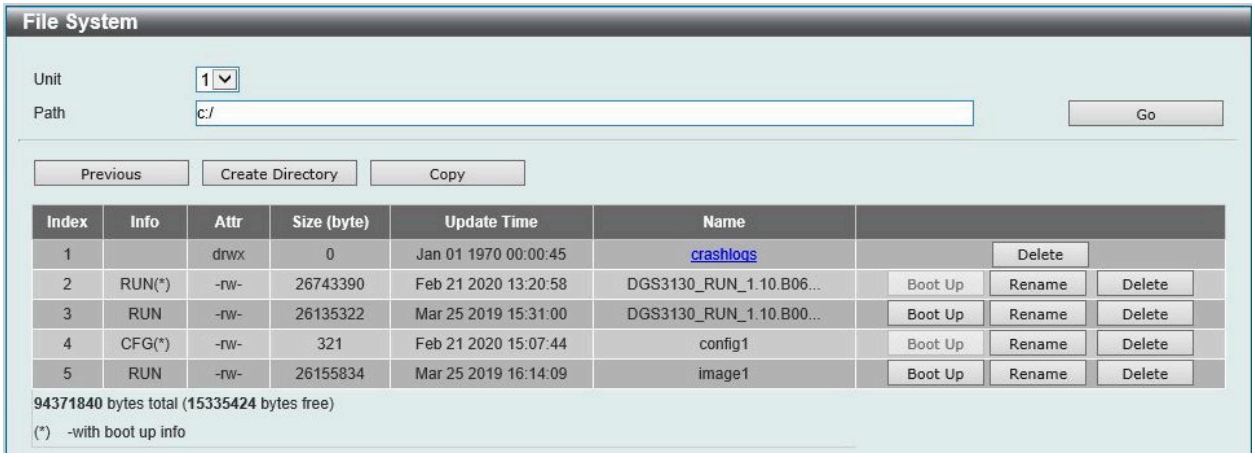


図 7-66　File System (Drive) 画面

以下の項目が表示されます。

項目	説明
Go	入力したパスへ進みます。
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 Up	指定したランタイムイメージをブートアップイメージとして設定します。
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。

注意　ブートコンフィグファイルが破損しているとスイッチは自動的に初期設定に戻ります。

注意　ブートイメージファイルが破損しているとスイッチは自動的にバックアップイメージファイルを使用します。

ファイルのコピー

1. 「Copy」ボタンをクリックすると、以下の画面が表示されます。

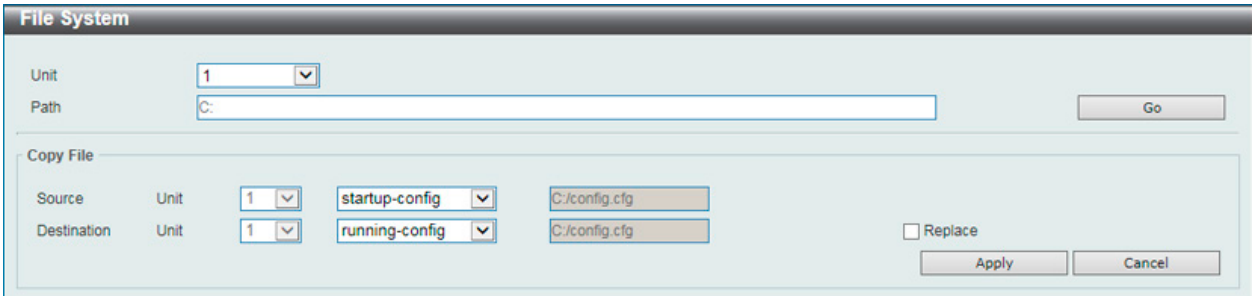


図 7-67　Flash File System Settings 画面 - Copy

2. このスイッチのファイルシステムにファイルをコピーする場合、送信元と送信先のパスを入力します。

項目	説明
Source	コピー元ファイルが保存されているスイッチのユニット ID と、コピーされるファイルのタイプを選択します。 • 選択肢：「startup-config」「Source File」 「Source File」選択時にはファイルパスを指定欄に入力します。
Destination	宛先スイッチのユニット ID とコピーファイルのタイプを選択します。 • 選択肢：「startup-config」「running-config」「Destination File」 「Destination File」選択時にはファイルパスを指定欄に入力します。「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。

3. 「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。

注意 copy コマンドや Flash への書き込み中は TELNET や CLI などの操作ができなくなります。書き込み終了までしばらくお待ちください。

重要 設定済みの状態で別のコンフィグファイルを running にコピーすることはできません。別のコンフィグをリストアする場合は、必ず running-config を消してからリストアするようにしてください。

Stacking（スタッキング設定）

補足　スタック機能は将来のファームウェアでサポート予定です。

本シリーズはスイッチのスタックをサポートしており、最大 9 台までのスタックが可能です。マスタースイッチ上で管理ポートを介して 1 つの IP アドレスで管理、または Telnet、GUI インタフェース（Web）、SNMP を介して複数の IP アドレスで管理することができます。
RJ-45/SFP+ ポートを使用したスイッチのスタックにより、ネットワークのアップグレードをリーズナブルでコストパフォーマンスの高い方法で実現します。これ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 6 個※のスタック用ポート / 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、RJ-45 ケーブルや SFP+ ダイレクトアタッチケーブル（DAC）、また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。
※ 10GBASE-T ポート× 2 と SFP+ × 4 スロットがスタック用に使用できます。実際に使用するのは、このうち 2 個または 4 個のポート / スロットです。

- 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円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、RJ-45 ケーブル、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 コネクタに接続された 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 6 ポー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、スタックに使用している 2/4 個のポート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。これらのポートはスタッキング専用ポートとなります。

補足　リングトポロジーを強く推奨します。

物理スタックでは「2 ポート」または「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。

以下は、RJ-45 ケーブル、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。「2 ポート」または「4 ポート」スタッキング設定を使用しています。

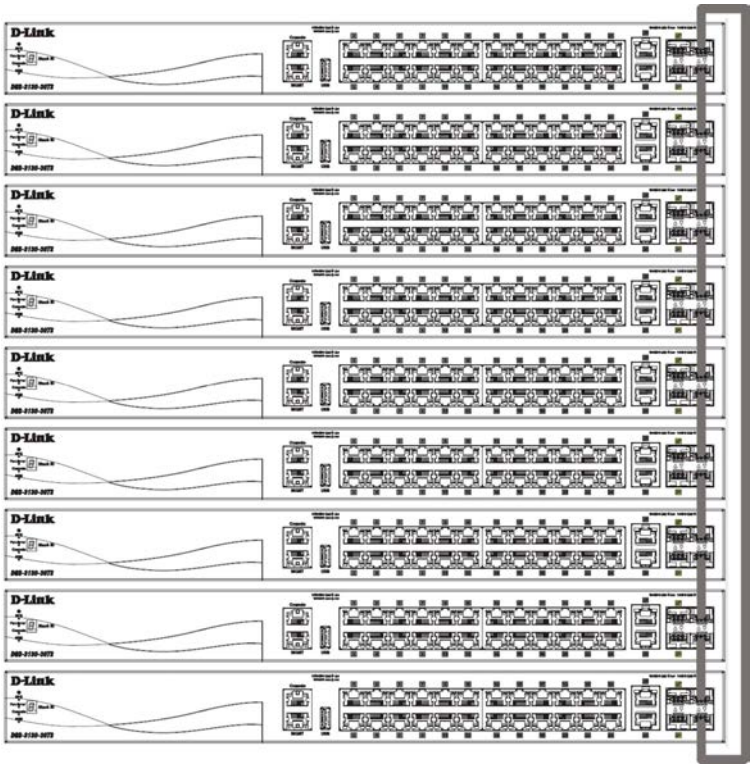


図 7-68　Duplex Ring でスタックされているスイッチ（2 ポートスタック /SFP+）

補足　スタッキングトポロジのその他の例については、「スタック接続について」を参照してください。

補足　本スイッチで実装される物理スタックは、他の製品で実装している物理スタックとは異なり機能を簡略化した Stacking Lite となります。

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。

注意 異なるスイッチのモデルでスタックを構成する場合、スタティックな BoxID を設定することを推奨します。新しく追加されたスイッチの BoxID のデバイスタイプが、コンフィグファイルの BoxID のデバイスタイプと異なる場合、新しく追加されたスイッチはデフォルトの設定を使用します。

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。

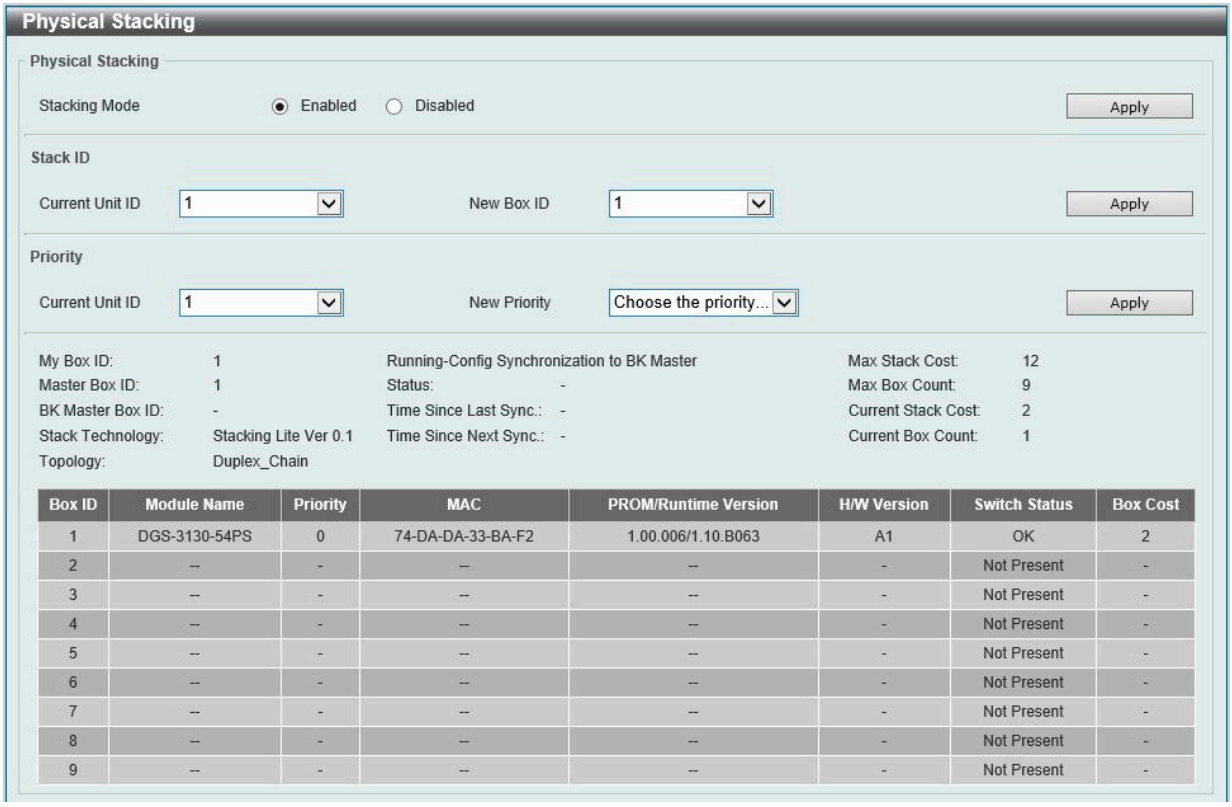


図 7-69　Physical Stacking 画面

以下の項目が表示されます。

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。 • 初期値：「Disabled」(無効)
Stack ID	
Current Unit ID	スタックにおけるスイッチのユニット番号を選択します。

項目	説明
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」はスイッチスタック内のスイッチに自動的にボックス番号を割り当てます。 • 選択可能範囲：1-9
Priority	
Current Unit ID	スタックにおけるスイッチのユニット番号を選択します。
New Priority	スイッチの優先度番号を表示します。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。 • 選択可能範囲：1-15

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

Stacking Bandwidth（スタッキング帯域）

本項目ではスタッキング帯域の設定、表示を行います。物理スタッキングを行う場合、ステータスを有効化し、2 ポート /4 ポートでのスタッキング設定を行う必要があります。

「2 ポート」の SFP+ または 10GBase-T 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。

- DGS-3130-30TS/30S/30PS は物理ポート 25 と 26、または 29 と 30 を「2 ポート」スタッキングに使用します。
- DGS-3130-54TS/54S/54PS は物理ポート 49 と 50、または 53 と 54 を「2 ポート」スタッキングに使用します。

「4 ポート」の SFP+ または Hybrid 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。

- DGS-3130-30TS/30S/30PS は物理ポート 25/26/29/30、または 27/28/29/30 を「4 ポート」スタッキングに使用します。
- DGS-3130-54TS/54S/54PS は物理ポート 49/50/53/54、または 51/52/53/54 を「4 ポート」スタッキングに使用します。

注意　スタッキング帯域の設定はスイッチをスタックする前に設定する必要があります。

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。

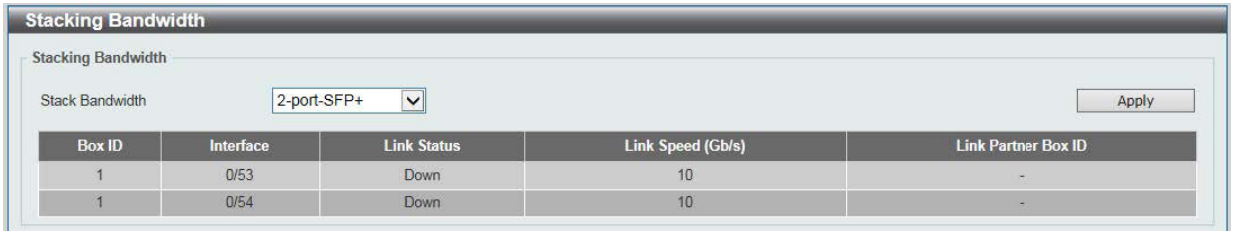


図 7-70　Stacking Bandwidth 画面

以下の項目が表示されます。

項目	説明
Stack Bandwidth	スタッキング帯域を選択します。 • 「2-Port-10GBaseT」- スタッキングに 10GBaseT ポートを 2 つ使用します。 • 「2-Port-SFP+」- スタッキングに SFP+ スロットを 2 つ使用します。 • 「4-Port-Hybrid」- スタッキングに 10GBaseT ポートを 2 つと、SFP+ スロットを 2 つ使用します。 • 「4-Port-SFP+」- スタッキングに SFP+ スロットを 4 つ使用します。

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

Virtual Stacking (SIM)（仮想スタック設定（SIM））

仮想（SIM）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）の概要

D-Link シングル IP マネジメントとは、スタックポートまたはモジュールを使用する代わりにイーサネット経由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。

- ネットワークを拡大し、増大する帯域幅に対する要求に対処しながら、小規模のワークグループや、ワイヤリングクローゼット（ユーザ接続エリア）を簡単に管理できるようになります。
- ネットワークに必要な IP アドレス数を減らします。
- スタック接続のために特別なケーブル配線を必要とせず、他のスタック技術ではトポロジ上の問題になる距離的制限を取り除きます。

D-Link シングル IP マネジメント（以下 SIM と呼びます）機能を搭載するスイッチには、以下の基本的なルールがあります。
- 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 / 無効にできます。また、SIM グループはご使用のネットワーク内でスイッチの操作に影響を与えることはありません。
- SIM には 3 つのクラスのスイッチがあります。Commander Switch（CS）はグループのマスタスイッチ、Member Switch（MS）は 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）は 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です。
- 1 つの SIM グループには、Commander Switch（CS）を 1 つだけ持つことができます。
- 特定の SIM グループ内のすべてのスイッチは、同じ IP サブネット（ブロードキャストドメイン）内にある必要があります。ルータを越えた位置にあるメンバの設定はできません。
- 1 つの SIM グループには、Commander Switch（番号：0）を含めずに、最大 32 台のスイッチ（番号：1-32）が所属できます。
- 同じ IP サブネット（ブロードキャストドメイン）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。
- マルチプル VLAN が設定されていると、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 3 つの異なる役割を持っています。

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、以下の特長を持っています。
   - IP アドレスを 1 つ持つ。
   - 他のシングル IP 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）- シングル IP グループに所属するスイッチで、CS からアクセスが可能です。MS は以下の特徴を持ちます。
   - 他のシングル IP グループの CS や MS ではない。
   - CS 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。CaS を SIM グループ内の MS として、本スイッチの機能を使用して手動で登録することが可能です。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。
   - 他のシングル IP グループの CS や MS ではない。
   - CS マネジメント VLAN 経由で CS に接続する。

上記の役割には、以下のルールを適用します。
- 各デバイスは、まず CS の状態から始まります。
- CS は、はじめに CaS に、その後 MS となり、SIM グループの MS へと遷移します。つまり CS から MS へ直接遷移することはできません。
- ユーザは、CS から CaS へ手動で遷移させることができます。
- 以下のような場合に MS から CaS に遷移します。
  - CS を介して CaS として設定される時。
  - CS から MS への Report パケットがタイムアウトになった時。
- ユーザが手動で CaS から CS に遷移するように設定できます。
- CS を介して CaS は MS に遷移するように設定されます。

SIM グループの CS として運用するスイッチを 1 台登録した後、スイッチを手動によりグループに追加して MS とします。CS はその後 MS へのアクセスのために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 へのアクセスを制御します。

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する代わりに、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。処理後、CS は MS から Response パケットを受け取り、これを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。しかし、自身の IP アドレスを持つ MS 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。

Single IP Settings（シングル IP 設定）

SIM の設定を行います。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。

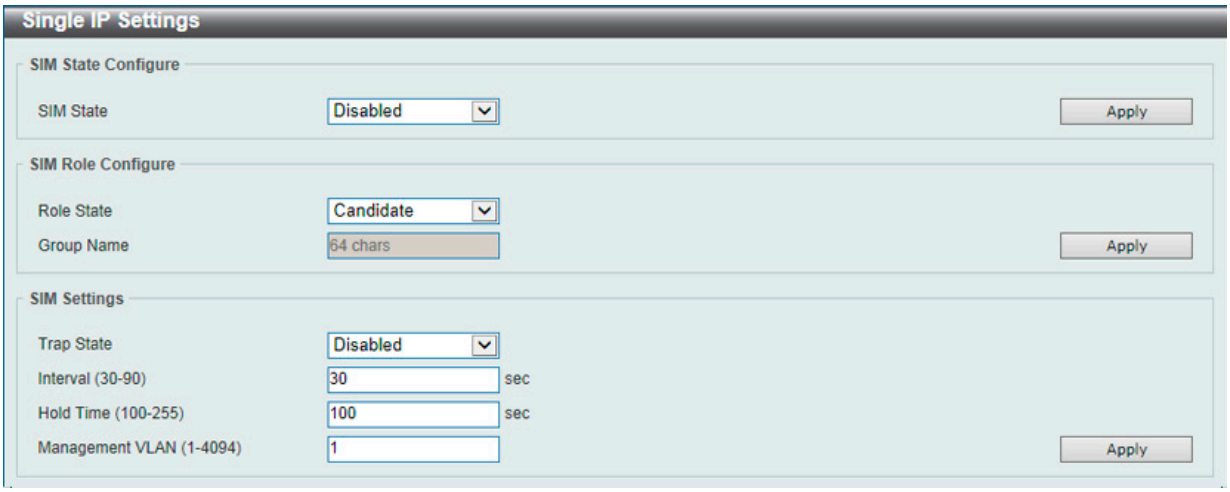


図 7-71　Single IP Settings 画面（CaS 無効状態）

以下の項目が表示されます。

項目	説明
SIM State Configure	
SIM State	SIM 機能を有効 / 無効に設定します。 • 初期値 :「Disabled」（無効）
SIM Role Configure	
Role State	プルダウンメニューからスイッチの 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）。ユーザは CS に他のスイッチを参加させて SIM グループを作成することができます。このオプションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。
Group Name	SIM グループ名を入力します。スイッチを SIM グループで分割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 (30-90)	スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔を設定します。 • 選択可能範囲：30-90（秒） • 初期値：30（秒）
Hold Time (100-255)	他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間を指定します。 • 選択可能範囲：100-255（秒） • 初期値は 100（秒）
Management VLAN	シングル IP マネージメントメッセージ VLAN ID を指定します。

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

スイッチを CS として登録すると、「Single IP Management」フォルダには 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 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。

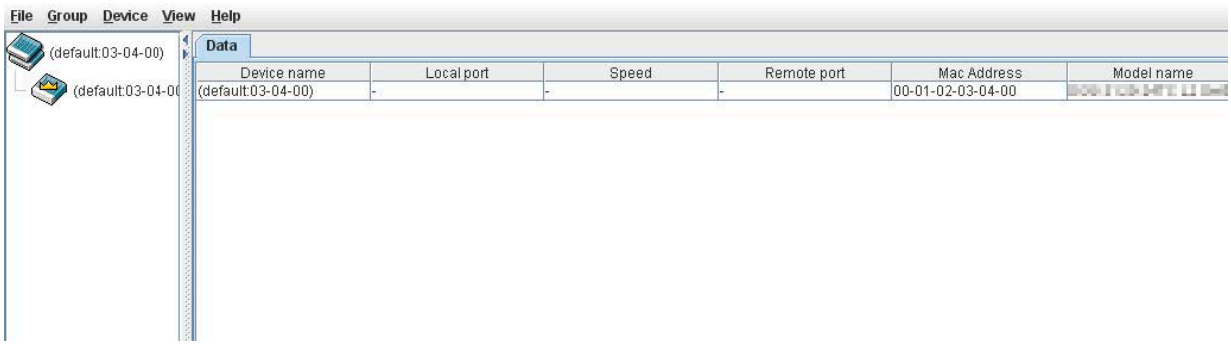


図 7-72　トポロジ画面

メニューバー

トポロジ画面には、デバイスの設定に使用するメニューバーが配置されています。



図 7-73　トポロジメニューバー

メニューバーには以下の 5 つのメニューが存在します。

「File」メニュー

- Print Topology – トポロジマップを印刷します。
- Preference – ポーリング間隔など表示プロパティを設定します。

「Group」メニュー

- Add to Group – グループに CaS を追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS を SIM グループに追加するための認証を行います。パスワードを入力して「Apply」ボタンをクリックするか、「Cancel」ボタンをクリックして画面を閉じます。



図 7-74　Input password ダイアログボックス

- Remove from Group – MS をグループから削除します。

「Device」メニュー

- Configure – 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 – ビューを最新の状態に更新します。
- Topology – トポロジビューを表示します。

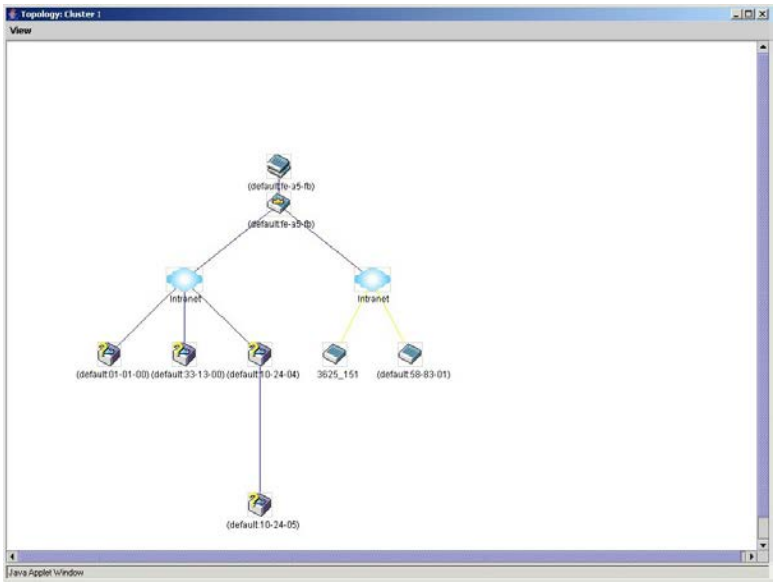


図 7-75　View >Topology 画面

「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指定すると、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。

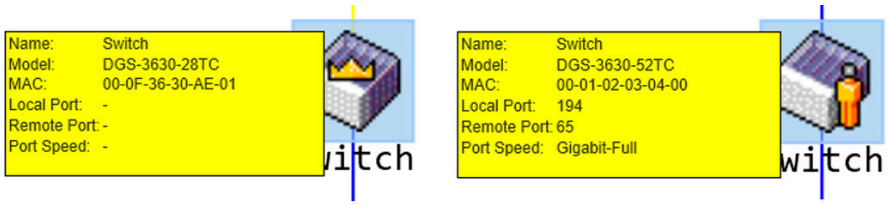


図 7-76　ツールヒントを利用したデバイス情報の表示

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。

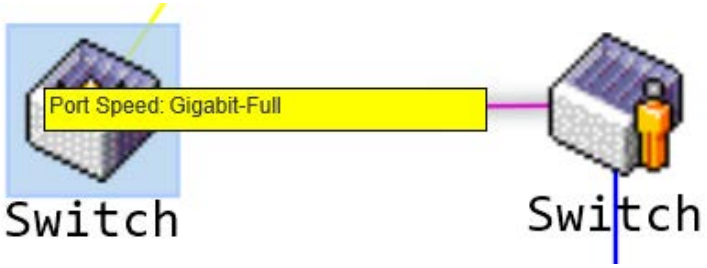


図 7-77　ツールヒントを利用したポート速度の表示

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、SIM グループ内でのスイッチの役割や、関連付けられているアイコンの種類に応じた様々な機能を実行できます。

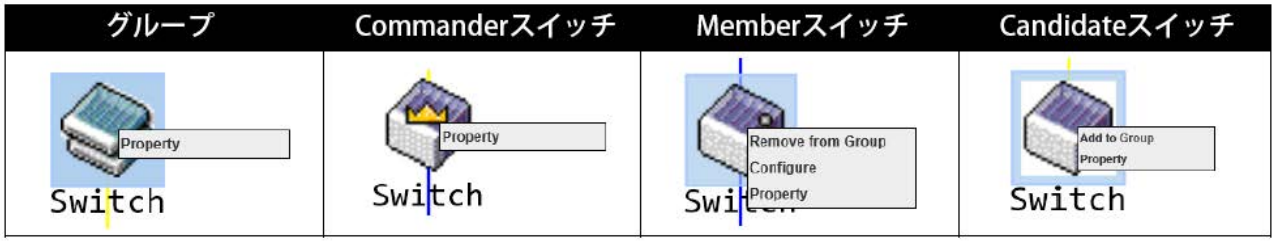


図 7-78　各アイコン上での右クリック

画面には以下の情報が表示されます。

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、スイッチの設定を可能にします。
Add to group （Candidate スイッチのみ）	CaS をグループに追加します。このオプションを選択すると、CaS が SIM グループに追加されるときにパスワード入力画面が表示されます。
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。

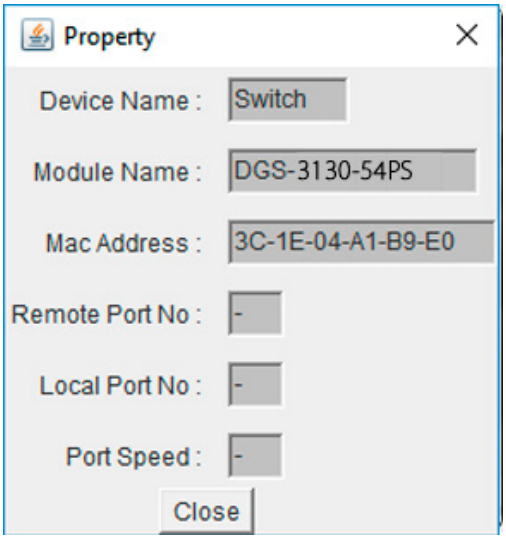


図 7-79　Property 画面

画面には以下の情報が表示されます。

項目	説明
Device Name	SIM グループ内のスイッチのデバイス名を表示します。デバイス名がない場合は、デフォルト名となり、識別のために MAC アドレスの終わり 6 桁が付加されます。
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。
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 – 現在の SIM バージョンなどの SIM 情報を表示します。

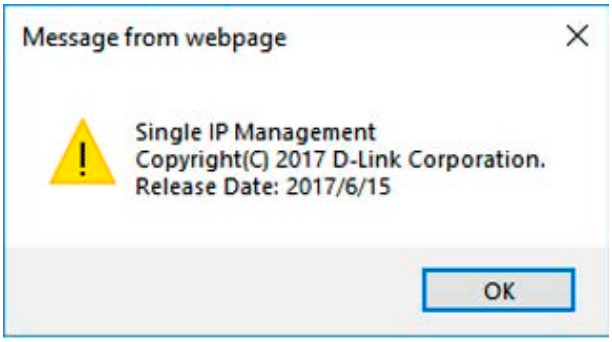


図 7-80　About ダイアログボックス

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。

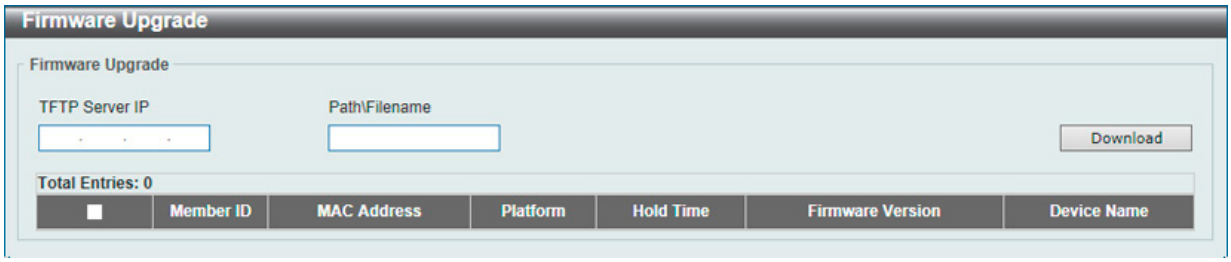


図 7-81　Firmware Upgrade 画面

ファームウェア更新手順

1. ダウンロード対象のスイッチを「Port」欄の下のチェックボックスで選択します。
2. ファームウェアを格納する「TFTP Server IP」を入力して、ファームウェアの「Path\Filename」を指定します。
3. 「Download」ボタンをクリックすると、ファイル転送が開始されます。

Configuration File Backup/ Restore（コンフィグレーションファイルの更新）

CS から MS に対して 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。

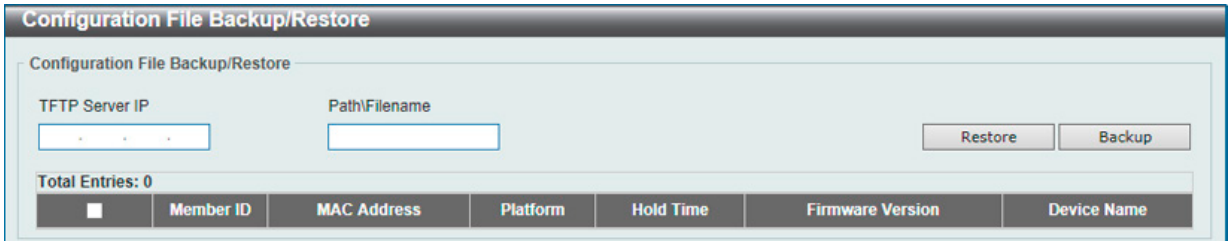


図 7-82　Configuration File Backup/Restore 画面

コンフィグレーションファイル更新手順

1. コンフィグレーションファイルのアップデート対象のスイッチを「Port」欄の下のチェックボックスで選択します。
2. ファームウェアを格納する「TFTP Server IP」を入力して、ファームウェアの「Path\Filename」を指定します。
3. 「Restore」ボタンをクリックすると、TFTP サーバからファイル転送が開始されます。「Backup」ボタンをクリックすると、TFTP サーバにファイルがバックアップされます。

Upload Log File（ログファイルのアップロード）

CS は、MS から指定したサーバにログファイルをアップロードすることができます。

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。

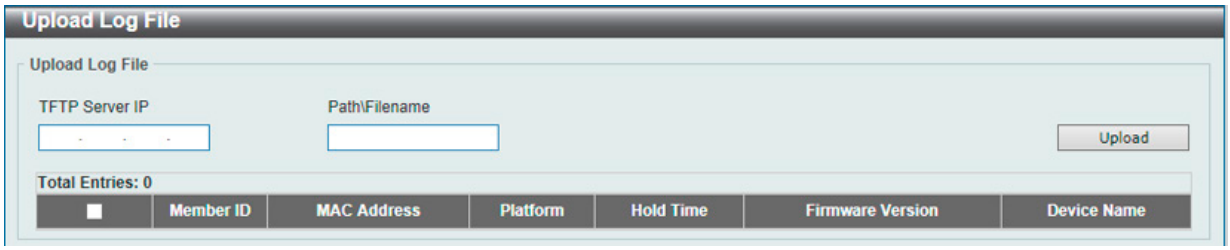


図 7-83　Upload Log File 画面

ログファイルのアップロード更新手順

1. ログを格納する「TFTP Server IP」と MS のログファイルの「Path\Filename」を入力します。
2. 「Upload」ボタンをクリックすると、TFTP サーバにログファイルが送信されます。

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

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

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

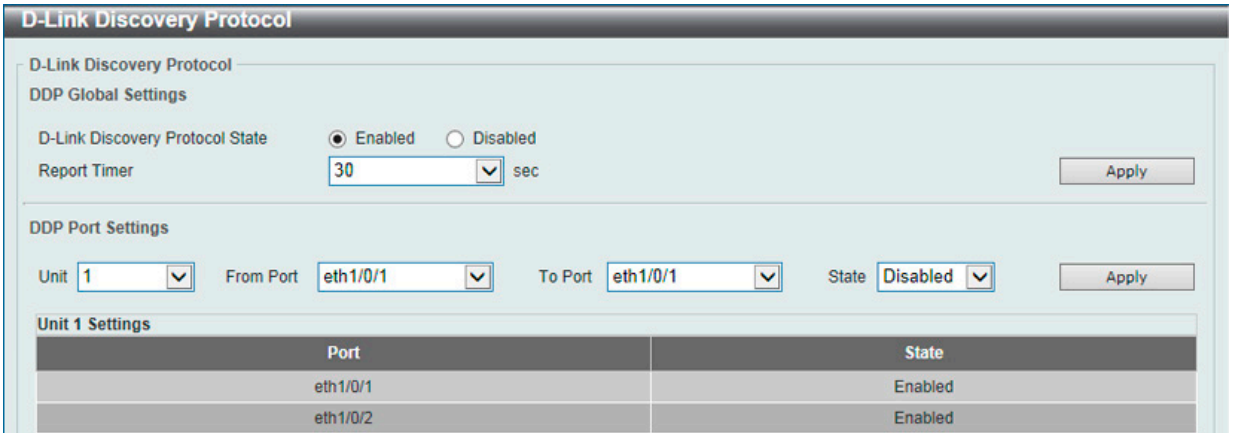


図 7-84　D-Link Discovery Protocol 画面

設定には以下の項目を使用します。

項目	説明
D-Link Discovery Protocol	
D-Link Discovery Protocol State	DDP 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（秒）を指定します。 • 選択肢：「30」「60」「90」「120」「Never」
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	DDP ポートを有効 / 無効に設定します。

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

SMTP Settings（SMTP 設定）

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

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。

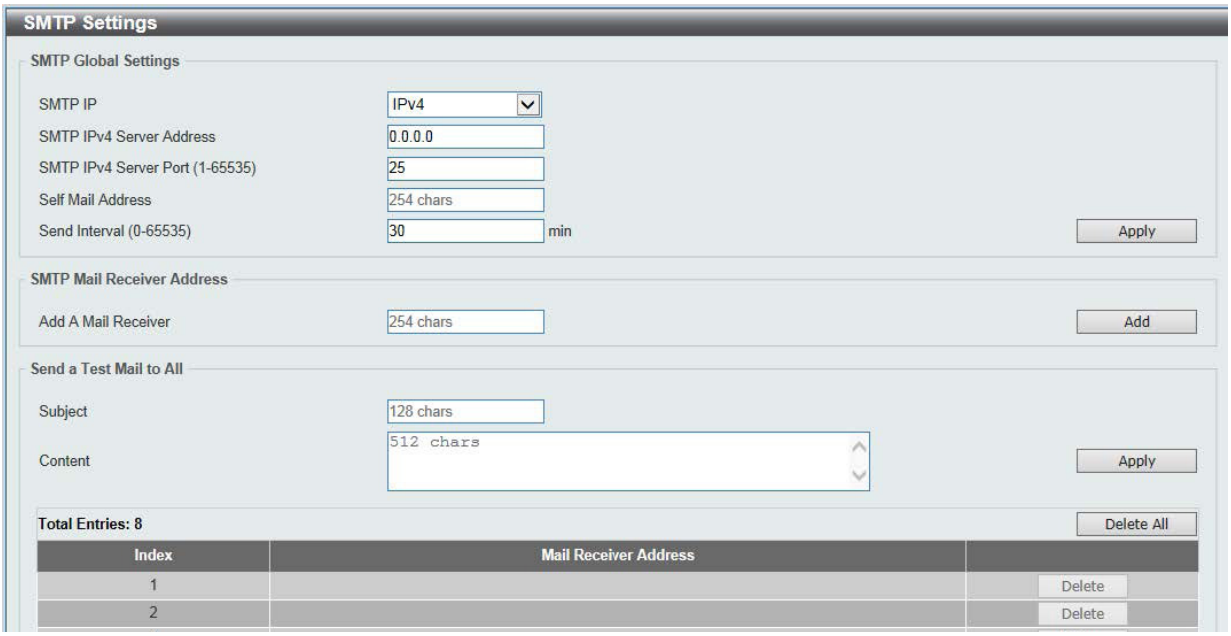


図 7-85　SMTP Settings 画面

設定には以下の項目を使用します。

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	SMTP サーバ IPv4 アドレスを指定します。
SMTP IPv6 Server Address	SMTP サーバ IPv6 アドレスを指定します。
SMTP IPv4 Server Port	SMTPIPv4 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	SMTPIPv6 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）

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

SMTP Mail Receiver Address

項目	説明
Add A Mail Receiver	受信する 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、設定内容に基づく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 字文字以内）

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

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。再起動スケジュールは 30 日以内に設定する必要があります。再起動スケジュールが実行され、再起動が開始されると、スイッチが再起動スケジュールを使用して再起動をした旨のログメッセージが生成されます。再起動、またはシャットダウン後に、再起動スケジュールは自動的に削除されます。再起動スケジュールが実行される前に、スイッチが手動で再起動やシャットダウンされた場合は、指定の再起動スケジュールはキャンセルされます。

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。

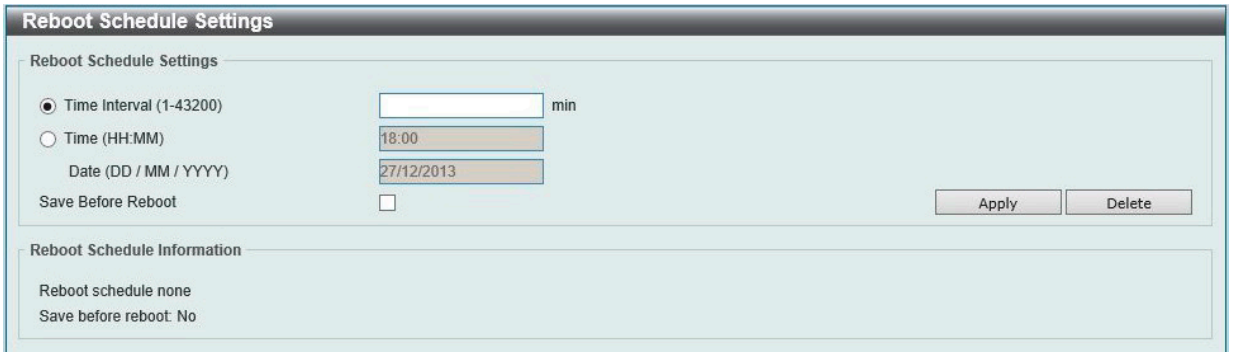


図 7-86　Reboot Schedule Settings 画面

以下の項目が表示されます。

項目	説明
Time Interval	再起動スケジュールの間隔を選択します。再起動は指定の間隔を過ぎると実行されます。 • 設定可能範囲：1-43200（分）（30 日）
Time	再起動を実行する時間を指定します。24 時間のフォーマットを使用します。(例；21:30） 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。
Date	再起動を実行する日付を指定します。「DD/MM/YYYY」のフォーマットを使用します。(例；23/12/2015） 30 日以内の再起動スケジュールが指定可能です。
Save Before Reboot	再起動実行前に行われた設定変更について保存します。

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

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

PPPoE の Circuit ID 挿入を設定します。

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。

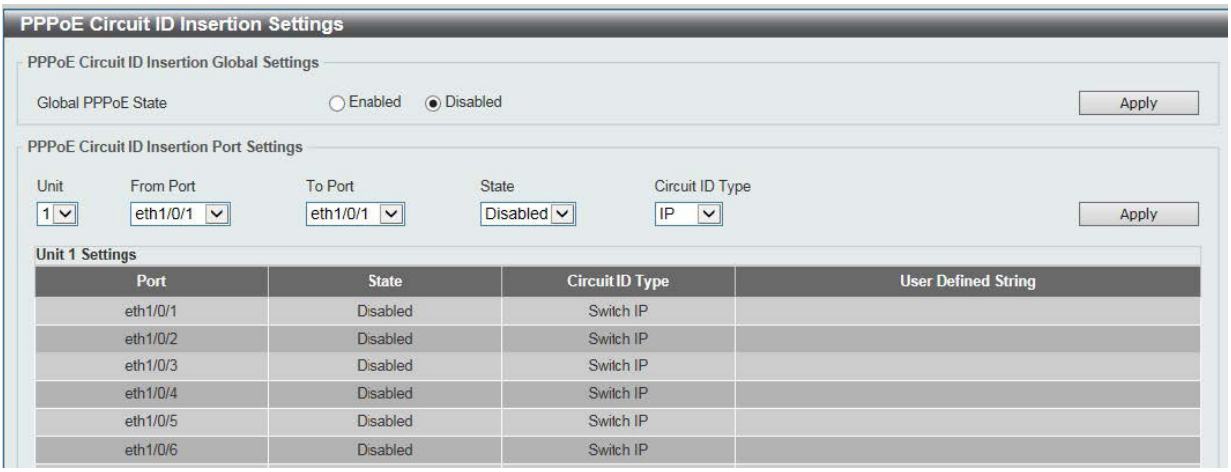


図 7-87　PPPoE Circuit ID Insertion Settings 画面

以下の項目が表示されます。

項目	説明
PPPoE Circuit ID Insertioin Global Settings	
Global PPPoE State	PPPoE Circuit ID 挿入を有効 / 無効に設定します。
PPPoE Circuit ID Insertioin 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	指定ポートで PPPoE Circuit ID 挿入を有効 / 無効に設定します。
Circuit ID Type	Circuit ID タイプを選択します。 • 選択肢：「IP」「MAC」「UDF」

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

SD Card Management（SD カード管理）

USB ドライバストレージなどのリムーバブル機器の設定を行います。

SD Card Backup Settings（SD カードへのバックアップ設定）

USB ストレージのバックアップの表示、設定を行います。SD 管理バックアップスケジュールエントリの作成、編集を行います。

Management > SD Card Management > SD Card Backup 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 7-88　SD Card Backup Settings 画面

以下の項目が表示されます。

SD Card Backup Settings

項目	説明
Backup Entry Name	SD カード管理バックアップスケジュール名を指定します。（32 文字以内）

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

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

エントリの編集

「Edit」ボタンをクリックすると、以下のパラメータを変更することができます。

項目	説明
Time Range	スケジュール範囲の指定を行います。
Type	バックアップの対象を選択します。 • 「Configuration」- バックアップの対象をコンフィグレーションに指定します。 • 「Log」- バックアップの対象をシステムログに指定します。
File Name	宛先ファイル名とパスを指定します。
State	バックアップスケジュールを有効 / 無効に設定します。

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

「Delete」ボタンをクリックして、エントリを削除します。

SD Card Execute Settings（SD カード実行設定）

USB ストレージからスイッチのファイルシステムへの設定を手動で実行するために使用します。

Management > SD Card Management > SD Card SD Card Execute 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。

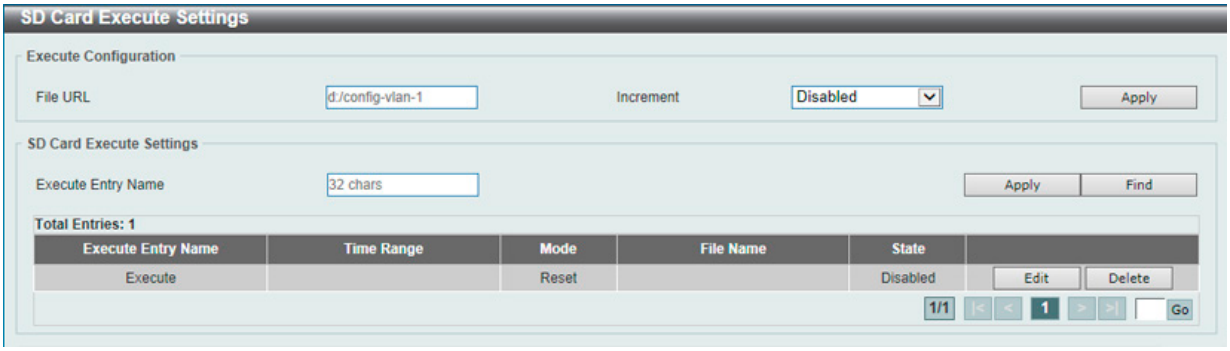


図 7-89　SD Card Execute Settings 画面

以下の項目が表示されます。

項目	説明
Execute Configuration	
File URL	設定ファイルの URL を指定します。現在のディレクトリが SD カードファイルシステムのディレクトリではない場合、フルパスを入力する必要があります。
Increment	Increment 機能を設定します。 • 「Increase」- 設定の実行前に、現在の設定がクリアされません。 • 「Reset」- 設定の実行前に現在の設定がクリアされます。
SD Card Execute Settings	
Execute Entry Name	実行エントリ名を指定します。（32 文字以内）

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

「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。

エントリの編集

特定のエントリを設定するには、「Edit」ボタンをクリックして以下のパラメータを変更します。

項目	説明
Time Range	適用するタイムレンジを指定します。
Mode	モードを指定します。 • 「Increase」- 設定の実行前に、現在の設定がクリアされません。 • 「Reset」- 設定の実行前に現在の設定がクリアされます。
File URL	設定ファイル名とパスを指定します。
State	スケジュール実行の有効 / 無効を設定します。

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

「Delete」ボタンをクリックして、エントリを削除します。

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

第 8 章　L2 Features（L2 機能の設定）

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。
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。

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。

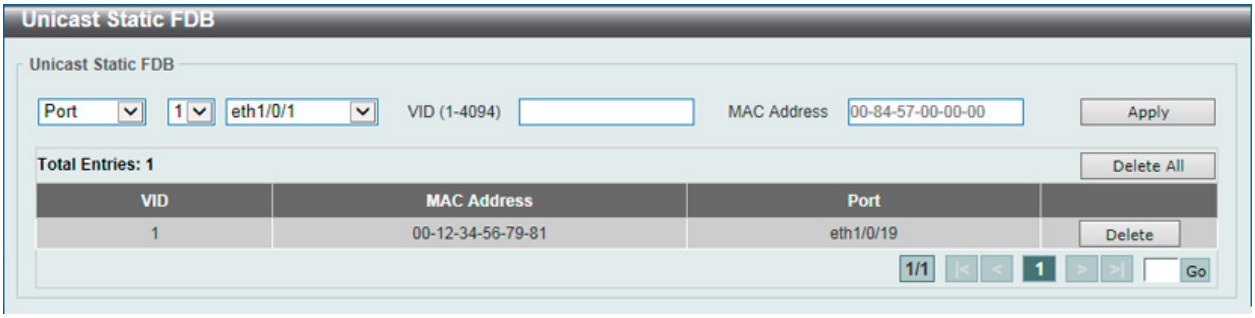


図 8-1　Unicast Static FDB 画面

以下の項目が表示されます。

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 アドレスを破棄します。 • 「Port」- 指定 MAC アドレスのあるポート番号を指定します。「ユニット ID: ポート番号」（例 1:5）または「ポート番号」（例 5）という形式とします。ポート番号だけを入力する場合、ユニット番号の初期値は 1 となります。 • 「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	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、ポート番号を入力します。
VID	ラジオボタンをクリックし、関連するユニキャスト MAC アドレスが存在する VLAN ID を入力します。
MAC Address	パケットがスタティックに送信される宛先の MAC アドレス。ユニキャスト MAC アドレスを指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。
「Delete All」ボタンをクリックして、テーブル上のすべてのエントリを削除します。

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

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。

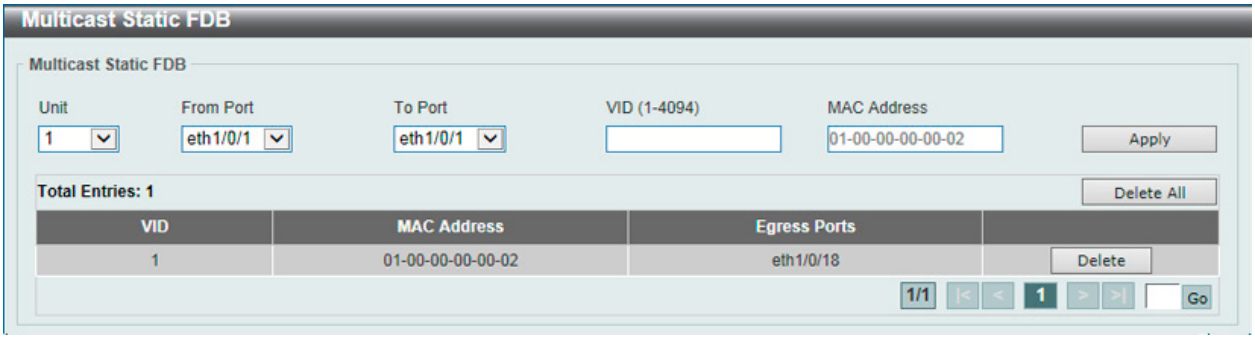


図 8-2　Multicast Static FDB 画面

以下の項目が表示されます。

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。
VID	指定の Multicast MAC アドレスが属する VLAN の VLAN ID を指定します。

項目	説明
MAC Address	マルチキャストパケットの送信先 MAC アドレスを入力します。マルチキャスト MAC アドレスを指定します。宛先 MAC アドレスの形式は「01-xx-xx-xxxxxx」です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。
「Delete All」ボタンをクリックして、テーブル上のすべてのエントリを削除します。

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

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

スイッチの MAC アドレステーブルを参照します。

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

Global Settings（グローバル設定タブ）

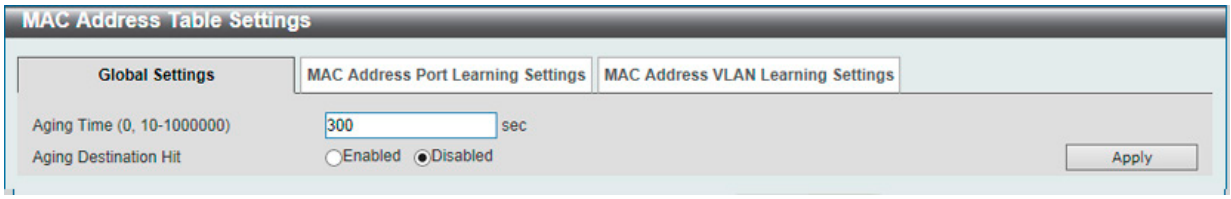


図 8-3　MAC Address Table Settings 画面（Global Settings）

以下の項目が表示されます。

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。 設定した時間中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。 • 入力可能範囲：0、10 ～ 1000000（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。

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

注意　Chip 制限により MAC アドレステーブルのエージングアウトには設定値の 1.5 倍～ 2 倍の時間がかかります。

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

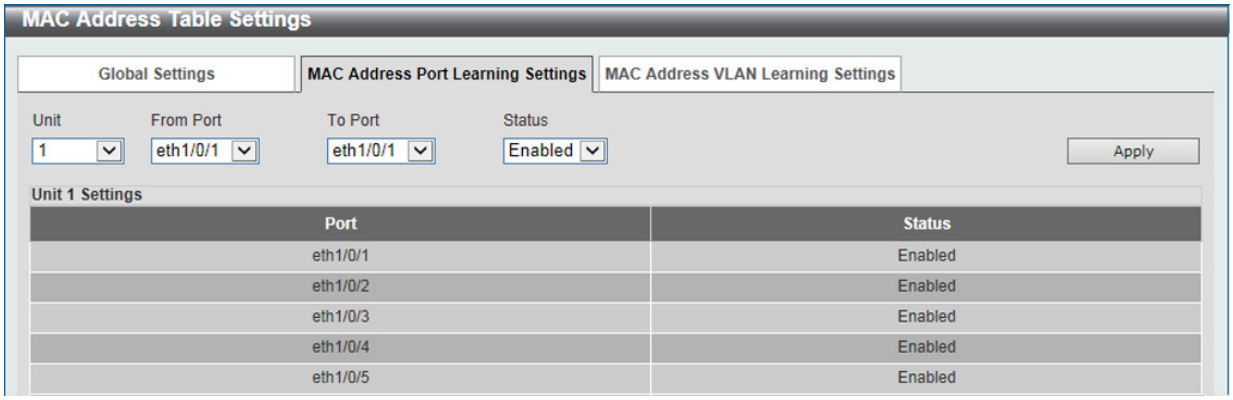


図 8-4　MAC Address Table Settings (MAC Address Port Learning Settings) 画面

以下の項目が表示されます。

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。
Status	MAC アドレスラーニングを有効 / 無効に設定します。

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

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

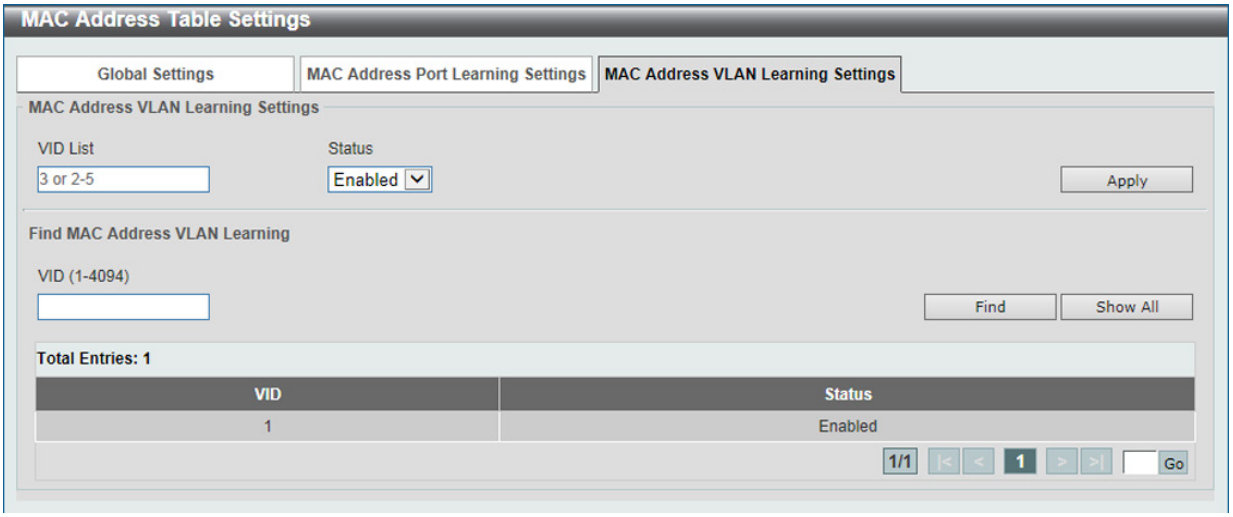


図 8-5　MAC Address Table Settings (MAC Address VLAN Learning Settings) 画面

以下の項目が表示されます。

項目	説明
VID List	表示するフォワーディングテーブルの VLAN ID を入力します。コンマ区切りで複数の ID を指定、または VID 範囲をハイフンで指定することも可能です。
Status	MAC アドレスラーニングを有効 / 無効に設定します。

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

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

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。

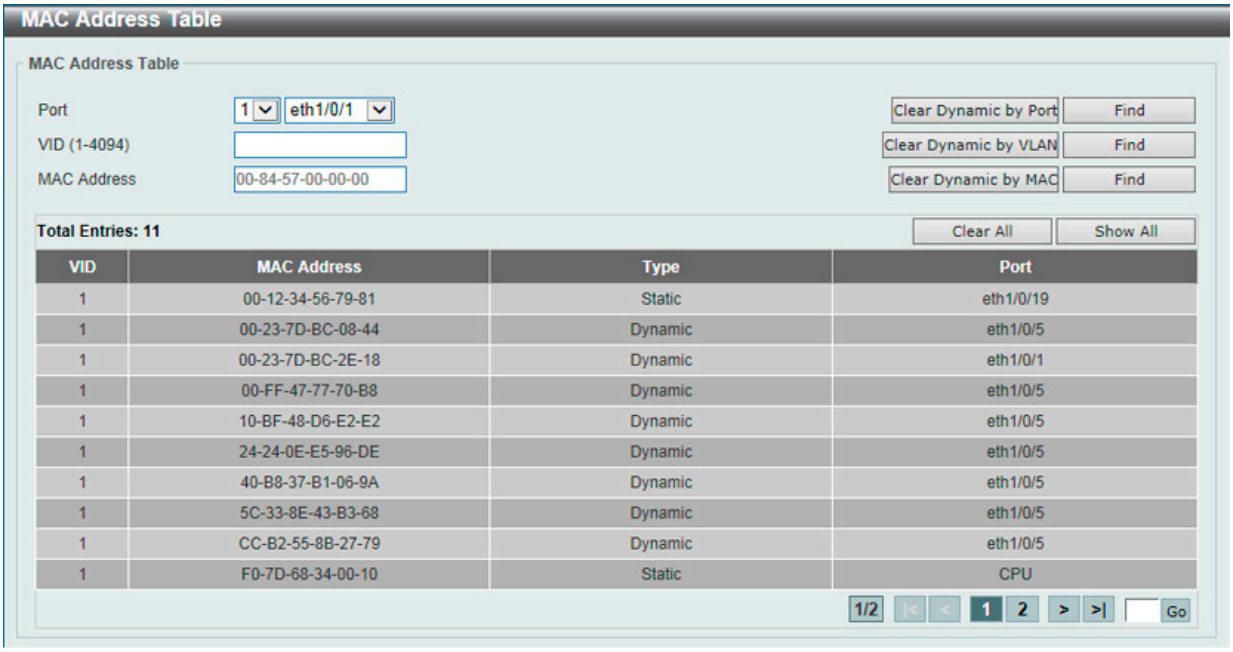


図 8-6　MAC Address Table 画面

以下の項目が表示されます。

項目	説明
Port	削除 / 表示するユニット ID およびポート番号を指定します。
VID	削除 / 表示するフォワーディングテーブルの VLAN ID を入力します。

項目	説明
MAC Address	削除 / 表示するフォワーディングテーブルの MAC アドレスを入力します。

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

エントリの検索 / 表示

「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。
「Show 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表示します。

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、テーブルのすべてのエントリを削除します。

MAC Notification（MAC 通知）

スイッチの MAC 通知をグローバルに設定します。また、スイッチの各ポートに MAC 通知を設定します。

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。

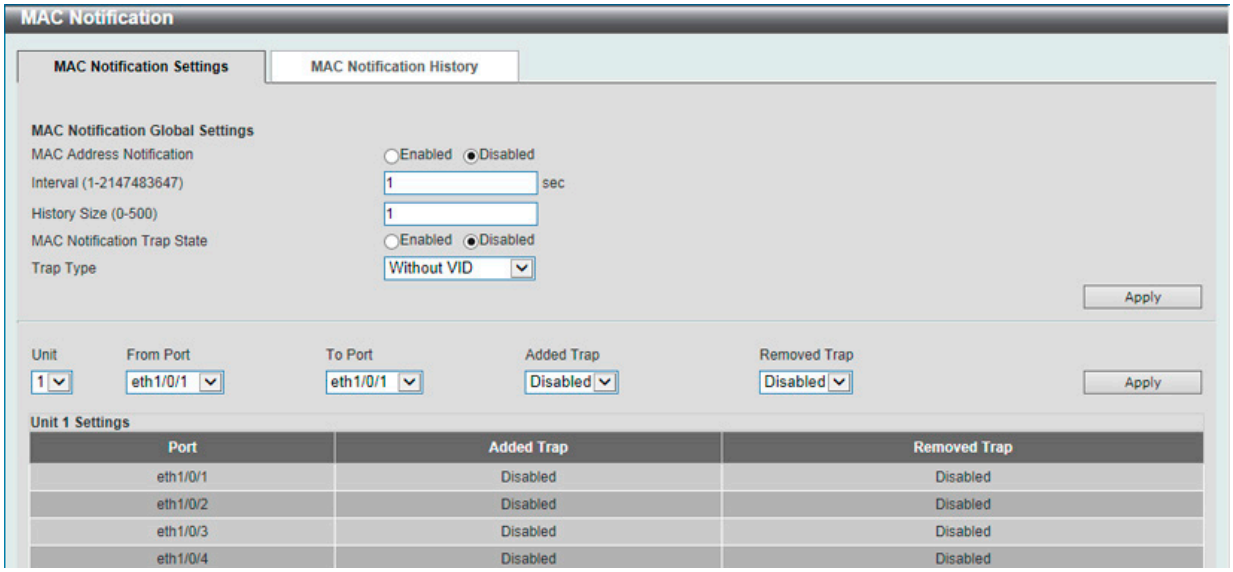


図 8-7　MAC Notification 画面

以下の項目が表示されます。

項目	説明
MAC Notification Global Settings	
MAC Address Notification	スイッチ上の 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。（最大 500 エントリ） • 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	MAC 通知設定を有効または無効に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。

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

MAC Notification History タブ

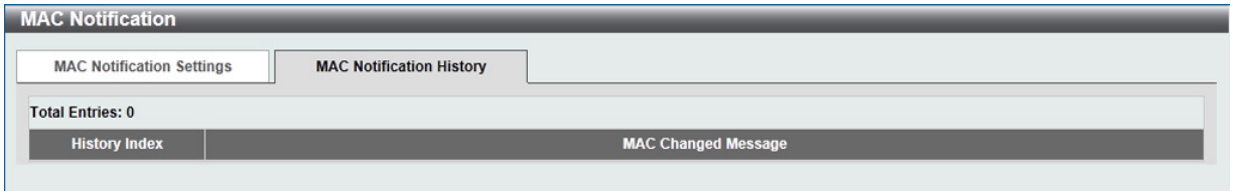


図 8-8　MAC Notification History 画面

MAC 通知メッセージの履歴が表示されます。

VLAN（VLAN 設定）

スイッチの VLAN 設定を行います。

802.1Q VLAN（802.1Q VLAN）

802.1Q VLAN を設定します。

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

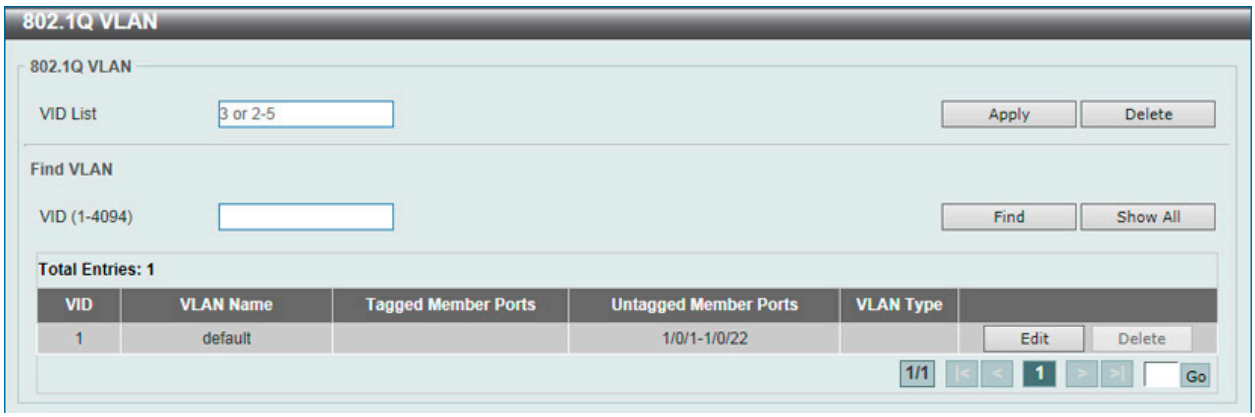


図 8-9　802.1Q VLAN Settings 画面

以下の項目が表示されます。

項目	内容
802.1Q VLAN	
VID List	作成する VID の範囲を指定します。
Find VLAN	
VID	表示する VLAN ID を指定します。 • 設定可能範囲：1-4094

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

エントリの検索 / 表示
「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。
「Show 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表示します。

エントリの削除
画面上部の「Delete」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。
または、画面下部の該当エントリの「Delete」ボタンをクリックします。

エントリの編集
「Edit」ボタンをクリックして、VLAN 名を編集します。

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

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

802.1v Protocol 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）

プロトコル VLAN グループを作成し、そのグループにプロトコルを追加します。802.1v プロトコル VLAN グループ設定は、各プロトコルのためにマルチプル VLAN をサポートし、同じ物理ポートに異なるプロトコルを持つタグなしポートの設定が可能です。例えば、同じ物理ポートに 802.1Q と 802.1v タグなし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。

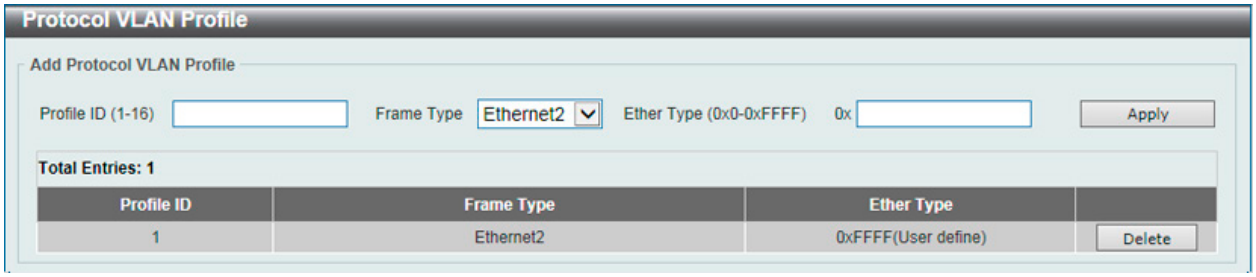


図 8-10　Protocol VLAN Profile 画面

以下の項目が表示されます。

項目	説明
Profile ID	802.1v プロトコル VLAN プロファイル ID 番号を指定します。 • 設定可能範囲：1-16
Frame Type	フレームタイプを選択します。本機能では、パケットヘッダに含まれるタイプオクテットを検証して、パケットとプロトコル定義 VLAN のマッピングを実行し、関連するプロトコルタイプを検出します。 • 選択肢：「Ethernet 2」「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。フレームタイプによって、オクテット文字列は以下のいずれかとなります。 • 「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 などです。 • 「IEEE802.3 SNAP」- 16 ビット (2 オクテット) の 16 進数です。 • 「IEEE802.3 LLC」- 2 オクテットの IEEE 802.2 Link Service Access Point(LSAP) ペアです。1 番目のオクテットは Destination Service Access Point（DSAP）のための値であり、2 番目のオクテットは送信元のための値です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、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。テーブルの下半分は定義済みのすべての設定を表示します。

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。

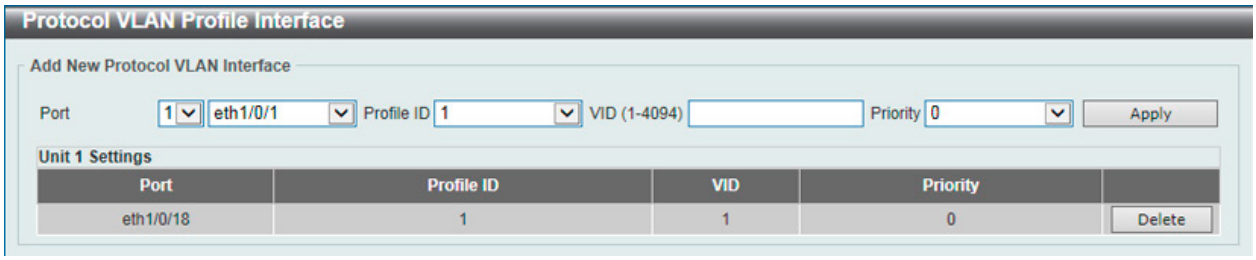


図 8-11　Protocol VLAN Profile Interface 画面

以下の項目が表示されます。

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 Profile ID を選択します。
VID	VID を入力します。 • 設定可能範囲：1-4094
Priority	802.1p デフォルトプライオリティを選択します。この設定は、スイッチに設定済みの 802.1p デフォルトプライオリティを書き換えるために使用されます。このプライオリティ値に一致するパケットは定義済みの CoS キューに送信されます。 • 設定可能範囲：1-7

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

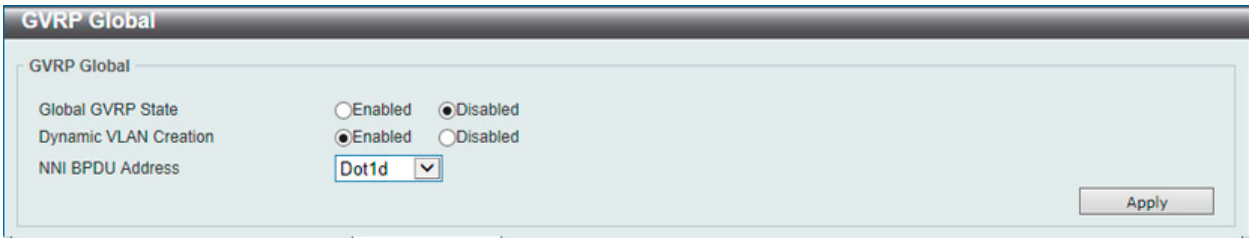


図 8-12　GVRP Global 画面

以下の項目が表示されます。

項目	説明
Global GVRP State	GVRP 状態をグローバルに有効 / 無効にします。 • 初期値：「Disabled」（無効）
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。これにより、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します。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」

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

GVRP Port（GVRP ポート設定）

GVRP ポート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。

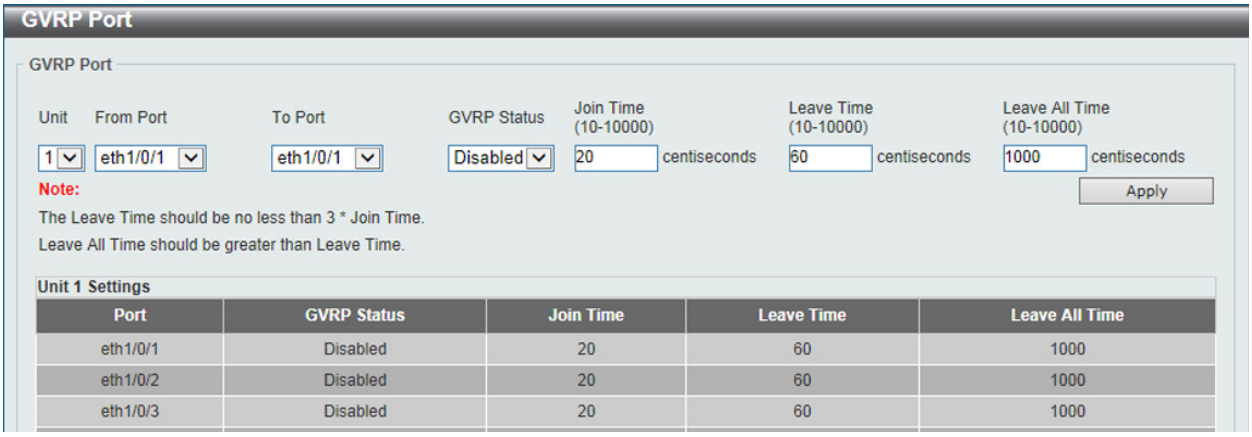


図 8-13　GVRP Port 画面

以下の項目が表示されます。

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。
GVRP Status	GVRP の各ポートにおけるステータスを設定します。有効にするとポートが自動的に VLAN のメンバになります。 •「Enabled」- 選択したポートで GVRP を有効にします。 •「Disabled」- 選択したポートで GVRP を無効にします。（初期値）
Join Time	で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（センチ秒）

項目	説明
Leave Time	センチ秒で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	センチ秒で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

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

GVRP Advertise VLAN（GVRP Advertise VLAN 設定）

GVRP advertised VLAN の設定、表示を行います。

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

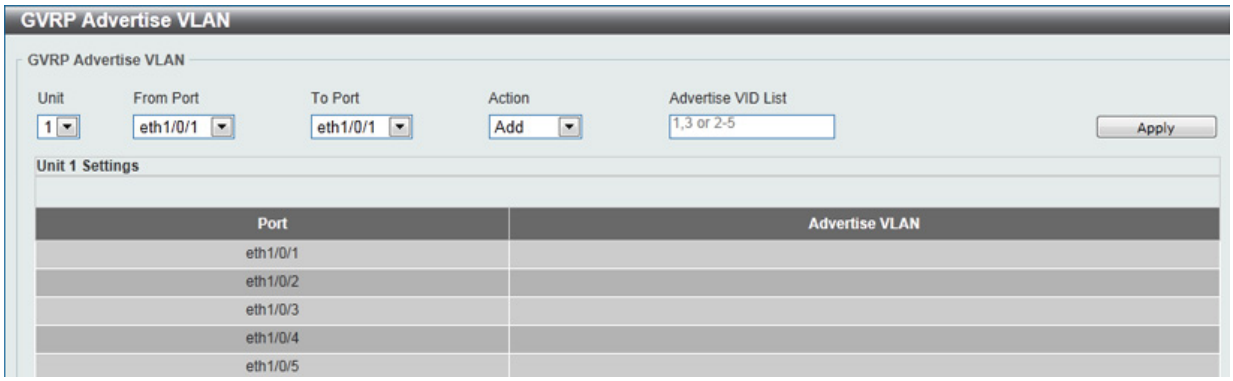


図 8-14　GVRP Advertise VLAN 画面

以下の項目が表示されます。

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。
Action	アドバタイズ VLAN によるポートマッピングの動作を選択します。「All」を選択するとすべてのアドバタイズ VLAN が使用されます。 • 選択肢：「All」「Add」「Remove」「Replace」
Advertise VID List	アドバタイズ VLAN ID を入力します。

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

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。

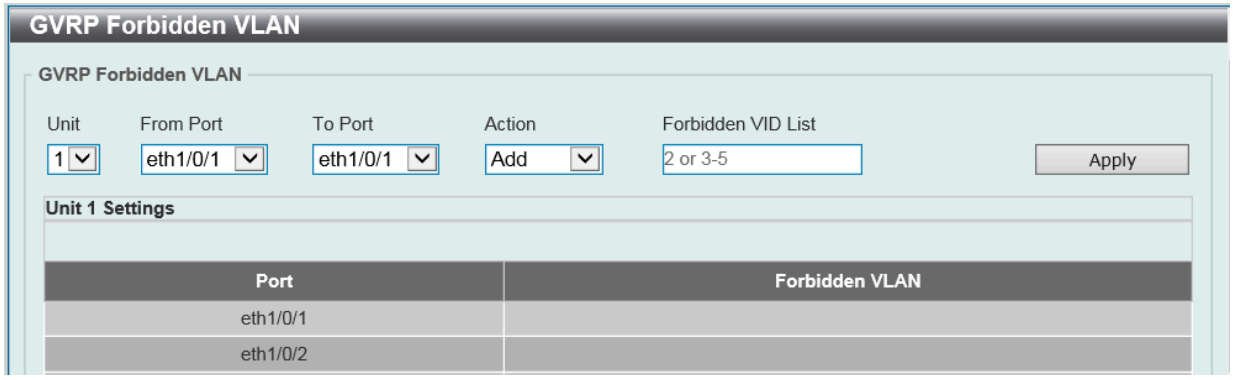


図 8-15　GVRP Forbidden VLAN 画面

以下の項目が表示されます。

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。

項目	説明
Action	禁止 VLAN によるポートマッピングの動作を選択します。「All」を選択するとすべての禁止 VLAN が使用されます。 • 選択肢：「All」「Add」「Remove」「Replace」
Forbidden VID List	禁止 VLAN ID を入力します。

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

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。

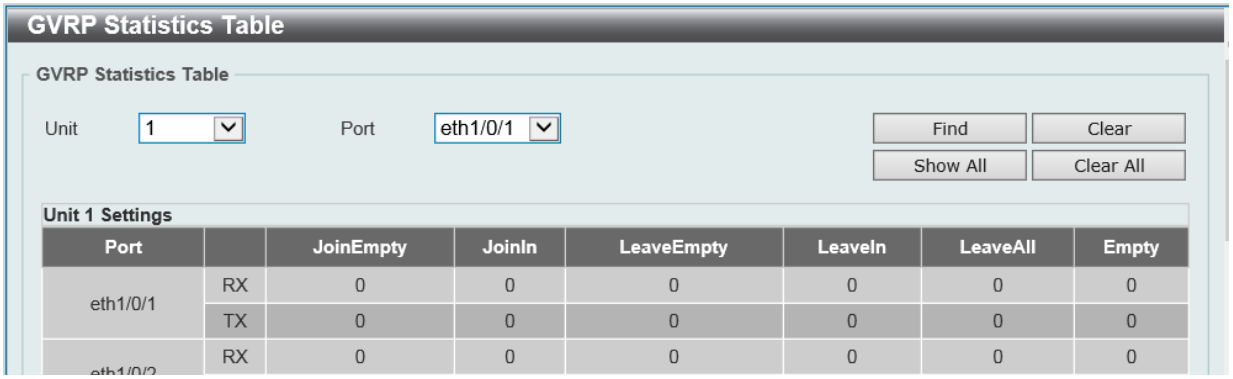


図 8-16　GVRP Statistics Table 画面

以下の項目が表示されます。

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 / 表示

「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。
「Show 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、指定条件に基づく統計情報をクリアします。
「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クリアします。

Asymmetric VLAN（Asymmetric VLAN 設定）

Asymmetric VLAN 設定します。

補足　本機能は将来のファームウェアでサポート予定です。

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。

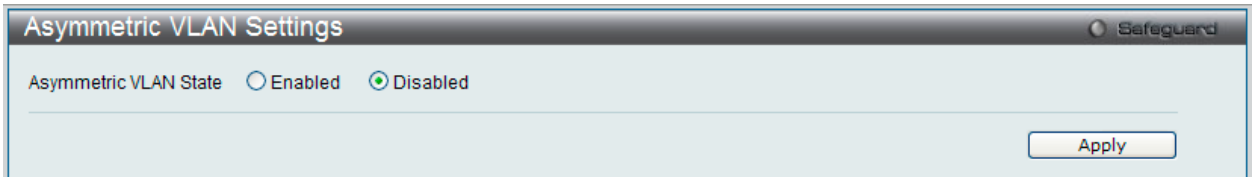


図 8-17　Asymmetric VLAN 画面

以下の項目が表示されます。

項目	説明
Asymmetric VLAN State	Asymmetric VLAN を有効 / 無効に設定します。

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

MAC VLAN（MAC VLAN 設定）

新しく MAC ベース VLAN エントリを作成し、設定済みのエントリを検索 / 編集 / 削除します。スタティック MAC ベース VLAN エントリが作成されると、ポートの VLAN は接続するデバイスによって変わります。

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。

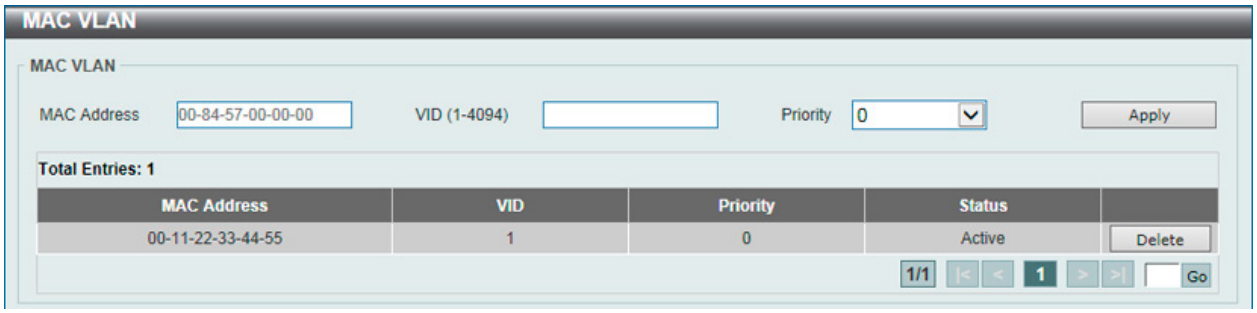


図 8-18　MAC VLAN 画面

以下の項目が表示されます。

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	プルダウンメニューを使用して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

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

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

VLAN Interface（VLAN インタフェース設定）

VLAN インタフェースの設定を行います。

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

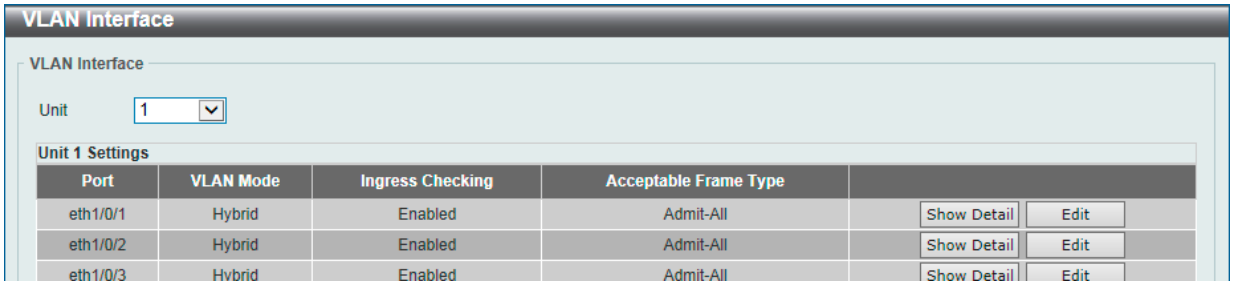


図 8-19　VLAN Interface 画面

以下の項目が表示されます。

項目	説明
Unit	設定 / 表示するユニットを指定します。

「Edit」ボタンをクリックすると設定を編集することができます。
「Show Detail」ボタンをクリックして、指定インタフェースの VLAN について詳細情報を表示します。

Show Deteil（VLAN 詳細情報の表示）

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



図 8-20　VLAN Interface (VLAN Detail) 画面

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

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

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

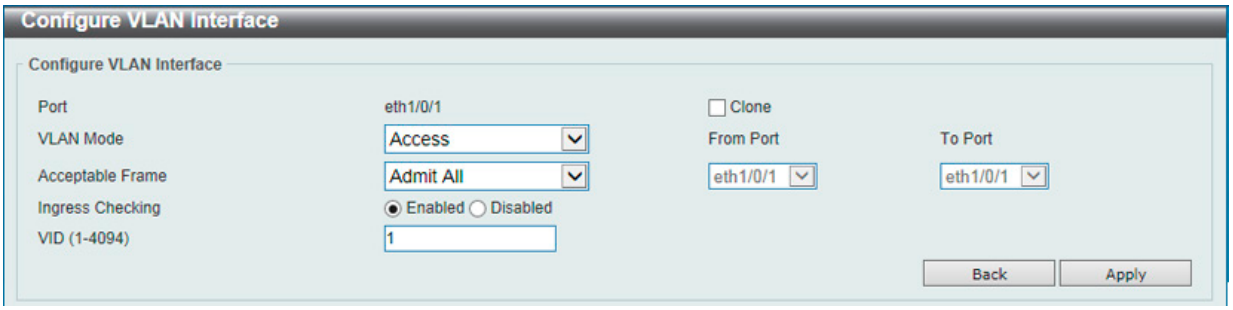


図 8-21　Configure VLAN Interface - Access 画面

以下の項目が表示されます。

項目	説明
VLAN Mode	VLAN モードをから選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」
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	設定する「VLAN ID」を指定します。 • 設定可能範囲：1-4094
Clone	クローンを有効にします。
From Port / To Port	本設定を適用するポート範囲を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

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

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

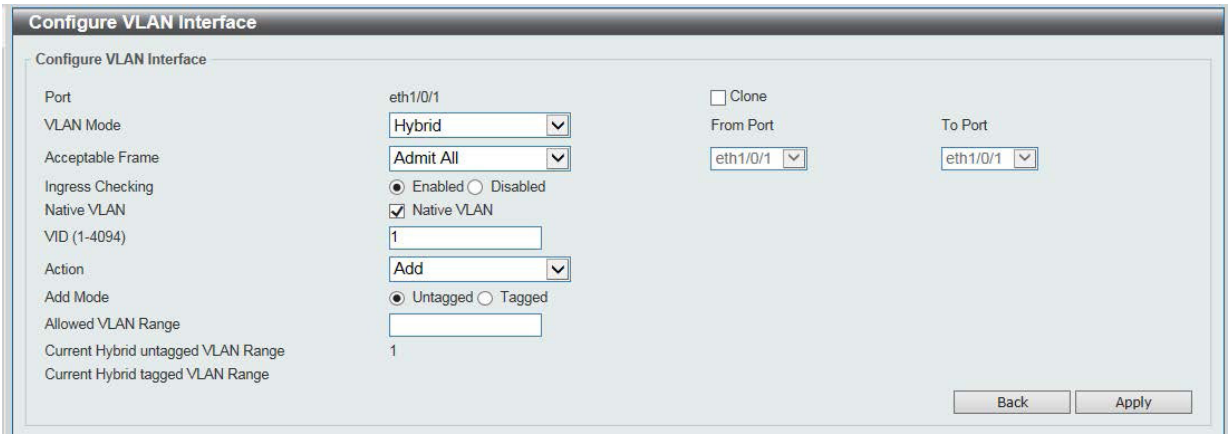


図 8-22　Configure VLAN Interface - Hybrid 画面

以下の項目が表示されます。

項目	説明
VLAN Mode	VLAN モードをから選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」
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。
VID	「Native VLAN」を有効にした後、「Native VLAN」に設定する「VLAN ID」を指定します。 • 設定可能範囲：1 -4094
Action	実行する動作を選択します。 • 選択肢：「Add」「Remove」「Tagged」「Untagged」
Add Mode	「Add Mode」のパラメータに「Untagged」または「Tagged」を追加します。
Allowed VLAN Range	許可する VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	本設定を適用するポート範囲を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前画面に戻ります。

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

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

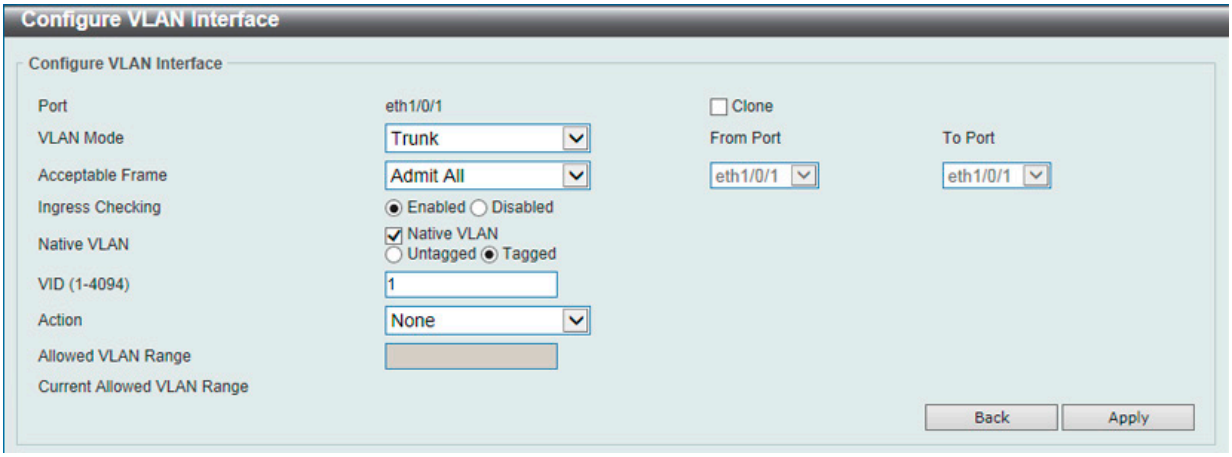


図 8-23　Configure VLAN Interface - Trunk 画面

以下の項目が表示されます。

項目	説明
VLAN Mode	VLAN モードをから選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」

項目	説明
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。また、Native VLAN による「Untagged」または「Tagged」フレームのサポートについて指定します。
VID	「Native VLAN」を有効にした後、「Native VLAN」に設定する「VLAN ID」を指定します。 • 設定可能範囲：1-4094
Action	実行する動作を選択します。 • 選択肢：「All」「Add」「Remove」「Except」「Replace」
Allowed VLAN Range	許可する VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	本設定を適用するポート範囲を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前画面に戻ります。

VLAN Mode - 802.1Q-Tunnel（VLAN モードが 802.1Q-Tunnel の場合）

「**L2 Features > VLAN > VLAN Interface**」画面で「Edit」をクリックします。「802.1Q-Tunnel」が選択すると次の画面が表示されます。

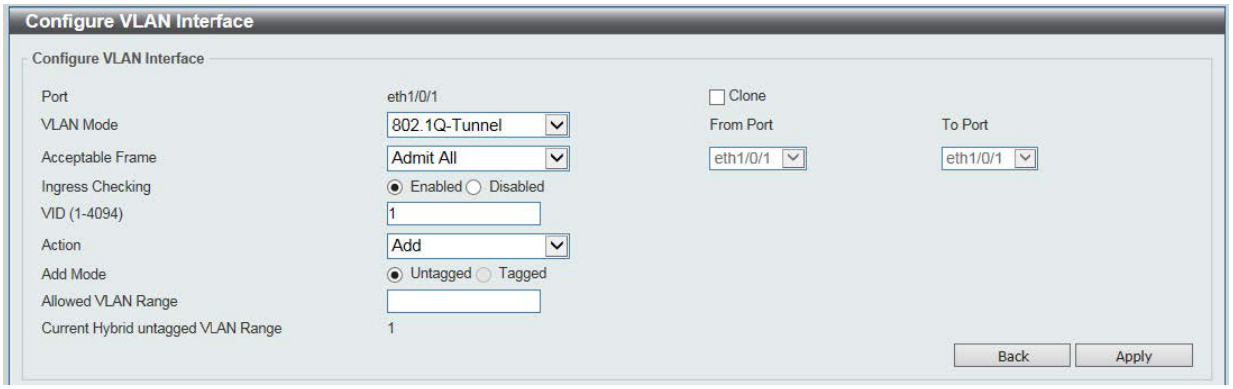


図 8-24　Configure VLAN Interface - 802.1Q-Tunnel 画面

以下の項目が表示されます。

項目	説明
VLAN Mode	VLAN モードをから選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」
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 に設定する「VLAN ID」を指定します。 • 設定可能範囲：1-4094
Action	実行する動作を選択します。 • 選択肢：「Add」「Remove」
Add Mode	Untagged パラメータを追加します。
Allowed VLAN Range	許可する VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	本設定を適用するポート範囲を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前画面に戻ります。

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

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

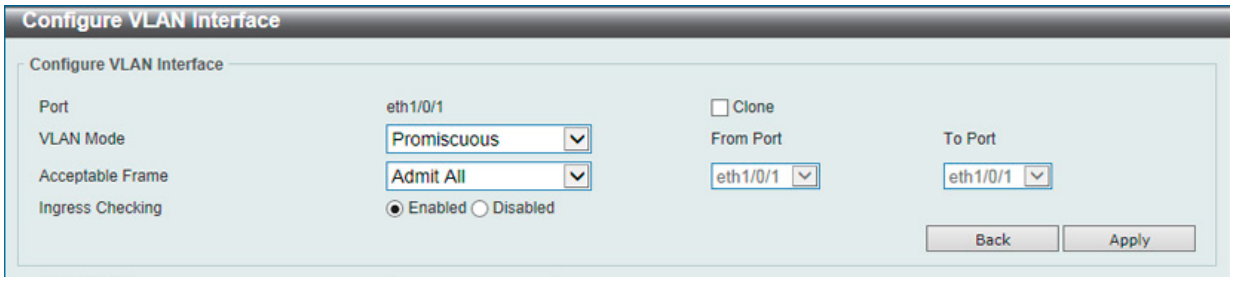


図 8-25　Configure VLAN Interface - Promiscuous 画面

以下の項目が表示されます。

項目	説明
VLAN Mode	VLAN モードをから選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
Clone	クローンを有効にします。
From Port / To Port	本設定を適用するポート範囲を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前画面に戻ります。

VLAN Mode - Host（VLAN モードが Host の場合）

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

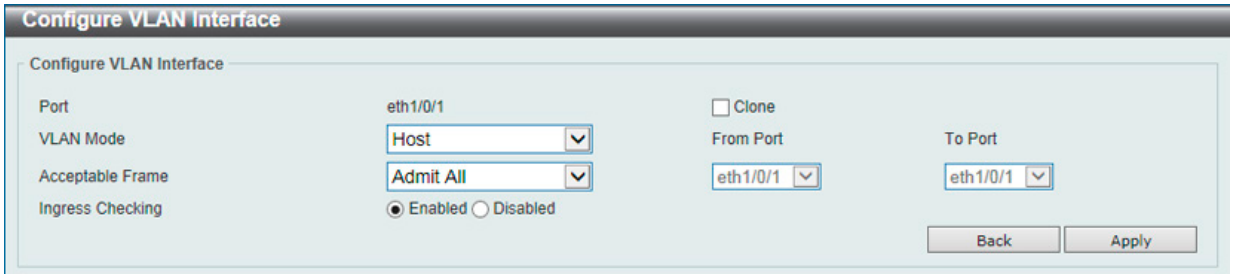


図 8-26　Configure VLAN Interface - Host 画面

以下の項目が表示されます。

項目	説明
VLAN Mode	VLAN モードをから選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Admit All」「Tagged Only」「Untagged Only」
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	クローンを有効にします。
From Port / To Port	本設定を適用するポート範囲を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前画面に戻ります。

Super VLAN（Super VLAN 設定）

Super VLAN は、複数のサブ VLAN（レイヤ 2 ブロードキャストドメイン）を 1 つの IP サブネットに集約するために使用されます。Super VLAN は物理メンバポートを持たず、また、サブ VLAN になることができません。IP インタフェースが Super VLAN として設定された場合、サブ VLAN 間の通信を行うために、自動的にプロキシ ARP が有効になります。複数のサブ VLAN から構成される Super VLAN を、複数設定することも可能です。

注意　Private VLAN と Super VLAN は相互排他機能です。Private VLAN は Super VLAN として設定できません。

注意　PrivL3 ルートプロトコル、マルチキャストプロトコル、IPv6 プロトコルは Super VLAN インタフェースで動作できません。

L2 Features > VLAN > Super 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 8-27　Super VLAN Settings 画面

以下の項目が表示されます。

項目	説明
Add Super VLAN	
Super VID List	作成する Super VLAN の VLAN を入力します。
Add Sub VLAN	
Super VID	サブ VLAN に関連する Super VLAN の VLAN ID を入力します。 • 設定可能範囲：1-4094
Sub VID List	Super VLAN のサブ VLAN を入力します。
Find Super VLAN	
Super VID	表示する Super VLAN の VLAN ID を入力します。 • 設定可能範囲：1-4094

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

エントリの検索 / 表示

「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。
「Show 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表示します。

エントリの削除

「Delete」ボタンをクリックして、エントリを削除します。
「SubVLAN ID」列の「Delete」ボタンをクリックして、特定エントリのサブ VLAN を削除します。

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

サブ VLAN の IP 範囲を設定

「IP Range List」リンクをクリックすると、以下の画面が表示されます。

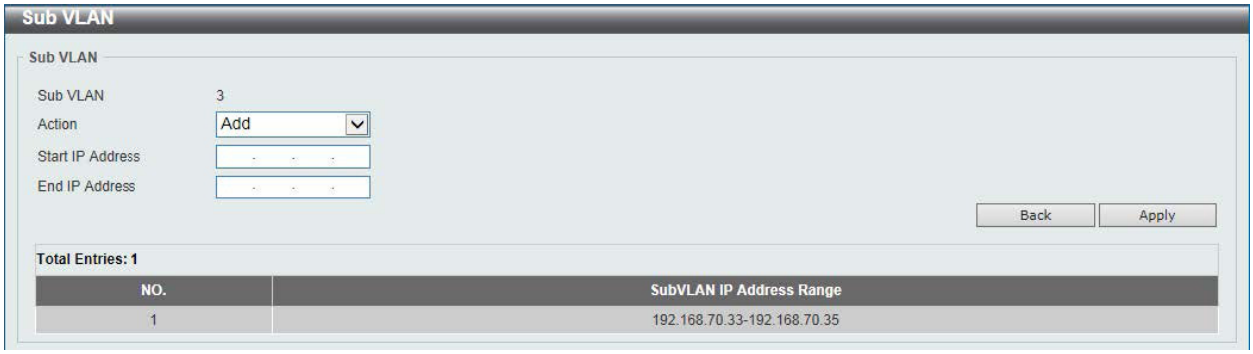


図 8-28　Sub VLAN Settings - IP Range List 画面

以下の項目が表示されます。

項目	説明
Action	サブ VLAN の指定 IP アドレスに対する動作を指定します。 • 選択肢：「Add（追加）」「Remove（削除）」
Start IP Address	開始 IP アドレスを入力します。
End IP Address	終了 IP アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をボタンをクリックして前のページに戻ります。

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

自動サーベイランス VLAN 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。

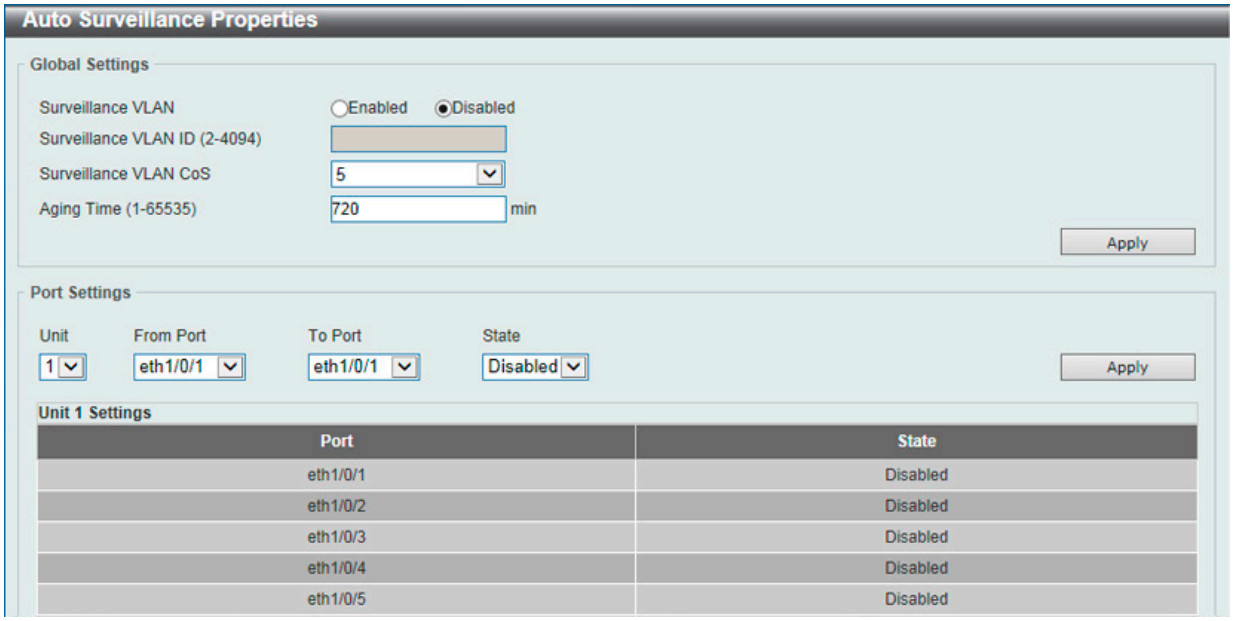


図 8-29　Auto Surveillance Properties 画面

以下の項目が表示されます。

項目	説明
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。サーベイランス VLAN として VLAN を割り当てる前に、通常の VLAN が作成されている必要があります。 • 設定可能範囲：2-4094

項目	説明
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。これにより、QoS データトラフィックとは区別されます。 • 設定可能範囲：0-7
Aging Time	エージングタイムを設定します。 エージングタイムは、ポートがオートサーベイランス VLAN メンバである場合にサーベイランス VLAN からポートを削除するために使用されます。最後のサーベイランスデバイスが、トラフィックの送信を止めて、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。サーベイ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） • 初期値：720（分）
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	指定したポートでサーベイランス VLAN を有効 / 無効にします。 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。

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

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

ユーザ定義のサーベイランストラフィックの OUI を設定します。

L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device の順にメニューをクリックして以下の画面を表示します。

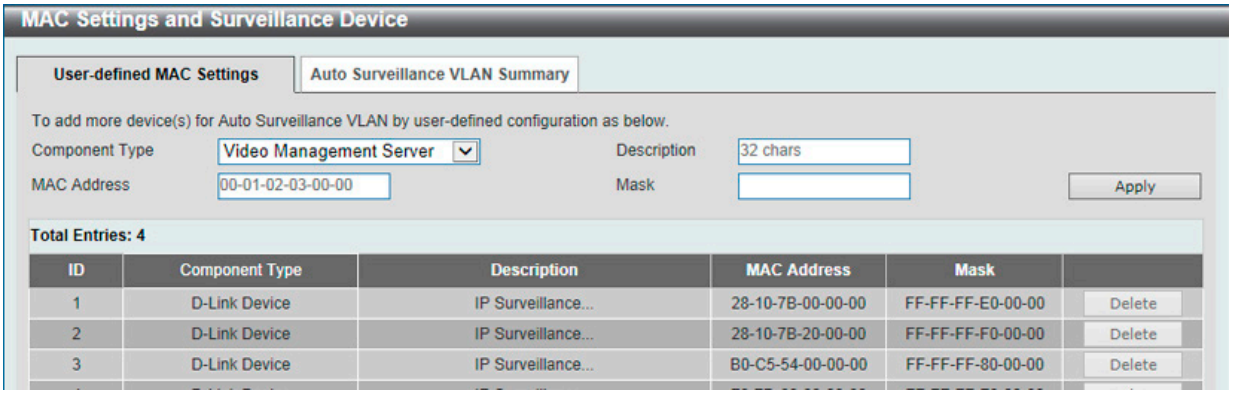


図 8-30　User -defined MAC Settings 画面

以下の項目が表示されます。

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 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。

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

自動サーベイランス VLAN サマリの表示

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

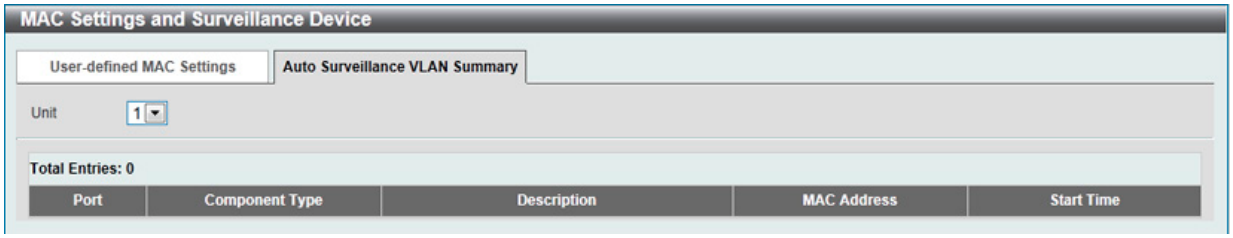


図 8-31　Auto Surveillance VLAN Summary 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

Voice VLAN（音声 VLAN）

Voice VLAN Global（音声 VLAN グローバル設定）

音声 VLAN は、IP 電話からの音声トラフィックを送信するのに使用される VLAN です。不規則にデータを送信すると IP 電話の音の品質を低下させるため、音声トラフィックの QoS（Quality of Service）が音声パケットの伝送優先度を通常のトラフィックより確実に高くなるように設定する必要があります。

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

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

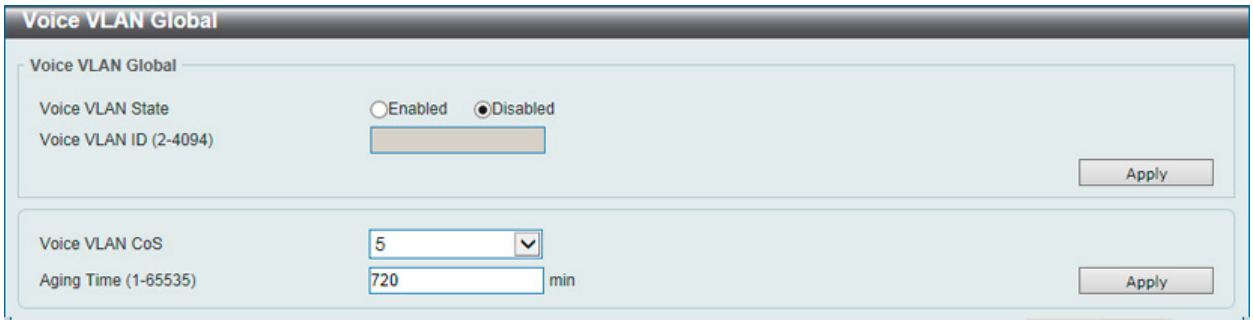


図 8-32　Voice VLAN Global Settings 画面

以下の項目が表示されます。

項目	説明
Voice VLAN State	音声 VLAN 機能のグローバルステータスを有効 / 無効に設定します。
Voice VID	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 の優先度を設定します。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。これにより、QoS データトラフィックとは区別されます。 • 設定可能範囲：0-7 • 初期値：5
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。 最後の音声デバイスが、トラフィックの送信を止めて、この音声デバイスの MAC アドレスがエージングタイムに到達すると、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） • 初期値：720（分）

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

Voice VLAN Port（音声 VLAN のポート設定）

ポートの音声 VLAN 情報を表示します。

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

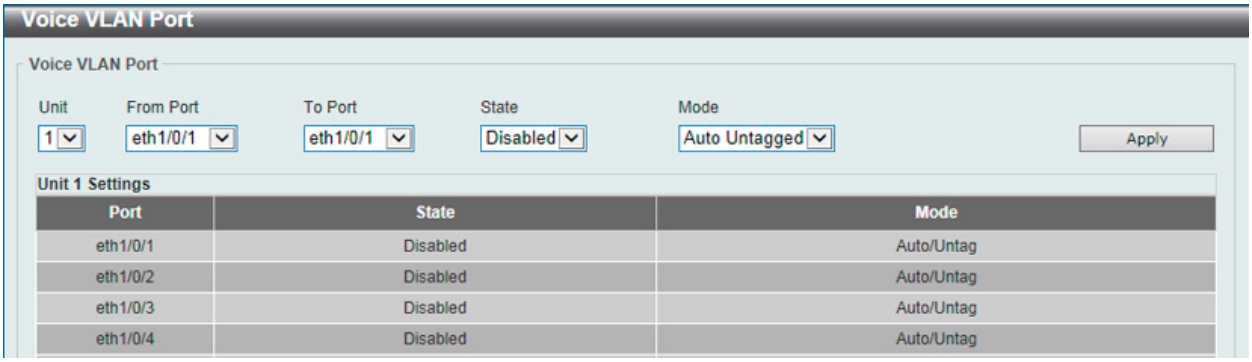


図 8-33　Voice VLAN Port 画面

以下の項目が表示されます。

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。
Mode	モードを選択します。 • 「Auto Untagged」- タグなしの音声 VLAN 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、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、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。

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

Voice VLAN OUI（音声 VLAN OUI 設定）

ユーザ定義の音声トラフィックの OUI を設定します。
OUI は音声トラフィックを識別するために使用されます。多くの定義済み OUI があり、必要に応じてユーザ定義の OUI を設定することもできます。
ユーザ定義 OUI は定義済みの OUI と同じとすることはできません。

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。

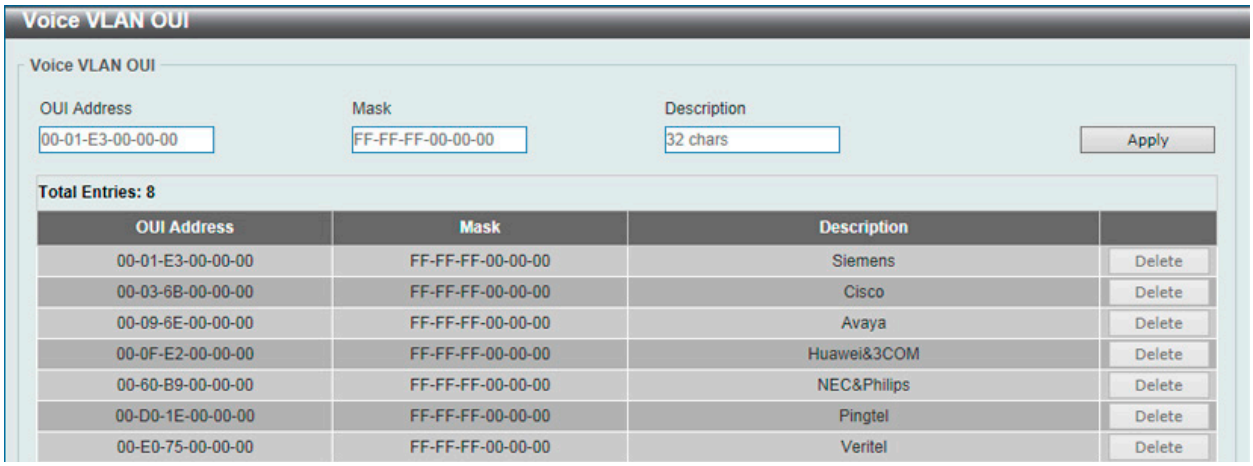


図 8-34　Voice VLAN OUI 画面

以下の項目が表示されます。

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 OUI MAC アドレスマスクを入力します。
Description	ユーザ定義 OUI に関する説明文を入力します。（32 文字以内）

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

Voice VLAN Device（音声 VLAN デバイス）

ポートに接続する音声デバイスを表示します。開始時刻はデバイスがこのポートで検出された時間です。また、アクティベート時間はデバイスが一番最近トラフィックを送信した時間です。

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。

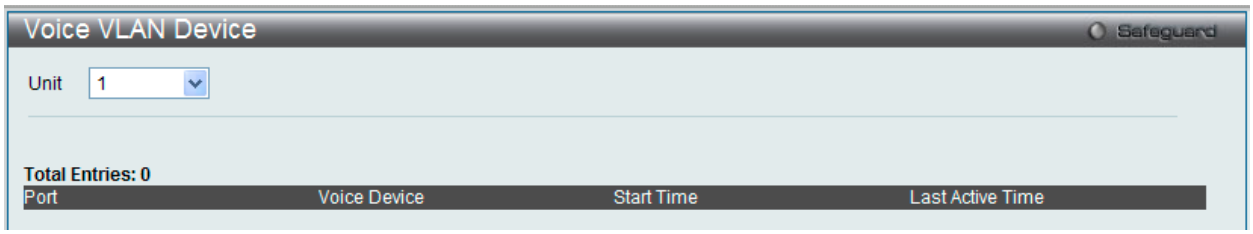


図 8-35　Voice VLAN Device 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

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

スイッチに接続する音声 VLAN LLDP-MED 音声デバイスを表示します。

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

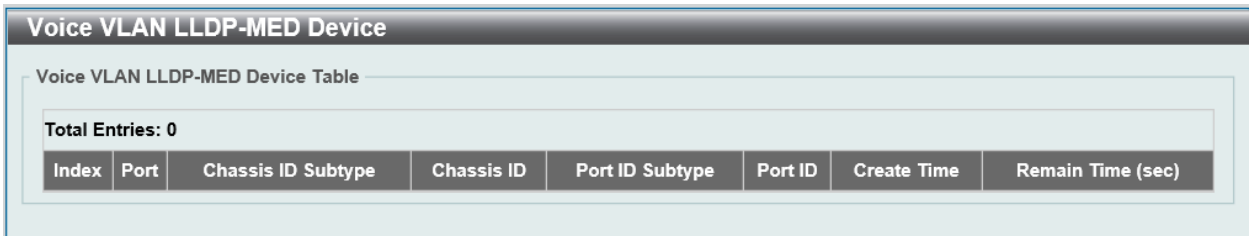


図 8-36　Voice VLAN LLDP-MED Voice Device 画面

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

Private VLAN（プライベート VLAN 設定）

プライベート VLAN のパラメータを設定します。

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。

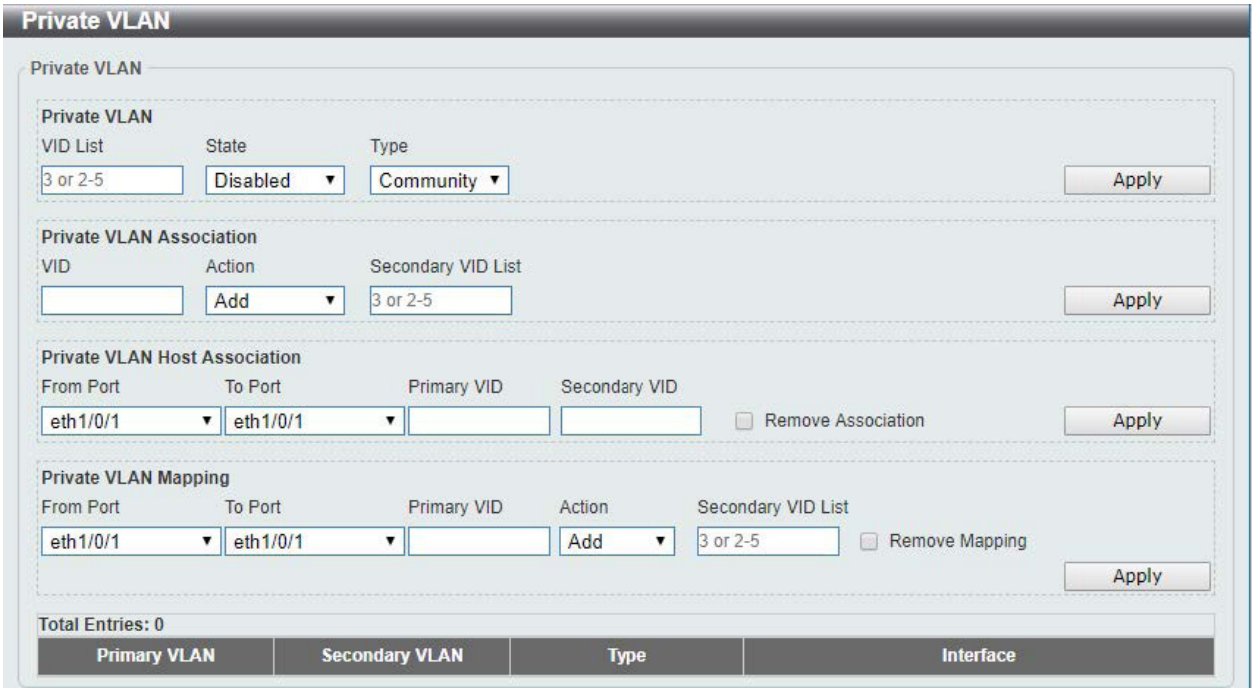


図 8-37　Private VLAN 画面

以下の項目が表示されます。

項目	説明
Private VLAN	
VID List	VLAN ID のリストを指定します。
State	プライベート VLAN の有効 / 無効を指定します。
Type	プライベート VLAN のタイプを指定します。 • 選択肢：「Community」「Isolated」「Primary」
Private VLAN Association	
VID	VLAN ID のリストを指定します。
Action	プライベート VLAN に対する動作を指定します。 • 選択肢：「Add」（追加）「Remove」（削除）
Secondary VID List	セカンダリ VLAN ID のリストを入力します。
Private VLAN Host Association	
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。
Primary VID	プライマリ VLAN ID を入力します。

項目	説明
Secondary VID	セカンダリ VLAN IDを入力します。「Remove Association」にチェックを入れると本コンフィグレーションは有効になりません。
Private VLAN Mapping	
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。
Primary VID	プライマリ VLAN ID を入力します。
Action	本設定の動作を指定します。 ・「Add」- 入力した情報に基づきエントリを追加します。 ・「Remove」- 入力した情報に基づきエントリを削除します。
Secondary VID	セカンダリ VLAN ID を入力します。「Remove Mapping」にチェックを入れると本コンフィグレーションは有効になりません。

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

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）

本項目では「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で 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「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。

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。

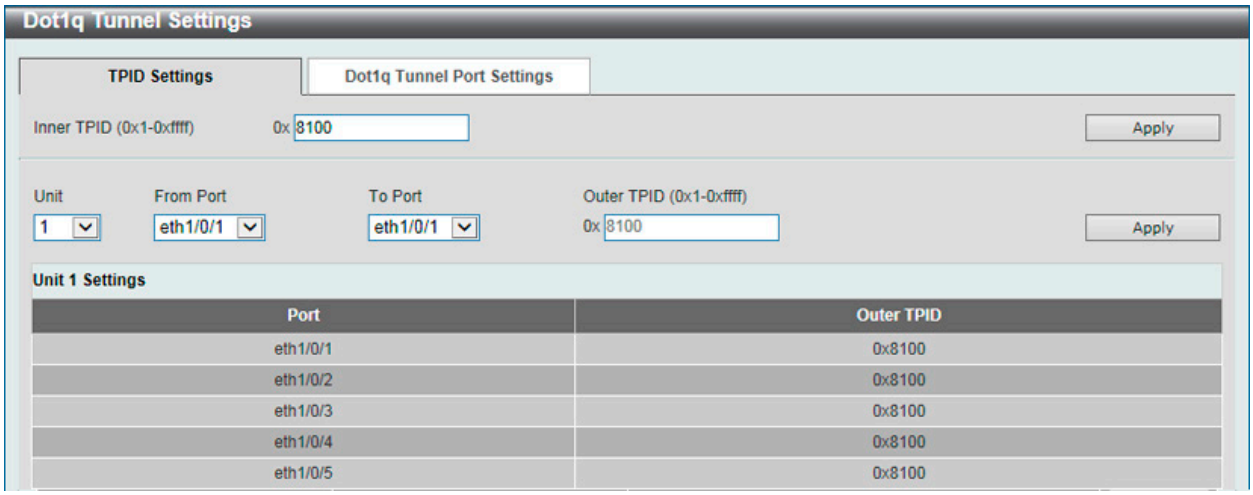


図 8-38　Dot1q Tunnel（TPID Settings）画面

以下の項目が表示されます。

項目	説明
Inner TPID	インナー TPID 値を 16 進数方式で指定します。インナー TPID によって、イングレスパケットが「C タグ付き」であるかどうかが決定します。このインナー TPID は各システムで設定されます。 ・ 設定可能範囲：0x1-0xFFFF
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。
Outer TPID	アウター TPID 値を 16 進数方式で指定します。 ・ 設定可能範囲：0x1-0xFFFF

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

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。

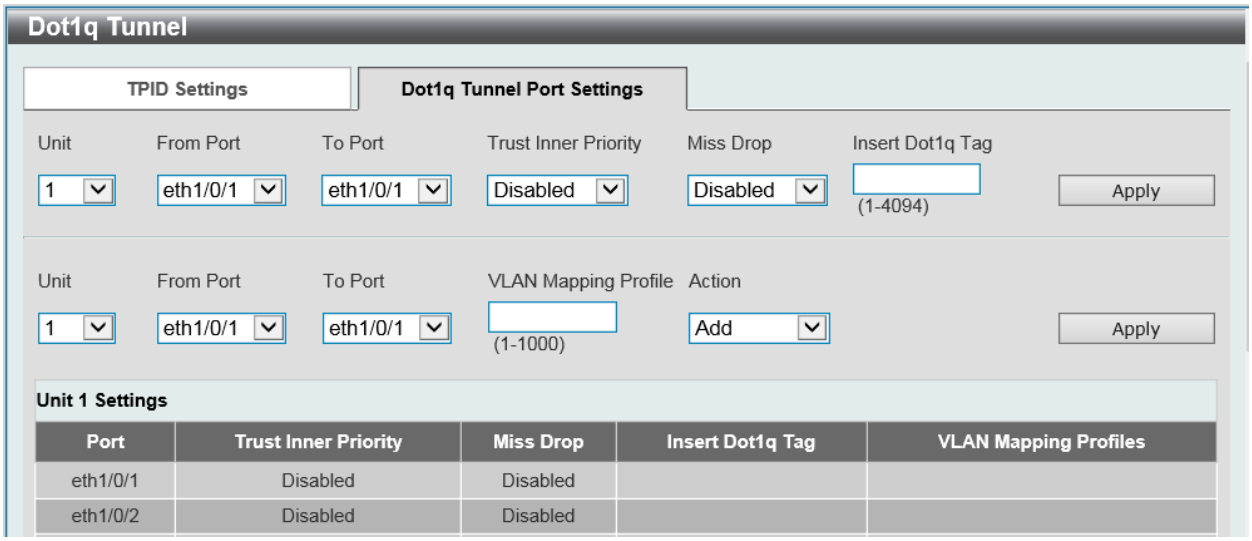


図 8-39　Dot1q Tunnel（Dot1q Tunnel Port Settings）画面

以下の項目が表示されます。

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。
Trust Inner Priority	「802.1Q Inner Trust Priority」を有効 / 無効に設定します。802.1Q トンネルポートでトラストプライオリティ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。
Miss Drop	「Miss Drop」を有効 / 無効に設定します。受信ポートで VLAN マッピング Miss Drop オプションが有効な場合、受信パケット VLAN が VLAN マッピングエントリやポートのルールと一致しないと、パケットは破棄されます。
Insert Dot1q Tag	802.1Q トンネルポートで受信したタグなしパケットに挿入される 802.1Q VLAN ID を指定します。 • 設定可能範囲：1-4094
VLAN Mapping Profile	VLAN マッピングプロファイル ID を指定します。値が低い方が優先度が高くなります。 • 設定可能範囲：1-1000
Action	本設定の動作を指定します。 • 「Add」- 入力した情報に基づきエントリを追加します。 • 「Remove」- 入力した情報に基づきエントリを削除します。

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

VLAN Mapping（VLAN マッピング）

本項目では VLAN マッピングの設定、表示を行います。インタフェースにプロファイルが適用されると、スイッチはプロファイルルールに従い受信パケットを照合します。パケットがルールに合致したことを確認すると、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、「送信 VID」の追加や削除、新しい送信タグの優先値設定、またはパケットの新しい入力 VID の設定などがあります。
この照合はプロファイル内にあるルールのシーケンス番号に依存しており、最初のエントリが合致す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、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 単位で設定されます。1 つのインタフェースに対し、複数の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。

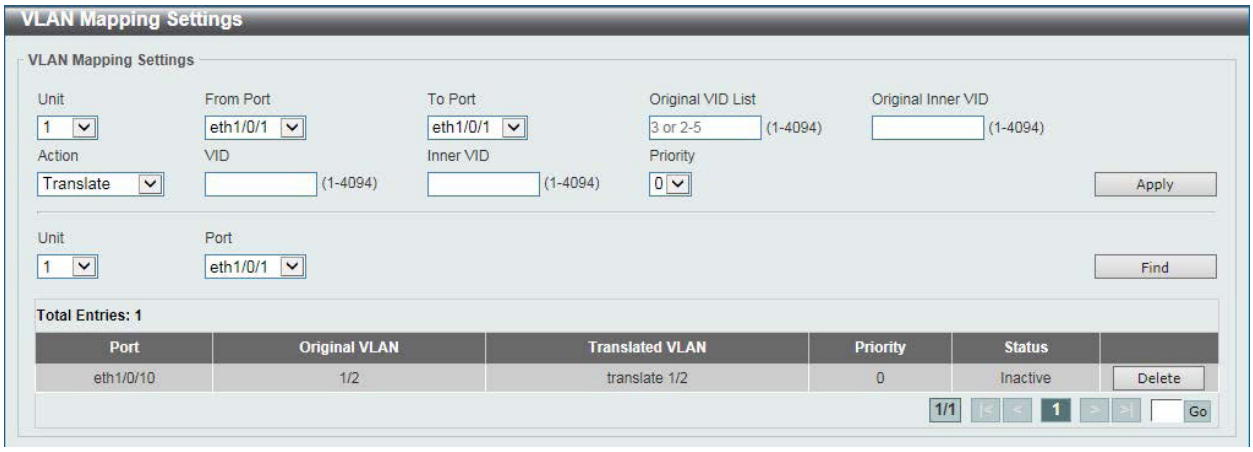


図 8-40　VLAN Mapping 画面

以下の項目が表示されます。

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。
Port	検索するポートを指定します。
Original VID List	オリジナルの VID リストを指定します。 • 設定可能範囲：1-4094
Original Inner VID	オリジナルのインナー 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」「Dot1q-tunnel」から指定します。 • 「Translate」- 一致したパケットの出力 VID と交換する VID を指定します。 • 「Dot1q-tunnel」- 一致したパケットに出力 VID を追加します。
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094
Inner VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
Priority	優先値を指定します。大きい値の方が優先度が高くなります。 • 設定可能範囲：0-7

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

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。

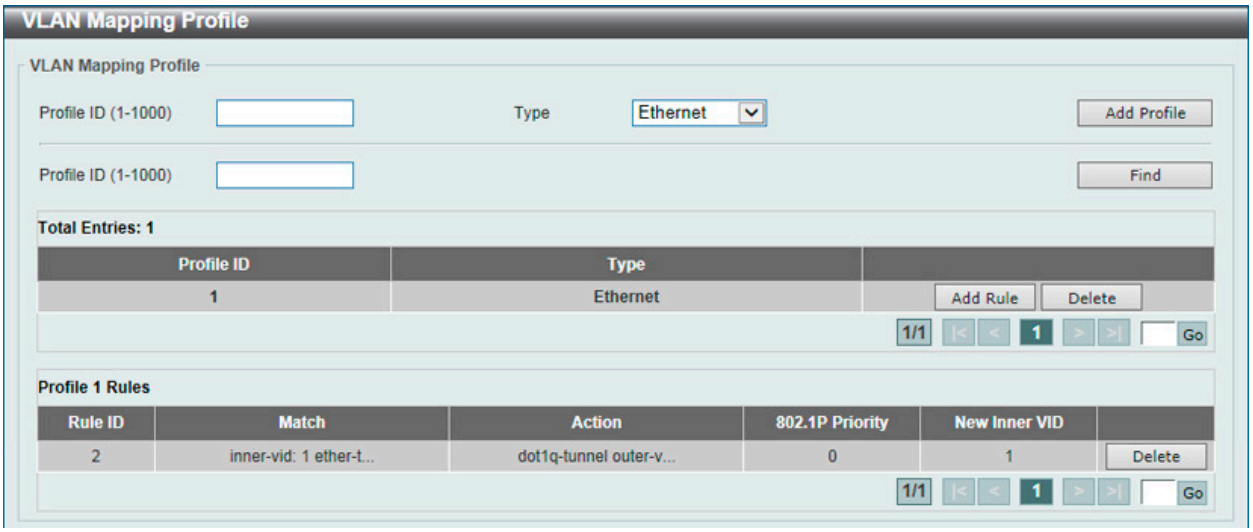


図 8-41　VLAN Mapping Profile 画面

以下の項目が表示されます。

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。値が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。 • 「Ethernet」- プロファイルは L2 フィールドを照合します。 • 「IP」- ロファイルは L3 フィールドを照合します。 • 「IPv6」- プロファイルは IPv6 宛先 / 送信元アドレスを照合します。 • 「Ethernet-IP」- プロファイルは L2/L3 IP フィールドを照合します。

「Add Profile」をクリックし、新しい VLAN マッピングプロファイルを追加します。

エントリの検索 / 表示

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの削除

「Delete」ボタンをクリックして、エントリを削除します。

ルールの追加

「Add Rule」をクリックし、新しいルールを追加します。
プロファイルタイプ毎のルール設定について、次ページ以降で説明します。

Add VLAN Mapping Rule（Ethernet）（VLAN マッピングルールの追加 /Ethernet）

「VLAN Mapping Profile」の Type で「Ethernet」を選択、「Add Rule」をクリックし、新しいルールを追加します。

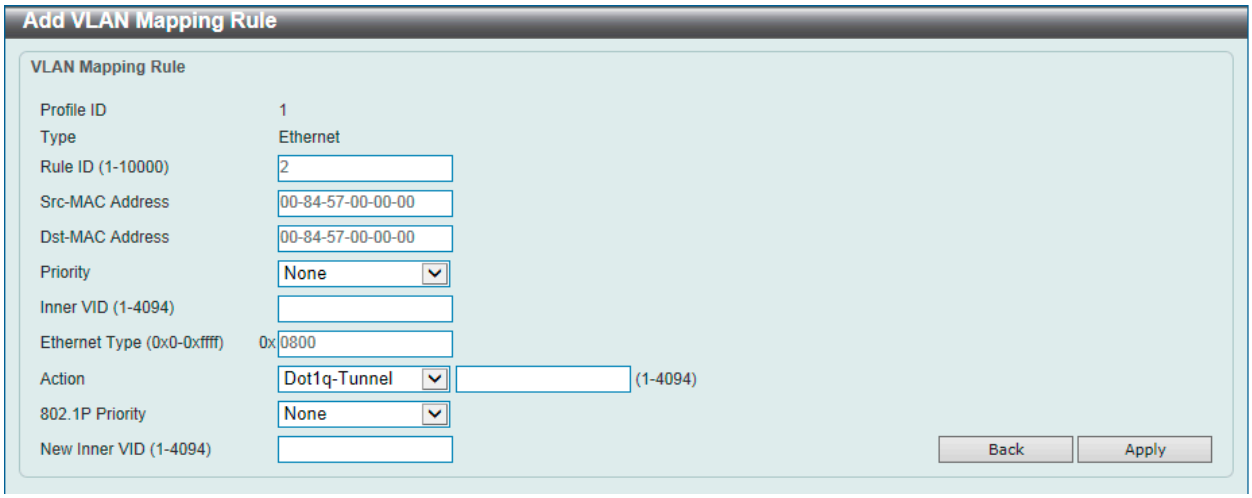


図 8-42　Add VLAN Mapping Rule（Ethernet）画面

以下の項目が表示されます。

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
Src-MAC Address	送信元 MAC アドレスを指定します。
Dst-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。値が大きい方が優先度が高くなります。 • 設定可能範囲：「None」（指定なし）、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。 • Translate - 一致したパケットの出力 VID と交換する VID を指定します。 • Dot1q-tunnel - 一致したパケットに出力 VID を追加します。
New Outer VID	新しいアウター VLAN ID を指定します。 • 設定可能範囲：1-4094
802.1P Priority	802.1p 優先値を指定します。値が大きい方が優先度が高くなります。 • 設定可能範囲：「None」（指定なし）、0-7
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。 • 設定可能範囲：1-4094

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

Add VLAN Mapping Rule（IP）（VLAN マッピングルールの追加 /IP）

「VLAN Mapping Profile」の Type で「IP」を選択、「Add Rule」をクリックし、新しいルールを追加します。

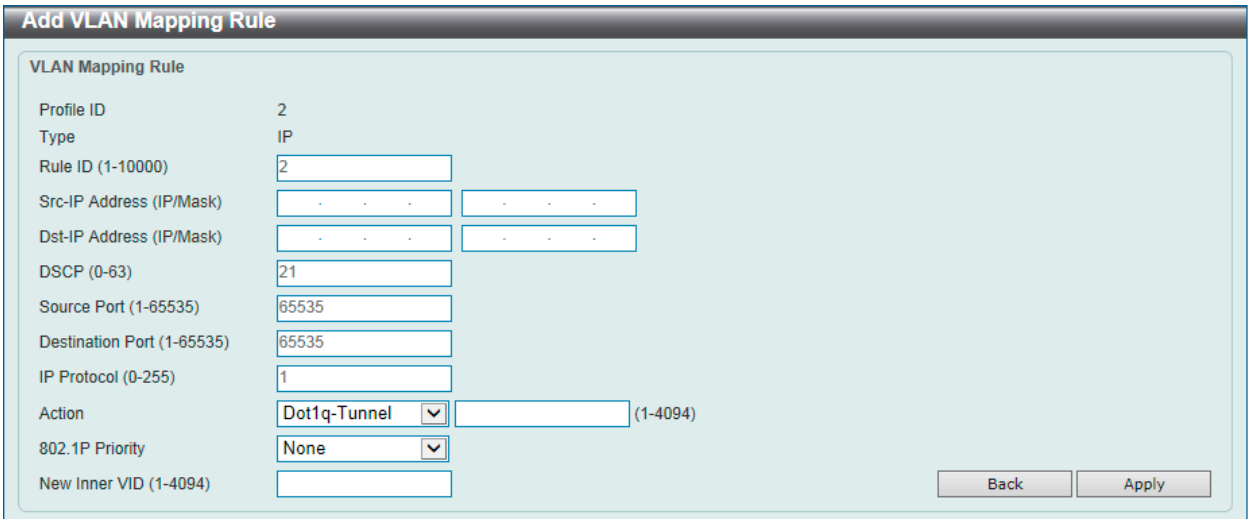


図 8-43　Add VLAN Mapping Rule（IP）画面

以下の項目が表示されます。

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
Src-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。
Dst-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 / Destination Port	送信元 / 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。 •「Translate」- 一致したパケットの出力 VID と交換する VID を指定します。 •「Dot1q-tunnel」- 一致したパケットに出力 VID を追加します。
New Outer VID	新しいアウター VLAN ID を指定します。 • 設定可能範囲：1-4094
802.1P Priority	802.1p 優先値を指定します。値が大きい方が優先度が高くなります。 • 設定可能範囲：「None」（指定なし）、0-7
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。 • 設定可能範囲：1-4094

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

Add VLAN Mapping Rule（IPv6）（VLAN マッピングルールの追加 /IPv6）

「VLAN Mapping Profile」の Type で「IPv6」を選択、「Add Rule」をクリックし、新しいルールを追加します。

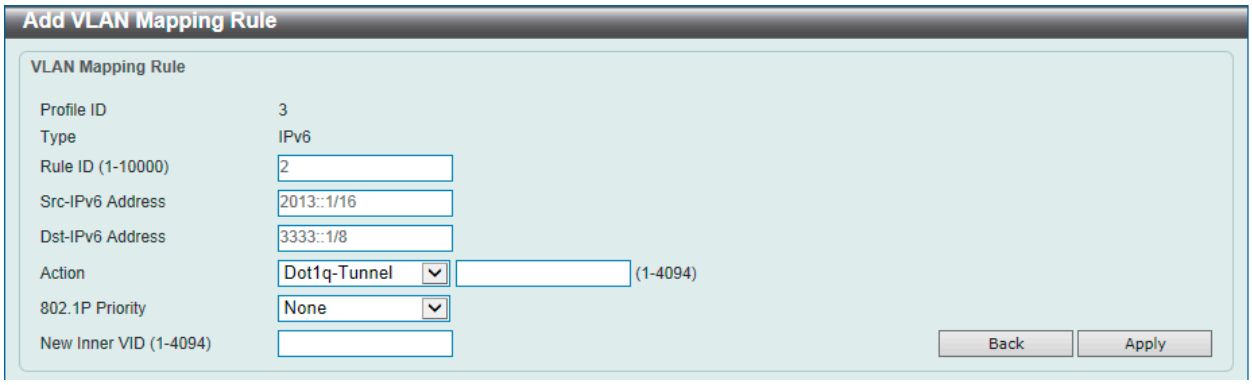


図 8-44　Add VLAN Mapping Rule（IPv6）画面

以下の項目が表示されます。

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
Src-IPv6 Address	送信元 IPv6 アドレスとプリフィクス長を指定します。
Dst-IPv6 Address	宛先 IPv6 アドレスとプリフィクス長を指定します。
Action	実行する動作を指定します。 •「Translate」- 一致したパケットの出力 VID と交換する VID を指定します。 •「Dot1q-tunnel」- 一致したパケットに出力 VID を追加します。
New Outer VID	新しいアウター VLAN ID を指定します。 • 設定可能範囲：1-4094
802.1P Priority	802.1p 優先値を指定します。値が大きい方が優先度が高くなります。 • 設定可能範囲：「None」（指定なし）、0-7
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。 • 設定可能範囲：1-4094

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

Add VLAN Mapping Rule（Ethernet-IP）（VLAN マッピングルールの追加 /Ethernet-IP）

「VLAN Mapping Profile」の Type で「Ethernet-IP」を選択、「Add Rule」をクリックし、新しいルールを追加します。

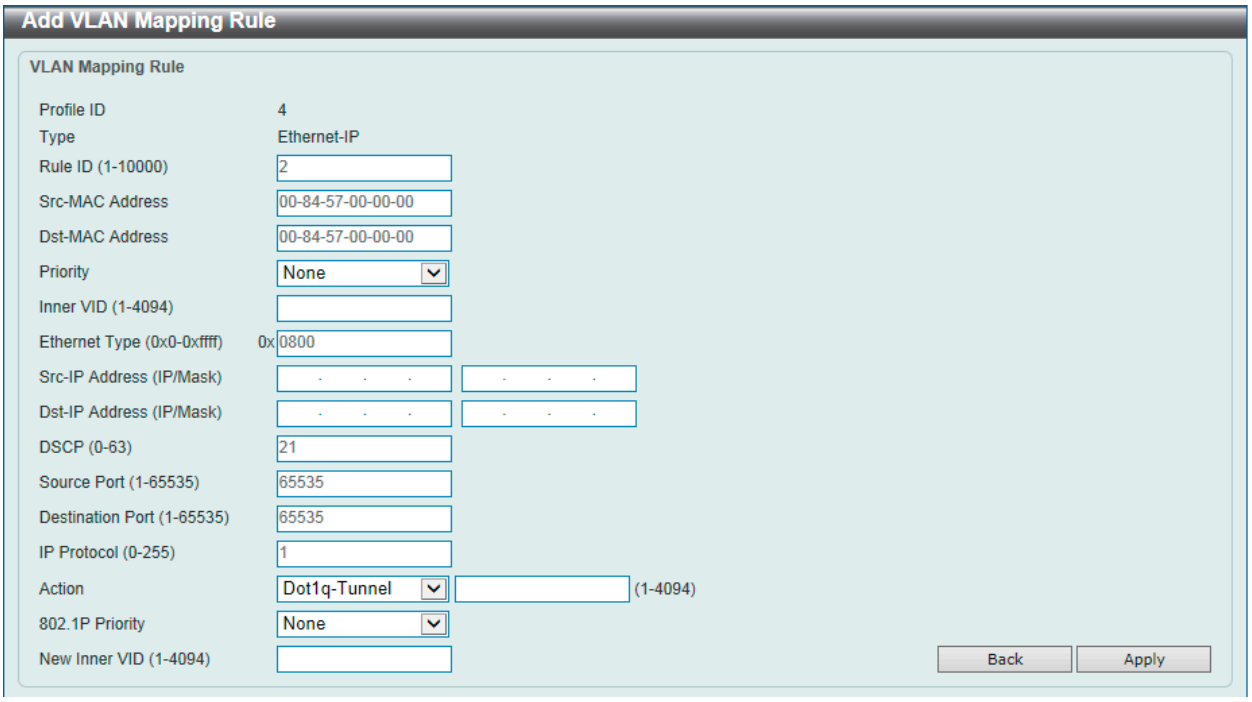


図 8-45　Add VLAN Mapping Rule（Ethernet-IP）画面

以下の項目が表示されます。

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
Src-MAC Address	送信元 MAC アドレスを指定します。
Dst-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。値が大きい方が優先度が高くなります。 • 設定可能範囲：「None」（指定なし）、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
Src-IP Address	送信元 IP アドレスとサブネットマスクを指定します。
Dst-IP Address	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 / Destination Port	送信元 / 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。 •「Translate」- 一致したパケットの出力 VID と交換する VID を指定します。 •「Dot1q-tunnel」- 一致したパケットに出力 VID を追加します。
New Outer VID	新しいアウター VLAN ID を指定します。 • 設定可能範囲：1-4094
802.1P Priority	802.1p 優先値を指定します。値が大きい方が優先度が高くなります。 • 設定可能範囲：「None」（指定なし）、0-7
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。 • 設定可能範囲：1-4094

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

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、以下の画面を表示します。

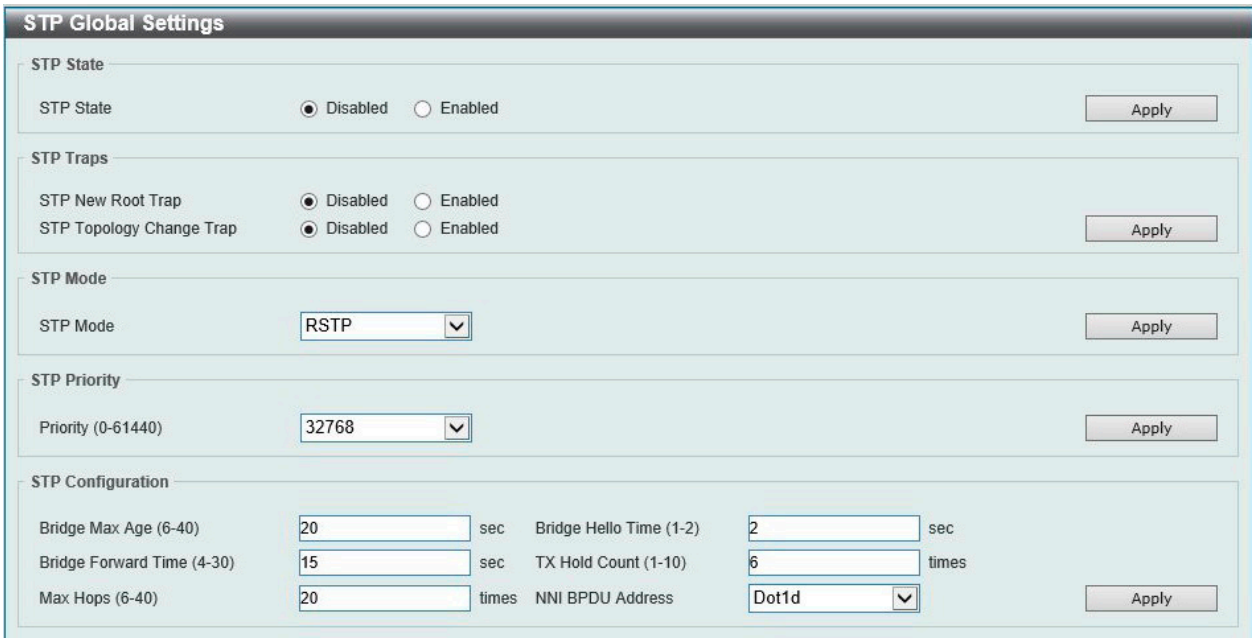


図 8-46　STP Global Settings 画面

以下の項目が表示されます。

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 Trap	
STP New Root Trap	新しいルートトラップ送信の有効 / 無効を設定します。
STP Topology Change Trap	トポロジ変更トラップ送信の有効 / 無効を設定します。

項目	説明
STP 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。 • 「STP」- スイッチ上で STP がグローバルに使用されます。 • 「RSTP」- スイッチ上で RSTP がグローバルに使用されます。 • 「MSTP」- スイッチ上で MSTP がグローバルに使用されます。
STP Priority	
Priority	STP 優先値を指定します。値が低い方の優先値が高くなります。 • 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際限なく循環し、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します。 • 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。詳しくは「STP ポート設定」セクションを参照してください。 • 設定可能範囲：1-2 秒 • 初期値：2（秒）
Bridge Forward Time (4-30)	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間、本値で指定した時間 Listening 状態を保ちます。 • 設定可能範囲：4-30（秒） • 初期値：15（秒）
Tx Hold Count (1-10)	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 • 初期値：6
Max Hops (6-40)	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。スイッチは、0 に到達すると、BPDU パケットは破棄され、ポートに保持していた情報を解放します。 • 設定可能範囲：6-40 • 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の決定に使用されます。「802.1d STP アドレス」と「802.1ad サービスプロバイダ STP アドレス」が使用されます。 • 選択肢：「Dot1d」「Dot1ad」 • 初期値：「Dot1d」

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

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。

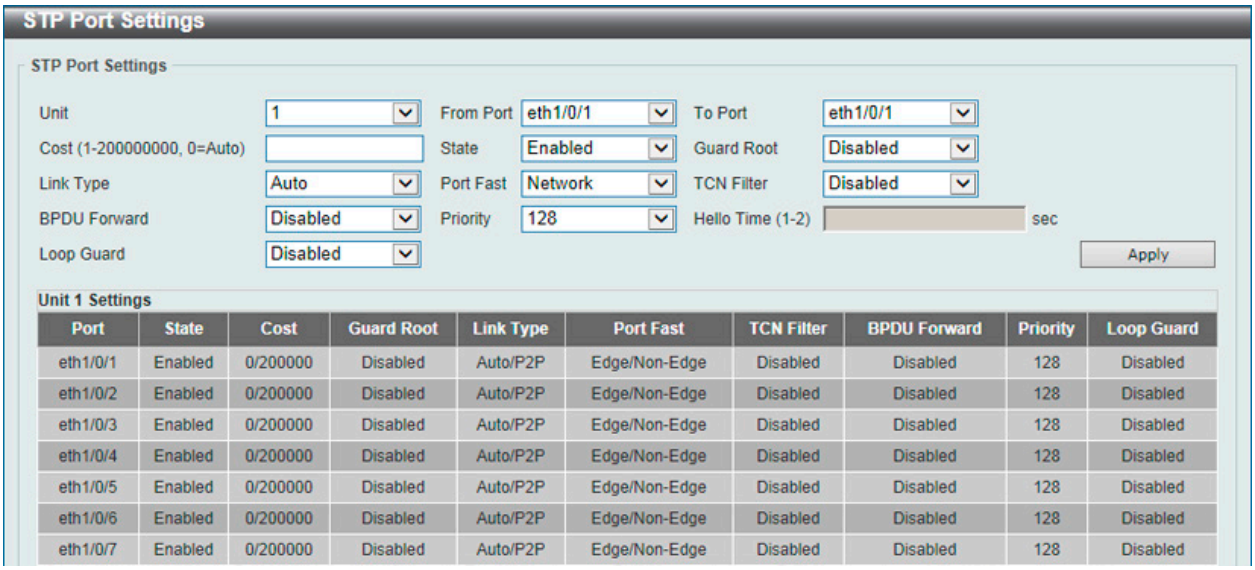


図 8-47　STP Port Settings 画面

以下の項目が表示されます。

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。
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適のパケット転送速度を自動的に設定します。（初期値） ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。 • 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほどパケット転送は頻繁に行われるようになります。
State	指定ポートの STP を有効 / 無効に設定します。 • 初期値：「Enabled」（有効）
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、半二重ポートは Shared 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。 • 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 が受信されず、転送状態に移行した場合、ポートファスト状態になります。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。（初期値） •「Disable」- 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」- 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。
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。有効にすると受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。 • 初期値：「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：0-40 • 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）

項目	説明
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。

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

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。ユーザはその項目を変更できますが、MSTI ID の変更や削除は行うことができません。

L2 Features > 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。

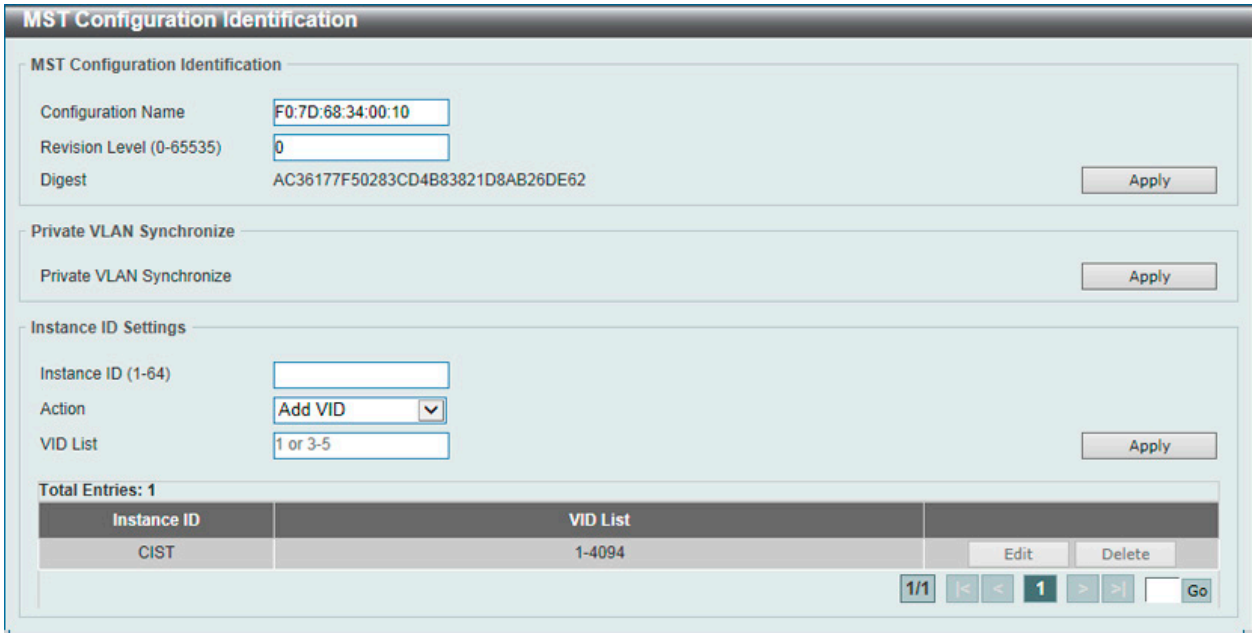


図 8-48　MST Configuration Identification 画面

以下の項目が表示されます。

項目	説明
Configuration Name	各 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 リージョンの値を設定します。Configuration Name に同期しています。スイッチ上の MSTP リー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
Instance ID	スイッチに Instance ID を設定します。 • 設定可能範囲：1-46
Action	MSTI に行う変更を選択します。 • 「Add VID」- VID List 項目に指定された VID を MSTI ID に追加します。 • 「Remove VID」- VID List 項目に指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。
「Edit」ボタンをクリックすると設定を編集することができます。「Instance ID Settings 」セクションで設定を変更後、「Apply」ボタンをクリックして設定内容を適用します。

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

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 8-49　STP Instance 画面

以下の項目が表示されます。

項目	説明
Instance Priority	「Edit」をクリック後、指定したインスタンスのためのプライオリティ（0-61440）を設定します。

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「Apply」ボタンをクリックして設定内容を適用します。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

MSTP Port Information（MSTP ポート情報）

現在の MSTP ポート情報の表示や、MSTI ID 単位でポート構成の更新を行います。ループが発生した場合に MSTP 機能はポートプライオリティを使用して、Forwarding 状態に遷移させるインタフェースを選択します。インタフェースに同じプライオリティ値が与えられている場合、MSTP は MAC アドレスの値が最小のインタフェースを Forwarding 状態にし、他のインタフェースをブロックします。

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。

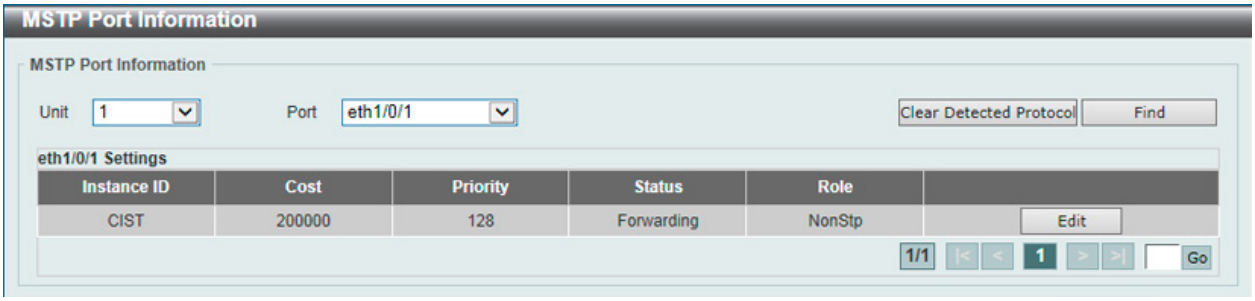


図 8-50　MSTP Port Information 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポートを指定します。
Cost	パケットを転送する相対的なコストを設定します。 • 設定可能範囲：1-200000000
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

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「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。
「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削除します。

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

ERPS (G.8032)（イーサネットリングプロテクション設定）

ERPS（Ethernet Ring Protection Switching）はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。これは、イーサネットリングネットワークに対して十分に考慮されたイーサネット操作、管理、およびメンテナンス機能と簡単な APS（automatic protection switching）プロトコルを統合することによって実行されます。ERPS はリングトポロジ内のイーサネットトラフィックに sub-50ms 保護を提供します。これはイーサネットレイヤにループが全く形成されないことを保証します。

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 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。

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 8-51　ERPS 画面

以下の項目が表示されます。

項目	説明
ERPS Version Settings	
ERPS Version	「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 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いている場合、「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みのインスタンスをサポート
ERPS Global Settings	
ERPS Trap State	ERPS トラップ送信を有効 / 無効に設定します。
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）

「Ethernet Ring G.8032」セクションで「Apply」ボタンをクリックして、設定内容に基づく ERP リングを作成します。
「Delete」ボタンをクリックして、エントリを削除します。

ERP リングの編集

「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。

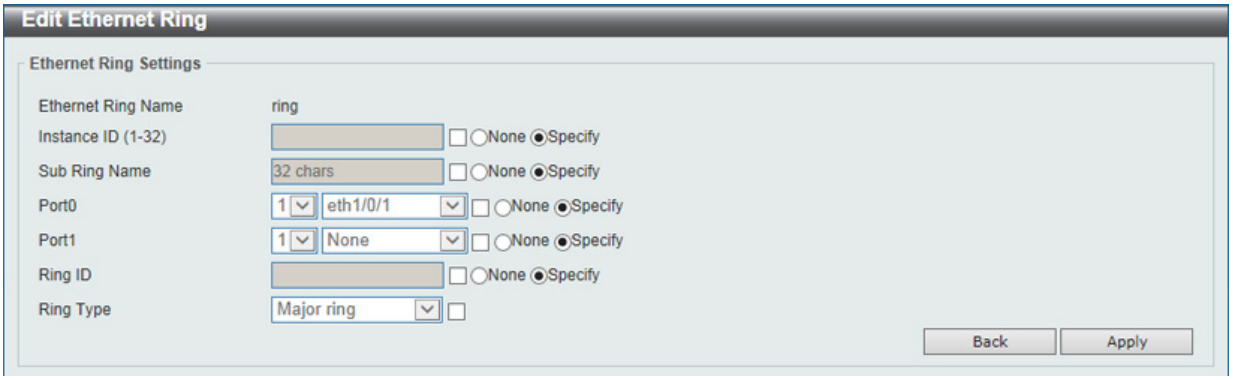


図 8-52　ERPS 画面 - Edit

以下の項目が表示されます。

項目	説明
Instance ID	チェックを入れ「ERP インスタンス」の番号を指定します。 「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	チェックを入れユニット ID を選択し、初期リングになるポート番号を指定します。 ドロップダウンメニューから「None」を選択すると、内部接続されたノード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	チェックを入れユニット ID を選択し、2 番目のリングになるポート番号を指定します。 ドロップダウンメニューから「None」を選択すると内部接続されたノード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	チェックを入れリングタイプを指定します。 • 選択肢：「Major Ring」「Sub Ring」

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

「Back」をクリックすると設定は破棄され前画面に戻ります。

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。

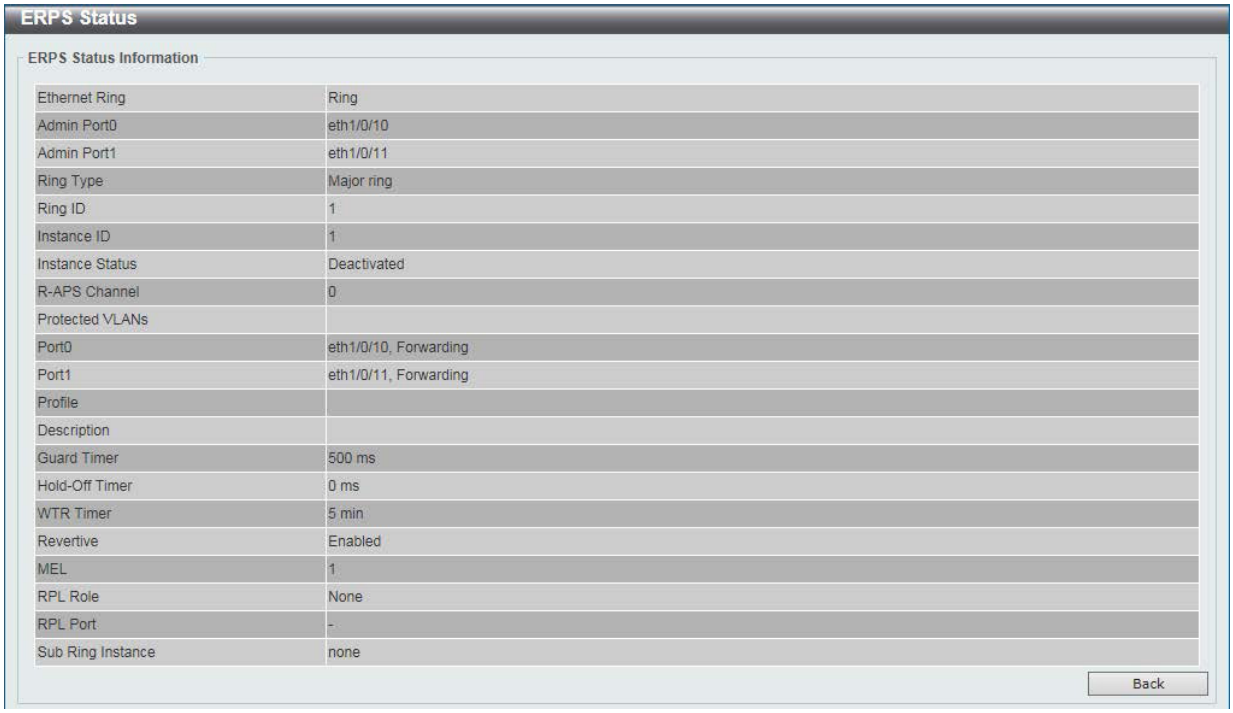


図 8-53　ERPS 画面 - Show Detail

「Back」をクリックすると前画面に戻ります。

「ERPS Brief」タブの表示

「ERPS Brief」タブをクリックすると、以下の画面が表示されます。

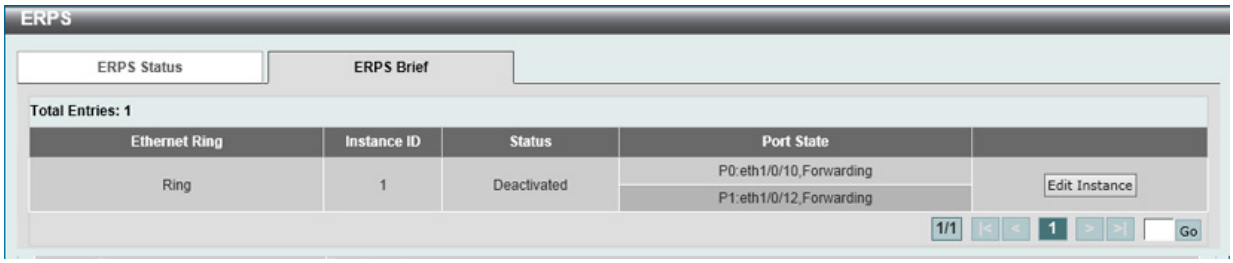


図 8-54　ERPS（ERPS Brief タブ）画面

ERP インスタンスを設定するには、「Edit Instance」をクリックします。

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

インスタンスの編集

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

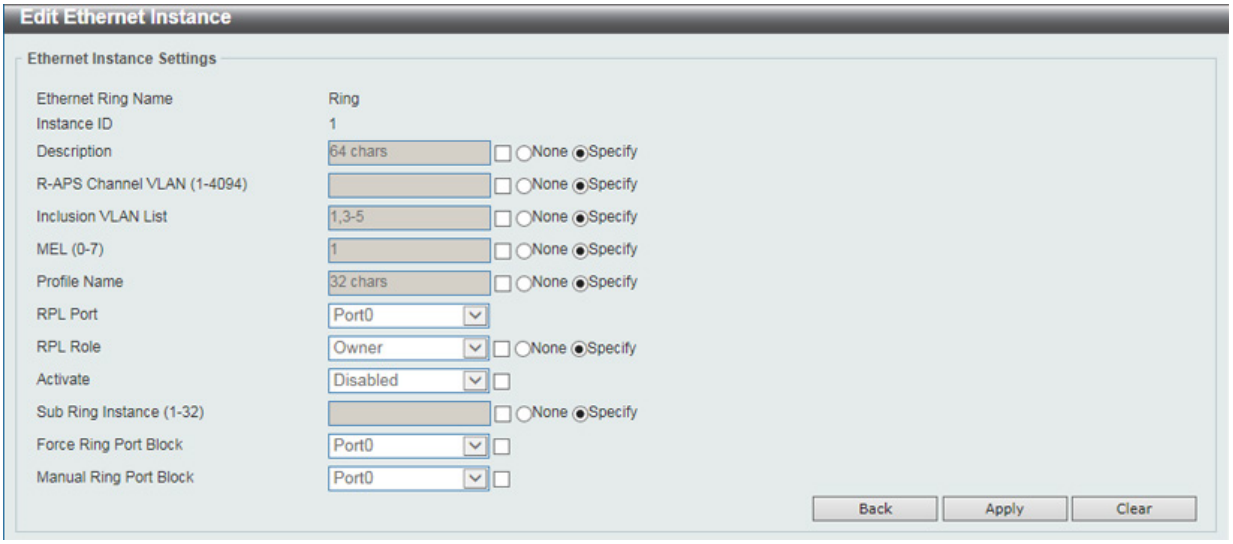


図 8-55　ERPS 画面 - Instance

以下の項目が表示されます。

項目	説明
Description	チェックを入れ「ERP インスタンス」の概要を指定します。（64 文字以内） 「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	チェックを入れ ERP インスタンスに関連する「G.8032」のプロファイルを指定します。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。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	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	チェックを入れ ERP インスタンスをアクティブにするか選択します。「Enable」の場合、ERP インスタンスはアクティブになります。 • 選択肢：「Enable」「Disable」
Sub Ring Instance	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」

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

「Clear All」ボタンをクリックして、設定内容をクリアします。

「Back」をクリックすると設定は破棄され前画面に戻ります。

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。

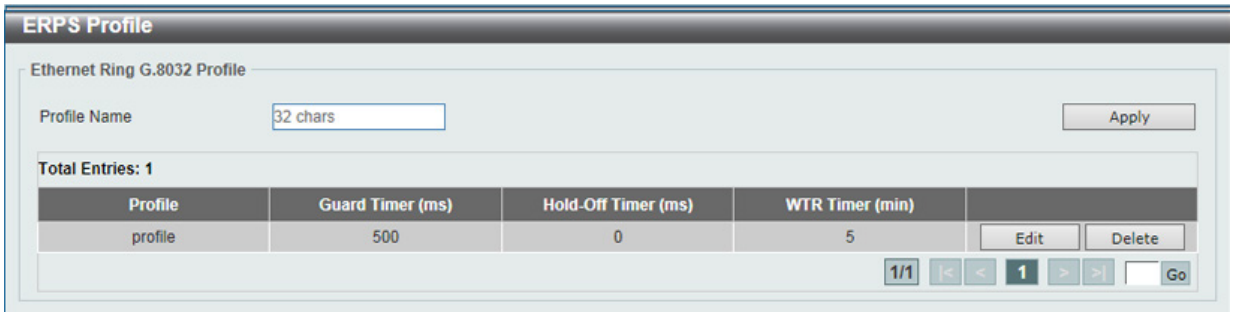


図 8-56　ERPS Profile 画面

以下の項目が表示されます。

項目	説明
Profile Name	「G.8032」のプロファイル名を指定します。（32 文字以内） 複数の ERP インスタンスを同じ「G.8032」プロファイルに指定できます。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。

「Profile Name」を入力し「Apply」をクリックして、ERP インスタンスに紐づける「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、エントリを削除します。

「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。

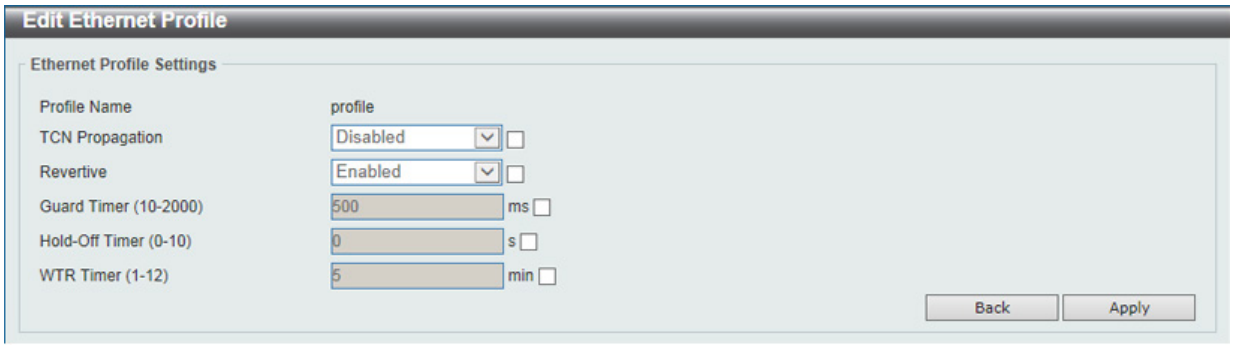


図 8-57　「G.8032」プロファイル画面 - Edit

以下の項目が表示されます。

項目	説明
TCN Propagation	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：「Enable」「Disable」
Revertive	チェックを入れ「Revertive」の設定を行います。本機能は送信エンティティへの復帰に使用します。例えば RPL がブロックされた場合などです。 • 選択肢：「Enable」「Disable」
Guard Timer	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	チェックを入れ WTR Timer の設定を行います。 • 設定可能範囲：1-12（分） • 初期値：5（分）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると設定は破棄され前画面に戻ります。

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 から受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは 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。ループバック検知機能はポート範囲に実行されます。

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。

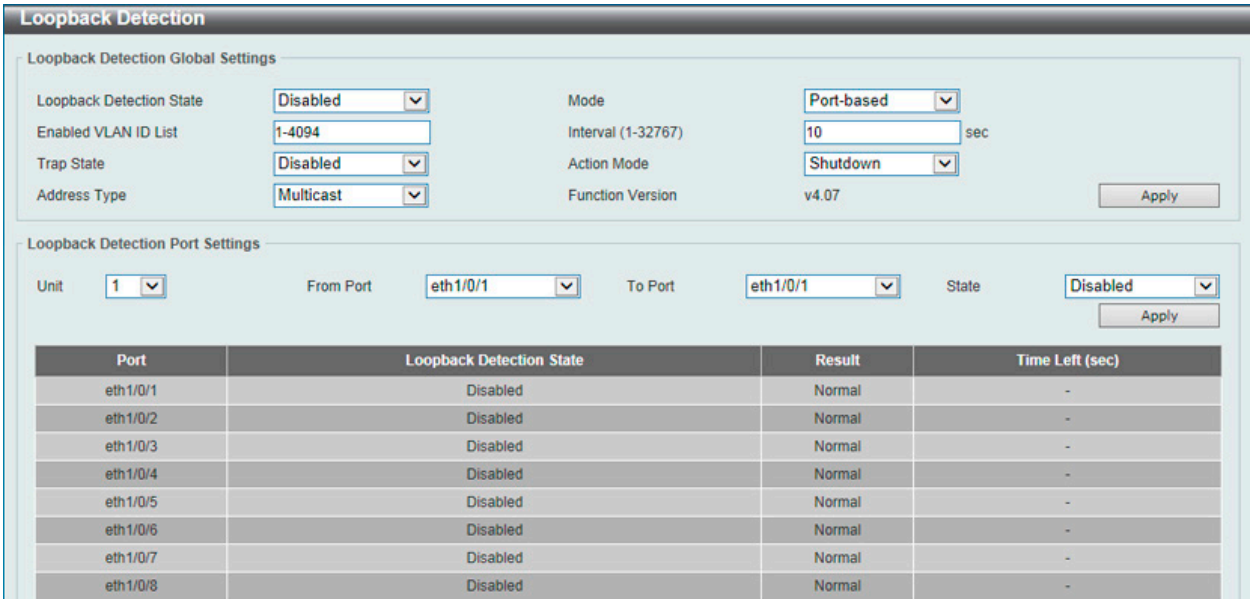


図 8-58　Loopback Detection 画面

以下の項目が表示されます。

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」
Enable VLAN ID List	「Mode」で「VLAN ID」を選択した場合、VLAN ID のリストを入力します。
Interval	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	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。

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

注意　「Untag（タグなし）」時でも「VID 0」は CTP に「Tag Field」を付与されます。規定上「VID 0」は「Untag（タグなし）」として扱われますが、古い一部のハードウェア製品（chipset 等）では破棄する場合があるのでご注意ください。

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。

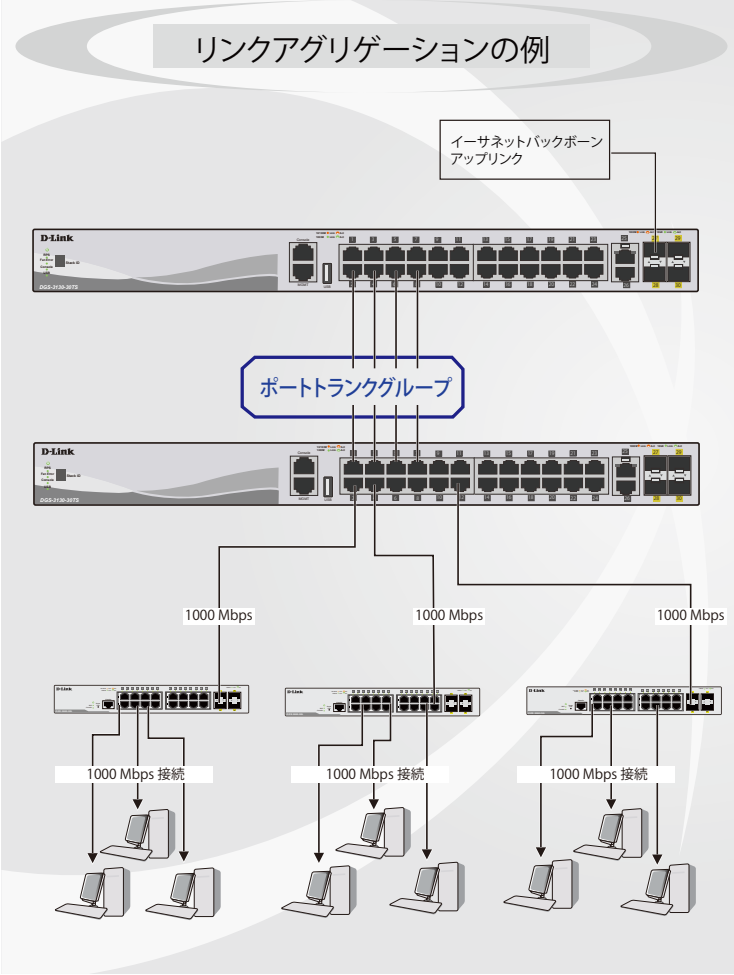


図 8-59　ポートトランクグループの例

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、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、スイッチレベルにおいて、リンクアグリゲーショングループを 1 つのリンクとして扱います。ポートレベルでは、STP はマスタポートのパラメータを使用してポートコストを計算し、リンクアグリゲーショングループの状態を決定します。スイッチに冗長化された 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はブロックされます（冗長リンクを持つ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。

注意　10/100/1000BASE-T ポートと SFP+ スロットでのリンクアグリゲーション、または SFP スロットと SFP+ スロットでのリンクアグリゲーションは利用できません。

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

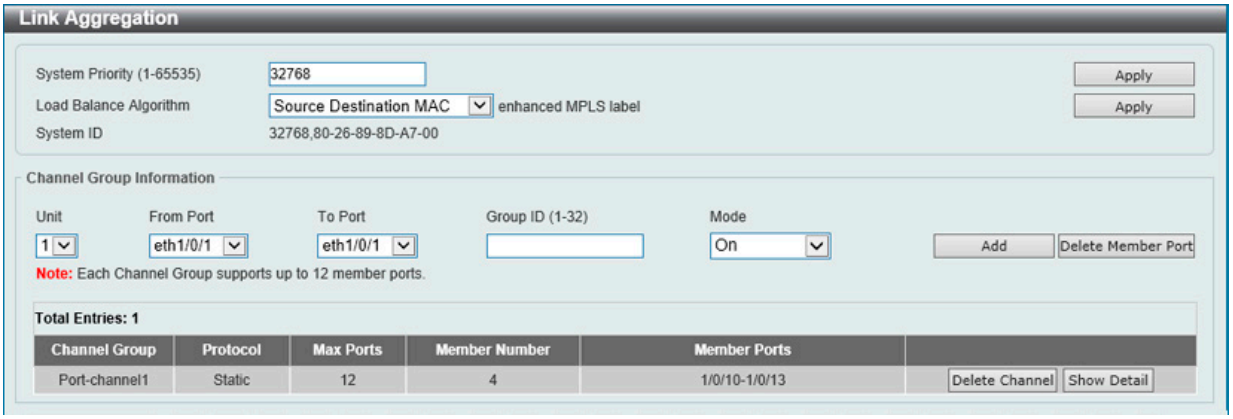


図 8-60　Link Aggregation 画面

以下の項目が表示されます。

項目	説明
System Priority	システム優先値を指定します。システム優先値はどのポートがポートチャネルに属するか、そしてどのポートがスタンドアロンモードに入るかを決定します。値の小さい方が高い優先度を示します。二つ以上のポートで同じ優先値を与えられた場合、ポート番号で優先値が決まります。 • 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」「Source L4 Port」「Destination L4 Port」「Source Destination L4 Port」 • 初期値：「Source Destination MAC」

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

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。ポートが初めてチャネルグループに参加すると、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。

ポートトランクグループの編集

チャネルの詳細情報を表示するには「Show Detail」をクリックします。

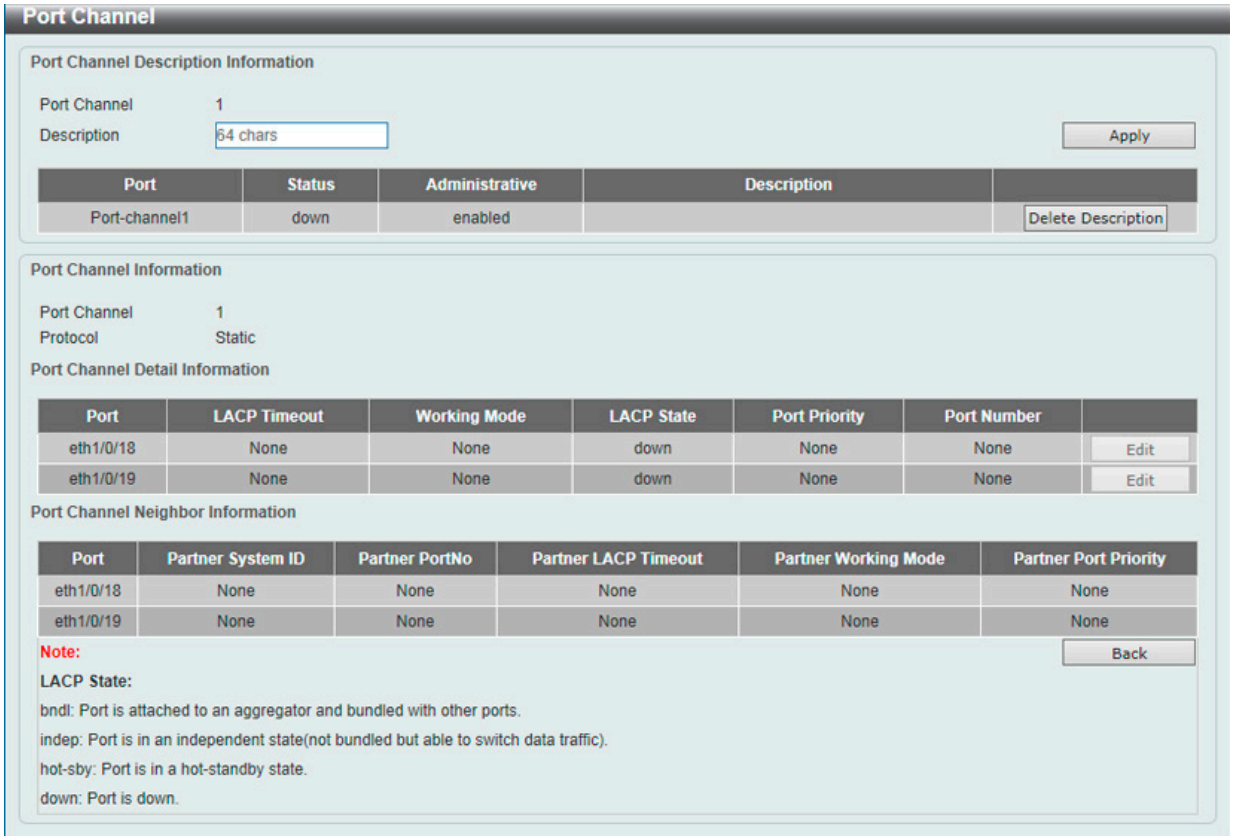


図 8-61　Port Channel 画面

以下の項目が表示されます。

Port Channel Description Information

項目	説明
Description	ポートチャネルの概要を指定します。（64 字以内）

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

「Delete Description」ボタンをクリックして、ポートチャネルの概要を削除します。

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。

「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。

「Back」ボタンをクリックし前の画面に戻ります。

L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）

レイヤ 2 プロトコルトンネリングポートを設定します。

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。

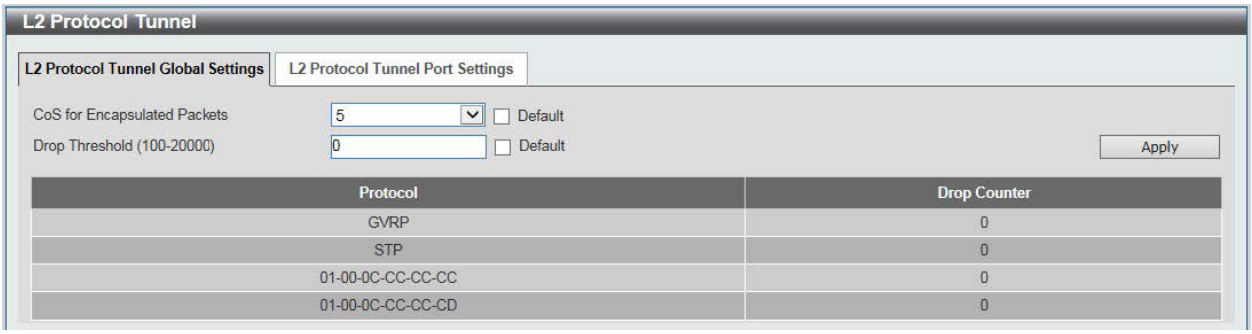


図 8-62　Layer 2 Protocol Tunneling（L2 Protocol Tunnel Global Settings）画面

以下の項目が表示されます。

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指定します。 • 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

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

L2 Protocol Tunnel Port Setting タブをクリックし、次の画面を表示します。

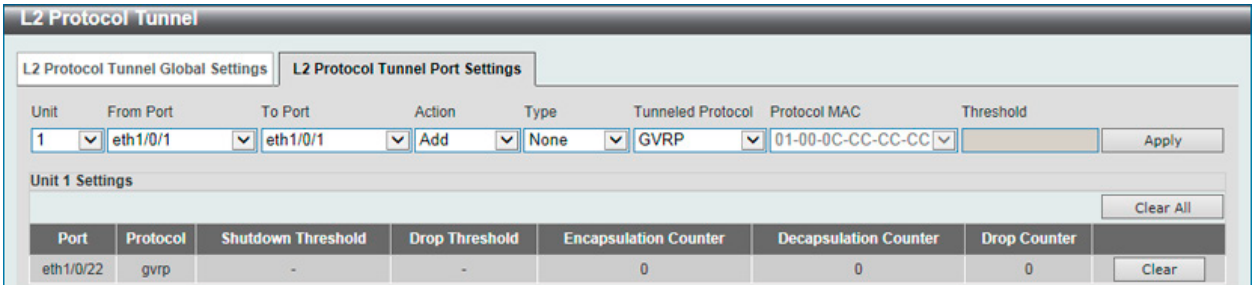


図 8-63　Layer 2 Protocol Tunneling（L2 Protocol Tunnel Port Settings）画面

以下の項目が表示されます。

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。
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	ポートタイプを指定します。 • 選択肢：「None」「Shutdown」「Drop」
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、トンネルする L2 プロトコルパケットの送信先 MAC アドレスを指定します。 • 選択肢：「01-00-0C-CC-CC-CC 」「01-00-0C-CC-CC-CD」
Threshold	「Type」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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear」ボタンをクリックして、カウンタ情報を削除します。
「Clear All」ボタンをクリックして、すべてのカウンタ情報を削除します。

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 Contro（l 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。また、スイッチを通過する IGMP メッセージの情報に基づいて、指定したデバイスに接続するポートをオープン / クローズできるようになります。

IGMP Snooping Settings（IGMP Snooping 設定）

IGMP Snooping 設定をグローバルに有効または無効にします。

IGMP Snooping 機能を利用するためには、まず、画面上にある「IGMP Snooping Global Settings」でスイッチ全体を有効にする必要があります。その後、対応する「Edit」ボタンをクリックして、各 VLAN に詳細な設定を行います。
IGMP Snooping を有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバに接続するポートをオープンまたは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ていないと判断すると、マルチキャストパケットの送信を停止します。

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

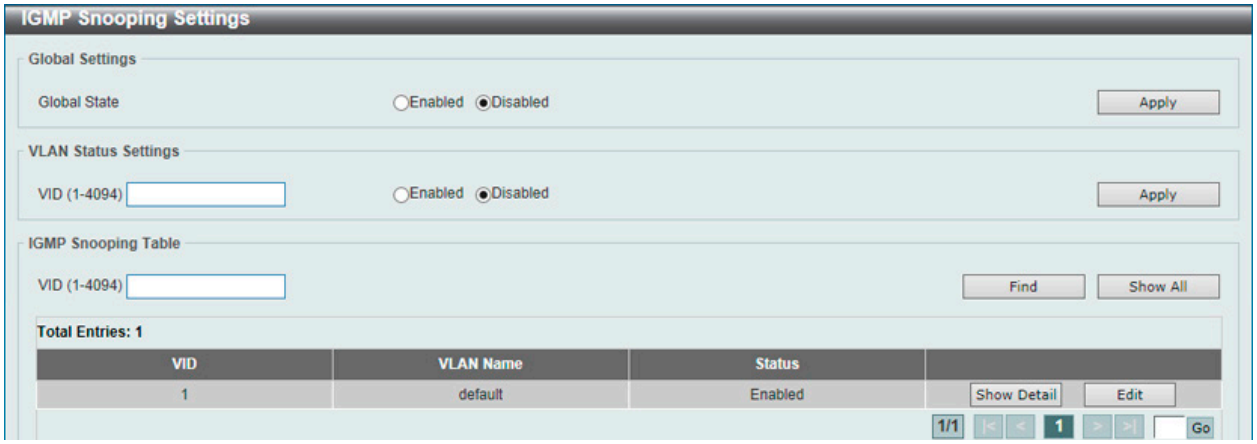


図 8-64　IGMP Snooping Settings 画面

以下の項目が表示されます。

項目	説明
Global Setting	
Global State	IGMP 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 IGMP Snooping を有効 / 無効に設定します。 • 設定可能範囲：1-4094
IGMP Snooping Table	
VID	IGMP Snooping 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

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
「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。
「Show 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表示します。

IGMP Snooping VLAN の詳細情報表示

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

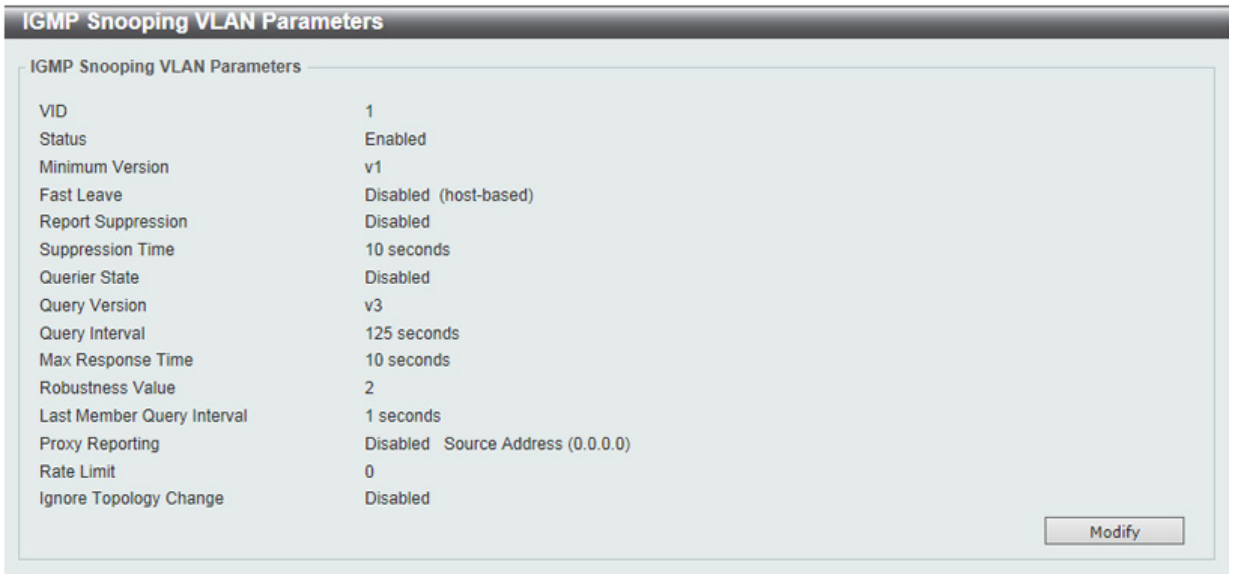


図 8-65　IGMP Snooping VLAN Parameters 画面

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

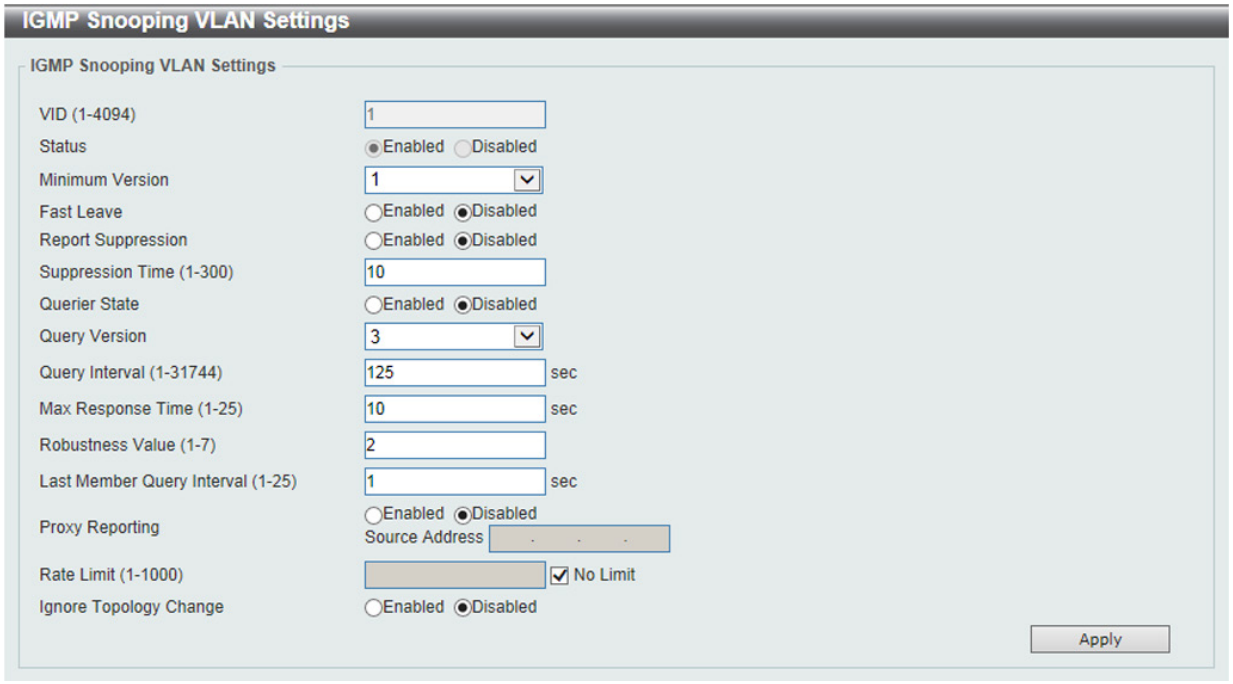


図 8-66 IGMP Snooping VLAN Settings 画面

以下の項目が表示されます。

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。この機能が有効になると、システムが IGMP done メッセージを受信すると、メンバシップはただちに失効します。

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。 有効になるとホストによるレポートの重複した送信は抑制されます。抑制は抑制時間（Suppression Time）を過ぎるまで続きます。同じグループに対する Report/Leave メッセージは、1 つのメッセージとして送信され、残りのメッセージは抑制されます。
Suppression Time	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）
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 クエリの送信間隔を指定します。 • 設定可能範囲：1-31744（秒） • 初期値：125（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） • 初期値：10（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。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。 • 設定可能範囲：1-7 • 初期値：2
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 • 初期値：1
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、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 / 無効にします。有効にするとトポロジの変更は無視されます。

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

注意 IGMP Snooping 機能には以下の制限があります。

- IGMPv3 SSM Leave を受信した際 Fast Leave として動作します。
- IGMPv3 の場合に expires: の項目が、Report を受けても更新されず、0DT0H0M0S のままとなります。
- IGMPv3 もしくは IGMPv3/IGMPv2 が混在した環境では fast-leave は機能しません。
- Querier Emulation を使用した際に、IGMPv2/v3 混在環境において、Specific Query は送信されません。
- Querier Emulation を IGMPv3 で使用した際に、Query に設定される Max Response Code の設定値は IGMPv2 と同じ値になります。
- Querier Emulation を IGMPv3 で使用した際に、Query に設定される Querier's Query Interval Code の設定値が正しくない制限があります。

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

「IGMP Snooping Group Table」を表示します。IGMP Snooping 機能では、スイッチを通過する IGMP パケットからマルチキャストグループ IP アドレスと対応する MAC アドレスを読み取ることができます。

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

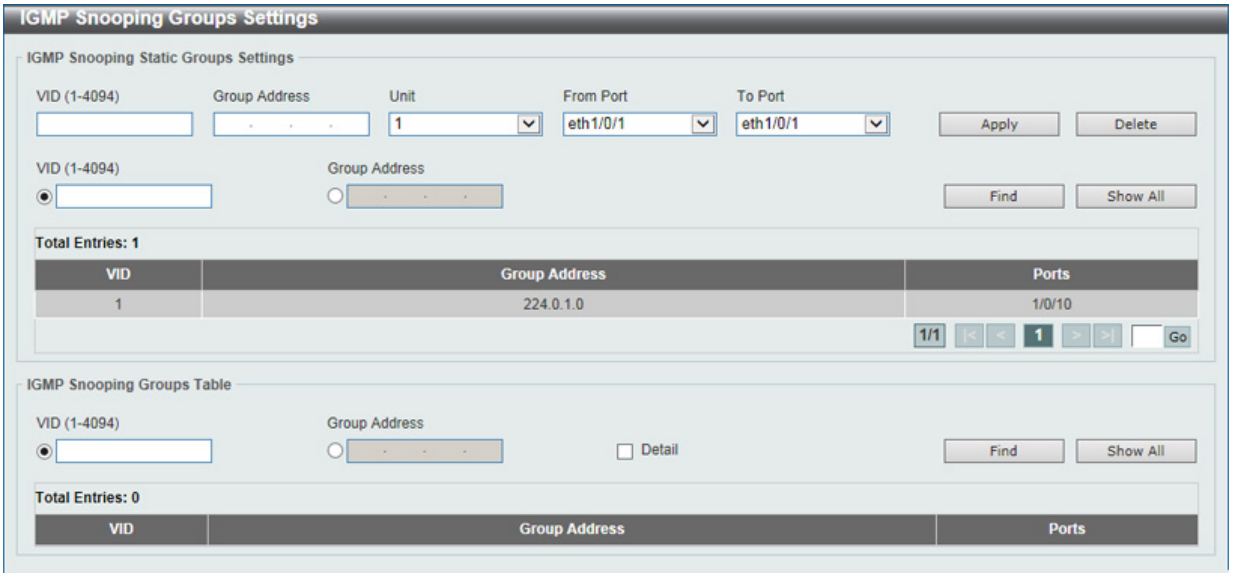


図 8-67　IGMP Snooping Groups Settings 画面

以下の項目が表示されます。

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

項目	説明
VID	登録または削除するマルチキャストグループの VLAN ID 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	設定するポートの範囲を設定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。

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

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

項目	説明
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。
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、指定条件に基づくエントリを検索 / 表示します。
「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。

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

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

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

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

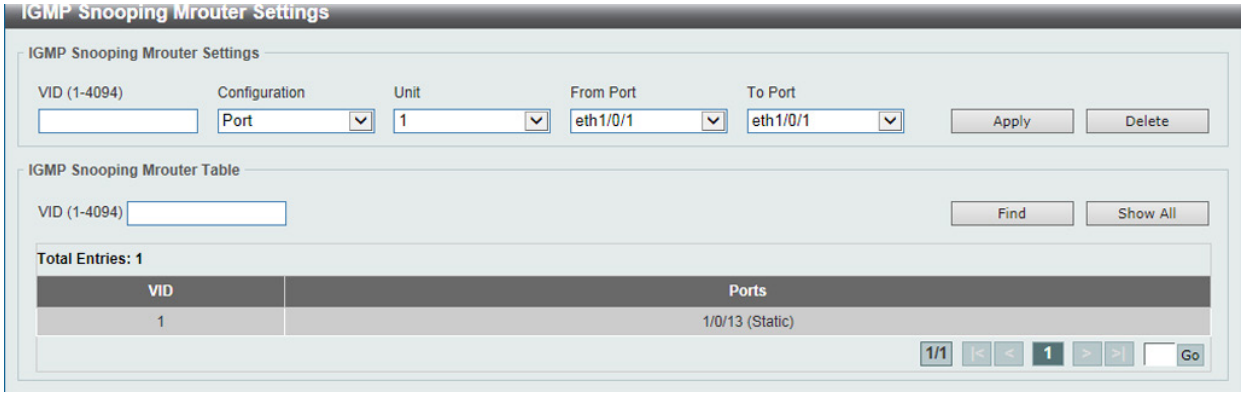


図 8-68　IGMP Snooping Mrouter Settings 画面

以下の項目が表示されます。

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。
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。
IGMP Snooping Mrouter Table	
VID	VLAN ID を入力します。

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

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

IGMP Snooping Statistics Settings（IGMP Snooping 統計設定）

現在の IGMP Snooping の統計情報を表示します。

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

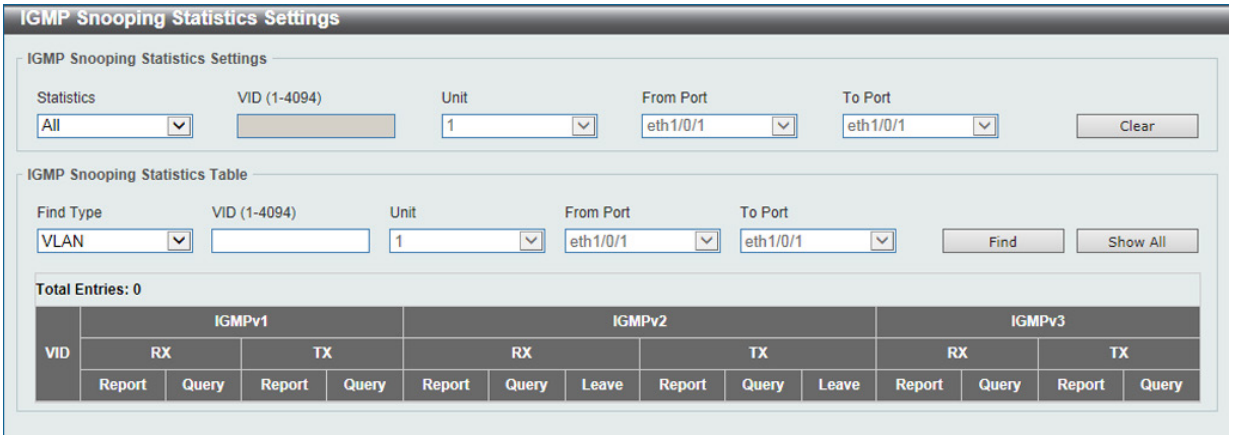


図 8-69　IGMP Snooping Statistics Settings 画面

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
IGMP Snooping Statistics Settings	
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	本設定を適用するユニットを選択します。「Statistics」で「Port」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Statistics」で「Port」を選択すると設定可能になります。
IGMP Snooping Statistics Table	
Find Type	インタフェースを選択します。 • 選択肢：「VLAN」「Port」
VID	VLAN ID1 から 4094 の間で指定します。「Find Type」で「VLAN」を選択すると設定可能になります。
Unit	本設定を適用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	設定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。

「Clear」ボタンをクリックして、統計情報をクリアします。
「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。
「Show 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表示します。

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設定します。

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。

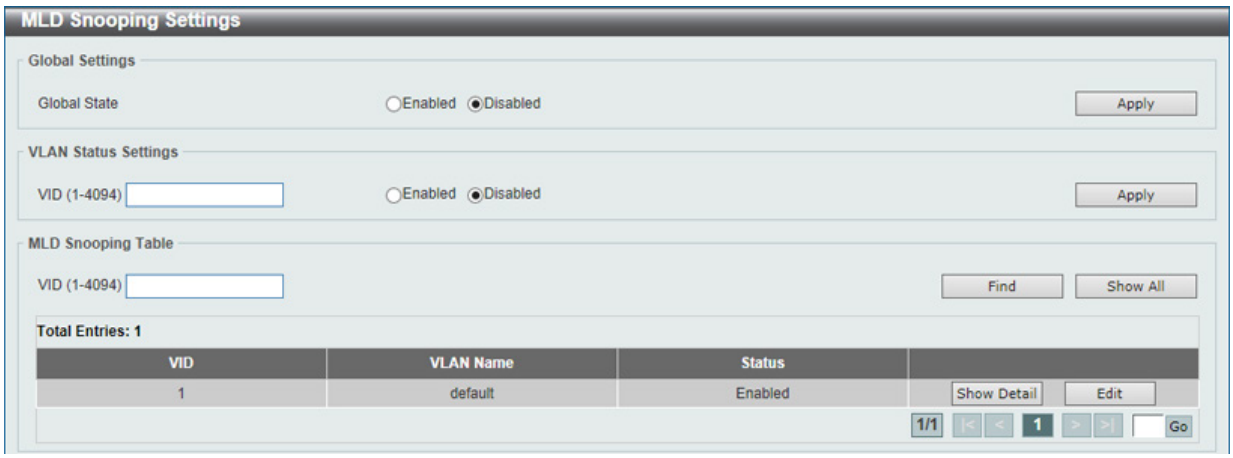


図 8-70　MLD Snooping Settings 画面

以下の項目が表示されます。

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 テーブルに表示する VLAN の VLAN ID を指定します。 • 設定可能範囲：1-4094

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

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 8-71　MLD Snooping VLAN Parameters 画面

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

MLD Snooping 機能の詳細設定

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。

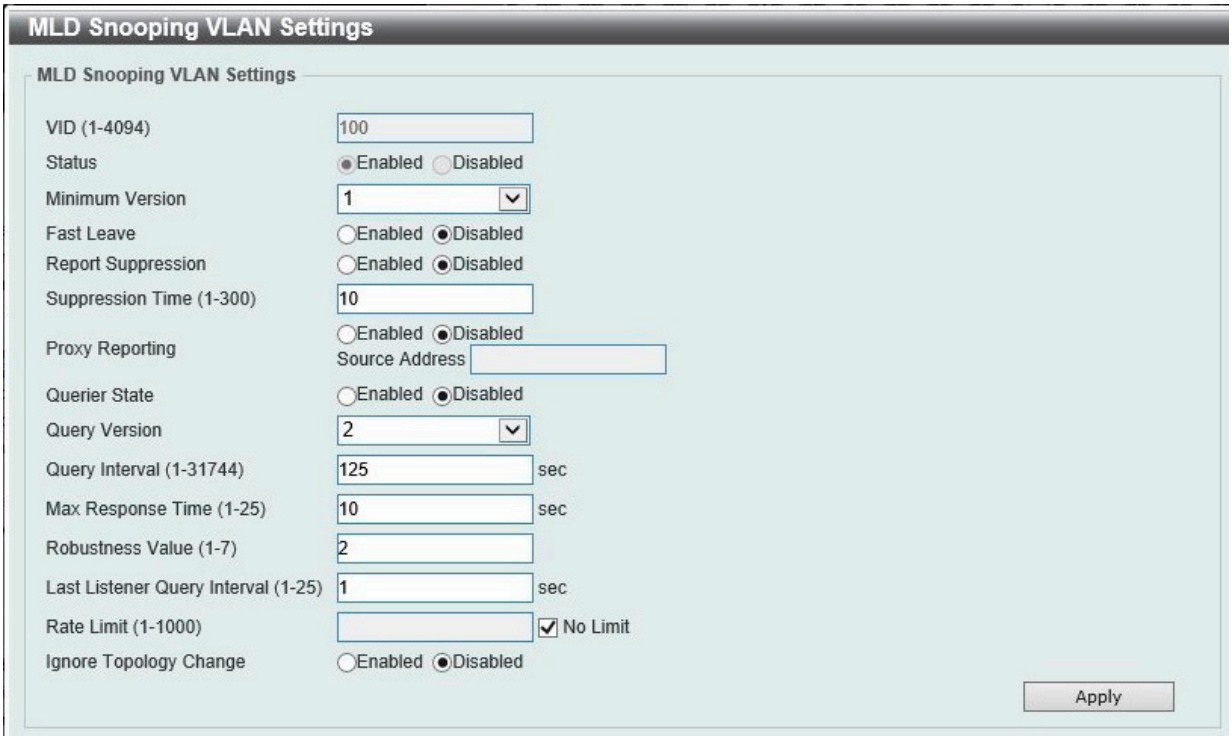


図 8-72 MLD Snooping VLAN Settings 画面

以下の項目が表示、または設定変更に使用できます。

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。
State	VLAN の MLD Snooping 機能お有効 / 無効ステータスを表示します。
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。この機能が有効になると、スイッチが MLD Leave 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は（Last Member Query Time の失効を待たずに）直ちにグループから脱退します。 • 初期値：「Disabled」（無効）
Report Suppression	特定の VLAN への 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。 レポートサスペンション機能は「MLDv1」「MLDv2」トラフィックでのみ機能します。 有効になるとホストによるレポートの送信は抑制されます。抑制は抑制時間（Suppression Time）を過ぎるまで続きます。
Suppression Time	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	プロキシレポーティングの送信元 IP アドレスを指定します。
Querier State	MLD Query パケットの送信を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
Query Version	MLD スヌーピングクエリアに送信されるクエリパケットのバージョンを選択します。 • 選択肢：「1」「2」
Query Interval	MLD query 送信間隔を指定します。 • 設定可能範囲：1-31744（秒） • 初期値：125（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） • 初期値は 10（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。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。 • 設定可能範囲：1-7 • 初期値：2
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。 • 初期値：1

項目	説明
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。

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

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

「MLD Snooping Group Table」を表示します。MLD Snooping 機能では、スイッチを通過する MLD パケットからマルチキャストグループ IP アドレスと対応する MAC アドレスを読み取ることができます。

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

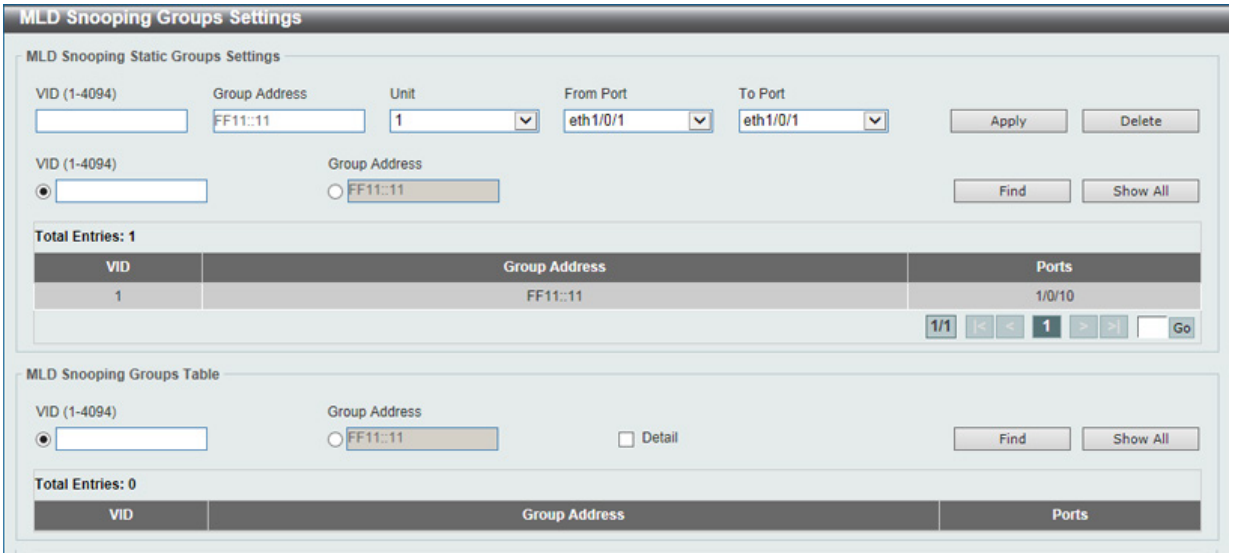


図 8-73　MLD Snooping Groups Settings 画面

以下の項目が表示されます。

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範囲を指定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。
MLD Snooping Groups Table	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。
Detail	MLD グループの詳細について表示します。

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

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

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

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

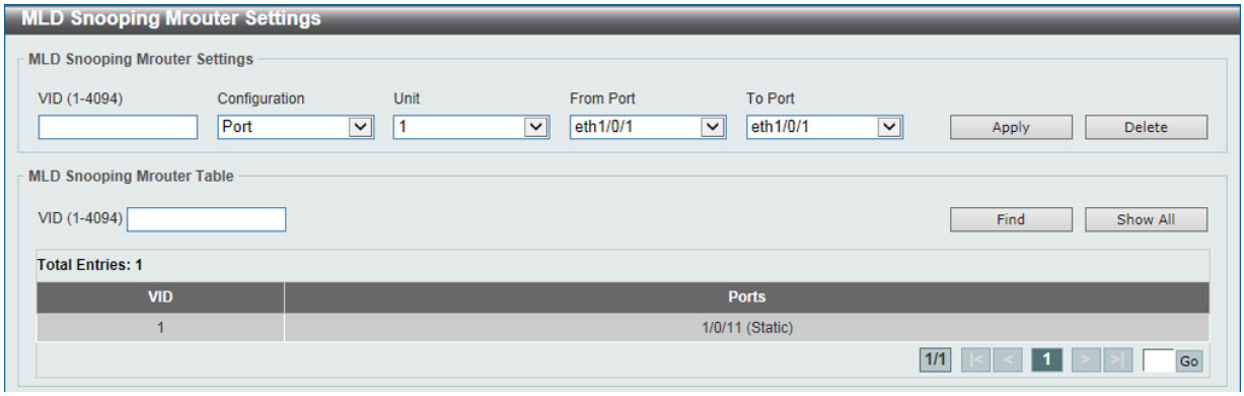


図 8-74　MLD Snooping Mrouter Settings 画面

以下の項目が表示されます。

項目	説明
MLD Snooping Mrouter Settings	
VID	VLAN ID を入力します。
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 Router 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取得を有効にします。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
MLD Snooping Mrouter Table	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094

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

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。

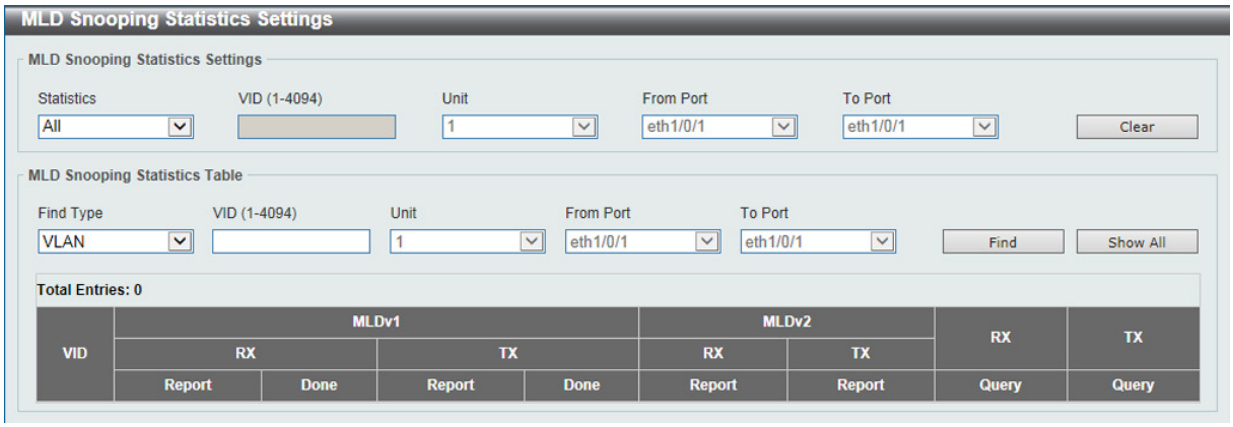


図 8-75　MLD Snooping Statistics Settings 画面

以下の項目が表示されます。

項目	説明
MLD Snooping Statistics Settings	
Statistics	インタフェースを選択します。 • 選択肢：「All」「VLAN」「Port」

項目	説明
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	本設定を適用するユニットを選択します。「Statistics」で「Port」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Statistics」で「Port」を選択すると設定可能になります。
MLD Snooping Statistics Table	
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	本設定を適用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	設定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。

「Clear」をクリックして、統計情報をクリアします。
「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。
「Show 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 をクリックして表示します。

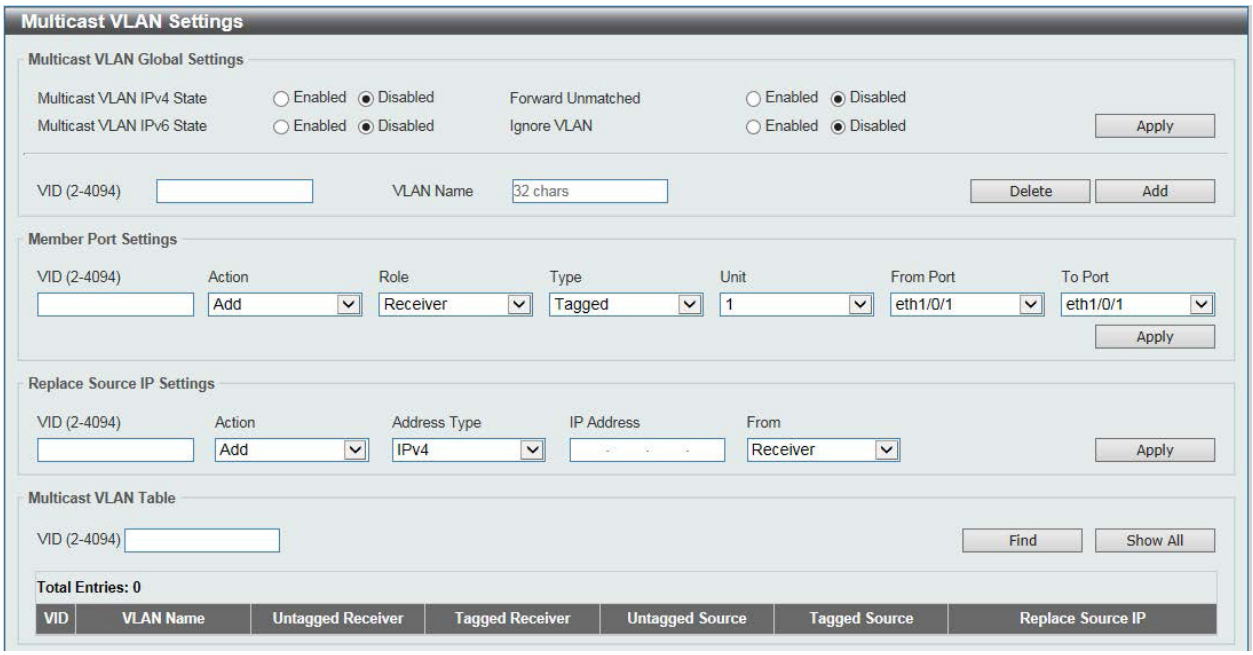


図 8-76　Multicast VLAN Settings 画面

以下の項目が表示されます。

項目	説明
Multicast VLAN Global Settings	
Multicast VLAN IPv4 State	マルチキャスト VLAN の IPv4 IGMP コントロールパケットを有効または無効に設定します。
Forward Unmatched	「Forward Unmatched」を有効または無効に設定します。 「タグなし」「どのプロファイルともマッチしない」「関連するデフォルト VLAN がマルチキャスト VLAN」「マルチキャスト VLAN でタグ付けされているが、どのプロファイルともマッチしない」などの条件の IGMP/MLD コントロールパケットを受信した場合、本設定で破棄（Drop）か転送（Forward）を指定します。初期値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 の IPv6 MLD コントロールパケットを有効 / 無効に設定します。
Ignore VLAN	「Ignore VLAN」を有効 / 無効に設定します。タグ付き IGMP/MLD コントロールパケットに対する設定となります。本設定を有効にすると、パケットの VLAN は無視され、プロファイルの照合を行って一致するマルチキャスト VLAN を検出します。

項目	説明
VID	作成 / 削除する 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 VLAN 名を指定します。
Member Port Settings	
VID	設定する VLAN の VID を指定します。 • 設定可能範囲：2-4094
Action	実行する動作を指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
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、当該ポートからの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、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 Source IP Settings	
VID	設定する VLAN の VID を指定します。 • 設定可能範囲：2-4094
Action	実行する動作を指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Address Type	アドレスの種類を指定します。 •「IPv4」- 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」- 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 アドレスは置き換えられます。 •「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 アドレスは置き換えられます。 • Both - マルチキャスト VLAN Receiver/Source ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスは置き換えられます。
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

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして、エントリを削除します。
「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。
「Show 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表示します。

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。

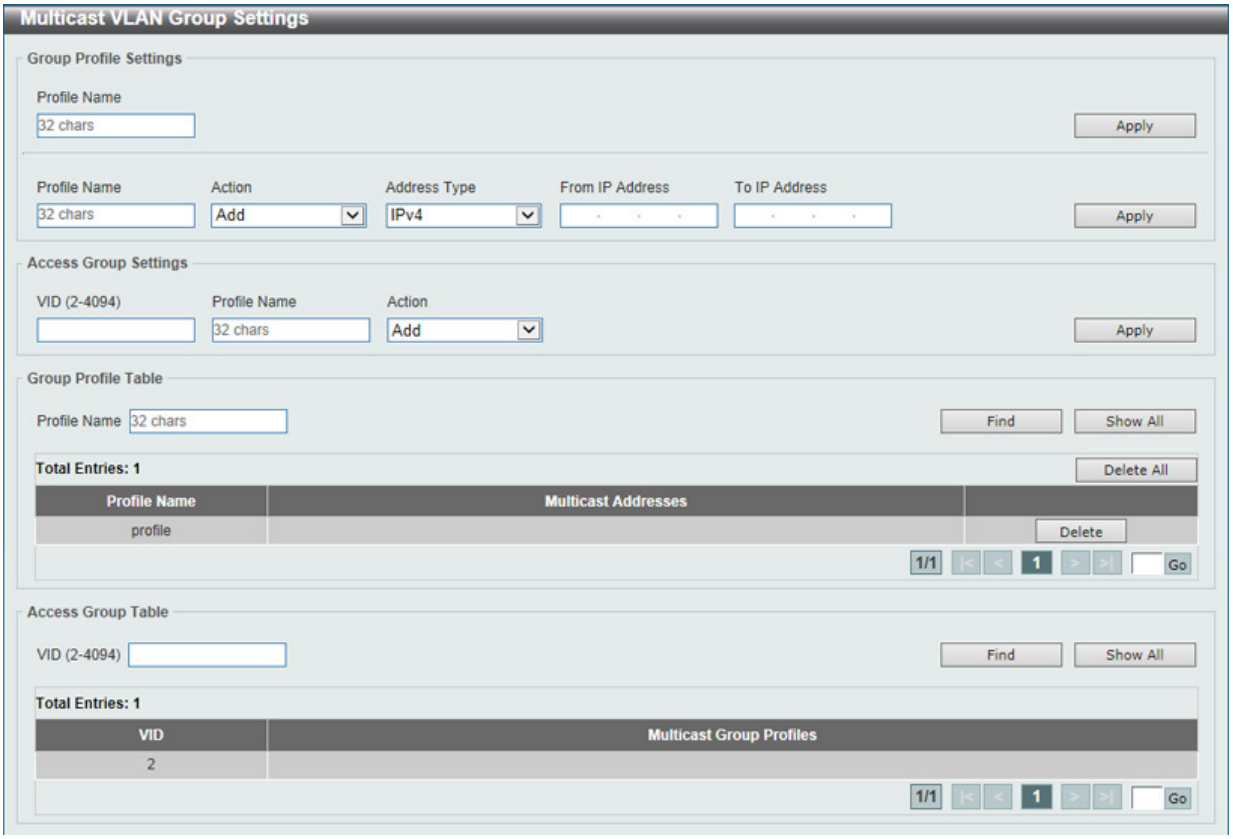


図 8-77　Multicast VLAN Group Settings 画面

以下の項目が表示されます。

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。複数の範囲をマルチキャスト VLAN プロファイルに追加することができます。単一のプロファイルに指定される 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	送信元 IPv4/IPv6 アドレスを指定します。
To IP Address	宛先 IPv4/IPv6 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。 • 選択肢：「Add（追加）」「Delete（削除）」
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

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

エントリの削除

「Delete」をクリックして、エントリを削除します。

「Delete All」ボタンをクリックして、テーブル上のすべての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、指定条件に基づくエントリを検索 / 表示します。
「Show All」ボタンをクリックして、テーブル上のすべてのエントリを表示します。

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

Multicast Filtering（マルチキャストフィルタリング）

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 8-78　Multicast Filtering Mode 画面

以下の項目が表示されます。

項目	説明
VID List	本設定を適用する VLAN の VLAN ID リストを入力します。
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」- 選択すると登録されたマルチキャストパケットはフォワーディングテーブルに基づいて転送され、登録されていないマルチキャストパケットは VLAN ドメインにフラッドします。 • 「Forward All」- 選択するとすべての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」- 選択すると登録されたマルチキャストパケットはフォワーディングテーブルに基づき転送され、登録されていないマルチキャストパケットはフィルタされます。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

LLDP

LLDP（Link Layer Discovery Protocol）は、IEEE 802 ネットワークに接続しているステーションから同じ IEEE 802 ネットワークに接続している他のステーションに通知を出します。本プロトコルによって送信される情報は、受信先によって標準の管理情報ベース（MIB）に格納されるので、SNMP（Simple Network Management Protocol）などの管理プロトコル使ったネットワーク管理システム（NMS）からその情報にアクセスできるようになります。

LLDP Global Settings（LLDP グローバル設定）

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

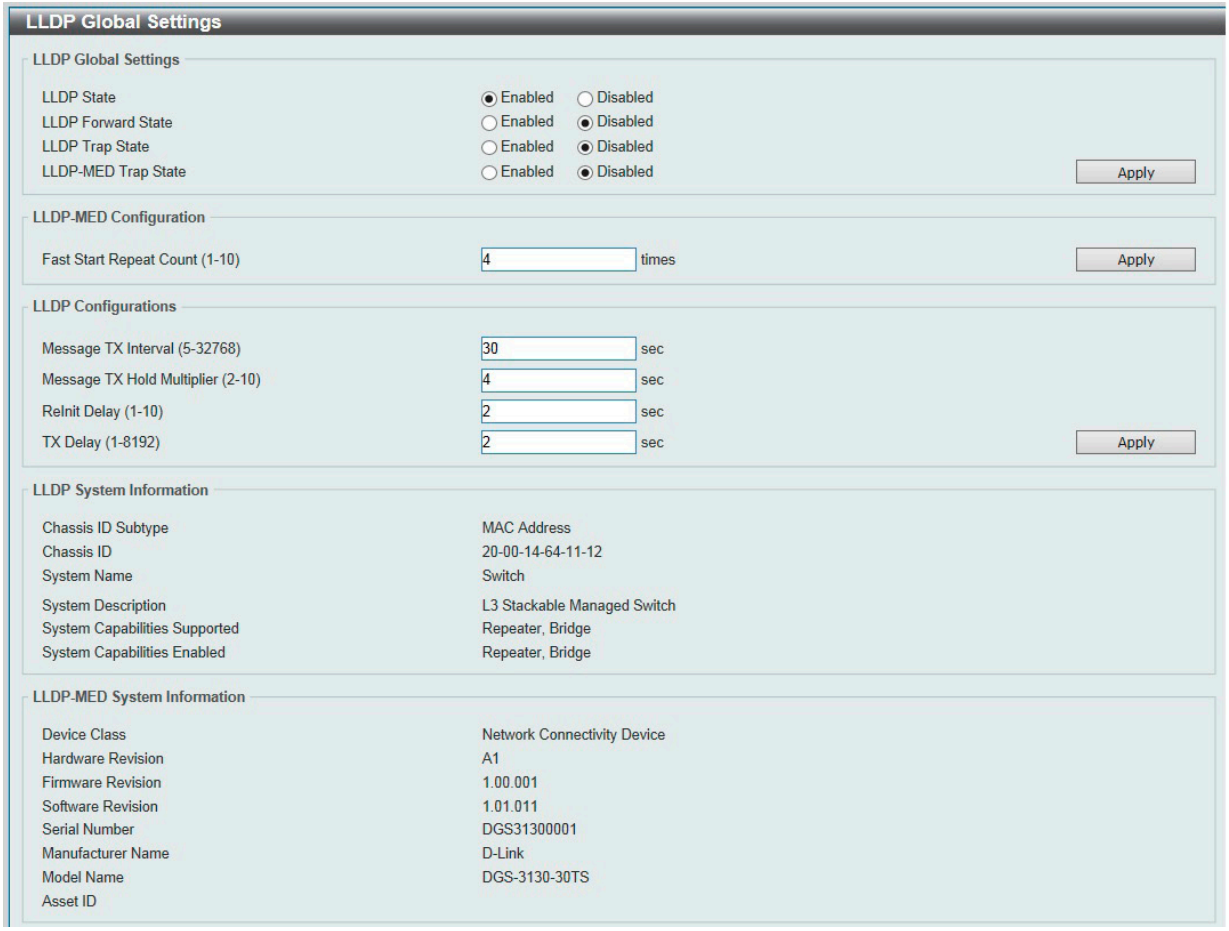


図 8-79　LLDP Global Settings 画面

以下の項目が表示されます。

項目	説明
LLDP State	スイッチにおける 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 Trap を有効 / 無効に設定します。
LLDP-MED Trap State	LLDP-MED Trap を有効 / 無効に設定します。
LLDP-MED Settings	
Fast Start Repeat Count	「LLDP-MED」ファストスタートリピートカウント値を指定します。 • 設定可能範囲：1-10
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。 • 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。 • 設定可能範囲：2-10
ReInit Delay	LLDP ポートが再初期化を行う前に待機する最小時間を指定します。 • 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。転送間隔の数値の 1/4 より大きくすることはできません。 • 設定可能範囲：1-8192（秒）

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

LLDP Port Settings（LLDP ポート設定）

LLDP ポートパラメータを設定します。

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

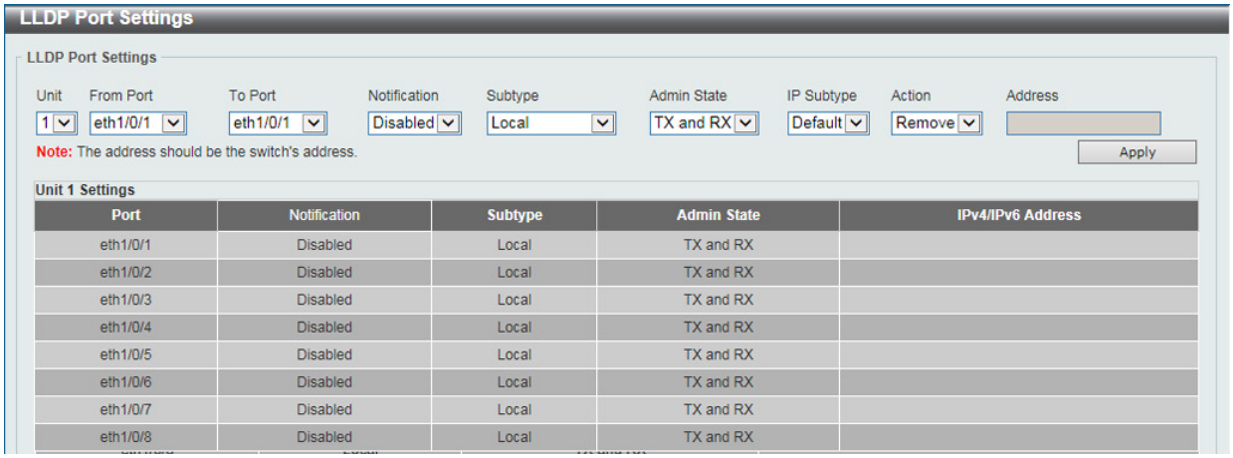


図 8-80　LLDP Port Settings 画面

以下の項目が表示されます。

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 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	通知のステータスを選択します。 • 「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	通知するエンティティの管理アドレスを入力します。

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

注意　入力の 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）

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 8-81　LLDP Management Address List 画面

以下の項目が表示されます。

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。 IPv4 を選択した場合、IPv4 アドレスを入力します。IPv6 を選択した場合、IPv6 アドレスを入力します。 • 選択肢：「All」「IPv4」「IPv6」

「Find」ボタンをクリックし、LLDP 管理情報を検索します。

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

LLDP パケットの TLV（Type-length-value）フィールドを使用すると、TLV エレメントとして特定の情報を送信することができます。スイッチのアクティブな LLDP ポートは、通常その外向き通知に常に必須データを含んでいます。必須データタイプには、4 つの基本的な情報タイプ（end f LLDPDU TLV、chassis ID TLV、port ID TLV および Time to Live TLV）があります。必須データタイプは無効にすることができません。さらに、オプションで選択可能な 4 つのデータタイプ（Port Description、System Name、System Description および System Capability）があります。

本画面では、個別のポートまたはポートグループに対してオプションの 4 つのベーシック TLV 設定を変更することができます。

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

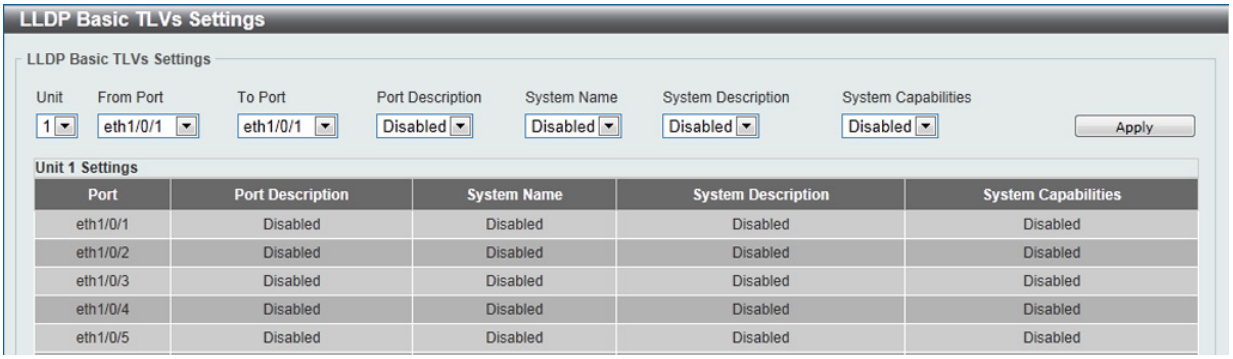


図 8-82　LLDP Basic TLVs Settings 画面

以下の項目が表示されます。

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。
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。
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。

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

LLDP 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。

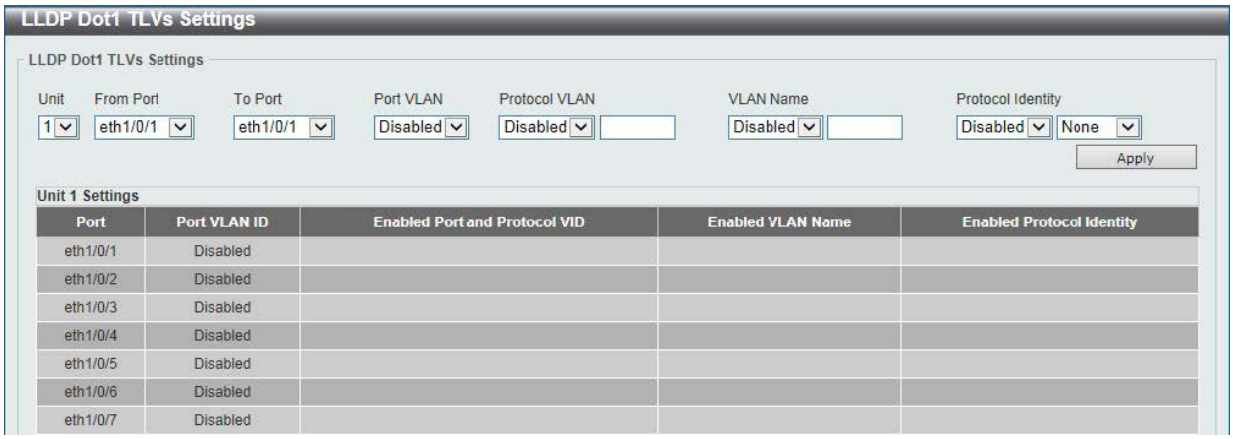


図 8-83　LLDP Dot1 TLVs Settings 画面

以下の項目が表示されます。

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。
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 VLAN ID TLV」は、VLAN ブリッジポートにタグなし / タグ付きフレームの PVID の通知を許可する固定長のオプション TLV です。
Protocol VLAN	プロトコル VLAN ID の通知を有効 / 無効に設定します。プロトコル VLAN ID TLV は、固定長のオプション TLV です。このオプションを利用すると、VLAN ブリッジポートにより、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。
VLAN Name	VLAN 名の通知を有効 / 無効に設定します。右の欄に VLAN 名 TLV の VLANID を入力します。
Protocol Identity	プロトコル識別子の通知を有効 / 無効に設定します。次に、対象とするプロトコルを「None」「EAPOL」「LACP」「GVRP」「STP」「All」から選択します。

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

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。

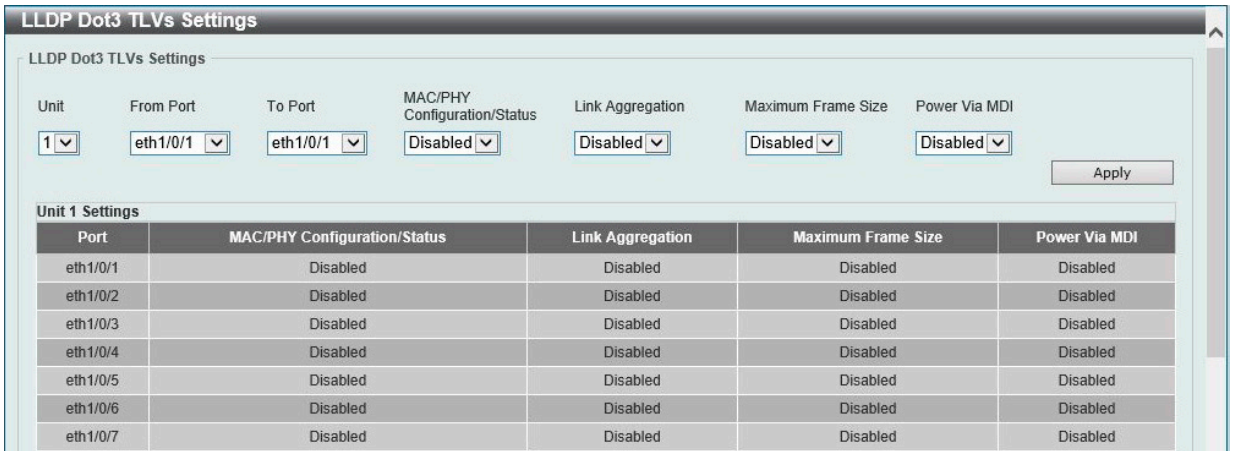


図 8-84　LLDP Dot3 TLVs Settings 画面

以下の項目が表示されます。

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。

項目	説明
MAC/PHY Configuration/Status	スイッチの MAC または PHY 状態の通知を有効 / 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	スイッチのリンクアグリゲーション状態の通知を有効 / 無効に設定します。 リンクアグリゲーション 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に設定されていない場合、ID は 0 となります。
Maximum Frame Size	最大フレームサイズの通知を有効 / 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。
Power Via MDI	「Power Via MDI」送信を有効 / 無効に設定します。

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

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

LLDP-MED TLV の送信を有効または無効に設定します。

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。

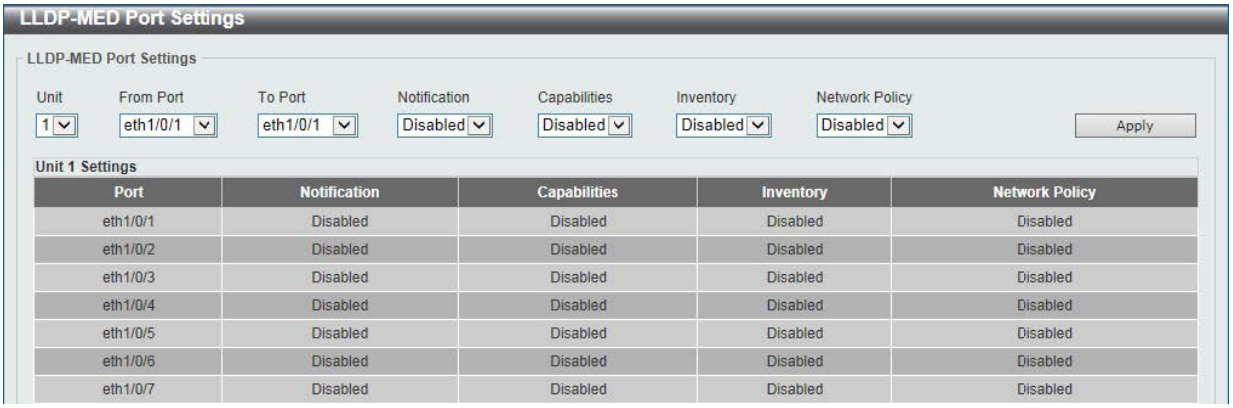


図 8-85　LLDP-MED Port Settings 画面

以下の項目が表示されます。

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。

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

LLDP Statistics Information（LLDP 統計情報）

スイッチにおける LLDP 統計情報と各ポートの設定を参照できます。

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。

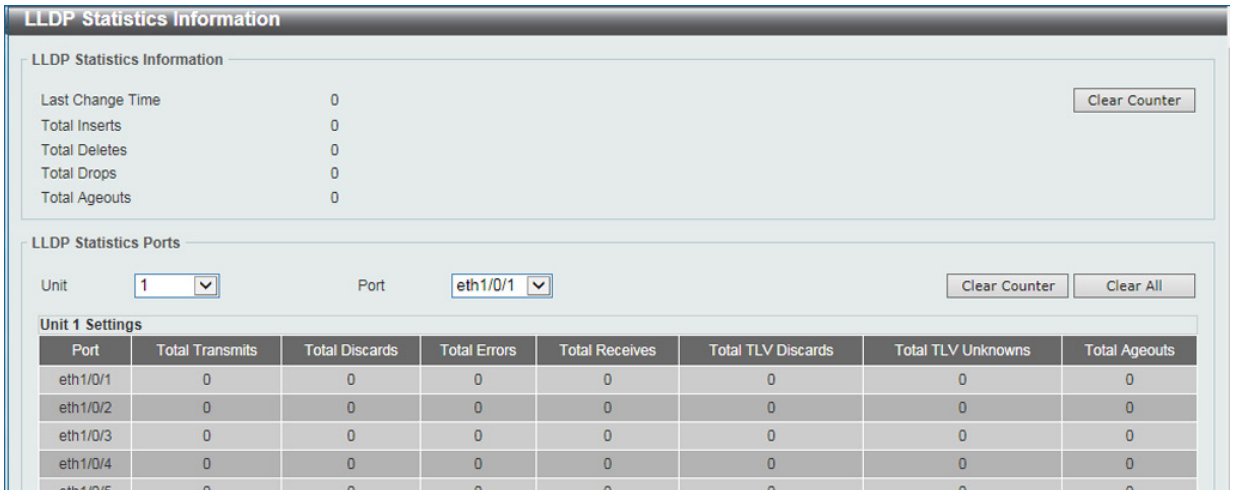


図 8-86　LLDP Statistics Information 画面

以下の項目が表示されます。

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

「Clear Counter」をクリックして、（指定条件に基づく）統計情報のカウンタ数をクリアします。
「Clear All」をクリックして、すべてのカウンタ数をクリアします。

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

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。

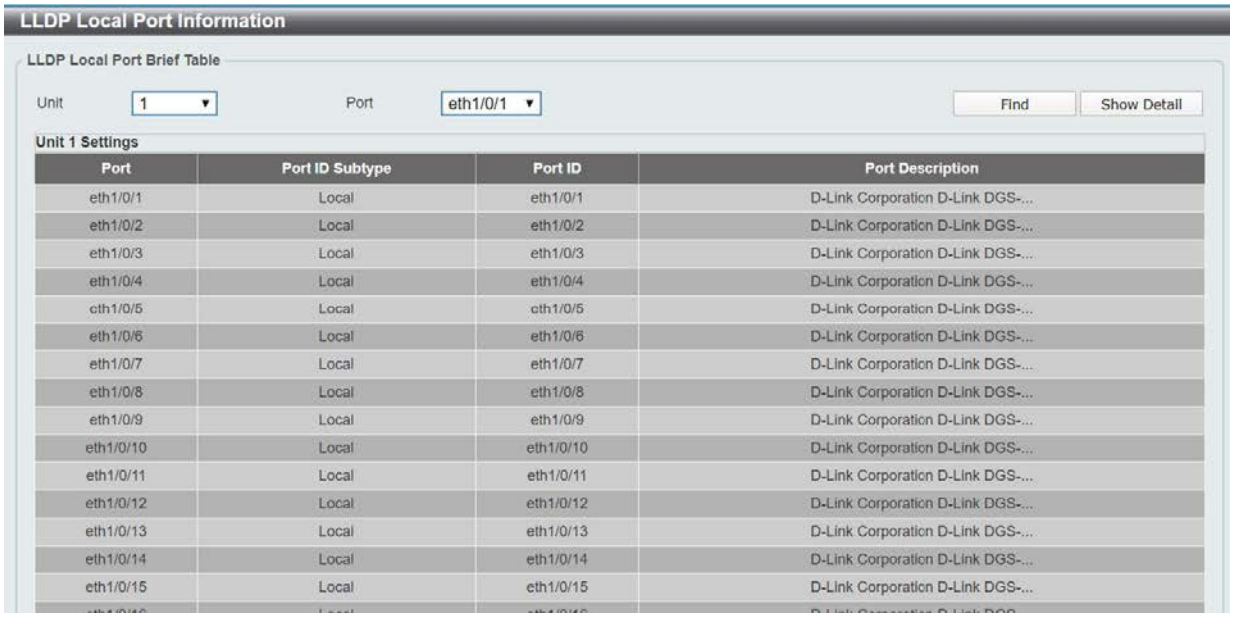


図 8-87　LLDP Local Port Information 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。
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、指定条件に基づくエントリを検索 / 表示します。

各パラメータの詳細の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。

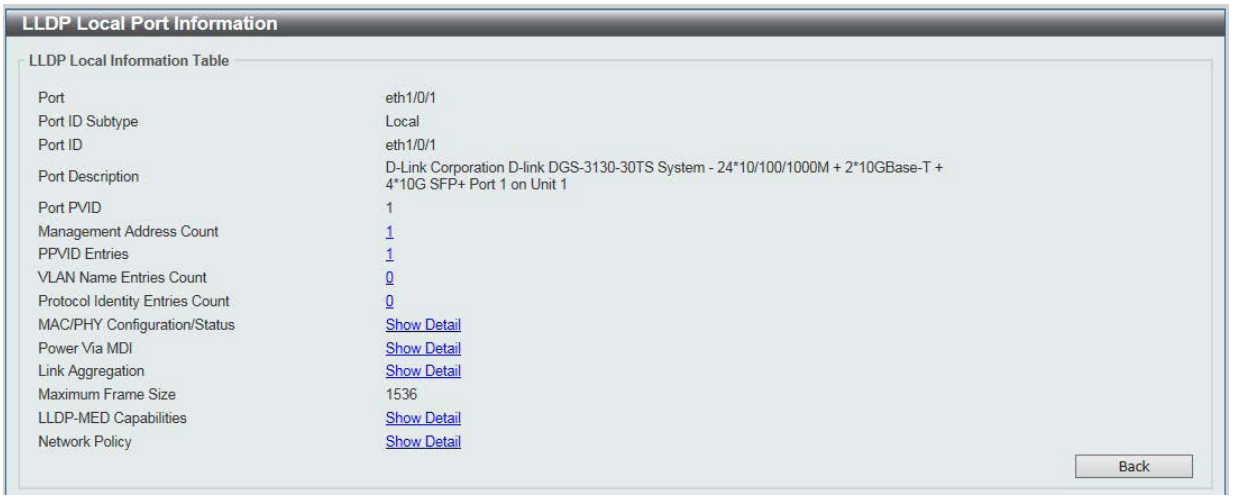


図 8-88　LLDP Local Port Information（Show Detail）画面

「MAC/PHY Configuration/Status」情報の参照

「LLDP Local Information Table」の各項目に表示される「Show Detail」リンクをクリックすると、画面下部に該当の情報が表示されます。



図 8-89　LLDP Local Port Information - MAC/PHY Configuration/Status 画面

「Back」ボタンをクリックし前画面に戻ります。

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

Neighbor から学習したポート情報を表示します。スイッチはリモートステーションからパケットを受信し、ローカルに情報を保存することができます。

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 8-90　LLDP Neighbor Port Information 画面

以下の項目が表示されます。

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

エントリの検索 / 表示

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Show All」ボタンをクリックして、テーブル上のすべてのエントリを表示します。

ポート情報の削除

「Clear」をクリックして、ポート情報を削除します。
「Clear All」ボタンをクリックして、すべてのポート情報を削除します。

詳細情報の表示

「Show Detail」をクリックして、ポート詳細情報を表示します。

第 9 章　L3 Features（レイヤ 3 機能の設定）

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 パケットの設定を行います。
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 アドレス形式のスタティックルートを設定します。
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。
Route Preference（ルート優先度設定）	ルート優先度を設定します。
ECMP Settings（ECMP 設定）	Equal-Cost Multi-Path (ECMP) ルーティング設定を行います。ロードバランシングハッシュアルゴリズムの設定と、同じ宛先の複数パスエントリに対しネクストホップを決定する際に使用されます。
IPv6 General Prefix（IPv6 汎用プリフィクス）	VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。
RIP（Routing Information Protocol）※	RIP（Routing Information Protocol）は、距離ベクトル型のルーティングプロトコルです。
RIPng Settings（RIPng 設定）※	RIPng（Routing Information Protocol next generation）の設定を行います。RIPng は、ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルであり、IPv6 ベースのネットワーク用です。
OSPF（OSPF 設定）※	OSPF を設定します。
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）※	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。
IP Route Filter（IP ルートフィルタ）	ルートマップの作成、更新を行います。
Policy Route（ポリシールート設定）	ポリシーベースルーティングの設定、表示を行います。
VRRP（VRRP 設定）	VRRP（Virtual Routing Redundancy Protocol）は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です。
VRRPv3 Settings（VRRPv3 設定）	VRRPv3 設定を行います。

※サポート予定のため、使用できません。

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。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。

ARP Elevation（ARP エレベーション）

本項目では「Address Resolution Protocol」(ARP) エレベーションの表示、設定を行います。宛先がスイッチ自身の場合に、スイッチに ARP トラフィックを送信することが可能です。このトラフィックは他の ARP パケットよりも高い優先度を持ちます。

L3 Features > ARP > ARP Elevation の順にクリックし、以下の画面を表示します。

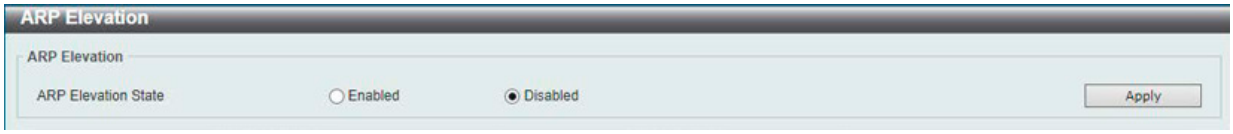


図 9-1　ARP Elevation 画面

以下の項目が表示されます。

項目	説明
ARP Elevation State	ARP エレベーションを有効 / 無効に設定します。

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

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 9-2　ARP Aging Time 画面

設定には以下の項目が表示されます。

項目	説明
Timeout	ARP テーブルエントリを保持する時間を設定します。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。 • 初期値：2（分）

「Edit」ボタンをクリックするとパラメータの設定が可能になります。「Apply」ボタンをクリックして設定内容を適用します。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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 9-3　Static ARP 画面

以下の項目が表示されます。

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、設定内容に基づくエントリを追加します。
「Delete」をクリックして、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。

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

Proxy ARP（プロキシ ARP）

プロキシ ARP 機能に関する基本設定を参照および編集します。

他のデバイスへ送信される ARP リクエストに対し、識別情報（IP および MAC アドレス）を元の ARP 応答者の代わりに応答する機能です。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）が別の機器に送信された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。

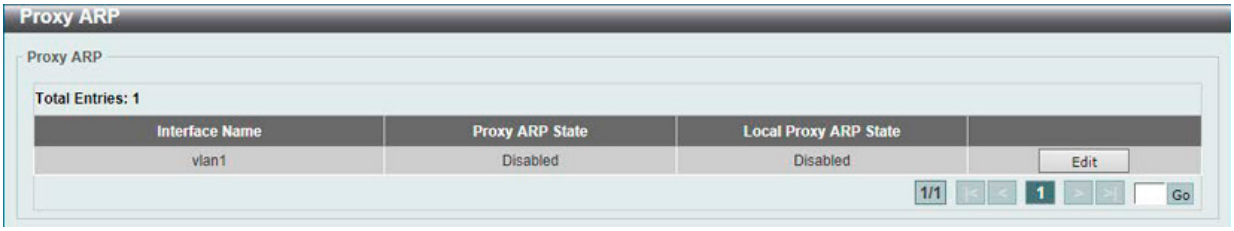


図 9-4　Proxy ARP 画面

以下の項目が表示されます。

項目	説明
Proxy ARP State	プロキシ ARP を有効 / 無効に設定します。
Local Proxy ARP State	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 機能は送信元 IP と宛先 IP が同じインタフェースの場合、スイッチがプロキシ ARP に返答します。

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「Apply」ボタンをクリックして設定内容を適用します。

ARP Table（ARP テーブルの参照）

スイッチ上の ARP エントリを表示、設定します。

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。

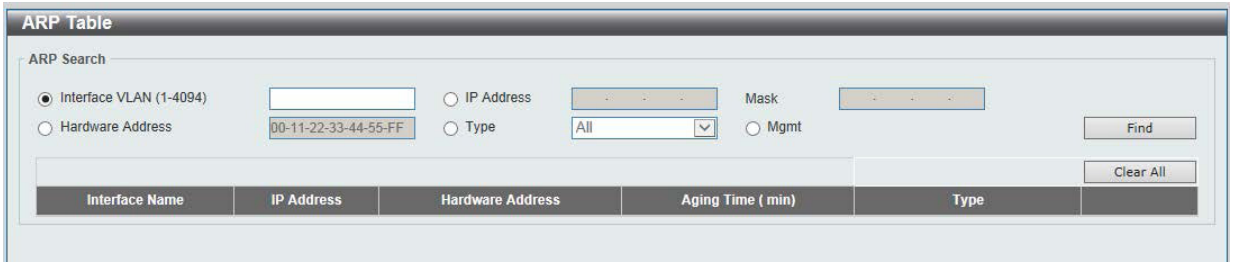


図 9-5　ARP Table 画面

設定には以下の項目が表示されます。

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」
Mgmt	管理ポートについての情報を表示します。

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。
「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削除します。

Gratuitous ARP（Gratuitous ARP 設定）

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た ARP リクエストであり、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ます。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。

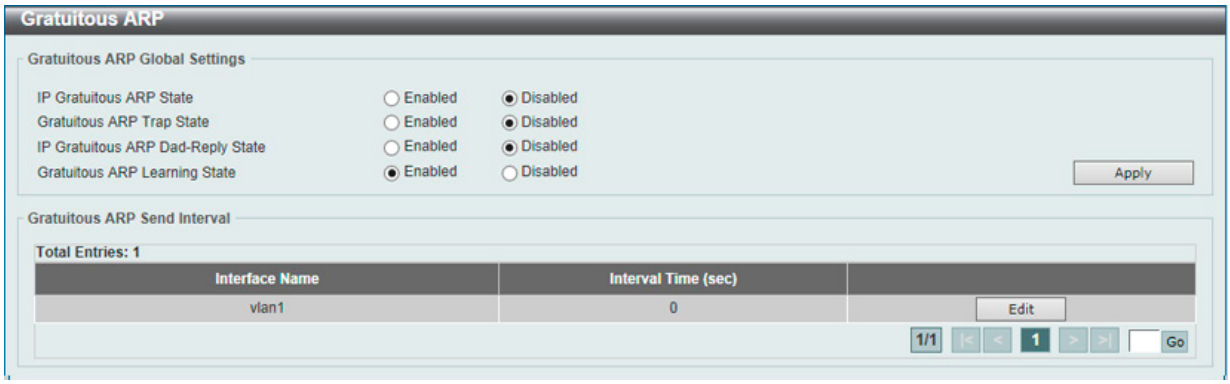


図 9-6　Gratuitous ARP 画面

以下の項目が表示されます。

Gratuitous ARP Global Settings

項目	説明
IP Gratuitous ARP State	ARP キャッシュテーブルの Gratuitous ARP パケットの習得を有効 / 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のみを学習します。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 / 無効に設定します。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。

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

Gratuitous ARP Send Interval

項目	説明
Interval Time(sec)	定期的に Gratuitous ARP を送信する間隔（秒）を入力します。0 は Gratuitous ARP リクエストが定期的に送信されないことを意味します。 • 初期値：0（秒）

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「Apply」ボタンをクリックして設定内容を適用します。

IPv6 Neighbor（IPv6 ネイバ設定）

スイッチの IPv6 ネイバ設定を行います。

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。

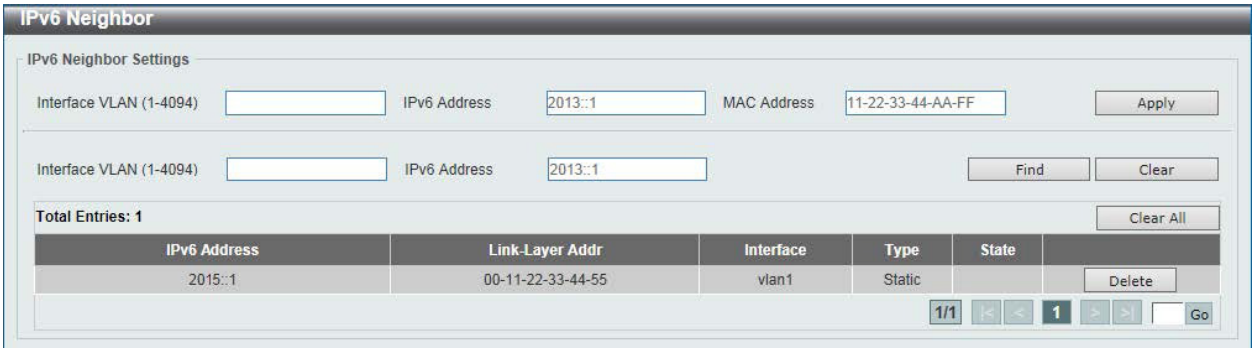


図 9-7　IPv6 Neighbor 画面

以下の項目が表示されます。

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 Neighbor の IPv6 アドレスを入力します。
MAC Address	対応する IPv6 デバイスの MAC アドレスを指定します。

IPv6 Neighbor を追加するには、画面上段の「Interface VLAN」、「IPv6 Address」および「MAC Address」を入力し、「Apply」ボタンをクリックします。
エントリを検索するには、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。
「Clear」または「Clear All」ボタンをクリックして、検索条件をリセットします。
「Delete」ボタンをクリックして、エントリを削除します。

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

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 IP インタフェース設定を行います。

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



図 9-8　IPv4 Interface 画面

スイッチの現在の IP インタフェース設定が表示されます。

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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

「Edit」ボタンをクリックして、以下の画面を表示します。

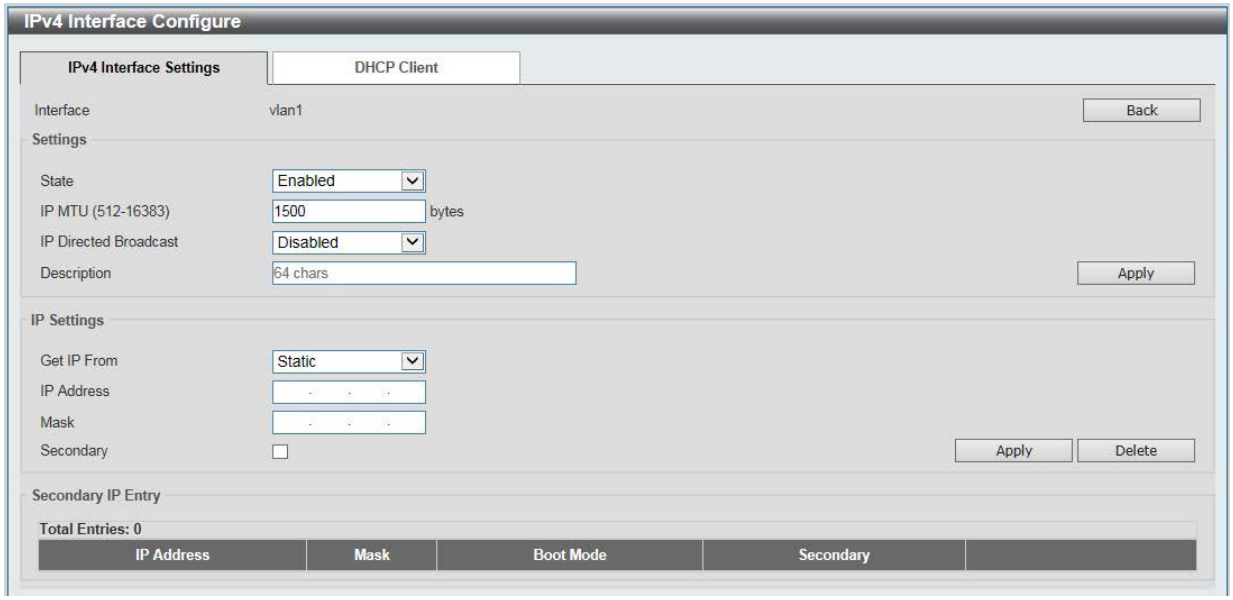


図 9-9　IPv4 Interface (Edit) 画面

以下の項目が表示されます。

項目	説明
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 / 無効にします。
IP MTU	使用する IP レイヤの 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 ダイレクト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 ダイレクト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	エントリの概要について入力します。（64 文字以内）

項目	説明
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	チェックを入れ、セカンダリインタフェースとして IPv4 アドレスとマスクを設定します。

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
入力 / 編集した変更を破棄し前のページに戻る場合は「Back」をクリックします。
「Delete」ボタンをクリックして、設定内容を削除します。

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

注意 IPv4 MTU が 1280 より小さい値で設定されている場合、IPv6 アドレスは付与できません。

IPv4 インタフェースの編集（DHCP Client）
「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。

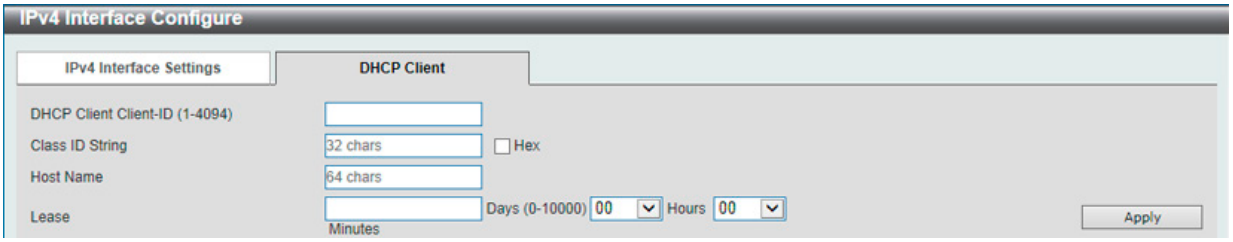


図 9-10　DHCP Client 画面

画面には以下の項目が表示されます。

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、ディスカバ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	最大 32 文字を使用してベンダクラス識別名を入力します。（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 ディスカバーメッセージに含まれるオプション 60 の値として使用されます。
Host Name	ホスト名を入力します。（64 文字以内）DHCP ディスカバー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 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）

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

IPv6 Interface（IPv6 インタフェース）

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



図 9-11　IPv6 Interface 画面

以下の項目が表示されます。（IPv6 Interface）

項目	説明
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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

「Show Detail」ボタンをクリックして、以下の画面を表示します。

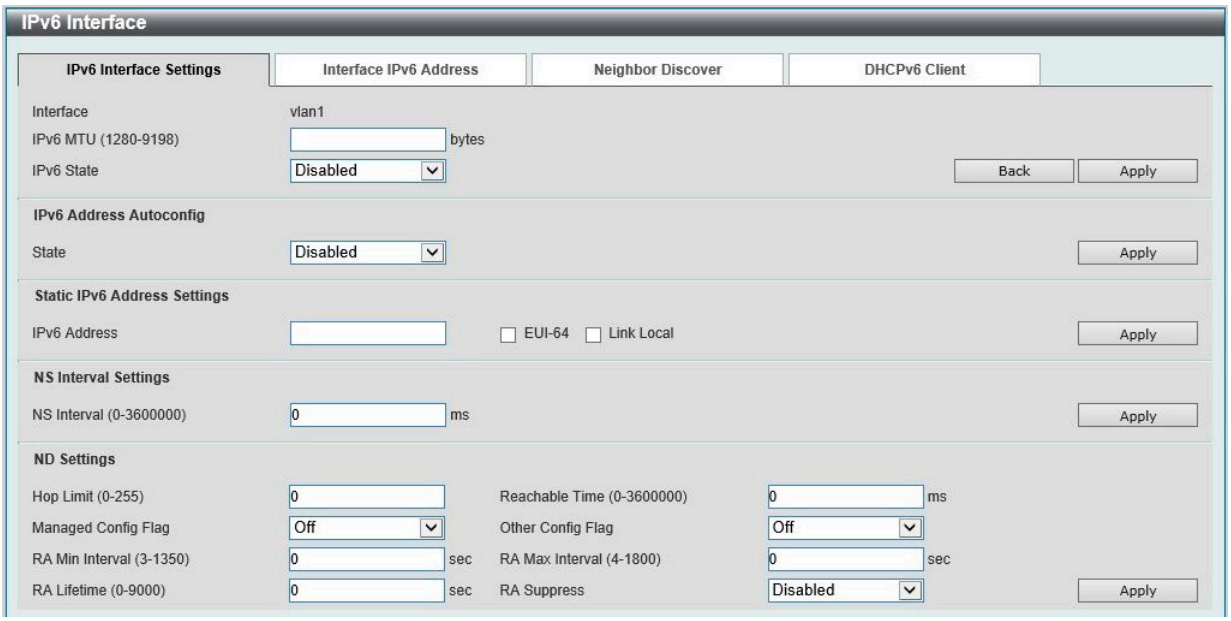


図 9-12　IPv6 Interface（IPv6 Interface Settings）画面

以下の項目が表示されます。

項目	説明
Interface	
IPv6 MTU	使用する IPv6 レイヤの MTU 値を入力します。RA メッセージ内での通知に使用されます。 • 設定可能範囲：1280 - 9198（Bytes） • 初期値：1500（Bytes）
IPv6 State	該当エントリの 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（stateless auto-configuration）を有効 / 無効に設定します。「Default」に指定すると、インタフェースの初期ルータが指定されます。初期ルータを使用すると初期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。
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。
NS Interval Settings	
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）
ND Settings	
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
Reachable Time	到達可能時間を指定します。「0」に指定すると、1200 秒となり、RA メッセージでは 0 を通知します。IPv6 ノードが、隣接しているノードの到達可否を判断する時間です。 • 設定可能範囲：0-3600000（ミリ秒）
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）

項目	説明
RA Lifetime	RA の生存時間を指定します。ホストは受信した RA に含まれる生存時間の値に基づき、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
RA Suppress	RA 通知の停止を有効 / 無効に設定します。

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

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

「Show Detail」ボタンをクリックして「Interface IPv6 Address」タブを選択すると、以下の画面が表示されます。



図 9-13　IPv6 Interface（Interface IPv6 Address）画面

「Delete」ボタンをクリックして、エントリを削除します。

IPv6 インタフェースの編集（ Neighbor Discover タブ）

「Show Detail」ボタンをクリックして「Neighbor Discover」タブを選択すると、以下の画面が表示されます。



図 9-14　IPv6 Interface（Neighbor Discover）画面

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「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）

「Show Detail」ボタンをクリックして「DHCPv6 Client」タブを選択すると、以下の画面が表示されます。

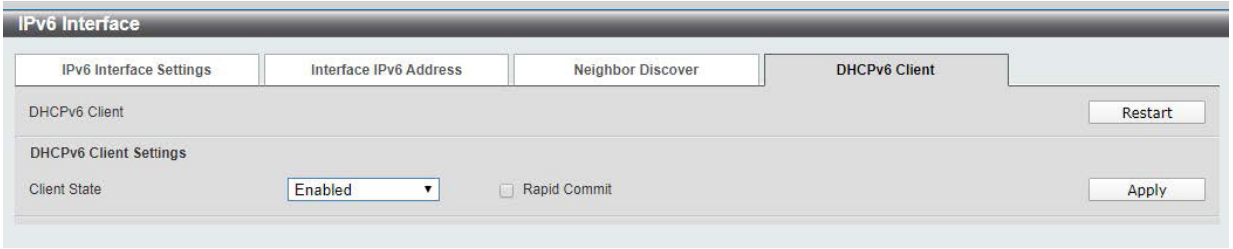


図 9-15　IPv6 Interface（DHCPv6 Client）画面

以下の項目が表示されます。

項目	説明
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。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Restart」ボタンをクリックすると、DHCPv6 クライアントサービスを再起動します。

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 9-16　Loopback Interface 画面

以下の項目が表示されます。

項目	説明
Interface Loopback	ループバックするインタフェース ID を入力します。 • 設定可能範囲：1-8

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

ループバックインタフェースの編集（Edit）
「Edit」ボタンをクリックして、以下の画面を表示します。

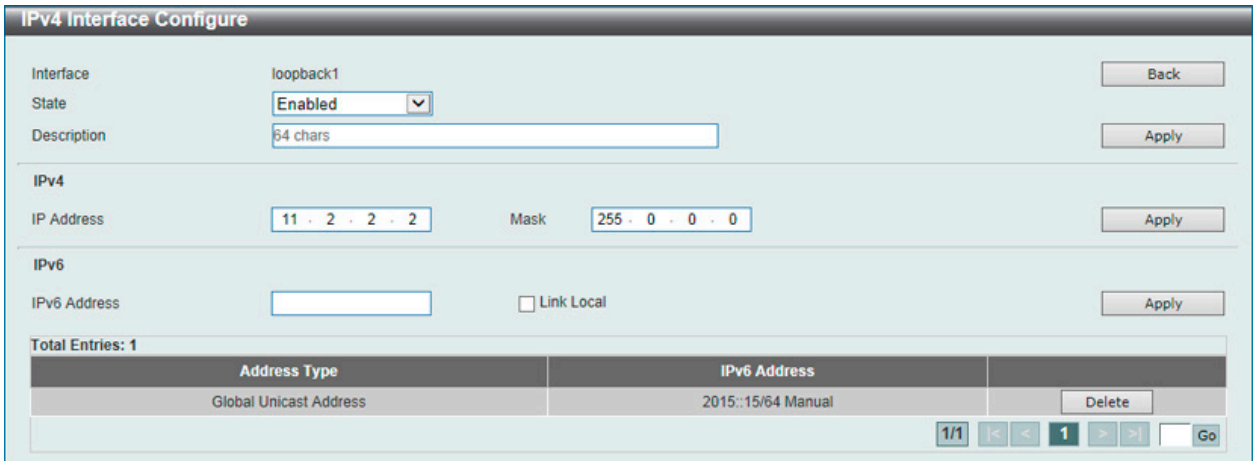


図 9-17　Loopback Interface Settings - Edit 画面

以下の項目が表示されます。

項目	説明
State	本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	本ループバックインタフェースの概要を入力します。（64 文字以内）
IP Address	本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。
Mask	本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 Address	本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	指定した 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。

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。
「Delete All」ボタンをクリックして、テーブル上のすべてのエントリを削除します。

「Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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。

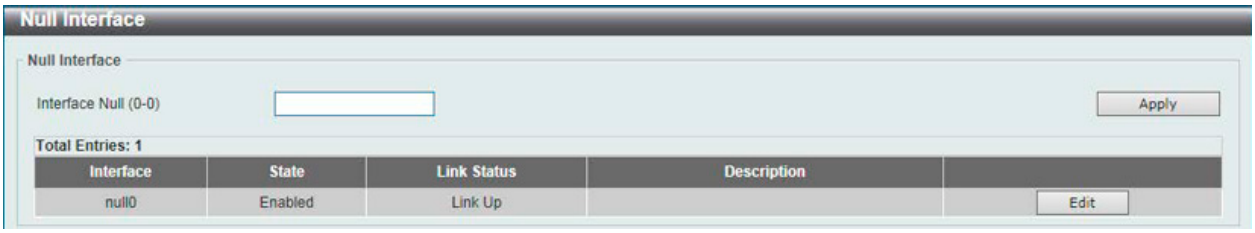


図 9-18　Null Interface 画面

以下の項目が表示されます。

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 Null インタフェースの概要を入力します。（64 文字以内）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Edit」ボタンをクリックすると設定を編集することができます。

UDP Helper（UDP ヘルパー）

IP 転送プロトコルの設定を行います。

IP Forward Protocol（IP 転送プロトコル）

本項目では、IP 転送プロトコルの設定、表示を行います。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。

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。

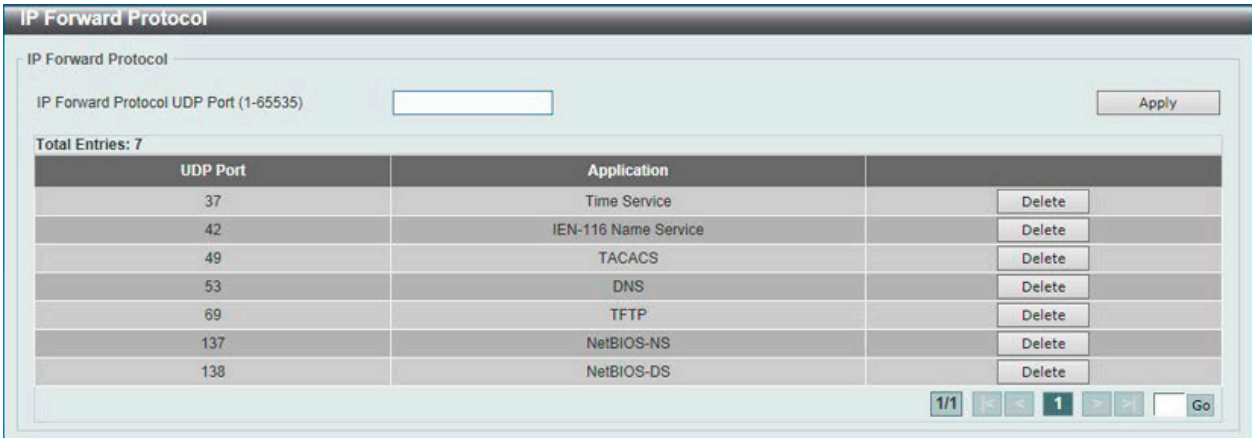


図 9-19　IP Forward Protocol 画面

以下の項目が表示されます。

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

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

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

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。以下の条件に一致した場合のみパケットが転送されます。

- 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 9-20　IP Helper Address 画面

以下の項目が表示されます。

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転送時のターゲット IPv4 アドレスを指定します。

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

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

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 には最大 512 個のスタティックルートエントリを作成することできます。
IPv4 スタティックルートでは、スタティックルートが設定されると、スイッチによってネクストホップルータに ARP リクエストパケットが送信されます。スイッチに対しネクストホップから ARP の応答が返されると、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。プライマリルートをなくした場合、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。

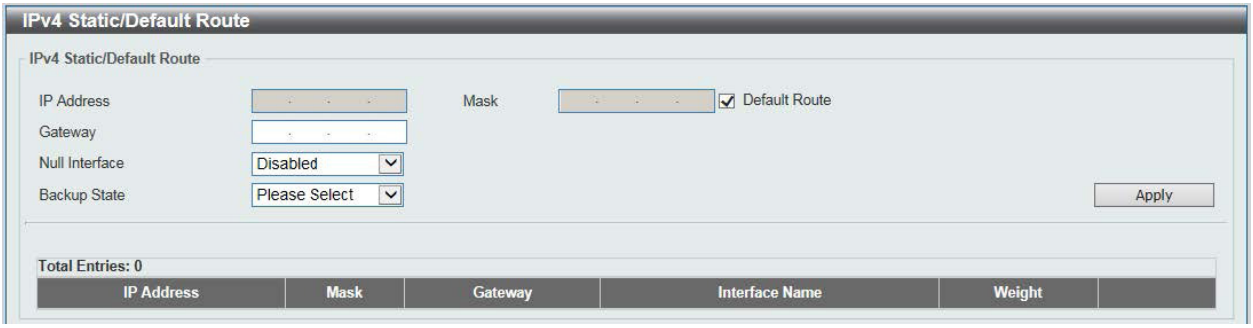


図 9-21　IPv4 Static/Default Route 画面

以下の項目が表示されます。

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」をチェックすると、IPv4 アドレスをデフォルトルートとして使用します。

項目	説明
Mask	対応するサブネットマスクを入力します。
Gateway	対応するゲートウェイ 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。 • 「Weight」-「0」以上かつ最大パス数よりも小さい値を指定します。 本数値はルーティングテーブルのルートパスの複製（複数コピー）に使用され、これによりトラフィックルーティングの際にパスが合致する確率が上がります。スタティックルートに Weight 値が指定されていない場合、パスのデフォルトはハッシュテーブルに存在します。「Weight」選択後に表示される空欄に数値（1-15）を指定します。

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

IPv4 Route Table（IPv4 ルートテーブル）

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。

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 9-22　IPv4 Route Table 画面

以下の項目が表示されます。

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。
RIP	本項目を選択すると、RIP ルートのみを表示します。
OSPF	本項目を選択すると、OSPF ルートのみを表示します。
Connected	接続されたルートのみを表示します。
Summary	ルーティングエントリのサマリを表示します。

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

IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定）

IPv6 アドレス形式のスタティックルートを設定します。

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。

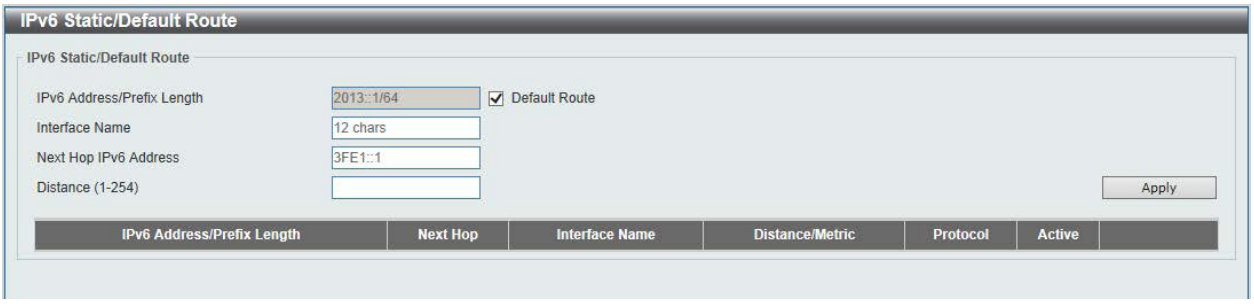


図 9-23　IPv6 Static/Default Route 画面

以下の項目が表示されます。

項目	説明
IPv6 Address/Prefix Length	スタティックルートに割り当てる IPv6 アドレスおよびプレフィックスを入力します。「Default Route」をチェックすると、このルートをデフォルトルートとして使用します。
Interface Name	スタティック IPv6 ルートが作成される IP インタフェース名を指定します。
Next Hop IPv6 Address	ネクストホップに対応する IPv6 アドレスを指定します。
Distance	スタティックルートの管理ディスタンスを指定します。小さい値の方が、より適切なルートを意味します。指定されないと初期値の「1」に設定されます。 • 設定可能範囲：1-254

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

IPv6 Route Table（IPv6 ルートテーブル）

現在の IPv6 ルーティング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。

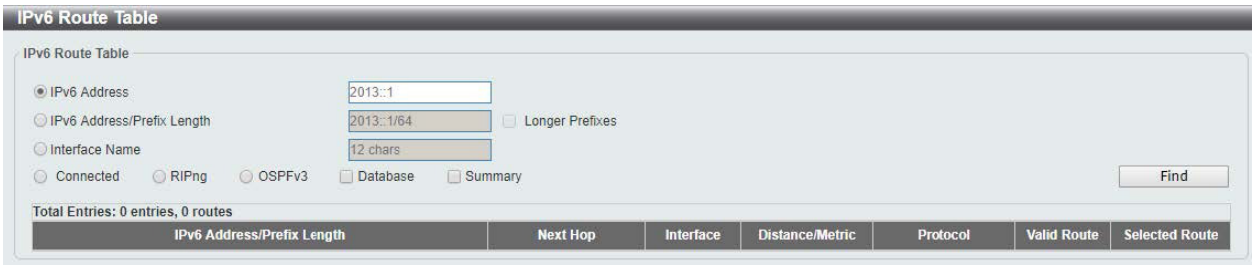


図 9-24　IPv6 Route Table 画面

以下の項目が表示されます。

項目	説明
IPv6 Address	表示するルートの宛先 IPv6 アドレスを指定します。
IPv6 Address/Prefix Length	表示するルートの IPv6 アドレスとプリフィクスを指定します。「Longer Prefixes」を指定するとプリフィクス長と同等、もしくはそれよりも長いプリフィクスの IPv6 ルートを表示します。
Interface Name	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を表示します。
RIPng	RIPng ルートエントリのみを表示します。
OSPFv3	OSPFv3 ルートエントリのみを表示します。
Database	ベストルートに加えて、ルーティングデータベース内の関連するすべてのエントリを表示します。
Summary	ルーティングエントリのサマリを表示します。

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

Route Preference（ルート優先度設定）

ルート優先度を設定します。ルート信頼度レーティングを示すディスタンスを設定します。ルートのディスタンス値が小さいほど優先度が高くなります。ディスタンスの値が 255 の場合、信頼度がないとみなされ、ルーティングパケットに適用されません。

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



図 9-25　Route Preference 画面

以下の項目が設定、表示に使用されます。

項目	説明
Distance Default	デフォルトルートの管理優先度値（ディスタンス）を設定します。 • 設定可能範囲：1-255 • 初期値：1
Distance Static	スタティックデフォルトルート優先度（ディスタンス）を指定します。 • 設定可能範囲：1-255 • 初期値：60

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

ECMP Settings（ECMP 設定）

Equal-Cost Multi-Path (ECMP) ルーティング設定を行います。ロードバランシングハッシュアルゴリズムの設定と、同じ宛先の複数パスエントリに対しネクストホップを決定する際に使用されます。

L3 Features > ECMP Settings をクリックし、以下の画面を表示します。

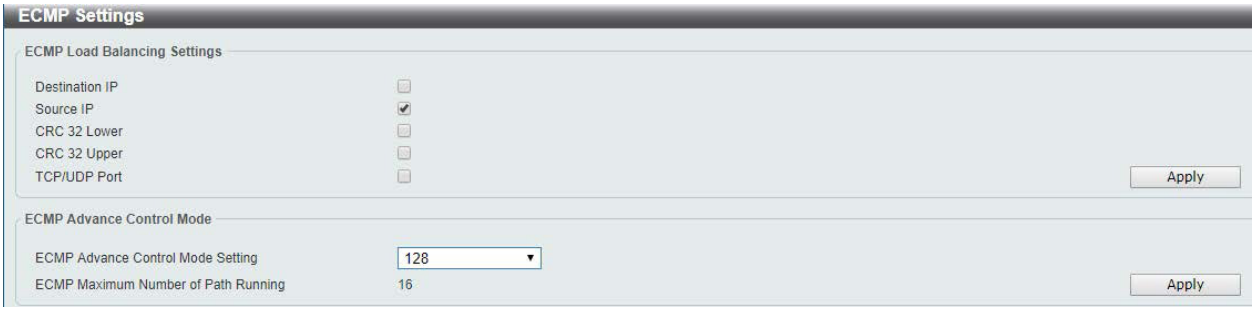


図 9-26　ECMP Settings 画面

以下の項目が使用できます。

項目	説明
ECMP Load Balancing Settings	
Destination IP	ECMP ハッシュ鍵として宛先 IP を使用します。
Source IP	ECMP ハッシュアルゴリズムとして送信元 IP の下位ビットを使用します。
CRC 32 Lower	ECMP ハッシュアルゴリズムとして CRC-32 の下位ビットを使用します。
CRC 32 Upper	ECMP ハッシュアルゴリズムとして CRC-32 の上位ビットを使用します。
TCP/UDP Port	ECMP ハッシュ鍵として TCP または UDP ポート番号を使用します。
ECMP Advance Control Mode	
ECMP Advance Control Mode Setting	ECMP アドバンスコントロールモードの設定を行います。この数値に従って、ECMP またはマルチパスルートの数、各 ECMP またはマルチパスルートのネクストホップ数が変更されます。 • 選択肢：「64」「128」「256」「512」「1024」

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

RIP（Routing Information Protocol）

RIP（Routing Information Protocol）は、距離ベクトル型のルーティングプロトコルです。

補足　本機能は将来のファームウェアでサポート予定です。

RIP Settings（RIP 設定）

IP インタフェースに RIP 設定を行います。

L3 Features > RIP > RIP 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。

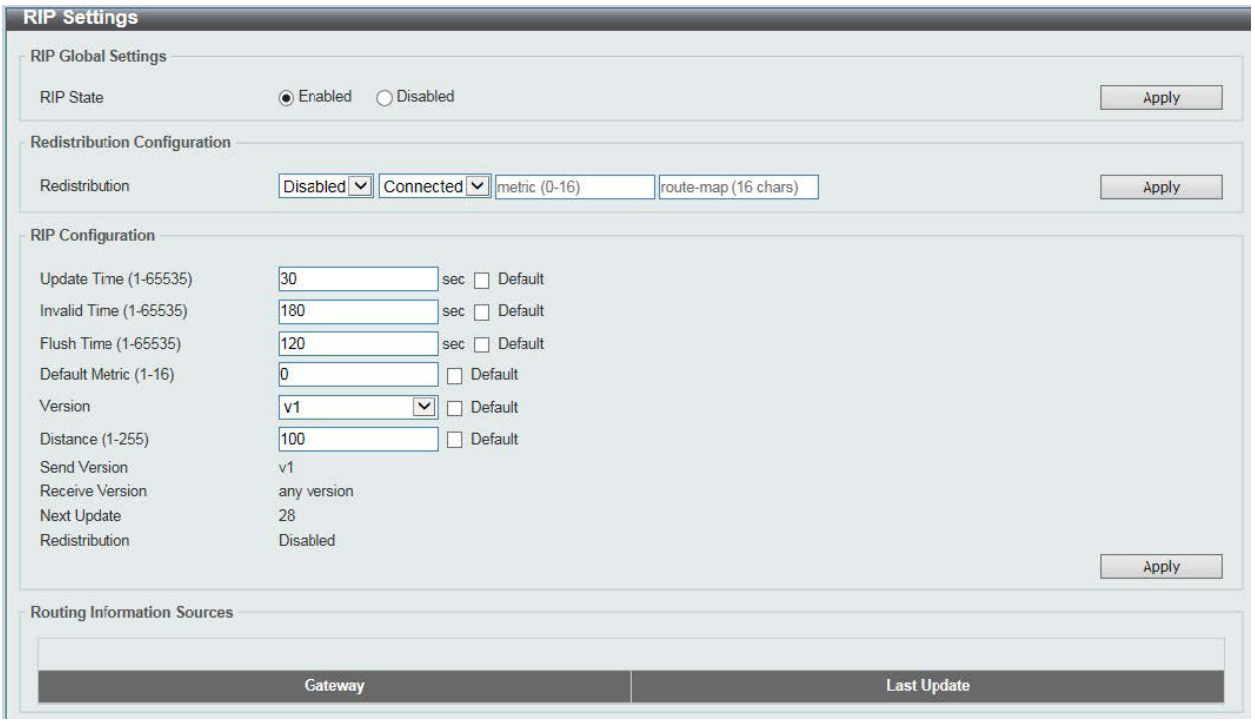


図 9-27　RIP Settings 画面

以下の項目が表示されます。

項目	説明
RIP Global Settings	
RIP State	RIP 機能を有効 / 無効に設定します。
Redistribution Configuration	
Redistribution	次の手順で指定します。 1. RIP redistribution（RIP 再分配）機能を有効 / 無効に設定します。 2. RIP に再分配されるルーティングプロトコル（ドメイン）を指定します。「Connected」「OSPF」「Static」から指定します。「Static」は IP スタティックルートを再分配します。「Connected」はインタフェースの IP アドレス設定の際に自動的に構築するルートを意味します。 3. 再分配ルートのメトリック値（0-16）を指定します。 4. 現在のルートプロトコルに再分配するルートのフィルタリングに使用するためのルートマップ名を指定します。指定されないと全てのルートが再分配されます。
RIP Configuration	
Update Time	RIP アップデートメッセージを送信する間隔を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
Invalid Time	Invalid タイム値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：180（秒）
Flush Time	Flush タイム値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：120（秒）

項目	説明
Default Metric	初期メトリック値を指定します。他のルーティングプロトコルからの再分配ルートで使用される初期メトリック値を指定します。再分配されるルートは他のプロトコルに学習され、RIP との互換性がないメトリックになる場合があります。メトリックの指定により、メトリックを同期します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-16（秒） • 初期値：0（秒）
Version	全インタフェースで初期バージョンとして使用されるグローバル RIP バージョンを指定します。「Default」を指定すると初期値を使用します。初期値では v1/v2 どちらも受信しますが、v1 のみ送信します。 • 選択肢：「v1（RIPv1）」「v2（RIPv2）」
Distance	RIP の管理ディスタンスを指定します。小さい値ほど適切なルートを意味します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-255 • 初期値：100

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

RIP Distribute List（RIP ディストリビュートリスト）

RIP ディストリビュートリストの設定を行います。

L3 Features > RIP > RIP Distribute 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 9-28　RIP Distribute List 画面

以下の項目が表示されます。

項目	説明
ACL Name	アクセスリスト名を入力します。（32 文字以内）
Interface Name	インスタンス名を入力します。（12 文字以内）

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

RIP Interface Settings（RIP インタフェース設定）

RIP インタフェースの設定を行います。

L3 Features > RIP > RIP Interface 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 9-29　RIP Interface Settings 画面

以下の項目が表示されます。

項目	説明
Network	RIP に使用される IPv4 ネットワークアドレスアドレスを指定します。本項目で指定するネットワークのサブネットを持つインタフェースの RIP が有効になります。

項目	説明
Passive Interface	パッシブインタフェースを有効 / 無効に設定します。本機能により、インタフェースのルーティングアップデートの送受信を無効にします。ただし、本インタフェースの他のルータから受信した RIP パケットは、継続して処理されます。パッシブインタフェースの名前（12 文字以内）を表示欄に入力します。「Default」を指定すると全インタフェースに適用されます。

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

エントリの編集
「Edit」をクリックすると、以下の画面が表示されます。



図 9-30　Configure RIP Interface 画面

以下の項目が表示されます。

項目	説明
Send Version	インタフェースで送信する RIP バージョンを選択します。 • 選択肢：「v1（RIPv1）」「v2（RIPv2）」
Receive Version	インタフェースで受信する RIP バージョンを選択します。 • 選択肢：「v1（RIPv1）」「v2（RIPv2）」
Send v2-broadcast	マルチキャストパケットではなくブロードキャストによる RIPv2 アップデート送信を有効／無効に設定します。
Authentication Mode	テキスト認証モードを有効 / 無効に設定します。
Authentication Text Password	認証テキストパスワードを入力します。（16 文字以内）認証モードが有効な場合に設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックして、前の画面に戻ります。

RIP Database（RIP データベース）

本項目では「Routing Information Protocol」(RIP) ルーティングデータベースの設定を行います。子ルートが存在しサマライズ（要約）されている場合、サマリアドレスがデータベース内に表示されます。最後のサマリアドレスの子ルートが無効になると、サマリアドレスはルーティングテーブルから削除されます。

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



図 9-31　RIP Database 画面

以下の項目が表示されます。

項目	説明
Network Address	ネットワークのサブネットプリフィクスとプリフィクス長を指定します。

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

RIPng（RIPng 設定）

スイッチは、RIPng（Routing Information Protocol next generation）をサポートしています。RIPng は、ルートの計算に使用されるルーティング情報を交換する、IPv6 ネットワーク用のルーティングプロトコルです。

補足　本機能は将来のファームウェアでサポート予定です。

RIPng Settings（RIPng 設定）

本画面では、RIPng の設定を行います。

L3 Features > RIPng > RIPng 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。

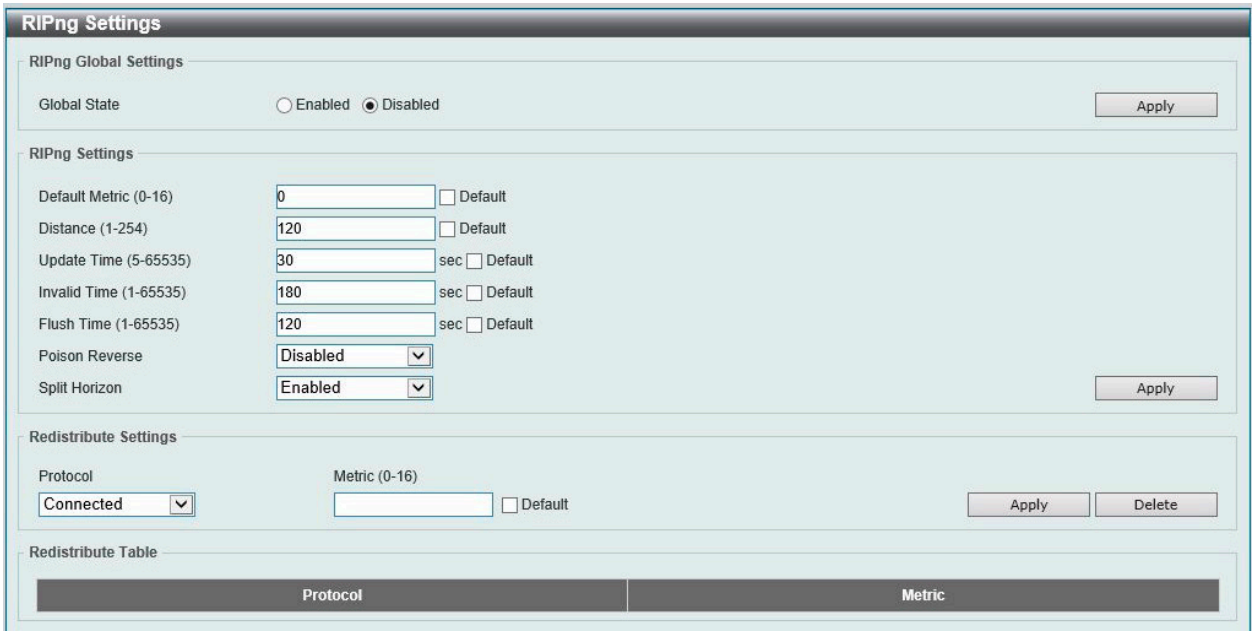


図 9-32　RIPng Settings 画面

以下の項目が表示されます。

項目	説明
RIPng Global Settings	
Global State	RIPng の状態を有効または無効に設定します。 • 初期値：「Disabled」（無効）
RIPng Settings	
Default Metric	初期メトリック値を指定します。他のルーティングプロトコルからの再分配ルートで使用される初期メトリック値を指定します。再分配されるルートは他のプロトコルに学習され、RIPng との互換性がないメトリックになる場合があります。メトリックを再指定することにより、メトリックを同期させることができます。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-16（秒） • 初期値：0（秒）
Distance	RIPng の管理ディスタンスを指定します。これは、ルートの信頼レートを意味します。小さい値ほど優先的なルートを意味します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-254 • 初期値：120
Update Timer	RIP アップデートメッセージを送信する間隔値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：5-65535（秒） • 初期値：30
Invalid Timer	Invalid タイマの値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：180（秒）
Flush Timer	Flush タイマの値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：120（秒）
Poison Reverse	「Poison Reverse」を有効 / 無効に設定します。本機能が有効の場合、インタフェースから学習したルートは不達のメトリックとともに同じインタフェースに通知されます。

項目	説明
Split Horizon	「Split Horizon」を有効 / 無効に設定します。「Split Horizon」が有効の場合、インタフェースから学習したルートは同じインタフェースに通知されません。
Redistribute Settings	
Protocol	RIPng に再分配されるルーティングプロトコル（ドメイン）を指定します。「Static」は IPv6 スタティックルートを再分配します。「Connected」は IPv6 インタフェースの IP アドレス設定の際に自動的に構築するルートを意味します。 • 選択肢：「Connected」「OSPF」「Static」
Metric	再分配されるルートのメトリックとして使用される値を指定します。「Default」は初期メトリック値を使用します。 • 設定可能範囲：0-16

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

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

本画面では、RIPng インタフェースの設定を行います。

L3 Features > RIPng > RIPng 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。

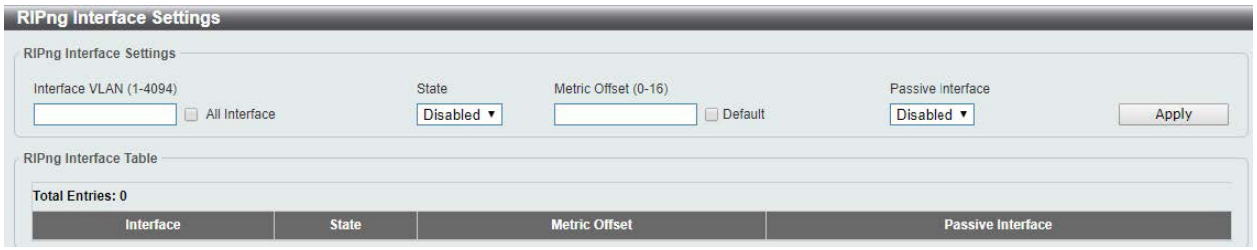


図 9-33　RIPng Interface Settings 画面

以下の項目が表示されます。

項目	説明
Interface VLAN	RIPng 設定の VLAN インタフェース名を入力します。「All Interface」を選択すると、全インタフェースに対して設定を適用します。 • 設定可能範囲：1-4094
State	指定の VLAN インタフェースで IPv6 RIP 機能を有効 / 無効に設定します。
Metric Offset	指定インタフェースで受信する IPv6 RIP ルートのメトリック値に本値を追加します。メトリックはホップカウントを参照します。初期値では、IPv6 RIP ルート受信時に、ルーティングテーブル挿入される前にメトリック値「1」がルートに追加されます。この設定を使用すると、各インタフェースで受信するルートのメトリックおよびルートの優先度を調整することができます。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-16 • 初期値：0
Passive Interface	パッシブインタフェースを有効 / 無効に設定します。本設定が無効になると、ルータはインタフェースを介して RIPng を送信しません。ただし、インタフェースで受信した他のルータからの RIPng パケットは、継続して処理されます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

RIPng Database（RIPng データベース）

本画面では、RIPng データベースの設定を行います。

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



図 9-34　RIPng Database 画面

以下の項目が表示されます。

項目	説明
IPv6 Address/Prefix Length	IPv6 アドレスを入力します。

「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。

OSPF（OSPF 設定）

OSPF の設定を行います。

補足　本機能は将来のファームウェアでサポート予定です。

OSPFv2（OSPFv2 設定）

L3 Features > OSPF > OSPFv2

OSPFv2 Process Settings（OSPF プロセス設定）

OSPFv2 プロセスを設定、表示します。

L3 Features > OSPF > OSPFv2 > OSPFv2 Process 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。

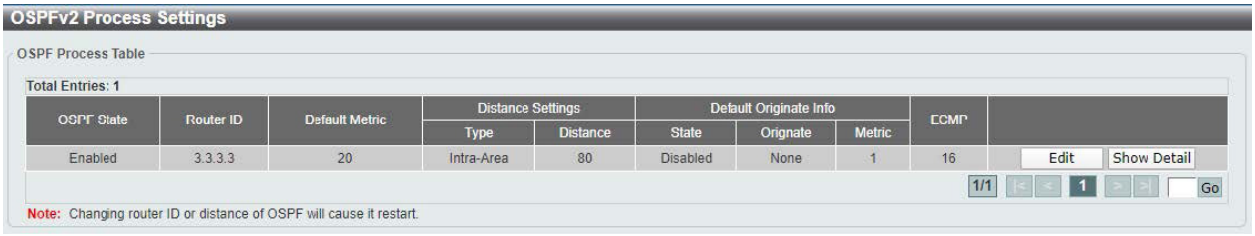


図 9-35　OSPFv2 Process Settings 画面

以下の項目が表示されます。

項目	説明
OSPF State	OSPFv2 機能を有効または無効に設定します。
Router ID	IPv4 アドレス形式でルータ ID を指定します。ルータ ID は、OSPF プロトコルを実行する各ルータにアサインされる 32 ビットの数値であり、AS 内のルータを固有に識別します。AS 内で、各ルータは一意のルータ ID を持ちます。
Default Metric	初期メトリック値を指定します。 • 設定可能範囲：1-16777214
Type	ディスタンス設定の種類を指定します。 • 「Inter-Area」- OSPF インターエリアルートのディスタンスを指定します。 • 「Intra-Area」- OSPF イントラエリアルートのディスタンスを指定します。 • 「External-1」-「type-1」のメトリックで、OSPF「external type-5」および「type-7」ルートのディスタンスを指定します。 • 「External-2」-「type-2」メトリックで、OSPF「external type-5」および「type-7」ルートのディスタンスを指定します。
Distance	管理ディスタンス値を指定します。 • 設定可能範囲：1-255
State	初期「Originate」情報を有効 / 無効に設定します。AS に向かう初期外部ルート (type-5 LSA) ネットワーク「0.0.0.0」の生成に使用されます。

項目	説明
Originate	「Originate」のオプションを指定します。「Always」を指定すると、再分配されたルート内にデフォルトルートが存在していても、常にデフォルトルートを生成し続けます。 • 選択肢：「Always」「None」
Metric	生成されたデフォルトルートにかかるコストを入力します。指定されないと初期メトリックは「1」になります。 • 設定可能範囲：1-65535

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「Apply」ボタンをクリックして設定内容を適用します。
「Show All」ボタンをクリックして、テーブル上のすべてのエントリを表示します。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

詳細情報の表示

「Show Detail」をクリックすると、以下の画面が表示されます。

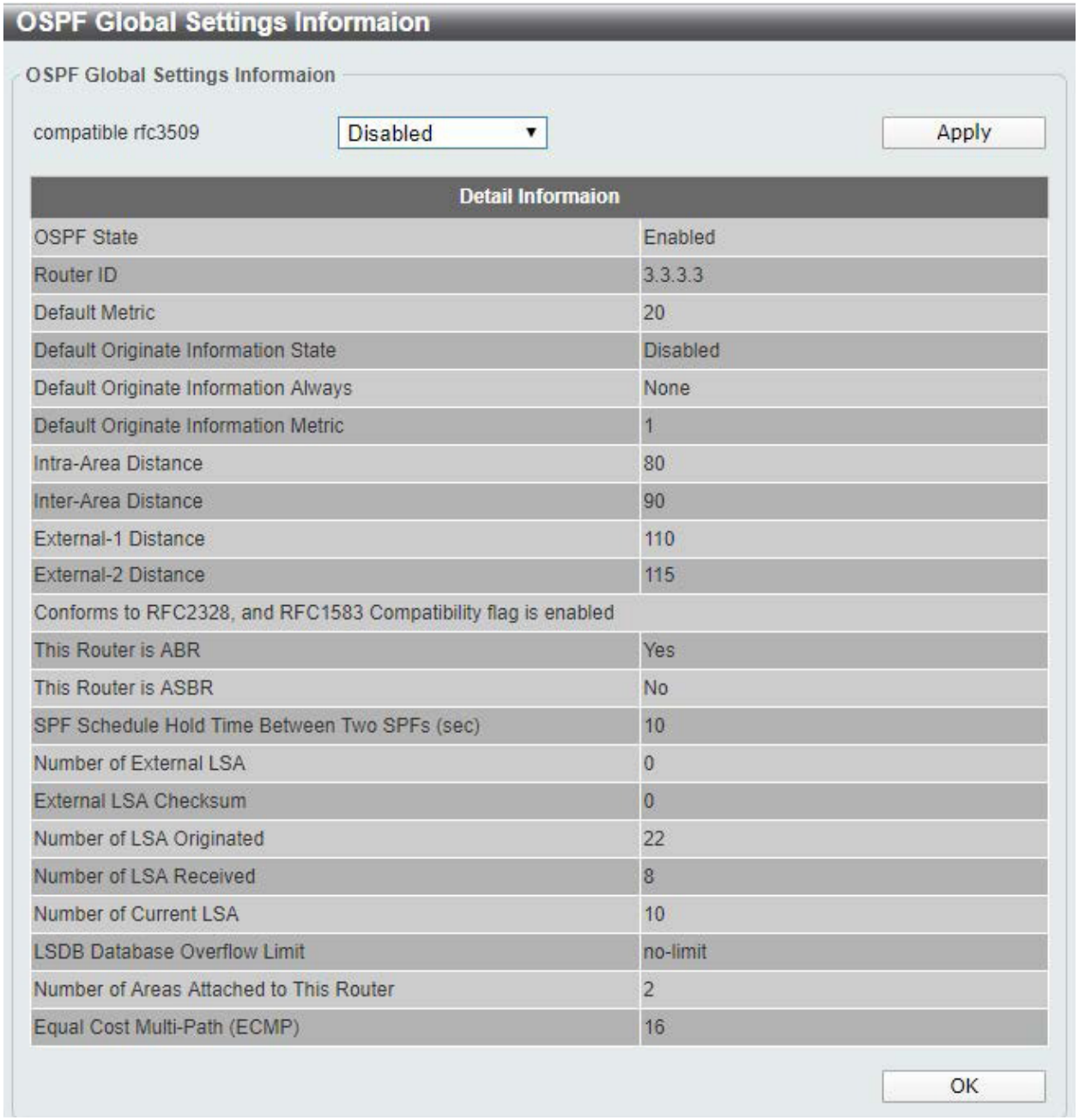


図 9-36　OSPFv2 Process Settings (Show Detail) 画面

以下の項目が表示されます。

項目	説明
Compatible RFC3509	Area Border Router (ABR) の実行を有効 / 無効に設定します。「RFC 3509」で定義されています。

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

OSPFv2 Distribute List（OSPFv2 ディストリビュートリスト）

OSPFv2 ディストリビュートリストの設定、表示を行います。

L3 Features > OSPF > OSPFv2 > OSPFv2 Distribute 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。

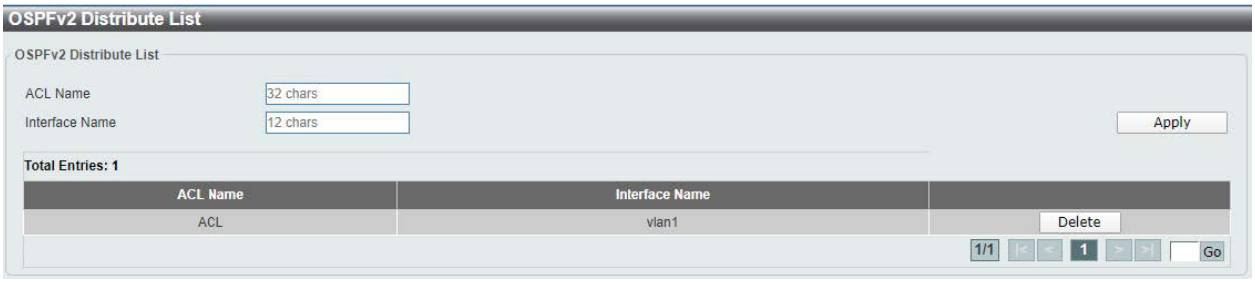


図 9-37　OSPFv2 Distribute List 画面

以下の項目が表示されます。

項目	説明
ACL Name	アクセスリスト名を入力します。（32 文字以内）
Interface Name	インタフェース名を入力します。（12 文字以内）

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

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

OSPFv2 GR Helper Settings（OSPFv2 GR ヘルパー設定）

OSPFv2 グレースフルリスタート（GR）ヘルパーの設定、表示を行います。

L3 Features > OSPF > OSPFv2 > OSPFv2 GR Helper 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 9-38　OSPFv2 GR Helper Settings 画面

以下の項目が表示されます。

項目	説明
Graceful Restart Helper	グレースフルリスタートヘルパーモードを指定します。 • 「Unspec」- OSPF グレースフルリスタートヘルパーモードが設定されません。 • 「Never」- OSPF グレースフルリスタートヘルパーモードを許可しません。 • 「Only Reload」- OSPF グレースフルリスタートヘルパーモードをリロード時のみ許可します。
Max Grace Period	最大グレース期間を指定します。 • 設定可能範囲：1-1800（秒）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

OSPFv2 Passive Interface Settings（OSPF パッシブインタフェース設定）

OSPFv2 パッシブインタフェースの設定、表示を行います。

L3 Features > OSPF > OSPFv2 > OSPFv2 Passive 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 9-39　OSPFv2 Passive Interface Settings 画面

以下の項目が表示されます。

項目	説明
Interface Name	使用するインタフェース名を指定します。（12 文字以内）「Default」を選択すると全ての有効なインタフェースを指定します。

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

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

OSPFv2 Area Settings（OSPFv2 エリア設定）

本項目では OSPFv2 エリア設定を行います。

L3 Features > OSPF > OSPFv2 > OSPFv2 Area 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。

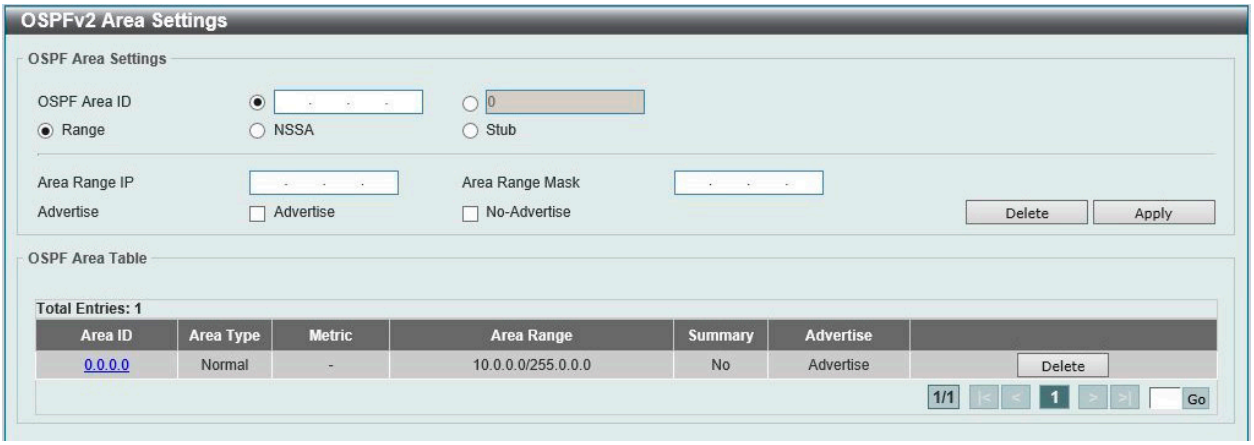


図 9-40　OSPFv2 Area Settings 画面

以下の項目が表示されます。

項目	説明
Area ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) または、10 進数（0-4294967295）を指定します。このエリアはインタフェースに設定されたサブネットが指定のネットワーク範囲で落ちた場合に、当該のインタフェースで作成されます。
Range	Area Border Router (ABR) の OSPF ルートをサマライズします。
NSSA	Not-So-Stubby Area (NSSA) として OSPF エリアをアサインします。
Stub	Stub エリアとして OSPF エリアを設定します。
Area Range IP	「Range」が選択されている場合、OSPF エリア範囲の IP アドレスを入力します。
Area Range Mask	「Range」が選択されている場合、OSPF エリア範囲のサブネットマスクを入力します。
Advertise	「Range」が選択されている場合、通知（Advertise）オプションを設定します。 • 「Advertise」- 指定範囲のアドレスの「Type-3 summary Link-State Advertisement (LSA)」を通知します。 • 「No-Advertise」-「Type-3 summary LSA」の通知を抑制します。コンポーネントのルートは存在しています。

項目	説明
Metric	「NSSA」または「Stub」選択時に有効です。「stub」エリアと「no-so-stubby」エリアに挿入される「Type-3」初期ルートに関連するメトリックを指定します。 • 設定可能範囲：0-65535 - 「Default Metric」- 初期コスト値を指定します。 - 「No-Summary」- 本エリアにサマリルートを挿入しません。

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

詳細設定の表示

「Area ID」のリンク（0.0.0.0）をクリックすると、以下の画面が表示されます。

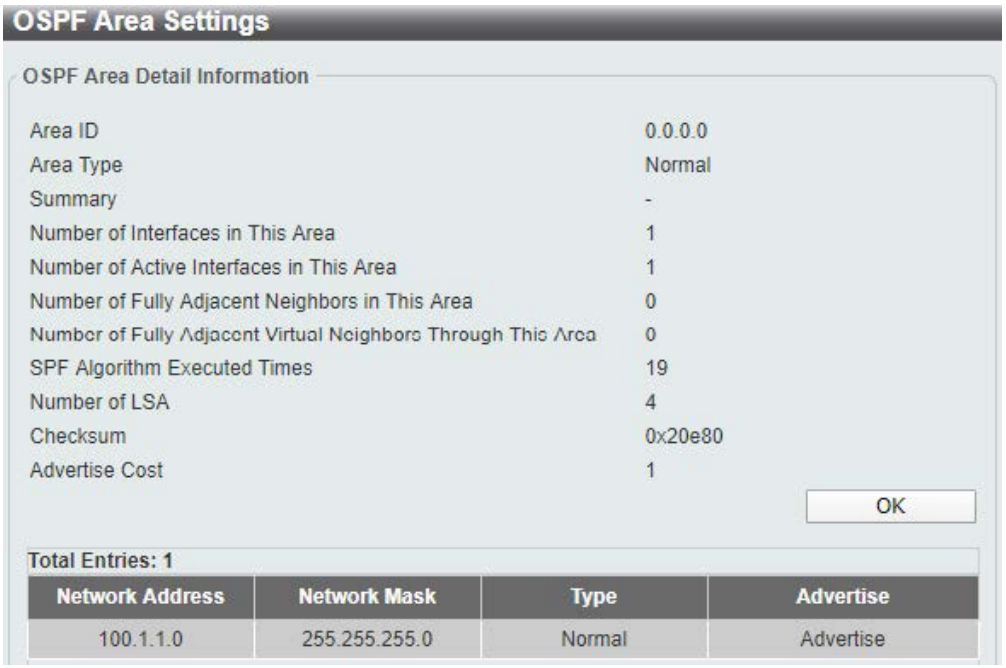


図 9-41　OSPFv2 Area Settings（Area ID）画面

「OK」ボタンをクリックして画面を閉じます。

OSPFv2 Interface Settings（OSPFv2 インタフェース設定）

スイッチの OSPFv2 インタフェースを設定します。

L3 Features > OSPF > OSPFv2 > OSPFv2 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 9-42　OSPFv2 Interface Settings 画面

以下の項目が表示されます。

項目	説明
OSPF Interface Settings	
Area ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) または、10 進数（0-4294967295）を指定します。
Network IP Address	IPv4 アドレスを指定します。

項目	説明
Network Mask	IPv4 サブネットマスクを指定します。
OSPF Interface Table	
Interface Name	インタフェース名を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「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。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Delete」ボタンをクリックして、エントリを削除します。

詳細情報の表示
「Show Detail」ボタンをクリックして、以下の画面を表示します。

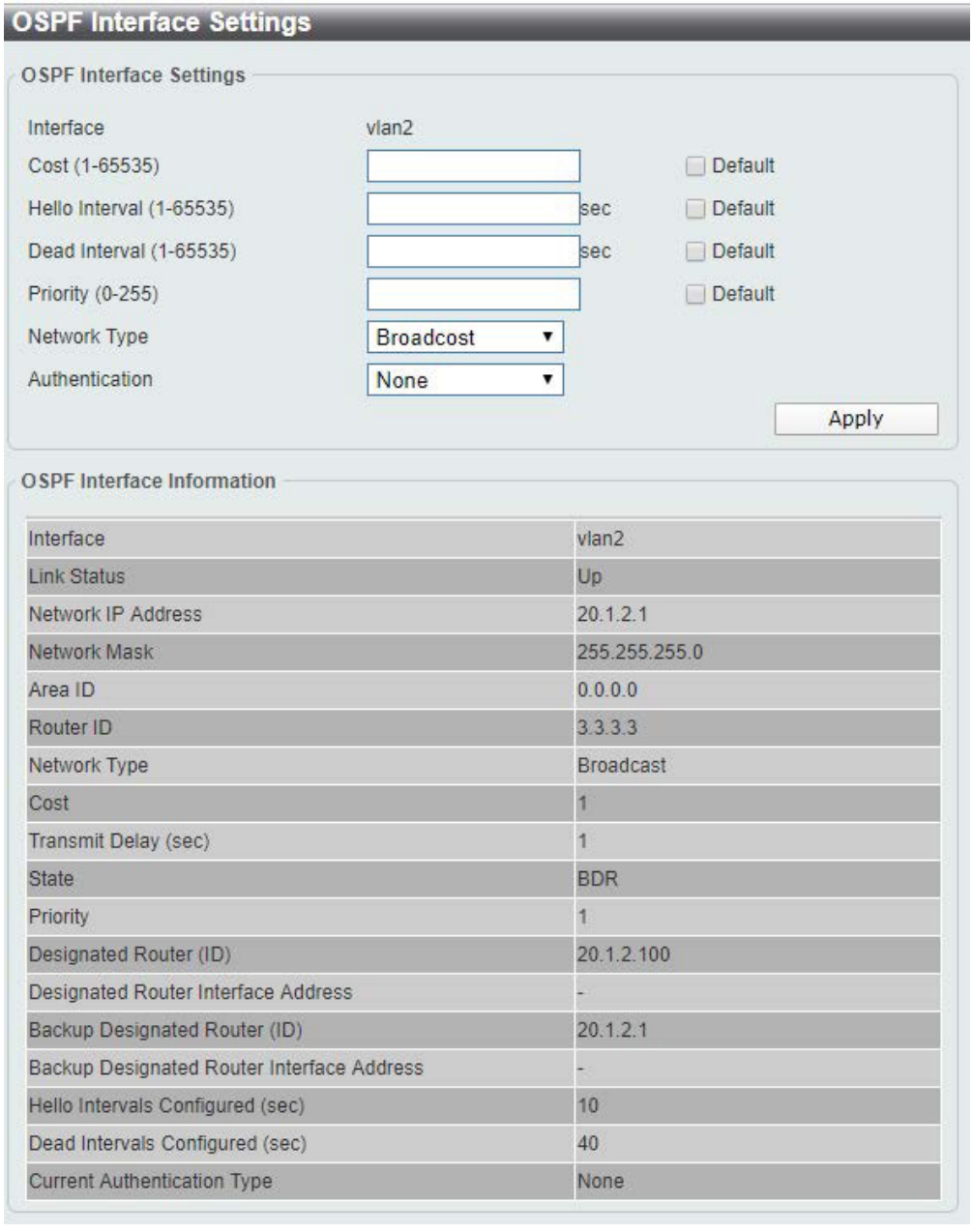


図 9-43　OSPFv2 Interface Settings (Show Detail) 画面

以下の項目が表示されます。

項目	説明
Cost	コストの値を指定します。インタフェースのコストはインタフェース内のパケット送信のオーバーヘッドに反映されます。コストはルータリンク通知の中でリンクコストとして通知されます。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535 • 初期値：1

項目	説明
Hello Interval	OSPF Hello パケットの送出間隔を指定します。Hello Interval は Hello パケット内で通知されます。ネットワーク内のすべてのルータに対し、同じ Hello Interval を設定してください。この間隔が短いと、トポロジ変更の検知が早くなりますが、ルーティングトラフィックが増加し、ルートの不安定さを招く恐れがあります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead Interval	隣接ルータが Hello パケットを最後に受信してから、送信側のルータがダウンしたと判断するまでの時間を指定します。本値には Hello Interval の倍数を指定します。この値は Hello パケット内で通知されます。ネットワーク内のすべてのルータに対し、同じ Dead Interval を設定してください。この間隔が短いと、トポロジ変更の検知が早くなりますが、ルーティングトラフィックが増加し、ルートの不安定さを招く恐れがあります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
Priority	代表ルータ選出のプライオリティを指定します。OSPF ルータは、マルチアクセスネットワークにおいて代表ルータを選出します。2 台のルータが代表ルータになろうとしている場合、高いプライオリティのルータが選出されます。同じプライオリティ値を持つ場合は、ルータ ID の高い方が優先されます。「0」の場合は代表ルータまたはバックアップ代表ルータとして選出されません。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-255 • 初期値：1
Network Type	ネットワークタイプを指定します。 • Broadcast - ネットワークタイプをブロードキャストとして指定します。 • Point-to-Point - ネットワークタイプを「point-to-point」として指定します。 ブロードキャストネットワークでは「DR」と「BDR」のみが他の全てのルータのネイバになることが可能です。「point-to-point」ネットワークでは、通信可能な 2 ルータのみがネイバになることが可能です。
Authentication	認証方法を選択します。 • 選択肢：「None」「Simple Password」「MD5」
Password	「Authentication」で「Simple Password」を選択した場合、シンプルテキストのパスワードを入力します。（8 文字以内）パスワードにはスペースを含めることはできません。 このパスワード情報は、ルータがルーティングプロトコルパケットを送信する際の OSPF ヘッダに挿入されます。各インタフェースのそれぞれのネットワークに対し、パスワードを設定します。同じネットワーク上のルータには同じパスワードを設定し、OSPF ルーティングデータが交換できるようにします。同じルーティングドメインのルータには同じパスワードを設定してください。
MD5 Key ID	MD5 暗号キー ID を入力します。 • 設定可能範囲：1-255
MD5	MD5 キーを指定します。（16 文字以内）スペースなしのアルファベット文字列で指定します。 MD5 モードでは OSPF メッセージ送信者は送信メッセージのメッセージダイジェストキーを元にメッセージのダイジェストを解析します。メッセージダイジェストとキー ID はパケット内でエンコードされます。パケットの受信者は、同じキー ID に関連するローカル定義されたメッセージダイジェストキーを元に、メッセージ中のダイジェストを検証します。 同じインタフェースのネイバルータに対しては同じキーを設定し、お互いに OSPF パケットが交換できるようにします。通常、同じインタフェースのすべてのネイバルータは同じキーを使用します。 MD5 ダイジェストモードでは、現在のメッセージ交換を中断することなく、ユーザーは新しいキーにロールオーバーできます。 ルータが古いキーを使用して隣接ルータと OSPF パケットを交換している処理中の場合、ユーザが新しいキーを設定すると、ルータは古いキーと新しいキーの両方に重複したパケットを送信し、ロールオーバープロセスを開始します。ネットワーク上のすべてのルータが新しいキーを学習するまで、重複したパケットが送信されます。 ロールオーバープロセスが完了した後、ユーザは古いキーを削除して、ルータが古いキーを使用してルータと通信できないようにする必要があります。

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

OSPFv2 Redistribute Settings（OSPFv2 再分配設定）

本項目では OSPFv2 再分配（redistribution）について、設定、表示します。外部ルートは ASBR により、「Type-5」外部ルートとしてノーマルエリアに、「Type-7」外部ルートとして NSSA スタブエリアに再分配されます。
再分配外部ルートが「Type-1」の場合、メトリックはインターナルメトリックを意味します。再分配外部ルートが「Type-2」の場合、メトリックは外部メトリックを意味します。内部メトリックは、ルータ自身から再分配ルータまでのコストと、宛先に到達するためにアドバタイズされたコストを考慮します。外部メトリックは、宛先に到達するためにアドバタイズされたメトリックのみを認識します。メトリックが初期メトリックとして設定されていない場合、他のプロトコルから再分配されたルートがメトリック値 20 を取得します。

L3 Features > OSPF > OSPFv2 > OSPFv2 Redistribute 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 9-44　OSPFv2 Redistribute Settings 画面

以下の項目が表示されます。

項目	説明
Protocol	再分配される送信元プロトコルを指定します。OSPF のようなルーティングプロトコルの場合、自律システムに外部として再分配されます。 • 選択肢：「Connected」「Static」「RIP」
Metric Type	メトリックの種類を指定します。OSPF ルーティングドメインに再分配されるルートの外部リンクタイプを指定します。メトリックタイプが指定されていないと、スイッチは「Type-2」外部ルートを採用します。 • 選択肢：「External Type-1」「External Type-2」
Metric	再分配ルートのメトリックを指定します。 • 設定可能範囲：1-16777214
Router Map Name	送信元ルーティングプロトコルからインポートされたルートをフィルタするルートマップ名を指定します。 指定されない場合、全ルートが再分配されます。

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

OSPFv2 Virtual Link Settings（OSPFv2 仮想リンク設定）

本項目では OSPFv2 仮想リンク設定を行います。「non-zero」エリアが物理的にゼロエリアと接続していない場合、仮想リンクを通じて必ず接続される必要があります。仮想リンクは「point-to-point」リンクです、ルータは OSPF メッセージをユニキャスト IP パケットとしてネイバルータに送信します。

L3 Features > OSPF > OSPFv2 > OSPFv2 Virtual Link 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。

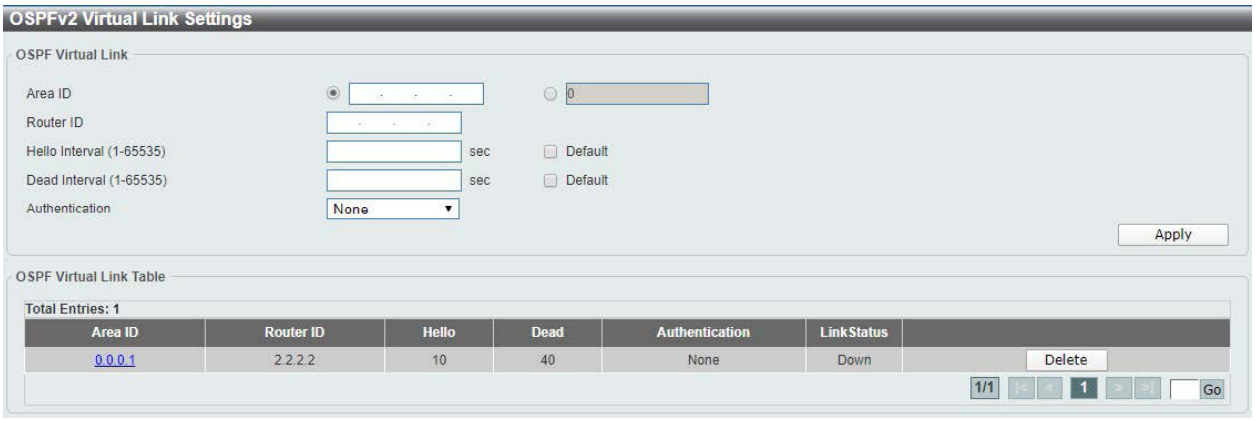


図 9-45　OSPF Virtual Link Settings 画面

以下の項目が表示されます。

項目	説明
OSPF Virtual Link	
Area ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) または、10 進数（0-4294967295）を指定します。このエリアは仮想リンクを確立するために使用されます。
Router ID	仮想リンクネイバのリモード ID を入力します。
Hello Interval	仮想リンクにおける Hello パケットの送出間隔を指定します。「Default」オプションにチェックを入れると、。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead Interval	Hello パケットを最後に受信してから、ネイバがオフラインになったと判断するまでの時間（秒）を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
Authentication	使用する認証を選択します。 • 選択肢：「None」「Simple Password」「MD5」
Password	「Authentication」で「Simple Password」を選択した場合、シンプルテキストのパスワードを入力します。（8 文字以内）
MD5 Key ID	「Authentication」で「MD5」を選択した場合、MD5 暗号キー ID を入力します。 • 設定可能範囲：1-255
MD5	「Authentication」で「MD5」を選択した場合、MD5 キーを指定します。（16 文字以内）スペースなしのアルファベット文字列で指定してください。

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

詳細情報の表示

「Area ID」のリンク（0.0.0.1）をクリックすると、以下の画面が表示されます。

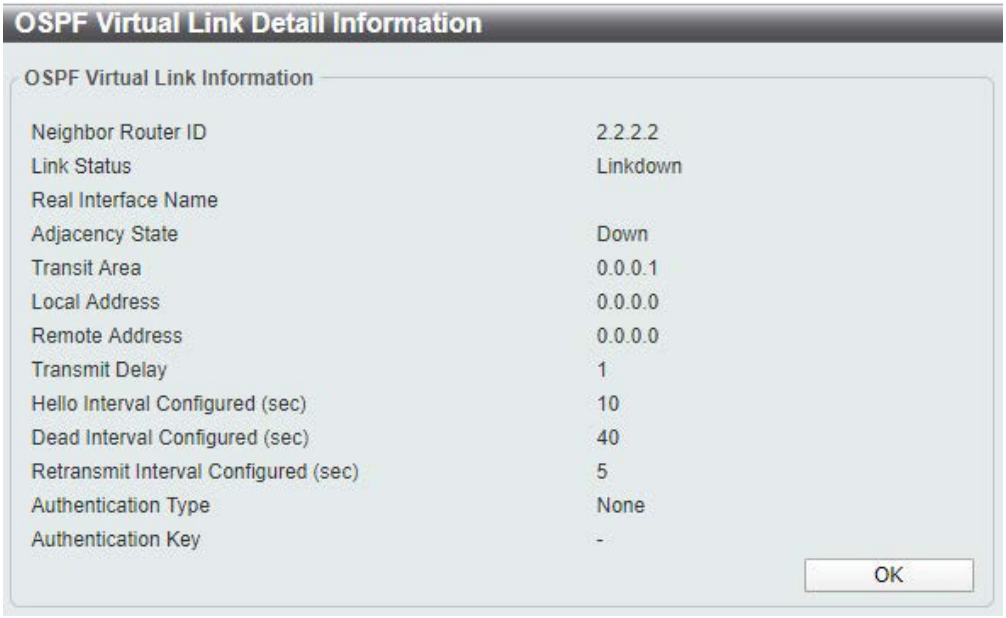


図 9-46　OSPFv2 Virtual Link Settings (0.0.0.1) 画面

OSPFv2 LSDB Table（OSPFv2 LSDB テーブル）

OSPFv2 Link State Database(LSDB) を表示します。

L3 Features > OSPF > OSPFv2 > OSPF LSDB 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。

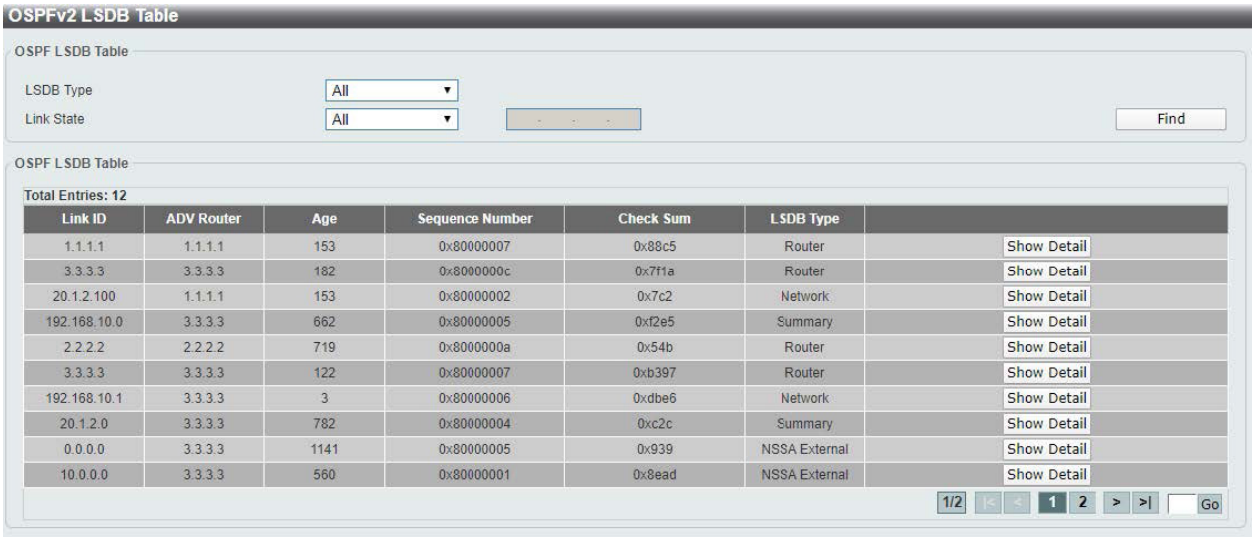


図 9-47　OSPFv2 LSDB Table Settings 画面

以下の項目が表示されます。

項目	説明
LSDB Type	表示する LSDB タイプを指定します。 • 選択肢：「All」「Router」「Network」「Summary」「ASBR Summary」「External」「Stub」「NSSA External」
Link State	表示するリンクステート情報を選択します。 • 「All」- 全ての「OSPFv2」リンクステート情報を表示します。 • 「Link State ID」- 指定するリンクステート ID に関する情報を表示します。表示される欄にリンクステート ID を入力します。 • 「Self Originate」- ローカルルータによって生成された LSA を表示します。 • 「Adv Router」- 通知ルータによって生成された全ての LSA を表示します。通知ルータ ID を空欄に入力します。

「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。

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

OSPFv2 LSDB の詳細表示

「Show Detail」リンクをクリックすると、以下の画面が表示されます。

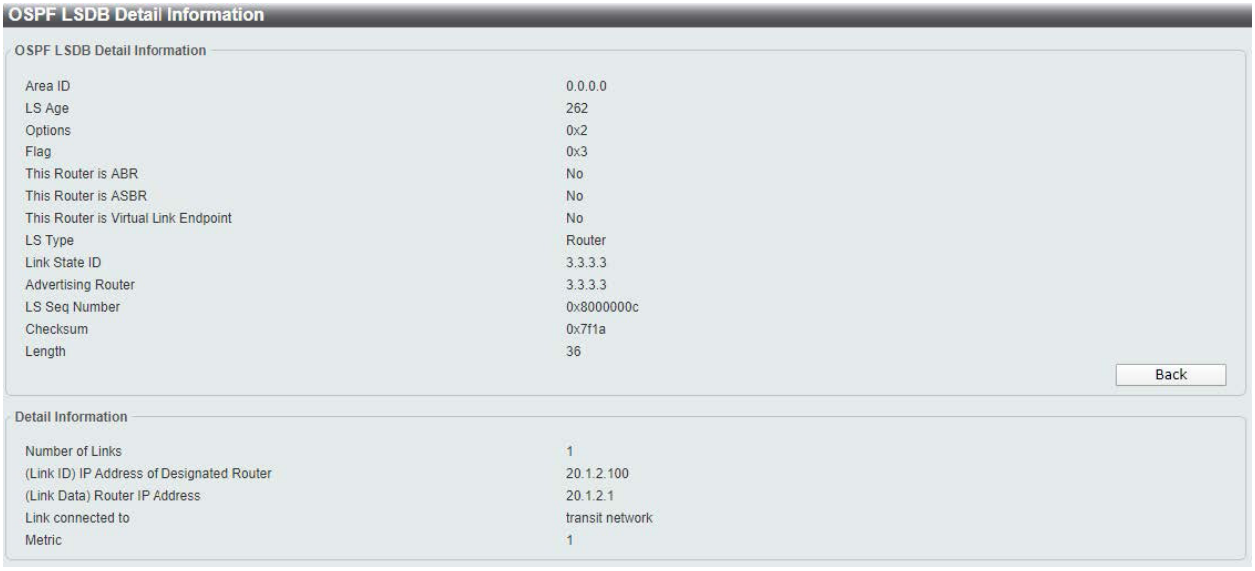


図 9-48　OSPFv2 LSDB Table 画面（Show Detail）

「Back」をボタンをクリックして前のページに戻ります。

OSPFv2 Neighbor Table（OSPF Neighbor テーブル）

インタフェースごとに OSPF-Neighbor 情報を表示します。

L3 Features > OSPF > OSPFv2 > OSPF Neighbor 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。

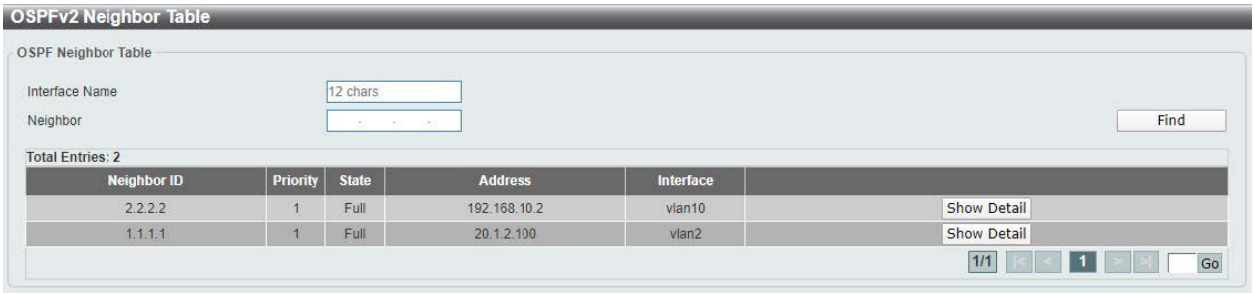


図 9-49　OSPFv2 Neighbor Table 画面

以下の項目が表示されます。

項目	説明
Interface Name	表示するインタフェース名を指定します。
Neighbor	Neighbor ルータの ID を入力します。

「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。

詳細情報の表示

「Show Detail」リンクをクリックすると、以下の画面が表示されます。



図 9-50　OSPFv2 Neighbor Table 画面（Show Detail）

「Back」をボタンをクリックして前のページに戻ります。

OSPFv2 Host Router Settings（OSPFv2 ホストルータ設定）

OSPFv2 ホスト経路設定を行います。ルータは Stub リンクに対し、ルータ LSA として特定のホストルートを通知します。

L3 Features > OSPF > OSPFv2 > OSPFv2 Host Route 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。

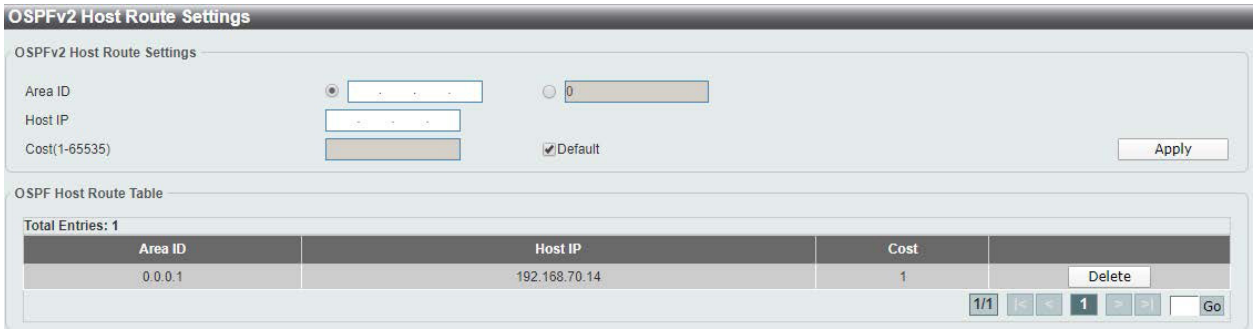


図 9-51　OSPFv2 Host Route Settings 画面

以下の項目が表示されます。

項目	説明
OSPFv2 Host Route Settings	
Area ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号 (IP アドレスと同じ xxx.xxx.xxx.xxx 形式) または、10 進数（0-4294967295）を指定します。
Host IP	使用するホストの IP アドレスを指定します。
Cost	スタブエントリのコスト (1-65535) を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535 • 初期値：1

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

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

OSPFv3

OSPFv3 Process Settings（OSPFv3 プロセス設定）

スイッチに OSPFv3 プロセス設定を行います。

L3 Features > OSPF > OSPFv3 > OSPFv3 Process 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。

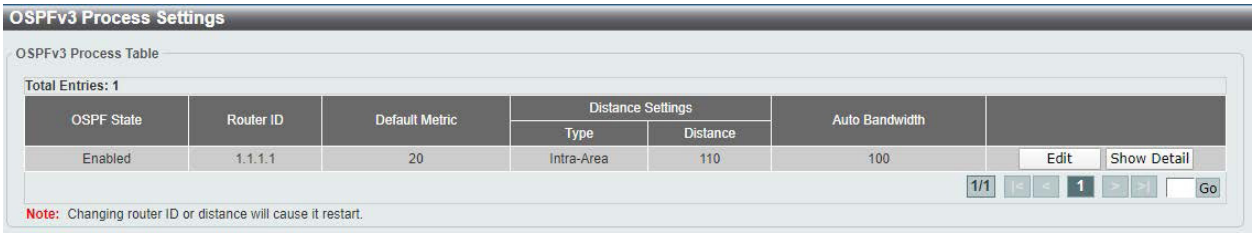


図 9-52　OSPFv3 Process Settings 画面

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

エントリの編集

「Edit」をクリックすると、以下の画面が表示されます。



図 9-53　OSPFv3 Process Settings (Edit) 画面

以下の項目が表示されます。

項目	説明
OSPF State	OSPFv3 ステータスを有効 / 無効に設定します。
Router ID	OSPF プロセスのルータ ID を入力します。
Default Metric	OSPF プロセスの初期メトリック値を指定します。この設定は、OSPFv3 再分配機能とともに使用され、現在のルーティングプロトコルを有効化してすべての再分配ルートに同じメトリック値を使用します。整合性のないメトリックを持つルートの再分配を行う場合、初期メトリックが役に立ちます。メトリックの直接変換ができない場合に、初期メトリックにより再分配が実行されます。 • 設定可能範囲：1-16777214 • 初期値：20
Type	ディスタンス設定種類を指定します。 • 「Inter-Area」- OSPF インターエリアルートのディスタンスを指定します。 • 「Intra-Area」- OSPF イントラエリアルートのディスタンスを指定します。 • 「External-1」- OSPF エクスターナルルート 1 のディスタンスを指定します。 • 「External-2」- OSPF エクスターナルルート 2 のディスタンスを指定します。
Distance	OSPF プロセスのディスタンス値を指定します。 • 設定可能範囲：1-254 • 初期値：110（全ての OSPF ルート）
Auto Bandwidth	自動帯域の値を指定します。インタフェースのメトリックの計算時に IPv6 OSPF が使用する参照値を制御します。 • 設定可能範囲：1-4294967

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

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

詳細情報の表示

「Show Detail」をクリックすると次の画面が表示されます。

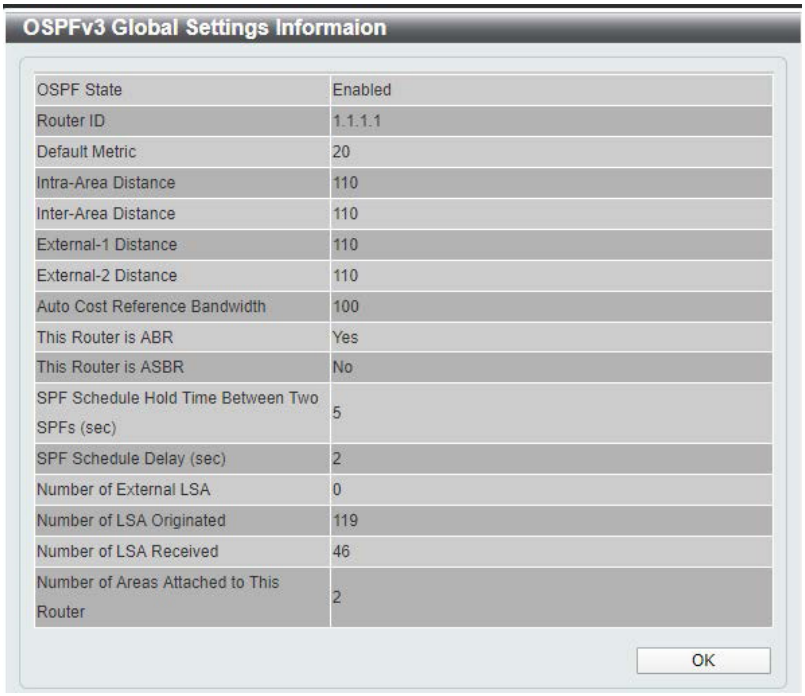


図 9-54　OSPFv3 Process Settings (Show Detail) 画面

「OK」ボタンをクリックして画面を閉じます。

OSPFv3 Passive Interface Settings（OSPFv3 パッシブインタフェース設定）

スイッチに OSPFv3 パッシブインタフェース設定を行います。インタフェースがパッシブ（受動）の場合、OSPF ルーティングアップデートパケットは指定のインタフェースを通じて送受信がされなくなります。

L3 Features > OSPF > OSPFv3 > OSPFv3 Passive 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。

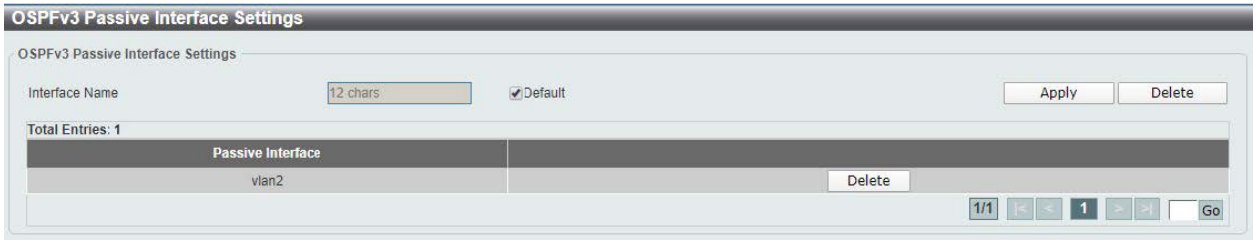


図 9-55　OSPFv3 Passive Interface Settings 画面

以下の項目が表示されます。

項目	説明
Interface Name	パッシブインタフェース名を指定します。(12 文字以内)「Default」を選択すると全てのインタフェースをパッシブインタフェースとして指定します。

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

「Delete」ボタンをクリックして、エントリを削除します。

OSPFv3 Area Settings（OSPFv3 エリア設定）

スイッチに OSPFv3 エリア設定を行います。

L3 Features > OSPF > OSPFv3 > OSPFv3 Area 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。

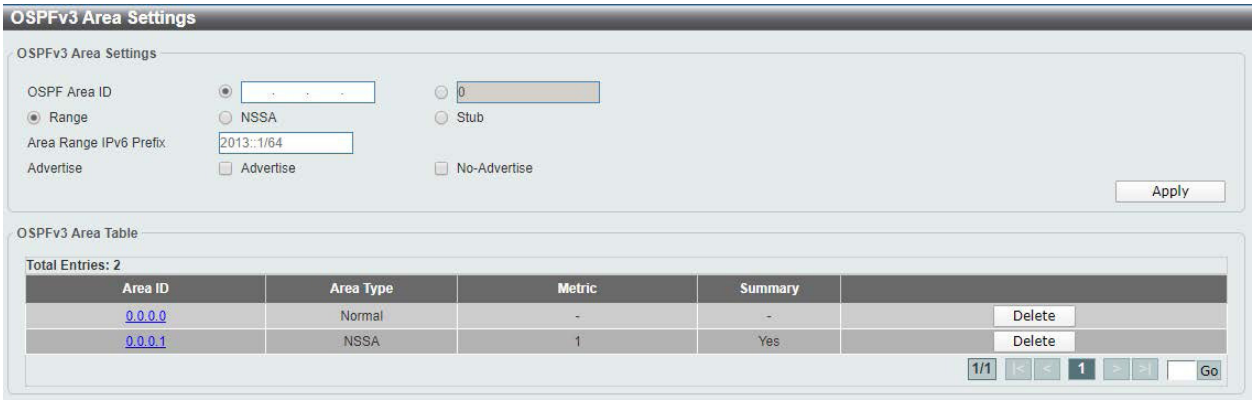


図 9-56　OSPFv3 Area Settings 画面

以下の項目が表示されます。

項目	説明
OSPFv3 Area Settings	
OSPF Area ID	OSPFv3 エリアの ID を指定します。IPv4 アドレス形式または 10 進数（0-4294967295）で入力します。
Range	Area Border Router (ABR) においてOSPFルートを集約します。ABRによって、1 つのサマリルートが他のエリアに通知されます。ルーティング情報はエリア境界で要約されます。エリアの外部に対しては、各アドレス範囲に対して 1 つのルートが通知されます。
NSSA	OSPF エリアを Not-So-Stubby Area（NSSA）エリアとして割り当てます。
Stub	OSPF エリアをスタブエリアとして定義します。
Area Range IPv6 Prefix	「Range」を指定後、OSPF エリア範囲 IPv6 プリフィクスとプリフィクス長を指定します。
Advertise	通知（Advertise）オプションを指定します。 • 「Advertise」- 指定アドレス範囲の「inter-area prefix Link-State Advertisement (LSA)」を通知します。 • 「No-Advertise」- 指定アドレス範囲に対し、「Do-Not-Advertise」を設定します。「inter-area prefix LSA」の通知を抑制します。コンポーネントネットワークは他のネットワークから認識されない状態のままです。
Metric	「NSSA」または「Stub」オプションを選択した場合、OSPFv3 スタブエリアのメトリックを指定します。「Default Metric」を選択するとエリアの初期メトリック値（1）を使用します。「No-Summary」を選択すると、ABR がスタブエリアに inter-area prefix LSA を送信することを防止します。 • 設定可能範囲：0-65535

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。
各タイプの「Area ID」のリンク（0.0.0.1）をクリックすると、詳細情報を表示することができます。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

NSSA タイプの「Area ID」のリンク（0.0.0.1）をクリックすると、以下の画面が表示されます。

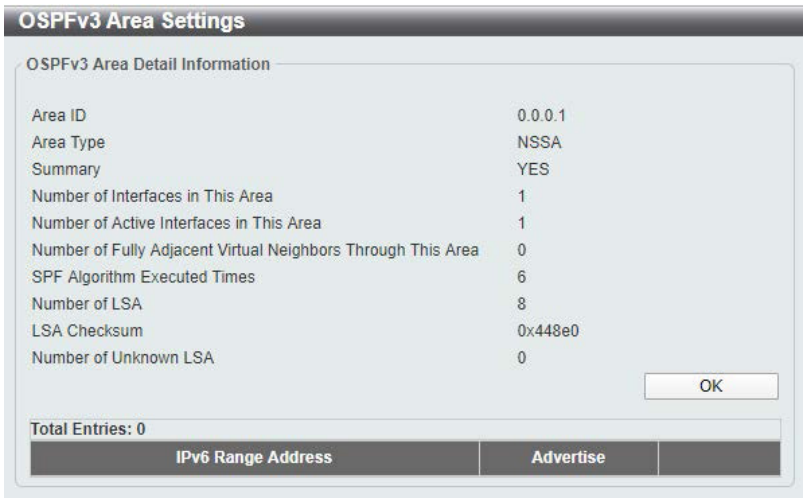


図 9-57　OSPFv3 Area Settings 画面 - NSSA

「OK」ボタンをクリックして画面を閉じます。

Normal タイプの「Area ID」のリンク（0.0.0.1）をクリックすると、以下の画面が表示されます。

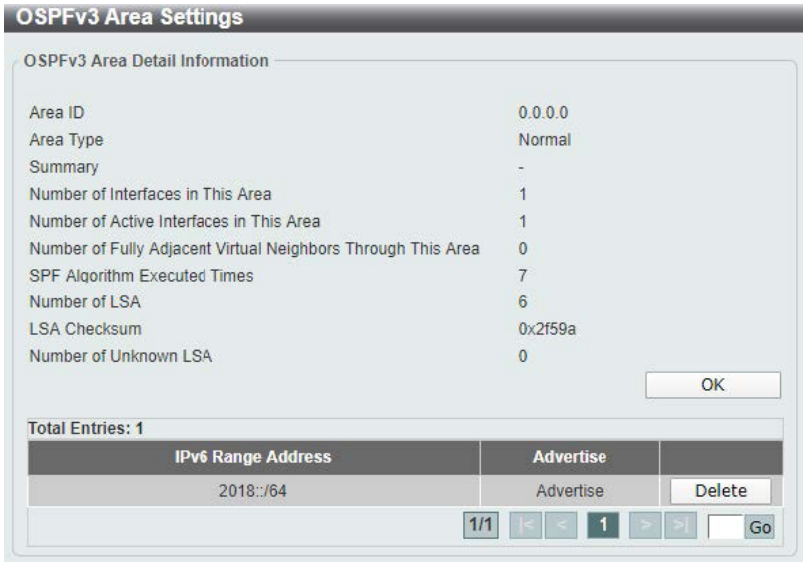


図 9-58　OSPFv3 Area Settings 画面 - Normal

「OK」ボタンをクリックして画面を閉じます。
「Delete」ボタンをクリックして、エントリを削除します。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

OSPFv3 Interface Settings（OSPFv3 インタフェース設定）

OSPFv3 設定または OSPFv3 インタフェース情報を表示します。

L3 Features > OSPF > OSPFv3 > OSPFv3 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 9-59　OSPFv3 Interface Settings 画面

以下の項目が表示されます。

項目	説明
OSPFv3 Interface Settings	
Instance ID	インスタンス ID を指定します。 • 設定可能範囲：0-255 • 初期値：0
Area ID	IPv4 アドレス形式または 10 進数（0-4294967295）でエリア識別子を指定します。
Interface Name	VLAN インタフェース名を入力します。（12 文字以内）
OSPFv3 Interface Table	
Interface Name	インタフェース名を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

詳細情報の表示 / 設定

「Interface」のリンクをクリックすると、以下の画面が表示されます。

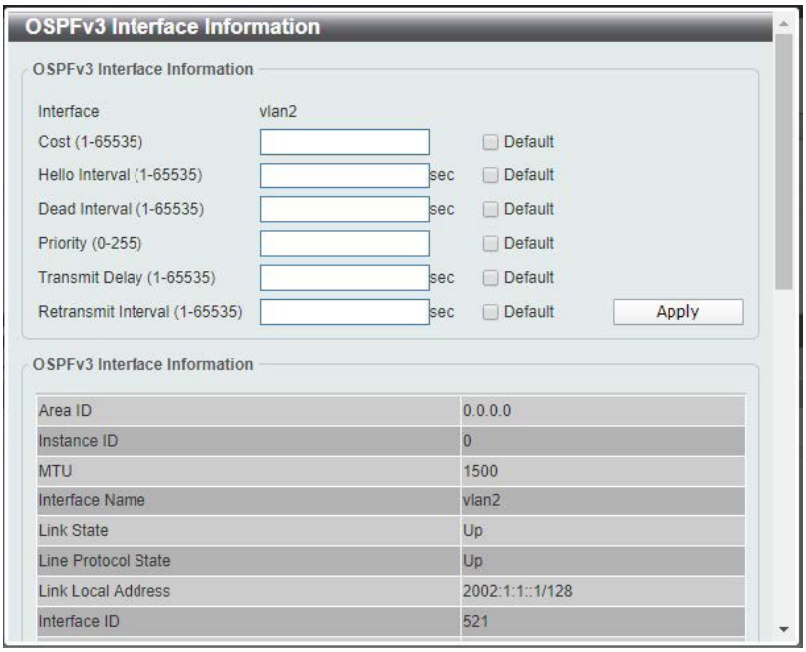


図 9-60　OSPFv3 Interface Information 画面

以下の項目が表示されます。

項目	説明
Cost	OSPFv3 コストを指定します。リンクステートメトリックとして示される整数値です。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535
Hello Interval	OSPF Hello パケットの送信間隔 を指定します。Hello パケットで通知されます。送信間隔が小さいほど、トポロジ変更が検出されやすくなりますが、ルーティングトラフィックが増加します。ネットワーク内の全てのルータおよびアクセスサーバには同じ値を設定する必要があります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead Interval	隣接ルータが Hello パケットを最後に受信してから、選択エリアがルータがダウンしたと判断するまでの時間を入力します。この値は Hello パケット内で通知されます。ネットワーク内の全てのルータおよびアクセスサーバには同じ値を設定する必要があります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒) • 初期値：40（秒）
Priority	代表ルータ (DR : Designated Router) の選出に使用するプライオリティ (0-255) を入力します。ネットワークの OSPF Designated Router (DR) を決定するための優先度となります。2 台のルータが代表ルータになろうとしている場合、高いプライオリティのルータが選出されます。同じプライオリティ値を持つ場合は、ルータ ID の高い方が優先されます。「0」の場合は代表ルータまたはバックアップ代表ルータとして選出されません。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-255 • 初期値：1
Transmit Delay	「Transmit Delay」値を指定します。Link-State Updates（LSU）は、パケット送信前に seconds 引数で指定された値だけ経過時間を増加させます。 指定する値は、インターフェイスの伝送遅延と伝搬遅延を考慮に入れる必要があります。リンク上で送信される前に遅延が追加されない場合、LSA がリンクを介して伝播する時間が考慮されないことになります。この設定は、非常に低速のリンクで特に重要です。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65533 • 初期値：1
Retransmit Interval	「Retransmit Interval」（再送信間隔）の値を指定します。LSA をネイバに送信後、ルータは通知を受信するまで保持します。指定の間隔（Retransmit Interval 値）、ルータが受信の通知を受け取らなかった場合、LSA を再送信します。余計な再送信を減らすため、再送信間隔は控えめに指定することを推奨します。間隔値は予想されるルータ間の往復の遅れよりも大きい値である必要があります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65533（秒） • 初期値：5（秒）

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

OSPFv3 Redistribute Settings（OSPFv3 再分配設定）

OSPFv3 再分配（redistribution）について設定、表示を行います。

L3 Features > OSPF > OSPFv3 > OSPFv3 Redistribute 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 9-61　OSPFv3 Redistribute Settings 画面

以下の項目が表示されます。

項目	説明
Protocol	再分配される送信元プロトコルを指定します。 • 選択肢：「Connected」「Static」「RIPng」
Metric Type	IPv6 OSPF ルーティングドメインに通知されるデフォルトルートの外部リンクタイプを指定します。メトリックタイプが指定されていないと、スイッチは「Type-2」外部ルートを採用します。IPv6 OSPF のみに適用されます。 • 選択肢：「External Type-1」「External Type-2」

項目	説明
Metric	メトリック値を指定します。この設定は、他のプロセスを IPv6 OSPF プロセスに再分配する際に使用されます。 • 設定可能範囲：1-16777214 • 初期値：20
Router Map Name	送信元ルーティングプロトコルからインポートされたルートをフィルタするルートマップ名を指定します。 指定されないと全ルートが再分配されます。

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

OSPFv3 Virtual Link Settings（OSPFv3 仮想リンク設定）

OSPFv3 仮想リンク設定を行います。

L3 Features > OSPF > OSPFv3 > OSPFv3 Virtual Link 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。

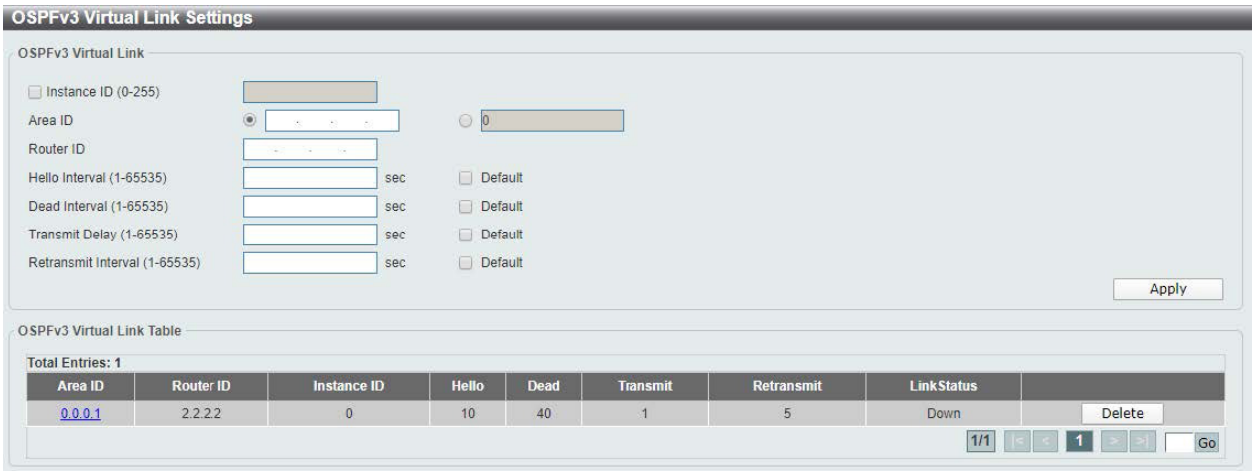


図 9-62　OSPFv3 Virtual Link Settings 画面

以下の項目が表示されます。

項目	説明
Instance ID	インタフェースのインスタンス ID を入力します。 • 設定可能範囲：0-255 • 初期値：0
Area ID	OSPFv3 エリア ID を指定します。IPv4 アドレス形式または 10 進数（0-4294967295）で入力します。
Router ID	仮想リンクネイバのルータ ID を入力します。
Hello Interval	ルータがインタフェース上で送信する Hello パケットの送出間隔を指定します。 • 設定可能範囲： 1-65535（秒） • 初期値：10（秒）
Dead Interval	隣接ルータが Hello パケットを最後に受信してから、選択エリアがルータがダウンしたと判断するまでの時間 を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲： 1-65535（秒） • 初期値：40（秒）
Transmit Delay	ルータがパケットを送信するまでに待機する時間を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲： 1-65533 • 初期値：1（秒）
Retransmit Interval	ルータがパケットを再送信するまでに待機する時間を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲： 1-65533（秒） • 初期値：5（秒）

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

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

詳細情報の表示

「Area ID」のリンク（0.0.0.1）をクリックすると、以下の画面が表示されます。

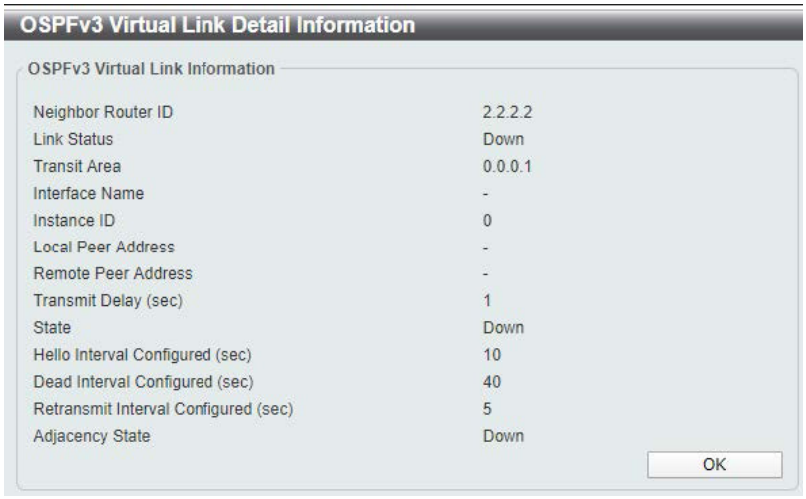


図 9-63　OSPFv3 Virtual Interface Settings - Area ID 画面

OSPFv3 LSDB Table（OSPFv3 LSDB テーブル）

OSPFv3 Link State Database（LSDB）を表示します。

L3 Features > OSPF > OSPFv3 > OSPFv3 LSDB 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。

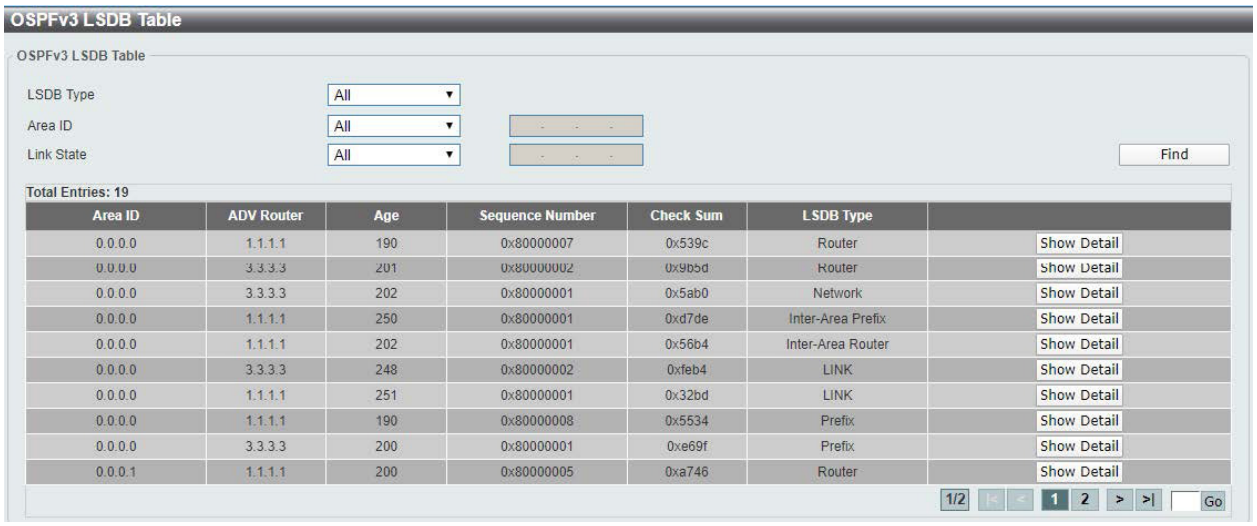


図 9-64　OSPFv3 LSDB Table 画面

以下の項目が表示されます。

項目	説明
LSDB Type	表示する LSDB タイプを指定します。 • 「All」- LSDB 情報の全種類を表示します。 • 「Router」- ルータ LSA の情報のみ表示します。 • 「Network」- ネットワーク LSA の情報のみ表示します。 • 「Prefix」-「intra-area-prefix LSA」の情報を表示します。 • 「Link」- リンク LSA の情報を表示します。 • 「Inter-Area Prefix」-「inter-area prefix LSA」に基づいた LSA の情報のみ表示します。 • 「Inter-Area Router」-「inter-area router LSA」に基づいた LSA の情報のみ表示します。 • 「External」-「external LSA」の情報のみ表示します。 • 「NSSA External」-「NSSA external LSA」の情報のみ表示します。
Area ID	エリア ID オプションを指定します。 • 「All」- すべての LSA を表示します。 • 「Area ID」- 指定エリアのすべての LSA を表示します。Area ID オプションを選択し、エリア ID を IPv4 アドレス形式で入力します。
Link State	表示されるリンクステート情報を選択します。 • 「All」- 全てのリンクステート情報を表示します。 • 「Self Originate」- ローカルルータによって起動している LSA を表示します。 • 「Adv Router」- 通知ルータによって起動済みの全ての LSA を表示します。通知ルータ ID を空欄に入力します。

「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。

エントリの詳細表示

「Show Detail」リンクをクリックすると、以下の画面が表示されます。



図 9-65　OSPFv3 LSDB Information 画面

「Back」をボタンをクリックして前のページに戻ります。

OSPFv3 Neighbor Table（OSPFv3 Neighbor テーブル）

OSPFv3 Neighbor 情報を表示します。

L3 Features > OSPF > OSPFv3 > OSPFv3 Neighbor 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。

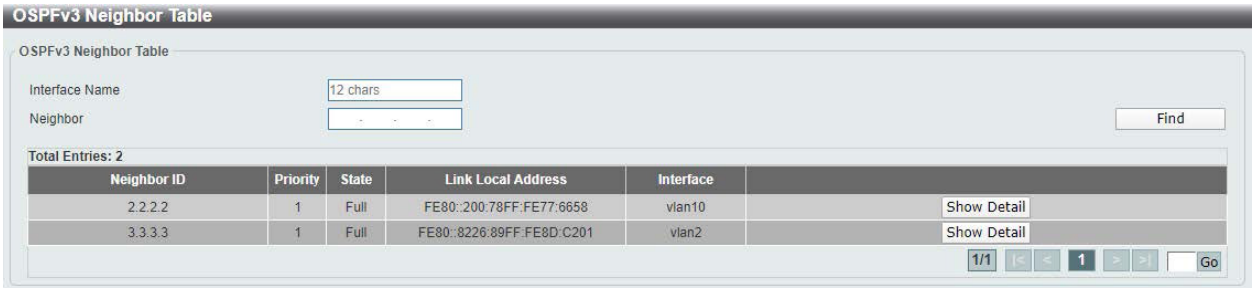


図 9-66　OSPFv3 Neighbor Table 画面

以下の項目が表示されます。

項目	説明
Interface Name	インタフェース名を指定します。
Neighbor	OSPF ネイバ ID を入力します。IPv4 アドレスで指定します。

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。

「Show 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表示します。

エントリの詳細表示

「Show Detail」リンクをクリックすると、以下の画面が表示されます。



図 9-67　OSPFv3 Neighbor Table (Show Detail) 画面

「Back」をボタンをクリックして前のページに戻ります。

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

補足　本機能は将来のファームウェアでサポート予定です。

Control Packet CPU Filtering（制御パケット CPU フィルタリング）

Control Packet CPU Filtering（制御パケット 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、以下の画面を表示します。

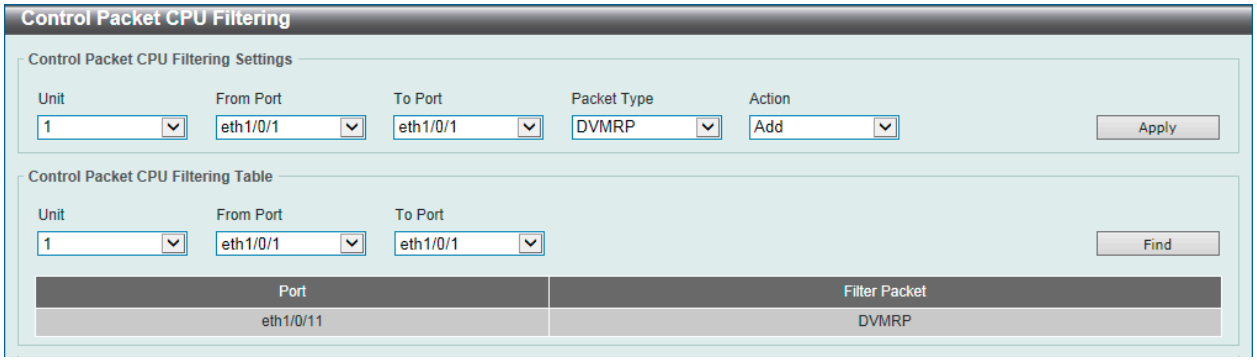


図 9-68　Control Packet CPU Filtering 画面

以下の項目が表示されます。

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	動作を指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Control Packet CPU Filtering Table	
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。

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

IP Route Filter（IP ルートフィルタ）

IP ルートマップの作成を行います。

Route Map（ルートマップ設定）

ルートマップの作成、更新を行います。

L3 Features > IP Route Filter > Route 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 9-69　Route Map 画面

以下の項目が表示されます。

項目	説明
Route Map Name	ルートマップ名を入力します。（16 文字以内）
Direction	一致するルールに対するアクションを指定します。 • 選択肢：「Permit(許可)」「Deny(拒否)」
Sequence ID	ルールエントリのシーケンス番号を指定します。 • 設定可能範囲：1-65535

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

「Match Clause」の編集

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

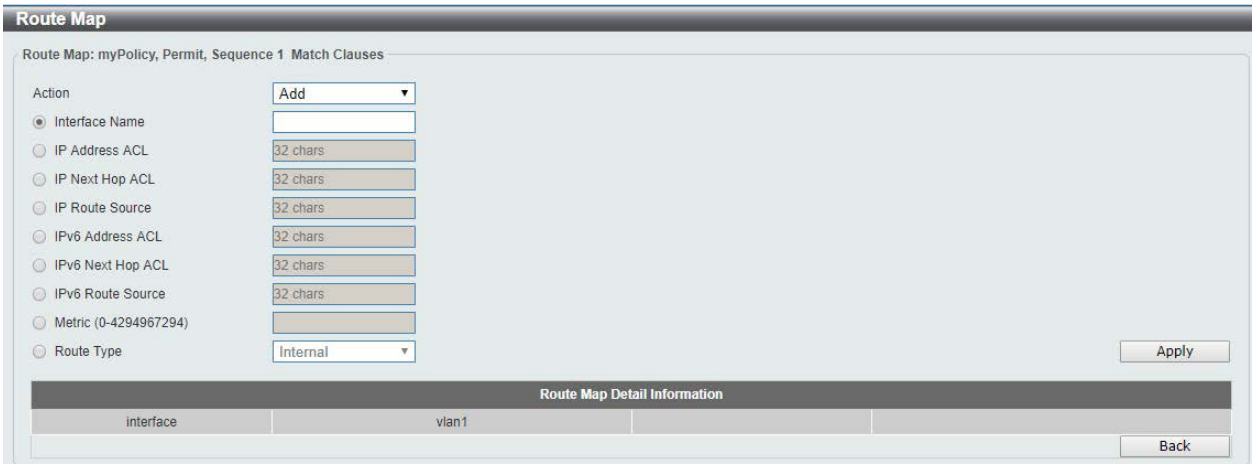


図 9-70　Route Map Settings - Match Clauses 画面

以下の項目が表示されます。

項目	説明
Action	シーケンスエントリを追加 / 削除します。 • 選択肢：「Add（追加）」「Delete（削除）」
Interface Name	インタフェース名を指定します。ルートの送信インタフェースにマッチする条件を定義します。
IP Address ACL	標準 / 拡張 IP アクセスリスト名を指定します。(32 文字以内) このアクセスリストに基づき、ルートの照合が行われます。

項目	説明
IP Next Hop ACL	標準 / 拡張 IP アクセスリスト名を指定します。（32 文字以内）このアクセスリストに基づき、ルートのネクストホップの照合が行われます。
IP Route Source	標準 / 拡張 IP アクセスリスト名を指定します。（32 文字以内）このアクセスリストに基づき、ルートの送信元の照合が行われます。
IPv6 Address ACL	IPv6 標準 / 拡張 IP アクセスリスト名を指定します。（32 文字以内）このアクセスリストに基づき、ルートの照合が行われます。
IPv6 Next Hop ACL	IPv6 標準 / 拡張 IP アクセスリスト名を指定します。(32 文字以内)このアクセスリストに基づき、ルートのネクストホップの照合が行われます。
IPv6 Route Source	IPv6 標準 / 拡張 IP アクセスリスト名を指定します。（32 文字以内）このアクセスリストに基づき、ルートの送信元の照合が行われます。
Metric	ルートのメトリック値を指定します。このオプションは、ルートメトリックにマッチする条件を指定します。 • 設定可能範囲：0-4294967294
Route Type	ルートタイプを指定します。 • 「Internal」- OSPF intr-area および inter-are ルートを指定します。 • 「External Type-1」- OSPF Type1 外部ルートを指定します。 • 「External Type-2」- OSPF Type2 外部ルートを指定します。 • 「Nssa-external」- OSPF nssa-external type-1 および type-2 ルートを指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をボタンをクリックして前のページに戻ります。

「Set Clauses」の編集

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

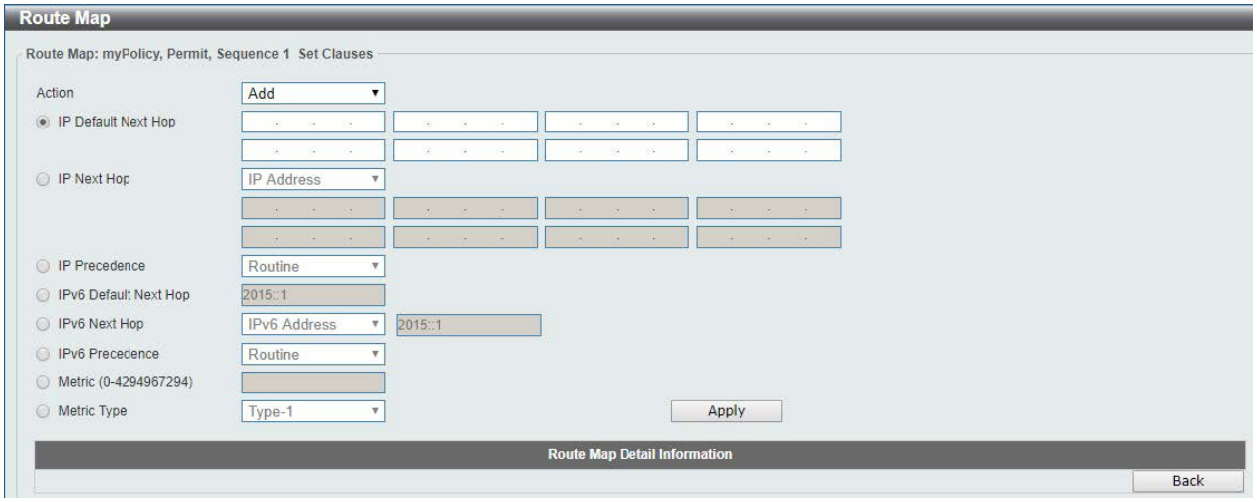


図 9-71　Route Map Settings - Set Clauses 画面

以下の項目が表示されます。

項目	説明
Action	シーケンスエントリを追加 / 削除します。 • 選択肢：「Add（追加）」「Delete（削除）」
IP Default Next Hop	パケットのルーティングに使用するデフォルトのネクストホップ IP アドレスを指定します。本機能は複数のデフォルトネクストホップルータの設定に使用されます。デフォルトネクストホップが既に設定済みの場合、後から設定したデフォルトネクストホップはデフォルトネクストホップリストに追加されます。最初のデフォルトネクストホップルータがダウンすると、次のデフォルトネクストホップルータがパケットのルートを開始します。最大 8 個までのデフォルトネクストホップ IP アドレスが入力できます。
IP Next Hop	ネクストホップ属性を設定します。定義済みのルートマップシーケンスの条件に一致したパケットを転送するネクストホップルータの設定となります。 • 「IP Address」- パケットを転送するネクストホップの IP アドレスを指定します。8 個までのアドレスを設定できます。 • 「Recursive」- ネクストホップルータとして再帰 IP アドレスを指定します。8 個までのアドレスを設定できます。
IP Precedence	IP 優先オプションを指定します。IP ヘッダに含まれる優先度の値となります。本設定は、ポリシールーティングが IPv4 パケットを含む場合のみ有効です。 • 選択肢：「Routine」「Priority」「Immediate」「Flash」「Flash Override」「Critical」「Internet」「Network」
IPv6 Default Next Hop	パケットのルーティングに使用するデフォルトの IPv6 ネクストホップアドレスを指定します。
IPv6 Next Hop	IPv6 ネクストホップ属性を設定します。定義済みのルートマップシーケンスの条件に一致したパケットを転送するネクストホップルータの設定となります。 • 「IP Address」- パケットを転送するネクストホップの IPv6 アドレスを指定します。 • 「Recursive」- ネクストホップルータとして再帰 IP アドレスを指定します。

項目	説明
IPv6 Precedence	IPv6 優先オプションを指定します。IPv6 ヘッダに含まれる優先度の値となります。本設定は、ポリシールーティングが IPv6 パケットを含む場合のみ有効です。 • 選択肢：「Routine」「Priority」「Immediate」「Flash」「Flash Override」「Critical」「Internet」「Network」
Metric	編集に使用されるメトリック値を入力します。 • 設定可能範囲：0-4294967294
Metric Type	編集に使用されるメトリックタイプを指定します。 •「Type-1」- OSPF エクスターナルタイプ 1 メトリックを指定します。 •「Type-2」- OSPF エクスターナルタイプ 2 メトリックを指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をボタンをクリックして前のページに戻ります。

Policy Route（ポリシールート設定）

ポリシーベースルーティングの設定、表示を行います。

L3 Features > Policy 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 9-72　Policy Route 画面

以下の項目を設定します。

項目	説明
Type	ポリシールートタイプを指定します。 • 選択肢：「IP Policy」「IPv6 Policy」

「Edit」をクリックして、エントリの編集を行います。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの編集
「Edit」ボタンをクリックすると、以下の編集画面になります。

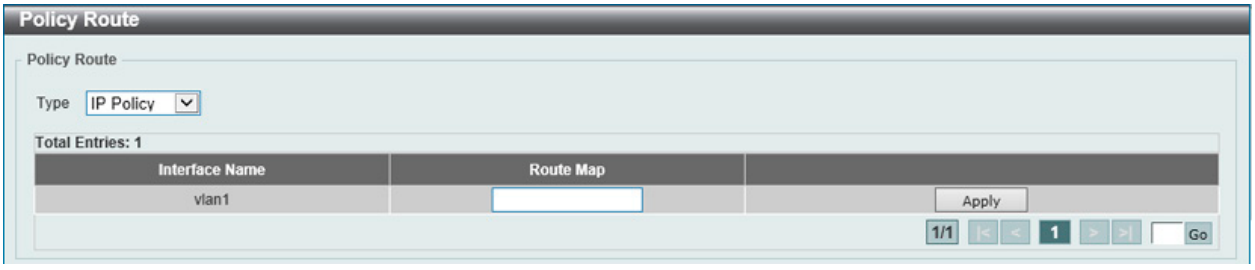


図 9-73　Policy Route Settings 画面 - Edit

以下の項目を設定します。

項目	説明
Route Map	ポリシールートエントリに使用されるルートマップ名を入力します。

項目を編集し、「Apply」ボタンをクリックして変更を適用します。

VRRP（VRRP 設定）

VRRP（Virtual Routing Redundancy Protocol）設定を表示、設定します。 同じ VRRP グループ内のすべてのルータは、同じ仮想ルータ ID と IP アドレスで設定されている必要があります。
仮想ルータグループには仮想ルータ ID が割り当てられ、この仮想ルータの IP アドレスが、それらのホストに設定されるデフォルトルータとなります。
仮想ルータの IP アドレスとして、ルータに設定された実際のアドレスまたは未使用の IP アドレスを指定することができます。仮想ルータのアドレスが実際の物理 IP アドレスである場合、このルータは IP アドレスの所有者（オーナー）となります。
同じ仮想ルータをサポートするルータグループ内で、マスターが選出されます。 他のルータはバックアップルータとなります。マスターは、仮想ルータに対して送信されるパケットの転送を行います。

L3 Features > VRRP 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。

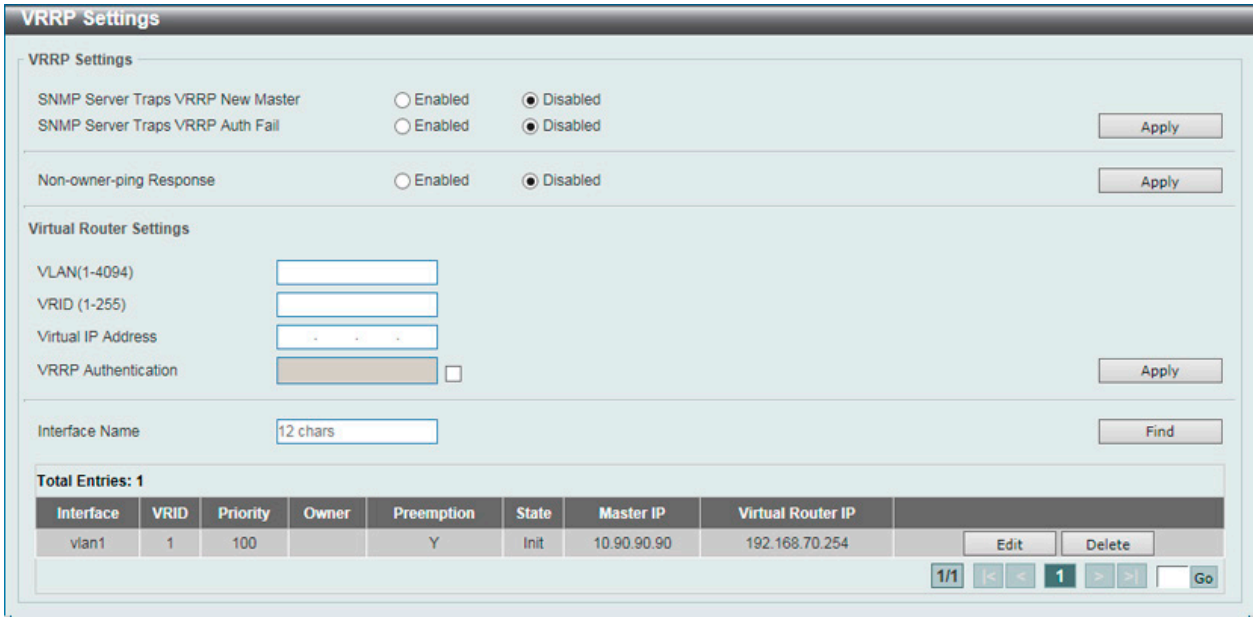


図 9-74　VRRP Settings 画面

以下の項目が表示されます。

項目	説明
VRRP Settings	
SNMP Server Traps VRRP New Master	新しい VRRP マスタの SNMP サーバトラップ機能を有効 / 無効に設定します。 有効にするとデバイスがマスタ状態になった時トラップが送信されます。
SNMP Server Traps VRRP Auth Fail	認証失敗時の SNMP サーバトラップ機能を有効 / 無効に設定します。有効にすると認証鍵 / 認証タイプが競合、または一致しないルータからパケットを受信した時にトラップが送信されます。
Non-owner-ping Response	「Non-owner-ping Response」（非オーナ Ping 応答）機能を有効 / 無効に設定します。本設定により、マスタ状態の仮想ルータが、IP Owner ではない IP アドレス宛ての ICMP エコーリクエストに応答するように設定できます。
Virtual Router Settings	
VLAN	VLAN ID を指定します。 • 設定可能範囲：1-4094
VRID	仮想ルータの ID を指定します。この値は VRRP グループの仮想ルータを識別するために使用します。 • 設定可能範囲：1-255
Virtual IP Address	仮想ルータグループの IPv4 アドレスを指定します。
VRRP Authentication	VRRP 認証を有効に指定し、インタフェースの VRRP 認証パスワードをプレーンテキストで指定します。（8 文字以内） 認証はインタフェースの全ての仮想ルータに適用されます。同じ VRRP グループのデバイスは同じ認証パスワードを保持している必要があります。
Interface Name	インタフェース名を指定します。（12 文字以内）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

エントリの編集

「Edit」をクリックすると、以下の画面が表示されます。



図 9-75　VRRP Settings (Edit) 画面

以下の項目が表示されます。

項目	説明
Advertisement Interval	通知間隔を指定します。マスタルータによる VRRP 通知の間隔となります。 • 設定可能範囲：1-255 • 初期値：1
Preemption	「Preemption」（優先置き換え）機能を有効 / 無効に設定します。 本設定により、より高いプライオリティを持つバックアップルータがより低いプライオリティを持つマスタルータの役割を引き継ぎます。
Priority	仮想ルータのマスタ選出のプロセスで使用する優先値を指定します。 • 設定可能範囲：1-254
Critical IP Address	クリティカル IPv4 アドレスを指定します。クリティカル IP アドレスが仮想ルータ上に設定されていると、この IP アドレスが到達不可の場合、仮想ルータは無効になります。各 VRRP グループは、それぞれ 1 つのクリティカル IP のみ追跡することができます。
Shutdown	シャットダウン機能を有効 / 無効に設定します。この設定により、インタフェースの仮想ルータが無効になります。非オーナルータをシャットダウンする前に、IP アドレスのオーナルータをシャットダウンしないように注意してください。

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

「Back」をクリックすると前のページに戻ります。

VRRPv3 Settings（VRRPv3 設定）

VRRPv3 設定を行います。

L3 Features > VRRPv3 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 9-76　VRRPv3 Settings 画面

以下の項目が表示されます。

項目	説明
VLAN	VLAN ID を指定します。 • 設定可能範囲：1-4094
VRID	作成する仮想ルータの ID を指定します。 • 設定可能範囲：1-255
Address Family	アドレスファミリを指定します。 •「IPv4」- IPv4 仮想ルータを指定します。

項目	説明
Interface Name	表示する VLAN インタフェース名を指定します。（12 文字以内）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

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

エントリの編集
「IPv4 Address Family」エントリの「Edit」をクリックすると、以下の画面が表示されます。



図 9-77　VRRPv3 Settings (Edit/IPv4 Address Family) 画面

以下の項目が表示されます。

項目	説明
Virtual IP Address	仮想 IPv4 アドレスを指定します。同じ VRRP グループの全てのルータは同じルータ ID と仮想アドレスで設定されている必要があります。仮想ルータの IP アドレスは不使用のアドレス、またはルータの実際のアドレスどちらでも指定可能です。仮想アドレスがインタフェースの実際のアドレスと同じ場合、仮想ルータは IP アドレスのオーナとなります。
Advertisement Interval	通知間隔を指定します。マスタルータによる VRRP 通知の間隔値です。マスタルータはコンスタントに VRRP 通知を送信します。VRRP グループ内の全仮想ルータは同じ間隔値である必要があります。 • 設定可能範囲：1-255
Preemption	「Preemption」（優先置き換え）機能を有効 / 無効に設定します。この設定により、より高いプライオリティを持つバックアップルータがより低いプライオリティを持つマスタルータの役割を引き継ぎます。
Priority	仮想ルータの優先値を指定します。VRRP グループのマスタ選出のプロセスで使用する優先値になります。最優先値の仮想ルータがマスタとなり、他のルータは VRRP グループにおいてバックアップとなります。最優先値のルータが複数存在する場合は、より大きい IPv4 アドレス値のルータがマスタとなります。VRRP グループの IPv4 アドレスオーナのルータは常に VRRP グループのマスタになり、一番高い優先値（255）となります。 • 設定可能範囲：1-254
Critical IP Address	クリティカル IPv4 アドレスを指定します。クリティカル IP アドレスが仮想ルータ上に設定されていると、この IP アドレスが到達不可の場合、仮想ルータは無効になります。各 VRRP グループは、それぞれ 1 つのクリティカル IP のみ追跡することができます。
Non-owner ping	「Non-owner ping」（非オーナ Ping）機能を有効 / 無効に設定します。本設定により、マスタ状態の非 IPv4 アドレスオーナの仮想ルータが、ICMP エコーリクエストに応答するように設定できます。
Shutdown	シャットダウン機能を有効 / 無効に設定します。この設定により、インタフェースの仮想ルータが無効になります。非オーナルータをシャットダウンする前に、IPv4 アドレスのオーナルータをシャットダウンしないように注意してください。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

第 10 章　QoS（QoS 機能の設定）

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。
WRED（WRED 設定）	WRED（WRED 設定）の設定を行います。

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。

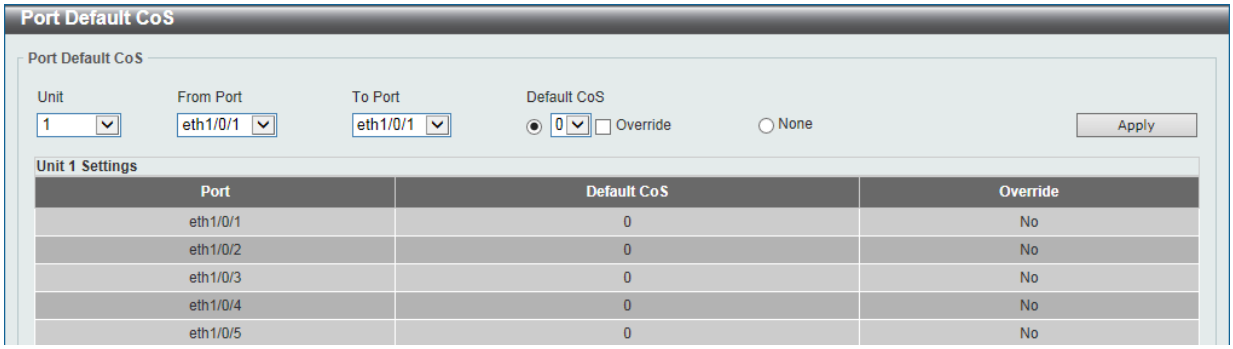


図 10-1　Port Default CoS 画面

以下の項目が表示されます。

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。
Default CoS	ポートにデフォルト 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

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

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

ポートスケジューラーメソッドを設定します。

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

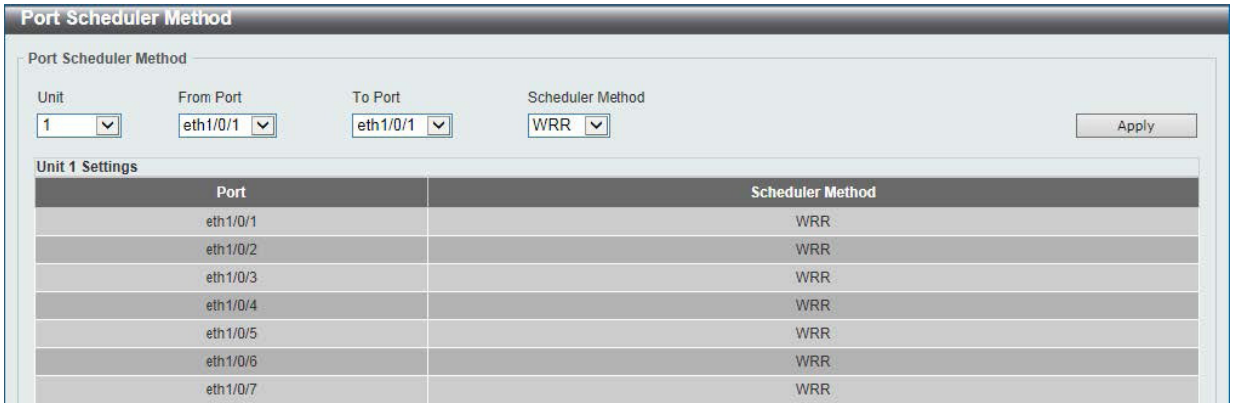


図 10-2　Port Scheduler Method 画面

以下の項目が表示されます。

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。

項目	説明
Scheduler Method	指定ポートに対するスケジューリングの方法を設定します。 「Strict Priority」(SP)、「Round-Robin」(RR)、「Weighted Round-Robin」(WRR)、「Weighted Deficit Round-Robin」(WDRR) から指定できます。初期値ではアウトプットキュースケジューリングアルゴリズムは「WRR」です。 • 「SP」- 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。 • 「RR」- すべてのキューは Round-Robin スケジューリングを使用します。キューを順番に見ながら、均等な比率でパケットが処理されます。 • 「WRR」- 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。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。 • 「WDRR」- 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数値にセットします。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。

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

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。

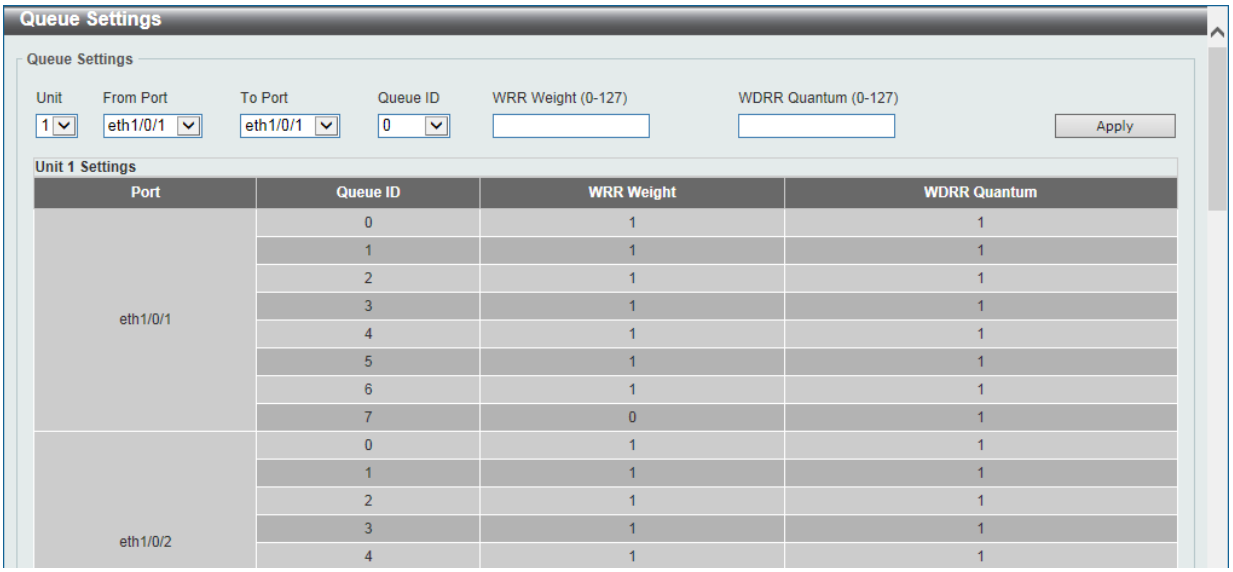


図 10-3　Queue Settings 画面

以下の項目が表示されます。

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。
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ストリクト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

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

CoS to Queue Mapping（CoS キューマッピング設定）

CoS-to-Queue マッピングの表示、設定を行います。

QoS > 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。

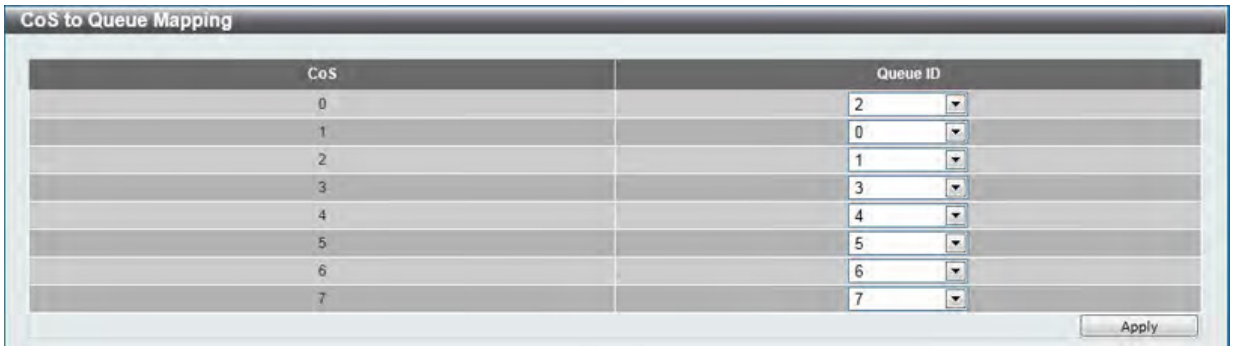


図 10-4　CoS to Queue Mapping 画面

以下の項目が表示されます。

項目	説明
Queue ID	プライオリティを割り当てるクラス（キュー）を設定します。「0」（クラス 0）は最も低い優先度のキューで、「7」（クラス 7）が最も高くなります。

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

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。

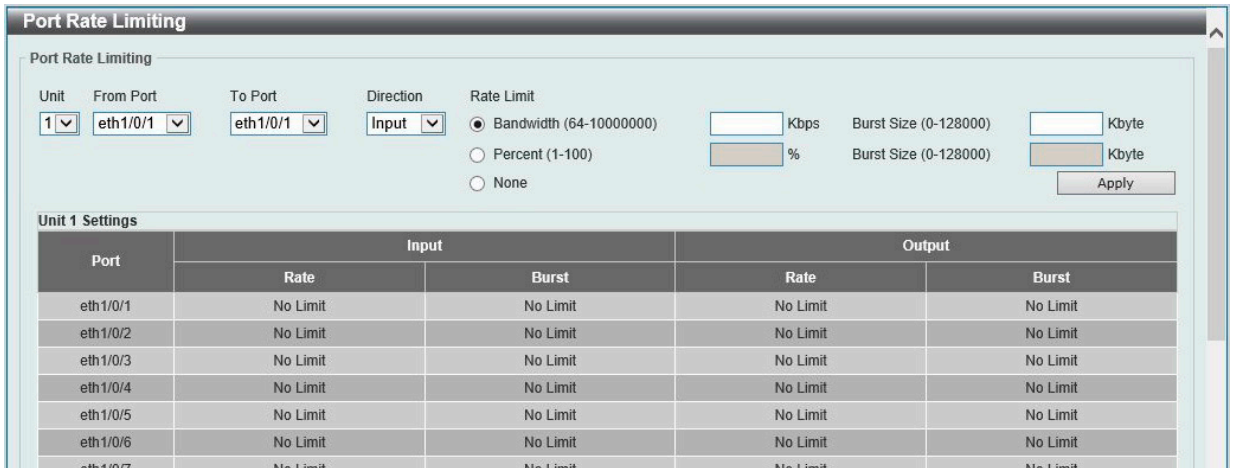


図 10-5　Port Rate Limiting 画面

以下の項目が表示されます。

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。
Direction	レート制限の対象を選択します。 • 選択肢：「Input（イングレス）」「Output（イーグレス）」
Rate Limit	レート制限の値を指定します。 •「Bandwidth」- 受信 / 送信の帯域値を入力欄に入力します。 - 設定可能範囲：64-10000000（Kbps） -「Burst Size」：0-128000（Kbytes） •「Percent」- 受信 / 送信の帯域パーセントを入力欄に入力します。 - 設定可能範囲：1-100（%） -「Burst Size」：0-128000（Kbytes） •「None」- 指定ポートのレート制限を削除します。指定の制限がインタフェースの最大スピードを超えることはありません。イングレス帯域に関して、受信したトラフィックが制限を超えた場合、PAUSE フレームまたはフローコントロールフレームを送信します。

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

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。

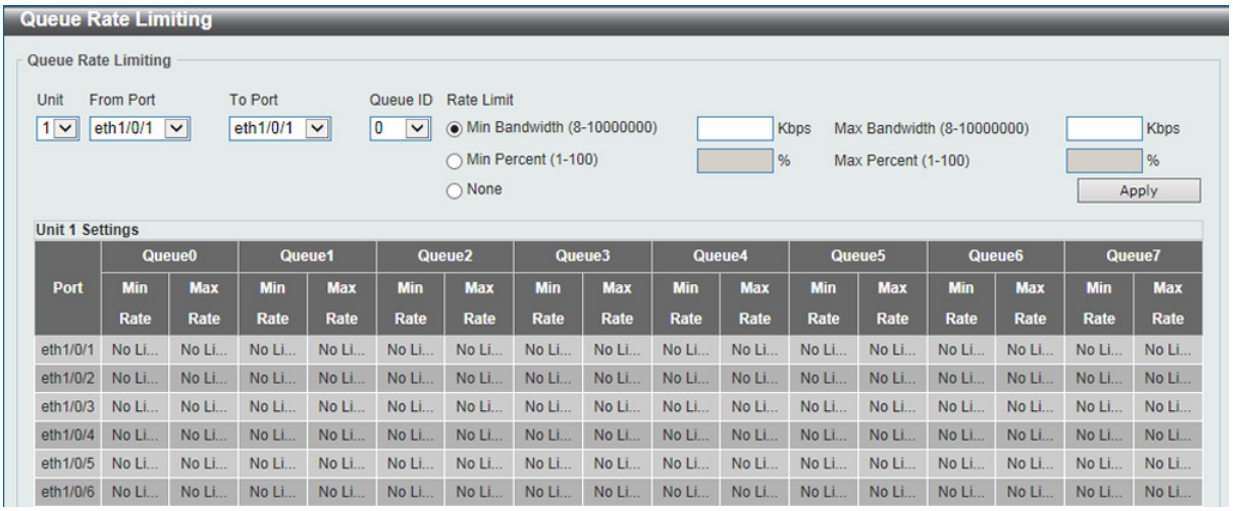


図 10-6　Queue Rate Limiting 画面

以下の項目が表示されます。

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。
Queue ID	キュー ID を指定します。「0」（クラス 0）は最も低い優先度のキューで、「7」（クラス 7）が最も高くなります。
Rate Limit	キューレート制限の設定を行います。 「Min Bandwidth」を選択し、最小限の帯域値を入力欄に入力します。この値は 8 から 10000000 Kbps で指定できます。また「Max Bandwidth」で最大限の帯域値も入力可能です。この値は 8 から 10000000 Kbps で指定できます。最小帯域が指定されるとこのキューから送信されるパケットが保証されます。最大値の帯域値が指定されると、その帯域が有効であっても、このキューからの送信パケットは最大の帯域幅を超えることができません。 最小の帯域を設定する時、設定する最小帯域の合計はインタフェース帯域の 75 パーセント以下に設定する必要があります。これにより、設定された最小値の帯域が保証されます。最も優先度の高いキューに対しては、必ずしも最小帯域を設定する必要はありません。全てのキューの最小帯域が一杯であっても、このキューのトラフィックは処理されるためです。 1 つの CoS における最小保証帯域は、物理ポートにまたがって使用することはできないため、このコマンドの設定は物理ポートにのみ設定可能でポートチャネルに対しては設定不可能です。 「Min Percent」では最小帯域パーセントを入力欄に入力します。この値は 1 から 100%で指定できます。最大値（Max Percent）も 1 から 100%で指定できます。

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

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）

本項目では「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、受信 DSCP は DSCP 変更マップに基づき他の DSCP に変化します。DSCP 変更は異なる DSCP 割り当てを持つドメインの統合にとても有効です。DSCP-CoS マップと DSCP-color マップはパケット本来の DSCP に基づいて動作します。すべての後続の動作は変更 DSCP に基づいています。

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。

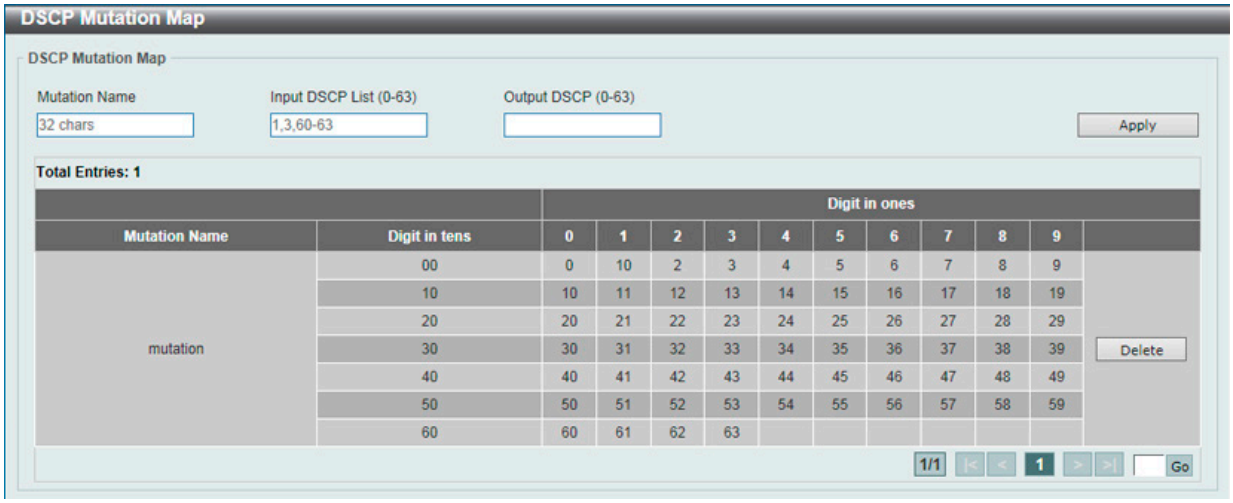


図 10-7　DSCP Mutation Map 画面

以下の項目が表示されます。

項目	説明
Mutation Name	DSCP 変更マップ名を指定します。（32 文字以内）
Input DSCP List	インプットされる DSCP リスト値を入力します。 • 設定可能範囲：0-63
Output DSCP	アウトプットされる DSCP 値を入力します。 • 設定可能範囲：0-63

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、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 and Mutation Binding（ポートトラスト設定）

本スイッチにおけるポートトラスト設定と表示を行います。

QoS > Advanced Settings > Port Trust State and Mutation 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。

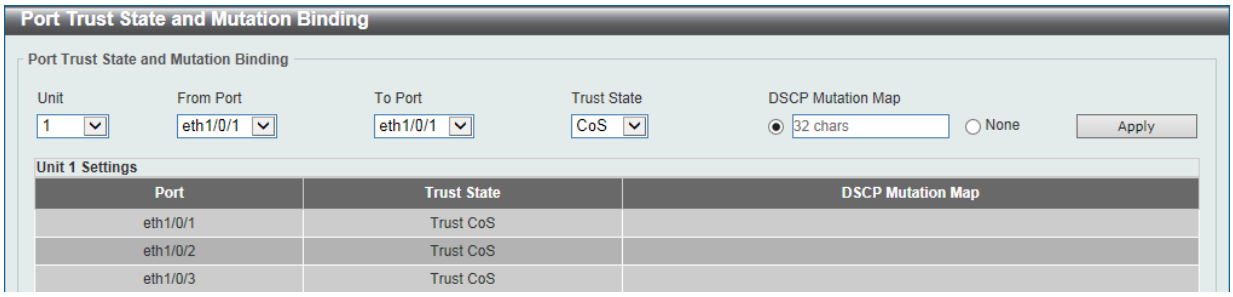


図 10-8　Port Trust State and Mutation Binding 画面

以下の項目が表示されます。

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。

項目	説明
Trust State	ポートトラストの設定をします。 ・ 設定可能範囲：「CoS」「DSCP」から選択可能です。
DSCP Mutation Map	DSCP 変更マップ名を入力します。（32 文字以内） 「None」を選択した場合、ポートに DSCP 変更マップを割り当てません。

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

DSCP CoS Mapping（DSCP CoS マップ設定）

本スイッチにおける DSCP CoS マップの設定と表示を行います。

QoS > 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。

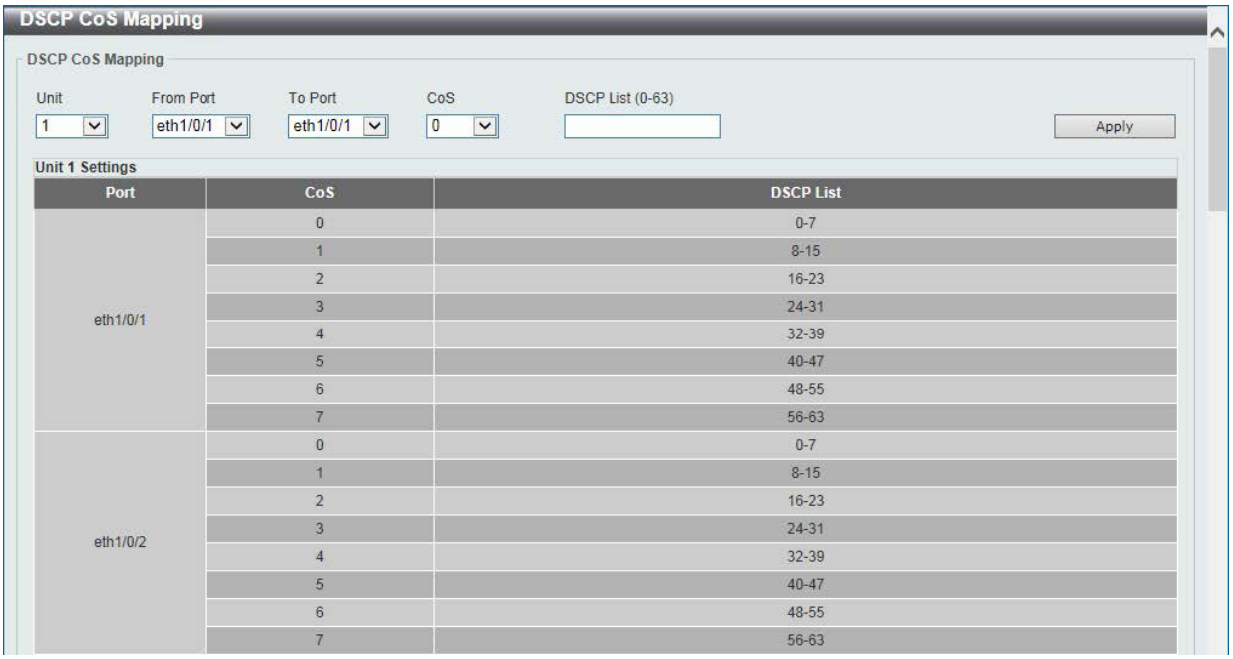


図 10-9　DSCP CoS Mapping 画面

以下の項目が表示されます。

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。
CoS	CoS の値を指定します。 ・ 設定可能範囲：0-7
DSCP List	DSCP リストの値を入力します。 ・ 設定可能範囲：0-63

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

CoS Color Mapping（CoS カラーマップ設定）

本スイッチにおける 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

以下の項目が表示されます。

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。
CoS List	カラーマップされる CoS の値を指定します。 • 設定可能範囲：0-7
Color	マップされるカラーを指定します。 • 選択肢：「Green」「Yellow」「Red」

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

DSCP Color Mapping（DSCP カラーマップ設定）

本スイッチにおける 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。

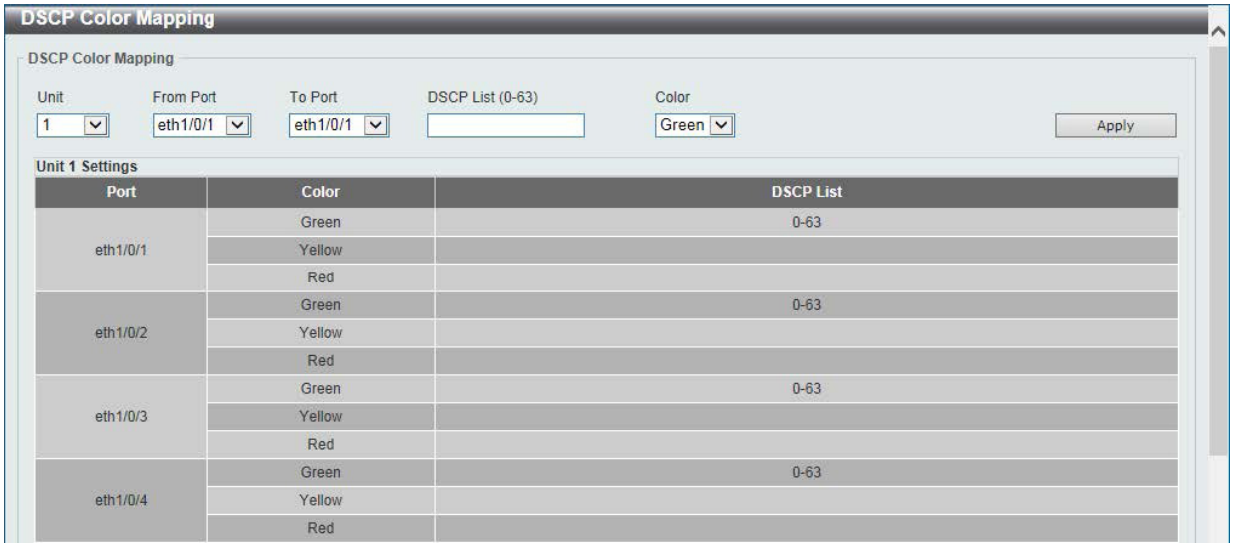


図 10-11　DSCP Color Mapping 画面

以下の項目が表示されます。

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。

項目	説明
DSCP List	カラーマップされる DSCP の値を指定します。 • 設定可能範囲：0-63
Color	マップされるカラーを指定します。 • 選択肢：「Green」「Yellow」「Red」

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

Class Map（クラスマップ設定）

本スイッチにおける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

以下の項目が表示されます。

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）」

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

一致条件の設定

「Match」ボタンをクリックすると下記の画面が表示されます。

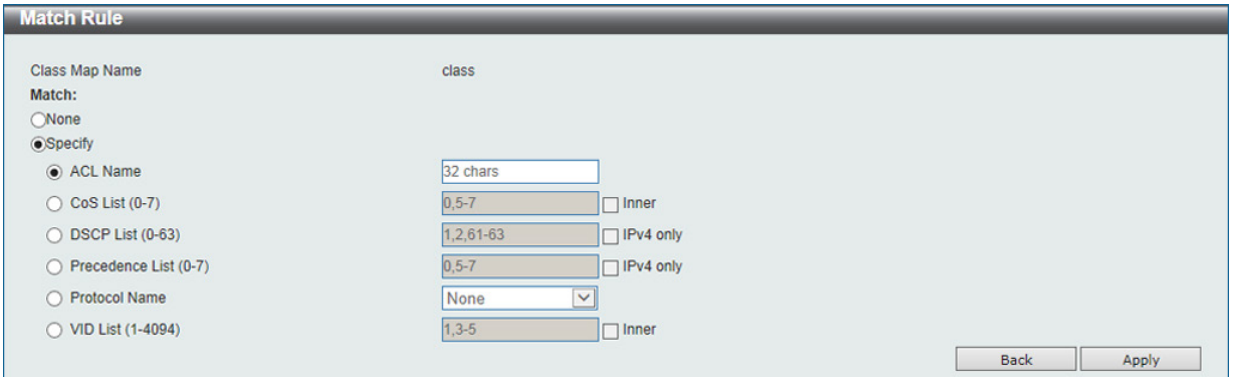


図 10-13　Match Rule 画面

以下の項目が表示されます。

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 リスト名（0-7）を指定します。「Inner」を指定すると、Layer 2 class of service (CoS) マーキングのインナモースト CoS of QinQ パケットを照合します。 • 「DSCP List」- クラスマップで照合する DSCP リスト名（0-63）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。 • 「Precedence List」- クラスマップで照合する優先リスト名（0-7）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。

項目	説明
	• 「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。「None」「ARP」「BGP」「DHCP」「DNS」「EGP」「FTP」「IPv4」「IPv6」「NetBIOS」「NFS」「NTP」「OSPF」「PPPOE」「RIP」「RTSP」「SSH」「Telnet」「TFTP」から選択可能です。 • 「VID List」- クラスマップで照合する VLAN リスト（1-4094）を指定します。「Inner」を指定すると、802.1Q ダブルタグ付きフレームのインナモースト VLAN ID と照合します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

Aggregate Policer（アグリゲートポリサー設定）

本スイッチにおけるアグリゲートポリサーの設定と表示を行います。

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。

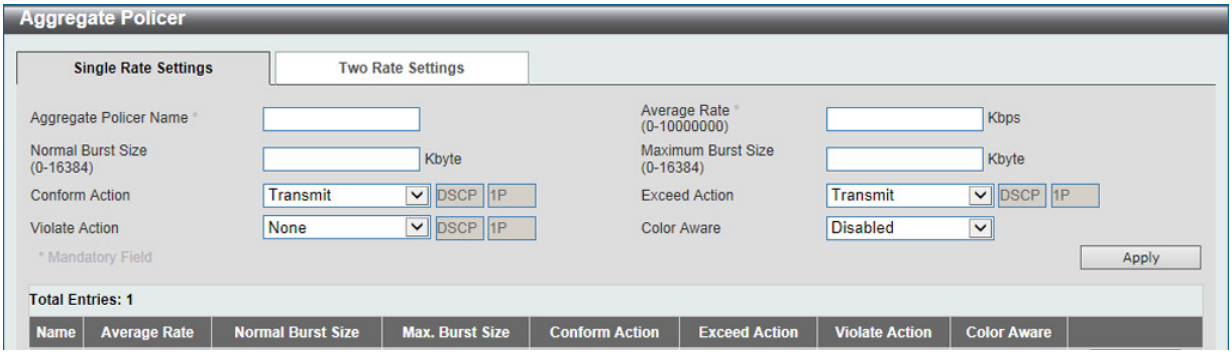


図 10-14　Aggregate Policer 画面

以下の項目が表示されます。

項目	説明
Aggregate Policer Name	アグリゲート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 ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。（初期値） • 「Set-DSCP-1p」-「IP DSCP」と「1P Transmit」の値を入力します。
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 ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。（初期値） • 「Set-DSCP-1p」-「IP DSCP」と「1P Transmit」の値を入力します。
Violate Action	シングルレートポリシングにおける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。「CIR」や「PIR」を順守しないパケットの動作を指定します。シングルレートのポリサーの場合、本項目の指定が行われないと、シングルレート 2 色ポリサーを作成します。2 レートポリサーの場合、本項目の指定が行われないと、初期設定は Exceed Action と同等になります。 • 「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 ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1p」-「IP DSCP」と「1P Transmit」の値を入力します。

項目	説明
Color Aware	「Color Aware」を有効/無効に指定します。「Color Aware」が無効化されている場合、ポリサーはブラインドモードで動作します。有効な場合、ポリサーは Color Aware モードで動作します。

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

「Two Rate Setting」タブをクリックすると次のページが表示されます。

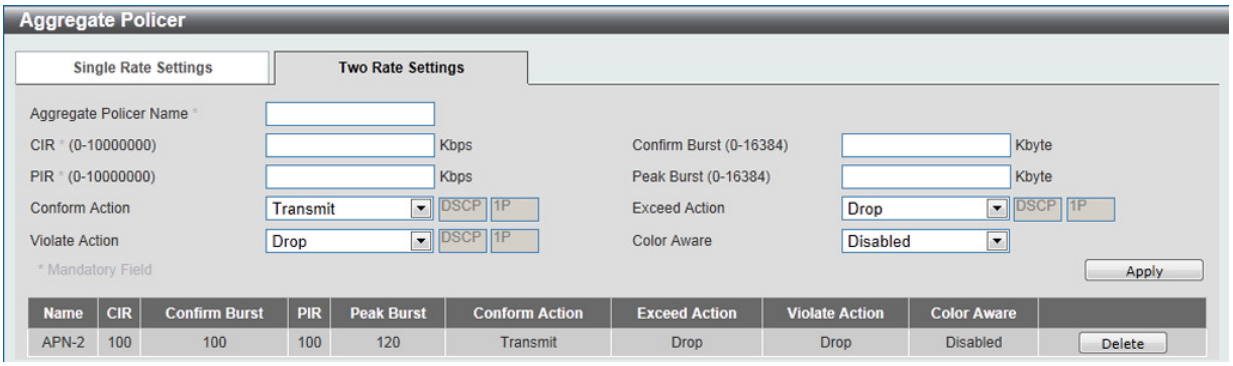


図 10-15　Two Rate Setting 画面

以下の項目が表示されます。

項目	説明
Aggregate Policer Name	アグリゲート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	ここでは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 ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。（初期値） • 「Set-DSCP-1p」-「IP DSCP」と「 1P Transmit」の値を入力します。
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 ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。（初期値） • 「Set-DSCP-1p」-「IP DSCP」と「 1P Transmit」の値を入力します。
Violate Action	シングルレートポリシングにおける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。「CIR」や「PIR」を順守しないパケットの動作を指定します。シングルレートのポリサーの場合、本項目で指定がされないと、シングルレート２色ポリサーを作成します。２レートポリサーの場合、本項目で指定されないと初期設定は Exceed Action と同等になります。 • 「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 ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1p」-「IP DSCP」と「 1P Transmit」の値を入力します。

項目	説明
Color Aware	「Color Aware」を有効/無効に指定します。「Color Aware」が無効化されている場合、ポリサーはブラインドモードで動作します。有効な場合、ポリサーは Color Aware モードで動作します。

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

Policy Map（ポリシーマップ設定）

本スイッチにおける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。

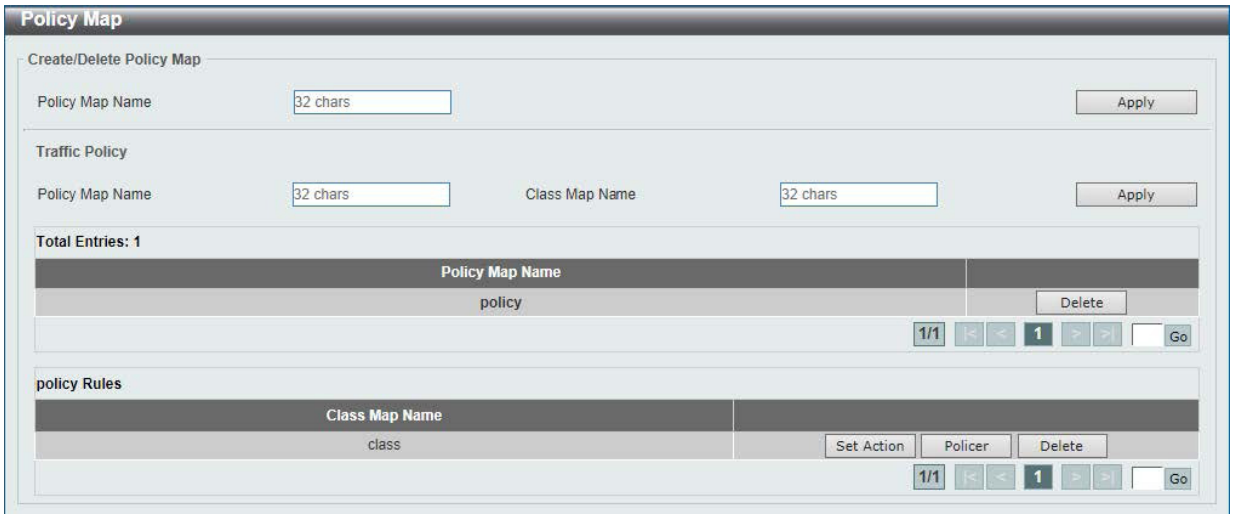


図 10-16　Policy Map 画面

以下の項目が表示されます。

Create/Delete Policy Map

項目	説明
Policy Map Name	ポリシーマップ名を指定します。（32 文字以内）

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

Traffic Policy

項目	説明
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）

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

アクションの設定

「Set Action」ボタンをクリックして、以下の画面を表示します。

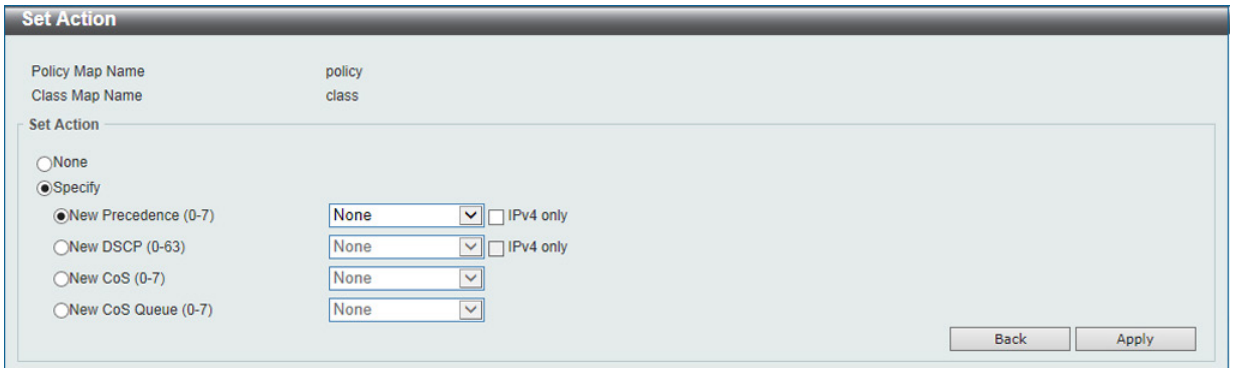


図 10-17　Set Action 画面

以下の項目が表示されます。

項目	説明
None	アクションを実行しません。
Specify	設定に基づいてアクションを実行します。
New Precedence	パケットの優先値を指定します。 「IPv4 only」にチェックを入れると IPv4 の優先度が設定されます。チェックを入れない場合、IPv4 と IPv6 優先度の両方が設定されます。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 ビットが優先度（Precedence）となります。本設定は、CoS キュー選択には影響ありません。 • 設定可能範囲：0-7
New DSCP	パケットの新しい DSCP 名を指定します。 「IPv4 only」にチェックを入れると IPv4 の DSCP が設定されます。チェックを入れない場合、IPv4 と IPv6 DSCP の両方が設定されます。本設定は、CoS キュー選択には影響ありません。 • 設定可能範囲：0-63
New CoS	パケットの新しい CoS 値を指定します。 本設定は、CoS キュー選択には影響ありません。 • 設定可能範囲：0-7
New CoS Queue	パケットの新しい CoS キューを指定します。元の CoS キュー選択を上書きします。ポリシーマップがインタフェースのイーグレスフローに適用される場合、本設定は効力を発揮しません。 • 設定可能範囲：0-7

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

ポリサー設定

「Policer」ボタンをクリックして、以下の画面を表示します。

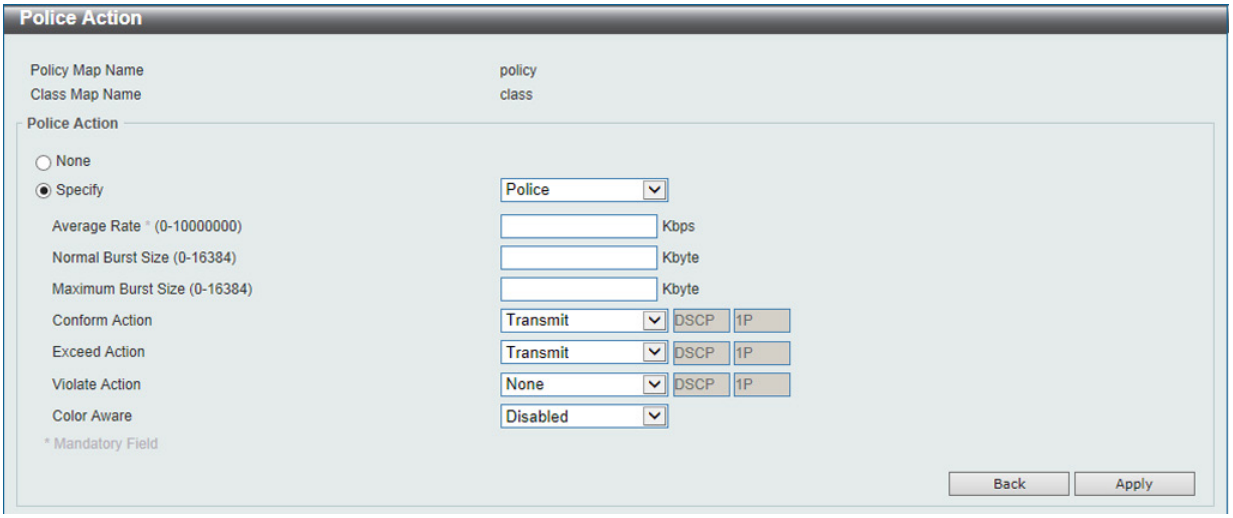


図 10-18　Policer 画面

以下の項目が表示されます。

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。
Average Rate	アベレージ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）
Confirm Action	ここでは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」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1p」- DSCP と CoS 値を設定して、新しい DSCP と CoS 値で送信します。

項目	説明
Exceed Action	ここでは黄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」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1p」- DSCP と CoS 値を設定して、新しい DSCP と CoS 値で送信します。
Violate Action	ここでは赤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」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1p」- DSCP と CoS 値を設定して、新しい DSCP と CoS 値で送信します。
Color Aware	「Color Aware」を有効 / 無効に指定します。本設定が無効な場合、ポリサーバはブラインドモードで動作します。有効の場合はポリサーは Color Aware モードで動作します。

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

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。

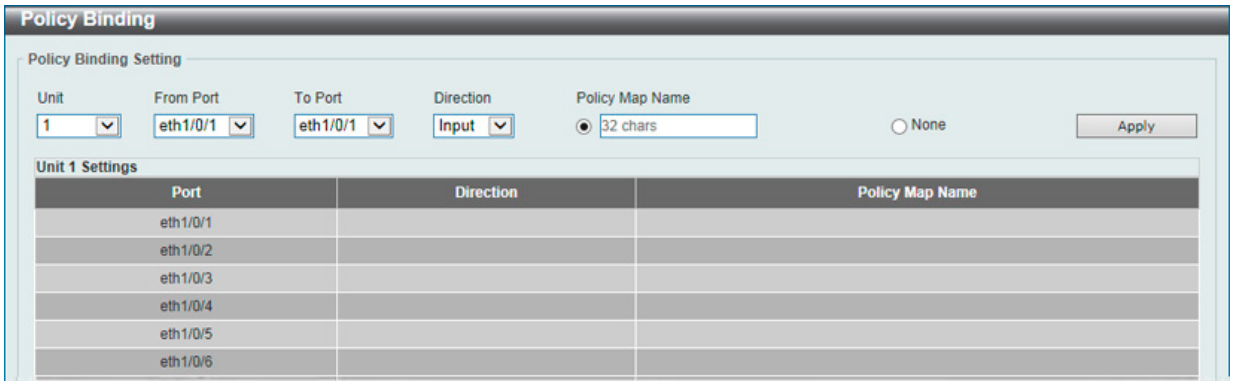


図 10-19　Policy Binding 画面

以下の項目が表示されます。

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。
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。

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

WRED（WRED 設定）

重み付けランダム早期検出（WRED）は、QoS キューの全体的なスループットを向上させる QoS 機能の 1 つです。この方式では、スイッチに設定された QoS の出力キューに基づいて、パケットと QoS キューを分析し、QoS キューに入るパケットにオーバーフローが発生しているかどうかを判断し、ランダムにパケットを破棄してキューへのパケットフローを最小化します。 WRED は、QoS キュー内の輻輳を回避する 2 つの方法を採用しています。

- 各 QoS キューには、パケットを受け入れる最小レベルと最大レベルが設定されます。キューの最大しきい値に達すると、スイッチはすべての入力パケットの破棄を開始します。これにより、QoS に割り当てられた帯域幅が最小化されます。最小しきい値を下回ると、スイッチはすべての入力パケットを受け入れます。

- 入力パケットが最大キューと最小キューの範囲内にある場合、スイッチはスロープ確率関数を使用し、キューが最大しきい値に達した際の破棄確率を決める最大破棄レートに基づき、ランダムなパケット破棄方法を決定します。キューが最大しきい値に近い場合、スイッチはランダムパケットの廃棄を増やしてキューへのフローを均等にし、優先度の高いキューへのオーバーフローを回避します。

WRED Profile（WRED プロファイル設定）

WRED プロファイル設定を行います。

QoS > WRED > WRED 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。

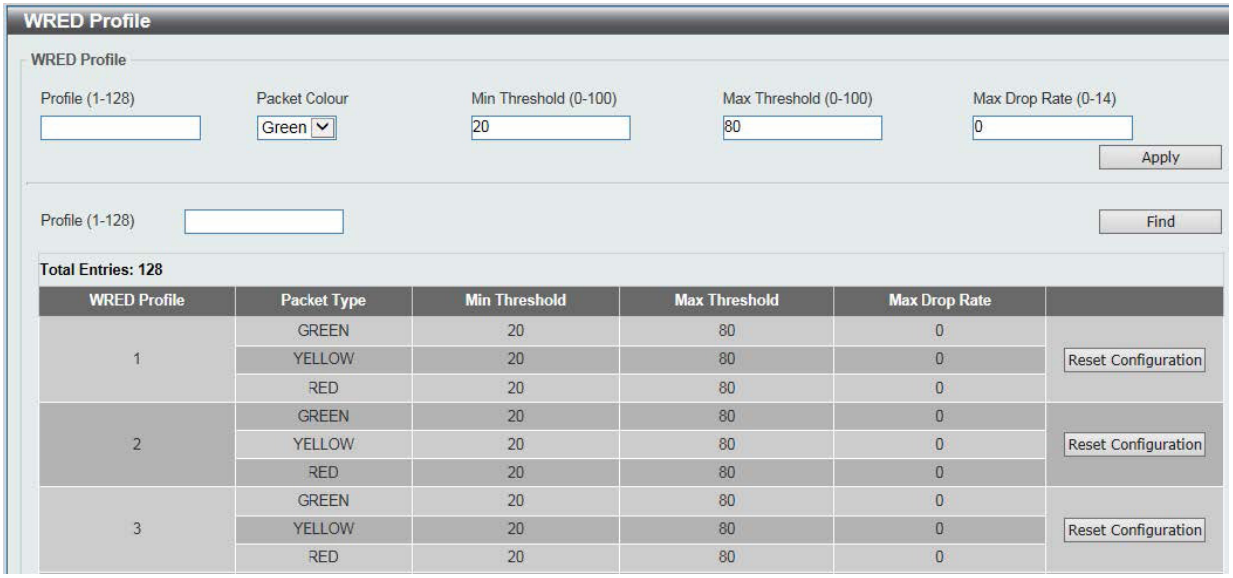


図 10-20　WRED Profile Settings 画面

以下の項目が表示されます。

項目	説明
Profile	WRED プロファイル ID を入力します。 • 設定可能範囲：1-128
Packet Colour	破棄するパケットカラーを選択します。 • 「Green」-「Green」パケットの WRED 破棄パラメータを設定します。 • 「Yellow」-「Yellow」パケットの WRED 破棄パラメータを設定します。 • 「Red」-「Red」パケットの WRED 破棄パラメータを設定します。
Min Threshold	WRED 破棄を開始する最小しきい値を入力します。 • 設定可能範囲：0-100
Max Threshold	パケットを破棄する最大しきい値を入力します。この値に達すると、キューに入力されるすべてのパケットは破棄されます。 • 設定可能範囲：0-100
Max Drop Rate	最大の破棄レートの値を入力します。平均キューサイズが最大しきい値に達した時の破棄確率となります。0 を指定すると、パケットは破棄されないか、ECN（Explicit Congestion Notification）マークが付与されます。 • 設定可能範囲：0-14

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「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。
「Reset Configuration」をクリックして、設定をリセットします。

WRED Queue（WRED キュー設定）

WRED のキュー設定を行います。
WRED は指定のしきい値を超えた平均キューサイズのパケットを破棄します。「Explicit Congestion Notification」(ECN) は指定しきい値を超えた平均キューサイズのパケットを破棄する代わりの、ECN パケット内の WRED の拡張機能です。WRED ECN 機能を使用すると、ネットワークの輻輳とパケットの送信遅延を示す信号として、ルータやエンドホストが ECN マークを使用します。

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

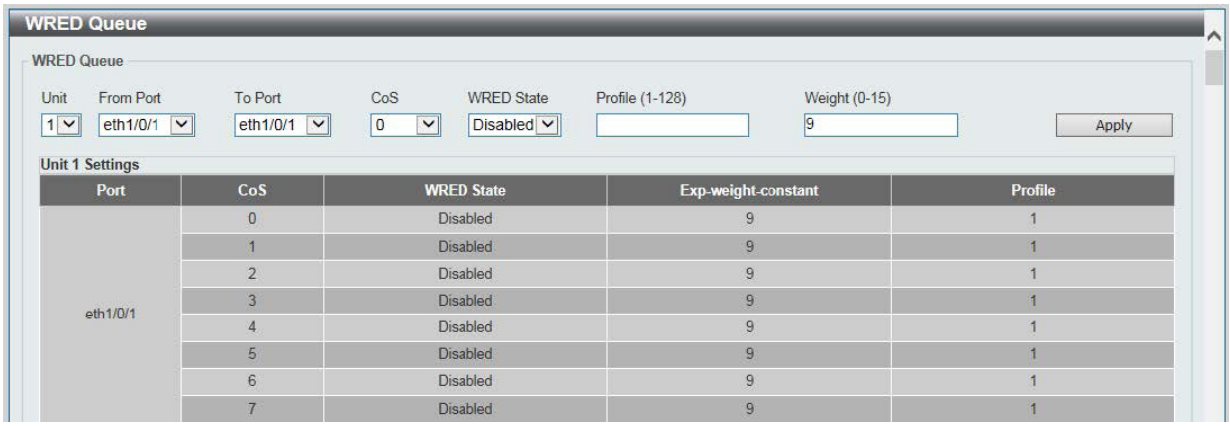


図 10-21　WRED Queue 画面

以下の項目が表示されます。

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。
CoS	CoS 値を指定します。 • 設定可能範囲：0-7
WRED State	指定ポートの WRED 状態を有効または無効にします。
Profile	WERD ポートとキューに使用するプロファイル ID を指定します。 • 設定可能範囲：1-128
Weight	指数 Weight 値を指定します。キューの平均キューサイズ計算に使用される、WRED の指数 Weight 要素として指定します。 • 設定可能範囲：0-15

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

第 11 章　ACL（ACL 機能の設定）

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）	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。
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 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 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。

ACL Configuration Wizard（ACL 設定ウィザードの開始）

ACL 設定ウィザードは、アクセスプロファイルと ACL ルールの新規作成を行います。

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。

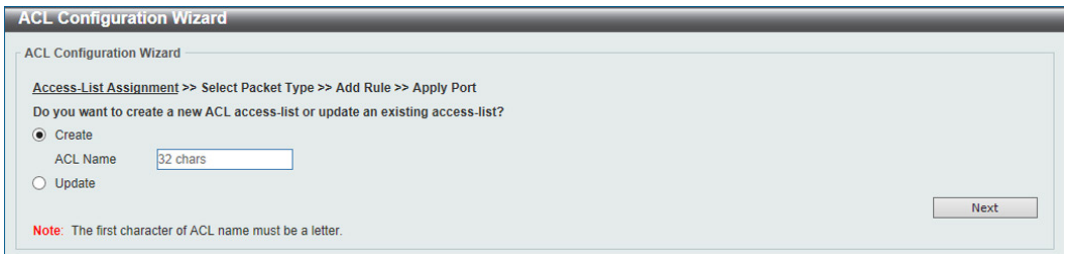


図 11-1　ACL Configuration Wizard（Create) 画面

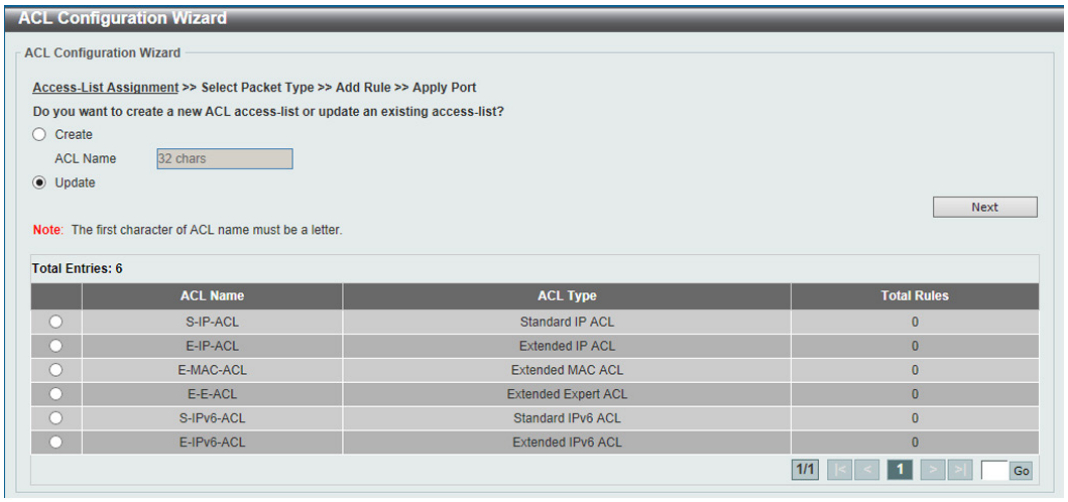


図 11-2　ACL Configuration Wizard（Update) 画面

以下の項目が表示されます。

項目	説明
Create	新しいアクセスルールを作成する場合は、「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、設定内容を更新する場合に選択します。

「Next」をクリックし、パケットタイプの選択を行います。

パケットタイプ選択（ACL 設定ウィザード）

「ACL Configuration Wizard」にて設定する ACL エントリを指定した後、パケットタイプを指定します。

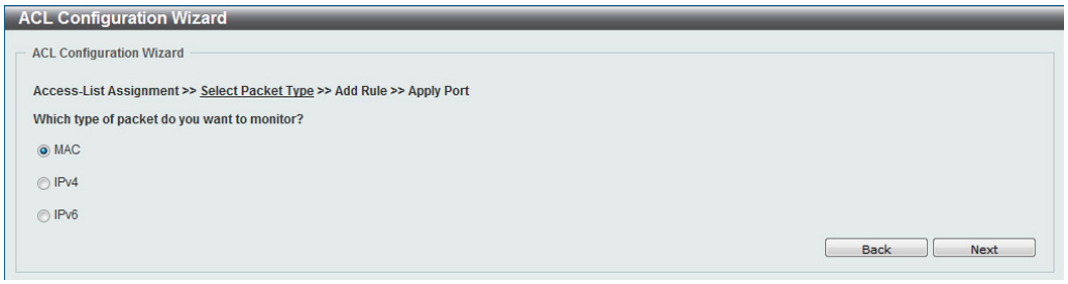


図 11-3　ACL Configuration Wizard (Select Packet Type) 画面

以下の項目が表示されます。

項目	説明
MAC	MAC ACL を作成 / 更新します。

項目	説明
IPv4	IPv4 ACL を作成 / 更新します。
IPv6	IPv6 ACL を作成 / 更新します。

「Next」をクリックして次の設定に進みます。
選択したパケットの種類により表示される画面が異なります。プロファイル種類別の設定方法に従い、設定を行います。
「Back」をクリックすると前のページに戻ります。

ルール追加（ACL 設定ウィザード）

「ACL Configuration Wizard」にて ACL のパケットタイプを指定した後、各パケットの 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 Rule の設定

MAC ACL Rule を設定します。
パケットタイプで「MAC」を選択し「Next」をクリックすると、以下の画面が表示されます。

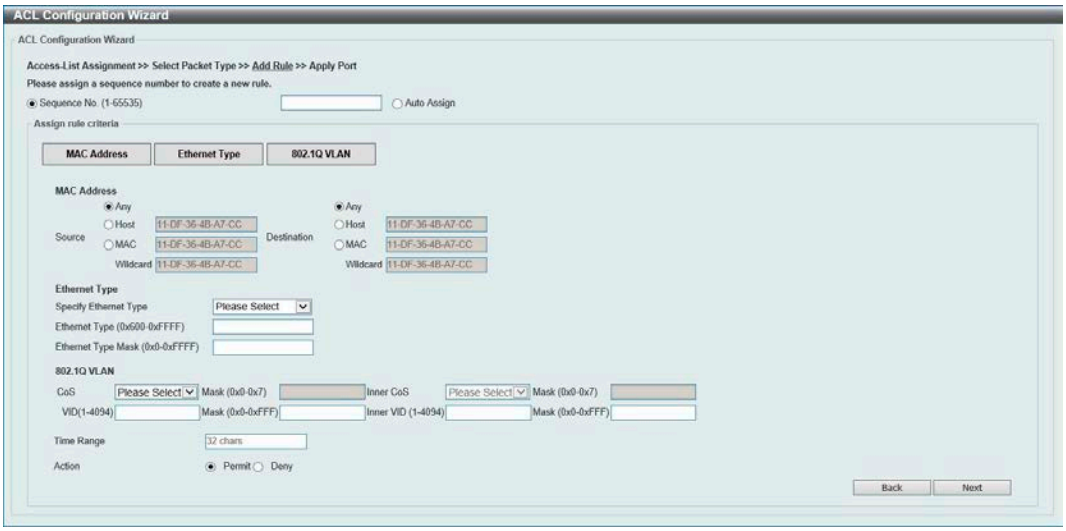


図 11-4　ACL Configuration Wizard - MAC ACL Rule 画面

以下の項目が表示されます。

項目	説明
Assign sequence number	
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
Assign Rule Criteria	
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。
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 0x0 から 0xFFFF の間で指定します。「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。
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

項目	説明
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）
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」をクリックします。
「Back」をクリックすると前のページに戻ります。

IPv4 ACL Rule の設定

IPv4 ACL Rule を設定します。
パケットタイプで「IPv4」を選択し「Next」をクリックすると、以下の画面が表示されます。

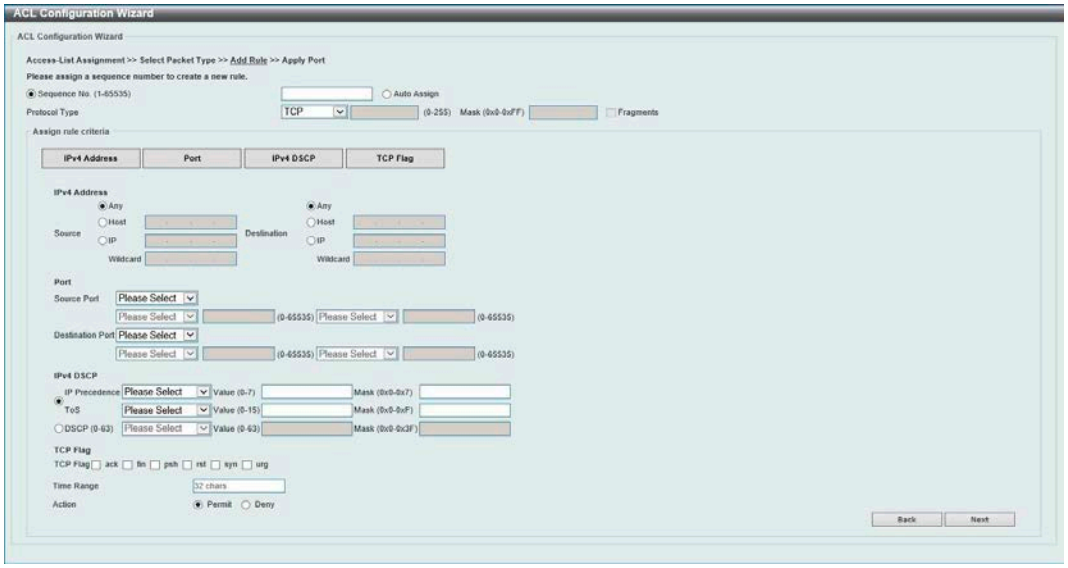


図 11-5　ACL Configuration Wizard -IPv4 画面

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。

すべてのプロトコル選択時に表示される項目（IPv4 ACL Rule）

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。
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「0 (routine)」「1 (priority)」「2（immediate）」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」 - 「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：「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「4（max-throughput)」「8（min-delay）」 - 「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」「UDP」選択時に表示される項目（IPv4 ACL Rule）

項目	説明
Port	
Source Port	送信元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。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「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	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。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「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」選択時に表示される項目（IPv4 ACL Rule）

項目	説明
TCP Flag	
TCP Flag	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」

「ICMP」選択時に表示される項目（IPv4 ACL Rule）

項目	説明
ICMP	
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	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 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 ACL Rule の設定

IPv6 ACL Rule を設定します。
パケットタイプで「IPv6」を選択し「Next」をクリックすると、以下の画面が表示されます。

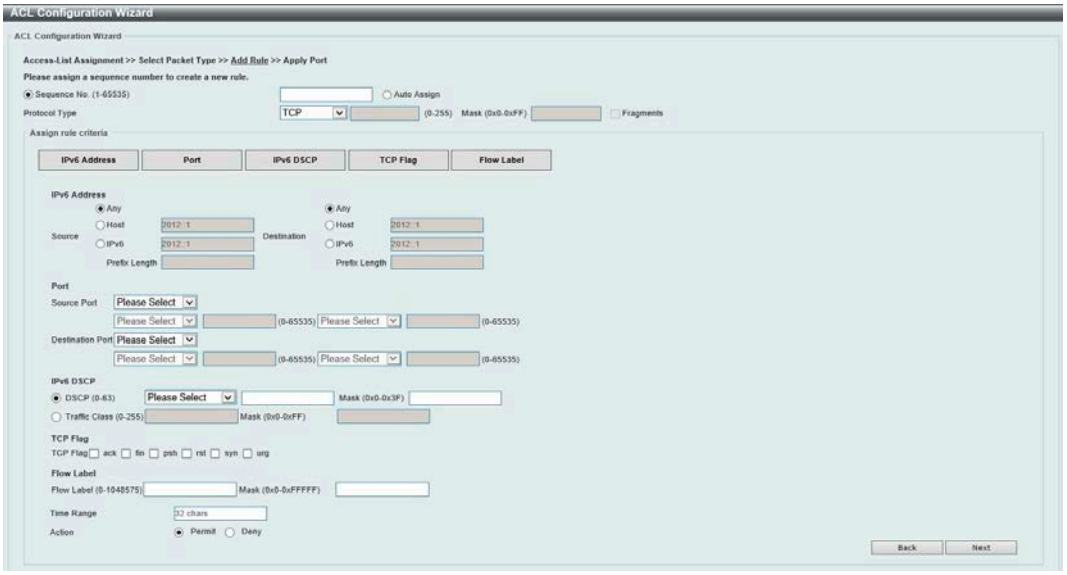


図 11-6　ACL Configuration Wizard - IPv6 画面

以下の項目が表示されます。

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指定します。
Assign rule criteria（ルール条件の割り当て）	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。
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）」

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。

すべてのプロトコル選択時に表示される項目（IPv6 ACL Rule）

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。
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）

「TCP」「UDP」選択時に表示される項目（IPv6 ACL Rule）

項目	説明
Port	
Source Port	送信元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。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「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	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。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「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」選択時に表示される項目（IPv6 ACL Rule）

項目	説明
TCP Flag	
TCP Flag	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」

「ICMP」選択時に表示される項目（IPv6 ACL Rule）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	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

項目	説明
Message Code	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

パケットタイプ、プロトコルの設定後、「Next」をクリックすると以下のポート設定画面が表示されます。

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。

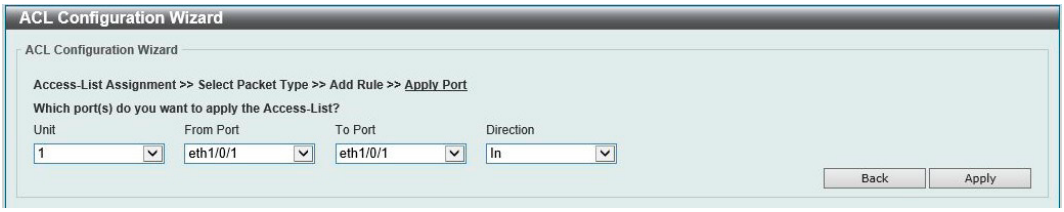


図 11-7　ACL Configuration Wizard (Apply Port) 画面

以下の項目が表示されます。

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。
Direction	方向を指定します。 • 選択肢：「In」「Out」

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

ACL Access List（ACL アクセスリスト）

ACL アクセスリストの設定、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。

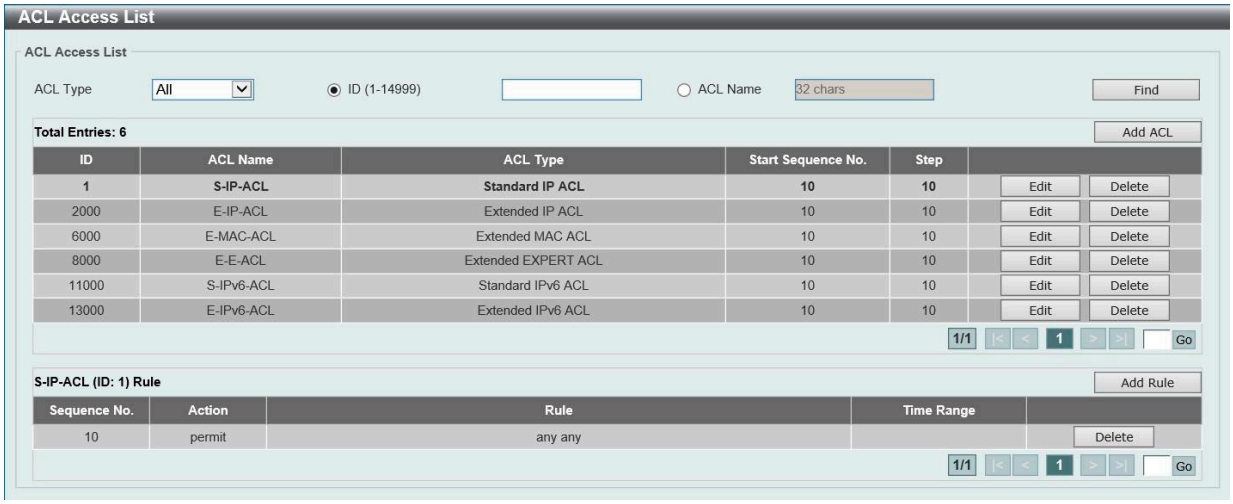


図 11-8　ACL Access List 画面

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」
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て、指定条件に基づくエントリを検索 / 表示します。
「Delete」をクリックして、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。

エントリの編集

「Edit」ボタンをクリックすると、以下の画面が表示されます。

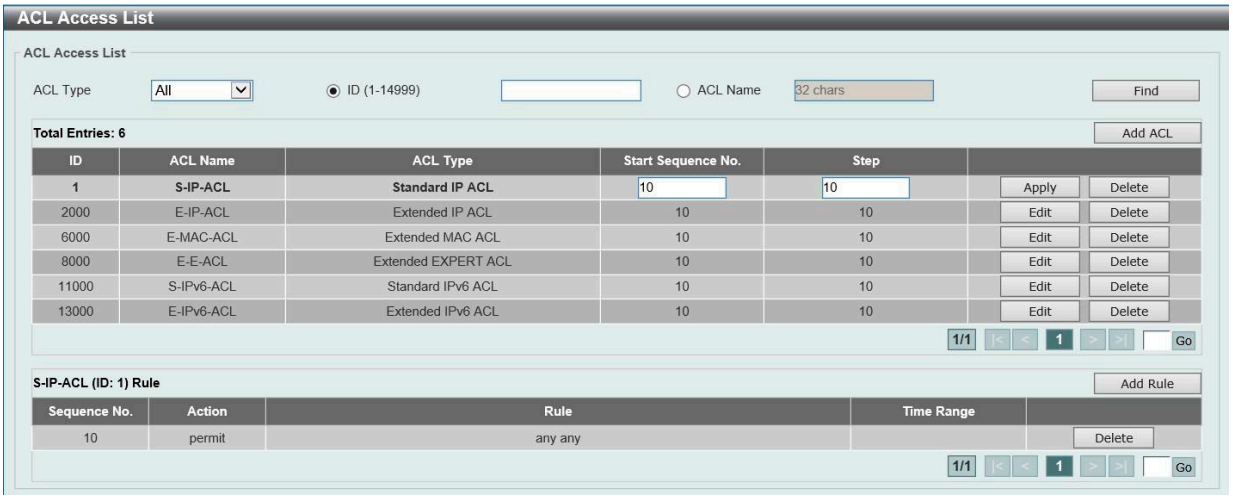


図 11-9　ACL Access List（Edit）画面

以下の項目が表示されます。

項目	説明
Start Sequence No.	開始シーケンス番号を指定します。
Step	シーケンス番号ステップを指定します。この値は、シーケンス番号が増加する値です。例えば、インクリメント（ステップ）値が「5」で開始シーケンス番号が「20」の場合、シーケンス番号は「25」「30」「35」「40」と続きます。 • 設定可能範囲：1-32 • 初期値：10

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

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 11-10　Add ACL Access List 画面

以下の項目が表示されます。

項目	説明
ACL Type	作成する ACL 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」
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
ACL Name	ACL 名を入力します。（32 文字以内）

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

Standard IP ACL（通常 IP 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。

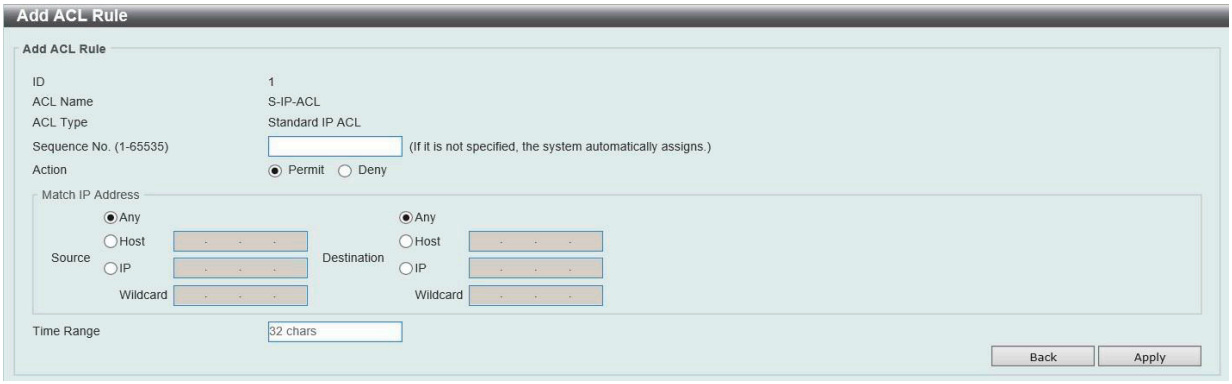


図 11-11　Standard IP ACL (Add Rule) 画面

以下の項目が表示されます。

項目	説明
Sequence No.	シーケンス番号を指定します。値が指定されないと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）」
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。
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）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

Extended IP ACL（拡張 IP ACL）

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。

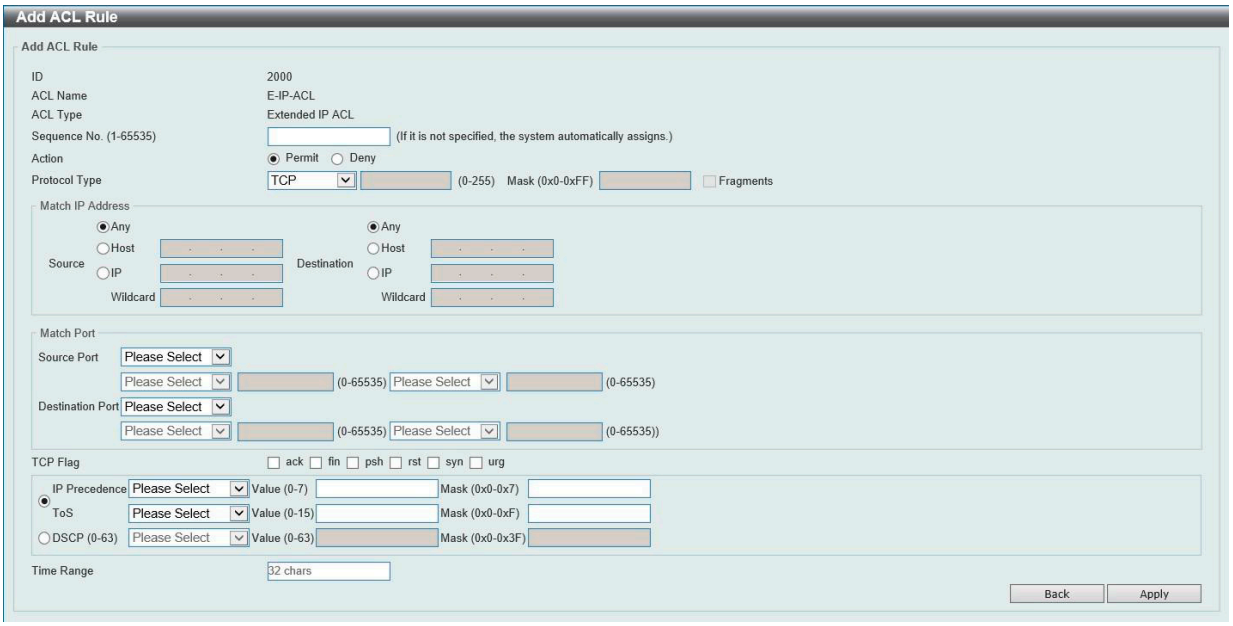


図 11-12　Extended IP ACL (Add Rule) 画面

以下の項目が表示されます。

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。値が指定されないと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。

すべてのプロトコル選択時に表示される項目（Extended IP ACL）

項目	説明
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。
IP Precedence	IP 優先値を指定します。 • 選択肢：「0 (routine)」「1 (priority)」「2（immediate）」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」 - 「Value」：IP 優先値を入力します。（0-7） - 「Mask」に 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：「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「4（max-throughput)」「8（min-delay)」 - 「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)
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)

「TCP」「UDP」選択時に表示される項目（Extended IP ACL）

項目	説明
Source Port	送信元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。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「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	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。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「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」選択時に表示される項目（Extended IP ACL）

項目	説明
TCP Flag	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」

「ICMP」選択時に表示される項目（Extended IP ACL）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	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 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

「ESP」「PCP」「Protocol ID」「None」選択時に表示される項目（Extended IPv4 ACL）

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Standard IPv6 ACL（通常 IPv6 ACL）

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。

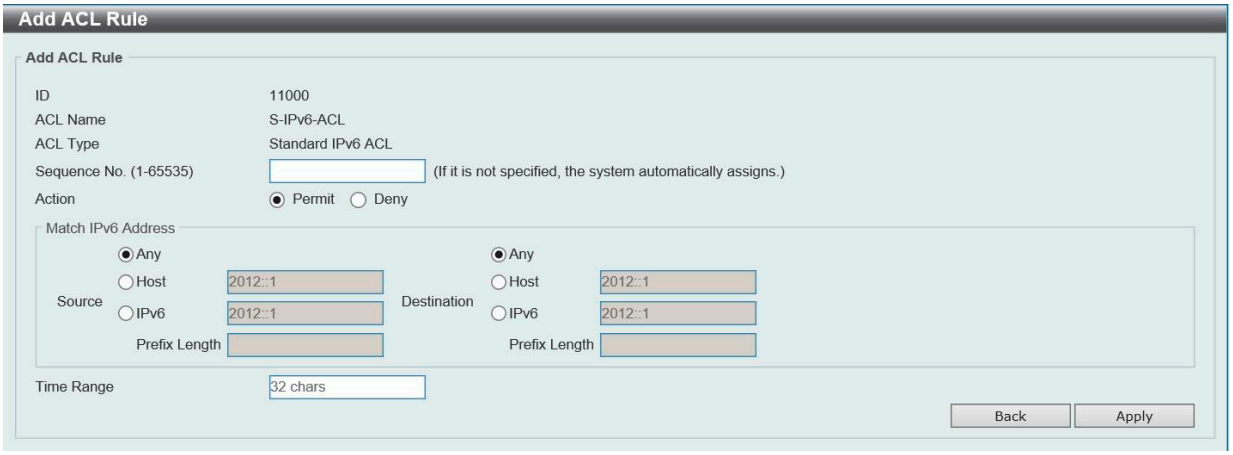


図 11-13　Standard IPv6 ACL (Add Rule) 画面

以下の項目が表示されます。

項目	説明
Sequence No.	シーケンス番号を指定します。値が指定されないと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）」
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。
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）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

Extended IPv6 ACL（拡張 IPv6 ACL）

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。

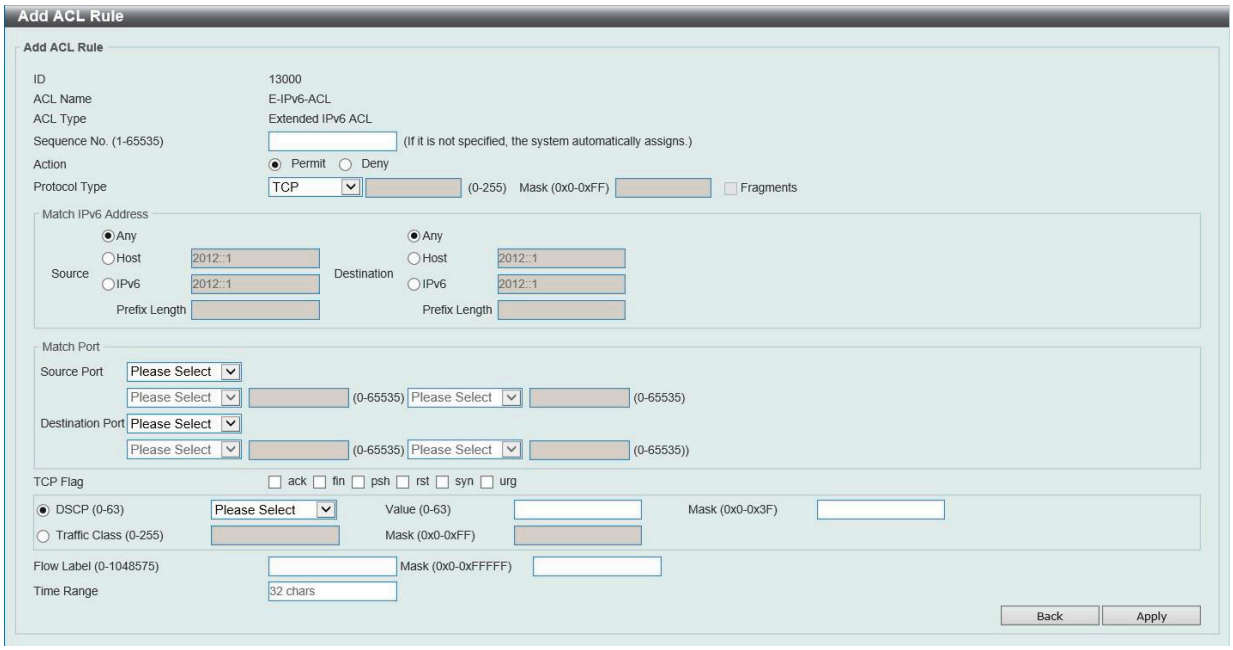


図 11-14　Extended IPv6 ACL (Add Rule) 画面

以下の項目が表示されます。

項目	説明
Sequence No.	シーケンス番号を指定します。値が指定されないと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。

すべてのプロトコル選択時に表示される項目（Extended IPv6 ACL）

項目	説明
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。
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値を入力します。（0x0-0xFF）

項目	説明
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）
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）

「TCP」「UDP」選択時に表示される項目（Extended IPv6 ACL）

項目	説明
Source Port	送信元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。 •「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「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	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。 •「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「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」選択時に表示される項目（Extended IPv6 ACL）

項目	説明
TCP Flag	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」

「ICMP」選択時に表示される項目（Extended IPv6 ACL）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	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。 • 設定が可能範囲：0-255
Message Code	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。 • 設定が可能範囲：0-255

「ESP」「PCP」「Protocol ID」「SCTP」「None」選択時に表示される項目（Extended IPv6 ACL）

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

Extended MAC ACL（拡張 MAC ACL）

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。

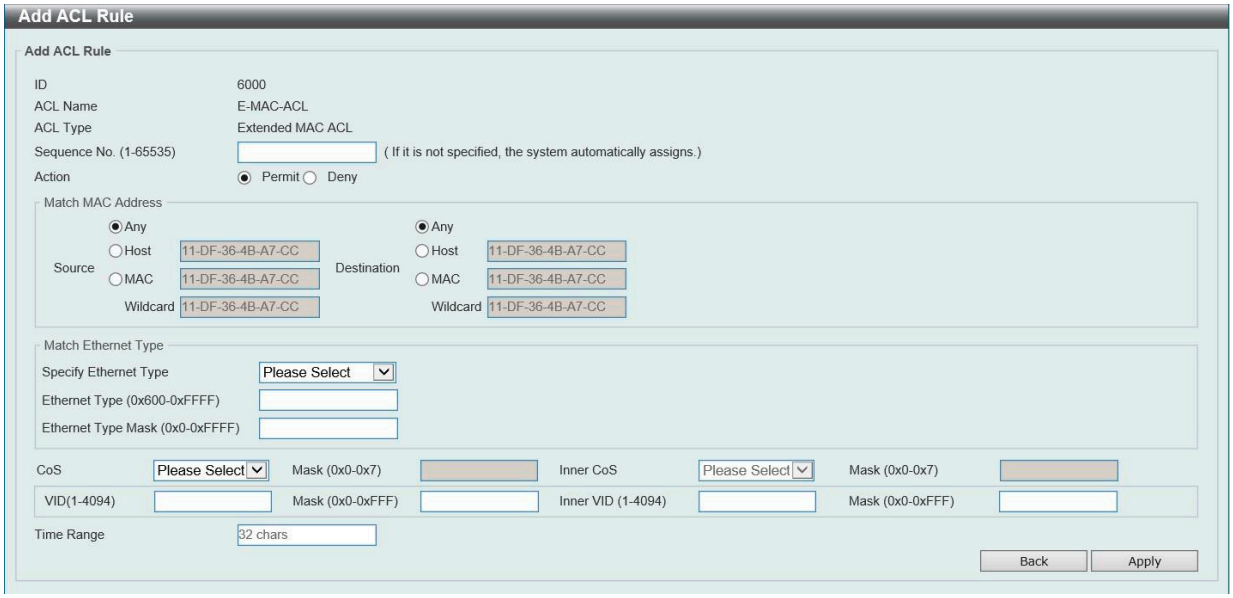


図 11-15　Extended MAC ACL (Add Rule) 画面

以下の項目が表示されます。

項目	説明
Sequence No.	シーケンス番号を指定します。値が指定されないと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）」
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。
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：0x600-0xFFFF
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
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	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）
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）
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）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

Extended Expert ACL（拡張詳細 ACL）

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。

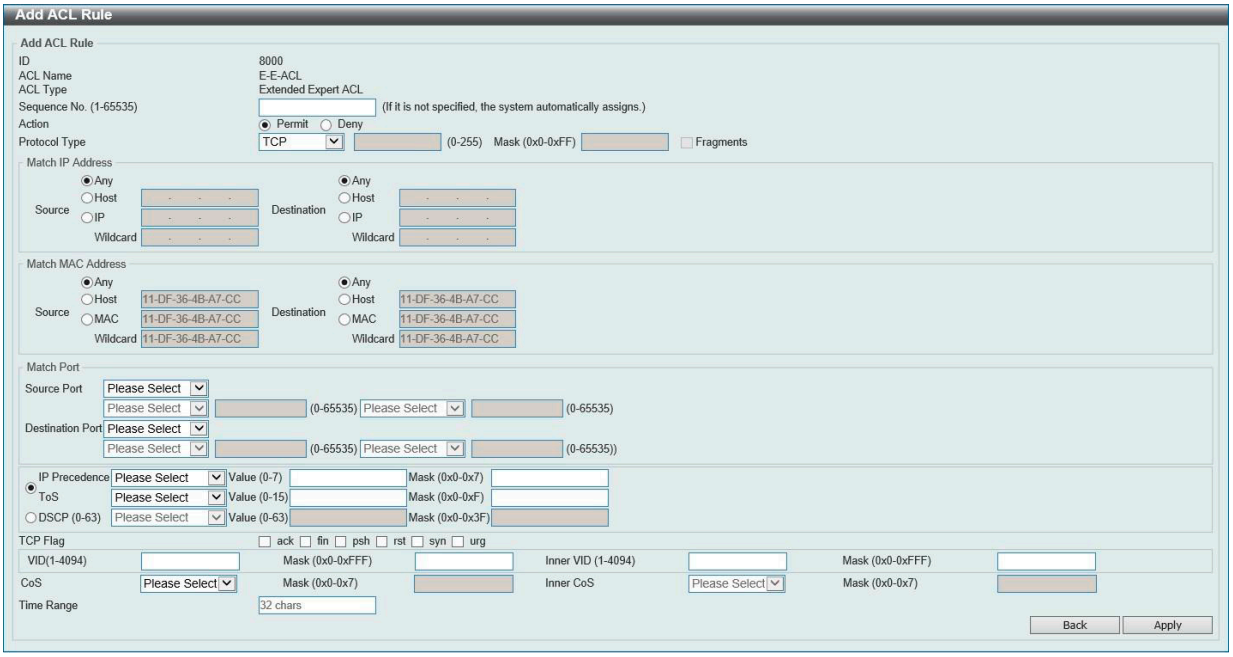


図 11-16　Extended Expert ACL (Add Rule) 画面

以下の項目が表示されます。

項目	説明
Sequence No.	シーケンス番号を指定します。値が指定されないと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。

すべてのプロトコル選択時に表示される項目（Extended Expert ACL）

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。

項目	説明
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。
IP Precedence	IP 優先値を指定します。 • 選択肢：「0 (routine)」「1 (priority)」「2（immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」 - 「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：「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「4（max-throughput)」「8（min-delay)」から指定できます。 - 「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）
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	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）
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）

「TCP」「UDP」選択時に表示される項目（Extended Expert ACL）

項目	説明
Source Port	送信元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。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート • 番号がない場合は項目欄に手動で指定できます。 • 「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	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。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート • 番号がない場合は項目欄に手動で指定できます。 • 「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」選択時に表示される項目（Extended Expert ACL）

項目	説明
TCP Flag	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」

「ICMP」選択時に表示される項目（Extended Expert ACL）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	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 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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

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。

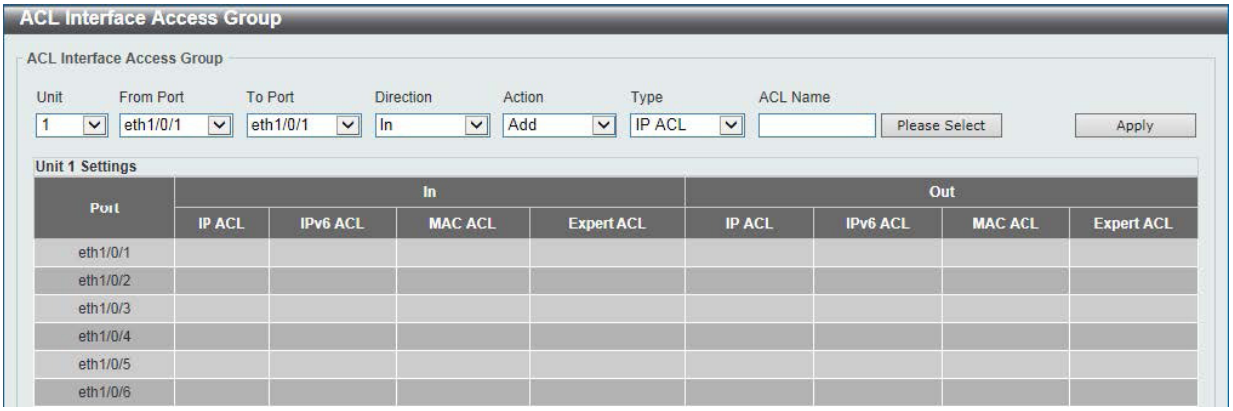


図 11-17　ACL Interface Access Group 画面

以下の項目が表示されます。

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。
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」
ACL Name	「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定します。

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

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 11-18　Please Select 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」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。

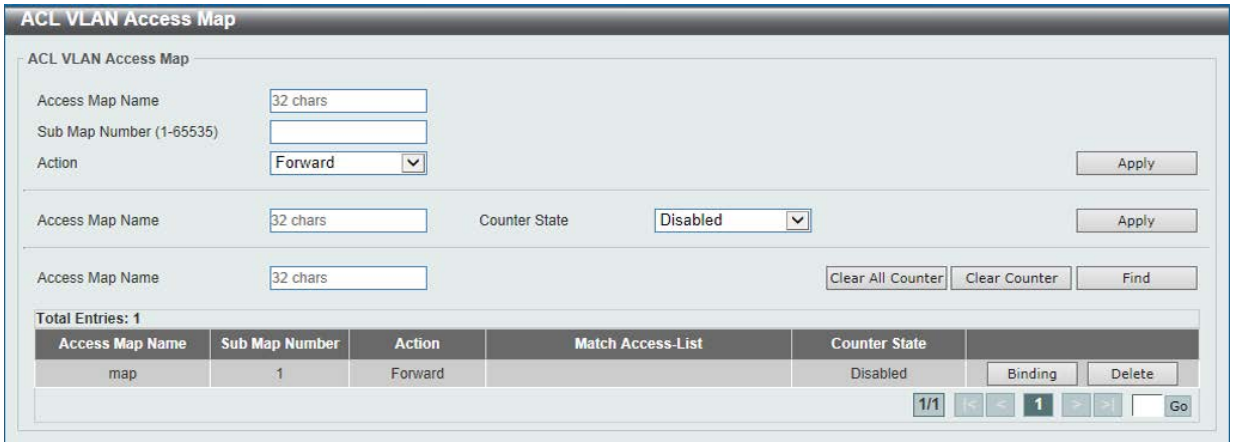


図 11-19　ACL VLAN Access Map 画面

以下の項目が表示されます。

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	サイト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。「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。 • 選択肢：「Forward」「Drop」「Redirect」
Counter State	カウンタの有効 / 無効を指定します。

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

カウンタの削除

「Clear All Counter」ボタンをクリックし、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、指定したアクセスマップのカウンタ情報を消去します。

エントリの検索 / 表示

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 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。

アクセスリストのバインディング

「Binding」ボタンをクリックし、アクセスリストを ACL VLAN アクセスマップにバインドします。

エントリの削除

「Delete」ボタンをクリックし、エントリを削除します。

Match Access-List（照合アクセスリスト設定）

「Binding」ボタンをクリックすると以下の画面が表示されます。

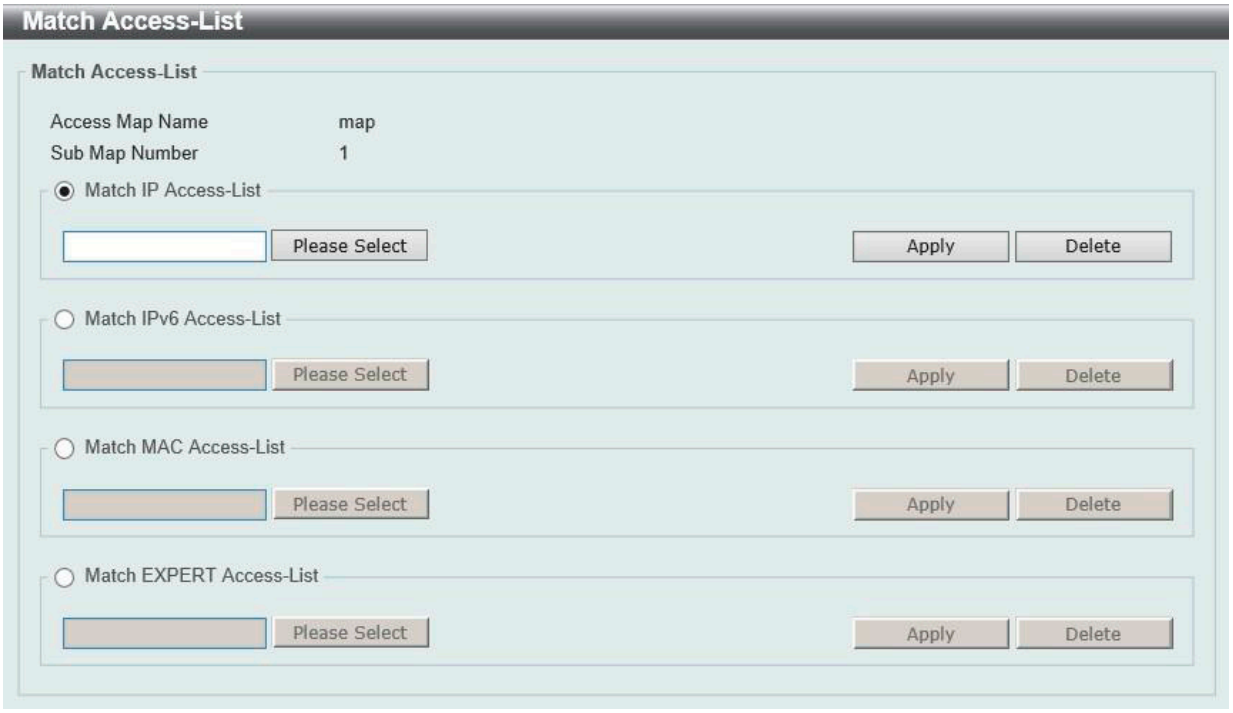


図 11-20　Match Access-List 画面

以下の項目が表示されます。

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します。
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します。
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します。
Match EXPERT Access-List	照合する EXPERT 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します。

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

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 11-21　Please Select 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」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 11-22　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 フィルタの追加 / 削除をします。 • 設定可能範囲：「Add（追加）」「Delete（削除）」
VID List	使用する VLAN ID リストを入力します。

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

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 > 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。

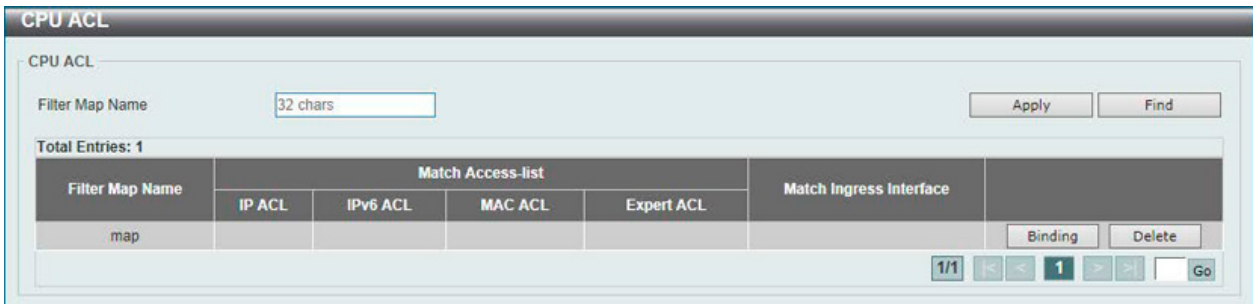


図 11-23　CPU ACL 画面

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）

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

エントリのバインディング

「Binding」ボタンをクリックすると以下の画面が表示されます。

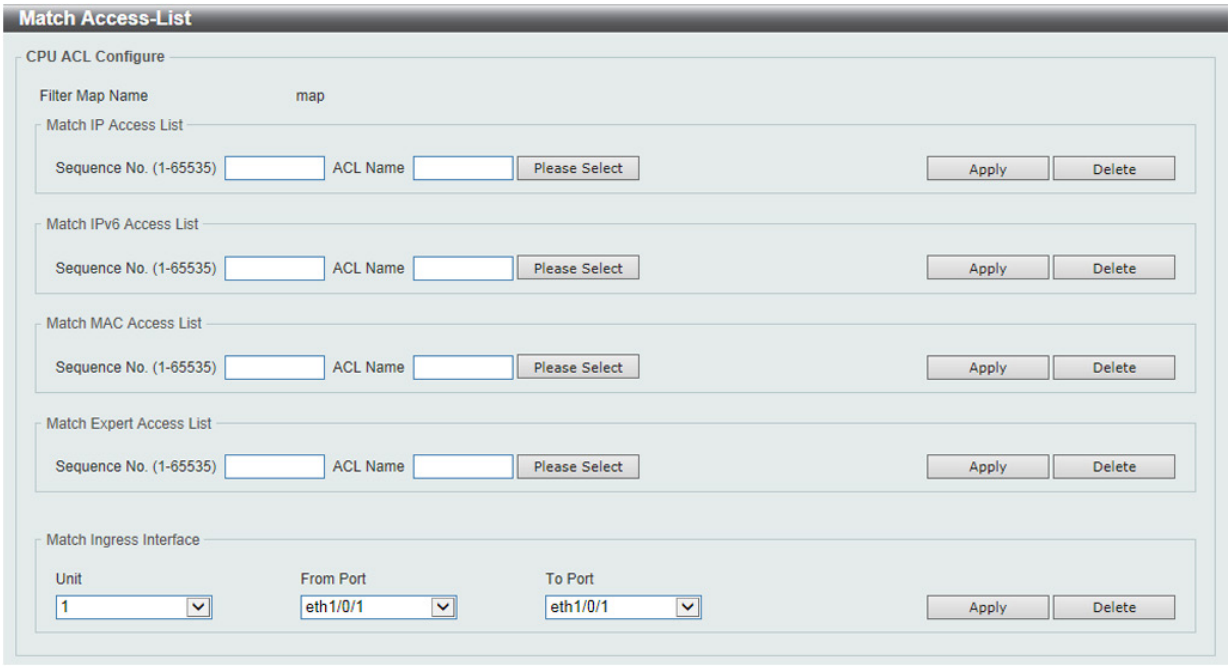


図 11-24　CPU ACL (Binding) 画面

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 から選択します。
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 から選択します。
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 から選択します。
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 から選択します。
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。

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

「Delete」ボタンをクリックし、指定条件に基づいてバインディングを削除します。

「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 11-25　Please Select 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」をクリックします。

第 12 章　Security（セキュリティ機能の設定）

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。
802.1X（802.1X 認証設定）	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 サーバの設定を行います。
TACACS+（TACACS+ 設定）	TACACS+ サーバの設定を行います。
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 アドレスとマッチしなかった 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。
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）※（一部）	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を制限を行います。
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。
SFTP Server Settings（SFTP サーバ設定）	「Secure File Transfer Protocol」(SFTP) サーバの設定、表示を行います。

※サポート予定のため、使用できません。

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機能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。

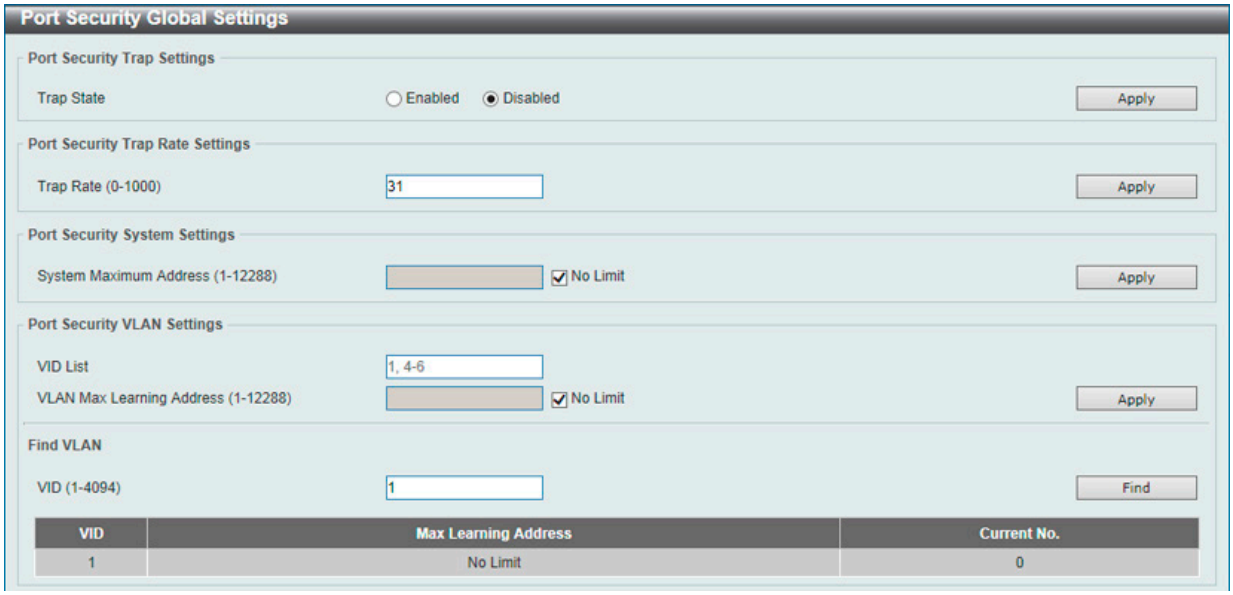


図 12-1　Port Security Global Settings 画面

以下の項目が表示されます。

項目	説明
Trap State	ポートセキュリティトラップ設定を有効 / 無効に設定します。
Trap Rate	毎秒のトラップ数を指定します。初期値の 31 では、SNMP トラップが全てのセキュリティ違反に対して生成されます。 • 設定可能範囲：0-1000 • 初期値：31
System Maximum Address	許可される最大 MAC アドレス数を入力します。指定しない場合、初期値の「No Limit」が適用され、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：1-12288
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 アドレスの最大値を指定します。「No Limit」を選択するとセキュアな MAC アドレスの最大数が適用されます。 • 設定可能範囲：1-12288
VID	表示する VLAN ID を指定します。

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

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。

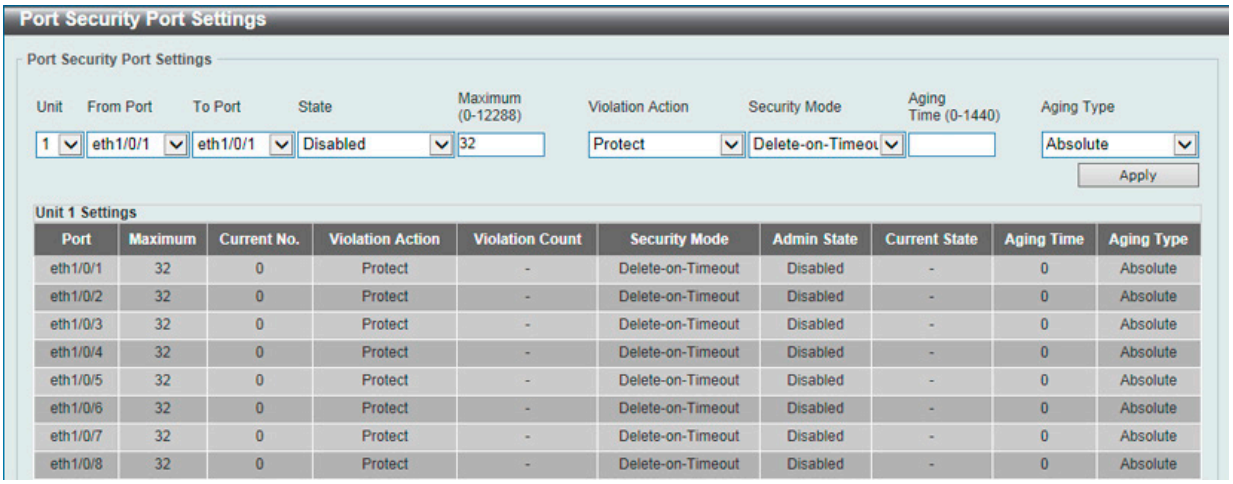


図 12-2　Port Security Port Settings 画面

以下の項目が表示されます。

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。
State	指定ポートへのポートセキュリティ機能を有効 / 無効に設定します。
Maximum	指定ポートで許可される安全な MAC アドレスの最大数を指定します。 • 設定可能範囲：0-64 • 初期値：32
Violation Action	違反に対する動作を指定します。 •「Protect」- ポートセキュリティレベルで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反カウントとしては数えられません。 •「Restrict」- ポートセキュリティレベルで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントされシステムログに記録されます。 •「Shutdown」- セキュリティ違反があるとポートをシャットダウンし、システムログに記録されます。
Security Mode	セキィ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です。 • 設定可能範囲：0-1440（分）
Aging Type	エージングの種類を指定します。 •「Absolute」- ポート上のすべてのアドレスは指定された時間を過ぎるとアドレスリストから削除されます。（初期値） •「Inactivity」- 指定の期間安全なアドレスからのトラフィックがない場合、エージアウトします。

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

Port Security 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。

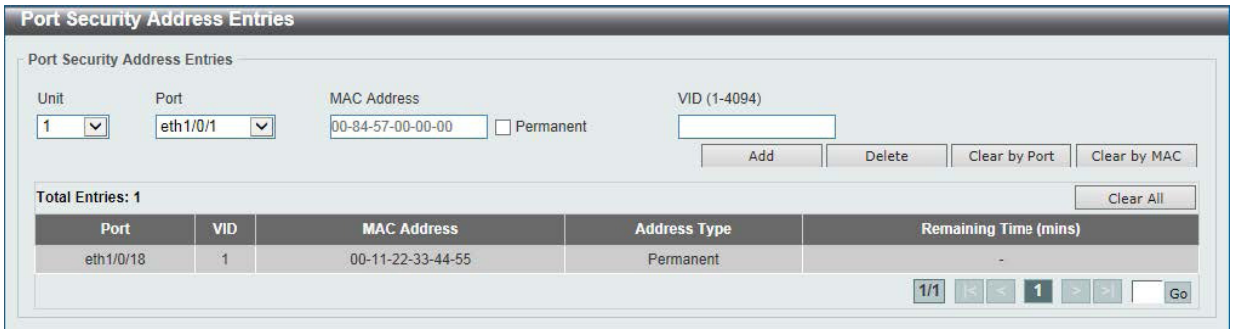


図 12-3　Port Security Address Entries 画面

以下の項目が表示されます。

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。
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、学習されたすべての MAC アドレスは、ユーザにより手動で削除されない限り保持されます。
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、指定条件に基づくエントリを追加します。
「Clear by Port」ボタンをクリックし、選択したポートに基づく情報を削除します。
「Clear by MAC」ボタンをクリックし、選択した MAC アドレスに基づく情報を削除します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を削除します。

エントリの削除

「Unit」「From Port/To Port」「MAC Address」を指定し、「Delete」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。

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

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。

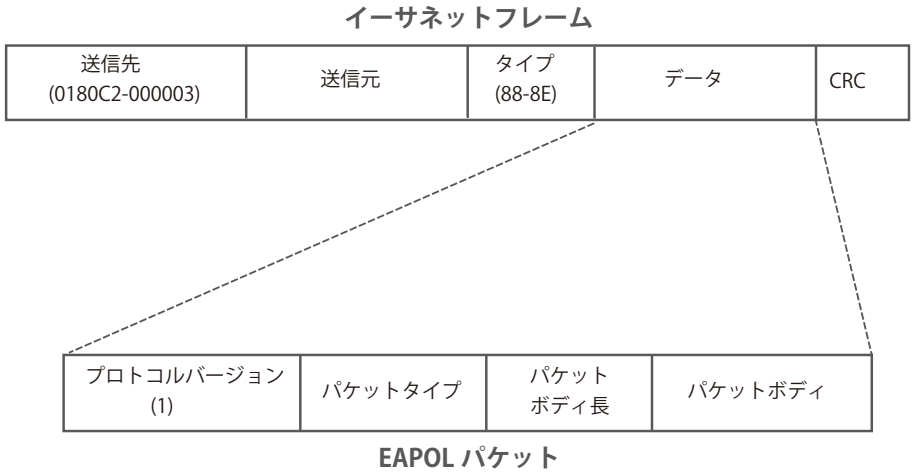


図 12-1　EAPOL パケット

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。

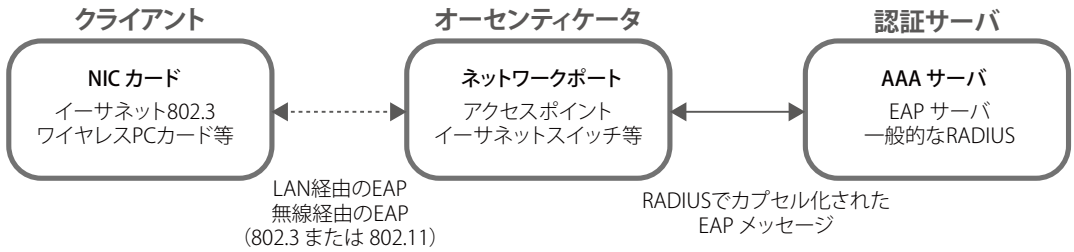


図 12-2　802.1X の 3 つの役割

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。

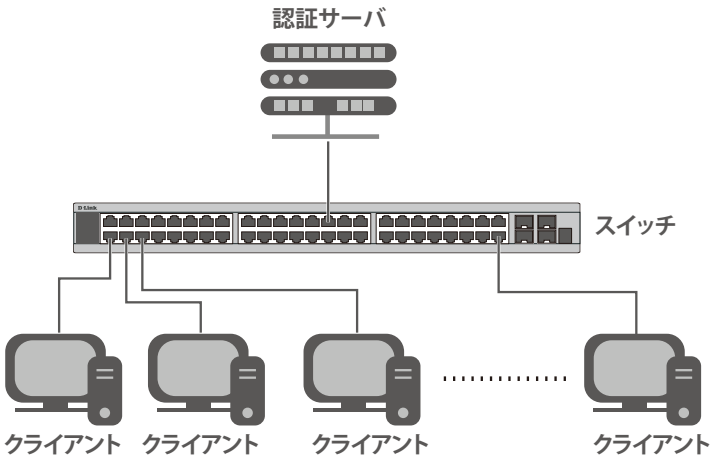


図 12-3　認証サーバ

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**）

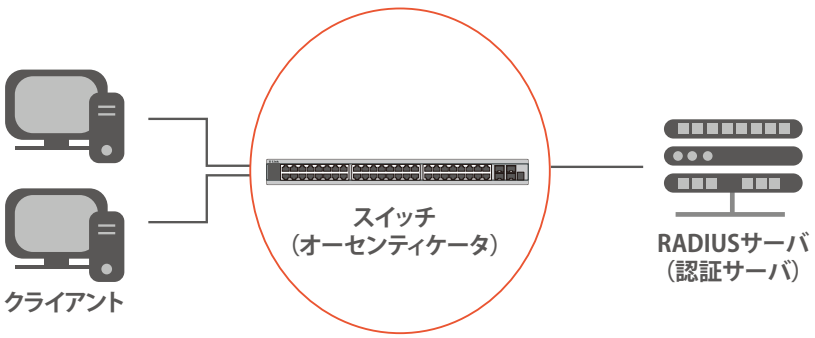


図 12-4　オーセンティケータ

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。

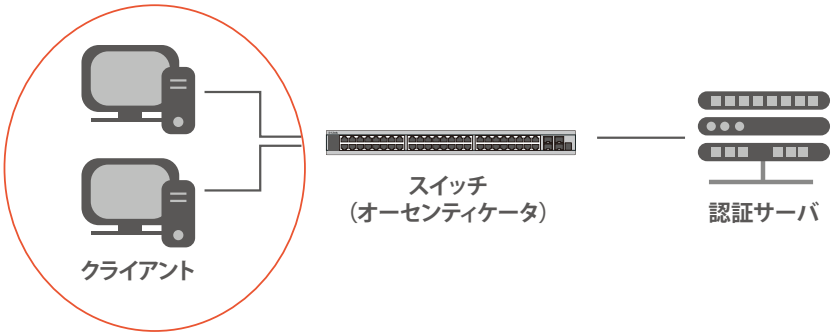


図 12-5　クライアント

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。

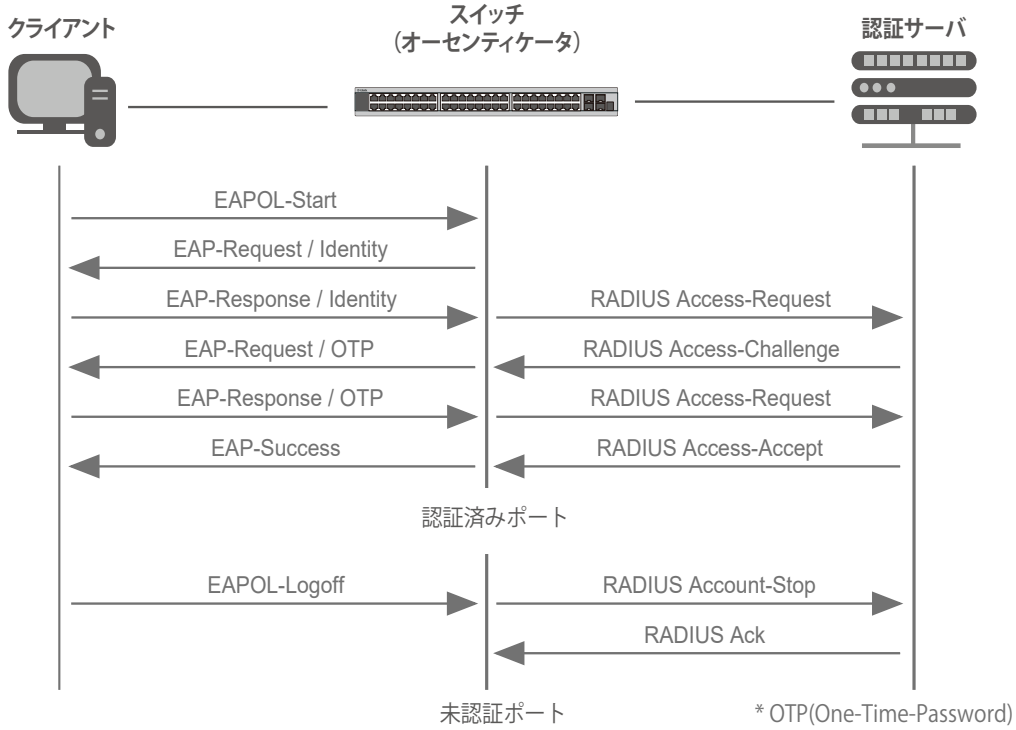


図 12-6　802.1X 認証プロセス

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 1000 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。

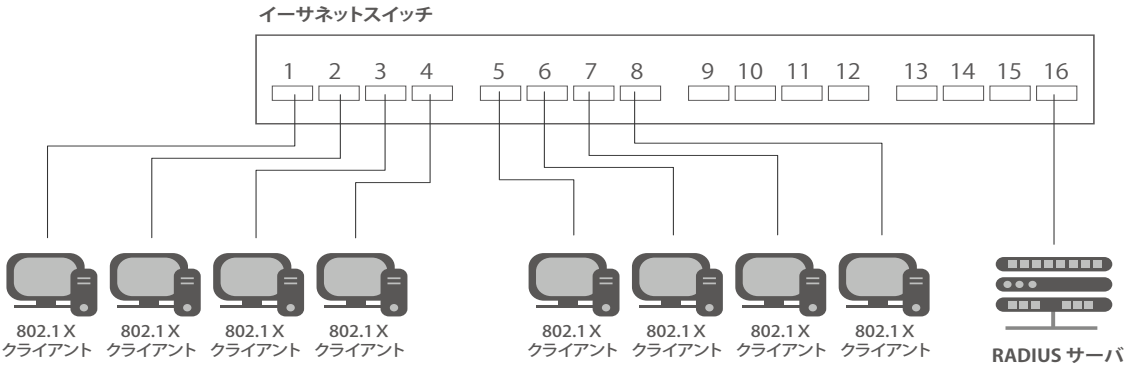


図 12-7　ポートベースアクセスコントロールのネットワーク構成例

■ 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。

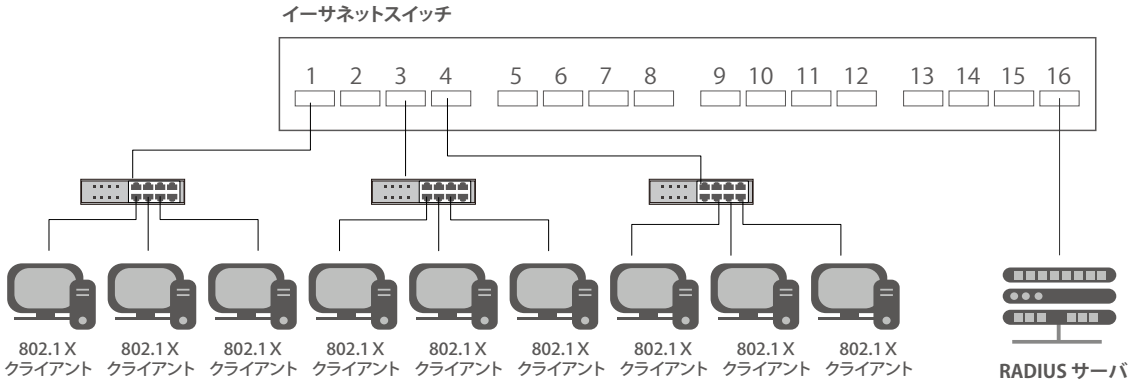


図 12-8　ホストベースアクセスコントロールのネットワーク構成例

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。

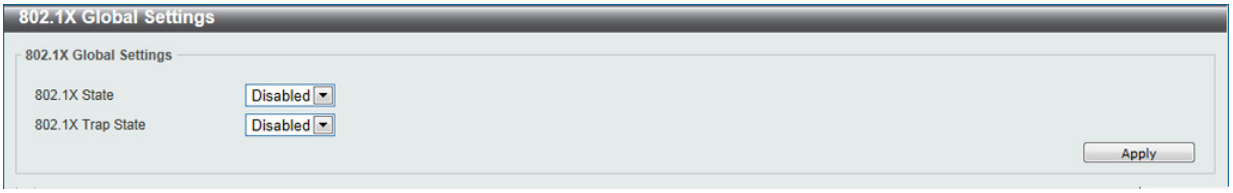


図 12-9　802.1X Global Settings 画面

以下の項目が表示されます。

項目	説明
802.1X State	802.1X 認証を有効 / 無効に設定します。
802.1X Trap State	802.1X トラップを有効 / 無効に設定します。

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

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。

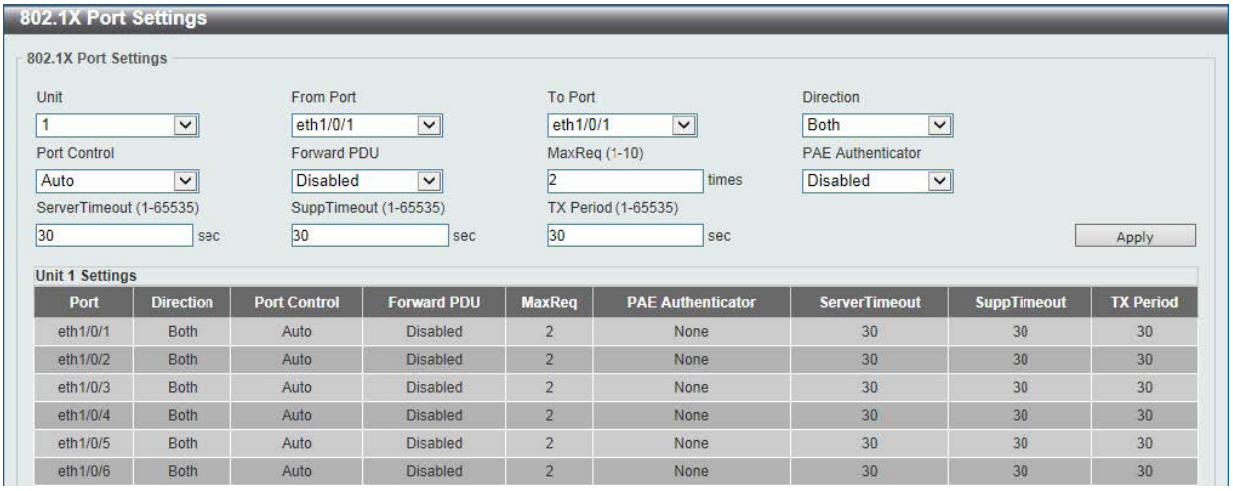


図 12-10　802.1X Settings 画面

以下の項目が表示されます。

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。
Direction	制御するトラフィックの方向を指定します。 • 「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。 • 「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処理します。（初期値）
Port Control	ポートの認証状態を指定します。 • 「ForceAuthorized（認証強制）」- 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（未認証強制）」- 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	バックエンドの認証ステートマシンが、認証プロセスを再開する前に、クライアントに対して Extensible Authentication Protocol（EAP）リクエストフレームを再送する最大回数を指定します。 • 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。 本項目では特定ポートを IEEE 802.1X Port Access Entity（PAE）オーセンティケータとして指定します。

項目	説明
ServerTimeout	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）
SuppTimeout	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）
TxPeriod	送信間隔を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）

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

Authentication Session Information（オーセンティケーションセッションの状態）

オーセンティケーションセッションの状態を表示します。

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

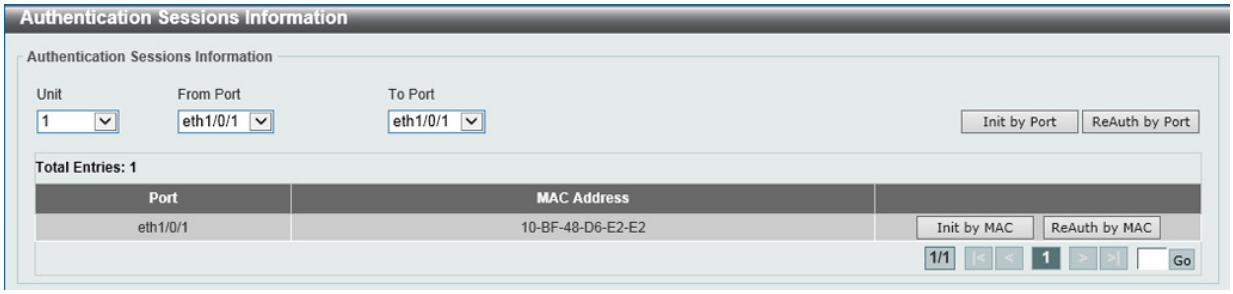


図 12-11　Authentication Session Information 画面

以下の項目が表示されます。

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

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

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

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。

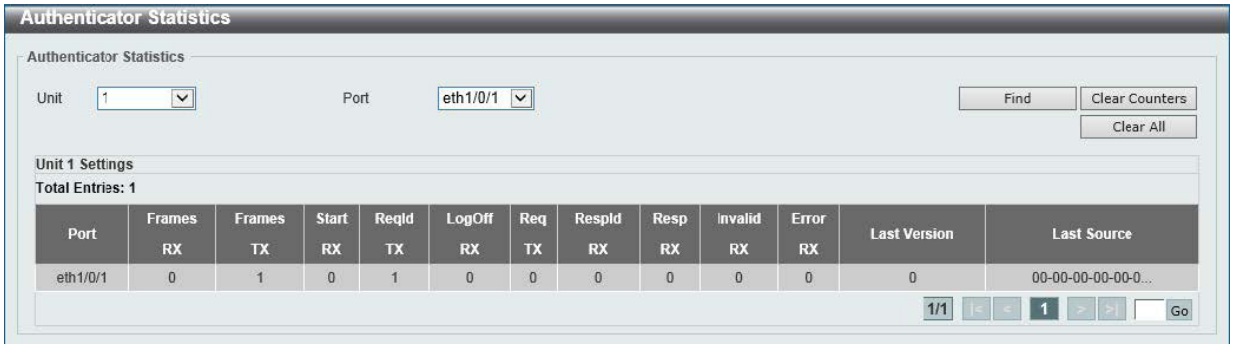


図 12-12　Authenticator Statics 画面

以下の項目が表示されます。

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

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。

「Clear Counters」ボタンをクリックして、指定条件に基づく情報を削除します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を削除します。

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

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 12-13　Authenticator Session Statistics 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。
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、入力した情報に基づくエントリを検出します。
「Clear Counters」ボタンをクリックし、選択に基づく情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

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。

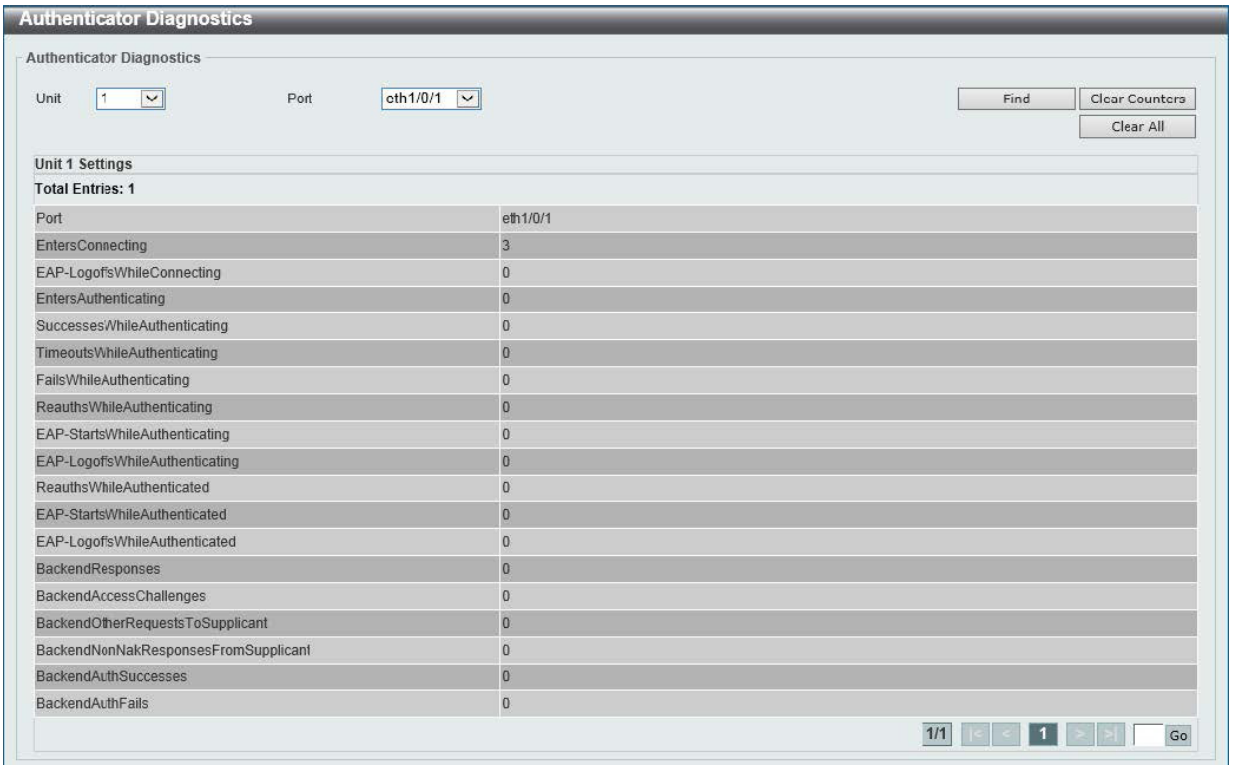


図 12-14　Authenticator Diagnostics 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

項目	説明
Port	表示するポート範囲を指定します。

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

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

AAA（AAA 設定）

本項目では AAA（Authentication、Authorization、Accounting）の有効 / 無効を行います。

AAA Global Settings（AAA グローバル設定）

本項目では AAA をグローバルに有効 / 無効に設定します。

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。

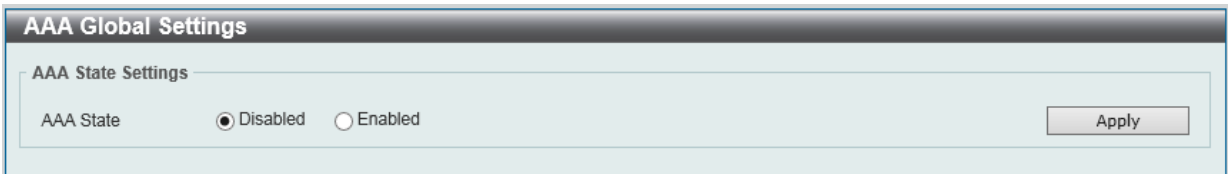


図 12-15　AAA Global Settings 画面

以下の項目が表示されます。

項目	説明
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。

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

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）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。

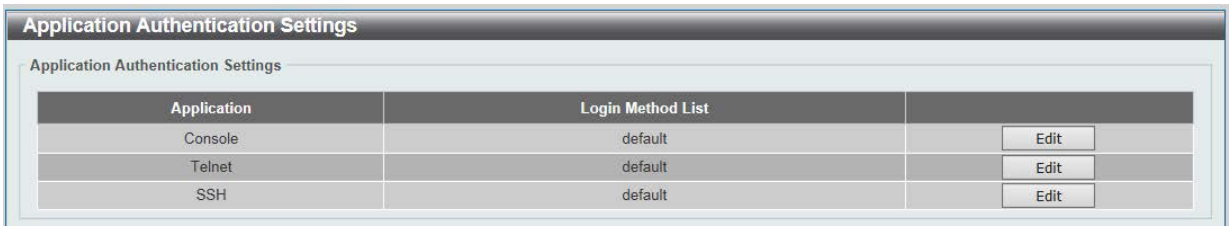


図 12-16　Application Authentication Settings 画面

エントリの編集
「Edit」をクリックすると、以下の画面が表示されます。

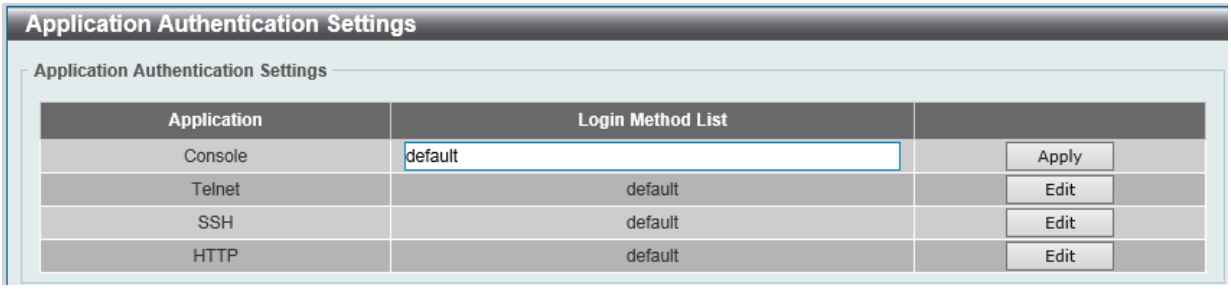


図 12-17　Application Authentication Settings (Edit) 画面

以下の項目が表示されます。

項目	説明
Login Method List	使用するログインメソッドリスト名を入力します。

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

Application Accounting Settings（アプリケーションアカウント設定）

アプリケーションアカウントを設定します。

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

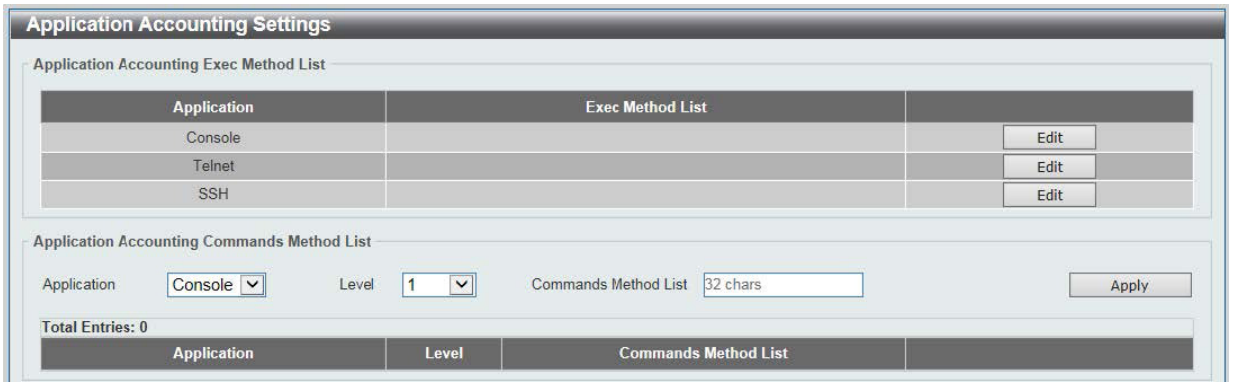


図 12-18　Application Accounting Settings 画面

エントリの編集

「Edit」をクリックすると、以下の画面が表示されます。

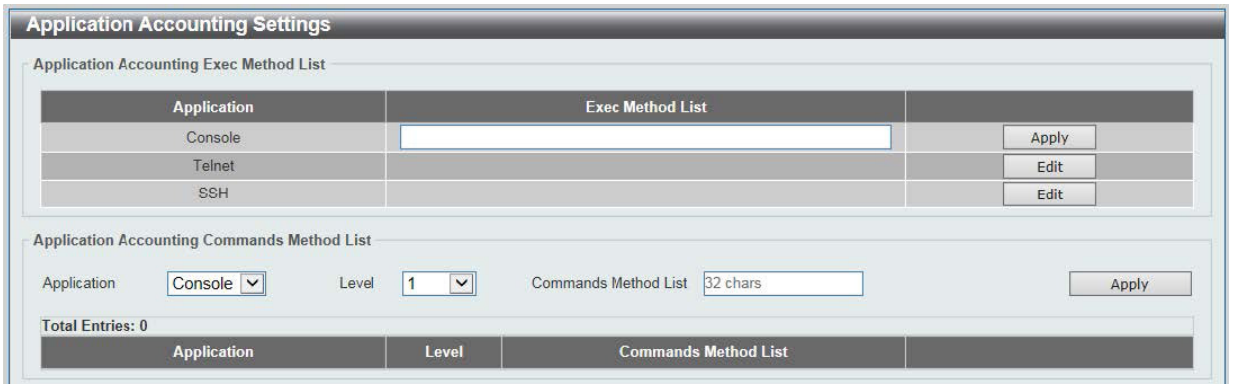


図 12-19　Application Accounting Settings (Edit) 画面

以下の項目が表示されます。

項目	説明
Exec Method List	使用する EXEC メソッドリスト名を入力します。
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。

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

「Delete」をクリックして、エントリを削除します。

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

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。

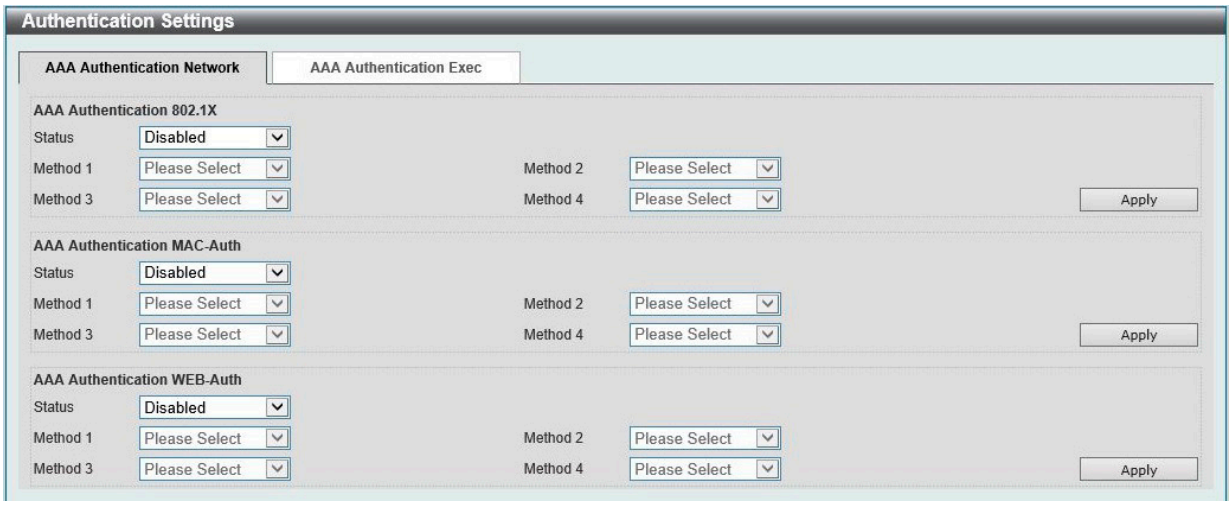


図 12-20　Authentication Settings -AAA Authentication Settings タブ画面

「AAA Authentication Network」タブ

「AAA Authentication Network」タブでは以下の設定を行います。

「AAA Authentication 802.1X」「AAA Authentication MAC-Auth」「AAA Authentication WEB-Auth」それぞれの項目において設定を行います。

項目	説明
Status	各項目の認証設定を有効 / 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」「local」「group」「radius」から選択します。 • 「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 文字までで入力可能です。 • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。

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

「AAA Authentication Exec」タブ

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

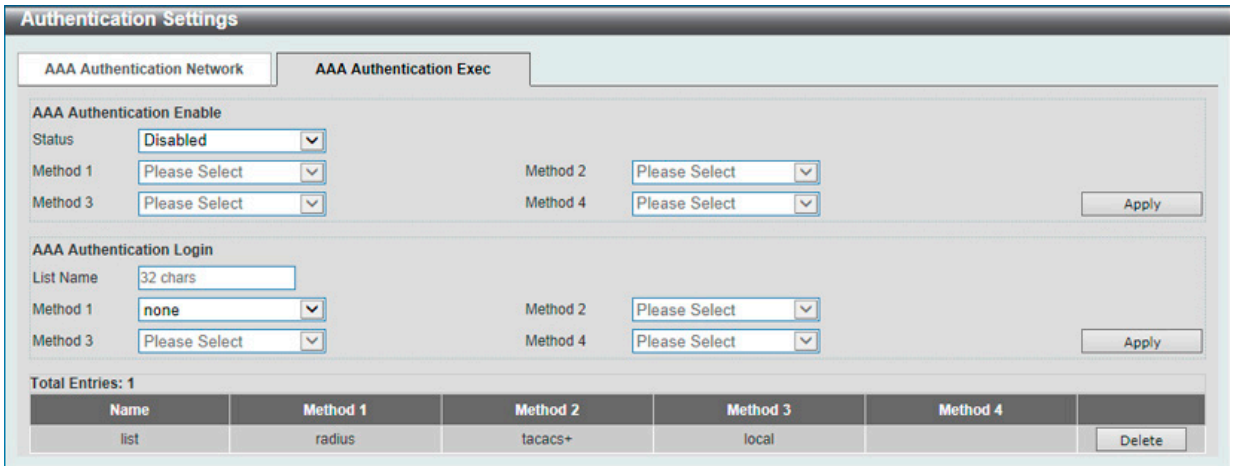


図 12-21　Authentication Settings -AAA Authentication Exec タブ画面

項目	説明
AAA Authentication Enable	
Status	AAA 認証設定を有効 / 無効に設定します。

項目	説明
Method 1 ～ 4	本設定項目のメソッドリストを選択します。「none」「enable」「group」「radius」「tacacs+」から選択します。 • 「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」- ローカルで有効な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 文字までで入力可能です。 • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。 • 「tacacs+」- TACACS+ サーバホストコマンドで定義された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」「local」「group」「radius」「tacacs+」から選択します。 • 「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 文字までで入力可能です。 • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。 • 「tacacs+」- TACACS+ サーバホストコマンドで定義されたサーバを使用します。

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

Accounting Settings（アカウンティング設定）

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、以下の画面を表示します。

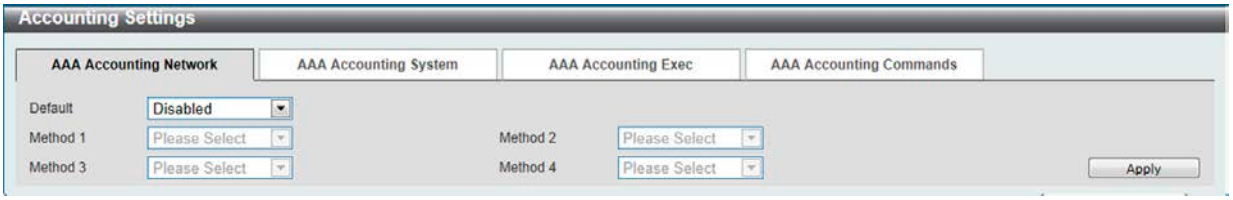


図 12-22　Accounting Settings 画面

「AAA Accounting Network」「AAA Accounting System」「AAA Accounting Exec」「AAA Accounting Commands」それぞれのタブで設定を行います。

項目	説明
「AAA Accounting Network」タブ	
Default	メソッドリストの有効 / 無効を指定します。
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+」
「AAA Accounting System」タブ	
Default	メソッドリストの有効 / 無効を指定します。
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+」
「AAA Accounting Exec」タブ	
List Name	使用する AAA アカウンティング EXE オプションのメソッドリストを入力します。
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+」
「AAA Accounting Commands」タブ	
Level	権限レベルを指定します。 • 設定可能範囲：1-15
List Name	使用する AAA アカウンティングコマンドオプションのメソッドリストを入力します。
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+」

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

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

RADIUS（RADIUS 設定）

RADIUS サーバの設定を行います。

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

RADIUS をグローバルに有効 / 無効にします。

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

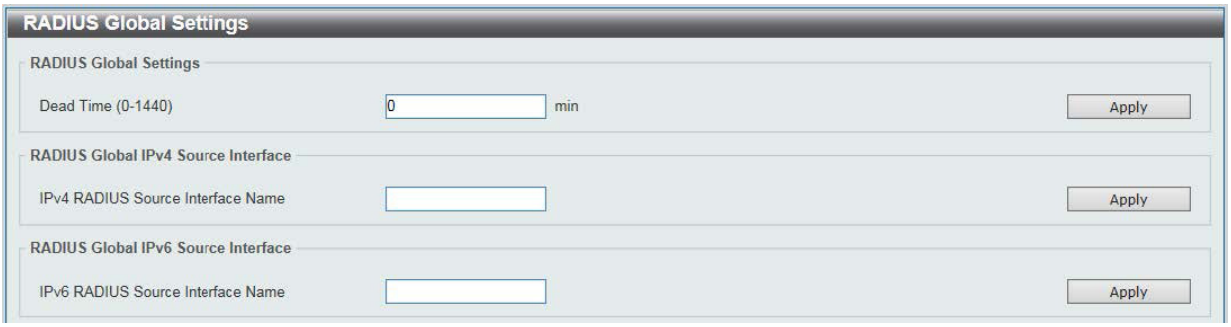


図 12-23　RADIUS Global Settings 画面

以下の項目が表示されます。

項目	説明
DeadTime	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。この設定により、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と連携する際、一度に一台のサーバと連携します。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、該当のサーバは「down」として認識され、「デッドタイム」タイマーが開始され、それ以後のリクエスト認証はデッドタイム時間が過ぎるまでスキップされます。 • 設定可能範囲：0-1440（分） • 初期値：0（分）
IPv4 RADIUS Source Interface Name	IPv4 RADIUS ソースインタフェース名を入力します。
IPv6 RADIUS Source Interface Name	IPv6 RADIUS ソースインタフェース名を入力します。

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

RADIUS Server Settings（RADIUS サーバの設定）

RADIUS サーバによって集約したユーザ管理や Sniffing やハッカーからの保護が可能になります。

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

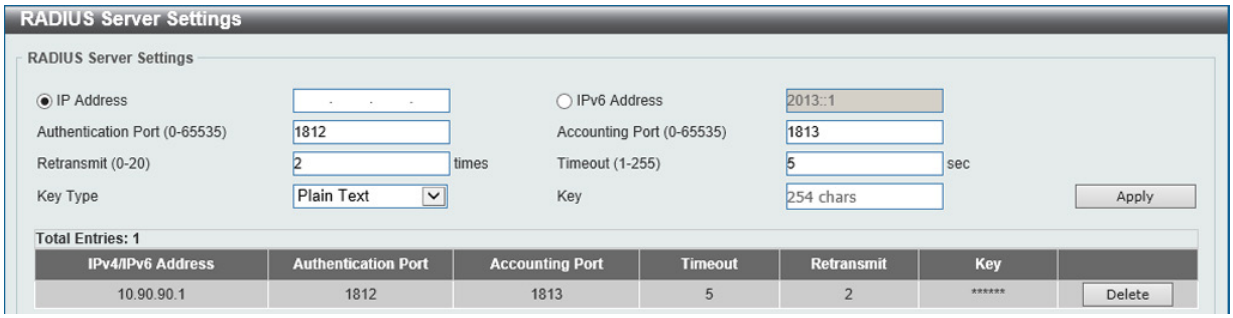


図 12-24　RADIUS Server Settings 画面

以下の項目が表示されます。

項目	説明
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。
Authentication Port	RADIUS 認証サーバの UDP ポートを入力します。認証を使用しない場合は「0」を指定します。 • 設定可能範囲：1-65535 • 初期値：1812

項目	説明
Accounting Port	RADIUS アカウントサーバのポートを入力します。認証を使用しない場合は「0」を指定します。 • 設定可能範囲：1-65535 • 初期値：1813
Retransmit	再送間隔を設定します。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（秒） • 初期値：2（秒）
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」「Encrypted」
Key	RADIUS サーバとの通信で使用する鍵を指定します。（32 文字以内）

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

注意　radius key にはスペースを含めることはできません。

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 12-25　RADIUS Group Server Settings 画面

以下の項目が表示されます。

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）
IP Address	グループサーバの IPv4 アドレスを入力します。
IPv6 Address	グループサーバの IPv6 アドレスを入力します。

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

詳細情報の表示

「Show Detail」をクリックすると、以下の画面が表示されます。

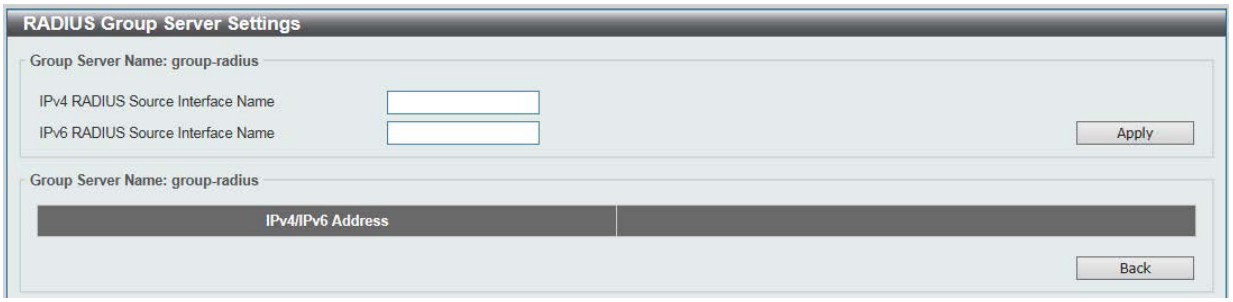


図 12-26　RADIUS Group Server Settings (Detail) 画面

以下の項目が表示されます。

項目	説明
IPv4 RADIUS Source Interface Name	IPv4 RADIUS ソースインタフェース名を入力します。
IPv6 RADIUS Source Interface Name	IPv6 RADIUS ソースインタフェース名を入力します。

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

「Back」をクリックして前の画面に戻ります。

RADIUS Statistic（RADIUS 統計情報）

RADIUS 統計情報の表示、設定を行います。

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



図 12-27　RADIUS Statistic 画面

以下の項目が表示されます。

項目	説明
Group Server Name	表示する 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、指定条件に基づく情報を削除します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を削除します。

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

TACACS+（TACACS+ 設定）

TACACS+ サーバの設定を行います。

TACACS+ Global Settings（TACACS+ サーバグローバル設定）

TACACS+ サーバをグローバルに有効 / 無効に指定します。

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



図 12-28　TACACS+ Global Settings 画面

以下の項目が表示されます。

項目	説明
IPv4 TACACS+ Source Interface Name	IPv4 TACACS+ ソースインタフェース名を入力します。

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

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。

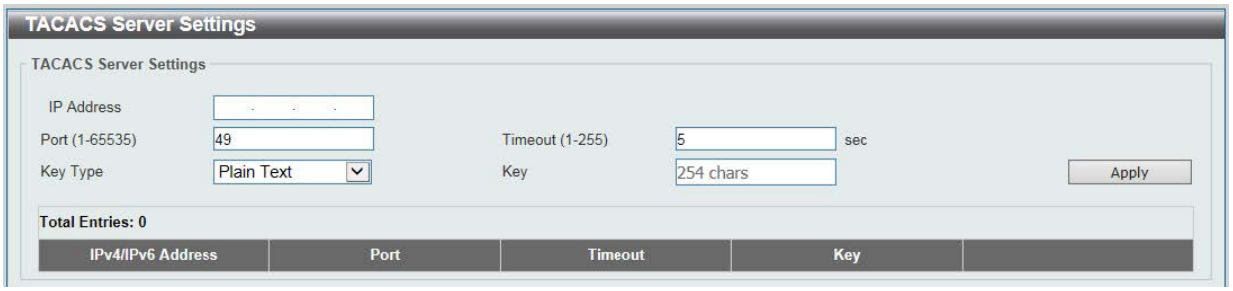


図 12-29　TACACS+ Server Settings 画面

以下の項目が表示されます。

項目	説明
IP Address	TACACS+ サーバの IPv4 アドレスを入力します。
Port	TACACS+ サーバのポートを入力します。 • 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」「Encrypted」
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）

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

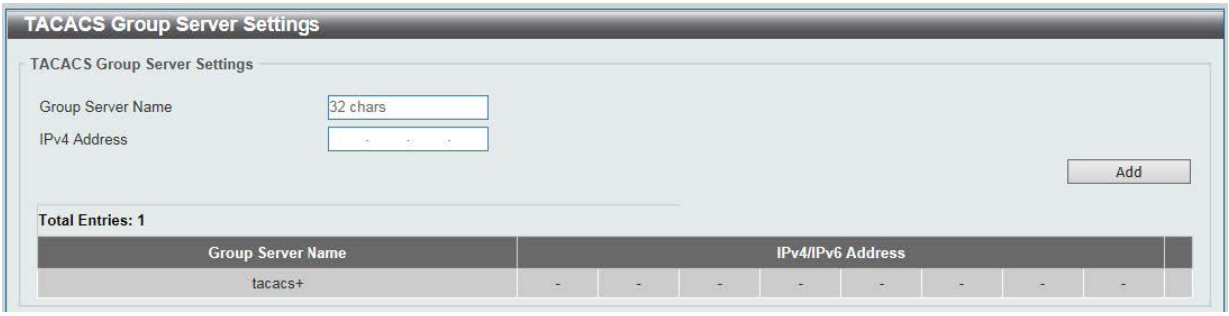


図 12-30　TACACS+ Group Server Settings 画面

以下の項目が表示されます。

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。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして、エントリを削除します。
「Show Detail」をクリックして、TACACS+ グループサーバの詳細情報を表示します。

TACACS+ Group Server Settings - Show Detail（TACACS+ グループサーバ詳細設定）



図 12-31　TACACS+ Group Server Settings - Show Detail 画面

以下の項目が表示されます。

項目	説明
IPv4 TACACS+ Source Interface Name	IPv4 TACACS+ ソースインタフェース名を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして、エントリを削除します。
「Back」をクリックして前の画面に戻ります。

TACACS+ Statistic（TACACS+ 統計情報）

TACACS+ 統計情報の表示、設定を行います。

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

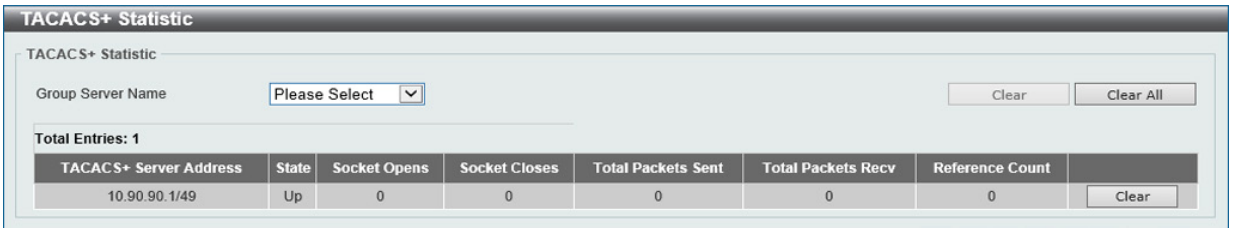


図 12-32　TACACS+ Statistic 画面

以下の項目が表示されます。

項目	説明
Group Server Name	TACACS+ グループサーバ名を選択します。

画面上部の「Clear」ボタンをクリックして、指定条件に基づく情報を削除します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を削除します。
テーブル上エントリ内の「Clear」ボタンをクリックし、エントリの情報を削除します。

IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）

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合させることにより、レイヤ間のデータ転送を可能にします。IP-MAC バインディングの第一の目的は、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。

補足　本機能は将来のファームウェアでサポート予定です。

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 スヌーピングについてグローバルに表示、設定します。

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 12-33　DHCP Snooping Global Settings 画面

以下の項目が表示されます。

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のリレーオプション 82 付き DHCP パケットのグローバルステータスを有効 / 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 スヌーピングステーションムーブを有効 / 無効に設定します。 本機能が有効な場合、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、新しい DHCP プロセスが同じ VLAN ID と MAC アドレスに属していることを検出した場合、他のポートへ移動することが可能です。

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

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。

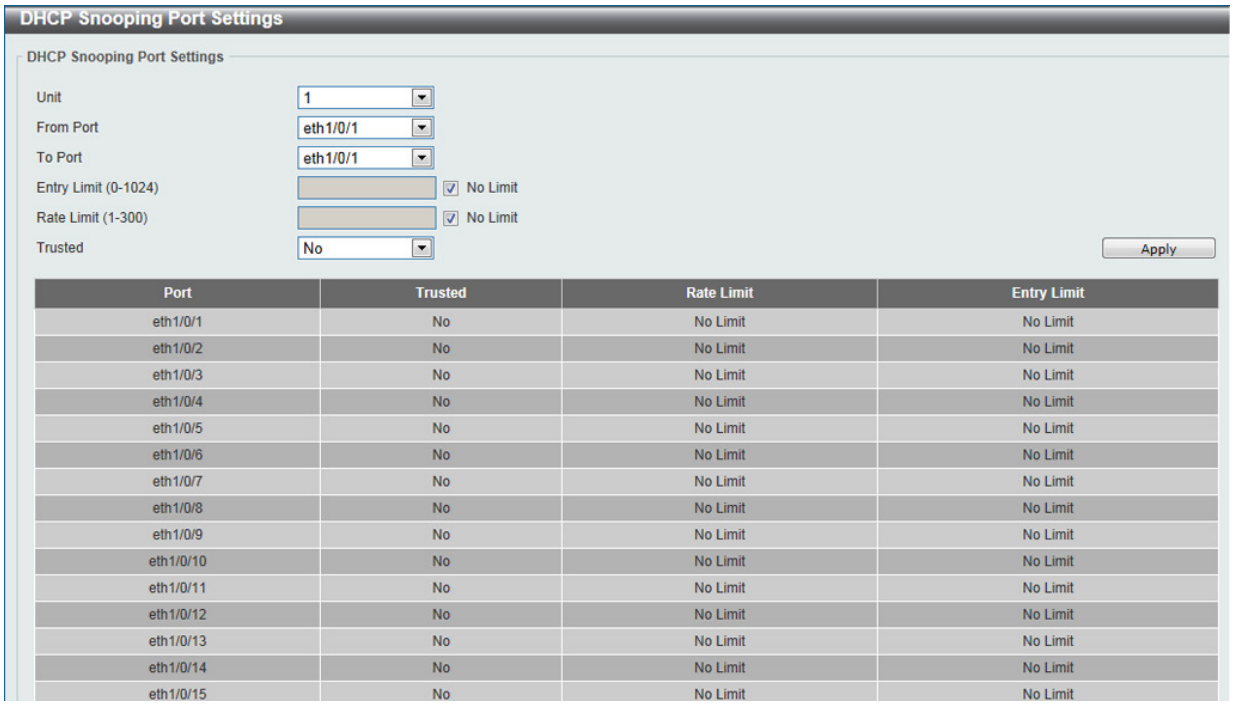


図 12-34　DHCP Snooping Port Settings 画面

以下の項目が表示されます。

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。
Entry Limit	エントリリミットの値を入力します。「No Limit」にチェックをすると、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」にチェックをすると、本機能は無効になります。 • 設定可能範囲：1-300
Trusted	トラストの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トラスト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アントラストとして設定します。DHCP スヌーピングは DHCP サーバとアントラスト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」

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

DHCP 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。

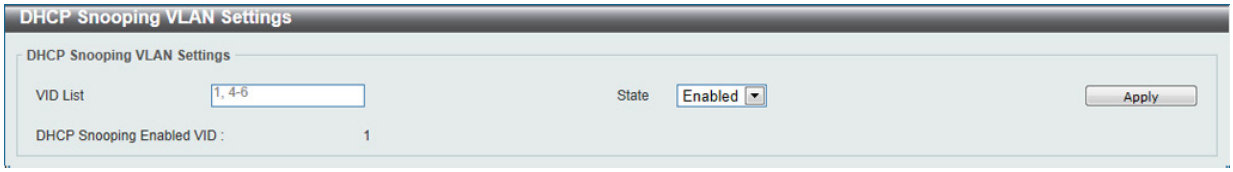


図 12-35　DHCP Snooping VLAN Settings 画面

以下の項目が表示されます。

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。

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

DHCP 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。

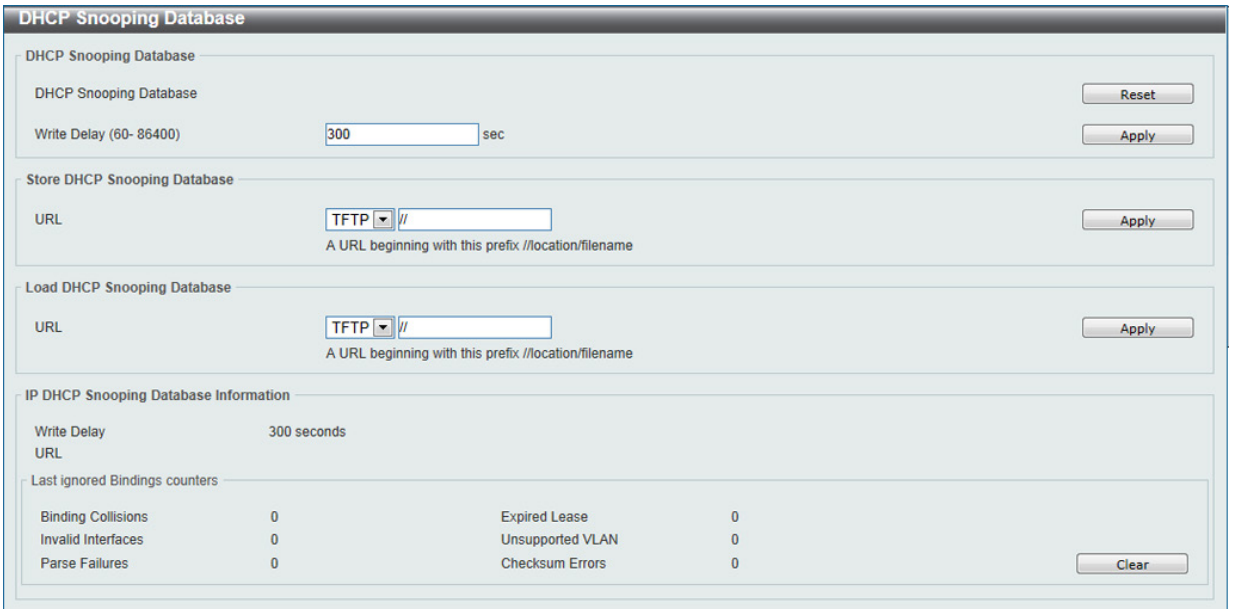


図 12-36　DHCP Snooping Database 画面

以下の項目が表示されます。

項目	説明
DHCP Snooping Database	
Write Delay	書き込み遅延の値を入力します。 • 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」

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear」ボタンをクリックして、カウンタ情報を削除します。
「Reset」ボタンをクリックして、入力した情報をリセットします。

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画面を表示します。

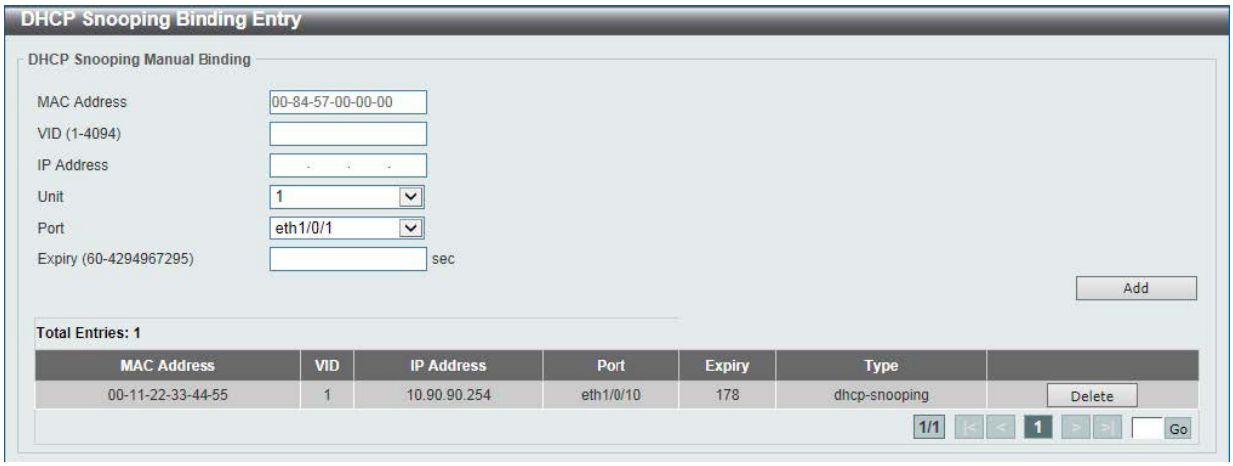


図 12-37　DHCP Snooping Binding Entry 画面

以下の項目が表示されます。

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。
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範囲を指定します。
Expiry	有効期限を入力します。 • 設定可能範囲：60-4294967295（秒）

「Add」をクリックして、設定内容に基づくエントリを追加します。
「Delete」をクリックして、エントリを削除します。

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

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。

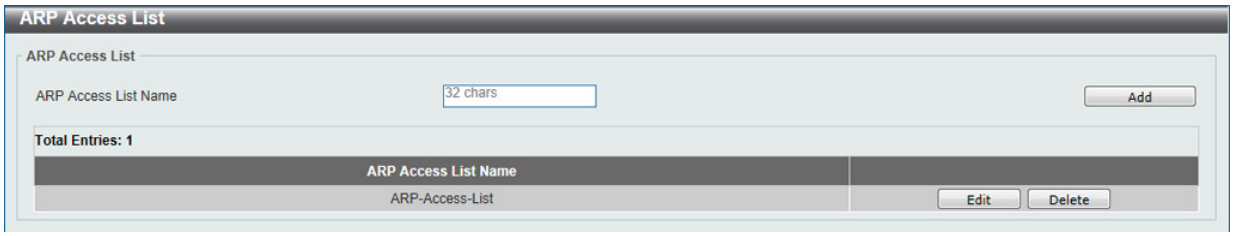


図 12-38　ARP Access List 画面

以下の項目が表示されます。

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」をクリックして、設定内容に基づくエントリを追加します。
「Delete」をクリックして、エントリを削除します。

エントリの編集

「Edit」ボタンをクリックすると、以下の画面が表示されます。

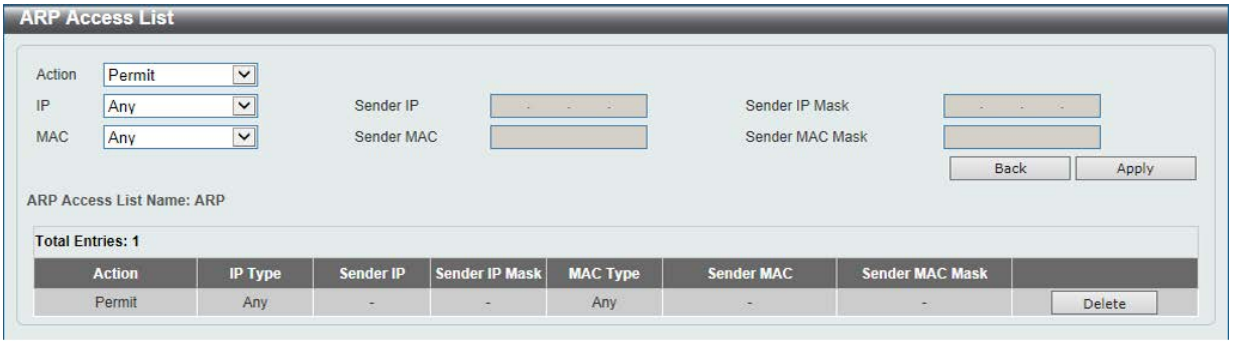


図 12-39　ARP Access List - Edit 画面

以下の項目が表示されます。

項目	説明
Action	実行する動作を指定します。 • 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	送信元 IP アドレスを「Host」「IP with Mask」から選択した後、使用する送信元 IP アドレスを入力します。
Sender IP Mask	「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	送信元 MAC アドレスを「Host」「MAC with Mask」から選択した後、使用する送信元 MAC アドレスを入力します。
Sender MAC Mask	「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。

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

「Delete」をクリックして、エントリを削除します。

「Back」をクリックして前のページに戻ります。

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。

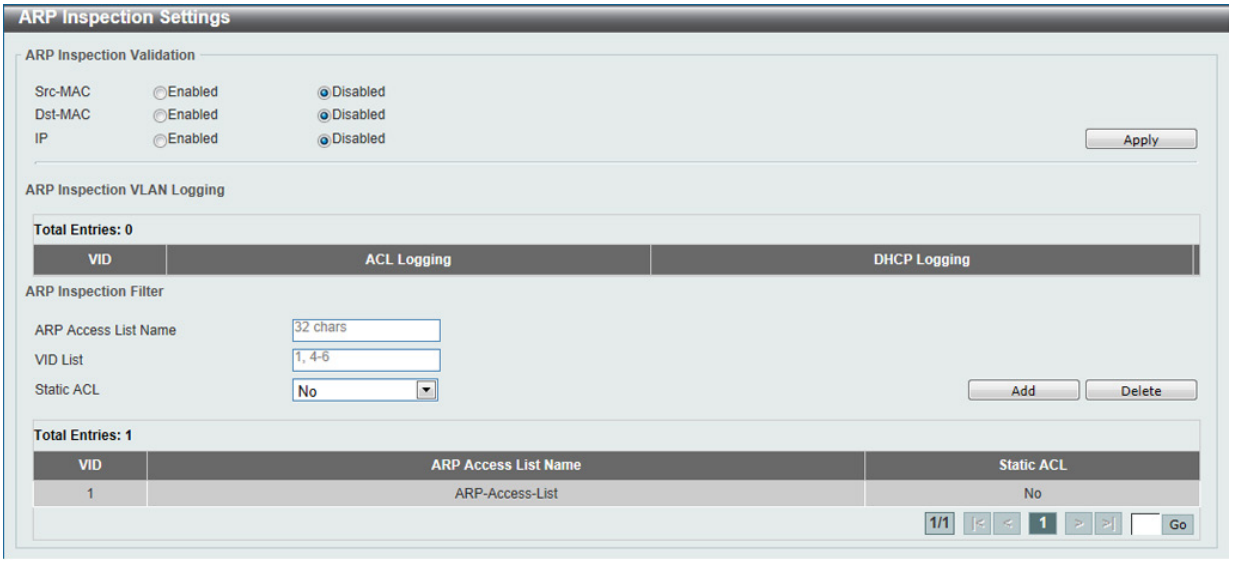


図 12-40　ARP Inspection Settings 画面

以下の項目が表示されます。

項目	説明
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 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。

項目	説明
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 アドレスの 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。

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

本画面の「ARP Inspection Filter」には以下の項目があります。

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）
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。

「Add」をクリックして、指定条件に基づくエントリを追加します。
「Delete」をクリックして、エントリを削除します。

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

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。

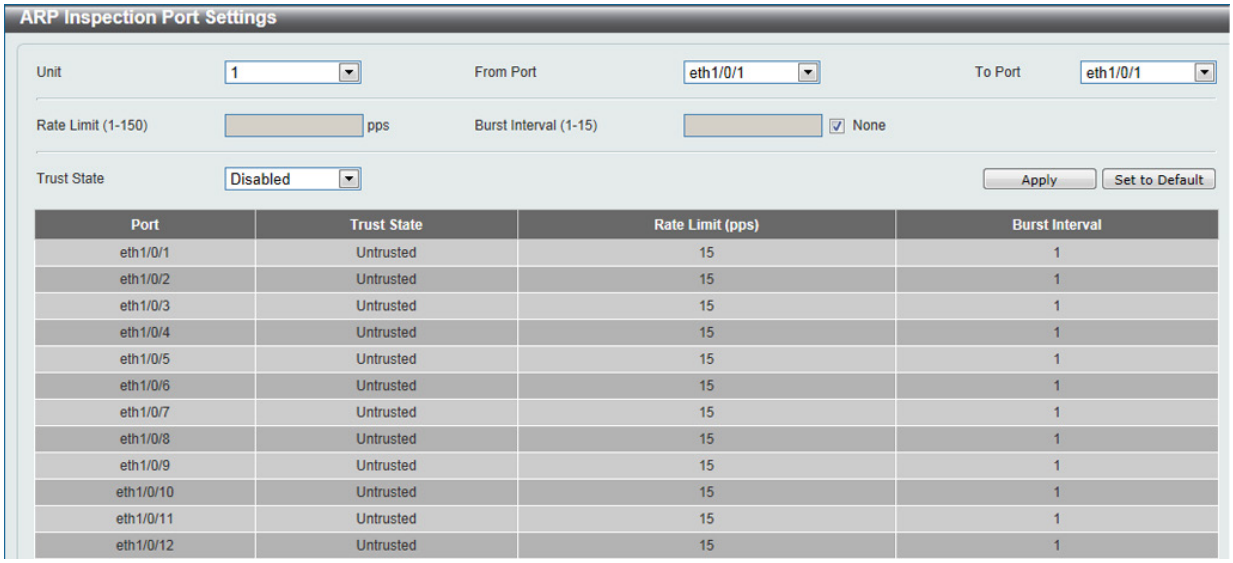


図 12-41　ARP Inspection Port Settings 画面

以下の項目が表示されます。

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。
Rate Limit	レート制限の値を入力します。 • 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」にチェックをす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。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Set to Default」ボタンをクリックすると、設定内容は初期値に戻ります。

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。

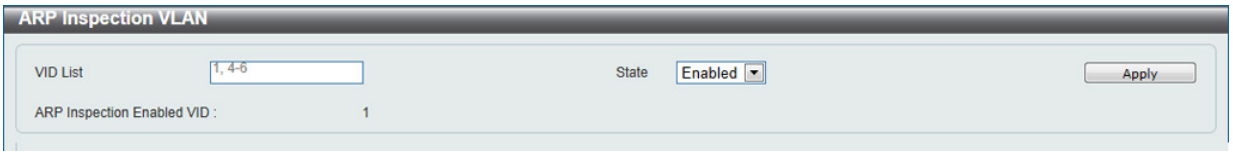


図 12-42　ARP Inspection VLAN 画面

以下の項目が表示されます。

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。

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

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。

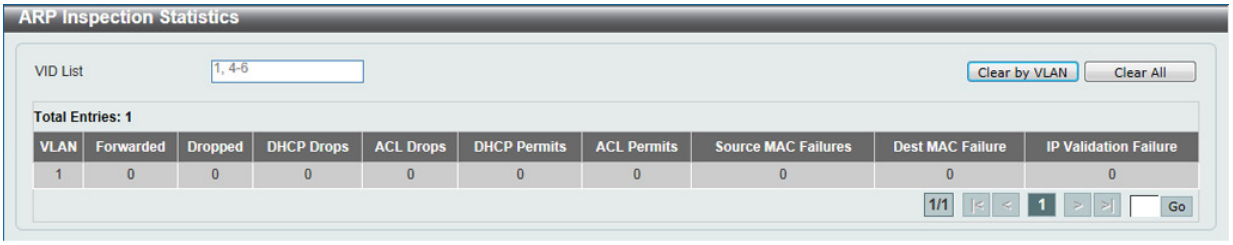


図 12-43　ARP Inspection Statistics 画面

以下の項目が表示されます。

項目	説明
VID List	設定する VLAN ID リストを入力します。

「Clear by VLAN」ボタンをクリックして、指定 VLAN ID に基づく情報を削除します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を削除します。

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

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 12-44　ARP Inspection Log 画面

以下の項目が表示されます。

項目	説明
Log Buffer	使用するログバッファの値を入力します。 • 設定可能範囲：1-1024 • 初期値：32

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear Log」ボタンをクリックして、ログを削除します。

IP Source Guard（IP ソースガード）

注意 IP ソースガードを使用する場合は、必ず、有効にするポートに所属しているすべての VLAN が”DHCP Snooping VLAN Settings”のページで有効に設定されている必要があります。

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 12-45　IP Source Guard Port Settings 画面

以下の項目が表示されます。

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。

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

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。

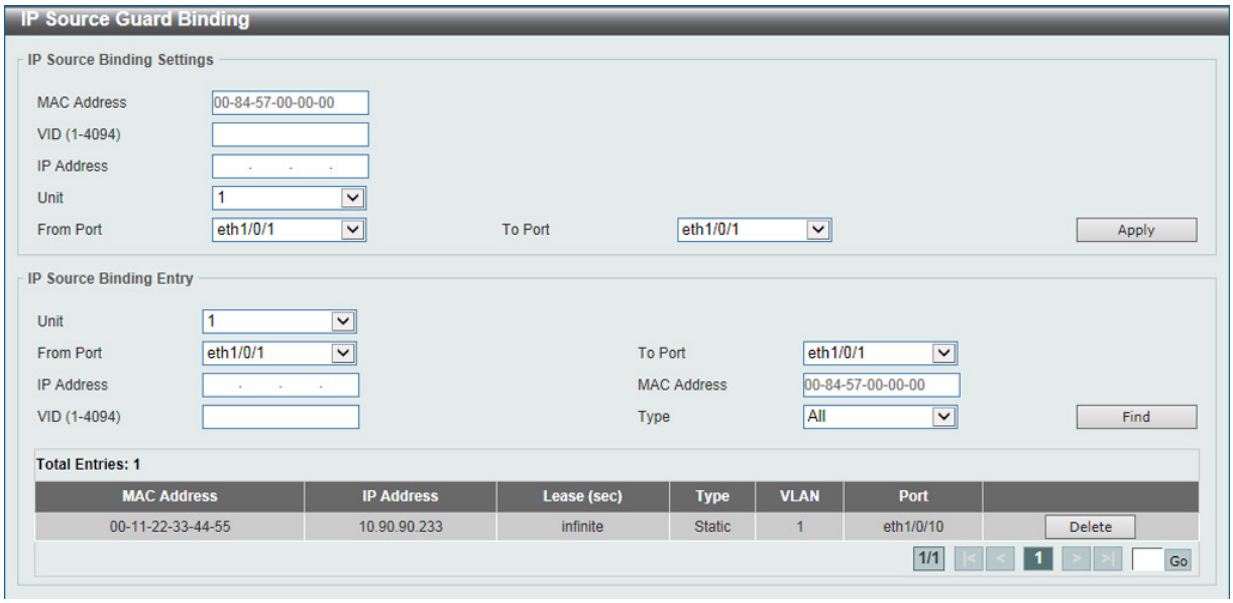


図 12-46　IP Source Guard Binding 画面

以下の項目が表示されます。

IP Source Binding Settings

項目	説明
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。

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

IP Source Binding Entry

項目	説明
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習得された 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。

「Delete」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、指定条件に基づくエントリを検索 / 表示します。

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

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 12-47　IP Source Guard HW Entry 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを指定します。
From Port/ To 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、指定条件に基づくエントリを検索 / 表示します。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Advanced Settings（アドバンス設定）

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。

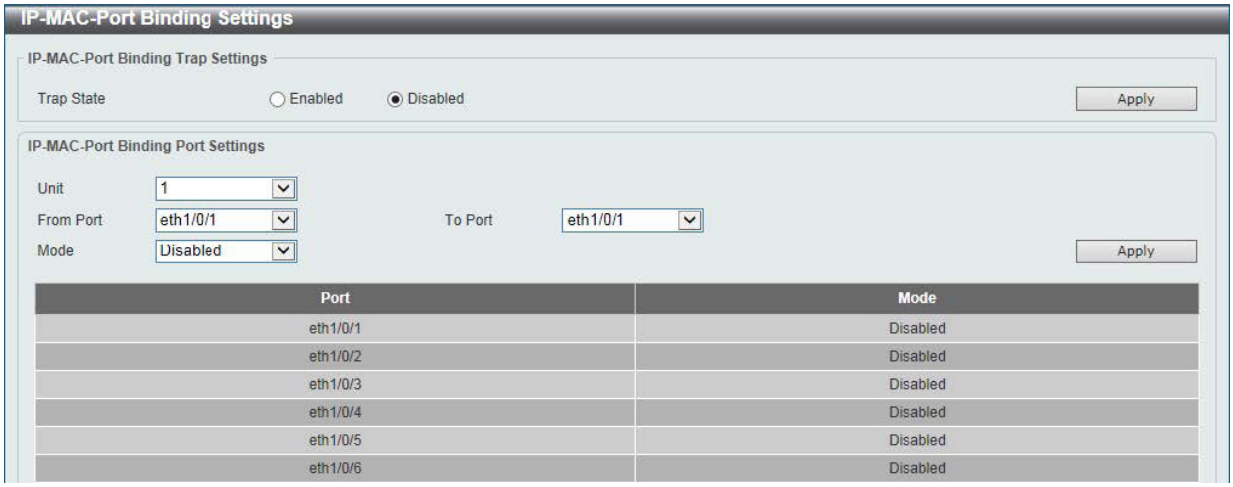


図 12-48　IP-MAC-Port Binding Settings 画面

以下の項目が表示されます。

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。 • 選択肢：「Disabled」「Strict」「Loose」 ポートが「IMPB strict-mode」のアクセスコントロールを有効にしている場合： 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。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。 ポートが「IMPB loose-mode」のアクセスコントロールを有効にしている場合： 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。

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

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。

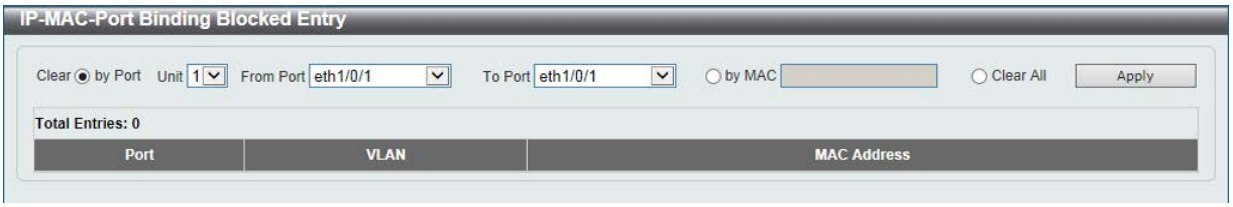


図 12-49　IP-MAC-Port Binding Blocked Entry 画面

以下の項目が表示されます。

項目	説明
Clear by Port	選択ポートに基づいたエントリテーブルをクリアします。
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を指定します。
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。項目欄に 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。

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

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。

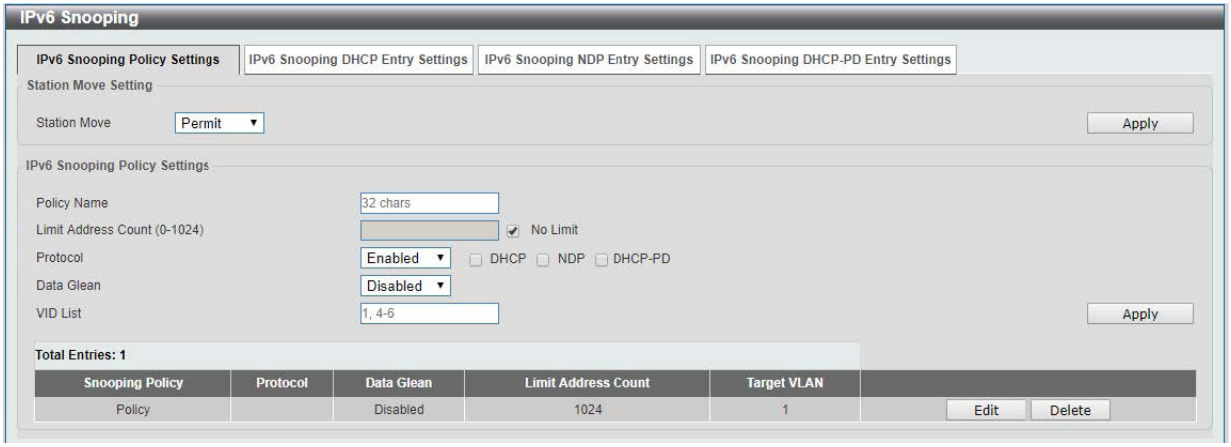


図 12-50　IPv6 Snooping 画面

以下の項目が表示されます。

項目	説明
Station Move Setting	
Station Move	ステーション移行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：0-1024

項目	説明
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 パケットのアドレスがスヌーピングされます。 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 スヌーピングはバインディングデータベースを作成します。 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 アドレスをアサインする前に、ホストは「Duplicate Address Detection」（DAD）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) も、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。
Data Glean	「data-glean」機能を有効 / 無効に設定します。状況によっては（DAD-NS パケットの損失やスイッチの再起動など）有効な IPv6 アドレスがバインディングテーブルで検出できず、それらのデバイス向け / からのトラフィックが IPv6 ソースガードで拒否されます。「data-glean」機能により IPv6 Duplicate Address Detection (DAD) を使用して紛失した IPv6 アドレスを回復する手段を提供します。
VID List	使用する VLAN ID リストを入力します。

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして、エントリを削除します。
「Edit」をクリックして、エントリを編集します。

IPv6 Snooping DHCP Entry Settings（IPv6 スヌーピング DHCP エントリ設定）

「IPv6 Snooping DHCP Entry Settings」タブを選択すると、以下の画面が表示されます。

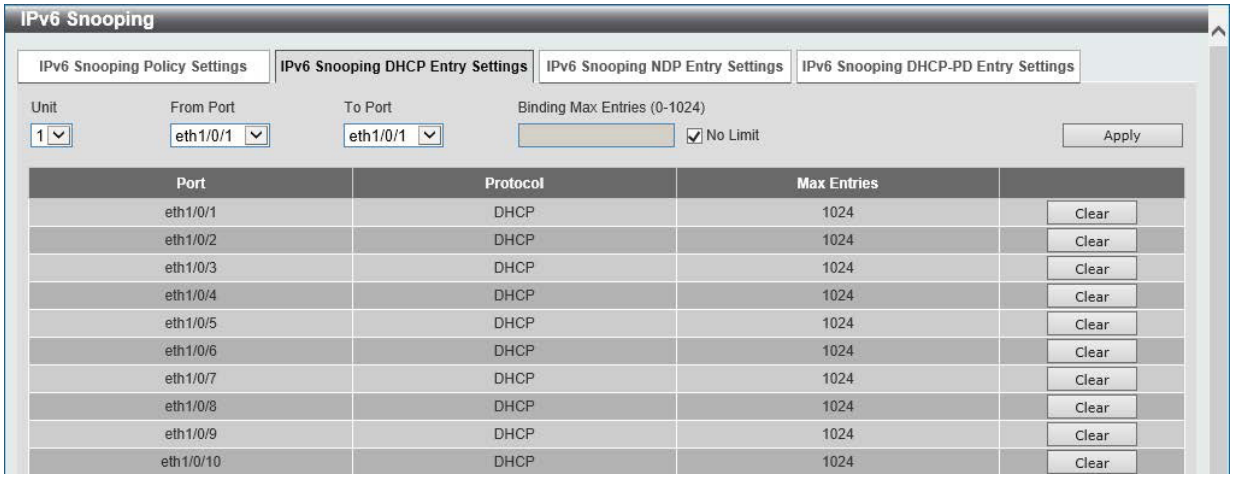


図 12-51　IPv6 Snooping DHCP Entry Settings 画面

以下の項目が表示されます。

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。
Binding Max Entries	許可される 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。 • 設定可能範囲：0-1024

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear」をクリックして、DHCPv6 スヌーピングクエリを指定ポートから削除します。

IPv6 Snooping NDP Entry Settings（IPv6 スヌーピング NDP エントリ設定）

「IPv6 Snooping NDP Entry Settings」タブを選択すると、以下の画面が表示されます。

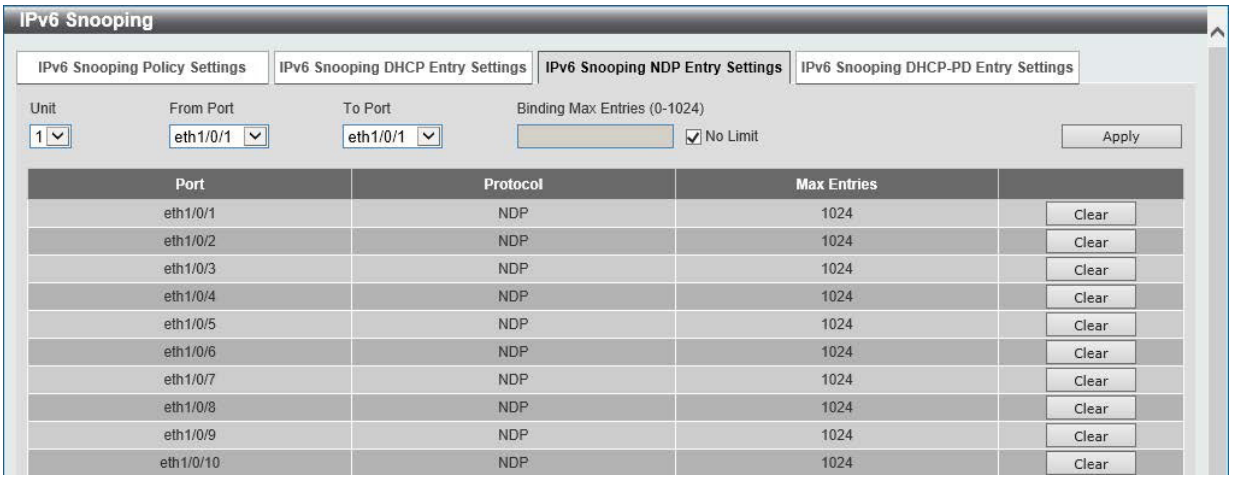


図 12-52　IPv6 Snooping NDP Entry Settings 画面

以下の項目が表示されます。

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。
Binding Max Entries	許可される 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。 • 設定可能範囲：0-1024

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear」をクリックして、ND スヌーピングクエリを指定ポートから削除します。

IPv6 Snooping DHCP-PD Entry Settings（IPv6 スヌーピング DHCP-PD エントリ設定）

「IPv6 Snooping DHCP-PD Entry Settings」タブを選択すると、以下の画面が表示されます。

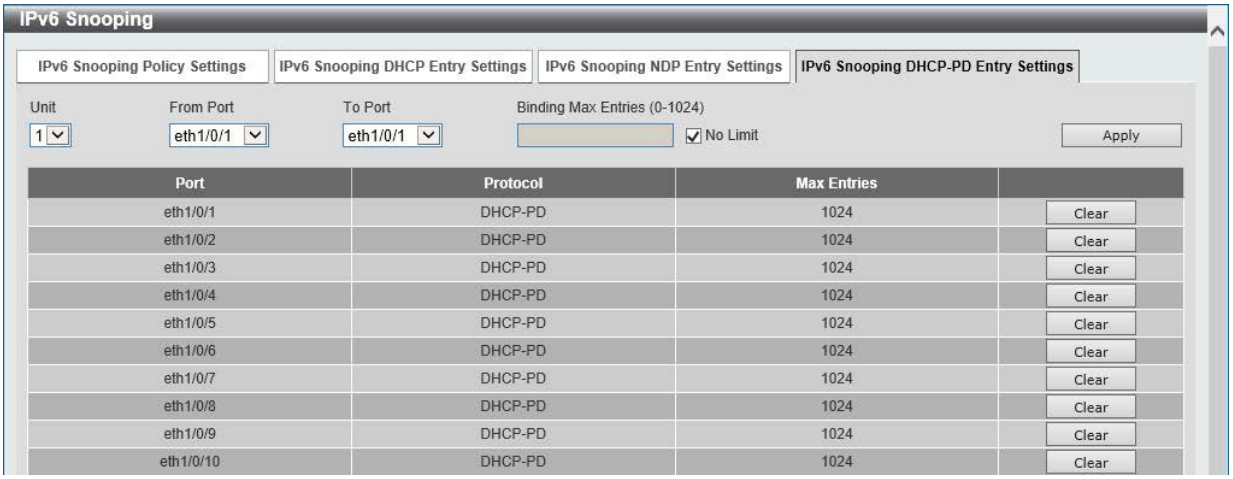


図 12-53　IPv6 Snooping DHCP-PD Entry Settings 画面

以下の項目が表示されます。

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。
Binding Max Entries	許可される 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。 • 設定可能範囲：0-1024

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear」をクリックして、DHCPv6 PD スヌーピングクエリを指定ポートから削除します。

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。

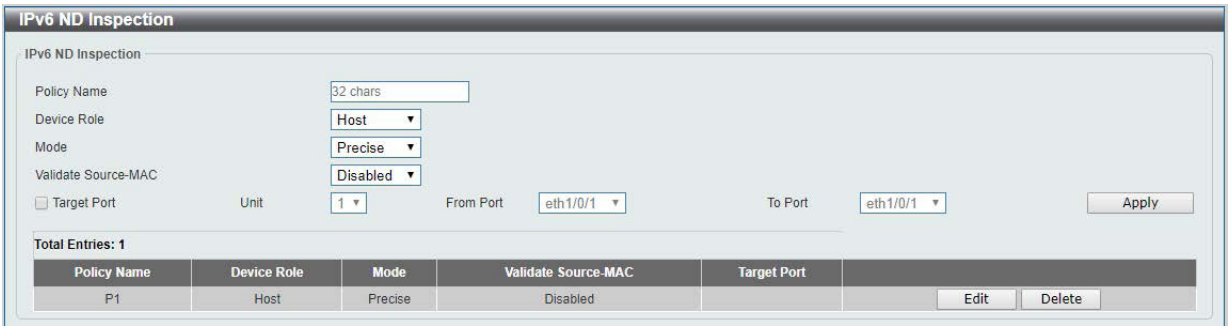


図 12-54　IPv6 ND Inspection 画面

以下の項目が表示されます。

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスロールを選択します。 • 「Host」- 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」- 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。 • 「Precise」- Precise モードを使用します。ND インスペクションではターゲットアドレスが DANA/NA パケット内の送信元アドレスと同じかどうかが検証されます。 • 「Fuzzy」- Fuzzy モードを使用します。ND インスペクションではバインディングテーブル内にターゲット及び送信元アドレスの両方が存在するかどうか検証します。
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	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。

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

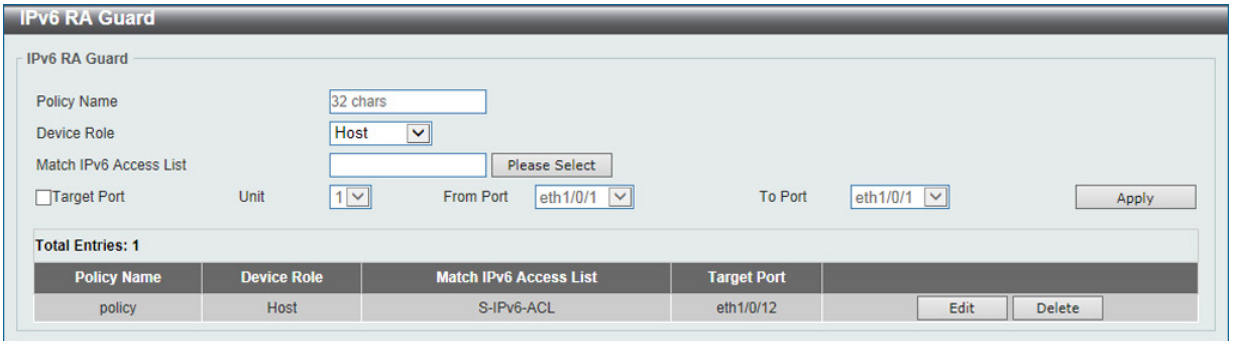


図 12-55　IPv6 RA Guard 画面

以下の項目が表示されます。

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスロールを選択します。「Host」「Router」から選択します。 • 「Host」- RA パケットはすべてブロックされます。（初期値） • 「Router」- RA パケットはポート宛ての 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、選択します。「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	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。

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

「Please Select」をクリックすると次の画面が表示されます。



図 12-56　IPv6 RA Guard (Please Select) 画面

設定するエントリを選択し「OK」をクリックします。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

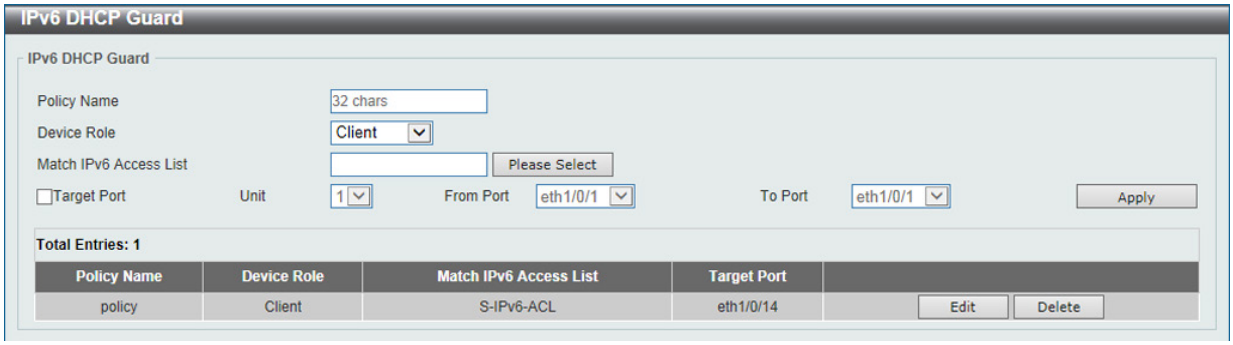


図 12-57　IPv6 DHCP Guard 画面

以下の項目が表示されます。

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスロールを選択します。 • 「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宛ての 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または選択します。「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	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。

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

「Please Select」をクリックすると次の画面が表示されます。



図 12-58　IPv6 Guard (Please Select) 画面

設定するエントリを選択し「OK」をクリックします。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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 12-59　IPv6 Source Guard Settings 画面

以下の項目が表示されます。

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）」
Link Local Traffic	リンクローカルアドレスによって送信された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）」
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	プリフィ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 プリフィクス検証機能を実行します。
IPv6 Source Guard Attach Policy Settings	
Target Port	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。

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

IPv6 Neighbor Binding（IPv6 ネイババインディング）

IPv6 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。

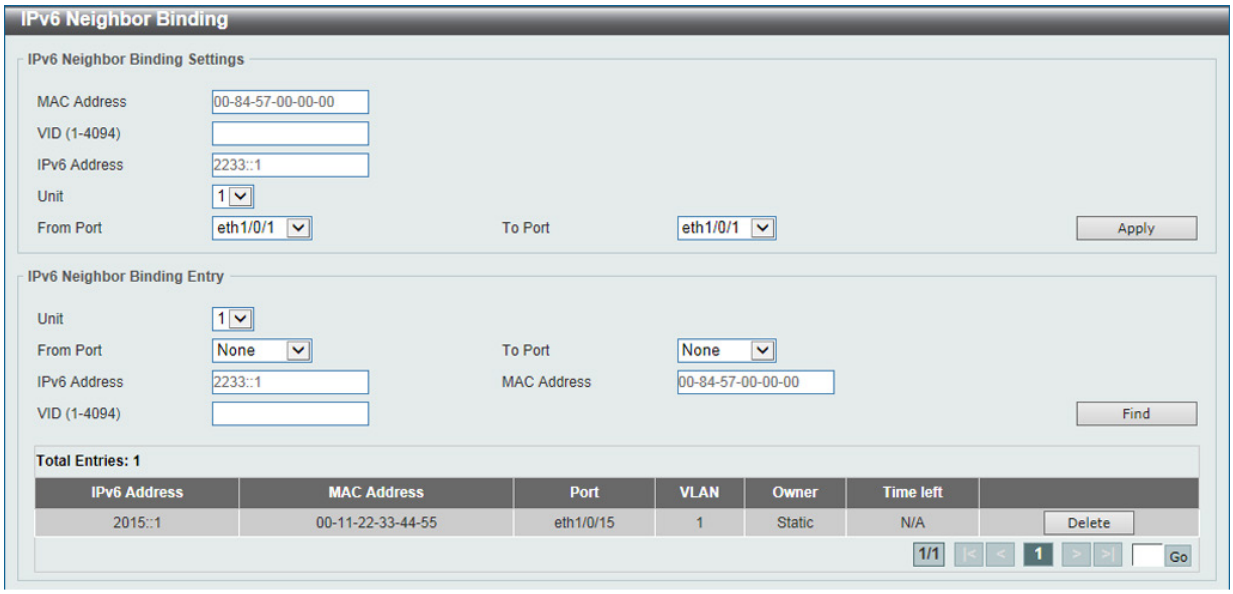


図 12-60　IPv6 Neighbor Binding 画面

以下の項目が表示されます。

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	表示するユニットを指定します。
From Port/ To Port	表示するポートを指定します。
IPv6 Address	表示する IPv6 アドレスを入力します。
MAC Address	表示する MAC アドレスを入力します。
VID	表示する VLAN ID を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして、エントリを削除します。
「Find」をクリックして、指定条件に基づくエントリを表示します。

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

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により 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グローバル設定の表示、設定をします。

Security > **DHCP Server Screening** > **DHCP Server Screening Global Settings** の順にメニューをクリックして画面を表示します。

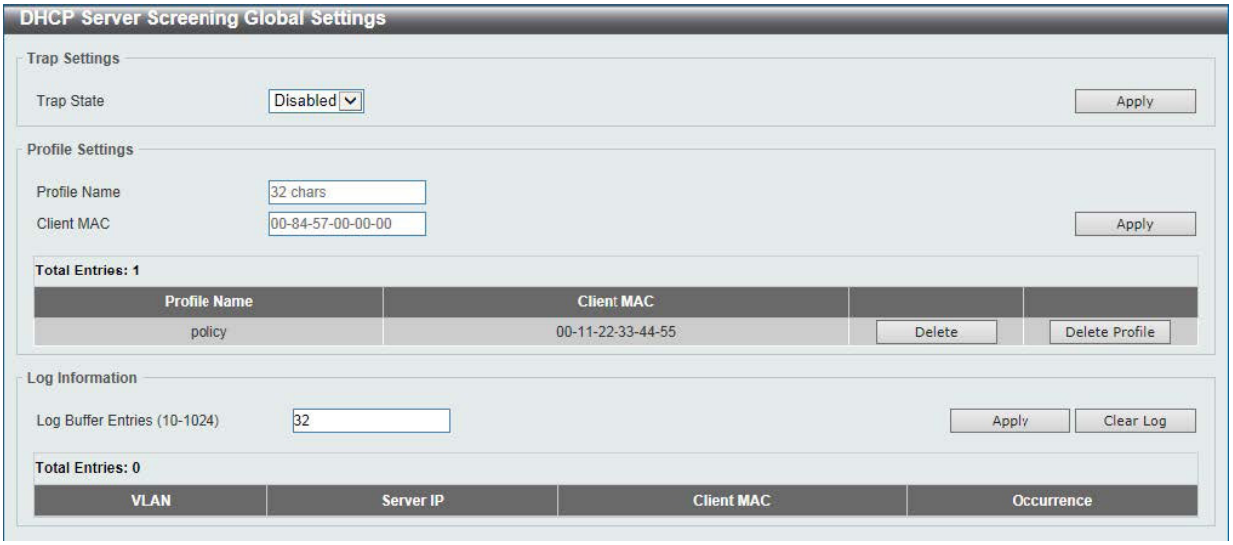


図 12-61　DHCP Server Screening Global Settings 画面

以下の項目が表示されます。

Trap Settings

項目	説明
Trap State	DHCP サーバスクリーニングトラップ機能を有効 / 無効に設定します。

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

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）
Client MAC	クライアント MAC アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして、プロファイルから MAC アドレスの設定を削除します。
「Delete Profile」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。 • 設定可能範囲：10-1024 • 初期値：32

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear Log」ボタンをクリックして、ログを削除します。

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、画面を表示します。

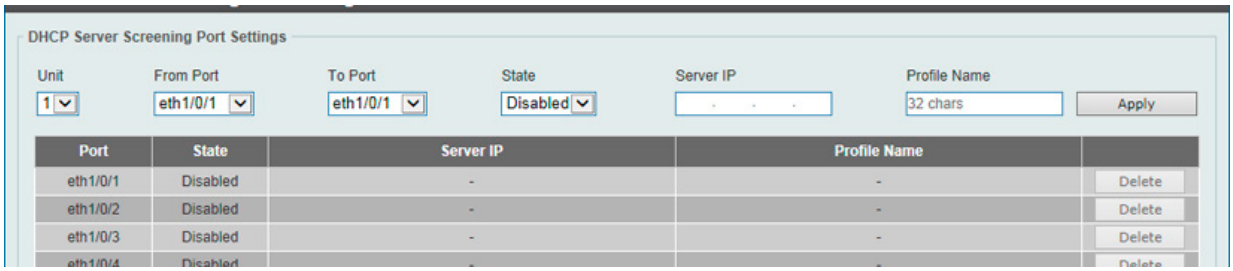


図 12-62　DHCP Server Screening Port Settings 画面

以下の項目が表示されます。

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。
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。

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

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。
エントリが作成されると、送信元 IP アドレスがエントリのゲートウェイ IP アドレスと一致し、かつ送信元 MAC アドレスがエントリのゲートウェイ MAC アドレスと一致しない ARP パケットは、システムによって破棄されます。送信元 IP アドレスがゲートウェイ IP アドレスと一致しない ARP パケットは、ASP によってバイパスされます。
ARP アドレスが設定済みのゲートウェイの 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 12-63　ARP Spoofing Prevention 画面

以下の項目が表示されます。

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。
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。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、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つはアタック状態です。アタック状態には、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。

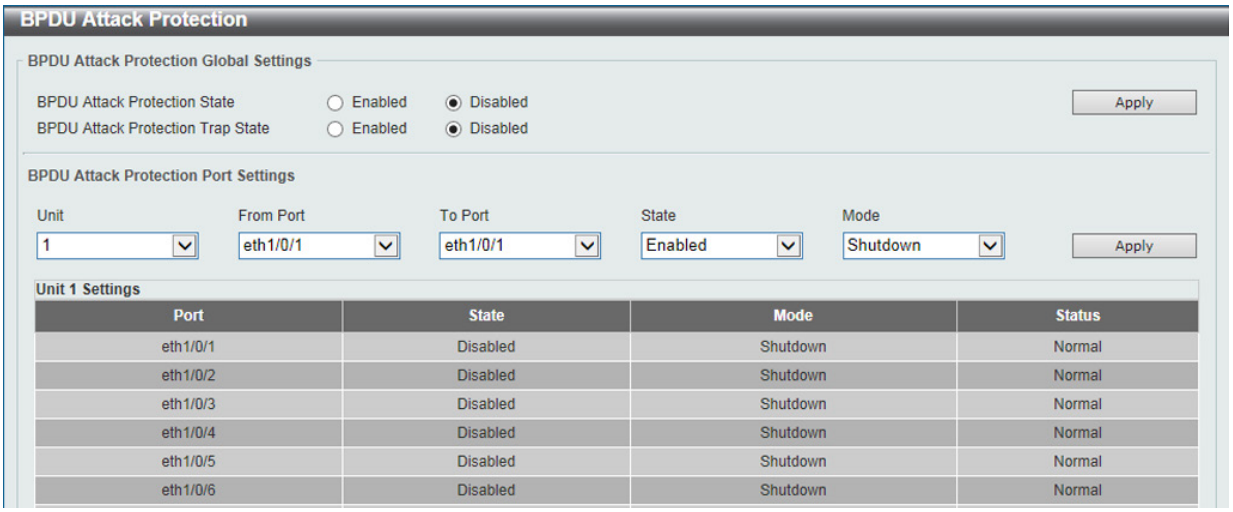


図 12-64　BPDU Attack Protection 画面

以下の項目が表示されます。

項目	説明
BPDU Attack Protection State	BPDU アタック防止機能を有効または無効にします。 • 初期値：「Disabled」（無効）
BPDU Attack Protection Trap State	トラップの状態を有効 / 無効に設定します。
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。
State	指定ポートに対してモードを有効または無効にします。
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」- ポートがアタック状態に入るとポートをシャットダウンします。

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

MAC 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。
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。
ローカルデータベースに基づいて認証を実行、または 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　本機能は将来のファームウェアでサポート予定です。

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。

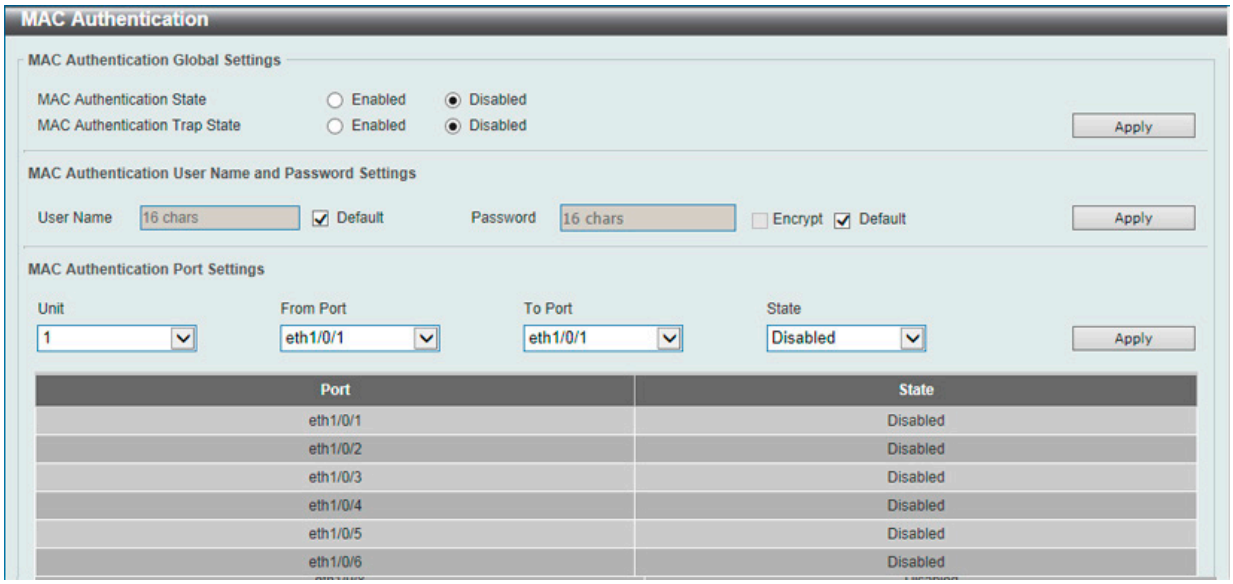


図 12-65　MAC Authentication 画面

以下の項目が表示されます。

項目	説明
MAC Authentication Global Settings	
MAC Authentication State	スイッチの 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 アドレスをパスワードとして指定します。
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。

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

Web-based Access Control（Web 認証）

補足　本機能は将来のファームウェアでサポート予定です。

Web ベース認証のログインは、スイッチを経由してインターネットにアクセスを試みる場合に、ユーザを認証するように設計された機能で、認証処理には HTTP/HTTPS プロトコルを使用します。Web ブラウザ経由で Web ページ (例 : http://www.dlink.com) の閲覧を行う場合に、スイッチは認証段階に進みます。スイッチは、HTTP/HTTPS パケットを検出し、このポートが未認証である場合に、ユーザ名とパスワードの画面を表示して、ユーザに問い合わせます。認証処理が完了するまで、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、認証サーバとなってローカルデータベースに基づく認証を行うか、または RADIUS クライアントとなってリモート RADIUS サーバと共に RADIUS プロトコルを介する認証処理を実行します。ユーザクライアントが 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。

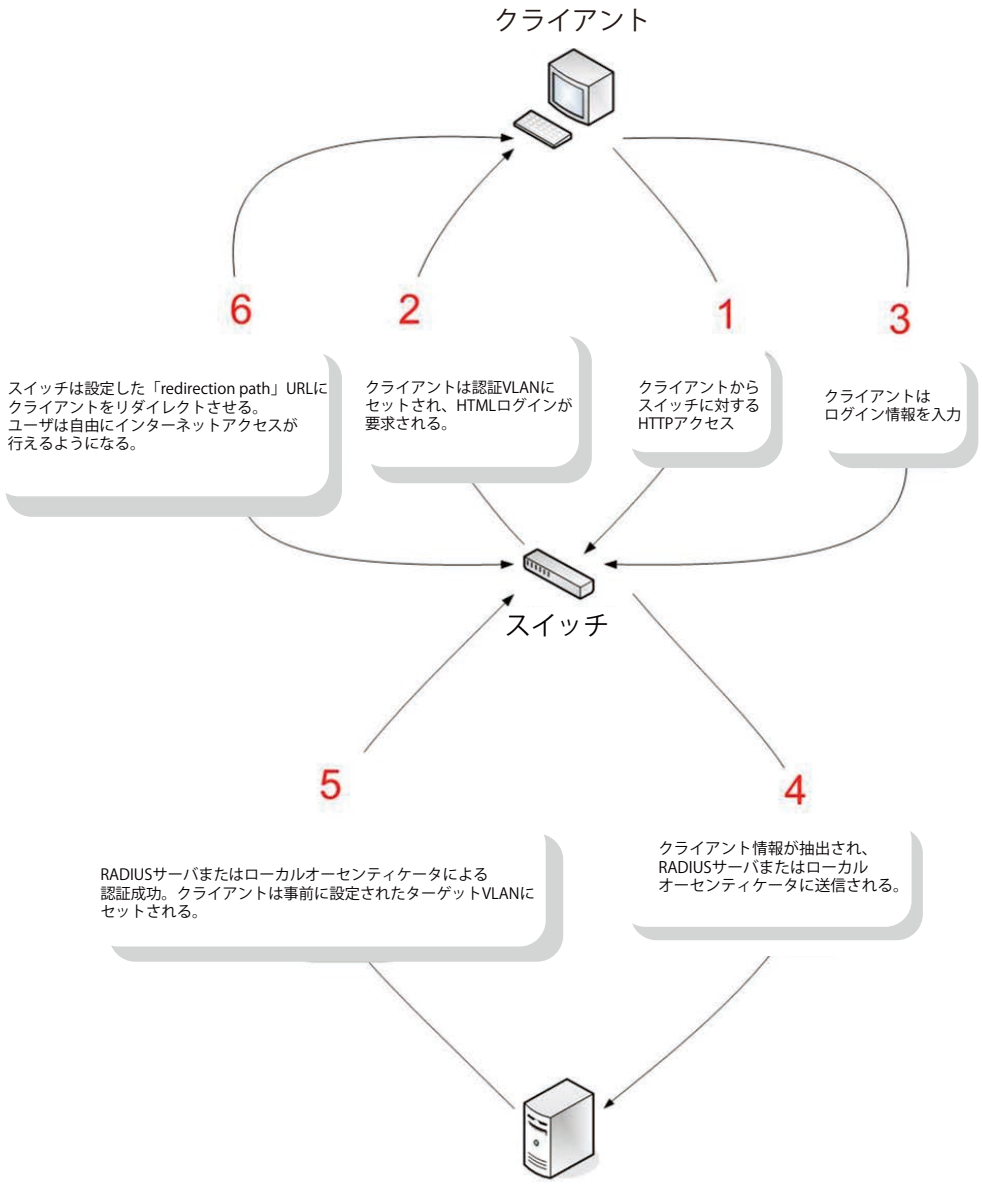
D-Link の WAC の実行には、WAC 機能が排他的に使用している仮想 IP が使用されます。これは、スイッチの他のモジュールには認識されません。実際、スイッチの他の機能への影響を避けるため、WAC は仮想 IP アドレスのみを使用してホストとの通信を行います。従って、すべての認証要求は、スイッチの物理インタフェースの IP アドレスではなく仮想 IP アドレスに送信される必要があります。

ホスト PC が仮想 IP 経由で WAC スイッチと通信する場合、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 から独立したものになります。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は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 にトラップされるため、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 アドレスを実際に所有しているサーバまたは PC とは通信ができません。ホストがサーバまたは PC にアクセスする必要がある場合、仮想 IP をサーバや 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、認証を適切に実行するために、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 実装の特徴の 1 つとして、HTTP または HTTPS プロトコルに対し、ユーザ定義のポート番号により TCP ポート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 にトラップされる 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。また、プロトコルが指定されない場合、初期値は HTTP になります。

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 サーバに対してターゲット VLAN などを含め適切な構成を行ってください。

Web Authentication（Web 認証設定）

スイッチの Web 認証設定をに行います。

Security > Web-based Access Control > Web Authentication をクリックし、以下の画面を表示します。



図 12-66　Web Authentication 画面

以下の項目が表示されます。

項目	説明
Web Authentication State	Web 認証機能を有効 / 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 IP 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た後に有効になります。ユーザは、仮想 IP アドレスを取得するために、DNS サーバに保存された FQDN URL を取得します。取得した IP アドレスは本コマンドで指定した仮想 IP アドレスと一致する必要があります。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	FQDN URL を指定します。（128 文字以内）
Redirection Path	リダイレクト URL を入力します。（128 文字以内）

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

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

WAC Port Settings（Web 認証ポート設定）

WAC ポート設定を行います。

Security > Web-based Access Control > WAC Port Settings をクリックし、以下の画面を表示します。

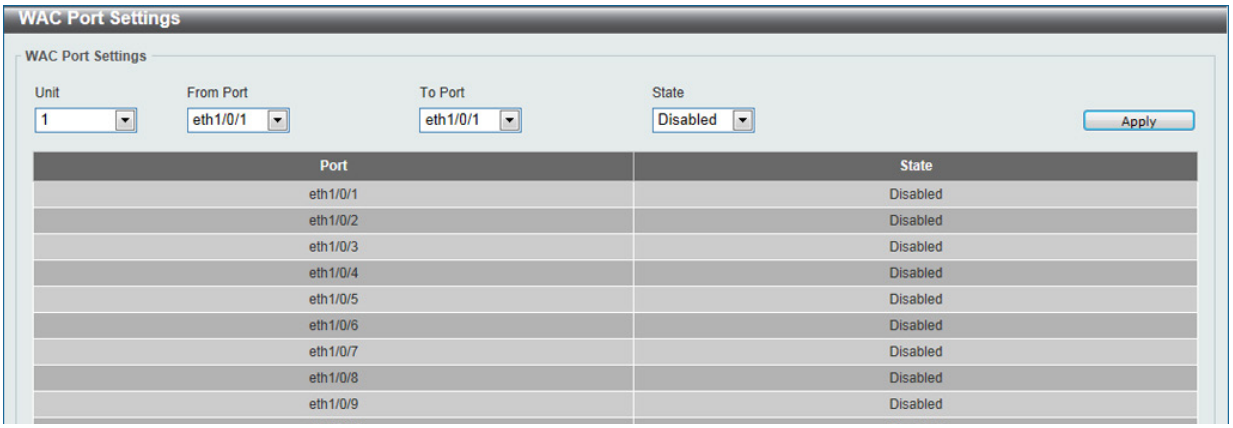


図 12-67　WAC Port Settings 画面

以下の項目が表示されます。

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。
State	WAC 機能を有効 / 無効に設定します。

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

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。

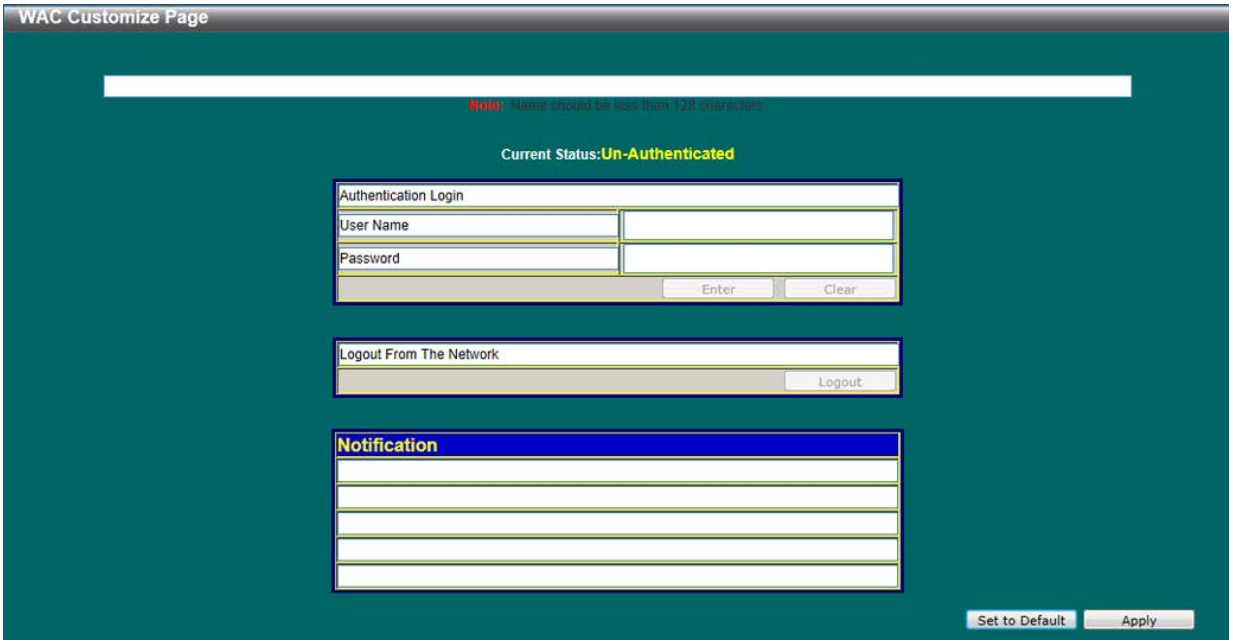


図 12-68　WAC Customize Page 画面

以下の項目が表示されます。

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）

項目	説明
Notification	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。

WAC ページの設定を変更するには、本画面の WAC 認証情報をすべて入力して「Apply」ボタンをクリックし、変更を適用します。
「Set to Default」ボタンをクリックして、全項目を初期設定に復元します。

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。

補足　本機能は将来のファームウェアでサポート予定です。

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。

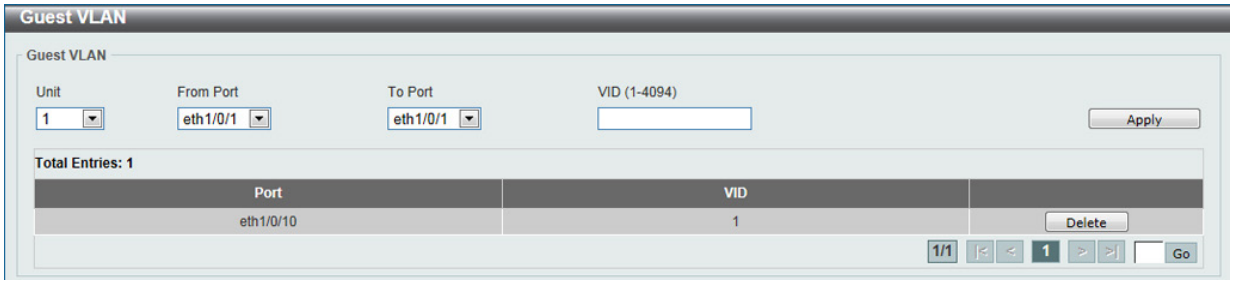


図 12-69　Guest VLAN 画面

以下の項目が表示されます。

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。
VID	設定する VLAN ID を入力します。 • 設定可能範囲：1-4094

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

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。

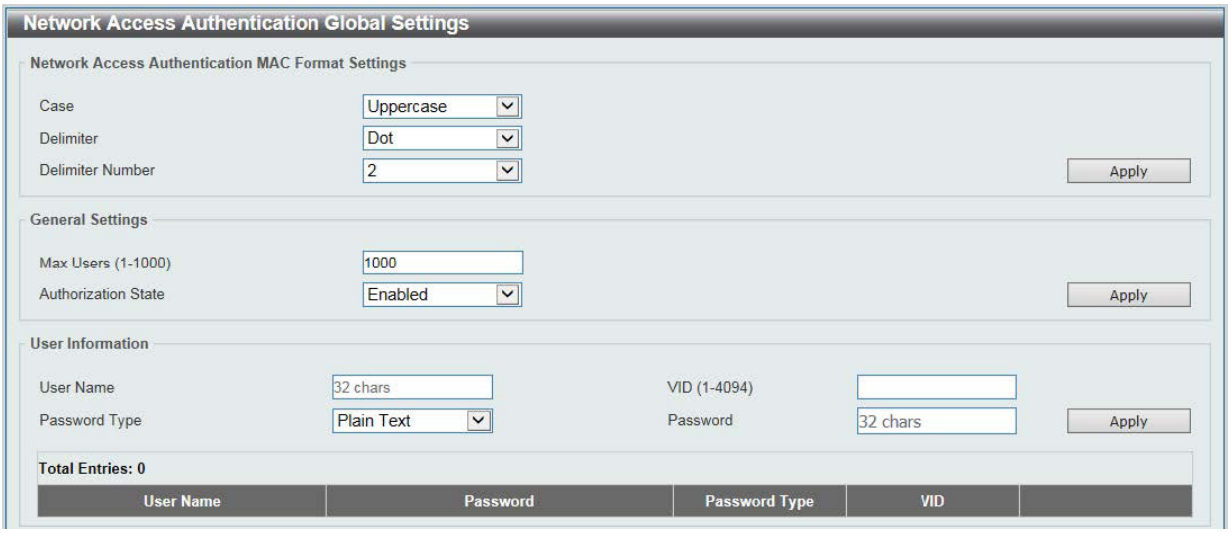


図 12-70　Network Access Authentication Global Settings 画面

以下の項目が表示されます。

項目	説明
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）または「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。区切り文字を持たない場合には「None」を選択します。 • 選択肢：「Hyphen（ハイフン）」「Colon（コロン）」「Dot（ドット）」
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	最大ユーザ数を指定します。 • 設定可能範囲：1-1000 • 初期値：1000
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。
Password Type	パスワードの種類を選択します。 • 選択肢：「Plain Text」「Encrypted」
Password	パスワードを入力します。

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

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。

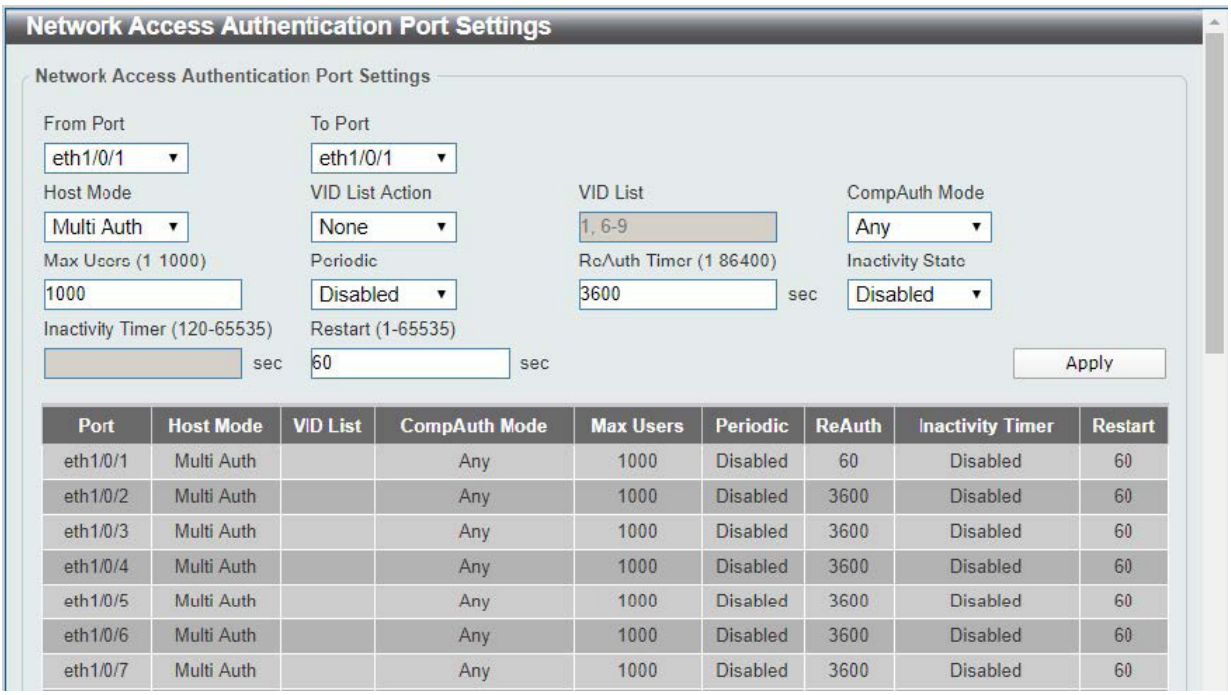


図 12-71　Network Access Authentication Port Settings 画面

以下の項目が表示されます。

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。
Host Mode	選択ポートに適用するホストモードを選択します。 • 選択肢：「Multi Host」「Multi Auth」 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。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有効です。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。各 VLAN の認証コントロールを行う必要があるトランクポートに対して、この設定が役に立ちます。ポートの認証モードがマルチホストに変更された場合、ポートに設定されている認証 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 ベースアクセスコントロール、WAC）への認証が通ると、そのまま認証に成功します。
Max Users	最大ユーザ数を指定します。 • 設定可能範囲：1-1000
Periodic	選択ポートの定期再認証を有効 / 無効に設定します。802.1X プロトコルにのみ影響します。
ReAuth Timer	再認証時間を指定します。 • 設定可能範囲：1-86400（秒） • 初期値：3600（秒）
Inactivity State	「Inactivity」（休止）を有効 / 無効に指定します。
Inactivity Timer	「Inactivity」（休止）を有効にした場合、休止時間の値を入力します。このパラメータは WAC と JWAC の認証プロトコルにのみ影響します。 • 設定可能範囲：120-65535（秒）

項目	説明
Restart	リスタート時間を入力します。 • 設定可能範囲：1-65535（秒）

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

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の情報表示、クリアを行います。

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。

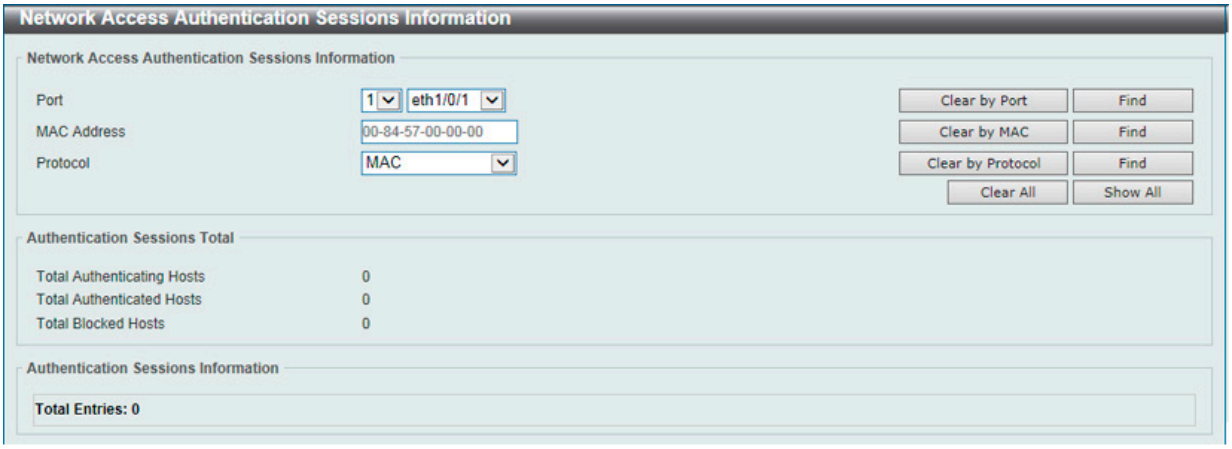


図 12-72　Network Access Authentication Sessions Information 画面

以下の項目が表示されます。

項目	説明
Port	表示するポートとユニットを指定します。
MAC Address	表示する 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」

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

情報の消去

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

エントリの検出 / 表示

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「View All」ボタンをクリックし、すべてのエントリを表示します。

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加してしまう可能性があります。このような問題を軽減するために、本スイッチ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、Safeguard Engine 機能が有効になり、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 IP パケットのための帯域を制限します。CPU 負荷がしきい値以下に下がった場合、セーフガードエンジンは動作を停止し、スイッチは 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「Protocol」「Manage」「Route」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、「Protocol」グループが最も高いプライオリティのパケットを受信し、（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）「Route」グループは最も優先度の低いパケットを受信します。「Protocol」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たプロトコルコントロールパケットです。「Manage」グループ内では、パケットは Telent や SSH などの相互通信プロトコルによって、ルータやシステムネットワーク管理インタフェースへ向かいます。「Route」グループで処理されるパケットは、ルータ CPU によって通常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。

以下の表ではプロトコルと対応するサブインタフェースを表示します。

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-Neighbor）
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)（ICMPv6-Other）
IGMP	Protocol	Internet Group Management Protocol（IGMP）
LACP	Protocol	Link Aggregation Control Protocol（LACP）
NTP	Protocol	Network Time Protocol
OSPF	Protocol	Open Shortest Path First
PIM	Protocol	Protocol Independent Multicast
PPPoE	Protocol	Point-to-point protocol over Ethernet
RIP	Protocol	Routing Information Protocol
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）
VRRP	Protocol	Virtual Router Redundancy Protocol
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ーフェースに対してまとめてアサイン、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アサインすることが可能です。本機能を使用して個々のプロトコルのレートリミットをカスタマイズする場合、不適切なレートリミットを設定すると、スイッチのパケットプロセスに異常をきたす場合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、CPU 使用率とトラフィック制限を制御するために、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ます。これにより、ネットワークを介してトラフィックをルーティングするスピード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。

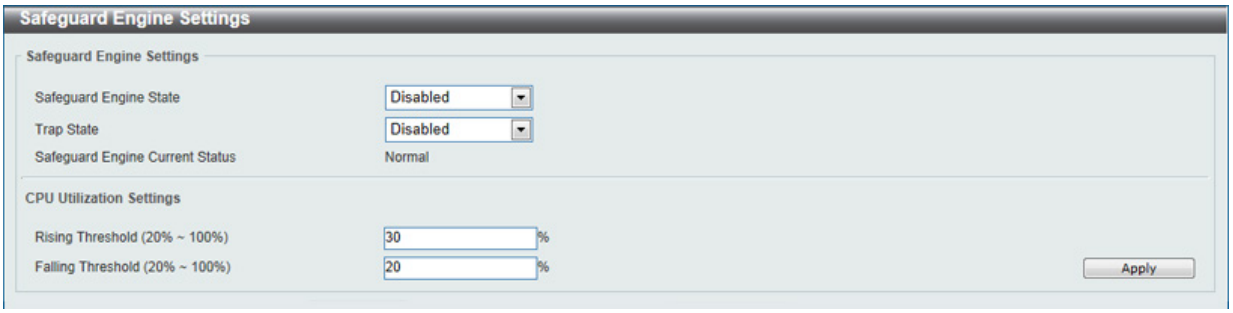


図 12-73　Safeguard Engine Settings 画面

以下の項目が表示されます。

項目	説明
Safeguard Engine Settings	
Safeguard Engine State	セーフガードエンジン機能を有効 / 無効に設定します。
Trap State	セーフガードエンジントラップを有効 / 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状態を表示します。
CPU Utilization Settings	
Rising Threshold	CPU 使用率の上昇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、設定値に基づいて Exhausted モードに入ります。 ・ 設定可能範囲：20-100（%）
Falling Threshold	CPU 使用率の下降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、Safeguard Engine 状態から Normal モードに戻ります。 ・ 設定可能範囲：20-100（%）

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

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 12-74　CPU Protect Counters 画面

以下の項目が表示されます。

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、指定条件に基づく情報を消去します。
「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。

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 12-75　CPU Protect Sub-Interface 画面

以下の項目が表示されます。

CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）

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。 • 選択肢：「Manage」「Protocol」「Route」
Rate Limit	レートリミットの値を入力します。「No Limit」を指定するとレートリミットを無効にします。 • 設定可能範囲：0-1024（パケット / 毎秒）

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

Sub-Interface Information（サブインタフェース情報）

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。 • 選択肢：「Manage」「Protocol」「Route」

「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 12-76　CPU Protect Type 画面

以下の項目が表示されます。

CPU Protect Type（CPU プロテクトタイプ）

項目	説明
Protocol Name	プロトコル名のオプションを選択します。
Rate Limit	レートリミットの値を入力します。「No Limit」を指定するとレートリミットを無効にします。 • 設定可能範囲：0-1024（パケット / 毎秒）

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

Protect Type Information（プロテクトタイプ情報）

項目	説明
Protocol Name	プロトコル名オプションを選択します。

「Find」ボタンをクリックし、指定条件に基づくエントリを検出します。

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。

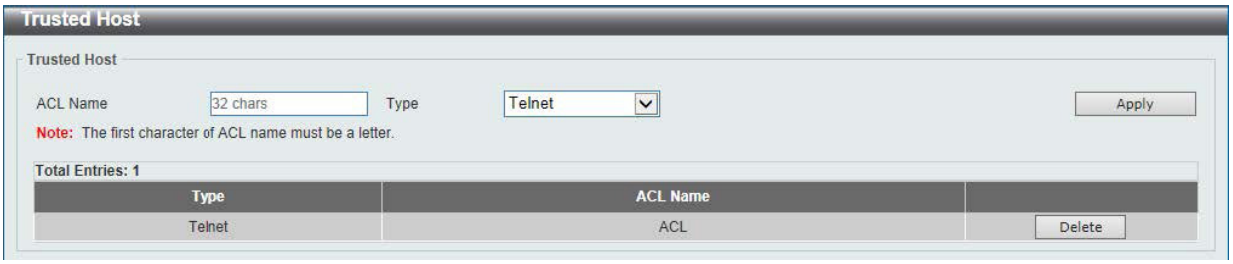


図 12-77　Trusted Host 画面

以下の項目が表示されます。

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」

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして、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、異なるインターフェイスタイプで構成できます。コマンドで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。

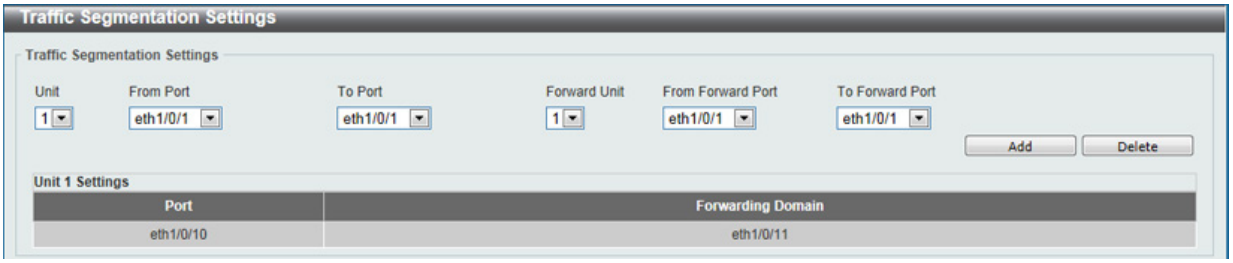


図 12-78　Traffic Segmentation 画面

以下の項目が表示されます。

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、設定内容に基づくエントリを追加します。
「Delete」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。

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。

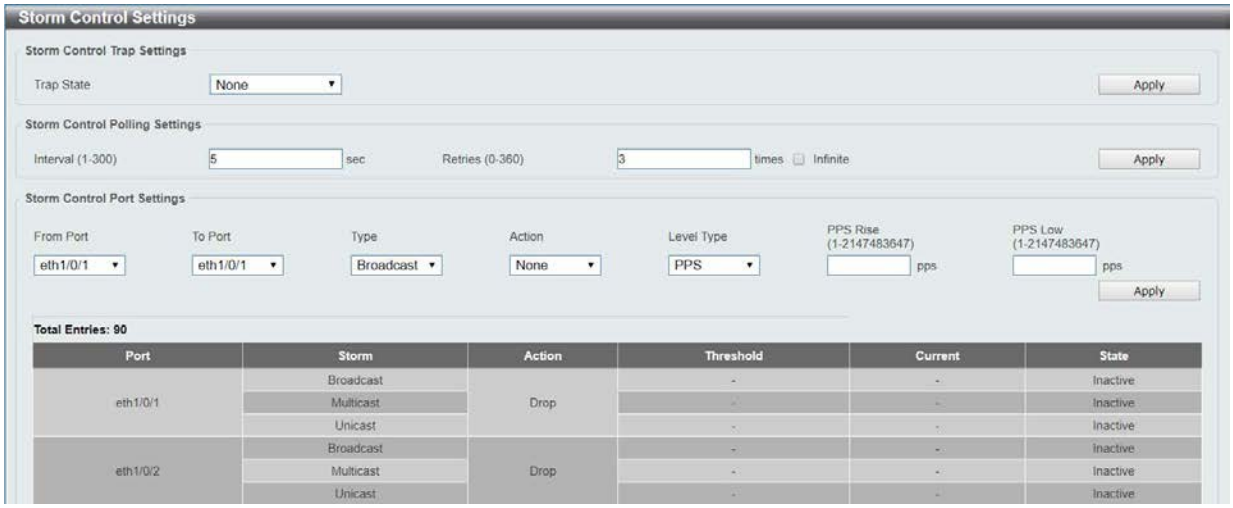


図 12-79　Storm Control Settings 画面

以下の項目が表示されます。

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	
Interval	インターバルの値を指定します。 • 設定可能範囲：1-300（秒） • 初期値：5（秒）
Retries	再試行回数を入力します。「Infinite」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：0-360 • 初期値：3
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。
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」- 指定したしきい値に達するとポートはシャットダウンされます。 • 「Drop」- 指定したしきい値に達するとパケットは破棄されます。
Level Type	レベルタイプを指定します。 • 選択肢：「PPS」「Kbps」「Level」
PPS Rise	1 秒あたりの増加パケット量について上限しきい値を指定します。「PPS Low」の値が指定されていない場合、初期値は指定した増加 PPS の 80%に指定されます。 • 設定可能範囲：1-2147483647（パケット / 毎秒）
PPS Low	1 秒あたりの減少パケット量について下限しきい値を指定します。「PPS Low」の値が指定されていない場合、初期値は指定した増加 PPS の 80%に指定されます。 • 設定可能範囲：1-2147483647（パケット / 毎秒）

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

「Level Type」で「Kbps」を選択すると、以下の画面が表示されます。



図 12-80　Storm Control (Kbps) 画面

項目	説明
KBPS Rise	上限 KBPS の値を指定します。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 / 毎秒で指定します。 • 設定可能範囲：1-2147483647（Kbps）
KBPS Low	下限 KBPS の値を指定します。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 / 毎秒で指定します。「Low PPS」の値が指定されていない場合、初期値は指定した上限 KBPS の 80%に指定されます。 • 設定可能範囲：1-2147483647（Kbps）

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

「Level Type」で「Level」を選択すると、以下の画面が表示されます。



図 12-81　Storm Control (Level) 画面

項目	説明
Level Rise	上限レベルについて入力します。本オプションはポートで受信するトラフィックの総帯域のパーセンテージを上限のしきい値として指定します。 • 設定可能範囲：1-100（%）
Level Low	下限レベルについて入力します。本オプションはポートで受信するトラフィックの総帯域のパーセンテージを下限のしきい値として指定します。「Level Low」の値が指定されていない場合、初期値は指定した上限レベルの 80%に指定されます。 • 設定可能範囲：1-100（%）

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

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。

- Land 攻撃：このタイプの攻撃には、送信元アドレスと宛先アドレスがターゲットデバイスのアドレスに設定されている IP パケットが使用されます。ターゲットデバイスが自身に対して継続的に応答してしまう可能性があります。
- Blat 攻撃：このタイプの攻撃は、ターゲットデバイスの宛先ポートと同じ TCP / UDP ソースポートでパケットを送信します。ターゲットデバイスが自身に対して応答してしまう可能性があります。
- TCP-Null：このタイプの攻撃には、シーケンス番号 0 でフラグを持たない特定のパケットを使用したポートスキャンが使用されます。
- TCP-Xmas：このタイプの攻撃には、シーケンス番号 0 で緊急（URG）、プッシュ（PSH）、および FIN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- TCP SYN-FIN：このタイプの攻撃には、SYN および FIN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- TCP SYN SrcPort Less 1024：このタイプの攻撃には、送信元ポート 0 ～ 1023 と SYN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- Ping of Death 攻撃：Ping of Death 攻撃は、コンピューターに対する攻撃の一種で、不正な形式の Ping または悪意のある Ping をコンピューターに送信します。 Ping のサイズは通常 64 バイトです（多くのコンピュータは、最大 IP パケットサイズである 65535 バイトより大きい Ping を処理できません）。このサイズの ping を送信すると、ターゲットコンピュータがクラッシュする可能性があります。従来、このバグは比較的簡単に悪用されていました。一般に、65536 バイトの Ping パケットを送信することはネットワークプロトコルの規定に違反しますが、断片化されている場合、このサイズのパケットが送信できてしまいます。ターゲットコンピュータがパケットを再構成すると、バッファオーバーフローが発生する可能性があり、システムクラッシュを引き起こすことがあります。
- TCP Tiny Fragment 攻撃：Tiny TCP Fragment 攻撃者は、IP フラグメンテーションを使用して非常に小さなフラグメントを作成し、TCP ヘッダ情報をパケットフラグメントに分割してルータのチェック機能を通過させ、攻撃を実行します。
- すべてのタイプ：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。

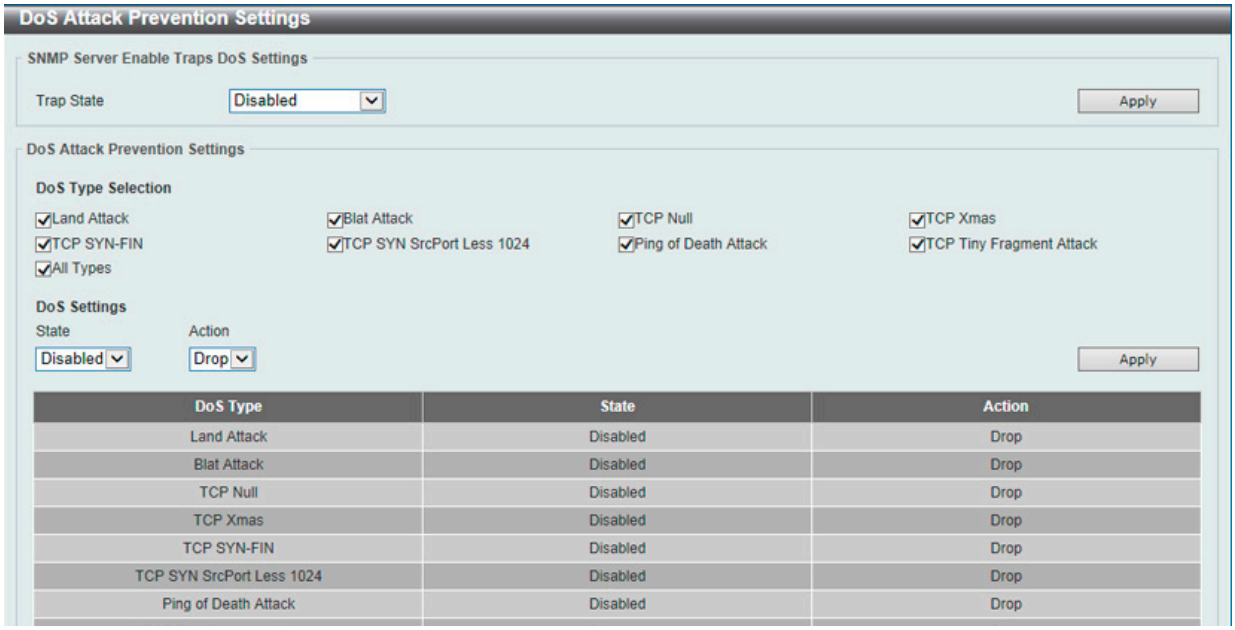


図 12-82　DoS Attack Prevention Settings 画面

以下の項目が表示されます。

項目	説明
SNMP Server Enable Traps DoS Settings	
Trap State	DoS 攻撃防止トラップ状態を有効 / 無効に設定します。
DoS Attack Prevention Settings	
DoS Type Selection	適切な DoS 攻撃防御のタイプを選択します。 • 「Land Attack」- DoS 攻撃防止タイプに LAND 攻撃を指定します。 • 「Blat Attack」- DoS 攻撃防止タイプに BLAT 攻撃を指定します。 • 「TCP Null」- DoS 攻撃防止タイプに TCP Null Scan 攻撃を指定します。 • 「TCP Xmas」- DoS 攻撃防止タイプに TCP Xmascan 攻撃を指定します。 • 「TCP SYN-FIN」- DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。 • 「TCP SYN SrcPort Less 1024」- DoS 攻撃防止タイプに TCP SYN Source Port Less 1024 攻撃を指定します。 • 「Ping Death Attack」- DoS 攻撃防止タイプに Ping Death Attack 攻撃を指定します。 • 「TCP Tiny Fragment Attack」- DoS 攻撃防止タイプに TCP Tiny Frag 攻撃を指定します。 • 「All Types」- DoS 攻撃防止タイプにすべての攻撃を指定します。
State	DoS 攻撃防止の状態を有効 / 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。

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

SSH（Secure Shell）

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. 「Host Key」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設定内容の確認に使用します。

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

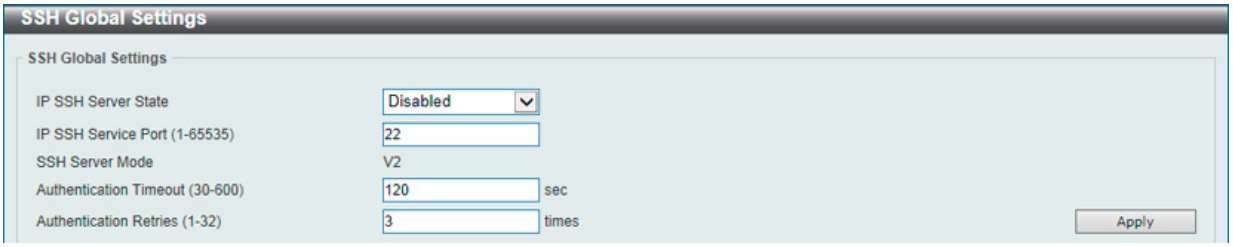


図 12-83　SSH Global Settings 画面

以下の項目が表示されます。

項目	説明
IP SSH Server State	グローバルに SSH 機能を有効 / 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 Attempts	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。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

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

Host Key（Host Key 設定）

SSH ホスト鍵を表示、生成します。

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。

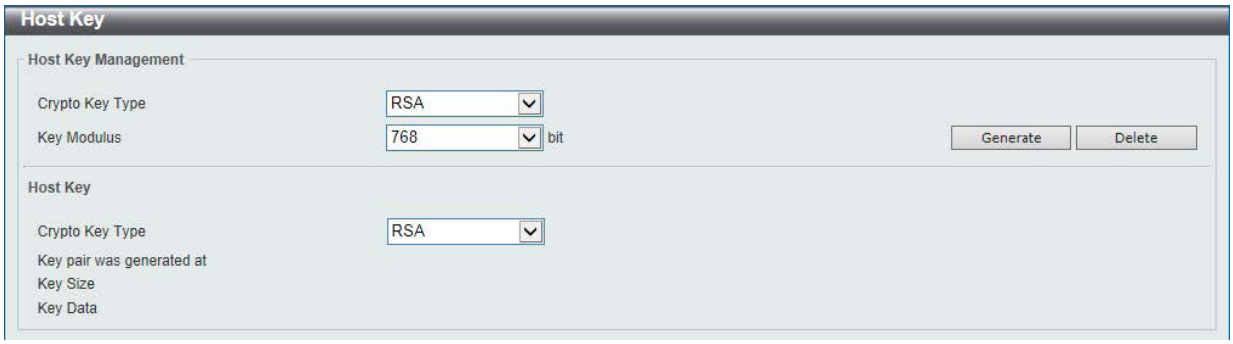


図 12-84　Host Key 画面

以下の項目が表示されます。

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：「Rivest Shamir Adleman (RSA)」「Digital Signature Algorithm (DSA)」
Key Modulus	鍵係数の値を入力します。 • 選択肢：「360」「512」「768」「1024」「2048」（ビット）
Host Key	
Crypto Key Type	暗号鍵の種類を選択します。 • 選択肢：「Rivest Shamir Adleman (RSA)」「Digital Signature Algorithm (DSA)」

「Generate」ボタンをクリックして、指定したホスト鍵を有効にします。
「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。

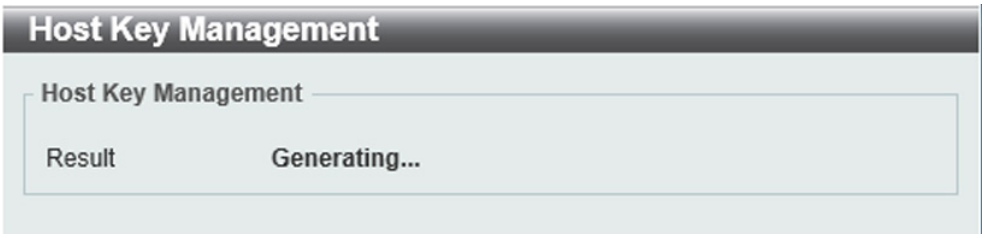


図 12-85　Host Key (Generating) 画面

「Generate」が終了すると、次の画面が表示されます。

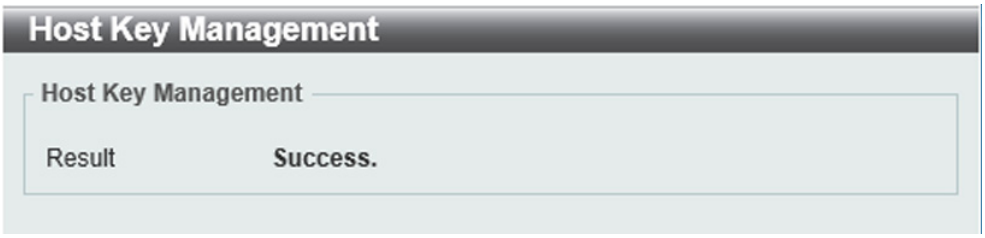


図 12-86　Host Key (Generating, Success) 画面

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 12-87　SSH Server Connection 画面

表示されるエントリの内容を確認します。

SSH User Settings（SSH ユーザ設定）

SSH ユーザの設定および設定内容を確認します。

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。

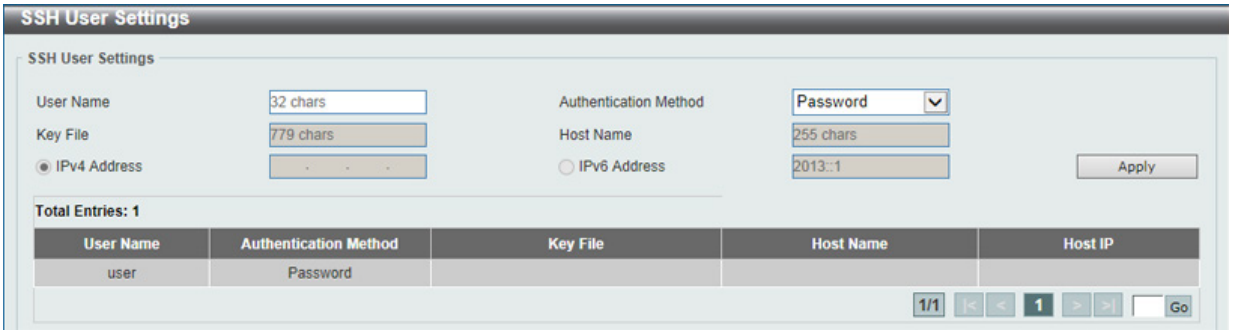


図 12-88　SSH User Settings 画面

以下の項目が表示されます。

項目	説明
User Name	SSH ユーザを識別するユーザ名を指定します。（半角英数字 32 文字以内）
Authentication Method	スイッチにアクセスを試みる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	「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	「Host-based」を選択した場合、ホスト名を入力します。
IPv4 Address	「Host-based」を選択した場合、IPv4 アドレスを入力します。
IPv6 Address	「Host-based」を選択した場合、IPv6 アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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、以下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）の 2 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 7 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。また、本スイッチは、SSLv3 および TLSv1/v2/v3 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 Global Settings」画面および「SSL Service Policy」画面では、スイッチで SSL を有効にして各種暗号スイートのステータスを設定することができます。暗号スイートは、認証セッションに使用される正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定するセキュリティ文字列です。スイッチには 7 個の暗号スイート設定が用意されており、特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

SSL 機能が有効化されると、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。

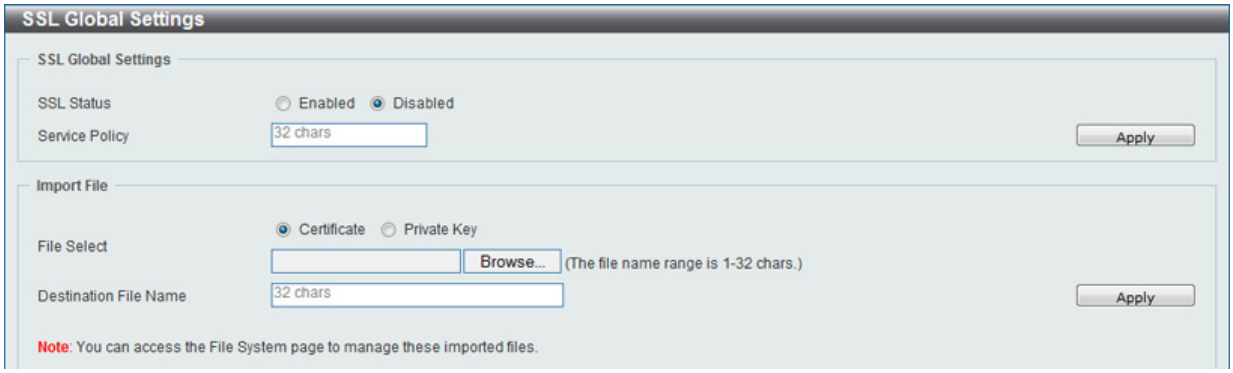


図 12-89　SSL Global Settings 画面

以下の項目が表示されます。

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。 • 初期値：「Disabled」（無効）
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、「Browse/ 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）

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

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。

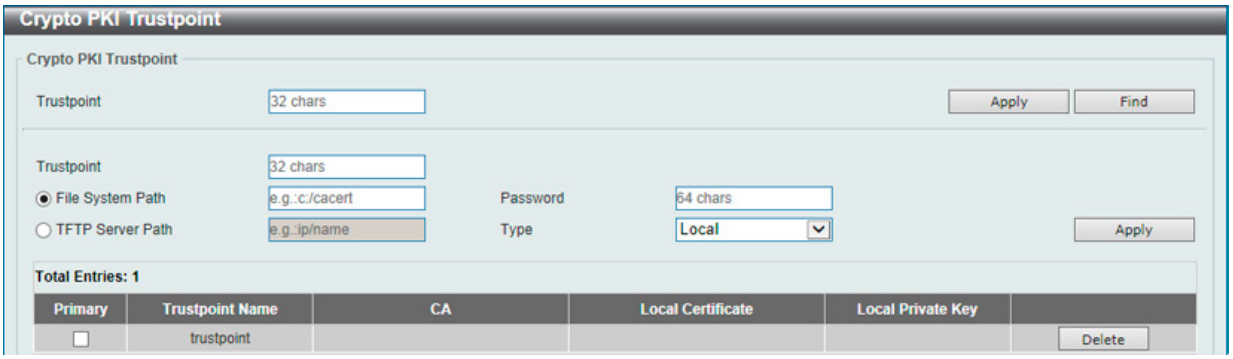


図 12-90　Crypto PKI Trustpoint 画面

以下の項目が表示されます。

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と「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」「ローカル証明書と鍵ペア」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」-「ローカル証明書と鍵ペア」のみインポートします。

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

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。

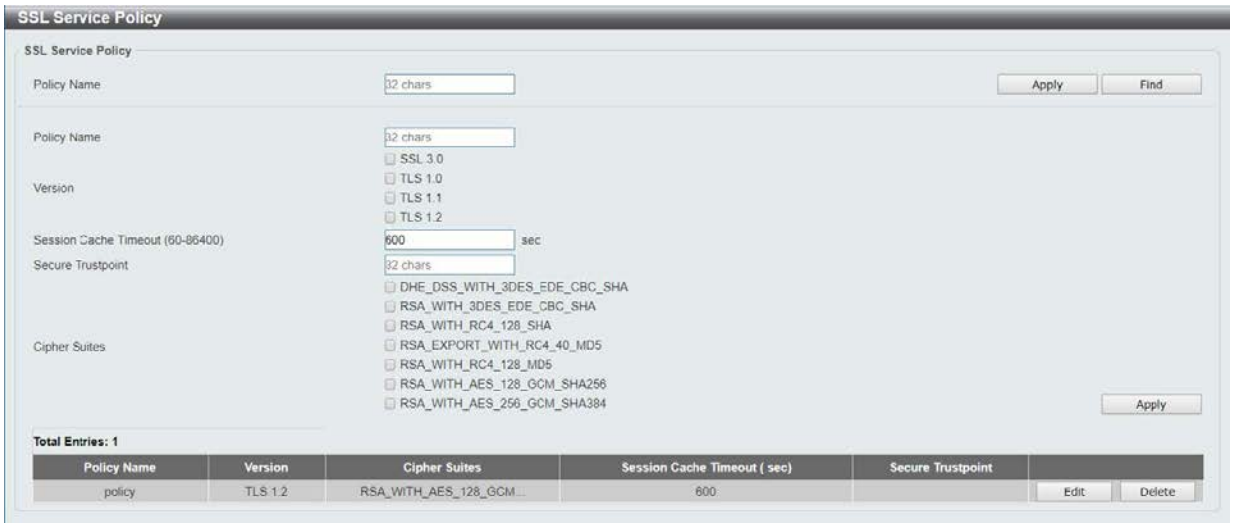


図 12-91　SSL Service Policy 画面

以下の項目が表示されます。

項目	説明
Policy Name	SSL サービスポリシー名を入力します。（32 文字以内）
Version	「Transport Layer Security」(TLS) および Secure Sockets Layer（SSL）のバージョンを指定します。 • 選択肢：「SSL 3.0」「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。

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

SFTP Server Settings（SFTP サーバ設定）

本項目では「Secure File Transfer Protocol」(SFTP) サーバの設定、表示を行います。SFTP は信頼できるデータストリームにおいて、リモートでセキュアなファイル転送を行うプロトコルです。SFTP 自身では認証やセキュリティ機能を提供しないため、SFTP サーバは SSH サーバのサブシステムとして動作します。

補足　IPv4 SFTP サーバのみサポートされています。

Security > SFTP 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。

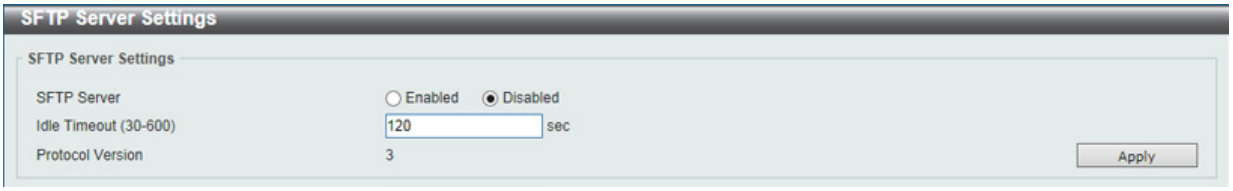


図 12-92　SFTP Server Settings 画面

以下の項目が表示されます。

項目	説明
SFTP Server	SFTP サーバを有効 / 無効に設定します。
Idle Timeout	アイドルタイムアウトの時間を設定します。SFTP サーバが指定時間 SFTP セッションの活動が行われていないことを検出すると、SFTP セッションは閉じられます。 • 設定可能範囲：30-600（秒） • 初期値：120（秒）

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

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設定を行います。

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。

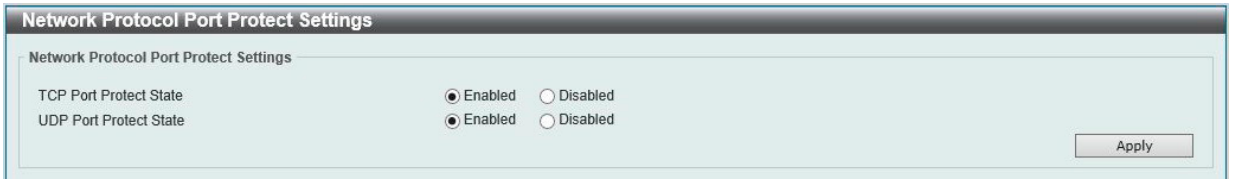


図 12-93　Network Protocol Port Protect Settings 画面

以下の項目が表示されます。

項目	説明
TCP Port Protect 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 Protect State	UDP ポート保護ステータスを有効 / 無効に指定します。

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

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）機能の設定を行います。

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。

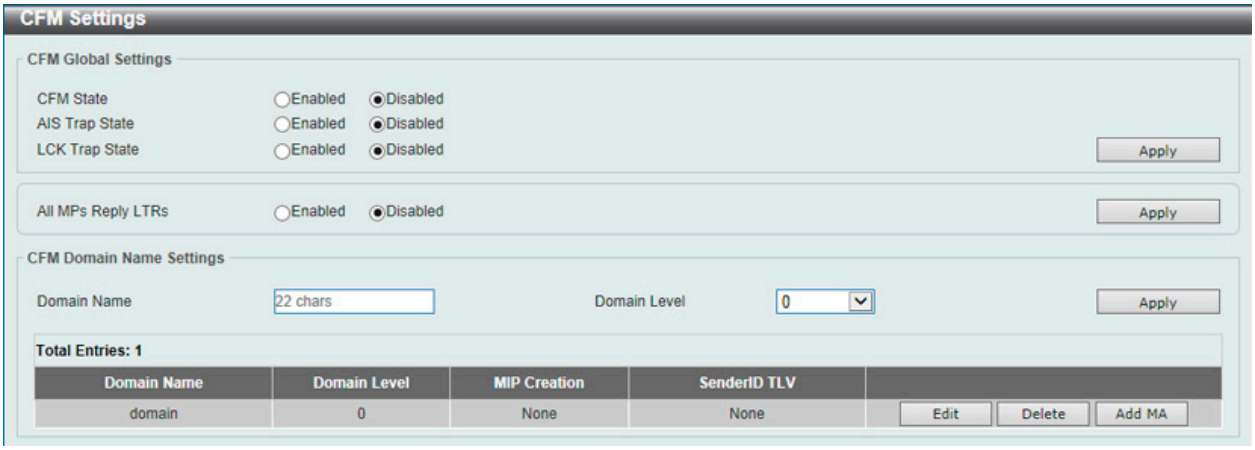


図 13-1　CFM Settings 画面

以下の項目が表示されます。

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。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。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	MPs 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。本機能を設定すると、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。各 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

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

エントリの編集

編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

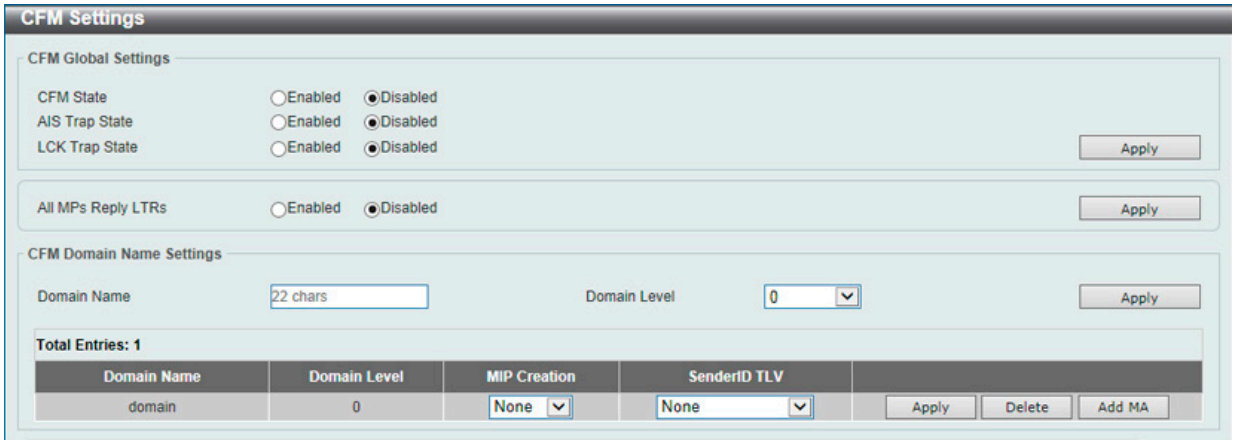


図 13-2　CFM Settings 画面 - Edit

以下の項目が表示されます。

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、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 のデフォルト転送を設定します。 • 「None」- SenderID TLV を転送しません。 • 「Chassis」- シャーシ ID 情報を持つ SenderID TLV を転送します。 • 「Manage」- 管理アドレス情報を持つ SenderID TLV を転送します。 • 「Chassis」- Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。

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

「Delete」ボタンをクリックして、エントリを削除します。

Add MA 設定（CFM 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「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　Add MA 画面

以下の項目が表示されます。

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 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。
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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。
「Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

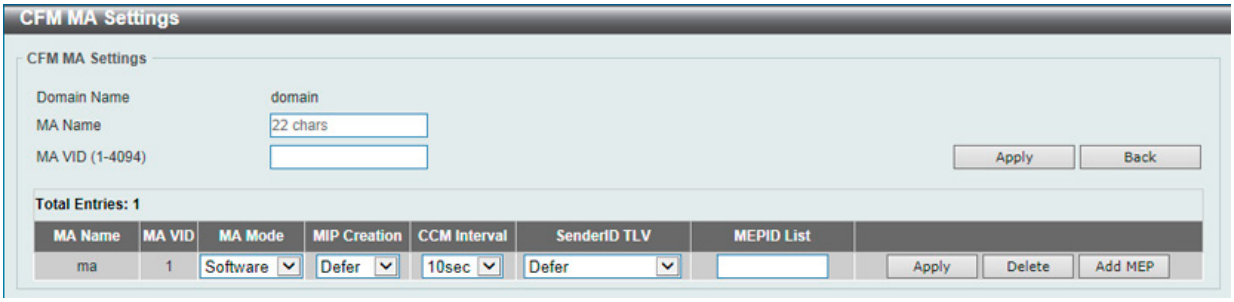


図 13-4　CFM MA Settings 画面 - Edit

以下の項目が表示されます。

項目	説明
MA Mode	MA の動作モードを選択します。 • 「Software」- MA は CFM ソフトウェアモードで動作します。 • 「Hardware」- MA は CFM ハードウェアモードで動作します。 CFM ハードウェアモードは、CCM 処理のパフォーマンスを改善するために使用されます。CFM ハードウェアモードでは、ハードウェアによって CCM パケットが処理され、通常、CPU には影響ありません。また、CCM インターバルを最小値の 3.3ms にセットすることが可能ですが、CPU 性能の制限により、この値は CFM ソフトウェアモードではサポートされていません。 また、CFM ハードウェアおよびソフトウェアモードは一緒に使用することができます。MA を CFM ハードウェアモードに設定すると、MA 内のすべての MEP が CFM ハードウェアモードで動作します。一部の MA で CCM 処理のパフォーマンスを考慮する場合（例えば 3.3ms および 10ms の CCM インターバルを必要とし、MA 内の MEP が Down MEP の場合）、ユーザは CFM ハードウェアモードを使用することができます。その他の MA については、CCM 処理のパフォーマンスに問題がない、または UP MEP や MIP を設定する必要がある、または全ての CFM 機能が必要な場合、CFM ソフトウェアモードを選択した方が良い場合があります。

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」- メンテナンスドメインに MIP を作成しません。 • 「Auto」- 次のいずれかの場合にこの 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 • 「Defer」- この MA が関連す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。 • 「3.3ms」- 3.3（ミリ秒） • 「10ms」- 10（ミリ秒） • 「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 の転送を制御します。 • 「None」- SenderID TLV を転送しません。 • 「Chassis」- シャーシ ID 情報を持つ SenderID TLV を転送します。 • 「Manage」- 管理アドレス情報を持つ SenderID TLV を転送します。 • 「Chassis」- Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。 • 「Defer」- この MA が関連す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

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

Add MEP 設定（CFM Settings）

MEP を追加します。

OAM > CFM > CFM 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。

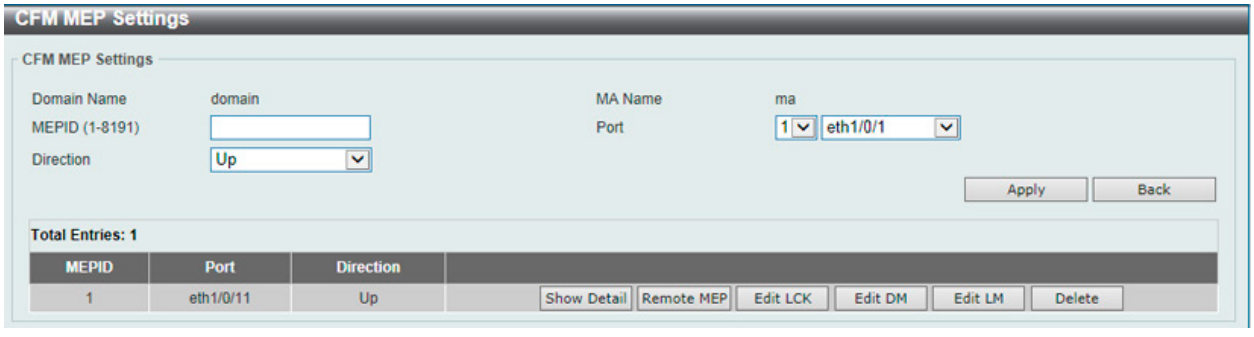


図 13-5　CFM MEP Settings 画面

以下の項目が表示されます。

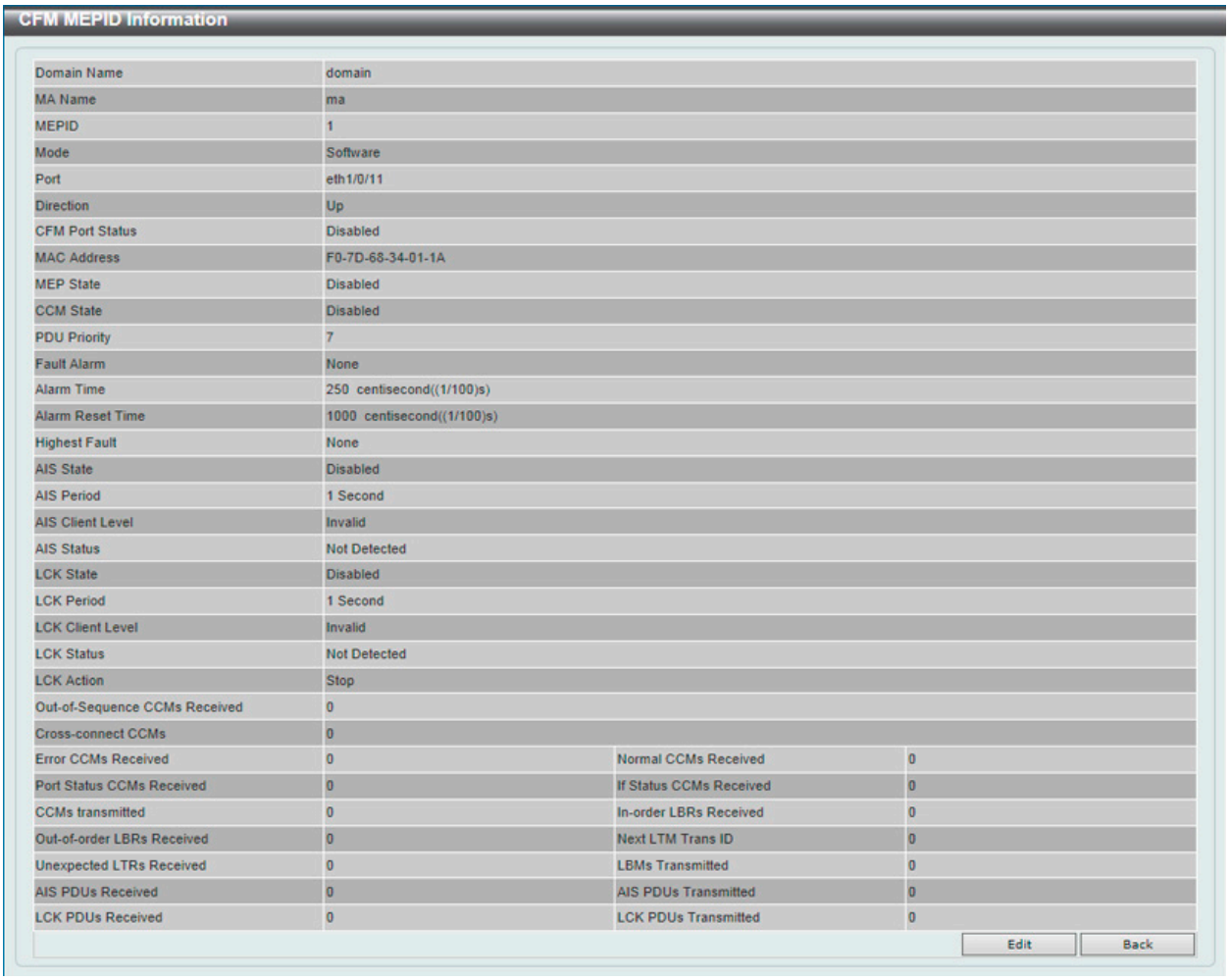
項目	説明
MEP ID	MEP ID を入力します。同一 MA 内に存在する MEP には、それぞれ固有の MEP ID を設定する必要があります。別の MD に設定される MA には同じ MA 識別子が設定されていても問題ありません。MEP を作成する前に、MA の MEP ID リストに MEP ID を設定しておく必要があります。 • 設定可能範囲：1-8191
Port	使用するユニットとポートを指定します。
Direction	MEP の方向を指定します。 • 「Up」- 内向き（アップ）MEP を作成します。 • 「Down」- 外向き（ダウン）MEP を作成します。

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

「Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

詳細情報の参照（Show Detail）

「Show Detail」ボタンをクリックし、以下の画面を表示します。



CFM MEPID Information

Domain Name	domain		
MA Name	ma		
MEPID	1		
Mode	Software		
Port	eth1/0/11		
Direction	Up		
CFM Port Status	Disabled		
MAC Address	F0-7D-68-34-01-1A		
MEP State	Disabled		
CCM State	Disabled		
PDU Priority	7		
Fault Alarm	None		
Alarm Time	250 centisecond((1/100)s)		
Alarm Reset Time	1000 centisecond((1/100)s)		
Highest Fault	None		
AIS State	Disabled		
AIS Period	1 Second		
AIS Client Level	Invalid		
AIS Status	Not Detected		
LCK State	Disabled		
LCK Period	1 Second		
LCK Client Level	Invalid		
LCK Status	Not Detected		
LCK Action	Stop		
Out-of-Sequence CCMs Received	0		
Cross-connect CCMs	0		
Error CCMs Received	0	Normal CCMs Received	0
Port Status CCMs Received	0	If Status CCMs Received	0
CCMs transmitted	0	In-order LBRs Received	0
Out-of-order LBRs Received	0	Next LTM Trans ID	0
Unexpected LTRs Received	0	LBMs Transmitted	0
AIS PDUs Received	0	AIS PDUs Transmitted	0
LCK PDUs Received	0	LCK PDUs Transmitted	0

Edit　Back

図 13-6　Show Detail Information 画面

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「Apply」ボタンをクリックして設定内容を適用します。

「Back」をボタンをクリックし、前のページに戻ります。

MEP の編集

「Edit」ボタンをクリックし、以下の画面を表示します。

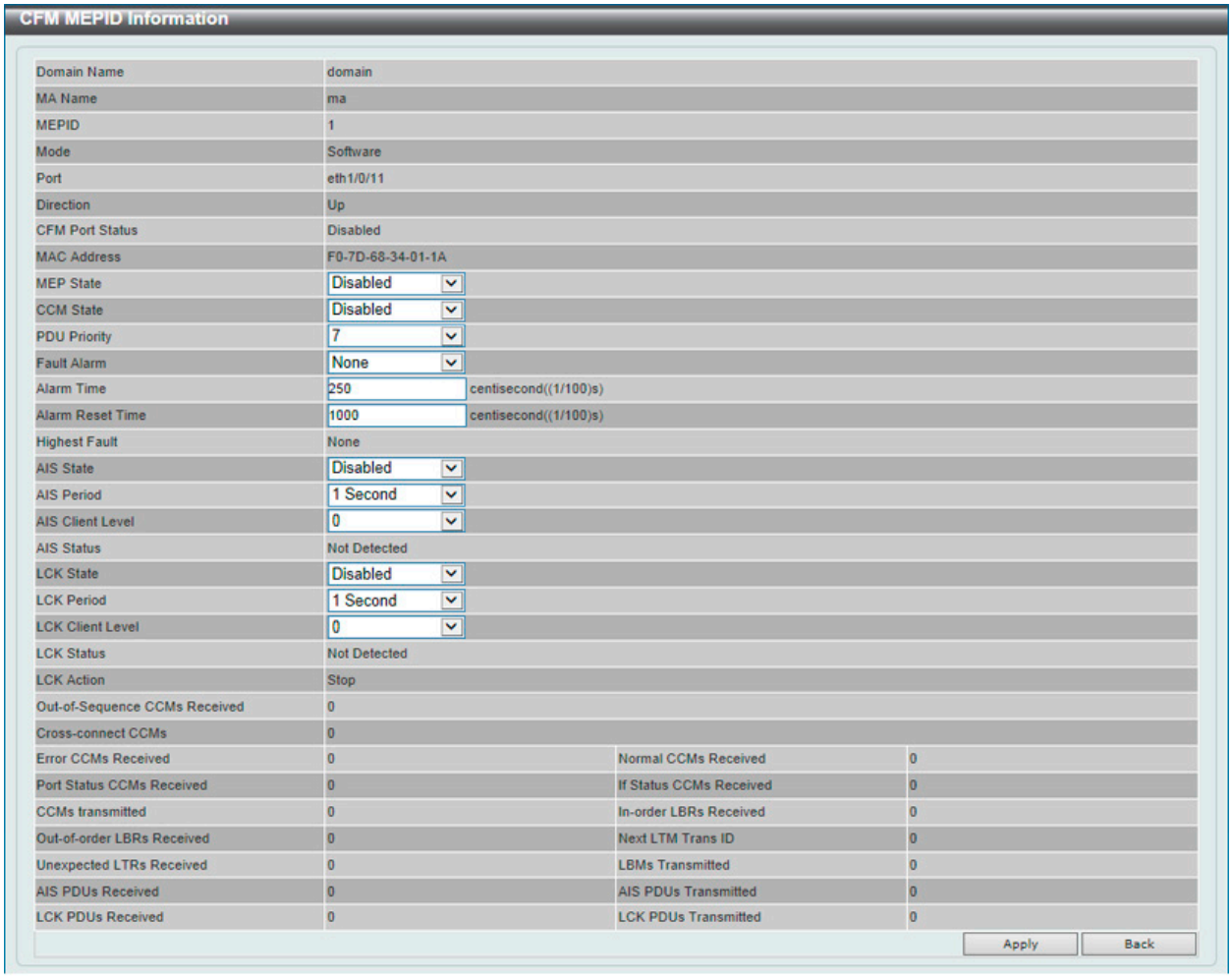


図 13-7　CFM MEP Information 画面 - Edit

以下の項目が表示されます。

項目	説明
MEP State	MEP 管理状態を有効 / 無効に設定します。
CCM State	CCM 送信状態を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
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、802.1p プライオリティがセットされます。 • 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。（初期値） • 「AI」I - 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「Some Remote MEP MAC Status Error」（リモート MEP の MAC ステータスエラー）以上である障害アラームだけが送信されます。 • 「Remote-CCM」- 優先度が「Some Remote MEP Down」（リモート MEP のダウン）以上である障害アラームだけが送信されます。 • 「Error-CCM」- 優先度が「Error CCM Received」（エラー CCM の受信）以上である障害アラームだけが送信されます。 • 「Xcon-CCM」- 優先度が「Cross-connect CCM Received」（クロスコネクト CCM の受信）以上である障害アラームだけが送信されます。
Alarm Time	障害検出後に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。

項目	説明
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、最も近いクライアントレイヤの MIP と MEP が存在する 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。
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、最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。 • 設定可能範囲：0-7

「Edit」ボタンをクリックすると設定を編集することができます。設定変更後、「Apply」ボタンをクリックして設定内容を適用します。
「Back」をボタンをクリックし、前のページに戻ります。

Remote MEP（CFM Settings）

Remote MEP を参照します。

OAM > CFM > CFM Settings 画面で「Remote MEP」ボタンをクリックします。

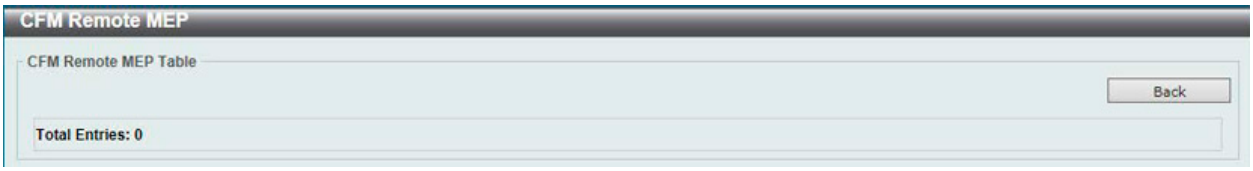


図 13-8　Remote MEP 画面

「Back」をクリックすると前のページに戻ります。

Edit LCK（CFM Settings）

LCK を編集します。

OAM > CFM > CFM Settings 画面で「Edit LCK」ボタンをクリックします。

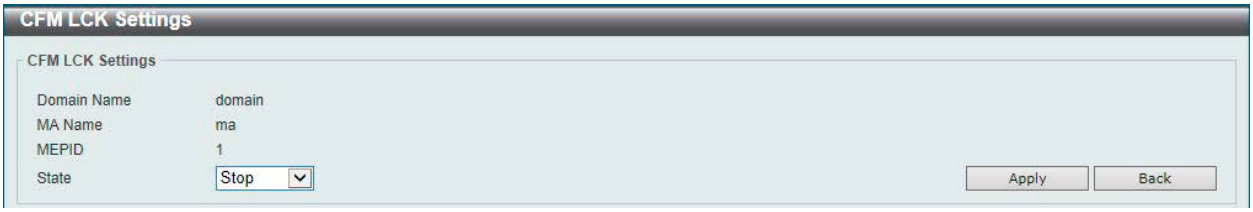


図 13-9　Edit LCK 画面

以下の項目が表示されます。

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）」

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

Edit DM（CFM Settings）

DM を編集します。

OAM > CFM > CFM Settings 画面で「Edit DM」ボタンをクリックします。

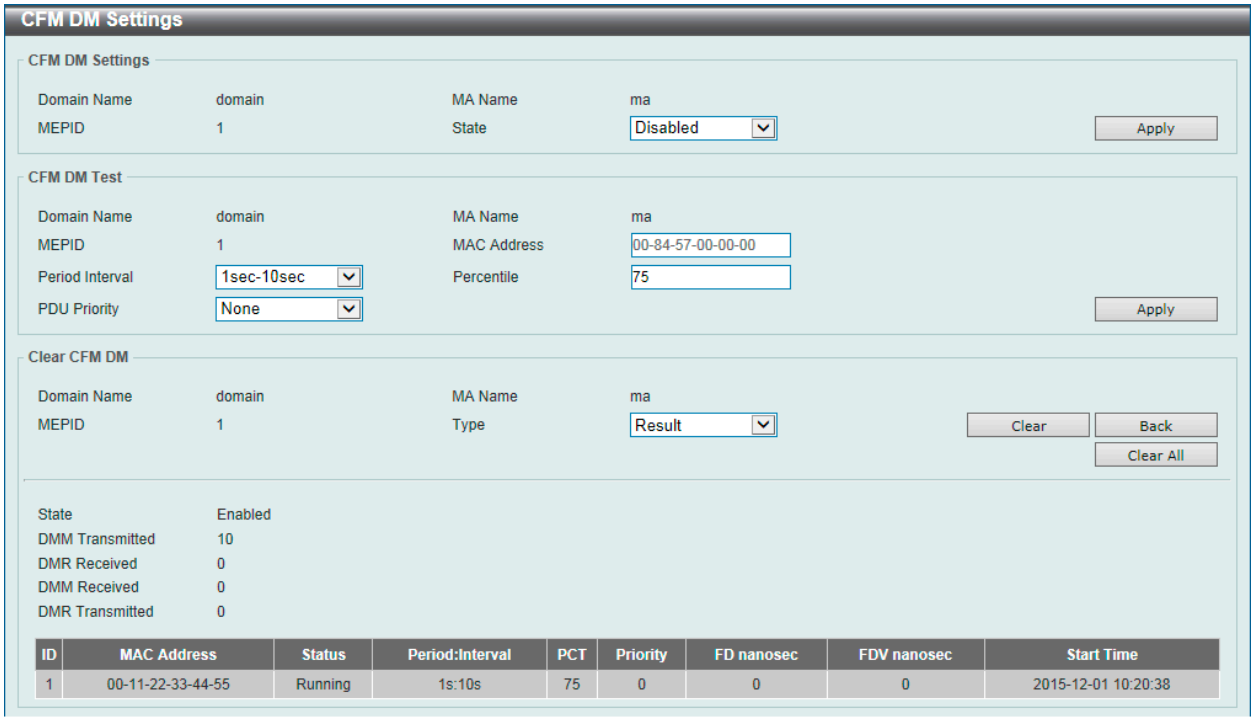


図 13-10　Edit DM 画面

以下の項目が表示されます。

項目	説明
CFM DM Settings	
State	「ITU Y.1731」フレーム「Delay Measurement」(DM) 機能を有効 / 無効に設定します。MEP で本機能が有効化されている場合、MEP はタイムスタンプを生成し、DMM メッセージ受信時に DMR メッセージを返信できるようになります。
CFM DM Test	
MAC Address	DM テストで使用する MAC アドレスを指定します。
Period Interval	DMM メッセージの送信間隔と診断の間隔を指定します。 • 「100ms-1sec」- 送信間隔は 100 ミリ秒、診断間隔は 1 秒です。 • 「1sec-10sec」- 送信間隔は 1 秒、診断間隔は 10 秒です。（初期値） • 「10sec-1min」- 送信間隔は 10 秒、診断間隔は 1 分です。
Percentile	パーセンタイル値を指定します。「Frame Delay」(FD) と「Frame Delay Variation」(FDV) のパーセンタイルを指定します。 • 設定可能範囲：0-100 • 初期値：75
PDU Priority	PDU 優先値を選択します。MEP によって送信される DMM メッセージ内にセットされる 802.1p 優先値を指定します。 • 設定可能範囲：0-7
Clear CFM DM	
Type	消去する情報の種類について指定します。 • 「Result」- DM 情報について消去します。 • 「Statistics」-「ETH-DM」フレーム (DMM と DMR) の統計について消去します。

「Clear」をクリックして、指定条件に基づく CFM DM 統計情報をクリアします。
「Clear All」をクリックして、すべての FM DM 統計情報をクリアします。
「Back」をクリックすると前のページに戻ります。

Edit LM（CFM Settings）

LM を編集します。

OAM > CFM > CFM Settings 画面で「Edit LM」ボタンをクリックします。

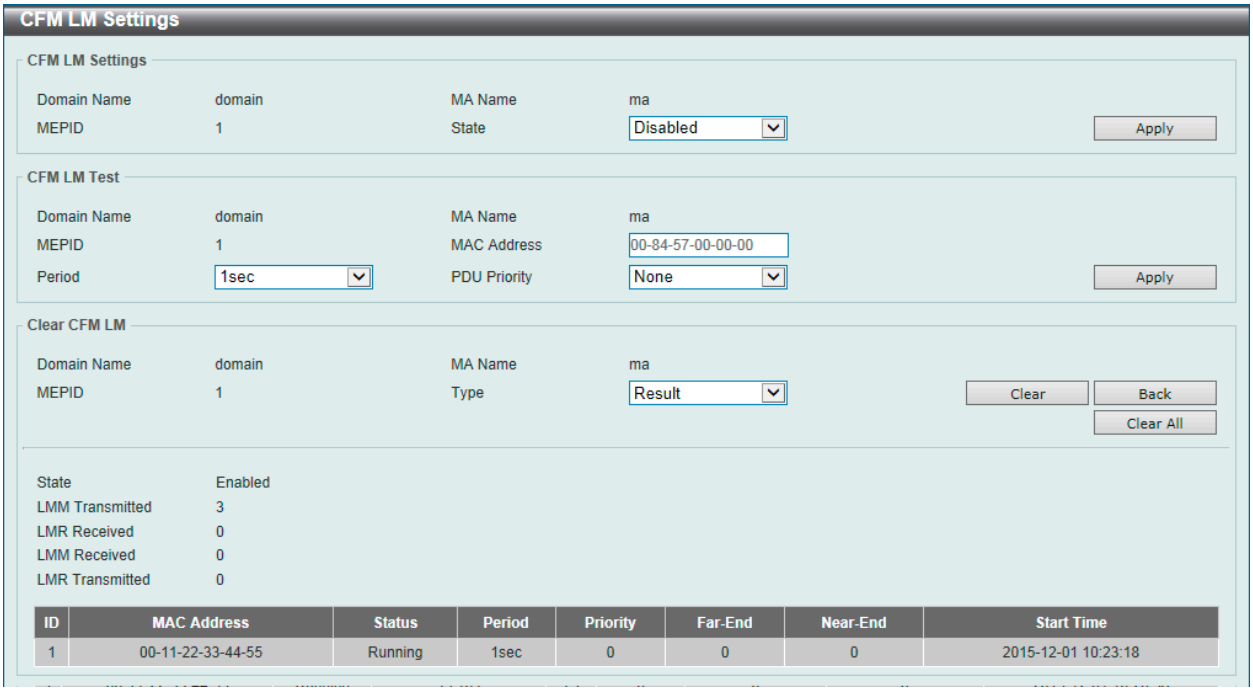


図 13-11　Edit LM 画面

以下の項目が表示されます。

項目	説明
CFM LM Settings	
State	「ITU Y.1731」フレーム「Loss Measurement」(LM) 機能を有効 / 無効に設定します。本設定を有効にすると、MEP はフレームロス計測のカウンタを維持し、LMM メッセージ受信時に LMR メッセージを返信できるようになります。
CFM LM Test	
MAC Address	MAC アドレスを指定します。
Period	LM PDU の送信間隔を指定します。 • 「100ms」- 送信間隔は 100 ミリ秒です。 • 「1sec」- 送信間隔は 1 秒です。 • 「10sec」- 送信間隔は 10 秒です。
PDU Priority	PDU 優先値を選択します。MEP によって送信される LMM メッセージに含まれる 802.1p 優先値を指定します。 • 設定可能範囲：0-7
Clear CFM LM	
Type	消去する情報の種類について指定します。 • 「Result」- LM 情報について消去します。 • 「Statistics」-「ETH-LM」フレーム (LMM と LMR) の統計について消去します。

「Clear」をクリックして、指定条件に基づく CFM LM 統計情報をクリアします。
「Clear All」をクリックして、すべての FM LM 統計情報をクリアします。
「Back」をクリックすると前のページに戻ります。

CFM Port Settings（CFM ポート設定）

CFM ポート状態を有効 / 無効に設定します。

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。

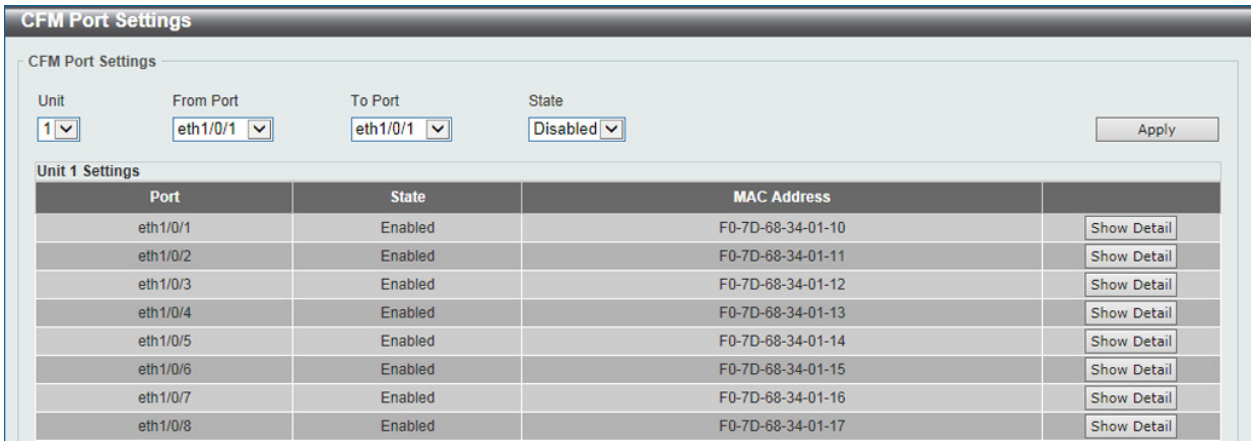


図 13-12　CFM Port Settings 画面

以下の項目が表示されます。

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。
State	特定ポートの CFM 設定を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）

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

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 13-13　CFM Port Settings - Show Detail 画面

「Back」をクリックすると前のページに戻ります。

CFM Loopback Test（CFM ループバックテスト）

CFM ループバックを設定します。

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。

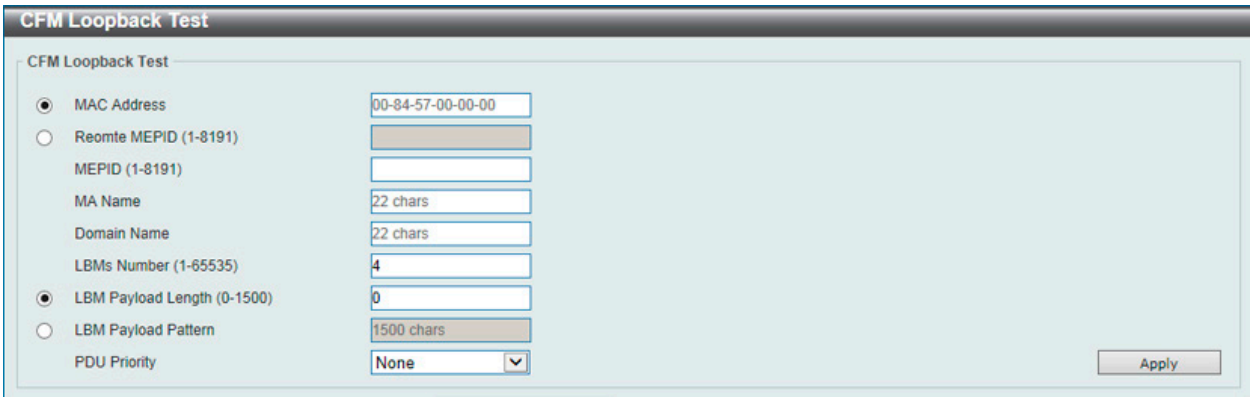


図 13-14　CFM Loopback Settings 画面

以下の項目が表示されます。

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 字以内）スペースは許可されません。
PDU Priority	送信される LBM に設定される 802.1p 優先度を指定します。指定しない場合、MA が送信した CCM と同じ優先度を使用します。 • 選択肢：0-7 • 初期値：「None」（なし）

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

CFM Linktrace Settings（CFM リンクトレース設定）

CFM リンクトレースを設定します。

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。

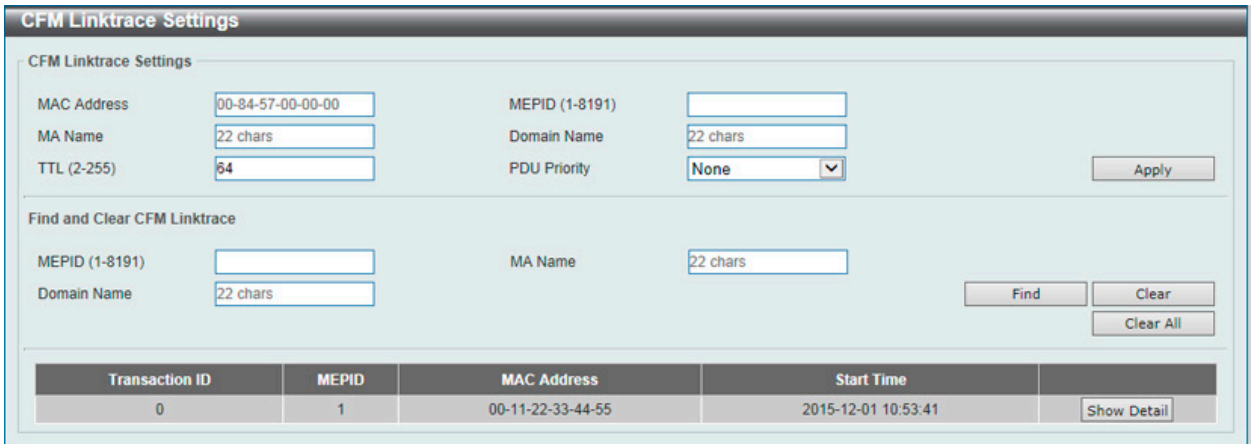


図 13-15　CFM Linktrace Settings 画面

以下の項目が表示されます。

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 優先度を選択します。指定しない場合、MEP が送信した CCM と同じ優先度を使用します。 • 選択肢：：0-7 • 初期値：「None」（なし）
Find and Clear CFM Linktrace	
MEP ID	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）

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear」をクリックして、指定条件に基づく情報をクリアします。
「Clear All」をクリックして、すべての情報をクリアします。
「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。

詳細情報の表示
エントリ検出後、「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。

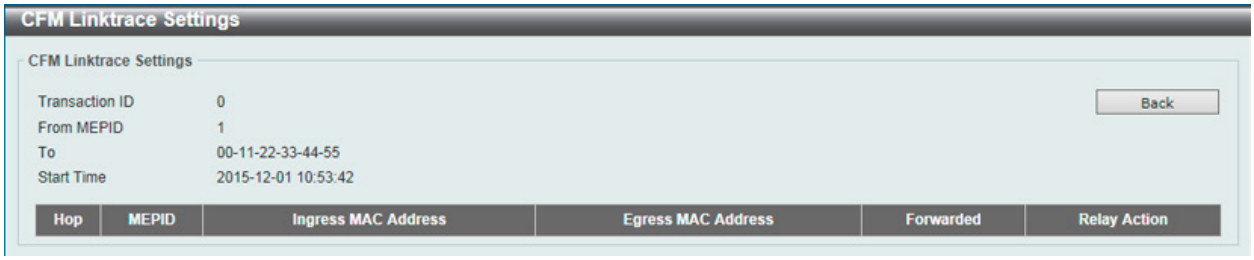


図 13-16　CFM Linktrace Settings 画面

「Back」をクリックすると前のページに戻ります。

CFM Packet Counter（CFM パケットカウンタ）

OSPF 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。

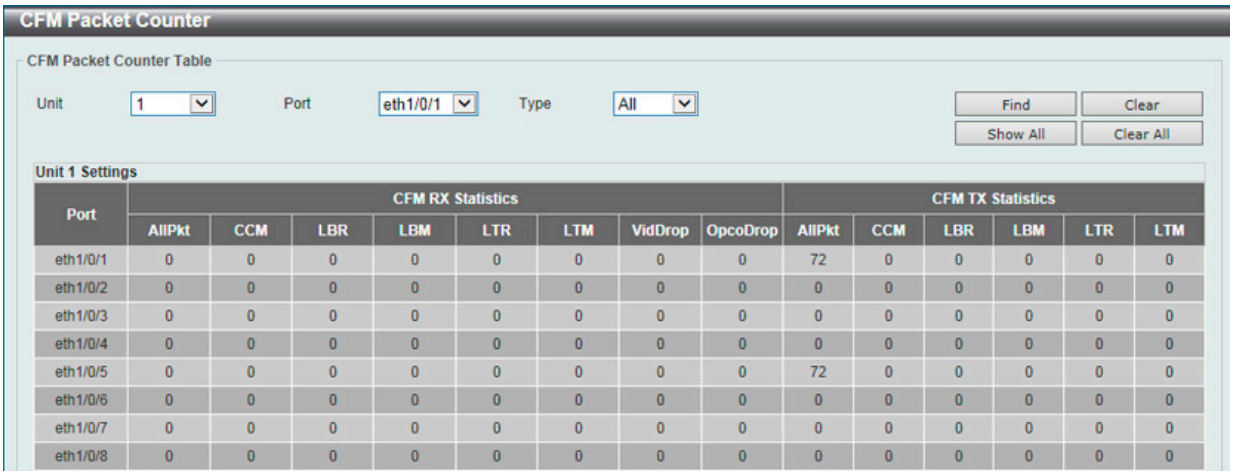


図 13-17　CFM Packet Counter 画面

画面には以下の項目があります。

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」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、指定条件に基づくカウンタ情報をクリアします。
「Clear All」をクリックすると、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 13-18　CFM Counter CCM 画面

「Clear」をクリックすると、すべての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 MIPCCM テーブル）

CFM MIPCCM 情報を表示します。

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 13-19　CFM MIP CCM Table 画面

CFM MEP Fault Table（CFM MEP 障害テーブル）

CFM MEP 障害テーブルを表示します。

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 13-20　CFM MEP Fault Table 画面

Cable Diagnostics（ケーブル診断機能）

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は UTP ケーブルを簡易的に確認するために設計されています。ケーブルの品質やエラーの種類を診断します。

補足　本機能は将来のファームウェアでサポート予定です。

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。

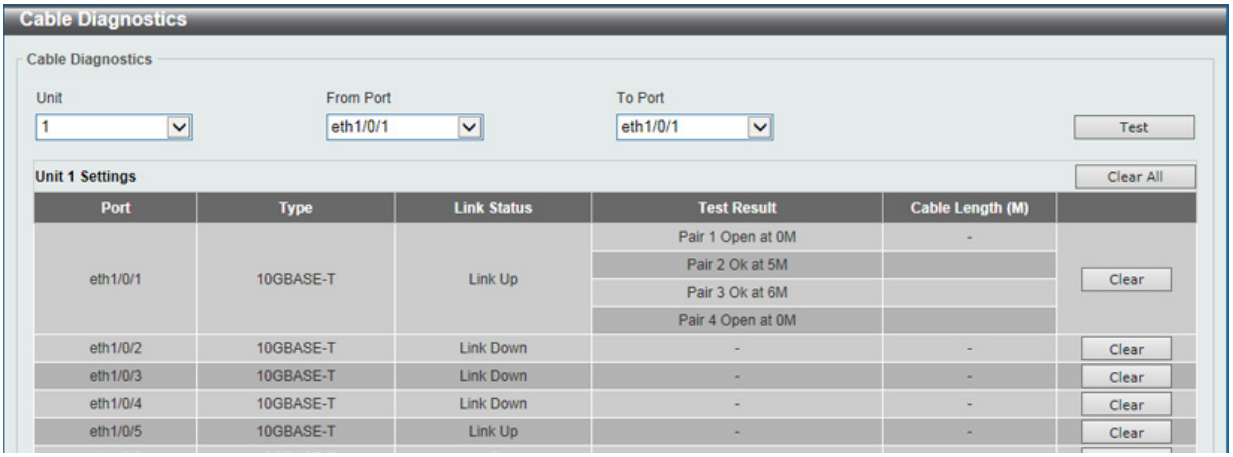


図 13-21　Cable Diagnostics 画面

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

注意　ケーブル診断を実行すると、対象のポートにおいてリンクダウンを伴います。

ケーブル診断機能の制限；

- GE ポートのみサポート
- 最大対応ケーブル長 120 メートル
- ケーブル長の誤差± 5 メートル

失敗した場合、以下のメッセージが表示されます。

項目	説明
Unknown	診断結果にはオープン、ショート、クロストークのステータスが含まれます。これらのいずれかのステータスとなった場合、不明エラーとなります。
NA	ケーブルが検出されませんでした。診断の仕様に当てはまらないか、品質が非常に悪い可能性があります。

Ethernet OAM（イーサネット OAM）

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。

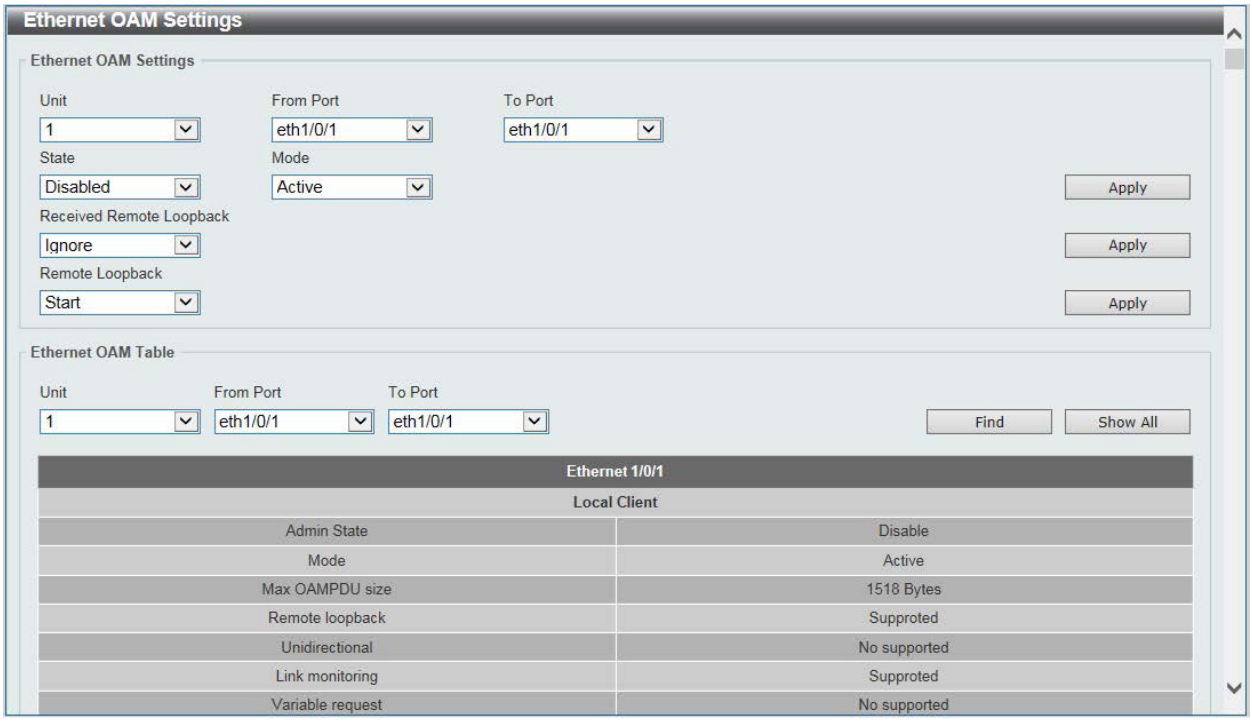


図 13-22　Ethernet OAM Settings 画面

以下の項目が表示されます。

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 状態の場合、ディスカバリが開始され、それ以外の場合、ピアから受信したディスカバリに反応します。
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 discovery 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。
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。

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

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

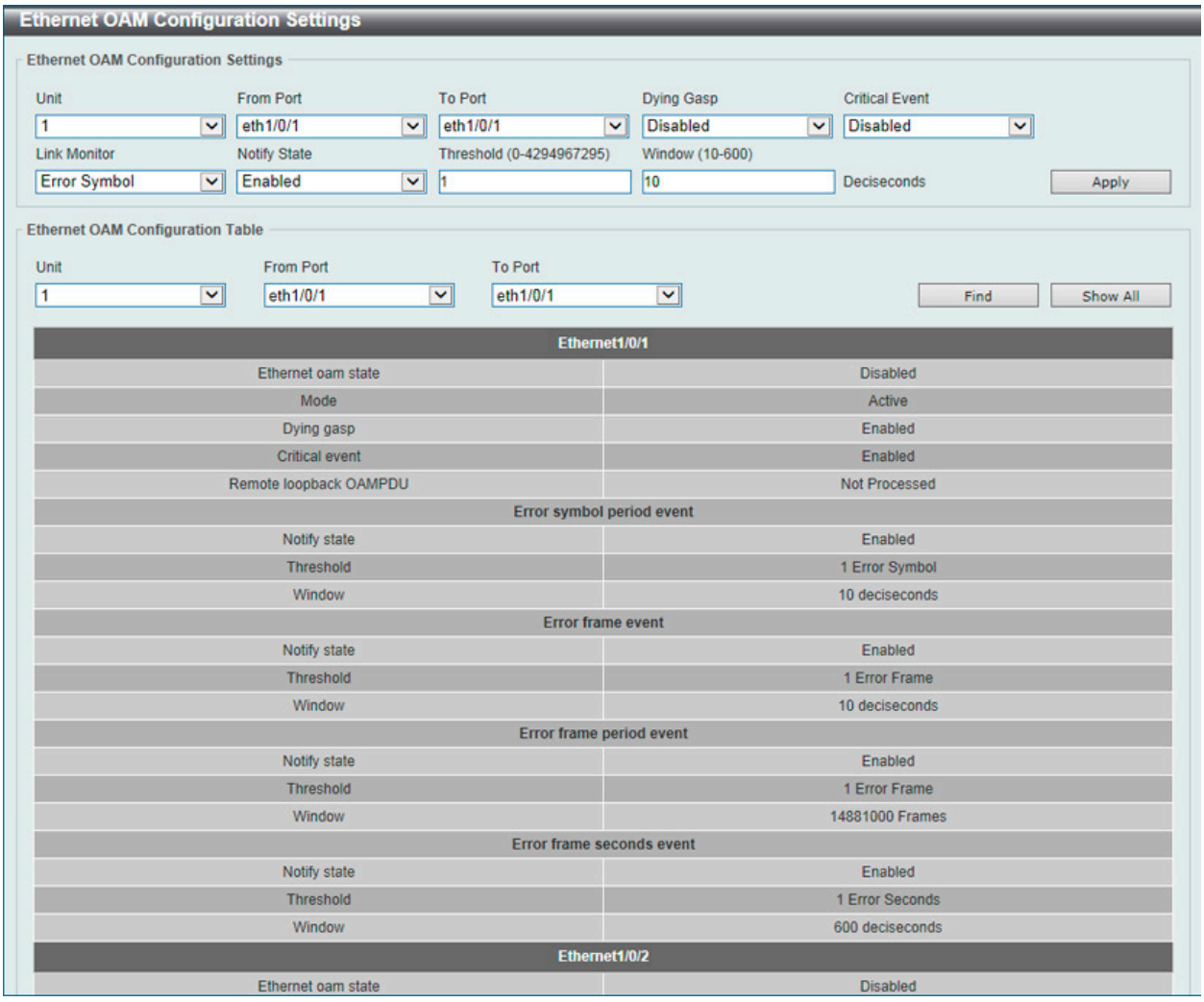


図 13-23　Ethernet OAM Configuration Settings 画面

以下の項目が表示されます。

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 Symbol」- イーサネット OAM エラーシンボル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」- 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	しきい値を設定します。 • 「Error Symbol」選択時 - シンボルエラーの数を入力します。指定期間（Window）におけるシンボルエラーの数がしきい値を超えた場合、イベントが生成されます。0-65535 の範囲で指定します。 • 「Error Frame」選択時 - フレームエラーの数を入力します。指定期間（Window）におけるフレームエラーの数がしきい値を超えた場合、イベントが生成されます。0-65535 の範囲で指定します。 • 「Error Frame Seconds」選択時 - フレームエラーの秒数を入力します。指定期間（Window）におけるフレームエラー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。1-900 の範囲で指定します。 • 「Error Frame Period」選択時 - フレームエラーの数を入力します。指定フレーム数（Window）におけるフレームエラーがしきい値を超えた場合、イベントが生成されます。1-65535 の範囲で指定します。
Window	ウィンドウを設定します。 • 「Error Symbol」選択時 - この期間内でシンボルエラー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シンボル期間イベント TLV が含まれます。10-600（デシ秒）の範囲で指定します。 • 「Error Frame」選択時 - この期間内でフレームエラー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フレーム期間イベント TLV が含まれます。10-600（デシ秒）の範囲で指定します。 • 「Error Frame Seconds」選択時 - この期間内でフレームエラー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フレーム秒サマリイベント TLV が含まれます。100-9000（デシ秒）の範囲で指定します。 • 「Error Frame Period」選択時 - この指定フレーム数で発生したフレームエラー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。148810-892860000 の範囲で指定します。
Ethernet OAM Configuration Table	
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。

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

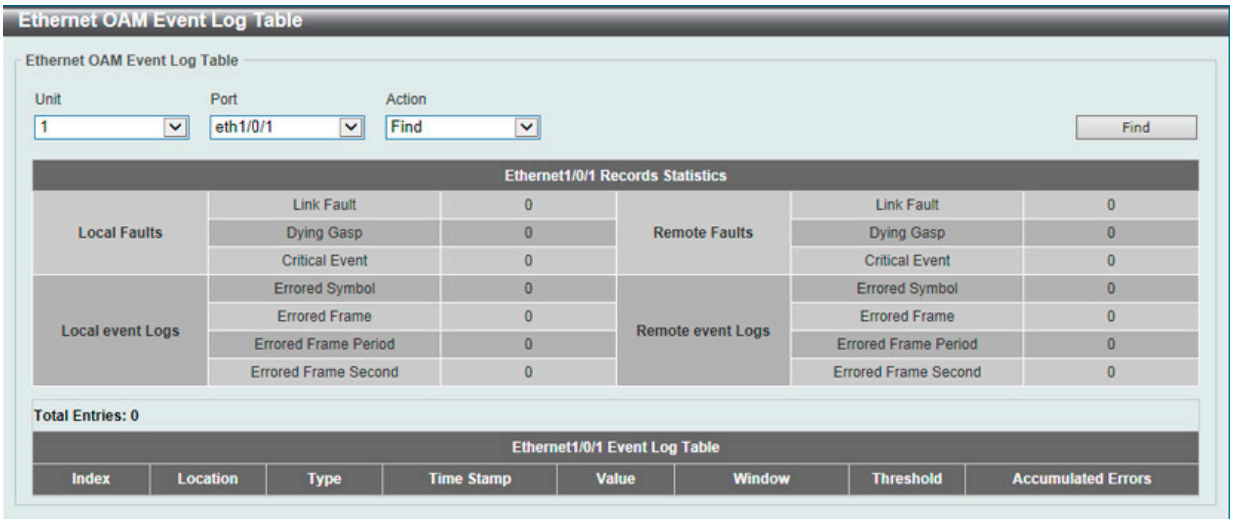


図 13-24　Ethernet OAM Event Log Table 画面

以下の項目が表示されます。

項目	説明
Unit	参照 / 削除するユニットを指定します。
Port	参照 / 削除するポート番号を選択します。
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。

「Find」ボタンをクリックし、指定ポートのログエントリを表示します。
「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、テーブル上の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）

スイッチの各ポートに関するイーサネット 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。

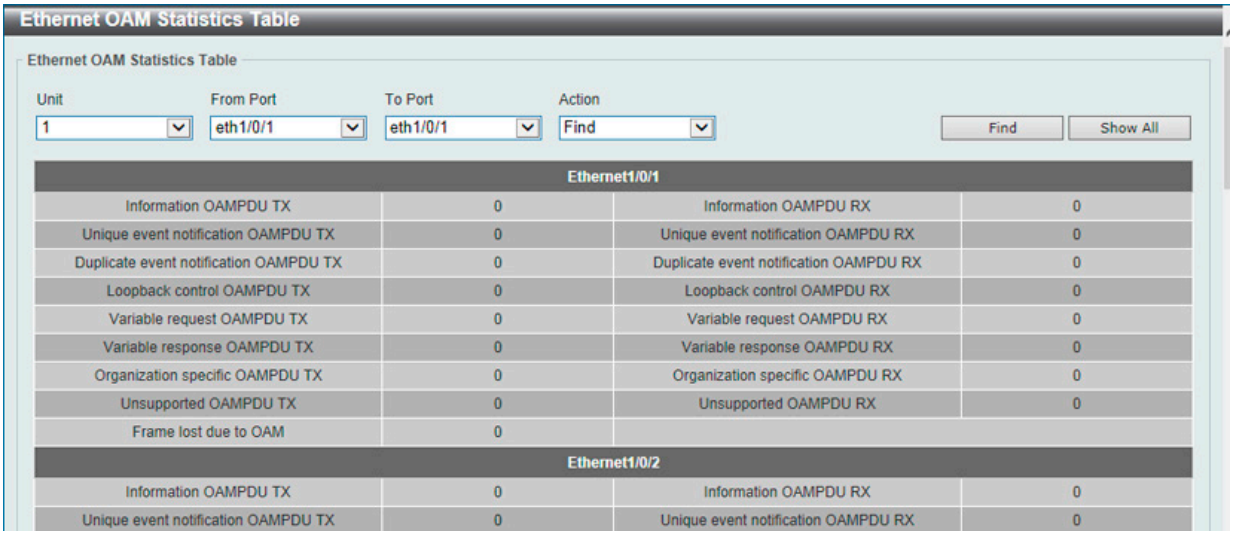


図 13-25　Ethernet OAM Statistics Table 画面

以下の項目が表示されます。

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。

項目	説明
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。

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

Ethernet OAM DULD Settings（イーサネット OAM DULD 設定）

スイッチの各ポートに関するイーサネット 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。

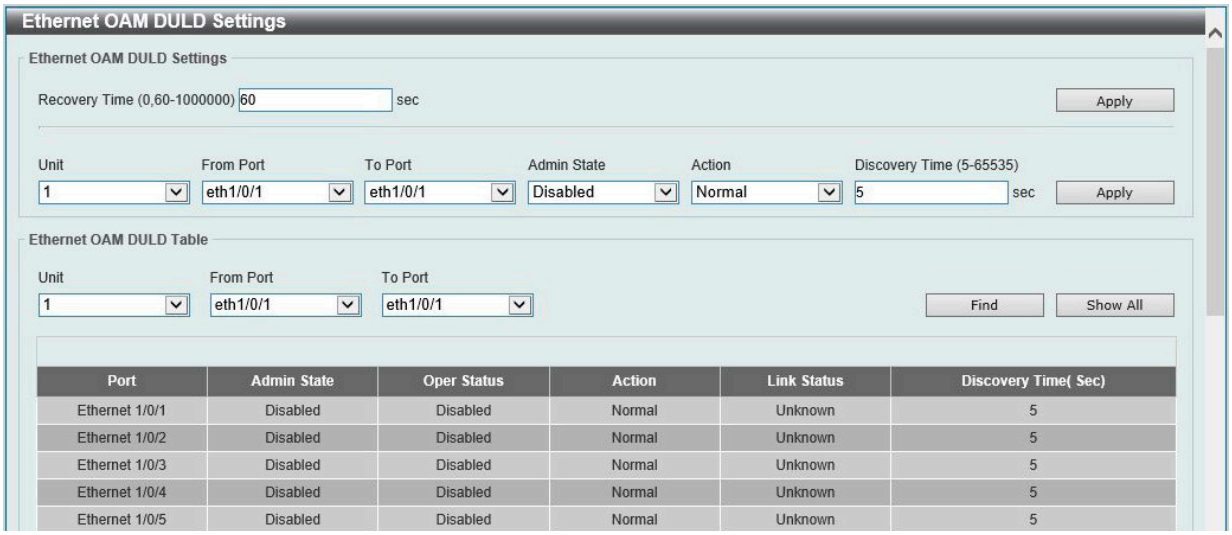


図 13-26　Ethernet OAM Statistics Table 画面

以下の項目が表示されます・

項目	説明
Ethernet OAM DULD Settings	
Recovery Time	リカバリタイムを設定します。
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。
Admin State	管理ステータスを有効 / 無効に設定します。
Action	アクションを選択します。 ・ 選択肢：「Normal」「Shutdown」
Discovery Time	ディスカバリタイムを設定します。

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックし、指定条件に基づくエントリを表示します。
「Show All」をクリックして、すべてのエントリを表示します。

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 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、Rx（受信）電力しきい値設定）を行うことができます。

DDM Settings（DDM 設定）

超過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。

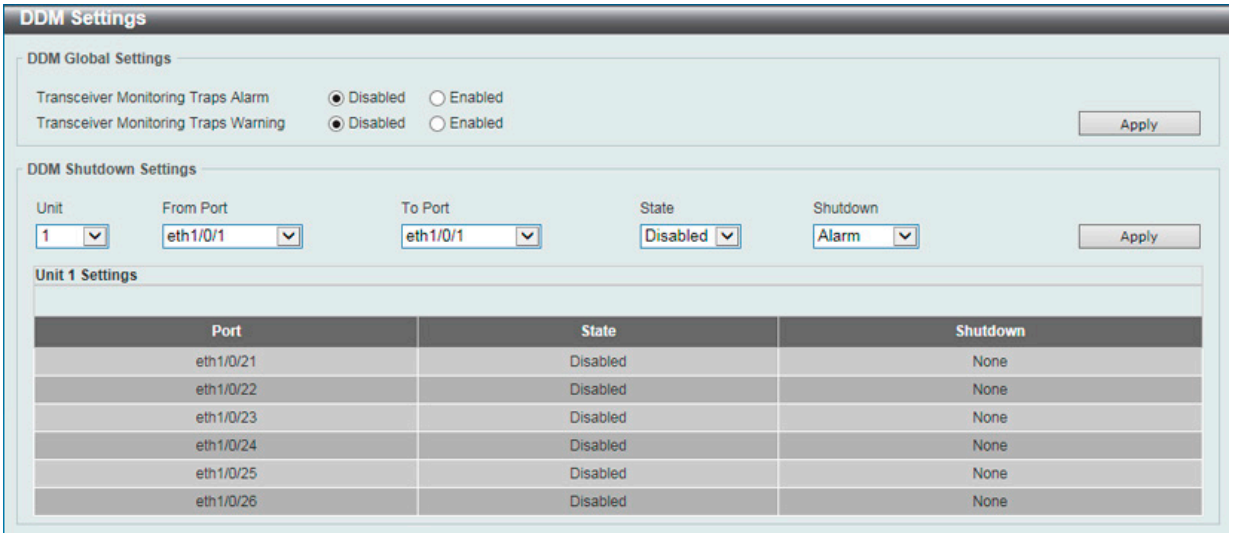


図 13-27　DDM Settings 画面

以下の項目が表示されます。

項目	説明
Transceiver Monitoring Traps Alarm	トランシーバモニタリングのトラップアラームを有効 / 無効に設定します。
Transceiver Monitoring Traps Warning	トランシーバモニタリングのトラップ警告を有効 / 無効に設定します。
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。
State	DDM の状態を有効 / 無効に設定します。
Shutdown	動作パラメータが Alarm または Warning 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」- 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」- 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）

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

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

スイッチの特定ポートに DDM 温度しきい値設定を行います。

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

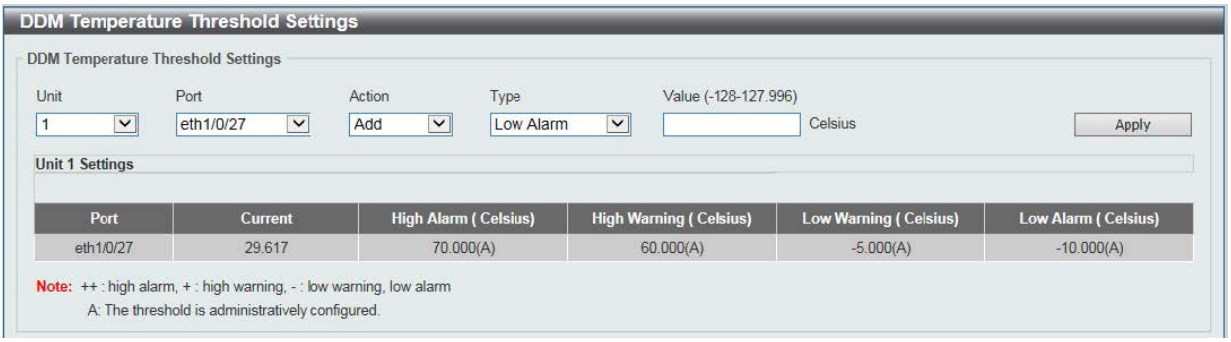


図 13-28　DDM Temperature Threshold Settings 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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（℃）

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

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

スイッチの特定ポートに電圧しきい値を設定します。

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

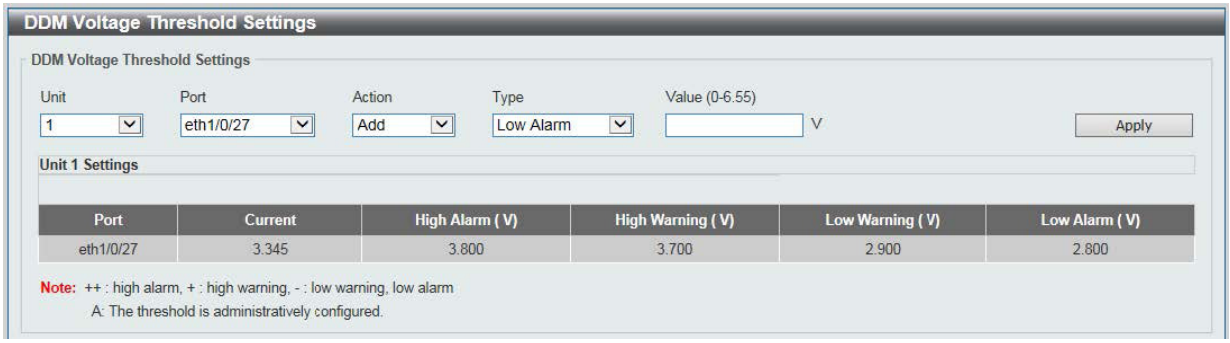


図 13-29　DDM Voltage Threshold Settings 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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）

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

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

スイッチの特定ポートにバイアス電流しきい値を設定します。

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

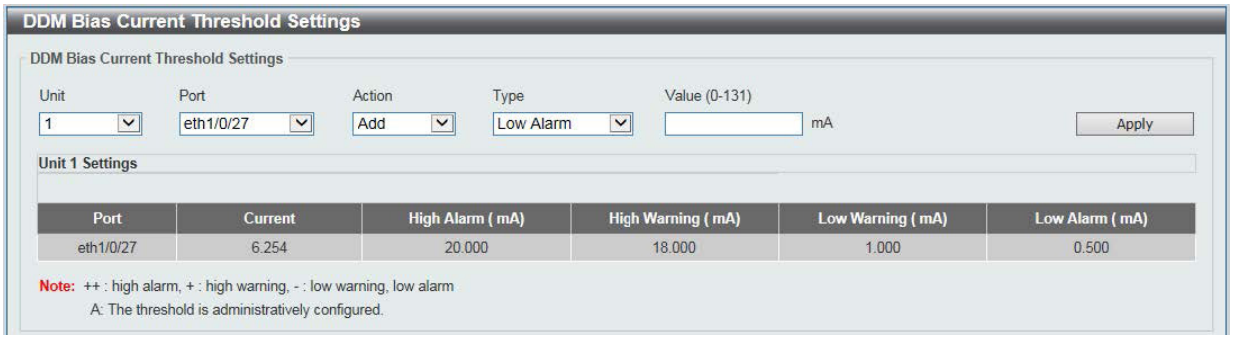


図 13-30　DDM Bias Current Threshold Settings 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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	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）

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

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

スイッチの特定ポートに送信電力しきい値を設定します。

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

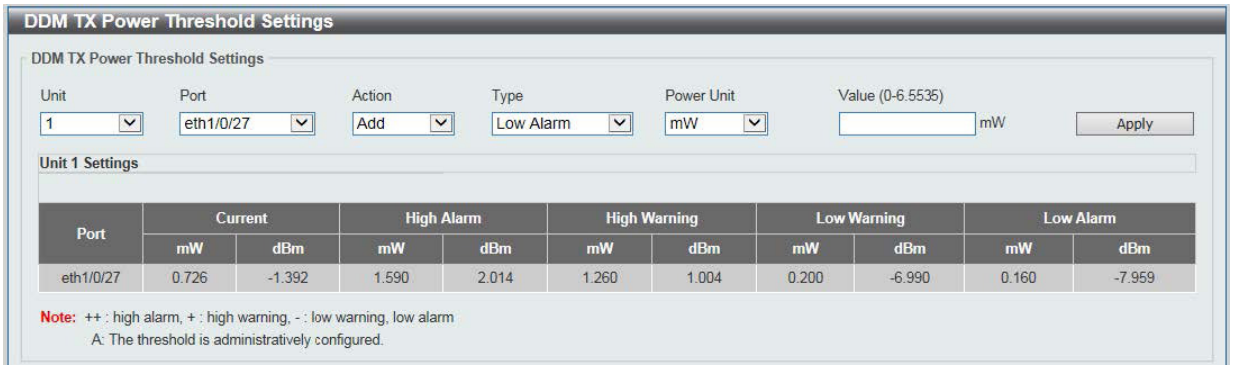


図 13-31　DDM TX Power Threshold Settings 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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」
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）

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

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

スイッチの特定ポートに受信電力しきい値を設定します。

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

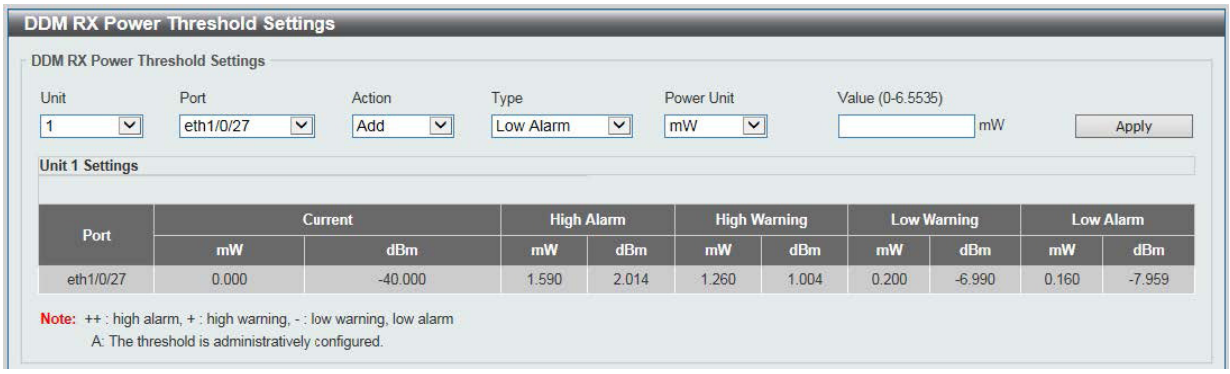


図 13-32　DDM RX Power Threshold Settings 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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）

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

DDM Status Table（DDM ステータステーブル）

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

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

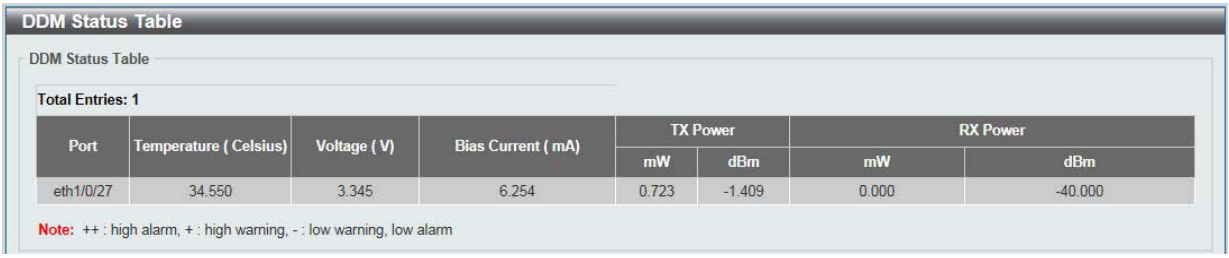


図 13-33　DDM Status Table 画面

以下の項目を表示します。

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

第 14 章　Monitoring（スイッチのモニタリング）

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
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（RFC3176）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。

Utilization（利用分析）

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。

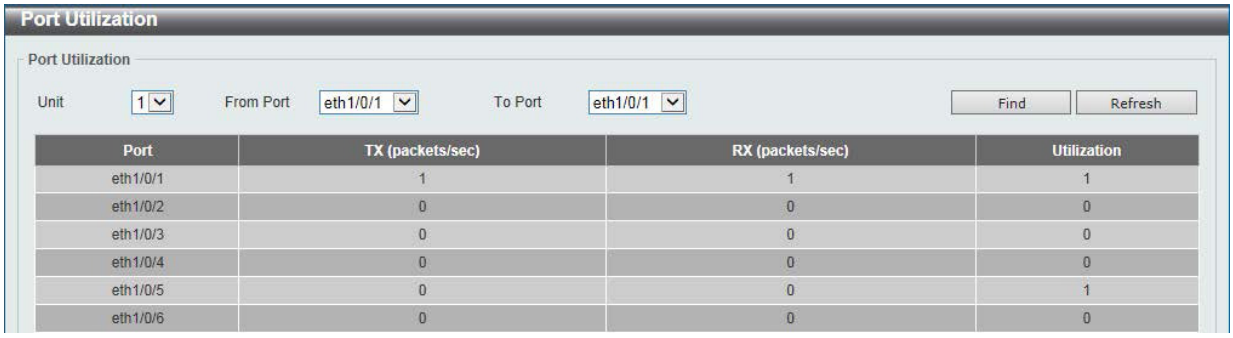


図 14-34　Port Utilization 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを指定します。
Port	表示するポート番号を選択します。

「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。
「Refresh」ボタンをクリックして、テーブルを更新します。

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）

ポート毎のパケット送受信の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。

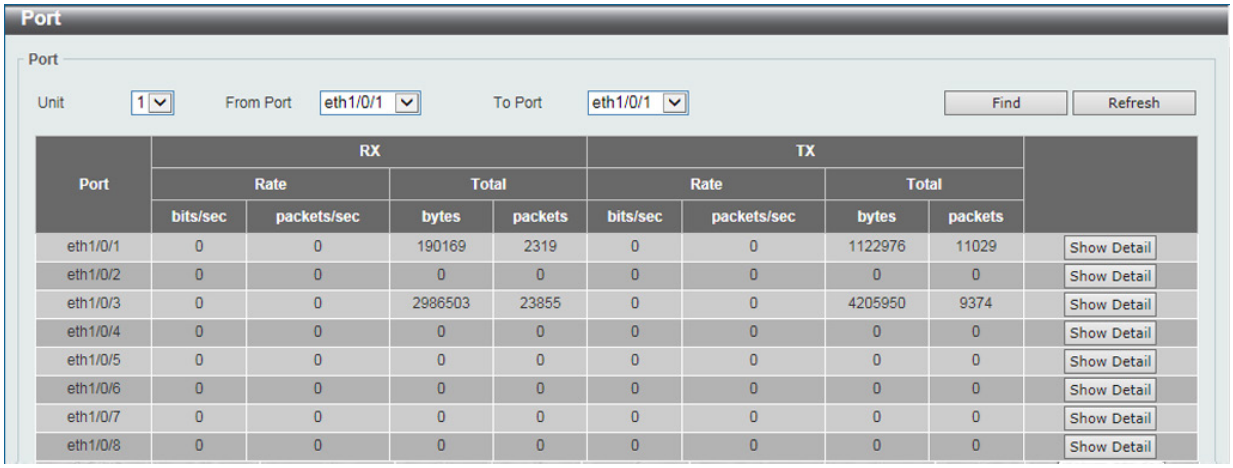


図 14-35　Port Statistics 画面

以下の項目が表示されます。

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

「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。
「Refresh」ボタンをクリックして、テーブルを更新します。

ポート毎の詳細情報の表示

「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。

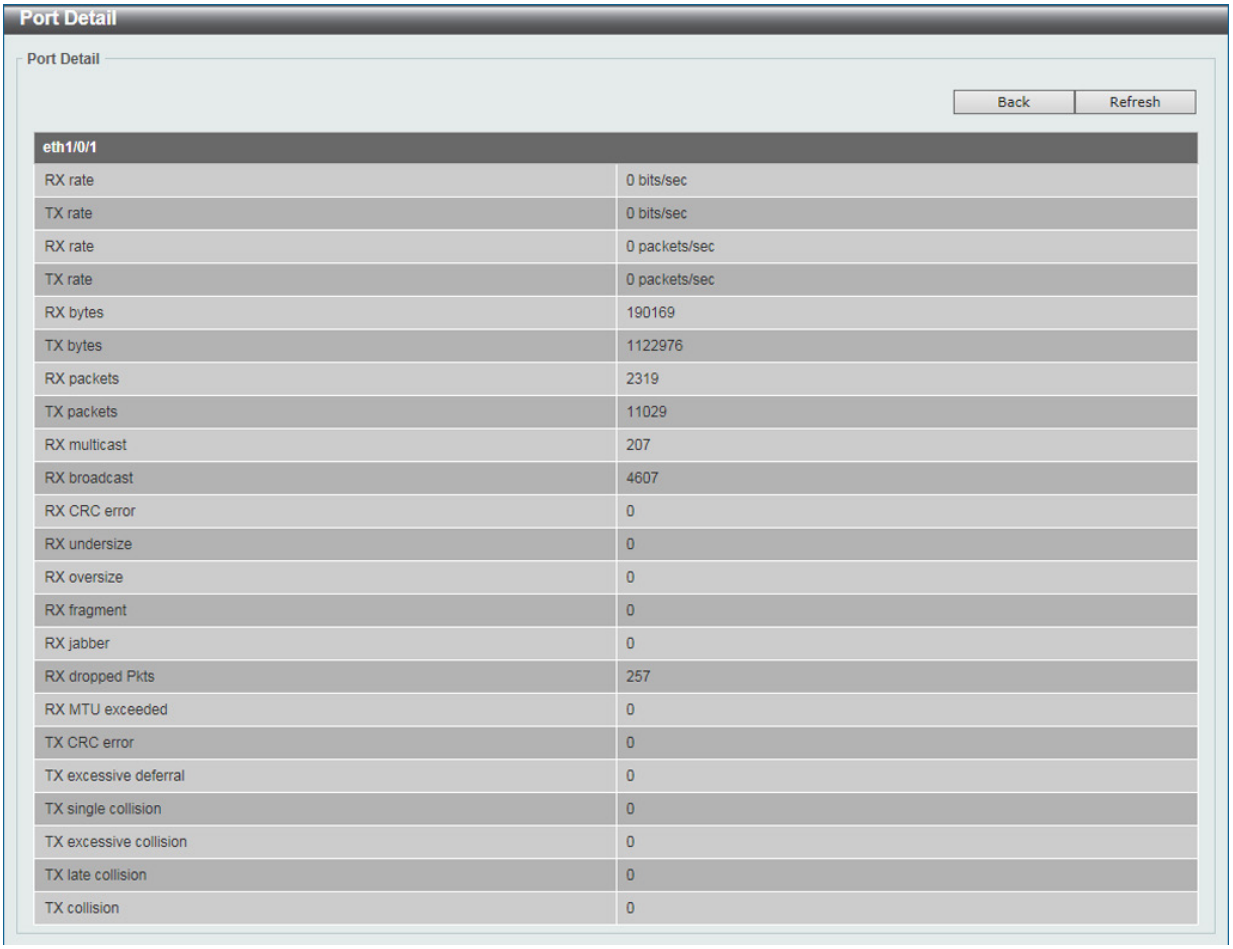


図 14-36　Port Statistics - Show Detail 画面

「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Back」ボタンをクリックし、前の画面に戻ります。

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。

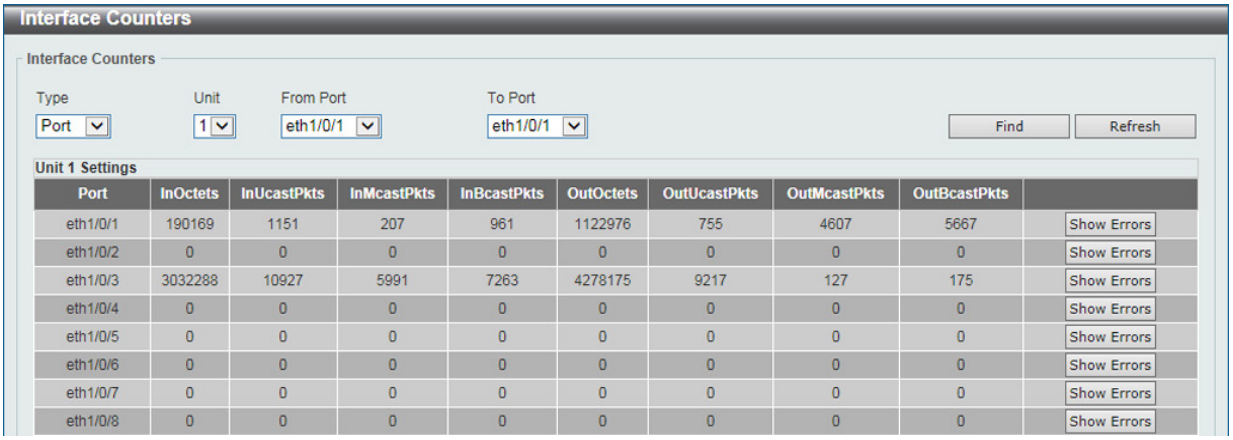


図 14-37　Interface Counters 画面

以下の項目が表示されます。

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指定します。

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

「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。
「Refresh」ボタンをクリックして、テーブルを更新します。

ポート毎のエラー情報の表示

「Show Errors」ボタンをクリックすると、次の画面が表示されます。

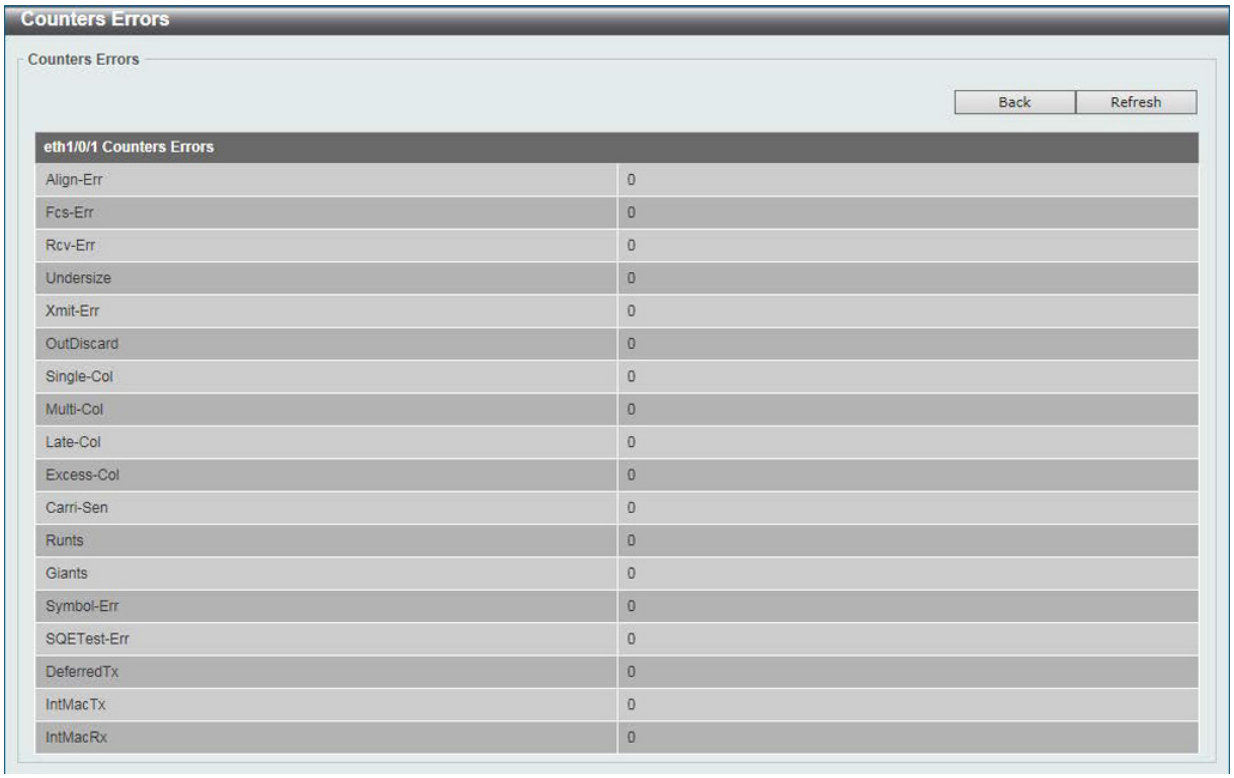


図 14-38　Interface Counters (Show Errors) 画面

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

Counters（カウンタ）

すべてのポートのカウンタ情報を表示、消去します。

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



図 14-39　Counters 画面

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Type	表示する情報のタイプを指定します。 ・ 選択肢：「Port」

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、指定条件に基づくエントリを検索 / 表示します。
「Refresh」ボタンをクリックして、テーブルを更新します。
「Clear」ボタンをクリックして、指定条件に基づく情報を消去します。
「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。

詳細情報の表示

「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。

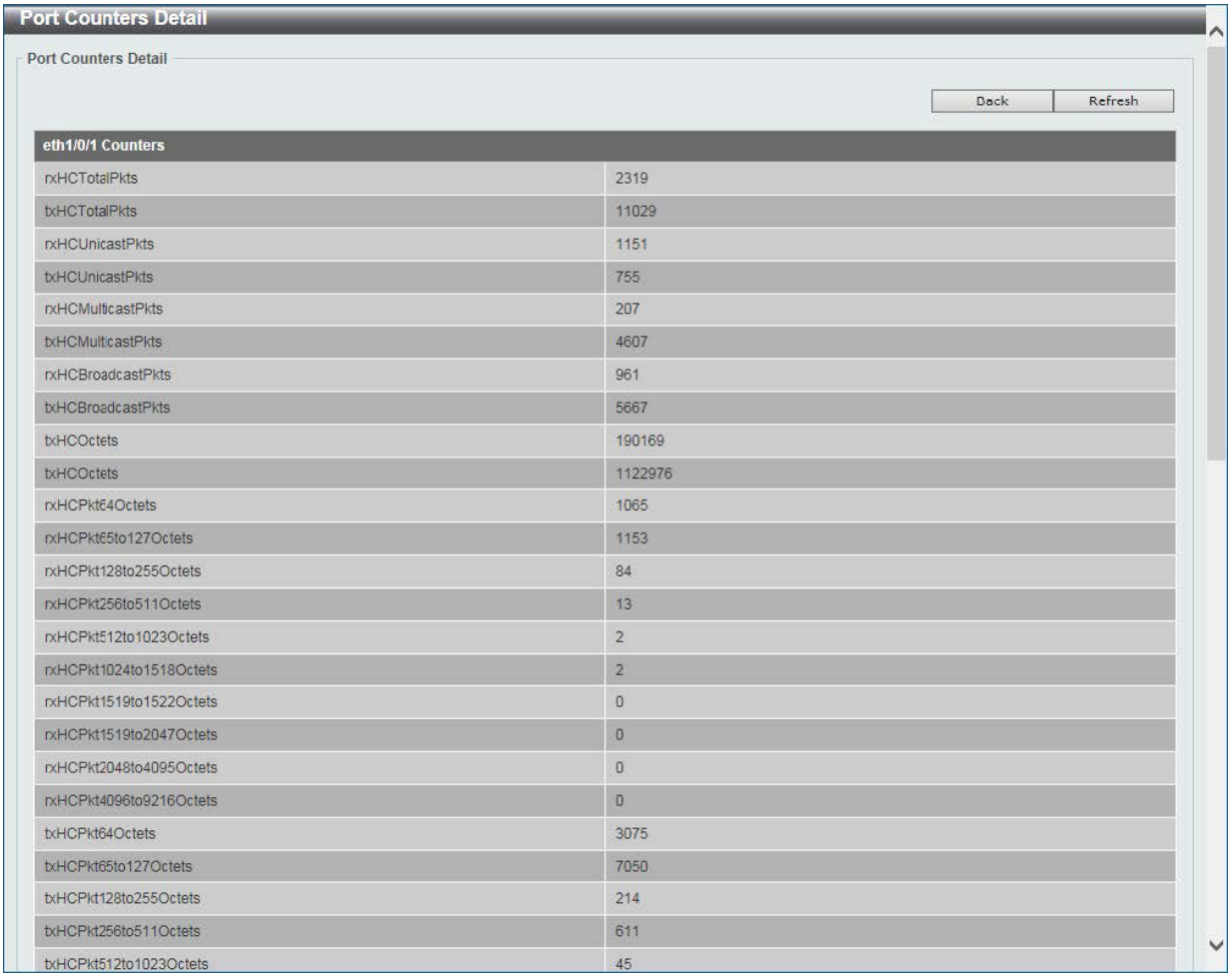


図 14-40　Port Counters Detail 画面

「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Back」ボタンをクリックし、前の画面に戻ります。

Mirror Settings（ミラー設定）

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

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

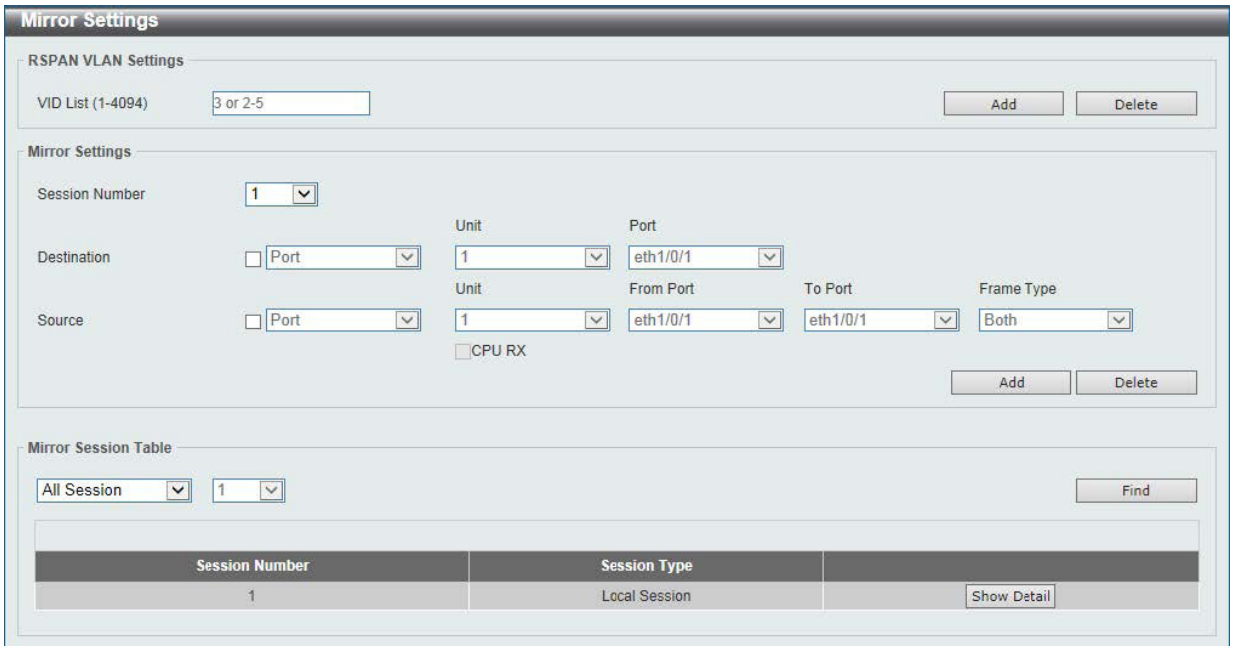


図 14-41　Mirror Settings 画面

以下の情報が表示されます。

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を設定します。 宛先タイプオプションとして • 「Port」-「Port」を選択した後に、宛先ユニットやポート番号を指定します。 • 「Remove VLAN」-「Remote VLAN」を選択した後に、宛先ユニットやポート番号を指定し、「VID」（2-4094）を指定します。 • 「Replace」-「Replace」を選択した後に、ACL 名と、「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を設定します。 • 「Port」-「Port」を選択した後に、ユニット ID と「From Port」および「To Port」の番号を指定します。また、「Frame Type」オプションを指定します。「Frame Type」で指定可能なオプションは「Both」「RX」「TX」「TX Forwarding」です。「Both」を選択すると送受信どちらのトラフィックもミラーされます。「RX」の場合、受信トラフィックのみミラーされ、「TX」は送信トラフィックのみミラーされます。「CPU RX」オプションにチェックを入れると、CPU RX トラフィックを監視します。 • 「ACL」- ACL プロファイル名を入力します。 • 「VLAN」-「VLAN」を選択した後に、「VID List」を指定し、Frame Type を選択します。 • 「Remove VLAN」-「Remote VLAN」を選択した後に「VID」（2-4094）を指定します。
Mirror Session Table	
Mirror Session Type	表示する情報のミラーセッションを選択します。 • 選択肢：「All Session」「Session Number」「Remote Session」「Local Session」 「Session Number」を選択した後、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、設定内容に基づくエントリを追加します。
「Delete」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。
「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。

注意　LACP/STP/ERPS などの機能によりパケットの送信が制限されている場合でも、TX のミラーリングは行われます。

詳細情報の表示

Show Detail」リンクをクリックし、以下の画面を表示します。

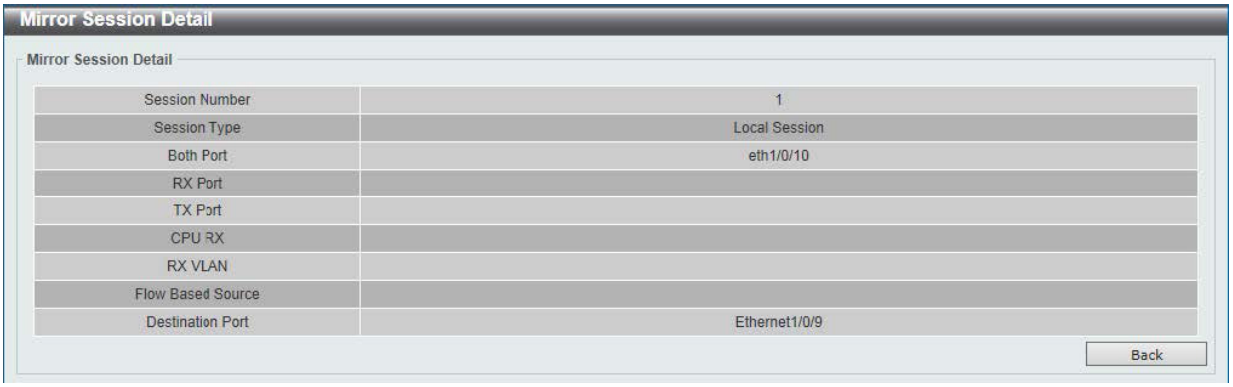


図 14-42　Mirror Settings - Show Detail 画面

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、設定します。

Monitoring > sFlow > sFlow Agent 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。

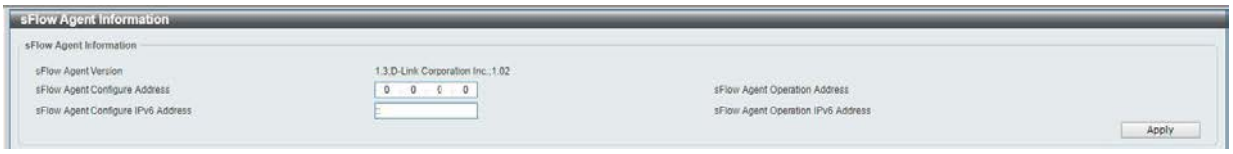


図 14-43　sFlow Agent Information 画面

以下の項目が表示されます。

項目	説明
sFlow Agent Version	sFlow エージェントバージョンを表示します。
sFlow Agent Address	sFlow エージェント IP アドレスを設定します。
sFlow Agent IPv6 Address	sFlow エージェント IPv6 アドレスを設定します。

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

sFlow Receiver Settings（sFlow レシーバ設定）

sFlow エージェントのレシーバ設定と設定表示を行います。レシーバは sFlow エージェントから消去や追加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。

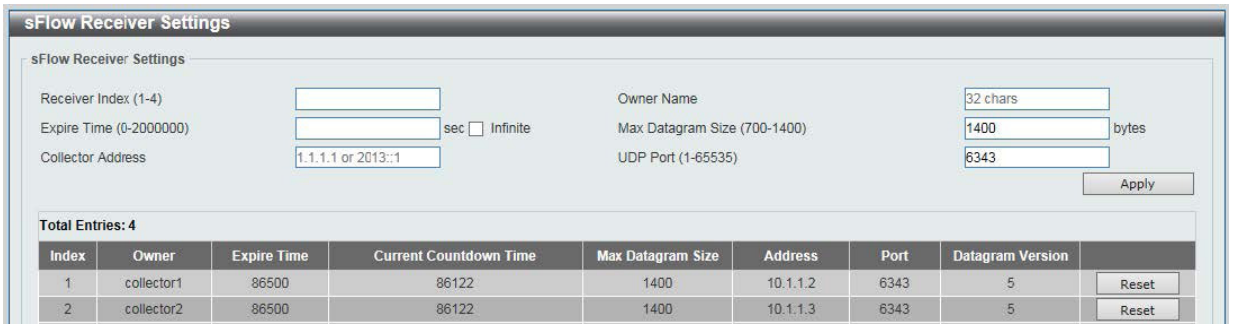


図 14-44　sFlow Receiver Settings 画面

以下の項目が表示されます。

項目	説明
Receiver Index	追加する 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）

項目	説明
Expire Time	タイムアウト時間を指定します。期限になるとエントリの設定値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 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
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 ポートを指定します。 • 設定可能範囲：1-65535 • 初期値：6343

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

ネットワークからサンプルパケットを取得するための設定をします。これには、サンプリングのレートや抽出されるパケットヘッダの量も含まれます。

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。

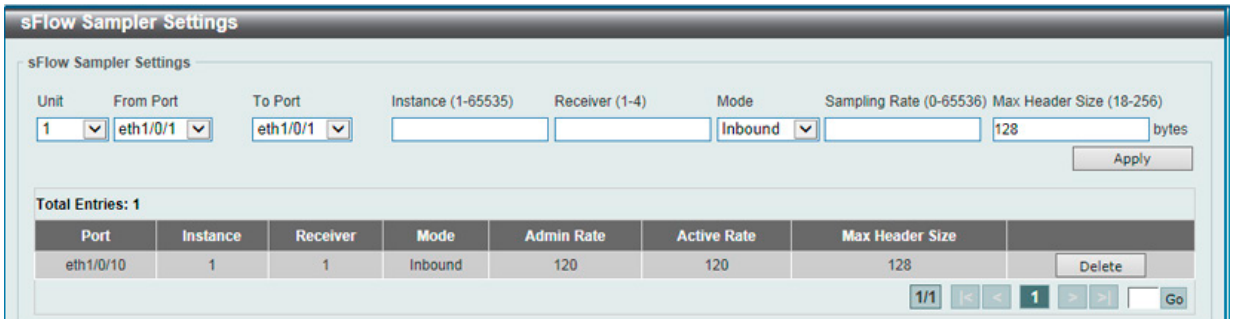


図 14-45　sFlow Sampler Settings 画面

以下の項目が表示されます。

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。
Instance	インタフェースに複数のサンプラを設定する場合、インスタンスの識別番号を指定します。
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」- サンプルのイングレスパケットを指定します。（初期値） •「Outbound」- サンプルのイーグレスパケットを指定します。
Sampling Rate	パケットサンプリングのレートを設定します。エントリ「0」は、パケットのサンプリングを無効にします。指定しない場合、初期値の「0」となります。 • 設定可能範囲：0-65536 • 初期値：0
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）

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

sFlow Poller Settings（sFlow ポーラ設定）

スイッチのポーラの設定を行います。

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 14-46　sFlow Poller Settings 画面

以下の項目が表示されます。

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。
Instance	1 つの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
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	ポーリングサンプリングの間隔を設定します。「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（秒）

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

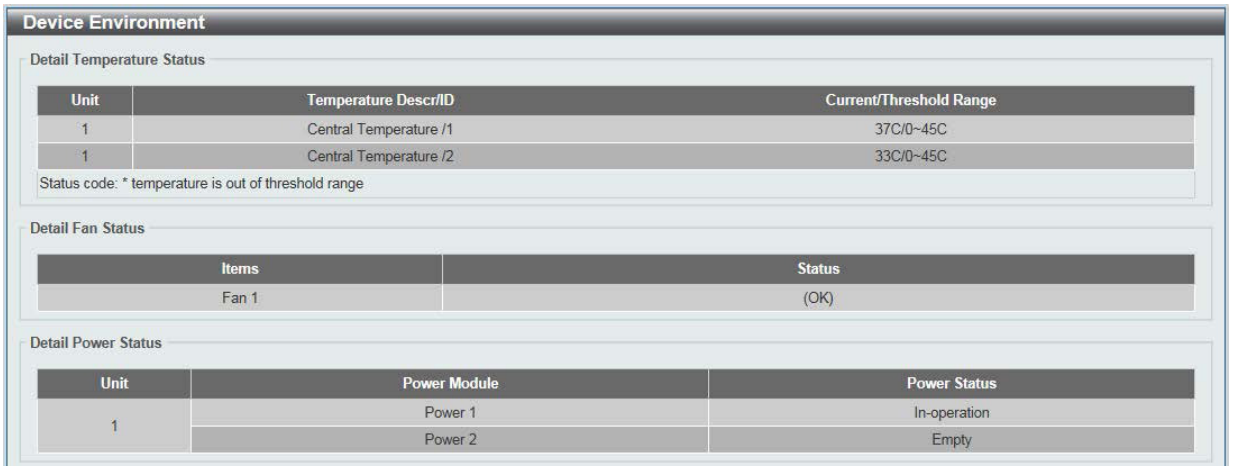


図 14-47　Device Environment 画面

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

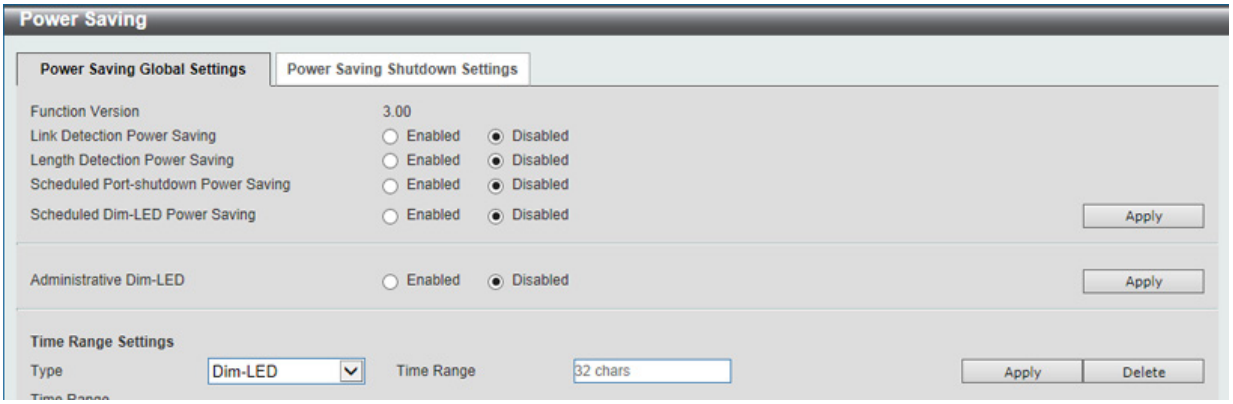


図 15-1　Power Saving - Power Saving Global Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Global Settings タブ	
Link Detection Power Saving	「リンク検出」を有効 / 無効に設定します。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。
Length Detection Power Saving	「ケーブル長検出」を有効 / 無効に設定します。本設定を有効にすると、ポートに接続されているケーブルの長さを自動的に検出し、必要に応じてポートの電力消費を調整します。
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 Dim-LED Power Saving	スケジュールによりスイッチの LED 照明を消すことで、消費電力を抑えます。
Administrative Dim-LED	ポート LED 機能の有効 / 無効を指定します。
Type	省電力モードの種類を指定します。 • 選択肢：「Dim-LED」
Time Range	上記省電力機能に対応するスケジュールを指定します。

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

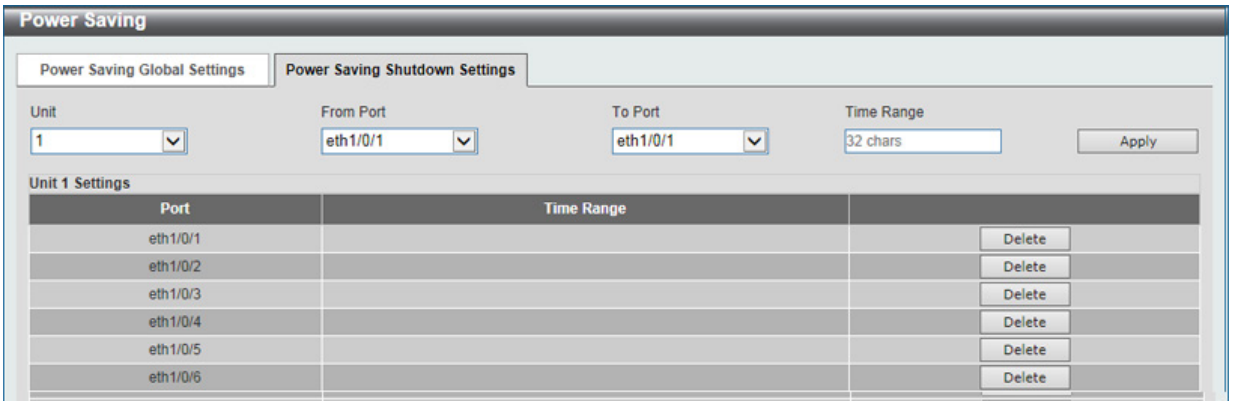


図 15-2　Power Saving - Power Saving Shutdown Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Shutdown Settings タブ	
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。

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

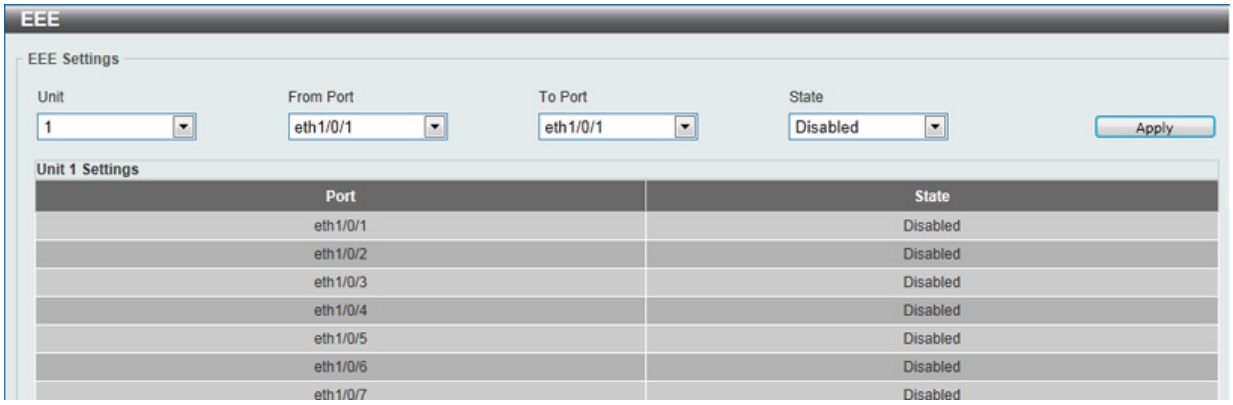


図 15-3　EEE 画面

以下の設定項目を使用して表示を変更します。

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。
State	本機能を有効 / 無効に設定します。

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

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

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

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 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）	各種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）	各種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。
Log Backup（ログファイルのバックアップ）	各種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）

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

コンフィグレーションの保存

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。

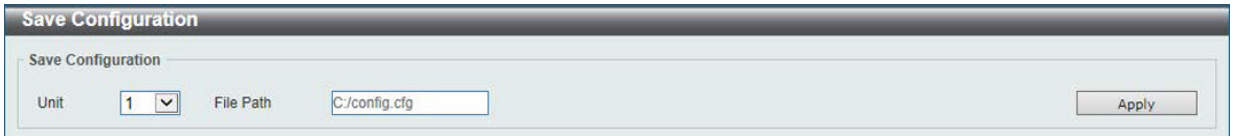


図 16-1　Save - Configuration 画面

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。

注意　copy コマンドや Flash への書き込み中は TELNET や CLI などの操作ができなくなります。書き込み終了までしばらくお待ちください。

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）

注意　copy コマンドや Flash への書き込み中は TELNET や CLI などの操作ができなくなります。書き込み終了までしばらくお待ちください。

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。

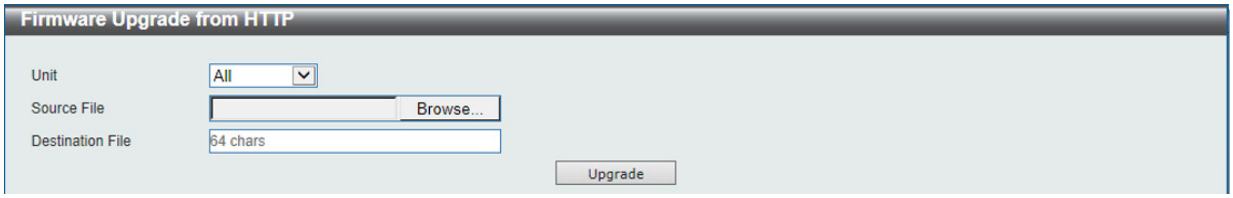


図 16-2　Firmware Upgrade from HTTP 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。（64 文字以内） 「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアが保存されるスイッチの場所を指定します。（64 文字以内）

「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。

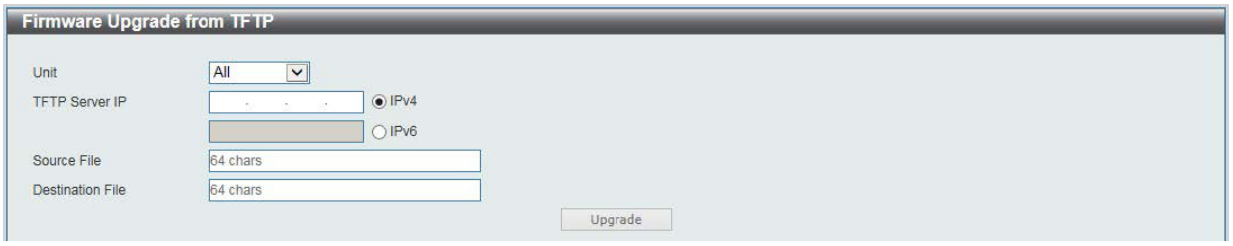


図 16-3　Firmware Upgrade from TFTP 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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） 「Browse/ 参照」ボタンをクリックし TFTP サーバ上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアが保存されるスイッチの場所を指定します。（64 文字以内）

「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 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 HTTP をクリックし、設定画面を表示します。

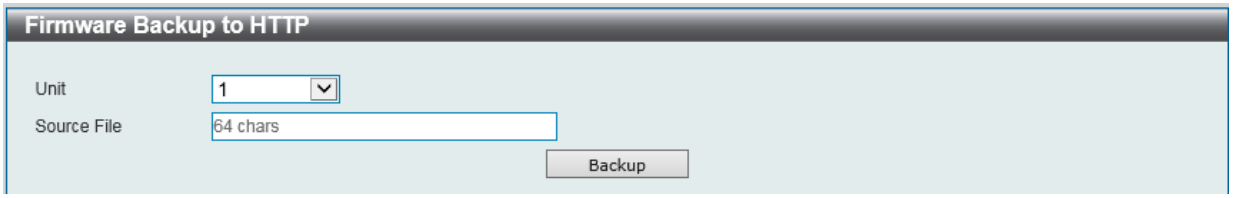


図 16-4　Firmware Backup to HTTP 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	スイッチ上でファームウェアが保存されているファイルパスとファイル名を入力します。（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。

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 16-5　Firmware Backup to TFTP 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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ファイルパスとファイル名を入力します。（64 文字以内）
Destination File	ファームウェアファイルがバックアップされる TFTP サーバの場所（パス / ファイル名）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。

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

重要　初期状態に何か設定が追加されている 状態で、別の設定を runnning-config にコピーすることはしないでください。予期せぬ動作の原因となります。必ず、running-config をクリアしてから、新しい設定を runnning-config にコピーするようにしてください。

注意　copy コマンドや Flash への書き込み中は TELNET や CLI などの操作ができなくなります。書き込み終了までしばらくお待ちください。

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

HTTP サーバを使用してローカル PC から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 16-6　Configuration Restore from HTTP 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	ローカル PC 上のコンフィグレーションパスとファイル名を入力します。（64 文字以内） 「Browse/ 参照」ボタンをクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定できます。
Destination File	コンフィグレーションファイルが保存されるスイッチの場所を指定します。（64 文字以内） 「running-config」オプションを選択すると、リストアと同時に実行中のコンフィグレーションファイルがリストア＆上書きされます。「startup-config」オプションを選択すると、ブートコンフィグレーションファイルがリストア＆上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

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

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

TFTP サーバを使用してローカル PC から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。

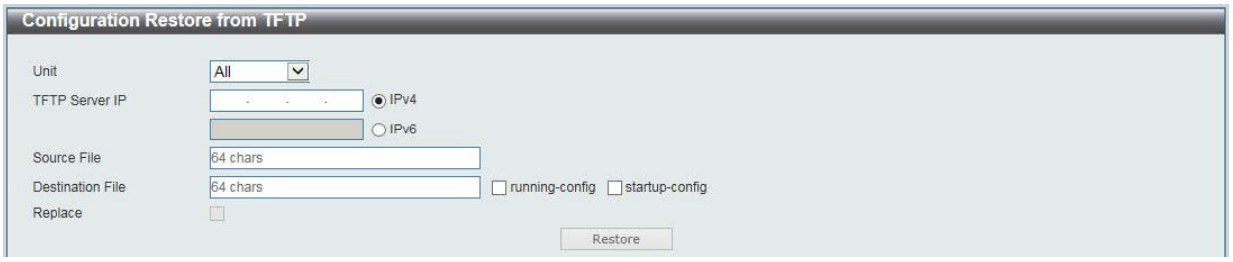


図 16-7　Configuration Restore from TFTP 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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）
Destination File	コンフィグレーションファイルが保存されるスイッチの場所を指定します。（64 文字以内） 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルがリストア＆上書きされます。「startup-config」オプションを選択するとブートコンフィグレーションファイルがリストア＆上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「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。

注意　初期状態に何か設定が追加されている状態で、別の設定を runnning-config にコピーすることはしないでください。予期せぬ動作の原因となります。必ず、running-config をクリアしてから、新しい設定を runnning-config にコピーするようにしてください。

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

HTTP サーバを使用してローカル 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。

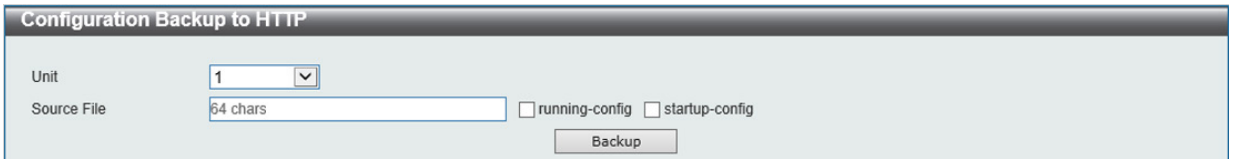


図 16-8　Configuration Backup to HTTP 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	スイッチ上でコンフィグレーションが保存されているパスとファイル名を入力します。（64 文字以内） 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup-config」オプションを選択するとブートアップコンフィグレーションファイルがバックアップされます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

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。

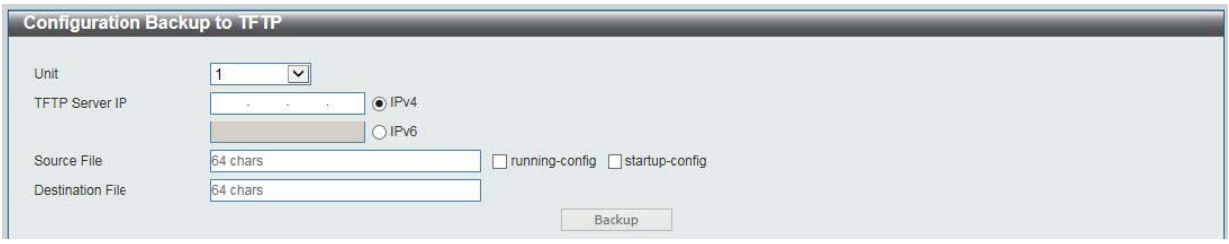


図 16-9　Configuration Backup to TFTP 画面

以下の項目が表示されます。

項目	説明
Unit	本設定を適用するユニットを選択します。
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	スイッチ上のコンフィグレーションファイルが保存されているパスとファイル名を入力します。（64 文字以内） 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup-config」オプションを選択するとブートコンフィグレーションファイルがバックアップされます。
Destination File	コンフィグレーションファイルが保存される TFTP サーバの場所を指定します。（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）

注意　copy コマンドや Flash への書き込み中は TELNET や CLI などの操作ができなくなります。書き込み終了までしばらくお待ちください。

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。

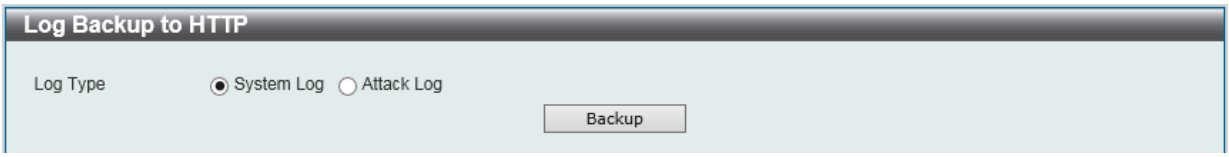


図 16-10　Log Backup to HTTP 画面

以下の項目が表示されます。

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 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 16-11　Log Backup to TFTP 画面

以下の項目が表示されます。

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。
Destination File	ログファイルが保存される TFTP サーバの場所を指定します。（64 文字以内）
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。

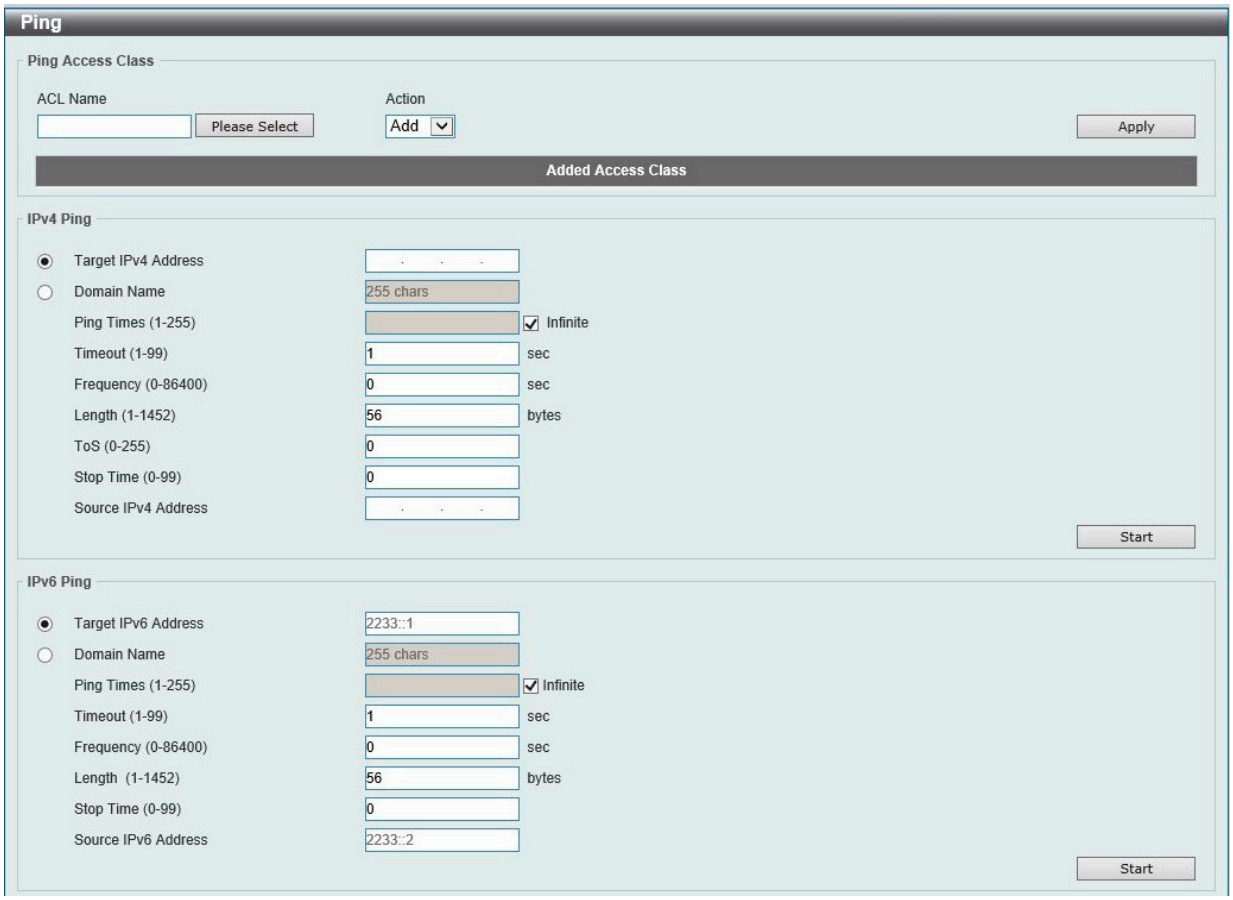


図 16-12　Ping 画面

以下の項目が表示されます。

項目	説明
Ping Access Class	
ACL Name	ACL 名を指定します。（32 文字以内）「Please Select」で既存の ACL を選択することができます。
Action	実行する動作を「Add」「Clear」から指定します。
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	Ping 長を指定します。送信データバイト数になります。ICMP ヘッダデータの 8 バイトと結合すると 64 の ICMP データバイトになります。VLAN（IEEE 802.1Q）タグ長は含まれません。 • 設定可能範囲：1-1420（Bytes） • 初期値：56（Bytes）
ToS	ToS 値を指定します。ICMP データグラムの QoS を指定します。 • 設定可能範囲：0-255

項目	説明
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」に指定すると自動的には止まらず、「Stop」をクリックするまで続きます。 • 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
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99（秒）までの間で指定できます。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。
Frequency	Ping 頻度を指定します。 • 設定可能範囲：0-86400
Length	Ping 長を指定します。送信データバイト数になります。ICMP ヘッダデータの 8 バイトと結合すると、64 の ICMP データバイトになります。VLAN（IEEE 802.1Q）タグ長は含まれません。 • 設定可能範囲：1-1420（Bytes） • 初期値：56（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」に指定すると自動的には止まらず、「Stop」をクリックするまで続きます。 • 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、各セクションでの Ping テストを実行します。

既存 ACL の選択画面

「Please Select」をクリックすると、以下の画面が表示されます。

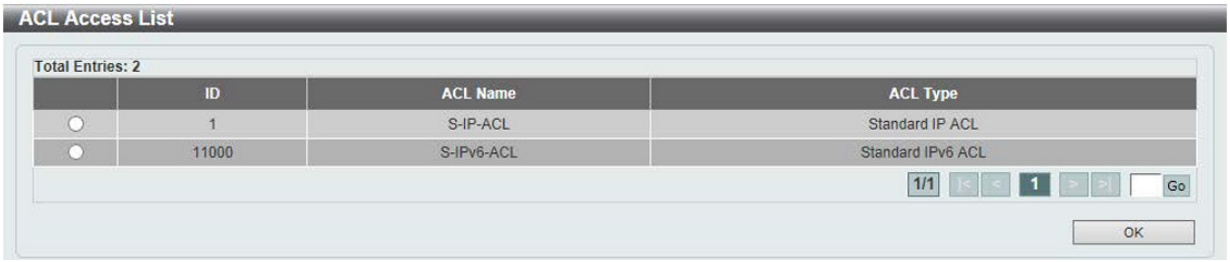


図 16-13　Ping (Please Select) 画面

設定するエントリを選択し「OK」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。

Ping 実行画面

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

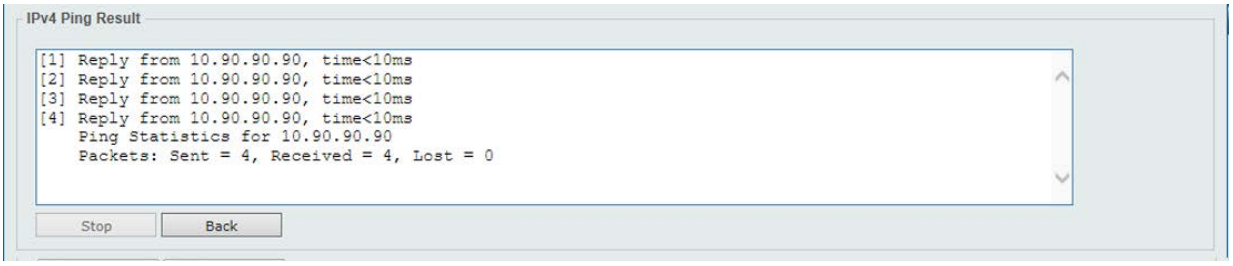


図 16-14　IPv4 Ping Result 画面

「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。

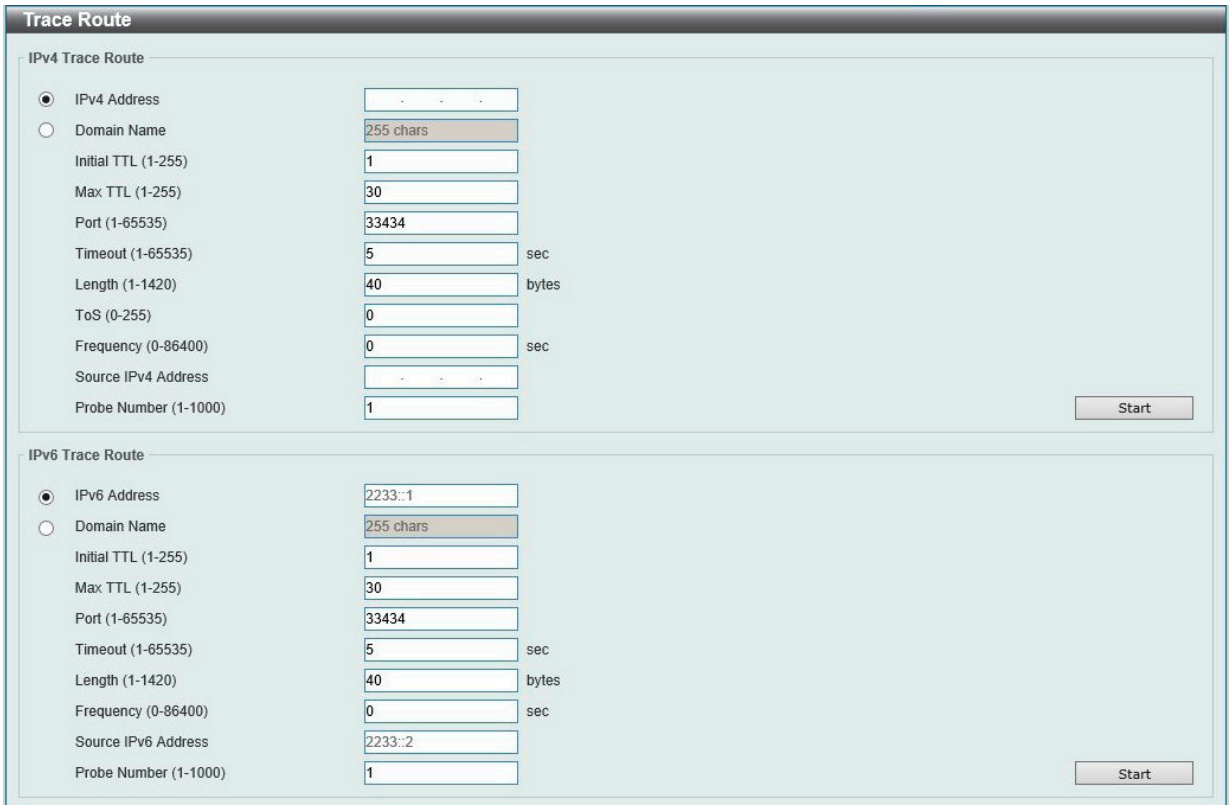


図 16-15　Trace Route 画面

以下の項目が表示されます。

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	最初の Time-To-Live（TTL）値を入力します。 • 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）
ToS	ToS 値を指定します。送信データグラムの IP ヘッダにセットされる値です。 • 設定可能範囲：0-255
Frequency	頻度を指定します。 • 設定可能範囲：0-86400
Source IPv4 Address	送信元 IPv4 アドレスを入力します。スイッチに設定された IPv4 アドレスのいずれかを指定します。
Probe Number	プローブ回数を指定します。 • 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	最初の Time-To-Live（TTL）値を入力します。 • 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	頻度を指定します。 • 設定可能範囲：0-86400
Source IPv6 Address	送信元 IPv6 アドレスを入力します。スイッチに設定された IPv6 アドレスのいずれかを指定します。
Probe Number	プローブ回数を指定します。 • 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。

以下の結果画面が表示されます。

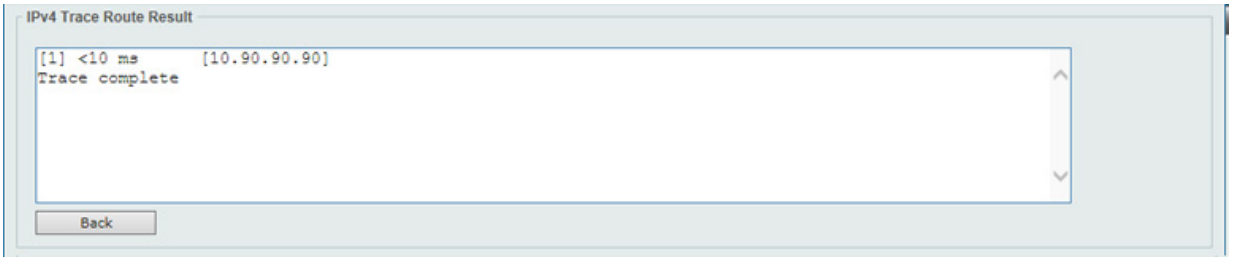


図 16-16　Trace Route Result（IPv4）画面

「Back」ボタンをクリックして、前の画面に戻ります。

Reset（リセット）

スイッチの設定内容を工場出荷時状態に戻します。

Tools > Reset をクリックし、次の設定画面を表示します。

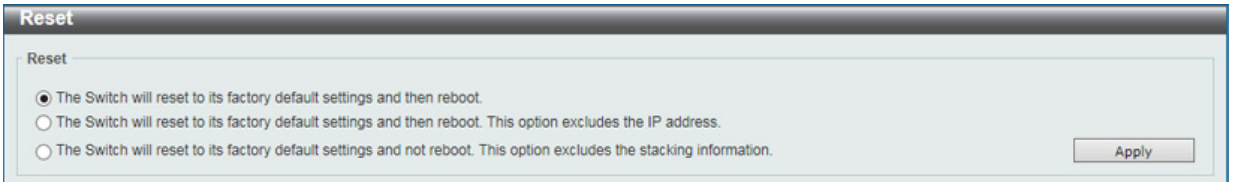


図 16-17　Reset System 画面

項目	説明
The Switch will reset to its factory default settings and then reboot.	スイッチを工場出荷時設定にリセットして、再起動を実行します。 （IP アドレス、スタック情報を含む）
The Switch will reset to its factory default settings and then reboot. This option excludes the IP address.	スイッチを工場出荷時設定にリセットして、再起動を実行します。 （IP アドレスは除く）
The Switch will reset to its factory default settings and not reboot. This option excludes the 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、リセット処理を開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

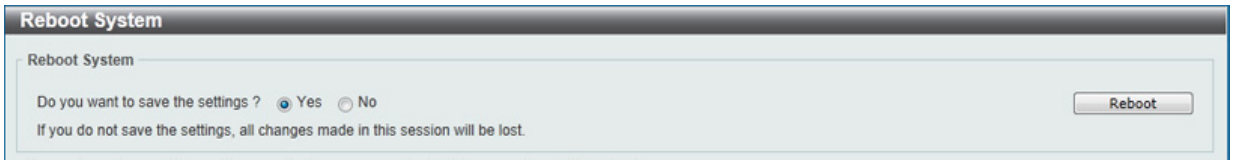


図 16-18　Reboot System 画面

以下の項目が表示されます。

項目	説明
Yes	スイッチは再起動する前に現在の設定を保存します。
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われます。

「Reboot」をクリックして再起動を開始します。

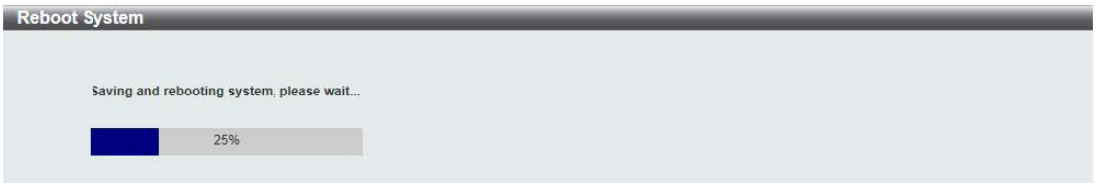


図 16-19　System Rebooting 画面

付録 A パスワードリカバリ手順

本スイッチシリーズでパスワードをリセットする手順について説明します。
ネットワークにアクセスするすべてのユーザに対し、認証を行うことが重要です。権限を持つユーザを許可す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利用したローカルログインです。パスワードの紛失 / 損失時には、ネットワーク管理者がパスワードをリセットする必要があります。このような場合に、このパスワードリカバリ機能を使用してパスワードを回復することができます。

次の手順を実行し、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リカバリします。
これらの手順を完了してパスワードをリセットしてください。

1. セキュリティ上の理由により、パスワードリカバリ機能は物理的にデバイスにアクセスする必要があります。物理的なアクセスが必要なため、デバイスのコンソールポートに直接接続している場合にのみ、本機能を利用することができます。ユーザは、端末エミュレーションソフトが導入されている端末または PC をスイッチのコンソールポートに接続する必要があります。
2. スイッチの電源をオンにします。「Password Recovery Mode」に移行するためには、「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」に移行すると、スイッチのすべてのポートが無効になります。

```
Boot Procedure                                          V1.00.006
--------------------------------------------------------------------------------

Power On Self Test ..................................... 100 %

MAC Address    : F0-7D-68-36-30-00
H/W Version    : A1

Please Wait, Loading 1.00.008 Runtime Image ............... 100 %
UART init ................................................. 100 %
```

```
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 password	ローカル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処理を開始します。
reload	保存とスイッチの再起動を実行します。
reload clear running-config	起動中の設定を工場出荷値に戻し、スイッチを再起動します。
show running-config	起動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表示される可能性のあるログイベントとそれらの意味を以下に示します。

Critical（重大）、Warning（警告）、Informational（報告）、Notice（通知）

ログの内容	緊急度	イベントの説明
802.1X		
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 • username：認証されているユーザ名 • interface-id：インタフェース名 • mac-addres：認証されたデバイスの MAC アドレス	Critical	802.1X 認証に失敗しました。
802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) **パラメータ説明：** • username：認証されたユーザ名 • interface-id：インタフェース名 • mac-addres：認証されたデバイスの MAC アドレス	Informational	802.1X 認証に成功しました。
AAA		
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。
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 の種類 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコル経由の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：認証されるユーザ名	Informational	ログインに成功しました。
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 の種類 例：Console、Telnet、SSH、Web、Web(SSL) • client-ip：IP プロトコル経由の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：認証されるユーザ名	Warning	ログインに失敗しました。
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 の種類 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコル経由の有効なクライアントの IP アドレス • 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：認証されるユーザ名	Warning	サーバタイムアウト、または不適切な設定によるログイン失敗。

ログの内容	緊急度	イベントの説明
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 の種類 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコル経由の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：認証されるユーザ名	Informational	特権の有効化に成功しました。
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 の種類 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコル経由の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：認証されるユーザ名	Warning	特権の有効化に失敗しました。
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 の種類 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコル経由の有効なクライアントの IP アドレス • 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：認証されるユーザ名	Warning	リモートサーバが有効なパスワード認証リクエストに応答しません。
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 サーバから認証された VLAN ID 割り当て • interface–id：認証されたクライアントのポート番号 • username：認証されるユーザ名	Informational	RADIUS が有効な VLAN ID 属性を割り当てました。
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：イングレスまたはイーグレス） • threshold: サーバから認証された帯域幅のしきい値割り当て • interface–id：認証されたクライアントのポート番号 • username：認証されるユーザ名	Informational	RADIUS が有効な帯域幅属性を割り当てました。
RADIUS server <server-ip> assigned 802.1p default priortiy: <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 サーバから認証された優先度割り当て • interface–id：認証されたクライアントのポート番号 • username：認証されるユーザ名	Informational	RADIUS が有効な優先度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
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：認証されるユーザ名 • interface–id：認証された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 スクリプトを割り当てましたが、不十分なリソースのためシステムへの適用に失敗しました。
ARP		
Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>). **パラメータ説明：** • ipaddr：IP アドレス • macaddr：MAC アドレス • unitID：ユニット番号 • portNum：ポート番号 • ipif_name：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 Save		
[Unit <unitID>]Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) **パラメータ説明：** • unitID：ボックス ID • username：現在のログインユーザ名 • ipaddr：クライアント IP アドレス	Informational	DDP の設定情報が自動で保存されました。
BPDU Potection		
<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 プロテクションモード - drop - block - shutdown	Informational	BPDU アタックが発生しました。
<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		
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 • 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。 CFM ハードウェアモードでは、リモート MEP 情報（mepid/macaddr）は不明です。	Critical	クロス接続が検出されました。

ログの内容	緊急度	イベントの説明
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 • 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。 CFM ハードウェアモードでは、リモート MEP 情報（mepid/macaddr）は不明です。	Warning	エラー CFM CCM パケットが検出されました。
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 • 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	Warning	MEP の CCM パケットを受信できません。
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 • 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	Warning	リモート MEP の MAC レポートがエラー状態です。
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 • 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	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		
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 • mepdirection：MEP の方向 - inward - outward • mepid：MEP の MEPID。「0」は不明な MEIPD を意味します。	Notice	AIS コンディションの検出
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 • mepdirection：MEP の方向 - inward - outward • mepid：MEP の MEPID。「0」は不明な MEIPD を意味します。	Notice	AIS コンディションの解消
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 • mepdirection：MEP の方向 - inward - outward • mepid：MEP の MEPID。「0」は不明な MEIPD を意味します。	Notice	LCK コンディションの検出
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 • mepdirection：MEP の方向 - inward - outward • mepid：MEP の MEPID。「0」は不明な MEIPD を意味します。	Notice	LCK コンディションの解消
Configuration/Firmware		
[Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバ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
[Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバ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。
[Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバ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。
[Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバ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。
[Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバ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。
[Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバ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
[Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバ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。
[Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバ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。
[Unit <unitID>,]Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • 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 • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Warning	未知のタイプのファイルのダウンロードに失敗しました。
DAD		
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：ポートインタフェース ID	Warning	DAD の間に DUT が「Neighbor Solicitation」(NS) メッセージを重複アドレスとともに受信しました。
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：ポートインタフェース ID	Warning	DAD の間に DUT が「Neighbor Advertisement」(NA) メッセージを重複アドレスとともに受信しました。

ログの内容	緊急度	イベントの説明
DDM		
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。以下のいずれかとなります。 - temperature - supply voltage - bias current - TX power - RX power - high-low：high/low	Warning	SFP パラメータのいずれかが警告しきい値を超えました。
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。以下のいずれかとなります。 - temperature - supply voltage - bias current - TX power - RX power - high-low：high/low	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。
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。以下のいずれかとなります。 - temperature - supply voltage - bias current - TX power - RX power - high-low：high/low	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。
DHCPv6 Client		
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。
DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name>. **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 クライアントが DHCPv6 サーバから ipv6 アドレスを取得しました。
The IPv6 address < ipv6address > on interface <ipif-name> starts renewing. **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得した IPv6 アドレスが更新を開始します。
The IPv6 address < ipv6address > on interface <ipif-name> renews success. **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスの更新に成功しました。

ログの内容	緊急度	イベントの説明
The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding. **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスのリバインドを開始します。
Log Message: The IPv6 address < ipv6address > on interface <ipif-name> rebinds success. **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスがリバインドに成功しました。
The IPv6 address < ipv6address > on interface <ipif-name> was deleted. **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバからの IPv6 アドレスが削除されました。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing. **パラメータ説明：** • ipv6networkaddr : デリゲイションルータから取得した IPv6 プレフィックス • intf-name : DHCPv6 クライアント PD インタフェース名	Informational	デリゲイションルータから取得した IPv6 プレフィックスは更新を開始します。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success. **パラメータ説明：** • ipv6networkaddr : デリゲイションルータから取得した IPv6 プレフィックス • intf-name : DHCPv6 クライアント PD インタフェース名	Informational	デリゲイションルータから取得した IPv6 プレフィックスは更新に成功しました。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding. **パラメータ説明：** • ipv6networkaddr : デリゲイションルータから取得した IPv6 プレフィックス • intf-name : DHCPv6 クライアント PD インタフェース名	Informational	デリゲイションルータから取得した IPv6 プレフィックスはリバインディングを開始します。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success. **パラメータ説明：** • ipv6networkaddr : デリゲイションルータから取得した IPv6 プレフィックス • intf-name : DHCPv6 クライアント PD インタフェース名	Informational	デリゲイションルータから取得した IPv6 プレフィックスはリバインドに成功しました。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted. **パラメータ説明：** • ipv6networkaddr : デリゲイションルータから取得した IPv6 プレフィックス • intf-name : DHCPv6 クライアント PD インタフェース名	Informational	デリゲイションルータからの IPv6 プレフィックスは削除されました。
DHCPv6 Server		
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。
The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096.	Informational	割り当てられた IPv6 アドレス数が 4096 に達しました。
Dynamic ARP Inspection		
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 パケットの種類。ARP パケットがリクエストか応答かを示します。 • ip-address：IP アドレス • mac-address：MAC アドレス • vlan-id：VLAN ID • interface-id：インタフェース ID	Warning	DAI が無効な ARP パケットを検出しました。

ログの内容	緊急度	イベントの説明
ERPS		
Manual Switch is issued on node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	Manual Switch が実行されました。
Signal fail detected on node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：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。
Signal fail cleared on node(MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	シグナル失敗がクリアされました。
Force Switch is issued on node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	Force Switch が実行されました。
Clear command is issued on node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	Clear コマンドが実行されました。
RPL owner conflicted on the node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	RPL オーナーが競合しています。
Ethernet OAM		
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。
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。
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	リモートで危機的なイベントが発生しました。
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：危機的なリンクイベントにより発生した状況について表示します。（例；OAM disable、Port shutdown、Port link down、Packet overload など）	Warning	ローカルで危機的なイベントが発生しました。
Error symbol period event received (Port < interface-id >) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでエラーシンボル期間イベントが発生しました。
Error frame event received(Port < interface-id >) **パラメータ説明：** • interface-id：インタフェース ID	Warning	エラーフレームイベントが発生しました。

ログの内容	緊急度	イベントの説明
Error 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。
Error 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。
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	リモートでループバックが開始されました。
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	リモートでループバックが停止しました。
Interface		
Port <portNum> link up, <link state> **パラメータ説明：** • portNum：ポート番号。整数値で機器の論理ポート番号 • link state：リンク状態（例：100Mbps FULL duplex）	Informational	ポートがリンクアップしました。
Port <portNum> link down. **パラメータ説明：** • portNum：ポート番号。整数値で機器の論理ポート番号	Informational	ポートがリンクダウンしました。
IP Directed Broadcast		
IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] **パラメータ説明：** • IP：ブロードキャスト IP 宛先アドレス。	Informational	あるサブネットにおいて IP ダイレクトブロードキャストレートが毎秒 50 パケットを超えました。
IP Directed Broadcast rate is high.	Informational	IP ダイレクトブロードキャストレートが毎秒 100 パケットを超えました。
IP Source Guard（IPSG）		
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：** • ip-address：IP アドレス • mac-address：MAC アドレス • vlan-id：VLAN ID • interface-id：インタフェース ID	Warning	DHCP スヌーピングエントリを ISPG テーブルにセットするにあたり、ハードウェアルールのリソースがありません。
LACP		
Link Aggregation Group <group_id> link up. **パラメータ説明：** • group-id：リンクアップ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。
Link Aggregation Group <group_id> link down. **パラメータ説明：** • group-id：リンクアップ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。
<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するポートのインタフェース名 • group-id：リンクアップ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します。

ログの内容	緊急度	イベントの説明
<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にアタッチするポートのインタフェース名 • group-id：リンクアップ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デタッチします。
LBD（ループバック検知）		
IfInfo LBD loop occurred. **パラメータ説明：** • IfInfo：インタフェース情報	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。
IfInfo LBD loop recovered. **パラメータ説明：** • IfInfo：インタフェース情報	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。
IfInfo VID <vlanID> LBD loop occurred. **パラメータ説明：** • IfInfo：インタフェース情報 • vlanID：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。
IfInfo VID <vlanID> LBD loop recovered. **パラメータ説明：** • IfInfo：インタフェース情報 • vlanID：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。
Loop VLAN number overflow.	Critical	ループバックが発生した VLAN の数が指定の数に達しました。
LLDP-MED		
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。

ログの内容	緊急度	イベントの説明
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。
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	Informational	LLDP-MED TLV の非互換性が検出されました。

ログの内容	緊急度	イベントの説明
Login/Logout		
[Unit <unitID>,]Successful login through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のユーザ名	Informational	コンソール経由のログインに成功しました。
[Unit <unitID>,] Login failed through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のユーザ名	Warning	コンソール経由のログインに失敗しました。
[Unit <unitID>,] Console session timed out (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のユーザ名	Informational	コンソールのセッションはタイムアウトしました。
[Unit <unitID>,] Logout through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のユーザ名	Informational	コンソール経由でログアウトしました。
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 • 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。
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。
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 • ipaddr：クライアントの IP アドレス	Informational	Telnet のセッションはタイムアウトしました。
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 • 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。
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 • 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。
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 • 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。
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 • ipaddr：クライアントの IP アドレス	Informational	SSH のセッションは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
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 • 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（MAC 認証）		
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：ホストが存在する VLAN ID	Informational	ホストは MAC 認証をパスしました。
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：ホストが存在する VLAN ID	Informational	ホストはエージアウトしました。
MAC-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：ホストが認証されたインタフェース • vlan-id：ホストが存在する VLAN ID	Critical	ホストは認証に失敗しました。
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ユーザの最大制限数に達しました。
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指定時間の間に最大ユーザ制限数を下回りました。
<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最大ユーザ制限数に達しました。
<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	インタフェースで認証されたユーザ数が指定時間の間に最大ユーザ制限数を下回りました。
MSTP Debug（MSTP デバッグ）		
Topology changed [([Instance:<InstanceID>] ,port:< portNum> ,MAC: <macaddr>)] **パラメータ説明：** • Instance-id：インスタンス ID • portNum：ポート番号 • macaddr：MAC アドレス	Notice	トポロジに変更がありました。
[CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>) **パラメータ説明：** • Instance-id：インスタンス ID • macaddr：MAC アドレス • value：優先値	Informational	新しいルートブリッジが選出されました。
Spanning Tree Protocol is enabled	Informational	スパニングツリープロトコル有効化
Spanning Tree Protocol is disabled	Informational	スパニングツリープロトコル無効化

ログの内容	緊急度	イベントの説明
New root port selected [([Instance:<InstanceID>], <portNum>)] **パラメータ説明：** • Instance-id：インスタンス ID • portNum：ポート番号	Notice	新しいルートポートが選出されました。
Spanning Tree port status change [([Instance:<InstanceID>], <portNum>)] <old_status> -> <new_status> **パラメータ説明：** • Instance-id：インスタンス ID • portNum：ポート番号 • old_status：旧ステータス • new_status：新ステータス	Notice	スパニングツリーポートのステートが変更されました。
Spanning Tree port role change. [([Instance:<InstanceID>], <[portNum>)] <old_role> -> <new_role> **パラメータ説明：** • Instance-id：インスタンス ID • portNum：ポート番号 • old_status：旧ロール • new_status：新ロール	Informational	スパニングツリーポートのロールが変更されました。
Spanning Tree instance created (Instance :< Instance-id >) **パラメータ説明：** • Instance-id：インスタンス ID	Informational	スパニングツリーインスタンスが作成されました。
Spanning Tree instance deleted (Instance :< Instance-id >) **パラメータ説明：** • Instance-id：インスタンス ID	Informational	スパニングツリーインスタンスが削除されました。
Spanning Tree version change (new version :< new_version>) **パラメータ説明：** • new_version：新しい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。
Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision_level>). **パラメータ説明：** • name：指定された MST リージョンの名前 • revision_level：リビジョンレベル	Informational	スパニングツリー MST 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。
Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> delete vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • Instance-id：インスタンス ID • startvlanid-endvlanid：削除する VLAN 範囲	Informational	スパニングツリー MST インスタンスから VLAN が削除されました。
Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • Instance-id：インスタンス ID • startvlanid-endvlanid：追加する VLAN 範囲	Informational	スパニングツリー MST コンフィグ ID VLAN マッピングテーブルが追加されました。
Spanning Tree port role change (Instance : <InstanceID>, <portNum>) to alternate port due to the guard root. **パラメータ説明：** • Instance-id：インスタンス ID • portNum：ポート番号	Informational	ガードルートによりスパニングツリーポートロールが交代します。

ログの内容	緊急度	イベントの説明
Spanning Tree loop guard blocking(Instance : <InstanceID>, <portNum>) **パラメータ説明：** • Instance-id：インスタンス ID • portNum：ポート番号	Informational	スパニングツリーループガードがブロックしています。
Peripheral（周辺機器）		
Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> **パラメータ説明：** • unitID：ユニット ID • thermal-sensor-descr：センサ ID • degree：温度	Warning	温度センサがアラーム状態に入りました。
Unit <unit-id> <thermal-sensor-descr> temperature back to normal **パラメータ説明：** • unitID：ユニット ID • thermal-sensor-descr：センサ ID • degree：温度	Informational	温度が通常に戻りました。
Unit <unit-id> <power-descr> failed **パラメータ説明：** • unitID：ユニット ID • power-descr：電源 ID	Critical	電源故障
Unit <unit-id> <power-descr> back to normal **パラメータ説明：** • unitID：ユニット ID • power-descr：電源 ID	Critical	電源回復
Unit <unit-id> External Alarm Channel <channelID> :<alarmMsg> **パラメータ説明：** • unitID：ユニット ID • channelID：チャネル ID • alarmMsg：アラームメッセージ	Critical	外部アラームステートが変更されました。
Port		
Port <port> link up, <nway> **パラメータ説明：** • port：論理ポート番号 • nway：リンクスピードと二重通信方式	Informational	ポートリンクアップしました。
Port <port> link down **パラメータ説明：** • port：論理ポート番号	Informational	ポートリンクダウンしました。
Port Security		
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	ポート上のアドレスが超過しました。
Limit on system entry number has been exceeded.	Warning	システム上のアドレスが超過しました。
Reboot Schedule		
Reboot scheduled in 5 minutes	Warning	5 分以内に再起動します。
Reboot scheduled in 1 minute	Critical	1 分以内に再起動します。

ログの内容	緊急度	イベントの説明
Safeguard		
Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. **パラメータ説明：** • unit-id：ユニット ID	Warning	CPU 使用率がしきい値を超え、スイッチは「exhausted」モードに移行しました。
Unit <unit-id>, Safeguard Engine enters NORMAL mode **パラメータ説明：** • unit-id：ユニット ID	Informational	CPU 使用率がしきい値を下回り、スイッチはノーマルモードに移行しました。
SNMP		
SNMP request received from <ipaddr> with invalid community string. **パラメータ説明：** • ipaddr：IP アドレス	Informational	SNMP リクエストは無効なコミュニティストリングを受信しました。
SSH		
SSH server is enabled	Informational	SSH サーバは有効です。
SSH server is disabled	Informational	SSH サーバは無効です。
SSL		
Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：SSL サーバへのログインユーザ名 • ipaddr：SSL クライアントの IP アドレス	Informational	Web（SSL）経由でログインに成功しました。
Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：SSL サーバへのログインユーザ名 • ipaddr：SSL クライアントの IP アドレス	warning	Web（SSL）経由でログインに失敗しました。
Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：SSL サーバへのログインユーザ名 • ipaddr：SSL クライアントの IP アドレス	warning	Web（SSL）セッションがタイムアウトしました。
Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：SSL サーバへのログインユーザ名 • ipaddr：SSL クライアントの IP アドレス	warning	Web（SSL）セッションからログアウトしました。
Stacking		
Unit: <unitID>, MAC: <macaddr> Hot insertion. **パラメータ説明：** • unitID：ユニット ID • macaddr：MAC アドレス ID	Informational	デバイスが挿入されました。
Unit: <unitID>, MAC: <macaddr> Hot removal. **パラメータ説明：** • unitID：ユニット ID • macaddr：MAC アドレス ID	Informational	デバイスが削除されました。
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。
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。

ログの内容	緊急度	イベントの説明
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：該当ボックスの MAC アドレス	Critical	ボックス ID が重複しています。
Stacking port <portID> link up. **パラメータ説明：** • portID：スタックポート番号	Critical	スタックポートがリンクアップしました。
Stacking port <portID> link down. **パラメータ説明：** • portID：スタックポート番号	Critical	スタックポートがリンクダウンしました。
SIO interface Unit <unitID> <SIOID > link up. **パラメータ説明：** • unitID：ボックス ID • SIOID：SIO ID	Critical	SIO インタフェースがリンクアップしました。
SIO interface Unit <unitID> <SIOID > link down. **パラメータ説明：** • unitID：ボックス ID • SIOID：SIO ID	Critical	SIO インタフェースがリンクダウンしました。
Telnet		
Successful login through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス • username：Telnet サーバへのログインユーザ名	Informational	Telnet 経由のログインに成功しました。
Login failed through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス • username：Telnet サーバへのログインユーザ名	Warning	Telnet 経由のログインに失敗しました。
Logout through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス • username：Telnet サーバへのログインユーザ名	Informational	Telnet からログアウトしました。
Telnet session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス • username：Telnet サーバへのログインユーザ名	Informational	Telnet セッションがタイムアウトしました。
WAC		
WAC unauthenticated user (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>) **パラメータ説明：** • string：ユーザ名 • ipaddr：IP アドレス • ipv6address：IPv6 アドレス • macaddr：MAC アドレス • unitID：ユニット ID • portNum：ポート番号	Warning	クライアントホストが認証に失敗しました。
Web-Authentication enters stop learning state	Warning	デバイス全体において認証ユーザ数が最大値に達しました。

ログの内容	緊急度	イベントの説明
Web-Authentication recovered from stop learning state	Warning	所定時間内にデバイス全体において認証ユーザ数が最大値を下回りました。
WAC authenticated user (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>) **パラメータ説明：** • string：ユーザ名 • ipaddr：IP アドレス • ipv6address：IPv6 アドレス • macaddr：MAC アドレス • unitID：ユニット ID • portNum：ポート番号	Informational	クライアントホストが認証に成功しました。
Web		
Successful login through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP サーバへのログインユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web 経由でのログインに成功しました。
Login failed through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP サーバへのログインユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Warning	Web 経由でのログインに失敗しました。
Web session timed out (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP サーバへのログインユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web セッションがタイムアウトしました。
Logout through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP サーバへのログインユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web 経由でのログアウトしました。

付録 C トラップログエントリ

本スイッチのトラップログエントリとそれらの意味を以下に示します。

カテゴリ	トラップ名	説明	OID
802.1X	dDot1xExtLoggedSuccess	ホストがログインに成功したときに送信されます。 （802.1X 認証にパス） 関連オブジェクト : (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.17 1.14.30.0.1
	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 : (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.17 1.14.30.0.2
802.3ah OAM	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： (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogWindowHi (6) dot3OamEventLogWindowLo (7) dot3OamEventLogThresholdHi (8) dot3OamEventLogThresholdLo (9) dot3OamEventLogValue (10) dot3OamEventLogRunningTotal (11) dot3OamEventLogEventTotal	1.3.6.1.2.1. 158.0.1
	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。 Binding objects: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogEventTotal	1.3.6.1.2.1. 158.0.2
Authentication Fail （認証失敗）	authenticationFailure	authenticationFailure トラップは、エージェントとして動作する SNMPv2 エンティティが、正しく認証されないプロトコルメッセージを受信したことを表します。すべての SNMPv2 実装はこのトラップを生成することができる必要がありますが、snmpEnableAuthenTraps オブジェクトでは、このトラップが生成されるかどうかを示します。	1.3.6.1.6.3.1. 1.5.5

カテゴリ	トラップ名	説明	OID
BPDU Protection	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 : (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.17 1.14.47.0.1
	dBpduProtectionAttackRecover	インタフェースで BPDU アタックが回復したときに送信されます。 関連オブジェクト : (1) ifIndex	1.3.6.1.4.1.17 1.14.47.0.2
CFM	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 : (1) dot1agCfmMepHighestPrDefect	1.3.111.2.802. 1.1.8.0.1
CFM Extension	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 : (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.171. 14.86.0.1
	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 : (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.171. 14.86.0.2
	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 : (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.171. 14.86.0.3
	dCfmLockCleared	ローカル MEP のロックステータスが解除された場合、生成されます。 関連オブジェクト : (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.171. 14.86.0.4
DDM	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。現在の値が「low warning」より大きく、「high warning」より小さい場合にのみリカバトラップを送信します。 関連オブジェクト : (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.14.72.0.1
	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 : (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.14.72.0.2

カテゴリ	トラップ名	説明	OID
DHCP サーバスクリーン防止	dDhcpFilterAttackDetected	DHCP サーバスクリーンが有効な場合、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 : (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.17 1.14.133.0.1
DoS 防止	dDosPreveAttackDetectedPacket	DoS アタックを検出したとき送信されます。 関連オブジェクト : (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.17 1.14.59.0.2
ERPS	dErpsFailuredetectedNotif	「dErpsNotificationEnabled」が 'true' でシグナル不具合が検出されると「dErpsFailureNotification」が送信されます。	1.3.6.1.4.1.171. 14.78.0.1
	dErpsFailureClearedNotif	「dErpsNotificationEnabled」が 'true' でシグナル不具合が解消されると「dErpsFailureClearedNotif」が送信されます。	1.3.6.1.4.1.171. 14.78.0.2
	dErpsRPLOwnerConflictNotif	「dErpsNotificationEnabled」が 'true' で RPL オーナコンフリクトが検出されると「dErpsOwnerConflictNotif」が送信されます。	1.3.6.1.4.1.171. 14.78.0.3
ErrDisable	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 : (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171. 14.45.0.1
	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 : (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171. 14.45.0.2
	esErrDisNotifyVlanDisabledAssert	VLAN 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 : (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID (3) esErrDisNotifyInfoLoopDetectedVID	1.3.6.1.4.1.171. 17.45.0.3
	esErrDisNotifyVlanDisabledClear	指定間隔の後、VLAN ループ再始動時に送信されます。 (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID (3) esErrDisNotifyInfoLoopDetectedVID	1.3.6.1.4.1.171. 17.45.0.4
Gratuitous ARP 機能	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 : (1) esIpExtGratuitousARPIpAddr (2) esIpExtGratuitousARPMacAddr (3) esIpExtGratuitousARPPortNumber (4) esIpExtIfCfgIfIndex	1.3.6.1.4.1.17 1.14.75.0.1
IP-MAC-Port Binding (IMPB)	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、アドレス違反通知が生成されます。 関連オブジェクト : (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.17 1.14.22.0.1

カテゴリ	トラップ名	説明	OID
LACP	linkUp	「linkUp」トラップは、コミュニケーションリンクの一つで「ifOperStatus」オブジェクトがダウン状態のままとなり、その後「notPresent」以外の別の状態に移行したことが、エージェントである SNMP エンティティによって検出されたことを意味します。この「別の状態」は「ifOperStatus」の値で確認することができます。 関連オブジェクト : (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
	linkDown	「linkUp」トラップは、コミュニケーションリンクの一つで「ifOperStatus」オブジェクトが「notPresent」以外の他の状態からダウン状態に移行しようとしていることが、エージェントである SNMP エンティティによって検出されたことを意味します。この「他の状態」は「ifOperStatus」の値で確認することができます。 関連オブジェクト : (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3
LBD	swPortLoopOccurred	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 : (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.17 1.14.46.0.1
	swPortLoopRestart	所定時間後、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 : (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.17 1.14.46.0.2
	swVlanLoopOccurred	LBD VLAN ベースモードにおいて、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 : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.17 1.14.46.0.3
	swVlanLoopRestart	所定時間後、LBD VLAN ベースモードにおいて、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 : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.17 1.14.46.0.4
LLDP-MED	lldpRemTablesChange	「lldpRemTablesChange」通知は「lldpStatsRemTableLastChangeTime」変更時に送信されます。 関連オブジェクト : (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802. 1.1.2.0.0.1
	lldpXMedTopologyChangeDetected	トポロジの変更を検出したローカルデバイスによって送信されます。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 / 移動したことを示します。 関連オブジェクト : (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808. 1.1.2.1.5.4795.0.1

カテゴリ	トラップ名	説明	OID
MAC-based アクセス コントロール	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 : (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.1
	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 : (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.2
	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 : (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.17 1.14.153.0.3
MAC Notification	dL2FdbMacNotification	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 : (1) dL2FdbMac ChangeNotifyInfo	1.3.6.1.4.1.17 1.14.3.0.1
	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 : (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.17 1.14.3.0.2
MSTP	newRoot	newRoot トラップは、送信エージェントがスパニングツリーの新しいルートになったことを示します。トラップは、ブリッジが新しいルートとして選出された後すぐに（Topology Change Timer の期限切れなどに応じて）、ブリッジによって送信されます。本トラップの実行はオプションです。	1.3.6.1.2.1.17 .0.1
	topologyChange	topologyChange トラップは、構成するいずれかのポートが 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。同じ変更に対して 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。本トラップの実行はオプションです。	1.3.6.1.2.1.17 .0.2

カテゴリ	トラップ名	説明	OID
Peripheral （周辺機器）	esEntityExtFanStatusChg	この通知は、ファンの失敗 / 回復を検知した時に Commander スイッチによって送信されます。 （「esEntityExtEnvFanStatus」が 'fault' または「esEntityExtEnvFanStatus」が 'ok'） 関連オブジェクト : (1) esEntityExtEnvFanUnitId (2) esEntityExtEnvFanIndex (3) esEntityExtEnvFanStatus	1.3.6.1.4.1.17 1.17.5.0.1
	esEntityExtThermalStatusChg	この通知は、温度警告の検出 / 回復時に Commander スイッチによって送信されます。 （「esEntityExtEnvTempStatus」が 'abnormal' または「esEntityExtEnvTempStatus」が 'ok'） 関連オブジェクト : Binding objects: (1) esEntityExtEnvTempUnitId (2) esEntityExtEnvTempIndex (3) esEntityExtEnvTempStatus	1.3.6.1.4.1.17 1.17.5.0.2
	esEntityExtPowerStatusChg	この通知は、電源モジュールの不具合検出 / 回復時、または取り外した時に Commander スイッチによって送信されます。 関連オブジェクト : (1) esEntityExtEnvPowerUnitId (2) esEntityExtEnvPowerIndex (3) esEntityExtEnvPowerStatus 電力状態の変更通知（電源モジュールの不具合、または不具合からの回復）	1.3.6.1.4.1.17 1.17.5.0.3
	pethMainPowerUsageOnNotification	トラップは、使用電力が PSE しきい値（「Usage Threshold」）を超えた場合に送信されます。通知間隔は最小で 500 ミリ秒です。 関連オブジェクト : (1) pethMainPseConsumptionPower	1.3.6.1.2.1.10 5.0.2
	pethMainPowerUsageOffNotification	トラップは、使用電力が PSE しきい値（「Usage Threshold」）を下回った場合に送信されます。通知間隔は最小で 500 ミリ秒です。 関連オブジェクト : (1) pethMainPseConsumptionPower	1.3.6.1.2.1.10 5.0.3
	esPoeIfPowerDeniedNotification	PSE ステータスが POWER_DENIED に移行したことを示します。通知間隔は最小で 500 ミリ秒です。 関連オブジェクト : (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.17 1.17.24.0.1
	esPoeIfPowerOverLoadNotification	PSE ステータスが ERROR_DELAY_OVER に移行したことを示します。通知間隔は最小で 500 ミリ秒です。 関連オブジェクト : (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.17 1.17.24.0.2
	esPoeIfPowerShortCircuitNotification	PSE ステータスが ERROR_DELAY_SHORT に移行したことを示します。通知間隔は最小で 500 ミリ秒です。 関連オブジェクト : (1) pethPsePortShortCounter	1.3.6.1.4.1.17 1.17.24.0.3

カテゴリ	トラップ名	説明	OID
Port Security（ポートセキュリティ）	dPortSecMacAddrViolation	ポートセキュリティトラップが有効な場合、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 アドレスによって生成されます。 関連オブジェクト： (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.17 1.14.8.0.1
Port（ポート）	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： (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1 1.5.4
	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： (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1 1.5.3
RMON	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、送信 SNMP トラップに設定されたイベントを生成します。 関連オブジェクト： (1)alarmIndex (2)alarmVariable (3)alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16 .0.1
	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、送信 SNMP トラップに設定されたイベントを生成します。 関連オブジェクト： (1)alarmIndex (2) alarmVariable (3)alarmSampleType (4)alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16 .0.2
Safeguard（セーフガード）	dSafeguardChgToExhausted	システムが操作モードがノーマルから exhausted に変更されたことを示します。 関連オブジェクト： (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0. 1
	dSafeguardChgToNormal	システムが操作モードが exhausted からノーマルに変更されたことを示します。 関連オブジェクト： (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0. 2

カテゴリ	トラップ名	説明	OID
SIM	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 : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.17.225.0.0.1 1
	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 : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.17.225.0.0.1 2
	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 : (1) esSingleIPMSMacAddr (2) ifIndex	1.3.6.1.4.1.17 1.17.225.0.0.1 3
	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 : (1) esSingleIPMSMacAddr (2) ifIndex	1.3.6.1.4.1.17 1.17.225.0.0.1 4
	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 : (1) esSingleIPMSMacAddr	1.3.6.1.4.1.17 1.17.225.0.0.1 5
	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 : (1) esSingleIPMSMacAddr	1.3.6.1.4.1.17 1.17.225.0.0.1 6
	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 : (1) esSingleIPMSMacAddr	1.3.6.1.4.1.17 1.17.225.0.0.1 7
	esSingleIpMSrisingAlarm	コマンダースイッチはメンバが上昇アラーム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 : (1) esSingleIpMSTrapMacAddr	1.3.6.1.4.1.17 1.17.225.0.0.1 8
	esSingleIpMSfallingAlarm	コマンダースイッチはメンバが下降アラーム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 : (1) esSingleIpMSTrapMacAddr	1.3.6.1.4.1.17 1.17.225.0.0.1 9
	esSingleIpMSmacNotification	コマンダースイッチはメンバが MAC アドレス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 : (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage	1.3.6.1.4.1.17 1.17.225.0.0.2 0
	esSingleIpMSPortTypeChange	コマンダースイッチはメンバがポートタイプ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 : (1) esSingleIpMSTrapMacAddr (2) ifIndex (3) esSingleIpMSTrapMessage	1.3.6.1.4.1.17 1.17.225.0.0.2 1

カテゴリ	トラップ名	説明	OID
SIM	esSingleIpMSPowerStatusChg	コマンダースイッチはメンバが電源ステータス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 : (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage	1.3.6.1.4.1.17 1.17.225.0.0.2 2
	esSingleIpMSPowerFailure	コマンダースイッチはメンバが電源不具合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 : (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage	1.3.6.1.4.1.17 1.17.225.0.0.2 3
	esSingleIpMSPowerRecover	コマンダースイッチはメンバが電源回復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 : (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage	1.3.6.1.4.1.17 1.17.225.0.0.1 4
Start （スタート）	coldStart	coldStart トラップは、エージェントとして動作する SNMPv2 エンティティが再起動し、それにより設定が変更された可能性があることを示します。	1.3.6.1.6.3.1. 1.5.1
	warmStart	warmStart トラップは、エージェントとして動作する SNMPv2 エンティティが再起動したことを示します。この再起動により設定は変更されません。	1.3.6.1.6.3.1. 1.5.2
Storm Control （ストーム コントロール）	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 : (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.14.25.0.1
	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 : (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.14.25.0.2
System File （システム ファイル）	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。	1.3.6.1.4.1.17 1.14.14.0.1
	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。	1.3.6.1.4.1.17 1.14.14.0.2
	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。	1.3.6.1.4.1.17 1.14.14.0.3
	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。	1.3.6.1.4.1.17 1.14.14.0.4
	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。	1.3.6.1.4.1.17 1.14.14.0.5
Upload/ Download	agentFirmwareUpgrade	SNMP 経由でのファームウェアアップグレードが終了した際、送信されます。 関連オブジェクト : (1) swMultiImageVersion	1.3.6.1.4.1.17 1.12.1.7.2.0.7
	agentCfgOperCompleteTrap	コンフィグレーションが保存、アップロード、ダウンロードされた場合、送信されます。 関連オブジェクト : (1) unitID (2) agentCfgOperate (3) agentLoginUserName	1.3.6.1.4.1.17 1.12.1.7.2.0.9

カテゴリ	トラップ名	説明	OID
VRRP	vrrpTrapNewMaster	送信エージェントが「Master」ステータスに移行した場合、送信されます。 関連オブジェクト : (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68 0.1
	vrrpTrapAuthFailure	ルータから受信したパケットの認証鍵または認証タイプが、本ルータの認証鍵または認証タイプと一致しない事を意味します。本トラップの適用はオプションです。 関連オブジェクト : (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.68 0.2
WAC （Web 認証）	esWebAuthLoggedSuccess	クライアントが Web 認証をパスして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 : (1) ifIndex (2) esnaSessionAuthVlan (3) esnaSessionClientMacAddress (4) esnaSessionClientAddrType (5) esnaSessionClientAddress (6) esnaSessionAuthUserName	1.3.6.1.4.1.17 1.17.154.0.1
	esWebAuthLoggedFail	クライアントが Web 認証に失敗して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 : (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.17 1.17.154.0.2

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。特権レベルが最小サポート値よりも小さい場合、または最大サポート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。	ユニット (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、または最大サポート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に使用します。	0-7	必須

ユーザは、RADIUS サーバの 802.1p デフォルトプライオリティ（例えば、優先度 7）を設定し、802.1X 認証や MAC ベース印象に成功した場合、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。

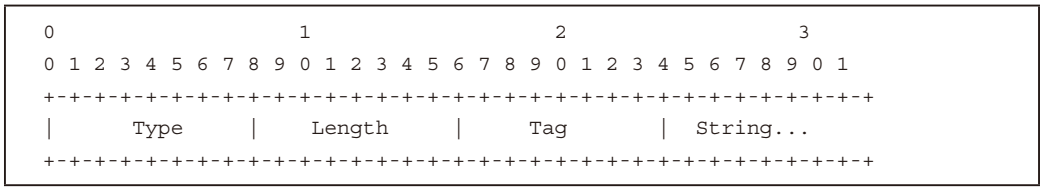
■ VLAN

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 割り当てを使うため、RFC3580 は RADIUS パケット内の以下のトンネル属性を定義しています。

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	A ストリング（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依存 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 名を検出できたことを確認します。

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、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。

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、ACP スクリプトは拒否されます。

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、RFC2865 リモート認証ダイヤルインユーザサービス（RADIUS)、RFC2866 RADIUS アカウンティング、RFC2868 トンネルプロトコルに対する RADIUS 属性、RFC2869 RADIUS 拡張で定義されています。
以下のリストは、D-LInk 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-3130

Traffic Segmentation（トラフィックセグメンテーション）

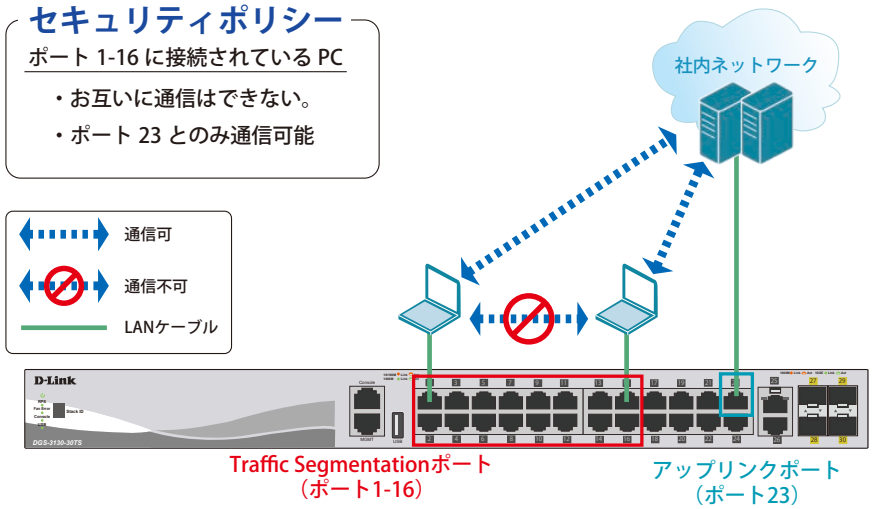


図 17-1　Traffic Segmentation（DGS-3130-30TS）

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）のセキュリティ設定をします。

```
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

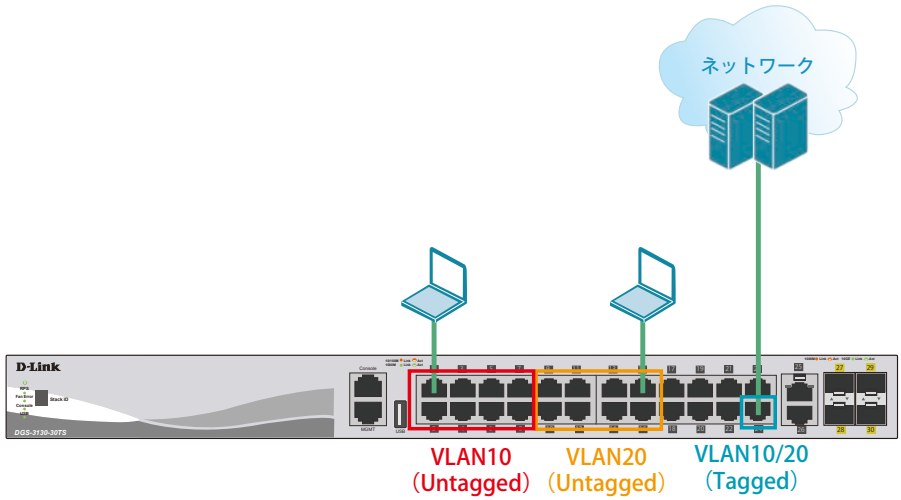


図 17-2　VLAN（DGS-3130-30TS）

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#configure terminal
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#configure terminal
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）

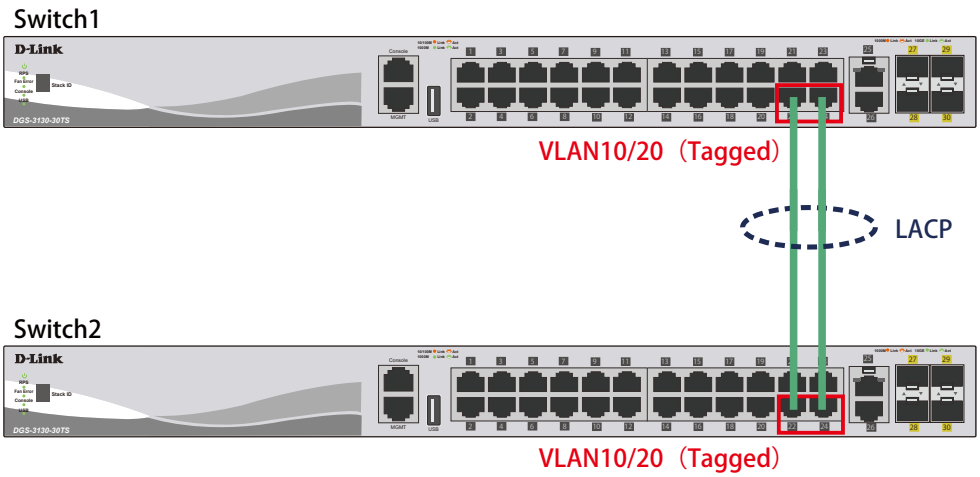


図 17-3　Link Aggregation（DGS-3130-30TS）

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#configure terminal
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. Link Aggregation のポートを設定します。

```
Switch(config)#interface port-channel 1
```

4. 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、各物理インターフェイス上では設定せず、Port-channel インターフェイス上で 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
```

5. 設定を保存します。

```
Switch#copy running-config startup-config
```

6. 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）

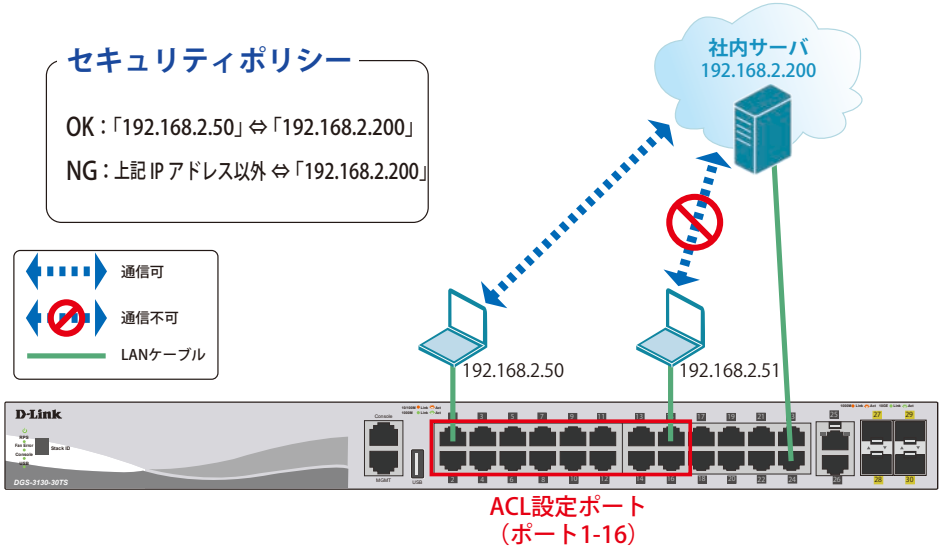


図 17-4　Access List（DGS-3130-30TS）

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（「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）

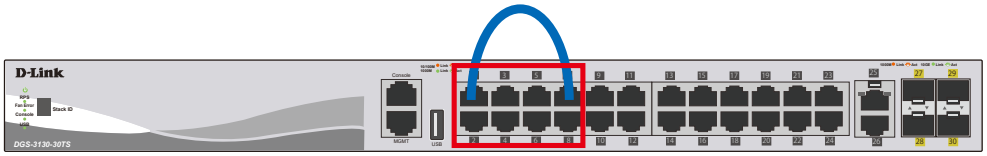


図 17-5　Loopback Detection（DGS-3130-30TS）

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#enable
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、インターフェイスモードにて「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)#spanning-tree state disable
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、設定するインターフェイスの「spanning-tree」の設定をまず「disable」にします。

注意 「spanning-tree」はデフォルトでグローバルでは「disable」に設定されていますが、各インターフェイス「enable」となっています。各インターフェイスにて「disable」設定が必要となります。

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、設定しているモード、対象の VLAN、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 有効 / 無効、確認間隔を表示します。）