D-Link DGS-3630 シリーズ

Gigabit Stackable Layer 3 Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

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

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

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

ご使用上の注意

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

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 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/product-assurance-provision

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

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

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 17

本マニュアルの対象者 19
表記規則について 19
製品名 / 品番一覧 19

第 1 章　本製品のご使用にあたって 20

DGS-3630 シリーズについて 20
ポート 21
前面パネル 21
　アラームポート（RJ-45） 23
　LED 表示 23
背面パネル 26
側面パネル 27

第 2 章　スイッチの設置 28

パッケージの内容 28
ネットワーク接続前の準備 28
ゴム足の取り付け (19 インチラックに設置しない場合) 29
19 インチラックへの取り付け 29
SFP/SFP+ ポートへのモジュールの取り付け 30
電源抜け防止クリップの装着 30
リダンダント電源システムの設置 33
　DPS-500A 33
　DPS-700 34
　DPS-800 35
電源の投入 35
　電源の異常 35

第 3 章　スイッチの接続 36

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

第 4 章　スイッチ管理の導入 38

管理オプション 38
端末をコンソールポートに接続する 38
　RJ-45 コンソールポートへの接続 38
Mini-USB コンソールポートの接続 39
　Mini-USB コンソールポートとコンピュータの接続 39
スイッチへの初回接続 41
アカウント作成 / パスワード設定 41
IP アドレスの割り当て 42
管理ポートへの接続 42
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 マネージャへのログイン 44
Web マネージャの画面構成 45
　Web マネージャのメイン画面について 45
Web マネージャのメニュー構成 46

第 6 章　System（スイッチの主な設定）　51

Device Information（デバイス情報）....52
System Information Settings（システム情報設定 ）....53
Peripheral Settings（環境設定）....53
Port Configuration（ポート設定）....54
Port Settings（スイッチのポート設定）....54
Port Status（ポートステータス）....55
Port GBIC....56
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）....57
Jumbo Frame（ジャンボフレームの有効化）....58
Interface Description（インタフェース概要）....58
Loopback Test（ループバックテスト）....59
PoE（PoE の管理）（DGS-3630-28PC/52PC）....60
PoE System（PoE システム設定）....60
PoE Status（PoE ステータス）....61
PoE Configuration（PoE ポート設定）....61
PD Alive（PD アライブ設定）....62
PoE Statistics（PoE 統計）....63
PoE Measurement（PoE 測定）....63
PoE LLDP Classification（PoE LLDP 分類表示）....64
System Log（システムログ構成）....65
System Log Settings（システムログ設定）....65
System Log Discriminator Settings（システムログディスクリミネーター設定）....67
System Log Server Settings（システムログサーバの設定）....67
System Log（Syslog ログ）....69
System Attack Log（システムアタックログ）....69
Time and SNTP（時刻設定）....70
Clock Settings（時間設定）....70
Time Zone Settings（タイムゾーン設定）....70
SNTP Settings（SNTP 設定）....72
Time Range（タイムレンジ設定）....73
PTP（PTP 設定）....74
PTP Global Settings（PTP グローバル設定）....74
PTP Port Global Settings（PTP ポートグローバル設定）....75
PTP Boundary Port Settings（PTP 境界ポート設定）....75
PTP P2P Transparent Port Settings（PTP P2P 透過ポート設定）....76
PTP Clock Information（PTP クロック情報の表示）....77
PTP Port Information (PTP ポート情報)....77
PTP Foreign Master Records Port Information（PTP 外部マスタレコードのポート情報）....77
USB Console Settings（USB コンソール設定）....78
SRM（Switch Resource Management 設定）....78
SRM Prefer Current Settings（SRM 最適化設定）....78
SRM Prefer Mode（SRM 設定モード）....79

第 7 章　Management（スイッチの管理）　80

Command Logging（コマンドログ設定）....81
User Accounts Settings（ユーザアカウント設定）....81
CLI Alias Settings（CLI エイリアス設定）....83
Password Encryption（パスワード暗号化）....83
Password Recovery（パスワードリカバリ）....84
Login Method（ログイン方法）....84
SNMP Settings（SNMP 設定）....85
SNMP Global Settings（SNMP グローバル設定）....86
SNMP Linkchange Traps Settings（SNMP リンクチェンジトラップ設定）....87
SNMP View Table Settings（SNMP ビューテーブル）....87
SNMP Community Table Settings（SNMP コミュニティテーブル設定）....88
SNMP Group Table Settings（SNMP グループテーブル）....89
SNMP Engine ID Local Settings（SNMP エンジン ID ローカル設定）....89
SNMP User Table Settings（SNMP ユーザテーブル設定）....90
SNMP Host Table Settings（SNMP ホストテーブル設定）....91
SNMP Context Mapping Table Settings（SNMP コンテキストマッピングテーブル設定）（EI/MI モードのみ）....92

RMON（RMON 設定）.....93
RMON Global Settings（RMON グローバル設定）.....93
RMON Statistics Settings（RMON 統計情報）.....93
RMON History Settings（RMON ヒストリ設定）.....94
RMON Alarm Settings（RMON アラーム設定）.....95
RMON Event Settings（RMON イベント設定）.....96
Telnet/Web（Telnet/Web 設定）.....97
Session Timeout（セッションタイムアウト）.....98
DHCP（DHCP 設定）.....99
Service DHCP（DHCP サービス）.....99
DHCP Class Settings（DHCP クラス設定）.....99
DHCP Server（DHCP サーバ）.....100
DHCPv6 Server（DHCPv6 サーバ設定）.....106
DHCP Relay（DHCP リレー）.....109
DHCPv6 Relay（DHCPv6 リレー）.....116
DHCP Auto Configuration（DHCP 自動コンフィグ設定）.....122
DHCP Auto Image Settings（DHCP 自動イメージ設定）.....122
DNS（ドメインネームシステム）.....123
DNS Global Settings（DNS グローバル設定）.....123
DNS Name Server Settings（DNS ネームサーバ設定）.....123
DNS Host Settings（DNS ホスト名設定）.....124
NTP（ネットワークタイムプロトコル）.....125
NTP Global Settings（NTP グローバル設定）.....125
NTP Server Settings（NTP サーバ設定）.....125
NTP Peer Settings（NTP ピア設定）.....126
NTP Access Group Settings（NTP アクセスグループ設定）.....127
NTP Key Settings（NTP 鍵設定）.....127
NTP Interface Settings（NTP インタフェース設定）.....128
NTP Associations（NTP アソシエーション）.....129
NTP Status（NTP ステータス）.....129
IP Source Interface（IP ソースインタフェース）.....130
File System（ファイルシステム設定）.....131
Stacking（スタッキング設定）.....132
Physical Stacking（物理スタッキング）.....135
Stacking Bandwidth（スタッキング帯域）.....136
Virtual Stacking (SIM)（仮想スタック設定（SIM））.....137
シングル IP マネジメント（SIM）の概要.....137
バージョン 1.61 へのアップグレード.....138
Single IP Settings（シングル IP 設定）.....138
Topology（トポロジ）.....139
Firmware Upgrade（ファームウェア更新）.....143
Configuration File Backup/ Restore（コンフィグレーションファイルの更新）.....143
Upload Log File（ログファイルのアップロード）.....144
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）.....144
SMTP Settings（SMTP 設定）.....145
Reboot Schedule Settings（再起動スケジュール設定）.....146
NLB FDB Settings（NLB FDB 設定）.....147
SD Card Management（SD カード管理）.....148
SD Card Backup Settings（SD カードへのバックアップ設定）.....148
SD Card Execute Settings（SD カード実行設定）.....149

第 8 章　L2 Features（L2 機能の設定）　150

FDB（FDB 設定）....151
Static FDB（スタティック FDB の設定）....151
MAC Address Table Settings（MAC アドレステーブル設定）....152
MAC Address Table（MAC アドレステーブル）....153
MAC Notification（MAC 通知）....154
VLAN（VLAN 設定）....155
802.1Q VLAN（802.1Q VLAN）....155
802.1v Protocol VLAN（802.1v プロトコル VLAN）....156
GVRP（GVRP の設定）....157
Asymmetric VLAN（Asymmetric VLAN 設定）....159
MAC VLAN（MAC VLAN 設定）....160
VLAN Interface（VLAN インタフェース設定）....160
L2VLAN Interface Description（L2VLAN インタフェース概要）....166
Subnet VLAN（サブネット VLAN）....167
Super VLAN（Super VLAN 設定）（EI/MI モードのみ）....167
Auto Surveillance VLAN（自動サーベイランス VLAN）....169
Voice VLAN（音声 VLAN）....170
Private VLAN（プライベート VLAN 設定）....173
VLAN Tunnel（VLAN トンネル）....174
Dot1q Tunnel（Dot1q トンネル）....174
VLAN Mapping（VLAN マッピング）....176
VLAN Mapping Profile（VLAN マッピングプロファイル）....177
STP（スパニングツリー設定）....180
802.1Q-2005 MSTP....180
802.1D-2004 Rapid STP....181
ポートの状態遷移....181
STP Global Settings（STP グローバル設定）....182
STP Port Settings（STP ポートの設定）....183
MST Configuration Identification（MST の設定）....184
STP Instance（STP インタンス設定）....185
MSTP Port Information（MSTP ポート情報）....185
ERPS (G.8032)（イーサネットリングプロテクション設定）....186
ERPS....186
ERPS Profile（ERPS プロファイル）....190
Loopback Detection（ループバック検知設定）....191
Link Aggregation（リンクアグリゲーション）....192
ポートトランクグループについて....192
MLAG（マルチシャーシリンクアグリゲーション）....194
MLAG Settings（MLAG 設定）....194
MLAG Group（MLAG グループ）....196
Flex Links（フレックスリンクス）....196
L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）....197
L2 Multicast Control（L2 マルチキャストコントロール）....198
IGMP Snooping（IGMP Snooping の設定）....198
MLD Snooping（MLD Snooping 設定）....205
Multicast VLAN（マルチキャスト VLAN）....212
PIM Snooping（PIM スヌーピング）....215
Multicast Filtering Mode（マルチキャストフィルタリングモード）....217
LLDP....218
LLDP Global Settings（LLDP グローバル設定）....218
LLDP Port Settings（LLDP ポート設定）....219
LLDP Management Address List（LLDP 管理アドレスリスト）....220
LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）....220
LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）....221
LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）....221
LLDP-MED Port Settings（LLDP-MED ポート設定）....222
LLDP-DCBX Port Settings（LLDP-DCBX ポート設定）....223
LLDP Statistics Information（LLDP 統計情報）....223
LLDP Local Port Information（LLDP ローカルポート情報）....224
LLDP Neighbor Port Information（LLDP ネイバポート情報）....225

第 9 章　L3 Features（レイヤ 3 機能の設定）　227

ARP（ARP 設定）....228
ARP Elevation（ARP エレベーション）....228
ARP Aging Time（ARP エージングタイム設定）....228
Static ARP（スタティック ARP 設定）....229
ARP Force Aging IP Address（ARP 強制エージアウト設定）....229
Proxy ARP（プロキシ ARP）....230
ARP Table（ARP テーブルの参照）....230
Gratuitous ARP（Gratuitous ARP 設定）....231
IPv6 Neighbor（IPv6 ネイバ設定）....232
Interface（インタフェース設定）....233
IPv4 Interface（IPv4 インタフェース）....233
IPv6 Interface（IPv6 インタフェース）....234
Loopback Interface（ループバックインタフェース設定）....237
Null Interface（Null インタフェース）....238
UDP Helper（UDP ヘルパー）....238
IP Forward Protocol（IP 転送プロトコル）....238
IP Helper Address（IP ヘルパーアドレス）....239
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定）....240
IPv4 Static Route BFD（IPv4 スタティックルート BFD）....241
IPv4 Route Table（IPv4 ルートテーブル）....241
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定）....242
IPv6 Static Route BFD（IPv6 スタティックルート BFD）....242
IPv6 Route Table（IPv6 ルートテーブル）....243
Route Preference（ルート優先度設定）....243
ECMP Settings（ECMP 設定）（EI/MI モードのみ）....244
IPv6 General Prefix（IPv6 汎用プリフィクス）....245
IP Tunnel Settings（IP トンネル設定）....245
URPF Settings（URPF 設定）....247
VRF（Virtual Routing and Forwarding）（EI/MI モードのみ）....248
VRF Settings（VRF 設定）....248
VRF Interface Settings（VRF インタフェース設定）....249
RIP（Routing Information Protocol）....250
RIP Settings（RIP 設定）....250
RIP Distribute List（RIP ディストリビュートリスト）....252
RIP Interface Settings（RIP インタフェース設定）....252
RIP Database（RIP データベース）....253
RIPng（RIPng 設定）....254
RIPng Settings（RIPng 設定）....254
RIPng Interface Settings（RIPng インタフェース設定）....255
RIPng Database（RIPng データベース）....255
OSPF（OSPF 設定）（EI/MI モードのみ）....256
OSPFv2（OSPFv2 設定）....256
OSPFv3....269
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）....279
IGMP（IGMP 設定）（EI/MI モードのみ）....279
MLD（MLD 設定）（EI/MI モードのみ）....282
IGMP Proxy（IGMP プロキシ）（EI/MI モードのみ）....285
MLD Proxy（MLD プロキシ）（EI/MI モードのみ）....287
DVMRP（EI/MI モードのみ）....289
PIM（PIM 設定）（EI/MI モードのみ）....291
IPMC（IP マルチキャスト設定）....314
IPv6MC（IPv6 マルチキャスト設定）....318
BGP（Border Gateway Protocol）（EI/MI モードのみ）....321
BGP Global Settings（BGP グローバル設定）....321
BGP Aggregate Address Settings（BGP アグリゲートアドレス設定）....322
BGP Network Settings（BGP ネットワーク設定）....323
BGP Route Redistribution Settings（BGP ルート再分配設定）....324
BGP Route Preference Settings（BGP ルート優先設定）....325
BGP Dampening Settings（BGP ダンプニング設定）....326
BGP Dampening Dampened Paths Table（BGP ダンプニングダンプドパステーブル）....327
BGP Dampening Flap Statistics Table（BGP ダンプニングフラップ統計テーブル）....328
BGP Reflector Settings（BGP リフレクタ設定）....329
BGP Confederation Settings（BGP コンフェデレーション設定）....329
BGP AS Path Access List Settings（BGP AS パスアクセスリストリスト設定）....330

BGP Community List Settings（BGP コミュニティリスト設定）.....330
BGP Extended Community List Settings（BGP 拡張コミュニティリスト設定）.....331
BGP Clear Settings（BGP クリア設定）.....332
BGP Summary Table（BGP サマリテーブル）.....332
BGP Routing Table（BGP ルーティングテーブル）.....333
BGP Labels Table（BGP ラベルテーブル）.....334
BGP Neighbor（BGP ネイバ設定）.....335
BFD（Bidirectional Forwarding Detection）.....344
BFD Settings（BFD 設定）.....344
BFD Neighbor Table（BFD ネイバテーブル）.....345
ISIS（Intermediate System to Intermediate System）（MI モードのみ）.....345
ISIS Global Settings（ISIS グローバル設定）.....345
ISIS Router Settings（ISIS ルータ設定）.....348
ISIS Interface Settings（ISIS インタフェース設定）.....350
ISIS Redistribute Settings（ISIS 再配分設定）.....352
ISIS Redistribute ISIS Settings（ISIS 再配分 ISIS 設定）.....353
ISIS Route Table（ISIS ルートテーブル）.....353
ISIS Database（ISIS データベース）.....354
ISIS Topology（ISIS トポロジ）.....354
ISIS Hostname（ISIS ホスト名）.....355
ISIS Neighbors（ISIS ネイバ）.....355
IP Route Filter（IP ルートフィルタ）.....356
IP Prefix List（IP プレフィックスリスト設定）（EI/MI モードのみ）.....356
Route Map（ルートマップ設定）.....357
Policy Route（ポリシールート設定）.....360
VRRP（VRRP 設定）.....361
VRRPv3 Settings（VRRPv3 設定）.....363

第 10 章　QoS（QoS 機能の設定）　365

Basic Settings（基本設定）.....366
Port Default CoS（ポートデフォルト CoS 設定）.....366
Port Scheduler Method（ポートスケジューラーメソッド設定）.....367
Queue Settings（QoS 設定）.....367
CoS to Queue Mapping（CoS キューマッピング設定）.....368
Port Rate Limiting（ポートレート制限設定）.....368
Queue Rate Limiting（キューレート制限設定）.....369
Queue Statistics Table（キュー統計テーブル）.....370
Advanced Settings（アドバンス設定）.....371
DSCP Mutation Map（DSCP 変更マップ設定）.....371
Port Trust State and Mutation Binding（ポートトラスト設定）.....371
DSCP CoS Mapping（DSCP CoS マップ設定）.....372
CoS Color Mapping（CoS カラーマップ設定）.....372
DSCP Color Mapping（DSCP カラーマップ設定）.....373
Class Map（クラスマップ設定）.....373
Aggregate Policer（アグリゲートポリサー設定）.....375
Policy Map（ポリシーマップ設定）.....377
Policy Binding（ポリシーバインディング設定）.....378
QoS PFC.....379
Network QoS Class Map（ネットワーク QoS クラスマップ）.....379
Network QoS Policy Map（ネットワーク QoS ポリシーマップ）.....380
Network QoS Policy Binding（ネットワーク QoS ポリシーバインディング）.....381
PFC Port Settings（PFC ポート設定）.....381
WRED（WRED 設定）.....382
WRED Profile（WRED プロファイル設定）.....382
WRED Queue（WRED キュー設定）.....383
WRED Drop Counter（WRED ドロップカウンタ設定）.....383
iSCSI（アイスカジー）.....384
iSCSI Settings（アイスカジー設定）.....384
iSCSI Sessions（アイスカジーセッション）.....385

第 11 章　ACL（ACL 機能の設定）　386

ACL Configuration Wizard（ACL 設定ウィザード）....387
ACL Configuration Wizard（ACL 設定ウィザードの開始）....387
パケットタイプ選択（ACL 設定ウィザード）....387
ルール追加（ACL 設定ウィザード）....388
ポート設定（ACL 設定ウィザード）....393
ACL Access List（ACL アクセスリスト）....393
Standard IP ACL（通常 IP ACL）....394
Extended IP ACL（拡張 IP ACL）....396
Standard IPv6 ACL（通常 IPv6 ACL）....401
Extended IPv6 ACL（拡張 IPv6 ACL）....403
Extended MAC ACL（拡張 MAC ACL）....408
Extended Expert ACL（拡張詳細 ACL）....411
ACL Interface Access Group（ACL インタフェースアクセスグループ）....416
ACL VLAN Access Map（ACL VLAN アクセスマップ）....417
Match Access-List（合致するアクセスリスト設定）....417
ACL VLAN Filter（ACL VLAN フィルタ設定）....418
CPU ACL（CPU ACL）....418

第 12 章　Security（セキュリティ機能の設定）　421

Port Security（ポートセキュリティ）....422
Port Security Global Settings（ポートセキュリティグローバル設定）....422
Port Security Port Settings（ポートセキュリティポート設定）....423
Port Security Address Entries（ポートセキュリティアドレスエントリ設定）....424
802.1X（802.1X 認証設定）....425
802.1X Global Settings（802.1X グローバル設定）....429
802.1X Port Settings（802.1X ポート設定）....429
Authentication Session Information（オーセンティケーションセッションの状態）....430
Authenticator Statistics（オーセンティケータ統計情報）....430
Authenticator Session Statistics（オーセンティケータセッション統計情報）....431
Authenticator Diagnostics（オーセンティケータ診断）....431
AAA（AAA 設定）....432
AAA Global Settings（AAA グローバル設定）....432
Application Authentication Settings（アプリケーションの認証設定）....432
Application Accounting Settings（アプリケーションアカウント設定）....433
Authentication Settings（認証設定）....434
Accounting Settings（アカウンティング設定）....435
RADIUS（RADIUS 設定）....436
RADIUS Global Settings（RADIUS グローバル設定）....436
RADIUS Server Settings（RADIUS サーバの設定）....436
RADIUS Group Server Settings（RADIUS グループサーバの設定）....437
RADIUS Statistic（RADIUS 統計情報）....438
TACACS+（TACACS+ 設定）....438
TACACS+ Global Settings（TACACS+ サーバグローバル設定）....438
TACACS+ Server Settings（TACACS+ サーバの設定）....439
TACACS+ Group Server Settings（TACACS+ グループサーバの設定）....439
TACACS+ Statistic（TACACS+ 統計情報）....440
IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）....441
IPv4....441
IPv6....451
DHCP Server Screening（DHCP サーバスクリーニング設定）....456
DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）....456
DHCP Server Screening Port Settings（DHCP サーバスクリーニングポート設定）....457
ARP Spoofing Prevention（ARP スプーフィング防止設定）....457
BPDU Attack Protection（BPDU アタック防止設定）....458
NetBIOS Filtering（NetBIOS フィルタリング設定）....459
MAC Authentication（MAC 認証）....459
Web-based Access Control（Web 認証）....460
Web Authentication（Web 認証設定）....462
WAC Port Settings（Web 認証ポート設定）....462
WAC Customize Page（WAC カスタマイズページ設定）....463
Network Access Authentication（ネットワークアクセス認証）....463
Guest VLAN（ゲスト VLAN 設定）....463
Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）....464
Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）....465
Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）....466

Safeguard Engine（セーフガードエンジン）....466
Safeguard Engine Settings（セーフガードエンジン設定）....467
CPU Protect Counters（CPU プロテクトカウンタ）....468
CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）....468
CPU Protect Type（CPU プロテクトタイプ）....469
Trusted Host（トラストホスト）....469
Traffic Segmentation（トラフィックセグメンテーション）....470
Storm Control Settings（ストームコントロール設定）....470
DoS Attack Prevention Settings（DoS 攻撃防止設定）....472
Zone Defense Settings（ゾーンディフェンス設定）....473
SSH（Secure Shell）....474
SSH Global Settings（SSH グローバル設定）....474
Host Key（Host Key 設定）....475
SSH Server Connection（SSH サーバ接続）....476
SSH User Settings（SSH ユーザ設定）....476
SSL（Secure Socket Layer）....477
SSL Global Settings（SSL グローバル設定）....477
Crypto PKI Trustpoint（暗号 PKI トラストポイント）....478
SSL Service Policy（SSL サービスポリシー）....479
SFTP Server Settings（SFTP サーバ設定）....479
SFTP Client Settings（SFTP クライアント設定）....480
Network Protocol Port Protect Settings（ネットワークプロトコルポートプロテクト設定）....480

第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)　481

CFM（Connectivity Fault Management : 接続性障害管理）....482
CFM Settings（CFM 設定）....482
CFM Port Settings（CFM ポート設定）....490
CFM Loopback Test（CFM ループバックテスト）....491
CFM Linktrace Settings（CFM リンクトレース設定）....491
CFM Packet Counter（CFM パケットカウンタ）....492
CFM Counter CCM（CFM カウンタ CCM）....493
CFM MIP CCM Table（CFM MIPCCM テーブル）....493
CFM MEP Fault Table（CFM MEP 障害テーブル）....493
Cable Diagnostics（ケーブル診断機能）....494
Ethernet OAM（イーサネット OAM）....495
Ethernet OAM Settings（イーサネット OAM 設定）....495
Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）....496
Ethernet OAM Event Log Table（イーサネット OAM イベントログテーブル）....497
Ethernet OAM Statistics Table（イーサネット OAM 統計情報テーブル）....498
Ethernet OAM DULD Settings（イーサネット OAM DULD 設定）....498
DDM（DDM 設定）....499
DDM Settings（DDM 設定）....499
DDM Temperature Threshold Settings（DDM 温度しきい値設定）....500
DDM Voltage Threshold Settings（DDM 電圧しきい値設定）....500
DDM Bias Current Threshold Settings（DDM バイアス電流しきい値設定）....501
DDM TX Power Threshold Settings（DDM 送信電力しきい値設定）....501
DDM RX Power Threshold Settings（DDM 受信電力しきい値設定）....502
DDM Status Table（DDM ステータステーブル）....502

第 14 章　MPLS（MI モードのみ）　503

MPLS LDP Information Settings（MPLS LDP 情報設定）....504
MPLS LSP Trigger Information（MPLS LSP トリガ情報）....506
MPLS Forwarding Settings（MPLS フォワーディング設定）....507
MPLS LDP Neighbor Password Settings（MPLS LDP ネイバパスワード設定）....508
MPLS LDP Neighbor Targeted Settings（MPLS LDP ネイバターゲット設定）....508
MPLS LDP Neighbor Information（MPLS LDP ネイバ情報）....509
MPLS Global Settings（MPLS グローバル設定）....509
MPLS LDP Interface Settings（MPLS LDP インタフェース設定）....510
MPLS LDP Session Information（MPLS LDP セッション情報）....511
MPLS LDP Statistic（MPLS LDP スタティスティック）....512
MPLS LDP Binding Table（MPLS LDP バインディングテーブル）....512
MPLS LDP Discovery Information（MPLS LDP ディスカバリ情報）....512
MPLS QoS Settings（MPLS QoS 設定）....513
Ping MPLS....516
Traceroute MPLS IPv4（トレースルート MPLS IPv4）....517

第 15 章　MPLS L2VPN（MI モードのみ） 518

VPWS Settings（VPWS 設定）....519
L2VC Interface Description（L2VC インタフェース概要）....521
VPLS Settings（VPLS 設定）....522
VPLS MAC Address Table（VPLS MAC アドレステーブル）....525

第 16 章　Monitoring（スイッチのモニタリング） 526

VLAN Counter（VLAN カウンタ）....527
Utilization（利用分析）....528
Port Utilization（ポート使用率）....528
History Utilization（使用履歴）....528
Statistics（統計情報）....530
Port（ポート統計情報）....530
CPU Port（CPU ポート）....531
Interface Counters（インタフェースカウンタ）....532
Interface History Counters（インタフェースカウント履歴）....533
Counters（カウンタ）....534
Mirror Settings（ミラー設定）....535
sFlow（sFlow 設定）....536
sFlow Agent Information（sFlow エージェント情報）....536
sFlow Receiver Settings（sFlow レシーバ設定）....537
sFlow Sampler Settings（sFlow サンプラ設定）....537
sFlow Poller Settings（sFlow ポーラ設定）....538
Device Environment（機器環境確認）....538
External Alarm Settings（外部アラーム設定）....539

第 17 章　Green（省電力機能） 540

Power Saving（省電力）....541
EEE（Energy Efficient Ethernet/ 省電力イーサネット）....542

第 18 章　OpenFlow 543

OpenFlow Settings（OpenFlow 設定）....544

第 19 章　Save and Tools（Save メニュー /Tools メニュー） 545

Save（Save メニュー）....546
Save Configuration（コンフィグレーションの保存）....546
Tools（Tools メニュー）....546
Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）....546
Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）....551
Certificate & Key Restore & Backup（証明書 / 鍵リストア＆バックアップ）....556
Log Backup（ログファイルのバックアップ）....561
Ping....563
Trace Route（トレースルート）....565
Reset（リセット）....566
Reboot System（システム再起動）....567
DLMS Settings（DLMS 設定）....567

付録 A パスワードリカバリ手順 568

付録 B システムログエントリ 569

付録 C トラップログエントリ 606

付録 D OpenFlow オブジェクト 619

Flow Table（フローテーブル）....619
Policy ACL Flow Table....619
Group Table（グループテーブル）....621
L2 Interface Group Entry Type....621
L2 Rewrite Group Entry Type....621
L2 Multicast Group Entry Type....622
L3 Unicast Group Entry Type....622
L3 ECMP Group Entry Type....623
Meter Table（メーターテーブル）....624

付録 E RADIUS 属性割り当て 625

付録 F IETF RADIUS 属性サポート 627

付録 G 機能設定例 628

対象機器について 628
Traffic Segmentation（トラフィックセグメンテーション） 629
VLAN 630
Link Aggregation（リンクアグリゲーション） 631
Access List（アクセスリスト） 633
Loopback Detection（LBD）（ループ検知） 634

はじめに

DGS-3630 シリーズユーザマニュアルは、本スイッチのインストールおよび操作方法を例題と共に記述しています。

第 1 章 本製品のご使用にあたって
- 本スイッチの概要とその機能について説明します。また、前面、背面、側面の各パネルと LED 表示について説明します。

第 2 章 スイッチの設置
- システムの基本的な設置方法について説明します。また、本スイッチの電源接続の方法についても紹介します。

第 3 章 スイッチの接続
- スイッチをご使用のネットワークに接続する方法を説明します。

第 4 章 スイッチの管理の導入
- パスワード設定、SNMP 設定、および各種デバイスからの本スイッチへの接続など基本的なスイッチの管理について説明します。

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

第 6 章 System（スイッチの主な設定）
- デバイス情報、ポート設定、ユーザアカウント、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）
- シングル IP マネジメント設定、SNMP 設定、Telnet 設定、Web 設定などの管理機能について説明します。

第 8 章 L2 Features（L2 機能の設定）
- VLAN、トランキング、スパニングツリー、LLDP などのレイヤ 2 機能について説明します。

第 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、ルート再配布設定、スタティック / ダイナミックルート設定、ルート優先度設定、RIP、OSPF、VRRP、IP マルチキャストルーティングプロトコル、BGP、BFD、ISIS、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、802.1p ユーザプライオリティなどの機能を含みます。

第 11 章 ACL（ACL 機能の設定）
- ACL アクセスリスト、ACL VLAN アクセスマップ、CPU ACL などの ACL（アクセスコントロールリスト）機能について説明します。

第 12 章 Security（セキュリティ機能の設定）
- 802.1X、トラストホスト、アクセス認証コントロール、ポートセキュリティ、トラフィックセグメンテーション、SSL、SSH、IP-MAC- ポートバインディング、IP マルチキャスト範囲の制限、Web ベースアクセスコントロール、MAC ベースアクセスコントロールおよびセーフガードエンジンなどのセキュリティ機能について説明します。

第 13 章 OAM (Operations, Administration, Maintenance：運用・管理・保守)
- CFM（接続性障害管理）、イーサネット OAM、DDM、ケーブル診断機能機能について説明します。

第 14 章 MPLS
- MPLS LDP、MPLS LSP、MPLS フォワーディング、MPLS QoS、Ping MPLS、トレースルート MPLS などについて説明します。

第 15 章 MPLS L2VPN
- VPWS 設定、L2VC インタフェース、VPLS 設定、VPLS MAC アドレステーブルなどについて説明します。

第 16 章 Monitoring（スイッチのモニタリング）
- CPU 使用率、パケット統計情報、エラー、パケットサイズ、ミラーリング、sFlow、外部アラーム設定などのモニタ機能について説明します。

第 17 章 Green（省電力機能）
- Power Saving（省電力）、EEE（Energy Efficient Ethernet/ 省電力イーサネット）について説明します。

第 18 章 OpenFlow
- OpenFlow の設定について説明します。

第 19 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、DLMS 設定について説明します。

付録 A パスワードリカバリ手順

- パスワードのリセット、リカバリについて説明します。

付録 B システムログエントリ

- スイッチのシステムログに表示される可能性のあ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

- トラップログエントリついて説明します。

付録 D OpenFlow オブジェクト

- OpenFlow オブジェクトについて説明します。

付録 E 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 F IETF RADIUS 属性サポート

- 現在スイッチによりサポートされる IETF RADIUS 属性一覧です。

付録 G 機能設定例

- スイッチの機能設定例です。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、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のある事項について説明します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "（13 ページ）をご参照ください。
`courier` フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
`courier` 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
`courier` 斜体	コマンドパラメータ（可変または固定）。	*`value`*
< >	可変パラメータ。< > にあたる箇所に値または文字を入力します。	<*`value`*>
[ ]	任意の固定パラメータ。	[*`value`*]
[< >]	任意の可変パラメータ。	[<*`value`*>]
{ }	{ } 内の選択肢から 1 つ選択して入力するパラメータ。	{*`choice1`* | *`choice2`*}
|（垂直線）	相互排他的なパラメータ。	*`choice1`* | *`choice2`*
[{ }]	任意のパラメータで、指定する場合はどちらかを選択します。	[{*`choice1`* | *`choice2`*}]

製品名 / 品番一覧

製品名	区分	品番
DGS-3630-28SC	**SI 版**	DGS-3630-28SCSI/A1
	EI 版	DGS-3630-28SCEI/A1
	MI 版	DGS-3630-28SCMI/A1
DGS-3630-28TC	**SI 版**	DGS-3630-28TCSI/A1
	EI 版	DGS-3630-28TCEI/A1
	MI 版	DGS-3630-28TCMI/A1
DGS-3630-52TC	**SI 版**	DGS-3630-52TCSI/A1
	EI 版	DGS-3630-52TCEI/A1
	MI 版	DGS-3630-52TCMI/A1
DGS-3630-28PC	**SI 版**	DGS-3630-28PCSI/A2
	EI 版	DGS-3630-28PCEI/A2
	MI 版	DGS-3630-28PCMI/A2
DGS-3630-52PC	**SI 版**	DGS-3630-52PCSI/A2
	EI 版	DGS-3630-52PCEI/A2
	MI 版	DGS-3630-52PCMI/A2

第 1 章　本製品のご使用にあたって

- DGS-3630 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

DGS-3630 シリーズについて

D-Link Green 機能を実装した DGS-3630 シリーズは、SMB からエンタープライズ向けの中規模ネットワークにおいて柔軟性、冗長性、セキュリティを実現し、安定したパフォーマンスでネットワーク通信を提供することが可能な高性能な次世代ギガビットレイヤ 3 スイッチです。
本シリーズは、DGS-3630-28TC、DGS-3630-52TC に加え、PoE/PoE+ に対応した DGS-3630-28PC、DGS-3630-52PC、SFP 多ポートに対応した DGS-3630-28SC の 5 製品で構成されています。全ての製品には 10GE SFP+ スロットが 4 つ搭載されており、物理スタック /10G アップリンクとして利用が可能です。また高密度 SFP ポートスイッチの利点を活かし、FTTB ネットワークのコアを形成します。ITU-T G.8032 準拠の E-RPS プロトコルに対応したリング構成による冗長化や、IEEE802.3ah、Q-in-Q などメトロイーサネット機能にも対応し、柔軟なネットワーク構築が可能です。また、ループ検知 / 遮断機能、ケーブル診断機能、デジタル診断モニタ（DDM）などの障害切り分けを容易にするサポート機能等が充実しています。

ニーズに合わせたイメージを選択

本スイッチは、ユーザのニーズに合わせて MPLS バージョン（MI）、エンハンスドバージョン (EI) とスタンダードバージョン (SI) に分かれており、必要な機能に応じて機器のバージョンを選択することが可能です。MI バージョン、EI バージョンは SI バージョンの全ての機能を搭載し、様々な機能を追加した高機能版となっております。主に EI バージョンは「OSPF」「BGP」や L3 マルチキャスト対応機能などを有し、MI バージョンは「IS-IS」や「MPLS L2/L3 VPN」などの VPN サービスを提供します。

IPv6 テクノロジー

本シリーズは、IPv6 Ready Logo Phase-2 を取得しています（DGS-3630-28PC/52PC は除く）。また、OSFPv3（EI/MI）、BGP4（EI/MI）、PIM SMv6（EI/MI）など IPv6 環境でのルーティングやマルチキャスト制御にも対応しています。

安定の可用性と多様な管理機能

「Switch Resource Management」(SRM) の実装により、「IP モード」「LAN モード」「L2 VPN モード」が選択可能になり、スイッチの使用モードによって L2/L3 テーブルサイズを変更され、各機能の最適化を行うことができます。更に DGS-3630 シリーズはネットワークマネージメントシステムや Web GUI、CLI を使用することでリモートからの管理や、SNMP などにより帯域外の多数の機器をコンソールポートを通して集権的に管理をすることが可能です。パネルには「mini-USB」「RJ45」二つのコンソールポート、USB ポート、MGMT ポートが装備され、広いニーズに対応した多彩な管理を実現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 SFP+ スロットを各 4 スロット搭載しています。10G SFP+ スロットでの最大 9 台までの物理スタックに対応し、帯域を最大 80G まで選択することが可能です。

本マニュアルでは、DGS-3630 シリーズの設置、管理、および設定の方法について記述しています。

ポート

DGS-3630 シリーズは以下のポートを搭載しています。

製品名	DGS-3630-28SC	DGS-3630-28TC	DGS-3630-28PC	DGS-3630-52TC	DGS-3630-52PC
10/100/1000BASE-T ポート (RJ-45) (PoE 給電)	4 (SFP 4 スロットとのコンボ)	24	24 (24)	48	48 (48)
SFP スロット	24	4 (1000BASE-T 4 ポートとのコンボ)	4 (1000BASE-T 4 ポートとのコンボ)	4 (1000BASE-T 4 ポートとのコンボ)	4 (1000BASE-T 4 ポートとのコンボ)
10 ギガ SFP+ スロット	4				
コンソールポート (RJ-45)	1				
コンソールポート (Mini USB)	1				
管理ポート (MGMT) (RJ-45)	1				
アラームポート (ALARM) (RJ-45)	1				
USB ポート (USB2.0)	1				

前面パネル

28TC/28SC の前面パネルには、10BASE-T/100BASE-TX/1000BASE-T ポート、SFP (コンボ) スロット、10 ギガ SFP +スロット、コンソールポート (RJ-45/Mini-USB)、RJ-45 管理ポート、アラームおよび USB ポートが配置されています。また、電源、コンソール、RPS (冗長電源システム)、USB、ファン、管理、およびオプションモジュール用の SFP ポートを含む各ポートの Link/Act/Speed の状態を表示する LED を搭載しています。「LED 表示」の項で詳細の動作について説明します。
52TC の前面パネルには、10BASE-T/100BASE-TX/1000BASE-T ポート、SFP コンボスロット、10 ギガ SFP +スロットが配置されています。また、電源、コンソール、RPS (冗長電源システム)、ファンおよびオプションモジュール用の SFP ポートを含む各ポートの Link/Act/Speed の状態を表示する LED を搭載しています。「LED 表示」の項で詳細の動作について説明します。

DGS-3630-28TC

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 24
- SFP コンボスロット x 4
- SFP+ スロット x 4
- RJ-45 アラームポート x 1
- RJ-45 コンソールポート x 1
- Mini-USB 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、Console、RPS、USB、Fan Err、MGMT、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

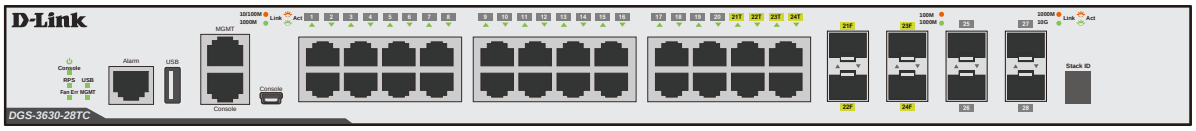


図 3-1　DGS-3630-28TC の前面パネル

DGS-3630-28SC

- SFP スロット x 24
- 10BASE-T/100BASE-TX/1000BASE-T コンボポート x4
- SFP+ スロット x 4
- RJ-45 アラームポート x 1
- RJ-45 コンソールポート x 1
- Mini-USB 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、Console、RPS、USB、Fan Err、MGMT、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

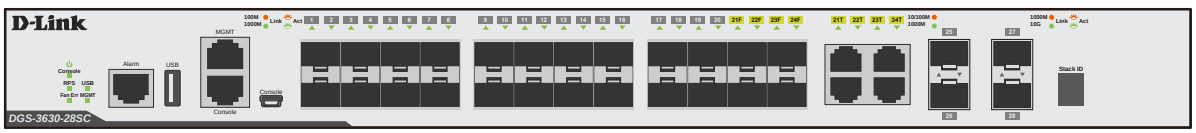


図 3-2　DGS-3630-28SC の前面パネル

DGS-3630-28PC

- 10BASE-T/100BASE-TX/1000BASE-T ポート（PoE 給電）x 24
- SFP コンボスロット x 4
- SFP+ スロット x 4
- RJ-45 アラームポート x 1
- RJ-45 コンソールポート x 1
- Mini-USB 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、Console、RPS、USB、Fan Err、MGMT、Link/Act/Speed（各ポート / スロット）
- Mode ボタン & LED：PoE、Link/Act
- スタックモジュール番号 LED

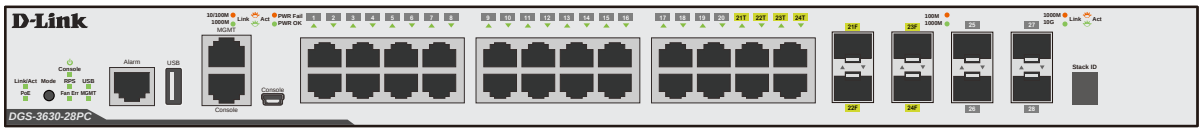


図 3-3　DGS-3630-28PC の前面パネル

DGS-3630-52TC

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 48
- SFP コンボスロット x 4
- SFP+ スロット x 4
- Power、Console、RPS、Fan Err、Link/Act/Speed（各ポート / スロット）
- スタックモジュール番号 LED

注意 RJ-45 アラームポート、RJ-45/Mini-USB コンソールポート、管理ポート、USB ポートは背面に配置されています。

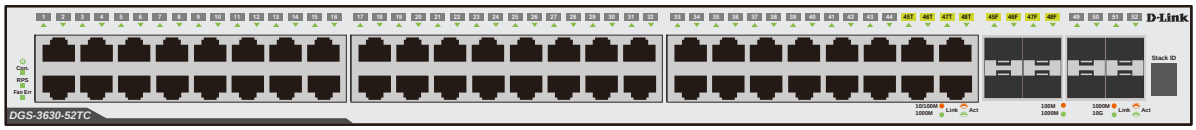


図 3-4　DGS-3630-52TC の前面パネル

DGS-3630-52PC

- 10BASE-T/100BASE-TX/1000BASE-T ポート（PoE 給電）x 48
- SFP コンボスロット x 4
- SFP+ スロット x 4
- Power、Console、RPS、Fan Err、Link/Act/Speed（各ポート / スロット）
- Mode ボタン & LED：PoE、Link/Act
- スタックモジュール番号 LED

注意 RJ-45 アラームポート、RJ-45/Mini-USB コンソールポート、管理ポート、USB ポートは背面に配置されています。

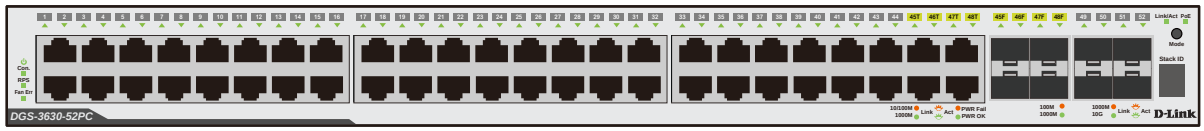


図 3-5　DGS-3630-52PC の前面パネル

アラームポート（RJ-45）

外部からの機器をアラームイベントのトリガとして、またはスイッチによって発動されたアラームイベントの受信機として、スイッチのアラームポート（RJ-45）に接続することが可能です。外部機器との接続は RJ45 コネクタのアラームポートを使用します。他の RJ45 接続と同様、4 ペアの銅線が使用され、2 ペアが温度センサなどの入力接続に、もう 2 ペアがスピーカや LED 用の出力接続に使用されます。

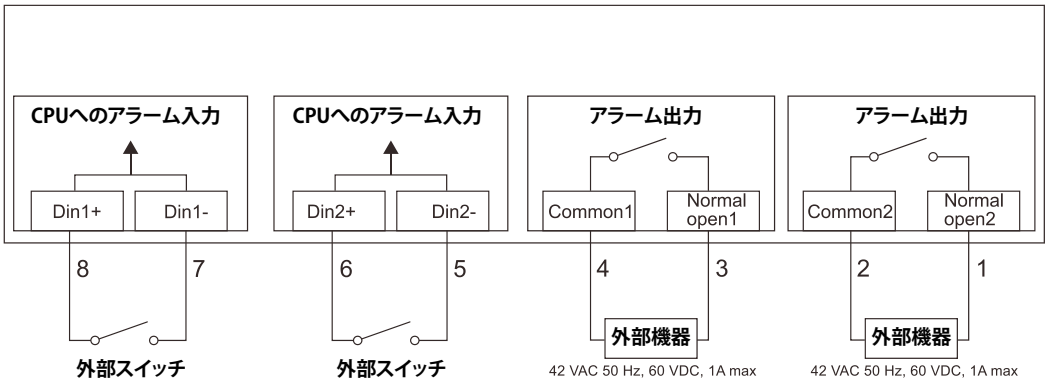


図 3-6　アラームコネクタ

アラームコネクタポート

コンタクト	アラームコネクタポート
1	Normal open2（42VAC 50Hz、60VDC、1Amax）
2	Common2（42VAC 50Hz、60VDC、1Amax）
3	Normal open1（42VAC 50Hz、60VDC、1Amax）
4	Common1（42VAC 50Hz、60VDC、1Amax）
5	Din2-（最大入力電圧：3VDC）
6	Din2+（最大入力電圧：3VDC）
7	Din1-（最大入力電圧：3VDC）
8	Din1+（最大入力電圧：3VDC）

アラーム入力は「pin-pairs」（ピンのペア）で行われ、ペア 1（Din1+/Din1-）そしてペア 2（Din2+/Din2-）はスイッチの CPU へのアラームシグナル送信に使用されます。「Din+」と「Din-」間の回路に短絡が生じるとアラームシグナルは CPU へ送信されます。アラーム出力も「pin-pairs」（ピンのペア）で行われ、ペア 1（Common1/Normal open1）そしてペア 2（Common2/Normal open2）はスイッチの CPU にコントロールされて、アラームシグナルを外部機器へ送信します。「Common」と「Normal」間の回路がオープンになると「42VAC/50Hz、60VDC、1A」が送信されます。CPU はイベント発生時にこの回路を短絡することができます。

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、Console、MGMT など、および各ポートについて LED をサポートします。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-3630-28TC



図 3-7　DGS-3630-28TC の前面パネル LED 配置図

DGS-3630-28SC

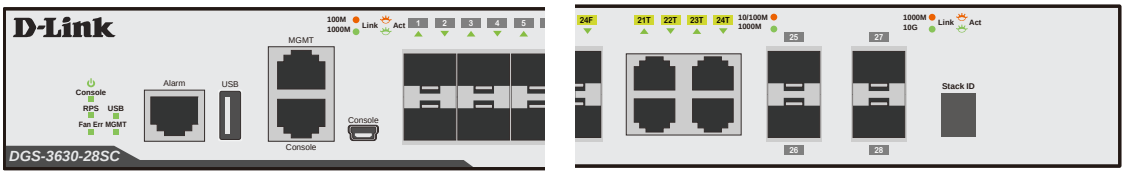


図 3-8　DGS-3630-28SC の前面パネル LED 配置図

DGS-3630-28PC



図 3-9　DGS-3630-28PC の前面パネル LED 配置図

DGS-3630-52TC

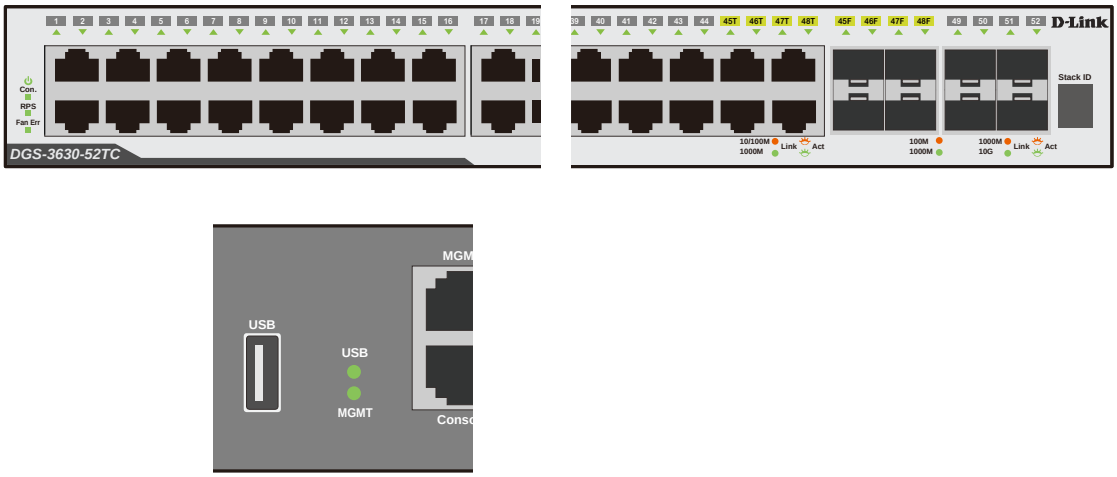


図 3-10　DGS-3630-52TC の背面パネル LED 配置図（上 : 前面 / 下 : 背面）

DGS-3630-52PC

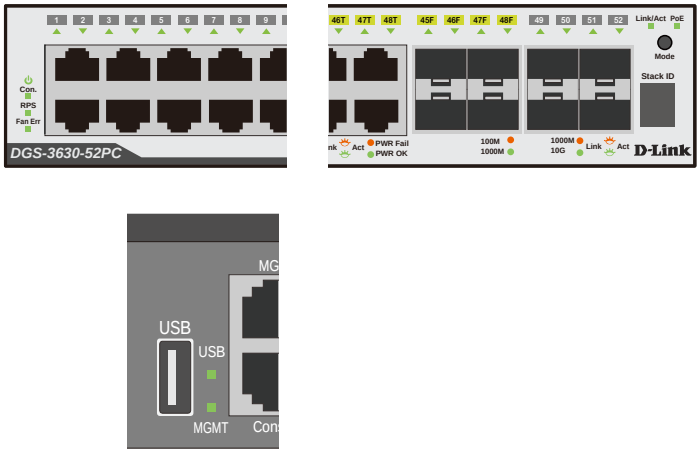


図 3-11　DGS-3630-52PC の背面パネル LED 配置図（上 : 前面 / 下 : 背面）

以下の表に LED の状態が意味するスイッチの状態を示します。

LED	色	状態	状態説明
Mode ボタン & LED（DGS-3630-28PC/52PC のみ）（PoE モード、Link/Act モードへの切り替え）			
PoE	緑	点灯	ポート LED は各ポートの PoE の状態について表示します。
Link/Act	緑	点灯	ポート LED は各ポートの Link/Act/Speed の状態について表示します。
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。
	–	消灯	スイッチに電源が供給されていません。
MGMT	緑	点灯	管理ポートでリンクが確立されています。
		点滅	ポートで通信が発生しています。
	–	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。
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。
	橙	点灯	Mini-USB コンソールポートのリンクが確立しています。
	–	消灯	リンクが確立していません。

LED	色	状態	状態説明
Fan Err	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。
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。
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 LED	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。
10/100/1000 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-3630-28PC/52PC）	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)
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。

背面パネル

DGS-3630-28TC、28SC、28PC

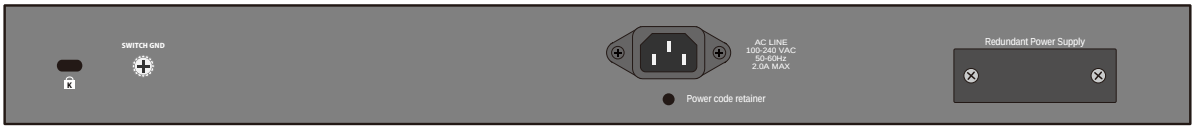


図 3-12　DGS-3630-28TC、28SC 背面パネル図



図 3-13　DGS-3630-28PC 背面パネル図

DGS-3630-28TC、28SC、28PC の背面パネルには、セキュリティスロット、接地コネクタ、電源抜け防止クリップ挿入口（28PC は除く）、AC 電源コネクタ、オプションの外部リダンダント電源用のコネクタが配備されています。オプションのリダンダント電源ユニット用のアウトレットがあります。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。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。

DGS-3630-52TC、52PC

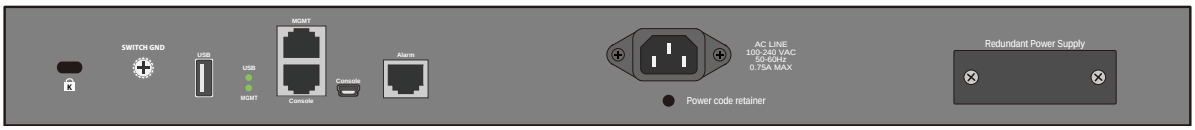


図 3-14　DGS-3630-52TC 背面パネル図



図 3-15　DGS-3630-52PC 背面パネル図

DGS-3630-52TC、52PC の背面パネルには、セキュリティスロット、接地コネクタ、USB ポート、ステータス LED（USB/MGMT）、MGMT ポート、コンソールポート (RJ-45)、コンソールポート (Mini-USB)、ALARM ポート、電源抜け防止クリップ挿入口（52PC は除く）、AC 電源コネクタ、オプションの外部リダンダント電源用のコネクタが配備されています。オプションのリダンダント電源ユニット用のアウトレットがあります。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。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。

側面パネル

システムのファンと通気口がスイッチにあり内部の熱を放出します。これらをふさがないようにご注意ください。スイッチの適切な通気のためには、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。最適な熱放出、空気の循環をしないとシステム障害や部品の激しい損傷を引き起こす場合がありますのでご注意ください。

DGS-3630-28TC、28SC

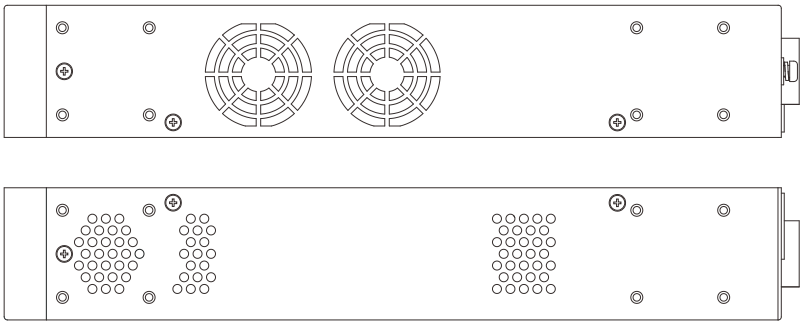


図 3-16　側面パネル図（DGS-3630-28TC / DGS-3630-28SC）

DGS-3630-52TC

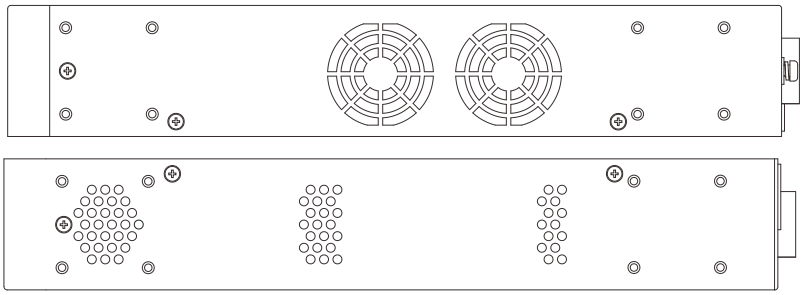


図 3-17　側面パネル図（DGS-3630-52TC）

DGS-3630-28PC、52PC

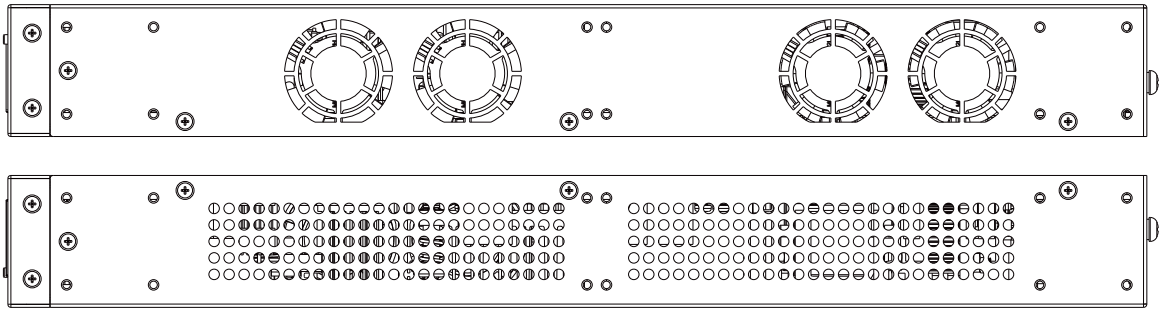


図 3-18　側面パネル図（DGS-3630-28PC / DGS-3630-52PC）

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
- USB/Mini-USB ケーブル　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（DGS-3630-28PC/52PC は除く）　x　1
- シリアルラベル　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、まずスイッチに同梱されていた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。

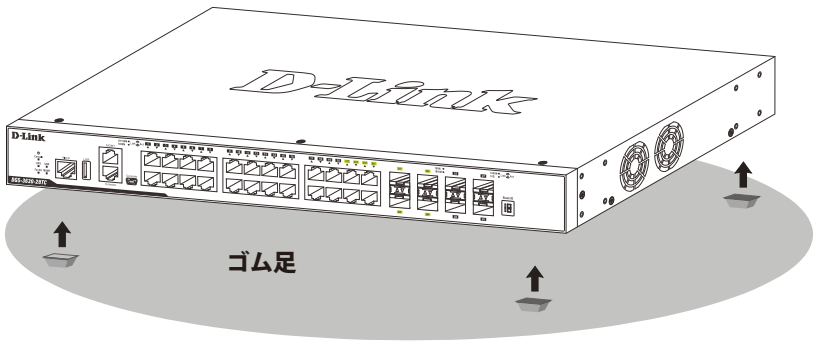


図 2-1　ゴム足の取り付け

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。

注意 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。

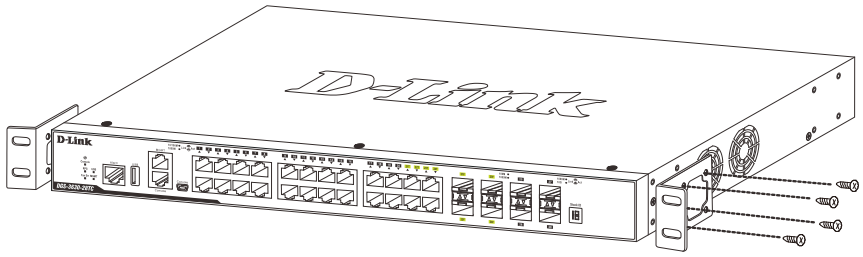


図 2-2　スイッチへのブラケットの取り付け図

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。

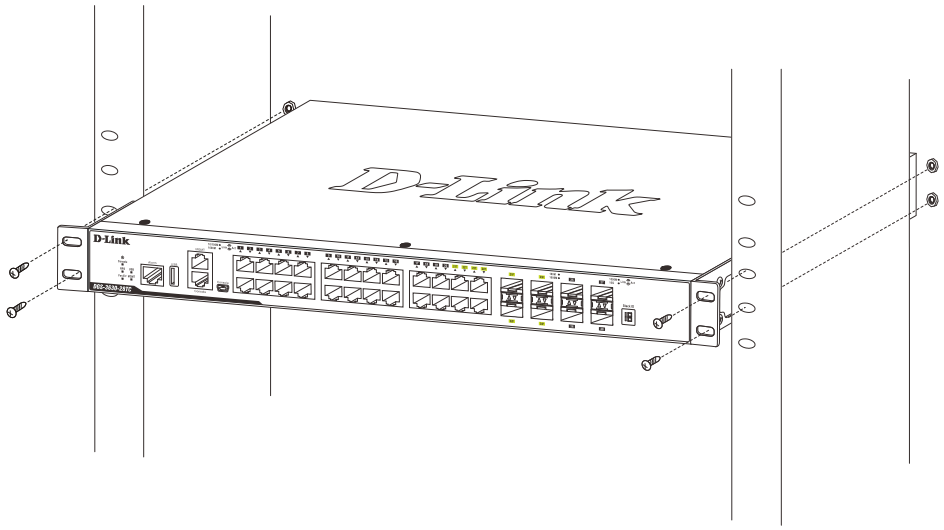


図 2-3　スイッチのラックへの設置図

SFP/SFP+ ポートへのモジュールの取り付け

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。

注意 コンボポートの SFP ポートモジュール挿入時は 1000BASE-T ポートとしての使用はできません。SFP ポートが優先されます。

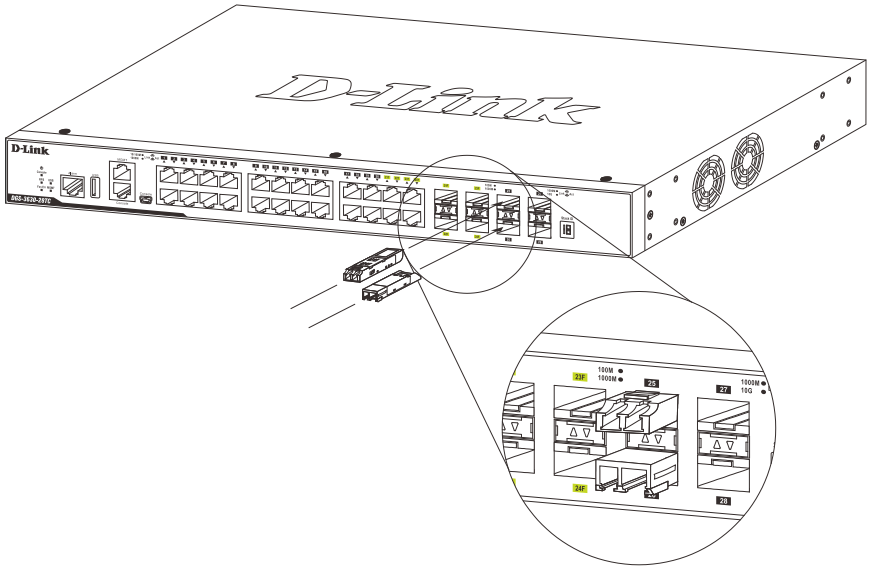


図 2-4　DGS-3630 シリーズ前面パネルの SFP ポートへのモジュールの挿入

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。

注意 DGS-3630-28PC/52PC は未サポートです。

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。

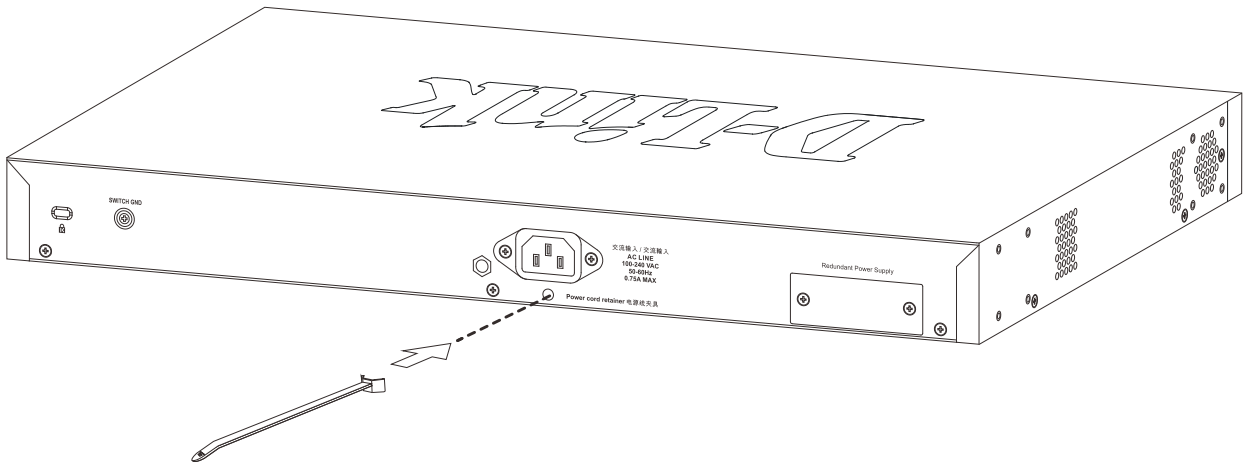


図 2-5　タイラップの挿し込み

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。

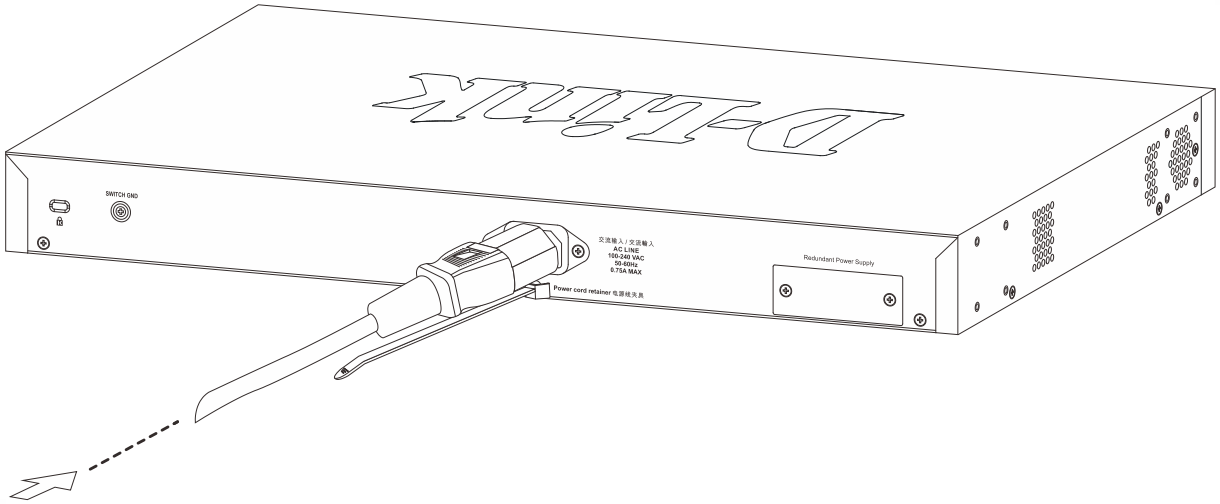


図 2-6　電源コード挿し込み

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。

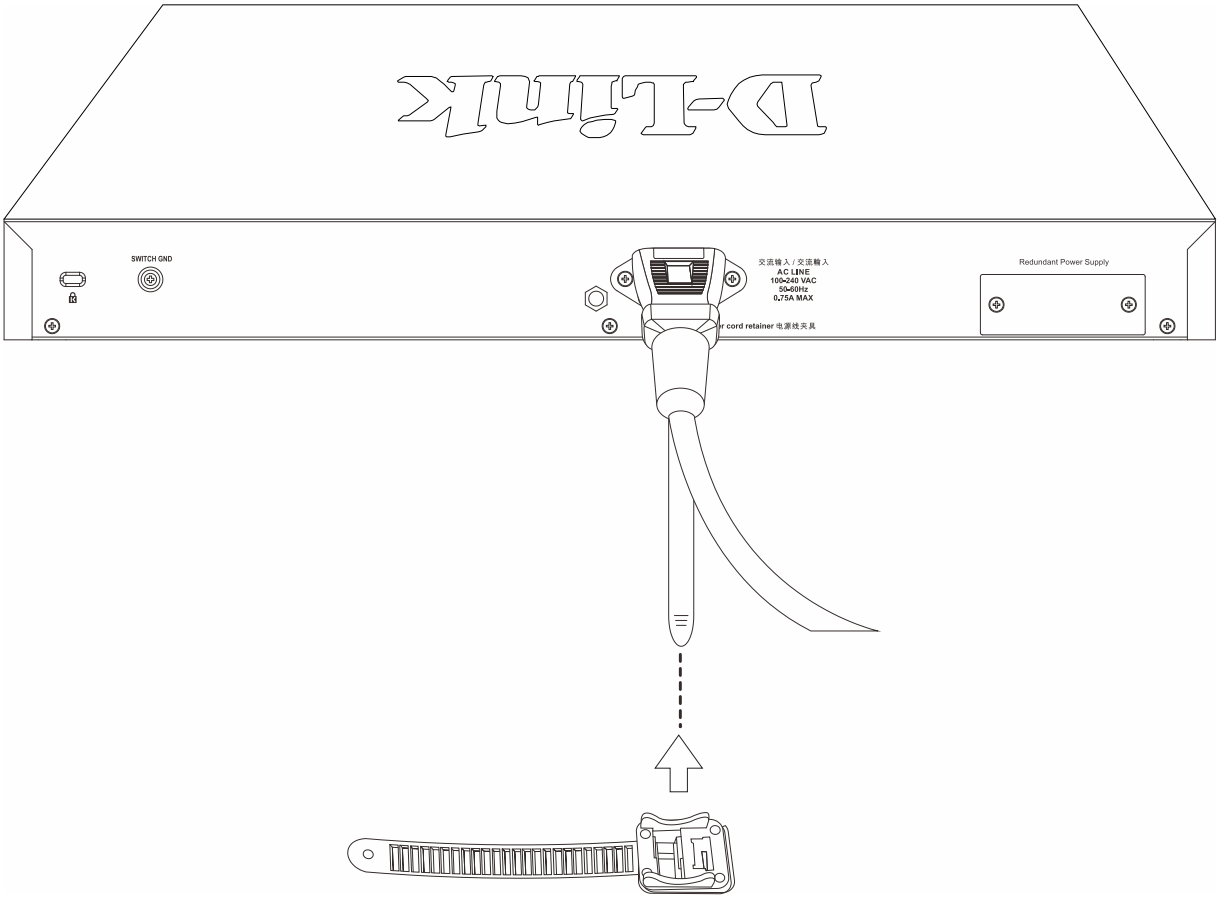


図 2-7　リテイナー（固定具）のスライド

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。

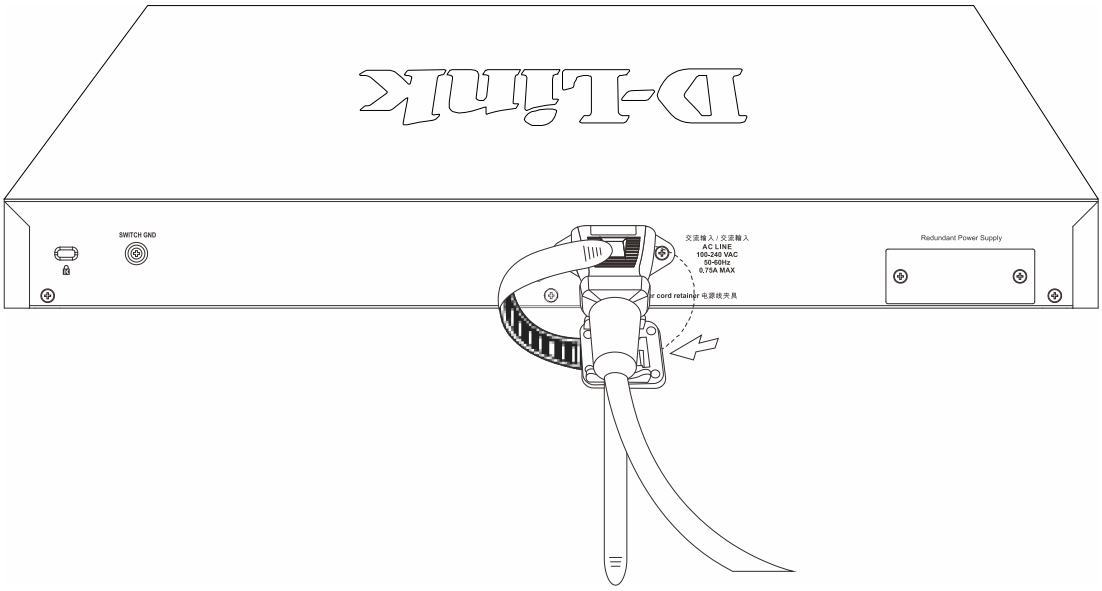


図 2-8　リテイナーの巻き付け、固定

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

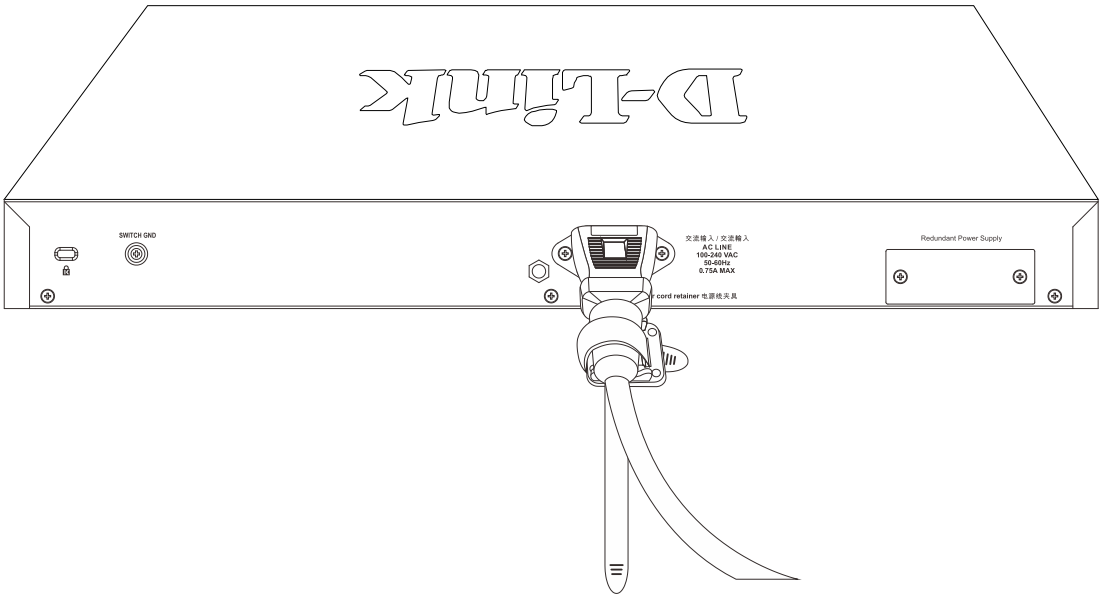


図 2-9　電源抜け防止クリップの固定確認

リダンダント電源システムの設置

DGS-3630 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-3630-28SC/28TC/52TC）、DPS-700（DGS-3630-28PC/52PC）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。

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。

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。

DPS-500A

DPS-500A は DGS-3630-28SC/28TC/52TC 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。

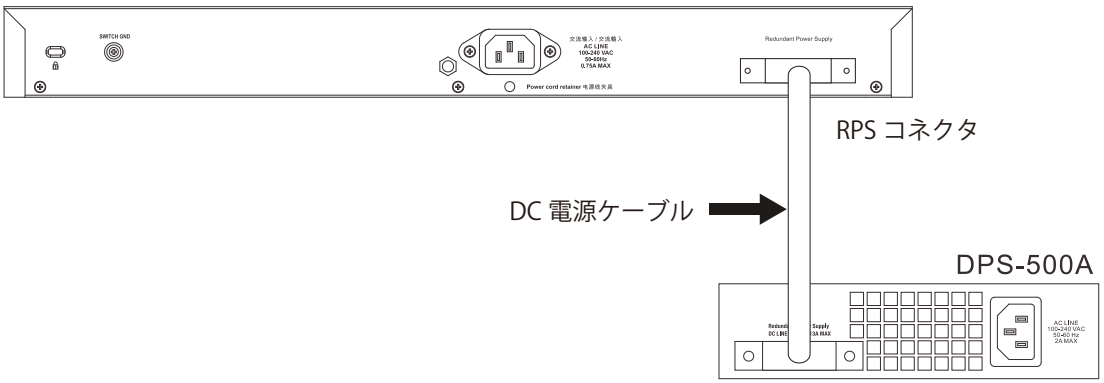


図 2-10　DGS-3630-28TC/SC と DPS-500A RPS の接続

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。

注意 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。

DPS-700

DPS-700 は DGS-3630-28PC/52PC 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。電源にはリダンダント電源同梱の AC 電源ケーブルをご使用ください。

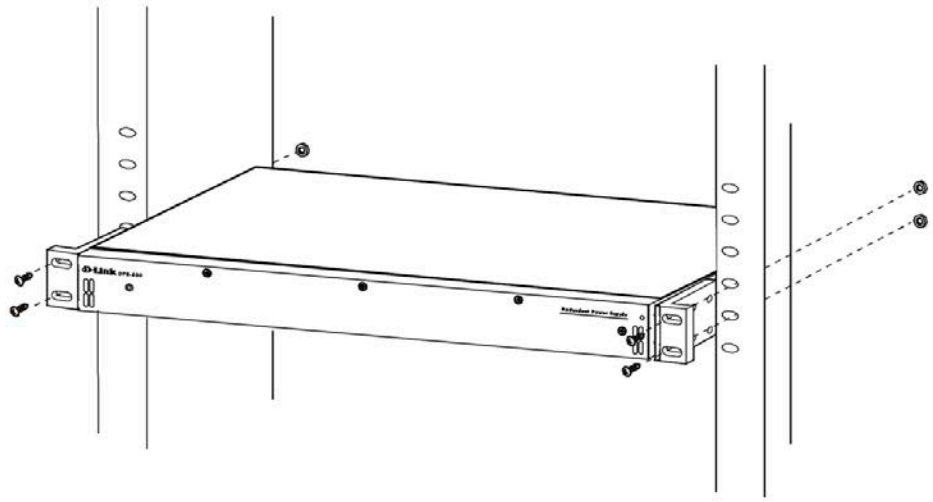


図 2-11　DPS-700 をラックに取り付ける

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。

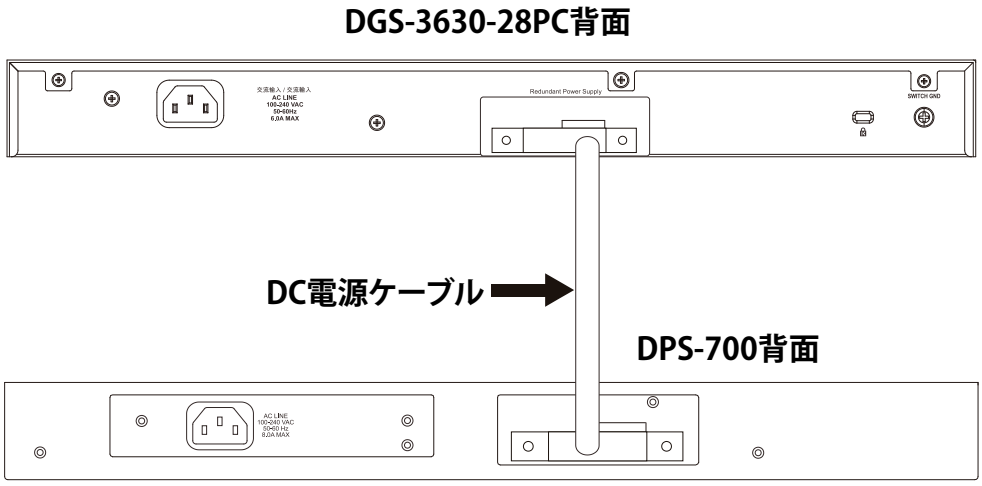


図 2-12　DPS-700 に取り付ける

注意　DGS-3630-28PC/52PC 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。

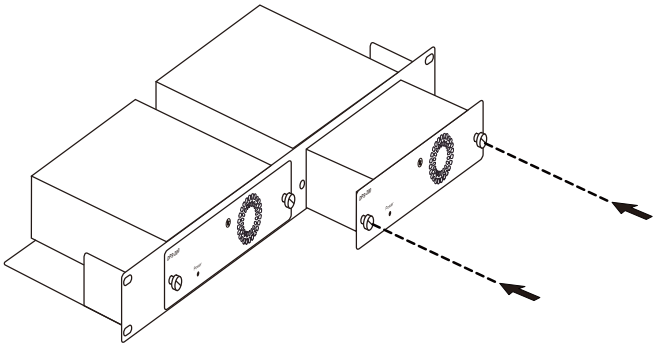


図 2-9　DPS-500A を DPS-800 に取り付ける

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。

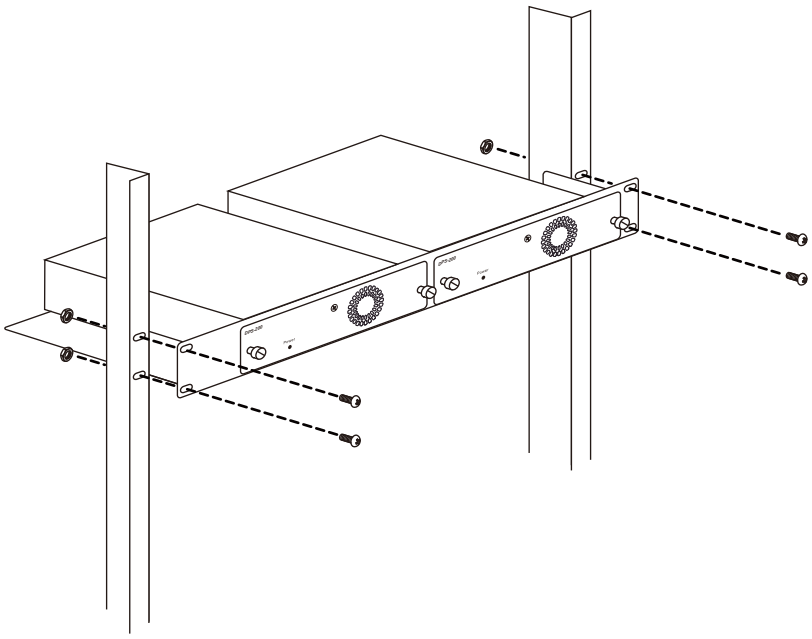


図 2-10　DPS-800 をラックに取り付ける

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。システムのリセット中、LED は点滅します。

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

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

エンドノードと接続する

「エンドノード」とは本スイッチと接続するネットワーク機器の一般的な呼称です。パソコン、ノート PC、アクセスポイント、プリントサーバ、VoIP 電話機などが該当します。各エンドノードは「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。

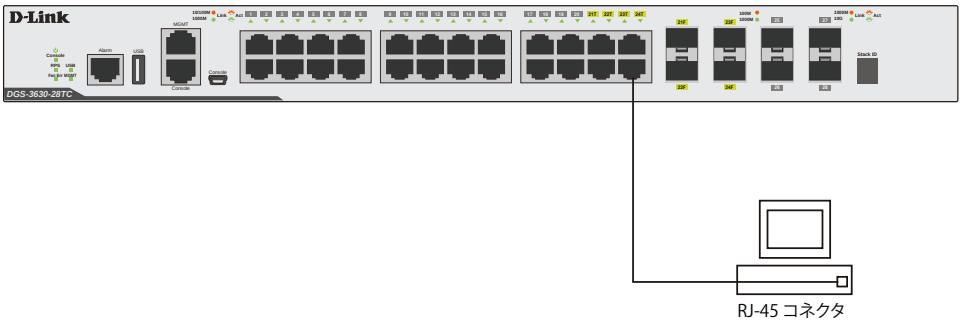


図 3-1　エンドノードと接続した図

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。

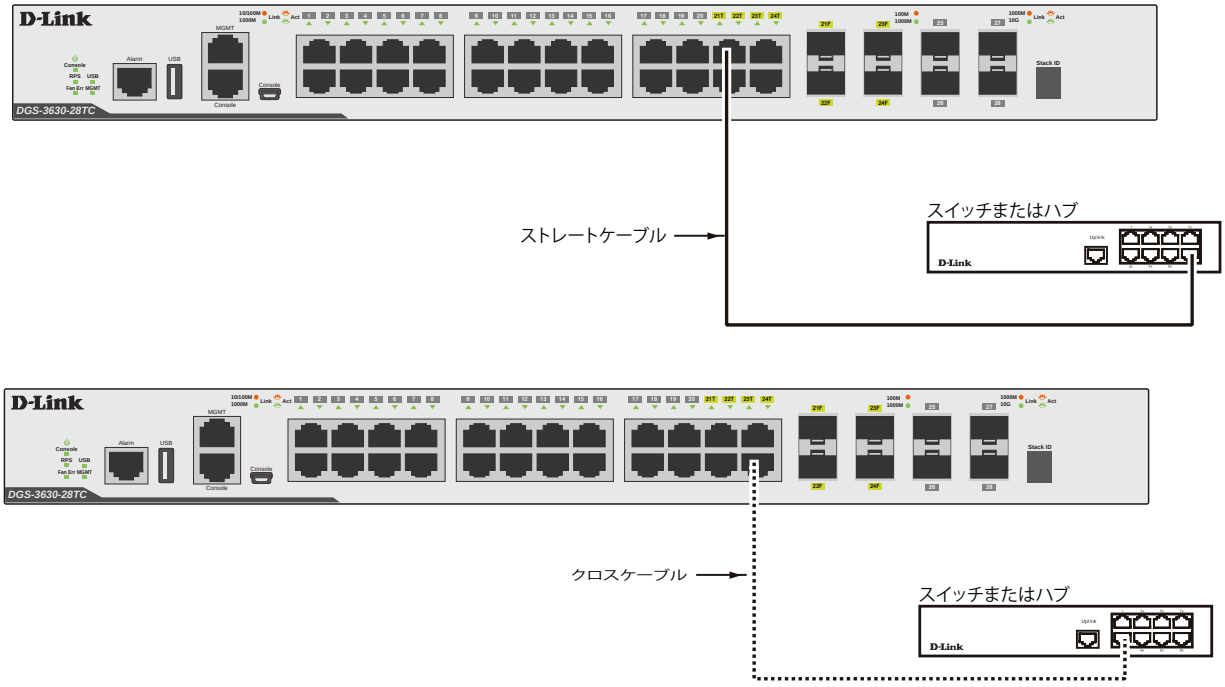


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

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

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

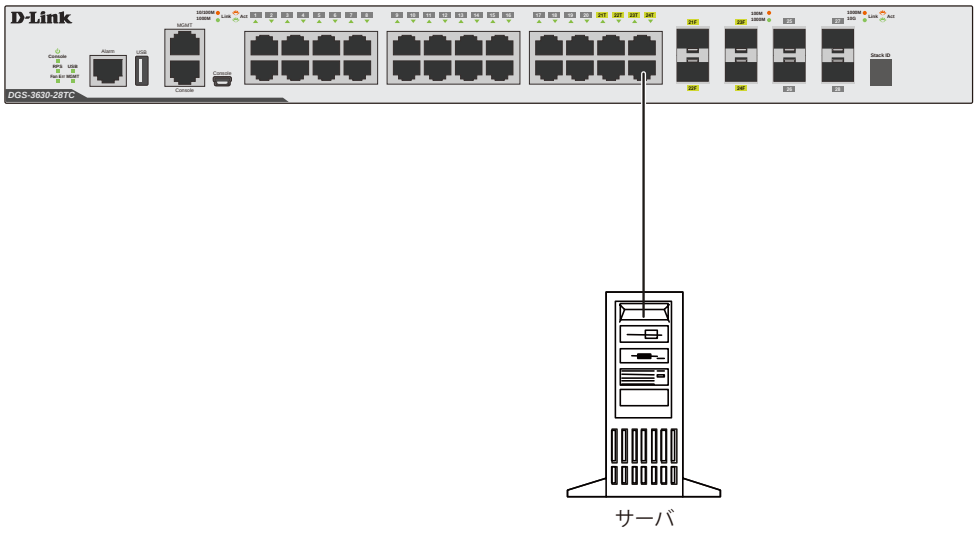


図 3-3　サーバ、PC、スイッチスタックとのアップリンク接続図

第 4 章　スイッチ管理の導入

- 管理オプション
- 端末をコンソールポートに接続する
- Mini-USB コンソールポートの接続
- スイッチへの初回接続
- パスワードの設定
- IP アドレスの割り当て
- 管理ポートへの接続
- SNMP 設定

管理オプション

本スイッチは設定、管理、そしてネットワーキングモニタを行う複数のアクセスプラットフォームを備えています。現状、以下のプラットフォームが用意されています。

- コマンドラインインタフェース管理（CLI）
  スイッチのフロントパネルにある管理ポート / コンソールポートを使用して、アウトオブバンドにて管理を行うことが可能です。他にもスイッチにあるどの LAN ポートを使用しても使える 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。

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

- Web ベースの管理インタフェース
  スイッチの Web UI には、Web ブラウザを使用して管理ポート、または RJ-45、SFP/SFP+ ポートに接続した LAN ポート経由でアクセスする事が可能です。スイッチの Web UI は HTTPS（SSL）接続を使用してアクセスする事も可能です。この管理インタフェースでは視覚的にスイッチの設定や確認を行うことが可能です。そして CLI でアクセスする事の出来るほとんどの機能に Web UI でもアクセスする事が可能です。 Web ブラウザは「Microsoft® Internet Explorer」「Mozilla® Firefox」「Google® Chrome」などが使用できます。

端末をコンソールポートに接続する

スイッチの前面パネルには RJ-45 と mini-USB のコンソールポートがあり、スイッチの設定や監視を行うリモートシステムに接続します。両ポートともスイッチとの物理接続を対応するケーブルで行います。

注意　RJ-45 と mini-USB の両ポートで同時に CLI 接続を行った場合、mini-USB 接続の方が高い優先性を持ちます。

RJ-45 コンソールポートへの接続

RJ-45 コンソールポートへの接続には次のものが必要です。

- RS-232C シリアルポートを持つターミナル、またはコンピュータとターミナルエミュレーションソフトウェア
- DB9 コネクタ（オス）と RJ-45 コネクタを持つコンソールケーブル（RJ-45/RS232C コンソールケーブル / 付属）

RJ-45 コンソールポートへの接続手順

1. 本製品付属の RS-232C ケーブルの RJ-45 コネクタをスイッチの RJ-45 コンソールポートに接続します。
2. ケーブルのもう一方を端末またはターミナルソフトが動作するコンピュータの RS-232 シリアルコネクタに接続します。以下の手順でターミナルソフトを設定します。
3. 「接続の設定」画面の「接続方法」で、適切なシリアルポート（COM1 または 2）を選択します。
4. 選択したポートの「プロパティ」画面で「115200」ビット / 秒にデータ速度を設定します。
5. 「データビット」は「8」、「ストップビット」は「1」、「パリティ」は「なし」に設定します。
6. 「フロー制御」は「なし」に設定します。
7. 「エミュレーションモード」を「VT100」に設定します。
8. 「ファンクションキー」、「方向キー」、「Ctrl キー」の使い方で「ターミナルキー」を選択します。「ターミナルキー」（Windows キーではない）の選択を確認します。
9. 端末設定の完了後、本スイッチに電源ケーブルを接続し、電源プラグをコンセントに接続します。端末でブートシーケンスが始まります。
10. ブートシーケンスが完了すると、コンソールのログイン画面が表示されます。
11. 購入後はじめてログインする場合は、ユーザ名（Username）とパスワード（Password）プロンプトで Enter キーを押します。本スイッチには、ユーザ名（Username）とパスワード（Password）の初期値はありません。はじめに、管理者によるユーザ名（Username）とパスワード（Password）の作成が必要です。既にユーザアカウントを作成している場合は、ログインし、続けて本スイッチの設定をします。

12. コマンドを入力して設定を行います。コマンドの多くは管理者レベルのアクセス権が必要です。次のセクションでユーザアカウントの設定について説明します。
13. 管理プログラムを終了する場合は、logout コマンド使用するか、ターミナルソフトを終了します。
14. 接続する端末または PC が以上の通り設定されたことを確認してください。

端末上で接続に問題が発生した場合は、ターミナルソフトの設定で「エミュレーション」が「VT-100」となっていることを確認してください。「エミュレーション」は「ハイパーターミナル」画面の「ファイル」メニューから「プロパティ」をクリックし、「設定」タブにて設定します。何も表示されない場合はスイッチの電源を切り再起動してください。

コンソールに接続すると、以下のようにコンソール画面が表示されます。この画面上でコマンドを入力し、管理機能を実行します。ユーザ名とパスワードの入力プロンプトが表示されます。初回接続時はユーザ名とパスワードは設定されていないため、「Enter」キーを 1 度押して CLI に接続します。

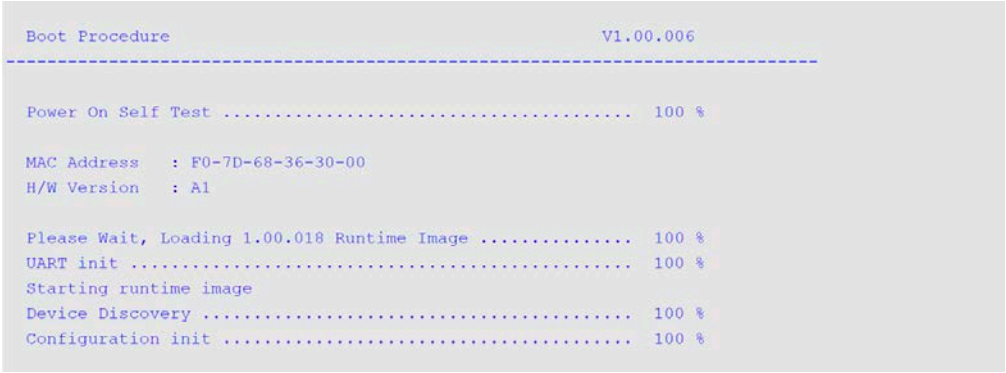


図 4-1　コンソールのブート画面

Mini-USB コンソールポートの接続

Mini-USB コンソールポートの接続には次の条件があります。

- ターミナルをエミュレートできる USB 2.0 ポートのあるターミナル、またはコンピュータ
- 5 ピンミニ B オスコネクタ /USB Type A オスコネクタのコンソールケーブル（付属）。コンソールポートとの物理的な接続に使用されます。
- ターミナルエミュレーションソフトウェアで使用される仮想 COM ポートをエミュレートするソフトウェア

Mini-USB コンソールポートとコンピュータの接続

1. コンピュータの仮想 COM ポートをエミュレートするソフトウェアをインストールします。
2. 付属のコンソールケーブルの USB Type A オスコネクタのコンピュータへの接続、5 ピンミニ B オスコネクタのスイッチのコンソールポートへの物理的な接続を行います。

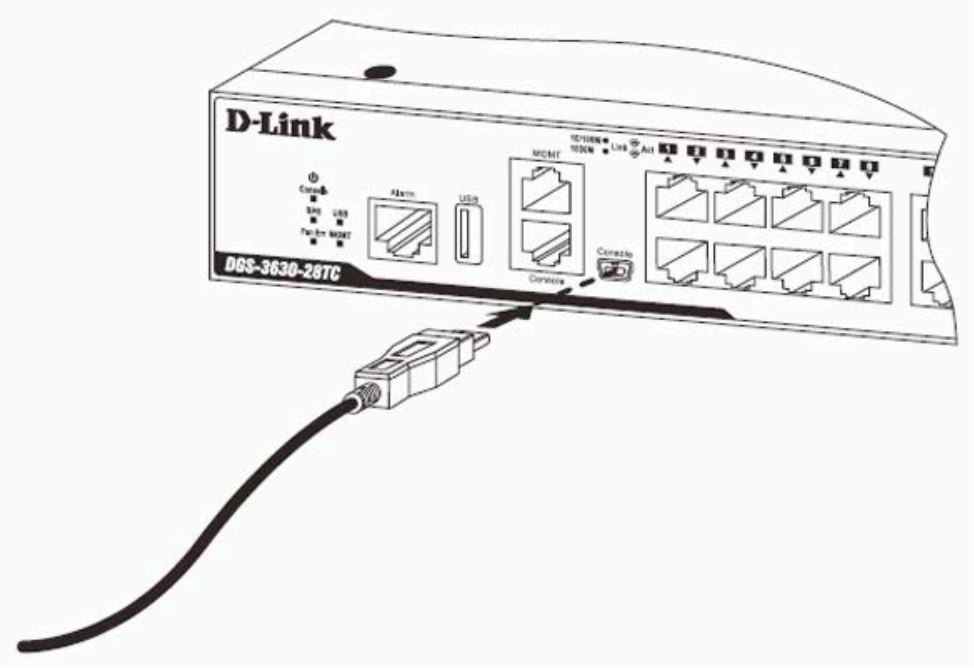


図 4-2　Mini-USB コンソールポートの接続

3. コンピュータの「デバイスマネージャ」でシリアルポート番号を確認します。仮想 COM ポートの名称は「Prolific USB-to-Serial Comm Port」です。

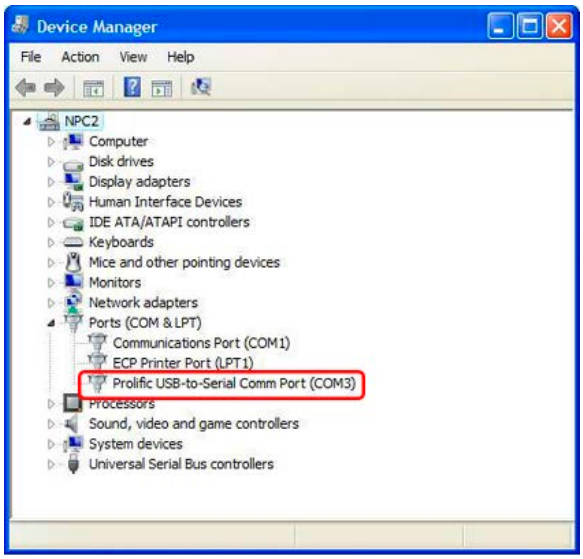


図 4-3　Device Manager

ターミナルエミュレーションソフトを次のように設定します。

- シリアルポート（COM1 または 2）を選択
- 「115200」ビット / 秒にデータ速度を設定
- 「データビット」は「8」、「ストップビット」は「1」、「パリティ」は「なし」に設定
- 「フロー制御」は「なし」に設定

コンソールに接続すると、以下のようにコンソール画面が表示されます。この画面上でコマンドを入力し、管理機能を実行します。

```
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 1.00.018 Runtime Image ..............  100 %
UART init ................................................  100 %
Starting runtime image
Device Discovery .........................................  100 %
Configuration init .......................................  100 %
```

図 4-4　コンソールのブート画面

スイッチへの初回接続

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

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

スイッチに初めて接続すると、次のログイン画面が表示されます。

```
                    DGS-3630-28PC Gigabit Ethernet Switch
                           Command Line Interface
                          Firmware: Build 2.10.B022
            Copyright(C) 2018 D-Link Corporation. All rights reserved.
Switch>
```

図 4-5　コマンドプロンプト

初回接続する場合、「Username」または「Password」は登録されていません。「Username」と「Password」には何も入力せず、「Enter」キーを押します。既に設定されている場合は、「Username」と「Password」の両方を入力します。
「Switch>」というコマンドプロンプトが表示されます。

注意 はじめにログインしたユーザが自動的に管理者権限を取得します。少なくとも一つは管理者レベルのユーザカウントを登録することをお勧めします。

アカウント作成 / パスワード設定

ログイン後、新たにユーザアカウントの作成が可能になります。本スイッチに対する不正アクセスを防ぐためには、作成するアカウントに対して必ず固有のパスワードを定義し、このパスワードは忘れないように記録しておいてください。

管理者レベルのアカウントを作成するコマンド、手順は以下の通りです。

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

図 4-6　アカウント作成コマンド画面

1.「enable」コマンドを入力することで「Privileged EXEC」モードにアクセスします。
2.「configure terminal」コマンドを入力することで「Global Configuration Mode」モードになります。
3.「username NewUser password 12345」コマンドを入力することで、ユーザ名 'NewUser' を作成し、パスワード「12345」を指定します。
4.「username NewUser privilege 15」コマンドを入力することで、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、「15」が最大、「1」が最小の権限レベルになります。
5.「line console」コマンドを入力することで「LINE Configuration」モードになります。
6.「login local」コマンドを入力することで、local line にログイン権限が必要となります。
7.「end」コマンドを入力して、「Privileged EXEC」モードを終了します。

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

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

IP アドレスの割り当て

同じネットワーク内の機器はそれぞれ固有の IP アドレスを使用する必要があります。この IP アドレスはネットワーク内の機器と通信するのに使用されます。
スイッチの IP アドレスはスイッチの Web UI にアクセスするために重要になります。スイッチの IP アドレス取得方法は以下の通りです。

このスイッチの IP アドレスは「10.90.90.90」、サブネットマスクの CIDR ノーテーションは「/8」で「255.0.0.0」に解釈されます。
これらの情報はどのようにも編集可能です。下記を参照ください。

```
Switch> enable
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 10.50.50.50 255.0.0.0
Switch(config-if)#
```

図 4-7　IP 変更コマンド画面

1.「enable」コマンドを入力することで「Privileged EXEC」モードにアクセスします。
2.「configure terminal」コマンドを入力することで「Global Configuration Mode」モードになります。
3.「interface vlan 1」コマンドを入力することで、デフォルト VLAN の「VLAN Configuration Mode」に入り、「interface vlan 1」を指定します。
4. コマンド「ip address 10.50.50.50 255.0.0.0」を入力して、IP アドレスを「10.50.50.50」、サブネットマスクを「255.0.0.0」に変更します。

管理ポートへの接続

スイッチの前面パネルには Out-of-Band（OOB）管理ポートがあります。ポートは、標準的なイーサネットケーブルを使用してノート PC に簡単に接続可能な RJ-45 ポートです。管理ポートを使ってスイッチに接続するために、Web ブラウザもしくは Telnet クライアントを使用することができます。

管理ポートを使用するためには、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ポートを接続します。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。

コンソールポート、または Web ベースのスイッチ管理インタフェースを通じて IP 設定または管理ポートのステータスを変更することができます。
管理ポートの設定を変更するためには、以下のコマンドを使用します。

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

IP 設定のステータスを参照するためには、以下のコマンドを使用します。

```
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#
```

注意　管理ポートの MAC アドレスは、「System MAC」を使用するため、「VLAN1」と重複します。

注意　VLAN インタフェースを経由して「Mgmt 0」の IP アドレス宛に通信を行うことはできません。

SNMP 設定

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

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

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

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

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

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

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

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

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

トラップ

トラップとは、スイッチ上で発生したイベントを、ネットワーク管理者に警告するためのメッセージです。イベントには、再起動（誰かが誤ってスイッチの電源を切ってしまった）などの重大なものから、ポートの状態変化を知らせるものまで幅広い種類があります。スイッチはトラップを生成して事前に設定された IP アドレスに送信します。典型的なトラップには、認証の失敗、トポロジの変化などがあります。

MIB

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

第 5 章　Web ベースのスイッチ管理

- Web ベースの管理について
- Web マネージャへのログイン
- Web マネージャの画面構成
- Web マネージャのメニュー構成

Web ベースの管理について

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

Web ベースの管理モジュールとコンソールプログラム（および Telnet）は、異なるインタフェースを経由して同じスイッチ内部のソフトウェアにアクセスし、その設定を行います。つまり、Web ベースでスイッチ管理を実行して行う設定は、コンソール接続によっても行うことができます。

Web マネージャへのログイン

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

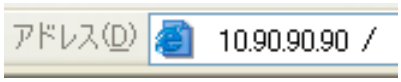


図 5-1　URL の入力

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

以下のユーザ認証画面が表示されます。

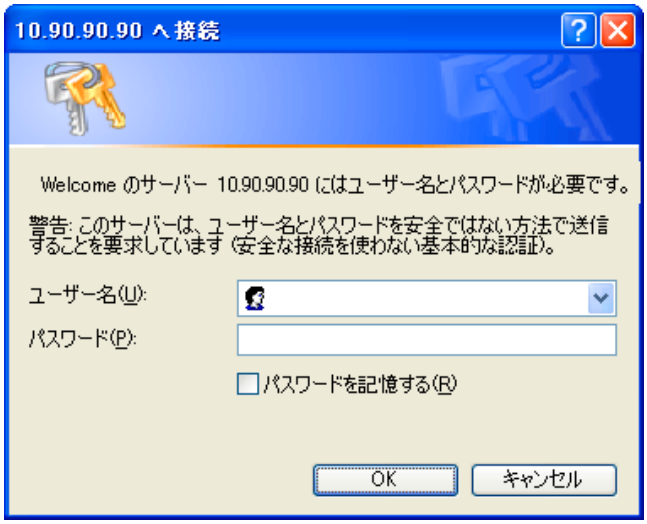


図 5-2　パスワード入力用画面

「ユーザー名」欄と「パスワード」欄を空白のまま「OK」をクリックし、Web ベースユーザインタフェースに接続します。Web ブラウザによって使用可能な機能を以下で説明します。
CLI でユーザ名、パスワードを既に設定している場合は、設定したパラメータを入力します。

注意 ユーザアカウント作成すると、Web からのアクセスには「ログイン名 / パスワード」が必要になります。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 マネージャの画面構成

Web マネージャ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 マネージャのメイン画面について

Web マネージャのメイン画面は 3 つのエリアで構成されています。

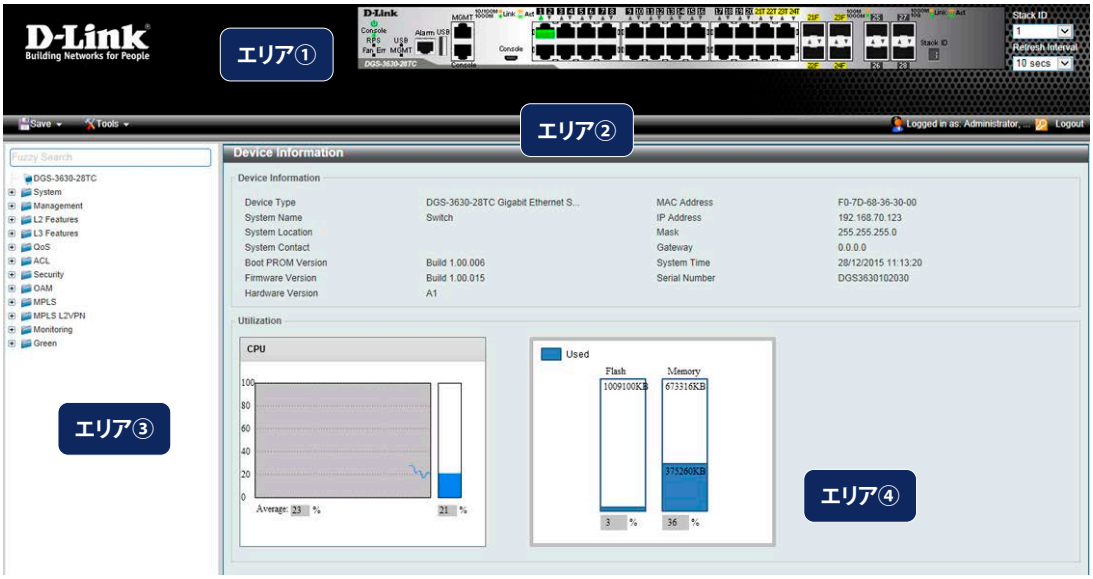


図 5-3　Web マネージャのメインページ

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、拡張モジュールが表示されます。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を表示します。表示するフォルダ、またはウインドウを選択します。フォルダを開きハイパーリンクのウィンドウをクリック、サブフォルダには上位フォルダに関連するカテゴリの詳細情報や設定項目が表示されます。
エリア④	選択したスイッチ情報の表示と設定を行うことができます。

注意　「ASCII」文字のみサポートします。

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

Web マネージャのメニュー構成

Web マネージャで本スイッチに接続し、ログイン画面でユーザ名とパスワードを入力して本スイッチの管理モードにアクセスします。
Web マネージャで設定可能な機能を次に説明します。

メインメニュー	サブメニュー	説明
System	Device Information（デバイス情報）	スイッチの主な設定情報を表示します。
	System Information Settings（システム情報設定 ）	スイッチの基本情報を表示します。
	Peripheral Settings（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。
	Interface Description（インタフェース概要）	スイッチの各ポートの概要、管理ステータスなどについて表示します。
	Loopback Test（ループバックテスト）	物理ポートインタフェースのループバック設定とループバックテストを行います。
	PoE（PoE の管理）（DGS-3630-28PC/52PC）	DGS-3630-28PC/52PC 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）	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。
	Time and SNTP（時刻設定）	スイッチに時刻を設定します。
	Time Range（タイムレンジ設定）	スイッチのタイムレンジを設定します。アクセスプロファイル機能を実行する期間を決定します。
	PTP（PTP 設定）	PTP（Precision Time Protocol : 高精度時刻同期方式）システムは、イーサネットネットワークを通して時刻を同期します。
	USB Console Settings（USB コンソール設定）	USB コンソールの設定、表示を行います。
	SRM（Switch Resource Management 設定）	「Switch Resource Management」（SRM）により大規模なリソースを最適化します。
Management	Command Logging（コマンドログ設定）	コマンドログ設定を有効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
	User Accounts Settings（ユーザアカウント設定）	スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。
	CLI Alias Settings（CLI エイリアス設定）	CLI エイリアスの設定を行います。
	Password Encryption（パスワード暗号化）	パスワードを暗号化し設定ファイルに保存します。
	Password Recovery（パスワードリカバリ）	パスワードリカバリを行います。例えば管理者がパスワードを忘れた場合に有効です。
	Login Method（ログイン方法）	各管理インタフェースでのログイン方法について設定します。
	SNMP（SNMP 設定）	SNMP 設定を有効にします。本スイッチシリーズは、SNMP v1、v2c、および v3 をサポートしています。
	RMON（RMON 設定）	SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効にします。
	Telnet/Web（Telnet/Web 設定）	スイッチに Telnet/Web 設定を有効にします。
	Session Timeout（セッションタイムアウト）	各セッション（Web やコンソールなど）のタイムアウトの設定をします。
	DHCP（DHCP 設定）	スイッチの DHCP について設定します。
	DHCP Auto Configuration（DHCP 自動コンフィグ設定）	DHCP 自動コンフィグ機能の設定を行います。
	DHCP Auto Image Settings（DHCP 自動イメージ設定）	DHCP 自動イメージ設定を行います。スタートアップ時に、外部サーバからイメージファイルを取得する機能です。
	DNS（ドメインネームシステム）	DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。
	NTP（ネットワークタイムプロトコル）	スイッチの時刻を同期するための NTP プロトコルの設定を行います。
	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）	フラッシュファイルシステムにより、Firmware、Config 情報、および Syslog 情報はフラッシュ内のファイルに保存されます。
	Stacking（スタッキング設定）	物理スタッキングの設定を行います。
	Virtual Stacking（SIM）（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。
	NLB FDB Settings（NLB FDB 設定）	ネットワークロードバランシング (NLB) の設定を行います。
	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。

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) の表示、設定を行います。 ERPS はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。
	Loopback Detection （ループバック検知設定）	ループバック検知（LBD）機能の設定を行います。
	Link Aggregation （リンクアグリゲーション）	Link Aggregation（リンクアグリゲーション / ポートトランキング機能）の設定を行います。
	MLAG	MLAG（Multi-Chassis Link Aggregation Group）の設定を行います。
	Flex Links（フレックスリンクス）	フレックスリンクス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 Contro（l 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 として知られている ARP 通知は、TAP と SPA が等しい場合、それを送信したホストに有効である SHA と SPA を含むパケット（通常 ARP リクエスト）です
	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 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 Static Route BFD （IPv4 スタティックルート BFD）	IPv4 スタティックルート BFD（Bidirectional Forwarding Detection）の設定を行います。
	IPv4 Route Table（IPv4 ルートテーブル）	IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。
	IPv6 Static/Default Route （IPv6 スタティック / デフォルトルート設定）	IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。
	IPv6 Static Route BFD （IPv6 スタティックルート BFD）	IPv6 スタティックルート BFD（Bidirectional Forwarding Detection）の設定を行います。
	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。小さい優先度値を持つルートほど高いプライオリティを持ちます。
	ECMP Settings（ECMP 設定）（EI/MI モードのみ）	ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。
	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。
	IP Tunnel Settings（IP トンネル設定）	IP トンネルを設定します。
	URPF Settings（URPF 設定）	「Unicast Reverse Path Forwarding」(URPF) の設定と表示を行います。
	VRF（Virtual Routing and Forwarding） （EI/MI モードのみ）	「Virtual Routing and Forwarding」(VRF) 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）をサポートしています。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）（EI/MI モードのみ）	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。
	BGP（Border Gateway Protocol） （EI/MI モードのみ）	BGP（Border Gateway Protocol）をサポートしています。これは AS（自律システム）内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブルを保持するレイヤ 3 ユニキャストルーティングプロトコルです。
	BFD（Bidirectional Forwarding Detection）	Bidirectional Forwarding Detection (BFD) の設定を行います。

メインメニュー	サブメニュー	説明
L3 Features	ISIS（Intermediate System to Intermediate System）（MI モードのみ）	Intermediate System to Intermediate System (ISIS) の設定を行います。
	IP Route Filter（IP ルートフィルタ）	IP プレフィックスリスト、ルートマップの作成、またはルートマップへのシーケンスの追加、およびシーケンスの削除を行います。
	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。
	QoS PFC	ネットワーク「Quality of Service」(QoS) プライオリティベースフローコントロール (PFC) クラスマップの設定を行います。
	WRED（WRED 設定）	WRED（WRED 設定）の設定を行います。
	iSCSI（ アイスカジー）	iSCSI の設定を行います。
ACL	ACL Configuration Wizard（ACL 設定ウィザード）	ACL 設定ウィザードは、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 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 の設定を行います。
	TACACS+（TACACS+ 設定）	TACACS+ の設定を行います。
	IMPB（IP-MAC-Port Binding/IP-MAC- ポートバインディング）	IP-MAC バインディングにより、スイッチにアクセスするユーザ数を制限します。
	DHCP Server Screening（DHCP サーバスクリーニング設定）	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
	ARP Spoofing Prevention（ARP スプーフィング防止設定）	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスとマッチしなかった 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。
	NetBIOS Filtering（NetBIOS フィルタリング設定）	NetBIOS フィルタリングの設定を行います。
	MAC Authentication（MAC 認証）	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
	Web-based Access Control（Web 認証）	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認証する機能です。
	Network Access Authentication（ネットワークアクセス認証）	Network Access Authentication（ネットワークアクセス認証）の設定を行います。
	Safeguard Engine（セーフガードエンジン）	セーフガードエンジンは、攻撃中にスイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。
	Trusted Host（トラストホスト）	トラストホストの設定を行います。
	Traffic Segmentation 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。
	Zone Defense Settings（ゾーンディフェンス設定）	「ゾーンディフェンス（Zone Defense）」機能の設定と表示を行います。

メインメニュー	サブメニュー	説明
Security	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）	本項目では「Secure File Transfer Protocol」(SFTP) サーバの設定、表示を行います。
	SFTP Client Settings（SFTP クライアント設定）	本項目では「Secure File Transfer Protocol」(SFTP) クライアントの設定、表示を行います。
	Network Protocol Port Protect Settings	ネットワークプロトコルポート保護設定を行います。
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）機能を実行します。スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定（アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx（送信）電力しきい値設定、および Rx（受信）電力しきい値設定）を行うことができます。
MPLS（MI モードのみ）	MPLS LDP Information Settings（MPLS LDP 情報設定）	「Multiprotocol Label Switching」(MPLS) の「Label Distribution Protocol」(LDP) 情報の設定を行います。
	MPLS LSP Trigger Information（MPLS LSP トリガ情報）	「Multiprotocol Label Switching」(MPLS) の「Label-Switched Label-Switched Path」(LSP) トリガ情報の設定を行います
	MPLS Forwarding Settings（MPLS フォワーディング設定）	MPLS フォワーディングの設定を行います。
	MPLS LDP Neighbor Password Settings（MPLS LDP ネイバパスワード設定）	MPLS LDP ネイバパスワードの設定を行います。
	MPLS LDP Neighbor Targeted Settings（MPLS LDP ネイバターゲット設定）	MPLS LDP ネイバターゲットの設定を行います。
	MPLS LDP Neighbor Information（MPLS LDP ネイバ情報）	MPLS LDP Neighbor Information（MPLS LDP ネイバ情報）の表示をします。
	MPLS Global Settings（MPLS グローバル設定）	MPLS Global Settings（MPLS グローバル設定）の設定を行います。
	MPLS LDP Interface Settings（MPLS LDP インタフェース設定）	MPLS LDP Interface Settings（MPLS LDP インタフェース設定）の設定をします。
	MPLS LDP Session Information（MPLS LDP セッション情報）	MPLS LDP Session Information（MPLS LDP セッション情報）の検出、表示をします。
	MPLS LDP Statistic（MPLS LDP スタティスティック）	MPLS LDP Statistic（MPLS LDP スタティスティック）の表示をします。
	MPLS LDP Binding Table（MPLS LDP バインディングテーブル）	MPLS LDP Binding Table（MPLS LDP バインディングテーブル）の表示をします。
	MPLS LDP Discovery Information（MPLS LDP ディスカバリ情報）	MPLS LDP Discovery Information（MPLS LDP ディスカバリ情報）の表示をします。
	MPLS QoS Settings（MPLS QoS 設定）	MPLS QoS Settings（MPLS QoS 設定）の設定、表示をします。
	Ping MPLS	指定 FEC の LSP の接続状態を確認します。
	Traceroute MPLS IPv4（トレースルート MPLS IPv4）	指定 FEC の LSP パストレースのような「hop-by-hop fault localization」を指定します。
MPLS L2VPN（MI モードのみ）	VPWS Settings（VPWS 設定）	「Virtual Private Wire Service」(VPWS) を設定を行います。
	L2VC Interface Description（L2VC インタフェース概要）	L2VC Interface Description（L2VC インタフェース概要）を設定を行います。
	VPLS Settings（VPLS 設定）	「Virtual Private LAN Service」(VPLS) を設定を行います。
	VPLS MAC Address Table（VPLS MAC アドレステーブル）	「VPLS MAC Address Table」（VPLS MAC アドレステーブル）を表示を行います。

メインメニュー	サブメニュー	説明
Monitoring	VLAN Counter（VLAN カウンタ）	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを指定します。
	Utilization（利用分析）	スイッチの Utilization（利用分析）を表示します。
	Statistics（統計情報）	スイッチの Statistics（統計情報）を表示します。
	Mirror Settings（ミラー設定）	ミラーリング機能の設定を行います。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、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）があります。
	sFlow（sFlow 設定）	sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。
	Device Environment（機器環境確認）	Device Environment（機器環境確認）ではスイッチの内部の温度状態を表示します。
	External Alarm Settings （外部アラーム設定）	外部アラーム設定はアラーム起動時のアラームメッセージについて設定します。
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。
OpenFlow	OpenFlow Settings（OpenFlow 設定）	OpenFlow の設定を行います。
Save	Save Configuration （コンフィグレーションの保存）	「Save Configuration」ではスイッチのコンフィグレーションを保存します。
Tools	Firmware Upgrade & Backup （ファームウェアアップグレード＆バックアップ）	様々なプロトコルを使用してファームウェアアップグレード / バックアップを実行します。
	Configuration Restore & Backup （コンフィグレーションリストア＆バックアップ）	様々なプロトコルを使用してコンフィグレーションリストア / バックアップを実行します。
	Certificate & Key Restore & Backup （証明書 / 鍵リストア＆バックアップ）	様々なプロトコルを使用して証明書と鍵のリストア / バックアップを実行します。
	Log Backup （ログファイルのバックアップ）	様々なプロトコルを使用してログファイルのバックアップを実行します。
	Ping	「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。
	Trace Route（トレースルート）	パケットの経路をスイッチに到着する前に遡ってトレースすることができます。
	Reset（リセット）	スイッチの設定内容を工場出荷時状態に戻します。
	Reboot System（システム再起動）	スイッチの再起動を行います。
	DLMS Settings（DLMS 設定）	「D-Link License Management System」(DLMS) の設定、表示を行います。

第 6 章　System（スイッチの主な設定）

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

サブメニュー	説明
Device Information（デバイス情報）	スイッチの主な設定情報を表示します。
System Information Settings（システム情報設定 ）	スイッチの基本情報を表示します。
Peripheral Settings（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。
Interface Description（インタフェース概要）	スイッチの各ポートの概要、管理ステータスなどについて表示します。
Loopback Test（ループバックテスト）	物理ポートインタフェースのループバック設定とループバックテストを行います。
PoE（PoE の管理）（DGS-3630-28PC/52PC）	PoE 機能の設定、表示を行います。（DGS-3630-28PC/52PC のみ）
System Log（ システムログ構成）	スイッチのフラッシュメモリにスイッチログを保存する方法を選択します。
Time and SNTP（時刻設定）	スイッチに時刻を設定します。
Time Range（タイムレンジ設定）	スイッチのタイムレンジを設定します。アクセスプロファイル機能を実行する期間を決定します。
PTP（PTP 設定）	PTP（Precision Time Protocol：高精度時刻同期方式）システムは、イーサネットネットワークを通して時刻を同期します。
USB Console Settings（USB コンソール設定）	USB コンソールの設定、表示を行います。
SRM（Switch Resource Management 設定）	「Switch Resource Management」（SRM）により大規模なリソースを最適化します。

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「DGS-3630 シリーズ」フォルダをクリックします。本画面には、スイッチの「MAC Address」（工場による設定のため変更不可）、「Boot PROM Version」と「Firmware Version」、「Hardware Version」などが表示されます。これらの情報は、PROM やファームウェアの更新状況の把握や他のネットワークデバイスのアドレステーブルにスイッチの MAC アドレスを登録する際の確認などに便利です。

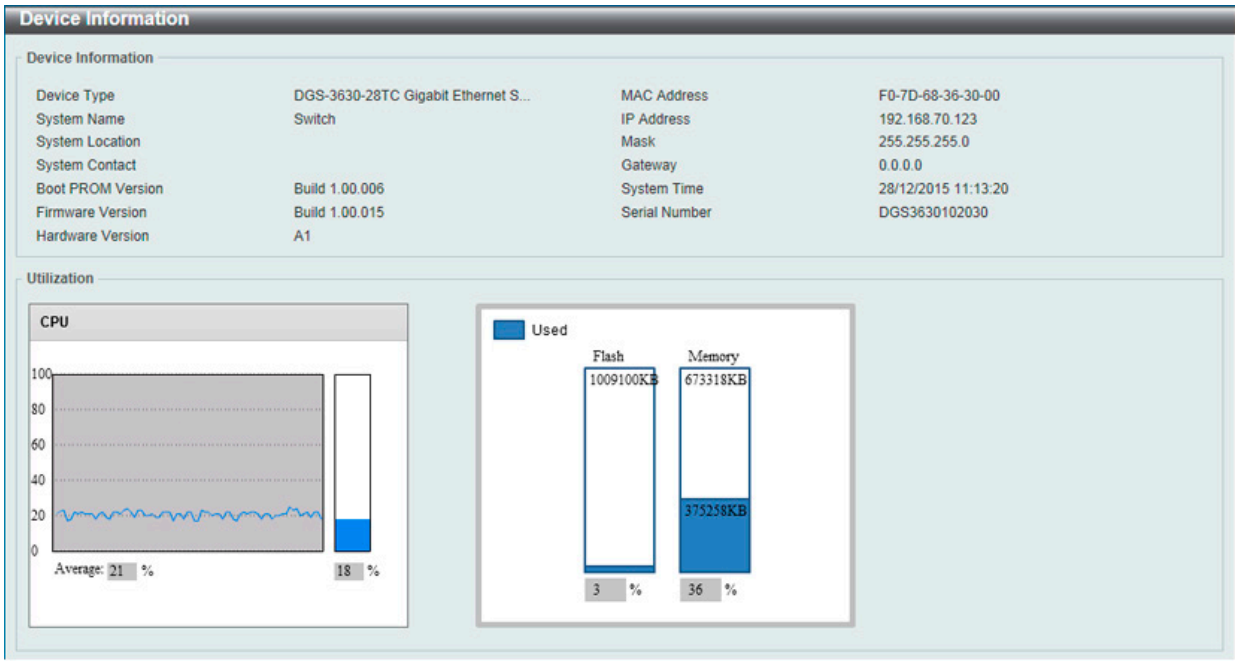


図 6-1　Device Information 画面

画面には以下の項目があります。

項目	説明
Device Information	
Device Type	工場にて定義した機種名と型式を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。（半角英数字 160 文字以内）
System Contact	担当者名を表示します。（半角英数字 31 文字以内）
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	最後のデバイスリセットからの経過時間を表示します。
Utilization	
CPU	CPU の使用率を表示します。
Flash	Flash の使用率を表示します。
Memory	Memory の使用率を表示します。

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

ここでは、スイッチの詳細情報を表示します。本画面の「System Information Settings」で「System Name」、「System Location」、「System Contact」などを入力し、スイッチの定義を行う際にも利用できます。また「Mangement Interface」で管理インタフェースの設定を行います。

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

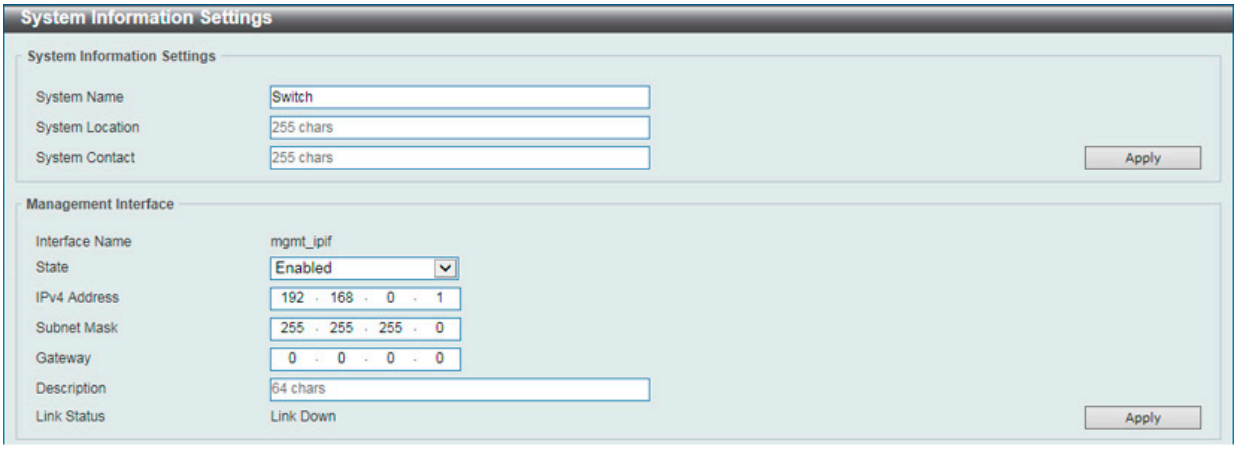


図 6-2　System Information Settings 画面

画面には次の項目があります。

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。（半角英数字 160 文字以内）
System Contact	スイッチの管理者情報を入力します。
Mangement Interface	
State	管理インタフェースの有効 / 無効を指定します。
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概要を指定します。（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 の順にクリックし、以下の画面を表示します。

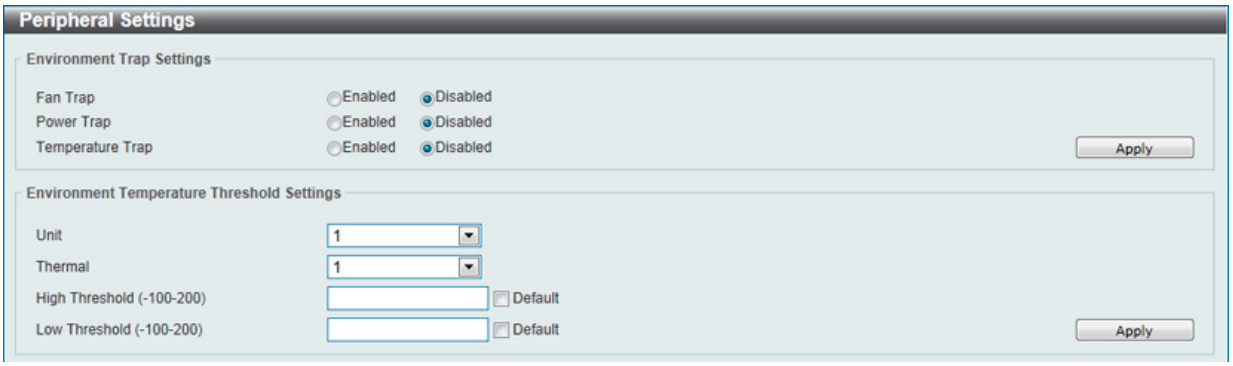


図 6-3　Peripheral Settings 画面

画面には以下の項目があります。

項目	説明
Environment Trap Settings	
Fan Trap	プルダウンメニューを使用して、ファン警告設定のトラップを有効 / 無効に設定します。
Power Trap	プルダウンメニューを使用して、電源警告設定のトラップを有効 / 無効に設定します。
Temperature Trap	プルダウンメニューを使用して、温度警告設定のトラップを有効 / 無効に設定します。

項目	説明
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。-100℃から 200℃の間で指定できます。「Default」をチェックす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。-100℃から 200℃の間で指定できます。「Default」をチェックすると初期値に戻ります。

「Apply」ボタンをクリックすると設定が更新されます。

Port Configuration（ポート設定）

各ポートの設定を行います。

Port Settings（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。「State」、「Speed/Duplex」、「Flow Control」、「Address Learning」、「Media Type」、および「MDIX」を含むさまざまなポート設定をスイッチに行うことができます。

注意 「10M」と「100M」は管理ポート（Mgmt 0）でのみ有効です。

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

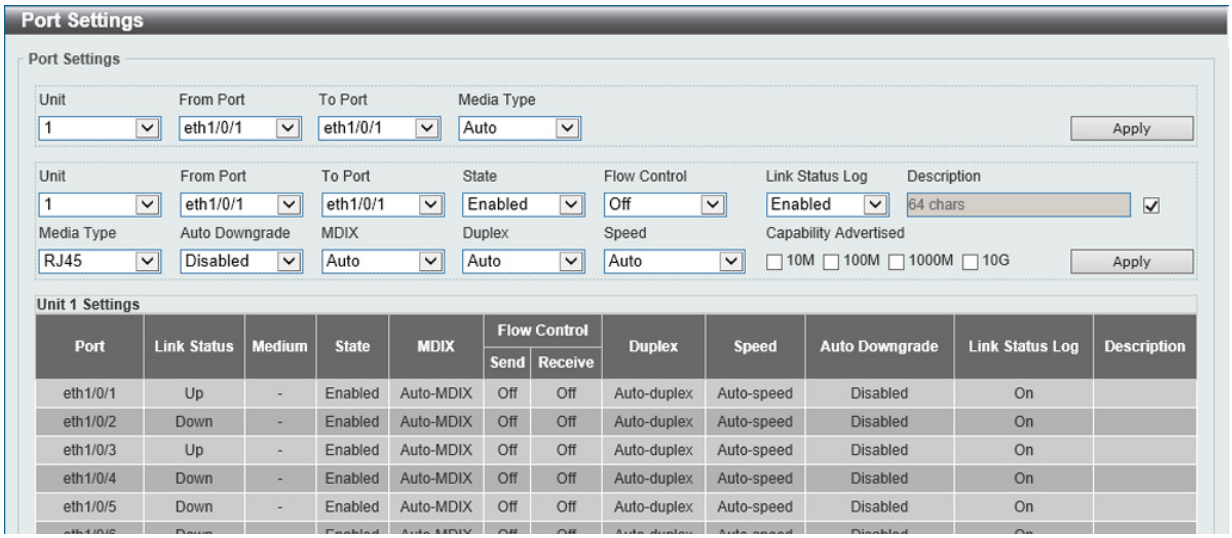


図 6-4　Port Settings 画面

画面には以下の項目があります。

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設定します。
Media Type	ポートメディアタイプを「Auto」「RJ45」「SFP」から選択します。SFP オプションは SFP+ を使用する 10G 接続も含まれます。
State	物理ポートの有効 / 無効を指定します。 • Enabled - 選択した物理ポートが有効です。 • Disabled - 選択した物理ポートが無効です。
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による制御を行います。「Auto」は自動的にいずれかを使用します。物理スタックのスイッチはサポートしていません。
Link Status Log	リンクステータスのログ機能を有効 / 無効にします。
Description	当該のポートについて 64 文字以内に概要を指定します。
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 / 無効にします。
MDIX	• Auto - 最適なケーブル接続を自動的に設定します。 • Normal - ケーブル接続に Normal を選択します。 • Cross - ケーブル接続に Cross を選択します。 「Normal」を選択すると、MDI モードにあるポートはストレートケーブルを通して PC のネットワークボード、またはクロスケーブルで別のスイッチのポート（MDI モード）に接続することができます。「Cross」を選択すると、MDIX モードにあるポートはストレートケーブルで別のスイッチのポート (MDI モード) に接続することができます。
Duplex	Duplex モードの選択を行います。「Auto」「Full」から選択します。半二重モードはサポートされていません。

項目	説明
Speed	「Speed」欄でポートの速度を選択します。ここでは指定したポートを指定した速度のみで接続するように手動で設定します。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 オプションには「Auto」「10M」「100M」「1000M」「1000M Master」「1000M Slave」「10G」「10G Master」および「10G Slave」があります。「Auto」以外のオプションのポート設定は固定となります。 マスタ設定 (1000M Master) によりポートはデュプレックス、さらに 2 つの接続している物理レイヤ間のマスタおよびスレーブを決定します。この関係は 2 つの物理レイヤ間のタイミングコントロール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設定されます。 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。その他の設定は両ポートのリンクダウンを引き起こします。 Auto - カッパーポートの設定を行います。オートネゴシエーションが開始され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が開始され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。10Mbps 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、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、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、送受信のタイミングについての動作を制御します。10Gbps 光ファイバ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、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、オートネゴシエーションの間、本機能は有効になります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Refresh」ボタンをクリックして、本画面を更新します。

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 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 10G ポートでの auto-downgrade はサポートされません。

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。

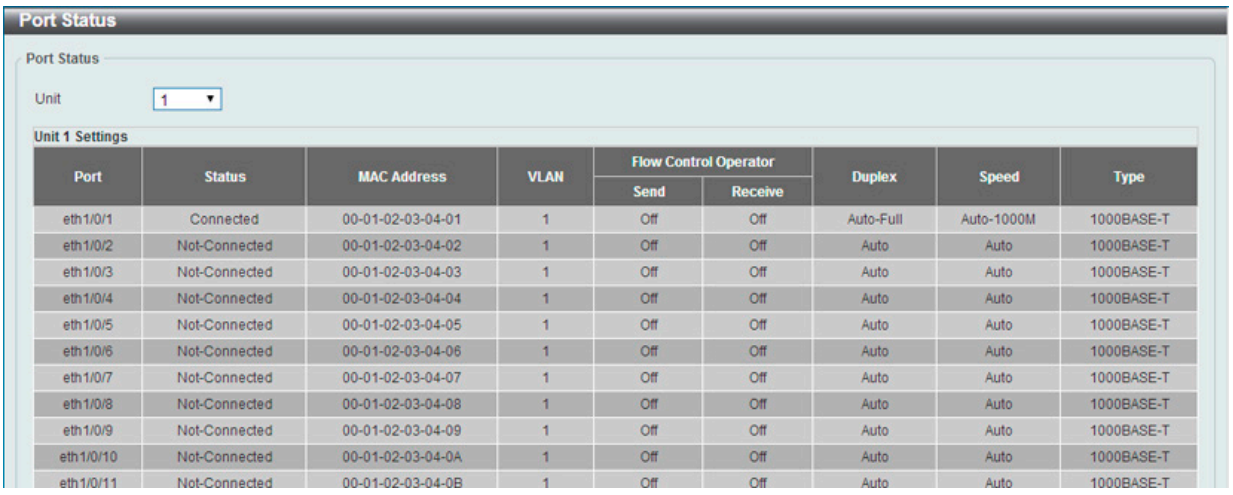


図 6-5　Port Status 画面

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。

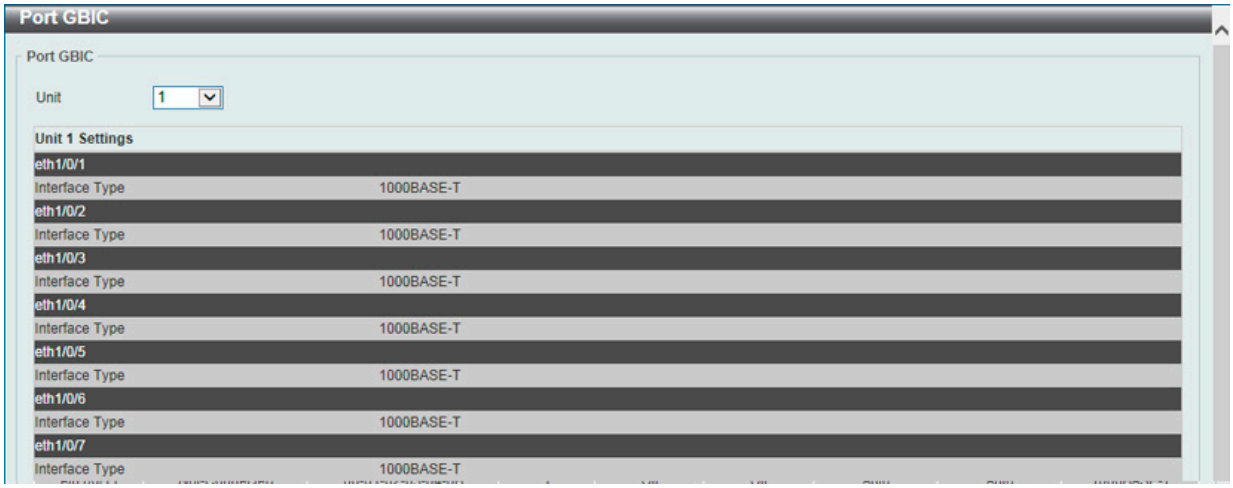


図 6-6　Port GBIC 画面

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）

以下の画面では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。

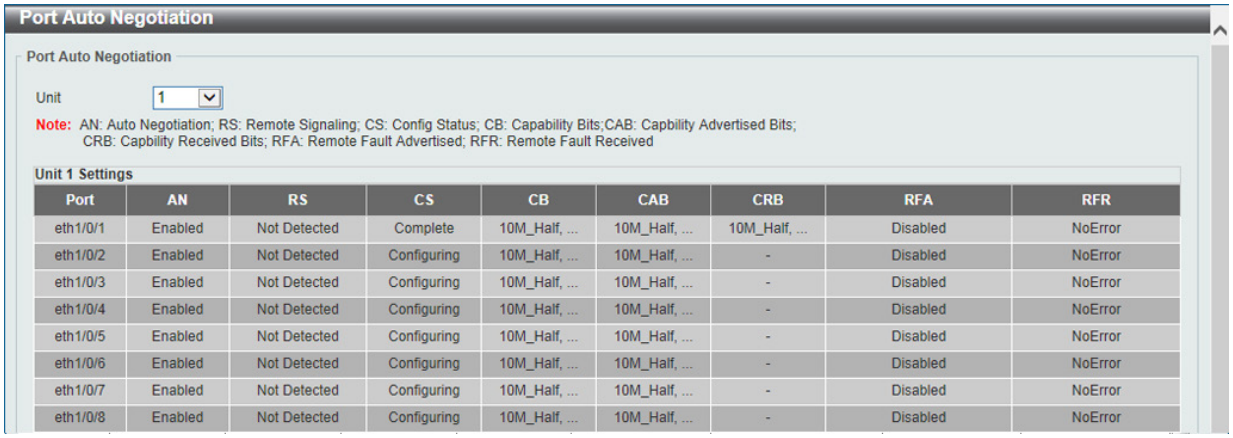


図 6-7　Port Auto Negotiation Information 画面

Error Disable Settings（エラーによるポートの無効）

以下の画面では、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で、スイッチが切断したポートに関する情報を表示します。

この画面を参照するためには、**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。

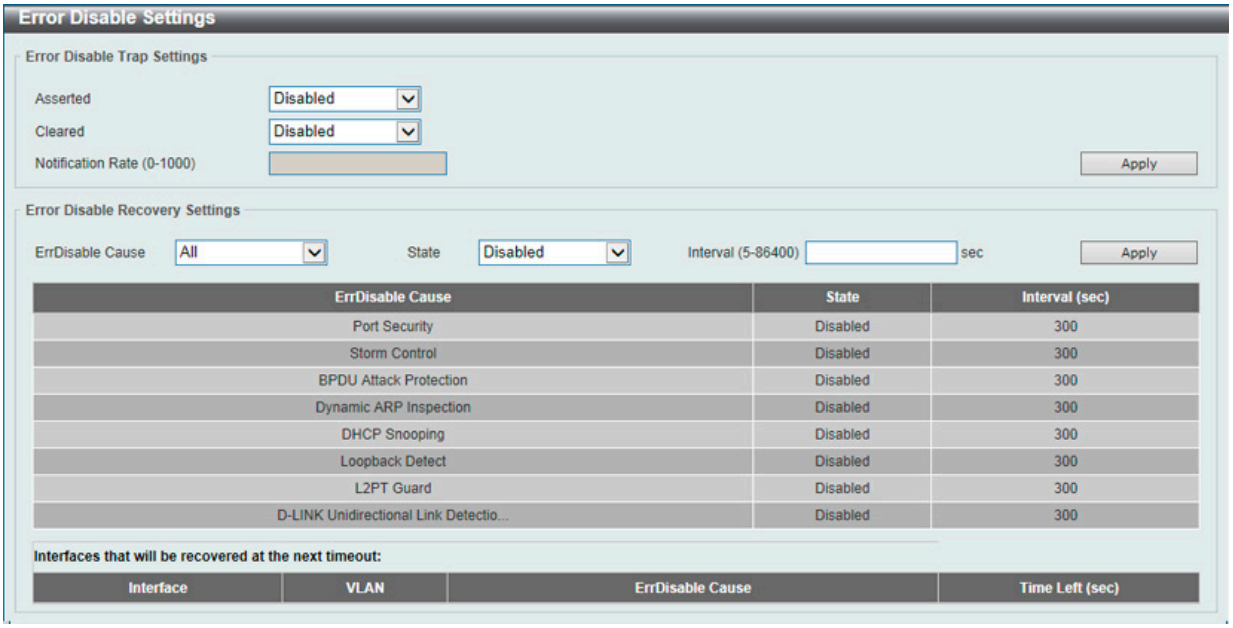


図 6-8　Port Error Disabled 画面

画面には以下の項目があります。

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、通知送信の有効 / 無効を指定します。
Cleared	エラー無効状態から回復したとき、通知送信の有効 / 無効を指定します。
Notification Rate	1 分あたりのトラップ数を入力します。指定したしきい値超えたパケットは破棄されます。0 から 1000 までの間で指定できます。

「Apply」ボタンをクリックすると設定が更新されます。

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次から選択します。 「All」「Port Security」「Storm Control」「BPDU Attack Protection」「Dynamic ARP Inspection」「DHCP Snooping」「Loopback Detect」「L2PT Guard」「DULD」
State	指定した原因によるエラー無効ポートの自動リカバリ機能を有効 / 無効にします。
Interval	ポートリカバリ実行の間隔時間を 5 から 86400（秒）で指定します。

「Apply」ボタンをクリックすると設定が更新されます。

Jumbo Frame（ジャンボフレームの有効化）

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 12288 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。

ここでは、スイッチでジャンボフレームを扱うことを可能にします。これによりオーバヘッド、処理時間、割り込みを確実に減らすことができます。

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

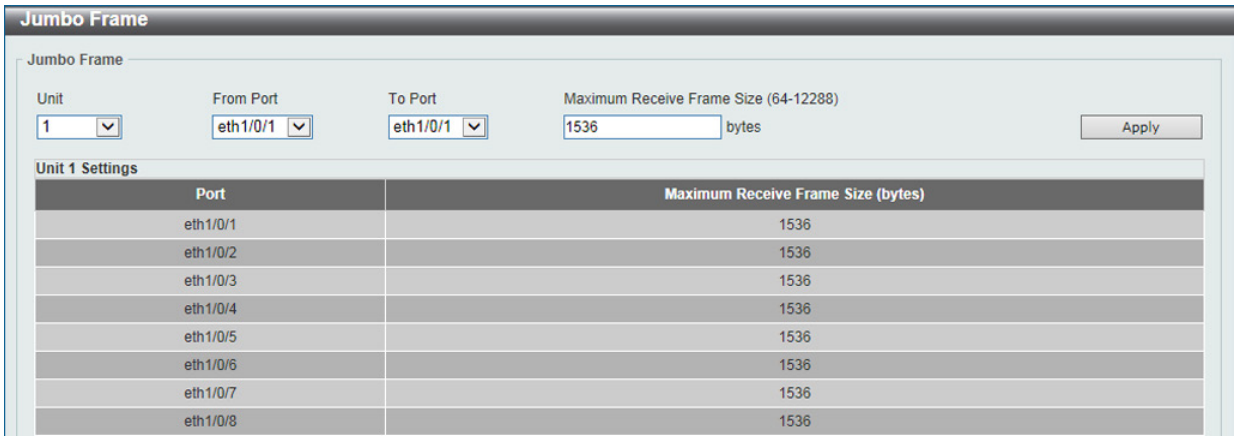


図 6-9　Jumbo Frame Settings 画面

画面には以下の項目があります。

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設定します。
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。 64 から 12288（バイト）まで指定可能で、初期値は 1536 バイトです。

「Apply」ボタンをクリックすると設定が更新されます。

Interface Description（インタフェース概要）

スイッチの各ポートの概要、管理ステータスなどについて表示します。

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

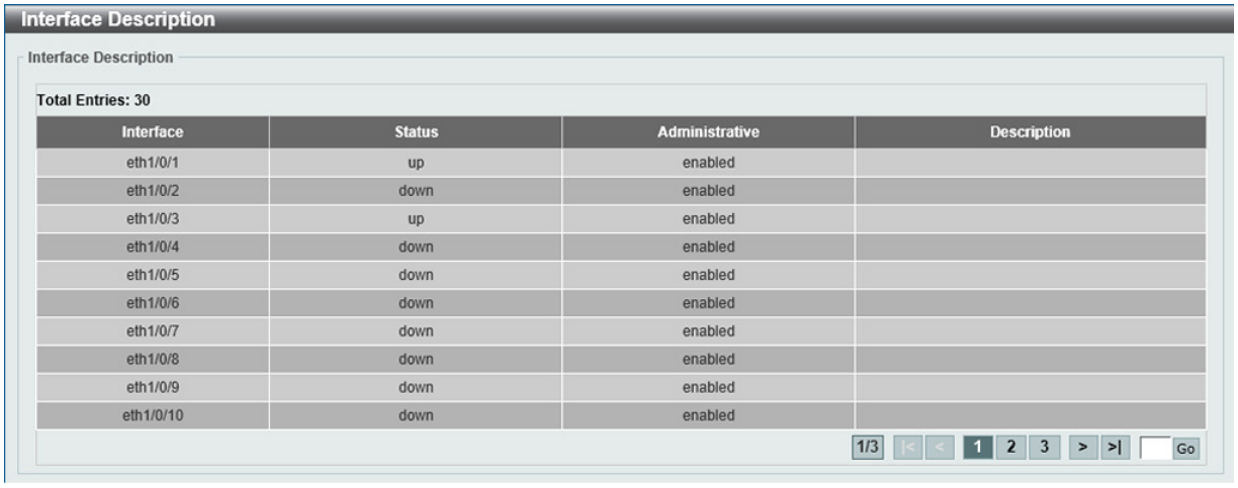


図 6-10　Interface Description 画面

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。

Loopback Test（ループバックテスト）

物理ポートインタフェースのループバック設定とループバックテストを行います。

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

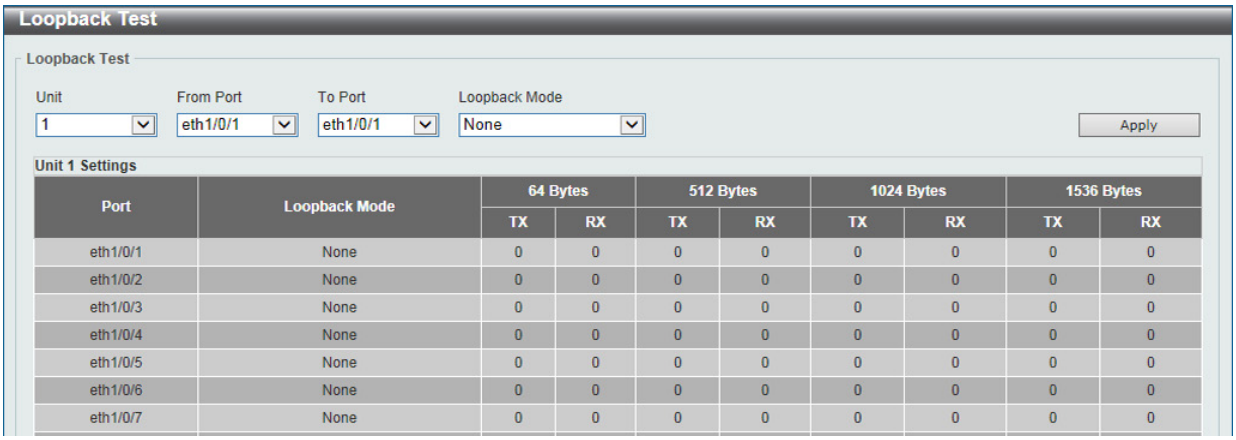


図 6-11　Loopback Test 画面

画面には以下の項目があります。

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設定します。
Loopback Mode	ループバックモードを指定します。 • None - ループバックモードを有効にしません。 • Internal MAC - インターナルループバックモードを MAC レイヤで指定します。 • Internal PHY Default - インターナルループバックモードを PHY レイヤで指定し初期メディアのテストをします。 • Internal PHY Copper - インターナルループバックモードを PHY レイヤで指定しカッパーメディアのテストをします。 • Internal PHY Fiber - インターナルループバックモードを PHY レイヤで指定し光ファイバメディアのテストをします。 • External MAC - エクスターナルループバックモードを MAC レイヤで指定します。 • External PHY Default - エクスターナルループバックモードを PHY レイヤで指定し初期メディアのテストをします。 • External PHY Copper - エクスターナルループバックモードを PHY レイヤで指定しカッパーメディアのテストをします。 • External PHY Fiber - エクスターナルループバックモードを PHY レイヤで指定し光ファイバメディアのテストをします。

「Apply」ボタンをクリックすると設定が更新されます。

PoE（PoE の管理）（DGS-3630-28PC/52PC）

DGS-3630-28PC/52PC は IEEE の 802.3af と IEEE802.3at 規格の PoE 機能をサポートしています。ポート 1-24/48 は 30W まで PoE、エンハンスドカテゴリ 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、「消費電力がシステム電源のリミットを超えている場合」と「各ポートの消費電力リミットを超えている場合」において動作します。
- Active circuit 防止機能は電力の不足が生じた場合、自動的にポートを無効にする機能です。他のポートは有効性は変わりません。

802.3af/at 準拠の受電機器の最大受信電力一覧：

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

PSE を使用したの最大電力一覧：

クラス	受電機器の最大受信電力
0	16.2W
1	4.2W
2	7.4W
3	16.2W
ユーザ定義	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。

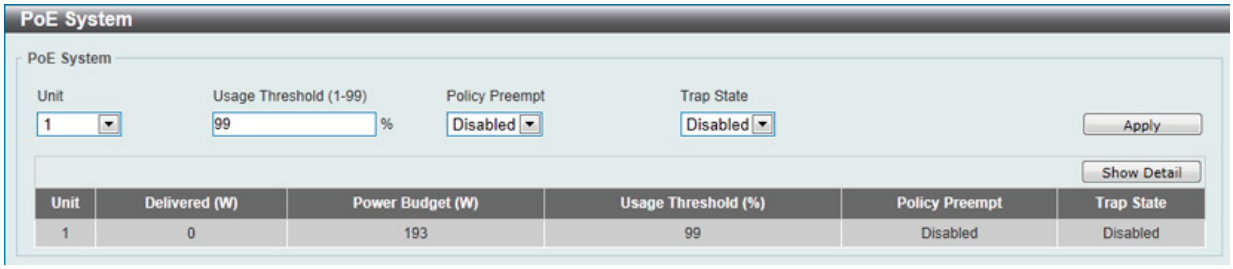


図 6-12　PoE System 画面

画面には以下の項目があります。

項目	説明
Unit	ユニット番号を設定します。全てのユニットを選択する場合は「All」にチェックします。
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。1 から 99（%）で指定できます。
Policy Preempt	電力供給不足となった新規接続のデバイスの優先値を高く指定し、既存の低優先度の電力供給デバイス（PD）接続の解除機能を有効 / 無効に指定します。
Trap State	PoE の通知送信について有効 / 無効を指定します。

「Apply」ボタンをクリックすると設定が更新されます。
「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 6-13　PoE System（Show Detail）画面

PoE Status（PoE ステータス）

各ポートの PoE ステータス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。

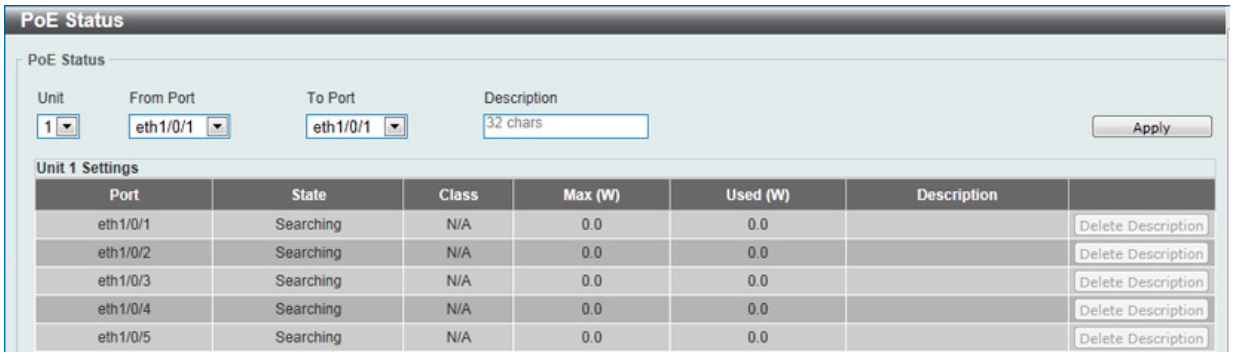


図 6-14　PoE Status 画面

画面には以下の項目があります。

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設定します。
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 文字以内で指定できます。

「Delete Description」ボタンをクリックすると入力した概要が削除されます。
「Apply」ボタンをクリックすると設定が更新されます。

PoE Configuration（PoE ポート設定）

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

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

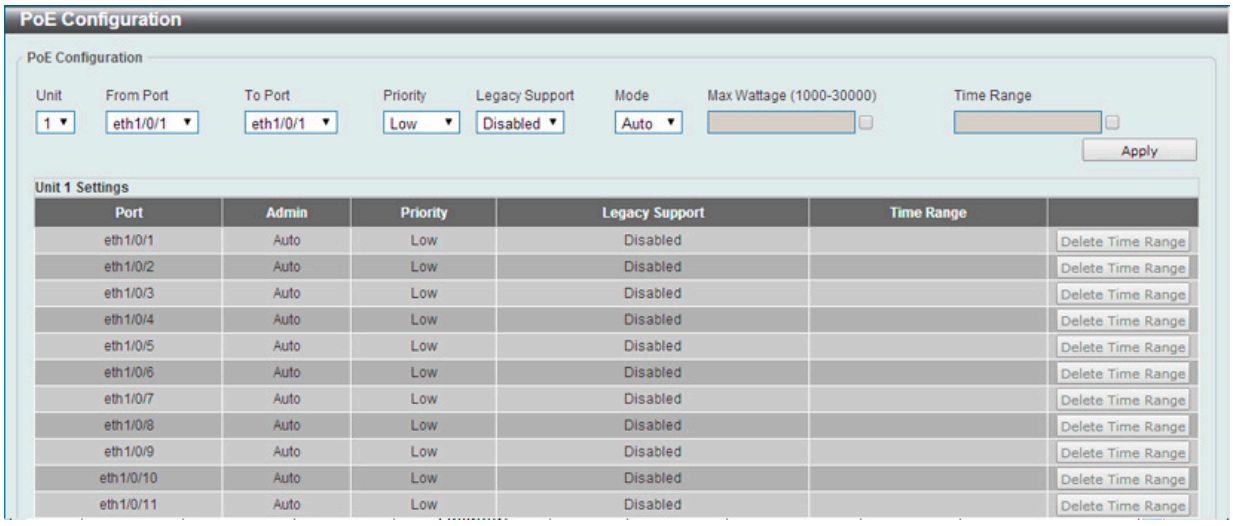


図 6-15　PoE Configuration 画面

画面には以下の項目があります。

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設定します。
Priority	プルダウンメニューを使ってポートの優先度（Critical、High、Low）を指定します。 ポート優先度はシステムがどのポートに優先的に電力供給を行うかを設定します。優先度には 3 段階あり「Critical」「High」「Low」で設定できます。
Legacy Support	レガシー PD へのサポートの有効 / 無効を指定します。
Mode	PoE ポートの電力管理モードを選択します。「Auto」か「Never」から指定できます。

項目	説明
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。「1000mW」から「30000mW」までで指定可能です。
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。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。

「Delete Description」ボタンをクリックすると入力した概要が削除されます。
「Apply」ボタンをクリックすると設定が更新されます。

注意 IEEE802.3at PD への給電に失敗する場合は、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か、対象のポートを 30W に手動設定してください。

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。

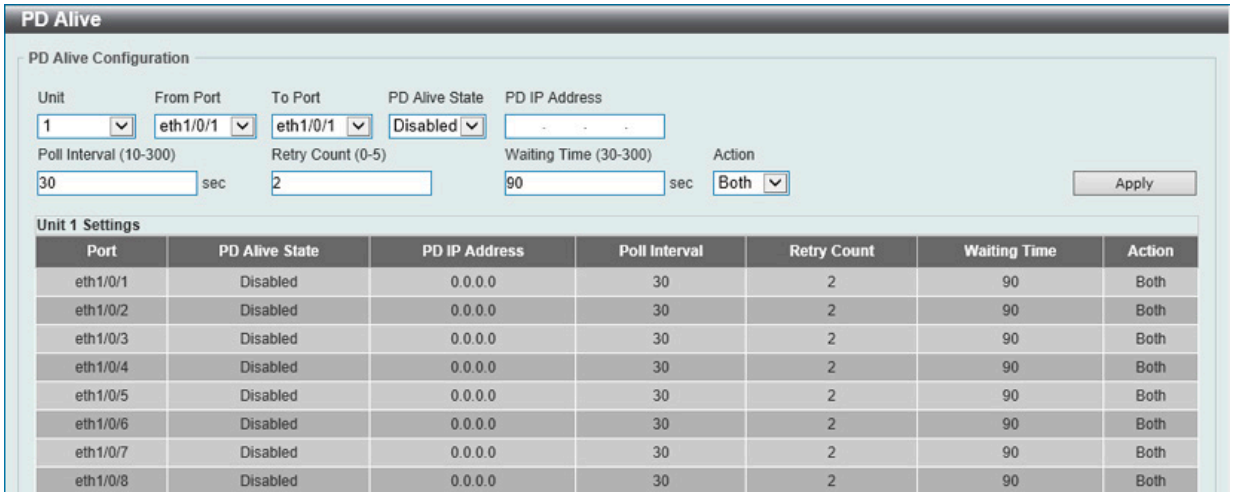


図 6-16　PD Alive 画面

画面には以下の項目があります。

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設定します。
PD Alive State	PoE アライブ機能を有効 / 無効にします。
PD IP Address	PD の IPv4 アドレスを指定します。
Poll Interval	ポールインターバル（10-300 秒）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。
Retry Count	リトライカウント（再試行回数 /0-5）を指定します。指定の PD からの回答がなかった際に Ping を再送信する回数を指定します。
Waiting Time	待機時間（30-300 秒）を指定します。指定の PD が再起動から回復するまでスイッチが待つ時間を指定します。
Action	実行する動作を指定します。 • Reset - PoE ポートをリセットします。 • Notify - 管理者に通知するログとトラップを送信します。 • Both - 管理者に通知するログとトラップを送信し、PoE ポートをリセットします。

「Apply」ボタンをクリックすると設定が更新されます。

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。

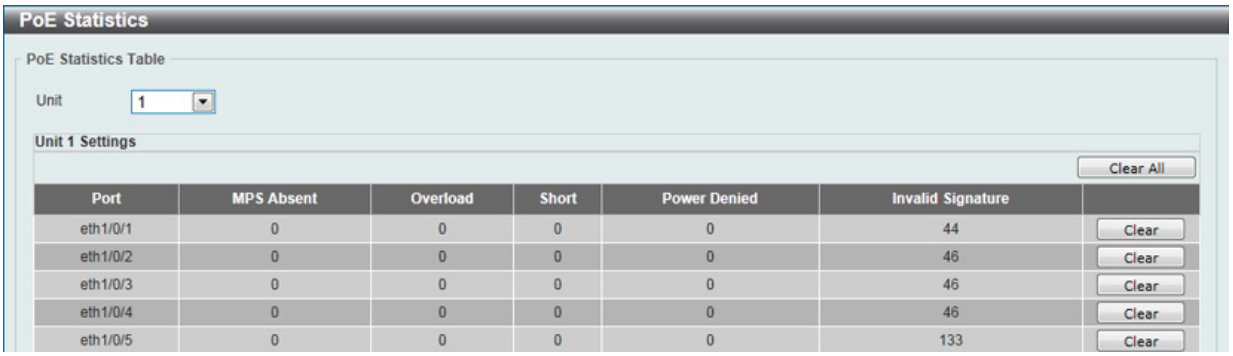


図 6-17　PoE Statistics 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。

「Clear All」ボタンをクリックすると全ポートの PoE 統計情報がクリアされます。
「Clear」ボタンをクリックすると対象ポートの PoE 統計情報がクリアされます。

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。

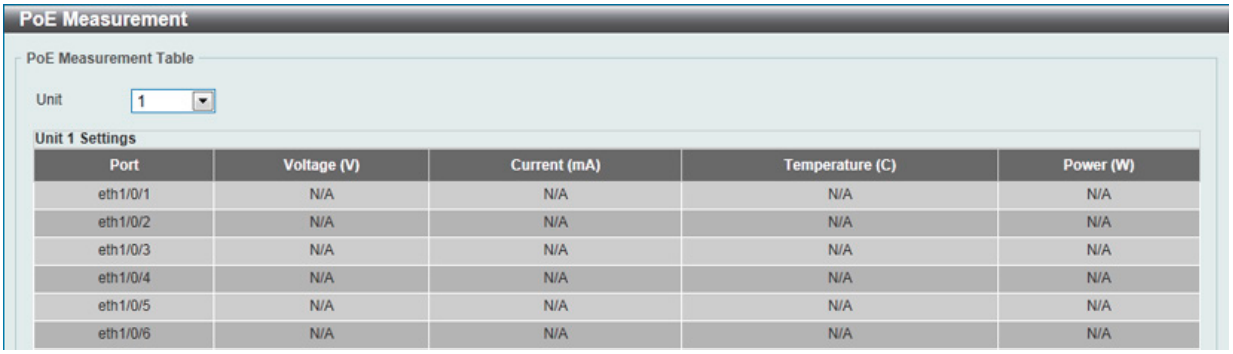


図 6-18　PoE Measurement 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。

PoE LLDP Classification（PoE LLDP 分類表示）

PoE の LLDP 分類情報を表示します。

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

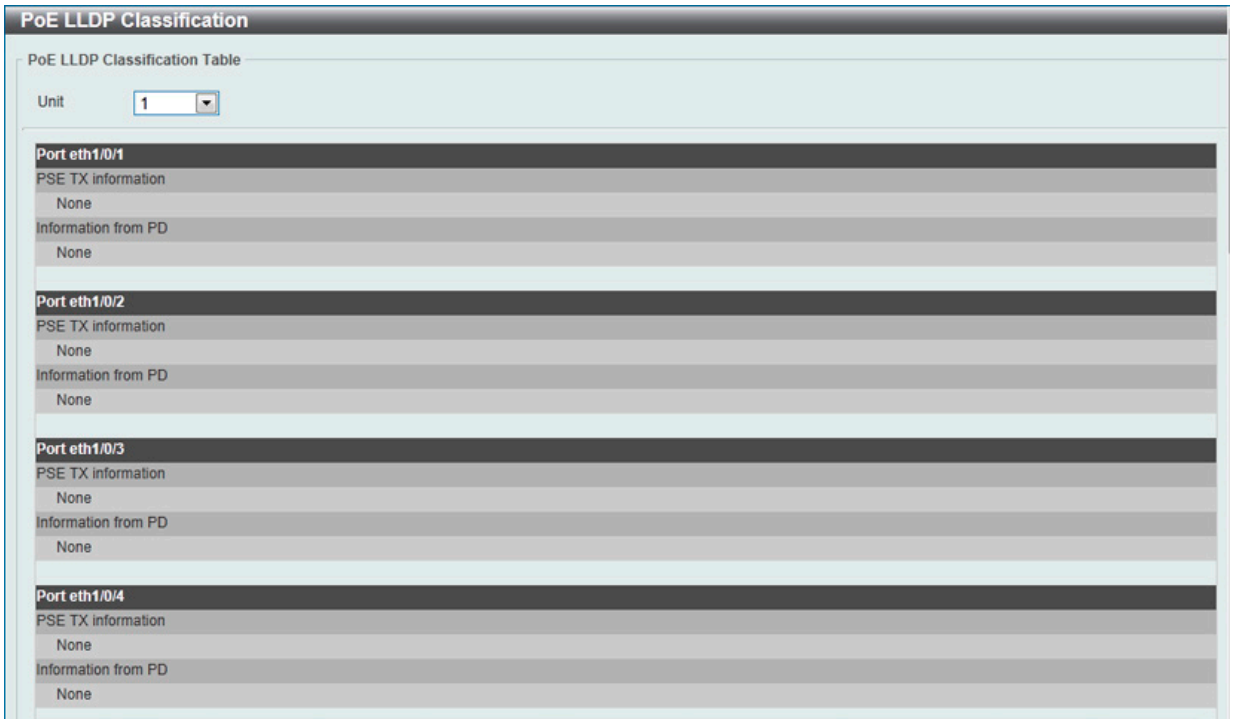


図 6-19　PoE LLDP Classification 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。

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。

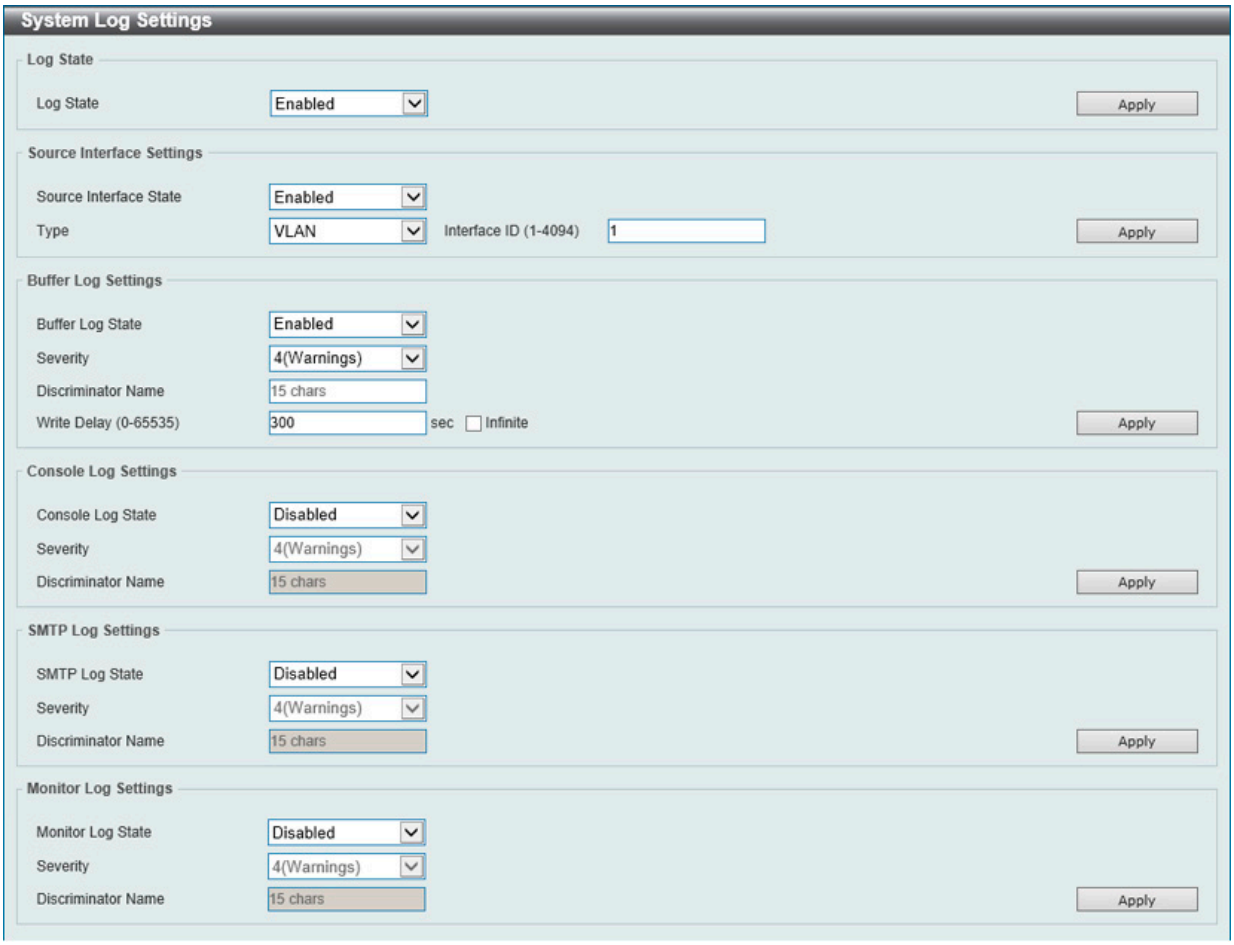


図 6-20　System Log Settings 画面

System Log Settings 画面には次の項目があります。

Log State（グローバルステート）

項目	説明
Log State	グローバルにシスログを有効 / 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。

Source Interface Settings（ソースインタフェース設定）

項目	説明
Source Interface State	ソースインタフェースをグローバルに有効 / 無効に指定します。
Type	インタフェースの種類を選択します。
Interface ID	インタフェース ID を指定します。ループバックインタフェースの場合、「1」から「8」、 管理インタフェース（Mgmt）の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。

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

Buffer Log Settings（バッファログ設定）

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

項目	説明
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1：Emergencies」（緊急）、「2：Alerts」（警告）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。
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。0 から 65535（秒）の間で指定できます。初期値は 300 秒です。「Infinite」にチェックを入れると本機能は無効になります。

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

Console Log Settings（コンソールログ設定）

項目	説明
Console Log State	コンソールログのグローバルステートを有効 / 無効にします。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1：Emergencies」（緊急）、「2：Alerts」（警告）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。

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。

SMTP Log Settings（SMTP ログ設定）

項目	説明
SMTP Log State	SMTP ログのグローバルステートを有効 / 無効にします。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1：Emergencies」（緊急）、「2：Alerts」（警告）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。

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。

Monitor Log Settings（SMTP ログ設定）

項目	説明
Monitor Log State	モニタログのグローバルステートを有効 / 無効にします。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1：Emergencies」（緊急）、「2：Alerts」（警告）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。

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。

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

システムログディスクリミネーターの設定、設定内容の表示を行います。

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

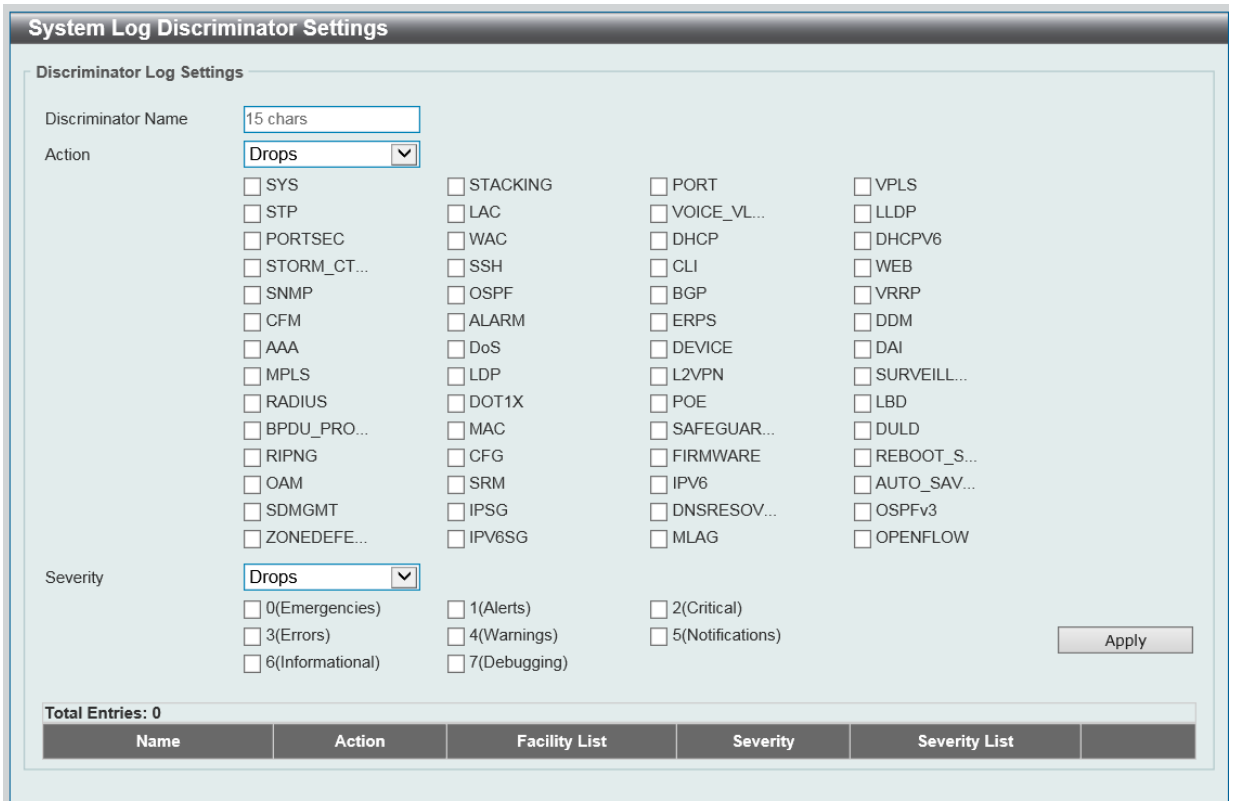


図 6-21　System Log Discriminator Settings 画面

本画面には次の項目があります。

項目	説明
Discriminator	ディスクリミネーターの名前を入力します。15 字以内に指定できます。
Facility	機能が実行する動作内容と選択した動作に関連する機能の種類を選択します。「Drops」「Includes」から選択します。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「1：Emergencies」（緊急）、「2：Alerts」（警告）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）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。
「Delete」ボタンをクリックすると指定のエントリが削除されます。

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

システムログはイベントの記録と管理、エラーと情報のメッセージをレポートします。イベントメッセージは、すべてのエラーレポートに Syslog プロトコルの推奨する固有のフォーマットを使用します。例えば、Syslog とローカルデバイスのレポートメッセージはその重要度や、メッセージを生成するアプリケーションを識別するためのメッセージ識別名を含みます。メッセージは緊急度かその関連する事項に基づいてフィルタされます。各メッセージの重要度によって、イベントメッセージの送信先となるイベントを記録するデバイスを決めることができます。

本スイッチは指定した 4 台までの Syslog サーバに Syslog メッセージを送信できます。

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



図 6-22　System Log Server Settings 画面

本画面には次の項目があります。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>Host IPv4 Address</td><td>ログを記録するサーバの IPv4 アドレスを設定します。</td></tr>
<tr><td>Host IPv6 Address</td><td>ログを記録するサーバの IPv6 アドレスを設定します。</td></tr>
<tr><td>UDP Port</td><td>ログを送信するサーバの UDP ポートを設定します。初期値は 514 です。
値は「514」、または「1024」から「65535」で指定します。</td></tr>
<tr><td>Severity</td><td>ログされる情報のレベルをプルダウンメニューから選択します。「1：Emergencies」（緊急）、「2：Alerts」（警告）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。</td></tr>
<tr><td>Facility</td><td>プルダウンメニューを使用して「0」から「23」までの間を選択します。
<table>
<tr><th>Facility 値</th><th>Facility 名</th><th>Facility 概要</th></tr>
<tr><td>0</td><td>kern</td><td>カーネルメッセージ</td></tr>
<tr><td>1</td><td>user</td><td>ユーザレベルメッセージ</td></tr>
<tr><td>2</td><td>mail</td><td>メールシステム</td></tr>
<tr><td>3</td><td>daemon</td><td>システム daemon</td></tr>
<tr><td>4</td><td>auth1</td><td>セキュリティ / 権限メッセージ 1</td></tr>
<tr><td>5</td><td>syslog</td><td>Syslog により内部生成されたメッセージ</td></tr>
<tr><td>6</td><td>lpr</td><td>ラインプリンタサブシステム</td></tr>
<tr><td>7</td><td>news</td><td>ネットワークニュースサブシステム</td></tr>
<tr><td>8</td><td>uucp</td><td>UUCP サブシステム</td></tr>
<tr><td>9</td><td>clock1</td><td>クロック daemon 1</td></tr>
<tr><td>10</td><td>auth2</td><td>セキュリティ / 権限メッセージ 2</td></tr>
<tr><td>11</td><td>ftp</td><td>FTP daemon</td></tr>
<tr><td>12</td><td>ntp</td><td>NTP サブシステム</td></tr>
<tr><td>13</td><td>logaudit</td><td>ログ検査</td></tr>
<tr><td>14</td><td>logalert</td><td>ログ警告</td></tr>
<tr><td>15</td><td>clock2</td><td>クロック daemon 2</td></tr>
<tr><td>16</td><td>local0</td><td>ローカル使用 0（local0）</td></tr>
<tr><td>17</td><td>local1</td><td>ローカル使用 1（local1）</td></tr>
<tr><td>18</td><td>local2</td><td>ローカル使用 2（local2）</td></tr>
<tr><td>19</td><td>local3</td><td>ローカル使用 3（local3）</td></tr>
<tr><td>20</td><td>local4</td><td>ローカル使用 4（local4）</td></tr>
<tr><td>21</td><td>local5</td><td>ローカル使用 5（local5）</td></tr>
<tr><td>22</td><td>local6</td><td>ローカル使用 6（local6）</td></tr>
<tr><td>23</td><td>local7</td><td>ローカル使用 7（local7）</td></tr>
</table></td></tr>
<tr><td>Discriminator</td><td>ディスクリミネーターの名前を入力します。15 字以内に指定できます。</td></tr>
<tr><td>VRF Name</td><td>VRF インスタンス名を指定します。12 字以内に指定できます。</td></tr>
</table>

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックすると指定のエントリが削除されます。

System Log（Syslog ログ）

スイッチの管理エージェントでまとめたローカルなヒストリ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。

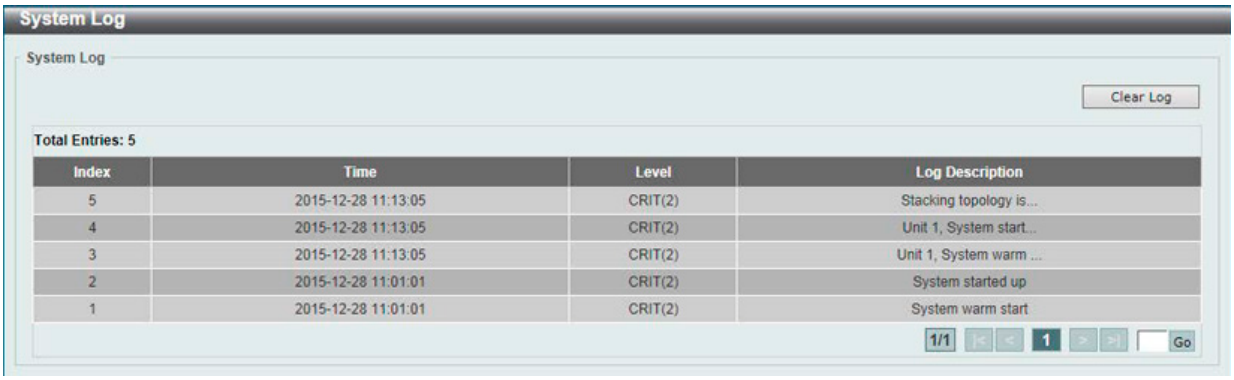


図 6-23　System Log 画面

スイッチは自身のログにイベント情報を記録できます。「Go」ボタンをクリックすると、「System Log」画面の次のページへ移動します。
「Clear Log」ボタンをクリックして、表示画面内のすべてのエントリをクリアします。

System Attack Log（システムアタックログ）

攻撃を受けたシステムログの閲覧 / 消去を行います。

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

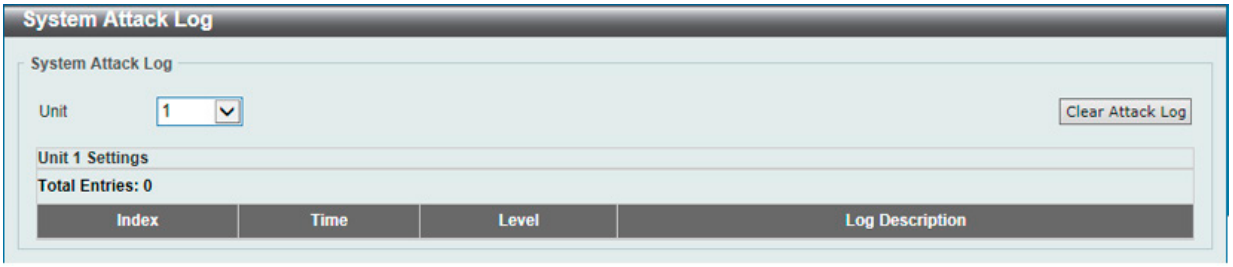


図 6-24　System Attack Log 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。

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

Time and SNTP（時刻設定）

System > Time and SNTP
SNTP（Simple Network Time Protocol）は、コンピュータのクロックにスイッチを同期させるために使用されます。

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。

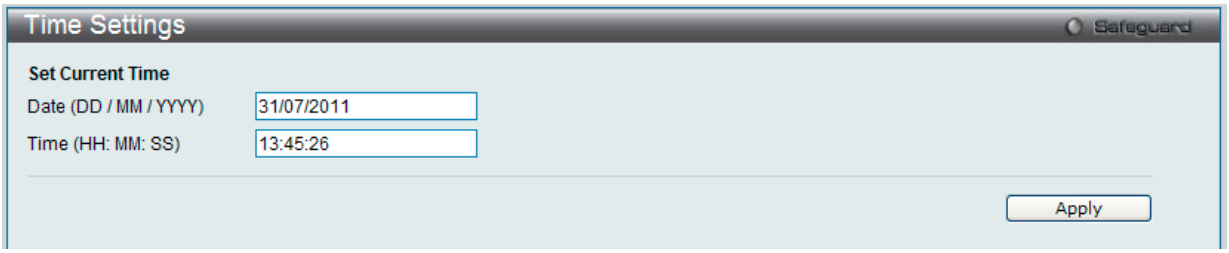


図 6-25　Time Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Date（DD/MM/YYYY）	システムクロックの更新を行うために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。
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。

「Apply」ボタンをクリックし、設定を適用します。

Time Zone Settings（タイムゾーン設定）

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

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

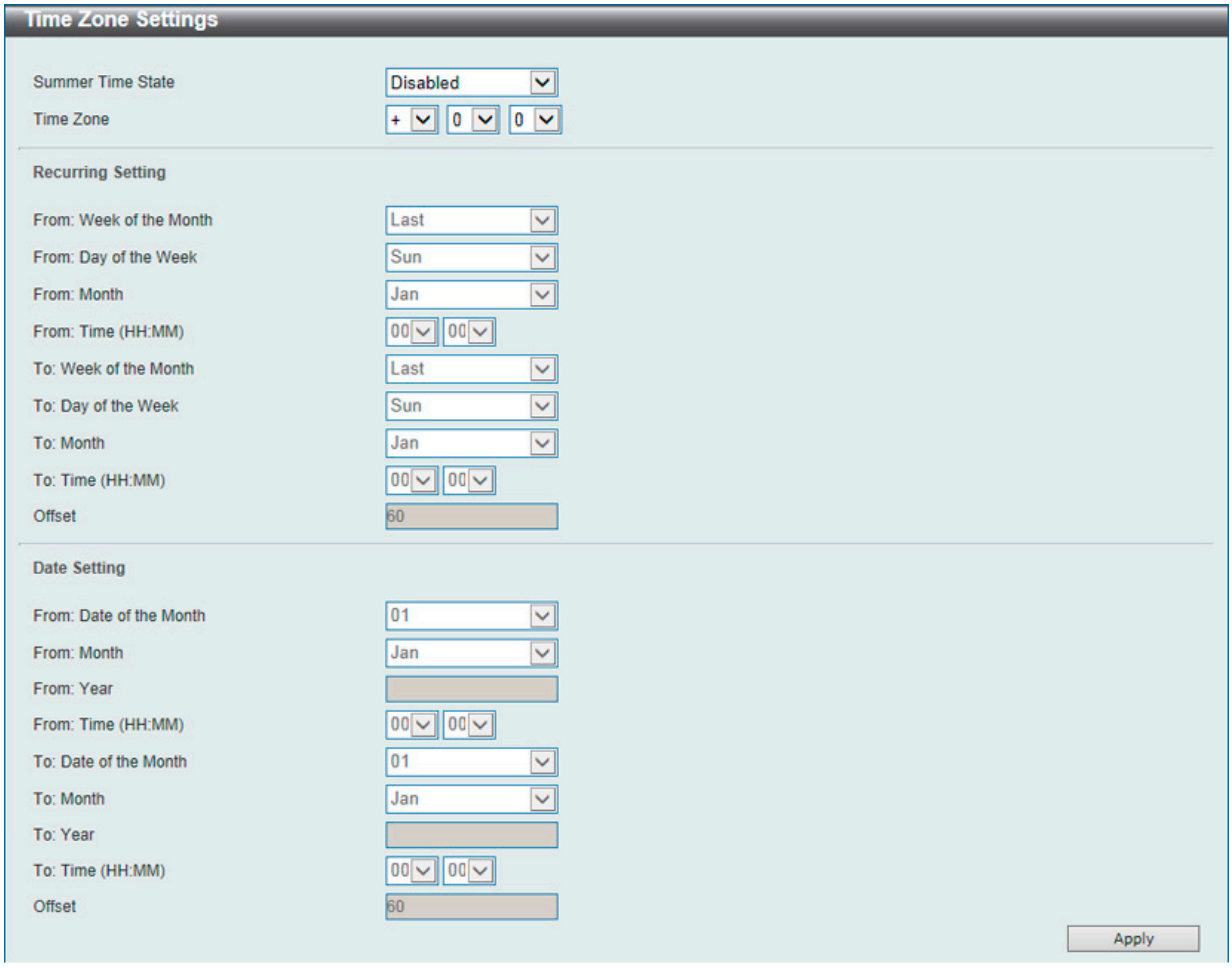


図 6-26　Time Zone Settings 画面

以下に、画面の各項目を示します。

項目	説明
Summer Time State	デバイスに設定するサマータイムの種類を設定します。 • Disabled - サマータイムを無効にします。（初期値） • Recurring Setting - サマータイムを周期的に有効にします。このオプションでは開始と終了のタイミングを指定月の指定週で設定する必要があります。 • Date Setting - サマータイムを日付指定で有効にします。このオプションでは開始と終了の日付を設定する必要があります。
Time Zone	UTC からのタイムゾーンを選択します。
Recurring Setting	
Recurring Setting モードを使用すると、サマータイムの設定を指定した期間で自動的に調整できるようになります。例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。	
From: Week Of The Month	月の第何週から 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。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。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。
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を指定します。初期値は 60（分）です。オフセットの範囲は「30」「60」「90」「120」から選択可能です。
Date Setting	
From: Date of the Month	サマータイムが始まる月日を指定します。
From: Month	サマータイムが開始する月を指定します。（毎年）
From: Day	サマータイムが開始する日を指定します。（毎年）
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	サマータイムが修了する月日を指定します。
To: Month	サマータイムが終了する月を指定します。（毎年）
To: Day	サマータイムが終了する日を指定します。（毎年）
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を指定します。初期値は 60（分）です。オフセットの範囲は「30」「60」「90」「120」から選択可能です。

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

SNTP Settings（SNTP 設定）

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

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

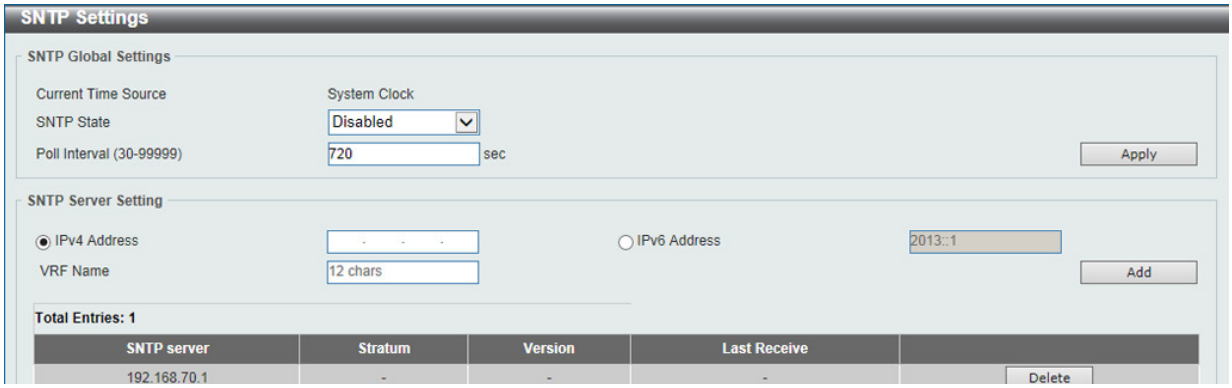


図 6-27　SNTP Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
SNTP Global Settings	
Current Time Source	現在の日付と時刻の提供元を表示します。
SNTP State	SNTP を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Poll Interval	同期する間隔（秒）を指定します。 「30」から「99999」（秒）で指定します。 初期値は「720 秒」です。
SNTP Server Settings	
IPv4 Address	SNTP 情報の取得元であるサーバの IP アドレスを設定します。
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。
VRF Name	VRF インスタンス名を指定します。12 字以内に指定できます。

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。
「Add」をクリックして SNTP サーバを追加します。
「Delete」をクリックして指定のエントリを削除します。

Time Range（タイムレンジ設定）

スイッチのタイムレンジを設定します。

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

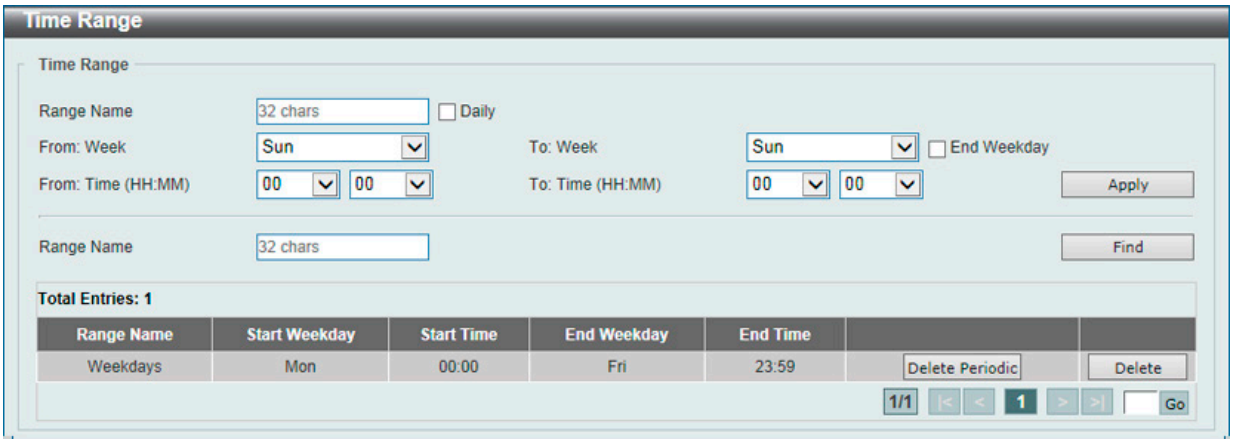


図 6-28　Time Range 画面

以下の項目を設定することができます。

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

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

エントリの削除

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

PTP（PTP 設定）

System > PTP

PTP（Precision Time Protocol : 高精度時刻同期方式）システムは、イーサネットネットワークを通して 1 マイクロ秒未満の精度で配信されるクロックに同期することができます。

PTP は、システムにおいて正確なクロックの同期を可能にする技術です。PTP はイーサネットおよび UDP を含むマルチキャストメッセージ送信をサポートするローカルエリアネットワークで通信するシステムに適切です。PTP により、様々な固有の精度、解像度、および安定性のクロックを含む異種システムはグランドマスタクロックへ同期が可能となります。

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

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

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

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

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

PTP Global Settings（PTP グローバル設定）

PTP 機能をグローバルに設定します。

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

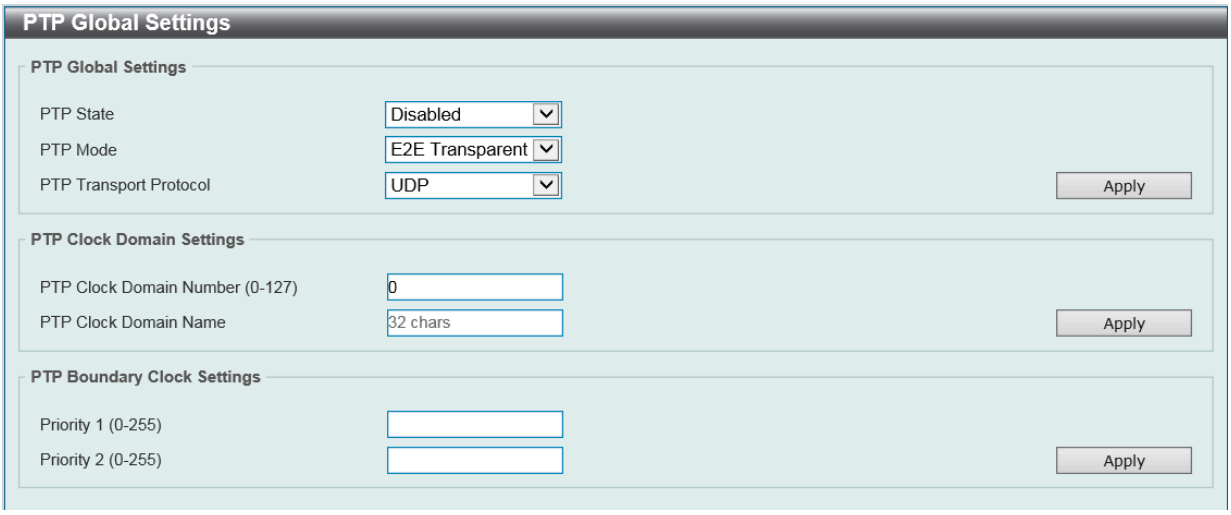


図 6-29　PTP Global Settings 画面

以下の項目が設定可能です。

項目	説明
PTP Global Settings	
PTP State	プルダウンメニューを使用して、PTP 状態を「Enabled」(有効)/「Disabled」(無効) にします。
PTP Mode	スイッチの PTP タイプを選択します。スイッチには、3 つ PTP デバイスタイプ、「Boundary」(境界)、「P2P Transparent」(ピアツーピア透過)、および「E2E Transparent」（エンドツーエンド透過）があります。初期値は「E2E Transparent」です。
PTP Transport Protocol	通信パスに使用する送信プロトコルを「Ethernet」「UDP」から選択します。初期値は UDP です。
PTP Clock Domain Settings	
Unit	本設定を適用するユニットを選択します。
PTP Clock Domain Number (0-127)	ローカルクロックのドメイン属性を入力します。すべての PTP メッセージ、データセット、ステートマシン、およびその他すべての PTP エンティティがいつも特定のドメイン番号に関連付けられます。範囲は 0-127 です。初期値は 0 です。
PTP Clock Domain Name	指定したドメイン番号に対してドメイン名を入力します。
PTP Boundary Clock Settings	
Priority 1	PTP 境界クロックの「Priority 1」を指定します。「Priority 1」の属性は「Best Master Clock（BMC）」アルゴリズムの実行に使用されます。低い値ほど優先値は高くなります。「0」が最優先になります。0 から 255 の間で指定します。

項目	説明
Priority 2	PTP 境界クロックの「Priority 2」を指定します。「Priority 2」の属性は「Best Master Clock（BMC）」アルゴリズムの実行に使用されます。「Priority 1」を基準にした BMC アルゴリズムの失敗にともない、「Priority 2」の属性が採用されます。低い値ほど優先値は高くなります。「0」が最優先になります。0 から 255 の間で指定します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

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

PTP の状態をポートごとに設定します。

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

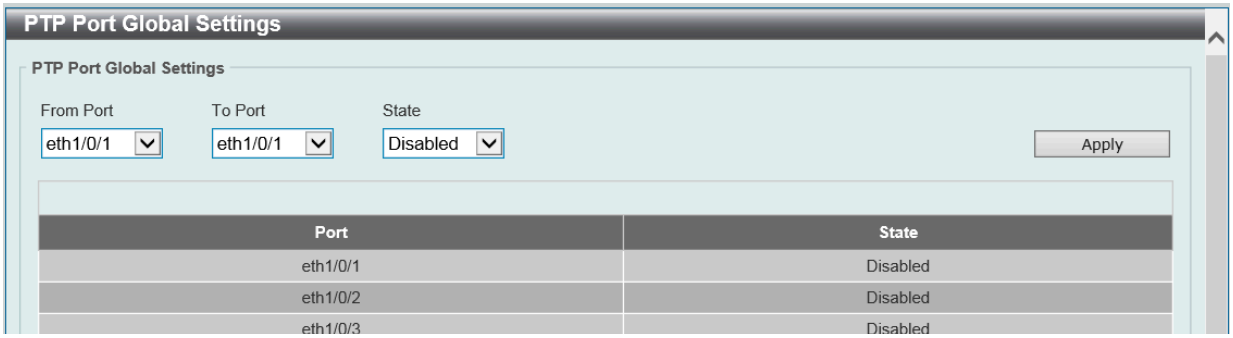


図 6-30　PTP Port Global Settings 画面

以下の項目が設定可能です。

項目	説明
From Port / To Port	この設定に使用するポート範囲を選択します。
State	プルダウンメニューを使用して、指定ポートの PTP 状態を「Enabled」(有効)/「Disabled」(無効) にします。

「Apply」ボタンをクリックして行った変更を適用します。

PTP Boundary Port Settings（PTP 境界ポート設定）

PTP 境界クロックの属性を設定します。PTP デバイスが境界タイプである場合に、本設定は機能します。

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

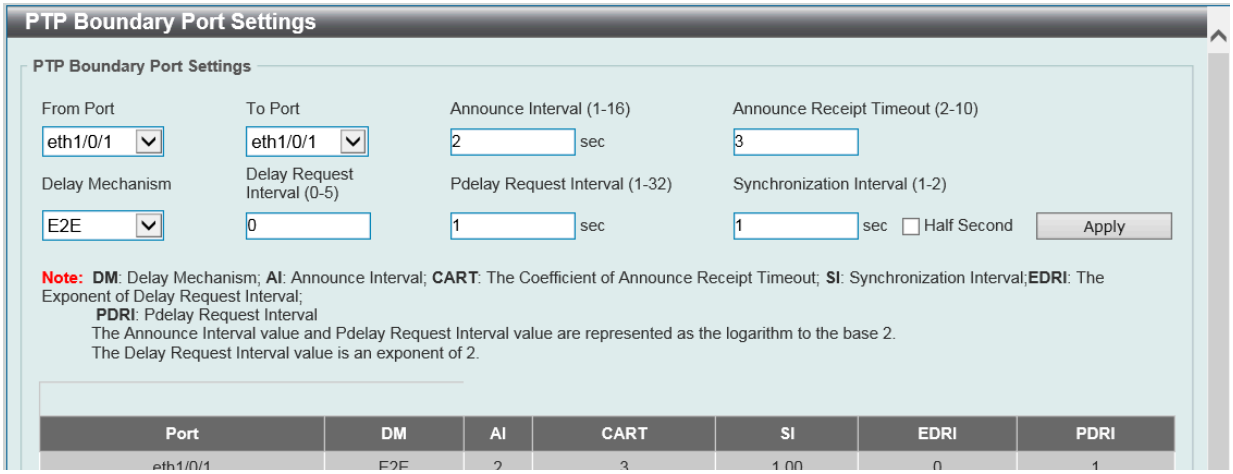


図 6-31　PTP Boundary Port Settings 画面

以下の項目が設定可能です。

項目	説明
From Port / To Port	この設定に使用するポート範囲を選択します。
Announce Interval (1-16)	ラジオボタンをクリックし、連続するアナウンスメッセージ間の平均時間を入力します。アナウンス間隔として参照されます。IEEE 1588 プロトコルに従い、アナウンス間隔の値は底を 2 とする測定時間（秒）の対数として表示されます。入力値は 1、2、4、8、または 16 とします。無効な数字が入力されると、それより大きくて最も近い値に自動的に調整されます。初期値は 2（秒）です。
Announce Receipt Timeout (2-10)	ラジオボタンをクリックして、ANNOUNCE_RECEIPT_TIMEOUT_EXPIRES イベントの発生前にアナウンスメッセージを受信せずに通過すべきアナウンス間隔を入力します。アナウンス間隔値の乗数は、アナウンス受信のタイムアウトの間隔に一致します。範囲は 2-10 です。

項目	説明
Delay Mechanism	プルダウンメニューを使用して、イベントメッセージの伝搬遅延時間を測定するメカニズムを指定します。 • E2E - ポートは Delay Request-response Mechanism を使用します。（初期値） • P2P - Peer Delay Mechanism を使用します。
Delay Request Interval (0-5)	スレーブがマスタ上の指定ポートに送信する連続する遅延要求メッセージの許容される間隔の平均を入力します。この間隔の平均は、マスタによって決定されて、通知されます。
Pdelay Request Interval (1-32)	連続する Pdelay_Request メッセージの許容される間隔の平均を入力します。
Synchronization Interval (1-2)	同期間隔を入力します。同期成功メッセージの平均時間間隔となります。IEEE 1588 プロトコル標準において、本値は、同期間隔の 2 を底とする対数とされています。1-2 秒の間で指定します。「Half Second」オプションにチェックを入れると、0.5 秒に設定されます。

「Apply」ボタンをクリックして行った変更を適用します。

PTP P2P Transparent Port Settings（PTP P2P 透過ポート設定）

P2P 透過クロックの Pdelay Request Interval を設定します。

System > PTP (Precise Time Protocol) > PTP P2P Transparent Port Settings の順にメニューをクリックし、以下の画面を表示します。

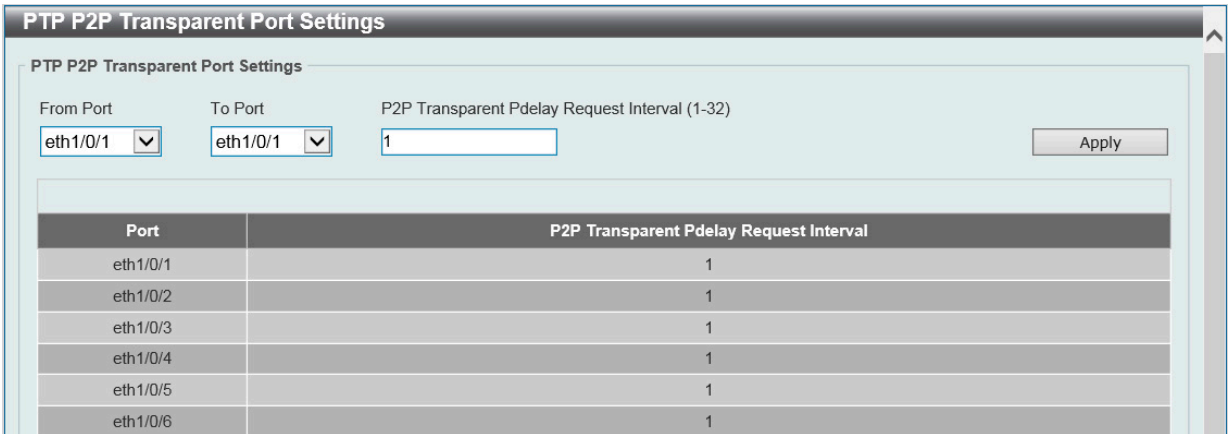


図 6-32　PTP Peer to Peer Transparent Port Settings 画面

以下の項目が設定可能です。

項目	説明
From Port / To Port	この設定に使用するポート範囲を選択します。
P2P Transparent Pdelay Request Interval (1-32)	連続する Pdelay_Request メッセージの許容される間隔の平均を入力します。

「Apply」ボタンをクリックして行った変更を適用します。

PTP Clock Information（PTP クロック情報の表示）

PTP クロックのアクティブな属性を表示します。PTP の状態が「PTP Global Settings」画面で無効にされると、PTP クロック ID は「0000000000000000」と表示されます。表示するユニットを指定します。

System > PTP > PTP Clock 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。

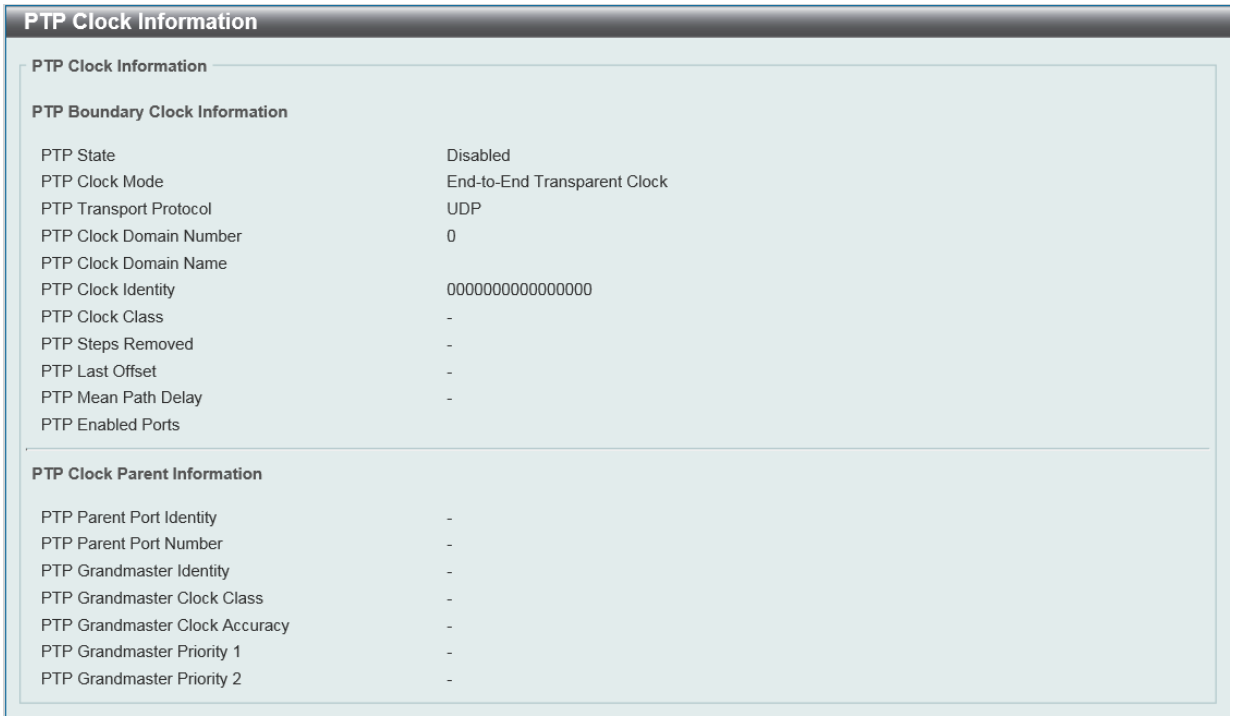


図 6-33　PTP Clock Information 画面

PTP Port Information (PTP ポート情報)

スイッチにおいて特別である PTP ポートのアクティブな属性を表示します。表示するユニットを指定します。

System > PTP > PTP 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。

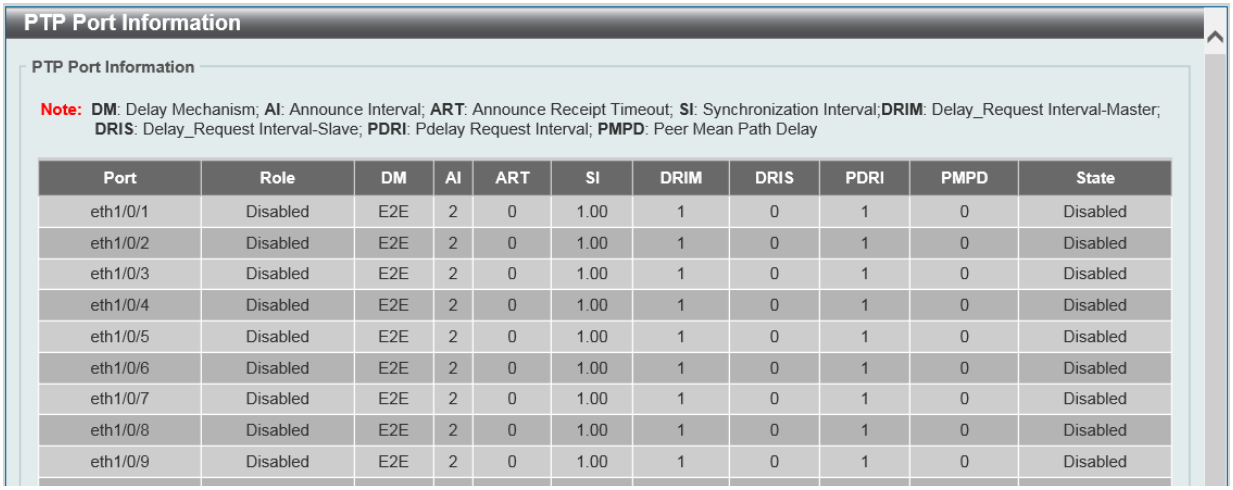


図 6-34　PTP Port Information 画面

PTP Foreign Master Records Port Information（PTP 外部マスタレコードのポート情報）

境界クロックの特定ポートにおける現在の外部マスタレコードを表示します。表示するユニットを指定します。

System > PTP > PTP Foreign Master Records 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 :

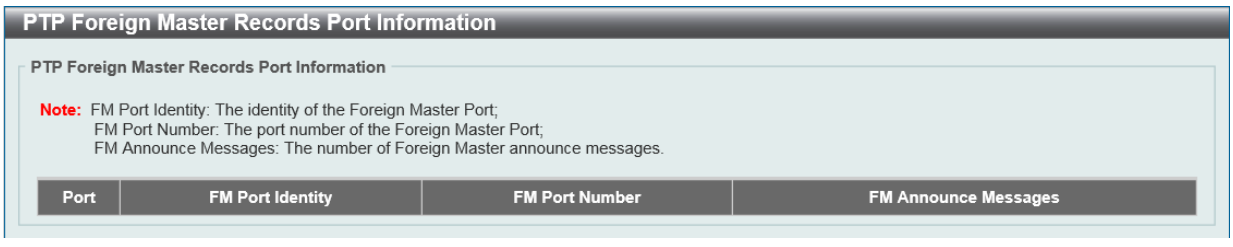


図 6-35　PTP Foreign Master Records Port Information 画面

USB Console Settings（USB コンソール設定）

USB コンソールの設定、表示を行います。

System > USB Console 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：

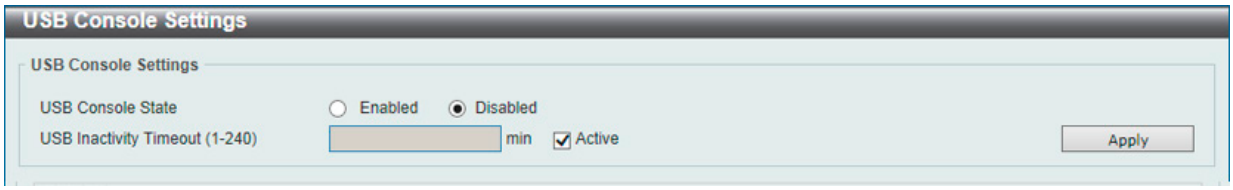


図 6-36　USB Console Settings 画面

以下の項目が設定可能です。

項目	説明
USB Console State	USB コンソールを有効 / 無効にします。
USB Inactivity Timeout	USB タイムアウトについて設定します。1-240（秒）の範囲で指定可能です。USB コンソールが無動作の状態が指定の秒数を過ぎるとタイムアウトします。「Active」を選択するとタイムアウトすることはありません。

「Apply」ボタンをクリックして行った変更を適用します。

注意　アクティブなコンソール接続が RJ45、mini-USB の両方で構築されている場合、mini-USB コンソールの方により高い優先値があります。

SRM（Switch Resource Management 設定）

System > SRM

「Switch Resource Management」（SRM）機能はアプリケーションによって必要な大規模なリソースを最適化します。これにより、より多くのエントリに必要なテーブルの提供や、不使用の機能によるリソースの消費などを抑えることなどにより、フレキシブルなリソース設定が提供されます。

SRM Prefer Current Settings（SRM 最適化設定）

SRM の設定、表示を行います。本画面は、スイッチにおける頻繁に使用する機能リソースの最適化を行う SRM モードの指定を行います。

System > SRM > SRM Prefer Current 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 6-37　SRM Prefer Current Settings 画面

以下の項目が設定可能です。

項目	説明
SRM Prefer Mode	SRM モードの選択を行います。 • LAN - スイッチを「LAN スイッチ」モードとして指定します。 • IP - スイッチを「IP ルート」モードとして指定します。 • L2VPN - スイッチを「L2VPN」モードとして指定します。

「Apply」ボタンをクリックして行った変更を適用します。

注意　SRM モードが指定されスイッチが再起動すると、テーブルサイズは変更されます。設定済みのスタティックエントリの数が、新しいテーブルサイズのスタティックエントリのしきい値を超えた場合、しきい値を超えたエントリは削除されます。

注意　スイッチが物理スタックされている場合、スタック内すべてのスイッチが同じ SRM モードで設定されている必要があります。

SRM Prefer Mode（SRM 設定モード）

SRM の設定モードの表示を行います。テーブル内の各機能の最大エントリ値を示す値などが表示されます。

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

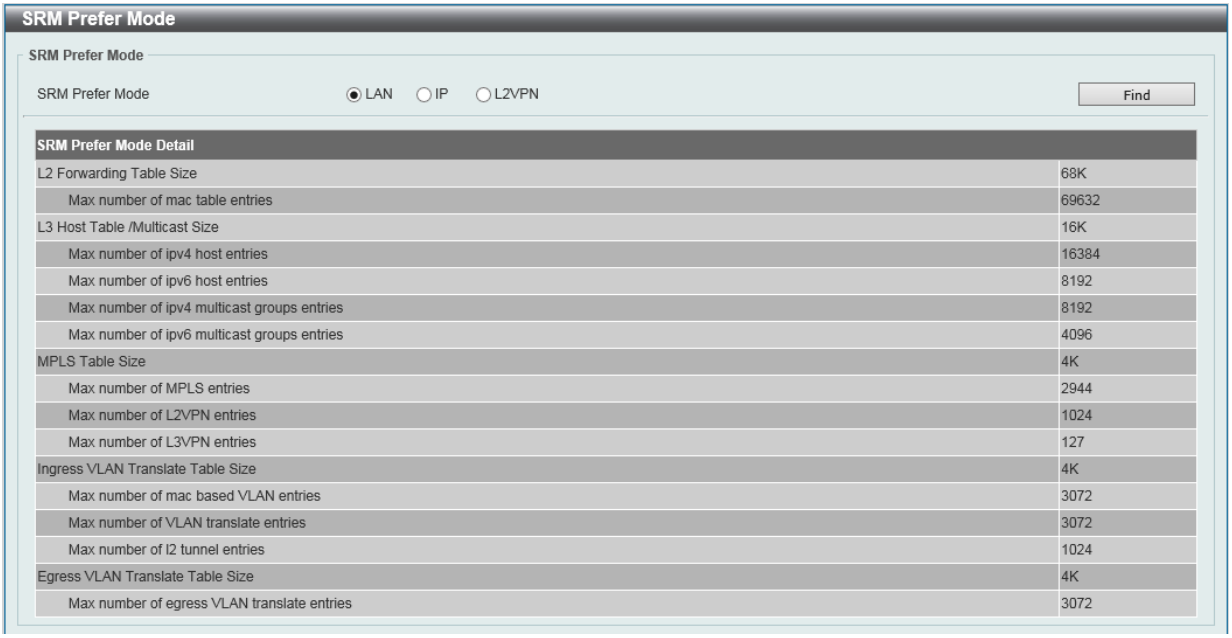


図 6-38　SRM Prefer Mode 画面

以下の項目を選択することが可能です。

項目	説明
SRM Prefer Mode	表示する SRM モードの選択を行います。「LAN」「IP」「L2VPN」から指定します。

Find をクリックして各 SRM モードの設定内容を表示します。

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）	コマンドログ設定を有効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
User Accounts Settings（ユーザアカウント設定）	スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。
CLI Alias Settings（CLI エイリアス設定）	CLI エイリアスの設定を行います。CLI エイリアスコマンドは指定の CLI コマンドと連携するカスタムの文字列になります。
Password Encryption（パスワード暗号化）	パスワードを暗号化し設定ファイルに保存します。
Password Recovery（パスワードリカバリ）	パスワードリカバリを行います。例えば管理者がパスワードを忘れた場合に有効です。
Login Method（ログイン方法）	各管理インタフェースでのログイン方法について設定します。
SNMP Settings（SNMP 設定）	SNMP 設定を有効にします。本スイッチシリーズは、SNMP v1、v2c、および v3 をサポートしています。
RMON（RMON 設定）	SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効にします。
Telnet/Web（Telnet/Web 設定）	スイッチに Telnet/Web 設定を有効にします。
Session Timeout（セッションタイムアウト）	各セッション（Web やコンソールなど）のタイムアウトの設定をします。
DHCP（DHCP 設定）	スイッチの DHCP について設定します。
DHCP Auto Configuration（DHCP 自動コンフィグ設定）	DHCP 自動コンフィグ機能の設定を行います。
DHCP Auto Image Settings（DHCP 自動イメージ設定）	DHCP 自動イメージ設定を行います。スタートアップ時に、外部サーバからイメージファイルを取得する機能です。
DNS（ドメインネームシステム）	DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。
NTP（ネットワークタイムプロトコル）	スイッチの時刻を同期するための NTP プロトコルの設定を行います。
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）	フラッシュファイルシステムにより、Firmware、Config 情報、および Syslog 情報はフラッシュ内のファイルに保存されます。
Stacking（スタッキング設定）	物理スタッキングの設定を行います。
Virtual Stacking（SIM）（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。
NLB FDB Settings（NLB FDB 設定）	ネットワークロードバランシング (NLB) の設定を行います。
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。

Command Logging（コマンドログ設定）

コマンドログ設定を有効または無効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。システムログには、コマンド及びコマンドを入力したユーザ情報が含まれます。スイッチの設定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。

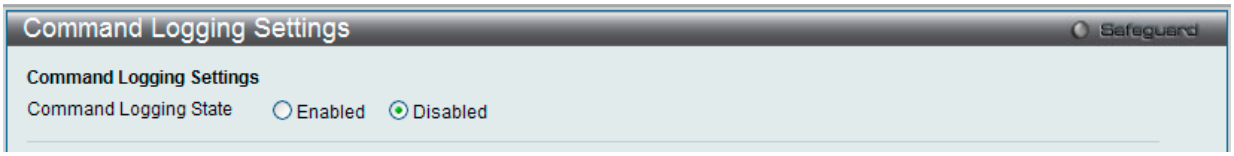


図 7-39　Command Logging Settings 画面

以下の項目を設定することができます。

項目	説明
Command Logging State	ラジオボタンを使用して機能を「Enabled」(有効)/「Disabled」(無効) にします。

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　スイッチの再起動中またはダウンロードしたコンフィグレーションの処理実行中は、すべてのコンフィグレーションコマンドがログに出力されるというわけではありません。または、ユーザが AAA 認証を使用してログインした際、ユーザが権限を取り替えるために「enable admin」コマンドを使用した場合には、ユーザ名を変更するべきではありません。

User Accounts Settings（ユーザアカウント設定）

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

注意　初期値ではユーザアカウントは設定されていません。

Web UI にはいくつかの設定方法が用意されています。いくつかの設定オプションはアカウントの権限レベルにより設定が可能になります。高い権限レベルを有するユーザアカウントはより多くの機能設定へのアクセスを行うことができます。

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

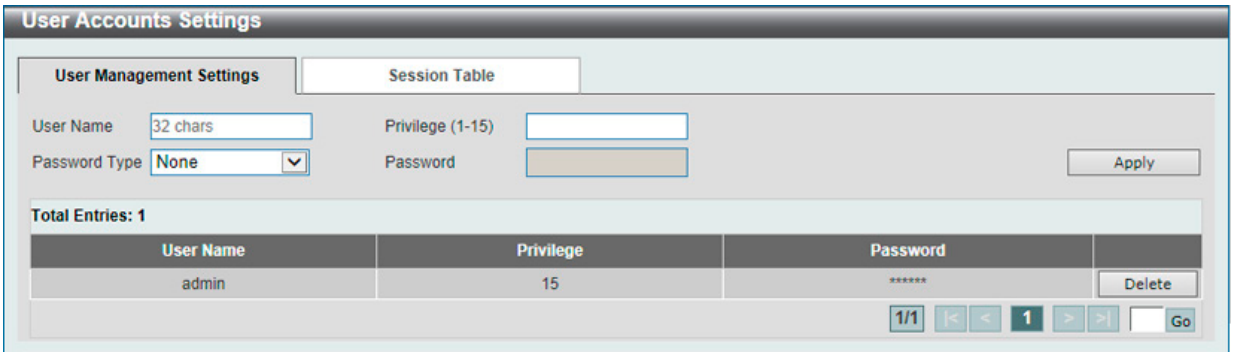


図 7-1　User Accounts Settings - User Management Settings 画面

画面には次の項目があります。

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

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

Session Table

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

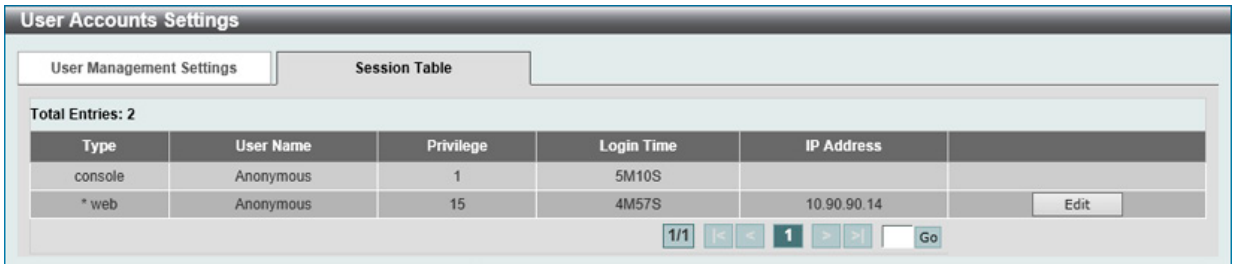


図 7-2　User Accounts Settings - Session Table 画面

User Level

「Session Table」タブで「Edit」をクリックするとユーザレベル設定が表示されます。

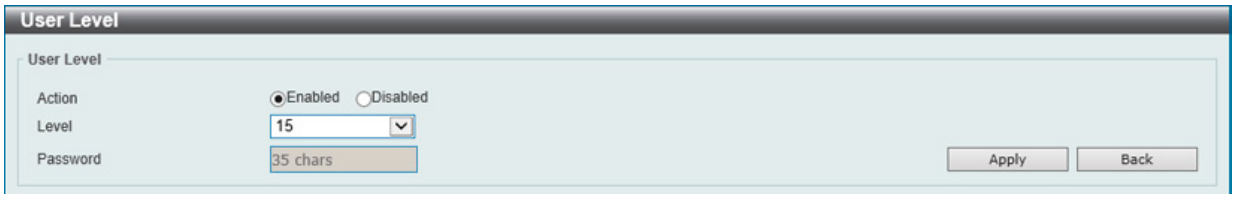


図 7-3　User Accounts Settings - User Level 画面

画面には次の項目があります。

項目	説明
Action	ユーザレベル設定を有効 / 無効に指定します。
Level	ユーザレベル（1-15）を指定します。
Password	パスワード（35 字以内）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。
「Back」ボタンをクリックし、前画面に戻ります。

CLI Alias Settings（CLI エイリアス設定）

CLI エイリアスの設定を行います。CLI エイリアスコマンドは指定の CLI コマンドと連携するカスタムの文字列になります。CLI で長文コマンドの繰り返し使用の際に有効です。

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

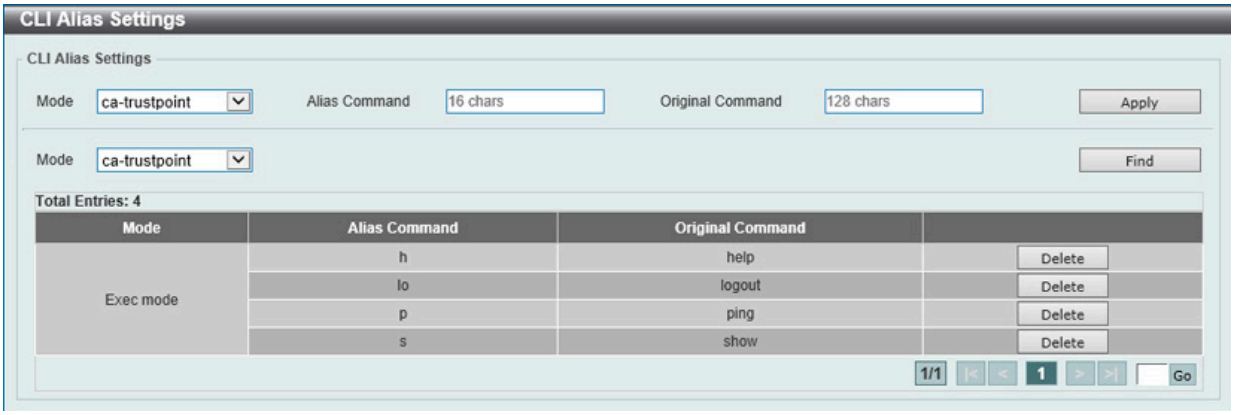


図 7-4　CLI Alias Settings 画面

画面には次の項目があります。

項目	説明
Mode	オリジナルコマンドのコマンドモードを指定します。
Alias Command	エイリアスコマンドを入力します。16 文字まで入力可能です。
Original Command	オリジナルコマンドを入力します。128 文字まで入力可能です。

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、入力した情報に基づく特定のエントリを検出します。
削除するエントリ横の「Delete」ボタンをクリックすると該当エントリは削除されます。

Password Encryption（パスワード暗号化）

パスワードを暗号化して設定ファイルに保存します。

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

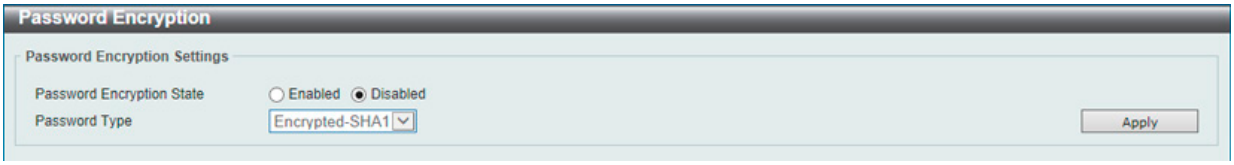


図 7-5　Password Encryption 画面

画面には次の項目があります。

項目	説明
Password Encryption State	パスワードの暗号化のコンフィグファイル保存ついての有効 / 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暗号化が可能です。 • Encrypted-MD5 -「MD-5」を使用してパスワード暗号化が可能です。

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。

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。例えば管理者がユーザアカウント更新時にパスワードを忘れた場合などに行います。

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

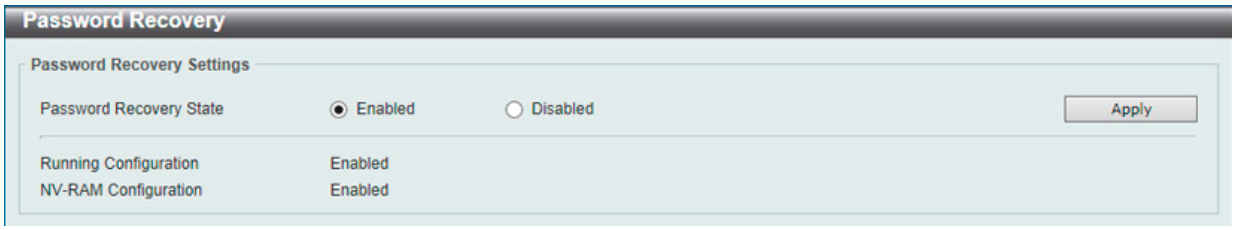


図 7-6　Password Recovery 画面

画面には次の項目があります。

項目	説明
Password Recovery State	パスワードリカバリを有効 / 無効に指定します。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からユーザアカウントのアップデートが可能で、パスワード機能は管理者権限レベルにアップデートされ、AAA 機能がローカル認証において無効にすることが可能です。実行中のコンフィグレーションはスタート時のコンフィグとして保存されます。再起動が必要です。

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。

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。

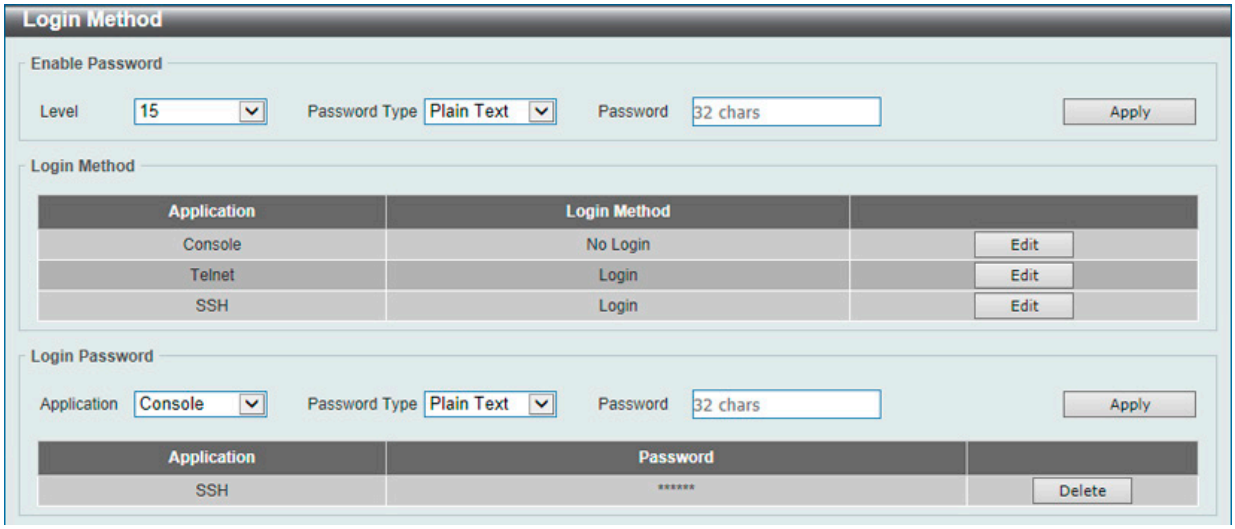


図 7-7　Login Method 画面

画面には次の項目があります。

項目	説明
Enable Password	
Level	ユーザの権限レベルを指定します。1 から 15 の間で指定可能です。
Password Type	暗号化の方法を「Plain Text」「Encrypted」「Encrypted-MD5」から選択します。
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）

項目	説明
Login Method	
Login Method	「Edit」ボタンをクリックしてパラメータの設定を行います。指定のアプリケーションへのログイン方法を選択します。「No Login」「Login」「Login Local」から選択可能です。「No Login」では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の必要がありません。「Login」では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」はユーザ名とパスワードの入力が必要になります。
Login Password	
Application	設定するアプリケーションを選択します。「Console」「Telnet」「SSH」から選択できます。
Password Type	暗号化の方法を「Plain Text」「Encrypted」「Encrypted-MD5」から選択します。
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）

「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、設定内容を編集できます。

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

SNMP Settings（SNMP 設定）

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

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

本スイッチシリーズは、SNMP バージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）をサポートしています。スイッチの監視と制御に使用する SNMP バージョンを選択することができます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

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

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

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

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

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

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

トラップ

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

MIB

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

本スイッチシリーズは、スイッチの環境に合わせた柔軟性のある SNMP 管理機能を採用しています。SNMP 管理機能は、ネットワークの要求やネットワーク管理者の好みに合わせてカスタマイズすることができます。SNMP バージョンの選択は、「SNMP V3」メニューから行うことができます。

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

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

SNMP Global Settings（SNMP グローバル設定）

SNMP グローバルステート設定を有効または無効にします。

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。

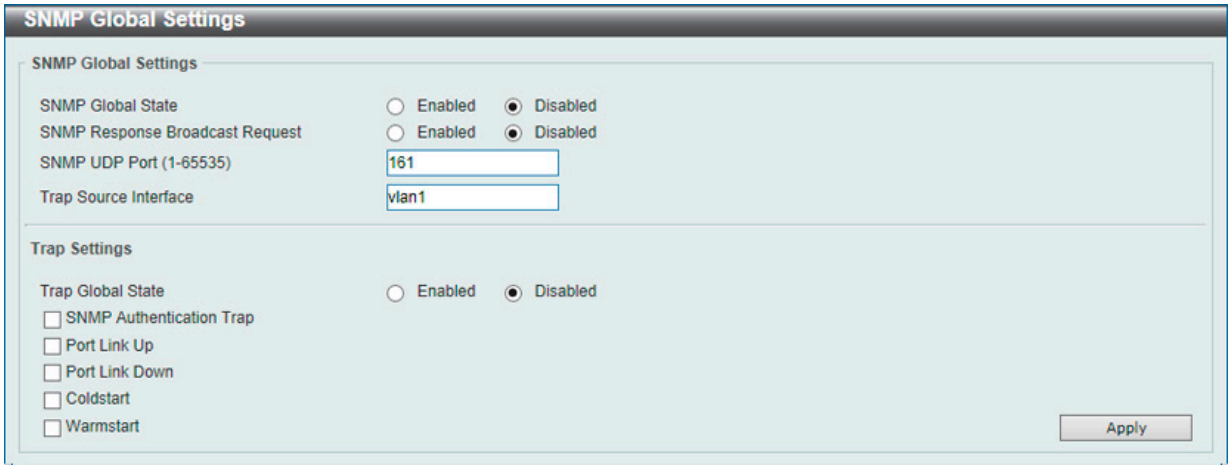


図 7-8　SNMP Global Settings 画面

以下の項目が使用されます。

SNMP Global Settings（SNMP グローバル設定）

項目	説明
SNMP Global State	SNMP 機能の有効 / 無効を選択します。
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 / 無効に指定します。
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（トラップ設定）

項目	説明
Trap Global State	SNMP トラップを有効 / 無効にします。
SNMP Authentication Trap	SNMP 認証失敗の通知送信の設定を行います。認証失敗トラップは、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 のバージョンによります。SNMPv1 または SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。
Port Link Up	ポートリンクアップ通知送信の設定を行います。リンクアップトラップは機器がリンクアップを認識すると実行します。
Port Link Down	ポートリンクダウン通知送信の設定を行います。リンクダウントラップは機器がリンクダウンを認識すると実行します。
Coldstart	コールドスタートを有効 / 無効にします。

項目	説明
Warmstart	ウォームスタートを有効 / 無効にします。

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

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。

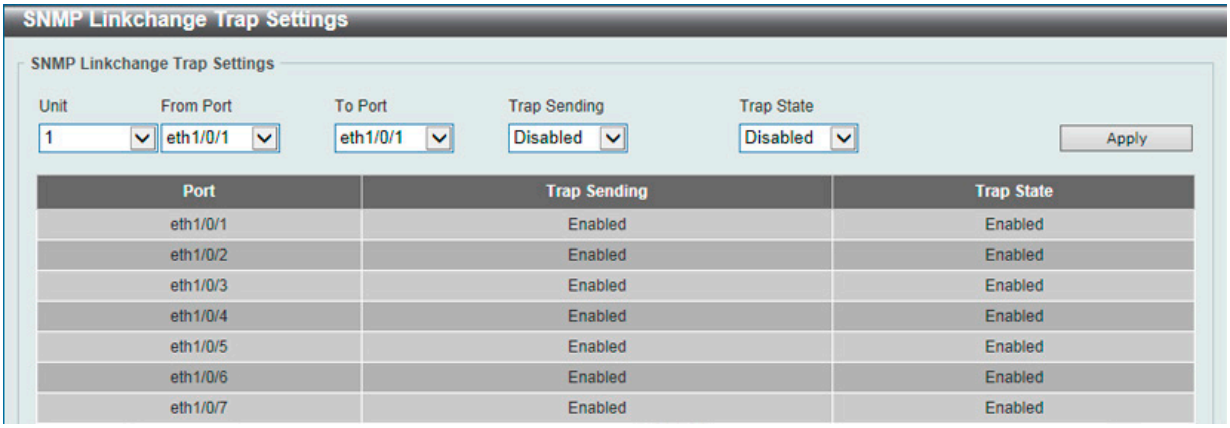


図 7-9　SNMP Linkchange Traps Settings 画面

以下の項目が使用されます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポートの始点 / 終点を設定します。
Trap Sending	SNMP 通知トラップ送信の有効 / 無効を指定します。
Trap State	SNMP リンクチェンジトラップの有効 / 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。

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。

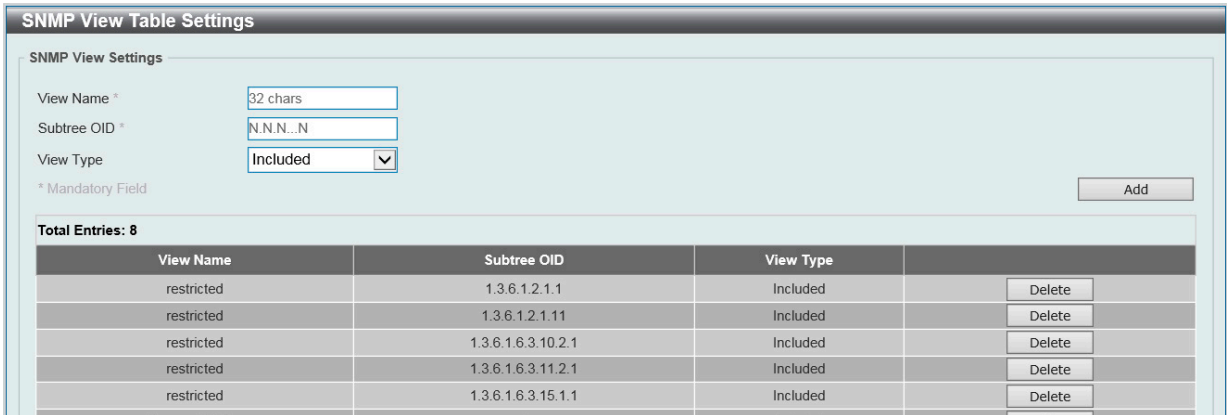


図 7-10　SNMP View Table Settings 画面

エントリの削除

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

エントリの新規作成

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

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。

以下の項目が使用されます。

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

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

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 コミュニティ名を登録します。コミュニティ名は、スイッチのエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。

- 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 アドレスが掲載されるアクセスリスト。
- MIB オブジェクトのすべてのサブセットを定義する MIB ビューは SNMP コミュニティにアクセス可能である。
- SNMP コミュニティにアクセス可能な MIB オブジェクトが Read/Write または Read-only レベルである。

エントリの設定

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

Management > SNMP > SNMP Community Table Settings の順にクリックし、以下の画面を表示します。



図 7-11　SNMP Community Table Settings 画面

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

項目	説明
Key Type	SNMP コミュニティのキーの種類を選択します。「Plain Text」「Encrypted」から選択可能です。
Community Name	32 文字までの半角英数字を入力し、SNMP コミュニティメンバを識別します。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。
View Name	32 文字までの半角英数字を入力します。本値は、リモート SNMP マネージャがアクセスすることのできる MIB グループの定義に使用します。View Name は SNMP View Table に存在する必要があります。
Access Right	• Read Only - 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りのみ可能となります。 • Read Write - 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取り、および書き込みが可能です。
IP Access-List Name	SNMP エージェントにアクセスするために文字列を使用するユーザを管理するアクセスリストの名前を入力します。

エントリの作成

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

エントリの削除

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

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

SNMP グループを登録します。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。

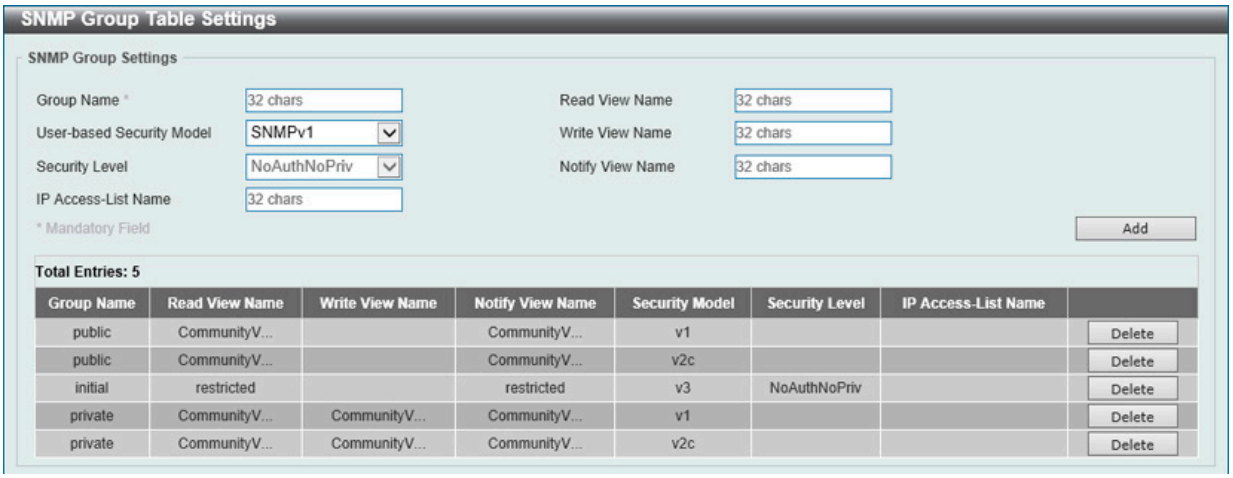


図 7-12　SNMP Group Table Settings 画面

「SNMP Group Table」画面のエントリの削除

エントリの行の「Delete」ボタンをクリックします。

「SNMP Group Table」画面への新規エントリの追加

上記画面に情報を入力し、「Add」ボタンをクリックします。

以下の項目が使用されます。

項目	説明
Group Name	32 文字までの半角英数字を入力します。SNMP ユーザのグループの識別に使用します。
User-based Security Model	• SNMPv1 - SNMP バージョン 1 が使用されます。 • SNMPv2c - SNMP バージョン 2c が使用されます。SNMP バージョン 2 は集中型、分散型どちらのネットワーク管理にも対応します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。 • SNMPv3 - SNMP バージョン 3 が使用されます。ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。
Security Level	セキュリティレベル設定は SNMP バージョン 3 にのみ適用されます。 • NoAuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットは認証も暗号化もされません。 • AuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化なしになります。 • AuthPriv - スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化ありになります。
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	SNMP メッセージを要求する SNMP グループ名を入力します。
Write View Name	SNMP エージェントに書き込み権限を与える SNMP グループ名を入力します。
Notify View Name	SNMP エージェントによるトラップメッセージを送信する SNMP グループ名を入力します。

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。

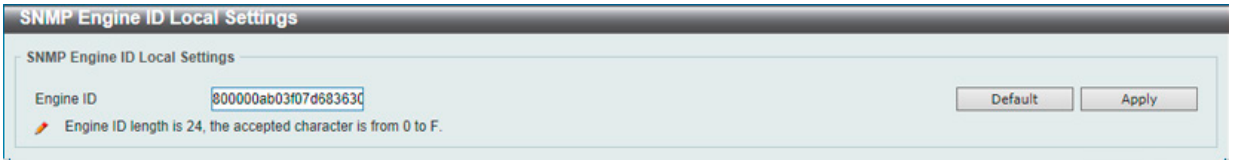


図 7-13　SNMP Engine ID Settings 画面

以下の項目を使用します。

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

新しいエンジン ID を入力し、「Apply」ボタンをクリックします。

「Default」をクリックするとエンジン ID は初期値に戻ります。

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

SNMP ユーザを登録します。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。

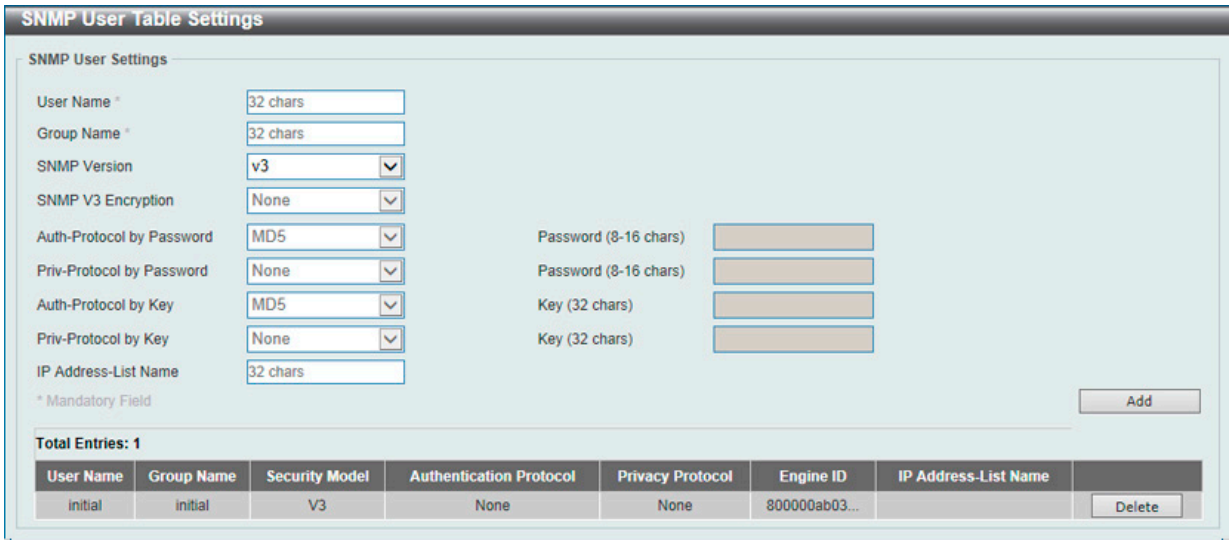


図 7-14　SNMP User Table Settings 画面

エントリの削除

エントリの行の「Delete」ボタンをクリックします。

エントリの新規登録

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

上記画面中の項目を以下に示します。

項目	説明
User Name	32 文字までの半角英数字。SNMP ユーザを識別します。
Group Name	作成した SNMP グループが SNMP メッセージを要求するために使用される名前です。
SNMP Version	• V1 - SNMP バージョン 1 が使用されています。 • V2 - SNMP バージョン 2 が使用されています。 • V3 - SNMP バージョン 3 が使用されています。
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 アルゴリズムレベルのユーザ認証を行います。 • Password - HMAC-SHA アルゴリズムレベルのパスワードか HMAC-MD5-96 パスワードによる認証を行います。
Auth-Protocol by Password Auth-Protocol by Key	本項目は「SNMP Version」で「V3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。本項目を選択後、「Password」/「Key」にパスワードを入力します。 • MD5 - HMAC-MD5-96 認証レベルが使用されます。（Password：半角英数字 8-16 文字 /Key：半角英数字 32 文字） • SHA - HMAC-SHA 認証プロトコルが使用されます。（Password：半角英数字 8-20 文字 /Key：半角英数字 40 文字）
Key	Auth-Protocol 鍵を入力します。（MD5：32 文字、SHA：40 文字）
Priv-Protocol by Password Priv-Protocol by Key	本項目は「SNMP Version」で「V3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 • None - 認証プロトコルは使用されていません。 • 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。本項目を選択後、「Password」/「Key」にパスワード（半角英数字 8-16 文字）、または Key（半角英数字 32 文字）を入力します。 • AES - AES 暗号が使用されます。本項目を選択後、「Password」/「Key」にパスワード（半角英数字 8-16 文字）、または Key（半角英数字 32 文字）を入力します。
Key	Priv-Protocol 鍵を入力します。（DES56/AES：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。

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。

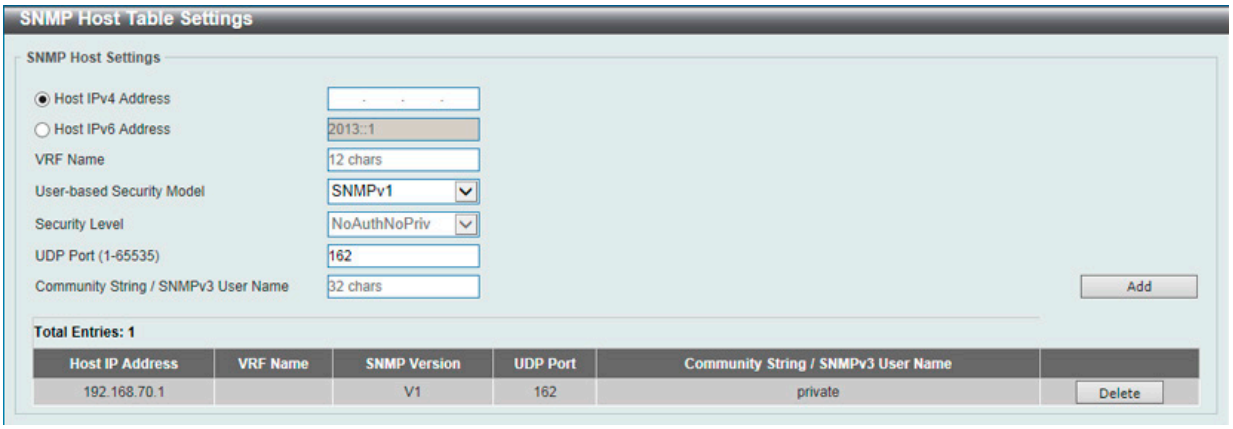


図 7-15　SNMP Host Table Settings 画面

以下の項目を設定します。

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
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。
VRF Name	VRF インスタンス名を 12 文字以内で入力します。
User-based Security Model	• 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	• NoAuthNoPriv : NoAuth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。 • AuthNoPriv : V3-Auth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。 • AuthPriv : V3-Auth-Priv セキュリティレベルの SNMP バージョン 3 が使用されます。
UDP Port	UDP ポート番号を入力します。UDP ポート番号の初期トラップは 162 です。UDP ポート範囲は 0 から 65535 です。いくつかのポート番号は他のプロトコルと衝突する可能性があります。
Community String/ SNMPv3 User Name	コミュニティ名または SNMP V3 ユーザ名を入力します。

エントリの削除

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

エントリの新規登録

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

SNMP Context Mapping Table Settings（SNMP コンテキストマッピングテーブル設定）（EI/MI モードのみ）

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

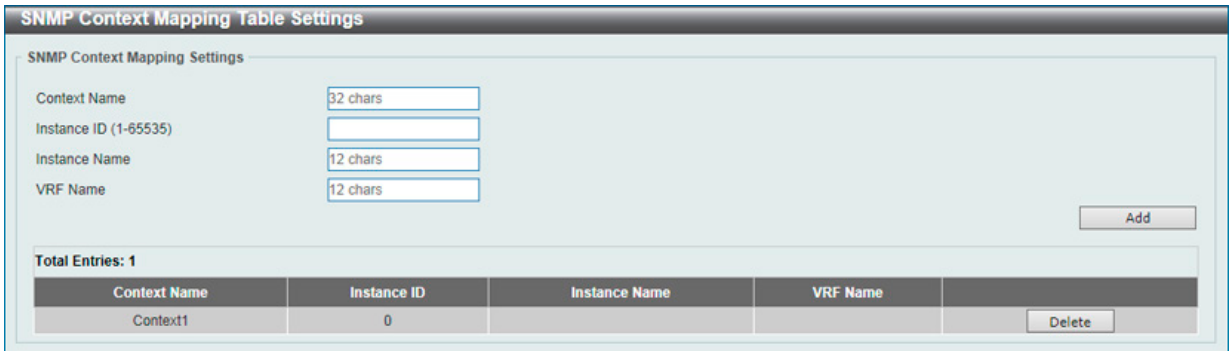


図 7-16　SNMP Context Mapping Table Settings 画面

以下の項目を設定します。

項目	説明
Context Name	SNMP View-based Access Control Model（VACM）コンテキスト名を 32 字以内で入力します。コンテキスト名は文字で開始する必要がありますが、終わりは文字、数字どちらでも構いません。それ以外は文字、数字、ハイフンが使用可能です。
Instance ID	OSPF インスタンス ID を入力します。（1-65535）
Instance Name	ISIS ルーティングエリアタグを 12 文字以内で入力します。
VRF Name	VRF インスタンス名を 12 文字以内で入力します。

エントリの削除

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

エントリの新規登録

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

RMON（RMON 設定）

スイッチの SNMP 機能に対するリモートモニタリング (RMON) ステータスを有効または無効にします。

RMON Global Settings（RMON グローバル設定）

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

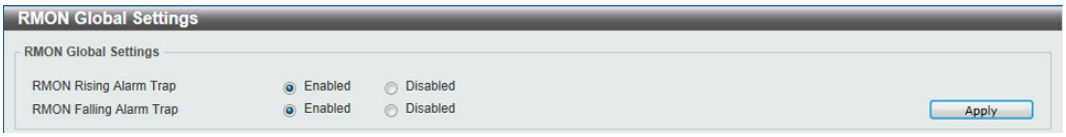


図 7-17　RMON Global Settings 画面

以下の項目が使用されます。

項目	説明
RMON Rising Alarm Trap	「RMON Rising Alarm Trap」を有効にします。
RMON Falling Alarm Trap	「RMON Falling Alarm Trap」を有効にします。

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

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「RMON Statistics Settings」画面を表示します。

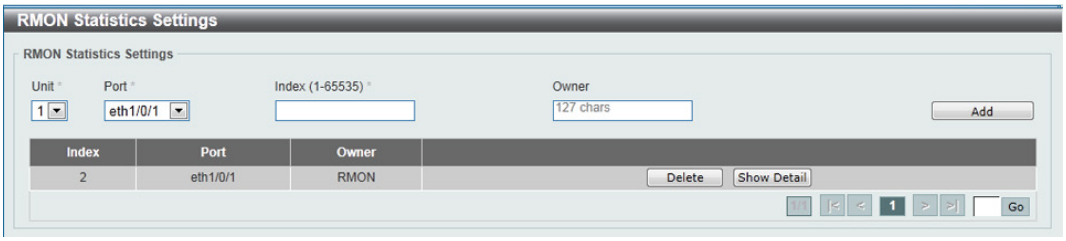


図 7-18　RMON Statistics Settings 画面

以下の項目が使用されます。

項目	説明
Unit	設定するユニットを選択します。
Port	RMON 情報を取得するポートを指定します。
Index (1 - 65535)	RMON イーサネット統計情報エントリの番号を指定します。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

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

統計情報の登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

統計情報の削除を行う場合

「Delete」をクリックします。

指定ポートの統計情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

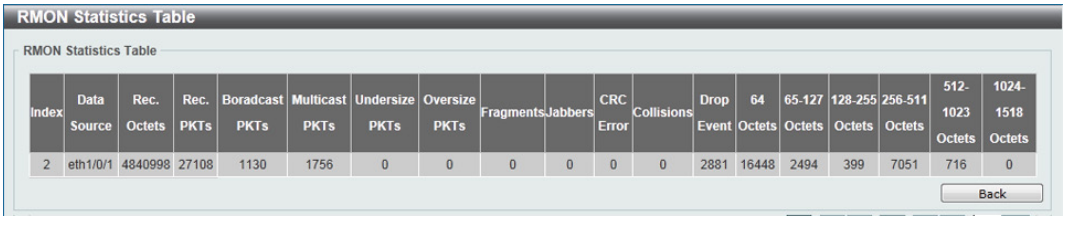


図 7-19　RMON Statistics Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

RMON History Settings（RMON ヒストリ設定）

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

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

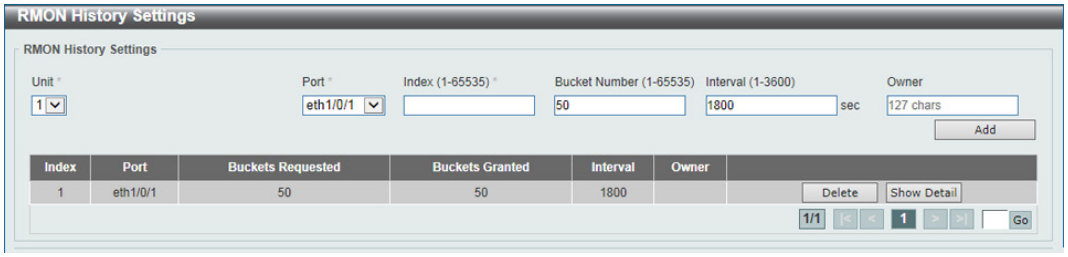


図 7-20　RMON History Settings 画面

以下の項目が使用されます。

項目	説明
Unit	設定するユニットを選択します。
Port	RMON 情報を取得するポートを指定します。
Index (1 - 65535)	ヒストリ制御エントリ番号を指定します。
Bucket Number(1 - 65535)	デバイスが保存するバケット数を指定します。初期値は 50 です。
Interval (1~3600)	ポートからサンプリングする間隔（秒）を設定します。 初期値：1800 (秒) 入力可能範囲：1-3600 (秒)
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

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

履歴情報の登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

履歴情報の削除を行う場合

「Delete」をクリックします。

指定ポートの履歴情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

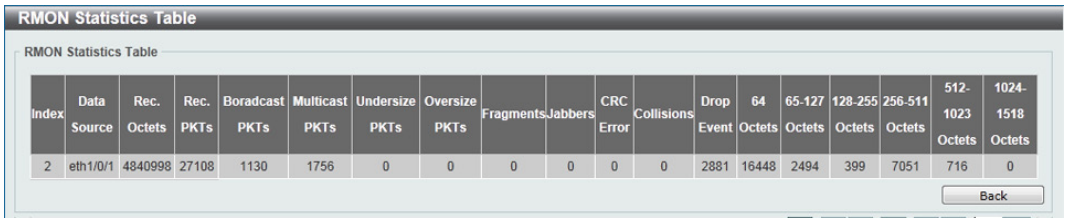


図 7-21　RMON History Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

RMON Alarm Settings（RMON アラーム設定）

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「RMON Alarm Settings」画面を表示します。

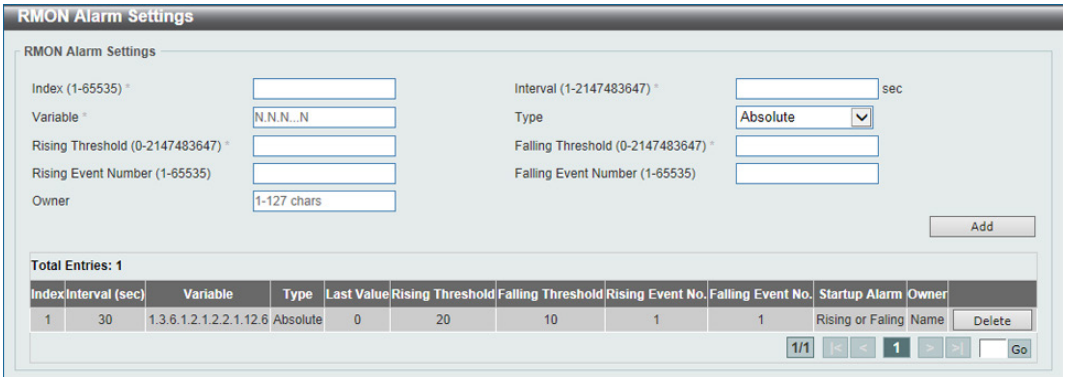


図 7-22　RMON Alarm Settings 画面

以下の項目が使用されます。

項目	説明
Index (1-65535)	特定のアラームを指定します。
Interval	アラームの間隔（秒）を定義します。1 から 2147483648（秒）の間で指定可能です。
Variable	選択した MIB 変数の値を指定します。
Type	選択した変数に対するサンプリング方式としきい値と比較する値を定義します。 • 「Delta」- 現在の値から最後にサンプリングされた値を引きます。値の差がしきい値と比較されます。 • 「Absolute」- サンプリング間隔の終わりで値を直接しきい値と比較します。
Rising Threshold	上昇しきい値を設定します。0 から 2147483647（秒）の間で指定可能です。
Falling Threshold	下降しきい値を設定します。0 から 2147483647（秒）の間で指定可能です。
Rising Event Number (1~65535)	上昇しきい値を超えたときに始動するイベントを設定します。 設定可能な項目は、ユーザ定義の RMON イベントです。1 から 65535（秒）の間で指定可能です。
Falling Event Number (1 ~ 65535)	下降しきい値を超えたときに始動するイベントを設定します。 設定可能な項目は、ユーザ定義の RMON イベントです。1 から 65535（秒）の間で指定可能です。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

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

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

「Delete」をクリックします。

RMON Event Settings（RMON イベント設定）

RMON イベント統計情報の定義、編集、および参照を行います。

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

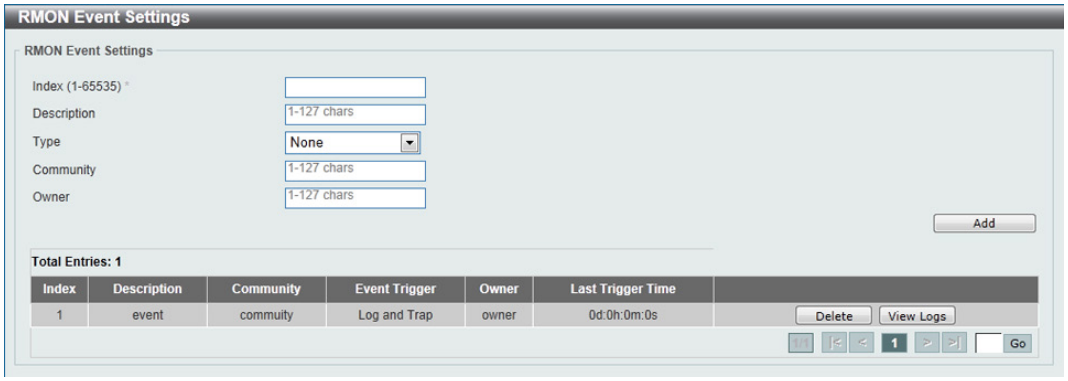


図 7-23　RMON Event Settings 画面

以下の項目が使用されます。

項目	説明
Index (1~65535)	イベントを指定します。
Description	ユーザ定義のイベントの記述を指定します。
Type	イベントタイプを指定します。 選択肢：「None」「Log」「SNMP Trap」「Log and Trap」 • None - イベントが発生しなかったことを示します。 • Log - イベントがログエントリであることを示します。 • Log and Trap - イベントがログエントリとトラップの両方であることを示します。
Community	イベントが所属するコミュニティを指定します。127 文字まで入力可能です。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

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

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

「Delete」をクリックします。

指定エントリのログ情報を表示する場合

「View Logs」をクリックします。以下の画面が表示されます。



図 7-24　Event Logs Table 画面

「Back」をクリックすると前ページへ移動します。

Telnet/Web（Telnet/Web 設定）

スイッチに Telnet/Web 設定をします。

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。

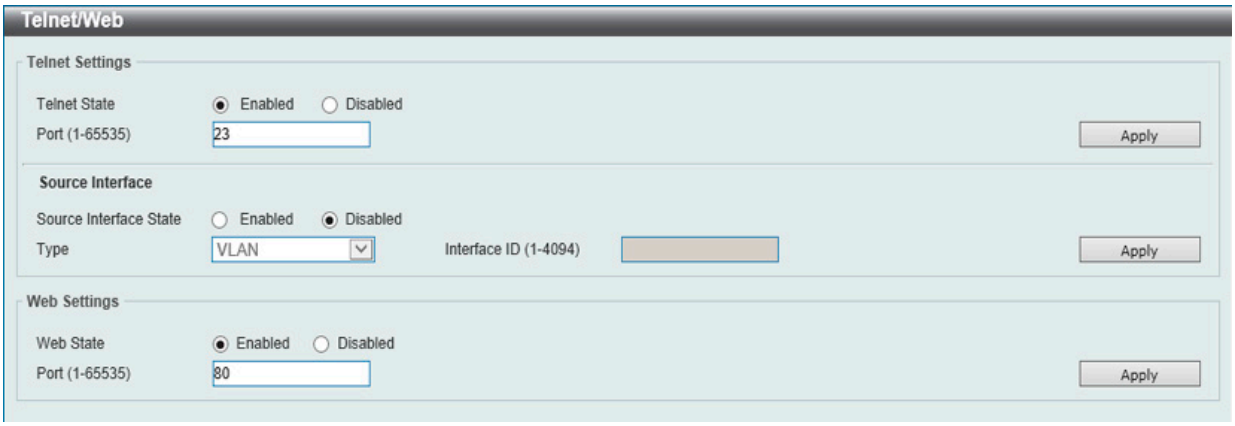


図 7-25　Telnet/Web Settings 画面

以下の項目が使用されます。

Telnet Settings

項目	説明
Telnet State	Telnet 設定は初期値で「Enabled」（有効）です。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。
Port (1-65535)	スイッチの Telnet マネジメントに使用される TCP ポート番号（1-65535）。Telnet プロトコルに通常使用される TCP ポートは 23 です。

「Apply」ボタンをクリックし、設定内容を適用してください。

Source Interface

項目	説明
Source Interface State	Source インタフェースの有効 / 無効を指定します。
Type	Source インタフェースの種類を指定します。「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。 「Loopback」選択時は 1-8、「Mgmt」選択時は 0 のみ、「VLAN」選択時は 1-4094 が選択可能です。

「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
Web State	Web ベースマネジメントは初期値で「Enabled」（有効）です。「Disabled」を選択し、ステータスを無効にすると、設定はすぐに適用され、Web インタフェースを使用したシステムの設定はできなくなります。
Port (1-65535)	スイッチの Web ベースマネジメントに使用される TCP ポート番号。Web プロトコルに通常使用される TCP ポートは 80 です。

「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。外向き（outgoing）セッションのタイムアウト値は、他スイッチの Telnet インタフェースに向けた、CLI 経由の「Console/Telnet/SSH」接続において使用されます。

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

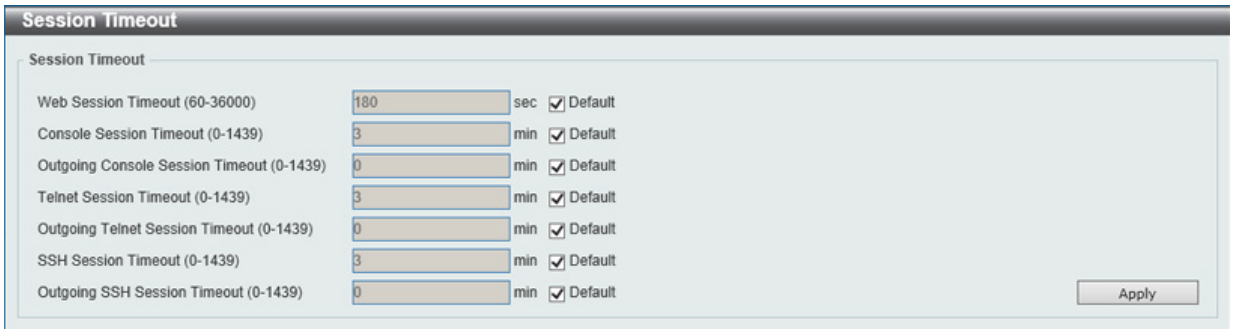


図 7-26　Session Timeout 画面

以下の項目が使用されます。

項目	説明
Web Session Timeout	Web セッションのタイムアウト時間（秒）を設定します。 「Default」にチェックを入れると初期値に戻ります。60 から 36000（秒）で設定可能です。初期値は 180 秒です。
Console Session Timeout	コンソールセッションのタイムアウト時間（分）を設定します。「Default」にチェックを入れると初期値に戻ります。0 から 1439（分）で設定可能です。0 に指定するとタイムアウトしません。初期値は 3 分です。
Outgoing Console Session Timeout	外向き（Outgoing）コンソールセッションのタイムアウト時間（分）を設定します。「Default」にチェックを入れると初期値に戻ります。0 から 1439（分）で設定可能です。0 に指定するとタイムアウトしません。初期値は 0 分です。
Telnet Session Timeout	Telnet セッションのタイムアウト時間（分）を設定します。「Default」にチェックを入れると初期値に戻ります。0 から 1439（分）で設定可能です。0 に指定するとタイムアウトしません。初期値は 3 分です。
Outgoing Telnet Session Timeout	外向き（Outgoing）Telnet セッションのタイムアウト時間（分）を設定します。「Default」にチェックを入れると初期値に戻ります。0 から 1439（分）で設定可能です。0 に指定するとタイムアウトしません。初期値は 0 分です。
SSH Session Timeout	SSH セッションのタイムアウト時間（分）を設定します。「Default」にチェックを入れると初期値に戻ります。0 から 1439（分）で設定可能です。0 に指定するとタイムアウトしません。初期値は 3 分です。
Outgoing SSH Session Timeout	外向き（Outgoing）SSH セッションのタイムアウト時間（分）を設定します。「Default」にチェックを入れると初期値に戻ります。0 から 1439（分）で設定可能です。0 に指定するとタイムアウトしません。初期値は 0 分です。

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（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。

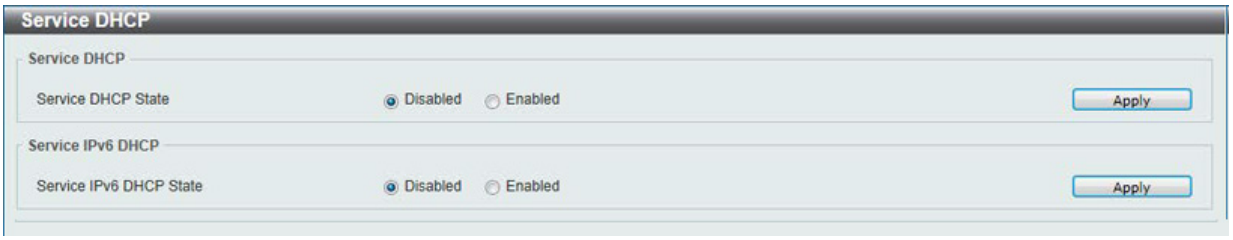


図 7-27　Service DHCP 画面

以下の項目が使用されます。

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）

スイッチの DHCP クラスとその合致する方式についての DHCP オプションについて表示、設定します。

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



図 7-28　DHCP Class Settings 画面

以下の項目が使用されます。

項目	説明
Class Name	DHCP クラス名を 32 文字までで指定します。

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

エントリの削除を行う場合

「Delete」をクリックします。

指定エントリの編集を行う場合

「Edit」をクリックします。以下の画面が表示されます。

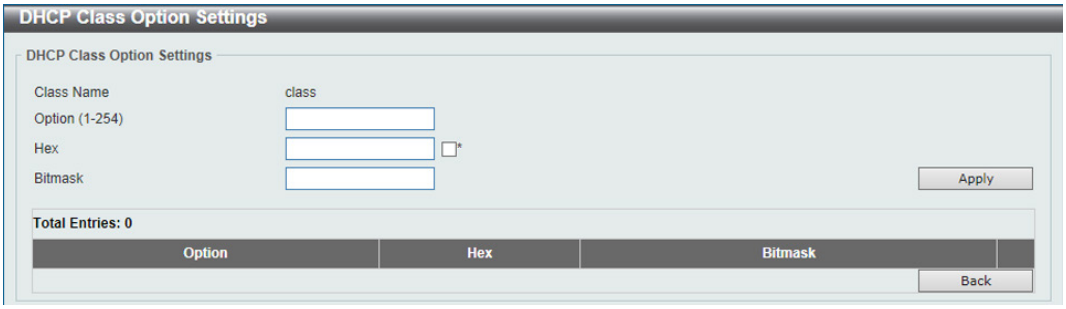


図 7-29　DHCP Class Option Settings（Edit）画面

以下の項目が使用されます。

項目	説明
Option	DHCP オプション番号をしてします。1-254 までで指定可能です。
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マッチされません。
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はマッチします。指定されない場合、16 進数のすべてのビットはチェックされます。

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。
「Back」をクリックすると前ページへ移動します。

エントリの削除を行う場合
「Delete」をクリックします。

DHCP Server（DHCP サーバ）

Management > DHCP > DHCP Server

DHCP（Dynamic Host Configuration Protocol）によってスイッチは、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 パラメータをこの情報を要求するデバイスに発行することができます。DHCP が有効なデバイスが起動すると、ローカルなネットワークに割り当てられます。このデバイスは DHCP クライアントであり、有効にすると、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、DHCP クライアントがローカル設定に利用する上記 IP 情報を含む応答をクライアントに返します。

ローカルに割り当てられたネットワークを利用するために、DHCP に関連する多くのパラメータを設定できます。これにより、割り当てた IP アドレスのリースタイム、DHCP プール内で許可されている IP アドレス範囲、ネットワークに同一のエントリを作成しないようにアドレスプール内の各 IP アドレスを排除する機能など自動 IP 設定を希望するクライアントの IP 設定をコントロールおよび制限します。また、DNS サーバまたはデフォルトルートの IP アドレスなどネットワークの別のデバイスに重要なデバイスの IP アドレスを割り当てることができます。

さらに、スタティック IP アドレスを必要とするネットワークメンテナンスに重要なデバイスの IP アドレスを同一に保つために、DHCP プール内の IP アドレスを指定した MAC アドレスに割り当てることができます。

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。

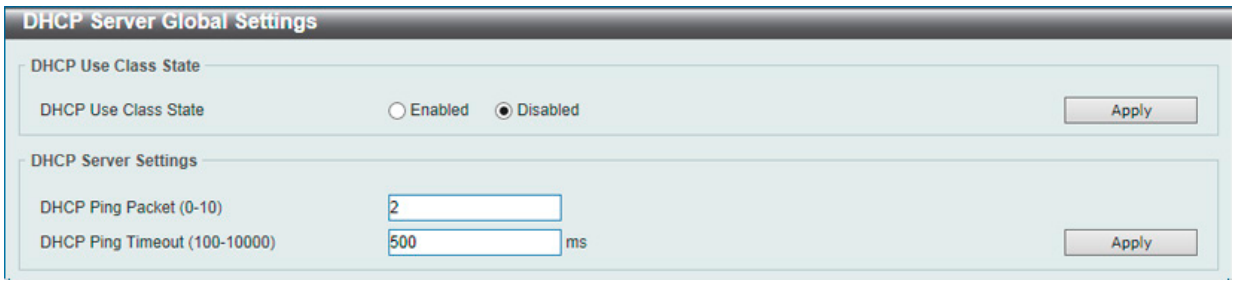


図 7-30　DHCP Server Global Settings 画面

以下のパラメータを設定できます。

パラメータ	説明
DHCP Use Class State	スイッチを DHCP サーバとしてグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
Ping Packets (0-10)	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（0-10）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。初期値は 2 パケットです。
Ping Timeout (10-10000)	ping パケットがタイムアウトになる前に DHCP サーバが待つ時間を選択します。初期値は 500 です。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

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

DHCP サーバプールの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 7-31　DHCP Server Pool Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Pool Name	DHCP サーバプール名を 32 字以内で入力します。

「Apply」ボタンをクリックし、設定内容を適用してください。
はじめに「Pool Name」欄に名前（半角英数字 12 文字以内）を入力して、「Add」をクリックすることによって、プールを作成します。一度作成されると、対応する「Edit Class」「Edit Option」「Configure」ボタンをクリックして、プールの設定を編集することができます。
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。

エントリの削除
「Delete」ボタンをクリックして、指定エントリを削除します。

エントリの編集（Edit Class）

「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。

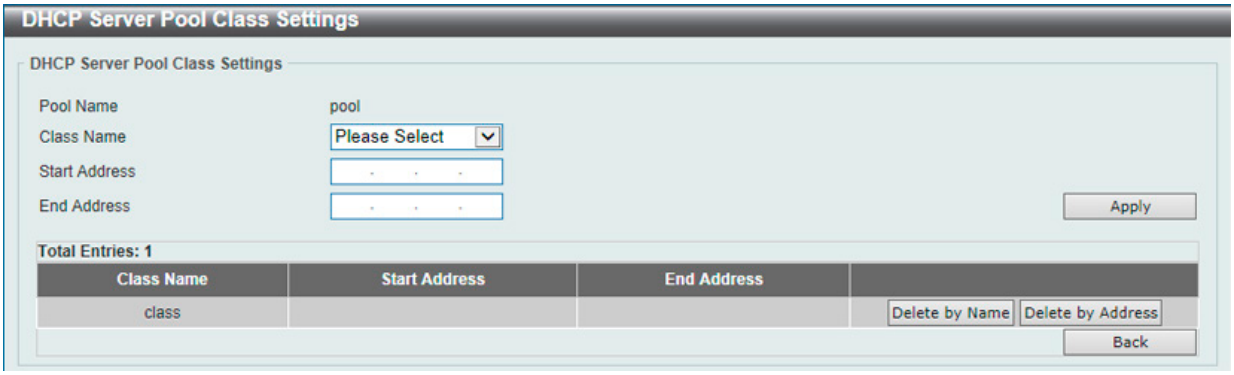


図 7-32　DHCP Server Pool Settings（Edit Class）画面

以下の項目を使用して設定、表示を行います。

項目	説明
Pool Name	パラメータを調整する DHCP プール名を表示します。
Class Name	対応する DHCP クラス名を指定します。
Start Address	DHCP クラスの開始 IPv4 アドレスを指定します。
End Address	DHCP クラスの終了 IPv4 アドレスを指定します。

「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 DHCP クラスを名前で削除します。
「Delete by Address」をクリックすると DHCP クラスをアドレスで削除します。
「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（Edit Option）

「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 7-33　DHCP Server Pool Settings（Edit Option）画面

以下の項目を使用して設定、表示を行います。

項目	説明
Pool Name	パラメータを調整する DHCP プール名を表示します。
Option	DHCP オプション番号（1-254）を指定します。
Type	DHCP オプションタイプを「ASCII」「Hex」「IP」から選択し、入力します。 • ASCII -「ASCII」文字列で入力します。最大 255 文字まで入力可能です。 • HEX - 16 進数文字列で入力します。最大 254 文字まで入力可能です。 • 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。

「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックすると指定の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（Configure）

「Configure」ボタンをクリックすると、以下の画面が表示されます。

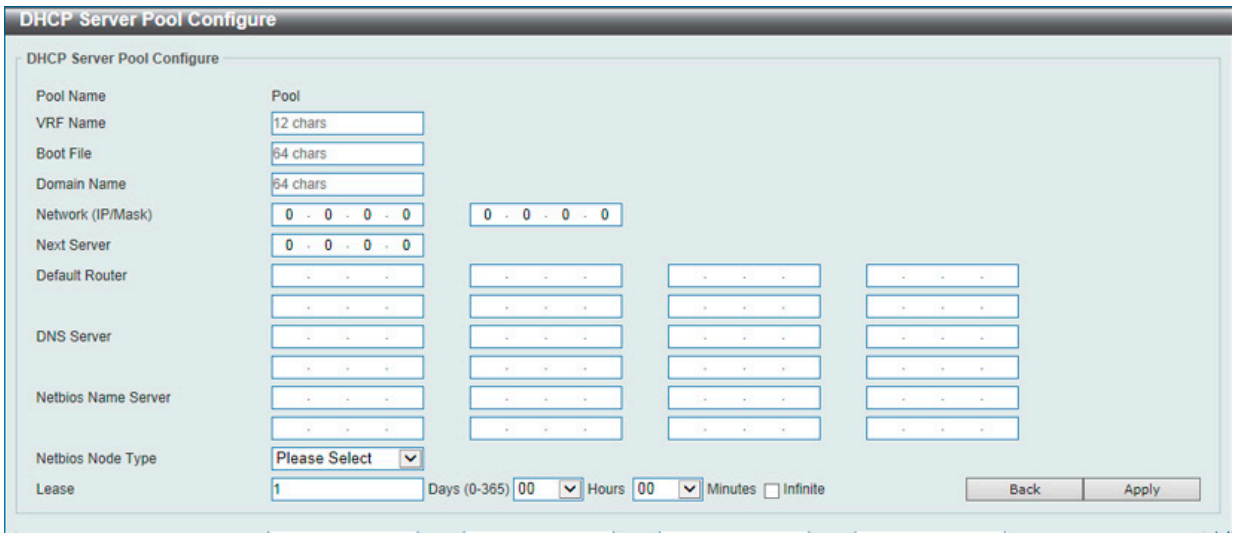


図 7-34　DHCP Server Pool Settings (Configure) 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Pool Name	パラメータを調整する DHCP プール名を表示します。
VRF Name	VRF インスタンス名を 12 文字以内で入力します。
Boot File	ブートイメージのファイル名（64 字以内）を指定します。
Domain Name	クライアントのドメイン名（64 字以内）を入力します。
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 DHCP クライアントに検索されます。TFTP サーバである必要があります。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	デフォルトルータの IP アドレス。DHCP クライアントに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。ルータは推奨される順に表示されます。デフォルトルータが既に設定済みの場合、あとで設定されたデフォルトルータがデフォルトインタフェースリストに追加されます。
DNS Server	DNS サーバの IP アドレス。DHCP クライアントが使用可能である 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 サーバは推奨される順に表示されます。DNS サーバが既に設定済みの場合、あとで設定された DNS サーバが DNS サーバリストに追加されます。
NetBIOS Name Server	WINS サーバの IP アドレス。WINS(Windows Internet Naming Service) は、マイクロソフト DHCP クライアントが通常グループ分けされているネットワーク内の IP アドレスにホスト名を関連付けるために使用する名前解決サービスです。最大 8 つの IP アドレスを指定できます。
NetBIOS Node Type	マイクロソフト DHCP クライアントの NetBIOS のノードタイプを設定します。プルダウンメニューを使用して、4 つのノードタイプ（Broadcast、Peer to Peer、Mixed および Hybrid）から選択します。「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）システムは、「point-to-point name queries」のみをネームサーバ（WINS）に使用します。「Mixed」（h-nod）システムは、まずブロードキャストを先に抽出し、その後ネームサーバを抽出します。「Hybrid」はまずネームサーバを先に抽出し、その後ブロードキャストを抽出します。「Hybrid」が推奨されます。
Lease	初期値では、DHCP サーバに割り当てられる各 IP アドレスのリース期間（アドレスが有効であることの時間）は 1 日です。 • Days - リースする日（0-365） • Hours - リースする時間（時） • Minutes - リースする時間（分） • Infinite - リース期間が無制限

「Apply」ボタンをクリックし、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に割り当てない IP アドレスを指定します。除外する複数のグループを定義するために本コマンドを繰り返して使用します。DHCP サーバは、DHCP プールサブネットにあるすべての IP アドレスを DHCP クライアントに割り当てることができるものとします。

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 7-35　DHCP Server Exclude Address 画面

以下の項目を使用して設定、表示を行います。

項目	説明
VRF Name	VRF インスタンス名を 12 文字以内で入力します。
Begin Address	除外する開始 IP アドレスを指定します。
End Address	除外する終了 IP アドレスを指定します。

IP アドレスまたは IP アドレス範囲を設定するために、範囲の「Begin Address」（開始アドレス）と「End Address」（終了アドレス）を入力し、「Add」ボタンをクリックします。設定したアドレス範囲は以下の画面下半分に表示されます。

エントリの削除
「Delete」ボタンをクリックして、指定エントリを削除します。

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。クライアントの IP アドレスを管理者が手動で割り当てるか、または DHCP サーバがプールから自動的に割り当てることができます。プールネットワークのアドレスからクライアントに IP アドレスを割り当てると、ダイナミックバインディングエントリが作成されます。

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。

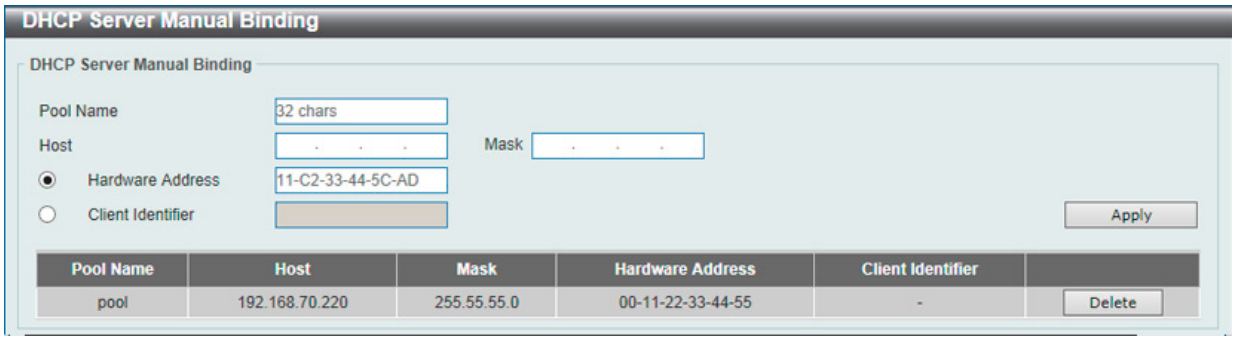


図 7-36　DHCP Server Manual Binding 画面

以下の項目を使用して設定、表示を行います。

項目	説明
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。
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 ホスト識別子の 16 進数表記について指定します。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。

「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。
「Delete」をクリックすると指定のエントリを削除します。

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

DHCP サーバダイナミックバインディングテーブルの表示と削除を行います。

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。

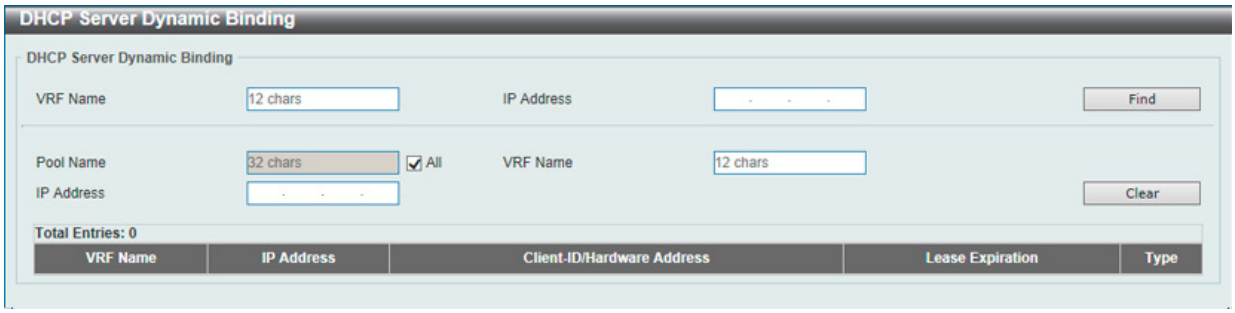


図 7-37　DHCP Server Dynamic Binding 画面

表示されるテーブルの各項目は以下の通りです。

パラメータ	説明
VRF Name	VRF インスタンス名を 12 文字以内で入力します。
IP Address	本スイッチの DHCP サーバ機能によってこのデバイスに割り当てられた IP アドレスを表示します。
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表示します。

「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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。

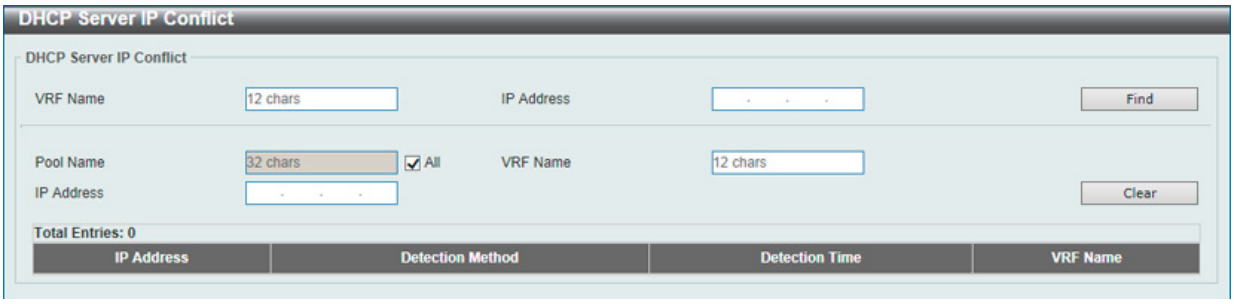


図 7-38　DHCP Conflict IP 画面

表示されるテーブルの各項目は以下の通りです。

パラメータ	説明
VRF Name	VRF インスタンス名を 12 文字以内で入力します。
IP Address	クリア / 登録された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表示します。

「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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。

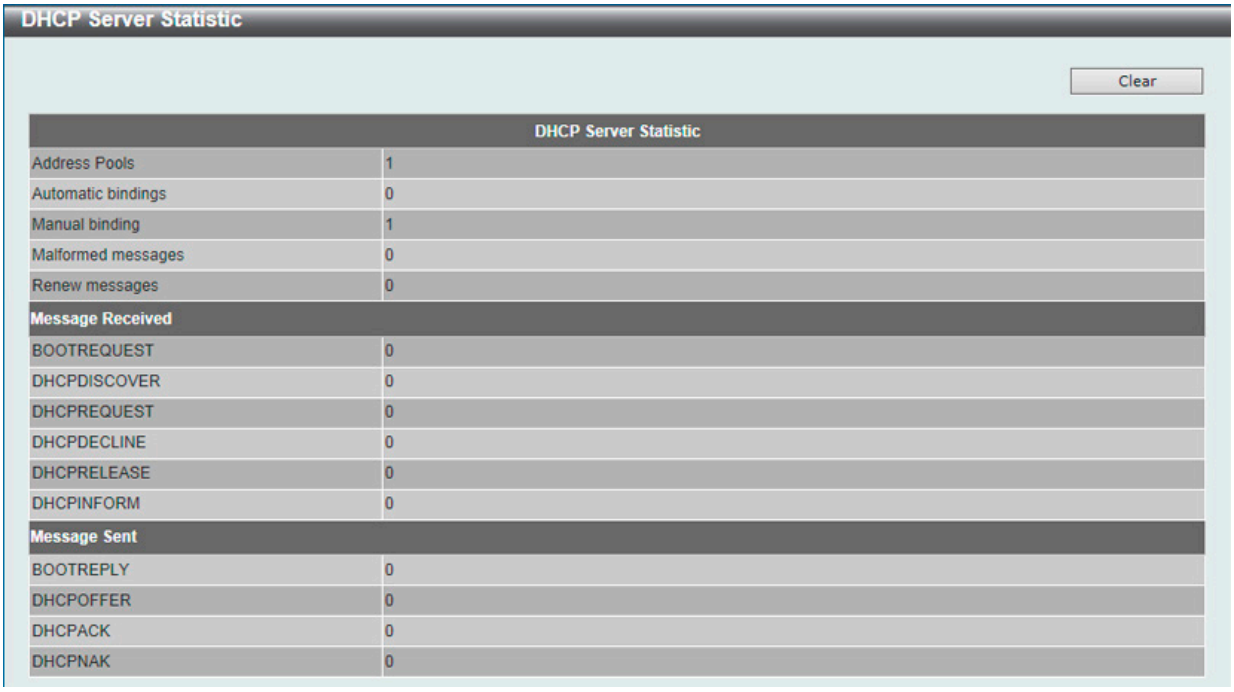


図 7-39　DHCP Server Statistic 画面

「Clear」ボタンをクリックして、エントリをクリアします。

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 7-40　DHCPv6 Server Pool Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Pool Name	DHCPv6 サーバプール名を入力します。

「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、入力した情報に基づいて指定エントリを削除します。
「Configure」ボタンをクリックして、該当エントリの編集を行います。
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（Configure）

「Configure」ボタンをクリックすると、以下の画面が表示されます。

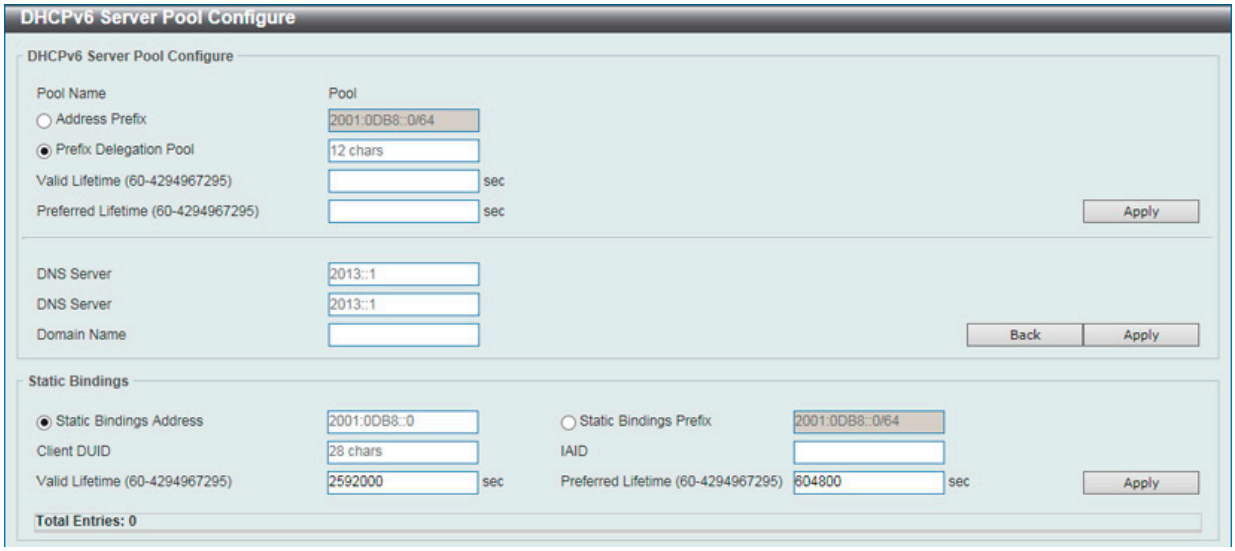


図 7-41　DHCPv6 Server Pool Settings (Configure) 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCPv6 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）
Prefix Delegation Pool	DHCPv6 サーバプールプレフィクス委任名を 12 字以内で入力します。
Valid Lifetime (60-4294967295)	指定プールに基づいた IPv6 アドレスが有効な状態を維持する時間 (秒) を入力します。初期値は「2592000」（30 日）です。
Preferred Lifetime (60-4294967295)	指定プールに基づいた IPv6 アドレスが preferred-lifetime 状態を維持する時間 (秒) を入力します。初期値は「604800」（7 日）です。
DNS Server	このプールに対する DNS サーバの IPv6 アドレスを入力します。
Domain Name	ドメイン名は、DNS と共にホスト名を解決する場合に DHCPv6 クライアントに使用されます。
Static Bindings	
Static Bindings Address	指定クライアントにアサインす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。

項目	説明
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 28 字以内で入力します。
IAID	「Identity Association Identifier」(IAID/IA 識別子) を入力します。IAID 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）の集合体を固有に識別します。
Valid Lifetime (60-4294967295)	指定プールに基づいた IPv6 アドレスが有効な状態を維持する時間 (秒) を入力します。初期値は「2592000」（30 日）です。
Preferred Lifetime (60-4294967295)	指定プールに基づいた IPv6 アドレスが preferred-lifetime 状態を維持する時間 (秒) を入力します。初期値は「604800」（7 日）です。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

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

DHCPv6 サーバローカルプールの表示および設定を行います。

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

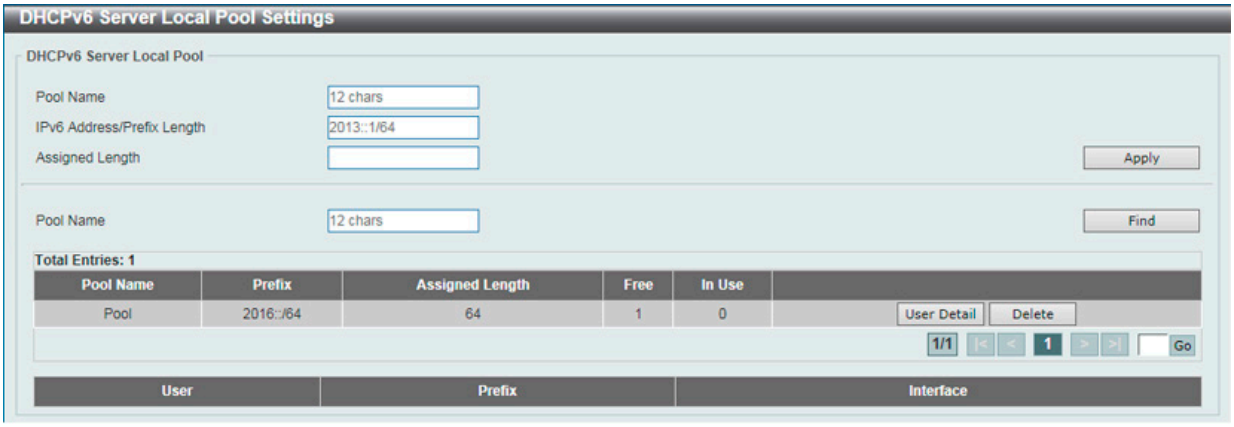


図 7-42　DHCPv6 Server Local Pool Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Pool Name	DHCPv6 サーバプール名を入力します。
IPv6 Address / Prefix Length	IPv6 プレフィクスアドレスとプレフィクス長を入力します。
Assigned Length	プール内のユーザに委任されるプレフィクス長を入力します。アサイン長の値はプレフィクス長の値より長い必要があります。

「Apply」ボタンをクリックして、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、入力した情報に基づいて指定エントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「User Detail」をクリックするとユーザについての詳細が表示されます。
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。

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

DHCPv6 サービスを希望するクライアントに割り当てない IPv6 アドレスの範囲を設定します。DHCPv6 サーバ、スイッチの IPv6 アドレスも含め、全アドレスをクライアントへアサインすることが可能です。本画面では IPv6 アドレス / アドレス範囲をアサインメントから除外します。除外されたアドレスはアドレスアサインメントにのみプールされます。

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。

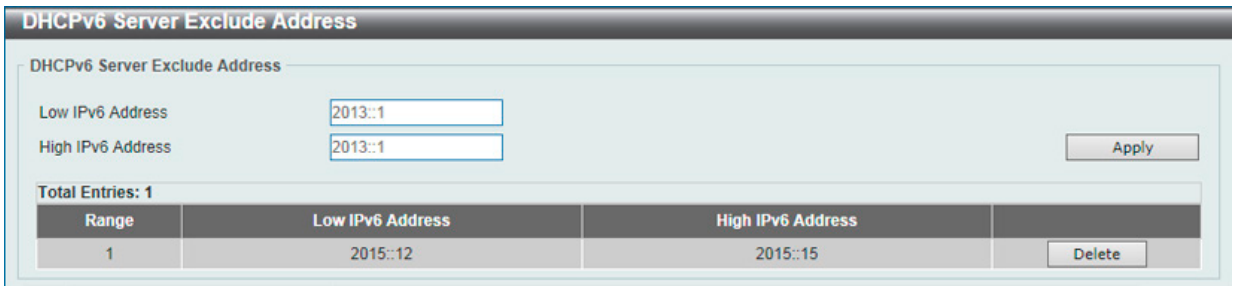


図 7-43　DHCPv6 Server Excluded Address Settings 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定の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、クリアします。

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

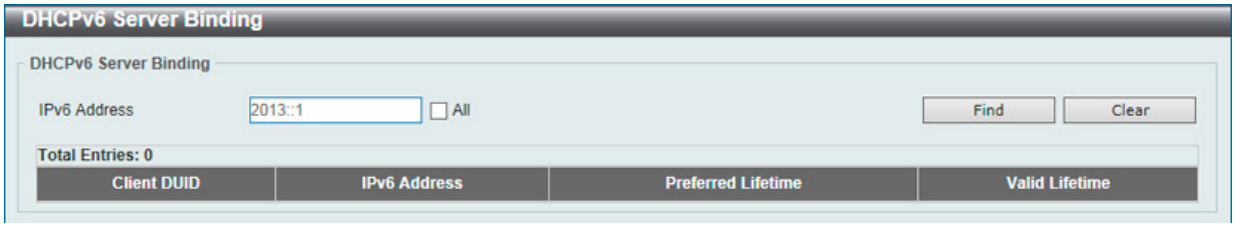


図 7-44　DHCPv6 Server Binding 画面

以下の項目を使用して設定、表示を行います。

項目	説明
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、入力した情報に基づく特定のエントリを検出します。
「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。

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

インタフェースごとに DHCPv6 サーバ状態を表示および設定します。

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

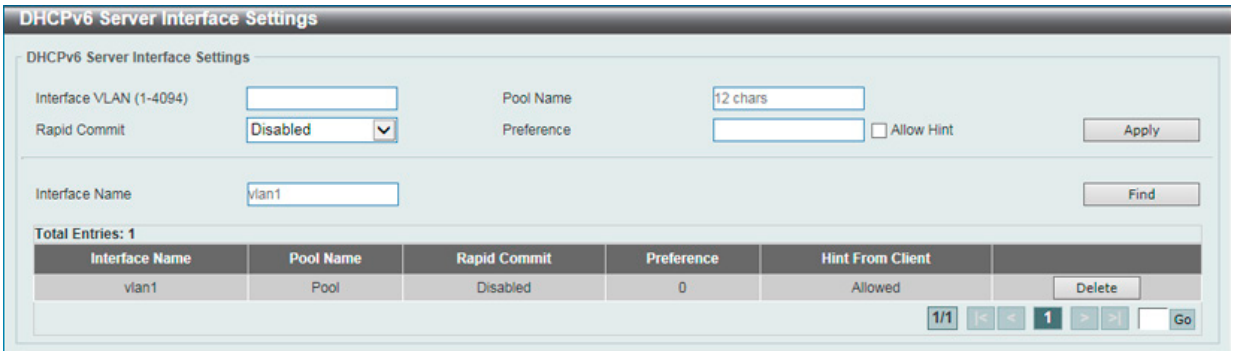


図 7-45　DHCPv6 Server Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface VLAN	インタフェース VLAN を指定します。1-4094 の間で指定可能です。
Pool Name	DHCPv6 サーバプール名を入力します。
Rapid Commit	2 メッセージ交換の有効 / 無効を指定します。初期値は無効です。
Preference	希望値を指定します。「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。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
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。

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。

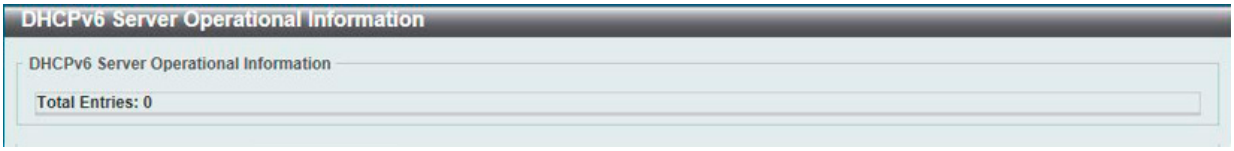


図 7-46　DHCPv6 Server Operational Information 画面

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。

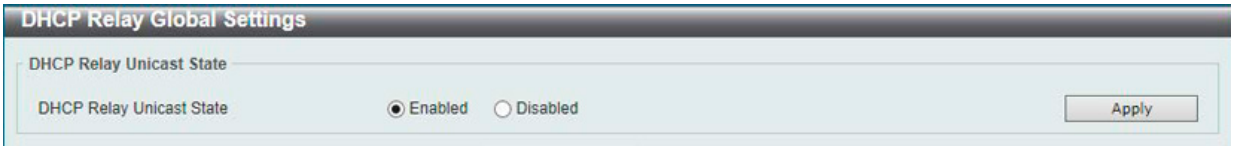


図 7-47　DHCP Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCP Relay Unicast State	DHCP リレーユニキャストをグローバルに有効 / 無効に指定します。

「Apply」をクリックし、設定内容を適用します。

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。

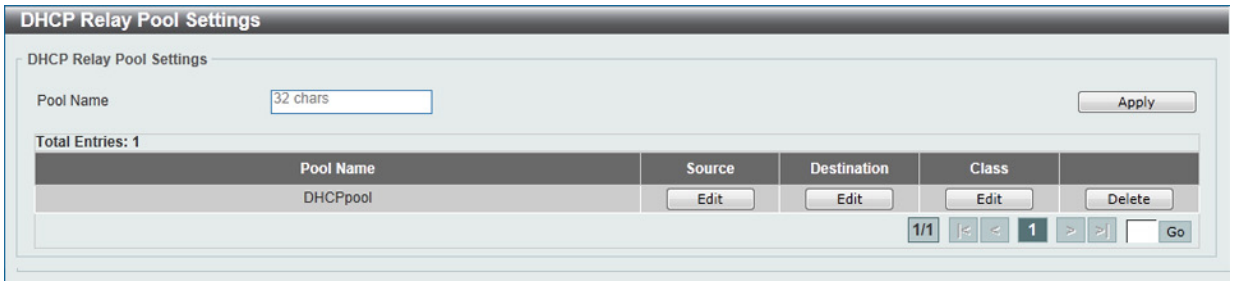


図 7-48　DHCP Relay Pool Settings 画面

以下の項目が使用されます。

項目	説明
Pool Name	32 文字以内でプール名を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

各プールエントリの編集を行う（Edit）

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

「Source」の編集を行う場合

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

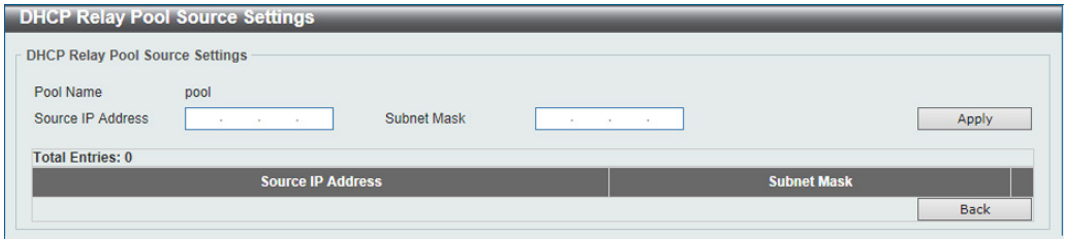


図 7-49　DHCP Relay Pool Source Settings 画面

以下の項目が使用されます。

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。
エントリの削除を行う際は「Delete」をクリックします。
「Back」をクリックすると前の画面へ戻ります。

「Destination」の編集を行う場合

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

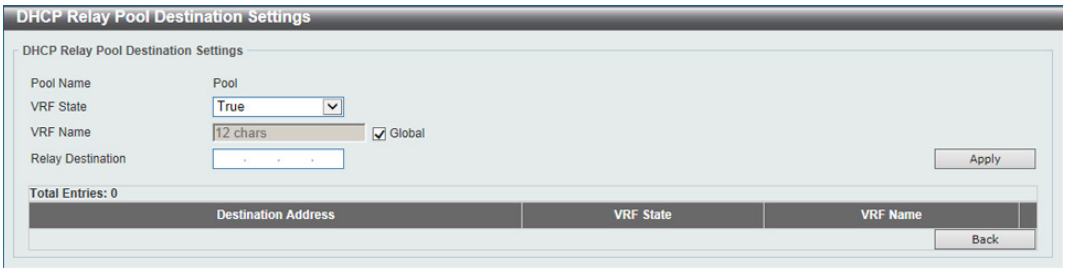


図 7-50　DHCP Relay Pool Destination Settings 画面

以下の項目が使用されます。

項目	説明
VRF State	VRF の状態を指定します。「True」「False」から指定可能です。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Global」オプションを使用するとグローバルアドレスから IP アドレスを指定します。
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。
エントリの削除を行う際は「Delete」をクリックします。
「Back」をクリックすると前の画面へ戻ります。

「Class」の編集を行う場合

「Class」下の「Edit」をクリックします。以下の画面が表示されます。

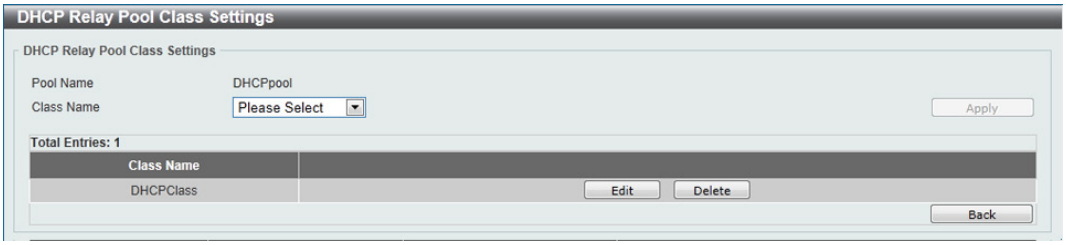


図 7-51　DHCP Relay Pool Class Settings 画面

以下の項目が使用されます。

項目	説明
Class Name	DHCP クラスの名前です。

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。
エントリの削除を行う際は「Delete」をクリックします。
「Back」をクリックすると前の画面へ戻ります。

クラス名の横の「Edit」ををクリックすると以下の画面が表示されます。

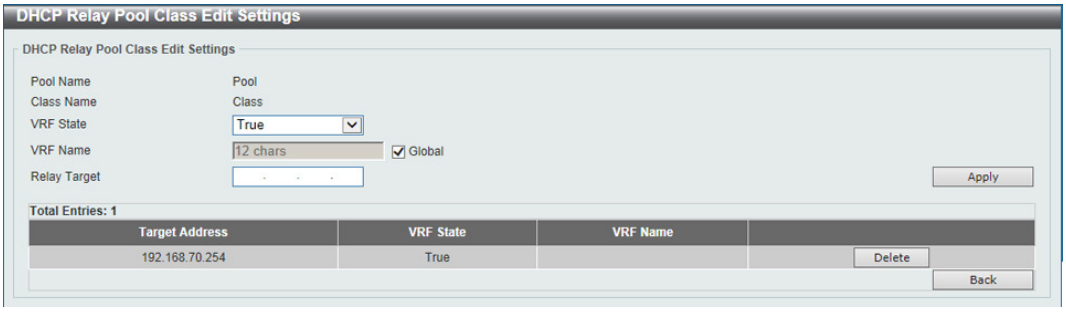


図 7-52　DHCP Relay Pool Class Settings 画面

以下の項目が使用されます。

項目	説明
VRF State	VRF の状態を指定します。「True」「False」から指定可能です。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Global」オプションを使用するとグローバルアドレスから IP アドレスを指定します。
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。
エントリの削除を行う際は「Delete」をクリックします。
「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。

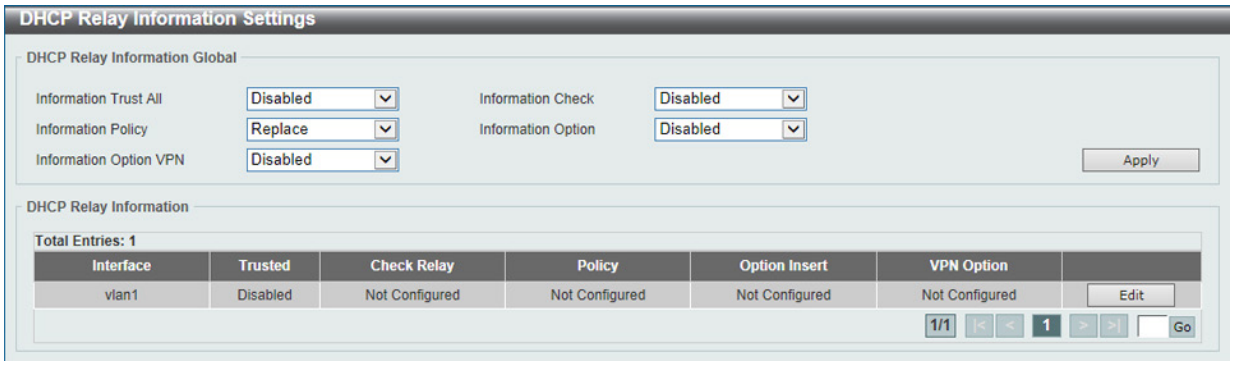


図 7-53　DHCP Relay Information Settings 画面

以下の項目が使用されます。

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 リレーパケットにあるリレーエージェントインフォメーションの破棄、または有効化を有効 / 無効に設定します。
Information Policy	「Replace」、「Drop」または「Keep」を選択します。初期値は「Replace」です。 • 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。 • 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のリレーの間にリレーエージェント情報（Option82）を挿入を有効 / 無効に設定します。
Information Option VPN	VPN 機能の情報オプションを有効 / 無効にします。DHCP リクエストパケットのリレーにおけるインタフェースの VPN 関連サブオプションの挿入を有効 / 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。
「Edit」をクリックして対応するインタフェースの編集を行うことができます。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

DHCP 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。

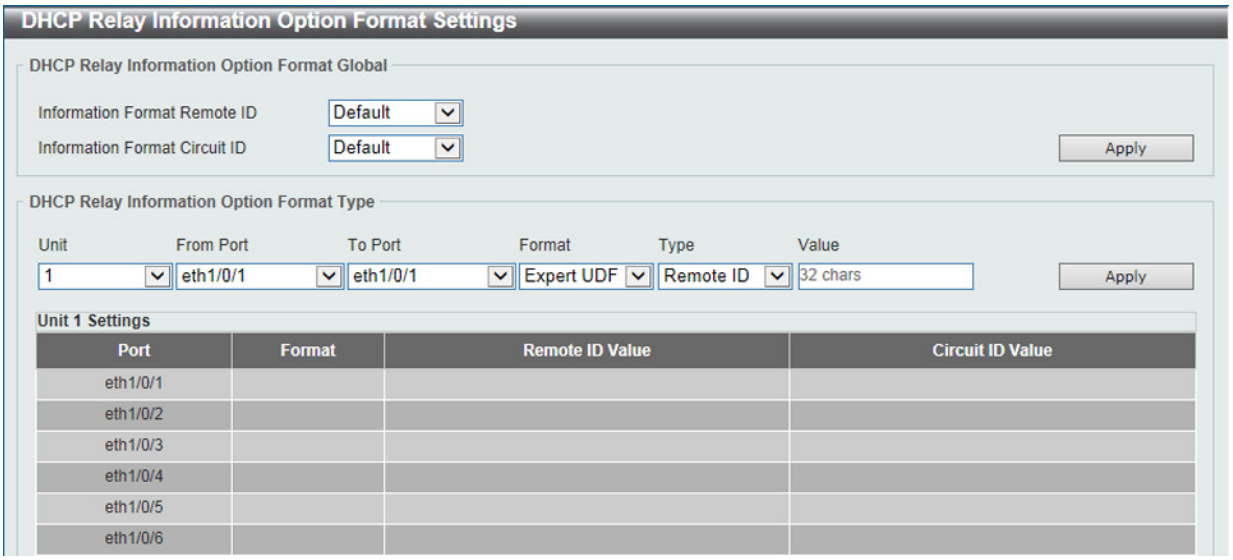


図 7-54　DHCP Relay Information Option Format Settings 画面

以下の項目が使用されます。

DHCP Relay Information Option Format Global

項目	説明
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 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。

設定を変更する際は、必ず「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 Information Option Format Type

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポートの始点 / 終点を設定します。
Format	「DHCP information circuit ID」のフォーマットを選択します。「Vendor3」を選択できます。
Type	「DHCP information circuit ID」の種類を選択します。「Remote ID」「Circuit ID」を選択できます。
Value	ベンダ定義の文字列を入力します。32 字まで指定可能です。

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

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。

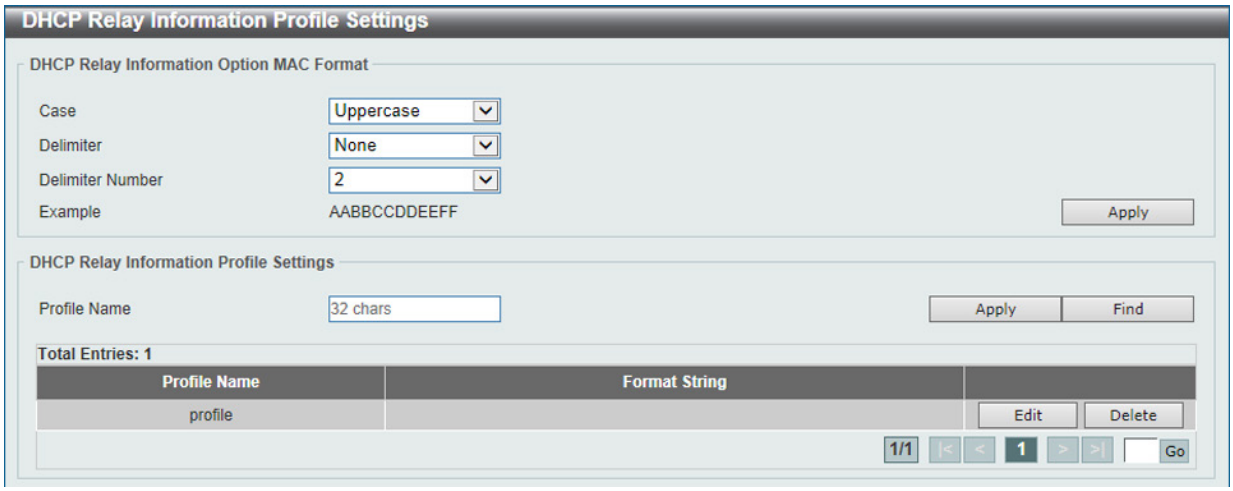


図 7-55　DHCP Relay Information Profile Settings 画面

以下の項目が使用されます。

項目	説明
DHCP 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「Uppercase」（大文字）または「Lowercase」（小文字）から選択します。（例 ;aa-bb-cc-dd-ee-ff（Lowercase）/AA-BB-CC-DD-EE-FF（Uppercase））
Delimiter	MAC アドレスを入力する際の区切り「Hyphen」（ハイフン）、「Colon」（コロン）または「Dot」（ドット）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 -「AA-BB-CC-DD-EE-FF」 • Colon -「AA:BB:CC:DD:EE:FF」 • Dot -「AA.BB.CC.DD.EE.FF」 • None -「AABBCCDDEEFF」
Delimiter Number	MAC アドレスにおける区切り数を選択します。「1」「2」「5」から指定します。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」
DHCP Relay Information Profile Settings	
Profile Name	オプション 82 のプロファイル名を入力します。
Format String	「Edit」をクリックし、ユーザ定義のオプション 82 フォーマット文字列を指定します。251 文字まで指定できます。ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた "Ethernet" のような形になります。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列、または 16 進数のどちらも含むことができます。 • 「%」後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。文字長オプションに対してフォーマットキー文字列の対応方法を設定します。「$」はスペースを埋め（0x20）、「0」は（0）を埋めます。「0」が初期値です。（オプション） • 「1-32」は文字長オプションです。どれくらいの文字やバイトがキー文字列に変換されるのかを指定します。もし変換済みキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。（オプション） • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。: • 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。 • 「sysname」はスイッチのシステム名を意味します。最大文字長は 128 です。ASCII 文字列のみ有効です。 • 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。

項目	説明
	• 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例，「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 • 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例，「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 • 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデバイスの場合、ユニット ID は「ip dhcp relay information option format remote-id」、そして「ip dhcp relay information option format circuit-id」コマンドで設定されます。 • 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 • 「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 • 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 • 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 • 「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合 (:) は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットキー文字列のいかなる組み合わせも可能です。「\」はエスケープキャラクターになります。「\」以後の特別なキャラクターはキャラクターそのものになります。例えば「\%」は「%」を意味します。フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列内のスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

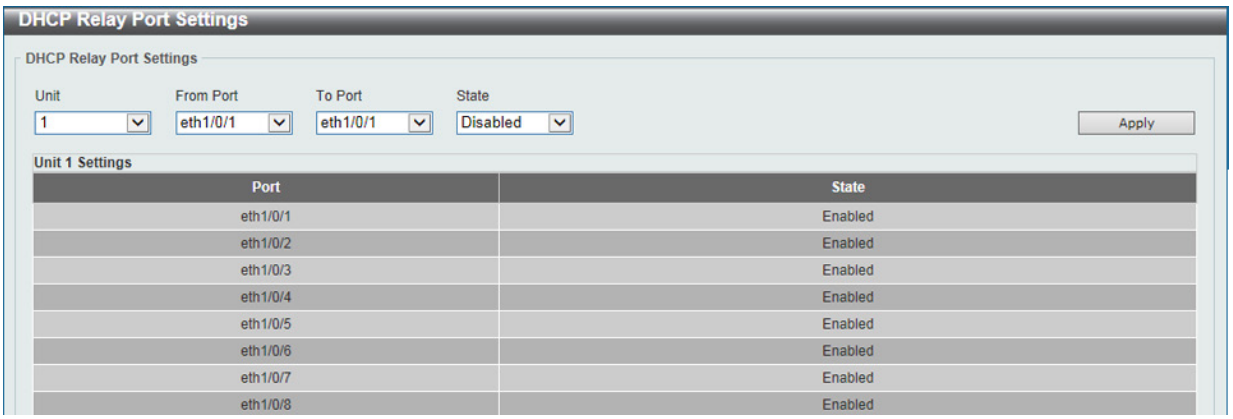


図 7-56　DHCP Relay Port Settings 画面

以下の項目が使用されます。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
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。

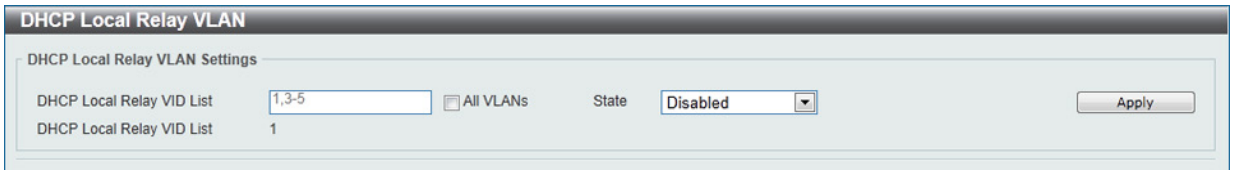


図 7-57　DHCP Local Relay VLAN 画面

以下の項目が使用されます。

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。

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。

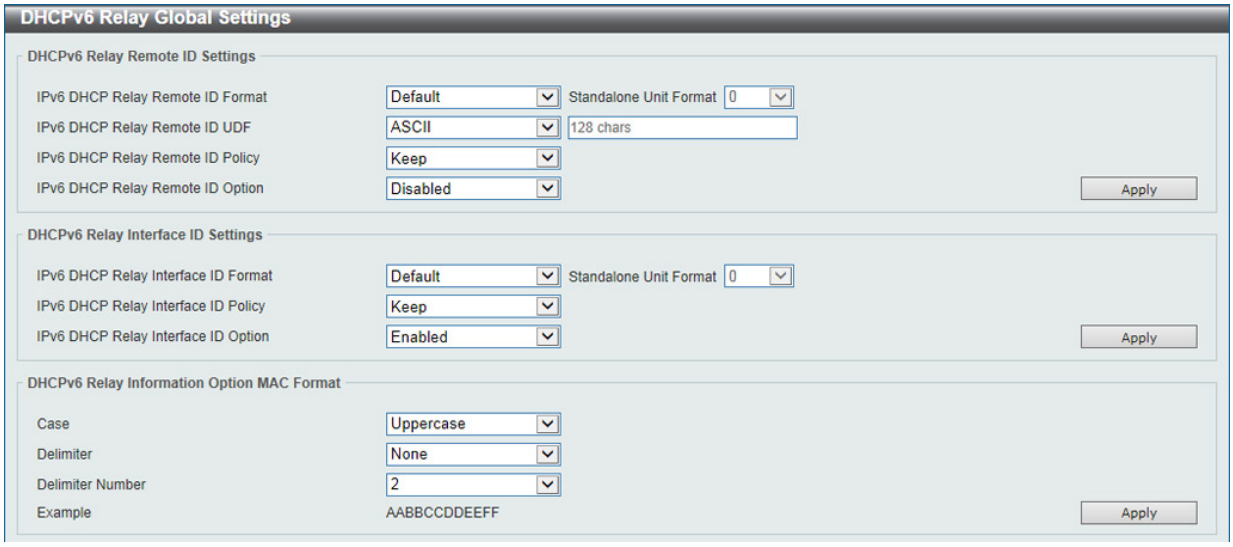


図 7-58　DHCPv6 Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCPv6 Relay Remote ID Settings	
IPv6 DHCP Relay Remote ID Format	リモート ID のサブタイプを指定します。 「Default」「CID With User Define」「User Define」「Expert UDF」から選択します。
Standalone Unit Format	「Expert UDF」を選択すると、ここでスタンドアロンユニットのフォーマットを選択します。「0」「1」が選択可能です。
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」「Hex」から選択します。 • ASCII -「ASCII」文字列で入力します。最大 128 文字まで入力可能です。 • HEX - 16 進数文字列で入力します。最大 256 文字まで入力可能です。
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」「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 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。

項目	説明
IPv6 DHCP Relay Remote ID Option	DHCP IPv6 リクエストパケットのリレーの間にリレーエージェント情報（Option37）の挿入を有効 / 無効に設定します。
DHCPv6 Relay Interface ID Settings	
IPv6 DHCP Relay Interface ID Format	インタフェース ID のフォーマットを指定します。 「Default」「CID」「User Define」「Vendor1」「Expert UDF」から選択します。
Standalone Unit Format	「Expert UDF」を選択すると、ここでスタンドアロンユニットのフォーマットを選択します。「0」「1」が選択可能です。
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のリレーの間にリレーエージェント情報（Option18）を挿入を有効 / 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「Uppercase」（大文字）または「Lowercase」（小文字）から選択します。（例 ;aa-bb-cc-dd-ee-ff（Lowercase）/AA-BB-CC-DD-EE-FF（Uppercase））
Delimiter	MAC アドレスを入力する際の区切り「Hyphen」（ハイフン）、「Colon」（コロン）または「Dot」（ドット）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 -「AA-BB-CC-DD-EE-FF」 • Colon -「AA:BB:CC:DD:EE:FF」 • Dot -「AA.BB.CC.DD.EE.FF」 • None -「AABBCCDDEEFF」
Delimiter Number	MAC アドレスにおける区切り数を選択します。「1」「2」「5」から指定します。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」

「Apply」ボタンをクリックし、設定を適用します。

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

DHCPv6 リレーインタフェース設定の表示と設定を行います。

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

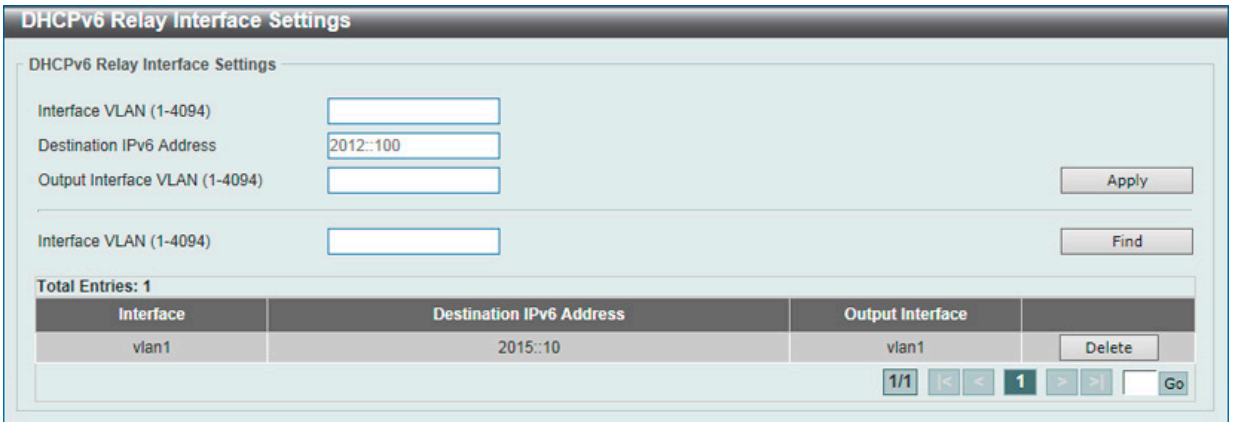


図 7-59　DHCPv6 Relay Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface VLAN	DHCPv6 リレーの VLAN を 1 から 4094 の間で指定します。
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入力します。

「Apply」ボタンをクリックし、設定を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

DHCPv6 リレーリモート ID プロファイル設定の表示と設定を行います。DHCPv6 リレーオプション 82 のプロファイルの作成に使用されます。

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



図 7-60　DHCPv6 Relay Remote ID Profile Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Profile Name	オプション 82 のプロファイル名を入力します。
Format String	「Edit」をクリックし、ユーザ定義のオプション 82 フォーマット文字列を指定します。251 文字まで指定できます。ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた "Ethernet" のような形になります。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":」のように ASCII 文字列、または 16 進数のどちらも含むことができます。 　• 「%」後の文字列はフォーマットされたキー文字列を意味します。 　• 「$」または「0」はフィルインディケータです。文字長オプションに対してフォーマットキー文字列の対応方法を設定します。「$」はスペースを埋め（0x20）、「0」は（0）を埋めます。「0」が初期値です。（オプション） 　• 「1-32」は文字長オプションです。どれくらいの文字やバイトがキー文字列に変換されるのかを指定します。もし変換済みキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。（オプション） 　• 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。: 　　• 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。 　　• 「sysname」はスイッチのシステム名を意味します。最大文字長は 128 です。ASCII 文字列のみ有効です。 　　• 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。 　　• 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例 , 「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 　　• 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例 , 「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 　　• 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデバイスの場合、ユニット ID は「ip dhcp relay information option format remote-id」、そして「ip dhcp relay information option format circuit-id」コマンドで設定されます。 　　• 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 　　• 「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 　　• 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 　　• 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 　• 「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合 (:) は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットキー文字列のいかなる組み合わせも可能です。「\」はエスケープキャラクターになります。「\」以後の特別なキャラクターはキャラクターそのものになります。例えば「\%」は「%」を意味します。フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列内のスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
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。

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

DHCPv6 リレーインタフェース ID プロファイル設定の表示と設定を行います。DHCPv6 リレーオプション 82 のプロファイルを作成に使用されます。

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



図 7-61　DHCPv6 Relay Interface ID Profile Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Profile Name	オプション 82 のプロファイル名を入力します。

Format String	「Edit」をクリックし、ユーザ定義のオプション 82 フォーマット文字列を指定します。251 文字まで指定できます。ルールは次の通りです。
	
	• 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた "Ethernet" のような形になります。ダブルコーテーションに括られない文字は 16 進数として認識されます。
	• フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列、または 16 進数のどちらも含むことができます。
	  • 「%」後の文字列はフォーマットされたキー文字列を意味します。
	  • 「$」または「0」はフィルインディケータです。文字長オプションに対してフォーマットキー文字列の対応方法を設定します。「$」はスペースを埋め（0x20）、「0」は（0）を埋めます。「0」が初期値です。（オプション）
	  • 「1-32」は文字長オプションです。どれくらいの文字やバイトがキー文字列に変換されるのかを指定します。もし変換済みキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。（オプション）
	  • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。：
	  • 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。
	  • 「sysname」はスイッチのシステム名を意味します。最大文字長は 128 です。ASCII 文字列のみ有効です。
	  • 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。
	  • 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例，「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。
	  • 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例，「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。
	  • 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデバイスの場合、ユニット ID は「ip dhcp relay information option format remote-id」、そして「ip dhcp relay information option format circuit-id」コマンドで設定されます。
	  • 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。
	  • 「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。
	  • 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。
	  • 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。

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

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
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。

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。

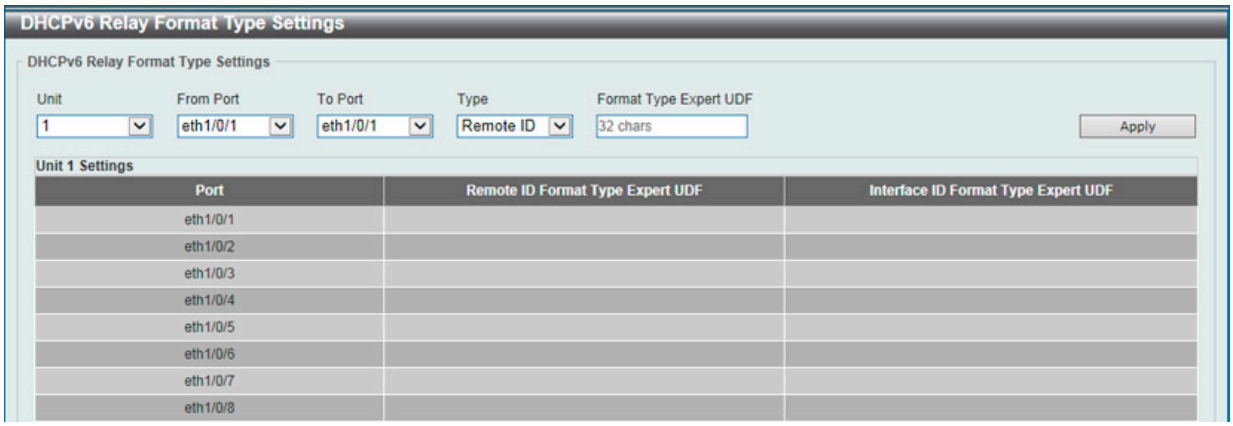


図 7-62　DHCPv6 Relay Format Type Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
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。

「Apply」ボタンをクリックし、設定を適用します。

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

DHCPv6 リレーポート設定を行います。

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

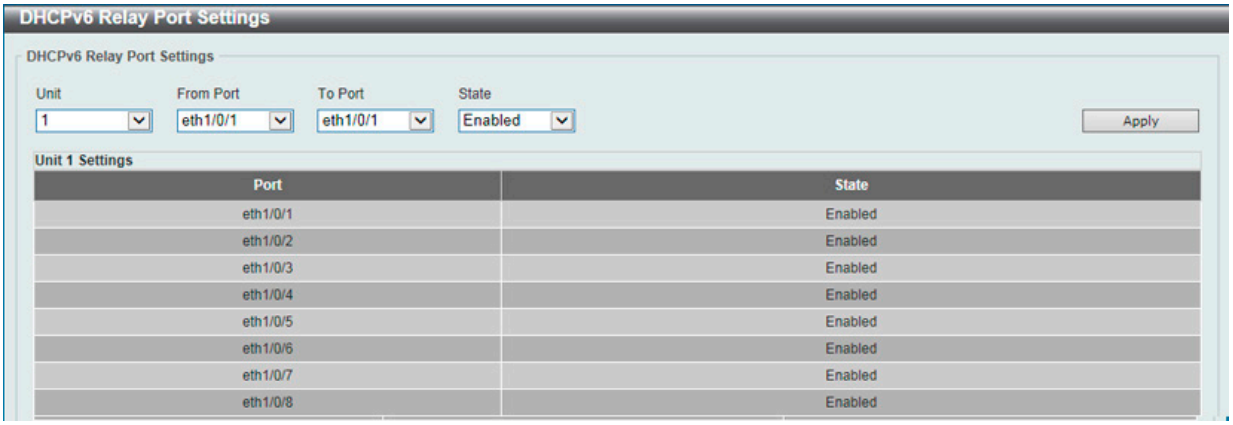


図 7-63　DHCPv6 Relay Port Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
State	指定ポートの DHCPv6 リレーポート機能を有効 / 無効に指定します。

「Apply」ボタンをクリックし、設定を適用します。

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

DHCPv6 ローカルリレー VLAN 設定を行います。DHCPv6 ローカルリレーが有効の場合、クライアントからのリクエストパケットにオプション 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 37DHCPv6 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。

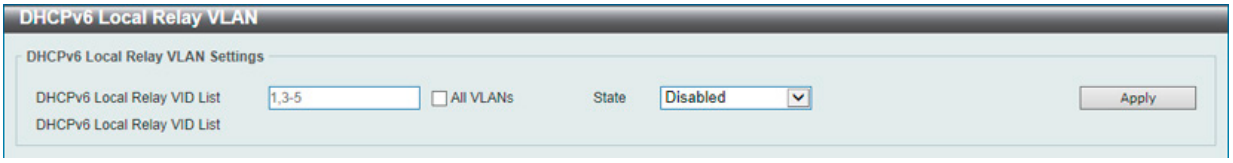


図 7-64　DHCPv6 Local Relay VLAN 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCPv6 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 / 無効に指定します。

「Apply」ボタンをクリックし、設定を適用します。

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

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。

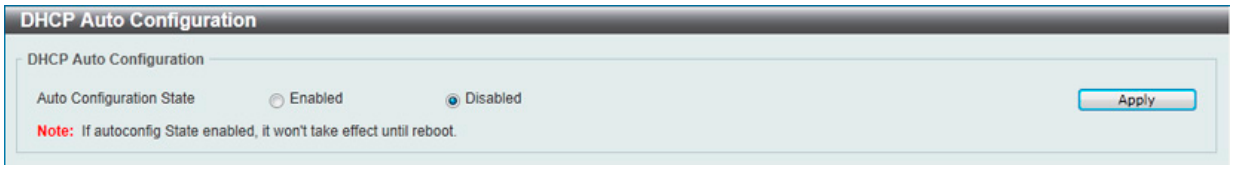


図 7-65　DHCP Auto Configuration 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」ボタンをクリックし、設定を適用します。

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

ここでは DHCP 自動イメージ設定を行います。スイッチのスタートアップ時に、DHCP サーバからの「DHCP OFFER」メッセージにその IP アドレスが含まれる外部 TFTP サーバから、イメージファイルを取得する機能を提供します。システムはこのイメージファイルを起動イメージとして使用します。システム起動時に自動イメージ機能が有効の場合、スイッチは自動的に DHCP クライアントになります。

DHCP クライアントは DHCP サーバからのネットワーク設定を取得しアクティブになり、DHCP サーバは TFTP サーバ IP アドレスとメッセージ付きイメージファイル名を含みます。スイッチはこの情報を受け、指定 TFTP サーバからの TFTP ダウンロード機能を実行します。このステージではシステムはコンソールにダウンロード設定を表示します。このレイアウトは「download firmware」コマンドを使用した場合と、同様になります。ファームウェアのダウンロードが完了すると、スイッチはただちに再起動します。

自動コンフィグ機能（auto-configuration）と自動イメージ（auto-image）機能のどちらも有効な場合、システムはイメージファイルを先にダウンロードし、次にコンフィグをダウンロードし再起動します。

スイッチはダウンロードされたファームウェアを必ずチェックします。現在のバージョンと同じ場合は、スイッチは自動イメージプロセスを終了します。ですが、自動コンフィグの場合は実行します。
本機能は自動コンフィグ機能と似ています。イメージファイル、コンフィグファイル両方とも同じ TFTP サーバに格納されており、DHCP オプションの項目は自動イメージ機能のみのために使用されておらず、自動コンフィグにも適用されています。TFTP サーバ IP アドレスは「DHCP siaddr」項目オプション 66、またはオプション 150 に存在します。オプション 66 とオプション 150、そして「siaddr」項目が DHCP 回答メッセージに同時に存在する場合、オプション 150 が先に解決されます。システムが TFTP サーバとの接続に失敗した場合、システムはオプション 66 を解決し、まだ TFTP サーバとの接続を確立できない場合「siaddr」は最後のチョイスになります。

スイッチがオプション 66 を TFTP サーバ名取得に使用する場合、オプション 6 を先に解決し DNS サーバの IP アドレスを取得します。スイッチが DNS サーバとの接続に失敗、またはオプション 6 が回答メッセージに含まれていない場合、スイッチはシステムで手動で設定された DNS サーバへの接続を試みます。

オプション 67 は、DHCP ヘッダの「file」項目が DHCP オプションに使用されている時に、ブートファイルの識別に使用されます。これは DHCP 自動コンフィグモード中のみで使用され、DHCP 自動イメージモードでは使用されません。さらなる情報については、「RFC 2132」を参照してください。イメージファイル名を指定する場合、DHCP オプション 125 (RFC 3925) が必ず使用されます。スイッチは「enterprise-number1」項目をチェックする必要があります。もしこの値が D-Link ベンダ ID (171) と違う場合、スイッチはプロセスを停止します。このオプションが一つ以上の項目を含んでいる場合、最初の「enterprise-number1」エントリのみ使用されます。

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

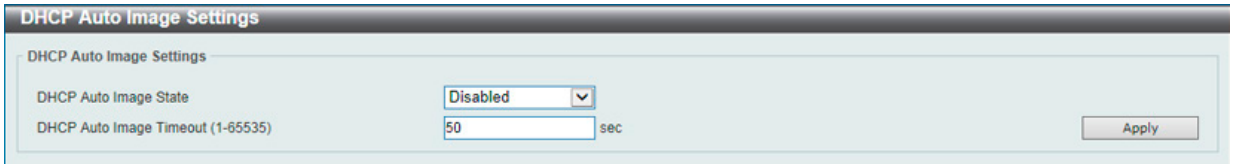


図 7-66　DHCP Auto Image Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCP Auto Image State	DHCP 自動イメージ機能を有効 / 無効にします。
DHCP Auto Image Timeout	DHCP 自動イメージ機能のタイムアウト時間を指定します。1 から 65535（秒）で指定可能です。

「Apply」ボタンをクリックし、設定を適用します。

DNS（ドメインネームシステム）

DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。DNS サーバは「name-to-address」翻訳を実行し、ドメイン名とアドレスの変換を行うためにいくつかのネームサーバと連絡を取る必要があります。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 サーバから得る場合と、初期設定時に手動で OS に設定する場合があります。

DNS Global Settings（DNS グローバル設定）

本項目ではグローバルに DNS を設定します。

Management > DHCP > 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。

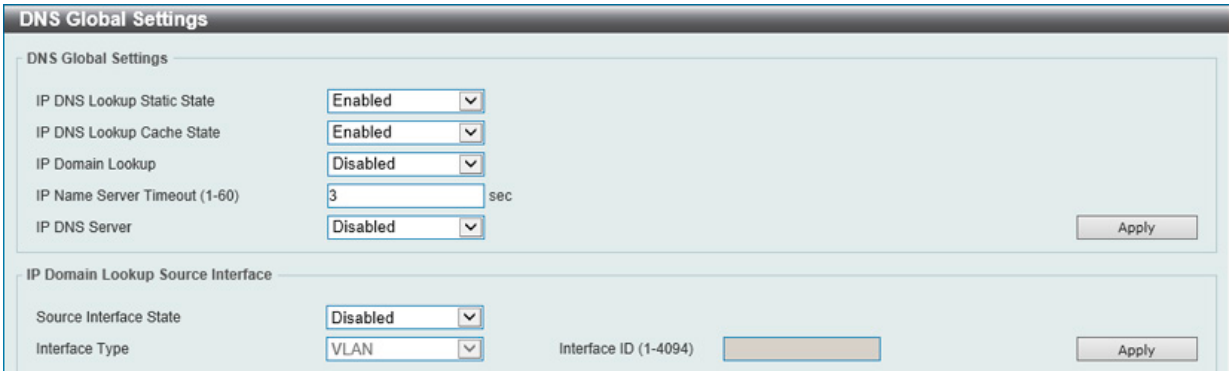


図 7-67　DNS Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
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 / 無効に指定します。
IP DNS Lookup Cache State	IP DNS ルックアップキャッシュを有効 / 無効に指定します。
IP Domain Lookup	IP ドメインルックアップを有効 / 無効に指定します。
IP Name Server Timeout	指定ネームサーバからの回答を待つタイムアウトを 1 から 60（秒）で指定します。
IP DNS Server	DNS サーバを有効 / 無効します。
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。
Interface ID	インタフェース ID を指定します。ループバックインタフェースの場合、「1」から「8」、 管理インタフェース（Mgmt）の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。

「Apply」ボタンをクリックし、設定を適用します。

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

スイッチに DNS のネームサーバを作成します。

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。

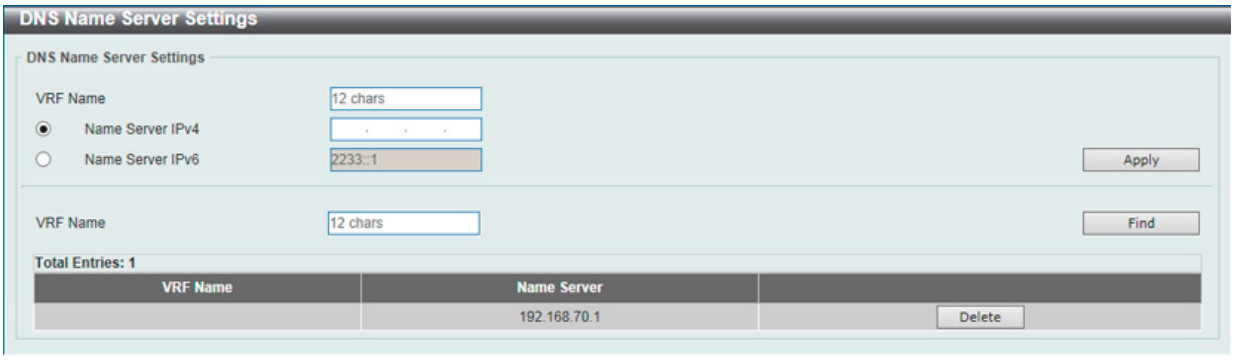


図 7-68　DNS Name Server Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Name Server IPv4	選択して DNS サーバの IPv4 アドレスを入力します。

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

「Apply」ボタンをクリックし、設定を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」ボタンをクリックして、指定エントリを削除します。

DNS Host Settings（DNS ホスト名設定）

ホスト名のスタティックマッピングの設定とホストテーブルの IP アドレスを設定します。

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

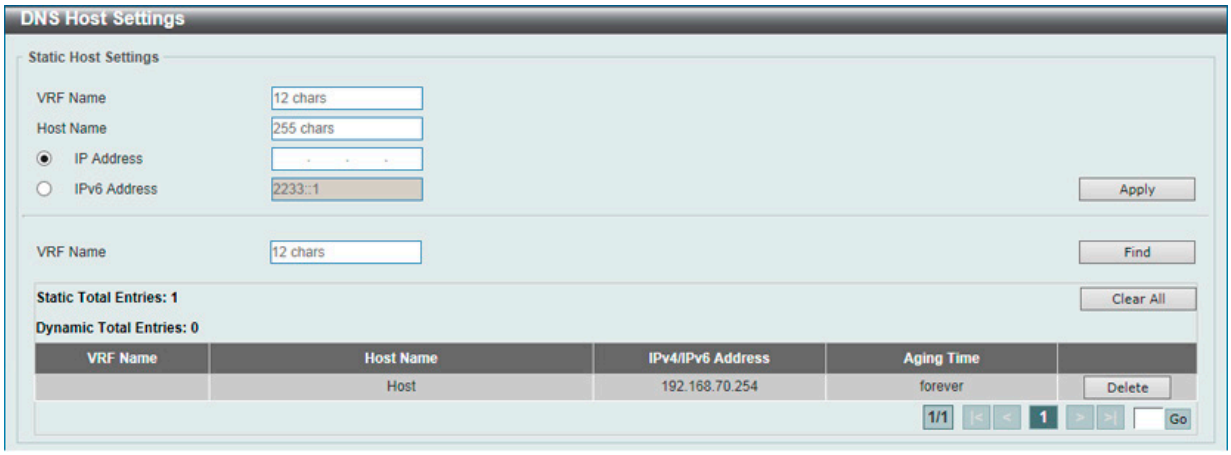


図 7-69　DNS Host Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Host Name	ホスト名を入力します。
IP Address	ホストの IPv4 アドレスを入力します。
IPv6 Address	ホストの IPv6 アドレスを入力します。

「Apply」ボタンをクリックし、設定を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「Delete」ボタンをクリックして、指定エントリを削除します。
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。

NTP（ネットワークタイムプロトコル）

スイッチが持つ時計の時刻を同期するための通信プロトコルの設定を行います。

NTP Global Settings（NTP グローバル設定）

NTP のグローバル設定を行います。

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

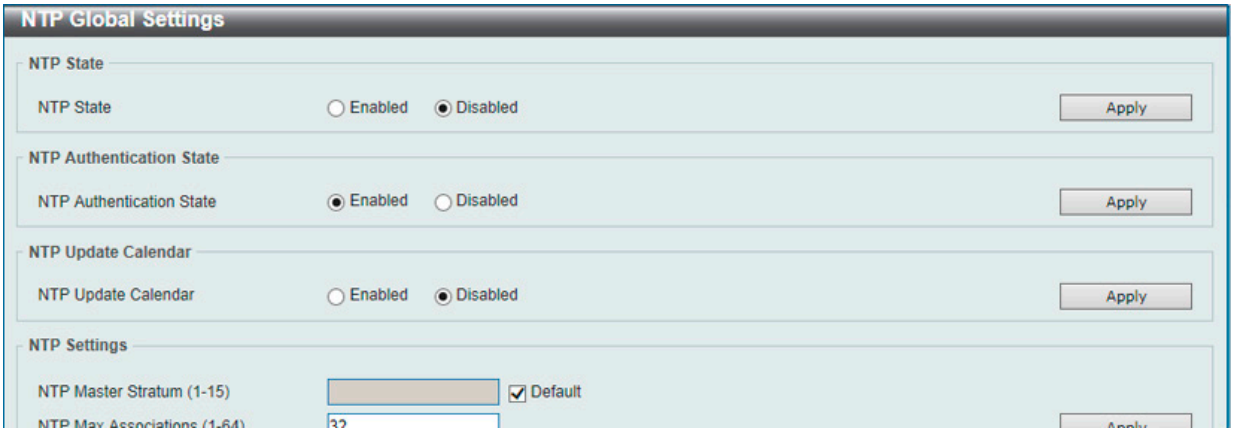


図 7-70　NTP Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
NTP State	
NTP State	NTP 機能をグローバルに有効 / 無効にします。
NTP Authentication State	
NTP Authentication State	NTP の認証を有効 / 無効にします。
NTP Update Calendar	
NTP Update Calendar	NTP のアップデートカレンダーを有効 / 無効にします。
NTP Settings	
NTP Master Stratum	NTP マスタの階層値を指定します。1 から 15 までで指定可能です。「Default」を指定すると初期値が適用されます。
NTP Max Associations	NTP への接続最大値を指定します。1 から 64 で指定可能です。

「Apply」ボタンをクリックし、設定を適用します。

NTP Server Settings（NTP サーバ設定）

NTP サーバの設定を行います。

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

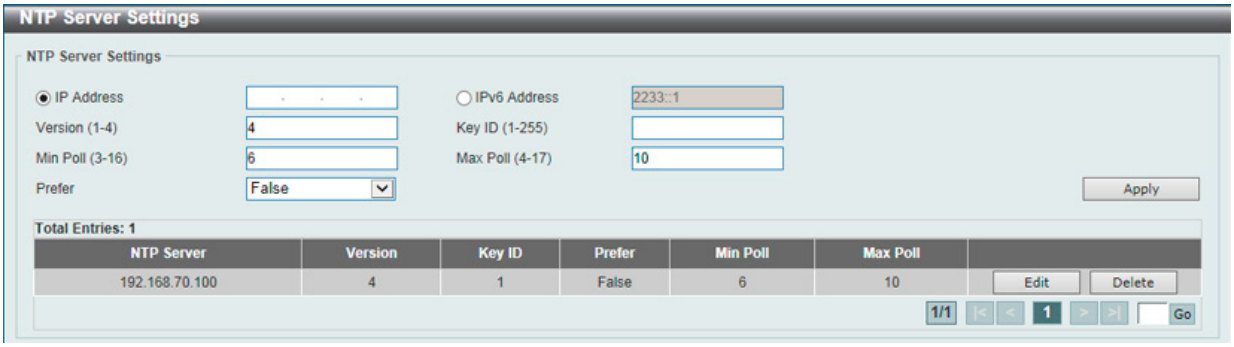


図 7-71　NTP Server Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IP Address	NTP サーバの IPv4 アドレスを指定します。
IPv6 Address	NTP サーバの IPv6 アドレスを指定します。
Version	NTP サーバのバージョンを指定します。1 から 4 で指定します。
Key ID	認証鍵 ID を指定します。1 から 255 で指定します。

項目	説明
Min Poll	NTP メッセージ送信の最小ポーリング間隔を指定します。3 から 16（秒）で指定します。
Max Poll	NTP メッセージ送信の最大ポーリング間隔を指定します。4 から 17（秒）で指定します。
Prefer	対象のサーバが好ましいか否かをリストに振り分けます。True または False から指定します。

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

NTP Peer Settings（NTP ピア設定）

NTP のピア設定を行います。

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

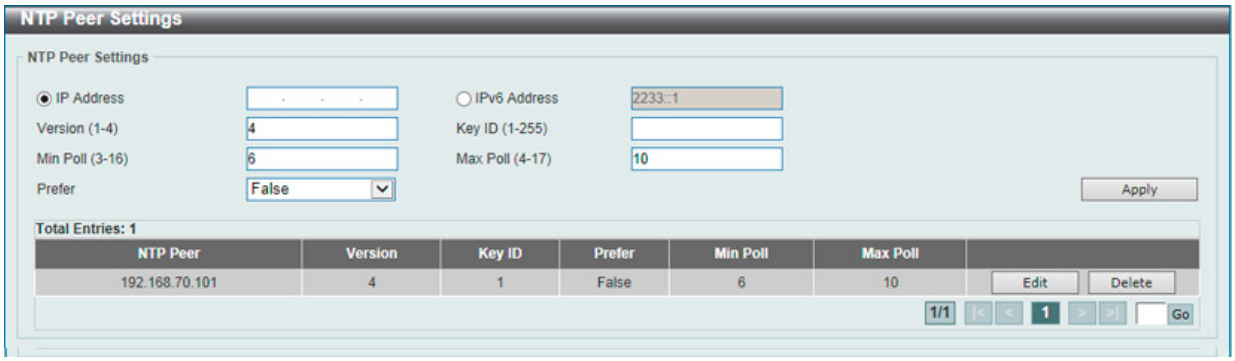


図 7-72　NTP Peer Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IP Address	NTP ピアの IPv4 アドレスを指定します。
IPv6 Address	NTP ピアの IPv6 アドレスを指定します。
Version	NTP ピアのバージョンを指定します。1 から 4 で指定します。
Key ID	認証鍵 ID を指定します。1 から 255 で指定します。
Min Poll	最小ポーリング間隔を指定します。3 から 16（秒）で指定します。
Max Poll	最大ポーリング間隔を指定します。4 から 17（秒）で指定します。
Prefer	対象のピアが好ましいか否かをリストに振り分けます。True または False から指定します。

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

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

NTP のアクセスグループ設定を行います。

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

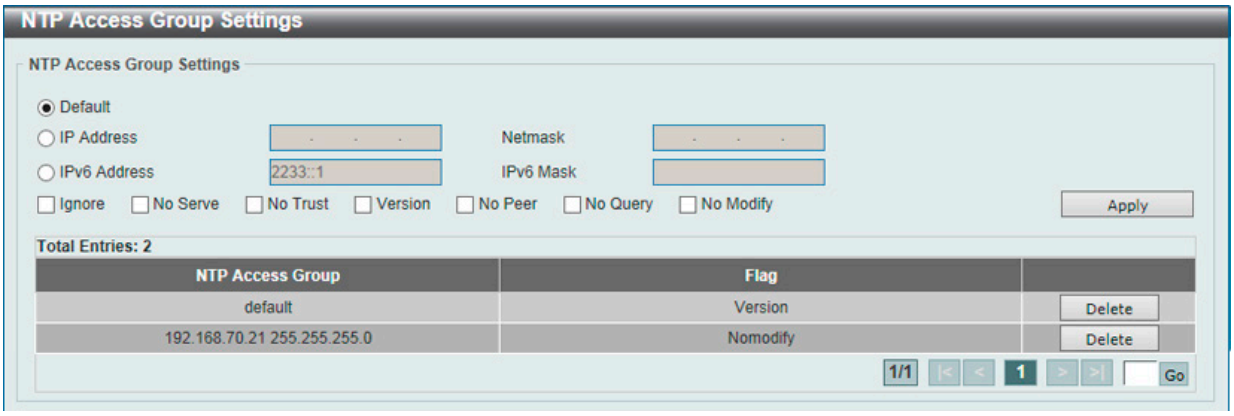


図 7-73　NTP Access Group Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Default	チェックを入れるとデフォルトのエントリ（0.0.0.0 /.0.0.0.0）が最小の優先値でリストに含まれます。
IP Address	ホスト / ネットワークの IPv4 アドレスを指定します。
Netmask	ホスト / ネットワークの IPv4 ネットワークマスクを指定します。
IPv6 Address	ホスト / ネットワークの IPv6 アドレスを指定します。
IPv6 Mask	ホスト / ネットワークの IPv6 ネットワークマスクを指定します。
Ignore	全ての NTP 関連パケットを無視します。
No Serve	全ての NTP 関連パケットを拒否します。（NTP コントロールクエリは除く）
No Trust	全ての暗号認証されていない NTP 関連パケットを拒否します。
Version	全ての NTP バージョンと合致しない NTP 関連パケットを拒否します。
No Peer	全ての認証されていないピアの NTP 関連パケットを拒否します。
No Query	全ての NTP コントロールクエリを拒否します。
No Modify	全てのサーバ状態を変更しようとする NTP コントロールクエリを拒否します。

「Apply」ボタンをクリックし、設定を適用します。「Delete」で指定エントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

NTP Key Settings（NTP 鍵設定）

NTP の鍵設定を行います。

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

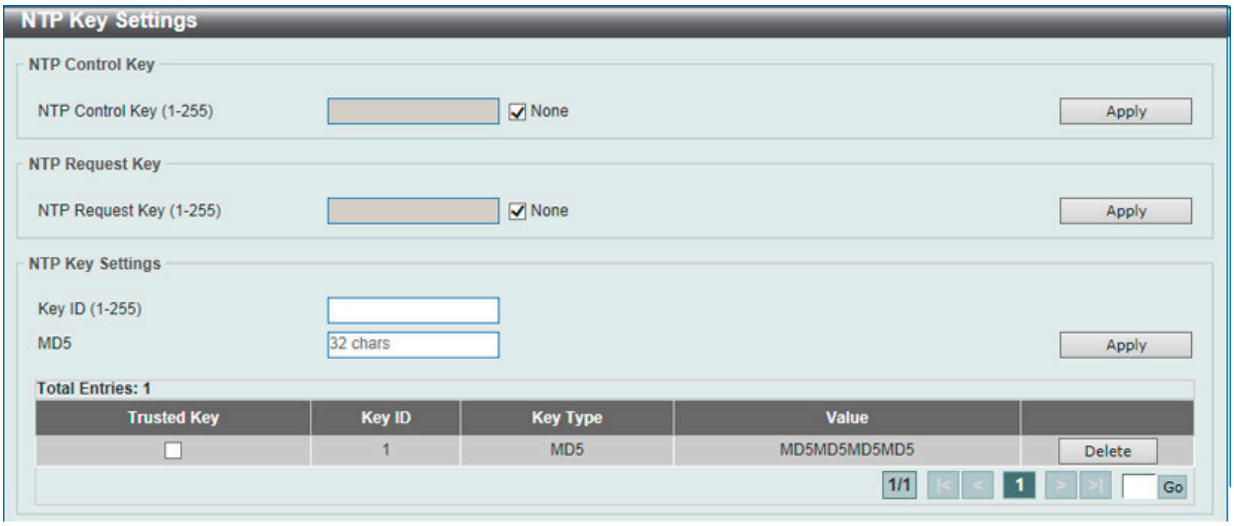


図 7-74　NTP Key Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
NTP Control Key	
NTP Control Key	NTP コントロールキー（制御鍵）を 1 から 255 で指定します。「None」を選択すると NTP コントロールキーは使用しません。
NTP Request Key	
NTP Request Key	NTP リクエストキー（要求鍵）を 1 から 255 で指定します。「None」を選択すると NTP リクエストキーは使用しません。
NTP Key Settings	
Key ID	NTP キーを 1 から 255 で指定します。
MD5	MD5 NTP キーを指定します。32 文字まで指定可能です。
Trusted Key	ピア NTP システムのキーが認証に合致するための設定を行います。

「Apply」ボタンをクリックし、設定を適用します。「Delete」で指定エントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

NTP Interface Settings（NTP インタフェース設定）

NTP のインタフェース設定を行います。

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



図 7-75　NTP Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
NTP State	「Edit」をクリックして該当インタフェース上の NTP 機能の有効 / 無効を指定します。

「Apply」ボタンをクリックし、設定を適用します。「Delete」で指定エントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

NTP Associations（NTP アソシエーション）

NTP アソシエーションを表示します。

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

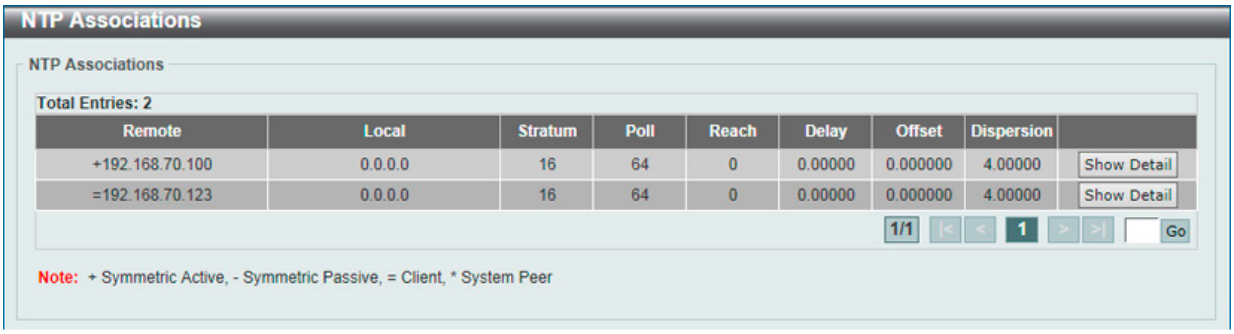


図 7-76　NTP Assosiations 画面

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

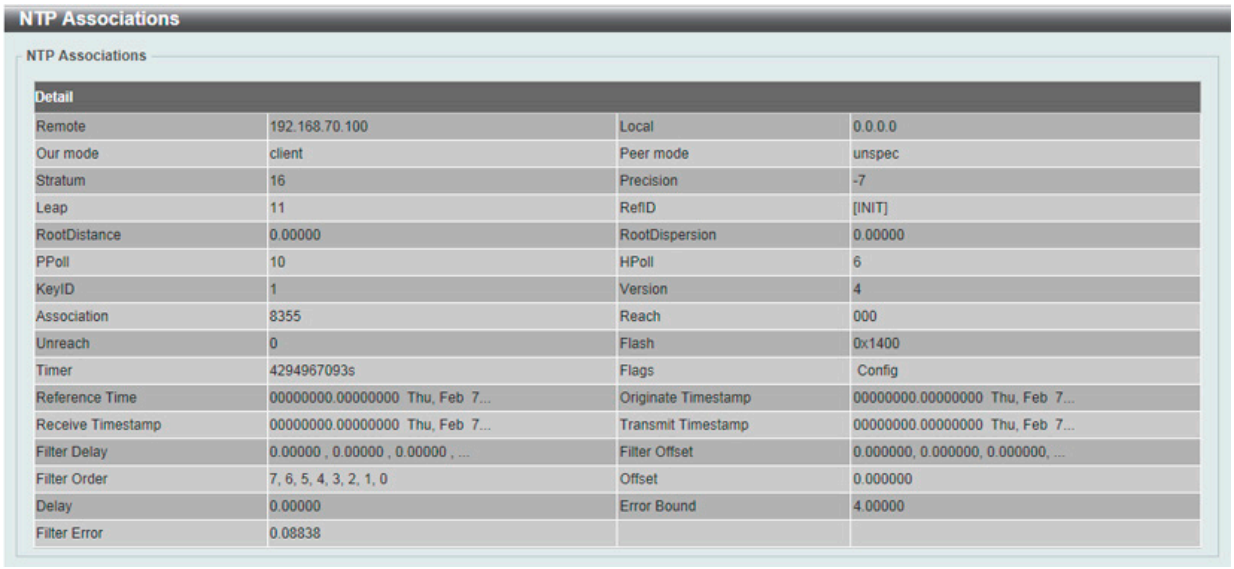


図 7-77　NTP Assosiations - Detail 画面

NTP Status（NTP ステータス）

NTP ステータスを表示します。

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

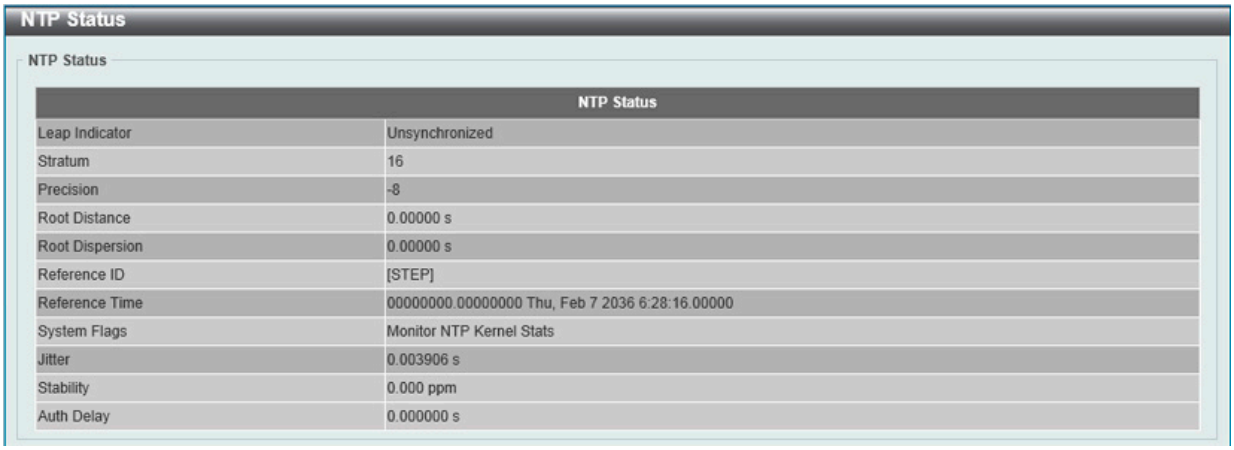


図 7-78　NTP Status 画面

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。

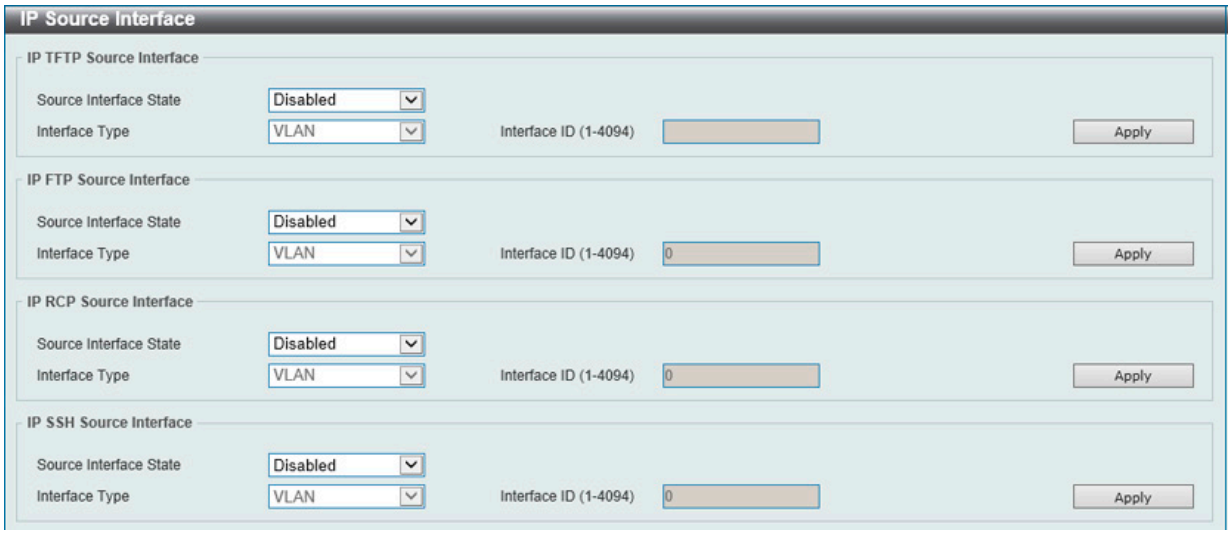


図 7-79　IP Source Interface 画面

以下の項目を使用して設定、表示を行います。

項目	説明
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。ループバックインタフェースの場合、「1」から「8」、 管理インタフェース（Mgmt）の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。
IP FTP Source Interface	
Source Interface State	IP FTP 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。ループバックインタフェースの場合、「1」から「8」、 管理インタフェース（Mgmt）の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。
IP RCP Source Interface	
Source Interface State	IP RCP 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。ループバックインタフェースの場合、「1」から「8」、 管理インタフェース（Mgmt）の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。
IP SSH Source Interface	
Source Interface State	IP SSH 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。ループバックインタフェースの場合、「1」から「8」、 管理インタフェース（Mgmt）の場合、常に「0」、VLAN インタフェースの場合、「1」から「4094」になります。

「Apply」ボタンをクリックし、設定を適用します。

File System（ファイルシステム設定）

フラッシュファイルシステムを使用する理由

古いスイッチシステムでは、ファームウェア、コンフィグレーション、およびログ情報は固定アドレスとサイズを持つフラッシュに保存されます。これは、最大のコンフィグレーションファイルが 2M バイトであり、現在のコンフィグレーションが 40K バイトにすぎなくても、フラッシュストレージスペースの 2M バイトを消費することを意味します。また、コンフィグレーションファイル番号とファームウェア番号は固定されています。コンフィグレーションファイルまたはファームウェアサイズが元々設計されたサイズを超えている場合、互換性の問題が発生します。

使用するシステムにおけるフラッシュファイルシステム

フラッシュファイルシステムは、フラッシュメモリにおける柔軟なファイル操作を提供します。すべてのファームウェア、コンフィグレーション情報、および Syslog ログ情報はフラッシュ内のファイルに保存されます。これは、すべてのファイルが取得したフラッシュスペースが固定されておらず、実ファイルサイズであることを意味します。フラッシュスペースが十分であれば、より多くのコンフィグレーションファイルまたはファームウェアファイルをダウンロードできます。また、フラッシュファイル情報の表示やファイル名の変更、および削除するコマンドを使用することができます。その上、必要に応じて、起動用のランタイムイメージや動作するコンフィグレーションファイルを設定できます。

ファイルシステムに不具合がある場合、Z- モデムを使用して直接システムにバックアップファイルをダウンロードすることができます。

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。

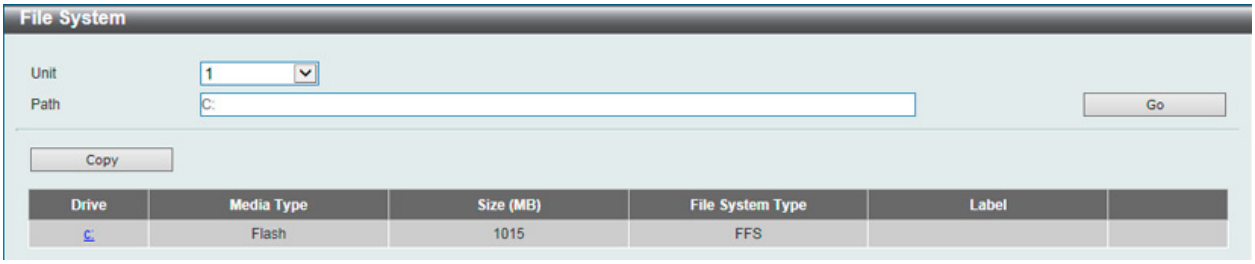


図 7-80　File System 画面

以下の項目を使用して設定、表示を行います。

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

「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。

「C:」リンクをクリックすると、以下の画面が表示されます。

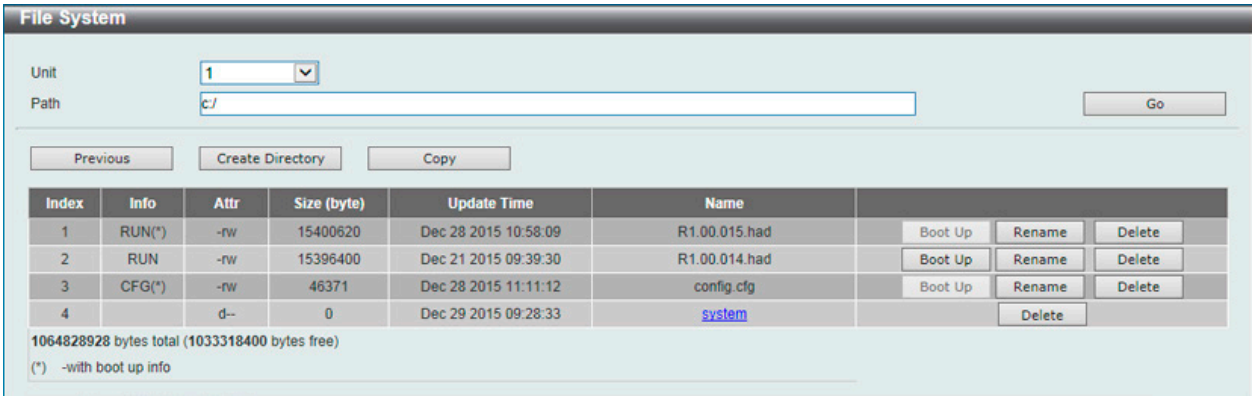


図 7-81　File System (Drive) 画面

以下の項目を使用して設定、表示を行います。

項目	説明
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	起動用のブートアップイメージとして指定したランタイムイメージを設定します。
Rename	指定ファイルを変更します。
Delete	ファイルシステムから指定ファイルを削除します。

ファイルのコピー

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。

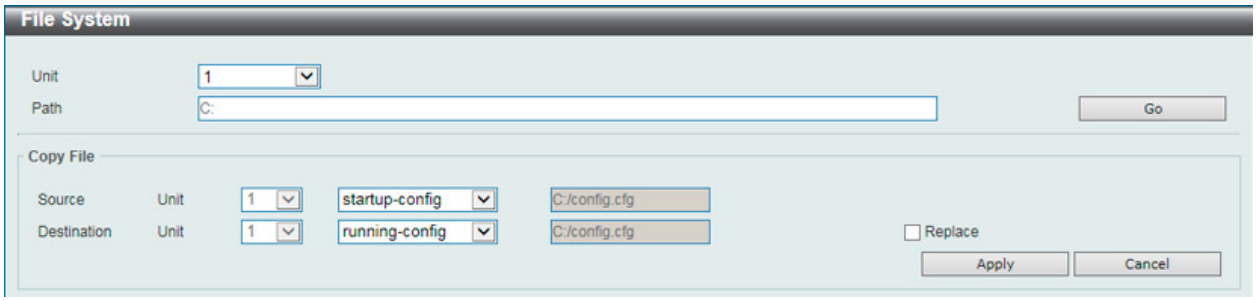


図 7-82　Flash File System Settings 画面 - Copy

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	コピー元ファイルのあ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。「startup-config」「Source File」から選択します。「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。「startup-config」「running-config」「Destination File」から選択します。「Destination File」選択時にはファイルパスを指定欄に入力します。「Replace」にチェックす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　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。

Stacking（スタッキング設定）

本スイッチは、スイッチのスタックをサポートしています。9 個のスイッチをコンソールポート、MGMT ポート経由の IP アドレス、または Telnet、GUI インタフェース (Web)、SNMP を使用した RJ45/SFP/SFP+ の複数 IP アドレスで 1 つに結合し、管理することができます。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。

- 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。そして、1 カ所中断が発生すると、データ転送は明らかに影響を受けます。

- 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光ファイバケーブルを使用した SFP ＋モジュール、または 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 4 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している時、最後の SFP+ ポート 2/4 つは他のデバイスやスイッチなどへのアップリンクとして使用できません。スタッキングはこれらのポートを使用してのみ可能です。

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し、有効にする必要があります。「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、光ファイバケーブルを使用した SFP ＋モジュール、または SFP ＋ダイレクトアタッチケーブルを使用して「2 ポート」スタッキング設定、「Duplex Chain」構成での物理スタック図です。

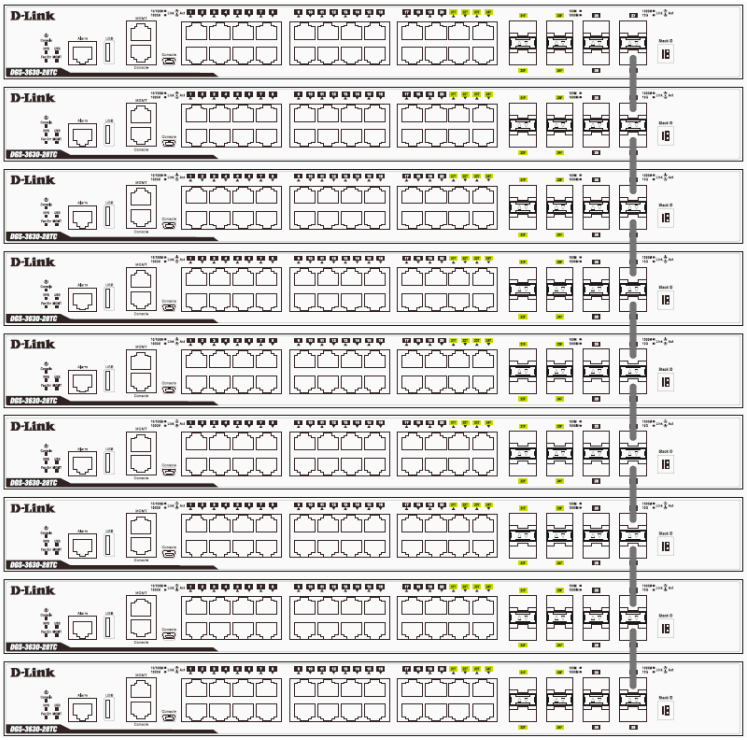


図 7-83　Duplex Chain でスタックされているスイッチ画面（SFP ＋）

光ファイバケーブルを使用した SFP ＋モジュール、または SFP ＋ダイレクトアタッチケーブルを使用して「2 ポート」スタッキング設定、「Duplex Ring」構成での物理スタック図です。

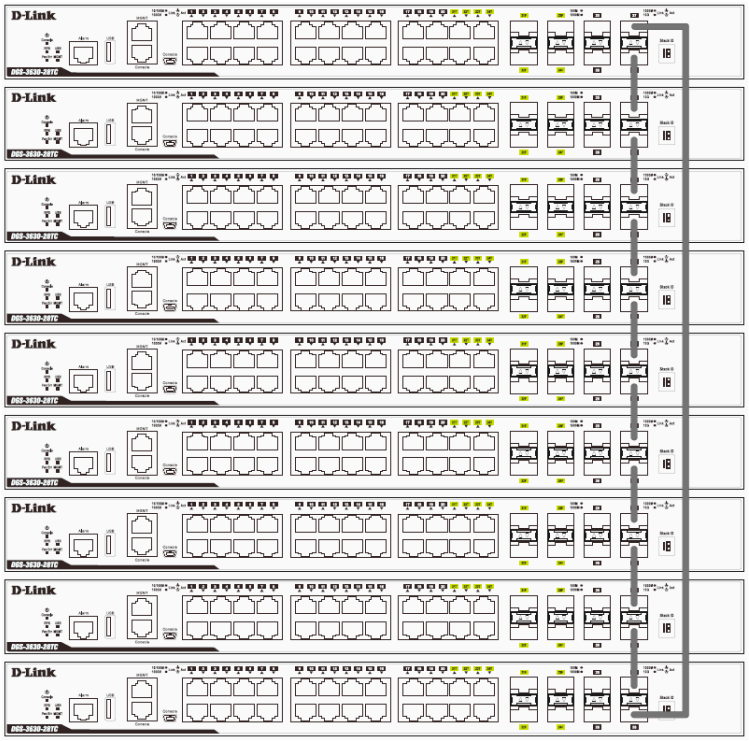


図 7-84　Duplex Ring でスタックされているスイッチ画面（SFP ＋）

注意 「Stacking Input/Output logical port 1」（SIO1）と「SIO2」は、それぞれ論理スタッキングポートのペアです。4 ポートスタッキングを行う場合、1 つの論理スタッキングポートのペア（例：スイッチ A の SIO2 × 2）が、接続先スイッチの同じ SIO（例：スイッチ B の SIO1 × 2）に接続するようにしてください。それぞれ異なるスイッチや異なる SIO ポートに接続された場合、安定したスタッキング接続を保証できません。SIO1/SIO2 に対応する物理ポートについては、136 ページの「Stacking Bandwidth（スタッキング帯域）」を参照してください。

以下の図は、4 ポートスタッキングにおける適切な接続例です。

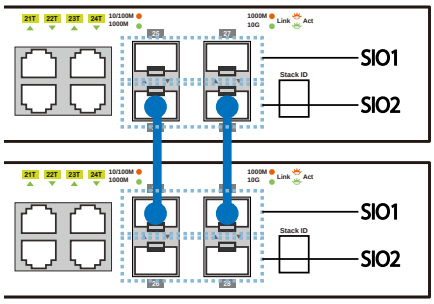


図 7-85　スイッチ間のケーブル接続①

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

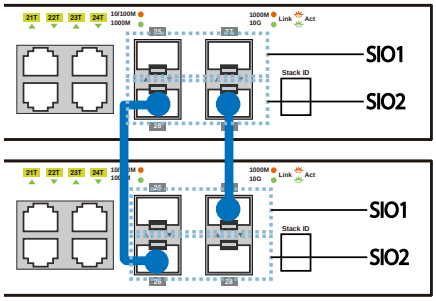


図 7-86　スイッチ間のケーブル接続②

スタック内のスイッチ役割

各トポロジにおいて、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に、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。本スイッチは、スイッチスタック内にあるスイッチに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。プライマリマスタには、スタックを物理的に構成する前、またはすべての優先度が同じである場合には最も数字の低い MAC アドレスを持つスイッチに決定します。また、スタックが自動的に決定される前に、最も高い優先度（低い番号ほど優先度は高くなります。）を本スイッチに割り当てることで手動で設定することができます。プライマリマスタは、スイッチの前面パネルの一番右にある LED によって 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。バックアップマスタは、スタックを物理的に構成する前、またはすべての優先度が同じである場合には 2 番目に数字の低い MAC アドレスに決定します。また、スタックが自動的に決定される前に、2 番目に高い優先度（低い番号ほど優先度は高くなります。）を本スイッチに割り当てることで手動で設定することができます。バックアップマスタは、物理的にスイッチの前面パネルの一番右にある 7 個のセグメント LED によって Box ID と「h」が表示されます。

- スレーブ
  スレーブスイッチは、残りのスイッチスタックを構成します。プライマリマスタまたはバックアップマスタスイッチではありません。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、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決定します。これらの役割は、はじめに優先度によって決定され、さらに優先度が同じである場合は、最も低い MAC アドレスによって決定されます。

スイッチが希望したトポロジで構成されると、スタックは機能する状態に到達するまでに 3 つの過程を経由します。
- 初期化状態 - これは、スタックの最初の状態で、ランタイムコードが設定および初期化され、システムは各スイッチが適切に機能していることを検証するために周辺機器の診断を行います。
- マスタ選出状態 - コードがロードされ、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、プライマリマスタが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き、残りのスイッチにコマンドを送信します。

これらの手順が終了すると、スイッチスタックは正常な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、動作中のスタック内またはスタック外のスイッチの「ホットスワップ」をサポートしています。いくつかの簡単な条件により、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、スタックからのスイッチの取り外しやスタックへの追加を行うことができます。

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、設定された優先度や MAC アドレスなど新たに追加されたコンフィグレーションによって、新しいスイッチはプライマリマスタ、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。しかし、共に以前の選出過程を経て、その結果、プライマリマスタとバックアップマスタを持った 2 つのスタックが追加されると、新しいプライマリマスタが、優先度または MAC アドレスに基づいて、既存のプライマリマスタから選出されます。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にプライマリマスタの全役割を引き継ぎます。この過程は、検出処理が完了するまで 1.5 秒ごとにスイッチスタックを通して循環するディスカバリパケットを使用して行われます。

「ホットリムーブ」の動作は、スタックが既に動作している場合にスタックからデバイスを取り外すことを意味します。ホットリムーブは、指定した間に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中の 1 つの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。デバイスが一度取り外されると、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。スタックから 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）のどれか 1 つが取り外される場合には、異なる過程がそれぞれの特定デバイス取り外しに発生します。

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 メッセージの使用を通じ、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 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、新しくバックアップマスタが前述の選出過程を経由して選ばれます。スタック内のスイッチは、取り外されたユニットの 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、データベース同期がスタックによって完了した際に、バックアップマスタは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はプライマリマスタの役割を引き受けて、新しいバックアップマスタが選出過程を経て選ばれます。スタック内のスイッチは、取り外されたユニットの 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。新しいプライマリマスタは、スタックとネットワーク内の矛盾を避けるために、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、選出過程では、直ちに処理を行い、新しいプライマリマスタとバックアップマスタを決定します。スタック内のスイッチは、取り外されたユニットの 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構成は、スタックに存在するスイッチに関するデータベースに残りますが、それらの機能には影響されません。

注意 スタックが検出過程にある時、Box ID の矛盾があると、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され、エラーメッセージが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生成されます。ユーザは、Box ID を再設定し、スタックを再起動する必要があります。

Physical Stacking（物理スタッキング）

物理スタッキングの設定を行います。

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

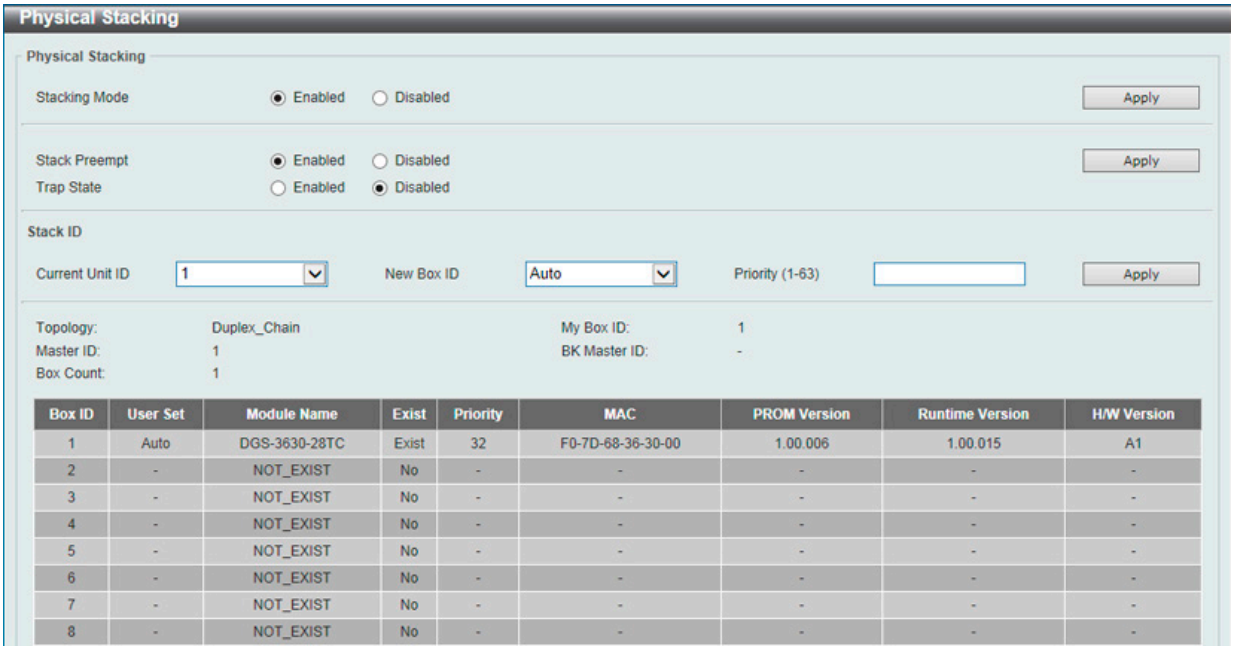


図 7-87　Physical Stacking 画面

設定および表示する項目は以下の通りです。

項目	説明
Physical Stacking	
Stacking Mode	初期値では「Disabled」(無効) になっています。
Stack Preempt	「Enabled」(有効)/「Disabled」(無効) にします。新しいデバイスが現在のスタックトポロジに追加した際にマスタロールが変更されないことを保証するために使用されます。「Disabled」（無効）を選択すると、スタックが安定した後にマスタの優先度は 0 になります。
Trap State	スタック関連の SNMP トラップの送信を有効 / 無効にします。
Stack ID	
Current Unit ID	スタックにおけるスイッチの現在のユニット番号を選択します。
New Box ID	「Current Unit ID」で選択したスタック内のスイッチに新しくボックス番号 (1-9) 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。
Priority (1-63)	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。

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。

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。物理スタッキングは有効化と、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」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-3630-28TC/28SC/28PC は物理ポート 27（SIO1）と 28（SIO2）を「2 ポート」スタッキングに使用します。
- DGS-3630-52TC/52PC は物理ポート 51（SIO1）と 52（SIO2）を「2 ポート」スタッキングに使用します。

「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。

- DGS-3630-28TC/28SC/28PC は物理ポート 25（SIO1）、26（SIO2）、27（SIO1）、28（SIO2）を「4 ポート」スタッキングに使用します。
- DGS-3630-52TC/52PC 物理ポート 49（SIO1）、50（SIO2）、51（SIO1）、52（SIO2）を「4 ポート」スタッキングに使用します。

注意 「Stacking Input/Output logical port 1」（SIO1）と「SIO2」は、それぞれ論理スタッキングポートのペアです。4 ポートスタッキングを行う場合、1 つの論理スタッキングポートのペア（例：スイッチ A の SIO2 × 2）が、接続先スイッチの同じ SIO（例：スイッチ B の SIO1 × 2）に接続するようにしてください。それぞれ異なるスイッチや異なる SIO ポートに接続された場合、安定したスタッキング接続を保証できません。

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。

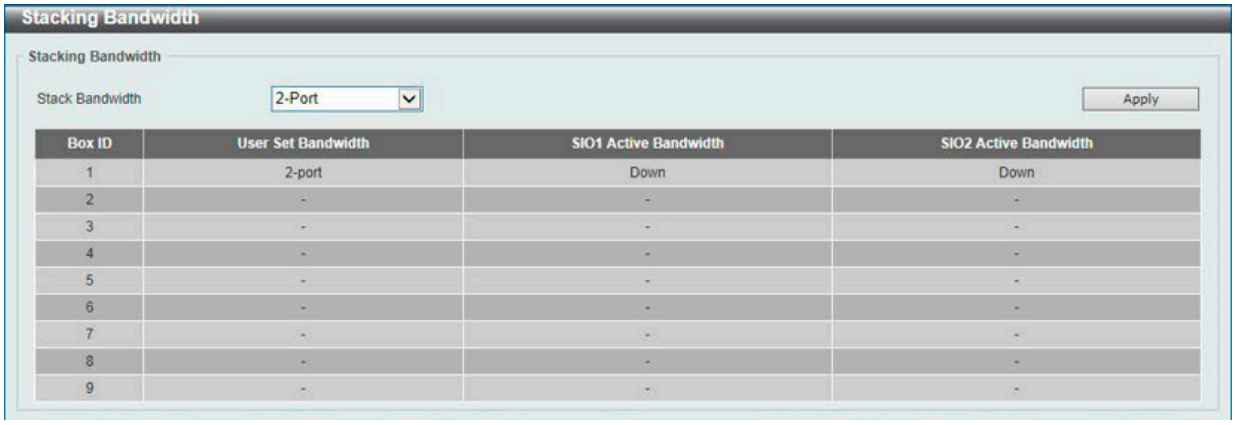


図 7-88　Stacking Bandwidth 画面

設定および表示する項目は以下の通りです。

項目	説明
Stack Bandwidth	スタッキング帯域を「2-Port」「4-Port」から指定します。

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。

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。

1. 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。
2. ネットワークに必要な IP アドレス数を減らします。
3. 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 ホップ以上はな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（リード権 / ライト権、リード権だけを含む）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。

バージョン 1.61 へのアップグレード

SIM 管理機能強化の目的で、本スイッチは本リリースにおいて、バージョン 1.61 にアップグレードしています。本バージョンでは以下の改善点が加わりました。

1. CS は、再起動または Web での異常検出によって、SIM グループから抜けたメンバスイッチを自動的に再検出する機能が搭載しました。この機能は、以前設定された SIM メンバが再起動の後に発行する Discovery パケットと Maintain パケットを使用することにより実現されます。一度 MS の MAC アドレスとパスワードが CS のデータベースに記録され、MS が再起動を行うと、CS はこの MS の情報をデータベースに保存し、MS が再検出された場合、これを SIM ツリーに自動的に戻します。これらのスイッチを再検出するために設定を行う必要はありません。

一度保存を行った MS の再検出ができないという場合もあります。例えば、スイッチの電源がオンになっていない場合、他のグループのメンバとなっている場合、または CS スイッチとして設定された場合は再検出処理をすることができません。

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

3. 本バージョンでは、以下のファームウェア、コンフィグレーションファイル、およびログファイルのアップロードやダウンロードを複数スイッチに対して行う機能が追加されました。

- ファームウェア : TFTP サーバから複数の MS に対するファームウェアダウンロードがサポートされました。
- コンフィグレーションファイル : TFTP サーバを使用した複数のコンフィグレーションのダウンロード / アップロード（コンフィグレーションの復元やバックアップ用）が可能になりました。
- ログ : 複数のログファイルを TFTP サーバにアップロード可能になりました。

4. より詳細に構成を確認しやすいようにトポロジ画面を拡大、縮小することができます。

Single IP Settings（シングル IP 設定）

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。

Web インタフェースを使用してスイッチの SIM を有効にするためには **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。

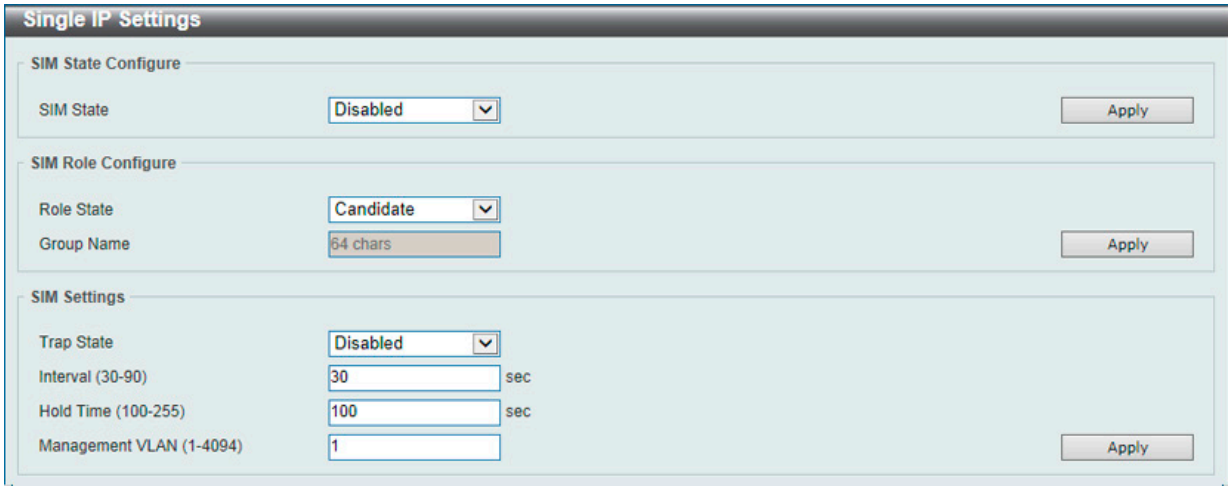


図 7-89　Single IP Settings 画面（CaS 無効状態）

以下の項目が使用できます。

項目	説明
SIM State Configure	
SIM State	プルダウンメニューから「Enabled」（有効）または「Disabled」（無効）を選択します。「Disabled」を選択すると、スイッチのすべての SIM 機能が無効になります。初期値は「Disabled」です。
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。以下の 2 つから選択できます。 • 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。本スイッチの SIM 機能の初期設定です。 • Commander - Commander Switch（CS）。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。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。

項目	説明
Group Name	SIM グループ名を入力します。
SIM Settings	
Trap State	SIM トラップを有効 / 無効にします。
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（秒）を設定します。CS スイッチに情報が送られてくると、接続する他のスイッチ（MS、CaS）の情報が CS に組み込まれます。値は 30-90（秒）の間から指定します。初期値は 30（秒）です。
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（秒）を指定します。値は 100-255（秒）の間から指定します。初期値は 100（秒）です。
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「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 設定が続けられるようになります。追加されるリンクは「Topology」、「Firmware Upgrade」、「Configuration Backup/Restore」、「Upload Log File」です。

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。本画面は表示のためには、ご使用のコンピュータに Java スクリプトが必要です。

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。

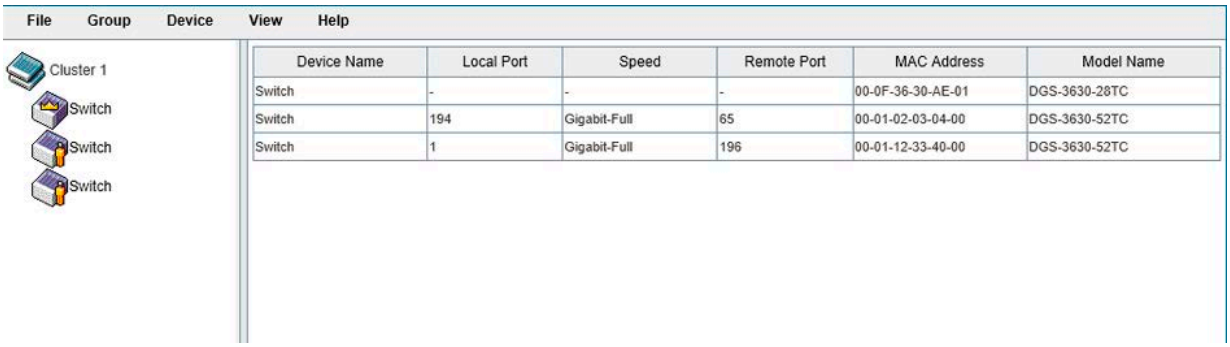


図 7-90　トポロジ画面

メニューバー

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



図 7-91　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（interval）など表示プロパティを設定します。

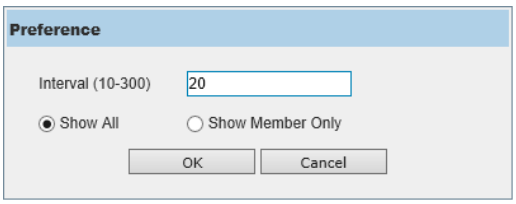


図 7-92　Preference

以下の項目が使用できます。

項目	説明
Interval	SIM トポロジ表示の更新間隔（10-300）を指定します。
Show All	トポロジにおいて全ての有効な SIM デバイスを表示します。
Show Member Only	トポロジにおいて SIM メンバデバイスのみを表示します。

設定を変更する際は、「OK」ボタンをクリックし、設定内容を適用してください。
「Cancel」ボタンをクリックし、変更した設定内容を破棄します。

「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。

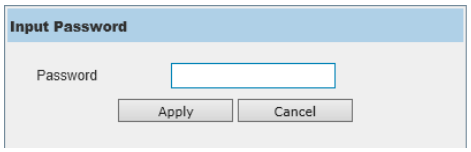


図 7-93　Input password ダイアログボックス

- 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。

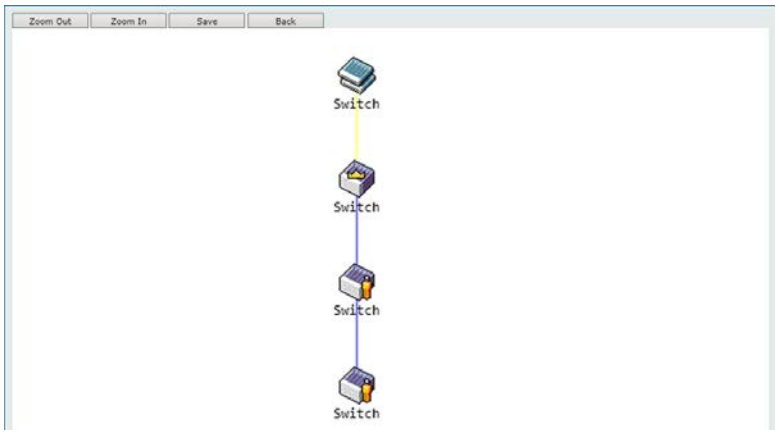


図 7-94　View >Topology 画面

「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。

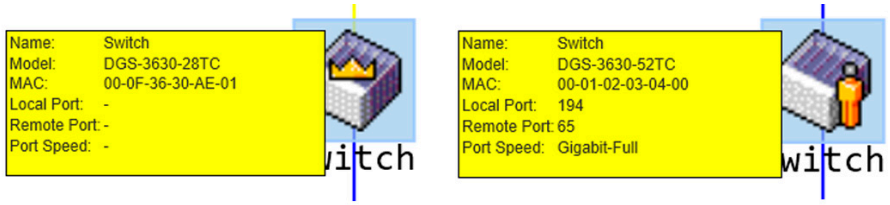


図 7-95　ツールヒントを利用したデバイス情報の表示

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。

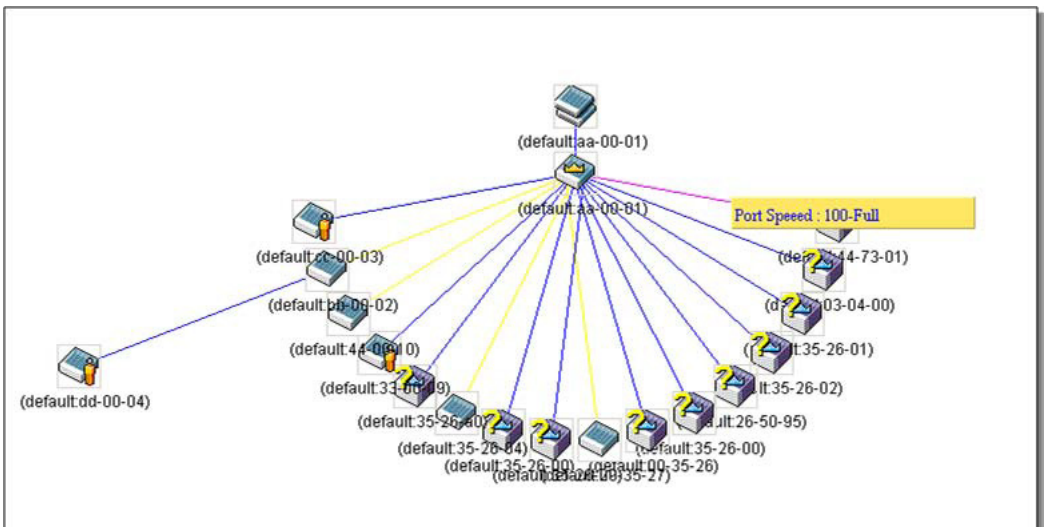


図 7-96　ツールヒントを利用したポート速度の表示①

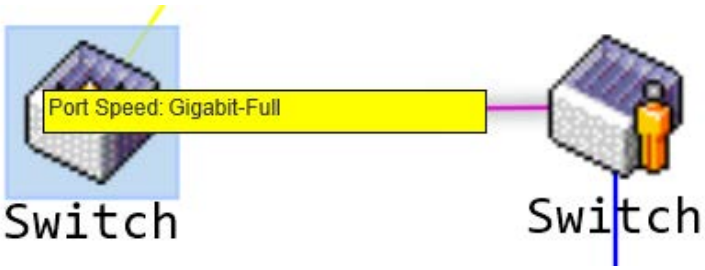


図 7-97　ツールヒントを利用したポート速度の表示②

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。

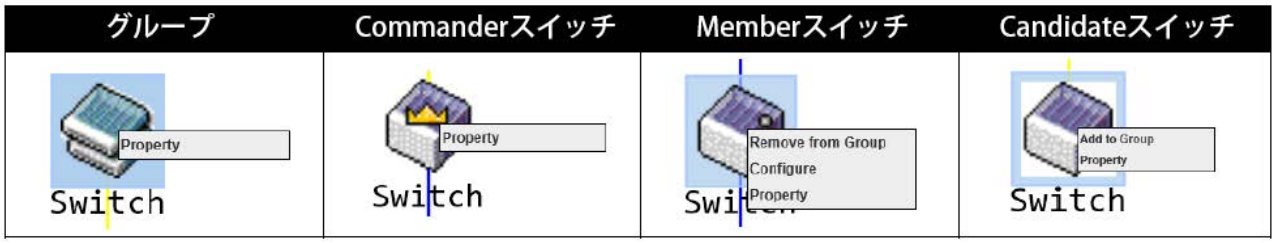


図 7-98　各アイコン上での右クリック

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、以下のパスワード入力画面が表示され、CaS スイッチを SIM グループに追加するための認証を行います。
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。

各アイコンの「Property」



図 7-99　各アイコンの Property

画面には以下の情報が表示されます。

項目	説明
Name	SIM グループ内のスイッチのデバイス名を表示します。デバイス名がない場合は、「default」が与えられ、識別のために MAC アドレスの終わり 6 桁が付加されます。
Module	スイッチのモジュール名を表示します。
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。

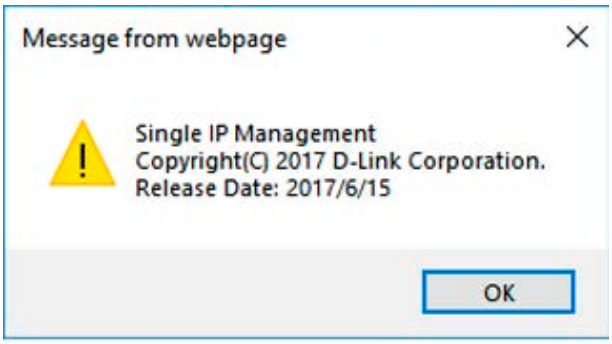


図 7-100　About ダイアログボックス

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。

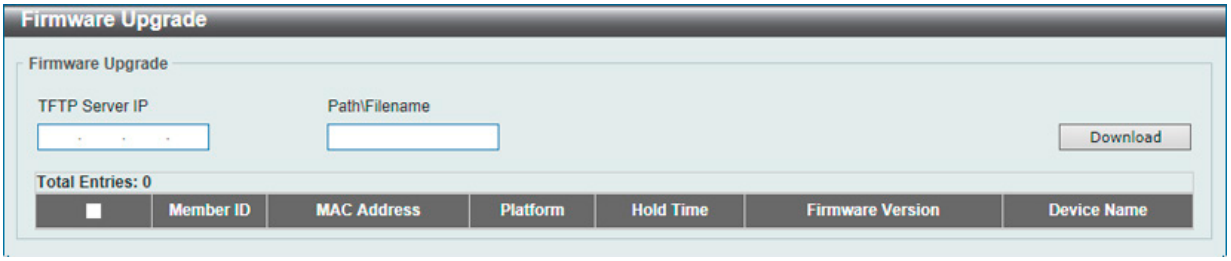


図 7-101　Firmware Upgrade 画面

MS は、「Port」（MS に接続する CS 上のポート）、「MAC Address」、「Model Name」、「Version」の情報と共にリスト表示されます。ダウンロード対象のスイッチは、「Port」欄の下のチェックボックスで選択します。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。「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。

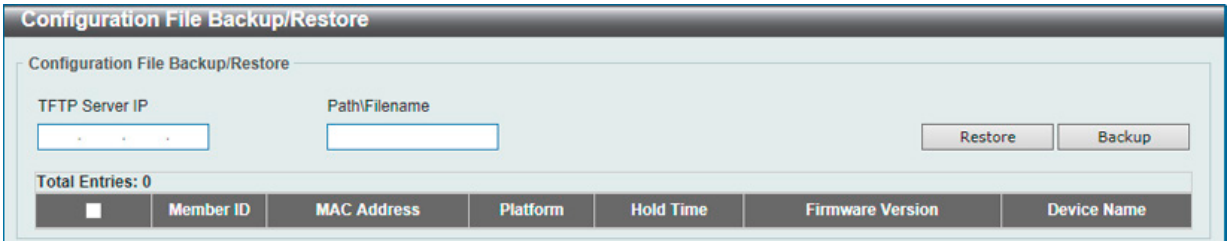


図 7-102　Configuration File Backup/Restore 画面

MS は「Port」（MS に接続する CS 上のポート）、「MAC Address」、「Model Name」、「Version」の情報と共にリスト表示されます。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は、「Port」欄の下のラジオボタンで選択します。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。「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送信したログファイルを依頼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。

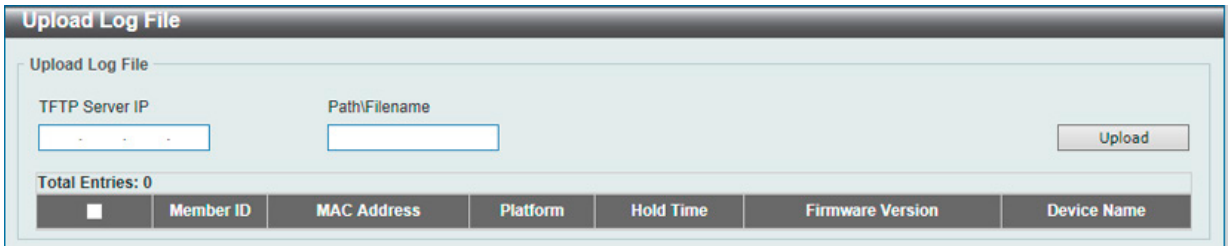


図 7-103　Upload Log File 画面

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。「Upload」ボタンをクリックすると TFTP サーバにログファイルを送信します。

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

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

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

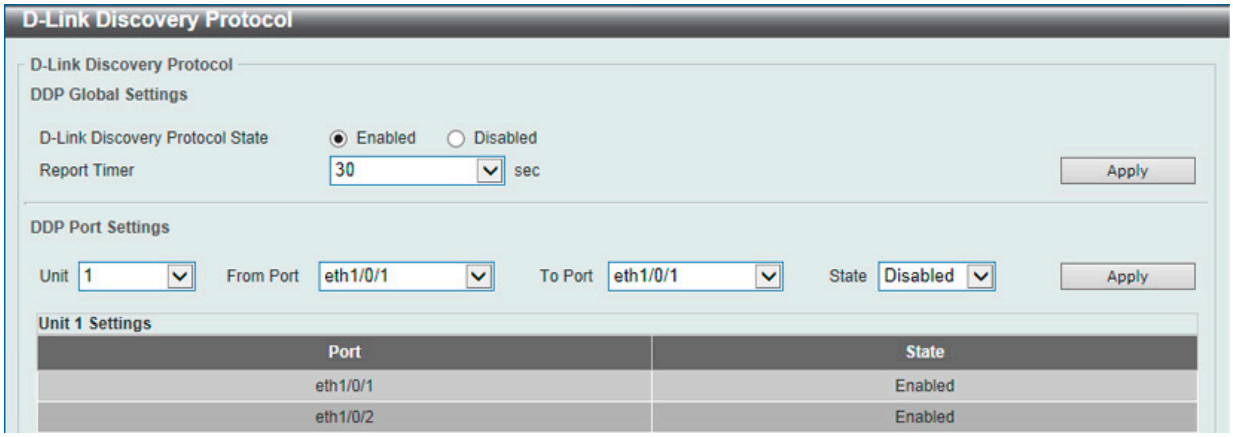


図 7-104　D-Link Discovery Protocol 画面

設定には以下の項目を使用します。

項目	説明
D-Link Discovery Protocol	
D-Link Discovery Protocol State	DDP をグローバルに有効にします。
Report Timer	DDP レポートメッセージの送信間隔（秒）を指定します。「30」「60」「90」「120」「Never」から指定できます。
DDP Port Settings	
Unit	設定するユニットを選択します。
From Port / To Port	ポートの始点 / 終点を設定します。
State	DDP ポートを有効 / 無効にします。

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

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。

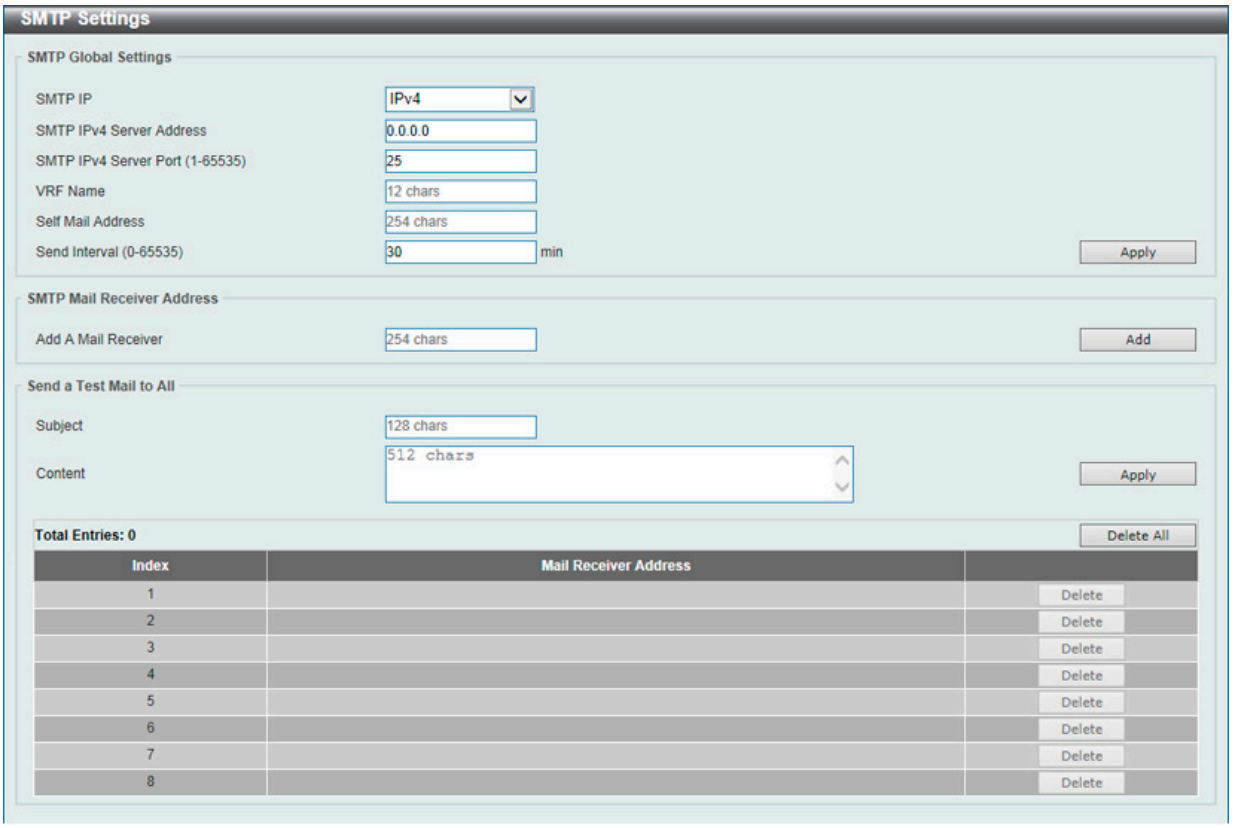


図 7-105　SMTP Settings 画面

設定には以下の項目を使用します。

項目	説明
SMTP Global Settings	
SMTP IP	SMTP サーバ IP アドレスタイプを指定します。「IPv4」「IPv6」から指定可能です。
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。1 から 65535 まで指定可能です。初期値は 25 です。
SMTP IPv6 Server Port	SMTPIPv6 サーバポート番号を指定します。1 から 65535 まで指定可能です。初期値は 25 です。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Self Mail Address	スイッチの E メールアドレスを指定します。254 字以内に指定します。
Send Interval	送信間隔を指定します。0 から 65535 まで指定可能です。初期値は 30（分）です。
SMTP Mail Receiver Address	
Add A Mail Receiver	受信する E メールアドレスを指定します。254 字以内に指定します。
Send a Test Mail to All	
Subject	E メールの件名を指定します。128 字以内に指定します。
Content	E メールの内容を指定します。512 字以内に指定します。

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。
「Delete」をクリックすると指定のエントリを削除します。
「Delete All」をクリックするとすべてのエントリを削除します。

Reboot Schedule Settings（再起動スケジュール設定）

本項目では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。スイッチが再起動スケジュールが実行される前に、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。

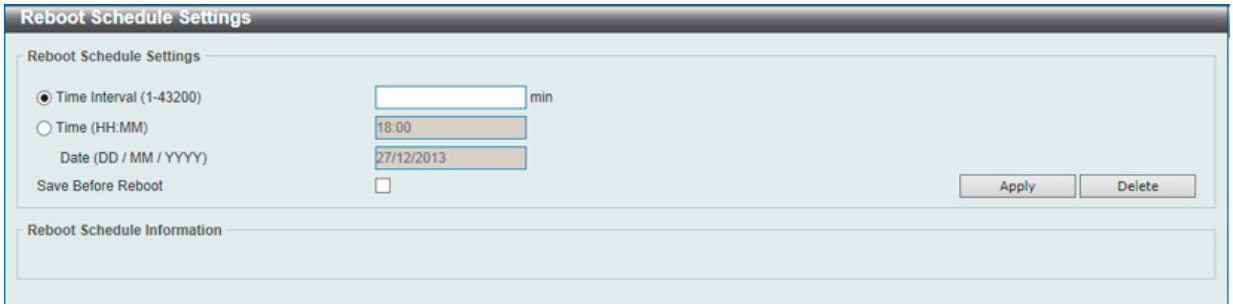


図 7-106　Reboot Schedule Settings 画面

設定には以下の項目を使用します。

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（分）を過ぎると実行されます。1 から 43200（30 日）の間で指定可能です。
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。

NLB FDB Settings（NLB FDB 設定）

本スイッチはネットワークロードバランシング (NLB) をサポートしています。これは、複数のサーバは同じ IP アドレスと MAC アドレスを共有する Microsoft サーバロードバランシングアプリケーションの MAC フォワーディングコントロールです。クライアントからのこのリクエストは、全てのサーバに転送されますが、その中の 1 つのみにより行われます。サーバは 2 つのモード「ユニキャストモード」と「マルチキャストモード」で動作可能です。

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

宛先となる MAC は共有 MAC になります。しかしサーバは応答パケットの送信元 MAC アドレスとして（共有 MAC よりむしろ）自身の MAC アドレスを使用します。つまり NLB ユニキャストアドレスは通常パケットの送信元 MAC アドレスではありません。

受信パケットがユニキャスト MAC アドレスと照合する宛先 MAC アドレスをを含んでいると、VLAN 設定に関わらず、指定のポートへ転送されます。

管理者は MAC アドレステーブルのスタティックアドレスを NLB アドレスとして設定はできません。しかし、MAC アドレスが NLB MAC アドレスエントリとして生成されている場合、同じ MAC アドレスは L2 MAC アドレステーブルにおいて学習されます。この場合、NLB はより高い優先値を持ち、自動的に学習された FDB には影響はありません。

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

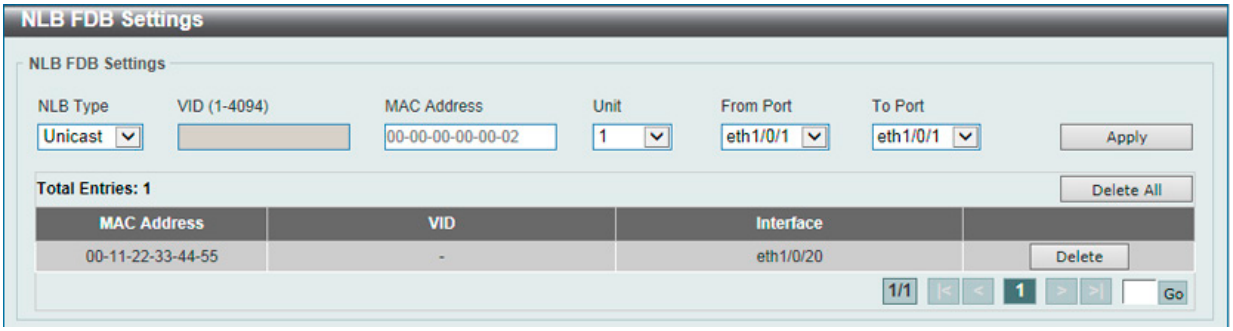


図 7-107　NLB FDB Settings 画面

以下の項目が設定可能です。

項目	説明
NLB Type	NLB タイプを「Unicast」「Multicast」から指定します。
VID	「Multicast」を選択した場合、設定する VLAN ID を入力します。
MAC Address	作成される NLB マルチキャスト FDB エントリの MAC アドレスを入力します。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Delete All」をクリックするとすべてのエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

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 7-108　SD Card Backup Settings 画面

以下の項目が表示されます。

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（32 字以内）を指定します。
Time Range	Edit をクリック後、スケジュール範囲の指定を行います。
Type	Edit をクリック後、設定するコンフィグレーション / ログのどちらか選択します。 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	Edit をクリック後、宛先ファイル名とパスを指定します。
State	Edit をクリック後、バックアップスケジュールの有効・無効を設定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

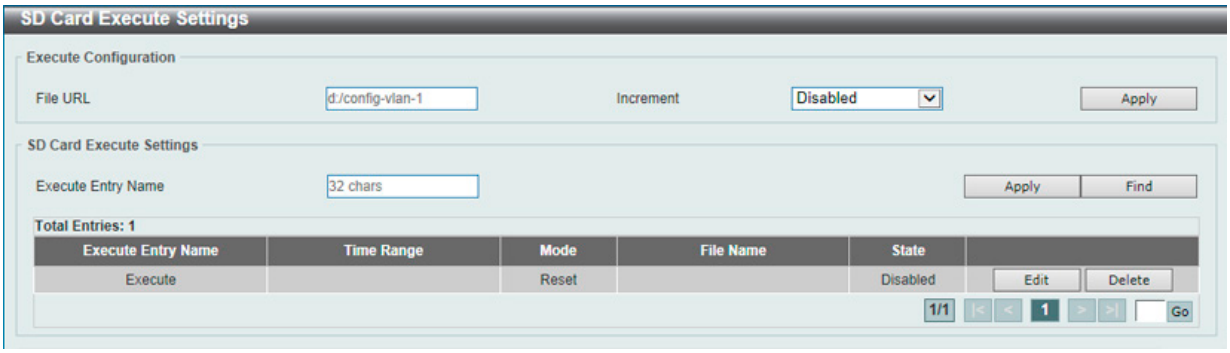


図 7-109　SD Card Execute Settings 画面

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それでない場合、フルパスを入力する必要があります。
Increment	本オプションが有効に設定されると、実行前に現在の設定がリセットされません。
SD Card Execute Settings	
Execute Entry Name	実行エントリ名を 32 字以内で指定します。
Time Range	Edit をクリック後、スケジュール範囲を設定します。
Mode	Edit をクリック後、モードを次から選択します。 「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	Edit をクリック後、設定ファイル名とパスを指定します。
State	Edit をクリック後、スケジュール実行の有効 / 無効を設定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

第 8 章　L2 Features（L2 機能の設定）

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

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

サブメニュー	説明
FDB（FDB 設定）	FDB（Forwarding DataBase）フォワーディングデータベースの設定を行います。
VLAN（VLAN 設定）	802.1Q スタティック VLAN の設定を行います。
VLAN Tunnel（VLAN トンネル）	802.1Q VLAN トンネルの設定を行います。
STP（スパニングツリー設定）	スパニングツリープロトコル（STP）設定を行います。3 つのバージョンの STP（802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。
ERPS (G.8032)（イーサネットリングプロテクション設定）	「Ethernet Ring Protection Switching」(ERPS) の表示、設定を行います。 ERPS はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。
Loopback Detection（ループバック検知設定）	ループバック検知（LBD）機能の設定を行います。
Link Aggregation（リンクアグリゲーション）	Link Aggregation（リンクアグリゲーション / ポートトランキング機能）の設定を行います。
MLAG（マルチシャーシリンクアグリゲーション）	複数のスイッチでリンクアグリゲーションを設定し、帯域の増加を行います。
Flex Links（フレックスリンクス）	フレックスリンクス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 Contro（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。

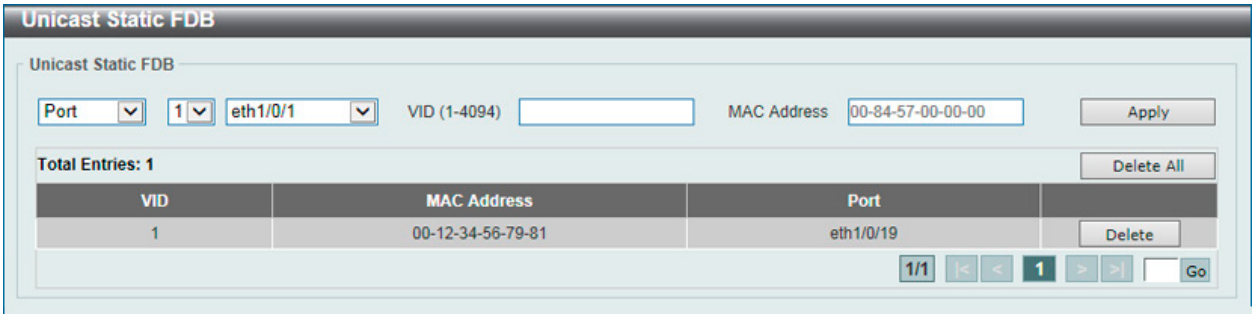


図 8-1　Unicast Static FDB 画面

以下の項目を使用して設定を行います。

項目	説明
Port/Drop	上記 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な FDB から MAC アドレスを破棄します。 • Port - 上記 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な FDB から MAC アドレスを破棄します。
Unit	設定を行うユニットを指定します。
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。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Delete All」をクリックするとすべてのエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

スイッチにスタティックなマルチキャストフォワーディングを設定します。

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

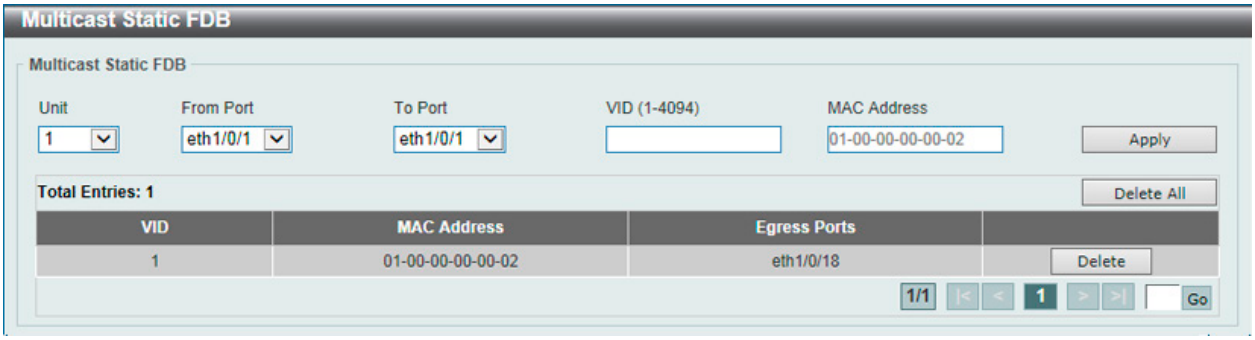


図 8-2　Multicast Static FDB 画面

以下の項目を使用して設定を行います。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
VID	指定の Multicast MAC アドレスが属する VLAN の VLAN ID。
MAC Address	マルチキャストパケットの送信先 MAC アドレス。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。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Delete All」をクリックするとすべてのエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

スイッチの MAC アドレスフォワーディングテーブルを参照します。スイッチが MAC アドレス、VLAN、およびポート番号間の関連性を学習するとテーブルに記載します。それらのエントリは、スイッチ経由でパケットを送信するのに使用されます。

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）

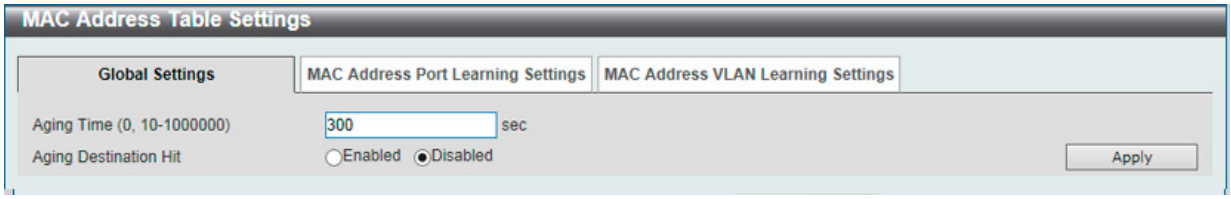


図 8-3　MAC Address Table Settings 画面（Global Settings）

以下の項目を使用して設定を行います。

項目	説明
Aging Time (10-1000000)	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	エージングタイム内に宛先アドレスにより受信します。

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。

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

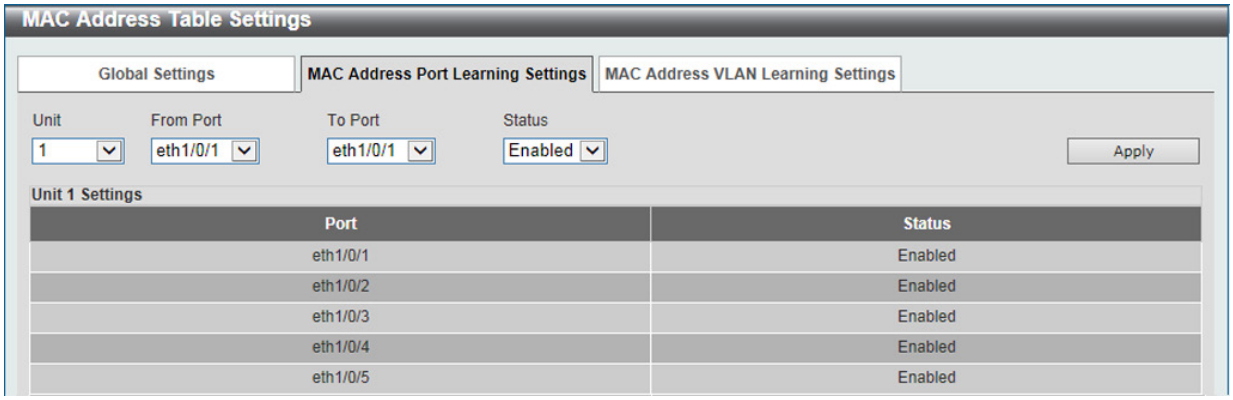


図 8-4　MAC Address Table Settings (MAC Address Port Learning Settings) 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
Status	MAC アドレスラーニングを有効 / 無効にします。

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

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

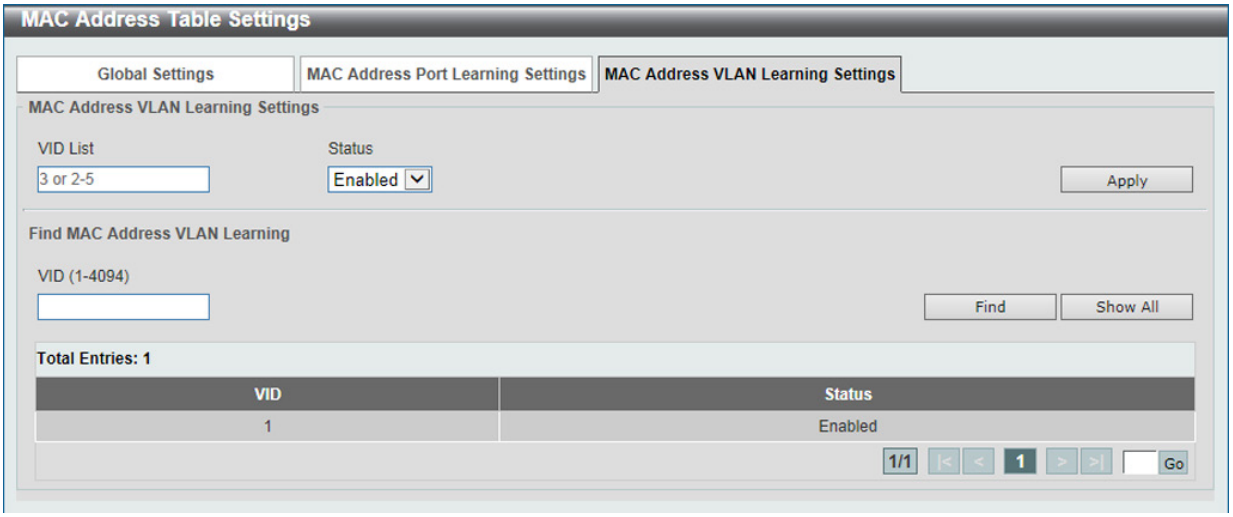


図 8-5　MAC Address Table Settings (MAC Address VLAN Learning Settings) 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
VID List	参照するフォワーディングテーブルの VLAN リストを入力します。
MAC Address	参照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。
Status	MAC アドレスラーニングを有効 / 無効にします。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

MAC Address Table（MAC アドレステーブル）

スイッチの MAC アドレスフォワーディングテーブルを参照します。スイッチが MAC アドレス、VLAN、およびポート番号間の関連性を学習するとテーブルに記載します。それらのエントリは、スイッチ経由でパケットを送信するのに使用されます。

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。

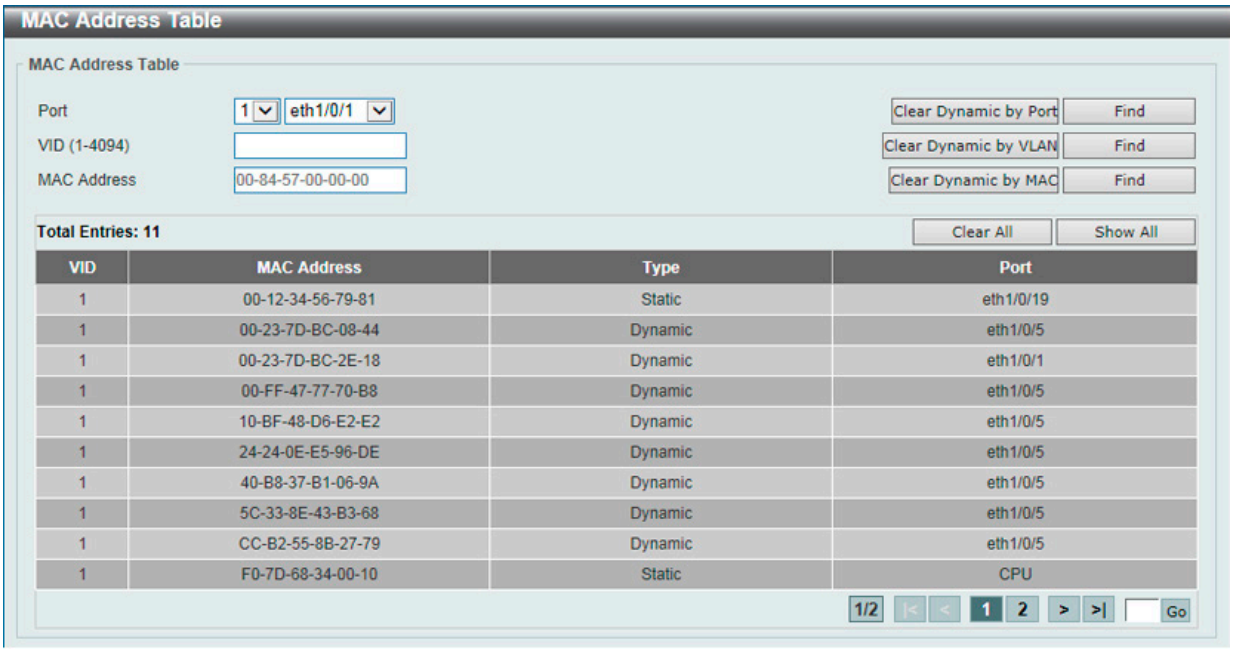


図 8-6　MAC Address Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	以下の MAC アドレスと関連付けられるポートを選択します。

項目	説明
VID	参照するフォワーディングテーブルの VLAN ID を入力します。
MAC Address	参照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
「Find」ボタンをクリックして、指定したポート、VLAN または MAC アドレスをキーとして検索します。

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

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

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

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。

注意 本機能をご使用になる場合、NMS 側で、MAC Notification トラップを受信できる環境が必要になります。E-mail や Syslog における通知には対応しておりません。

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。

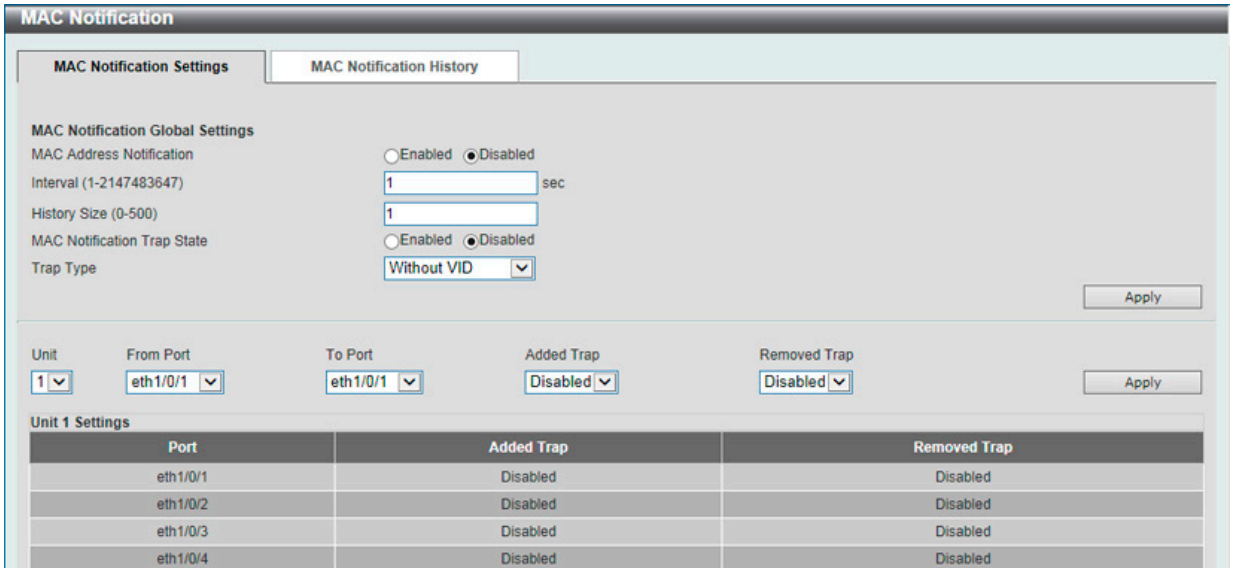


図 8-7　MAC Notification 画面

以下の項目を使用して設定を行います。

項目	説明
MAC Address Notification	スイッチ上の MAC 通知をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
Interval (1-2147483647 sec)	通知を行う間隔（秒）。初期値 : 1（秒）
History Size (0-500)	通知用に使用するヒストリログの最大エントリ数（最大 500 エントリ）。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 を含みません。 • With VID - トラップ情報に VLAN ID を含みます。
Unit	設定するユニットを選択します。
From Port /To Port	プルダウンメニューから、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「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

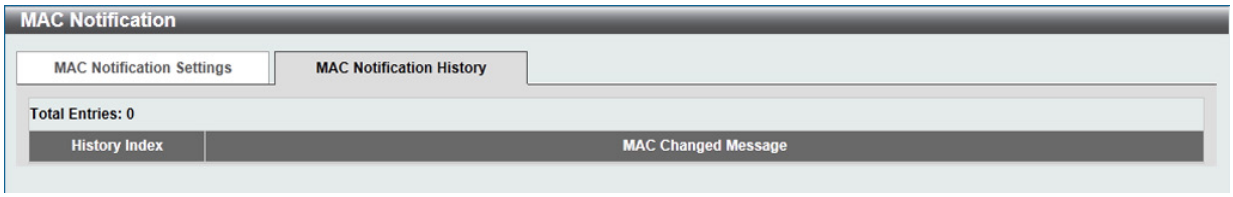


図 8-8　MAC Notification History 画面

MAC 通知メッセージの履歴が表示されます。

VLAN（VLAN 設定）

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

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

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。

VLAN リストの表示

「VLAN List」タブでは、既に設定されている VLAN の VLAN ID と VLAN 名が表示されます。

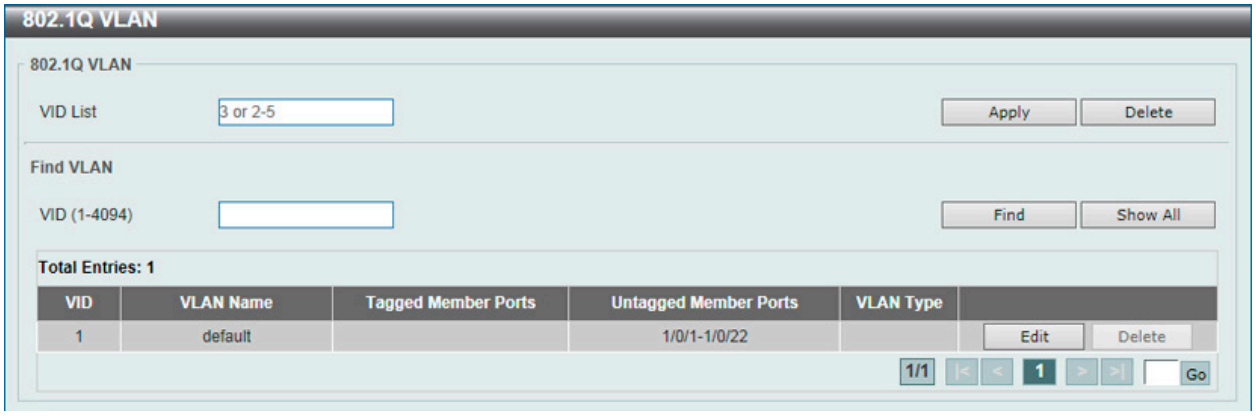


図 8-9　802.1Q VLAN Settings 画面

以下の項目が表示されます。

項目	内容
802.1Q VLAN	
VID List	VID の範囲を指定します。
Find VLAN	
VID(1-4094)	表示する VLAN ID を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

802.1v Protocol VLAN フォルダには次の 2 つの画面があります。:「Protocol VLAN Profile」および「Protocol VLAN Profile Interface」

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

本テーブルで、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。

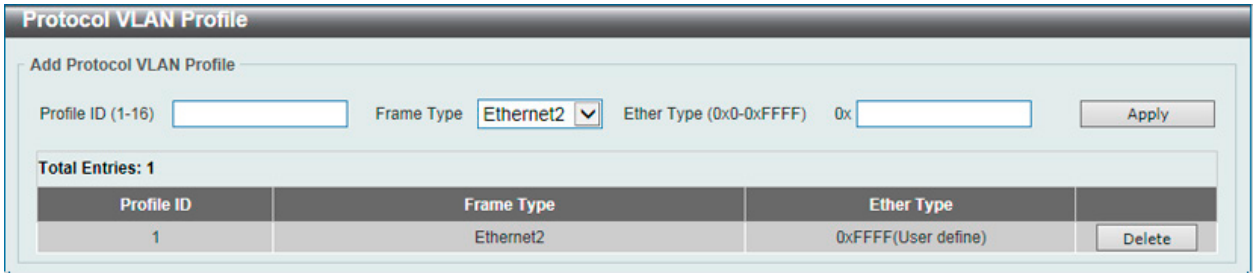


図 8-10　Protocol VLAN Profile 画面

以下の項目を使用して、設定します。

項目	説明
Profile ID	802.1v プロトコル VLAN プロファイル ID 番号を 1-16 の範囲から指定します。
Frame Type	フレームタイプを選択します。本機能は、関連するプロトコルのタイプを検出するためにパケットヘッダのタイプオクテットを検証することで、パケットをプロトコルで定義された VLAN にマップします。「Ethernet 2」「LLC」「SNAP」から選択します。
Ether Type	グループに対してイーサネットタイプを指定します。プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。入力形式は 0x0 から 0xffff です。オクテット文字列は、フレームタイプによって、以下に示す値の 1 つを持っています。 • 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。はじめのオクテットは、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。

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

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

プロトコル VLAN ポートの設定を行います。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。

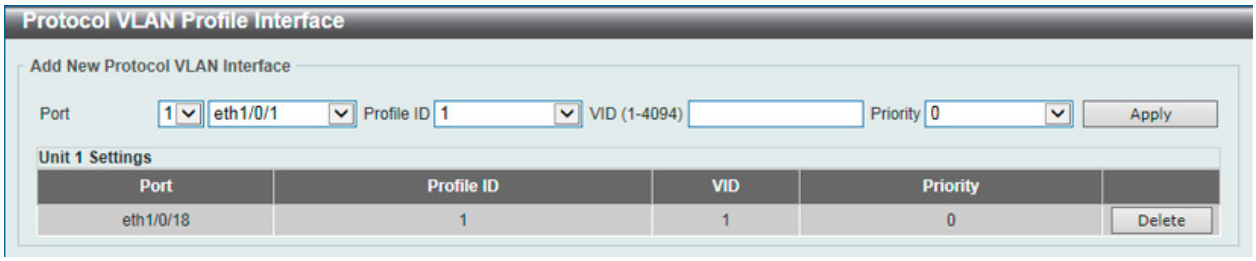


図 8-11　Protocol VLAN Profile Interface 画面

以下の項目を使用して、設定します。

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	対応するボタンをチェックし、プルダウンメニューから定義済みの Profile ID を選択します。
VID (1-4094)	対応するボタンをチェックし、VID を入力します。これは、VLAN 名と共に、ユーザが作成する VLAN を識別するために使用する ID です。
Priority	スイッチに設定済みの 802.1p デフォルトプライオリティ（パケットが送られる CoS キューを決定するために使用）の設定を書き換える場合に使用します。本項目を選択すると、スイッチが受信したパケット内の本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。本画面で設定した基準に一致するパケットが、指定された CoS キューに送られる前に、パケットの 802.1p デフォルトプライオリティを、「Priority（0-7）」に指定した値に書き換える場合に対応するボックスをクリックします。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。

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

GVRP（GVRP の設定）

GVRP Global（GVRP グローバル設定）

GVRP（GARP VLAN Registration Protocol）が有効なスイッチ同士で VLAN 構成情報を共有するかどうかを指定することができます。さらに、Ingress を「Enabled」（有効）にすることで、VID がポートの PVID と一致しない入力パケットをフィルタしてトラフィックを制限します。
設定内容は、設定画面下部のテーブルで参照することができます。

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。

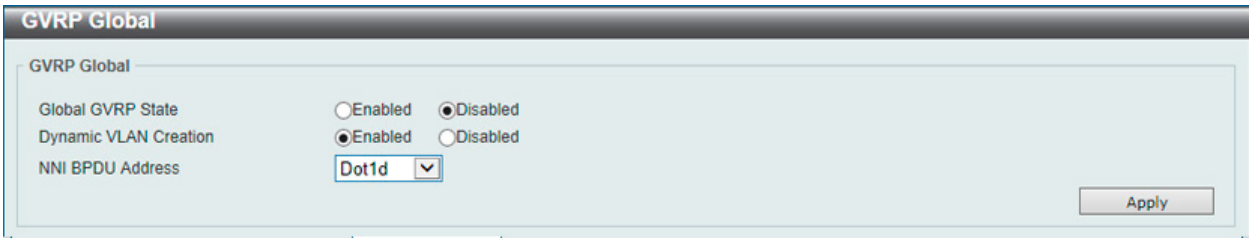


図 8-12　GVRP Global 画面

本画面には次の項目があります。

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。 • Enabled - デバイスで GVRP を有効に設定します。 • Disabled - デバイスで GVRP を無効に設定します。（初期値）
Dynamic VLAN Creation	ダイナミック VLAN クリエーション機能を有効 / 無効に指定します。
NNI BPDU Address	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、802.1ad サービスプロバイダの GVRP アドレスまたはユーザ定義のマルチキャストを使用します。「Dot1d」「Dot1ad」から指定します。

「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

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。

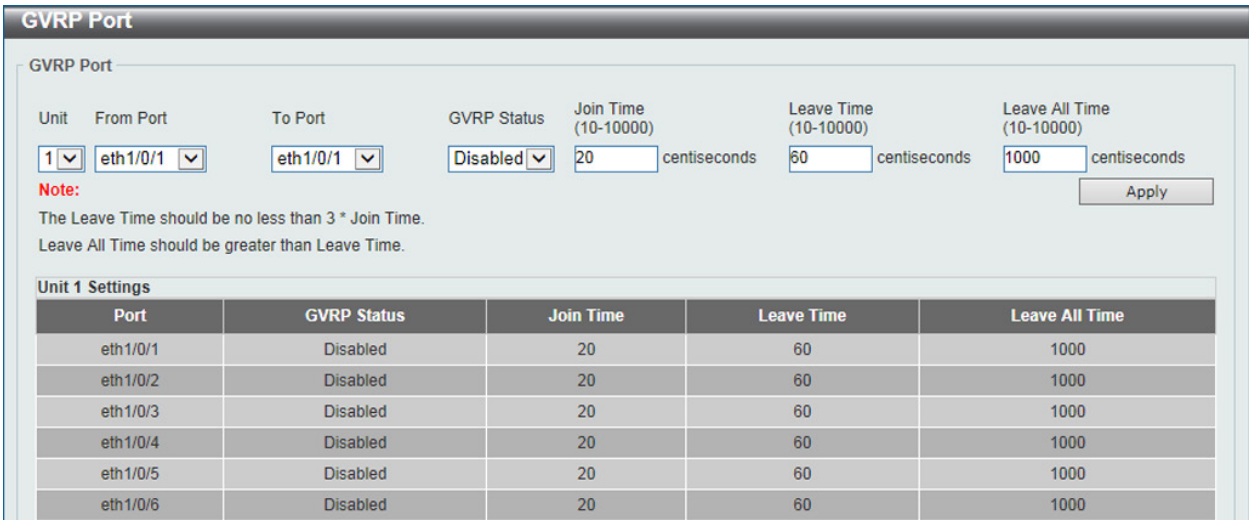


図 8-13　GVRP Port 画面

本画面には次の項目があります。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
GVRP Status	GVRP が各ポートで有効かどうかを設定します。有効にするとポートが自動的に VLAN のメンバになります。 • Enabled - 選択したポートで GVRP を有効にします。 • Disabled - 選択したポートで GVRP を無効にします。（初期値）

項目	説明
Join Time (10-10000)	センチ秒で開始時間を設定します。初期値は 20 です。
Leave Time (10-10000)	センチ秒で終了時間を設定します。初期値は 60 です。
Leave All Time (10-10000)	センチ秒で全終了時間を設定します。初期値は 1000 です。

「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

GVRP Advertise VLAN（GVRP Advertise VLAN 設定）

GVRP advertised VLAN の設定、表示を行います。

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

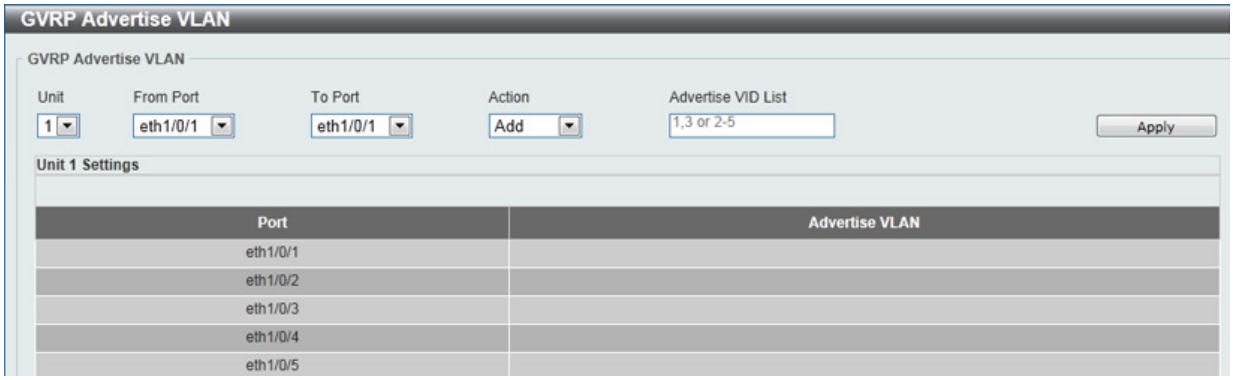


図 8-14　GVRP Advertise VLAN 画面

画面には次の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
Action	アドバタイズ VLAN によるポートマッピングの動作を選択します。「All」「Add」「Remove」「Replace」から選択可能です。「All」を選択するとすべてのアドバタイズ VLAN が使用されます。
Advertise VID List	アドバタイズ VLAN ID を入力します。

「Apply」ボタンをクリックし、設定を適用します。

GVRP Forbidden VLAN（GVRP Forbidden VLAN 設定）

GVRP Forbidden VLAN の設定、表示を行います。

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

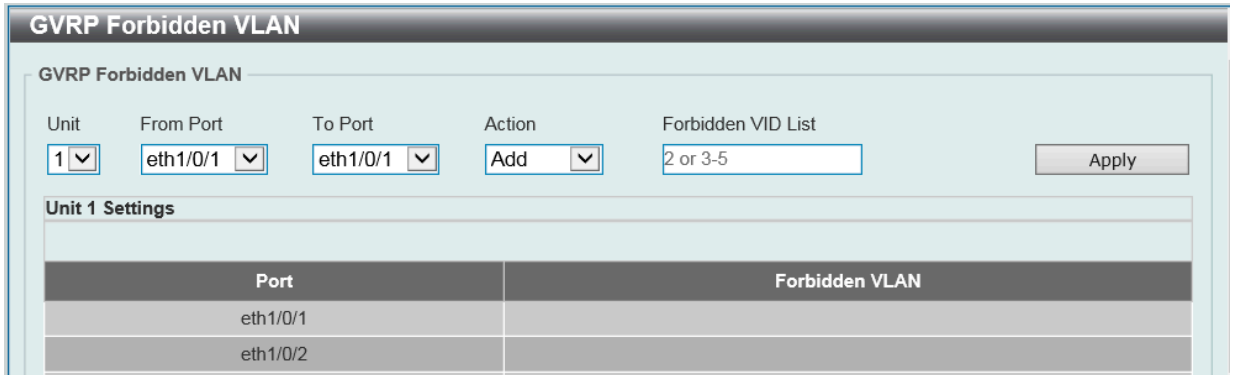


図 8-15　GVRP Forbidden VLAN 画面

画面には次の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
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」「Add」「Remove」「Replace」から選択可能です。「All」を選択するとすべての禁止 VLAN が使用されます。
Forbidden VID List	禁止 VLAN ID を入力します。

「Apply」ボタンをクリックし、設定を適用します。

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。

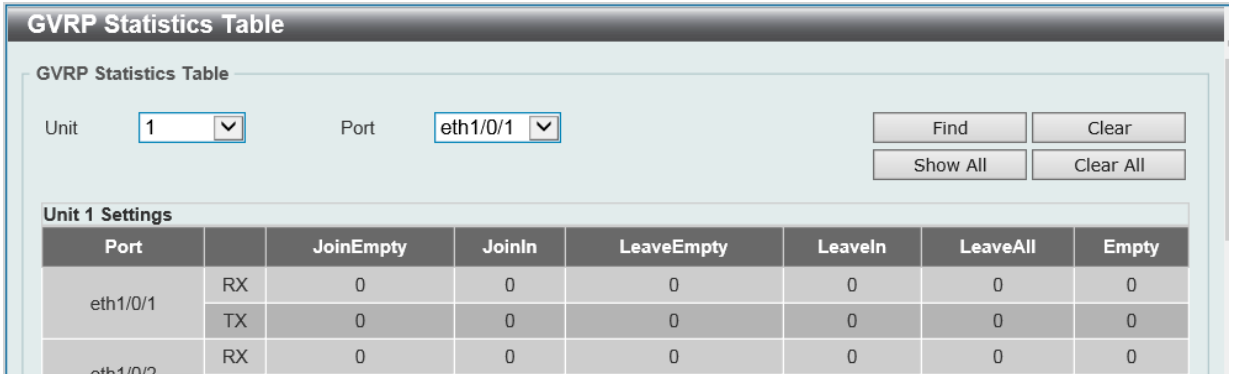


図 8-16　GVRP Statistics Table 画面

画面には次の項目があります。

項目	説明
Unit	統計情報を表示するユニットを指定します。
Port	統計情報を表示するポートを指定します。

エントリの検索

「Find」ボタンをクリックして、エントリを検索します。

エントリの削除

「Clear」ボタンをクリックして、表示されたエントリを削除します。

全エントリの表示

「Show All 」ボタンをクリックして、すべてのエントリを表示します。

全表示エントリの削除

「Clear All 」ボタンをクリックして、すべての表示エントリを削除します。

Asymmetric VLAN（Asymmetric VLAN 設定）

共有 VLAN 学習（SVL : Shared VLAN Learning）は Asymmetric VLAN のための第一の必要条件となる例です。通常の環境下では、VLAN 環境で通信する 1 組の装置は、同じ VLAN を使用して送受信します。しかし、Asymmetric VLAN が必要とされる場合、B に送信するために A に使用される VLAN と A に送信するために使用される VLAN の 2 つの異なる VLAN を使用することが便利です。このタイプの設定が必要とされる例は、クライアントが異なる IP サブネットにある場合、または機密に関連する必要性があり、クライアント間のトラフィックを分ける場合です。

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。

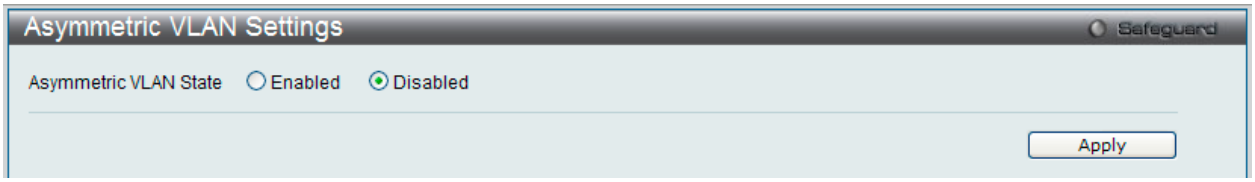


図 8-17　Asymmetric VLAN 画面

「Asymmetric VLAN State」を「Enabled」（有効）または「Disabled」（無効）に設定し、「Apply」ボタンをクリックして、変更を有効にします。

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。

エントリがポートに作成されると、ポートは自動的に指定した VLAN のタグなしメンバポートになります。スタティック MAC ベース VLAN のエントリがユーザに作成されると、このユーザからのトラフィックはこのポートで動作する認証機能に関わらず指定 VLAN の下で送信されます。

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。

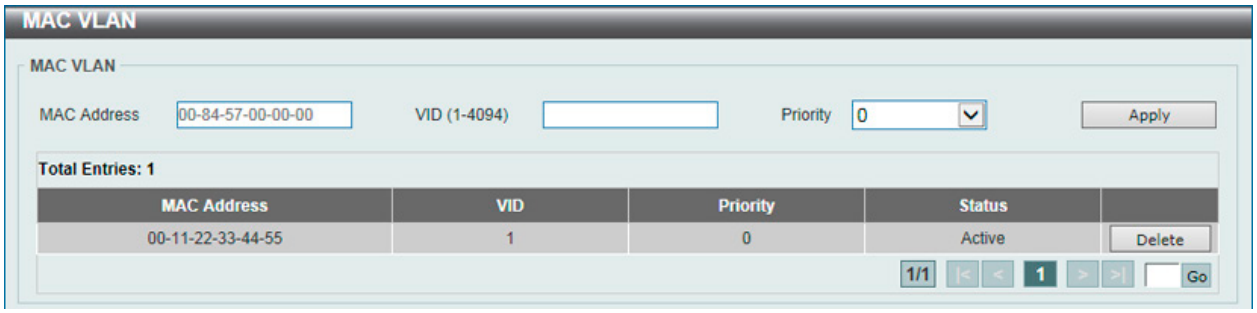


図 8-18　MAC VLAN 画面

以下の項目を使用して設定します。

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（0-7）を選択します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

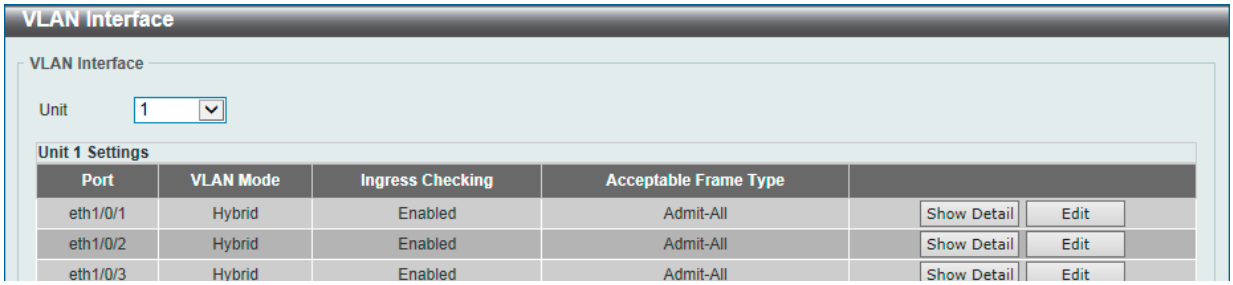


図 8-19　VLAN Interface 画面

項目	説明
Unit	設定、表示するユニットを指定します。

エントリの編集

「Edit」ボタンをクリックして、指定エントリの編集をします。

VLAN 詳細情報の表示

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

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」が選択すると次の画面が表示されます。

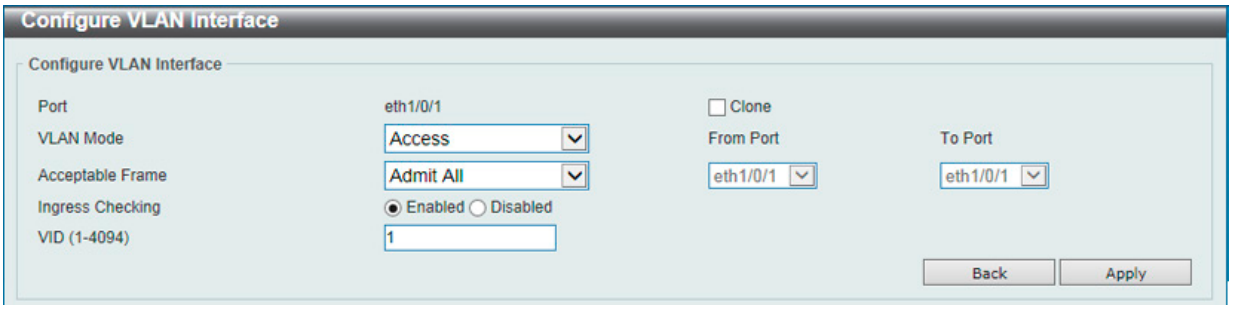


図 8-21　Configure VLAN Interface - Access 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
VID	設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」ボタンをクリックし、設定を適用します。
「Back」をクリックすると前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」が選択すると次の画面が表示されます。

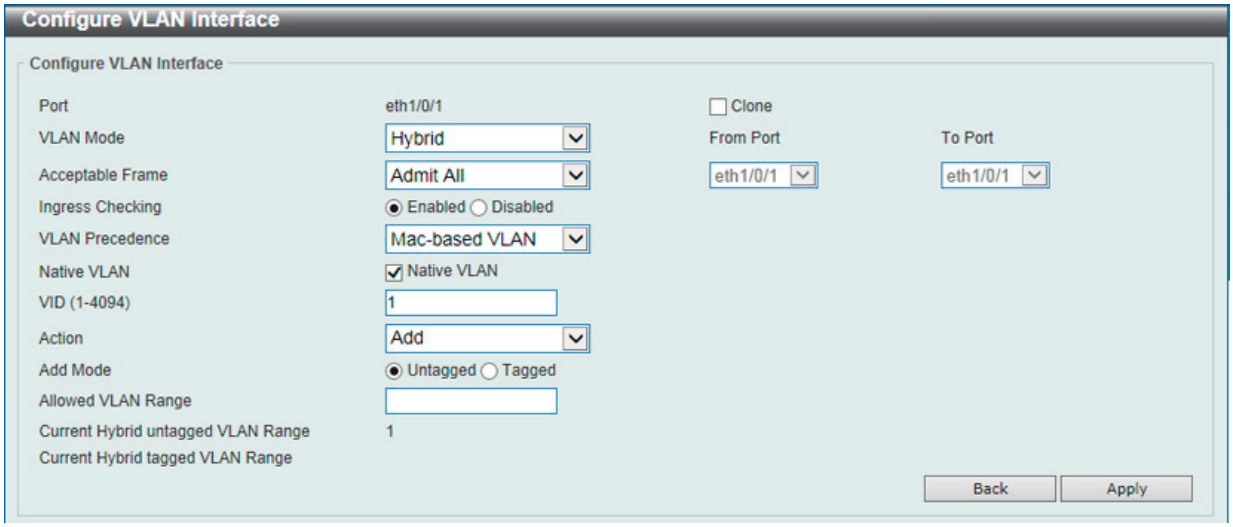


図 8-22　Configure VLAN Interface - Hybrid 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
VLAN Precedence	優先 VLAN を「Mac-based VLAN」「Subnet-based VLAN」から選択します。
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。1 から 4094 で指定可能です。
Action	実行する動作を「Add」「Remove」「Tagged」「Untagged」から選択します。
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	許可した 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	設定するポートの始点 / 終点を設定します。

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

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

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

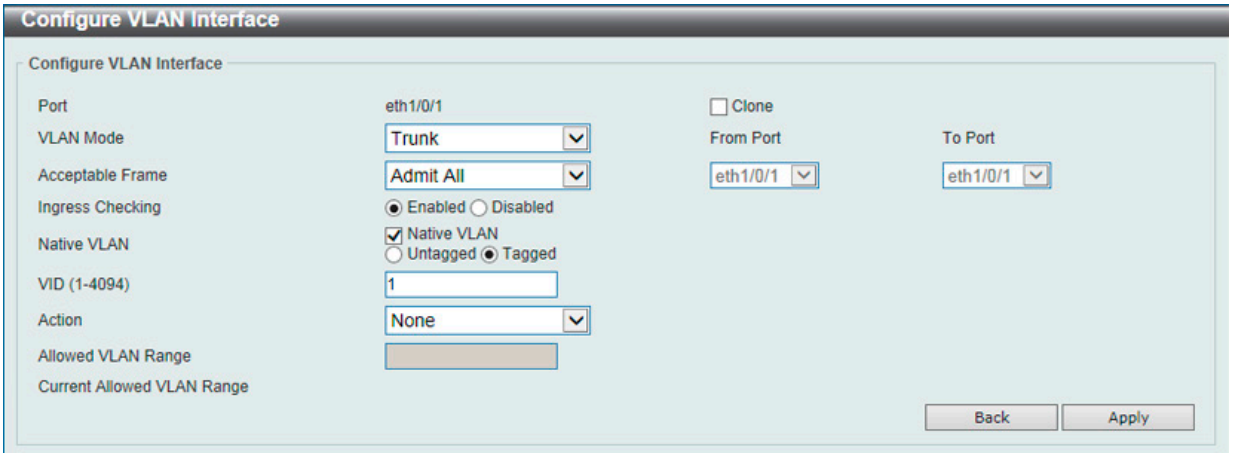


図 8-23　Configure VLAN Interface - Trunk 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	「Native VLAN」を有効にします。また「Native VLAN」が「Untagged」または「Tagged」フレームをサポートしている場合選択します。
VID	「Native VLAN」を有効にした後、「Native VLAN」に設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「All」「Add」「Remove」「Except」「Replace」から選択します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

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

VLAN Mode - 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。

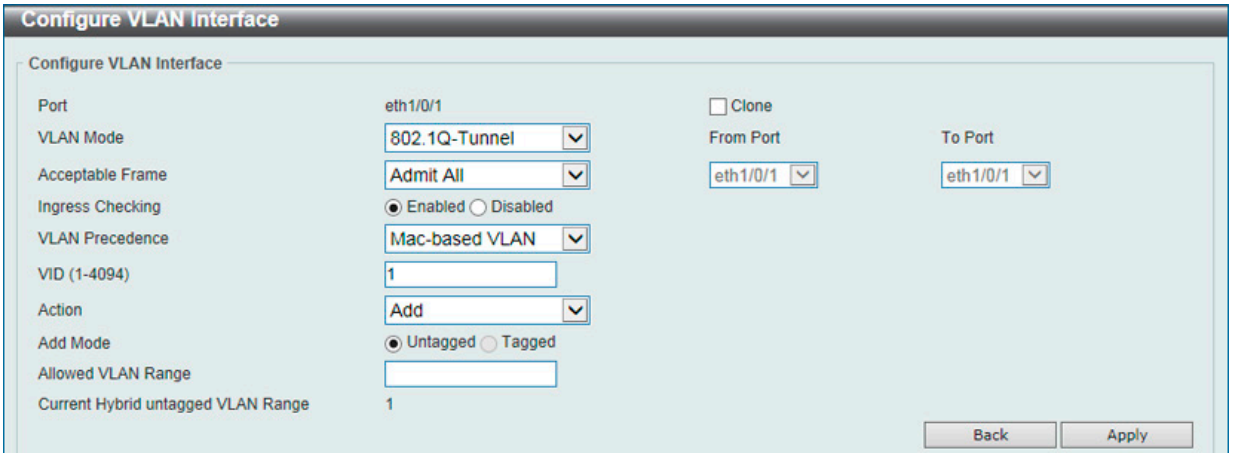


図 8-24　Configure VLAN Interface - 802.1Q-Tunnel 画面

画面には次の項目があります。

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

項目	説明
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
VLAN Precedence	優先 VLAN を「Mac-based VLAN]「Subnet-based VLAN」から選択します。
VID	VLAN に設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「Add」「Remove」から選択します。
Add Mode	Untagged パラメータを追加します。
Allowed VLAN Range	許可した 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	設定するポートの始点 / 終点を設定します。

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

VLAN Mode - 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。

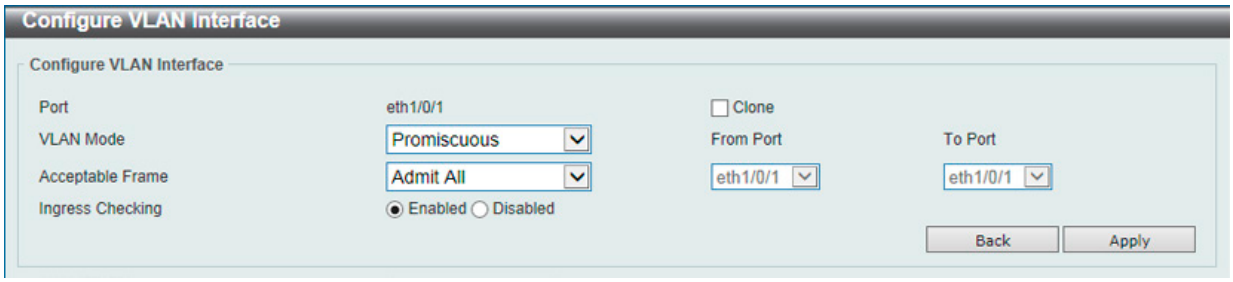


図 8-25　Configure VLAN Interface - Promiscuous 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

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

VLAN Mode - 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。

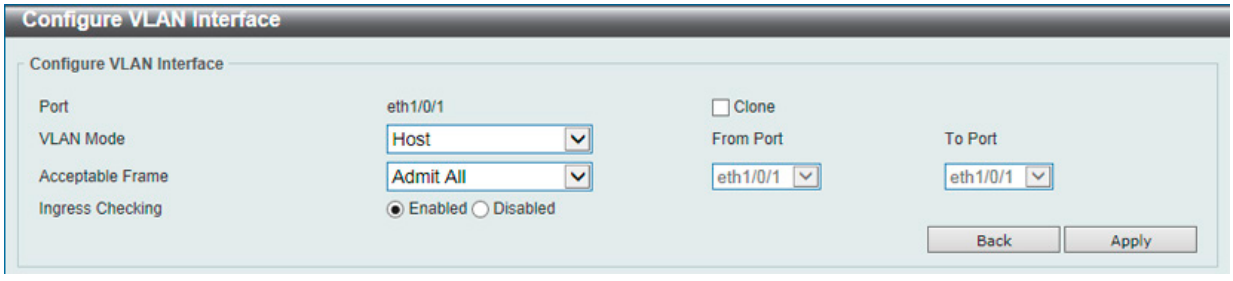


図 8-26　Configure VLAN Interface - Host 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Clone	クローンを有効にします。

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

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

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

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

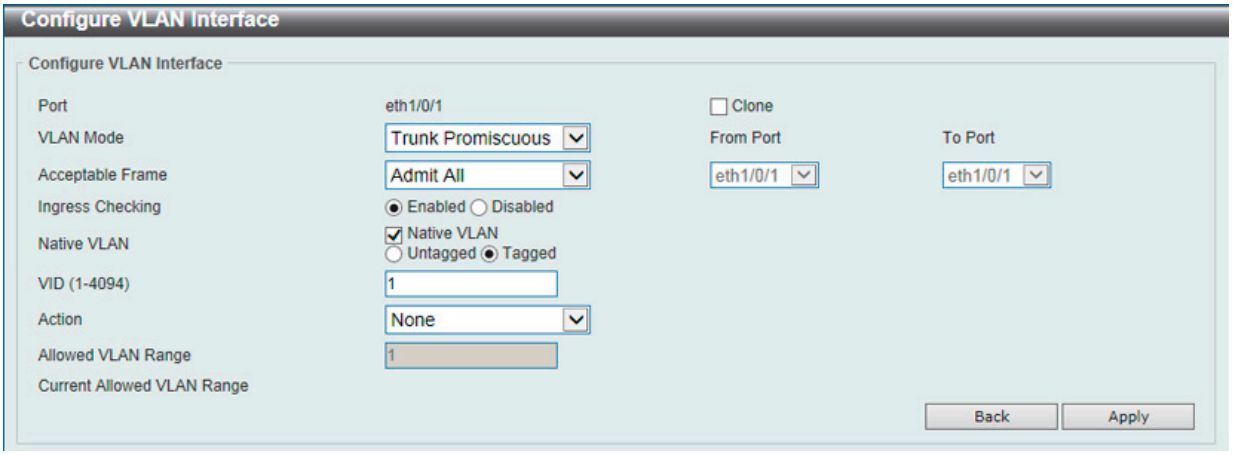


図 8-27　Configure VLAN Interface - Trunk Promiscuous 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	「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。1 から 4094 で指定可能です。
Action	実行する動作を「All」「Add」「Remove」「Except」「Replace」から選択します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

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

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

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

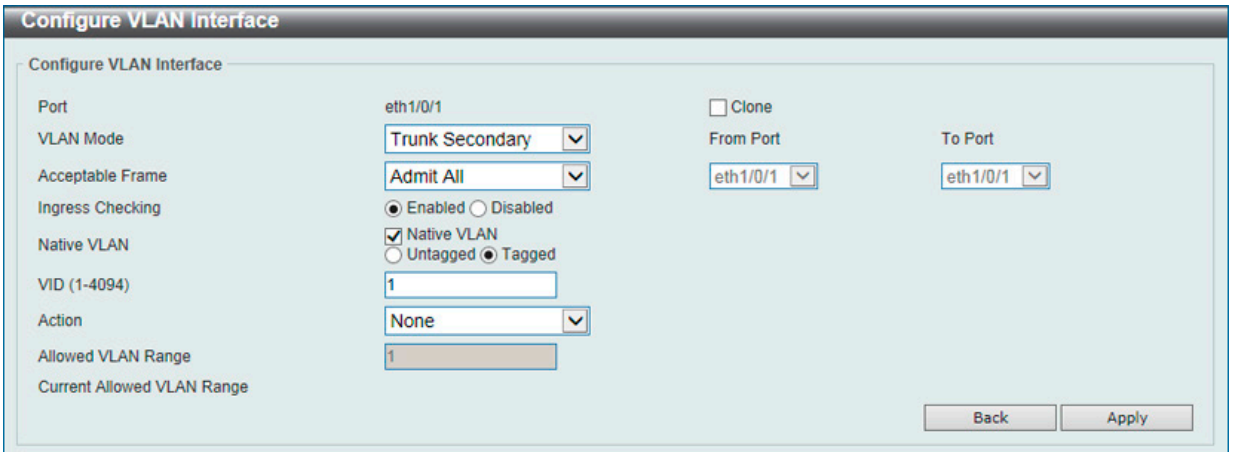


図 8-28　Configure VLAN Interface - Trunk Secondary 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」「802.1Q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	「Native VLAN」を有効にします。「Untagged」「Tagged」フレームも選択します。
VID	「Native VLAN」を有効にした後、「Native VLAN」に設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「All」「Add」「Remove」「Except」「Replace」から選択します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Clone	クローンを有効にします。
From Port / To Port	設定するポートの始点 / 終点を設定します。

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

L2VLAN Interface Description（L2VLAN インタフェース概要）

L2 VLAN インタフェースの概要について表示、設定を行います。

L2 Features > VLAN > L2VLAN Interface Description をクリックします。次の画面が表示されます。

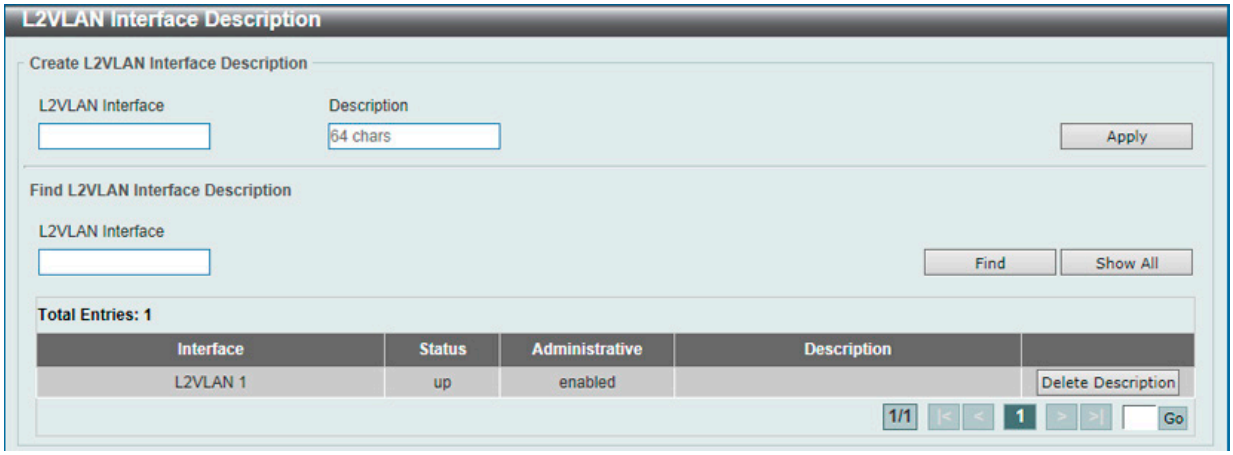


図 8-29　L2VLAN Interface Description 画面

画面には次の項目があります。

項目	説明
L2VLAN Interface	L2 VLAN インタフェースの ID を指定します。
Description	L2 VLAN インタフェースの概要を入力します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Delete Description」をクリックすると指定の L2 VLAN の概要を削除します。
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。

Subnet VLAN（サブネット VLAN）

サブネット VLAN エントリは IP サブネットベースの VLAN クラシフィケーションルールです。ポートにタグなしまたはプライオリティタグを持つ IP パケットを受信すると、送信元 IP アドレスがサブネット VLAN エントリへの照合のために使用されます。エントリのサブネットに送信元 IP があると、パケットはこのサブネットのために定義された VLAN に分類されます。

サブネット VLAN のパラメータを設定します。

L2 Features > VLAN > Subnet 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 8-30　Subnet VLAN 画面

以下の項目を使用して設定します。

項目	説明
IPv4 Network Prefix / Prefix Length	使用する IPv4 アドレスとプレフィクス長を入力します。
IPv6 Network Prefix / Prefix Length	使用する IPv6 アドレスとプレフィクス長を入力します。
VID	VID 値のリストを入力します。
Priority	優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Super VLAN（Super VLAN 設定）（EI/MI モードのみ）

Super VLAN は、同じ IP サブネットにある複数のサブ VLAN を集約するために使用されます。サブ VLAN は L2 の独立したブロードキャストドメインです。Super VLAN はホストがサブ VLAN にある物理メンバポートを持つことができません。一度、IP インタフェースが Super VLAN に割り当てられると、プロキシ ARP はサブ VLAN 間の通信のためにインタフェースで自動的に有効にされます。IP インタフェースが Super VLAN に割り当てられると、他の VLAN に割り当てられることはできなくなります。Super VLAN は他の Super VLAN のサブ VLAN となることはできません。

注意

1. 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。
2. L3 ルートプロトコル、マルチキャストプロトコルは Super VLAN インタフェースで動作できません。

Super VLAN を設定します。

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。

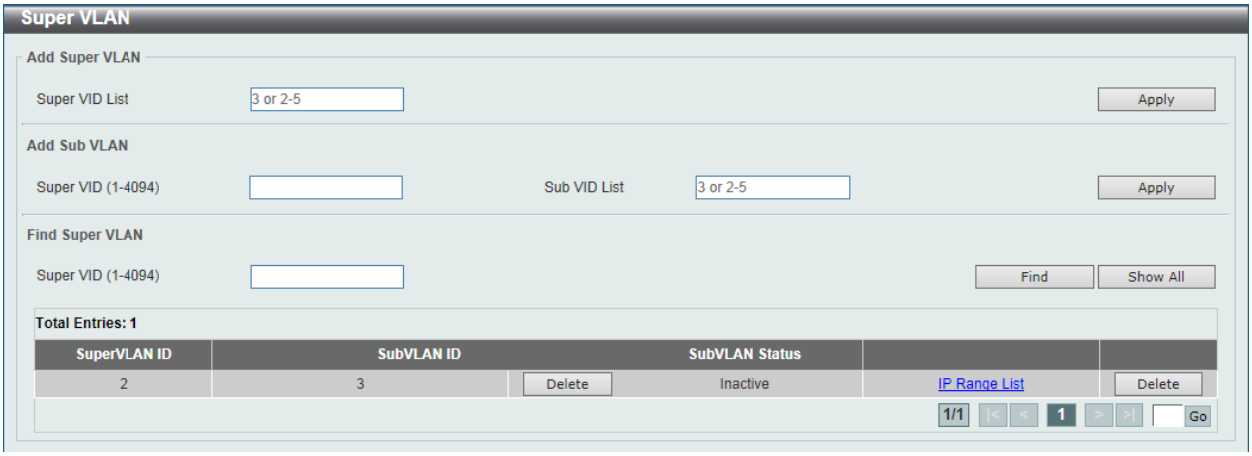


図 8-31　Super VLAN Settings 画面

以下の項目を使用して設定します。

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（1 - 4094）を入力します。
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（1 - 4094）を入力します。

「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「IP Range List」をクリックするとサブ VLAN に IP 範囲を指定することができます。

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。

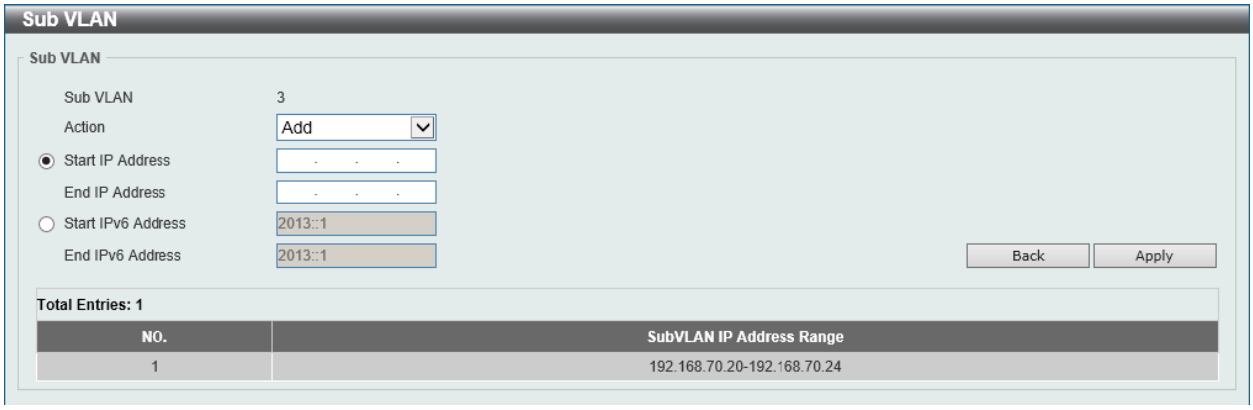


図 8-32　Sub VLAN Settings - IP Range List 画面

以下の項目を使用して設定します。

項目	説明
Action	サブ VLAN の指定 IP アドレスを追加（Add）または削除（Remove）します。
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。
Start IPv6 Address	開始 IPv6 アドレスを入力します。
End IPv6 Address	終了 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。
「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。

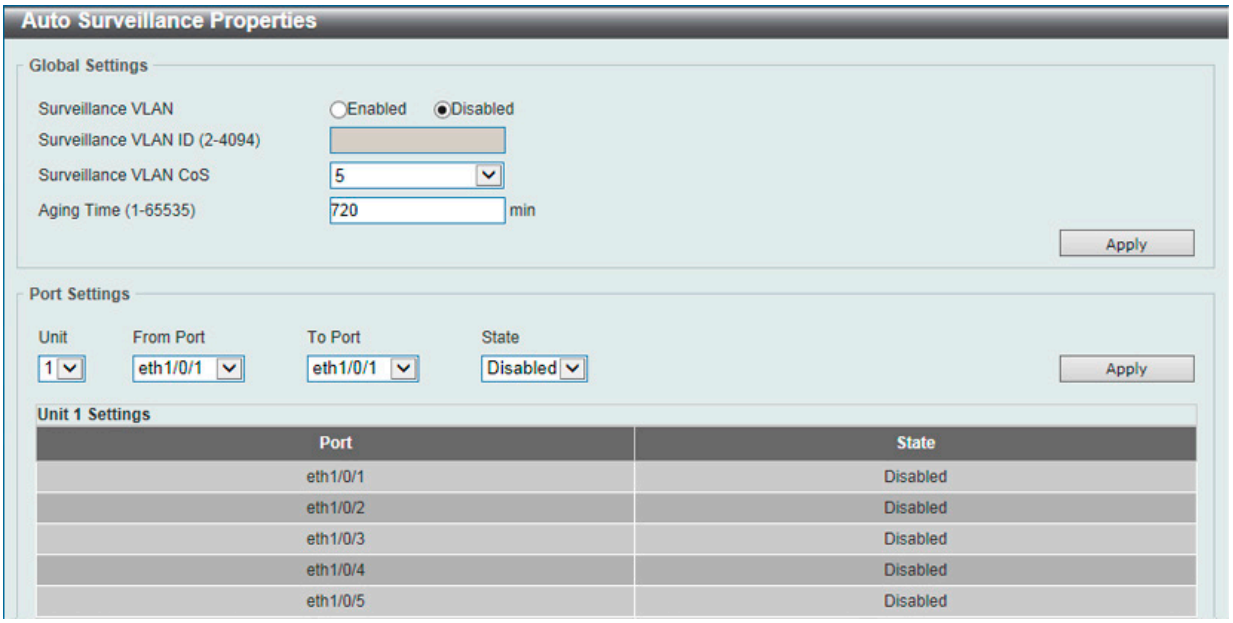


図 8-33　Auto Surveillance Properties 画面

画面には次の項目があります。

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。2 から 4094 で指定できます。
Surveillance VLAN CoS	サーベイランス VLAN の優先値を指定します。0 から 7 で指定できます。
Aging Time	エージングタイム（1-65535 分）を設定します。 初期値は 720（分）です。 エージングタイムは、ポートがオートサーベイランス VLAN メンバである場合にサーベイランス VLAN からポートを削除するために使用されます。最後のサーベイランスデバイスが、トラフィックの送信を止めて、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。サーベイ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。
Port Settings	
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
State	指定したポートでサーベイランス VLAN を有効 / 無効にします。 サーベイランス VLAN が有効な場合、ポートはアンタグのサーベイランス VLAN メンバとして自動的に学習され、受信したアンタグのサーベイランスパケットはサーベイランス VLAN に転送されます。受信したパケットの送信元 MAC アドレスが OUI（Organizationally Unique Identifier）アドレスに一致している場合、そのパケットはサーベイランスパケットとして認識されます。

「Apply」ボタンをクリックし、設定を適用します。

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

ユーザ定義のサーベイランストラフィックの OUI を設定します。

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

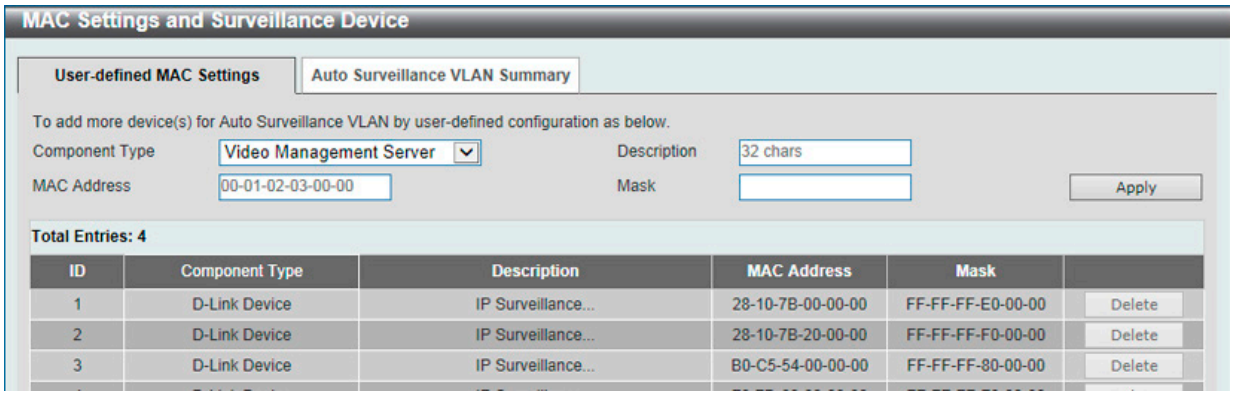


図 8-34　User -defined MAC Settings 画面

以下の項目を使用して設定します。

項目	説明
Component Type	プルダウンメニューを使用して、サーベイランス VLAN が自動検出可能なサーベイランスコンポーネントを選択します。選択可能項目は次の通りです。:「Video Management Server」「VMS Client/Remote Viewer」「Video Encoder」「Network Storage」「Other IP Surveillance Device」
Description	ユーザ定義 OUI に関する説明を入力します。（最大 32 文字）
MAC Address	ユーザ定義の OUI MAC アドレスを入力します。
Mask	ユーザ定義 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。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

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。

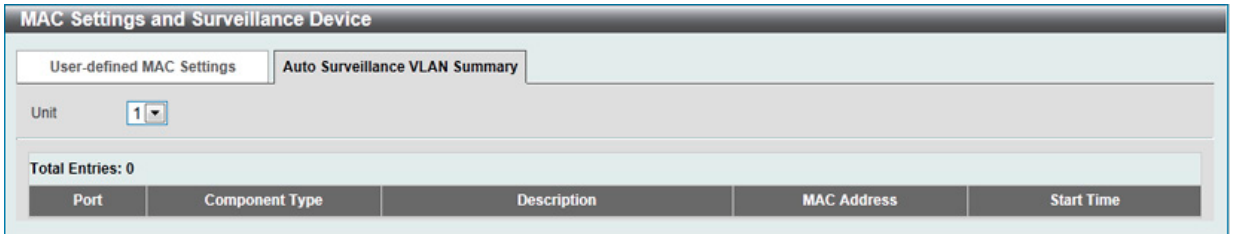


図 8-35　Auto Surveillance VLAN Summary 画面

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。

音声 VLAN をグローバルに有効 / 無効にします。

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

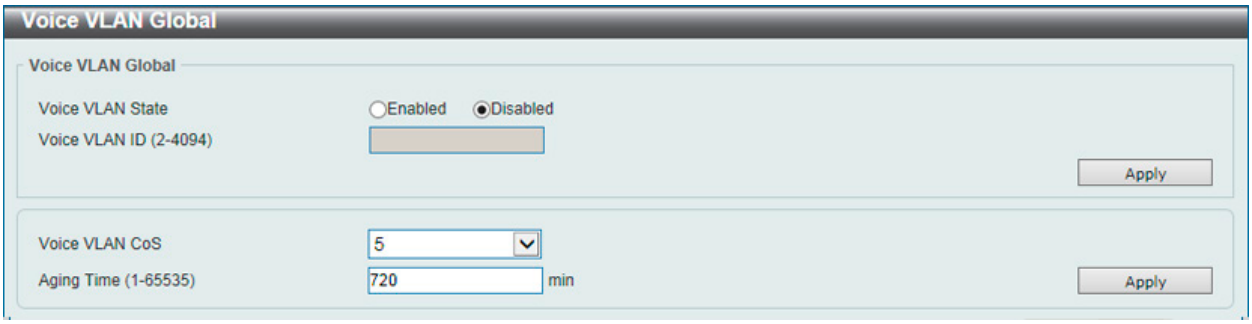


図 8-36　Voice VLAN Global Settings 画面

以下の項目を使用して設定します。

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

音声 VLAN の有効化

「Voice VLAN State」を「Enabled」にして音声 VLAN を有効にする VLAN を「Voice VLAN Name」または「Voice VID」で指定後、「Apply」ボタンをクリックします。

音声 VLAN のパラメータ設定

音声 VLAN の有効後、「Priority」、「Aging Time」または「Log State」を設定後、「Apply」ボタンをクリックします。

Voice VLAN Port（音声 VLAN のポート設定）

ポートの音声 VLAN 情報を表示します。

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

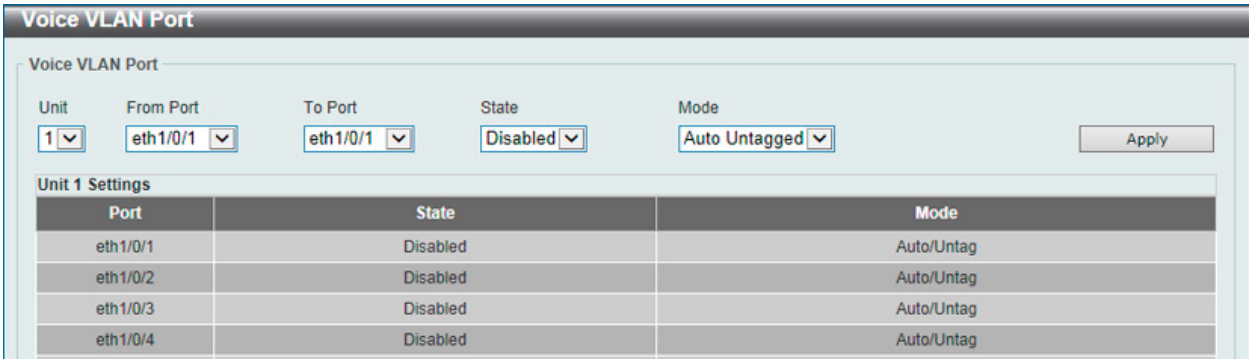


図 8-37　Voice VLAN Port 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を選択します。
State	指定ポートの音声 VLAN 機能を有効 / 無効に設定します。 音声 VLAN が有効になると、受信した音声パケットは音声 VLAN として送信されます。受信した音声 VLAN パケットの送信元 MAC アドレスが OUI アドレスに一致すると、音声 VLAN と認識されます。

項目	説明
Mode	モードを選択します。 • Auto Untagged - タグなしの音声 VLAN が自動的に学習されます。 • Auto Tagged - タグ付きの音声 VLAN タ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お優先度は変更されます。タグなしパケットは音声 VLAN で転送されます。 スイッチが LLDP-MED パケットを受信した場合、VLAN ID、Tagged フラグ、優先度フラグがチェックされます。スイッチは Tagged フラグ、優先度フラグに従います。

「Apply」ボタンをクリックして行った変更を適用します。

Voice VLAN OUI（音声 VLAN OUI 設定）

ユーザ定義の音声トラフィックの OUI を設定します。
OUI は音声トラフィックを識別するために使用されます。多くの定義済み OUI があり、必要に応じて、さらにユーザ定義の OUI を設定できます。
ユーザ定義 OUI は定義済みの OUI と同じ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。

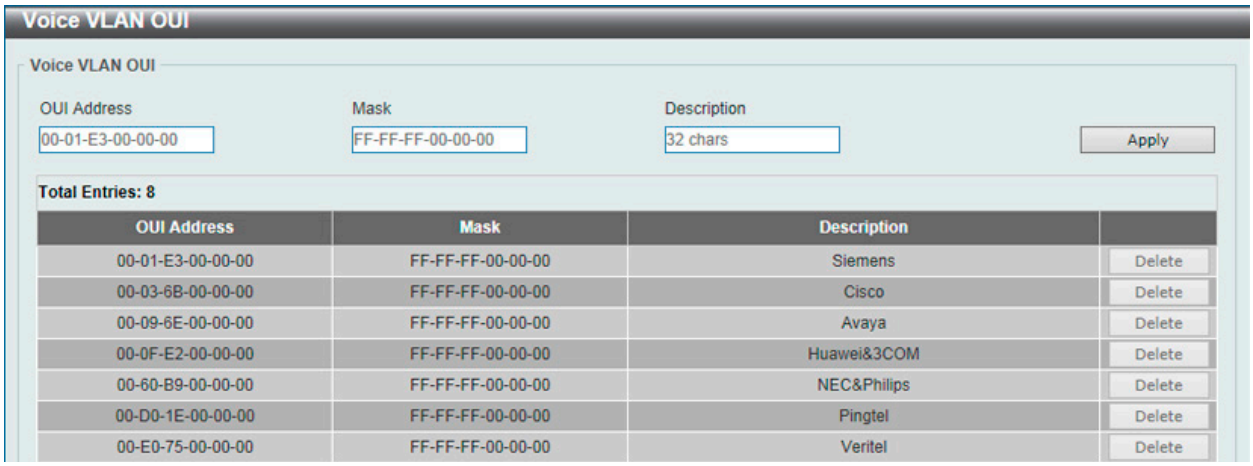


図 8-38　Voice VLAN OUI 画面

以下の項目を使用して設定します。

項目	説明
OUI Address	ユーザ定義の OUI MAC アドレス。
Mask	ユーザ定義 OUI MAC アドレスマスク。
Description	ユーザ定義 OUI に関する説明文。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの削除
「Delete」ボタンをクリックして、指定エントリを削除します。

Voice VLAN Device（音声 VLAN デバイス）

ポートに接続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る時間です。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。

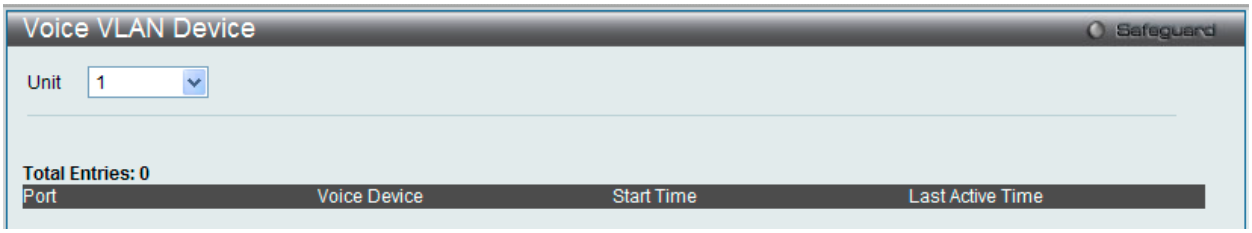


図 8-39　Voice VLAN Device 画面

以下の項目を使用して設定します。

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。

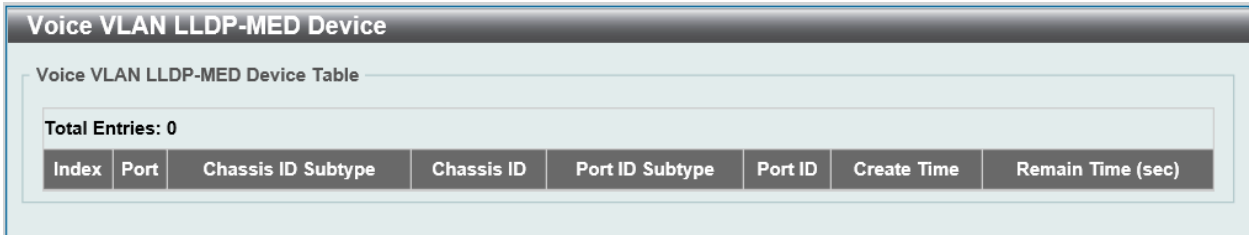


図 8-40　Voice VLAN LLDP-MED Voice Device 画面

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。

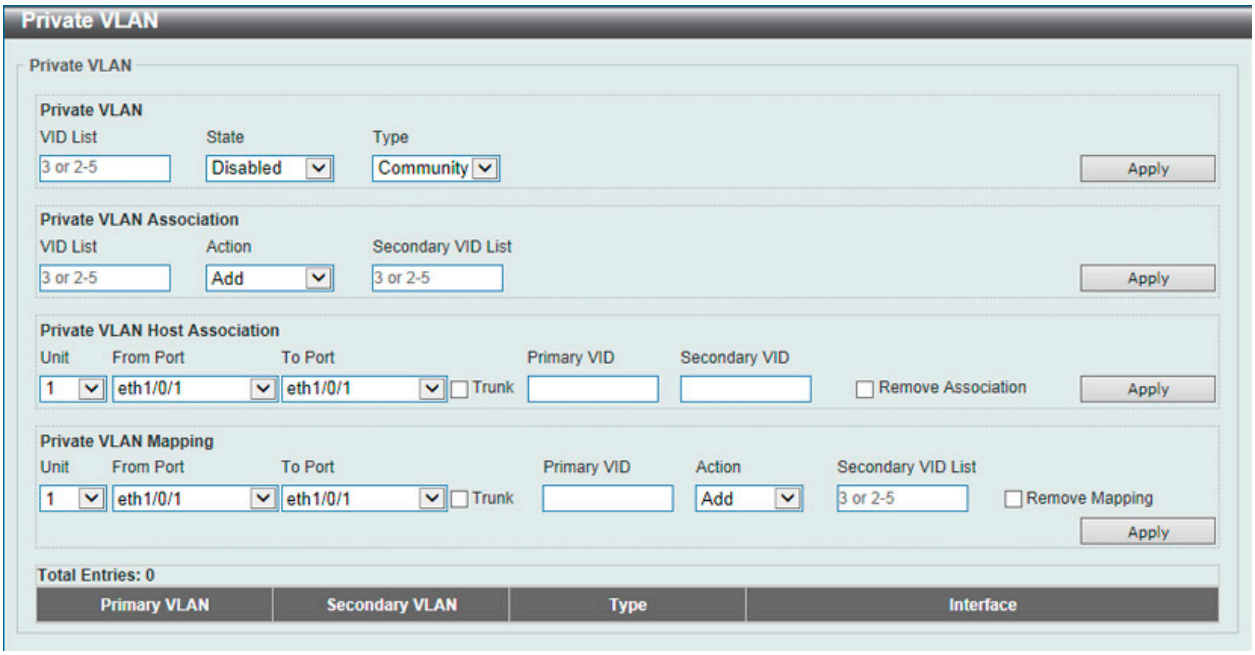


図 8-41　Private VLAN 画面

以下の項目を使用して設定します。

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。「Community」「Isolated」「Primary」から指定します。
Private VLAN Association	
VID List	VLAN ID のリストを指定します。
Action	プライベート VLAN の動作を指定します。「Add」「Remove」「Disabled」から指定します。
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	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。「Trunk」オプションをチェックすると本設定にトランクポートを指定します。
Primary VID	プライマリ VLAN ID を入力します。
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	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。「Trunk」オプションをチェックすると本設定にトランクポートを指定します。
Primary VID	プライマリ VLAN ID を入力します。
Action	「Add」- 入力した情報に基づきエントリを追加します。 「Remove」- 入力した情報を削除します。
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。

「Apply」をクリックし、設定内容を適用します。

VLAN Tunnel（VLAN トンネル）

L2 Features > VLAN Tunnel
VLAN トンネルの設定を行います。

Dot1q Tunnel（Dot1q トンネル）

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 においての「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。
プロバイダブリッジネットワークに接続するポートの、802.1Q トンネリングイーサネットタイプのみを設定すると、サービス VLAN のタグ付きフレームを送受信します。トンネルイーサネットタイプが設定されると、指定の値は選択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。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。

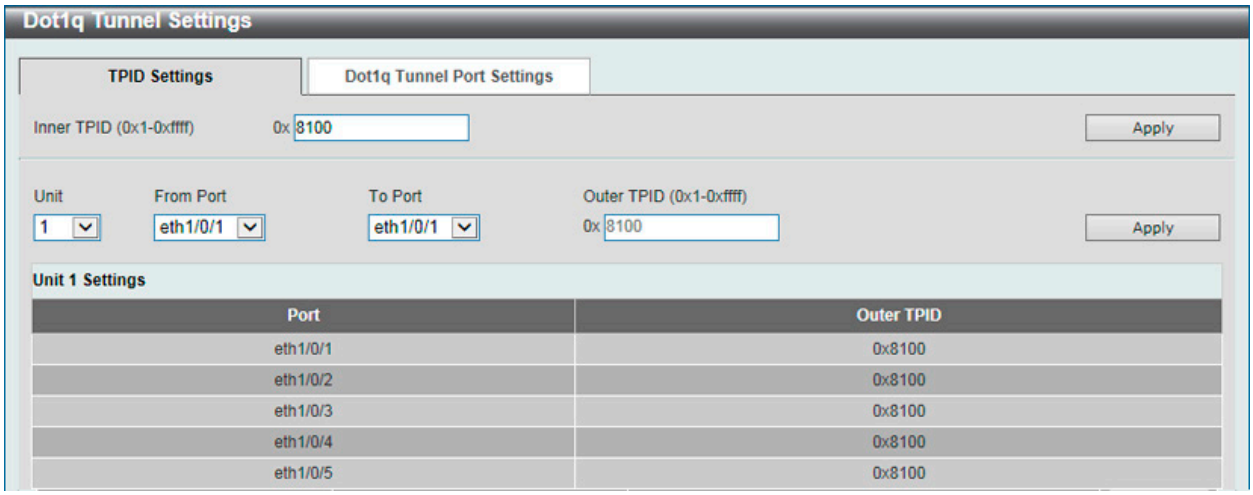


図 8-42　Dot1q Tunnel（TPID Settings）画面

以下の項目を使用して設定します。

項目	説明
Inner TPID	インナー TPID 値を指定します。16 進数方式です。「0x1」から「0xFFFF」の間で指定します。インナー TPID はイングレスパケットが「C タグ付き」であるかを指定します。このインナー TPID は各システムで設定されます。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Outer TPID	アウター TPID 値を指定します。16 進数方式です。「0x1」から「0xFFFF」の間で指定します。

「Apply」ボタンをクリックして行った変更を適用します。

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。

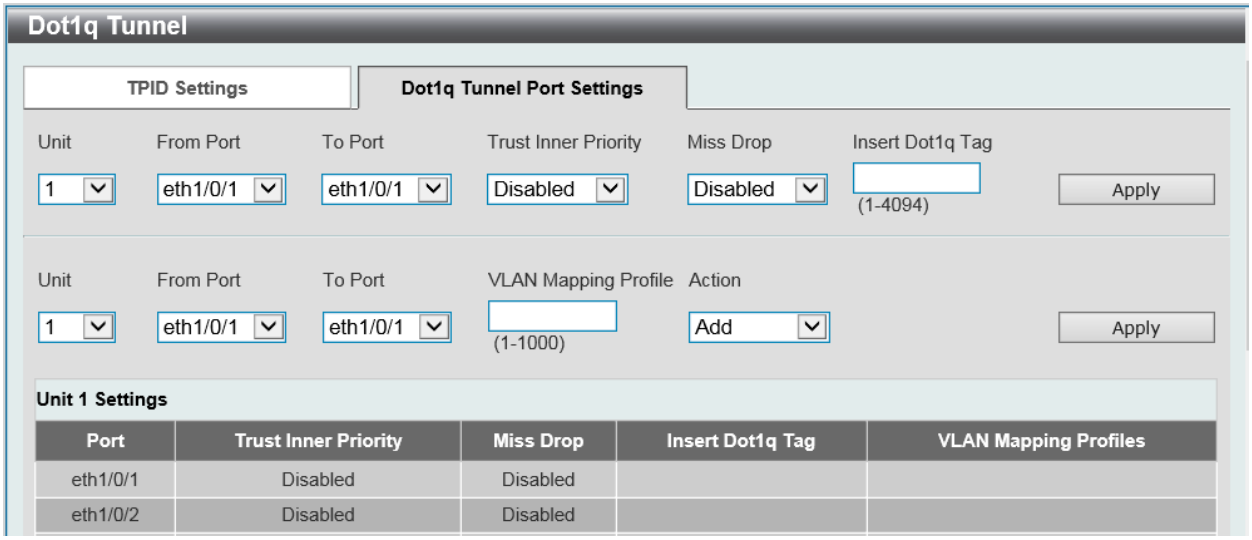


図 8-43　Dot1q Tunnel（Dot1q Tunnel Port Settings）画面

以下の項目を使用して設定します。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Trust Inner Priority	「802.1Q Inner Trust Priority」を有効 / 無効に指定します。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 / 無効に指定します。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 は VLAN マッピングエントリやポートのルールとマッチしなくなり、パケットは破棄されます。
Insert Dot1q Tag	802.1Q トンネルポートに受信したタグなしパケットに挿入される 802.1Q VLAN ID を 1 から 4094 の間で指定します。
VLAN Mapping Profile	VLAN マッピングプロファイル ID（1-1000）を指定します。値が低い方が優先度が高くなります。
Action	「Add」- 入力した情報に基づきエントリを追加します。 「Remove」- 入力した情報を削除します。

「Apply」ボタンをクリックして行った変更を適用します。

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アプライされると、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操作が実行されます。この操作は「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、最初の操作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。複数のタイプのプロファイルが一つのインタフェースに設定可能です。

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。

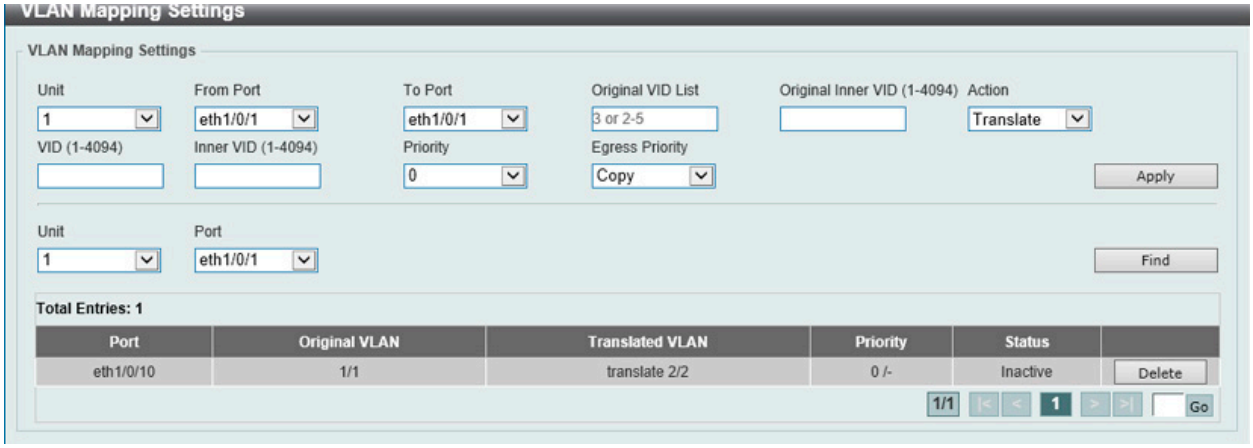


図 8-44　VLAN Mapping 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
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（1-4094）を指定します。
Original Inner VID	オリジナルのインナー VID（1-4094）を指定します。
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。 • 「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。 • 「Dot1q-tunnel」- マッチしたパケットに出力 VID を追加します。
VID	VLAN ID（1-4094）を指定します。
Inner VID	インナー VLAN ID（1-4094）を指定します。
Priority	優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
Egress Priority	VLAN トンネルインタフェースのイーグレス C タグ（C-tag）優先値を指定します。次の項目から選択します。 • Copy - サービス VLAN 優先値のコピーを使用します。 • 0 to 7 - イーグレス C-tag 優先値を 0-7 の範囲で指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

VLAN Mapping Profile（VLAN マッピングプロファイル）

本項目では VLAN マッピングプロファイルの設定、表示を行います。

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

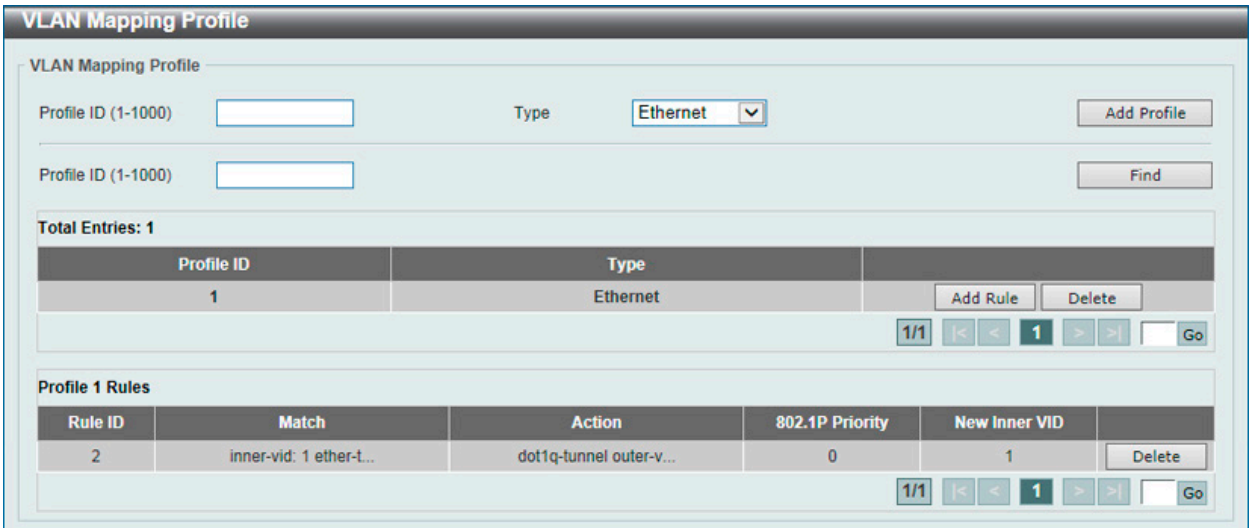


図 8-45　VLAN Mapping Profile 画面

以下の項目を使用して設定します。

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。1-1000 の範囲で指定できます。値が低い方が優先度が高くなります。
Type	プロファイルタイプを「Ethernet」「IP」「IPv6」「Ethernet-IP」から指定します。 • Ethernet - L2 項目にマッチするプロファイルを指定します。 • IP - L3 IP 項目にマッチするプロファイルを指定します。 • IPv6 - IPv6 宛先 / 送信元アドレスにマッチするプロファイルを指定します。 • Ethernet-IP - L2/L3 IP 項目にマッチするプロファイルを指定します。

「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。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Add Rule」をクリックし、新しいルールを追加します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

「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。

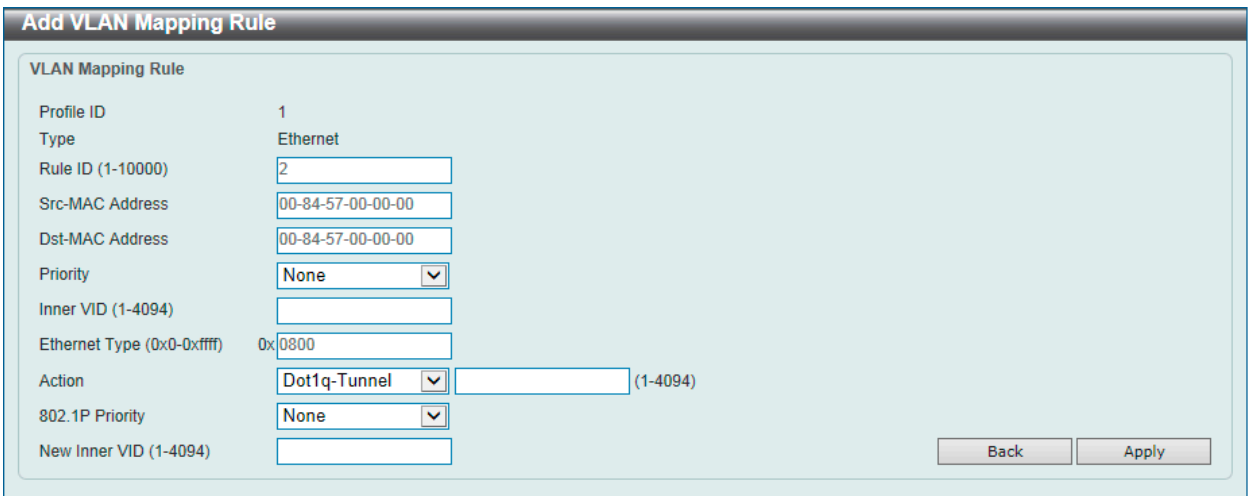


図 8-46　Add VLAN Mapping Rule（Ethernet）画面

以下の項目を使用して設定します。

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。1 から 10000 の間で指定可能です。
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。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
Inner VID	インナー VLAN ID（1-4094）を指定します。
Ethernet Type	イーサネットタイプを指定します。「0x0」から「0xFFFF」の間で指定可能です。
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。 • 「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。 • 「Dot1q-tunnel」- マッチ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（1-4094）を指定します。
802.1P Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID（1-4094）を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。

「Back」をクリックすると前のページに戻ります。
「Apply」をクリックし、設定内容を適用します。

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。

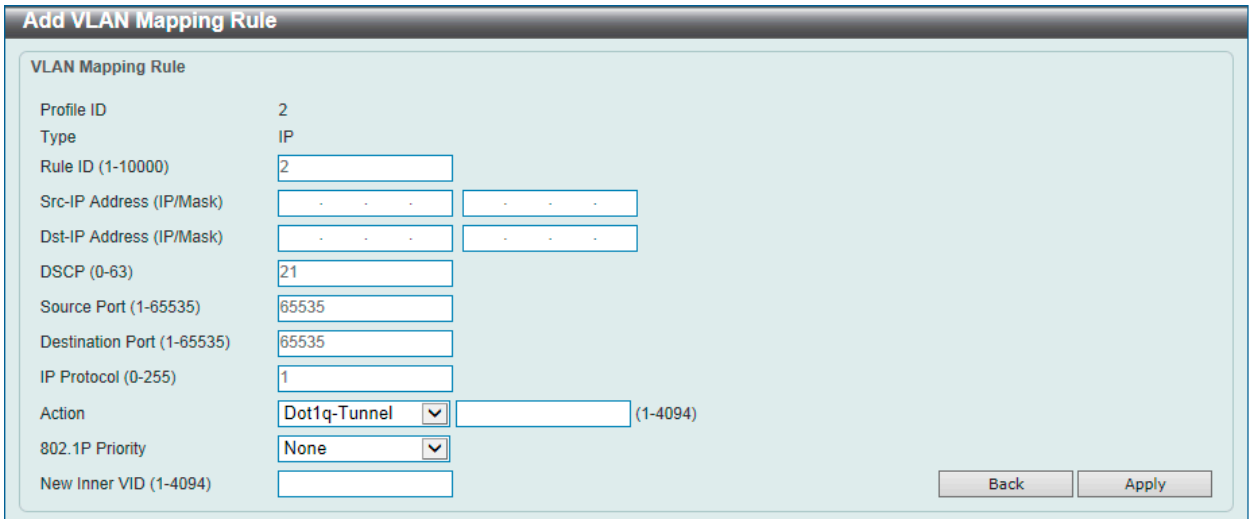


図 8-47　Add VLAN Mapping Rule（IP）画面

以下の項目を使用して設定します。

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。1 から 10000 の間で指定可能です。
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。0-63 の範囲で指定できます。
Source / Destination Port	送信元 / 宛先 TCP/UDP ポート（1 - 65535）を指定します。
IP Protocol	L3 IP プロトコル値（0-255）を指定します。
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。 • 「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。 • 「Dot1q-tunnel」- マッチ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（1-4094）を指定します。
802.1P Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID（1-4094）を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。

「Back」をクリックすると前のページに戻ります。
「Apply」をクリックし、設定内容を適用します。

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。

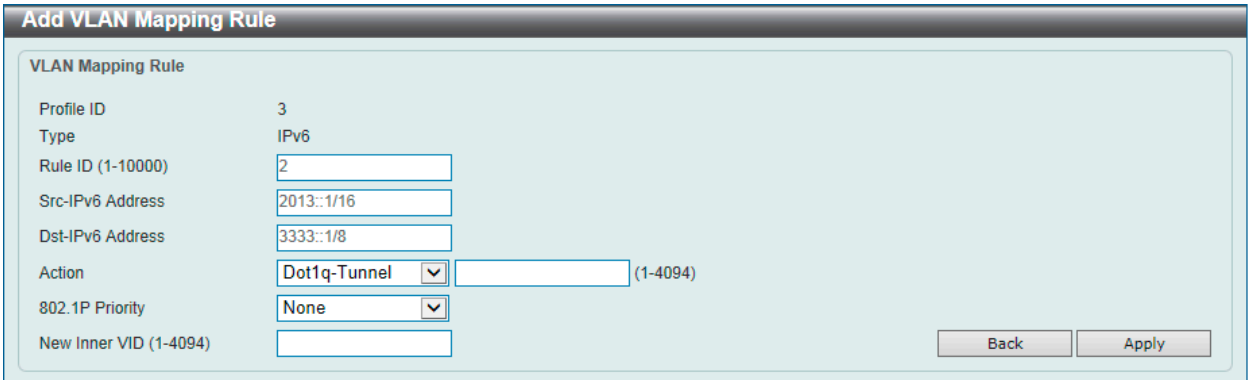


図 8-48　Add VLAN Mapping Rule（IPv6）画面

以下の項目を使用して設定します。

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。1 から 10000 の間で指定可能です。
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」「Dot1q-tunnel」から指定します。 • 「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。 • 「Dot1q-tunnel」- マッチ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（1-4094）を指定します。
802.1P Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID（1-4094）を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。

「Back」をクリックすると前のページに戻ります。
「Apply」をクリックし、設定内容を適用します。

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。

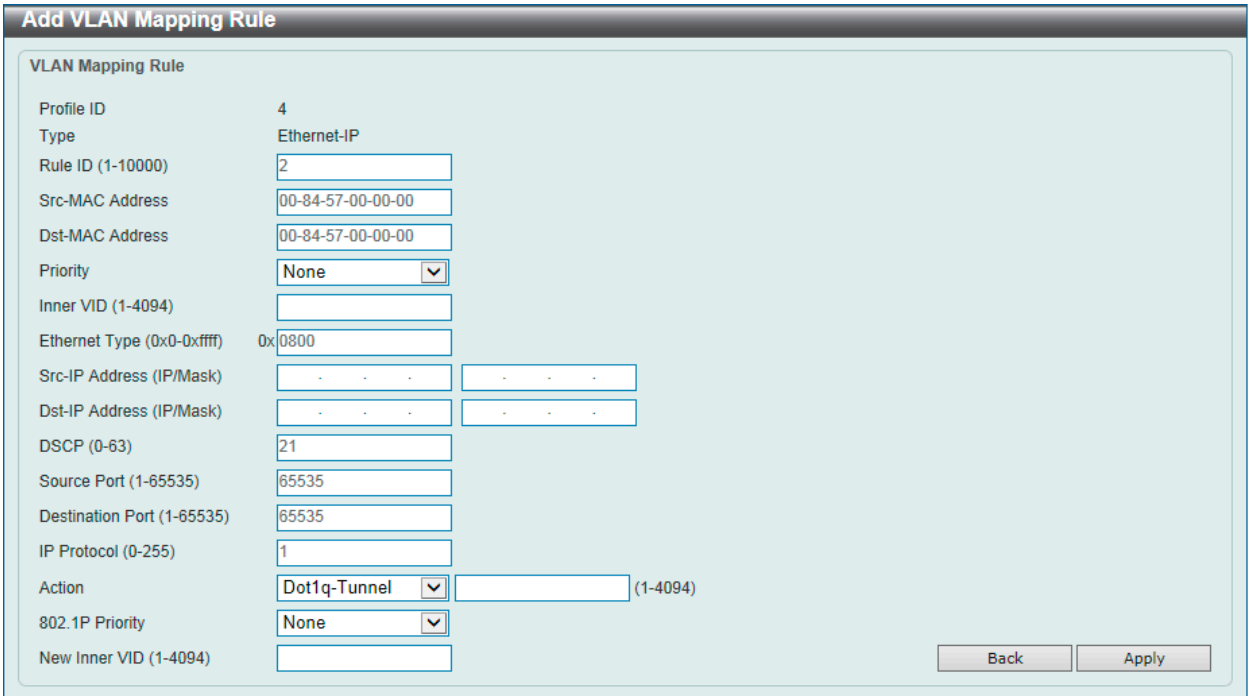


図 8-49　Add VLAN Mapping Rule（Ethernet-IP）画面

以下の項目を使用して設定します。

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。1 から 10000 の間で指定可能です。
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。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
Inner VID	インナー VLAN ID（1-4094）を指定します。
Ethernet Type	イーサネットタイプを指定します。「0x0」から「0xFFFF」の間で指定可能です。
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。0-63 の範囲で指定できます。
Source / Destination Port	送信元 / 宛先 TCP/UDP ポート（1 - 65535）を指定します。
IP Protocol	L3 IP プロトコル値（0-255）を指定します。
Action	実行する動作を指定します。「Translate」「Dot1q-tunnel」から指定します。 • 「Translate」- マッチしたパケットの出力 VID と交換する VID を指定します。 • 「Dot1q-tunnel」- マッチ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（1-4094）を指定します。
802.1P Priority	802.1p 優先値を指定します。0-7 の範囲で指定できます。値が高い方が優先度が高くなります。
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID（1-4094）を指定します。「Dot1q-tunnel」を選択時のみ指定可能です。

「Back」をクリックすると前のページに戻ります。
「Apply」をクリックし、設定内容を適用します。

STP（スパニングツリー設定）

L2 Features > STP

本スイッチは 3 つのバージョンのスパニングツリープロトコル（IEEE 802.1D-1998 STP、IEEE 802.1D-2004 Rapid STP、および IEEE 802.1Q-2005 MSTP）をサポートしています。ネットワーク管理者の間では IEEE 802.1D-1998 STP が最も一般的なプロトコルとして認識されていますが、D-Link のマネジメントスイッチには IEEE 802.1D-2004 RSTP と IEEE 802.1Q-2005 MSTP も導入されています。これらの技術について、以下に概要を紹介します。また、802.1D-1998 STP、802.1D-2004 RSTP および 802.1Q-2005 MSTP の設定方法についても説明します。

802.1Q-2005 MSTP

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

VLAN が指定されたフレームは、これらの 3 つのスパニングツリープロトコル（STP、RSTP、MSTP）のいずれかを使用し、相互接続されたブリッジを介して素早く適切に処理されます。

MSTI ID（MST インスタンス ID）は、これらのインスタンスをクラス分けする ID です。MSTP では、複数のスパニングツリーを CIST（Common and Internal STP）で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を判定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジのように見せかけます。そのため、VLAN が割り当てられた各フレームは、定義 VLAN の誤りや対応するスパニングツリーに関係なくシンプルで完全なフレーム処理が保持されたまま、ネットワーク上で管理用に設定されたリージョン内において異なるデータ経路を通ることができます。

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

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

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

1. スイッチに MSTP 設定を行います。（「STP Bridge Global Settings」画面の「STP Version」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。（「STP Instance Settings」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
Learning	Learning	Learning	不可能	可能
Forwarding	Forwarding	Forwarding	可能	可能

RSTP では、タイマ設定への依存がなくなり、Forwarding 状態への高速な遷移が可能になりました。RSTP 準拠のブリッジは、他の RSTP に準拠するブリッジリンクのフィードバックを素早く検知します。ポートはトポロジの安定を待たずに Forwarding 状態へ遷移することができます。こうした高速な状態遷移を実現するために、RSTP プロトコルでは以下の 2 つの新しい変数（Edge Port と P2P Port）が使用されています。

Edge Port

エッジポートは、ループが発生しないセグメントに直接接続しているポートに対して設定することができます。例えば、1 台のワークステーションに接続しているポートがこれに該当します。エッジポートとして指定されたポートは、Listening 及び Learning の段階を経ずに、直接 Forwarding 状態に遷移します。エッジポートは BPDU パケットを受け取った時点でそのステータスを失い、通常のスパニングツリーポートに変わります。

P2P Port

P2P ポートにおいても高速な状態遷移が可能です。P2P ポートは他のブリッジとの接続に使用されます。RSTP と MSTP では、手動で設定の変更が行われていない限り、全二重モードで動作しているすべてのポートは P2P ポートと見なされます。

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

RSTP や MSTP はレガシー機器と相互運用が可能で、必要に応じて BPDU パケットを 802.1D-1998 形式に自動的に変換することができます。ただし、802.1D-1998 STP を使用しているセグメントでは、MSTP や RSTP の利点である高速な状態遷移やトポロジ変更の検出を享受することはできません。また、これらのプロトコルでは、セグメント上でレガシー機器の更新により RSTP や MSTP を使用する場合に必要となる変数が用意されており、マイグレーションの際に使用されます。

2 つのレベルで動作するスパニングツリープロトコル

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

STP Global Settings（STP グローバル設定）

STP をグローバルに設定します。

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

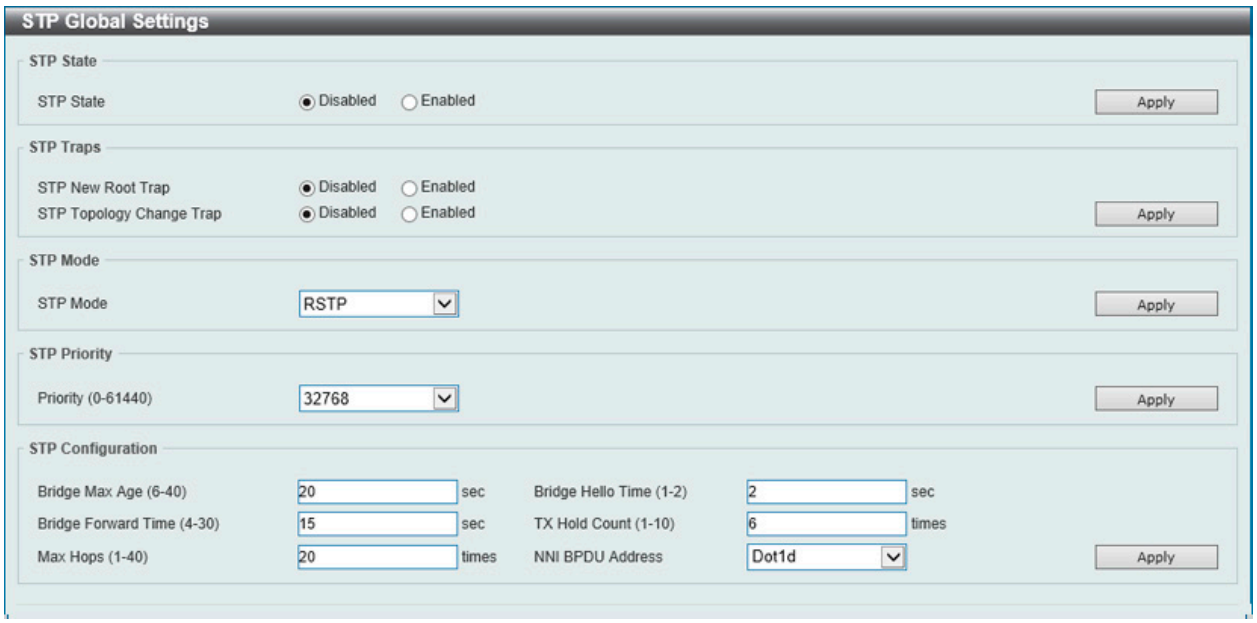


図 8-50　STP Global Settings 画面

設定には以下の項目が使用されます。

項目	説明
STP State	
STP State	STP をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
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。
STP Mode	
STP Mode	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。 • MSTP - スイッチ上で MSTP がグローバルに使用されます。
STP Priority	
Priority	STP 優先値を指定します。0 から 61440 までで指定可能です。初期値は 32768 です。低い方が優先値は高いです。
STP Configuration	
Bridge Max Age (6-40)	本項目は、古い情報がネットワーク内の冗長パスをずっと循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40（秒）の範囲から値を指定します。初期値では 20（秒）が指定されています。
Bridge Hello Time (1-2)	ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために BPDU パケットを 2 回送信します。本値は、1 回目の送信と 2 回目の送信との間の時間です。STP または RSTP が「STP Version」で選択された場合だけ本項目は表示されます。MSTP に対して、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。1-2 秒で指定します。初期値は 2（秒）です。

項目	説明
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 状態に移行する間に本値で指定した時間 Listening 状態を保ちます。4-30（秒）の範囲から指定します。初期値は 15（秒）です。
Tx Hold Count (1-10)	Hello パケットの最大送信回数を指定します。1-10 の範囲から指定します。初期値は 6 です。
Max Hops (1-40)	スイッチが送信した BPDU パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BPDU パケットを破棄し、ポートに保持していた情報を解放します。ホップカウントは 1-40 で指定します。初期値は 20 です。
NNI BPDU Address	NNI BPDU アドレスを指定します。「Dot1d」「Dot1ad」から指定可能です。初期値では「Dot1d」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。

「Apply」ボタンをクリックし、設定を適用します。

STP Port Settings（STP ポートの設定）

STP をポートごとに設定します。

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

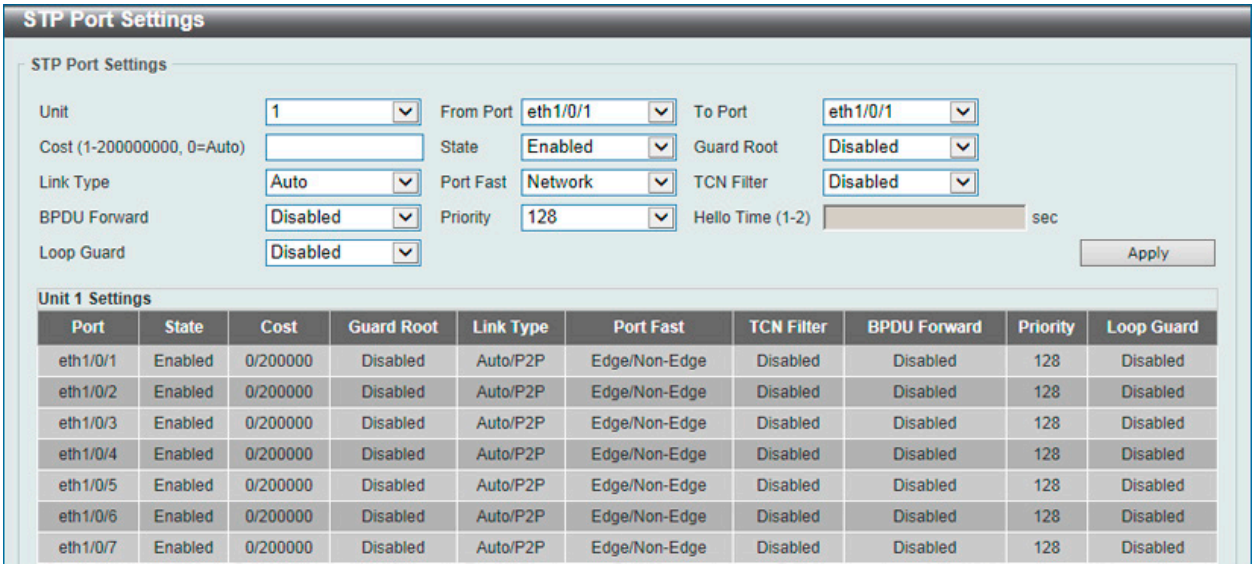


図 8-51　STP Port Settings 画面

参照 STP グループと VLAN グループを関連付けて定義することをお勧めします。

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port	連続するポートグループの最初の番号を設定します。
To Port	連続するポートグループの最後の番号を設定します。
Cost (1-200000000, 0=Auto)	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。初期値は 0（Auto）です。 • 0（Auto）- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。 ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。 • 値 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほどパケット転送は頻繁に行われるようになります。
State	ポートグループでの STP の「Enabled」（有効）/「Disabled」（無効）を設定します。初期値は「Enabled」です。
Guard Root	Guard Root の「Enabled」（有効）/「Disabled」（無効）を設定します。
Link Type	リンクの種類を設定します。初期値は「Auto」です。 • P2P - P2P ポートとしてリンクを共有します。P2P ポートは全二重でなくてはならないという制限があります。 • Shared - 半二重ポートとして認識されます。 • Auto - 可能であれば常に P2P となるように設定します。ポートが、例えば強制的に半二重になるなど状態を維持できない場合には、Shared と同様の状態になります。

項目	説明
Port Fast	ポートファストオプションを指定します。 「Network」「Disabled」「Edge」から選択します。「Network」モデム内だとポートは3秒だけ非ポートファスト状態に残ります。ポートは BPDU が受信されず、転送状態に変更されるとポートファスト状態に変更します。のちに BPDU を受信すると非ポートファストへ戻ります。「Disable」モードではポートは常に非ポートファスト状態です。常に転送状態への変化のために「forward-time delay」を待ちます。「Edge」モードではポートは「forward-time delay」を待たずに直接 STP 転送状態に変化します。インタフェースが「BPDU」を受信すると非ポートファストへ移行します。初期値では「Network」になります。
TCN Filter	TCN（Topology Change Notification）フィルタを有効 / 無効に設定します。 ポートの TCN フィルタリングを有効にすると、域内のアドレスフラッシングを発生させるネットワークのコア域への外部ブリッジを ISP により防ぐために有効です。 こういったブリッジは管理者のコントロール下で構築されることはないためです。ポートが TCN フィルタモードに設定されると、ポートは無視されることにより TC イベントは受信されます。初期値は無効です。
BPDU Forward	BPDU パケットの転送を「Enabled」（有効）または「Disabled」（無効）にします。 有効にすると受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。初期値は無効です。
Priority	優先値を指定します。0 から 240 で指定可能です。初期値は 128 です。少ない方が優先値は高くなります。
Hello Time	ハロータイムの値を指定します。1 から 2（秒）の間で指定可能です。 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。
Loop Guard	指定ポートでのループガードを有効 / 無効に指定します。STP ループガードは 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 ループはリダンダントトポロジ内の STP ブロックポートが、フォワーディングステートへ移行する際に発生するエラーにより生成されます。これは通常、物理リダンダントトポロジのポートの一つ（STP ブロックポートである必要なし）が、STP BPDU を受信しなくなることにより発生します。これにより、STP は継続した BPDU の受信や送信をポートにあてがわれた役割に依存することになります。宛先ポートは BPDU を送信し、非宛先ポートは BPDU を受信することになります。 物理リダンダントトポロジのポートの一つが BPDU を受信しなくなると、STP がトポロジをループ解除状態と認識します。最終的にブロック / バックアップだった幾つかのポートが宛先、そしてフォワーディングステートになり、ループを生成します。

「Apply」ボタンをクリックし、設定を有効にします。

注意 BPDU の送出をポートベースで有効とする場合は、はじめに以下の設定を行ってください。

1. STP をグローバルに無効とする。
2. BPDU の送出をグローバルに有効とする。

これらの設定は、前述の「STP Bridge Global Settings」メニューで行います。

MST Configuration Identification（MST の設定）

スイッチ上で MST インスタンスの設定を行います。本設定は MSTI（マルチプルスパニングツリーインスタンス）を識別するためのものです。スイッチは初期状態で 1 つの CIST（Common Internal STP）を持ちます。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。

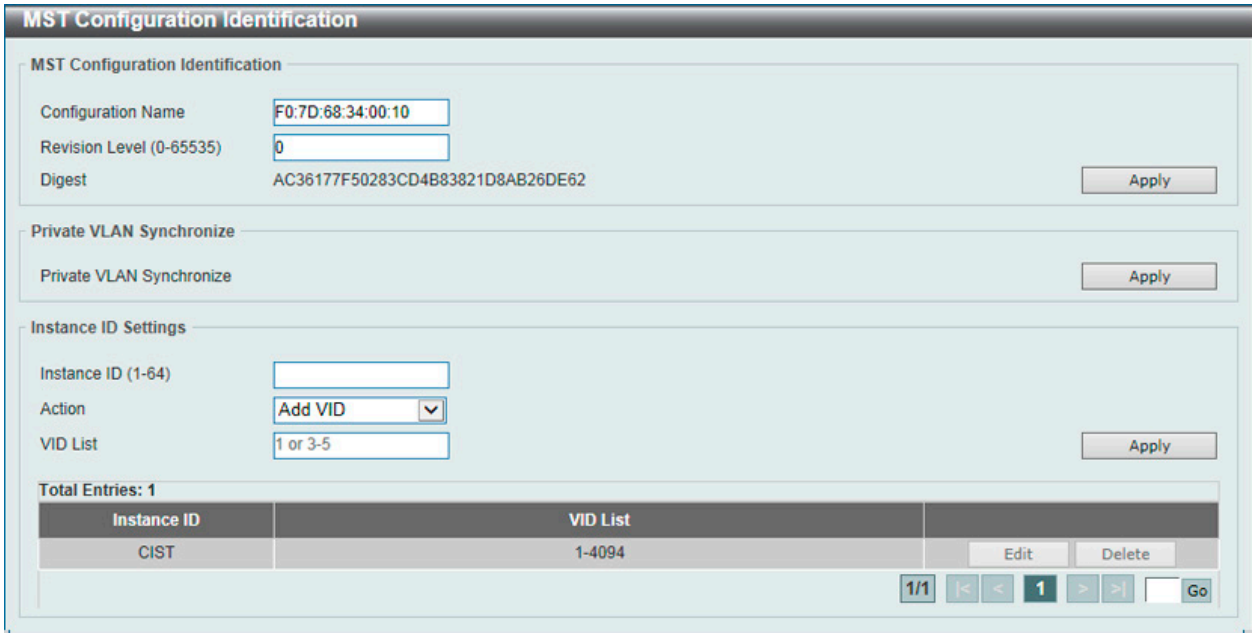


図 8-52　MST Configuration Identification 画面

上記画面には以下の項目が含まれます。

項目	説明
Configuration Name	各 MSTI（Multiple Spanning Tree Instance）を識別するためにスイッチに名前を設定します。 名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level (0-65535)	スイッチ上に設定された MST リージョンの値を設定します。Configuration Name に同期しています。初期値は 0 です。
Instance ID	1-46 の番号を入力し、スイッチに Instance ID を設定します。
Action	MSTI に行う変更を選択します。 • Add VID - VID List 項目に指定された VID を MSTI ID に追加します。 • Remove VID - VID List 項目に指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

STP Instance（STP インタンス設定）

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。

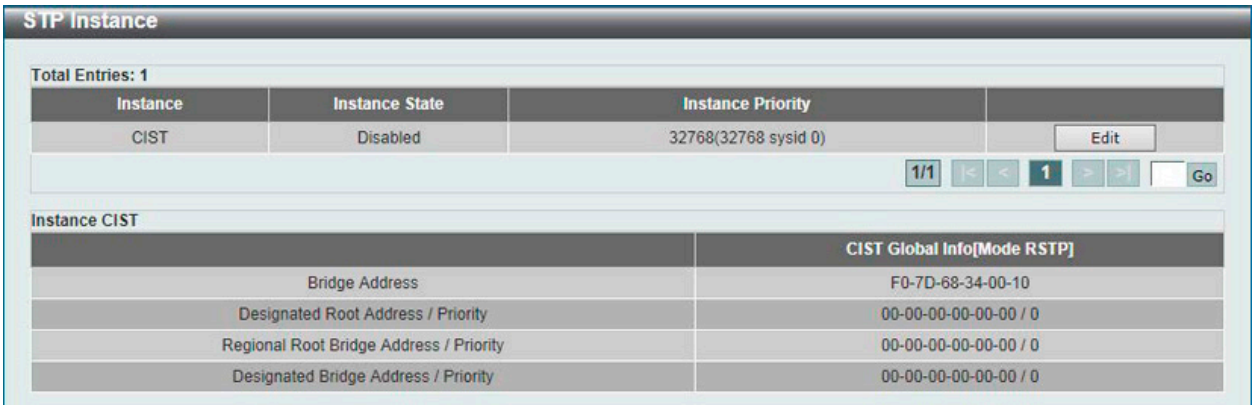


図 8-53　STP Instance 画面

本画面には以下の情報があります。

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

「Apply」をクリックし、設定内容を適用します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

MSTP Port Information（MSTP ポート情報）

本画面では現在の MSTP ポート情報が表示され、MSTI ID 単位でポート構成の更新を行います。ループが発生した場合に MSTP 機能はポートプライオリティを使用して、Forwarding 状態に遷移させるインタフェースを選択します。最初に選択したいインタフェースには高いプライオリティ（小さい数値）を与え、最後に選択したいインタフェースには低いプライオリティ（大きい数値）を与えます。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。低いプライオリティ値ほど転送パケットに対して高いプライオリティを意味することにご注意ください。

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

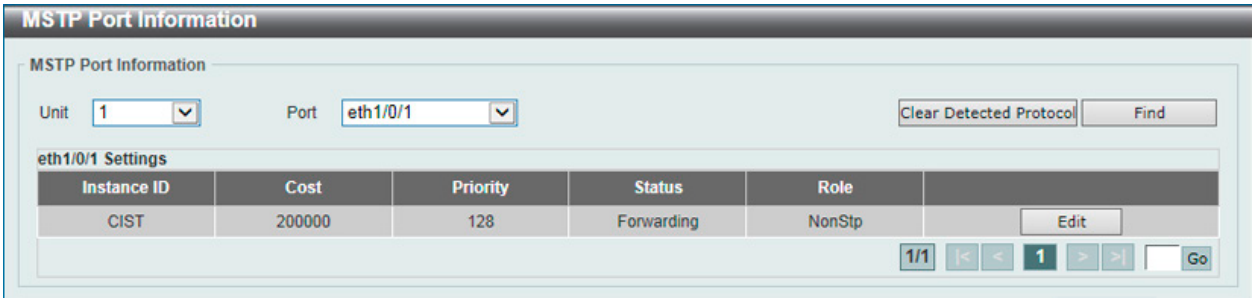


図 8-54　MSTP Port Information 画面

以下の項目を設定または参照できます。

項目	説明
Unit	設定を行うユニットを指定します。
Port	適用するポートを選択します。
Internal Path Cost (1-200000000)	インタフェースを STP インスタンスで選択する場合、指定ポートにパケットを転送する相対的なコストを設定します。「Edit」をクリックして、指定インスタンスの編集を行います。 • 0（Auto）- インタフェースに自動的で最適な最速のルートを設定します。（初期値） • 値 1-200000000 - ループが発生した場合、この範囲で指定した値を使用した最短のルートを設定します。コストが小さいほど高速で伝送されます。
Priority	ポートインタフェースのプライオリティ（0-240）までの値を指定します。高いプライオリティほど、パケットの転送は優先されます。値が低いほどプライオリティは高くなります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear Detected Protocol」ボタンをクリックし、選択したポートの検出したプロトコル設定をクリアします。
特定ポートの MSTP 設定を参照するためには、プルダウンメニューでポート番号を選択し、「Find」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

ERPS (G.8032)（イーサネットリングプロテクション設定）

ERPS (Ethernet Ring Protection Switching) はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。これは、イーサネットリングネットワークに対して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（RPL : Ring Protection Link）を回避するためにブロックされます。障害が発生すると、保護スイッチングは障害のあるリンクをブロックして RPL のブロックを解除します。障害が解決すると、保護スイッチングは再度 RPL をブロックして、障害が解決したリンクのブロックを解除します。

ERPS

本項目では「Ethernet Ring Protection Switching」(ERPS) の表示、設定を行います。STP とループバック検知 (LBD) は ERPS の有効化の前にリングポートで無効になる必要があります。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。

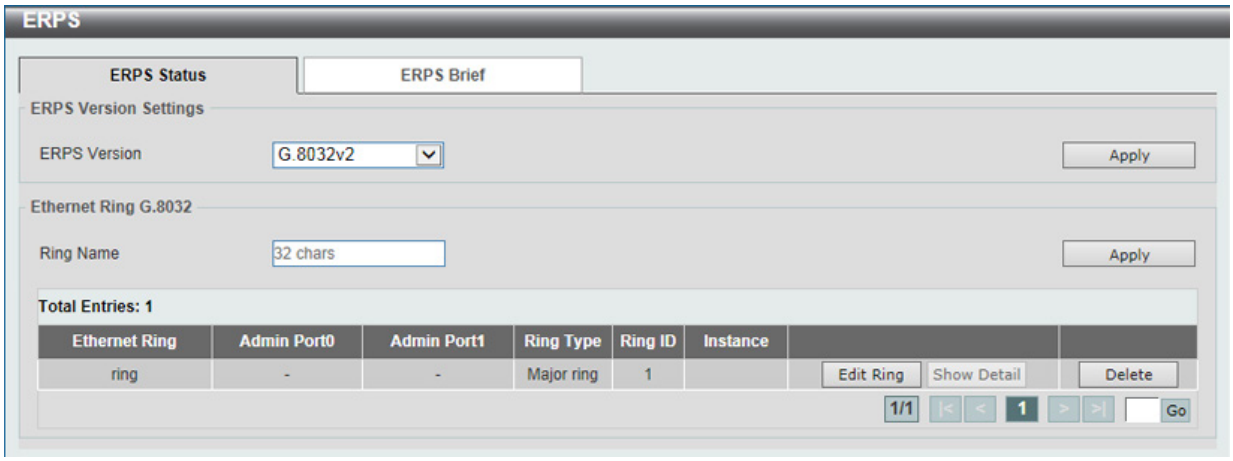


図 8-55　ERPS 画面

上記画面には以下の項目が含まれます。

項目	説明
ERPS Version Settings	
ERPS Version	ERPS バージョンを選択します。「G.8032v1」「G.8032v2」から選択可能です。 「G.8032v2」では以下の事が可能です。: • 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。 • 物理リングのリング ID を持つ「R-APS PDU 宛先アドレス」の送信設定 「G.8032v2」が実行中の機器に対し「G.8032v1」を設定する前に、「G.8032v1」がサポートしない全ての ERPS 設定を削除する必要があります。でないとバージョンの変更は行えません。ERPS バージョンの変更は実行中のプロトコルの再起動を促します。 「G.8032v2」から「G.8032v1」へ変更する前に、次の設定であることをチェックする必要があります。: • 手動（Manual）または強制（force）スイッチコマンドの消去 • 内部接続のメジャーリングインスタンスとサブリングインスタンス機器が違う「R-APS VLAN ID」を保持している。 • 物理リング内で一つのみのインスタンスがサポートされている。 イーサネットリング機器がイーサネットリングで「ITU-T G.8032v1」と「ITU-T G.8032v2」を同時に存在させている場合、「G.8032v2」機器におい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。 • 内部接続のメジャーリングインスタンスとサブリングインスタンス機器が、それぞれ違う「R-APS VLAN ID」の保持 • 手動（Manual）または強制（force）スイッチコマンドの消去 • 物理リング内で一つのみのインスタンスをサポート
Ethernet Ring G.8032	
Ring Name	ERP インスタンス名を入力します。（最大 32 文字）

「Apply」をクリックして「ITU-T G.8032 ERP リング」を作成します。
「Edit Ring」をクリックして ERP リングを編集します。
「Show Detail」をクリックして「ITU-T G.8032 ERP リング」の情報について表示します。
「Delete」をクリックして指定の「ITU-T G.8032 ERP リング」を削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Ring の編集

1. 「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。

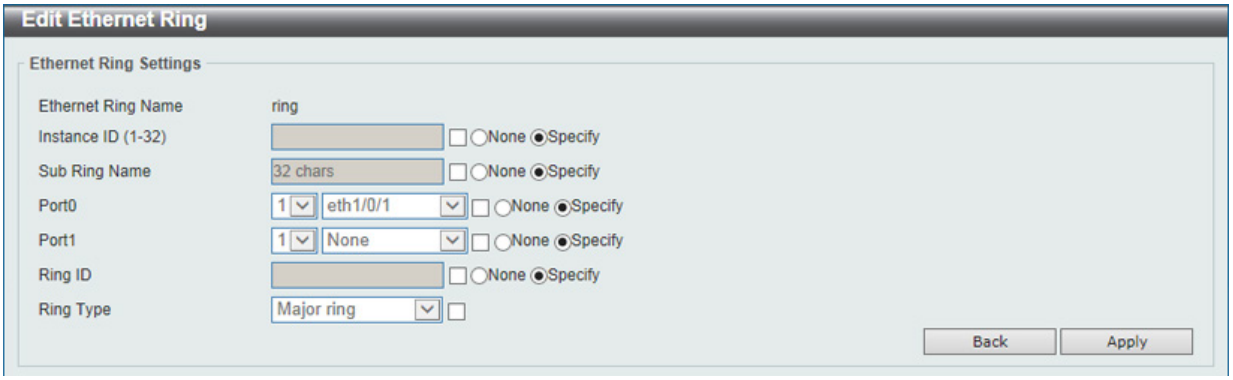


図 8-56　ERPS 画面 - Edit

設定対象となる項目は以下の通りです。

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

項目	説明
Ring ID	チェックを入れリング ID を指定します。1-239 まで指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Ring Type	チェックを入れリングタイプを指定します。「Major Ring」「Sub Ring」から指定します。

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

Ring の編集

1. 「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。

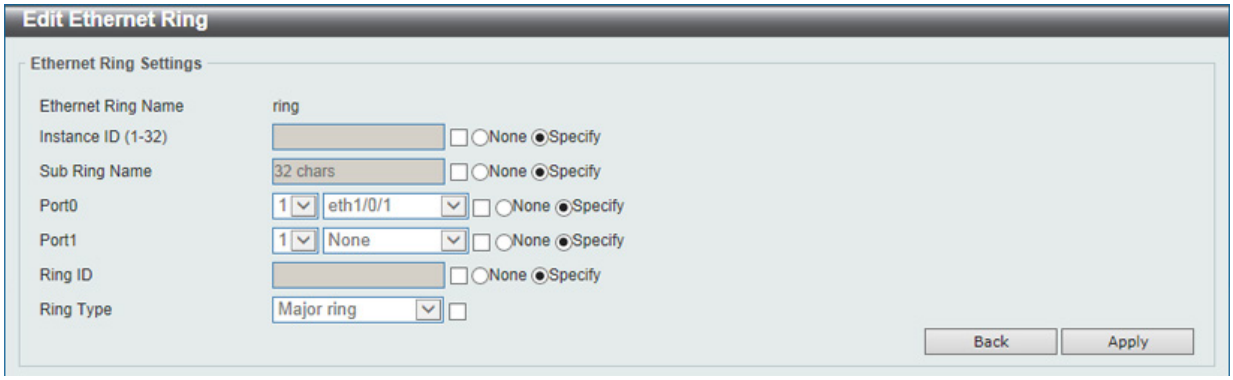


図 8-57　ERPS 画面 - Edit

設定対象となる項目は以下の通りです。

項目	説明
Instance ID	チェックを入れ「ERP インスタンス」の番号を指定します。32 まで指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Sub Ring Name	チェックを入れ「サブリング名」を指定します。32 文字まで指定可能です。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Port0	チェックを入れユニット ID と初期リングになるポート番号を指定します。ドロップダウンメニューから「None」を選択すると内部接続されたノードはオープンリングのエンドポイントのローカルノードとして指定されます。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Port1	チェックを入れユニット ID と 2 番目のリングになるポート番号を指定します。ドロップダウンメニューから「None」を選択すると内部接続されたノードはオープンリングのエンドポイントのローカルノードとして指定されます。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Ring ID	チェックを入れリング ID を指定します。1-239 まで指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Ring Type	チェックを入れリングタイプを指定します。「Major Ring」「Sub Ring」から指定します。

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

「ERPS Brief」タブの表示

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

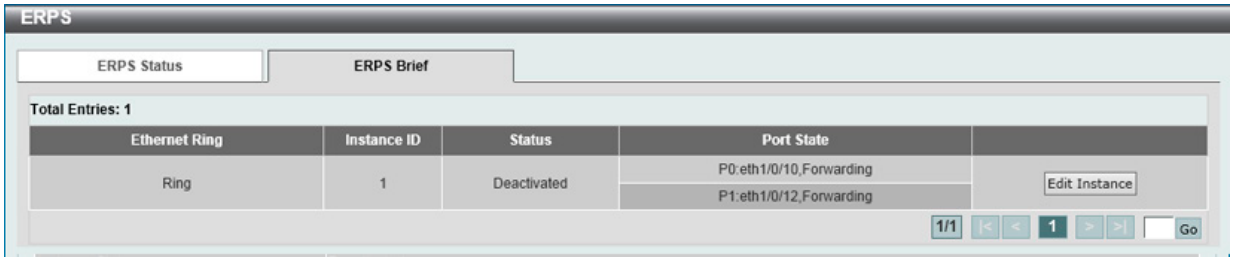


図 8-58　ERPS（ERPS Brief タブ）画面

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

Instance の編集（Edit Instance）

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

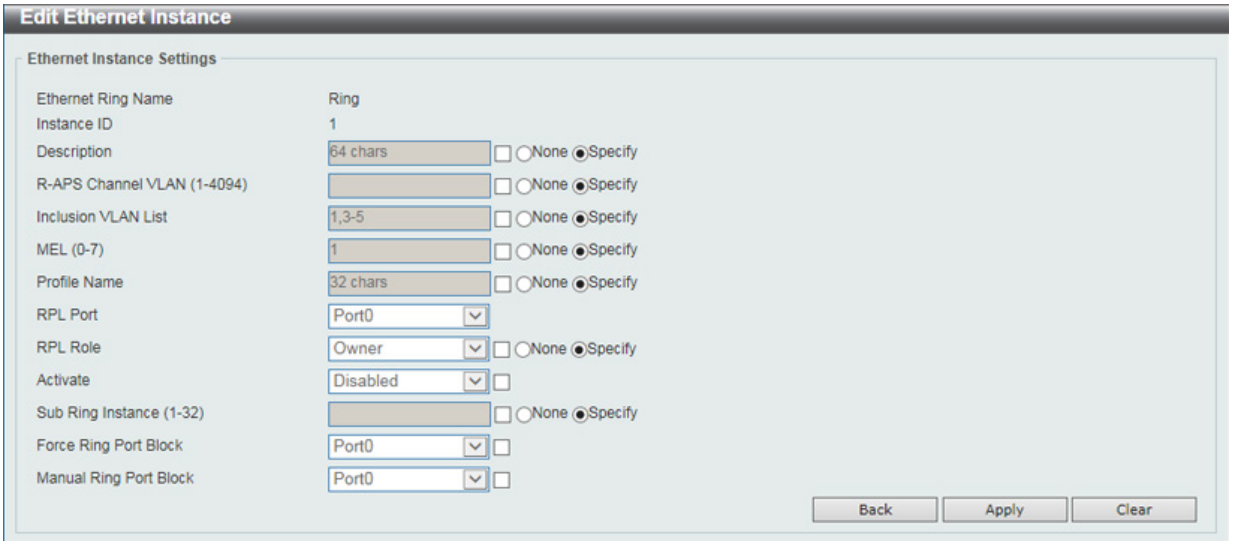


図 8-59　ERPS 画面 - Instance

設定対象となる項目は以下の通りです。

項目	説明
Description	チェックを入れ「ERP インスタンス」の概要を指定します。64 文字まで指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
R-APS Channel VLAN	チェックを入れ「ERP インスタンス」の「R-APS Channel VLAN ID」を指定します。サブインスタンスの「APS channel VLAN」はサブリングの過疎チャネルでもあります。1 から 4094 までの間で指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Inclusion VLAN List	チェックを入れインスタンスに含まれる VLAN リストを指定します。 「-」を使用すると範囲として指定され、「,」を使用すると個別に複数の VLAN を指定します（例;「VLAN1 から 5」は「1-5」、「VLAN1 と 3 と 5」は「1,3,5」）。指定された VLAN は ERP のメカニズムで保護されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
MEL	チェックを入れ ERP インスタンスの「MEL」を指定します。0 から 7 までの間で指定可能です。 同じ ERP インスタンスの全てのリングノードの MEL 値は同一です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Profile Name	チェックを入れ ERP インスタンスに関連する「G.8032」のプロファイルを指定します。複数の ERP インスタンスが同じ G.8032 プロファイルに含まれることも可能です。同じプロファイルに含まれるインスタンスは同じセットの VLAN や一つのインスタンスに保護される VLAN、他のインスタンスに保護される LAN のサブセットを保護します。32 文字まで指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
RPL Port	チェックを入れ RPL ポートオプションを選択します。オプションは「Port0」「Port1」から指定します。 選択されたオプションは RPL ポートとして設定されます。
RPL Role	チェックを入れノードが RPL オーナかネイバかを選択します。「Enable/Disable」から選択し、「Enable」の場合、RPL は「オーナ」として設定されます。
Activate	チェックを入れ ERP インスタンスをアクティブにするか選択します。「Enable/Disable」から選択し、「Enable」の場合、ERP インスタンスはアクティブになります。
Sub Ring Instance	チェックを入れ ERP インスタンスに関連する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に使用されます。1-32 字まで指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
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。リンク不具合などが発生すると、この強制インスタンスポートブロックは、設定後すぐに有効になります。 オプションは「Port0」「Port1」から指定します。
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。MS が設定されており、リンク不具合の発生や FS 状態が空白である場合、この強制インスタンスポートブロックは、設定後すぐに有効になります。 オプションは「Port0」「Port1」から指定します。

「Back」をクリックすると設定は破棄され前画面に戻ります。
「Apply」をクリックして設定を適用します。
「Clear All」をクリックすると入力したエントリを全てクリアします。

ERPS Profile（ERPS プロファイル）

ERPS プロファイル設定を行います。

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

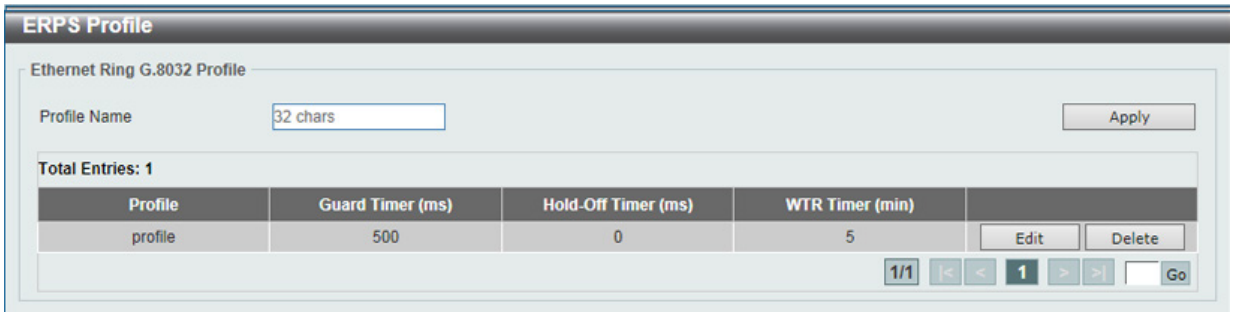


図 8-60　ERPS Profile 画面

設定対象となる項目は以下の通りです。

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

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

「G.8032」プロファイルの編集

1. 「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。

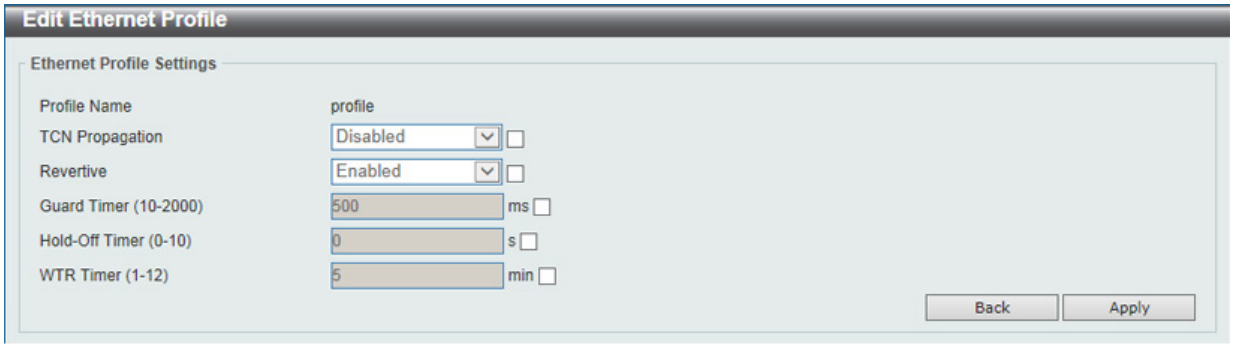


図 8-61　「G.8032」プロファイル画面 - Edit

設定対象となる項目は以下の通りです。

項目	説明
TCN Propagation	チェックを入れ「TCN Propagation」の設定を行います。「Enable/Disable」から選択します。 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。
Revertive	チェックを入れ「Revertive」の設定を行います。「Enable/Disable」から選択します。本機能は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。
Guard Timer	チェックを入れ Guard Timer の設定を行います。10 から 2000（ミリ秒）の間で指定可能です。初期値は 500（ミリ秒）です。
Hold-Off Timer	チェックを入れ Hold-Off Timer の設定を行います。0 から 10（秒）の間で指定可能です。初期値は 0（秒）です。
WTR Timer	チェックを入れ WTR Timer の設定を行います。1 から 12（分）の間で指定可能です。初期値は 5（分）です。

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

Loopback Detection（ループバック検知設定）

ループバック検知（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。

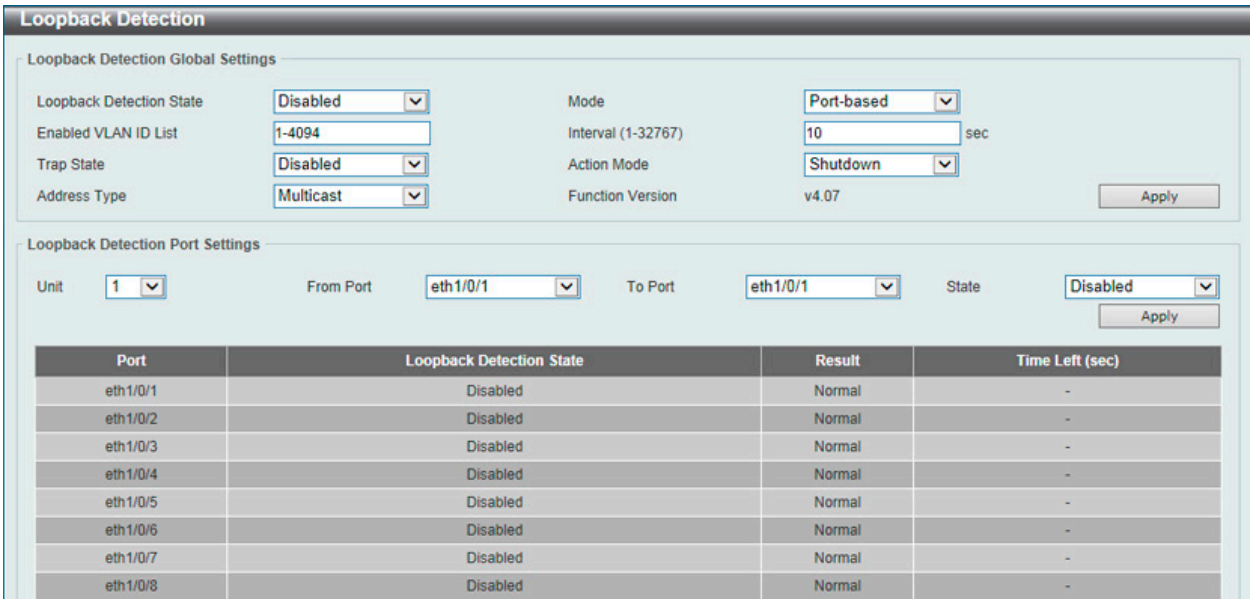


図 8-62　Loopback Detection 画面

本画面には次の項目があります。

項目	説明
Loopback Detection Global Settings	
Loopback Detection State	ループバック検知機能を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Mode	プルダウンメニューで「Port Based」または「VLAN Based」を選択します。
Enable VLAN ID List	「Mode」で「VLAN ID」を選択した場合 VLAN ID のリストを入力します。
Interval (1-32767)	ループ検知間隔を設定します。（1-32767 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「Multicast」「Broadcast」から指定します。
Loopback Detection Port Settings	
Unit	設定するユニットを指定します。
From Port	プルダウンメニューで開始ポートを選択します。
To Port	プルダウンメニューで終了ポートを選択します。
State	「Enabled」（有効）または「Disabled」（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。

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）

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。

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 1 ～ 12 個までの物理ポートを割り当てることができます。

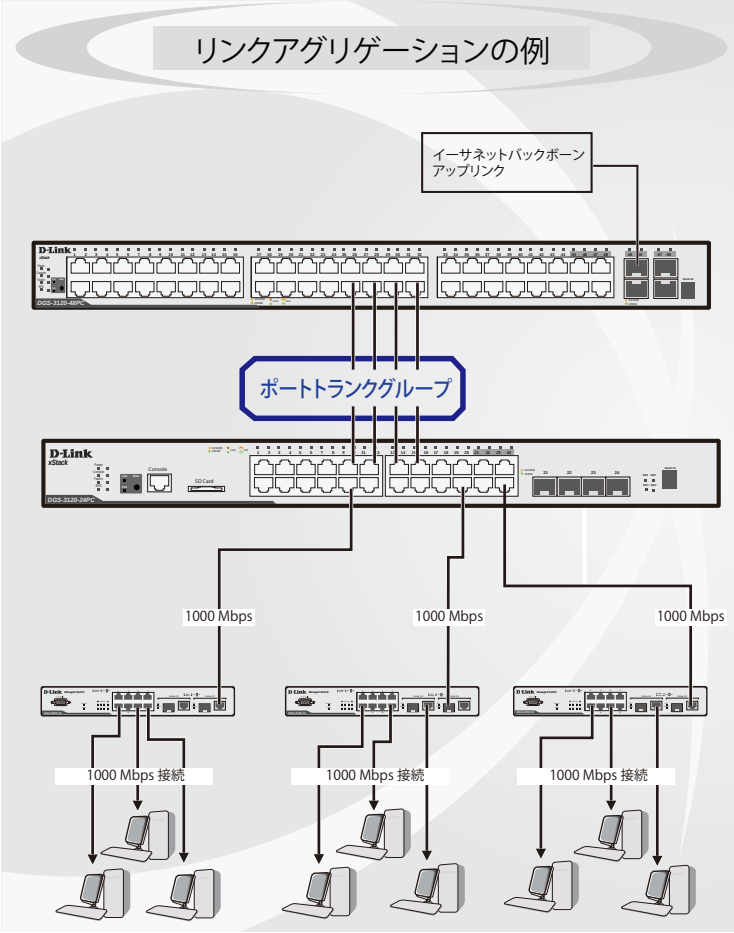


図 8-63　ポートトランクグループの例

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、1 ～ 12 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。

同じグループに含まれるポートはすべて同じ VLAN に属し、スパニングツリープロトコル（STP）ステータス、スタティックマルチキャスト、ストームコントロール、トラフィックセグメンテーション、および 802.1p デフォルトプライオリティの設定についても同じ構成となっている必要があります。また、ポートセキュリティ、ポートミラーリング、および 802.1X は無効にする必要があります。さらに、集約するリンクはすべて同じ速度で、全二重モードで設定されている必要があります。

リンクアグリゲーショングループではマスタポートを 1 つ指定します。マスタポートに設定された、VLAN 設定を含む全ての構成オプションがグループ全体に適用されます。

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 /SFP コンボスロットと 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。

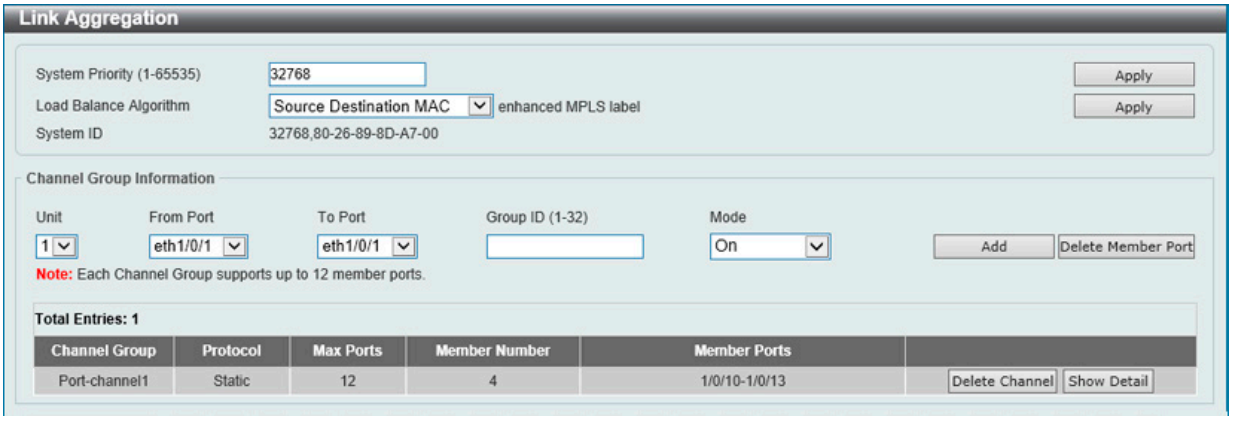


図 8-64　Link Aggregation 画面

本画面には次の項目があります。

項目	説明
System Priority	システム優先値を指定します。1 から 65535 の間で指定できます。初期値は 32768 です。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、そしてポートがスタンドアロンモードに入るかを決定します。低い値の方が高い優先値を示します。二つ以上のポートで同じ優先値を与えられた場合、ポート番号で優先値が決まります。
Load Balance Algorithm	ポートトランクグループを構成するポートのロードバランスに使用するアルゴリズムを選択します。「Source MAC」、「Destination MAC」、「Source Destination MAC」、「Source IP」、「Destination IP」、「Source Destination IP」「Source L4 Port」「Destination L4 Port」「Source Destination L4 Port」から指定してください。 初期値は「Source Destination MAC」です。
Unit	設定するユニットを指定します。
From Port / To Port	設定するポートの範囲を設定します。
Group ID (1-32)	グループの ID 番号（1-32）を設定します。
Mode	モードを指定します。「On」「Active」「Passive」から指定できます。 • On - チャネルグループタイプは固定です。 • Active - Active ポートは LACP 制御フレームの処理と送信を行います。これにより LACP 準拠のデバイス同士はネゴシエーションとリンクの集約を行い、グループは必要に応じて動的に変更されます。グループへのポート追加、または削除などのグループの変更を行うためには、少なくともどちらかのデバイスで LACP ポートを Active に設定する必要があります。また、両方のデバイスは LACP をサポートしている必要があります。 • Passive - Passive ポートは自分から LACP 制御フレームの送信を行いません。リンクするポートグループがネゴシエーションを行い、動的にグループの変更を行うためには、コネクションのどちらか一端が Active な LACP ポートである必要があります。（初期値）

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

ポートトランキンググループの設定

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

注意 レイヤ 3/ レイヤ 4 のアルゴリズムを利用している場合でも、「FDB にエントリがない、またはフラッディング対象」の場合は、MAC アルゴリズムが利用されます。

注意 リンクトラップを有効にした場合、同時にリンクアグリゲーションのリンクトラップも有効になります。

ポートトランクグループの編集

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

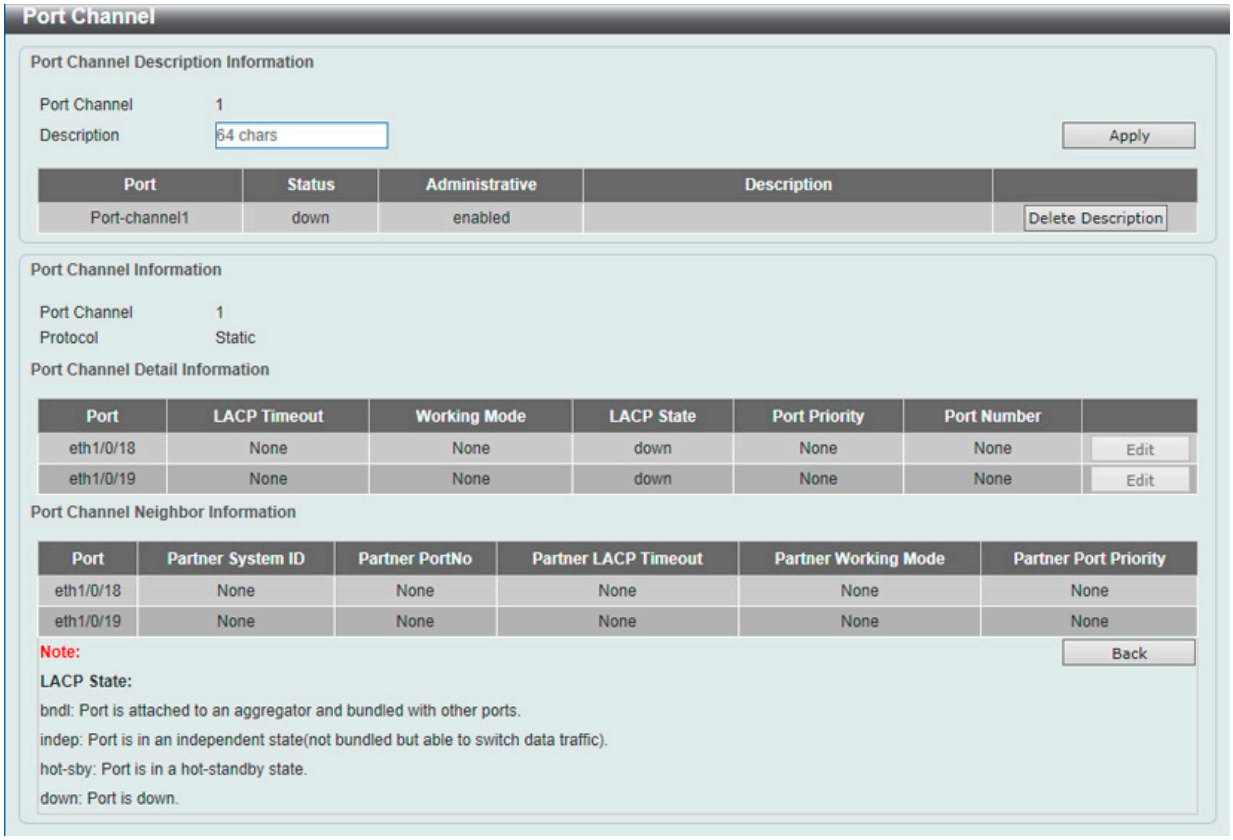


図 8-65　Port Channel 画面

「Description」にポートチャネルの概要を指定します。64 字まで指定可能です。
「Delete Description」でポートチャネルの概要を指定します。
編集するエントリの「Edit」ボタンをクリックします。
「Back」ボタンをクリックし前の画面に戻ります。

MLAG（マルチシャーシリンクアグリゲーション）

MLAG（マルチシャーシリンクアグリゲーション /Multi-Chassis Link Aggregation Group）ではポートブロックや不要なリンクスピードの低下、スイッチ / ケーブル接続の不具合を発生させるイベントなどに対処するため、ネットワークスイッチの帯域の増加を行います。「MLAG ピア」となったスイッチは同じ MLAG ドメインにある他の「MLAG ピア」スイッチと「Peer-Link（ピアリンク）」を通じて接続します。
MLAG ピアスイッチと接続した MLAG パートナースイッチは、ネットワーク内で単一の「MLAG スイッチ」として認識されます。その 2 台の MLAG ピアスイッチは MLAG 機能を除き、それぞれスタンドアロンのスイッチとして別々な操作が可能です。MLAG を使用すると物理的に拡張したトポロジ間でデータトラフィックの送受信が可能になります。
MLAG ピア接続を構築するには同じファームウェアをインストールした同じ機種のスイッチである必要があります。MLAG ピア接続を構築するスイッチは設定後の不安定化を避けるために「Link Aggregation」「MLAG Portchannel」「Interface」「VLAN settings」の項目において、設定内容を全く同じにする必要があります。
MLAG ピアスイッチはスタンドアロンで使用し、物理スタッキングが無効化されている必要があります。

MLAG Settings（MLAG 設定）

MLAG 設定ついて表示します。MLAG の設定は必ずもう一方の MLAG ピアスイッチと接続する前に行います。設定内容はスイッチが再起動した後に有効になります。グループ内の全てのスイッチは必ず同じ MLAG バージョンで動作している必要があります。

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



図 8-66　MLAG Settings (Disabled) 画面

「MLAG State」で MLAG を有効 / 無効（初期値）にします。有効にし、スイッチの再起動を行うと次の画面になり各設定項目が表示されます。

MLAG Settings(有効時)

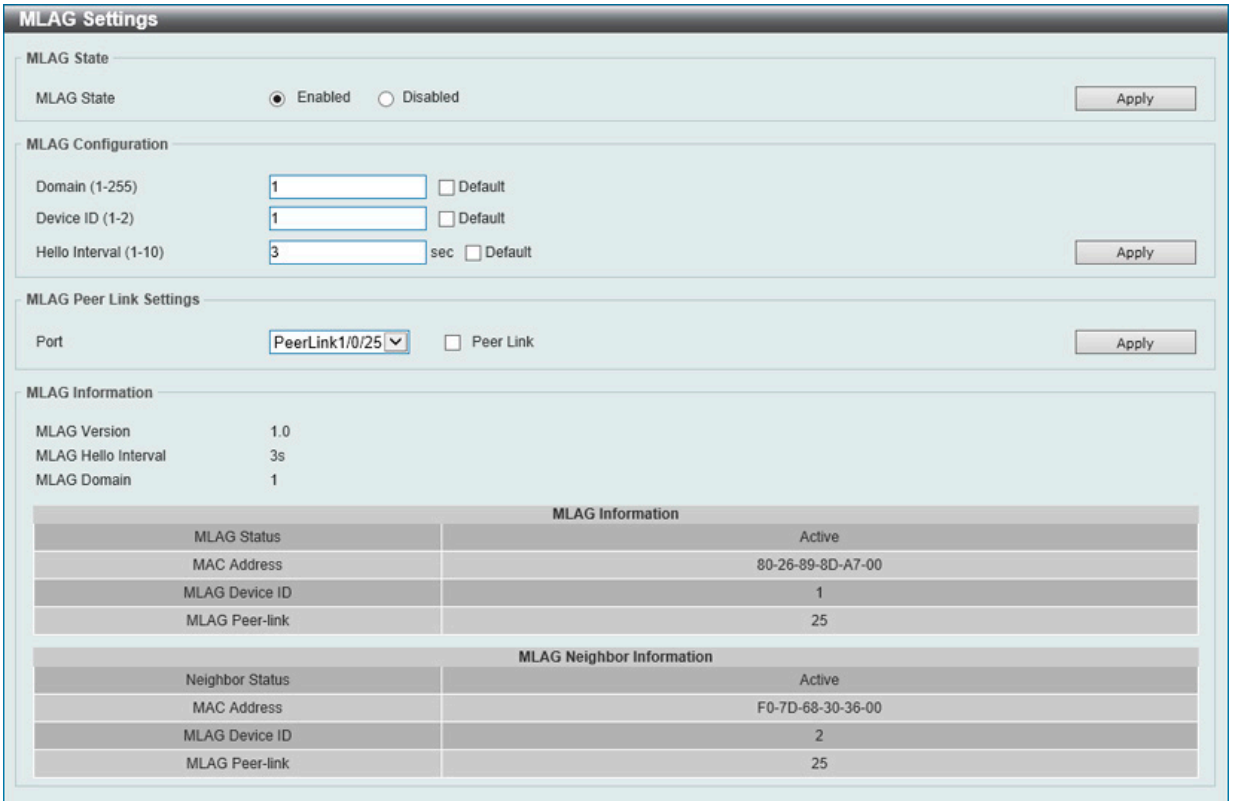


図 8-67　MLAG Settings (Enabled) 画面

本画面には次の項目があります。

項目	説明
MLAG State	MLAG を有効 / 無効（初期値）にします。有効の状態でのみ MLAG の設定が可能です。
Domain	MLAG ドメイン ID（1-255）を指定します。「Default」にチェックを入れると初期値（1）が適用されます。
Device ID	MLAG デバイス ID（1-2）を指定します。「Default」にチェックを入れると初期値（1）が適用されます。
Hello Interval	MLAG ハローインターバル ID（1-10 秒）を指定します。MLAG ハローメッセージの送信間隔（秒）になります。 「Default」にチェックを入れると初期値（3 秒）が適用されます。
Port	Peer-Link（ピアリンク）に使用する物理ポートを指定します。
Peer Link	指定したポートを Peer-Link（ピアリンク）ポートとして指定します。MLAG ピアスイッチとの接続に使用します。

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。

MLAG Group（MLAG グループ）

MLAG グループついて表示します。

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

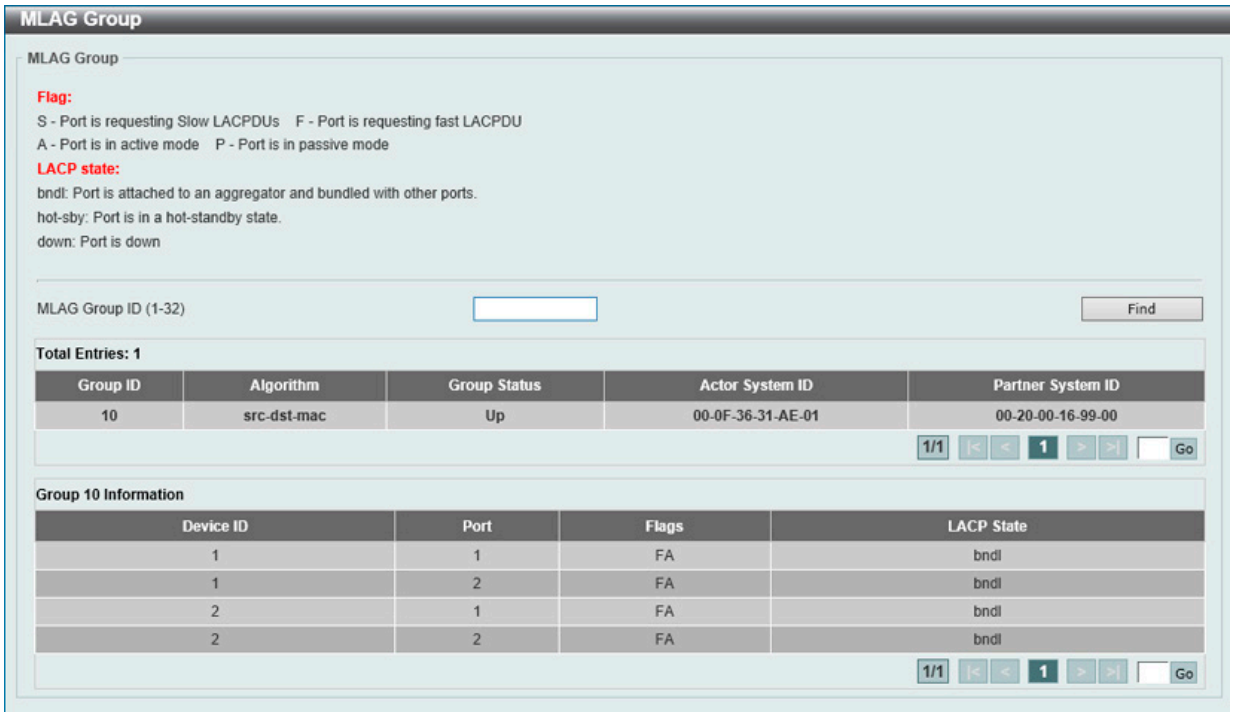


図 8-68　MLAG Group 画面

本画面には次の項目があります。

項目	説明
MLAG Group ID	MLAG Group ID（1-32）を指定します。

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

Flex Links（フレックスリンクス）

本項目ではフレックスリンクス機能の表示、設定について説明します。フレックスリンクスは L2 インタフェースのペアのうち、一つがもう片方のバックアップとして動作する機能です。フレックスリンクスにより、STP や LBD 等のリンクレベルでの冗長性が提供されます。

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

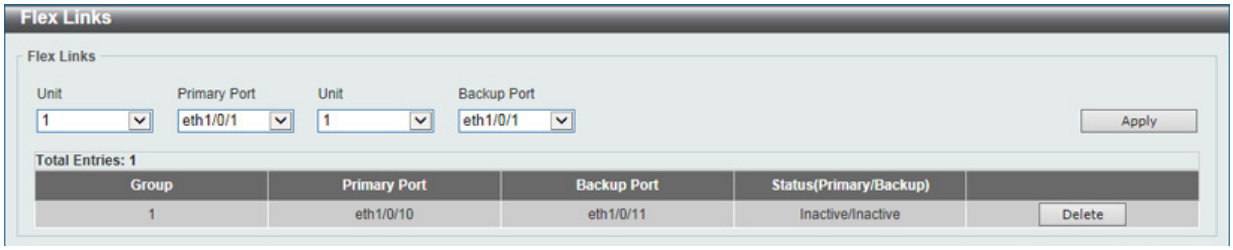


図 8-69　Flex Links 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	プライマリポートの存在するユニットを指定します。
Primary Port	プライマリポートを指定します。
Unit	セカンダリポートの存在するユニットを指定します。
Backup Port	セカンダリポートを指定します。

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

注意　フレックスリンクスは、STP、ERPS、LBD 機能と相互排他になります。

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。

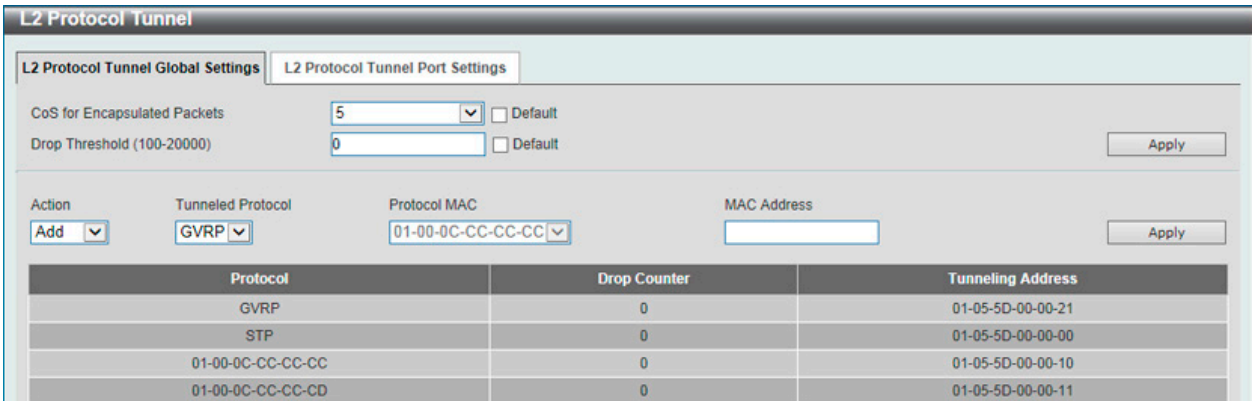


図 8-70　Layer 2 Protocol Tunneling（L2 Protocol Tunnel Global Settings）画面

以下の項目を使用して、設定および表示を行います。

項目	説明
CoS for Encapsulated Packets	カプセル化されたパケットの CoS 値（0-7）を指定します。「Default」を指定すると初期値を指定します。
Drop Threshold	破棄しきい値を指定します。100 - 20000 で指定可能です。初期値は「0」です。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。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。指定のプロトコルへ / からの L2PT トンネリングマルチキャストアドレスを追加 / 削除します。
Tunneled Protocol	トンネルプロトコルを選択します。このプルダウンメニューでは以下のオプションを表示します。 • STP - 設定のアドレスに STP パケットをトンネルします。 • GVRP - 設定のアドレスに GVRP パケットをトンネルします。 • MAC - 指定の宛先アドレス付きのプロトコルパケットを設定のアドレスにトンネルします。 • All - 設定のアドレスに全パケットをトンネルします。
Protocol MAC	トンネルプロトコルに MAC 選択時に 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。現時点では、MAC アドレスは、01-00-0C-CC-CC-CC または 01-00-0C-CC-CC-CD です。
MAC Address	指定のプロトコルをトンネルする MAC アドレスを入力します。この MAC アドレスはリザーブされたものや、他のプロトコルで使用のものは指定できません。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

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

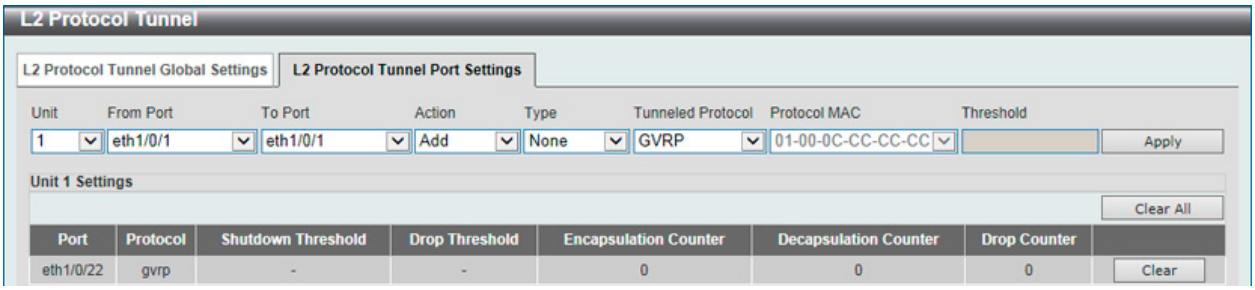


図 8-71　Layer 2 Protocol Tunneling（L2 Protocol Tunnel Port Settings）画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。
Type	ポートタイプを指定します。「None」「Shutdown」および「Drop」が選択可能です。

項目	説明
Tunneled Protocol	トンネルプロトコルを選択します。このプルダウンメニューでは以下のオプションを表示します。 • STP - 設定のアドレスに STP パケットをトンネルします。 • GVRP - 設定のアドレスに GVRP パケットをトンネルします。 • MAC - 指定の宛先アドレス付きのプロトコルパケットを設定のアドレスにトンネルします。 • All - 設定のアドレスに全パケットをトンネルします。
Protocol MAC	トンネルプロトコルに Protocol MAC 選択時に 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。現時点では、MAC アドレスは、01-00-0C-CC-CC-CC または 01-00-0C-CC-CC-CD です。
Threshold	「Type」で「Shutdown」「Drop」を指定した場合、しきい値（1-4096）を入力します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します
「Clear」をクリックすると入力したエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。

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

IGMP（Internet Group Management Protocol）Snooping 機能を始めとした L2 Multicast Contro（I 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もう存在していないと判断すれば、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。

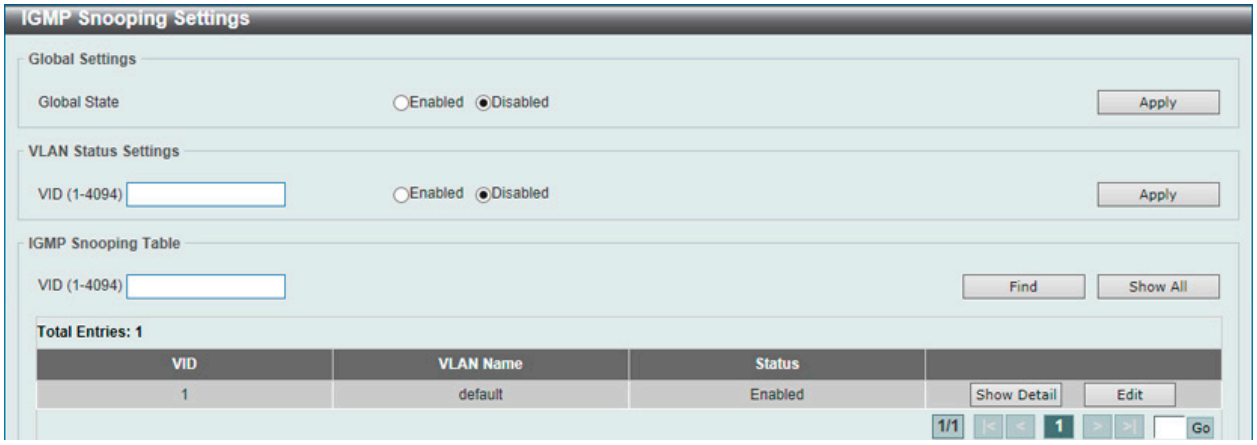


図 8-72　IGMP Snooping Settings 画面

画面には以下の項目があります。

項目	説明
Global Setting	
Global State	IGMP Snooping の有効 / 無効を設定します。 • Enabled - デバイスで IGMP Snooping を有効にします。 • Disabled - デバイスで IGMP Snooping を無効に設定します。（初期値）
VLAN Status Settings	
VID	VLAN 上の IGMP Snooping を有効 / 無効にし、VLAN を識別する VLAN ID を指定します。 • Enabled - VLAN を有効にします。 • Disabled - VLAN を無効に設定します。（初期値）

項目	説明
IGMP Snooping Table	
VID	IGMP Snooping Table 上の VLAN を表示させるための VLAN ID を指定します。 • Find - 指定の VLAN ID を入力して指定のエントリを表示します。 • Show All - IGMP Snooping Table 上のすべてのエントリを表示します。

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

IGMP Snooping VLAN の詳細情報表示

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

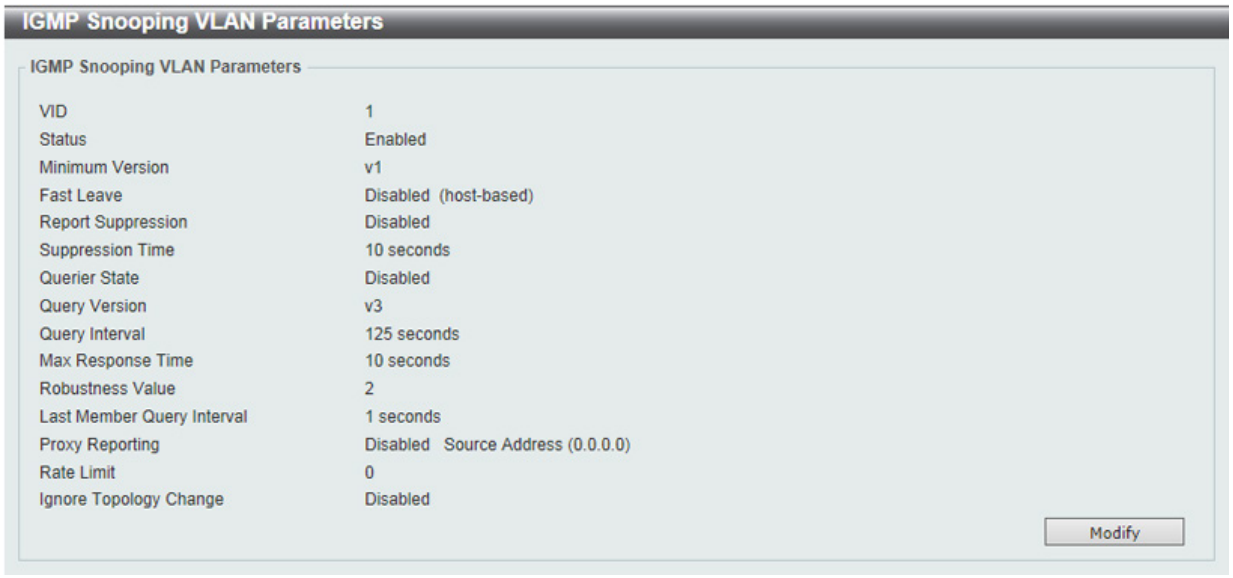


図 8-73　IGMP Snooping VLAN Parameters 画面

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

IGMP Snooping 機能の詳細設定

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

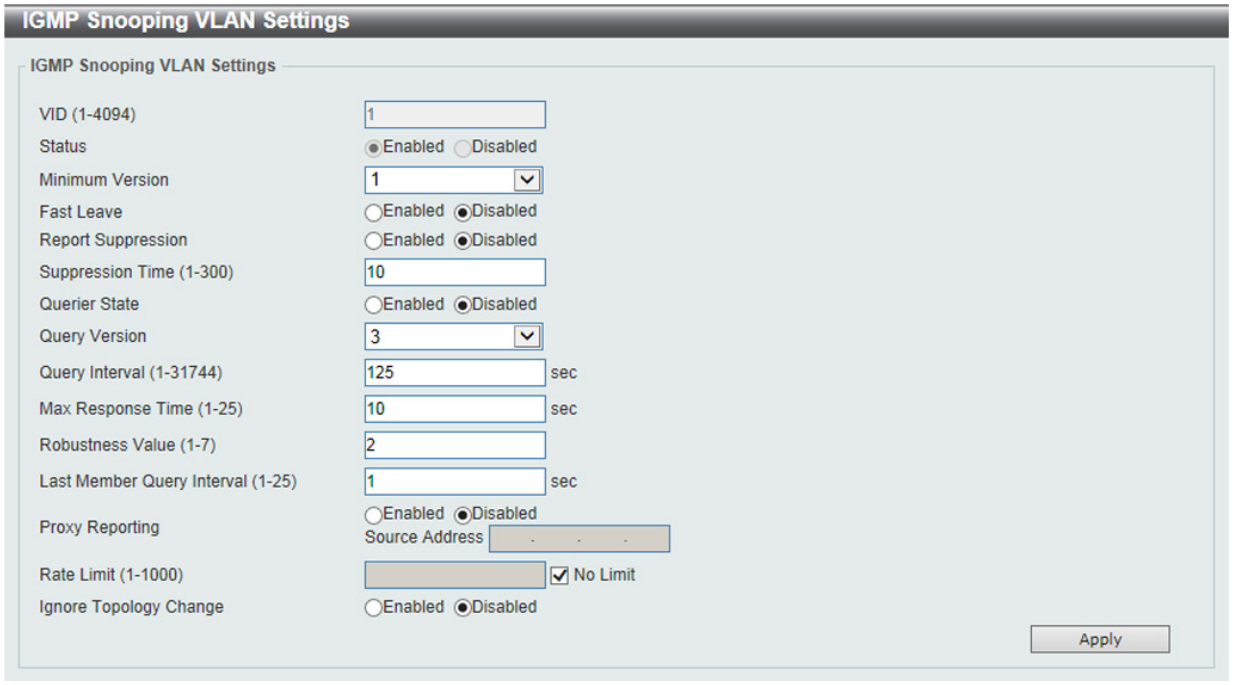


図 8-74 IGMP Snooping VLAN Settings 画面

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	IGMP Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
Status	指定した VLAN への IGMP Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。

項目	説明
Minimum Version	VLAN に許可された IGMP ホストの最小バージョンを選択します。
Fast Leave	「Enabled」（有効）にすると、Fast Leave 機能が有効になります。この機能が有効になると、システムが最新メンバから 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。Fast Leave が有効な場合、指定のキューは生成されません。
Report Suppression	特定の VLAN への IGMP スヌーピングレポートの抑制を「Enabled」（有効）/「Disabled」（無効）にします。 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。1 から 300（秒）で設定可能です。
Querier State	「Enabled」（有効）にすると IGMP Query パケットを送信可能になります。初期値は「Disabled」（無効）です。
Query Version	IGMP スヌーピングクエリアに送信されるクエリパケットのバージョンを選択します。「1」「2」「3」から選択可能です。
Query Interval	IGMP query 送信間隔（秒）。1-31744 の範囲から指定します。初期値は 125 です。
Max Response Time (1-25)	IGMP response report を送信するまでの最大時間（秒）。1-25 の範囲から指定します。初期値は 10（秒）です。
Robustness Value (1-7)	パケットロスへの抵抗力を示します。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。1-255 の範囲から指定します。初期値は 2 です。
Last Member Query Interval (1-25)	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の Max Response Time 欄に設定する値（Last Member Query Interval）。また、同 Query の送信間隔でもあります。初期値は 1 です。
Proxy Reporting	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
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（1-1000）を指定します。「No Limit」を指定すると本プロファイルでのレートリミットをなくします。
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 Fast-Leave を設定したポート配下に複数の端末を配置しないでください。

注意 IGMP Snooping について、fast-leave は IGMPv2 のみサポートしています。

IGMP Snooping AAA Settings（IGMP Snooping AAA 設定）

IGMP Snooping AAA 設定を指定、表示します。

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

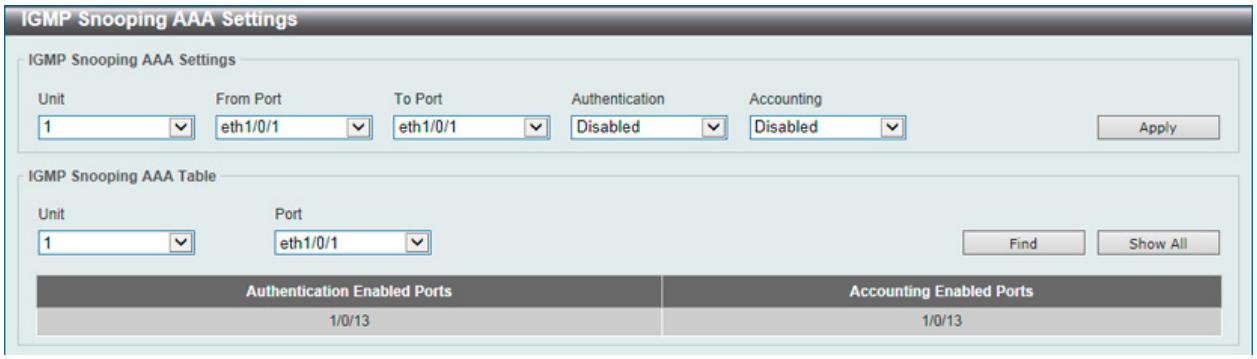


図 8-75　IGMP Snooping AAA Settings 画面

画面には以下の項目があります。

項目	説明
IGMP Snooping AAA Settings	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Authentication	認証を有効 / 無効にします。「IGMP join メッセージ」認証機能の有効 / 無効において使用します。有効時にクライアントがグループへの参加を希望する場合、システムにより認証が実行されます。
Accounting	アカウンティングを有効 / 無効にします。リスナーによる IGMP グループへの参加時にアカウンティングの有効 / 無効を指定します。有効時にクライアントがグループへの参加する場合、アカウンティングメッセージが RADIUS に送信されます。
IGMP Snooping AAA Table	
Unit	設定を行うユニットを指定します。
Port	設定を行うポートを指定します。

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

IGMP Snooping 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。

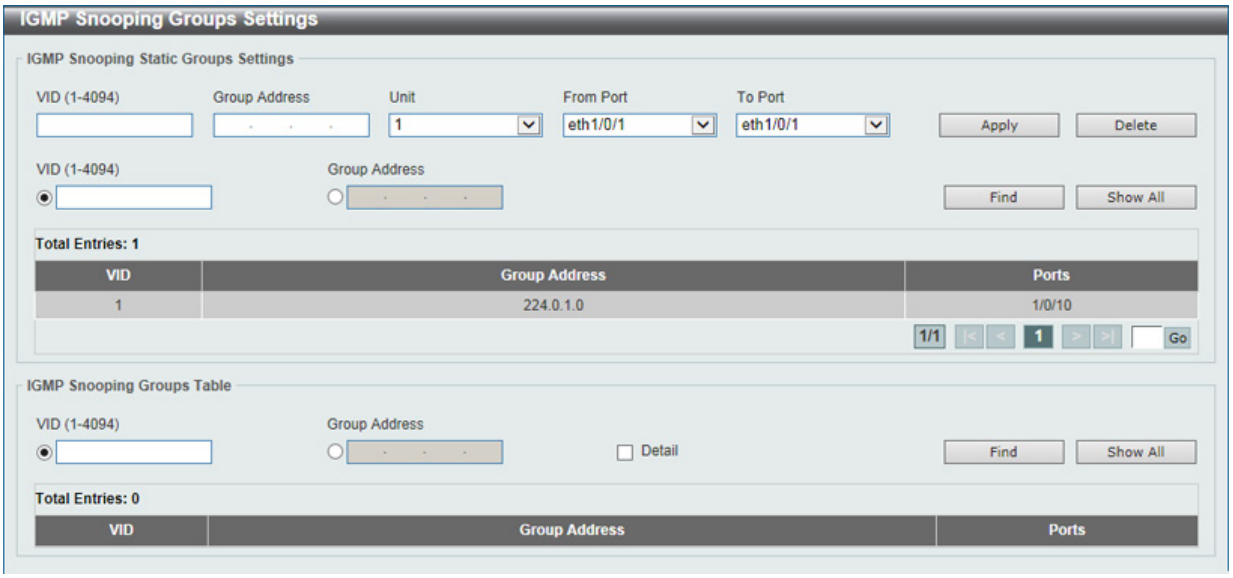


図 8-76　IGMP Snooping Groups Settings 画面

以下の項目を使用して、設定します。

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

項目	説明
IGMP Snooping Static Groups Settings	
VID	登録または削除するマルチキャストグループの VLAN ID（1-4094）を入力します。
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	設定するユニットを選択します。
From Port / To Port	設定するポート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（1-4094）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。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

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

項目	説明
IGMP 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。
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、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。
「Show Detail」指定のエントリの詳細情報を表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IGMP Snooping Filter Settings（IGMP Snooping フィルタ 設定）

IGMP Snooping フィルタの設定を行います。

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

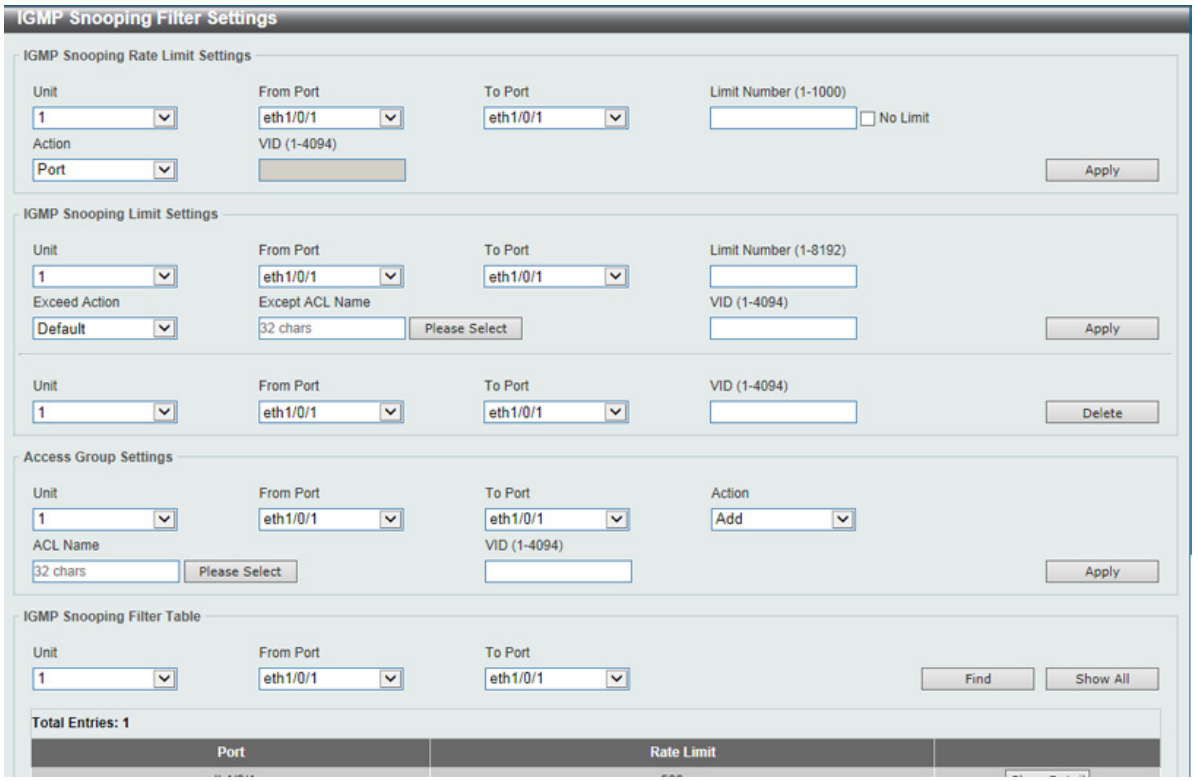


図 8-77　IGMP Snooping Filter Settings 画面

以下の項目を使用して、設定します。

IGMP Snooping Rate Limit Settings（IGMP スヌーピングレートリミット設定）

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Limit Number	制限する数を指定します。指定のインタフェースでスイッチがプロセス可能な IGMP コントロールパケットのレートを指定します。1-1000（パケット / 秒）で指定可能です。「No Limit」で制限を設定しません。
Action	実行するインタフェースを指定します。「Port」「VLAN」から指定可能です。
VID	「Action」で「VLAN」を選択すると表示されます。トランクポートの VLAN に受信するパケットに対して、フィルタします。VLAN を 1-4094 から指定します。

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ます。

IGMP Snooping Limit Settings（IGMP スヌーピングリミット設定）

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Limit Number	制限する数を指定します。生成される IGMP キャッシュエントリ数の制限をします。1-8192 で指定可能です。
Exceed Action	しきい値を超過した場合の動作について指定します。本パラメータでは制限が超過した場合の、新規学習グループの取り扱いに対しての動作を指定します。 • Default - 初期動作を指定します。 • Drop - 新規グループは破棄されます。 • Replace - 新規グループは古いグループと代替されます。
Except ACL Name	通常の IP アクセスリストを指定します。本アクセスリストに許可されたグループ (*,G) は制限から外れます。グループ (*,G) の許可にはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。32 字以内で指定可能です。「Please Select」をクリックすることにより、既に存在するアクセスリストから今回の設定に有効なアクセスリストを見つけることができます。
VID	トランクポートの VLAN に受信するパケットに対して、フィルタします。VLAN を 1-4094 から指定します。

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ます。
「Delete」をクリックすると指定のエントリを削除します。

Access Group Settings（アクセスグループ設定）

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Action	入力した情報に基づき新しいエントリの追加「Add」または、既存エントリの削除「Delete」を行います。
ACL Name	通常の IP アクセスリストを指定します。グループ (*,G) の許可にはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。32 字以内で指定可能です。「Please Select」をクリックすることにより、既に存在するアクセスリストから今回の設定に有効なアクセスリストを見つけることができます。
VID	設定する VLAN を指定します。VLAN を 1-4094 から指定します。

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ます。

IGMP Snooping Filter Table（IGMP スヌーピングフィルタ設定）

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。
「Show Detail」指定のエントリの詳細情報を表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Please Select をクリックすると次の画面が表示されます。



図 8-78　Please Select 画面

ACL 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。

Show Detail をクリックすると次の画面が表示されます。



図 8-79　Show Detail 画面

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

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

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

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

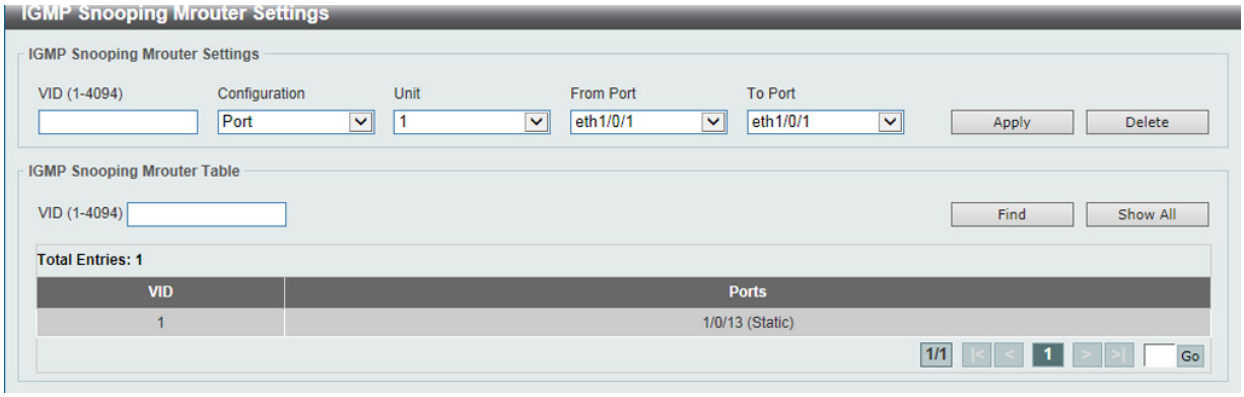


図 8-80　IGMP Snooping Mrouter Settings 画面

画面には以下の項目があります。

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

項目	説明
IGMP Snooping Mrouter Settings	
VID	VLAN ID を入力します。
Configuration	ポートの設定を行います。「Port」「Forbidden Port」から選択します。 • Port - マルチキャストが有効なルータと接続するポート範囲を設定します。プロトコルに関係なくマルチキャスト有効ルータに全てのパケットが届くことを確実にします。 • 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。禁止されたルータポートはルーティングパケットを送信しません。
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。

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

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

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

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

IGMP Snooping Statistics Settings（IGMP Snooping 統計設定）

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。

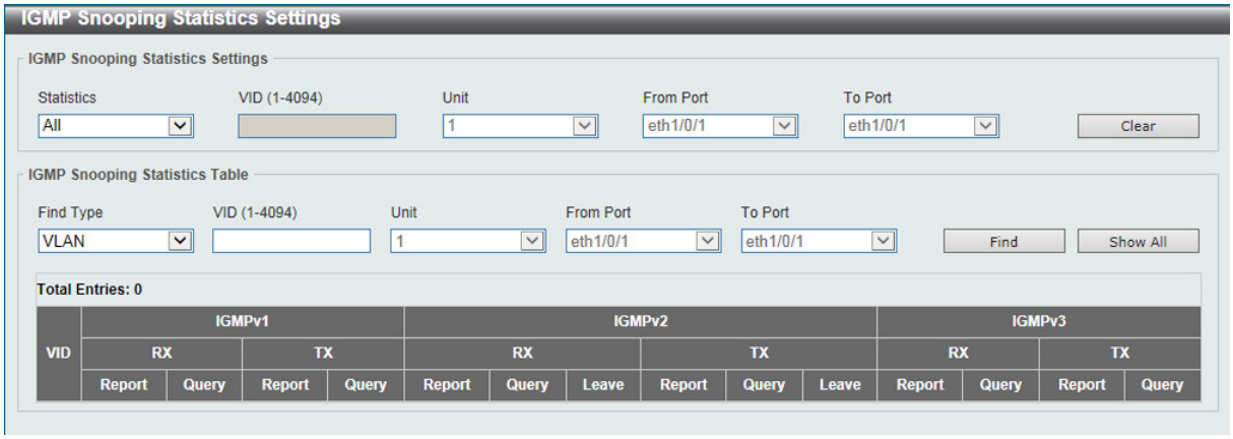


図 8-81　IGMP Snooping Statistics Settings 画面

以下の項目が表示されます。

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

項目	説明
Statistics	インタフェースを選択します。「All」「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Statistics」で「VLAN」を選択すると設定可能になります。
Unit	設定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。

「Clear」をクリックすると表示された統計情報がクリアされます。

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

項目	説明
Find Type	インタフェースを選択します。「VLAN」「Port」から選択します。
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	設定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。

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

MLD Snooping（MLD Snooping 設定）

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

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

MLD コントロールメッセージ

MLD Snooping バージョン 1 の実行には、デバイス間で 3 つのタイプのメッセージが送信されます。これらのメッセージは、130、131、132 および 143 にラベル付けされた ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query
IPv4 の IGMPv2 Host Membership Query（HMQ）と類似のものです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query は全マルチキャストアドレスに Listening ポートすべてにマルチキャストデータを送信する準備が整ったことを通知するために使用します。また、Multicast Specific query は特定のマルチキャストアドレスに送信準備が整ったことを通知するために使用します。 2 つのメッセージタイプは IPv6 ヘッダ内のマルチキャスト終点アドレス、および Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別します。

2. Multicast Listener Report Version1
IGMPv2 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

3. Multicast Listener Done
IGMPv2 の Leave Group Message と類似のものです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからマルチキャストデータを受信せず、このアドレスからのマルチキャストデータとともに" done"（完了）した旨を伝えます。スイッチは本メッセージを受信すると、この Listening ポートには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しません。

4. Multicast Listener Report、Version 2
IGMPv3 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

MLD Snooping Settings（MLD スヌーピング設定）

MLD Snooping 設定を有効または無効にします。

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

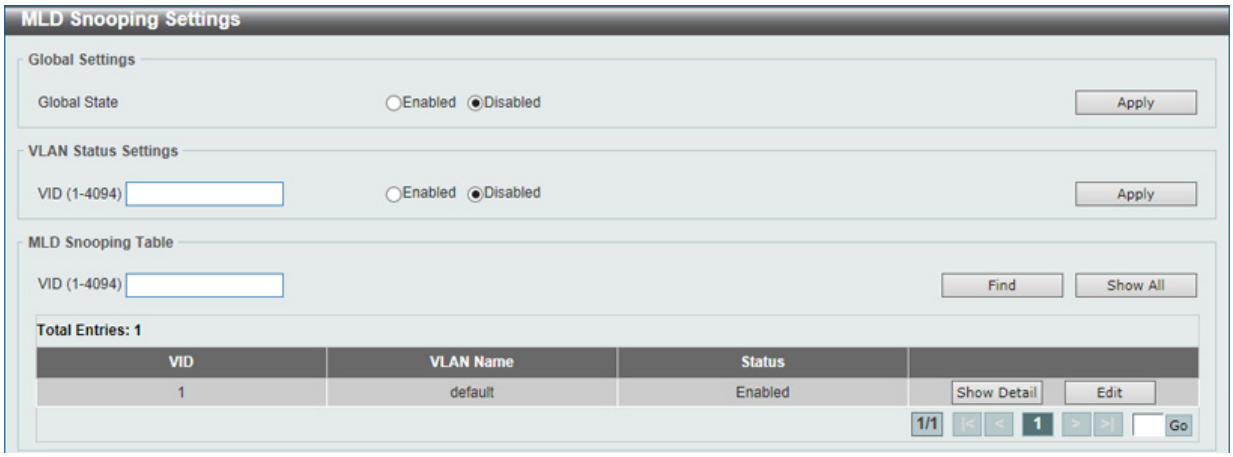


図 8-82　MLD Snooping Settings 画面

画面には以下の項目があります。

項目	説明
Global Setting	
Global State	MLD Snooping の有効 / 無効を設定します。 • Enabled - デバイスで MLD Snooping を有効にします。 • Disabled - デバイスで MLD Snooping を無効に設定します。（初期値）
VLAN Status Settings	
VID	VLAN 上の MLD Snooping を有効 / 無効にし、VLAN を識別する VLAN ID を指定します。 • Enabled - VLAN を有効にします。 • Disabled - VLAN を無効に設定します。（初期値）
MLD Snooping Table	
VID	MLD Snooping Table 上の VLAN を表示させるための VLAN ID を指定します。 • Find - 指定の VLAN ID を入力して指定のエントリを表示します。 • Show All - MLD Snooping Table 上のすべてのエントリを表示します。

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

MLD Snooping VLAN の詳細情報表示

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

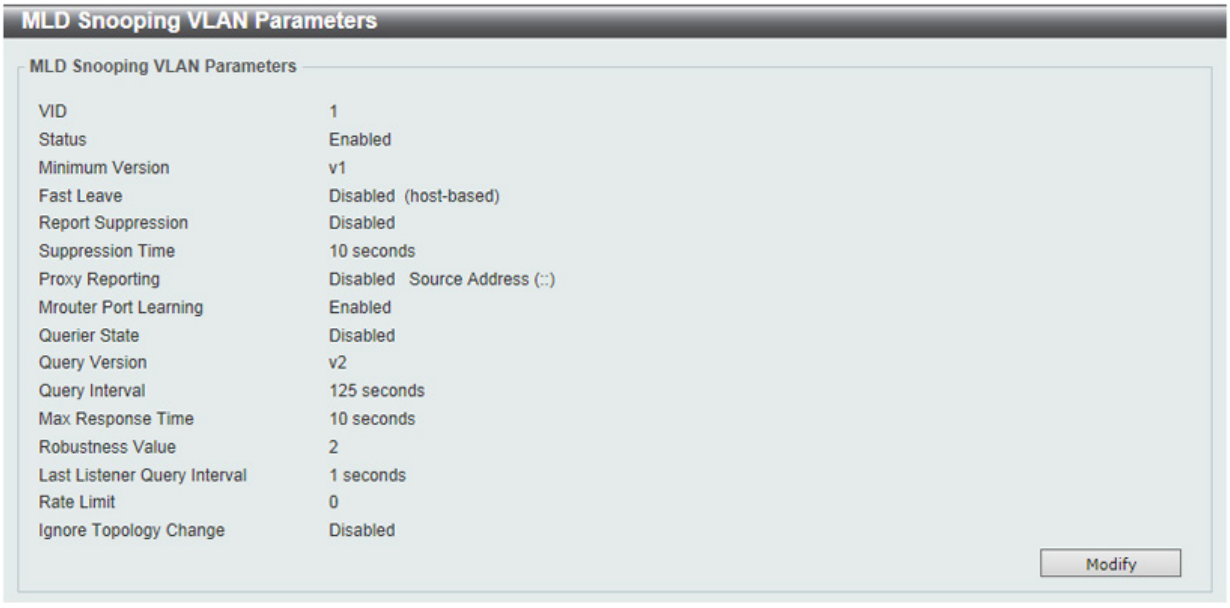


図 8-83　MLD Snooping VLAN Parameters 画面

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

MLD Snooping 機能の詳細設定

「MLD Snooping Settings」で関連する 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。

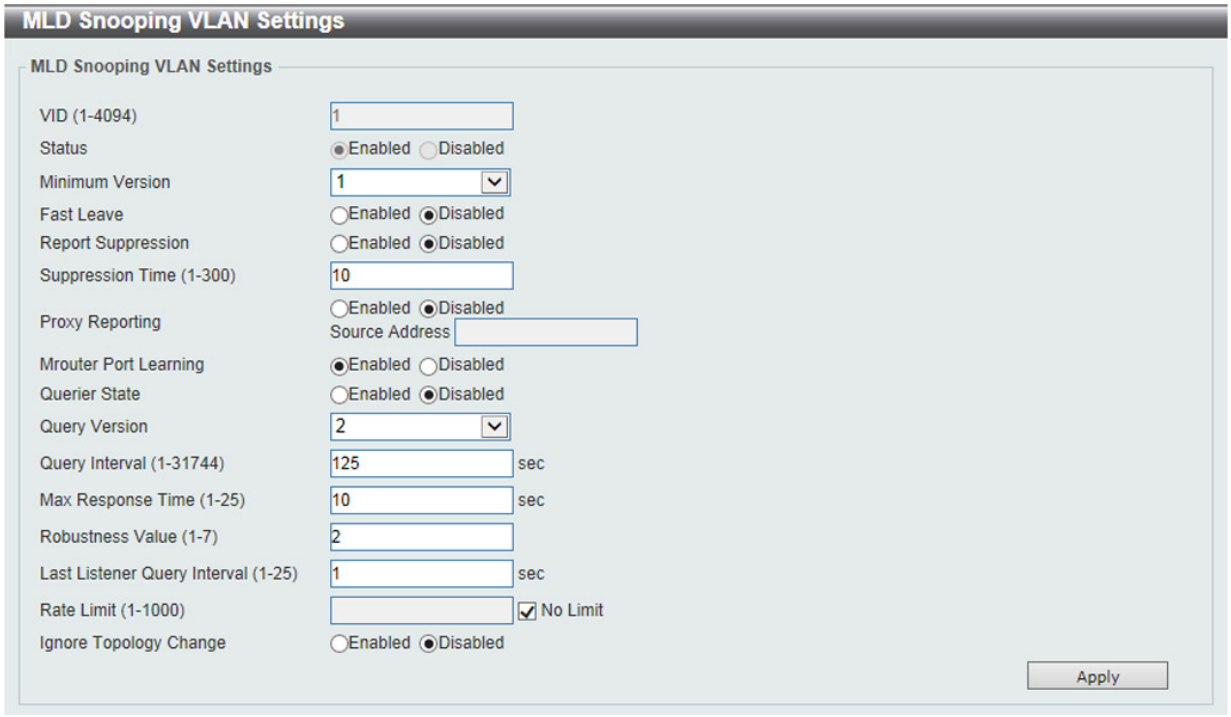


図 8-84 MLD Snooping VLAN Settings 画面

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	指定した VLAN への MLD Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。
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。1-2 で選択します。
Fast Leave	「Enabled」（有効）にすると、Fast Leave 機能が有効になります。この機能が有効になると、スイッチが MLD Leave Report パケットを受信する時、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。初期値は「Disabled」（無効）です。
Report Suppression	特定の VLAN への MLD スヌーピングレポートの抑制を「Enabled」（有効）/「Disabled」（無効）にします。 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。1 から 300（秒）で設定可能です。
Proxy Reporting	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
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。
Mrouter Port Learning	マルチキャストルータポートラーニングを有効 / 無効にします。
Querier State	「Enabled」（有効）にすると MLD Query パケットを送信可能になります。初期値は「Disabled」（無効）です。
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。「1」「2」から選択可能です。
Query Interval	MLD query 送信間隔（秒）。1-31744 の範囲から指定します。初期値は 125 です。
Max Response Time (1-25)	MLD response report を送信するまでの最大時間（秒）。1-25 の範囲から指定します。初期値は 10（秒）です。
Robustness Value (1-7)	パケットロスへの抵抗力を示します。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。1-255 の範囲から指定します。初期値は 2 です。
Last Listener Query Interval	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の Max Response Time 欄に設定する値（Last Listener Query Interval）。また、同 Query の送信間隔でもあります。初期値は 1 です。
Rate Limit	レートリミット（1-1000）を指定します。「No Limit」を指定すると本プロファイルでのレートリミットをなくします。
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。

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。

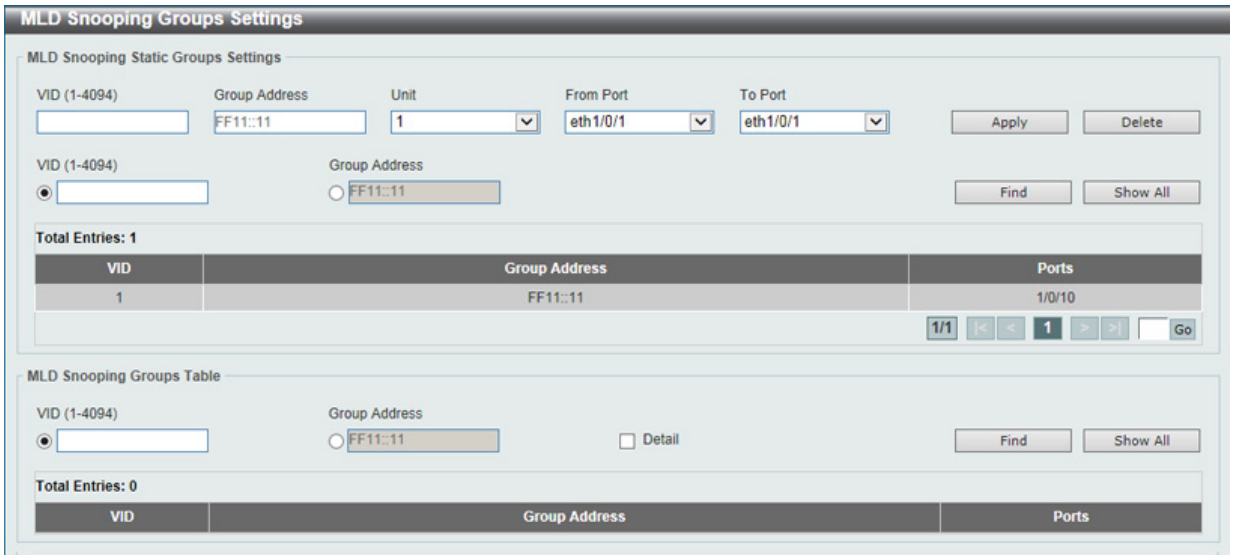


図 8-85　MLD Snooping Groups Settings 画面

以下の項目を使用して、設定します。

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

項目	説明
MLD Snooping Static Groups Settings	
VID	登録または削除する IPv6 マルチキャストグループの VLAN ID（1-4094）を入力します。
Group Address	登録または削除する IPv6 マルチキャストグループの IPv6 アドレスを入力します。
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート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。
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。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

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

項目	説明
MLD Snooping Groups Table	
VID	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（1-4094）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。
Detail	MLD グループの詳細について表示します。

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

MLD Snooping Filter Settings（MLD Snooping フィルタ Settings）

MLD Snooping フィルタの設定を行います。

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

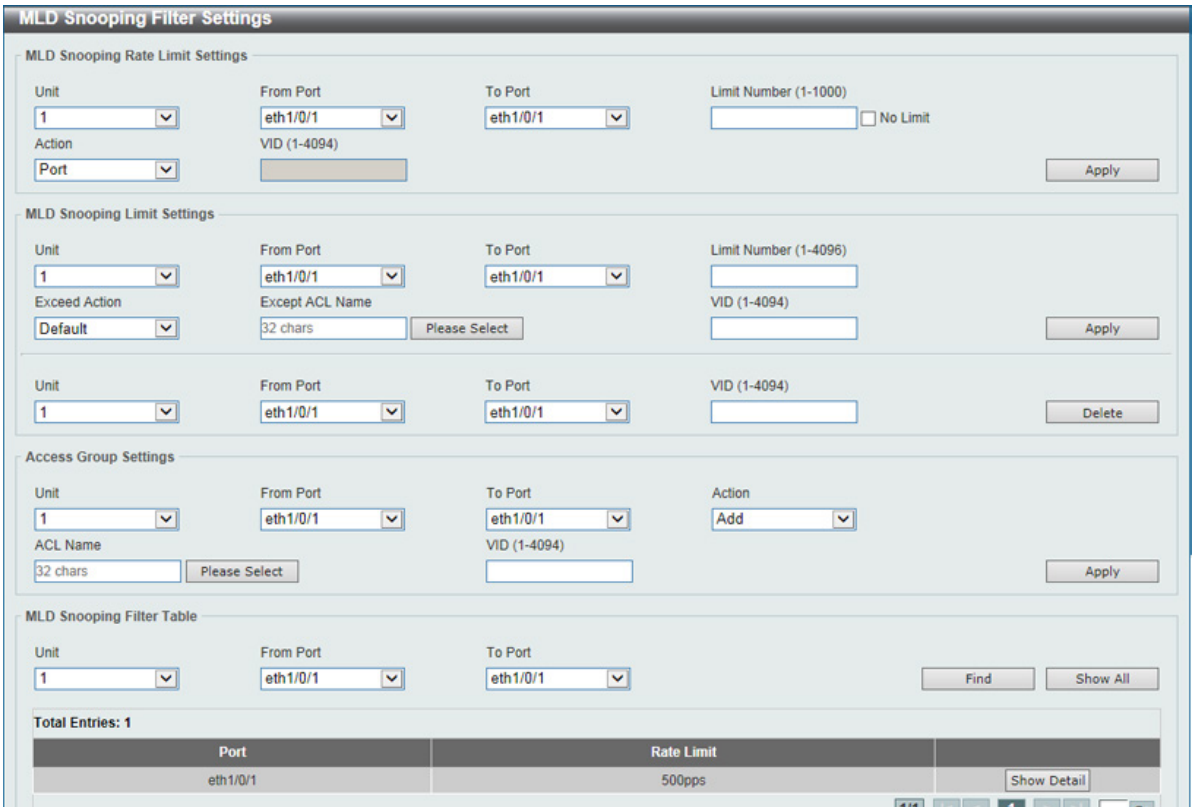


図 8-86　MLD Snooping Filter Settings 画面

以下の項目を使用して、設定します。

MLD Snooping Rate Limit Settings（MLD スヌーピングレートリミット設定）

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Limit Number	制限する数を指定します。指定のインタフェースでスイッチがプロセス可能な MLD コントロールパケットのレートを指定します。1-1000（パケット / 秒）で指定可能です。「No Limit」で制限を設定しません。
Action	実行するインタフェースを指定します。「Port」「VLAN」から指定可能です。
VID	「Action」で「VLAN」を選択すると表示されます。トランクポートの VLAN に受信するパケットに対して、フィルタします。VLAN を 1-4094 から指定します。

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ます。

MLD Snooping Limit Settings（MLD スヌーピングリミット設定）

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Limit Number	制限する数を指定します。生成される MLD キャッシュエントリ数の制限をします。1-4096 で指定可能です。
Exceed Action	しきい値を超過した場合の動作について指定します。本パラメータでは制限が超過した場合の、新規学習グループの取り扱いに対しての動作を指定します。 • Default - 初期動作を指定します。 • Drop - 新規グループは破棄されます。 • Replace - 新規グループは古いグループと代替されます。
Except ACL Name	通常の IP アクセスリストを指定します。本アクセスリストに許可されたグループ (*,G) は制限から外れます。グループ (*,G) の許可にはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。32 字以内で指定可能です。「Please Select」をクリックすることにより、既に存在するアクセスリストから今回の設定に有効なアクセスリストを見つけることができます。
VID	トランクポートの VLAN に受信するパケットに対して、フィルタします。VLAN を 1-4094 から指定します。

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ます。
「Delete」をクリックすると指定のエントリを削除します。

Access Group Settings（アクセスグループ設定）

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
Action	入力した情報に基づき新しいエントリの追加「Add」または、既存エントリの削除「Delete」を行います。
ACL Name	通常の IP アクセスリストを指定します。グループ (*,G) の許可にはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。32 字以内で指定可能です。「Please Select」をクリックすることにより、既に存在するアクセスリストから今回の設定に有効なアクセスリストを見つけることができます。
VID	設定する VLAN を指定します。VLAN を 1-4094 から指定します。

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ます。

MLD Snooping Filter Table（MLD スヌーピングフィルタ設定）

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。
「Show Detail」指定のエントリの詳細情報を表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Please Select をクリックすると次の画面が表示されます。



図 8-87　Please Select 画面

ACL 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。

Show Detail をクリックすると次の画面が表示されます。



図 8-88　Show Detail 画面

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

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

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。

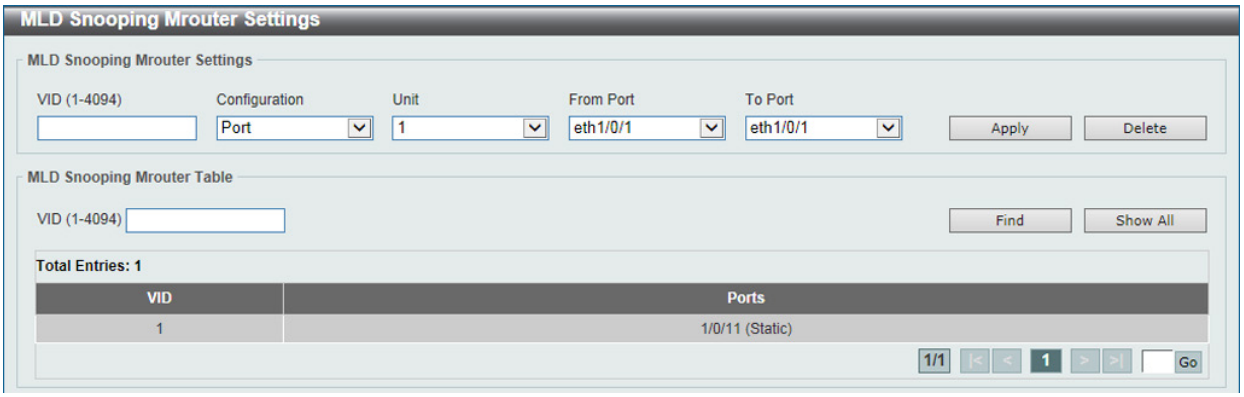


図 8-89　MLD Snooping Mrouter Settings 画面

画面には以下の項目があります。

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

項目	説明
MLD Snooping Mrouter Settings	
VID	VLAN ID を入力します。
Configuration	ポートの設定を行います。「Port」「Forbidden Port」「Learn pimv6」から選択します。 • Port - マルチキャストが有効なルータと接続するポート範囲を設定します。プロトコルに関係なくマルチキャスト有効ルータに全てのパケットが届くことを確実にします。 • 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。禁止されたルータポートはルーティングパケットを送信しません。 • 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	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。

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

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

項目	説明
MLD Snooping Mrouter Table	
VID	VLAN ID（1-4094）を入力します。

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

MLD Snooping Statistics Settings（MLD Snooping 統計設定）

現在の MLD Snooping の統計情報を表示します。

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

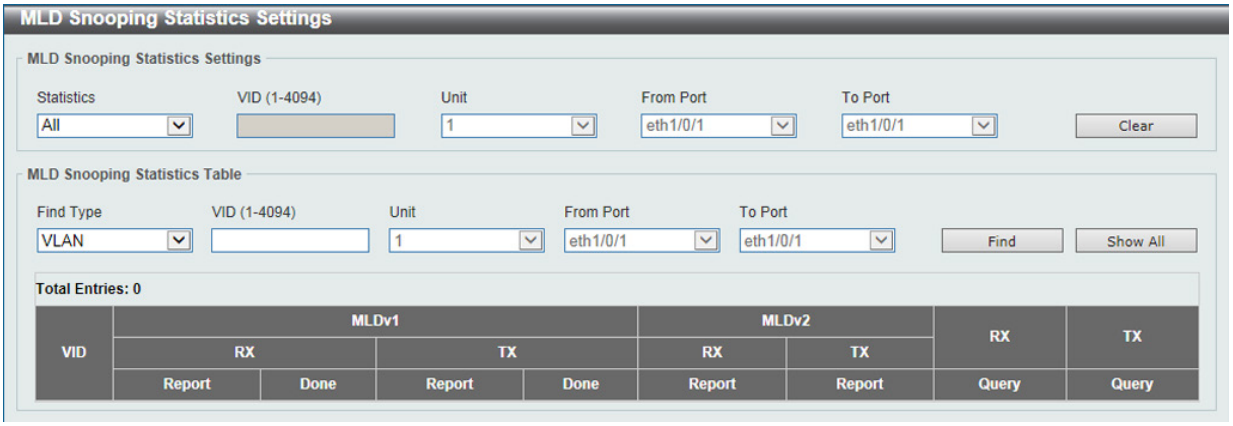


図 8-90　MLD Snooping Statistics Settings 画面

以下の項目が表示されます。

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

項目	説明
Statistics	インタフェースを選択します。「All」「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Statistics」で「VLAN」を選択すると設定可能になります。
Unit	設定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。

「Clear」をクリックすると表示された統計情報がクリアされます。

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

項目	説明
Find Type	インタフェースを選択します。「VLAN」「Port」から選択します。
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	設定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。

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

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。

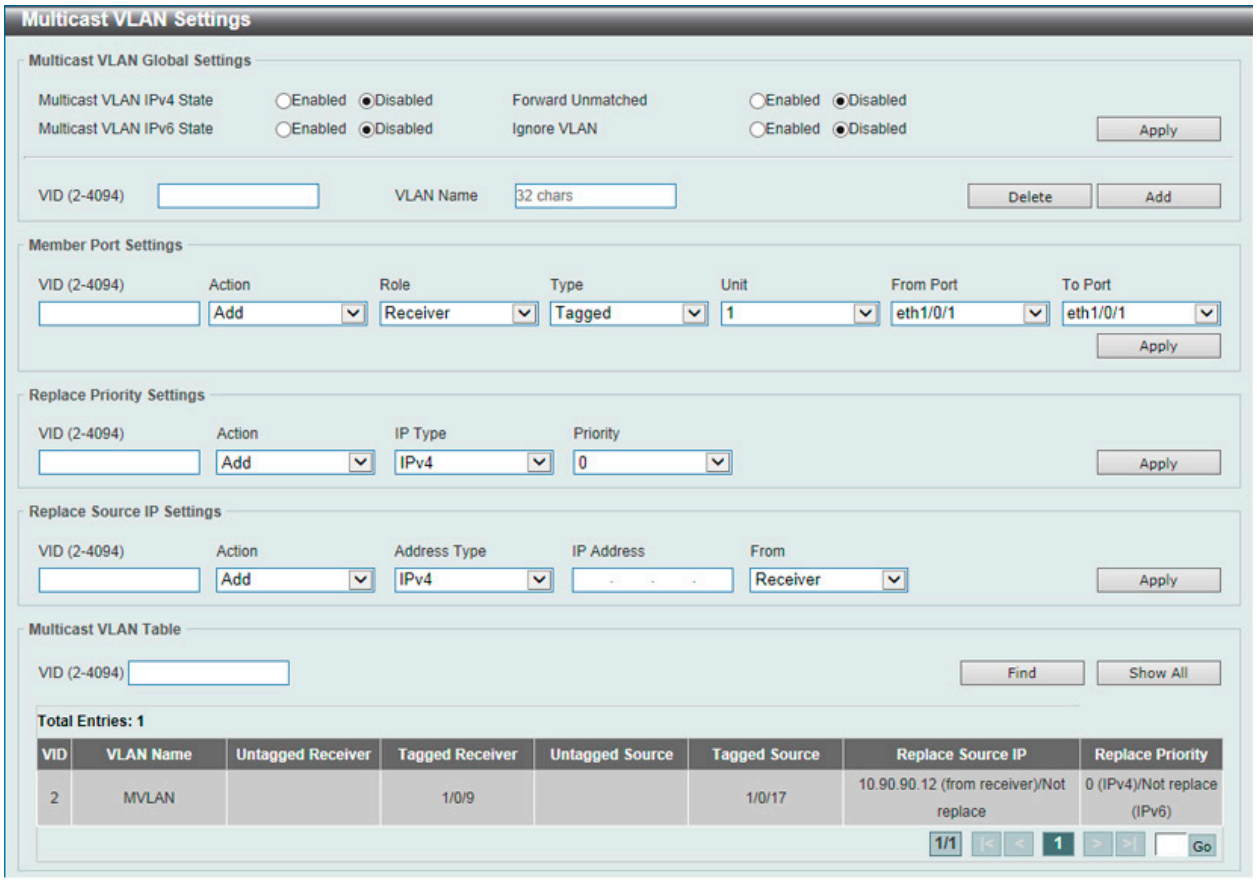


図 8-91　Multicast VLAN Settings 画面

以下の項目を使用して設定します。

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します。
Forward Unmatched	「Forward Unmatched」を有効または無効にします。 「タグなし」「どのプロファイルともマッチしない」「マルチキャスト VLAN が関連する初期 VLAN」「マルチキャスト VLAN にタグ付けも、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または無効にします。
Ignore VLAN	「Ignore VLAN」を有効 / 無効に指定します。本設定ではタグ付き IGMP/MLD コントロールパケットの設定を行います。有効にするとパケットの VLAN は無視され、プロファイルにマッチするマルチキャスト VLAN を検出します。スイッチは受信する IGMP、または MLD コントロールパケットを無視し、マッチするプロファイルを照合します。
VID (2-4094)	作成 / 削除する VLAN の VID（2-4094）を指定します。
VLAN Name	作成 / 削除する VLAN 名を指定します。
Member Port Settings	
VID (2-4094)	設定する VLAN の VID（2-4094）を指定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。
Role	メンバポートの役割を指定します。「Receiver」「Source」から指定可能です。 • 「Receiver」- マルチキャスト VLAN のマルチキャストデータのみを受信する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のみを送信す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」「Untagged」から指定可能です。 • 「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 をタグ付けされます。 • 「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	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Replace Priority Settings	
VID (2-4094)	設定する VLAN の VID（2-4094）を指定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。
IP Type	メンバポートの種類を指定します。「 IPv4」「IPv6」から指定可能です。 • 「IPv4」- マルチキャスト VLAN に転送される IPv4 マルチキャストパケットの優先値を再マップします。 • 「IPv6」- マルチキャスト VLAN に転送される IPv6 マルチキャストパケットの優先値を再マップします。
Priority	優先値を指定します。0-7 の範囲で指定できます。値が低い方が優先度が高くなります。
Replace Source IP Settings	
VID (2-4094)	設定する VLAN の VID（2-4094）を指定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。
Address Type	アドレスの種類を指定します。「 IPv4」「IPv6」から指定可能です。 • 「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	送信元を指定します。「Receiver」「Source」「Both」 「Receiver」- マルチキャスト VLAN 受信ポートに受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを交代します。 「Source」- マルチキャスト VLAN 送信元ポートに受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを交代します。 • Both - マルチキャスト VLAN（送受信）ポートに受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを交代します。
Multicast VLAN Table	
VID (2-4094)	設定する VLAN の VID（2-4094）を指定します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Multicast VLAN Group Settings（マルチキャスト VLAN グループ設定）

マルチキャスト VLAN グループの設定、表示を行います。

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

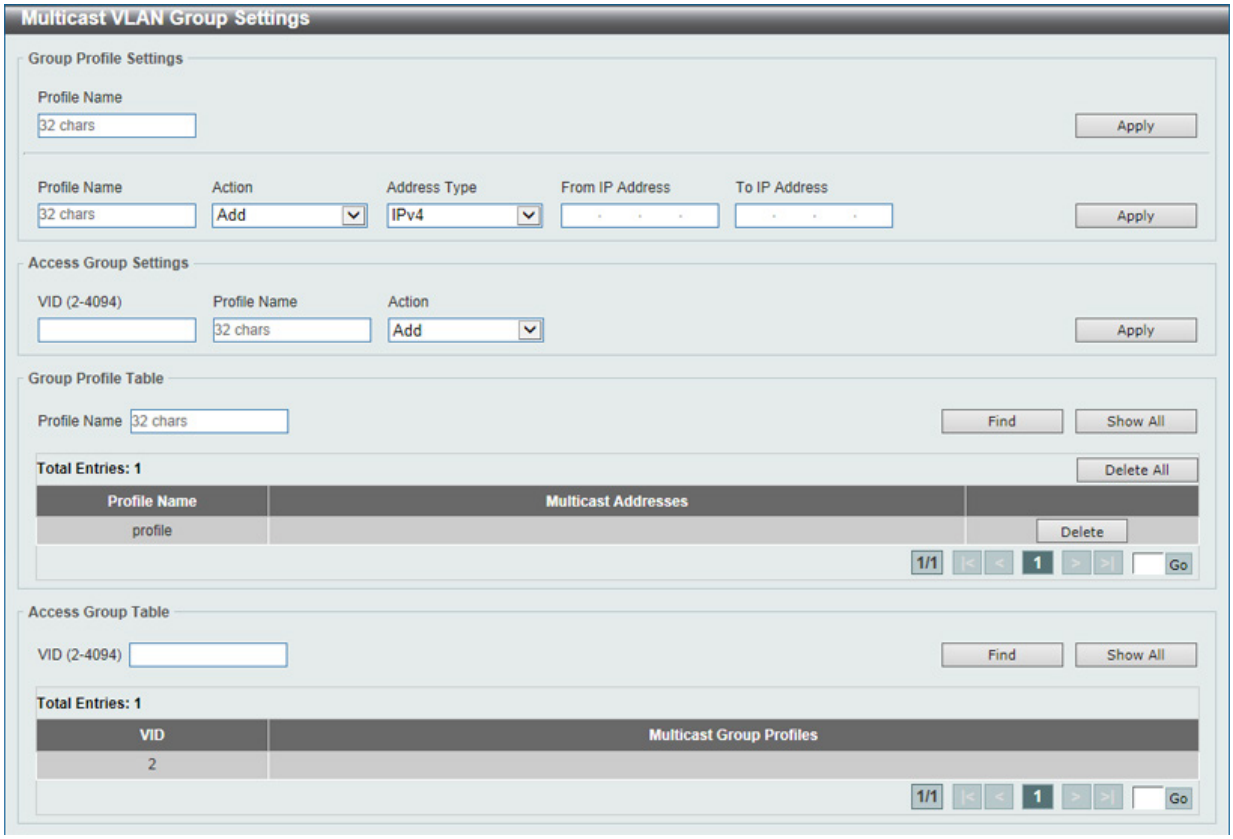


図 8-92　Multicast VLAN Group Settings 画面

以下の項目を使用して、設定します。

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（32 字以内）を指定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。マルチプルの範囲をマルチキャスト VLAN プロファイルに追加できます。単一のプロファイルに指定されている 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。
Address Type	アドレスタイプを指定します。「IPv4」「IPv6」から指定します。 • 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（2-4094）を指定します。
Profile Name	マルチキャスト VLAN のグループプロファイル名（32 字以内）を指定します。
Action	実行する動作を指定します。「Add」「Delete」から指定できます。
Group Profile Table	
Profile Name	マルチキャスト VLAN のグループプロファイル名（32 字以内）を指定します。
Access Group Table	
VID	VLAN ID（2-4094）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ます。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Delete All」をクリックするとすべてのエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

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

PIM Snooping（PIM スヌーピング）

L2 Features > L2 Multicast Control > PIM Snooping

PIM Snooping Global Settings（PIM スヌーピンググローバル設定）

Protocol Independent Multicast（PIM）をグローバルに設定します。

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



図 8-93　PIM Snooping Global Settings 画面

画面には以下の項目があります。

項目	説明
Global Setting	
Global State	PIM Snooping の有効 / 無効を設定します。 • Enabled - デバイスで PIM Snooping を有効にします。 • Disabled - デバイスで PIM Snooping を無効に設定します。（初期値）
VLAN Status Settings	
VID	VLAN 上の PIM Snooping を有効 / 無効にし、VLAN を識別する VLAN ID（1-4094）を指定します。 • Enabled - VLAN を有効にします。 • Disabled - VLAN を無効に設定します。（初期値）
PIM Snooping Table	
VID	PIM Snooping Table 上の VLAN を表示させるための VLAN ID（1-4094）を指定します。

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。

PIM Snooping Neighbor Settings（PIM スヌーピングネイバ設定）

PIM スヌーピングネイバテーブルを表示します。

L2 Features > L2 Multicast Control > PIM Snooping > PIM Snooping Neighbor Table をクリックして表示します。



図 8-94　PIM Snooping Neighbor Table 画面

画面には以下の項目があります。

項目	説明
VID	表示する VLAN を識別する VLAN ID（1-4094）を指定します。

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。

PIM Snooping Mroute Table（PIM Snooping マルチキャストルートテーブル）

PIM スヌーピングマルチキャストルートテーブルを表示します。

L2 Features > L2 Multicast Control > PIM Snooping > PIM Snooping Mroute Table をクリックして表示します。

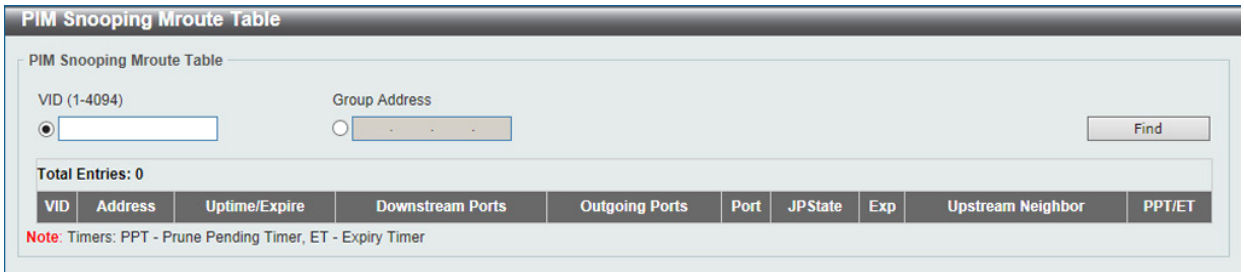


図 8-95　PIM Snooping Mroute Table 画面

画面には以下の項目があります。

項目	説明
PIM Snooping Mrouter Table	
VID	VLAN ID（1-4094）を入力します。
Group Address	選択しグループアドレスを指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

PIM Snooping Statistics Table（PIM Snooping 統計テーブル）

現在の PIM Snooping の統計情報を表示します。

L2 Features > L2 Multicast Control > PIM Snooping > PIM Snooping 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。

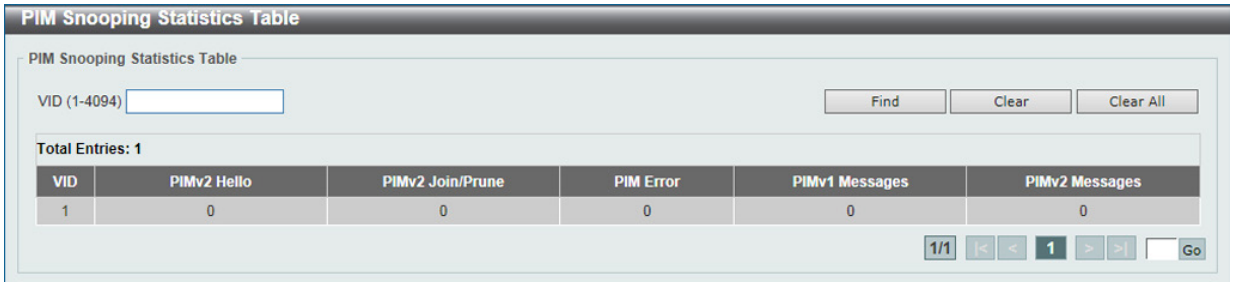


図 8-96　PIM Snooping Statistics Table 画面

以下の項目が表示されます。

項目	説明
VID	VLAN ID（1-4094）を指定します。

「Clear」をクリックすると表示された統計情報がクリアされます。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Multicast Filtering Mode（マルチキャストフィルタリングモード）

L2 マルチキャストフィルタリング設定を行います。

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

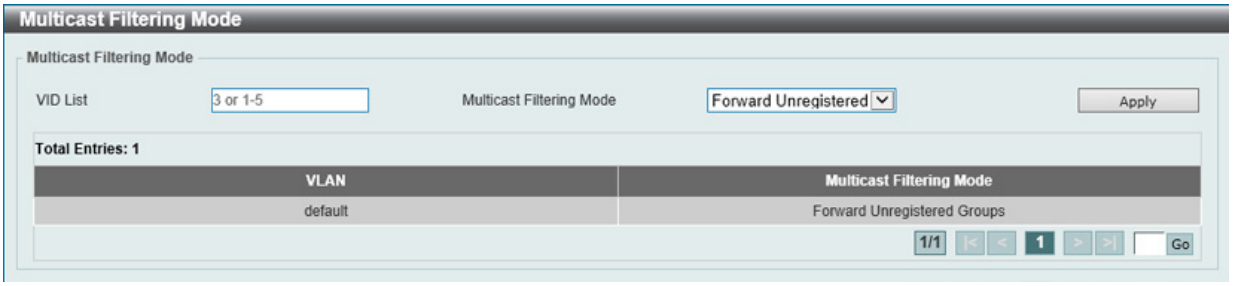


図 8-97　Multicast Filtering Mode 画面

以下の項目を使用して、設定します。

項目	説明
VID List	設定する 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」「Forward All」「Filter Unregistered」から選択可能です。 • 「Forward Unregistered」- 選択すると登録されたマルチキャストパケットはフォワーディングテーブルに基づいて転送され、登録されていないマルチキャストパケットは VLAN ドメインに基づきフラッドします。 • 「Forward All」- 選択するとすべてのマルチキャストパケットは VLAN ドメインに基づきフラッドします。 • 「Filter Unregistered」- 選択すると登録されたマルチキャストパケットはフォワーディングテーブルに基づき転送され、登録されていないマルチキャストパケットはフィルタされます。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

LLDP

L2 Features > LLDP

LLDP（Link Layer Discovery Protocol）は、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。

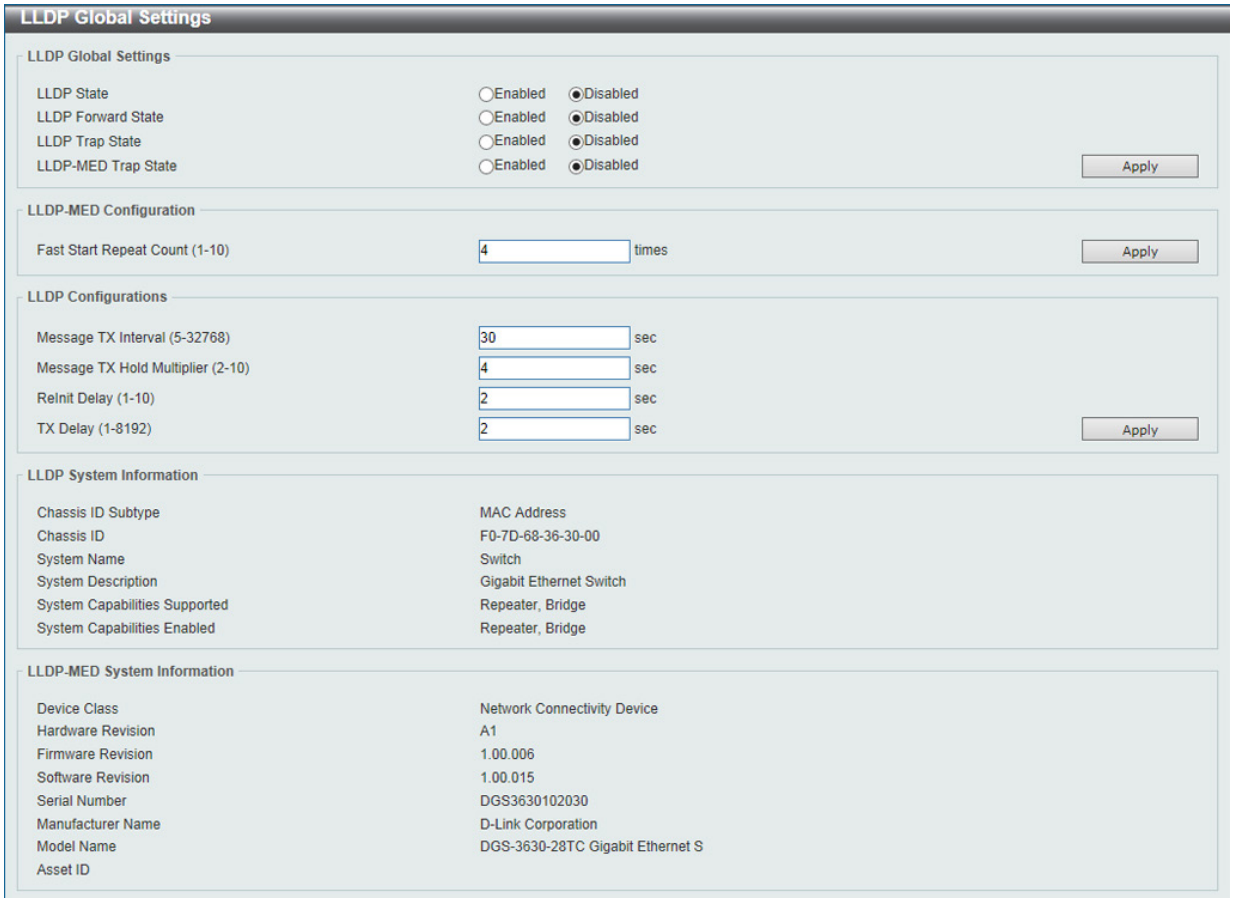


図 8-98　LLDP Global Settings 画面

以下の項目を設定できます。

項目	説明
LLDP State	スイッチにおける LLDP 機能を「Enabled」（有効）または「Disabled」（無効）にします。
LLDP Forward State	同じ IEEE 802 ネットワークに割り当てられた他のステーションに通知するために LLDP 機能のメッセージ転送を「Enabled」（有効）または「Disabled」（無効）にします。 「LLDP」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 / 無効に指定します。
LLDP-MED Trap State	LLDP-MED Trap を有効 / 無効に指定します。
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。1 から 10 の間で指定できます。
LLDP Configurations	
Message TX Interval (5-32768)	アクティブなポートが通知を再送する方法を制御します。パケット伝送間隔を変更するために、5-32768（秒）の範囲で値を入力します。
Message TX Hold Multiplier (2-10)	LLDP スイッチに使用される乗数を変更することで LLDP Neighbor に LLDP 通知を作成して送信する有効期間（TTL : Time-to-Live）を計算します。指定通知の TTL（Time-to-Live）の期限が来ると、通知データは Neighbor スイッチの MIB から削除されます。
ReInit Delay (1-10)	LLDP ポートが LLDP 無効にするコマンドを受け取った後、再初期化を行う前に待機する最小時間です。LLDP Reinit Delay を変更するために、1-10（秒）から値を入力します。

項目	説明
TX Delay (1-8192)	LLDP MIB のコンテンツ変更のために、LLDP ポートが連続した LLDP 通知の送信を遅らせる最短時間（遅延間隔）を変更します。LLDP TX Delay を変更するために、1-8192（秒）から値を入力します。

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。

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。

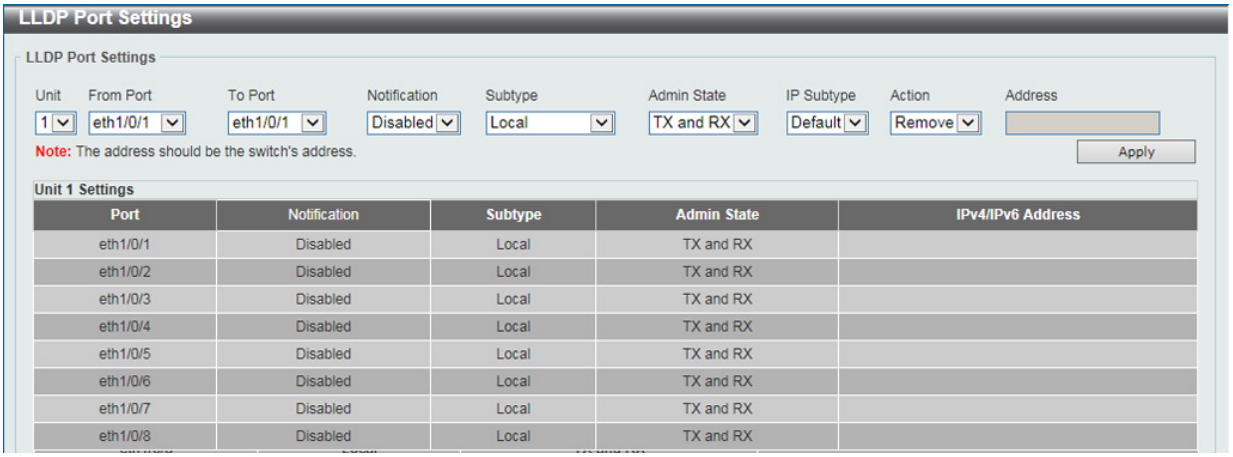


図 8-99　LLDP Port Settings 画面

以下の項目を設定できます。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	プルダウンメニューを使用して設定するポート範囲を指定します。
Subtype	プルダウンメニューを使用して LLDP TLV(s) のサブタイプを選択します。「MAC Address」「Local」から選択可能です。
Notification	プルダウンメニューを使用して LLDP 通知を「Enabled」（有効）または「Disabled」（無効）にします。
Admin State	プルダウンメニューを通知のステータスを選択します。: Tx（送信のみ）、Rx（受信のみ）、Tx And Rx（送受信）または「Disabled」（無効）。 TX - ローカル LLDP エージェントは LLDP フレーム送信のみします。 RX - ローカル LLDP エージェントは LLDP フレーム受信のみします。 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します。 Disabled - ローカル LLDP エージェントは LLDP フレームの送受信をしません。 初期値は TX and RX です。
IP Subtype	プルダウンメニューを使用して送信する IP アドレスの種類を選択します。
Address	通知するエンティティの管理アドレスを入力します。
Action	ポートベースの管理アドレス機能を「Enabled」（有効）または「Disabled」（無効）にします。

「Apply」ボタンをクリックし、変更を有効にします。

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 8-100 LLDP Management Address List 画面

以下の項目を設定できます。

項目	説明
Subtype	表示する LLDP 管理アドレスのサブタイプを「All」「IPv4」「IPv6」から選択します。

「Find」ボタンをクリックし、LLDP 管理情報を検索します。

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

TLV（Type-length-value）は、LLDP パケット内の TLV エレメントとして特定の送信情報を許可します。本スイッチにおけるベーシック TLV 設定を有効にします。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いつも必須データを含んでいます。外向き LLDP 通知からこれらのデータタイプの 1 個以上を除外するために、個別のポートまたはポートグループに設定できる 4 つのオプションデータがあり、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。
本スイッチにおけるベーシック TLV 設定を有効にします。

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。

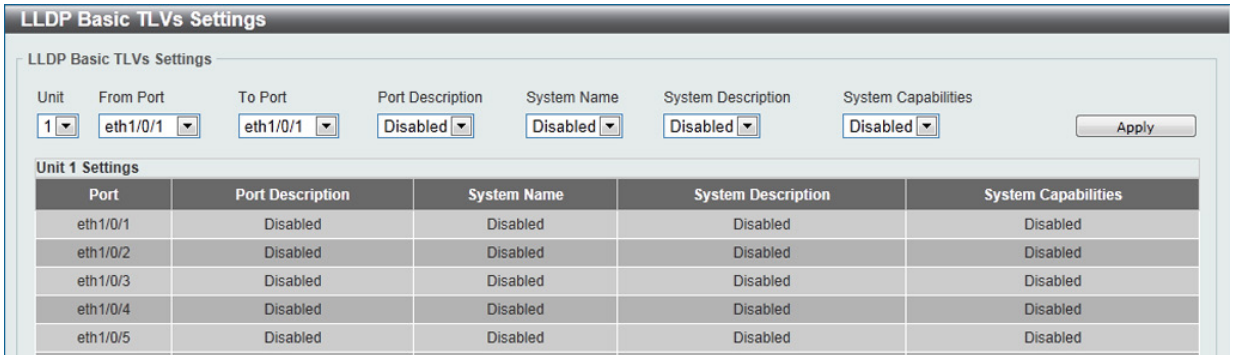


図 8-101 LLDP Basic TLVs Settings 画面

プルダウンメニューを使用してベーシック TLV 設定を「Enabled」（有効）/「Disabled」（無効）にします。

以下の項目を設定できます。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
Port Description	ポート説明を「Enabled」（有効）/「Disabled」（無効）にします。
System Name	システム名を「Enabled」（有効）/「Disabled」（無効）にします。
System Description	システム説明を「Enabled」（有効）/「Disabled」（無効）にします。
System Capabilities	システム能力を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

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

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

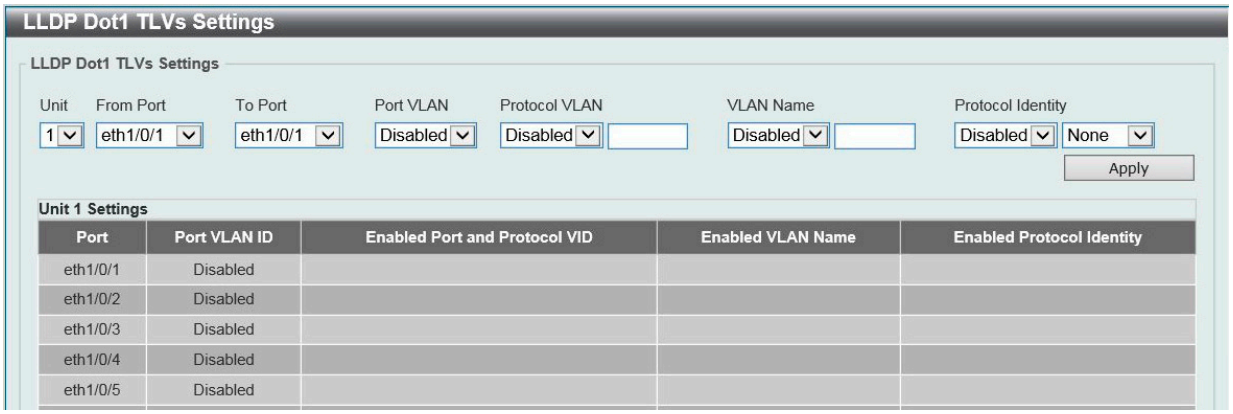


図 8-102　LLDP Dot1 TLVs Settings 画面

以下の項目が使用できます。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
Port VLAN	ポート VLAN ID TLV の通知を「Enabled」（有効）/「Disabled」（無効）にします。 「ポート VLAN ID TLV」は VLAN ブリッジポートにタグなし・タグ付きフレームの PVID の通知を許可するオプションのフィックス長 TLV です。
Protocol VLAN	プロトコル VLAN ID の通知を「Enabled」（有効）/「Disabled」（無効）にします。 対象となるプロトコル VLAN を右の欄で VLAN ID で指定します。
VLAN Name	VLAN 名の通知を「Enabled」（有効）/「Disabled」（無効）にします。 対象となるプロトコル VLAN を右の欄で VLAN ID で指定します。
Protocol Identity	プロトコル識別子の通知を「Enabled」（有効）/「Disabled」（無効）にします。 次に対象とするプロトコルを None、EAPOL、LACP、GVRP、STP または All から選択します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

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

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

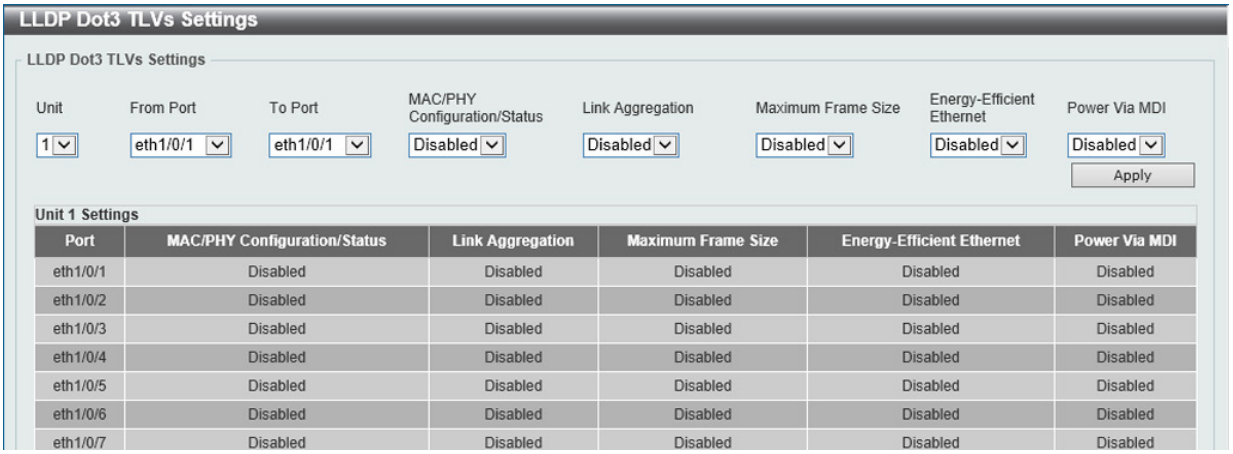


図 8-103　LLDP Dot3 TLVs Settings 画面

以下の項目を設定できます。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
MAC/PHY Configuration/Status	スイッチの MAC または PHY 状態の通知を「Enabled」（有効）/「Disabled」（無効）にします。
Link Aggregation	スイッチのリンクアグリゲーション状態の通知を「Enabled」（有効）/「Disabled」（無効）にします。

項目	説明
Maximum Frame Size	最大フレームサイズの通知を「Enabled」（有効）/「Disabled」（無効）にします。
Energy-Efficient Ethernet	「Energy-Efficient Ethernet TLV」送信を有効 / 無効に指定します。「Energy-Efficient Ethernet TLV」はパケットが送信されていないリンクのエネルギー消費を削減する機能です。
Power Via MDI	「MDI TLV」経由での電力送信を有効 / 無効にします。IEEE802.3 PMD の実装により接続した電力供給のないシステムに対し電力を供給します。「Power Via MDI TLV」により IEEE 802.3 LAN ステーションに MDI 電力サポート機能を提供するネットワーク管理を実現します。

「Apply」ボタンをクリックし、変更を有効にします。

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

LLDP-MED TLV の送信を有効または無効にします。

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

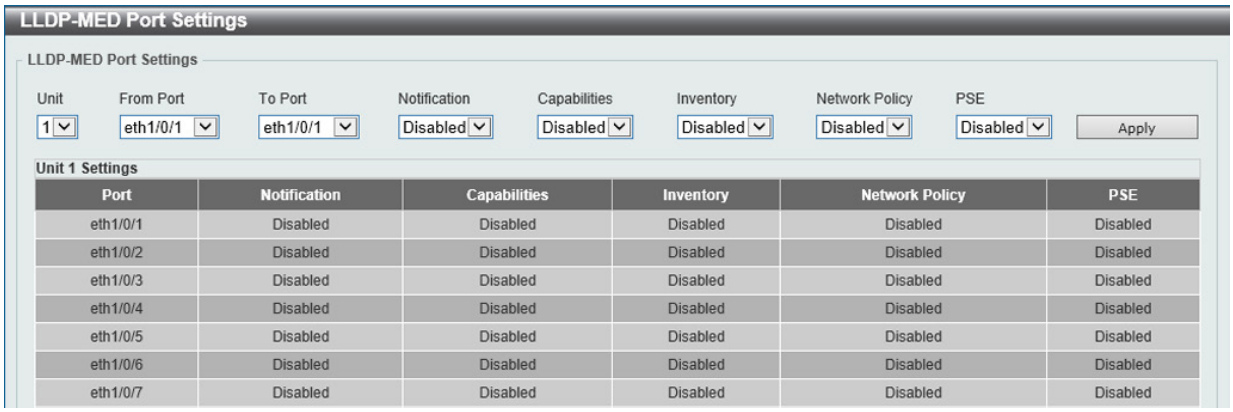


図 8-104　LLDP-MED Port Settings 画面

以下の項目が使用できます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Notification	「LLDP-MED notification TLV」の送信を有効 / 無効にします。
Capabilities	「LLDP-MED capabilities TLV」の送信を有効 / 無効にします。
Inventory	「LLDP-MED inventory TLV」の送信を有効 / 無効にします。
Network Policy	「LDP-MED network policy TLV」の送信を有効 / 無効にします。
PSE	「MDI TLV」経由での LLDP-MED 拡張電力送信を有効 / 無効にします。接続しているデバイスが「PSE」または「PD」である必要があります。

「Apply」ボタンをクリックして変更を適用します。

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

LLDP-DCBX（Data Center Bridging Exchange）TLV の送信を有効または無効にします。

L2 Features > LLDP > LLDP-DCBX 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。

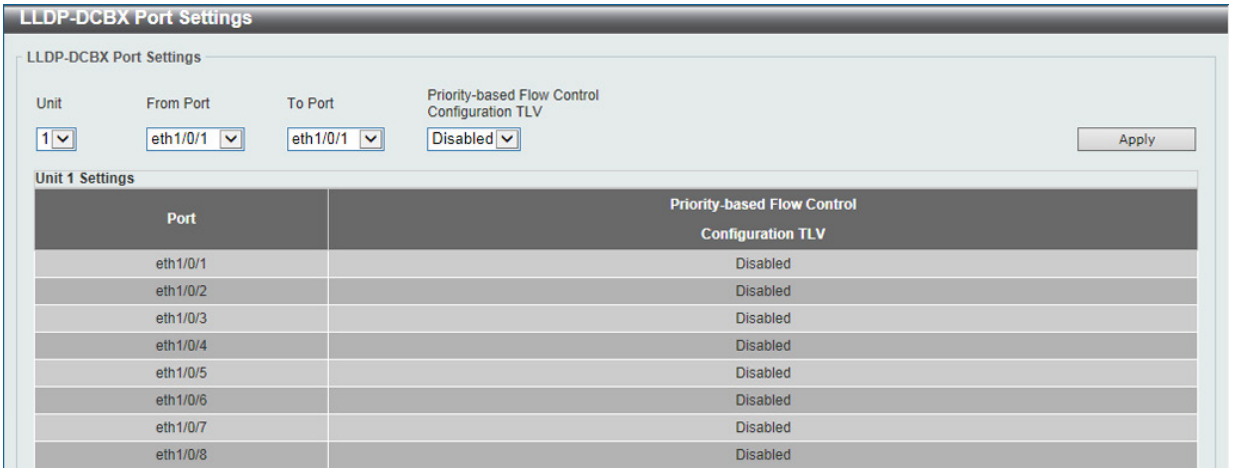


図 8-105　LLDP-DCBX Port Settings 画面

以下の項目が使用できます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Priority-based Flow Control Configuration TLV	「Priority-based Flow Control」(PFC) Configuration TLV を有効 / 無効に指定します。有効にすると「PFC Configuration TLV」が送信されます。「PFC TLV」はブリッジポートに現在の状況と PFC の今後の動作についての通知を許可します。

「Apply」ボタンをクリックして変更を適用します。

LLDP Statistics Information（LLDP 統計情報）

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。

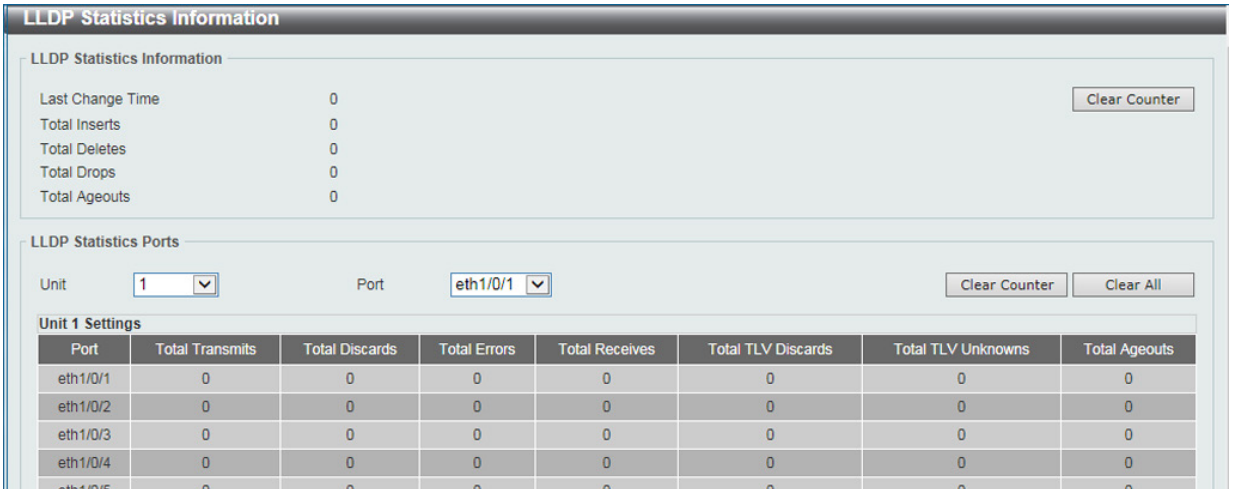


図 8-106　LLDP Statistics Information 画面

以下の項目が使用できます。

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）

以下のローカルポートの要約テーブルにポートベースの情報を表示します。

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。

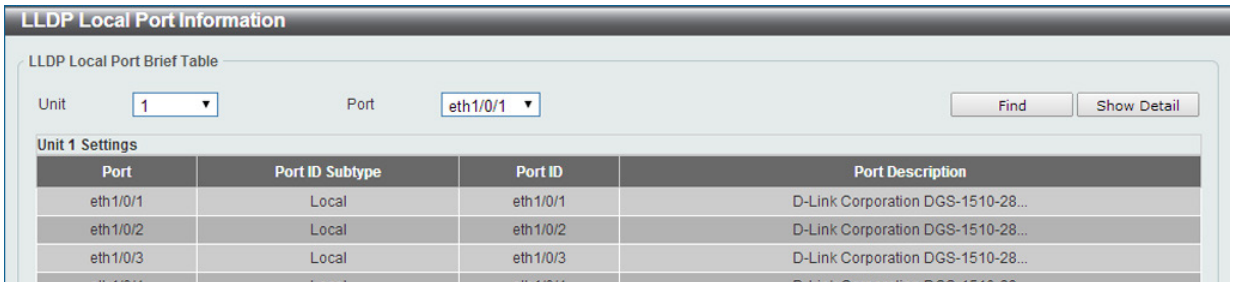


図 8-107 LLDP Local Port Information 画面

以下の項目が使用できます。

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。

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

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。

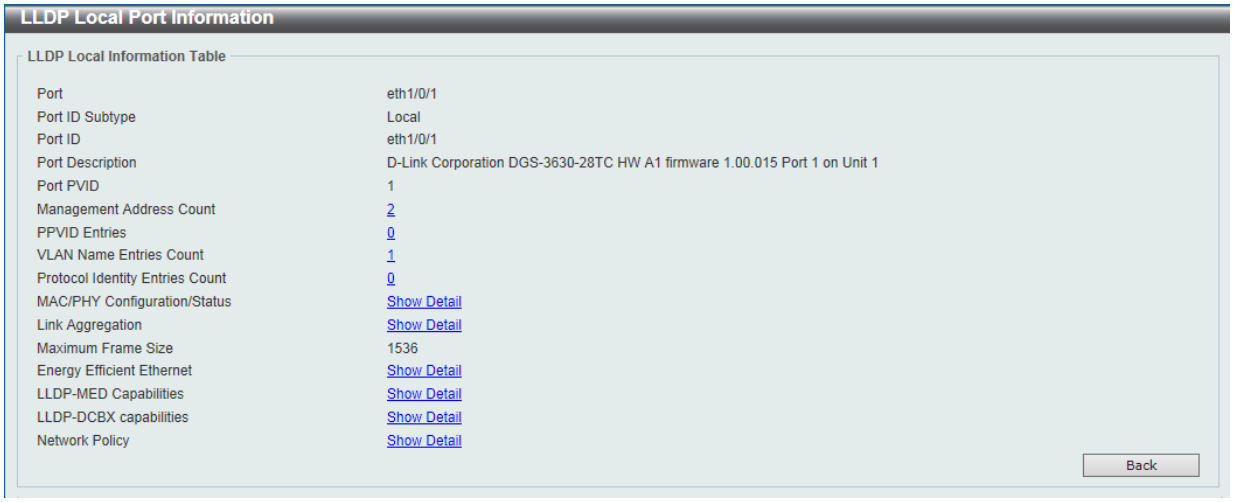


図 8-108 LLDP Local Port Information（Show Detail）画面

「MAC/PHY Configuration/Status」情報の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。

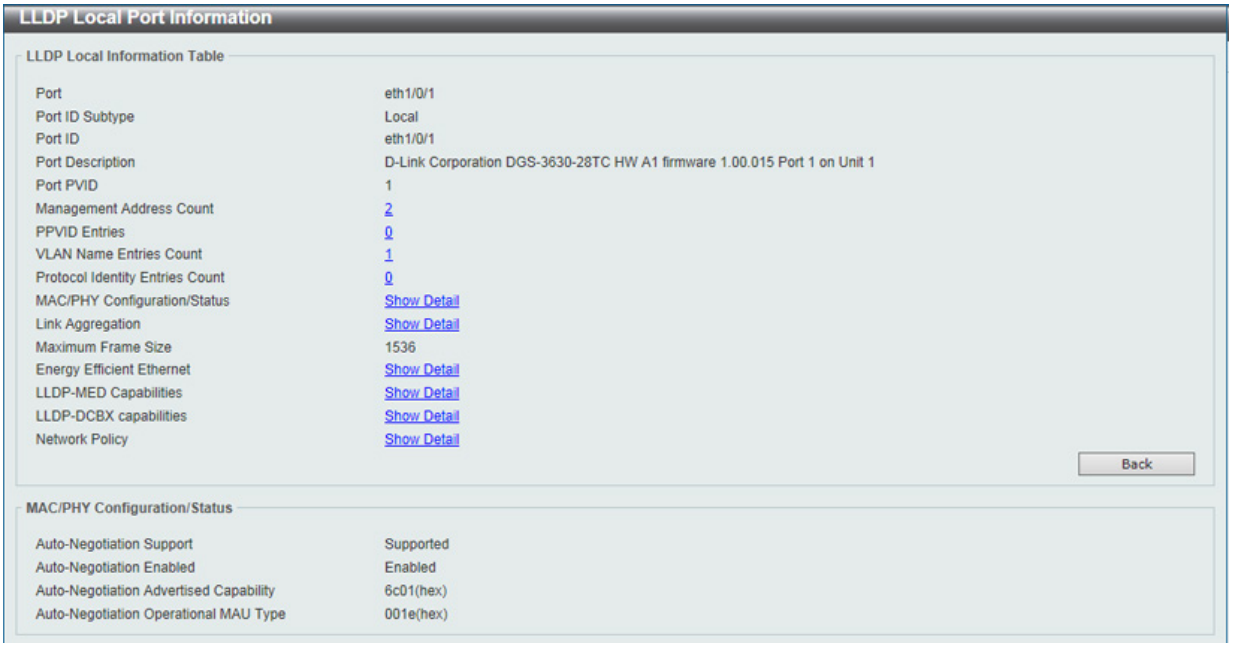


図 8-109　LLDP Local Port Information - MAC/PHY Configuration/Status 画面

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。

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。

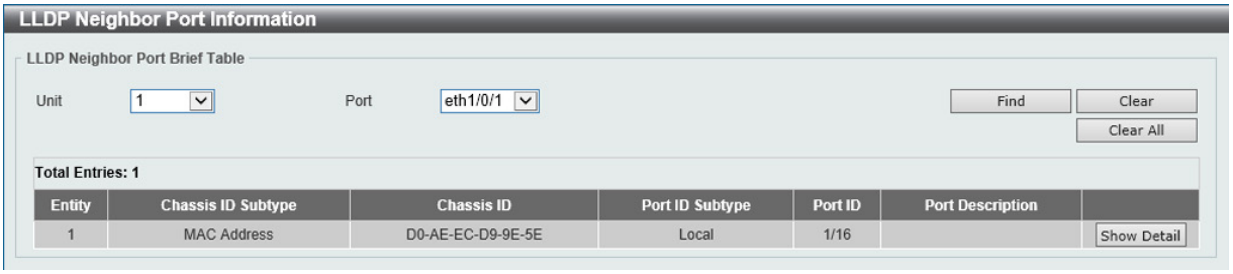


図 8-110　LLDP Neighbor Port Information 画面

以下の項目が使用できます。

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。

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

「Clear」をクリックしてポート情報をクリアします。

「Clear All」をクリックして全てのポート情報をクリアします。

「Show Detail」をクリックして指定ポート詳細情報を表示します。

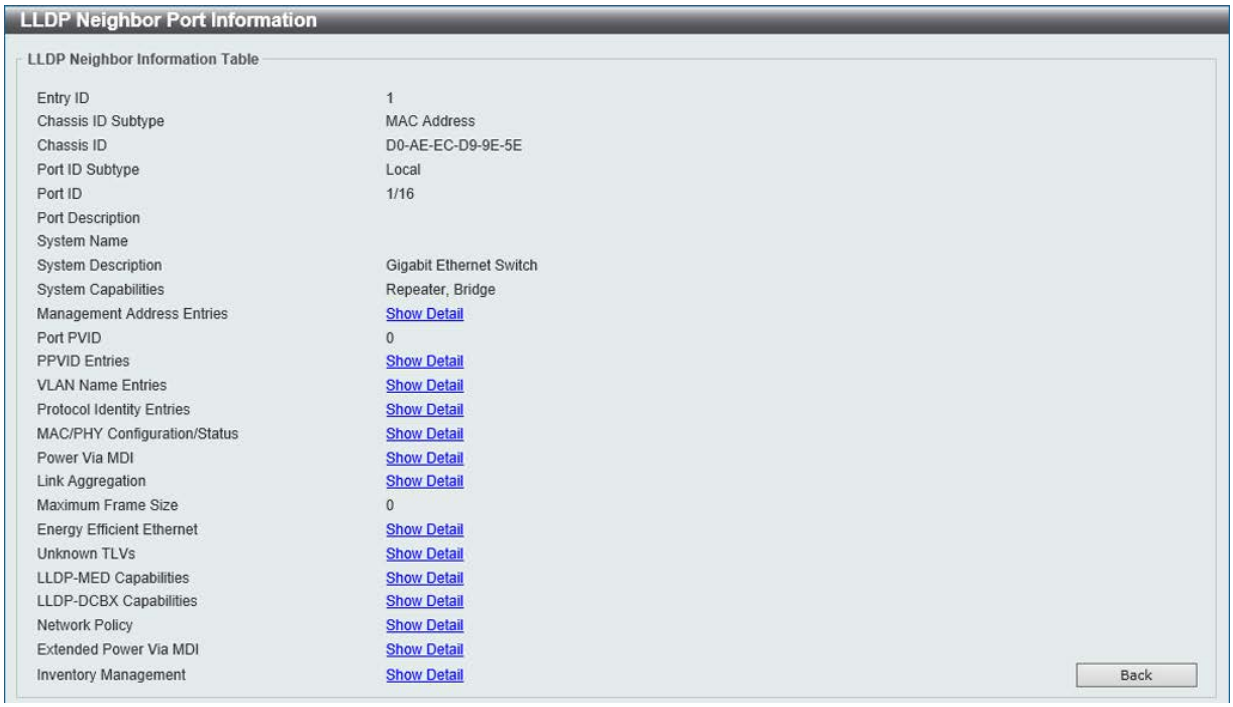


図 8-111　LLDP Neighbor Port Information（Show Detail）画面

表示された項目の「Show Detail」をクリックすると、当該項目についての詳細情報を表示します。（例 :MAC/PHY Configuration/Status）

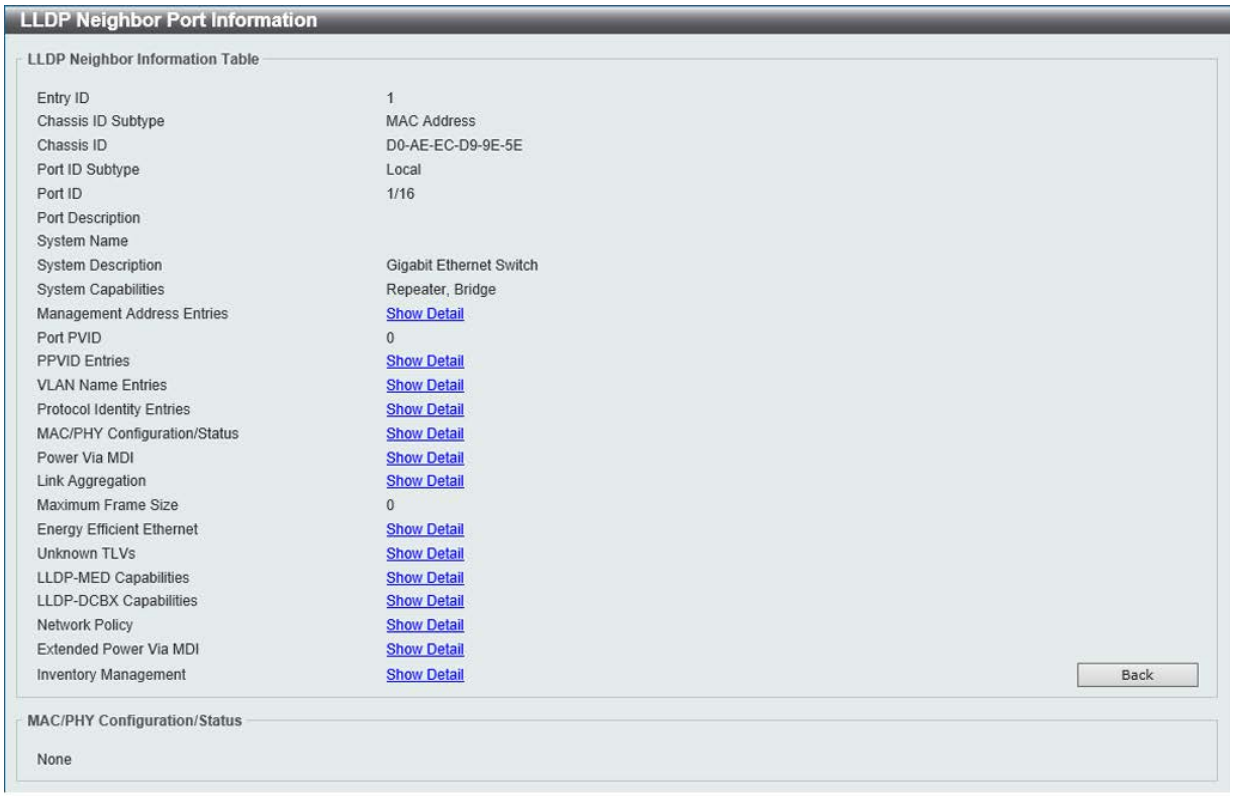


図 8-112　LLDP Neighbor Port Information（Show Detail - MAC/PHY Configuration/Status）画面

「Back」ボタンをクリックし前画面に戻ります。

第 9 章　L3 Features（レイヤ 3 機能の設定）

L3 Features メニューを使用し、本スイッチにレイヤ 3 機能を設定することができます。

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

サブメニュー	説明
ARP（ARP 設定）	ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
Gratuitous ARP（Gratuitous ARP 設定）	Gratuitous ARP として知られている ARP 通知は、TAP と SPA が等しい場合、それを送信したホストに有効である SHA と SPA を含むパケット（通常 ARP リクエスト）です
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 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 Static Route BFD（IPv4 スタティックルート BFD）	IPv4 スタティックルート BFD（Bidirectional Forwarding Detection）の設定を行います。
IPv4 Route Table（IPv4 ルートテーブル）	IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定）	IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。
IPv6 Static Route BFD（IPv6 スタティックルート BFD）	IPv6 スタティックルート BFD（Bidirectional Forwarding Detection）の設定を行います。
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。小さい優先度値を持つルートほど高いプライオリティを持ちます。
ECMP Settings（ECMP 設定）	ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。
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。
IP Tunnel Settings（IP トンネル設定）	IP トンネルを設定します。
URPF Settings（URPF 設定）	「Unicast Reverse Path Forwarding」(URPF) の設定と表示を行います。
VRF（Virtual Routing and Forwarding）	「Virtual Routing and Forwarding」(VRF) 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）をサポートしています。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。
BGP（Border Gateway Protocol）	BGP（Border Gateway Protocol）をサポートしています。これは AS（自律システム）内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブルを保持するレイヤ 3 ユニキャストルーティングプロトコルです。
BFD（Bidirectional Forwarding Detection）	Bidirectional Forwarding Detection (BFD) の設定を行います。
ISIS（Intermediate System to Intermediate System）	Intermediate System to Intermediate System (ISIS) の設定を行います。
IP Route Filter（IP ルートフィルタ）	IP プレフィックスリスト、ルートマップの作成、またはルートマップへのシーケンスの追加、およびシーケンスの削除を行います。
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。

ARP（ARP 設定）

L3 Features > ARP

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値にあります。

L3 Features > ARP > ARP Elevation

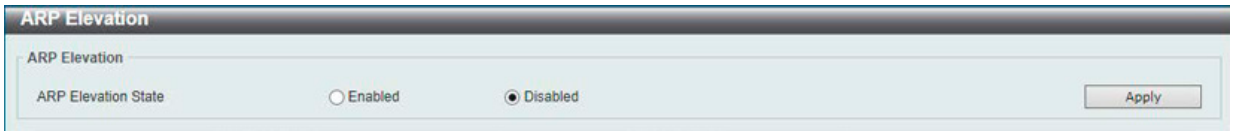


図 9-1　ARP Elevation 画面

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 / 無効に指定します。

「Apply」をクリックし、設定内容を適用します。

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を使用します。

項目	説明
Timeout	ARP テーブルエントリのリクエストから、エントリを保持する時間（分）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。初期値は 20 分です。

ARP エージングタイムの編集

1. 編集するエントリの「Edit」ボタンをクリックします。
2. 「ARP Aging Time」を設定します。
3. 「Apply」ボタンをクリックします。

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

Static ARP（スタティック 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する TCP/IP プロトコルです。ここでは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。
スタティックエントリを ARP テーブルに定義します。スタティックエントリを定義する場合、継続的なエントリを入力し、IP アドレスを MAC アドレスに変換するために使用します。以下の手順で ARP 情報を定義します。

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

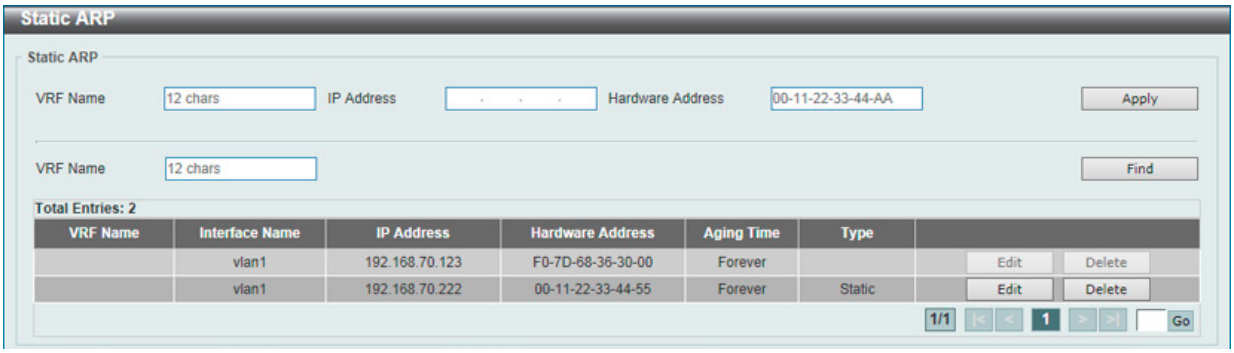


図 9-3　Static ARP 画面

以下の項目が表示されます。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
ARP Aging Time (0-65535)	ARP エントリのエージングタイム（分）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。範囲は 0-65535（分）です。初期値は 20（分）です。
IP Address	MAC アドレスとスタティックに結びつける IP アドレスを設定します。
Hardware Address	ARP テーブルで IP アドレスとスタティックに結びつける MAC アドレスを設定します。
VRF Name	検索する VRF インスタンス名を 12 字以内で入力します。「Find」をクリックし VRF を検出します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

ARP Force Aging IP Address（ARP 強制エージアウト設定）

「ARP Force Aging IP Address」ではネクストホップルートエントリにアサインされている ARP エントリを VRF と IP アドレスで指定し、手動でエージアウトさせます。

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

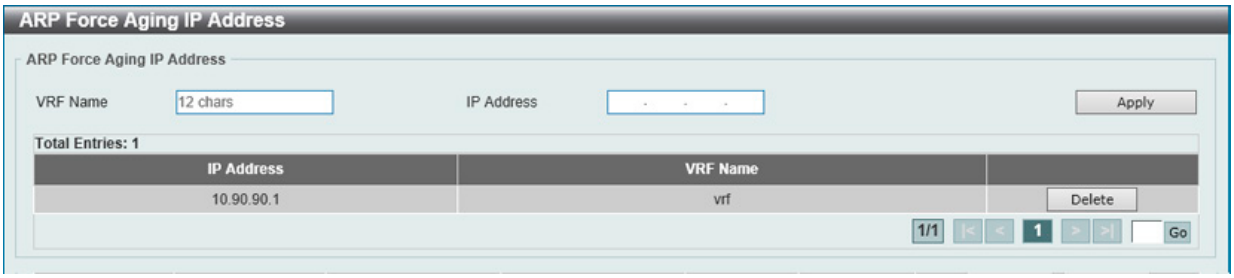


図 9-4　ARP Force Aging IP Address 画面

以下の項目が表示されます。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で指定します。
IP Address	手動でエージアウトさせる ARP エントリの IP アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

プロキシ ARP 機能は、別の機器に対し IP/MAC アドレスを見せかけて送信される ARP リクエストに対して、スイッチが本来の ARP 回答元として返答します。従って、スタティックのルーティングやデフォルトゲートウェイを設定せずに、目的の宛先にパケットをルートすることが可能です。ホスト（通常レイヤ 3 スイッチ）は別の機器に送信されたパケットに応答します。例えばホスト A と B が異なる物理ネットワークに属している場合、B は A からの ARP ブロードキャストリクエストを受信も応答もしません。しかし、A の物理ネットワークがルータまたはレイヤ 3 スイッチを介して B に接続されると、ルータまたはレイヤ 3 スイッチは A からの ARP リクエストを参照することが可能です。ローカルプロキシ ARP 機能は送信元 IP アドレスと宛先 IP アドレスが同じ場合、スイッチがプロキシ ARP に応答することを許可します。

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。

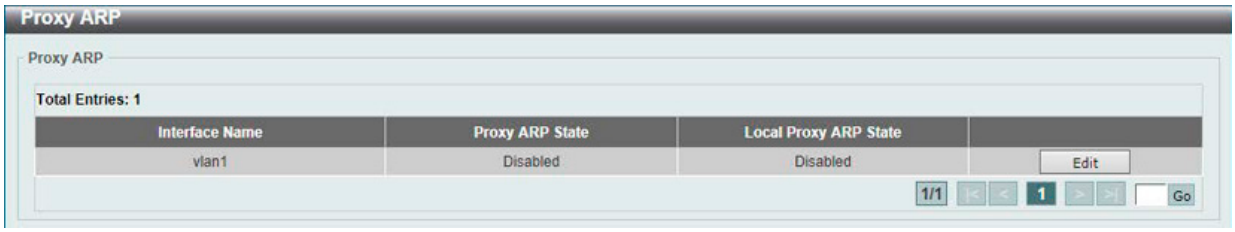


図 9-5　Proxy ARP 画面

以下の項目を使用します。

項目	説明
Proxy ARP State	プロキシ ARP を有効 / 無効にします。
Local Proxy ARP State	ローカルプロキシ ARP を有効 / 無効にします。 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。

設定を変更する際は、必ず「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

1. 編集するエントリの「Edit」ボタンをクリックします。
2. 指定エントリを編集して、IP インタフェースのプロキシ ARP の状態を選択します。
3. 「Apply」ボタンをクリックします。

初期値では「Proxy ARP」「Local Proxy ARP State」の両方とも無効になります。

ARP Table（ARP テーブルの参照）

スイッチ上の現在の ARP エントリを表示します。

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。

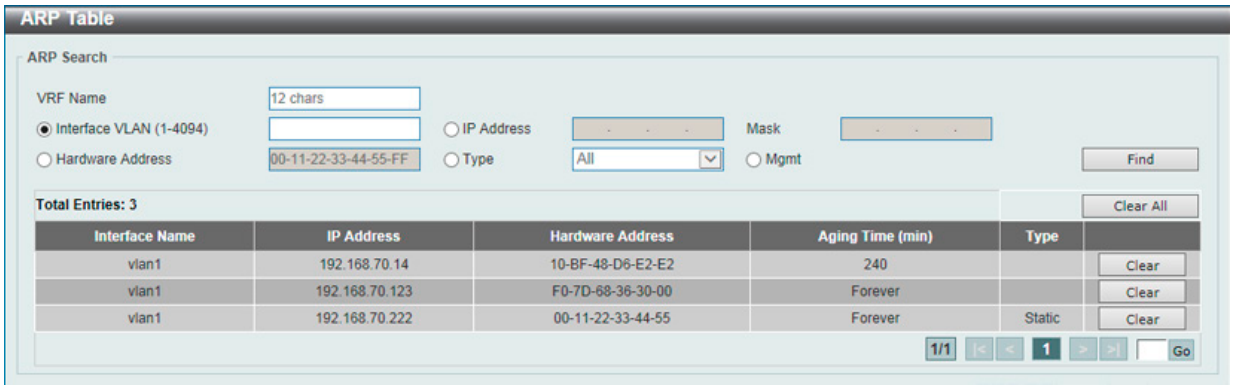


図 9-6　ARP Table 画面

設定には以下の項目を使用します。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Interface VLAN	表示するインタフェースの VLAN ID を入力します。1 から 4094 で指定できます。
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。「All」「Dynamic」から指定できます。

項目	説明
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入力した情報に基づく指定のエントリを検索します。
「Clear All」ボタンをクリックするとテーブル上のエントリが全て消去されます。
削除するエントリの「Delete」ボタンをクリックするとエントリが削除されます。

Gratuitous ARP（Gratuitous ARP 設定）

Gratuitous ARP として知られている ARP 通知は、TAP と SPA が等しい場合、それを送信したホストに有効である SHA と SPA を含むパケット（通常 ARP リクエスト）です。このリクエストは、応答を求めることを意図されたものでなく、パケットを受信する他のホストの ARP キャッシュを更新しません。

本機能は、起動時に多くのオペレーティングシステムで一般的に行われています。これは、ネットワークカードの変更により、MAC アドレスに対する IP アドレスのマッピングが変更になっていても、他のホストがまだその ARP キャッシュに古いマップを持っているというような問題が発生した場合に、その問題を解決します。

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。

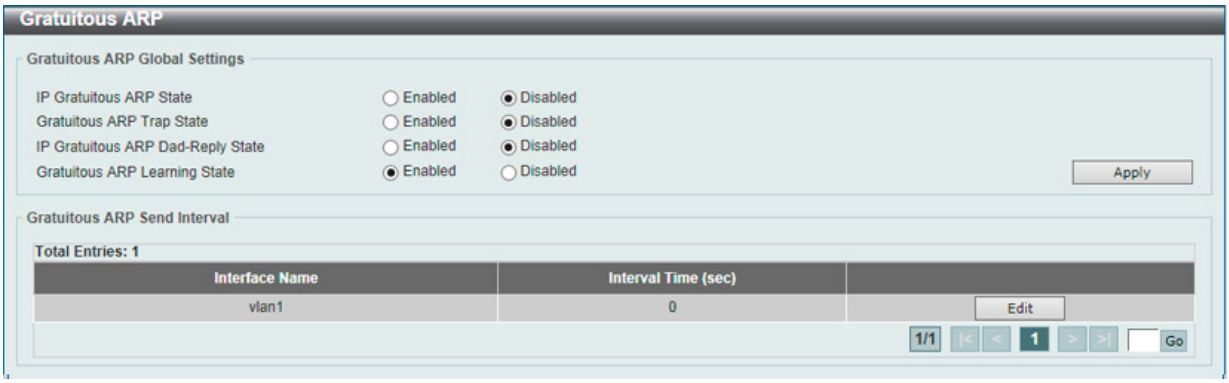


図 9-7　Gratuitous ARP 画面

設定には以下の項目を使用します。

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 / 無効にします。
Gratuitous ARP Trap State	Gratuitous ARP トラップ を有効 / 無効にします。
IP Gratuitous ARP Dad-Reply State	IP Gratuitous ARP Dad-reply を有効 / 無効にします。
Gratuitous ARP Learning State	受信した Gratuitous ARP パケットに基づいて、ARP キャッシュの更新を有効または無効にします。スイッチが ARP テーブルに Gratuitous ARP パケットと送信元の IP アドレスを受信すると、ARP エントリを更新する必要があります。初期値は「Disabled」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。

「Edit」をクリックして指定エントリを再編集します。以下の項目を使用して設定します。

項目	説明
Gratuitous ARP Send Interval	
Interval Time(sec)	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。初期値は 0(秒) です。

「Gratuitous ARP Global Settings」セクションにある「Apply」ボタンをクリックしてこのセクションで行った変更を適用します。
「Gratuitous ARP Send Interval」セクションにある「Apply」ボタンをクリックして行った変更を適用します。

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。

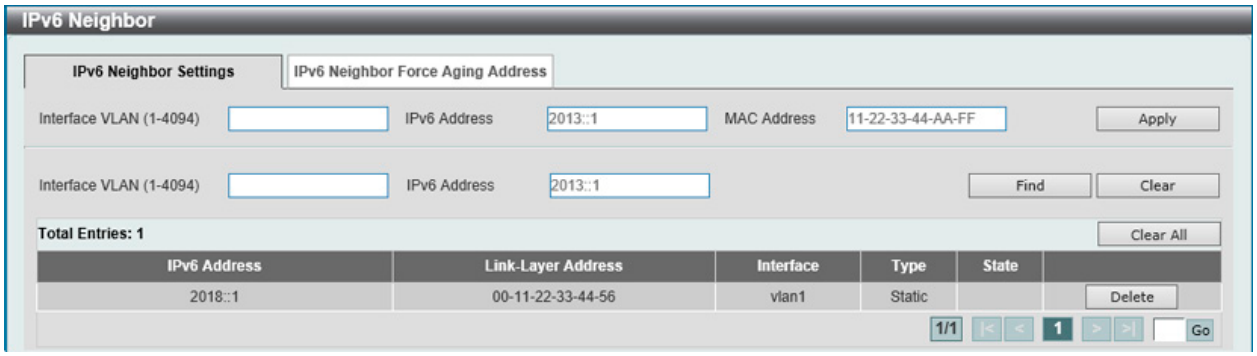


図 9-8　IPv6 Neighbor 画面

「IPv6 Neighbor Settings」タブには次の項目があります。

項目	説明
Interface VLAN	IPv6 Neighbor のインタフェース VLAN（1-4094）を指定します。
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 の新規登録

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。

エントリの検索

画面中央の「Interface VLAN」、「IPv6 Address」を入力し「Find」ボタンをクリックします。

検索結果の削除

検索結果を削除するには、「Clear」、表示されているすべてのエントリを削除するには、「Clear All」ボタンをクリックします。

エントリの削除

該当エントリの「Delete」ボタンをクリックします。

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

「IPv6 Neighbor Force Aging Address」タブをクリックすると次の画面が表示されます。

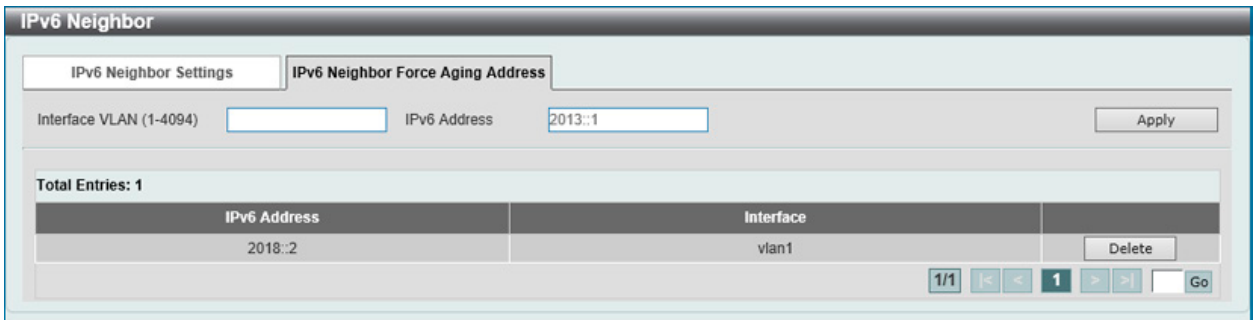


図 9-9　IPv6 Neighbor Force Aging Address 画面

「IPv6 Neighbor Force Aging Address」タブには次の項目があります。

項目	説明
Interface VLAN	IPv6 Neighbor のインタフェース VLAN（1-4094）を指定します。
IPv6 Address	強制的にエージアウトする IPv6 Neighbor キャッシュエントリの IPv6 アドレスを入力します。

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

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 9-10　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。1 から 4094 までで入力可能です。

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。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」ボタンをクリックして、指定エントリを削除します。

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

指定エントリの「Edit」ボタンをクリックして以下の画面を表示します。

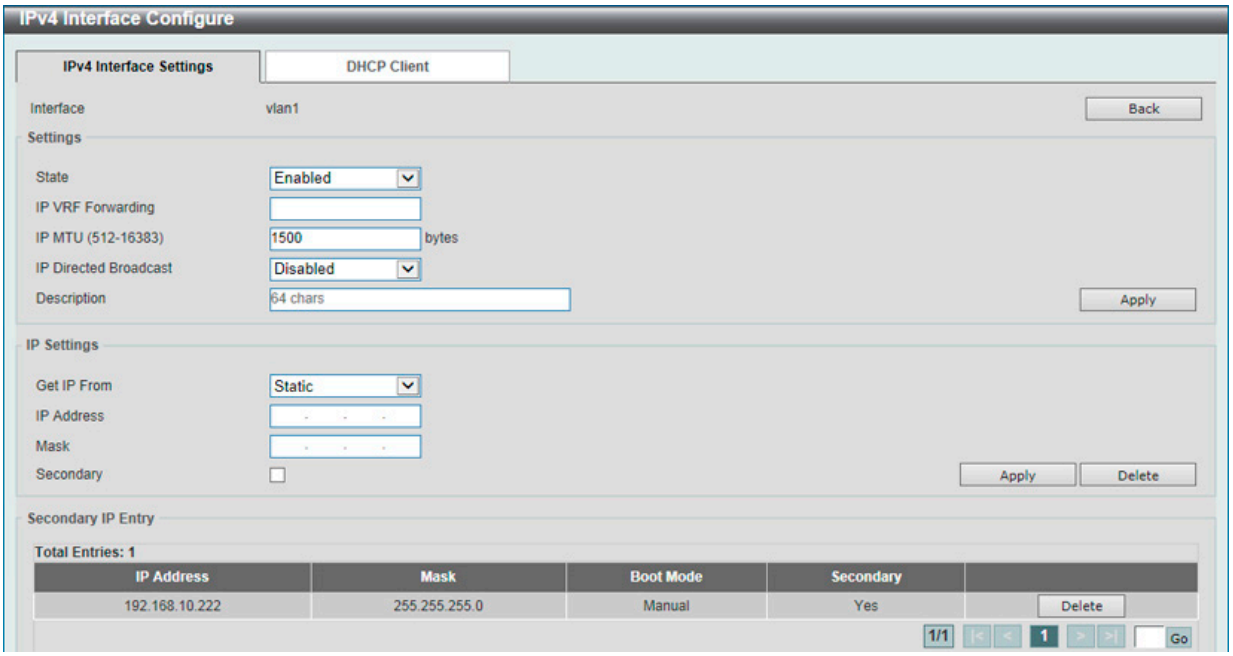


図 9-11　IPv4 Interface (Edit) 画面

以下の項目を使用して設定を行います。

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 VRF Forwarding	転送される VRF インスタンス名を 12 字以内で入力します。
IP MTU	使用する IP レイヤの MTU 値を入力します。値は 512 to 16383（bytes）の範囲です。初期値は 1500 です。
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「Enabled」（有効）/「Disabled」（無効）にします。
Description	エントリの概要について入力（64 字以内）します。
Get IP From	IPv4 アドレス、サブネットマスク、デフォルトゲートウェイに設定する「Static」「DHCP」プロトコルを選択します。
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 IPv4 アドレスとマスクをセカンダリインタフェースとして設定します。

「Apply」ボタンをクリックし、設定を有効にします。
入力 / 指定した変更を破棄し前のページに戻る場合は「Back」をクリックします。
「Delete」ボタンをクリックして、指定エントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv4 インタフェースの編集（DHCP Client）

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

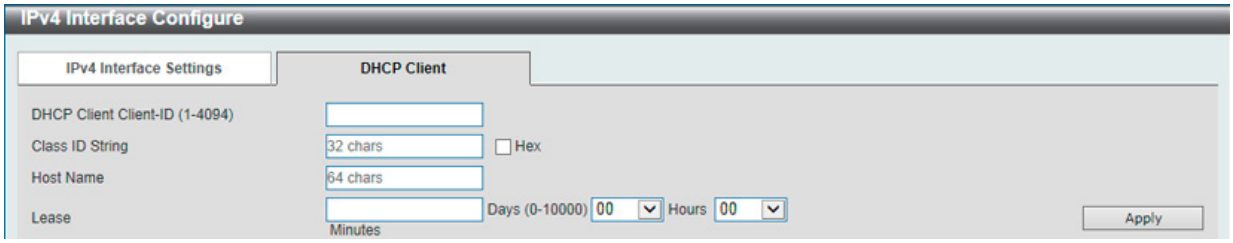


図 9-12　DHCP Client 画面

画面には以下の項目が表示されます。

項目	説明
DHCP Client Client-ID	VLAN インタフェースを入力します。この 16 進数 MAC アドレスはディスカバメッセージを送信するクライアント ID として使用されます。
Class ID String	最大 32 文字を使用してベンダクラス識別名を入力します。「Hex」にチェックを入れると 16 進数方式になります。
Host Name	ホスト名を入力します。最大 64 文字で入力可能です。ホスト名はアルファベットで始まり、アルファベットまたは数字で終わるようにします。
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。

設定を変更する際は、必ず「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 / 指定した変更を破棄し前のページに戻る場合は「Back」をクリックします。
「Delete」ボタンをクリックして、指定エントリを削除します。

IPv6 Interface（IPv6 インタフェース）

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



図 9-13　IPv6 Interface 画面

以下の項目が表示されます。（IPv6 Optimistic DAD）

項目	説明
IPv6 Optimistic DAD State	IPv6 Optimistic DAD 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。

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。1 から 4094 までで入力可能です。

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。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

指定エントリの「Show Detail」ボタンをクリックして以下の画面を表示します。

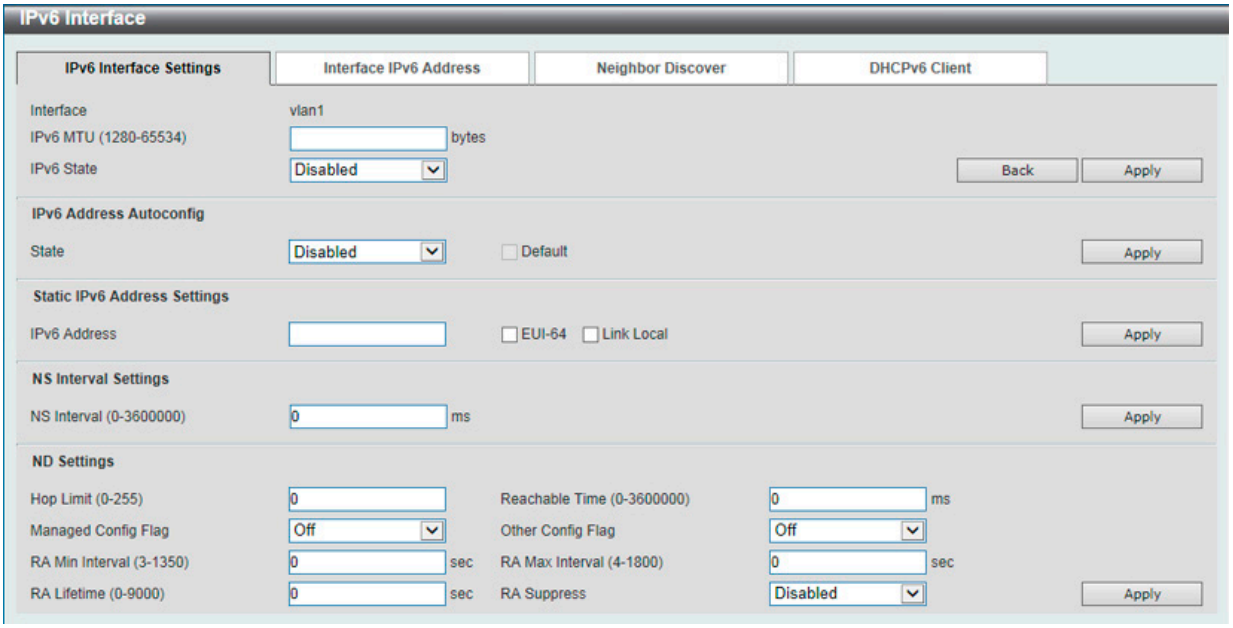


図 9-14　IPv6 Interface（IPv6 Interface Settings）画面

以下の項目を使用して設定を行います。

項目	説明
Interface	
IPv6 MTU	使用する IPv6 レイヤの MTU 値（Byte）を入力します。値は 1280 - 65534 の範囲です。初期値は 1500 です。RA メッセージ内での通知に使用されます。
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	自動設定（stateless auto-configuration）を有効 / 無効に指定します。「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。
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	NS Interval を 0 から 3600000 ミリ秒で設定します。
ND Settings	
Hop Limit (0-255)	この RA メッセージを受信するホストに送信されるパケットのために IPv6 ヘッダ内の「hop_limit」フィールドの初期値を指定します。
Reachable Time (0-3600000)	到達可能時間（0-3600000/ ミリ秒）を指定します。「0」に指定すると、ルータはインタフェースで 1200 秒使い、RA メッセージでは 0 を通知します。到達可能時間はノードが隣接しているノードを到達可能と見なすまでの時間（ミリ秒）を指定します。
Managed Config Flag	• On - この RA を受信するホストは、ステートレスアドレス設定から取得したアドレスに加え、アドレス取得のためにステートフルアドレス設定プロトコルを使用する必要があります。 • Off - アドレス取得のためにステートフルアドレス設定を使用した RA の受信を停止します。
Other Config Flag	• On - この RA を受信するホストは、ステートレスアドレス設定から取得したアドレスに加え、アドレス取得のためにステートフルアドレス設定プロトコルを使用する必要があります。 • Off - アドレス取得のためにステートフルアドレス設定を使用した RA の受信を停止します。
RA Min Interval	RA 通知が送信される最小時間（3-1350 秒）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。
RA Max Interval	RA 通知が送信される最大時間（4-1800 秒）を入力します。
RA Lifetime	RA の生存時間（0-9000 秒）を指定します。
RA Suppress	RA 通知の停止を有効 / 無効にします。

「Apply」ボタンをクリックし、設定を有効にします。

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

指定エントリの「Show Detail」ボタンをクリックして、「Interface IPv6 Address」タブを表示します。

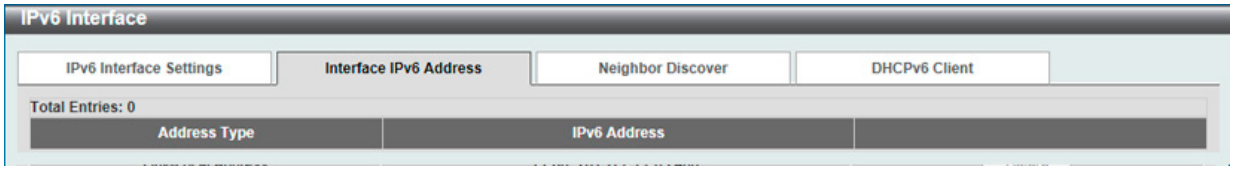


図 9-15　IPv6 Interface（Interface IPv6 Address）画面

エントリの削除

対象のエントリの「Delete」ボタンをクリックします。

IPv6 インタフェースの編集（ Neighbor Discover タブ）

指定エントリの「Show Detail」ボタンをクリックして、「Neighbor Discover」タブを表示します。



図 9-16　IPv6 Interface（Neighbor Discover）画面

IPv6 インタフェースの編集（DHCPv6 Client タブ）

指定エントリの「Show Detail」ボタンをクリックして、「DHCPv6 Client」を表示します。

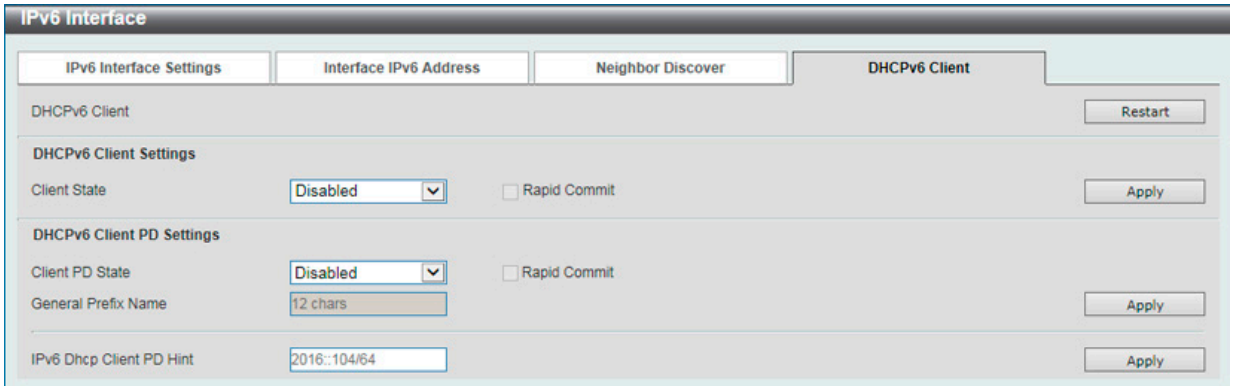


図 9-17　IPv6 Interface（DHCPv6 Client）画面

以下の項目を使用して設定を行います。

項目	説明
DHCPv6 Client	
Restart	「Restart」をクリックすると、DHCPv6 クライアントサービスを再始動します。
DHCPv6 Client Settings	
Client State	DHCPv6 クライアントを有効 / 無効に指定します。「Rapid Commit」にチェックを入れると、プリフィクス委任のメッセージ交換を実行します。
DHCPv6 Client PD Settings	
Client PD State	指定インタフェースに Prefix Delegation (PD) をリクエストする DHCPv6 クライアントプロセスを有効 / 無効に指定します。「Rapid Commit」にチェックを入れると、プリフィクス委任のメッセージ交換を実行します。
General Prefix Name	IPv6 の一般的なプリフィクス名（12 字以内）を指定します。
IPv6 DHCP Client PD Hint	メッセージに含まれる IPv6 プリフィクスのヒントを指定します。

「Apply」ボタンをクリックし、設定を有効にします。

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、それを無効または削除するまで通常アクティブな論理 IP インタフェースで、どんな物理インタフェースの状態からも独立しています。

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 9-18　Loopback Interface 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
Interface Loopback	ループバックするインタフェース ID（1-8）を入力します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

ループバックインタフェースの編集（Edit）

1. 「Edit」（編集）ボタンをクリックして、以下の画面を表示します。

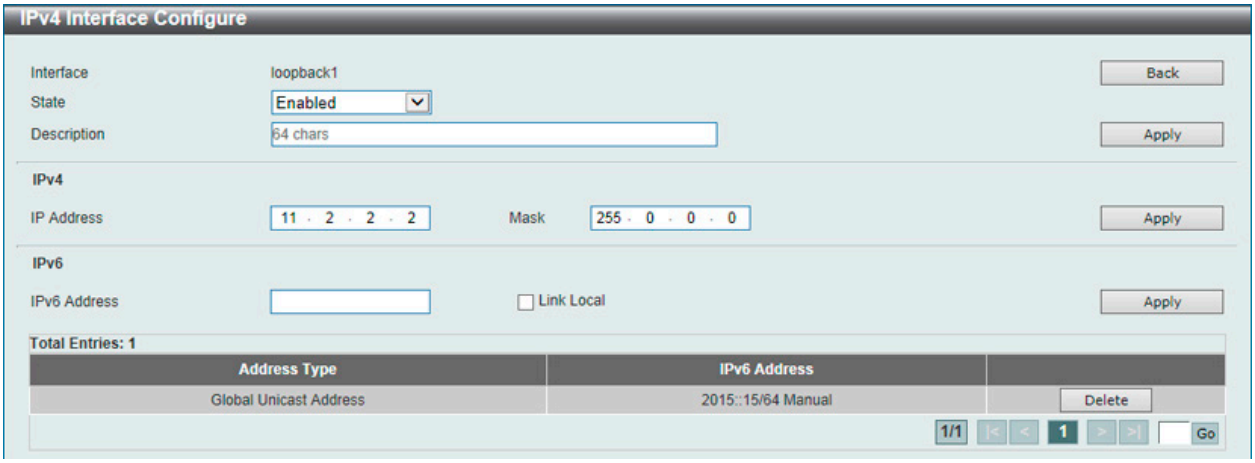


図 9-19　Loopback Interface Settings - Edit 画面

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
State	本ループバックインタフェースを有効 / 無効に指定します。
Description	本ループバックインタフェースの概要（64 字以内）を指定します。
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。

2. 該当項目を入力後、「Apply」ボタンをクリックし、設定内容を適用します。
「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。

インタフェースの削除

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

Null Interface（Null インタフェース）

Null インタフェースを設定します。

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

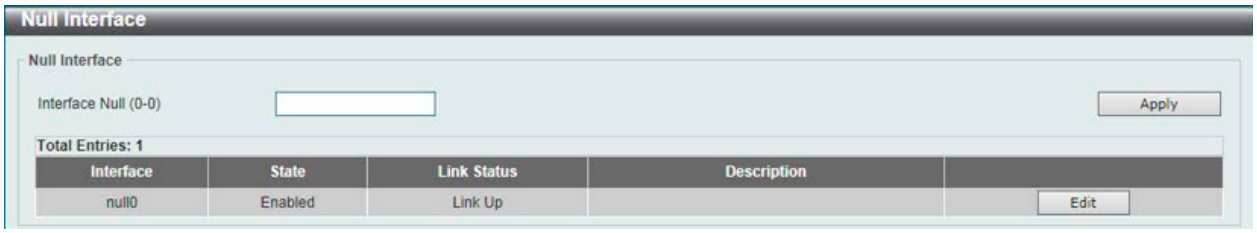


図 9-20　Null Interface 画面

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
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（64 字以内）を指定します。

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

UDP Helper（UDP ヘルパー）

L3 Features > UDP Helper
IP 転送プロトコルの設定を行います。

IP Forward Protocol（IP 転送プロトコル）

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。

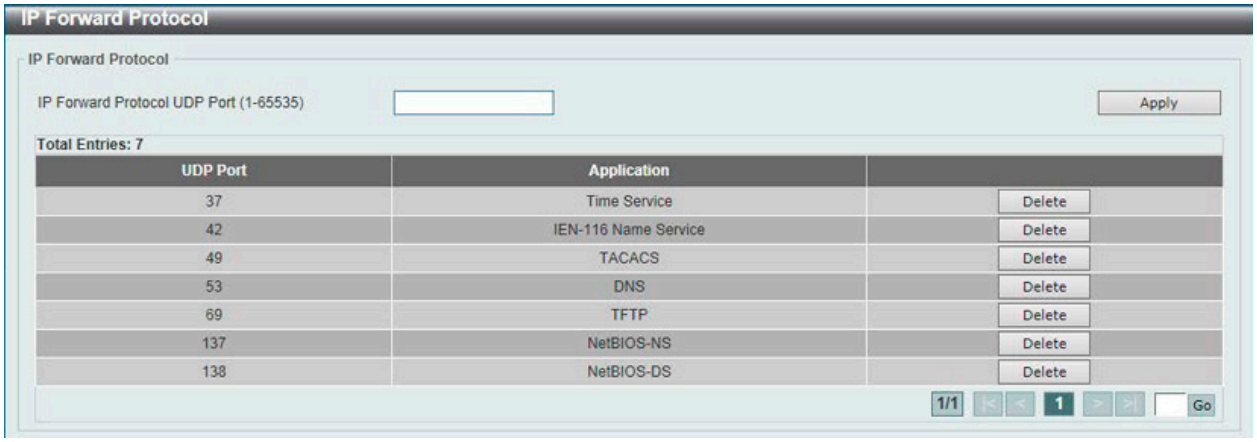


図 9-21　IP Forward Protocol 画面

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
IP Forward Protocol UDP Port	転送する UDP サービスの宛先ポート（1-65535）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IP Helper Address（IP ヘルパーアドレス）

本項目では UDP ブロードキャストパケットを転送するターゲットアドレスの追加 / 削除を指定します。本機能は IP アドレスがアサインされた受信インタフェースのみ有効です。システムは以下の制限をクリアした場合のみパケットを転送します。

- 宛先 MAC アドレスがブロードキャストアドレスである。
- 宛先 IP アドレスがオールワンブロードキャストである。
- パケットが IPv4 UDP パケットである。
- 「IP TTL 値」が「2」以上である。

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



図 9-22　IP Helper Address 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
Interface VLAN	VLAN インタフェース ID（1-4094）を指定します。
VRF State	VRF の状態を指定します。「True」「False」から指定可能です。
VRF Name	VRF インスタンス名を 12 字以内で入力します。「Global」を指定すると IP アドレスはグローバルアドレスとして指定されます。
Helper Address	UDP ブロードキャストパケットの転送のためのターゲット IPv4 アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定）

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のために、スタティックルートが一度設定されると、スイッチは設定されたネクストホップルータに ARP リクエストパケットを送信します。ARP の応答をネクストホップからスイッチが取得すると、ルートは有効になりますが、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。
また、スイッチはフローティングスタティックルートをサポートしています。これは、同じネットワークにある異なるネクストホップデバイスに代替のスタティックルートを作成できるものです。この 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リンクアップし、アクティブな状態になります。本スイッチのフォワーディングテーブル内へのエントリは IP アドレスのサブネットマスクとゲートウェイの両方を使用して行います。

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。

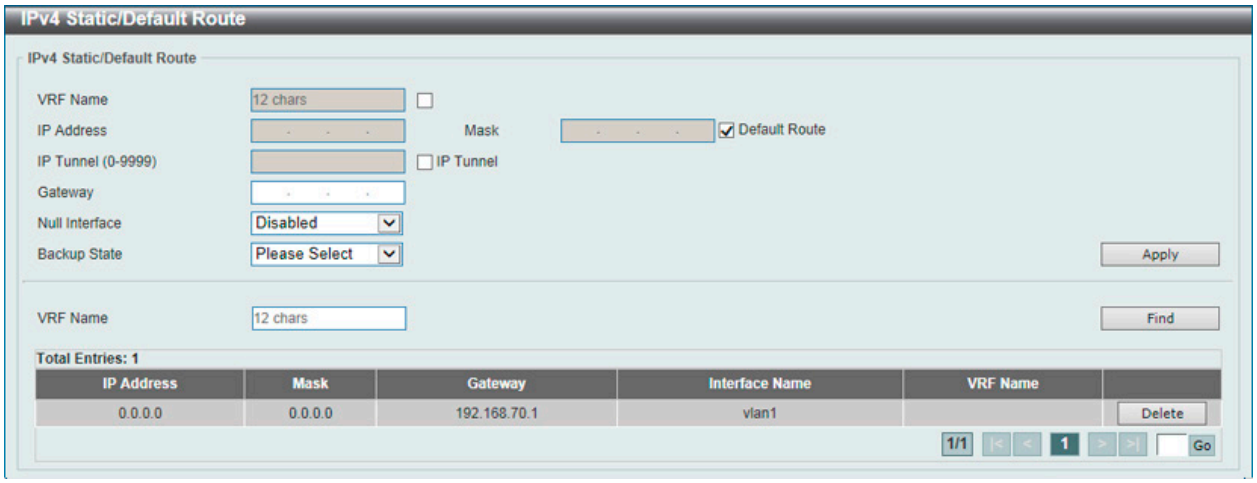


図 9-23　IPv4 Static/Default Route 画面

画面には以下の項目が表示されます。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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、デフォルトルートに割り当てられます。
Mask	対応するサブネットマスクを入力します。
IP Tunnel	IP トンネル ID（0-9999）を指定します。
Gateway	対応するゲートウェイ IP アドレスを入力します。
Null Interface	ネクストホップとして Null インタフェースを有効または無効にします。Null インタフェースはトラフィックをフィルタする別の方法を提供します。Null インタフェースに送信されるパケットはスイッチに破棄されます。
Backup State	Primary、Backup、または Weight から選択します。 • Primary - 宛先へのルートをプライマリルートとして指定します。 • Backup - 宛先へのルートをバックアップルートとして指定します。 • Weight -「0」以上の重みを指定しますが、最大パス数よりは小さくなります。 本数値はルーティングテーブルの指定ルートパスの複製（複数の）に使用され、これによりパスはトラフィックルーティングに当たる確率が上がります。「Weight」選択後に表示される空欄に数値（1-64）を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの削除
対象のエントリの行の「Delete」ボタンをクリックします。

IPv4 Static Route BFD（IPv4 スタティックルート BFD）

本項目では IPv4 スタティックルート BFD（Bidirectional Forwarding Detection）の設定と表示を行います。

L3 Features > IPv4 Static Route BFD の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　IPv4 Static Route BFD 画面

画面には以下の項目が表示されます。

項目	説明
Interface Name	BFD セッションを作成するインタフェース名を 12 字以内で入力します。
IP Address	BFD ピアの IP アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv4 Route Table（IPv4 ルートテーブル）

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。

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。

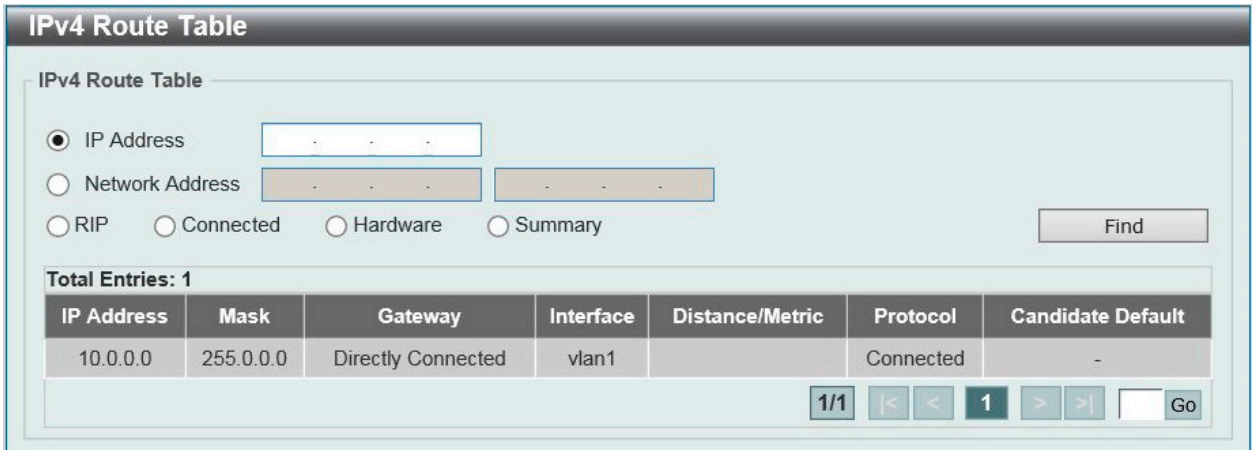


図 9-25　IPv4 Route Table 画面

画面には以下の項目が表示されます。一部項目は EI/MI モードのみに対応しています。

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 ルートだけを表示します。
OSPF	本項目を選択すると、OSPF ルートだけを表示します。
BGP	本項目を選択すると、BGP ルートだけを表示します。
ISIS	本項目を選択すると、ISIS ルートエントリを表示します。
Connected	接続中のみ機器を表示します。
Hardware	チェックを入れるとチップに記録されたルートのみ表示されます。
Summary	アクティブなルーティングエントリのサマリを表示します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定）

IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。

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。

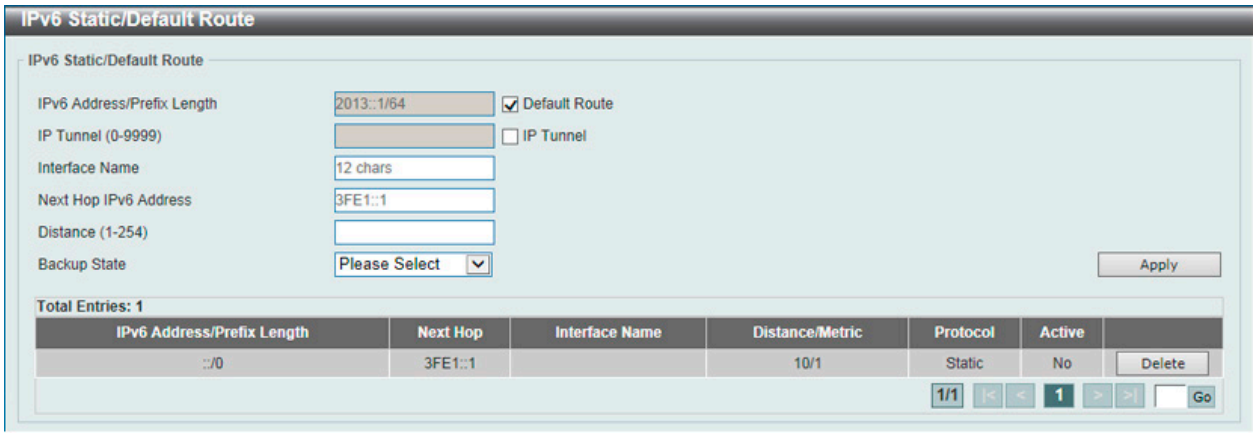


図 9-26　IPv6 Static/Default Route 画面

画面には以下の項目が表示されます。

項目	説明
IPv6 Address/Prefix Length	ルートの宛先ネットワークを入力するか、「Default」をチェックしてデフォルトルートに割り当てます。
IP Tunnel	「IP Tunnel」をチェックして、使用する IP トンネル名を入力します。
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	IPv6 形式におけるネクストホップゲートウェイアドレスに対応する IPv6 アドレスを指定します。
Distance	スタティックルートの管理ディスタンス（1-254）を指定します。低値がより良い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。
Backup State	各 IPv6 アドレスは 1 つのプライマリルートを持っており、一方、他のルートはバックアップ状態に割り当てられる必要があります。プライマリルートに障害が発生すると、スイッチはバックアップルートを試します。IPv6 が設定されるバックアップ状態を示します。「Primary」または「Backup」を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの削除

テーブル内の削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

IPv6 Static Route BFD（IPv6 スタティックルート BFD）

本項目では IPv6 スタティックルート BFD（Bidirectional Forwarding Detection）の設定と表示を行います。

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

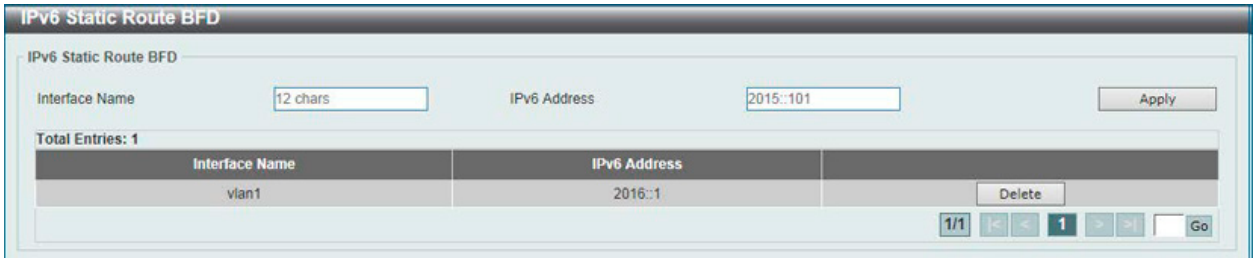


図 9-27　IPv6 Static Route BFD 画面

画面には以下の項目が表示されます。

項目	説明
Interface Name	BFD セッションを作成するインタフェース名を 12 字以内で入力します。
IPv6 Address	BFD ピアの IPv6 アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv6 Route Table（IPv6 ルートテーブル）

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 9-28　IPv6 Route Table 画面

画面には以下の項目が表示されます。一部項目は EI（または MI）モードのみに対応しています。

項目	説明
IPv6 Address	プルダウンメニューから本項目を選択し、IPv6 アドレスを入力します。
IPv6 Address/Prefix Length	プルダウンメニューから本項目を選択し、ルートの IPv6 アドレスとプ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	プルダウンメニューから本項目を選択し、表示するインタフェース名を指定します。
Connected	本項目を選択すると、接続中のみ機器を表示します。
RIPng	本項目を選択すると、RIPng ルートエントリを表示します。
OSPFv3	本項目を選択すると、OSPFv3 ルートエントリを表示します。
ISIS	本項目を選択すると、ISIS ルートエントリを表示します。
BGP	本項目を選択すると、BGP ルートだけを表示します。
Database	本項目を選択すると、ベストルートの代わりにルーティングデータベースの関連するすべてのエントリを表示します。
Hardware	本項目を選択すると、ハードウェアテーブルに記述されているルートだけを表示します。
Summary	本項目を選択すると、アクティブな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、入力した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Route Preference（ルート優先度設定）

ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。ルート信頼度レーティングを示唆するディスタンスを設定します。低いディスタンスがより高い優先値を意味します。ディスタンス 255 のルートは信頼度がないと見なされ、ルーティングパケットとしてインストールされません。

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。

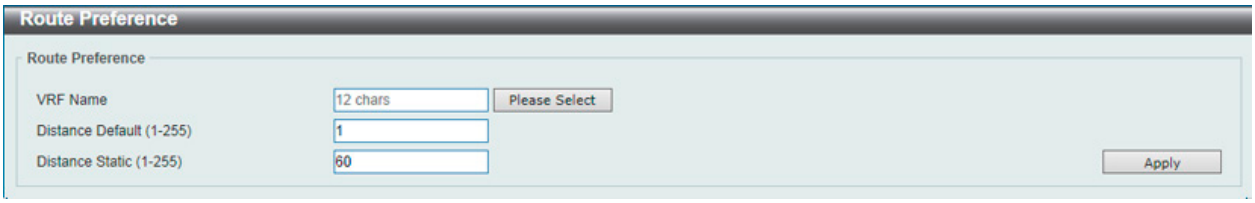


図 9-29　Route Preference 画面

以下の項目が設定、表示に使用されます。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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（1-255）します。初期値は 1 です。
Distance Static	Static 初期ルート優先度（ディスタンス）を指定（1-255）します。初期値は 60 です。

「Apply」ボタンをクリックし、設定を有効にします。

「Please Select」をクリックすると次の画面が表示されます。

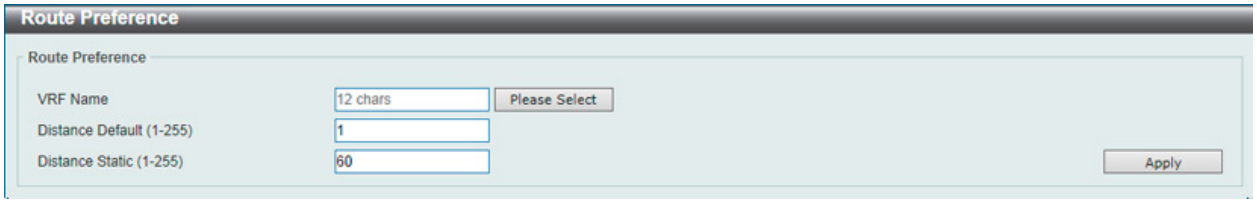


図 9-30　Route Preference（Please Select）画面

VRF エントリを選択し、「OK」ボタンをクリックして、VRF エントリを選択します。
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。

ECMP Settings（ECMP 設定）（EI/MI モードのみ）

このスイッチに ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。

L3 Features > ECMP Settings をクリックし、以下の画面を表示します。

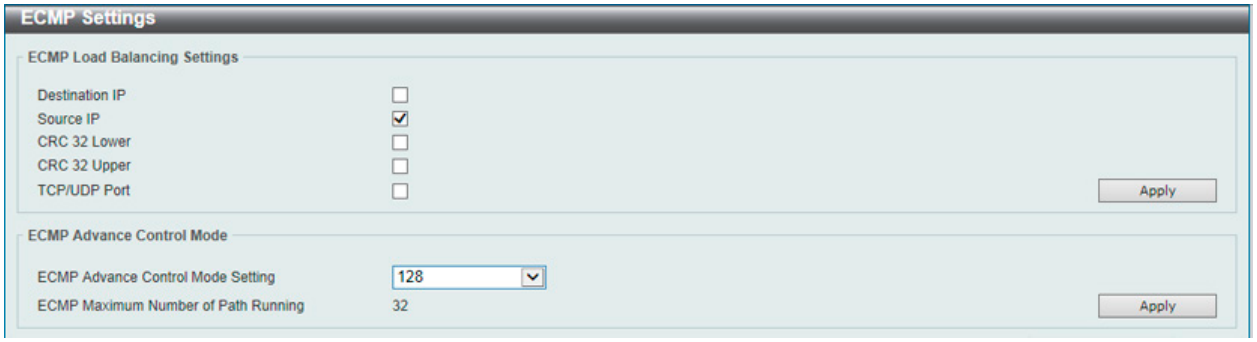


図 9-31　ECMP Settings 画面

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。本設定では ECMP とマルチパスルートの数値と各 ECMP、またはマルチパスルートのネクストホップ値を指定の値に変更、設定します。「64」「128」「256」「512」「1024」から指定します。

「Apply」ボタンをクリックして行った変更を適用します。

IPv6 General Prefix（IPv6 汎用プリフィクス）

本項目では、VLAN インタフェース IPv6 汎用プリフィクスの設定、表示を行います。

L3 Features > IPv6 General Prefix をクリックし、以下の画面を表示します。

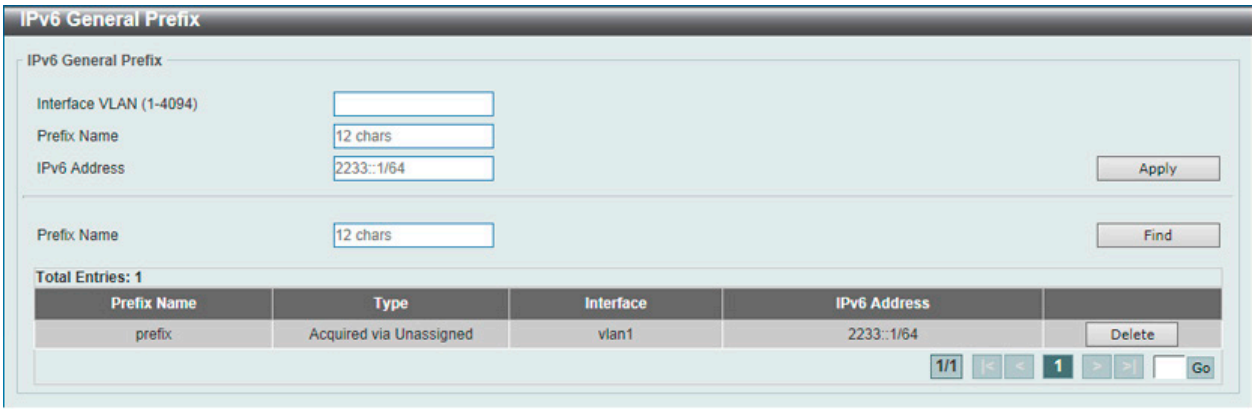


図 9-32　IPv6 General Prefix 画面

以下の項目が使用できます。

項目	説明
Interface VLAN	VLAN インタフェース ID（1-4094）を指定します。
Prefix Name	IPv6 汎用プリフィクスエントリ名（12 字以内）を指定します。
IPv6 Address	IPv6 アドレスとプリフィクス長を指定します。IPv6 アドレスのプリフィクス長は VLAN インタフェースのローカルサブネットでもあります。

「Apply」ボタンをクリックして行った変更を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IP Tunnel Settings（IP トンネル設定）

IP トンネルを設定します。

L3 Features > IP Tunnel Settings の順にメニューをクリックして以下の画面を表示します。

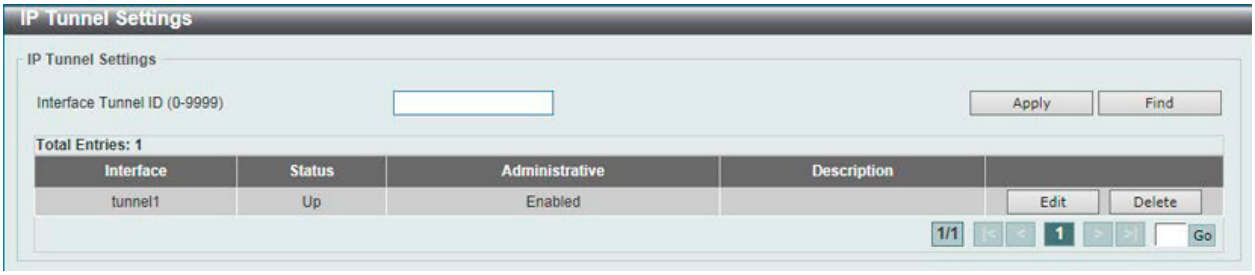


図 9-33　IP Tunnel Settings 画面

以下の項目が使用されます。

項目	説明
Interface Tunnel ID	IP トンネルのインタフェース ID（0-9999）を入力します。

エントリの登録
「Add」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。

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

エントリの削除
テーブル内の削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの編集

1. 編集するポートの「Edit」ボタンをクリックし、以下の画面を表示します。

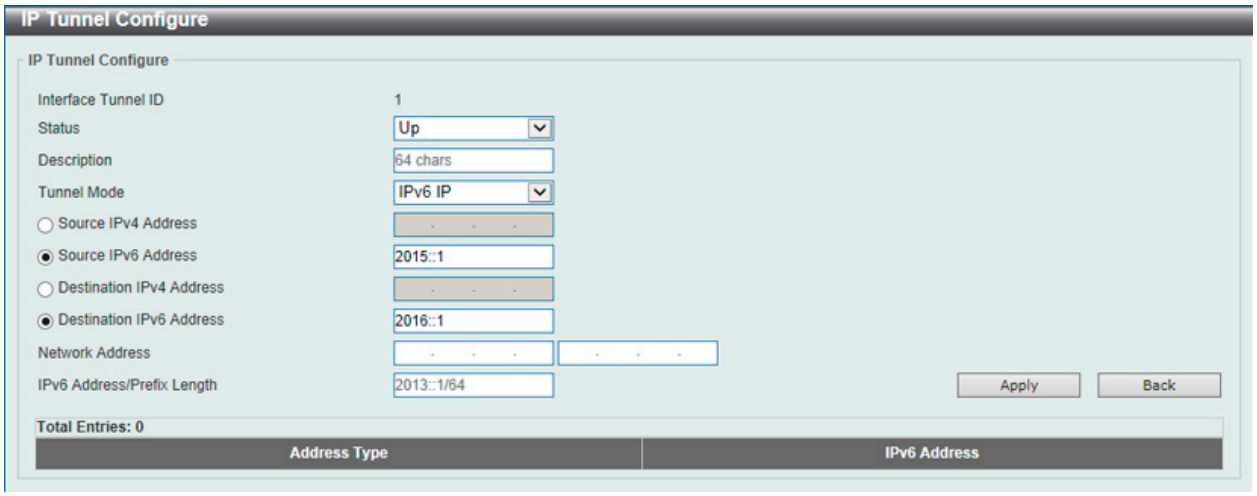


図 9-34　IP tunnel Settings - Edit 画面

以下の項目が使用されます。

項目	説明
Status	IP トンネルインタフェースの状態を「Up」「Down」から指定します。
Description	IP トンネルインタフェースの概要（64 字以内）を指定します。
Tunnel Mode	プルダウンメニューを使用してトンネルモードを選択します。「IPv6 IP」「6to4」「ISATAP」「GRE IP」「GRE IPv6」から選択します。 • IPv6 IP - IPv6 IP トンネルインタフェースとして指定します。 • 6to4 - 6to4 トンネルインタフェースとして指定します。 • ISATAP - ISATAP トンネルインタフェースとして指定します。 • GRE IP - GRE IP トンネルインタフェースとして指定します。到達プロトコルは IPv4 プロトコルです。 • GRE IPv6 - GRE IP トンネルインタフェースとして指定します。到達プロトコルは IPv6 プロトコルです。
Source IPv4/IPv6 Address	送信元 IPv4/IPv6 アドレスを指定します。
Destination IPv4/IPv6 Address	送信先 IPv4/IPv6 アドレスを指定します。
Network Address	アドレスネットワークアドレスを入力します。
IPv6 Address/Prefix Length	IPv6 アドレスネットワークアドレスとプリフィクス長を入力します。

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

「Back」をボタンをクリックして前のページに戻ります。

URPF Settings（URPF 設定）

本項目では「Unicast Reverse Path Forwarding」(URPF) の設定と表示を行います。ネットワークへの攻撃としてよくある手段に、IPv4/IPv6 送信元アドレススプーフィング発動があります。この方法として、ターゲットに知られた / 信頼された送信アドレスのネットワークにトラフィックを送信します。防御が設定されていない場合、ネットワーク組織は複数の種類の攻撃にオープンになり、トラッフィックを許可してしまいます。ユニキャスト RPF はルータを通過する不正 / 偽造 IPv4/IPv6 アドレスによって生成された問題を軽減させることができます。

L3 Features > URPF Settings の順にメニューをクリックして以下の画面を表示します。

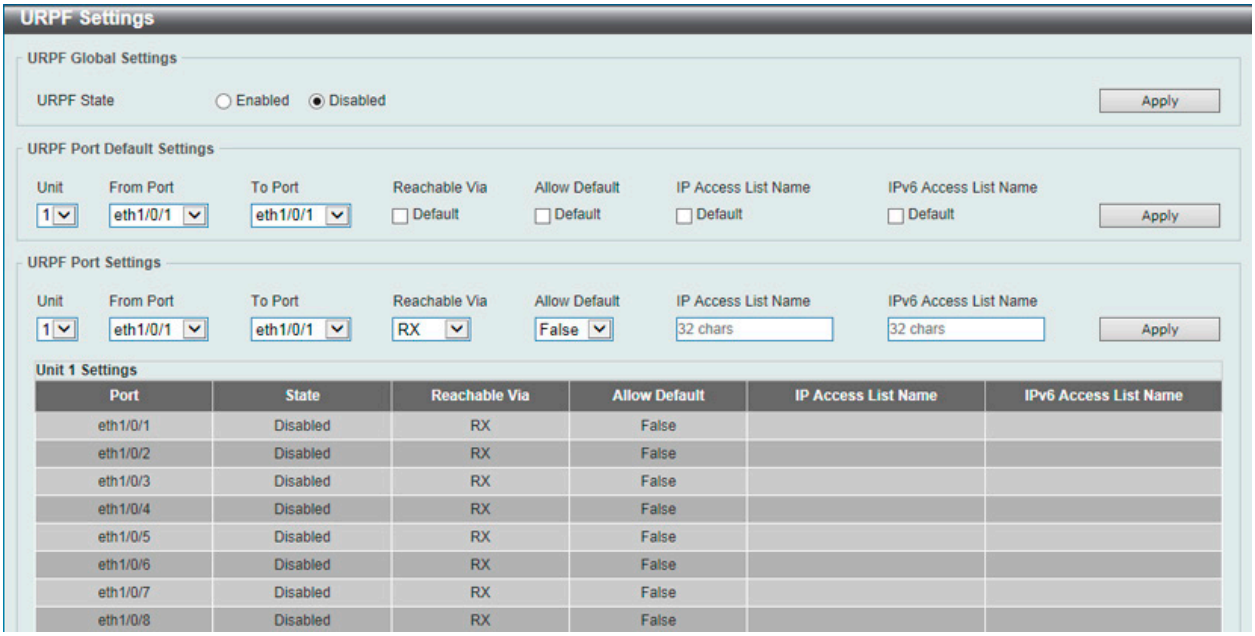


図 9-35　URPF Settings 画面

以下の項目が使用されます。

項目	説明
URPF Global Settings	
URPF State	URPF を有効 / 無効に指定します。 注意 有効になると、まずハードウェアルーティングテーブルの「Session Initiation Protocol」(SIP) を使った検出が必要になり、その後「Dynamic Inspection Protocol」(DIP) を使用します。これによりテーブルは半分に分割され、IP ルーティングテーブルは半分に削減されます。本設定はコンフィグを保存した上で、スイッチを再起動して初めて有効になります。
URPF Port Default Settings	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Reachable Via	「RX」経由の到達可能な初期設定を使用します。
Allow Default	「default allow」の初期設定を使用します。「False」を意味します。
IP Access List Name	初期設定の IP アクセスリストを使用します。
IPv6 Access List Name	初期設定の IPv6 アクセスリストを使用します。
URPF Port Default Settings	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Reachable Via	「Reachable Via」のオプションを選択します。 • Any - 送信元アドレスがルーティングテーブルに存在しているか確かめます。(loose モードとして認識されます。) • RX - 送信元アドレスがルーティングテーブルに存在しているか、また送信元とマッチする内向きインタフェースがパケットが受信するインタフェースを通して到達可能かを確かめます。
Allow Default	「Allow Default」のオプションを選択します。 • True - ユニキャスト RPF 確認の初期ルートを使用します。 • False - ユニキャスト RPF 確認の初期ルートを使用しません。
IP Access List Name	URPF チェックに使用する IP アクセスリスト名（32 字以内）を指定します。
IPv6 Access List Name	URPF チェックに使用する IPv6 アクセスリスト名（32 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。

VRF（Virtual Routing and Forwarding）（EI/MI モードのみ）

「Virtual Routing and Forwarding」(VRF) の設定を行います。

VRF Settings（VRF 設定）

本項目では「Virtual Routing and Forwarding」(VRF) の設定、表示を行います。

L3 Features > VRF > VRF Settings の順にメニューをクリックして以下の画面を表示します。



図 9-36　VRF Settings 画面

以下の項目が使用されます。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」ボタンをクリックすると、以下の画面が表示されます。

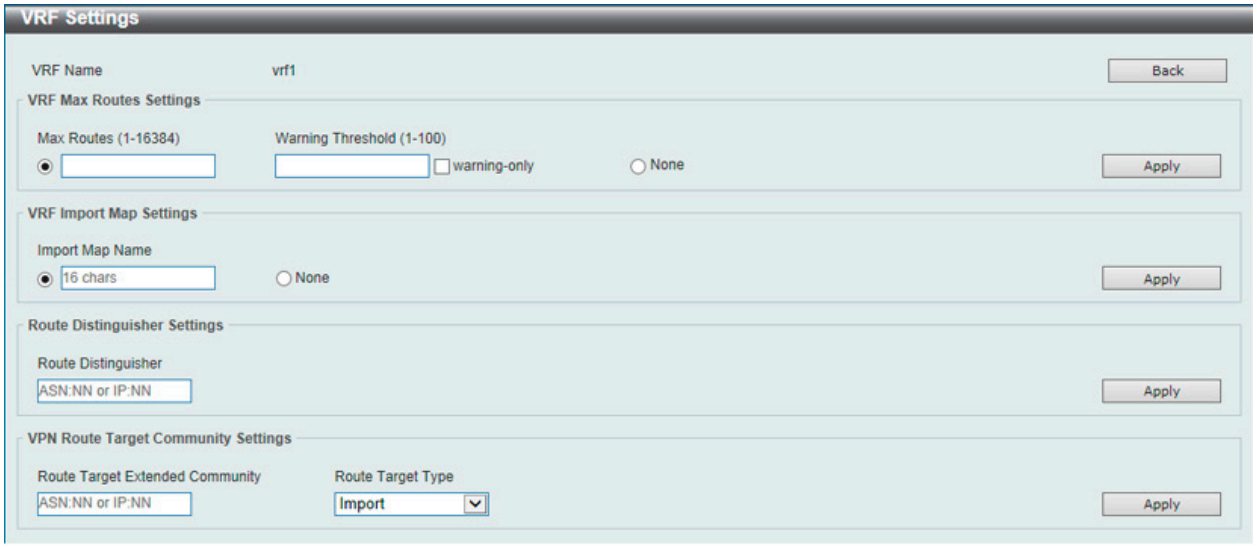


図 9-37　VRF Settings (Edit) 画面

以下の項目が使用されます。「Back」をクリックすると前のページに戻ります。

項目	説明
VRF Max Routes Settings	
Max Routes	VRF 内の最大ルート数（1-16384）を入力します。
Warning Threshold	警告しきい値を指定します。これ以上ハードウェアに記録できないルート数のしきい値に達すると通知メッセージが送信されます。1-100 パーセントで指定します。「warning-only」を指定すると、しきい値を超えると通知が発生するものの、ハードウェアへの記録は継続します。
None	制限を指定しません。
VRF Import Map Settings	
Import Map Name	VRF のインポートルートマップを指定します。
None	VRF のインポートルートマップを無効にします。

項目	説明
Route Distinguisher Settings	
Route Distinguisher	VRF の Route Distinguisher (RD) を指定します。VPN-IPv4 プリフィクスを作成する 8 バイトの値を IPv4 プリフィクス指定します。
VPN Route Target Community Settings	
Route Target Extended Community	ルートターゲットを指定します。ルートターゲットは VPN のアプリケーションです。 VRF 一つにつき複数のルートターゲットがあります。
Route Target Type	ルートターゲットの種類を指定します。 • Import - ターゲット VPN 拡張コミュニティからのインポートルーティング情報となるインポートルートを追加します。 • Export - ターゲット VPN 拡張コミュニティからのエクスポートルーティング情報となるエクスポートルートを追加します。 • Both - インポートルート / エクスポートルートどちらも追加します。

「Apply」をクリックし、設定内容を適用します。

「Show Detail」をクリックすると、以下の画面が表示されます。

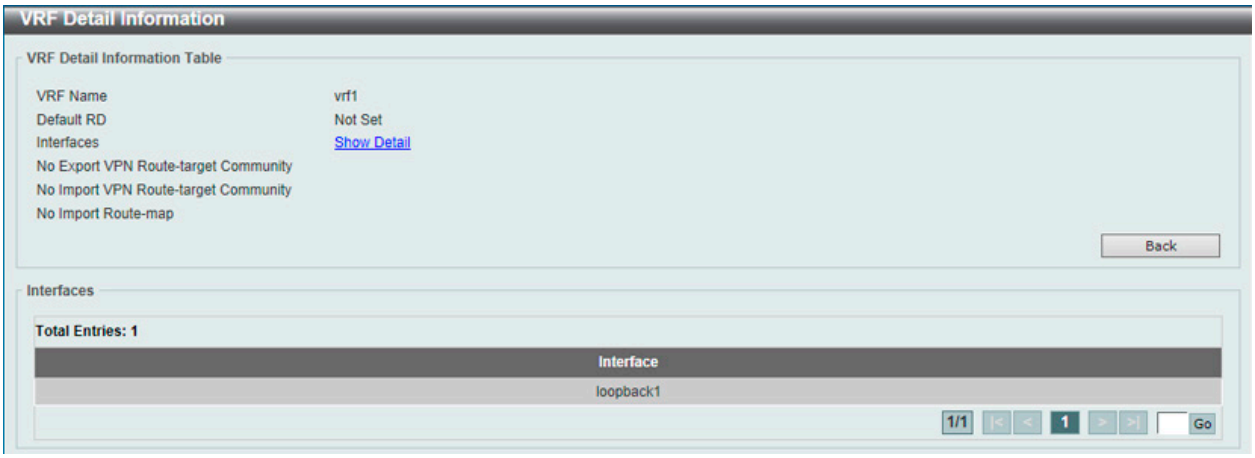


図 9-38　VRF Settings (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

VRF Interface Settings（VRF インタフェース設定）

本項目では VRF インタフェースの設定、表示を行います。

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

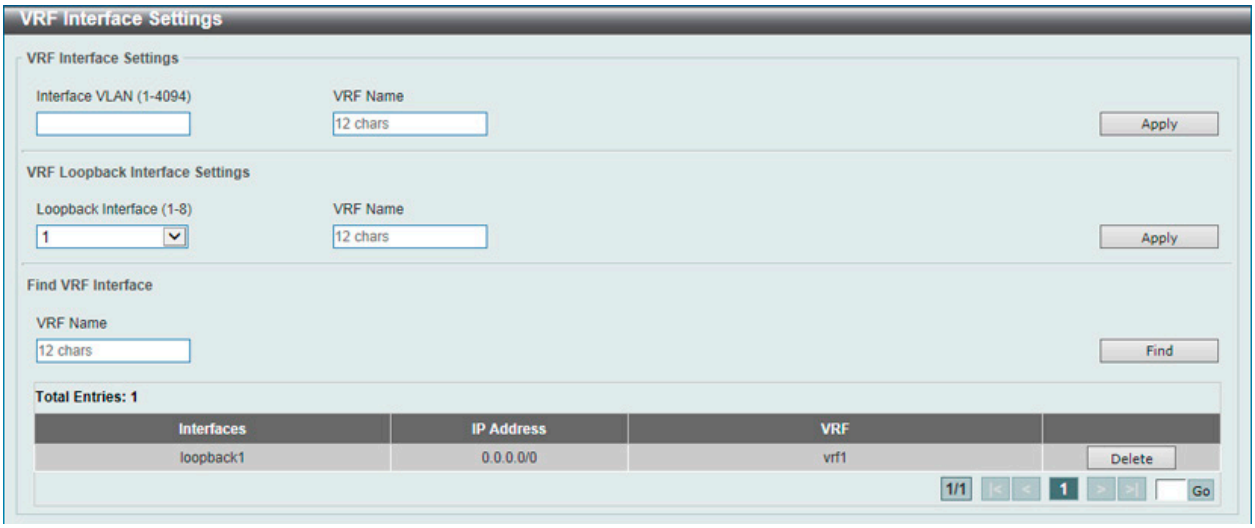


図 9-39　VRF Interface Settings 画面

以下の項目が使用されます。

項目	説明
VRF Interface Settings	
Interface VLAN	VLAN インタフェース ID（1-4094）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。

項目	説明
VRF Loopback Interface Settings	
Loopback Interface	ループバックインタフェース ID（1-8）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Find VRF Interface	
VRF Name	VRF インスタンス名を 12 字以内で入力します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
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。

RIP（Routing Information Protocol）

L3 Features > RIP
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。

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。RIPの設定を行ったインタフェースのリストが表示されます。



図 9-40　RIP Settings 画面

以下の項目があります。

項目	説明
RIP Global Settings	
RIP State	RIP の状態を有効または無効にします。初期値は無効です。
VRF Address Family Table	
VRF Name	RIP の状態を有効または無効にします。初期値は無効です。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

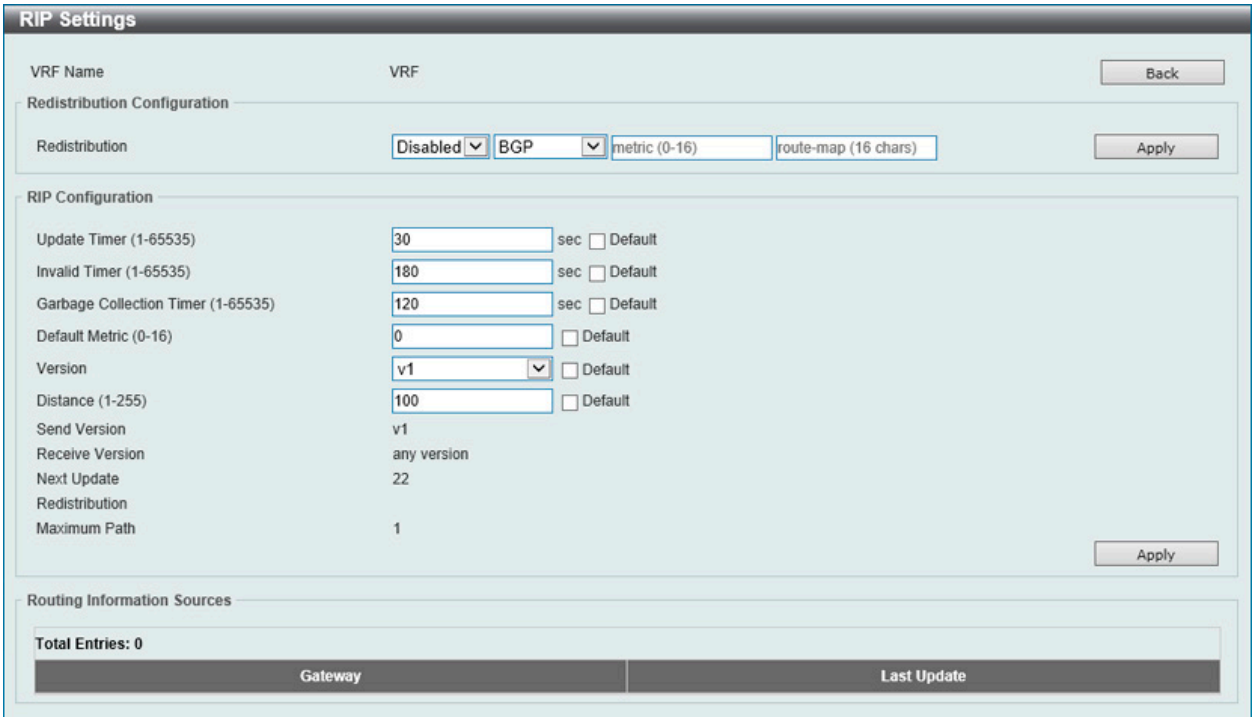


図 9-41　RIP Settings 画面 – Edit 画面

RIP インタフェースの設定に使用する項目は以下の通りです。「Back」をクリックすると前のページに戻ります。

項目	説明
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 / 無効に指定します。 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。「BGP」「Connected」「OSPF」「Static」「ISIS」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値（1-65535 秒）を入力します。「Default」を指定すると初期値の「30」を指定します。
Invalid Time	無効にする値（1-65535 秒）を入力します。「Default」を指定すると初期値の「180」を指定します。
Garbage Collection Timer	フラッシュ値（1-65535 秒）を入力します。「Default」を指定すると初期値の「120」を指定します。
Default Metric	初期メトリック値（0-16 秒）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、メトリックが同期します。「Default」を指定すると初期メトリック値（0）を指定します。
Version	全インタフェースで使用される初期バージョンとしてのグローバル RIP バージョンを指定します。「v1（RIPv1）」「v2（RIPv2）」から指定します。「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。
Distance	RIP の管理ディスタンス（1-255）を指定します。低い値ほど良いルートを意味します。「Default」を指定すると初期値である 100 を使用します。

「Apply」をクリックし、設定内容を適用します。

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。

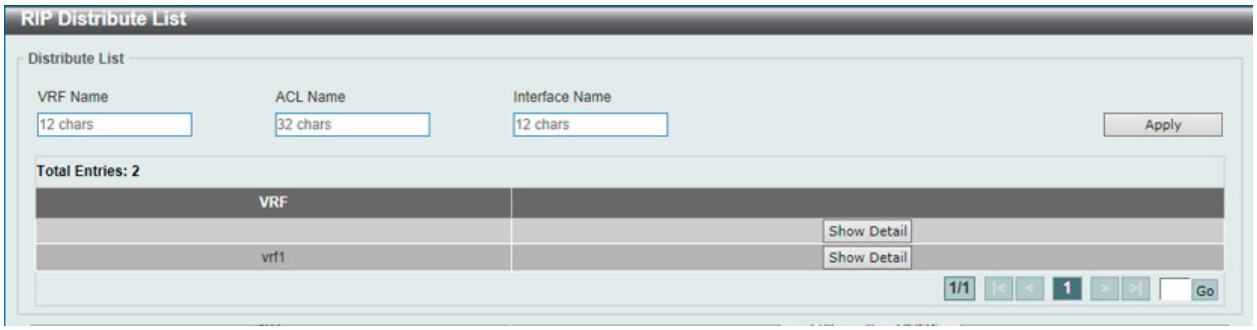


図 9-42　RIP Distribute List 画面

以下の項目があります。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
ACL Name	アクセスリスト名を 32 字以内で入力します。
Interface Name	インスタンス名を 12 字以内で入力します。

「Apply」をクリックし、設定内容を適用します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Show Detail」をクリックすると、以下の画面が表示されます。



図 9-43　RIP Distribute List (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

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。

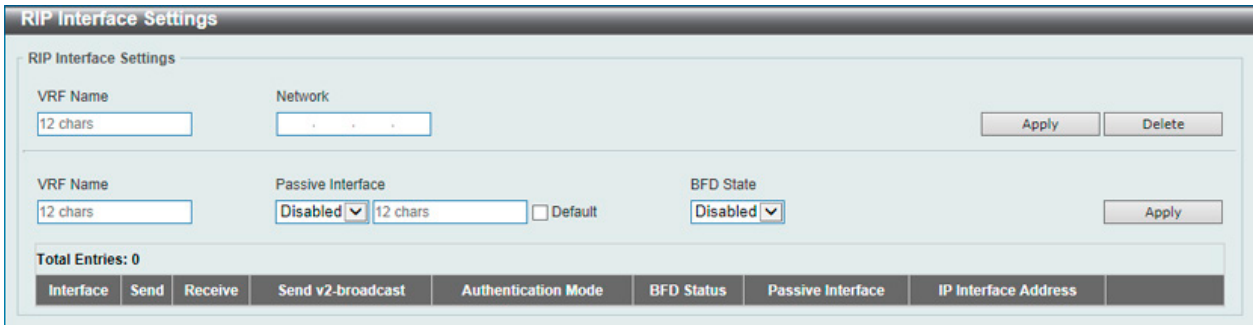


図 9-44　RIP Interface Settings 画面

以下の項目があります。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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。
Passive Interface	パッシブインタフェースを有効 / 無効に指定します。インタフェースのルーティングアップデートの送信 / 受信を無効にします。しか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 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。

項目	説明
BFD State	指定インタフェースの BFD 機能を有効 / 無効に指定します。BFD がインタフェースで有効な場合、ルータは現在のインタフェースの RIP ピアとともに BFD ピアを作成し、新しい RIP ピアが追加されると、BFD ピアが作成されます。RIP ピアが RIP 無効により削除されると、関連する BFD ピアもまた削除されます。BFD セッションが落ちると、ピアにより学習された RIP セッションもまた削除されます。

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

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。サマリアドレスは、子ルートがサマライズ（要約）されている場合、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 9-45　RIP Database 画面

以下の項目があります。

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。
VRF Name	VRF インスタンス名を 12 字以内で入力します。

「Apply」をクリックし、設定内容を適用します。
「Show All」をクリックして、すべてのエントリを表示します。

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。

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て以下の画面を表示します。

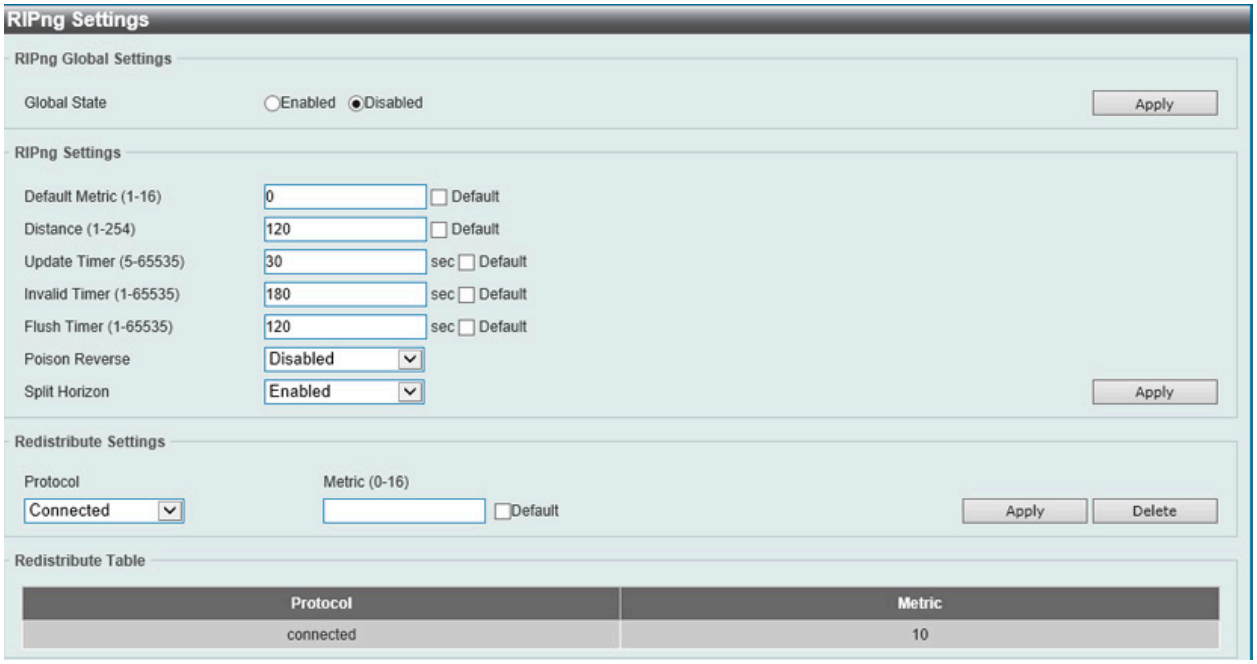


図 9-46　RIPng Settings 画面

以下の項目があります。

項目	説明
RIPng Global Settings	
Global State	RIPng の状態を有効または無効にします。初期値は無効です。
RIPng Settings	
Default Metric	初期メトリック値（1-16 秒）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。メトリックの指定により、メトリックが同期します。「Default」を指定すると初期メトリック値（0）を指定します。
Distance	RIPng の管理ディスタンス（1-254）を指定します。低い値ほど良いルートを意味します。「Default」を指定すると初期値である 120 を使用します。
Update Timer	RIP アップデートメッセージを送信する間隔値（5-65535 秒）を入力します。「Default」を指定すると初期値の「30」を指定します。
Invalid Timer	無効にする値（1-65535 秒）を入力します。「Default」を指定すると初期値の「180」を指定します。
Flush Timer	フラッシュ値（1-65535 秒）を入力します。「Default」を指定すると初期値の「120」を指定します。
Poison Reverse	「Poison Reverse」を有効 / 無効に指定します。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。
Split Horizon	「Split Horizon」を有効 / 無効に指定します。「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。「BGP」「Connected」「OSPF」「Static」「ISIS」から指定します。「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。
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（0-16）を指定します。「Default」は初期メトリック値を使用します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定の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て以下の画面を表示します。



図 9-47　RIPng Interface Settings 画面

以下の項目を使用します。

項目	説明
Interface VLAN	RIPng 設定の VLAN インタフェース名（1-4094）を入力します。「All Interface」を選択すると全インタフェースで適用します。
State	指定の VLAN インタフェースで IPv6 RIP 機能を有効 / 無効に指定します。
Metric Offset	指定インタフェースに受信する IPv6 RIP ルートのメトリックに本値（1-16）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。複数のインタフェースに受信するルートのメトリックとルートへの干渉に使用します。「Default」を指定すると初期値の「1」を指定します。
BFD State	IPv6 RIP インタフェースの BFD 機能を有効 / 無効に指定します。
Passive Interface	パッシブインタフェースを有効 / 無効に指定します。インタフェースのルーティングアップデートの送信 / 受信を無効にします。しかし本インタフェースの他のルータから受信した RIPng 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 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。

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

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て以下の画面を表示します。



図 9-48　RIPng Database 画面

以下の項目を使用します。

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、入力したエントリを検出します。

OSPF（OSPF 設定）（EI/MI モードのみ）

L3 Features > OSPF

OSPF（Open Shortest Path First）ルーティングプロトコルは、Link-State アルゴリズムを使用して宛先ネットワークまでのルートを決定します。「リンク」はルータ上のインタフェースを指し、「State」（状態）はそのインタフェースと隣接するルータ間の関係を指しています。「State」には、IP アドレス、サブネットマスク、インタフェースに接続しているネットワークタイプ、そのネットワークに接続する他のルータなどの情報があります。「Link-State」情報は、Link-State データベースに集められ、OSPF が動作するルータによって維持されます。
OSPF では、ルータがどのように通信を行い、Link-State データベースを維持するかについて規定し、また OSPF を使用するネットワークトポロジについての概念を定義しています。
ルータ間の Link-State アップデートのトラフィックを制限するために、OSPF ではエリアという概念が定義されています。1 つのエリア内にあるすべてのルータは、1 つの Link-State データベースを共有し、1 つのルータによってデータベースに変更が生じると、それをトリガーとして同一エリア内にあるすべてのルータの Link-State データベースが更新されます。ルータのうち、複数のエリアに接続しているものを境界ルータ（Border Router）と呼びます。境界ルータはエリア間のルーティング情報を配信する役割を担います。
1 つのエリアが、エリア 0 またはバックボーンとして定義されます。このエリアは、ネットワークの中心的なエリアで、他のすべてのエリアはこのバックボーンエリアに（ルータを経由して）接続します。バックボーンエリアにはルータのみが接続し、あるエリアでルーティング情報の変更が発生するとバックボーンに伝えられ、そこから他のネットワークへ伝播されるような構造になっています。
OSPF を使用したネットワークを構築する際は、まずバックボーン（エリア 0）を構築し、そこからネットワークを広げるように構築することをお勧めします。

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、表示にします。

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。

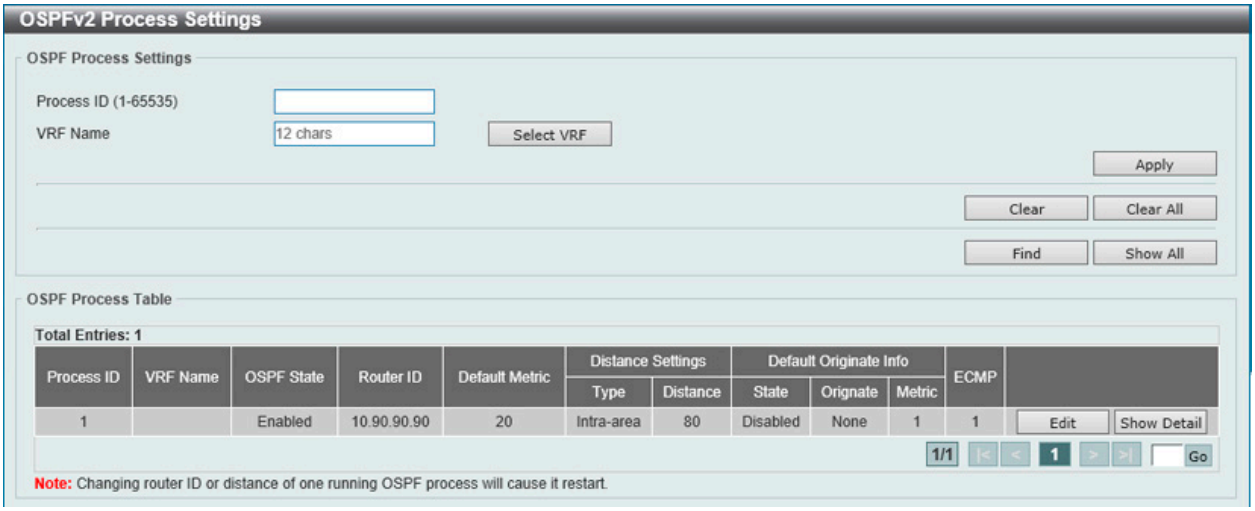


図 9-49　OSPFv2 Process Settings 画面

以下の項目があります。

項目	説明
Process ID	OSPF プロセス ID（1-65535）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。「Select VRF」をクリックすると設定済みの VRF インスタンスを使用します。

「Apply」をクリックし、設定内容を適用します。
「Clear」をクリックし、指定プロセスをクリアします。
「Clear All」をクリックし、全ての指定プロセスをクリアします。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

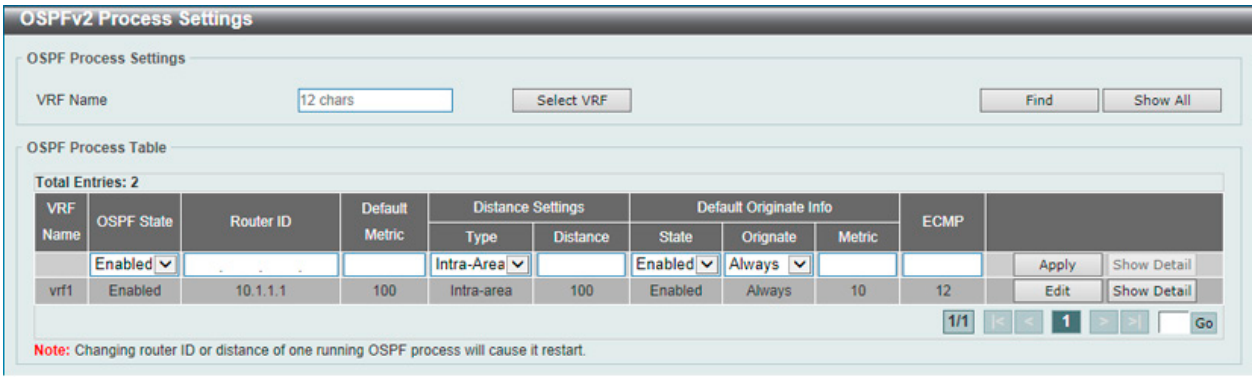


図 9-50　OSPFv2 Process Settings (Edit) 画面

以下の項目があります。

項目	説明
OSPF State	指定 VRF インスタンスの OSPFv2 機能を「Enabled」（有効）/「Disabled」（無効）にします。
Router ID	IPv4 アドレスフォーマットのルータ 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 ビットの数です。AS 内のルータを固有に識別します。各ルータは固有のルータ ID を持ちます。ルータが既に起動中で設定が済んでいる場合、新しいルータ ID はすぐに割り振られません。OSPF の再装填や再起動時に適用されます。
Default Metric	初期メトリック値（1-16777214）を指定します。
Type	ディスタンス設定種類を指定します。「Intra-Area」「Inter-Area」「External-1」「External-2」から指定します。 • 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「external type-5」と「type-1」メトリック付き「type-7」ルートのディスタンスを指定します。 • External-2 - OSPF「external type-5」と「type-2」メトリック付き「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（1-255）を指定します。
State	初期「Originate」情報を有効 / 無効に指定します。AS に向かう初期外部ルート (type-5 LA) ネットワーク「0.0.0.0」の生成に使用されます。
Originate	「Originate」のオプションを指定します。「Always」「None」から指定します。「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。
Metric	生成されたデフォルトルートにかかるコスト（1-65535）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。
ECMP	ECMP 値（1-64）を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

「Show Detail」をクリックすると、以下の画面が表示されます。

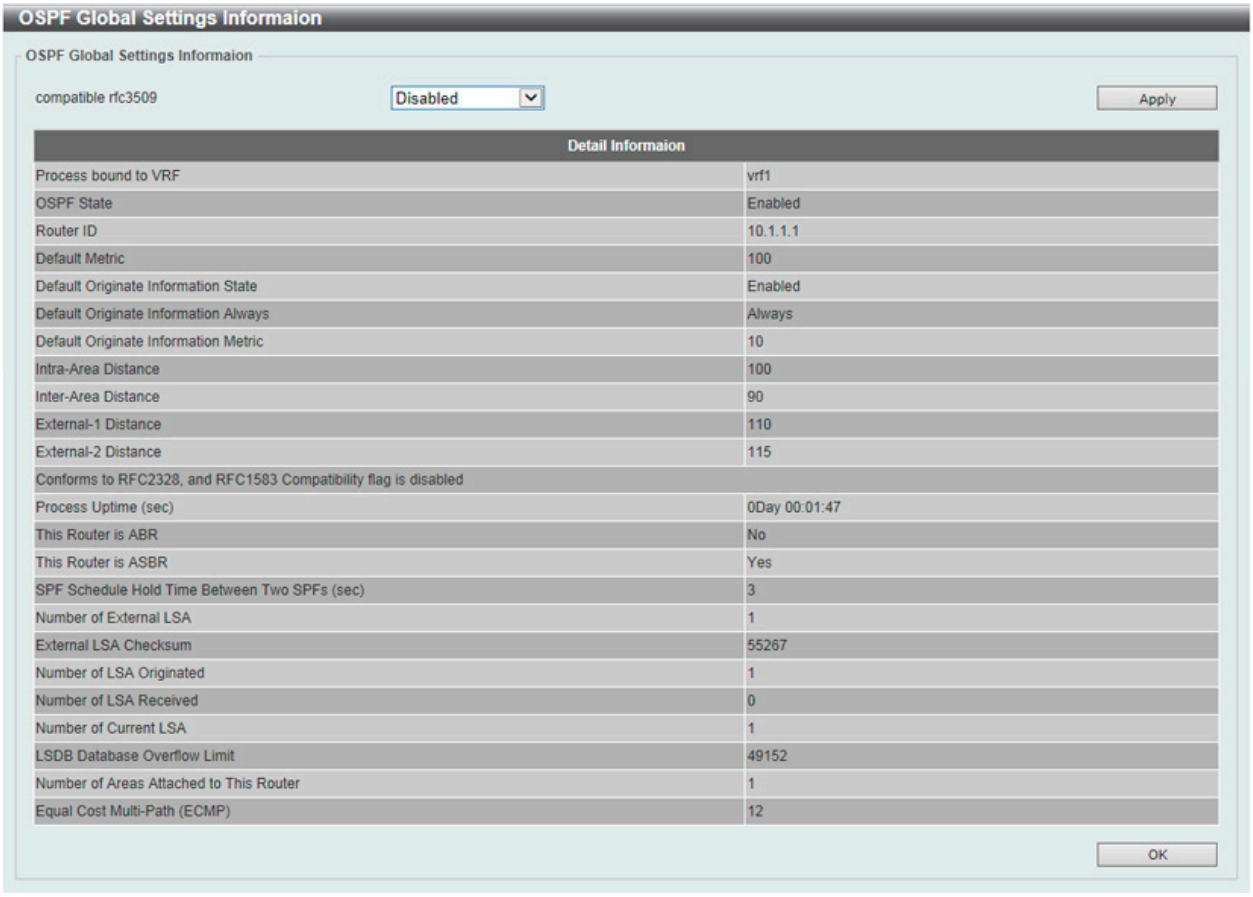


図 9-51　OSPFv2 Process Settings (Show Detail) 画面

以下の項目があります。

項目	説明
Compatible RFC3509	Area Border Router (ABR) の実行を有効 / 無効に指定します。「RFC 3509」で定義されています。

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

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。

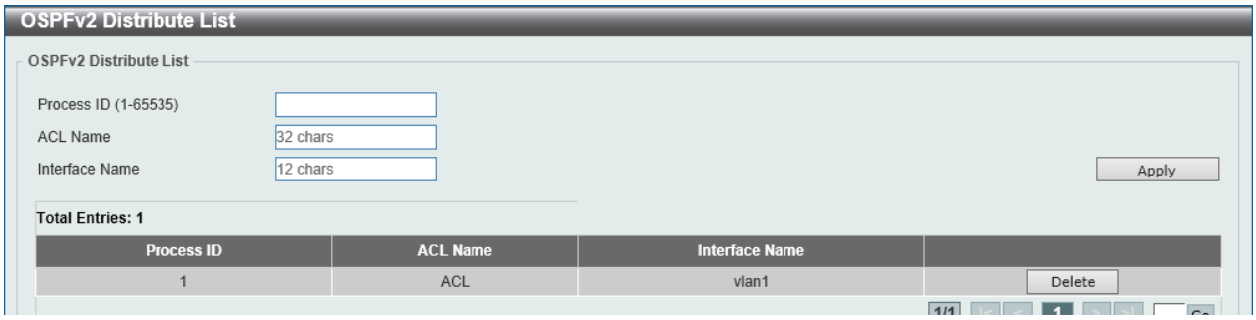


図 9-52　OSPFv2 Distribute List 画面

以下の項目があります。

項目	説明
Process ID	プロセス ID（1-65535）を指定します。
ACL Name	アクセスリスト名を 32 字以内で入力します。
Interface Name	インタフェース名を 12 字以内で入力します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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 9-53　OSPFv2 GR Helper Settings 画面

以下の項目があります。

項目	説明
Process ID	プロセス ID（1-65535）を指定します。
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。 • Only Upgrade - OSPF グレースフルリスタートヘルパーモードをアップグレード時のみ許可します。
Max Grace Period	最大グレース期間（1-1800 秒）を指定します。

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

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 9-54　OSPFv2 Passive Interface Settings 画面

以下の項目があります。

項目	説明
Process ID	プロセス ID（1-65535）を指定します。
Interface Name	使用するインタフェース名（12 字以内）を指定します。「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。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

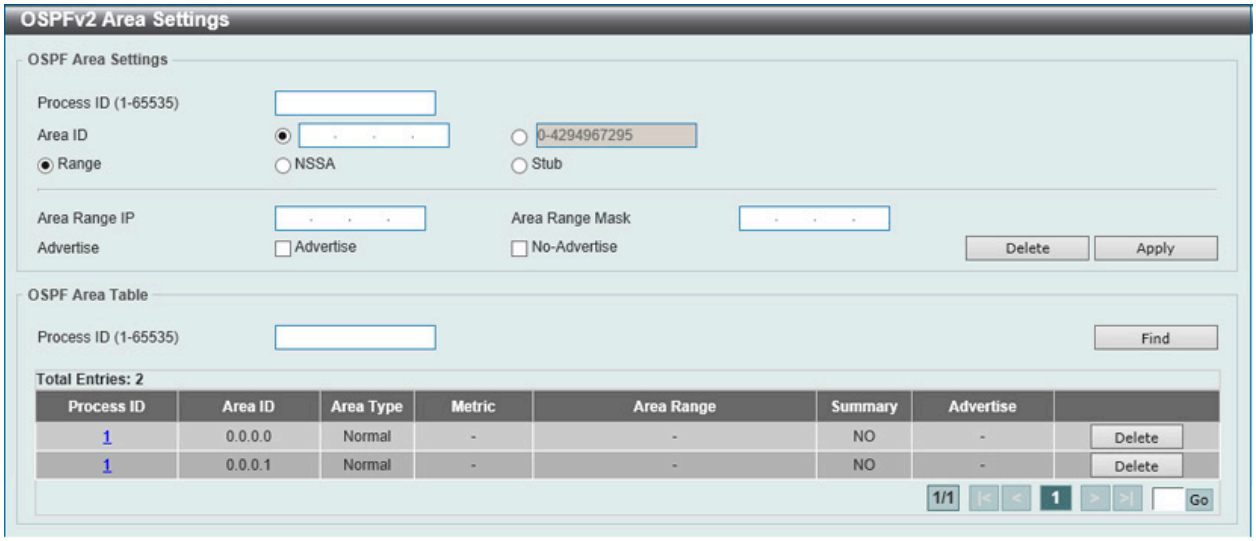


図 9-55　OSPFv2 Area Settings 画面

OSPF エリア集約の設定は、以下の項目を使用して行います。

項目	説明
Process ID	プロセス ID（1-65535）を指定します。
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	OSPF エリアに対応するネットワークを識別する IP アドレス範囲を入力します。
Area Range Mask	OSPF エリアに対応するネットワークを識別するネットマスク範囲を入力します。

項目	説明
Advertise	通知（Advertise）を有効または無効にします。 • 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。コンポネントのルートが背後に存在しています。
Default Cost	「NSSA」または「Stub」選択時に有効です。初期コスト値（0-65535）を指定します。「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コストです。 • Default - 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ない場合、指定します。
OSPF Area Table	
Process ID	プロセス ID（1-65535）を指定します。

「Apply」ボタンをクリックして行った変更を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Process ID」のリンクをクリックすると、以下の画面が表示されます。

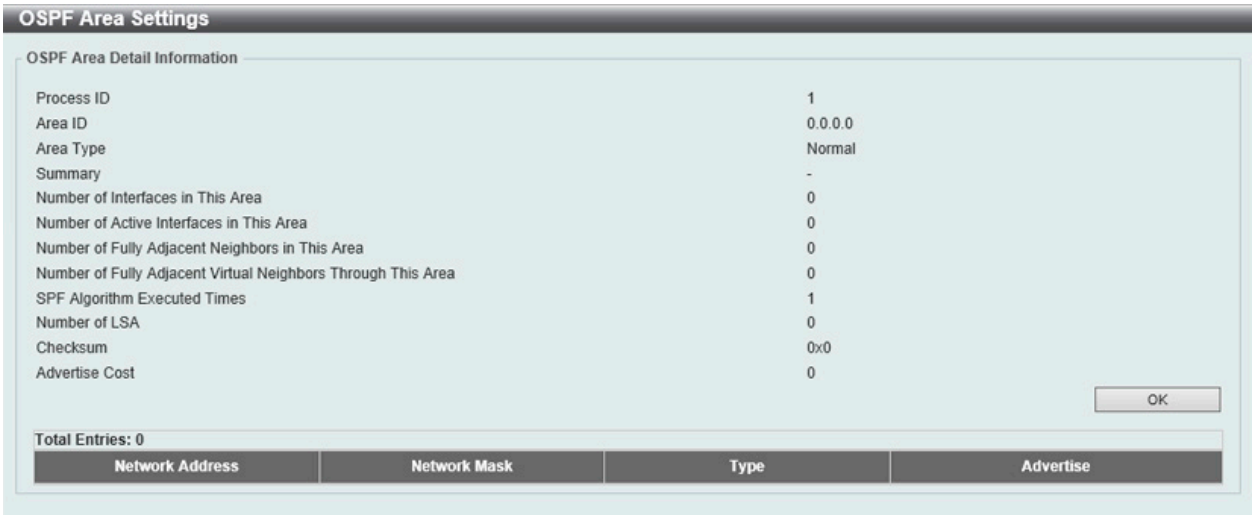


図 9-56　OSPFv2 Area Settings（Process ID）画面

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

OSPFv2 Interface Settings（OSPFv2 インタフェース設定）

このスイッチの 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。

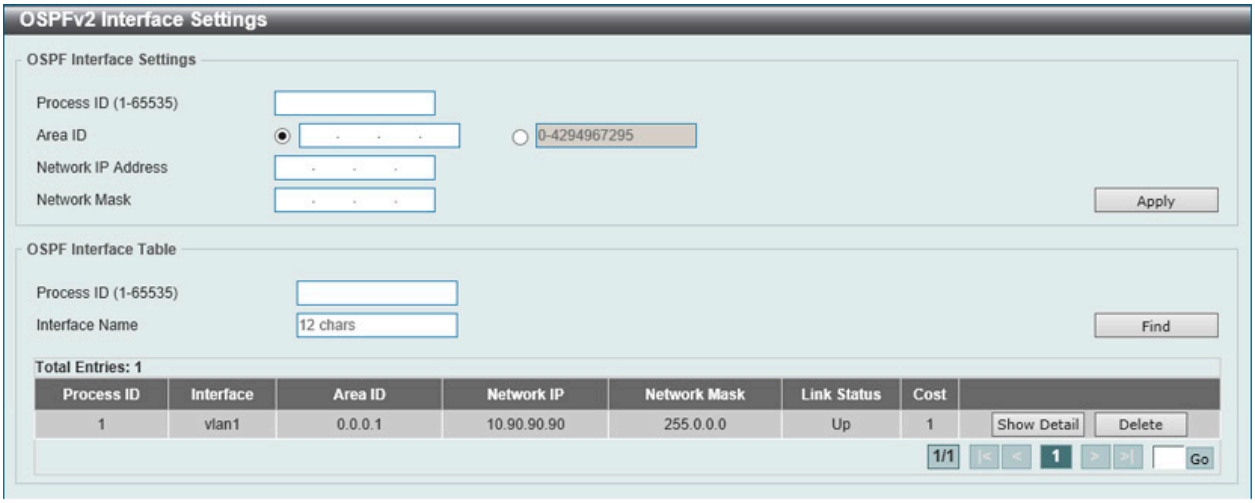


図 9-57　OSPFv2 Interface Settings 画面

以下の項目があります。

項目	説明
OSPF Interface Settings	
Process ID	プロセス ID（1-65535）を指定します。

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。
Network IP Address	IPv4 アドレスを指定します。
Network Mask	IPv4 サブネットマスクを指定します。
OSPF Interface Table	
Process ID	プロセス ID（1-65535）を指定します。
Interface Name	インタフェース名を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Find」ボタンをクリックして、入力したインタフェースを検出します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。

1. 編集するポートの「Show Detail」ボタンをクリックし、以下の画面を表示します。

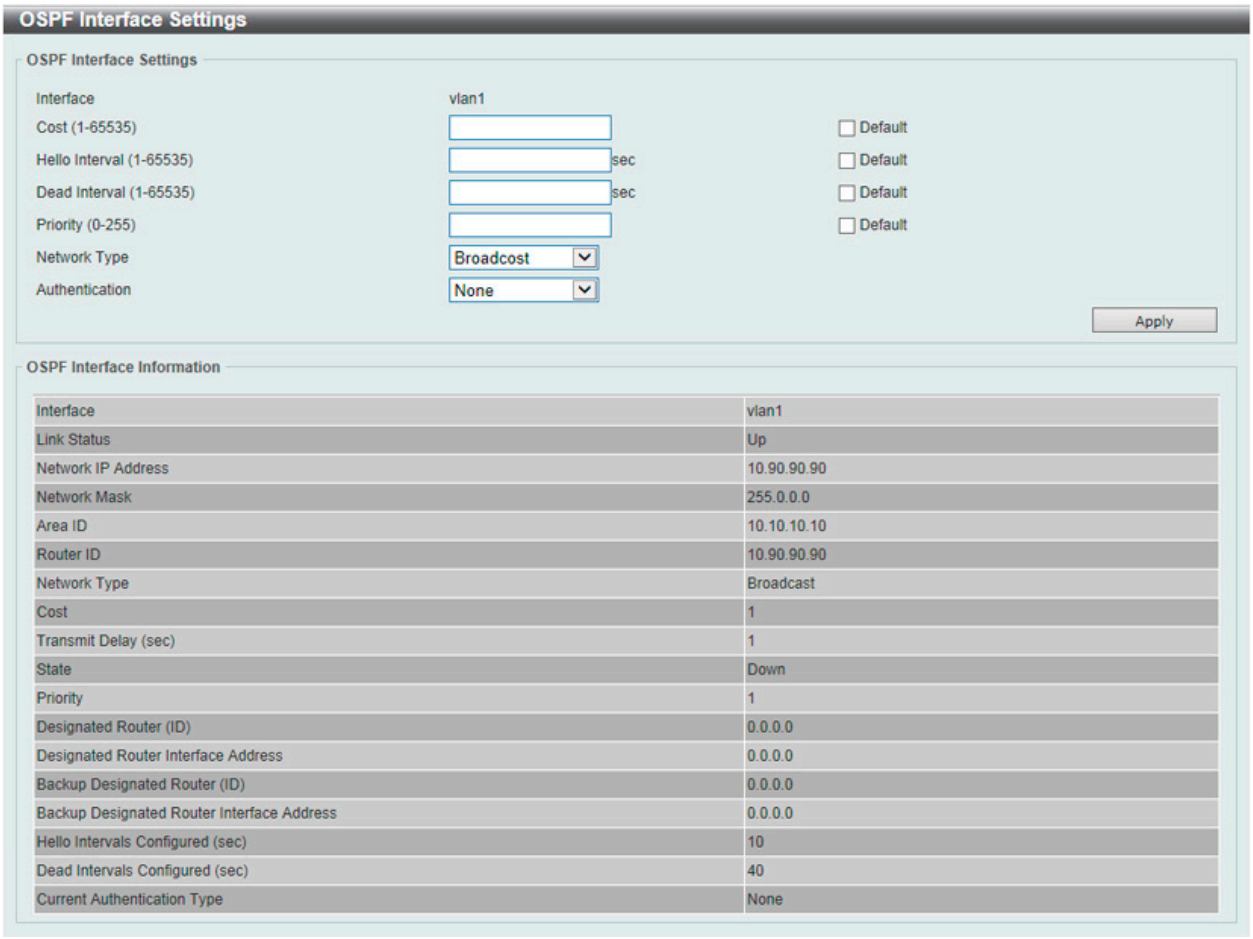


図 9-58　OSPFv2 Interface Settings (Show Detail) 画面

以下の項目があります。

項目	説明
Cost	コストの値（1-65535）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。コストはインタフェースのスピードに比例します。コストは手動または自動でアサインすることが可能です。初期値ではインタフェースのコストは帯域情報に基づき計算されます。コストは参照した帯域情報に対応して「1」になります。「Default」を指定すると初期期の「1」を採用します。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔（秒）を指定します。
Dead Interval (1-65535)	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（秒）。本値には Hello Interval の倍数を指定します。
Priority	代表ルータ選出のプライオリティ（0-255）を指定します。ルータプライオリティ 0 が指定されると、スイッチはそのネットワークの代表ルータとして選出されなくなります。

項目	説明
Network Type	ネットワークタイプを次から指定します。 • 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、通信できる 2 ルータのみが隣接者になることが可能です。
Authentication	OSPF ルーティングドメインでの OSPF パケットの送受信時における認証方法を設定します。 • None - 認証を行いません。 • Simple Password - パケットが認証済みルータからのものであるかを判断するためにシンプルパスワードを使用します。本モードを選択した場合、「Password」に 8 文字までのパスワードを指定します。 • MD5 -「MD5 Key Table Configuration」メニューで登録された暗号キーを使用します。本モードを選択した場合、「Key ID」欄に、登録済みのキーの中から 1 つを入力します。
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（8 字以内）を入力します。
MD5 Key ID	MD5 暗号キー ID(1-255) を入力します。
MD5	MD5 キー（16 字）を指定します。シンタックスはスペースなしのアルファベット文字列です。 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解析されたダイジェストに対するメッセージを確認します。 ネイバルータの同じキー ID は同じ文字列で定義されます。インタフェースのすべての隣接するルータは、それぞれ OSPF パケットを交換するために同じキーを使用する必要があります。

「Apply」ボタンをクリックして行った変更を適用します。

OSPFv2 BFD Settings（OSPFv2 BFD 設定）

このスイッチの OSPFv2 インタフェースを設定します。

L3 Features > OSPF > OSPFv2 > OSPF BFD 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　OSPFv2 BFD Settings 画面

以下の項目があります。

項目	説明
BFD State	指定インタフェースの BFD 機能を有効 / 無効に指定します。BFD がインタフェースで有効な場合、ルータは現在のインタフェースの OSPF ネイバとともに BFD セッションを作成します。BFD セッションが落ちると、学習された OSPF セッションもまた削除されます。

「Apply」ボタンをクリックして行った変更を適用します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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、または「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。内部メトリックは自身から宛先に到達するまでの通知コスト追加した、ルータ再分配のルートコストを認識します。外部メトリックは宛先に到達するまでの通知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。

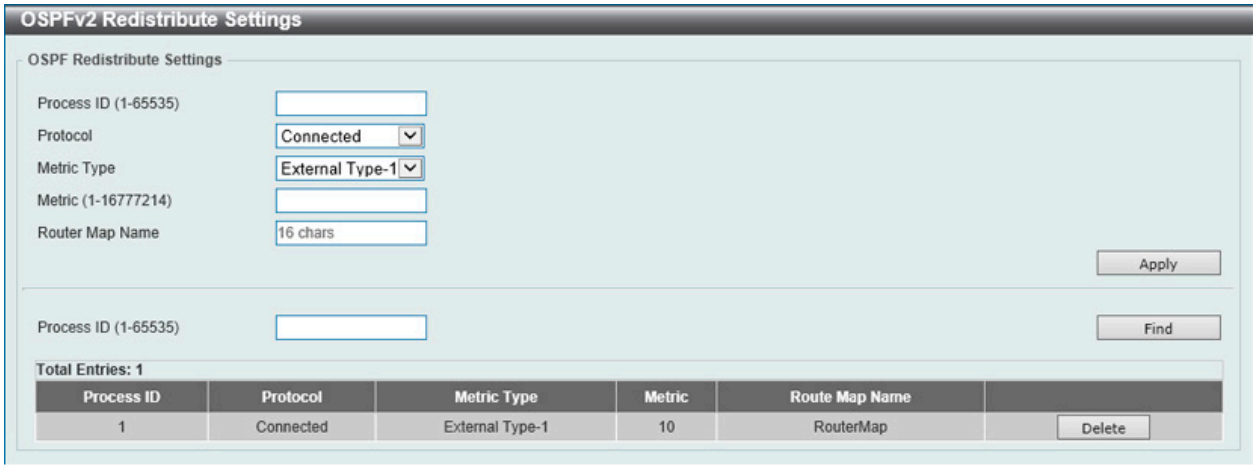


図 9-60　OSPFv2 Redistribute Settings 画面

以下の項目があります。

項目	説明
Process ID	プロセス ID（1-65535）を指定します。
Protocol	再分配される送信元プロトコルを指定します。「Connected」「Static」「RIP」「BGP」「ISIS」から指定します。OSPF のようなルーティングプロトコルの場合、自立したシステムに外部として再分配されます。
Metric Type	メトリックの種類を指定します。「External Type-1」「External Type-2」から指定します。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。
Metric	再分配ルートのメトリック（1-16777214）を指定します。
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。

「Apply」ボタンをクリックして行った変更を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定の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。

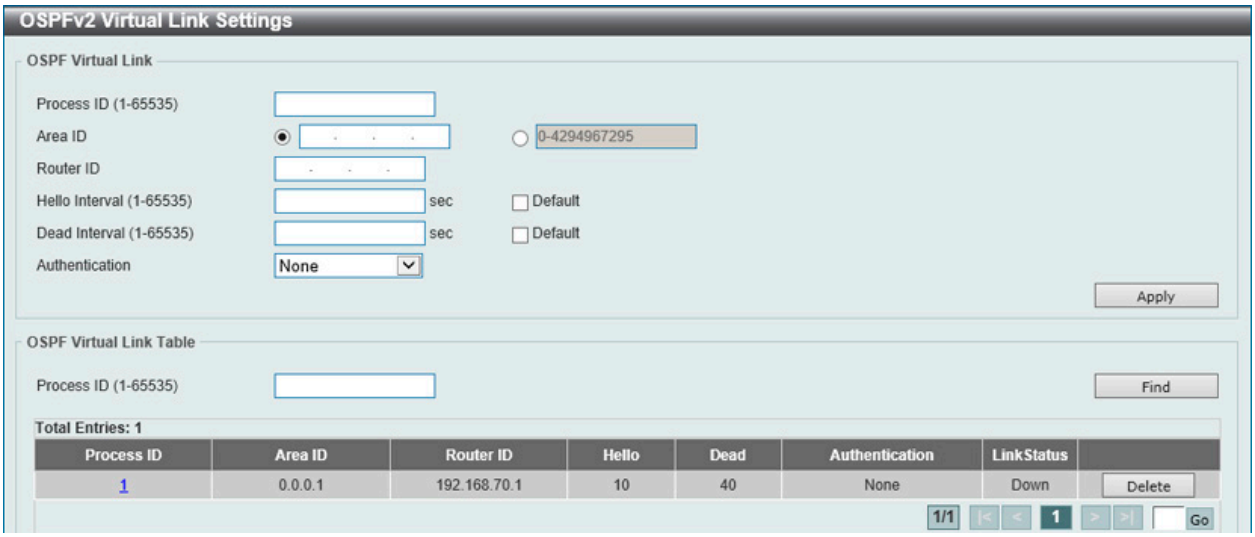


図 9-61　OSPF Virtual Link Settings 画面

以下の項目が表示されます。

項目	説明
OSPF Virtual Link	
Process ID	プロセス ID（1-65535）を指定します。
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。
Router ID	リモートエリアの OSPFv2 ルータ ID。リモートエリアの Area Border Router(エリア境界ルータ) 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) を表示します。これは Neighbor ルータのルータ ID です。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔（秒）を指定します。同一ネットワークのルータには同じ「Hello Interval」、「Dead Interval」、「Authorization Type」、「Authorization Key」が設定される必要があります。
Dead Interval (1-65535)	隣接ルータが Hello パケットを最後に受信してから、選択エリアがダウンしたと判断するまでの時間（秒）を入力します。1 から 65535（秒）で指定します。本値には Hello Interval の倍数を指定します。
Authentication	使用する認証を選択します。「None」、「Simple Password」または「MD5」を選択します。「Simple Password」認証を選択するとパスワードの入力が必要です。「MD5」認証を選択すると KEY ID の入力が必要です。
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。
MD5 Key ID	MD5 暗号キー ID(1-255) を入力します。
MD5	MD5 キー（16 字）を指定します。シンタックスはスペースなしのアルファベット文字列です。
OSPF Virtual Link Table	
Process ID	プロセス ID（1-65535）を指定します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

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

エントリを指定し「OK」をクリック、設定内容を適用します。

「Process ID」のリンクをダブルクリックすると次の画面が表示されます。

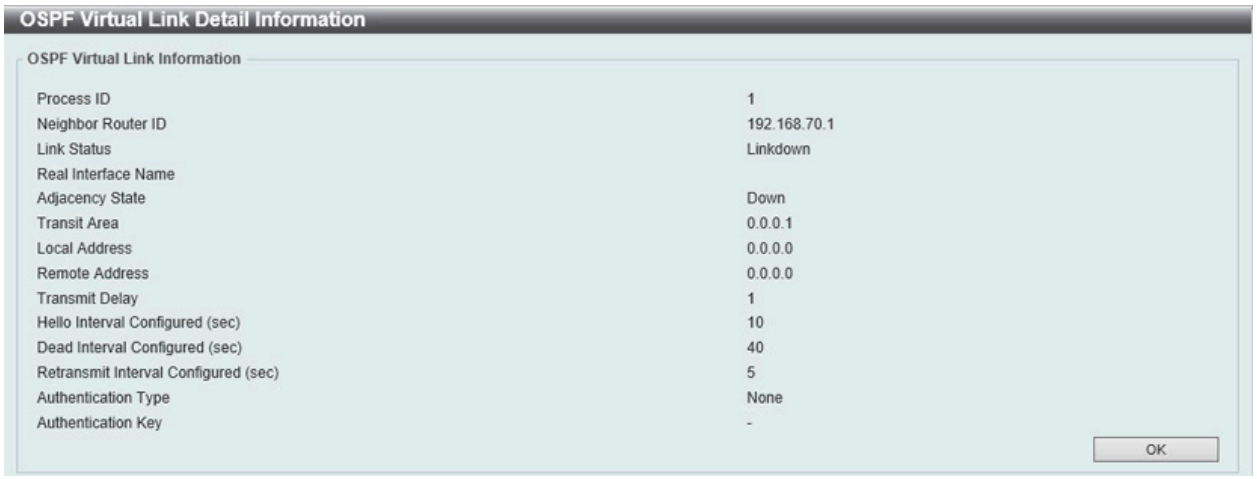


図 9-62　OSPFv2 Virtual Link Settings (Double Click) 画面

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。

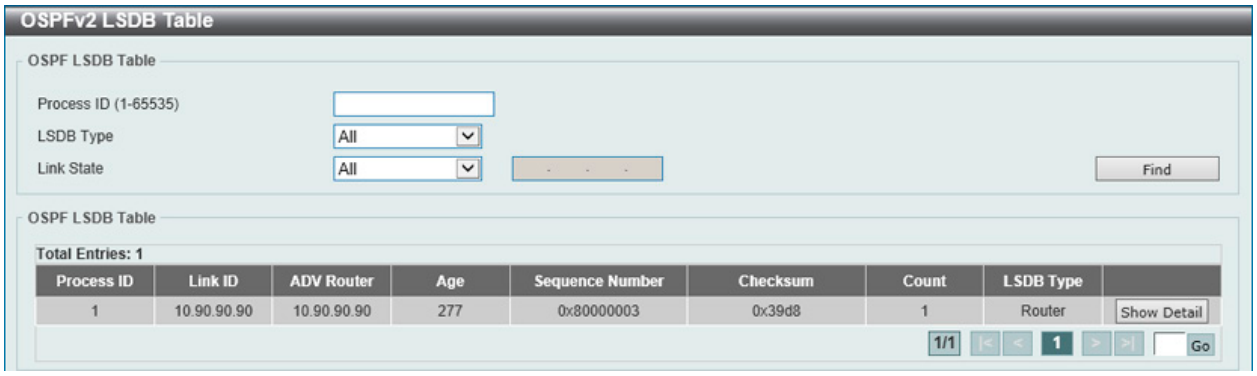


図 9-63　OSPFv2 LSDB Table Settings 画面

以下の項目を使用します。

項目	説明
Process ID	プロセス ID（1-65535）を指定します。
LSDB Type	表示する LSDB タイプを指定します。「All」「Router」「Network」「Summary」「ASBR Summary」「External」「Stub」「NSSA External」から選択します。
Link State	表示されるリンクステート情報を選択します。「All」「Link State ID」「Self Originate」「Adv Router」から選択します。 「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 を指定します。 「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、指定したエントリを検索します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。
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。
エントリを指定し「OK」をクリック、設定内容を適用します。

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。

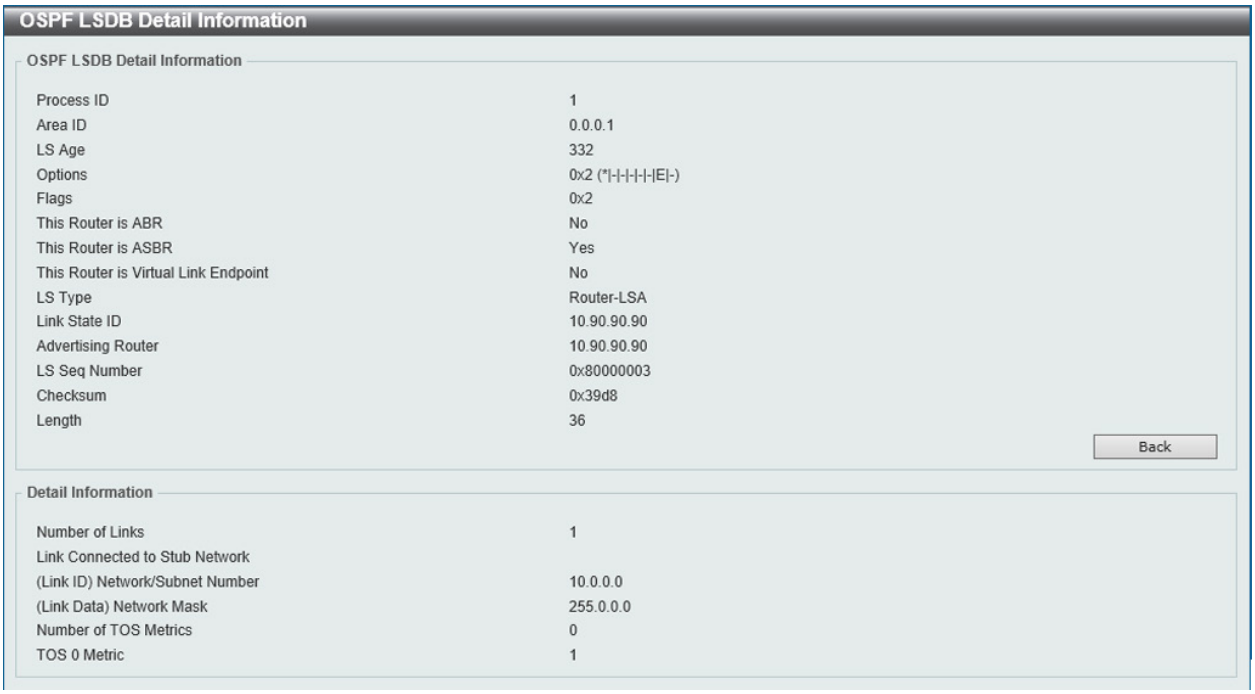


図 9-64　OSPFv2 LSDB Table 画面（Show Detail）

「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。

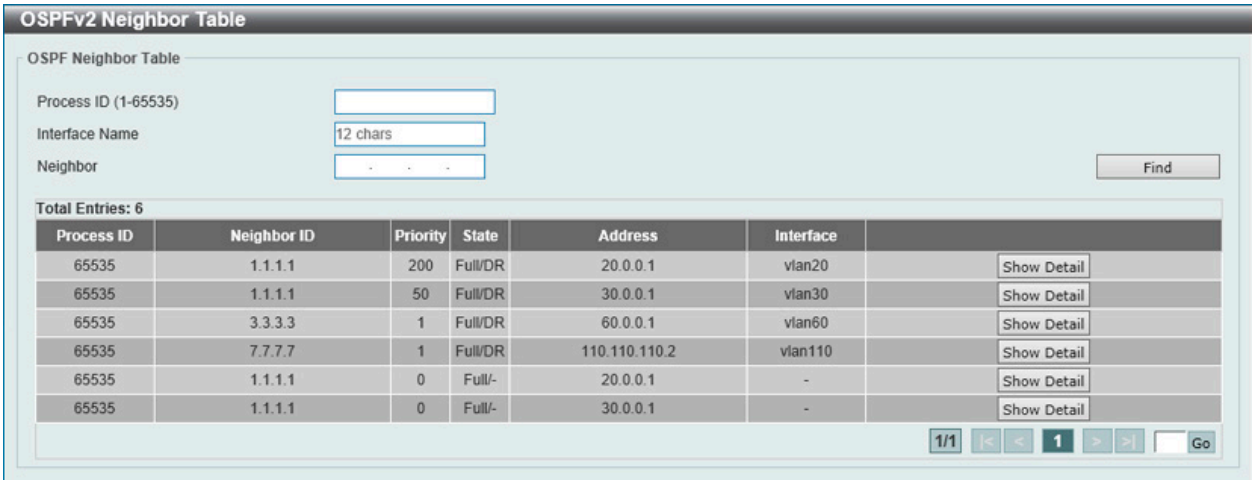


図 9-65　OSPFv2 Neighbor Table 画面

以下の項目を使用します。

項目	説明
Process ID	プロセス ID（1-65535）を指定します。
Interface Name	使用されるインタフェースを指定します。
Neighbor	Neighbor ルータの ID を入力します。

エントリの参照
「Find」ボタンをクリックして、指定したエントリを検索します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

「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。

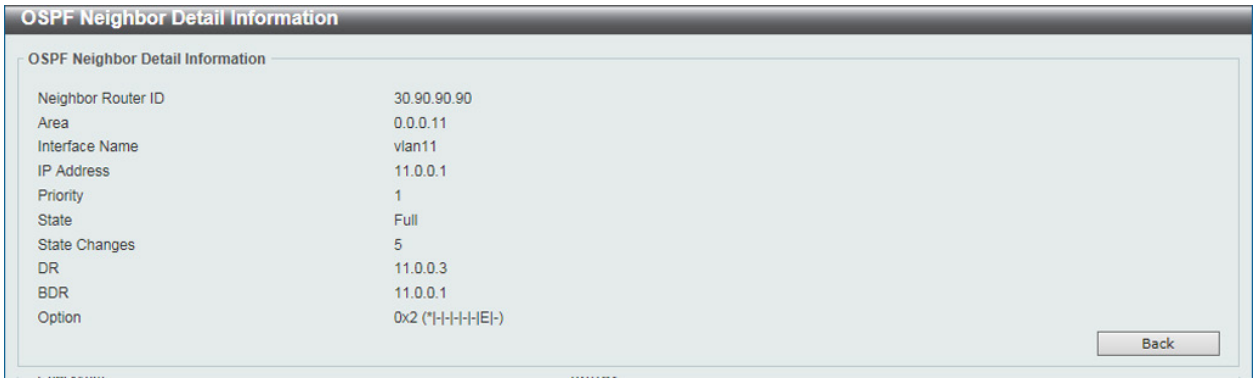


図 9-66　OSPFv2 Neighbor Table 画面（Show Detail）

「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。
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。

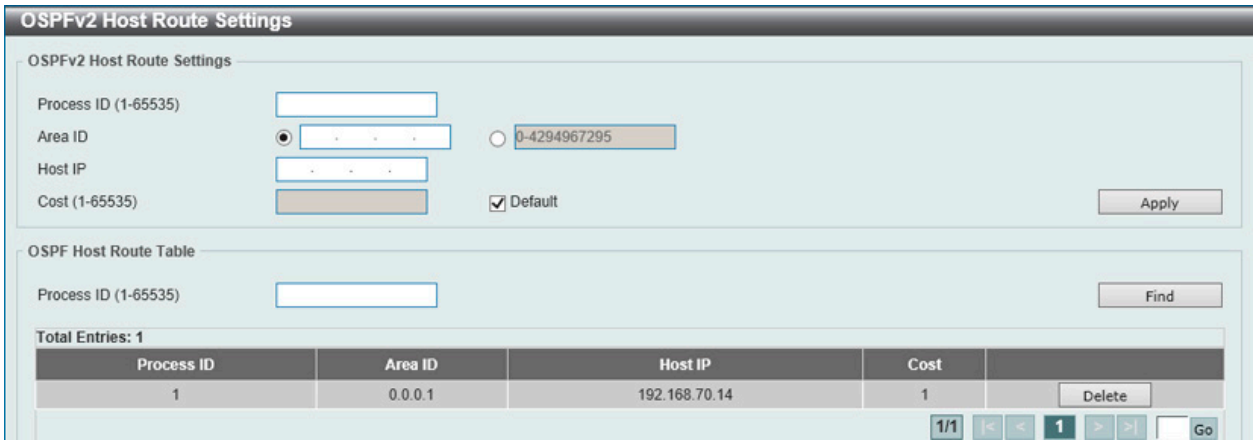


図 9-67　OSPFv2 Host Route Settings 画面

以下のフィールドを使用して OSPF ホストルートの設定を行います。

項目	説明
OSPFv2 Host Route Settings	
Process ID	プロセス ID（1-65535）を指定します。
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。
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」を指定すると初期値（1）を使用します。
OSPF Host Route Table	
Process ID	プロセス ID（1-65535）を指定します。

「Apply」ボタンをクリックして行った変更を適用します。
「Find」ボタンをクリックして、指定したエントリを検索します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
エントリを指定し「OK」をクリック、設定内容を適用します。

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て以下の画面を表示します。

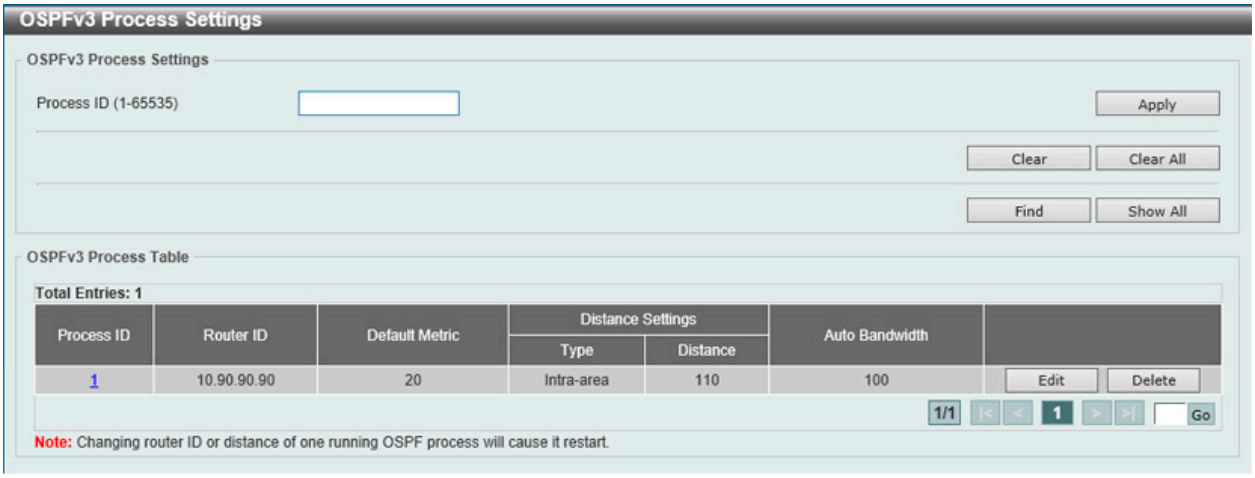


図 9-68　OSPFv3 Process Settings 画面

以下の項目を使用します。

項目	説明
Process ID	OSPFv3 のプロセス ID（1-65535）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Edit」をクリックして、指定エントリの編集を行います。
「Process ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。
「Clear」をクリックすると入力したエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。
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。

「Edit」をクリックすると、以下の画面が表示されます。

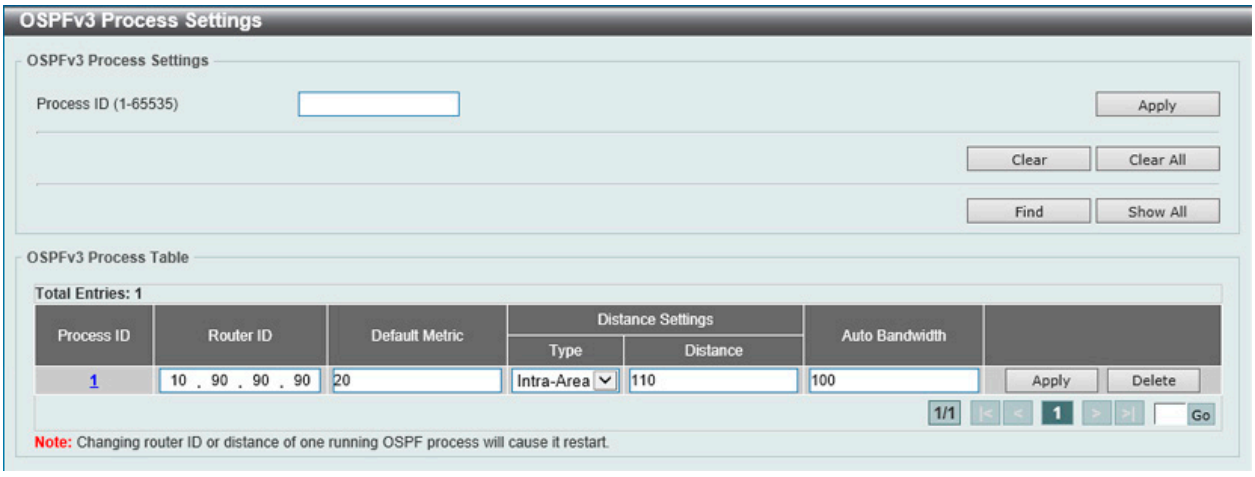


図 9-69　OSPFv3 Process Settings (Edit) 画面

以下の項目を使用します。

項目	説明
Router ID	OSPF プロセスのためのルータ ID を入力します。
Default Metric	初期メトリック値（1-16777214）を指定します。初期値は 20 です。全ての再分配ルートに同じメトリックを使用する、現在のルーティングプロトコルを有効にする OSPFv3 再分配機能と共同で使用されます。初期メトリックは不適合なメトリックの再分配ルートの問題を解決します。メトリックが直接コンバートされなくても、初期メトリックを使用して、適当な代替策を提供し、再分配を実行します。

項目	説明
Type	ディスタンス設定種類を指定します。「Intra-Area」「Inter-Area」「External」から指定します。 • 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 - OSPF エクスターナル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（1-254）を指定します。初期値は 110 で全ての OSPF ルートの値です。
Auto Bandwidth	自動帯域の値（1-4294967）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コントロールする機能です。

「Apply」ボタンをクリックして行った変更を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Process ID」のリンクを指定すると次の画面が表示されます。

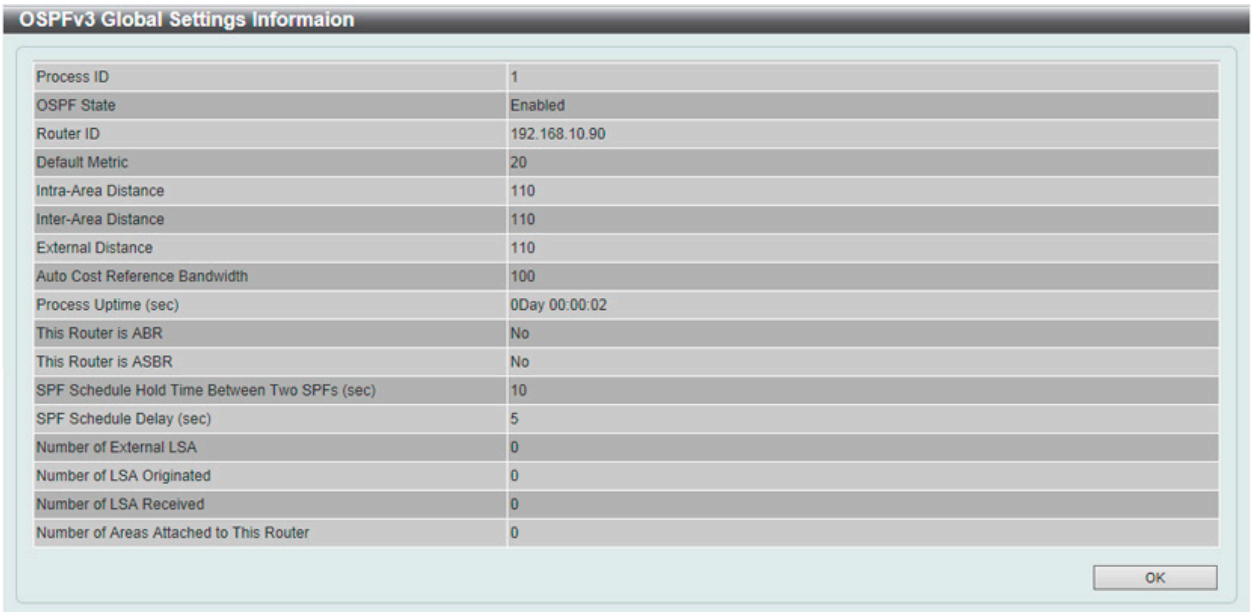


図 9-70　OSPFv3 Process Settings (Process ID) 画面

「OK」をクリックして画面を終了し前画面に戻ります。

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（受動態）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の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て以下の画面を表示します。



図 9-71　OSPFv3 Passive Interface Settings 画面

以下の項目を使用します。

項目	説明
Process ID	OSPFv3 のプロセス ID（1-65535）を指定します。
Interface Name	パッシブインタフェース名（12 字以内）を指定します。「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。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

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て以下の画面を表示します。

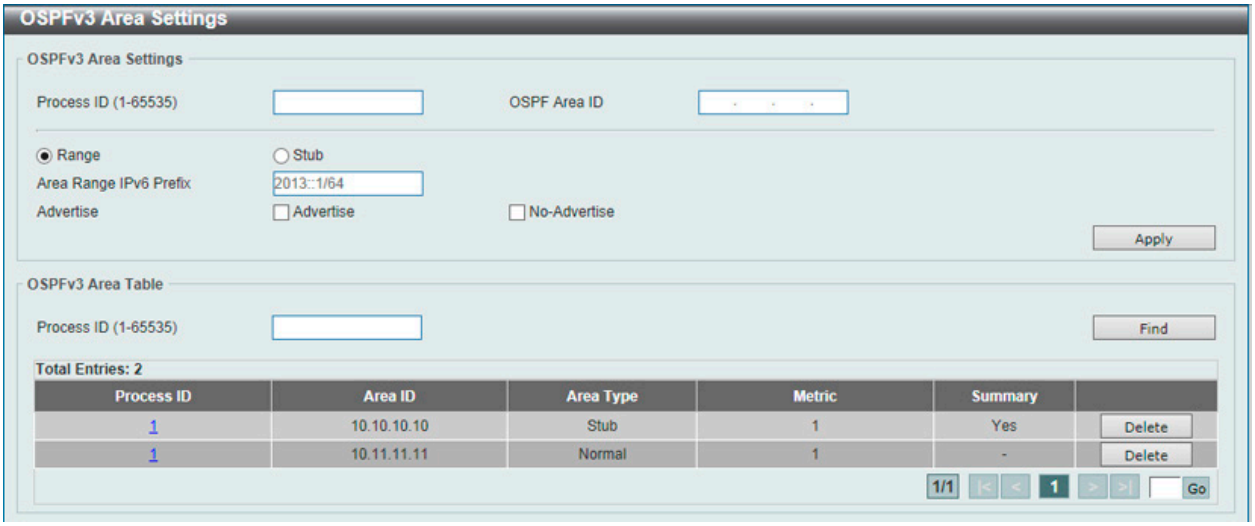


図 9-72　OSPFv3 Area Settings 画面

以下の項目を使用します。

項目	説明
OSPFv3 Area Settings	
Process ID	OSPF のプロセス ID（1-65535）を指定します。
OSPF Area ID	OSPFv3 エリアの ID を指定します。IPv4 アドレス形式で入力します。
Range	Area Border Router (ABR) の OSPF ルートをサマライズします。
Stub	指定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）を有効または無効にします。 • Advertise - 指定範囲のアドレスの「inter-area prefix Link-State Advertisement (LSA)」を通知します。 • No-Advertise -「inter-area prefix LSA」の通知を抑制します。コンポネントのルートが背後に存在しています。
Metric (0-65535)	OSPFv3 スタブエリアの初期コストを指定します。「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」を選択するとスタブエリアの inter-area prefix LSA からの ABR を阻止します。
OSPFv3 Area Table	
Process ID	OSPF のプロセス ID（1-65535）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Process ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Stub」エリアの「Process ID」をクリックすると、以下の画面が表示されます。



図 9-73　OSPFv3 Area Settings 画面 - Stub

「OK」をクリックして画面を終了し前画面に戻ります。

「Normal」エリアの「Process ID」をクリックすると、以下の画面が表示されます。

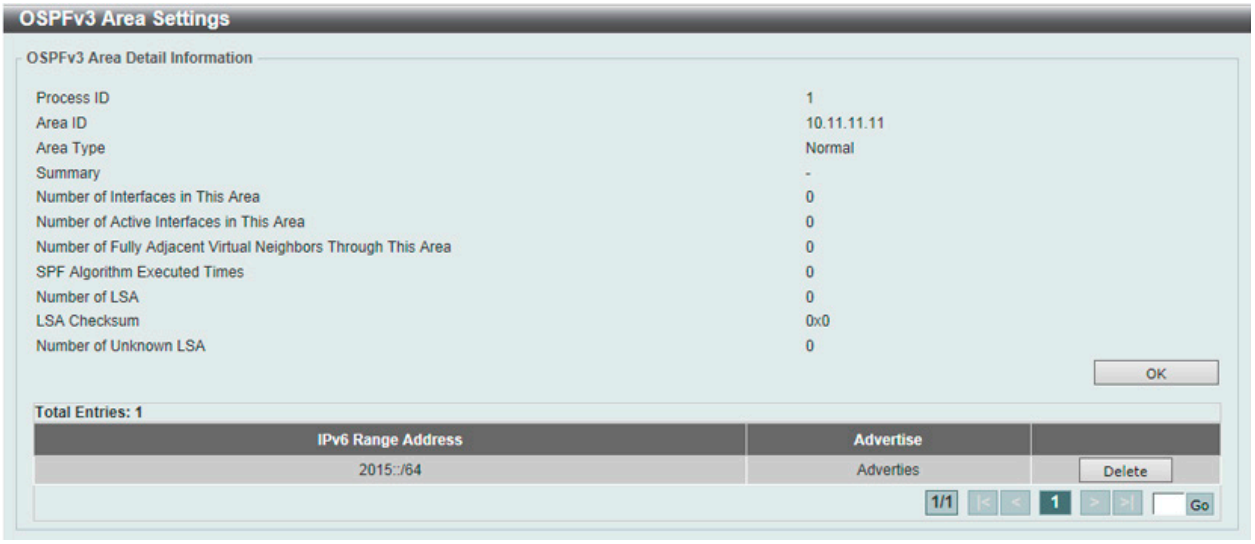


図 9-74　OSPFv3 Area Settings 画面 - Normal

「OK」をクリックして画面を終了し前画面に戻ります。
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。

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て以下の画面を表示します。

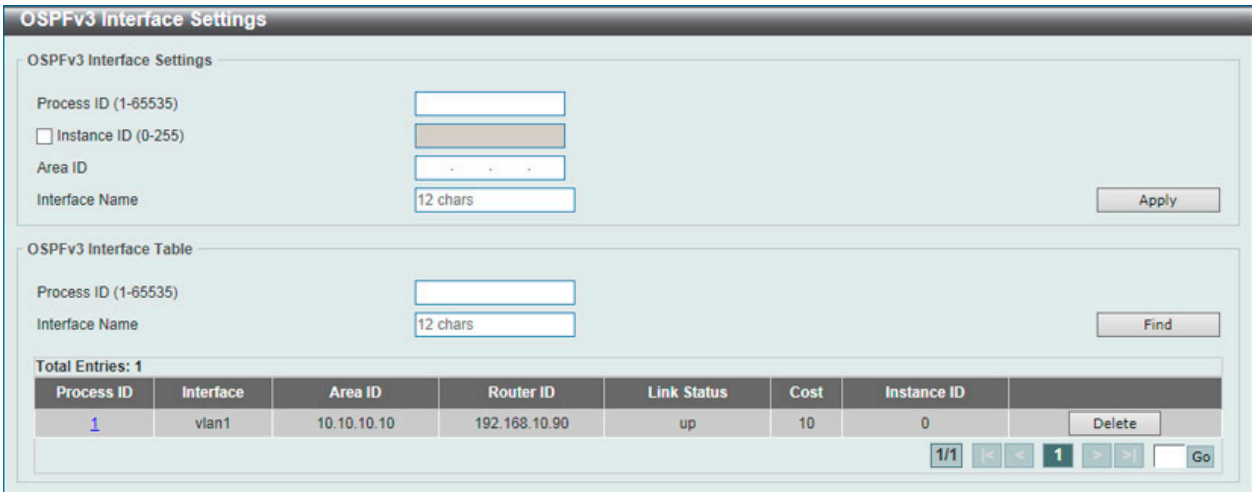


図 9-75　OSPFv3 Interface Settings 画面

以下の項目を使用します。

項目	説明
OSPFv3 Interface Settings	
Process ID	IPv6 OSPF ルーティングのプロセス ID（1-65535）を指定します。
Instance ID	インスタンス ID（0-255）を指定します。初期値は「0」
Area ID	エリアの識別子として IPv4 アドレスを指定します。
Interface Name	VLAN インタフェース名（12 字以内）を入力します。
OSPFv3 Interface Table	
Process ID	IPv6 OSPF ルーティングのプロセス ID（1-65535）を指定します。
Interface Name	インタフェース名を入力します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Process ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Process ID」をクリックすると、以下の画面が表示されます。

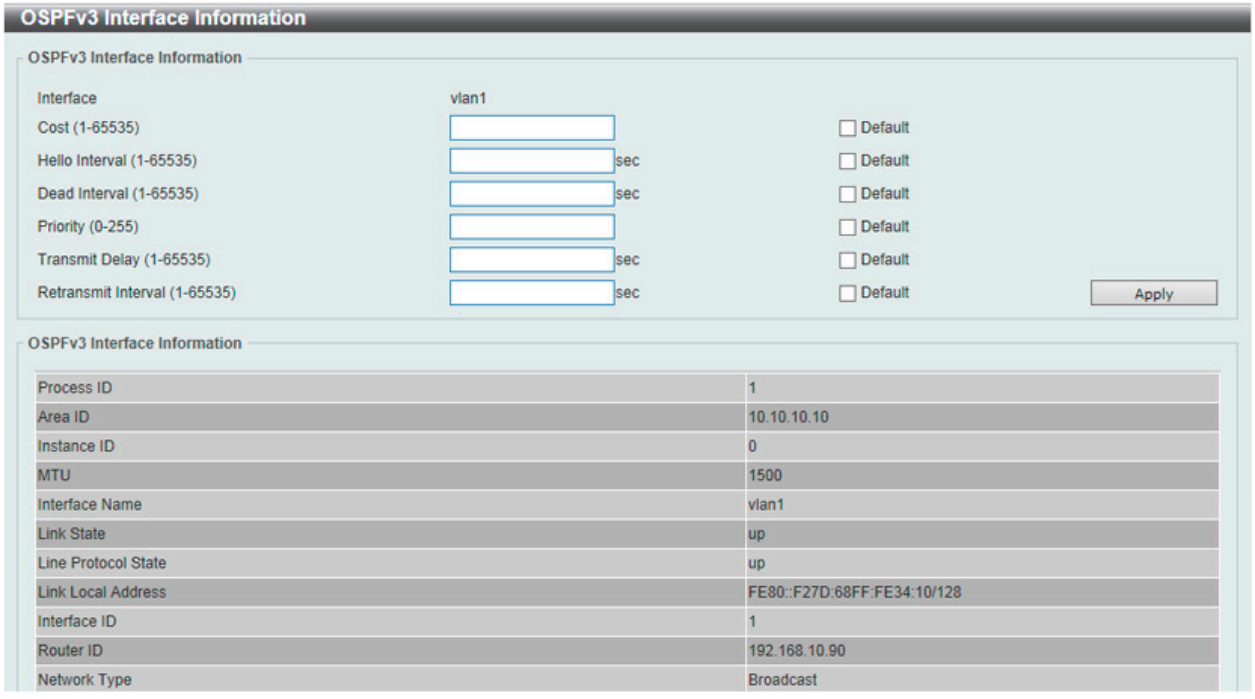


図 9-76　OSPFv3 Interface Settings 画面 - Process ID

「OK」をクリックして画面を終了し前画面に戻ります。
以下の項目を使用します。

項目	説明
Cost	指定した OSPFv3 インタフェースに到達する際の OSPFv3 コスト (1-65535) を指定します。「Default」を指定すると初期値を使用します。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔（秒）を指定します。同じリンクの全ルータには同じ「Hello Interval」と「Dead Interval」が設定される必要があります。「Default」を指定すると初期値を使用します。初期値は 10 です。
Dead Interval (1-65535)	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 (秒) を入力します。本値には Hello Interval の倍数を指定します。「Default」を指定すると初期値を使用します。初期値は 40 です。
Priority (0-255)	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。「Default」を指定すると初期値を使用します。初期値は 1 です。ネットワークの OSPF Designated Router (DR) の優先値決定に使用します。二つのルータが DR になろうとした場合、より高い優先値のルータが（DR）になります。二つのルータの優先値が同じ場合、より高いルータ ID を持つ方が高い優先性を持ちます。「non-zero」ルータ優先値を持つルータのみが宛先、またはバックアップ宛先ルータになりえます。複数アクセスネットワーク（非 point-to-point）のルータ優先値のみ指定します。
Transmit Delay	「Transmit Delay」値（1-65533）を指定します。「Default」を指定すると初期値（1）を使用します。
Retransmit Interval	「Retransmit Interval」（再送信間隔）の値（1-65533 秒）を指定します。LSA をネイバに送信後、ルータは LSA を受信の通知まで保持します。指定の間隔、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」を指定すると初期値（5）を使用します。

「Apply」ボタンをクリックして行った変更を適用します。

OSPFv3 Redistribute Settings（OSPFv3 リディストリビュート設定）

OSPFv3 リディストリビュート（再分配）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。

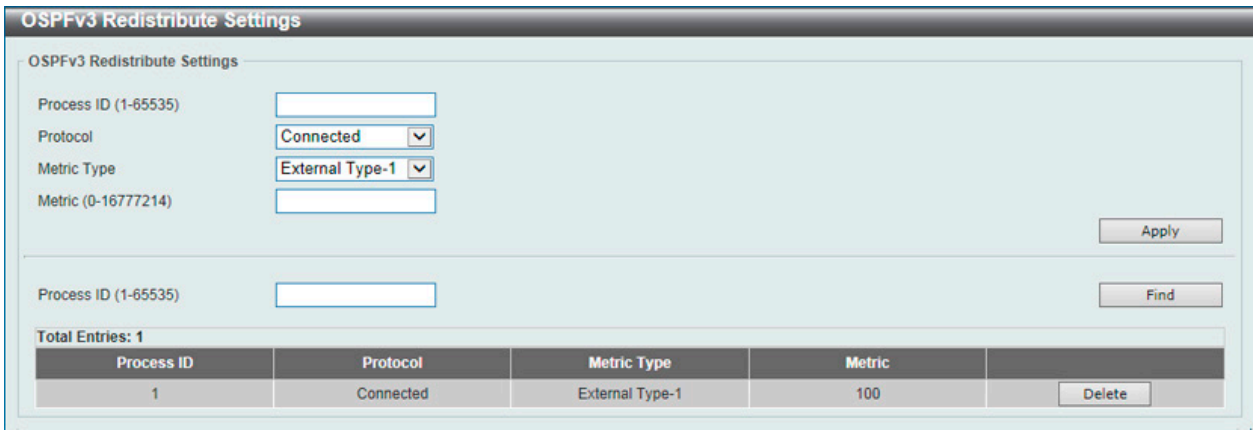


図 9-77　OSPFv3 Redistribute Settings 画面

以下の項目があります。

項目	説明
Process ID	IPv6 OSPF ルーティングのプロセス ID（1-65535）を指定します。
Protocol	再分配される送信元プロトコルを指定します。「Connected」「Static」「RIP」「BGP」「ISIS」から指定します。OSPF のようなルーティングプロトコルの場合、自立したシステムに外部として再分配されます。
Metric Type	メトリックの種類を指定します。「External Type-1」「External Type-2」から指定します。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。
Metric	再分配ルートのメトリック（1-16777214）を指定します。

「Apply」ボタンをクリックして行った変更を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定の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て以下の画面を表示します。

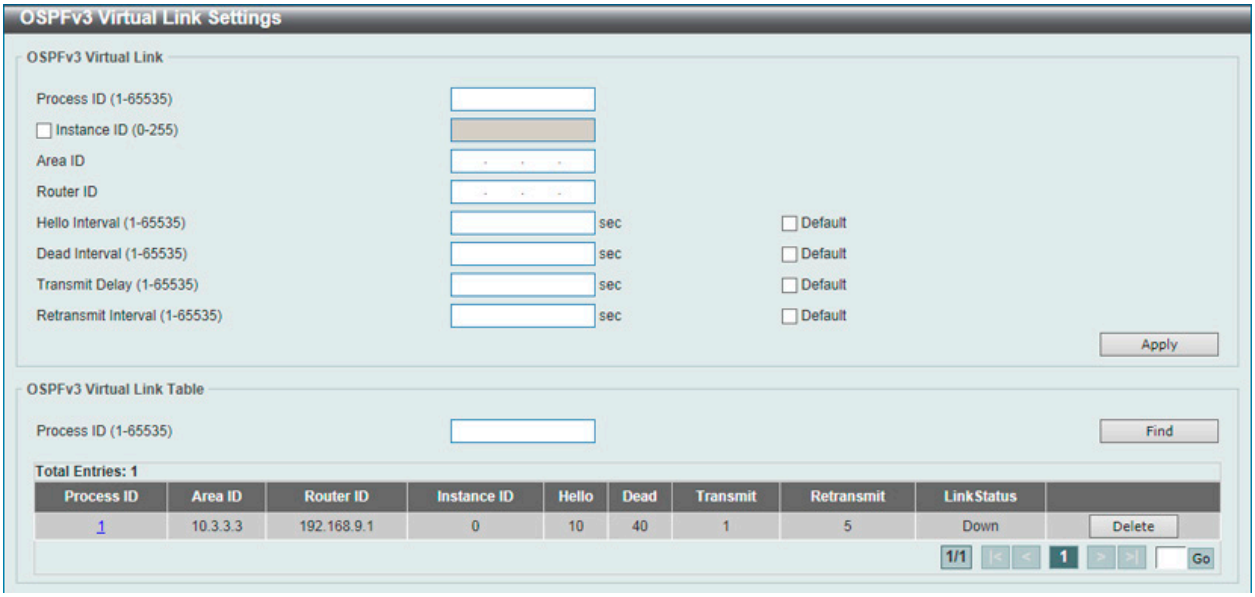


図 9-78　OSPFv3 Virtual Link Settings 画面

以下の項目を使用します。

項目	説明
Process ID	IPv6 OSPF ルーティングのプロセス ID（1-65535）を指定します。
Instance ID (0-255)	インタフェースのインスタンス ID（0-255）を入力します。初期値は 0 です。
Area ID	OSPFv3 ドメイン内の OSPFv3 エリアをユニークに識別する 32 ビットの番号を IPv4 アドレス形式で入力します。
Router ID	リモートエリアの OSPFv3 ルータ ID。
Hello Interval (1-65535)	OSPF Hello パケットの送出間隔（秒）を指定します。同じリンクの全ルータには同じ「Hello Interval」と「Dead Interval」が設定される必要があります。初期値は 10（秒）です。
Dead Interval (1-65535)	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（秒）を入力します。
Transmit Delay	「Transmit Delay」値（1-65533）を指定します。「Default」を指定すると初期値（1）を使用します。
Retransmit Interval	「Retransmit Interval」（再送信間隔）の値（1-65533 秒）を指定します。「Default」を指定すると初期値（5）を使用します。

「Apply」をクリックし、設定内容を適用します。

「Delete」をクリックすると指定のエントリを削除します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Process ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。

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

「Process ID」をクリックすると、以下の画面が表示されます。



図 9-79　OSPFv3 Virtual Interface Settings - Edit 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て以下の画面を表示します。

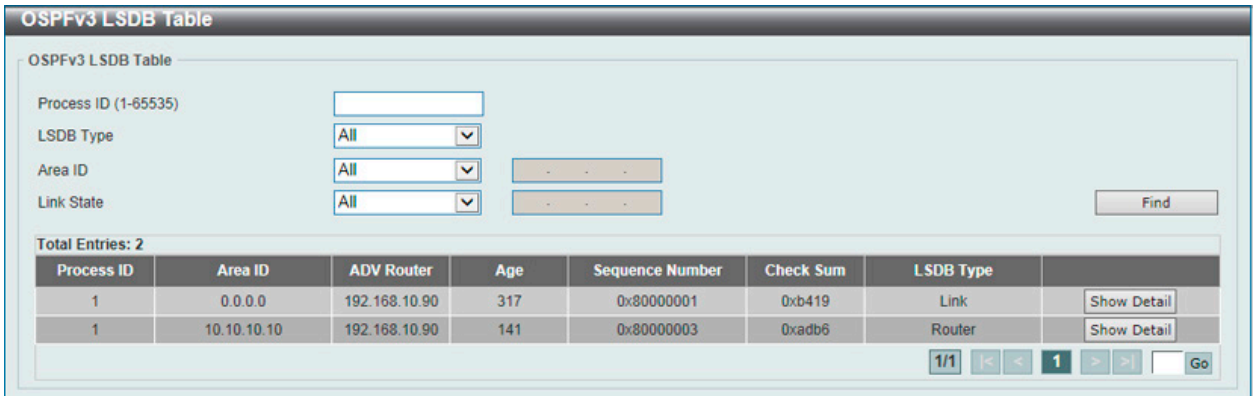


図 9-80　OSPFv3 LSDB Table 画面

以下の項目を使用します。

項目	説明
Process ID	IPv6 OSPF ルーティングプロセスの ID（1-65535）を指定します。ローカルにアサインされルータの各 IPv6 OSPF ルーティングプロセス固有である必要があります。
LSDB Type	表示する LSDB タイプを指定します。「All」「Router」「Network」「Prefix」「Link」「Inter-Area Prefix」「Inter-Area Router」「External」から選択します。 「All」- LSOB 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。
Area ID	エリア ID オプションを指定します。「All」「Area ID」から指定可能です。すべての LSA を指定のエリアから表示するには、「Area ID」を指定し、OSPF エリア ID を空欄に入力します。IPv4 アドレスの形式で指定します。
Link State	表示されるリンクステート情報を選択します。「All」「Self Originate」「Adv Router」から選択します。 「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、指定したエントリを検索します。

エントリの詳細表示

例えば「Router LSA」の下の「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 9-81　OSPFv3 LSDB Router LSA Table 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て以下の画面を表示します。



図 9-82　OSPFv3 Neighbor Table 画面

以下の項目を使用します。

項目	説明
Process ID	IPv6 OSPFv3 プロセスの ID（1-65535）を指定します。
Interface Name	Neighbor が組み込まれている IP インタフェースを指定します。
Neighbor	Neighbor のルータ 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、指定したエントリを検索します。

エントリの詳細表示

例えば「Router LSA」の下の「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 9-83　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。

OSPFv3 Border Router Table（OSPFv3 ボーダールーターテーブル）

OSPFv3 ボーダールーターについての情報を表示します。

L3 Features > OSPF > OSPFv3 > OSPFv3 Border Router Table の順にメニューをクリックして以下の画面を表示します。

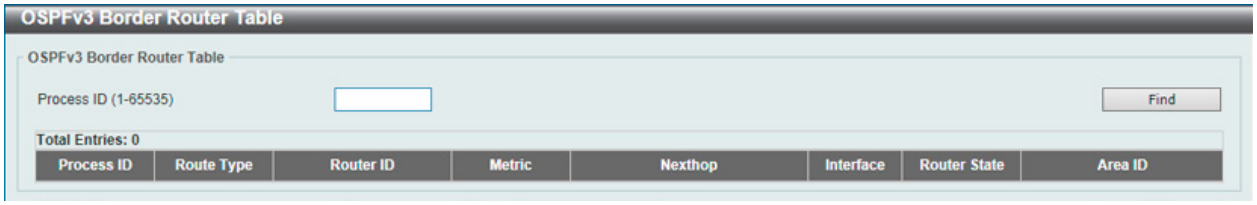


図 9-84　OSPFv3 Border Router Table 画面

以下の項目を使用します。

項目	説明
Process ID	IPv6 OSPF ルーティングプロセスの ID（1-65535）を指定します。

「Find」ボタンをクリックして、指定したエントリを検索します。

IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）

L3 Features > IP Multicast Routing Protocol

IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）の設定を行います。

IGMP（IGMP 設定）（EI/MI モードのみ）

L3 Features > IP Multicast Routing Protocol > IGMP

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

IGMP（Internet Group Management Protocol）は、IP インタフェースごとを基本にスイッチに設定されます。スイッチに設定した各 IP インタフェースは、以下の「IGMP Interface Settings」画面に表示されます。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Interface Settings の順にメニューをクリックして、以下の画面を表示します。



図 9-85　IGMP Interface Settings 画面

以下の項目を使用します。

項目	説明
Interface VLAN	本設定に使用する IP インタフェース VLAN を指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
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

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

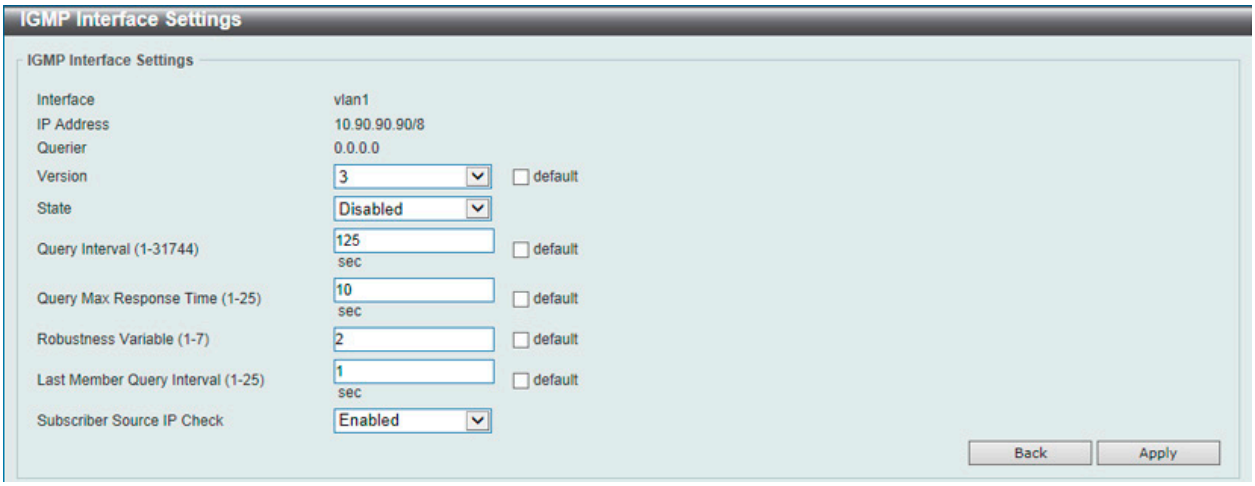


図 9-86　IGMP Interface Settings - Edit 画面

以下の項目を使用します。

項目	説明
Version	インタフェースにおける IGMP クエリを解釈するのに使用する IGMP のバージョンを選択します。 「Default」を指定すると初期値を使用します。
State	プルダウンメニューを使用して、IP インタフェースの IGMP を「Enabled」(有効)/「Disabled」(無効) にします。初期値は Disabled です。
Query Interval (1-31744)	IGMP クエリを送信する間隔（1-31744）を指定します。初期値は 125（秒）です。「Default」を指定すると初期値を使用します。
Query Max Response Time (1-25)	IGMP response report を送信するまでの最大時間（1-25 秒）を入力します。初期値は 10（秒）です。「Default」を指定すると初期値を使用します。

項目	説明
Robustness Variable (1-7)	大量のパケットの喪失が予想されるサブネットワークで許可される調整変数。1-7 の範囲で入力します。大量のパケットの喪失が予想されるサブネットワークでは大きい数値を使用します。初期値は 2 です。「Default」を指定すると初期値を使用します。
Last Member Query Interval (1-25)	Leave Group メッセージをへの応答で送信するものも含め。Group-Specific Query メッセージの送信間隔（1-25）を入力します。初期値は 1（秒）です。「Default」を指定すると初期値を使用します。
Subscriber Source IP Check	「subscriber source IP check」を有効 / 無効に指定します。初期値では、インタフェースとして、同じネットワーク内にの送信元 IP を指定するインタフェースに受信する IGMP リポートまたはリーブメッセージです。同じネットワークにない場合、メッセージ情報は IGMP プロトコルに学習されません。

2. 項目を編集後「Apply」ボタンをクリックします。
「Back」をボタンをクリックして前のページに戻ります。

注意 IGMP Snooping において Querier Emulation をご利用の環境で、Specific Query の間隔が設定値より短くなります。

IGMP Static Group Settings（IGMP スタティックグループ設定）

スイッチスタックにおける IGMP スタティックグループを設定します。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Static Group Table の順にメニューをクリックして以下の画面を表示します。

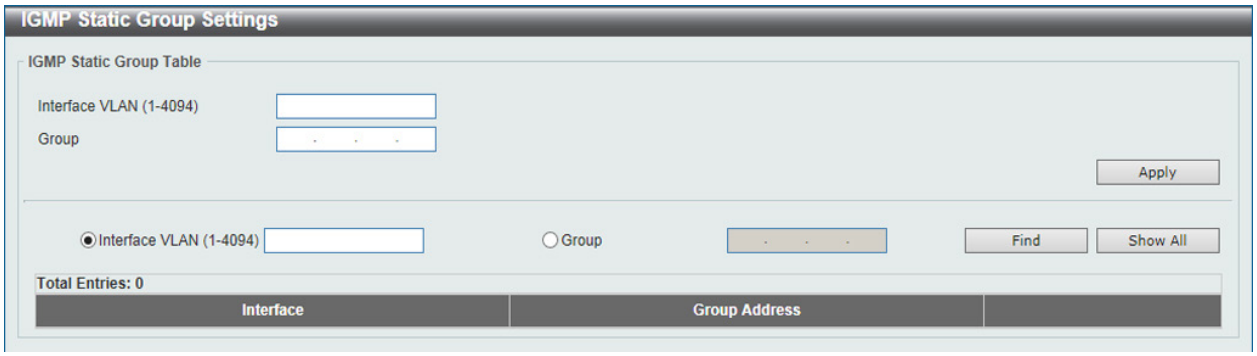


図 9-87　IGMP Static Group Settings 画面

以下の項目を使用します。

項目	説明
Interface VLAN	本設定に使用する IP インタフェース VLAN（1-4094）を指定します。
Group	マルチキャストグループ IP アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

IGMP Dynamic Group Table（IGMP ダイナミックグループテーブル）

本項目では、IGMP ダイナミックグループ情報の表示、設定を行います。IGMP バッファは同じサブネット内のホストであるダイナミックマルチキャストグループを含むリストを保有しています。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Dynamic Group Table の順にメニューをクリックして以下の画面を表示します。

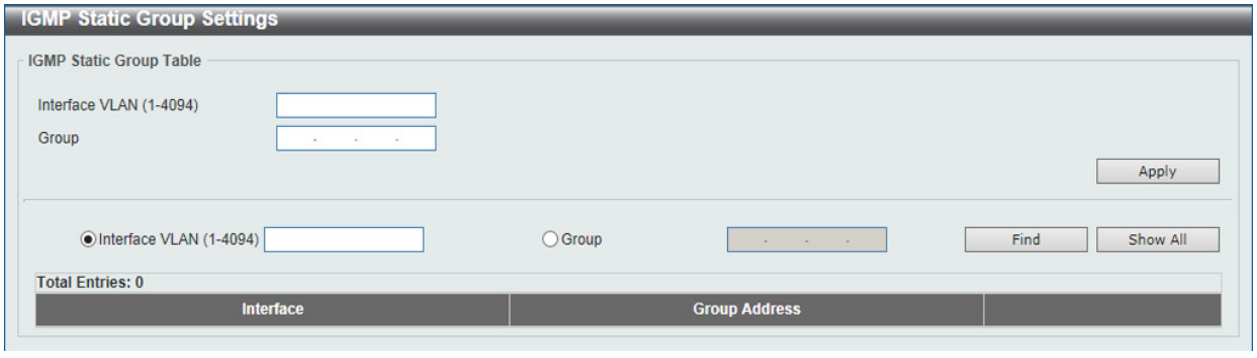


図 9-88　IGMP Dynamic Group Table 画面

以下の項目を使用します。

項目	説明
Interface VLAN	本設定に使用する IP インタフェース VLAN（1-4094）を指定します。
Group	マルチキャストグループ IP アドレスを指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Clear」をクリックすると入力したエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

IGMP SSM Mapping Settings（IGMP SSM マッピング設定）

本項目では、IGMP SSM マッピングの設定、表示を行います。「Source Specific Multicast」(SSM) の開発により、ネットワークサービスプロバイダは IP マルチキャストアドレスの管理を簡易に行うことが可能です。
SSM が有効な場合、「last hop」のルータは付属の IGMPv3 ホストから、SSM 範囲から破棄された INCLUDE リクエスト（S,G）を受信したチャネル（S,G）のソースベースツリーを構築します。
これらのケースは付属のホストが、(*, G) リクエストのみを提供する IGMPv1 または IGMPv2 ホストである場合です。SSM マッピングでは、リクエストされたマルチキャストグループが SSM 範囲内で落ちる場合、ルータは、ここで定義された送信元アドレスマッピングのグループアドレスに基づく、(*, G) から (S, G) へのリクエスト wp マップできるようになります。そしてルータはソースベースツリーをマップします (S, G)。もし複数のアソシエーションが存在する場合、ルータは (S, G) ソースベースツリーを各 S に構築します。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP SSM Mapping Settings の順にメニューをクリックして以下の画面を表示します。

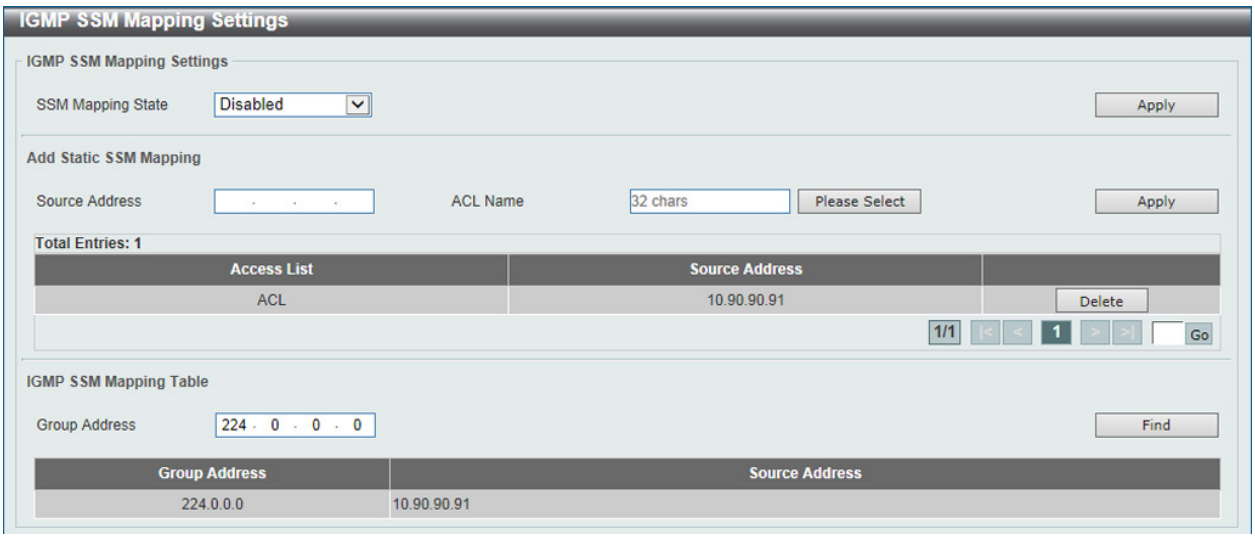


図 9-89　IGMP SSM Mapping Settings 画面

以下の項目を使用します。

項目	説明
IGMP SSM Mapping Settings	
SSM Mapping State	IGMPv1/IGMPv2 ホストのための SSM マッピング機能を有効 / 無効に指定します。
Add Static SSM Mapping	
Source Address	アクセスリストで定義されたグループの送信元アドレスを指定します。
ACL Name	マップされるマルチキャストグループを含む IP アクセスリスト名を指定します。グループを許可するには、送信元アドレスの項目に「any」を指定し、アクセスアドレスエントリの宛先アドレス項目にグループアドレスを指定します。「Please Select」を指定すると既存のアクセスリストを選択することも可能です。
IGMP SSM Mapping Table	
Group Address	IGMP マルチキャストグループアドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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

「Please Select」をクリックすると、次の画面を表示します。



図 9-90　IGMP SSM Mapping Settings (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。

MLD（MLD 設定）（EI/MI モードのみ）

Multicast Listener Discovery(MLD) は、IGMP が IPv4 ルータで使用されたように、IPv6 ルータによって使用され、直接接続するリンク上のマルチキャストリスナ (マルチキャストパケットの受信を希望するノード) の存在の検出し、どのマルチキャストアドレスが Neighbor ノードに関連するかを特に検出します。プロトコルは別々のプロトコルを使用する代わりに ICMPv6 に埋め込まれています。MLDv1 は IGMPv2,MLDv2 は IGMPv3 に似ています。

MLD Interface Settings（MLD インタフェース設定）

MLD インタフェース設定を行います。

L3 Features > IP Multicast Routing Protocol > MLD > MLD Interface Settings の順にメニューをクリックして以下の画面を表示します。

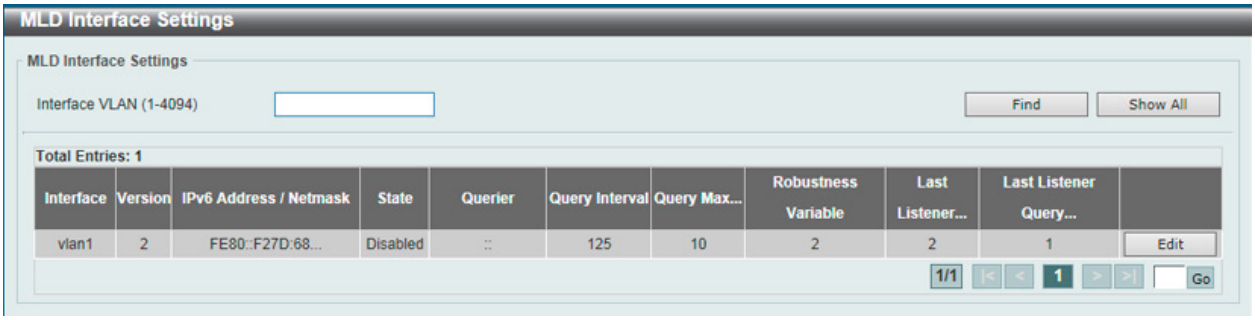


図 9-91　MLD Interface Settings 画面

以下の項目を使用します。

項目	説明
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

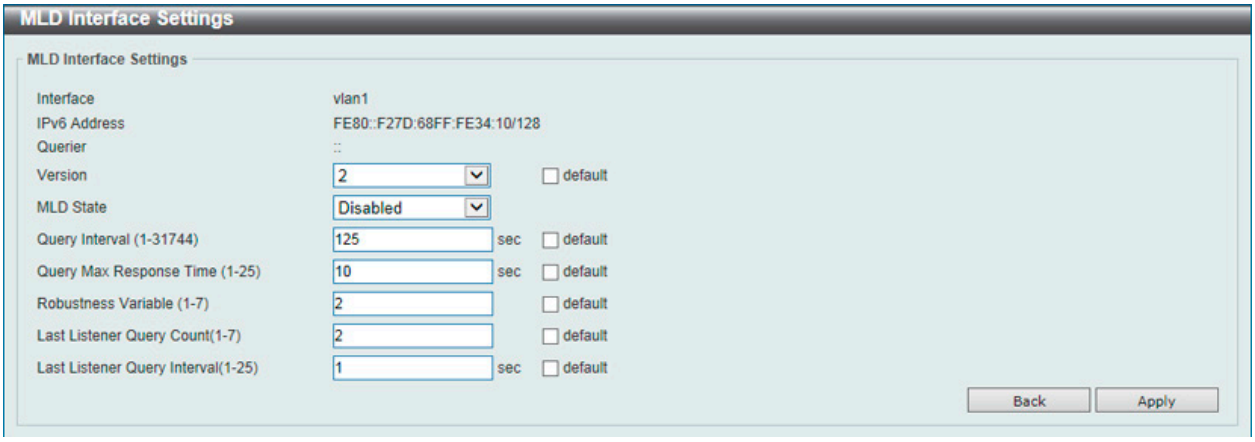


図 9-92　MLD Interface Settings - Edit 画面

以下の項目を使用します。

項目	説明
Version	送信するインタフェースおよび処理するパケットバージョンを決定する MLD バージョンを選択します。 1-2 から選択可能です。「Default」を指定すると初期値（MLDv2）を使用します。
MLD State	プルダウンメニューを使用して、IP インタフェースの MLD を「Enabled」(有効)/「Disabled」(無効) にします。初期値は「Disabled」です。
Query Interval (1-31744)	MLD クエリの送出間隔（1-31744）を指定します。初期値は 125（秒）です。「Default」を指定すると初期値を使用します。
Query Max Response Time	MLD response report を送信するまでの最大時間（1-25 秒）を入力します。初期値は 10（秒）です。「Default」を指定すると初期値を使用します。
Robustness Variable (1-7)	大量のパケットの喪失が予想されるサブネットワークで許可される調整変数。2-7 の範囲で入力します。大量のパケットの喪失が予想されるサブネットワークでは大きい数値を使用します。初期値は 2 です。「Default」を指定すると初期値を使用します。
Last Listener Query Count	ラストメンバクエリカウント値 (1-7) を指定します。ルータがグループ内にローカルメンバがいないと認識する前に、「group-specific」または「group-source specific」クエリ送信の設定を行います。ルータがタイムアウトまでにホストからレポートを受領しない場合、ルータはインタフェースのマルチキャストグループトラフィックの送信を中止します。「Default」を指定すると初期値（2）を使用します。
Last Member Query Interval (1-25)	Leave Group メッセージをへの応答で送信するものも含め、Group-Specific Query メッセージの送信間隔 (1-25) を入力します。初期値は 1（秒）です。「Default」を指定すると初期値を使用します。

「Apply」ボタンをクリックして行った変更を適用します。
「Back」をボタンをクリックして前のページに戻ります。

MLD Static Group Settings（MLD スタティックグループ設定）

MLD スタティックグループ設定を行います。付属のホストが MLD プロトコルをサポートしていない場合に MLD スタティックグループを作成します。設定すると、グループメンバエントリが MLD キャッシュに追加されます。

L3 Features > IP Multicast Routing Protocol > MLD > MLD Static Group Settings の順にメニューをクリックして以下の画面を表示します。

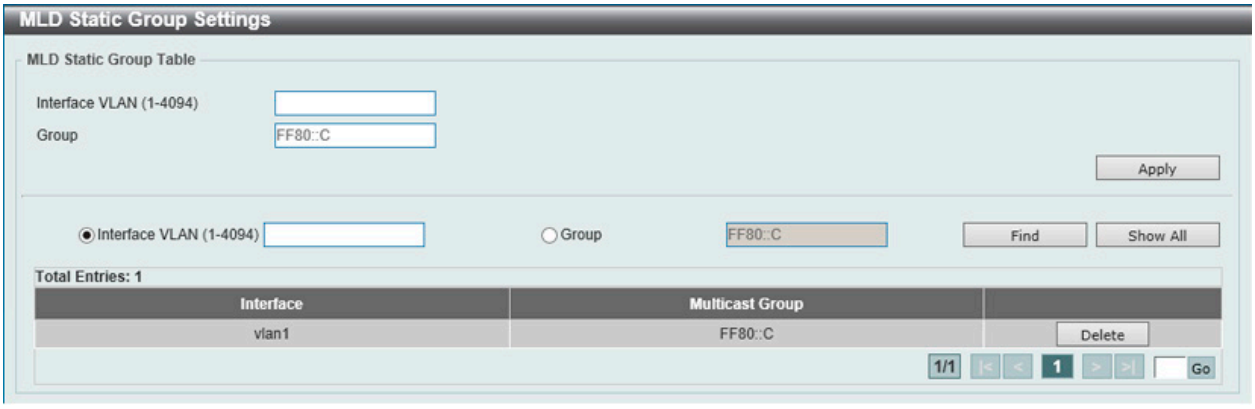


図 9-93　MLD Static Group Settings 画面

以下の項目を使用します。

項目	説明
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
Group	IPv6 マルチキャストグループアドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

MLD Group Table（MLD グループテーブル）

スイッチにおける MLD スタティックグループを表示します。

L3 Features > IP Multicast Routing Protocol > MLD > MLD Group Table の順にメニューをクリックして以下の画面を表示します。



図 9-94　MLD Group Table 画面

以下の項目を使用します。

項目	説明
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
Group	IPv6 グループアドレスを入力します。

「Find」ボタンをクリックして、入力したインタフェースを検出します。
「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

MLD SSM Mapping Settings（MLD SSM マッピング設定）

本項目では、MLD SSM マッピングの設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > MLD > MLD SSM Mapping Settings の順にメニューをクリックして以下の画面を表示します。

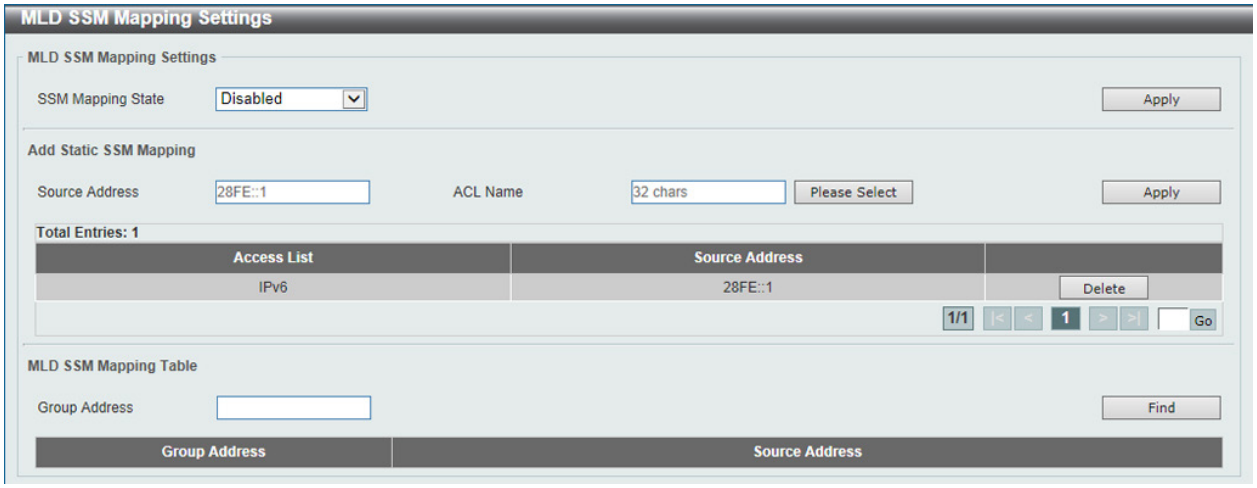


図 9-95　MLD SSM Mapping Settings 画面

以下の項目を使用します。

項目	説明
MLD SSM Mapping Settings	
SSM Mapping State	MLD SSM マッピング機能を有効 / 無効に指定します。
Add Static SSM Mapping	
Source Address	アクセスリストで定義されたグループの送信元アドレスを指定します。
ACL Name	マップされるマルチキャストグループを含む IPv6 アクセスリスト名（32 字以内）を指定します。「Please Select」を指定すると既存のアクセスリストを選択することも可能です。
MLD SSM Mapping Table	
Group Address	IPv6 マルチキャストグループアドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Please Select」をクリックすると、次の画面を表示します。



図 9-96　MLD SSM Mapping Settings (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。

IGMP Proxy（IGMP プロキシ）（EI/MI モードのみ）

IGMP プロキシは、IGMP フォワーディングに基づいてアップストリームでは IGMP のホスト部分を、ダウンストリームでは IGMP のルータ部分を実行して、エッジボックスなどのデバイスに VLAN を横切るマルチキャストトラフィックを複製します。これによりコアネットワークに送信される IGMP コントロールパケット数を削減します。

IGMP Proxy Settings（IGMP プロキシ設定）

IGMP プロキシの状態と IGMP プロキシのアップストリームインタフェースを設定します。

L3 Features > IP Multicast Routing Protocol > IGMP Proxy > IGMP Proxy 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。

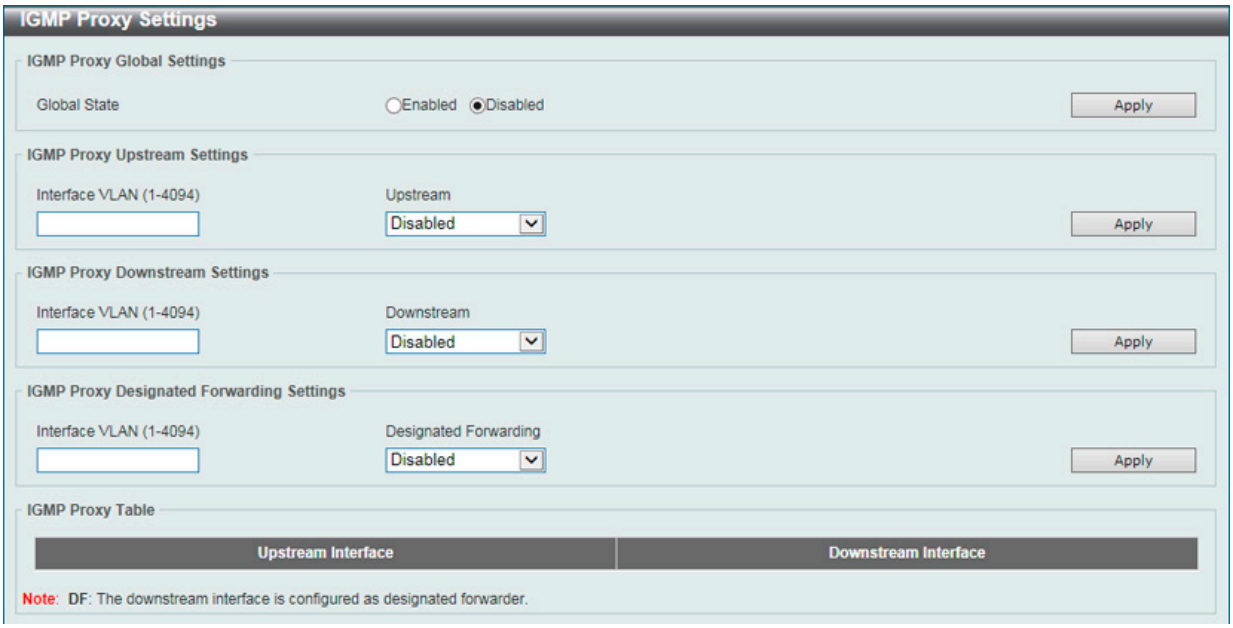


図 9-97　IGMP Proxy Settings 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
IGMP Proxy Global Settings	
Global State	ラジオボタンを使用して IGMP プロキシのグローバル状態を「Enabled」(有効)/「Disabled」(無効) にします。
IGMP Proxy Upstream Settings	
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
Upstream	アップストリーム IGMP プロキシとしてのインタフェースを有効 / 無効に指定します。
IGMP Proxy Downstream Settings	
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
Downstream	ダウンストリーム IGMP プロキシとしてのインタフェースを有効 / 無効に指定します。
IGMP Proxy Designated Forwarding Settings	
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
Designated Forwarding	ノンクエリア IGMP プロキシダウンストリームインタフェースでの指定転送について有効 / 無効に指定します。複数の IGMP ベース転送者によるダウンストリームリンクの、ローカルループとリダンダント（冗長）トラフィックを避けるために、IGMP プロキシは LAN の単一の転送者を選出するために、IGMP クエリアエレクションを使用します。このオプションによりノンクエリアデバイスが転送者になります。本機能はインタフェースがダウンストリームインタフェースでない場合、またはアップストリームインタフェースの場合には有効にはなりません。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

IGMP Proxy Group Table（IGMP プロキシグループテーブル）

IGMP プロキシグループ設定を参照します。

L2 Features > L2 Multicast Control > IGMP Proxy > IGMP Proxy Group 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。

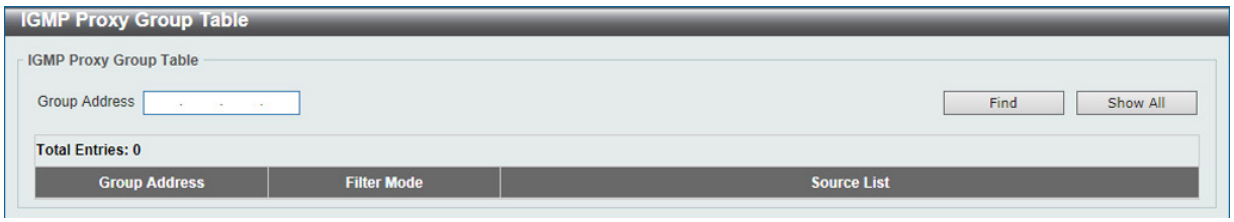


図 9-98　IGMP Proxy Group 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Group Address	IPv4 グループマルチキャストアドレスを入力します。

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

IGMP Proxy Forwarding Table（IGMP フォワーディングテーブル）

IGMP プロキシのフォワーディング情報を検索、表示します。

L3 Features > IP Multicast Routing Protocol > IGMP Proxy > IGMP Proxy Forwarding 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。

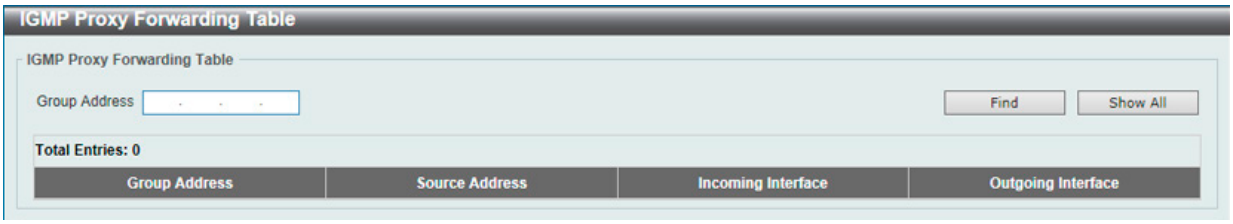


図 9-99　IGMP Proxy Forwarding Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Group Address	IPv4 グループマルチキャストアドレスを入力します。

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

MLD Proxy（MLD プロキシ）（EI/MI モードのみ）

MLD プロキシはアップストリームインタフェースでホストの役割を果たします。MLD Report パケットはルータポートに送信されます。MLD プロキシはダウンストリームインタフェースでルータの役割を果たします。これによりコアネットワークに送信される MLD コントロールパケット数を削減します。

MLD Proxy Settings（MLD プロキシ設定）

MLD プロキシの状態と MLD プロキシのアップストリームインタフェースを設定します。

L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy 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。

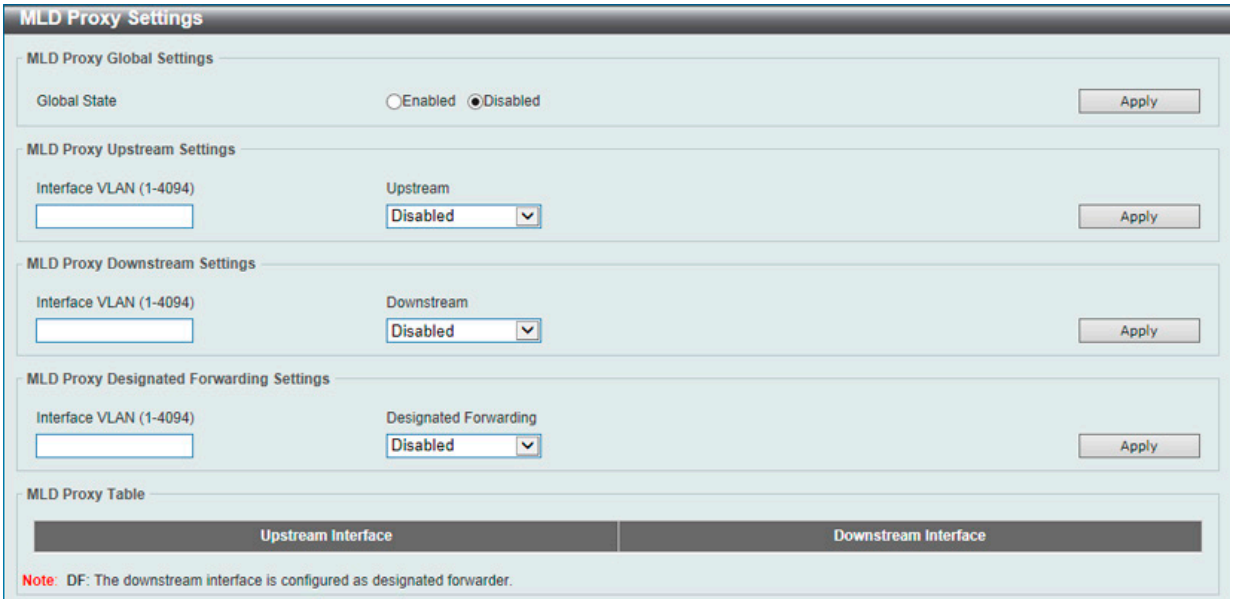


図 9-100　MLD Proxy Settings 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
MLD Proxy Global Settings	
Global State	ラジオボタンを使用して MLD プロキシのグローバル状態を「Enabled」(有効)/「Disabled」(無効) にします。
MLD Proxy Upstream Settings	
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
Upstream	アップストリーム MLD プロキシとしてのインタフェースを有効 / 無効に指定します。
MLD Proxy Downstream Settings	
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。

項目	説明
Downstream	ダウンストリーム MLD プロキシとしてのインタフェースを有効 / 無効に指定します。
MLD Proxy Designated Forwarding Settings	
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
Designated Forwarding	ノンクエリア MLD プロキシダウンストリームインタフェースでの指定転送について有効 / 無効に指定します。複数の MLD ベース転送者によるダウンストリームリンクの、ローカルループとリダンダント（冗長）トラフィックを避けるために、MLD プロキシは LAN の単一の転送者を選出するために、MLD クエリアエレクションを使用します。このオプションによりノンクエリアデバイスが転送者になります。本機能はインタフェースがダウンストリームインタフェースでない場合、またはアップストリームインタフェースの場合には有効にはなりません。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

MLD Proxy Group Table（MLD プロキシグループテーブル）

MLD プロキシグループテーブルを参照します。

L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy Group 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。

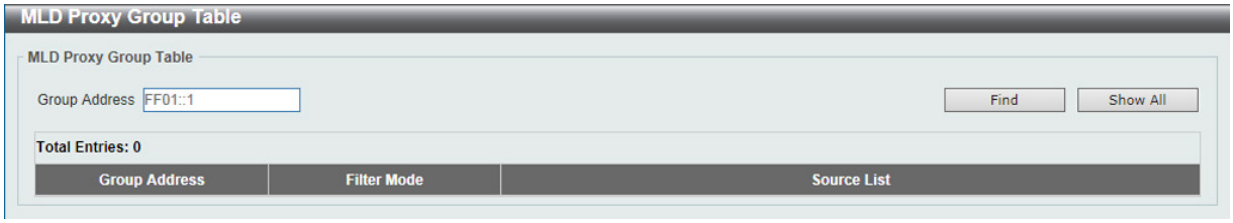


図 9-101　MLD Proxy Group Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Group Address	IPv6 グループマルチキャストアドレスを入力します。

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

MLD Proxy Forwarding Table（MLD フォワーディングテーブル）

MLD プロキシのダウンストリームインタフェースを設定します。MLD プロキシのダウンストリームインタフェースは MLD Snooping が有効な VLAN である必要があります。

L3 Features > IP Multicast Routing Protocol > MLD Proxy > MLD Proxy Forwarding 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。

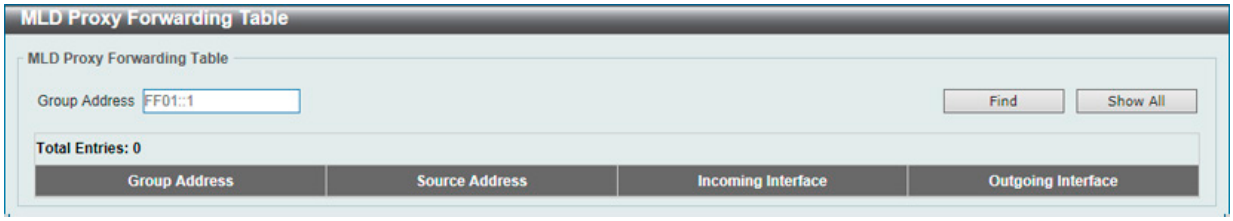


図 9-102　MLD Proxy Forwarding Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Group Address	IPv6 グループマルチキャストアドレスを入力します。

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

DVMRP（EI/MI モードのみ）

L3 Features > IP Multicast Routing Protocol > DVMRP

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

DVMRP インタフェース設定を行います。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Interface Settings の順にメニューをクリックして以下の画面を表示します。



図 9-103 DVMRP Interface Settings 画面

以下の項目を使用します。

項目	説明
Interface Name	DVMRP のインタフェース名を入力します。

「Find」ボタンをクリックして、入力したインタフェースを検出します。
「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの編集

1. 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。

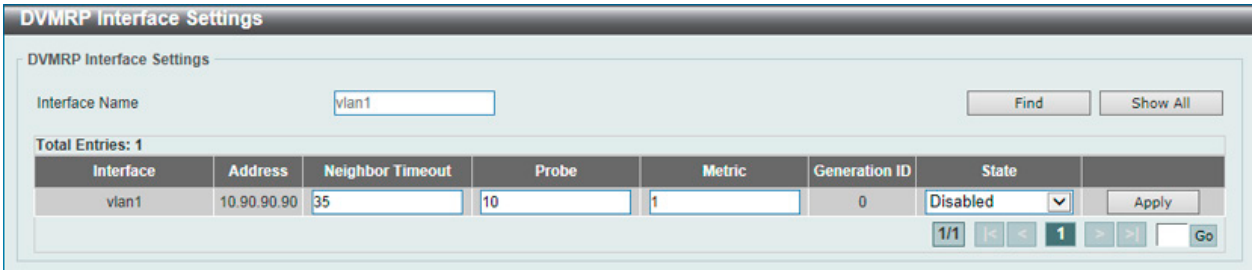


図 9-104 DVMRP Interface Settings 画面 - Edit

以下の項目を使用します。

項目	説明
Neighbor Timeout	ネイバライフタイム値（1-65535 秒）を指定します。ルータがネイバからのプルーブメッセージをネイバタイムアウトまで受領しない場合、ネイバはダウンします。初期値は 35 です。
Probe	DVMRP プルーブインターバル（1-65535 秒）を指定します。初期値は 10 です。
Metric	メトリック値（1-32）を指定します。「32」は不達を意味します。各ソースネットワークにレポートされるのは、レポートされたルートのルートメトリックになります。メトリックはルータ起源のレポートとソースネットワーク間のインタフェースメトリックの総量になります。DVMRP ではメトリック「32」は不達を意味します。これにより全 DVMRP ネットワーク間の広がりを制限し、プロトコルの収束時間の上限値として必要な値です。
State	指定インタフェースでの DVMRP 機能を有効 / 無効に指定します。

2. 項目を編集後「Apply」ボタンをクリックします。

DVMRP Routing Table（DVMRP ルーティングテーブル）

スイッチにおける DVMRP ルーティングテーブルを表示します。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Routing Table の順にメニューをクリックして以下の画面を表示します。



図 9-105　DVMRP Routing Table 画面

以下の項目を使用します。

項目	説明
Source Network	送信先の IPv4 ネットワークアドレスとネットマスクを入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

DVMRP Neighbor Table（DVMRP Neighbor テーブル）

スイッチにおける DVMRP Neighbor テーブルを表示します。

L3 Features > IP Multicast Routing Protocol > DVMRP > DVMRP Neighbor Table の順にメニューをクリックして以下の画面を表示します。

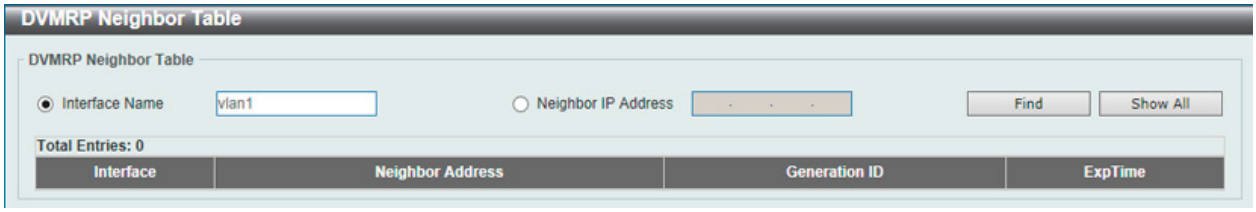


図 9-106　DVMRP Neighbor Table 画面

以下の項目を使用します。

項目	説明
Interface Name	インタフェース名を入力します。
Neighbor IP Address	ネイバの IP アドレスを入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

PIM（PIM 設定）（EI/MI モードのみ）

L3 Features > IP Multicast Routing Protocol > PIM

PIM (Protocol Independent Multicast) は、LAN、WAN またはインターネット上にデータの 1 対多および多対多の配布を提供する IP（Internet Protocol）ネットワーク用のマルチキャストルーティングプロトコルのファミリです。PIM は、自身のトポロジ検出メカニズムを含まないため、プロトコルに依存しませんが、RIP または OSPF など他の従来型ルーティングプロトコルが提供するルーティング情報を使用します。本スイッチは PIM, Dense Mode (PIM-DM)、Sparse Mode (PIM-SM)、PIM Source Specific multicast (PIM-SSM)、および Sparse-Dense Mode (PIM-DM-SM) の 4 つの PIM タイプをサポートしています。

PIM-SM（Protocol Independent Multicast-Sparse Mode）

Sparse Mode (PIM-SM) は、基本的なユニキャストルーティング情報または個別のマルチキャストが可能なルーティング情報をベースに使用できるマルチキャストルーティングプロトコルです。これは、グループごとの RP（Rendezvous Point）を元に単方向の共有ツリーを構築し、オプションで送信元ごとに最短パスツリーを作成します。

PIM-SM は、ネットワークをマルチキャストパケットでフラッドさせる多くのマルチキャストルーティングプロトコルと異なり、Rendezvous Point(RP) を使用して、トラフィックを明示的にマルチキャストグループの一部であるルータに対し転送します。この RP は PIM-SM が有効であるルータからすべてのリクエストを取得し、その情報を分析してネットワーク内でリクエストしているルータに対して送信元から受信したマルチキャスト情報を返します。この方法を通じ、配信ツリーは、ルートとしての RP とともに作成されます。この配信ツリーは、すべての PIM-SM が有効である全ルータを保持しています。RP はこれらのルータから収集した情報をここに保存しています。

多くのルータがマルチアクセスネットワークの一部である場合に、代表ルータ (DR) が選出されます。DR の第一の機能は RP に Join/Prune メッセージを送信することです。LAN 上で最も高いプライオリティを持つルータが DR として選出されます。最も高いプライオリティへの接続がある場合、より高い IP アドレスを持つルータが選出されます。

PIM-SM 設定で作成される 3 番目のルータタイプは、Boot Strap Router(BSR) です。BSR の目的は、RP 情報を収集し、LAN 上の PIM-SM が有効であるルータにリレーすることです。RP はスタティックに設定されますが、BSR メカニズムが RP を決定することもできます。複数の Candidate BSR(C-BSR) がネットワーク上に設定されますが、1 つの BSR だけが、RP 情報を処理するために選出されます。どの C-BSR が、BSR になるかが明白でない場合、すべての C-BSR は、PIM-SM が有効であるネットワークに Boot Strap Messages(BSM) を放出し、より高いプライオリティを持つ C-BSR が BSR として選出されます。一度決定されると、BSR は、PIM-SM ネットワークで Candidate RP から送信される RP データを収集し、それを編集し、周期的な BSM を使用して LAN 上に送信します。すべての PIM-SM ルータは Boot Strap メカニズムから RP 情報を取得し、データベースに保持します。

マルチキャストグループの検出（Discovery）と接続（Join）

Hello パケットは PIM-SM ルータを検出しますが、これらのルータは DR と RP 間で交換される Join/Prune メッセージを使用することでマルチキャストグループからの接合または「Pruned」を行います。Join/Prune メッセージは、マルチキャストデータを受信するためにどのインタフェースがあるのか、またはないのかを効果的に記述しているルータ間で中継されるパケットです。これらのメッセージは、頻繁に設定されネットワーク上に送信され、Hello パケットがはじめに受信される場合にだけルータに有効となります。Hello パケットは、ルータが存在し、RP の配信ツリーの一部になる準備中であることを簡単に記述しています。ルータが IGMP グループのメンバを受け入れて、PIM-SM が有効である場合、興味があるルータは明確な Join/Prune メッセージを RP に送信します。それは、送信元から興味があるルータにマルチキャストデータを順番に送信し、グループのための一定方向の配布ツリーを作成します。マルチキャストパケットは、その後これらのツリー上の全ノードに送信されます。一度 Prune メッセージが RP の送信ツリーのメンバであるルータに受信されると、ルータはその配信ツリーからそのインタフェースを削除します。

配信ツリー

2 つのタイプの配信ツリーが PIM-SM プロトコル、Rendezvous-Point Tree(RPT) および最短経路ツリー (Shortest Path Tree:SPT) に存在します。RP は、マルチキャストデータを受信することが可能なすべての外向きインタフェースに、送信元から受信した特定のマルチキャストデータを送信します。しかし、一度ルータが送信元の位置を決定すると、SPT は、RP などの送信元と送信先の間のホップを除去して作成されます。これは、マルチキャストデータ転送速度のしきい値を設定することで設定されます。しきい値を越えると、データの経路は SPT に切り換えます。従って、より近いリンクが送信元と宛先の間で作成され、以前に使われたホップを取り除き、マルチキャストパケットが送信元から最終到達先に送信される時間を短縮します。

Register と Register Suppression メッセージ

マルチキャストソースは、いつも意図する受信グループに接合するわけではありません。最初のホップルータ (DR) は、グループのメンバでなくても、または明示された送信元も持たなくてもマルチキャストデータを送信することができます。それは本質的に、この情報を RP 配信ツリーに中継する方法についての情報を持っていないと言うことを意味しています。この問題は、Register と Register-Stop メッセージを通じて緩和されます。DR が受信したはじめのマルチキャストパケットがカプセル化され、RP に送信されます。RP は逆にカプセル化を解いて RP 配信ツリーの下に向かってパケットを送信します。ルートが確立すると、SPT が作成され、ルータを直接ソースに接続するか、マルチキャストトラフィックフローを開始して、DR から RP への通信を行います。後者の場合、カプセル化されているタイプとカプセル化されていないタイプで同じパケットが 2 回送信される可能性があります。RP はこの不備を検出し、カプセル化されたパケットの送信を停止するようにリクエストをしている DR に Register-stop メッセージを戻します。

Assert メッセージ

PIM-SM が使用可能なネットワークにおいて、時々パラレルパスが送信元から受信先に対して作成されます。これは複数の受信先が 2 回同じマルチキャストパケットを受信することを意味しています。この状況を改善するために、Assert メッセージが受信デバイスから両方のマルチキャストソースに送信され、どのルータが受信者に必要なマルチキャストデータを送信するかを決定します。最短メトリック (ホップカウント) を持つ送信元がプライマリマルチキャストソースとして選出されます。このメトリックは Assert メッセージ内に含まれています。

PIM-SSM

SSM（Source Specific Multicast）機能は、IP マルチキャストの拡張機能です。ここではデータトラフィックは受信者が明確に参加しているというマルチキャスト送信元だけから受信者に送信されます。SSM 範囲のマルチキャストグループにおいて、送信元を指定したマルチキャスト配信ツリー (共有ツリーはない) だけが作成されます。

IANA（Internet Assigned Numbers Authority）は SSM アプリケーションとプロトコルのために 232.0.0.0 ～ 232.255.255.255 のアドレス範囲を予約しています。スイッチは IP マルチキャストアドレス範囲 224.0.0.0 ～ 239.255.255.255 の任意のサブセットに SSM を設定できます。

PIM-DM

PIM-DM(Protocol Independent Multicast-Dense Mode) プロトコルは、オーバヘッド削減の目的ではなく、マルチキャストパケットの配送を保証するために利用されるため、低遅延で高帯域のネットワークに適したプロトコルです。

PIM-DM マルチキャストルーティングプロトコルは、下流のルータがマルチキャストメッセージの受信を希望していると仮定し、下流のルータからのプルーンメッセージ (削除メッセージ) を受けて、マルチキャスト配信ツリーから、マルチキャストグループメンバの存在しない枝葉を Pruned します (削除します)。

PIM-DM には明示的な “Join" メッセージは存在しません。その代わりに、すべてのインタフェースマルチキャストメッセージの定期的なフラッディングに依存し、タイマの期限切れ (Join/Prune インターバル) を待つか、または下流のルータが明示的な “Prune" メッセージを送信して、その枝にはマルチキャストメンバが存在しない旨を示すのを待ちます。PIM-DM はその後マルチキャスト配信ツリーからこれらの枝を削除します。

マルチキャスト配信ツリーから刈り込まれた枝も、マルチキャスト配信グループへの参加を (将来的に) 希望している可能性があります。そのため、プロトコルは定期的にデータベースから “Prune(削除)" 情報を削除し、その枝のすべてのインタフェース宛てにマルチキャストメッセージのフラッディングを行います。この、“Prune" 情報の削除を行う間隔が Join/Prune インターバルです。

PIM-SM-DM

PIM-SM では、RP は送信側の最初のホップルータです。最初のホップは、送信側がいつデータを送信するか RP を持っていないと、パケットを破棄し、何も実行しません。Sparse-Dense モードはこの条件で有益です。Sparse-Dense モードで、パケットがすべての外向きのインタフェースでフラッドし、pruning/joining(prune/graft) が RP が検出されない場合にと外向きのインタフェースを制御することが可能です。つまり、PIM Sparse-Dense モードは、マルチキャストグループがどのモードで操作するかによって操作の Sparse モードまたは Dense モードのどちらかで扱われます。インタフェースがマルチキャストトラフィックを受信する場合、グループに既知の RP があれば、インタフェースの現在の操作モードは Sparse モードになり、そうでない場合、インタフェースの現在の操作モードは Dense モードになります。

PIM for IPv4（IPv4 用 PIM の設定）

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4

PIM Interface（PIM インタフェース設定）

PIM インタフェースの設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Interface の順にメニューをクリックして以下の画面を表示します :

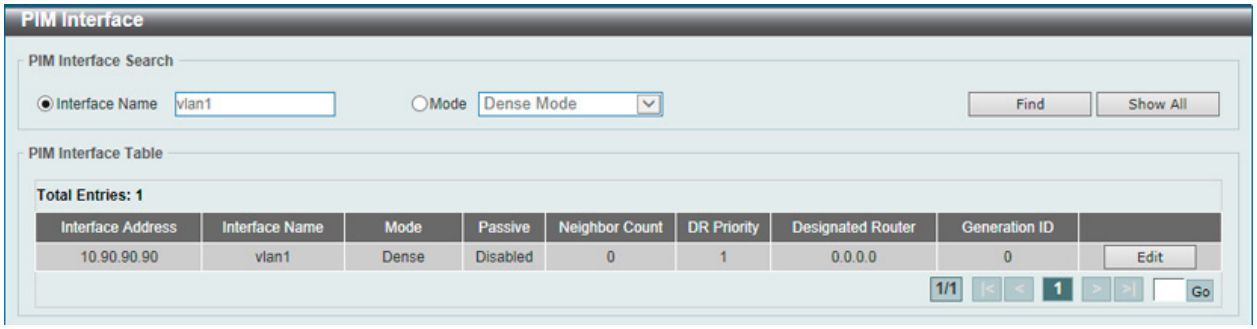


図 9-107 PIM Interface Settings 画面

以下の項目を使用します。

項目	説明
Interface Name	インタフェース名を指定します。

項目	説明
Mode	使用する PIM プロトコルのタイプ (Sparse Mode(SM)、Dense Mode(DM)、または Spare-Dense Mode(SM-DM)) を選択します。初期値は「DM」です。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

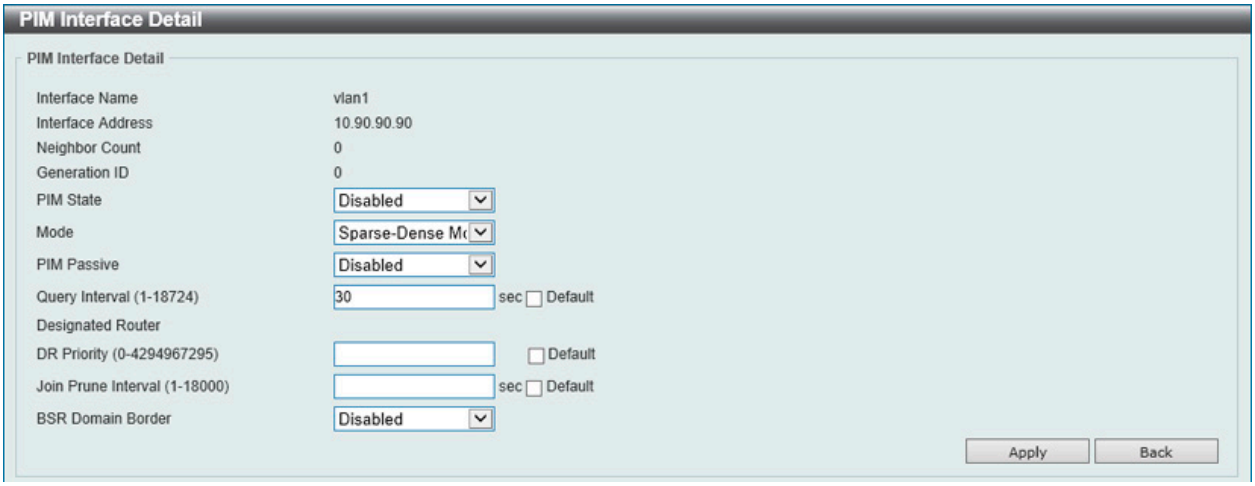


図 9-108 PIM Interface Settings - Edit 画面

以下の項目を使用します。

項目	説明
PIM State	PIM を「Enabled」(有効)/「Disabled」(無効) にします。初期値は Disabled です。
Mode	使用する PIM プロトコルのタイプ (Sparse Mode(SM)、Dense Mode(DM)、または Spare-Dense Mode(SM-DM)) を選択します。初期値は「DM」です。 • Dense Mode -「PIM-DM」送信元が送信を開始した時、すべてのダウンストリームルータはマルチキャストデータストリームの受信を希望します。基本的にはマルチキャストデータストリームはダウンストリームルータとグループメンバのインタフェースでフラッドします。ダウンストリームルータやグループメンバがない場合、ルータはマルチキャストデータが必要とされていないことを示すプルーンメッセージを送信します。 • Sparse Mode - マルチキャストトラフィックが「Sparse Mode」のインタフェースに受信すると、最初のホップルータは登録メッセージをカプセル化し、RP へ送信します。ルータがファーストホップでない場合、mroute エントリを元にトラフィックは転送されます。「sparse」モードインタフェースは mroute メンバインタフェースのように混雑した状態となり、ダウンストリームルータから、または sprse モードインタフェースのグループメンバ からのジョインメッセージを受信します。PIM ジョインプロセスはシェアツリーまたはソースツリーの作成を開始します。 • Sparse-Dense Mode - インタフェースが「PIM Sparse-Dense」モードとして設定されると、インタフェースから受信したマルチキャストグループはどちらの「sparse」/「dense」モードでも操作が可能になります。インタフェースがマルチキャストトラフィックを受信すると、グループの RP を学習済みの場合、グループは「sparse」モードで操作されます。そうでない場合マルチキャストグループは「dense」モードで動作します。
PIM Passive	PIM パッシブ機能を有効 / 無効に指定します。パッシブモードが有効の場合、インタフェースは PIM の送信も、PIM メッセージの受信も行いません。ルータはネットワークで唯一の PIM ルータとして動作します。本機能は LAN に PIM ルータが一つのみある場合、使用します。
Query Interval (1-18724)	この IP インタフェースから 1 ホップ隣の隣接ルータに Hello パケットを送信する間隔を設定します。これらの Hello パケットは他の PIM が有効なルータを検出し、PIM が有効なネットワーク上の DR としてプライオリティを指定するために使用されます。1-18724(秒) で指定します。初期値は 30(秒) です。
DR Priority (0-4294967295)	IP インタフェースのマルチアクセスネットワークで DR になるためのプライオリティを入力します。0-4294967295 で入力します。初期値は 1 です。
Join Prune Interval (1-18000)	どのマルチキャストグループが PIM の有効なネットワークに接合し、そのグループから削除または「Pruned」を設定する Join/Prune パケットを送信する間隔を設定します。1-18000(秒) で指定します。初期値は 60(秒) です。
BSR Domain Border	「Bootstrap Router」(BSR) ドメインボーダー機能を有効 / 無効に指定します。PIM は有効なインタフェースでのみ有効です。インタフェースでこの機能を使用すると、ドメイン間の BSR メッセージを交換を回避するために、他のドメインを隣接させます。

2. 項目を編集後「Apply」ボタンをクリックします。
「Back」をボタンをクリックして前のページに戻ります。

PIM BSR Candidate（PIM BSR Candidate 設定）

PIM が有効なネットワークで Boot Strap Router(BSR) になるために、Candidate Boot Strap Router(C-BSR) 設定と指定 IP インタフェースのプライオリティを設定します。Boot Strap Router はネットワーク上のどのルータがマルチキャストグループに対して RP として選出され、他の PIM-SM が有効なルータに RP 情報を収集して、配布するのかを決定する情報を保持しています。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM BSR Candidate の順にメニューをクリックして以下の画面を表示します。

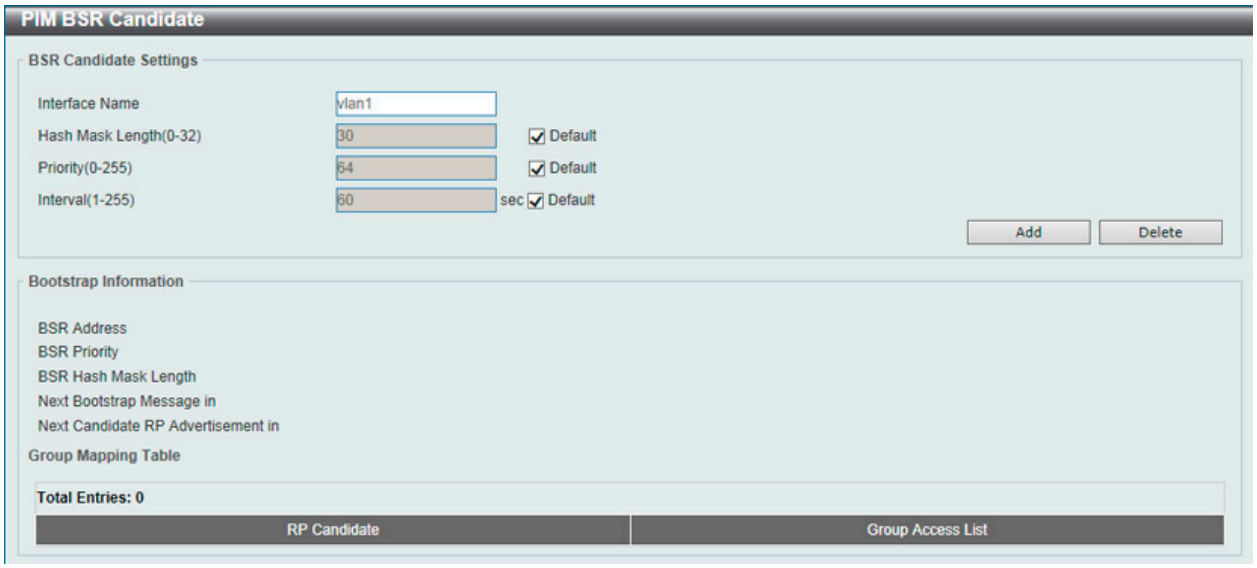


図 9-109 PIM BSR Candidate 画面

以下の項目を使用します。

項目	説明
Interface name	インタフェース名を入力します。
Hash Mask Length	ハッシュマスク長を入力します。これは Candidate RP の IP アドレスとマルチキャストグループアドレスと共に使用されます。ルータに使用されるハッシュアルゴリズムが PIM-SM の有効なネットワークでどの C-RP が RP になるかを決定するために計算します。0-32 で指定します。初期値は 30 です。
Priority	「Candidate Bootstrap Router」(CBSR) プライオリティ値（0-255）を指定します。最優先値での設定が望まれます。優先値が同じ場合、最高値の IP アドレスを持つルータが優先的になります。「Default」を指定すると初期値（64）を使用します。
Interval	スイッチが PIM の有効なネットワークに Boot Strap Messages(BSM) を送信する間隔を 1-255 で入力します。初期値は 60(秒) です。

「Apply」ボタンをクリックして行った変更を適用します。
「Delete」をクリックすると指定のエントリを削除します。

PIM RP Address（PIM RP アドレス設定）

本画面では RP マッピングを行うスタティックマルチキャストグループの設定、表示を行います。マルチキャストドメインでは RP マッピングのスタティックマルチキャストグループは BSR とともに使用されます。すべてのドメイン内のルータは RP マッピングに矛盾のないマルチキャストグループを保持する必要があります。レジスタメッセージを起動する最初のホップルータは、指定グループに向けられた PIM レジスタメッセージを送信するための RP を決定するマッピングエントリを使用します。ジョインメッセージを起動する最後のホップルータは、指定グループに向けられたジョイン / プルーンメッセージを送信するための RP を決定するマッピングエントリを使用します。ルータがジョインメッセージを受信すると、メッセージ転送のためにマッピングエントリをチェックします。RP がレジスタメッセージを受信する時、ルータがマルチキャストグループへの正しい RP でない場合、レジスタ停止メッセージが送信されます。複数の RP が単一のアクセスリストとともに定義されます。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Address の順にメニューをクリックして以下の画面を表示します。

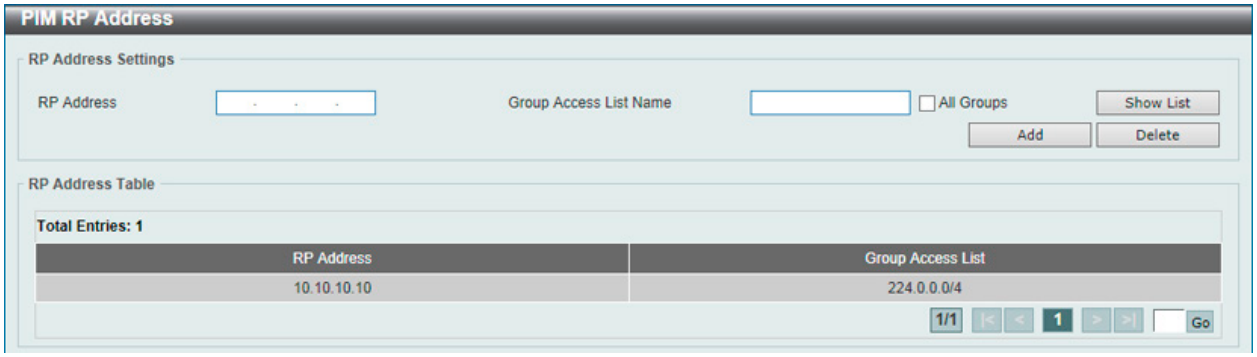


図 9-110 PIM RP Address 画面

以下の項目を使用します。

項目	説明
RP Address	RP IPv4 アドレスを入力します。
Group Access List Name	使用する通常のアクセスリストを指定します。「Show List」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。「All Groups」を指定すると「RP」を全マルチキャストグループにマップします。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの登録

「Add」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。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

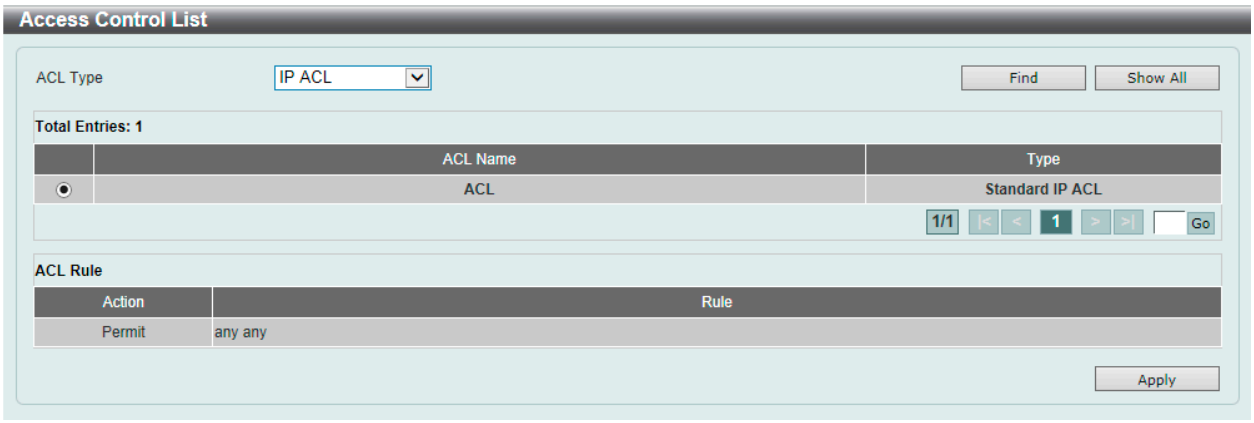


図 9-111　PIM RP Address (Show List) 画面

以下の項目を使用します。

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。 「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Apply」をクリックし、設定内容を適用します。

PIM RP Candidate（PIM RP Candidate 設定）

本画面では PIM RP Candidate の設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Candidate の順にメニューをクリックして以下の画面を表示します。

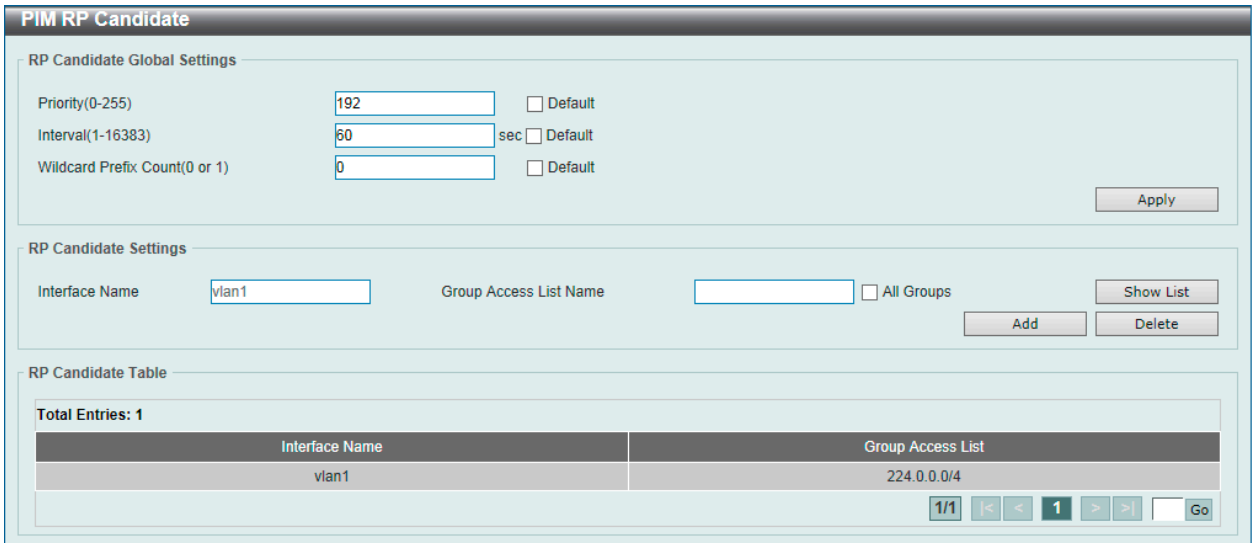


図 9-112　PIM RP Candidate 画面

以下の項目を使用します。

項目	説明
RP Candidate Global Settings	
Priority	「candidate RP」プライオリティ値（0-255）を指定します。「Default」を指定すると初期値（192）を使用します。
Interval	「candidate RP」を送信する間隔を 1-16383 で入力します。Default」を指定すると初期値（60 秒）を使用します。
Wildcard Prefix Count	C-RP メッセージのマルチキャストグループアドレスワイルドカード (224.0.0.0/4) プリフィクスカウント値（0-1）を指定します。「Default」を指定すると初期値（0）を使用します。
RP Candidate Settings	
Interface name	インタフェース名を入力します。
Group Access List Name	使用する通常のアクセスリストを指定します。「Show List」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。「All Groups」を指定すると「RP」を全マルチキャストグループにマップします。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの登録

「Add」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。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

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

「Show List」をクリックすると、以下の画面が表示されます。

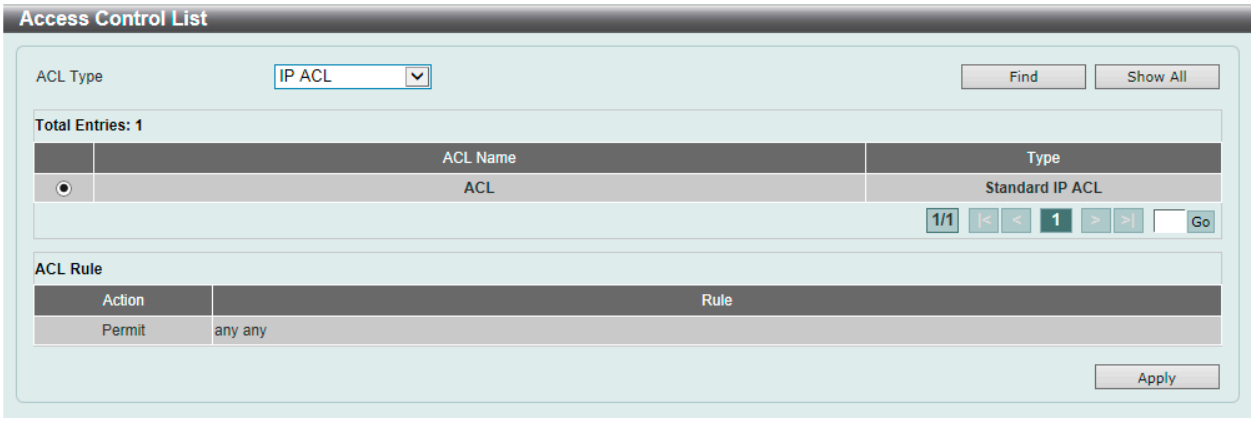


図 9-113　PIM RP Candidate (Show List) 画面

以下の項目を使用します。

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。 「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Apply」をクリックし、設定内容を適用します。

PIM RP Table（PIM RP テーブル）

本画面では PIM RP 情報の検索、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Table の順にメニューをクリックして以下の画面を表示します。

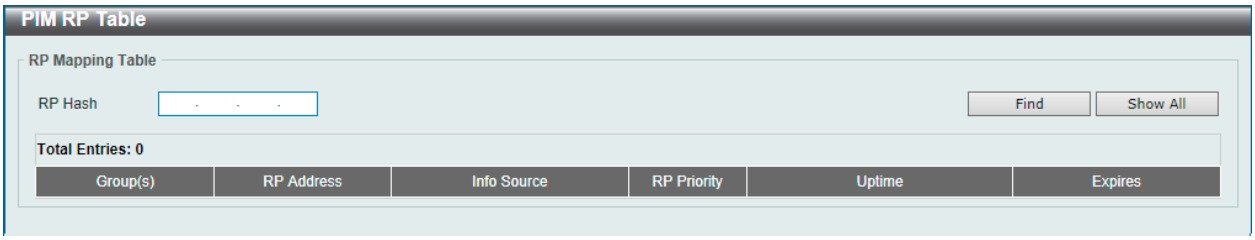


図 9-114　PIM RP Table 画面

以下の項目を使用します。

項目	説明
RP Hash	IPv4 マルチキャストグループアドレスを指定します。

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

PIM Register Settings（PIM レジスタ設定）

本画面では PIM レジスタの設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Register Settings の順にメニューをクリックして以下の画面を表示します。

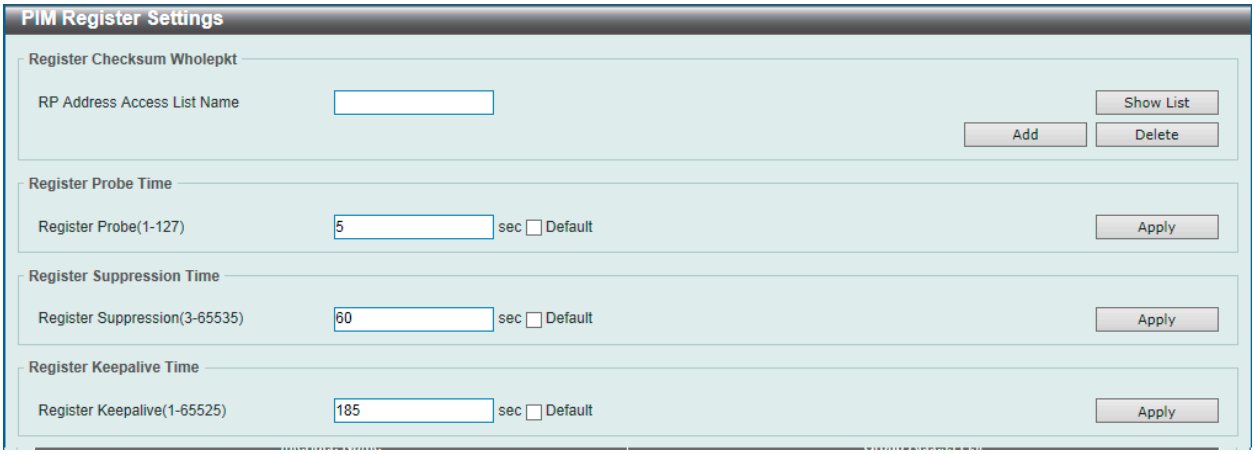


図 9-115　PIM Register Settings 画面

以下の項目を使用します。

項目	説明
Register Checksum Wholepkt	
RP Address Access List Name	使用する通常のアクセスリストを指定します。「Show List」をクリックして既存のアクセスリストを指定することも可能です。
Register Probe Time	
Register Probe	Register-Stop メッセージの再送を起こすように DR が Null-Register を RP に送信する場合に Register-Stop Timer (RST) が期限切れになるまでの時間を入力します。「Default」を選択すると初期値（5 秒）を指定します。
Register Suppression Time	
Register Suppression	レジスタ抑止タイムアウト値（3-65535）を入力します。DR がレジスタ停止メッセージを受領すると、抑止タイマが指導します。抑止の間、DR は RP へのレジスタメッセージを停止します。最初のホップルータで本機能を使用します。レジスタプローブタイムはレジスタ停止タイマのネガティブ値を防ぐためにも、レジスタ抑止タイムの半分以下である必要があります。最少タイマ値は「3」です。「Default」を選択すると初期値（60 秒）を指定します。

項目	説明
Register Keepalive Time	
Register Keepalive	キープアライブ間隔（1-65525 秒）を入力します。「Default」を選択すると初期値（185 秒）を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの登録

「Add」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。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

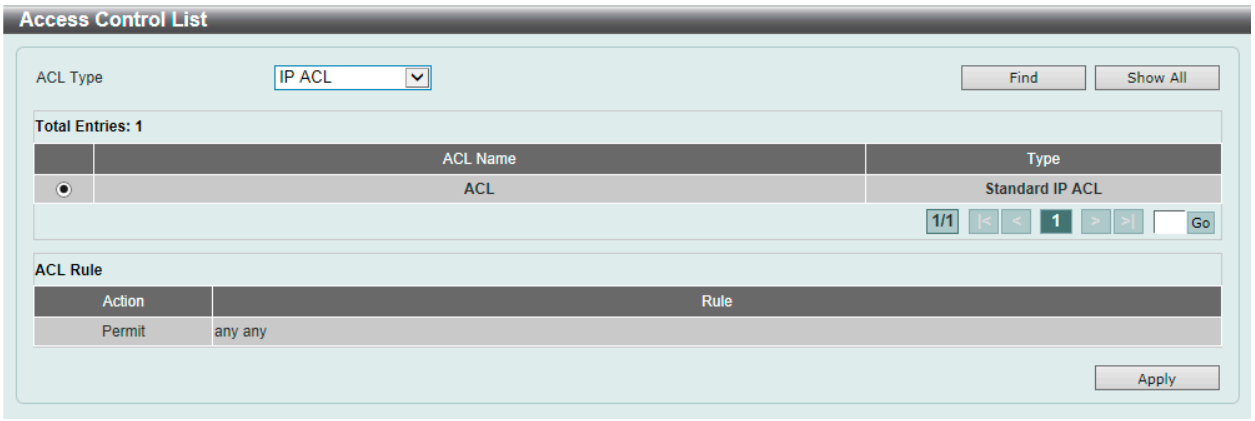


図 9-116 Show List 画面

以下の項目を使用します。

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。 「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」をクリックして、すべてのエントリを表示します。

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

「Apply」をクリックし、設定内容を適用します。

PIM SPT Threshold Settings（PIM SPT しきい値設定）

本画面では PIM SPT しきい値を表示、設定します。最後のホップルータで使用します。PIM-SM モードだと、送信元からのマルチキャストトラフィックは「RPT シェアツリー」を通じて受信者へフローされます。最初のパケット最後のホップルータに受信されると、トラフィックの各グループは、次の二つのモードのどちらかで操作可能です。「Infinity」モードだとトラフィックはシェアツリーのフォローし、「0」モードの場合、ソースツリーが構築され、トラフィックスイッチオーバがソースツリーに向かいます。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM SPT Threshold Settingsの順にメニューをクリックして以下の画面を表示します。

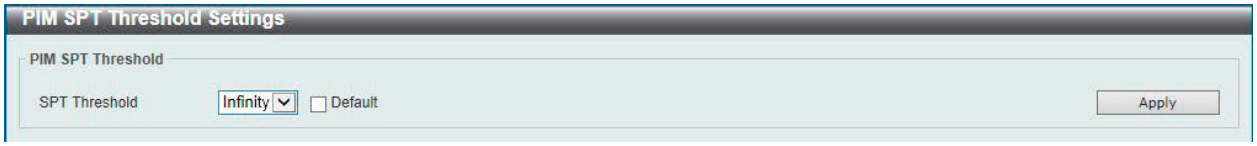


図 9-117 PIM SPT Threshold Settings 画面

以下の項目を使用します。

項目	説明
SPT Threshold	SPT しきい値を指定します。 「0」- 最初のパケットの到着でソースツリーを構築します。 「Infinity」- シェアツリーに依存します。 「Default」を選択すると初期値（Infinity）を指定します。

「Apply」をクリックし、設定内容を適用します。

PIM SSM Settings（PIM SSM 設定）

本画面では PIM SSM の設定、表示を行います。最後のホップルータでのみ使用可能です。SSM が有効な場合、最後のホップルータは、添付のホストから SSM 範囲内で破棄される (S,G) リクエストを含む IGMPv3 を受信するチャンネル (S,G) のソースベースツリーの構築を開始します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM SSM Settings の順にメニューをクリックして以下の画面を表示します。

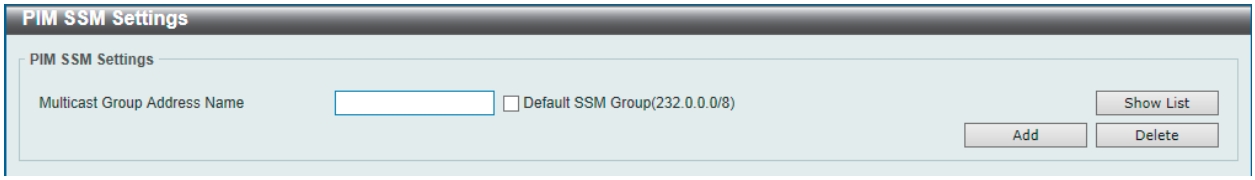


図 9-118 PIM SSM Settings 画面

以下の項目を使用します。

項目	説明
Multicast Group Address Name	ユーザ指定 SSM グループアドレスを定義する通常の IP アクセスリストを指定します。グループアドレスはルールエントリの宛先 IP アドレス項目で定義されます。「Show List」から既存のアクセスリストを指定することも可能です。「Default SSM Group」(232.0.0.0/8) オプションを指定すると、初期値の SSM グループアドレス（232/8）を指定します。

エントリの登録

「Add」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。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

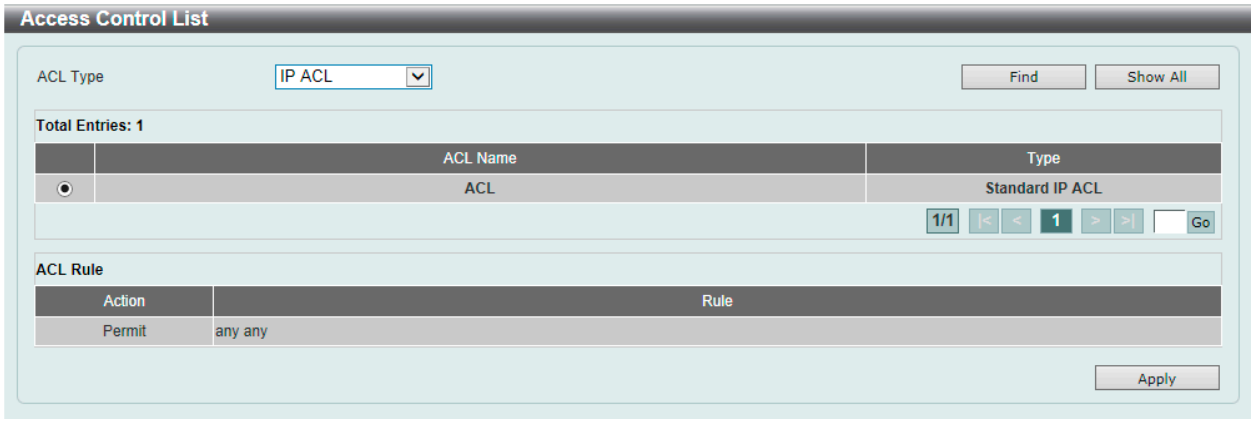


図 9-119 Show List 画面

以下の項目を使用します。

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。 「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Apply」をクリックし、設定内容を適用します。

PIM Neighbor Table（PIM ネイバテーブル）

本画面では PIM ネイバ情報の検索、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Neighbor Table の順にメニューをクリックして以下の画面を表示します。

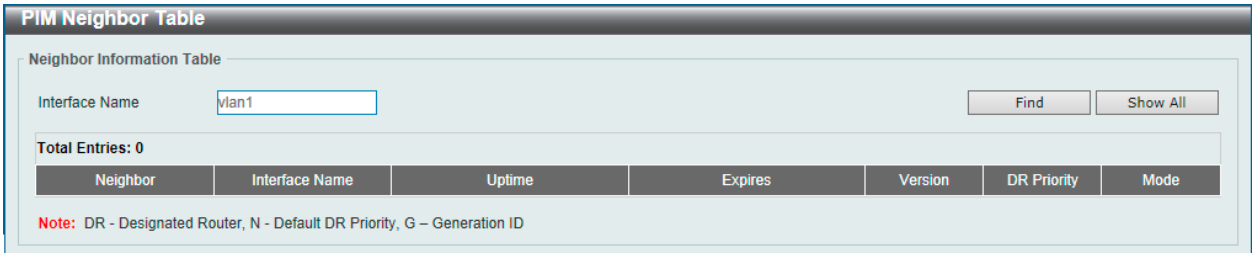


図 9-120　PIM Neighbor Table 画面

以下の項目を使用します。

項目	説明
Interface Name	PIM-SM ネイバ情報を表示する VLAN インタフェースを指定します。

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

PIM for IPv6（IPv6 用 PIM の設定）

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6

PIM for IPv6 Interface（PIM IPv6 インタフェース設定）

PIM IPv6 インタフェースの設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Interface の順にメニューをクリックして以下の画面を表示します：

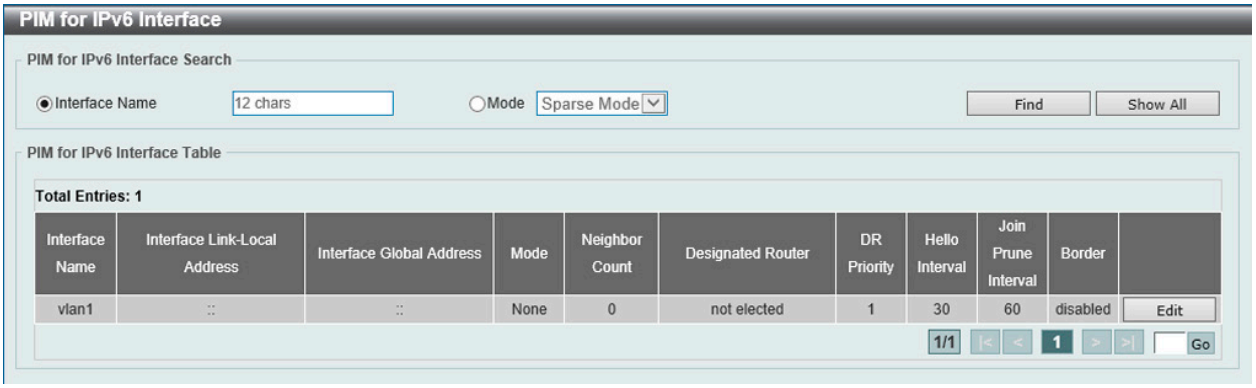


図 9-121　PIM for IPv6 Interface 画面

以下の項目を使用します。

項目	説明
Interface Name	VLAN インタフェース名を指定します。
Mode	フィルタ検索における IPv6 PIM エントリの操作モードを「Sparse Mode」「Dense Mode」から指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

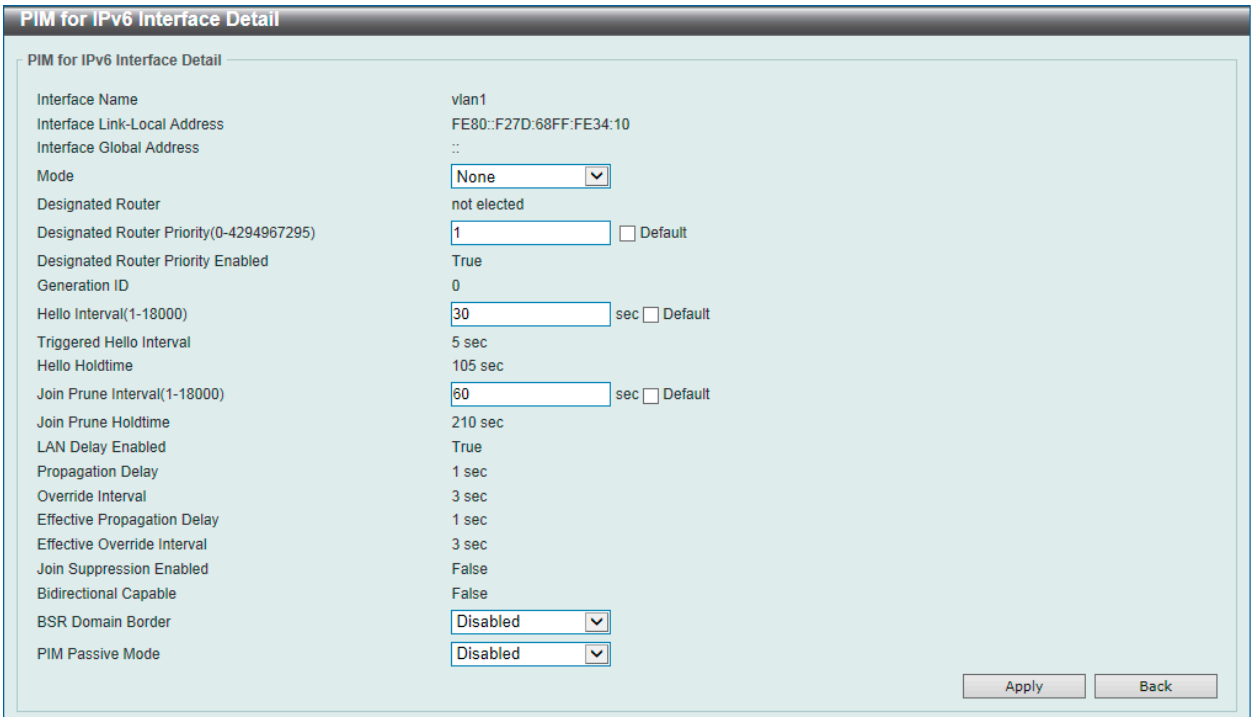


図 9-122　PIM for IPv6 Interface (Edit) 画面

以下の項目を使用します。

項目	説明
Mode	使用する IPv6 PIM プロトコルのタイプ（「None」「Sparse Mode（SM）」「Dense Mode」）を選択します。
Designated Router Priority (0-4294967295)	本インタフェースに送信される IPv6 の PIM Hello メッセージの DR Priority（DR 優先度）オプションに挿入される Designated Router Priority（代表ルータ優先度）値を入力します。この値が高いほど高い優先度を示します。
Hello Interval (1-18000)	この IP インタフェースから 1 ホップ隣の隣接ルータに Hello パケットを送信する間隔を設定します。これらの Hello パケットは他の PIM が有効なルータを検出し、PIM が有効なネットワーク上の SM としてプライオリティを指定するために使用されます。1-18000(秒) で指定します。初期値は 30(秒) です。
Join Prune Interval (0-18000)	本ルータが IPv6 インタフェースのこの PIM に IPv6 の PIM Join/Prune メッセージを送信する頻度を入力します。0 の値は「無限」の間隔を示しており、定期的な IPv6 の PIM Join/Prune メッセージがこのインタフェースに送信されるべきではないことを示します。
BSR Domain Border	プルダウンメニューを使用して、IPv6 PIM ドメインの境界のとなるインタフェースを「Enabled」(有効)/「Disabled」(無効) にします。このインタフェースが境界を設定すると、Bootstrap（BSR）ルータメッセージがそこを経由して送信または受信されることを防止します。
PIM Passive Mode	PIM パッシブ機能を有効 / 無効に指定します。パッシブモードが有効の場合、インタフェースは PIM の送信も、PIM メッセージの受信も行いません。ルータはネットワークで唯一の PIM ルータとして動作します。本機能は LAN に PIM ルータが一つのみある場合、使用します。

2.　項目を編集後「Apply」ボタンをクリックします。

「Back」をボタンをクリックして前のページに戻ります。

PIM for IPv6 BSR Candidate Settings（PIM for IPv6 BSR Candidate 設定）

本項目では「IPv6 PIM BSR candidate」設定を行います。「PIM-SM」の動作にのみ影響を与えます。これによりルータは全ての PIM ネイバに BSR アドレスとしての宛先インタフェースのアドレスとともに、「bootstrap」メッセージを送信するようになります。「PIM-SM」ドメインは RP 情報の通知と収集に責任のある固有の「BSR」(Bootstrap Router) を含んでいる必要があります。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 BSR Candidate Settings の順にメニューをクリックして以下の画面を表示します。

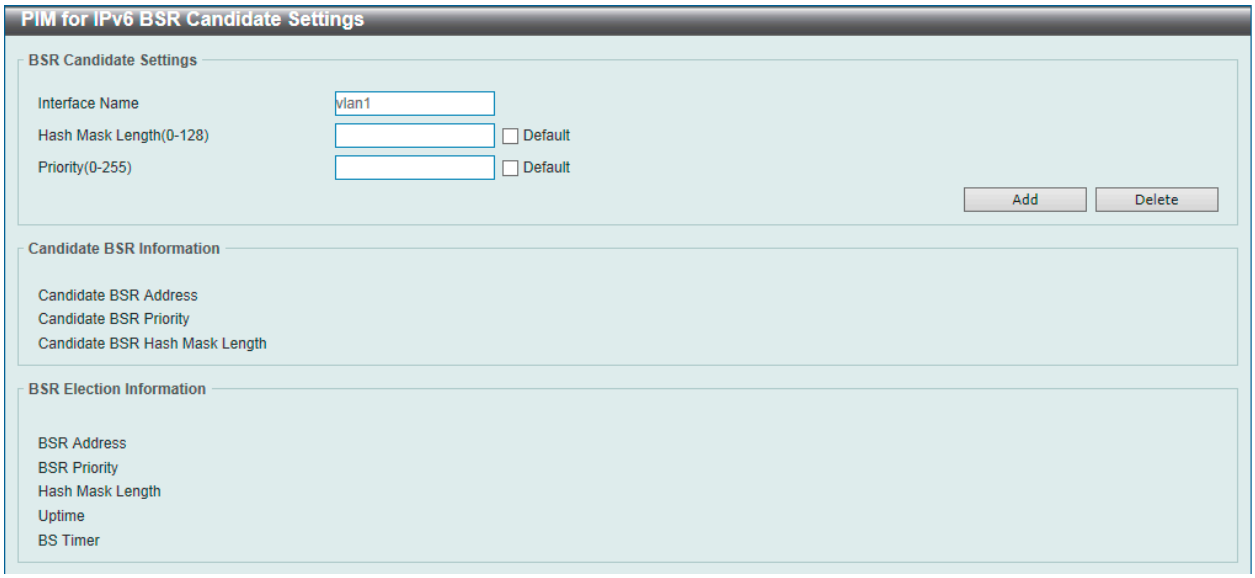


図 9-123　PIM for IPv6 BSR Candidate Settings 画面

以下の項目を使用します。

項目	説明
Interface name	インタフェース VLAN 名を入力します。
Hash Mask Length	ハッシュマスク長を入力します。これは Candidate RP の IP アドレスとマルチキャストグループアドレスと共に使用されます。ルータに使用されるハッシュアルゴリズムが PIM-SM の有効なネットワークでどの C-RP が RP になるかを決定するために計算します。0-128 で指定します。初期値は 126 です。
Priority	「Candidate Bootstrap Router」(CBSR) プライオリティ値（0-255）を指定します。最優先値での設定が望まれます。優先値が同じ場合、最高値の IP アドレスを持つルータが優先的になります。「Default」を指定すると初期値 (64) を使用します。

「Add」をクリックし、入力した情報に基づくエントリを追加します。
「Delete」をクリックすると指定のエントリを削除します。

PIM for IPv6 BSR Table（PIM for IPv6 BSR テーブル）

本項目は「IPv6 PIM BSR」情報を表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 BSR Table の順にメニューをクリックして以下の画面を表示します。



図 9-124　PIM for IPv6 BSR Table 画面

PIM for IPv6 RP Address（PIM for IPv6 RP アドレス）

本画面では IPv6 PIM RP アドレスの設定、表示を行います。「PIM-SM」の動作にのみ影響を与えます。
「sparse」モードで動作するマルチキャストグループの RP アドレスを手動で定義します。一つ以上のグループに単一の RP を使用します。アクセスリストによって設定された条件により、どのグループが RP を使用するのかを決定します。複数の RP が定義可能で、それぞれ単一のアクセスリストを保持します。新しい設定内容は古いものを上書きします。
ドメインの全てのルータは RP マッピングに有効なマルチキャストグループを保持している必要があります。レジスタメッセージを起動する最初のホップルータは、指定グループへの PM レジスタメッセージを送信する RP を決定するマッピングエントリを使用します。ジョインメッセージを起動する最後のホップルータは、指定グループへのジョイン / プルーンメッセージを送信する RP を決定するマッピングエントリを使用します。ルータがジョインメッセージを受信すると、メッセージの転送にマッピングエントリをチェックします。RP がレジスタメッセージを受信する時、マルチキャストグループにとってルータが正しい RP でない場合、レジスタ停止メッセージが送信されます。
PIM ドメインが埋め込まれた RP を使用する場合、RP は手動で「埋め込み RP 範囲」の RP として設定されます。他のルータが IPv6 グループアドレスからの RP アドレスを発見します。それらのルータがスタティック RP を埋め込み RP の代わりとして選択する場合、指定の埋め込み RP グループ範囲はスタティック RP のアクセスリスト内で設定されます。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 RP Address の順にメニューをクリックして以下の画面を表示します。

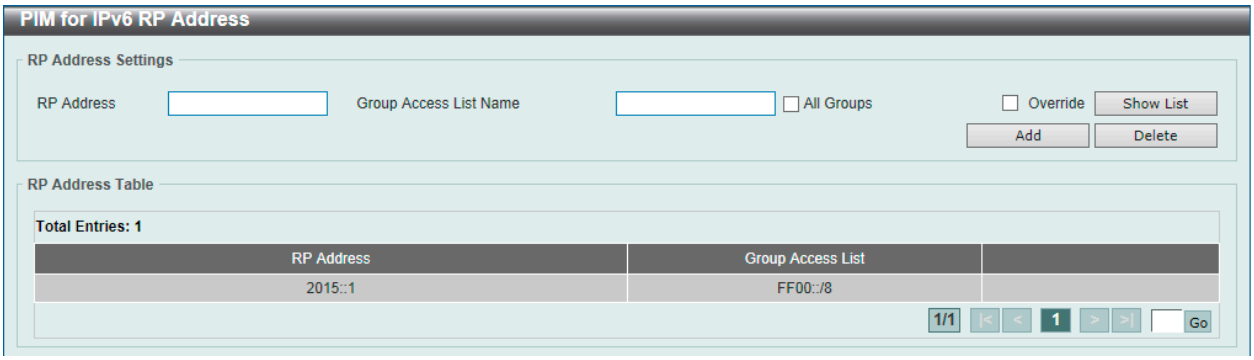


図 9-125　PIM for IPv6 RP Address 画面

以下の項目を使用します。

項目	説明
RP Address	RP IPv6 アドレスを入力します。
Group Access List Name	使用する通常の IPv6 アクセスリストを指定します。「Show List」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。「All Groups」を指定すると「RP」を全マルチキャストグループにマップします。
Override	自動的に学習した RP をスタティック RP が上書きします。

「Add」をクリックし、入力した情報に基づくエントリを追加します。

エントリの登録
「Add」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。

エントリの削除
「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

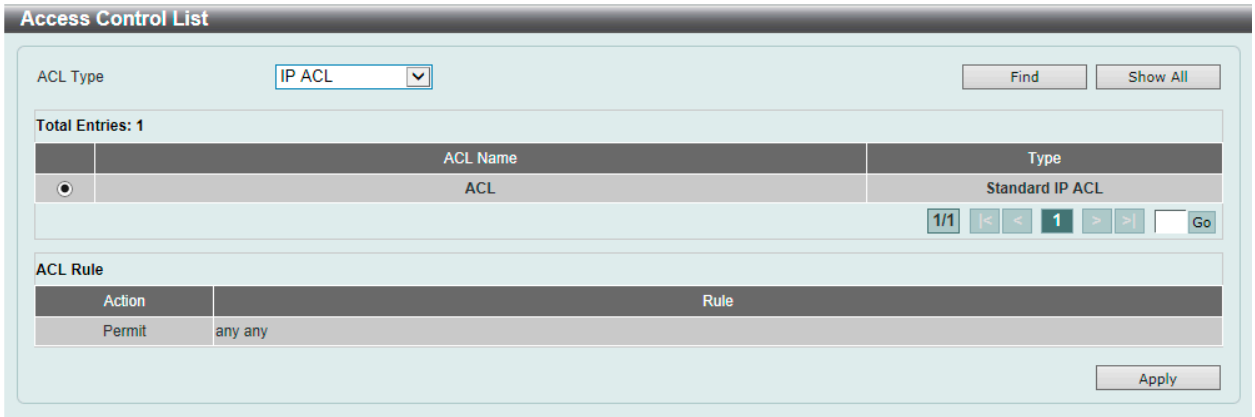


図 9-126　Show List 画面

以下の項目を使用します。

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。 「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Apply」をクリックし、設定内容を適用します。

PIM for IPv6 RP Candidate（PIM for IPv6 RP Candidate 設定）

スイッチの IPv6 PIM RP（Rendezvous Point）candidate に関連する項目を設定します。各インタフェースに一つずつのアクセスリストのみ指定可能です。最新の設定を行うと古い設定は上書きされます。異なるインタフェースに対してそれぞれ設定することが可能です。「PIM-SM」の動作にのみ影響を与えます。これによりルータは BSR に candidate RP として「PIMv2」メッセージを送信するようになります。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Candidate の順にメニューをクリックして以下の画面を表示します。

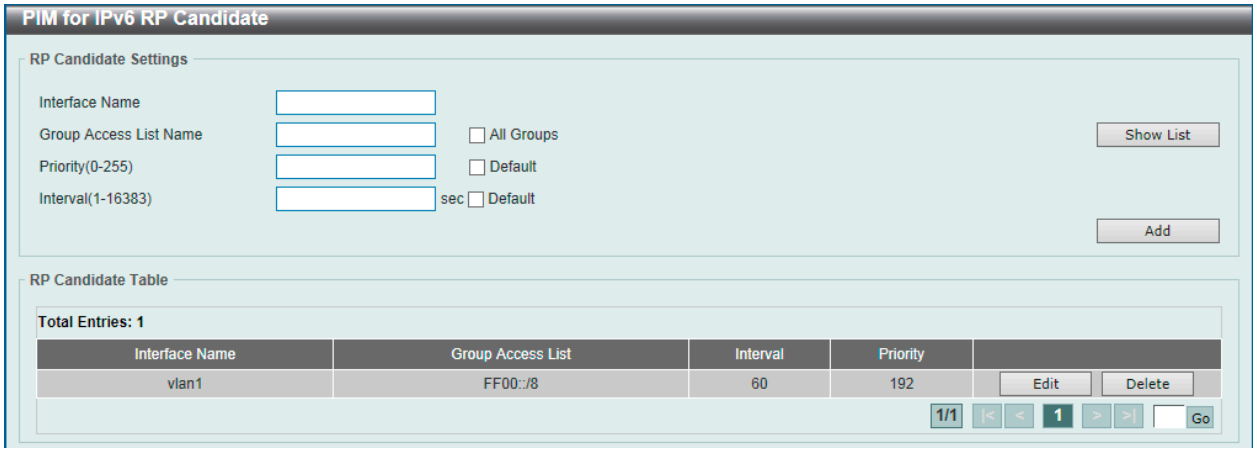


図 9-127　PIM for IPv6 RP Candidate 画面

以下の項目を使用します。

項目	説明
Interface Name	Candidate RP として機能するインタフェースを入力します。
Group Access List Name	使用する通常のアクセスリストを指定します。「Show List」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。「All Groups」を指定すると「RP」を全マルチキャストグループにマップします。
Priority (0-255)	選出処理に使用される RP 優先度値を入力します。「Default」を指定すると初期値（192）を使用します。
Interval (1-16383)	Candidate RP 通知間隔（秒）を入力します。「Default」を指定すると初期値（60）を使用します。

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

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

「Show List」をクリックすると、以下の画面が表示されます。

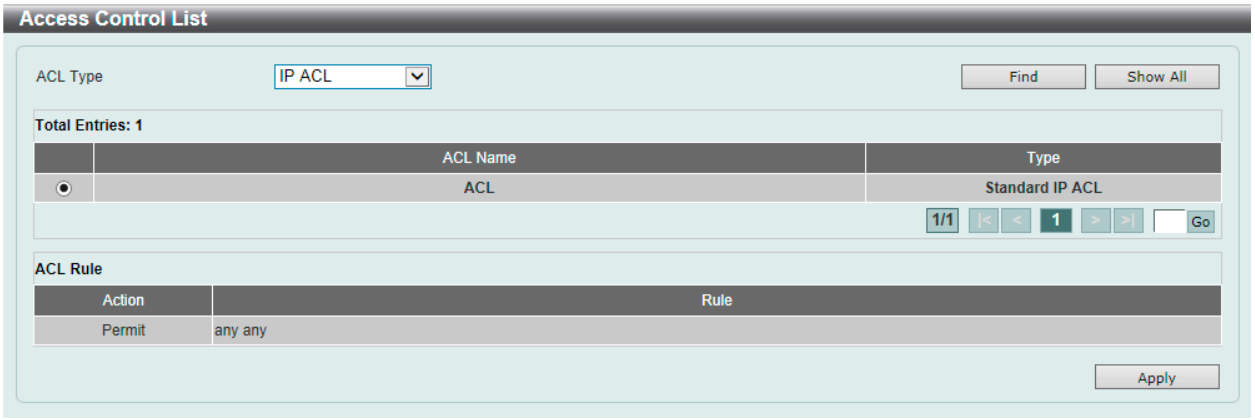


図 9-128　Show List 画面

以下の項目を使用します。

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。 「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Apply」をクリックし、設定内容を適用します。

「Edit」をクリックすると、以下の画面が表示されます。

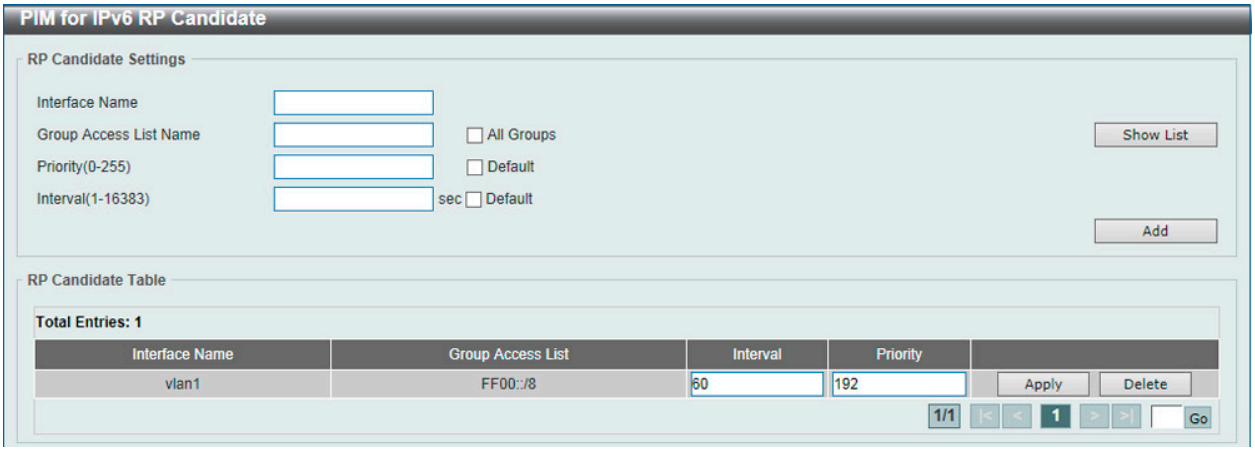


図 9-129　PIM for IPv6 RP Candidate (Edit) 画面

以下の項目を使用します。

項目	説明
Interval	「RP candidate」通知間隔値（1-16383 秒）を指定します。
Priority	RP 優先値（0-255）を指定します。

「Apply」をクリックし、設定内容を適用します。

PIM for IPv6 RP Embedded Settings（PIM for IPv6 RP 埋め込み設定）

本項目では、IPv6 PIM embedded の設定と、表示を行います。「Embedded RP」は IPv6 マルチキャストグループアドレスにエンコードされた RP のアドレスを定義するアドレス割当ポリシーです。これによりイントラドメインマルチキャスト同様に、スケーラブルなインタードメインマルチキャストの配置を簡略化します。RP 情報とともに埋め込まれた IPv6 マルチキャストグループアドレスは RP 埋め込みを意味するフラッグ値「7」の「ff70::/12」から開始します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Embedded Settings の順にメニューをクリックして以下の画面を表示します。

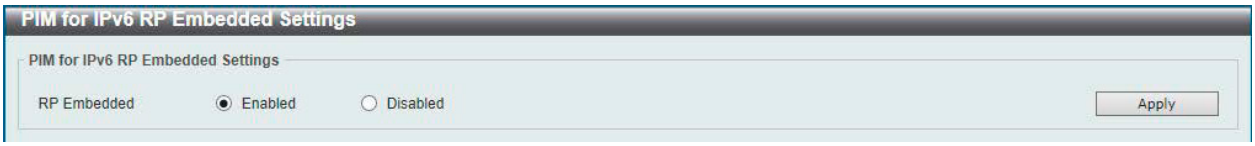


図 9-130　PIM for IPv6 RP Embedded Settings 画面

以下の項目を使用します。

項目	説明
Embedded	RP 埋め込みを有効 / 無効に指定します。

「Apply」をクリックし、設定内容を適用します。

PIM for IPv6 RP Table（PIM for IPv6 RP テーブル）

本項目では、IPv6 PIM RP 情報を表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 RP Table の順にメニューをクリックして以下の画面を表示します。

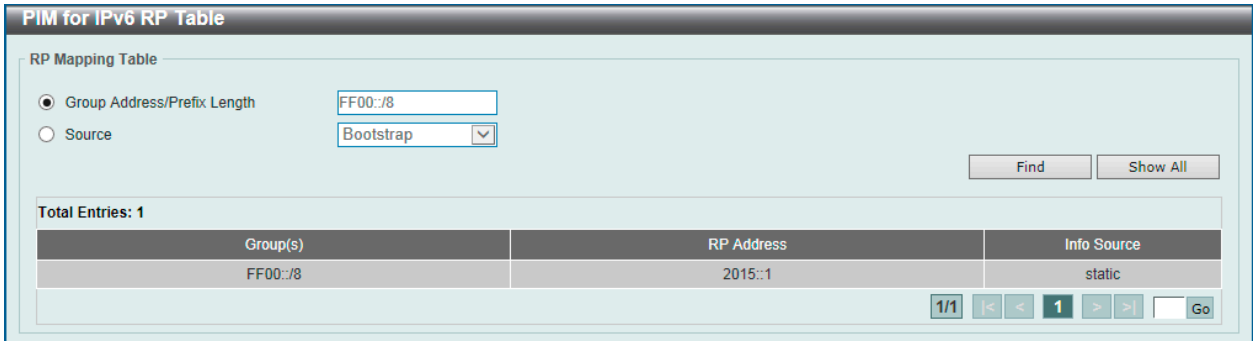


図 9-131　PIM for IPv6 RP Table 画面

以下の項目を使用します。

項目	説明
Group Address/Prefix Length	マルチキャストグループ IPv6 アドレスとプレフィクス長を指定します。
Source	ソースを指定します。「Bootstrap」「Embedded RP」「Static」から指定します。 • Bootstrap - BSR を通じて学習した範囲を表示します。 • Embedded RP - 埋め込み RP を通じて学習したグループ範囲を表示します。 • Static - 手動設定でして指定した範囲を表示します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

PIM for IPv6 Register Settings（PIM for IPv6 レジスタ設定）

本画面では IPv6 PIM レジスタの設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 Register Settings の順にメニューをクリックして以下の画面を表示します。

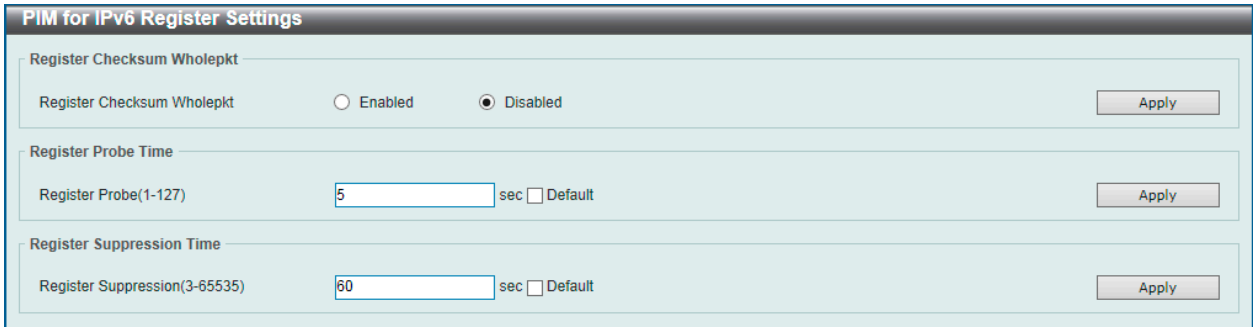


図 9-132　PIM for IPv6 Register Settings 画面

以下の項目を使用します。

項目	説明
Register Checksum Wholepkt	
Register Checksum Wholepkt	全パケットのレジスタチェックサムを有効 / 無効に指定します。有効にすると、ルータはデータポーションを含めた全 PIM メッセージのレジスタメッセージのチェックサムを計算します。初期値はレジスタチェックサム方法は PIM RFC コンプライアントでレジスタメッセージ内のデータポーションは除かれます。
Register Probe Time	
Register Probe	Register-Stop メッセージの再送を起こすように DR が Null-Register を RP に送信する場合に Register-Stop Timer (RST) が期限切れになるまでの時間（1-127 秒）を入力します。「Default」を選択すると初期値（5 秒）を指定します。
Register Suppression Time	
Register Suppression	レジスタ抑止タイムアウト値（3-65535）を入力します。DR がレジスタ停止メッセージを受領すると、抑止タイマが指導します。抑止の間、DR は RP へのレジスタメッセージを停止します。最初のホップルータで本機能を使用します。レジスタプローブタイムはレジスタ停止タイマのネガティブ値を防ぐためにも、レジスタ抑止タイムの半分以下である必要があります。最少タイマ値は「3」です。「Default」を選択すると初期値（60 秒）を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

PIM for IPv6 SPT Threshold Settings（PIM for IPv6 SPT しきい値設定）

本画面では PIM for IPv6 SPT しきい値を表示、設定します

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 SPT Threshold Settings の順にメニューをクリックして以下の画面を表示します。

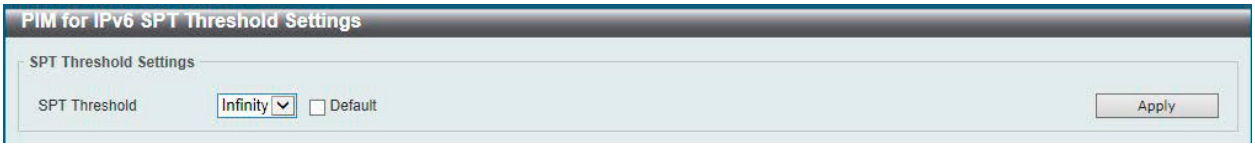


図 9-133　PIM for IPv6 SPT Threshold Settings 画面

以下の項目を使用します。

項目	説明
SPT Threshold	SPT しきい値を指定します。 「0」- 最初のパケットの到着でソースツリーを構築します。 「Infinity」- シェアツリーに依存します。 「Default」を選択すると初期値（Infinity）を指定します。

「Apply」をクリックし、設定内容を適用します。

PIM for IPv6 SSM Settings（PIM for IPv6 SSM 設定）

本画面では IPv6 PIM SSM の設定、表示を行います。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 SSM Settingsの順にメニューをクリックして以下の画面を表示します。



図 9-134　PIM for IPv6 SSM Settings 画面

以下の項目を使用します。

項目	説明
Multicast Group Address Name	ユーザ指定 SSM グループアドレスを定義する通常の IP アクセスリストを指定します。グループアドレスはルールエントリの宛先 IP アドレス項目で定義されます。「Show List」から既存のアクセスリストを指定することも可能です。 「Default SSM Group」オプションを指定すると、初期値の SSM グループアドレス（FF3x::/32）を指定します。

エントリの登録

「Add」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。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Show List」をクリックすると、以下の画面が表示されます。

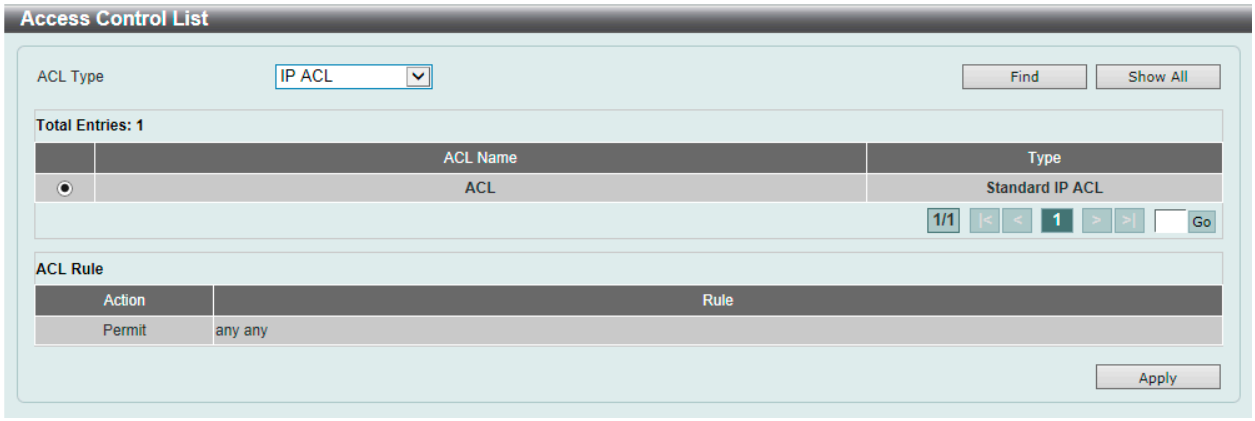


図 9-135　Show List 画面

以下の項目を使用します。

項目	説明
ACL Type	テーブル内の既存の表示する ACL タイプを指定します。 「IP ACL」「Expert IP ACL」「IPv6 ACL」「Expert IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL List	使用するアクセスリストを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Apply」をクリックし、設定内容を適用します。

PIM for IPv6 (S,G) Keepalive Time（PIM for IPv6 (S,G) キープアライブ時間）

本項目では「IPv6 PIM (S,G)」キープアライブ時間の設定、表示を行います。明示的な (S, G) ローカルメンバシップや (S, G) ジョインメッセージの受信がない間、PIM ルータが (S, G) ステートを維持するキープアライブタイマを指定します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 (S,G) Keepalive Time の順にメニューをクリックして以下の画面を表示します。

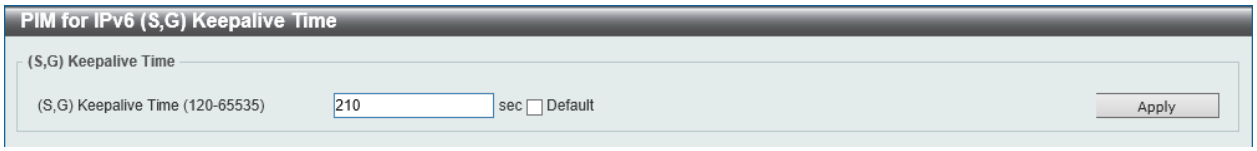


図 9-136　PIM for IPv6 (S,G) Keepalive Time 画面

以下の項目を使用します。

項目	説明
(S,G) Keepalive Time	有効な値は 120-65535 です。明示的な (S, G) ローカルメンバシップや (S, G) Join メッセージの受信がない間、PIM ルータが (S, G) ステートを維持する (S,G) キープアライブタイマを指定します。「Default」を選択すると初期値（120 秒）を指定します。

「Apply」をクリックし、設定内容を適用します。

PIM for IPv6 Mroute Table（PIM for IPv6 マルチキャストルーティングテーブル）

IPv6 マルチキャストルーティングテーブルの全エントリを表示します。スイッチスターグループ (*,G) エントリからソースグループ (S,G) エントリを作成することにより、マルチキャストルーティングテーブルを設定します。スター (*) は全ソースアドレスを意味し、"S" は単一ソースアドレス、"G" は宛先マルチキャストグループアドレスを意味します。(S,G) エントリの作成には、ソフトウェア は「Reverse Path Forwarding」(RPF) を通じてユニキャストルーティングテーブル内の宛先グループへの最良のパスを使用します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM for IPv6 Mroute Table の順にメニューをクリックして以下の画面を表示します。

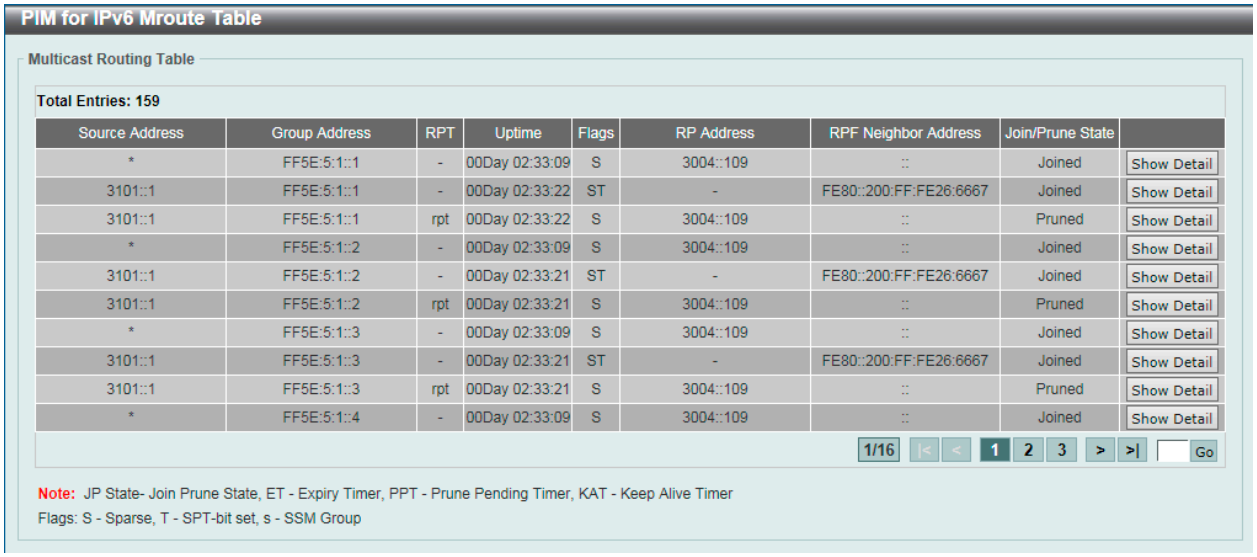


図 9-137　PIM for IPv6 Mroute Table 画面

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。

「Show Detail」をクリックすると次の画面が表示されます。



図 9-138　PIM for IPv6 Mroute Table (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。
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。

PIM for IPv6 Neighbor Table（IPv6 PIM Neighbor テーブル）

現在の IPv6 PIM Neighbor ルータテーブルを表示します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Neighbor Table の順にメニューをクリックして以下の画面を表示します。

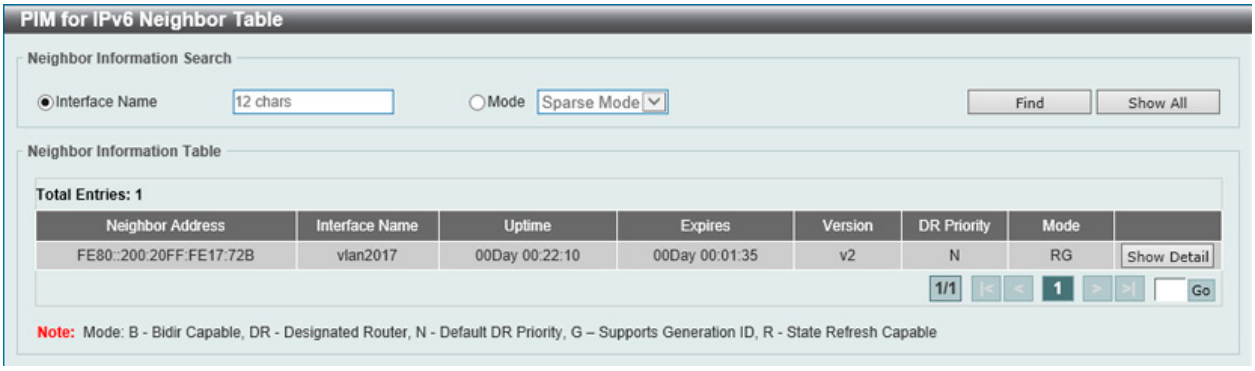


図 9-139　PIM for IPv6 Neighbor Table 画面

以下の項目を使用します。

項目	説明
Interface Name	現在の IPv6 PIM Neighbor ルーティングテーブルを表示する IP インタフェース名を指定します。
Mode	フィルタ検索における IPv6 PIM エントリの操作モードを「Sparse Mode」「Dense Mode」から指定します。

「Find」ボタンをクリックして、入力したインタフェースを検出します。
「Show All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。



図 9-140　PIM for IPv6 Neighbor Table (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

MSDP（MSDP 設定）

L3 Features > IP Multicast Routing Protocol > PIM > MSDP

MSDP Global Settings（MSDP グローバル設定）

Multicast Source Discovery Protocol (MSDP) の表示、グローバル設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP Global Settings の順にメニューをクリックして以下の画面を表示します。

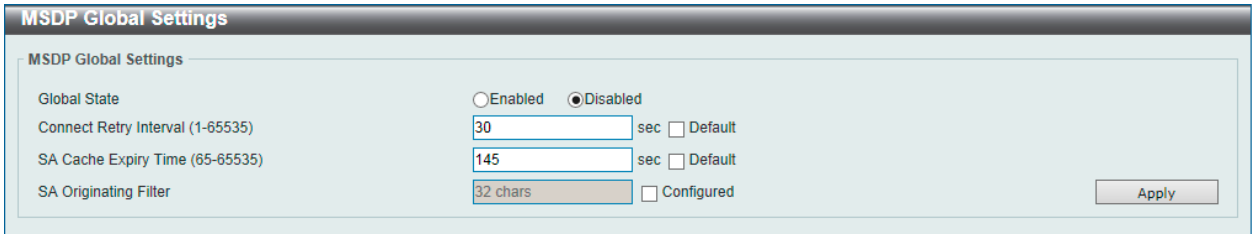


図 9-141　MSDP Global Settings 画面

以下の項目を使用します。

項目	説明
Global State	MSDP をグローバルに有効 / 無効に指定します。
Connect Retry Interval	接続再試行間隔（1-65535 秒）を指定します。MSDP ピアがピアリングセッションがリセットされ再接続を試みるまでの時間間隔を指定します。間隔を大きく開けると接続までに時間を要するようになります。「1-60 秒」以内での設定を推奨します。「Default」を選択すると初期値（30）を指定します。
SA Cache Expiry Time	「Source-Active」(SA) キャッシュの期限値 (65-65535 秒) を設定します。SA キャッシュエントリの期限設定に使用します。SA の間隔は元々 60 秒で修正はできません。したがって、SA キャッシュ期限により、ネットワーク上の想定されるパケットロスに対して非明示的に調整を行います。「Default」を選択すると初期値を指定します。
SA Originating Filter	「Configured」を指定し、SA オリジナルフィルタの文字列を指定します。文字列は 32 字以内で指定します。RP によって MSDP の実行が設定されていて、該当の RP をレジスタする全ローカルソースへの SA メッセージを作成します。リストのフィルタ設定により、RP は、通常 IP アクセスリストでマッチする指定グループに送信する、ローカルソースへの SA メッセージを開始します。「Configured」オプションを選択しフィルタ文字列を指定しないことにより、全ローカルソースのオリジナル SA メッセージからの RP は防ぐことができます。

「Apply」をクリックし、設定内容を適用します。

MSDP Peer Settings（MSDP ピア設定）

Multicast Source Discovery Protocol (MSDP) の表示、ピア設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP Peer Settings の順にメニューをクリックして以下の画面を表示します。

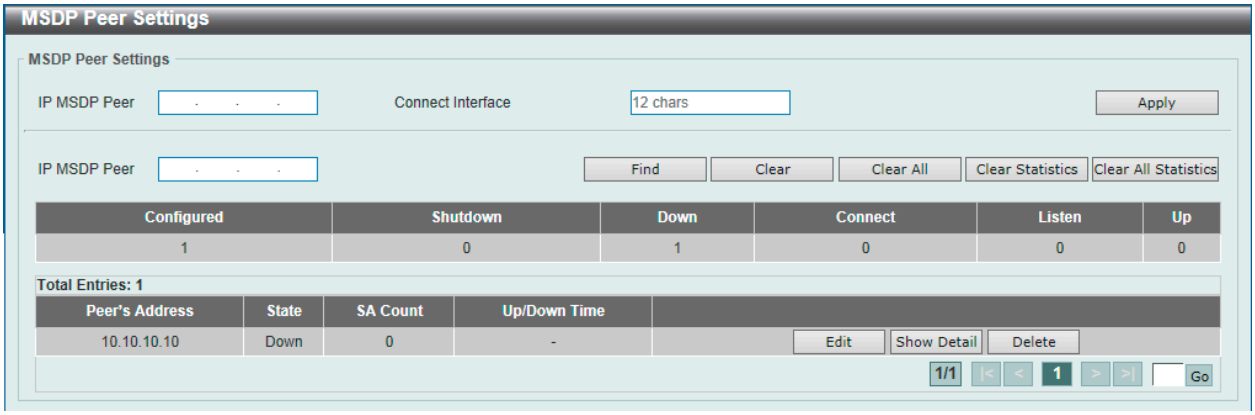


図 9-142　MSDP Peer Settings 画面

以下の項目を使用します。

項目	説明
IP MSDP Peer	MSDP ピア IP アドレスを指定します。
Connect Interface	接続インタフェース（12 字以内）を指定します。ソース IP アドレスに TCP 接続を使用するローカルインタフェースを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Clear」をクリックすると入力したエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「Clear Statistics」をクリックすると入力したエントリの統計情報をクリアします。
「Clear All Statistics」をクリックすると入力したエントリの統計情報を全てクリアします。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

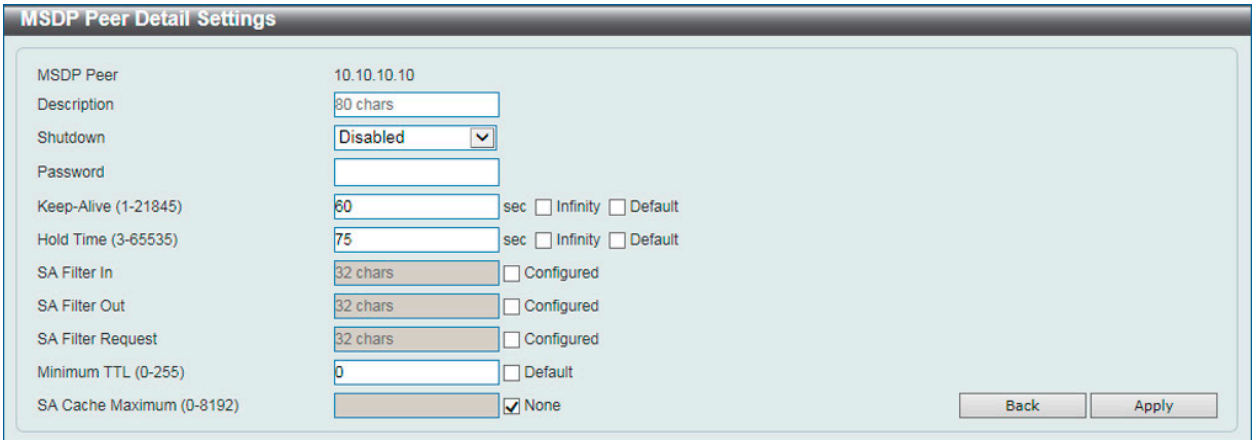


図 9-143　MSDP Peer Settings (Edit) 画面

以下の項目を使用します。

項目	説明
Description	MSDP ピアの概要（80 字以内）を指定します。
Shutdown	シャットダウンを有効 / 無効に指定します。シャットダウンは既存の MSDP ピアで必ず設定する必要があります。MSDP ピアがシャットダウン状態にある場合、ピア間の TCP 接続は構築されません。MSDP ピアはシャットダウン状態でなくなる場合、ピア間の TCP 接続は再構築を試みます。
Password	ピア間の TCP 接続用 MD5 パスワードを指定します。MD5 認証は MSDP ピアで同じパスワードを設定する必要があります。

項目	説明
Keep-Alive	キープアライブ値（1-21845 秒）を指定します。キープアライブ間隔はリモートサイドの MSDP TCP 接続で設定のホールド時間よりも短い必要があります。そうしないと MSDP キープアライブメッセージを受信前にリモートサイドの MSDP TCP 接続は切断されてしまいます。「Infinity」を指定すると MSDP ピアはキープアライブメッセージを送信しません。「Default」を選択すると初期値（60）を指定します。
Hold Time	ホールド時間（3-65535 秒）を指定します。ホールド時間間隔はリモートサイドの MSDP TCP 接続で設定のキープアライブ間隔よりも長い必要があります。そうしないと MSDP キープアライブメッセージを受信前にリモートサイドの MSDP TCP 接続は切断されてしまいます。「Infinity」を指定すると MSDP ピアは切断されません。「Default」を選択すると初期値を指定します。
SA Filter In	「Configured」を指定して、「SA filter-in」文字列（32 字以内）を指定します。ルータは指定ピアからの全 SA メッセージを受信します。本項目を指定しないと、ルータは指定ピアからの全 SA メッセージを無視します。設定することにより、ルータはスタンダード IP アクセスリストで定義され、マッチした指定ピア (S, G) からの SA メッセージのみを受信します。
SA Filter Out	「Configured」を指定して、「SA filter-out」文字列（32 字以内）を指定します。ルータは全 SA メッセージを MSDP ピアに転送します。本項目を指定しないと、ルータは指定ピアへの全 SA メッセージ転送を無視します。設定することにより、ルータはスタンダード IP アクセスリストで定義され、マッチした指定ピア (S, G) への SA メッセージのみを転送します。
SA Filter Request	「Configured」を指定して、「SA filter Request」文字列（32 字以内）を指定します。ルータは指定ピアからの全 SA リクエストメッセージを処理します。本項目を指定しないと、ルータは指定ピアからの全 SA リクエストメッセージを無視します。設定することにより、ルータはスタンダード IP アクセスリストで定義され、マッチした指定ピア (S, G) からの SA リクエストメッセージのみを処理します。
Minimum TTL	最小 TTL 値（0-225）を指定します。SA メッセージが MSDP ピアから送信された時、SA メッセージ内のマルチキャストデータパケットの「Time-To-Live」(TTL) 値が減少し、減少した TTL 値が SA メッセージが送信された MSDP ピアで設定の最小 TTL 値よりも小さい場合、SA は送信されません。「Default」を選択すると初期値（0）を指定します。
SA Cache Maximum	最大 SA キャッシュ値（0-8192）を指定します。SA キャッシュの最大値が 0 に設定されると、スイッチはピアからの SA キャッシュエントリを学習しません。SA キャッシュの最大値が既存の SA キャッシュエントリよりも小さい場合、古い既存の SA キャッシュエントリは最大 SA キャッシュ値と SA キャッシュエントリ数が同じになるまで、削除されます。「None」を指定すると SA キャッシュエントリの制限がなくなります。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

「Show Detail」をクリックすると、以下の画面が表示されます。

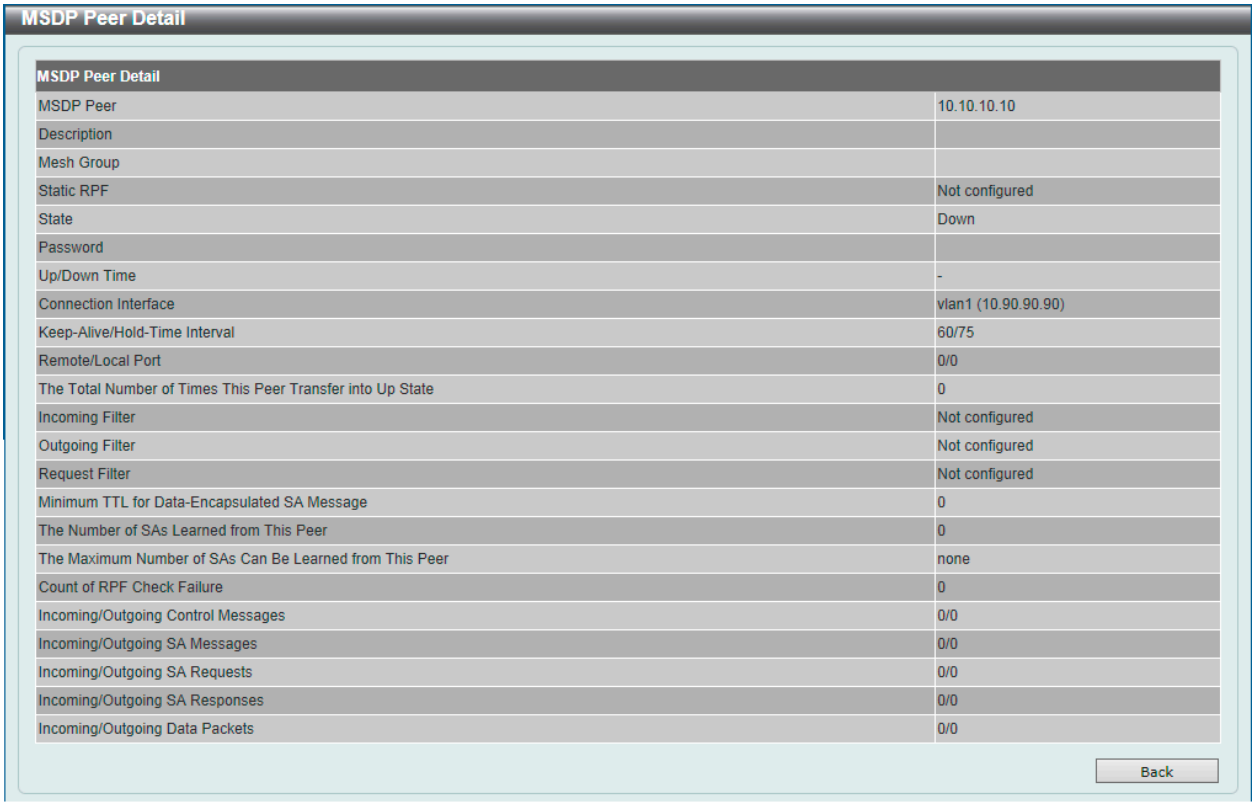


図 9-144　MSDP Peer Settings (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

MSDP SA Cache（MSDP SA キャッシュ）

Multicast Source Discovery Protocol (MSDP)SA のキャッシュ設定を行います。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP SA Cache の順にメニューをクリックして以下の画面を表示します。

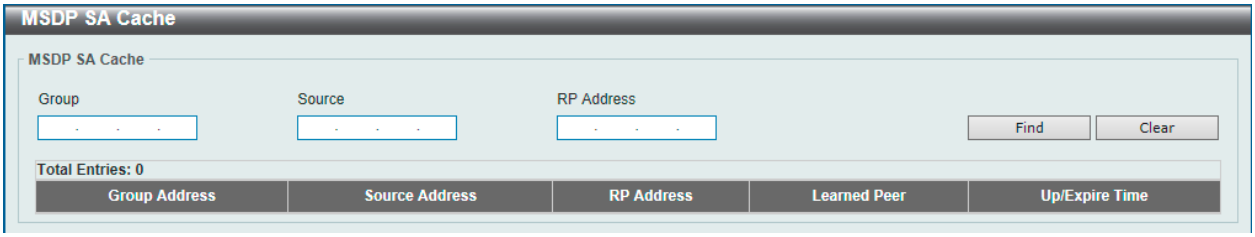


図 9-145　MSDP SA Cache 画面

以下の項目を使用します。

項目	説明
Group	グループアドレスを指定します。
Source	ソースアドレスを指定します。
RP Address	RP アドレスを指定します。

「Clear」をクリックすると入力したエントリをクリアします。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

MSDP Static RPF Settings（MSDP スタティック RPF 設定）

本項目では、MSDP スタティック RPF 設定を行います。スタティック RPF ピアを設定する前に、MSDP ピアを追加する必要があります。RP プリフィクスリストが設定されると、ピアはプリフィクスリストの RP のみのスタティック RPF になります。複数のスタティック RPF ピアが RP プリフィクスリスト抜きで設定されると、一番小さい接続ピアのみが有効なスタティック RPF ピアになります。MSDP ピアがスタティック RPF ピアに複数回設定されていると、最新の設定が有効になります。MSDP ピアが一つしかない場合、該当の MSDP ピアはスタティック RPF ピアとなります。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP Static RPF Settings の順にメニューをクリックして以下の画面を表示します。



図 9-146　MSDP Static RPF Settings 画面

以下の項目を使用します。

項目	説明
Peer Address	MSDP ピアアドレスを指定します。
RP List	RP プリフィクスリストを定義するスタンダード IP リスト（32 字以内）を指定します。
RP Address	RP アドレスを指定します。

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

MSDP Mesh Group Settings（MSDP メッシュグループ設定）

本項目では、MSDP メッシュグループの設定を行います。MSDP ピアを追加するメッシュグループに追加する前に、MSDP ピアを追加する必要があります。MSDP ピアが複数のメッシュグループに追加されている場合、最新の設定内容が有効になります。

L3 Features > IP Multicast Routing Protocol > PIM > MSDP > MSDP Mesh Group Settings の順にメニューをクリックして以下の画面を表示します。

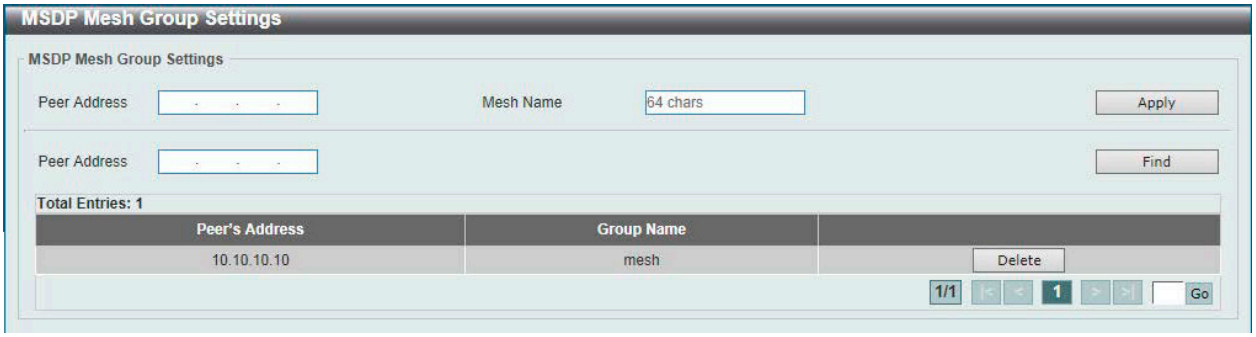


図 9-147　MSDP Mesh Group Settings 画面

以下の項目を使用します。

項目	説明
Peer Address	MSDP ピアアドレスを指定します。
Mesh Name	メッシュグループ名（64 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPMC（IP マルチキャスト設定）

L3 Features > IP Multicast Routing Protocol > IPMC

IP Multicast Global Settings（IP マルチキャストグローバル設定）

IP Multicast Global Settings（IP マルチキャストグローバル設定）の表示、グローバル設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Global Settings の順にメニューをクリックして以下の画面を表示します。

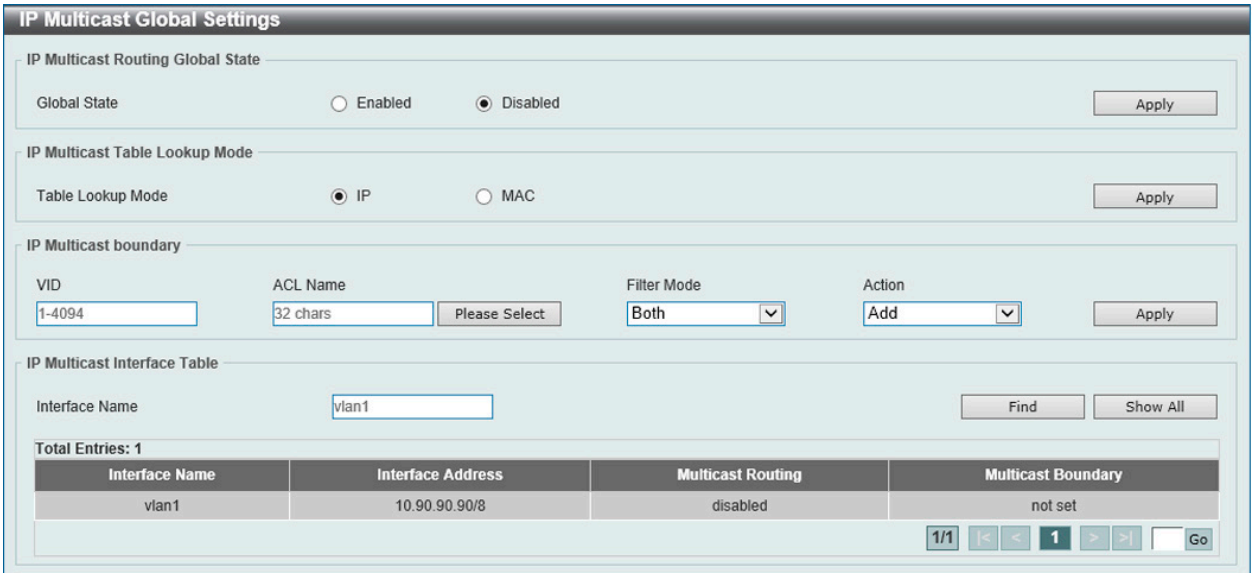


図 9-148　IP Multicast Global Settings 画面

以下の項目を使用します。

項目	説明
IP Multicast Routing Global State	
Global State	IP マルチキャストルーティングを有効 / 無効に指定します。IP マルチキャストルーティングが無効の場合、マルチキャストルーティングプロトコルが有効でも、システムはルーティングマルチキャストパケットを停止します。

項目	説明
IP Multicast Table Lookup Mode	
Table Lookup Mode	IP マルチキャストフォワーディングルックアップモードを指定します。 • IP - マルチキャストフォワーディングルックアップを IP アドレス基準で行います。 • MAC - マルチキャストフォワーディングルックアップを MAC アドレス基準で行います。
IP Multicast Boundary	
VID	VLAN ID（1-4094）を指定します。
ACL Name	指定する IP アクセスリスト名（32 字以内）を指定します。 「Please Select」を指定すると既存のアクセスリストを選択することも可能です。
Filter Mode	フィルタモードを指定します。 • Both - インカミング / アウトゴーイングどちらのトラフィックもフィルタします。 • Out - インタフェースに到着する PIM ジョインメッセージ、または IGMP ジョインメッセージをフィルタします。このフィルタリングにより、インタフェースが拒否エントリ (G) (S,G) の外向きインタフェースになることを防止します。 • In - インタフェースに到着するマルチキャストユーザトラフィックを指定のアクセスリストに基づきフィルタします。このフィルタリングにより、指定ソースからの指定グループや指定グループのマルチキャストトラフィックなどをフィルタします。
Action	動作を「Add」「Delete」から指定します。
IP Multicast Interface Table	
Interface Name	表示するインタフェース名を指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Please Select」をクリックすると、次の画面を表示します。



図 9-149 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。

IP Multicast Route Settings（IP マルチキャストルート設定）

IP Multicast Route Settings（IP マルチキャストルート設定）の表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Route Settings の順にメニューをクリックして以下の画面を表示します。

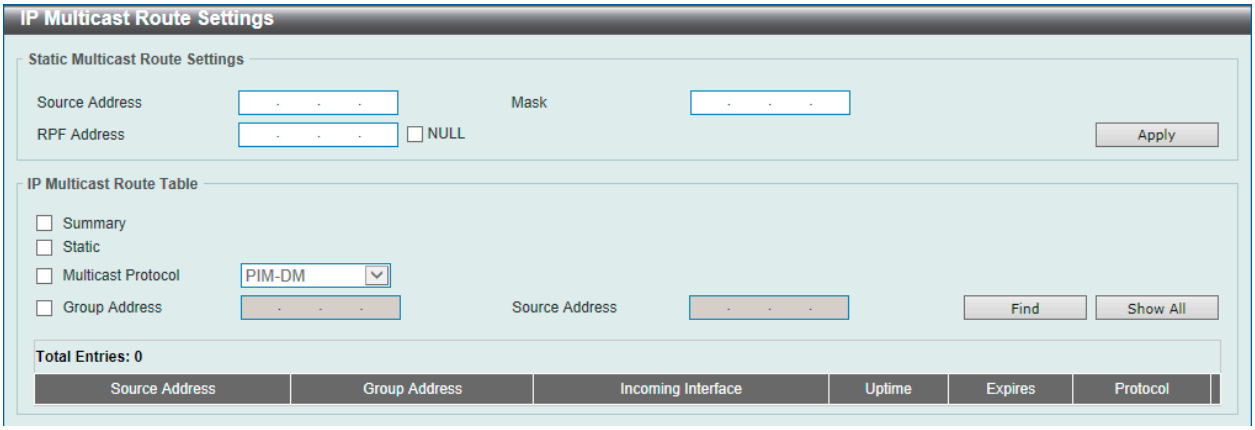


図 9-150 IP Multicast Route Settings 画面

以下の項目を使用します。

項目	説明
Static Multicast Route Settings	
Source Address	マルチキャストソースとなるネットワークアドレスを指定します。
Mask	マルチキャストソースとなるサブネットマスクを指定します。
RPF Address	RPF ネイバ IP アドレスを入力します。「NULL」オプションを選択すると、ソースネットワークから送信されたマルチキャストトラフィックの RPF チェックは必ず失敗します。
IP Multicast Route Table	
Summary	IP マルチキャストルーティングテーブルのサマリについて表示します。
Static	マルチキャストスタティックルートを表示します。
Multicast Protocol	表示するマルチキャストプロトコルを選択します。「PIM-DM」「PIM-SM」「DVMRP」から選択可能です。
Group Address	マルチキャストグループ IP アドレスを指定します。
Source Address	マルチキャストソース IP アドレスを指定します。

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

IP Multicast RPF Table（IP マルチキャスト RPF テーブル）

IP Multicast RPF Table（IP マルチキャスト RPF テーブル）の表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast RPF Table の順にメニューをクリックして以下の画面を表示します。

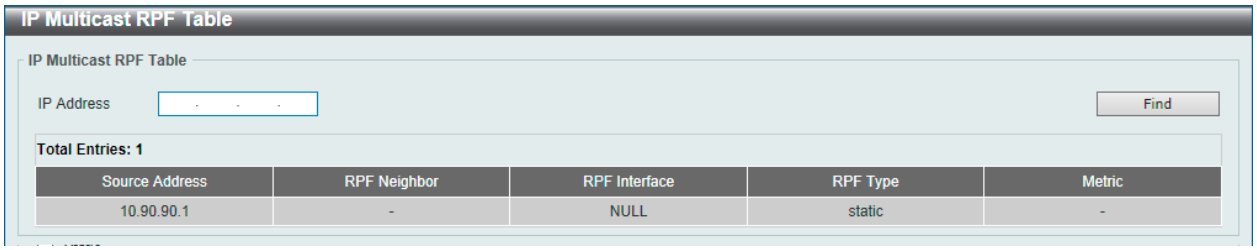


図 9-151　IP Multicast RPF Table 画面

以下の項目を使用します。

項目	説明
IP Address	ユニキャスト IPv4 アドレスを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

IP Multicast Forwarding Cache（IP マルチキャストフォワーディングキャッシュ）

IP Multicast Forwarding Cache（IP マルチキャストフォワーディングキャッシュ）の表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Forwarding Cache の順にメニューをクリックして以下の画面を表示します。

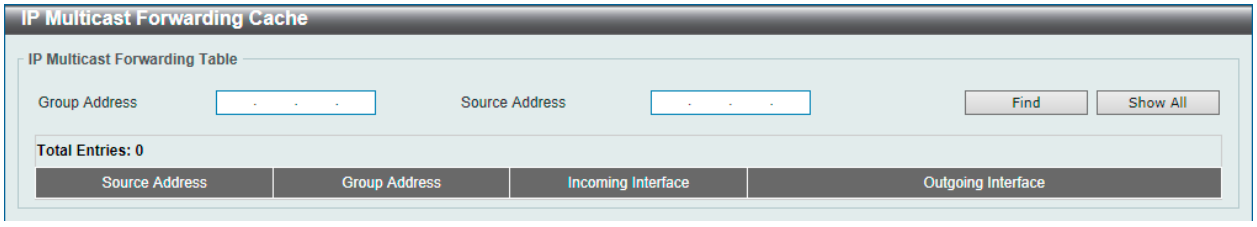


図 9-152　IP Multicast Forwarding Cache 画面

以下の項目を使用します。

項目	説明
Group Address	マルチキャストグループ IP アドレスを指定します。
Source Address	マルチキャストソース IP アドレスを指定します。

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

IP Multicast Protocol Statistics（IP マルチキャストプロトコル統計）

IP Multicast Protocol Statistics（IP マルチキャストプロトコル統計）の表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Protocol Statistics の順にメニューをクリックして以下の画面を表示します。

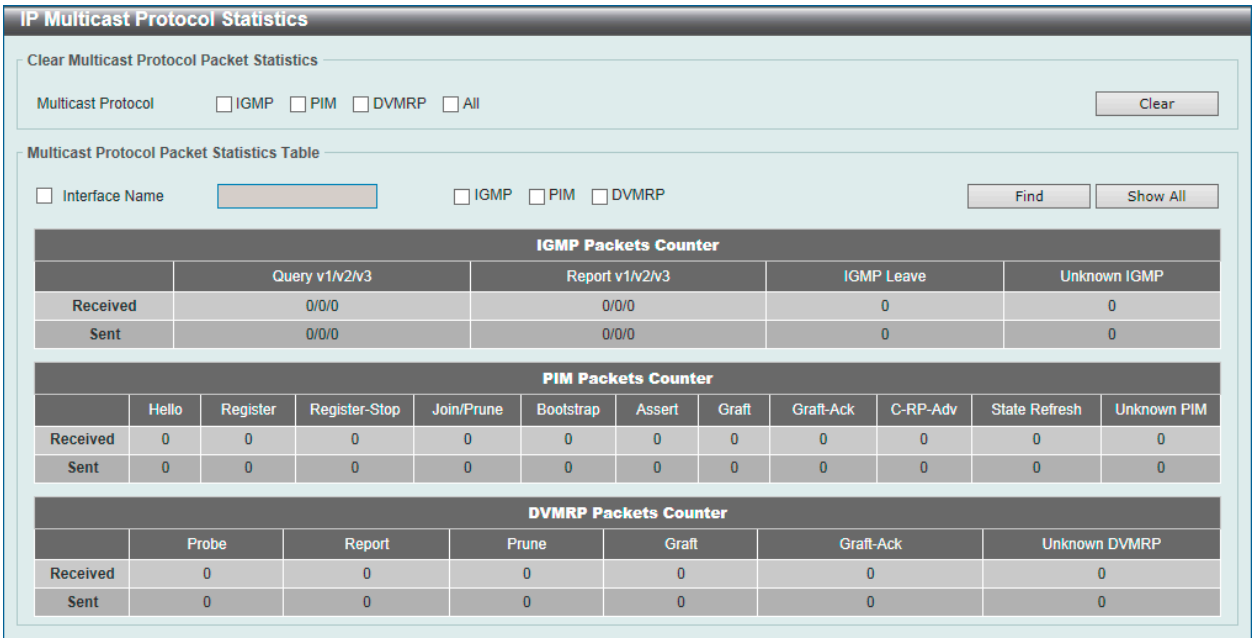


図 9-153　IP Multicast Protocol Statistics 画面

以下の項目を使用します。

項目	説明
Clear Multicast Protocol Packet Statistics	
Multicast Protocol	クリアするマルチキャストプロトコルを選択します。「IGMP」「PIM」「DVMRP」「All」から選択可能です。
Multicast Protocol Packet Statistics Table	
Interface Name	本設定に使用するインタフェース名を指定します。
Multicast Protocol	表示するマルチキャストプロトコルを選択します。「IGMP」「PIM」「DVMRP」から選択可能です。

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

Control Packet CPU Filtering（IP マルチキャストプロトコル統計）

IP Multicast Protocol Statistics（IP マルチキャストプロトコル統計）の表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > Control Packet CPU Filtering の順にメニューをクリックして以下の画面を表示します。

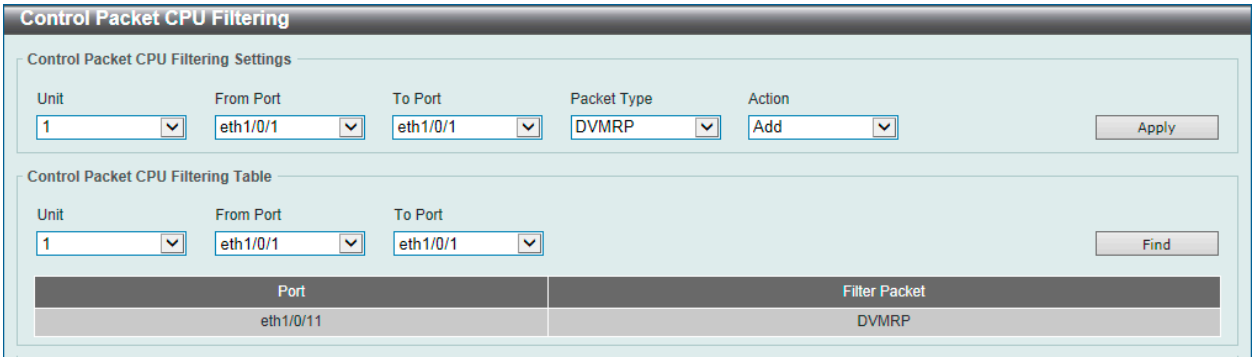


図 9-154　Control Packet CPU Filtering 画面

以下の項目を使用します。

項目	説明
Control Packet CPU Filtering Settings	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

項目	説明
Packet Type	パケットの種類を指定します。 • DVMRP - CPU は送信した「DVMRP L3 コントロールパケット」を破棄します。 • PIM - CPU は送信した「PIM L3 コントロールパケット」を破棄します。 • IGMP Query - CPU は送信した「IGMP Query L3 コントロールパケット」を破棄します。 • OSPF - CPU は送信した「OSPF L3 コントロールパケット」を破棄します。 • RIP - CPU は送信した「RIP L3 コントロールパケット」を破棄します。 • VRRP - CPU は送信した「VRRP L3 コントロールパケット」を破棄します。
Action	動作を「Add」「Delete」から指定します。
Control Packet CPU Filtering Table	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

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

IPv6MC（IPv6 マルチキャスト設定）

L3 Features > IP Multicast Routing Protocol > IPv6MC

IPv6 Multicast Global Settings（IPv6 マルチキャストグローバル設定）

IPv6 Multicast Global Settings（IPv6 マルチキャストグローバル設定）の表示、グローバル設定を行います。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Multicast Global Settings の順にメニューをクリックして以下の画面を表示します。

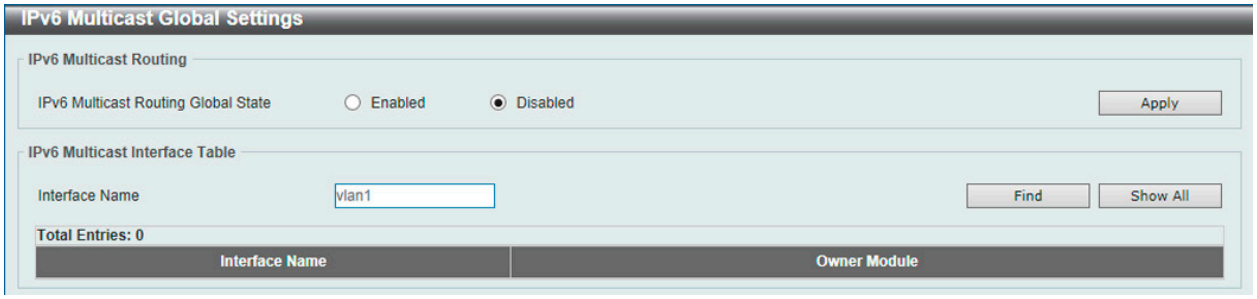


図 9-155　IPv6 Multicast Global Settings 画面

以下の項目を使用します。

項目	説明
IPv6 Multicast Routing	
IPv6 Multicast Routing Global State	IPv6 マルチキャストルーティングを有効 / 無効に指定します。IPv6 マルチキャストルーティングが無効の場合、マルチキャストルーティンプロトコルが有効でも、システムはルーティングマルチキャストパケットを停止します。
IPv6 Multicast Interface Table	
Interface Name	本設定に使用するインタフェース VLAN を指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv6 Static Multicast Route Settings（IPv6 スタティックマルチキャストルート設定）

本項目では IPv6 スタティックマルチキャストルート設定を行います。PIM コントロールは自身のルーティングテーブルがなく、ユニキャストルーティングテーブルを使用して、ネットワークに届くリバースパスフォワーディングインタフェースを決定します。ネットワークの RPF アドレスを使用するスタティックマルチキャストルートを設定します。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Static Multicast Route Settings の順にメニューをクリックして以下の画面を表示します。

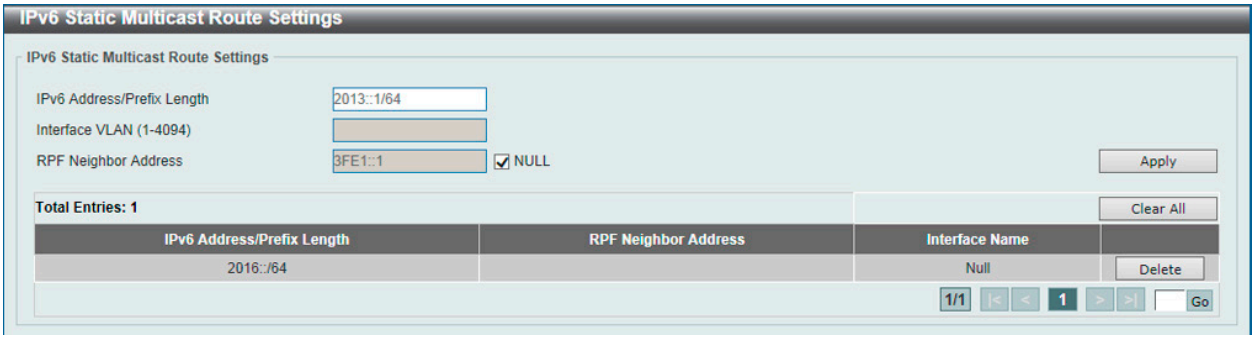


図 9-156 IPv6 Static Multicast Route Settings 画面

以下の項目を使用します。

項目	説明
IPv6 Address/Prefix Length	マルチキャストソースの IPv6 ネットワークアドレスとプリフィクス長を指定します。
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
RPF Neighbor Address	RPF ネイバ IPv6 アドレスを入力します。「NULL」オプションを選択すると、ソースネットワークから送信されたマルチキャストトラフィックの RPF チェックは必ず失敗します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Clear All」をクリックすると入力したエントリを全てクリアします。
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。

IPv6 Multicast Routing Table（IPv6 マルチキャストルーティングテーブル）

IPv6 Multicast Route Table（IPv6 マルチキャストルートテーブル）の表示、設定を行います。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Table の順にメニューをクリックして以下の画面を表示します。

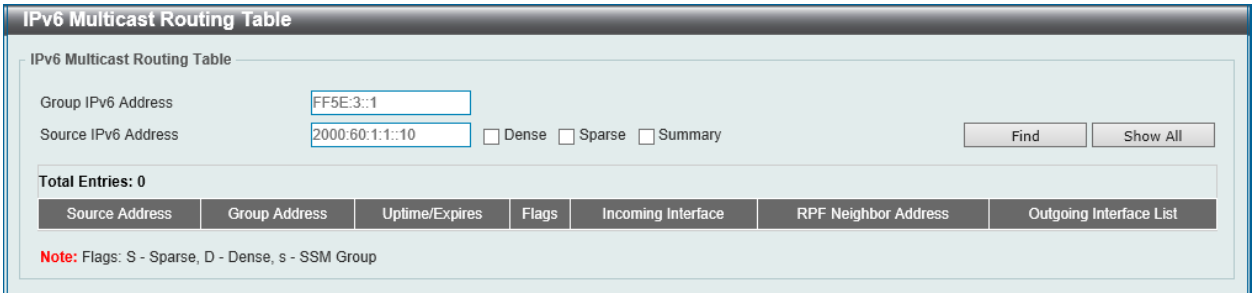


図 9-157 IPv6 Multicast Routing Table 画面

以下の項目を使用します。

項目	説明
Group IPv6 Address	マルチキャストグループ IPv6 アドレスを指定します。
Source IPv6 Address	マルチキャストソース IPv6 アドレスを指定します。 • Dense - PIM-DM ルートのみ表示します。 • Sparse - PIM-SM ルートのみ表示します。 • Summary - IPv6 マルチキャストルーティングテーブルにおける 1 行の要約されたサマリを表示します。

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

IPv6 Multicast Forwarding Cache Table（IPv6 マルチキャストフォワーディングキャッシュテーブル）

IPv6 Multicast Forwarding Cache Table（IPv6 マルチキャストフォワーディングキャッシュテーブル）の表示、設定を行います。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Multicast Forwarding Cache Table の順にメニューをクリックして以下の画面を表示します。



図 9-158 IPv6 Multicast Forwarding Cache Table 画面

以下の項目を使用します。

項目	説明
Group IPv6 Address	マルチキャストグループ IPv6 アドレスを指定します。
Source IPv6 Address	マルチキャストソース IPv6 アドレスを指定します。

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

IPv6 RPF Table（IPv6 RPF テーブル）

IPv6 RPF Table（IPv6 RPF テーブル）の表示、設定を行います。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 RPF Table の順にメニューをクリックして以下の画面を表示します。

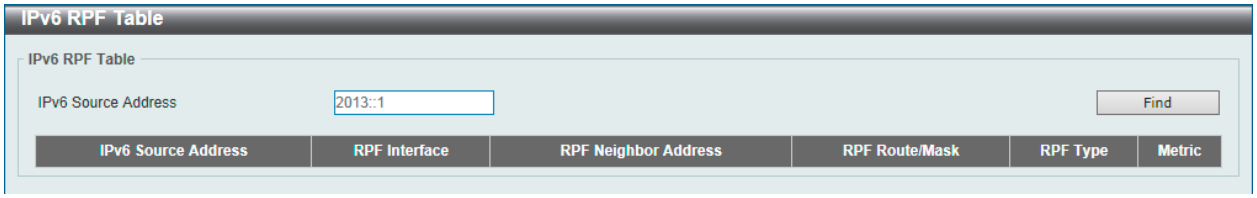


図 9-159 IPv6 RPF Table 画面

以下の項目を使用します。

項目	説明
IPv6 Source Address	ユニキャストホスト IPv6 アドレスを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

BGP（Border Gateway Protocol）（EI/MI モードのみ）

L3 Features > BGP

スイッチは BGP（Border Gateway Protocol）をサポートしています。これは、AS（自律システム）内のネットワーク到達性を指定する IP ネットワークまたはプレフィックスのテーブルを保持するレイヤ 3 ユニキャストルーティングプロトコルです。BGP はパス、ネットワークポリシー、そして / または、ルールセットに基づいて経路の決定をします。

BGP Global Settings（BGP グローバル設定）

スイッチに BGP のグローバル設定を行います。

L3 Features > BGP > BGP Global Settings の順にメニューをクリックして以下の画面を表示します。

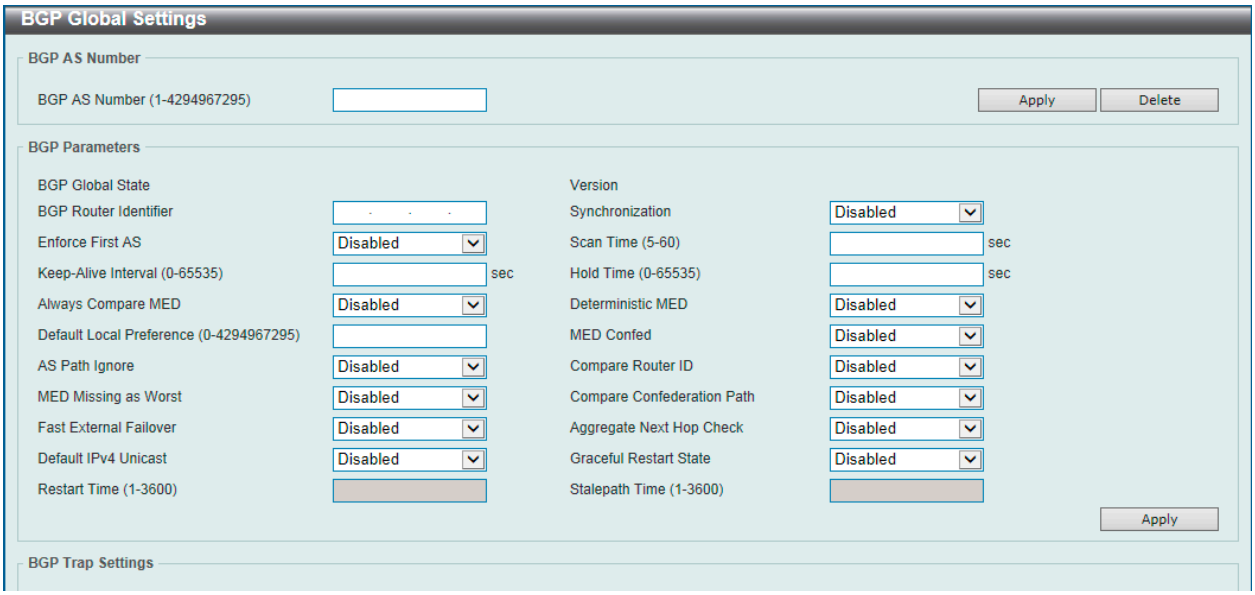


図 9-160　BGP Global Settings 画面

以下の項目を使用して設定を行います。

項目	説明
BGP AS Number	
BGP AS Number (1-4294967295)	1-4294967295 の範囲の BGP AS 番号を入力します。
BGP AS Number	
BGP Router Identifier	BGP ルータ ID を設定します。BGP ルータを識別する ID。0 に設定されると、ルータ ID は自動的に決定されます。ネットワーク内で固有のルータ ID を指定する必要があります。
Synchronization	通常、そのルートがローカルであるか、または IGP に存在していない場合、BGP スピーカは外部の Neighbor にルートを通知しません。初期値では、BGP と IGP 間の同期はオフであり、BGP は IGP からのルート確認を待たないでネットワークルートを通知することができます。本機能により、BGP が他の AS(自律) システムに利用可能にする前に AS 内のルータとアクセスサーバはルートを持つことができます。
Enforce First AS	AS リスト内の最初の AS として Neighbor の AS を実行します。設定を有効にすると、外部 Neighbor から受信する更新のうち受信した更新内の AS_PATH の最初に Neighbor の自律システム (AS) を持たない更新は拒否されて、Neighbor はクローズされます。本機能を有効にすると、許可されていないシステムからのトラフィックを許可しないことで、BGP ネットワークのセキュリティの 1 つに追加されます。
Scan Time	BGP スキャンタイマ値を 5-60(秒) で設定します。または「Default」をチェックします。初期値は 60(秒) です。
Keepalive Interval (0-65535)	有効な値は 0-65535 です。keepalive メッセージがピアに送信される間隔を指定します。値が 0 に設定されると、keepalive メッセージは送信されません。初期値は 60(秒) です。BGP 接続を実装する 2 つのルータが、異なる keepalive タイマを持つ場合、より小さい keepalive タイマが使用されます。タイマを特定の Neighbor に指定すると、Neighbor の指定タイマが適用されます。
Hold Time (0-65535)	有効な値は 0-65535 です。keepalive メッセージが holdtime を超えて受信されると、システムはピアを Dead として判断します。初期値は 180(秒) です。holdtime が 0 に設定されると、無期限となります。BGP 接続を実装する 2 つのルータが、異なる保持時間を持つ場合、より小さい保持時間が使用されます。タイマを特定の Neighbor に指定すると、Neighbor の指定タイマが適用されます。保持時間は、keepalive 時間の少なくとも 3 倍である必要があります。
Always compare MED	異なる AS 内の Neighbor からの受信したパスに対する MED の比較を有効または無効にします。初期値では無効です。
Deterministic MED	同じ AS 内の Neighbor からの受信したパスに対する MED の決定的な比較を有効または無効にします。初期値では、本設定は無効です。
Default Local Preference (0-4294967295)	0-4294967295 の範囲でデフォルトローカル優先度を指定します。初期値は 100 です。

項目	説明
Med Confed	選択すると、BGP プロセスは、コンフェデレーションピアから受信するルートの MED を比較します。パスに外部 AS を持つルートには、比較は行われません。
AS Path Ignore	選択すると、BGP プロセスは経路選定プロセスで AS パスを無視します。
Compare Router ID	選択すると、BGP プロセスは経路選定プロセスでルータ ID を含めます。同様のルートは比較され、最も低いルータ ID を持つルートが選択されます。
MED Missing As Worst	選択すると、BGP プロセスは MED 属性が欠けているルートに infinity(無限) の値を割り当てます。無効にすると、BGP プロセスは、MED 属性が欠けているルートに本ルートがベストパスとして選択されるように 0 の値を割り当てます。
Compare Confederation Path	選択すると、BGP プロセスは、受信するルートのコンフェデレーション AS のパス長を比較します。コンフェデレーション AS のパス長が短いほど、よいルートとなります。
Fast External Fallover	fast external fallover 機能を有効または無効にします。これは、外部の BGP ピアセッションを、これらのピアに到達するのに使用されているリンクがダウンすると、直ちにリセットするように Border Gateway Protocol(BGP) ルーティングプロセスを設定します。初期値は有効です。
Aggregate Next Hop Check	aggregate next hop check 機能を有効または無効にします。BGP アグリゲートルートのネクストホップチェックを設定します。同じネクストホップ属性を持つルートだけが、BGP アグリゲートネクストホップチェックが有効な場合に集約されます。初期値は無効です。
Default IPv4 Unicast	デフォルトでの IPv4 ユニキャスト機能を有効にします。IPv4 ユニキャスト情報の交換に使用します。
Graceful Restart State	BGP ネイバの BGP グレースフルリスタートステートを有効または無効にします。
Restart Time	グレースフルリスタート時間（1-3600 秒）を指定します。ネイバリスタートの最大時間を指定します。
Stalepath Time	「Stalepath」時間（1-3600 秒）を指定します。「stalepath」待ちからネイバリスタートまでの最大時間値を指定します。
BGP Trap Settings	
Peer Established Trap State	BGP ピア構築トラップを有効 / 無効に指定します。
Peer Backward-Trans Trap State	ピアアイドルトラップを有効 / 無効に指定します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

BGP Aggregate Address Settings（BGP アグリゲートアドレス設定）

Border Gateway Protocol(BGP) データベースにアグリゲートエントリを作成します。
ルートアグリゲーションはルーティングエントリの減少に使われるメカニズムです。アグリゲートされたルートは、ルーティングテーブルで作成されます。アグリゲートされたルートはローカル AS から送信されます。アグリゲーションフラグはアグリゲートされたエントリから失われる可能性のある指定ルート情報の AS パス情報を示すために設定されます。

L3 Features > BGP > BGP Aggregate Address Settings の順にメニューをクリックして以下の画面を表示します。

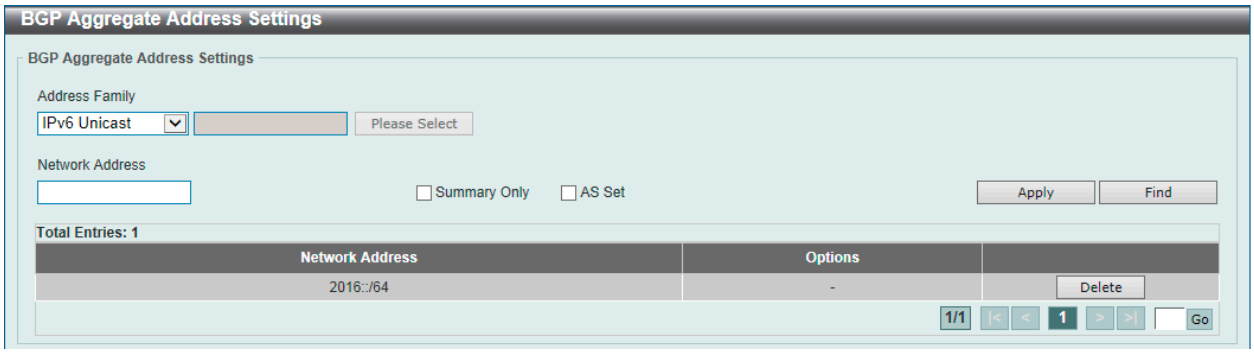


図 9-161　BGP Aggregate Address Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Network Address	集約される IPv4/IPv6 アドレスとネットマスクを入力します。
Summary Only	チェックして、指定ルートの通知を停止します。初期値はチェックなしです。
AS Set	AS 設定パス情報を生成します。初期値はチェックなしです。

「Apply」ボタンをクリックして変更を適用します。

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

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

「Please Select」をクリックすると、次の画面が表示されます。



図 9-162 Please Select（VRF）画面

使用する VRF 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。

BGP Network Settings（BGP ネットワーク設定）

Border Gateway Protocol(BGP) が通知するネットワークを指定します。

L3 Features > BGP > BGP Network Settings の順にメニューをクリックして以下の画面を表示します。



図 9-163 BGP Network Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Network Address	集約される IPv4/IPv6 アドレスとネットマスクを入力します。
Route Map Name	通知されるネットワークに適用するルートマップを指定します。指定しない場合、すべてのネットワークを通知します。

「Apply」をクリックし、設定内容を適用します。

エントリの検索
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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

「Please Select」をクリックすると、次の画面が表示されます。



図 9-164 Please Select（VRF）画面

使用する VRF 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。

BGP Route Redistribution Settings（BGP ルート再分配設定）

BGP Route Redistribution Settings（BGP ルート再分配設定）の設定を行います。ルーティングドメインから BGP へのルート再分配に使用します。

L3 Features > BGP > BGP Route Redistribution Settings の順にメニューをクリックして以下の画面を表示します。

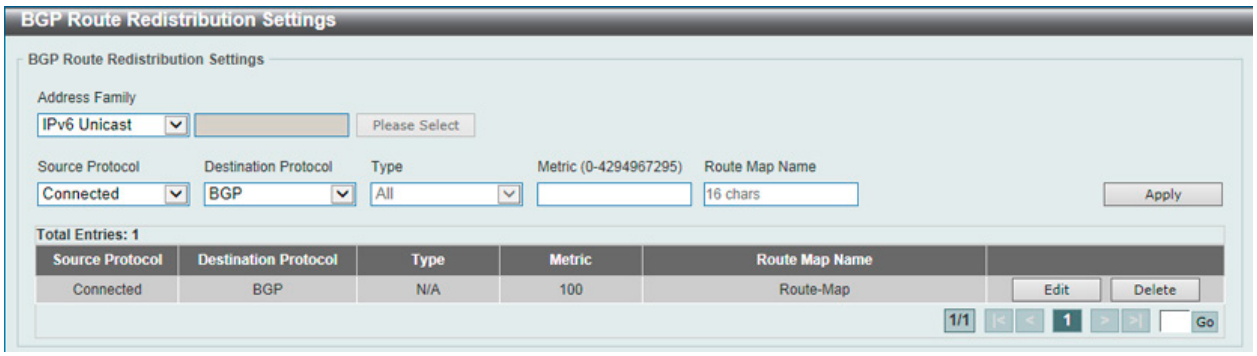


図 9-165 BGP Route Redistribution Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Source Protocol	プルダウンメニューを使用して送信元のプロトコルを選択します。 • Connected - BGP への接続ルートに再分配します。 • Static - BGP へのスタティックルートに再分配します。 • RIP - BGP への RIP ルートに再分配します。 • OSPF - BGP への OSPF ルートに再分配します。 • ISIS - BGP への ISIS ルートに再分配します。
Destination Protocol	送信先のプロトコルは BGP です。
Type	「Source Protocol」で「OSPF」を選択した場合、これは設定可能となります。 • All - OSPF AS-internal と OSPF AS-external の両方のルートを RIP または BGP に再配布します。 • Internal - OSPF AS-internal ルートだけに再配布します。 • External - Ext Type1 と Ext Type2 ルートを含む OSPF AS-external ルートだけに再配布します。 • External Type1 - OSPF AS-external type-1 ルートだけを再配布します。 • External Type2 - OSPF AS-external type-2 ルートだけを再配布します。 • Internal-E1 - OSPF AS-external type-1 と OSPF AS-internal ルートだけを再配布します。 • Internal-E2 - OSPF AS-external type-2 と OSPF AS-internal ルートだけを再配布します。
Metric (0-4294967295)	再配布ルートに RIP メトリックを指定します。
Route Map Name	特定のルートを再配布するかどうか決定する基準として使用されるルートマップを指定します。

「Apply」をクリックし、設定内容を適用します。

エントリの検索
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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

「Please Select」をクリックすると、次の画面が表示されます。



図 9-166 Please Select（VRF）画面

使用する VRF 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。

BGP Route Preference Settings（BGP ルート優先設定）

BGP Route Preference Settings（BGP ルート優先設定）の設定、表示を行います。

L3 Features > BGP > BGP Route Preference Settings の順にメニューをクリックして以下の画面を表示します。

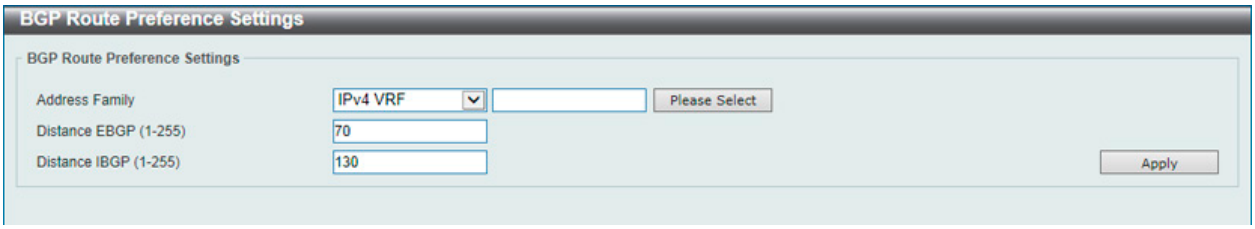


図 9-167 BGP Route Preference Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Distance EGBP	ディスタンス eBGP ルート優先値（1-255: IPv4/VRF アドレスファミリー）（1-254: IPv6/VRF アドレスファミリー）を指定します。
Distance IBGP	ディスタンス iBGP ルート優先値（1-255: IPv4/VRF アドレスファミリー）（1-254: IPv6/VRF アドレスファミリー）を指定します。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-168 Please Select（VRF）画面

使用する VRF 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。

BGP Dampening Settings（BGP ダンプニング設定）

Border Gateway Protocol(BGP) 処理のダンプニング設定を行います。本コマンドの目的は、ルートのダンプニングを排除して、フラッピングルートによりネットワークが不安定になることを避けることにあります。

L3 Features > BGP > BGP Dampening Settings の順にメニューをクリックして以下の画面を表示します。

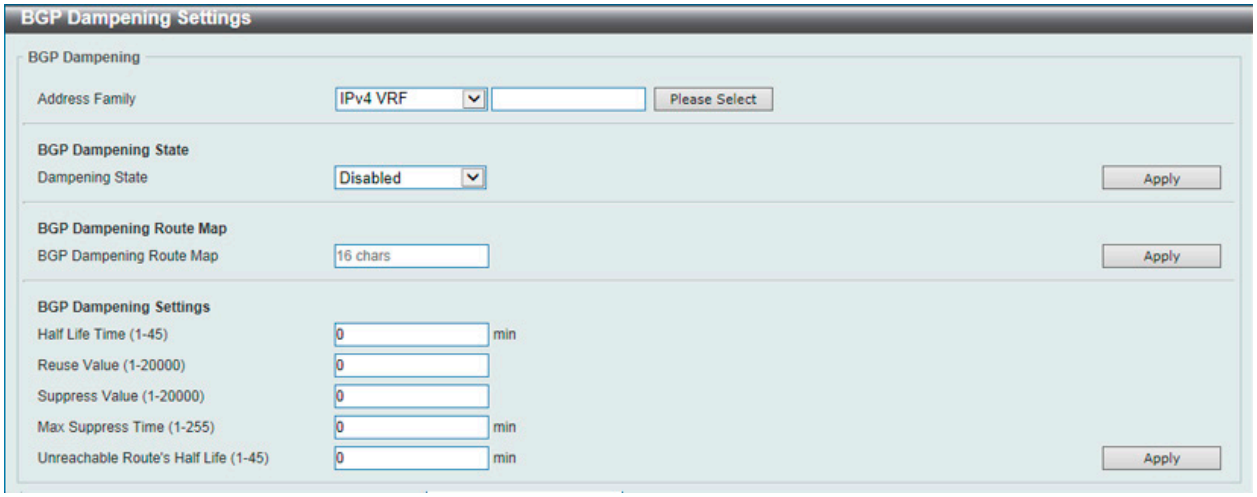


図 9-169 BGP Dampening Settings 画面

以下の項目を使用して設定を行います。

項目	説明
BGP Dampening	
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
BGP Dampening	
Dampening State	プルダウンメニューを使用して、BGP ダンプニング機能の状態を「Enabled」(有効)/「Disabled」(無効) にします。
BGP Dampening Route Map	
BGP Dampening Route Map	BGP ダンプニングルートマップ名（16 字以内）を入力します。
BGP Dampening Settings	
Half Life Time (1-45)	到達経路のペナルティが半分にダウンする時間 (分) を指定します。 初期値は 15(分) です。
Reuse Value (1-20000)	再利用値を入力します。フラッピングルートへのペナルティが本値以下にダウンすると、ルートは抑制されません。初期値は 750 です。
Suppress Value (1-20000)	抑制値を入力します。ペナルティがこの制限を超過すると、ルートは抑制されます。初期値は 2000 です。
Max Suppress Time (1-255)	ルートが抑制される最大時間 (分) を入力します。初期値は 60(分) です。
Un Reachability Half Life (1-45)	未到達経路のペナルティが半分にダウンする時間 (分) を指定します。初期値は 15(分) です。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-170 Please Select（VRF）画面

使用する VRF 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。

BGP Dampening Dampened Paths Table（BGP ダンプニングダンプドパステーブル）

BGP Dampening Dampened Paths Table（BGP ダンプニングダンプドパステーブル）の表示、クリアをしてします。

L3 Features > BGP > BGP Dampening Dampened Paths Table の順にメニューをクリックして以下の画面を表示します。

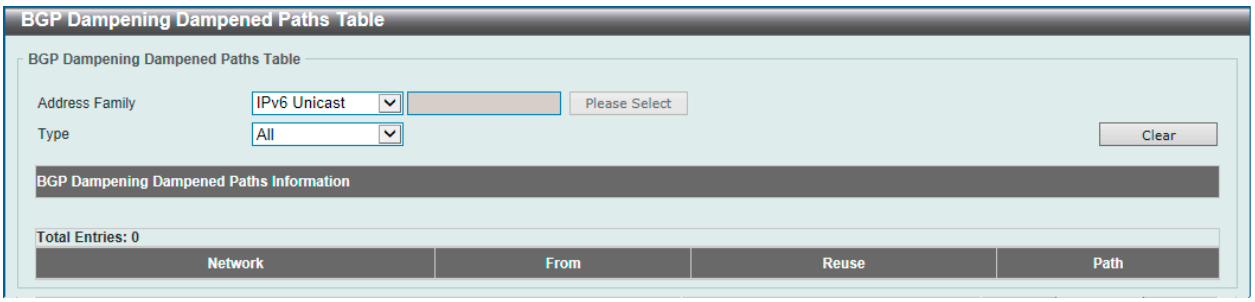


図 9-171　BGP Dampening Dampened Paths Table 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Type	ダンプニングダンプドパスの「Type」を指定します。 • All - 全ての BGP ダンプニングダンプドパスを表示、クリアします。 • IP Address - 入力した IPv4 アドレスに基づく BGP ダンプニングダンプドパスを表示、クリアします。 • Network Address - 入力した IPv4 ネットワークアドレスに基づく BGP ダンプニングダンプドパスを表示、クリアします。 • IPv6 Address - 入力した IPv6 アドレスに基づく BGP ダンプニングダンプドパスを表示、クリアします。 • IPv6 Network Address - 入力した IPv6 ネットワークアドレスに基づく BGP ダンプニングダンプドパスを表示、クリアします。

「Clear」をクリックすると入力したエントリをクリアします。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-172　Please Select（VRF）画面

使用する VRF 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。

BGP Dampening Flap Statistics Table（BGP ダンプニングフラップ統計テーブル）

BGP Dampening Flap Statistics Table（BGP ダンプニングフラップ統計テーブル）の表示、クリアをしてします。

L3 Features > BGP > BGP Dampening Flap Statistics Table の順にメニューをクリックして以下の画面を表示します。

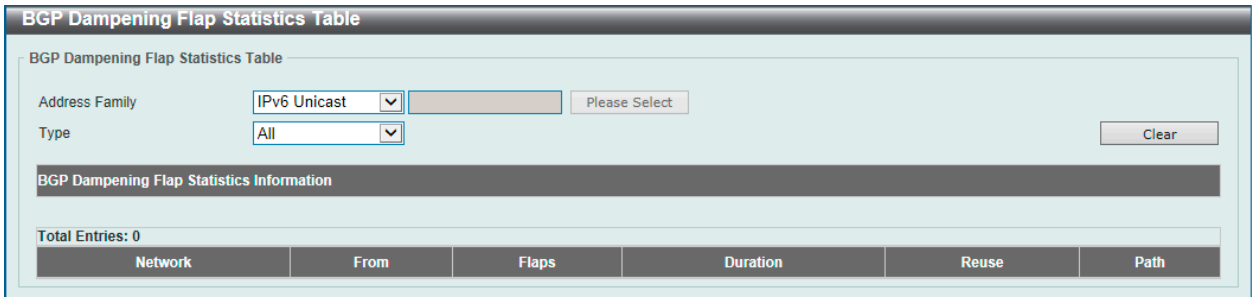


図 9-173 BGP Dampening Flap Statistics Table 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Type	「Type」を指定します。 • All - 全ての BGP ダンプニングフラップ統計を表示、クリアします。 • IP Address - 入力した IPv4 アドレスに基づく BGP ダンプニングフラップ統計を表示、クリアします。 • Network Address - 入力した IPv4 ネットワークアドレスに基づく BGP ダンプニングフラップ統計を表示、クリアします。 • IPv6 Address - 入力した IPv6 アドレスに基づく BGP ダンプニングフラップ統計を表示、クリアします。 • IPv6 Network Address - 入力した IPv6 ネットワークアドレスに基づく BGP ダンプニングフラップ統計を表示、クリアします。

「Clear」をクリックすると入力したエントリをクリアします。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-174 Please Select（VRF）画面

使用する VRF 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。

BGP Reflector Settings（BGP リフレクタ設定）

BGP リフレクタの設定、表示を行います。

L3 Features > BGP > BGP Reflector Settings の順にメニューをクリックして以下の画面を表示します。

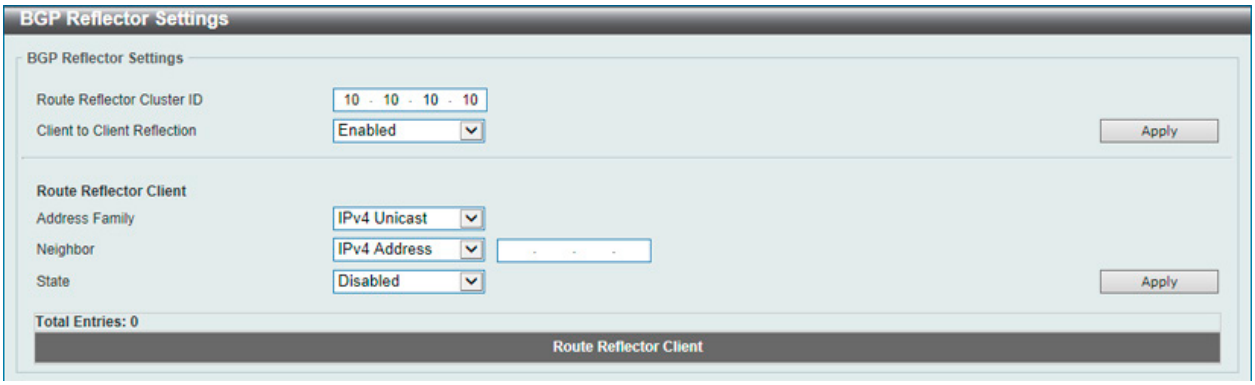


図 9-175　BGP Reflector Settings 画面

以下の項目を使用して設定を行います。

項目	説明
BGP Reflector Settings	
Route Reflector Cluster ID	クラスタ ID の IP アドレスを指定します。
Client to Client Reflection	クライアントからクライアントへのリフレクションを有効または無効にします。
BGP Reflector Client	
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	クライアントとなる「Neighbor」を指定します。 • IPv4 Address - ネイバリングルータの IPv4 アドレスを指定します。 • Peer Group - ルートリフレクタクライアントとなるピアグループ名を指定します。 • IPv6 Address - ネイバリングルータの IPv6 アドレスを指定します。
State	状態を有効または無効にします。有効にすると、指定した Neighbor は、BGP リフレクタクライアントになります。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

BGP Confederation Settings（BGP コンフェデレーション設定）

BGP のコンフェデレーション設定を行います。

L3 Features > BGP > BGP Confederation Settings の順にメニューをクリックして以下の画面を表示します。

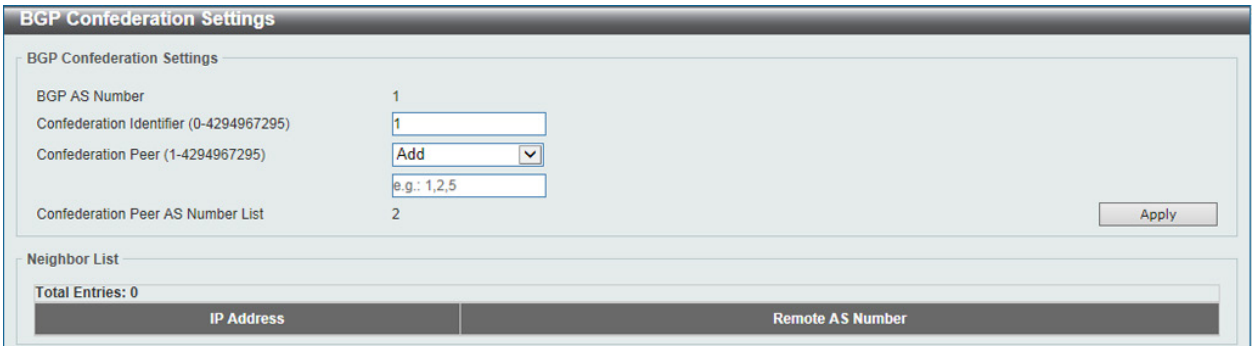


図 9-176　BGP Confederation Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Confederation Identifier (0-4294967295)	BGP コンフェデレーションを指定するのに使用する AS 番号を入力します。
Confederation Peer	プルダウンメニューを使用して追加（Add）または削除（Delete）を選択し、BGP コンフェデレーションピア ID(1-4294967295) を指定します。

「Apply」ボタンをクリックして行った変更を適用します。

BGP AS Path Access List Settings（BGP AS パスアクセスリストリスト設定）

AS パスアクセスリストを設定します。

L3 Features > BGP > BGP AS Path Access Settings の順にメニューをクリックして以下の画面を表示します。

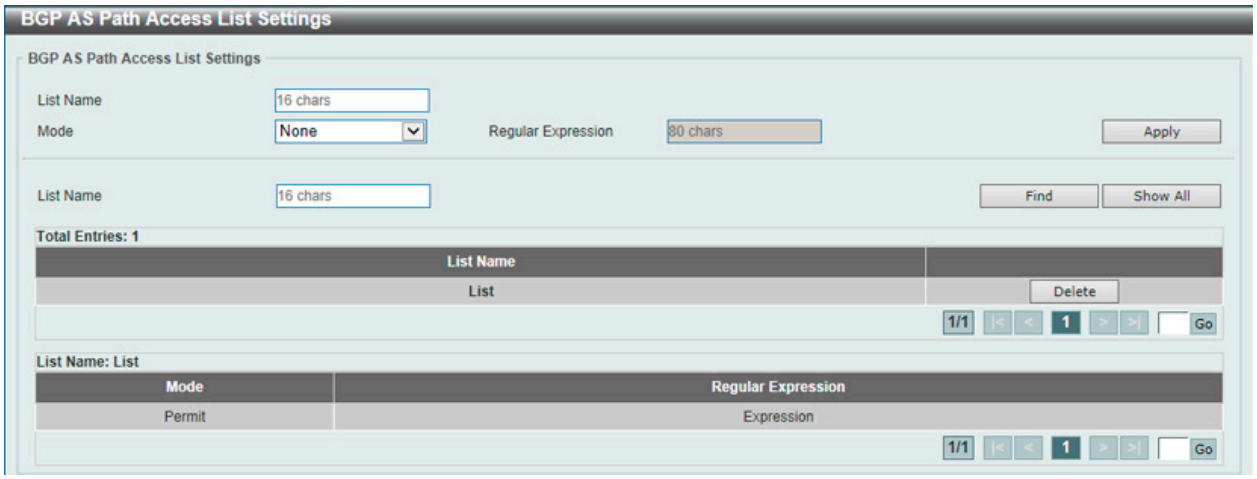


図 9-177 BGP AS Path Access List Settings 画面

以下の項目を使用して設定を行います。

項目	説明
List Name	AS パスアクセスリスト名を入力します。
Mode	プルダウンメニューを使用して、条件の一致に基づいて通知について「Permit」（許可）、「Deny」（拒否）または「None」（何もしない）を指定します。
Regular Expression	as_path フィルタを定義する正規表現（80 字以内）を入力します。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの参照

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

エントリの削除

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

BGP Community List Settings（BGP コミュニティリスト設定）

BGP コミュニティリストに照合ルールを設定します。

L3 Features > BGP > BGP Community List Settings の順にメニューをクリックして以下の画面を表示します。

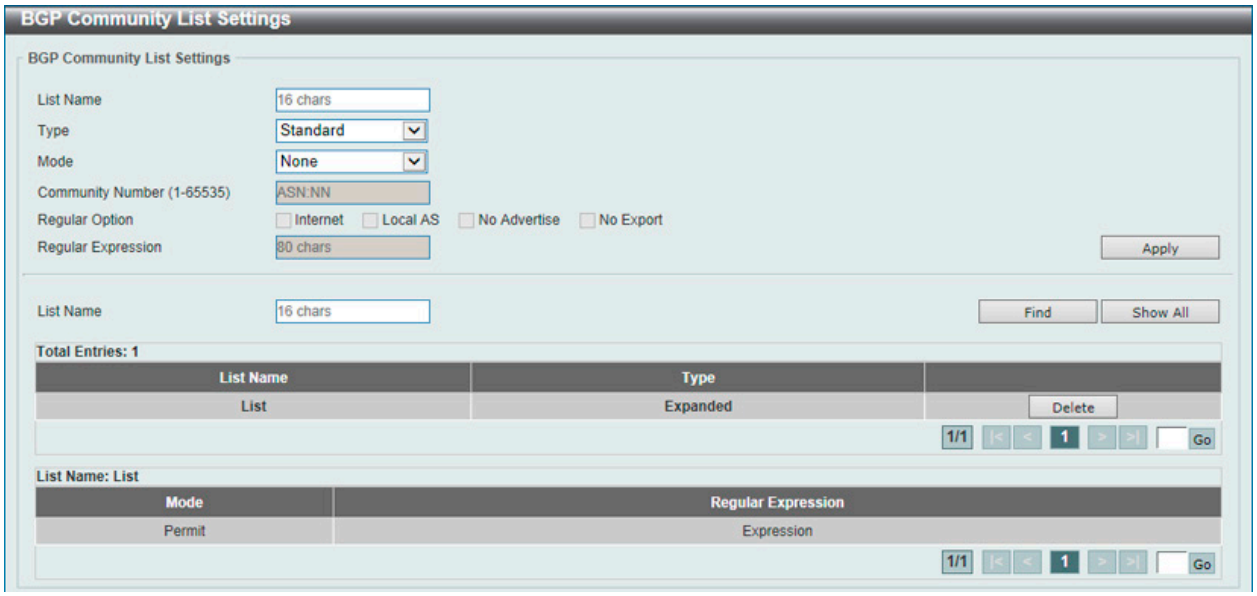


図 9-178 BGP Community List Settings 画面

以下の項目を使用して設定を行います。

項目	説明
List Name	コミュニティリスト名（16 字以内）を入力します。
Type	プルダウンメニューを使用して Standard または Expanded を選択します。Standard は標準的なコミュニティリストを設定し、Expanded は拡大コミュニティリストを設定します。
Mode	プルダウンメニューを使用して、ルールが一致した場合のルートのアクション「Permit」（許可）、「Deny」（拒否）または「None」（何もしない）を指定します。
Community Number	コミュニティ番号を指定します。「AA:NN」の形式のユーザ定義の番号で、「AA」は AS 番号、「NN」はユーザが定義する番号を指定します。スペースによって区切られた複数のコミュニティ番号も指定可能です。
Regular Option	標準的なオプションを選択します。 • Internet - このコミュニティを持つルートをすべてのピア (内部または外部) に送信します。 • Local AS - このコミュニティを持つルートは同じ AS のピアに送信されますが、同じコンフェデレーション内の別のサブ AS にあるピアと外部のピアには送信されません。 • No Advertise - このコミュニティを持つルートはどんなピア (内部または外部) にも通知されません。 • No Export - このコミュニティを持つルートはコンフェデレーション内の同じ AS か別のサブ AS にあるピアに送信されますが、外部の BGP(eBGP) ピアには送信されません。
Regular Expression	コミュニティセットの値を入力します。80 文字以内で指定します。

「Apply」ボタンをクリックして行った変更を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。
削除するエントリの「Delete」ボタンをクリックします。

BGP Extended Community List Settings（BGP 拡張コミュニティリスト設定）

BGP 拡張コミュニティリストを設定します。

L3 Features > BGP > BGP Extended Community List Settings の順にメニューをクリックして以下の画面を表示します。

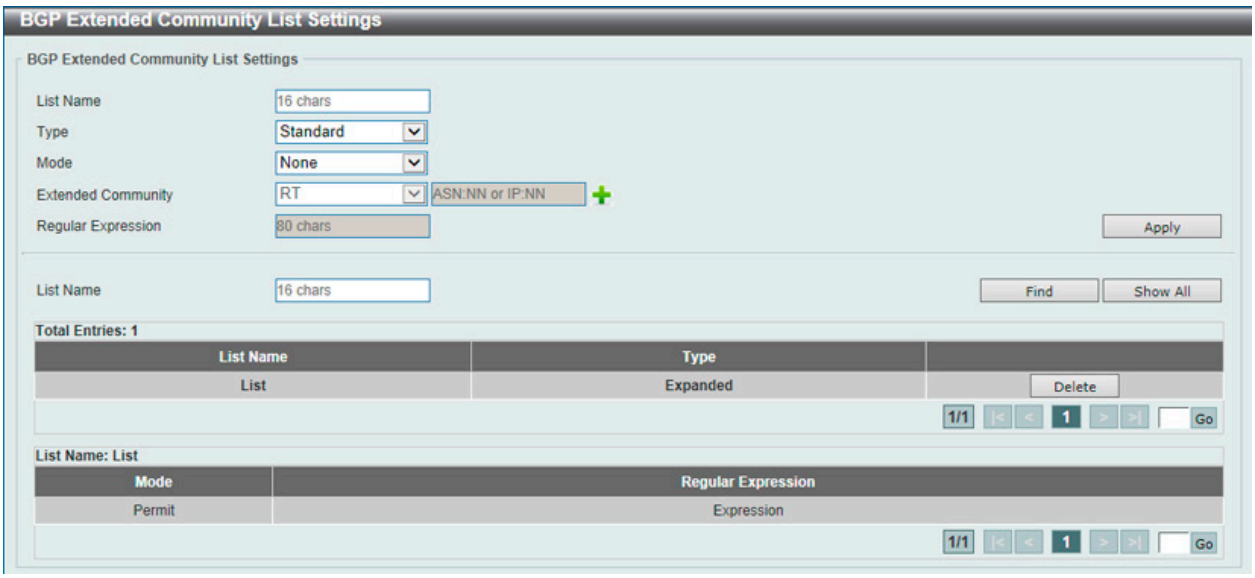


図 9-179 BGP Extended Community List Settings 画面

以下の項目を使用して設定を行います。

項目	説明
List Name	拡張コミュニティリスト名（16 字以内）を入力します。
Type	プルダウンメニューを使用して Standard または Expanded を選択します。Standard は標準的な拡張コミュニティリストを設定し、Expanded は拡大拡張コミュニティリストを設定します。
Mode	プルダウンメニューを使用して、ルールが一致した場合のルートのアクション「Permit」（許可）、「Deny」（拒否）または「None」（何もしない）を指定します。
Extended Community	拡張コミュニティを指定します。 • RT -「Route Target」(RT) を使用します。 • SoO -「Site-of-Origin」(SoO) を使用します。 表示される欄に拡張コミュニティ文字列を入力します。
Regular Expression	コミュニティセットの値を入力します。80 文字以内で指定します。

「Apply」ボタンをクリックして行った変更を適用します。

BGP Clear Settings（BGP クリア設定）

ハードまたはソフト再構成を使用して Border Gateway Protocol(BGP) をリセットします。

L3 Features > BGP > BGP Clear Settings の順にメニューをクリックして以下の画面を表示します。

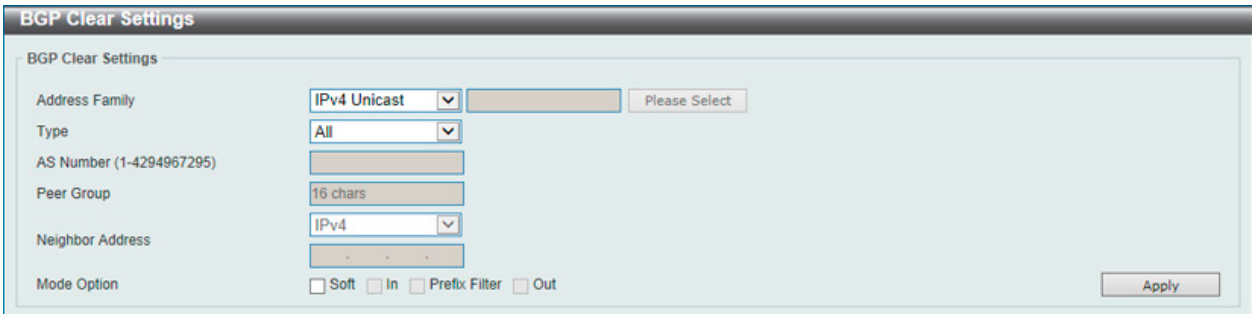


図 9-180 BGP Clear Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。 • VPNv4 - VPNv4 アドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Type	BGP タイプを指定します。 • All - 指定アドレスの全ての BGP ピアセッションをクリアします。 • AS Number - 指定した AS の BGP ピアセッションをクリアします。 • Peer Group - ピアグループの BGP ピアセッションをクリアします。 • Neighbor Address - ネイバアドレスの BGP ピアセッションをクリアします。 • External - ハード / ソフト再設定を使用した BGP ピアセッションをクリアします。
AS Number (1-4294967295)	「Type」メニューで「AS」を選択した場合、AS 番号を入力します。
Peer Group	「Type」メニューで「Peer Group」を選択した場合、ピアグループ名を入力します。
Mode Option	希望のモードをチェックします。: Soft、In、Prefix Filter または Out • Soft - ソフトリセットを開始します。セッションを切断しません。 • In - 内向き再構成を開始します。 • Prefix Filter - 既存の Outbound Route Filter (ORF) プリフィクスリストをクリアすることで、ピアルータからの ORF プリフィクスリストを更新し、新しいルートの更新を行います。 • Out - 外向きの再構成を開始します。 「in」も「out」キーワードも指定されないと、内向きと外向きのセッションの両方がリセットされます。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

BGP Summary Table（BGP サマリテーブル）

BGP サマリ情報を表示します。

L3 Features > BGP > BGP Summary Table の順にメニューをクリックして以下の画面を表示します。

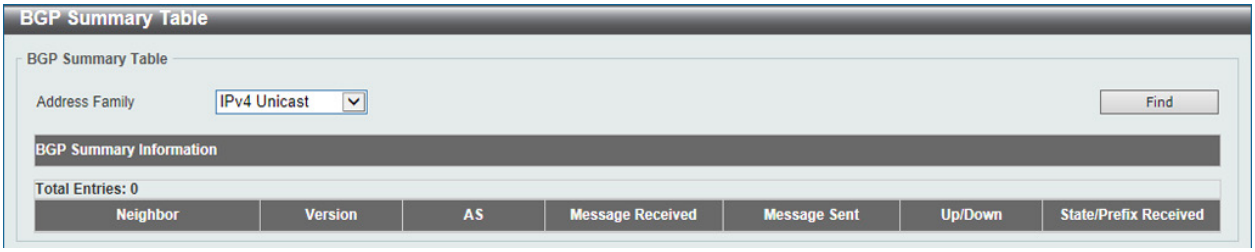


図 9-181 BGP Summary Table 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。 • IPv6 Multicast - IPv6 マルチキャストアアドレスファミリーを指定します。 • VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。 • VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。 • VPNv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-182 Please Select（VRF）画面

使用する VRF 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。

BGP Routing Table（BGP ルーティングテーブル）

BGP ルーティングを表示します。

L3 Features > BGP > BGP Routing Table の順にメニューをクリックして以下の画面を表示します。



図 9-183 BGP Routing Table 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。 • VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。 • VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。 • VPNv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • L2VPN VPLS All - L2VPN VPLS アドレスファミリーの全情報を指定します。 • L2VPN VPLS RD - L2VPN VPLS アドレスファミリーの Route Distinguisher (RD) 情報を指定します。 • L2VPN VPLS VFI - L2VPN VPLS アドレスファミリーの VFI インスタンス（12 字以内）を指定します。

項目	説明
Type	プルダウンメニューを使用して、「Type」を指定します。選択タイプに基づいて以下のパラメータを変更します。 • IP Address - 特定の IPv4 アドレス /IPv6 アドレスを指定します。 • Netowork - 特定の IPv4/IPv6 ネットワークアドレスを指定します。「Longer Prefixes」をチェックして、指定ルートの通知を停止します。 • Route Map - ルートマップを指定します。「Route Map Name」ルートマップ名（16 字以内）/「L2VPN Prefix」に一致するルートを表示します。 • CIDR Only - CIDR（Classless Inter-Domain Routing）を指定します。 • Community - BGP コミュニティを指定します。「Community Set」コミュニティセットを入力します。「Local AS」- ローカル AS の外側には送信しません。(既知のコミュニティ)。「No Advertise」- どんなピアにも通知しません。(既知のコミュニティ)。「No Export」- ネクスト AS にエクスポートしません。(既知のコミュニティ)。「Internet」- インターネットに送信します (既知のコミュニティ)。「Exact Match」- 指定されると、コミュニティは正確に一致する必要があります。「L2VPN Prefix」- L2VPN プリフィクスを入力します。 • Community List - コミュニティリストを入力します。「Exact Match」が指定されると、コミュニティは正確に一致する必要があります。「L2VPN Prefix」- L2VPN プリフィクスを入力します。 • Filter List -「Filter List Name」フィルタリスト名を入力します。「L2VPN Prefix」- L2VPN プリフィクスを入力します。 • Inconsistent AS - 同じプレフィックスと異なる AS パスオリジンを持つ場合にルートを表示します。「L2VPN Prefix」- L2VPN プリフィクスを入力します。 • Quote Regexp -「Regexp」-「Regular Expression」にマッチするルートを指定します。「L2VPN Prefix」- L2VPN プリフィクスを入力します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-184 Please Select（VRF）画面

使用する VRF 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。

BGP Labels Table（BGP ラベルテーブル）

BGP ラベルテーブルを表示します。

L3 Features > BGP > BGP Labels Table の順にメニューをクリックして以下の画面を表示します。

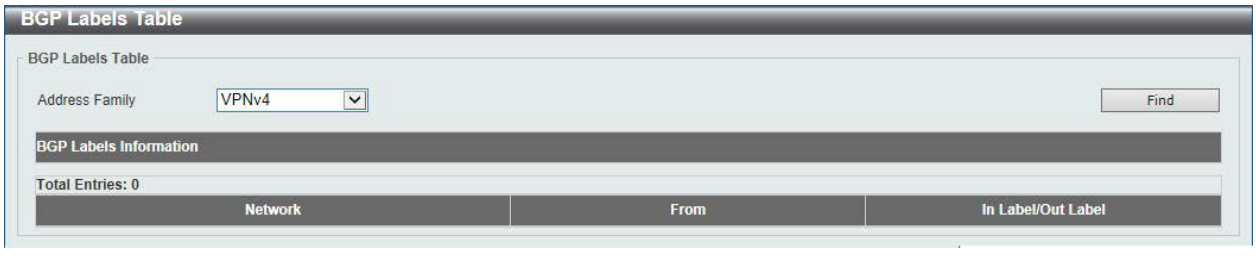


図 9-185 BGP Labels Table 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。 • VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。 • VPNv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-186　Please Select（VRF）画面

使用する VRF 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。

BGP Neighbor（BGP ネイバ設定）

Neighbor（ネイバ設定）

BGP ネイバを設定、表示します。

L3 Features > BGP > BGP Neighbor > Neighbor の順にメニューをクリックして以下の画面を表示します。

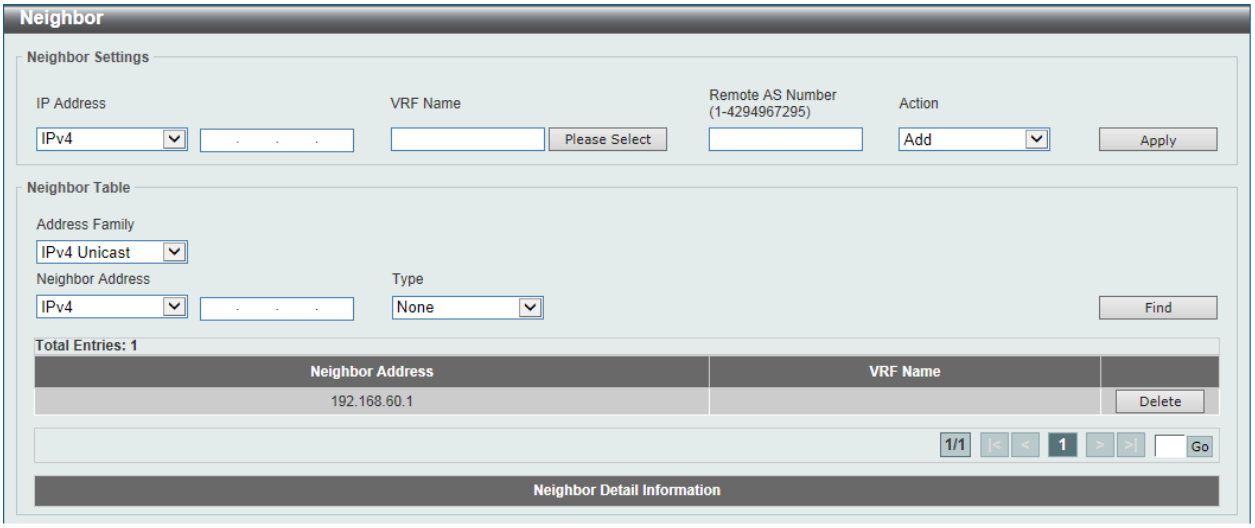


図 9-187　Neighbor（BGP）画面

以下の項目を使用して設定を行います。

項目	説明
Neighbor Settings	
IP Address	ネイバルータの IPv4/IPv6 アドレスを指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Please Select」で事前に設定済みの VRF を選択することが可能です。
Remote AS Number (1-4294967295)	リモート AS 番号を入力します。範囲は 1-4294967295 です。
Action	実行する動作を指定します。「Add」（追加）「Delete」（削除）から指定します。
Neighbor Table	
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。 • VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。 • VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。 • VPNv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • L2VPN VPLS - L2VPN VPLS アドレスファミリーの全情報を指定します。
Neighbor Address	ネイバルータの IPv4/IPv6 アドレスを指定します。

項目	説明
Type	プルダウンメニューを使用して各種タイプを選択します。 • None - 表示するタイプを指定しません。 • Advertised Routes - BGP Neighbor に通知されるルートを表示します。 • Received Routes - この Neighbor から受信したルートを表示します。 • Routes - Neighbor から学習したルーティングテーブル内のルートを表示します。 • Received Prefix Filter - BGP Neighbor から受信したプレフィックスフィルタ情報を表示します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-188 Please Select（VRF）画面

使用する VRF 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。

Peer Group（Peer グループ設定）

Border Gateway Protocol (BGP) ネイバ Peer グループを設定します。

L3 Features > BGP > BGP Neighbor > Peer Group の順にメニューをクリックして以下の画面を表示します。

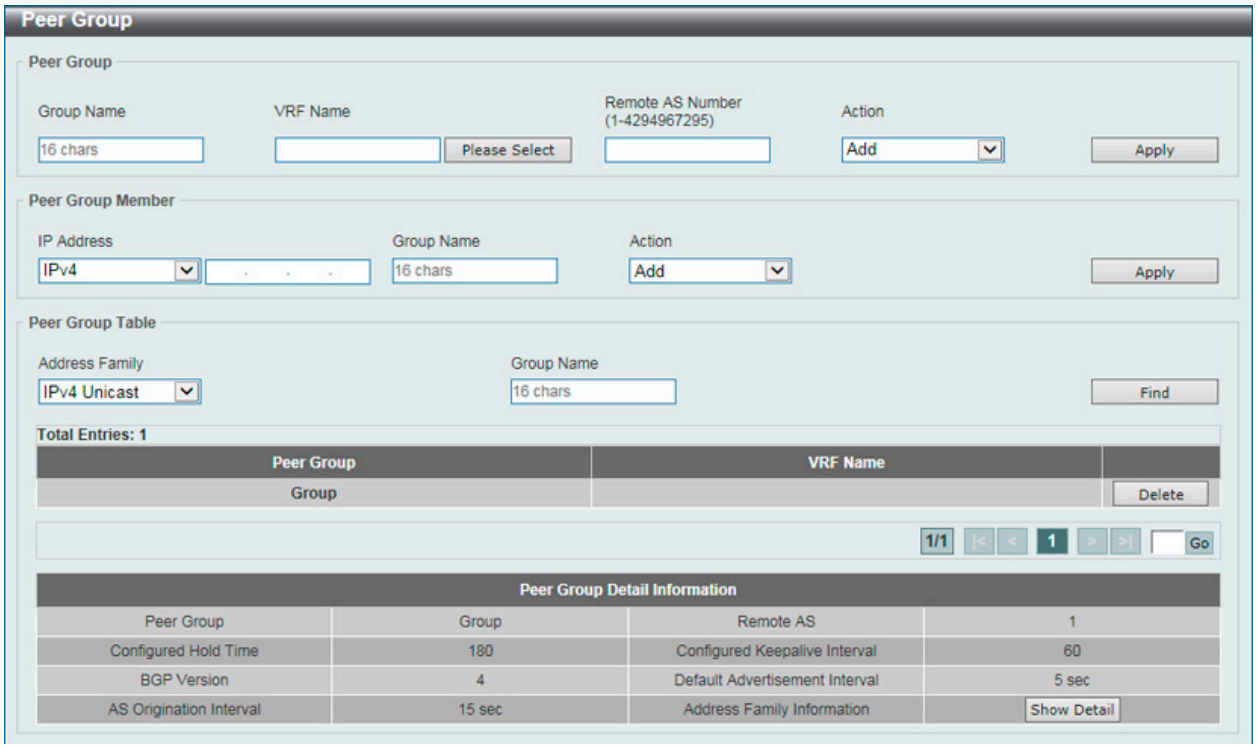


図 9-189 Peer Group 画面

以下の項目を使用して設定を行います。

項目	説明
Peer Group	
Group Name	BGP ピアグループ名（16 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Please Select」で事前に設定済みの VRF を選択することが可能です。

項目	説明
Remote AS Number (1-4294967295)	リモート AS 番号を入力します。範囲は 1-4294967295 です。
Action	実行する動作を指定します。「Add」（追加）「Delete」（削除）から指定します。
Peer Group Member	
IP Address	ピアグループメンバの IPv4/IPv6 アドレスを指定します。
Group Name	BGP ピアグループ名（16 字以内）を指定します。
Action	実行する動作を指定します。「Add」（追加）「Delete」（削除）から指定します。
Peer Group Table	
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • VPNv4 All - 全 VPNv4 アドレスファミリーを指定します。 • VPNv4 RD - Route Distinguisher (RD) VPNv4 アドレスファミリーを指定します。 • VPNv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。
Group Name	BGP ピアグループ名（16 字以内）を指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-190 Please Select（VRF）画面

使用する VRF 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。

「Show Detail」をクリックすると、次の画面が表示されます。

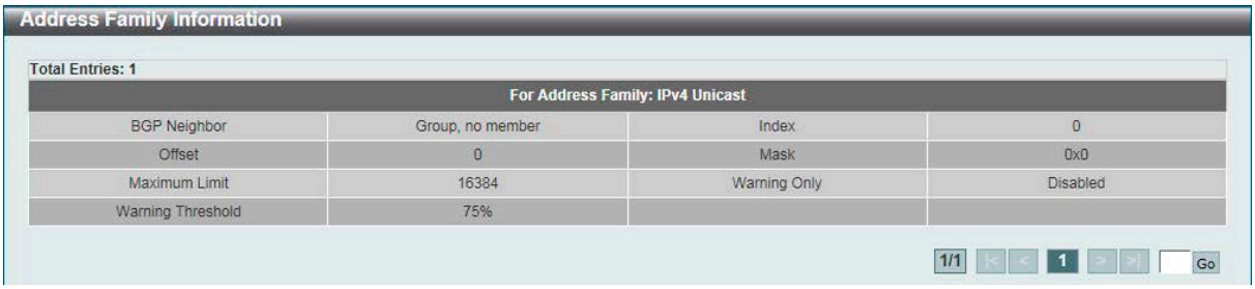


図 9-191 Show Detail（Peer Group）画面

「Back」をクリックすると前のページに戻ります。
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。

Neighbor Activate（ネイバ有効化）

Border Gateway Protocol (BGP) ネイバを有効化します。

L3 Features > BGP > BGP Neighbor > Neighbor Activate の順にメニューをクリックして以下の画面を表示します。

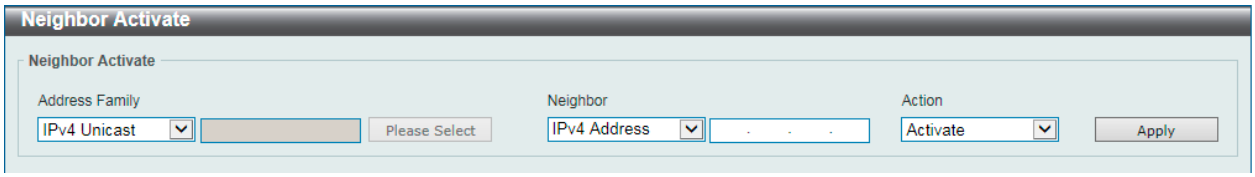


図 9-192 Neighbor Activate 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。 • VPNv4 - VPNv4 アドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。 • IPv4 Address - ネイバの IPv4 アドレスを指定します。 • Peer Group - ネイバとなるピアグループ名を指定します。 • IPv6 Address - ネイバの IPv6 アドレスを指定します。
Action	実行する動作を指定します。「Activate」（有効化）「Activate」（無効化）から指定します。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-193 Please Select（VRF）画面

使用する VRF 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。

Neighbor Shutdown（ネイバシャットダウン）

Border Gateway Protocol (BGP) ネイバをシャットダウンします。

L3 Features > BGP > BGP Neighbor > Neighbor Shutdown の順にメニューをクリックして以下の画面を表示します。

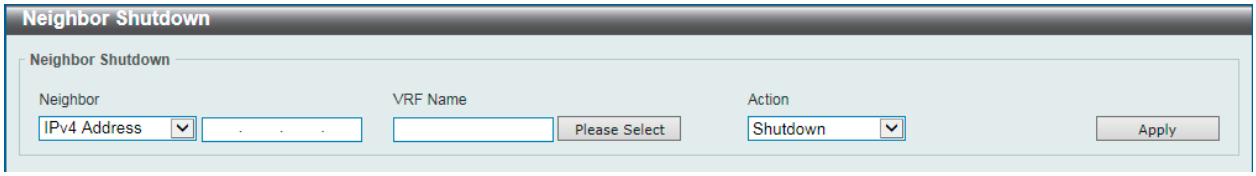


図 9-194 Neighbor Shutdown 画面

以下の項目を使用して設定を行います。

項目	説明
Neighbor	ネイバを選択、指定します。 • IPv4 Address - ネイバの IPv4 アドレスを指定します。 • Peer Group - ネイバのピアグループ名を指定します。 • IPv6 Address - ネイバの IPv6 アドレスを指定します。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Please Select」で事前に設定済みの VRF を選択することが可能です。
Action	実行する動作を指定します。「Shutdown」「No Shutdown」から指定します。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-195 Please Select（VRF）画面

使用する VRF 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。

Neighbor Map Settings（ネイバマップ設定）

Border Gateway Protocol (BGP) ネイバマップを設定、表示します。

L3 Features > BGP > BGP Neighbor > Neighbor Map Settings の順にメニューをクリックして以下の画面を表示します。

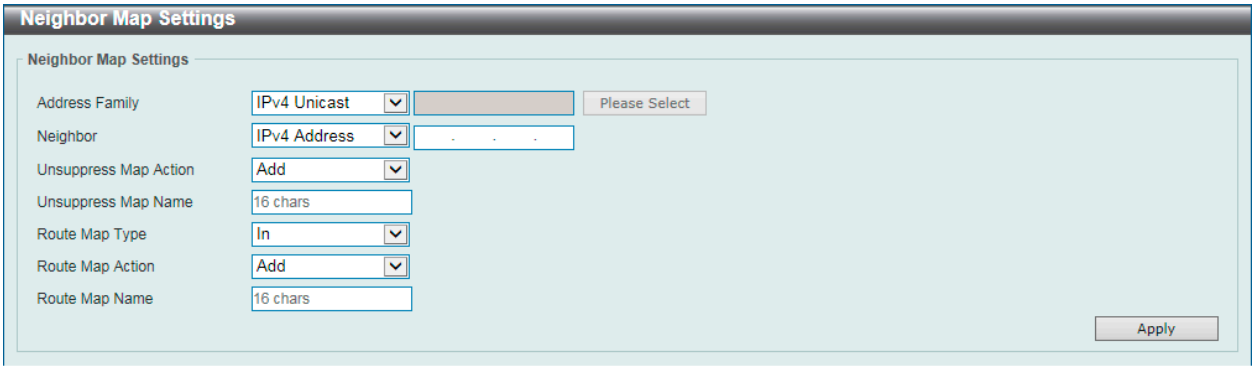


図 9-196 Neighbor Map Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。 • VPNv4 - VPNv4 アドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。 • IPv4 Address - ネイバの IPv4 アドレスを指定します。 • Peer Group - ネイバとなるピアグループ名を指定します。 • IPv6 Address - ネイバの IPv6 アドレスを指定します。
Unsuppress Map Action	「Unsuppress Map Action」の設定を行います。アドレスアグリゲートにより抑制されている通知ルートを選択的に使用するルータマップ名を追加 / 削除「Add」「Delete」します。
Unsuppress Map Name	アドレスアグリゲートにより抑制されている通知ルートを選択的に使用するルートマップ名 (16 字以内) を指定します。
Route Map Type	プルダウンメニューを使用して In または Out を選択します。In は Neighbor からの内向きルートで、Out はピアに送信する外向きルートを示します。
Route Map Action	ルートマップの動作を追加または削除から指定します。
Route Map Name	内向きまたは外向きルートに適用するルートマップ名（16 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-197 Please Select（VRF）画面

使用する VRF 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。

Neighbor Filter Settings（ネイバフィルタ設定）

Border Gateway Protocol (BGP) ネイバフィルタを設定、表示します。

L3 Features > BGP > BGP Neighbor > Neighbor Filter Settings の順にメニューをクリックして以下の画面を表示します。

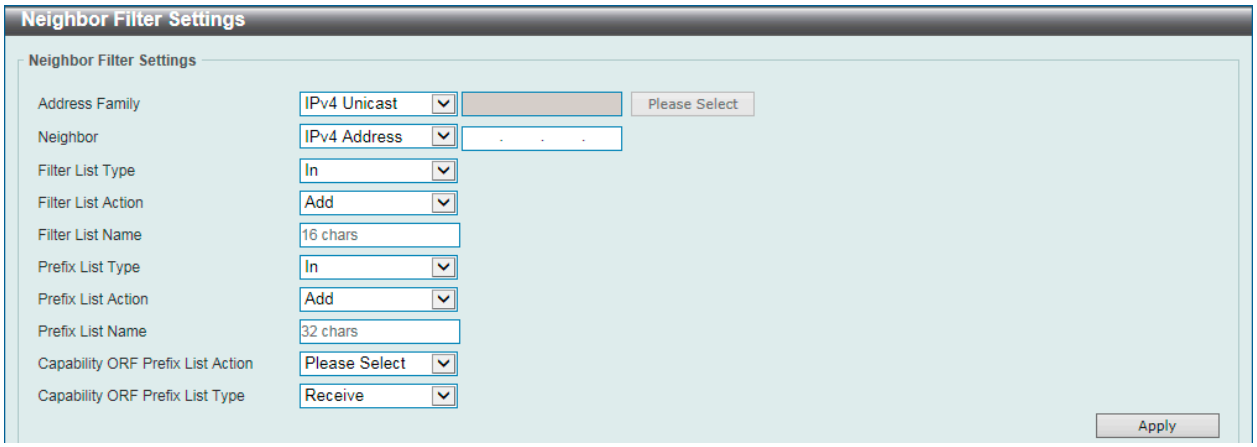


図 9-198 Neighbor Filter Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。 • VPNv4 - VPNv4 アドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。 • IPv4 Address - ネイバの IPv4 アドレスを指定します。 • Peer Group - ネイバとなるピアグループ名を指定します。 • IPv6 Address - ネイバの IPv6 アドレスを指定します。
Filter List Type	フィルタするルートの内向きまたは外向きを「In」または「Out」で指定します。
Filter List Action	フィルタリストの追加または削除を使用します。「Add」「Delete」で指定します。
Filter List Name	フィルタリスト名（16 字以内）を指定します。
Prefix List Type	フィルタするネイバ「から / へ」の通知を、内向きまたは外向き、「In」または「Out」で指定します。
Prefix List Action	プリフィクスリストの追加または削除を使用します。「Add」「Delete」で指定します。
Prefix List Name	プリフィクスリスト名（32 字以内）を指定します。
Capability ORF Prefix List Action	ORF プリフィクスリスト機能を有効 / 無効に指定します。BGP ORF 機能はピアのプリフィクス交換の数の減少に使用します。通常、ローカル / リモートルータのペアで指定します。単方向 / 双方向でも指定可能です。

項目	説明
Capability ORF Prefix List Type	外向きルートフィルタプレフィックスリスト機能を設定します。 以下の値と共に送信することができます。 • Receive - ORF プレフィックスリスト機能を受信方向に有効にします。ローカルルータはリモートルータによって通知されるプレフィックスフィルタリストをインストールします。 • Send - ORF プレフィックスリスト機能を送信方向に有効にします。ローカルルータは ORF プレフィックスリスト機能のためにリモートルータに通知します。 • Both - ORF プレフィックスリスト機能を送受信両方向で有効にします。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-199 Please Select（VRF）画面

使用する VRF 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。

Neighbor Maximum Prefix Settings（ネイバ最大プレフィクス設定）

Border Gateway Protocol (BGP) ネイバ最大プレフィクスを設定、表示します。BGP ネイバから受け入れることのできる最大プレフィクス数を指定します。

L3 Features > BGP > BGP Neighbor > Neighbor Maximum Prefix Settings の順にメニューをクリックして以下の画面を表示します。

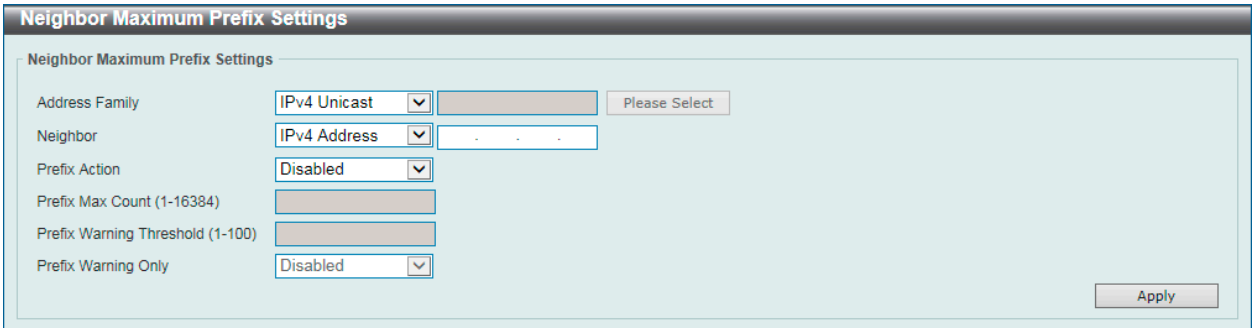


図 9-200 Neighbor Maximum Prefix Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。 • VPNv4 - VPNv4 アドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。 • IPv4 Address - ネイバの IPv4 アドレスを指定します。 • Peer Group - ネイバとなるピアグループ名を指定します。 • IPv6 Address - ネイバの IPv6 アドレスを指定します。
Prefix Action	プレフィクス動作を「有効 / 無効」から指定します。
Prefix Max Count (1-16384)	指定したネイバから許可されるプレフィックスの最大数を入力します。
Prefix Warning Threshold (1-100)	ルータにおける最大のプレフィックス制限が警告メッセージの生成を開始するパーセントを指定する整数を入力します。範囲は 1-100 です。

項目	説明
Prefix Warning Only	プルダウンメニューを使用して、プレフィックスの警告のみ「Enabled」(有効)/「Disabled」(無効) にします。ピアリングセッションを終了する代わりに最大のプレフィックス制限を超過する際にルータがログメッセージを生成することを許可します。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-201　Please Select（VRF）画面

使用する VRF 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。

Neighbor General Settings（ネイバー般設定）

Border Gateway Protocol (BGP) ネイバの一般設定を行います。

L3 Features > BGP > BGP Neighbor > Neighbor General Settings の順にメニューをクリックして以下の画面を表示します。

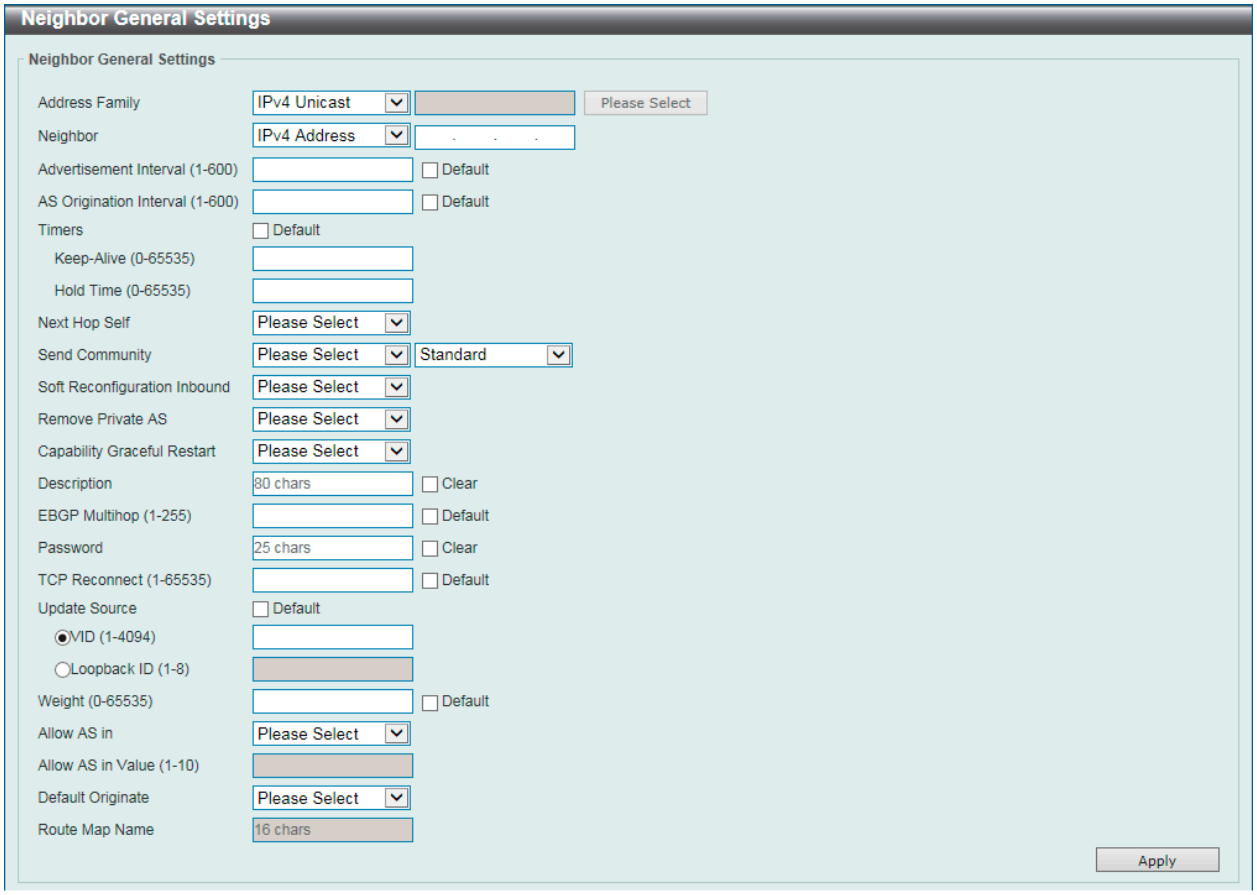


図 9-202　Neighbor General Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Address Family	アドレスファミリを選択します。 • IPv4 Unicast - IPv4 ユニキャストアドレスファミリーを指定します。 • IPv4 VRF - VRF インスタンス（12 字以内）を指定します。VRF インスタンス名を入力するか、「Please Select」で既存の VRF インスタンスを選択します。 • IPv4 Multicast - IPv4 マルチキャストアドレスファミリーを指定します。 • L2VPN VPLS - L2VPN VPLS アドレスファミリーを指定します。 • VPNv4 - VPNv4 アドレスファミリーを指定します。 • IPv6 Unicast - IPv6 ユニキャストアドレスファミリーを指定します。
Neighbor	ネイバを選択、指定します。 • IPv4 Address - ネイバの IPv4 アドレスを指定します。 • Peer Group - ネイバとなるピアグループ名を指定します。 • IPv6 Address - ネイバの IPv6 アドレスを指定します。
Advertisement Interval (1-600)	BGP プロセスがピアに更新メッセージを送信する間隔（1-600）を指定します。 「Default」を選択すると初期値を指定します。
AS Origination Interval (1-600)	AS の生成するルーティング更新を送信する最小間隔を入力します。範囲は 1-600 です。 「Default」を選択すると初期値を指定します。
Timers	タイマーを指定します。 • Keepalive (0-65535) - keepalive メッセージがピアに送信される間隔を指定します。BGP 接続を実装する 2 つのルータが、異なる keepalive タイマを持つ場合、小さい方の keepalive タイマは設定されません。範囲は 0-65535 です。keepalive 値が 0 に設定されると、keepalive メッセージは送信されません。ネイバ指定の keepalive 設定をクリアします。 • Hold Time (0-65535) - keepalive メッセージが本値を超えても受信されないと、システムはピアを Dead として判断します。BGP 接続を実装する 2 つのルータが、異なる保持時間を持つ場合、小さい保持時間が使用されます。範囲は 0-65535 です。
Next Hop Self	ネクストホップセルフ属性を有効または無効にします。
Send community	「Standard」「Extended」「Both」を選択します。これは BGP Neighbor に送信される（されない）コミュニティ属性を指定します。 • Standard - 標準コミュニティだけが送信されます（されません）。 • Extended - 拡張コミュニティだけが送信されます（されません）。 • Both - 標準 / 拡張、どちらのコミュニティも送信されます（されません）。
Soft Reconfiguration Inbound	内向きソフト再構成機能を有効または無効にします。
Remove Private AS	本設定が有効になると、BGP 更新パケットにおける AS パス属性内のプライベートの AS 番号は破棄されます。
Capability Graceful Restart	グレースフルリスタート機能を有効 / 無効に指定します。 ネイバにグレースフルリスタート機能の有効 / 無効を通知します。
Description	BGP ネイバの概要（80 字以内）を指定します。「Clear」を選択すると概要を消去します。
EBGP Multihop (1-255)	ネイバに送信される eBGP マルチホップ TTL（1-255）を指定します。これによりルータはローカルピアと直接接続していない eBGP ピアとの BGP セッションを構築します。「Default」を選択すると初期値を指定します。
Password	BGP ピア間で使用するパスワード（25 字以内）を指定します。「Clear」を選択すると消去します。
TCP Reconnect	TCP 再接続ポート値（1-65535）を指定します。TCP 接続が失敗した後、BGP が TCP 接続リクエストをピアに送信する際の最小間隔値を指定します。「Default」を選択すると初期値（120 秒）を指定します。
Update Source	TCP 接続の BGP セッションによって使用されるインタフェースを指定します。「Default」を選択すると初期値を指定します。 • VID - VLAN ID（1-4094）を指定します。 • Loopback - ループバックインタフェースの ID（1-8）を指定します。
Weight	BGP ウェイト値（0-65535）を指定します。 指定ネイバからの受信したルートにアサインするウェイトを指定します。 「Default」を選択すると初期値を指定します。
Allow AS in	「Allow AS In」を有効 / 無効に指定します。これによりルータは受信 BGP パケット内に自身の AS 番号を表示させることができます。
Allow AS in Value (1-10)	「Allow AS In」値（1-10）を指定します。 ローカル AS の最大数を指定し、アップデートパケットの AS パス属性に表示させます。
Default Originate	デフォルトオリジネート機能を有効または無効にします。これによりネイバへのデフォルトルートの起動を有効にします。
Route Map Name	ルートマップ名（1-16）を指定します。

「Apply」をクリックし、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-203 Please Select（VRF）画面

使用する VRF 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。

BFD（Bidirectional Forwarding Detection）

L3 Features > BFD

BFD Settings（BFD 設定）

Bidirectional Forwarding Detection (BFD) の設定、表示を行います。

L3 Features > BFD > BFD Settings の順にメニューをクリックして以下の画面を表示します。

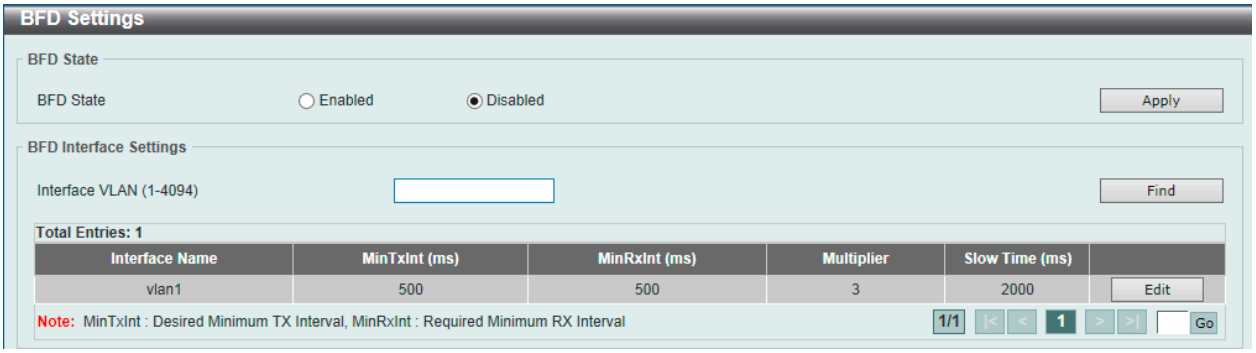


図 9-204 BFD Settings 画面

以下の項目を使用して設定を行います。

項目	説明
BFD State	
BFD State	BFD を有効 / 無効に指定します。
BFD Interface Settings	
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

対象エントリで「Edit」をクリックすると次の画面が表示します。

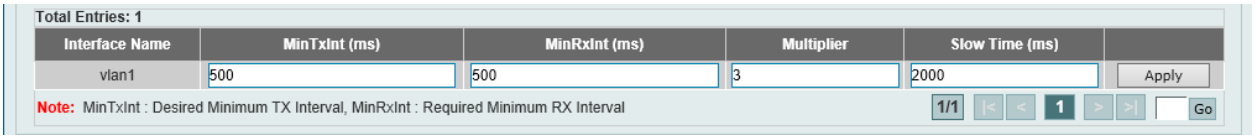


図 9-205 BFD Settings (Edit) 画面

以下の項目を使用して設定を行います。

項目	説明
MinTxInt	BFD パケットを送信する最小間隔値（50-1000 ミリ秒）を指定します。
MinRxInt	システムがサポートする BFD パケットを受信する最小間隔値（50-1000 ミリ秒）を指定します。
Multiplier	BFD 検出時間乗算値（3-99）を指定します。
Slow Time	BFD スロータイム値（1000-3000 ミリ秒）を指定します。

「Apply」をクリックし、設定内容を適用します。

BFD Neighbor Table（BFD ネイバテーブル）

Bidirectional Forwarding Detection (BFD) ネイバテーブルの表示を行います。

注意 実際の動作速度は設定内容やトラフィックの状況で変わります。実環境に BFD を設定する前にテストを実施することをお勧めします。

L3 Features > BFD > BFD Neighbor Table の順にメニューをクリックして以下の画面を表示します。

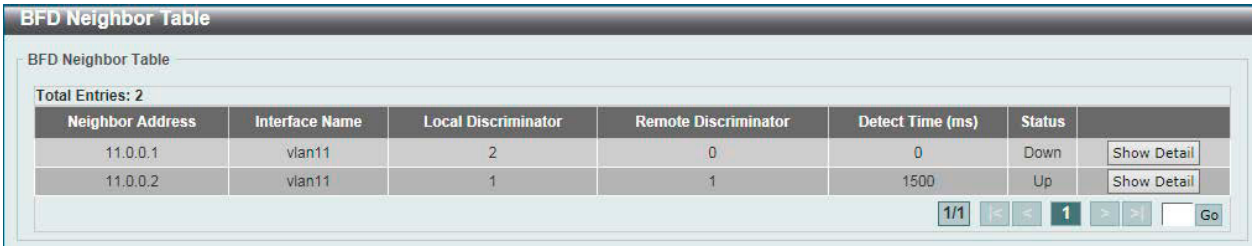


図 9-206 BFD Neighbor Table 画面

「Show Detail」をクリックして、指定エントリの詳細について表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Show Detail」をクリックすると、以下の画面が表示されます。

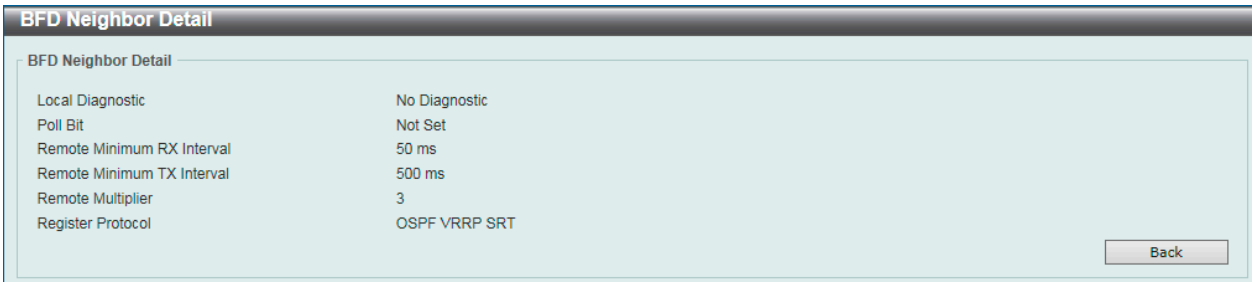


図 9-207 BFD Neighbor Table (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

ISIS（Intermediate System to Intermediate System）（MI モードのみ）

L3 Features > ISIS

Intermediate System to Intermediate System (ISIS) の設定を行います。

ISIS Global Settings（ISIS グローバル設定）

Intermediate System to Intermediate System (ISIS) の設定、表示を行います。

L3 Features > ISIS > ISIS Global Settings の順にメニューをクリックして以下の画面を表示します。

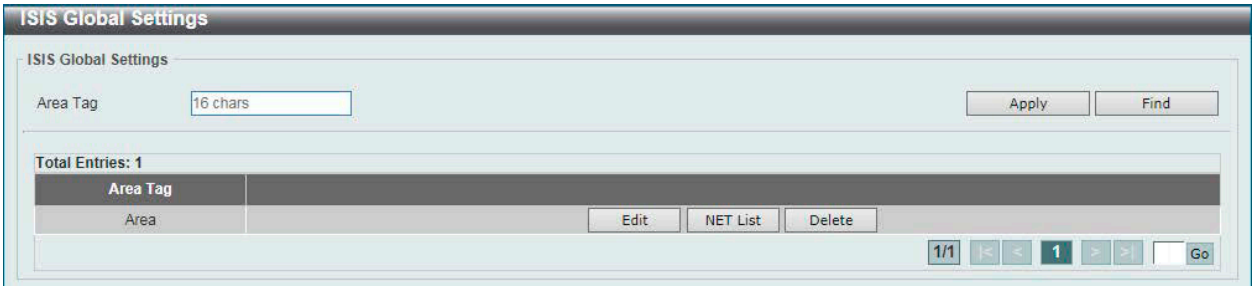


図 9-208 ISIS Global Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Area Tag	ISIS エリアタグ（16 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「NET List」をクリックして、すべてのエントリを表示します。
「Edit」をクリックして、指定エントリの編集を行います。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

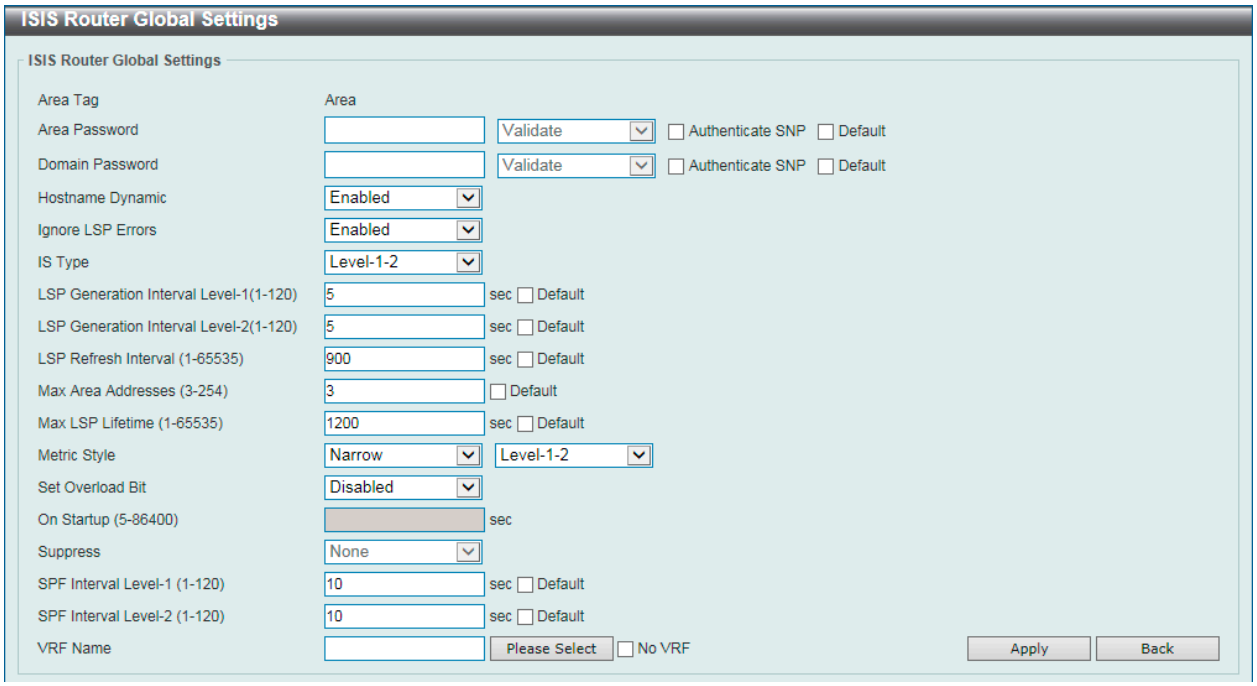


図 9-209 ISIS Global Settings (Edit) 画面

以下の項目を使用して設定を行います。

項目	説明
Area Password	ISIS エリア認証パスワードを指定します。エリアの全スイッチに、非認証のスイッチによるリンクステートデータベースへの不正ルーティング情報の挿入を防止します。パスワードはプレーンテキストに変換され、現時点で唯一の認証方法になります。「Authenticate SNP」を指定するとパスワードを「sequence number PDU」(SNP) に挿入します。 • Validate - SNP へのパスワード挿入と SNP によるパスワード受信を指定します。 • Send Only - SNP へのパスワード挿入のみを指定します。 「Default」を選択すると初期値を指定します。
Domain Password	ISIS ドメイン認証パスワードを指定します。「Authenticate SNP」を指定するとパスワードを「sequence number PDU」(SNP) に挿入します。 • Validate - SNP へのパスワード挿入と SNP によるパスワード受信を指定します。 • Send Only - SNP へのパスワード挿入のみを指定します。 「Default」を選択すると初期値を指定します。
Hostname Dynamic	ダイナミックホスト名を有効 / 無効に指定します。ISIS ダイナミックホスト名マッピングを有効に指定します。 ダイナミックホスト名メカニズムはネットワーク間の「router-name-to-system-ID」マッピング情報を分配する「Link-State Protocol」(LSP) フラッディングを使用します。ネットワークの各ルータはシステム ID ルータ名マッピング情報のルーティングテーブルへのインストールを試みます。ルータが既に通知を急に停止したネットワークのダイナミックネーム Type, Length, Value (TLV) を通知している場合、最後に受信したマッピング情報は最大一時間、ダイナミックホストテーブルに残り、ネットワーク管理者にネットワークに問題が発生している間、マッピングエントリテーブルのエントリを表示します。
Ignore LSP Errors	「Ignore LSP Errors」（LSP エラー無視）を有効 / 無効に指定します。バッドチェックサムのリンクステートパケットの無視 (LSPs) に使用されます。ISIS プロトコル定義は受信者から除かれる不正のデータリンクチェックサムの受信 LSP を必要とし、パケットの再起動を実行を引き起こします。しかしネットワークがデータ衝突を起こすリンクの保持や、同時に正しいデータリンクチェックサムの LSP の通達などを実行する場合、大量パケットの排除や再起動などが繰り返し発生する場合があります。このような状況はネットワークの不動作のレンダリングを発生させるため、パケットの除外よりも LSP を無視するコマンドを使用します。
IS Type	「IS type」を指定します。ISIS ルーティングプロセスのインスタンスのルーティングレベルの設定に使用されます。 • Level1 - レベル 1 ルーティングのみ実行します。スイッチはエリア内の宛先のみ学習します。レベル 2 ルーティングはレベル 1-2 の両ルータで実行されます。 • Level-1-2 - レベル 1-2 ルーティングを実行します。 • Level-2 - レベル 2 ルーティングのみを実行します。
LSP Generation Interval Level-1	LSP 生成間隔レベル 1（1-120 秒）を指定します。レベル 1 エリアのみのリンクステートパケット生成間隔の設定に使用します。ネットワークの不安定期間に、LSP 生成レートの減少に使用します。ルータの CPU 起動と ISIS ネイバへの LSP 送信の減少に使用されます。「Default」を選択すると初期値を指定します。
LSP Generation Interval Level-2	LSP 生成間隔レベル 2（1-120 秒）を指定します。レベル 2 エリアのみのリンクステートパケット生成間隔の設定に使用します。ネットワークの不安定期間に、LSP 生成レートの減少に使用します。ルータの CPU 起動と ISIS ネイバへの LSP 送信の減少に使用されます。「Default」を選択すると初期値を指定します。

項目	説明
LSP Refresh Interval	LSP 更新間隔値（1-65535）を指定します。リンクステートパケット再生成の設定を行います。 ライフタイムが切れる前に LSP は一定期間で更新される必要があります。本項目で設定された値は「Max LSP Lifetime」で設定されたパラメータの値よりも少ない必要があります。そうでない場合、LSP は更新前にタイムアウトします。LSP ライフタイムの設定ミスは LSP 更新間隔よりも小さい設定値を設定することで、LSP のタイムアウトを防ぐ LSP 更新間隔の減少をもたらします。更新間隔を短くすると、リンク使用率は上昇しますがリンクステートデータベース破損が検出されない時間を減らすことができます。更新間隔を長くすると、更新パケットのフラッディングによるリンク使用率を減らすことができます。「Default」を選択すると初期値を指定します。
Max Area Addresses	最大エリアアドレス値（3-254）を指定します。追加マニュアルアドレスの設定により、ISIS エリアサイズの最大化を行います。「Default」を選択すると初期値を指定します。
Max LSP Lifetime	最大 LSP ライフタイム値（1-65535）を指定します。リンクステートパケットの最大ライフタイム値を指定します。「Default」を選択すると初期値を指定します。

Metric Style	メトリックスタイルを指定します。ISIS プロセス生成とメトリックスタイル受領を設定します。
	• Narrow - 旧スタイルメトリック TLV を生成します。
	• Wide - 新スタイルメトリック TLV を生成します。
	• Narrow Transition - 旧スタイルメトリック TLV を生成し、新旧両スタイルメトリック TLV を受け入れます。
	• Wide Transition - 新スタイルメトリック TLV を生成し、新旧両スタイルメトリック TLV を受け入れます。
	• Transition - 新旧両スタイルメトリック TLV を生成します。各メトリックスタイルは選択したレベルになります。
	  • Level-1 - レベル 1 ルーティングのみ有効に指定します。
	  • Level-1-2 - レベル 1/2 ルーティングを有効に指定します。
	  • Level-2 - レベル 2 ルーティングのみ有効に指定します。

Set Overload Bit	「Set Overload Bit」の有効 / 無効に指定します。「non-pseudo」ノード LSP におけるオーバロードビットの設定 ISIS プロセスを強制します。通常オーバロードビットの設定はルータに問題が発生した場合に許可されます。例えばルータにメモリ不足が発生している場合、LSPDB が完了していないことでルーティングテーブルの未完了 / 不適当な結果が発生します。LSP のオーバロードビットの設定で、他のルータが、問題から回復するまでに SPF 計算における不確かなルータを無視することができます。
On Startup	オーバロードビット設定の開始時間（5-86400 秒）を指定します。システムスタート時のオーバロードビットの設定を行います。オーバロードビットは指定の時間残ります。
Suppress	抑制オプションを指定します。サブシークエントキーワード / キーワードによって識別される、抑制されるプリフィクスタイプを指定します。 • None - 他の ISIS レベルから、そして通知された他のプロトコルから学習した、如何なる IP プリフィクスを防止しません。 • Interlevel - 通知された他の ISIS レベルから学習した IP プリフィクスを防止します。 • External - 通知された他のプロトコルから学習した IP プリフィクスを防止します。 • Both - 他の ISIS レベルから、そして通知された他のプロトコルから学習した、全ての IP プリフィクスを防止します。
SPF Interval Level-1	SPF 間隔レベル 1 値（1-120 秒）を指定します。レベル 1 エリアでのみの SPF 計算の ISIS スロットルをカスタムします。「Default」を選択すると初期値を指定します。
SPF Interval Level-2	SPF 間隔レベル 2 値（1-120 秒）を指定します。レベル 2 エリアでのみの SPF 計算の ISIS スロットルをカスタムします。「Default」を選択すると初期値を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。 「Please Select」で事前に設定済みの VRF を選択することが可能です。「No VRF」で VRF インスタンスを指定しません。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-210 Please Select（VRF）画面

使用する VRF 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。

「NET List」をクリックすると、次の画面が表示されます。



図 9-211　ISIS Global Settings (NET List) 画面

以下の項目を使用して設定を行います。

項目	説明
NET	NET Network Services Access Point (NSAP) アドレスを指定します。 「Intermediate System」(IS) は NSAP として知られるアドレスによって識別されます。NSAP は「ISO10589」によって指定された 3 つのパートに分割されます。「NET」は最後のバイトが常に「n-selector」そして「zero」となる NSAP です。「NET」は 8 から 20 バイト長です。「Multiple NET」はエリアの分割、統合が可能です。IP ルーティングでのみ実行され、「NET」は必ずシステム ID とエリア ID を定義されている必要があります。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

ISIS Router Settings（ISIS ルータ設定）

Intermediate System to Intermediate System (ISIS) ルータの設定、表示を行います。

L3 Features > ISIS > ISIS Router Settings の順にメニューをクリックして以下の画面を表示します。

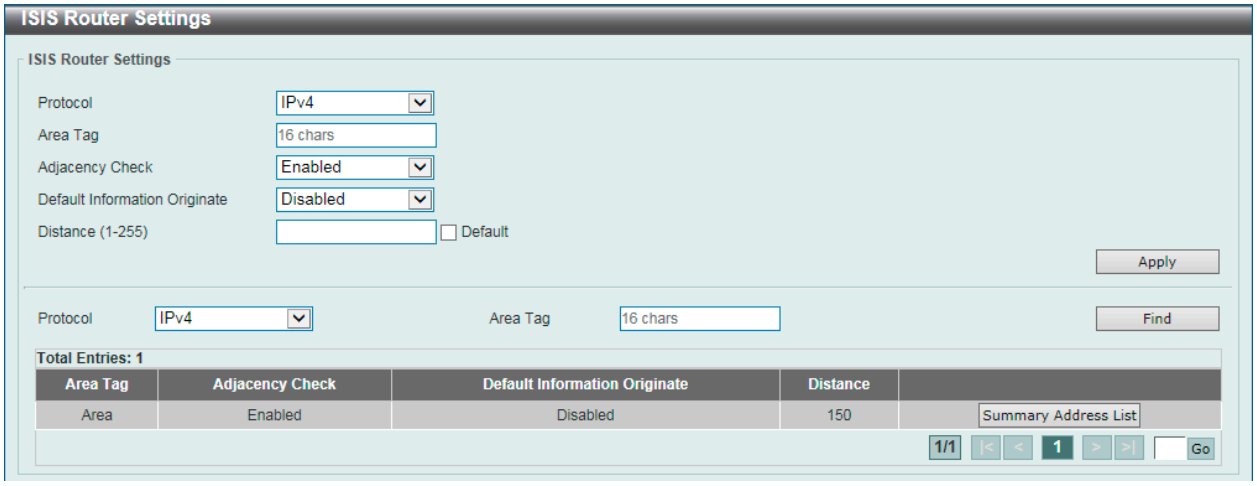


図 9-212　ISIS Router Settings（IPv4）画面

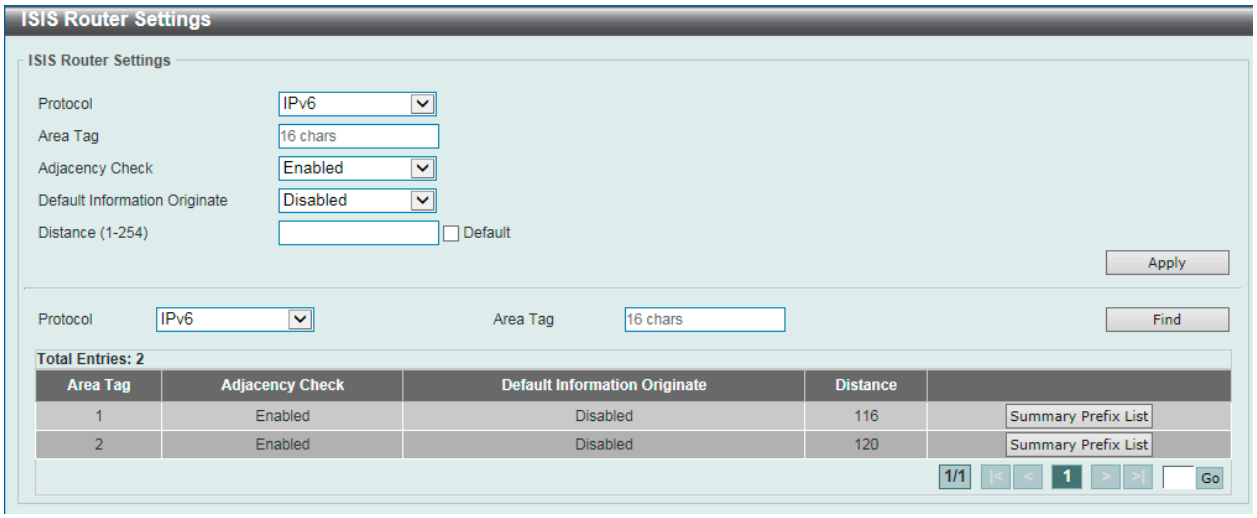


図 9-213　ISIS Router Settings（IPv6）画面

以下の項目を使用して設定を行います。

項目	説明
Protocol	プロトコル（IPv4/IPv6）を指定します。
Area Tag	ISIS エリアタグ（16 字以内）を指定します。有効な Ip インタフェースにおいてルーティングプロセスタグを指定します。
Adjacency Check	「Adjacency Check」を有効 / 無効に指定します。ISIS はハローパケットでの整合性チェックの実行と同じプロトコルをサポートするネイバリングルータとの隣接を形成します。本項目はその有効 / 無効を確認します。
Default Information Originate	「Default Information Originate」を有効 / 無効に指定します。有効にすると、ISIS が Level-2 Link-State Packets (LSP) のデフォルトルートの通知を実行します。
Distance	「Distance」を指定します。ISIS ルートの管理ディスタンス（1-255/IPv4、1-254/IPv6）です。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Summary Address List」をクリックして、サマリアドレスリストを指定します。
「Summary Prefix List」をクリックして、サマリプリフィクスリストを指定します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Summary Address List」をクリックすると、次の画面が表示されます。

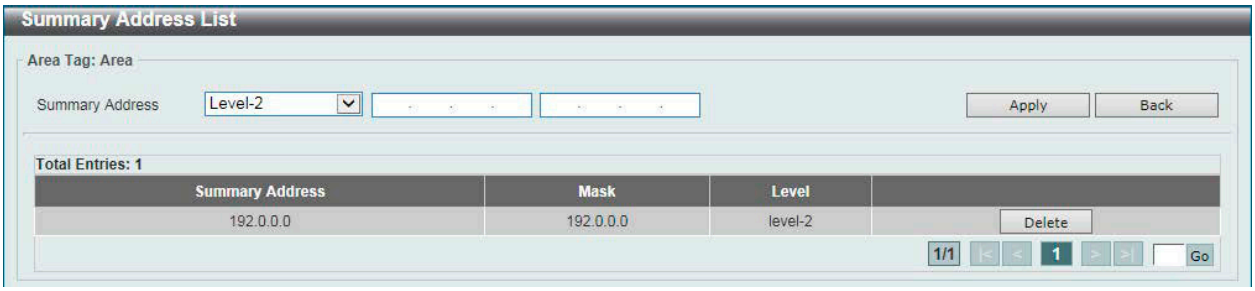


図 9-214 ISIS Router Settings (Summary Address List) 画面

項目	説明
Summary Address	サマリアドレスとレベルを指定します。ISIS のアドレスアグリゲートを行います。 複数のサマリ化可能アドレスグループにはレベルを付与することができます。ルートは同様にレベルを付与される他のルーティングプロトコルから学習します。サマリを通知するメトリックは指定の全ルートのメトリックで最小です。本コマンドではルーティングテーブルのサイズを減少させることができます。本コマンドはまた、リンクステートパケットとリンクステートデータベースのサイズを減少させることも可能です。サマリ通知は多くのルートに依存しているためネットワークの安定性にも有効です。単一のルートフラップはほとんどの場合、フラップのサマリ通知になりません。サマリアドレスの欠点は、他のルートの場合の方が、より少ない情報で各宛先へ最適なルーティングテーブルを計算できます。 • Level-1 - レベル 1 で再配分される唯一のルートを指定の IP アドレスとマスク値でサマリ化します。 • Level-1-2 - エリア内のレベル 1 ルートがレベル 2ISIS に到達可能なステータスを通知され、レベル 1 と 2 ISIS で再配分されるルートをサマリ化します。 • Level-2 - レベル 1 ルーティングによって学習するルートがレベル 2 が IP アドレスとマスク値を設定されたバックボーンとともにサマリ化されます。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Summary Prefix List」をクリックすると、次の画面が表示されます。



図 9-215 ISIS Router Settings (Summary Prefix List) 画面

項目	説明
Summary Prefix	レベルを選択しサマリプリフィクスを入力します。 • Level-1 - レベル 1 で再配分される唯一のルートを指定の IP アドレスとマスク値でサマリ化します。 • Level-1-2 - エリア内のレベル 1 ルートがレベル 2ISIS に到達可能なステータスを通知され、レベル 1 と 2 ISIS で再配分されるルートをサマリ化します。 • Level-2 - レベル 1 ルーティングによって学習するルートがレベル 2 が IP アドレスとマスク値を設定されたバックボーンとともにサマリ化されます。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

Intermediate System to Intermediate System (ISIS) インタフェースの設定、表示を行います。

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

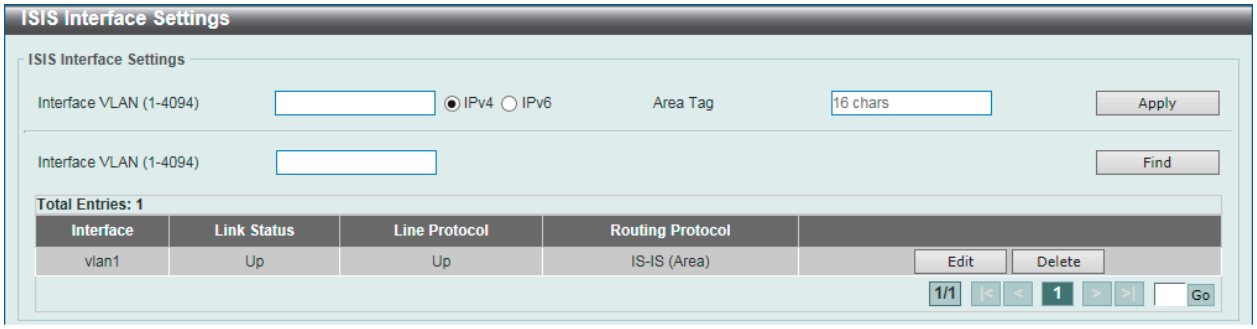


図 9-216 ISIS Interface Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Interface VLAN	本設定に使用するインタフェース VLAN（1-4094）を指定します。
IPv4	インタフェースにおいて IPv4 の ISIS ルーティングプロトコル有効に指定します。
IPv6	インタフェースにおいて IPv6 の ISIS ルーティングプロトコル有効に指定します。
Area Tag	ISIS エリアタグ（16 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」をクリックして、指定エントリの編集を行います。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

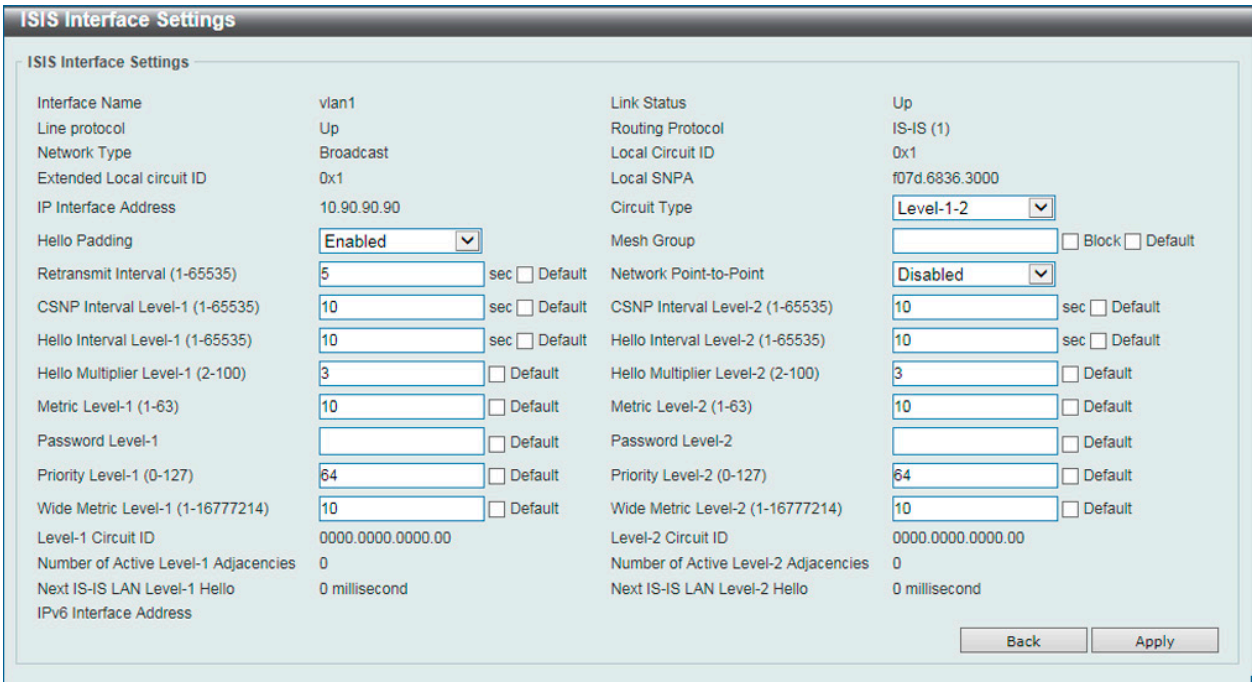


図 9-217 ISIS Interface Settings (Edit) 画面

以下の項目を使用して設定を行います。

項目	説明
Circuit Type	サーキットタイプを指定します。 • Level-1 - レベル 1 隣接のみ指定します。 • Level-1-2 - レベル 1/2 隣接を指定します。 • Level-2 - レベル 2 隣接を指定します。
Hello Padding	「Hello Padding」を有効 / 無効に指定します。ISIS ハローパケットは「maximum transmission unit」(MTU) サイズまで大きくされます。フル MTU までの ISIS ハローパケットの巨大化は大きいフレームの送信問題などを発生させるエラーの早期検出や、隣接インタフェースでの MTU のミスマッチなどを発生させるエラーも検出などに有効です。両インタフェースの MTU が同じである場合において、ネットワーク帯域の消費を避けるために本機能を無効化します。
Mesh Group	メッシュグループの番号を指定します。 point-to-point ネットワーク間の「Link-State Packet」(LSP) フラッディングの最適化に使用します。 「Block」でインタフェースでの LSP フラッディングの発生はありません。「Default」を選択すると初期値を指定します。
Retransmit Interval	「Retransmit Interval」（再送信間隔）の値（1-65533 秒）を指定します。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。
Network Point-to-Point	「Network Point-to-Point」を有効 / 無効に指定します。統合 ISIS ルーティングプロトコルを使用してブロードキャストリンクの代わりに「ポイントトゥポイント」のようにブロードキャストメディアを使用する 2 つのネットワーク機器を機能させます。
CSNP Interval Level-1	「level-1 CSNP」の送信間隔（1-65535 秒）の指定をします。宛先ルータにのみ有効です。「Default」を選択すると初期値を指定します。
CSNP Interval Level-2	「level-2 CSNP」の送信間隔（1-65535 秒）の指定をします。宛先ルータにのみ有効です。「Default」を選択すると初期値を指定します。
Hello Interval Level-1	「level-1 ハローパケット」の送信間隔（1-65535 秒）の指定をします。宛先ルータにのみ有効です。「Default」を選択すると初期値を指定します。
Hello Interval Level-2	「level-2 ハローパケット」の送信間隔（1-65535 秒）の指定をします。宛先ルータにのみ有効です。「Default」を選択すると初期値を指定します。
Hello Multiplier Level-1	「Hello Multiplier」の値（2-100）を入力します。ハローマルチプライヤ時間は ISIS ハローパケットのハローインターバルホールドタイムと同じです。小さいハローマルチプライヤは早い収束を取得します。ルーティングとしては不安定です。ネットワークの安定性が必要な場合は、ハローマルチプライヤ時間は長い方が理想です。「Default」を選択すると初期値を指定します。
Hello Multiplier Level-2	「Hello Multiplier」の値（2-100）を入力します。「Default」を選択すると初期値を指定します。
Metric Level-1	ISIS メトリック値を指定します。他の宛先へのリンクネットワークや他の宛先のネットワーク内の各リンクのコスト計算に使用されます。メトリックは SPF レベル 1 ルーティングの唯一の SPF 計算です。 「Default」を選択すると初期値を指定します。
Metric Level-2	ISIS メトリック値を指定します。他の宛先へのリンクネットワークや他の宛先のネットワーク内の各リンクのコスト計算に使用されます。メトリックは SPF レベル 2 ルーティングの唯一の SPF 計算です。 「Default」を選択すると初期値を指定します。

項目	説明
Password Level-1	レベル 1 ルーティング使用時の ISIS パスワード（16 字以内）を指定します。本ルータと形成する隣接からの非認証ルータの防止を有効にし、ネットワークを侵入者から守ります。パスワードはプレーンテキストとして交換されるため、セキュリティに制限があります。「Default」を選択すると初期値を指定します。
Password Level-2	レベル 2 ルーティング使用時の ISIS パスワード（16 字以内）を指定します。本ルータと形成する隣接からの非認証ルータの防止を有効にし、ネットワークを侵入者から守ります。パスワードはプレーンテキストとして交換されるため、セキュリティに制限があります。「Default」を選択すると初期値を指定します。
Priority Level-1	レベル 1 ルーティング使用時の優先値（0-127）を指定します。優先値は LAN のどのルータが DIS になるかを決めます。優先値はハローパケットで通知されます。最高の優先値を持つデバイスが DIS になります。ISIS では宛先ルータのバックアップはありません。0 に近い値の優先値設定はシステムが DIS になるチャンスは低いですが、完全に防げるわけではありません。システムが高い優先値を持っていると現在の DIS からその座を引き継ぎます。優先値が同値の場合、MAC アドレスの値の大きさで、決まります。「Default」を選択すると初期値を指定します。
Priority Level-2	レベル 2 ルーティング使用時の優先値（0-127）を指定します。優先値は LAN のどのルータが DIS になるかを決めます。優先値はハローパケットで通知されます。最高の優先値を持つデバイスが DIS になります。ISIS では宛先ルータのバックアップはありません。0 に近い値の優先値設定はシステムが DIS になるチャンスは低いですが、完全に防げるわけではありません。システムが高い優先値を持っていると現在の DIS からその座を引き継ぎます。優先値が同値の場合、MAC アドレスの値の大きさで、決まります。「Default」を選択すると初期値を指定します。
Wide Metric Level-1	リンクにアサインする広いメトリック値（1-16777214）を指定し、レベル 1 ルーティングの他の宛先へのネットワーク内のリンク経由の他のルータからのコストを計算します。 「Default」を選択すると初期値を指定します。
Wide Metric Level-2	リンクにアサインする広いメトリック値（1-16777214）を指定し、レベル 2 ルーティングの他の宛先へのネットワーク内のリンク経由の他のルータからのコストを計算します。 「Default」を選択すると初期値を指定します。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

ISIS Redistribute Settings（ISIS 再配分設定）

Intermediate System to Intermediate System (ISIS) 再分配の設定、表示を行います。

L3 Features > ISIS > ISIS Redistribute Settings の順にメニューをクリックして以下の画面を表示します。

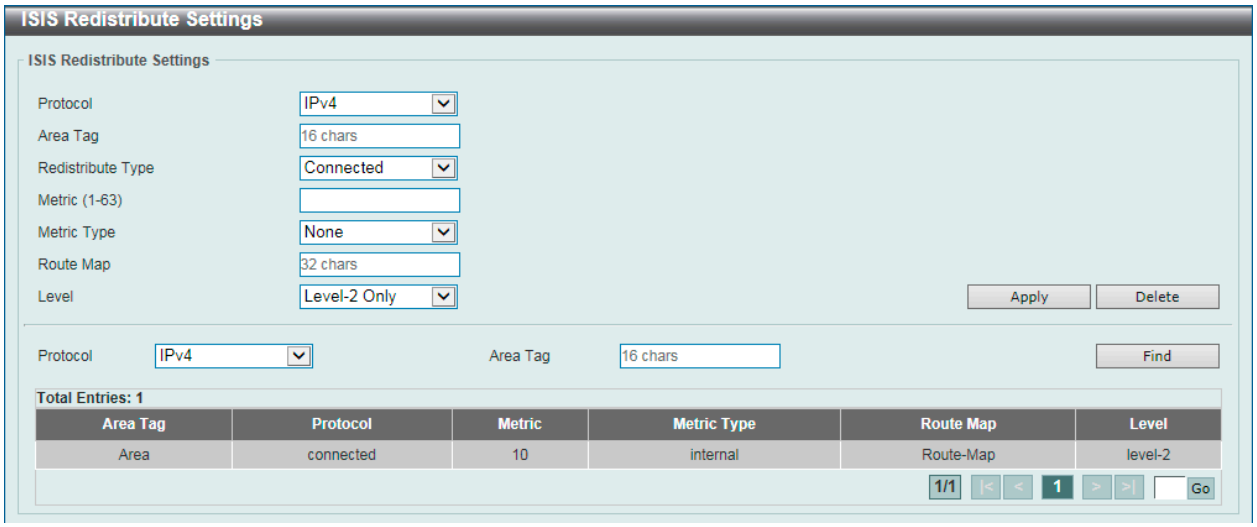


図 9-218 ISIS Redistribute Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Protocol	プロトコル（IPv4/IPv6）を指定します。
Area Tag	ISIS エリアタグ（16 字以内）を指定します。
Redistribute Type	プルダウンメニューを使用して再分配のタイプを選択します。 • Connected - ISIS への接続ルートに再分配します。 • Static - ISIS へのスタティックルートに再分配します。 • RIP - ISIS への RIP ルートに再分配します。 • OSPF - ISIS への OSPF ルートに再分配します。 • ISIS - ISIS への ISIS ルートに再分配します。
Metric	再分配ルートのメトリック（1-63）を指定します。
Metric Type	メトリックの種類を指定します。「None」「Internal」「External」から指定します。
Route Map	ルートマップを（32 字以内）指定します。

項目	説明
Level	ルーティングレベルを指定します。「Level-1」「Level-1-2」「Level-2 Only」から指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

ISIS Redistribute ISIS Settings（ISIS 再配分 ISIS 設定）

Intermediate System to Intermediate System (ISIS) 再分配 ISIS 設定、表示を行います。レベル 1 から 2（レベル 2 から 1）の ISIS ルート再配分に使用します。

L3 Features > ISIS > ISIS Redistribute ISIS Settings の順にメニューをクリックして以下の画面を表示します。

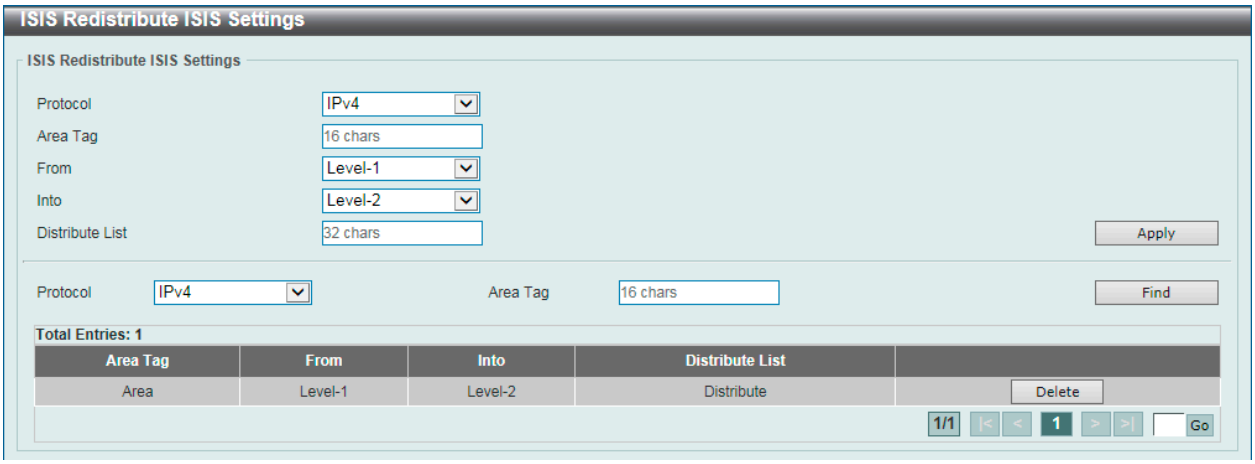


図 9-219 ISIS Redistribute ISIS Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Protocol	プロトコル（IPv4/IPv6）を指定します。
Area Tag	ISIS エリアタグ（16 字以内）を指定します。
From	再配分を行う元のレベルを指定します。「Level-1」「Level-2」から指定します。
Into	再配分を行う先のレベルを指定します。「Level-1」「Level-2」から指定します。
Distribute List	分配リスト（32 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

ISIS Route Table（ISIS ルートテーブル）

Intermediate System to Intermediate System (ISIS) ルートテーブル ISIS を表示します。

L3 Features > ISIS > ISIS Route Table の順にメニューをクリックして以下の画面を表示します。

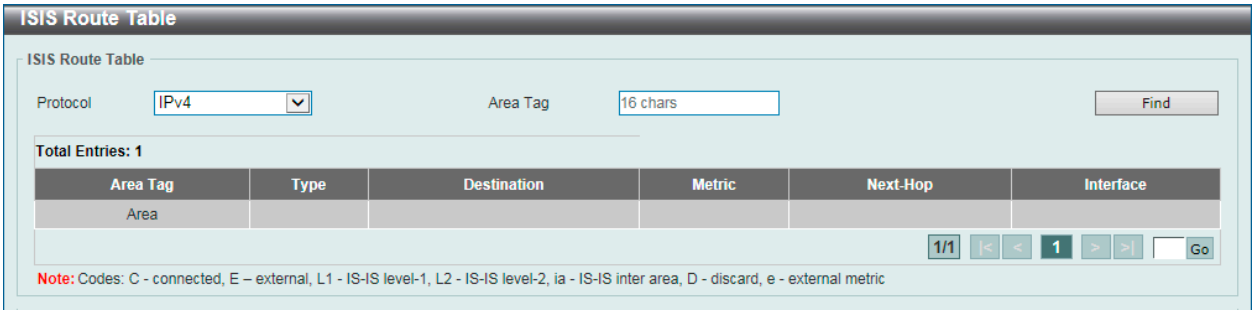


図 9-220 ISIS Route Table 画面

以下の項目を使用して設定を行います。

項目	説明
Protocol	プロトコル（IPv4/IPv6）を指定します。
Area Tag	ISIS エリアタグ（16 字以内）を指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

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。

ISIS Database（ISIS データベース）

Intermediate System to Intermediate System (ISIS) データベースを表示します。

L3 Features > ISIS > ISIS Database の順にメニューをクリックして以下の画面を表示します。

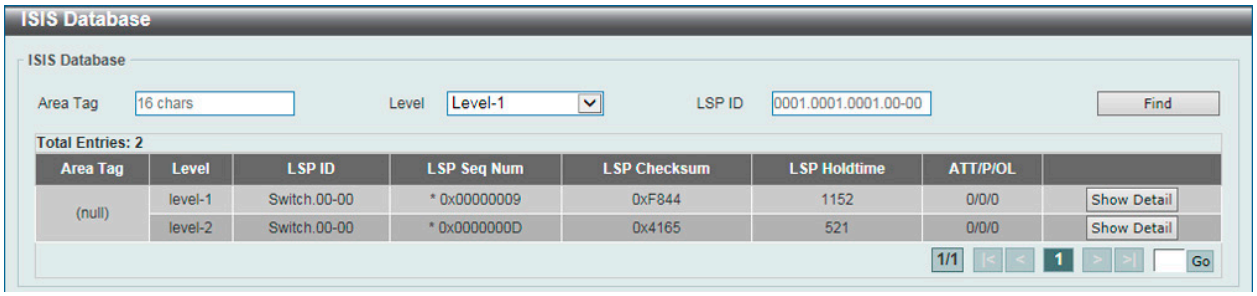


図 9-221　ISIS Database 画面

以下の項目を使用して設定を行います。

項目	説明
Area Tag	ISIS エリアタグ（16 字以内）を指定します。
Level	ルーティングレベルを指定します。「Level-1」「Level-2」から指定します。
LSP ID	表示する LSP ID を指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

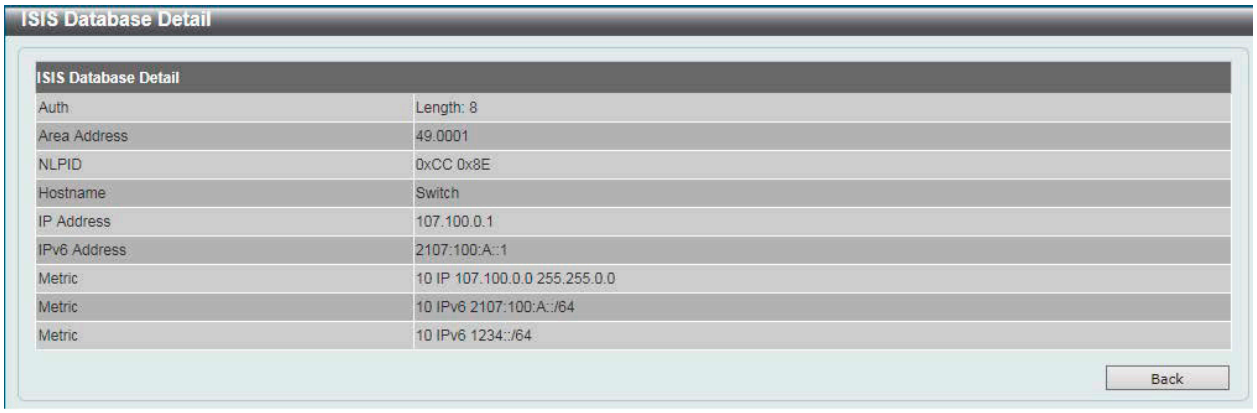


図 9-222　ISIS Database (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

ISIS Topology（ISIS トポロジ）

Intermediate System への ISIS パスを表示します。

L3 Features > ISIS > ISIS Topology の順にメニューをクリックして以下の画面を表示します。

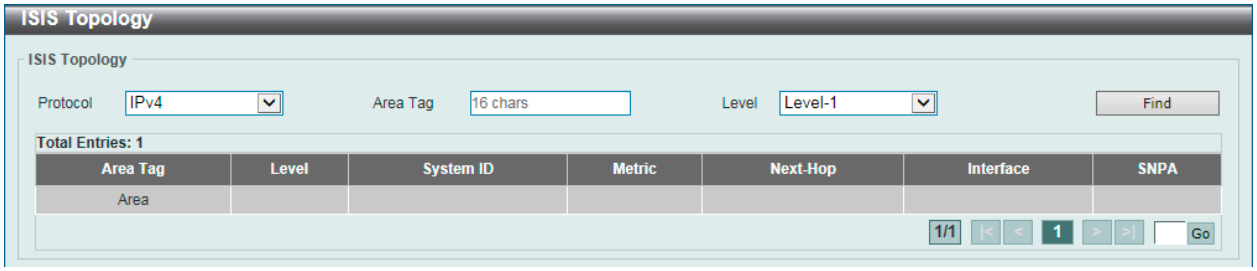


図 9-223　ISIS Topology 画面

以下の項目を使用して設定を行います。

項目	説明
Protocol	プロトコル（IPv4/IPv6）を指定します。
Area Tag	ISIS エリアタグ（16 字以内）を指定します。
Level	ルーティングレベルを指定します。「Level-1」「Level-2」から指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
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。

ISIS Hostname（ISIS ホスト名）

ISIS の「ルータ名 - システム ID」マッピングテーブルエントリを表示します。

L3 Features > ISIS > ISIS Hostname の順にメニューをクリックして以下の画面を表示します。

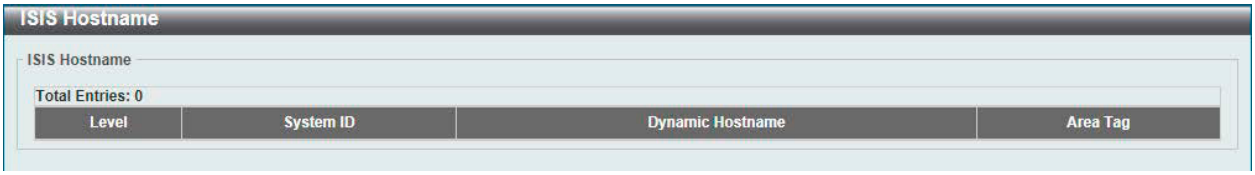


図 9-224 ISIS Hostname 画面

ISIS Neighbors（ISIS ネイバ）

Intermediate System to Intermediate System (ISIS) ネイバ情報を表示します。

L3 Features > ISIS > ISIS Neighbors の順にメニューをクリックして以下の画面を表示します。

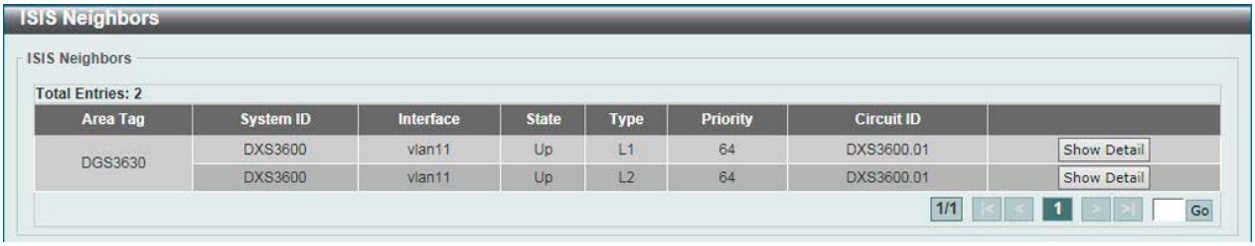


図 9-225 ISIS Neighbors 画面

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。
「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

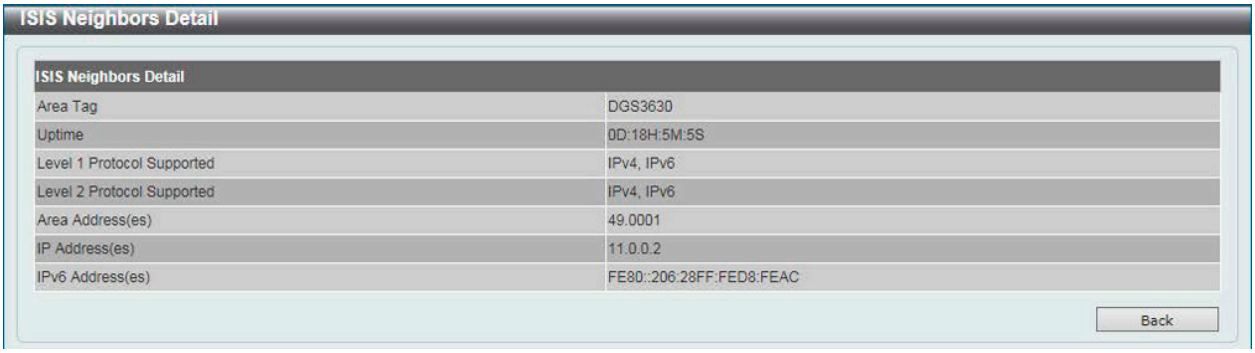


図 9-226 ISIS Neighbors (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

IP Route Filter（IP ルートフィルタ）

IP プレフィックスリスト、ルートマップの作成を行います。

IP Prefix List（IP プレフィックスリスト設定）（EI/MI モードのみ）

IP プレフィックスリストを作成します。

L3 Features > IP Route Filter > IP Prefix List の順にメニューをクリックして以下の画面を表示します。

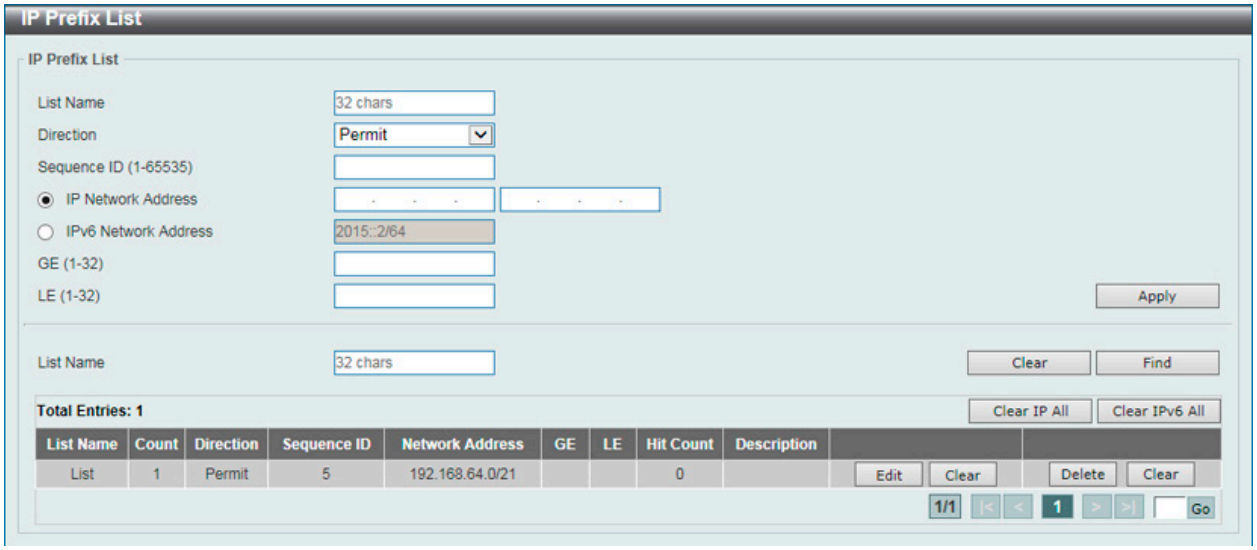


図 9-227　IP Prefix List 画面

以下の項目を使用して設定を行います。

項目	説明
List Name	プレフィックスリスト（32 字以内）を識別する名称を入力します。
Direction	プルダウンメニューを使用して、指定ネットワークを「Permit」(許可) または「Deny」(拒否) します。
Sequence ID (1-65535)	ルールエントリのシーケンス番号を指定します。
IP Network Address	IPv4 ネットワークアドレスを入力します。
IPv6 Network Address	IPv6 ネットワークアドレスを入力します。
GE (1-32/IPv4_1-128/IPv6)	一致する最小プレフィックス長を入力します。
LE (1-32/IPv4_1-128/IPv6)	一致する最大プレフィックス長を入力します。

「Apply」をクリックし、設定内容を適用します。
「Clear」をクリックすると入力したエントリをクリアします。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。
「Clear IP All」をクリックすると入力した IP エントリを全てクリアします。
「Clear IPv6 All」をクリックすると入力した IPv6 エントリを全てクリアします。
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。

Route Map（ルートマップ設定）

ルートマップの作成、またはルートマップへのシーケンスの追加、およびシーケンスの削除を行います。

L3 Features > IP Route Filter > Route Map の順にメニューをクリックして以下の画面を表示します。



図 9-228 Route Map 画面

以下の項目を使用して設定を行います。

項目	説明
Route Map Name	ルートマップ名を入力します。
Direction	プルダウンメニューを使用して、一致するルールを「Permit」(許可) または「Deny」(拒否) します。
Sequence ID (1-65535)	ルールエントリのシーケンス番号を指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Match Clause」の編集

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

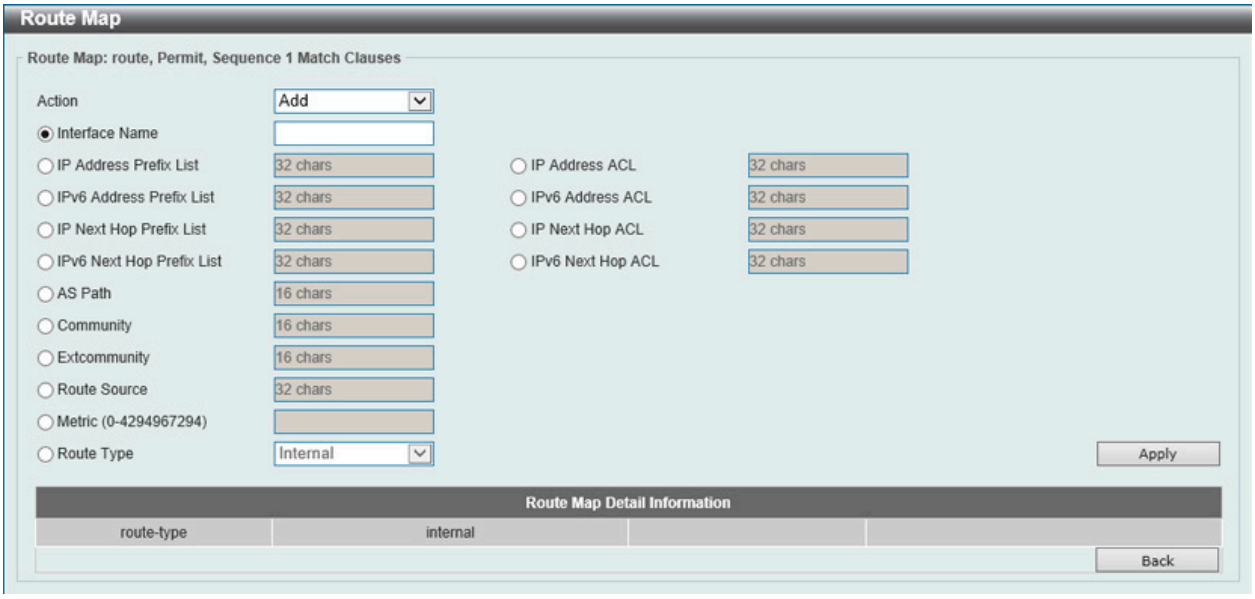


図 9-229 Route Map Settings - Match Clauses 画面

以下の項目を使用して設定を行います。

項目	説明
Action	プルダウンメニューを使用して、シーケンスエントリを「Add」（追加）または「Delete」（削除）します。
Interface Name	インタフェース名を指定します。外部インタフェースにマッチするルートの条件を定義します。
IP Address Prefix List	IP プレフィックスリスト（32 字以内）を指定します。本リストにマッチするルートの条件を定義します。
IP Address ACL	IP ACL リスト（32 字以内）を指定します。本リストにマッチするルートの条件を定義します。
IPv6 Address Prefix List	IPv6 プレフィックスリスト（32 字以内）を指定します。本リストにマッチするルートの条件を定義します。
IPv6 Address ACL	IPv6 ACL リスト（32 字以内）を指定します。本リストにマッチするルートの条件を定義します。
IP Next Hop Prefix List	IP ネクストホッププレフィクスリスト（32 字以内）を指定します。本リストにマッチするルートの条件を定義します。

項目	説明
IP Next Hop ACL	IP ネクストホップ ACL リスト（32 字以内）を指定します。本リストにマッチするルートの条件を定義します。
IPv6 Next Hop Prefix List	IPv6 ネクストホッププレフィクスリスト（32 字以内）を指定します。本リストにマッチするルートの条件を定義します。
IPv6 Next Hop ACL	IPv6 ネクストホップ ACL リスト（32 字以内）を指定します。本リストにマッチするルートの条件を定義します。
AS Path	IP/IPv6 アクセスリスト名（16 字以内）を指定します。本リストにマッチするルートの条件を定義します。
Community	スタンダード / エクステンデッド IPv4/IPv6 アクセスリスト名（16 字以内）を指定します。本リストにマッチするルートのコミュニティ条件を定義します。
Extcommunity	スタンダード / エクステンデッド IPv4/IPv6 アクセスリスト名（16 字以内）を指定します。本リストにマッチするルートのエクステンデッドコミュニティ条件を定義します。
Route Source	スタンダード / エクステンデッド IPv4/IPv6 アクセスリスト名（32 字以内）を指定します。本リストにマッチするルートソースの条件を定義します。
Metric	ルートのメトリック値（0-4294967294）を指定します。
Route Type	ルートタイプを指定します。 • Internal - OSPF AS-internal ルートを指定します。 • External - Ext Type1 と Ext Type2 ルートを含む OSPF AS-external ルートを指定します。 • External Type1 - OSPF AS-external type-1 ルートを指定します。 • External Type2 - OSPF AS-external type-2 ルートを指定します。

2. 「Apply」ボタンをクリックして行った変更を適用します。

「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

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

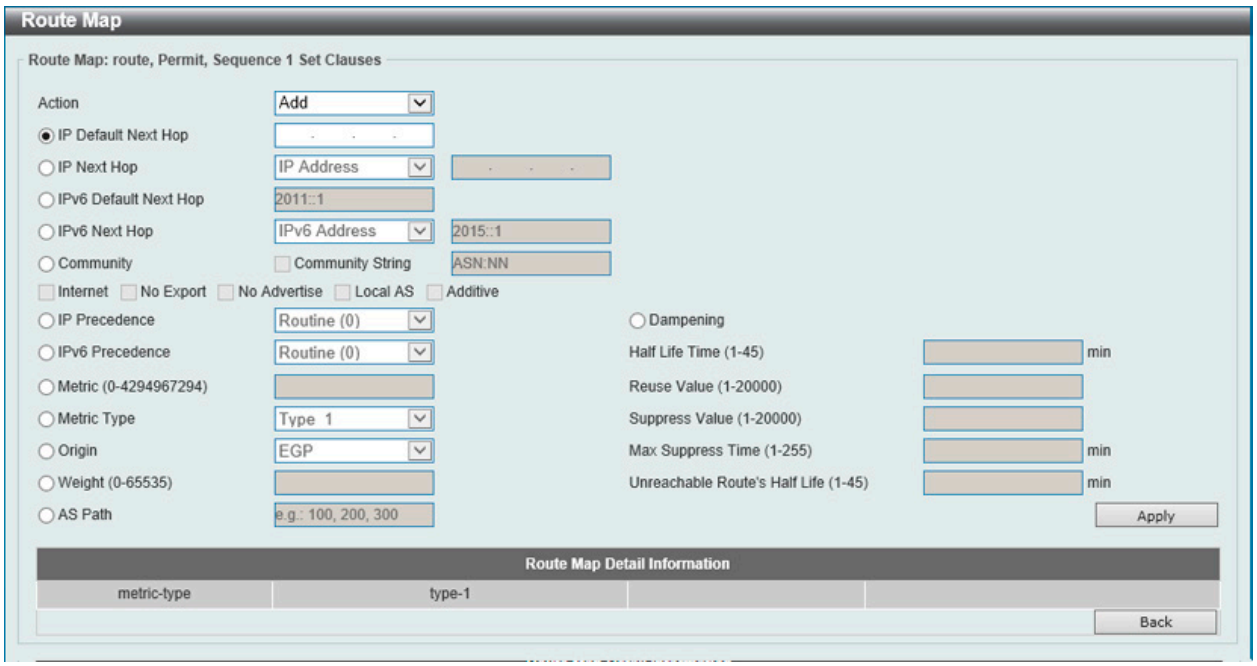


図 9-230 Route Map Settings - Set Clauses 画面

以下の項目を使用して設定を行います。

項目	説明
Action	プルダウンメニューを使用して、シーケンスエントリを「Add」（追加）または「Delete」（削除）します。
IP Default Next Hop	パケットのルート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 16 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。プルダウンメニューを使用して「IP Address」「Peer Address」および「Recursive」を選択します。 • IP Address - 設定する IP アドレス。 • Peer Address - これはイングレスとイーグレス両方に有効です。イングレス方向では、ネクストホップが Neighbor ピアアドレスに設定されます。イーグレス方向では、パケットのルートに関連するネクストホップがローカルルータ ID アドレスになります。 • Recursive - ネクストホップルータとして繰り返し使用する IP アドレスを指定します。

項目	説明
IPv6 Default Next Hop	パケットのルートに使用するデフォルトのネクストホップ IPv6 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 16 つまでのデフォルトネクストホップ IPv6 アドレスが入力できます。
IPv6 Next Hop	IPv6 ネクストホップ属性を設定します。ルートマップシーケンスの条件の照合にパスするパケットをルートするネクストホップルータを指定します。 • IP Address - パケットをルートするネクストホップ 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繰り返し使用する IPv6 アドレスを指定します。
Community	使用するコミュニティ、またはルートのオリジナルのコミュニティに追加されるコミュニティを指定します。 • Community String - コミュニティは 4 バイト長 (AS 番号用に 2 バイト、ネットワーク番号用に 2 バイト) です。この値は「:」(コロン) によって区切られた 2 バイトの番号 2 つによって設定されています。両方の番号の範囲は 1-65535 です。コミュニティ設定は、「,」(カンマ) で区切ることによって複数のコミュニティで形成されます。コミュニティストリングの例は 200:1024, 300:1025, 400:1026 です。 • Internet - このコミュニティを持つルートをすべてのピア (内部または外部) に送信します。 • No Export - このコミュニティを持つルートはコンフェデレーション内の同じ AS か別のサブ AS にあるピアに送信されますが、外部の BGP(eBGP) ピアには送信されません。 • No Advertise - このコミュニティを持つルートはどんなピア (内部または外部) にも通知されません。 • Local AS - このコミュニティを持つルートは同じ AS のピアに送信されますが、同じコンフェデレーション内の別のサブ AS にあるピアと外部のピアには送信されません。 • Additive - このキーワードを指定すると、指定したコミュニティストリングをオリジナルのコミュニティストリングに追加します。指定しないと、指定したコミュニティストリングはオリジナルのコミュニティストリングを置き換えます。
IP Precedence	IP 優先オプションを指定します。「Routine」「Priority」「Immediate」「Flash」「Flash Override」「Critical」「Internet」「Network」から指定します。IP ヘッダの優先値を設定します。ポリシールーティングが IPv4 パケットを含む場合有効になる機能です。
IPv6 Precedence	IPv6 優先オプションを指定します。「Routine」「Priority」「Immediate」「Flash」「Flash Override」「Critical」「Internet」「Network」から指定します。IPv6 ヘッダの優先値を設定します。ポリシールーティングが IPv6 パケットを含む場合有効になる機能です。
Metric (0-4294967294)	メトリックを入力します。メトリックがルートマップで設定されたイーグレスでない限り、BGP ルータは初期値ではルートに関連するメトリックを送信しません。BGP ルートがメトリックを持つルートを受信すると、このメトリックはベストパス選択に使用されます。これは、ルートのイングレス設定であるメトリックによって上書きされます。受信ルートがメトリックが設定したメトリック属性またはメトリックイングレスのいずれかを持っていると、デフォルトメトリック「0」がベストパス選択のためにルートに関連付けられます。med-missing-as-worst がルータに有効になると、「infinite」(無限) の値がルートに関連付けられます。これはイングレスとイーグレス両方に有効です。
Metric Type	編集に使用す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。
Origin	ルートの開始先を入力します。それは以下の 3 つの値 (EGP、IGP、または、incomplete) の 1 つです。 • IGP -「Interior Gateway Protocol」（IGP）をプレフィクスの由来とする設定です。 • EGP -「Exterior Gateway Protocol」（EGP）をプレフィクスの由来とする設定です。 • Incomplete - 不明なソースをプレフィクスの由来とする設定です。
Weight (0-65535)	一致するルートの重み付けを入力します。これは、Neighbor から受信したルートのために neighbor weight コマンドで指定した重み付けを上書きします。重み付けが neighbor weight コマンドで指定されるか、またはルートマップによって設定されないと、別の BGP ピアを通して学習されたルートは、デフォルトの重み付け 0 を持ちます。ローカルルートの重み付けは通常 32768 です。これはイングレスにだけ有効です。
AS Path	AS リストを最初に付加するのに使用される AS パスリストを指定します。
Dampening	ダンプニングの値を指定します。5 つのアイテムを指定可能です。 • Half Life Time - ペナルティとして到達可能ルートが半分に減らされるハーフライフ時間値（1-45/ 分）を指定します。 • Reuse Value - 再使用値（0-20000）を指定します。本値よりルートのペナルティ値が低い場合、ルートは圧縮されません。 • Suppress Value - 圧縮値（0-20000）を指定します。本値よりルートのペナルティ値が高い場合、ルートは圧縮されます。 • Maximum Suppress Time - 圧縮されるルートの最大圧縮時間値（1-255）を指定します。 • Unreachable Route's Half Life - ペナルティとして不達ルートが半分に減らされるハーフライフ時間値（1-45/ 分）を指定します。

「Apply」ボタンをクリックして行った変更を適用します。
「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 9-231　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。「IP Policy」「IPv6 Policy」から指定します。

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

エントリの編集

1. ポリシールートの編集をするためには、「Edit」ボタンをクリックして以下の画面を表示します。

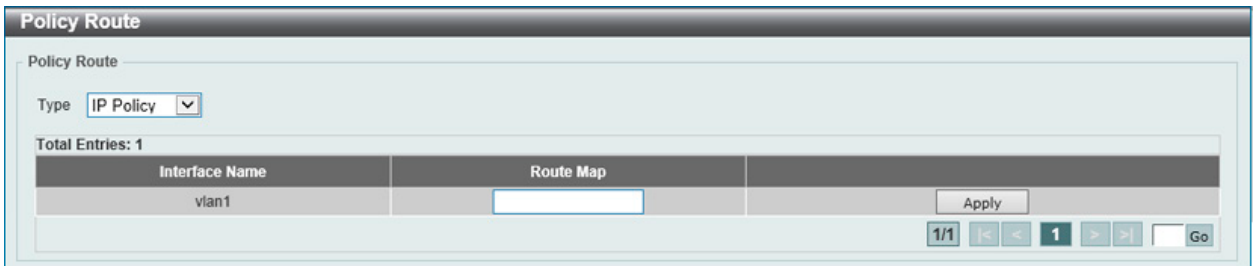


図 9-232　Policy Route Settings 画面 - Edit

以下の項目を設定します。

項目	説明
Route Map	ポリシールートマップ名を入力します。

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

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。VRRP ルータのうち、仮想ルータと対向する IP アドレスの制御を行うものをマスタルータと呼び、このルータが本 IP アドレス向けのパケットを送出します。また、エンドホストは LAN 上の仮想ルータの IP アドレスをデフォルトのファーストホップとして使用できます。VRRP 機能を使用して、管理者はすべてのエンドホストにダイナミックルーティングやルート検出プロトコルの設定を行わなくても、デフォルトパスコストを取得することができます。

LAN 上に静的に設定されたデフォルトルートは、障害発生箇所となる傾向があります。VRRP 機能はこの障害を回避するために、選出プロトコルを使用して LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を割り当てるよう設計されています。仮想ルータがダウンすると、選出プロトコルが優先度の最も高い仮想ルータを選び、LAN 上のマスタルータに任命します。これによりダウンした箇所に関係なく、リンクとコネクションはその状態を保つことができます。

VRRP では、1 台の物理的ルータの代わりに、物理的ルータのグループから構成される仮想ルータを導入します。仮想ルータは 2 台以上の物理ルータから構成され、その中で実際に稼動するのは 1 台のみです。その仮想ルータの中で実際に稼動しているルータが停止した場合、自動的に別のルータに切り替わり稼動を開始します。実際に稼動している物理ルータをマスタルータと呼び、マスタルータ異常時に備えて待機している物理ルータをバックアップルータと呼びます。

スイッチに仮想ルータ用の VRRP 機能を設定するためには、IP インタフェースが存在し、その IP アドレスが VLAN に所属している必要があります。VRRP 用 IP インタフェースはスイッチの VLAN（IP インタフェース）ごとに設定します。VRRP 機能が正しく動作するために、同じ VRRP グループ内の VRRP ルータは、同じ設定内容を持つ必要があります。

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。

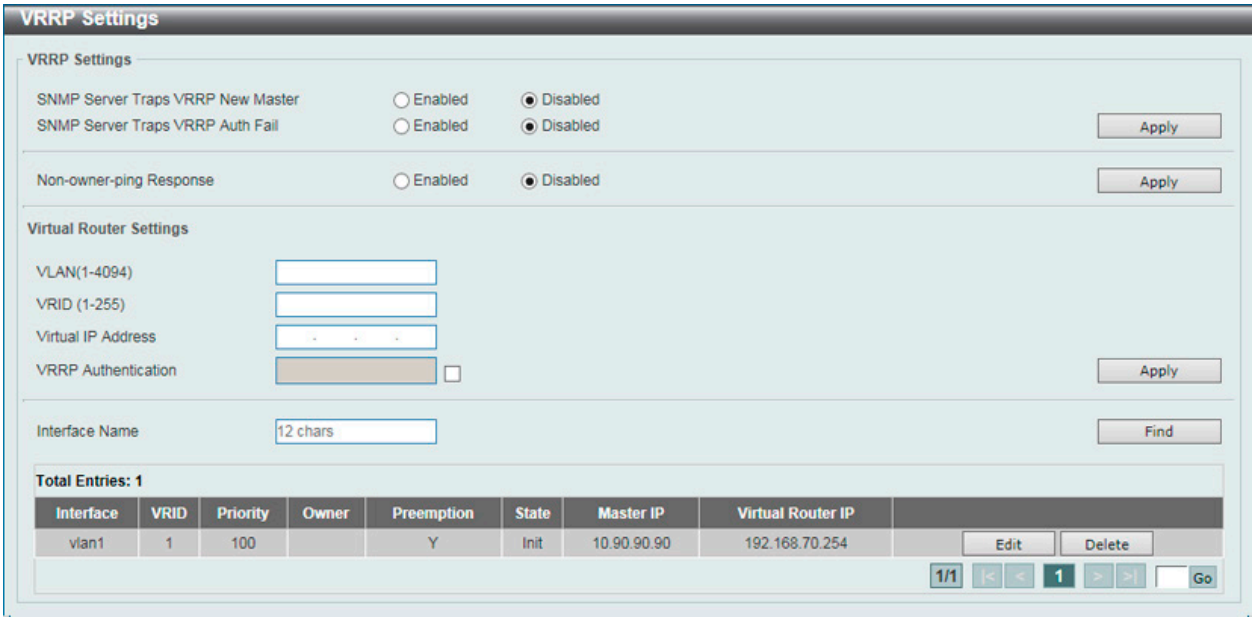


図 9-233　VRRP Settings 画面

以下の項目を使用して設定を行います。

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 / 無効に指定します。 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 / 無効に指定します。有効にすると認証鍵 / 認証タイプが衝突、または一致しないルータからパケットを受領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 / 無効に指定します。マスタ状態の仮想ルータによる、本仮想ルータと関連のある「ICMP エコーリクエスト」への応答を有効にします。
Virtual Router Settings	
VLAN	VLAN ID（1-4094）を指定します。
VRID (1-255)	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。
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（8 字以内）をプレーンテキストで指定します。 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（12 字以内）を指定します。

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

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

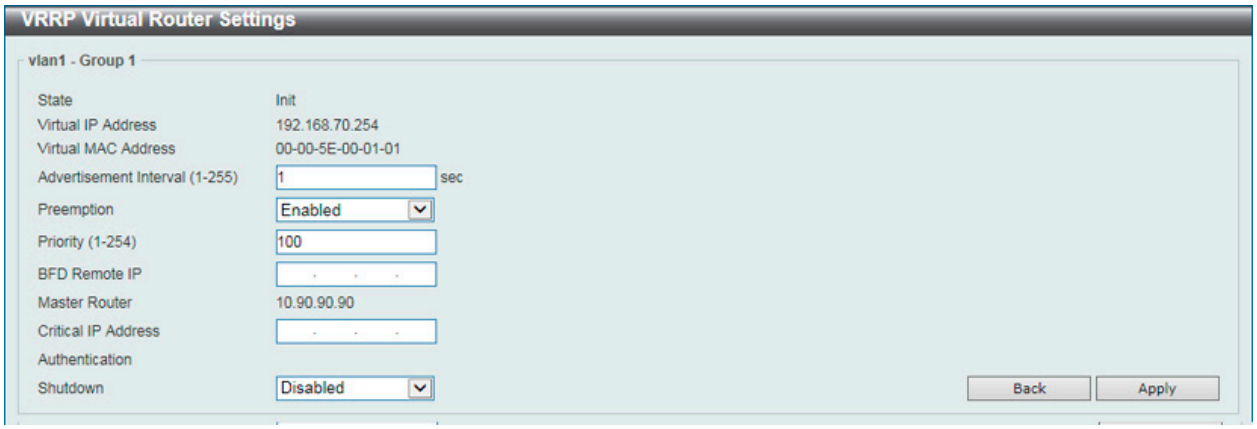


図 9-234 VRRP Settings (Edit) 画面

以下の項目を使用して設定を行います。

項目	説明
Advertisement Interval	通知間隔（1-255）を指定します。マスタルータによる VRRP 通知の間隔値です。初期値は「1」です。
Preemption	「Preemption」（優先置き換え）機能を有効 / 無効に指定します。 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と置き替わるかどうかを設定します。
Priority (1-254)	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。
BFD Remote IP	「Bidirectional Forwarding Detection」(BFD) リモート IP アドレスを指定します。本 IP アドレスは同じ VRRP 仮想グループの実存デバイスの実存 IP アドレスである必要があります。BFD セッションはこの VRRP ルータとピア間で生成されます。セッションが落ちると VRRP はバックアップステートになり、マスタと交換します。
Critical IP Address	インターネットへの最も直接的な経路、またはこの仮想ルータからの他のクリティカルなネットワーク接続を提供する物理デバイスの IP アドレスを入力します。これはネットワークにある本物のデバイスの IP アドレスです。仮想ルータからこの IP アドレスへの接続に失敗すると、仮想ルータは自動的に無効になります。新しいマスタは VRRP グループに所属するバックアップルータから選出されます。異なる Critical IP Address が VRRP グループに所属する異なるルータに割り当てられ、インターネットまたは他のクリティカルネットワーク接続に複数の経路を定義します。
Shutdown	シャットダウンを有効 / 無効に指定します。インタフェースの仮想ルータを無効にします。他のオーナルータをシャットダウンする前に、指定 IP アドレスのルータをシャットダウンするミスを回避する目的です。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

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 9-235 VRRPv3 Settings 画面

以下の項目を使用して設定を行います。

項目	説明
VLAN	VLAN ID（1-4094）を指定します。
VRID (1-255)	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。
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。 • IPv6 - IPv6 仮想ルータを指定します。
Interface Name	インタフェース名（12 字以内）を指定します。

「Apply」ボタンをクリックし、設定を有効にします。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「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。

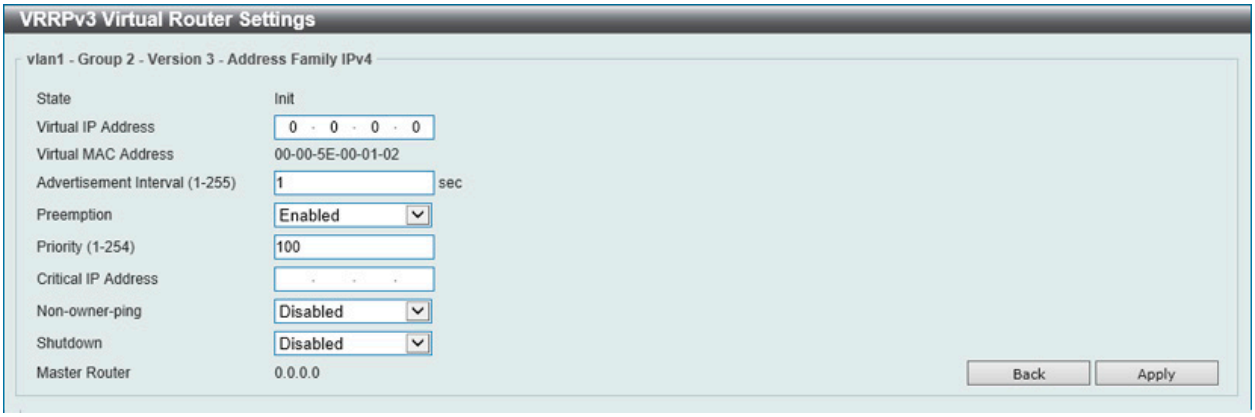


図 9-236 VRRPv3 Settings (Edit/IPv4 Address Family) 画面

以下の項目を使用して設定を行います。

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、またはルータの実存のアドレスである必要があります。仮想アドレスがインタフェースの実存するアドレスと同等の場合、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（1-255）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。
Preemption	「Preemption」（優先置き換え）機能を有効 / 無効に指定します。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と置き替わるかどうかを設定します。

項目	説明
Priority (1-254)	仮想ルータの優先値（1-254）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 グループの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、最高値（255）となります。
Critical IP Address	インターネットへの最も直接的な経路、またはこの仮想ルータからの他のクリティカルなネットワーク接続を提供する物理デバイスの IP アドレスを入力します。これはネットワークにある本物のデバイスの IP アドレスです。仮想ルータからこの IP アドレスへの接続に失敗するとが、仮想ルータは自動的に無効になります。新しいマスタは VRRP グループに所属するバックアップルータから選出されます。異なる Critical IP Address が VRRP グループに所属する異なるルータに割り当てられ、インターネットまたは他のクリティカルネットワーク接続に複数の経路を定義します。
Non-owner ping	「Non-owner ping」（非オーナ Ping）機能を有効 / 無効に指定します。マスタステートの非 IP アドレスオーナ仮想ルータによる IPv4 アドレスの ICMP エコーリクエスト、または IPv6 アドレスの ND リクエストへの応答を有効にします。
Shutdown	シャットダウンを有効 / 無効に指定します。インタフェースの仮想ルータを無効にします。他のオーナルータをシャットダウンする前に、指定 IP アドレスのルータをシャットダウンするミスを回避する目的です。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

「IPv6 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。

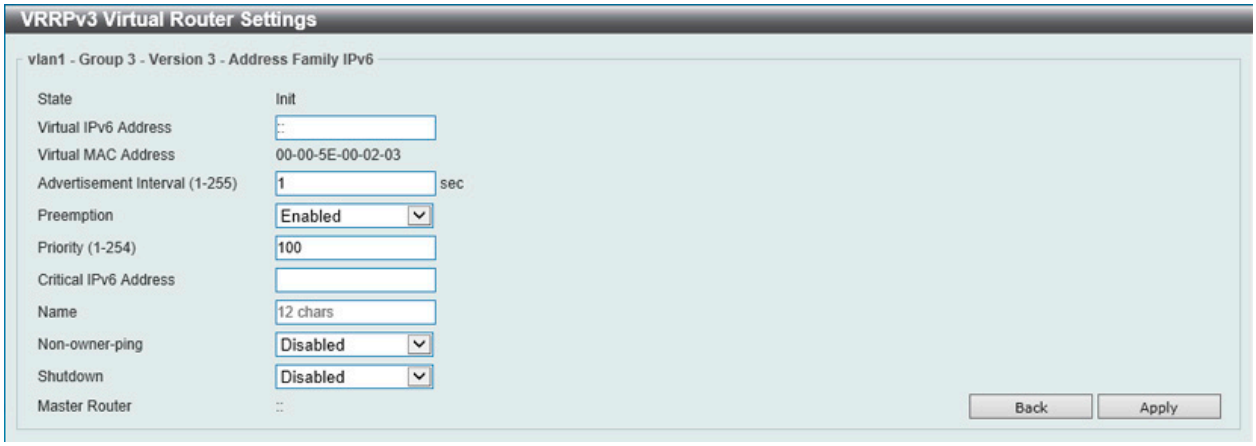


図 9-237　VRRPv3 Settings (Edit/IPv6 Address Family) 画面

以下の項目を使用して設定を行います。

項目	説明
Virtual IPv6 Address	仮想 IPv6 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、またはルータの実存のアドレスである必要があります。仮想アドレスがインタフェースの実存するアドレスと同等の場合、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（1-255）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。
Preemption	「Preemption」（優先置き換え）機能を有効 / 無効に指定します。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と置き替わるかどうかを設定します。
Priority (1-254)	仮想ルータの優先値（1-254）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 グループの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、最高値（255）となります。
Critical IPv6 Address	インターネットへの最も直接的な経路、またはこの仮想ルータからの他のクリティカルなネットワーク接続を提供する物理デバイスの IPv6 アドレスを入力します。これはネットワークにある本物のデバイスの IPv6 アドレスです。仮想ルータからこの IPv6 アドレスへの接続に失敗するとが、仮想ルータは自動的に無効になります。新しいマスタは VRRP グループに所属するバックアップルータから選出されます。異なる Critical IPv6 Address が VRRP グループに所属する異なるルータに割り当てられ、インターネットまたは他のクリティカルネットワーク接続に複数の経路を定義します。
Non-owner ping	「Non-owner ping」（非オーナ Ping）機能を有効 / 無効に指定します。マスタステートの非 IP アドレスオーナ仮想ルータによる IPv4 アドレスの ICMP エコーリクエスト、または IPv6 アドレスの ND リクエストへの回答を有効にします。
Shutdown	シャットダウンを有効 / 無効に指定します。インタフェースの仮想ルータを無効にします。他のオーナルータをシャットダウンする前に、指定 IPv6 アドレスのルータをシャットダウンするミスを回避する目的です。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

第 10 章　QoS（QoS 機能の設定）

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

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

サブメニュー	説明
Basic Settings（基本設定）	QoS の Basic Settings（基本設定）を行います。
Advanced Settings（アドバンス設定）	QoS の Advanced Settings（アドバンス設定）を行います。
QoS PFC	ネットワーク「Quality of Service」(QoS) プライオリティベースフローコントロール (PFC) クラスマップの設定を行います。
WRED（WRED 設定）	WRED（WRED 設定）の設定を行います。
iSCSI（アイスカジー）	iSCSI 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。

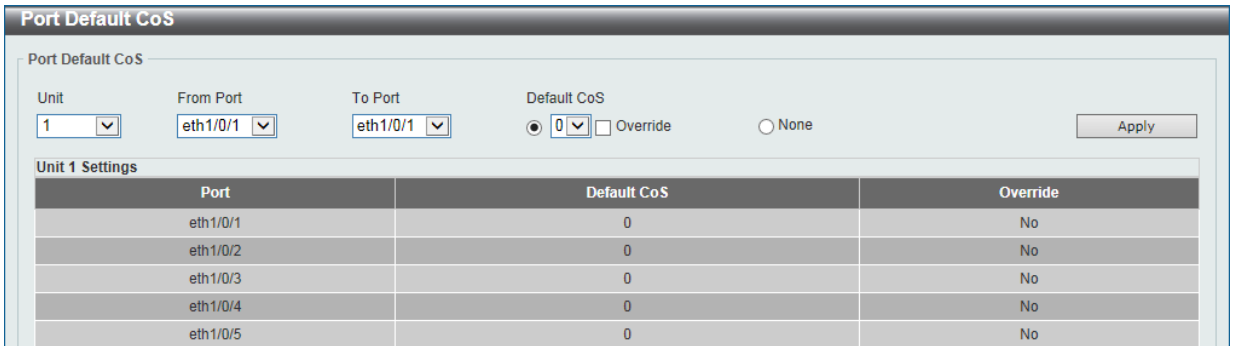


図 10-1　Port Default CoS 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
Default CoS	ポートに初期 CoS を指定します。0 から 7 の間で指定可能です。「Override」にチェックを入れるとポートに受信したすべてのパケット（タグありなし関わらず）にポートの CoS が適用されます。「None」を選択すると、初期設定を有効にします。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。「Class-0」（クラス 0）は最も低い優先度のキューで、「Class-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 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。

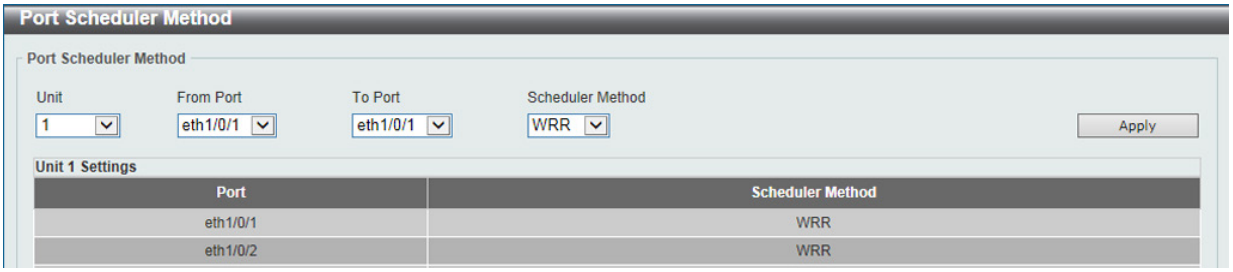


図 10-2　Port Scheduler Method 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Scheduler Method	指定ポートに対するスケジューリングの方法を設定します。 「Strict Priority」(SP)、「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。「WDRR」は送信キューに蓄積したバックログクレジットのセットを供給することで作動します。 はじめに各キューはクレジットカウンタを量の値として設定します。CoS キューからのパケットが送信される度に、パケットのサイズはクレジットカウンタから差し引かれ、サービスの権利は次の低い CoS キューに移行されます。 クレジットカウンタが 0 以下になると、クレジットが補完されるまでキューは停止します。すべての CoS キューが 0 に到達するとクレジットカウンタは補完されます。すべてのパケットはクレジットカウンタが 0 かそれ以下の場合、実行され最後のパケットも全て送信されます。こうなった場合、クレジットは補完されます。クレジットが補完されるといくつかのクレジットは各 QoS キュークレジットカウンタに追加されます。各 CoS キューの集合体はユーザ定義に基づいてそれぞれ同じではありません。SP モードでの CoS キューの設定はより優先値の高い CoS キューがストリクトプライオリティーモードで設定されている必要があります。優先値の高い CoS キューからパケットが送信されると、関連した重量（Weight）が 1 差し引かれ、次の低い CoS キューがのパケットが実行されます。CoS キューの重量（Weight）がゼロになると、補完されるまでキューは実行されません。すべての CoS キューの重量（Weight）が 0 に到達すると同時にその重量（Weight）は補完されます。

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。

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。

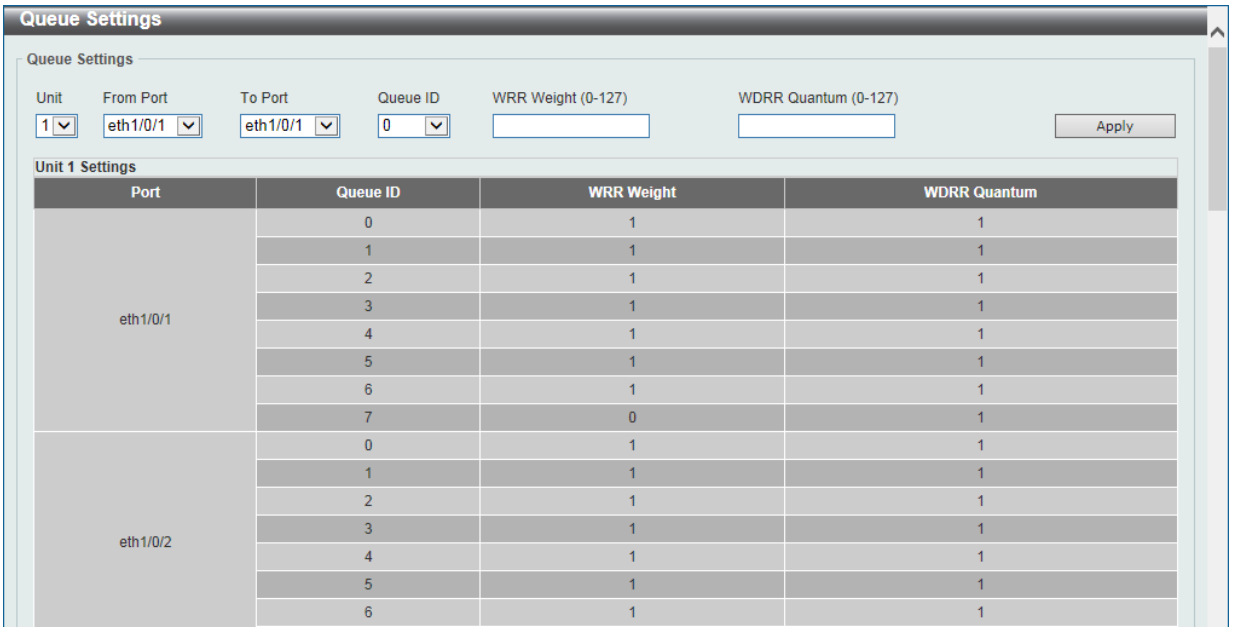


図 10-3　Queue Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Queue ID	キュー ID を指定します。0 から 7 の間で指定可能です。
WRR Weight	WRR の値を入力します。0 から 127 の間で指定可能です。「Expedited Forwarding」(EF) の要件を満たすには最高のキューは常に「Per-hop Behavior」(PHB) により選択されキューのスケジュールモードはストリクトプライオリティである必要があります。そのため最後のキューの重さは「Differentiate Service」がサポートされている間は 0 に設定する必要があります。
WDRR Quantum	「WDRR Quantum」の値を入力します。0 から 127 の間で指定できます。

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

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

本画面には以下の項目があります。

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。

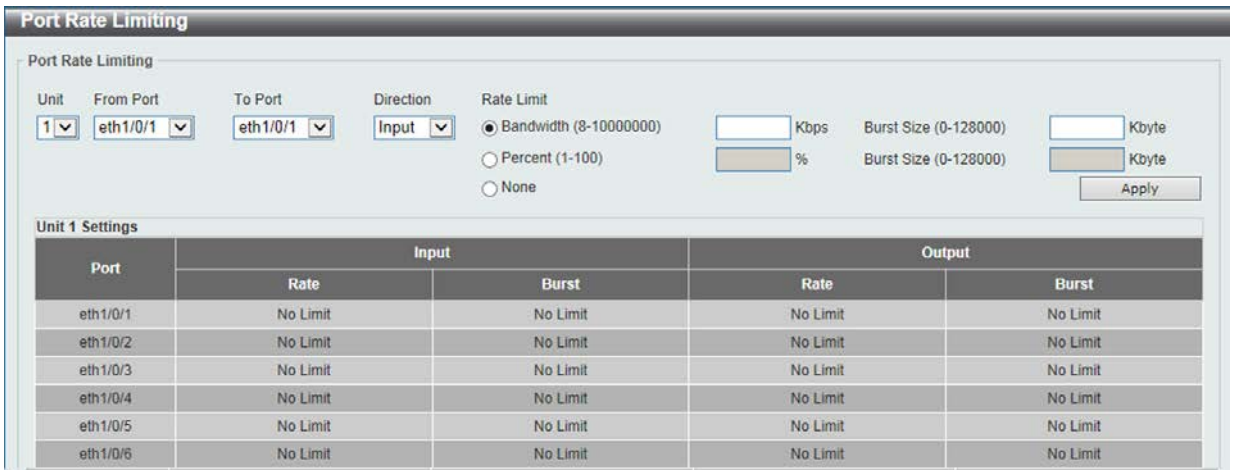


図 10-5　Port Rate Limiting 画面

以下の項目を設定または表示できます。

項目	説明
Unit	設定するユニット名を選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Direction	レート制限の対象を Input（イングレス）、Output（イーグレス）から選択します。

項目	説明
Rate Limit	レート制限の値を指定します。 • 「Bandwidth」-「Bandwidth」を選択し、受信 / 送信の帯域値を入力欄に入力します。この値は 8 から 10000000 Kbps で指定できます。また「Burst Size」の値も 0 から 128000Kbytes で指定可能です。 • 「Percent」-「Percent」を選択し、受信 / 送信の帯域パーセントを入力欄に入力します。この値は 1 から 100%で指定できます。また「Burst Size」の値も 0 から 128000 kilobytes で指定可能です。 • 「None」-「None」を選択すると指定ポートのレート制限を削除します。指定の制限はインタフェースの最大スピードを超えません。イングレスは受信したトラフィックが制限を超えた場合、フレーム、またはフローコントロールフレームを停止します。

「Apply」ボタンをクリックして行った変更を適用します。

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。

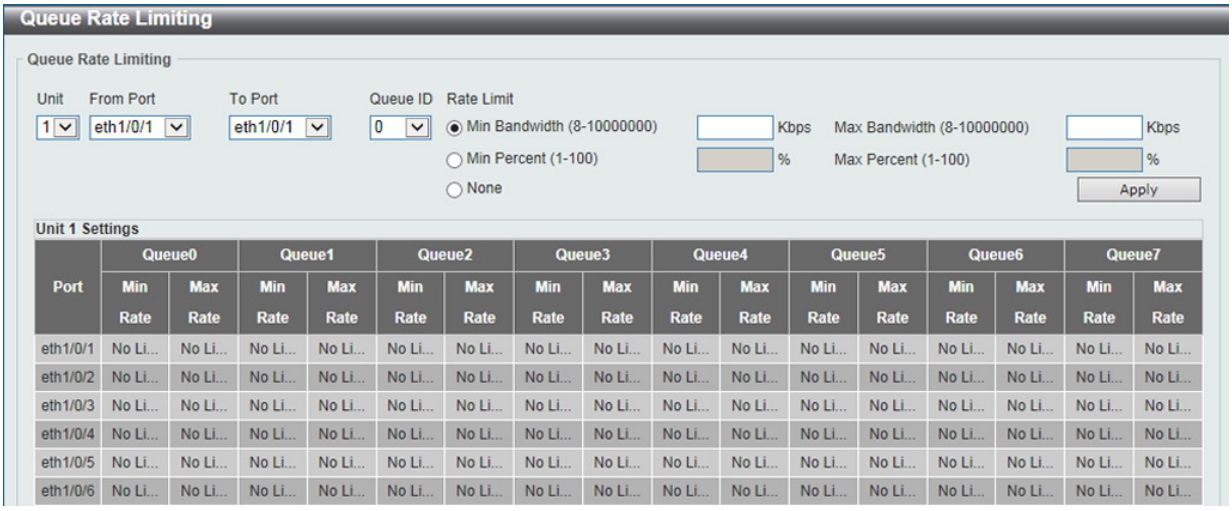


図 10-6　Queue Rate Limiting 画面

以下の項目を設定または表示できます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。
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は保障されます。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集合体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。 最高に厳しい優先キューの最小保証帯域は必ずしも必要という訳ではありません。これはすべてのキューの最小帯域が条件を満たしていれば、キューのトラフィックは実行されるからです。 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は不可能です。それは一つの CoS の最小保証帯域は物理ポート間では使用不可能だからです。 「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。

「Apply」ボタンをクリックして行った変更を適用します。

注意　キュー帯域幅制御の最小グラニュラリティは 64Kbps です。システムは自動的に 64 倍の数に調整します。

Queue Statistics Table（キュー統計テーブル）

キュー統計テーブルを表示します。

QoS > Basic Settings > Queue 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。

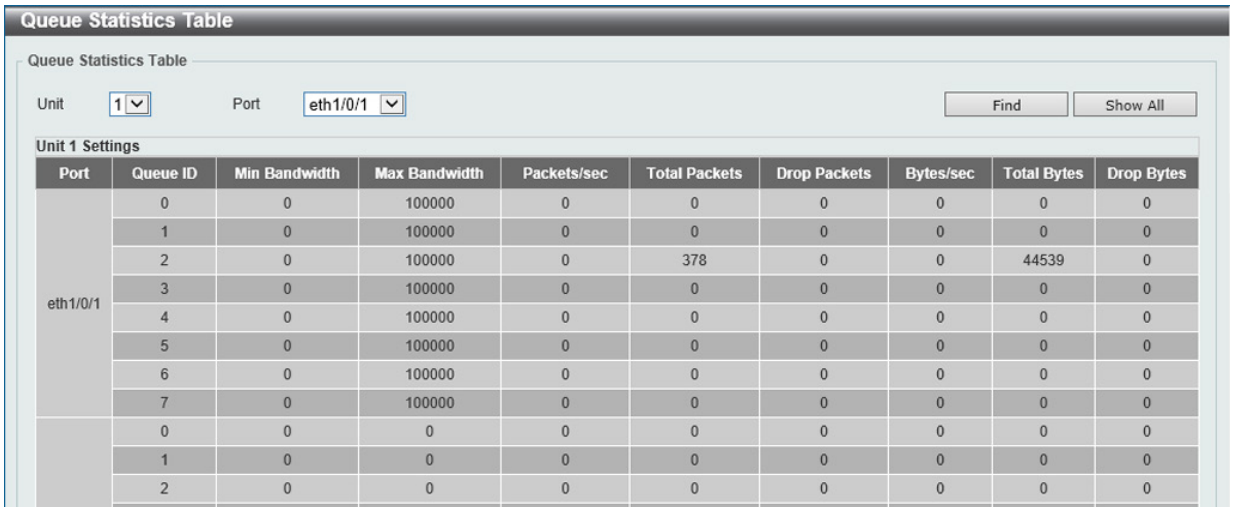


図 10-7　Queue Statistics Table 画面

以下の項目を設定または表示できます。

項目	説明
Unit	ユニットを選択します。
Port	ポートを選択します。

ポートを選択し「Find」ボタンをクリックして、指定のポートについて表示します。
「Show All」ボタンをクリックして全ポートについて表示します。

Advanced Settings（アドバンス設定）

QoS の Advanced Settings（アドバンス設定）を行います。

DSCP Mutation Map（DSCP 変更マップ設定）

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 DSCP 変更マップに基づき受信 DSCP は QoS 動作の前に他の DSCP に変化します。DSCP 変更は違う DSCP タスク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。

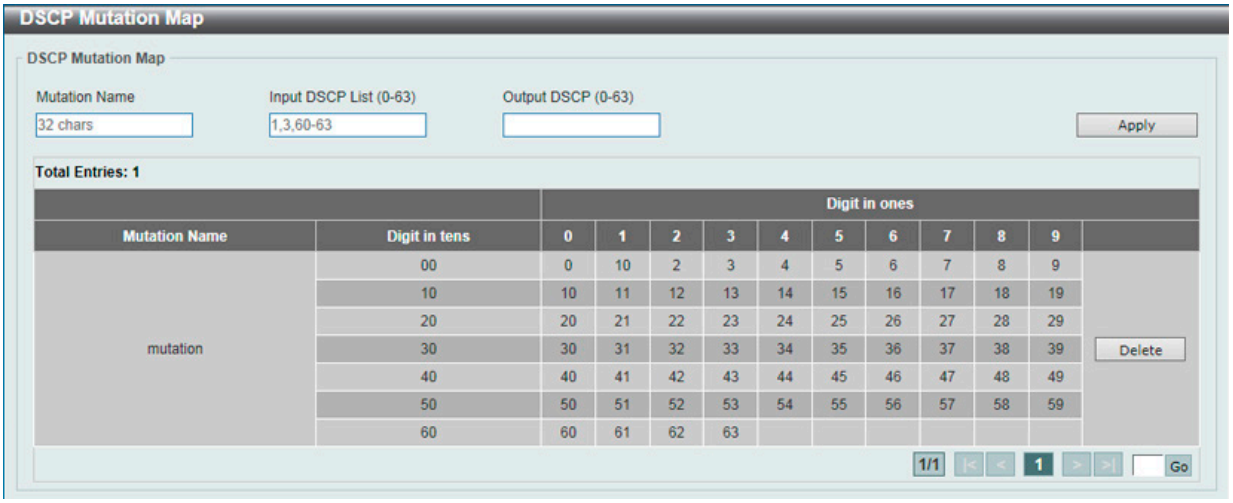


図 10-8　DSCP Mutation Map 画面

本画面には次の項目があります。

項目	説明
Mutation Name	DSCP 変更マップ名を指定します。32 文字以内で指定可能です。
Input DSCP List	インプットされる DSCP リスト値を入力します。0 から 63 で指定可能です。
Output DSCP	アウトプットされる DSCP 値を入力します。0 から 63 で指定可能です。

「Apply」ボタンをクリックし、各項目の変更を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Port Trust State 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。

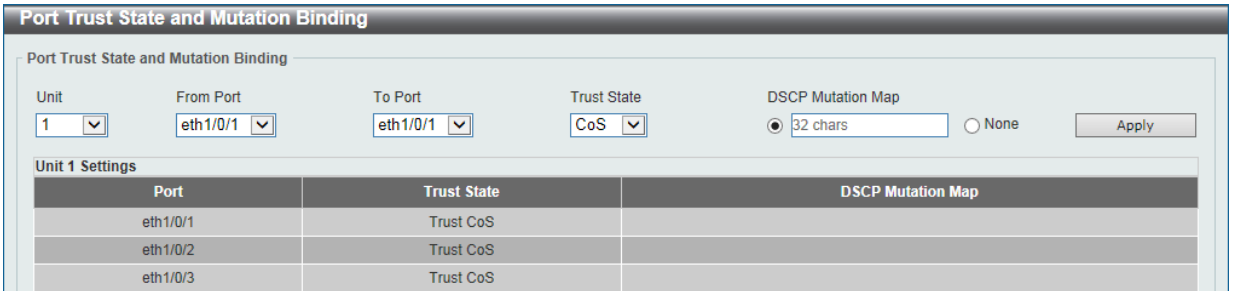


図 10-9　Port Trust State and Mutation Binding 画面

以下の項目を設定または表示できます。

項目	説明
Unit	設定するユニット名を選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Trust State	ポートトラストの設定をします。「CoS」「DSCP」から選択可能です。
DSCP Mutation Map	DSCP 変更マップ名を入力します。32 文字以内で設定可能です。 「None」を選択するとどのポートに DSCP 変更マップを指定しません。

「Apply」ボタンをクリックして行った変更を適用します。

DSCP CoS Mapping（DSCP CoS マップ設定）

本スイッチにおける DSCP CoS マップの設定と表示を行います。

QoS > 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。

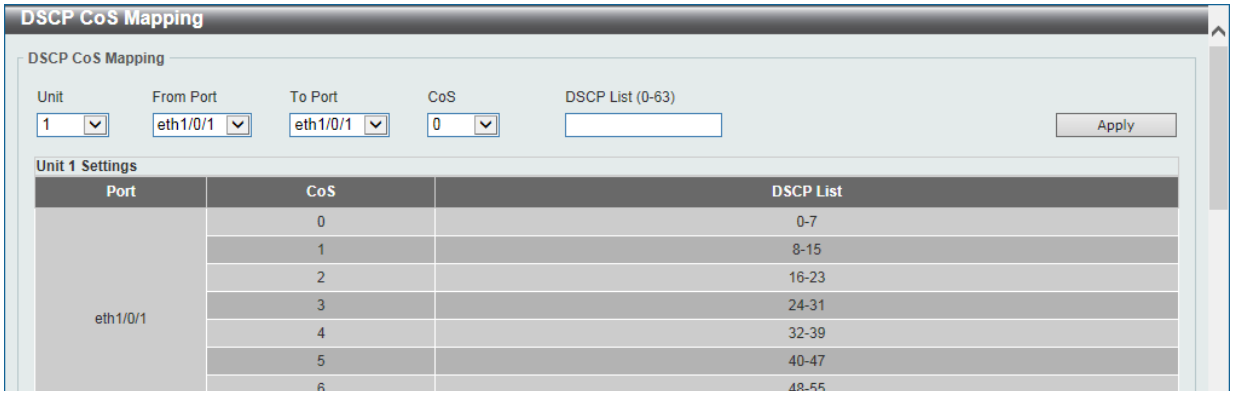


図 10-10　DSCP CoS Mapping 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
CoS	CoS の値を指定します。0 から 7 の間で指定可能です。
DSCP List (0-63)	DSCP リストの値を入力します。0 から 63 の範囲で設定します。

設定を変更する際は、必ず「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 10-11　CoS Color Mapping 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
CoS List	カラーマップされる CoS の値を指定します。0 から 7 の間で指定可能です。
Color	マップされるカラーを指定します。「Green」「Yellow」「Red」から指定可能です。

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

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。

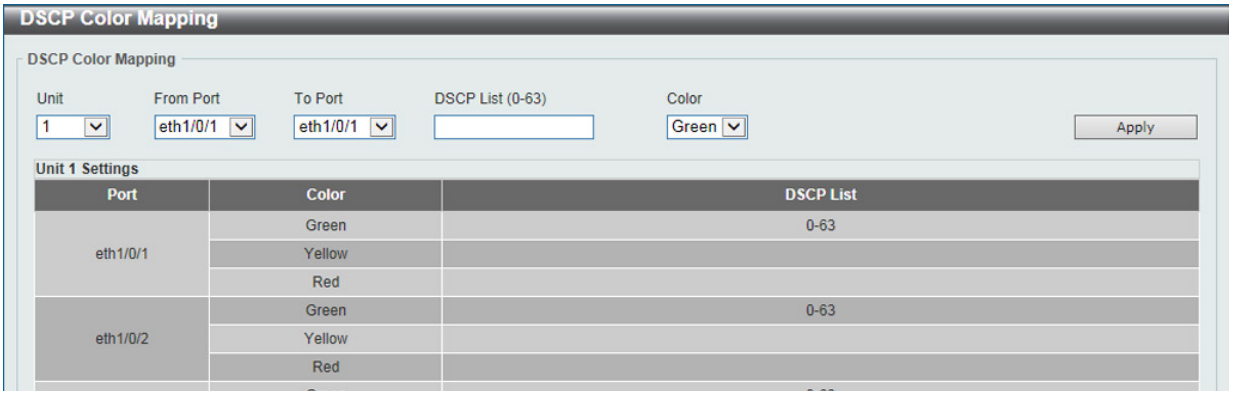


図 10-12 DSCP Color Mapping 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
DSCP List	カラーマップされる DSCP の値を指定します。0 から 63 の間で指定可能です。
Color	マップされるカラーを指定します。「Green」「Yellow」「Red」から指定可能です。

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

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 10-13 Class Map 画面

本画面には以下の項目があります。

項目	説明
Class Map Name	クラスマップ名を指定します。32 文字まで指定可能です。
Multiple Match Criteria	複数のマッチクライテリアを指定します。「Match All」「Match Any」から選択可能です。

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

「Match」ボタンをクリックすると下記の画面が表示されます。

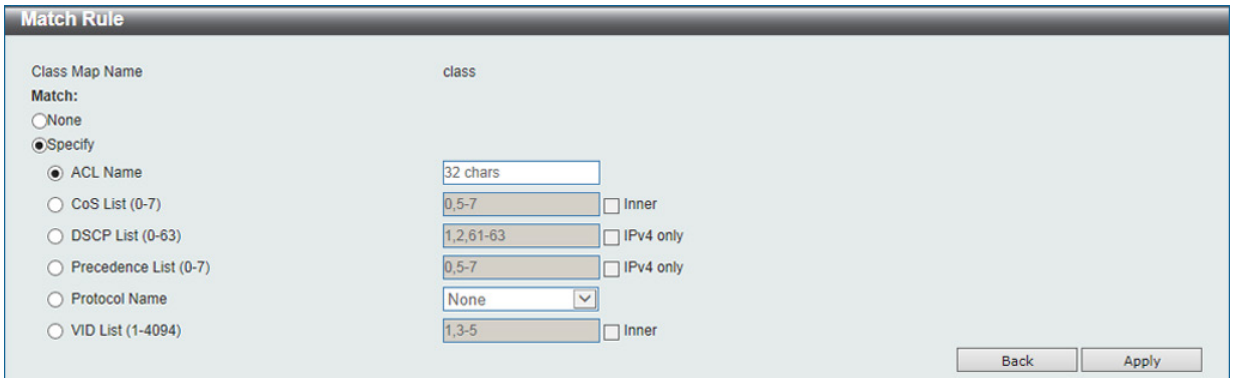


図 10-14　Match Rule 画面

本画面には以下の項目があります。

項目	説明
None	このクラスマップと何もマッチさせない場合選択します。
Specify	このクラスマップと下記のオプションのどれかをマッチさせる場合に選択します。
ACL Name	クラスマップとマッチさせるアクセスリスト名を指定します。32 文字まで指定できます。
CoS List	クラスマップとマッチさせる CoS リスト名を指定します。0 から 7 まで指定できます。「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 パケットとマッチさせます。
DSCP List	クラスマップとマッチさせる DSCP リスト名を指定します。0 から 63 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケットのみとマッチします。チェックを入れないと IPv4/v6 どちらのパケットともマッチします。
Precedence List	クラスマップとマッチさせる優先リスト名を指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケットのみとマッチします。チェックを入れないと IPv4/v6 どちらのパケットともマッチします。IPv6 パケットの場合、IPv6 ヘッダのトラフィッククラスにある 3 つの重要なビットになります。
Protocol Name	クラスマップとマッチさせ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	クラスマップとマッチさせる VLAN リストを指定します。1 から 4094 まで指定できます。 「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 とマッチさせます。

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。

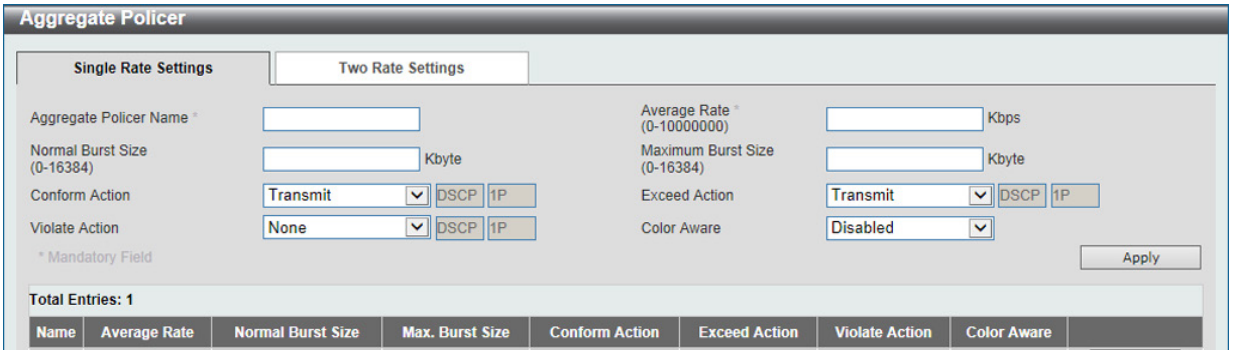


図 10-15　Aggregate Policer 画面

本画面には以下の項目があります。

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。0 から 10000000 kbps まで指定可能です。
Normal Burst Size	ノーマルバーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。
Maximum Burst Size	最大バーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。
Confirm Action	ここでは緑色パケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Transmit」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「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。 • 「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Exceed Action	レート制限を超えたパケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Transmit」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「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。 • 「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Violate Action	ノーマル、そしてシングルレートの最大バーストサイズを超えたパケットに行う操作を指定します。 「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。オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「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。 • 「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Color Aware	「Color Aware」を有効 / 無効に指定します。「Color Aware」が指定されないとポリサー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。
「Delete」をクリックすると指定の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。

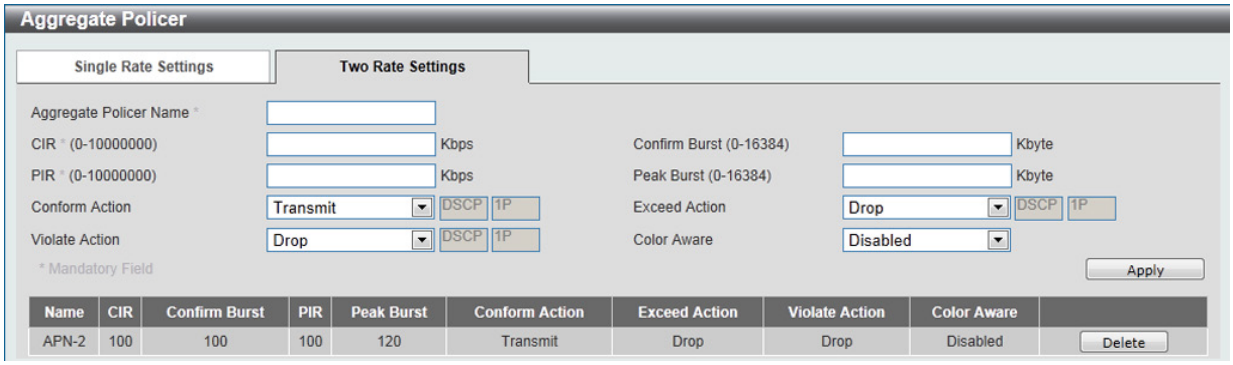


図 10-16 Two Rate Setting 画面

本画面には以下の項目があります。

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 値を入力します。0 から 10000000 kbps まで指定可能です。 コミットされたパケットは 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。0 から 16384 Kbytes まで指定可能です。 Confirm Burst は kbps における最初のトークンバケットのバーストサイズになります。
PIR	PIR 値を入力します。0 から 10000000 kbps まで指定可能です。 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	ピークバーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。 ピークバーストサイズは kbps における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行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Transmit」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「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。 • 「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Exceed Action	レート制限を超えたパケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Transmit」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「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。 • 「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Violate Action	ノーマル、そしてシングルレートの最大バーストサイズを超えたパケットに行う操作を指定します。 「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。オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「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。 • 「Set-DSCP-1p」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Color Aware	「Color Aware」を有効 / 無効に指定します。「Color Aware」が指定されないとポリサー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 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。

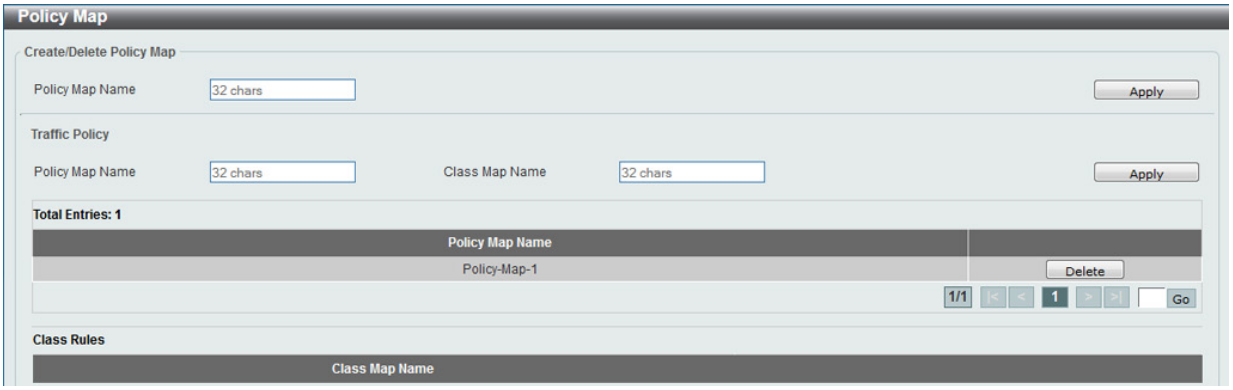


図 10-17　Policy Map 画面

本画面の「Create/Delete Policy Map」には以下の項目があります。

項目	説明
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。

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

本画面の「Traffic Policy」には以下の項目があります。

項目	説明
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。
Class Map Name	クラスマップ名を指定します。32 文字まで指定可能です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Policer」ボタンをクリックし、指定のポリシーマップのポリサーアクション設定をします。
「Delete」ボタンをクリックし、指定のエントリを削除します。

「Set Action」ボタンをクリックし、指定のポリシーマップの設定をします。以下の画面が表示されます。

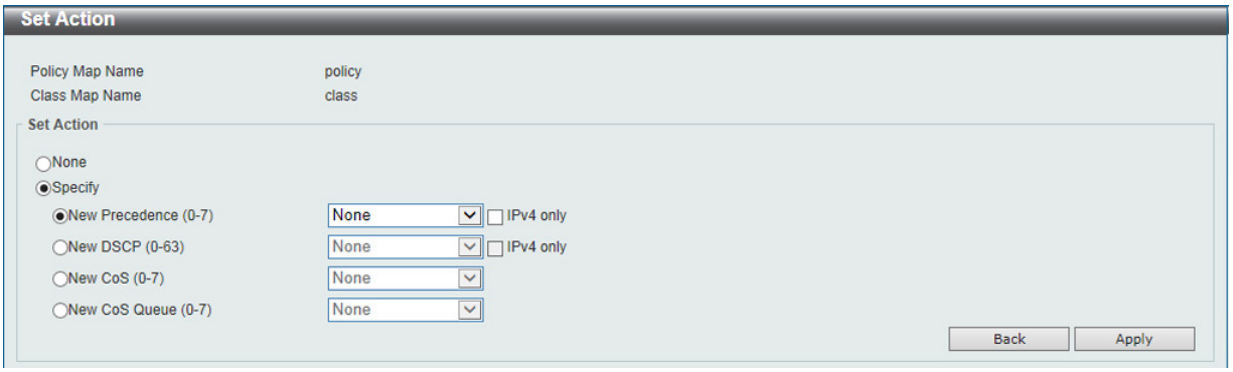


図 10-18　Set Action 画面

本画面には以下の項目があります。

項目	説明
None	このマップと何もマッチさせない場合選択します。
Specify	このマップとオプションのどれかをマッチさせる場合に選択します。
New Precedence	パケットの優先値を指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー選択には影響ありません。
New DSCP	パケットの新しい DSCP 名を指定します。0 から 63 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー選択には影響ありません。
New CoS	パケットの新しい CoS 値を指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー選択には影響ありません。
New CoS Queue	パケットの新しい CoS キューを指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー上書きします。

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。

「Policer」ボタンをクリックすると以下の画面が表示されます。

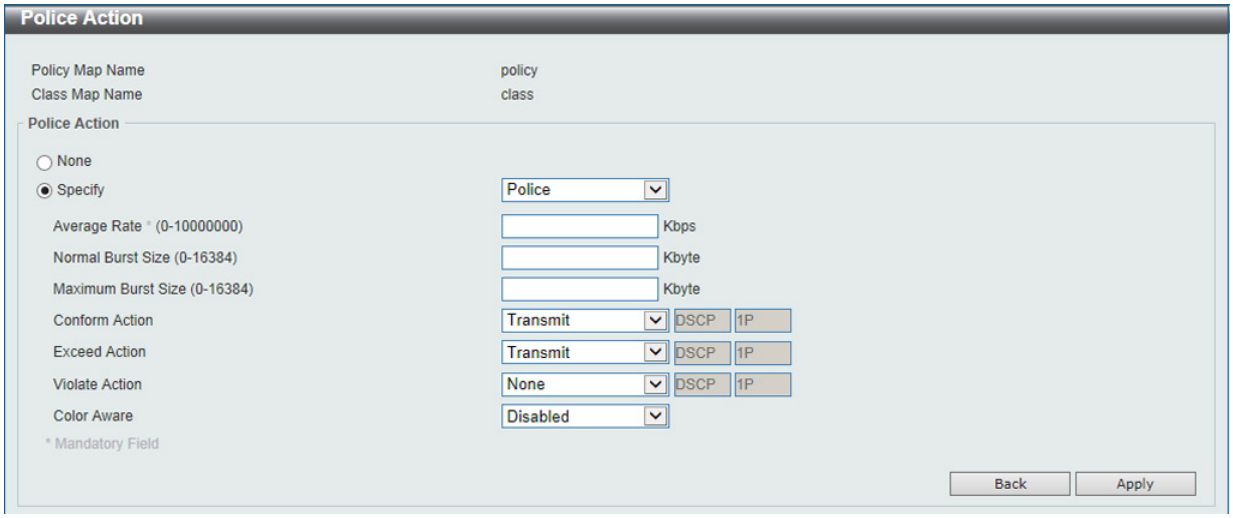


図 10-19　Policer 画面

本画面には以下の項目があります。

項目	説明
None	このマップと何もマッチさせない場合選択します。
Specify	このマップとオプションのどれかをマッチさせる場合に選択します。
Average Rate	アベレージレート値（0-10000000/Kbps）を入力します。
Normal Burst Size	ノーマルバーストサイズ（0-16384/Kbyte）を入力します。
Maximum Burst Size	最大バーストサイズ（0-16384/Kbyte）を入力します。
Confirm Action	ここでは緑色パケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Transmit」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Exceed Action	ここでは黄色パケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Transmit」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Violate Action	ここでは赤色パケットに行う操作を指定します。 「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。オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Color Aware	「Color Aware」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。

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。

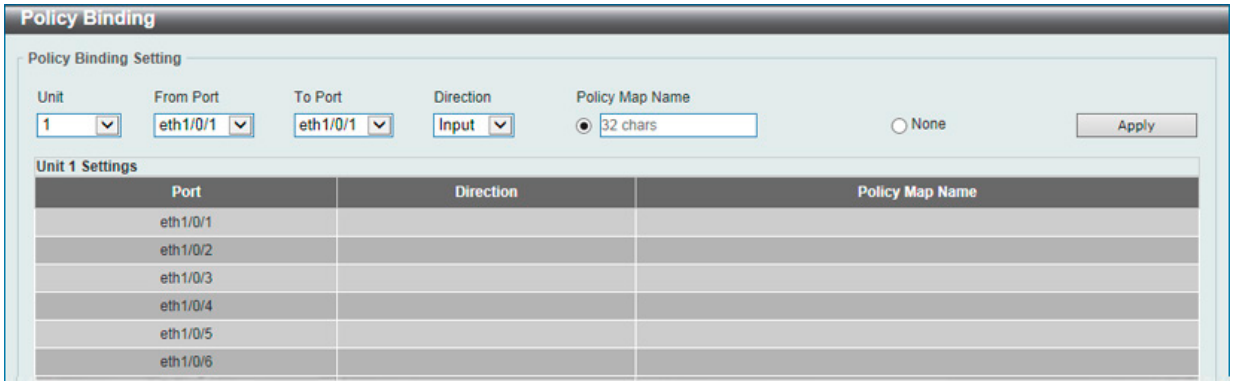


図 10-20　Policy Binding 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
Direction	方向を指定します。「Input」「Output」が選択可能です。「Input」は指定のイングレストラフィックのことです。「Output」は指定のイーグレストラフィックのことです。
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。「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。

QoS PFC

ネットワーク「Quality of Service」(QoS) プライオリティベースフローコントロール (PFC) クラスマップの設定を行います。

Network QoS Class Map（ネットワーク QoS クラスマップ）

本項目ではネットワーク「Quality of Service」(QoS) プライオリティベースフローコントロール (PFC) クラスマップの設定、表示を行います。
ポリシーバインディング設定を行います。

QoS > QoS PFC > Network QoS 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。

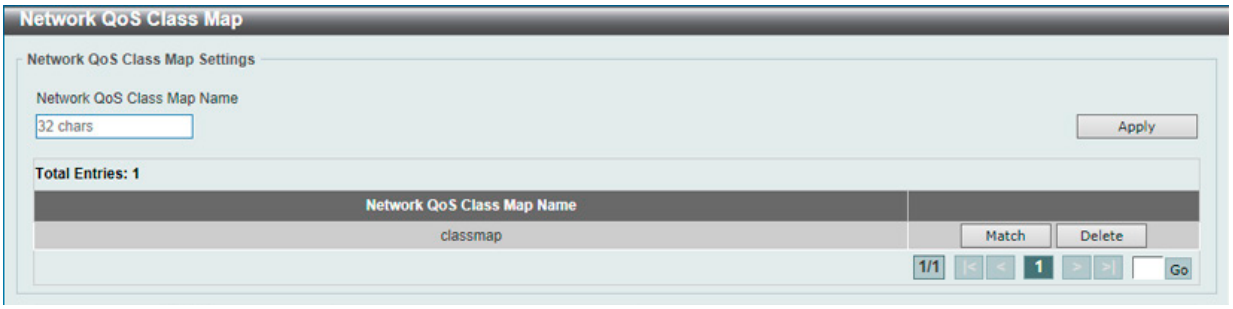


図 10-21　Network QoS Class Map 画面

本画面には以下の項目があります。

項目	説明
Network QoS Class Map Name	トラフィックポリシーのネットワーク QoS クラスマップ名（32 字以内）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」をクリックすると指定のエントリを削除します。
「Match」をクリックすると指定のエントリのマッチルール設定を設定します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Match」をクリックすると、以下の画面が表示されます。

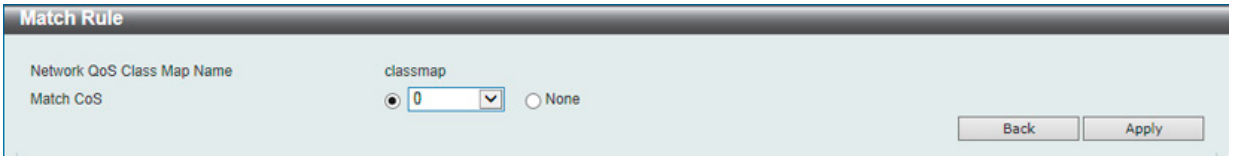


図 10-22　Network QoS Class Map (Match) 画面

本画面には以下の項目があります。

項目	説明
Match CoS	マッチする IEEE 802.1Q Class of Service (CoS) 値（0-7）を指定します。パケットを受信するとパケットはインターナル CoS に配布されます。インターナル CoS は CoS に基づいたキューマップへの送信キューを選択するのに使用されます。高い値の CoS キューは高い優先値を保持します。「None」を選択すると該当の CoS 値でのマッチングを無効にします。

「Back」をクリックすると前のページに戻ります。
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

Network QoS Policy Map（ネットワーク QoS ポリシーマップ）

本項目ではネットワーク「Quality of Service」(QoS) ポリシーマップの設定、表示を行います。

QoS > QoS PFC > Network QoS 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。

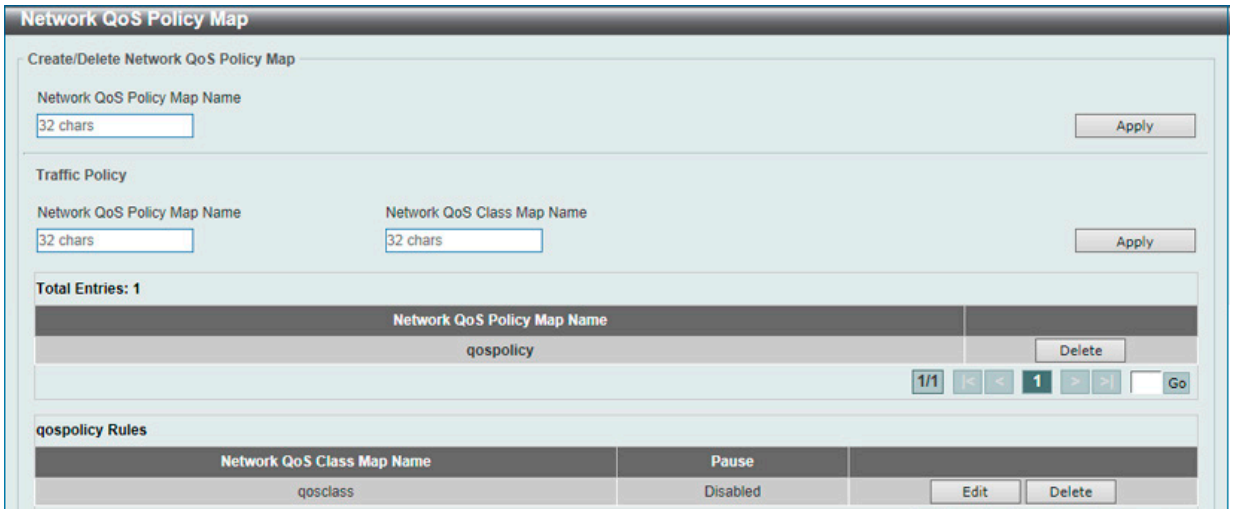


図 10-23 Network QoS Policy Map 画面

本画面には以下の項目があります。

項目	説明
Create/Delete Network QoS Policy Map	
Network QoS Policy Map Name	トラフィックポリシーのネットワーク QoS ポリシーマップ名（32 字以内）を指定します。
Traffic Policy	
Network QoS Policy Map Name	トラフィックポリシーのネットワーク QoS ポリシーマップ名（32 字以内）を指定します。
Network QoS Class Map Name	トラフィックポリシーのネットワーク QoS クラスマップ名（32 字以内）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」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
「Edit」をクリックして、指定エントリの編集を行います。

「Edit」をクリックすると、以下の画面が表示されます。

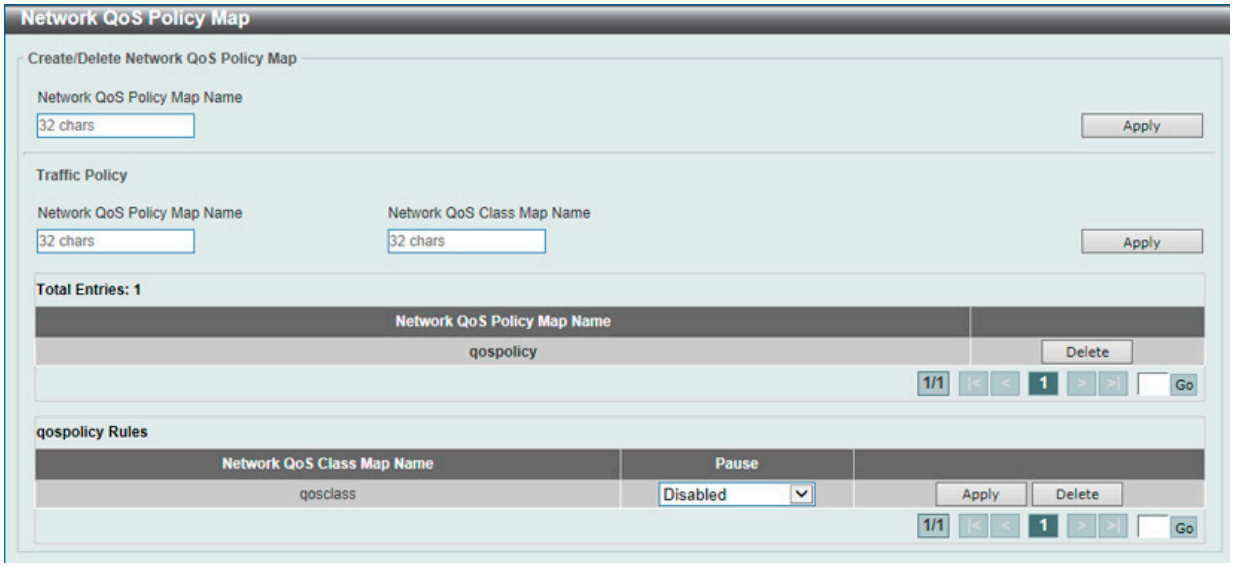


図 10-24 Network QoS Policy Map (Edit) 画面

本画面には以下の項目があります。

項目	説明
Pause	「Pause」機能を有効 / 無効に指定します。タイプネットワーク QoS ポリシーマップ内参照クラスの PFC を有効にします。

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

Network QoS Policy Binding（ネットワーク QoS ポリシーバインディング）

本項目ではネットワーク「Quality of Service」(QoS) ポリシーバインディングの設定、表示を行います。

QoS > QoS PFC > Network QoS 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 10-25　Network QoS Policy Binding 画面

本画面には以下の項目があります。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Direction	「Input」を指定します。インタフェースでポリシーマップはイングレスフローとなります。
Network QoS Policy Map Name	トラフィックポリシーのネットワーク QoS ポリシーマップ名（32 字以内）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

PFC Port Settings（PFC ポート設定）

本項目では Priority-based Flow Control (PFC) の設定、表示を行います。

注意　Priority-based Flow Control (PFC) は 10G ポートでのみ有効です。

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

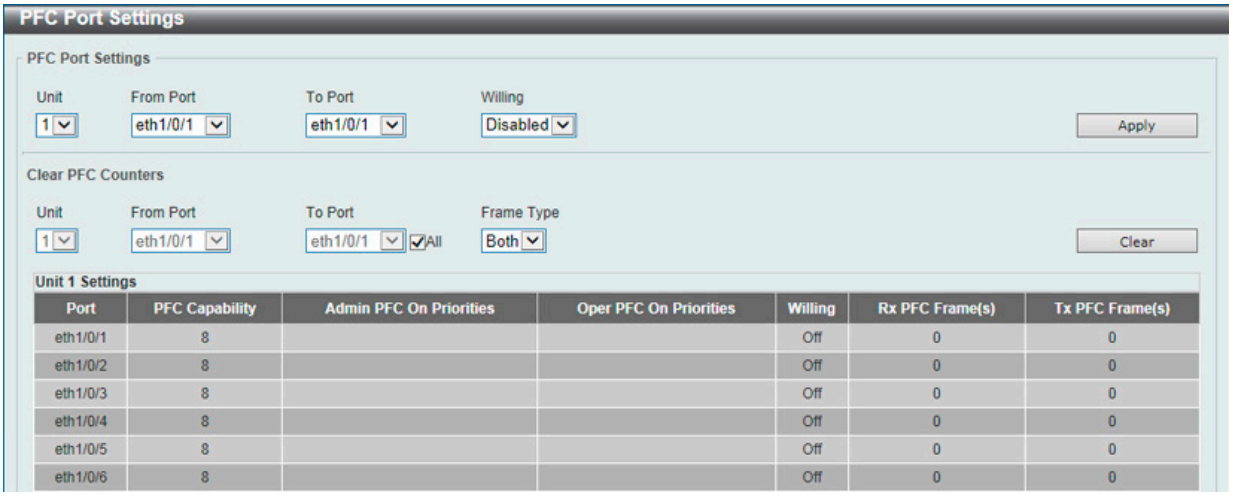


図 10-26　PFC Port Settings 画面

本画面には以下の項目があります。

項目	説明
PFC Port Settings	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

項目	説明
Willing	「Willing」機能を有効 / 無効に指定します。「Data Center Bridging Exchange Protocol」(DCBX) PFC willing 機能は指定ポートでリモートシステムからの PFC 設定を受け入れる機能です。
Clear PFC Counters	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Frame Type	クリアするフレームタイプを指定します。 • RX - 受信 PFC フレームカウンタをクリアします。 • TX - 送信 PFC フレームカウンタをクリアします。 • Both - 送受信 PFC フレームカウンタをクリアします。

「Apply」をクリックし、設定内容を適用します。
「Clear」をクリックすると入力したエントリをクリアします。

WRED（WRED 設定）

WRED のプロファイルやキュー、ドロップカウンタの設定を行います。

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。

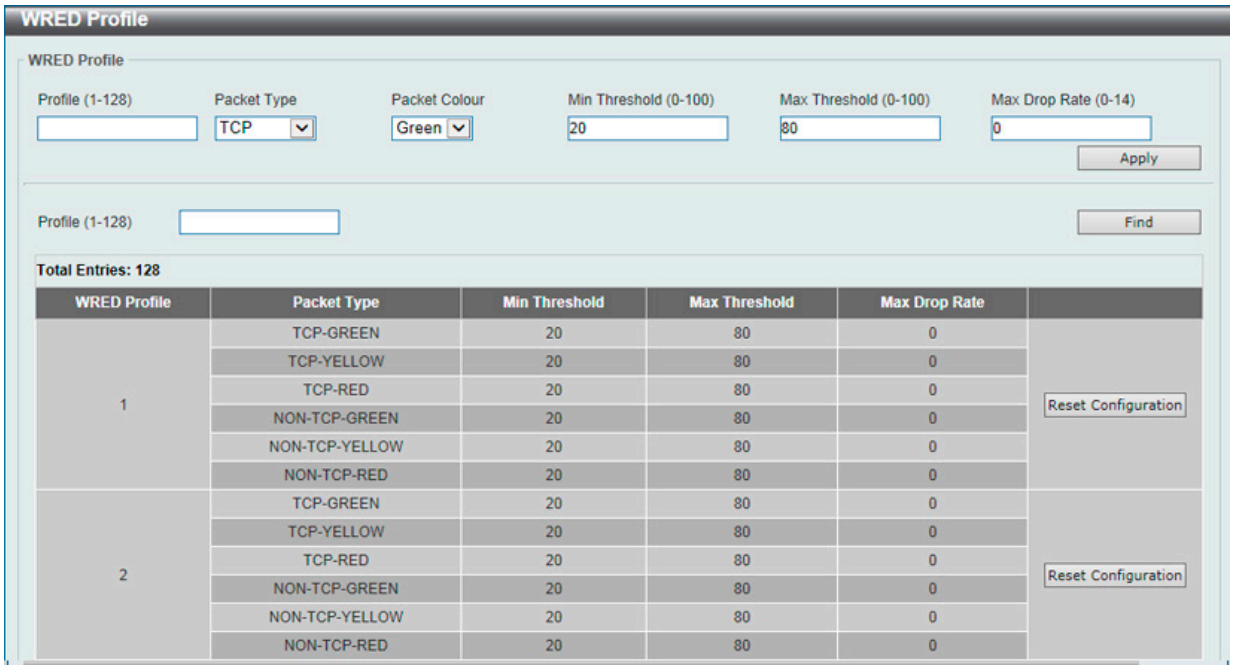


図 10-27　WRED Profile Settings 画面

本画面には以下の項目があります。

項目	説明
Profile (1-128)	WRED プロファイル ID を入力します。
Packet Type	パケットタイプ（TCP または Non-TCP）を選択します。
Packet Colour	破棄するパケットカラー（Green、Yellow または Red）を選択します。
Min Threshold (0-100)	使用するしきい値（最小）を入力します。キューサイズがこの値より高いと、カラー「Yellow」が割り当てられます。キューサイズがこの値より低いと、カラー「Green」が割り当てられ、破棄されないことを保証されます。「Yellow」パケットの動作は、このカラーのプロファイル設定に依存します。
Max Threshold (0-100)	使用するしきい値（最大）を入力します。キューサイズがこの値より低いと、カラー「Yellow」が割り当てられます。キューサイズがこの値より高いと、カラー「Red」が割り当てられ、破棄されます。「Yellow」パケットの動作は、このカラーのプロファイル設定に依存します。
Max Drop Rate (0-14)	最大の破棄レートの値を入力します。

「Apply」ボタンをクリックして行った変更を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Reset Configuration」をクリックして指定エントリの再設定を行います。

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 機能の設定時にルータとエンドホストはネットワークの密集と送信遅延状態を示す「しるし」として使用します。

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。

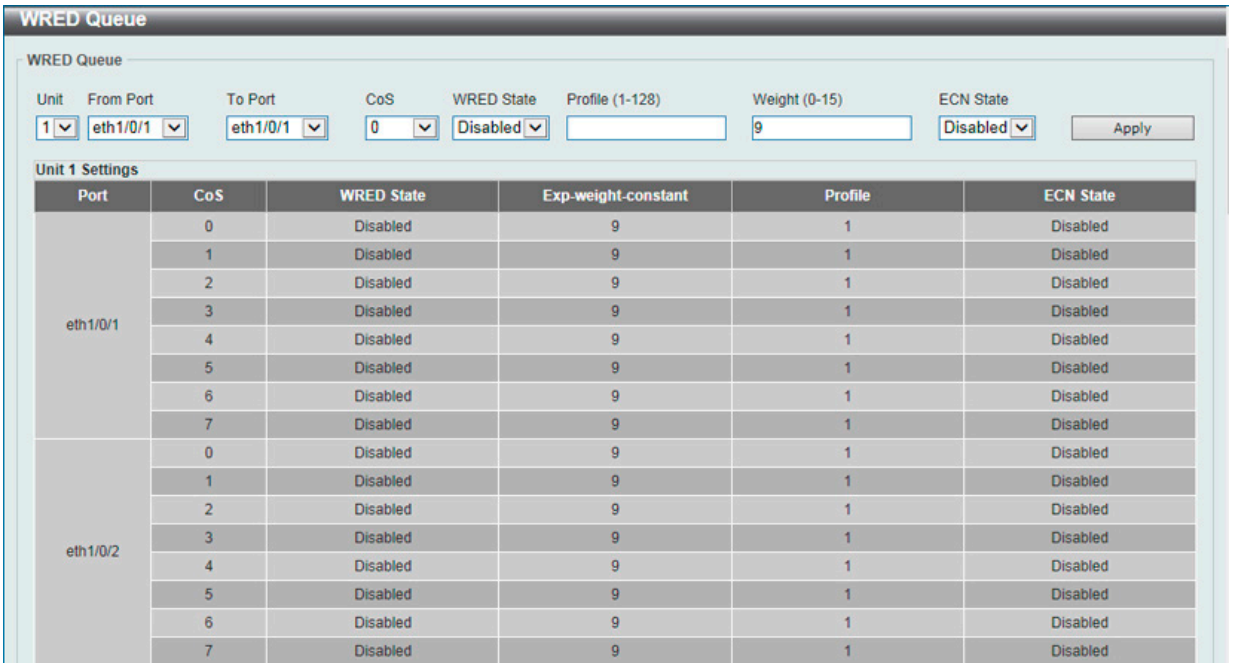


図 10-28 WRED Queue 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。
CoS	CoS 値（0-7）を指定します。
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。
Weight (0-15)	通常のキューサイズ計算における重み付け（0-15）を指定します。
ECN State	指定ポートの ECN 機能を有効 / 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。

WRED Drop Counter（WRED ドロップカウンタ設定）

WRED のドロップカウンタの設定、表示を行います。

QoS > WRED > WRED Drop 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 10-29 WRED Drop Counter 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。

「Clear」をクリックすると入力したエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。

iSCSI（アイスカジー）

QoS > iSCSI
iSCSI アウェアネスアプリケーションは iSCSI のフローの自動 QoS 優先対応で使用され、次の動作カテゴリに分類されます。:

- iSCSI セッションの構築と終了の検出と iSCSI プロトコルを使用したスヌーピングパケットによる接続
- 進行中の iSCSI セッションデータベースとストアデータ用接続の維持。これにより目的の QoS 対応セッションのデータパケット提供のルールを分類することができます。
- iSCSI セッショントラフィックに必要なルール群分類の導入と削除。
- セッション終了パケット未受信時のセッションエントリのエージアウトを許可する iSCSI セッションの動作確認。

iSCSI Settings（アイスカジー設定）

iSCSI の設定、表示を行います。

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

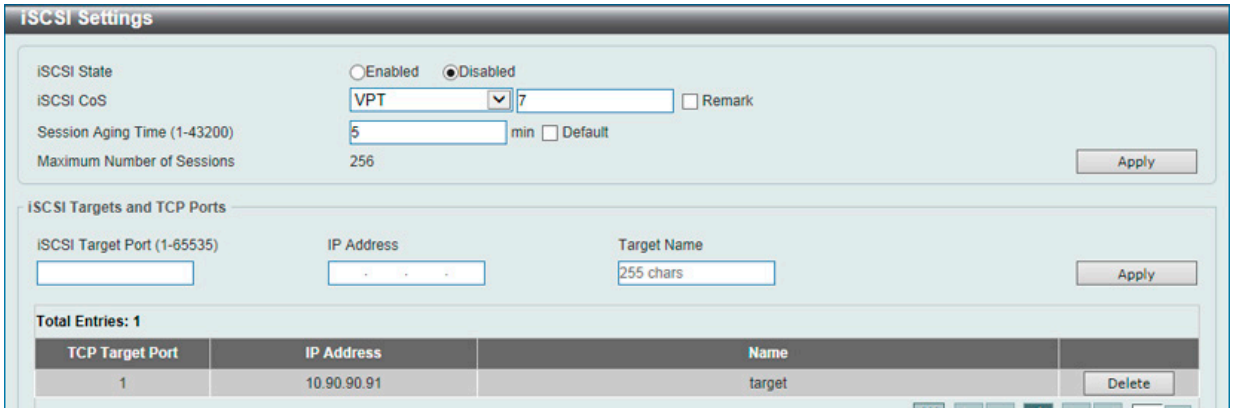


図 10-30 iSCSI Settings 画面

本画面には以下の項目があります。

項目	説明
iSCSI State	iSCSI アウェアネス機能を有効 / 無効に指定します。
iSCSI CoS	設定する iSCSI CoS を指定します。 • VPT - iSCSI セッションパケットをアサインする「VLAN Priority Tag」(VPT) を指定します。VPT 値を指定します。 • DSCP - iSCSI セッションパケットをアサインする「DSCP」を指定します。DSCP 値を指定します。 • Default - 初期値を使用します。初期値では VPT が「7」で使用されます。 イーグレス時に VPT または DSCP の iSCSI フレームをマークする「Remark」を指定します。
Session Aging Time	セッションエージング時間（1-43200/ 分）を指定します。iSCSI セッションのエージング時間に使用します。現在の設定よりもエージング時間を長くする場合、現在のセッションはタイムアウトされ、新しいエージング時間が採用されます。現在の設定よりもエージング時間を短くする場合、新しいエージング時間よりも長い現セッションは削除され、新しいエージング時間よりも短い、または同じ現セッションは続行され、新しいエージング時間が採用されます。「Default」を指定すると初期値（5 分）を使用します。

「Apply」をクリックし、設定内容を適用します。

「iSCSI Targets and TCP Ports」には以下の項目があります。

項目	説明
iSCSI Target Port	iSCSI ターゲットポート番号（1-65535）を指定します。
IP Address	iSCSI ターゲットの IP アドレスを指定します。
Target Name	iSCSI ターゲット名を指定します。文字列は 255 字まで指定可能す。手動での設定の他に、「iSNS」または「sendTargets」の応答から取得可能です。イニシエータは「iSCSI Initiator Name」と「iSCSI ターゲット名」を最初のセッション / 接続時にログインリクエストとして表示します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

iSCSI Sessions（アイスカジーセッション）

iSCSI のセッションを表示します。

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



図 10-31　iSCSI Sessions 画面

第 11 章　ACL（ACL 機能の設定）

ACL メニューを使用し、本スイッチにアクセスプロファイルおよびルールの設定を行うことができます。

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

サブメニュー	説明
ACL Configuration Wizard（ACL 設定ウィザード）	ACL 設定ウィザードは、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 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。

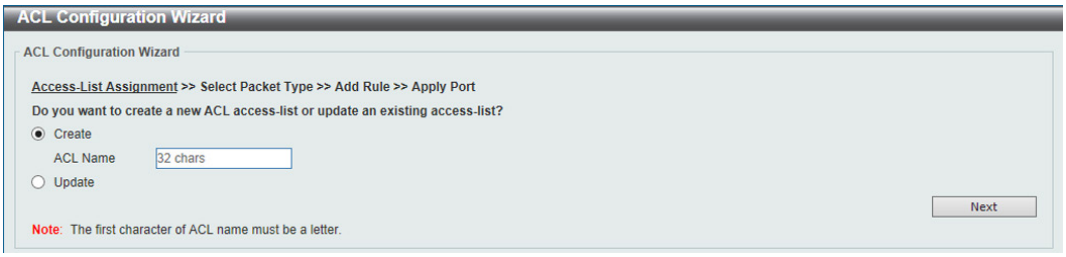


図 11-1　ACL Configuration Wizard（Create）画面

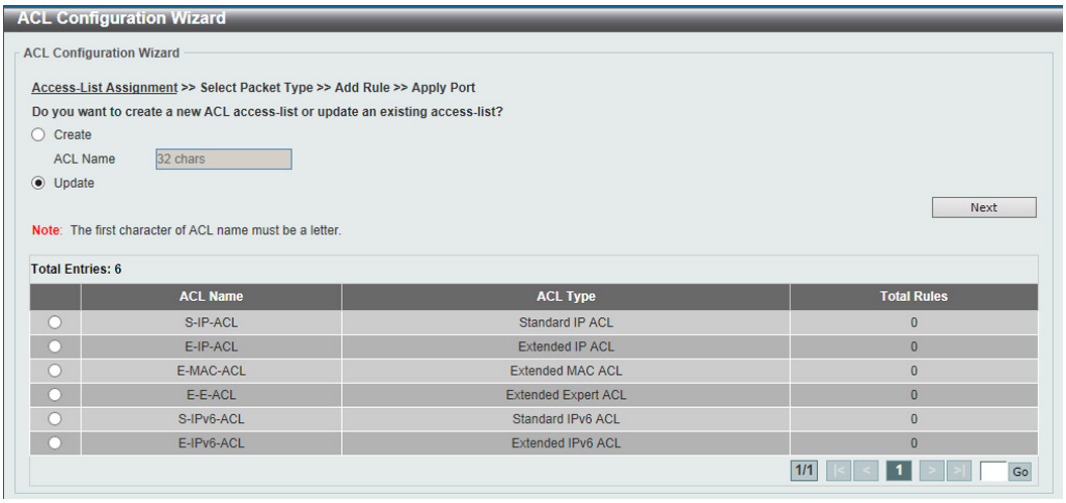


図 11-2　ACL Configuration Wizard（Update）画面

本画面には以下の項目があります。

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	ACL 名（32 字以内）を指定します。
Update	既存の ACL アクセスリストを表示し、エントリを再設定する場合に選択します。

「Next」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。

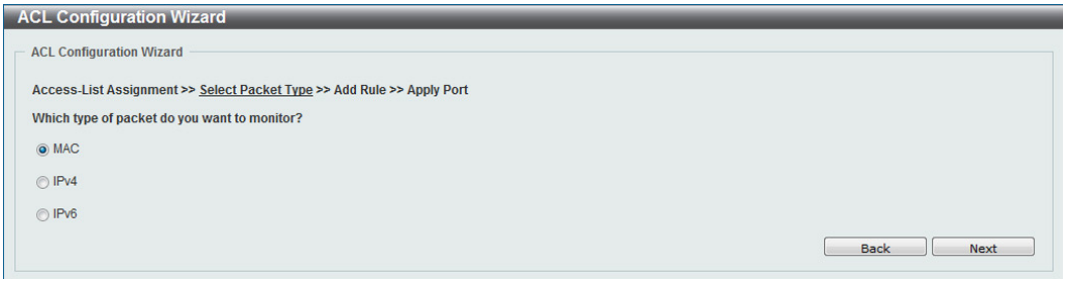


図 11-3　ACL Configuration Wizard (Select Packet Type) 画面

本画面には以下の項目があります。

項目	説明
MAC	MAC アドレスから送信されたパケットを対象に ACL を適用します。
IPv4	IPv4 アドレスから送信されたパケットを対象に ACL を適用します。

項目	説明
IPv6	IPv6 アドレスから送信されたパケットを対象に ACL を適用します。

「Next」をクリックします。選択したパケットの種類により次に表示される画面が違います。プロファイルの種類に合わせた設定方法に従い設定を行います。

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。「MAC」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

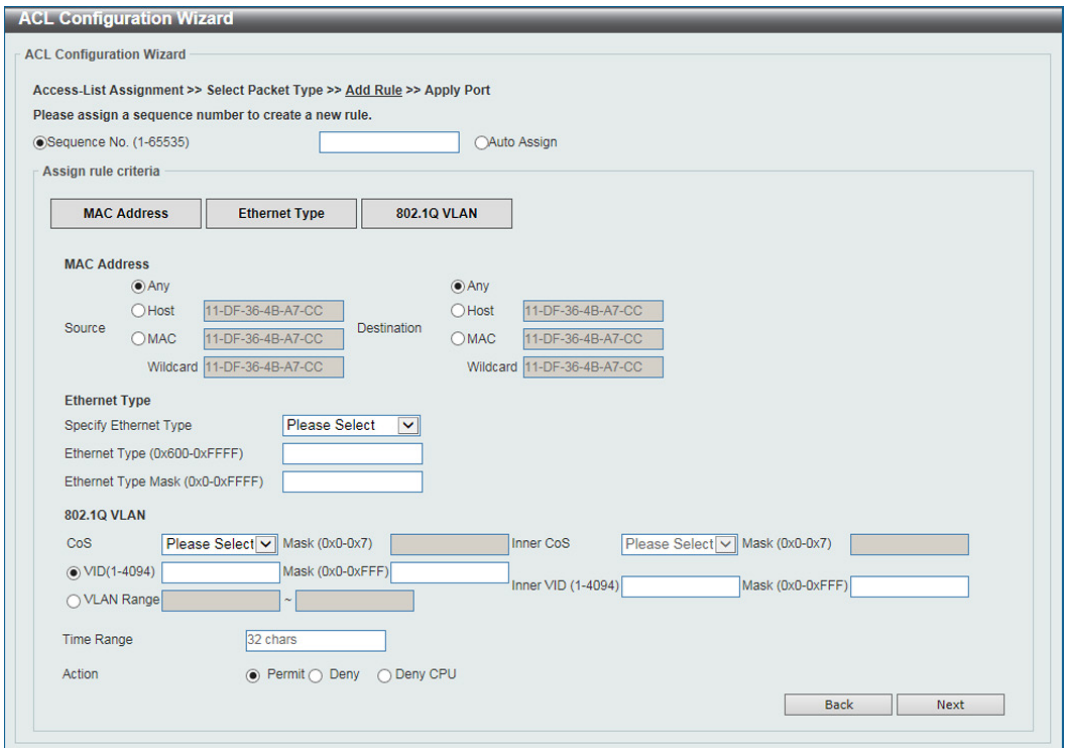


図 11-4　ACL Configuration Wizard - MAC ACL Rule 画面

画面に表示される項目

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign	新規ルール用のシーケンス番号を自動でアサインします。
Assign Rule Criteria（MAC アドレスの設定）	
Source	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「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」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「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。「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」から選択します。
Ethernet Type	イーサネットタイプの 16 進数値を指定します。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき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。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき適切な値が入力されます。
CoS	CoS の値を入力します。0 から 7 の間で入力できます。「Mask」にマスクを入力します。

項目	説明
Inner CoS	inner CoS の値を入力します。0 から 7 の間で入力できます。「Mask」にマスクを入力します。
VID	ACL ルールに関連する VLAN ID を入力します。1 から 4094 の間で入力可能です。「Mask」にマスクを入力します。
Inner VID	ACL ルールに関連する inner VLAN ID を入力します。1 から 4094 の間で入力可能です。「Mask」にマスクを入力します。
VLAN Range	ACL ルールに関連する VLAN 範囲を入力します。1 から 4094 の間で入力可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルールド動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。

「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。「IPv4」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

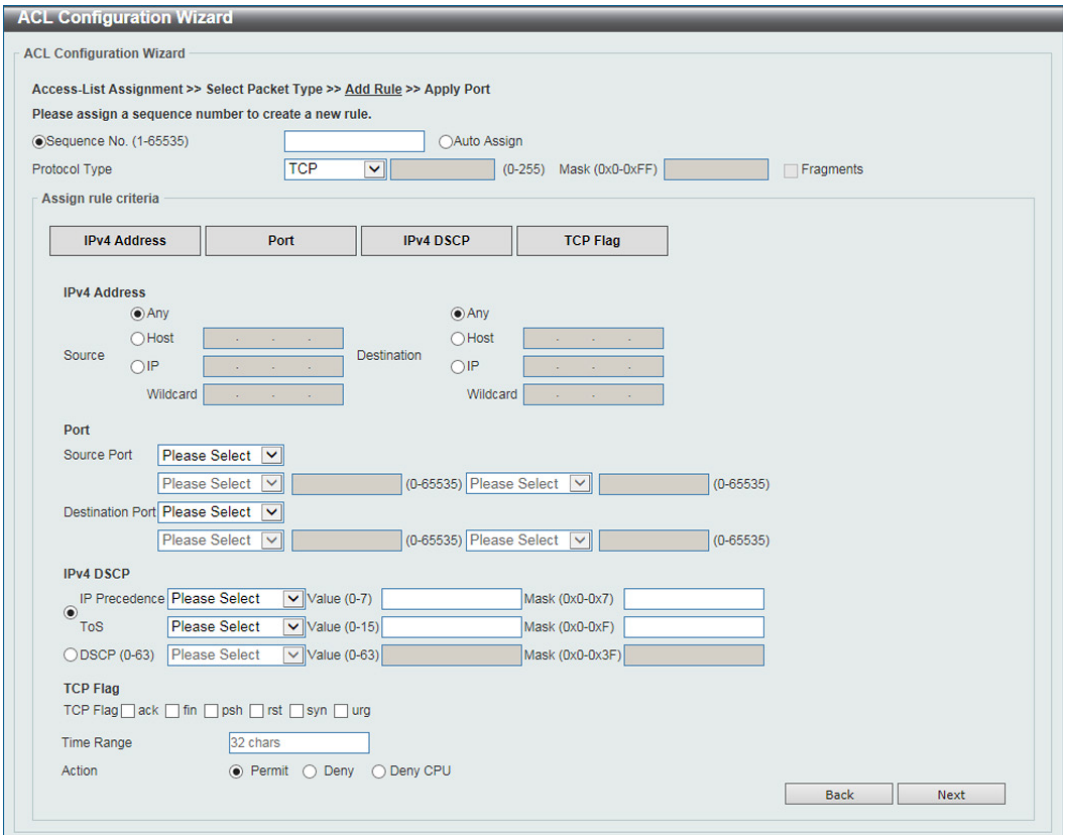


図 11-5　ACL Configuration Wizard -IPv4 画面

画面に表示される項目

項目	説明
Assign sequence number:（シーケンス番号の指定）	
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign	新規ルール用のシーケンス番号を自動でアサインします。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」から選択します。 • 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（IPv4 ACL Rule）

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。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」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。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。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。「Mask」にマスクを入力します。
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。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。「Mask」にマスクを入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」にマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルールド動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。

「TCP」選択時に表示される項目（IPv4 ACL Rule）

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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。
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。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。

「UDP」選択時に表示される項目（IPv4 ACL Rule）

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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。

「ICMP」選択時に表示される項目（IPv4 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。自動的に ICMP メッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目（IPv4 ACL Rule）

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。

「Next」をクリックします。

IPv6 ACL Rule の設定

IPv6 ACL Rule を設定します。「IPv6」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

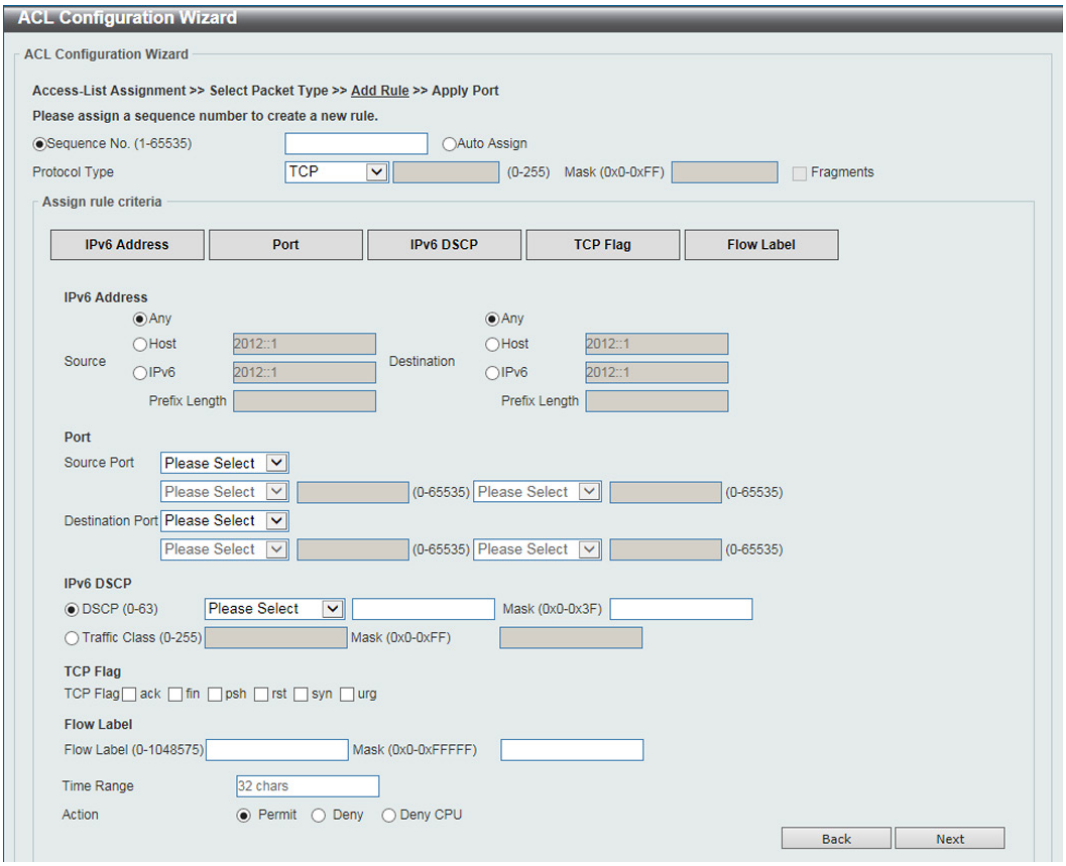


図 11-6　ACL Configuration Wizard -IPv6 画面

画面に表示される項目

項目	説明
Assign sequence number:（シーケンス番号の指定）	
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign	新規ルール用のシーケンス番号を自動でアサインします。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「ESP」「PCP」「Protocol ID」「SCTP」「None」から選択します。 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。 • 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。

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
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。

項目	説明
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」には適用するマスクを入力します。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。「Mask」には適用するマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルールド動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。

「TCP」選択時に表示される項目（IPv6 ACL Rule）

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。
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。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。

「UDP」選択時に表示される項目（IPv6 ACL Rule）

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。

「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。自動的に ICMP メッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

「ESP」「PCP」「Protocol ID」「SCTP」「None」選択時に表示される項目（IPv6 ACL Rule）

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。

「Next」をクリックします。

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。

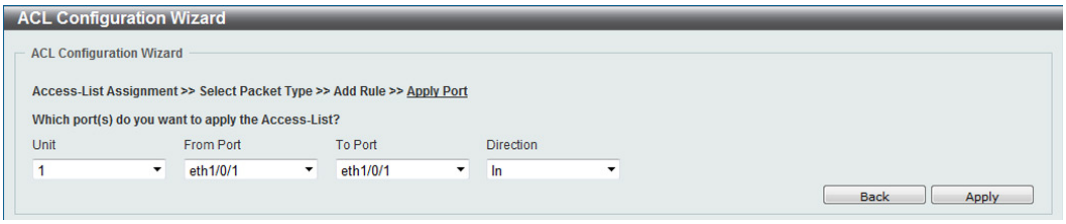


図 11-7　ACL Configuration Wizard (Apply Port) 画面

画面に表示される項目

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポート範囲を指定します。
Direction	方向を指定します。「In」「Out」が選択可能です。

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

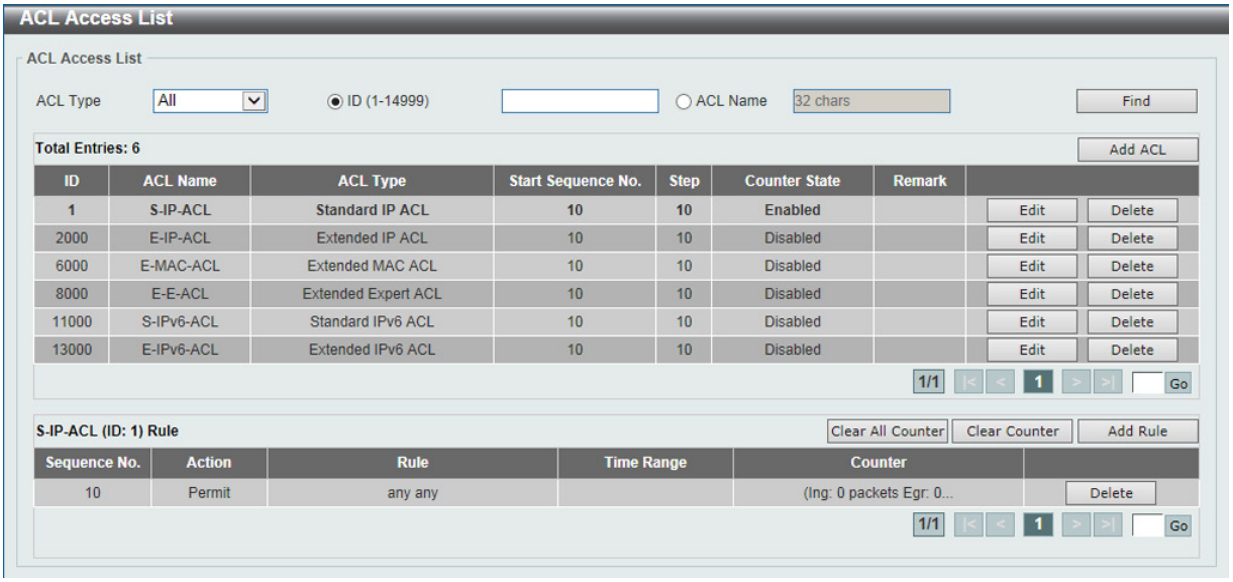


図 11-8　ACL Access List 画面

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。「All」「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ID	ACL ID を入力します。1 から 14999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Find」ボタンをクリックし、入力した情報を元に特定のエントリを指定します。
「Clear All Counter」ボタンをクリックし、表示されたすべてのカウンタ情報を消去します。
「Clear Counter」ボタンをクリックし、表示された指定ルールのカウンタ情報を消去します。
「Add Rule」ボタンをクリックし、ACL ルールを作成します。
「Add ACL」ボタンをクリックし、新しい ACL プロファイルを作成します。
「Edit」をクリックして、指定エントリの編集を行います。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Standard IP ACL（通常 IP ACL）

Standard IP ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

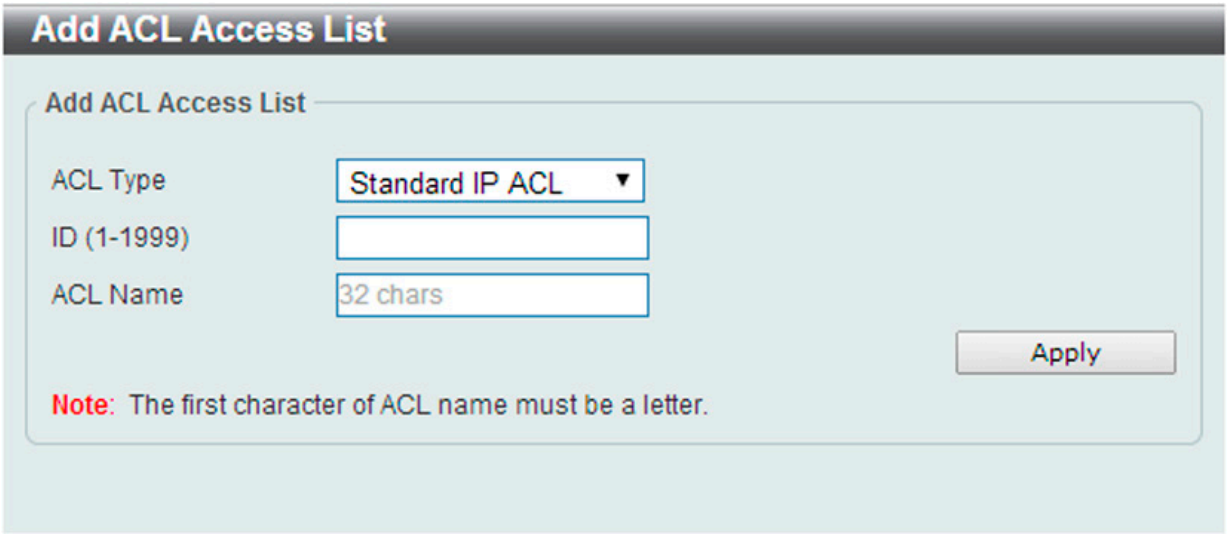


図 11-9　Standard IP ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。1 から 1999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

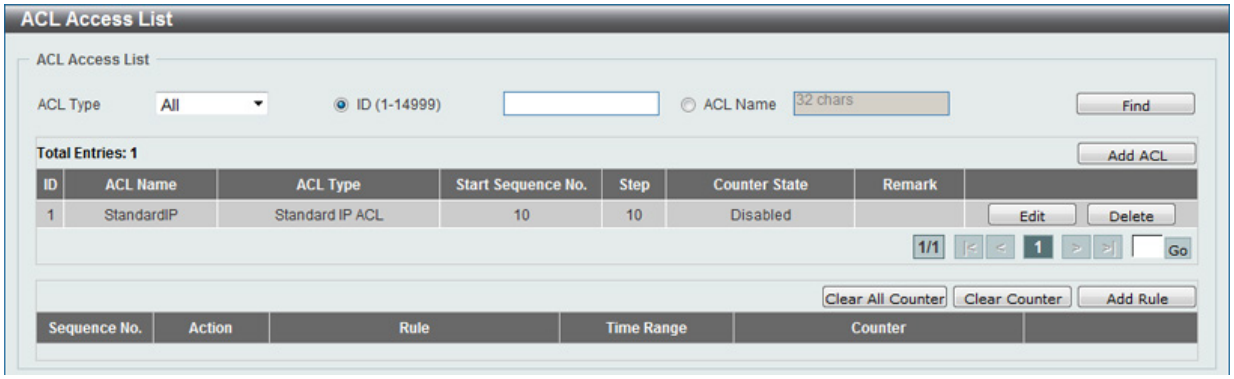


図 11-10　Standard IP ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
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。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Standard IP ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

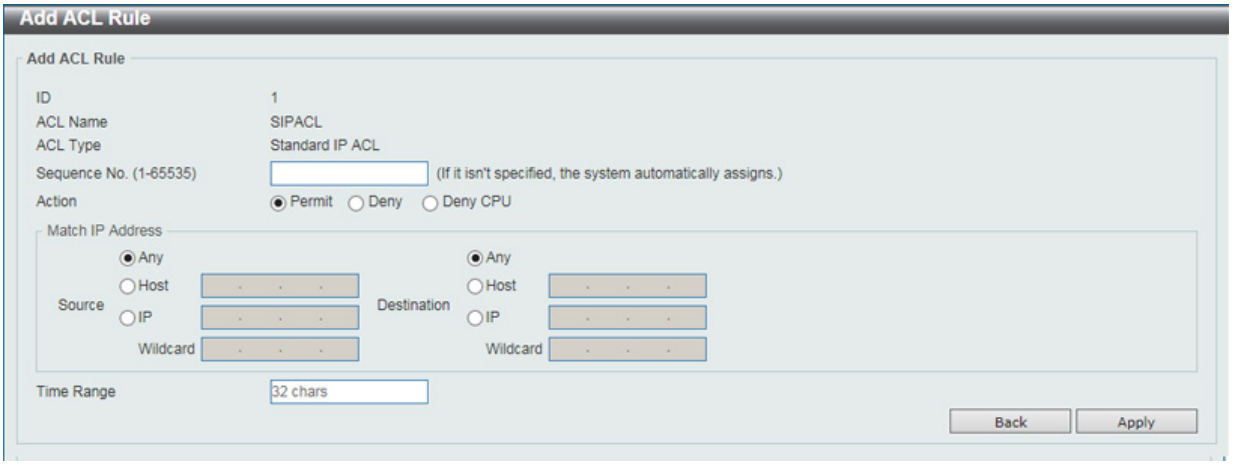


図 11-11　Standard IP ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。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」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「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。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Standard IP ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

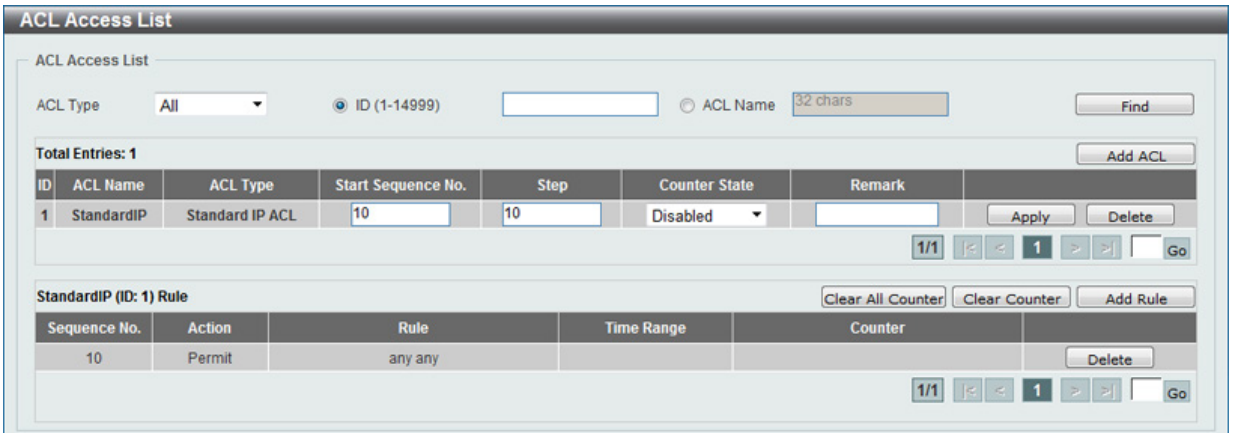


図 11-12　Standard IP ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

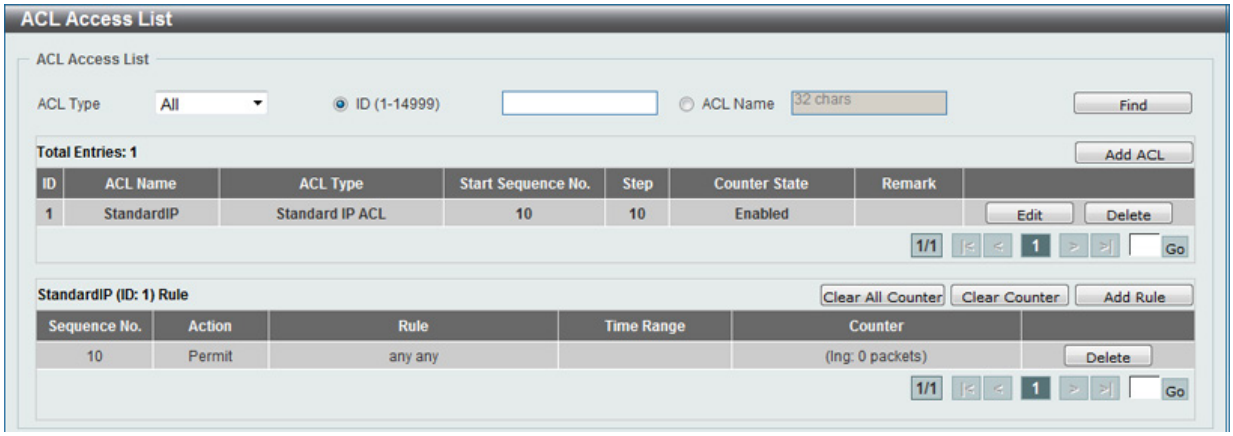


図 11-13 Standard IP ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。
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。

Extended IP ACL（拡張 IP ACL）

Extended IP ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

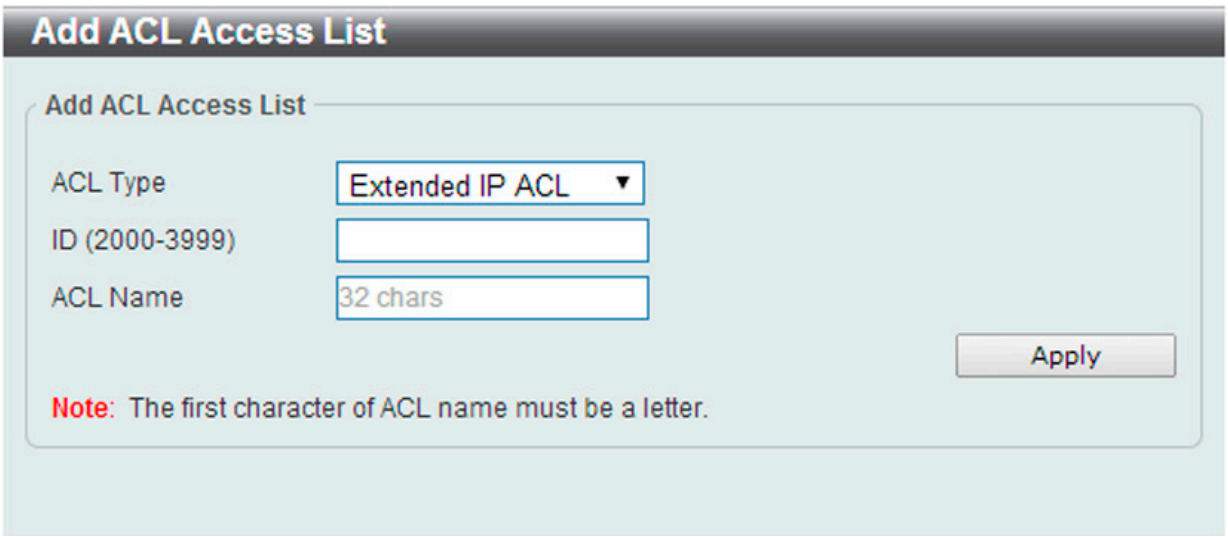


図 11-14 Extended IP ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。2000 から 3999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

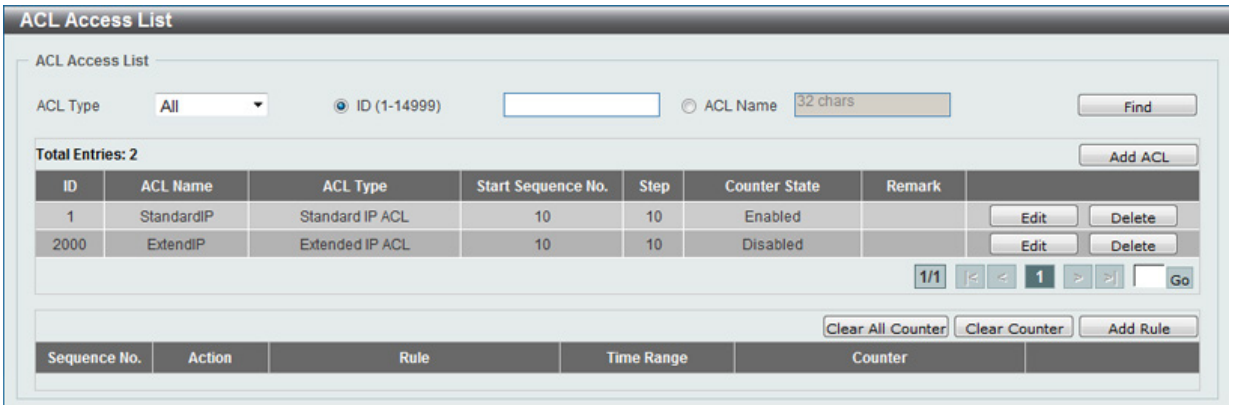


図 11-15　Extended IP ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
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。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended IP ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

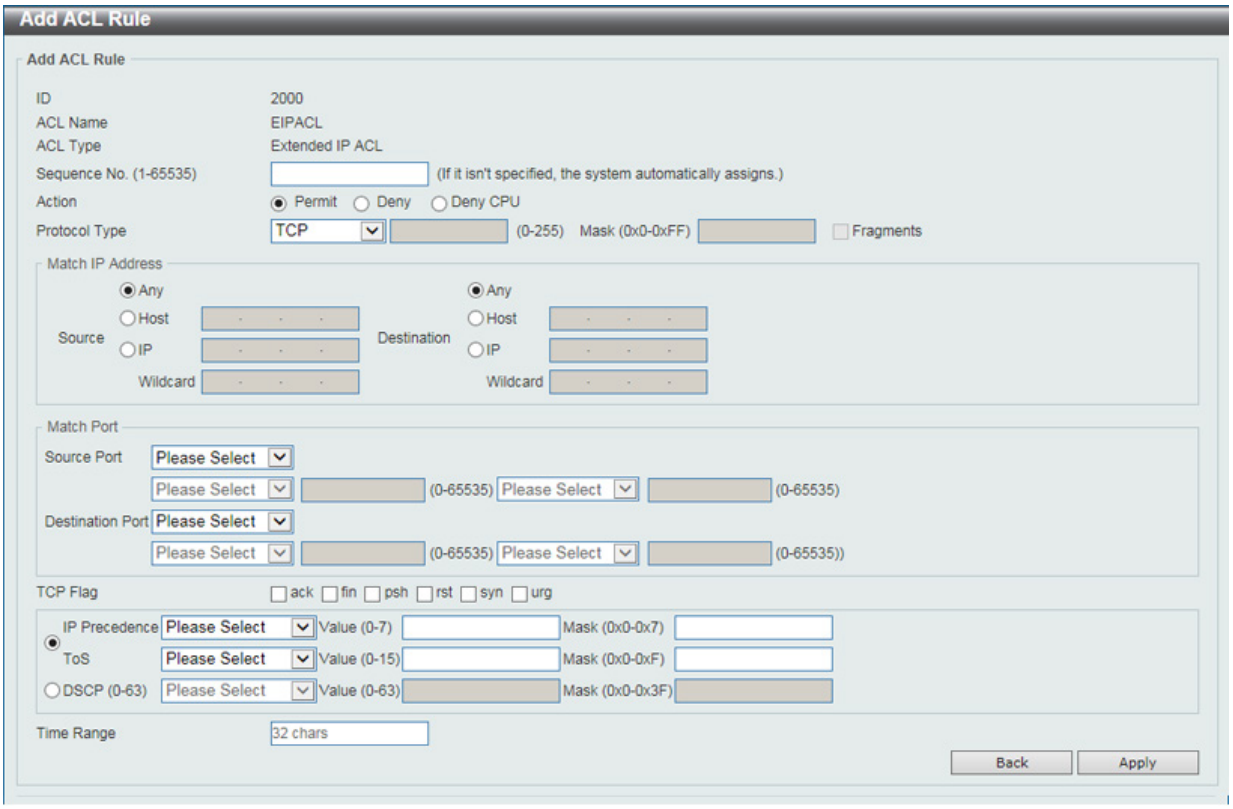


図 11-16　Extended IP ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Protocol Type	プロトコルの種類を選択します。「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」から選択します。 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。

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タイプに表示される項目（Extended IP ACL）

「Protocol Type」でどの項目を選択しても表示される項目です。（以下の画面は TCP 選択時のものです。）

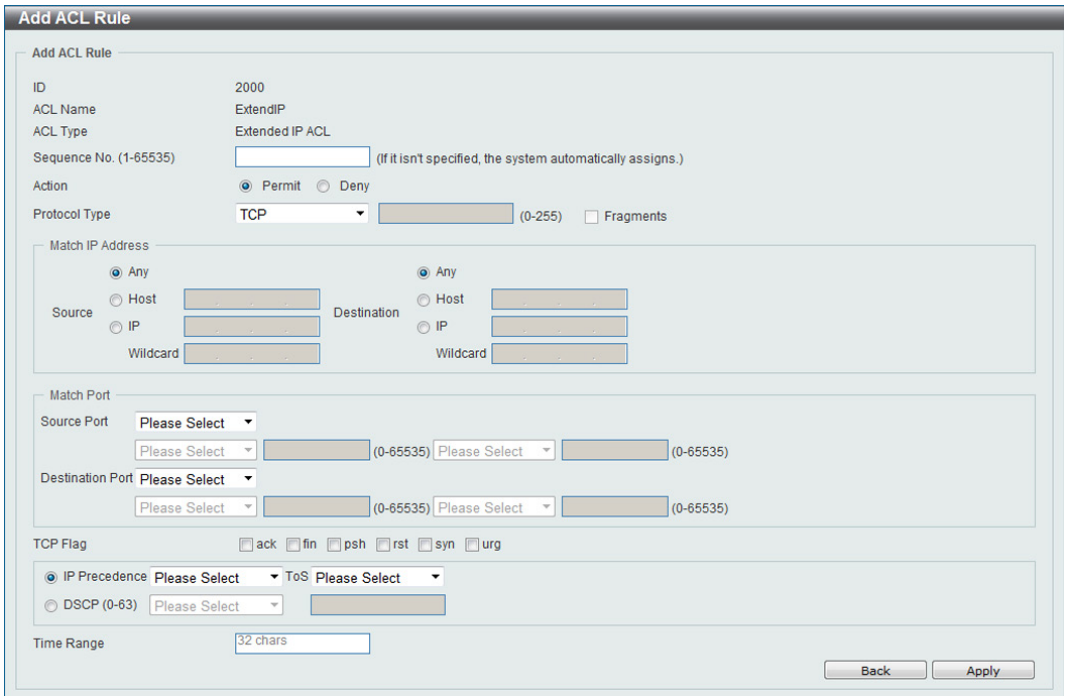


図 11-17　Extended IP ACL (Add Rule) TCP 画面

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」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。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」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。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。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。「Mask」には適用するマスクを入力します。
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。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」には適用するマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「TCP」選択時に表示される項目（Extended IP ACL）

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。
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。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。

「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選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。

「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。自動的に ICMP メッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目（Extended IP 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。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Extended IP ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

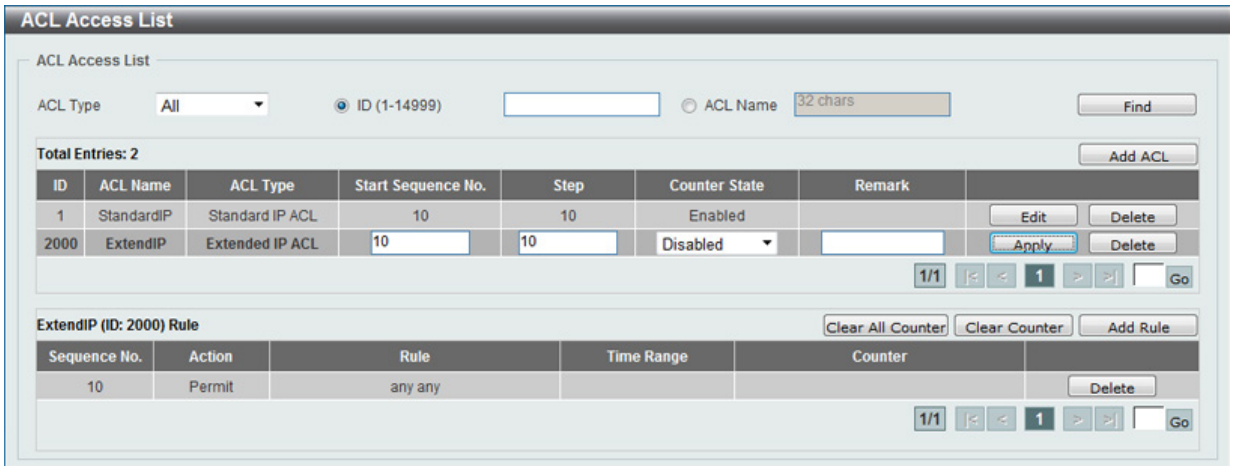


図 11-18 Extended IP ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

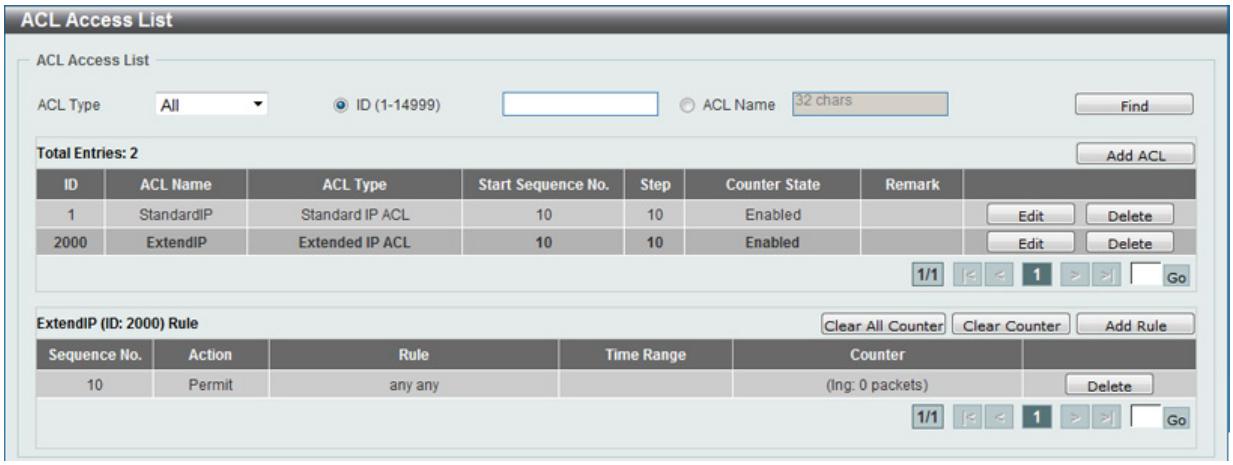


図 11-19 Extended IP ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。
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。

Standard IPv6 ACL（通常 IPv6 ACL）

Add ACL（Standard IPv6 ACL の作成）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

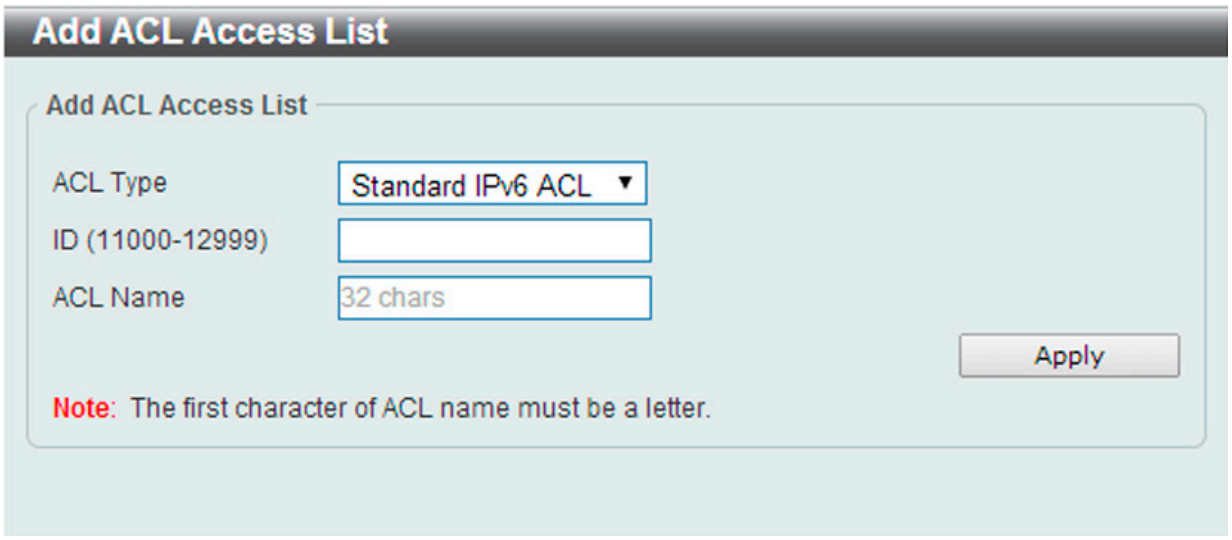


図 11-20 Standard IPv6 ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。11000 から 12999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

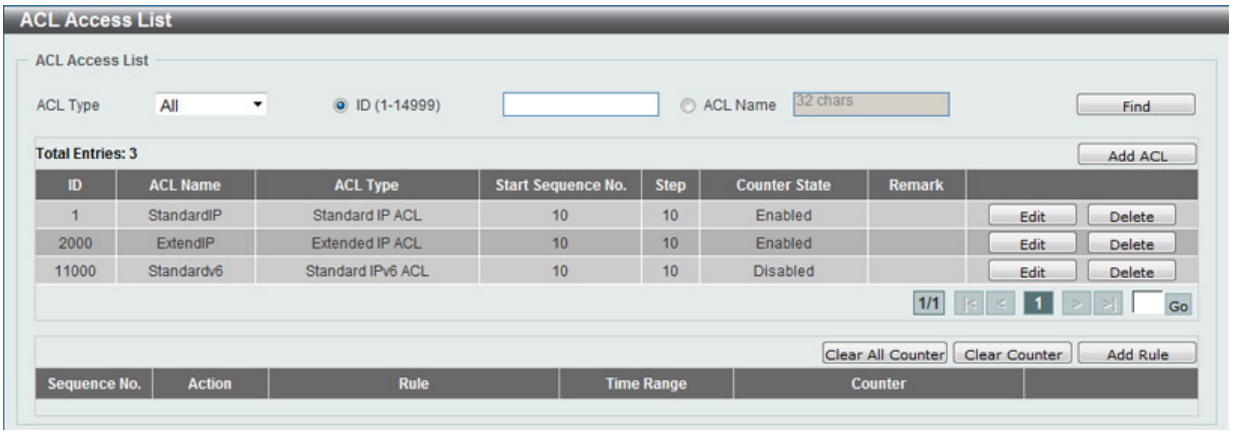


図 11-21 Standard IPv6 ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
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。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Standard IPv6 ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

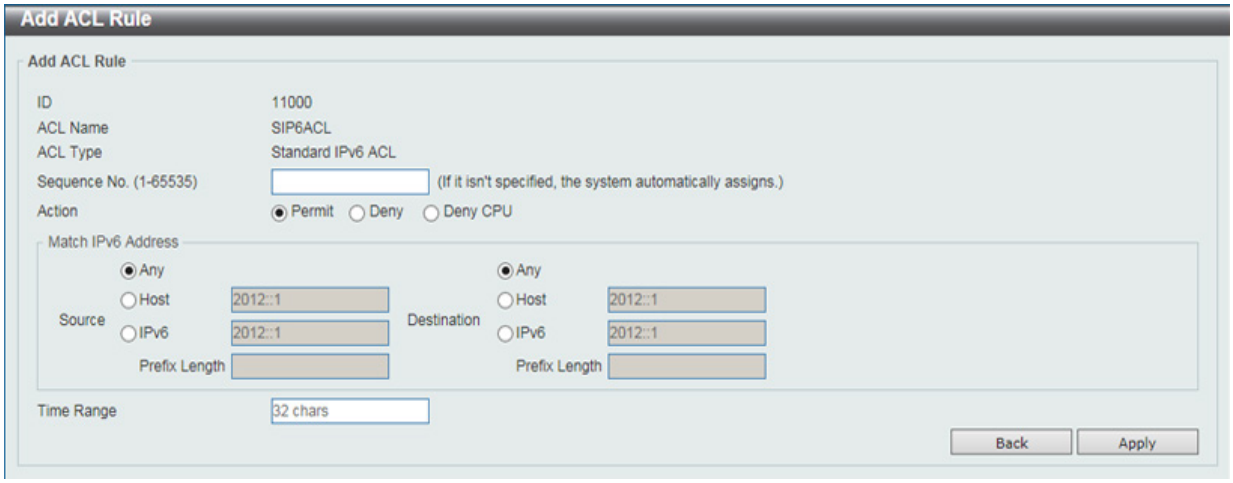


図 11-22 Standard IPv6 ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」オプションが選択可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」オプションが選択可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「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。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Standard IPv6 ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

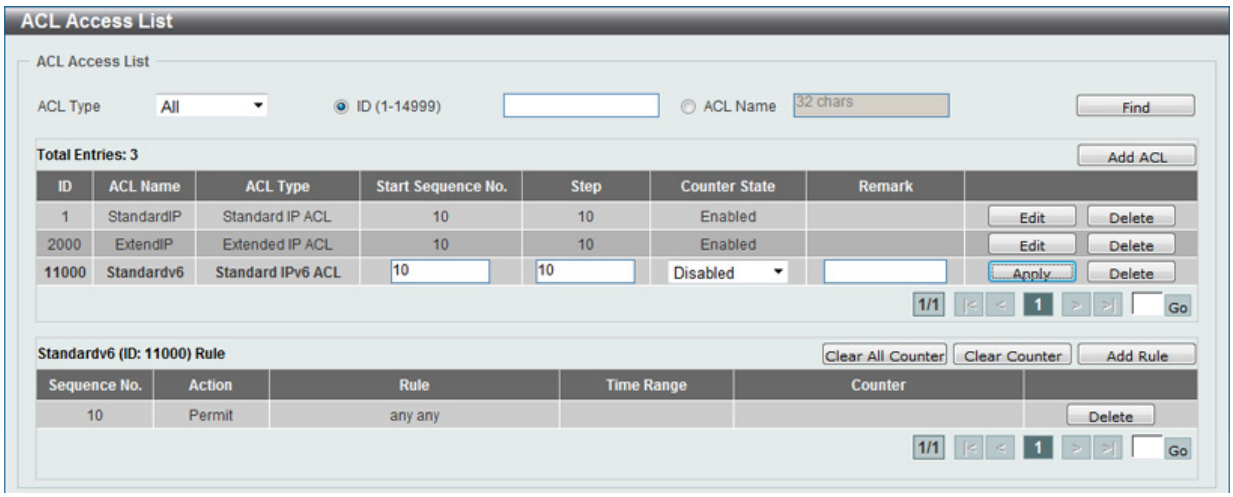


図 11-23 Standard IPv6 ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

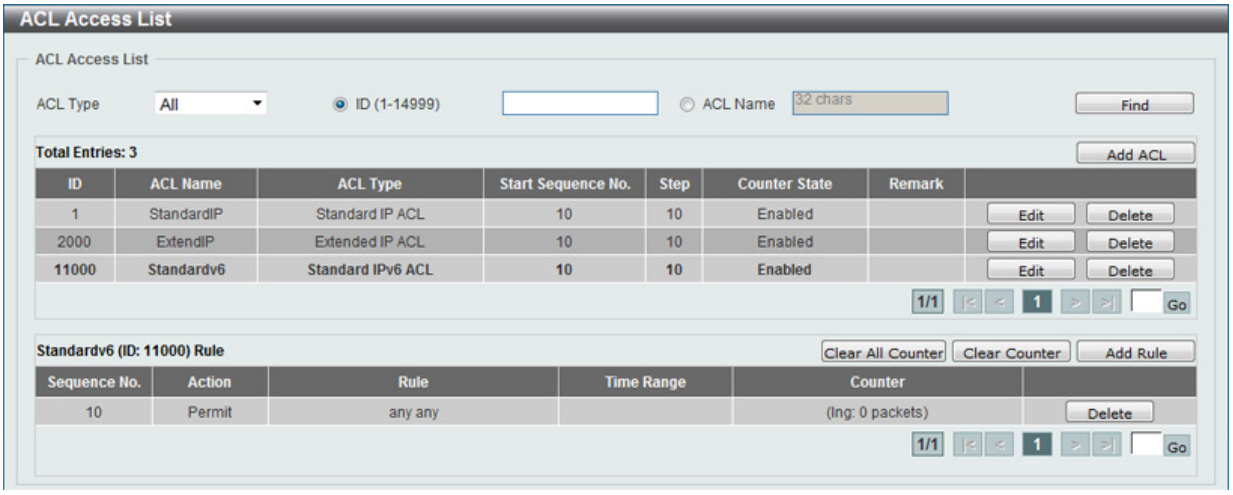


図 11-24　Standard IPv6 ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。
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。

Extended IPv6 ACL（拡張 IPv6 ACL）

Extended IPv6 ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

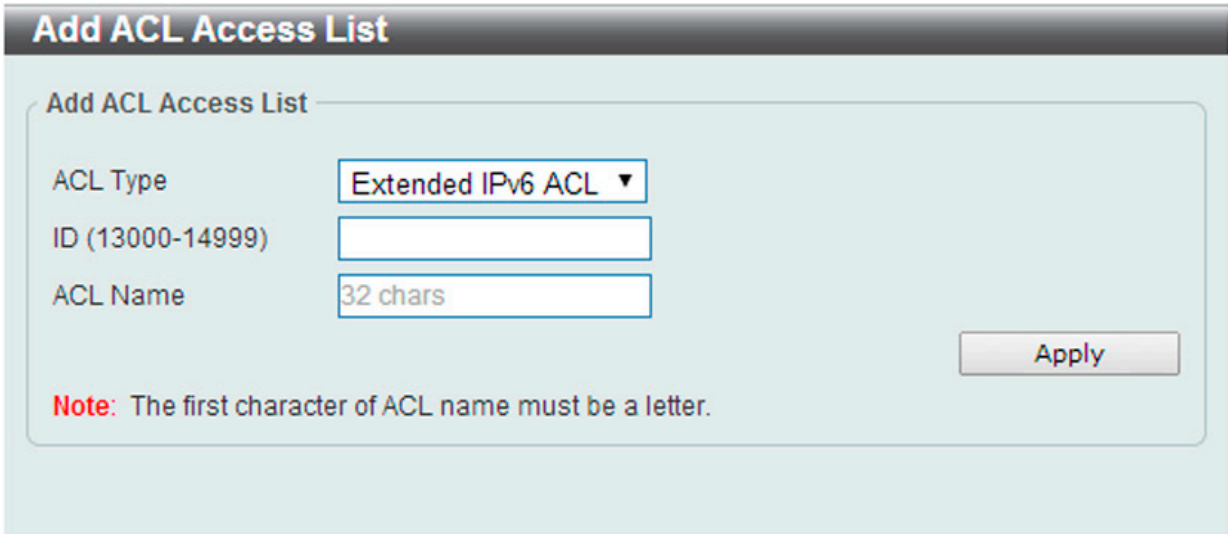


図 11-25　Extended IPv6 ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。

項目	説明
ID	ACL ID を入力します。13000 から 14999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

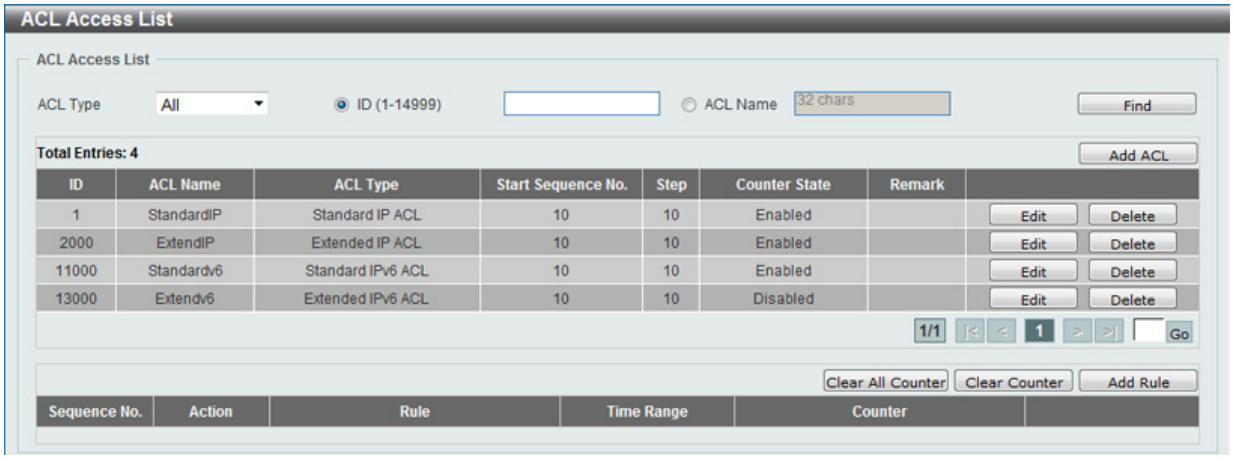


図 11-26 Extended IPv6 ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
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。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended IPv6 ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

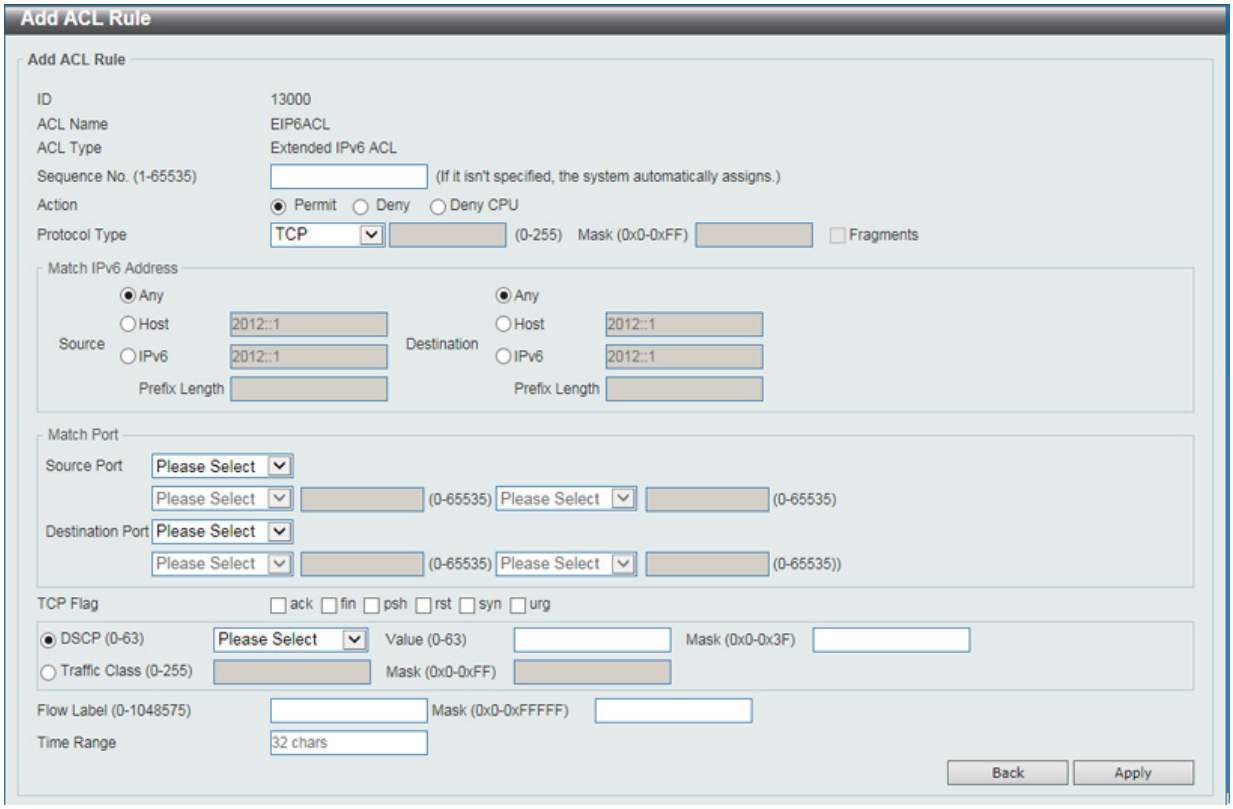


図 11-27 Extended IPv6 ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「ESP」「PCP」「Protocol ID」「SCTP」「None」から選択します。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。

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タイプに表示される項目（Extended IPv6 ACL）

「Protocol Type」でどの項目を選択しても表示される項目です。（以下の画面は TCP 選択時のものです。）

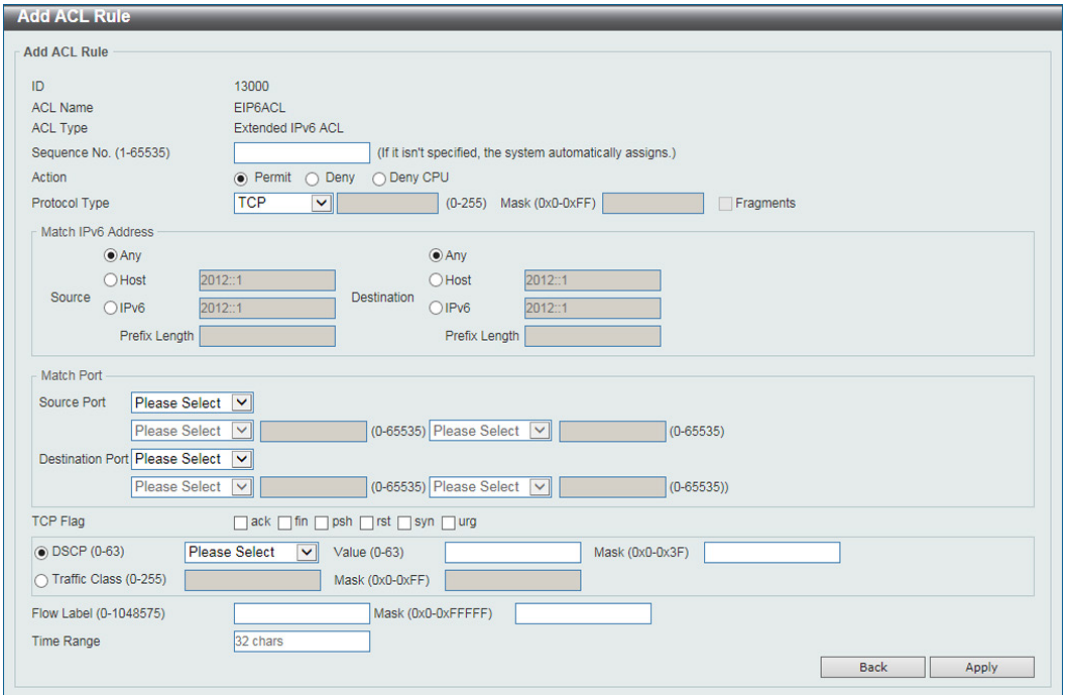


図 11-28　Extended IPv6 ACL (Add Rule) TCP 画面

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」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」には適用するマスクを入力します。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。「Mask」には適用するマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「TCP」選択時に表示される項目（Extended IPv6 ACL）

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。

項目	説明
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。
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。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。

「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選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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」には適用するマスクを入力します。

「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。自動的に ICMP メッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

「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。

「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。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Extended IPv6 ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

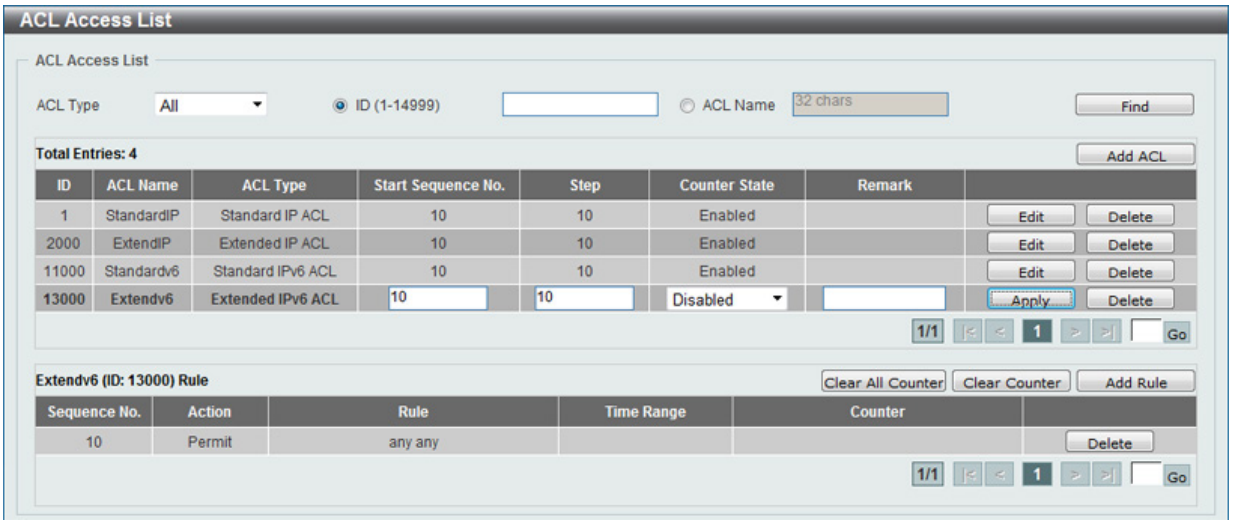


図 11-29　Extended IPv6 ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

Extended MAC ACL（拡張 MAC ACL）

Extended MAC ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

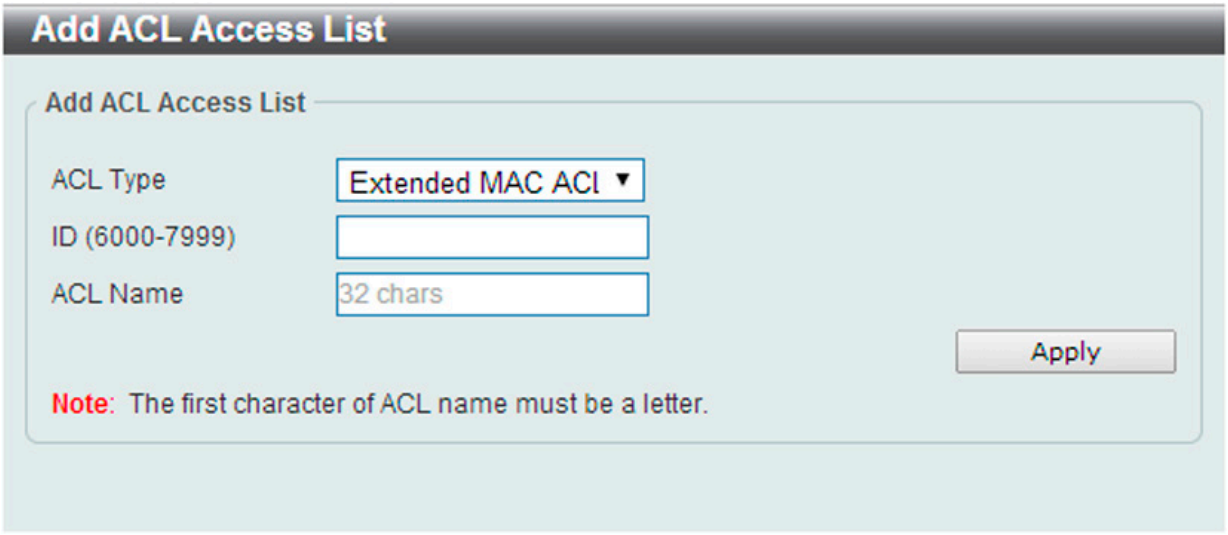


図 11-30 Extended MAC ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。6000 から 7999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

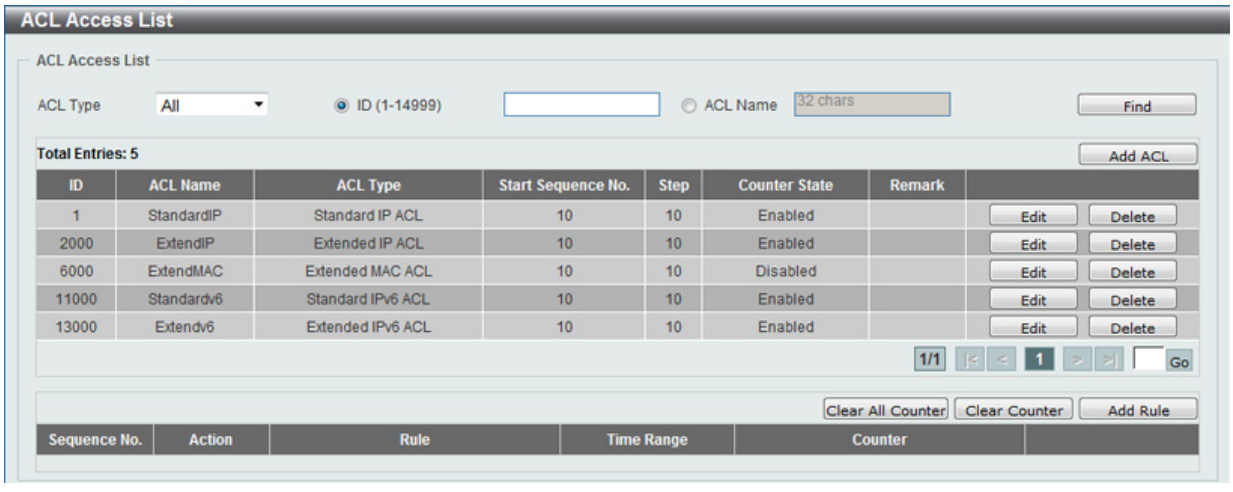


図 11-31 Extended MAC ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
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。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended MAC ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

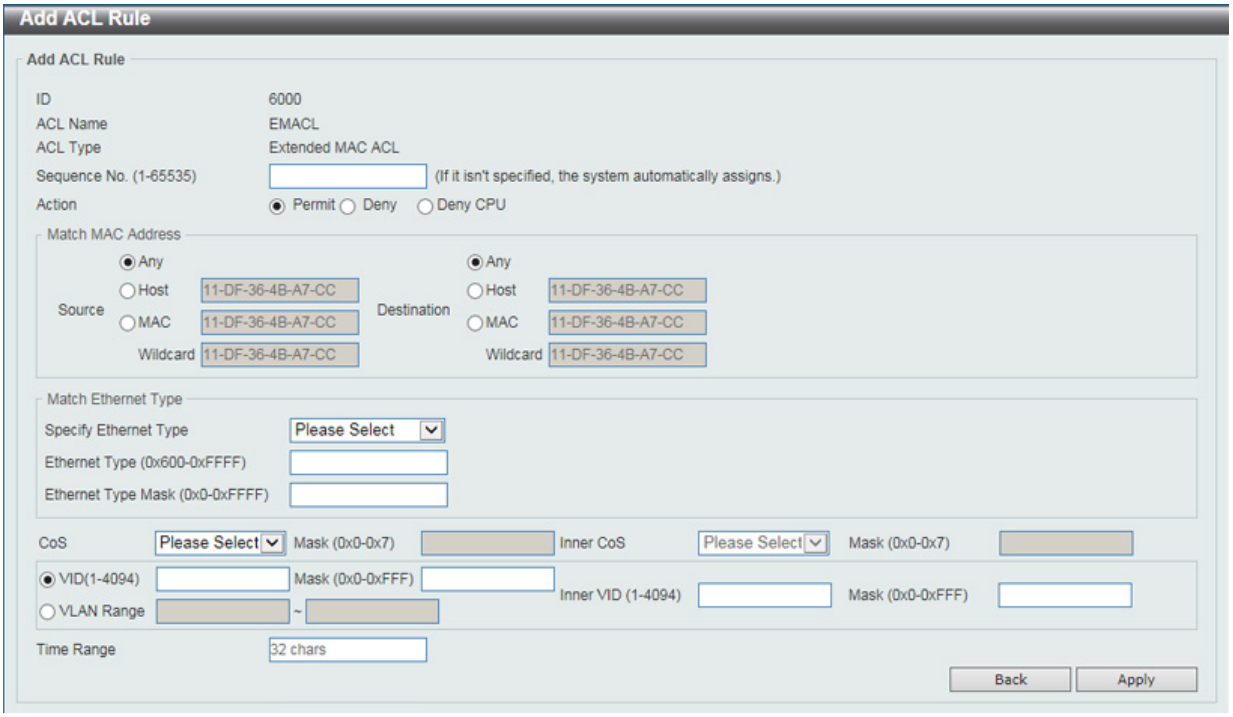


図 11-32　Extended MAC ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535):	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Source:	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「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」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「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。「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」から選択します。
Ethernet Type	イーサネットタイプの 16 進数値を指定します。0x600 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき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。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき適切な値が入力されます。
CoS	CoS の値を入力します。0 から 7 の間で入力できます。「Mask」には適用するマスクを入力します。
Inner CoS	Inner CoS の値を入力します。0 から 7 の間で入力できます。「Mask」には適用するマスクを入力します。
VID	ACL ルールに関連する VLAN ID を入力します。1 から 4094 の間で入力可能です。「Mask」には適用するマスクを入力します。
Inner VID	ACL ルールに関連する Inner VID を入力します。1 から 4094 の間で入力可能です。「Mask」には適用するマスクを入力します。
VLAN Range	ACL ルールに関連す VLAN 範囲を入力します。1 から 4094 の間で入力可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「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。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Extended MAC ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

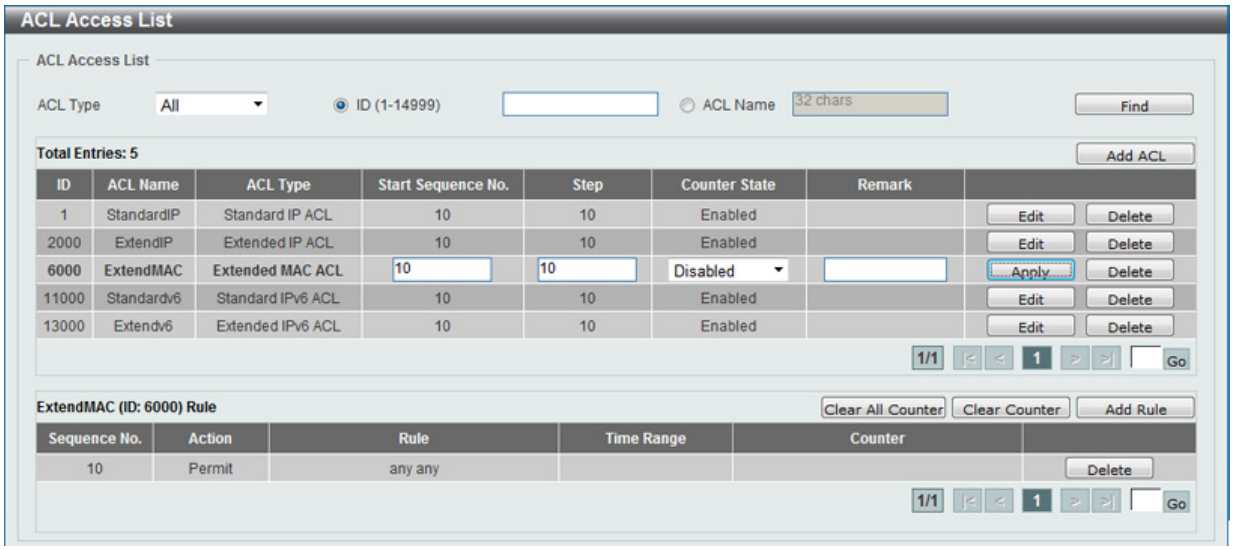


図 11-33 Extended MAC ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

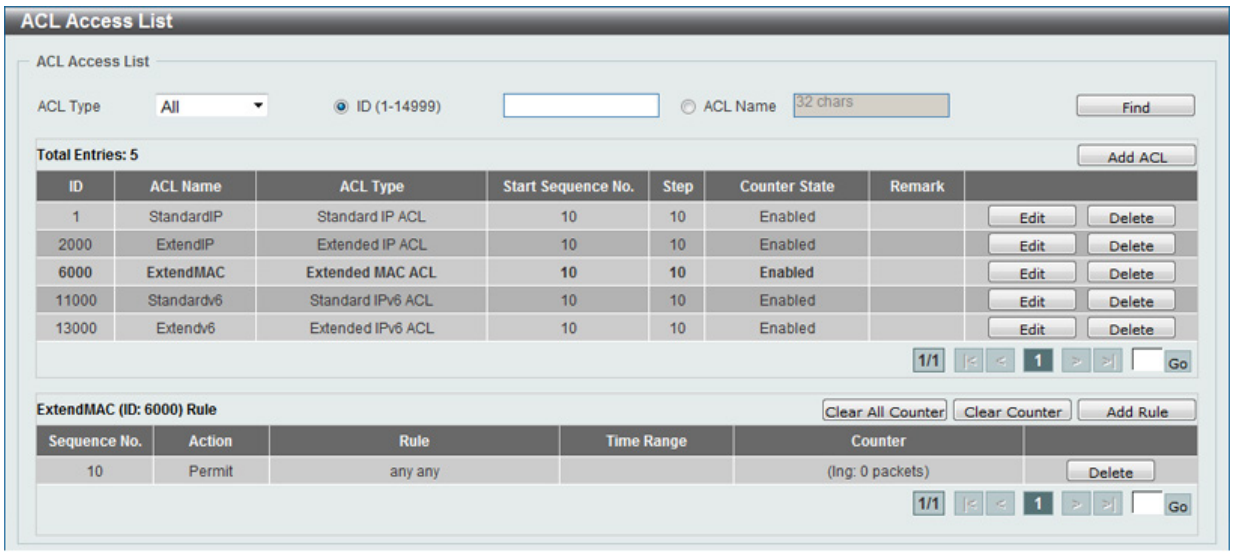


図 11-34 Extended MAC ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。
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。

Extended Expert ACL（拡張詳細 ACL）

Extended Expert ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

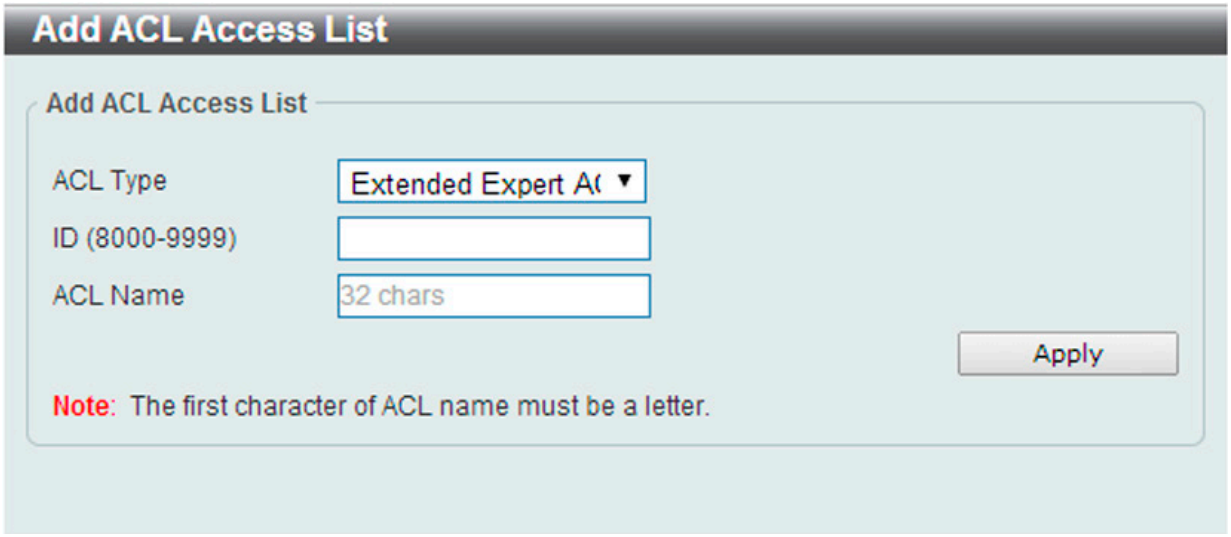


図 11-35 Extended Expert ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。8000 から 9999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

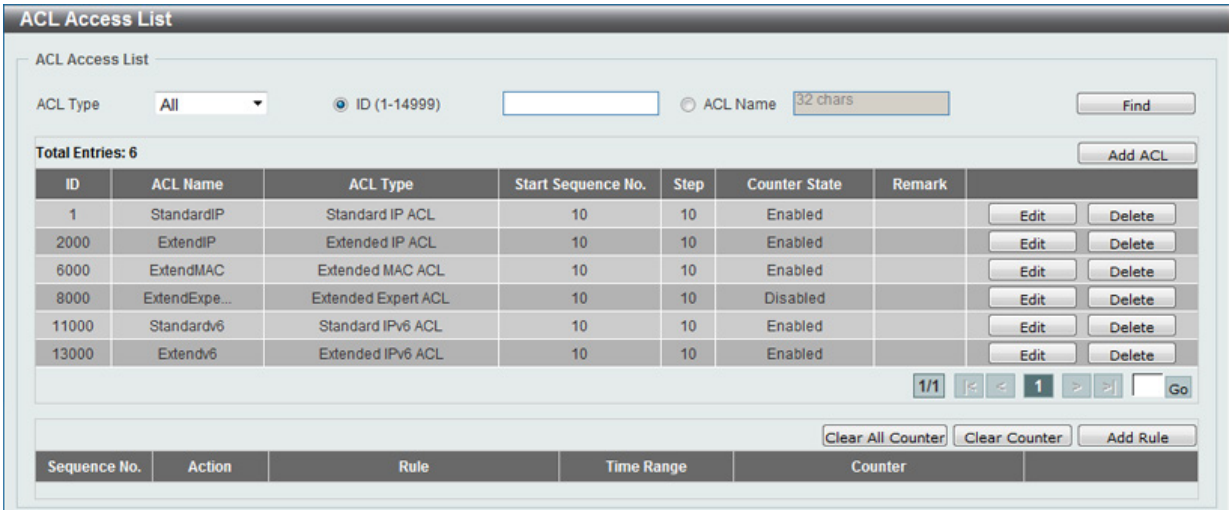


図 11-36 Extended Expert ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
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。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended Expert ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

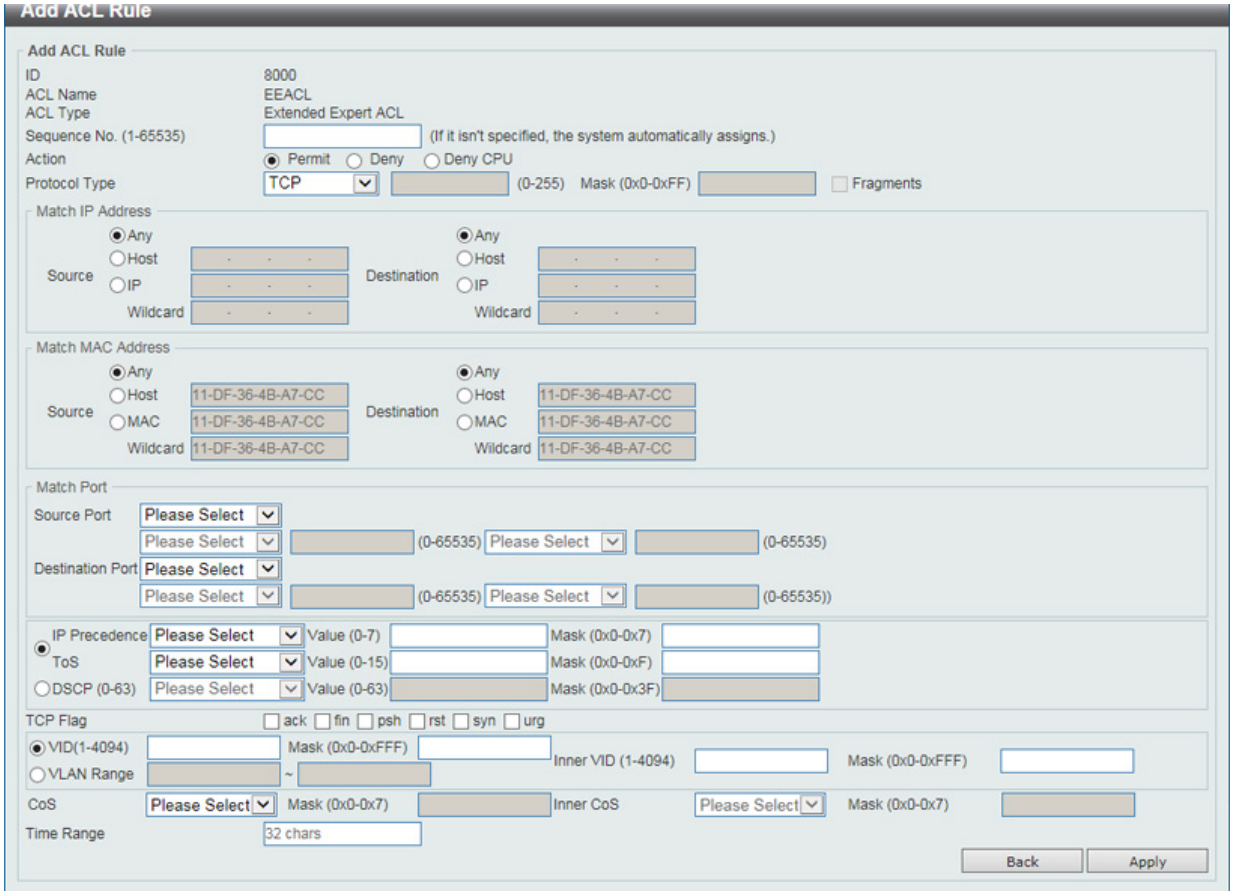


図 11-37　Extended Expert ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」「Deny CPU」から指定できます。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」から選択します。 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。

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タイプに表示される項目（Extended Expert ACL）

「Protocol Type」でどの項目を選択しても表示される項目です。（以下の画面は TCP 選択時のものです。）

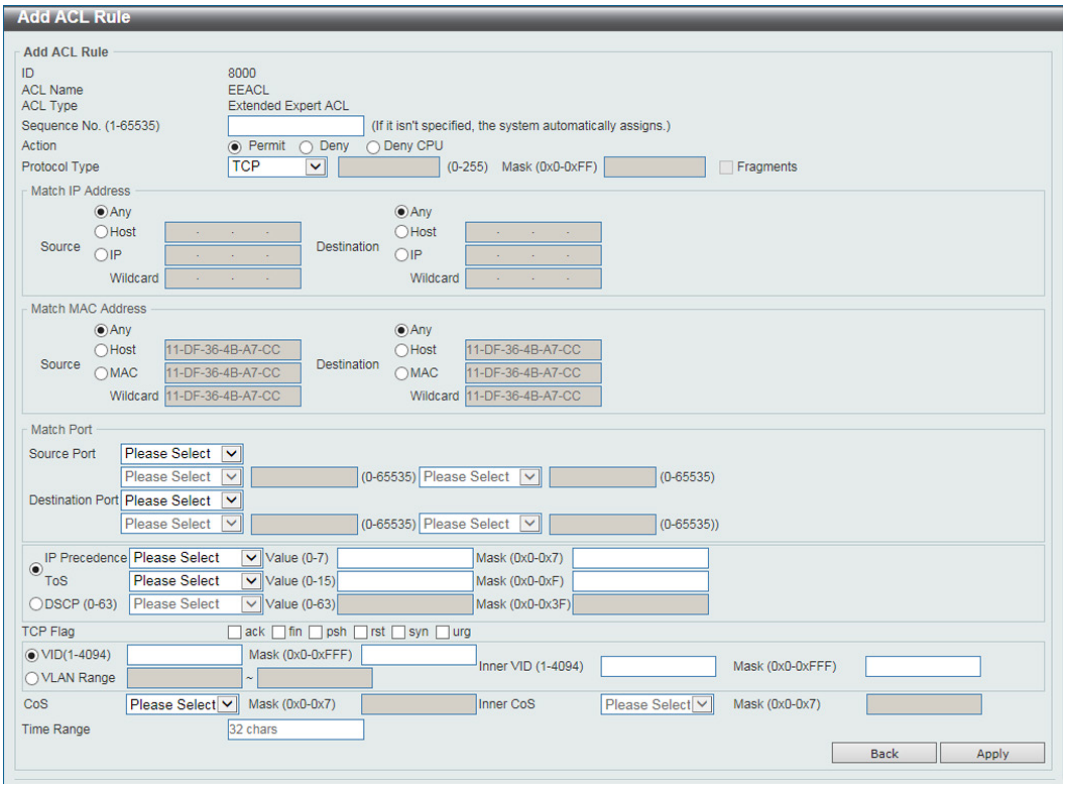


図 11-38　Extended Expert ACL (Add Rule) TCP 画面

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
Source IP Address	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination IP Address	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Source MAC Address	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「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 MAC Address	宛先の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「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。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。「Mask」には適用するマスクを入力します。
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。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。「Mask」には適用するマスクを入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。「Mask」には適用するマスクを入力します。
CoS	CoS の値を入力します。0 から 7 の間で入力できます。「Mask」には適用するマスクを入力します。
Inner CoS	Inner CoS の値を入力します。0 から 7 の間で入力できます。「Mask」には適用するマスクを入力します。
VID	ACL ルールに関連する VLAN ID を入力します。1 から 4094 の間で入力可能です。「Mask」には適用するマスクを入力します。

項目	説明
Inner VID	ACL ルールに関連する Inner VID を入力します。1 から 4094 の間で入力可能です。「Mask」には適用するマスクを入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「TCP」選択時に表示される項目（Extended Expert ACL）

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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。
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。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。

「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選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると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。

「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。自動的に ICMP メッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。

「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目（Extended Expert 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。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Extended Expert ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

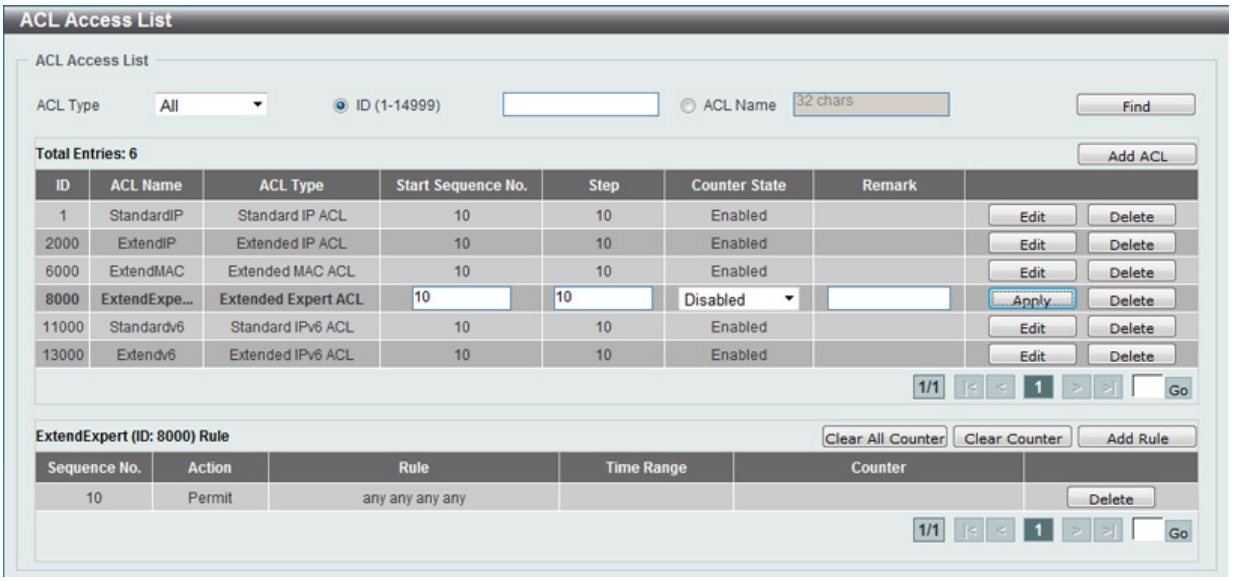


図 11-39 Extended Expert ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

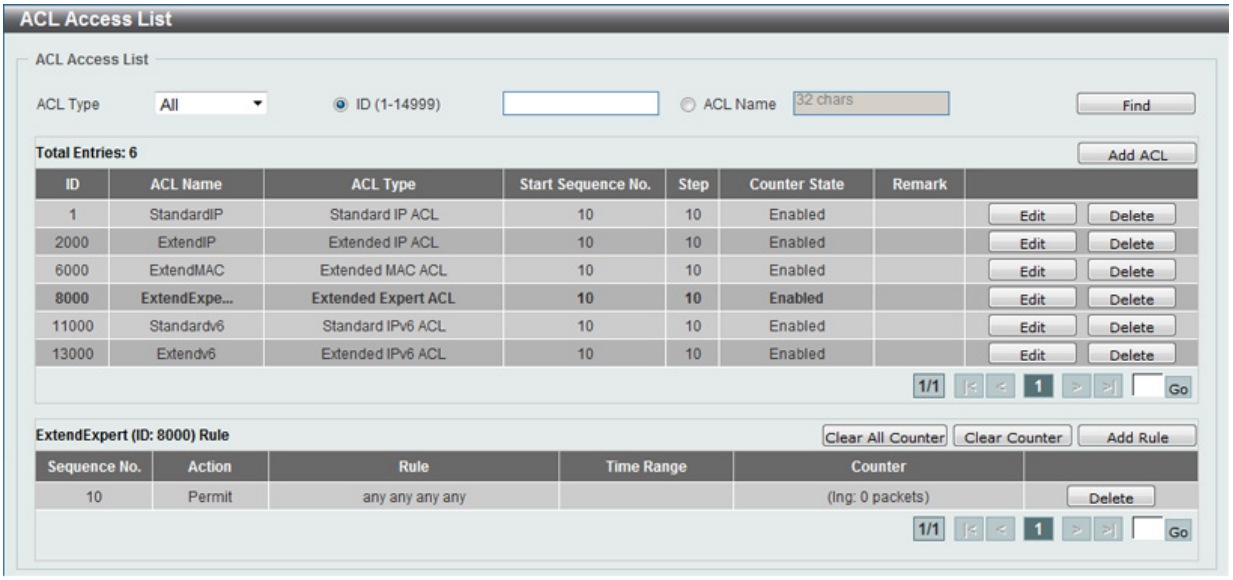


図 11-40 Extended Expert ACL (Rule Display) 画面

「Delete」ボタンをクリックして、指定ルールを削除します。
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。

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。

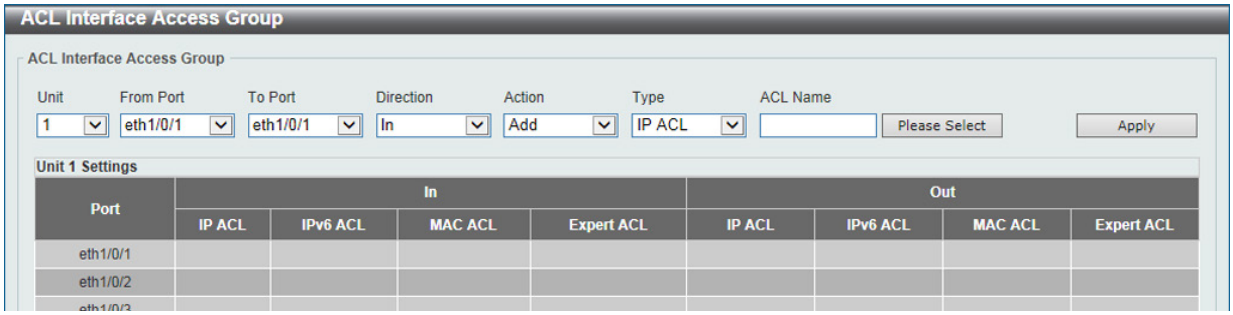


図 11-41　ACL Interface Access Group 画面

画面に表示される項目

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
Direction	方向を指定します。「In」が選択可能です。
Action	ACL インタフェースアクセスグループの追加 / 削除をします。「Add」「Delete」から選択します。
Type	ACL の種類を選択します。「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL Name	ACL 名を入力します。32 文字以内で入力できます。

「Please Select」ボタンをクリックし、作成した ACL プロファイルを選択します。
「Apply」ボタンをクリックして、設定を適用します。

「Please Select」ボタンをクリックすると次の画面が表示されます。



図 11-42　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。

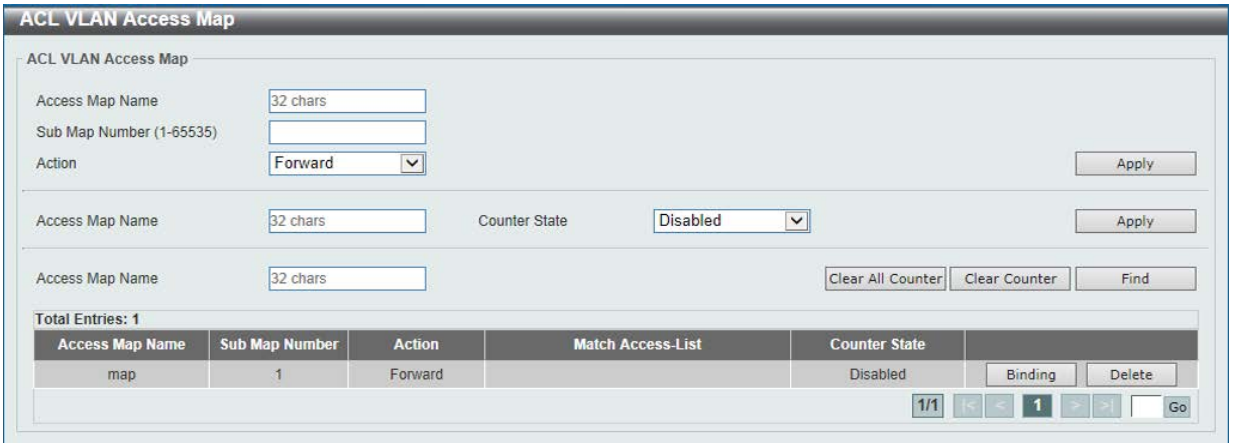


図 11-43　ACL VLAN Access Map 画面

画面に表示される項目

項目	説明
Access Map Name	アクセスマップ名を入力します。32 文字以内で入力できます。
Sub Map Number	サイトマップ番号を入力します。1 から 65535 までで指定できます。
Action	本項目の動作を指定します。「Forward」「Drop」「Redirect」から指定可能です。「Redirect」を選択ドロップダウンリストからリダイレクトされるインタフェースを選択できます。
Counter State	カウンターの有効 / 無効を指定します。

「Apply」ボタンをクリックして、設定を適用します。
「Clear All Counter」ボタンをクリックし、表示されたすべてのカウンタ情報を消去します。
「Clear Counter」ボタンをクリックし、表示された指定ルールのカウンタ情報を消去します。
「Find」ボタンをクリックし、入力した情報を元に特定のエントリを指定します。
「Binding」ボタンをクリックし、新しく合致したアクセスリストを指定します。
「Delete」ボタンをクリックし、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Match Access-List（合致する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 11-44　Match Access-List 画面

画面に表示される項目

項目	説明
Match IP Access-List	「Standard」（通常）または「Extended」（拡張）の IP ACL を選択します。
Match IPv6 Access-List	「Standard」（通常）または「Extended」（拡張）の IPv6 ACL を選択します。
Match MAC Access-List	「Standard」（通常）または「Extended」（拡張）の MAC ACL を選択します。

「Please Select」ボタンをクリックし、作成した ACL プロファイルを選択します。
「Apply」ボタンをクリックして、設定を適用します。

「Delete」ボタンをクリックし、指定エントリを削除します。

「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 11-45 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。

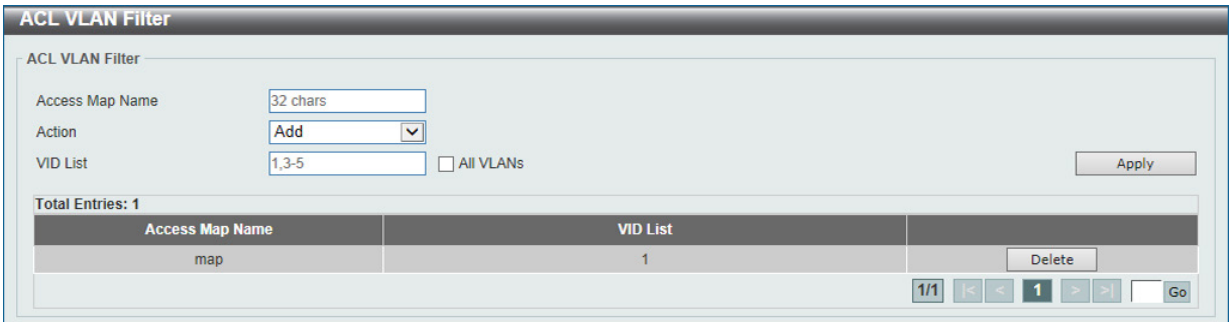


図 11-46 ACL VLAN Filter 画面

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 文字以内で入力できます。
Action	ACL VLAN フィルタの追加 / 削除をします。「Add」「Delete」から選択します。
VID List	使用する VLAN ID リストを入力します。「All VLAN」を選択するとスイッチに設定されているすべての VLAN が対象となります。

「Apply」ボタンをクリックして、設定を適用します。
「Delete」ボタンをクリックし、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

CPU ACL（CPU ACL）

本スイッチは、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。

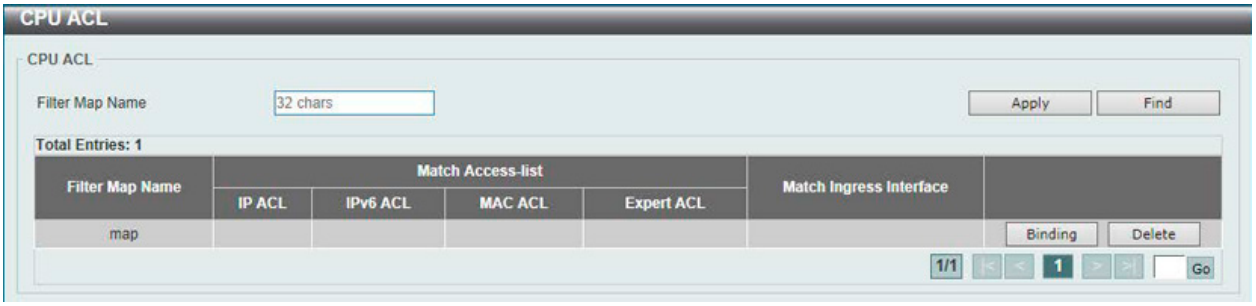


図 11-47 CPU ACL 画面

項目	説明
Filter Map Name	CPU ACL フィルタマップ名（32 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Binding」ボタンをクリックし、新しく合致したアクセスリストを指定します。
「Delete」ボタンをクリックし、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

「Binding」ボタンをクリックすると以下の画面が表示されます。

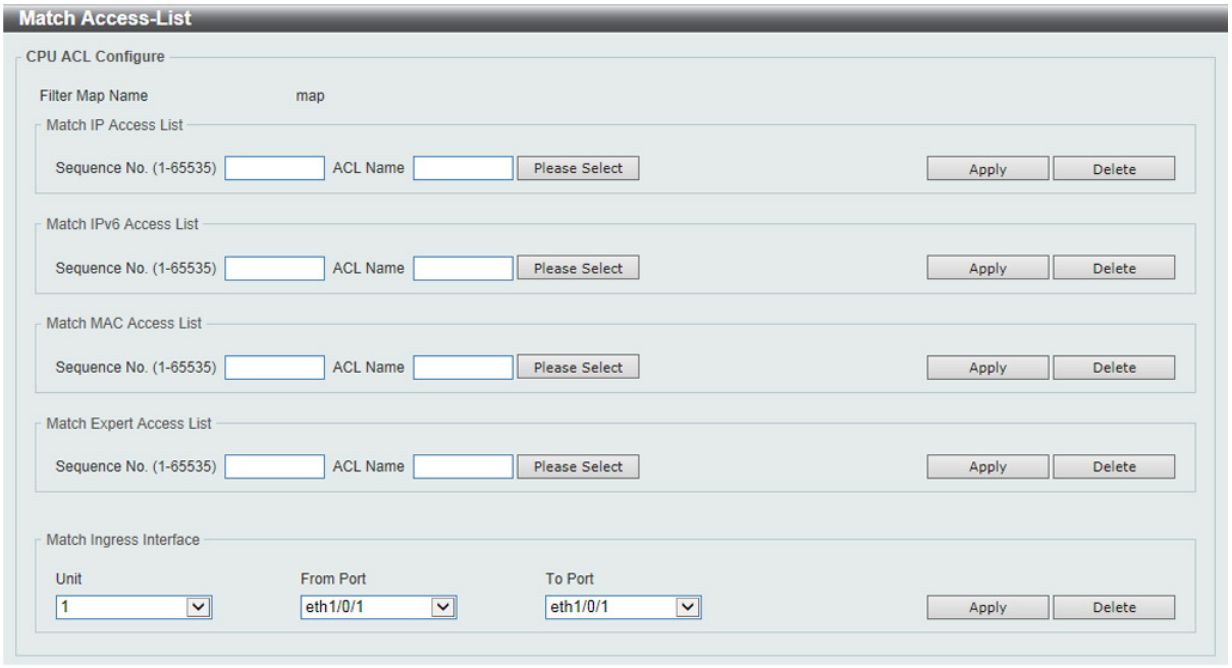


図 11-48 CPU ACL (Binding) 画面

画面に表示される項目

項目	説明
Match IP Access List	
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。「1」が最優先値となります。
ACL Name	マッチする「standard」または「extended」IP アクセスリスト名（32 字以内）を指定します。 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match IPv6 Access List	
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。「1」が最優先値となります。
ACL Name	マッチする「standard」または「extended」アクセスリスト名（32 字以内）を指定します。 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match MAC Access List	
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。「1」が最優先値となります。
ACL Name	マッチする「standard」または「extended」アクセスリスト名（32 字以内）を指定します。 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match Expert Access List	
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。「1」が最優先値となります。
ACL Name	マッチする「standard」または「extended」アクセスリスト名（32 字以内）を指定します。 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match Expert Access List	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

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

「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 11-49 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）

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

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

サブメニュー	説明
Port Security（ポートセキュリティ）	ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。
802.1X（802.1X 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 の設定を行います。
TACACS+（TACACS+ 設定）	TACACS+ の設定を行います。
IMPB （IP-MAC-Port Binding/IP-MAC- ポートバインディング）	IP-MAC バインディングにより、スイッチにアクセスするユーザ数を制限します。
DHCP Server Screening （DHCP サーバスクリーニング設定）	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
ARP Spoofing Prevention （ARP スプーフィング防止設定）	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスとマッチしなかった 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。
NetBIOS Filtering （NetBIOS フィルタリング設定）	NetBIOS フィルタリングの設定を行います。
MAC Authentication（MAC 認証）	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
Web-based Access Control（Web 認証）	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認証する機能です。
Network Access Authentication （ネットワークアクセス認証）	Network Access Authentication（ネットワークアクセス認証）の設定を行います。
Safeguard Engine （セーフガードエンジン）	セーフガードエンジンは、攻撃中にスイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。
Trusted Host（トラストホスト）	トラストホストの設定を行います。
Traffic Segmentation （トラフィックセグメンテーション）	トラフィックセグメンテーション機能はポート間のトラフィックの流れを制限を行います。
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。
Zone Defense Settings （ゾーンディフェンス設定）	「ゾーンディフェンス（Zone Defense）」機能の設定と表示を行います。
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。
SFTP Client Settings（SFTP クライアント設定）	「Secure File Transfer Protocol」(SFTP) クライアントの設定、表示を行います。
Network Protocol Port Protect Settings （ネットワークプロトコルポートプロテクト設定）	ネットワークプロトコルポートプロテクションの設定、表示を行います。

Port Security（ポートセキュリティ）

ポートセキュリティは、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。

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。

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。

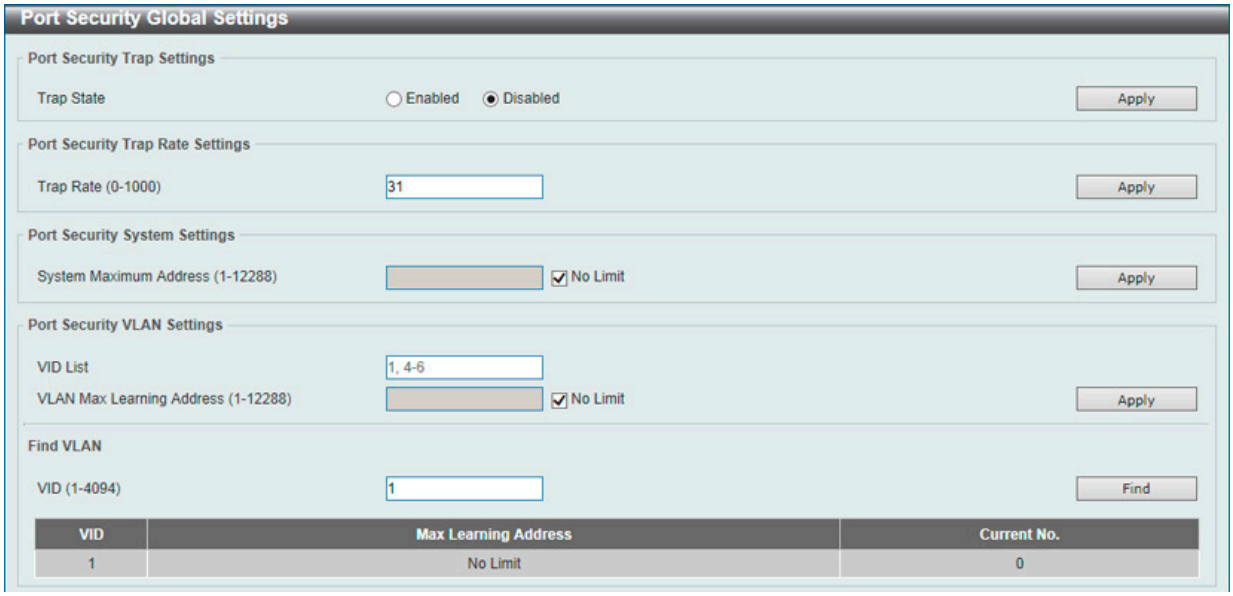


図 12-1　Port Security Global Settings 画面

本画面には以下の項目があります。

項目	説明
Trap State	ポートセキュリティトラップ設定を「Enabled」（有効）または「Disabled」（無効）にします。
Trap Rate	毎秒のトラップ数を指定します。0 から 1000 までの間で指定できます。初期値の 31 は SNMP トラップがあらゆるセキュリティ違反に対して動作することを意味します。
System Maximum Address	システムの最大 MAC アドレス数を入力します。1 から 12288 まで指定可能です。指定しない場合、または「No Limit」にチェックを入れた場合、初期値の「No Limit」となり、スイッチに MAC アドレス最大数が適用されます。
VID List	VLAN ID（s）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（1-12288）を指定します。「No Limit」を選択すると無制限に MAC アドレスを学習します。
VID	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お行います。

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。

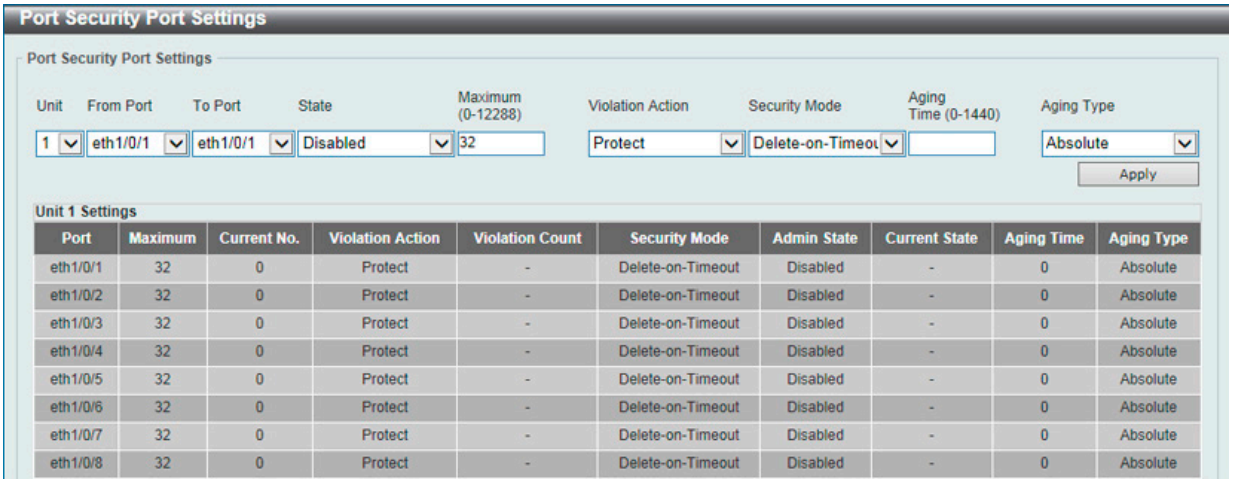


図 12-2　Port Security Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
State	指定ポートへのポートセキュリティ機能を有効 / 無効にします。
Maximum	指定ポートで許可される安全な MAC アドレスの最大数を指定します。0 から 12288 まで指定可能で初期値は 32 です。
Violation Action	違反に対する動作を指定します。「Protect」「Restrict」「Shutdown」から指定可能です。 「Protect」を選択すると、ポートセキュリティレベルで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反カウントとしては数えられません。 「Restrict」を選択すると、ポートセキュリティレベルで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントされシステムログに記録されます。 「Shutdown」を選択すると、セキュリティ違反があるとポートをシャットダウンし、システムログに記録されます。
Security Mode	セキィリティモードを選択します。「Permanent」「Delete-on-Timeout」から選択可能です。「Permanent」を選択するとすべての学習した MAC アドレスは手動でエントリを削除しない限り削除されません。「Delete-on-Timeout」を選択するとすべての学習した 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、手動でエントリを削除します。
Aging Time	指定ポートの自動取得アドレスに使用するエージングタイムです。0 から 1440 分の間で指定可能です。
Aging Type	エージングの種類を指定します。「Absolute」「Inactivity」から指定します。「Absolute」を指定すると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。初期値になります。「Inactivity」を指定すると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。

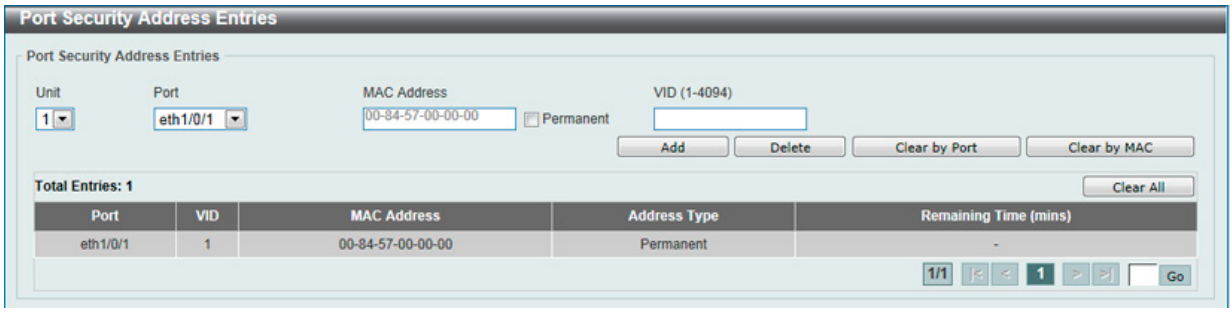


図 12-3　Port Security Address Entries 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
MAC Address	MAC アドレスを入力します。
VID	VLAN ID を指定します。1 から 4094 の間で指定できます。

「Add」ボタンをクリックして、入力した情報に基づく新しいエントリを追加します。
「Delete」ボタンをクリックし、入力した情報に基づく新しいエントリを削除します。
「Clear by Port」ボタンをクリックし、選択したポートに基づく情報を消去します。
「Clear by MAC」ボタンをクリックし、選択した MAC アドレスに基づく情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

802.1X（802.1X 認証設定）

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 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。本方式は、ネットワークへアクセスするユーザを認証するために 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・サーバ間で中継することにより実現します。以下の図は基本的な EAPOL パケットの構成を示しています。

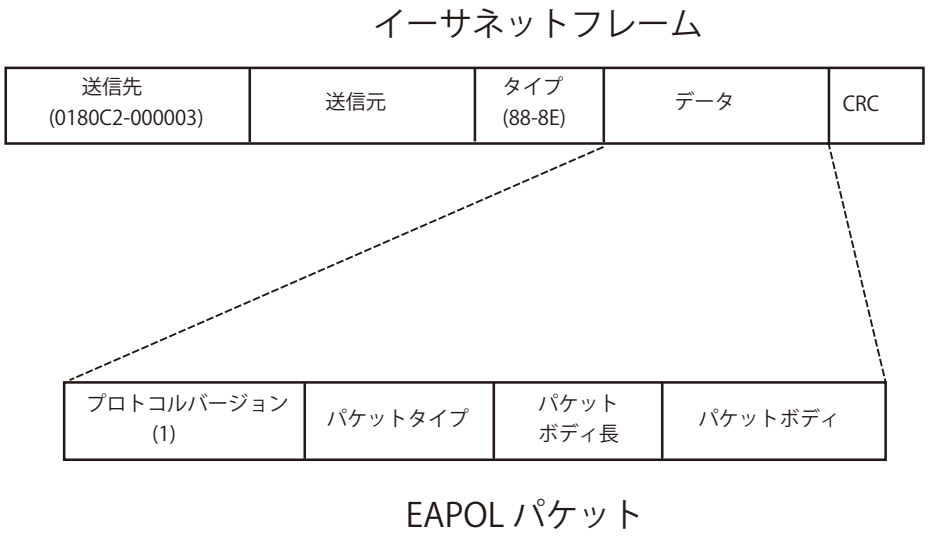


図 12-4　EAPOL パケット

本方法を使用すると、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、承認が与えられるまでの間指定ポート経由で送受信される唯一のトラフィックです。802.1X アクセスコントロール方式は 3 つの役割を持っており、それぞれがアクセスコントロールセキュリティ方法の作成、状態の保持および動作のために必要不可欠です。

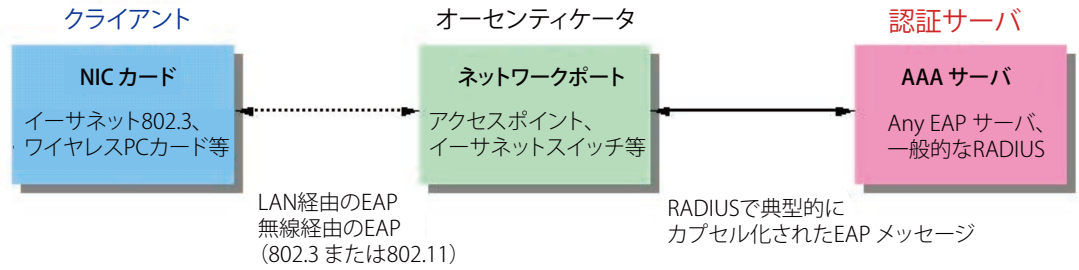


図 12-5　802.1X の 3 つの要素

以下の項では、クライアント、オーセンティケータ、および認証サーバのそれぞれの役割について詳しく説明します。

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。認証サーバ上では RADIUS サーバプログラムを実行し、またそのサーバのデータがオーセンティケータ側（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受ける前に、認証サーバ（RADIUS）による認証を受ける必要があります。認証サーバは、RADIUS サーバとクライアントの間で EAPOL パケットを通じて信頼できる情報を交換し、そのクライアントの LAN やスイッチサービスへのアクセス許可の有無をスイッチに通知します。このように、認証サーバの役割は、ネットワークにアクセスを試みるクライアントの身元を保証することです。

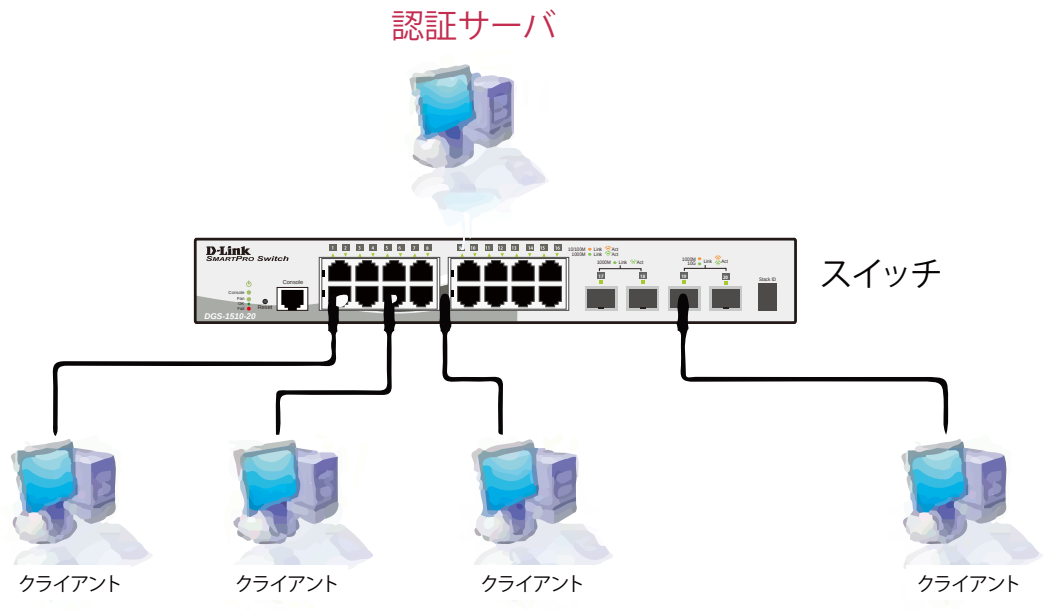


図 12-6　認証サーバ

オーセンティケータ

オーセンティケータ（スイッチ）は、認証サーバとクライアントの間を取り持つ、仲介の役割を果たします。802.1X を使用する場合、オーセンティケータサーバには 2 つの目的があります。 1 つ目の目的は、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 つ目の目的は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正しく設定するためには、以下の 3 つの手順を実行する必要があります。

1. 802.1X 機能を有効にします。（**Security > 802.1X > 802.1X Global Settings**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Port Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > RADIUS > RADIUS Server Settings**）

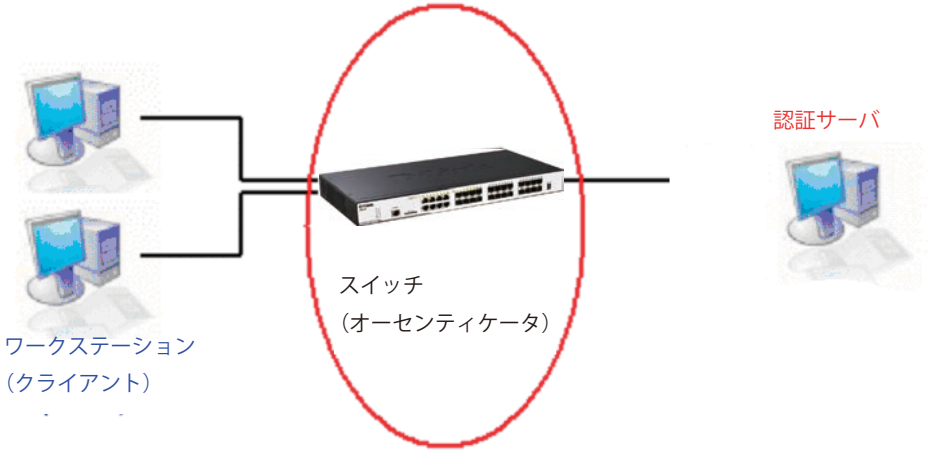


図 12-7　オーセンティケータ

クライアント

クライアントとは、簡単に言うと LAN やスイッチが提供するサービスへのアクセスを希望するワークステーションです。クライアントとなるワークステーションでは、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。Windows XP 使用の場合には、OS 内に既にそのようなソフトウェアが組み込まれています。それ以外の場合には、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、またスイッチからの要求に対しても応答します。

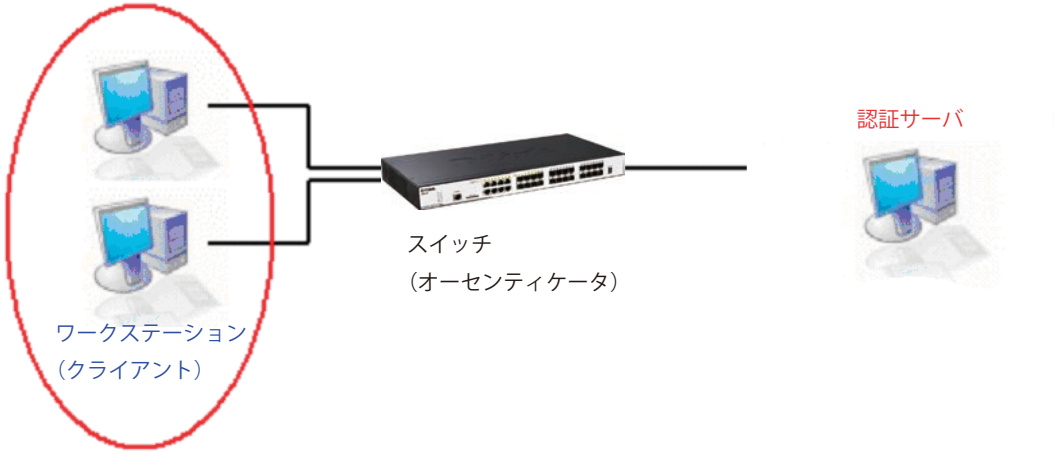


図 12-8　クライアント

認証プロセス

これらの 3 つの要素により、802.1X プロトコルはネットワークへのアクセスを試みるユーザの認証を安定的かつ安全に行います。認証に成功する前は、EAPOL トラフィックのみが特定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 の設定で MAC アドレスも指定されている場合は 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。D-Link が実装する 802.1X では以下の 2 種類のアクセスコントロールが選択できます。

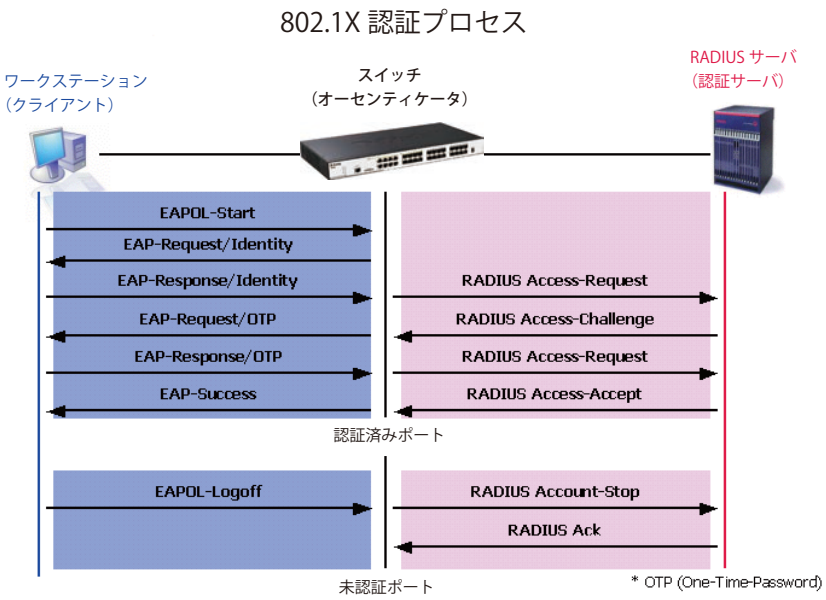


図 12-9　802.1X 認証プロセス

本スイッチの 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、1 人のユーザがリモートの RADIUS サーバにポートごとの認証をリクエストし、残りのユーザも同じポートを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、スイッチは自動的に各ポートに対して 448 件までの MAC アドレスを自動的に学習してリストに追加します。スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に各 MAC アドレスの認証を行います。

ポートベースのネットワークアクセスコントロール

802.1X の開発の本来の目的は、LAN 上で Point to Point プロトコルの機能を利用することでした。インフラストラクチャのように単一の LAN セグメントが 2 個以上のデバイスを持たない場合、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あるアクティブなデバイスの接続を示すイベントや、アクティブなデバイスが非アクティブ状態に遷移することを示すイベントの検知を行います。これらのイベントをポートの認証状態の制御に利用し、ポートでの認証が行わない場合に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。

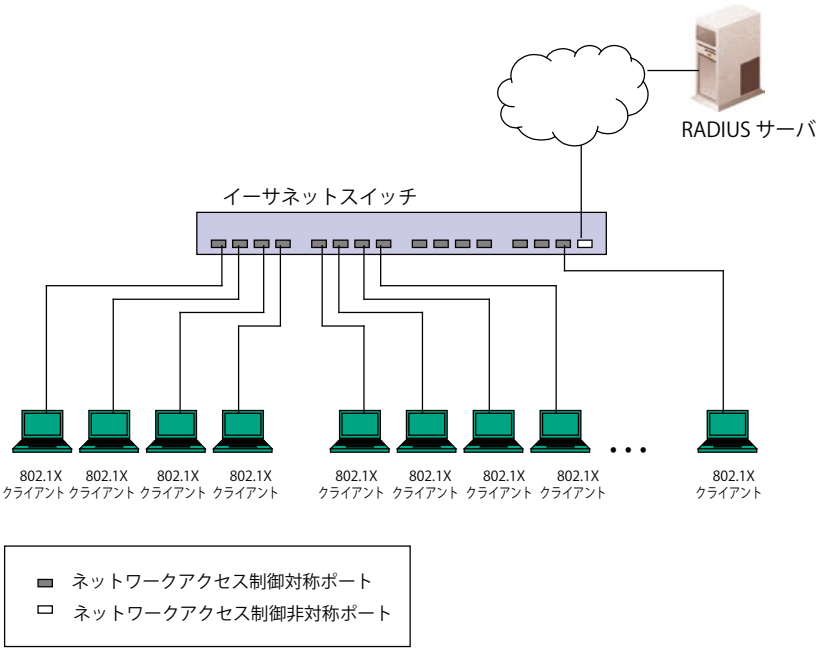


図 12-10　典型的なポートベースアクセスコントロールのネットワーク構成例

一度接続デバイスが認証に成功すると、ポートは Authorized（認証済み）状態になり、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となりません。そのため、ポートが 1 台以上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 に対して事実上アクセスを許可することになります。このような状態のセキュリティは明らかに脆弱であると言えます。

ホストベースのネットワークアクセスコントロール

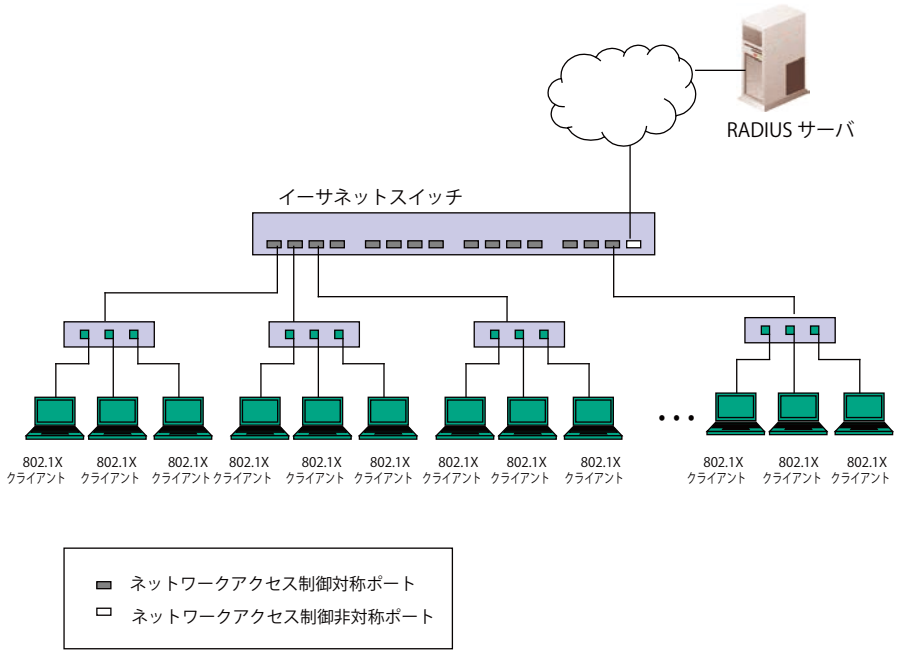


図 12-11　典型的な MAC ベースアクセスコントロールのネットワーク構成例

共有 LAN セグメント内で 802.1X を活用するためには、LAN へのアクセスを希望する各デバイスに「仮想」ポートを定義する必要があります。するとスイッチは共有 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、それら仮想ポートを EAPOL の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 と通信するための仮想ポートを確立します。

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

本画面では 802.1X グローバル設定を行います。

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

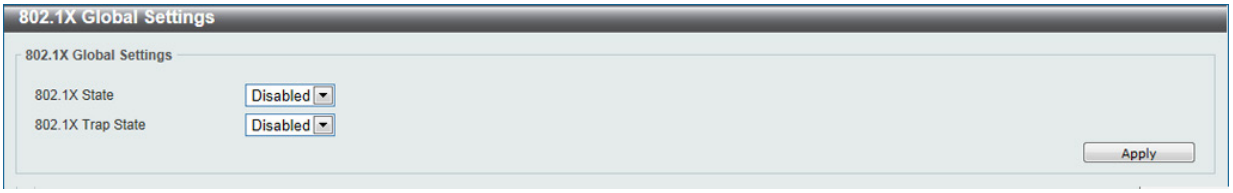


図 12-12　802.1X Global Settings 画面

この画面では以下の機能を設定できます。

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。

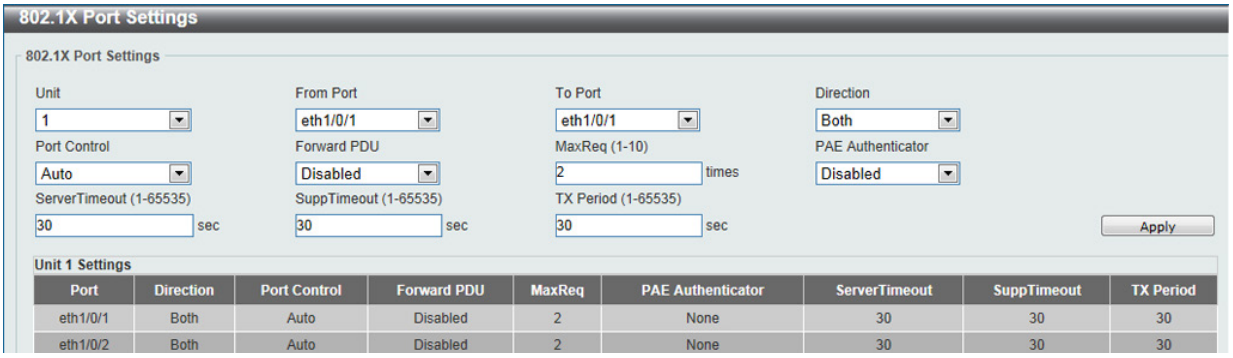


図 12-13　802.1X Settings 画面

この画面では以下の機能を設定できます。

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象の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。初期値は「both」です。 • 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。
Port Control	ポートの認証状態を指定します。 • ForceAuthorized - 802.1X を無効にします。この場合、ポートが認証状態になるのに、どのような認証の交換も必要ありません。つまり、ポートは 802.1X ベースの認証無しのトラフィックを送受信します。 • ForceUnauthorized - ポートは常に認証されていない状態になり、クライアントからの認証要求を無視します。スイッチはクライアントに対して認証サービスを提供しません。 • Auto - 802.1X を有効にし、ポートはまず、認証されていない EAPOL フレームだけを送受信できる状態になります。リンク状態が接続、切断と変化したり、EAPOL-start フレームを受け取ると認証プロセスが始まります。スイッチはクライアントの識別を要求し、クライアントと認証サーバ間の認証メッセージの中継を開始します。（初期値）
Forward PDU	PDU 要求の再送を有効 / 無効にします。
MaxReq (1-10)	認証セッションがタイムアウトになるまでに EAP リクエストをクライアントに送信する最大の回数を指定します。1 から 10 までの間で指定可能です。初期値は 2 です。
PAE Authenticator	PAE Authenticator を有効 / 無効に指定します。 本項目では特定ポートを IEEE 802.1X Port Access Entity（PAE）認証として指定します。
ServerTimeout (1-65535)	Authenticator と認証サーバの通信が切れてタイムアウト状態となる時間を指定します。初期値は 30（秒）です。
SuppTimeout (1-65535)	Authenticator とクライアントの通信が切れてタイムアウト状態となる時間を指定します。初期値は 30（秒）です。
TxPeriod (1-65535)	PAE を管理する Authenticator の TxPeriod の値を指定します。EAP Request/Identity パケットがクライアントに送信される間隔を決定します。初期値は 30（秒）です。

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

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。

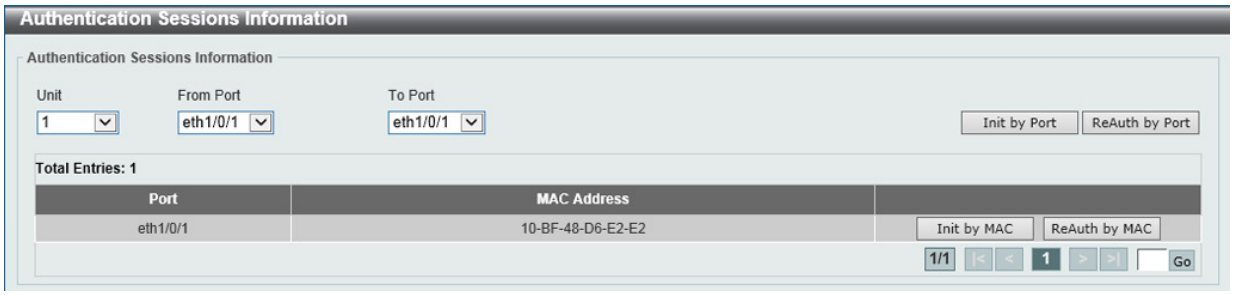


図 12-14　Authentication Session Information 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象のポート範囲を指定します。

「Init by Port」ボタンをクリックして、入力した情報に基づくセッション情報を起動します。
「ReAuth by Port」ボタンをクリックして、入力した情報に基づく再認証（Re-Authenticate）を行います。
「Init by MAC」ボタンをクリックして、入力した情報に基づくセッション情報を起動します。
「ReAuth by MAC」ボタンをクリックして、入力した情報に基づく再認証（Re-Authenticate）を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

オーセンティケータの統計情報を表示します。

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

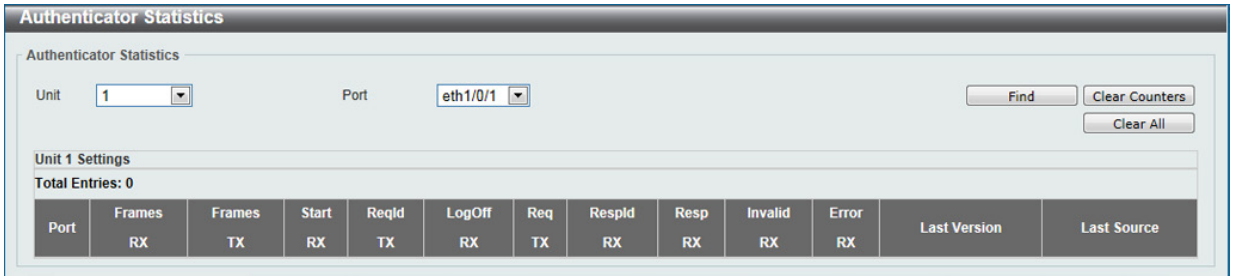


図 12-15　Authenticator Statics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して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。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Authenticator Session Statistics（オーセンティケータセッション統計情報）

オーセンティケータセッションの統計情報を表示します。

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



図 12-16　Authenticator Session Statistics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して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。

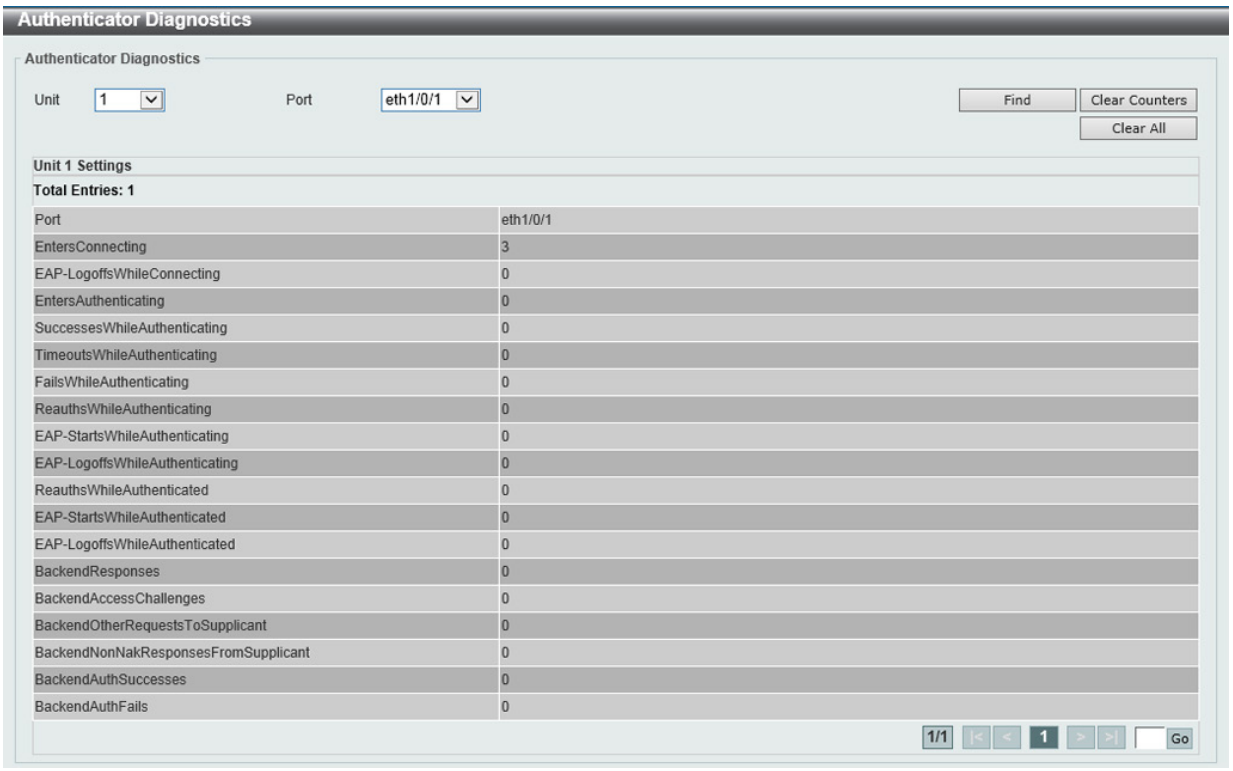


図 12-17　Authenticator Diagnostics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して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。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

AAA（AAA 設定）

Security > AAA
本項目では AAA（Authentication、Authorization、Accounting）の有効 / 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。

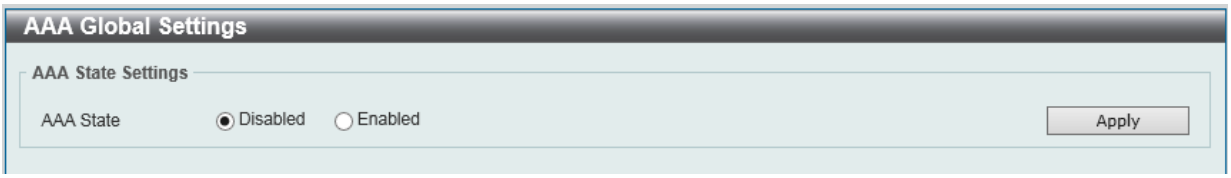


図 12-18 AAA Global Settings 画面

「AAA State」をグローバルに「有効」(Eneable) /「無効」(Disable）をグローバルに指定します。

Application Authentication Settings（アプリケーションの認証設定）

ログインする際に使用するスイッチの設定用アプリケーション（コンソール、Telnet、SSH、HTTP）を設定します。

Security > Access Authentication Control > Application Authentication Settings の順にクリックし、以下の画面を表示します。

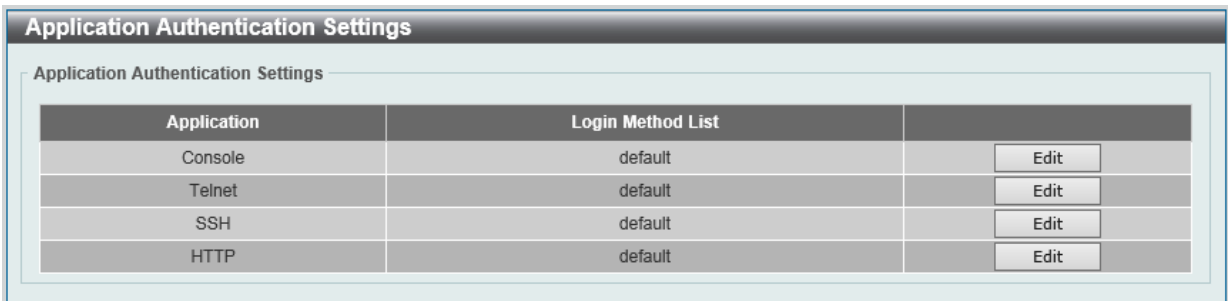


図 12-19 Application Authentication Settings 画面

指定エントリの「Edit」ボタンをクリックし編集を行います。
「Edit」をクリックすると、以下の画面が表示されます。

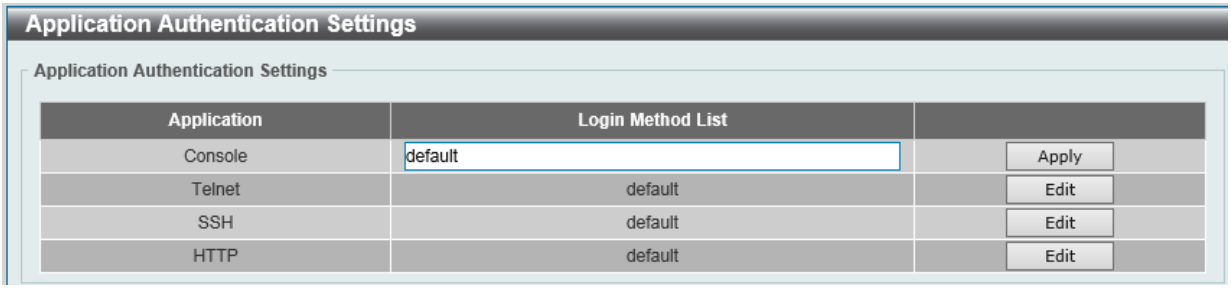


図 12-20 Application Authentication Settings (Edit) 画面

以下の項目を使用して、設定を行います。

項目	説明
Login Method List	指定エントリの「Edit」ボタンをクリックし編集を行います。使用するログインメソッドリスト名を入力します。

設定を変更する際は、必ず「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。

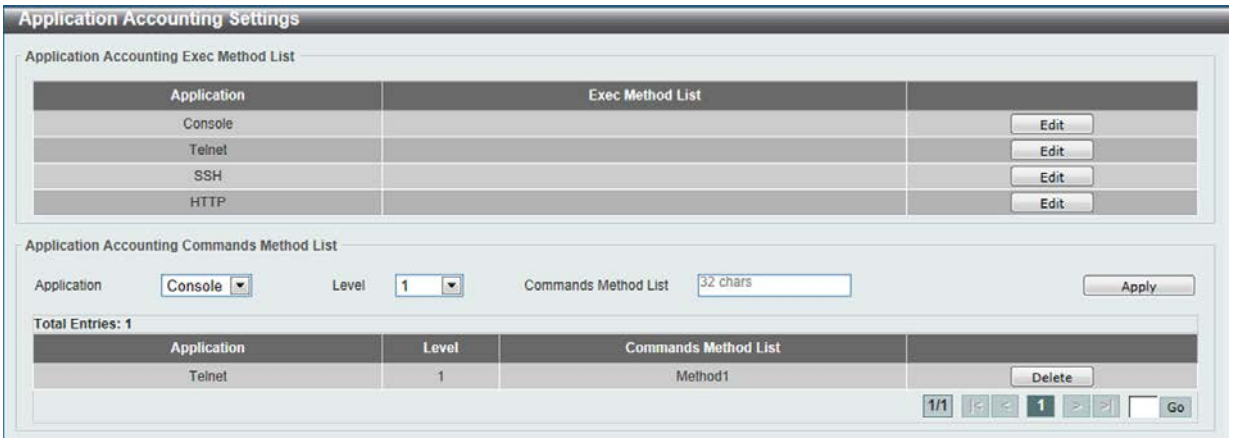


図 12-21　Application Accounting Settings 画面

「Edit」をクリックして指定エントリの設定を行います。
「Edit」をクリックすると、以下の画面が表示されます。

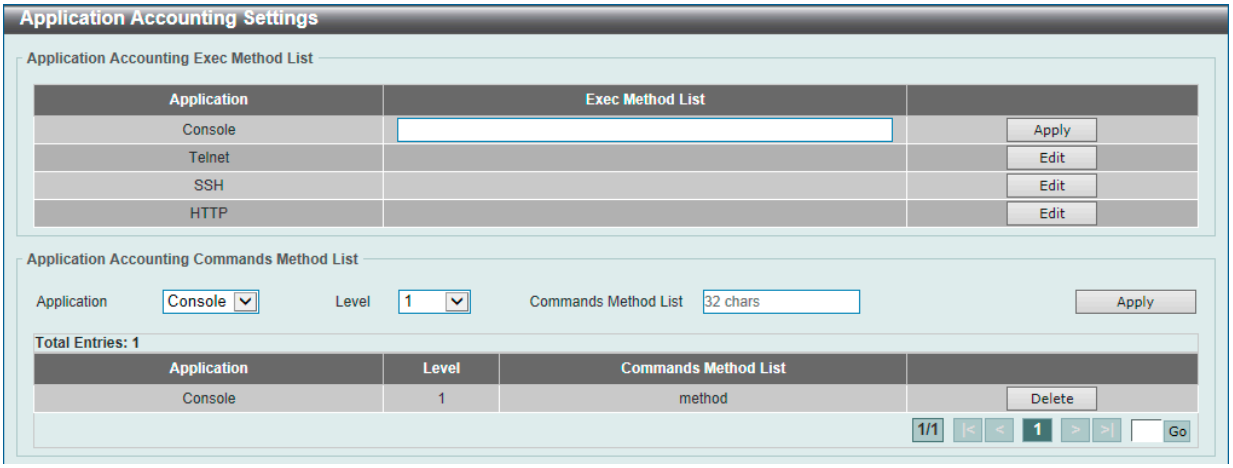


図 12-22　Application Accounting Settings (Edit) 画面

以下の項目を使用して、設定を行います。

項目	説明
Exec Method List	指定エントリの「Edit」ボタンをクリックし編集を行います。使用する 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。「Console」「Telnet」「SSH」から選択します。
Level	権限レベルを指定します。1 から 15 の間で指定できます。
Commands Method List	使用するコマンドメソッドリストを入力します。

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

Authentication Settings（認証設定）

AAA ネットワークと EXEC 認証設定を行います。

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

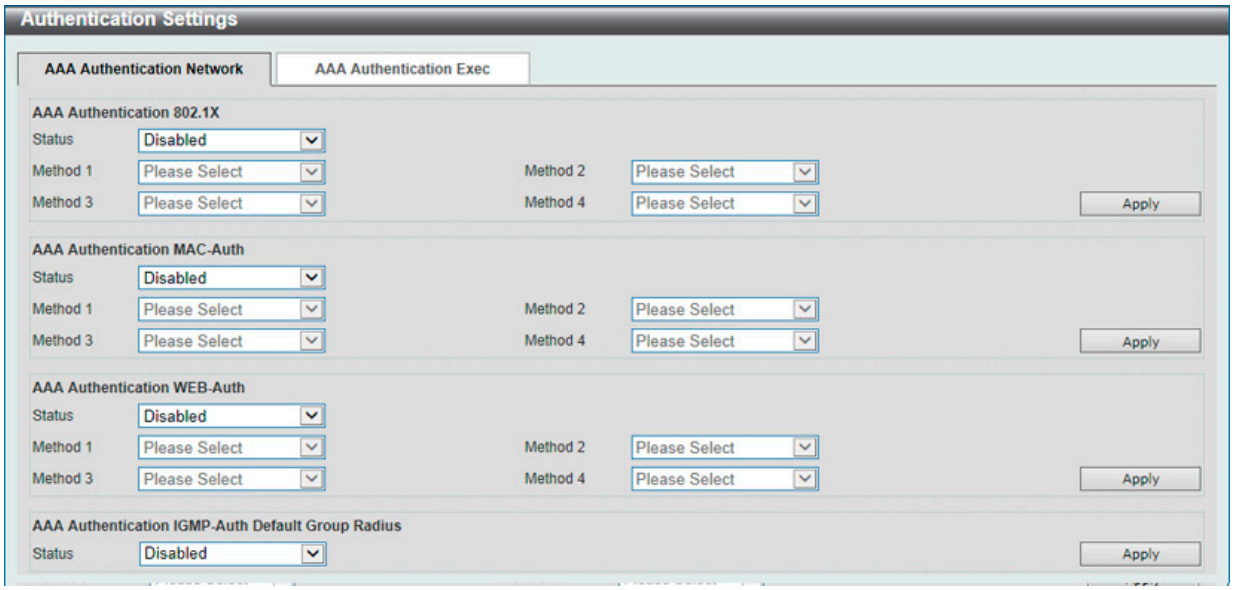


図 12-23　Authentication Settings -AAA Authentication Settings タブ画面

「AAA Authentication Network」タブ

「AAA Authentication Network」タブ内の設定を行います。
「AAA Authentication 802.1X」「AAA Authentication JWAC」「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	各項目の認証設定の「有効」(Eneable) /「無効」(Disable) を設定します。
Method 1 to 4	本背亭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。

設定を変更する際は、必ず「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」タブをクリックして、タブ内の設定を行います。

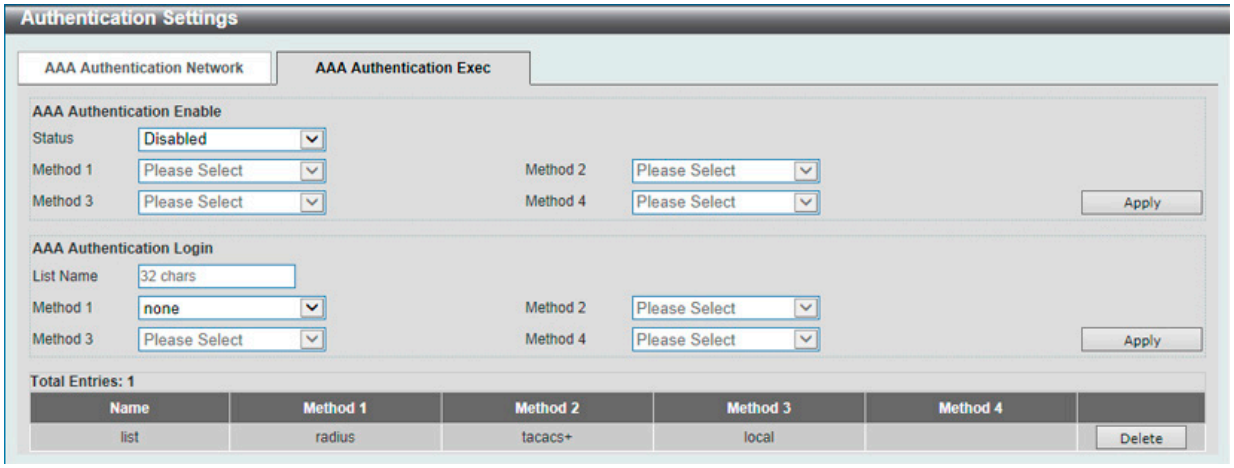


図 12-24　Authentication Settings -AAA Authentication Exec タブ画面

項目	説明
AAA Authentication Enable（AAA 認証有効）	
Status	AAA 認証設定の「有効」(Eneable) /「無効」(Disable) を設定します。
Method 1 to 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。
AAA Authentication Login（AAA 認証ログイン）	
List Name	AAA 認証ログインオプションを使用するメソッドリスト名を入力します。

項目	説明
Status	AAA 認証設定の「有効」(Eneable) /「無効」(Disable) を設定します。
Method 1 to 4	使用する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。

設定を変更する際は、必ず「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。

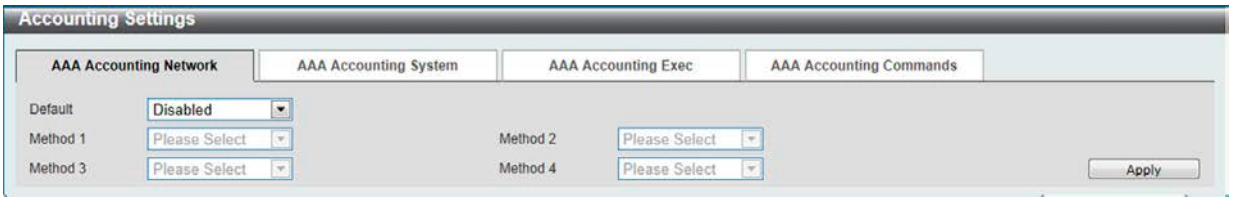


図 12-25 Accounting Settings 画面

「AAA Accounting Network」「AAA Accounting System」「AAA Accounting Exec」「AAA Accounting Commands」それぞれのタブにおいて設定を行います。

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 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「tacacs+」から選択します。
「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 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「tacacs+」から選択します。
「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 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「tacacs+」から選択します。
「AAA Accounting Commands」タブ	
Level	権限レベルを指定します。1 から 15 までで指定可能です。
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 to 4	使用するメソッドリストを選択します。「none」「group」「tacacs+」から選択します。

「Delete」をクリックして指定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。
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。

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。

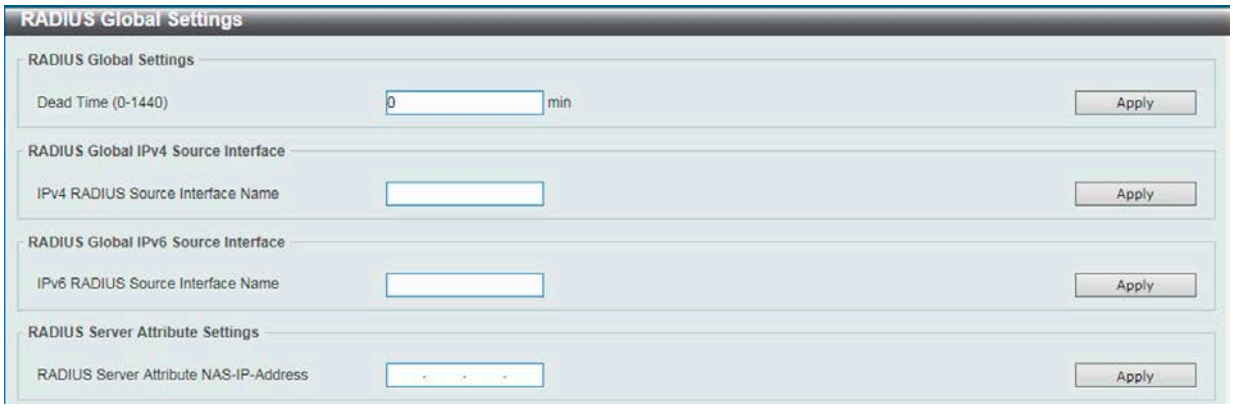


図 12-26　RADIUS Global Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
DeadTime (0-1440)	デッドタイムの設定を行います。1 から 1440（分）の間で指定できます。初期値は「0」です。0 に設定されている場合、応答しないサーバは「Dead」として認識されることはありません。この設定により、応答しないサーバホストエントリをスキップする「デッドタイム」が設定され認証プロセスは改善されます。システムが認証サーバと連携して動作する場合、一度に一つのサーバと連携します。もし連携しようとしたサーバが応答しない場合、システムは次のサーバとの連携を模索します。システムにより応答しないサーバが見つけられると、該当のサーバは「down」として認識され、「デッドタイム」タイマーが開始され、それ以後のリクエスト認証はデッドタイム時間が過ぎるまでスキップされます。
IPv4 RADIUS Source Interface Name	IPv4 RADIUS アドレスソースインタフェース名を入力します。
IPv6 RADIUS Source Interface Name	IPv6 RADIUS アドレスソースインタフェース名を入力します。
RADIUS Server Attribute NAS-IP-Address	RADIUS サーバ属性 NAS-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。

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。

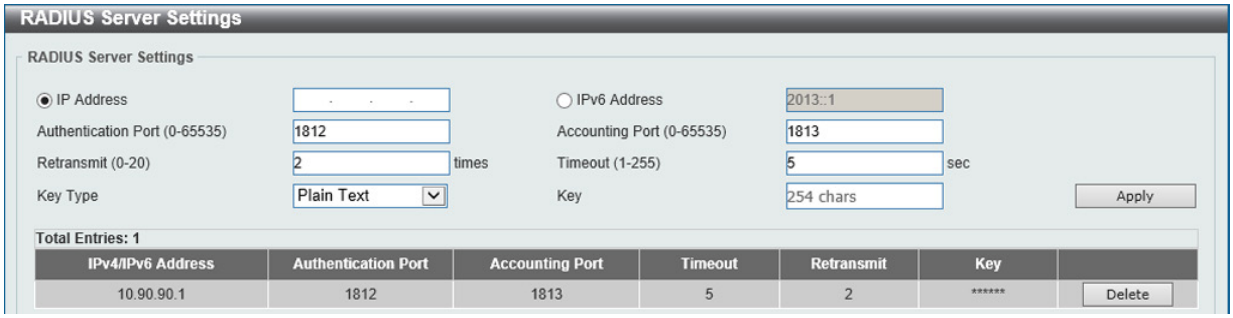


図 12-27　RADIUS Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。
Authentication Port (1-65535)	RADIUS 認証サーバの UDP ポートです。初期値は 1812 です。
Accounting Port (1-65535)	RADIUS アカウントサーバのポートです。初期値は 1813 です。
Retransmit (0-20)	RADIUS サーバの再転送間隔（秒）を設定します。初期値は 3（秒）です。
Timeout (1-255)	RADIUS サーバのタイムアウト時間（秒）を設定します。初期値は 5（秒）です。
Key Type	RADIUS サーバに設定する鍵の種類を選択します。「Plain Text」「Encrypted」から選択します。
Key	RADIUS サーバに設定したものと同一の鍵を指定します。254 文字以内で指定します。

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

RADIUS 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 12-28 RADIUS Group Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Group Server Name	RADIUS グループサーバ名を入力します。15 文字までで指定可能です。
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。

設定を変更する際は、必ず「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。
「Show Detail」をクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

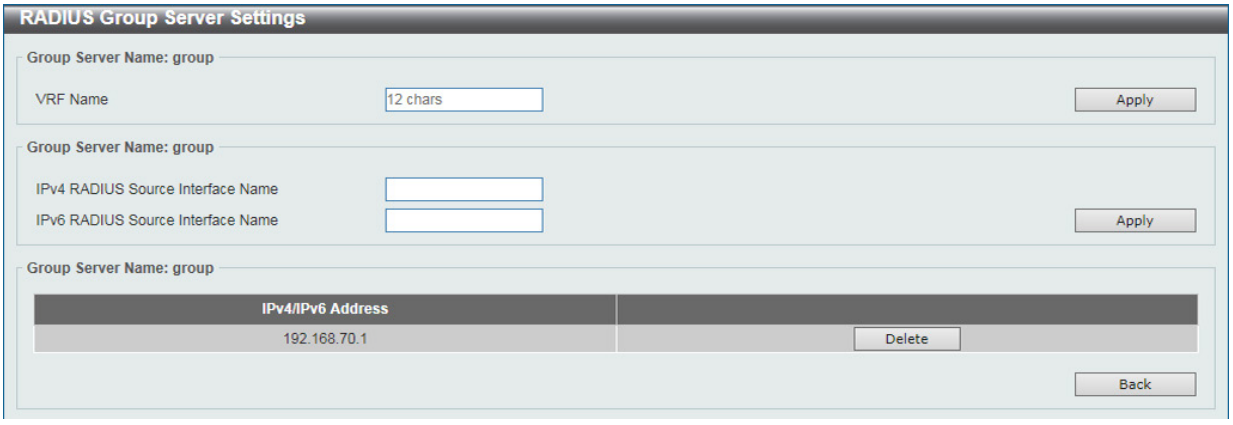


図 12-29 RADIUS Group Server Settings (Detail) 画面

この画面では以下の情報を確認、設定できます。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
IPv4 RADIUS Source Interface Name	IPv4 RADIUS アドレスソースインタフェース名を入力します。
IPv6 RADIUS Source Interface Name	IPv6 RADIUS アドレス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」をクリックして指定エントリを削除します。
「Back」をクリックして以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。

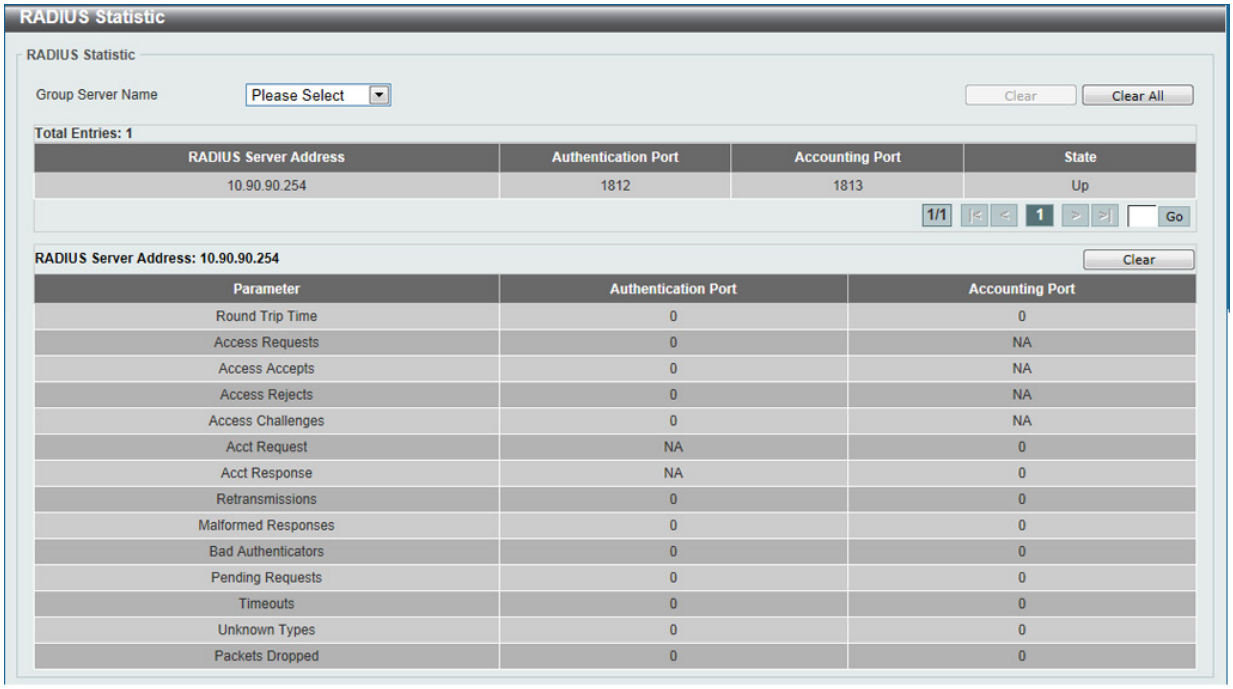


図 12-30 RADIUS Statistic 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Group Server Name	表示する RADIUS グループサーバ名を選択します。

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

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。

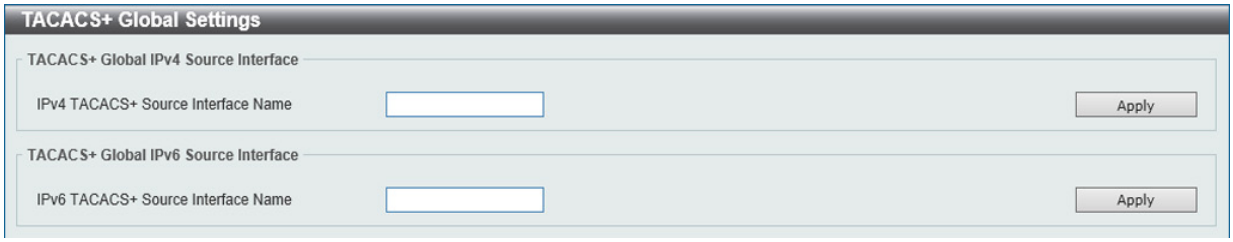


図 12-31 TACACS+ Global Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
IPv4 TACACS+ Source Interface Name	IPv4 TACACS+ ソースインタフェース名を入力します。

項目	説明
IPv6 TACACS+ Source Interface Name	IPv6 TACACS+ アドレス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。

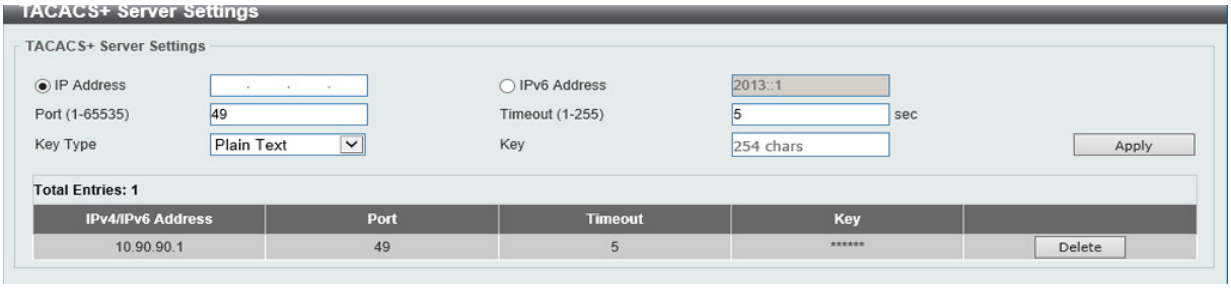


図 12-32 TACACS+ Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
IP Address	TACACS+ サーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ サーバの IPv6 アドレスを入力します。
Port (1-65535)	TACACS+ サーバのポートです。初期値は 49 です。
Timeout (1-255)	TACACS+ サーバのタイムアウト時間（秒）を設定します。初期値は 5（秒）です。
Key Type	TACACS+ サーバに設定する鍵の種類を選択します。「Plain Text」「Encrypted」から選択します。
Key	TACACS+ サーバに設定したものと同一の鍵を指定します。254 文字以内で指定します。

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

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。

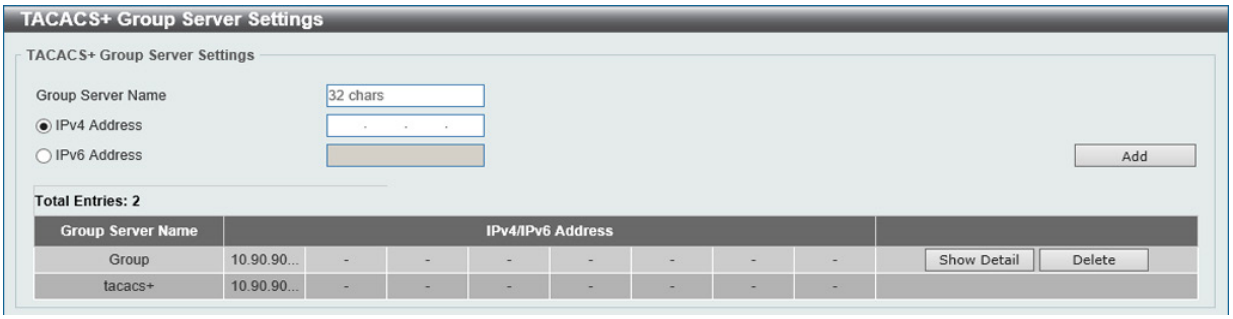


図 12-33 TACACS+ Group Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Group Server Name	TACACS+ グループサーバ名を入力します。32 文字までで指定可能です。
IPv4 Address	TACACS+ グループサーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ グループサーバの IPv6 アドレスを入力します。

設定を変更する際は、必ず「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。
「Show Detail」をクリックすると TACACS+ グループサーバの詳細情報について表示されます。

TACACS+ Group Server Settings - Show Detail（TACACS+ グループサーバ詳細設定）

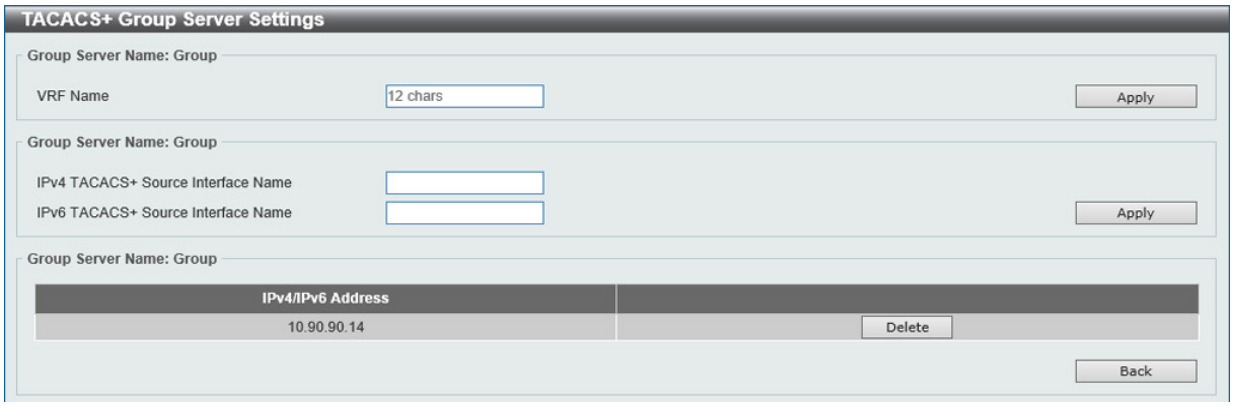


図 12-34 TACACS+ Group Server Settings - Show Detail 画面

この画面では以下の情報を確認、設定できます。

項目	説明
VRF Name	VRF インスタンス名を 12 字以内で入力します。
IPv4 TACACS+ Source Interface Name	IPv4 TACACS+ ソースインタフェース名を入力します。
IPv6 TACACS+ Source Interface Name	IPv6 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」をクリックして指定エントリを削除します。
「Back」をクリックして以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。

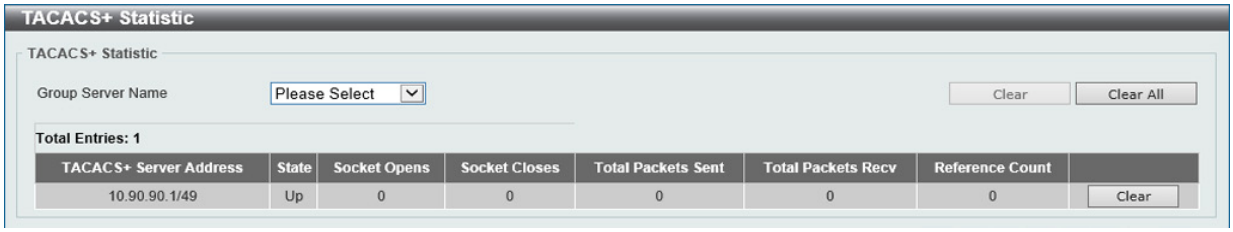


図 12-35 TACACS+ Statistic 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Group Server Name	表示する TACACS+ グループサーバ名を選択します。

「Clear」ボタンをクリックし、選択に基づいて表示した情報を消去します。
「Clear by Group」ボタンをクリックし、選択したグループのすべて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。

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数を制限することです。IP アドレスと MAC アドレスのペアを、事前に設定したデータベースと比較を行い、認証クライアントのみがスイッチのポートアクセスできるようにします。もしくは DHCP スヌーピングが有効な場合において、スイッチがスヌーピング DHCP パケットから自動的に IP/MAC ペアを学習し、IMPB ホワイトリストに保存することで、認証クライアントのポートアクセスが可能になります。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。本機能はポートベースであるため、ポートごとに本機能を有効 / 無効にすることができます。

IPv4

DHCPv4 Snooping（DHCPv4 スヌーピング）

DHCP Snooping Global Settings（DHCP スヌーピンググローバル設定）

DHCP スヌーピング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 12-36 DHCP Snooping Global Settings 画面

本画面には以下の項目があります。

項目	説明
DHCP Snooping	DHCP スヌーピングをグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
Information Option Allow Untrusted	不明インタフェースのリレーオプション 82 付き DHCP パケットをグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
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 アドレスの合致確認を「Enabled」（有効）または「Disabled」（無効）にします。
Station Move Deny	DHCP スヌーピングステーションムーブを有効 / 無効にします。 有効の場合、指定ポートにある同じ 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事を検出した場合、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。

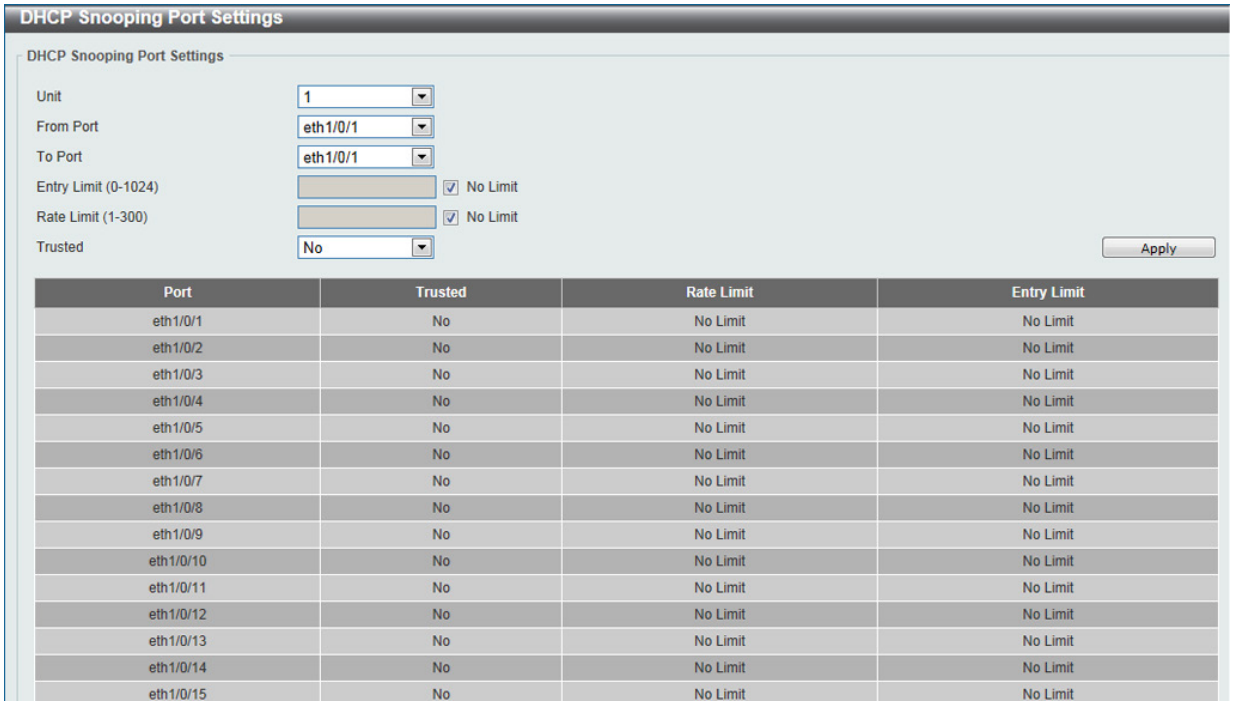


図 12-37　DHCP Snooping Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象の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。0 から 1024 の間で入力可能です。「No Limit」にチェックをすると、本機能は無効になります。
Rate Limit	レートリミットの値を入力します。1 から 300 の間で入力可能です。「No Limit」にチェックをすると、本機能は無効になります。
Trusted	トラストのオプションを選択します。「No」または「Yes」から選択します。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。

設定を変更する際は、必ず「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。

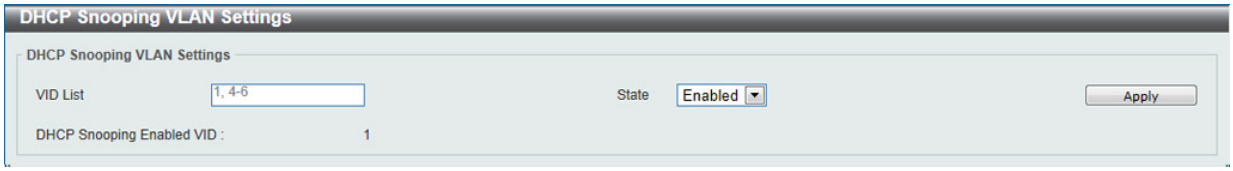


図 12-38　DHCP Snooping VLAN Settings 画面

本画面には以下の項目があります。

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。

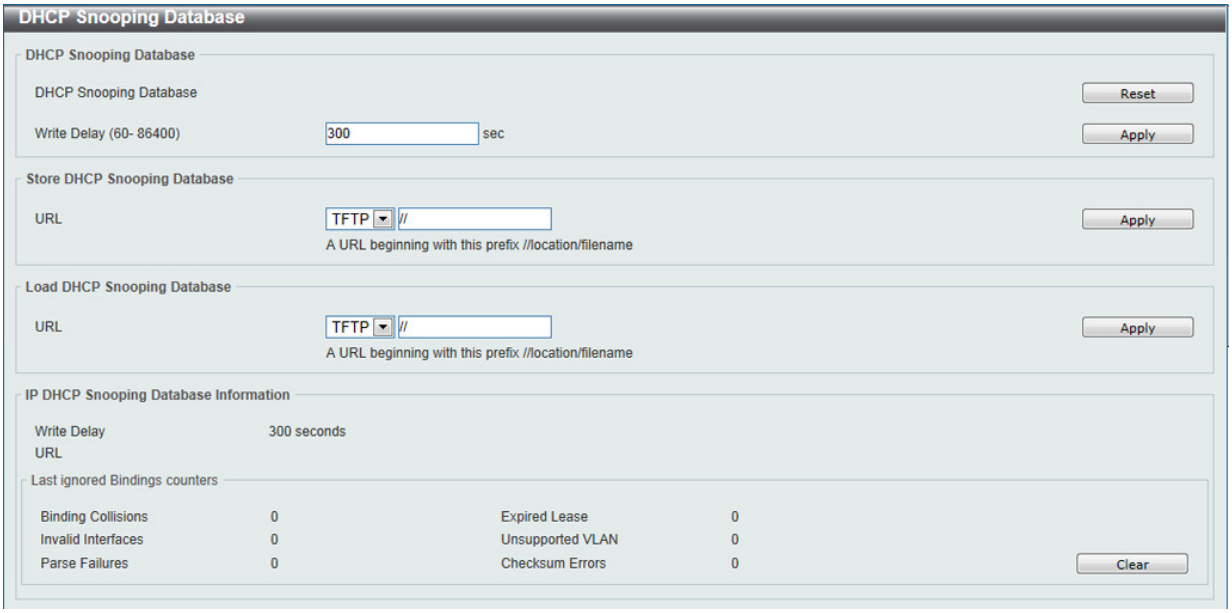


図 12-39 DHCP Snooping Database 画面

本画面には以下の項目があります。

項目	説明
DHCP Snooping Database	
Write Delay	書き込み遅延の値を入力します。60 から 86400（秒）の間で指定できます。初期値は 300 秒です。 「Apply」ボタンをクリックし、設定内容を適用してください。
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、ストアされる DHCP スヌーピングデータベースの URL を入力します。選択できるロケーションは TFTP、FTP、Flash です。
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、ロードされる DHCP スヌーピングデータベースの URL を入力します。選択できるロケーションは TFTP、FTP、Flash です。

「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear」ボタンをクリックするとカウンタ情報が消去されます。
「Reset」ボタンをクリックすると入力した情報がリセットされます。

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。

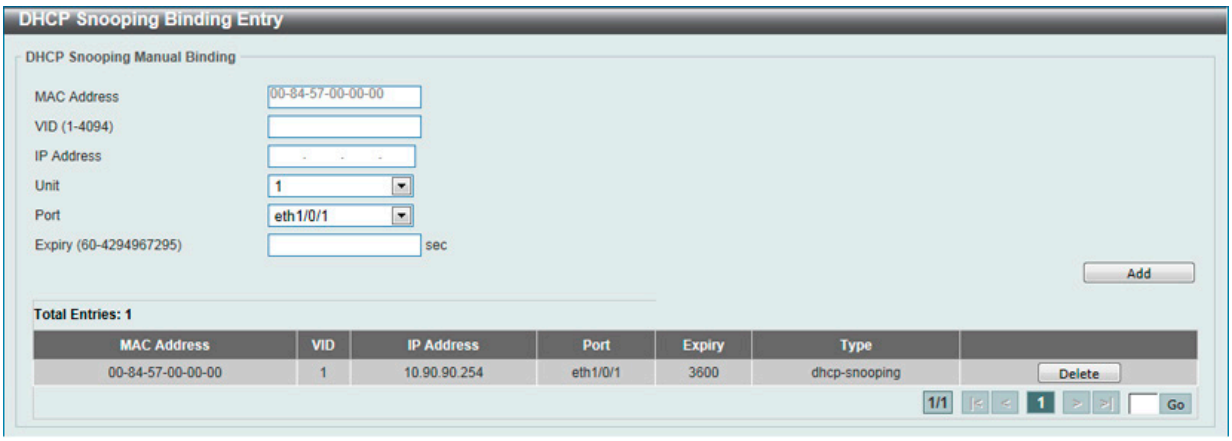


図 12-40 DHCP Snooping Binding Entry 画面

本画面には以下の項目があります。

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。1 から 4094 の間で入力可能です。
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	設定するユニットを指定します。
Port	設定するポートを指定します。
Expiry	有効期限を入力します。60 から 4294967295（秒）で指定可能です。

「Add」をクリックして入力した情報を元に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Dynamic ARP Inspection（ダイナミック ARP インスペクション）

ARP Access List（ARP アクセスリスト）

ARP アクセスリストの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List の順にクリックして、以下の画面を表示します。

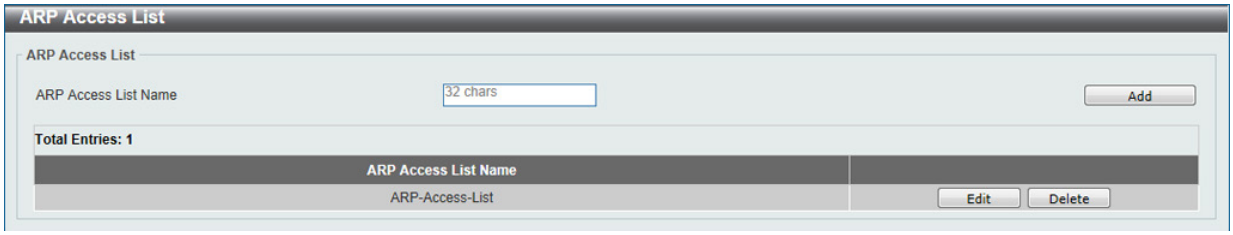


図 12-41　ARP Access List 画面

本画面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 文字まで入力可能です。

「Add」をクリックして入力した情報を元に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。

エントリの編集

「Edit」ボタンをクリックして指定のエントリを編集します。以下の画面が表示されます。

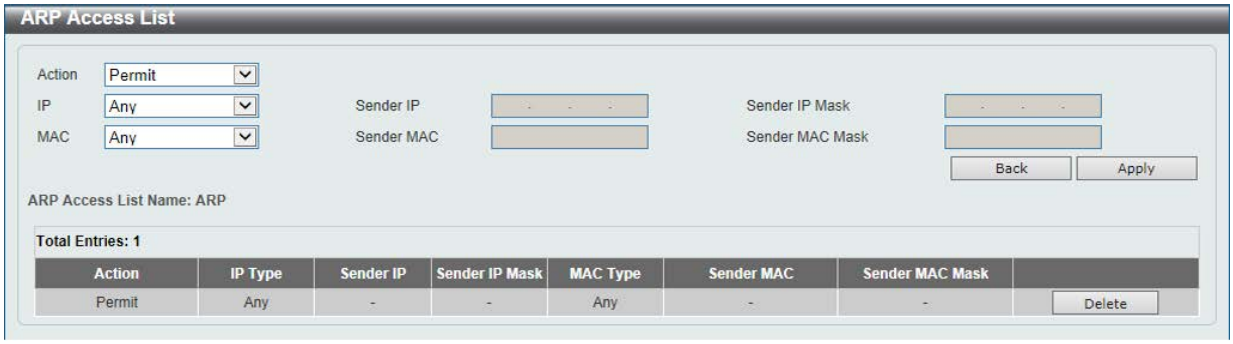


図 12-42　ARP Access List - Edit 画面

本画面には以下の項目があります。

項目	説明
Action	動作について指定します。「Permit」「Deny」から選択します。
IP	使用する送信者の IP アドレスの種類を指定します。「Any」「Host」「IP with Mask」から指定します。
Sender IP	送信者の IP アドレスを「Host」「IP with Mask」から選択した後、使用する送信者の IP アドレスを入力します。
Sender IP Mask	「IP with Mask」を選択した場合、使用する送信者の IP マスクを入力します。
MAC	送信者の MAC アドレスの種類を指定します。「Any」「Host」「MAC with Mask」から指定します。
Sender MAC	送信者の MAC アドレスを「Host」「MAC with Mask」から選択した後、使用する送信者の MAC アドレスを入力します。
Sender MAC Mask	「MAC with Mask」を選択した場合、使用する送信者の MAC マスクを入力します。

「Back」をクリックして前のページに戻ります。
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。
「Delete」をクリックして指定エントリを削除します。

ARP Inspection Settings（ARP インスペクション設定）

ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings の順にクリックして、以下の画面を表示します。

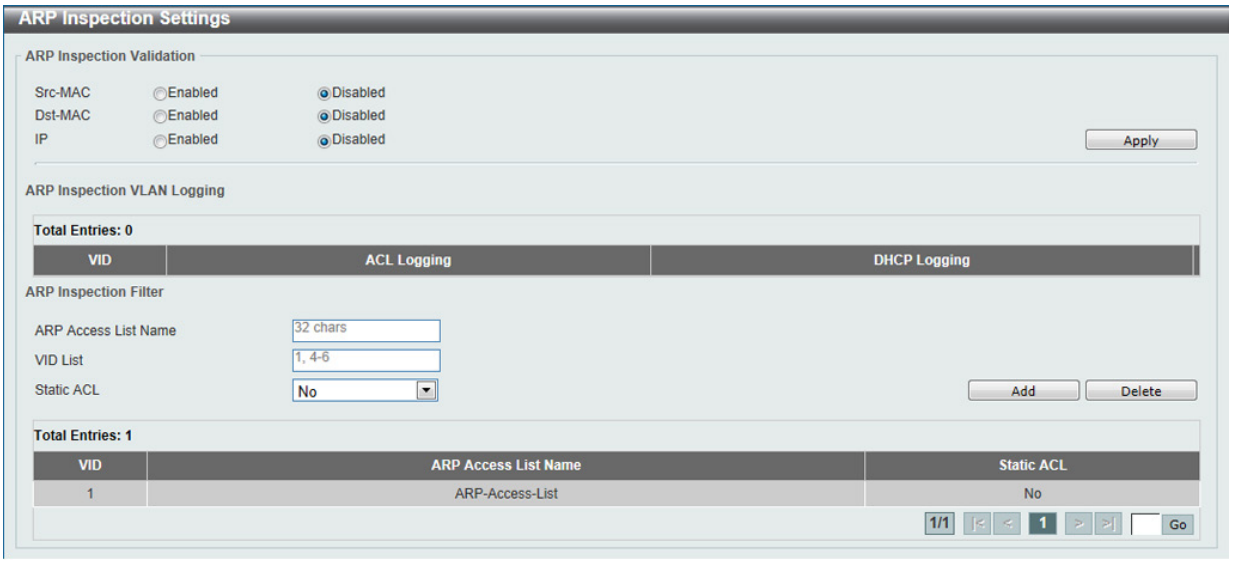


図 12-43　ARP Inspection Settings 画面

本画面には以下の項目があります。

項目	説明
Src-MAC	送信元 MAC の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 本体内の送信者 MAC アドレスに対する送信元 MAC アドレスのイーサネットヘッダの一貫性や ARP リクエスト、応対パケットなどをチェックします。
Dst-MAC	宛先 MAC の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 本体内の宛先 MAC アドレスに対する宛先 MAC アドレスのイーサネットヘッダの一貫性や ARP リクエスト、応対パケットなどをチェックします。
IP	IP の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や予期せぬ IP アドレスの ARP 本体をチェックします。本オプションはまた 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 の妥当性を確認します。IP アドレス「0.0.0.0」「255.255.255.255」に向かうパケットとすべての IP マルチキャストは破棄されます。送信者 IP アドレスはすべての ARP リクエストとレスポンスでチェックされ、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 文字まで入力可能です。
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」をクリックして入力した情報を元に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ARP Inspection Port Settings（ARP インスペクションポート設定）

ポートでの ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings の順にクリックして、以下の画面を表示します。

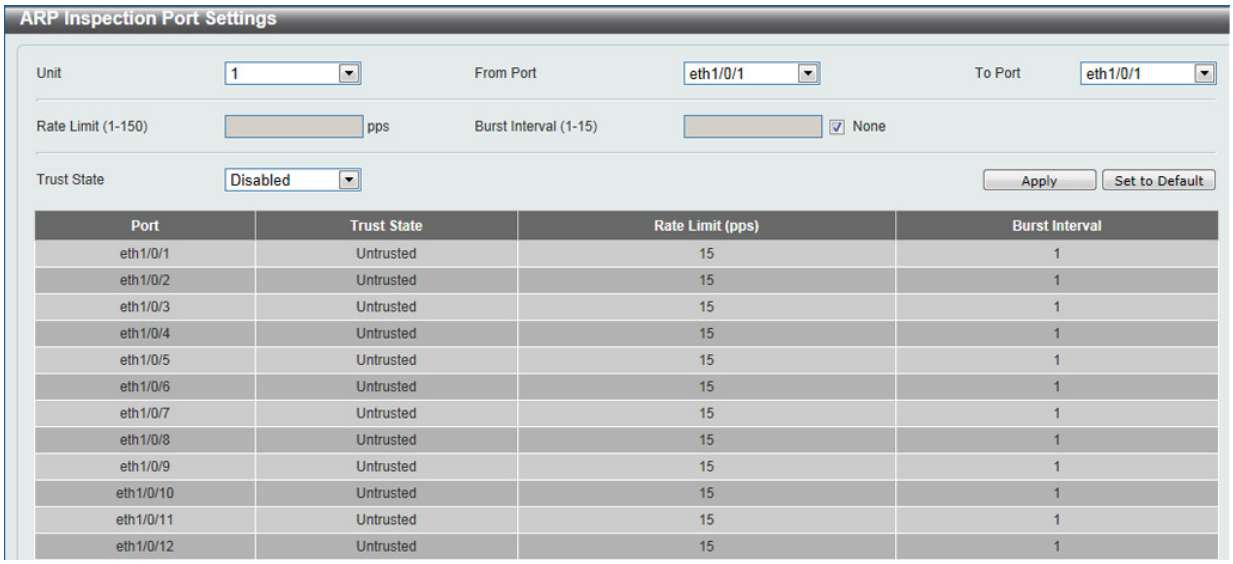


図 12-44　ARP Inspection Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。
Rate Limit	レート制限の値を入力します。1 から 150（パケット / 秒）の間で設定します。
Burst Interval	バーストインターバルの値を入力します。1 から 15 の間で設定します。「None」にチェックをするとオプションは無効になります。
Trust State	トラスト状態について有効 / 無効にします。

「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変更します。

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。

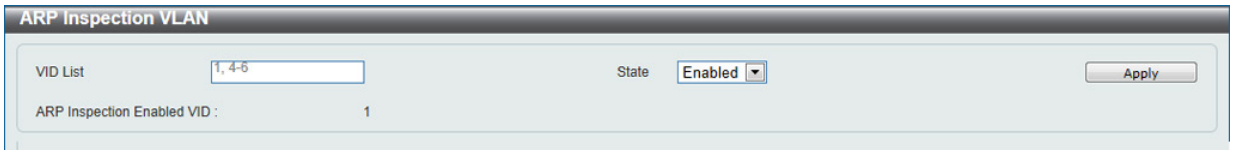


図 12-45　ARP Inspection VLAN 画面

本画面には以下の項目があります。

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。

「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。

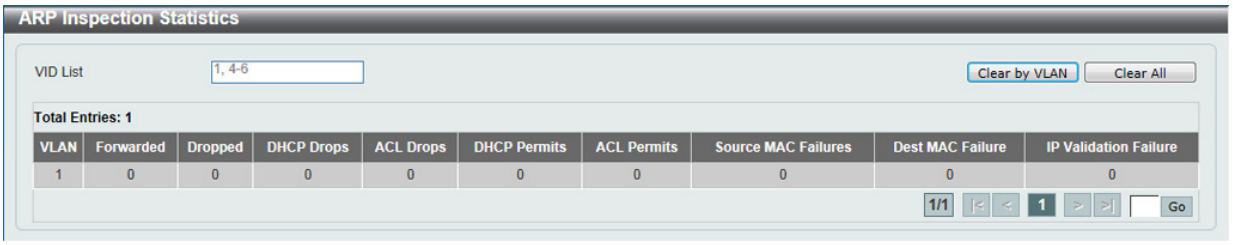


図 12-46 ARP Inspection Statistics 画面

本画面には以下の項目があります。

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、入力した VLAN ID についての情報を消去します。
「Clear All」ボタンをクリックし、テーブルのすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ARP Inspection Log（ARP インスペクションログ）

ARP インスペクションログ情報の表示、消去、設定を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log の順にクリックして、以下の画面を表示します。



図 12-47 ARP Inspection Log 画面

本画面には以下の項目があります。

項目	説明
Log Buffer	使用するログバッファの値を入力します。1 から 1024 の間で指定可能です。初期値は 32 です。

「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、ログを消去します。

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し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。

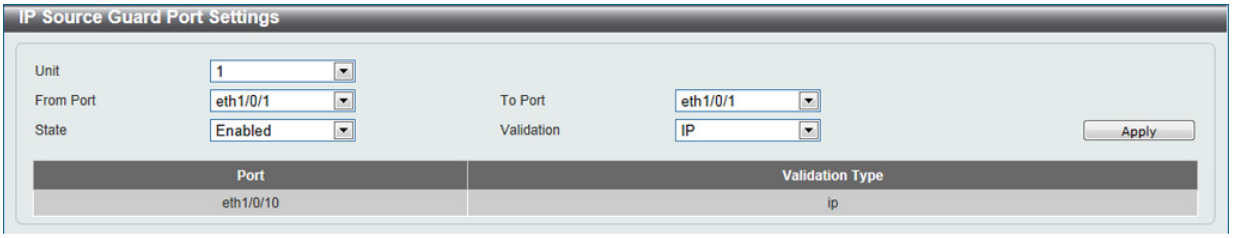


図 12-48 IP Source Guard Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。
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」「IP-MAC」から選択します。「IP」を選択すると受信パケットの IP アドレスがチェックされます。 「IP-MAC」を選択すると受信パケットの IP アドレスと MAC アドレスがチェックされます。

「Apply」ボタンをクリックし、設定内容を適用してください。

IP Source Guard VLAN Settings（IP ソースガード VLAN 設定）

IP ソースガード VLAN（IPSG VLAN）の表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard VLAN Settings の順にクリックして、以下の画面を表示します。

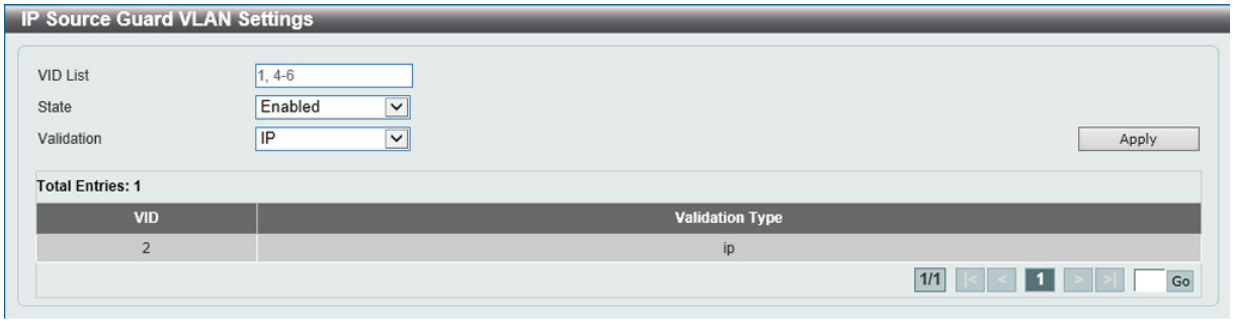


図 12-49 IP Source Guard VLAN Settings 画面

本画面には以下の項目があります。

項目	説明
VID List	VLAN ID 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」「IP-MAC」から選択します。「IP」を選択すると受信パケットの IP アドレスがチェックされます。 「IP-MAC」を選択すると受信パケットの IP アドレスと MAC アドレスがチェックされます。

「Apply」ボタンをクリックし、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。

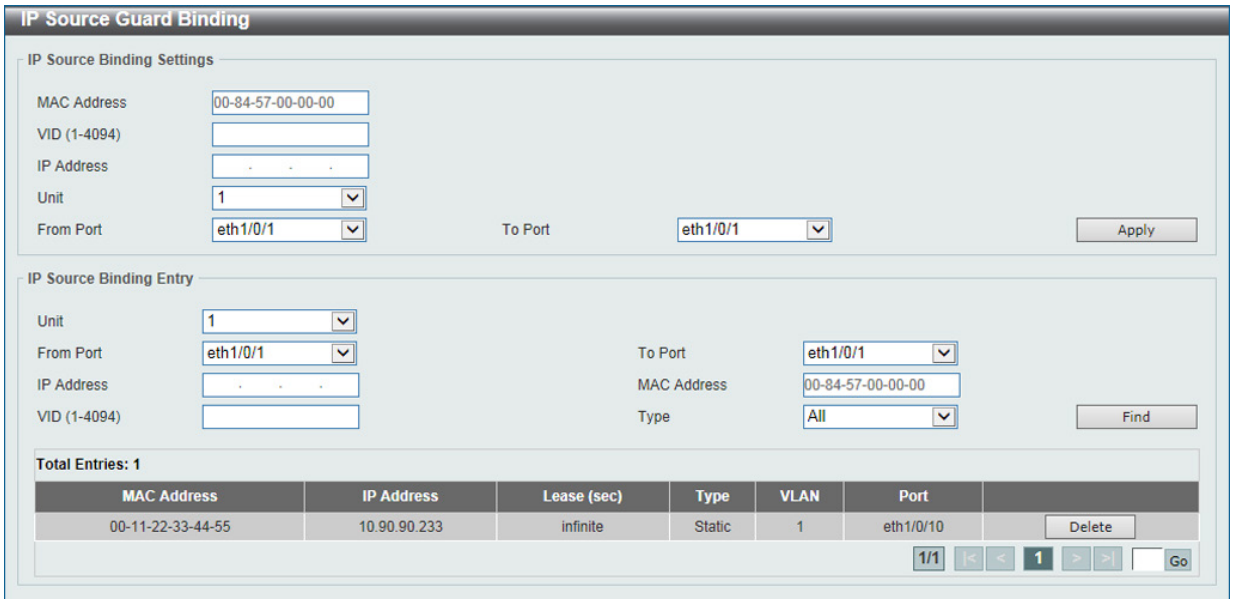


図 12-50 IP Source Guard Binding 画面

本画面には以下の項目があります。

項目	説明
IP Source Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
IP Address	バインディングエントリの IP アドレスを入力します。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

「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	
Unit	このクエリで設定するユニットを指定します。
From Port/ To Port	このクエリで選択したポートから連続した複数のポートを設定できます。
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」「DHCP Snooping」「Static」から選択します。「All」を選択するとすべての DHCP バインディングエントリが表示されます。「DHCP Snooping」を選択すると、DHCP バインディングスヌーピングに習得された IP ソースガードバインディングが表示されます。「Static」を選択すると手動で設定した IP ソースガードバインディングが表示されます。

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。
「Delete」をクリックして指定エントリを削除します。
「Find」をクリックして入力した情報を元に指定のエントリを表示します。

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 12-51　IP Source Guard HW Entry 画面

本画面には以下の項目があります。

項目	説明
Unit	このクエリで使用するユニットを指定します。
From Port/ To Port	このクエリで選択したポートから連続した複数のポートを設定できます。

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。
「Find」をクリックして入力した情報を元に指定のエントリを表示します。

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。

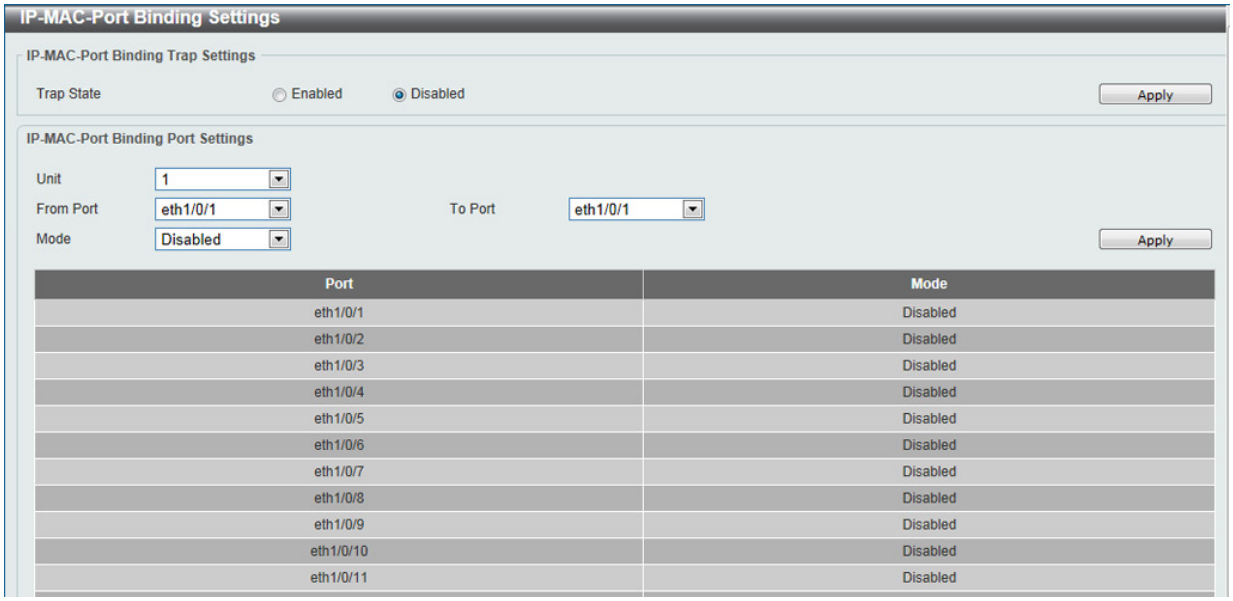


図 12-52 IP-MAC-Port Binding Settings 画面

本画面には以下の項目があります。

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。

「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 Port Settings	
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。
Mode	アクセスコントロールのモードを選択します。「Disabled」「Strict」「Loose」から選択します。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時は、ホストは ARP/IP パケット送信後にそれらの ARP/IP 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、そして受領ポート番号が、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 スヌーピングを習得したダイナミックバインディングエントリに定義されたエントリにマッチ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、ホストは ARP/IP パケット送信後にそれらの ARP/IP パケットがバインディングチェックを通過せず、ポートへのアクセスを拒否されます。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、そして受領ポート番号が、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 スヌーピングを習得したダイナミックバインディングエントリに定義されたエントリにマッチする必要があります。

設定後、「Apply」ボタンをクリックして設定を有効にします。

IP-MAC-Port Binding Blocked Entry（IP-MAC ポートバインディングブロックエントリ）

IP-MAC ポートバインディングブロックエントリの表示、消去を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry の順にクリックして、以下の画面を表示します。

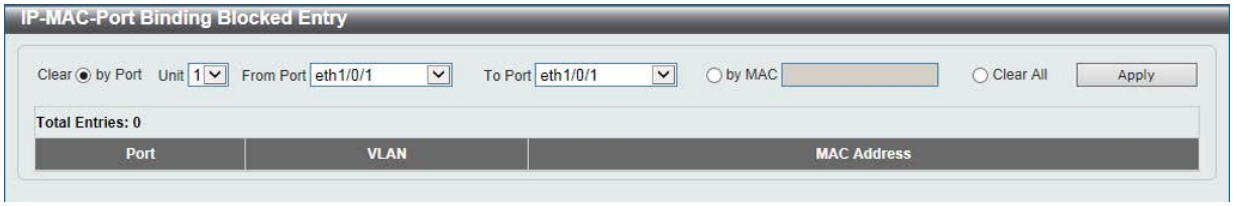


図 12-53 IP-MAC-Port Binding Blocked Entry 画面

本画面には以下の項目があります。

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にします。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。
Clear by MAC	MAC アドレスを含むエントリを消去します。項目欄にクリアされる MAC アドレスを入力します。
Clear All	MAC アドレスを含むすべてのエントリを消去します。

設定後、「Apply」ボタンをクリックして設定を有効にします。

IPv6

IPv6 Snooping（IPv6 スヌーピング）

IPv6 スヌーピングについて表示、設定します。

Security > IMPB > IPv6 > IPv6 Snooping の順にクリックして、以下の画面を表示します。

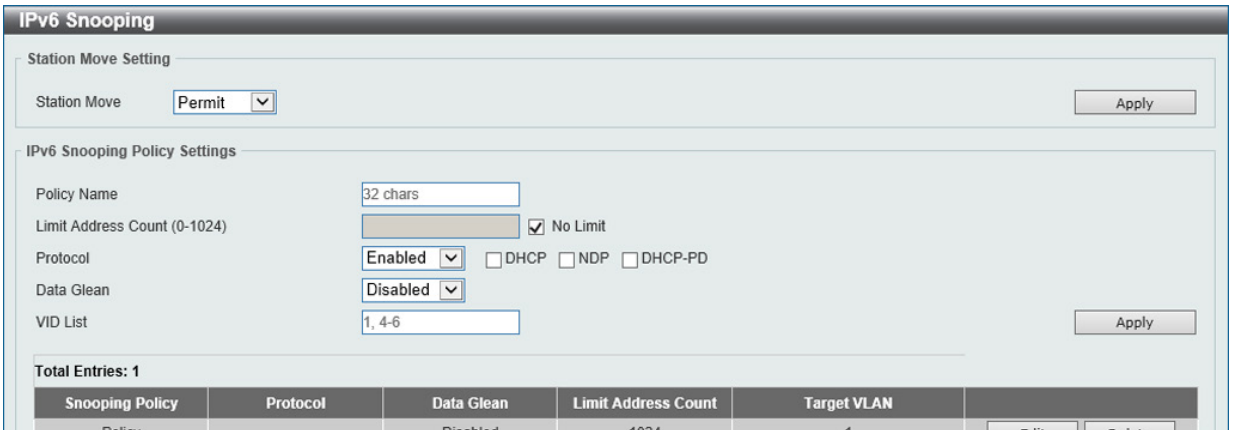


図 12-54 IPv6 Snooping 画面

本画面には以下の項目があります。

項目	説明
Station Move Setting	
Station Move	ステーション動作について設定します。「Permit」「Deny」から指定します。

「Apply」ボタンをクリックし、設定内容を適用してください。

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 文字内で指定可能です。
Limit Address Count	アドレスカウント制限の値を指定します。0 から 1024 まで指定可能です。 「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。
Protocol	本ポリシーに対応するプロトコルを選択します。「DHCP」「NDP」「DHCP-PD」から選択可能です。DHCPv6 スヌーピングはアドレス割り当ての段階での DHCPv6 クライアントとサーバ間の DHCPv6 パケットを傍受します。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 スヌーピングはステートレスな自動設定 IPv6 アドレスと手動設定 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) もまた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。
Data Glean	「data-glean」機能を有効 / 無効にします。ある状況下（DAD-NS パケットの喪失やスイッチの再起動）においては有効な 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。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Delete」をクリックして指定エントリを削除します。
「Edit」をクリックして指定エントリを編集します。

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。

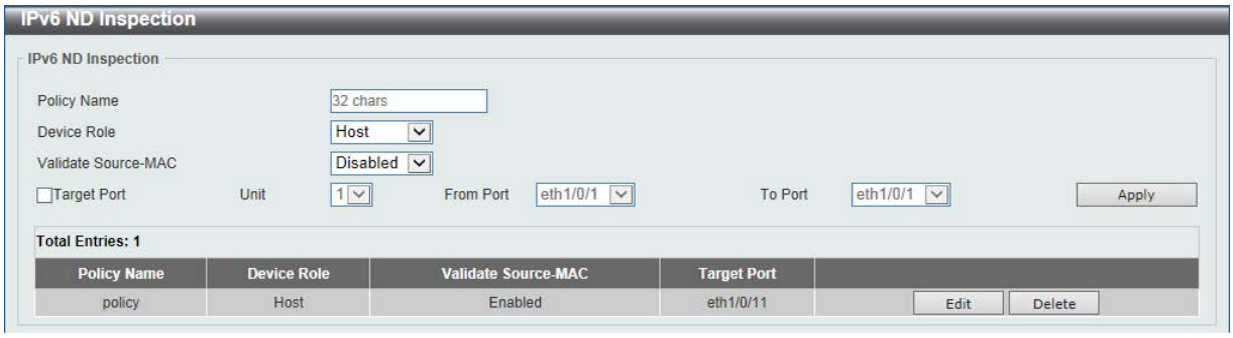


図 12-55 IPv6 ND Inspection 画面

本画面には以下の項目があります。

項目	説明
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Device Role	デバイスロールを選択します。「Host」「Router」から選択します。初期値では「Host」に設定され、NS、NA メッセージのインスペクションは動作します。「Router」を選択した場合、NS、NA のインスペクションは動作しません。NS/NA インスペクションを動作させるときは、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の妥当性の確認が必要です。
Validate Source-MAC	送信 MAC アドレスオプションの妥当性確認を有効 / 無効にします。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する送信元 MAC アドレスを確認します。リンクレイヤアドレスと MAC アドレスが違う場合、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	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Delete」をクリックして指定エントリを削除します。
「Edit」をクリックして指定エントリを編集します。

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。

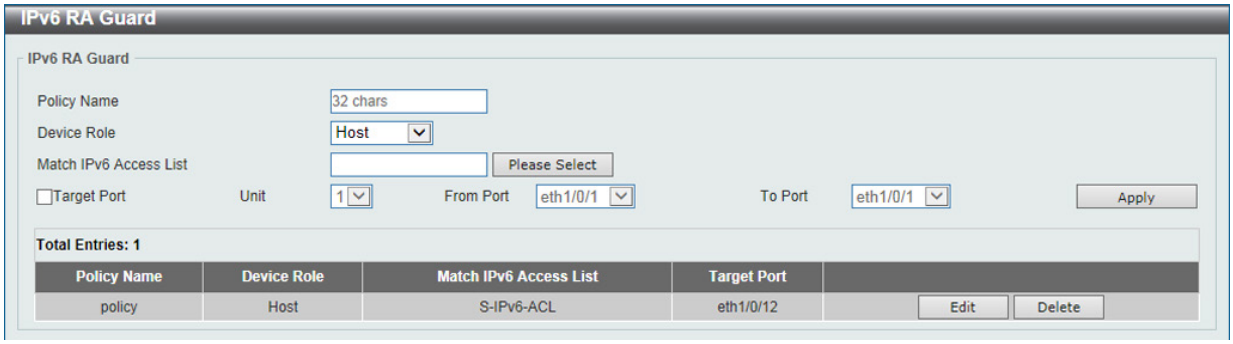


図 12-56 IPv6 RA Guard 画面

本画面には以下の項目があります。

項目	説明
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Device Role	デバイスロールを選択します。「Host」「Router」から選択します。初期値では「Host」に設定され、RA パケットはすべてブロックされます。「Router」を選択した場合、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	マッチさせる IPv6 アクセスリストを入力、選択します。

項目	説明
Target Port	チェックを入れターゲットポートを指定します。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Delete」をクリックして指定エントリを削除します。
「Edit」をクリックして指定エントリを編集します。
「Please Select」をクリックすると次の画面が表示されます。



図 12-57 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。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv6 DHCP Guard（IPv6 DHCP ガード）

IPv6 DHCP ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 DHCP Guard の順にクリックして、以下の画面を表示します。

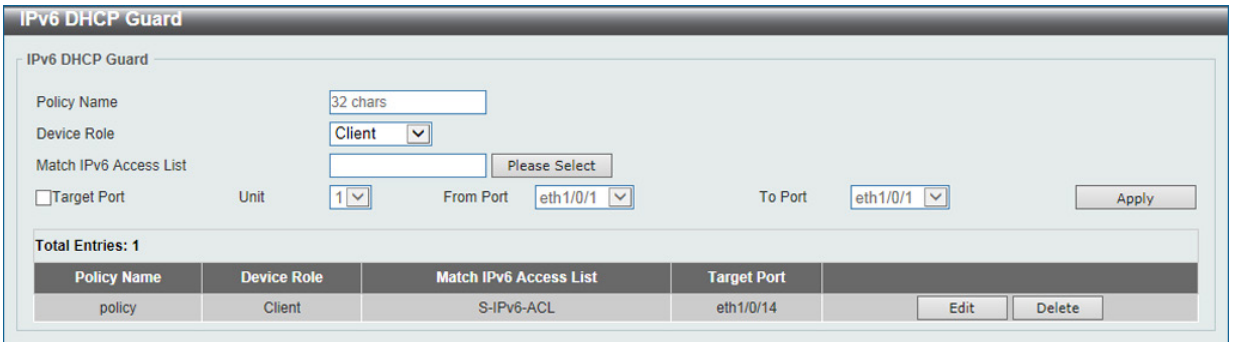


図 12-58 IPv6 DHCP Guard 画面

本画面には以下の項目があります。

項目	説明
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Device Role	デバイスロールを選択します。「Client」「Server」から選択します。初期値では「Client」に設定され、DHCPv6 サーバからの DHCPv6 パケットはすべてブロックされます。「Server」を選択した場合、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	マッチさせる 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、既存のエントリから選択します。
Target Port	チェックを入れターゲットポートを指定します。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Delete」をクリックして指定エントリを削除します。
「Edit」をクリックして指定エントリを編集します。

「Please Select」をクリックすると次の画面が表示されます。



図 12-59 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。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv6 Source Guard（IPv6 ソースガード）

IPv6 Source Guard Settings（IPv6 ソースガード設定）

IPv6 ソースガードの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings の順にクリックして、以下の画面を表示します。

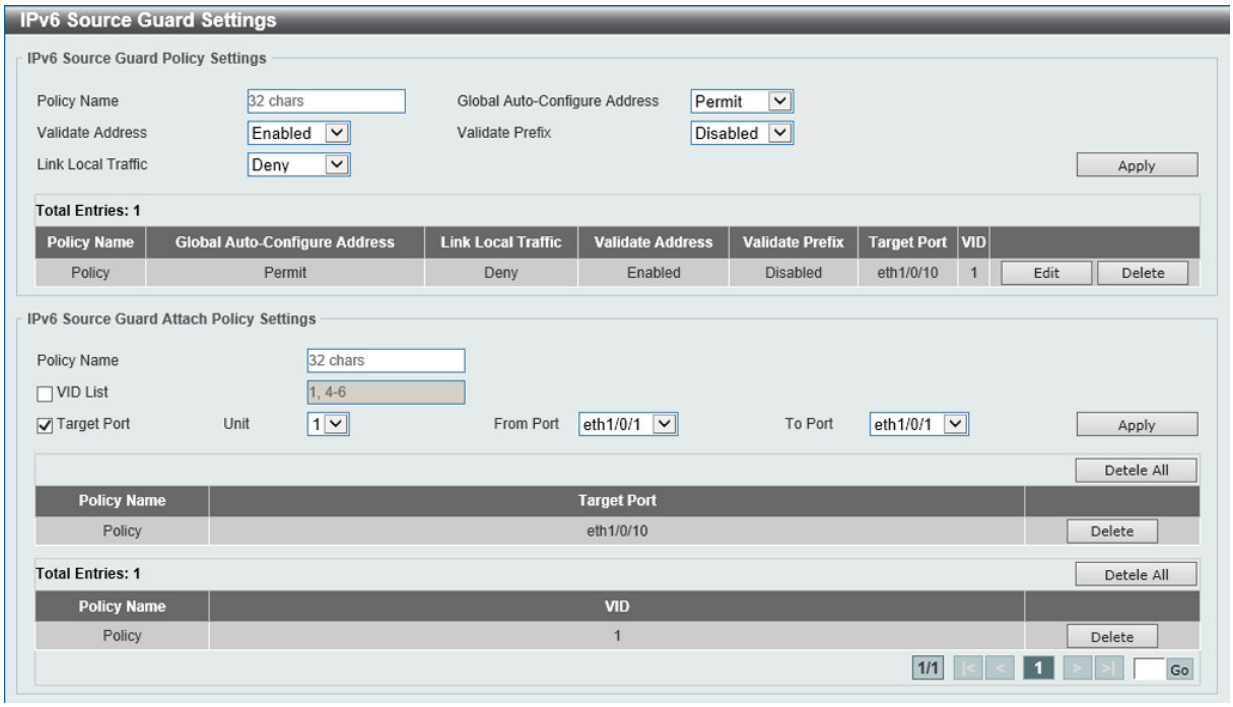


図 12-60 IPv6 Source Guard Settings 画面

本画面には以下の項目があります。

項目	説明
IPv6 Source Guard Policy Settings	
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
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。リンクのすべてのグローバルアドレスが DHCP と送信トラフィックから設定アドレスのホストをブロックしたい管理者よってアサインされている場合、有効です。
Validate Address	「validate（認証）」アドレス機能を有効 / 無効に指定します。IPv6 ソースガードで認証アドレス機能を有効にします。
Validate Prefix	「validate（認証）」プリフィクス機能を有効 / 無効に指定します。IPv6 ソースガードで IPv6 認証プリフィクス機能を有効に指定します。
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の許可 / 拒否を選択します。
IPv6 Source Guard Attach Policy Settings	
Policy Name	ポリシー名（32 文字まで）を指定します。
VID List	ターゲット VLAN の VLAN ID を指定します。

項目	説明
Target Port	ターゲットポートを指定します。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

「Apply」ボタンをクリックし、設定内容を適用してください。
「Edit」をクリックして、指定エントリの編集を行います。
「Delete」をクリックすると指定のエントリを削除します。

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。

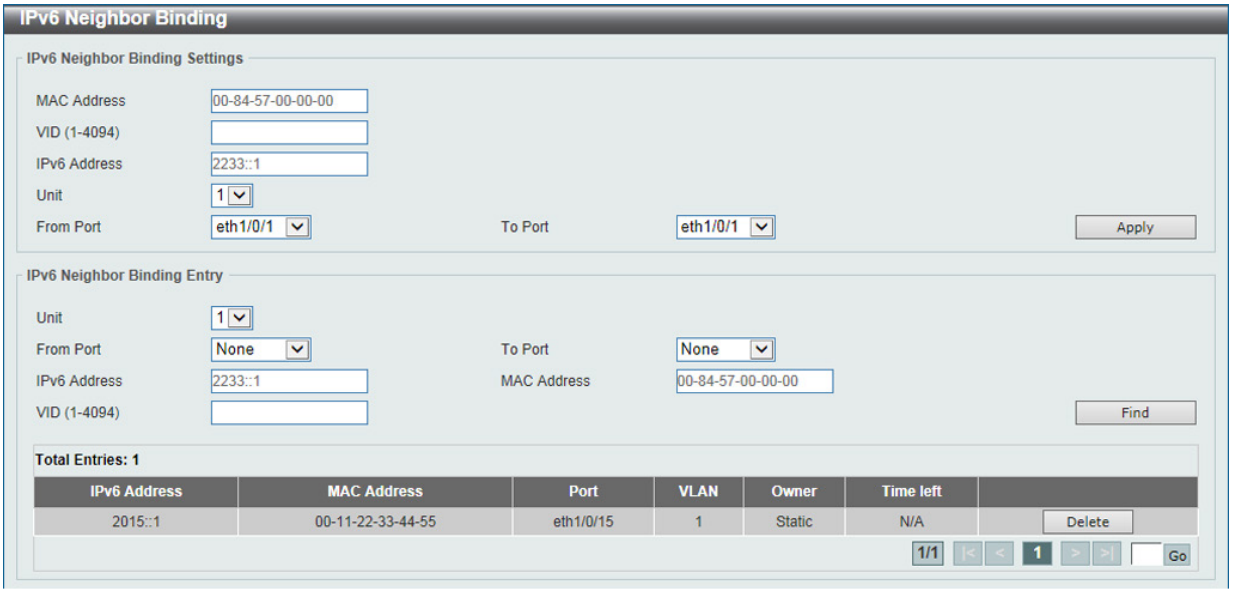


図 12-61　IPv6 Neighbor Binding 画面

本画面には以下の項目があります。

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。1 から 4094 の間で指定します。
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	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

「Apply」ボタンをクリックし、設定内容を適用してください。

IPv6 Neighbor Binding Entry	
Unit	このクエリで設定するユニットを指定します。
From Port/ To Port	このクエリで選択したポートから連続した複数のポートを設定できます。
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。
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	表示する VLAN ID を入力します。

「Delete」をクリックして指定エントリを削除します。
「Find」をクリックして入力した情報を元に指定のエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

DHCP Server Screening（DHCP サーバスクリーニング設定）

DHCP サーバ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。この DHCP サーバフィルタ機能が有効になると指定ポートからのすべての DHCP サーバパケットはフィルタされます。

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。

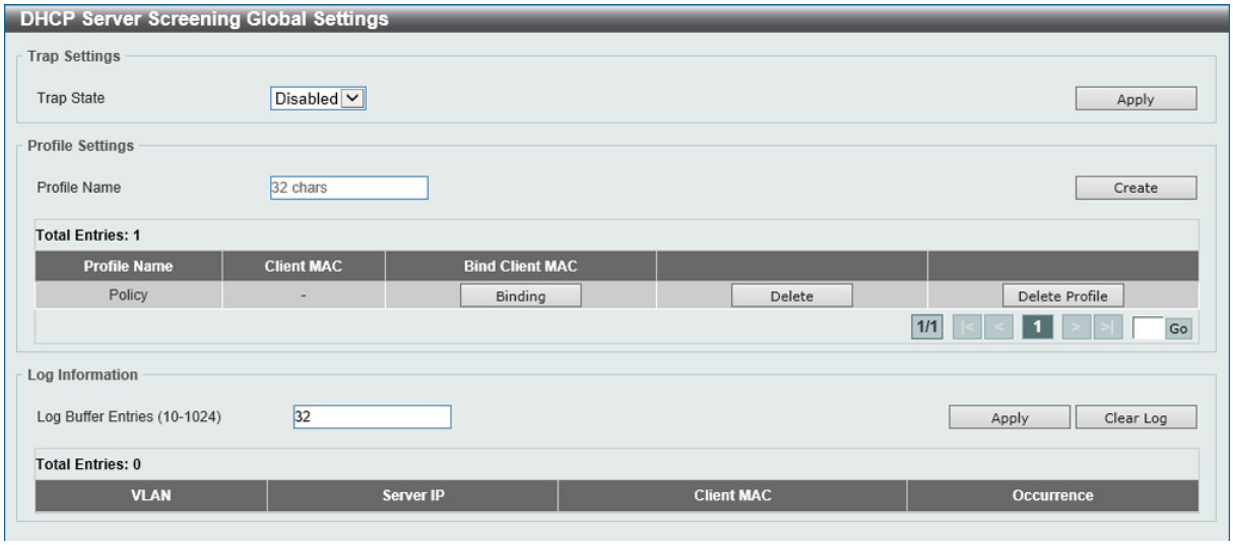


図 12-62 DHCP Server Screening Global Settings 画面

本画面には以下の項目があります。

項目	説明
Trap Settings	
Trap State	DHCP サーバスクリーニングトラップ機能を「Enabled」（有効）/「Disabled」（無効）にします。

「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	
Profile Name	プロファイル名を入力します。32 文字内で指定可能です。

「Create」ボタンをクリックし、設定内容にて作成します。
「Delete」をクリックして指定エントリを削除します。
「Delete Profile」をクリックして指定プロファイルを削除します。

Log Information	
Log Buffer Entries	ログバッファエントリ数を入力します。10 から 1024 までで指定します。初期値は 32 です。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Clear Log」ボタンをクリックしてログを消去します。

「Binding」ボタンをクリックすると以下の画面が表示されます。

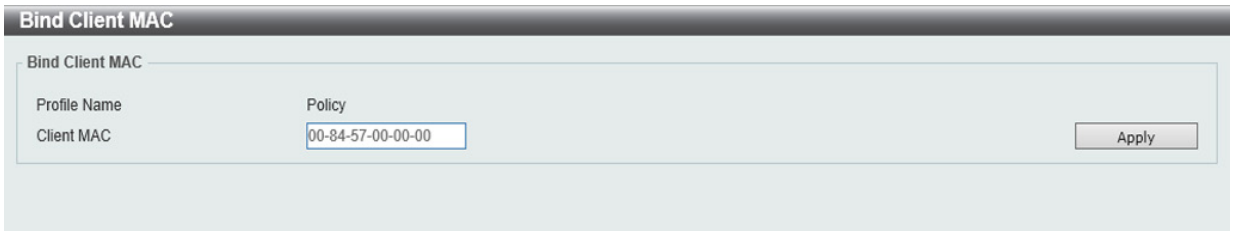


図 12-63 DHCP Server Screening Global Settings（Binding Client）画面

本画面には以下の項目があります。

項目	説明
Client MAC	使用する MAC アドレスを指定します。

設定後、「Apply」ボタンをクリックして設定を有効にします。

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。

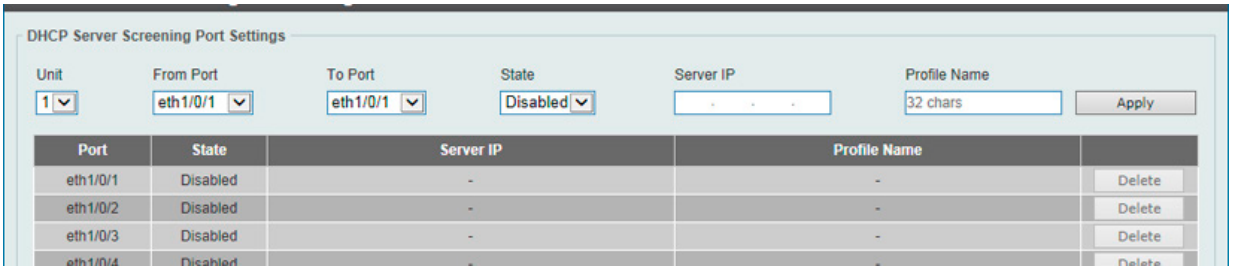


図 12-64 DHCP Server Screening Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	選択したポートから連続した複数のポートを設定できます。
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、入力した情報に基づいて指定エントリを削除します。

ARP Spoofing Prevention（ARP スプーフィング防止設定）

ユーザは保護されたゲートウェイに対し、MAC のスプーフィングを防ぐためにスプーフィング防止を設定することができます。エントリーが作成された場合に、送信先 ARP パケットはエントリのゲートウェイ IP にマッチしているが、送信先 MAC フィールドもしくは送信元 MAC フィールドのどちらかがエントリのゲートウェイ MAC と合致しない場合はシステムにより破棄されます。
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。もし ARP アドレスが設定したゲートウェイの IP アドレス、MAC アドレスそしてポートリストなどとマッチする場合、受信ポートが ARP トラストかどうかは関係なく Dynamic ARP Inspection (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。

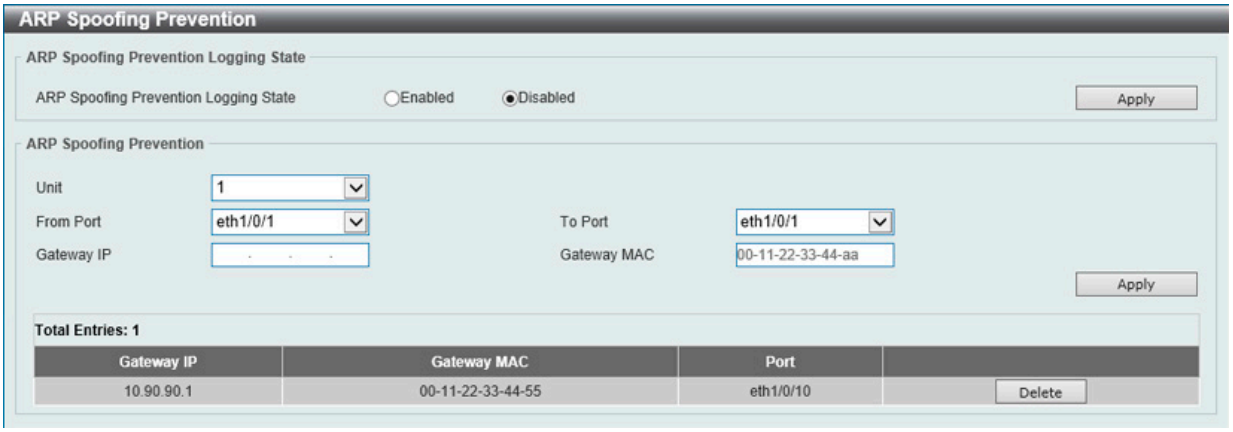


図 12-65 ARP Spoofing Prevention 画面

以下の項目を使用して、設定します。

項目	説明
ARP Spoofing Prevention Logging State	
ARP Spoofing Prevention Logging State	ARP スプーフィング防止ロギング状態を有効 / 無効に指定します。
ARP Spoofing Prevention	
Unit	設定するユニットを指定します。
From Port / To Port	選択したポートから連続した複数のポートを設定できます。
Gateway IP	ゲートウェイの IP アドレスを入力します。
Gateway MAC	ゲートウェイの MAC アドレスを入力します。

「Apply」ボタンをクリックし、変更を有効にします。
「Delete」ボタンをクリックして、指定エントリを削除します。

BPDU Attack Protection（BPDU アタック防止設定）

スイッチのポートにBPDU防止機能を設定します。通常、BPDU防止機能には2つの状態があります。1つは正常な状態で、もう1つはアタック状態です。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行います。このように、BPDU 防止は STP が無効なポートにだけ有効にすることができます。BPDU 防止では、「STP Port Settings」画面の「Forward BPDU」に設定したものより高い優先度を持っています。つまり、ポートが「STP Port Settings」画面の「Forward BPDU」に設定されており、BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

BPDU 防止では、BPDU の処理を決定するために設定した BPDU トンネルポートより高い優先度を持っています。つまり、ポートが「Tunnel STP Port(s)」で BPDU トンネルポートとして設定されていると、ポートは STP BPDU を転送します。しかし、ポートで BPDU 防止が有効であると、ポートは 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。

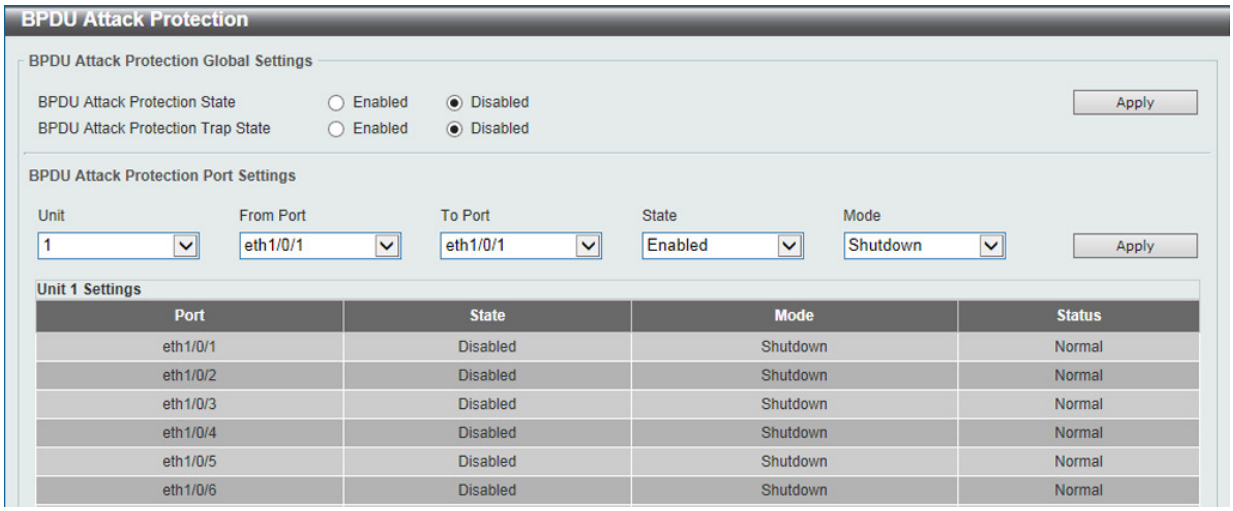


図 12-66　BPDU Attack Protection 画面

以下の項目を使用して、設定します。

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。初期値は無効です。
BPDU Attack Protection Trap State	トラップの状態を有効 / 無効にします。
Unit	設定するユニットを選択します。
From Port / To Port	設定を使用するポート範囲を選択します。
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すべての受信 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。

「Apply」ボタンをクリックし、変更を有効にします。

NetBIOS Filtering（NetBIOS フィルタリング設定）

本項目では NetBIOS フィルタリングの設定、表示を行います。

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

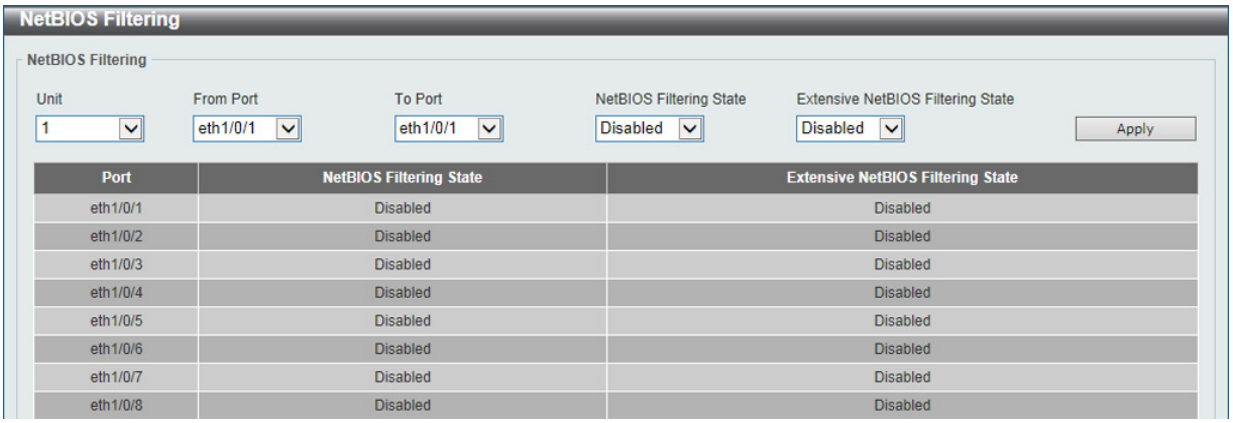


図 12-67　NetBIOS Filtering 画面

以下の項目を使用して、設定します。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
NetBIOS Filtering State	指定ポートでの NetBIOS フィルタリングを有効 / 無効に指定します。これにより物理ポートでの NetBIOS パケットが許可 / 拒否されます。
Extensive NetBIOS Filtering State	指定ポートでの Extensive NetBIOS フィルタリングを有効 / 無効に指定します。これにより物理ポートでの NetBIOS パケット over 802.3 フレームが許可 / 拒否されます。

「Apply」ボタンをクリックし、変更を有効にします。

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。
スイッチはローカル認証方式、RADIUS サーバ認証方式のどちらもサポートされています。MAC アドレス認証では MAC アドレス情報がローカルまたは RADIUS サーバに認証権限用にデータベース化されます。

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

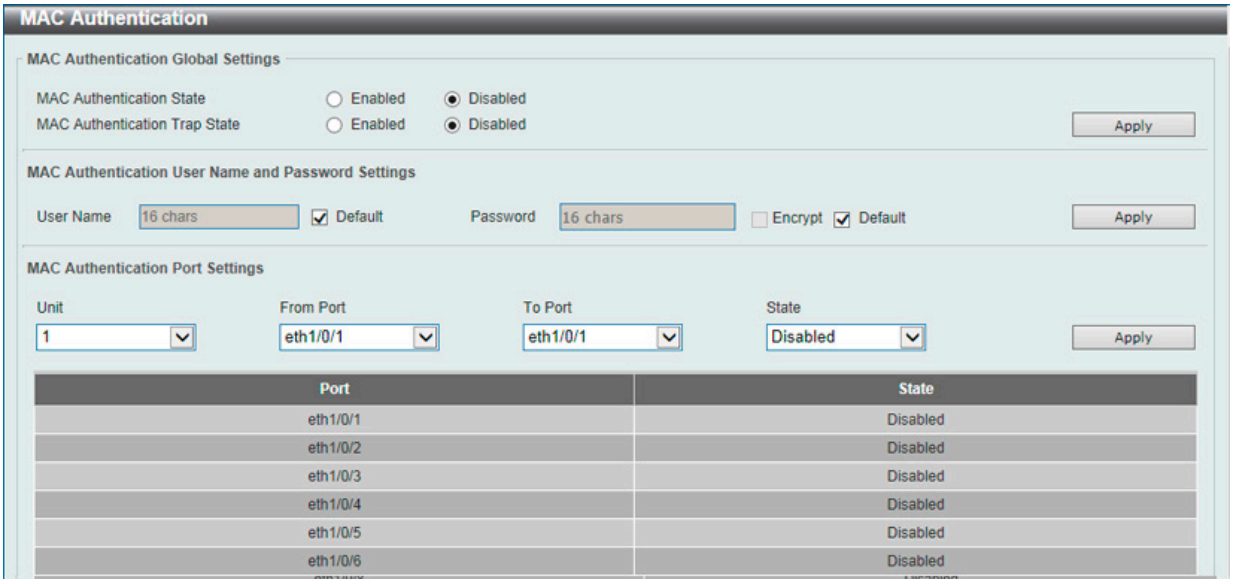


図 12-68　MAC Authentication 画面

以下の項目を参照、または設定可能です。

項目	説明
MAC Authentication Global Settings	
MAC Authentication State	「Enabled」（有効）または「Disabled」（無効）を選択し、スイッチの MAC 認証をグローバルに設定します。初期値は「Disabled」です。
MAC Authentication Trap State	MAC 認証のトラップのステータスを有効 / 無効にします。

「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 User Name and Password Settings	
User Name	MAC 認証のユーザ名を入力します。16 文字まで入力可能です。「Default」にチェックを入れるとクライアントの MAC アドレスが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。

「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 Port Settings	
Unit	設定するユニットを指定します。
From Port / To Port	選択したポートから連続した複数のポートを設定できます。
State	MAC 認証のポート指定を有効 / 無効にします。

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

Web-based Access Control（Web 認証）

Web ベース認証のログインは、スイッチを経由してインターネットにアクセスを試みる場合に、ユーザを認証するように設計された機能で、認証処理には HTTP/HTTPS プロトコルを使用します。Web ブラウザ経由で Web ページ (例 : 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。認証処理を通過するまで、ユーザはインターネットにアクセスすることはできません。

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

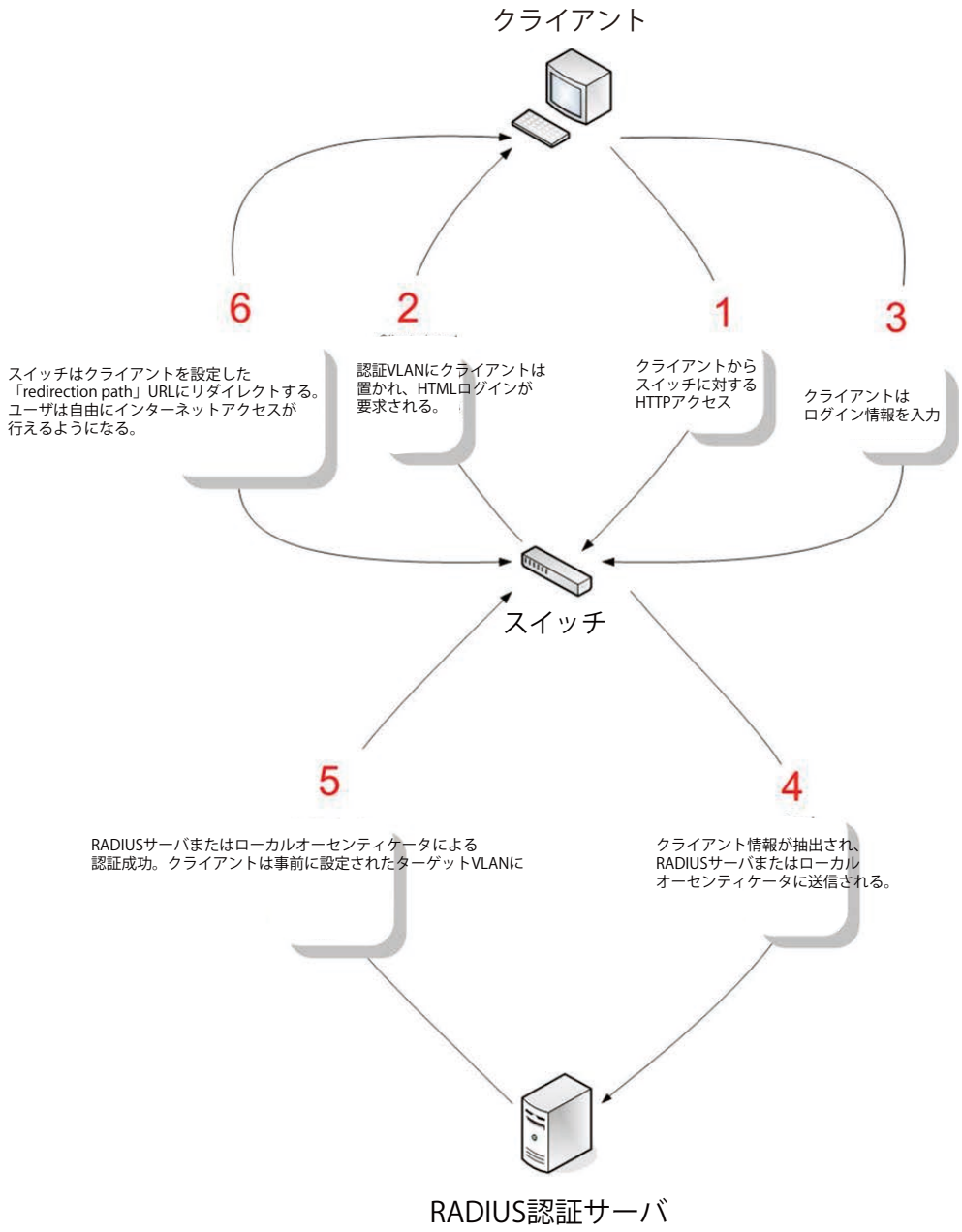
D-Link の WAC の実行には、WAC 機能が排他的に使用し、スイッチの他のモジュールに知られていない仮想 IP を使用します。実際は、スイッチの他の機能への影響を避ける場合にだけ、WAC は仮想 IP アドレスを使用してホストとの通信を行います。そのため、すべての認証要求を仮想 IP アドレスに送信し、スイッチの物理インタフェースの IP アドレスには送信しないようにする必要があります。

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

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

スイッチの WAC の実行は、ユーザ定義のポート番号により HTTP または HTTPS プロトコルのいずれかに対して TCP ポートを設定できることを特徴としています。HTTP か HTTPS に対するこの TCP ポートは、認証処理のために CPU にトラップされる HTTP か HTTPS パケットを識別するためやログインページにアクセスするために使用されます。指定しない場合、HTTP に対するポート番号の初期値は 80、HTTPS に対するポート番号の初期値は 443 となります。プロトコルも指定されないと、プロトコルの初期値は 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を実現させるために、認証に関わる各ノードで行われる基本の 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 アドレス取得のために DHCP を使用している場合、認証 VLAN はクライアントが IP アドレス取得を行えるように、DHCP サーバまたは DHCP リレー機能を持つ必要があります。
2. アクセスプロファイル機能のように、スイッチ上に存在する機能の中には HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
3. 認証に RADIUS サーバを使用する場合、Web 認証を有効にする前に、ターゲット VLAN を含む必要な項目を入力して RADIUS サーバの設定を行ってください。

注意 WAC/JWAC 認証では、System インタフェースが Up している必要があります。

Web Authentication（Web 認証設定）

スイッチの Web 認証設定をに行います。

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



図 12-69 Web Authentication 画面

以下の項目を使用して、設定を行います。

項目	説明
Web Authentication State	Web 認証機能を「Enable」（有効）/「Disable」（無効）にします。
Trap State	Web 認証のトラップの状態を有効 / 無効にします。
Virtual IPv4	仮想 IP アドレスを入力します。このアドレスは WAC にだけ使用され、スイッチの他のモジュールには知られません。すべての Web 認証のプロセスはこの IPv4 アドレスとの連携で行われますが、しかし仮想 IP はどの ICMP パケットや ARP リクエストにも応答しません。そのため仮想 IP はスイッチやホスト 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。でなければ Web 認証は正しく動作しません。設定した URL は仮想 IP アドレスが設定された後、有効になります。仮想 IP アドレス取得のために DNS サーバにストアされた FQDN URL をユーザは取得します。取得した IP アドレスは本コマンドで指定した仮想 IP アドレスと一致する必要があります。もし仮想 IPv4 アドレスが設定されない場合、IPv4 は Web 認証を開始することができません。
Virtual IPv6	仮想 IPv6 アドレスを入力します。もし仮想 IPv6 アドレスが設定されない場合、IPv6 は Web 認証を開始することができません。
Virtual URL	仮想 URL を指定します。128 文字以内で指定できます。
Redirection Path	認証に成功し、ターゲット VLAN に割り当てられたユーザを導く Web サイトの URL を入力します。128 文字以内で指定できます。

「Apply」ボタンをクリックし、設定を有効にします。

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

WAC Port Settings（Web 認証ポート設定）

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

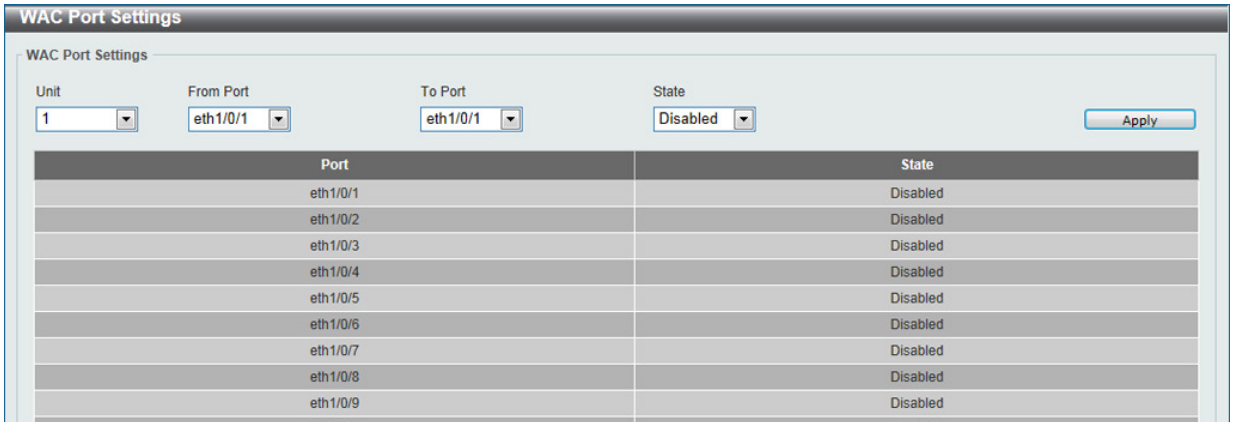


図 12-70 WAC Port Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポート範囲を設定します。
State	本機能を「Enabled」（有効）/「Disabled」（無効）にします。

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

WAC Customize Page（WAC カスタマイズページ設定）

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。

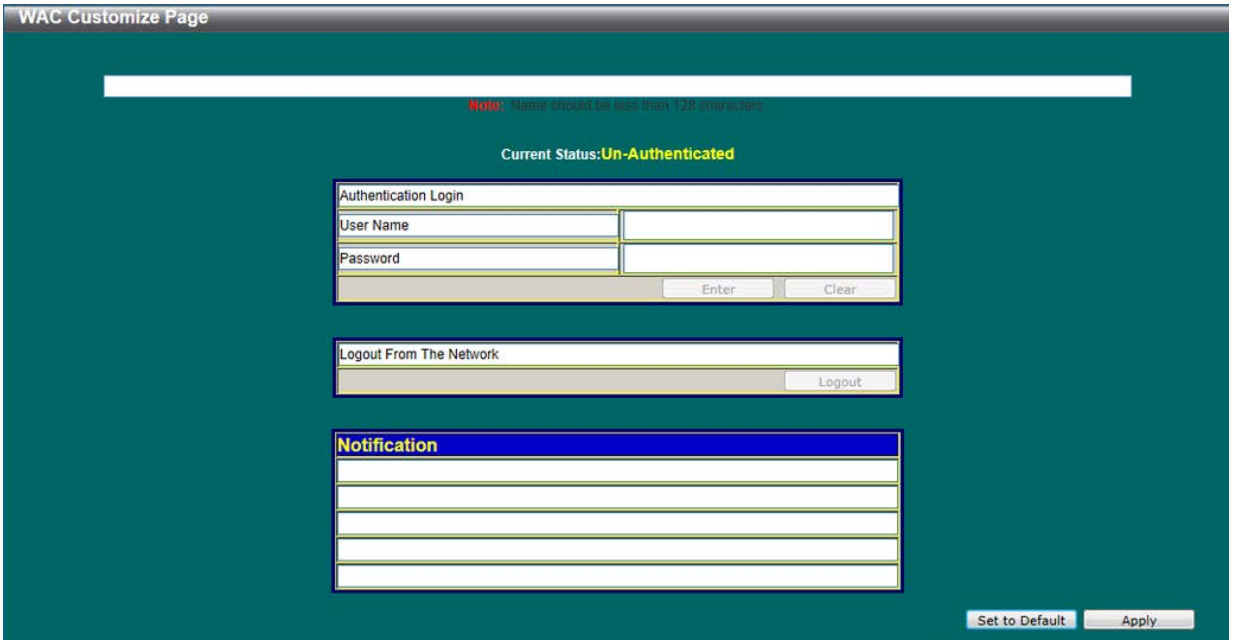


図 12-71　WAC Customize Page 画面

以下の項目を使用して、設定を行います。

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

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

Network Access Authentication（ネットワークアクセス認証）

Network Access Authentication（ネットワークアクセス認証）の設定を行います。

Guest VLAN（ゲスト VLAN 設定）

ネットワークアクセス認証のゲスト VLAN の表示、設定を行います。

Security > Network Access Authentication > Guest VLAN の順にメニューをクリックし、以下の画面を表示します。

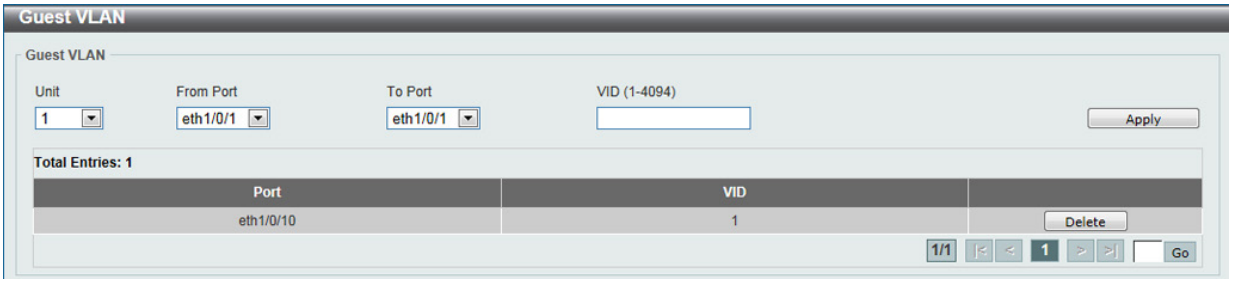


図 12-72　Guest VLAN 画面

以下の項目を使用して設定を行います。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
VID	設定する VLAN ID を入力します。1 から 4094 まで指定できます。

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

Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）

ネットワークアクセス認証のグローバルに設定します。

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。

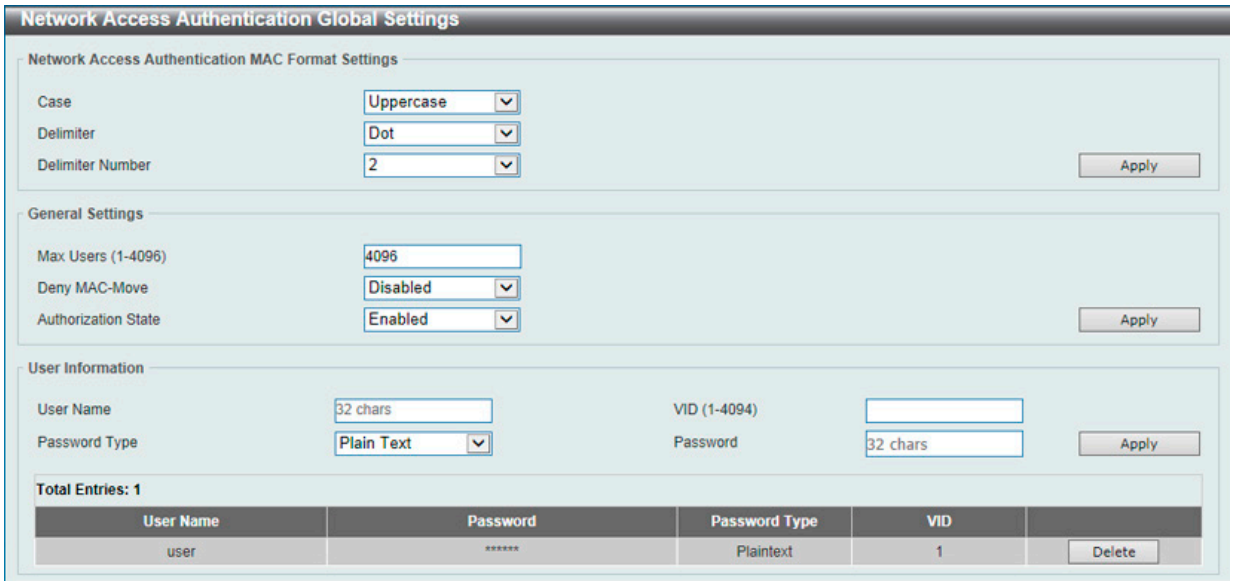


図 12-73　Network Access Authentication Global Settings 画面

本画面には以下の項目があります。

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「Uppercase」（大文字）または「Lowercase」（小文字）から選択します。
Delimiter	MAC アドレスを入力する際の区切り「Hyphen」（ハイフン）、「Colon」（コロン）または「Dot」（ドット）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。
Delimiter Number	MAC アドレスにおける区切り数を選択します。「1」「2」「5」から指定します。
General Settings	
Max Users	最大ユーザ数を指定します。1 から 1000 の間で指定できます。初期値は 1000 です。
Deny MAC-Move	「MAC-move」機能の拒否を有効 / 無効を指定します。 本オプションは認証ホストが複数スイッチポートのローミングする場合、指定ポートのみ認証される状態からポートを複数認証モードにして、ホストの認証ポートの移動を可能にする機能です。ホストによる認証ポート間の移動には二つの状況が考えられます。再認証が必要になるか次のルールに従い再認証なしで新しいポートへ直接移動します。もし新しいポートが元々のポートと同じ認証設定であれば、再認証は不要です。ホストは新しいポートに同じ認証属性を引き継ぎます。認証ホストはポート 1 からポート 2 へローミングができ、再認証なしで認証属性を引き継ぎます。もし新しいポートが元々のポートと違う認証設定の場合、再認証の必要があります。ポート 1 の認証ホストはポート 2 へ移動して再認証を受けます。もし新しいポートが認証方式を有効にしていない場合、ステーションは直接新しいポートへ移動させられます。そして元々のポートとのセッションは削除されます。ポート 1 の認証ホストはポート 2 へ移動可能です。 本機能が無効の場合、認証ホストは他のポートへ移動可能ですが違反エラーとして認識されます。
Authorization State	認証について有効 / 無効に指定します。本オプションについては権限設定の受容の有効 / 無効に使用されます。権限への認証が有効になると、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、権限が有効になると許容されます。「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。しかし「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 文字まで入力可能です。
VID	VLAN ID を入力します。
Password Type	パスワード種類を選択します。「Plain Text」「Encrypted」から選択可能です。
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、指定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。

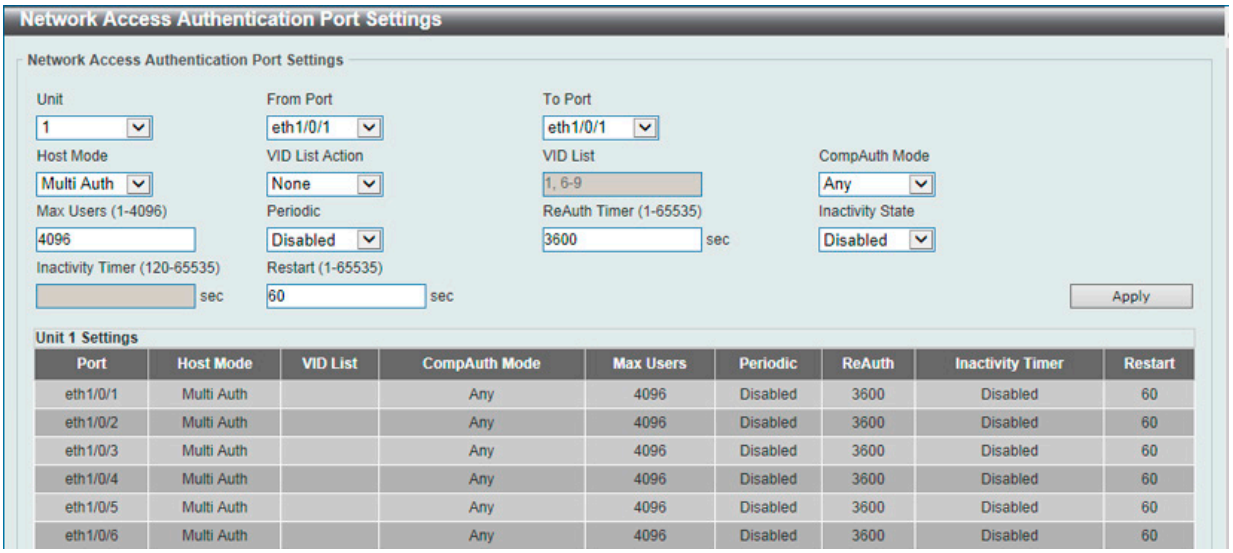


図 12-74　Network Access Authentication Port Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Host Mode	選択ポートと関連するホストモードを選択します。「Multi Host」「Multi Auth」から選択します。ポートがマルチホストモードで動作していて一つのホストが認証されている場合、すべての他のホストはポートへのアクセスを許可されます。802.1X 認証に従い、再認証失敗や認証ユーザーのログオフなどの場合、ポートはしばらくの間ブロックされます。一定期間終了後 EAPOL パケットのプロセスにてポートはリストアします。ポートがマルチ認証モードで動作しており、各ホストがポートへのアクセスに認証が必要な場合、ホストは MAC アドレスとして認識され、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	ホストモードでマルチ認証オプションを選択した後、次の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。これは複数の認証要件があるスイッチの複数 VLAN に有効です。クライアントが認証されたのちに、クライアントは他の VLAN に受信をしても再認証されません。これは各 VLAN の認証コントロールを行うトランクポートにとって有効です。ポートの認証モードがマルチホストに変更された場合、ポートにある以前の認証 VLAN はクリアされます。
CompAuth Mode	コンパウンド認証モードのオプションを選択します。「Any」「MAC-WAC」から選択します。「Any」を選択すると、あらゆる認証方式（802.1X, MAC-based Access Control, WAC）でのアクセスを指定します。「MAC-WAC」を選択すると MAC ベースの認証を最初に検証します。クライアントがパスをすると、WAC が次に検証され、最終的には両方が認証がパスされる必要があります。
Max Users	最大ユーザ数を指定します。1 から 1000 の間で指定できます。
Periodic	選択ポートの定期再認証を有効 / 無効にします。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。1 から 65535（秒）で指定します。初期値では 3600 秒です。
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。120 から 65535（秒）です。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。
Restart	リスタート時間を入力します。1 から 65535（秒）の間で指定可能です。

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

Network Access Authentication 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。

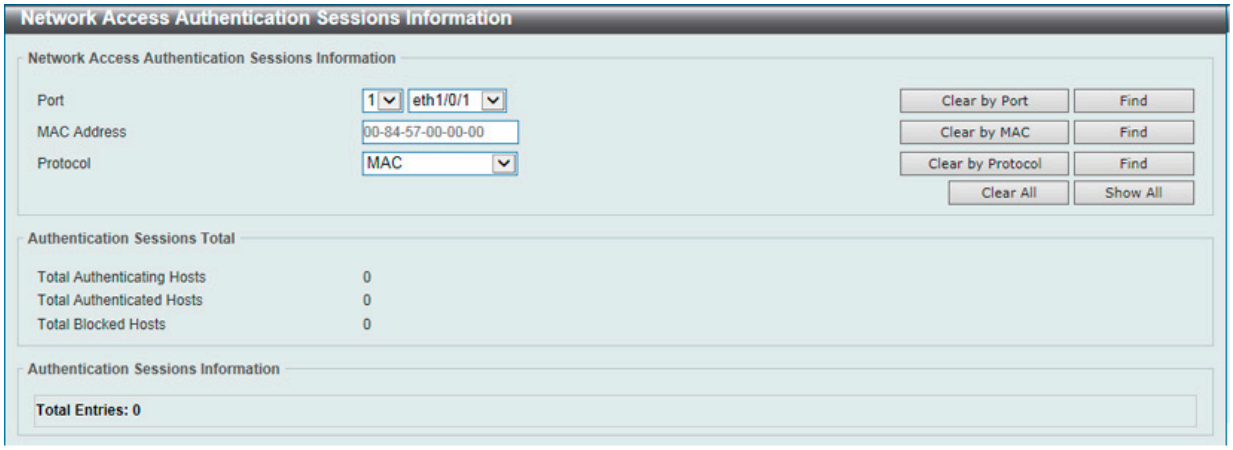


図 12-75　Network Access Authentication Sessions Information 画面

以下の項目を使用して設定を行います。

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。「MAC」「WAC」「JWAC」「DOT1X」から選択します。

「Apply」ボタンをクリックし、設定を有効にします。
「Clear by Port」ボタンをクリックし、選択したポートに基づく情報を消去します。
「Clear by MAC」ボタンをクリックし、選択した MAC アドレスに基づく情報を消去します。
「Clear 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。
「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 はその対応量を超えて増加してしまう可能性があります。このような問題を軽減するために、本スイッチのソフトウェアにセーフガードエンジン機能を付加しました。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。省パワーモード（exhausted mode）の場合、スイッチは ARP と IP パケットのための帯域を制限します。もし CPU の稼働がしきい値以下に下がった場合、セーフガードエンジンは動作を停止しスイッチは省パワーモードを脱却し通常モードへ移行します。

CPU に宛てられるパケットは 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認識するうえで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」があります。通常、「Protocol」グループは、スイッチの CPU プロセスがパケットを受信した時に、最高のプライオリティ受信し、そして「Route」グループは、スイッチの CPU が入り込むルーティングパケットのプロセスの中で、グループの最低の優先値を受信します。「Protocol」グループでの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。管理（Manage）グループ内で、パケットは Telent や SSH と同様に、インタラクティブアクセスプロトコルの内容でルータやシステムネットワークマネジメントインタフェースへ向かいます。「Route」グループではパケットは 通常ルータ CPU トラバース（行ったり来たり）するルート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)
BGP	Protocol	Border Gateway Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol（DHCP）
DNS	Protocol	Domain Name System（DNS）
DVMRP	Protocol	Distance Vector Multicast Routing Protocol

プロトコル名	サブインタフェース（グループ）	概要
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。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に注意しなければいけないのは、本機能を使用して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。

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、さまざまなトラフィックフロー（ARP、IP）に帯域幅を割り当てます。これは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うためには、**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。

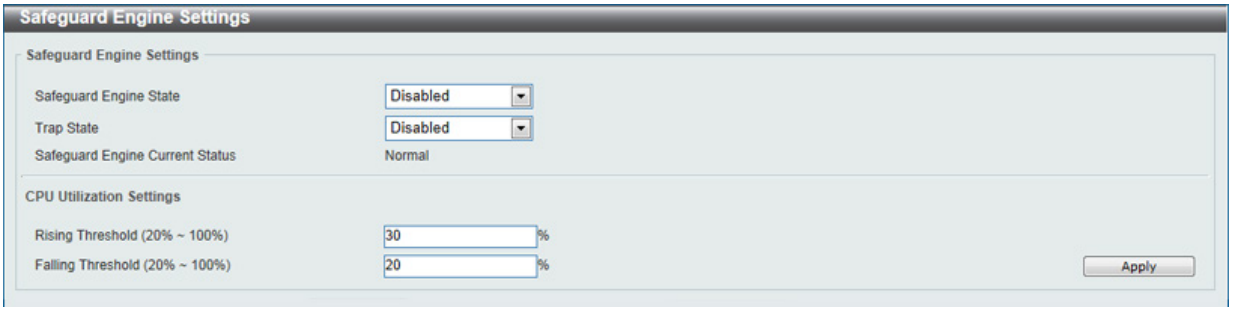


図 12-76 Safeguard Engine Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Safeguard Engine Settings	
Safeguard Engine State	セーフガードエンジン機能を「Enabled」（有効）/「Disabled」（無効）にします。
Trap State	セーフガードエンジントラップを「Enabled」（有効）/「Disabled」（無効）にします。
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 (20% ~ 100%)	Safeguard Engine を有効にする前に許容可能な CPU 使用率のレベルを設定します。CPU 使用率がこのしきい値に到達すると、ここで設定した項目に基づいて、Exhausted モードに入ります。
Falling Threshold (20% ~ 100%)	許容可能な CPU 使用率のレベルを設定します。スイッチは CPU 使用率がこのしきい値に到達すると Safeguard Engine 状態から Normal モードに戻ります。

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。

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。

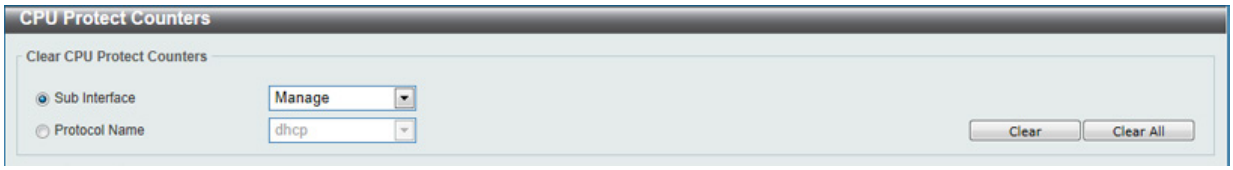


図 12-77 CPU Protect Counters 画面

以下の項目を使用して、設定を行います。

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。「Manage」「Protocol」「Route」「All」から選択します。 CPU プロテクトに関連したサブインタフェースのカウンタの消去を指定します。
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、設定に基づいた情報を消去します。

「Clear All」ボタンをクリックし、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 12-78 CPU Protect Sub-Interface 画面

以下の項目を使用して、設定を行います。

項目	説明
CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）	
Sub Interface	サブインタフェースのオプションを選択します。「Manage」「Protocol」「Route」から選択します。
Rate Limit	レートリミットの値を入力します。0 から 1024 パケット / 毎秒の間で指定できます。 「No Limit」を指定するとレートリミットを無効にします。

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

項目	説明
Sub-Interface Information（サブインタフェース情報）	
Sub Interface	サブインタフェースのオプションを選択します。「Manage」「Protocol」「Route」から選択します。

「Find」ボタンをクリックし、入力した情報を元に指定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。

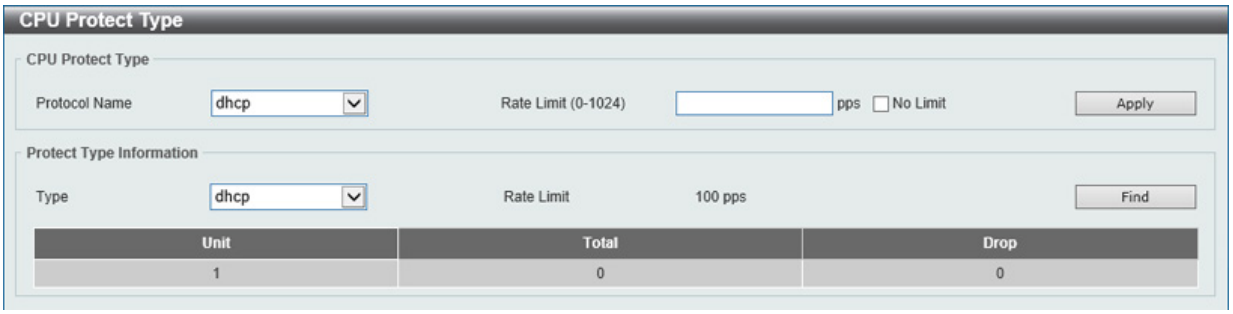


図 12-79 CPU Protect Type 画面

以下の項目を使用して、設定を行います。

項目	説明
CPU Protect Type（CPU プロテクトタイプ）	
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。0 から 1024 パケット / 毎秒の間で指定できます。 「No Limit」を指定するとレートリミットを無効にします。

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

項目	説明
Protect Type Information（プロテクトタイプ情報）	
Type	プロトコルタイプを選択します。選択するとアサインするレートリミットの値が表示されます。 「unit」を選択した場合、物理スタックのユニット ID を選択します。

「Find」ボタンをクリックし、入力した情報を元に指定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。

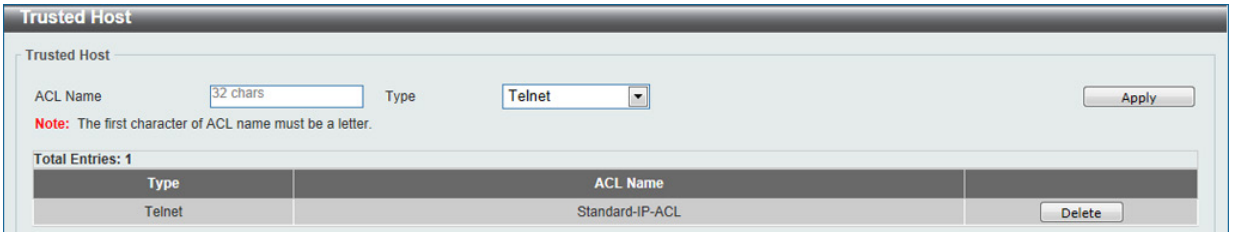


図 12-80 Trusted Host 画面

以下の項目を使用して、設定を行います。

項目	説明
ACL Name	使用する ACL 名を入力します。32 文字までで指定可能です。
Type	トラストホストの種類を指定します。「Telnet」「SSH」「Ping」「HTTP」「HTTPS」から指定します。

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

「Delete」をクリックして指定のエントリを削除します。

Traffic Segmentation（トラフィックセグメンテーション）

トラフィックセグメンテーション機能は、（単一 / 複数）ポート間のトラフィックの流れを制限するために使用します。「トラフィックフローの分割」という方法は、「VLAN によるトラフィック制限」に似ていますが、さらに制限的です。本機能によりマスタスイッチ CPU のオーバヘッドを増加させないようにトラフィックを操作することが可能です。

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

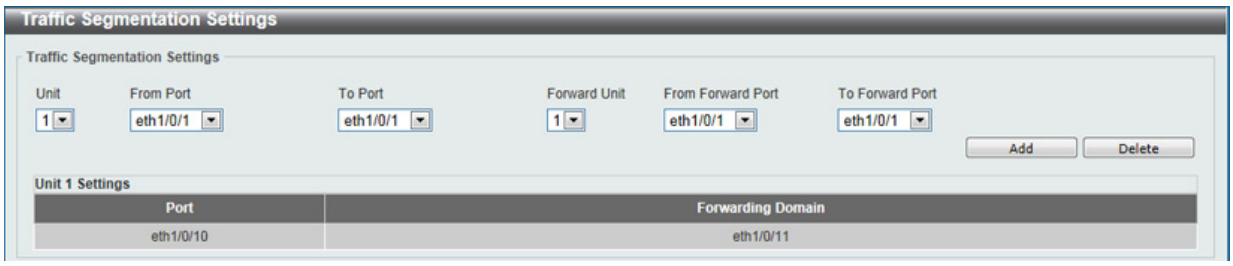


図 12-81　Traffic Segmentation 画面

以下の項目を使用して設定を行います。

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

Storm Control Settings（ストームコントロール設定）

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。

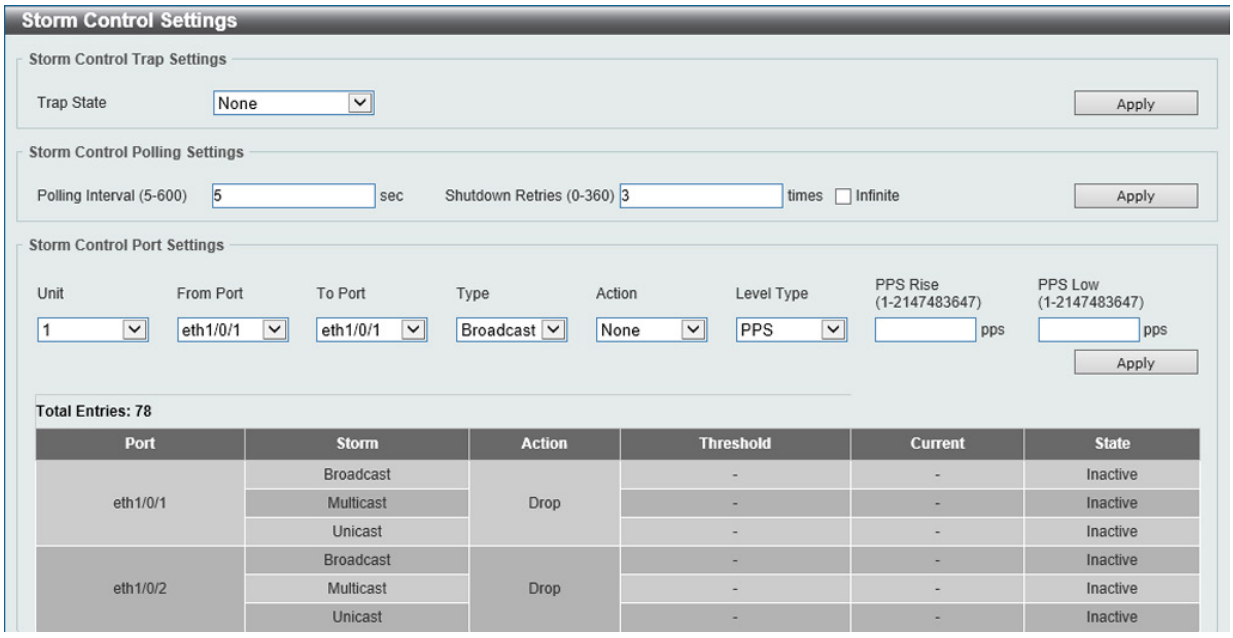


図 12-82　Storm Control Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Storm Control Trap Settings（ストームコントロールトラップ設定）	
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」「Storm Occur」「Storm Clear」「Both」から指定できます。「None」が選択されるとトラップは送信されません。「Storm Occur」が選択されると、ストームの発生を検出した時点でトラップは通知されます。「Storm Clear」が選択されるとストームが解消された時点でトラップは通知されます。

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。

項目	説明
Storm Control Polling Settings（ストームコントロールポーリング設定）	
Polling Interval	インターバルの値を指定します。5 から 600（秒）で指定できます。初期値は 5 秒です。
Shutdown Retries	再試行の値を入力します。0 から 360 で指定できます。初期値は 3 です。「Infinite」にチェックを入れると本機能は無効になります。

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

項目	説明
Storm Control Port Settings（ストームコントロールポート設定）	
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Type	コントロールするストームの種類を選択します。「Broadcast」「Multicast」「Unicast」から指定できます。シャットダウンモードで選択すると、ユニキャストは「Known」「Unknown」両方が設定してある場合、どちらにも対応しポートはシャットダウンします。そうでない場合は「Unknown」にのみ対応します。
Action	動作について指定します。「None」「Shutdown」「Drop」から指定します。「None」を指定するとストームパケットをフィルタしません。「Shutdown」は選択すると、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」を選択すると指定したしきい値に達するとパケットを破棄します。
Level Type	レベルタイプを指定します。「PPS」「Kbps」「Level」から選択します。
PPS Rise	毎秒のパケット増加の上限値について指定します。毎秒増加するパケットの量について上限しきい値を指定します。0 から 2147483647 パケット毎秒で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。
PPS Low	毎秒のパケット減少の下限値について指定します。毎秒減少するパケットの量について下限しきい値を指定します。0 から 2147483647 パケット毎秒で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。

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。

「Level Type」で「Kbps」を選択すると、以下の画面が表示されます。

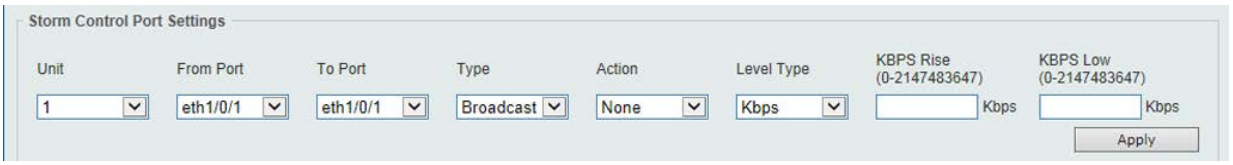


図 12-83 Storm Control (Kbps) 画面

項目	説明
KBPS Rise	上限 KBPS の値を指定します。ポートに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。0 から 2147483647 Kbps の間で指定できます。
KBPS Low	下限 KBPS の値を指定します。ポートに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。0 から 2147483647 Kbps の間で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。

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。

「Level Type」で「Level」を選択すると、以下の画面が表示されます。

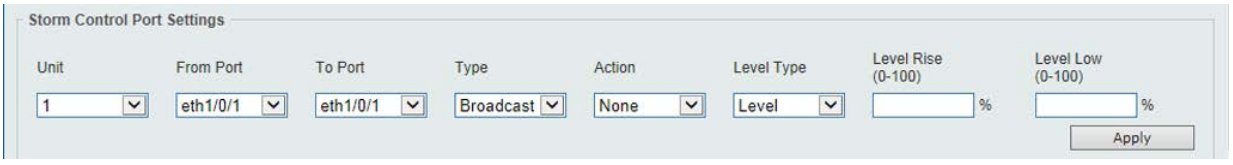


図 12-84 Storm Control (Level) 画面

項目	説明
Level Rise	下限レベルについて入力します。本オプションはポートに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。0 から 100%で指定可能です。
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に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。0 から 100%で指定可能です。「Level Low」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。

注意 Level に 0 を指定した場合、H/W Entry が作成されるまでの間、スイッチは対象の通信を許可します。

注意 Multicast を指定した場合、予約 MAC Address(VRRP、OSPF、IGMP、MLD など) に対する制限は適用されません。

注意 % および kbps を指定した場合は、受信 Frame Size を　64 Octet 固定長とし、Packet per second に基づいて表示するため、状態を正しく反映しません。

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。

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。

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。

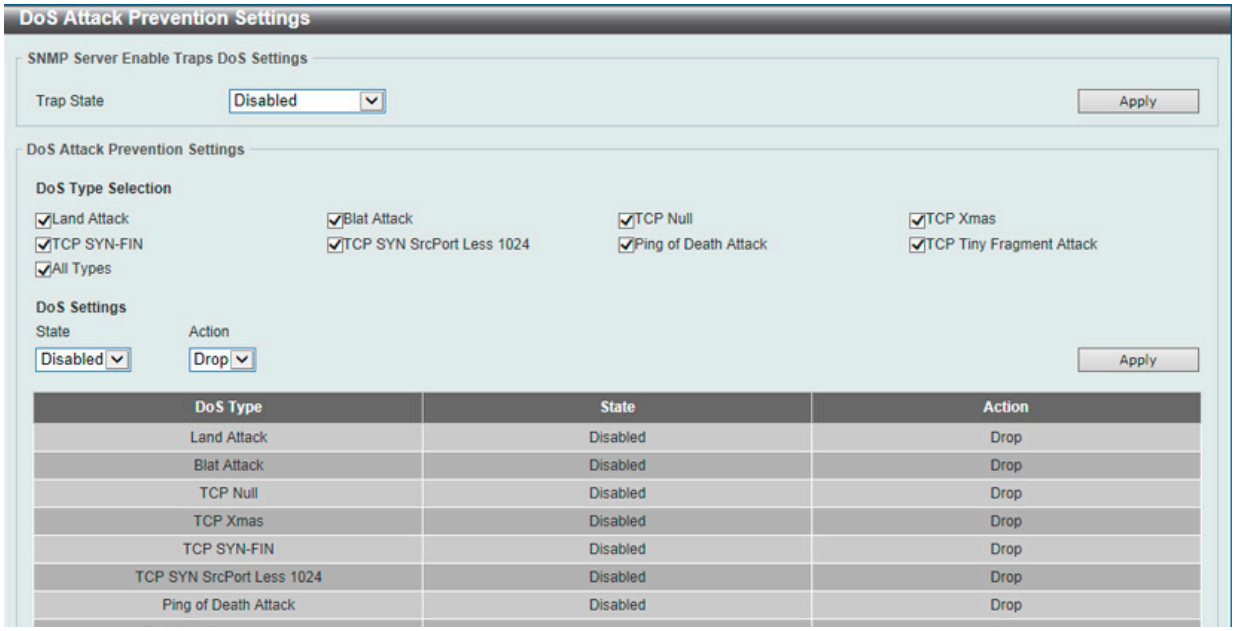


図 12-85　DoS Attack Prevention Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
SNMP Server Enable Traps DoS Settings	
Trap State	本オプションは、DoS 攻撃防止トラップ状態を有効または無効にします。
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 攻撃防止の状態を指定します。 • Enabled - DoS 攻撃防止の状態を有効にします。 • Disabled - DoS 攻撃防止の状態を無効にします。
Action	DoS 攻撃防止機能により行われる操作を無効にします。 • Drop - 一致する DoS 攻撃パケットをすべて破棄します。

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

Zone Defense Settings（ゾーンディフェンス設定）

「ゾーンディフェンス（Zone Defense）」機能の設定と表示を行います。ゾーンディフェンスが有効な場合、ACL リソースがゾーンディフェンスのために使用されます。十分な ACL リソースがない場合は、本機能を有効にすることはできません。ゾーンディフェンスはネットワークトラフィックの異常がファイアウォールに設定したしきい値に到達すると実行されます。この場合、ファイアウォールは即座にスイッチにコンタクトし、コマンドを実行します。その結果、疑いのあるホストからのあらゆるトラフィックをブロックします。

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

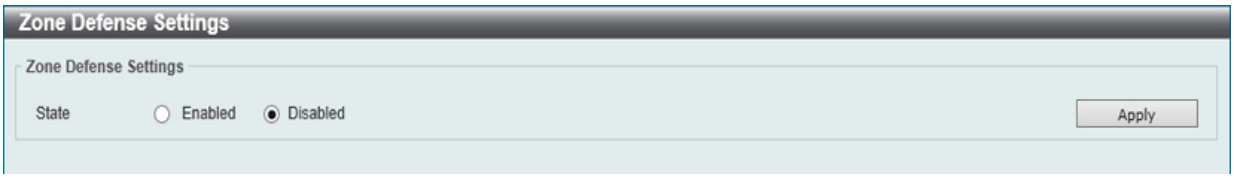


図 12-86　Zone Defense Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
State	本機能を有効 / 無効にします。

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

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管理者レベルのユーザアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
2. 「SSH User Settings」画面を使用して、ユーザアカウントを設定します。この時スイッチが 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。

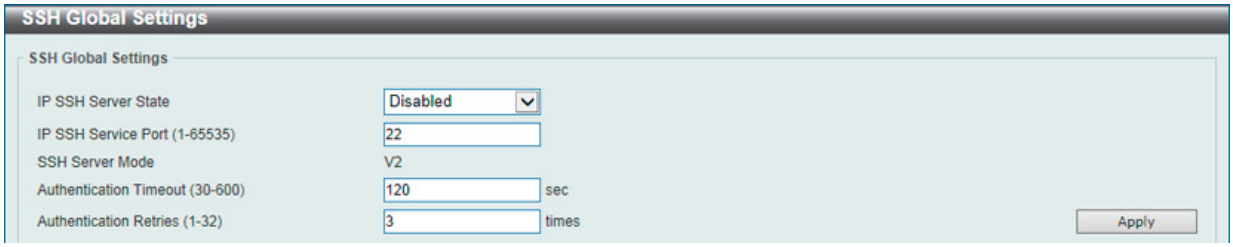


図 12-87 SSH Global Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
IP SSH Server State	グローバルに SSH 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
IP SSH Service Port (1-65535)	SSH サービスポート番号を設定します。初期値は 22 です。
Authentication Timeout(30-600)	認証のタイムアウト時間を指定します。30 から 600（秒）が指定できます。初期値は 120（秒）です。
Authentication Retries Attempts (1-32)	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スイッチは接続を切り、ユーザは再度スイッチに接続する必要があります。1 から 32 が指定できます。初期値は 3 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。

Host Key（Host Key 設定）

SSH ホスト鍵の設定（有効化）および設定内容の確認に使用します。

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。

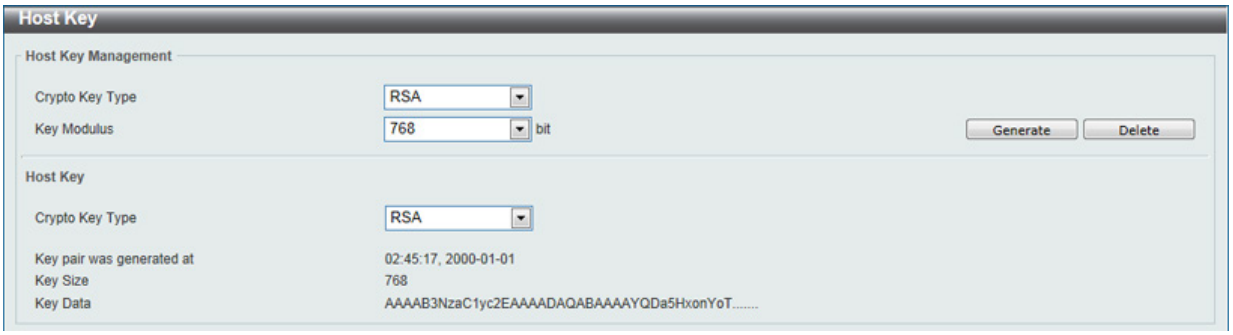


図 12-88 Host Key 画面

設定および表示する項目は以下の通りです。

項目	説明
Host Key Management	
Crypto Key Type	暗号鍵の種類を選択します。「Rivest Shamir Adleman (RSA)」または「Digital Signature Algorithm (DSA)」から選択します。
Key Modulus	鍵係数の値を入力します。「360」「512」「768」「1024」「2048」ビットから選択します。
Host Key	
Crypto Key Type	暗号鍵の種類を選択します。「Rivest Shamir Adleman (RSA)」または「Digital Signature Algorithm (DSA)」から選択します。

「Generate」ボタンをクリックし、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、指定したホスト鍵を削除します。

注意 スタック構成において、設定済みで「Key」の無い「Stack slave」を組み込んだ場合は同期されません。

「Generate」ボタンをクリックすると次の画面が表示されます。

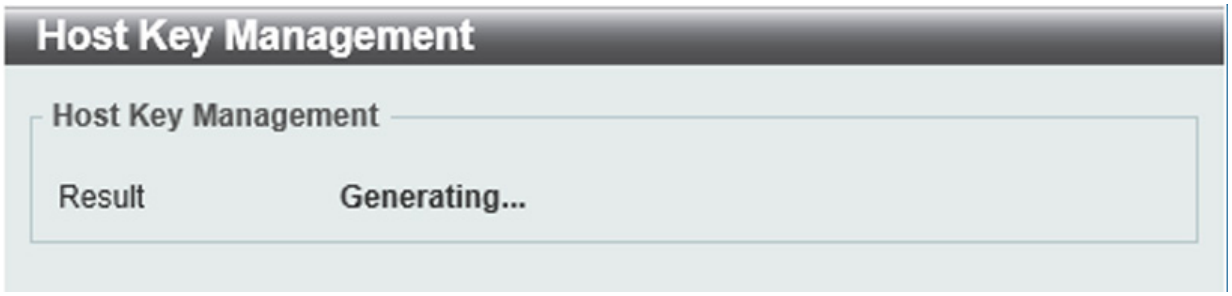


図 12-89 Host Key (Generating) 画面

「Generate」が終了すると次の画面が表示されます。

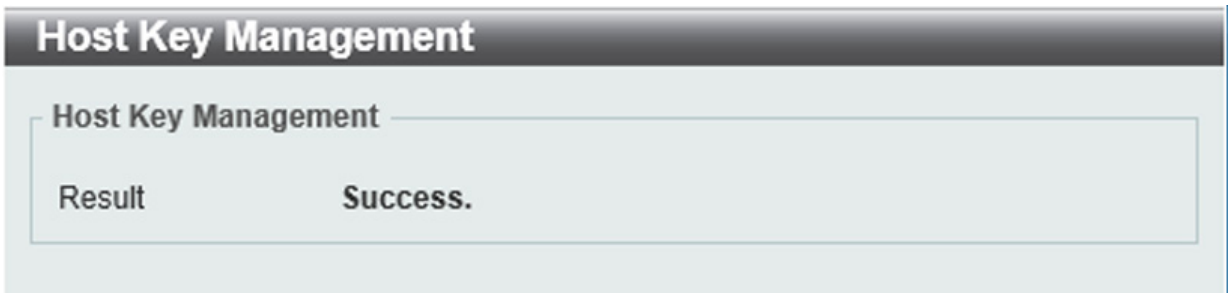


図 12-90 Host Key (Generating, Success) 画面

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 12-91 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。

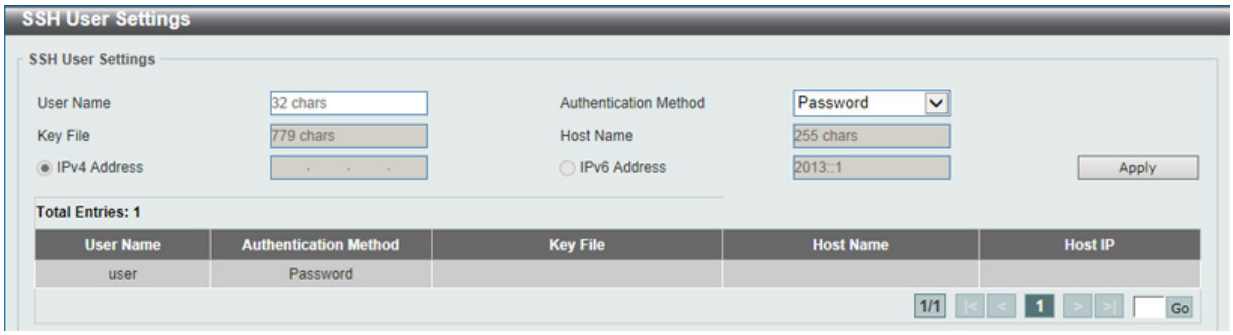


図 12-92 SSH User Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
User Name	SSH ユーザを識別するユーザ名を 32 文字までの半角英数字で指定します。
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以下から指定します。 • Host Based - 認証用にリモート SSH サーバを使用する場合に選択します。本項目を選択すると、SSH ユーザ識別のために以下の情報を入力することが必要になります。 • Password - 管理者定義のパスワードを使用して認証を行う場合に選択します。本項目を選択すると、スイッチは管理者にパスワードの入力（確認のため 2 回）を促します。 • Public Key - SSH サーバ上の公開鍵を使用して認証を行う場合に選択します。
Key File	「Public Key」または「Host-based」を選択した場合ここで公開鍵（Public Key）を入力します。
Host Name	リモート SSH ユーザを識別する 31 文字までの半角英数字を入力します。本項目は「Authentication Method」で「Host Based」を選択した場合のみ入力が必要です。
IPv4 Address	SSH ユーザの IPv4 アドレスを入力します。本項目は「Authentication Method」で「Host Based」を選択した場合のみ入力が必要です。
IPv6 Address	SSH ユーザの IPv6 アドレスを入力します。本項目は「Authentication Method」で「Host Based」を選択した場合のみ入力が必要です。

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。
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。

SSL（Secure Socket Layer）

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

1. 鍵交換（Key Exchange）
   暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。
2. 暗号化（Encryption）
   暗号スイートの次の段階は、クライアントとサーバ間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
   - ストリーム暗号（Stream Ciphers）– スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとサーバ間で一致させる必要があります。
   - CBC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）と AES（Advanced Encryption Standard）で定義する 3 DES EDE 暗号化コードをサポートし、暗号文を生成します。
3. ハッシュアルゴリズム（Hash Algorithm）
   暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）、SHA256 の 3 種類のハッシュアルゴリズムをサポートします。

これら 3 つのパラメータは、スイッチ上での 11 個の選択肢として独自に組み合わされ、サーバとクライアント間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。本スイッチは、TLSv1.0/1.1/1.2 をサポートしています。SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する場合があります。

「SSL Configuration Settings」画面では、ネットワークマネージャが SSL を有効にしてスイッチに暗号スイートを設定できます。暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。スイッチは SSL 機能のための 11 種類の暗号スイートを持ち、特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

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

SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者の情報や認証のための鍵やデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバとクライアントが一致した証明書ファイルを持つ必要があります。スイッチは、拡張子 ".der" を持つ証明書のみをサポートします。スイッチは証明書が既にロードされている形で発送されますが、ユーザの環境によっては、さらにダウンロードが必要になる場合があります。

SSL Global Settings（SSL グローバル設定）

SSL グローバル設定を行います。

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

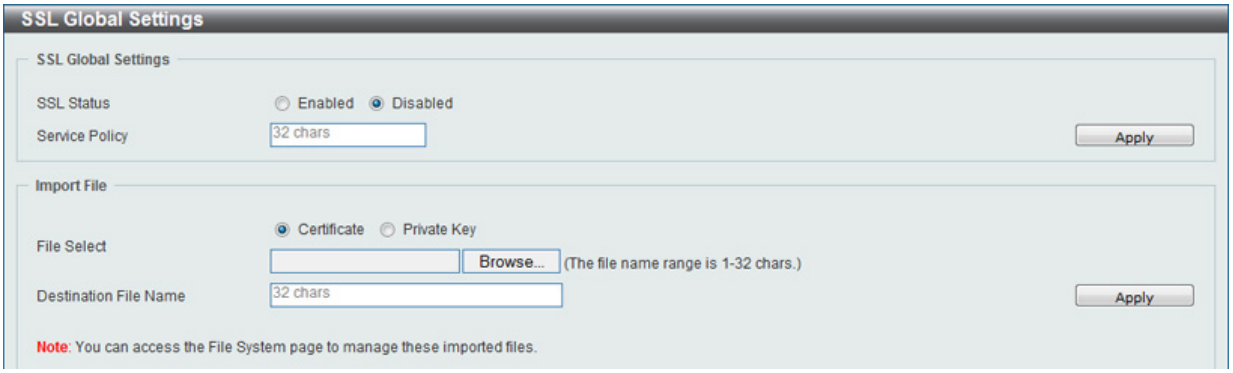


図 12-93　SSL Global Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
SSL Global Settings	
SSL Status	SSL をグローバルに「Enabled」（有効）、「Disabled」（無効）に設定します。初期値は「Disabled」です。
Service Policy	SSL ポリシー名を入力します。32 文字まで指定できます。

項目	説明
Import File	
File Select	ロードされるファイル種類を指定します。「Certificate」「Private Key」から指定可能です。ファイル種類を選択した後、「Browse/ 参照」ボタンをクリックして、適切なファイルを選択しローカルコンピュータにロードします。
Destination File Name	宛先ファイル名を指定します。32 文字まで指定可能です。

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

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。

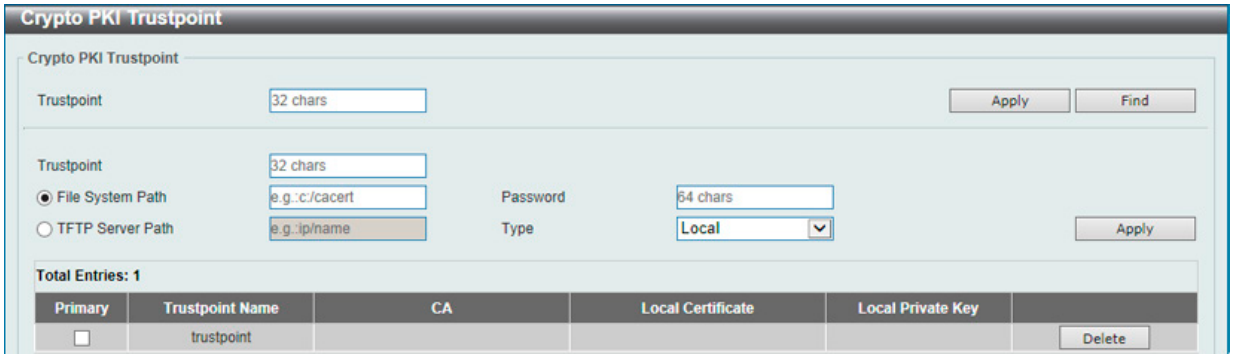


図 12-94 Crypto PKI Trustpoint 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
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 文字まで指定できます。
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。パスフレーズは 64 文字まで指定可能です。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」「Local」。「Both」を選択すると「CA 証明書」「ローカル証明書の鍵ペア」をインポートします。「CA」を選択すると「CA 証明書」のみインポートします。「Local」を選択すると「ローカル証明書の鍵ペア」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、入力した情報に基づいて指定エントリを検出します。
「Delete」ボタンをクリックして、指定エントリを削除します。

SSL Service Policy（SSL サービスポリシー）

SSL サービスポリシーの表示、設定を行います。

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

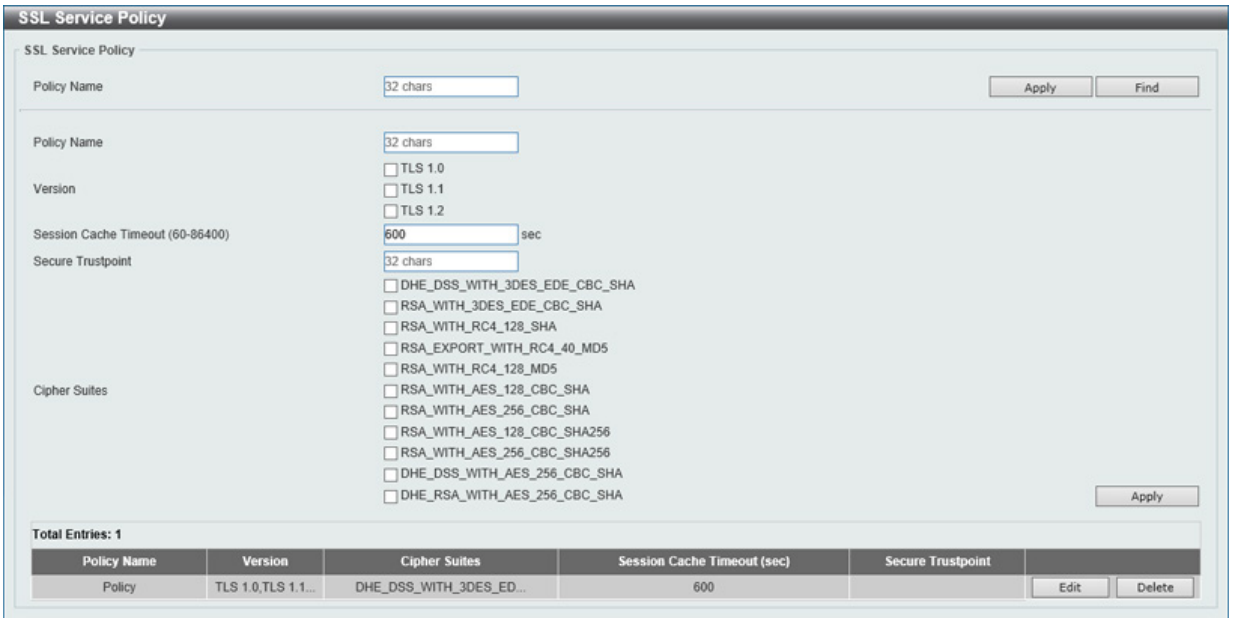


図 12-95　SSL Service Policy 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
Policy Name	SSL サービスポリシー名を入力します。32 文字まで指定可能です。
Version	「Transport Layer Security」(TLS) バージョンを指定します。「TLS 1.0」「TLS 1.1」「TLS 1.2」から指定します。
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。初期値は 600（秒）です。
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 文字まで指定可能です。
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、入力した情報に基づいて指定エントリを検出します。
「Edit」ボタンをクリックして、指定エントリを編集します。
「Delete」ボタンをクリックして、指定エントリを削除します。

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けるリモートでセキュアなファイルトランスファープロトコルです。SFTP はそれ自身で認証や、セキュリティを提供しないため、SFTP サーバを SSH サーバのサブシステムとして構築させる必要があります。

注意　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。

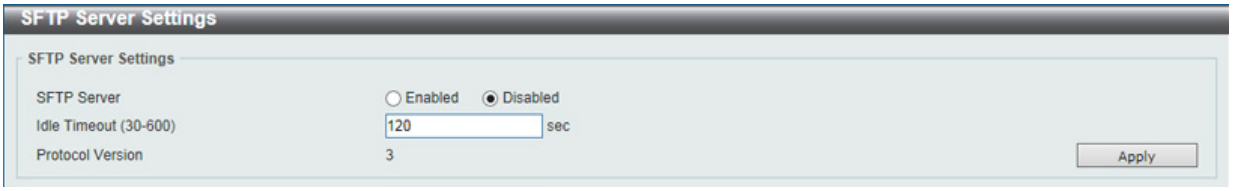


図 12-96　SFTP Server Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
SFTP Server	SFTP サーバ有効 / 無効に指定します。
Idle Timeout	アイドルタイムアウトの時間を設定します。SFTP サーバが指定値の時間 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。30-600 秒です。初期値は 120 秒です。

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

SFTP Client Settings（SFTP クライアント設定）

本項目では「Secure File Transfer Protocol」(SFTP) クライアントの設定、表示を行います。

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

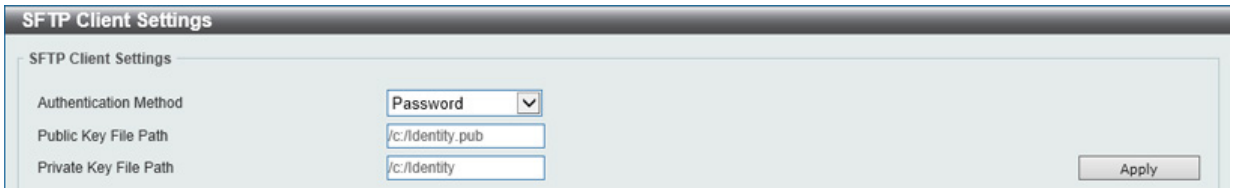


図 12-97 SFTP Client Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
Authentication Method	SFTP クライアントの認証方法を指定します。 • Password - ユーザ名 / パスワードで認証します。 • Public key - パブリックキー（公開鍵）で認証します。
Public Key File Path	SFTP クライアントのパブリックキーファイル名 / パスを指定します。
Private Key File Path	SFTP クライアントのプライベートキーファイル名 / パスを指定します。

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。

Network Protocol Port Protect Settings（ネットワークプロトコルポートプロテクト設定）

本項目ではネットワークプロトコルポートプロテクションの設定、表示を行います。

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。

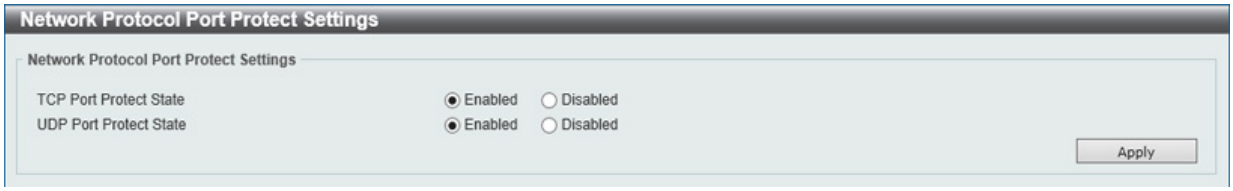


図 12-98 Network Protocol Port Protect Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
TCP Port Protect State	TCP ポートネットワークプロトコルプロテクション機能を有効 / 無効にします。
UDP Port Protect State	UDP ポートネットワークプロトコルプロテクション機能を有効 / 無効にします。

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

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

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

サブメニュー	説明
CFM（Connectivity Fault Management : 接続性障害管理）	CFM 機能を設定します。
Cable Diagnostics（ケーブル診断機能）	スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。
Ethernet OAM（イーサネット OAM）	ポートにイーサネット OAM モード、イベント、ログを設定します。
DDM（DDM 設定）	Digital Diagnostic Monitoring（DDM）機能を実行します。スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定（アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx（送信）電力しきい値設定、および Rx（受信）電力しきい値設定）を行うことができます。

CFM（Connectivity Fault Management : 接続性障害管理）

CFM は IEEE 802.1ag に定義されており、ネットワークにおける接続性故障の検出、隔離、およびレポートを行う標準規格です。CFM は サービスインスタンスごとの End-to-End の OAM（Operations : 操作、Administration : 管理、および Maintenance : メンテナンス）のための機能です。802.1ag によって定義されるように、CFM 機能にはパスの発見、障害検出、故障検証、分離、および故障通知があります。
イーサネット CFM フレームには、特別なイーサネットタイプ（0x8902）があります。すべての CFM メッセージは VLAN ベースごとにメンテナンスドメインに制限されます。CFM フレームペイロードの固有のユニークな OpCode によって識別される様々なメッセージタイプがあります。
CFM メッセージタイプには Continuity Check Message（CCM: 連続性チェックメッセージ）、Loopback Message と Response（LBM: ループバックメッセージ、LBR: ループバックレスポンス）、および Link Trace Message と Response（LTM: リンクトレースメッセージ、LTR: リンクトレースレスポンス）が含まれます。

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。

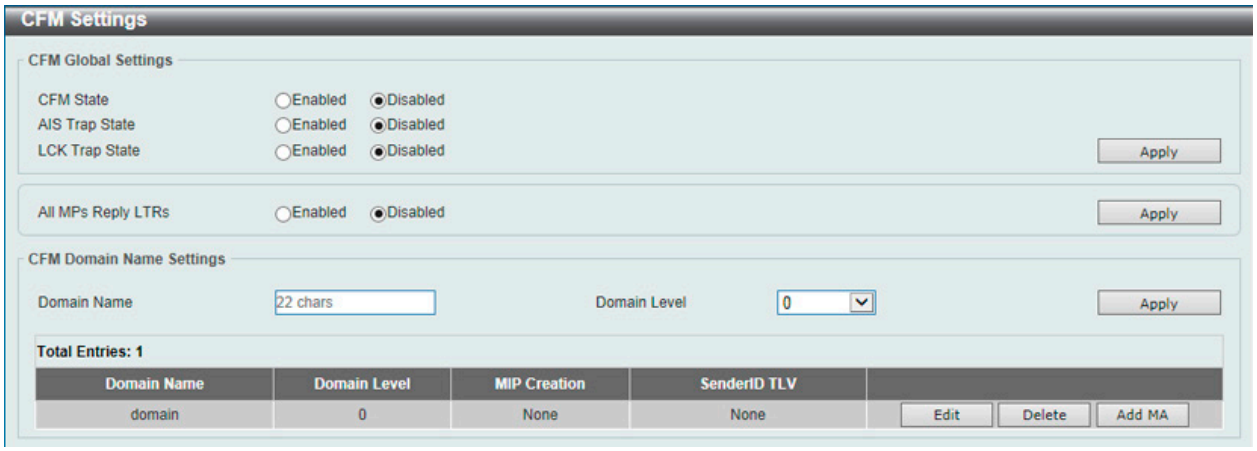


図 13-1　CFM Settings 画面

以下の項目を設定できます。

項目	説明
CFM Global Settings	
CFM State	CFM 機能を有効または無効にします。
AIS Trap State	「Alarm Indication Signal」(LCK) トラップ機能を有効 / 無効に指定します。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」(AIS) トラップ機能を有効 / 無効に指定します。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	Link Trace Reply（LTR）メッセージに応答するために、すべての MP（メンテナンスポイント）を有効または無効にします。
CFM Domain Name Settings	
Domain Name	メンテナンスドメインの名称を入力します。22 文字内で指定します。
Domain Level	メンテナンスドメインのレベルを選択します。レベルは、0-7 の範囲で設定します。0 が最も低く、7 が最も高いレベルです。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

エントリの編集

1. 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。

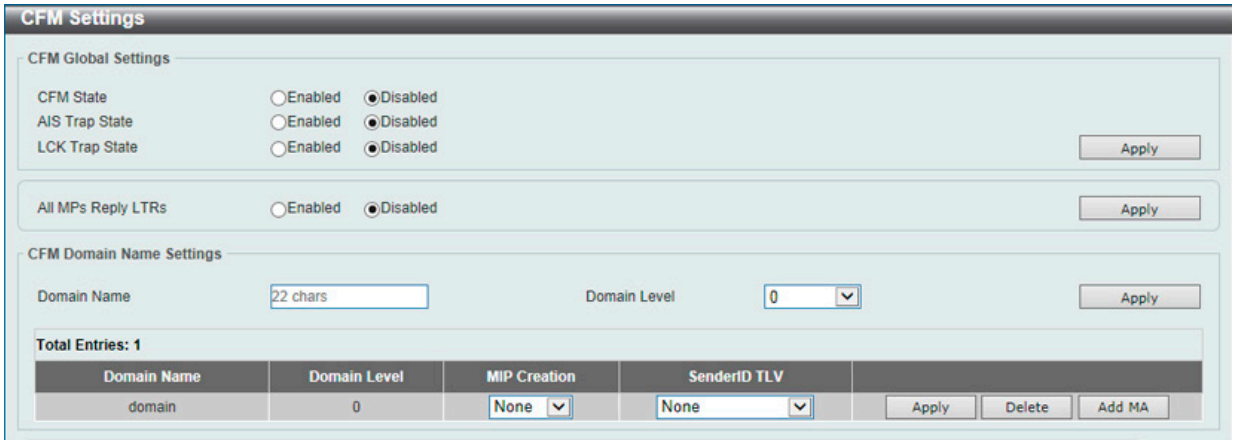


図 13-2　CFM Settings 画面 - Edit

以下の項目を設定できます。

項目	説明
MIP Creation	MIP の作成を制御します。 • None - MIP を作成しません。（初期値） • Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッチでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。 • Explicit - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。
Sender ID TLV	SenderID TLV の転送を制御します。 • None - SenderID TLV を転送しません。（初期値） • 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。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

注意 グループ名は 22 文字未満とします。

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

以下の項目が使用できます。

項目	説明
MA Name	メンテナンスアソシエーションの名称（22 字以内）を入力します。
MA VID (1-4094)	VLAN 識別子（1-4094）。異なる MA は異なる VLAN に関連付ける必要があります。

「Apply」をクリックし、設定内容を適用します。
「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。
「Add MEP」ボタンをクリックして、MEP（Maintenance End Point）エントリを追加します。

エントリの削除

テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。

エントリの編集

1. エントリ横の「Edit」ボタンをクリックして以下の画面を表示します。

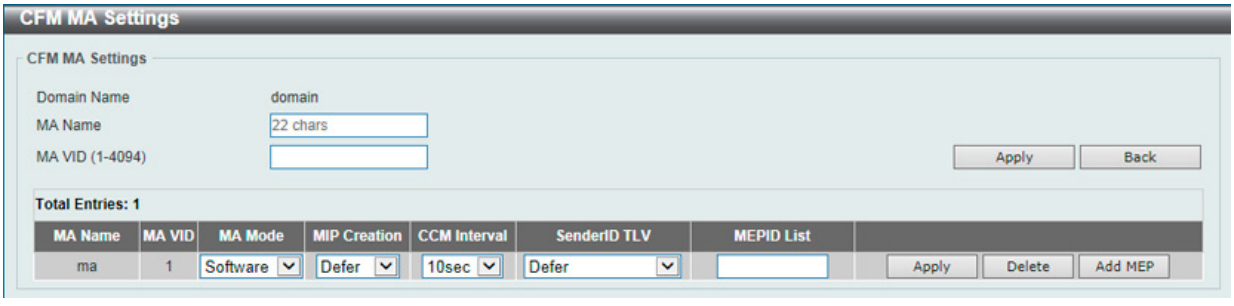


図 13-4　CFM MA Settings 画面 - Edit

以下の項目が使用できます。

項目	説明
MA Mode	プルダウンメニューを使用して、MA の動作モード（CFM ソフトウェアまたはハードウェアモード）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。（初期値） • Hardware - MA は CFM ハードウェアモードで動作します。
MIP Creation	MIP の作成を制御します。 • None - MIP を作成しません。（ハードウェアモード : 初期値） • 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。（ソフトウェアモード : 初期値） • Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッチでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。 • Explicit - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。 注意 CFM ハードウェアモードでは初期値は「None」です。
SenderID TLV	これは、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）
CCM Interval	これは CCM 送信間隔です。 • 3.3ms - 3.3（ミリ秒）。これは CFM ハードウェアモードでのみ動作します。 • 10ms - 10（ミリ秒）。これは CFM ハードウェアモードでのみ動作します。 • 100ms - 100（ミリ秒）。推奨されません。テストの目的のために使用します。 • 1sec - 1（秒） • 10sec - 10（秒）（初期値） • 1min - 1（分） • 10min - 10（分）
MEPID List	メンテナンスアソシエーションに含まれる MEP ID を指定します。 初期値では、初めて作成されたメンテナンスアソシエーションには MEP ID はありません。MEP ID の範囲は、1-8191 です。

2. 項目設定後、「Apply」ボタンをクリックします。

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。

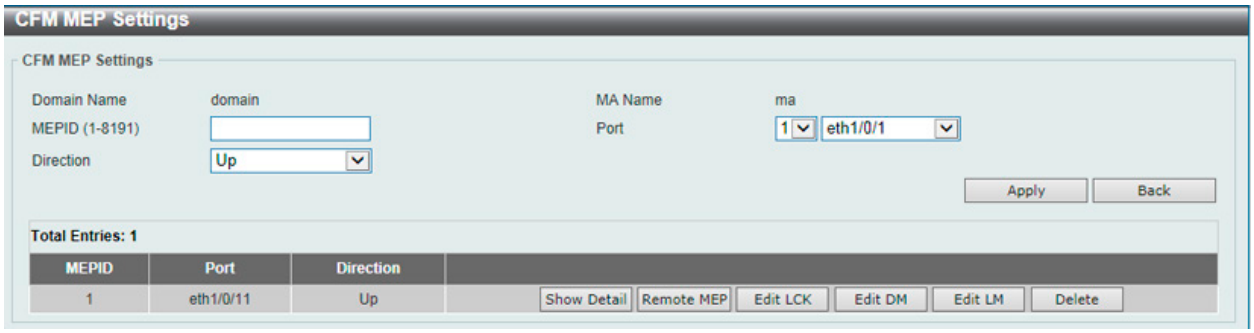


図 13-5　CFM MEP Settings 画面

以下の項目を設定できます。

項目	説明
MEP ID (1-8191)	MA の MEP ID リストに設定される MEP ID を入力します。
Port	プルダウンメニューを使用してポートを指定します。本ポートは MA の関連付けられている VLAN メンバである必要があります。CFM ハードウェアモードでは、本ポートは MA の関連付けられている VLAN のメンバである必要があります。

項目	説明
Direction	MEP の方向を指定します。 • Up - 内向き（アップ）MEP。内向きの MEP は、内側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。そして、フレームの送信元が内向きまたは外向きにかかわらず、より高いレベルにあるすべての CFM フレームを転送します。 • Down - 外向き（ダウン）MEP。外向きのポートは、ブリッジリレー機能側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。それは、そのレベルにあるすべての CFM フレームを処理して、ブリッジポートからから受信する低いレベルの CFM フレームすべてを破棄します。外向きポートは、フレームの送信先の方向にかかわらず、より高いレベルにあるすべての CFM フレームを転送します。

項目設定後、「Add」ボタンをクリックします。
「Apply」ボタンをクリックして行った変更を適用します。
「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。

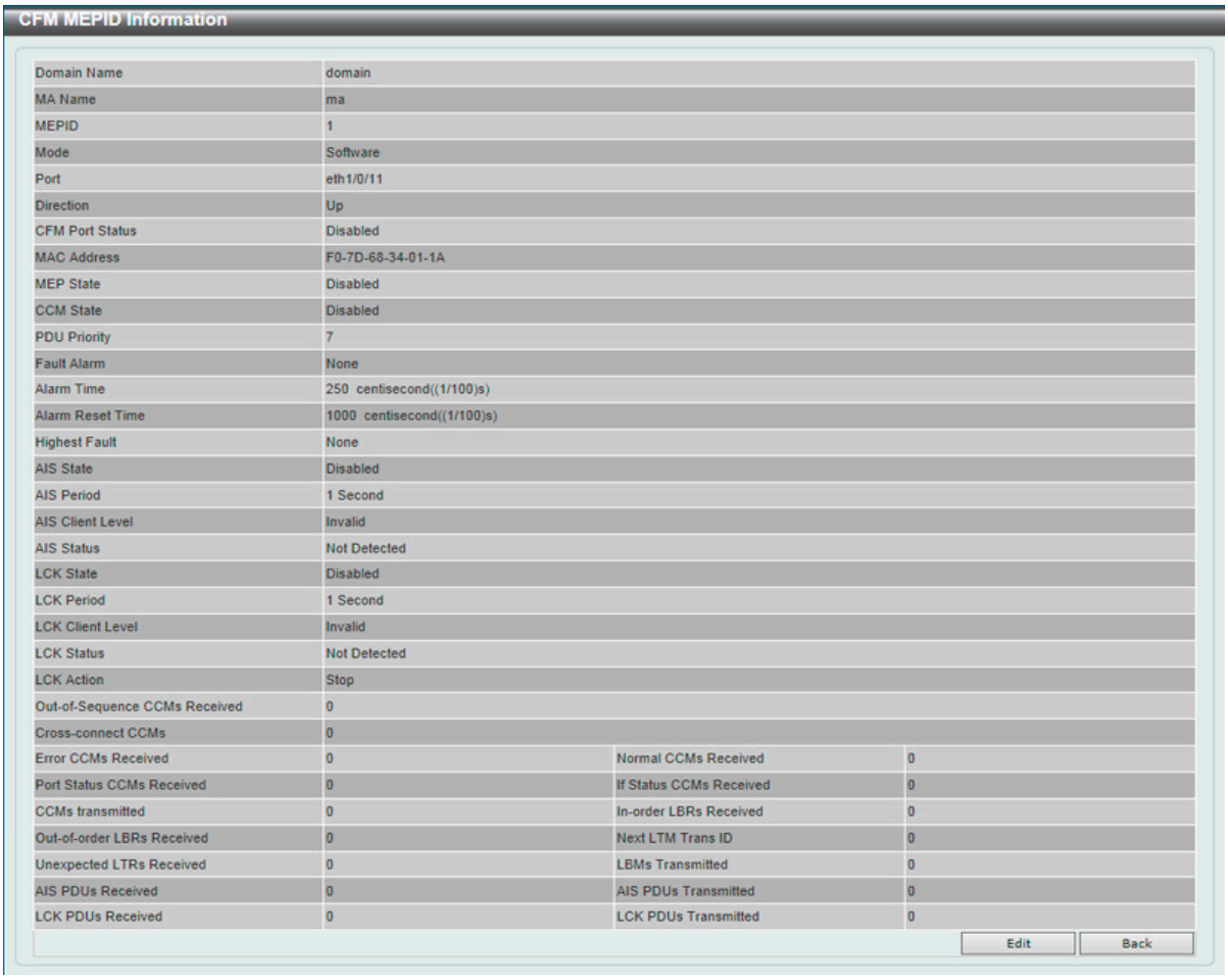


図 13-6　Show Detail Information 画面

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。

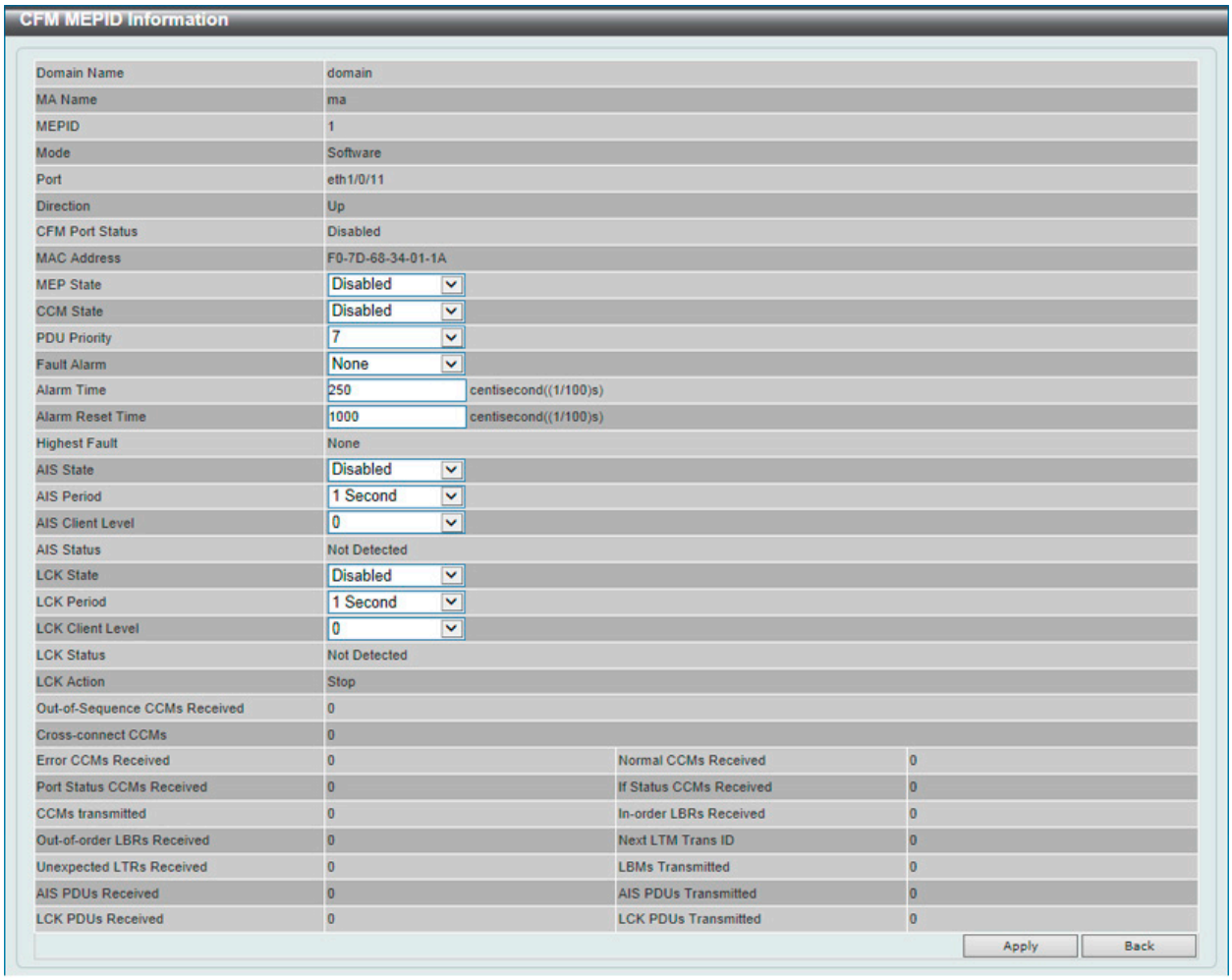


図 13-7　CFM MEP Information 画面 - Edit

以下の項目を設定または表示できます。

項目	説明
MEP State	MEP 管理状態を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
CCM State	CCM 送信状態を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
PDU Priority	802.1p 優先度は MEP によって送信された CCM および LTM メッセージに設定されます。初期値は 7 です。
Fault Alarm	これは、MEP によって送信される障害アラームの制御タイプです。 • All - すべての障害アラームのタイプが送信されます。 • MAC-Status - 優先度が「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。 • None - 障害アラームは送信されません。（初期値）
Alarm Time (250-1000)	これは、障害検出後に障害アラームが送信されるまでの経過時間です。範囲は 250-1000（センチ秒）です。初期値は 250（センチ秒）です。
Alarm Reset Time (250-1000)	これは、障害による再度アラーム送信前の検知が始動されるまでの待機時間です。範囲は 250-1000（センチ秒）です。初期値は 1000(センチ秒) です。
AIS State	チェックし、プルダウンメニューを使用して、AIS 機能を「Enabled」(有効)/「Disabled」(無効) にします。
AIS Period	チェックし、プルダウンメニューを使用して、AIS PDU 送信間隔を選択します。
AIS Client Level	チェックし、プルダウンメニューを使用して、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。オプションを 0-7 からを選択します。
LCK State	チェックし、プルダウンメニューを使用して、LCK 機能を「Enabled」(有効)/「Disabled」(無効) にします。

項目	説明
LCK Period	チェックし、プルダウンメニューを使用して、LCK PDU 送信間隔を選択します。
LCK Client Level	チェックし、プルダウンメニューを使用して、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。オプションを 0-7 からを選択します。

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。

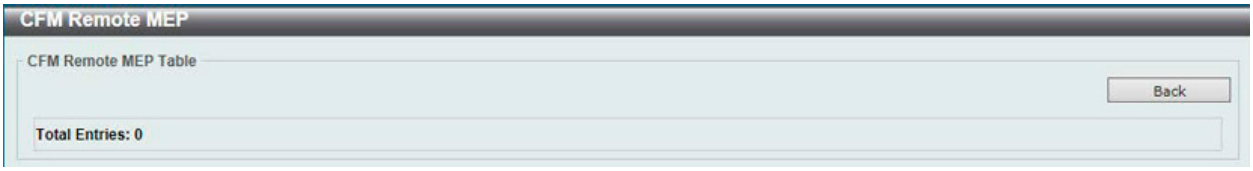


図 13-8　Remote MEP 画面

「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。

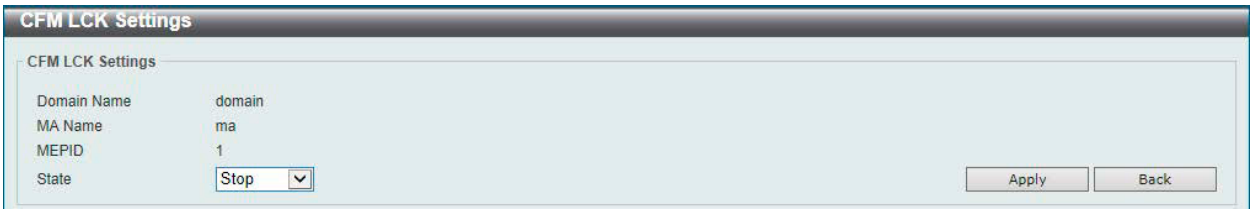


図 13-9　Edit LCK 画面

ロック動作を「Start」「Stop」から指定します。これにより MEP においてクライアントレベル MEP に LCK PDU を送信します。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

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。

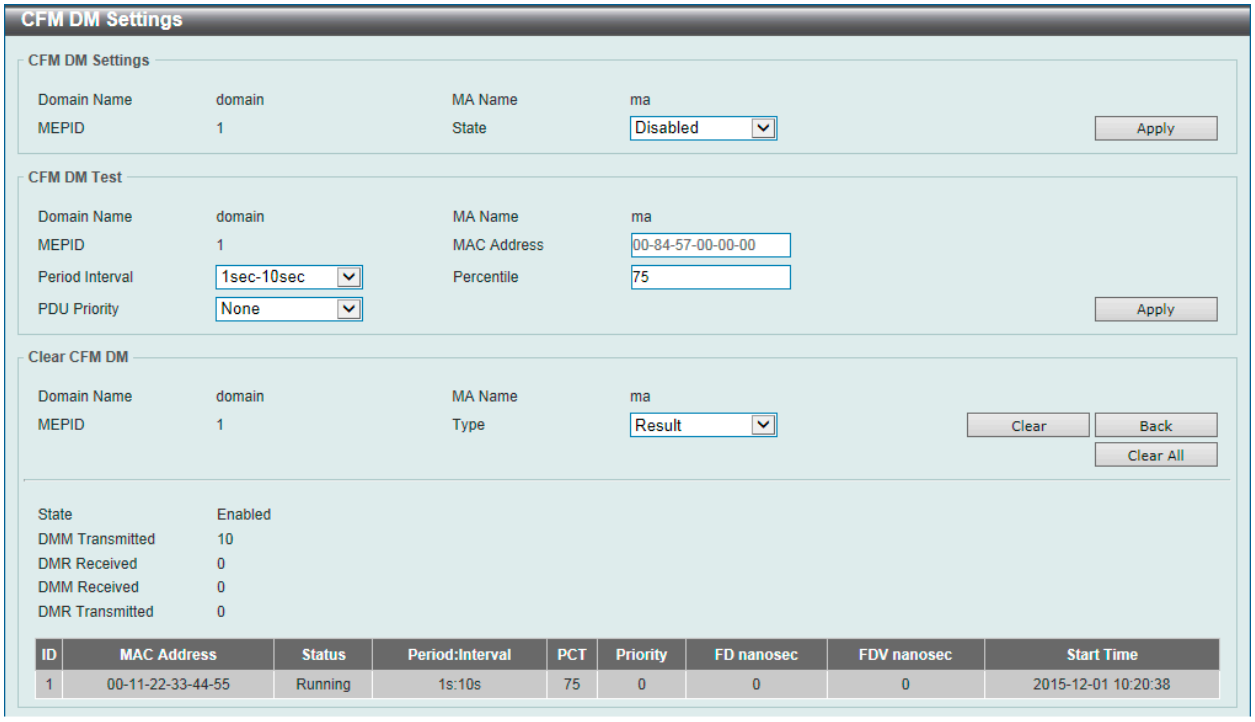


図 13-10 Edit DM 画面

以下の項目を設定または表示できます。

項目	説明
CFM DM Settings	
State	「ITU Y.1731」フレーム「Delay Measurement」(DM) 機能を有効 / 無効に指定します。有効にすると MEP はタイムスタンプを実行し、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	MAC アドレスを指定します。
Period Interval	DMM メッセージと診断の送信間隔を指定します。 • 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（0-100）を指定します。初期値は 75 です。
PDU Priority	PDU 優先値（0-7）を選択します。MEP に送信される DMM メッセージの 802.1p 優先値を指定します。
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」をクリックすると入力したエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「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。

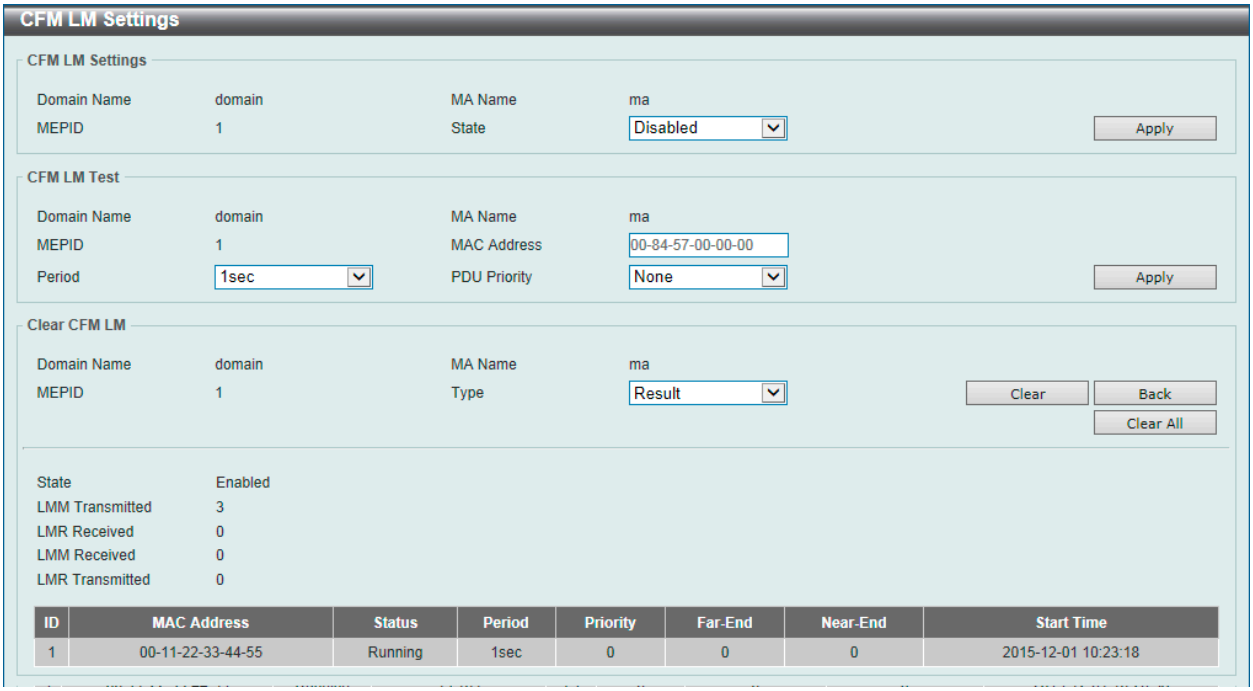


図 13-11　Edit LM 画面

以下の項目を設定または表示できます。

項目	説明
CFM LM Settings	
State	「ITU Y.1731」フレーム「Loss Measurement」(LM) 機能を有効 / 無効に指定します。有効にすると MEP 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。
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（0-100）を指定します。初期値は 75 です。
PDU Priority	PDU 優先値（0-7）を選択します。MEP に送信される LMM メッセージの 802.1p 優先値を指定します。
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」をクリックすると入力したエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「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 ポート状態を有効または無効にします。

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

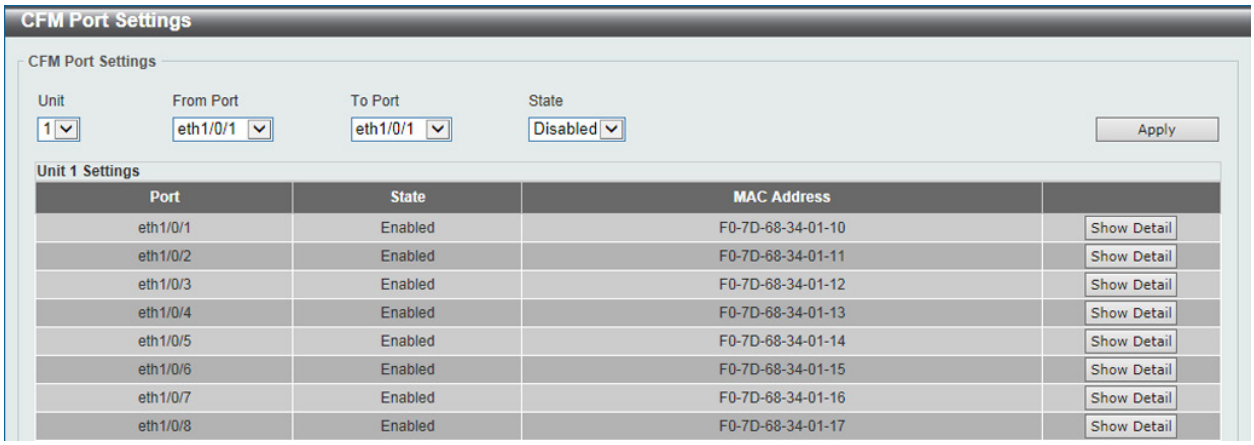


図 13-12 CFM Port Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	設定を行うユニットを指定します。
From Port/To Port	本設定に使用されるポート範囲を選択します。
State	特定ポートの CFM 設定を有効または無効にします。初期値は無効です。

「Apply」ボタンをクリックし、変更を有効にします。

「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。

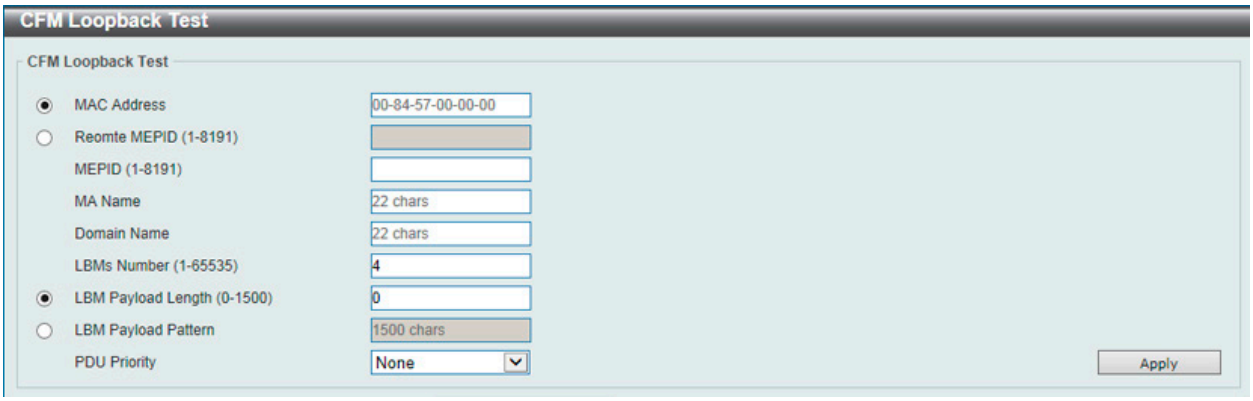


図 13-14 CFM Loopback Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
MAC Address	宛先 MAC アドレスを入力します。
Remote MEPID (1-8191)	Remote MEP ID を入力します。
MEP ID (1-8191)	MEP ID を入力します。
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。
Domain Name	使用するメンテナンスドメイン名を指定します。
LBMs Number (1-65535)	送信する LBM 数を指定します。初期値は 4 です。1 ～ 65525 の範囲で指定します。
LBM Payload Length (0-1500)	送信される LBM のペイロード長を指定します。初期値は 0 です。
LBM Payload Pattern (Max: 1500 characters)	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 に含まれることになる任意の数のデータとなります。1500 字以内で指定し、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（0-7）を指定します。指定しない場合、MA が送信した CCM と LTM と同じ優先度を使用します。初期値は「None」（なし）です。

「Apply」ボタンをクリックし、変更を有効にします。

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。

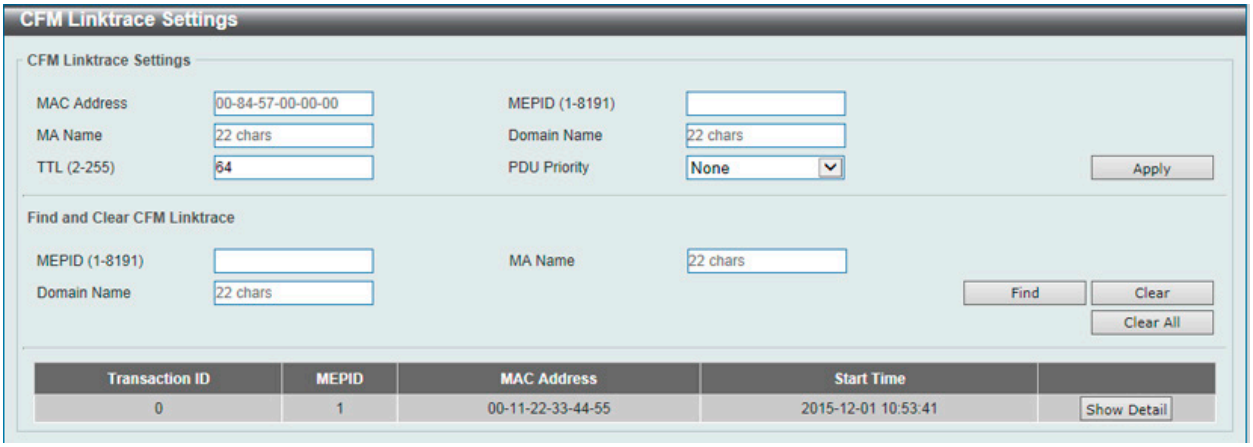


図 13-15 CFM Linktrace Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
CFM Linktrace Settings	
MAC Address	送信先 MAC アドレスを入力します。
MEP ID (1-8191)	使用するエンドポイント ID を指定します。
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。
Domain Name	使用するメンテナンスドメイン名を指定します。
TTL (2-255)	リンクトレースメッセージの TTL 値。初期値は 64 です。範囲は 2-255 です。
PDU Priority	送信される LTM に設定される 802.1p 優先度（0-7）。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。
Find and Clear CFM Linktrace	
MEP ID (1-8191)	使用するエンドポイント ID を指定します。
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。
Domain Name	使用するメンテナンスドメイン名を指定します。

「Apply」ボタンをクリックし、変更を有効にします。
「Clear」をクリックすると入力したエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。

エントリの参照
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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。

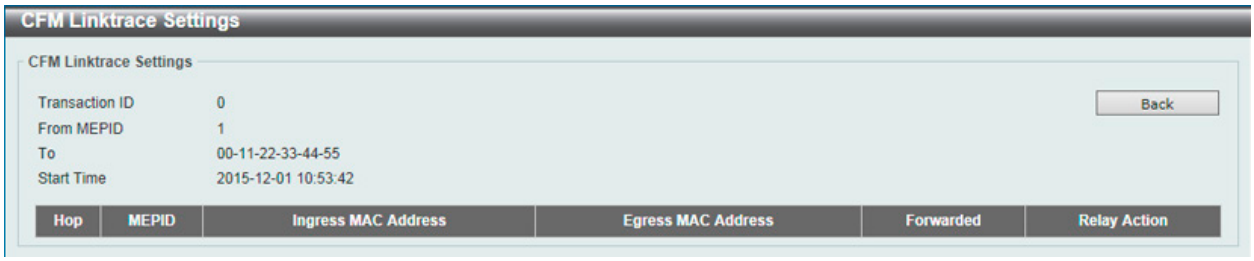


図 13-16 CFM Linktrace Settings 画面

「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。CFM ハードウェアモードにおける MEP の CCM パケット統計情報はカウントしません。

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。

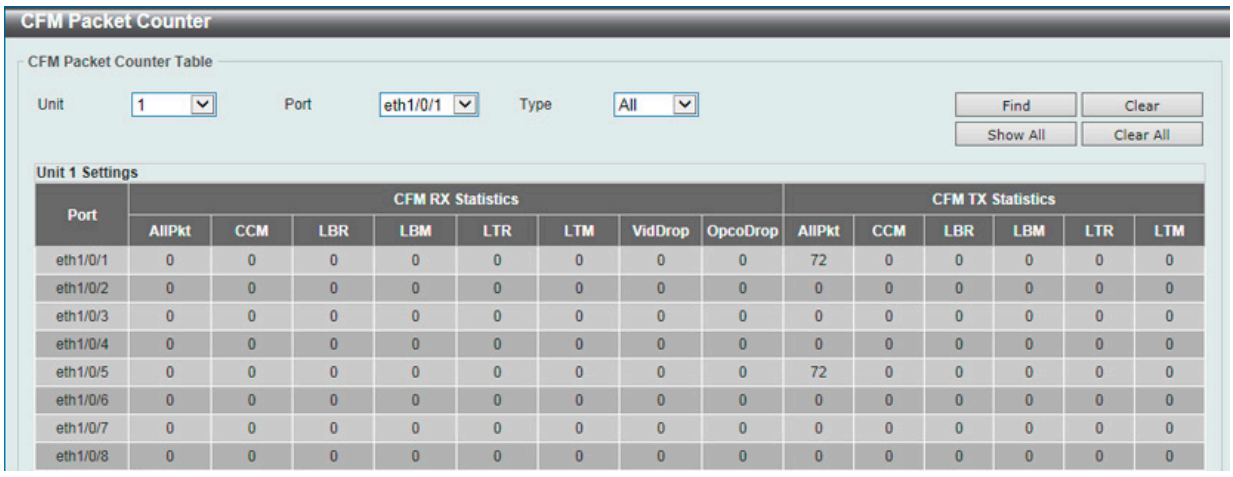


図 13-17 CFM Packet Counter 画面

画面には以下の項目があります。

項目	説明
Unit	設定を行うユニットを指定します。
Port	参照するポートを選択します。

項目	説明
Type	• RX - 受信したすべての CFM パケットを表示します。 • TX - 送信したすべての CFM パケットを表示します。 • All - 送受信したすべての CFM パケットを表示します。

参照するポート番号を入力し、「Find」ボタンをクリックします。
「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「Show All」をクリックして、すべてのエントリを表示します。

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」をクリックすると入力したエントリをクリアします。
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。

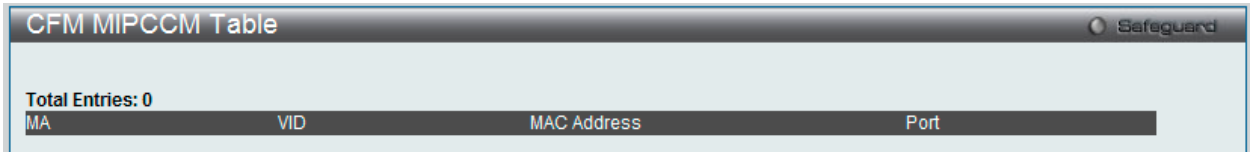


図 13-19 CFM MIP CCM Table 画面

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。

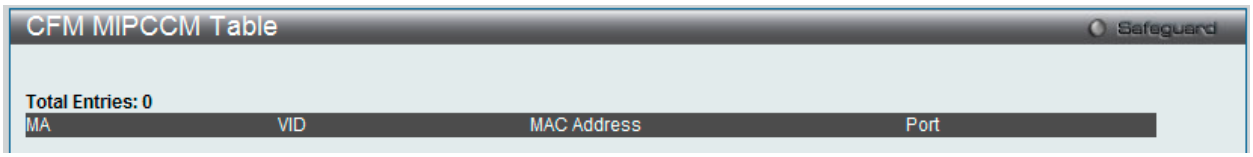


図 13-20 CFM MEP Fault Table 画面

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。

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。

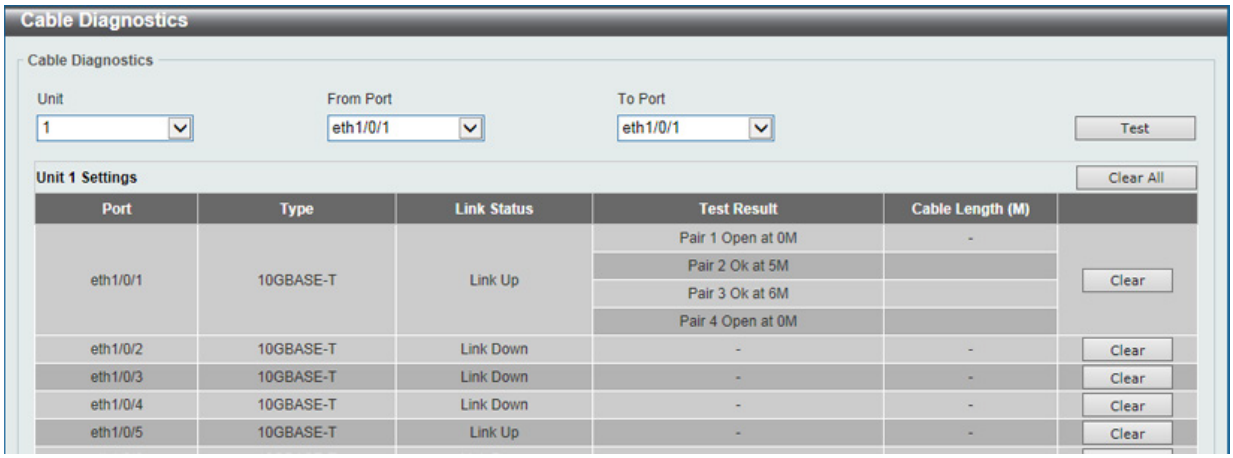


図 13-21 Cable Diagnostics 画面

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

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。

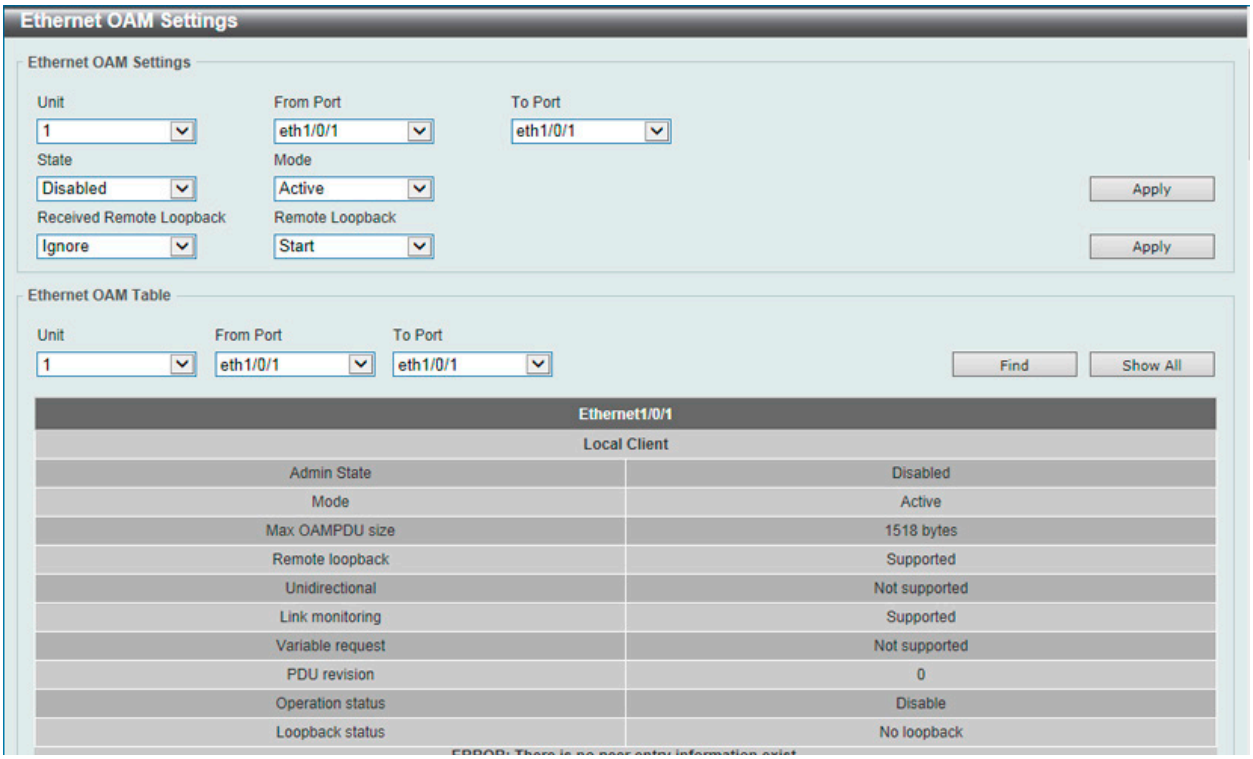


図 13-22 Ethernet OAM Settings 画面

以下の項目を設定できます。

項目	説明
Ethernet OAM Settings	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
State	OAM 機能を有効または無効にします。初期値は無効です。 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	動作するモード（「Active」または「Passive」）を指定します。初期モードは「Active」です。 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	クライアントが受信したイーサネット OAM リモートループバックコマンドの処理を指定します。 • Process - 受信したイーサネット OAM リモートループバックコマンドを処理します。 • Ignore - 受信したイーサネット OAM リモートループバックコマンドを無視します。（初期値） 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が処理されます。受信したリモートループバック機能を無視すると、ポートがリモートループバックモードに移行することが回避されます。
Remote Loopback	• 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	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Apply」ボタンをクリックし、変更を有効にします。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「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。

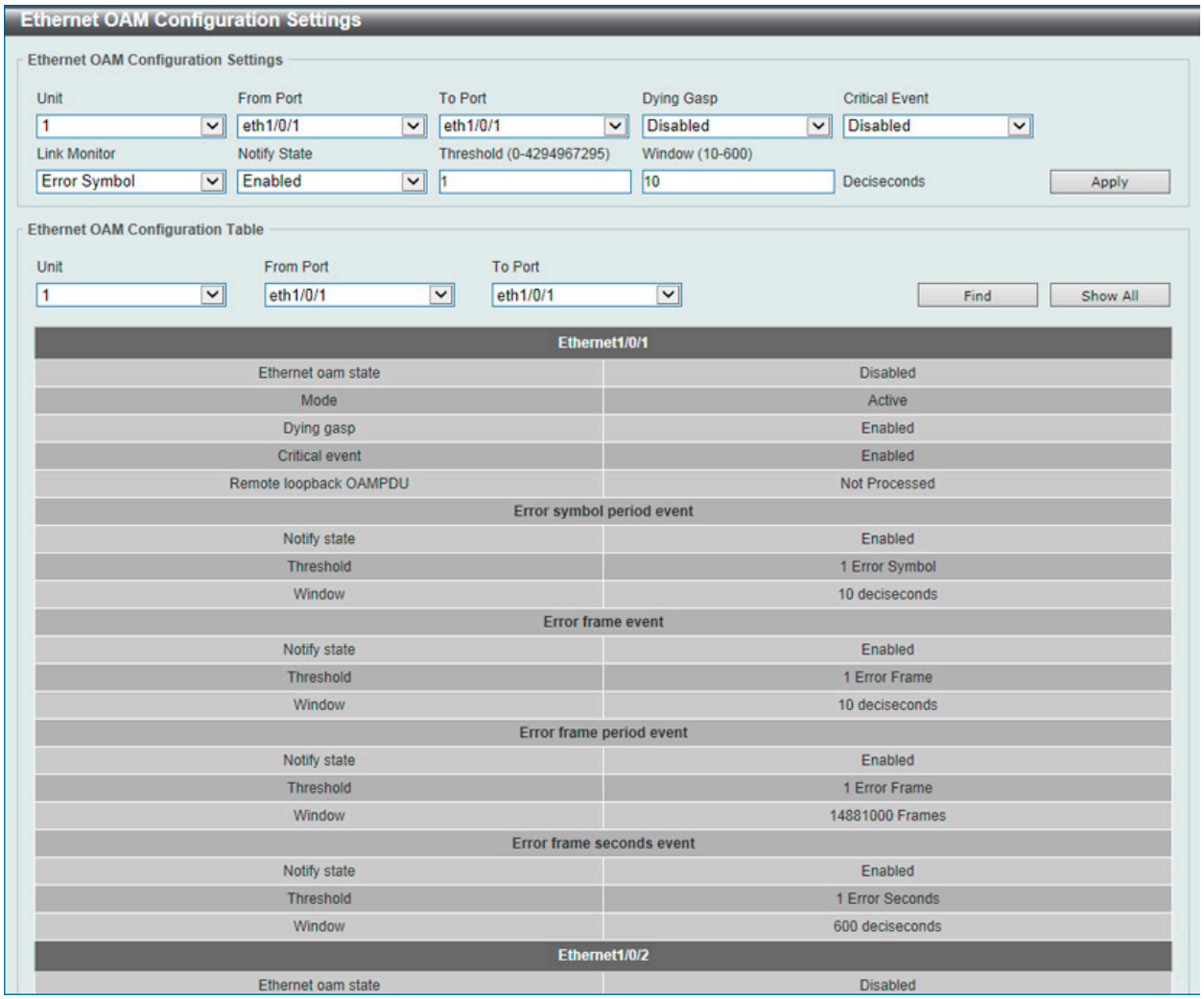


図 13-23 Ethernet OAM Configuration Settings 画面

以下の項目を設定できます。

項目	説明
Ethernet OAM Configuration Settings	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポート範囲を指定します。
Dying Gasp	「Dying Gasp」を有効 / 無効に指定します。リモートデバイスの電源障害など回復不可能なイベントの発生の検出を指定します。
Critical Event	イーサネット OAM のクリティカルなリンクイベント機能を有効 / 無効に指定します。イベント機能が無効になると、ポートは対応するクリティカルなリンクイベントを送信しません。
Link Monitor	ポートにイーサネット OAM リンクモニタリング (Error Symbol) を設定します。リンクモニタリング機能は、さまざまな条件のもとでリンク障害を検出して示すメカニズムを提供します。OAM はコード化されたシンボルのエラー数と共にフレームエラー数により統計情報をモニタリングします。シンボルエラー数が、期間内に定義したしきい値以上になる場合およびイベント通知状態 (Notify) が有効になる場合、リモート OAM ピアに通知するエラーシンボル期間のイベントを生成します。使用可能オプションは、Error Symbol、Error Frame、Error Frame Period、および Error Frame Second です。
Notify State	イベント通知を有効または無効にします。初期値は有効です。

項目	説明
Threshold (0-4294967295)	イベント生成のためには、期間内に要求以上のにシンボルエラー数を指定します。しきい値は 0 - 4294967295 の範囲です。初期値は 1 です。
Window (1000-6000)	エラーフレームまたはシンボルのサマリイベントの期間（デシ秒）を入力します。
Ethernet OAM Configuration Table	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポート範囲を指定します。

「Apply」ボタンをクリックし、設定を有効にします。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「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。

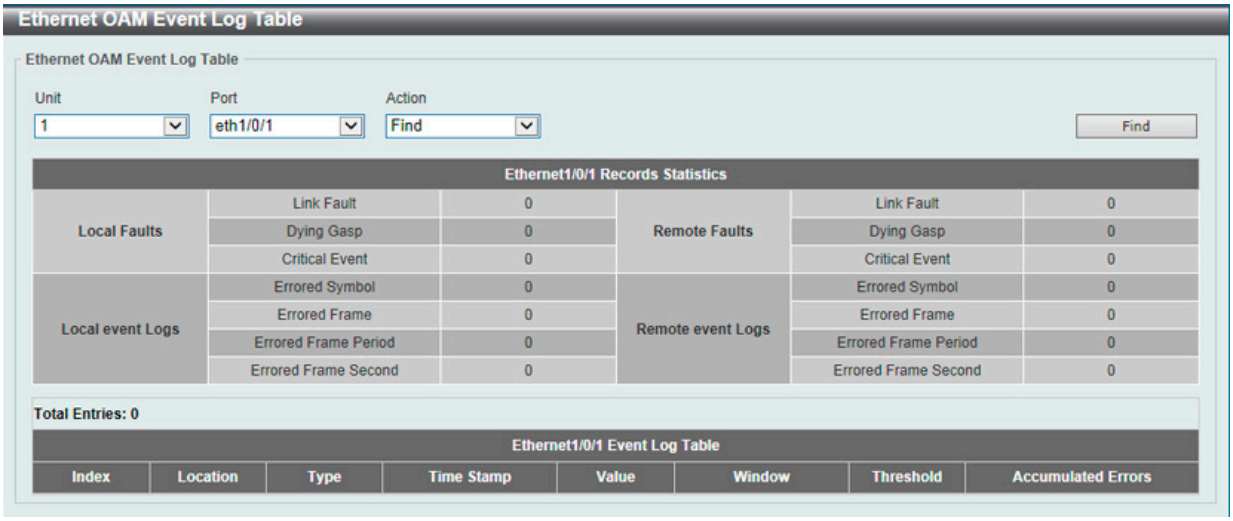


図 13-24　Ethernet OAM Event Log Table 画面

以下の項目を設定できます。

項目	説明
Unit	参照するユニットを指定します。
Port	参照するポート番号を選択します。

参照するポート番号またはポートリストを指定し、「Action」で「Find」を指定します。
エントリを削除するためには、適切な情報を入力して、「Action」で「Clear」ボタンをクリックします。

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。

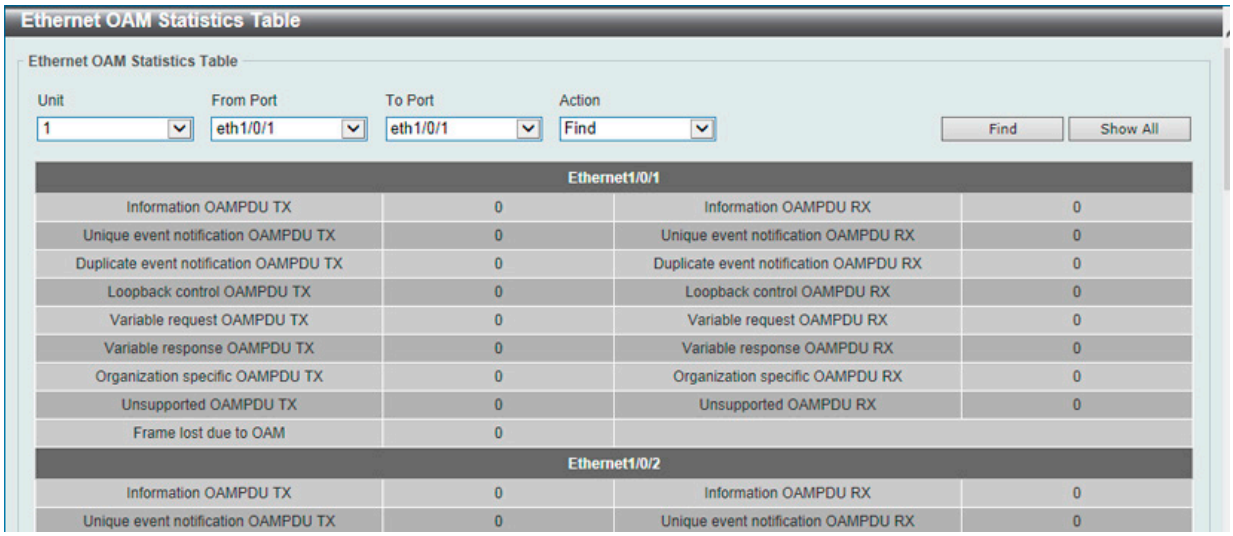


図 13-25　Ethernet OAM Statistics Table 画面

以下の項目を設定できます。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

参照するポート番号またはポートリストを指定し、「Action」で「Find」を指定します。
エントリを削除するためには、適切な情報を入力して、「Action」で「Clear」ボタンをクリックします。

Ethernet OAM DULD Settings（イーサネット OAM DULD 設定）

本項目では Ethernet OAM「D-Link Unidirectional Link Detection」(DULD) の設定、表示を行います。DULD は「802.3ah」イーサネット OAM の拡張機能です。PHY サポート外の単方向「ポイント to ポイント」イーサネットリンクの検出を行います。OAM ベンダの仕様メッセージが検出に使用されます。検出のプロセスは OAM ディスカバリの開始後、設定のディスカバリ時間内でのネゴシエーションを完了していない状態で開始します。

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

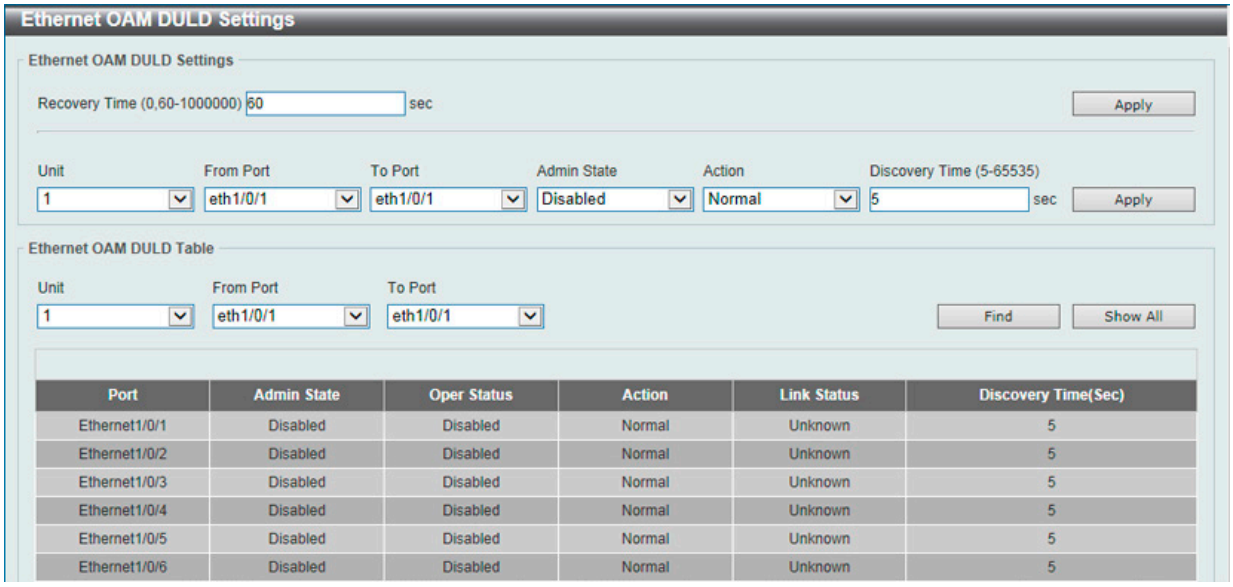


図 13-26　Ethernet OAM DULD Settings 画面

以下の項目を設定できます。

項目	説明
Ethernet OAM DULD Settings	
Recovery Time	DULD によって無効化されたポートの回復にかかる時間間隔を指定します。設定時間が過ぎると DULD による無効ポートは自動的に回復します。「0」は本機能の無効を意味します。「0」または「60」から「1000000」（秒）で設定します。

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Admin State	プルダウンメニューか選択ポートの単方向リンク検出状態を「Enabled」(有効) または「Disabled」(無効) に設定します。
Action	プルダウンメニューを使用してモード（「Shutdown」および「Normal」）を選択します。 • Shutdown - 単方向のリンクが検出されると、ポートを無効にしてイベントをログに出力します。 • Normal - 単方向のリンクが検出した場合にイベントを単にログに出力します。
Discovery Time (5-65535)	これらのポートの Neighbor 検出時間を入力します。検出がタイムアウトになると、単方向リンク検出が開始します。
Ethernet OAM DULD Table	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

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

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

DDM Settings（DDM 設定）

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

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

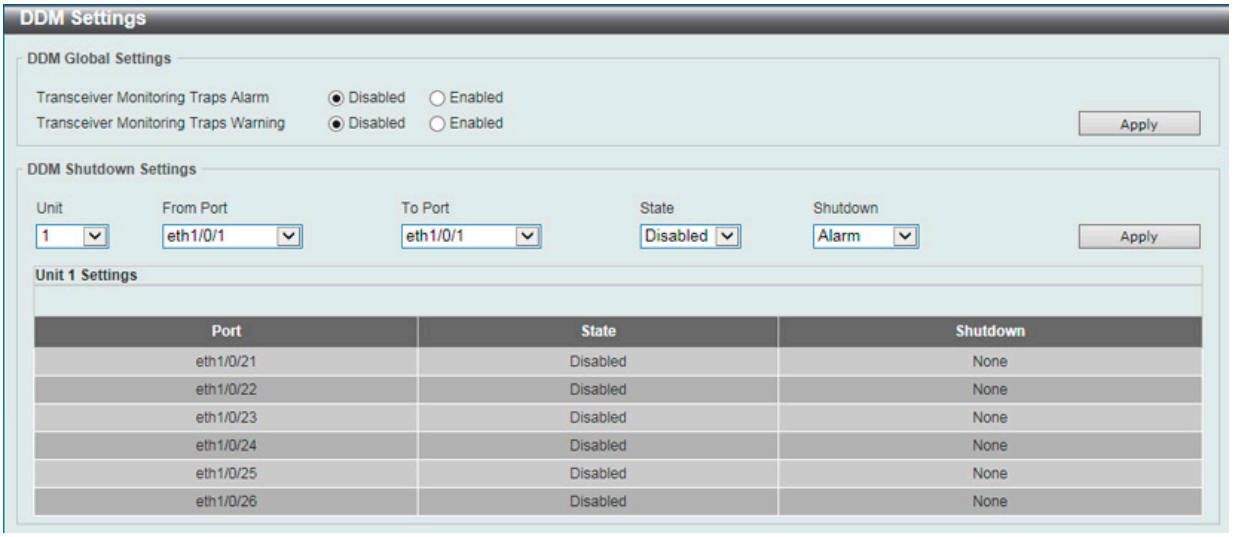


図 13-27 DDM Settings 画面

以下の項目を使用して設定します。

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

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

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

スイッチの特定ポートに DDM 温度しきい値設定を行います。

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

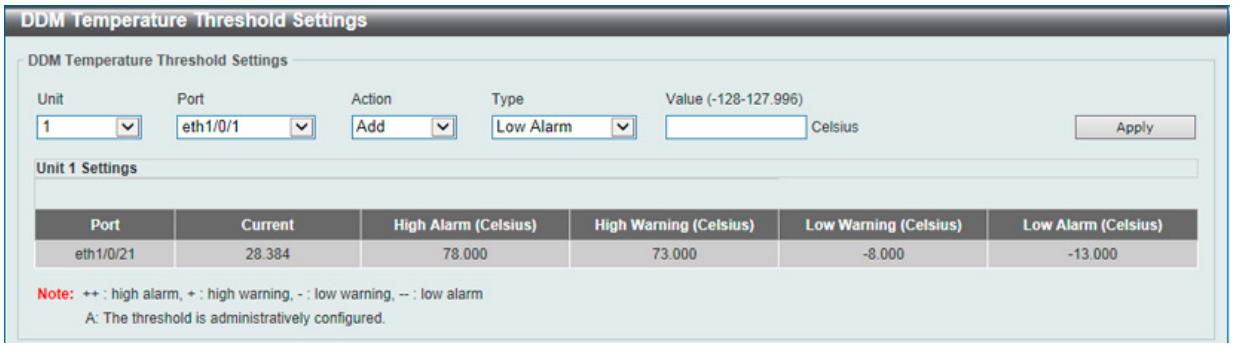


図 13-28　DDM Temperature Threshold Settings 画面

以下の項目を使用して設定します。

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

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

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

スイッチの特定ポートに電圧しきい値を設定します。

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

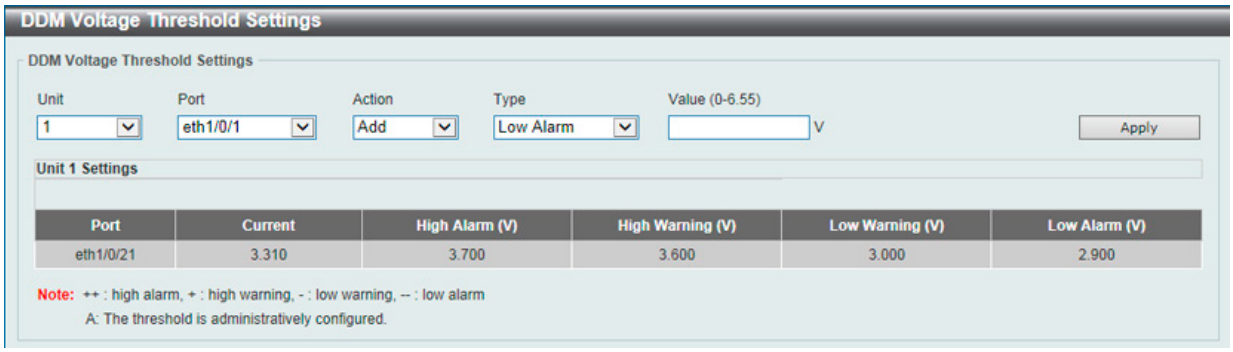


図 13-29　DDM Voltage Threshold Settings 画面

以下の項目を使用して設定します。

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

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

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

スイッチの特定ポートにバイアス電流しきい値を設定します。

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

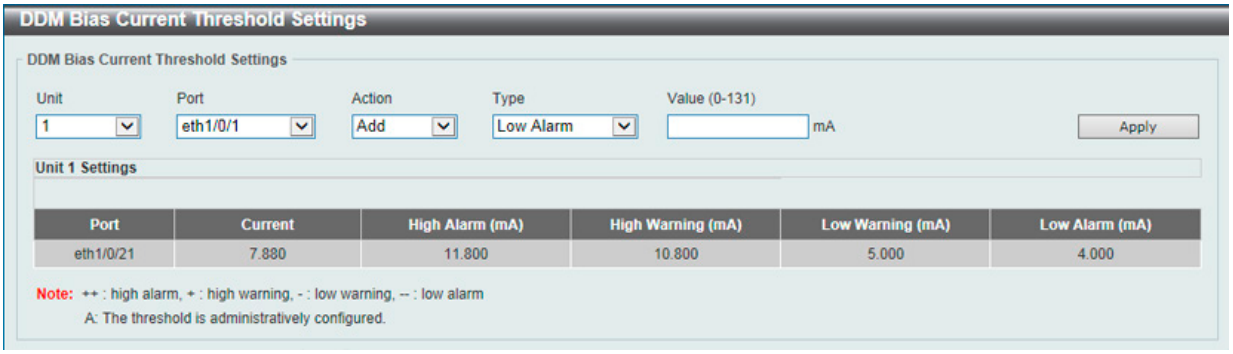


図 13-30　DDM Bias Current Threshold Settings 画面

以下の項目を使用して設定します。

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

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

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

スイッチの特定ポートに送信電力しきい値を設定します。

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

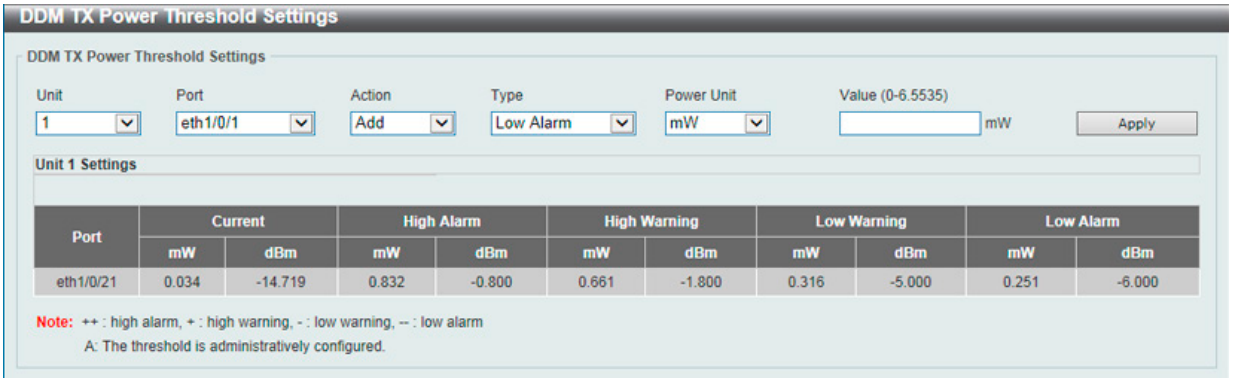


図 13-31　DDM TX Power Threshold Settings 画面

以下の項目を使用して設定します。

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

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

注意　DEM-431XT-DD（H/W：A1）を利用する場合、"TX power high warning threshold exceeded" のログが記録される場合は、「high alarm dbm」を「0」、「high warning dbm」を「-1」に設定してください。

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。

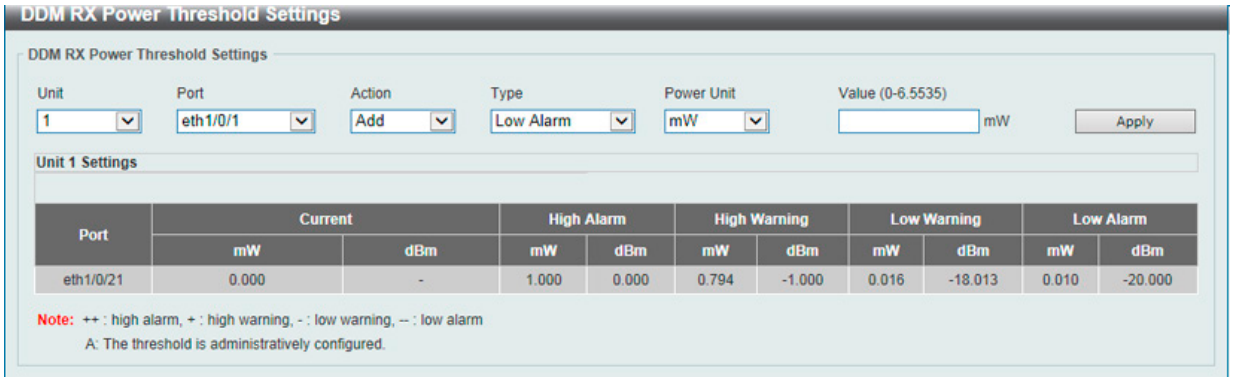


図 13-32　DDM RX Power Threshold Settings 画面

以下の項目を使用して設定します。

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

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

DDM Status Table（DDM ステータステーブル）

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

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

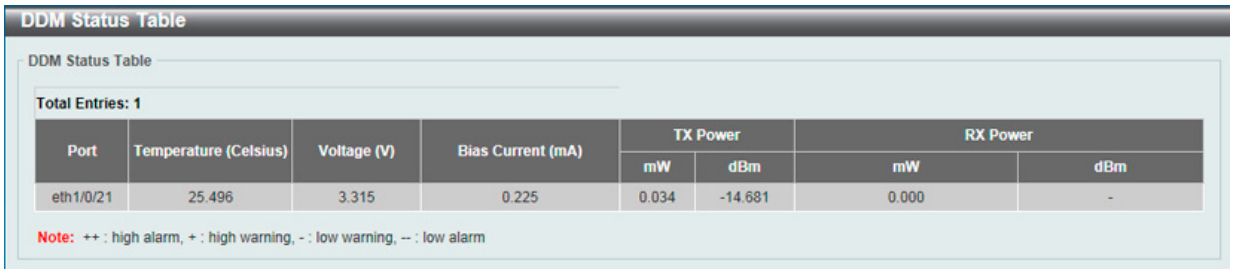


図 13-33図 13-8　　DDM Status Table 画面

以下の項目を表示します。

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

第 14 章　MPLS（MI モードのみ）

以下は MPLS 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
MPLS LDP Information Settings（MPLS LDP 情報設定）	「Multiprotocol Label Switching」(MPLS) の「Label Distribution Protocol」(LDP) 情報の設定を行います。
MPLS LSP Trigger Information（MPLS LSP トリガ情報）	「Multiprotocol Label Switching」(MPLS) の「Label-Switched Label-Switched Path」(LSP) トリガ情報の設定を行います。
MPLS Forwarding Settings（MPLS フォワーディング設定）	MPLS フォワーディングの設定を行います。
MPLS LDP Neighbor Password Settings（MPLS LDP ネイバパスワード設定）	MPLS LDP ネイバパスワードの設定を行います。
MPLS LDP Neighbor Targeted Settings（MPLS LDP ネイバターゲット設定）	MPLS LDP ネイバターゲットの設定を行います。
MPLS LDP Neighbor Information（MPLS LDP ネイバ情報）	MPLS LDP Neighbor Information（MPLS LDP ネイバ情報）の表示をします。
MPLS Global Settings（MPLS グローバル設定）	MPLS Global Settings（MPLS グローバル設定）の設定を行います。
MPLS LDP Interface Settings（MPLS LDP インタフェース設定）	MPLS LDP Interface Settings（MPLS LDP インタフェース設定）の設定をします。
MPLS LDP Session Information（MPLS LDP セッション情報）	MPLS LDP Session Information（MPLS LDP セッション情報）の検出、表示をします。
MPLS LDP Statistic（MPLS LDP スタティスティック）	MPLS LDP Statistic（MPLS LDP スタティスティック）の表示をします。
MPLS LDP Binding Table（MPLS LDP バインディングテーブル）	MPLS LDP Binding Table（MPLS LDP バインディングテーブル）の表示をします。
MPLS LDP Discovery Information（MPLS LDP ディスカバリ情報）	MPLS LDP Discovery Information（MPLS LDP ディスカバリ情報）の表示をします。
MPLS QoS Settings（MPLS QoS 設定）	MPLS QoS Settings（MPLS QoS 設定）の設定、表示をします。
Ping MPLS	指定 FEC の LSP の接続状態を確認します。
Traceroute MPLS IPv4（トレースルート MPLS IPv4）	指定 FEC の LSP パストレースのような「hop-by-hop fault localization」を指定します。

注意　MPLS については MI モードのみとなっています。

MPLS LDP Information Settings（MPLS LDP 情報設定）

本項目では、「Multiprotocol Label Switching」(MPLS)「Label Distribution Protocol」(LDP) 情報の設定、表示を行います。

MPLS > MPLS LDP 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。

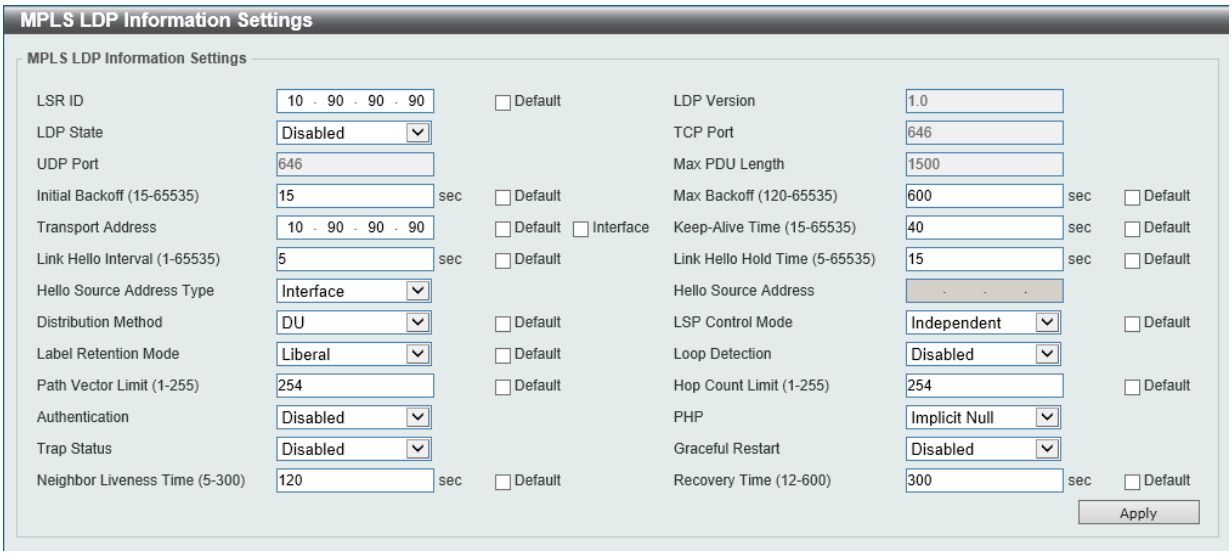


図 14-1　MPLS LDP Information Settings 画面

以下の項目を設定できます。

項目	説明
LSR ID	LSR ID を指定します。LSR ID はインタフェースの IPv4 アドレスであり、MPLS ネットワークで LSR を特定するのに使用されます。「Default」を指定すると初期設定を使用します。
LDP Version	LDP バージョンが表示されます。
LDP State	LDP を有効 / 無効に指定します。
TCP Port	LDP TCP ポートが表示されます。
UDP Port	LDP UDP ポートが表示されます。
Max PDU Length	最大 LDP PDU 長が表示されます。
Initial Backoff	初期バックオフ時間を入力します。LDP バックオフメカニズムは、互換性なく設定された 2 つの LSR が、セッション確立失敗という無限のシーケンスに陥ることを防ぎます。セッション確立の試みが非互換性のために失敗するなら、アクティブな LSR は次の試みを遅らせて、セッション確立を再試行します。この値は 15-65535（秒）である必要があります。「Default」を選択すると初期値（15 秒）を指定します。
Max Backoff	最大のバックオフ時間を入力します。この値は 120-65535（秒）である必要があります。「Default」を選択すると初期値（600 秒）を指定します。
Transport Address	トランスポート IPv4 アドレスを選択します。トランスポートアドレスは、LDP TCP 接続を確立するのに使用されます。「Interface」をトランスポートアドレスとして設定すると、各インタフェースの IP アドレスがトランスポートアドレスとして使用されます。「Default」を選択すると初期値を指定します。
Keep-Alive Time	キープアライブ時間を入力します。LDP は各ピアセッションのためにキープアライブタイマを保持します。キープアライブタイマがピアからの LDP PDU の受信なしで期限が切れると、LDP はピアが失敗したと結論づけて、LDP セッションを終えます。各 LSR は、セッションをアクティブに保つために一定の間隔を置いて LDP ピアにキープアライブメッセージを送信します。この値は 15-65535（秒）である必要があります。「Default」を選択すると初期値（40）を指定します。
Link Hello Interval	Hello メッセージを送信する間隔を入力します。この値は 1-65535(秒) である必要があります。「Default」を選択すると初期値（5）を指定します。
Link Hello Hold Time	Hello の保持時間を入力します。この値は 5-65535(秒) である必要があります。「Default」を選択すると初期値（15）を指定します。
Hello Source Address Type	Hello パケットの送信元アドレスタイプを指定します。 • Interface - 各インタフェースの IP アドレスを指定します。 • Router ID - LSR ID (ルータ ID) を指定します。 • IP Address - 手動で入力した IP アドレスを指定します。
Hello Source Address	Hello パケットの送信元アドレスとなる IP アドレスを指定します。

項目	説明
Distribution Method	配布方式を選択します。「Default」を選択すると初期値（DU）を指定します。 • DU - 配布モードを「Downstream-Unsolicited」に設定します。 • DoD - 配布モードを「Downstream-on-Demand」に設定します。 「Downstream-on-Demand」に設定されると、ダウンストリーム LSR はアップストリームの接続が行き過ぎたリクエストをした場合、ラベルマッピングを通知します。「Downstream-Unsolicited」に設定されると、ダウンストリーム LSR はルーティングテーブルでラベルが学習されるとラベルマッピングを通知します。
LSP Control Mode	LSP 制御モードを選択します。「Default」を選択すると初期値（Independent）を指定します。 • Independent LSP Control（独立 LSP 制御）- 各 LSR は独自にラベルを FEC に割り当てて、ラベル配布ピアにその割り当てを配布します。 • Ordered LSP Control（順次 LSP 制御）- その FEC のためのイーグレス LSR である場合、またはその FEC のネクストホップから FEC へのラベル割り当てを既に受信している場合にだけ、LSR はラベルを FEC に割り当てます。
Label Retention Mode	LDP ラベル保持モードを選択します。「Default」を選択すると初期値（Liberal）を指定します。 • Conservative - ラベル配布方式が Downstream-Unsolicited（DU）で、ラベル保持モードが「Conservative」である場合、LSR が、（その FEC のネクストホップでない）LSR からラベル割り当てを一度受信すると、割り当てを破棄します。 • Liberal - ラベル保持モードが「Liberal」であると、その割り当てを維持します。これは、ネクストホップに変更があった場合に LSP の迅速なセットアップを補助します。
Loop Detection	LDP ループ検知モードを有効または無効にします。LDP ループ検知メカニズムは、ループする LSP を検知するためにラベル要求とラベルマッピングメッセージによって運ばれた Path Vector および Hop Count TLV を利用します。
Path Vector Limit	使用するパスベクトルの制限値を入力します。この値は 1-255 である必要があります。 「Default」を選択すると初期値（254）を指定します。
Hop Count Limit	使用するホップカウントの制限値を入力します。この値は 1-255 である必要があります。 「Default」を選択すると初期値（254）を指定します。
Authentication	LDP 認証オプションを有効または無効にします。認証が有効であると、LSR は MD5 アルゴリズムを適用して、ピアに送信される TCP セグメントのために MD5 ダイジェストを計算します。この計算は TCP セグメントと同様にピアパスワードを利用します。LSR が MD5 ダイジェストと共に TCP セグメントを受信すると、MD5 ダイジェストを算出し、自身の記録を使用して、ダイジェストを受信したダイジェストと比較することで、セグメントを有効にします。比較でエラーとなると、セグメントは送信側に応答せずに破棄されます。LSR はパスワードが設定されていない LSR からの LDP Hello メッセージをすべて無視します。
PHP	PHP（Penultimate Hop Popping）の動作を選択します。LSR を「egress」に、PHP を「Implicit NULL」（暗黙 NULL）に設定する場合、Implicit NULL ラベルを上流（Penultimate Hop: 最後から 2 番目のホップ）に配布します。その後、上流は PHP を行います。Penultimate Hop に配布されたラベルを「Explicit NULL」に設定すると、Penultimate Hop はそれをポップ（ラベル削除）しません。
Trap Status	LDP トラップの状態を有効または無効にします。
Graceful Restart	「Graceful Restart」を有効 / 無効に指定します。「LDP Graceful Restart」は Label Switching Router's (LSR) 制御の再起動時に、MPLS トラッフィクへの悪影響を最小限にとどめるメカニズムです。これにより LDP は LDP セッションリカバリの間、MPLS フォワーディングステートを保持し、データに影響を与えません。「Graceful Restart」はローカル / ピアの両方が有効な場合において、LDP セッションで使用されます。
Neighbor Liveness Time	「Neighbor Liveness Time」値を入力します。機器がダウンしたネイバとの LDP セッションを検出した場合、再接続時間において LDP コミュニケーションの再構築を試みます。再接続時間（Reconnection Time）はネイバによって通知された FT 再接続タイムアウト値よりも少ない値と、ローカル生存時間に基づいて、設定されます。LDP セッションが再接続時間内で構築されなかった場合、すべての関連するラベルフォワーディングエントリは削除されます。「LDP Graceful Restart」が有効な場合、通知された FT 再接続タイムアウトはネイバ生存タイム値に基づいて設定されます。5-300 秒の間で指定可能です。「Default」を選択すると初期値を指定します。
Recovery Time	リカバリタイムを指定します。「LDP Graceful Restart」が有効時で、LDP セッションが再構築された場合、デバイスはリカバリタイムの間、ネイバのラベルマッピング情報交換を完了します。リカバリタイムが過ぎると、デバイスは全てのラベルフォワーディングエントリを削除します。「12 - 600」秒で指定可能です。「Default」を選択すると初期値を指定します。

「Apply」をクリックし、設定内容を適用します。

MPLS LSP Trigger Information（MPLS LSP トリガ情報）

本項目では、「Multiprotocol Label Switching」(MPLS)「Label-Switched Label-Switched Path」(LSP) トリガ情報の設定、表示を行います。LSP トリガフィルタルールは LSP 構築のトリガとなる IP ルート制御に使われる IP アクセスリストルールです。

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

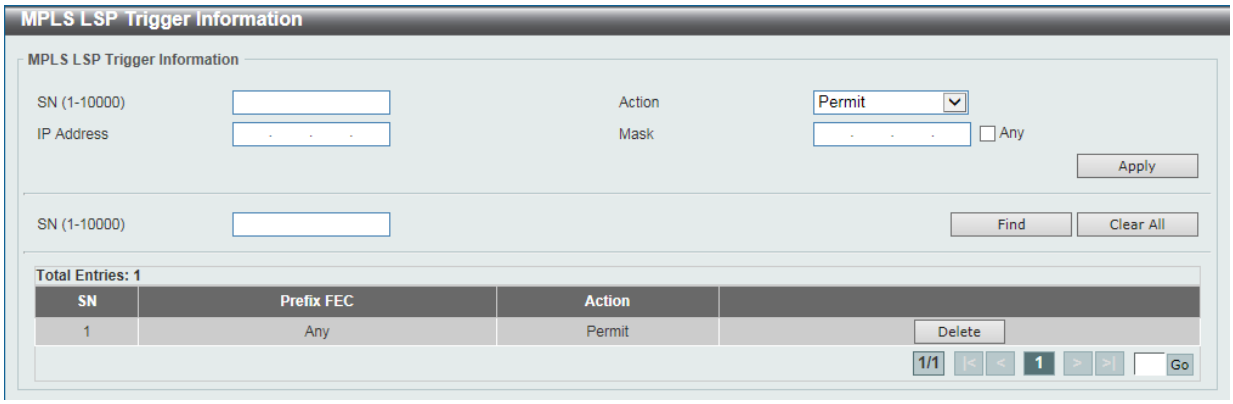


図 14-2　MPLS LSP Trigger Information 画面

以下の項目を設定できます。

項目	説明
SN	LSP トリガフィルタルールのシーケンス番号 (1-10000) を指定します。新しくルールを作成する場合に指定されていないと、SN は 10 から始まり 10 ずつ増加していきます。
Action	動作を指定します。 Permit - LSP 構築における LDP による IP prefix FEC フォローを許可します。 Deny - LSP 構築における LDP による IP prefix FEC フォローを許可しません。
IP Address	ルールが適用される IPv4 アドレス FEC を指定します。
Mask	ルールが適用されるサブネットマスク FEC を指定します。「Any」を選択するとどの IP プリフィクス FEC でも適用されます。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
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。

MPLS Forwarding Settings（MPLS フォワーディング設定）

本項目では、MPLS フォワーディングの設定、表示を行います。
「Static FTN Settings」セクションではスタティック「FEC-To-NHLFE」マップ (FTN) エントリの追加 / 削除を行います。FEC は「Forwarding Equivalence Class」を意味し、NHLFE は「Next Hop Label Forwarding Entry」を意味します。イングレス「Label Edge Router」(LER) では、「Forwarding Equivalence Class 」(FEC) に分類された内向きパケットは MPLS ラベルとともにプッシュされ、「FEC-to-NHLFE」(FTN) に従い、ネクストホップに転送されます。
「Static ILM Settings」セクションではスタティック「Incoming Label Map」(ILM) エントリの追加 / 削除を行います。LSR では内向きラベルにマッチした内向き MPLS パケット ILM の設定に基づき処理されます。ラベル操作は内向きトップラベルから設定した外向きラベルへ変換され、パケットはネクストホップに転送されます。

MPLS > MPLS Forwarding 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。

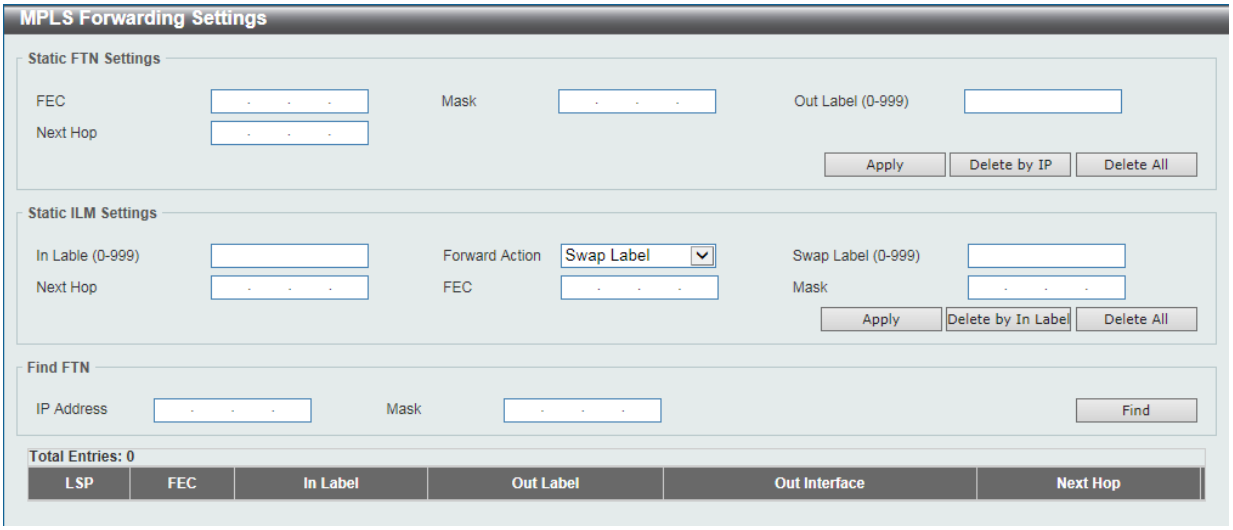


図 14-3　MPLS Forwarding Settings 画面

以下の項目を設定できます。

項目	説明
Static FTN Settings	
FEC	スタティック FTN の FEC IPv4 アドレスを指定します。
Mask	スタティック FTN の FEC サブネットマスクを指定します。
Out Label	FEC のアウトラベル値（0-999）を指定します。
Next Hop	FEC のネクストホップ IPv4 アドレスを指定します。
Static ILM Settings	
In Label	ILM の内向きラベル（0-999）を指定します。
Forward Action	転送動作について指定します。「Swap Label」「Pop」から指定します。
Swap Label	「Swap Label」を選択後、「Swap Label」（0-999）を指定します。
Next Hop	「Swap Label」を選択後、FEC のネクストホップ IPv4 アドレスを指定します。
FEC	「ILM」に関連する、FEC IPv4 アドレスを指定します。
Mask	「ILM」に関連する、FEC サブネットマスクを指定します。
Find FTN	
IP Address	FTN の FEC IPv4 アドレスを指定します。
Mask	FTN の FEC サブネットマスクを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete by IP」をクリックすると指定のエントリを IP アドレスに基づき削除します。
「Delete by In Label」をクリックすると指定のエントリを「In Label」に基づき削除します。
「Delete All」をクリックするとすべてのエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

注意　MPLS が無効な「Connected 経路」は、MPLS テーブルに載せることはできません。

MPLS LDP Neighbor Password Settings（MPLS LDP ネイバパスワード設定）

本項目では、MPLS LDP ネイバパスワードの設定、表示を行います。MD5 認証が有効な場合、同じパスワードを交換して、LSR はピアとのみセッションを構築します。パスワードの設定はリンクネイバかターゲットネイバとの交渉で適用されます。

MPLS > MPLS LDP Neighbor Password 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 14-4　MPLS LDP Neighbor Password Settings 画面

以下の項目を設定できます。

項目	説明
Neighbor IP	ネイバ IPv4 アドレスを指定します。ネイバ（ピア）の LSR ID でもあります。
Password	LDP ピアパスワードを指定します。「Default」を指定すると初期値（空欄）を使用します。

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

MPLS LDP Neighbor Targeted Settings（MPLS LDP ネイバターゲット設定）

本項目では、MPLS LDP ネイバターゲットの設定、表示を行います。LDP はネイバ検出のためにターゲットハローメッセージを指定の期間で送信します。検出されたネイバは、LDP はタイマを一時停止します。ネイバはネイバからのハローメッセージを一定期間内に受信しない場合、タイマは期限切れになります。

MPLS > MPLS LDP Neighbor Targeted 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。

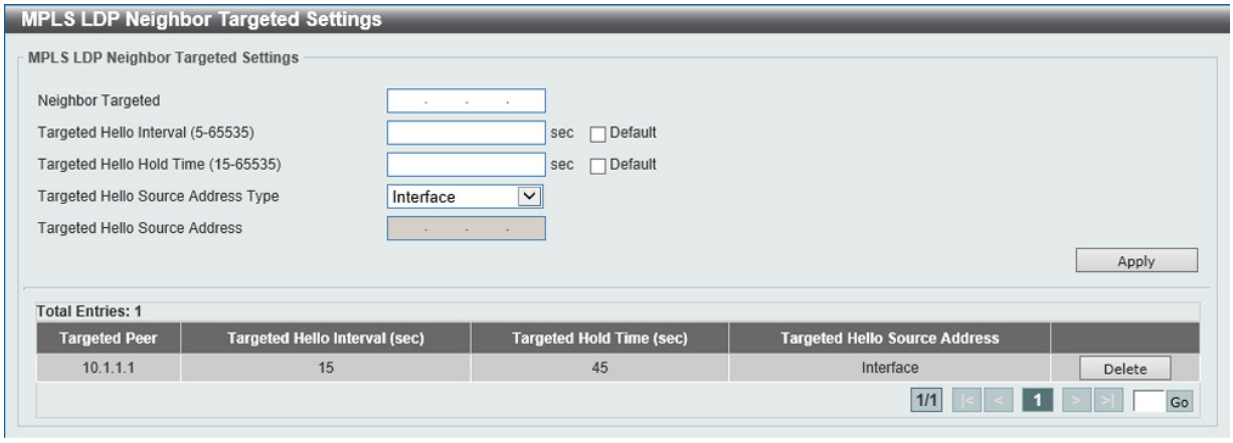


図 14-5　MPLS LDP Neighbor Targeted Settings 画面

以下の項目を設定できます。

項目	説明
Neighbor Targeted	使用するターゲットピアの IP アドレスを入力します。ターゲットとするピアの LSR ID とします。
Targeted Hello Interval	Target Hello メッセージを送信する間隔を入力します。この値は 5-65535(秒) である必要があります。 「Default」を指定すると初期値を使用します。
Targeted Hello Hold Time	Target Hello の保持時間を入力します。この値は 15-65535(秒) である必要があります。 「Default」を指定すると初期値を使用します。
Targeted Hello Source Address Type	Target Hello の送信元アドレスタイプを指定します。 • Interface - 各インタフェースの IP アドレスを指定します。 • Router ID - LSR ID (ルータ ID) を指定します。 • IP Address - 手動で入力した IP アドレスを指定します。
Targeted Hello Source Address	Target Hello の送信元アドレスとなる IP アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

MPLS LDP Neighbor Information（MPLS LDP ネイバ情報）

本項目では、MPLS LDP Neighbor Information（MPLS LDP ネイバ情報）の表示とクリアをします。

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

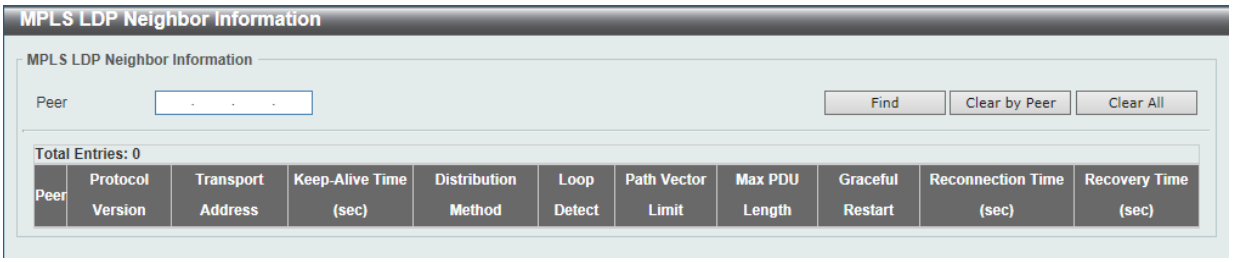


図 14-6　MPLS LDP Neighbor Information 画面

以下の項目を設定できます。

項目	説明
Peer	ピア LSR ID（IP アドレス）を入力します。

「Clear by Peer」をクリックすると入力したピア情報をクリアします。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

MPLS Global Settings（MPLS グローバル設定）

本項目では、MPLS Global Settings（MPLS グローバル設定）の設定、表示をします。

MPLS > MPLS 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。

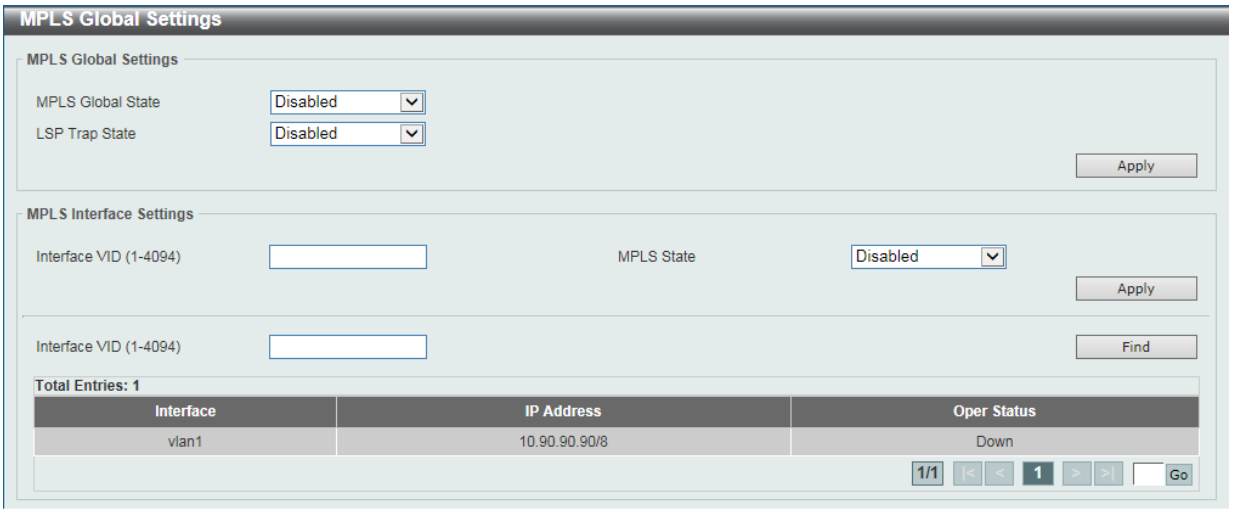


図 14-7　MPLS Global Settings 画面

以下の項目を設定できます。

項目	説明
MPLS Global Settings	
MPLS Global State	MPLS 機能を有効 / 無効に指定します。
LSP Trap State	MPLS LSP トラップを有効 / 無効に指定します。
MPLS Interface Settings	
Interface VID	インタフェース VLAN ID（1-4094）を指定します。
MPLS State	MPLS 機能を有効 / 無効に指定します。

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

MPLS LDP Interface Settings（MPLS LDP インタフェース設定）

本項目では、MPLS LDP Interface Settings（MPLS LDP インタフェース設定）の設定、表示をします。

MPLS > MPLS LDP 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。

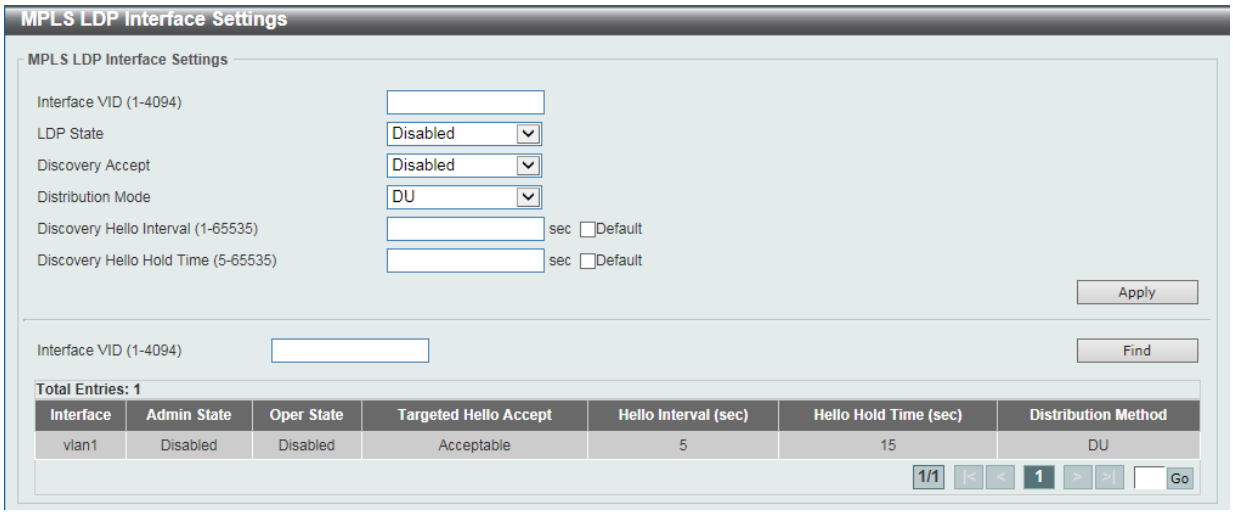


図 14-8　MPLS LDP Interface Settings 画面

以下の項目を設定できます。

項目	説明
Interface VID	インタフェース VLAN ID（1-4094）を指定します。
LDP State	LDP 機能をインタフェースで有効 / 無効に指定します。
Discovery Accept	「Discovery Accept」を有効 / 無効に指定します。「targeted hello message」の受信が無効の場合、そして受信「targeted hello」が設定されたローカルのターゲットピアから来たものではない場合、メッセージは無視されます。「targeted hello message」受信が有効の場合、LSR は全てのネイバから受信した「targeted hello messages」を評価します。
Distribution Mode	配布方式を選択します。「Default」を選択すると初期値（DU）を指定します。 • DU - 配布モードを「Downstream-Unsolicited」に設定します。 • DoD - 配布モードを「Downstream-on-Demand」に設定します。
Discovery Hello Interval	Discovery Hello メッセージを送信する間隔を入力します。この値は 1-65535(秒) である必要があります。 「Default」を指定すると初期値を使用します。
Discovery Hello Hold Time	Discovery Hello の保持時間を入力します。この値は 5-65535(秒) である必要があります。 「Default」を指定すると初期値を使用します。

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

MPLS LDP Session Information（MPLS LDP セッション情報）

本項目では、MPLS LDP Session Information（MPLS LDP セッション情報）の検出、表示をします。

MPLS > MPLS LDP 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。

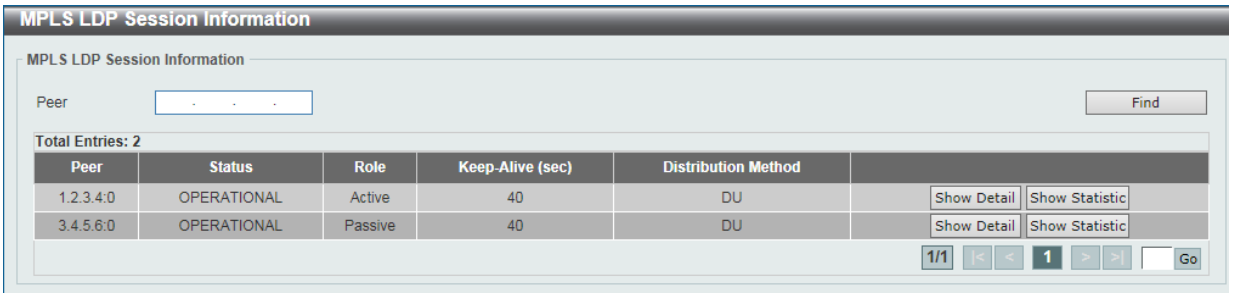


図 14-9　MPLS LDP Session Information 画面

以下の項目を設定できます。

項目	説明
Peer	LSR ID としての IP アドレスを指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show Statistics」をクリックして、統計情報を表示します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Show Detail」をクリックすると、以下の画面が表示されます。

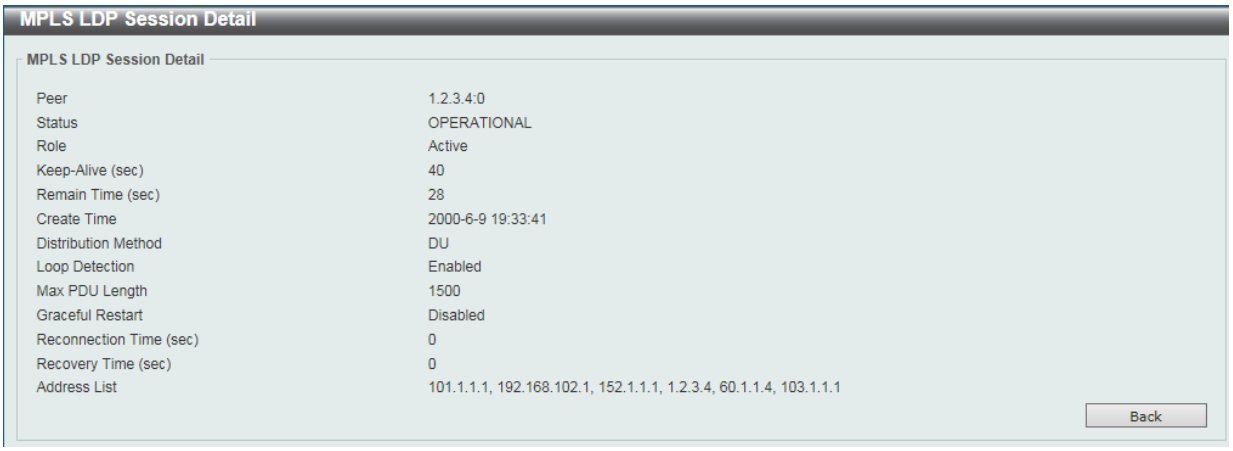


図 14-10　MPLS LDP Session Information (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

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

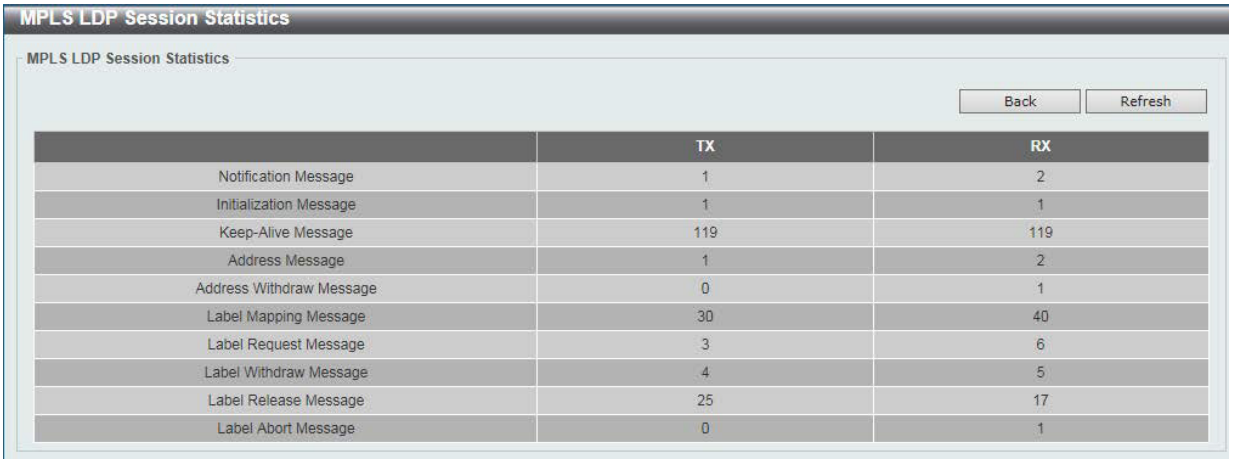


図 14-11　MPLS LDP Session Information (Show Statistics) 画面

「Back」をクリックすると前のページに戻ります。

MPLS LDP Statistic（MPLS LDP スタティスティック）

本項目では、MPLS LDP Statistic（MPLS LDP スタティスティック）の表示をします。

MPLS > MPLS LDP 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 14-12　MPLS LDP Statistic 画面

MPLS LDP Binding Table（MPLS LDP バインディングテーブル）

本項目では、MPLS LDP Binding Table（MPLS LDP バインディングテーブル）の表示をします。

MPLS > MPLS LDP Binding 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 14-13　MPLS LDP Binding Table 画面

MPLS LDP Discovery Information（MPLS LDP ディスカバリ情報）

本項目では、MPLS LDP Discovery Information（MPLS LDP ディスカバリ情報）の表示をします。

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

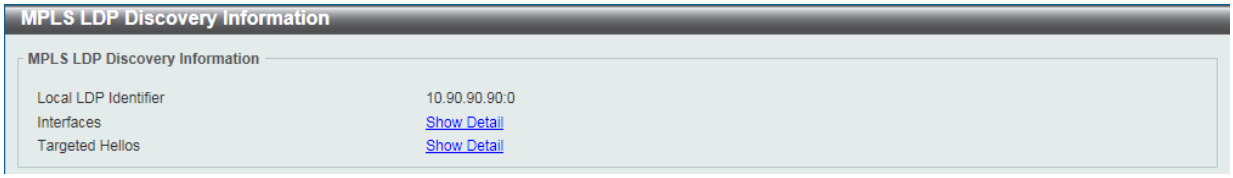


図 14-14　MPLS LDP Discovery Information 画面

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

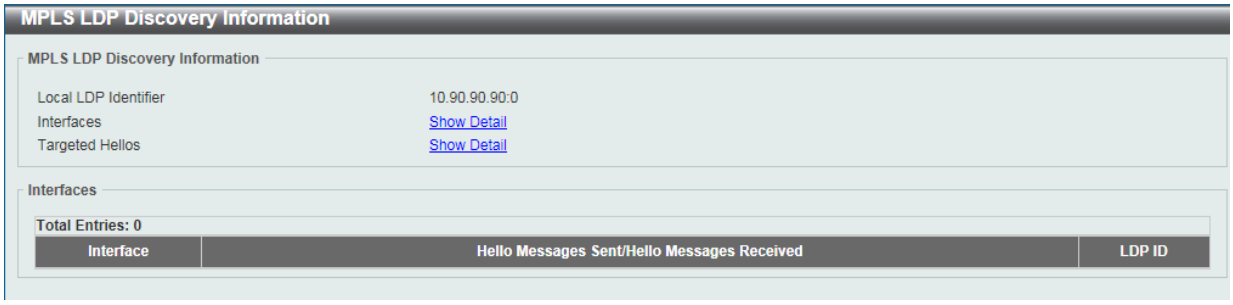


図 14-15　MPLS LDP Discovery Information (Show Detail) 画面

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

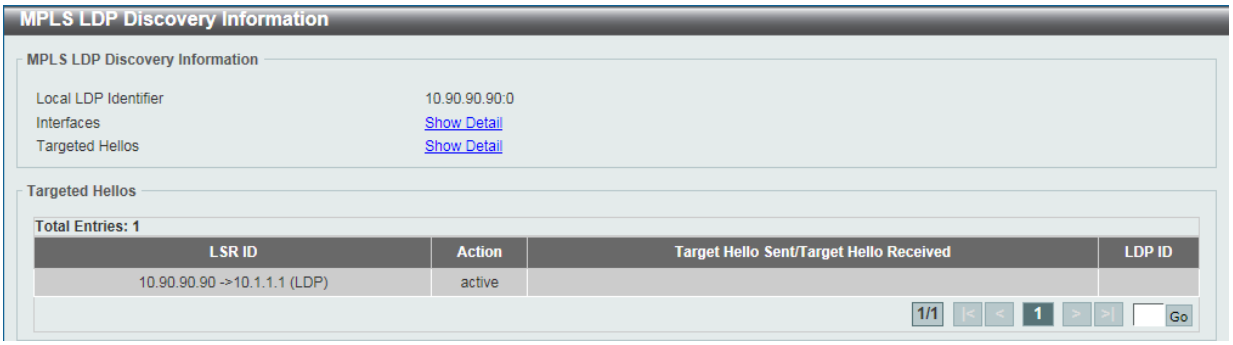


図 14-16　MPLS LDP Discovery Information (Show Detail - Targeted Hellos) 画面

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。

MPLS QoS Settings（MPLS QoS 設定）

本項目では、MPLS QoS Settings（MPLS QoS 設定）の設定、表示をします。

MPLS > MPLS QoS 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。

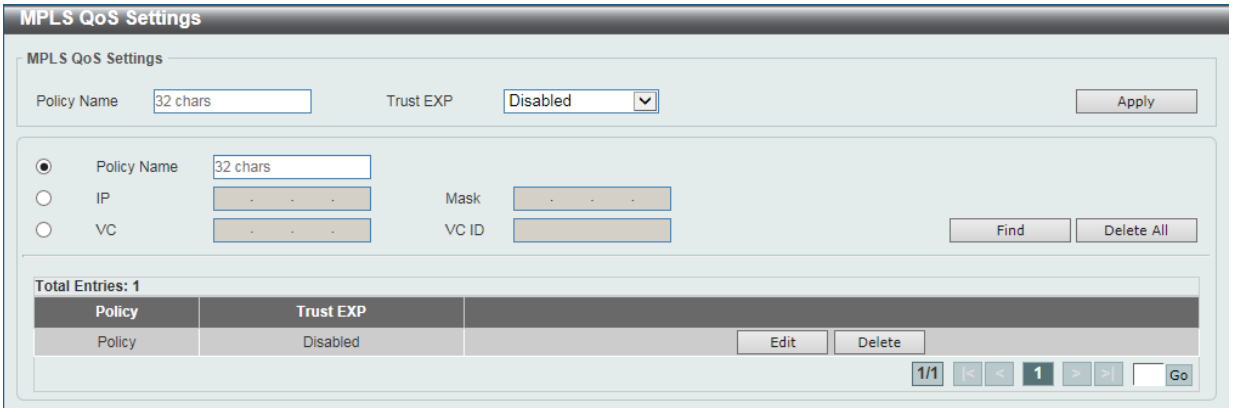


図 14-17　MPLS QoS Settings 画面

以下の項目を設定できます。

項目	説明
Policy Name	「MPLS QoS」ポリシー名（32 字以内）を指定します。「MPLS QoS」ポリシーは「MPLS FEC」に適用可能です。
Trust EXP	トラスト EXP 機能を有効 / 無効に指定します。EXP がトラストされると、マッチしたパケットは EXP に従い MPLS QoS ポリシーのプライオリティマッピングにスケジュールされます。 そうでない場合、パケットは「802.1p」プライオリティに従いスケジュールされます。
IP	QoS ポリシーに関連する FEC IP アドレスを指定します。
Mask	QoS ポリシーに関連する FEC サブネットマスクを指定します。
VC	QoS ポリシーに関連する FEC VC アドレスを指定します。
VC ID	QoS ポリシーに関連する FEC VC ID アドレスを指定します。

「Apply」をクリックし、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックすると指定のエントリを削除します。
「Delete All」をクリックするとすべてのエントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

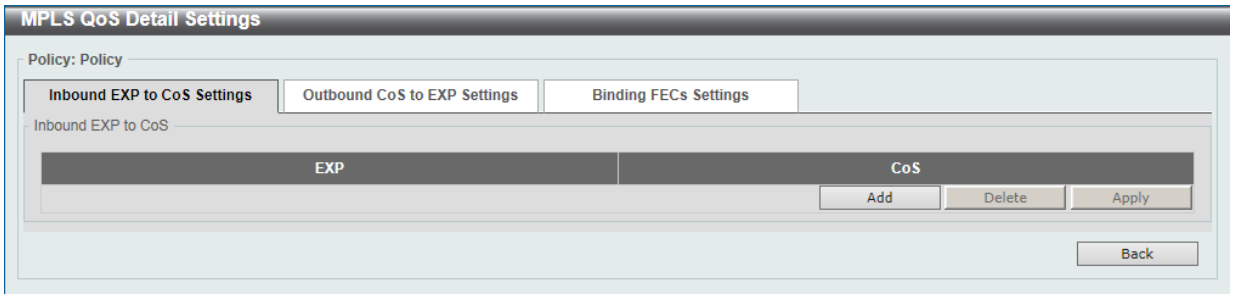


図 14-18 MPLS QoS Settings (Edit) 画面

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。
「Delete」をクリックすると指定のエントリを削除します。
「Add」をクリックするとエントリを追加します。

「Add」をクリックすると、以下の画面が表示されます。

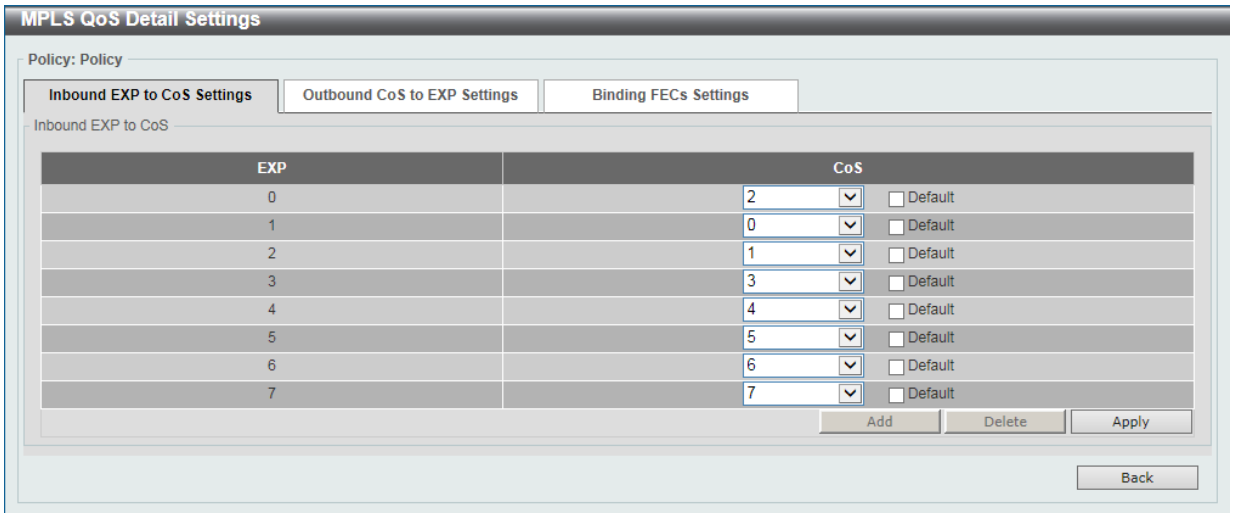


図 14-19 MPLS QoS Settings (Edit, Add) 画面

以下の項目を設定できます。

項目	説明
CoS	EXP 値にマップする CoS 値のリスト (0-7) を選択します。「Class of Service」(CoS) を「Experimental bits」(EXP) へのマッピングポリシーの設定を行います。「Default」を指定すると初期値を使用します。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

「Outbound CoS to EXP Settings」タブをクリックすると、以下の画面が表示されます。

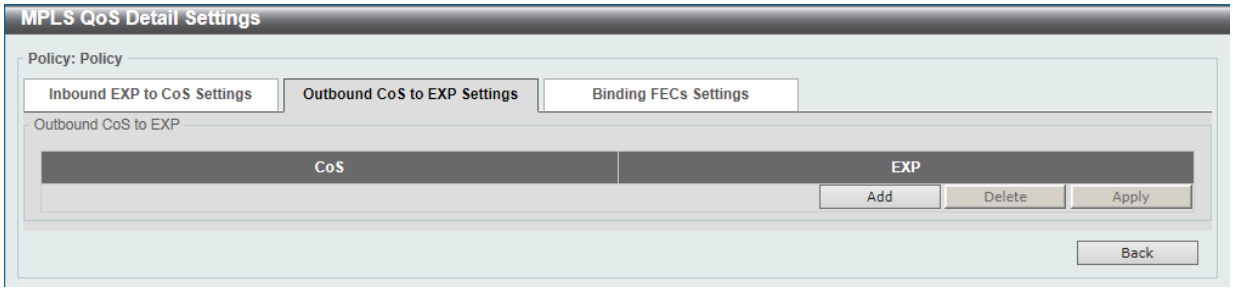


図 14-20 MPLS QoS Settings (Edit, Outbound CoS to EXP Settings) 画面

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。
「Delete」をクリックすると指定のエントリを削除します。
「Add」をクリックするとエントリを追加します。

「Add」をクリックすると、以下の画面が表示されます。

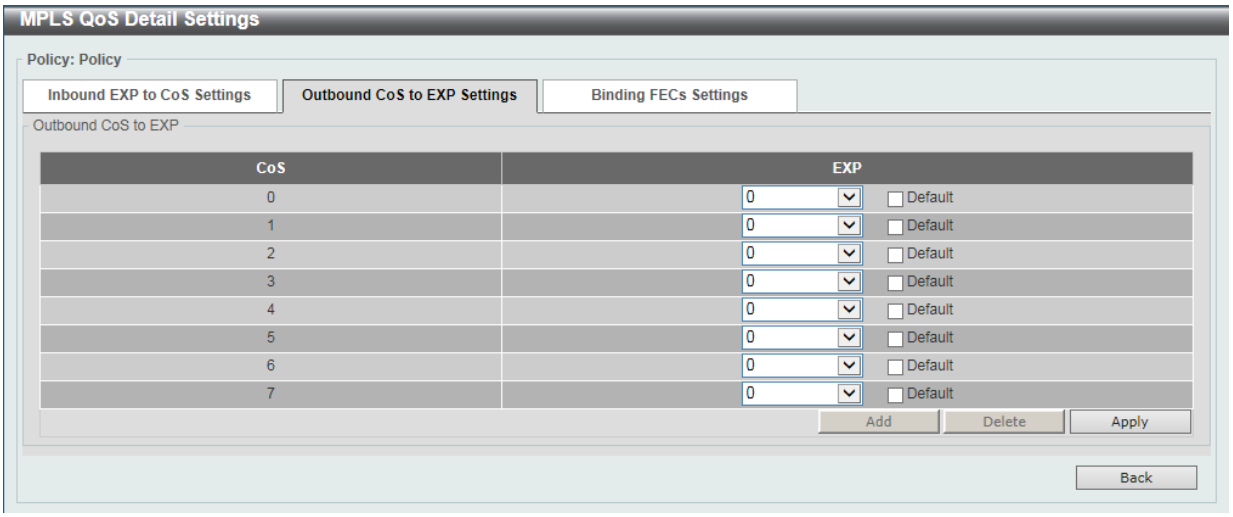


図 14-21　MPLS QoS Settings (Edit, Outbound CoS to EXP Settings, Add) 画面

以下の項目を設定できます。

項目	説明
EXP	CoS 値にマップする EXP 値（0-7）を選択します。「Default」を指定すると初期値を使用します。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

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

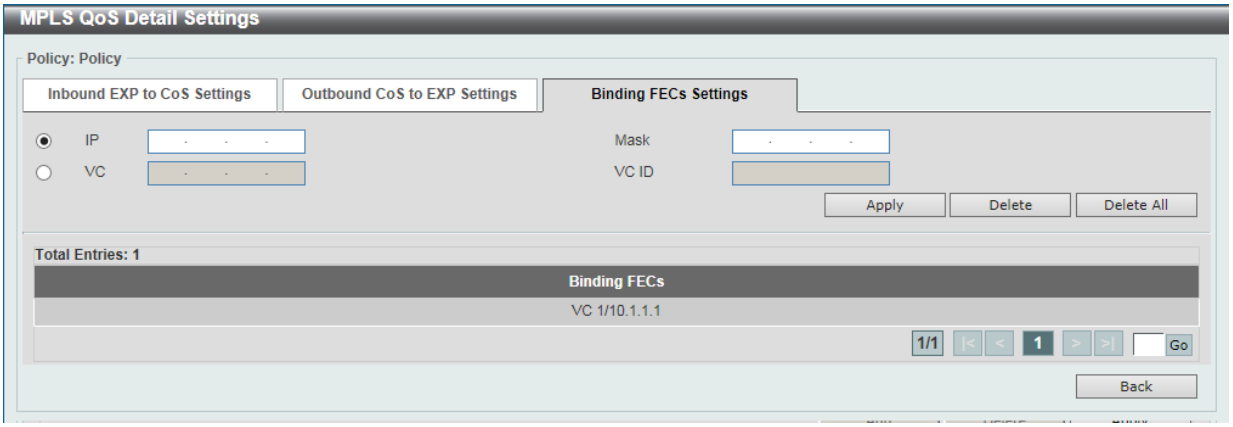


図 14-22　MPLS QoS Settings (Edit, Binding FECs Settings) 画面

以下の項目を設定できます。

項目	説明
IP	MPLS QoS ポリシーに関連する FEC IP アドレスを指定します。
Mask	FEC サブネットマスクを指定します。
VC	FEC VC アドレスを指定します。
VC ID	FEC VC ID を指定します。

「Apply」をクリックし、設定内容を適用します。
「Back」をクリックすると前のページに戻ります。

「Delete」をクリックすると指定のエントリを削除します。
「Delete All」をクリックするとすべてのエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Ping MPLS

本項目では、指定 FEC の LSP の接続状態を確認します。FEC に LSP がない場合、“Destination unreachable” メッセージが表示されます。そうでない場合は、「MPLS echo」リクエストメッセージが指定の FEC の LSP とともに送信されます。イーグレス LSR リクエストメッセージを受信した場合、「MPLS echo」返信メッセージをリクエストメッセージの送信者に返信します。送信者がタイムアウト前にメッセージを受信できない場合、“Request timed out” メッセージが表示されます。

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

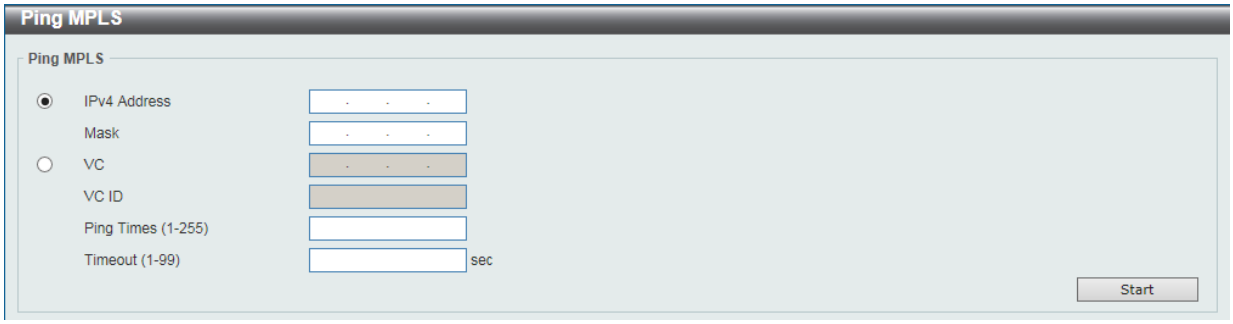


図 14-23 Ping MPLS 画面

以下の項目を設定できます。

項目	説明
IPv4 Address	接続性をチェックされる LSP の FEC IPv4 アドレスを指定します。
Mask	FEC サブネットマスクを指定します。
VC	FEC VC IP アドレスを指定します。
VC ID	FEC VC ID を指定します。
Ping Times	Ping の回数（1-255）を指定します。送信される Ping パケットの回数です。
Timeout	タイムアウト値（1-99 秒）を指定します。

「Start」をクリックし、MPLS Ping を開始します。

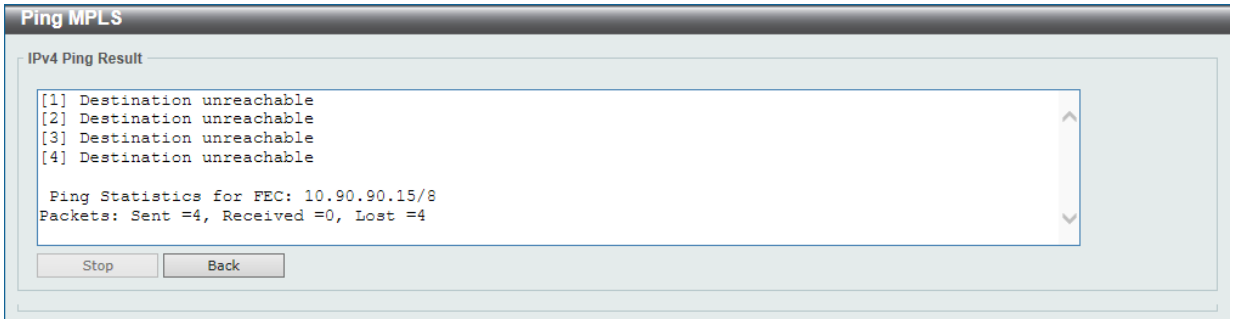


図 14-24 Ping MPLS (Start) 画面

「Stop」をクリックして MPLS Ping を停止します。
「Back」をクリックすると前のページに戻ります。

Traceroute MPLS IPv4（トレースルート MPLS IPv4）

本項目では、指定 FEC の LSP パストレースのような「hop-by-hop fault localization」を指定します。FEC に LSP がない場合、“Destination unreachable” メッセージが表示されます。そうでない場合は、「MPLS echo」リクエストメッセージが指定の FEC の LSP とともに送信されます。MPLS エコーリクエスト最遠ラベル内の TTL は 1、2、3 といった具合に設定されます。各 LSR においてエコーリクエストは期限が強制的に切れます。LSR は MPLS エコーリプライに戻ります。送信者がタイムアウト前に返信を受信できない場合、トレースルートは停止します。

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

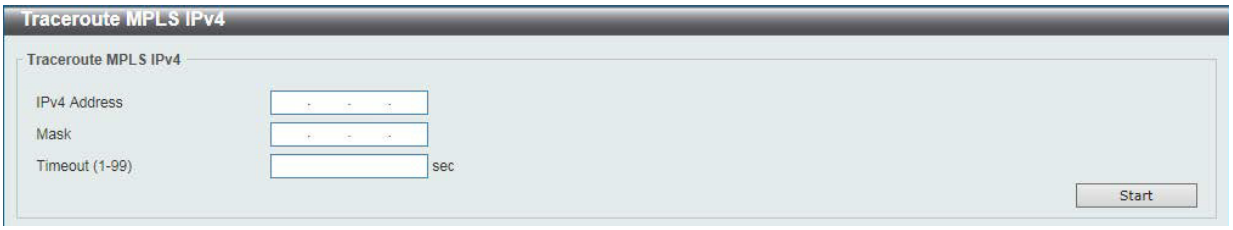


図 14-25 Traceroute MPLS IPv4 画面

以下の項目を設定できます。

項目	説明
IPv4 Address	接続性をチェックされる LSP の FEC IPv4 アドレスを指定します。
Mask	FEC サブネットマスクを指定します。
Timeout	タイムアウト値（1-99 秒）を指定します。

「Start」をクリックし、MPLS トレースルートを開始します。

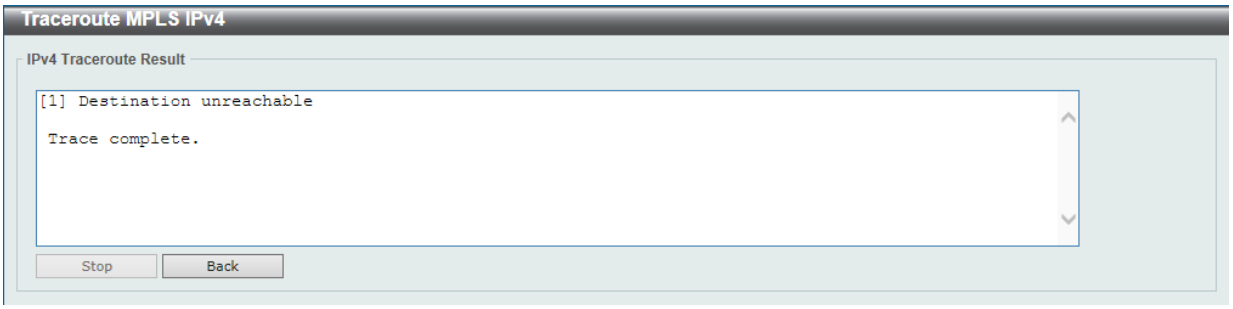


図 14-26 Traceroute MPLS IPv4 (Start) 画面

「Stop」をクリックして MPLS Ping を停止します。
「Back」をクリックすると前のページに戻ります。

第 15 章　MPLS L2VPN（MI モードのみ）

以下は MPLS L2VPN 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
VPWS Settings（VPWS 設定）	「Virtual Private Wire Service」(VPWS) を設定を行います。
L2VC Interface Description（L2VC インタフェース概要）	L2VC Interface Description（L2VC インタフェース概要）を設定を行います。
VPLS Settings（VPLS 設定）	「Virtual Private LAN Service」(VPLS) を設定を行います。
VPLS MAC Address Table（VPLS MAC アドレステーブル）	「VPLS MAC Address Table」（VPLS MAC アドレステーブル）を表示を行います。

注意　MPLS L2VPN については MI モードのみとなっています。

VPWS Settings（VPWS 設定）

本項目では、「Virtual Private Wire Service」(VPWS) を表示、設定を行います。

MPLS L2VPN > VPWS 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。

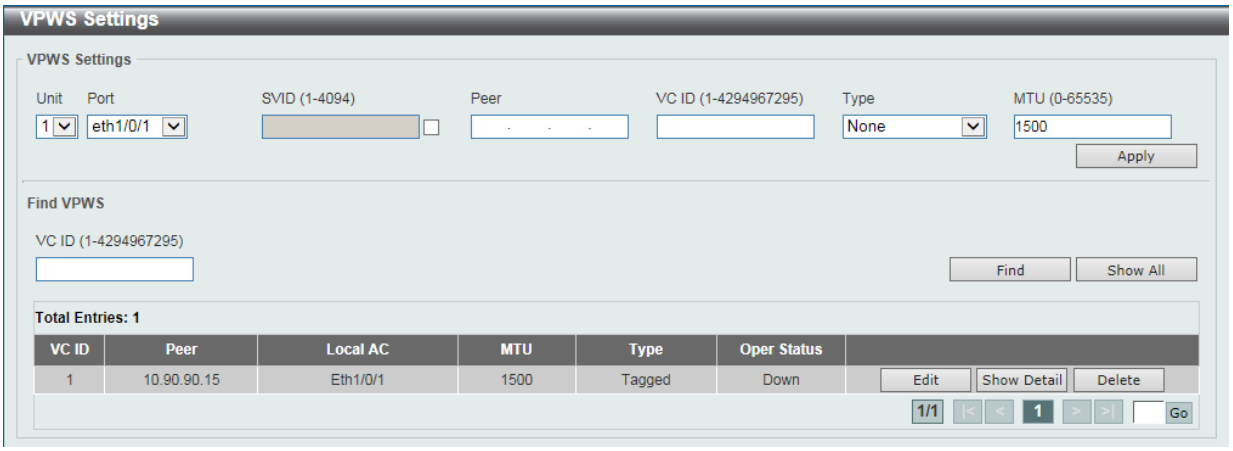


図 15-1　VPWS Settings 画面

以下の項目を設定します。

項目	説明
VPWS Settings	
Unit	設定を行うユニットを指定します。
Port	設定するポートを指定します。
SVID	カプセル化された VLAN ID（1-4094）を指定します。
Peer	PE のピア IP アドレスを入力します。ピア IP アドレスはその LSR ID とします。
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。この値は 1-4294967295 である必要があります。
Type	タイプを「None」「Manual」「Raw」「Tagged」「Manual Raw」「Manual Tagged」から指定します。 Raw モードで動作している場合、S- タグは PW には送信されません。Tagged モードで動作している場合、S- タグは PW に送信されます。初期値では PW タイプは Ethernet タグモードにあります。
MTU	リモートピアに通知されるローカルな CE PE リンクの MTU 値を入力します。MTU に 0 を指定すると、LDP はローカルな MTU に通知されません。MTU はローカルとリモートの両方で同じである必要があり、違う場合、PW は成功しません。指定しないと、MTU の初期値を使用します。MTU 値の初期値は 1500 です。この値は 0-65535 である必要があります。
Find VPWS	
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。この値は 1-4294967295 である必要があります。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

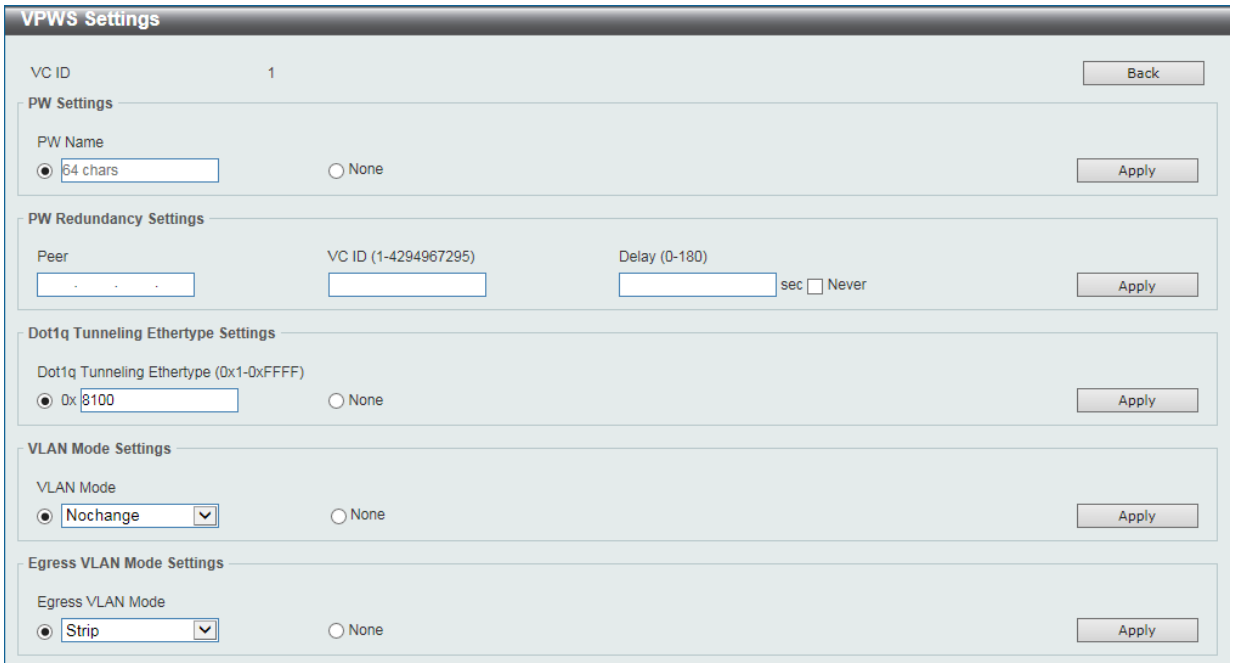


図 15-2　VPWS Settings (Edit) 画面

「Back」をクリックすると前のページに戻ります。

以下の項目を設定できます。

項目	説明
PW Settings	
PW Name	Pseudo-Wire (PW) 名（64 字以内）を入力します。「None」を指定すると初期値を使用します。
PW Redundancy Settings	
Peer	PE のピア IP アドレスを入力します。ピア IP アドレスはその LSR ID とします。
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。この値は 1-4294967295 である必要があります。
Delay	「Delay」値（0-180 秒）を指定します。指定の遅延時間の後にプライマリ PW に戻ります。「Never」を指定するとプライマリ PW へ戻る事はありません（初期値）。
Dot1q Tunneling Ethertype Settings	
Dot1q Tunneling Ethertype	サービス VLAN タグのアウタ TPID を指定します。 16 進数形式の「0x1-0xFFFF」で指定します。「None」を指定すると無効になります。
VLAN Mode Settings	
VLAN Mode	PW の VLAN モードを指定します。 • No Change - イングレスパケットの VLAN タグを変更しません。イーサネット VLAN ベース AC 時のみ有効です。 • Add VLAN - イングレスパケットの VLAN タグを追加します。ポートベース AC の初期動作は VLAN ID 0 の追加になります。イーサネット / イーサネット VLAN ベース AC 時のみ有効です。 • Change VLAN - イングレスパケットの VLAN タグを指定の VLAN ID に変更します。イーサネット VLAN ベース AC 時のみ有効です。 「None」を指定すると初期値を使用します。
Egress VLAN Mode Settings	
Egress VLAN Mode	PW のイーグレス VLAN モードを指定します。 • Strip - AC でイーグレスする前にパケットの「outer-tag」を分離します。 • Change VLAN - AC でイーグレスする前にパケットの「outer-tag」を AC の VLAN ID に変更します。イーサネット VLAN ベース AC 時のみ有効です。 「None」を指定すると初期値を使用します。

「Apply」をクリックし、設定内容を適用します。

「Show Detail」をクリックすると、以下の画面が表示されます。



図 15-3　VPWS Settings (Show Detail) 画面

L2VC Interface Description（L2VC インタフェース概要）

本項目では、L2VC Interface Description（L2VC インタフェース概要）を表示、設定を行います。

MPLS L2VPN > L2VC Interface Description の順にメニューをクリックし、以下の画面を表示します。

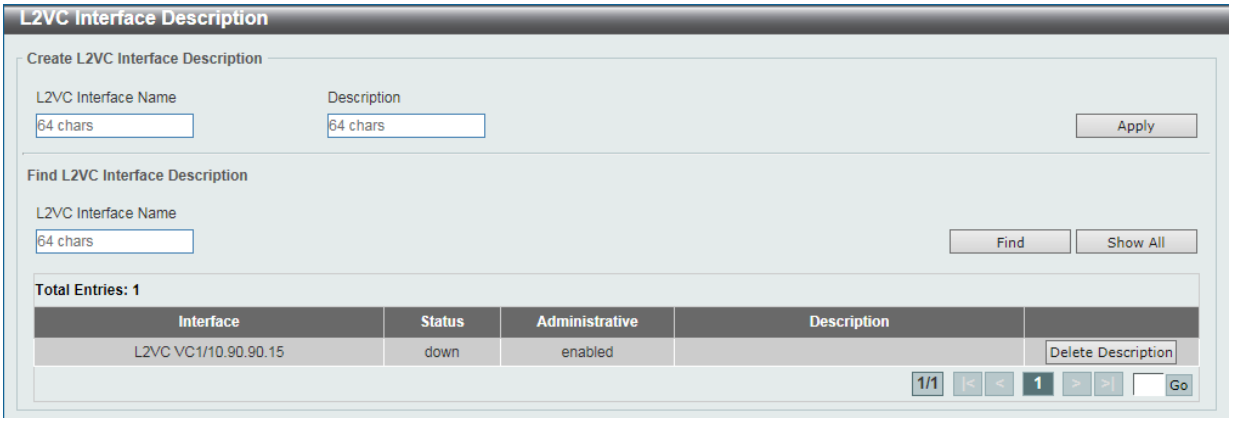


図 15-4　L2VC Interface Description 画面

以下の項目を設定します。

項目	説明
Create L2VC Interface Description	
L2VC Interface Name	L2VC インタフェース名（64 字以内）を指定します。
Description	L2VC インタフェース概要（64 字以内）を指定します。
Find L2VC Interface Description	
L2VC Interface Name	L2VC インタフェース名（64 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete Description」をクリックすると指定のエントリの概要を削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

VPLS Settings（VPLS 設定）

本項目では、「Virtual Private LAN Service」(VPLS) を表示、設定を行います。

MPLS L2VPN > VPLS 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。

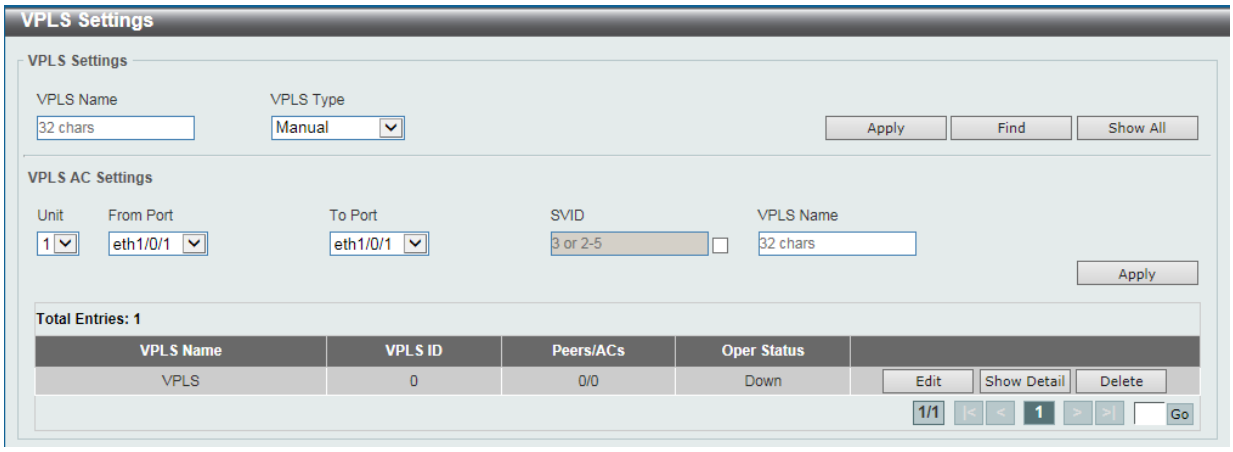


図 15-5　VPLS Settings 画面

以下の項目を設定します。

項目	説明
VPLS Settings	
VPLS Name	VPLS 名（32 字以内）を指定します。
VPLS Type	VPLS タイプを指定します。 • Manual - ネイバを手動で指定し、通達に LDP を使用します。 • Autodiscovery - ネイバを自動検出し、通達に BGP を使用します。
VPLS AC Settings	
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
SVID	SVID（1-4094）を指定します。
VPLS Name	VPLS 名（32 字以内）を指定します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックすると指定のエントリを削除します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Show Detail」をクリックして、指定エントリの詳細について表示します。
「Edit」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

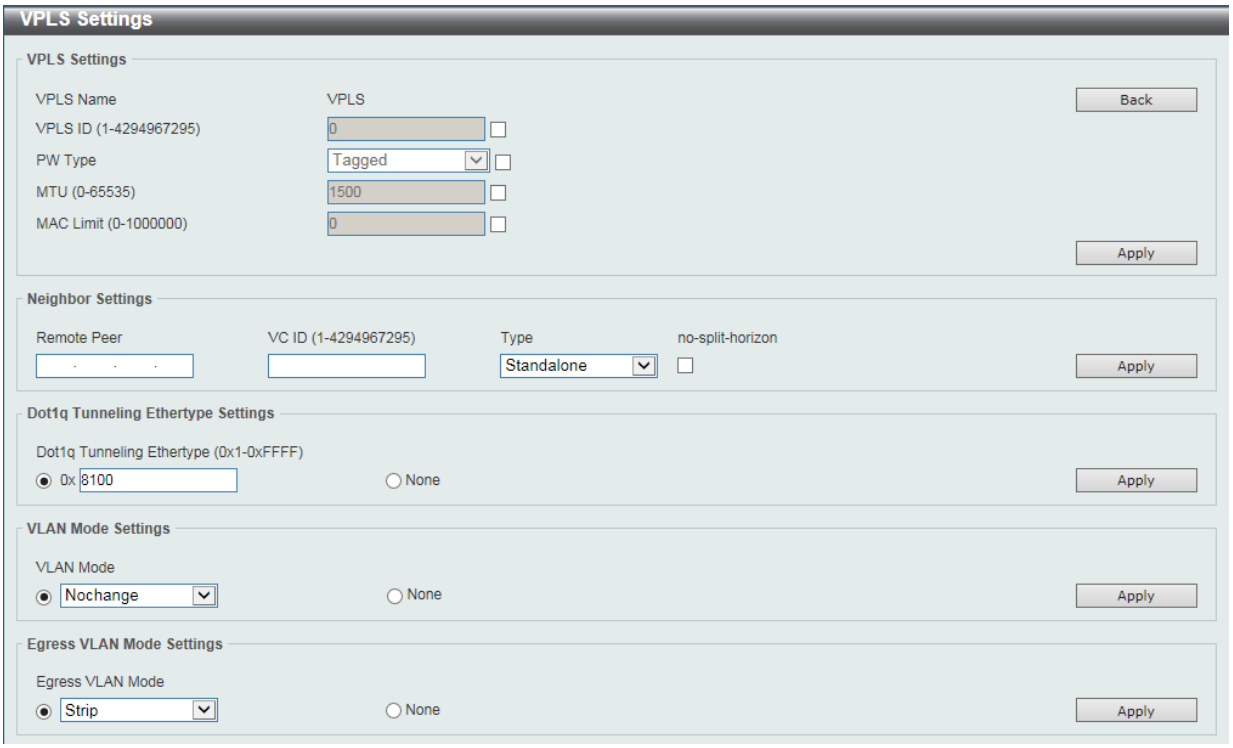


図 15-6　VPLS Settings (Edit) 画面

「Back」をクリックすると前のページに戻ります。

以下の項目を設定できます。

項目	説明
VPLS Settings	
VPLS ID	VPLS インスタンス ID を入力します。この値は「1-4294967295」である必要があります。
PW Type	PW タイプを「Raw」「Tagged」「Manual Raw」から指定します。 • Raw - イーサネット Raw モードでの動作を意味します。VPLS のすべての PW のカプセル化はイーサネット Raw モードで行われます。 • Tagged - イーサネット Tagged モードでの動作を意味します。VPLS のすべての PW のカプセル化はイーサネット Tagged モードで行われます。
MTU	リモートピアに通知される VPLS のローカルな AC リンクの MTU 値を入力します。MTU はローカルとリモートの両方で同じである必要があり、違う場合、PW は成功しません。MTU に 0 を指定すると、ローカルな MTU は VPLS のリモートピアに通知されません。指定しないと、MTU 値の初期値は 1500 です。この値は 0-65535 である必要があります。
MAC Limit	MAC リミットを指定します。VPLS の MAC アドレスエントリ学習制限値を指定します。「non-zero」MAC アドレス学習制限が指定、または MAC アドレス学習制限値を超えると、VPLS の未学習送信元 MAC アドレスのパケットは破棄されます。0-1000000 の間で指定可能です。
Neighbor Settings	
Remote Peer	PE がどのピアに属しているのかを識別する LSR ID を指定します。
VC ID	PW VC ID を入力します。この値は 1-4294967295 である必要があります。 VPLS のピアを固有に識別する IP アドレスに指定します。指定されないと「PW ID」は VPLS の VPN ID により指定されます。
Type	タイプを指定します。「Backup」「Standalone」から指定可能です。「Backup」オプションでは H-VPLS の PW 冗長のためにバックアップピアを作成します。
No-Split-Horizon	スポーク PW としてピアを使用します。 VPLS の他の PW からのパケットはこの PW に転送され、この PW からのパケットは VPLS のまた別の PW に転送されます。本オプションが指定されていない場合、ピアはネットワーク PW として使用されます。VPLS の他のネットワーク PW からのパケットこの PW には転送されません。そしてこの PW からのパケットは VPLS の他のネットワーク PW に転送されません。
Dot1q Tunneling Ethertype Settings	
Dot1q Tunneling Ethertype	サービス VLAN タグのアウタ TPID を指定します。 16 進数形式の「0x1-0xFFFF」で指定します。

項目	説明
VLAN Mode Settings	
VLAN Mode	PW の VLAN モードを指定します。 • No Change - イングレスパケットの VLAN タグを変更しません。イーサネット VLAN ベース AC 時のみ有効です。 • Add VLAN - イングレスパケットの VLAN タグを追加します。ポートベース AC の初期動作は VLAN ID 0 の追加になります。イーサネット / イーサネット VLAN ベース AC 時のみ有効です。 • Change VLAN - イングレスパケットの VLAN タグを指定の VLAN ID に変更します。イーサネット VLAN ベース AC 時のみ有効です。 「None」を指定すると初期値を使用します。
Egress VLAN Mode Settings	
Egress VLAN Mode	PW のイーグレス VLAN モードを指定します。 • Strip - AC でイーグレスする前にパケットの「outer-tag」を分離します。 • Change VLAN - AC でイーグレスする前にパケットの「outer-tag」を AC の VLAN ID に変更します。イーサネット VLAN ベース AC 時のみ有効です。 「None」を指定すると初期値を使用します。

「Apply」をクリックし、設定内容を適用します。

「Show Detail」をクリックすると、以下の画面が表示されます。

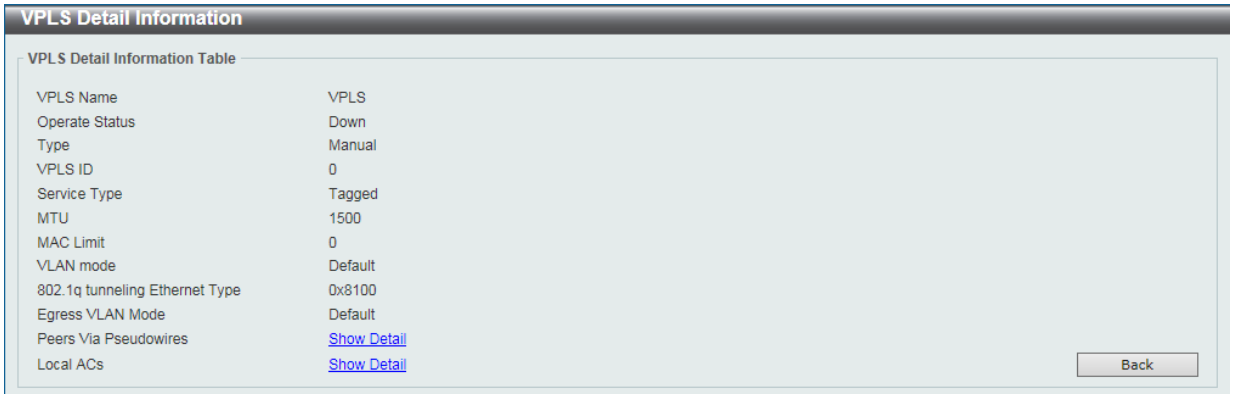


図 15-7　VPLS Settings (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

「Peers Via Pseudowires」の「Show Detail」をクリックすると、以下の画面が表示されます。

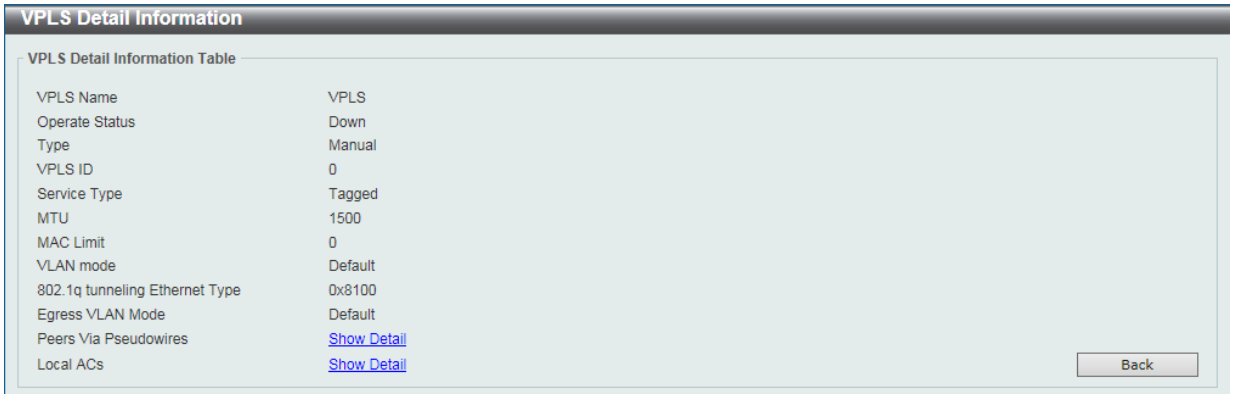


図 15-8　VPLS Settings (Show Detail) 画面

「Back」をクリックすると前のページに戻ります。

VPLS MAC Address Table（VPLS MAC アドレステーブル）

本項目では、VPLS MAC Address Table（VPLS MAC アドレステーブル）を表示、クリアを行います。

MPLS L2VPN > VPLS 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。

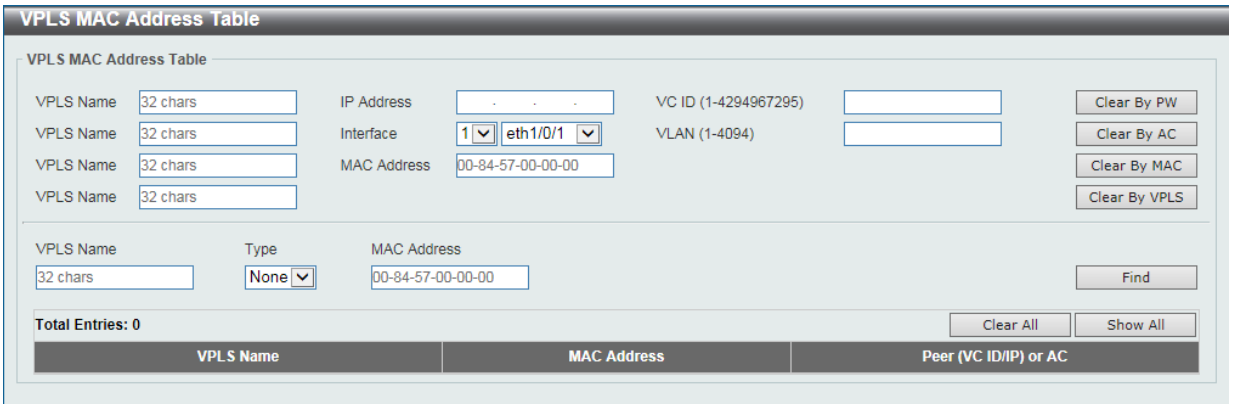


図 15-9　VPLS MAC Address Table 画面

以下の項目を設定します。

項目	説明
VPLS Name	VPLS インスタンス名（32 字以内）を指定します。
IP Address	ピアが属する PE を識別する LSR ID を指定します。
VC ID	PW VC ID（1-4294967295）を指定します。
Interface	設定を行うユニット / ポートを指定します。
VLAN	VLAN ID（1-4094）を指定します。
MAC Address	MAC アドレスを指定します。
Type	サーチクエリでの情報を指定します。「None」「Peer」「AC」から指定します。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。
「Clear All」をクリックすると入力したエントリを全てクリアします。
「Clear By PW」をクリックして指定した「PW」に関連する情報をクリアします。
「Clear By AC」をクリックして指定した「AC」に関連する情報をクリアします。
「Clear By MAC」をクリックして指定した「MAC」に関連する情報をクリアします。
「Clear By VPLS」をクリックして指定した「VPLS」に関連する情報をクリアします。

第 16 章　Monitoring（スイッチのモニタリング）

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

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

サブメニュー	説明
VLAN Counter（VLAN カウンタ）	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを指定します。
Utilization（利用分析）	スイッチの Utilization（利用分析）を表示します。
Statistics（統計情報）	スイッチの Statistics（統計情報）を表示します。
Mirror Settings（ミラー設定）	ミラーリング機能の設定を行います。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、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）があります。
sFlow（sFlow 設定）	sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。
Device Environment（機器環境確認）	Device Environment（機器環境確認）ではスイッチの内部の温度状態を表示します。
External Alarm Settings（外部アラーム設定）	外部アラーム設定はアラーム起動時のアラームメッセージについて設定します。

VLAN Counter（VLAN カウンタ）

本画面では、VLAN カウンタの設定、表示を行います。指定の L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを指定します。

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

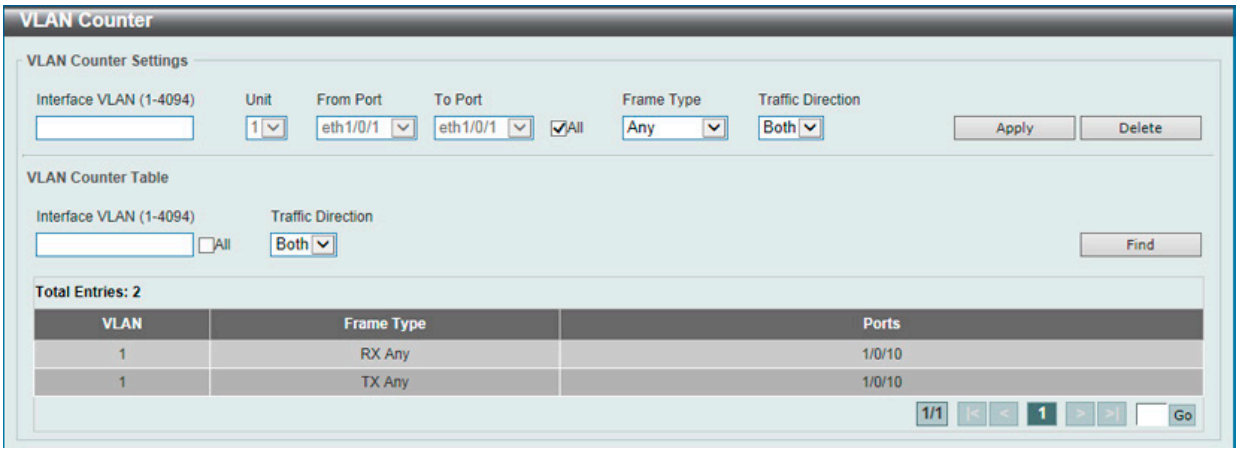


図 16-1　VLAN Counter 画面

以下の設定項目が使用できます。

項目	説明
VLAN Counter Settings	
Interface VLAN	インタフェース VLAN（1-4094）を指定します。
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの始点 / 終点を設定します。「All」を指定すると全ポートを指定します。
Frame Type	フレームタイプを指定します。 • Broadcast - ブロードキャストフレームのみをカウントします。 • Multicast - マルチキャストフレームのみをカウントします。 • Unicast - ユニキャストフレームのみをカウントします。 • Any - フレームタイプに関係なく全てのフレームをカウントします。 • All - 上記全てのフレームをカウントします。
Traffic Direction	トラフィックの向きを指定します。 • RX - イングレストラフィックを指定します。 • TX - イーグレストラフィックを指定します。 ・Both - 両方のトラフィックをカウントします。
VLAN Counter Table	
Interface VLAN	インタフェース VLAN（1-4094）を指定します。「All」を指定すると全 VLAN を指定します。
Traffic Direction	トラフィックの向きを指定します。 • RX - イングレストラフィックを指定します。 • TX - イーグレストラフィックを指定します。 ・Both - 両方のトラフィックをカウントします。

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、入力した情報を元に指定のエントリを検出します。
「Detele」ボタンをクリックし、指定したエントリを削除します。

Utilization（利用分析）

CPU 使用率、ポートの帯域使用率などを表示します。

Port Utilization（ポート使用率）

本画面では、ポートの帯域使用率を表示します。

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

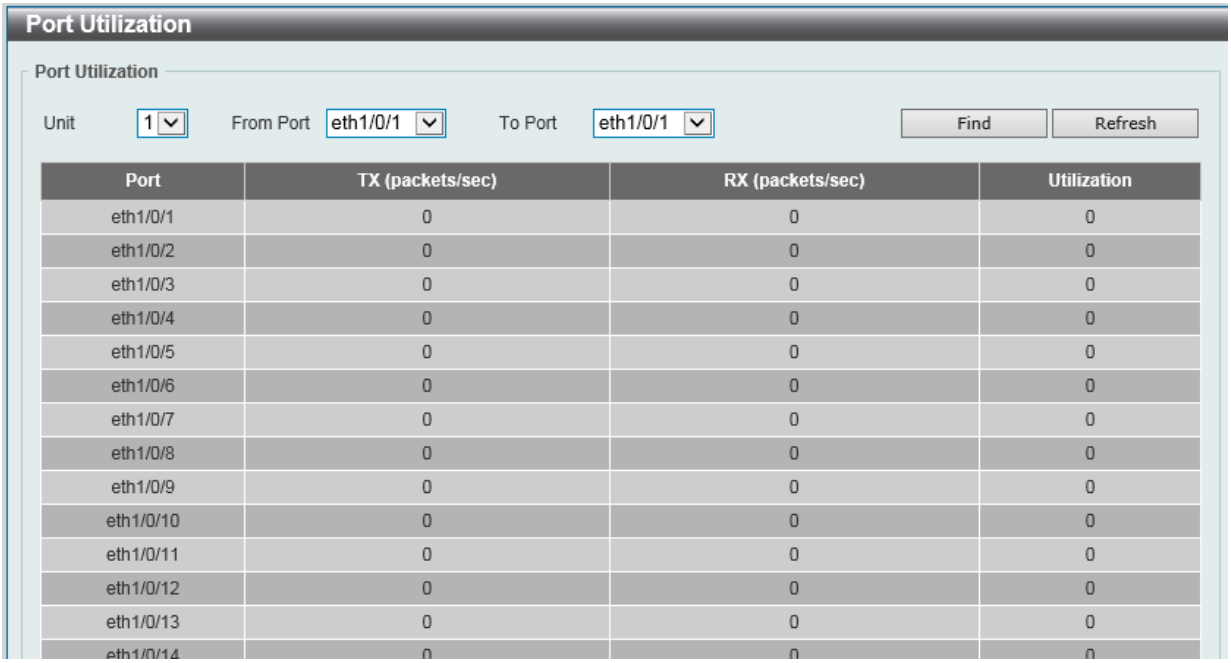


図 16-2　Port Utilization 画面

以下の設定項目が使用できます。

項目	説明
Unit	表示するユニットを指定します。
Port	プルダウンメニューで統計情報を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、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。

History Utilization（使用履歴）

本項目ではメモリ、CPU およびポートの使用履歴について表示します。

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

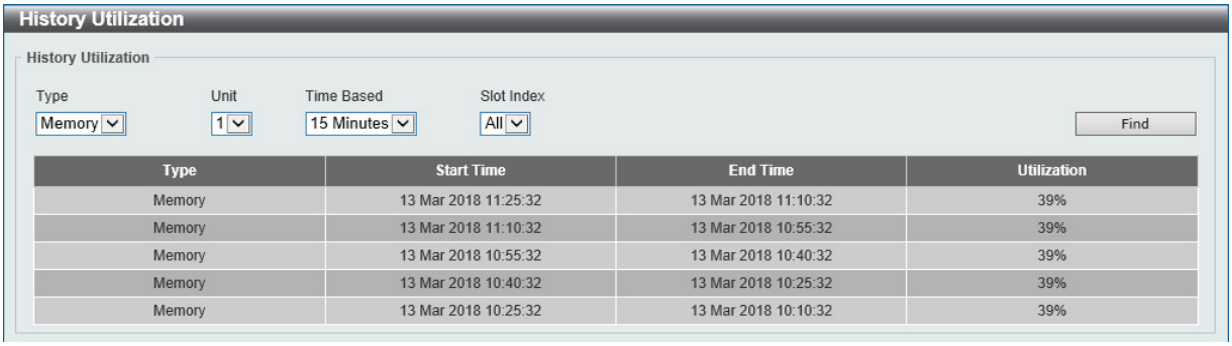


図 16-3　History Utilization (Memory) 画面

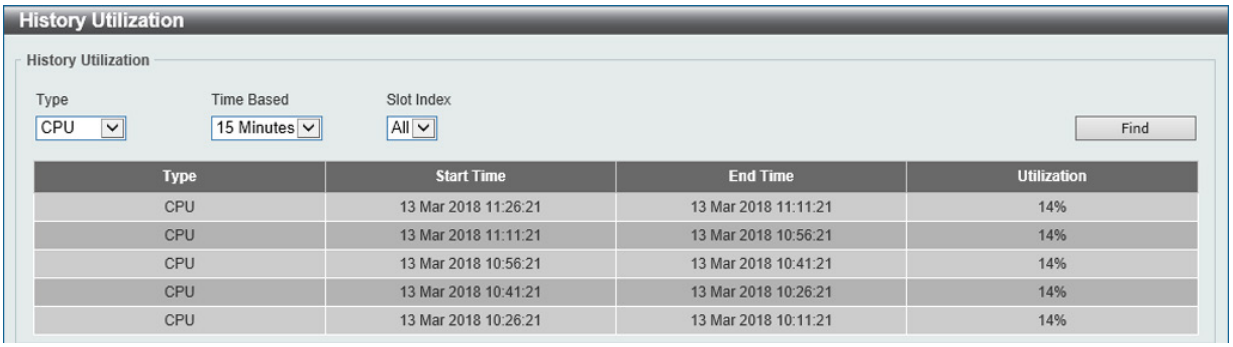


図 16-4　History Utilization (CPU) 画面

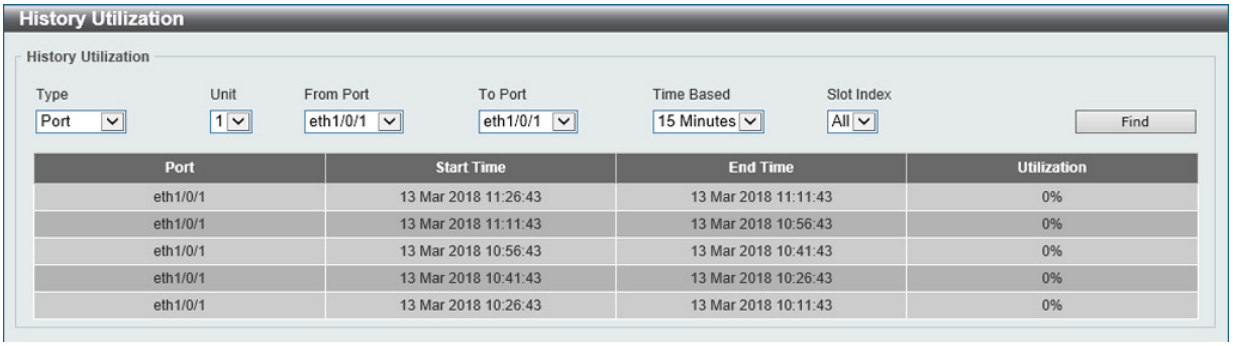


図 16-5　History Utilization (Port) 画面

以下の設定項目が使用できます。

項目	説明
Type	表示する使用項目を指定します。 • Memory - メモリの使用履歴を表示します。 • CPU - CPU の使用履歴を表示します。 • Port - ポートの使用履歴を表示します。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。
Time Based	表示する統計情報の期間を指定します。 • 15 Minutes - 15 分間の使用情報を表示します。 • 1 Day - 1 日の使用情報を表示します。 「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。
Slot Index	スロットのインデックスを指定します。「All」、「1-5」（15 Minutes 選択時）、「1-2（1 Day 選択時）」で指定可能です。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。

Statistics（統計情報）

スイッチの統計情報を表示します。

Port（ポート統計情報）

ポートのパケット情報を表示します。

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。

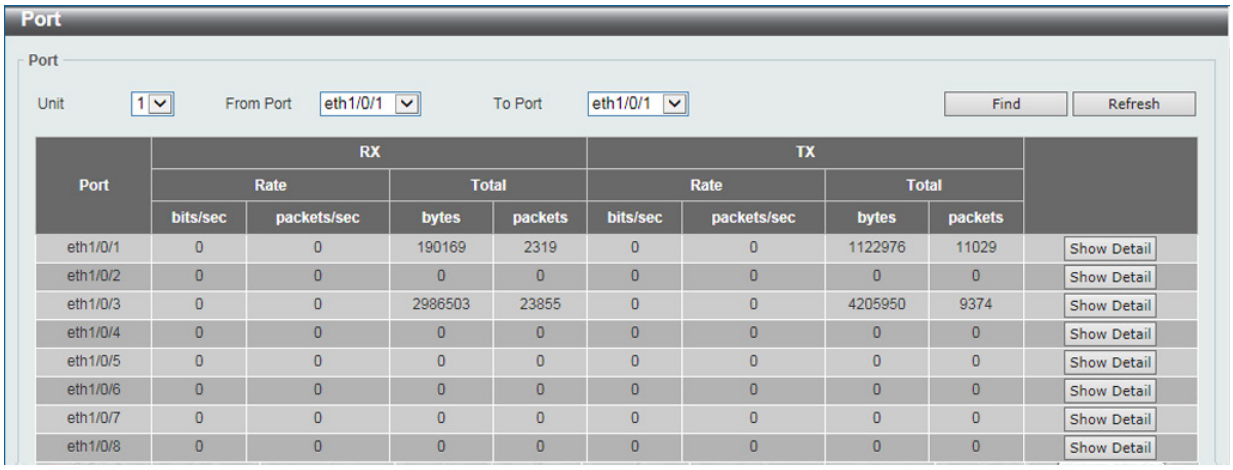


図 16-6　Port Statistics 画面

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
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、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。

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

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

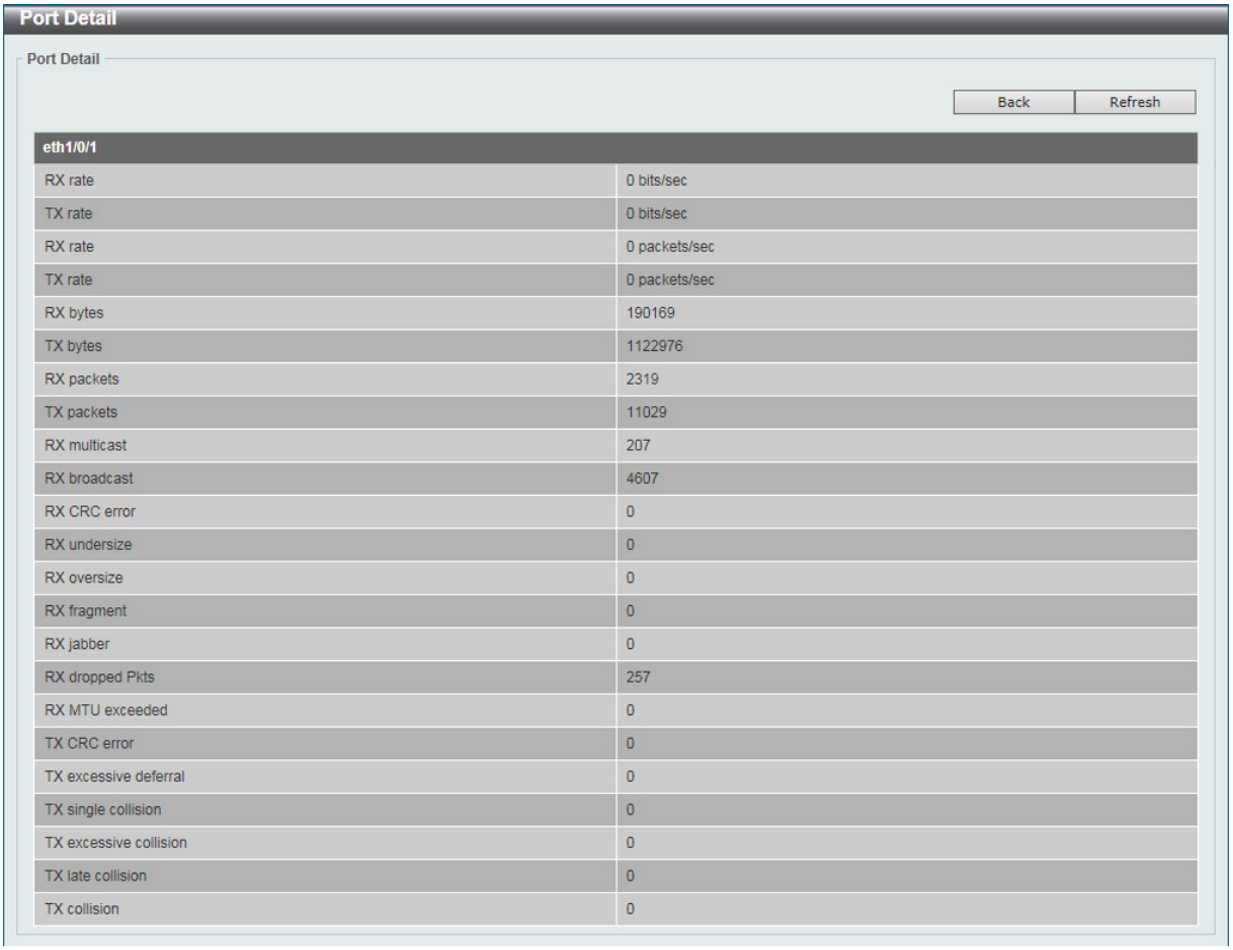


図 16-7　Port Statistics - Show Detail 画面

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

CPU Port（CPU ポート）

CPU の統計情報について表示します。

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

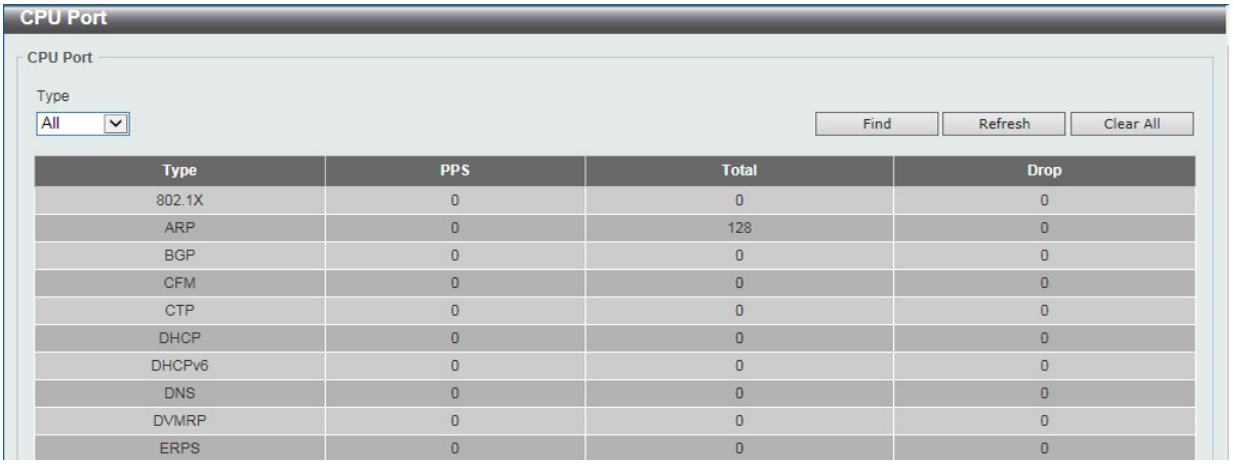


図 16-8　CPU Port 画面

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	表示するタイプを指定します。「All」「L2」「L3」「Protocol」から指定可能です。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。

「Refresh」ボタンをクリックし、テーブルを再起動します。
「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。

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。

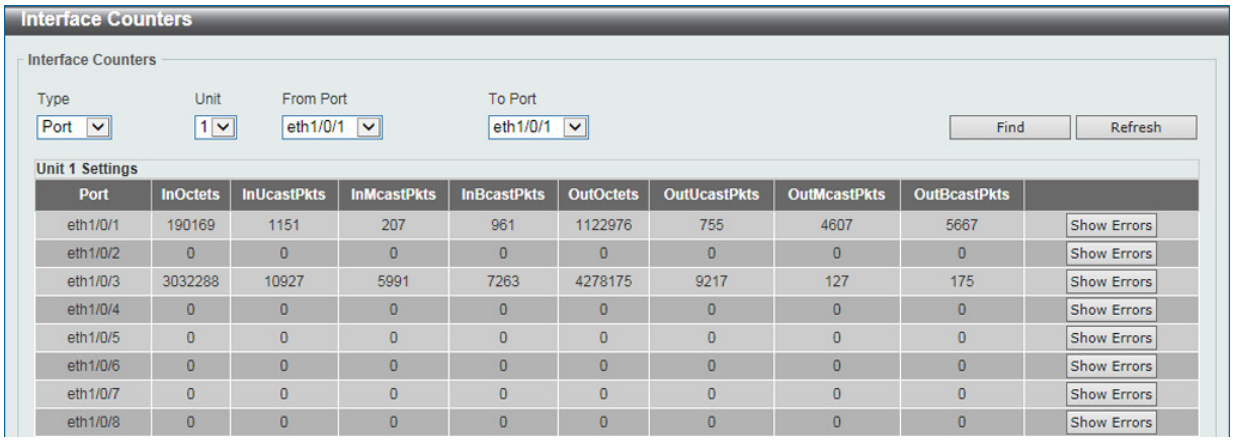


図 16-9　Interface Counters 画面

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	表示するタイプを指定します。「Port」「VLAN」から指定可能です。
Unit	設定を行うユニットを指定します。
From Port / To Port	設定するポートの始点 / 終点を設定します。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。
「Show Errors」ボタンをクリックすると、指定ポートのエラー情報について表示します。

「Show Errors」ボタンをクリックすると、次の画面が表示されます。

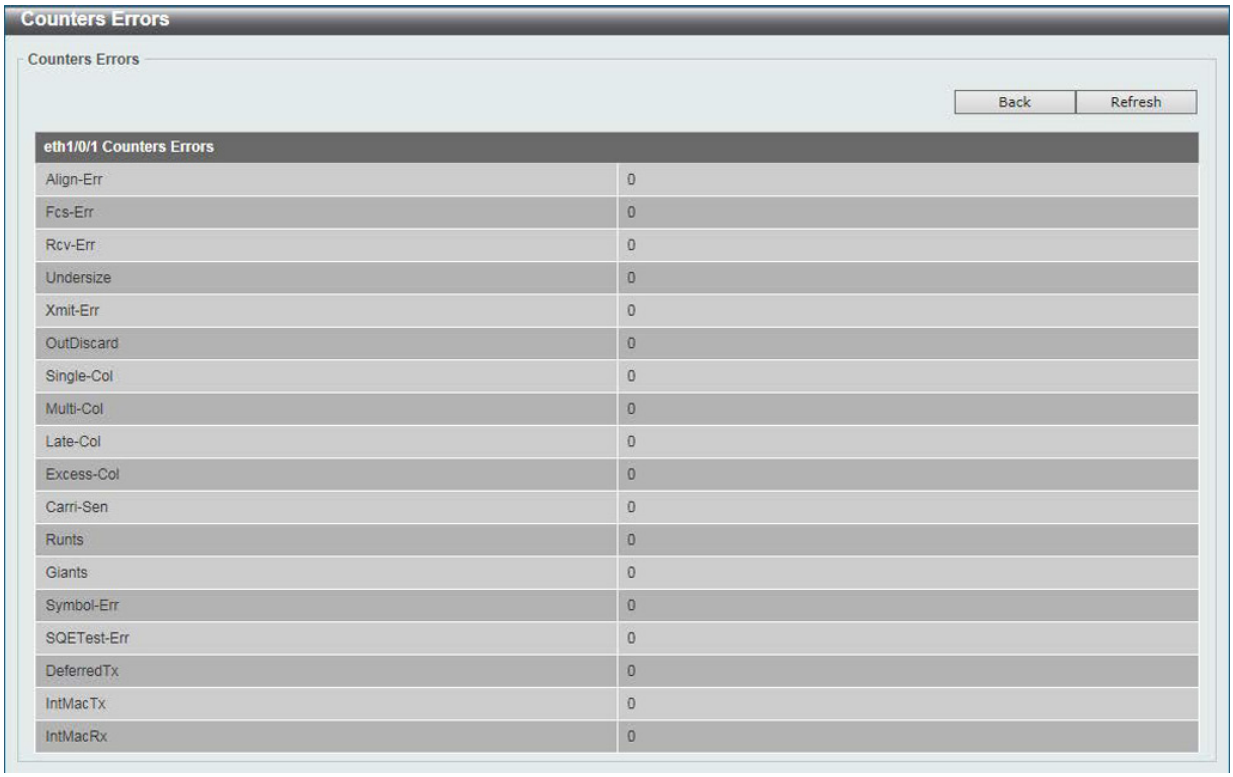


図 16-10　Interface Counters (Show Errors) 画面

「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、テーブルを再起動します。

「Type」で「VLAN」を選択すると、次の画面が表示されます。



図 16-11　Interface Counters (VLAN) 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	表示するタイプを指定します。「Port」「VLAN」から指定可能です。
Interface VLAN	表示する VLAN ID を指定します。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。

Interface History Counters（インタフェースカウント履歴）

本項目ではインタフェースにおけるカウンタの履歴を表示します。

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

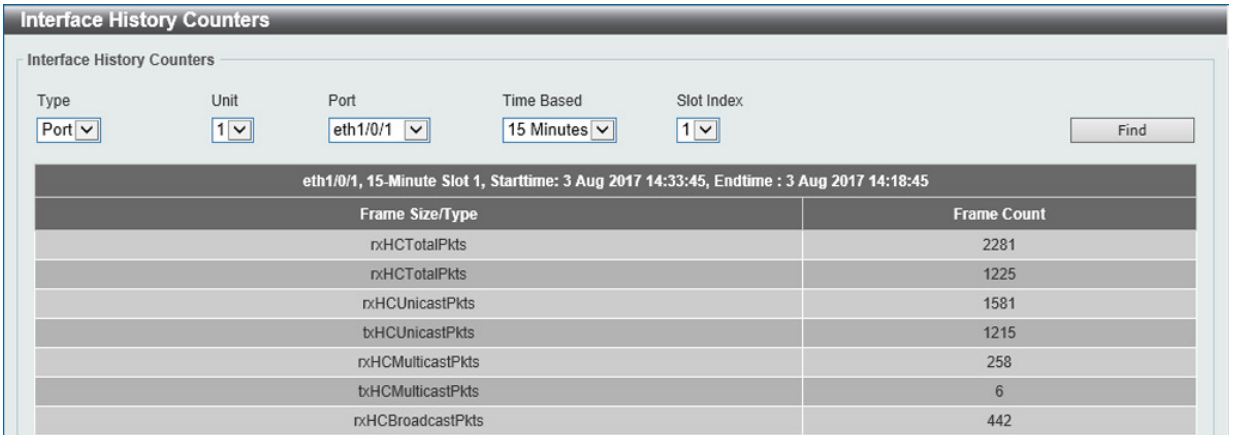


図 16-12　Interface History Counters 画面

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。
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。
Time Based	表示する統計情報の期間を指定します。 • 15 Minutes - 15 分間の使用情報を表示します。 • 1 Day - 1 日の使用情報を表示します。 「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。
Slot Index	スロットのインデックスを指定します。「All」、「1-5」（15 Minutes 選択時）、「1-2（1 Day 選択時）」で指定可能です。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。

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。

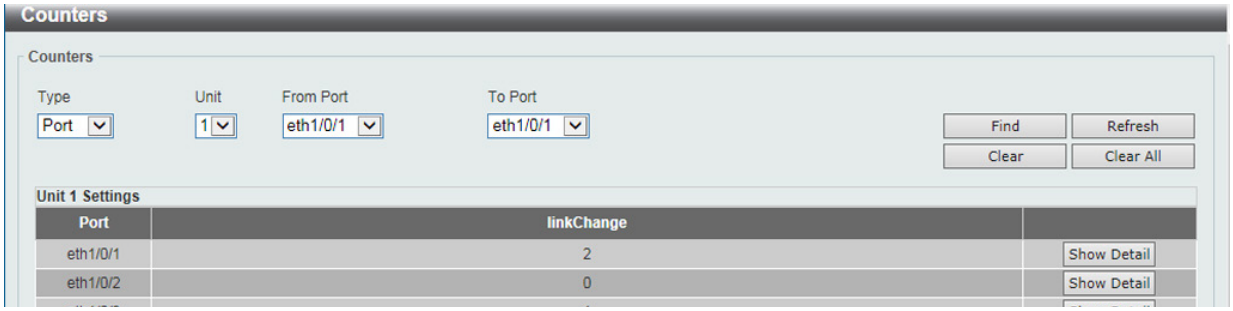


図 16-13　Counters 画面

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	表示するタイプを指定します。「Port」「VLAN」から指定可能です。
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、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。
「Clear」ボタンをクリックし、指定ポートの情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。
「Show Detail」ボタンをクリックし、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

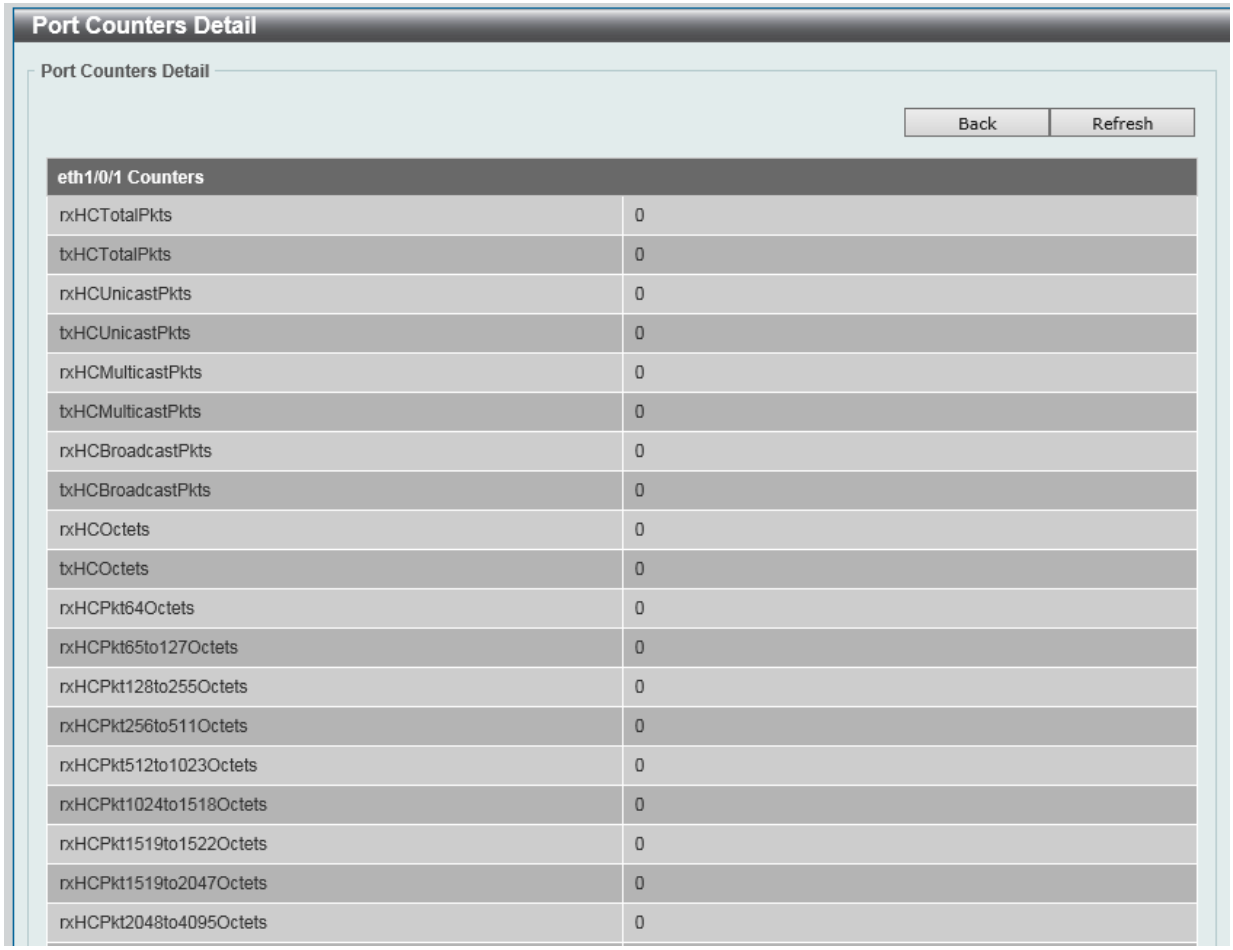


図 16-14　Port Counters Detail 画面

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

「Type」で「VLAN」を選択すると、次の画面が表示されます。



図 16-15　Interface Counters (VLAN) 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	表示するタイプを指定します。「Port」「VLAN」から指定可能です。
Interface VLAN	表示する VLAN ID を指定します。

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

Mirror Settings（ミラー設定）

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

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

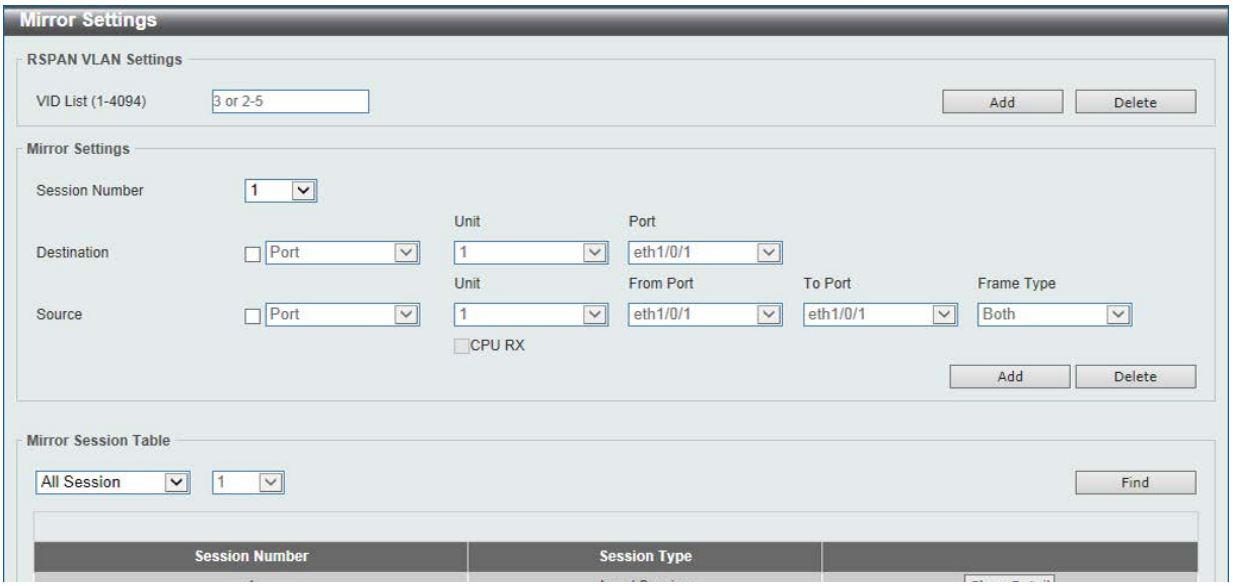


図 16-16　Mirror Settings 画面

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	該当エントリのセッション番号を指定します。1 から 4 までで指定可能です。
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について設定します。 宛先タイプオプションとして「Port」「Remote VLAN」「Replace」を選択します。 • 「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。 • 「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）も指定します。 • 「Replace」を選択した後に、ACL 名と、「VID」（2-4094）も指定します。

項目	説明
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について設定します。 送信元タイプオプションとして「Port」「ACL」「VLAN」「Remote VLAN」から選択します。「Port」を選択した後に、「From Port」と「To Port」の番号を指定します。最後に「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。「TX Forwarding」はポートが「STG Forwarding」状態の場合、送信トラフィックのみミラーされます。「ACL」オプションを選択した場合は ACL プロファイル名を表示される項目欄に入力します。 • 「VLAN」を選択した後に、「VID List」を指定し、Frame Type を選択します。 • 「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。「All Session」「Session Number」「Remote Session」「Local Session」から選択します。 「Session Number」を選択すると表示されるドロップダウンメニューからセッション番号を選択します。1 から 4 の間で選択可能です。

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

注意 ミラー機能において、TX を設定している場合、Source Port が STP、ERPS などにより、Block の状態のために実際には送信していない場合でも、宛先ポートにモニタします。

注意 LACP/STP/ERPS/802.1X/MBA 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。

「Show Detail」リンクをクリックし、以下の画面を表示します。



図 16-17　Mirror Settings - Show Detail 画面

sFlow（sFlow 設定）

sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。sFlow モニタリングシステムのアーキテクチャとサンプル技術は、サイトレベル、または企業レベルでの高速スイッチ / ルータネットワークにおける継続的なトラフィックモニタリングを提供します。

注意 sFlow の機能において、「Agent Address」は「Vlan 1」に設定された IP アドレスを使用し、これを変更する事はできません。「Vlan 1」の IP アドレスが設定されていない場合、または「Interface vlan 1」が存在しない場合は「Agent Address」は「0.0.0.0」となります。

sFlow Agent Information（sFlow エージェント情報）

sFlow エージェント情報を表示します。

Monitoring > sFlow > sFlow 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。

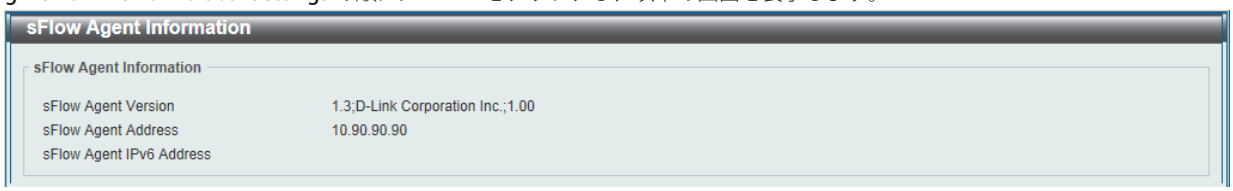


図 16-18　sFlow Agent Information 画面

以下の項目が表示されます。

項目	説明
sFlow Agent Version	現在の 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 アドレスを表示します。
sFlow Agent IPv6 Address	sFlow エージェント IPv6 アドレスを表示します。

「Apply」ボタンをクリックして、設定を有効にします。

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。

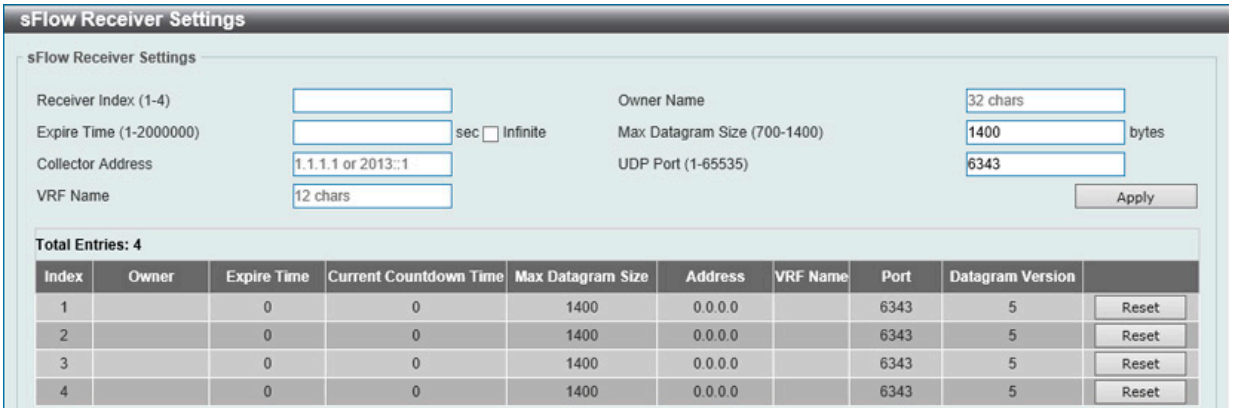


図 16-19　sFlow Receiver Settings 画面

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（1-4）を指定します。最大 4 個のエントリを追加できます。
Owner Name	sFlow レシーバオーナ名を指定します 32 文字まで指定できます。
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はリセットされます。1-2000000（秒）の範囲から指定します。 「Infinite」を設定するとサーバはタイムアウトしません。
Max Datagram Size (700-1400)	1 つの sFlow データにパッケージ化する最大データバイト数を指定します。 700 から 1400 で設定でき、初期値は 1400（バイト）です。
Collector Address	リモート sFlow コレクタの IP（v4/v6）アドレスを指定します。
UDP Port (1-65535)	リモート sFlow コレクタの UDP ポートを指定します。初期値は 6343 です。
VRF Name	VRF インスタンス名を 12 字以内で入力します。

「Apply」ボタンをクリックして、設定を有効にします。「Reset」ボタンをクリックして、指定エントリの設定を初期値に戻します。

sFlow Sampler Settings（sFlow サンプラ設定）

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。

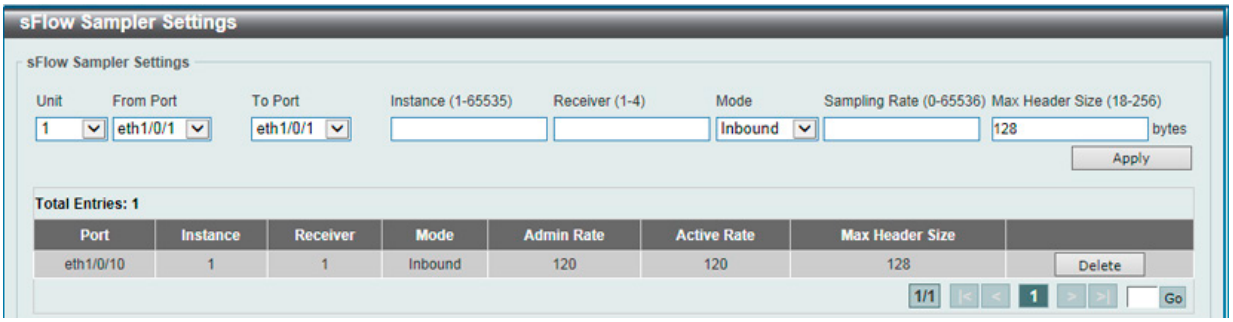


図 16-20　sFlow Sampler Settings 画面

以下の項目が表示されます。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	パケットサンプリングの設定を行うポートおよびポート範囲を指定します。
Instance	複数のサンプラを一つのインスタンスで使用する場合、インスタンスの識別番号を指定します。
Receiver (1-4)	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。1 から 4 までの間で指定可能です。

項目	説明
Mode	モードを指定します。「Inbound」または「Outbound」から指定します。「Inbound」を選択するとサンプルのイングレスパケットを指定します（初期値）。「Outbound」を選択すると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。0-65536 の値を指定します。エントリ「0」は、パケットのサンプリングを無効にします。0 が初期値であるため、指定しないと本機能は動作しません。
MAX Header Size (18-256)	本項目はサンプリングされるパケットヘッダのバイト数を設定します。このサンプルサンプリングされるヘッダは、アナライザサーバに送信されるデータと共にカプセル化されます。18-256 バイトの値を設定します。初期値は 128 バイトです。

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

sFlow Poller Settings（sFlow ポーラ設定）

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 16-21　sFlow Poller Settings 画面

以下の項目が表示されます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポーリングの設定を行うポートおよびポート範囲を指定します。
Instance	複数のサンプラを一つのインスタンスで使用する場合、インスタンスの識別番号を指定します。
Receiver (1-4)	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。1 から 4 までの間で指定可能です。
Interval (0-120)	ポーリングサンプリングの間隔を設定します。0 から 120（秒）で指定可能です。「0」を入力すると機能は無効になります。初期値は「0」です。

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

Device Environment（機器環境確認）

本画面ではスイッチの内部温度状態を表示します。

Monitoring > Device Environment をクリックして次の画面を表示します。

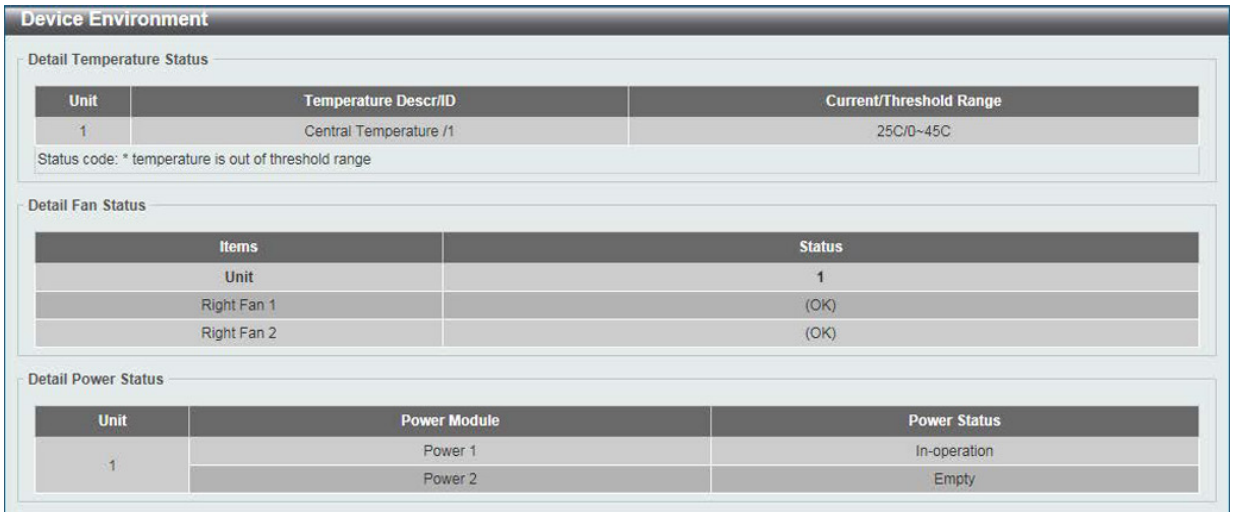


図 16-22　Device Environment 画面

External Alarm Settings（外部アラーム設定）

外部アラーム設定はアラームが起動した時のアラームメッセージについて設定します。
Monitoring > **External 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。

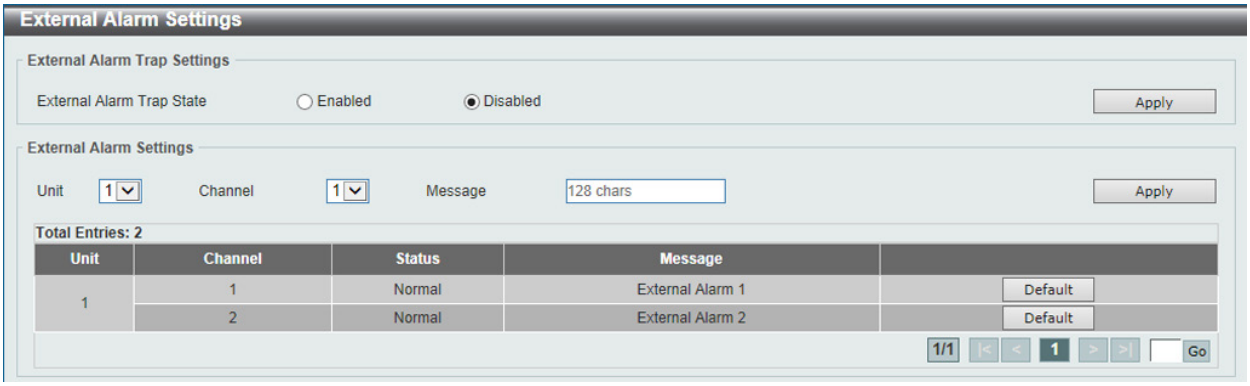


図 16-23　External Alarm Settings 画面

以下の項目が表示されます。

項目	説明
External Alarm Trap Settings	
External Alarm Trap State	外部アラームトラップを有効 / 無効に指定します。
External Alarm Settings	
Unit	設定を行うユニットを指定します。
Channel	設定するチャネル（1-2）を指定します。
Message	チャネルに紐づくアラームメッセージ（128 字以内）を指定します。

「Apply」ボタンをクリックして、設定を有効にします。
「Default」ボタンをクリックして、初期値に戻ります。
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。

第 17 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

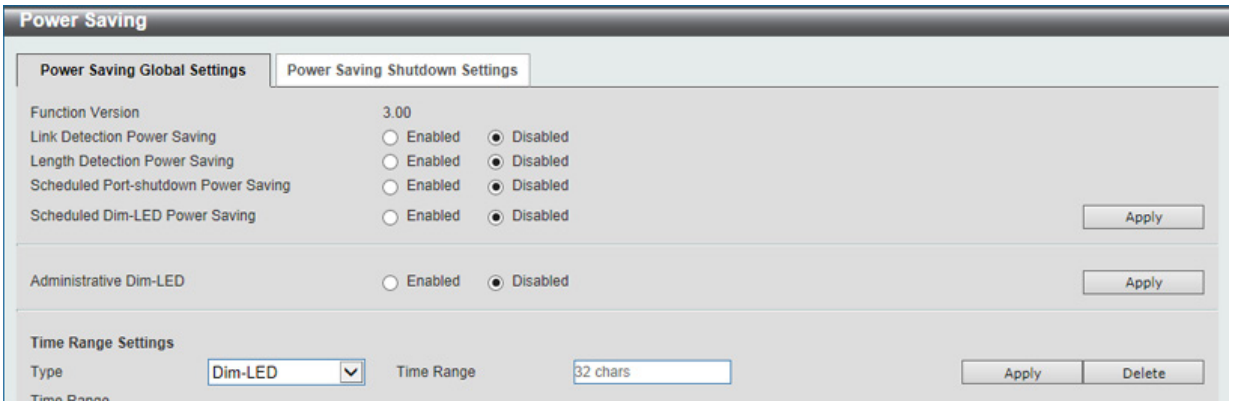


図 17-1　Power Saving - Power Saving Global Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Global Settings タブ	
Link Detection Power Saving	「リンク検出」を有効 / 無効に指定します。有効にするとリンクダウンしているポートへの電力供給は止められ、スイッチの消費電力を抑えます。これによりリンクアップしているポートへの影響はありません。
Length Detection Power Saving	「ケーブル長検出」を有効 / 無効に指定します。有効にするとケーブルの長さに応じて必要な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。「Dim-LED」「Hibernation」から指定できます。
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。画面は自動的に更新されます。
「Delete」ボタンをクリックし指定のエントリを削除します。

注意　「Hibernation」（休止）機能を有効にする場合、物理スタック機能は無効である必要があります。

Power Saving Shutdown Settings タブ

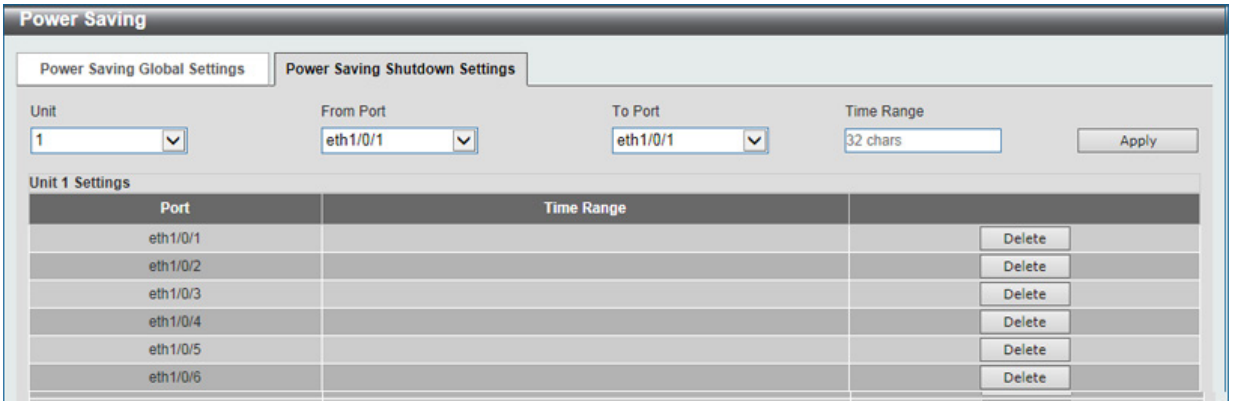


図 17-2　Power Saving - Power Saving Shutdown Settings タブ画面

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	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Time Range	ポートに対応するスケジュール名を指定します。

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

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

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

Green > EEE メニューをクリックし、以下の画面を表示します。

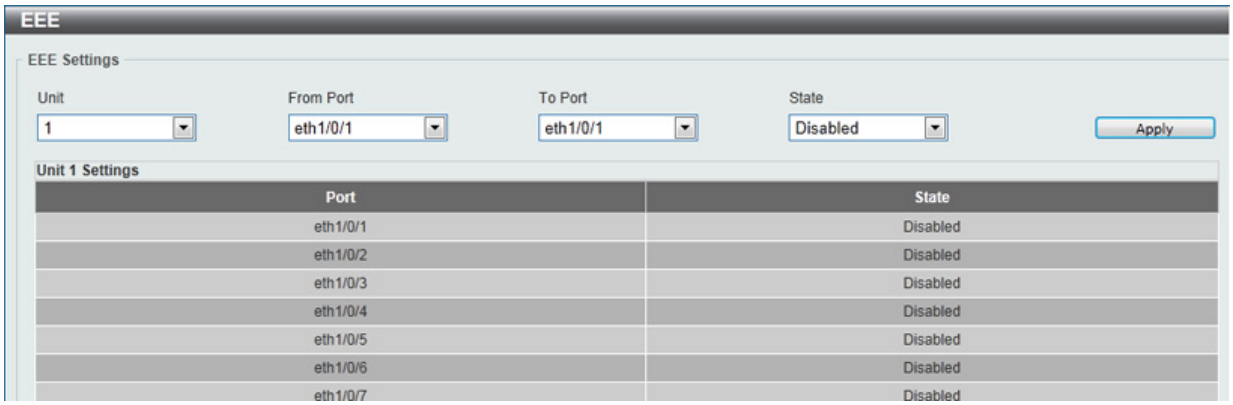


図 17-3　EEE 画面

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	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
State	本機能を有効 / 無効に指定します。

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

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 18 章　OpenFlow

以下は Openflow 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
Openflow Settings（OpenFlow 設定）	OpenFlow の設定を行います。

注意　OpenFlow V1.3 のみサポートされています。OpenFlow コントローラ側のプロトコルバージョンが同じであることをご確認下さい。

OpenFlow Settings（OpenFlow 設定）

OpenFlow の設定を行います。

注意 現在のバージョンでは WebUI による OpenFlow の設定はサポートされていません。CLI をご利用ください。

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

OpenFlow Global Settings タブ

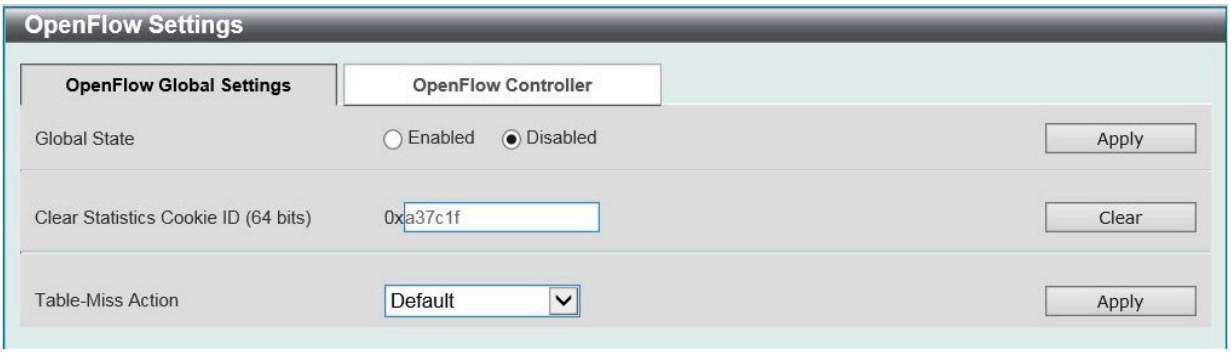


図 18-1　OpenFlow Settings - OpenFlow Global Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
OpenFlow Global Settings タブ	
Global State	OpenFlow をグローバルで有効 / 無効に設定します。
Clear Statistics Cookie ID (64 bits)	クッキー ID を指定して「Clear」ボタンをクリックすると、Flow テーブル内の指定したエントリの統計情報が削除されます。
Table-Miss Action	Table-miss フローエントリに対するアクションを指定します。 • 「Default」- Table-miss エントリが設定されていません。 • 「Drop」- Clear-Actions インストラクションを実行します。不明なパケットは破棄されます。 • 「Controller」Apply-Actions インストラクションを実行します。不明なパケットはコントローラに送信されます。

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

OpenFlow Controller タブ

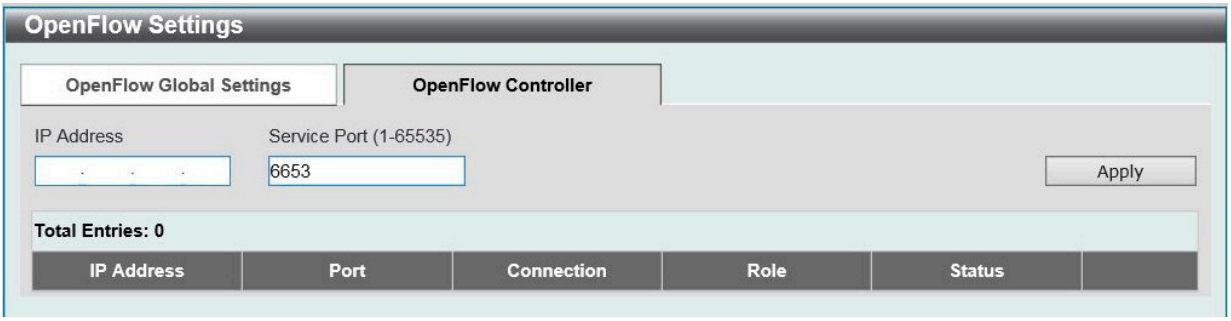


図 18-2　OpenFlow Settings - OpenFlow Controller タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
OpenFlow Controller タブ	
IP Address	OpenFlow コントローラの IP アドレスを入力します。
Service Port (1-65535)	OpenFlow コントローラのポート番号を入力します。

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

第 19 章　Save and Tools（Save メニュー /Tools メニュー）

メンテナンス用のメニューを使用し、本スイッチのリセットおよび再起動等を行うことができます。

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

サブメニュー	説明
Save メニュー	
Save Configuration（コンフィグレーションの保存）	コンフィグレーションをスイッチに保存します。
Tools メニュー	
Firmware Upgrade & Backup（ファームウェアアップグレード&バックアップ）	様々なプロトコルを使用してファームウェアアップグレード / バックアップを実行します。
Configuration Restore & Backup（コンフィグレーションリストア&バックアップ）	様々なプロトコルを使用してコンフィグレーションリストア / バックアップを実行します。
Certificate & Key Restore & Backup（証明書 / 鍵リストア&バックアップ）	様々なプロトコルを使用して証明書と鍵のリストア / バックアップを実行します。
Log Backup（ログファイルのバックアップ）	様々なプロトコルを使用してログファイルのバックアップを実行します。
Ping	「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。
Trace Route（トレースルート）	パケットの経路をスイッチに到着する前に遡ってトレースすることができます。
Reset（リセット）	スイッチの設定内容を工場出荷時状態に戻します。
Reboot System（システム再起動）	スイッチの再起動を行います。
DLMS Settings（DLMS 設定）	「D-Link License Management System」(DLMS) の設定、表示を行います。

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

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Type」プルダウンメニューの「Configuration」を選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。

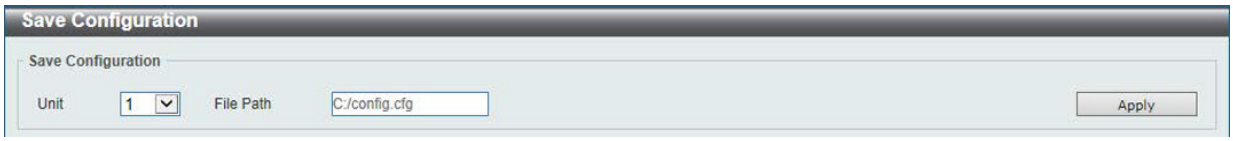


図 19-1　Save - Configuration 画面

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、DLMS 設定を行います。

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

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

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

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

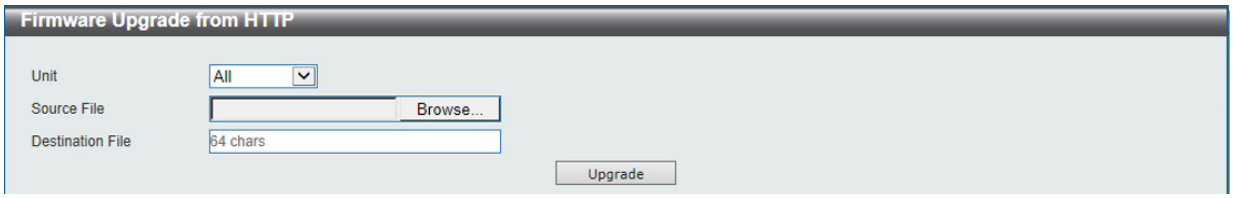


図 19-2　Firmware Upgrade from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定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 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

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

TFTP を使用してファームウェアアップグレードを実行します。

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

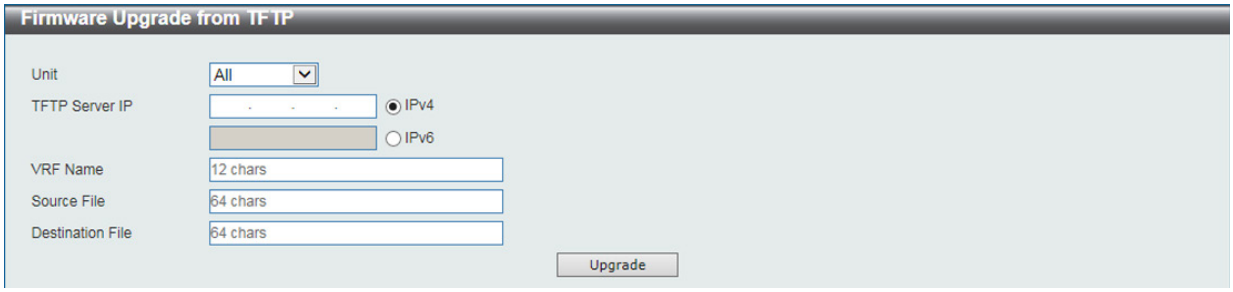


図 19-3　Firmware Upgrade from TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定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」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

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

FTP を使用してファームウェアアップグレードを実行します。

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

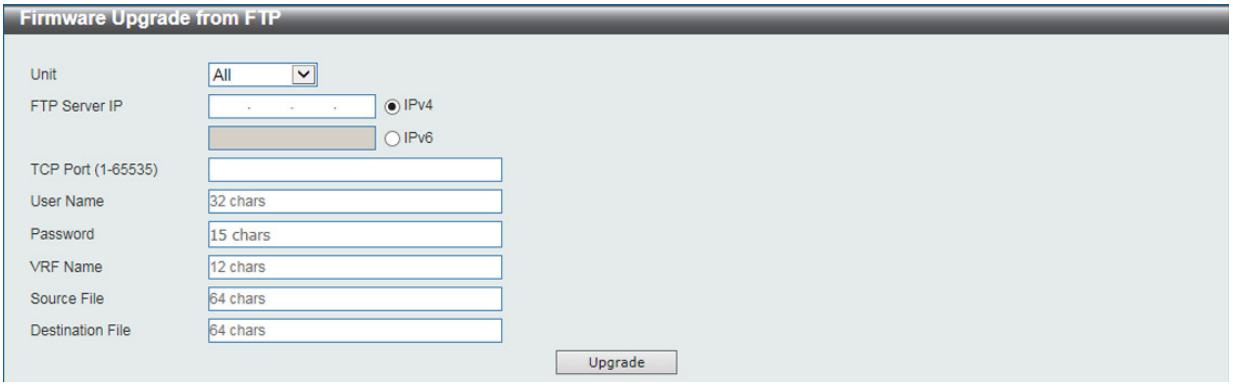


図 19-4　Firmware Upgrade from FTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号（1-65535）を指定します。
User Name	FTP 接続のユーザ名（32 字以内）を指定します。
Password	FTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

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

RCP を使用してファームウェアアップグレードを実行します。

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

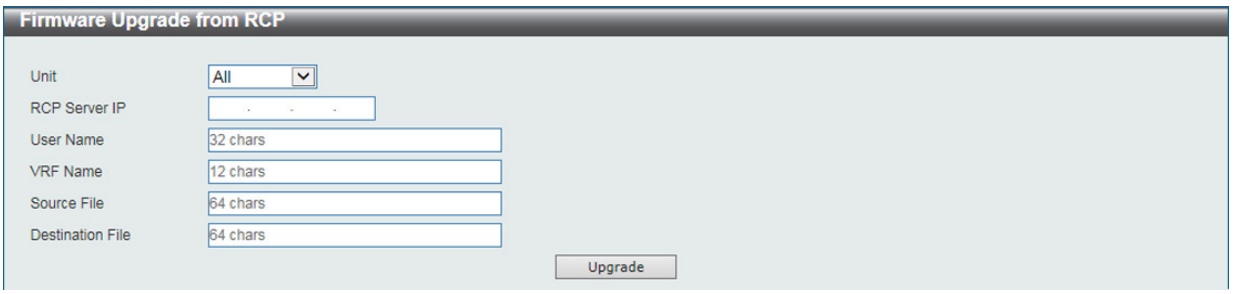


図 19-5　Firmware Upgrade from RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続のユーザ名（32 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

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

SFTP を使用してファームウェアアップグレードを実行します。

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

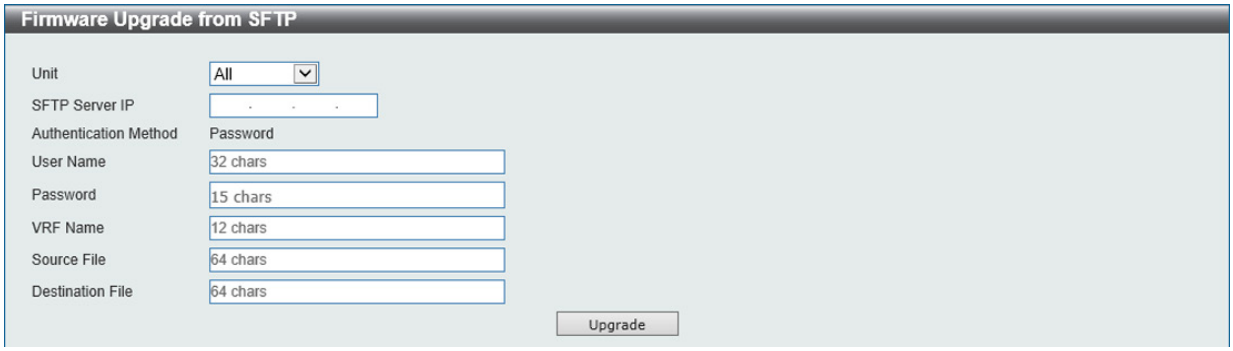


図 19-6　Firmware Upgrade from SFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。
Authentication Method	認証方法が表示されます。
User Name	SFTP 接続のユーザ名（32 字以内）を指定します。
Password	SFTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

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

HTTP 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。

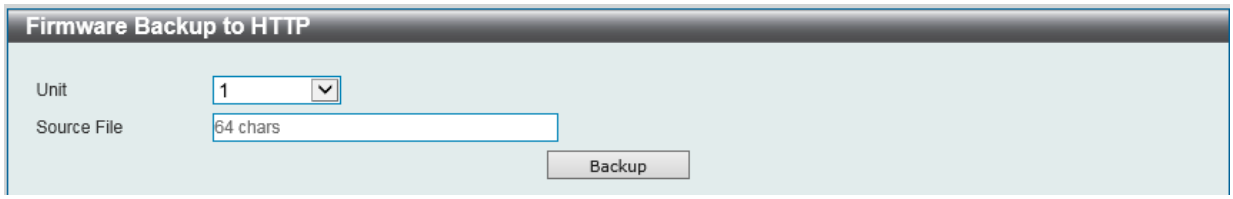


図 19-7　Firmware Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。

「Backup」ボタンをクリックしてバックアップを開始します。

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。

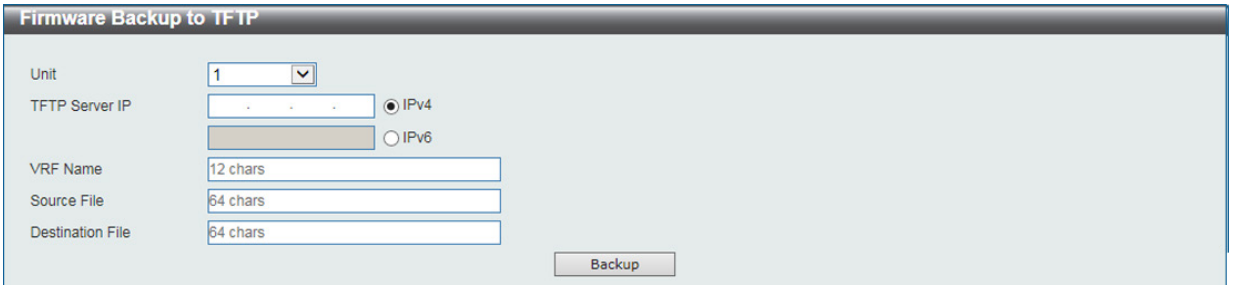


図 19-8　Firmware Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定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」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。
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 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

FTP を使用してファームウェアバックアップを実行します。

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

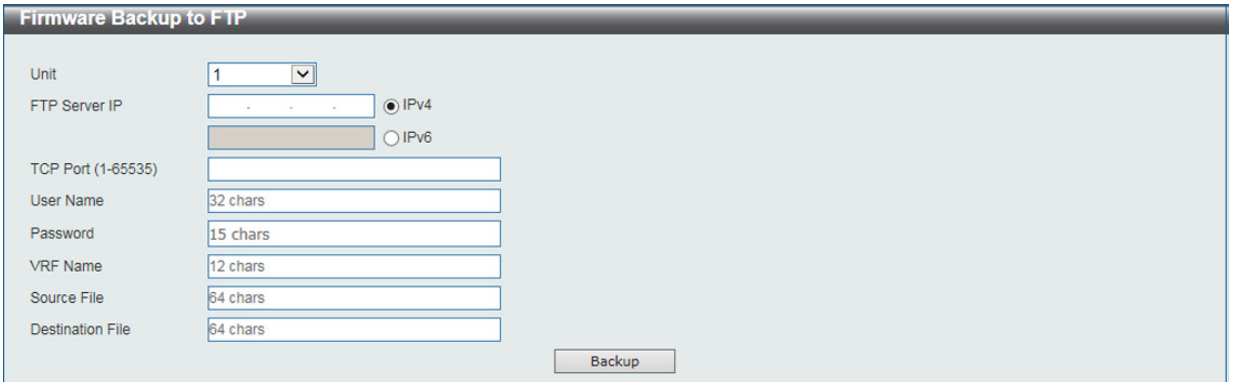


図 19-9　Firmware Backup to FTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号（1-65535）を指定します。
User Name	FTP 接続のユーザ名（32 字以内）を指定します。
Password	FTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチ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 文字まで指定します。
Destination File	ファームウェアがストアされる FTP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

RCP を使用してファームウェアバックアップを実行します。
Tools > Firmware Backup & Backup > firmware Backup to RCP をクリックし、設定画面を表示します。

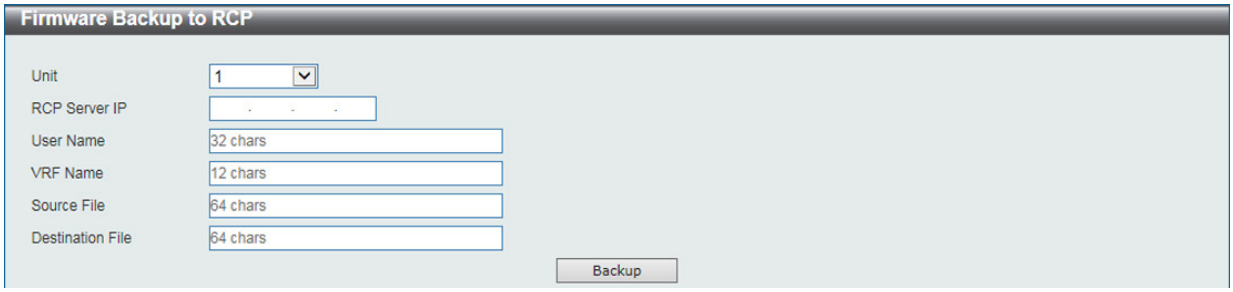


図 19-10 Firmware Backup to RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続のユーザ名（32 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチ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 文字まで指定します。
Destination File	ファームウェアがストアされる RCP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

SFTP を使用してファームウェアバックアップを実行します。
Tools > Firmware Backup & Backup > firmware Backup to SFTP をクリックし、設定画面を表示します。

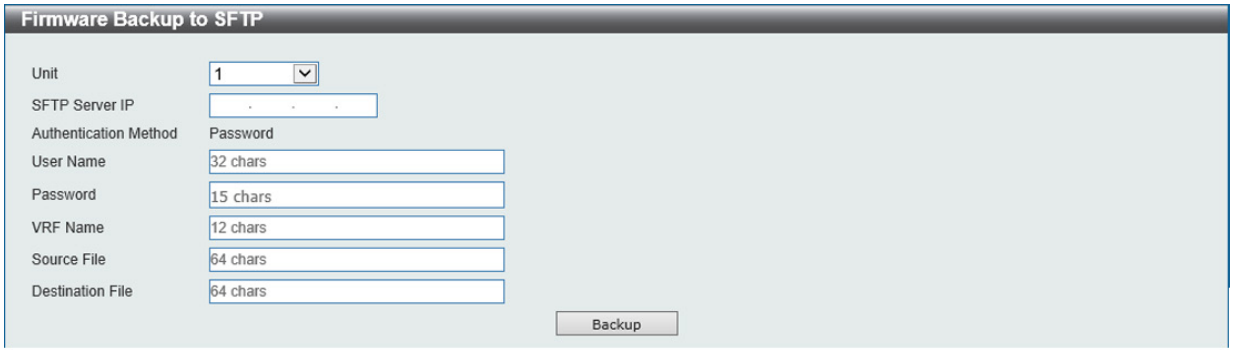


図 19-11 Firmware Backup to SFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。
Authentication Method	認証方法が表示されます。
User Name	SFTP 接続のユーザ名（32 字以内）を指定します。
Password	SFTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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 文字まで指定します。 「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

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

HTTP サーバを使用してローカル PC から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 19-12 Configuration Restore from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	ローカル PC にあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。 「Browse/ 参照」ボタンをクリックしてローカル PC 上の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ストアされるスイッチの場所を指定します。64 文字までで指定できます。 「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は上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
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。

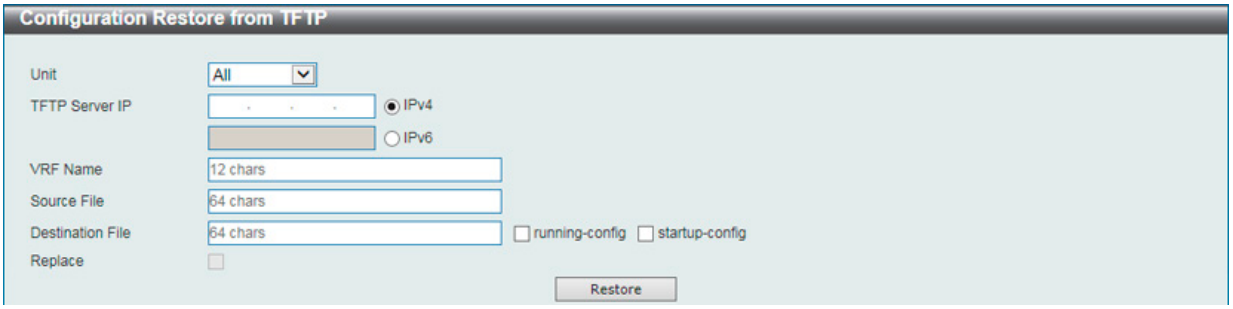


図 19-13 Configuration Restore from TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定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」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	TFTP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「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は上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
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 FTP（FTP サーバからコンフィグレーションのリストア）

FTP サーバ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 FTP をクリックし、設定画面を表示します。

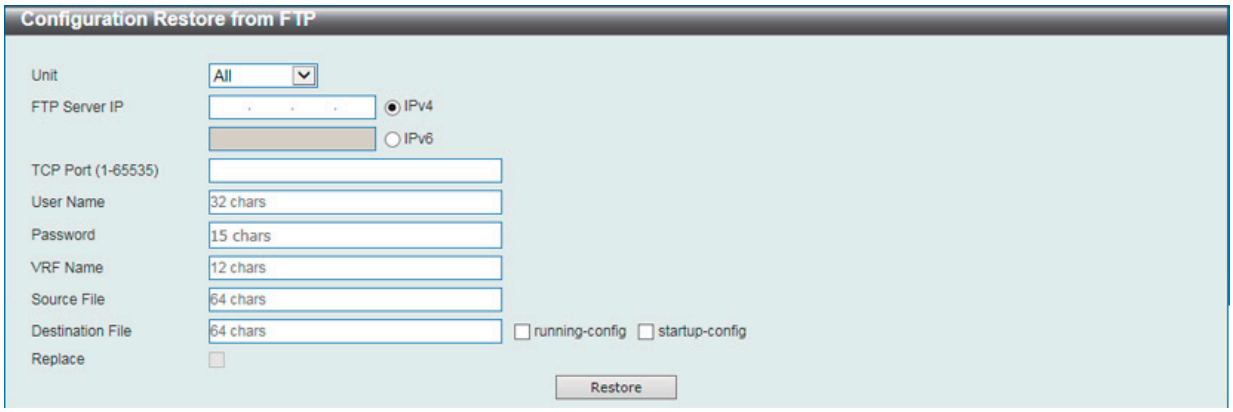


図 19-14 Configuration Restore from FTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号（1-65535）を指定します。
User Name	FTP 接続のユーザ名（32 字以内）を指定します。
Password	FTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	FTP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「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は上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
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 RCP（RCP サーバからコンフィグレーションのリストア）

RCP サーバ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 RCP をクリックし、設定画面を表示します。

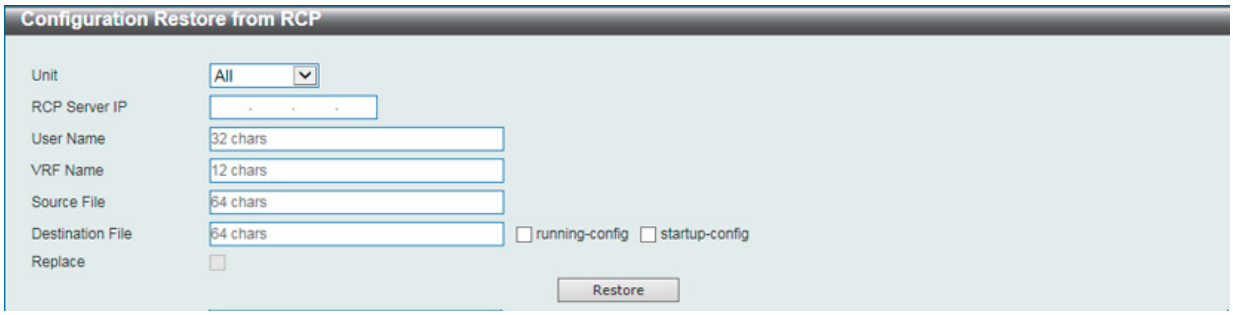


図 19-15 Configuration Restore from RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、RCP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、RCP サーバの IPv6 アドレスを入力します。
User Name	RCP 接続のユーザ名（32 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	RCP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。

項目	説明
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「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は上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
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 SFTP（SFTP サーバからコンフィグレーションのリストア）

SFTP サーバ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 SFTP をクリックし、設定画面を表示します。

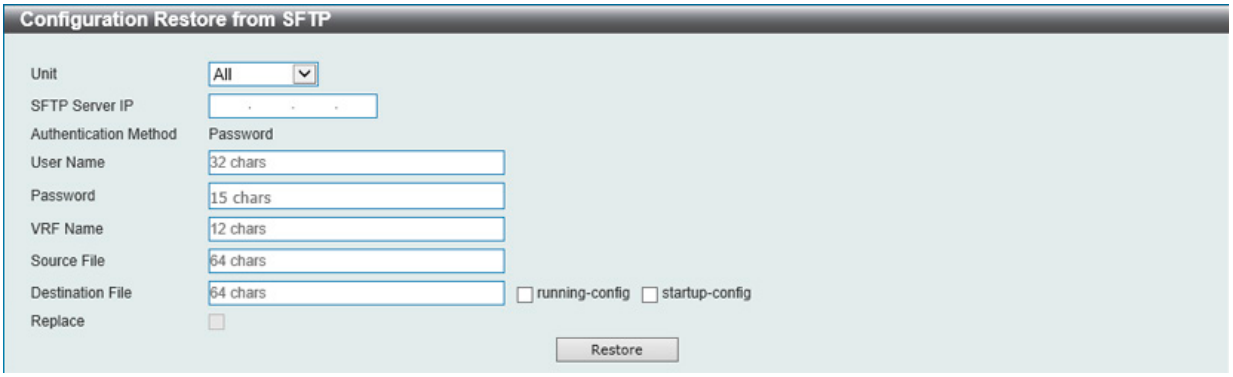


図 19-16 Configuration Restore from SFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、SFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続のユーザ名（32 字以内）を指定します。
Password	SFTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	SFTP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「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は上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
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 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。

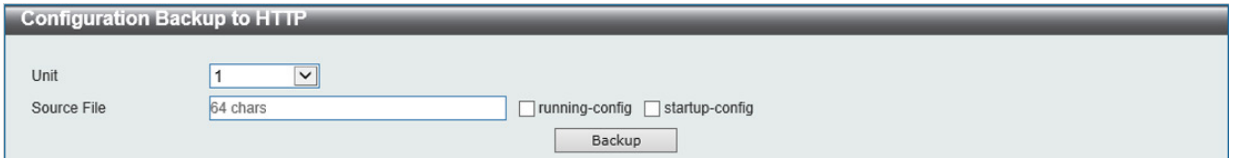


図 19-17 Configuration Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「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起動時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。

「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。

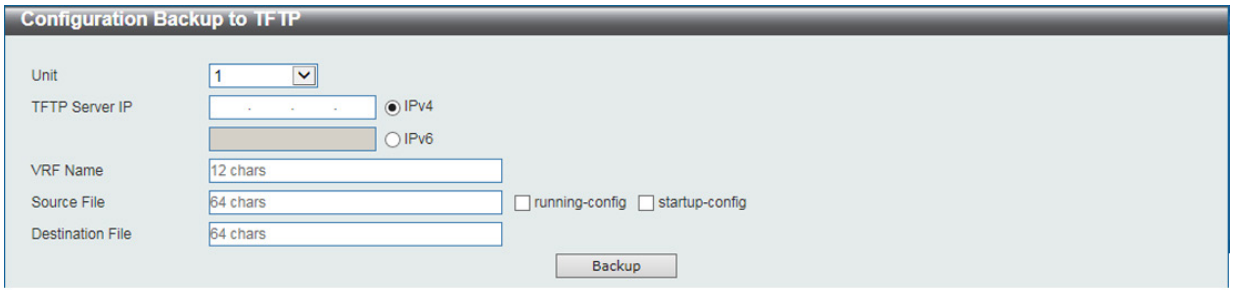


図 19-18 Configuration Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定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」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「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起動時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。
Destination File	コンフィグレーションファイルがストアされる TFTP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

FTP サーバにコンフィグレーションバックアップを行います。

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

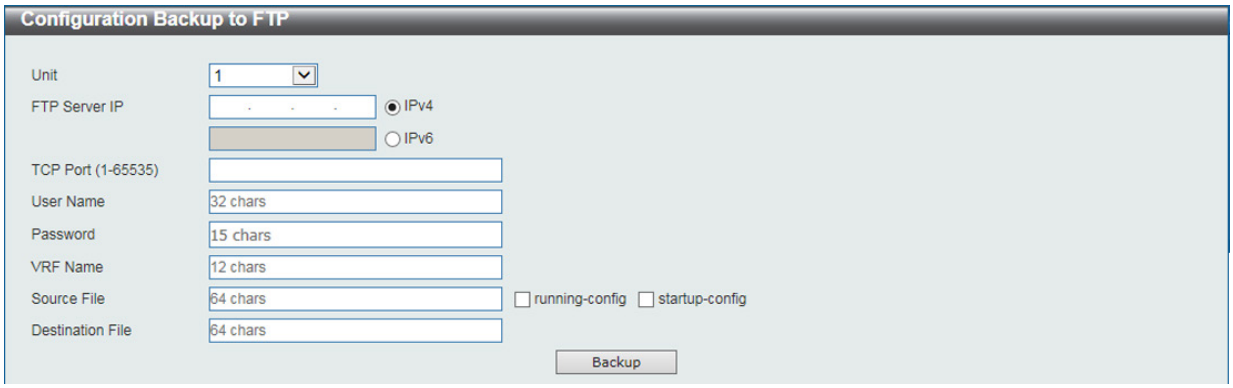


図 19-19 Configuration Backup to FTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号（1-65535）を指定します。
User Name	FTP 接続のユーザ名（32 字以内）を指定します。
Password	FTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「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起動時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。
Destination File	コンフィグレーションファイルがストアされる FTP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

RCP サーバにコンフィグレーションバックアップを行います。

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

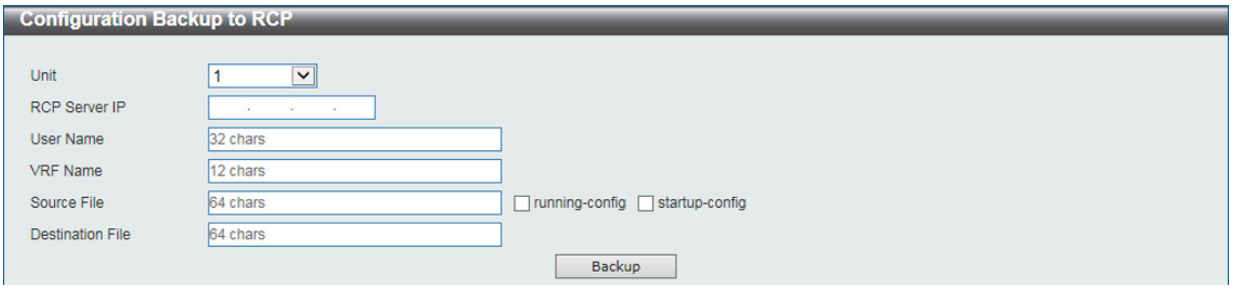


図 19-20 Configuration Backup to RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続のユーザ名（32 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「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起動時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。
Destination File	コンフィグレーションファイルがストアされる RCP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

SFTP サーバにコンフィグレーションバックアップを行います。

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

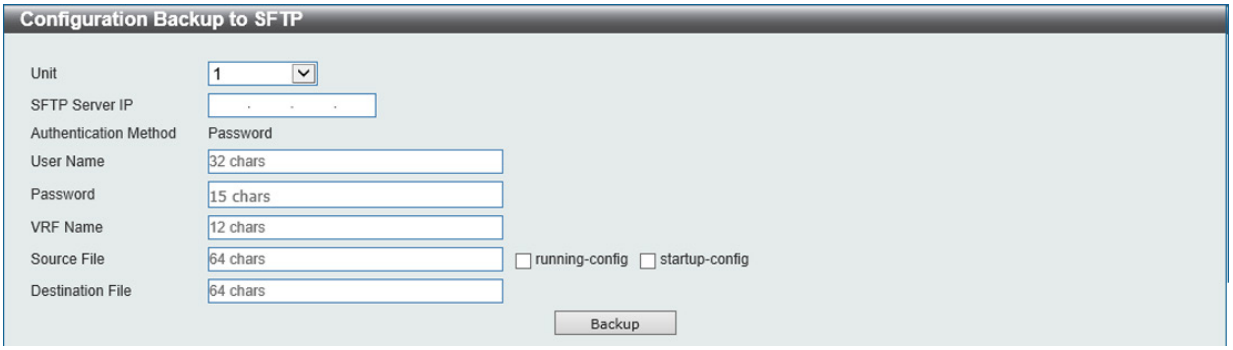


図 19-21 Configuration Backup to SFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。
User Name	SFTP 接続のユーザ名（32 字以内）を指定します。
Password	SFTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「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起動時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。
Destination File	コンフィグレーションファイルがストアされる SFTP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Certificate & Key Restore & Backup（証明書 / 鍵リストア＆バックアップ）

Certificate & Key Restore from HTTP（HTTP を使用した証明書 / 鍵リストア）

HTTP を使用してローカル PC から証明書 / 鍵リストアを実行します。

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



図 19-22 Certificate & Key Restore from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Restore」ボタンをクリックしてリストアを開始します。

Certificate & Key Restore from TFTP（TFTP を使用した証明書 / 鍵リストア）

TFTP を使用して証明書 / 鍵リストアを実行します。

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

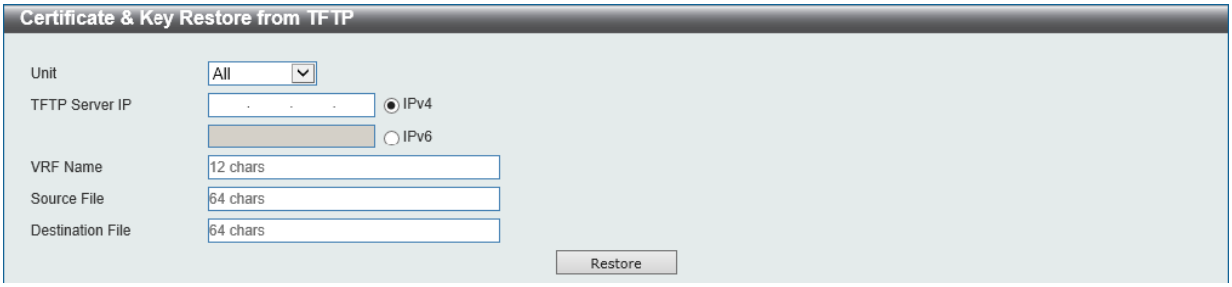


図 19-23 Certificate & Key Restore from TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定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」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Restore」ボタンをクリックしてリストアを開始します。

Certificate & Key Restore from FTP（FTP を使用した証明書 / 鍵リストア）

FTP を使用して証明書 / 鍵リストアを実行します。

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

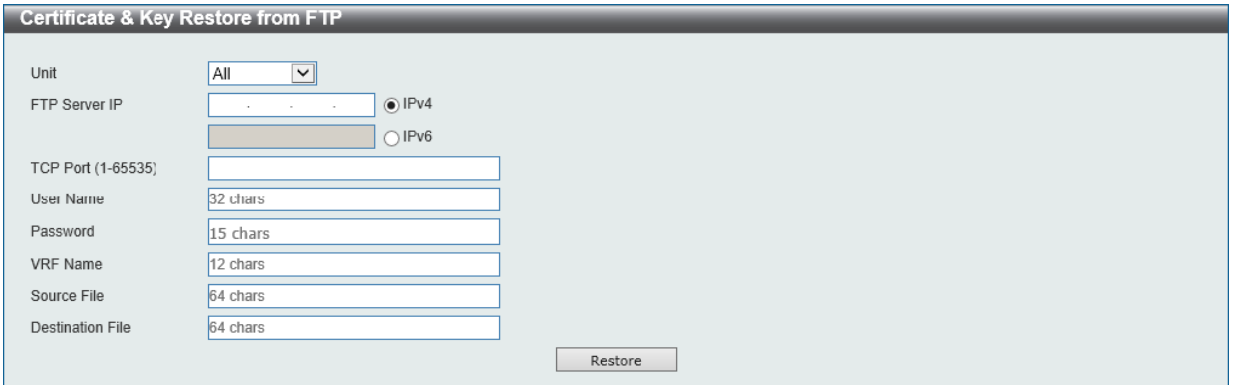


図 19-24 Certificate & Key Restore from FTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号（1-65535）を指定します。
User Name	FTP 接続のユーザ名（32 字以内）を指定します。
Password	FTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Restore」ボタンをクリックしてリストアを開始します。

Certificate & Key Restore from RCP（RCP を使用した証明書 / 鍵リストア）

RCP を使用して証明書 / 鍵リストアを実行します。

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

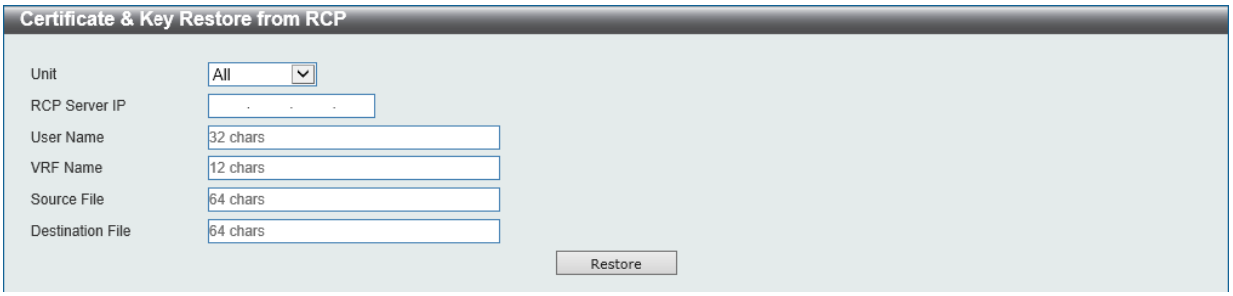


図 19-25 Certificate & Key Restore from RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続のユーザ名（32 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Restore」ボタンをクリックしてリストアを開始します。

Certificate & Key Restore from SFTP（SFTP を使用した証明書 / 鍵リストア）

SFTP を使用して証明書 / 鍵リストアを実行します。

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

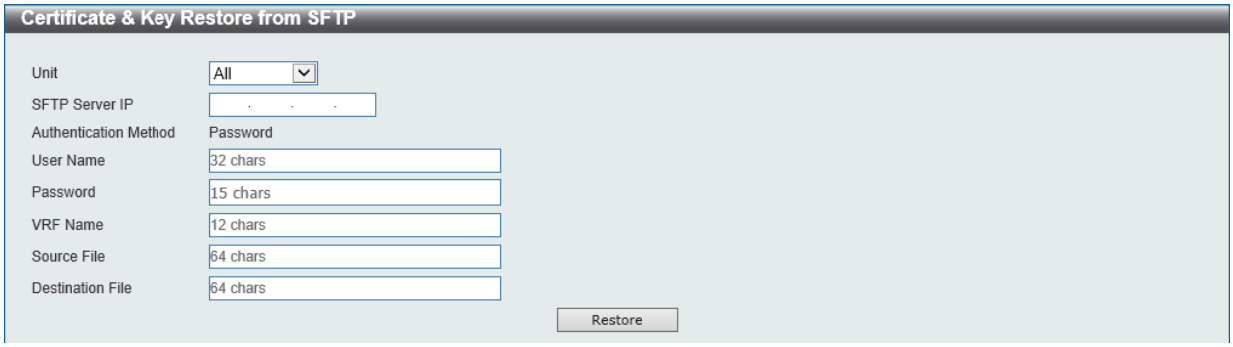


図 19-26 Certificate & Key Restore from SFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。
User Name	SFTP 接続のユーザ名（32 字以内）を指定します。
Password	SFTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Restore」ボタンをクリックしてリストアを開始します。

Certificate & Key Backup to HTTP（HTTP を使用した証明書 / 鍵バックアップ）

HTTP サーバに証明書 / 鍵バックアップを行います。

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

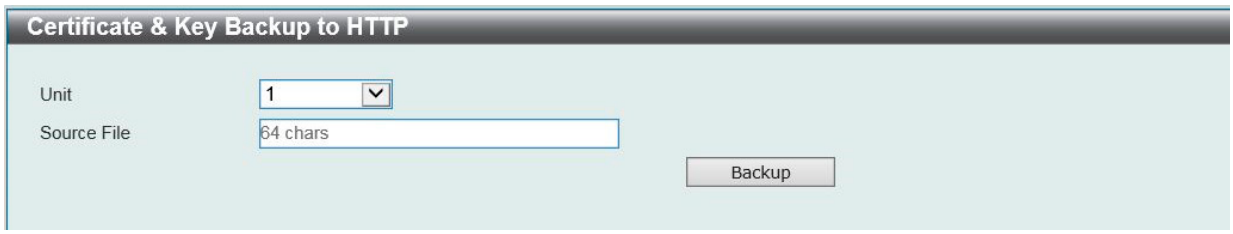


図 19-27 Certificate & Key Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。

「Backup」ボタンをクリックしてバックアップを開始します。

Certificate & Key Backup to TFTP（TFTP を使用した証明書 / 鍵バックアップ）

TFTP サーバに証明書 / 鍵バックアップを行います。

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

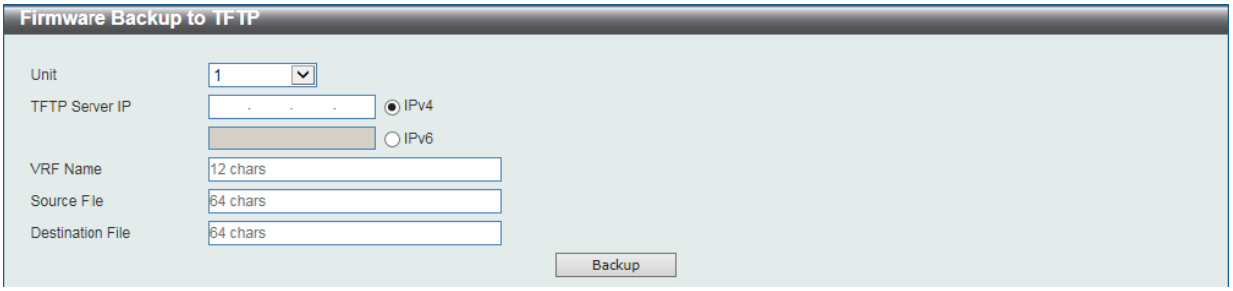


図 19-28 Certificate & Key Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定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」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。
Destination File	証明書 / 鍵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 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Certificate & Key Backup to FTP（FTP を使用した証明書 / 鍵バックアップ）

FTP を使用して証明書 / 鍵バックアップを実行します。

Tools > Certificate & Key Backup & Backup > Certificate & Key Backup to FTP をクリックし、設定画面を表示します。

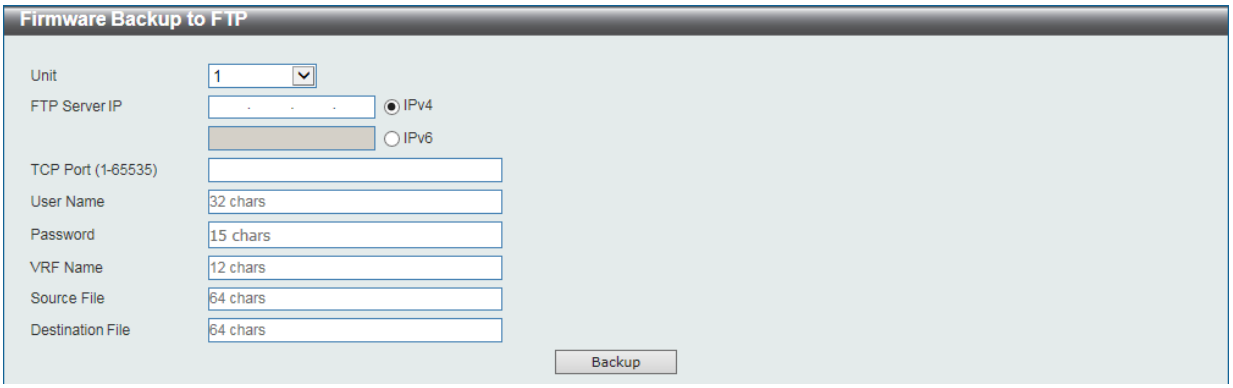


図 19-29 Certificate & Key Backup to FTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、FTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号（1-65535）を指定します。
User Name	FTP 接続のユーザ名（32 字以内）を指定します。
Password	FTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。
Destination File	証明書 / 鍵がストアされる FTP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Certificate & Key Backup to RCP（RCP を使用した証明書 / 鍵バックアップ）

RCP を使用して証明書 / 鍵バックアップを実行します。

Tools > Certificate & Key Backup & Backup > Certificate & Key Backup to RCP をクリックし、設定画面を表示します。

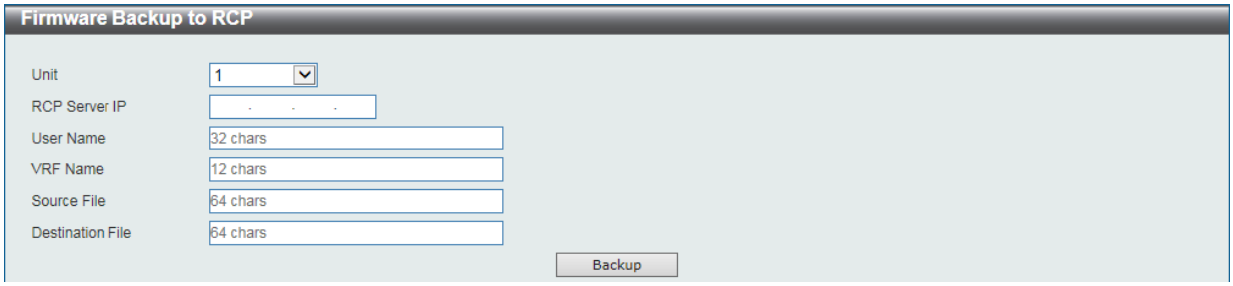


図 19-30 Certificate & Key Backup to RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続のユーザ名（32 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	スイッチにある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。
Destination File	証明書 / 鍵がストアされる RCP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Certificate & Key Backup to SFTP（SFTP を使用した証明書 / 鍵バックアップ）

SFTP を使用して証明書 / 鍵バックアップを実行します。

Tools > Certificate & Key Backup & Backup > Certificate & Key Backup to SFTP をクリックし、設定画面を表示します。

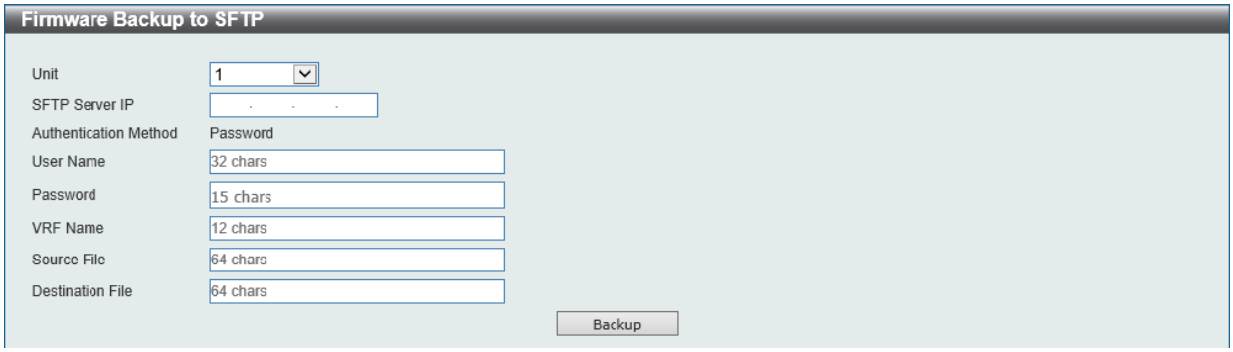


図 19-31 Certificate & Key Backup to SFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
SFTP Server IP	SFTP サーバの IP アドレスを入力します。
Authentication Method	認証方法が表示されます。
User Name	SFTP 接続のユーザ名（32 字以内）を指定します。
Password	SFTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Source File	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。
Destination File	証明書 / 鍵がストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Log Backup（ログファイルのバックアップ）

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

HTTP サーバを使用してローカル PC へのシステムログのバックアップを行います。

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

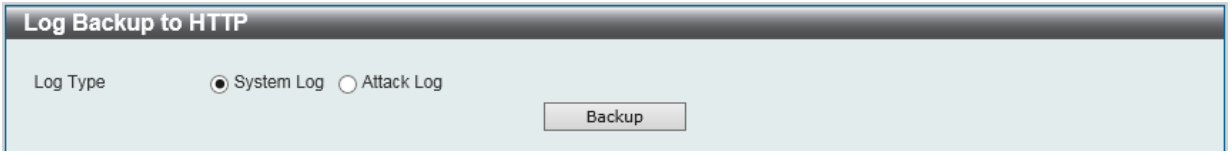


図 19-32 Log Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
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」オプションを選択するとシステムログエントリをバックアップします。「Attack Log」オプションを選択すると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。

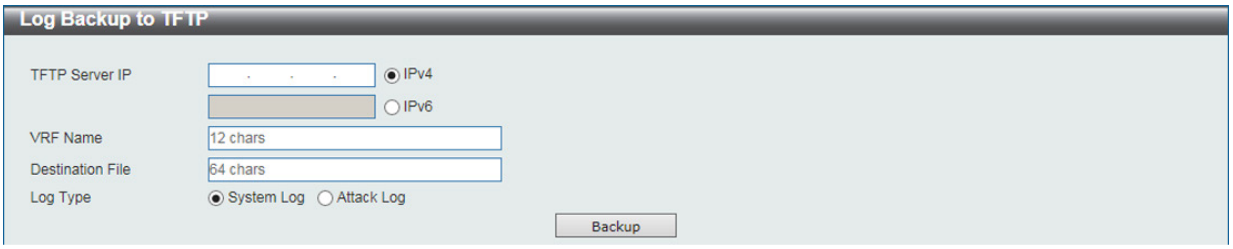


図 19-33 Log Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Destination File	ログファイルがストアされる TFTP サーバの場所を指定します。64 文字までで指定できます。
Log Type	バックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップします。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。

「Backup」ボタンをクリックしてバックアップを開始します。

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

RCP サーバへのシステムログのバックアップを行います。

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

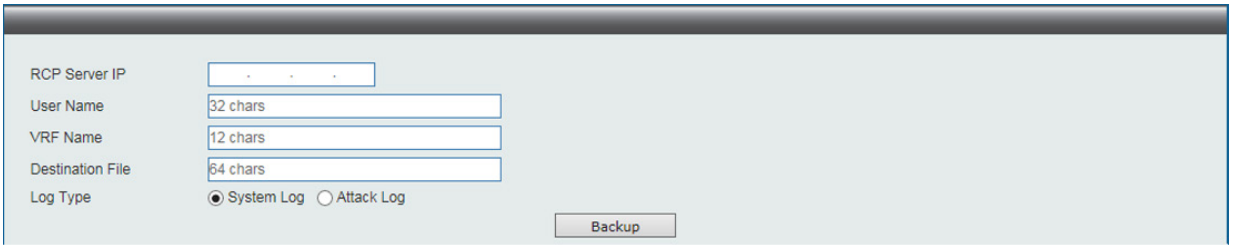


図 19-34 Log Backup to RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
RCP Server IP	RCP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、RCP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、RCP サーバの IPv6 アドレスを入力します。
User Name	RCP 接続のユーザ名（32 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Destination File	ログファイルがストアされる RCP サーバの場所を指定します。64 文字までで指定できます。
Log Type	バックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップします。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。

「Backup」ボタンをクリックしてバックアップを開始します。

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

SFTP サーバへのシステムログのバックアップを行います。

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

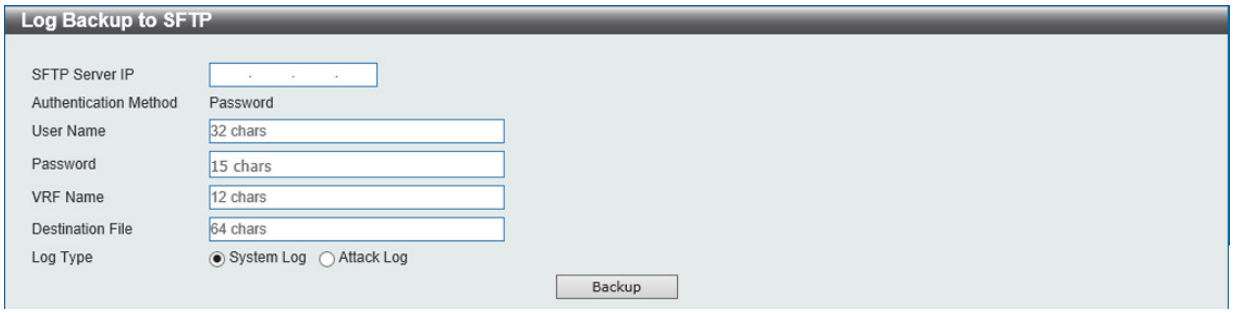


図 19-35 Log Backup to SFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
SFTP Server IP	SFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、SFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、SFTP サーバの IPv6 アドレスを入力します。
User Name	SFTP 接続のユーザ名（32 字以内）を指定します。
Password	SFTP 接続のパスワード（15 字以内）を指定します。
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Destination File	ログファイルがストアされる SFTP サーバの場所を指定します。64 文字までで指定できます。
Log Type	バックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップします。「Attack Log」オプションを選択すると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。これはネットワーク上のスイッチと機器の接続状況を確認するうえで非常に有効です。

Tools > Ping をクリックし、設定画面を表示します。

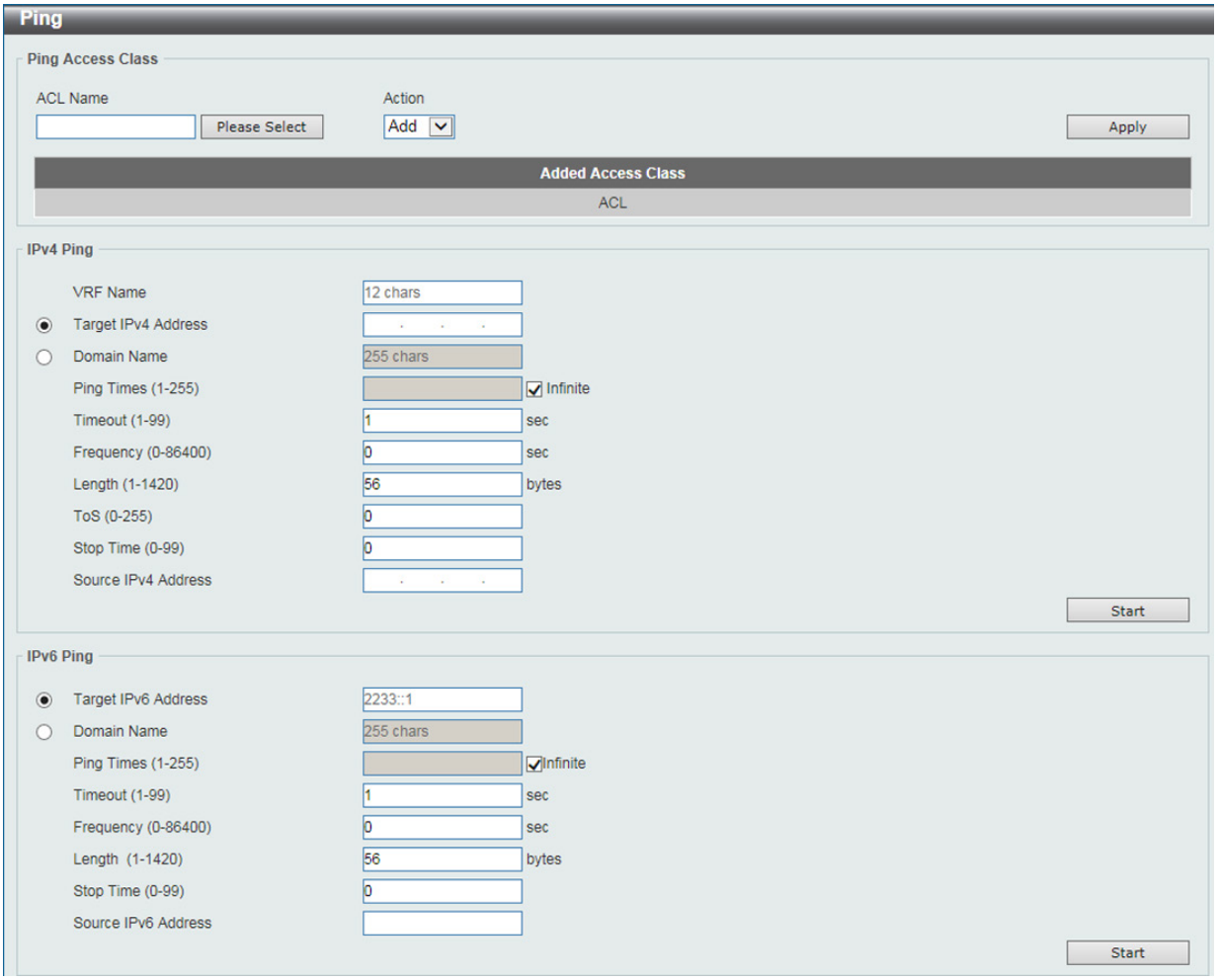


図 19-36 Ping 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Ping Access Class	
ACL Name	ACL 名（32 字以内）を指定します。「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	
VRF Name	VRF インスタンス名を 12 字以内で入力します。
Target IPv4 Address	Ping する 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	繰り返し行う Ping の回数を入力します。1 から 255 の間で指定できます。「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99（秒）までの間で指定できます。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。
Frequency	Ping 頻度（0-86400）を指定します。
Length	Ping 長（1-1420/ バイト）を指定します。送信データバイトの数になります。初期値は 56 で、ICMP ヘッダデータの 8 バイトと結合した時に、64 の ICMP データバイトになります。あらゆる「VLAN」「IEEE 802.1Q タグ長」は含まれません。
ToS	ToS 値（0-255）を指定します。ICMP データグラムの QoS を指定します。
Stop Time	停止時間（0-99）を指定します。本項目で指定の回数を過ぎると Ping を停止します。「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。
Source IPv4 Address	送信元 IPv4 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちのど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 アドレスやプライマリ IP アドレスになります。

項目	説明
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	繰り返し行う Ping の回数を入力します。1 から 255 の間で指定できます。 「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99（秒）までの間で指定できます。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。
Frequency	Ping 頻度（0-86400）を指定します。
Length	Ping 長（1-1420/ バイト）を指定します。送信データバイトの数になります。初期値は 56 で、ICMP ヘッダデータの 8 バイトと結合した時に、64 の ICMP データバイトになります。あらゆる「VLAN」「IEEE 802.1Q タグ長」は含まれません。
Stop Time	停止時間（0-99）を指定します。本項目で指定の回数を過ぎると Ping を停止します。「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。
Source IPv6 Address	送信元 IPv6 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちのど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 アドレスやプライマリ IP アドレスになります。

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

「Please Select」をクリックすると、以下の画面が表示されます。

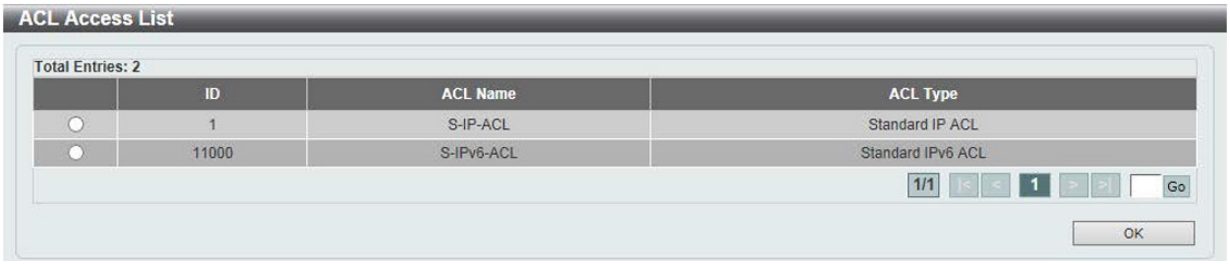


図 19-37 Ping (Please Select) 画面

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。

「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 19-38 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。

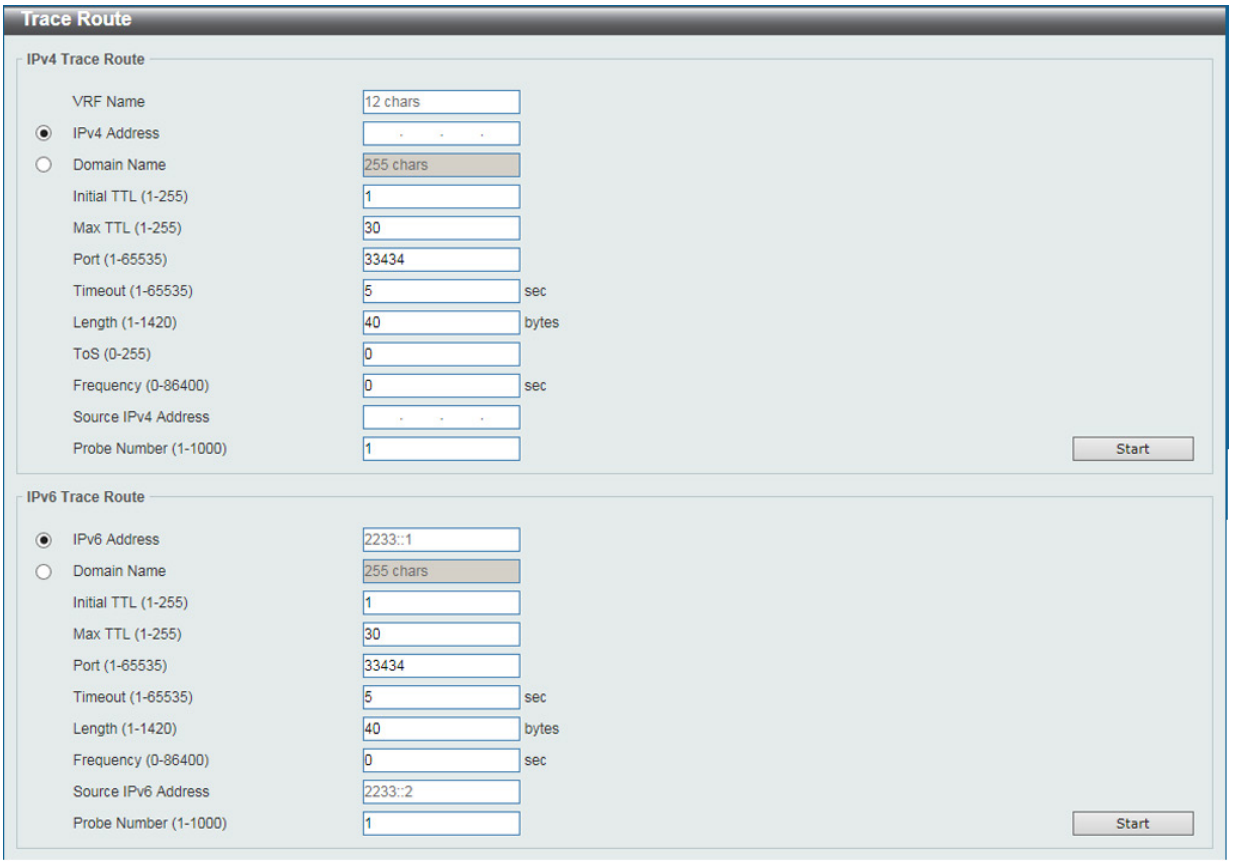


図 19-39 Trace Route 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IPv4 Trace Route	
VRF Name	VRF インスタンス名を 12 字以内で入力します。
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(1-255)	初期トレースルートリクエストの有効期間です。
Max TTL(1-255)	トレースルートリクエストの有効期間。２つのデバイス間のネットワークパスを検索する場合に traceroute コマンドが通過するルータの最大数です。
Port (1-65535)	ポート数。ポート番号 1-65535 で指定します。
Timeout (1-65535)	リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。1-65535（秒）で指定します。
Length	Ping 長（1-1420/ バイト）を指定します。送信データバイトの数になります。
ToS	ToS 値（0-255）を指定します。外部データグラムの IP ヘッダを指定します。
Frequency	Ping 頻度（0-86400）を指定します。
Source IPv4 Address	送信元 IPv4 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちのどれかを入力することが可能です。
Probe Number(1-1000)	予定された traceroute パス上の次のホップに probe パケットをスイッチが送信する回数を指定します。初期値は 1 です。

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

項目	説明
IPv6 Trace Route	
IPv6 Address	宛先ステーションの IPv6 アドレス
Domain Name	宛先のドメイン名を入力します。
Initial TTL(1-255)	初期トレースルートリクエストの有効期間です。
Max TTL(1-255)	トレースルートリクエストの有効期間。２つのデバイス間のネットワークパスを検索する場合に traceroute コマンドが通過するルータの最大数です。
Port (1-65535)	ポート数。ポート番号 1-65535 で指定します。

項目	説明
Timeout (1-65535)	リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。1-65535（秒）で指定します。
Length	Ping 長（1-1420/ バイト）を指定します。送信データバイトの数になります。
Frequency	Ping 頻度（0-86400）を指定します。
Source IPv6 Address	送信元 IPv6 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちのどれかを入力することが可能です。
Probe Number(1-1000)	予定された traceroute パス上の次のホップに probe パケットをスイッチが送信する回数を指定します。初期値は 1 です。

「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。

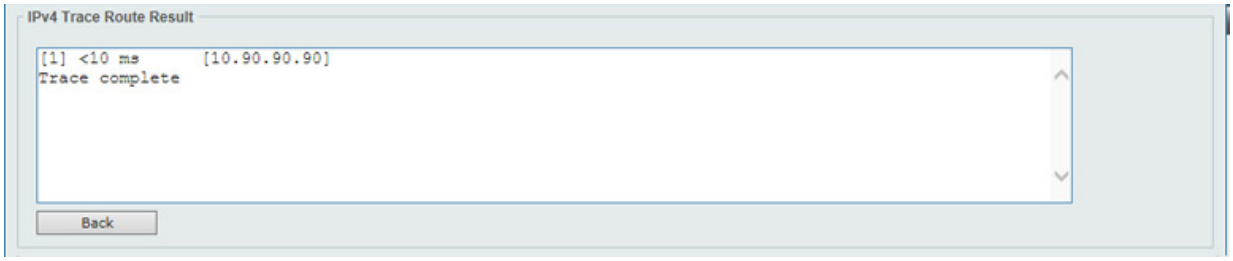


図 19-40 Trace Route Result（IPv4）画面

「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。

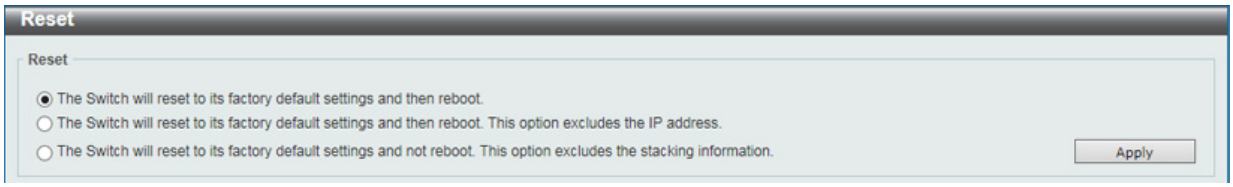


図 19-41 Reset System 画面

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、保存、再起動を実行します。 (IP アドレス、スタック情報を含む)
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の設定に戻し、保存、再起動を実行します。 (IP アドレスは除く)
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、リセット操作を開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

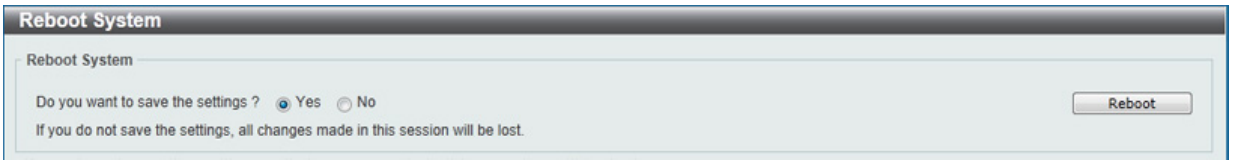


図 19-42　Reboot System 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Yes	スイッチは再起動する前に現在の設定を保存します。
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	スイッチは再起動します。

「Reboot」をクリックして再起動を開始します。

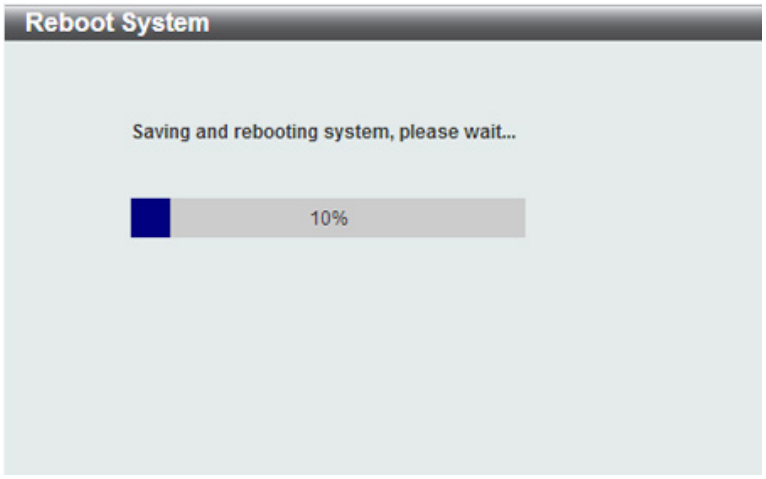


図 19-43　System Rebooting 画面

DLMS Settings（DLMS 設定）

本項目では「D-Link License Management System」(DLMS) の設定、表示を行います。
ライセンスは特定の機能を有効にする場合において指定します。「License keys」は購入する必要があります。物理的なパッケージとして印刷されているか、メールやポータルなどで画面に表示される場合もあります。ユーザは「Global Registration Portal」（GRP）にてライセンスキーを登録し、アクティベーションコードを取得する必要があります。様々な機能の有効化 / ロック解除において、適切にアクティベーションコードを取得してインストールする必要があります。アクティベーションコードのインストールに成功すると、スイッチは再起動しライセンスのアクティベートを行います。

Tools > DLMS Settings をクリックし、次の設定画面を表示します。

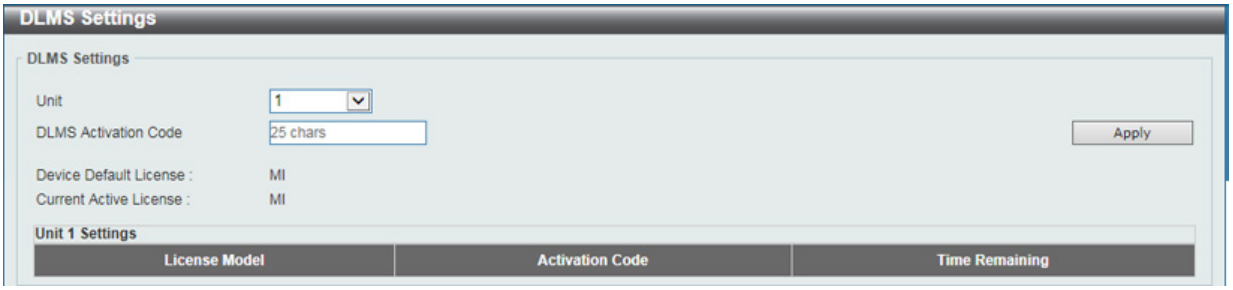


図 19-44　DLMS Settings 画面

項目	説明
Unit	設定を行うユニットを指定します。
DLMS Activation Code	DLMS アクティベーションコード（25 字以内）を指定します。

「Apply」ボタンをクリックして、リセット操作を開始します。

付録 A パスワードリカバリ手順

弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。
権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用することです。ネットワーク管理者は、パスワードが忘れられたり、壊れた場合に、これらのパスワードをリセットする必要があります。このパスワードリカバリ機能は、そのような場合にネットワーク管理者を助けるものです。以下にパスワードを容易に回復するパスワードリカバリ機能の使用方法を説明します。

以下の手順を終了するとパスワードはリセットされます。

1. セキュリティの理由のため、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ことが必要です。そのため、デバイスのコンソールポートへの直接接続を行っている場合だけ、本機能を適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を使用して、スイッチのコンソールポートに端末または PC を接続する必要があります。
2. 電源をオンにします。「Password Recovery Mode」に入るためには、「UART init」が 100% までロードされた後 2 秒以内に、ホットキー「 ^ 」を押します。「Password Recovery Mode」に一度入ると、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-68-34-00-10
H/W Version   : A1

Please Wait, Loading 2.00.008 Runtime Image ............... 100 %
UART init ................................................. 100 %
Starting runtime image
```

```
Password Recovery Mode
Switch(reset-config)#
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
no enable password	全アカウントレベルのパスワードを削除します。
no login 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手順を開始します。
reload	スイッチを再起動します。
reload clear running-config	起動中の設定を工場出荷値に戻し、保存、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：** • username：認証されているユーザ名 • interface-id：スイッチインタフェース番号 • 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 タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	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 タイプ。 例：Console、Telnet、SSH、Web、Web(SSL) • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	Warning	ログインに失敗しました。

ログの内容	緊急度	イベントの説明
Login failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • server-ip：AAA サーバ IP アドレス • username：認証されるユーザ名	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。
Successful enable privilege through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：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 タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	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 タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • server-ip：AAA サーバ IP アドレス • username：認証されるユーザ名	Warning	リモートサーバが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。

ログの内容	緊急度	イベントの説明
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。
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。
ARP Spoofing Prevention		
Gateway <ipaddr> is under attack by <macaddr> from <intf-name> **パラメータ説明：** • ipaddr：IP アドレス • macaddr：MAC アドレス • intf_name：インタフェース名	Warning	偽の ARP パケットが ARP スプーフィング防止に検出されました。

ログの内容	緊急度	イベントの説明
Auto image		
The downloaded firmware was successfully executed by DHCP Auto image update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：IP アドレス	Informational	DHCP 自動イメージによるファームウェアダウンロードは成功しました。
The downloaded firmware was not successfully executed by DHCP Autoimage update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：IP アドレス	Informational	DHCP 自動イメージによるファームウェアダウンロードは失敗しました。
Auto Save		
CONFIG-6-DDPSAVECONFIG: [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：ユーザ名 • ipaddr：IP アドレス	Informational	DDP の設定情報が自動で保存されました。
Auto Surveillance VLAN		
New surveillance device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface–id：インタフェース名（ID） • mac-address：MAC アドレス	Informational	インタフェースで新しい監視デバイスが検出されました。
<interface-id> add into surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名（ID） • vid：VLAN ID	Informational	サーベイランス VLAN が有効のインタフェースが自動的にサーベイランス VLAN に追加されました。
<interface-id> remove from surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名（ID） • vid：VLAN ID	Informational	インタフェースがサーベイランス VLAN から離脱しました。同時に一定の期間内に当該のインタフェースに監視デバイスが検出されず、ログメッセージが送信されました。
BGP		
BGP-6-ESTABLISH: BGP connection is successfully established (Peer:<ipaddr>). **パラメータ説明：** • ipaddr：IP アドレス	Informational	ピアとの BGP FSM の構築に成功しました。
BGP-6-NORMALCLOSE: BGP connection is normally closed (Peer:<ipaddr>). **パラメータ説明：** • ipaddr：IP アドレス	Informational	BGP 接続が通常通り閉じました。
BGP-4-ERRCLOSE: BGP connection is closed due to error (Code:<num> Subcode:<num> Field:<field> Peer:<ipaddr>). **パラメータ説明：** • num：エラーコード / サブコード • filed：エラー発生場所 • ipaddr：IP アドレス	Warning	BGP 接続がエラーによって閉じました。（エラーコード、エラーサブコード、RFC 参照のデータ項目）

ログの内容	緊急度	イベントの説明
BGP-4-RCVUNKOWNERR: BGP Notify: unknown Error code(num), Sub Error code(num), Peer:<ipaddr>. **パラメータ説明：** • num：エラーコード / サブコード • ipaddr：IP アドレス	Warning	RFC4271 による未定義のエラーコード / エラーサブコード付き BGP 通知パケットの受信
BGP-4-BADNHOP: BGP Update Attr NHop: Erroneous NHop <ipaddr> Peer:<ipaddr>. **パラメータ説明：** • ipaddr：IP アドレス	Warning	ネクストホップポイントがローカルインタフェースの BGP アップデートパケットの受信
BGP-4-EVENTCLOSE: BGP connection is closed due to Event: <num> (Peer:<ipaddr>). **パラメータ説明：** • num：RFC4271 で定義されたイベント • ipaddr：IP アドレス	Warning	イベント発生による BGP 接続の切断（イベントは RFC で定義）
BGP-4-NOTIFYCLOSE: BGP connection is closed due to Notify: Code <num> Subcode <num> (Peer:<ipaddr>). **パラメータ説明：** • num：RFC4271 で定義されたエラーコード / エラーサブコード • ipaddr：IP アドレス	Warning	通知パケットの受信による BGP 接続の切断（RFC 定義のエラーコード / エラーサブコード）
BGP-6-PEERPFXMAX: The number of prefix received reaches <num>, max <limit> (Peer <ipaddr>). **パラメータ説明：** • num：受信したプリフィクス • limit：受信可能なプリフィクスの値 • ipaddr：IP アドレス	Informational	BGP のプリフィクスが最大しきい値に到達しました。
BGP-6-TOTALPFXMAX: The total number of prefix received reaches max prefix limit.	Informational	受信 BGP プリフィクスの総数がしきい値を超えました。
BGP-4-RCVUNNECEAS4PATH: Received AS4-PATH attribute from new (4-bytes AS) peer. (Peer <ipaddr>). **パラメータ説明：** • ipaddr：IP アドレス	Warning	新しい BGP ピア（4 バイト AS）から BGP が不要な「AS4-PATH」属性を受信しました。
BGP-4-RCVUNNECEAS4AGGRE: Received AS4-AGGREGATOR attribute from new (4-bytes AS) peer. (Peer <ipaddr>). **パラメータ説明：** • ipaddr：IP アドレス	Warning	新しい BGP ピア（4 バイト AS）から BGP が不要な「AS4-AGGREGATOR」属性を受信しました。
BGP-4-RCVASCONFEDINAS4PATH: Received AS_CONFED_SEQUENCE or AS_CONFED_SET path segment type in AS4-PATH attribute. (Peer <ipaddr>). **パラメータ説明：** • ipaddr：IP アドレス	Warning	BGP が「AS4-PATH」属性の「AS_CONFED_SEQUENCE or AS_CONFED_SET」パスセグメントタイプを受信しました。
BGP-4-RCVBADAS4AGGRE: Received invalid AS4- AGGREGATOR attribute. Value : <STRING> (Peer <ipaddr>). **パラメータ説明：** • ipaddr：IP アドレス	Warning	BGP 無効な「AS4-AGGREGATOR」属性を受信しました。

ログの内容	緊急度	イベントの説明
BGP-4-RCVBADAS4PATH: Received invalid AS4-PATH attribute. Value : <STRING> (Peer <ipaddr>). **パラメータ説明：** • ipaddr：IP アドレス	Warning	BGP 無効な「AS4-PATH」属性を受信しました。
BPDU Potection（BPDU 攻撃防御）		
<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。モードは、ドロップ、ブロック、またはシャットダウンにすることができます。	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」または「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。
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」または「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。

ログの内容	緊急度	イベントの説明
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」または「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」または「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」または「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
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」または「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」または「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

ログの内容	緊急度	イベントの説明
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」または「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」または「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。
[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。

ログの内容	緊急度	イベントの説明
[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、ログに追加…
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、ログに追加…

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。しきい値タイプは以下のうちのどれか 1 つ。 - temperature - supply voltage - bias current - TX power - RX power - high-low：高もしくは低しきい値	Warning	SFP パラメータのど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。しきい値タイプは以下のうちのどれか 1 つ。 - temperature - supply voltage - bias current - TX power - RX power - high-low：高もしくは低しきい値	Critical	SFP パラメータのど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。しきい値タイプは以下のうちのどれか 1 つ。 - temperature - supply voltage - bias current - TX power - RX power - high-low：高もしくは低しきい値	Warning	SFP パラメータのど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。

ログの内容	緊急度	イベントの説明
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。
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。
DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> **パラメータ説明：** • intf-name：DHCPv6 クライアント PD インタフェース名	Informational	DHCPv6 クライアント PD インタフェースの管理者ステートが変更されました。
DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> **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	DHCPv6 クライアント PD が、デリゲイションルータから IPv6 プレフィックスを取得しました。
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。

ログの内容	緊急度	イベントの説明
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 Relay		
DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] **パラメータ説明：** • <ipif-name>：DHCPv6 リレーエージェントインタフェース名	Informational	特定のインタフェースの管理者ステートの DHCPv6 リレーが変更されました。
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。
DLMS		
Illegal activation code (AC: <string25>). **パラメータ説明：** • <string25>：アクティベーションコード	Informational	入力したアクティベーションコードが違法のものです。
License expired (license:<license-model>, AC: <string25>). **パラメータ説明：** • <string25>：アクティベーションコード	Critical	ライセンスが期限切れです。
License successfully installed (license:<license-model>, AC: <string25>). **パラメータ説明：** • <license-model>：ライセンスモデル名 • <string25>：アクティベーションコード	Informational	ライセンスのインストールに成功しました。
Unbound Activation Code (AC: <string25>). **パラメータ説明：** • <string25>：アクティベーションコード	Critical	アクティベーションコードが紐づいていません（Unbound）。
License will expire in 30 days. (license:<license-model>, AC: <string25>). **パラメータ説明：** • <license-model>：ライセンスモデル名 • <string25>：アクティベーションコード	Informational	ライセンスの期限が 30 日以内に迫っています。

ログの内容	緊急度	イベントの説明
DNS Resolver		
[DNS_RESOLVER(1):]Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr> **パラメータ説明：** • domainame：ドメイン名文字列 • ipaddr：IP アドレス	Informational	重複するドメイン名キャッシュが追加され、ダイナミックドメイン名キャッシュが削除されました。
DoS Prevention		
<dos-type> is dropped from (IP: <ip-address> Port <interface-id>). **パラメータ説明：** • dos-type：DoS 攻撃タイプ • ip-address:：IP アドレス • interface-id:：インタフェース名	Notice	DoS 攻撃を検出しました。
DULD		
DULD <INTERFACE-ID> is detected as unidirectional link. **パラメータ説明：** • INTERFACE-ID：インタフェース名	Warning	DULD はインタフェースが単一方向性であることを検出しました。
Dynamic ARP Inspection（DAI）		
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、「request」か「ARP response」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。
Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) **パラメータ説明：** • type：ARP パケットの種類。ARP パケットが、「request」か「ARP response」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	Informational	DAI が有効な ARP パケットを検出しました。
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	ノードにスイッチがイシューされました。
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	ノードにシグナル失敗が検出されました。

ログの内容	緊急度	イベントの説明
"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	ノードの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	フォーススイッチがイシューされました。
"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	クリアコマンドがイシューされました。
"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 オーナーがノードでコンフリクトしています。
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。
Device encountered an OAM dying gasp event	Warning	ローカルで「Dying gasp」イベントが発生。
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。
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。
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。
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。
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。

ログの内容	緊急度	イベントの説明
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。
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発生。
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。
Device encountered an errored symbol period event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	シンボル期間イベントでエラーが発生しています。
Device encountered an errored frame event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	フレームイベントでエラーが発生しています。
Device encountered an errored frame period event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	フレーム期間イベントでエラーが発生しています。
Device encountered an errored frame seconds summary event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	フレーム秒サマリイベントでエラーが発生しています。
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。

ログの内容	緊急度	イベントの説明
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当たり、ハードウェアルールのリソースがない場合、シスログが記録されます。
IPv6 Source Guard		
Failed to set IPv6SG 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：IPv6 アドレス • mac-address：MAC アドレス • vlanid：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 IPv6SG テーブルにセットするに当たり、ハードウェアルールのリソースがない場合、シスログが記録されます。
IPv6 Snooping		
Failed to glean (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) **パラメータ説明：** • IPADDR：IPv6 アドレス • MACADDR：MAC アドレス • vlanid：VLAN ID • INTERFACE_ID：インタフェース ID	Notice	IPv6 Data Glean に失敗しました。
Glean to recover (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) **パラメータ説明：** • IPADDR：IPv6 アドレス • MACADDR：MAC アドレス • vlanid：VLAN ID • INTERFACE_ID：インタフェース ID	Informational	IPv6 Data Glean に成功しました。

ログの内容	緊急度	イベントの説明
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す。
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す。
<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。
<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。

ログの内容	緊急度	イベントの説明
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。

ログの内容	緊急度	イベントの説明
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。
Login/Logout		
[Unit <unitID>,]Successful login through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：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：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：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：ユーザ名	Informational	コンソール経由でログアウトしました。

ログの内容	緊急度	イベントの説明
Successful login through Telnet (Username: <username>, IP: <ipaddr | ipv6address>) **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 • ipv6addr：クライアントの IPv6 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 | ipv6address>) **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 • ipv6addr：クライアントの IPv6 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 | ipv6address>) **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 • ipv6addr：クライアントの IPv6 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 | ipv6address>) **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 • ipv6addr：クライアントの IPv6 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 • ipv6addr：クライアントの IPv6 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 • ipv6addr：クライアントの IPv6 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 • ipv6addr：クライアントの IPv6 アドレス	Informational	SSH のセッションはタイムアウトしました。
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 • ipv6addr：クライアントの IPv6 アドレス	Informational	SSH 経由でログアウトしました。

ログの内容	緊急度	イベントの説明
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時間間隔内のの最大ユーザ制限数未満になりました。
<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	インタフェースの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	インタフェースの認証されたユーザ数が時間間隔内の最大ユーザ制限数未満になりました。
MLAG		
Multi-Chassis Link Aggregation Group <group id > <link status> **パラメータ説明：** • group id：MLAG のグループ ID • Link status：リンクステータス 値のリスト： 1. link up：グループの最初のメンバポートがリンクアップ状態です。 2. link down：グループの最後のメンバポートがリンクダウン状態です。	Informational	MLAG グループのリンクステータスが変更されました。
The MLAG logical switch is <status> **パラメータ説明：** • status：論理スイッチのステータス 値のリスト： 1. built up：MLAG の論理スイッチが確立しています。 2. destroy：MLAG の論理スイッチが削除されました。	Informational	MLAG 論理スイッチのステータスが変更されました。

ログの内容	緊急度	イベントの説明
The MLAG state is conflict (<conflict>) **パラメータ説明：** • conflict：競合の原因 値のリスト： 1. domain is different：ドメインがピアデバイスと異なります。 2. device id is same：デバイス ID がピアスイッチと同じです。 3. hello interval is different：hello 間隔がピアスイッチと異なります。 4. MLAG found third device：3 つ目のデバイスが MLAG に接続されました。 5. peer-link is not set：ピアリンクのインタフェースが設定されていません。	Informational	MLAG グループで競合が発生しています。
The MLAG group <group_id> is down (<causes>) **パラメータ説明：** • group id：MLAG のグループ ID • causes：設定が異なっている原因 値のリスト： 1. group ID is not existed：MLAG のグループ ID が存在しません。 2. algorithm is different：リンクアグリゲーションのアルゴリズムが異なります。 3. total member port is over maximum number：ローカルポート数とピアポート数がサポートされる数を超えています。	Informational	MLAG グループでピアと異なる設定が使用されています。
MPLS		
LSP <lsp_id> is up **パラメータ説明：** • lsp-id：インスタンス ID	Informational	LSP がアップされました。
LSP <lsp_id> is down **パラメータ説明：** • lsp-id：インスタンス ID	Informational	LSP がダウンされました。
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定されました。
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定されました。
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：旧ステータス • new_status：新ステータス	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：削除する VLAN 範囲の開始 VID • endvlanid：削除する VLAN 範囲の終了 VID	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：削除する VLAN 範囲の開始 VID • endvlanid：削除する VLAN 範囲の終了 VID	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。

ログの内容	緊急度	イベントの説明
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	ガードルートのためにスパニングツリーポートロールが交代します。
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。
OSPFv2 Enhancement（OSPFv2 エンハンスメント）		
OSPF interface <intf-name> changed state to [Up | Down] **パラメータ説明：** • intf-name：OSPF インタフェース	Informational	OSPF インタフェースのリンクステートが変更されました。
OSPF protocol on interface <intf-name> changed state to [Enabled | Disabled] **パラメータ説明：** • intf-name：OSPF インタフェース	Informational	OSPF インタフェースの管理者ステートが変更されました。
OSPF interface <intf-name> changed from area <area-id> to area <area-id> **パラメータ説明：** • intf-name：OSPF インタフェース • area-id：OSPF エリア ID	Informational	OSPF インタフェースがエリア変更されました。
OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full **パラメータ説明：** • intf-name：OSPF インタフェース • nbr-id：ネイバルータ ID	Notice	OSPF ネイバステートが「Loading」から「Full」に変更されました。
OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down **パラメータ説明：** • intf-name：OSPF インタフェース • nbr-id：ネイバルータ ID	Notice	OSPF ネイバステートが「Full」から「Down」に変更されました。
OSPF nbr <nbr-id> on interface <intf-name> dead timer expired **パラメータ説明：** • intf-name：OSPF インタフェース • nbr-id：ネイバルータ ID	Notice	OSPF ネイバステートデッドタイマ期限が切れました。
OSPF nbr <nbr-id> on virtual link changed state from Loading to Full **パラメータ説明：** • nbr-id：ネイバルータ ID	Notice	OSPF 仮想ネイバステートが「Loading」から「Full」に変わりました。
OSPF nbr <nbr-id> on virtual link changed state from Full to Down **パラメータ説明：** • nbr-id：ネイバルータ ID	Notice	OSPF 仮想ネイバステートが「Full」から「Down」に変わりました。

ログの内容	緊急度	イベントの説明
OSPF router ID changed to <router-id> **パラメータ説明：** • nbr-id：OSPF ルータ ID	Informational	OSPF ルータ ID が変更されました。
Peripheral（周辺機器）		
Unit <unit-id>, <fan-descr> back to normal **パラメータ説明：** • unitID：ユニット ID • <fan-descr>：ファン概要	Critical	ファンが回復しました。
Unit <unit-id> <fan-descr> failed **パラメータ説明：** • unitID：ユニット ID • <fan-descr>：ファン概要	Critical	ファンの故障
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。
PoE		
Unit <unit-id> usage threshold <percentage> is exceeded **パラメータ説明：** • unitID：ユニット ID • percentage：使用率しきい値	Warning	総電力の使用率がしきい値を超えました。

ログの内容	緊急度	イベントの説明
Unit <unit-id> usage threshold <percentage> is recovered **パラメータ説明：** • unitID：ユニット ID • percentage：使用率しきい値	Warning	総電力の使用率がしきい値を下回りました。
PD alive check failed. (Port: <portNum>, PD: <ipaddr>) **パラメータ説明：** • portNum：ポート番号 • ipaddr：IP アドレス	Warning	PD が Ping リクエストに回答しません。
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
Limit on system entry number has been exceeded	Warning	システム上のアドレスが超過
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。
System was restarted by schedule in an interval time	Informational	指定間隔での再起動
System was restarted by schedule at specific time	Informational	指定時間での再起動
Configuration was saved by schedule	Informational	スケジュールされた再起動の前にコンフィグを保存します。
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、Syslog に記録されます。
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、Syslog に記録されます。
SD Card Management		
Entry <entry-name> to execute configuration <filename> at time <time-range> failure. **パラメータ説明：** • entry-name：実行スケジュール設定エントリ • filename：ファイル名 • time-range：時間範囲	Warning	実行スケジュールの設定失敗

ログの内容	緊急度	イベントの説明
Entry <entry-name> to backup <type>:<filename> at time <time-range> failure. **パラメータ説明：** • entry-name：実行スケジュール設定エントリ • type：設定 / ログ • filename：ファイル名 • time-range：時間範囲	Warning	実行スケジュールの設定 / ログ失敗
Entry <entry-name> to execute configuration <filename> success at time <time-range> **パラメータ説明：** • entry-name：実行スケジュール設定エントリ • filename：ファイル名 • time-range：時間範囲	Informational	実行スケジュールの設定成功
Entry <entry-name> to backup <type>:<filename> success at time <time-range> **パラメータ説明：** • entry-name：実行スケジュール設定エントリ • type：設定 / ログ • filename：ファイル名 • time-range：時間範囲	Informational	実行スケジュールの設定 / ログ成功
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。
SRM		
Unit <unitID> SRM mode is different with master **パラメータ説明：** • unitID：ユニット ID	Alert	スタック成功時にマスタにより違う SRM モードのスレーブが確認されました。
SSH		
SSH server is enabled	Informational	SSH サーバは有効
SSH server is disabled	Informational	SSH サーバは無効
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。

ログの内容	緊急度	イベントの説明
Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>) **パラメータ説明：** • Stack_TP_TYPE：スタッキングトポロジタイプ 1. Ring 2. Chain • unitID：ボックス ID • Macaddr：MAC アドレス	Critical	スタッキングトポロジ変更
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
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
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：MAC アドレス	Critical	ボックス ID が重複
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
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
SIO interface Unit <unitID> <SIOID > link up **パラメータ説明：** • unitID：SIO インタフェースがリンクアップしているボックス ID • SIOID：SIO インタフェース番号。サポートされている SIO インタフェース番号は「SIO1」か「SIO2」です。	Critical	SIO インタフェースがリンクアップ
SIO interface Unit <unitID> <SIOID > link down **パラメータ説明：** • unitID：SIO インタフェースがリンクアップしているボックス ID • SIOID：SIO インタフェース番号。サポートされている SIO インタフェース番号は「SIO1」か「SIO2」です。	Critical	SIO インタフェースがリンクダウン

ログの内容	緊急度	イベントの説明
Storm Control		
<Broadcast | Multicast | Unicast> storm is occurring on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Warning	ストーム発生
<Broadcast | Multicast | Unicast> storm is cleared on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Informational	ストームが解消されました。
<interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Warning	パケットストームによりポートシャットダウン
System		
[Unit <unitID>,]System warm start **パラメータ説明：** • unitID：ユニット ID	Critical	システムがウォームスタートしました。
[Unit <unitID>,]System cold start **パラメータ説明：** • unitID：ユニット ID	Critical	システムがコールドスタートしました。
[Unit <unitID>,]System started up. **パラメータ説明：** • unitID：ユニット ID	Critical	システムが起動しました。

ログの内容	緊急度	イベントの説明
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 サーバーにログインするユーザ名	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 サーバーにログインするユーザ名	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 サーバーにログインするユーザ名	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 サーバーにログインするユーザ名	Informational	Telnet セッションのタイムアウト
Traffic Control		
<interface-id> Broadcast storm is occurring **パラメータ説明：** • interface-id：インタフェース ID	Warning	ブロードキャストストームが発生
<interface-id> Broadcast storm is cleared **パラメータ説明：** • interface-id：インタフェース ID	Informational	ブロードキャストストームが解消
<interface-id> Multicast storm is occurring **パラメータ説明：** • interface-id：インタフェース ID	Warning	マルチキャストストームが発生
<interface-id> Multicast storm is cleared **パラメータ説明：** • interface-id：インタフェース ID	Informational	マルチキャストストームが解消
<interface-id> Unicast storm is occurring **パラメータ説明：** • interface-id：インタフェース ID	Warning	ユニキャストストームが発生
<interface-id> Unicast storm is cleared **パラメータ説明：** • interface-id：インタフェース ID	Informational	ユニキャストストームが解消
<interface-id> is currently shut down due to a packet storm. **パラメータ説明：** • interface-id：インタフェース ID	Warning	パケットストームの発生に伴い、ポートシャットダウン

ログの内容	緊急度	イベントの説明
Voice VLAN		
New voice device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface-id：インタフェース ID • mac-address：MAC アドレス	Informational	インタフェースで音声機器が検出されました。
<interface-id> add into voice VLAN <vid> **パラメータ説明：** • vid：VLAN ID • interface-id：インタフェース ID	Informational	自動音声 VLAN モードのインタフェースが音声 VLAN に追加されました。
<interface-id> remove from voice VLAN <vid> **パラメータ説明：** • vid：VLAN ID • interface-id：インタフェース ID	Informational	インタフェースが音声 VLAN から離脱し、一定期間内に音声機器がインタフェースに検出されませんでした。ログメッセージが送信されます。
VPLS		
VPLS <vpls_name> link up **パラメータ説明：** • vpls_name：VPLS 名	Informational	VPLS がリンクアップ
VPLS <vpls_name> link down **パラメータ説明：** • vpls_name：VPLS 名	Informational	VPLS がリンクダウン
VPWS		
Pseudowire id <vc_id> peer ip <ipaddr> link down **パラメータ説明：** • vc_id：pseudowire ID • ipaddr：IP アドレス	Informational	Pseudowire がリンクダウン
Pseudowire id <vc_id> peer ip <ipaddr> link up **パラメータ説明：** • vc_id：pseudowire ID • ipaddr：IP アドレス	Informational	Pseudowire がリンクアップ
Pseudowire id <vc_id> peer ip <ipaddr>is deleted **パラメータ説明：** • vc_id：pseudowire ID • ipaddr：IP アドレス	Informational	Pseudowire が削除
Pseudowire id <vc_id> peer ip <ipaddr> link standby **パラメータ説明：** • vc_id：pseudowire ID • ipaddr：IP アドレス	Informational	Pseudowire リンクがスタンドバイ
VRRP Debug（VRRP デバッグ）		
VR <vr-id> at interface <intf-name> switch to Master **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Informational	ある仮想ルータがマスタに移行しました。

ログの内容	緊急度	イベントの説明
VR <vr-id> at interface <intf-name> switch to Backup **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Informational	ある仮想ルータがバックアップに移行しました。
VR <vr-id> at interface <intf-name> switch to Init **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Informational	ある仮想ルータが「Init」に移行しました。
Authentication type mismatch on VR <vr-id> at interface <intf-name> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Warning	認証タイプが受信した VRRP アドバタイズメッセージと合致しません。
Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名 • Auth-type：VRRP インタフェース認証タイプ	Warning	受信した VRRP アドバタイズメッセージのチェックに失敗しました。
Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Warning	受信した VRRP アドバタイズメッセージのチェックにエラーが発生しました。
Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Warning	受信した VRRP アドバタイズメッセージと仮想ルータ ID が合致しません。
Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Warning	受信した VRRP アドバタイズメッセージとアドバタイズメント間隔が合致しません。
Added a virtual MAC <vrrp-mac-addr> into L2 table **パラメータ説明：** • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Notice	仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。
Deleted a virtual MAC <vrrp-mac-addr> from L2 table **パラメータ説明：** • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Notice	仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。
Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Notice	仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。

ログの内容	緊急度	イベントの説明
Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Notice	仮想 MAC アドレスがスイッチの L3 テーブルから削除されました。
Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> **パラメータ説明：** • vrrp-mac-addr：VRRP 仮想 MAC アドレス • vrrp-errcode：VRRP プロトコル動作のエラーコード	Error	スイッチチップ L2 テーブルへの仮想 MAC の追加に失敗しました。
Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> **パラメータ説明：** • vrrp-mac-addr：VRRP 仮想 MAC アドレス • vrrp-errcode：VRRP プロトコル動作のエラーコード	Error	スイッチチップ L2 テーブルの仮想 MAC の削除に失敗しました。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Error	スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。L3 テーブルは満杯です。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • mac-port：VRRP 仮想 MAC のポート番号	Error	スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したポートが無効です。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • mac-intf：VRRP 仮想 MAC アドレスを基にしたインタフェース	Error	スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したインタフェースが無効です。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • mac-box：VRRP 仮想 MAC アドレスを基にしたインタフェース	Error	スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したボックスが無効です。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • vrrp-errcode：VRRP プロトコル動作のエラーコード	Error	スイッチチップの L3 テーブルへの仮想 MAC の追加に失敗しました。

ログの内容	緊急度	イベントの説明
Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode> **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • vrrp-errcode：VRRP プロトコル動作のエラーコード	Error	スイッチチップの L3 テーブルへの仮想 MAC の削除に失敗しました。
WAC		
Web-Authentication host login fail (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>, VID: <vlan-id>) **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 • vlan-id：VLAN ID	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た時、本ログが生成されます。
Web-Authentication recovered from stop learning state	Warning	タイムインターバルのデバイス全体において認証ユーザ数が最大値を割り込んだ時、本ログが生成されます。
Web-Authentication host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>, VID: <vlan-id>) **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 • vlan-id：VLAN ID	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：ユーザ名 • ipaddr：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：ユーザ名 • ipaddr：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：ユーザ名 • ipaddr：IP アドレス	Informational	Web セッションがタイムアウトしました。

ログの内容	緊急度	イベントの説明
Logout through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web 経由でのログアウトしました。
Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web 経由でのログイン成功（SSL）
Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Warning	Web 経由でのログイン失敗（SSL）
Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web セッションがタイムアウトしました。（SSL）
Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web 経由でのログアウト成功（SSL）
Zone Defense		
Zone defense function has been enabled by <session> (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • session：ユーザセッション（Console, SNMP, WEB, Telnet） • username：ユーザ名 • ipaddr：IP アドレス	Warning	ゾーンディフェンスが有効化されました。
Zone defense function has been disabled by <session> (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • session：ユーザセッション（Console, SNMP, WEB, Telnet） • username：ユーザ名 • ipaddr：IP アドレス	Warning	ゾーンディフェンスが無効化されました。

付録 C トラップログエントリ

スイッチにおいて現れる可能性のある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、SNMPv2 エンティティが、エージェントロールで動作し、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。SNMPv2 のすべての実装は、このトラップを生成することができる必要がある一方、snmpEnableAuthenTraps オブジェクトは、このトラップが生成されるか否かを示します。	1.3.6.1.6.3.1. 1.5.5

カテゴリ	トラップ名	説明	OID
BGP	bgpEstablishedNotification	BGP FSM が完成状態になった時に、「bgpEstablishedNotification」イベントが起動します。 関連オブジェクト : (1) bgpPeerRemoteAddr (2) bgpPeerLastError (3) bgpPeerState	1.3.6.1.2.1.15.0.1
	bgpBackwardTransNotification	BGP FSM が高い値から低い値への移行時に、「bgpBackwardTransNotification」イベントが起動します。 関連オブジェクト : (1) bgpPeerRemoteAddr (2) bgpPeerLastError (3) bgpPeerState	1.3.6.1.2.1.15.0.2
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 が鍵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 の鍵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

カテゴリ	トラップ名	説明	OID
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 > low warning または現在の値 < high warning にときにのみリカバトラップを送信します。 関連オブジェクト : (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
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とき、スイッチが偽造 DHCP サーバパケットを受信すると、攻撃パケットを受信したイベントをトラップ送信します。 関連オブジェクト : (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

カテゴリ	トラップ名	説明	OID
External Alarm	dExternalAlarmStatusChg	外部警告ステートが変更されると、コマンダスイッチは本通知を送信します。 関連オブジェクト : (1) dExternalAlarmUnitID (2) dExternalAlarmChannel (3) dExternalAlarmStatus	1.3.6.1.4.1.171. 14.32.0.1
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) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.17 1.14.75.0.1
IP-MAC-Port Binding（IMPB）	dImpbViolationTrap	アドレス違反通知は IP-MAC ポートバインディングアドレス違反が検出された際に生成されます。 関連オブジェクト : (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.17 1.14.22.0.1
LACP	linkUp	「linkUp」トラップはエージェント役の SNMP エンティティによって、コミュニケーションリンクの一つがダウンステートに残り、「notPresent」ステート以外の他のステートに移行する「ifOperStatus」オブジェクトの検出を意味します。他のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
	linkDown	「linkDown」トラップはエージェント役の SNMP エンティティによって、コミュニケーションリンクの一つがダウンステートに残り、「notPresent」ステート以外の他のステートに移行する「ifOperStatus」オブジェクトの検出を意味します。他のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3

カテゴリ	トラップ名	説明	OID
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	間隔時間後、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	インタフェースに VID ループが発生したときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.17 1.14.46.0.3
	swVlanLoopRestart	間隔時間後、VID のインタフェースループが再スタートしたときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.17 1.14.46.0.4
LDP	mplsLdpInitSessionThresholdExceeded	「backoff」有効時、セッション初期化メッセージ数が「mplsLdpEntityInitSessionThreshold」のしきい値を超えると送信されます。	1.3.6.1.2.1.10. 166.4.0.1
	mplsLdpPathVectorLimitMismatch	「mplsLdpEntityPathVectorLimit」が指定のエントリで「mplsLdpPeerPathVectorLimit」の値と合致しない場合、送信されます。	1.3.6.1.2.1.10. 166.4.0.2
	mplsLdpSessionUp	「mplsLdpSessionState」ステートが「operational(5)」ステートになると送信されます。	1.3.6.1.2.1.10. 166.4.0.3
	mplsLdpSessionDown	「mplsLdpSessionState」ステートが「operational(5)」ステートになると送信されます。	1.3.6.1.2.1.10. 166.4.0.4
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	ローカルポートに新しいリモートデバイスがアタッチされた、またはリモートデバイスがポートから切断 / 移動した場合のトポロジの変更を感知するローカルデバイスによって送信されます。 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
MPLS	mplsXCUp	「mplsXCOperStatus」オブジェクトが「mplsXCTable」において近接するエントリが他のステートから「Up」ステートになった際、送信されます。	1.3.6.1.2.1.10. 166.2.0.1
	mplsXCDown	「mplsXCOperStatus」オブジェクトが「mplsXCTable」において近接するエントリが他のステートから「Down」ステートになった際、送信されます。	1.3.6.1.2.1.10. 166.2.0.2
MSTP	newRoot	newRoot トラップは、送信側のエージェントがスパニングツリーの新しいルートになったことを示します。トラップは、新しいルートとして選出された後にすぐにブリッジによって送信され、その選出に続いてすぐに Topology Change Timer のアクションの起動などを行います。 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、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。本トラップは、newRoot トラップが同様の変更に対して送信される場合には送信されません。 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）	dEntityExtFanStatusChg	ファン状態の変更通知 （ファンの不具合 (dEntityExtEnvFanStatus is 'fault') または回復 (dEntityExtEnvFanStatus is 'ok')） 関連オブジェクト： (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.2.1.17 1.14.5.0.1
	dEntityExtThermalStatusChg	温度状態の変更通知 （温度警告 (dEntityExtEnvTempStatus is 'abnormal') または回復 (dEntityExtEnvTempStatus is 'ok')） 関連オブジェクト： (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.2.1.17 1.14.5.0.2
	dEntityExtPowerStatusChg	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） 関連オブジェクト： (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.2.1.17 1.14.5.0.3

カテゴリ	トラップ名	説明	OID
PIM6-SM	pimNeighborLoss	「pimNeighborLoss」通知はネイバとの近隣性の消失時を意味します。本通知はネイバタイマが期限切れになり、同じ IP バージョン、より低い IP アドレスの同じインタフェースにネイバがいない場合に起動します。本通知はカウンタ「pimNeighborLossCount」が増加し、「pimNieghborLossNotificationsPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト : (1) pimNeighborUpTime	1.3.6.1.2.1. 157.0.1
	pimInvalidRegister	「pimInvalidRegister」通知はデバイスによって不正な PIM Register メッセージが受信された場合に起動します。本通知はカウンタ「pimInvalidRegisterMsgsRcvd」が増加し、「pimInvalidRegisterNotificationPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト : (1) pimGroupMappingPimMode (2) pimInvalidRegisterAddressType (3) pimInvalidRegisterOrigin (4) pimInvalidRegisterGroup (5) pimInvalidRegisterRp	1.3.6.1.2.1. 157.0.2
	pimInvalidJoinPrune	「pimInvalidJoinPrune」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimInvalidJoinPruneMsgsRcvd」が増加し、「pimInvalidJoinPruneNotificationPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト : (1) pimGroupMappingPimMode (2) pimInvalidJoinPruneAddressType (3) pimInvalidJoinPruneOrigin (4) pimInvalidJoinPruneGroup (5) pimInvalidJoinPruneRp (6) pimNeighborUpTime	1.3.6.1.2.1. 157.0.3
	pimRPMappingChage	「pimRPMappingChange」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimRPMappingChangeCount」が増加し、「pimRPMappingChangeNotificationPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト : (1) pimGroupMappingPimMode (2) pimGroupMappingPrecedence	1.3.6.1.2.1. 157.0.4
	pimInterfaceElection	「pimInterfaceElection」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimInterfaceElectionWinCount」が増加し、「pimInterfaceElectionNotificationPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト : (1) pimInterfaceAddressType (2) pimInterfaceAddress	1.3.6.1.2.1. 157.0.5

カテゴリ	トラップ名	説明	OID
PoE	pethMainPowerUsageOnNotification	使用率が PSE しきい値に到達した事を示唆しています。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105 .0.2
	pethMainPowerUsageOffNotification	使用率が PSE しきい値を下回った事を示唆しています。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105 .0.3
	dPoeIfPowerDeniedNotification	PSE 状況ダイアグラムが POWER_DENIED になった事を示唆する通知です。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171 .14.24.0.1
	dPoeIfPowerOverLoadNotification	PSE 状況ダイアグラムが ERROR_DELAY_OVER になった事を示唆するトラップです。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.171 .14.24.0.2
	dPoeIfPowerShortCircuitNotification	PSE 状況ダイアグラムが ERROR_DELAY_SHORT になった事を示唆するトラップです。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethPsePortShortCounter	1.3.6.1.4.1.171 .14.24.0.3
	dPoeIfPdAliveFailOccurNotification	PD が動作を中止、回答不能になった事を示唆するトラップです。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。	1.3.6.1.4.1.171 .14.24.0.4
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 アドレスが送出するトリガトラップメッセージです。 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
Reboot Schedule	agentRebootIn5Min	再起動のカウントダウンが 5 分になった時点で送信されます。	1.3.6.1.4.1.171. 14.170.0.1
	agentRebootIn1Min	再起動のカウントダウンが 1 分になった時点で送信されます。	1.3.6.1.4.1.171. 14.170.0.2

カテゴリ	トラップ名	説明	OID
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、SNMP トラップの送信に設定されたイベントを生成します。 関連オブジェクト : (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、NSMP トラップの送信に設定されたイベントを生成します。 関連オブジェクト : (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をノーマルから exhausted に変更したことを示します。 関連オブジェクト : (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を exhausted からノーマルに変更したことを示します。 関連オブジェクト : (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 1.12.8.6.0.11
	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 1.12.8.6.0.12
	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) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.13
	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) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.14
	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) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.15
	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) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.16
	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) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.17

カテゴリ	トラップ名	説明	OID
Stacking	dStackInsertNotification	ユニットホットインサート（活線挿入）の通知です。 関連オブジェクト： (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.1
	dStackRemoveNotification	ユニットホットリムーブ（活線抜出）の通知です。 関連オブジェクト： (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.2
	dStackFailureNotification	ユニットスタック失敗の通知です。 関連オブジェクト： (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.3
	dStackTPChangeNotification	スタックトポロジ変更の通知です。 関連オブジェクト： (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.4
	dStackRoleChangeNotification	スタックユニットロール変更の通知です。 関連オブジェクト： (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.5
Start（スタート）	coldStart	coldStart トラップは、SNMPv2 エンティティが、エージェントロールで動作し、自身を再起動し、設定が変更されたかもしれないことを表します。	1.3.6.1.6.3.1.1.5.1
	warmStart	warmStart トラップは、SNMPv2 エンティティが、エージェントロールで動作し、設定が変更されないような再起動を表します。	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

カテゴリ	トラップ名	説明	OID
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
VPWS	pwDown	「pwTable」において「pwOperStatus」オブジェクトの近接するエントリが他のステートから「down (2) 」または「lowerLayerDown (6)」ステートになった際、送信されます。(「notPresent (5)」からの移行時は除く)	1.3.6.1.2.1. 10.246.0.1
	pwUp	「pwTable」において「pwOperStatus」オブジェクトの近接するエントリが他のステートから「up (1)」ステートになった際、送信されます。(「notPresent (5)」からの移行時は除く)	1.3.6.1.2.1. 10.246.0.2
	pwDeleted	PW が削除された時に送信されます。(例 ; 「pwRowStatus」が「destroy (6)」にセットされる、または「non-MIB」アプリケーションか「auto-discovery」のプロセス上、PW が削除された場合)	1.3.6.1.2.1. 10.246.0.3
VRRP	vrrpTrapNewMaster	送信エージェントが「Master」に変換された場合、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	ルータからの受信したパケットの認証鍵、または認証タイプがルータの認証鍵、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)	swWACLoggedSuccess	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) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.17 1.14.154.0.1
	swWACLoggedFail	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 1.14.154.0.2

付録 D OpenFlow オブジェクト

アプリケーション開発者は、OpenFlow プロトコル V1.3 を使用してオブジェクトのプログラムを行うことができます。ここでは、プログラム可能なオブジェクト（Flow Table、Group Table エントリ、Meter Table エントリのオブジェクト）について説明します。

Flow Table（フローテーブル）

Flow Table Number Assignments

Flow Table 名	Flow Table ID	Default Table Miss Action
Policy ACL Flow Table	0	Drop

Flow Table Counters

フィールド	説明
Reference Count (Active Entries)	テーブル内のアクティブエントリ数の参照カウント
Packet Lookups	サポートされていません。
Packet Matches	サポートされていません。

Policy ACL Flow Table

Policy ACL Flow Table Match Fields

フィールド	説明
IN_PORT	スイッチの入力ポートです。
IN_PHY_PORT	スイッチの物理入力ポートです。
ETH_DST	イーサネット宛先アドレスです。 注意 IPv6 Flow（ETH_TYPE=0x86DD）はサポートされていません。
ETH_SRC	イーサネット送信元アドレスです。 注意 IPv6 Flow（ETH_TYPE=0x86DD）はサポートされていません。
ETH_TYPE	イーサネットフレームタイプです。 注意 Policy ACL Flow Table は、2 つの相互排他論理サブテーブルに構成されます。IPv6 論理テーブルの Flow エントリは、IPv6 パケット（ETH_TYPE=0x86DD）のみに一致します。非 IPv6 論理テーブルは非 ipv6 パケットに一致します。（ETH_TYPE ≠ 0x86DD、または ETH_TYPE の指定なしの場合）
VLAN_VID	VLAN ID です。 注意 0x1000（OFPVID_PRESENT）でプログラムされる必要があります。
VLAN_PCP	VLAN の優先度です。
IP_DSCP	IP DSCP（ToS フィールド内の 6 ビット）です。
IP_PROTO	IP プロトコルです。
IPV4_SRC	送信元 IPv4 アドレスです。
IPV4_DST	宛先 IPv4 アドレスです。
TCP_SRC	送信元 TCP ポートです。
TCP_DST	宛先 TCP ポートです。
UDP_SRC	送信元 UDP ポートです。
UDP_DST	宛先 UDP ポートです。
SCTP_SRC	送信元 SCTP ポートです。
SCTP_DST	宛先 SCTP ポートです。
ARP_SPA	ARP 送信元 IPv4 アドレスです。
IPV6_SRC	送信元 IPv6 アドレスです。
IPV6_DST	宛先 IPv6 アドレスです。

Policy ACL Flow Table Instructions

フィールド	説明
Write-Actions	Policy ACL Flow Table Action Set テーブルのアクションのみ指定可能です。
Apply-Actions	Policy ACL Flow Table Action List Actions テーブルのアクションのみ指定可能です。
Clear-Actions	アクションセットを削除します。
Goto-Table	サポートされていません。
Write-Metadata	サポートされていません。
Meter	指定されたメーターを適用します。メーターエントリはフローの設定前に存在している必要があります。

Policy ACL Flow Table Action List Actions

フィールド	説明
Output	出力ポートを設定します。物理ポート及び予約済みのコントローラポートがサポートされています。
Set-Field	VLAN_PCP、IP_ECN、IP_DSCP フィールドがサポートされています。

Policy ACL Flow Table Action Set

フィールド	説明
Group	このテーブルの後のパケットを処理するために出力グループエントリを設定します。ルール及びパケットの種類と一致するグループが存在する必要があります。以下のいずれかになります。 • レイヤ 2 インタフェースグループエントリ • レイヤ 2 リライトグループエントリ • レイヤ 2 マルチキャストグループエントリ • レイヤ 3 ユニキャストグループエントリ • レイヤ 3 ECMP グループエントリ

Policy ACL Flow Table Counters

フィールド	説明
Received Packets	このフローエントリによって受信されるパケット数です。
Received Bytes	このフローエントリによって受信されるパケット byte 数です。
Duration (Seconds)	フローエントリがセットされてから経過した時間（秒）です。

制限事項

Policy ACL Flow Table は 2 つの排他論理サブテーブルに構成されます。1 つは IPv6 Flow に一致し、もう 1 つは非 IPv6 Flow に一致します。これら 2 つのテーブルは単一のテーブルとみなされる必要があります。以下の制限があります。

- IPv6 パケットは、Policy ACL Flow テーブルの 2 つのルールに一致する可能性があります。本問題を回避するため、非 IPv6 論理テーブルに、ETH_TYPE または他の Match Field を追加することを推奨します。
- 異なるサブテーブルの 2 つのルールに対し、同じメーターを適用することはできません。異なるルールに対しては、それぞれ別のメーターを適用することを推奨します。

Group Table（グループテーブル）

L2 Interface Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は L2 Interface Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは Indirect です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

L2 Interface Group Entry Naming Conversion

フィールド	Bits	説明
Interface ID	0-15	インタフェース ID を指定します。
Chain ID	16-27	他のグループタイプエントリと紐づく ID を 1-4094 の範囲で指定します。
Kind	28-31	0（L2 インタフェース）

L2 Interface Group Entry Bucket Actions

フィールド	説明
Output	物理ポートのみでサポートされています。

L2 Interface Group Entry Counters

フィールド	説明
Reference Count（Flow Entries）	現在このグループエントリを参照しているフローエントリまたはグループエントリの数です。
Duration（Seconds）	グループエントリがセットされてから経過した時間（秒）です。

L2 Rewrite Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は L2 Rewrite Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは Indirect です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

L2 Rewrite Group Entry Naming Conversion

フィールド	Bits	説明
ID	0-27	本タイプのグループエントリを区別するためのインデックス値です。
Kind	28-31	1（L2 Rewrite）

L2 Rewrite Group Entry Bucket Actions

フィールド	説明
Group	このフィールドはレイヤ 2 インタフェースグループエントリに紐づく必要があります。
Set-Field	ETH_DST、ETH_SRC、VLAN_VID フィールドを設定します（オプション）。

L2 Rewrite Group Entry Counters

フィールド	説明
Reference Count（Flow Entries）	現在このグループエントリを参照しているフローエントリまたはグループエントリの数です。
Duration（Seconds）	グループエントリがセットされてから経過した時間（秒）です。

L2 Multicast Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は L2 Multicast Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは All です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

L2 Multicast Group Entry Naming Conversion

フィールド	Bits	説明
Index	0-15	これらの種類のグループのインデックスです。
Chain ID	16-27	レイヤ 2 インタフェースグループエントリの参照に使用されます。1-4094 の範囲で指定します。
Kind	28-31	3（L2 マルチキャスト）

L2 Multicast Group Entry Bucket Actions

フィールド	説明
Group	このフィールドはレイヤ 2 インタフェースグループエントリに紐づきます。該当エントリの Chain ID 名コンポーネントは、本グループエントリ名の Chain ID コンポーネントに一致します。

L2 Multicast Group Entry Counters

フィールド	説明
Reference Count（Flow Entries）	現在このグループエントリを参照しているフローエントリまたはグループエントリの数です。
Duration（Seconds）	グループエントリがセットされてから経過した時間（秒）です。

L3 Unicast Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は L3 Unicast Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは Indirect です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

L3 Unicast Group Entry Naming Conversion

フィールド	Bits	説明
ID	0-27	本タイプのグループエントリを区別するためのインデックス値です。
Kind	28-31	2（L3 ユニキャスト）

L3 Unicast Group Entry Bucket Actions

フィールド	説明
Group	このフィールドはレイヤ 2 インタフェースグループエントリに紐づく必要があります。
Decremented TTL	デクリメント TTL です。 注意 不正な TTL の検証はサポートされていません。
Set-Field	ETH_DST、ETH_SRC、VLAN_VID フィールドを設定します（オプション）。

L3 Unicast Group Entry Counters

フィールド	説明
Reference Count（Flow Entries）	現在このグループエントリを参照しているフローエントリまたはグループエントリの数です。
Duration（Seconds）	グループエントリがセットされてから経過した時間（秒）です。

L3 ECMP Group Entry Type

フィールド	説明
Group Identifier	32 ビットの符号なし整数で、OpenFlow のグループを一意に識別します。命名規則は L3 ECMP Group Entry Naming Conversion テーブルの通りです。
Group Type	グループのタイプは Select です。
Counters	グループ毎のエントリカウンタを指定します。
Action Buckets	単一のアクションバケットがサポートされます。

L3 ECMP Group Entry Naming Conversion

フィールド	Bits	説明
ID	0-27	レイヤ 3 ECMP グループエントリを区別するために使用されます。
Kind	28-31	7（L3 ECMP）

L3 ECMP Group Entry Bucket Actions

フィールド	説明
Group	レイヤ 3 ユニキャストグループエントリに紐付きます。

L3 ECMP Group Entry Counters

フィールド	説明
Reference Count（Flow Entries）	現在このグループエントリを参照しているフローエントリまたはグループエントリの数です。
Duration（Seconds）	グループエントリがセットされてから経過した時間（秒）です。

Meter Table（メーターテーブル）

Meter Table Entry Parameters

フィールド	説明
Meter Identifier	メーターインスタンスです。
Flags	ビット位置です。 • 0：Kbps（Kbps」と「Packets」は同時に使用できません） • 1：Packets（Kbps」と「Packets」は同時に使用できません） • 2：Burst（必須） • 3：Stats（サポートされていません）
Meter Bands	1 つのメーター帯域のみサポートされています。
Counters	メーター毎のエントリカウンタを指定します。

Meter Entry Counters

フィールド	説明
Flow Count	現在このメーターテーブルエントリを参照しているフローエントリ数です。
Input Packet Count	サポートされていません。
Input Byte Count	サポートされていません。
Duration（Seconds）	メーターテーブルエントリがセットされてから経過した時間（秒）です。

Meter Band Configuration Parameters

フィールド	説明
Band Type	帯域のタイプは Drop のみサポートされています。
Rate	メーター帯域が選択される際に使用されます。帯域に適用される最小値のレートを定義します。
Burst	メーター帯域の粒度を定義します。
Counters	サポートされていません。

付録 E RADIUS 属性割り当て

本スイッチの RADIUS 属性割り当てが次のモジュールに使用されます。
「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」

RADIUS 属性タイプ：
- 特権レベル
- イングレス / イーグレス帯域幅
- 802.1p 初期値優先度
- VLAN
- ACL

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。以下は帯域幅のパラメータを表しています。

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	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特権レベル（RADIUS サーバによる）を割り当てます。しかしながら、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いかなる特権レベルも割り当てません。特権レベルは、最小サポート値よりも小さく、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。

RADIUS サーバにより Ingress/Egress 帯域を割り当てるには、正しいパラメータが RADIUS サーバに設定されている必要があります。以下に、帯域のパラメータを示します。

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	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、MAC ベースアクセスコントロール、WAC 認証に成功した場合、デバイスはポートへ帯域（RADIUS サーバによる）を割り当てます。しかしながら、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、ポートにいかなる帯域も割り当てません。帯域属性が RADIUS サーバ上で "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、帯域が "0" より小さいもしく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。

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、正しいパラメータが RADIUS サーバに設定されている必要があります。以下に、802.1p デフォルトプライオリティのパラメータを示します。

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	4	必須
Attribute-Specific Field	802.1p 初期値優先度の割り当に使用します。	0-7	必須

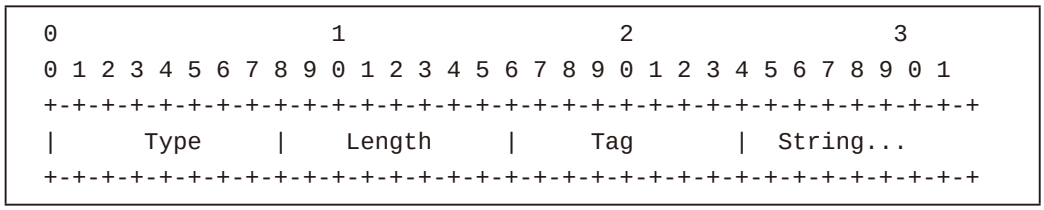
ユーザは、RADIUS サーバの 802.1p 優先度属性（例えば、優先度 7）を設定し、802.1X、MAC ベースアクセスコントロール、WAC 認証に成功した場合、デバイスはポートに 802.1p デフォルト優先度（RADIUS サーバによる）を割り当てます。しかしながら、ユーザが優先度属性を設定せず、認証が成功した場合、デバイスは、このポートにプライオリティを割り当てません。RADIUS サーバで設定された優先度属性が、範囲外の値（> 7）である場合、デバイスに設定しません。

RADIUS サーバにより VLAN を割り当てるには、正しいパラメータが 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、使用される（トンネルイニシエータの場合）トンネリングプロトコルもしくは、使用中の（トンネルターミネータの場合）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（異なる RFC 2868 の）

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）
他 (0x00, 0x03 ~ 0x1F, >0x1F)	スイッチが VLAN の設定文字列を受信するとき、まずはじめに VLAN ID と考えます。つまり、スイッチはすべての存在している 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 名だと考え、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。

ユーザが設定された RADIUS サーバの VLAN 属性（VID3 など）を持ち、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。しかしながら、ユーザが VLAN 属性を設定していない場合、ポートはゲスト 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。

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。以下は ACL のパラメータを表します。

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	14 (ACL スクリプト)	必須

ベンダ指定属性	説明	値	使用法
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

ユーザは RADIUS サーバの ACL 属性を設定（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; など）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 サーバーによる ACL スクリプトを割り当てます。アクセスコンフィグモードに移行したり、出たりすることは対である必要があります。そうでなければ、ACP スクリプトは拒否されます。

付録 F 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）属性は、特定の認証、承認、情報、リクエストとリプライに対する設定詳細を実行します。本付録は現在スイッチによりサポートされる RADIUS 属性一覧です。

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 は、ベンダが、追加で自身の RADIUS 属性を作成することを許可します。D-Link VSA についてのより詳しい情報は、下記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、トンネルプロトコルサポートに対する RFC2868 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た 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

ナンバー	IETF 属性
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 G 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-3630

Traffic Segmentation（トラフィックセグメンテーション）

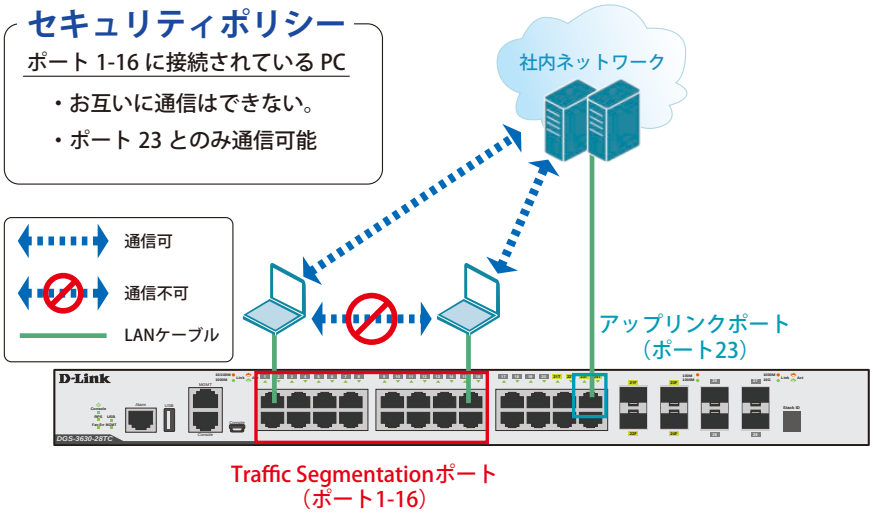


図 20-1　Traffic Segmentation（DGS-3630-28TC）

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

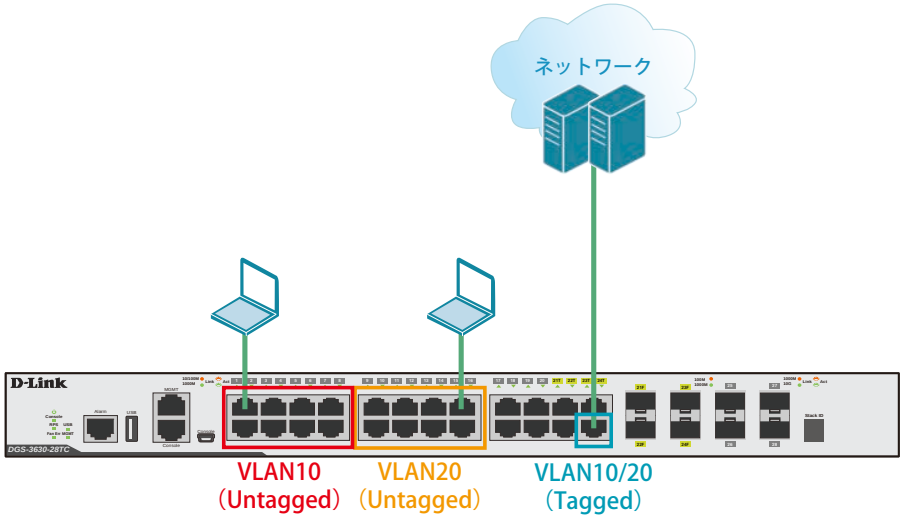


図 20-2 VLAN（DGS-3630-28TC）

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）

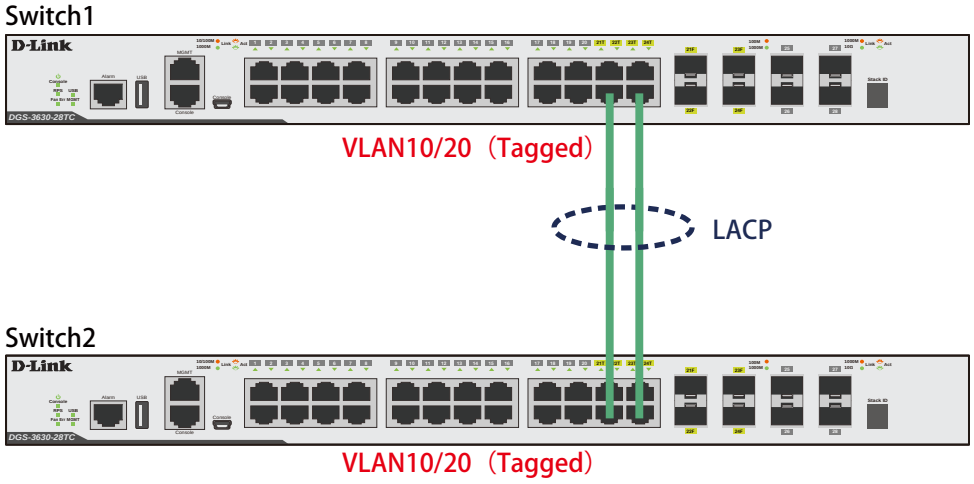


図 20-3 Link Aggregation（DGS-3630-28TC）

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）

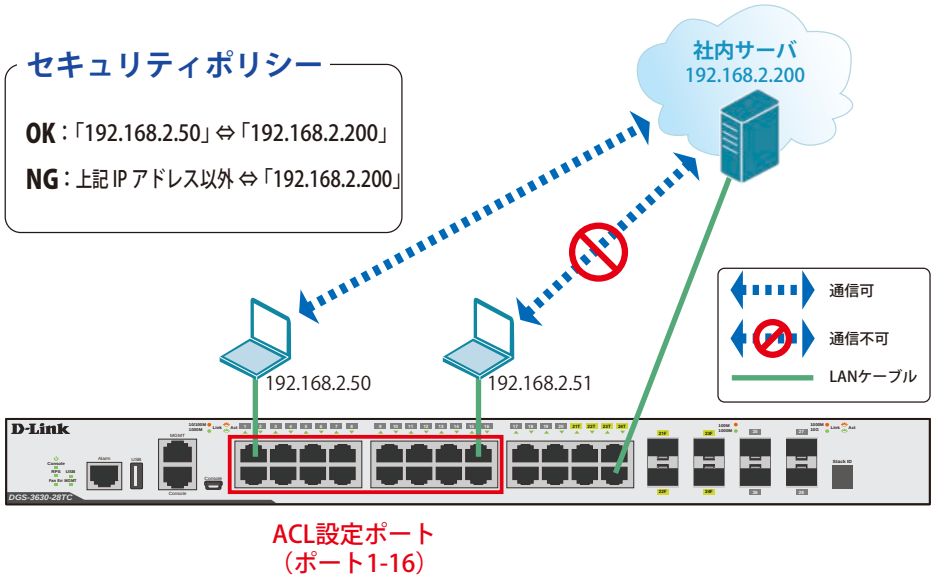


図 20-4　Access List（DGS-3630-28TC）

概要

ポート 1~16 に対し、アクセスリストを設定します。ポート 1~16 に接続される端末の IP の中から、「192.168.2.50」の端末から社内サーバ（192.168.2.200）へのアクセスは許可し、それ以外の端末から社内サーバへのアクセスは禁止するように設定します。

設定手順

1. アクセスリストに名前（extended ACL）を付けて定義します。
   「192.168.2.50 ⇔ 192.168.2.200」間の通信を許可するルールを追加します。
   「192.168.2.200」へのすべての通信を拒否するルールを追加します。

```
Switch#configure terminal
Switch(config)#ip access-list extended ACL
Switch(config-ip-ext-acl)#permit 192.168.2.50 0.0.0.0 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#deny any 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#end
```

2. アクセスリストのルールを、適用対象ポート 1 ～ 16 へ設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#ip access-group ACL in
Switch(config-if-range)#end
```

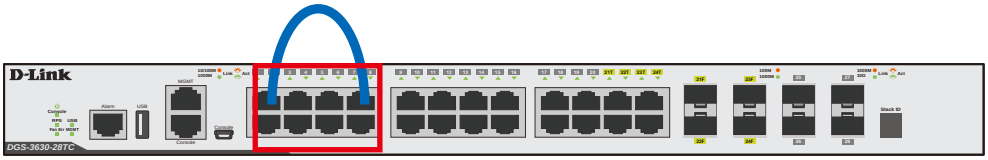
3. 設定を保存します。

```
Switch#copy running-config startup-config
```

4. 情報確認

```
Switch#show access-list
Switch#show access-list ip
Switch#show access-group
```

Loopback Detection（LBD）（ループ検知）



ループを検知したPortをシャットダウンします。
（ポート1-8）

図 20-5 Loopback Detection（DGS-3630-28TC）

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。）