D-Link DXS-3610 シリーズ

10 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、傷害または物的損害が発生するおそれがあります。

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

⚠危険

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

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

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

VCCI - A

ご使用上の注意

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

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

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

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

ラック搭載型製品に関する一般的な注意事項

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

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

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

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

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

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

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

安全にお使いいただくために

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

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

注意 製品に貼られているラベルや「Warranty Void Sticker」(シール) をはがさないでください。はがしてしまうとサポートを受けられなくなります。

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

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

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

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

目次

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

はじめに 16

本マニュアルの対象者 18
表記規則について 18
製品名 / 品番一覧 18

第 1 章　本製品のご使用にあたって 19

DXS-3610 シリーズについて 19
搭載ポート 20
前面パネル 21
　LED 表示 22
背面パネル 24
　LED 表示 24
側面パネル 25

第 2 章　スイッチの設置 26

パッケージの内容 26
ネットワーク接続前の準備 26
ゴム足の取り付け (19 インチラックに設置しない場合) 27
19 インチラックへの取り付け 27
QSFP28/SFP+ スロットへのモジュールの取り付け 29
電源スロットへの AC 電源モジュールの取り付け 30
ファンスロットへのファンモジュールの取り付け 31
スマートファンについて 31

第 3 章　スイッチの接続 32

エンドノードと接続する 32
ハブまたはスイッチと接続する 32
バックボーンまたはサーバと接続する 33
Stacking（スタッキング設定） 34

第 4 章　スイッチ管理について 36

Web GUI による管理 36
SNMP による管理 36
CLI による管理 36
　端末をコンソールポートに接続する 36
　ユーザアカウント / パスワードの設定 37
　IP アドレスの割り当て 38
管理ポートへの接続 38

第 5 章　Web ベースのスイッチ管理 39

Web ベースの管理について 39
Web マネージャへのログイン 39
Web マネージャの画面構成 40
　Web マネージャのメイン画面について 40
Web マネージャのメニュー構成 41

第 6 章　System（スイッチの主な設定） 46

Device Information（デバイス情報） 47
System Information Settings（システム情報設定 ） 48
Peripheral Settings（環境設定） 49
Port Configuration（ポート設定） 50
　Port Settings（スイッチのポート設定） 50
　Port Status（ポートステータス） 52
　Port GBIC 52
　Port Auto Negotiation（オートネゴシエーション） 53
　Error Disable Settings（エラーによるポートの無効） 53
　Jumbo Frame（ジャンボフレームの有効化） 54
　Interface Breakout（インタフェースブレイクアウト） 54

Interface Description（インタフェース概要）.....55
Loopback Test（ループバックテスト）.....55
System Log（システムログ構成）.....56
System Log Settings（システムログ設定）.....56
System Log Discriminator Settings（システムログディスクリミネータ設定）.....57
System Log Server Settings（システムログサーバの設定）.....58
System Log（Syslog ログ）.....59
System Attack Log（システムアタックログ）.....59
Time and SNTP（時刻設定）.....60
Clock Settings（時間設定）.....60
Time Zone Settings（タイムゾーン設定）.....60
SNTP Settings（SNTP 設定）.....62
Time Range（タイムレンジ設定）.....63
PTP（PTP 設定）.....64
PTP Global Settings（PTP グローバル設定）.....64
PTP Port Global Settings（PTP ポートグローバル設定）.....65
PTP Boundary Port Settings（PTP 境界ポート設定）.....66
PTP P2P Transparent Port Settings（PTP P2P 透過ポート設定）.....67
PTP Clock Information（PTP クロック情報の表示）.....67
PTP Port Information (PTP ポート情報).....68
PTP Foreign Master Records Port Information（PTP 外部マスタレコードのポート情報）.....68
SRM（Switch Resource Management 設定）.....69
SRM Prefer Current Settings（SRM 最適化設定）.....69
SRM Prefer Mode（SRM 設定モード）.....70

第 7 章　Management（スイッチの管理）　71

Command Logging（コマンドログ設定）.....72
User Accounts Settings（ユーザアカウント設定）.....72
Password Encryption（パスワード暗号化）.....74
Password Recovery（パスワードリカバリ）.....74
Login Method（ログイン方法）.....75
SNMP（SNMP 設定）.....76
トラップ.....76
MIB.....76
SNMP Global Settings（SNMP グローバル設定）.....77
SNMP Linkchange Trap Settings（SNMP リンクチェンジトラップ設定）.....78
SNMP View Table Settings（SNMP ビューテーブル設定）.....78
SNMP Community Table Settings（SNMP コミュニティテーブル設定）.....79
SNMP Group Table Settings（SNMP グループテーブル）.....80
SNMP Engine ID Local Settings（SNMP エンジン ID ローカル設定）.....81
SNMP User Table Settings（SNMP ユーザテーブル設定）.....81
SNMP Host Table Settings（SNMP ホストテーブル設定）.....82
SNMP Context Mapping Table Settings（SNMP コンテキストマッピングテーブル設定）.....83
RMON（RMON 設定）.....84
RMON Global Settings（RMON グローバル設定）.....84
RMON Statistics Settings（RMON 統計情報）.....84
RMON History Settings（RMON ヒストリ設定）.....85
RMON Alarm Settings（RMON アラーム設定）.....86
RMON Event Settings（RMON イベント設定）.....87
Telnet/Web（Telnet/Web 設定）.....88
Session Timeout（セッションタイムアウト）.....89
DHCP（DHCP 設定）.....90
Service DHCP（DHCP サービス）.....90
DHCP Class Settings（DHCP クラス設定）.....90
DHCP Pool Settings（DHCP プール設定）.....91
DHCP Server（DHCP サーバ）.....92
DHCPv6 Server（DHCPv6 サーバ設定）.....98
DHCP Relay（DHCP リレー）.....103
DHCPv6 Relay（DHCPv6 リレー）.....110
DHCP Auto Configuration（DHCP 自動コンフィグ設定）.....116
DHCP Auto Image Settings（DHCP 自動イメージ設定）.....117
DNS（ドメインネームシステム）.....118
DNS Global Settings（DNS グローバル設定）.....118
DNS Name Server Settings（DNS ネームサーバ設定）.....119
DNS Host Settings（DNS ホスト名設定）.....119

IP Source Interface（IP ソースインタフェース）.....120
File System（ファイルシステム設定）.....121
Stacking（スタッキング設定）.....123
Physical Stacking（物理スタッキング）.....126
Stacking Bandwidth（スタッキング帯域）.....127
シングル IP マネジメント（SIM）設定.....128
シングル IP マネジメント（SIM）の概要.....128
シングル IP マネジメント（SIM）のルールと動作.....128
バージョン 1.61 へのアップグレード.....129
Single IP Settings（シングル IP 設定）.....130
Topology（トポロジ）.....131
Firmware Upgrade（ファームウェア更新）.....134
Configuration File Backup/ Restore（コンフィグレーションファイルのバックアップ / リストア）.....135
Upload Log File（ログファイルのアップロード）.....135
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）.....136
DDP Settings.....136
DDP Neighbors（DDP 隣接機器）.....136
SMTP Settings（SMTP 設定）.....137
Reboot Schedule Settings（再起動スケジュール設定）.....138
NLB FDB Settings（NLB FDB 設定）.....139

第 8 章　L2 Features（L2 機能の設定）　140

FDB（FDB 設定）.....141
Static FDB（スタティック FDB の設定）.....141
MAC Address Table Settings（MAC アドレステーブル設定）.....142
MAC Address Table（MAC アドレステーブル）.....144
MAC Notification（MAC 通知）.....145
VLAN（VLAN 設定）.....146
VLAN Configuration Wizard（VLAN 設定ウィザード）.....146
802.1Q VLAN（802.1Q VLAN）.....147
VLAN Interface（VLAN インタフェース）.....148
802.1v Protocol VLAN（802.1v プロトコル VLAN）.....154
GVRP（GVRP の設定）.....155
MVRP（MVRP の設定）.....158
Asymmetric VLAN（Asymmetric VLAN 設定）.....159
MAC VLAN（MAC VLAN 設定）.....160
L2VLAN Interface Description（L2VLAN インタフェース概要）.....160
Subnet VLAN（サブネット VLAN）.....161
Super VLAN（Super VLAN 設定）.....161
Auto Surveillance VLAN（自動サーベイランス VLAN）.....163
Voice VLAN（音声 VLAN）.....165
Private VLAN（プライベート VLAN 設定）.....168
VLAN Tunnel（VLAN トンネル）.....169
Dot1q Tunnel（Dot1q トンネル）.....169
VLAN Mapping（VLAN マッピング）.....171
VLAN Mapping Profile（VLAN マッピングプロファイル）.....172
STP（スパニングツリー設定）.....177
802.1Q-2005 MSTP.....177
802.1D-2004 Rapid STP.....177
ポートの状態遷移.....177
STP Global Settings（STP グローバル設定）.....179
STP Port Settings（STP ポートの設定）.....180
MST Configuration Identification（MST の設定）.....182
STP Instance（STP インタンス設定）.....183
MSTP Port Information（MSTP ポート情報）.....183
ERPS (G.8032)（イーサネットリングプロテクション設定）.....184
ERPS.....184
ERPS Profile（ERPS プロファイル）.....188
Loopback Detection（ループバック検知設定）.....189
Link Aggregation（リンクアグリゲーション）.....190
ポートトランクグループについて.....190
MLAG（マルチシャーシリンクアグリゲーション）.....193
MLAG Settings（MLAG 設定）.....193
MLAG Group（MLAG グループ）.....195

Flex Links（フレックスリンク）.....195
L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）.....196
L2 Multicast Control（L2 マルチキャストコントロール）.....197
IGMP Snooping（IGMP Snooping の設定）.....197
MLD Snooping（MLD スヌーピング）.....204
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）.....226

第 9 章　L3 Features（レイヤ 3 機能の設定）　228

ARP（ARP 設定）.....229
ARP Elevation（ARP エレベーション）.....229
ARP Aging Time（ARP エージングタイム設定）.....229
Static ARP（スタティック ARP 設定）.....230
Proxy ARP（プロキシ ARP）.....231
ARP Table（ARP テーブルの参照）.....231
Gratuitous ARP（Gratuitous ARP 設定）.....232
IPv6 Neighbor（IPv6 ネイバ設定）.....233
Interface（インタフェース設定）.....234
IPv4 Interface（IPv4 インタフェース）.....234
IPv6 Interface（IPv6 インタフェース）.....236
Loopback Interface（ループバックインタフェース設定）.....239
Null Interface（Null インタフェース）.....240
UDP Helper（UDP ヘルパー）.....240
IP Forward Protocol（IP 転送プロトコル）.....240
IP Helper Address（IP ヘルパーアドレス）.....241
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定）.....242
IPv4 Static Route BFD（IPv4 スタティックルート BFD）.....243
IPv4 Route Table（IPv4 ルートテーブル）.....243
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定）.....244
IPv6 Static Route BFD（IPv6 スタティックルート BFD）.....245
IPv6 Route Table（IPv6 ルートテーブル）.....245
Route Preference（ルート優先度設定）.....246
ECMP Settings（ECMP 設定）.....246
IPv6 General Prefix（IPv6 汎用プレフィックス）.....247
IP Tunnel Settings（IP トンネル設定）（EI モードのみ）.....247
URPF Settings（URPF 設定）.....249
VRF（Virtual Routing and Forwarding）（EI モードのみ）.....250
VRF Settings（VRF 設定）.....250
VRF Interface Settings（VRF インタフェース設定）.....252
RIP（Routing Information Protocol）.....253
RIP Settings（RIP 設定）.....253
RIP Distribute List（RIP ディストリビュートリスト）.....255
RIP Interface Settings（RIP インタフェース設定）.....256
RIP Database（RIP データベース）.....257
RIPng（RIPng 設定）.....258
RIPng Settings（RIPng 設定）.....258
RIPng Interface Settings（RIPng インタフェース設定）.....259
RIPng Database（RIPng データベース）.....260
OSPF（OSPF 設定）.....260
OSPFv2（OSPFv2 設定）.....260

OSPFv3 273
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル） 285
IGMP（IGMP 設定）（EI モードのみ） 285
MLD（MLD 設定）（EI モードのみ） 289
IGMP Proxy（IGMP プロキシ）（EI モードのみ） 292
MLD Proxy（MLD プロキシ）（EI モードのみ） 294
DVMRP（EI モードのみ） 296
PIM（PIM 設定）（EI モードのみ） 298
IPMC（IP マルチキャスト設定） 326
IPv6MC（IPv6 マルチキャスト設定） 331
BGP（Border Gateway Protocol）（EI モードのみ） 333
BGP Global Settings（BGP グローバル設定） 333
BGP Aggregate Address Settings（BGP アグリゲートアドレス設定） 335
BGP Network Settings（BGP ネットワーク設定） 336
BGP Route Redistribution Settings（BGP ルート再配布設定） 337
BGP Route Preference Settings（BGP ルート優先設定） 338
BGP Dampening Settings（BGP ダンプニング設定） 339
BGP Dampening Dampened Paths Table（BGP ダンプニングダンプドパステーブル） 340
BGP Dampening Flap Statistics Table（BGP ダンプニングフラップ統計テーブル） 341
BGP Reflector Settings（BGP リフレクタ設定） 342
BGP Confederation Settings（BGP コンフェデレーション設定） 343
BGP AS Path Access List Settings（BGP AS パスアクセスリストリスト設定） 343
BGP Community List Settings（BGP コミュニティリスト設定） 344
BGP Extended Community List Settings（BGP 拡張コミュニティリスト設定） 345
BGP Clear Settings（BGP クリア設定） 346
BGP Summary Table（BGP サマリテーブル） 347
BGP Routing Table（BGP ルーティングテーブル） 347
BGP Labels Table（BGP ラベルテーブル） 349
BGP Neighbor（BGP ネイバ設定） 350
BFD（Bidirectional Forwarding Detection） 360
BFD Settings（BFD 設定） 360
BFD Neighbor Table（BFD ネイバテーブル） 361
ISIS（Intermediate System to Intermediate System）（EI モードのみ） 362
ISIS Global Settings（ISIS グローバル設定） 362
ISIS Router Settings（ISIS ルータ設定） 366
ISIS Interface Settings（ISIS インタフェース設定） 368
ISIS Redistribute Settings（ISIS 再配布設定） 370
ISIS Redistribute ISIS Settings（ISIS 再配布 ISIS 設定） 371
ISIS Route Table（ISIS ルートテーブル） 371
ISIS Database（ISIS データベース） 372
ISIS Topology（ISIS トポロジ） 373
ISIS Hostname（ISIS ホスト名） 373
ISIS Neighbors（ISIS ネイバ） 374
IP Route Filter（IP ルートフィルタ） 375
IP Prefix List（IP プレフィックスリスト設定）（EI モードのみ） 375
Route Map（ルートマップ設定） 376
Policy Route（ポリシールート設定） 379
VRRP（VRRP 設定） 380
VRRPv3 Settings（VRRPv3 設定） 382

第 10 章　QoS（QoS 機能の設定） 384

Basic Settings（基本設定） 385
Port Default CoS（ポートデフォルト CoS 設定） 385
Port Scheduler Method（ポートスケジューラメソッド設定） 385
Queue Settings（QoS 設定） 386
CoS to Queue Mapping（CoS キューマッピング設定） 387
Port Rate Limiting（ポートレート制限設定） 387
Queue Rate Limiting（キューレート制限設定） 388
Advanced Settings（アドバンス設定） 389
DSCP Mutation Map（DSCP 変更マップ設定） 389
Port Trust State and Mutation Binding（ポートトラスト設定 & 変更マップバインディング） 389
DSCP CoS Mapping（DSCP CoS マップ設定） 390
CoS Color Mapping（CoS カラーマップ設定） 390
DSCP Color Mapping（DSCP カラーマップ設定） 391
Class Map（クラスマップ設定） 391
Aggregate Policer（アグリゲートポリサー設定） 393
Policy Map（ポリシーマップ設定） 395

Policy Binding（ポリシーバインディング設定）.....397
QoS PFC.....398
Network QoS Class Map（ネットワーク QoS クラスマップ）.....398
Network QoS Policy Map（ネットワーク QoS ポリシーマップ）.....399
Network QoS Policy Binding（ネットワーク QoS ポリシーバインディング）.....400
PFC Port Settings（PFC ポート設定）.....401
WRED（WRED 設定）.....402
WRED Profile（WRED プロファイル設定）.....402
WRED Queue（WRED キュー設定）.....403
WRED Drop Counter（WRED ドロップカウンタ設定）.....404
iSCSI（アイスカジー）.....405
iSCSI Settings（アイスカジー設定）.....405
iSCSI Sessions（アイスカジーセッション）.....406

第 11 章　ACL（ACL 機能の設定）　407

ACL Configuration Wizard（ACL 設定ウィザード）.....408
ACL Configuration Wizard（ACL 設定ウィザードの開始）.....408
パケットタイプ選択（ACL 設定ウィザード）.....409
ルール追加（ACL 設定ウィザード）.....409
ポート設定（ACL 設定ウィザード）.....418
ACL Access List（ACL アクセスリスト）.....419
Standard IP ACL（通常 IP ACL）.....421
Extended IP ACL（拡張 IP ACL）.....422
Standard IPv6 ACL（通常 IPv6 ACL）.....424
Extended IPv6 ACL（拡張 IPv6 ACL）.....425
Extended MAC ACL（拡張 MAC ACL）.....427
Extended Expert ACL（拡張詳細 ACL）.....428
ACL Interface Access Group（ACL インタフェースアクセスグループ）.....431
ACL VLAN Access Map（ACL VLAN アクセスマップ）.....432
Match Access-List（照合アクセスリスト設定）.....433
ACL VLAN Filter（ACL VLAN フィルタ設定）.....434
CPU ACL（CPU ACL 設定）.....435

第 12 章　Security（セキュリティ機能の設定）　437

Port Security（ポートセキュリティ）.....438
Port Security Global Settings（ポートセキュリティグローバル設定）.....438
Port Security Port Settings（ポートセキュリティポート設定）.....439
Port Security Address Entries（ポートセキュリティアドレスエントリ設定）.....440
802.1X（802.1X 設定）.....441
802.1X Global Settings（802.1X グローバル設定）.....445
802.1X Port Settings（802.1X ポート設定）.....445
Authentication Session Information（認証セッションの状態）.....446
Authenticator Statistics（オーセンティケータ統計情報）.....446
Authenticator Session Statistics（オーセンティケータセッション統計情報）.....447
Authenticator Diagnostics（オーセンティケータ診断）.....447
AAA（AAA 設定）.....448
AAA Global Settings（AAA グローバル設定）.....448
Application Authentication Settings（アプリケーションの認証設定）.....449
Application Accounting Settings（アプリケーションアカウント設定）.....450
Authentication Settings（認証設定）.....451
Accounting Settings（アカウンティング設定）.....453
RADIUS（RADIUS 設定）.....455
RADIUS Global Settings（RADIUS グローバル設定）.....455
RADIUS Server Settings（RADIUS サーバの設定）.....456
RADIUS Group Server Settings（RADIUS グループサーバの設定）.....457
RADIUS Statistic（RADIUS 統計情報）.....458
TACACS+（TACACS+ 設定）.....459
TACACS+ Global Settings（TACACS+ サーバグローバル設定）.....459
TACACS+ Server Settings（TACACS+ サーバの設定）.....460
TACACS+ Group Server Settings（TACACS+ グループサーバの設定）.....460
TACACS+ Statistic（TACACS+ 統計情報）.....461
IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）.....462
IPv4.....462
IPv6.....473
DHCP Server Screening（DHCP サーバスクリーニング設定）.....479
DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）.....479

DHCP Server Screening Port Settings（DHCP サーバスクリーニングポート設定）....480
ARP Spoofing Prevention（ARP スプーフィング防止設定）....481
BPDU Attack Protection（BPDU アタック防止設定）....482
NetBIOS Filtering（NetBIOS フィルタリング設定）....483
MAC Authentication（MAC 認証）....484
Web-based Access Control（Web 認証）....485
Web Authentication（Web 認証設定）....487
WAC Port Settings（Web 認証ポート設定）....488
WAC Customize Page（WAC カスタマイズページ設定）....488
Network Access Authentication（ネットワークアクセス認証）....489
Guest VLAN（ゲスト VLAN 設定）....489
Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）....489
Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）....491
Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）....492
Safeguard Engine（セーフガードエンジン）....493
Safeguard Engine Settings（セーフガードエンジン設定）....494
CPU Protect Counters（CPU プロテクトカウンタ）....494
CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）....495
CPU Protect Type（CPU プロテクトタイプ）....495
Trusted Host（トラストホスト）....496
Traffic Segmentation（トラフィックセグメンテーション）....496
Storm Control Settings（ストームコントロール設定）....497
DoS Attack Prevention Settings（DoS 攻撃防止設定）....499
SSH（Secure Shell）....500
SSH Global Settings（SSH グローバル設定）....500
Host Key（Host Key 設定）....501
SSH Server Connection（SSH サーバ接続）....502
SSH User Settings（SSH ユーザ設定）....502
SSL（Secure Socket Layer）....503
SSL Global Settings（SSL グローバル設定）....504
Crypto PKI Trustpoint（暗号 PKI トラストポイント）....505
SSL Service Policy（SSL サービスポリシー）....506
SFTP Server Settings（SFTP サーバ設定）....507
Network Protocol Port Protect Settings（ネットワークプロトコルポート保護設定）....507

第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)　508

CFM（Connectivity Fault Management : 接続性障害管理）....509
CFM Settings（CFM 設定）....509
CFM Port Settings（CFM ポート設定）....516
CFM Loopback Test（CFM ループバックテスト）....517
CFM Linktrace Settings（CFM リンクトレース設定）....518
CFM Packet Counter（CFM パケットカウンタ）....519
CFM Counter CCM（CFM カウンタ CCM）....519
CFM MIP CCM Table（CFM MIP CCM テーブル）....520
CFM MEP Fault Table（CFM MEP 障害テーブル）....520
Cable Diagnostics（ケーブル診断機能）....521
Ethernet OAM（イーサネット OAM）....522
Ethernet OAM Settings（イーサネット OAM 設定）....522
Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）....523
Ethernet OAM Event Log Table（イーサネット OAM イベントログテーブル）....524
Ethernet OAM Statistics Table（イーサネット OAM 統計情報テーブル）....525
Ethernet OAM DULD Settings（イーサネット OAM DULD 設定）....526
DDM（DDM 設定）....527
DDM Settings（DDM 設定）....527
DDM Temperature Threshold Settings（DDM 温度しきい値設定）....528
DDM Voltage Threshold Settings（DDM 電圧しきい値設定）....528
DDM Bias Current Threshold Settings（DDM バイアス電流しきい値設定）....529
DDM TX Power Threshold Settings（DDM 送信電力しきい値設定）....529
DDM RX Power Threshold Settings（DDM 受信電力しきい値設定）....530
DDM Status Table（DDM ステータステーブル）....530

第 14 章　MPLS（EI モードのみ） 531

MPLS LDP Information Settings（MPLS LDP 情報設定） 532
MPLS LSP Trigger Information（MPLS LSP トリガ情報） 534
MPLS Forwarding Settings（MPLS フォワーディング設定） 535
MPLS LDP Neighbor Password Settings（MPLS LDP ネイバパスワード設定） 536
MPLS LDP Neighbor Targeted Settings（MPLS LDP ネイバターゲット設定） 537
MPLS LDP Neighbor Information（MPLS LDP ネイバ情報） 537
MPLS Global Settings（MPLS グローバル設定） 538
MPLS LDP Interface Settings（MPLS LDP インタフェース設定） 539
MPLS LDP Session Information（MPLS LDP セッション情報） 540
MPLS LDP Statistic（MPLS LDP スタティスティック） 541
MPLS LDP Binding Table（MPLS LDP バインディングテーブル） 541
MPLS LDP Discovery Information（MPLS LDP ディスカバリ情報） 542
MPLS QoS Settings（MPLS QoS 設定） 543
Ping MPLS 546
Traceroute MPLS IPv4（トレースルート MPLS IPv4） 547

第 15 章　MPLS L2VPN（EI モードのみ） 548

VPWS Settings（VPWS 設定） 549
L2VC Interface Description（L2VC インタフェース概要） 551
VPLS Settings（VPLS 設定） 552
VPLS MAC Address Table（VPLS MAC アドレステーブル） 556

第 16 章　Monitoring（スイッチのモニタリング） 557

VLAN Counter（VLAN カウンタ） 558
Utilization（利用分析） 559
　Port Utilization（ポート使用率） 559
　History Utilization（使用履歴） 560
Statistics（統計情報） 561
　Port（ポート統計情報） 561
　CPU Port（CPU ポート） 562
　Interface Counters（インタフェースカウンタ） 563
　Interface History Counters（インタフェースカウント履歴） 564
　Counters（カウンタ） 565
Mirror Settings（ミラー設定） 567
sFlow（sFlow 設定） 568
　sFlow Agent Information（sFlow エージェント情報） 568
　sFlow Receiver Settings（sFlow レシーバ設定） 568
　sFlow Sampler Settings（sFlow サンプラ設定） 569
　sFlow Poller Settings（sFlow ポーラ設定） 570
Device Environment（機器環境確認） 570

第 17 章　Green（省電力機能） 571

Power Saving（省電力） 572
EEE（Energy Efficient Ethernet/ 省電力イーサネット） 573

第 18 章　OpenFlow 574

OpenFlow Settings（OpenFlow 設定） 575

第 19 章　Save and Tools（Save メニュー /Tools メニュー） 577

Save（Save メニュー） 578
　Save Configuration（コンフィグレーションの保存） 578
Tools（Tools メニュー） 578
　Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ） 578
　Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ） 582
　Certificate & Key Restore & Backup（証明書 / 鍵リストア＆バックアップ） 587
　Log Backup（ログファイルのバックアップ） 591
　Ping 593
　Trace Route（トレースルート） 595
　Reset（リセット） 597
　Reboot System（システム再起動） 597
　DLMS Settings（DLMS 設定） 598

付録 599

付録 A パスワードリカバリ手順 599
付録 B システムログエントリ 600
付録 C トラップログエントリ 632
付録 D RADIUS 属性割り当て 643
付録 E IETF RADIUS 属性サポート 645
付録 F 機能設定例 647
対象機器について 647
Traffic Segmentation（トラフィックセグメンテーション） 647
VLAN 648
Link Aggregation（リンクアグリゲーション） 649
Access List（アクセスリスト） 651
Loopback Detection（LBD）（ループ検知） 652

はじめに

DXS-3610 シリーズユーザマニュアルは、シリーズの設置方法および操作方法について記載しています。

- 第 1 章　本製品のご使用にあたって
  - 本スイッチの概要とその機能について説明します。また、前面、背面、側面の各パネルと LED 表示について説明します。
- 第 2 章　スイッチの設置
  - スイッチの設置方法、電源接続の方法について説明します。
- 第 3 章　スイッチの接続
  - スイッチをご使用のネットワークに接続する方法を説明します。
- 第 4 章　スイッチ管理について
  - パスワード設定、SNMP 設定、および各種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、システムログ設定、時刻設定などの基本機能の設定について説明します。
- 第 7 章　Management（スイッチの管理）
  - ユーザアカウント、シングル IP マネジメント設定、SNMP 設定、Telnet 設定、Web 設定などの管理機能について説明します。
- 第 8 章　L2 Features（L2 機能の設定）
  - VLAN、リンクアグリゲーション、スパニングツリー、LLDP などのレイヤ 2 機能について説明します。
- 第 9 章　L3 Features（レイヤ 3 機能の設定）
  - ARP 設定、インタフェース設定、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 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、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、ケーブル診断機能について説明します。
- 第 14 章　MPLS（EI モードのみ）
  - 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（EI モードのみ）
  - 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、パケットのエラーやパケットサイズなどの統計情報、ミラーリング、sFlow などのモニタ機能について説明します。
- 第 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

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

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、使用にあたっての注意事項について説明します。

警告 警告では、ネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

補足 補足では、特長や技術についての詳細情報について説明します。

参照 参照では、別項目での説明へ誘導します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

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

製品名 / 品番一覧

製品名	HW バージョン	区分	品番
DXS-3610-54T	A1	SI 版	DXS-3610-54TSI/A1
	A1	EI 版	DXS-3610-54TEI/A1
DXS-3610-54S	A1	SI 版	DXS-3610-54SSI/A1
	A1	EI 版	DXS-3610-54SEI/A1

第 1 章　本製品のご使用にあたって

- DXS-3610 シリーズについて
- 搭載ポート
- 前面パネル
- 背面パネル
- 側面パネル

DXS-3610 シリーズについて

DXS-3610 シリーズは、10G イーサネットスイッチングとルーティングを備えた、低遅延かつ高パフォーマンスなレイヤ 3 スタッカブル 10G マネージドスイッチです。1U サイズ・前面から背面へのエアフロー設計で、エンタープライズやキャンパスなどの集約ネットワーク環境に適しています。DXS-3610-54T には 1000/10G Base-T ポート× 48 と 100G QSFP28 スロット× 6、DXS-3610-54S には 10G SFP+ スロット× 48 と 100G QSFP28 スロット× 6 が搭載されています。システム要件に応じて、100G スロットをアップリンクまたはスタッキングに設定することが可能です。

高いパフォーマンスと高可用性

DXS-3610 シリーズは、100G アップリンクポート× 6 を搭載し、最大 1607Mpps の転送レート、最大 2.16Tbps のスイッチング容量を持つ高性能 10G レイヤ 3 スイッチです。また、ホットスワップ対応のモジュラー式電源とファントレイが搭載されており、冗長性の高い高可用性アーキテクチャを提供します。100G ポートを使用して、最大 12 台までの物理スタックを最大 1200Gbps の帯域で構築することも可能です。

ニーズに合わせたライセンス選択

本シリーズには、エンハンスドイメージ（EI）とスタンダードイメージ（SI）のライセンスが用意されており、必要な機能に応じていずれかのライセンスを選択することが可能です。EI ライセンスは SI ライセンス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ります。EI 版では、IGMP、MLD、PIM-DM/SM/SDM/SSM、DVMRP などの L3 マルチキャスト機能や BGP のほか、L2/L3MPLS VPN をサポートしています。

多様な管理機能 / オープンアーキテクチャ

Web GUI、CLI による管理のほか、SNMP による集中管理を行うことが可能です。IEEE802.3ah（リンク OAM）、CFM などの障害切り分けを容易にするサポート機能等も充実しています。SRM（Resource Management）機能を使用すると、モードに応じてテーブルサイズを調整できるため、スイッチの使用目的によりスイッチ機能を最適化できます。

充実したセキュリティ機能と冗長性

本シリーズは、RADIUS を介した 802.1X ユーザ認証や、ACL を含む充実したセキュリティ機能を提供します。また、GVRP などの多様な VLAN 機能、QoS の設定が可能であり、セキュリティとパフォーマンスの向上を図ることができます。さらに、STP/RSTP/MSTP に加えて、ERPS や FlexLink などの高度なリンク冗長技術もサポートしています。

搭載ポート

DXS-3610 シリーズは以下のポートを搭載しています。

製品名	DXS-3610-54T	DXS-3610-54S
1000/10G BASE-T	48	—
10G SFP+ スロット	—	48
100G QSFP28 スロット	6	
コンソールポート (RJ-45)	1	
管理ポート (MGMT) (RJ-45)	1	
Micro USB ポート (USB2.0)	1	

■ DXS-3610 シリーズスイッチ対応オプションモジュール

本シリーズでサポートされるオプションモジュールは以下の通りです。

光トランシーバ

種別	製品名
QSFP28(100Giga) ※1	DEM-Q2801Q-SR4
	DEM-Q2810Q-LR4
SFP+(10Giga) ※2	DEM-431XT
	DEM-432XT
Copper SFP+（10Giga） ※2	DEM-410T ※3 ※4
WDM 対応 1 芯 SFP(1Giga) ※2	DEM-330T
	DEM-330R
2 芯 SFP(1Giga) ※2	DEM-310GT
	DEM-311GT
Copper SFP(1Giga) ※2	DGS-712

※1 QSFP28 スロットのみで使用可能です。

※2 SFP+ スロットでのみ使用可能です。

※3 DEM-410T を使用する場合、環境温度（室温）が 40℃までの環境での利用のみをサポートします。そのため、この場合のスイッチの動作温度範囲も 0~40℃までとなりますので、十分にご注意ください。

※4 DEM-410T の取り付けは、スイッチ 1 台に対し最大 4 個までとなります。

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

ダイレクトアタッチケーブル

種別	製品名
SFP+ ダイレクトアタッチケーブル	DEM-CB100S
	DEM-CB300S
QSFP28 ダイレクトアタッチケーブル	DEM-CB100Q28

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

前面パネル

スイッチの前面パネルは、以下のコンポーネントで構成されています。

ポート	説明
1000/10G BASE-T ポート（DXS-3610-54T のみ）	1000Mbps または 10Gbps の速度で通信を行う RJ-45 イーサネットポートです。
10 G SFP+ スロット（DXS-3610-54S のみ）	1000Mbps または 10Gbps の速度で通信を行う SFP+ スロットです。
100G QSFP28 スロット	40Gbps または 100Gbps の速度で通信を行う QSFP28 スロットです。
RJ-45 コンソールポート	コマンドラインインタフェース（CLI）に接続し、スイッチの管理を行います。 管理ノードのシリアルポートと通信を行うアウトオブバンド（OOB）ポートです。
RJ-45 管理（MGMT）ポート	コマンドラインインタフェース（CLI）または Web インタフェース（Web UI）に接続し、スイッチの管理を行います。SNMP 通信も本ポートから行うことができます。標準の LAN アダプタとの通信を行うアウトオブバンド（OOB）ポートです。本ポートは 10/100/1000Mbps の速度で通信を行います。
MicroUSB ポート	USB フラッシュドライブを挿入すると、追加のストレージスペースが提供されます。スイッチの NVRAM との間でファームウェアイメージやコンフィグレーションファイルをコピーすることができます。
リセットボタン	スイッチの再起動や、工場出荷時の設定へのリセットを行います。 • 1-4 秒押下 - スイッチを再起動します。保存されていない設定は失われます。 • 5-10 秒押下 - コンフィグレーションを工場出荷時の設定へ戻します。
情報タグ	前面パネル右側には、スライド式の情報タグがあります。スイッチの製品コード、ハードウェアバージョン、シリアル番号、MAC アドレスが記載されています。QR コードをスキャンして、これらの情報を入手することも可能です。
各種 LED	電源、RPS、ファンエラー、コンソール、USB、MGMT、Link/Act/Speed の動作状態を表示します。

DXS-3610-54T

- 1000/10G BASE-T ポート x 48
- 100G QSFP28 スロット x 6
- RJ-45 コンソールポート x 1
- RJ-45 管理（MGMT）ポート x 1
- MicroUSB ポート x 1
- LED：Locator、Power、Status、Fan、Link/Act（各ポート / スロット）
- リセットボタン
- 情報タグ

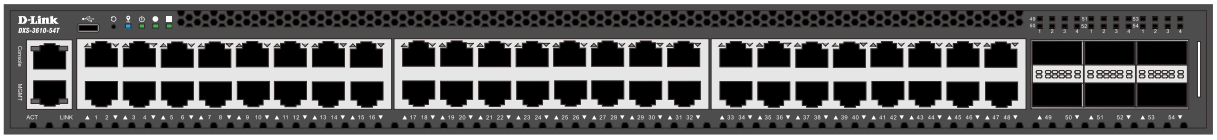


図 3-1　DXS-3610-54T の前面パネル

DXS-3610-54S

- 10G SFP+ スロット x 48
- 100G QSFP28 スロット x 6
- RJ-45 コンソールポート x 1
- RJ-45 管理（MGMT）ポート x 1
- MicroUSB ポート x 1
- LED：Locator、Power、Status、Fan、Link/Act（各ポート / スロット）
- リセットボタン
- 情報タグ

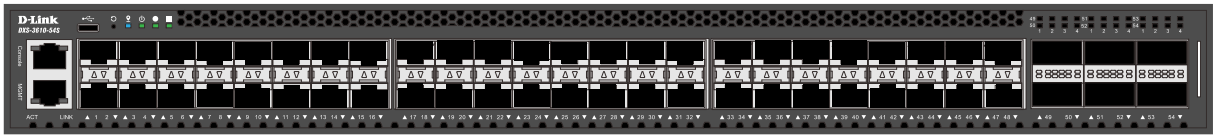


図 3-2　DXS-3610-54S の前面パネル

LED 表示

LED 表示により、スイッチとネットワークの状態を確認することができます。

DXS-3610-54T

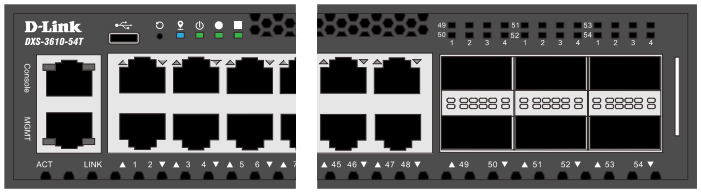


図 3-3　DXS-3610-54T の前面パネル LED 配置図

DXS-3610-54S

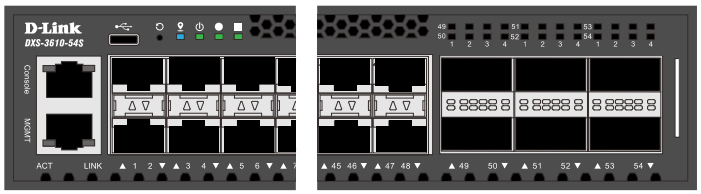


図 3-4　DXS-3610-54S の前面パネル LED 配置図

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。

通常動作時の LED 表示

LED	色	状態	状態説明
システム LED			
Locator	青	点灯	ユーザがログインしています。
	ー	消灯	ロケータ機能が無効です。
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。
		点滅	システム自己診断テストを実行中です。
	橙	点滅	電源に不具合が発生しています。または、電圧 / 電流 / 温度が高すぎます。
	ー	消灯	スイッチに電源が供給されていません。
Status	緑	点灯	POST 処理が完了し、正常に動作しています。
		点滅	POST 処理を実行中です。
	橙	点滅	POST 処理 / 電源 / ファンに不具合が発生しています。または、温度が高すぎます。
	ー	消灯	スイッチに電源が供給されていません。
Fan	緑	点灯	ファンが正常に動作しています。
	橙	点滅	ファンに不具合が発生しています。
	ー	消灯	スイッチに電源が供給されていません。
MGMT	緑	点灯	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。
	ー	消灯	リンクが確立されていない、もしくはポートが無効化されています。
1000/10G 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	リンクが確立されていない、もしくはポートが無効化されています。
SFP+ スロット LED			
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	リンクが確立されていない、もしくはポートが無効化されています。

LED	色	状態	状態説明
QSFP28 スロット LED			
Link/ACT	白（LED 1）	点灯	100Gbps でリンクが確立しています。
		点滅	100Gbps でデータを送受信しています。
	青（LED 4）	点灯	40Gbps でリンクが確立しています。
		点滅	40Gbps でデータを送受信しています。
	ー	消灯	リンクが確立されていない、もしくはポートが無効化されています。
スタック（マスタ）	白（LED 1）	点灯	マスタスイッチにおいて 100Gbps でリンクが確立している場合、LED1 と 2 が同時に点灯します。
	橙（LED 2）	点滅	100Gbps 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。
スタック（スレーブ）	橙（LED 3）	点灯	スレーブスイッチにおいて 100Gbps でリンクが確立している場合、LED3 と 4 が同時に点灯します。
	青（LED 4）	点滅	100Gbps 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。

システム起動時の LED 表示

フェーズ	LED	状態説明
第 1 段階	Locator	LED が青色に点灯します。
	Power	消灯
	Status	消灯
	Fan	消灯
	ポート Link/Act	消灯
第 2 段階	Locator	消灯
	Power	消灯
	Status	消灯
	Fan	消灯
	ポート Link/Act	消灯
第 3 段階	Locator	消灯
	Power	LED が緑色に点灯します。
	Status	LED が緑色に点滅します。
	Fan	LED が緑色に点灯します。
	ポート Link/Act	消灯
第 4 段階	Locator	消灯
	Power	LED が緑色に点灯します。
	Status	LED が緑色に点灯します。
	Fan	LED が緑色に点灯します。
	ポート Link/Act	消灯
システム準備完了	全 LED	通常の LED 動作になります。

背面パネル

DXS-3610-54T/54S の背面パネルには、接地コネクタ、電源モジュールスロット、ファンモジュールスロット、また、各モジュールの状態を表示する LED を搭載しています。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。

DXS-3610-54T/54S

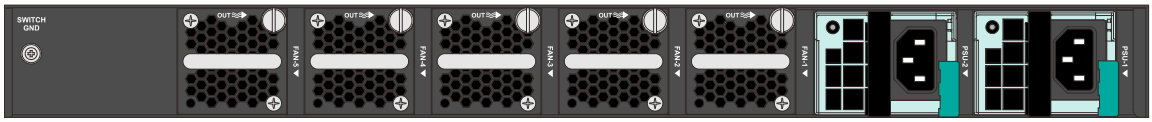


図 3-5　DXS-3610-54T/54S の背面パネル

コンポーネント	説明
スイッチ GND	接地用ケーブルの片側をスイッチ GND に接続し、もう一方をラックなどの接地ポイントに接続します。
ファンモジュールスロット	ホットスワップ可能な 5 つの冗長ファンモジュールスロットが搭載されています。4 つのファンモジュールがアクティブ状態となり、4 つのうちの 1 つがエラーになるまで 5 つ目のファンモジュールは待機状態となります。
電源モジュールスロット	ホットスワップ、負荷分散可能な 2 つの電源モジュールスロットが搭載されています。2 つの電源モジュールが取り付けられている場合、電源が負荷分散されます。 取り付け可能なモジュールは以下の通りです。 • **DXS-PWR700AC** 700W AC パワーサプライトレイ（前面から背面へのエアフロー）

補足　本体ご購入時には、標準で DXS-PWR700AC が 2 つ、ファンモジュールが 5 つ搭載されています。

LED 表示

以下の表に LED の状態が意味するモジュールの状態を示します。

電源 / ファンモジュールの LED 表示

LED	色	状態	状態説明
電源モジュール	緑	点灯	電源が供給され、正常に動作しています。
		点滅	電源は供給されていませんが、5VSB（スタンバイ電源）が動作しています。
	橙	点灯	電源の重大イベントが発生しています。 電源 / ファンエラー、またはシステムのシャットダウンを引き起こす可能性があります。
		点滅	電源の警告イベントが発生しています。 高温 / 高出力 / 高電流や、ファンの低速を引き起こす可能性があります。
		消灯	電源が供給されていません。
ファンモジュール	緑	点灯	ファンが正常に動作しています。
		点滅	ファンに不具合が発生しています。
	ー	消灯	スイッチに電源が供給されていません。

側面パネル

DXS-3610-54T/54S の側面パネルには、ラックマウント用のネジ穴およびネジが配置されています。

DXS-3610-54T/54S

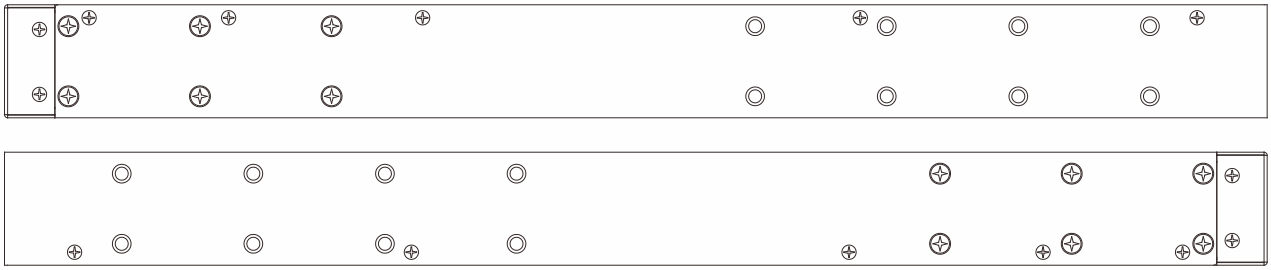


図 3-6　DXS-3610-54T/54S の側面パネル

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
- QSFP28/SFP+ スロットへのモジュールの取り付け
- 電源スロットへの AC 電源モジュールの取り付け
- ファンスロットへのファンモジュールの取り付け
- スマートファンについて

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
- 取り付け済み AC 電源モジュール（DXS-PWR700AC）　x　2
- 取り付け済みファンモジュール　x　5
- AC 電源ケーブル　x　2
- RJ-45/RS232C コンソールケーブル　x　1
- micro-USB/Type-A USB ケーブル　x　1
- ゴム足　x　4
- 19 インチラックマウントキット（ブラケット、ネジ）　x　1
- クイックインストールガイド　x　1
- PL シート　x　1

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

ネットワーク接続前の準備

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

- スイッチは、しっかりとした水平面で耐荷重性のある場所に設置してください。また、スイッチの上に重いものを置かないでください。
- 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本スイッチの周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後 10 cm 以上の空間を保つようにしてください。
- スイッチは動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- スイッチは強い電磁場が発生するような場所（モータの周囲など）や、振動、ほこり、および直射日光を避けて設置してください。
- スイッチを水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

ゴム足の取り付け (19 インチラックに設置しない場合)

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

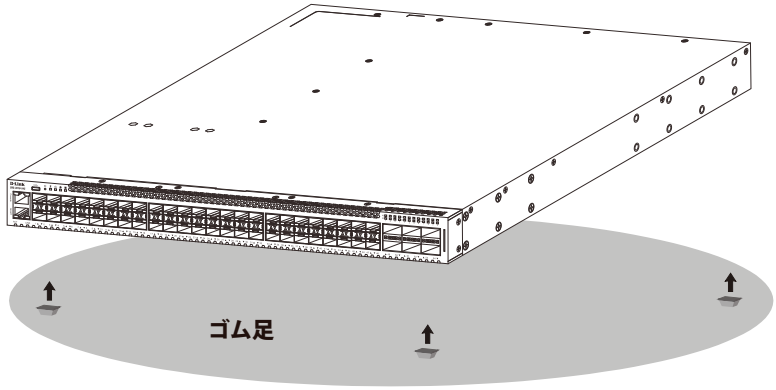


図 2-1　ゴム足の取り付け

19 インチラックへの取り付け

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

1. 電源ケーブルおよびケーブル類が本体、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、スイッチの正面側の側面に、正面側のブラケットを取り付けます。

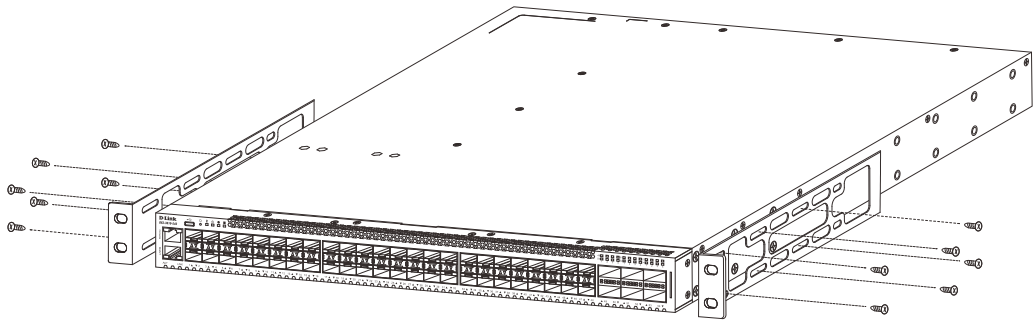


図 2-2　スイッチへの正面側ブラケットの取り付け図①

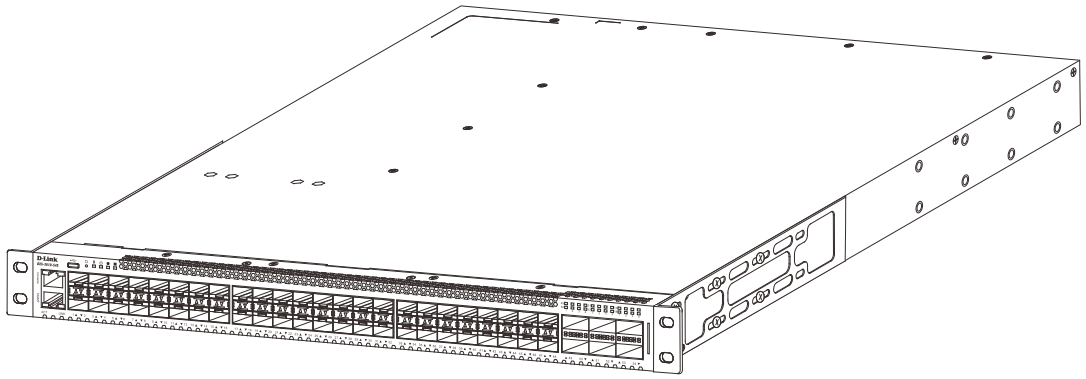


図 2-3　スイッチへの正面側ブラケットの取り付け図②

3. 背面側のブラケットを、下図のようにスライドさせて取り付けます。

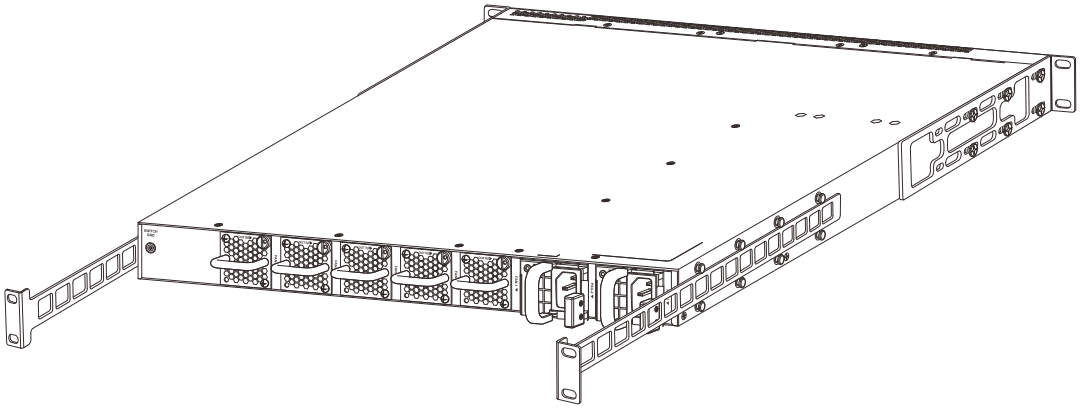


図 2-4　スイッチへの背面側ブラケットの取り付け図

4. 付属のネジを使用し、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。

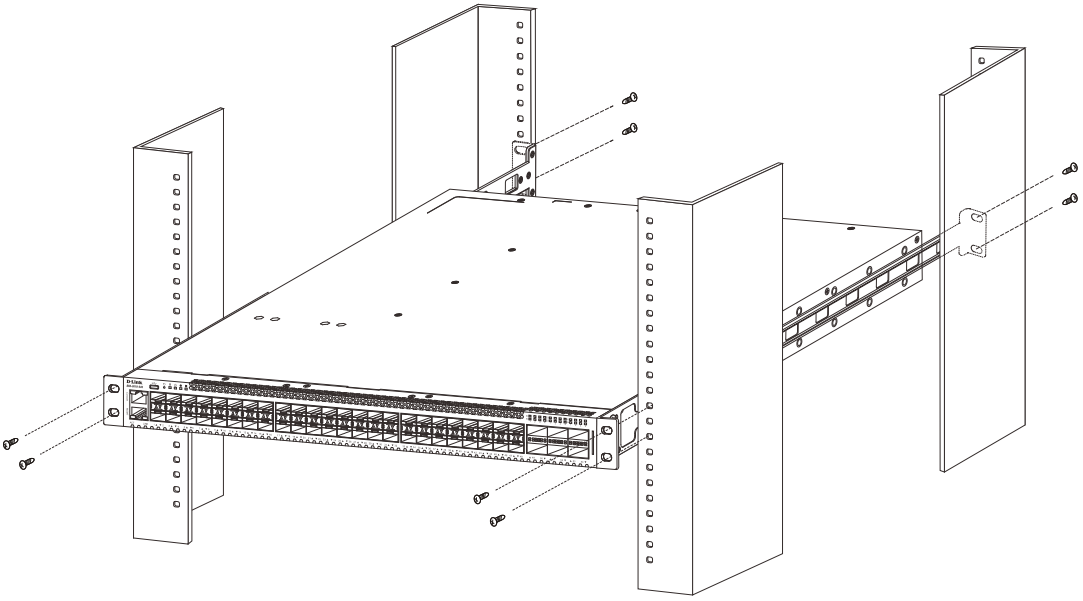


図 2-5　19 インチラックへの取り付け図

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

QSFP28/SFP+ スロットへのモジュールの取り付け

本シリーズには QSFP28 スロット、SFP + スロット（DXS-3610-54S のみ）が搭載されています。 これらスロットを使用して、標準の RJ45 接続をサポートしないさまざまなネットワークデバイスをスイッチに接続することができます。

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

以下に、スイッチの QSFP28 スロットに QSFP+/QSFP28 モジュールを挿入した例を図に示します。

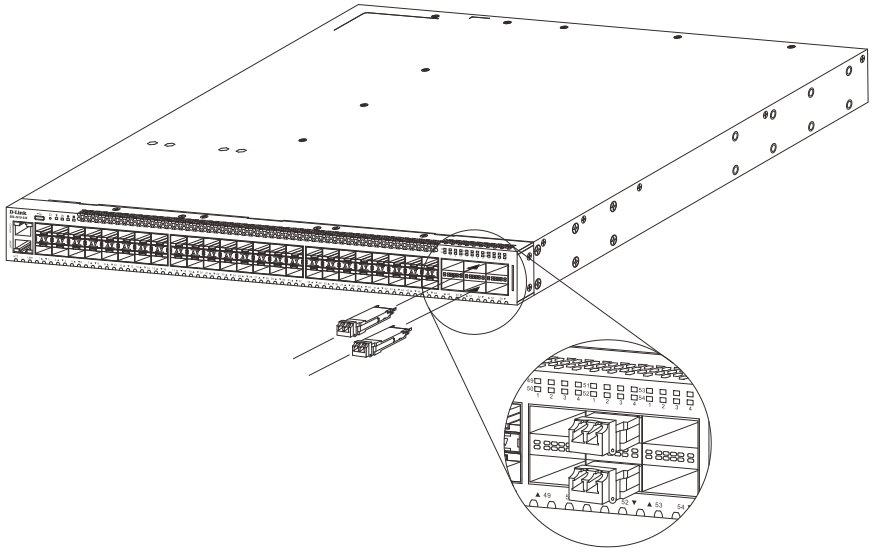


図 2-6　DXS-3610 シリーズ前面パネルの QSFP28 ポートへのモジュールの挿入

以下に、スイッチの SFP+ スロットに SFP/SFP+ モジュールを挿入した例を図に示します。

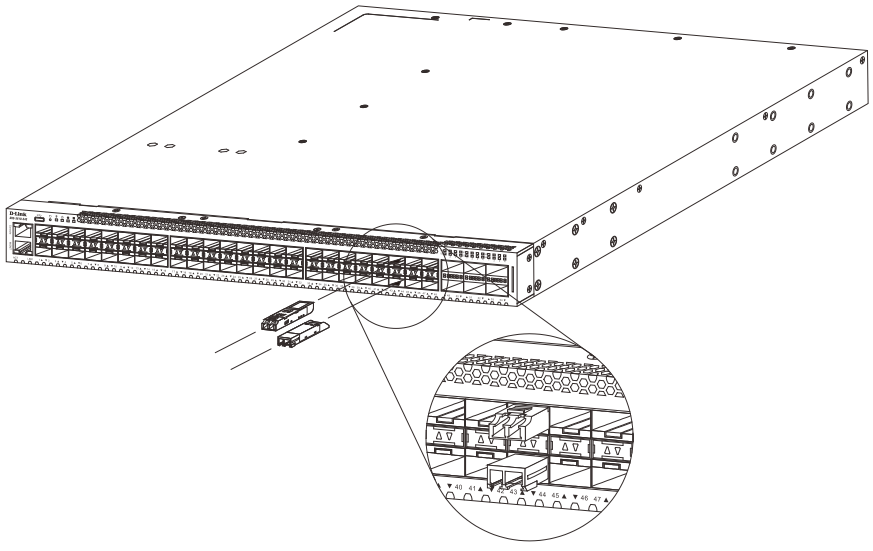


図 2-7　DXS-3610 シリーズ前面パネルの SFP+ ポートへのモジュールの挿入

参照 対応モジュールの一覧は「搭載ポート」を参照してください。

電源スロットへの AC 電源モジュールの取り付け

スイッチには、AC 電源モジュールを取り付けることができます。
AC 電源モジュールを交換または追加する必要がある場合、以下の手順を参照し、AC 電源モジュールの適切な取り付けを行ってください。

補足　スイッチのご購入時に 2 つの電源モジュールが取り付けられています。

AC 電源モジュールはホットスワップ対応で、スイッチの電源が入っている状態で 2 台目の PSU モジュールを取り付けたり取り外したりできます。

取り付け済みの AC 電源モジュールを取り外すには、該当モジュールに接続された AC 電源コードを取り外し、リリースクリップを横に押します。
そのまま電源モジュールを PSU モジュールスロットから慎重に引き出します。

注意　設計上、リリースクリップを横に押す前に AC 電源コードを取り外す必要があります。AC 電源コードが接続されたままの場合は、リリースクリップを押し込むことはできません。

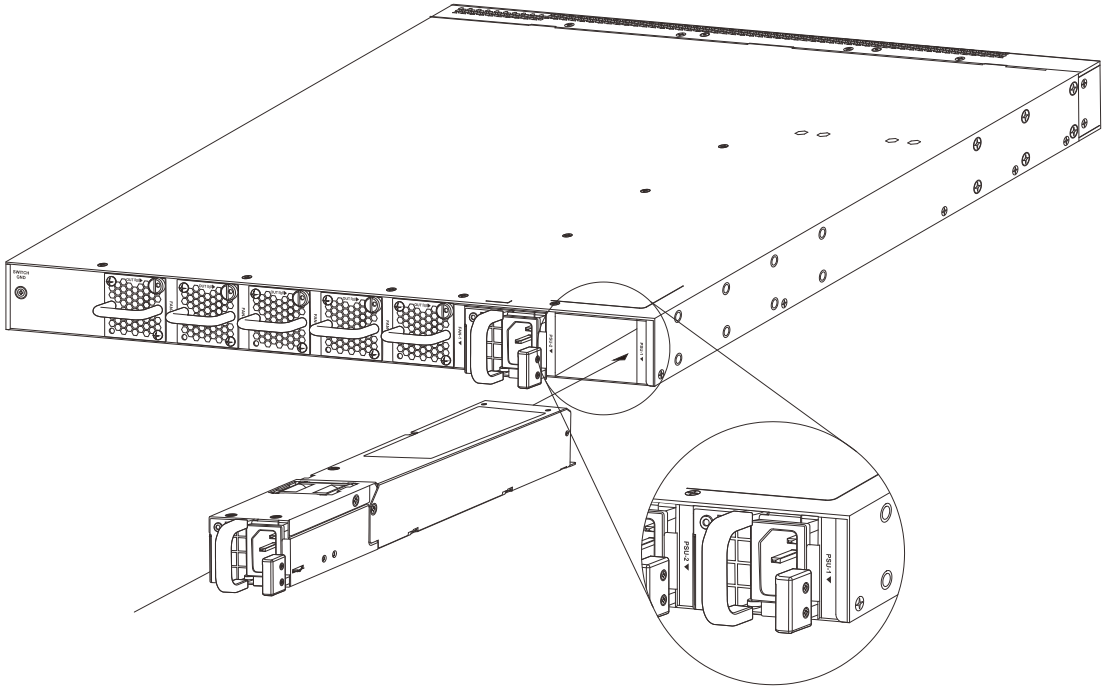


図 2-8　電源モジュールの取り付け

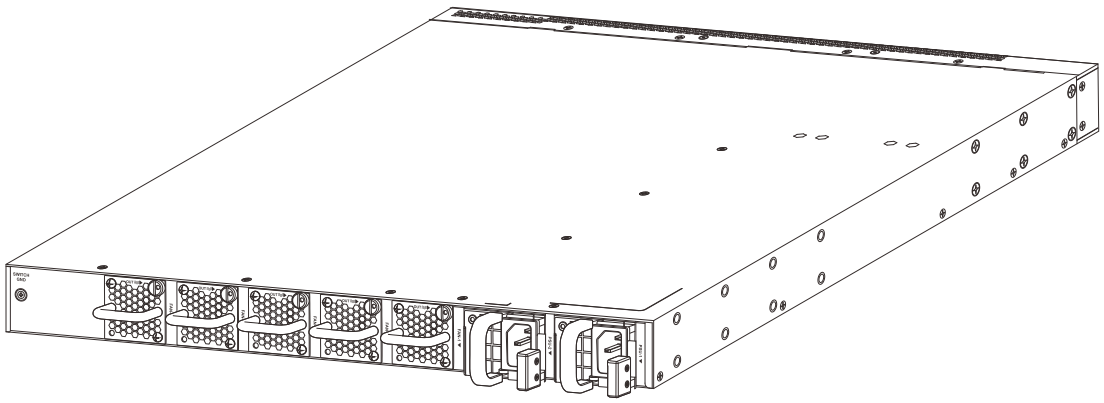


図 2-9　ファンモジュールの取り付け完了

電源モジュールの取り付けが適切に完了したら、電源ケーブルを本スイッチの電源モジュールに接続し、電源ケーブルのプラグを電源コンセントに接続します。スイッチには電源スイッチ / ボタンは搭載されていません。電源ケーブル接続後、システムは自動的にオンとなり、50/60Hz、100 ～ 240VAC 内の電圧に調整されます。

2 つ目の電源モジュールは「PSU-2」と記載された 2 番目の電源モジュールスロットに挿入することができます。1 番目の電源に不具合が発生した場合、2 番目の電源がスイッチに電力を供給します。この切り替えは、即時かつ自動的に行われます。

ファンスロットへのファンモジュールの取り付け

このセクションでは、ファンモジュールをファンモジュールスロットに取り付ける方法について説明します。本スイッチの背面パネルには、5 つのファンモジュールスロットがあります。これらのスロットには、Front-to-Back（FB/ 前面から背面）のファンモジュールを取り付けることができます。ご購入時の状態では、スイッチには 5 つのファンモジュールが取り付けられています。

注意　ファンモジュールは特定のエアフローをサポートしています。このエアフローは、取り付けられている PSU モジュールと同じである必要があります。デフォルトのエアフローは、取り付けられているすべての PSU モジュールおよびファンモジュールにおいて「前面から背面」です。

取り付け済みのファンモジュールを取り外すには、マイナスドライバを使用してラグボルト（スロットドライブヘッド付き）を緩め、ファンモジュールをファンモジュールスロットから慎重に引き出します。新しいファンモジュールをスロットに挿入し、ラグボルトを締めてファンモジュールを固定します。

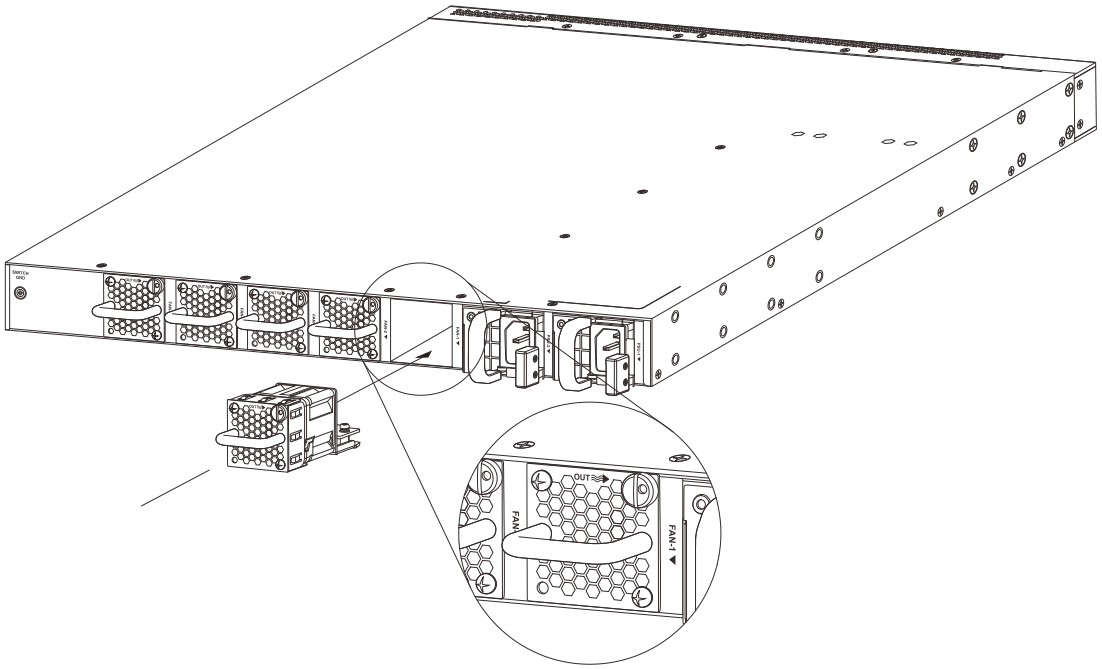


図 2-10　ファンモジュールの取り付け

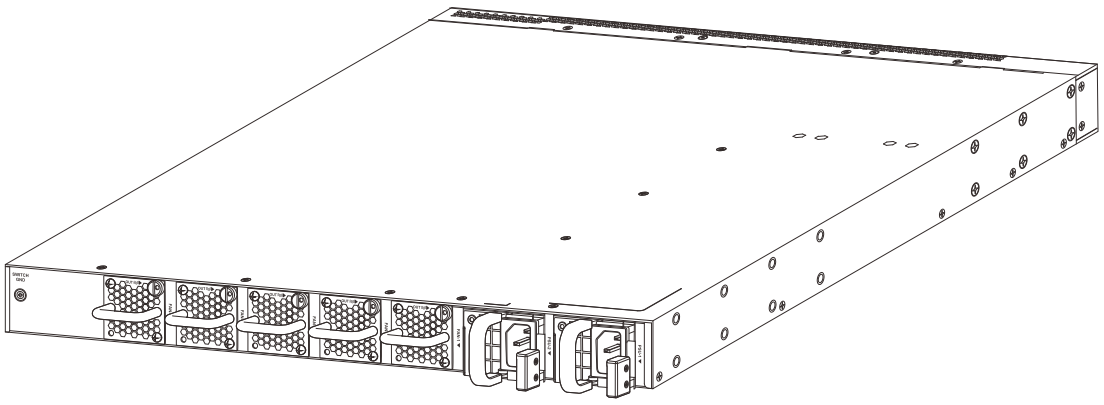


図 2-11　電源モジュールの取り付け完了

スマートファンについて

ファンモジュールは、IC センサの温度計測値に応じて自動的に速度を調整することができます。この機能は非常に感度が高く、ファンの速度を調整して内部温度を正確に制御することができます。

次の表は、内部温度によるファン速度の変化について示しています。

DXS-3610-54T

ファン状態		温度上昇時	温度下降時
低速	Ultra Low	24℃未満	
↑	Very Low	34℃を超えたとき 「Ultra Low」から「Very Low」に切り替わります。	28℃を下回ったとき 「Low」から「Very Low」に切り替わります。
↕	Low	39℃を超えたとき 「Very Low」から「Low」に切り替わります。	34℃を下回ったとき 「Medium」から「Low」に切り替わります。
↓	Medium	47℃を超えたとき 「Low」から「Medium」に切り替わります。	42℃を下回ったとき 「High」から「Medium」に切り替わります。
高速	High	49℃を上回ったとき	

DXS-3610-54S

ファン状態		温度上昇時	温度下降時
低速	Ultra Low	22℃未満	
↑	Very Low	28℃を超えたとき 「Ultra Low」から「Very Low」に切り替わります。	28℃を下回ったとき 「Low」から「Very Low」に切り替わります。
↕	Low	36℃を超えたとき 「Very Low」から「Low」に切り替わります。	34℃を下回ったとき 「Medium」から「Low」に切り替わります。
↓	Medium	44℃を超えたとき 「Low」から「Medium」に切り替わります。	42℃を下回ったとき 「High」から「Medium」に切り替わります。
高速	High	48℃を上回ったとき	

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
- Stacking（スタッキング設定）

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

エンドノードと接続する

「エンドノード」とは本スイッチと接続するネットワーク機器の一般的な呼称です。パソコン、ノート PC、アクセスポイント、プリントサーバ、VoIP 電話機などが該当します。各エンドノードは RJ-45 ネットワークポートを有している必要があります。通常、エンドノードは標準のツイストペア UTP/STP ネットワークケーブルを使用してスイッチと接続します。接続が正常に確立されると、対応するポートの 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。

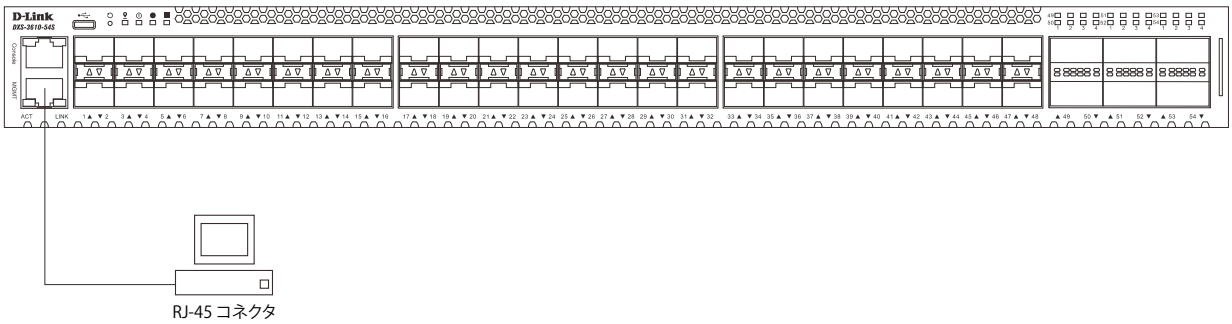


図 3-1　エンドノードと接続した図

ハブまたはスイッチと接続する

本スイッチは、ネットワーク内の他のスイッチやハブに接続することができます。

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 5e の UTP/STP ケーブル：1000BASE-TX ハブまたはスイッチと接続する。
- カテゴリ 6/6a/7 以上の UTP/STP ケーブル：10G BASE-T スイッチと接続する。
- 光ファイバケーブル : SFP+/QSFP28 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。

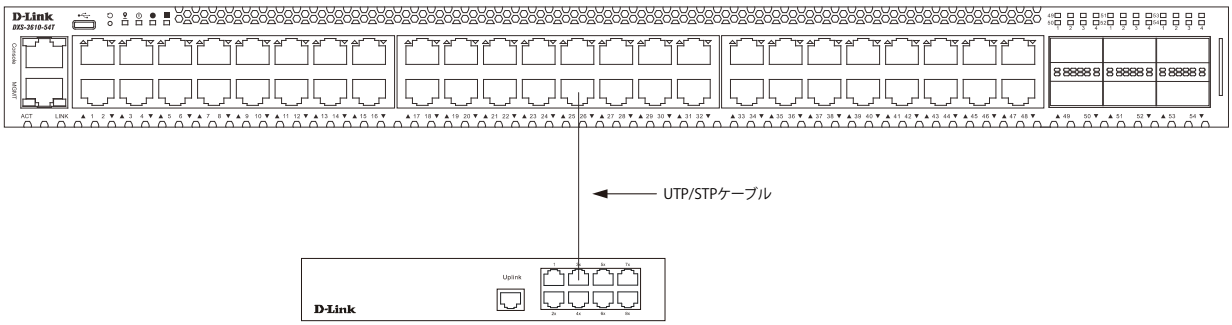


図 3-2　ハブまたはスイッチと接続した図

バックボーンまたはサーバと接続する

本スイッチは、ネットワークバックボーン、サーバ、サーバファームへの接続に適しています。

- RJ45 ポート - 1/10Gbps の速度で動作します。
- SFP+ ポート - 1/10Gbps の速度で動作します。
- QSFP28 ポート - 40/100Gbps の速度で動作します。

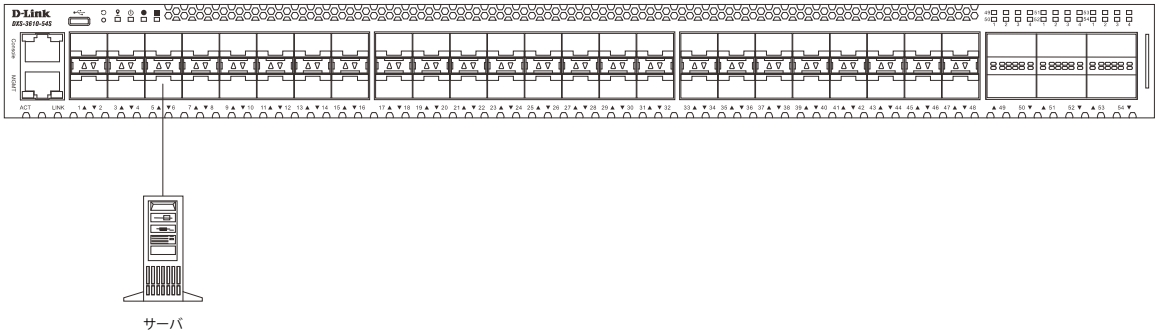


図 3-3　サーバと接続した図

Stacking（スタッキング設定）

本スイッチは、スイッチの物理スタックをサポートしています。Telnet、GUI インタフェース（Web）、コンソールポート、管理（MGMT）ポートまたは SNMP を介して 1 つの IP アドレスで管理することができます。物理スタックによりお使いのネットワークの信頼性、サービス性、そして可用性が向上します。本シリーズの各スイッチは、前面に 6 個のスタック用スロットを搭載しスタッキング可能なデバイスを接続することができます。スタックポートを設定した後、QSFP28 ダイレクトアタッチケーブル（DAC）もしくは光ファイバーケーブルを使用して、スタックポート間を接続し、2 つのトポロジのうちいずれかを形成することができます。

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

- Duplex Ring - Duplex Ring は、データが双方向に転送できるようにリングまたは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、QSFP28 モジュールに接続された光ファイバケーブル、または QSFP28 スロットに接続された QSFP28 ダイレクトアタッチケーブルを使用して、物理的にスタックすることが可能です。最後の 6 つの QSFP28 スロットのみ物理スタックに使用できます。

注意 スタッキングが有効になっている場合、最後の QSFP28 スロット 2/4/6 つは 100Gbps で動作します。スタック機能は 40Gbps をサポートしていません。

以下は、QSFP28 モジュールに接続された光ファイバケーブル、または QSFP28 ダイレクトアタッチケーブルを使用した「Duplex Chain」構成での物理スタック図です。「2 ポート」スタッキング設定を使用しています。

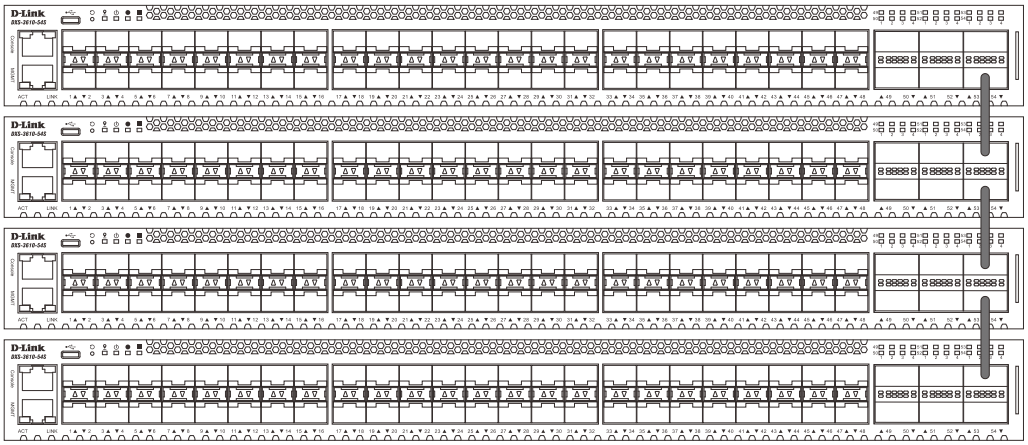


図 3-4　Duplex Chain でスタックされているスイッチ（QSFP28）

以下は、QSFP28 モジュールに接続された光ファイバケーブル、または QSFP28 ダイレクトアタッチケーブルを使用した「Duplex Ring」構成での物理スタック図です。「2 ポート」スタッキング設定を使用しています。

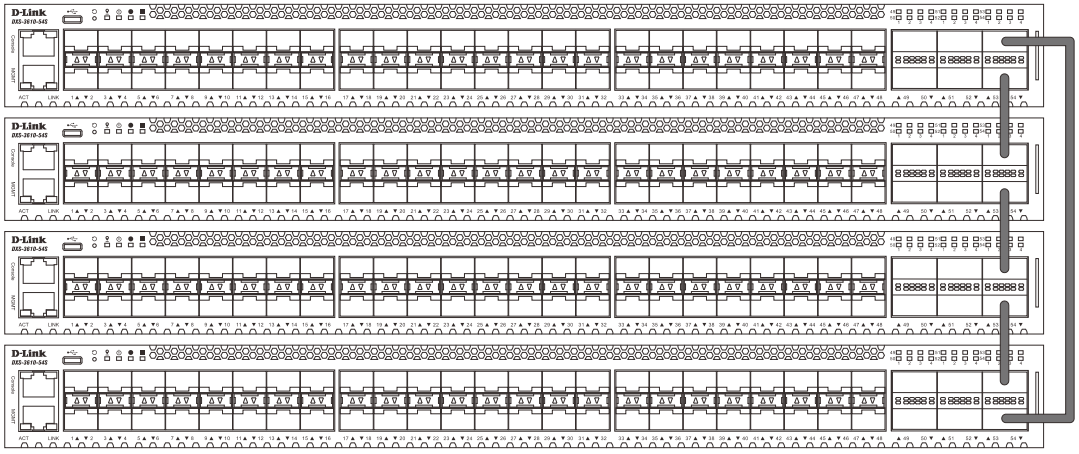


図 3-5　Duplex Ring でスタックされているスイッチ（QSFP28）

物理スタックでは「2 ポート」「4 ポート」「6 ポート」スタッキングコンフィグレーションを設定することができます。
スタッキングポートの設定と、それに対応する SIO ポートペアは以下の通りです。

設定	論理 SIO1	論理 SIO2	帯域幅
2 ポート	ポート 53	ポート 54	400Gbps（全二重）
4 ポート	ポート 51、53	ポート 52、54	800Gbps（全二重）
6 ポート	ポート 49、51、53	ポート 50、52、54	1200Gbps（全二重）

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 /6 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。

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。

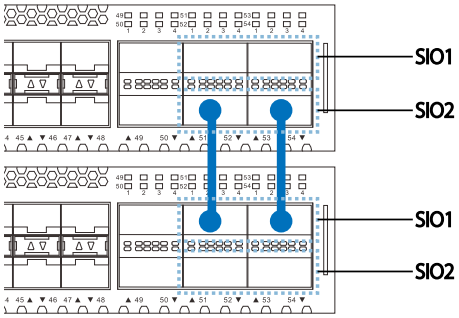


図 3-6　　スイッチ間のケーブル接続①

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。

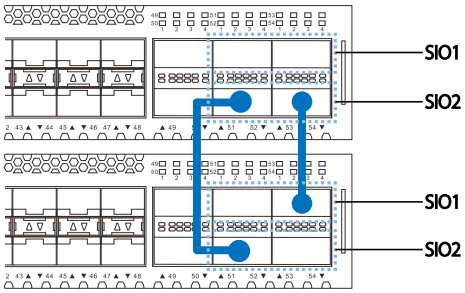


図 3-7　　スイッチ間のケーブル接続②

第 4 章　スイッチ管理について

- Web GUI による管理
- SNMP による管理
- CLI による管理
- 管理ポートへの接続

Web GUI による管理

Microsoft® Internet Explorer などの Web ブラウザによって、本製品の設定をグラフィカルに表示し、管理することができます。

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

SNMP による管理

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

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

CLI による管理

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

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

端末をコンソールポートに接続する

ケーブルの接続

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

ターミナルソフトの設定

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

ログインとログアウト

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

注意　パスワードの大文字と小文字は区別されます。

4. コマンドを入力し、必要な設定を行います。

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

ユーザアカウント / パスワードの設定

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

注意　工場出荷時のユーザアカウントおよびパスワードは「admin」、権限レベルは「15」です。
はじめてログインした際は、本スイッチに対する不正アクセスを防ぐために、ユーザ名に対して必ず新しいパスワードを設定してください。
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。

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

1. 「enable」コマンドを入力し、Privileged EXEC モードにアクセスします。
2. 「configure terminal」コマンドを入力し、Global Configuration モードにアクセスします。
3. 「username Administrator password 12345」コマンドを入力し、ユーザ名「Administrator」、パスワード「12345」を指定します。
4. 「username Administrator privilege 15」コマンドを入力し、ユーザアカウントに権限レベル 15 を指定します。
   権限レベルは 1 から 15 まで指定できます。「15」が最大、「1」が最小の権限レベルです。
5. 「line console」コマンドを入力し、LINE Configuration モードにアクセスします。
6. 管理インタフェースにアクセス可能なユーザアカウントが作成されました。コマンドは「login local」です。

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

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-config startup-config」コマンドを使用して実行中の設定ファイルをスタート時の設定ファイルとしてコピーする必要があります。

IP アドレスの割り当て

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

- IP アドレスの初期値：10.90.90.90/8

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

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

管理ポートへの接続

スイッチの前面パネルには管理ポート（MGMT ポート）があります。
このポートは、標準的なイーサネットケーブルを使用して管理 PC に簡単に接続することができる RJ-45 ポートです。Web ブラウザまたは Telnet クライアントを使用して、管理ポート経由でスイッチに接続します。

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、管理ポートの IP 設定や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 default-gateway 192.168.0.254
Switch(config-if)#
```

IP 設定のステータスを参照するには、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#
```

Web インタフェースを使用する場合、**System > System Information Settings** から設定を行います。

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。

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 Web ブラウザを使用して、HTTP または HTTPS（SSL）プロトコル経由で Web ベースの管理画面にアクセスします。

Web マネージャへのログイン

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合わせるか、本スイッチを端末側の IP インタフェースに合わせてください。

以下のユーザ認証画面が表示されます。

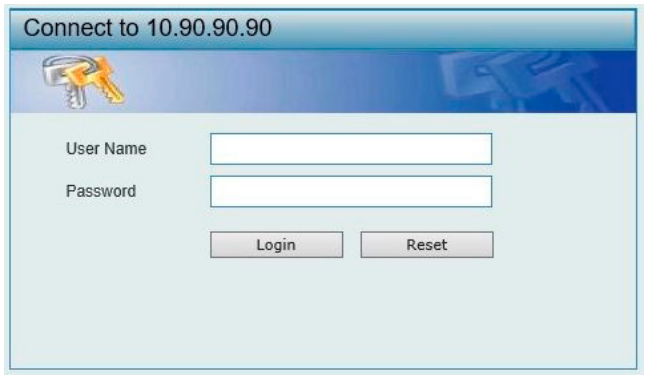


図 5-2　ログイン画面

ユーザ名とパスワードを設定済みの場合は、入力してログインします。
工場出荷時はユーザ名とパスワードは設定されていません。

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

補足　入力値は ASCII 文字のみをサポートします。

Web マネージャの画面構成

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

Web マネージャのメイン画面について

Web マネージャのメイン画面は 3 つのエリアで構成されています。

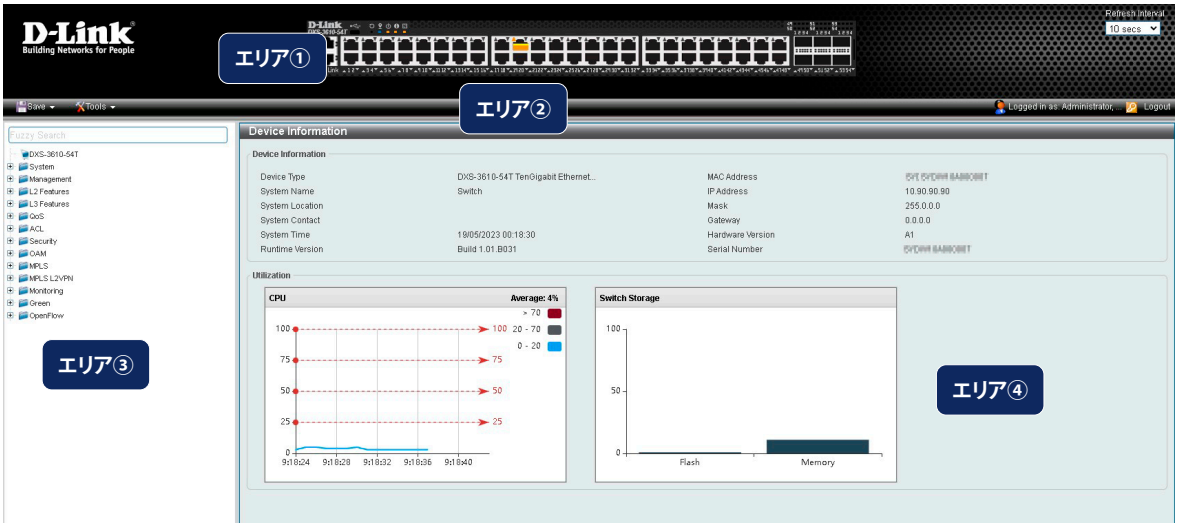


図 5-3　Web マネージャのメインページ

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。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	スイッチの再起動、コンフィグレーションのバックアップとリストア、ファームウェアの更新、設定の初期化などを行う「Tools」メニューと設定の保存を行う「Save」メニューがあります。 ツールバーの右側には、現在接続中のユーザ名とスイッチの IP アドレス、ログアウトボタンが表示されます。
エリア③	WebUI を使用して設定可能な機能のツリービューが表示されます。ツリー項目をクリックして各機能の設定画面に移動します。製品名をクリックすると、デバイス情報画面が表示されます。 また、メニュー項目をキーワードで検索するための検索フィールドも用意されています。
エリア④	ツリービューで選択した各機能の設定画面が表示されます。

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

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

Web マネージャのメニュー構成

Web マネージャで設定可能な機能一覧は以下の通りです。

メインメニュー	サブメニュー	説明
System	Device Information（デバイス情報）	スイッチの主な設定情報を表示します。
	System Information Settings（システム情報設定 ）	スイッチの基本情報を表示します。
	Peripheral Settings（環境設定）	システムの警告温度や環境トラップの設定を行います。
	Port Configuration（ポート設定）	スイッチポートの詳細設定などを行います。
	Interface Description（インタフェース概要）	スイッチの各ポートの概要、管理ステータスなどについて表示します。
	Loopback Test（ループバックテスト）	物理ポートインタフェースのループバック設定とループバックテストを行います。
	System Log（ システムログ構成）	スイッチのフラッシュメモリにスイッチログを保存する方法を設定します。
	Time and SNTP（時刻設定）	スイッチに時刻を設定します。
	Time Range（タイムレンジ設定）	スイッチで使用されるタイムレンジを設定します。ACL などに使用されます。
	PTP（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。
	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。
	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。
	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、ファームウェア、コンフィグレーション情報、および Syslog 情報はフラッシュ内のファイルに保存されます。
	Stacking（スタッキング設定）	物理スタッキングの設定を行います。
	シングル IP マネジメント（SIM）設定	仮想（SIM）スタッキングの設定を行います。
	D-Link Discovery Protocol（D-Link ディスカバリプロトコル）	D-Link ディスカバリプロトコル（DDP）の設定を行います。
	SMTP Settings（SMTP 設定）	Simple Mail Transfer Protocol (SMTP) の設定を行います。
	Reboot Schedule Settings（再起動スケジュール設定）	スイッチの再起動スケジュール設定を行います。
	NLB FDB Settings（NLB FDB 設定）	ネットワークロードバランシング (NLB) の設定を行います。

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（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）	MLAG（Multi-Chassis Link Aggregation Group）の設定を行います。
	Flex Links（フレックスリンク）	フレックスリンク機能の設定を行います。
	L2 Protocol Tunnel （レイヤ 2 プロトコルトンネル）	L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）の設定を行います。
	L2 Multicast Control （L2 マルチキャストコントロール）	IGMP（Internet Group Management Protocol）Snooping 機能を始めとした L2 Multicast Control（L2 マルチキャストコントロール）の設定を行います。
	LLDP	Link Layer Discovery Protocol（LLDP）の設定を行います。
L3 Features	ARP（ARP 設定）	ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
	Gratuitous ARP（Gratuitous ARP 設定）	Gratuitous ARP の設定を行います。
	IPv6 Neighbor（IPv6 ネイバ設定）	IPv6 ネイバ設定を行います。
	Interface（インタフェース設定）	IP インタフェース設定を行います。
	UDP Helper（UDP ヘルパー）	IP 転送プロトコルの設定を行います。本機能は指定の UDP サービスタイプのパケットの転送を有効にします。また UDP ブロードキャストパケットを転送するターゲットアドレスを指定します。
	IPv4 Static/Default Route （IPv4 スタティック / デフォルトルート設定）	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 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。
	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 汎用プレフィックス）	VLAN インタフェース IPv6 汎用プレフィックスの設定を行います。
	IP Tunnel Settings（IP トンネル設定）（EI モードのみ）	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 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）	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 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）（EI 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 設定ウィザードを使用して、アクセスプロファイルと ACL ルールの新規作成・更新を行います。
	ACL Access List（ACL アクセスリスト）	ACL アクセスリストの設定を行います。
	ACL Interface Access Group（ACL インタフェースアクセスグループ）	ACL インタフェースアクセスグループの設定を行います。
	ACL VLAN Access Map（ACL VLAN アクセスマップ）	ACL VLAN アクセスマップの設定を行います。
	ACL VLAN Filter（ACL VLAN フィルタ設定）	ACL VLAN フィルタの設定を行います。
	CPU ACL（CPU ACL 設定）	CPU インタフェースフィルタリング機能の設定を行います。
Security	Port Security（ポートセキュリティ）	ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。
	802.1X（802.1X 設定）	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。
	AAA（AAA 設定）	AAA（Authentication、Authorization、Accounting）の設定を行います。
	RADIUS（RADIUS 設定）	RADIUS の設定を行います。
	TACACS+（TACACS+ 設定）	TACACS+ の設定を行います。
	IMPB（IP-MAC-Port Binding/IP-MAC- ポートバインディング）	IP-MAC バインディングにより、スイッチにアクセスするユーザ数を制限します。
	DHCP Server Screening（DHCP サーバスクリーニング設定）	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
	ARP Spoofing Prevention（ARP スプーフィング防止設定）	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスと一致しなかった IP アドレスの ARP パケットをバイパスします。
	BPDU Attack Protection（BPDU アタック防止設定）	スイッチのポートに BPDU 防止機能を設定します。
	NetBIOS Filtering（NetBIOS フィルタリング設定）	NetBIOS フィルタリングの設定を行います。
	MAC Authentication（MAC 認証）	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
	Web-based Access Control（Web 認証）	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認証する機能です。
	Network Access Authentication（ネットワークアクセス認証）	Network Access Authentication（ネットワークアクセス認証）の設定を行います。
	Safeguard Engine（セーフガードエンジン）	セーフガードエンジンは、攻撃中にスイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。
	Trusted Host（トラストホスト）	トラストホストの設定を行います。
	Traffic Segmentation Settings（トラフィックセグメンテーション）	トラフィックセグメンテーション機能はポート間のトラフィックの流れの制限を行います。
	Storm Control Settings（ストームコントロール設定）	ストームコントロールの設定を行います。
	DoS Attack Prevention Settings（DoS 攻撃防止設定）	各 DoS 攻撃に対して防御設定を行います。

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。
	Network Protocol Port Protect Settings（ネットワークプロトコルポート保護設定）	ネットワークプロトコルポート保護設定を行います。
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 (EI 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）を表示します。
	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）の設定を行います。
	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、表示を行います。
	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）を表示します。
	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）を表示します。
	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）を表示します。
	MPLS QoS Settings（MPLS QoS 設定）	MPLS QoS Settings（MPLS QoS 設定）の設定、表示を行います。
	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にホップごとの障害点特定に使用されます。
MPLS L2VPN (EI モードのみ)	VPWS Settings（VPWS 設定）	「Virtual Private Wire Service」(VPWS) の設定を行います。
	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）の設定を行います。
	VPLS Settings（VPLS 設定）	「Virtual Private LAN Service」(VPLS) の設定を行います。
	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）を表示します。

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作成します。
	Utilization（利用分析）	スイッチの Utilization（利用分析）を表示します。
	Statistics（統計情報）	スイッチの Statistics（統計情報）を表示します。
	Mirror Settings（ミラー設定）	ミラーリング機能の設定を行います。対象ポートで送受信するフレームをコピーし、フレームの出力先を他のポートに変更する機能（ポートミラーリング）です。
	sFlow（sFlow 設定）	sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。
	Device Environment（機器環境確認）	Device Environment（機器環境確認）ではスイッチの内部の温度状態を表示します。
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（環境設定）	システムの警告温度や環境トラップの設定を行います。
Port Configuration（ポート設定）	スイッチポートの詳細設定などを行います。
Interface Description（インタフェース概要）	スイッチの各ポートの概要、管理ステータスなどについて表示します。
Loopback Test（ループバックテスト）	物理ポートインタフェースのループバック設定とループバックテストを行います。
System Log（システムログ構成）	スイッチのフラッシュメモリにスイッチログを保存する方法を設定します。
Time and SNTP（時刻設定）	スイッチに時刻を設定します。
Time Range（タイムレンジ設定）	スイッチのタイムレンジを設定します。ACL などに使用されます。
PTP（PTP 設定）	PTP（Precision Time Protocol : 高精度時刻同期方式）システムは、イーサネットネットワークを通して時刻を同期します。
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）

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

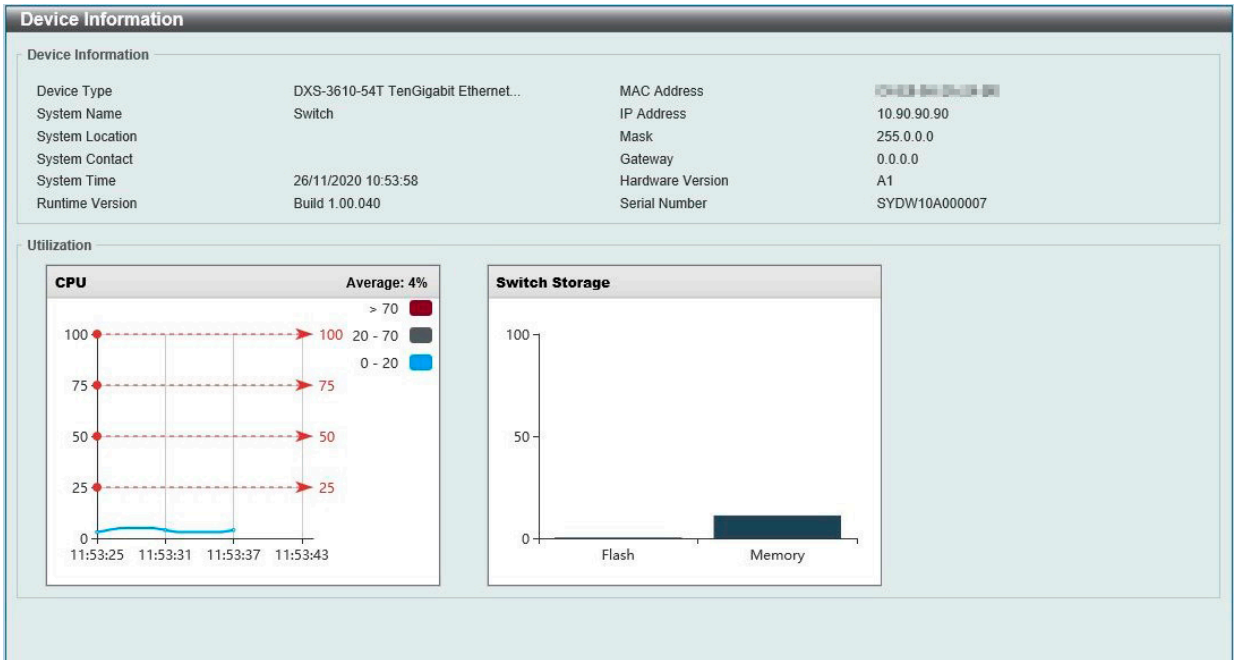


図 6-1　Device Information 画面

画面に表示される項目：

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

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

スイッチのシステム情報と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、以下の画面を表示します。

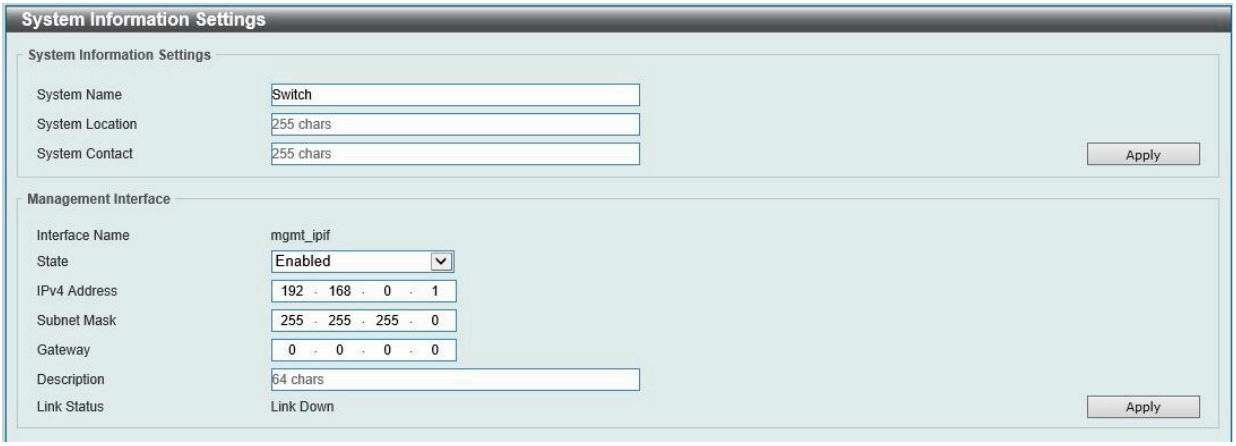


図 6-2　System Information Settings 画面

画面に表示される項目：

項目	説明
System Information Settings	
System Name	必要に応じて、スイッチのシステム名を変更します。ネットワーク内での識別名となります。
System Location	必要に応じて、システムが稼働している場所を定義します。
System Contact	必要に応じて、スイッチの管理者情報を入力します。
Management 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 アドレスを入力します。
Subnet Mask	管理インタフェースのサブネットマスクを入力します。
Gateway	管理インタフェースのゲートウェイ IPv4 アドレスを入力します。
Description	管理インタフェースの説明を入力します。（半角英数字 64 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

Peripheral Settings（環境設定）

システムの警告温度や環境トラップの設定を行います。

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

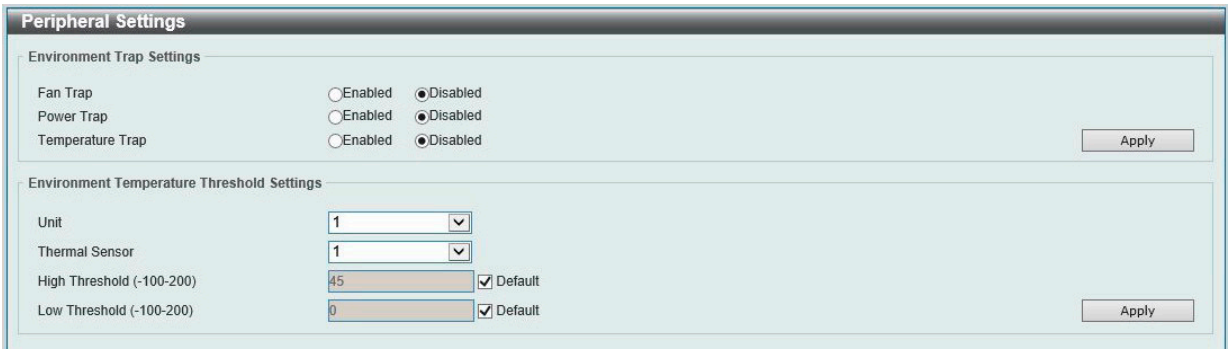


図 6-3　Peripheral Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

Port Configuration（ポート設定）

各ポートの設定を行います。

Port Settings（スイッチのポート設定）

スイッチポートの詳細を設定します。

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

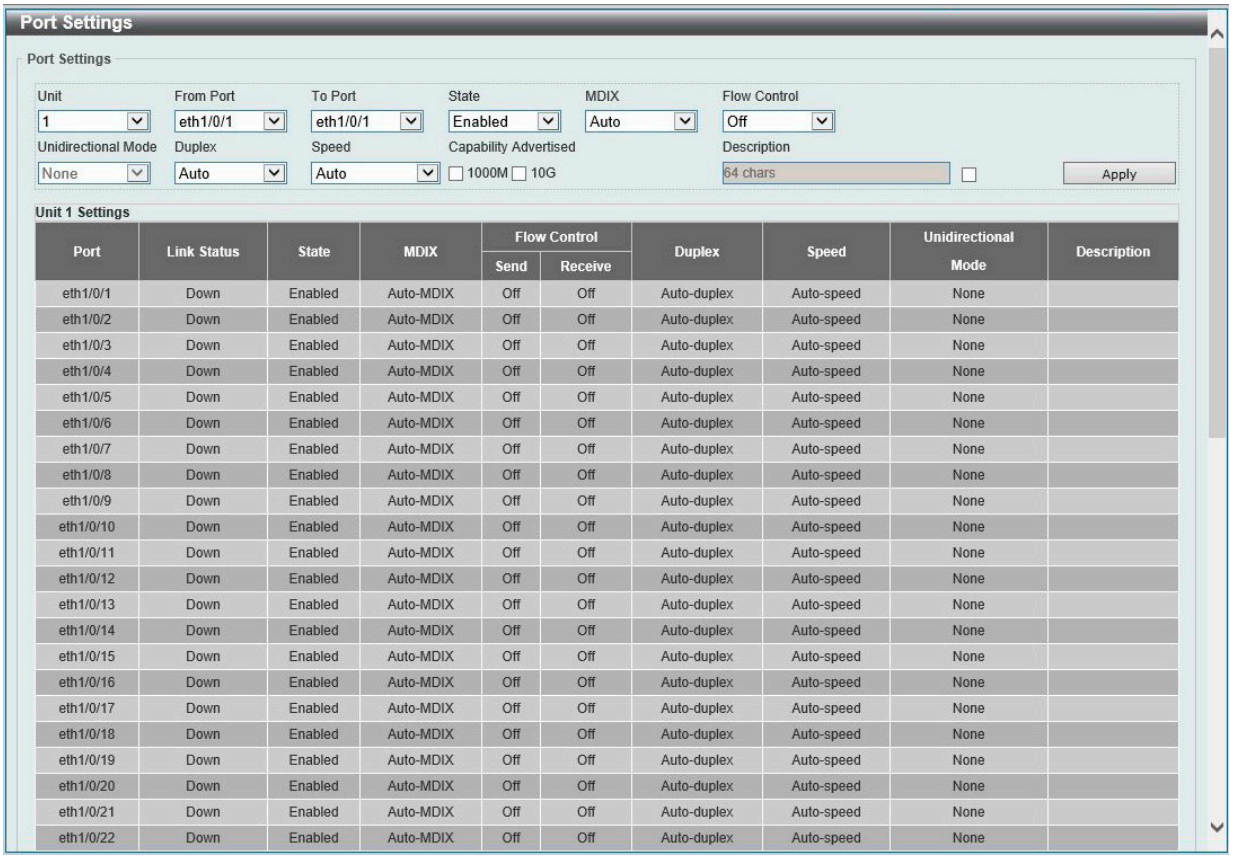


図 6-4　Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
State	物理ポートのステータスを有効 / 無効に設定します。
MDIX	MDIX オプションを選択します。 • 「Auto」- 最適なケーブル接続を自動的に設定します。 • 「Normal」- 通常のケーブル接続の場合は、このオプションを選択します。このオプションを選択すると、ポートは MDIX モードになり、ストレートケーブルを使用して PC の NIC に接続するか、クロスケーブルを介して別のスイッチのポート（MDI モード）に接続できます。 • 「Cross」- ポートは MDI モードとなり、ストレートケーブルで別のスイッチのポート (MDIX モード) に接続することができます。
Flow Control	「On」（フロー制御あり）または「Off」（フロー制御なし）を選択します。物理スタックのスイッチはサポートしていません。
Unidirectional Mode	単方向モードを選択します。 • 「None」- ポートを介した双方向通信を指定します。 • 「Send Only」- ポートを介した外向きの単方向通信のみを指定します。 • 「Receive Only」- ポートを介した内向きの単方向通信のみを指定します。
Duplex	Duplex モードの選択を行います。半二重モードはサポートされていません。 • 選択肢：「Auto」「Full」

項目	説明
Speed	ポートの速度を選択します。速度を指定すると、指定のポートで接続速度が固定となります。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 • **「Auto」** - copper ポートの場合、オートネゴシエーションを開始してリンクパートナーと速度、フローコントロールの調整を行います。光ファイバポートの場合、オートネゴシエーションを開始してリンクパートナーとクロック、フローコントロールの調整を行います。 • **「1000M」** - ポート速度を 1Gbps に固定します。 • **「1000M Master」** - ポート速度を 1Gbps に固定し、送受信のタイミング制御におけるマスタとして指定します。 • **「1000M Slave」** - ポート速度を 1Gbps に固定し、送受信のタイミング制御におけるスレーブとして指定します。 • **「10G」** - ポート速度を 10Gbps に固定します。 • **「10G Master」** - ポート速度を 10Gbps に固定し、送受信のタイミング制御におけるマスタとして指定します。 • **「10G Slave」** - ポート速度を 10Gbps に固定し、送受信のタイミング制御におけるスレーブとして指定します。 • **「40G」** - ポート速度を 40Gbps に固定します。 • **「100G」** - ポート速度を 100Gbps に固定します。 • マスタ設定 (1000M Master/10G Master) - 該当ポートは Duplex、速度、物理レイヤタイプについてアドバタイズを行います。また、接続された物理レイヤ間のマスタ・スレーブ関係を決定します。これらの関係は、2 つの物理レイヤ間のタイミング制御を確立するために必要です。タイミング制御は、ローカルソースによってマスタの物理層にセットされます。 • スレーブ設定 (1000M Slave/10G Slave) - ループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わせます。一方の接続にマスタを設定した場合、他方の接続はスレーブとする必要があります。それ以外の設定を行うと、両ポートのリンクダウンを引き起こします。
Capability Advertised	上記「Speed」が「Auto」に設定されている場合、指定した項目がオートネゴシエーションの間にアドバタイズされます。
Description	ポートの説明を入力します。（64 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

注意 Half duplex をサポートしません。

注意 SFP+/QSFP28 ポートでは、auto-negotiation および auto-speed はサポートされません。

注意 1000/10GBase-X は Auto Negotiation のみをサポートします。

注意 10/100Mbps をサポートしません。

注意 DXS-3610-54T の Copper ポートは Auto Negotiation のみをサポートします。

Port Status（ポートステータス）

ポートの状態、設定について表示します。

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

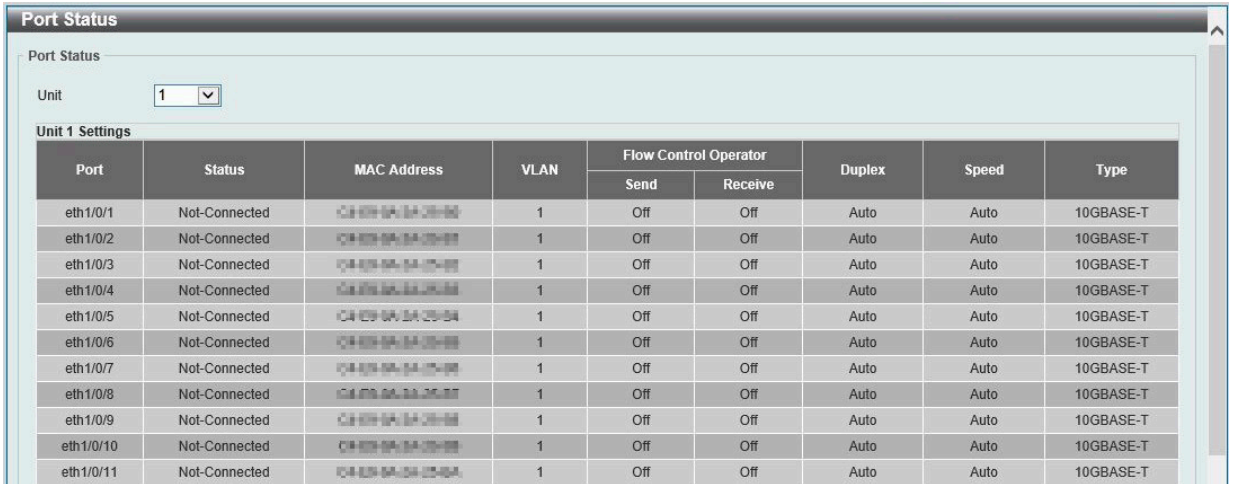


図 6-5　Port Status 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

Port GBIC

各物理ポートの GBIC 情報について表示します。

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

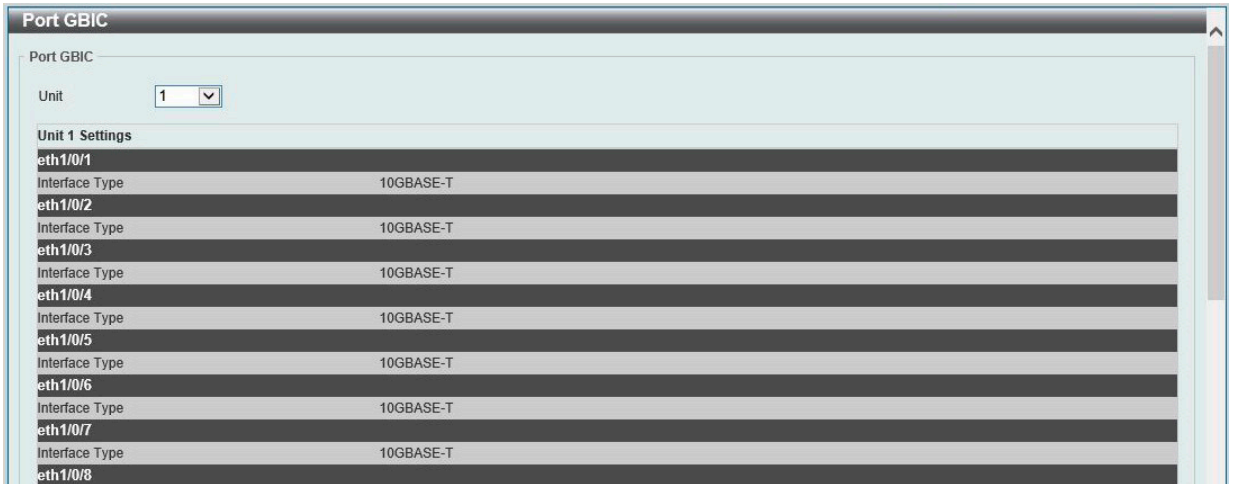


図 6-6　Port GBIC 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

Port Auto Negotiation（オートネゴシエーション）

オートネゴシエーションの詳細情報を表示します。

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



図 6-7　Port Auto Negotiation 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

Error Disable Settings（エラーによるポートの無効）

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

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

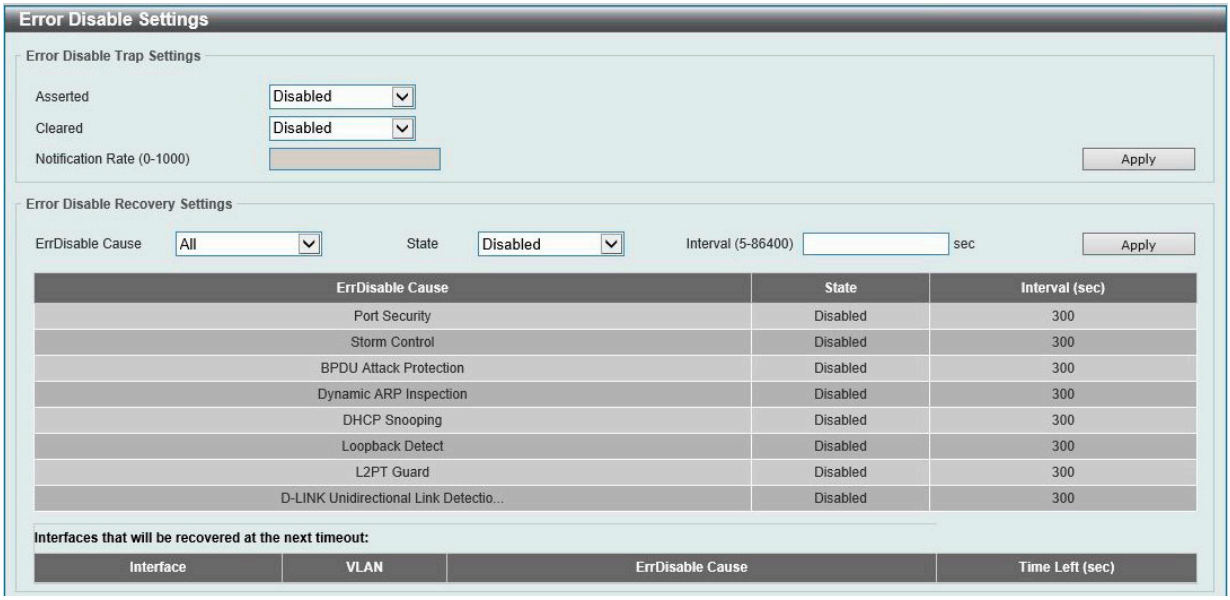


図 6-8　Error Disable Settings 画面

画面に表示される項目：

項目	説明
Error Disable Trap Settings	
Asserted	エラー無効状態になったときの通知送信の有効 / 無効を指定します。
Cleared	エラー無効状態から回復したときの通知送信の有効 / 無効を指定します。
Notification Rate	1 分あたりのトラップ数を入力します。指定したしきい値を超えたパケットは破棄されます。 • 設定可能範囲：0-1000 • 初期値：0 初期値の「0」は、無効状態が変更されるたびに SNMP トラップが生成されることを示します。
Error Disable Recovery Settings	
ErrDisable Cause	エラー無効の原因を選択します。 • 選択肢：「All」「Port Security」「Storm Control」「BPDU Attack Protection」「Dynamic ARP Inspection」「DHCP Snooping」「Loopback Detect」「L2PT Guard」「DULD」
State	指定した原因によるエラー無効ポートの自動リカバリ機能を有効 / 無効に設定します。
Interval	ポートリカバリ実行の間隔を指定します。 • 設定可能範囲：5-86400（秒） • 初期値：300（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

Jumbo Frame（ジャンボフレームの有効化）

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。ジャンボフレームは、1518 バイト以上のペイロードを持つイーサネットフレームです。本スイッチは最大 9216 バイトまでのジャンボフレームをサポートします。本機能を設定することにより、オーバヘッド、処理時間、割り込みを減らすことができます。

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



図 6-9　Jumbo Frame 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Maximum Receive Frame Size	受信フレームサイズの最大値を入力します。 • 設定可能範囲：64-9216（bytes） • 初期値：1536（bytes）

「Apply」ボタンをクリックして、設定内容を適用します。

Interface Breakout（インタフェースブレイクアウト）

注意　本機能は未サポートです。

100Gbps ポートのブレイクアウト設定を行います。
ブレイクアウト設定を適用できるのは、以下の 2 グループからそれぞれ 1 ポートずつ、合計 2 ポートのみです。
- グループ 1 (ポート 49、50、52）
- グループ 2 (ポート 51、53、54）

MLAG ピアポートまたはスタッキングに使用されているポートには、ブレイクアウト設定を適用できません。

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

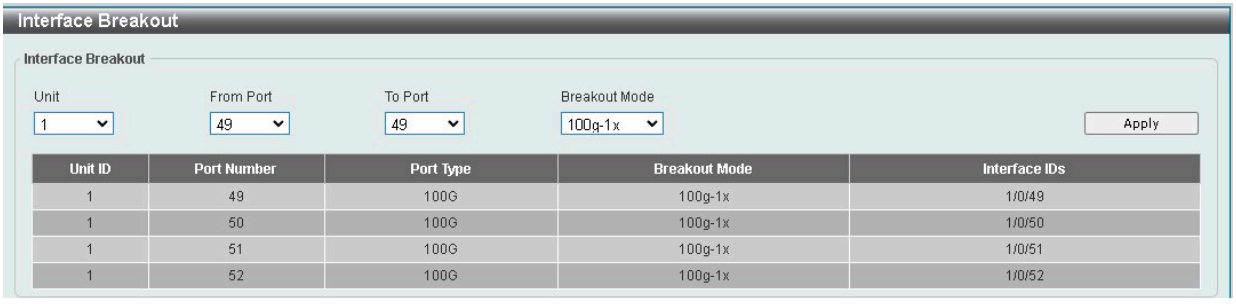


図 6-10　Interface Breakout 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポートを指定します。 • 選択肢：「49」「50」「51」「52」「53」「54」
Breakout Mode	ブレイクアウトモードを選択します。 • 「25g-4x」- 100Gbps ポートを 4 つの 25Gbps ポートに分割します。 • 「100g-1x」- 単一の 100 Gbps ポートに戻すように指定します。 • 「10g-4x」- 100Gbps ポートを 4 つの 10Gbps ポートに分割します。

「Apply」ボタンをクリックして、設定内容を適用します。

Interface Description（インタフェース概要）

スイッチの各ポートのリンク状態、管理ステータス、概要を表示します。

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

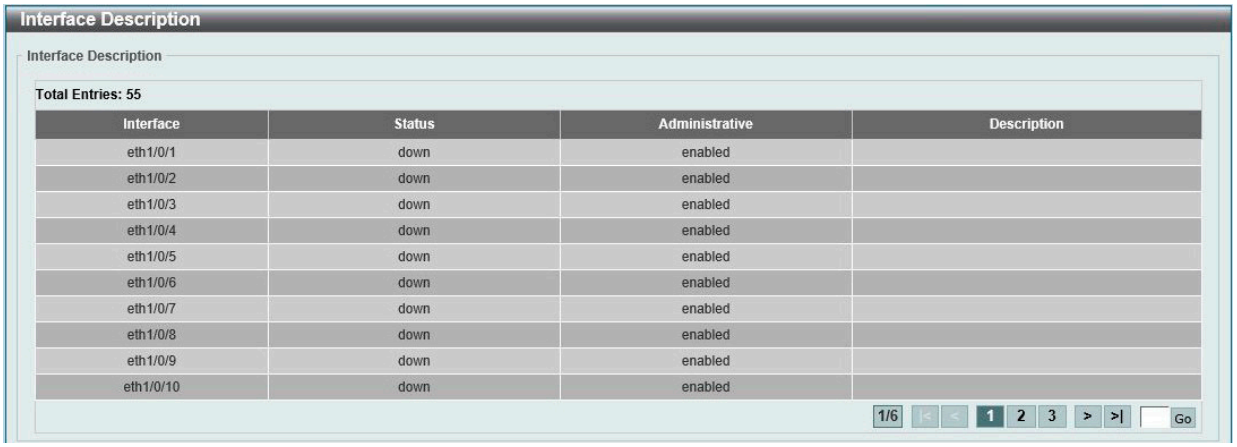


図 6-11　Interface Description 画面

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

Loopback Test（ループバックテスト）

物理ポートインタフェースのループバック設定とループバックテストを行います。

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

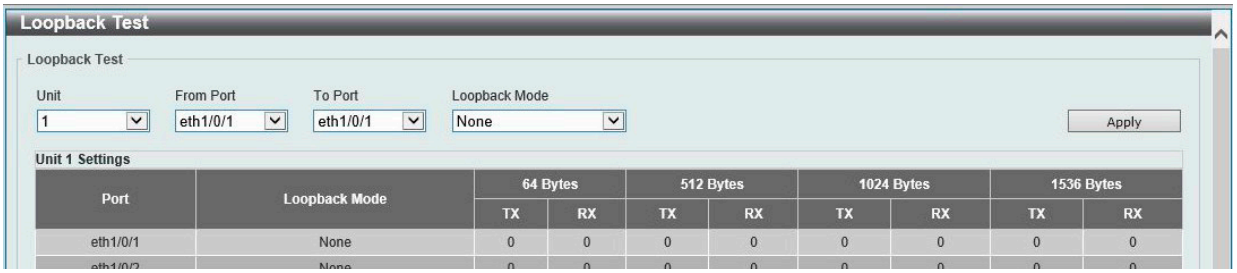


図 6-12　Loopback Test 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

注意　以下の機能を有効にしている場合、内部 PHY（Internal PHY）および内部 MAC（Internal MAC）のループバックモードは機能しません。
- STP/ ループバック検知 / ミラーリング / ポートチャネル設定

※ループバックモードや各機能の組み合わせにより、併用可否は異なります。

System Log（システムログ構成）

システムログの設定を行います。

System Log Settings（システムログ設定）

システムログ機能のステータスや、ログの保存方法などを設定します。

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

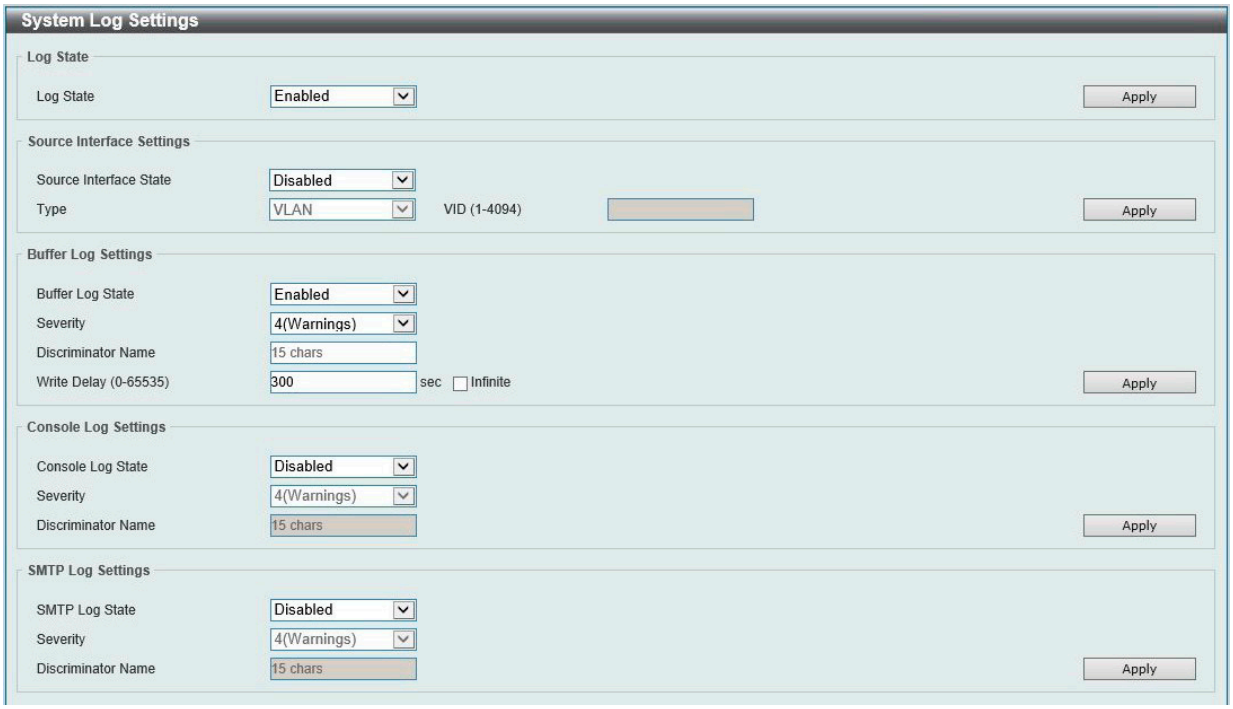


図 6-13　System Log Settings 画面

画面に表示される項目：

項目	説明
Log State	
Log State	シスログのグローバルステータスを有効 / 無効に指定します。
Source Interface Settings	
Source Interface State	ソースインタフェースのグローバルステータスを有効 / 無効に指定します。
Type	インタフェースの種類を選択します。 • 選択肢：「Loopback」「Mgmt」「VLAN」
Interface ID	インタフェース ID を指定します。 • 設定可能範囲：1-8（Loopback 選択時）、0（Mgmt 選択時）、1-4094（VLAN 選択時）
Buffer Log Settings	
Buffer Log State	バッファログのグローバルステータスを有効 / 無効に指定します。 • 選択肢：「Enable」「Disabled」「Default」 「Default」を選択すると、バッファログのグローバルステータスは初期設定に従います。
Severity	ログ出力される情報のレベルを選択します。 • 選択肢：「0：Emergencies」（緊急）、「1：Alerts」（アラート）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Discriminator Name	ディスクリミネータの名前を入力します。（15 文字以内）このディスクリミネータプロファイルで指定されたフィルタリング条件に基づき、バッファログメッセージがフィルタされます。
Write Delay	フラッシュにロギングバッファを書き込む間隔を指定します。 • 設定可能範囲：0-65535（秒） • 初期値：300（秒） 「Infinite」にチェックを入れると本機能は無効になります。
Console Log Settings	
Console Log State	コンソールログのグローバルステータスを有効 / 無効に指定します。
Severity	ログ出力される情報のレベルを選択します。 • 選択肢：「1：Emergencies」（緊急）、「2：Alerts」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）

項目	説明
Discriminator Name	ディスクリミネータの名前を入力します。（15 文字以内）このディスクリミネータプロファイルで指定されたフィルタリング条件に基づき、コンソールログメッセージがフィルタされます。
SMTP Log Settings	
SMTP Log State	SMTP ログのグローバルステータスを有効 / 無効に指定します。
Severity	ログ出力される情報のレベルを選択します。 • 選択肢：「1：Emergencies」（緊急）、「2：Alerts」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Discriminator Name	ディスクリミネータの名前を入力します。（15 文字以内）このディスクリミネータプロファイルで指定されたフィルタリング条件に基づき、SMTP ログメッセージがフィルタされます。

「Apply」ボタンをクリックして、設定内容を適用します。

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

システムログディスクリミネータの設定、設定内容の表示を行います。

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

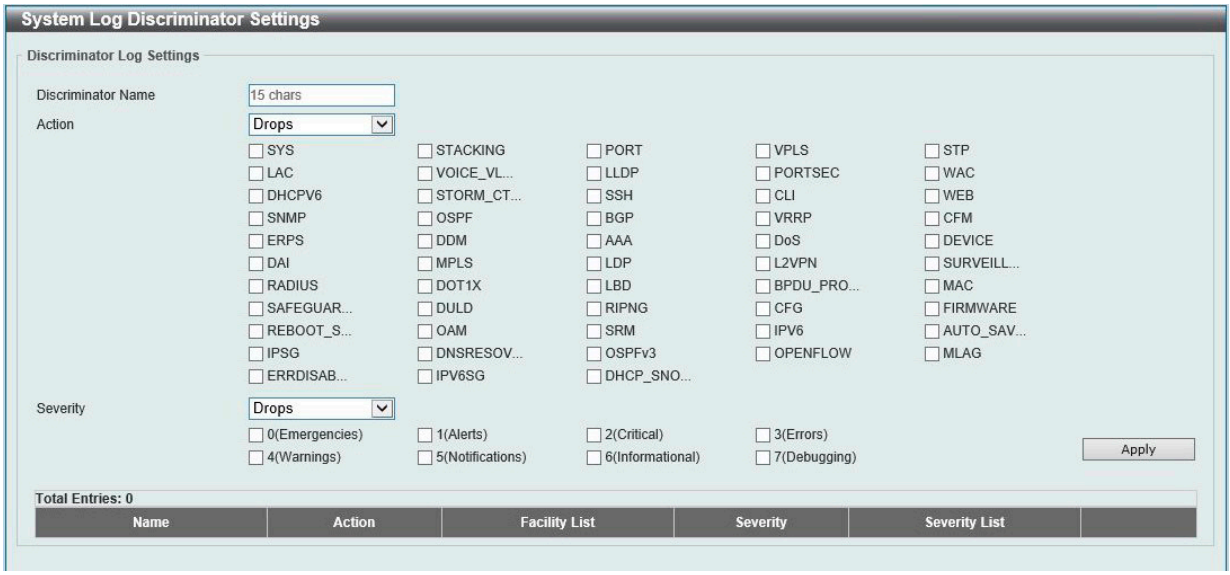


図 6-14　System Log Discriminator Settings 画面

画面に表示される項目：

項目	説明
Discriminator	ディスクリミネータの名前を入力します。（15 文字以内）
Action	ログファシリティに対する動作を「Drops（破棄）」「Includes（含める）」から選択し、対象とするファシリティの種類のチェックボックスにチェックを入れます。
Severity	ログセベリティに対する動作を「Drops（破棄）」「Includes（含める）」から選択し、ログ出力される情報のレベルのチェックボックスにチェックを入れます。セベリティは以下の種類から選択します。 • 選択肢：「1：Emergencies」（緊急）、「2：Alerts」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）

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

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

シスログサーバを設定します。

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



図 6-15　System Log Server Settings 画面

画面に表示される項目：

項目	説明
Host IPv4 Address	システムログサーバの IPv4 アドレスを設定します。
Host IPv6 Address	システムログサーバの IPv6 アドレスを設定します。
UDP Port	システムログサーバの UDP ポートを設定します。 • 設定可能範囲：514、1024-65535 • 初期値：514
Severity	ログ出力される情報のレベルを選択します。 • 選択肢：「1：Emergencies」（緊急）、「2：Alerts」（アラート）、「3：Critical」（重大）、「4：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Facility	ログ出力されるファシリティの番号を選択します。 • 選択可能範囲：0-23
Discriminator	ディスクリミネータの名前を入力します。（15 文字以内）ログサーバへ送信されるログメッセージのフィルタリングで使用されます。
VRF Name （EI モードのみ）	Virtual Routing and Forwarding（VRF）のインスタンス名を指定します。（12 文字以内）

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

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

System Log（Syslog ログ）

システムログの閲覧 / 消去を行います。

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

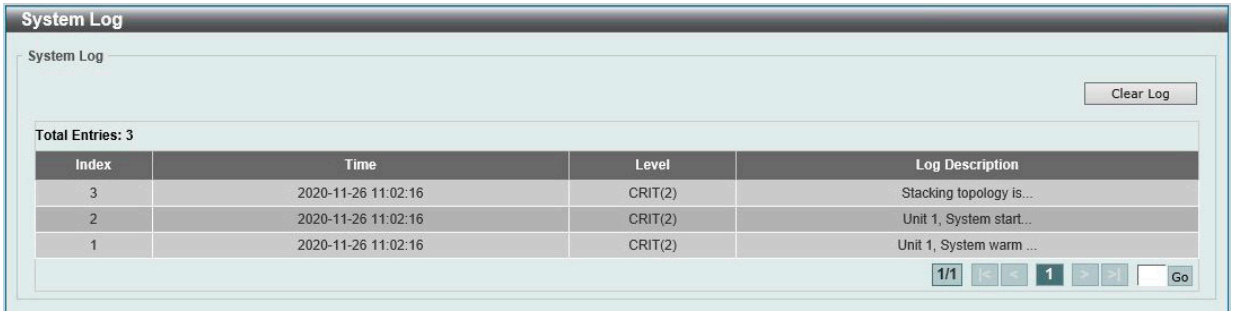


図 6-16　System Log 画面

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

System Attack Log（システムアタックログ）

システム攻撃ログの閲覧 / 消去を行います。

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



図 6-17　System Attack Log 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

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

Time and SNTP（時刻設定）

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

Clock Settings（時間設定）

スイッチの時刻を設定します。

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



図 6-18　Clock Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

Time Zone Settings（タイムゾーン設定）

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

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

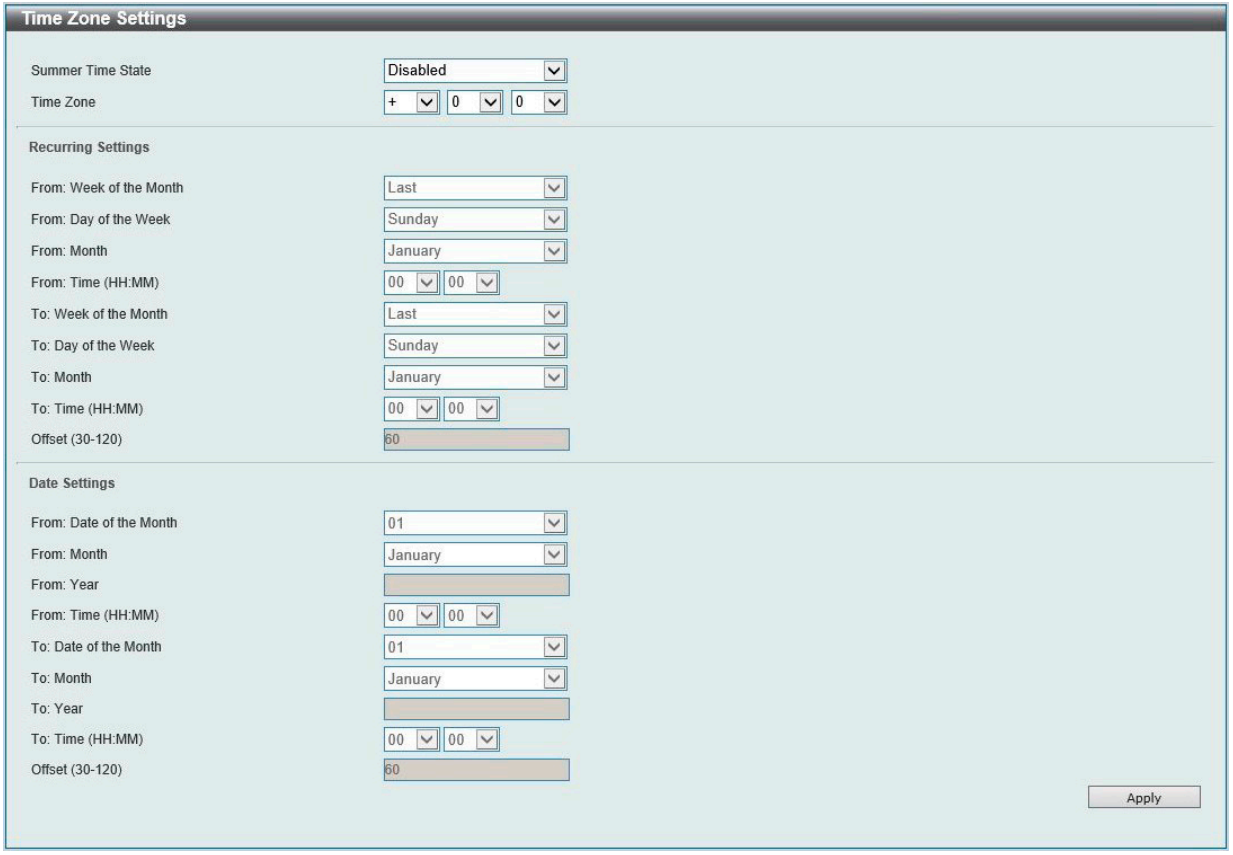


図 6-19　Time Zone Settings 画面

表示される項目：

項目	説明
Summer Time State	デバイスに設定するサマータイムの種類を設定します。 • 「Disabled」- サマータイムを無効にします。（初期値） • 「Recurring Setting」- サマータイムを周期的に有効にします。このオプションでは、指定月の指定曜日にサマータイムが開始 / 終了します。 • 「Date Setting」- サマータイムを日付指定で有効にします。このオプションでは、指定年月日にサマータイムが開始 / 終了します。
Time Zone	ローカルタイムゾーンの UTC からのオフセットを指定します。
Recurring 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	月の第何週からサマータイムが始まるかを設定します。 • 「Last」- 月の最後の週に設定します。 • 「First」- 月の最初の週に設定します。 • 「Second」- 月の 2 番目の週に設定します。 • 「Third」- 月の 3 番目の週に設定します。 • 「Fourth」- 月の 4 番目の週に設定します。
From: Day of the Week	サマータイムが開始する曜日を指定します。 • 選択肢：「Sunday」「Monday」「Tuesday」「Wednesday」「Thursday」「Friday」「Saturday」
From: Month	サマータイムが開始する月を指定します。 • 選択肢:「January」「February」「March」「April」「May」「June」「July」「August」「September」「October」「November」「December」
From: Time (HH:MM)	サマータイムが開始する時間を指定します。
To: Week of the Month	月の第何週でサマータイムが終わるかを設定します。 • 「Last」- 月の最後の週に設定します。 • 「First」- 月の最初の週に設定します。 • 「Second」- 月の 2 番目の週に設定します。 • 「Third」- 月の 3 番目の週に設定します。 • 「Fourth」- 月の 4 番目の週に設定します。
To: Day of the Week	サマータイムが終了する曜日を指定します。
To: Month	サマータイムが終了する月を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。 • 設定可能範囲：30-120 • 初期値：60（分）
Date Setting	
From: Date of the Month	サマータイムが開始する日にちを指定します。
From: Month	サマータイムが開始する月を指定します。
From: Year	サマータイムが開始する年を指定します。
From: Time (HH:MM)	サマータイムが開始する時間を指定します。
To: Date of the Month	サマータイムが終了する日にちを指定します。
To: Month	サマータイムが終了する月を指定します。
To: Year	サマータイムが終了する年を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。 • 設定可能範囲：30-120 • 初期値：60（分）

「Apply」ボタンをクリックして、設定内容を適用します。

SNTP Settings（SNTP 設定）

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

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

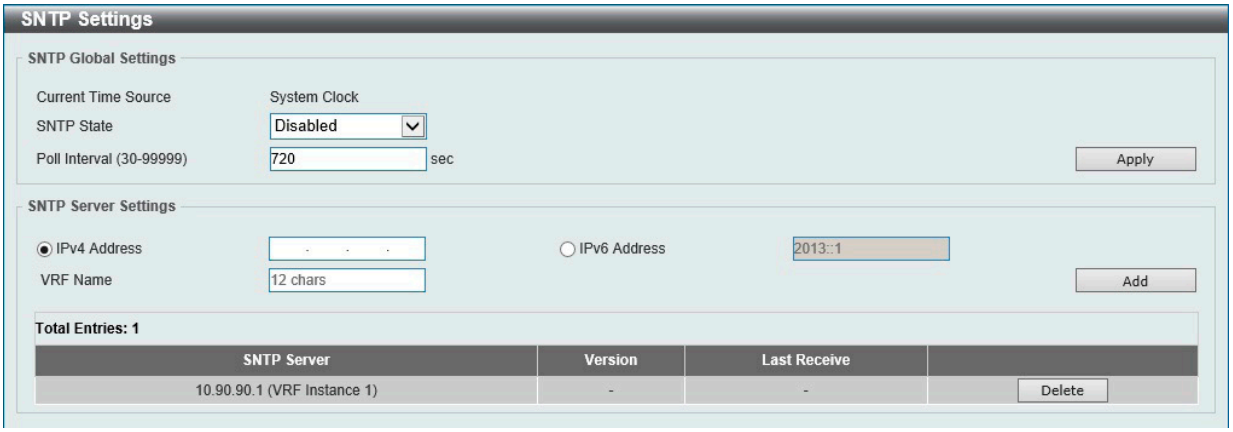


図 6-20　SNTP Settings 画面

画面に表示される項目：

項目	説明
SNTP Global Settings	
Current Time Source	現在の日付と時刻の提供元を表示します。
SNTP State	SNTP ステータス を有効 / 無効に設定します。
Poll Interval	同期する間隔を指定します。 • 設定可能範囲：30-99999（秒） • 初期値：720（秒）
SNTP Server Settings	
IPv4 Address	SNTP 情報の取得元であるサーバの IPv4 アドレスを設定します。
IPv6 Address	SNTP 情報の取得元であるサーバの IPv6 アドレスを設定します。
VRF Name（EI モードのみ）	VRF インスタンス名を指定します。（12 文字以内）

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

注意　一部の NTPv4 サーバについて、SNTP による時刻同期が出来ない場合があります。

Time Range（タイムレンジ設定）

スイッチの ACL 機能などで使用するスケジュールを定義します。

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

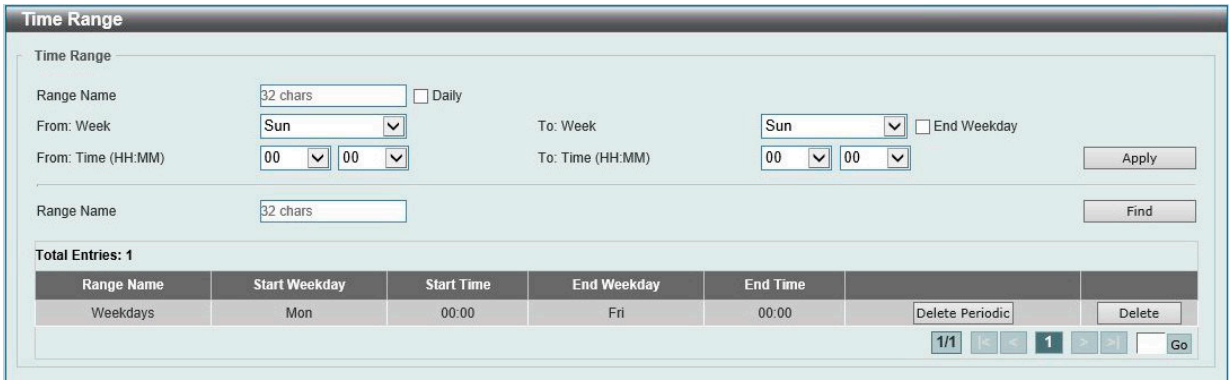


図 6-21　Time Range 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定のエントリを検索します。

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

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

PTP（PTP 設定）

System > PTP

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

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

同期プロセスは 2 つの処理に分かれます。

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

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

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

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

PTP Global Settings（PTP グローバル設定）

PTP 機能のグローバルステータスを設定します。

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

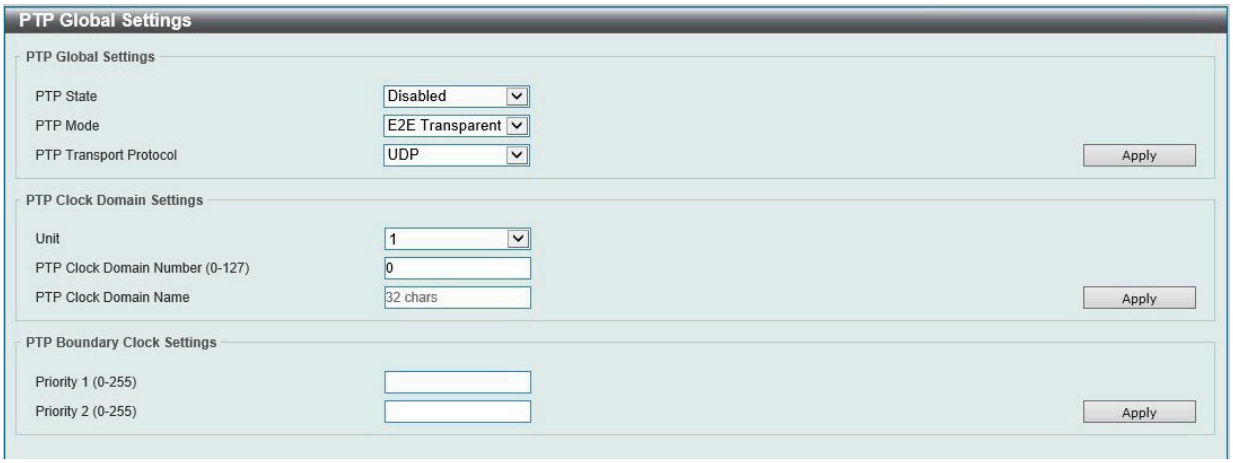


図 6-22　PTP Global Settings 画面

画面に表示される項目：

項目	説明
PTP Global Settings	
PTP State	PTP 機能を有効 / 無効に設定します。 PTP 機能が有効になっている場合、スイッチポートはフィールドを修正するために滞留時間を追加します。PTP 機能が無効の場合、すべてのポートはマルチキャストフィルタリングの設定に従って PTP パケットを転送します。
PTP Mode	PTP タイプを選択します。 • 「Boundary」- スイッチを境界クロックとして指定します。 • 「P2P Transparent」- スイッチをピアツーピア透過クロックとして指定します。これは、Precision Time Protocol（PTP）イベント通過時間の情報と、リンクの伝播遅延の補正を提供するクロックです。リンクは PTP イベントメッセージを受信しているポートに接続されます。ピアツーピア透過クロック上のポートは、ピア遅延メカニズムを使用して PTP ポート間の伝播遅延を計算します。 • 「E2E Transparent」- スイッチをエンドツーエンド透過クロックとして指定します。エンドツーエンド透過クロックは、スレーブクロックとマスタクロック間のエンドツーエンド遅延測定メカニズムの使用をサポートします。エンドツーエンド透過クロック上のポートは、伝搬遅延メカニズムに依存しません。
PTP Transport Protocol	PTP トランスポートプロトコルを選択します。 • 「Ethernet」- PTP のトランスポートプロトコルを IEEE802.3 Ethernet に指定します。 • 「UDP」- PTP のトランスポートプロトコルを IPv4 UDP に指定します。

項目	説明
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	PTP クロックドメイン番号を入力します。すべての PTP メッセージ、データセット、ステートマシン、その他すべての PTP エンティティは、常に特定のドメイン番号に関連付けられます。 • 設定可能範囲：0-127
PTP Clock Domain Name	PTP クロックドメイン名を入力します。（32 文字以内）この名前はユーザ参照用です。
PTP Boundary Clock Settings	
Priority 1	PTP 境界クロックの「Priority1」の値を入力します。この値は、「Best Master Clock（BMC）」の実行で使用されます。低い値ほど優先度は高くなります。「0」は最優先であることを示します。 • 設定可能範囲：0-255
Priority 2	PTP 境界クロックの「Priority2」の値を入力します。この値は、「Best Master Clock（BMC）」の実行で使用されます。低い値ほど優先度は高くなります。「0」は最優先であることを示します。 • 設定可能範囲：0-255 BMC アルゴリズムによる、Priority 1、クロックのクラス、クロックの精度の値に基づくクロックの順序付けが失敗する場合、Priority 2 属性を使用して、他のデバイスと比較して低い値を作成できます。

「Apply」ボタンをクリックして、設定内容を適用します。

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

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

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

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

ポート毎の PTP ステータスを設定します。

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



図 6-23　PTP Port Global Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

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。本設定は、PTP デバイスが境界タイプである場合に有効です。

System > PTP (Precise Time Protocol) > 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。

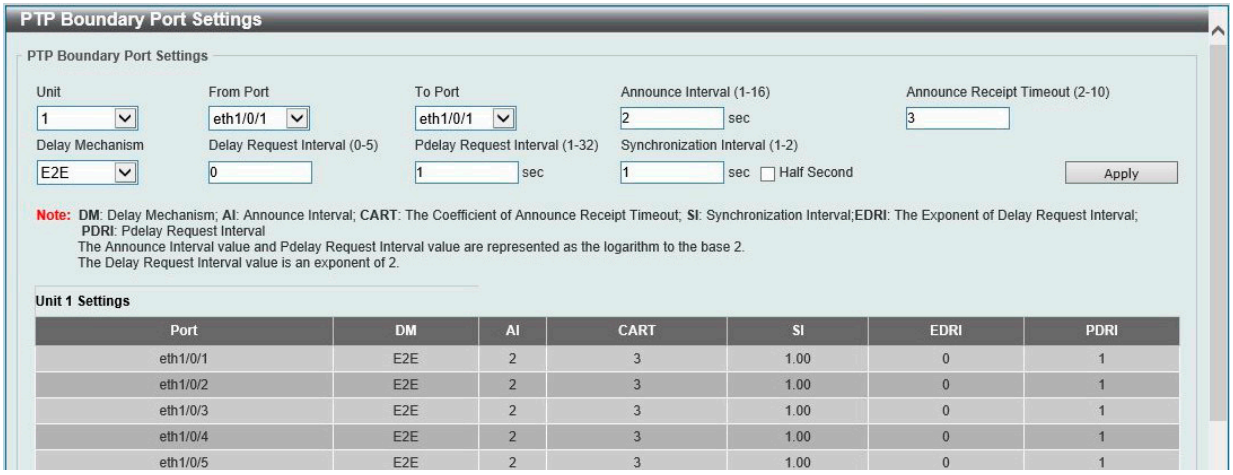


図 6-24　PTP Boundary Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Announce Interval	アナウンス間隔を入力します。連続するアナウンスメッセージの平均時間間隔を示します。 IEEE 1588 プロトコルにおいて、アナウンス間隔の値は、指数を 2 とするこの時間（秒）の対数とされています。 • 設定可能範囲：1-16（秒）
Announce Receipt Timeout	アナウンス受信タイムアウト値を入力します。アナウンスメッセージを受信しないまま所定時間が経過すると、ANNOUNCE_RECEIPT_TIMEOUT_EXPIRES イベントが発生します。ここで指定した値はアナウンス間隔値で乗算され、アナウンス受信タイムアウトの間隔に一致します。 • 設定可能範囲：2-10
Delay Mechanism	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」- Delay Request-response Mechanism を使用します。 •「P2P」- Peer Delay Mechanism を使用します。
Delay Request Interval	遅延要求間隔の値を入力します。これは、スレーブからマスタ上の特定のポートに送信される、連続した遅延要求メッセージ間の許容される平均時間間隔です。この値はマスタによって決定され、アドバタイズされます。IEEE 1588 プロトコルに準拠した遅延要求間隔の値は 2 の指数となります。また、この間隔の最小値は「Synchronization Interval」の整数値、最大値は「Synchronization Interval」の 32 倍である整数値となります。「Synchronization Interval」が 0.5 秒で、「Delay Request Interval」が「0」の場合、連続する遅延要求メッセージ間の許容時間間隔は自動的に 1 秒に調整されます。 • 設定可能範囲：0-5
Pdelay Request Interval	ピア遅延要求間隔の値を入力します。これは、連続するピア遅延要求メッセージ間で許容される平均時間間隔です。IEEE1588 プロトコルにおいてこの値は、底を 2 とするこの時間（秒）の対数とされています。 • 設定可能範囲：1-32（秒）
Synchronization Interval	同期間隔を入力します。連続する同期メッセージ間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この値は、2 を底とするこの時間（秒）の対数とされています。 • 設定可能範囲：1-2（秒） 「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、設定内容を適用します。

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。

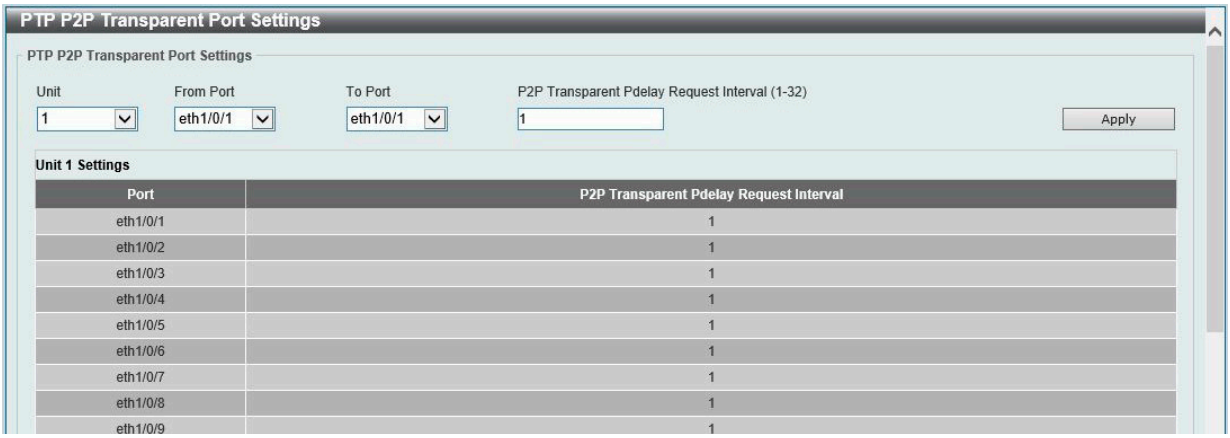


図 6-25　PTP P2P Transparent Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
P2P Transparent Pdelay Request Interval	P2P 透過ピア遅延要求間隔の値を入力します。 • 設定可能範囲：1-32

「Apply」ボタンをクリックして、設定内容を適用します。

PTP Clock Information（PTP クロック情報の表示）

PTP クロック情報を表示します。PTP クロックのアクティブ属性を表示します。

System > PTP (Precise Time Protocol) > 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。

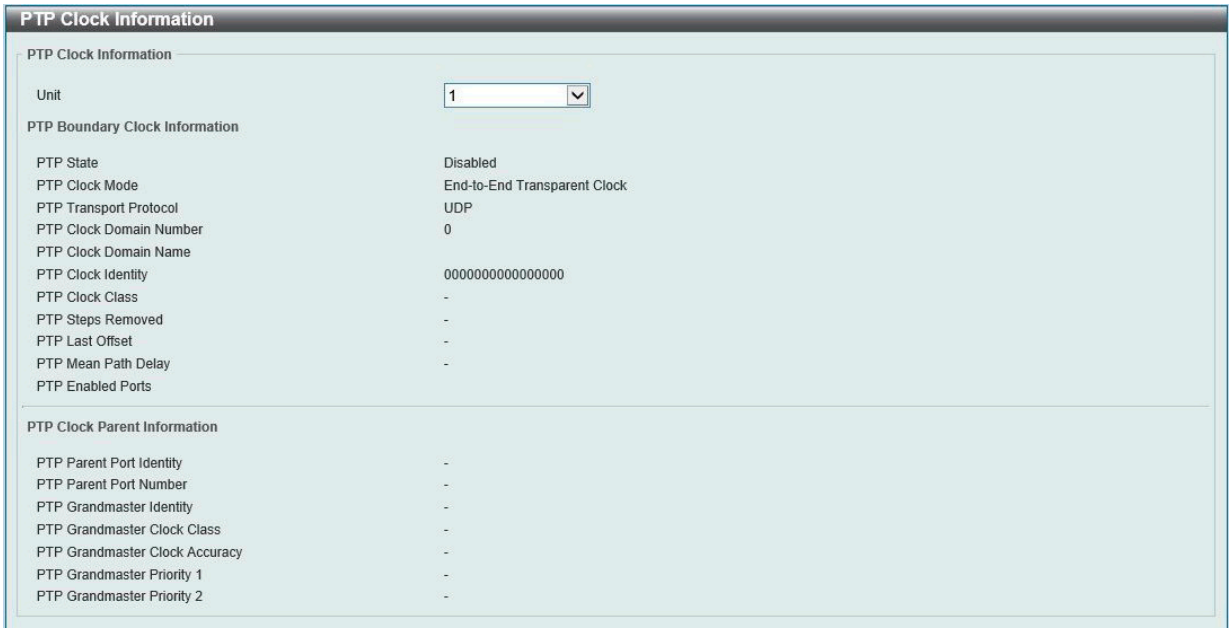


図 6-26　PTP Clock Information 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

PTP Port Information (PTP ポート情報)

PTP ポート情報を表示します。

System > PTP (Precise Time Protocol) > 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。

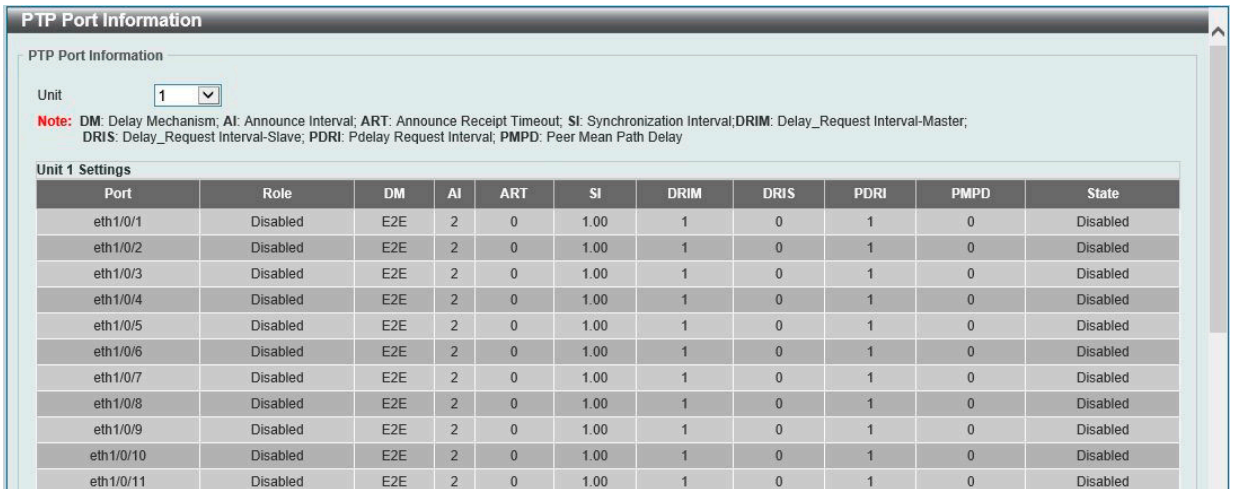


図 6-27　PTP Port Information 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

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

外部マスタレコードを表示します。

System > PTP (Precise Time Protocol) > 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。

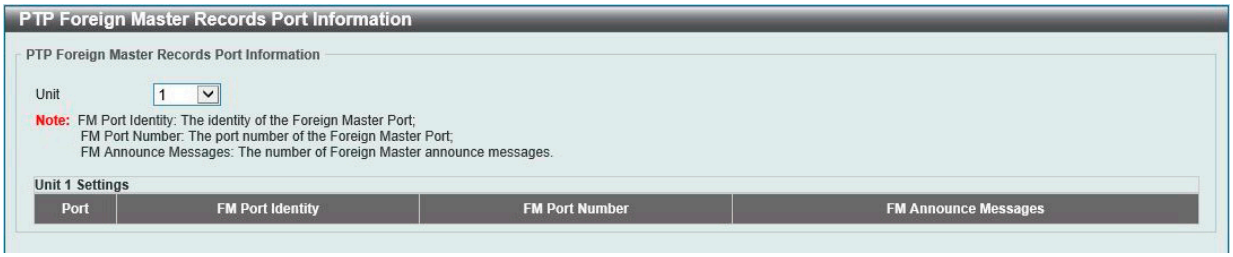


図 6-28　PTP Foreign Master Records Port Information 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

SRM（Switch Resource Management 設定）

System > SRM

SRM（Switch Resource Management）機能は、アプリケーションの要件に応じてリソースを分散および最適化する機能です。テーブルのエントリ数に応じたリソースを割り当て、未使用の機能でリソースを浪費しないようにすることで、リソースを柔軟に利用することができます。

SRM Prefer Current Settings（SRM 最適化設定）

SRM の設定、表示を行います。各種機能のリソース最適化で使用する SRM モードを指定します。

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 6-29　SRM Prefer Current Settings 画面

画面に表示される項目：

項目	説明
SRM Prefer Mode	SRM 設定モードを選択します。 • 「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、設定内容を適用します。

注意　SRM モードが指定されスイッチが再起動すると、テーブルサイズが変更されます。起動コンフィグレーションに定義されている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数を超えた場合、超過し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、スタック内のすべてのスイッチが同じ SRM モードに設定されている必要があります。

SRM Prefer Mode（SRM 設定モード）

SRM 設定モードの表示を行います。テーブルのエントリは固定値であり、機能ごとに許可された最大数となります。

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 6-30　SRM Prefer Mode 画面

画面に表示される項目：

項目	説明
SRM Prefer Mode	表示する SRM モードを選択します。 • 選択肢：「LAN」「IP」「L2VPN」

「Find」ボタンをクリックして、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。
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。
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、ファームウェア、コンフィグレーション情報、および Syslog 情報はフラッシュ内のファイルに保存されます。
Stacking（スタッキング設定）	物理スタッキングの設定を行います。
シングル IP マネジメント（SIM）設定	仮想（SIM）スタッキングの設定を行います。
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）	D-Link ディスカバリプロトコル（DDP）の設定を行います。
SMTP Settings（SMTP 設定）	Simple Mail Transfer Protocol (SMTP) の設定を行います。
Reboot Schedule Settings（再起動スケジュール設定）	スイッチの再起動スケジュール設定を行います。
NLB FDB Settings（NLB FDB 設定）	ネットワークロードバランシング (NLB) の設定を行います。

Command Logging（コマンドログ設定）

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

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

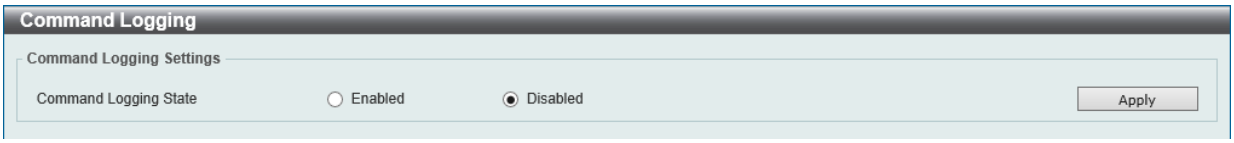


図 7-1　Command Logging 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

User Accounts Settings（ユーザアカウント設定）

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

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



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

画面に表示される項目：

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

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

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

Session Table

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

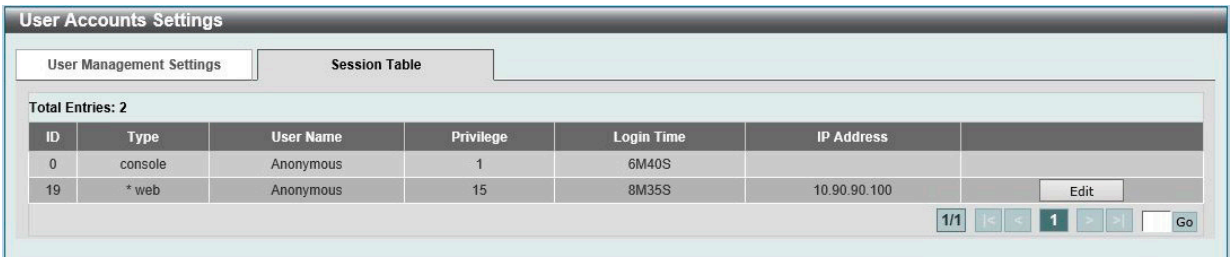


図 7-3　User Accounts Settings - Session Table 画面

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

■ User Privilege（ユーザ権限）

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



図 7-4　User Accounts Settings - User Privilege 画面

画面に表示される項目：

項目	説明
Action	ユーザレベルのセキュリティ設定を有効 / 無効に設定します。
Privilege	アカウントの権限レベルを指定します。 • 設定可能範囲：1-15
Password	パスワードを入力します。（32 文字以内）

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

Password Encryption（パスワード暗号化）

パスワードを暗号化して設定ファイルに保存します。

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



図 7-5　Password Encryption 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

Password Recovery（パスワードリカバリ）

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

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



図 7-6　Password Recovery 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

Login Method（ログイン方法）

各管理インタフェースへのログイン方法について表示、設定します。

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

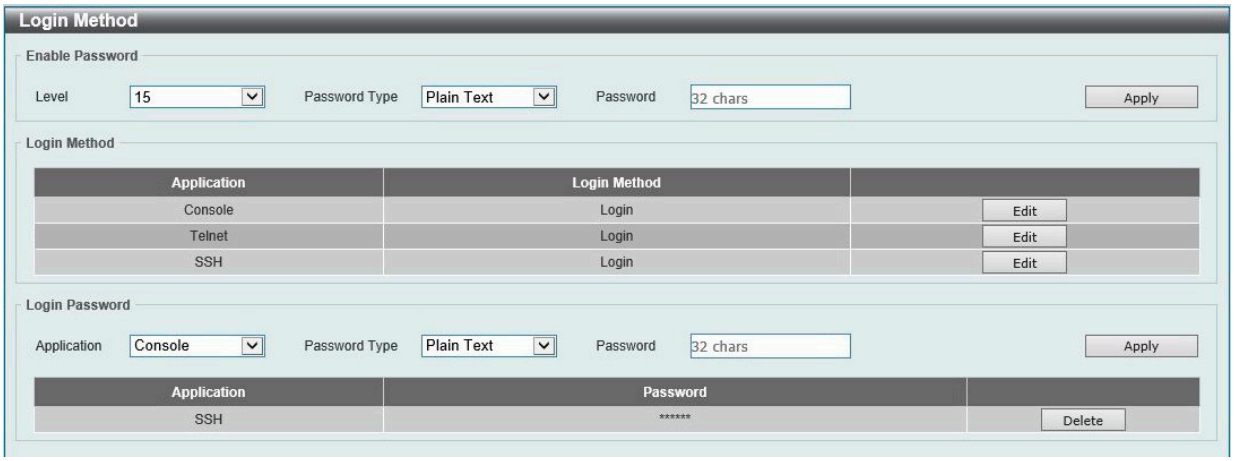


図 7-7　Login Method 画面

画面に表示される項目：

項目	説明
Enable Password	
Level	ユーザの権限レベルを指定します。 • 設定可能範囲：1-15
Password Type	暗号化の方法を選択します。 •「Plain Text」- パスワードはプレーンテキストで保存されます。（初期値） •「Encrypted-SHA1」- パスワードは「SHA-1」を使用して暗号化されます。 •「Encrypted-MD5」- パスワードは「MD-5」を使用して暗号化されます。
Password	ユーザアカウントのパスワードを入力します。 •「Plain Text」選択時：32 文字以内（大文字と小文字を区別、スペースを含める） •「Encrypted-SHA1」選択時：35 バイト（大文字と小文字を区別） •「Encrypted-MD5」選択時：31 バイト（大文字と小文字を区別）
Login Method	
Login Method	「Edit」ボタンをクリックしてパラメータの設定を行います。指定のアプリケーションへのログイン方法を選択します。 •「No Login」- 指定アプリケーションへアクセスするためのログイン認証は不要です。 •「Login」- 指定アプリケーションへアクセスするにはパスワードを入力する必要があります。 •「Login Local」- 指定アプリケーションへアクセスするにはユーザ名とパスワードの入力が必要になります。
Login Password	
Application	設定するアプリケーションを選択します。 • 選択肢：「Console」「Telnet」「SSH」
Password Type	暗号化の方法を選択します。 • 選択肢：「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」
Password	選択したアプリケーションで使用するパスワードを入力します。 指定のアプリケーションのログイン方法が「Login」に設定されている時のパスワードになります。 •「Plain Text」選択時：32 文字以内（大文字と小文字を区別、スペースを含める） •「Encrypted-SHA1」選択時：35 バイト（大文字と小文字を区別） •「Encrypted-MD5」選択時：31 バイト（大文字と小文字を区別）

「Apply」ボタンをクリックして、設定内容を適用します。
「Edit」ボタンをクリックすると、設定内容を編集できます。

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

SNMP（SNMP 設定）

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

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

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

■ SNMP のバージョンについて

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

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

● SNMPv1 と SNMPv2c

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

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

● SNMPv3

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

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

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

トラップ

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

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

MIB

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

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

SNMP Global Settings（SNMP グローバル設定）

SNMP およびトラップのグローバル設定を行います。

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

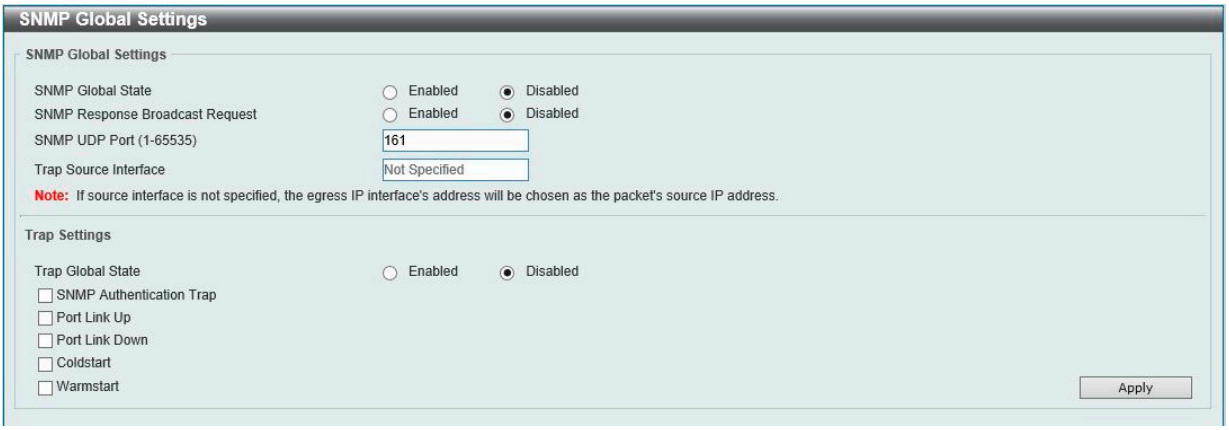


図 7-8　SNMP Global Settings 画面

画面に表示される項目：

項目	説明
SNMP Global Settings	
SNMP Global State	SNMP 機能を有効 / 無効に設定します。
SNMP Response Broadcast Request	ブロードキャスト SNMP GetRequest パケットに対するサーバの応答を有効 / 無効に設定します。
SNMP UDP Port	SNMP UDP ポート番号を指定します。
Trap Source Interface	SNMP トラップパケットを送信する送信元アドレスとして使用される IP アドレスのインタフェースを入力します。
Trap Settings	
Trap Global State	SNMP トラップを有効 / 無効に設定します。
SNMP Authentication Trap	SNMP 認証失敗の通知を有効にするには、本オプションにチェックを入れます。機器が正しく認証されていない SNMP メッセージを受信すると、authenticationFailuretrap トラップが生成されます。認証方法は使用している SNMP のバージョンによって異なります。SNMPv1 または SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。
Port Link Up	ポートリンクアップ通知を有効にするには、本オプションにチェックを入れます。通信リンクのいずれかが起動すると、linkUp トラップが生成されます。
Port Link Down	ポートリンクダウン通知を有効にするには、本オプションにチェックを入れます。通信リンクのいずれかがダウンすると、linkDown トラップが生成されます。
Coldstart	coldStart 通知を有効にするには、本オプションにチェックを入れます。
Warmstart	warmStart 通知を有効にするには、本オプションにチェックを入れます。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　SNMP Trap の送信元インタフェースは以下の仕様となります。

(1) mgmt 0 優先
(2) vlan interface から送信の場合は source-interface に従います。（connected の送信元 IP を使用しない）

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

SNMP リンクチェンジトラップを設定します。

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

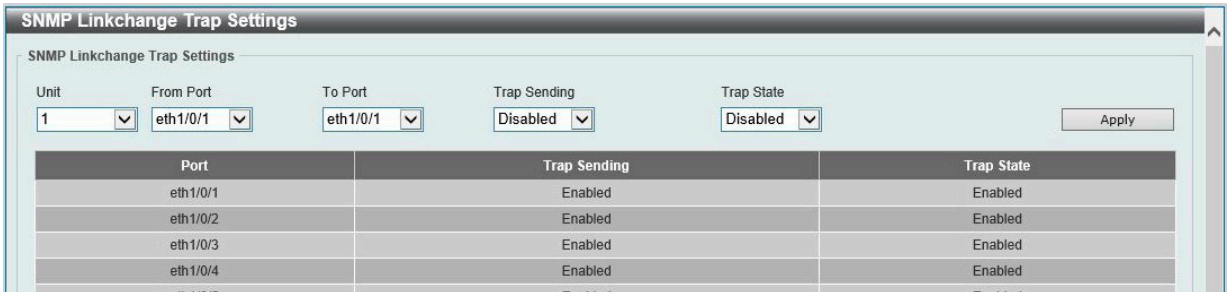


図 7-9　SNMP Linkchange Trap Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

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

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

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



図 7-10　SNMP View Table Settings 画面

画面に表示される項目：

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

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

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

SNMP マネージャとエージェントの関係を定義する SNMP コミュニティ名の登録を行います。コミュニティ名は、スイッチのエージェントへのアクセスを行う際のパスワードの役割をします。コミュニティ名に関連するアクセス制限は以下の通りです。

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

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



図 7-11　SNMP Community Table Settings 画面

画面に表示される項目：

項目	説明
Key Type	SNMP コミュニティのキーの種類を選択します。 • 選択肢：「Plain Text」「Encrypted」
Community Name	SNMP コミュニティメンバを識別するためのコミュニティ名を入力します。（半角英数字 32 文字以内）本コミュニティ名は、リモートの SNMP マネージャがスイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用されます。
View Name	ビュー名を入力します。（半角英数字 32 文字以内）リモート SNMP マネージャがアクセスすることのできる MIB グループの識別に使用します。「View Name」が「SNMP View Table」で定義されている必要があります。
Access Right	アクセス権限の種類を設定します。 •「Read Only」- 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りのみ可能となります。 •「Read Write」- 指定した Community Name を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取り、および書き込みが可能です。
IP Access-List Name	ユーザを制限するために使用するアクセスリストの名前を入力します。許可されるユーザは、コミュニティ文字列を使用して SNMP にアクセスすることができます。
Context Name	コンテキスト名を入力します。（32 文字以内）

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

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

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

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

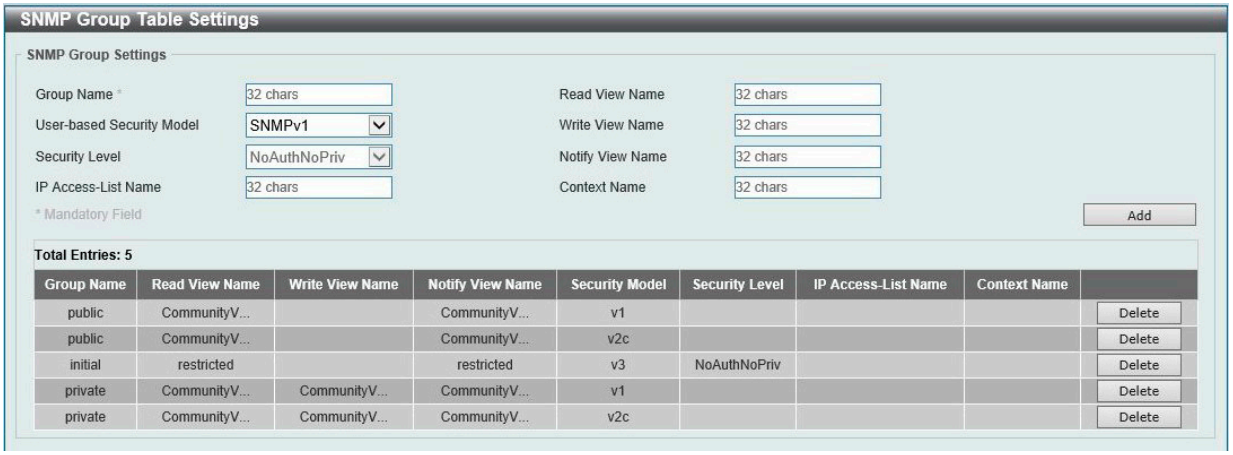


図 7-12　SNMP Group Table Settings 画面

画面に表示される項目：

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

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

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

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

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

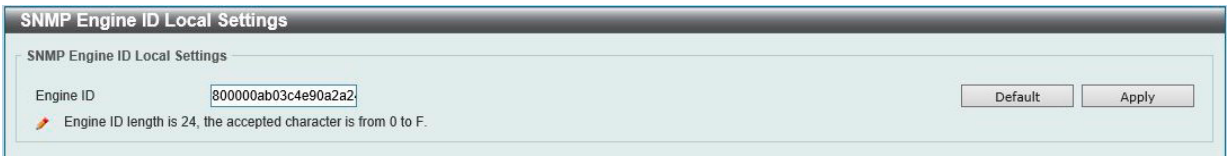


図 7-13　SNMP Engine ID Local Settings 画面

画面に表示される項目：

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

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

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

SNMP ユーザの登録、表示を行います。

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

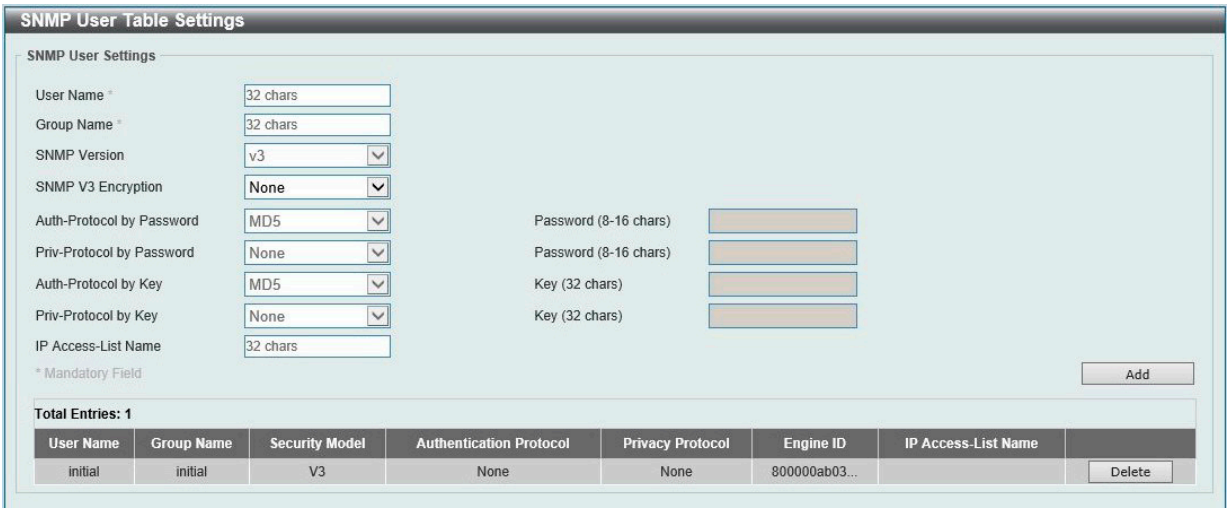


図 7-14　SNMP User Table Settings 画面

画面に表示される項目：

項目	説明
User Name	SNMP ユーザ名を入力します。（32 文字以内）
Group Name	ユーザが属する SNMP グループ名を入力します。（32 文字以内）
SNMP Version	SNMP v3 を使用することを指定します。
SNMP V3 Encryption	SNMP v3 に対して暗号化を有効にします。 • 選択肢：「None「Password」「Key」
Auth-Protocol by Password	「SNMP V3 Encryption」で「Password」を選択した場合に有効になります。本項目を選択後、「Password」にパスワードを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。（Password：半角英数字 8-16 文字） • 「SHA」- HMAC-SHA 認証プロトコルが使用されます。（Password：半角英数字 8-20 文字）
Priv-Protocol by Password	「SNMP V3 Encryption」で「Password」を選択した場合に有効になります。本項目を選択後、「Password」にパスワードを入力します。 • 「None」- 認証プロトコルは使用されていません。 • 「DES56」- CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されています。（Password：半角英数字 8-16 文字） • 「AES128」- AES 暗号が使用されます。（Password：半角英数字 8-16 文字）
Auth-Protocol by Key	「SNMP V3 Encryption」で「Key」を選択した場合に有効になります。本項目を選択後、「Key」に暗号キーを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。（Key：半角英数字 32 文字） • 「SHA」- HMAC-SHA 認証プロトコルが使用されます。（Key：半角英数字 40 文字）
Priv-Protocol by Key	「SNMP V3 Encryption」で「Key」を選択した場合に有効になります。本項目を選択後、「Key」に暗号キーを入力します。 • 「None」- 認証プロトコルは使用されていません。 • 「DES56」- CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されています。（Key：半角英数字 32 文字） • 「AES128」- AES 暗号が使用されます。（Key：半角英数字 32 文字）

項目	説明
IP Access-List Name	ユーザに関連付ける標準 IP アクセスコントロールリストの名前を入力します。

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

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

SNMP トラップの送信先を設定します。

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

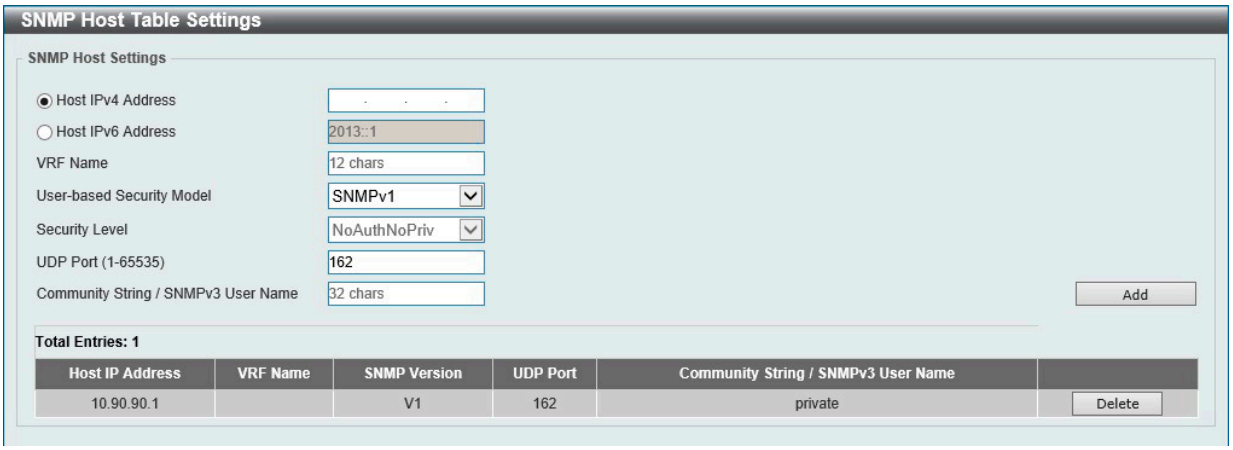


図 7-15　SNMP Host Table Settings 画面

画面に表示される項目：

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv6 アドレスを入力します。
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
User-based Security Model	SNMP バージョンを選択します。 • 「SNMPV1」- SNMP バージョン 1 を使用します。 • 「SNMPV2c」- SNMP バージョン 2c を使用します。 • 「SNMPV3」- SNMP バージョン 3 を使用します。
Security Level	「SNMPv3」を選択した場合、セキュリティレベルを設定します。 • 「NoAuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証も暗号化も行われません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証は行われますが暗号化は行われません。 • 「AuthPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証 / 暗号化が行われます。
UDP Port	UDP ポート番号を入力します。ポート番号によっては他のプロトコルと競合する可能性があります。 • 設定可能範囲：1-65535 • 初期値：162
Community String / SNMPv3 User Name	コミュニティ名または SNMP V3 ユーザ名を入力します。

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

SNMP Context Mapping Table Settings（SNMP コンテキストマッピングテーブル設定）

SNMP コンテキストマッピングテーブルの表示、設定を行います。

Management > SNMP > SNMP Context Mapping 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。

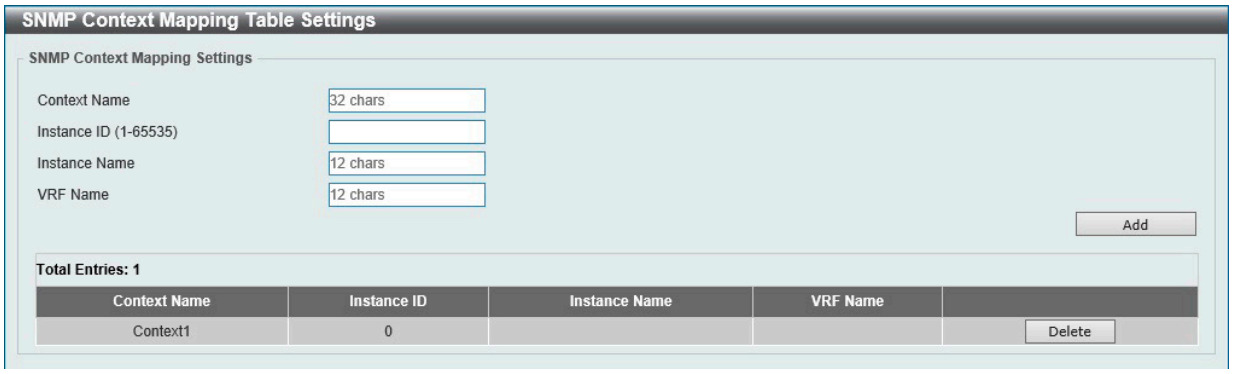


図 7-16　SNMP Context Mapping Table Settings 画面

画面に表示される項目：

項目	説明
Context Name	SNMP View-based Access Control Model（VACM）コンテキスト名を入力します。（32 文字以内）コンテキスト名の先頭はアルファベット、末尾はアルファベットまたは数字で設定することができます。それ以外はアルファベット、数字、ハイフンが使用可能です。
Instance ID	インスタンス ID を入力します。 • 設定可能範囲：1-65535
Instance Name	インスタンス名を入力します。（12 文字以内）
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）

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

RMON（RMON 設定）

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

RMON Global Settings（RMON グローバル設定）

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

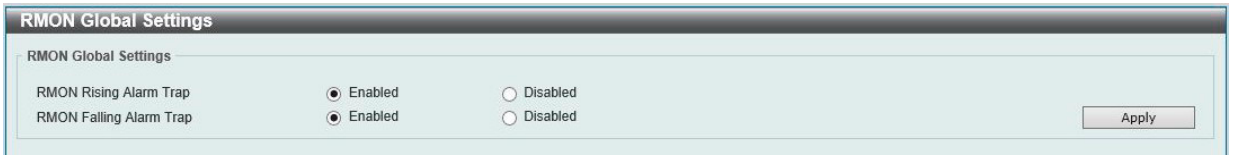


図 7-17　RMON Global Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

RMON Statistics Settings（RMON 統計情報）

RMON 統計情報を表示、設定します。

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



図 7-18　RMON Statistics Settings 画面

画面に表示される項目：

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

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Show Detail」ボタンをクリックして、特定のポートの VLAN の詳細情報を表示します。
複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

指定ポートの統計情報を表示する場合

「Show Detail」をクリックすると、以下の画面が表示されます。

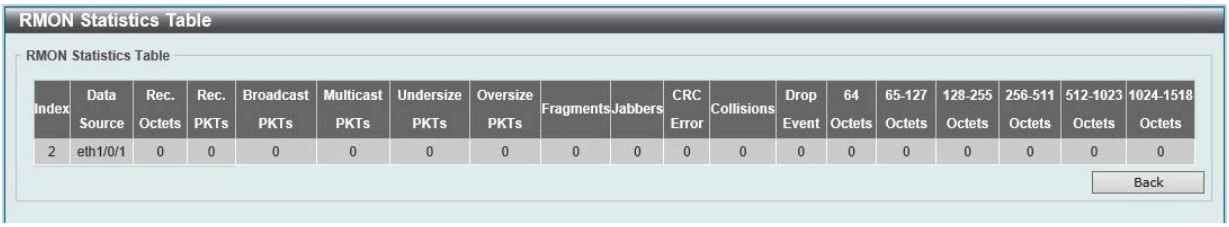


図 7-19　RMON Statistics Table 画面

前の画面に戻るには、「Back」ボタンをクリックします。

RMON History Settings（RMON ヒストリ設定）

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

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

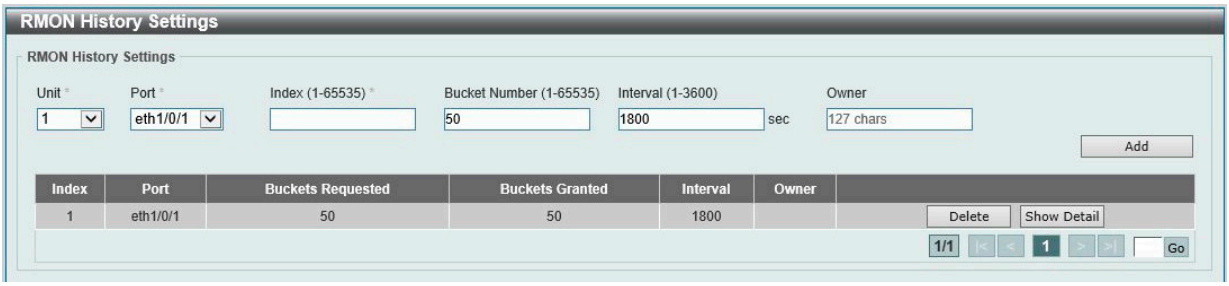


図 7-20　RMON History Settings 画面

画面に表示される項目：

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

「Add」ボタンをクリックして、エントリを追加します。

「Delete」ボタンをクリックして、エントリを削除します。

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

指定ポートの履歴情報を表示する場合

「Show Detail」をクリックすると、以下の画面が表示されます。



図 7-21　RMON History Table 画面

前の画面に戻るには、「Back」ボタンをクリックします。

RMON Alarm Settings（RMON アラーム設定）

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

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

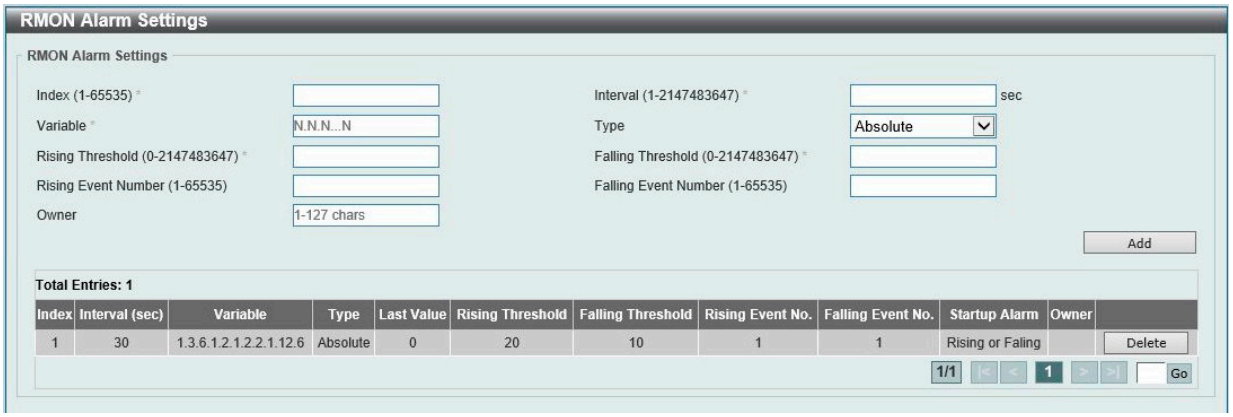


図 7-22　RMON Alarm Settings 画面

画面に表示される項目：

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

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

RMON Event Settings（RMON イベント設定）

RMON イベント統計情報の定義、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、以下の画面を表示します。

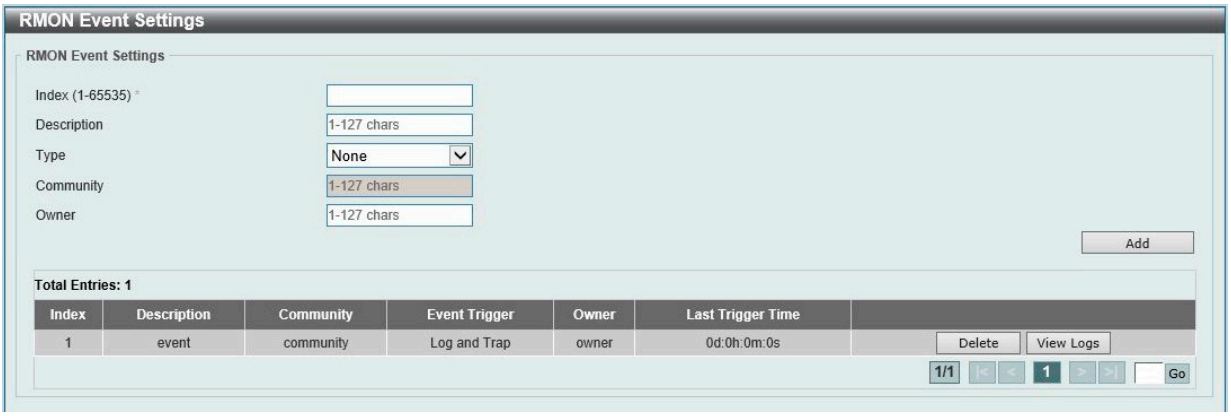


図 7-23　RMON Event Settings 画面

画面に表示される項目：

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

「Add」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「View Logs」ボタンをクリックして、特定のポートの詳細情報を表示します。
複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

指定エントリのログ情報を表示する場合

「View Logs」をクリックすると、以下の画面が表示されます。



図 7-24　Event Logs Table 画面

前の画面に戻るには、「Back」ボタンをクリックします。

Telnet/Web（Telnet/Web 設定）

スイッチの Telnet/Web 設定を行います。

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



図 7-25　Telnet/Web 画面

画面に表示される項目：

項目	説明
Telnet Settings	
Telnet State	Telnet サーバ機能を有効 / 無効に設定します。
Port	スイッチの Telnet 管理に使用する TCP ポート番号を入力します。Telnet プロトコルに通常使用される TCP ポートは 23 です。 • 設定可能範囲：1-65535
Source Interface	
Source Interface State	Source インタフェースの有効 / 無効を設定します。
Type	Source インタフェースの種類を指定します。 • 選択肢：「Loopback」「Mgmt」「VLAN」
Interface ID	インタフェース ID を指定します。 • 設定可能範囲：1-8（Loopback 選択時）、0（Mgmt 選択時）、1-4094（VLAN 選択時）
Web Interface	
Web State	Web ベースマネジメントの有効 / 無効を設定します。
Port	スイッチの Web ベース管理に使用される TCP ポート番号を入力します。Web プロトコルに通常使用される TCP ポートは 80 です。 • 設定可能範囲：1-65535

「Apply」ボタンをクリックして、設定内容を適用します。

Session Timeout（セッションタイムアウト）

各セッション（Web やコンソールなど）のタイムアウトの設定をします。

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

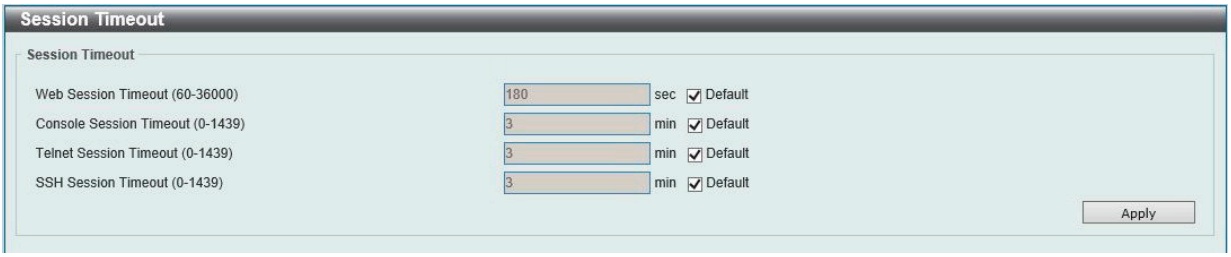


図 7-26　Session Timeout 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

注意　Telnet 経由で line telnet の session-timeout を変更しても、現在の Session に変更は反映されません。

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 サービスについて設定します。

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



図 7-27　Service DHCP 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

DHCP Class Settings（DHCP クラス設定）

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

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

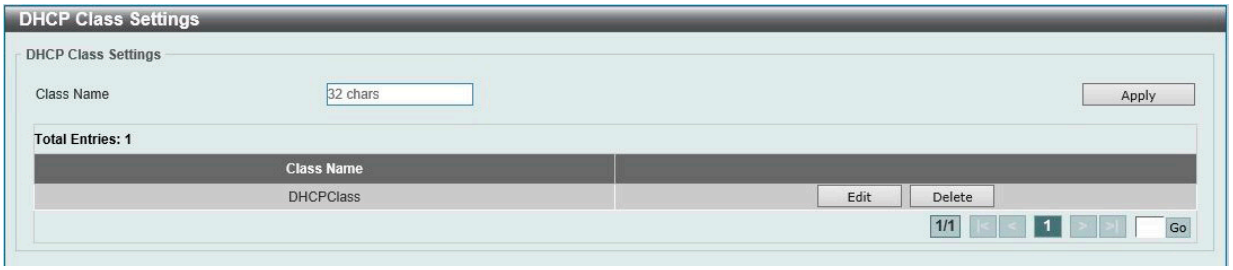


図 7-28　DHCP Class Settings 画面

画面に表示される項目：

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

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

指定エントリの編集を行う場合
「Edit」をクリックします。以下の画面が表示されます。

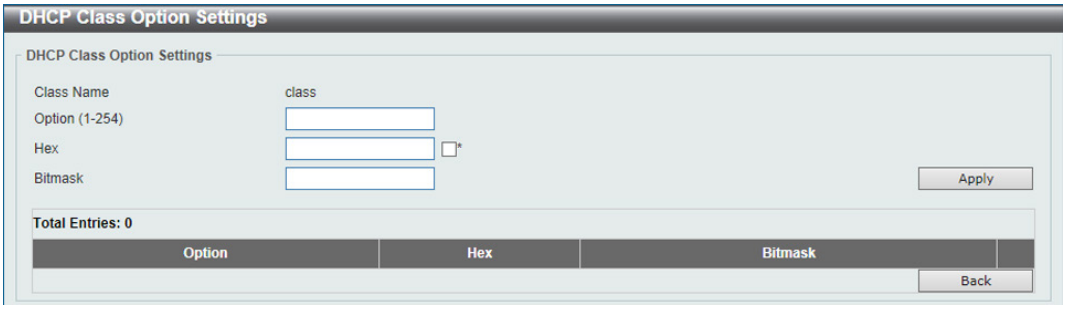


図 7-29　DHCP Class Option Settings（Edit）画面

画面に表示される項目：

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

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

前の画面に戻るには、「Back」ボタンをクリックします。

DHCP Pool Settings（DHCP プール設定）

DHCP プールの設定を行います。

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



図 7-30　DHCP Pool Settings 画面

画面に表示される項目：

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

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

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

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

DHCP Server（DHCP サーバ）

Management > DHCP > DHCP Server

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

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

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

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

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。

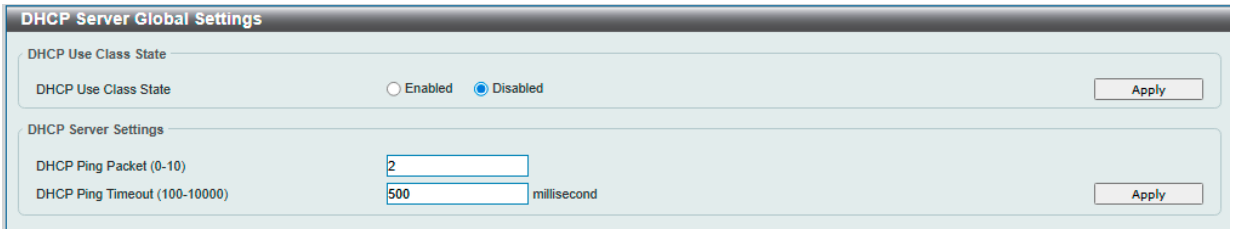


図 7-31　DHCP Server Global Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、各セクションで行った変更を適用します。

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

DHCP サーバプールの設定を行います。

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



図 7-32　DHCP Server Pool Settings 画面

画面に表示される項目：

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

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

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

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。

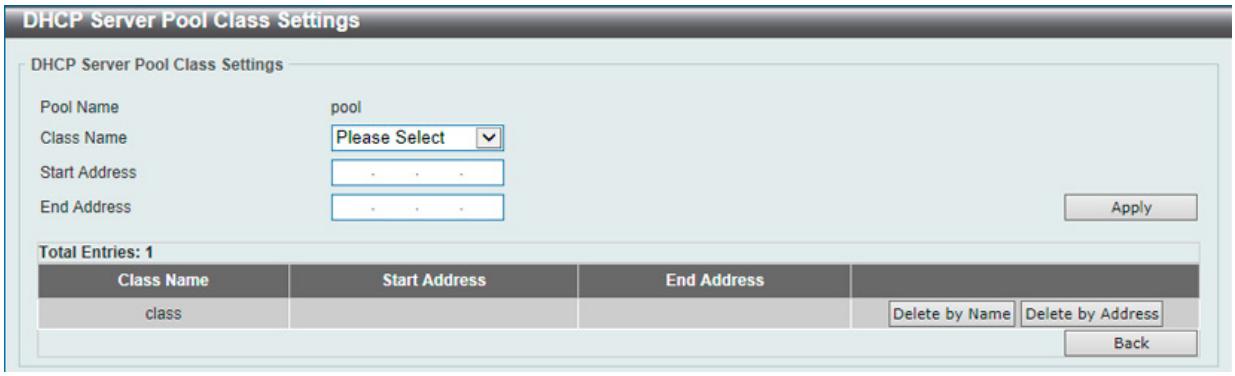


図 7-33　DHCP Server Pool Settings（Edit Class）- DHCP Server Pool Class Settings 画面

画面に表示される項目：

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

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

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

エントリの編集（Edit Option）

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



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

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

「Delete」ボタンをクリックして、エントリを削除します。

前の画面に戻るには、「Back」ボタンをクリックします。

エントリの編集（Configure）

「Configure」ボタンをクリックすると、以下の画面が表示されます。

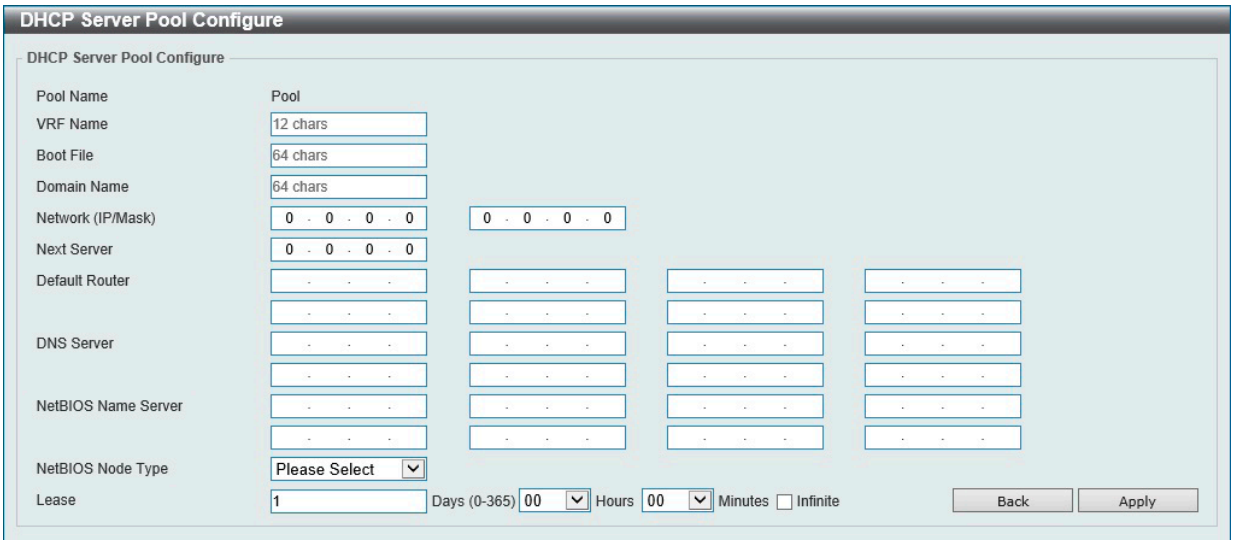


図 7-35　DHCP Server Pool Settings（Configure）- DHCP Server Pool Configure 画面

画面に表示される項目：

項目	説明
Pool Name	編集する DHCP プール名が表示されます。
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Boot File	ブートイメージのファイル名を指定します。（64 文字以内）
Domain Name	クライアントのドメイン名を入力します。（64 文字以内）
Network (IP/Mask)	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。

項目	説明
Next Server	ネクストサーバの IP アドレスを指定します。本サーバに格納されているブートイメージファイルが DHCP クライアントによって検索されます。一般的に TFTP サーバが使用されます。ネクストサーバの IP アドレスは 1 つのみ指定できます。
Default Router	DHCP クライアントのデフォルトルータの IP アドレスを入力します。最大 8 つの IP アドレスを指定できます。本ルータの IP アドレスはクライアントのサブネットと同じサブネットである必要があります。ルータは優先度の高い順に並んでいます。デフォルトルータが既に設定済みの場合、後から設定されたデフォルトルータはデフォルトルータリストに追加されます。
DNS Server	DHCP クライアントが使用する DNS サーバの IP アドレスを入力します。最大 8 つの IP アドレスを指定できます。DNS サーバは優先度の高い順に並んでいます。DNS サーバが既に設定済みの場合、後から設定された DNS サーバは DNS サーバリストに追加されます。
NetBIOS Name Server	DHCP クライアントが使用する WINS サーバの IP アドレスを指定します。最大 8 つの IP アドレスを指定できます。サーバは優先度の高い順に並んでいます。ネームサーバが既に設定済みの場合、後から設定されたネームサーバはネームサーバリストに追加されます。
NetBIOS Node Type	マイクロソフト DHCP クライアントの NetBIOS ノードタイプを指定します。このオプションでは、NetBIOS において登録および名前解決に使用する方法を選択します。 • 「Broadcast」- システムはブロードキャストを使用します。 • 「Peer to Peer」（p-node）- ネームサーバ（WINS）に対して Peer to Peer による名前クエリのみを使用します。 • 「Mixed」（m-node）- まずブロードキャストを使用し、その後ネームサーバへの問い合わせを行います。 • 「Hybrid」（h-node）- まずネームサーバへの問い合せを行い、その後ブロードキャストを使用します。 「Hybrid」を使用することを推奨します。
Lease	アドレスプールから割り当てるアドレスのリース期間を指定します。 • 「Days」- リースする日数（0-365） • 「Hours」- リースする時間（時） • 「Minutes」- リースする時間（分） • 「Infinite」- リース期間が無制限

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

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

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

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



図 7-36　DHCP Server Exclude Address 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Begin Address	除外する IP アドレス範囲の開始 IP アドレスを指定します。
End Address	除外する IP アドレス範囲の終了 IP アドレスを指定します。

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

DHCP Server Manual Binding Ext（拡張 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 アドレス間のマッピングです。手動のバインディングエントリによって、IP アドレスとクライアント識別子をバインディング、または IP アドレスと MAC アドレスをバインディングすることができます。

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

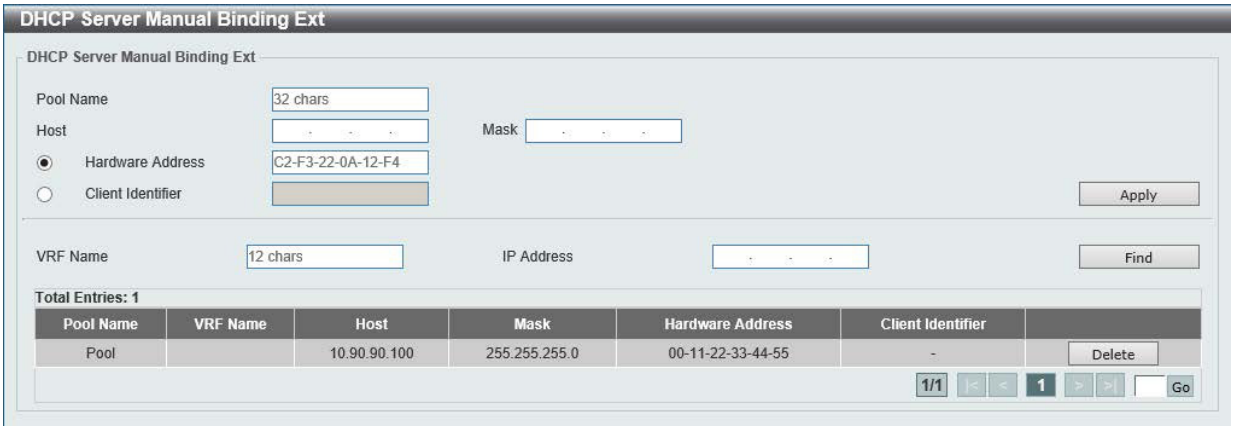


図 7-37　DHCP Server Manual Binding Ext 画面

画面に表示される項目：

項目	説明
Pool Name	マニュアルバインディングエントリを作成する DHCP プール名を入力します。（32 文字以内）
Host	DHCP ホストの IP アドレスを入力します。
Mask	DHCP ホストのネットワークのサブネットマスクを入力します。
Hardware Address	DHCP ホストの MAC アドレスを入力します。
Client Identifier	DHCP ホスト識別子を 16 進数表記で指定します。クライアント識別子はメディアタイプと MAC アドレスによってフォーマットされています。
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
IP Address	ホストの IP アドレスを入力します。

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

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

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

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

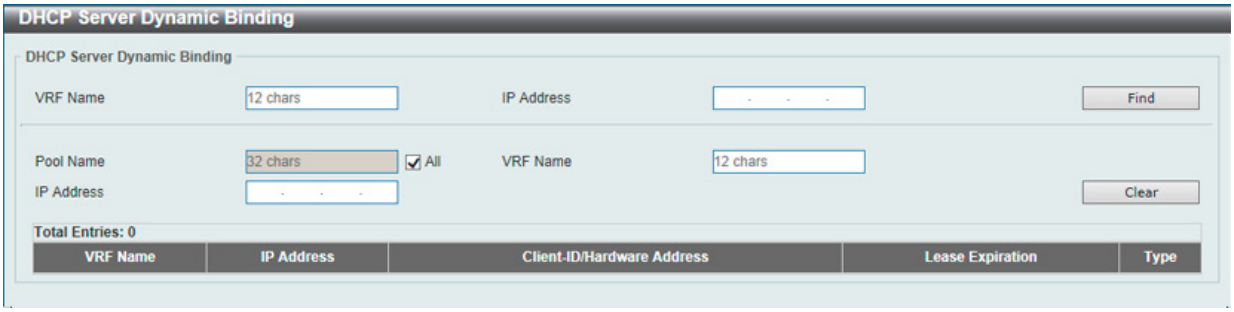


図 7-38　DHCP Server Dynamic Binding 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
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。
Pool Name	DHCP サーバプール名を入力します。「All」オプションにチェックを入れると、全てのプールのバインディングエントリを削除します。
Binding IP Address	バインディング IP アドレスを入力します。

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

DHCP Server IP Conflict（DHCP サーバ IP 重複）

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

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

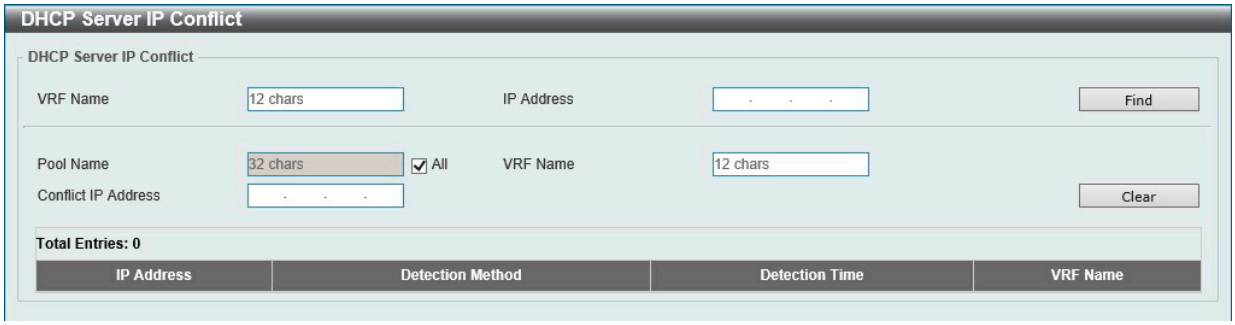


図 7-39　DHCP Server IP Conflict 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
IP Address	検出する重複エントリの IPv4 アドレスを入力します。
Pool Name	DHCP サーバプール名を入力します。「All」オプションにチェックを入れると、全てのプールの重複エントリを削除します。
Conflict IP Address	クリアする重複エントリの IPv4 アドレスを入力します。

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

DHCP Server Statistics（DHCP サーバ統計）

DHCP サーバの統計情報を表示します。

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

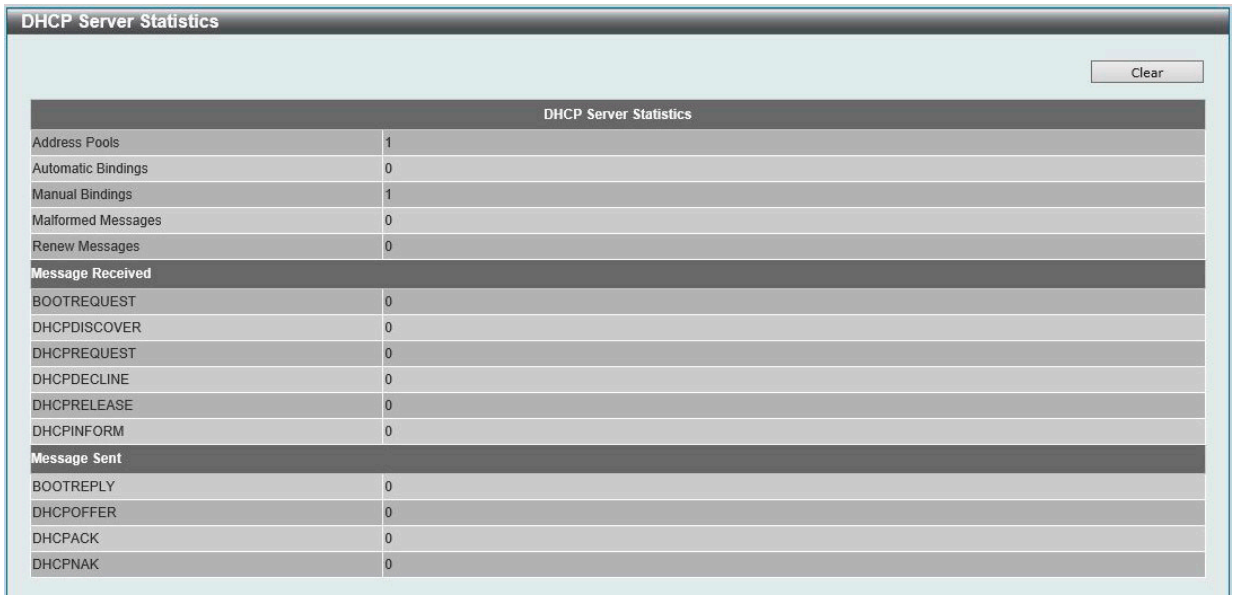


図 7-40　DHCP Server Statistics 画面

「Clear」ボタンをクリックして、統計情報をクリアします。

DHCPv6 Server（DHCPv6 サーバ設定）

Management > DHCP > DHCPv6 Server

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

注意 DHCPv6 サーバ機能について、バインディングエントリが存在しない Rebind パケットを無視します。

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

DHCPv6 プールの作成および設定を行います。

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



図 7-41　DHCPv6 Server Pool Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Configure」ボタンをクリックして、該当エントリの編集を行います。
複数ページ存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動することができます。

エントリの編集（Configure）
「Configure」ボタンをクリックすると、以下の画面が表示されます。

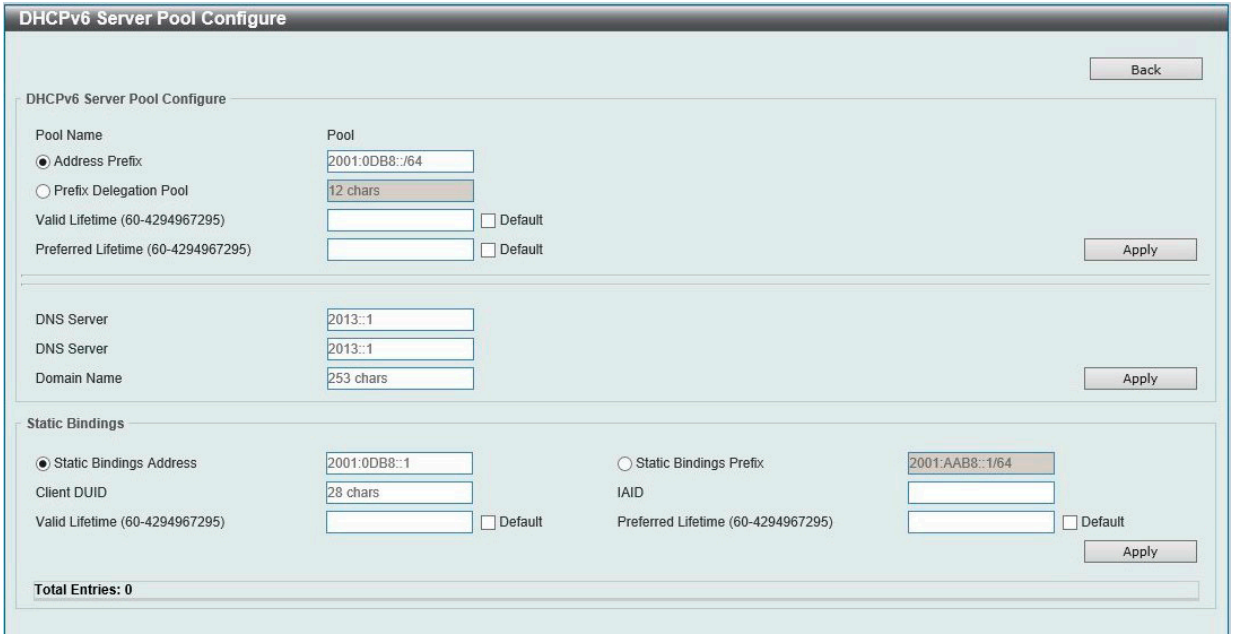


図 7-42　DHCPv6 Server Pool Settings (Configure) - DHCPv6 Server Pool Configure 画面

画面に表示される項目：

項目	説明
DHCPv6 Server Pool Configure	
Address Prefix	DHCPv6 サーバプール IPv6 ネットワークアドレスとプレフィックス長を入力します。（例：2015::0/64）
Prefix Delegation Pool	DHCPv6 サーバプールプレフィックス委任名を入力します。（12 文字以内）
Valid Lifetime	IPv6 アドレスが有効な状態を維持する時間を入力します。「Preferred Lifetime」よりも大きい値である必要があります。 • 設定可能範囲：60-4294967295（秒） • 初期値：2592000（秒）（30 日） 「default」にチェックを入れると、初期値が使用されます。

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

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

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

DHCPv6 サーバローカルプールの表示および設定を行います。

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

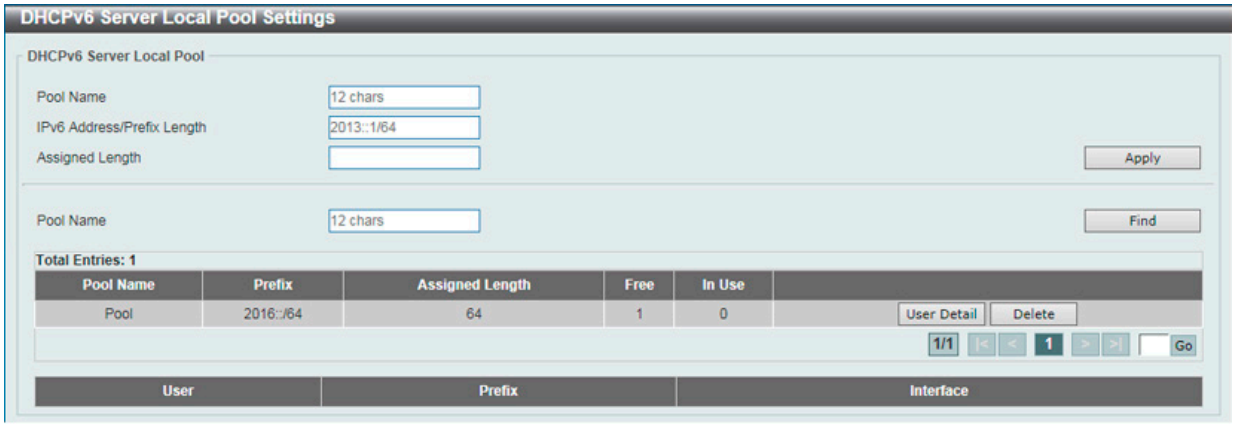


図 7-43　DHCPv6 Server Local Pool Settings 画面

画面に表示される項目：

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

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

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

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

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

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



図 7-44　DHCPv6 Server Exclude Address 画面

画面に表示される項目：

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

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

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。

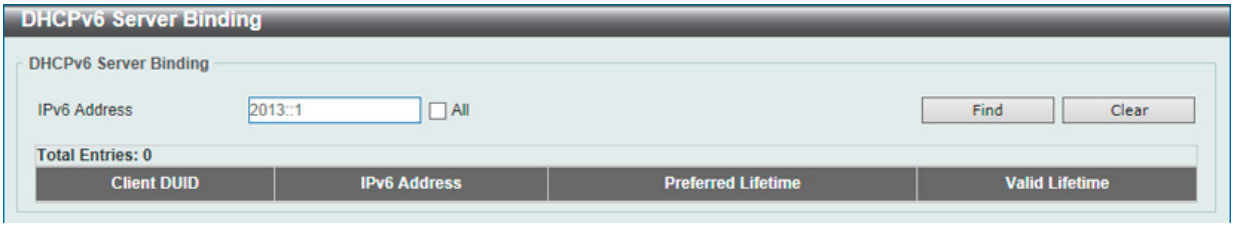


図 7-45　DHCPv6 Server Binding 画面

画面に表示される項目：

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

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

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。

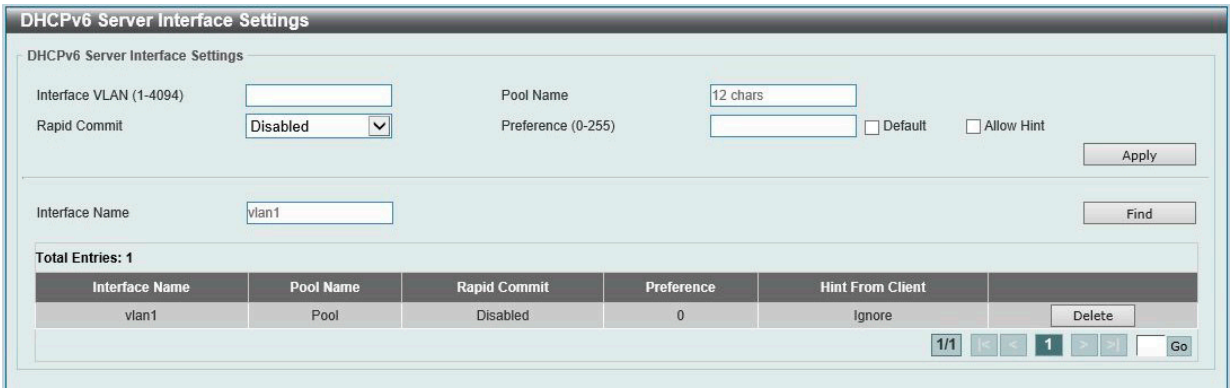


図 7-46　DHCPv6 Server Interface Settings 画面

画面に表示される項目：

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

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

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

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

DHCPv6 サーバ状態を表示します。

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

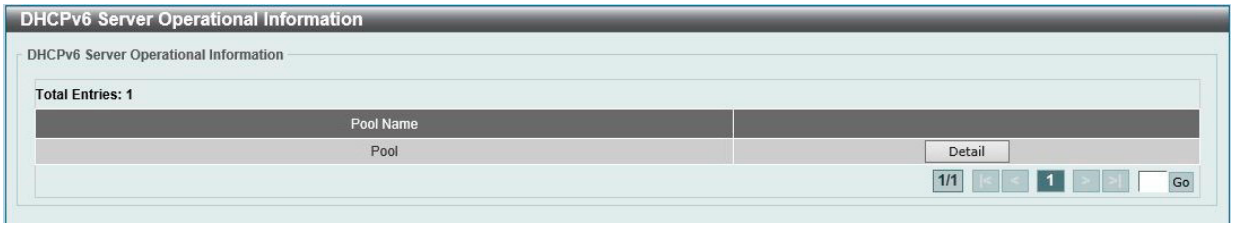


図 7-47　DHCPv6 Server Operational Information 画面

「Detail」ボタンを選択すると、以下の画面が表示されます。

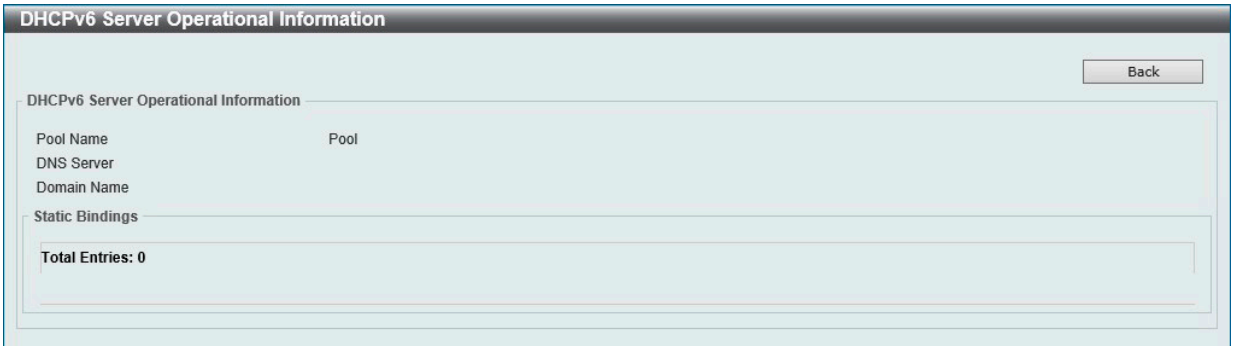


図 7-48　DHCPv6 Server Operational Information - Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

DHCP Relay（DHCP リレー）

Management > DHCP > DHCP Relay

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。

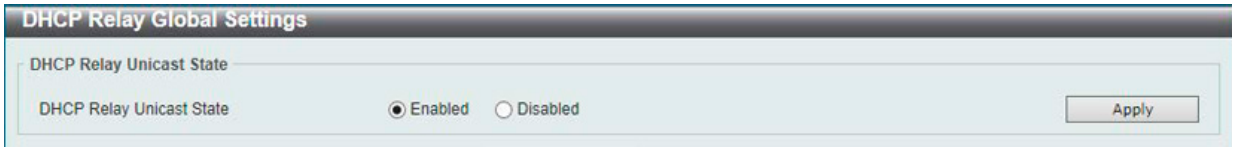


図 7-49　DHCP Relay Global Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

注意　DHCP リレーが有効の場合、discover パケットが対象 VLAN 内に flooding されません。

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

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

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



図 7-50　DHCP Relay Pool Settings 画面

画面に表示される項目：

項目	説明
Pool Name	プール名を指定します。（32 文字以内）

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

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

各プールエントリの編集を行う（Edit）

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

■「Source」の編集を行う場合

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

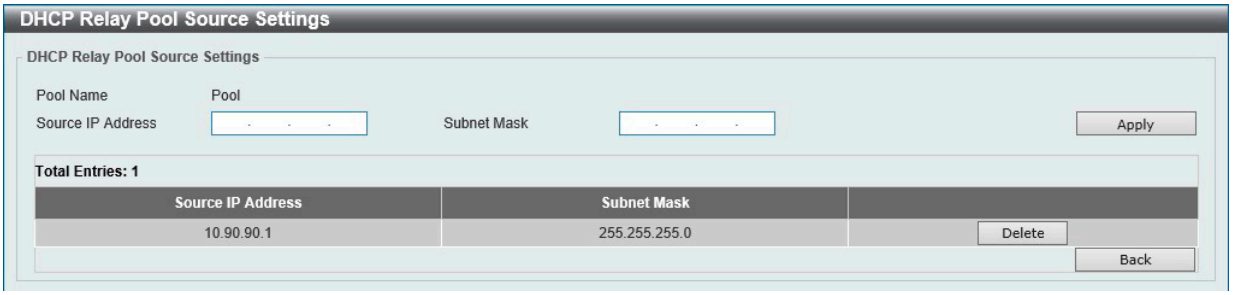


図 7-51　DHCP Relay Pool Source Settings 画面

画面に表示される項目：

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

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

前の画面に戻るには、「Back」ボタンをクリックします。

■「Destination」の編集を行う場合

「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 7-52　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 （EI モードのみ）	VRF のステータスを指定します。 • 選択肢：「True」「False」
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内） 「Global」オプションにチェックを入れると、IP アドレスはグローバルアドレスから選択されます。
Relay Destination	リレー宛先 DHCP サーバの IP アドレスを入力します。

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

前の画面に戻るには、「Back」ボタンをクリックします。

■ 「Class」の編集を行う場合

「Class」下の「Edit」をクリックします。以下の画面が表示されます。

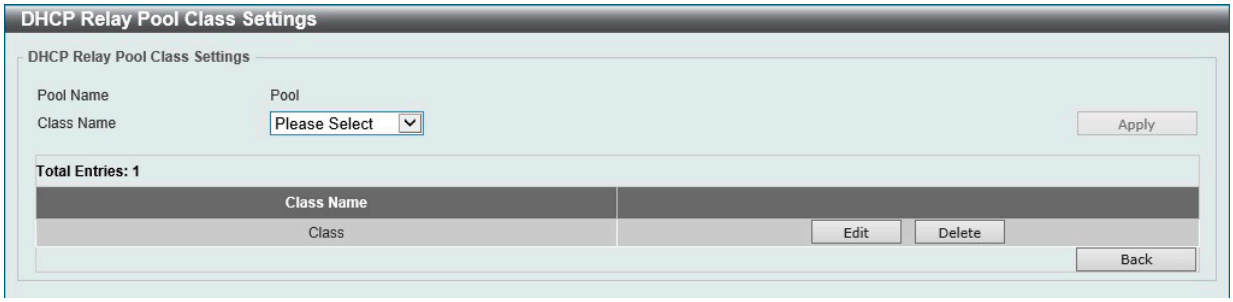


図 7-53　DHCP Relay Pool Class Settings 画面

画面に表示される項目：

項目	説明
Class Name	DHCP クラスの名前を選択します。

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

前の画面に戻るには、「Back」ボタンをクリックします。

クラス名の横の「Edit」をクリックすると以下の画面が表示されます。

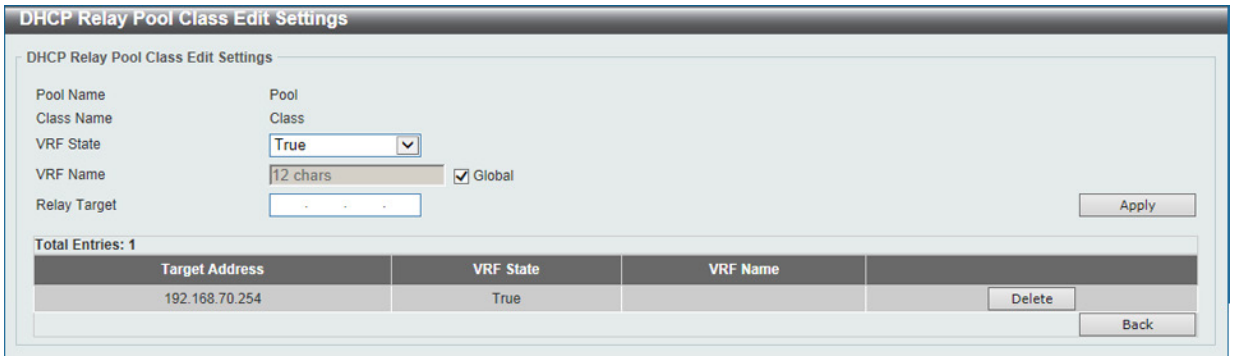


図 7-54　DHCP Relay Pool Class Edit Settings 画面

画面に表示される項目：

項目	説明
VRF State （EI モードのみ）	VRF のステータスを指定します。 • 選択肢：「True」「False」
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内） 「Global」オプションにチェックを入れると、IP アドレスはグローバルアドレスから選択されます。
Relay Target	DHCP クラスで設定したオプションの値パターンと一致するパケットをリレーする DHCP リレーターゲットを入力します。

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

前の画面に戻るには、「Back」ボタンをクリックします。

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

DHCP リレー情報の設定を行います。

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

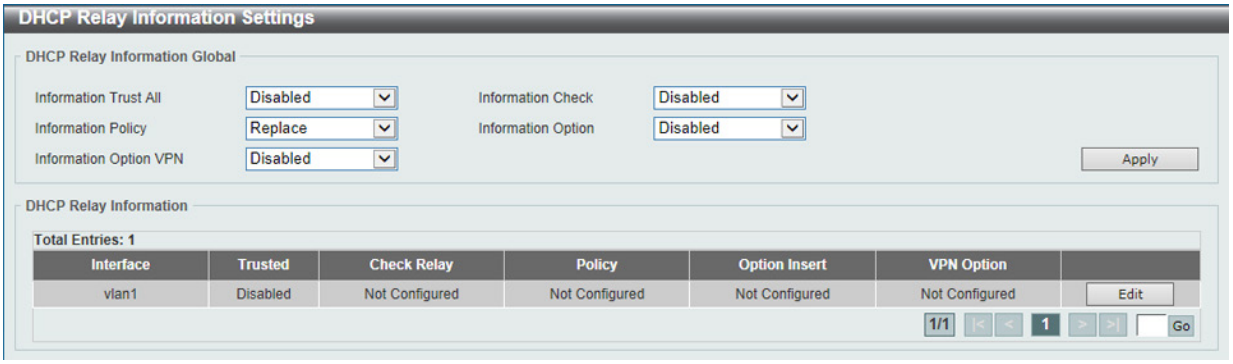


図 7-55　DHCP Relay Information Settings 画面

画面に表示される項目：

項目	説明
Information Trust All	すべてのインタフェースで DHCP リレーエージェントによる IP DHCP リレーインフォメーションへの信頼を有効 / 無効に設定します。
Information Check	DHCP リレーエージェントによる、受信した DHCP リレーパケットに含まれるリレーエージェントインフォメーションの検証と破棄を有効 / 無効に設定します。
Information Policy	DHCP リレーエージェントのオプション 82 再転送ポリシーを選択します。 • 「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。 • 「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。
Information Option	DHCP リクエストパケットがリレーされる間のリレーエージェント情報（Option82）の挿入を有効 / 無効に設定します。
Information Option VPN	情報オプションの VPN 機能を有効 / 無効に設定します。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 / 無効に設定するために使用します。

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

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

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

DHCP 情報フォーマットの表示、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。

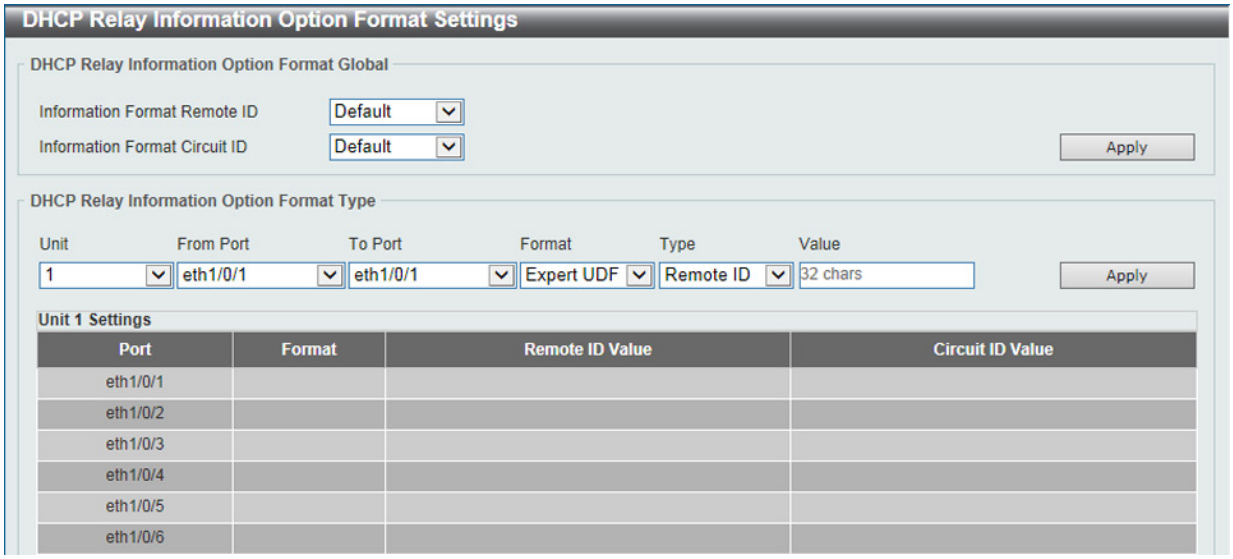


図 7-56　DHCP Relay Information Option Format Settings 画面

画面に表示される項目：

項目	説明
DHCP Relay Information Option Format Global	
Information Format Remote ID	「DHCP information remote ID」のサブオプションを選択します。 • 「Default」- リモート ID 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を選択します。
Information Format Circuit ID	「DHCP information circuit ID」のサブオプションを選択します。 • 「Default」- 初期値のサーキット ID を使用します。 • 「User Define」- ユーザ定義のサーキット ID を使用します。（32 文字以内） • 「Vendor1」- サーキット ID はベンダ 1 を使用します。 • 「Expert UDF」- Expert UDF サーキット ID を使用します。スタンドアロンのユニットフォーマットを選択します。
DHCP Relay Information Option Format Type	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Format	Expert UDF フォーマットを指定します。
Type	リレー情報オプションの種類を選択します。 • 選択肢：「Remote ID」「Circuit ID」
Value	オプション 82 情報として、リモート / サーキット ID サブオプションに含まれるベンダ定義の文字列を入力します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

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。

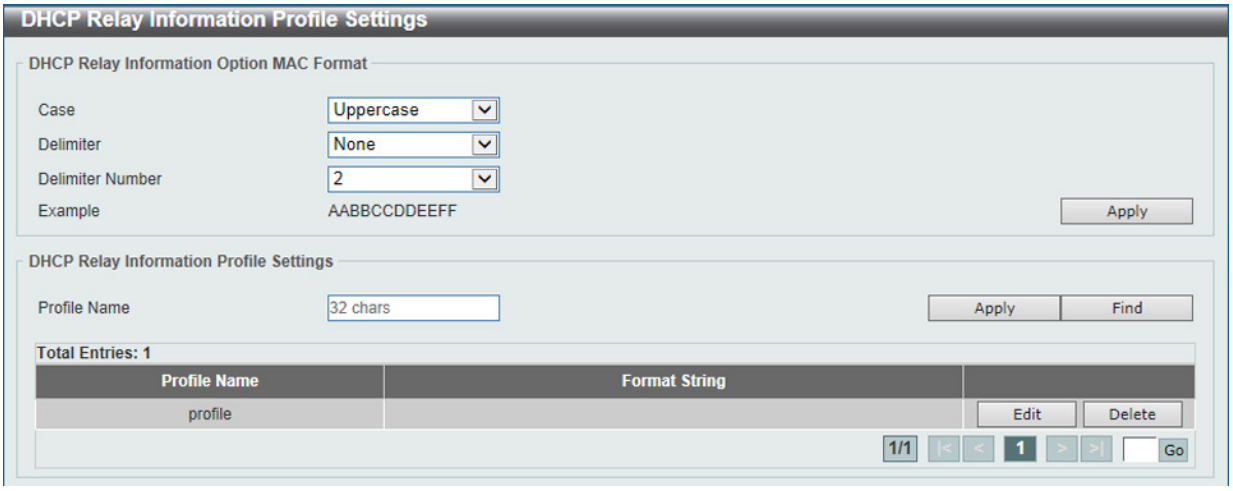


図 7-57　DHCP Relay Information Profile Settings 画面

画面に表示される項目：

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 アドレスの形式を選択します。 • 「Lowercase」- 小文字を使用します。（例：aa-bb-cc-dd-ee-ff） • 「Uppercase」- 大文字を使用します。（例：AA-BB-CC-DD-EE-FF）
Delimiter	MAC アドレスを入力する際の区切りを選択します。区切り文字を持たない場合には「None」を選択します。各項目の例は次の通りです。 • 「Hyphen」（ハイフン）-「 AA-BB-CC-DD-EE-FF」 • 「Colon」（コロン）-「 AA:BB:CC:DD:EE:FF」 • 「Dot」（ドット）-「 AA.BB.CC.DD.EE.FF」 • 「None」（なし）-「 AABBCCDDEEFF」
Delimiter Number	MAC アドレスにおける区切り数を選択します。各項目の例は次の通りです。 • 「1」-「AABBCC.DDEEFF」 • 「2」-「AABB.CCDD.EEFF」 • 「5」-「AA.BB.CC.DD.EE.FF」
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。プロファイルにより、ユーザ定義の Option82 エントリを作成します。
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 文字以内）ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた形式（例："Ethernet"）とします。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列と 16 進数の両方を含むことができます。 • 「%」の後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。（オプション）フォーマットキー文字列において文字長オプションの指定文字数（バイト数）を満たすために使用されます。 - 「$」はスペース（0x20）を埋めます。 - 「0」は（0）を埋めます。「0」が初期値です。 • 「1-32」は文字長オプションです。（オプション）キー文字列に変換される文字やバイトの文字数 / バイト数を指定します。変換されたキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。 • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。 - 「devtype」は機器のモデル名です。ASCII 文字列のみ有効です。 - 「sysname」はスイッチのシステム名を意味します。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。

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。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。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 0 です。 - 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「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、この最後の文字（":"）は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットされたキー文字列を任意に組み合わせることができます。「\」はエスケープ文字であり、「\」の後の特殊文字はそのままになります。例えば「\%」は「%」を意味し、フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列に含まれないスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。

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

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

DHCP リレーポートの設定、表示を行います。

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

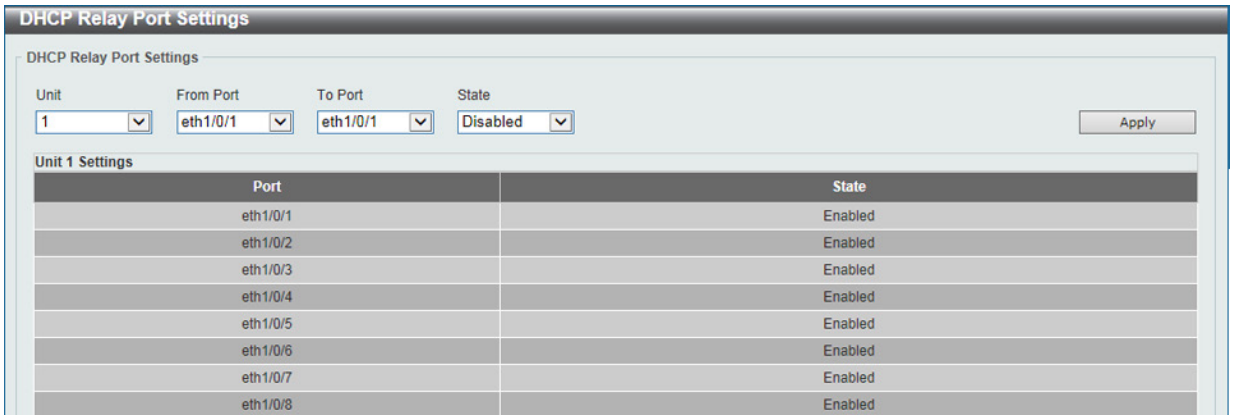


図 7-58　DHCP Relay Port Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

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

VLAN、またはグループ VLAN のリレー設定を行います。

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

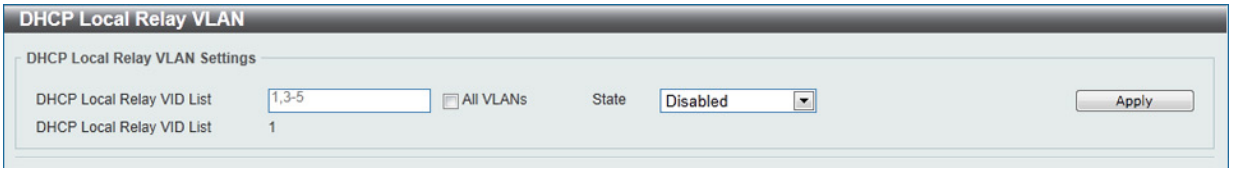


図 7-59　DHCP Local Relay VLAN 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

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

DHCPv6 Relay（DHCPv6 リレー）

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

スイッチの DHCPv6 リレー機能を設定します。

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

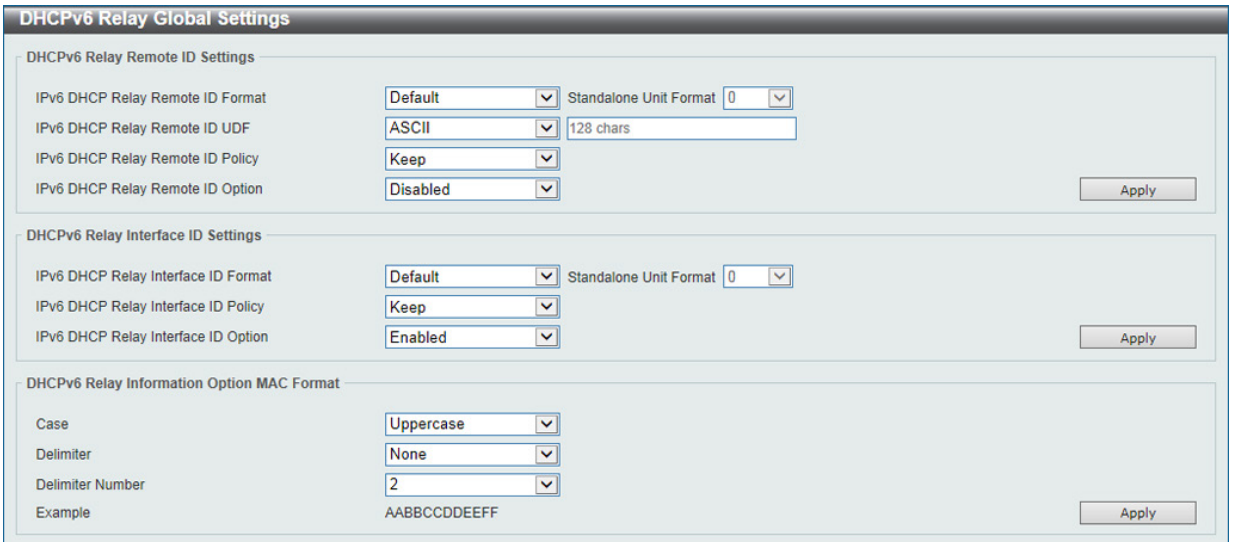


図 7-60　DHCPv6 Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCPv6 Relay Remote ID Settings	
IPv6 DHCP Relay Remote ID Format	IPv6 DHCP リレーのリレー ID フォーマットを選択します。 • 選択肢：「Default」「CID With User Define」「User Define」「Expert UDF」
Standalone Unit Format	「Expert UDF」を選択した場合、スタンドアロンユニットのフォーマットを選択します。 • 選択肢：「0」「1」
IPv6 DHCP Relay Remote ID UDF	リモート ID のユーザ定義項目 (UDF) の入力形式 を選択します。 • 「None」- リモート ID の UDF を空のままにします。 • 「ASCII」- ASCII 文字列で入力します。（128 文字以内） • 「HEX」- 16 進数文字列で入力します。（256 文字以内）
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。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプション 37 リレー情報を保持します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にオプション 37 リレー情報があった場合はそのパケットを破棄します。

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のリレーエージェント情報（Option37）の挿入を有効 / 無効に設定します。
DHCPv6 Relay Interface ID Settings	
IPv6 DHCP Relay Interface ID Format	インタフェース ID のフォーマットを指定します。 • 選択肢：「Default」「CID」「Vendor1」「Expert UDF」
Standalone Unit Format	「Expert UDF」を選択した場合、スタンドアロンユニットのフォーマットを選択します。 • 選択肢：「0」「1」
IPv6 DHCP Relay Interface ID Policy	DHCPv6 リレーエージェントのオプション 18 フォワーディングポリシーを選択します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプション 18 リレー情報を保持します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にオプション 18 リレー情報があった場合はそのパケットを破棄します。
IPv6 DHCP Relay Interface ID Option	DHCP IPv6 リクエストパケットのリレーの間のリレーエージェント情報（Option18）の挿入を有効 / 無効に設定します。
DHCPv6 Relay Information Option MAC Format	
Case	MAC アドレスの形式を選択します。 • 「Lowercase」- 小文字を使用します。（例：aa-bb-cc-dd-ee-ff） • 「Uppercase」- 大文字を使用します。（例：AA-BB-CC-DD-EE-FF）
Delimiter	MAC アドレスを入力する際の区切りを選択します。区切り文字を持たない場合には「None」を選択します。各項目の例は次の通りです。 • 「Hyphen」（ハイフン）-「AA-BB-CC-DD-EE-FF」 • 「Colon」（コロン）-「AA:BB:CC:DD:EE:FF」 • 「Dot」（ドット）-「AA.BB.CC.DD.EE.FF」 • 「None」（なし）-「AABBCCDDEEFF」
Delimiter Number	MAC アドレスにおける区切り数を選択します。各項目の例は次の通りです。 • 「1」-「AABBCC.DDEEFF」 • 「2」-「AABB.CCDD.EEFF」 • 「5」-「AA.BB.CC.DD.EE.FF」

「Apply」ボタンをクリックして、設定を適用します。

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

DHCPv6 リレーインタフェース設定の表示と設定を行います。

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

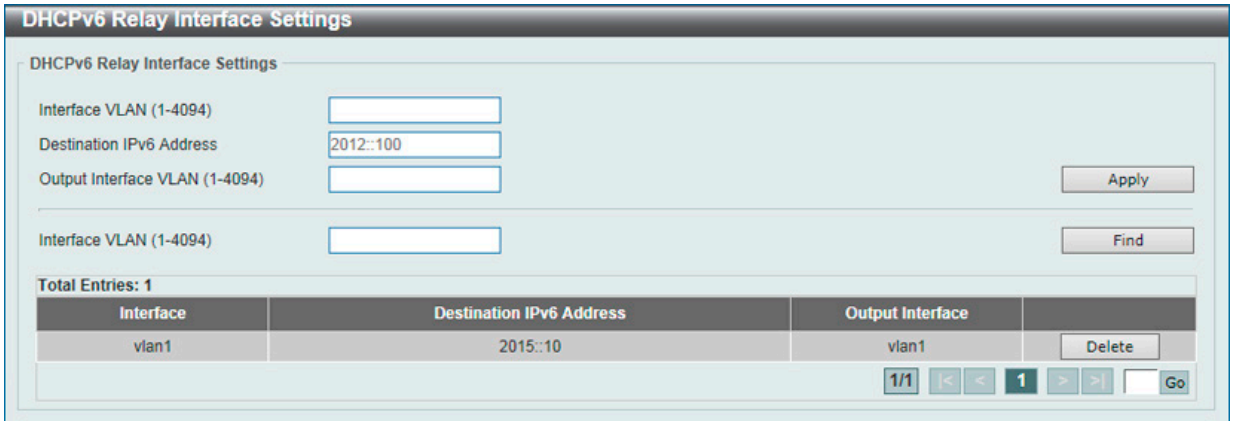


図 7-61　DHCPv6 Relay Interface Settings 画面

画面に表示される項目：

項目	説明
Interface VLAN	DHCPv6 リレーの VLAN を指定します。 • 設定可能範囲：1-4094
Destination IPv6 Address	DHCPv6 リレーの宛先アドレスを入力します。
Output Interface VLAN	リレー宛先の送信インタフェースを指定します。 • 設定可能範囲：1-4094

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

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

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

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

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



図 7-62　DHCPv6 Relay Remote ID Profile Settings 画面

画面に表示される項目：

項目	説明
Profile Name	オプション 37 のプロファイル名を入力します。（32 文字以内）
Format String	「Edit」をクリックし、ユーザ定義のオプション 37 フォーマット文字列を指定します。（251 文字以内）ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた形式（例："Ethernet"）とします。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列と 16 進数の両方を含むことができます。 • 「%」の後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。（オプション）フォーマットキー文字列において文字長オプションの指定文字数（バイト数）を満たすために使用されます。 - 「$」はスペース（0x20）を埋めます。 - 「0」は（0）を埋めます。「0」が初期値です。 • 「1-32」は文字長オプションです。（オプション）キー文字列に変換される文字やバイトの文字数 / バイト数を指定します。変換されたキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。 • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。 - 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。 - 「sysname」はスイッチのシステム名を意味します。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。 - 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデバイスの場合、ユニット ID は 0 です。 - 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 • 「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合、この最後の文字（":"）は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットキー文字列のいかなる組み合わせも可能です。「\」はエスケープ文字であり、「\」の後の特殊文字はそのままになります。例えば「\%」は「%」を意味し、フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列に含まれないスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。

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

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

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

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



図 7-63　DHCPv6 Relay Interface ID Profile Settings 画面

画面に表示される項目：

項目	説明
Profile Name	オプション 18 のプロファイル名を入力します。（32 文字以内）
Format String	「Edit」をクリックし、ユーザ定義のオプション 18 フォーマット文字列を指定します。（251 文字以内）ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた形式（例："Ethernet"）とします。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列と 16 進数の両方を含むことができます。 • 「%」の後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。（オプション）フォーマットキー文字列において文字長オプションの指定文字数（バイト数）を満たすために使用されます。 - 「$」はスペース（0x20）を埋めます。 - 「0」は（0）を埋めます。「0」が初期値です。 • 「1-32」は文字長オプションです。（オプション）キー文字列に変換される文字やバイトの文字数 / バイト数を指定します。変換されたキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。 • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。 - 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。 - 「sysname」はスイッチのシステム名を意味します。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。 - 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。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。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。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 0 です。 - 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「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、この最後の文字（":"）は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットキー文字列のいかなる組み合わせも可能です。「\」はエスケープ文字であり、「\」の後の特殊文字はそのままになります。例えば「\%」は「%」を意味し、フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列に含まれないスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「Apply」ボタンをクリックして、エントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。

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

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

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

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

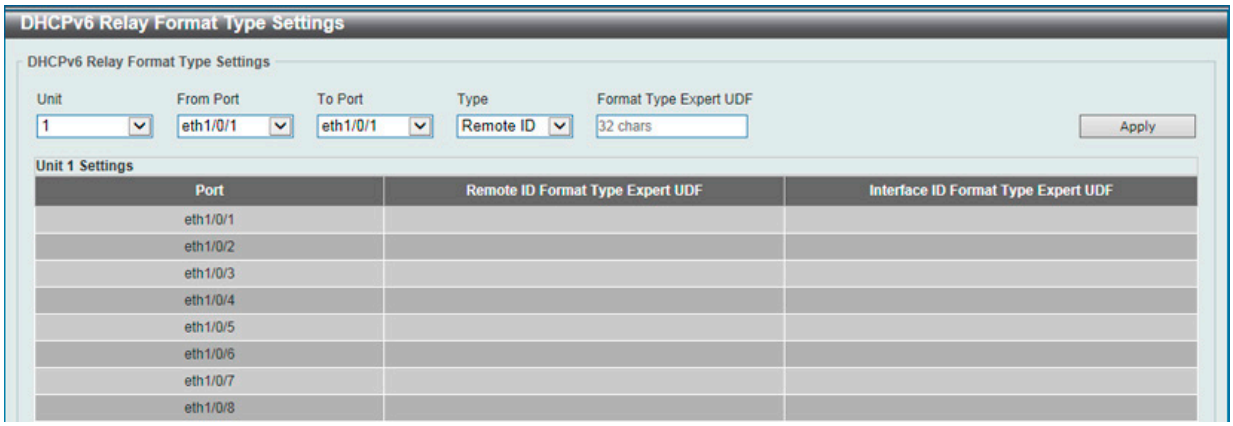


図 7-64　DHCPv6 Relay Format Type Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定を適用します。

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

DHCPv6 リレーポート設定を行います。

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

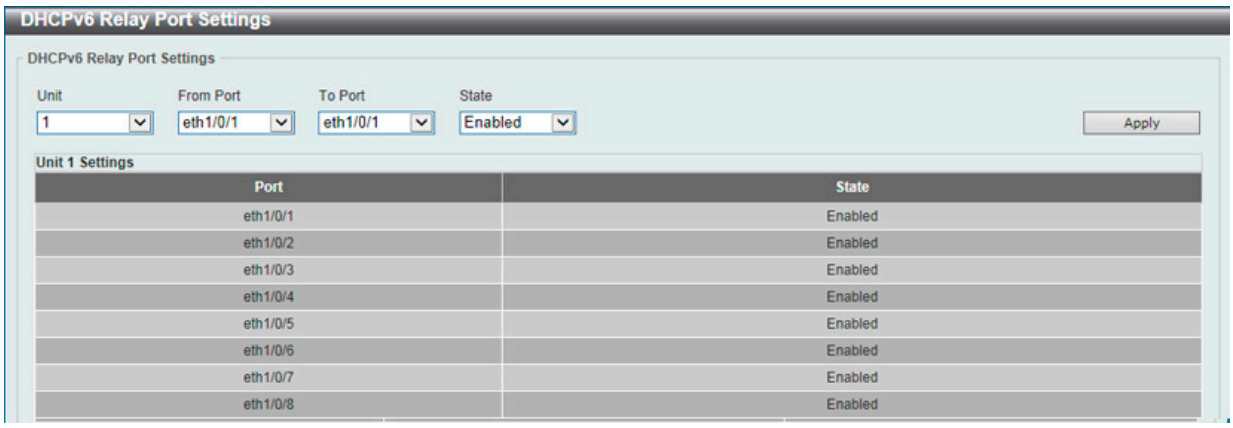


図 7-65　DHCPv6 Relay Port Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定を適用します。

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

DHCPv6 ローカルリレー VLAN 設定を行います。DHCPv6 ローカルリレーが有効の場合、クライアントからのリクエストパケットにオプション 37 と 18 を追加します。オプション 37 のチェックステートが有効の場合、クライアントからのリクエストパケットをチェックし、オプション 37 の DHCPv6 リレー機能が含まれる場合、パケットを破棄します。無効の場合、ローカルリレー機能は、オプション 37 が有効であろうとなかろうと、常にオプション 37 をリクエストパケットに追加します。DHCPv6 ローカルリレー機能はサーバからのパケットを直接クライアントに転送します。

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

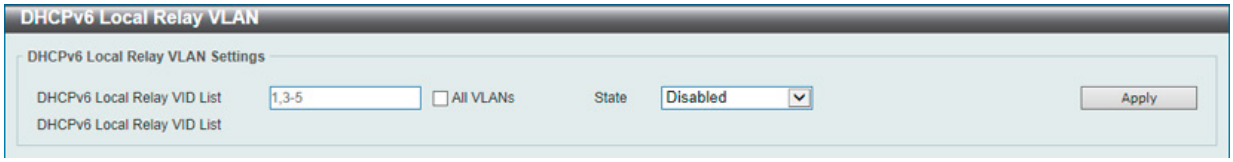


図 7-66　DHCPv6 Local Relay VLAN 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定を適用します。

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

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。

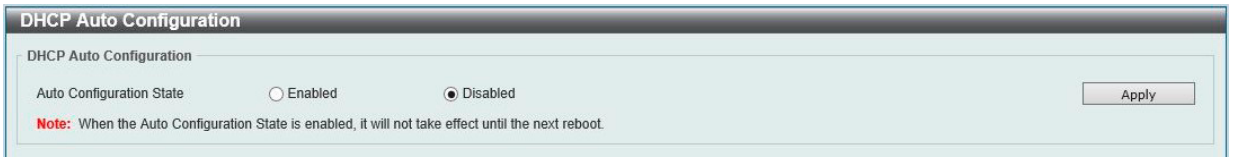


図 7-67　DHCP Auto Configuration 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定を適用します。

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

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

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

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

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

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

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

オプション 67 は、DHCP ヘッダの「file」フィールドが DHCP オプションに使用されている場合に、ブートファイルを識別するために使用されます。これは、DHCP 自動コンフィギュレーションモードでのみ使用でき、DHCP 自動イメージモードでは使用できません。詳細については、RFC2132 を参照してください。イメージファイル名を指定する場合は、DHCP オプション 125（RFC3925）を使用する必要があります。本スイッチでは enterprise-number1 フィールドを確認する必要があります。値が D-Link ベンダ ID（171）でない場合、プロセスが停止します。オプションが複数のフィールドを含む場合、最初のエントリ enterprise-number1 のみが使用されます。

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

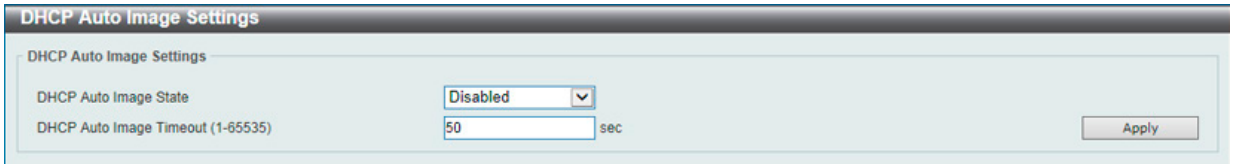


図 7-68　DHCP Auto Image Settings 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定を適用します。

DNS（ドメインネームシステム）

DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けを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ネームサーバと通信を行います。ドメインネームサービスを行うデバイスのアドレスは、DHCP または BOOTP サーバから取得する場合と、初期設定時に手動で OS に設定する場合があります。

DNS Global Settings（DNS グローバル設定）

DNS のグローバル設定を行います。

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

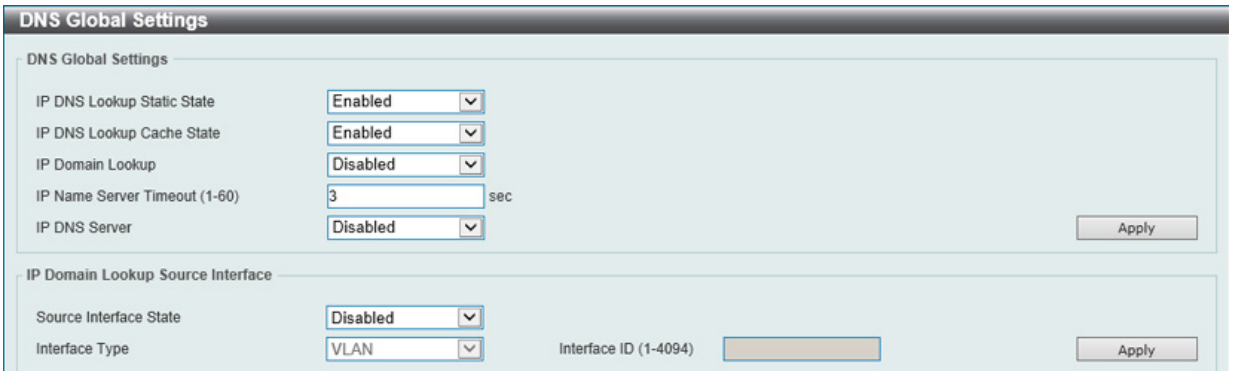


図 7-69　DNS Global Settings 画面

画面に表示される項目：

項目	説明
DNS Global Settings	
IP DNS Lookup Static State	IP DNS ルックアップのスタティックステータスを有効 / 無効に設定します。
IP DNS Lookup Cache State	IP DNS ルックアップのキャッシュを有効 / 無効に設定します。
IP Domain Lookup	IP ドメインルックアップを有効 / 無効に設定します。
IP Name Server Timeout	指定ネームサーバからの回答を待つ待機時間を指定します。 • 設定可能範囲：1-60（秒）
IP DNS Server	DNS サーバを有効 / 無効に設定します。
IP Domain Lookup Source Interface	
Source Interface State	ソースインタフェースを有効 / 無効に設定します。
Interface Type	インタフェースの種類を指定します。 • 選択肢：「Loopback」「MGMT」「VLAN」
Interface ID	ソースインタフェースの ID を指定します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）

「Apply」ボタンをクリックして、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 IP アドレスを設定します。

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



図 7-70　DNS Name Server Settings 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Name Server IPv4	選択して DNS サーバの IPv4 アドレスを入力します。
Name Server IPv6	選択して DNS サーバの IPv6 アドレスを入力します。

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

DNS Host Settings（DNS ホスト名設定）

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

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

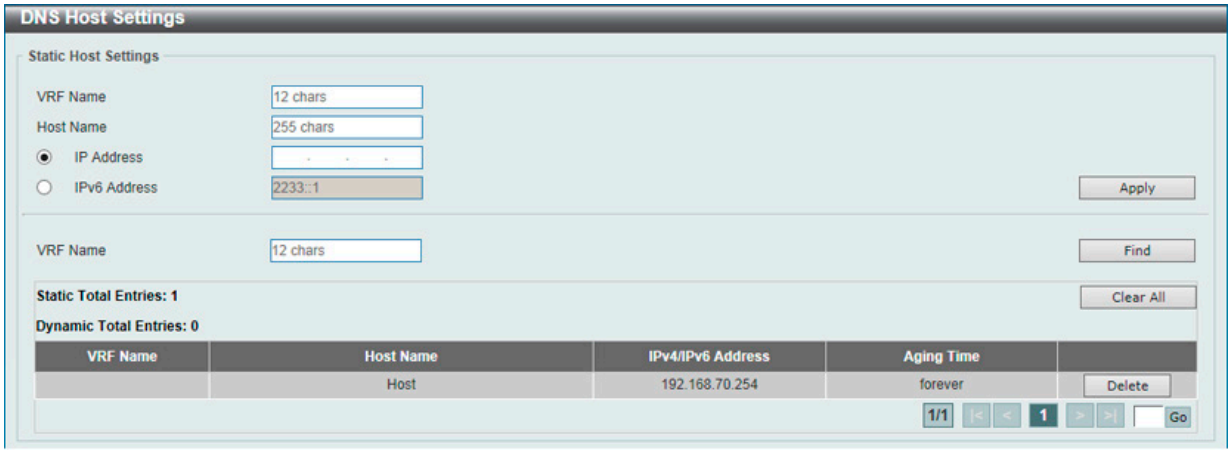


図 7-71　DNS Host Settings 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Host Name	ホスト名を入力します。
IP Address	ホストの IPv4 アドレスを入力します。
IPv6 Address	ホストの IPv6 アドレスを入力します。

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

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

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 7-72　IP Source Interface 画面

画面に表示される項目：

項目	説明
IP TFTP Source Interface	
Source Interface State	IP TFTP ソースインタフェースを有効 / 無効に設定します。
Interface Type	インタフェース種類を指定します。 • 選択肢：「Loopback」「MGMT」「VLAN」
Interface ID	インタフェース ID を指定します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）
IP FTP Source Interface	
Source Interface State	IP FTP ソースインタフェースを有効 / 無効に設定します。
Interface Type	インタフェース種類を指定します。 • 選択肢：「Loopback」「MGMT」「VLAN」
Interface ID	インタフェース ID を指定します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）
IP RCP Source Interface	
Source Interface State	IP RCP ソースインタフェースを有効 / 無効に設定します。
Interface Type	インタフェース種類を指定します。 • 選択肢：「Loopback」「MGMT」「VLAN」
Interface ID	インタフェース ID を指定します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）

「Apply」ボタンをクリックして、設定を適用します。

File System（ファイルシステム設定）

スイッチのファイルシステムを閲覧、管理および設定します。

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

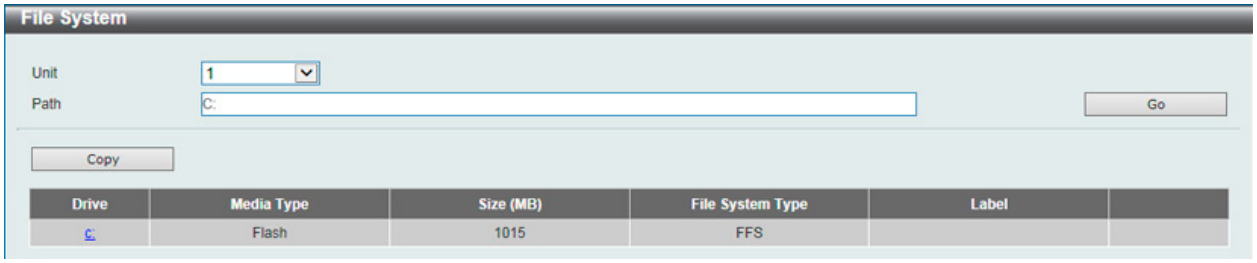


図 7-73　File System 画面

画面に表示される項目：

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

「Go」ボタンをクリックして、入力したパスに遷移します。
「Copy」ボタンをクリックして、指定のファイルをスイッチへコピーします。
「C:」リンクをクリックして、「C:」ドライブに遷移します。

「C:」リンクをクリックすると、以下の画面が表示されます。

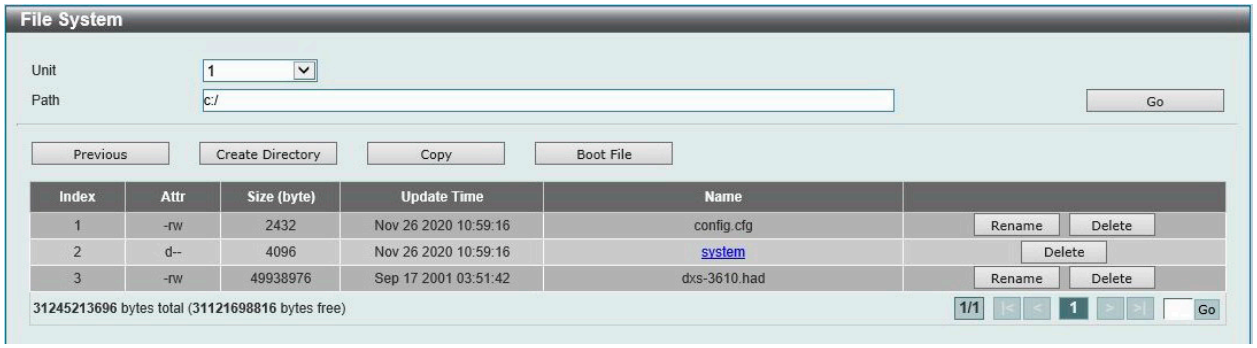


図 7-74　File System (Drive) 画面

画面に表示される項目：

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

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

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

ファイルのコピー

「Copy」ボタンをクリックすると、以下の画面が表示されます。

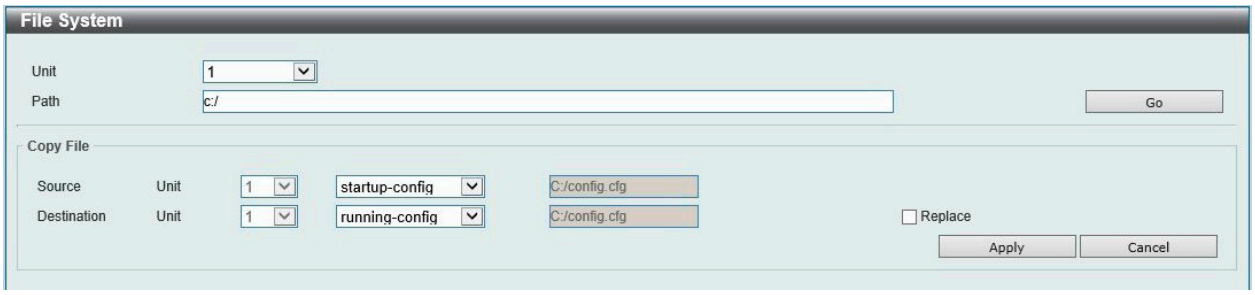


図 7-75　File System (Copy) 画面

画面に表示される項目：

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

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

起動ファイルの指定

「Boot File」ボタンをクリックすると、以下の画面が表示されます。

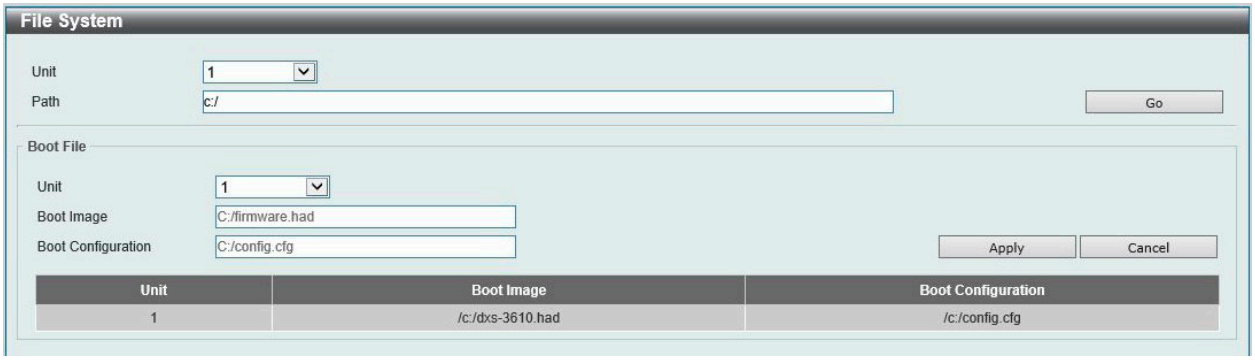


図 7-76　File System (Boot File) 画面

画面に表示される項目：

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

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

Stacking（スタッキング設定）

本スイッチは、スイッチの物理スタックをサポートしています。Telnet、GUI インタフェース（Web）、コンソールポート、管理（MGMT）ポートまたは SNMP を介して 1 つの IP アドレスで管理することができます。物理スタックによりお使いのネットワークの信頼性、サービス性、そして可用性が向上します。本シリーズの各スイッチは、前面に 6 個のスタック用スロットを搭載しスタッキング可能なデバイスを接続することができます。スタックポートを設定した後、QSFP28 ダイレクトアタッチケーブル（DAC）もしくは光ファイバーケーブルを使用して、スタックポート間を接続し、2 つのトポロジのうちいずれかを形成することができます。

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

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

本シリーズのスイッチは、QSFP28 モジュールに接続された光ファイバケーブル、または QSFP28 スロットに接続された QSFP28 ダイレクトアタッチケーブルを使用して、物理的にスタックすることが可能です。最後の 6 つの QSFP28 スロットのみ物理スタックに使用できます。

注意　スタッキングが有効になっている場合、最後の QSFP28 スロット 2/4/6 つは他のデバイスやスイッチなどへのアップリンクとして使用できません。これらのスロットはスタッキング専用スロットとなります。

以下は、QSFP28 モジュールに接続された光ファイバケーブル、または QSFP28 ダイレクトアタッチケーブルを使用した「Duplex Chain」構成での物理スタック図です。「2 ポート」スタッキング設定を使用しています。

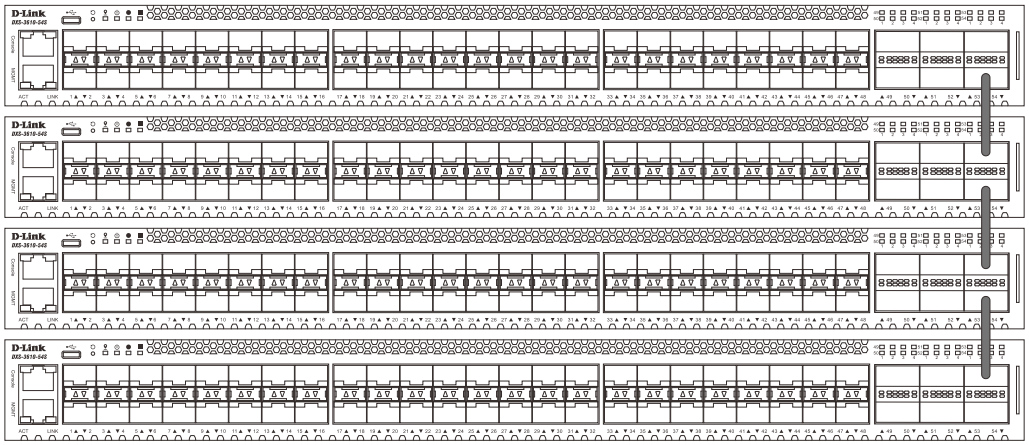


図 7-77　Duplex Chain でスタックされているスイッチ（QSFP28）

以下は、QSFP28 モジュールに接続された光ファイバケーブル、または QSFP28 ダイレクトアタッチケーブルを使用した「Duplex Ring」構成での物理スタック図です。「2 ポート」スタッキング設定を使用しています。

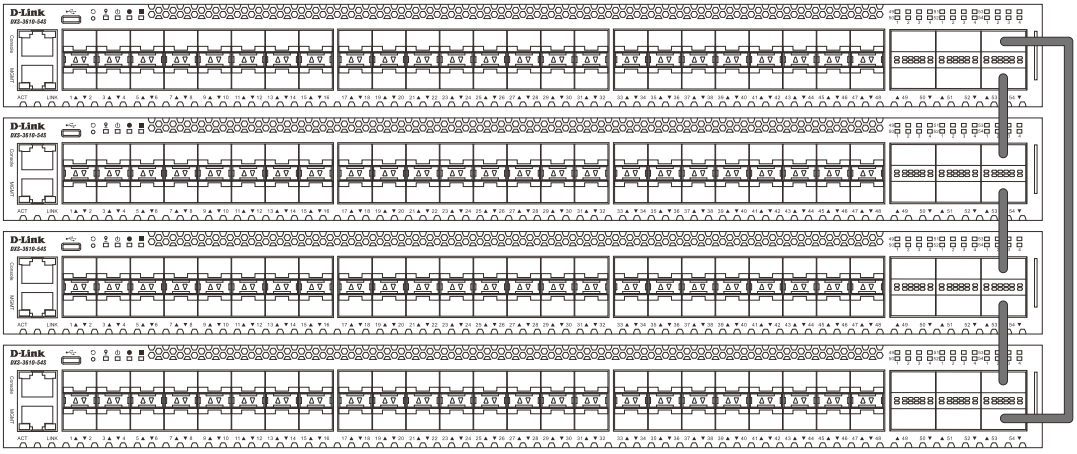


図 7-78　Duplex Ring でスタックされているスイッチ（QSFP28）

物理スタックでは「2 ポート」「4 ポート」「6 ポート」スタッキングコンフィグレーションを設定することができます。
スタッキングポートの設定と、それに対応する SIO ポートペアは以下の通りです。

設定	論理 SIO1	論理 SIO2	帯域幅
2 ポート	ポート 53	ポート 54	400Gbps（全二重）
4 ポート	ポート 51、53	ポート 52、54	800Gbps（全二重）
6 ポート	ポート 49、51、53	ポート 50、52、54	1200Gbps（全二重）

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 /6 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。

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。

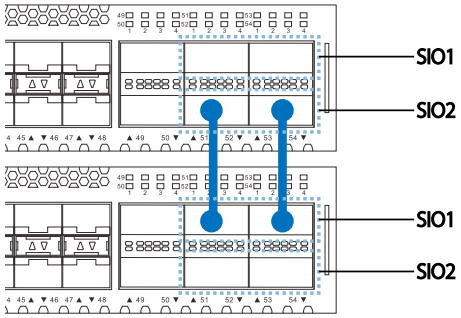


図 7-79　スイッチ間のケーブル接続①

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。

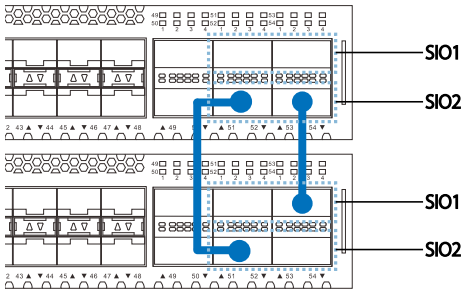


図 7-80　スイッチ間のケーブル接続②

スタック内のスイッチ役割

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

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

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

- スレーブ
  スレーブスイッチは、プライマリマスタまたはバックアップマスタではないスイッチスタックの残りのスイッチです。プライマリマスタおよびバックアップマスタが故障、またはスタックから取り外される場合に、それらの機能を引き継ぎます。スレーブスイッチは、マスタに要求された操作

を実行して、スタックとスタックトポロジにある近接スイッチの状態をモニタします。さらに、バックアップマスタがプライマリマスタになるとバックアップマスタのコマンドに従います。スレーブスイッチは、バックアップマスタがプライマリマスタに移行する場合や、バックアップマスタが故障、またはスイッチから取り外される場合に、セルフチェックを行い、自身がバックアップマスタになるかどうかを決定します。プライマリマスタとバックアップマスタの両方が故障、またはスイッチから取り外される場合、プライマリマスタになるかどうかを決定します。これらの役割はプライオリティによって決定され、プライオリティが同じである場合は、最も値の小さい MAC アドレスによって決定されます。

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

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

これらの処理が完了すると、スイッチスタックは通常の操作モードに入ります。

スタックスイッチのスワップ

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

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

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

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

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

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

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

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

Physical Stacking（物理スタッキング）

物理スタッキングの設定を行います。

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

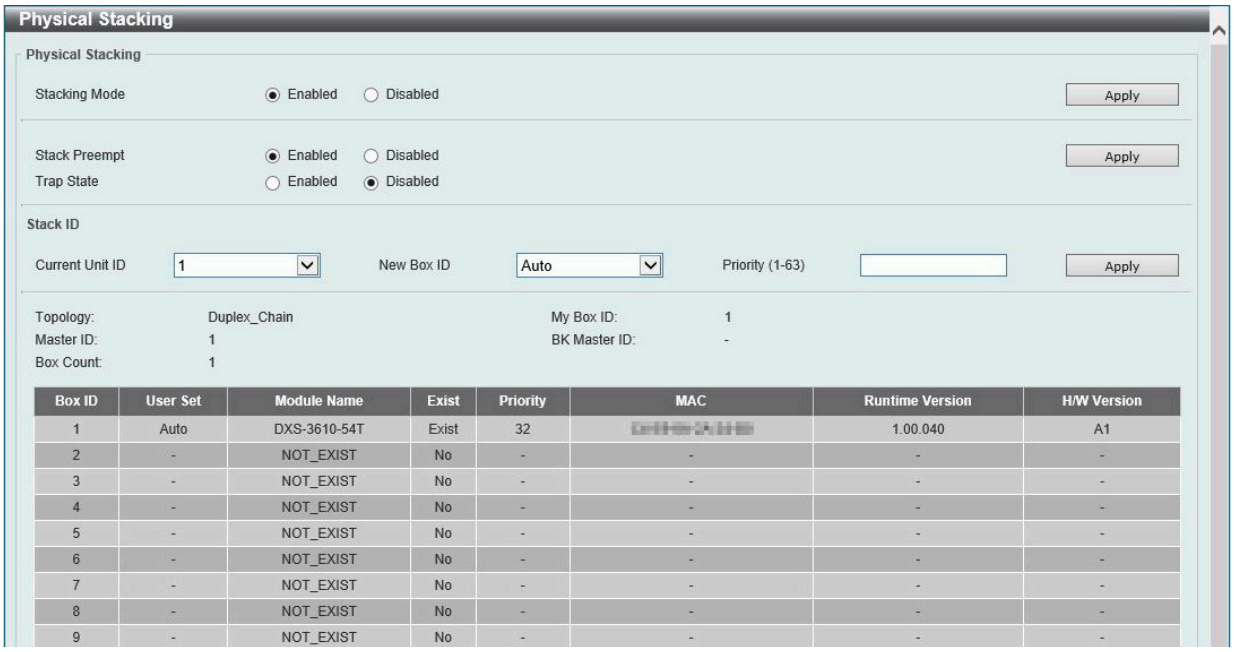


図 7-81　Physical Stacking 画面

画面に表示される項目：

項目	説明
Physical Stacking	
Stacking Mode	スタッキングモードを有効 / 無効に設定します。
Stack Preempt	Stack Preempt 機能の有効 / 無効を設定します。「Disabled」（無効）に設定した場合、現在のマスタスイッチの優先度が 0 に変更され、新しいデバイスを現在のスタックトポロジに追加した場合でも、マスターとなるスイッチが変更されません。
Trap State	スタック関連の SNMP トラップの送信を有効 / 無効に設定します。
Stack ID	
Current Unit ID	スタックにおけるスイッチの現在のユニット番号を選択します。
New Box ID	「Current Unit ID」で選択したスタック内のスイッチに、新しくボックス番号を指定します。「Auto」を選択すると、自動的にボックス番号を割り当てます。 • 設定可能範囲：1-12
Priority	スイッチの優先度番号を指定します。低い値ほど高いプライオリティを示します。スタック内で最も低い優先度番号を持つボックス（スイッチ）が、プライマリマスタです。プライマリマスタスイッチは、スイッチスタックにおけるアプリケーションを設定するために使用されます。 • 設定可能範囲：1-63

「Apply」ボタンをクリックして、設定内容を適用します。

Stacking Bandwidth（スタッキング帯域）

スタッキング帯域の設定、表示を行います。スタッキングに使用できるのは、最後の 6 つの QSFP28 ポートのみです。

物理スタックでは「2 ポート」「4 ポート」「6 ポート」スタッキングコンフィグレーションを設定することができます。
スタッキングポートの設定と、それに対応する SIO ポートペアは以下の通りです。

設定	論理 SIO1	論理 SIO2	帯域幅
2 ポート	ポート 53	ポート 54	400Gbps（全二重）
4 ポート	ポート 51、53	ポート 52、54	800Gbps（全二重）
6 ポート	ポート 49、51、53	ポート 50、52、54	1200Gbps（全二重）

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 /6 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。

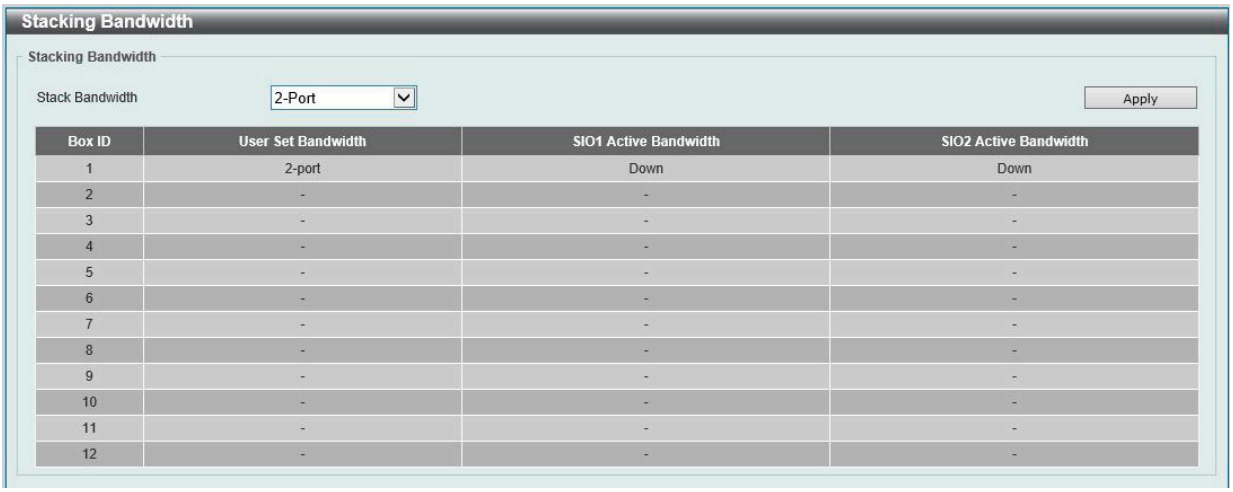


図 7-82　Stacking Bandwidth 画面

画面に表示される項目：

項目	説明
Stack Bandwidth	スタッキング帯域を指定します。 • 「2-Port」- スタックに 2 つのポートを使用します。 • 「4-Port」- スタックに 4 つのポートを使用します。 • 「6-Port」- スタックに 6 つのポートを使用します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意 Stack Port の帯域幅は Stack Member が存在する状態において変更はできません。

シングル IP マネジメント（SIM）設定

シングル IP マネジメント（SIM）の設定を行います。

シングル IP マネジメント（SIM）の概要

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

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

シングル IP マネジメント（SIM）のルールと動作

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

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

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

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

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

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

これらの役割には、さらに以下のルールが適用されます。

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

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

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

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

バージョン 1.61 へのアップグレード

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

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

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

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

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

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

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



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

Single IP Settings（シングル IP 設定）

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

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

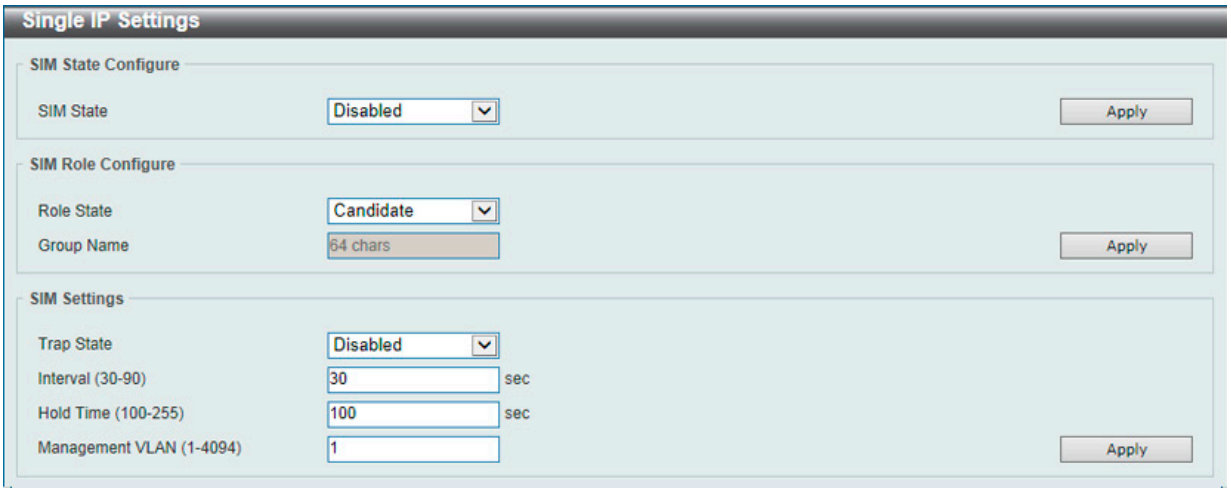


図 7-83　Single IP Settings 画面

画面に表示される項目：

項目	説明
SIM State Configure	
SIM State	SIM 機能を有効 / 無効に設定します。
SIM Role Configure	
Role State	スイッチの SIM での役割を選択します。 • 「Candidate」- Candidate Switch（CaS）は SIM グループメンバではありませんが、Commander スイッチに接続しています。（初期値） • 「Commander」- Commander Switch（CS）。ユーザは CS に他のスイッチを参加させて SIM グループを作成することができます。また、このオプションを選択すると、本スイッチで SIM の設定が可能になります。
Group Name	SIM グループ名を入力します。スイッチを SIM グループで分割する場合のオプションです。
SIM Settings	
Trap State	SIM トラップを有効 / 無効に設定します。
Interval	スイッチが Discovery パケットを送信する送信間隔を設定します。 • 選択可能範囲：30-90（秒）
Hold Time	他のスイッチから送信された Discovery パケットの情報をスイッチが保持する時間を指定します。 • 選択可能範囲：100-255（秒）
Management VLAN	シングル IP マネージメントメッセージの VLAN ID を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

スイッチを CS として登録すると、「Single IP Management」フォルダには 4 つのリンクが追加され、Web を使用した SIM 設定ができるようになります。

CS スイッチで設定可能なメニューリンク：

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

Topology（トポロジ）

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

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

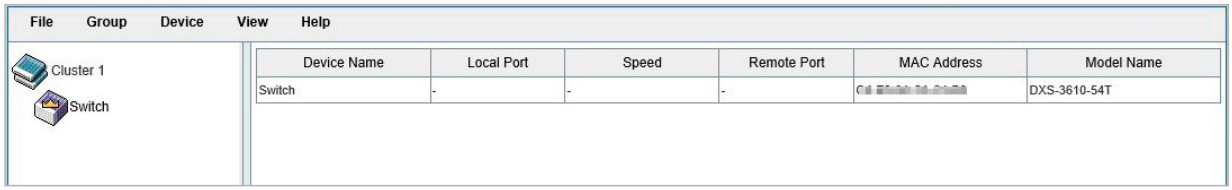


図 7-84　トポロジ画面

メニューバー

トポロジ画面には、デバイスの設定用に以下のメニューバーが配置されています。



図 7-85　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。

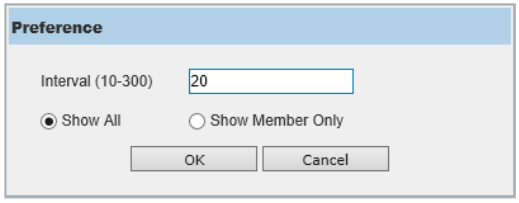


図 7-86　Preference 画面

以下の項目が使用できます。

項目	説明
Interval	SIM トポロジ表示の更新間隔を指定します。 • 設定可能範囲：10-300
Show All	トポロジ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。

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

■「Group」メニュー

- **Add to Group** – グループに 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。

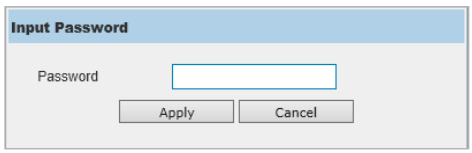


図 7-87　Input password 画面

- **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。

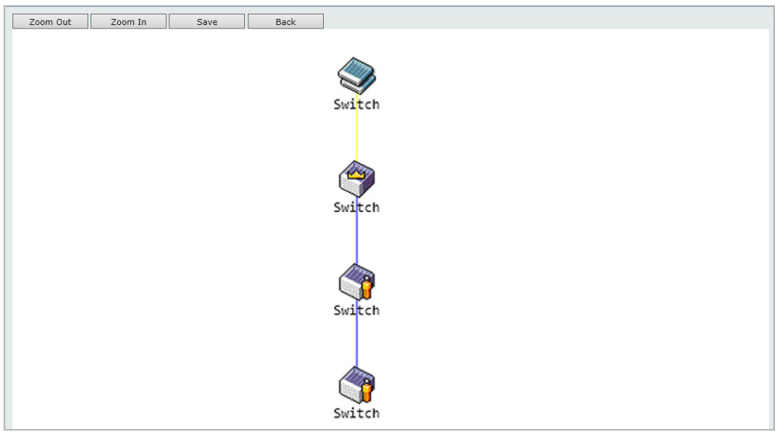


図 7-88　View >Topology 画面

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

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

本画面で表示されるアイコンは以下の通りです。

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

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

ツールヒント

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

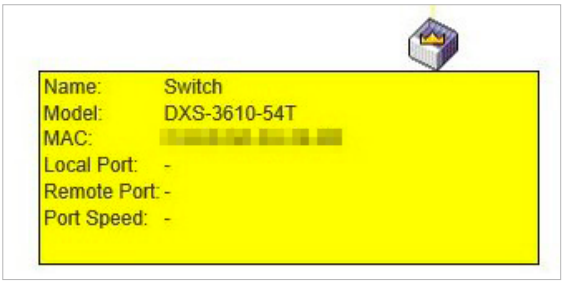


図 7-89　ツールヒントを利用したデバイス情報の表示

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。

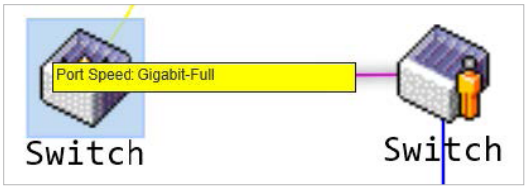


図 7-90　ツールヒントを利用したポート速度の表示

右クリックメニュー

デバイスのアイコン上で右クリックすると、SIM グループ内でのスイッチの役割や、関連付けられているアイコンの種類に応じた様々な機能を実行できます。

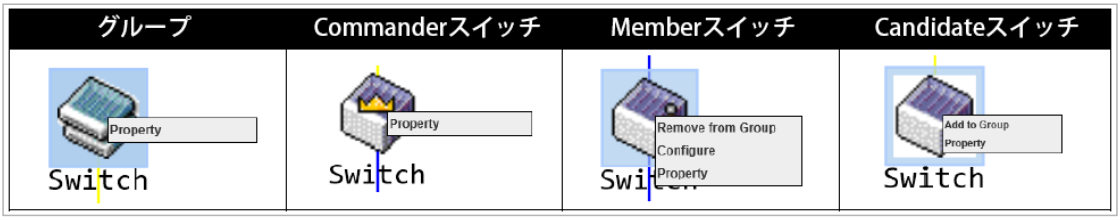


図 7-91　各アイコン上での右クリック

画面に表示される項目：

項目	説明
Property	ポップアップ画面が開き、デバイスの情報を表示します。
Configure （Member スイッチのみ）	Web 管理機能を起動して、スイッチの設定を行うことができます。
Add to group （Candidate スイッチのみ）	CaS をグループに追加します。このオプションを選択すると、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 7-92　Property 画面

画面に表示される項目：

項目	説明
Name	SIM グループ内のスイッチのデバイス名を表示します。
Module	スイッチのモジュール名を表示します。

項目	説明
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** – SIM の Copyright 情報とリリース日を表示します。



図 7-93　About 画面

Firmware Upgrade（ファームウェア更新）

CS から MS へのファームウェアの更新を行います。

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

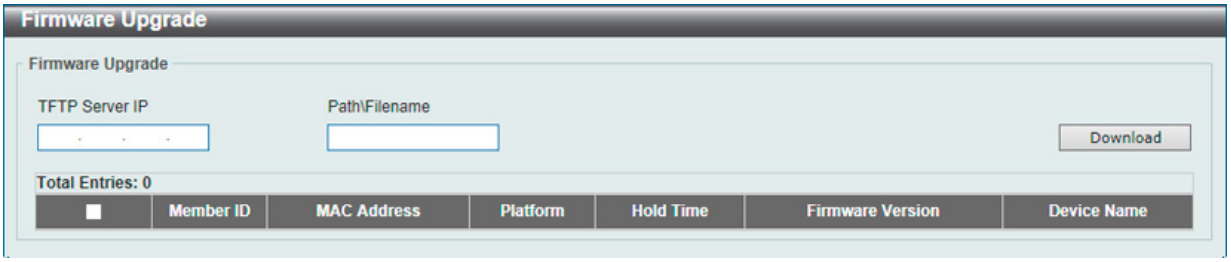


図 7-94　Firmware Upgrade 画面

画面に表示される項目：

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

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

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

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

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

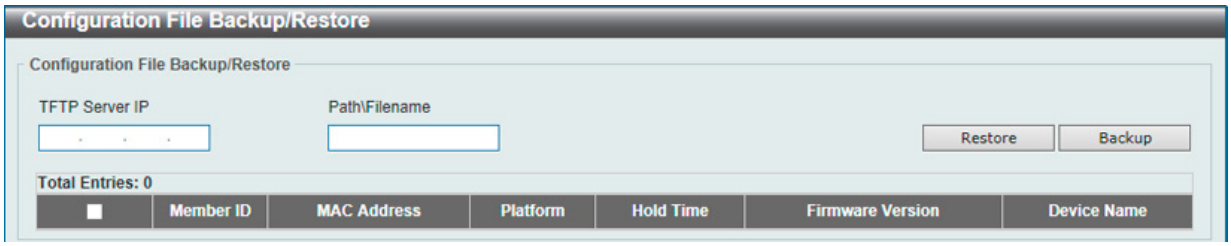


図 7-95　Configuration File Backup/Restore 画面

画面に表示される項目：

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

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

Upload Log File（ログファイルのアップロード）

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

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

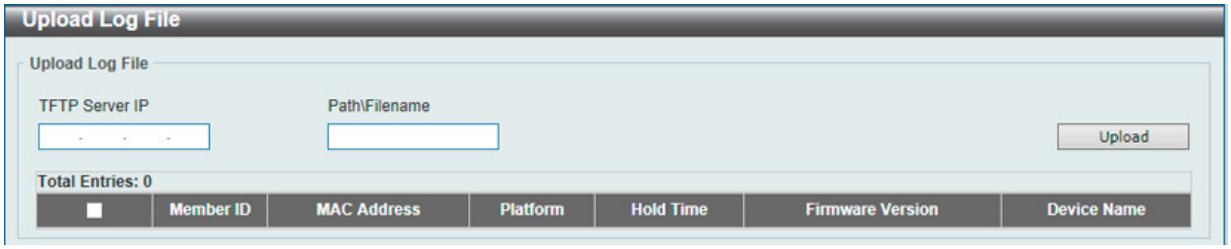


図 7-96　Upload Log File 画面

画面に表示される項目：

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

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

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

DDP Settings

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

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

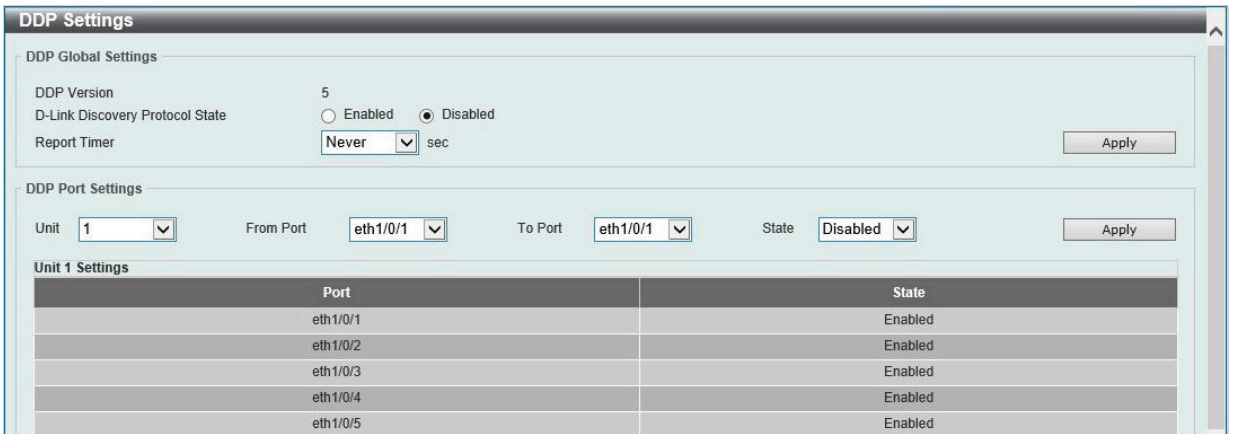


図 7-97　DDP Settings 画面

画面に表示される項目：

項目	説明
D-Link Discovery Protocol	
D-Link Discovery Protocol State	DDP のグローバルステータスを有効 / 無効に設定します。
Report Timer	DDP レポートメッセージの送信間隔を以下から指定します。 • 「30」「60」「90」「120」「Never」（秒） 「Never」を選択すると、スイッチはレポートメッセージの送信を停止します。
DDP Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートの DDP 機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

DDP Neighbors（DDP 隣接機器）

DDP 隣接機器の表示を行います。

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

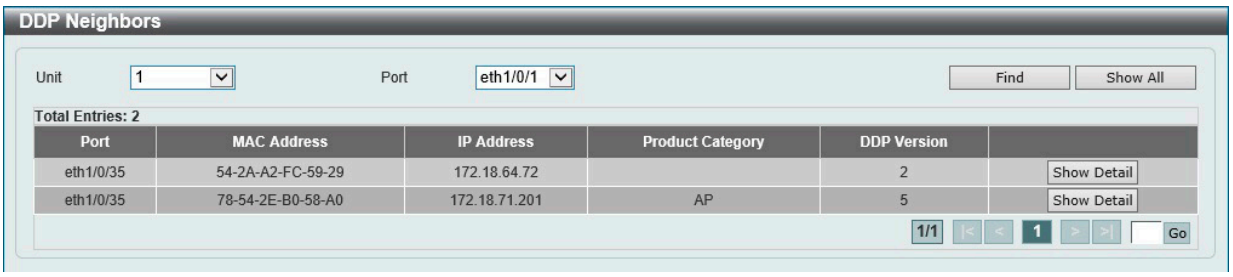


図 7-98　DDP Neighbors 画面

画面に表示される項目：

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

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

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

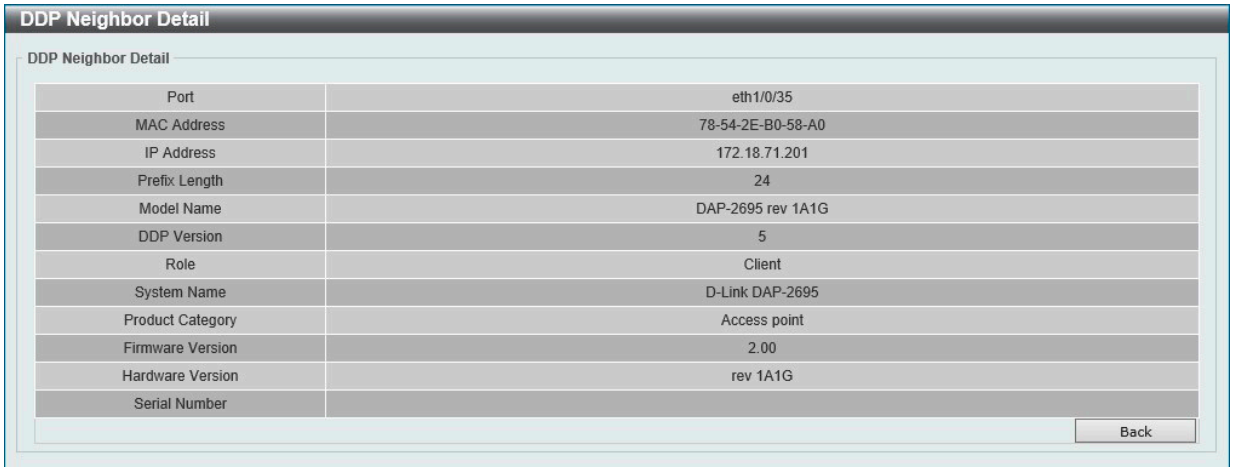


図 7-99　DDP Neighbors (Show Detail) - DDP Neighbor Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

SMTP Settings（SMTP 設定）

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

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

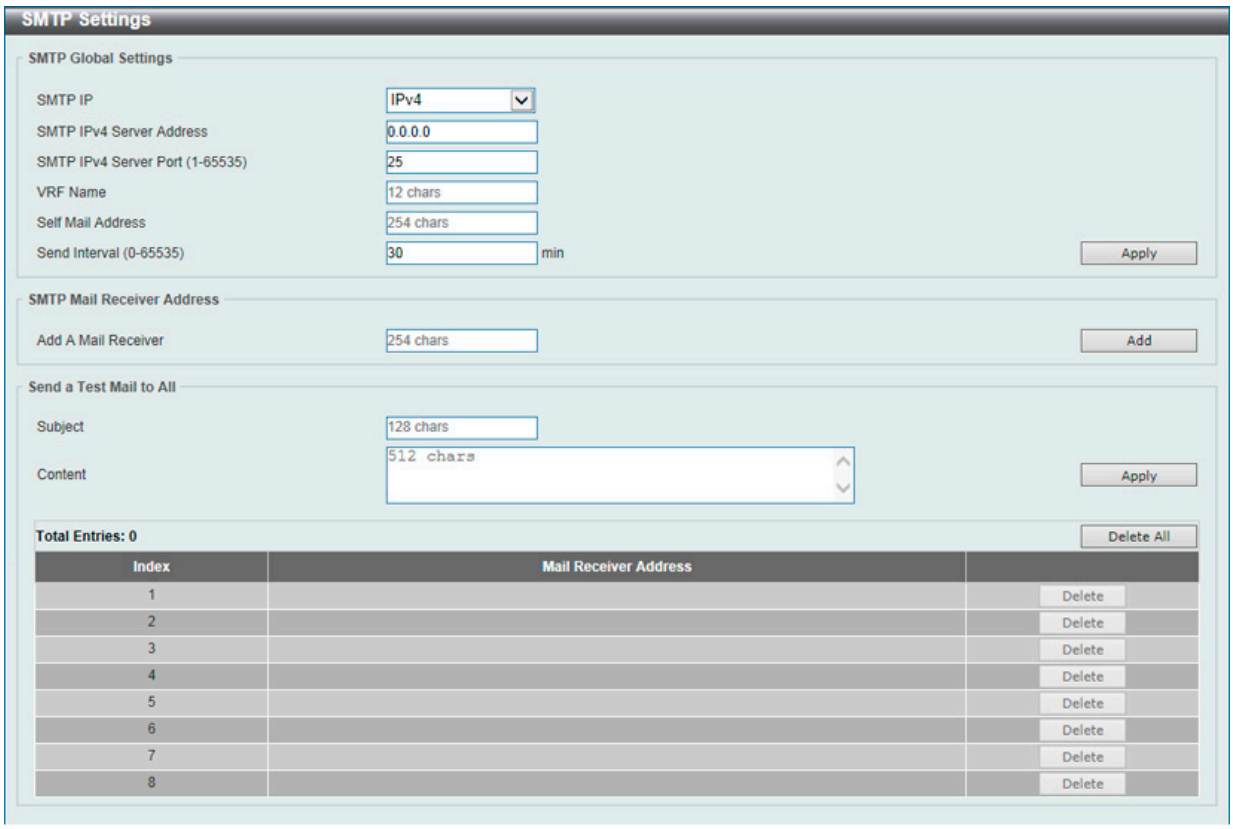


図 7-100　SMTP Settings 画面

画面に表示される項目：

SMTP Global Settings

項目	説明
SMTP IP	SMTP サーバ IP アドレスタイプを指定します。 • 選択肢：「IPv4」「IPv6」
SMTP IPv4 Server Address	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。

項目	説明
SMTP IPv4 Server Port	SMTP IPv4 サーバポート番号を指定します。 • 設定可能範囲：1-65535 • 初期値：25
SMTP IPv6 Server Port	SMTP IPv6 サーバポート番号を指定します。 • 設定可能範囲：1-65535 • 初期値：25
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Self Mail Address	スイッチの E メールアドレスを指定します。（254 文字以内）
Send Interval	送信間隔を指定します。 • 設定可能範囲：0-65535（分） • 初期値：30（分）

「Apply」ボタンをクリックして、設定内容を適用します。

SMTP Mail Receiver Address

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

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

Send a Test Mail to All

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

「Apply」ボタンをクリックして、設定内容を適用します。

Reboot Schedule Settings（再起動スケジュール設定）

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

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

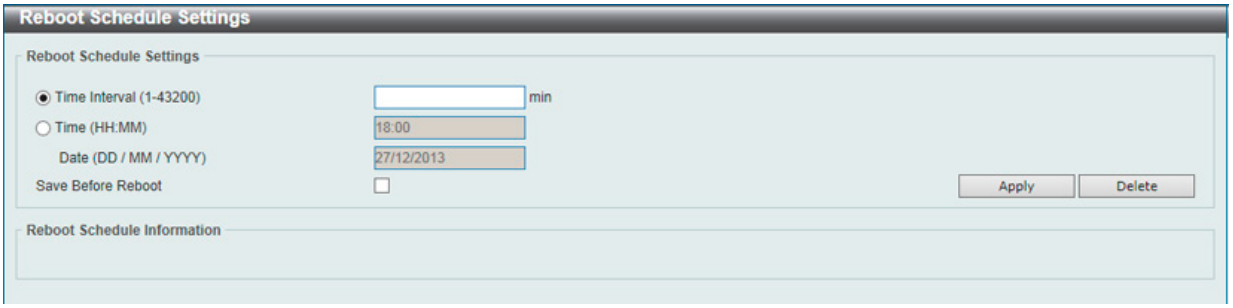


図 7-101　Reboot Schedule Settings 画面

画面に表示される項目：

項目	説明
Time Interval	再起動スケジュールの間隔を選択します。指定の間隔を過ぎると再起動が実行されます。 • 設定可能範囲：1-43200（分）（30 日）
Time	再起動を実行する時間を指定します。24 時間のフォーマットを使用します。(例；21:30) 日付が指定されていない場合、次の 24 時間以内の指定時間に再起動が実行されます。
Date	再起動を実行する日付を指定します。「DD/MM/YYYY」のフォーマットを使用します。(例；23/12/2015) 30 日以内の再起動スケジュールが指定可能です。
Save Before Reboot	再起動実行前に、変更されたすべての設定内容を保存します。

「Apply」ボタンをクリックして、設定内容を適用します。

NLB FDB Settings（NLB FDB 設定）

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

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

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

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

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

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。

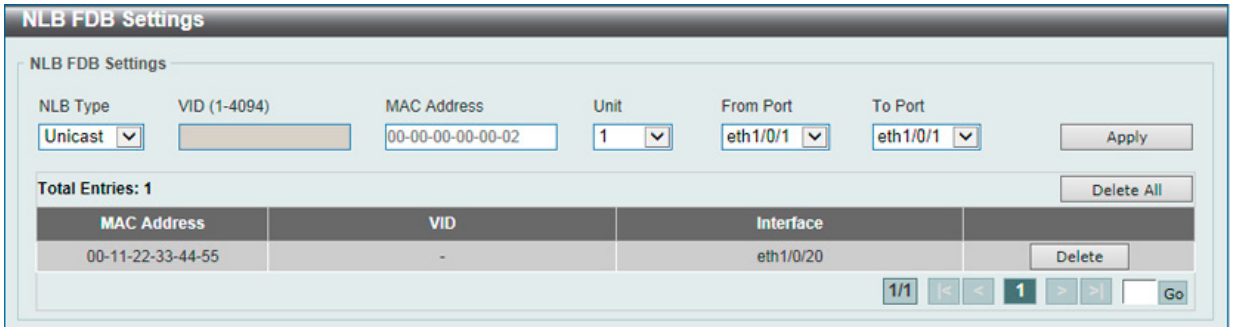


図 7-102　NLB FDB Settings 画面

画面に表示される項目：

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

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

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

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。

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）	フレックスリンク機能の設定を行います。
L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）	L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）の設定を行います。
L2 Multicast Control（L2 マルチキャストコントロール）	IGMP（Internet Group Management Protocol）Snooping 機能始めとした L2 Multicast Control（L2 マルチキャストコントロール）の設定を行います。
LLDP	Link Layer Discovery Protocol（LLDP）の設定を行います。

FDB（FDB 設定）

FDB（Forwarding DataBase/ フォワーディングデータベース）の設定を行います。

Static FDB（スタティック FDB の設定）

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

スイッチにスタティックなユニキャストフォワーディングを設定します。

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

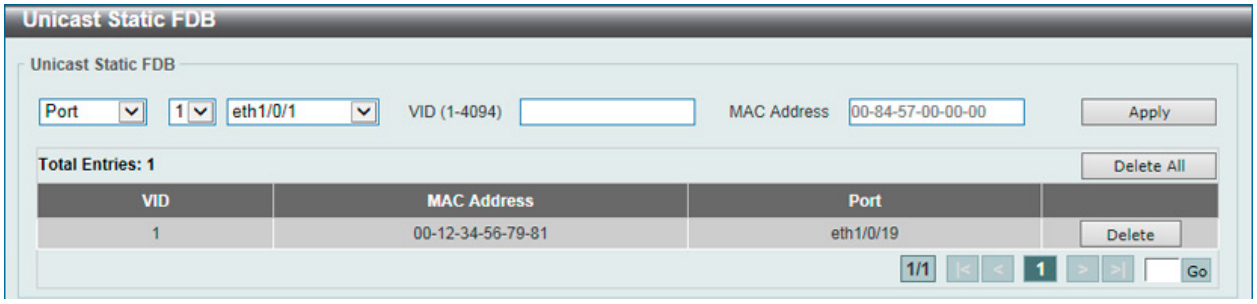


図 8-1　Unicast Static FDB 画面

画面に表示される項目：

項目	説明
Port/Drop	指定 MAC アドレスのあるポート番号を指定します。また、本オプションはユニキャストのスタティック FDB から MAC アドレスを削除することもできます。 • 「Port」- 指定 MAC アドレスのあるポート番号を指定します。 • 「drop」- ユニキャストのスタティック FDB から MAC アドレスを破棄します。
Unit	本設定を適用するユニットを選択します。
Port Number	「Port」を選択した場合、ポート番号を入力します。
VID	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 アドレスを入力します。ユニキャスト MAC アドレスを指定します。

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

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

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

スイッチにスタティックなマルチキャストフォワーディングを設定します。

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

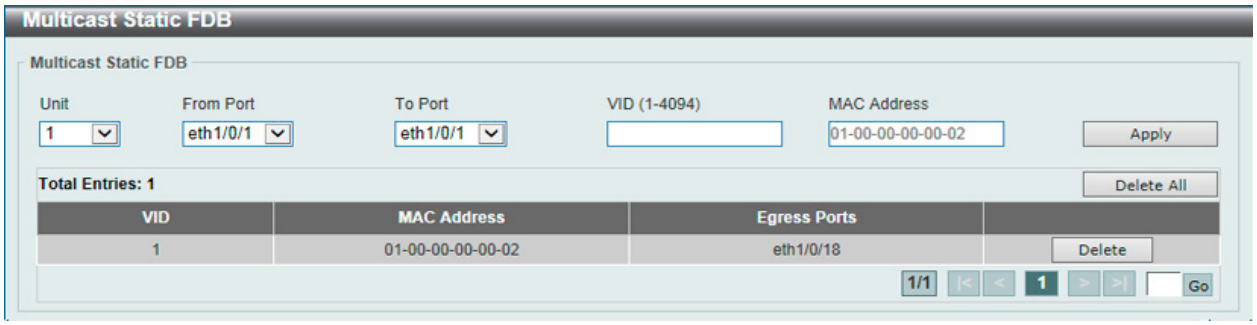


図 8-2　Multicast Static FDB 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
VID	指定の Multicast MAC アドレスが所属する VLAN の VLAN ID を入力します。
MAC Address	マルチキャストパケットの送信先スタティック MAC アドレスを入力します。マルチキャスト MAC アドレスを指定します。

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

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

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

スイッチの MAC アドレステーブルの設定を行います。

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

Global Settings（グローバル設定タブ）

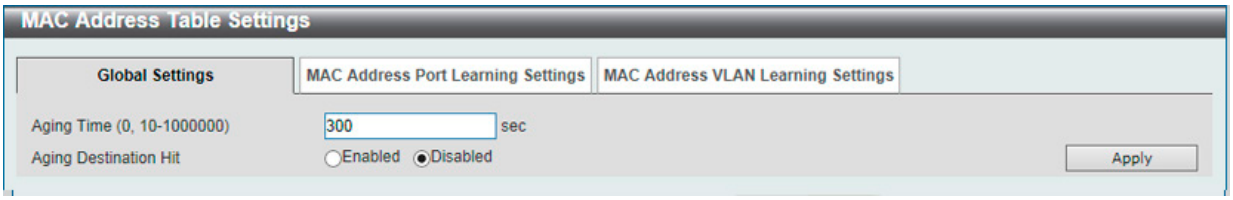


図 8-3　MAC Address Table Settings（Global Settings）画面

画面に表示される項目：

項目	説明
Aging Time	MAC アドレステーブルのエージングタイムを入力します。 設定した時間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。 • 設定可能範囲：0，10-1000000（秒） • 初期値：300（秒） 0 に設定した場合、学習した MAC アドレスは削除されません。
Aging Destination Hit	送信元 MAC アドレスだけでなく、宛先 MAC アドレスによる MAC アドレステーブルの更新を有効 / 無効に設定します。MAC アドレスのエージングタイムアウトによるフラッディングを抑えることができます。

「Apply」ボタンをクリックして、設定内容を適用します。

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

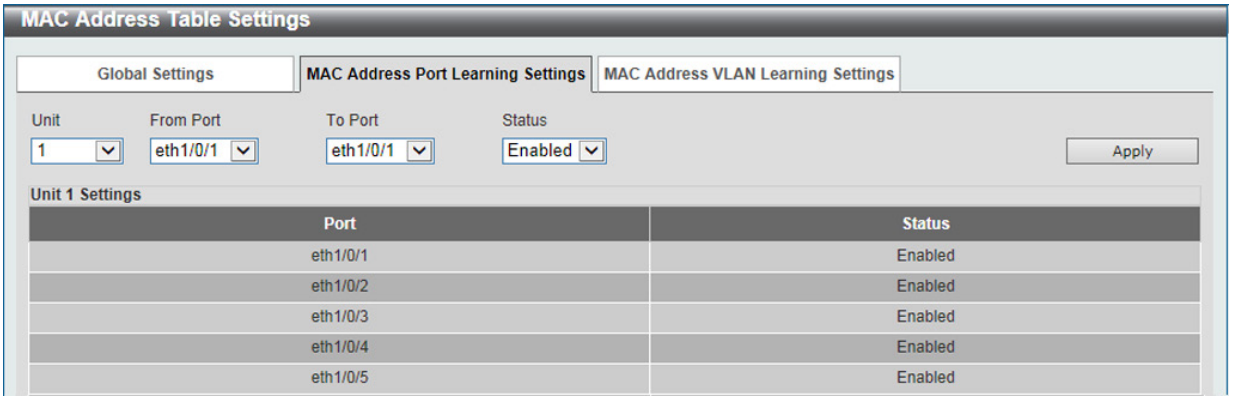


図 8-4　MAC Address Table Settings (MAC Address Port Learning Settings) 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

注意　MAC Address Port Learning の無効設定時、学習済みアドレスはエージングアウトまで保持、未学習の送信元 MAC アドレスのパケットはフラッディングします。

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

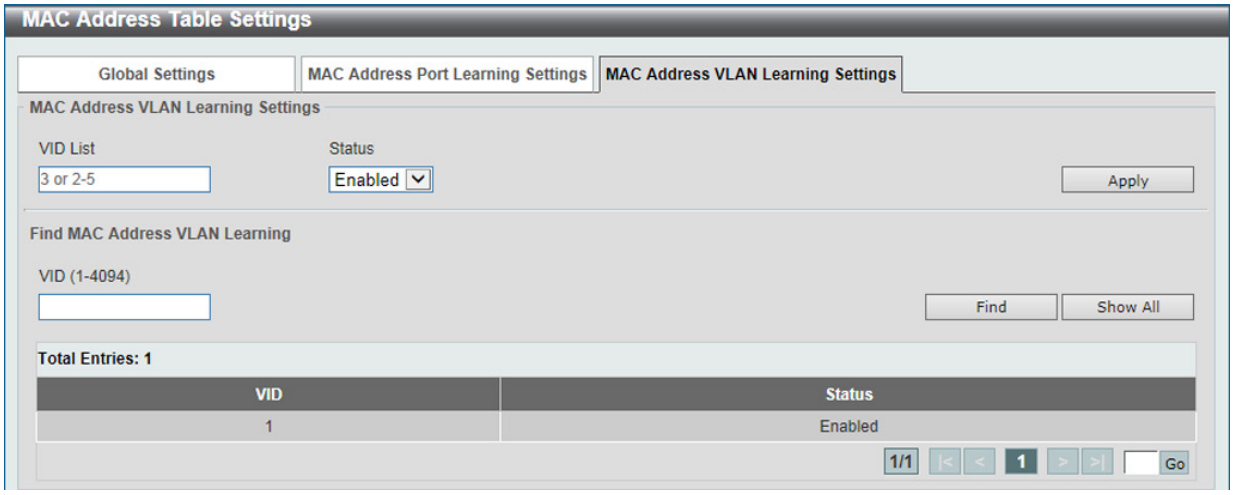


図 8-5　MAC Address Table Settings (MAC Address VLAN Learning Settings) 画面

画面に表示される項目：

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

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

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

MAC Address Table（MAC アドレステーブル）

スイッチの MAC アドレスフォワーディングテーブルを参照します。

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

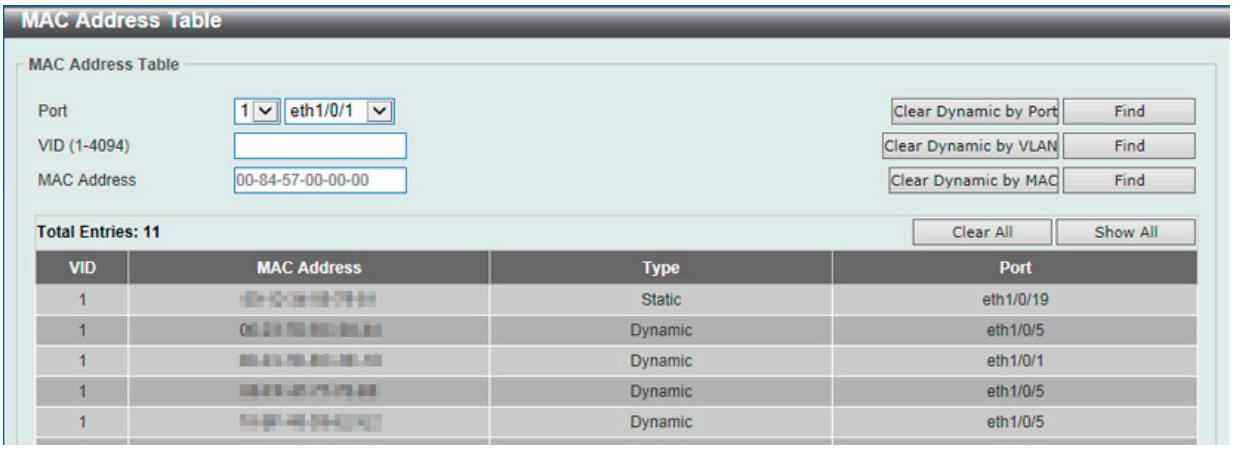


図 8-6　MAC Address Table 画面

画面に表示される項目：

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

エントリの検索 / 表示

「Find」ボタンをクリックして、指定したポート、VLAN または MAC アドレスをキーとして検索します。
「Show All」ボタンをクリックして、アドレステーブルのすべてのエントリを表示します。

ダイナミックエントリの削除

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

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

MAC Notification（MAC 通知）

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

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。

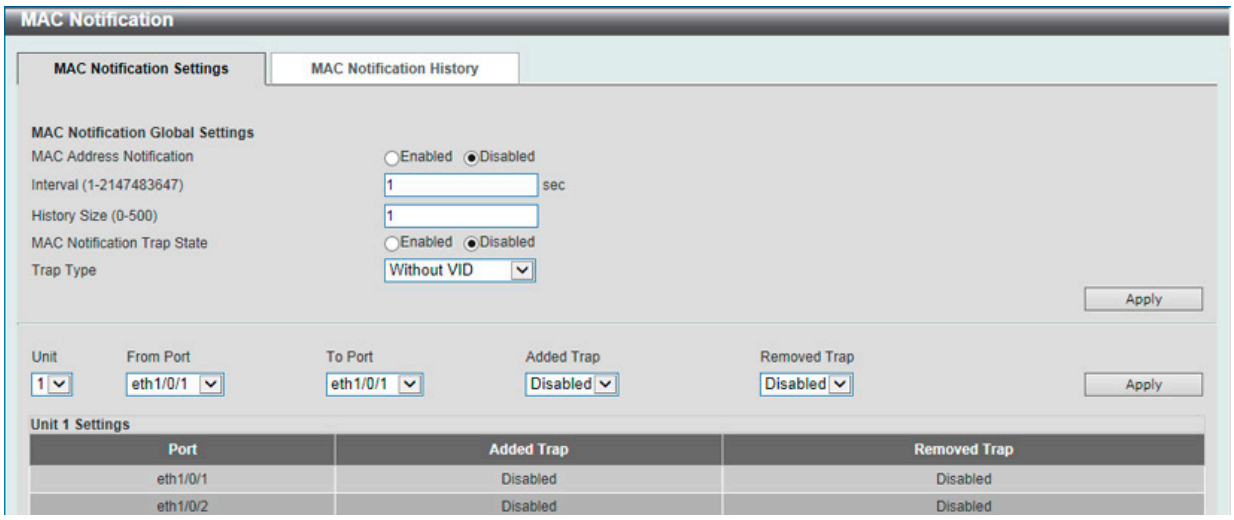


図 8-7　MAC Notification（MAC Notification Settings）画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

MAC Notification History タブ

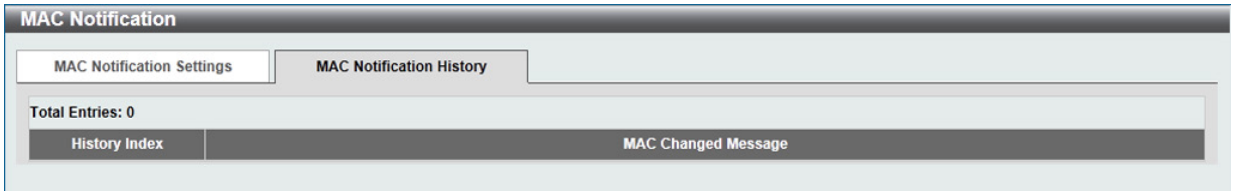


図 8-8　MAC Notification（MAC Notification History）画面

MAC 通知メッセージの履歴が表示されます。

VLAN（VLAN 設定）

スイッチの VLAN 設定を行います。

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

ウィザードを使用して VLAN の作成と設定を行います。

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



図 8-9　VLAN Configuration Wizard 画面

画面に表示される項目：

項目	内容
Create VLAN	新しく VLAN を作成する場合に選択します。VID を 1-4094 の間で入力します。
Configure VLAN	作成済みの VLAN を編集する場合に選択します。設定する VID を 1-4094 の間で入力します。

「Next」をクリックし、以下の画面で設定を行います。

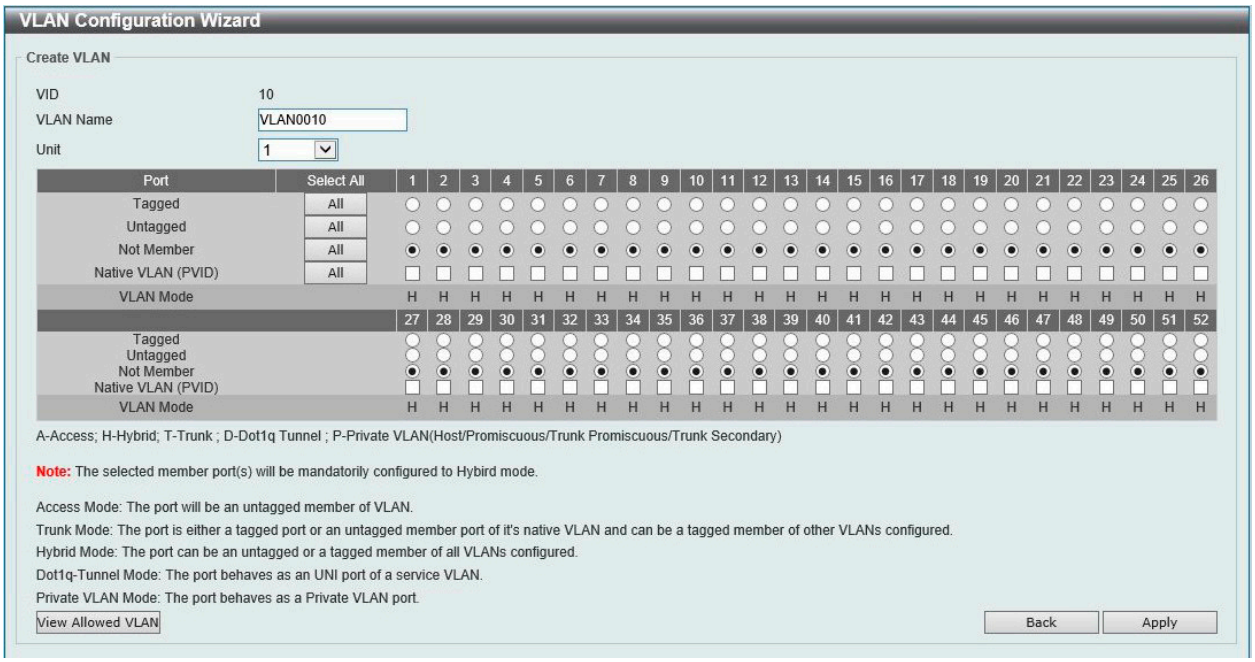


図 8-10　VLAN Configuration Wizard 画面

画面に表示される項目：

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

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

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

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

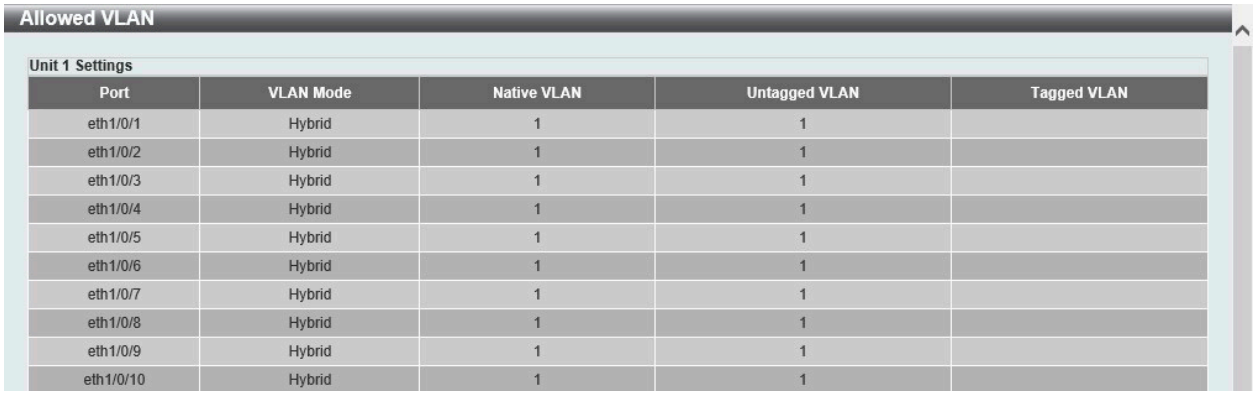


図 8-11　Allowed VLAN 画面

802.1Q VLAN（802.1Q VLAN）

802.1Q VLAN を設定します。

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

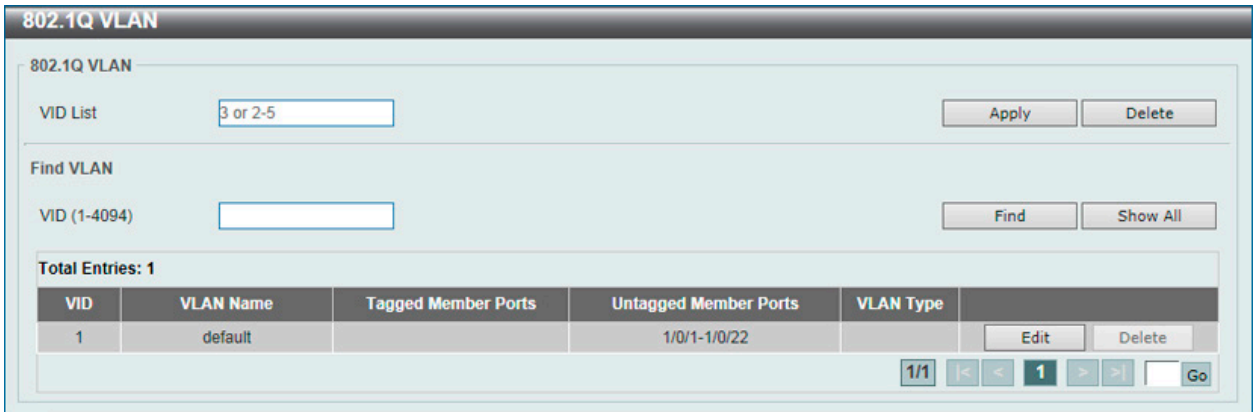


図 8-12　802.1Q VLAN Settings 画面

画面に表示される項目：

項目	内容
802.1Q VLAN	
VID List	作成する VLAN ID または VLAN ID の範囲を指定します。

項目	内容
Find VLAN	
VID	表示する VLAN ID を指定します。
VLAN Name	既存エントリの「Edit」ボタンをクリックした後、VLAN 名を編集することができます。

「Apply」ボタンをクリックし、VLAN エントリを作成します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

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

VLAN Interface（VLAN インタフェース）

VLAN インタフェースの設定を行います。

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

VLAN Interface（VLAN インタフェース設定）

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

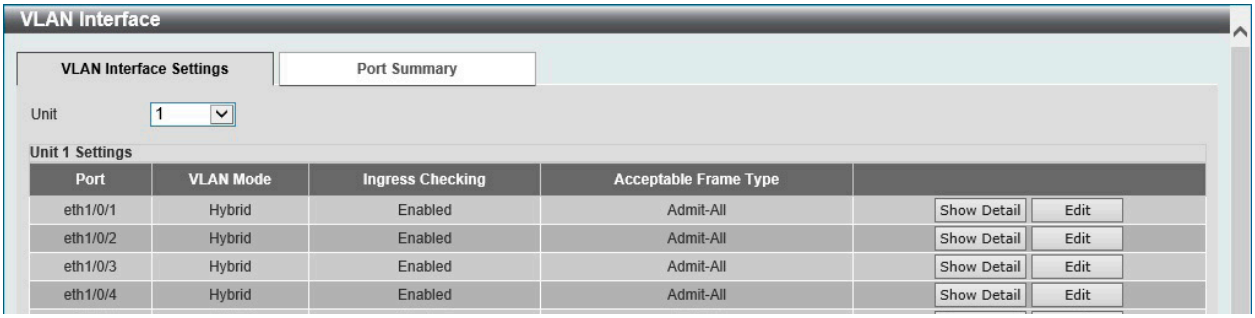


図 8-13　VLAN Interface 画面 - VLAN Interface Settings タブ

画面に表示される項目：

項目	説明
Unit	表示 / 設定を行うユニットを選択します。

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

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 Detail（VLAN 詳細情報の表示）

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



図 8-14　VLAN Interface Information 画面

前の画面に戻るには、「Back」ボタンをクリックします。

■ Edit（VLAN インタフェース設定の編集）

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

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

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

● VLAN モード「Access」を選択した場合：

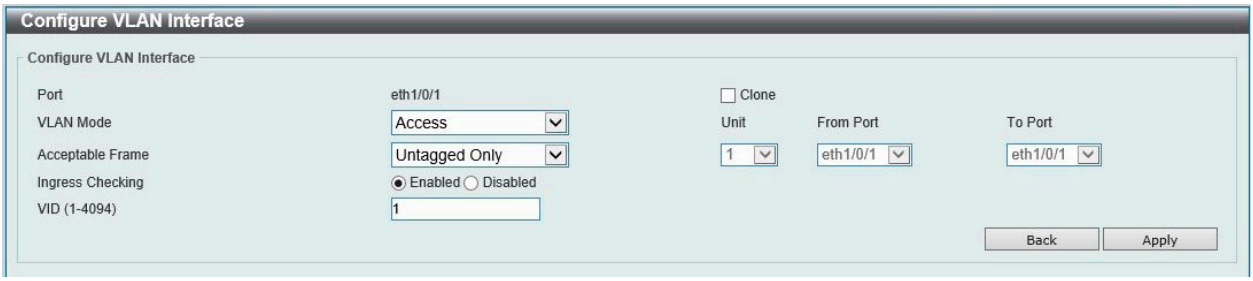


図 8-15　Configure VLAN Interface 画面（Access 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Access」を選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
VID	VLAN ID を指定します。 • 設定可能範囲：1 -4094
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

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

● VLAN モード「Hybrid」を選択した場合：

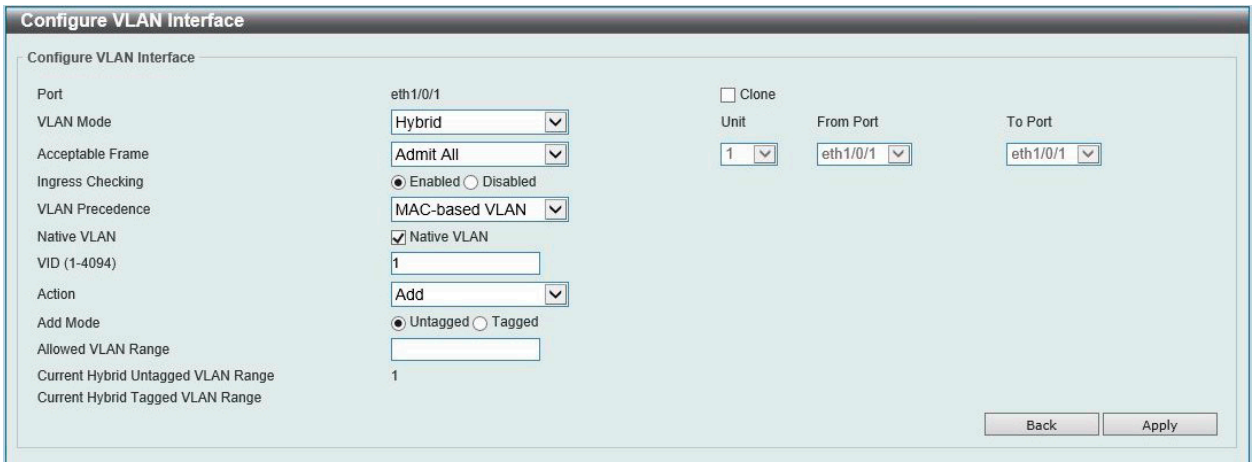


図 8-16　Configure VLAN Interface 画面（Hybrid 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Hybrid」を選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」

項目	内容
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
VLAN Precedence	優先 VLAN を選択します。 • 「Mac-based VLAN」「Subnet-based VLAN」
Native VLAN	Native VLAN を有効にします。
VID	Native VLAN を有効にした場合は、設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
Action	実行する動作を選択します。 • 選択肢：「Add」「Remove」「Tagged」「Untagged」
Add Mode	「Add Mode」のパラメータとして、タグ付きまたはタグなしを指定します。 • 選択肢：「Untagged」「Tagged」
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

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

注意　「Allowed VLAN Range」には最大 256 文字まで入力可能です。

● **VLAN モード「Trunk」を選択した場合：**

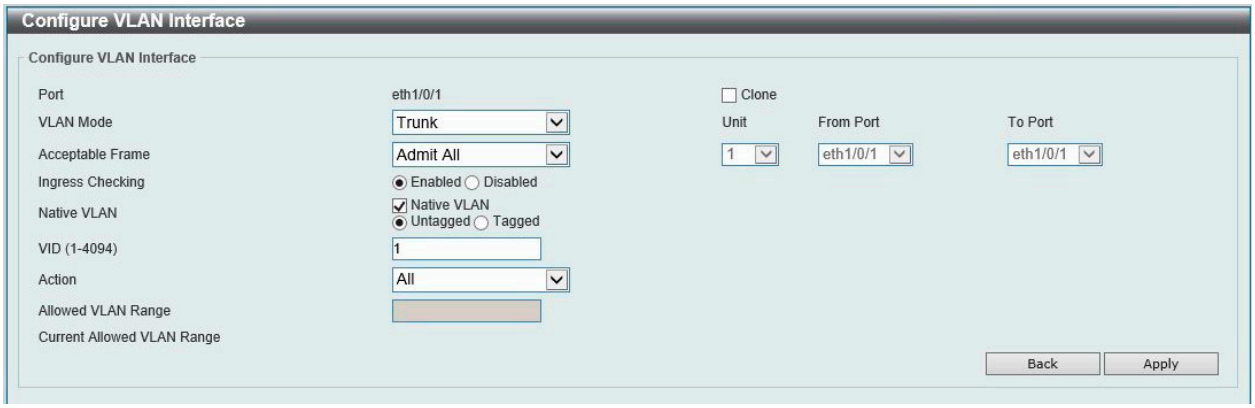


図 8-17　Configure VLAN Interface 画面（Trunk 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Trunk」を選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
Native VLAN	Native VLAN を有効にします。「Untagged」または「Tagged」フレームを選択します。
VID	Native VLAN を有効にした場合は、設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
Action	実行する動作を選択します。 • 選択肢：「None」「All」「Add」「Remove」「Except」「Replace」
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

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

注意　「Allowed VLAN Range」には最大 256 文字まで入力可能です。

● **VLAN モード「Dot1q-Tunnel」を選択した場合：**

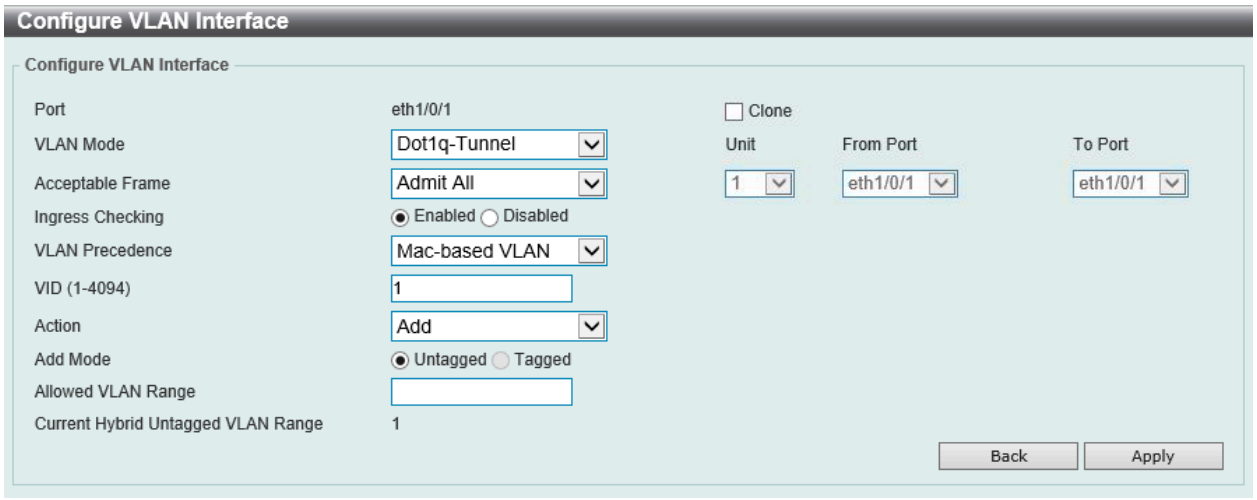


図 8-18　Configure VLAN Interface 画面（Dot1q-Tunnel 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Dot1q-Tunnel」を選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
VLAN Precedence	優先 VLAN を選択します。 • 「Mac-based VLAN」「Subnet-based VLAN」
VID	設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
Action	実行する動作を選択します。 • 選択肢：「Add」「Remove」
Add Mode	「Add Mode」のパラメータに「Untagged」を追加します。
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

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

注意　「Allowed VLAN Range」には最大 256 文字まで入力可能です。

● **VLAN モード「Promiscuous」を選択した場合：**

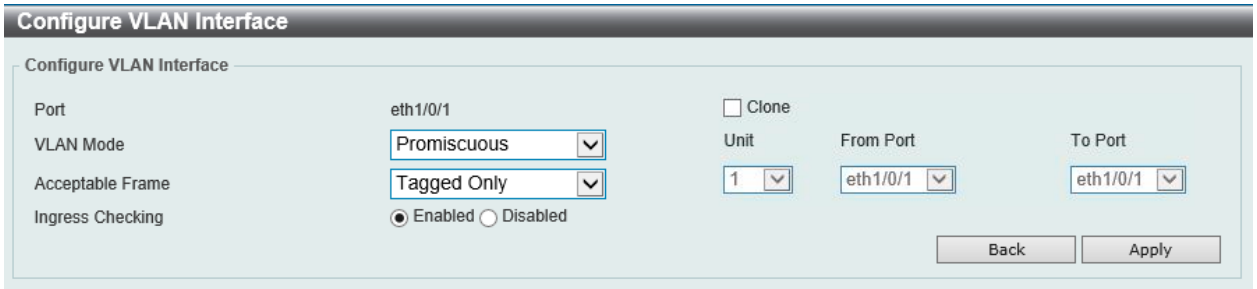


図 8-19　Configure VLAN Interface 画面（Promiscuous 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Promiscuous」を選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」

項目	内容
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

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

● **VLAN モード「Host」を選択した場合：**

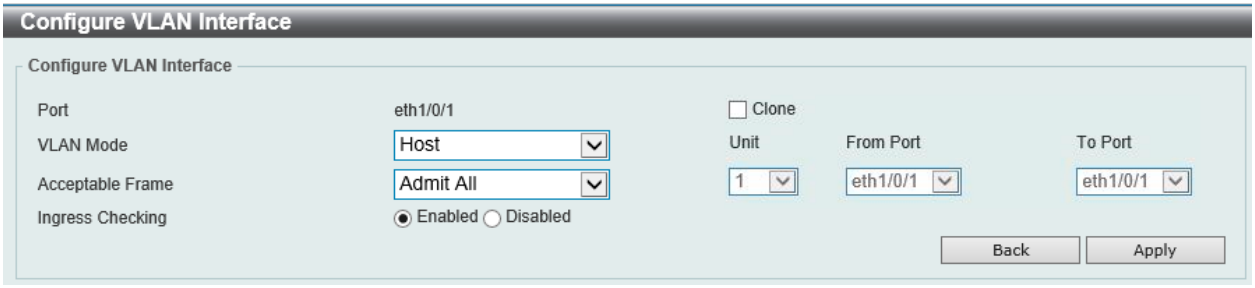


図 8-20　Configure VLAN Interface 画面（Host 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Host」を選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

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

● **VLAN モード「Trunk Promiscuous」を選択した場合：**

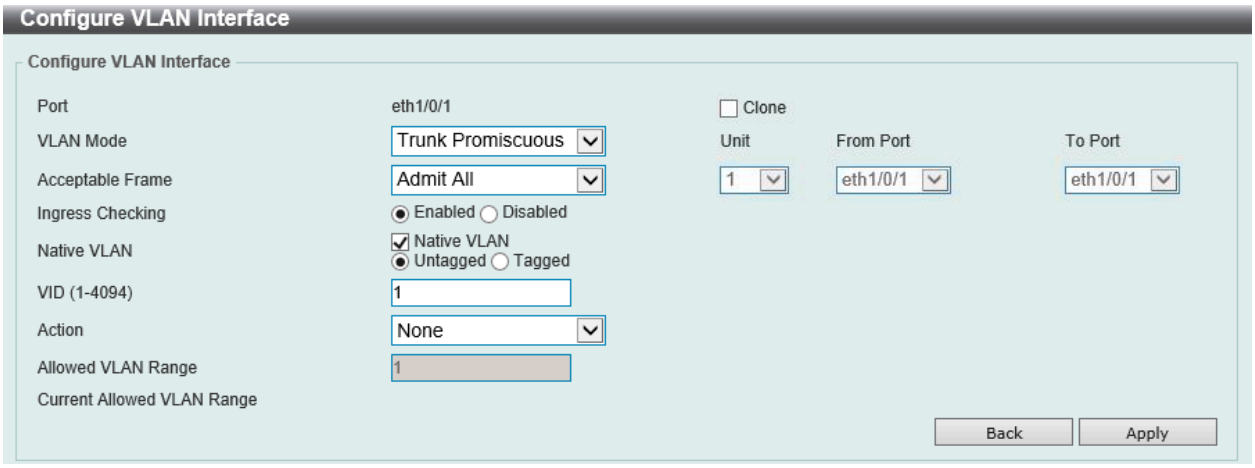


図 8-21　Configure VLAN Interface 画面（Trunk Promiscuous 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Trunk Promiscuous」を選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」

項目	内容
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
Native VLAN	Native VLAN を有効にします。「Untagged」または「Tagged」フレームを選択します。
VID	Native VLAN を有効にした場合は、設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
Action	実行する動作を選択します。 • 選択肢：「None」「All」「Add」「Remove」「Except」「Replace」
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

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

注意　「Allowed VLAN Range」には最大 256 文字まで入力可能です。

● **VLAN モード「Trunk Secondary」を選択した場合：**

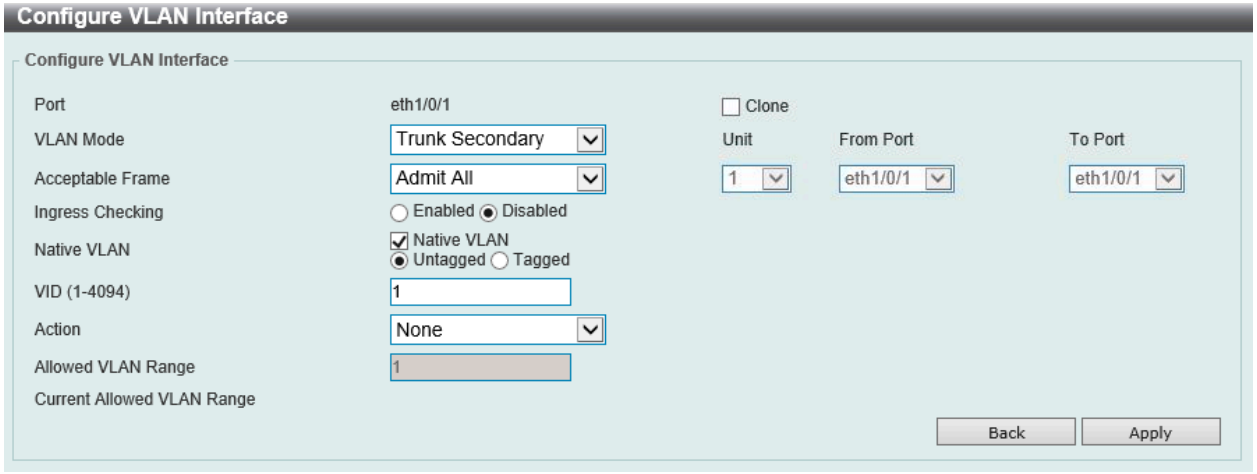


図 8-22　Configure VLAN Interface 画面（Trunk Secondary 選択時）

画面に表示される項目：

項目	内容
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードをから選択します。ここでは「Trunk Secondary」を選択します。 • 選択肢：「Access」「Hybrid」「Trunk」「Dot1q-Tunnel」「Promiscuous」「Host」「Trunk Promiscuous」「Trunk Secondary」
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に設定します。
Native VLAN	Native VLAN を有効にします。「Untagged」または「Tagged」フレームを選択します。
VID	Native VLAN を有効にした場合は、設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
Action	実行する動作を選択します。 • 選択肢：「None」「All」「Add」「Remove」「Except」「Replace」
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
Unit	設定内容をコピーするユニットを指定します。
From Port / To Port	設定内容をコピーするポート範囲を指定します。

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

注意　「Allowed VLAN Range」には最大 256 文字まで入力可能です。

Port Summary（ポートサマリー）

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

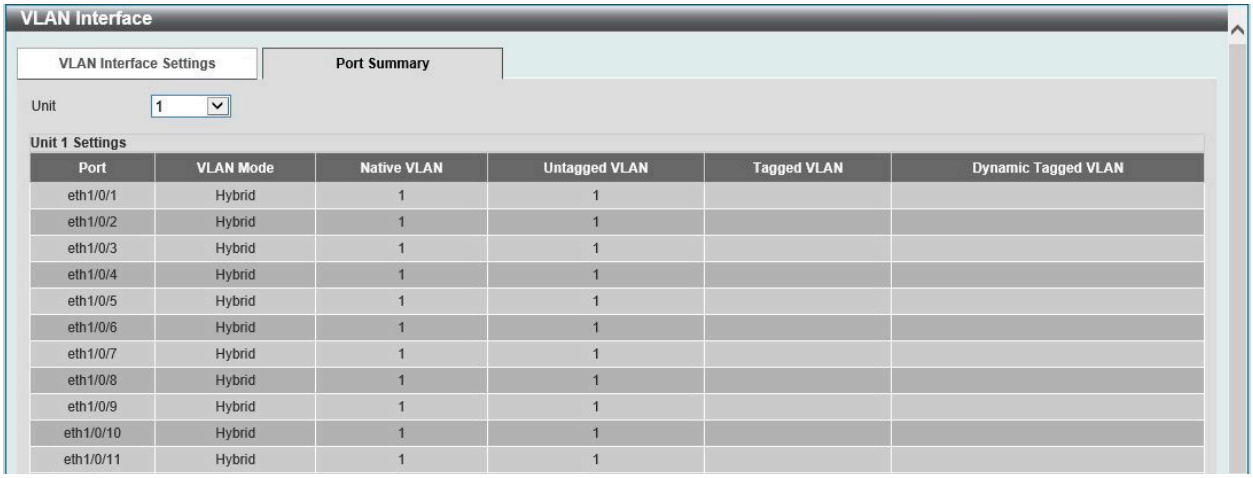


図 8-23　VLAN Interface 画面 - Port Summary タブ

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

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

802.1v プロトコル VLAN の設定を行います。

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

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

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

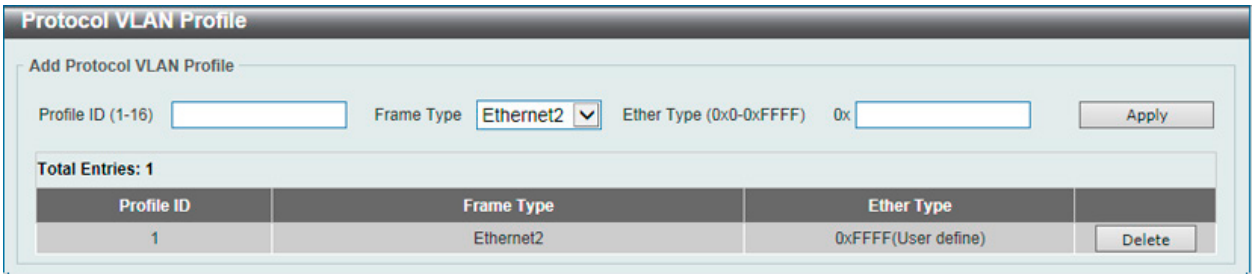


図 8-24　Protocol VLAN Profile 画面

画面に表示される項目：

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

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

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

プロトコル VLAN ポートの設定を行います。

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

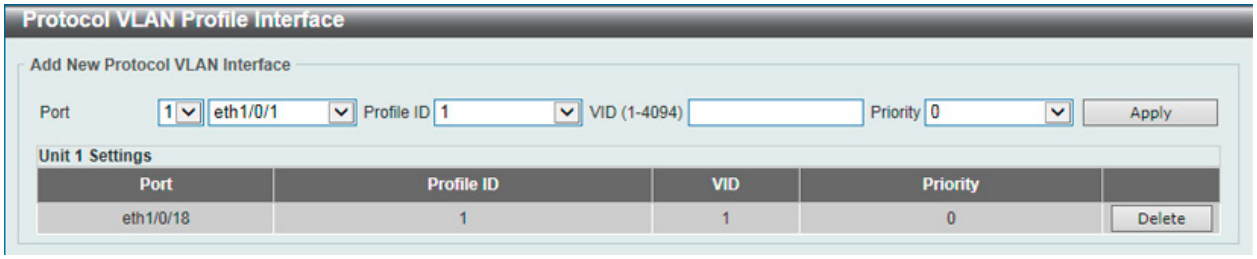


図 8-25　Protocol VLAN Profile Interface 画面

画面に表示される項目：

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

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

GVRP（GVRP の設定）

GVRP Global（GVRP グローバル設定）

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

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

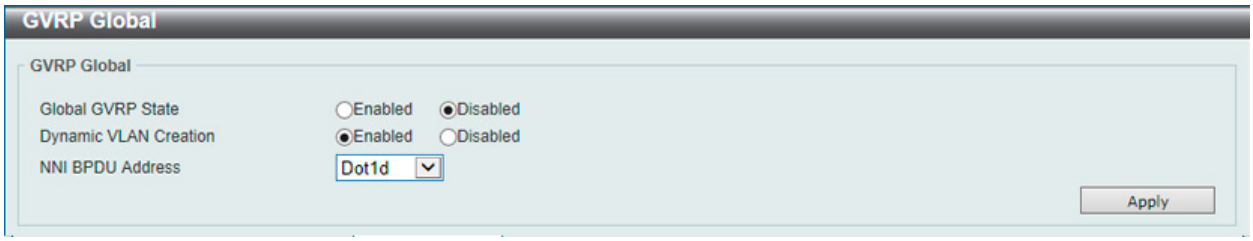


図 8-26　GVRP Global 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

GVRP Port（GVRP ポート設定）

ポート毎に GVRP のパラメータを設定します。

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

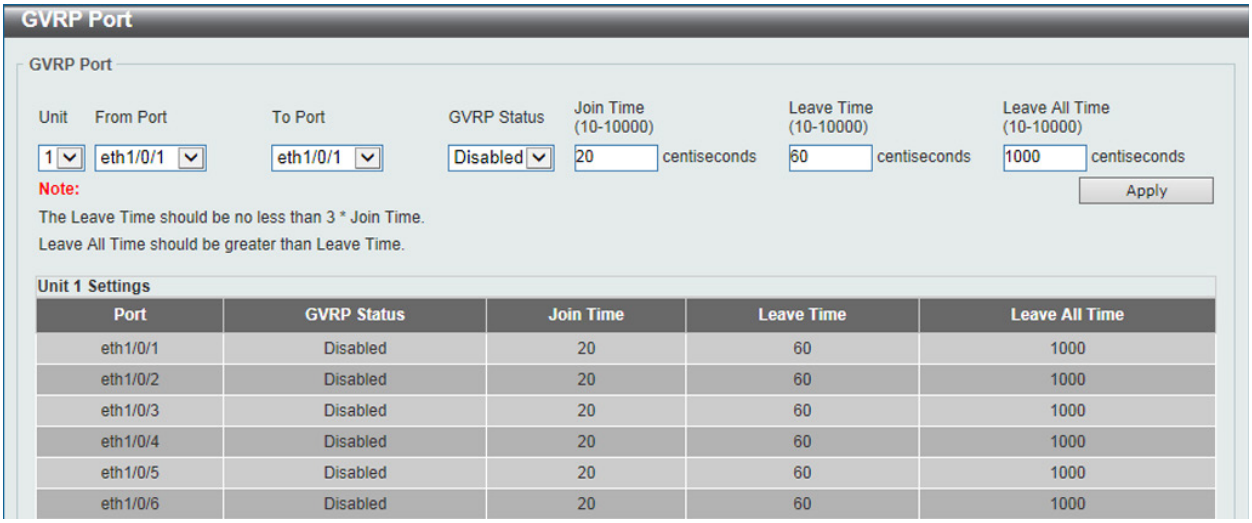


図 8-27　GVRP Port 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
GVRP Status	各ポートの GVRP ステータスを有効 / 無効に設定します。有効にするとポートが自動的に VLAN のメンバになります。 • 初期値：「Disabled（無効）」
Join Time	開始時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 初期値：20
Leave Time	終了時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 初期値：60
Leave All Time	全終了時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 初期値：1000

「Apply」ボタンをクリックして、設定内容を適用します。

GVRP Advertise VLAN（GVRP アドバタイズ VLAN 設定）

GVRP アドバタイズ VLAN の設定、表示を行います。

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

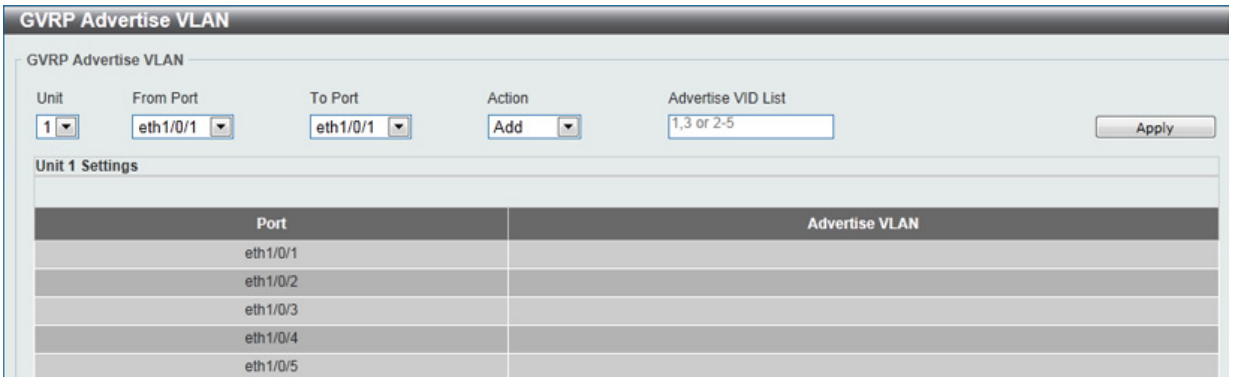


図 8-28　GVRP Advertise VLAN 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。

項目	説明
From Port / To Port	本設定を適用するポート範囲を指定します。
Action	アドバタイズ VLAN に対するアクションを選択します。「All」を選択するとすべてのアドバタイズ VLAN が対象となります。 • 選択肢：「All」「Add」「Remove」「Replace」
Advertise VID List	アドバタイズ VLAN ID を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

GVRP Forbidden VLAN（GVRP Forbidden VLAN 設定）

GVRP Forbidden VLAN の設定、表示を行います。

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

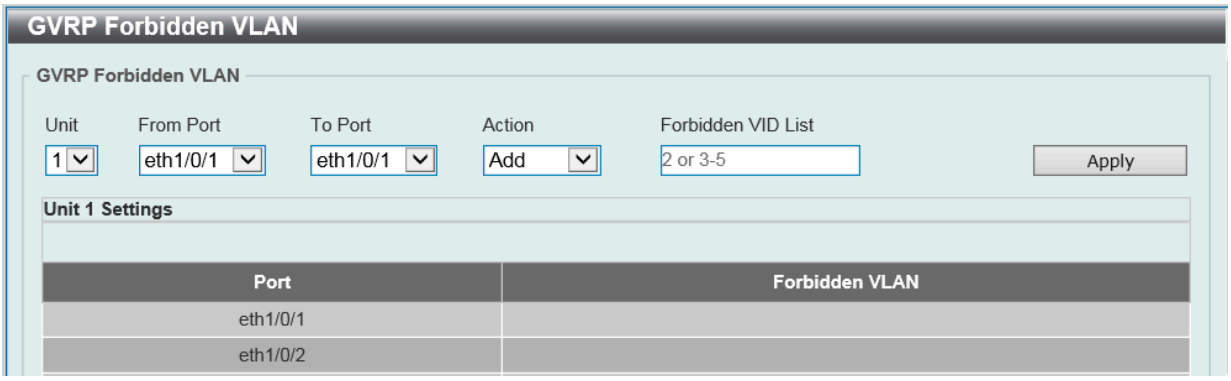


図 8-29　GVRP Forbidden VLAN 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Action	禁止 VLAN に対するアクションを選択します。「All」を選択するとすべての禁止 VLAN が対象となります。 • 選択肢：「All」「Add」「Remove」「Replace」
Forbidden VID List	禁止 VLAN ID を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

GVRP Statistics Table（GVRP 統計テーブル）

GVRP の統計情報を表示します。

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

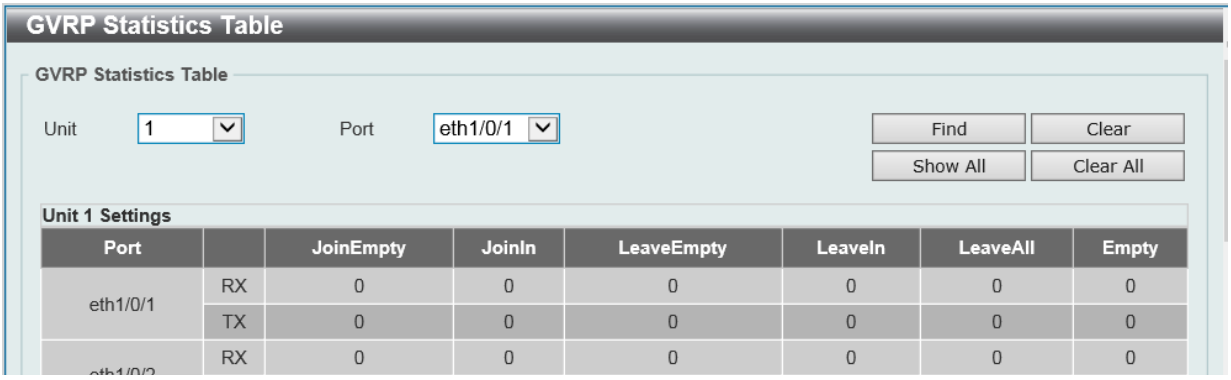


図 8-30　GVRP Statistics Table 画面

画面に表示される項目：

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

エントリの検索
「Find」ボタンをクリックして、エントリを検索します。
「Show All 」ボタンをクリックして、すべてのエントリを表示します。

エントリの削除
「Clear」ボタンをクリックして、指定ポートのエントリを削除します。
「Clear All 」ボタンをクリックして、すべてのエントリを削除します。

MVRP（MVRP の設定）

MVRP Global（MVRP グローバル設定）

MVRP（Multiple VLAN Registration Protocol）の設定を行います。

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



図 8-31　MVRP Global Settings 画面

画面に表示される項目：

項目	説明
Global MVRP State	MVRP のグローバルステータスを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

MVRP Port Settings（MVRP ポート設定）

ポート毎に MVRP のパラメータを設定します。

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

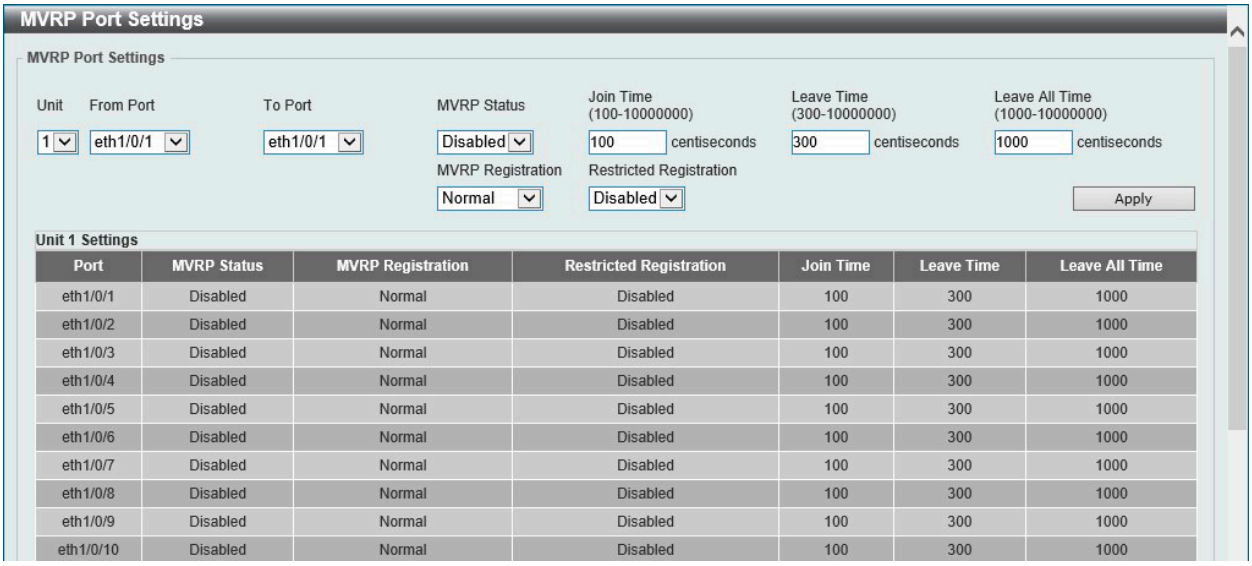


図 8-32　MVRP Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
MVRP Status	各ポートの MVRP ステータスを有効 / 無効に設定します。
Join Time	開始時間を設定します。 • 設定可能範囲：100-10000000（センチ秒）
Leave Time	終了時間を設定します。 • 設定可能範囲：300-10000000（センチ秒）
Leave All Time	全終了時間を設定します。 • 設定可能範囲：1000-10000000（センチ秒）

項目	説明
MVRP Registration	MVRP の登録方法を選択します。 • 「Normal」- すべての MVRP 要求とメッセージについて、受信および処理を実行します。 • 「Fixed」- 追加の MVRP 要求とメッセージを無視します。ポート上の既存の登録はすべて保持されます。 • 「Forbidden」- VLAN1 を除くすべての VLAN の登録について、ポート上で解除されます。
Restricted Registration	登録の制限を有効 / 無効に設定します。本設定を有効にした場合、VLAN にスタティック VLAN エントリが存在し、このポートの Registrar Administrative Control の値が Normal Registration である場合にのみ、新しいダイナミック VLAN エントリの作成が許可されます。

「Apply」ボタンをクリックして、設定内容を適用します。

MVRP Statistics（MVRP 統計）

MVRP の統計情報を表示します。

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

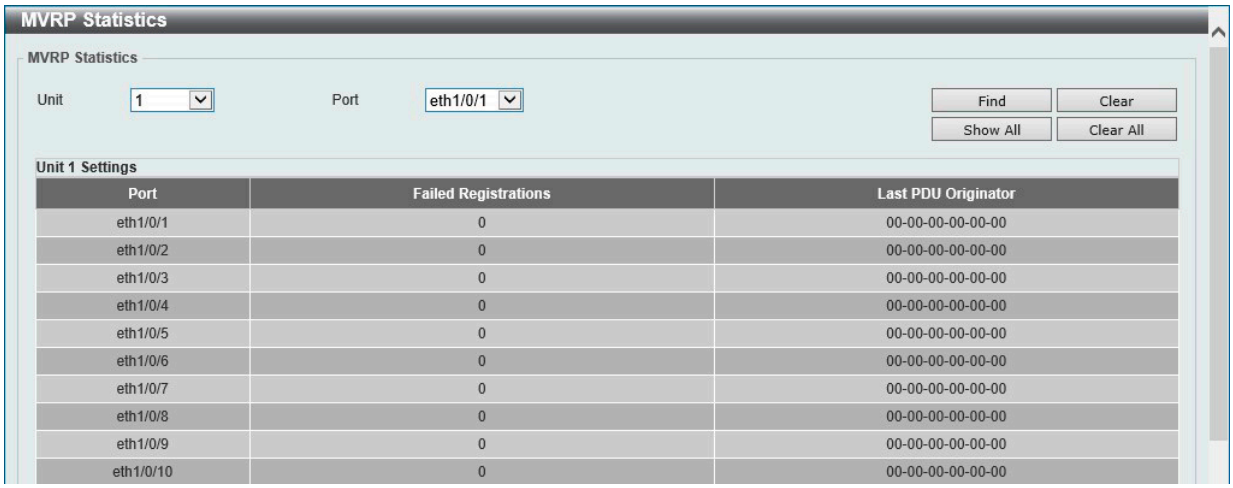


図 8-33　MVRP Statistics 画面

画面に表示される項目：

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

エントリの検索

「Find」ボタンをクリックして、指定ポートのエントリを検索します。
「Show All 」ボタンをクリックして、すべてのエントリを表示します。

エントリの削除

「Clear」ボタンをクリックして、指定ポートのエントリを削除します。
「Clear All 」ボタンをクリックして、すべてのエントリを削除します。

Asymmetric VLAN（Asymmetric VLAN 設定）

Asymmetric VLAN を 設定します。

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

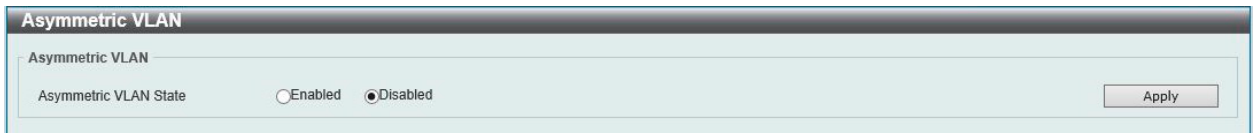


図 8-34　Asymmetric VLAN 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、設定内容を適用します。

注意　Asymmetric VLAN は、重複する全 VLAN に学習した MAC Address を乗せる事により異なる Native VLAN 間の Flooding を抑止します。

MAC VLAN（MAC VLAN 設定）

MAC ベース VLAN を設定、表示します。スタティック MAC ベース VLAN エントリが作成されると、ポートの VLAN は接続するデバイスによって変わります。

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

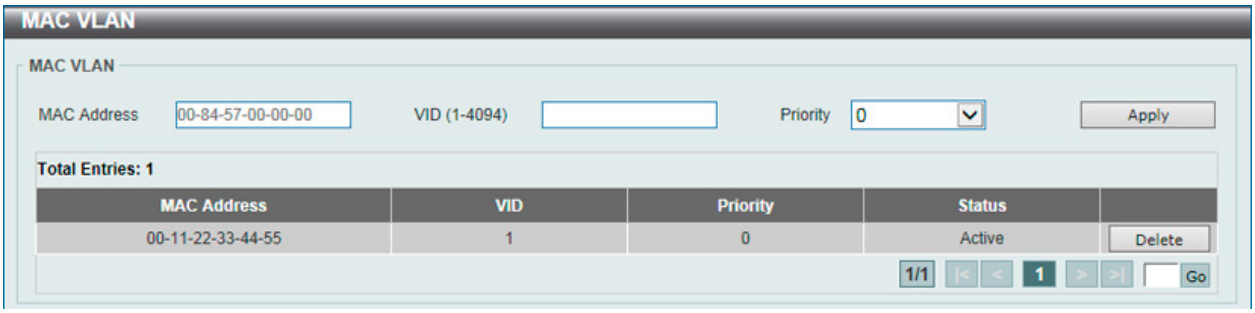


図 8-35　MAC VLAN 画面

画面に表示される項目：

項目	説明
MAC Address	ユニキャスト MAC アドレスを入力します。
VID	VLAN ID を入力します。
Priority	タグなしパケットに割り当てる優先度を選択します。 • 設定可能範囲：0-7

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

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

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

L2 VLAN インタフェースについて表示、設定を行います。

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

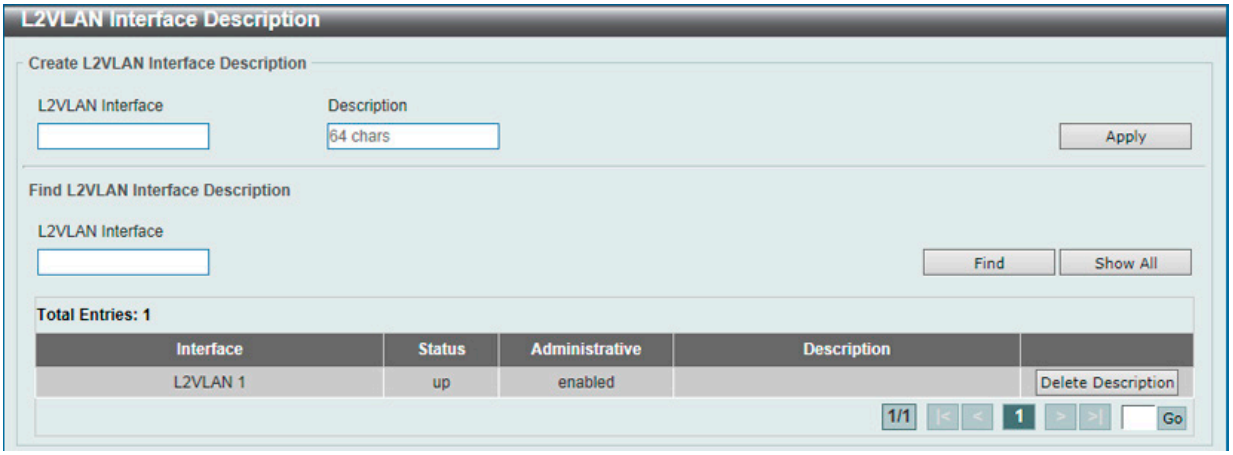


図 8-36　L2VLAN Interface Description 画面

画面に表示される項目：

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

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

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 を設定します。サブネット VLAN エントリは、IP サブネットベースの VLAN 分類ルールです。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 エントリに照合されます。送信元 IP がエントリのサブネットに存在する場合、パケットはこのサブネットに定義された VLAN に分類されます。

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。

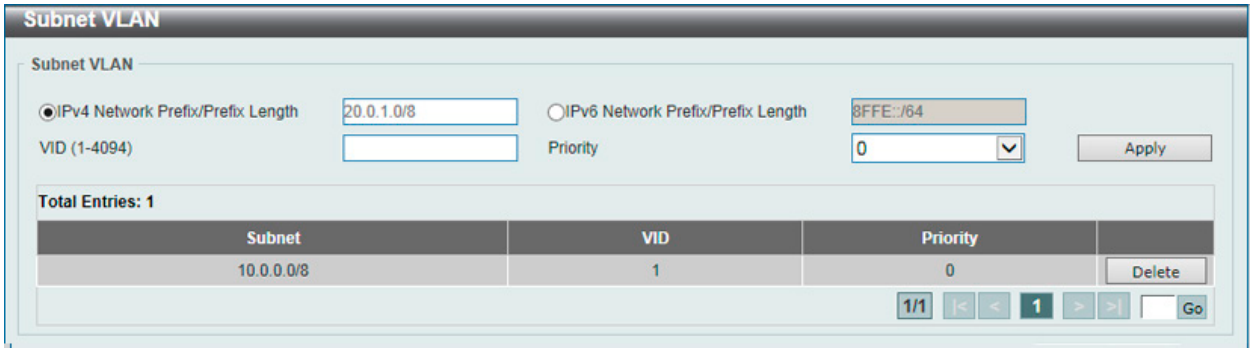


図 8-37　Subnet VLAN 画面

画面に表示される項目：

項目	説明
IPv4 Network Prefix / Prefix Length	サブネット VLAN の IPv4 アドレスとプレフィックス長を入力します。
IPv6 Network Prefix / Prefix Length	サブネット VLAN の IPv6 アドレスとプレフィックス長を入力します。
VID	サブネット VLAN の VID を入力します。
Priority	優先度を選択します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

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

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）

Super VLAN エントリの表示と設定を行います。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 に物理メンバポートを設定することはできません。また、Super VLAN とサブ VLAN を同時に設定することはできません。IP インタフェースが Super VLAN に割り当てられると、サブ VLAN 間の通信のためにインタフェースでプロキシ ARP が自動的に有効になります。Super VLAN を複数設定することも可能であり、各 Super VLAN は複数のサブ VLAN で構成されます。

注意　Private VLAN と Super VLAN は相互排他機能です。Private VLAN は Super VLAN として設定できません。
L3 ルーティングプロトコル、マルチキャストプロトコル、IPv6 プロトコルは、Super VLAN インタフェースで動作できません。

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

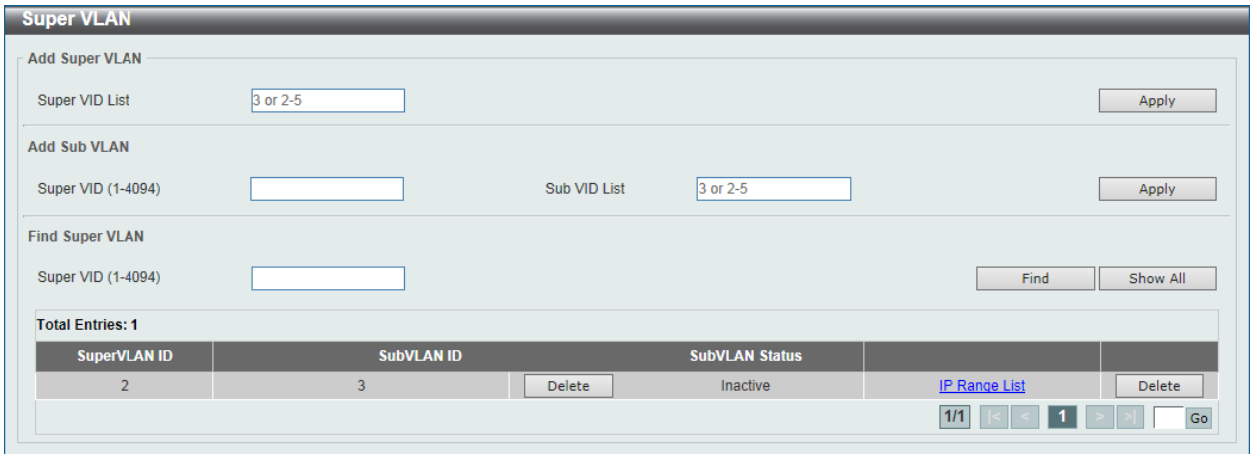


図 8-38　Super VLAN 画面

画面に表示される項目：

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 に関連づける Super VLAN の VLAN ID を入力します。 • 設定可能範囲：1-4094
Sub VID List	Super VLAN のサブ VLAN を入力します。
Find Super VLAN	
Super VID	表示する Super VLAN の VLAN ID を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「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。
「IP Range List」ボタンをクリックすると、サブ VLAN に IP 範囲を指定することができます。

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。

■ 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。

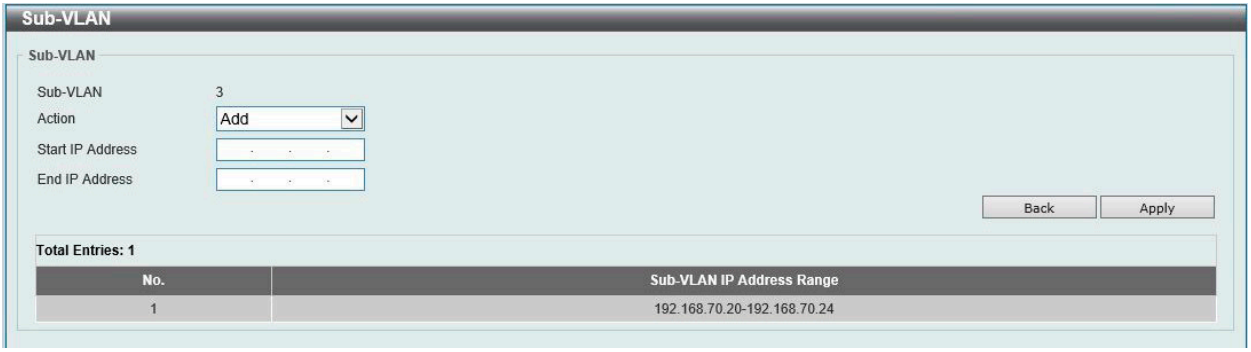


図 8-39　Sub-VLAN 画面

画面に表示される項目：

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	サブ VLAN の IP アドレス範囲の開始 IP アドレスを入力します。
End IP Address	サブ VLAN の IP アドレス範囲の終了 IP アドレスを入力します。

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

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

自動サーベイランス VLAN は、IP サーベイランスサービスを強化するための機能です。音声 VLAN と同様、D-Link IP カメラからのビデオトラフィックに対して自動的に VLAN をアサインします。優先度が高いこと、また個別の VLAN を使用することで、サーベイトラフィックの品質とセキュリティを保証します。

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

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

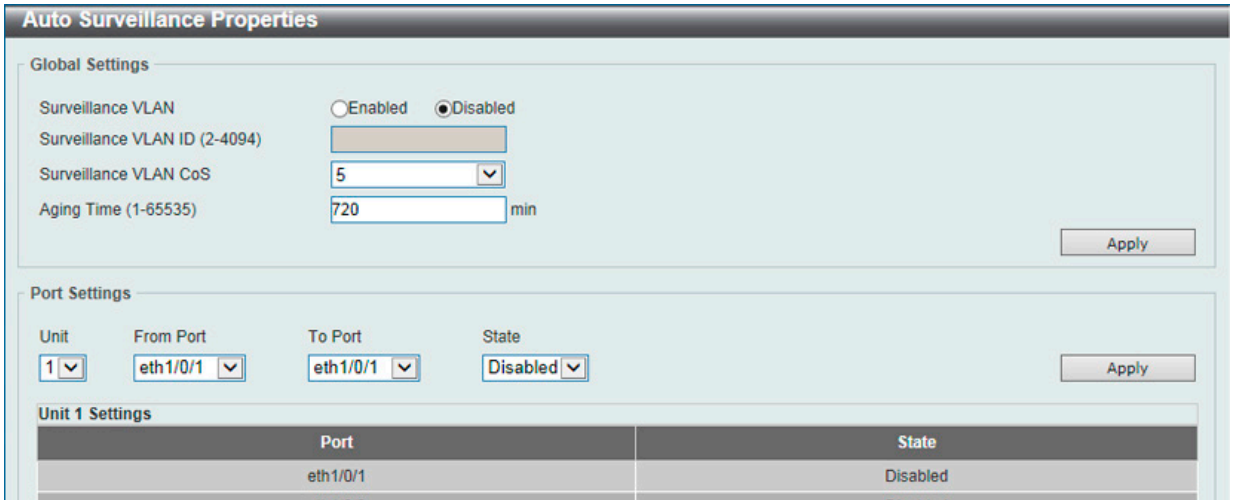


図 8-40　Auto Surveillance Properties 画面

画面に表示される項目：

項目	説明
Global Settings	
Surveillance VLAN	サーベイランス VLAN を有効 / 無効に設定します。
Surveillance VLAN ID	サーベイランス VLAN の VLAN ID を指定します。VLAN をサーベイランス VLAN に割り当てる前に、通常の VLAN として作成する必要があります。 • 設定可能範囲：2-4094
Surveillance VLAN CoS	サーベイランス VLAN の優先値を指定します。 サーベイランス VLAN が有効化されたポートで受信したサーベイランスパケットは、この CoS 値でマークされます。これにより、QoS データトラフィックとは区別されます。 • 設定可能範囲：0-7
Aging Time	エージングタイムを設定します。本機能は、サーベイランス VLAN ダイナミックメンバポートのエージングタイムを設定するために使用されます。サーベイランスデバイスがトラフィックの送信を停止し、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。サーベイランストラフィックがエージングタイム内に再開すると、エージングタイマはキャンセルされます。 • 設定可能範囲：1-65535（分）
Port Settings	
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
State	指定したポートでサーベイランス VLAN を有効 / 無効に設定します。 サーベイランス VLAN が有効な場合、ポートはアンタグのサーベイランス VLAN メンバとして自動的に学習され、受信したアンタグのサーベイランスパケットはサーベイランス VLAN に転送されます。受信したパケットの送信元 MAC アドレスが OUI（Organizationally Unique Identifier）アドレスに一致している場合、そのパケットはサーベイランスパケットとして認識されます。

「Apply」ボタンをクリックして、設定内容を適用します。

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

サーベイランスデバイスの表示と MAC アドレスの設定を行います。

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。

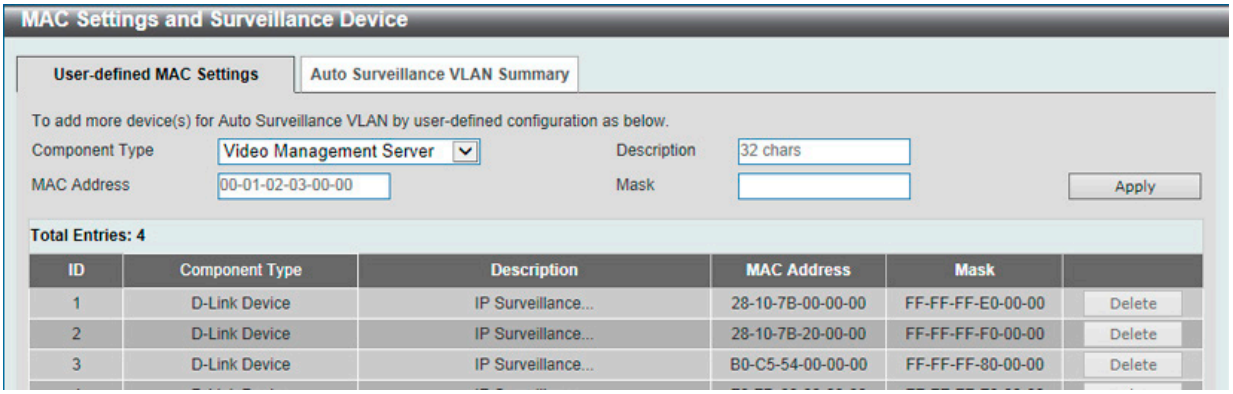


図 8-41　MAC Settings and Surveillance Device 画面 - User-defined MAC Settings タブ

画面に表示される項目：

項目	説明
Component Type	サーベイランス VLAN が自動検出可能なサーベイランスコンポーネントを選択します。 • 選択肢：「Video Management Server」「VMS Client/Remote Viewer」「Video Encoder」「Network Storage」「Other IP Surveillance Device」
Description	ユーザ定義の OUI に関する説明を入力します。（32 文字以内）
MAC Address	ユーザ定義の OUI MAC アドレスを入力します。受信パケットの MAC アドレスが OUI パターンにいずれかと一致すると、そのパケットはサーベイランスパケットとして識別されます。
Mask	ユーザ定義 OUI MAC アドレスマスクを入力します。

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

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。

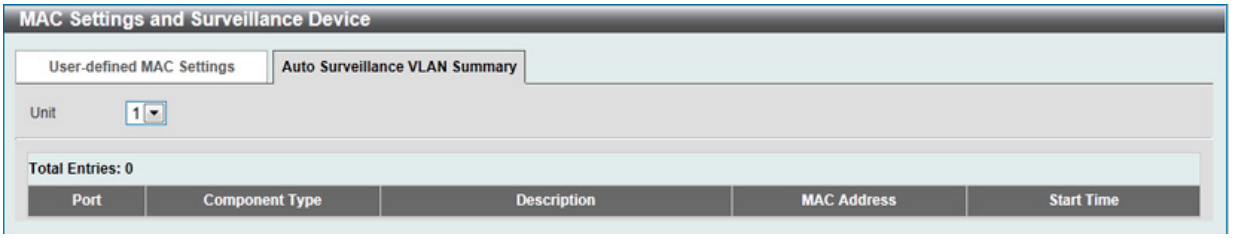


図 8-42　MAC Settings and Surveillance Device 画面 - Auto Surveillance VLAN Summary タブ

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

Voice VLAN（音声 VLAN）

Voice VLAN Global（音声 VLAN グローバル設定）

音声 VLAN の設定を行います。本スイッチの音声 VLAN は 1 つのみです。

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

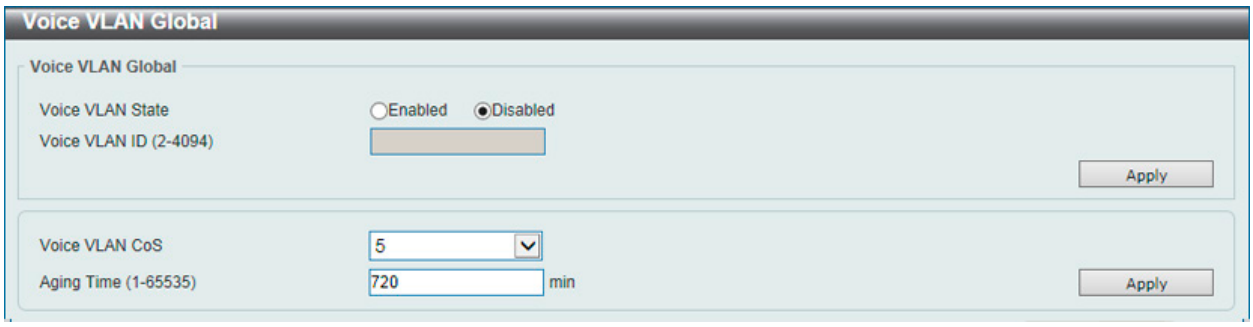


図 8-43　Voice VLAN Global Settings 画面

画面に表示される項目：

項目	説明
Voice VLAN State	音声 VLAN 機能を有効 / 無効に設定します。
Voice VID	音声 VLAN の VLAN ID を入力します。指定する VLAN は事前に作成しておく必要があります。 • 設定可能範囲：2-4094
Voice VLAN CoS	音声 VLAN の優先度を設定します。音声 VLAN が有効化されたポートで受信した音声パケットは、この CoS 値でマークされます。これにより、QoS データトラフィックとは区別されます。 • 設定可能範囲：0-7
Aging Time	自動学習された音声デバイスと音声 VLAN 情報のエージングタイム を設定します。 音声デバイスがトラフィックの送信を停止し、この音声デバイスの MAC アドレスがエージングタイムに到達すると、音声 VLAN エージングタイマが開始されます。 ポートは音声 VLAN のエージングタイム経過後に音声 VLAN から削除されます。 音声トラフィックがエージングタイム内に再開すると、エージングタイマはキャンセルされます。 • 設定可能範囲：1-65535（分）

「Apply」ボタンをクリックして、設定内容を適用します。

Voice VLAN Port（音声 VLAN のポート設定）

ポートの音声 VLAN を設定、表示します。

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

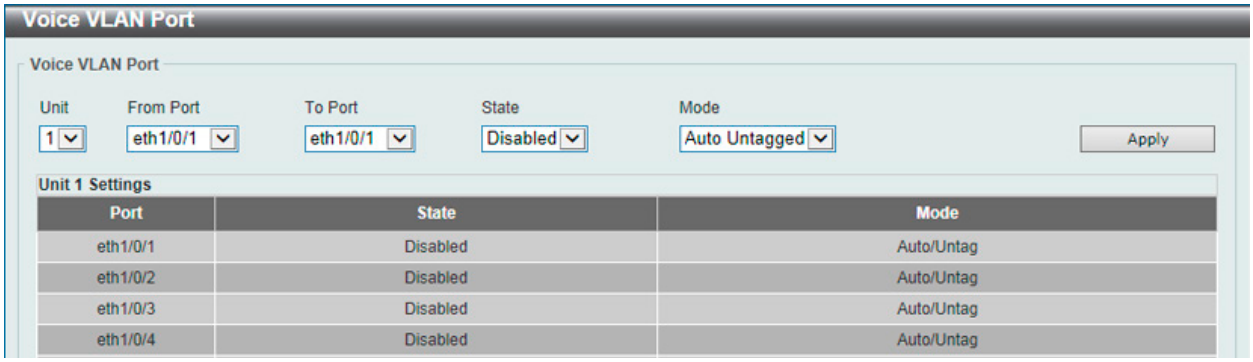


図 8-44　Voice VLAN Port 画面

画面に表示される項目：

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

項目	説明
Mode	モードを選択します。 • 「Auto Untagged」- タグなしの音声 VLAN メンバシップが自動的に学習されます。 • 「Auto Tagged」- タグ付きの音声 VLAN メンバシップが自動的に学習されます。 • 「Manual」- 音声 VLAN メンバシップを手動で設定します。 指定ポートで自動学習が有効化されている場合、音声 VLAN メンバは自動的に学習され、エージアウトします。 「Auto Tagged」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、タグ付きメンバとして音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなしパケットは Port VLAN ID（PVID）で転送されます。 「Auto Untagged」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、タグなしメンバとして音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなしパケットは音声 VLAN で転送されます。 スイッチが LLDP-MED パケットを受信した場合、VLAN ID、Tagged フラグ、優先度フラグがチェックされます。スイッチは Tagged フラグ、優先度フラグに従います。

「Apply」ボタンをクリックして、設定内容を適用します。

Voice VLAN OUI（音声 VLAN OUI 設定）

ユーザ定義の音声トラフィックの OUI を設定します。
OUIは音声トラフィックを識別するために使用されます。受信パケットのソースMACアドレスがOUIパターンのいずれかと一致した場合、受信パケットは音声パケットとして識別されます。定義済み OUI に加えて、ユーザ定義の OUI を追加することができます。
ユーザ定義 OUI は定義済みの OUI と同じにすることはできません。

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 8-45　Voice VLAN OUI 画面

画面に表示される項目：

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

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

Voice VLAN Device（音声 VLAN デバイス）

ポートに接続する音声デバイスを表示します。

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



図 8-46　Voice VLAN Device 画面

画面に表示される項目：

項目	説明
Unit	表示するユニットを選択します。

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

スイッチに接続する音声 VLAN LLDP-MED デバイスを表示します。

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

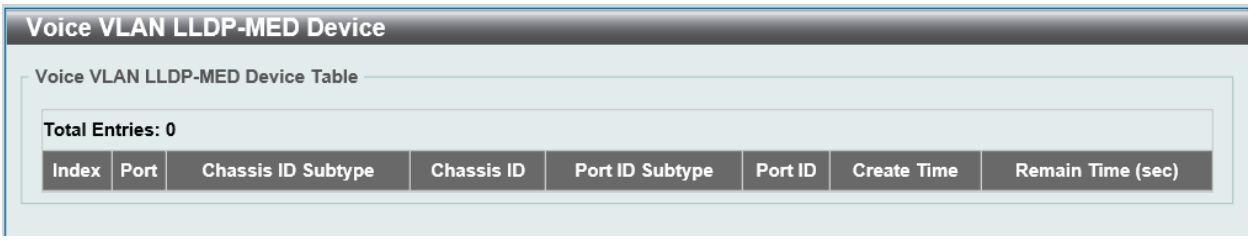


図 8-47　Voice VLAN LLDP-MED Device 画面

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

Private VLAN（プライベート VLAN 設定）

プライベート VLAN の設定を行います。

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

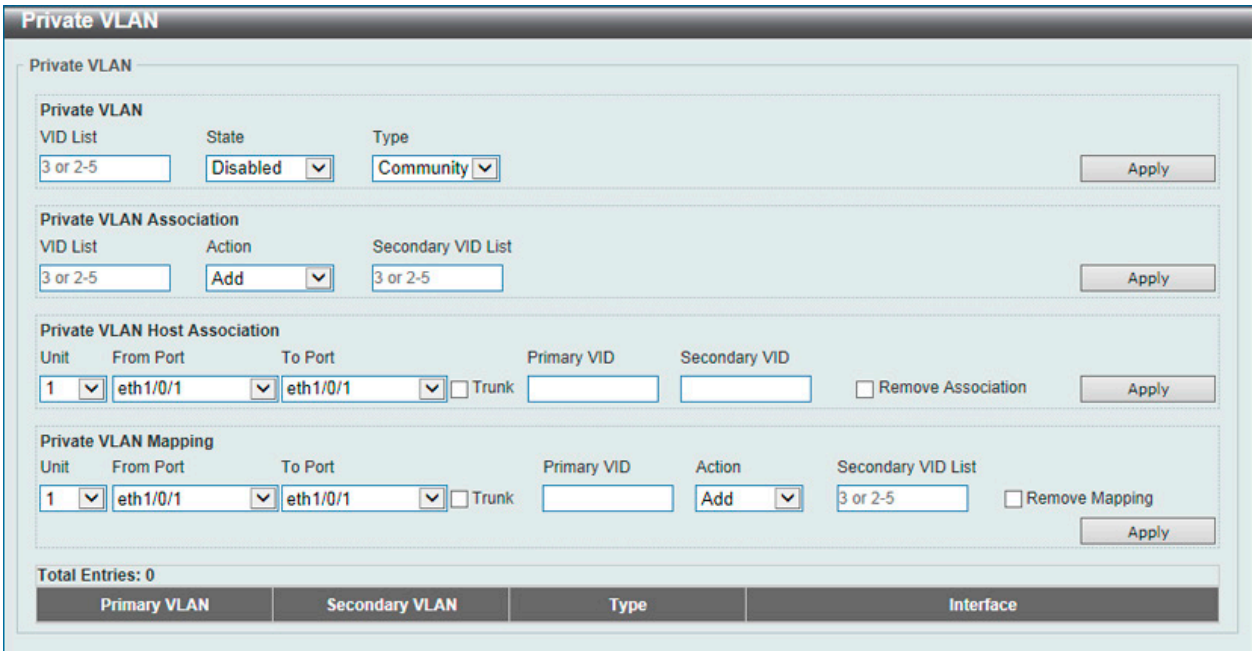


図 8-48　Private VLAN 画面

画面に表示される項目：

項目	説明
Private VLAN	
VID List	プライベート VLAN の VLAN ID を指定します。
State	プライベート VLAN を有効 / 無効に設定します。
Type	プライベート VLAN のタイプを指定します。 • 選択肢：「Community」「Isolated」「Primary」
Private VLAN Association	
VID List	プライベート VLAN の VLAN ID を指定します。
Action	プライベート VLAN に対して実行するアクションを指定します。 • 選択肢：「Add」「Remove」「Disabled」
Secondary VID List	セカンダリ VLAN の VLAN ID を入力します。
Private VLAN Host Association	
Unit	設定を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。「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 の VLAN ID を入力します。
Secondary VID	セカンダリ VLAN の VLAN ID を入力します。「Remove Association」にチェックを入れると本設定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	本設定を適用するポート範囲を指定します。「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 の 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」- 入力した情報に基づきエントリを削除します。
Secondary VID	セカンダリ VLAN の VLAN ID を入力します。「Remove Mapping」にチェックを入れると本設定は有効になりません。

「Apply」ボタンをクリックして、設定内容を適用します。

VLAN Tunnel（VLAN トンネル）

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

Dot1q Tunnel（Dot1q トンネル）

802.1Q VLAN トンネルの設定、表示を行います。

802.1Q トンネルポートはサービス VLAN において「User Network Interface」(UNI) ポートとして動作します。サービス VLAN のタグ付きメンバであるトランクポートは、サービス VLAN の「Network Node Interface」(NNI) ポートとして動作します。
サービス VLAN タグ付きフレームを送受信するプロバイダブリッジネットワークに接続するポートに対し、802.1Q トンネリングイーサネットタイプを設定します。トンネルイーサネットタイプが設定されると、この値はポートの送信フレームの出力 VLAN タグ「Tag Protocol ID」(TPID) に指定されます。また、指定 TPID は当該ポートの受信フレームのサービス VLAN タグの識別にも使用されます。

L2 Features > VLAN Tunnel > Dot1q Tunnel の順にメニューをクリックし、以下の画面を表示します。

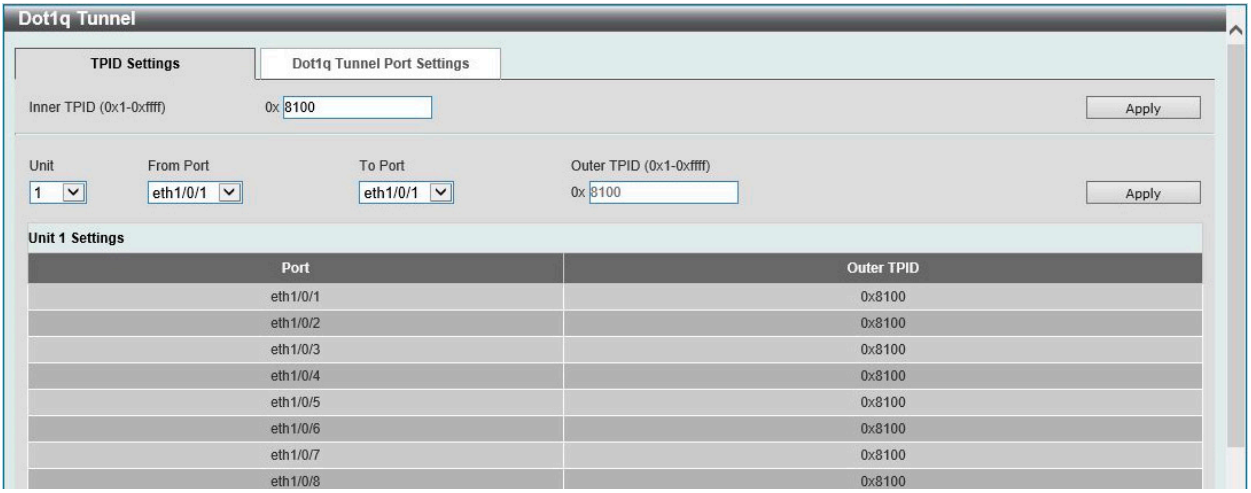


図 8-49　Dot1q Tunnel 画面 - TPID Settings タブ

画面に表示される項目：

項目	説明
Inner TPID	インナー TPID 値を指定します。インナー TPID は、イングレスパケットが「C タグ付き」であるかどうかを判別するために使用されます。このインナー TPID はシステム毎に設定することができます。 • 設定可能範囲：0x1-0xFFFF（16 進数方式）
Unit	設定を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Outer TPID	アウター TPID 値を指定します。 • 設定可能範囲：0x1-0xFFFF（16 進数方式）

「Apply」ボタンをクリックして、設定内容を適用します。

Dot1q Tunnel Port Settings タブをクリックすると以下の画面が表示されます。

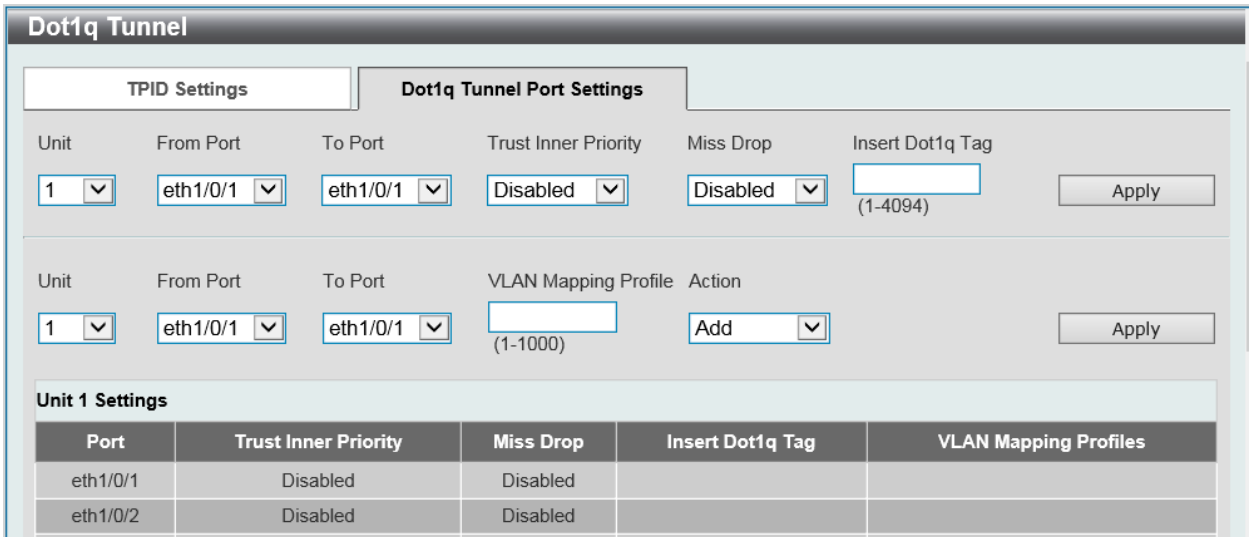


図 8-50　Dot1q Tunnel 画面 - Dot1q Tunnel Port Settings タブ

画面に表示される項目：

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Trust Inner Priority	802.1Q Inner Trust Priority 機能を有効 / 無効に設定します。802.1Q トンネルポートで Trust Priority オプションが有効な場合、受信パケットの VLAN タグの優先値はサービス VLAN タグにコピーされます。
Miss Drop	Miss Drop 機能を有効 / 無効に設定します。受信ポートで VLAN マッピング Miss Drop オプションが有効な場合、受信パケット VLAN が VLAN マッピングエントリやポートのルールと一致しないと、パケットは破棄されます。
Insert Dot1q Tag	802.1Q トンネルポートで受信したタグなしパケットに挿入される 802.1Q VLAN ID を指定します。 • 設定可能範囲：1-4094
VLAN Mapping Profile	VLAN マッピングプロファイル ID を指定します。値の小さい方が優先度が高くなります。 • 設定可能範囲：1-1000
Action	• 「Add」- 入力した情報に基づきエントリを追加します。 • 「Remove」- 入力した情報に基づきエントリを削除します。

「Apply」ボタンをクリックして、設定内容を適用します。

VLAN Mapping（VLAN マッピング）

VLAN マッピングの設定、表示を行います。

インタフェースにプロファイルが適用されると、スイッチはプロファイルルールに従い受信パケットを照合します。パケットがルールに合致したことを確認すると、ルールに設定されたアクションが実行されます。このアクションには、outer VID の追加や置換、新しい outer タグの優先値設定、またはパケットの新しい inner VID の設定などがあります。
照合の順序はプロファイル内にあるルールのシーケンス番号に依存しており、最初のエントリが合致すると照合は停止します。シーケンス番号が設定されていない場合、自動的に付与されます。シーケンス番号は、10 から始まり 10 ずつ増加します。1 つのインタフェースに対し、複数の異なるタイプのプロファイルを設定することができます。

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

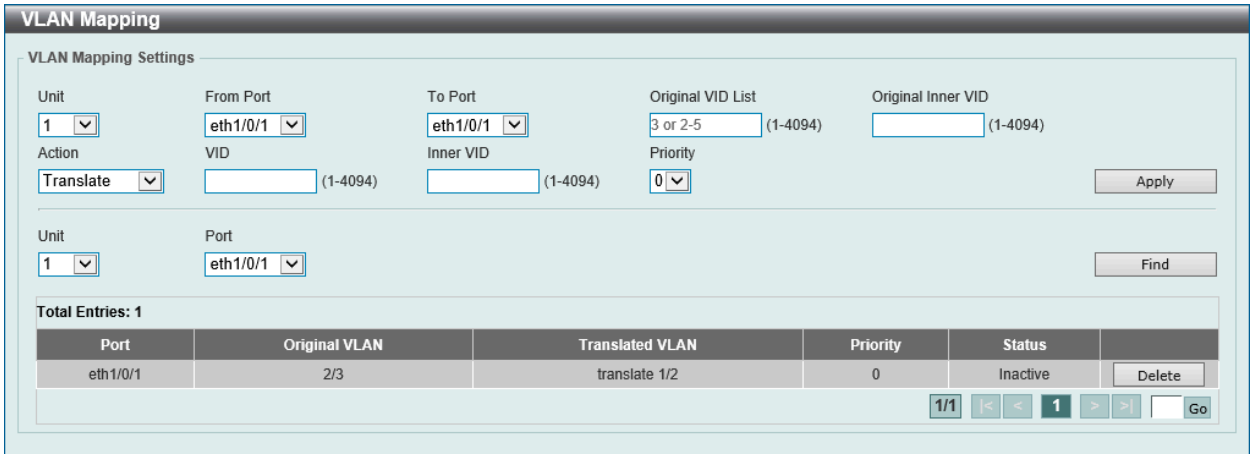


図 8-51　VLAN Mapping 画面

画面に表示される項目：

項目	説明
Unit	設定を行うユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Port	検索するポートを指定します。
Original VID List	オリジナルの VID リストを指定します。 • 設定可能範囲：1-4094
Original Inner VID	オリジナルのインナー VID を指定します。 • 設定可能範囲：1-4094
Action	実行する動作を指定します。 •「Translate」- VID が一致したパケットのアウター VID と交換する VID を指定します。 •「Dot1q-tunnel」- VID が一致したパケットにアウター VID を追加します。
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094
Inner VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
Priority	優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

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

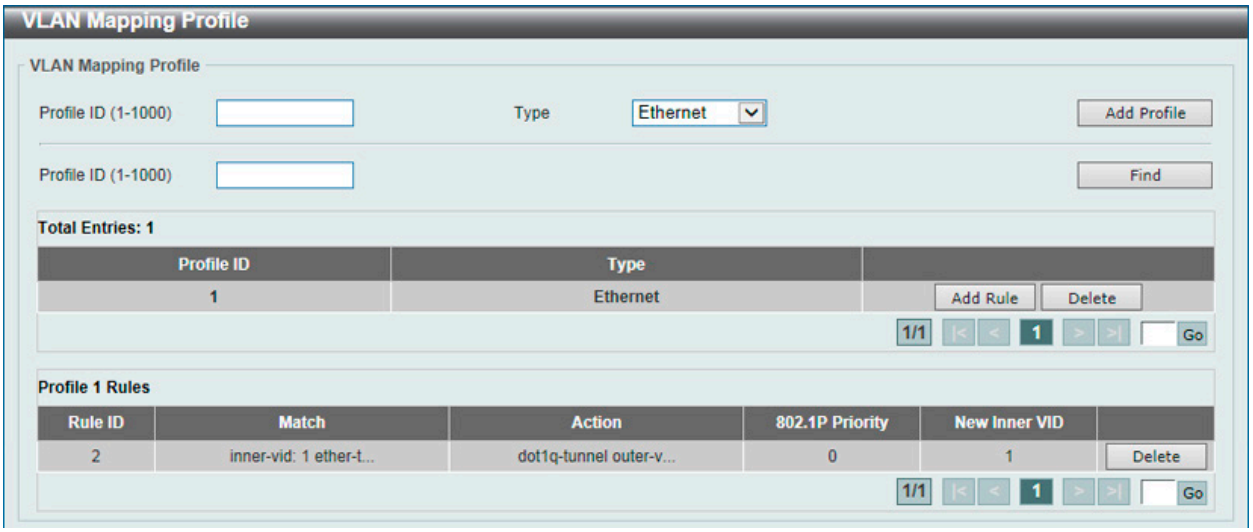


図 8-52　VLAN Mapping Profile 画面

画面に表示される項目：

項目	説明
Profile ID	VLAN マッピングプロファイルの ID を入力します。値の小さい方が優先度が高くなります。 • 設定可能範囲：1-1000
Type	プロファイルタイプを指定します。 • 「Ethernet」- プロファイルは L2 項目を照合します。 • 「IP」- プロファイルは L3 IP 項目を照合します。 • 「IPv6」- プロファイルは IPv6 宛先 / 送信元アドレス項目を照合します。 • 「Ethernet-IP」- プロファイルは L2/L3 IP 項目を照合します。

「Add Profile」ボタンをクリックして、新しい VLAN マッピングプロファイルを追加します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Add Rule」ボタンをクリックして、新しいルールを追加します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

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

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

「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。

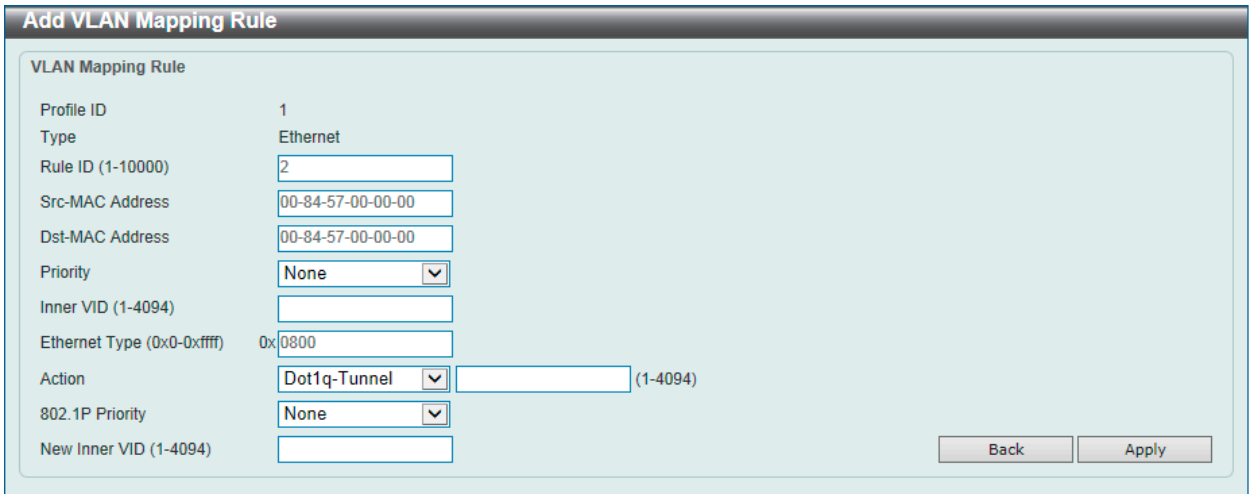


図 8-53　Add VLAN Mapping Rule（Ethernet）画面

画面に表示される項目：

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
Src-MAC Address	送信元 MAC アドレスを指定します。
Dst-MAC Address	宛先 MAC アドレスを指定します。
Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
Inner VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
Ethernet Type	イーサネットタイプを指定します。 • 設定可能範囲：0x0-0xFFFF
Action	実行する動作を指定します。 • 「Translate」- 一致したパケットのアウター VID と交換する VID を指定します。 • 「Dot1q-tunnel」- 一致したパケットにアウター VID を追加します。
802.1P Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID を指定します。 • 設定可能範囲：1-4094

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

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

「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。

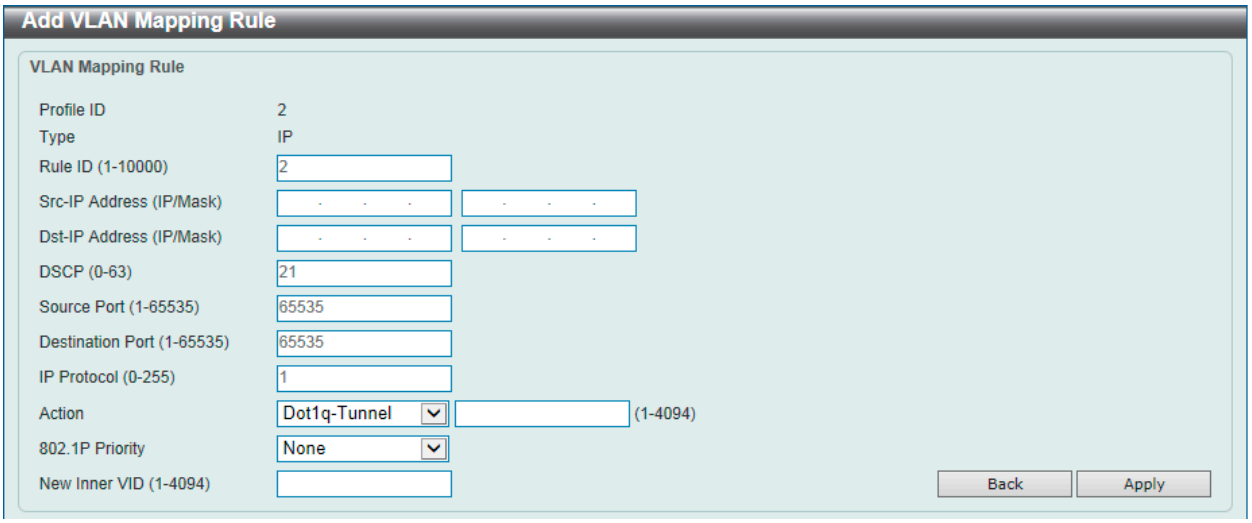


図 8-54　Add VLAN Mapping Rule（IP）画面

画面に表示される項目：

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
Src-IP Address (IP/Mask)	送信元 IP アドレスとサブネットマスクを指定します。
Dst-IP Address (IP/Mask)	宛先 IP アドレスとサブネットマスクを指定します。
DSCP	DSCP 値を指定します。 • 設定可能範囲：0-63
Source / Destination Port	送信元 / 宛先 TCP/UDP ポートを指定します。 • 設定可能範囲：1-65535
IP Protocol	L3 IP プロトコル値を指定します。 • 設定可能範囲：0-255
Action	実行する動作を指定します。 • 「Translate」- 一致したパケットのアウター VID と交換する VID を指定します。 • 「Dot1q-tunnel」- 一致したパケットにアウター VID を追加します。
802.1P Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID を指定します。 • 設定可能範囲：1-4094

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

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

「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。

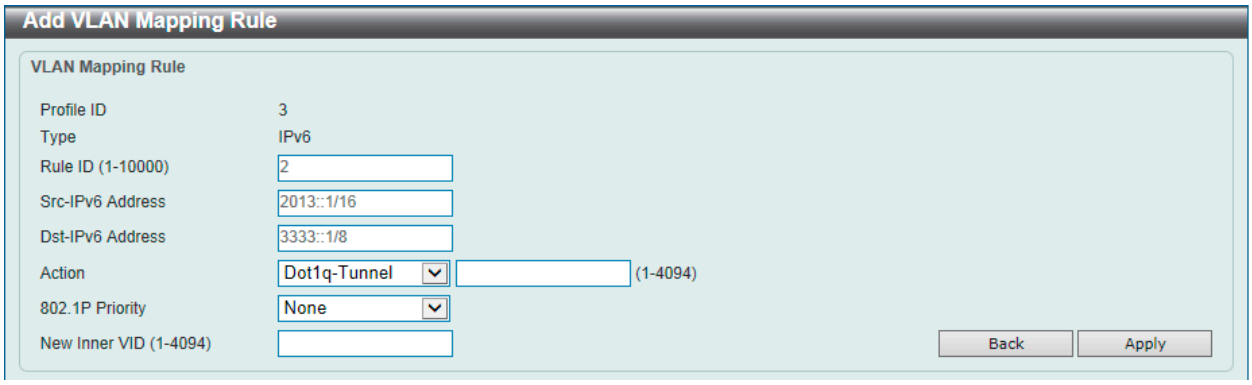


図 8-55　Add VLAN Mapping Rule（IPv6）画面

画面に表示される項目：

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
Src-IPv6 Address	送信元 IPv6 アドレスとプレフィックス長を指定します。
Dst-IPv6 Address	宛先 IPv6 アドレスとプレフィックス長を指定します。
Action	実行する動作を指定します。 • 「Translate」- 一致したパケットのアウター VID と交換する VID を指定します。 • 「Dot1q-tunnel」- 一致したパケットにアウター VID を追加します。
802.1P Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID を指定します。 • 設定可能範囲：1-4094

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

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

「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。

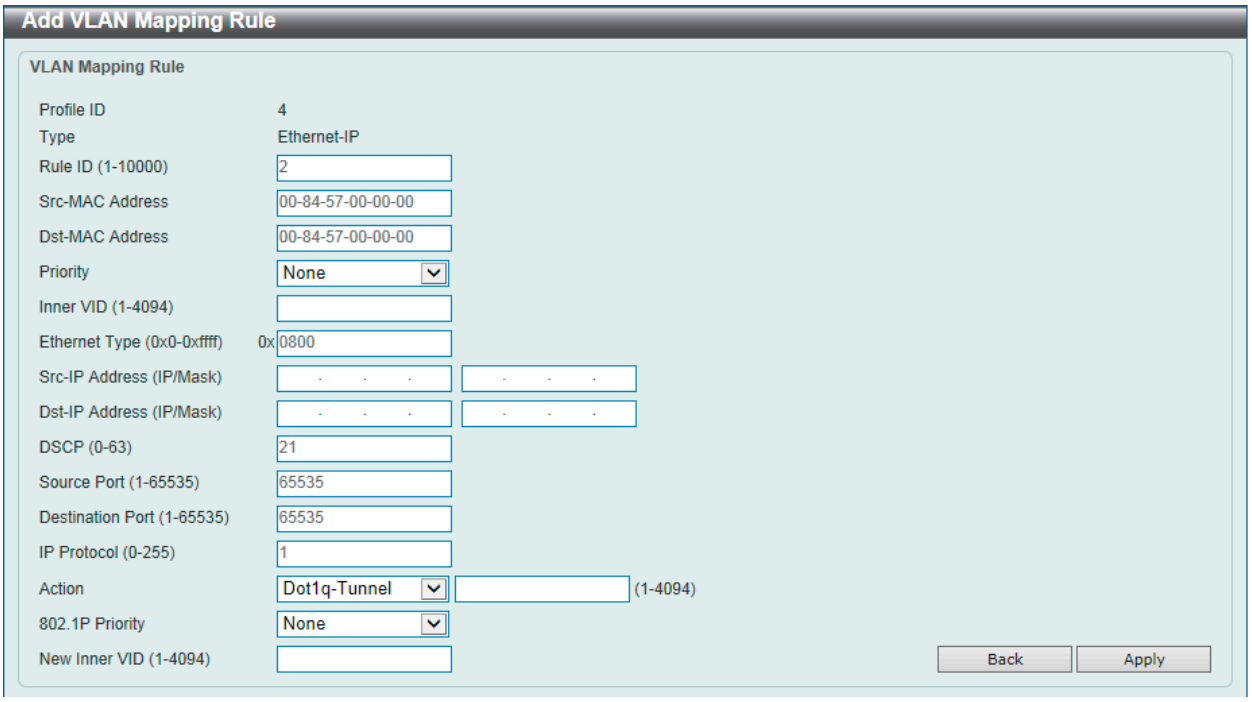


図 8-56　Add VLAN Mapping Rule（Ethernet-IP）画面

画面に表示される項目：

項目	説明
Rule ID	VLAN マッピングルール ID を入力します。指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
Src-MAC Address	送信元 MAC アドレスを指定します。
Dst-MAC Address	宛先 MAC アドレスを指定します。
Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
Inner VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
Ethernet Type	イーサネットタイプを指定します。 • 設定可能範囲：0x0-0xFFFF
Src-IP Address	送信元 IP アドレスとサブネットマスクを指定します。
Dst-IP Address	宛先 IP アドレスとサブネットマスクを指定します。
DSCP	DSCP 値を指定します。 • 設定可能範囲：0-63
Source / Destination Port	送信元 / 宛先 TCP/UDP ポートを指定します。 • 設定可能範囲：1-65535
IP Protocol	L3 IP プロトコル値を指定します。 • 設定可能範囲：0-255
Action	実行する動作を指定します。 • 「Translate」- 一致したパケットのアウター VID と交換する VID を指定します。 • 「Dot1q-tunnel」- 一致したパケットにアウター VID を追加します。
802.1P Priority	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
New Inner VID	「Dot1q-tunnel」を選択後、新しいインナー VLAN ID を指定します。 • 設定可能範囲：1-4094

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

STP（スパニングツリー設定）

L2 Features > STP

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

802.1Q-2005 MSTP

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

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

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

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

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

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

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

802.1D-2004 Rapid STP

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

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

ポートの状態遷移

3 つのプロトコル間の根本的な相違点は、ポートがどのように Forwarding 状態に遷移するかという点と、この状態遷移がトポロジ内でのポートの役割（Forwarding/Not Forwarding）にどのように対応するかという点にあります。802.1D-1998 規格で使用されていた 3 つの状態「Disabled」「Blocking」「Listening」が、MSTP 及び RSTP では「Discarding」という 1 つの状態に統合されました。いずれの場合も、ポートはパケットの送信を行わない状態です。STP の「Disabled」「Blocking」「Listening」であっても、RSTP/MSTP の「Discarding」であっても、ネットワークトポロジ内では「非アクティブ状態」であり、機能の差はありません。以下の表では、3 つのプロトコルにおけるポートの状態遷移の違いを示しています。

トポロジの計算については、3 つのすべてのプロトコルにおいて同様に行われます。各セグメントにはルートブリッジへのパスが 1 つ存在し、すべてのブリッジで BPDU パケットをリッスンします。RSTP/MSTP では、ルートブリッジから BPDU を受信しなくても BPDU パケットが Hello パケット送信毎に送信されます。ブリッジ間の各リンクはリンクの状態を素早く検知することができるため、リンク断絶時の素早い検出とトポロジの調整が可能となります。802.1D-1998 規格では、隣接するブリッジ間においてこのような素早い状態検知が行われません。

ポート状態の比較

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

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

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

Edge Port

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

P2P Port

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

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

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

2 つのレベルで動作するスパニングツリープロトコル

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

STP Global Settings（STP グローバル設定）

STP をグローバルに設定します。

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

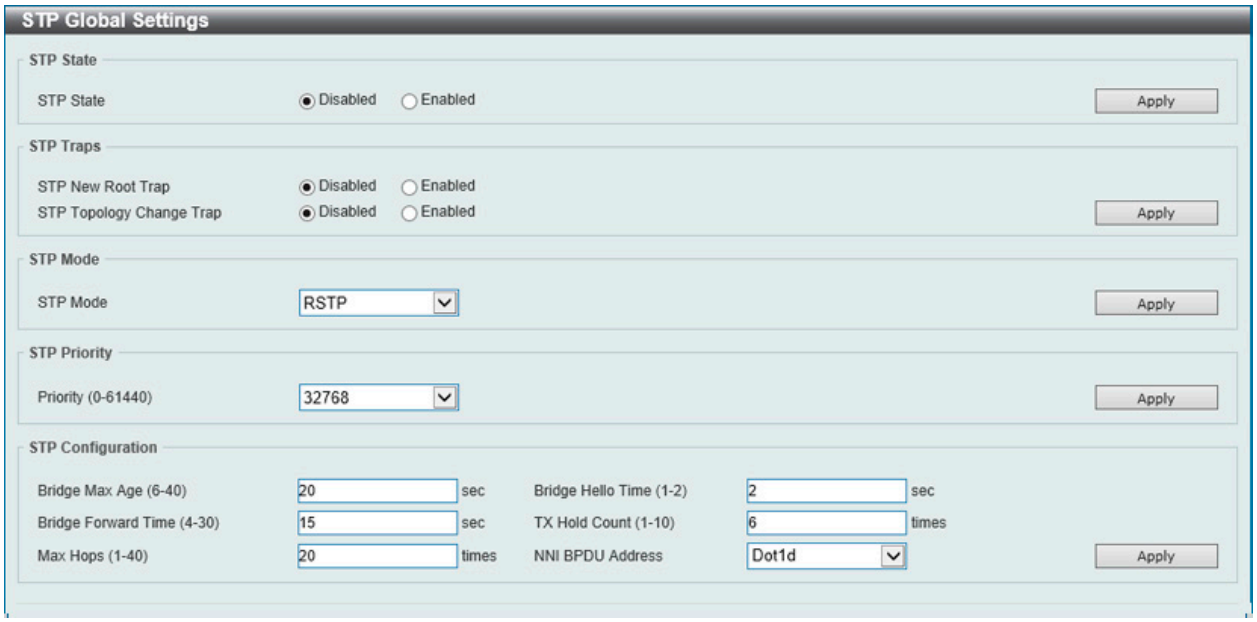


図 8-57　STP Global Settings 画面

画面に表示される項目：

項目	説明
STP State	
STP State	STP のグローバルステータスを有効 / 無効に設定します。
STP Traps	
STP New Root Trap	新しいルートトラップ送信を有効 / 無効に設定します。
STP Topology Change Trap	トポロジ変更トラップ送信を有効 / 無効に設定します。
STP Mode	
STP Mode	スイッチで使用する STP のバージョンを選択します。 • 「STP」- スイッチ上で STP がグローバルに使用されます。 • 「RSTP」- スイッチ上で RSTP がグローバルに使用されます。 • 「MSTP」- スイッチ上で MSTP がグローバルに使用されます。
STP Priority	
Priority	STP 優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0-61440 • 初期値：32768
STP Configuration	
Bridge Max Age	ブリッジの最大エージタイマを設定します。本項目は、古い情報がネットワーク内の冗長パスを無限に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。この値はルートブリッジによりセットされ、ブリッジで相互接続された LAN 内のデバイスと本スイッチの STP 設定値が整合性を持っていることを確認するために使用されます。 • 設定可能範囲：6-40（秒） • 初期値：20（秒）
Bridge Hello Time	Bridge Hello タイムを入力します。ルートブリッジは、他のスイッチに自身がルートブリッジであることを示すために BPDU パケットを送信します。本値は、BPDU パケットの送信間隔です。「STP Mode」で STP または RSTP が選択された場合にのみ本項目が表示されます。MSTP については、Hello Time はポートごとに設定される必要があります。 • 設定可能範囲：1-2（秒） • 初期値：2（秒）
Bridge Forward Time	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間、本値で指定した時間 Listening 状態を保ちます。 • 設定可能範囲：4-30（秒） • 初期値：15（秒）
Tx Hold Count	Hello パケットの最大送信回数を指定します。 • 設定可能範囲：1-10 • 初期値：6

項目	説明
Max Hops	スパニングツリー範囲のデバイス間で、スイッチが送信した BPDU パケットが破棄されるまでのホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。0 に到達すると、BPDU パケットが破棄され、ポートに保持していた情報は解放されます。 • 設定可能範囲：1-40 • 初期値：20
NNI BPDU Address	NNI BPDU アドレスを指定します。このパラメータはサービスプロバイダネットワークの STP の BPDU プロトコルアドレスを決定するために使用されます。「802.1d STP アドレス」と「802.1ad サービスプロバイダ STP アドレス」が使用されます。 • 選択肢：「Dot1d」「Dot1ad」

「Apply」ボタンをクリックして、設定内容を適用します。

STP Port Settings（STP ポートの設定）

STP をポートごとに設定します。

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

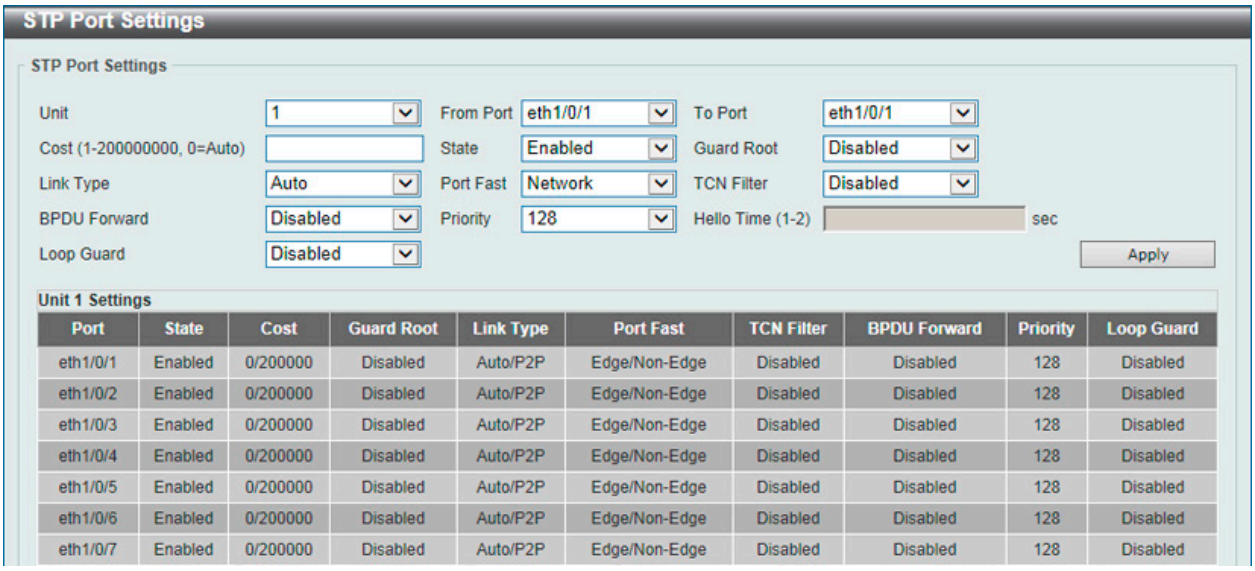


図 8-58　STP Port Settings 画面

補足　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。

画面に表示される項目：

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Cost	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。ポートのコストは自動か、メトリックの値で設定します。 • 0（Auto）- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。（初期値） ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。 • 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が小さいほどパケット転送は頻繁に行われるようになります。
State	指定ポートでの STP を有効 / 無効に設定します。
Guard Root	Guard Root を有効 / 無効に設定します。
Link Type	リンクの種類を設定します。全二重ポートは P2P ポートとして判別され、半二重ポートは Shared ポートとして判別されます。Shared 設定の場合、ポートは即時に Forwarding 状態にはなりません。 • 選択肢：「Auto」「P2P」「Shared」 • 初期値：「Auto」

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」- ポートは 3 秒だけ非ポートファスト状態に残ります。BPDU が受信されない場合、ポートファスト状態に移行し、その後転送状態に移行します。その後、BPDU を受信すると非ポートファスト状態へ戻ります。（初期値） • 「Disabled」- ポートは常に非ポートファスト状態です。常に「forward-time delay」の時間待機し、転送状態へ移行します。 • 「Edge」- ポートは「forward-time delay」の時間を待たずに直接 STP 転送状態に移行します。インタフェースが「BPDU」を受信すると非ポートファストへ移行します。
TCN Filter	TCN（Topology Change Notification）フィルタを有効 / 無効に設定します。本オプションが有効な場合、ポートで受信した TC イベントは無視されます。 • 初期値：「Disabled」（無効）
BPDU Forward	BPDU パケットの転送を有効 / 無効に設定します。有効にすると受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。 • 初期値：「Disabled」（無効）
Priority	優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0-240 • 初期値：128
Hello Time	ハロータイムの値を指定します。この設定は指定ポートによる各設定メッセージの定期的な送信の間隔となります。 • 設定可能範囲：1- 2（秒）
Loop Guard	指定ポートでのループガードを有効 / 無効に設定します。 本機能は、L2 フォワーディングループ（STP ループ）に対する追加の防御機能です。STP ループは、冗長トポロジ内の STP ブロッキングポートが、誤ってフォワーディングステートへ移行する際に発生します。これは通常、物理冗長トポロジ内のポートの一つ（必ずしも STP ブロッキングポートではない）が、STP BPDU を受信しなくなることにより発生します。このような状況において、BPDU の送受信はポートに割り当てられた役割に依存することになります。つまり、指定ポート（Designated Port）は BPDU を送信し、非指定ポート（Non Designated Port）は BPDU を受信します。 物理冗長ポロジのポートの一つが BPDU を受信しなくなると、STP はトポロジをループ解除状態と認識します。これにより、ブロッキング / バックアップポートであった代替ポートが、指定ポート（Designated Port）となりフォワーディングステートに移行します。この結果ループが発生します。

「Apply」ボタンをクリックして、設定内容を適用します。

MST Configuration Identification（MST の設定）

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

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

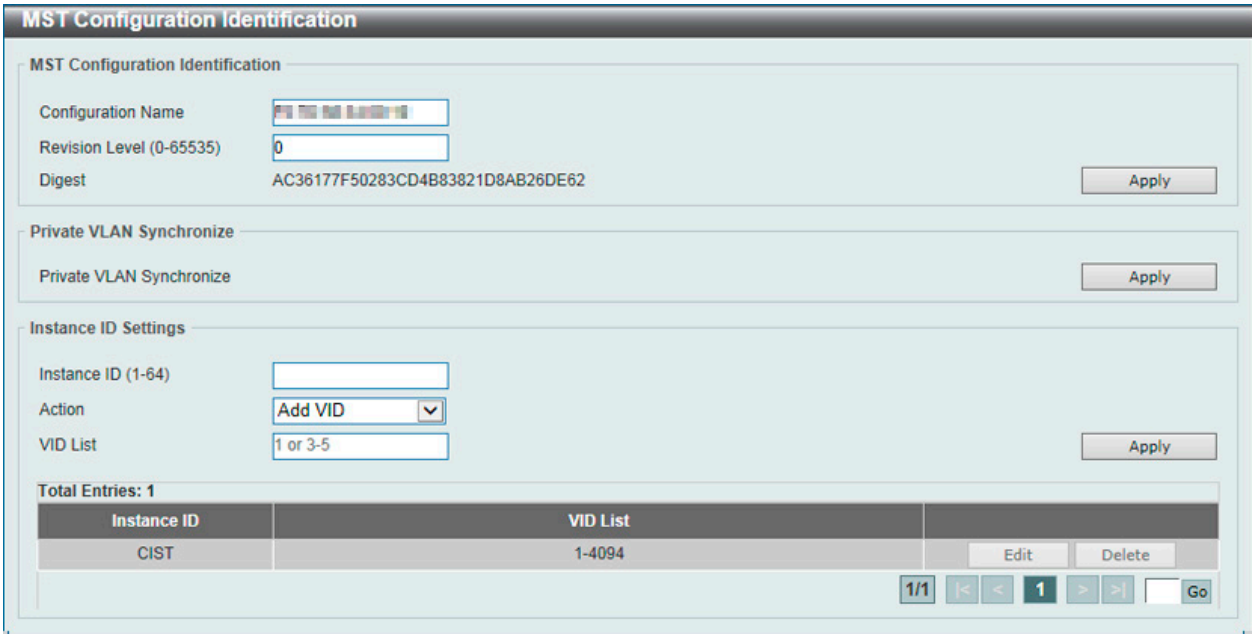


図 8-59　MST Configuration Identification 画面

画面に表示される項目：

項目	説明
MST Configuration Identification	
Configuration Name	MSTI（Multiple Spanning Tree Instance）を識別するための名前を設定します。 名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level	MST リージョンの値を設定します。Configuration Name とともに、スイッチ上の MSTP リージョンを識別するために使用します。 • 設定可能範囲：0-65535 • 初期値：0
Private VLAN Synchronize	
Private VLAN Synchronize	「Apply」ボタンをクリックすると、プライベート VLAN の同期を行います。
Instance ID Settings	
Instance ID	スイッチに Instance ID を設定します。 • 設定可能範囲：1-64
Action	MSTI に行う変更を選択します。 •「Add VID」- VID List 項目に指定された VID を MSTI ID に追加します。 •「Remove VID」- VID List 項目に指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

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

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

STP Instance（STP インタンス設定）

STP インスタンスの設定を行います。

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



図 8-60　STP Instance 画面

画面に表示される項目：

項目	説明
Instance Priority	「Edit」をクリック後、指定したインスタンスのプライオリティを設定します。 • 設定可能範囲：0-61440

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

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

MSTP Port Information（MSTP ポート情報）

現在の MSTP ポート情報の表示や、MSTI ID 単位でポート構成の更新を行います。

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。

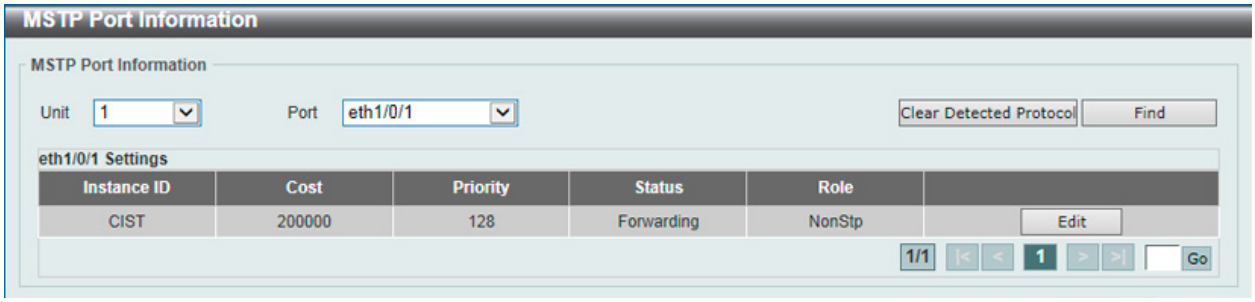


図 8-61　MSTP Port Information 画面

画面に表示される項目：

項目	説明
Unit	エントリを表示 / 削除するユニットを指定します。
Port	エントリを表示 / 削除するポートを選択します。
Cost	パケットを転送するコストを設定します。 • 設定可能範囲：1-200000000
Priority	優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0-240 • 初期値：128

「Clear Detected Protocol」ボタンをクリックして、選択したポートの検出したプロトコル設定をクリアします。
「Find」ボタンをクリックして、特定ポートの MSTP 設定を参照します。
「Edit」ボタンを選択して、特定のエントリを再設定します。

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。

ERPS (G.8032)（イーサネットリングプロテクション設定）

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

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

ERPS

本項目では「Ethernet Ring Protection Switching」（ERPS）の表示、設定を行います。ERPS を有効化する前に、STP とループバック検知 (LBD) をリングポートで無効にする必要があります。ERPS は「R-APS VLAN」リングポート、RPL ポート、RPL オーナが設定されていない状態では、有効にできません。

注意　ERPS バージョンを変更するとプロトコルが再起動します。

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。

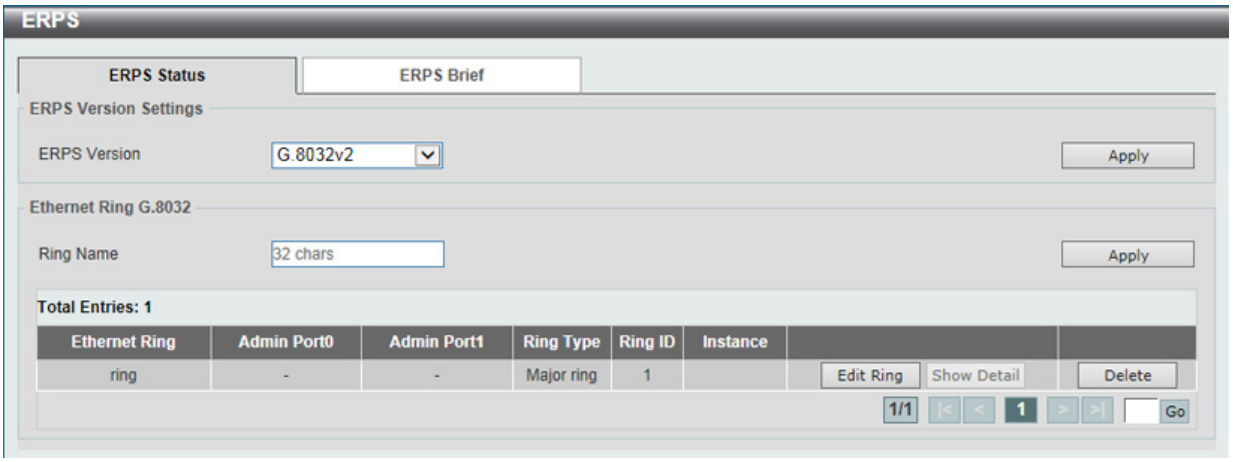


図 8-62　ERPS 画面 - ERPS Status タブ

画面に表示される項目：

項目	説明
ERPS Version Settings	
ERPS Version	ERPS バージョンを選択します。 • 選択肢：「G.8032v1」「G.8032v2」 「G.8032v2」では以下の機能をサポートしています。 - 物理リング内のマルチインスタンス - 「manual」「force」「clear」などの操作コマンド - 物理リングの RING-ID を持つ R-APS PDU 宛先アドレスの送信 「G.8032v2」を実行している機器に対し「G.8032v1」を設定する前に、「G.8032v1」がサポートしない全ての ERPS 設定を削除する必要があります。そうでない場合バージョンの変更は行えません。ERPS バージョンを変更すると、実行中のプロトコルは再起動します。 「G.8032v2」から「G.8032v1」へ変更する前に、次の設定であることをチェックする必要があります。 • 手動（Manual）または強制（force）スイッチコマンドの消去 • 相互接続のメジャーリングインスタンスとサブリングインスタンス機器が、それぞれ異なる「R-APS VLAN ID」を保持していること • 物理リング内で一つのインスタンスのみをサポート イーサネットリングで「ITU-T G.8032v1」と「ITU-T G.8032v2」のイーサネットリングノードが同時に存在している場合、「G.8032v2」機器に対して次の設定を行う必要があります。 • 全ての物理リング ID は初期値の 1 であること • 相互接続ノードのメジャーリングインスタンスとサブリングインスタンス機器が、それぞれ異なる「R-APS VLAN ID」を保持していること • Manual Switch または Force Switch コマンドが削除されていること • 物理リング内で一つのインスタンスのみをサポート

項目	説明
Ethernet Ring G.8032	
Ring Name	ERP インスタンス名を入力します。（32 文字以内）

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

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

■ Ring の編集

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

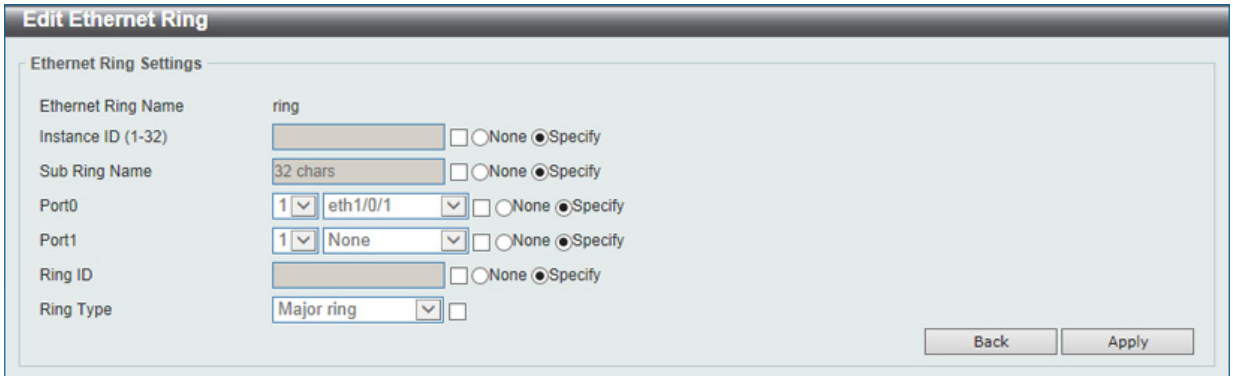


図 8-63　ERPS（Edit）- Edit Ethernet Ring 画面

画面に表示される項目：

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

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

ERP リング詳細情報の表示

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

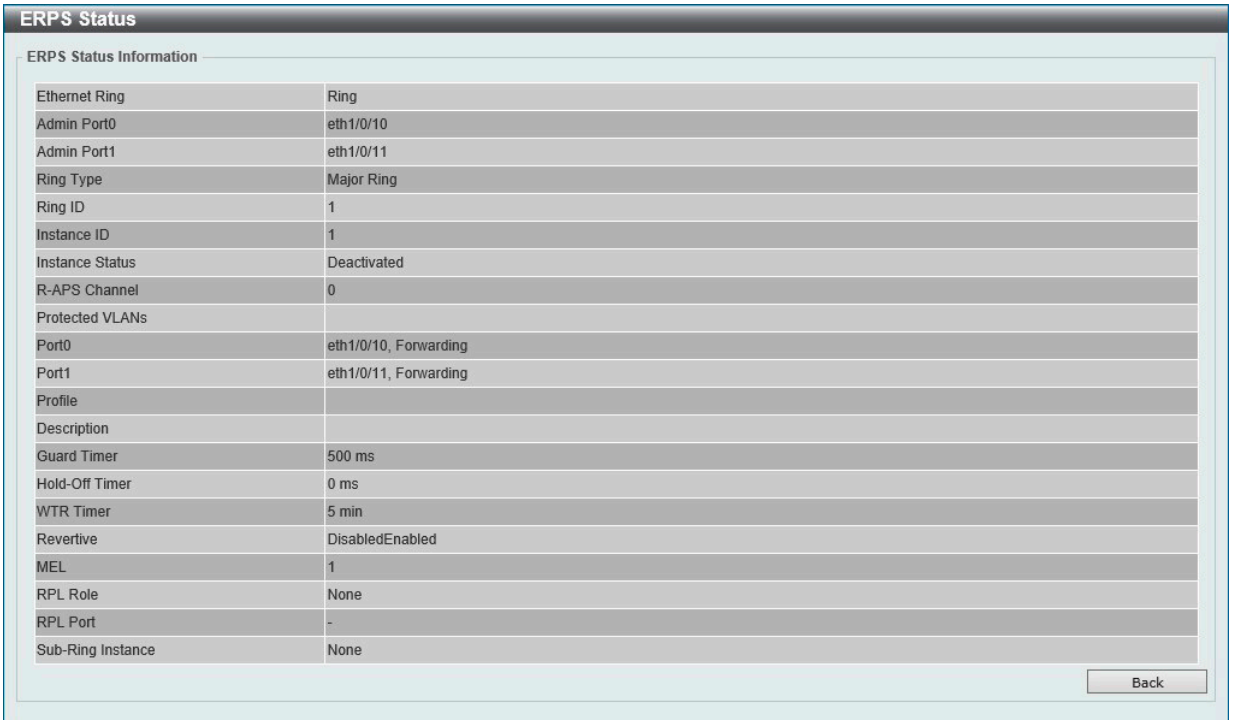


図 8-64　ERPS Status 画面

前の画面に戻るには、「Back」ボタンをクリックします。

「ERPS Brief」タブの表示

「ERPS Brief」タブをクリックすると、以下の画面が表示されます。

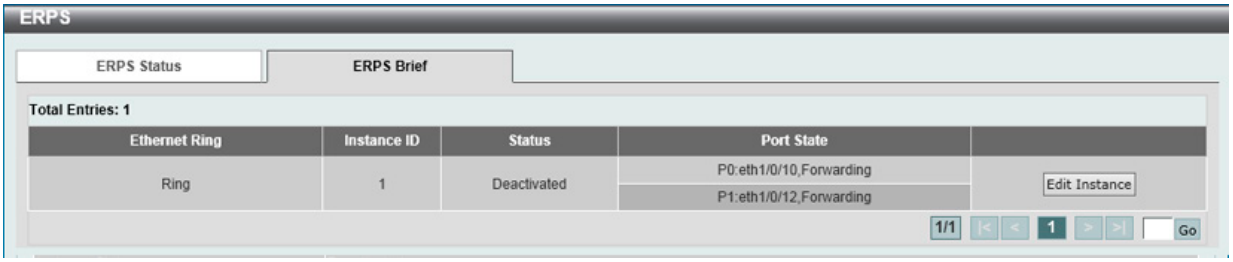


図 8-65　ERPS 画面 - ERPS Brief タブ

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

■ Instance の編集（Edit Instance）

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

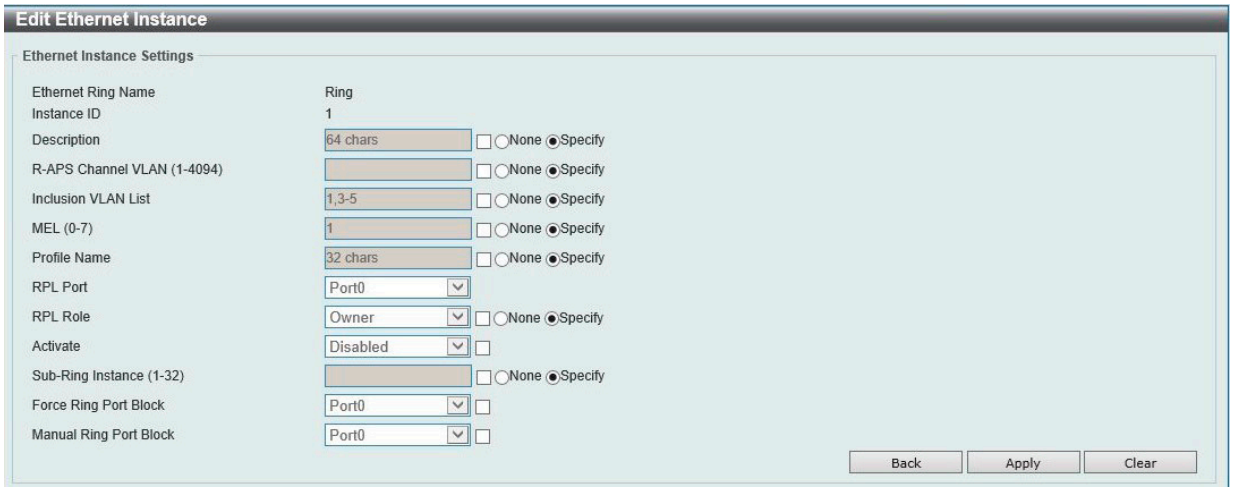


図 8-66　ERPS（Instance）- Edit Ethernet Instance 画面

画面に表示される項目：

項目	説明
Description	チェックを入れ「ERP インスタンス」の概要を指定します。（64 文字以内） 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
R-APS Channel VLAN	チェックを入れ「ERP インスタンス」の「R-APS Channel VLAN ID」を指定します。サブインスタンスの「APS channel VLAN」はサブリングの仮想チャネルでもあります。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-4094
Inclusion VLAN List	チェックを入れインスタンスに含まれる VLAN リストを指定します。VLAN 範囲や個別の指定が可能です（例：「VLAN1 から 5」は「1-5」、「VLAN1 と 3 と 5」は「1,3,5」）。指定された VLAN は ERP のメカニズムで保護されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
MEL	チェックを入れ ERP インスタンスの「MEL」を指定します。 同じ ERP インスタンスに所属する全てのリングノードの MEL 値は同じ値である必要があります。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：0-7
Profile Name	チェックを入れ ERP インスタンスに関連する「G.8032」のプロファイルを指定します（32 文字以内）。同じ G.8032 プロファイルに複数の ERP インスタンスを含めることも可能です。同じプロファイルに含まれる各インスタンスは、同じ VLAN セットを保護します。つまり、この場合 VLAN セットは複数の異なるインスタンスに保護されることになります。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
RPL Port	チェックを入れ RPL ポートオプションを選択します。選択されたオプションは RPL ポートとして設定されます。 • 選択肢：「Port0」「Port1」
RPL Role	チェックを入れノードの種類を選択します。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 選択肢：「Owner」「Neighbor」
Activate	チェックを入れ ERP インスタンスをアクティブにするか選択します。「Enabled」の場合、ERP インスタンスはアクティブになります。 • 選択肢：「Enabled」「Disabled」
Sub-Ring Instance	チェックを入れ ERP インスタンスの識別子を指定します。物理リングインスタンスのサブリングインスタンスを指定する場合に使用されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-32
Force Ring Port Block	チェックを入れブロックされる ERP インスタンスポートを選択します。リンク不具合などの発生有無にかかわらず、本設定が有効になると即時にインスタンスポートがブロックされます。 • 選択肢：「Port0」「Port1」
Manual Ring Port Block	チェックを入れブロックされる ERP インスタンスポートを選択します。リンク不具合や FS（強制切替）がない場合、MS が設定されたポートがブロックされます。 • 選択肢：「Port0」「Port1」

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、このエントリに関連付けられた強制 / 手動の設定をクリアします。
前の画面に戻るには、「Back」ボタンをクリックします。

ERPS Profile（ERPS プロファイル）

ERPS プロファイル設定を行います。

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

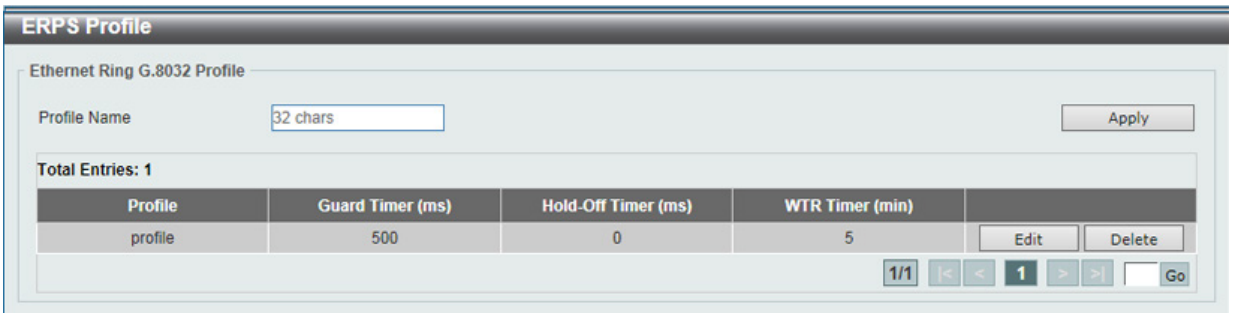


図 8-67　ERPS Profile 画面

画面に表示される項目：

項目	説明
Profile Name	「G.8032」のプロファイル名を指定します（32 文字以内）。複数の ERP インスタンスを同じ「G.8032」プロファイルに関連づけることができます。同じプロファイルに含まれる各インスタンスは、同じ VLAN セットを保護します。つまり、この場合 VLAN セットは複数の異なるインスタンスに保護されることになります。

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

■「G.8032」プロファイルの編集

「Edit 」ボタンをクリックすると、以下の設定画面が表示されます。

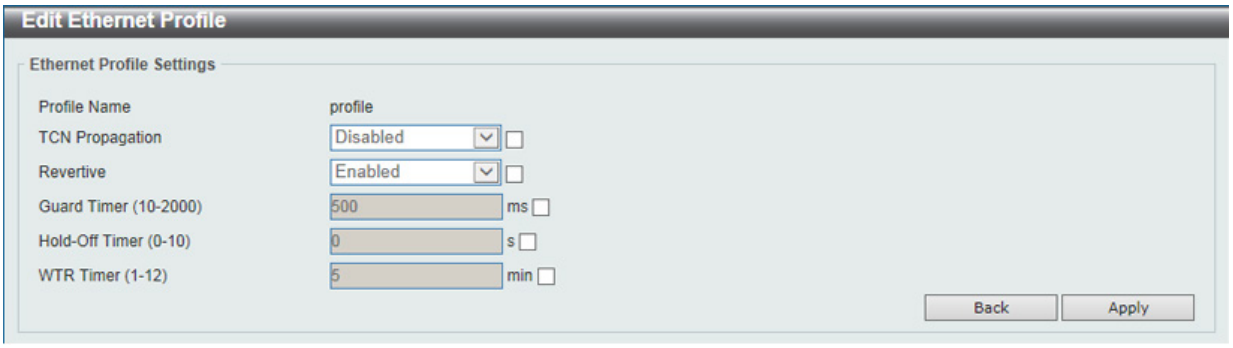


図 8-68　ERPS Profile（Edit）- Edit Ethernet Profile 画面

画面に表示される項目：

項目	説明
TCN Propagation	チェックを入れ「TCN Propagation」の設定を行います。本機能はサブ ERP インスタンスからメジャーインスタンスへのトポロジ変更の通知の伝播を有効にします。 • 選択肢：「Enabled」「Disabled」
Revertive	チェックを入れ「Revertive」の設定を行います。RPL がブロックされた場合などに、稼働中の送信エンティティに戻すために使用されます。
Guard Timer	チェックを入れ Guard Timer の設定を行います。 • 設定可能範囲：10-2000（ミリ秒） • 初期値：500（ミリ秒）
Hold-Off Timer	チェックを入れ Hold-Off Timer の設定を行います。 • 設定可能範囲：0-10（秒） • 初期値：0（秒）
WTR Timer	チェックを入れ Wait To Restore（WTR）Timer の設定を行います。 • 設定可能範囲：1-12（分） • 初期値：5（分）

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

Loopback Detection（ループバック検知設定）

ループバック検知（LBD）機能は、特定のポートに生成されるループを検出するために使用されます。本機能は、CTP(Configuration Testing Protocol) パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN で受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートは再起動 (Normal 状態へ遷移) を行います。

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

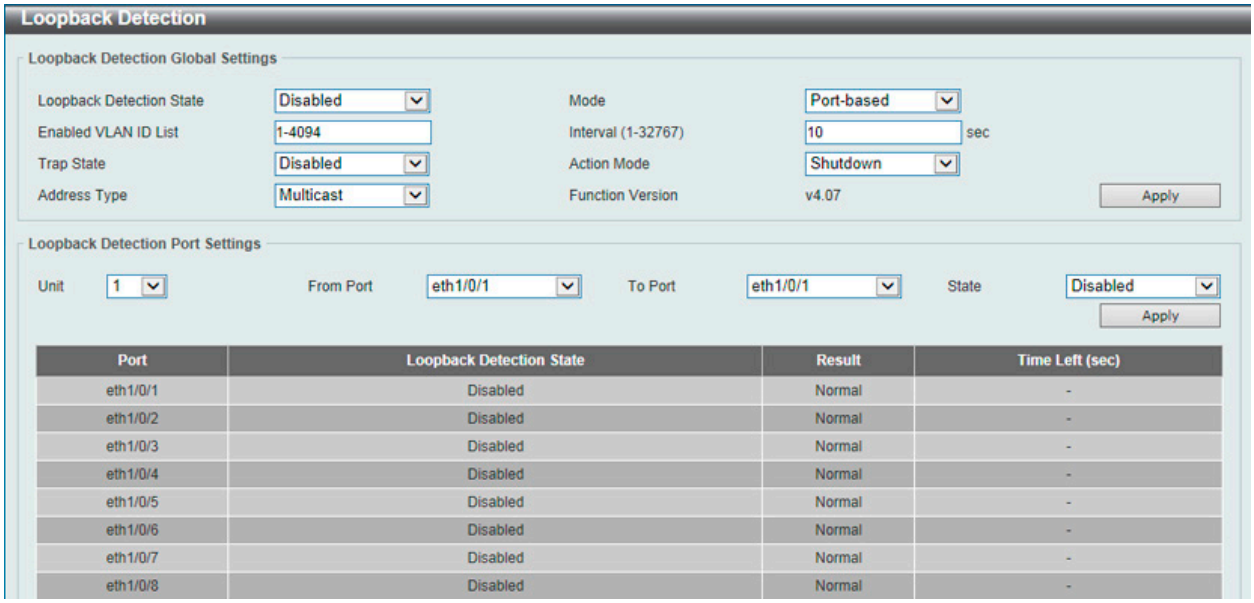


図 8-69　Loopback Detection 画面

画面に表示される項目：

項目	説明
Loopback Detection Global Settings	
Loopback Detection State	ループバック検知機能を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
Mode	ループ検知のモードを選択します。 • 選択肢：「Port-based」「VLAN-based」
Enabled VLAN ID List	「Mode」で「VLAN ID」を選択した場合、VLAN ID のリストを入力します。
Interval	ループ検知間隔を設定します。本設定の間隔で Configuration Test Protocol（CTP）パケットが送信され、ループバックイベントを検知します。 • 設定可能範囲：1-32767（秒） • 初期値：10（秒）
Traps State	ループバック検出トラップを有効 / 無効に設定します。
Action Mode	動作モードを指定します。 • 「Shutdown」- ループ検出時にポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックします。 • 「None」- ループ検出時でもポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックしません。
Address Type	アドレスタイプを選択します。 • 選択肢：「Multicast」「Broadcast」
Loopback Detection Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	ポートのループバック検知ステータスを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　LBD を VLAN-based モードでご利用の場合、同時に検出可能な VLAN 数は検出順に 100 までに制限されます。

注意　VLAN モードで使用した場合、CTP パケットは 100VLANs/Port/Interval ずつ送信されます。CTP は 100VLANs を検出後、該当の VLAN のみに送出されます。

注意　ポートチャネルに対してループバック検知を有効化すると、CTP はリンクアップしている最若番インタフェースから送出されます。

Link Aggregation（リンクアグリゲーション）

ポートトランクグループについて

ポートトランクグループは、複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。トランクグループは最大 32 個まで作成可能であり、各グループには 12 個までの物理ポートを割り当てることができます。

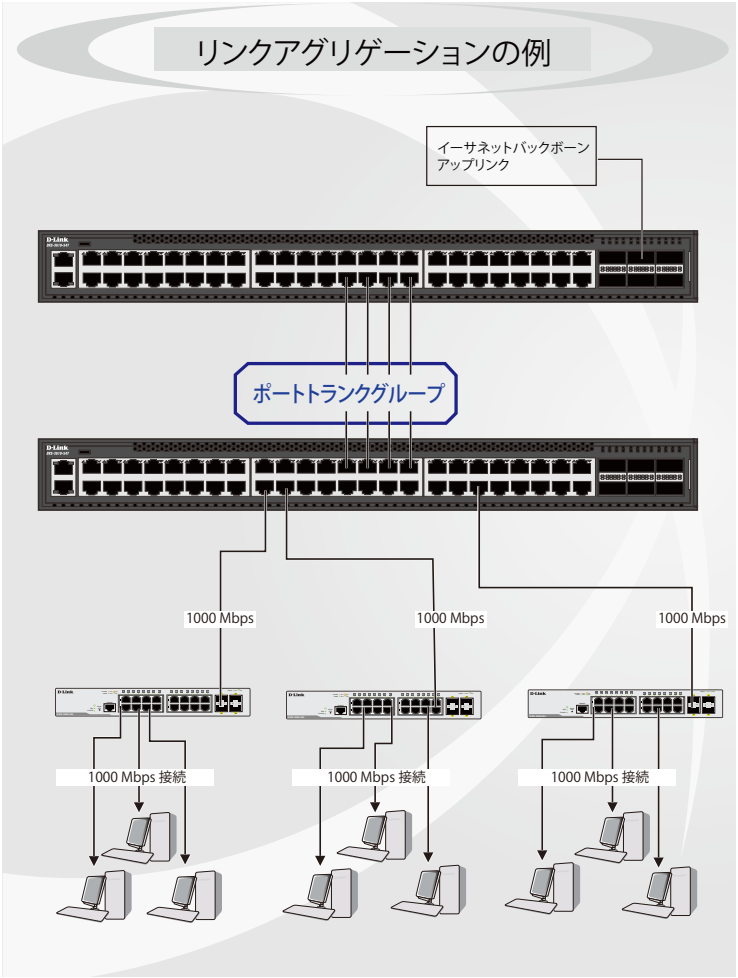


図 8-70　ポートトランクグループの例

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、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。グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断が発生した場合、ネットワークトラフィックはグループ内の他のリンクに振り分けられます。

スパニングツリープロトコル（STP）は、リンクアグリゲーショングループを 1 つのリンクとして扱います。スイッチに冗長化された 2 つのリンクアグリゲーショングループが設定されている場合、STP において片方のグループ全体がブロックされます。（冗長リンクを持つ 1 つのポートがブロックされるケースと同様）。

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

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

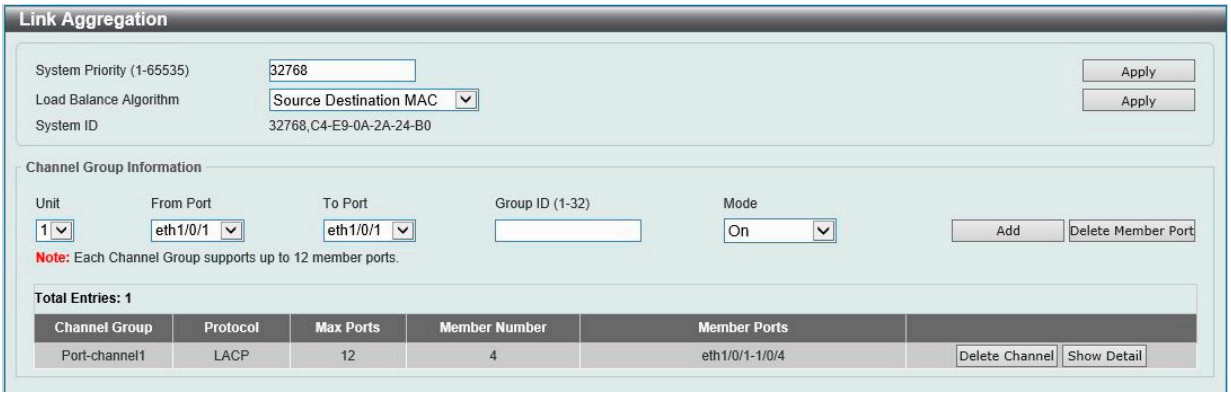


図 8-71　Link Aggregation 画面

画面に表示される項目：

項目	説明
System Priority	システムプライオリティを指定します。 本値により、接続するスイッチ間で「Actor」となるシステムが決定され、そのシステムのポートプライオリティが使用されます。値の小さい方が高い優先度を示します。システムプライオリティが同じ値の場合、MAC ID の小さいシステムが選出されます。その後、「Actor」スイッチのポートプライオリティの値により、ポートチャネルに属するかスタンドアロンモードになるかが決定します。ポートプライオリティが同じ値の場合、ポート番号で優先値が決まります。 • 設定可能範囲：1-65535 • 初期値：32768
Load Balance Algorithm	ロードバランスに使用するアルゴリズムを選択します。 • 選択肢：「Source MAC」「Destination MAC」「Source Destination MAC」「Source IP」「Destination IP」「Source Destination IP」「Source L4 Port」「Destination L4 Port」「Source Destination L4 Port」 • 初期値：「Source Destination MAC」

「Apply」ボタンをクリックして、設定内容を適用します。

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。

Channel Group Information

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
Group ID	グループの ID 番号を設定します。ポートが初めてチャネルグループに参加すると、自動的にポートチャネルが作成されます。各インタフェースは複数のチャネルグループに参加することはできません。 • 設定可能範囲：1-32
Mode	動作モードを指定します。チャネルグループは、固定もしくは LACP メンバのどちらかのみで構成されます。チャネルグループが決定すると、他のタイプのインタフェースはそのチャネルグループに参加できません。 • 「On」- チャネルグループタイプは固定です。 • 「Active」- チャネルグループは LACP になります。LACP パケットを送信してネゴシエーションを開始します。 • 「Passive」- チャネルグループは LACP になります。LACP パケットへの応答のみ行います。

各項目を入力後、「Add」ボタンをクリックし、ポートトランキンググループを作成します。
「Delete Channel」ボタンをクリックして、チャネルを削除します。
「Delete Member Port」ボタンをクリックして、特定グループのメンバポートを削除します。

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

■ **ポートトランキンググループの編集**

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。

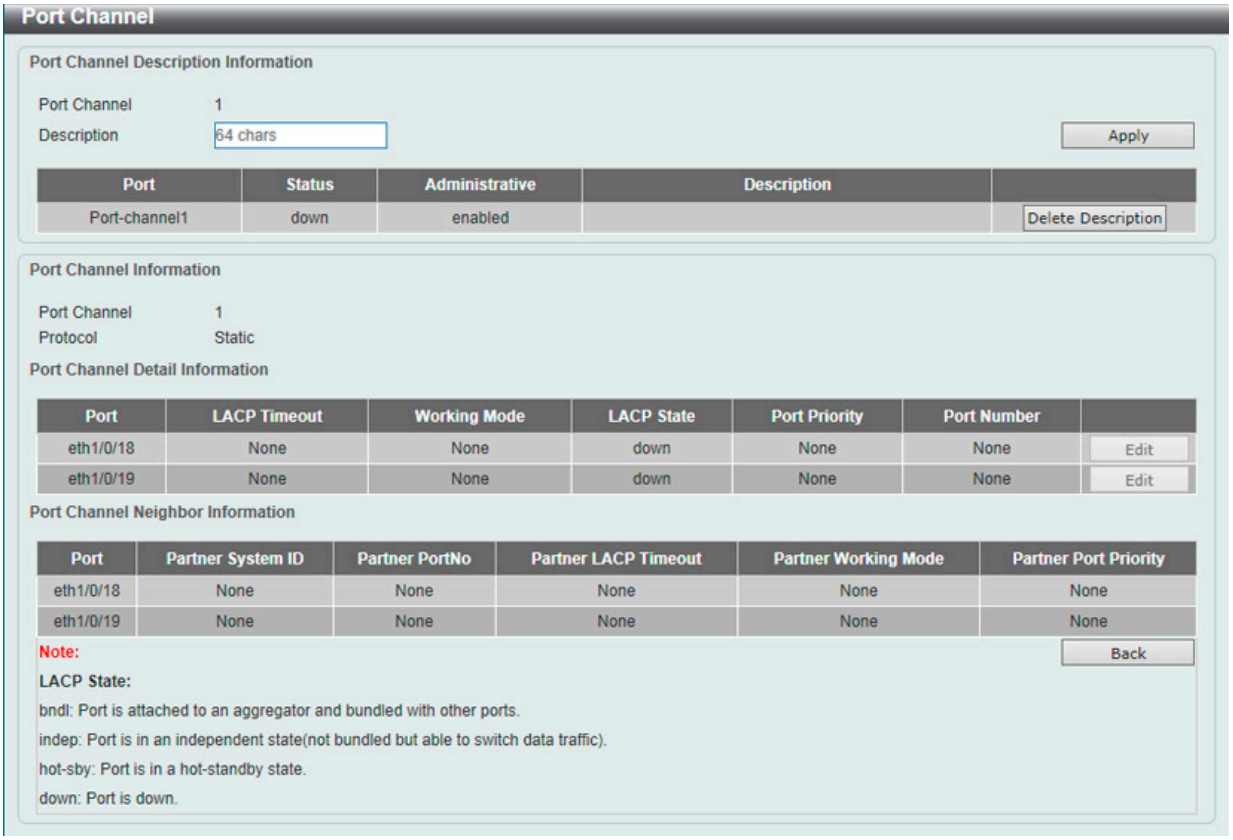


図 8-72　Port Channel 画面

以下の項目が表示されます。

Port Channel Description Information

項目	説明
Description	ポートチャネルの説明を入力します。（64 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete Description」ボタンをクリックして、ポートチャネルの概要を削除します。

Port Channel Information

項目	説明
Port Channel Detail Information	
LACP Timeout	LACP タイムアウトを設定します。 • 選択肢：「Short」「Long」
Working Mode	動作モードを指定します。 • 「Active」- LACP パケットを送信してネゴシエーションを開始します。 • 「Passive」- LACP パケットへの応答のみ行います。
Port Priority	ポートプライオリティを設定します。

「Edit」ボタンをクリックしてパラメータを設定後、「Apply」ボタンをクリックして設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

注意　同一チャネルグループ内でリンク速度が異なるインタフェースは bndl になりません。

MLAG（マルチシャーシリンクアグリゲーション）

マルチシャーシリンクアグリゲーション（MLAG）を使用すると、ネットワーク内のスイッチの帯域幅を増やしたり、ポートのブロックや不必要な再コンバージェンス遅延を防止したり、スイッチやケーブル接続に障害が発生した場合に信頼性の高いフェイルオーバソリューションを提供したりできます。

「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、これらのピアスイッチをネットワーク内で単一の「MLAG スイッチ」として認識します。2 つの MLAG ピアスイッチは、MLAG 機能を除き、2 つの独立したスタンドアロンスイッチとして動作します。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。また、MLAG ピア接続を構築するスイッチでは、システムが不安定になることを避けるために次の設定を同じにする必要があります。

- 「Link Aggregation」「MLAG Port channel」「Interface」「VLAN settings」

MLAG ピアスイッチは、物理スタック機能が無効になっているスタンドアロンスイッチである必要があります。

注意　VRRP を含む L3 機能との併用はできません。

注意　MLAG は Static LAG をサポートしません。

MLAG Settings（MLAG 設定）

MLAG の設定を行います。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 8-73　MLAG Settings (Disabled) 画面

画面に表示される項目：

項目	説明
MLAG State	MLAG 機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

MLAG を有効にし、スイッチの再起動を行うと次の画面が表示されます。

MLAG Settings(有効時)

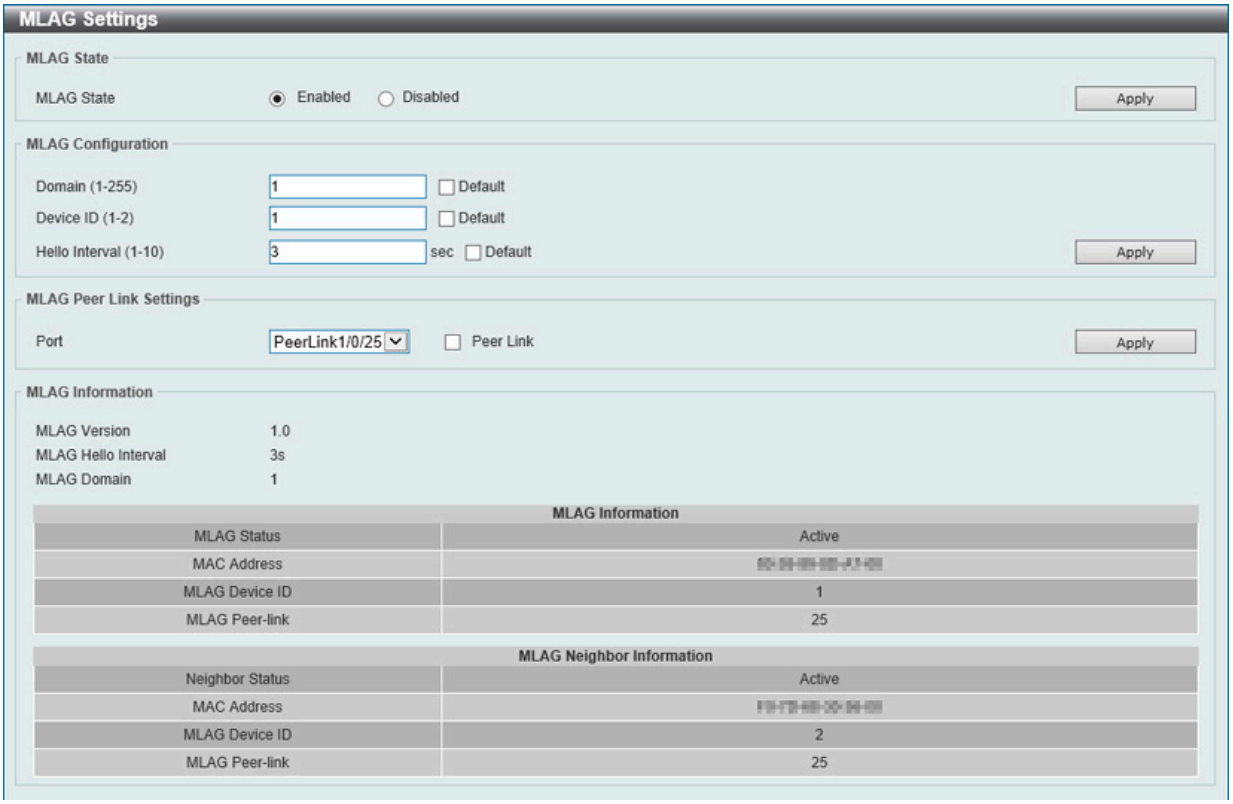


図 8-74　MLAG Settings (Enabled) 画面

画面に表示される項目：

項目	説明
MLAG State	
MLAG State	MLAG 機能を有効 / 無効に設定します。
MLAG Configuration	
Domain	MLAG ドメイン ID を指定します。「Default」にチェックを入れると初期値が適用されます。 • 設定可能範囲：1-255 • 初期値：1
Device ID	MLAG デバイス ID を指定します。「Default」にチェックを入れると初期値が適用されます。 • 設定可能範囲：1-2 • 初期値：1
Hello Interval	MLAG ハローインターバルを指定します。MLAG ハローメッセージの送信間隔になります。 「Default」にチェックを入れると初期値が適用されます。 • 設定可能範囲：1-10（秒） • 初期値：3（秒）
MLAG Peer Link Settings	
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。

「Apply」ボタンをクリックして、設定内容を適用します。

MLAG Group（MLAG グループ）

MLAG グループについて表示します。

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

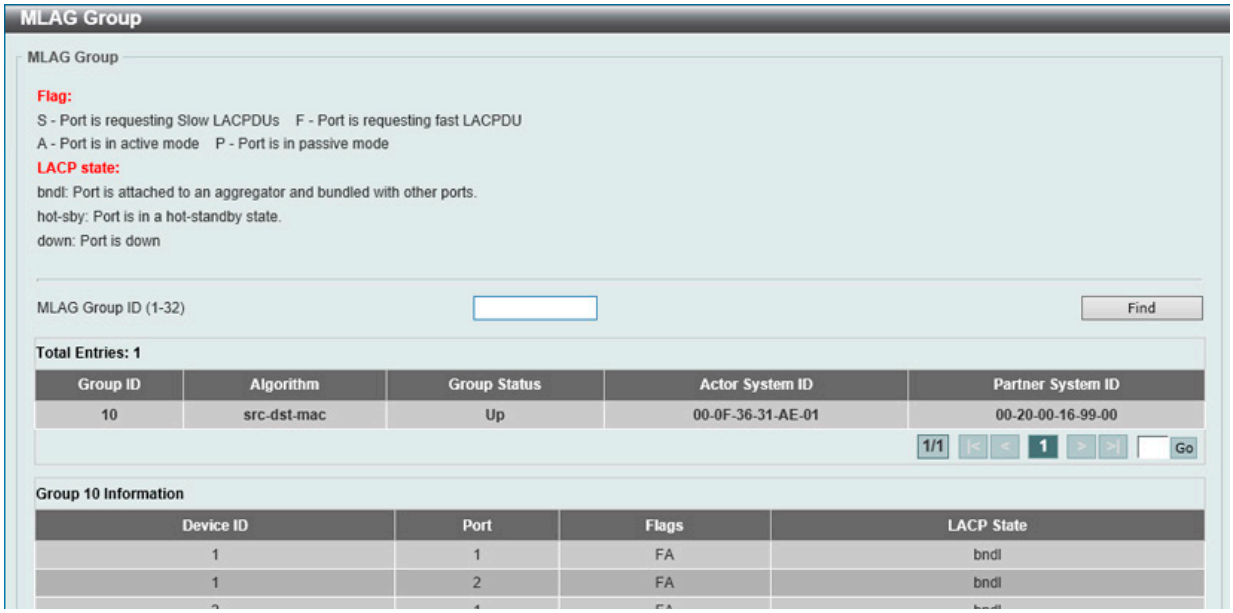


図 8-75　MLAG Group 画面

画面に表示される項目：

項目	説明
MLAG Group ID	MLAG Group ID を指定します。 • 設定可能範囲：1-32

「Find」ボタンをクリックして、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）

フレックスリンク機能を設定します。本機能では、レイヤ 2 インタフェースのペアを作成しインタフェースのバックアップを設定します。STP や LBD の代替機能として、リンクレベルでの冗長性を提供します。

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

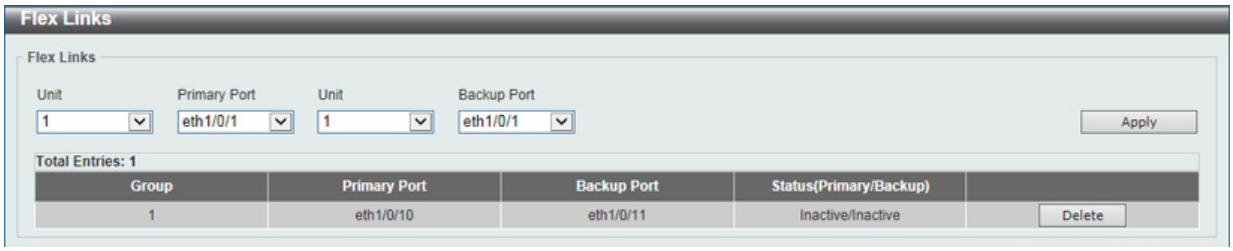


図 8-76　Flex Links 画面

画面に表示される項目：

項目	説明
Unit	プライマリポートのユニットを指定します。
Primary Port	プライマリポートを指定します。
Unit	バックアップポートのユニットを指定します。
Backup Port	バックアップポートを指定します。

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

注意　フレックスリンクは、STP、ERPS、LBD 機能と相互排他になります。

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。

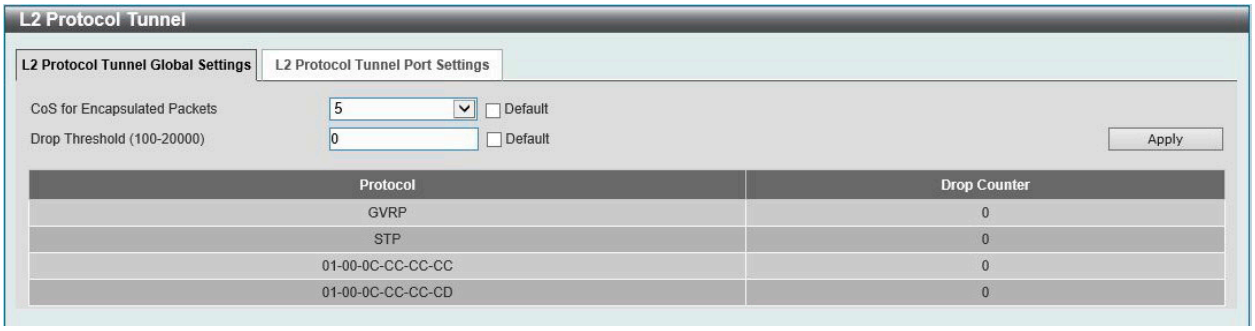


図 8-77　L2 Protocol Tunnel 画面 - L2 Protocol Tunnel Global Settings タブ

画面に表示される項目：

項目	説明
CoS for Encapsulated Packets	カプセル化されたパケットの CoS 値を指定します。「Default」を指定すると初期値を指定します。 • 設定可能範囲：0-7
Drop Threshold	破棄しきい値を指定します。L2 プロトコルパケットのトンネリングはパケットのカプセル化、非カプセル化、フォワーディングに CPU 処理容量を消費します。本オプションを使用することにより、システムにより処理される全 L2 プロトコルパケットの数にしきい値を設け、消費される CPU プロセス帯域を制限します。パケットの最大値がしきい値を超えた場合、超えた分のパケットは破棄されます。「Default」を指定すると初期値を使用します。 • 設定可能範囲：100-20000 • 初期値：0

「Apply」ボタンをクリックして、設定内容を適用します。

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

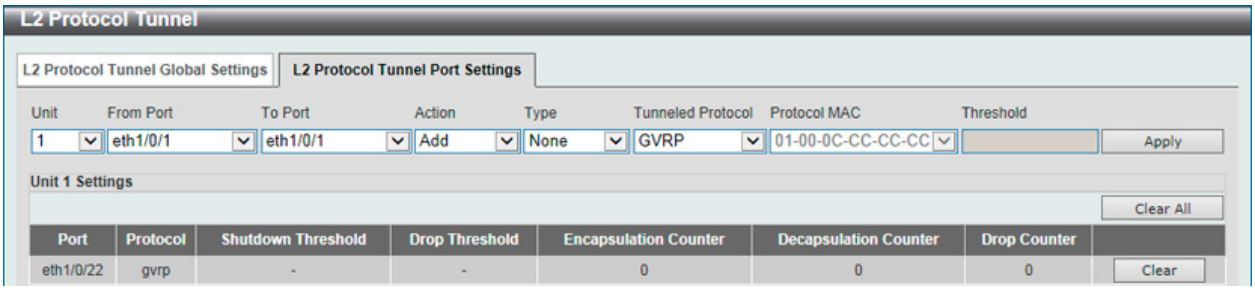


図 8-78　L 2 Protocol Tunnel 画面 - L2 Protocol Tunnel Port Settings タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Action	実行する動作を指定します。 • 「Add」- 入力した情報に基づいてエントリを追加します。 • 「Delete」- 入力した情報に基づいてエントリを削除します。
Type	ポートタイプを指定します。 • 選択肢：「None」「Shutdown」「Drop」
Tunneled Protocol	トンネルされるプロトコルを選択します。 • 選択肢：「GVRP」「STP」「Protocol MAC」「All」
Protocol MAC	トンネルプロトコルに「Protocol MAC」を選択した場合、プロトコル MAC オプションを指定します。 • 選択肢：「01-00-0C-CC-CC-CC 」「01-00-0C-CC-CC-CD」
Threshold	ポートタイプで「Shutdown」「Drop」を指定した場合、しきい値を入力します。 • 設定可能範囲：1-4096

「Apply」ボタンをクリックして、各セクションで行った変更を適用します。
「Clear」ボタンをクリックして、指定エントリのカウンタ情報をクリアします。
「Clear All」ボタンをクリックして、すべてのカウンタ情報をクリアします。

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

IGMP（Internet Group Management Protocol）Snooping 機能を始めとした L2 Multicast Control（L2 マルチキャストコントロール）の設定を行います。

IGMP Snooping（IGMP Snooping の設定）

IGMP（Internet Group Management Protocol）Snooping 機能を利用すると、スイッチはネットワークステーションまたはデバイスと IGMP ホスト間で送信される IGMP クエリと IGMP レポートを認識するようになります。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、まず本機能をスイッチ全体で有効にする必要があります。その後、対応する「Edit」ボタンをクリックして、各 VLAN に詳細な設定を行います。IGMP Snooping を有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバに接続するポートをオープンまたはクローズできるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストが存在しなくなった場合、マルチキャストパケットの送信を停止します。

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。

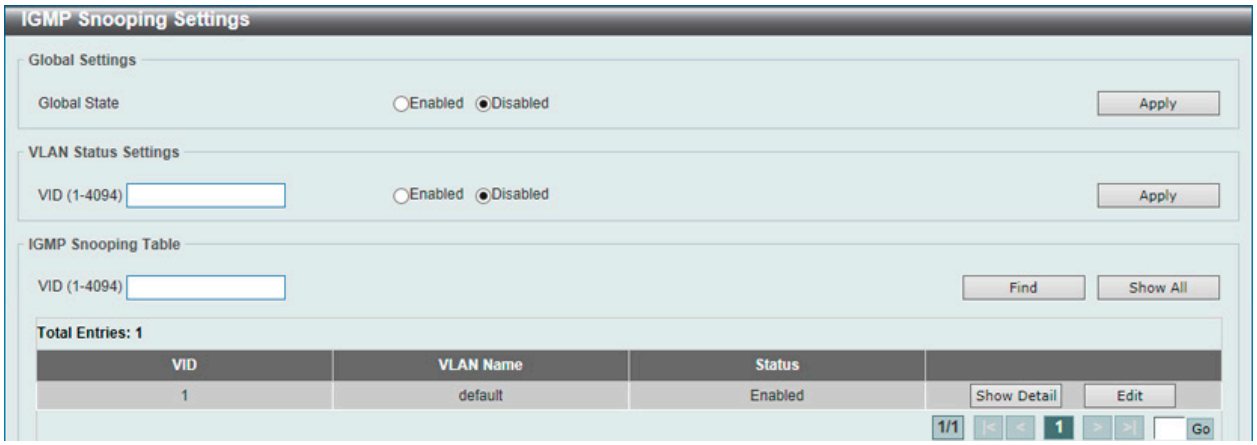


図 8-79　IGMP Snooping Settings 画面

画面に表示される項目：

項目	説明
Global Setting	
Global State	IGMP Snooping のグローバルステータスを有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
VLAN Status Settings	
VID	VLAN を識別する VLAN ID を入力し、指定 VLAN 上の IGMP Snooping を有効 / 無効に設定します。 • 設定可能範囲：1-4094
IGMP Snooping Table	
VID	IGMP Snooping テーブルに表示する VLAN の VLAN ID を指定します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した VLAN ID のエントリを表示します。
「Show All」ボタンをクリックして、IGMP 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。

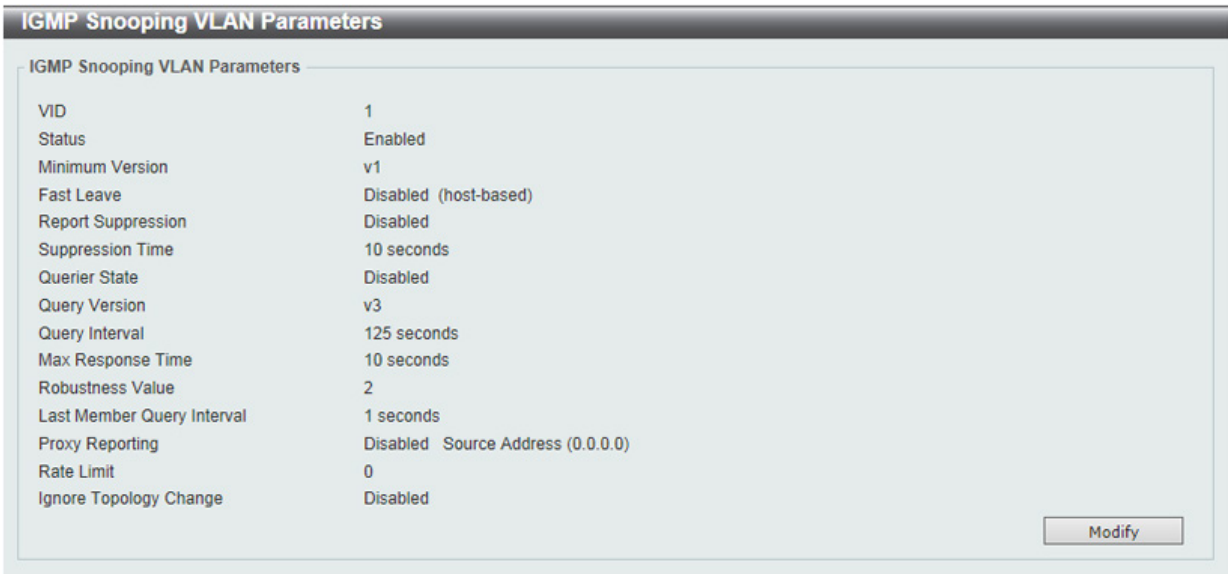


図 8-80　IGMP Snooping VLAN Parameters 画面

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

■ IGMP Snooping 機能の詳細設定

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

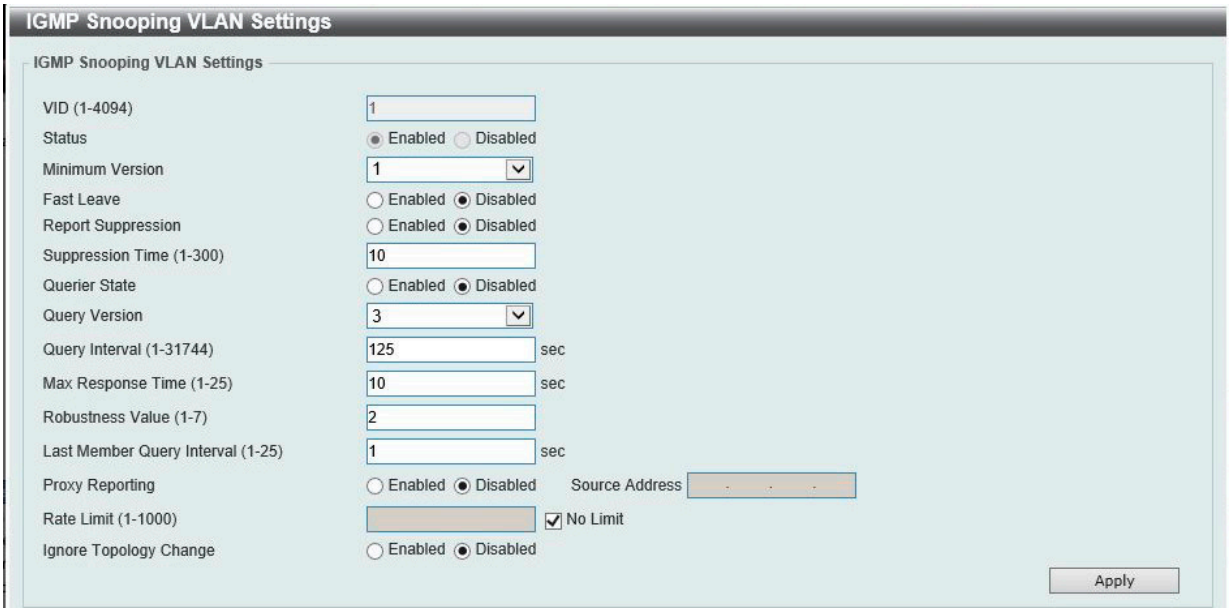


図 8-81 IGMP Snooping VLAN Settings 画面

画面に表示される項目：

項目	説明
VID	IGMP Snooping 設定を変更する VLAN を識別する VLAN ID が表示されます。
Status	VLAN の IGMP Snooping 機能の有効 / 無効ステータスが表示されます。
Minimum Version	VLAN に対して許可される IGMP ホストの最小バージョンを選択します。 • 選択肢：「1」「2」「3」
Fast Leave	Fast Leave 機能を有効 / 無効に設定します。この機能が有効になると、システムが IGMP done メッセージを受信すると、メンバシップがすぐに削除されます。
Report Suppression	特定の VLAN への IGMP スヌーピングレポートの抑制を有効 / 無効に設定します。 レポートサスペンション機能は「IGMPv1」「IGMPv2」トラフィックでのみ機能します。 有効になるとホストによるレポートの重複した送信は抑制されます。抑制は抑制時間（Suppression Time）を過ぎるまで続きます。同じグループに対する Report/Leave メッセージは、1 つのメッセージのみが送信され、残りのメッセージは抑制されます。

項目	説明
Suppression Time	スヌーピングレポートの抑制時間を設定します。 • 設定可能範囲：1-300（秒）
Querier State	クエリア機能を有効 / 無効に設定します。
Query Version	IGMP スヌーピングクエリアで送信されるクエリパケットのバージョンを選択します。 • 選択肢：「1」「2」「3」
Query Interval	IGMP スヌーピングクエリアが General クエリを送信する間隔を指定します。 • 設定可能範囲：1-31744（秒）
Max Response Time	IGMP スヌーピングクエリでアドバタイズされる最大応答時間を指定します。 • 設定可能範囲：1-25（秒）
Robustness Value	パケットロスに対するロバストネス変数を指定します。 • 設定可能範囲：1-7
Last Member Query Interval	IGMP スヌーピングクエリアが IGMP Group-Specific クエリまたは Group-Source-Specific (Channel) クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1-25（秒）
Proxy Reporting	プロキシレポーティング機能を有効 / 無効に設定します。
Source Address	プロキシレポーティングの送信元 IP アドレスを指定します。
Rate Limit	レートリミットを指定します。「No Limit」を指定すると、プロファイルにレート制限が適用されません。 • 設定可能範囲：1-1000
Ignore Topology Change	「Ignore Topology Change」機能を有効 / 無効にします。有効にするとトポロジの変更は無視されます。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　IGMP Snooping について、fast-leave は IGMPv2 のみサポートしています。

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

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

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

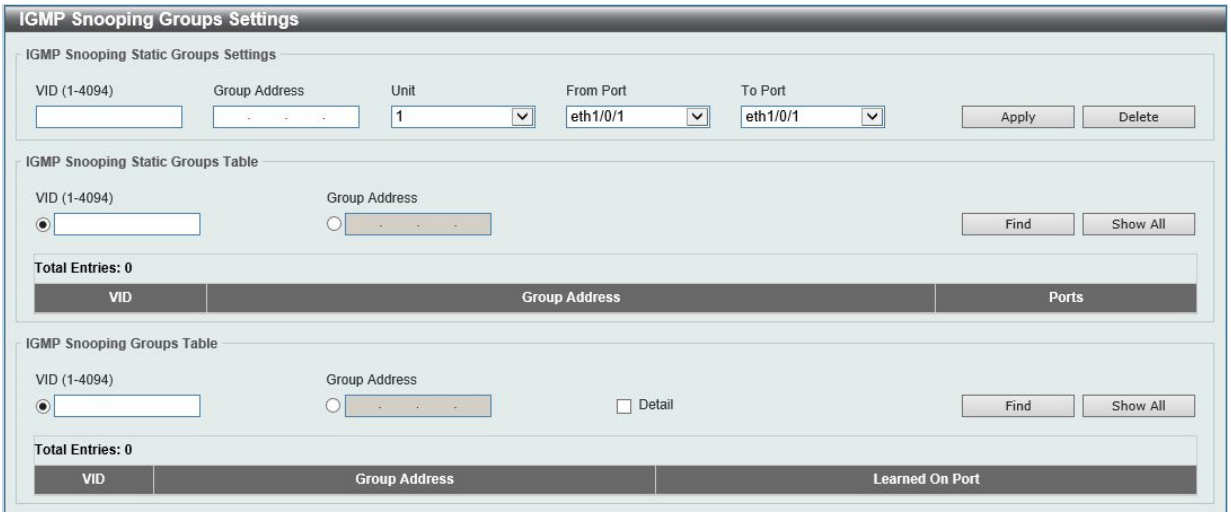


図 8-82　IGMP Snooping Groups Settings 画面

以下の項目を使用して、設定します。

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

項目	説明
IGMP Snooping Static Groups Settings	
VID	登録または削除するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	登録または削除するマルチキャストグループの IP アドレスを入力します。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。
IGMP Snooping Static Groups Table	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094

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

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

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

項目	説明
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。
Detail	IGMP グループの詳細情報を表示します。

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

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

IGMP Snooping Filter Settings（IGMP Snooping フィルタ 設定）

IGMP Snooping フィルタの設定を行います。

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

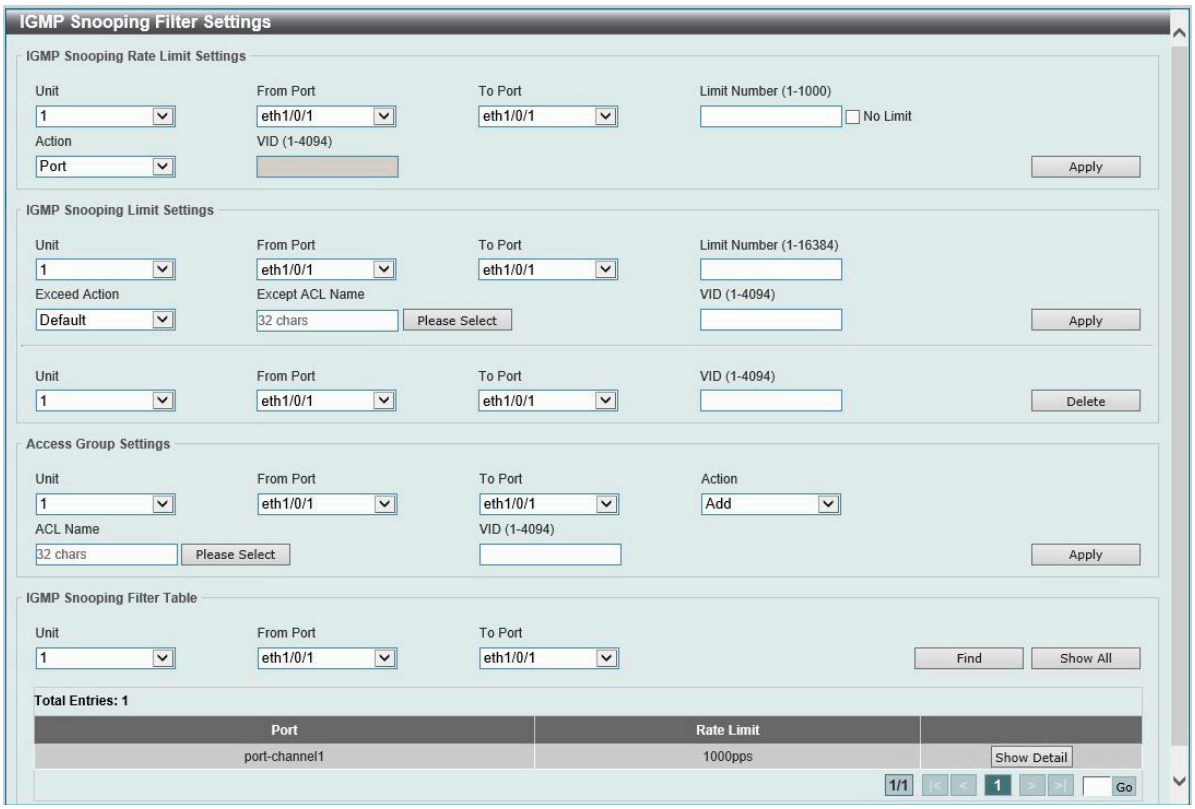


図 8-83　IGMP Snooping Filter Settings 画面

以下の項目を使用して、設定します。

IGMP Snooping Rate Limit Settings（IGMP スヌーピングレートリミット設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Limit Number	指定のインタフェースでスイッチが処理可能な IGMP コントロールパケットのレートを指定します。「No Limit」を指定すると、制限を行いません。 • 設定可能範囲：1-1000（パケット / 秒）
Action	実行するインタフェースを指定します。 • 選択肢：「Port」「VLAN」

項目	説明
VID	「Action」で「VLAN」を選択すると表示されます。この VLAN で受信するパケットに対して、フィルタします。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。

IGMP Snooping Limit Settings（IGMP スヌーピングリミット設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Limit Number	生成される IGMP キャッシュエントリ数の上限値を指定します。 • 設定可能範囲：1-16384
Exceed Action	しきい値を超過した場合の動作について指定します。制限を超えた場合、新しく学習したグループに対して以下の処理を実行します。 •「Default」- デフォルトのアクションを実行します。 •「Drop」- 新規グループは破棄されます。 •「Replace」- 新規グループは古いグループに置き換わります。
Except ACL Name	標準 IP アクセスリストを指定します（32 文字以内）。アクセスリストに許可されたグループ (*,G) は制限から外れます。グループ (*,G) を許可するにはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「Please Select」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	トランクポートのレイヤ 2 VLAN 名を入力します。この VLAN で受信するパケットにフィルタを適用します。 • 設定可能範囲：1-4094

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

Access Group Settings（アクセスグループ設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Action	•「Add」- 入力した情報に基づき新しいエントリを追加します。 •「Delete」- 入力した情報に基づき既存エントリを削除します。
ACL Name	標準 IP アクセスリストを指定します（32 文字以内）。グループ (*,G) への参加をユーザに許可する場合に使用します。アクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「Please Select」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	設定する VLAN を指定します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。

IGMP Snooping Filter Table（IGMP スヌーピングフィルタテーブル）

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

「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」ボタンをクリックして、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 8-84　ACL Access List 画面

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

「**Show Detail**」をクリックすると次の画面が表示されます。



図 8-85　IGMP Snooping Detail Filter table (Show Detail) 画面

前の画面に戻るには、「Back」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

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。

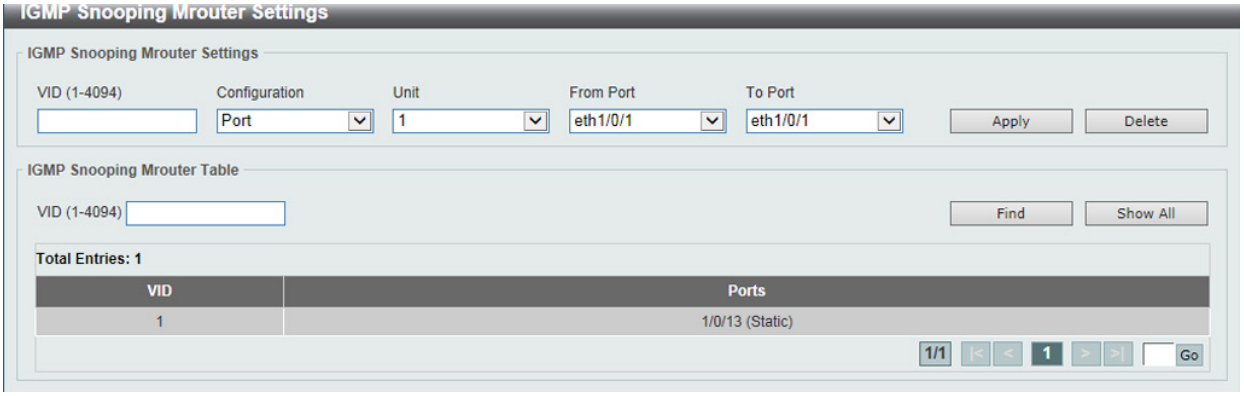


図 8-86　IGMP Snooping Mrouter Settings 画面

画面には以下の項目があります。

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

項目	説明
IGMP Snooping Mrouter Settings	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094
Configuration	ポートの設定を行います。 • 「Port」- ポートをマルチキャストルータポートに指定します。 • 「Forbidden Router Port」- ポートを非マルチキャストポートに指定します。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。

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

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

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

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

IGMP Snooping Statistics Settings（IGMP Snooping 統計設定）

IGMP Snooping の統計情報を表示します。

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

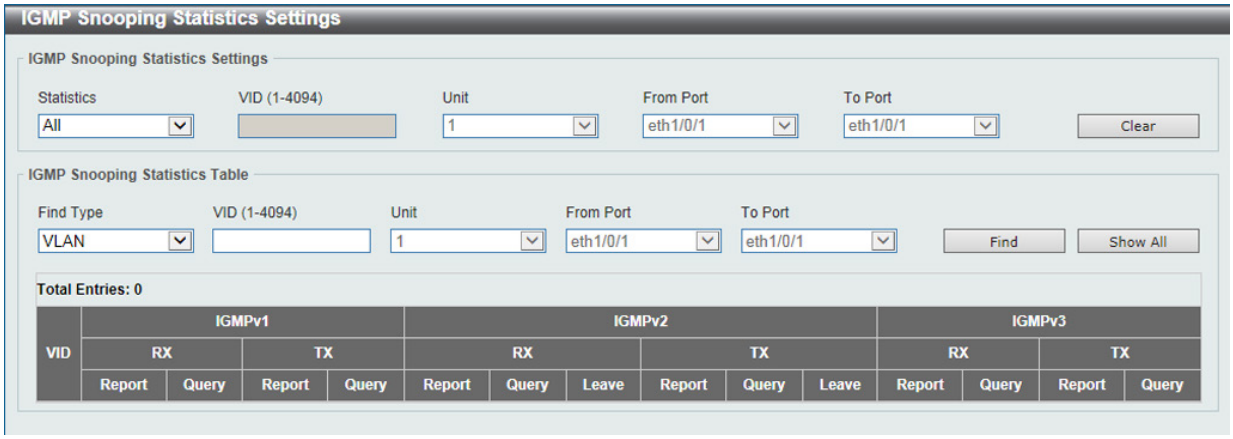


図 8-87　IGMP Snooping Statistics Settings 画面

以下の項目が表示されます。

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

項目	説明
Statistics	インタフェースを選択します。 • 選択肢：「All」「VLAN」「Port」
VID	VLAN ID を指定します。「Statistics」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
Unit	本設定を適用するユニットを選択します。「Statistics」で「Port」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Statistics」で「Port」を選択すると設定可能になります。

「Clear」ボタンをクリックして、IGMP スヌーピング関連の統計情報をクリアします。

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

項目	説明
Find Type	インタフェースを選択します。 • 選択肢：「VLAN」「Port」
VID	VLAN ID を指定します。「Find Type」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
Unit	本設定を適用するユニットを選択します。「Find Type」で「Port」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Find Type」で「Port」を選択すると設定可能になります。

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

MLD Snooping（MLD スヌーピング）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じ機能を持つ、IPv6 用のマルチキャストトラフィック制御機能です。VLAN 上でマルチキャストデータを要求するポートを検出するために使用されます。MLD Snooping では、所定の VLAN 上のすべてのポートにマルチキャストトラフィックを流すのではなく、要求元ポートとマルチキャストの送信元によって生成される MLD クエリと MLD レポートを使用して、データを受信したいポートに対してのみ、マルチキャストデータを転送します。
MLD Snooping は、エンドノードと MLD ルータとの間で交換される MLD 制御パケットのレイヤ 3 部分を調べることでパケットを処理します。スイッチは、ルートがマルチキャストトラフィックをリクエストしていることを検出すると、そのルートに直接接続されているポートを IPv6 マルチキャストテーブルに追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のエントリには、該当ポートや VLAN ID、関連する IPv6 マルチキャストグループアドレスが記録され、このポートはアクティブな Listening ポートと見なされます。アクティブな Listening ポートのみがマルチキャストグループデータを受信します。

MLD コントロールメッセージ

MLD Snooping を使用するデバイス間で以下の MLD コントロールメッセージが交換されます。これらのメッセージは、130、131、132 および 143 でラベル付けされた 4 つの ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query – IPv4 の IGMPv2 Host Membership Query（HMQ）に相当するメッセージです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query はリンク上のすべての Listening ポートに対し送信され、Multicast Specific Query は、特定のマルチキャストアドレスに対して送信されます。この 2 種類のメッセージは、IPv6 ヘッダ内のマルチキャスト宛先アドレス及び Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別されます。
2. Multicast Listener Report – IGMPv2 の Host Membership Report（HMR）に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。
3. Multicast Listener Done – IGMPv2 の Leave Group Message に相当するメッセージです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからのマルチキャストデータの受信を停止すること、つまり、このアドレスからのマルチキャストデータが "done"（完了）となった旨を伝えます。スイッチが本メッセージを受信すると、この Listening ホストには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しなくなります。
4. Multicast Listener Report Version2 – IGMPv3 の Host Membership Report（HMR）に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

MLD Snooping Settings（MLD スヌーピング設定）

MLD Snooping 設定を有効または無効にします。

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

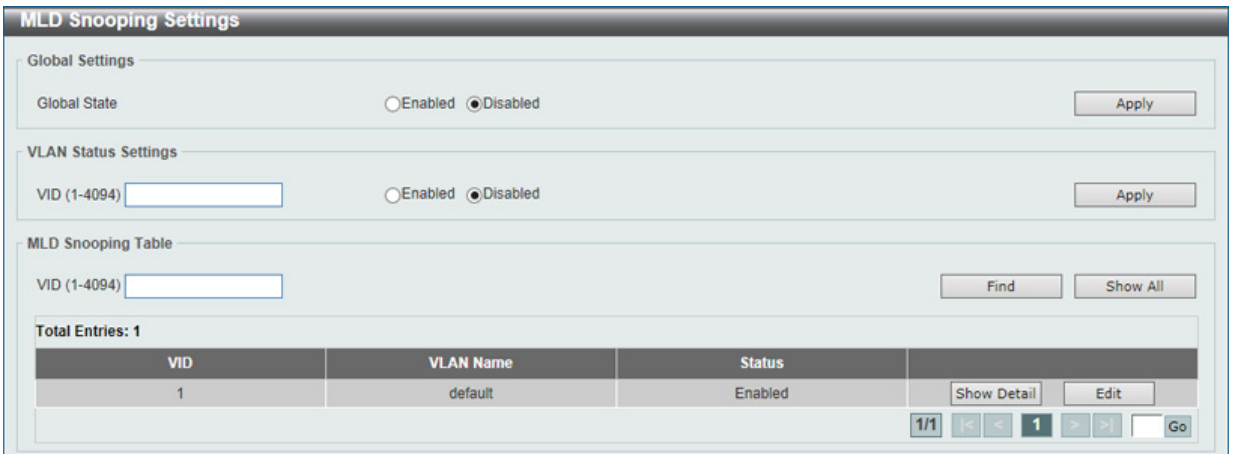


図 8-88　MLD Snooping Settings 画面

画面に表示される項目：

項目	説明
Global Setting	
Global State	MLD Snooping のグローバルステータスを有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
VLAN Status Settings	
VID	VLAN を識別する VLAN ID を入力し、指定 VLAN 上の MLD Snooping を有効 / 無効に設定します。 • 設定可能範囲：1-4094

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

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した VLAN ID のエントリを表示します。
「Show All」ボタンをクリックして、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。

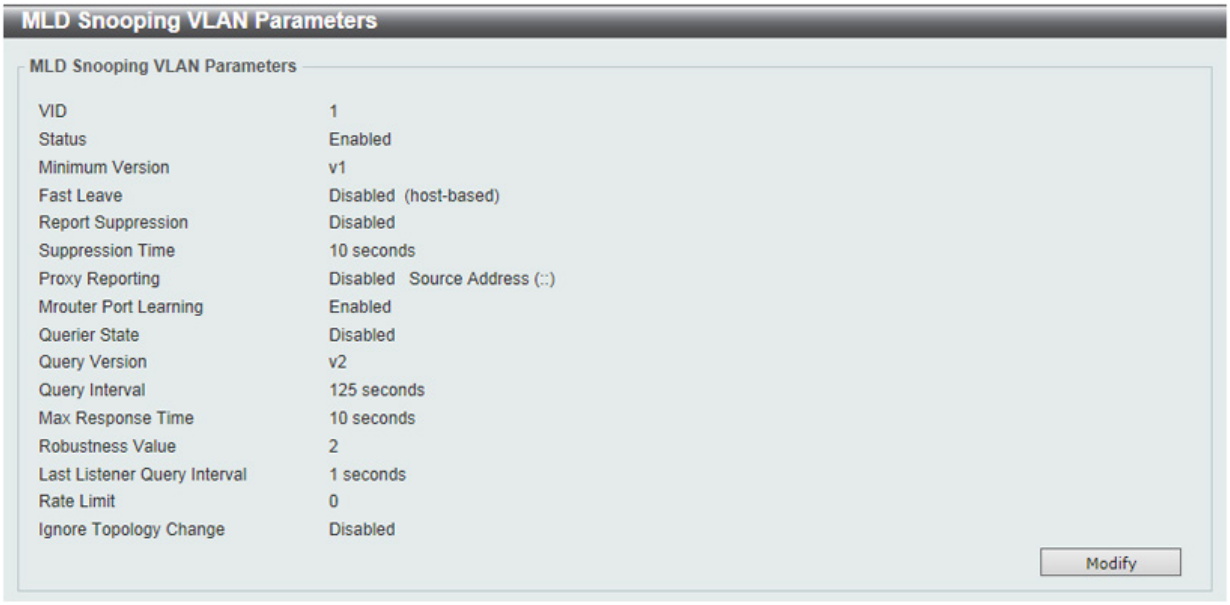


図 8-89　MLD Snooping VLAN Parameters 画面

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

MLD Snooping 機能の詳細設定
「MLD Snooping Settings」で関連する 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。

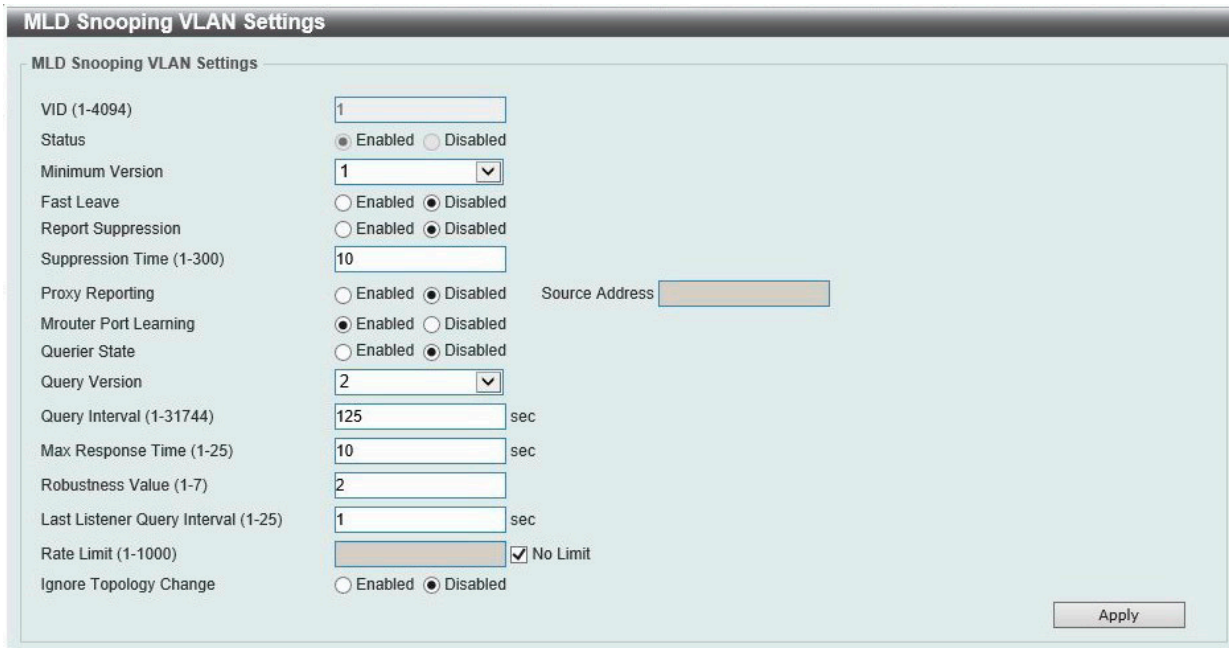


図 8-90 MLD Snooping VLAN Settings 画面

画面に表示される項目：

項目	説明
VID	MLD Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
Status	VLAN の MLD Snooping 機能を有効 / 無効ステータスを表示します。

項目	説明
Minimum Version	VLAN に許可された MLD ホストの最小バージョンを選択します。 • 選択肢：「1」「2」
Fast Leave	Fast Leave 機能の有効 / 無効を設定します。本機能が有効の場合、スイッチが MLD Leave メッセージを受信すると、マルチキャストグループのメンバは直ちにグループから脱退します。
Report Suppression	特定の VLAN への MLD スヌーピングレポートの抑制を有効 / 無効に設定します。
Suppression Time	スヌーピングレポートの抑制時間を設定します。 • 設定可能範囲：1-300（秒）
Proxy Reporting	プロキシレポーティング機能を有効 / 無効に設定します。
Source Address	プロキシレポーティングの送信元 IP アドレスを指定します。
Mrouter Port Learning	mrouter ポート学習機能を有効 / 無効に設定します。
Querier State	MLD クエリア機能を有効 / 無効に設定します。
Query Version	MLD スヌーピングクエリアによって送信される General クエリパケットのバージョンを選択します。 • 選択肢：「1」「2」
Query Interval	MLD スヌーピングクエリアが MLD General クエリメッセージを送信する間隔を入力します。 • 設定可能範囲：1-31744（秒）
Max Response Time	MLD スヌーピングクエリでアドバタイズされる最大応答時間を指定します。 • 設定可能範囲：1-25（秒）
Robustness Value	パケットロスに対するロバストネス変数を指定します。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。 • 設定可能範囲：1-7
Last Listener Query Interval	MLD スヌーピングクエリアが MLD Group-Specific クエリまたは Group-Source-Specific (Channel) クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1-25
Rate Limit	レートリミットを指定します。「No Limit」を指定すると本プロファイルでは制限がなしになります。 • 設定可能範囲：1-1000
Ignore Topology Change	「Ignore Topology Change」を有効 / 無効に設定します。有効にするとトポロジの変更は無視されます。

「Apply」ボタンをクリックして、設定内容を適用します。

注意 MLD Snooping について、fast-leave は MLDv1 のみサポートします。

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

MLD スヌーピングスタティックグループの表示と設定、および MLD スヌーピンググループの表示を行います。

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

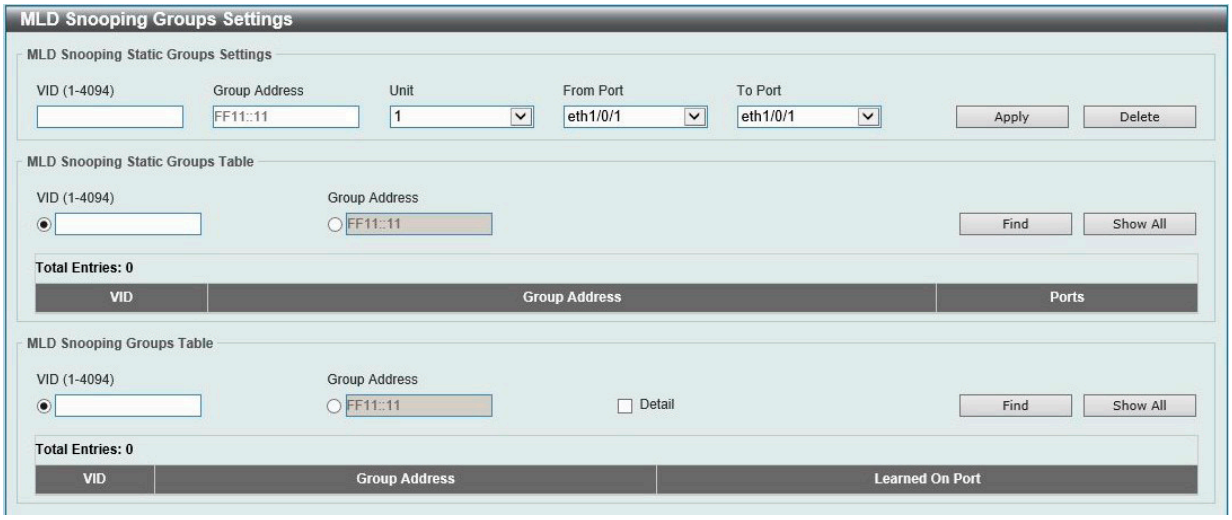


図 8-91　MLD Snooping Groups Settings 画面

以下の項目を使用して、設定します。

■ MLD Snooping Static Groups Settings/Table（MLD スヌーピングスタティックグループ設定 / テーブル）

項目	説明
MLD Snooping Static Groups Settings	
VID	登録または削除する IPv6 マルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	登録または削除する IPv6 マルチキャストグループの IPv6 アドレスを入力します。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
MLD Snooping Static Groups Table	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

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

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

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

MLD Snooping Filter Settings（MLD Snooping フィルタ設定）

MLD Snooping フィルタの設定を行います。

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

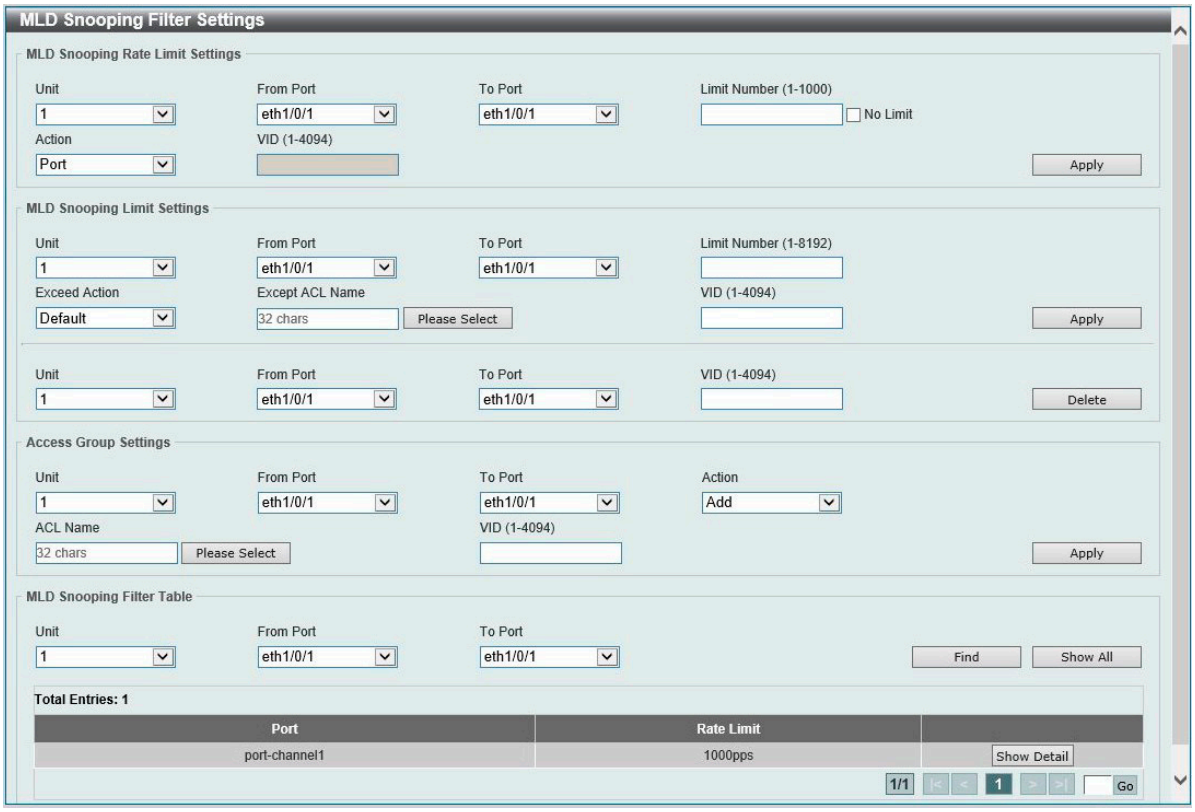


図 8-92　MLD Snooping Filter Settings 画面

以下の項目を使用して、設定します。

■ MLD Snooping Rate Limit Settings（MLD スヌーピングレートリミット設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
Limit Number	指定のインタフェースでスイッチが処理可能な MLD コントロールパケットのレートを指定します。「No Limit」で制限を設定しません。 • 設定可能範囲：1-1000（パケット / 秒）
Action	実行するインタフェースを指定します。 • 選択肢：「Port」「VLAN」
VID	「Action」で「VLAN」を選択した場合、VLAN ID を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。

■ MLD Snooping Limit Settings（MLD スヌーピングリミット設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
Limit Number	生成される MLD キャッシュエントリ数の上限値を指定します。 • 設定可能範囲：1-8192
Exceed Action	制限を超えた場合、新しく学習したグループに対して以下の処理を実行します。 • 「Default」- デフォルトのアクションを実行します。 • 「Drop」- 新規グループは破棄されます。 • 「Replace」- 新規グループは古いグループに置き換わります。
Except ACL Name	標準 IP アクセスリストを指定します（32 文字以内）。アクセスリストに許可されたグループ (*,G) は制限から除外されます。グループ (*,G) を許可するにはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「Please Select」をクリックして、作成済みのアクセスリストを選択することもできます。

項目	説明
VID	トランクポートのレイヤ2 VLAN 名を入力します。このVLAN で受信するパケットにフィルタを適用します。 • 設定可能範囲：1-4094

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

■ Access Group Settings（アクセスグループ設定）

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。
Action	• 「Add」- 入力した情報に基づき新しいエントリを追加します。 • 「Delete」- 入力した情報に基づき既存エントリを削除します。
ACL Name	標準 IP アクセスリストを指定します（32 文字以内）。グループ (*,G) への参加をユーザに許可する場合に使用します。アクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「Please Select」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	設定する VLAN を指定します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。

■ MLD Snooping Filter Table（MLD スヌーピングフィルタテーブル）

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

「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」ボタンをクリックして、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 8-93　ACL Access List 画面

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

「Show Detail」をクリックすると次の画面が表示されます。



図 8-94　MLD Snooping Detail Filter Table（Show Detail）画面

前の画面に戻るには、「Back」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

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。

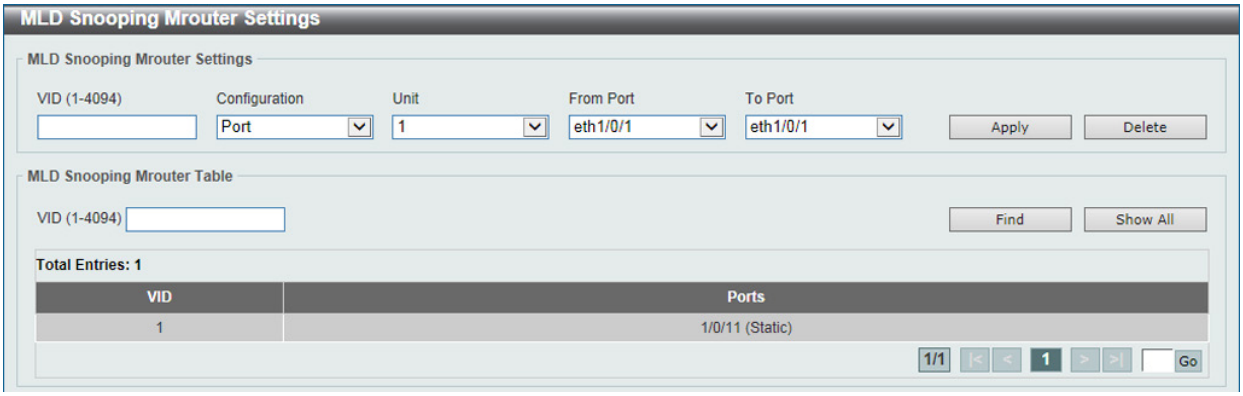


図 8-95　MLD Snooping Mrouter Settings 画面

画面には以下の項目があります。

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

項目	説明
MLD Snooping Mrouter Settings	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094
Configuration	ポートの設定を行います。 • 「Port」- マルチキャストが有効なルータと接続するポート範囲を設定します。 • 「Forbidden Port」- マルチキャストが有効なルータと接続しないポート範囲を設定します。 • 「Learn pimv6」- マルチキャストルータポートの自動取得を有効にします。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポートの範囲を設定します。

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

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

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

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

MLD Snooping Statistics Settings（MLD Snooping 統計設定）

現在の MLD Snooping の統計情報を表示します。

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

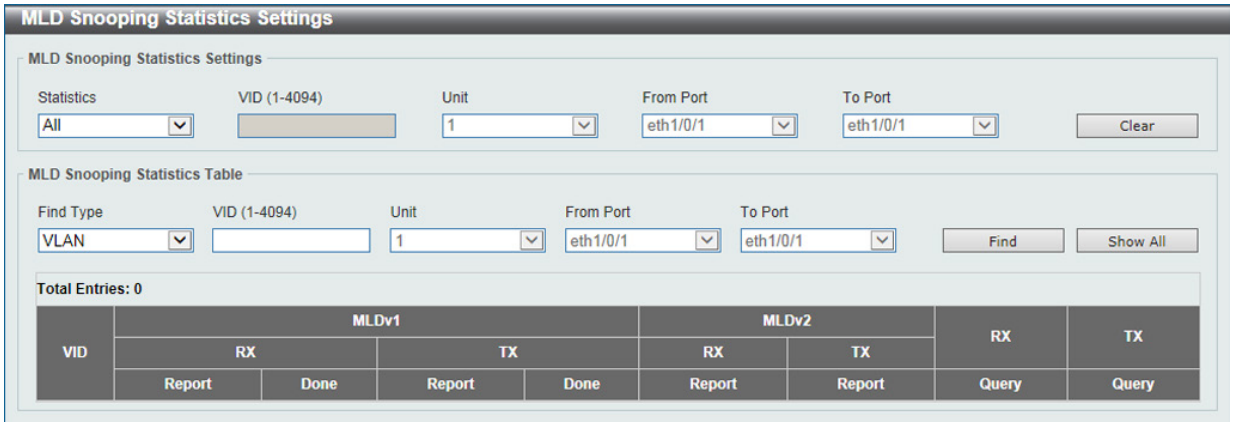


図 8-96　MLD Snooping Statistics Settings 画面

以下の項目が表示されます。

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

項目	説明
Statistics	インタフェースの種類を選択します。 • 選択肢：「All」「VLAN」「Port」
VID	VLAN ID を指定します。「Statistics」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
Unit	本設定を適用するユニットを選択します。「Statistics」で「Port」を選択すると設定可能になります。
From Port / To Port	本設定を適用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」ボタンをクリックして、MLD スヌーピング関連の統計情報をクリアします。

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

項目	説明
Find Type	インタフェースの種類を選択します。 • 選択肢：「VLAN」「Port」
VID	VLAN ID を指定します。「Find Type」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
Unit	本設定を適用するユニットを選択します。「Find Type」で「Port」を選択すると設定可能になります。
From Port / To Port	本設定を適用するポートの範囲を設定します。「Find Type」で「Port」を選択すると設定可能になります。

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

Multicast VLAN（マルチキャスト VLAN）

L2 Features > L2 Multicast Control > Multicast VLAN

Multicast VLAN Settings（マルチキャスト VLAN 設定）

マルチキャスト VLAN の設定を行います。

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

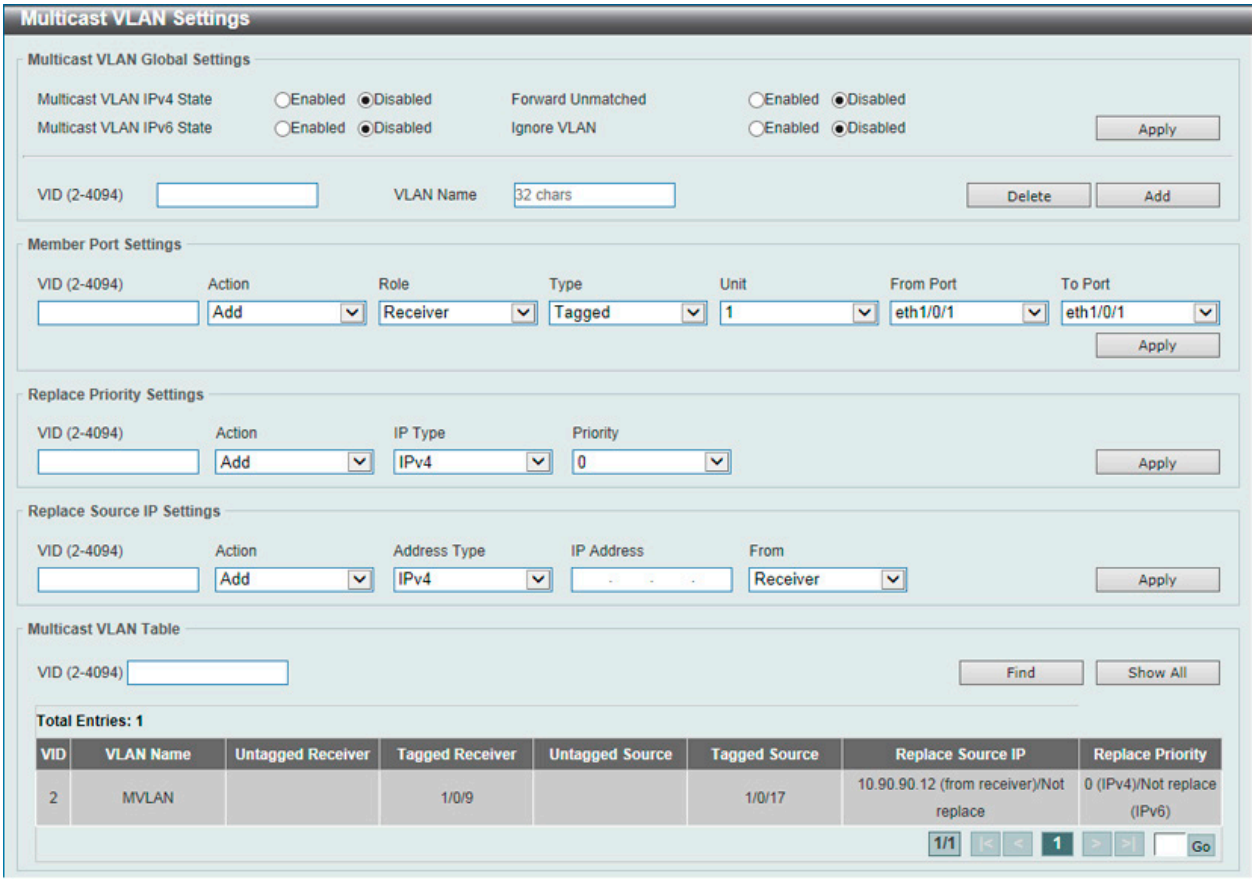


図 8-97　Multicast VLAN Settings 画面

画面に表示される項目：

項目	説明
Multicast VLAN Global Settings	
Multicast VLAN IPv4 State	マルチキャスト VLAN における IPv4 IGMP コントロールパケット処理を有効 / 無効に設定します。
Forward Unmatched	「Forward Unmatched」を有効 / 無効に設定します。 以下のいずれかの場合に、本設定に応じて転送または破棄されます。 - 受信 IGMP/MLD コントロールパケットがアンタグパケットであり、プロファイルに一致しない、かつ関連するデフォルト VLAN がマルチキャスト VLAN の場合 - 受信 IGMP/MLD コントロールパケットがマルチキャスト VLAN のタグ付きパケットであり、プロファイルに一致しない場合 初期値ではパケットは破棄されます。
Multicast VLAN IPv6 State	マルチキャスト VLAN における IPv6 MLD コントロールパケット処理を有効 / 無効に設定します。
Ignore VLAN	タグ付き IGMP/MLD コントロールパケットに対する「Ignore VLAN」を有効/無効に設定します。本設定を有効にすると、受信 IGMP/MLD コントロールパケットの VLAN は無視され、プロファイルの照合を行います。
VID	作成 / 削除するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
VLAN Name	作成 / 削除するマルチキャスト VLAN の VLAN 名を指定します。
Member Port Settings	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
Action	実行する動作を指定します。 • 選択肢：「Add（追加）」「Delete（削除）」

項目	説明
Role	メンバポートの役割を指定します。 • 「Receiver」- マルチキャスト VLAN のマルチキャストデータ受信のみを行うサブスクライバポートとして設定します。 • 「Source」- マルチキャスト VLAN のマルチキャストデータ送信を行うことができるアップリンクポートとして設定します。
Type	メンバポートの種類を指定します。 • 「Tagged」- ポートがタグ付きメンバに指定されると、当該ポートから送信されるパケットはマルチキャスト VLAN ID でタグ付けされます。 • 「Untagged」- ポートがタグなしメンバに指定されると、当該ポートから送信されるパケットはタグ無しフォームで転送されます。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Replace Priority Settings	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
Action	実行する動作を指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
IP Type	アドレスの種類を指定します。 • 「IPv4」- マルチキャスト VLAN で送信する IPv4 マルチキャストパケットにプライオリティを再マッピングします。 • 「IPv6」- マルチキャスト VLAN で送信する IPv6 マルチキャストパケットにプライオリティを再マッピングします。
Priority	優先値を指定します。 • 設定可能範囲：0-7
Replace Source IP Settings	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
Action	実行する動作を指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Address Type	アドレスの種類を指定します。「 IPv4」「IPv6」から指定可能です。 • 「IPv4」- ルータに送信される IGMP コントロールパケットの送信元 IPv4 アドレスを指定します。 • 「IPv6」- ルータに送信される MLD コントロールパケットの送信元 IPv6 アドレスを指定します。
IP Address	IPv4/IPv6 アドレスを指定します。
From	送信元オプションを指定します。 • 「Receiver」- マルチキャスト VLAN Receiver ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。 • 「Source」- マルチキャスト VLAN Source ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。 • 「Both」- 全てのマルチキャスト VLAN ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。
Multicast VLAN Table	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094

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

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

Multicast VLAN Group Settings（マルチキャスト VLAN グループ設定）

マルチキャスト VLAN グループの設定、表示を行います。

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

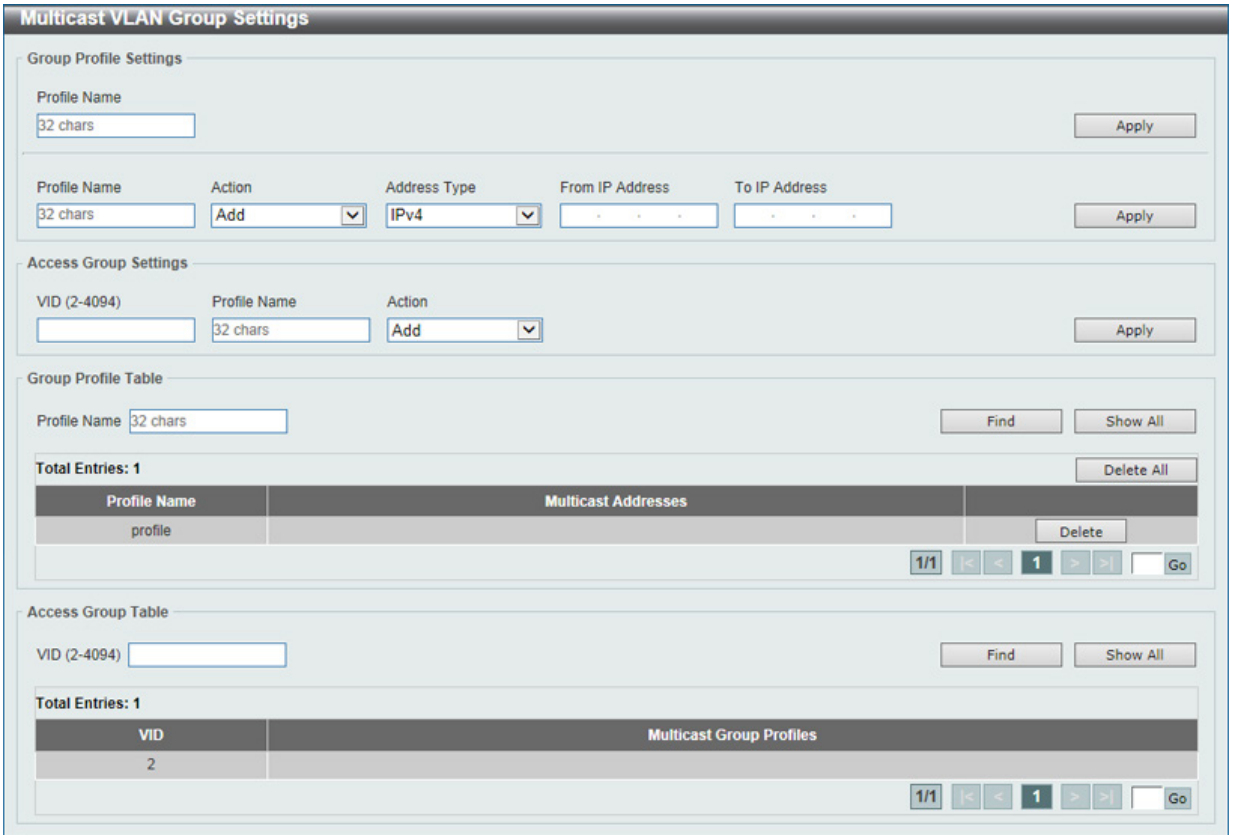


図 8-98　Multicast VLAN Group Settings 画面

画面に表示される項目：

項目	説明
Groups Profile Settings	
Profile Name	マルチキャスト VLAN のグループプロファイル名を指定します。（32 文字以内）
Action	実行する動作を指定します。マルチキャスト VLAN プロファイルには複数の範囲を追加することができます。同じプロファイルに対して指定される IP アドレス範囲は同じアドレスファミリである必要があります。 • 選択肢：「Add（追加）」「Delete（削除）」
Address Type	アドレスタイプを指定します。 • 「IPv4」- IPv4 マルチキャストアドレスを使用します。 • 「IPv6」- IPv6 マルチキャストアドレスを使用します。
From IP Address	IPv4/IPv6 アドレス範囲の開始アドレスを指定します。
To IP Address	IPv4/IPv6 アドレス範囲の終了アドレスを指定します。
Access Group Settings	
VID	VLAN ID を指定します。 • 設定可能範囲：2-4094
Profile Name	マルチキャスト VLAN のグループプロファイル名を指定します。（32 文字以内）
Action	実行する動作を指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Group Profile Table	
Profile Name	マルチキャスト VLAN のグループプロファイル名を指定します。（32 文字以内）
Access Group Table	
VID	VLAN ID を指定します。 • 設定可能範囲：2-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Delete All」ボタンをクリックすして、すべてのエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

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

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。

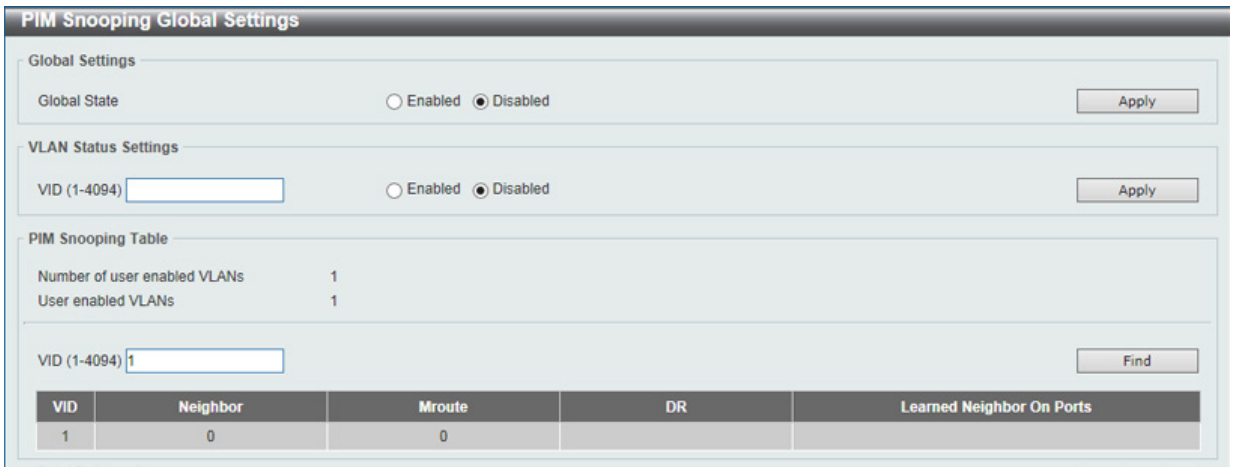


図 8-99　PIM Snooping Global Settings 画面

画面に表示される項目：

項目	説明
Global Settings	
Global State	PIM スヌーピングのグローバルステータスを有効 / 無効に設定します。
VLAN Status Settings	
VID	PIM スヌーピング機能を使用する VLAN ID を入力します。また、指定 VLAN 上の PIM スヌーピングを有効 / 無効に設定します。 • 設定可能範囲：1-4094
PIM Snooping Table	
VID	PIM スヌーピングテーブルで表示する VLAN の VLAN ID を指定します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した VLAN ID のエントリを表示します。

PIM Snooping Neighbor（PIM スヌーピングネイバ）

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 8-100　PIM Snooping Neighbor Table 画面

画面に表示される項目：

項目	説明
VID	表示する VLAN を識別する VLAN ID を指定します。 • 設定可能範囲：1-4094

「Find」ボタンをクリックして、指定した VLAN ID 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。

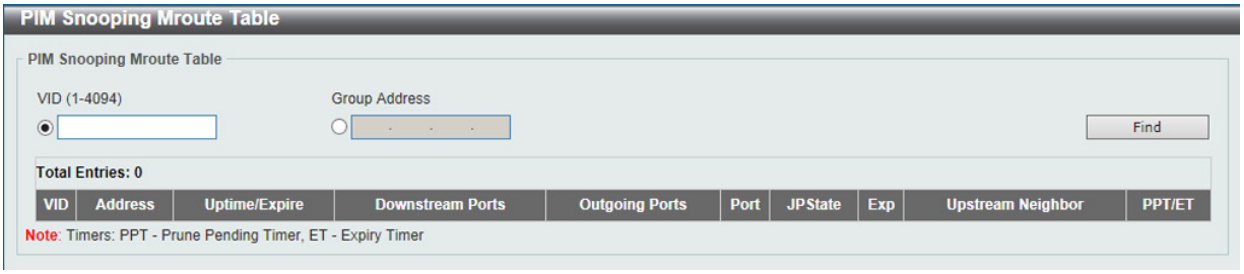


図 8-101　PIM Snooping Mroute Table 画面

画面に表示される項目：

項目	説明
VID	表示する VLAN を識別する VLAN ID を指定します。 • 設定可能範囲：1-4094
Group Address	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）

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。

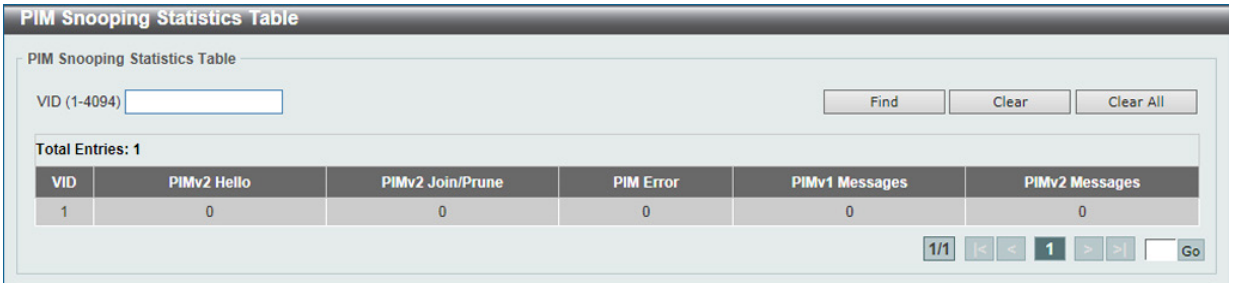


図 8-102　PIM Snooping Statistics Table 画面

画面に表示される項目：

項目	説明
VID	検索 / 削除するエントリの VLAN を識別する VLAN ID を指定します。 • 設定可能範囲：1-4094

「Find」ボタンをクリックして、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、指定した VLAN の統計情報をクリアします。
「Clear All」ボタンをクリックして、すべての統計情報をクリアします。

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

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。

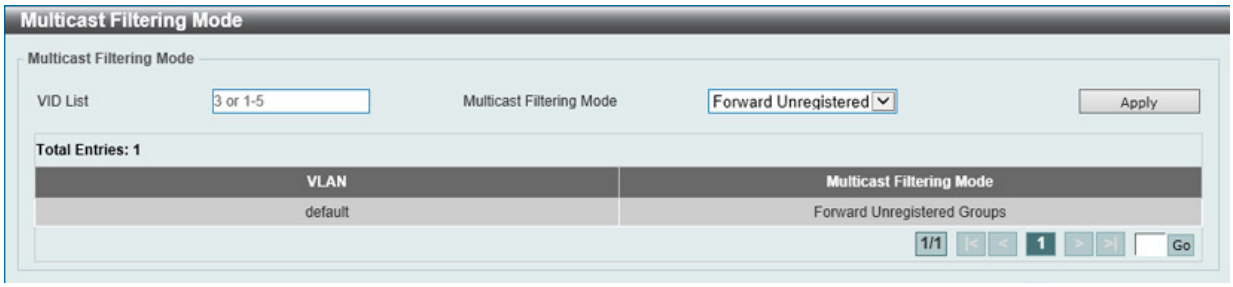


図 8-103　Multicast Filtering Mode 画面

画面に表示される項目：

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

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

LLDP

L2 Features > LLDP

LLDP（Link Layer Discovery Protocol）は、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）に格納されるため、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。

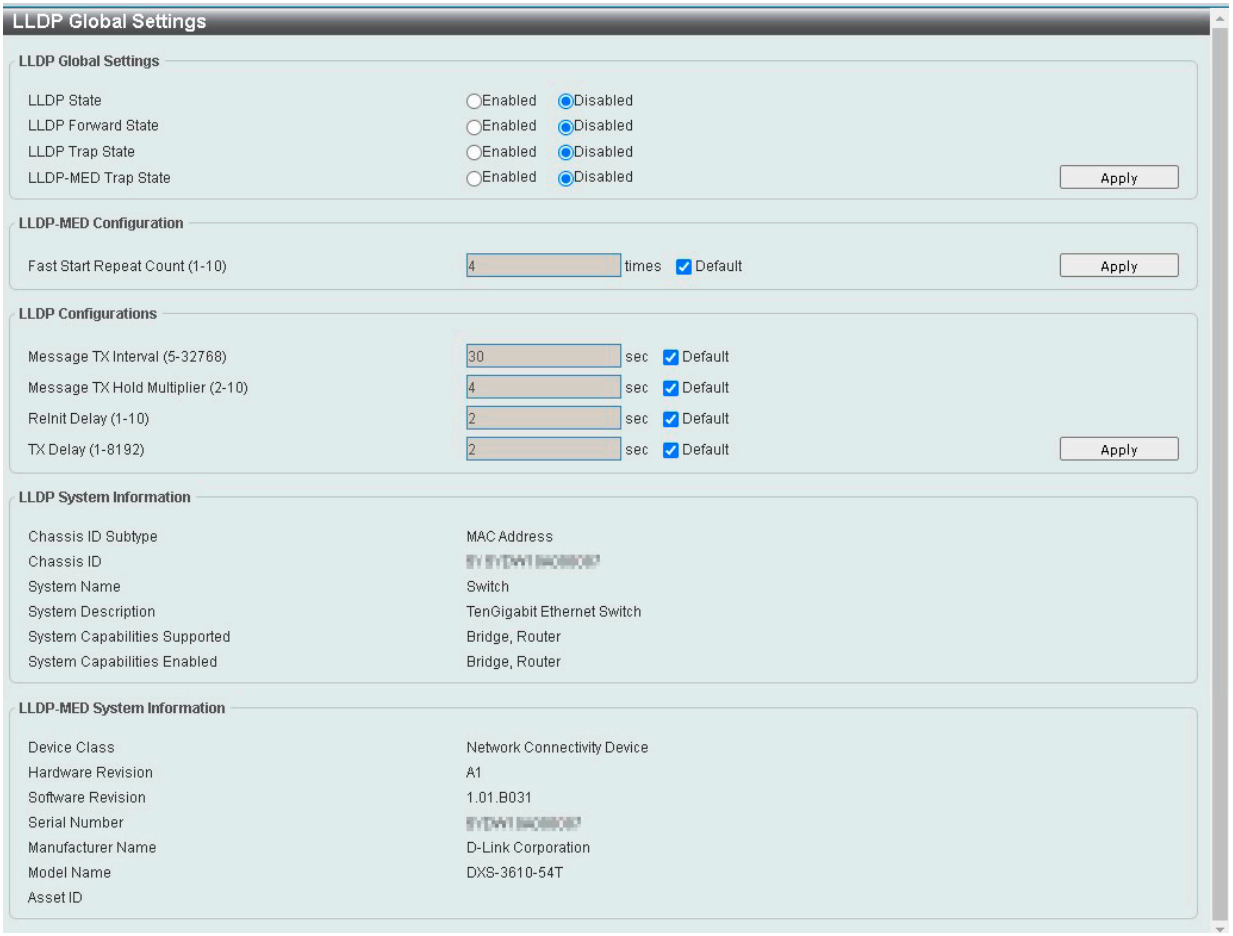


図 8-104　LLDP Global Settings 画面

画面に表示される項目：

項目	説明
LLDP Global Settings	
LLDP State	スイッチにおける LLDP 機能を有効 / 無効に設定します。
LLDP Forward State	LLDP 転送ステータスを有効 / 無効に設定します。「LLDP Status」が 無効で「LLDP Forward Sate」が有効の場合、受信した「LLDPDU」パケットは転送されます。
LLDP Trap State	LLDP トラップを有効 / 無効に設定します。
LLDP-MED Trap State	LLDP-MED トラップを有効 / 無効に設定します。
LLDP-MED Configuration	
Fast Start Repeat Count	「LLDP-MED」ファストスタートリピートカウント値を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-10
LLDP Configurations	
Message TX Interval	物理インタフェースの LLDP アドバタイズメント送信間隔を設定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：5-32768（秒）
Message TX Hold Multiplier	LLDPDU の TTL 値を計算するために使用される、LLDPDU 転送間隔に対する乗数を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：2-10

項目	説明
ReInit Delay	LLDP ポートが再初期化を行うまでの待機時間を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-10（秒）
TX Delay	インタフェースで LLDPDU を送信するまでの待機時間を指定します。転送間隔の数値の 1/4 より大きくすることはできません。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-8192（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

LLDP Port Settings（LLDP ポート設定）

LLDP ポート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。

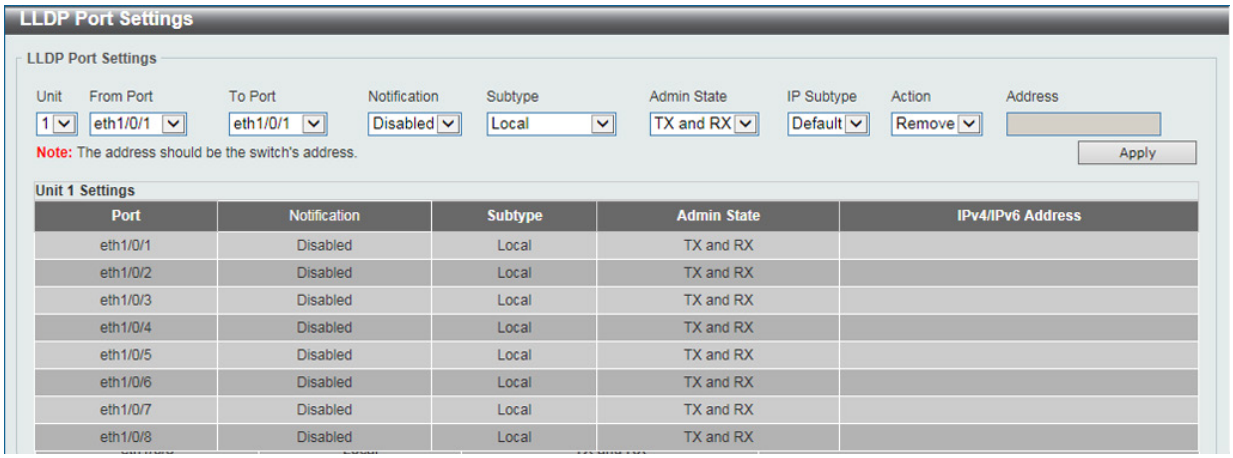


図 8-105　LLDP Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Notification	LLDP 通知を有効 / 無効に設定します。
Subtype	LLDP TLV のサブタイプを選択します。 • 選択肢：「MAC Address」「Local」
Admin State	LLDP フレームの送受信オプションを選択します。 • 「TX」- ローカル LLDP エージェントは LLDP フレーム送信のみを行います。 • 「RX」- ローカル LLDP エージェントは LLDP フレーム受信のみを行います。 • 「TX and RX」- ローカル LLDP エージェントは LLDP フレームの送受信を行います。（初期値） • 「Disabled」- ローカル LLDP エージェントは LLDP フレームの送受信を行いません。
IP Subtype	送信する IP アドレスの種類を選択します。 • 選択肢：「Default」「IPv4」「IPv6」
Action	実行する動作を選択します。 • 選択肢：「Remove（削除）」「Add（追加）」
Address	送信する IP アドレスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　入力する IPv4/IPv6 アドレスは既存の LLDP 管理 IP アドレスである必要があります。

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

LLDP 管理アドレスリストを表示します。

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

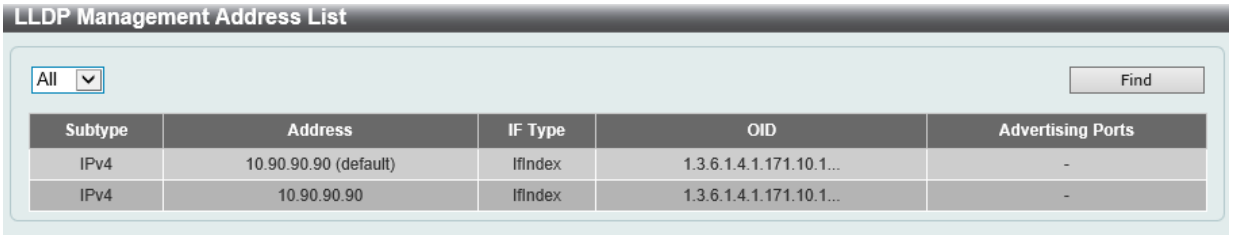


図 8-106　LLDP Management Address List 画面

画面に表示される項目：

項目	説明
Subtype	表示する LLDP 管理アドレスのサブタイプを選択します。 • 「All」- すべてのエントリを表示します。 • 「IPv4」- IPv4 アドレスを入力します。 • 「IPv6」- IPv6 アドレスを入力します。

「Find」ボタンをクリックして、LLDP 管理情報を検索します。

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

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

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

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

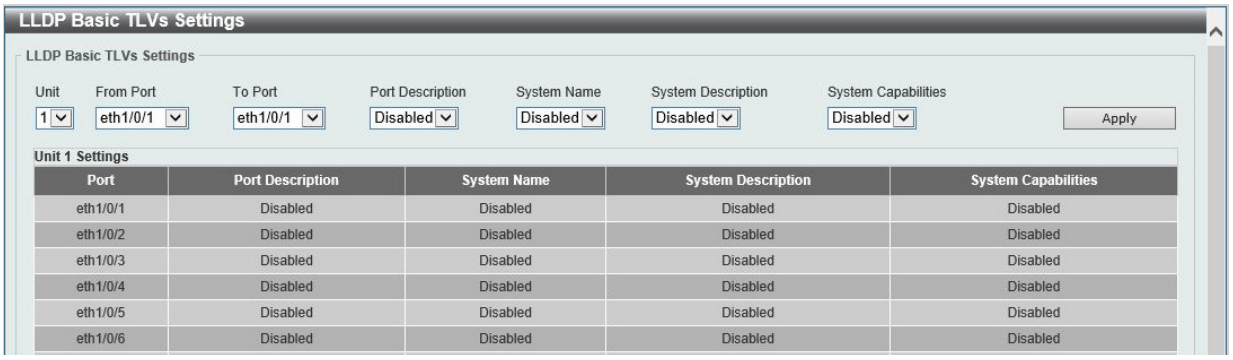


図 8-107　LLDP Basic TLVs Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Port Description	ポート説明オプションを有効 / 無効に設定します。
System Name	システム名オプションを有効 / 無効に設定します。
System Description	システム説明オプションを有効 / 無効に設定します。
System Capabilities	システム能力オプションを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

VLAN 関連の TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

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

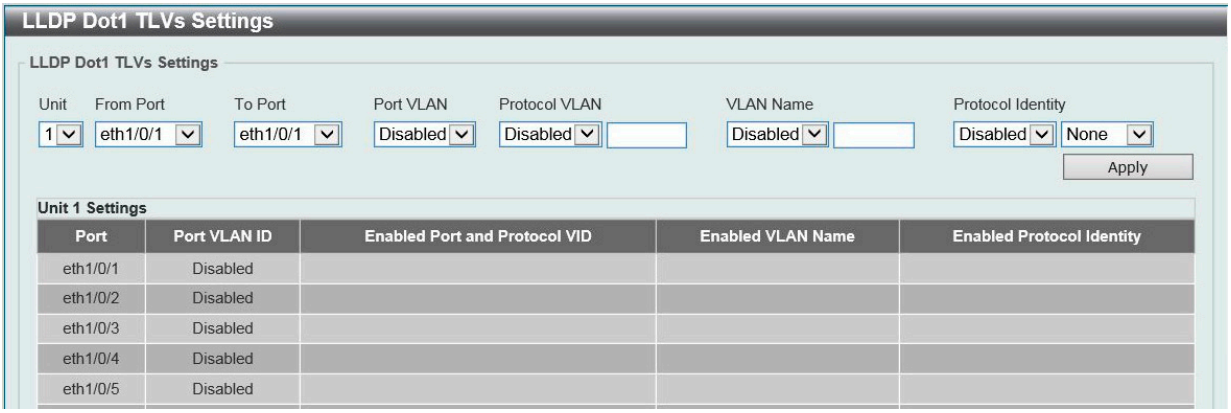


図 8-108　LLDP Dot1 TLVs Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Port VLAN	ポート VLAN ID TLV の通知を有効 / 無効に設定します。このオプションを利用すると、VLAN ブリッジポートにより、アンタグまたはプライオリティタグ付きのフレームに紐づくポート VLAN ID（PVID）を通知することが可能です。固定長のオプション TLV です。
Protocol VLAN	Port and Protocol VLAN ID（PPVID）TLV の通知を有効 / 無効に設定します。右の欄に VLAN ID を入力します。
VLAN Name	VLAN 名 TLV の通知を有効 / 無効に設定します。右の欄に VLAN 名 TLV の VLAN ID を入力します。
Protocol Identity	プロトコル識別子 TLV およびプロトコル名の通知を有効 / 無効に設定します。対象とするプロトコルを「None」「EAPOL」「LACP」「GVRP」「STP」「All」から選択します。

「Apply」ボタンをクリックして、設定内容を適用します。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

イーサネット関連の TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

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

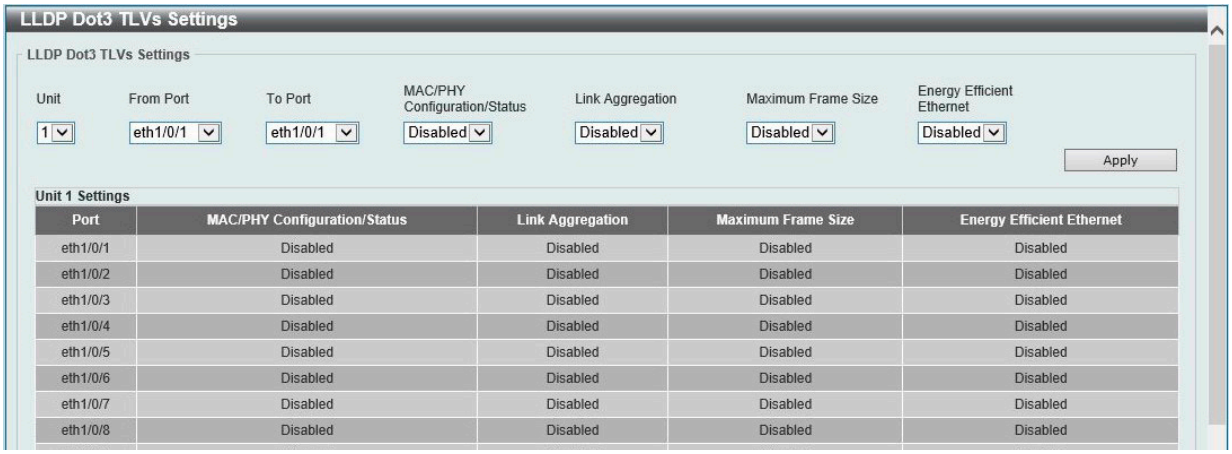


図 8-109　LLDP Dot3 TLVs Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
MAC/PHY Configuration/Status	MAC/PHY Configuration/Status TLV の通知を有効 / 無効に設定します。 （1）送信 IEEE 802.3 LAN ノードの Duplex およびビットレートの Capability、（2）送信 IEEE 802.3 LAN ノードの現在の Duplex およびビットレート設定を判別するオプションの TLV です。

項目	説明
Link Aggregation	リンクアグリゲーション TLV の通知を有効 / 無効に設定します。 リンクアグリゲーション TLV には以下の情報が含まれます。 - リンクはリンクアグリゲーション可能かどうか - リンクは現在リンクアグリゲーションに設定されているか / 集約ポートのチャンネル ID ポートがリンクアグリゲーションに設定されていない場合、ID は 0 となります。
Maximum Frame Size	最大フレームサイズ TLV の通知を有効 / 無効に設定します。 この TLV は、実装された MAC/PHY の最大フレームサイズ性能を示します。
Energy Efficient Ethernet	Energy Efficient Ethernet TLV の通知を有効 / 無効に設定します。Energy Efficient Ethernet TLV は、パケットが送信されていないときのリンクのエネルギー省電力機能を示します。

「Apply」ボタンをクリックして、設定内容を適用します。

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

LLDP-MED TLV の送信を有効または無効に設定します。

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

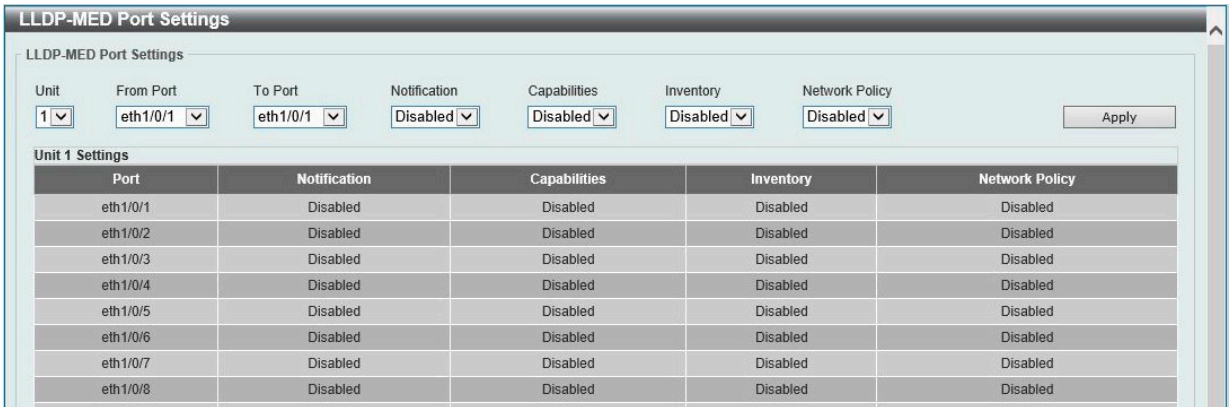


図 8-110　LLDP-MED Port Settings 画面

以下の項目が使用できます。

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Notification	「LLDP-MED notification TLV」の送信を有効 / 無効に設定します。
Capabilities	「LLDP-MED capabilities TLV」の送信を有効 / 無効に設定します。
Inventory	「LLDP-MED inventory TLV」の送信を有効 / 無効に設定します。
Network Policy	「LDP-MED network policy TLV」の送信を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

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

LLDP-DCBX（Data Center Bridging Exchange プロトコル）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。

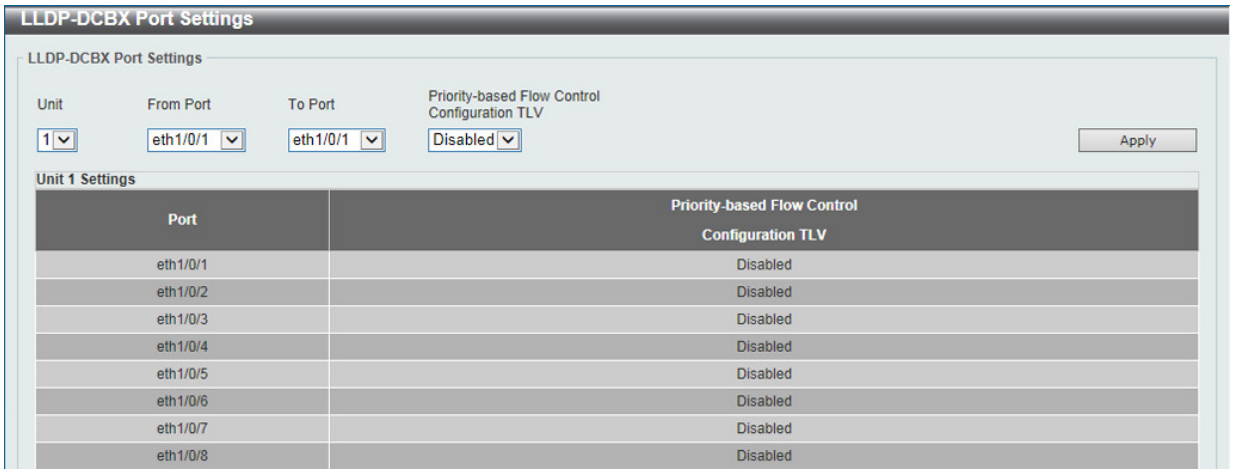


図 8-111　LLDP-DCBX Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Priority-based Flow Control Configuration TLV	「Priority-based Flow Control」(PFC) Configuration TLV の送信を有効 / 無効に設定します。 PFC TLV は、ブリッジポートが PFC の現在の動作ステータスと許容ビットをアドバタイズできるようにするオプションの TLV です。

「Apply」ボタンをクリックして、設定内容を適用します。

LLDP Statistics Information（LLDP 統計情報）

スイッチにおける LLDP 統計情報を参照します。

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

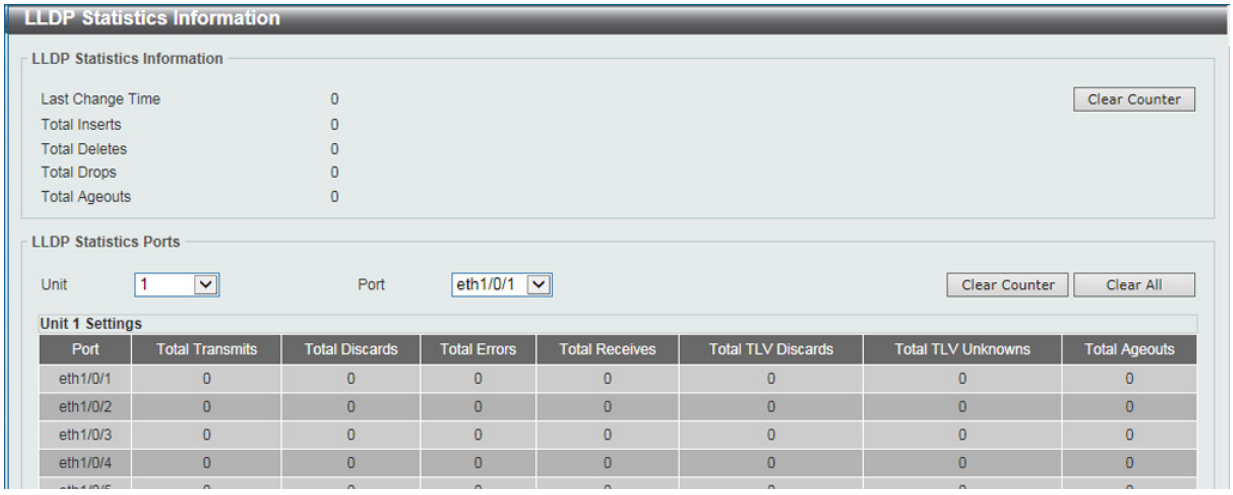


図 8-112　LLDP Statistics Information 画面

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

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

外向きの LLDP 通知に含まれる情報を表示します。

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

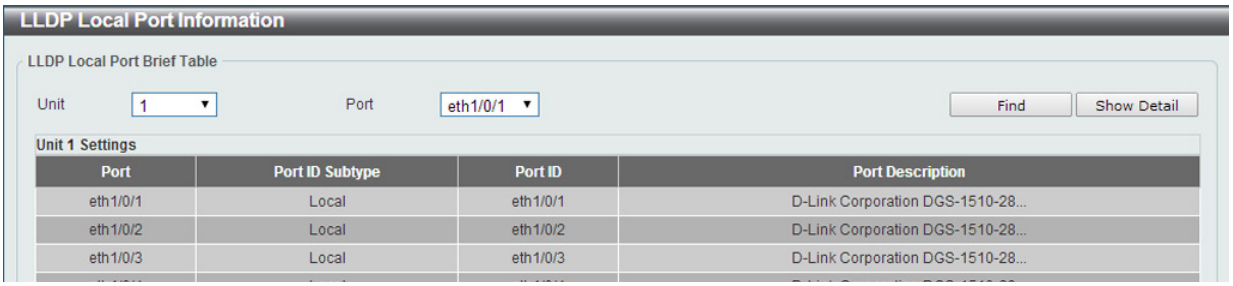


図 8-113　LLDP Local Port Information 画面

画面に表示される項目：

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

「Find」ボタンをクリックして、指定ポートのエントリを表示します。

詳細情報の参照

「Show Detail」ボタンをクリックし、以下の画面を表示します。

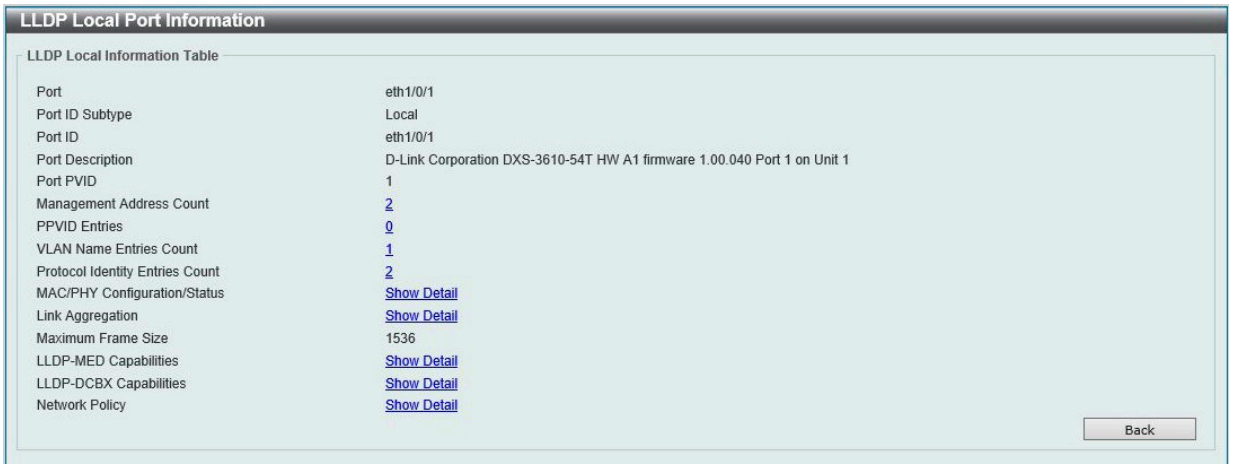


図 8-114　LLDP Local Port Information（Show Detail）画面

各パラメータの詳細の参照

各項目の「Show Detail」リンクをクリックすると、画面下部に情報が表示されます。

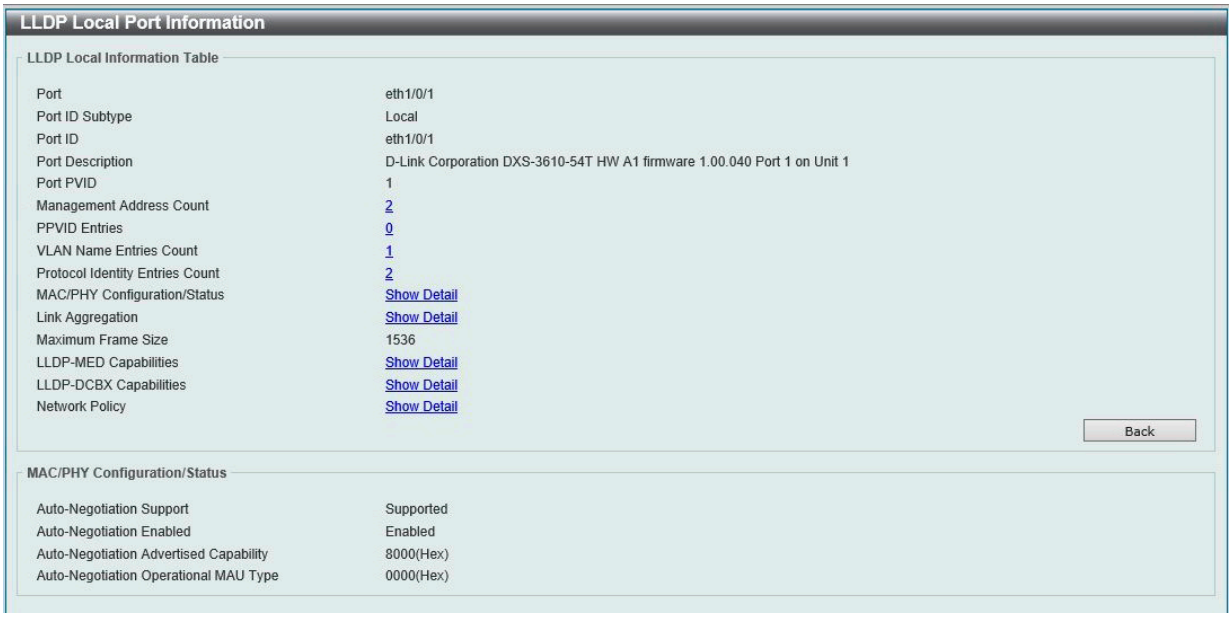


図 8-115　LLDP Local Port Information - MAC/PHY Configuration/Status 画面

前の画面に戻るには、「Back」ボタンをクリックします。

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

Neighbor から学習した LLDP 情報を表示します。

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

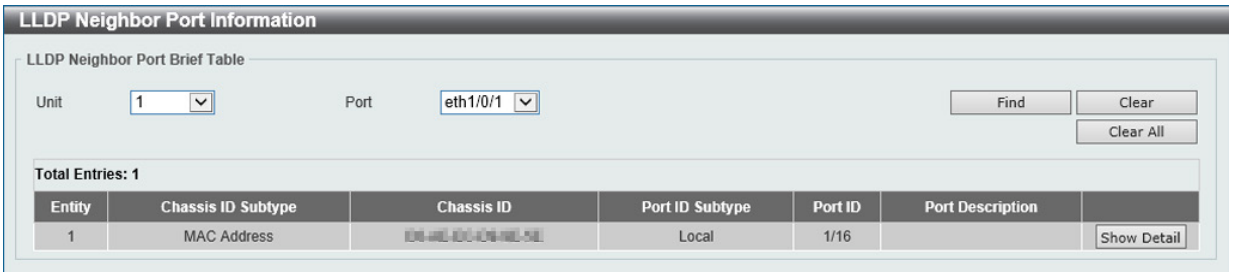


図 8-116　LLDP Neighbor Port Information 画面

画面に表示される項目：

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

「Find」ボタンをクリックして、指定ポートのエントリを表示します。
「Clear」ボタンをクリックして、特定のポート情報をクリアします。
「Clear All」ボタンをクリックして、全てのポート情報をクリアします。

「Show Detail」をクリックして指定ポートの詳細情報を表示します。

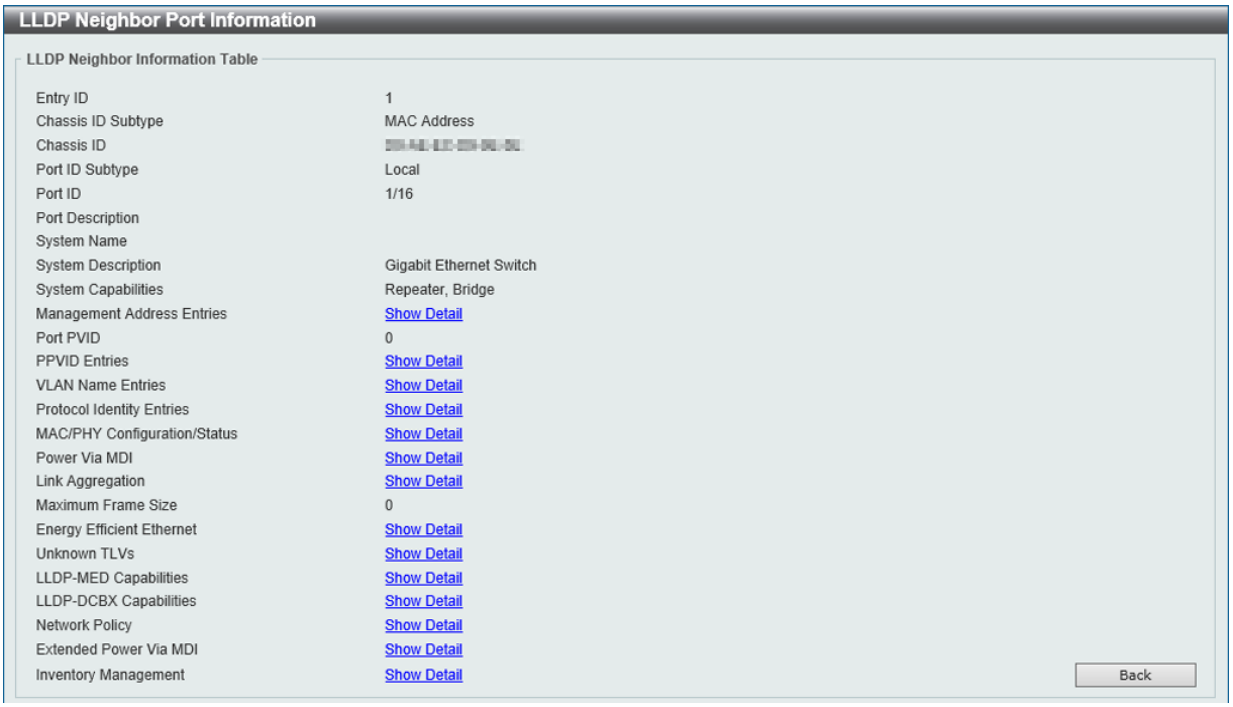


図 8-117　LLDP Neighbor Port Information（Show Detail）画面

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が表示されます。（例 :MAC/PHY Configuration/Status）

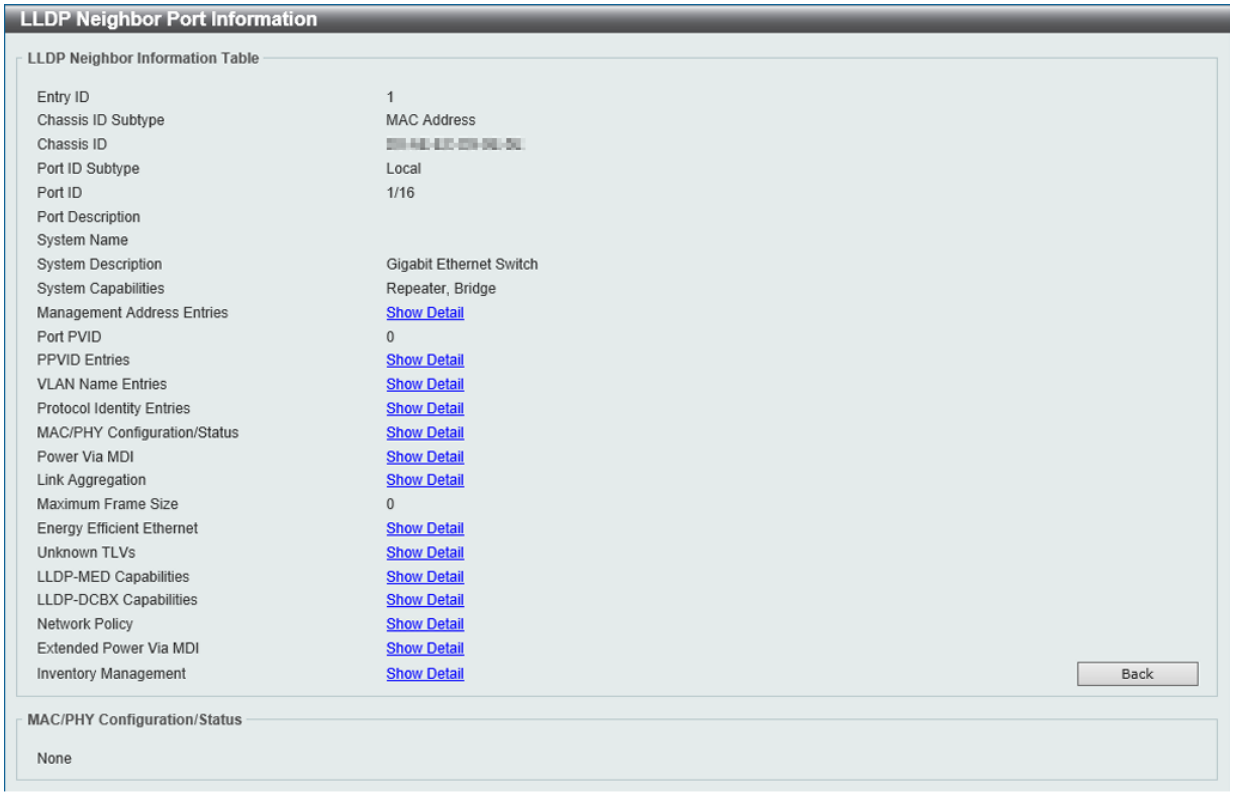


図 8-118　LLDP Neighbor Port Information（Show Detail - MAC/PHY Configuration/Status）画面

前の画面に戻るには、「Back」ボタンをクリックします。

第 9 章　L3 Features（レイヤ 3 機能の設定）

L3 Features メニューを使用し、本スイッチにレイヤ 3 機能を設定することができます。

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

サブメニュー	説明
ARP（ARP 設定）	ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
Gratuitous ARP（Gratuitous ARP 設定）	Gratuitous ARP の設定を行います。
IPv6 Neighbor（IPv6 ネイバ設定）	IPv6 ネイバ設定を行います。
Interface（インタフェース設定）	IP インタフェース設定を行います。
UDP Helper（UDP ヘルパー）	IP 転送プロトコルの設定を行います。本機能は指定の UDP サービスタイプのパケットの転送を有効にします。また UDP ブロードキャストパケットを転送するターゲットアドレスを指定します。
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定）	本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。
IPv4 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 汎用プレフィックス）	VLAN インタフェース IPv6 汎用プレフィックスの設定を行います。
IP Tunnel Settings（IP トンネル設定）（EI モードのみ）	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 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）	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 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。
ISIS（Intermediate System to Intermediate System）（EI 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（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 パケットよりも優先されます。

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

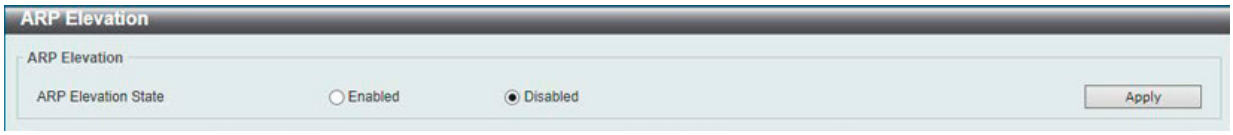


図 9-1　ARP Elevation 画面

画面に表示される項目：

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

「Apply」ボタンをクリックして、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。

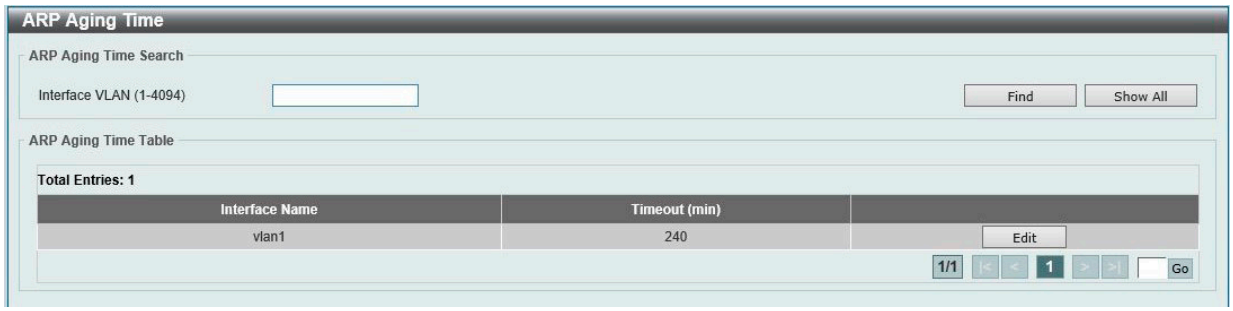


図 9-2　ARP Aging Time 画面

画面に表示される項目：

項目	説明
Interface VLAN	インタフェース VLAN ID を入力します。 • 設定可能範囲：1-4094
Timeout	ARP エージングタイムアウト値（分）を入力します。この時間が経過すると、エントリはテーブルから削除されます。

「Find」ボタンをクリックして、指定 VLAN に基づいてエントリを検索します。
「Show All」ボタンをクリックして、すべての ARP エージングタイムエントリを表示します。

ARP エージングタイムの編集

編集するエントリの「Edit」ボタンをクリックし、タイムアウト値を設定します。「Apply」ボタンをクリックして、設定内容を適用します。

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

Static ARP（スタティック ARP 設定）

スタティックエントリを ARP テーブルに定義します。

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

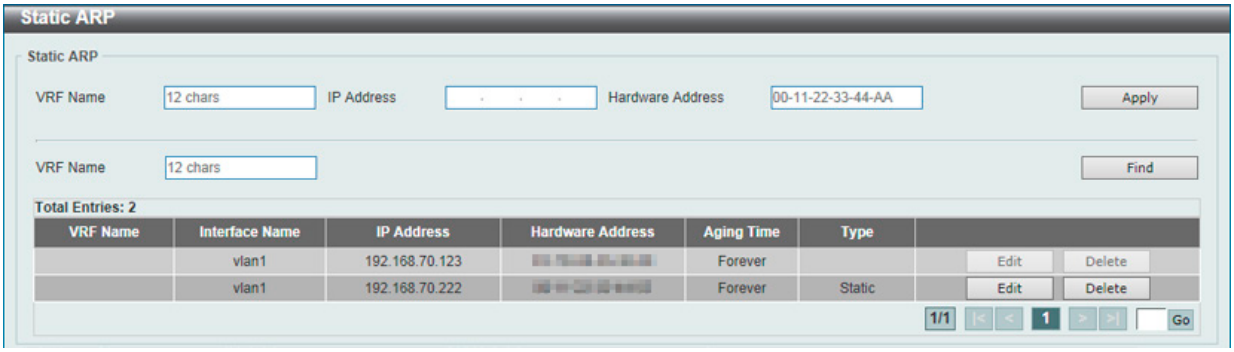


図 9-3　Static ARP 画面

画面に表示される項目：

Static ARP Setting

項目	説明
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
IP Address	MAC アドレスに紐づける IP アドレスを設定します。
Hardware Address	IP アドレスに紐づける MAC アドレスを設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

スタティック ARP テーブル

項目	説明
VRF Name（EI モードのみ）	検索する VRF インスタンス名入力します。（12 文字以内）

「Find」ボタンをクリックして、指定した VRF に基づきエントリを検出します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。

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

注意　スタティック ARP エントリの最大数は 512 です。

Proxy ARP（プロキシ ARP）

プロキシ ARP の設定を参照および編集します。

プロキシ ARP 機能は、他のデバイスへ送信される ARP リクエストに対し、識別情報（IP および MAC アドレス）を元の ARP 応答者の代わりに応答する機能です。これにより、スタティックのルーティングやデフォルトゲートウェイを設定せずに、目的の宛先にパケットをルートすることが可能です。ホスト（通常レイヤ 3 スイッチ）は別の機器宛てのパケットに応答します。

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

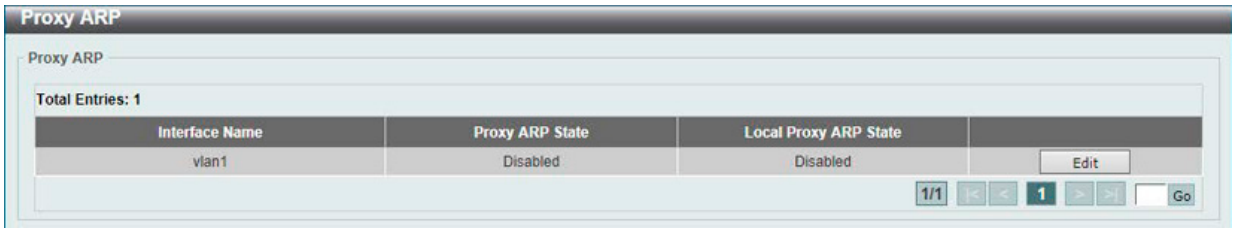


図 9-4　Proxy ARP 画面

画面に表示される項目：

項目	説明
Proxy ARP State	プロキシ ARP を有効 / 無効に設定します。
Local Proxy ARP State	ローカルプロキシ ARP を有効 / 無効に設定します。 ローカルプロキシ ARP 機能は、送信元 IP と宛先 IP が同じインタフェースにある場合に、スイッチがプロキシ ARP に返答します。

「Edit」ボタンを選択して、特定エントリの設定を編集します。
「Apply」ボタンをクリックして、設定内容を適用します。

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

ARP Table（ARP テーブルの参照）

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。

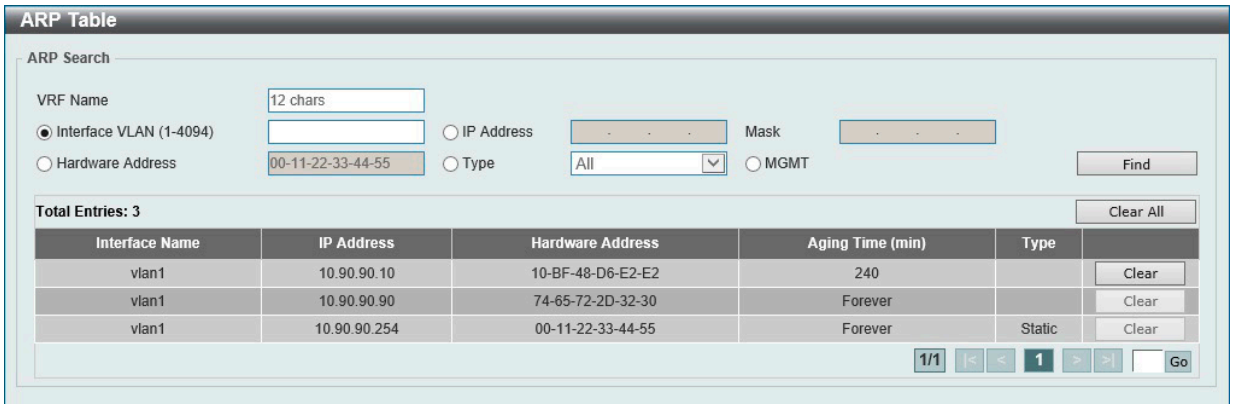


図 9-5　ARP Table 画面

画面に表示される項目：

項目	説明
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Interface VLAN	表示するインタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094
IP Address	表示する IP アドレスを入力します。
Mask	上記 IP アドレスのマスクを指定します。
Hardware Address	表示する MAC アドレスを入力します。
Type	表示する ARP の種類を指定します。 • 選択肢：「All」「Dynamic」
MGMT	管理ポートについての情報を表示します。

「Find」ボタンをクリックして、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」ボタンをクリックして、テーブル上のエントリをすべて消去します。
削除するエントリの「Clear」ボタンをクリックして、エントリを削除します。

Gratuitous ARP（Gratuitous ARP 設定）

Gratuitous ARP リクエストパケットは、送信元 / 宛先 IP アドレスが送信元デバイスのアドレスに設定され、宛先 MAC アドレスがブロードキャストアドレスとなっている ARP リクエストパケットです。通常、Gratuitous ARP リクエストパケットを使用して、IP アドレスが他のデバイスと競合していないかどうかを検出したり、インタフェースに接続されたホストの ARP キャッシュエントリを事前ロードまたは再構成したりします。

Gratuitous ARP のグローバル設定を行います。

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

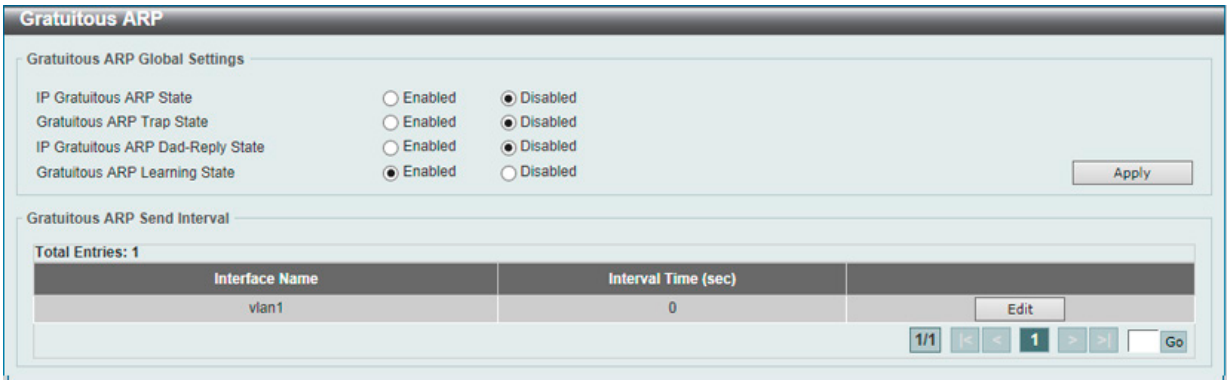


図 9-6　Gratuitous ARP 画面

画面に表示される項目：

項目	説明
IP Gratuitous ARP State	ARP キャッシュテーブルの Gratuitous ARP パケットの習得を有効 / 無効に設定します。
Gratuitous ARP Trap State	Gratuitous ARP トラップ を有効 / 無効に設定します。
IP Gratuitous ARP Dad-Reply State	IP Gratuitous ARP Dad-reply を有効 / 無効に設定します。
Gratuitous ARP Learning State	Gratuitous ARP 学習を有効 / 無効に設定します。システムは通常、ARP 応答パケットや、スイッチの IP アドレスに対応する MAC アドレスを問い合せるための通常の ARP リクエストパケットからのみ ARP エントリを学習します。このオプションを使用すると、受信した Gratuitous ARP パケットに基づく ARP エントリの学習を有効 / 無効に設定します。Gratuitous ARP パケットは、送信元アドレスと問合せ IP アドレスが同一のパケットです。

「Apply」ボタンをクリックして、設定内容を適用します。

「Edit」をクリックして指定エントリを編集します。以下の項目を使用して設定します。

項目	説明
Gratuitous ARP Send Interval	
Interval Time(sec)	Gratuitous ARP を送信する間隔（秒）を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6 Neighbor（IPv6 ネイバ設定）

スイッチの IPv6 ネイバ設定を行います。

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

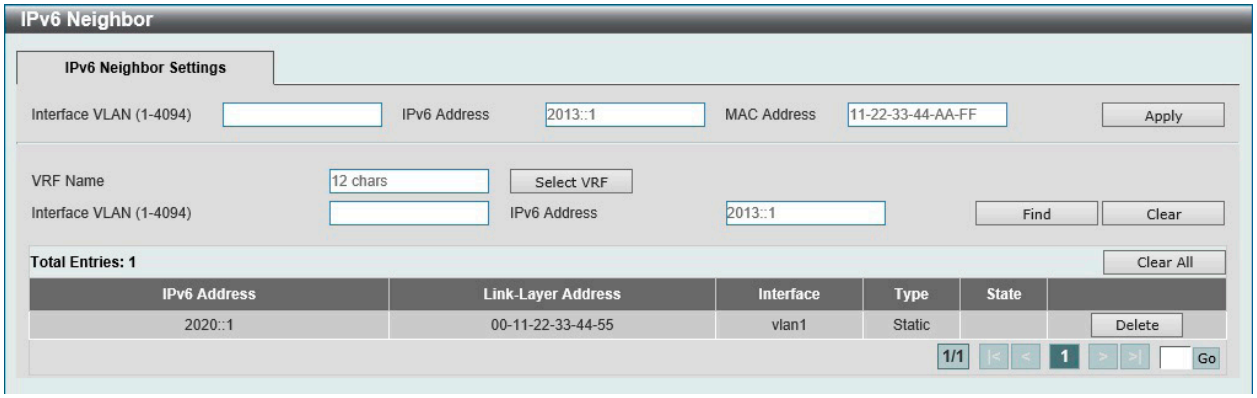


図 9-7　IPv6 Neighbor 画面

画面に表示される項目：

項目	説明
Interface VLAN	IPv6 Neighbor のインタフェース VLAN を指定します。 • 設定可能範囲：1-4094
IPv6 Address	IPv6 アドレスを入力します。
MAC Address	MAC アドレスを指定します。
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。

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。

ダイナミックエントリの削除

指定インタフェースのダイナミックエントリ情報を削除するには、「Clear」ボタンをクリックします。
すべてのダイナミックエントリ情報を削除するには、「Clear All」ボタンをクリックします。

エントリの削除

該当エントリの「Delete」ボタンをクリックします。

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

Interface（インタフェース設定）

スイッチの IP インタフェース設定を行います。

注意　Vlan Interface を経由して Mgmt 0 の IP アドレス宛に通信を行う事はできません。

注意　Mgmt Port の MAC Address は System MAC を使用し、Vlan 1 と重複するため、同じ スイッチに接続して Mgmt Port と Vlan 1 は使用できません。

IPv4 Interface（IPv4 インタフェース）

スイッチの IP インタフェース設定を行います。

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



図 9-8　IPv4 Interface 画面

スイッチの現在の IP インタフェース設定が表示されます。

項目	説明
Interface VLAN	設定、表示するインタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094

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

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

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。

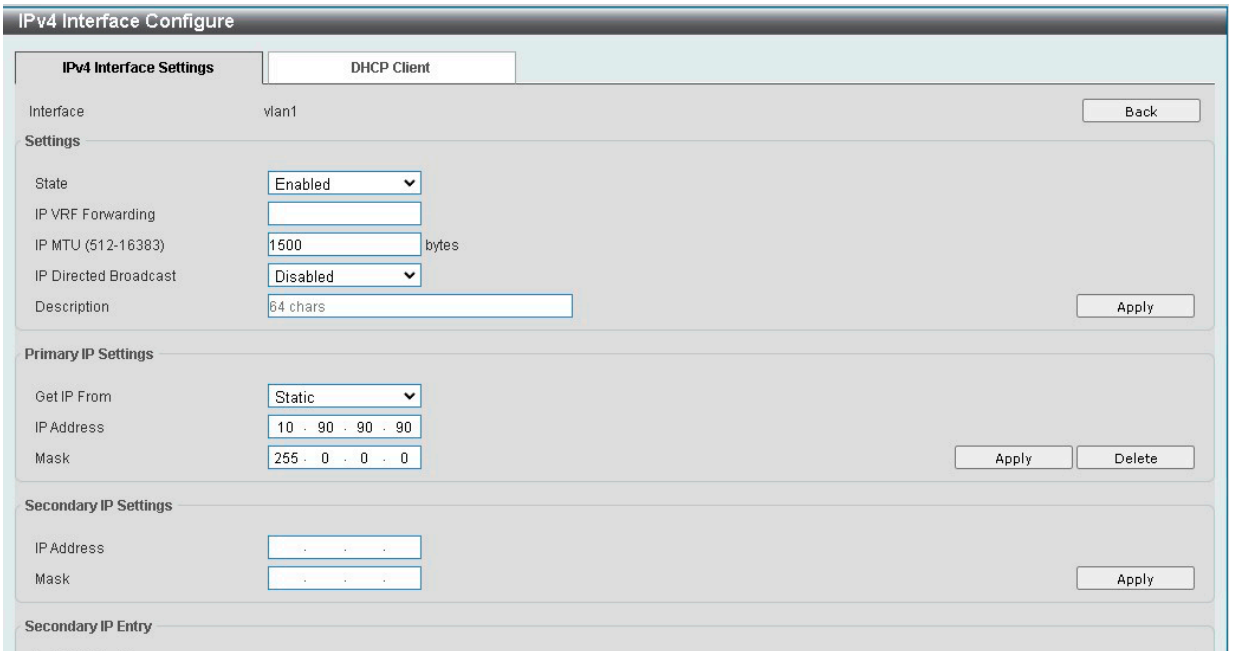


図 9-9　IPv4 Interface Configure 画面 - IPv4 Interface Settings タブ

画面に表示される項目：

項目	説明
Settings	
State	該当エントリの IPv4 インタフェースをグローバルに有効 / 無効にします。
IP VRF Forwarding （EI モードのみ）	転送される VRF インスタンスの名前を入力します。

項目	説明
IP MTU	MTU 値を入力します。 • 設定可能範囲：512-16383（bytes） • 初期値：1500（bytes）
IP Directed Broadcast （EI モードのみ）	IP インタフェースの IP ディレクティッドブロードキャストの状態を有効 / 無効に設定します。 受信した IP ディレクティッドブロードキャストパケットについて、宛先ネットワークが直接スイッチに接続されている場合、そのパケットを転送するように設定します。
Description	エントリの説明を入力します。（64 文字以内）
Primary IP Settings	
Get IP From	IP アドレスの設定方法を選択します。 •「Static」- インタフェースに設定する IPv4 アドレスを手動で設定します。 •「DHCP」- ローカルネットワーク上の DHCP サーバから自動的に IPv4 情報を取得します。
IP Address	IPv4 インタフェースに割り当てる IPv4 アドレスを入力します。
Mask	IPv4 インタフェースに割り当てるサブネットマスクを入力します。
Secondary IP Settings	
IP Address	セカンダリインタフェースの IPv4 アドレスを設定します。
Mask	セカンダリインタフェースのサブネットマスクを設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。
「Delete」ボタンをクリックして、指定エントリを削除します。
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。

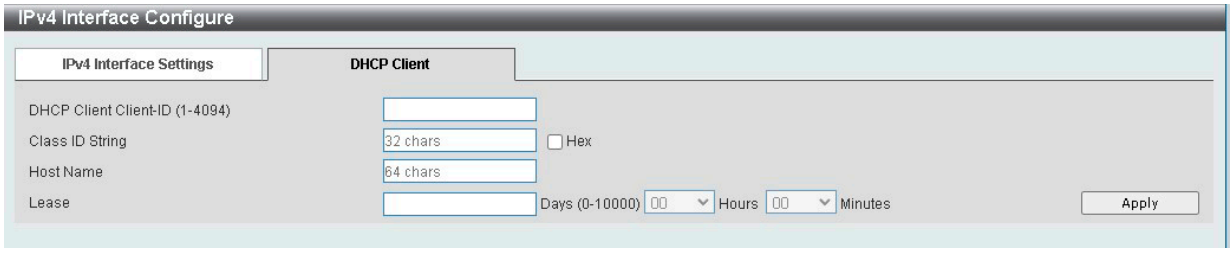


図 9-10　IPv4 Interface Configure 画面 - DHCP Client タブ

画面に表示される項目：

項目	説明
DHCP Client Client-ID	DHCP クライアント ID を入力します。この ID は VLAN インタフェースを指定します。該当インタフェースの 16 進数 MAC アドレスは、DISCOVER メッセージと一緒に送信されるクライアント ID として使用されます。 • 設定可能範囲：1-4094
Class ID String	クラス識別名を入力します（32 文字以内）。「Hex」にチェックを入れると 16 進数方式（64 文字以内）になります。 DHCP DISCOVER メッセージに含まれるオプション 60 の値として使用されます。
Host Name	ホスト名を入力します。（64 文字以内）DHCP DISCOVER メッセージと一緒に送信されるホスト名オプションの値です。
Lease	DHCP サーバから割り振られる IP アドレスのリース時間を指定します。オプションで時間と分を指定することもできます。 • 設定可能範囲：0-10000（日）

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6 Interface（IPv6 インタフェース）

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



図 9-11　IPv6 Interface 画面

以下の項目が表示されます。

IPv6 Optimistic DAD

項目	説明
IPv6 Optimistic DAD State	IPv6 Optimistic Duplicate Address Detection（DAD）を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6 Interface

項目	説明
Interface VLAN	設定、表示する IPv6 インタフェースの VLAN ID を入力します。 ・ 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show Detail」ボタンをクリックして、IPv6 インタフェースエントリの詳細を表示、設定します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

注意　DAD により、自身の NS を受信した場合、該当の IPv6 Address がアップしません。

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。

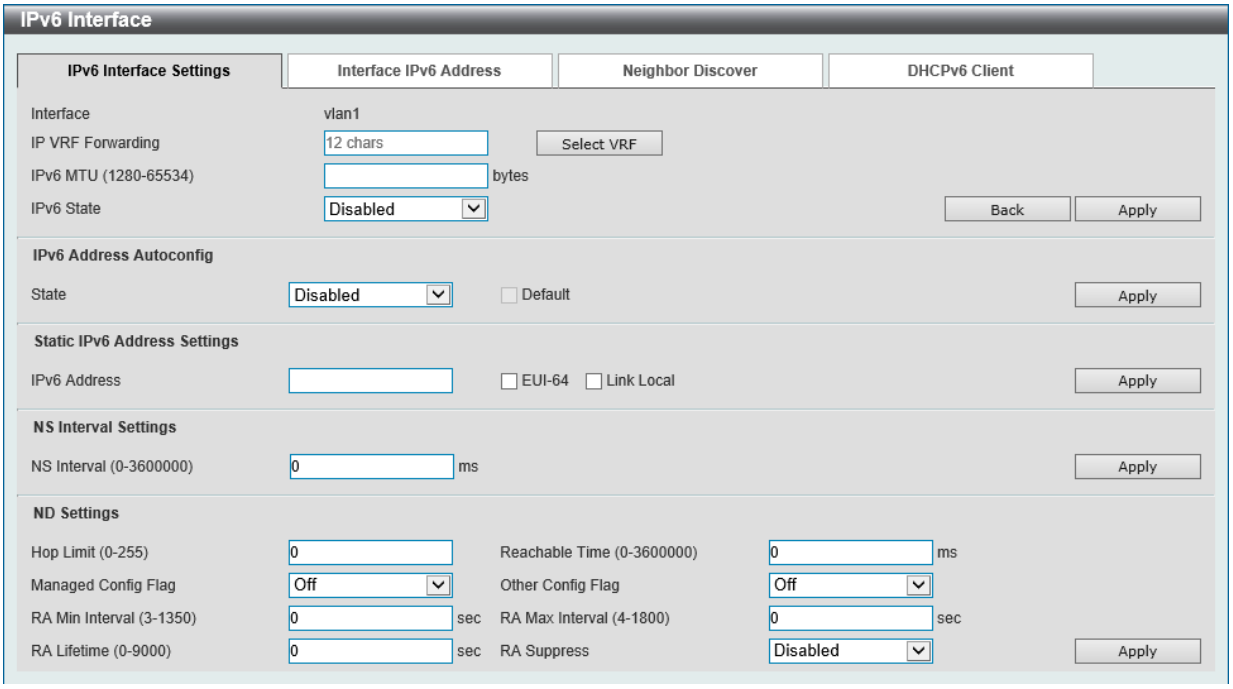


図 9-12　IPv6 Interface（IPv6 Interface Settings）画面

画面に表示される項目：

項目	説明
Interface	
IP VRF Forwarding （EI モードのみ）	転送される VRF インスタンスの名前を入力します。「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
IPv6 MTU	使用する IPv6 レイヤの MTU 値を入力します。RA メッセージ内でアドバタイズされる MTU の値です。 • 設定可能範囲：1280 - 65534（Bytes） • 初期値：1500（Bytes）
IPv6 State	該当エントリの IPv6 インタフェースをグローバルに有効 / 無効にします。
IPv6 Address Autoconfig	
State	ステートレス自動設定を使用した IPv6 アドレスの自動設定を有効 / 無効に設定します。「Default」に指定すると、このインタフェースでデフォルトルータが選択されている場合、そのデフォルトルータを使用してデフォルトルートがインストールされます。このオプションは 1 つのインタフェースのみで指定可能です。
Static IPv6 Address Settings	
IPv6 Address	IPv6 インタフェースに割り当てる IPv6 アドレスを入力します。 •「EUI-64」- EUI-64 インタフェース ID を使用してインタフェースの IPv6 アドレスを設定します。 •「Link Local」- IPv6 インタフェースにリンクローカルアドレスを使用します。
NS Interval Settings	
NS Interval	Neighbor Solicitation（NS）間隔を指定します。0 に指定された場合、1 秒間隔となり、RA メッセージには 0（未指定）の値がアドバタイズされます。 • 設定可能範囲：0-3600000（ミリ秒）（1000 の倍数）
ND Settings	
Hop Limit	ホップリミットを指定します。システムから送信される IPv6 パケットも、最初のホップリミット値としてこの値を使用します。 • 設定可能範囲：0-255
Reachable Time	到達可能時間を指定します。「0」に指定すると、1200 秒となり、RA メッセージでは 0（未指定）の値がアドバタイズされます。到達可能時間は、IPv6 ノードが、隣接しているノードの到達可否を判断する時間です。 • 設定可能範囲：0-3600000（ミリ秒）
Managed Config Flag	Managed Config Flag オプションを有効 / 無効に設定します。このフラグが有効な RA を受信すると、ネイバホストはステートフル設定プロトコルを使用して IPv6 アドレスを取得します。
Other Config Flag	Other Config Flag オプションを有効 / 無効に設定します。本設定を有効にすると、接続ホストはステートフル設定プロトコルを使用して、IPv6 アドレス以外の自動設定情報を取得します。
RA Min Interval	RA 通知の送信間隔の最小時間を入力します。最大値の 3/4 より大きくしないでください。 • 設定可能範囲：3-1350（秒）
RA Max Interval	RA 通知の送信間隔の最大時間を入力します。 • 設定可能範囲：4-1800（秒）
RA Lifetime	RA の有効期間を指定します。ホストは受信した RA に含まれる有効期間の値に基づき、送信元ルータをデフォルトルータとして使用します。 • 設定可能範囲：0-9000（秒）
RA Suppress	RA 抑制機能を有効 / 無効に設定します。

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

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

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。

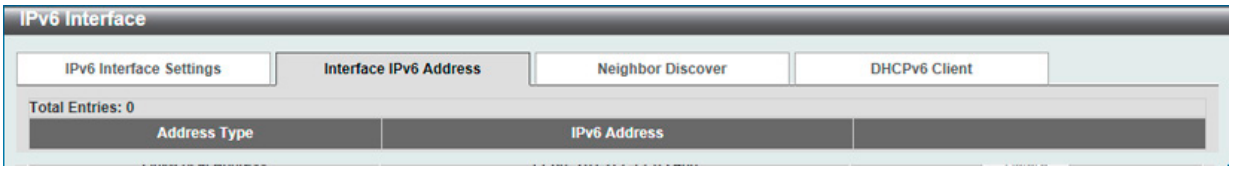


図 9-13　IPv6 Interface（Interface IPv6 Address）画面

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 9-14　IPv6 Interface（Neighbor Discover）画面

「Edit」をクリックすると、以下の項目を編集することができます。

項目	説明
Preferred Life Time	推奨有効期間を入力します。 • 設定可能範囲：0-4294967295（秒）
Valid Life Time	有効期間を入力します。 • 設定可能範囲：0-4294967295（秒）
Link Flag	リンクフラグ機能の有効 / 無効を選択します。
Autoconfig Flag	自動設定フラグ機能の有効 / 無効を選択します。

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6 インタフェースの編集（DHCPv6 Client タブ）

指定エントリの「Show Detail」ボタンをクリックして、「DHCPv6 Client」タブを表示します。

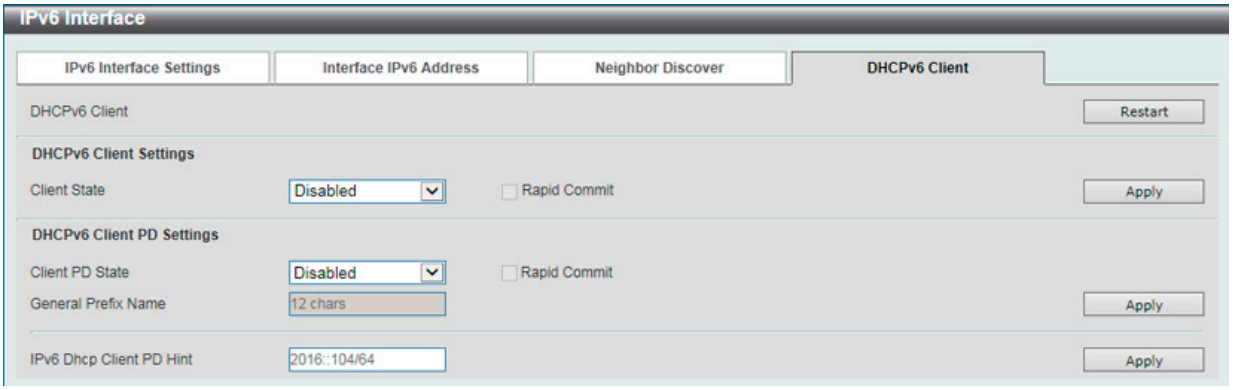


図 9-15　IPv6 Interface（DHCPv6 Client）画面

画面に表示される項目：

項目	説明
DHCPv6 Client	
DHCPv6 Client	「Restart」をクリックすると、DHCPv6 クライアントサービスを再始動します。
DHCPv6 Client Settings	
Client State	DHCPv6 クライアントを有効 / 無効に設定します。アドレス配布では通常 4 個のメッセージ交換を行いますが、「Rapid Commit」にチェックを入れると、2 個のメッセージ交換を実行します。rapid-commit オプションは Solicit メッセージに含まれます。

項目	説明
DHCPv6 Client PD Settings	
Client PD State	指定インタフェースを介して Prefix Delegation (PD) をリクエストする DHCPv6 クライアントプロセスを有効 / 無効に設定します。アドレス配布では通常 4 個のメッセージ交換を行いますが、「Rapid Commit」にチェックを入れると、2 個のメッセージ交換を実行します。rapid-commit オプションは Solicit メッセージに含まれます。
General Prefix Name	IPv6 汎用プレフィックス名（12 文字以内）を指定します。
IPv6 DHCP Client PD Hint	ヒントとしてメッセージで送信される IPv6 プレフィックスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

Loopback Interface（ループバックインタフェース設定）

ループバックインタフェースを設定します。ループバックインタフェースは論理インタフェースであり、常に UP 状態となります。

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



図 9-16　Loopback Interface 画面

画面に表示される項目：

項目	説明
Interface Loopback	ループバックするインタフェース ID を入力します。 • 設定可能範囲：1-8

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

ループバックインタフェースの編集（Edit）

「Edit」（編集）ボタンをクリックして、以下の画面を表示します。

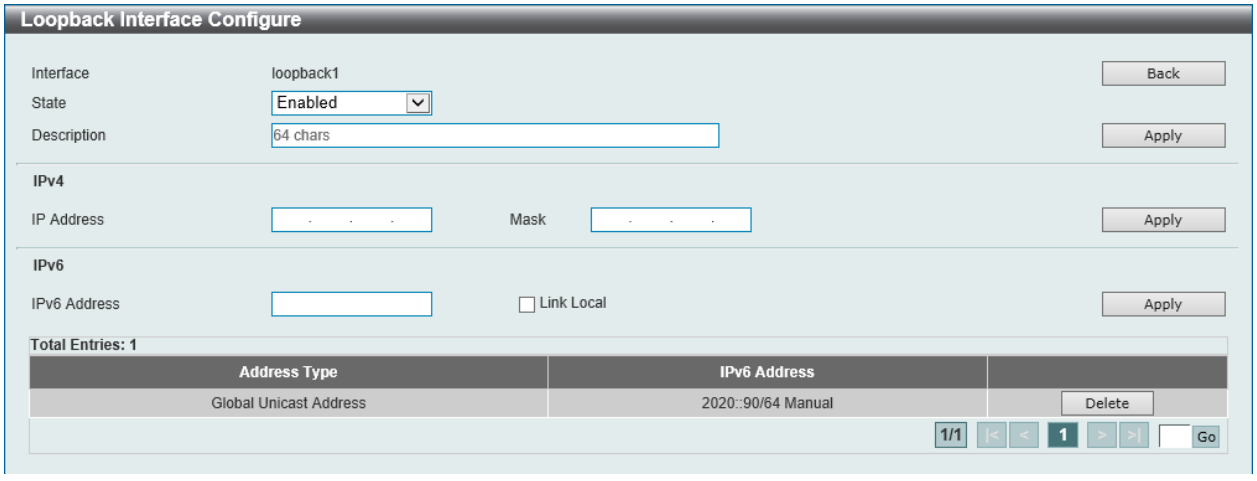


図 9-17　Loopback Interface Settings（Edit）- Loopback Interface Configure 画面

画面に表示される項目：

項目	説明
State	本ループバックインタフェースを有効 / 無効に設定します。
Description	本ループバックインタフェースの説明（64 文字以内）を指定します。
IPv4	
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。

項目	説明
IPv6	
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。

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

インタフェースの削除
「Delete」ボタンをクリックして、指定エントリを削除します。

Null Interface（Null インタフェース）

Null インタフェースを設定します。

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

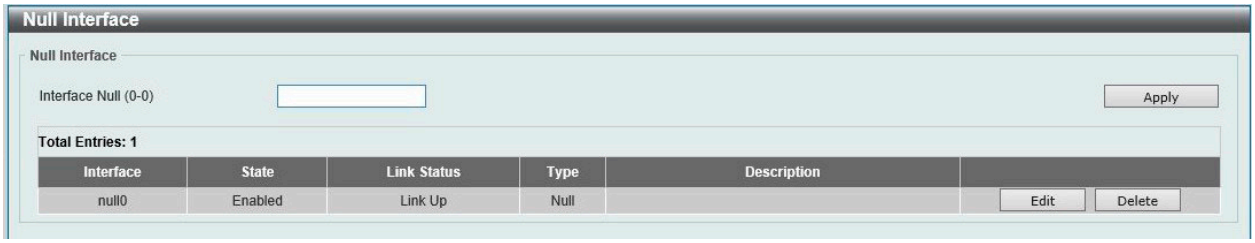


図 9-18　Null Interface 画面

画面に表示される項目：

項目	説明
Interface Null	Null インタフェース ID（0）を指定します。「0」のみ指定可能です。
Description	「Edit」をクリックし Null インタフェースの概要を入力します。（64 文字以内）

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

注意　Connected への Null0 経路は参照されません

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。

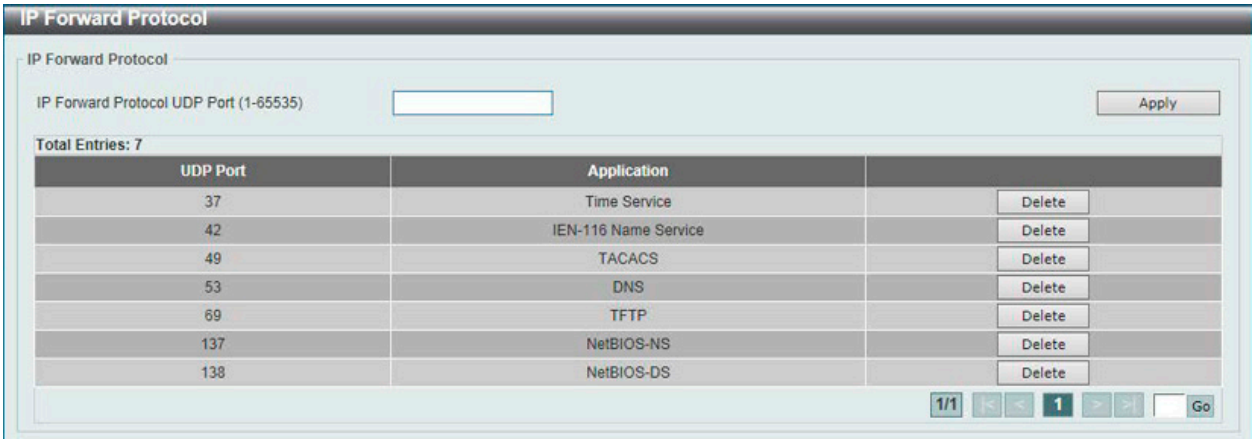


図 9-19　IP Forward Protocol 画面

画面に表示される項目：

項目	説明
IP Forward Protocol UDP Port	転送する UDP サービスの宛先ポートを指定します。 • 設定可能範囲：1-65535

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

IP Helper Address（IP ヘルパーアドレス）

本項目では UDP ブロードキャストパケットを転送するターゲットアドレスの追加 / 削除を指定します。本機能は IP アドレスがアサインされた受信インタフェースのみ有効です。システムは以下の条件を満たす場合のみパケットを転送します。

- 宛先 MAC アドレスがブロードキャストアドレスである。
- 宛先 IP アドレスがオールワンブロードキャストである。
- パケットが IPv4 UDP パケットである。
- 「IP TTL 値」が「2」以上である。

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



図 9-20　IP Helper Address 画面

画面に表示される項目：

項目	説明
Interface VLAN	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
VRF State (EI モードのみ)	VRF の状態を指定します。 • 選択肢：「True」「False」
VRF Name (EI モードのみ)	VRF インスタンス名を入力します（12 文字以内）。「Global」を指定するとグローバル VRF インスタンスを使用します。
Helper Address	UDP ブロードキャストパケットの転送先 IPv4 アドレスを指定します。

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

IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート設定）

IPv4 スタティックおよびデフォルトルートの設定を行います。

IPv4 スタティックルートが設定されると、スイッチによってネクストホップルータに ARP リクエストパケットが送信されます。スイッチに対しネクストホップから ARP の応答が返されると、ルートが有効になります。ただし、ARP エントリが既に存在している場合には、ARP 要求は送信されません。

スイッチはフローティングスタティックルートをサポートしています。ユーザは、異なるネクストホップを持つ代替のスタティックルートを作成することができます。この 2 個目のネクストホップデバイスのルートは、プライマリスタティックルートがダウンした場合のバックアップ用スタティックルートであると見なされます。プライマリルートが失われた場合、バックアップルートがアクティブになり、トラフィックの転送を開始します。

本スイッチのフォワーディングテーブル内のエントリは、IP アドレス、サブネットマスクおよびゲートウェイを使用して作成します。

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

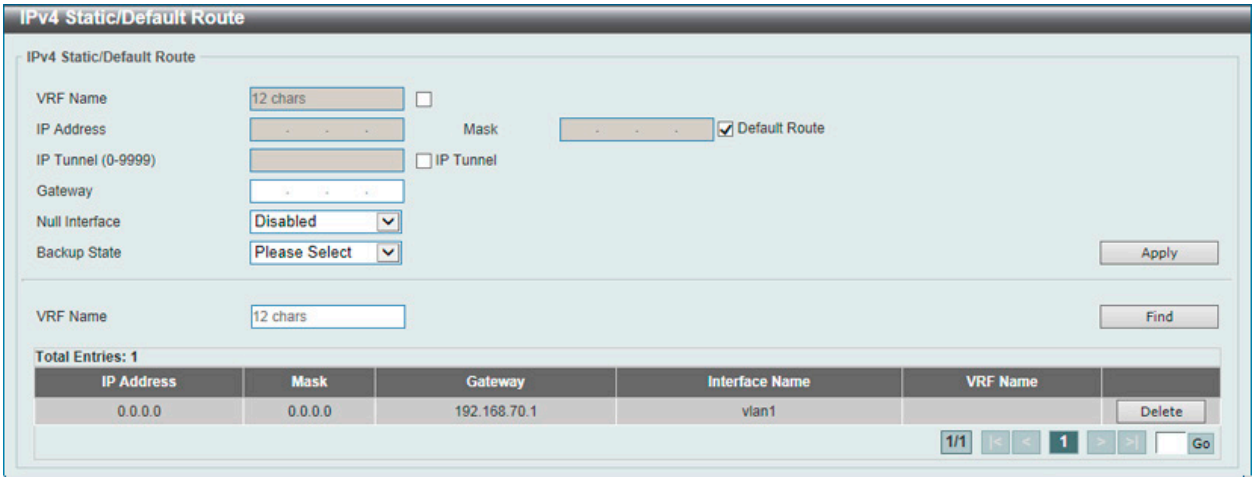


図 9-21　IPv4 Static/Default Route 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	チェックボックスにチェックを入れ、VRF インスタンス名を入力します。（12 文字以内）
IP Address	スタティックルートに割り当てる IPv4 アドレスを入力します。「Default Route」をチェックすると、IPv4 アドレスとしてデフォルトルートを使用します。
Mask	このルートのサブネットマスクを入力します。
IP Tunnel （EI モードのみ）	IP トンネル機能を使用するには、「IP Tunnel」のチェックボックスにチェックを入れ、トンネル ID を入力します。 • 設定可能範囲：0-9999
Gateway	このルートのゲートウェイ IP アドレスを入力します。
Null Interface	Null インタフェースを有効 / 無効に設定します。
Backup State	バックアップオプションを選択します。 • 「Primary」- 宛先へのプライマリルートとしてルートを指定します。 • 「Backup」- 宛先へのバックアップルートとしてルートを指定します。 • 「Weight」-「0」より大きく、最大パス数より小さい重みの数値を指定します。本数値はルーティングテーブルのルートパスの複製（複数コピー）に使用され、これによりトラフィックルーティングの際にパスが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、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報を基にエントリを検索します。

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 9-22　IPv4 Static Route BFD 画面

画面に表示される項目：

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入力します。（12 文字以内）
IP Address	BFD ピアの IP アドレスを指定します。

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

IPv4 Route Table（IPv4 ルートテーブル）

IPv4 ルートテーブルを表示します。

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

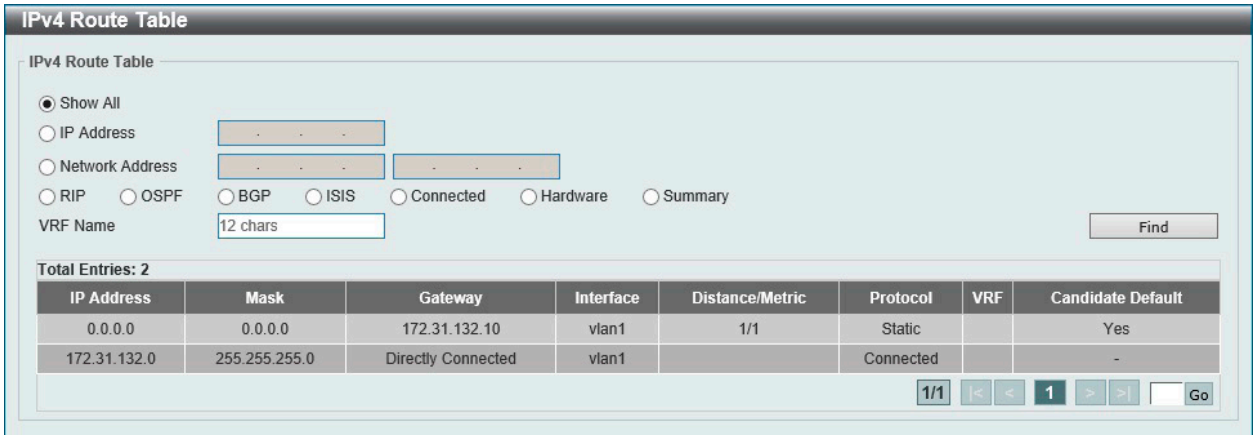


図 9-23　IPv4 Route Table 画面

画面に表示される項目：

項目	説明
Show All	すべての IPv4 ルートを表示します。
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	RIP ルートのみを表示します。
OSPF	OSPF ルートのみを表示します。
BGP（EI モードのみ）	BGP ルートのみを表示します。
ISIS（EI モードのみ）	ISIS ルートのみを表示します。
Connected	接続されたルートのみを表示します。
Hardware	ハードウェアチップに記録されたルートのみ表示されます。
Summary	スイッチに設定されているルートソースの概要と数が表示されます。
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）

「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート設定）

IPv6 スタティックルートまたはデフォルトルートを表示および設定します。

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

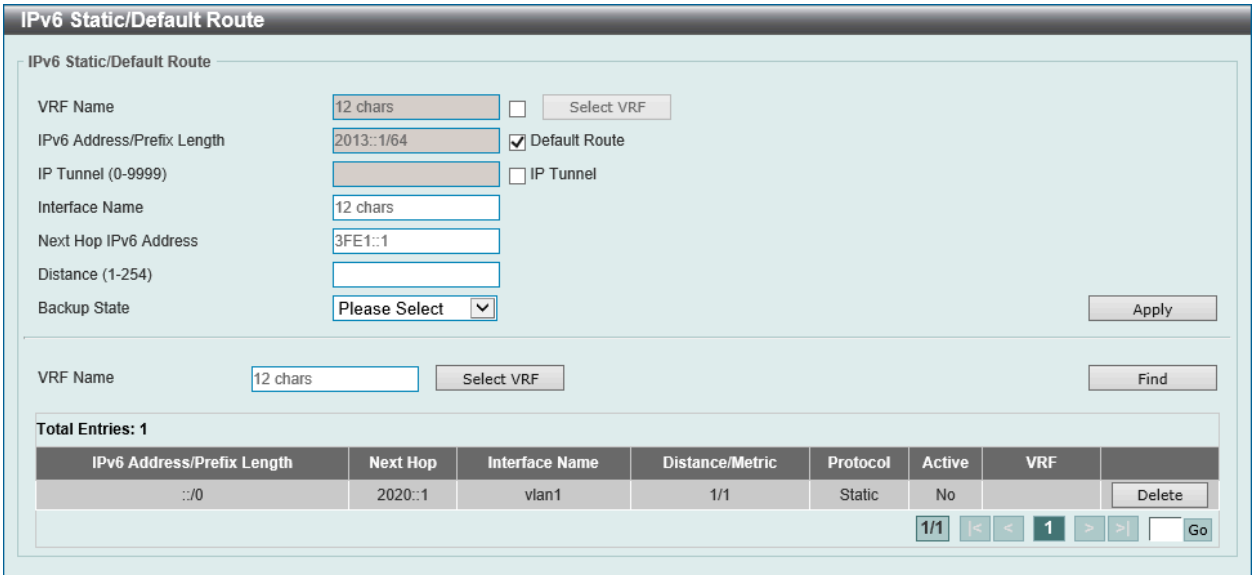


図 9-24　IPv6 Static/Default Route 画面

画面に表示される項目：

項目	説明
VRF Name	チェックボックスにチェックを入れ、VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
IPv6 Address/Prefix Length	スタティックルートに割り当てる IPv6 アドレスおよびプレフィックスを入力します。「Default Route」をチェックすると、このルートをデフォルトルートとして使用します。
IP Tunnel （EI モードのみ）	IP トンネル機能を使用するには、「IP Tunnel」のチェックボックスにチェックを入れ、トンネル ID を入力します。 • 設定可能範囲：0-9999
Interface Name	このルートを関連づけるインタフェースの名前を入力します。
Next Hop IPv6 Address	ネクストホップ IPv6 アドレスを指定します。
Distance	スタティックルートのアドミニストレーティブディスタンスを指定します。小さい値の方が、より適切なルートを意味します。 • 設定可能範囲：1-254 • 初期値：1
Backup State	バックアップオプションを選択します。 • 「Primary」- 宛先へのプライマリルートとしてルートを指定します。 • 「Backup」- 宛先へのバックアップルートとしてルートを指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報を基にエントリを検索します。

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。

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。

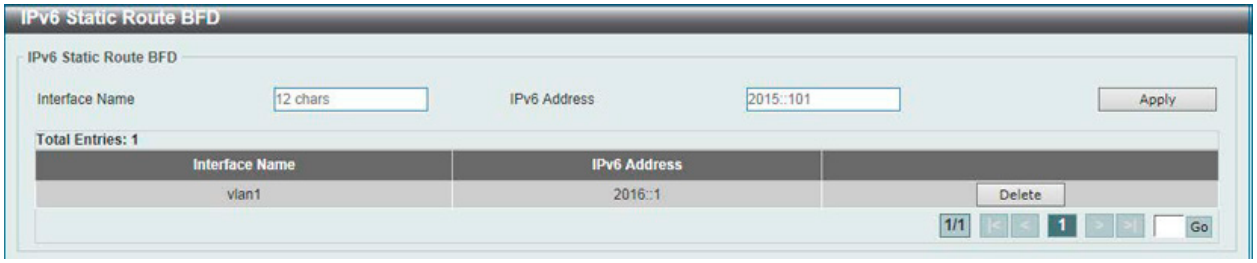


図 9-25　IPv6 Static Route BFD 画面

画面に表示される項目：

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入力します。（12 文字以内）
IPv6 Address	BFD ピアの IPv6 アドレスを指定します。

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

IPv6 Route Table（IPv6 ルートテーブル）

IPv6 ルートテーブルを表示します。

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

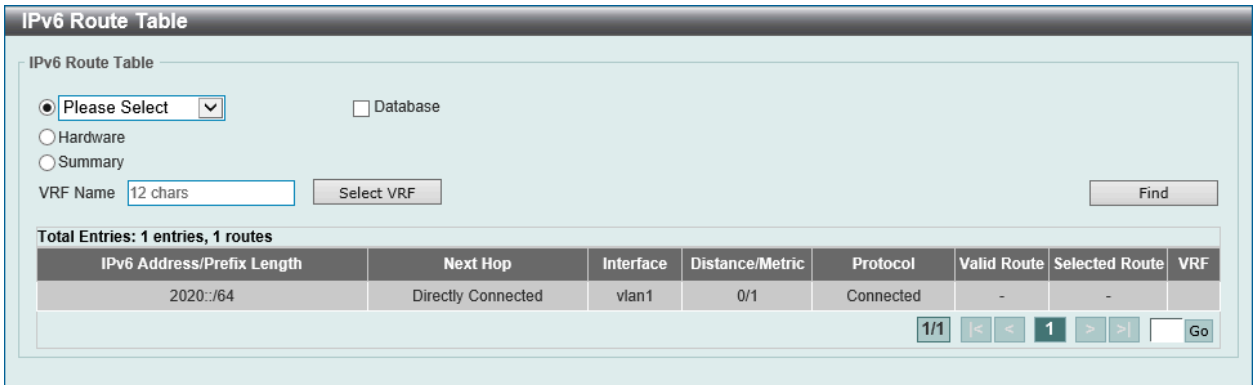


図 9-26　IPv6 Route Table 画面

画面に表示される項目：

項目	説明
Please Select	プルダウンメニューから表示する項目を選択します。 • 「IPv6 Address」- 表示するルートの IPv6 アドレスを入力します。 • 「IPv6 Address/Prefix Length」- 表示するルートの IPv6 アドレスとプレフィックスを指定します。「Longer Prefixes」を指定するとプレフィックス長と同等、もしくはそれよりも長いプレフィックスの IPv6 ルートを表示します。 • 「Interface Name」- 表示するインタフェース名を指定します。 • 「Connected」- 接続されたルートのみを表示します。 • 「RIPng」- RIPng ルートのみを表示します。 • 「OSPFv3」- OSPFv3 ルートのみを表示します。 • 「ISIS」（EI モードのみ）- ISIS ルートのみを表示します。 • 「BGP」（EI モードのみ）- BGP ルートのみを表示します。 「Database」にチェックを入れると、ベストルートだけでなく、ルーティングデータベース内のすべてのエントリを表示します。
Hardware	ハードウェアチップに記録されたルートのみ表示されます。
Summary	スイッチに設定されているルートソースの概要と数が表示されます。

項目	説明
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）

「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Route Preference（ルート優先度設定）

ルート優先度を設定します。ルート信頼度レーティングを示すディスタンスを設定します。ルートのディスタンス値が小さいほど優先度が高くなります。

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。

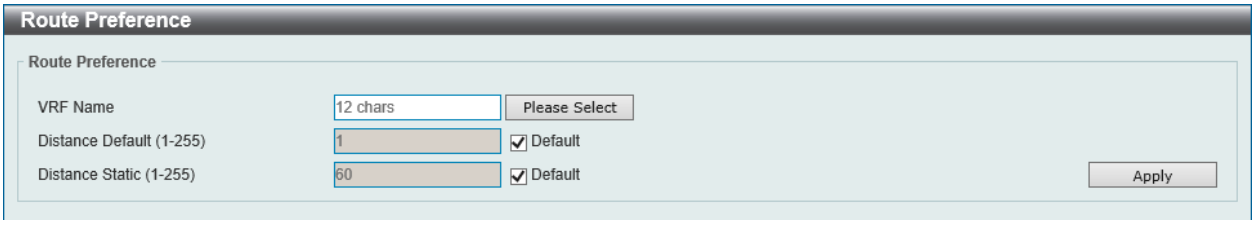


図 9-27　Route Preference 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Distance Default	デフォルトルートのアドミニストレーティブディスタンスを指定します。 • 設定可能範囲：1-255 • 初期値：1
Distance Static	スタティックルートのアドミニストレーティブディスタンスを指定します。 • 設定可能範囲：1-255 • 初期値：60

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

ECMP Settings（ECMP 設定）

Equal-Cost Multi-Path (ECMP) ルーティング設定を行います。負荷分散ハッシュアルゴリズムの設定と、同じ宛先の複数パスエントリに対しネクストホップを決定する際に使用されます。

L3 Features > ECMP Settings をクリックし、以下の画面を表示します。

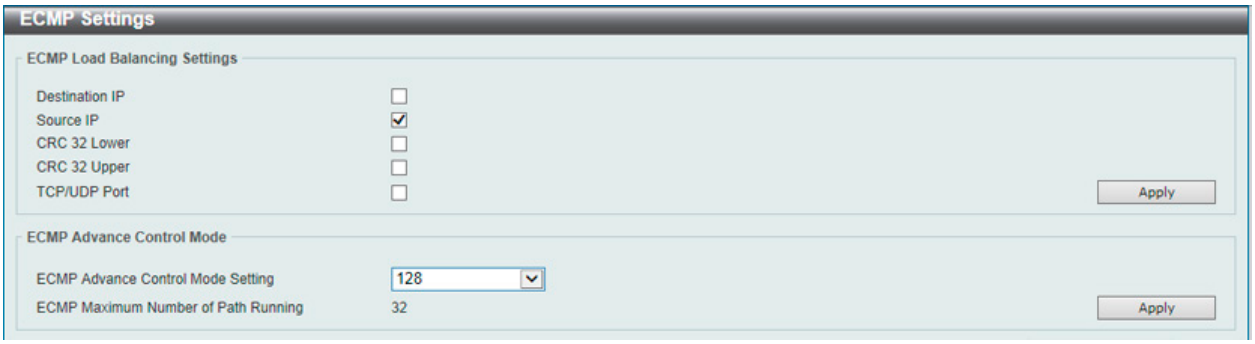


図 9-28　ECMP Settings 画面

画面に表示される項目：

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 の最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。

項目	説明
CRC 32 Upper	ECMP ハッシュアルゴリズムとして CRC-32 の上位ビットを使用します。
TCP/UDP Port	ECMP ハッシュ鍵として TCP または UDP ポート番号を使用します。
ECMP Advance Control Mode	
ECMP Advance Control Mode Setting	ECMP アドバンスコントロールモードの設定を行います。この数値に従って、ECMP またはマルチパスルートの数、各 ECMP またはマルチパスルートのネクストホップ数が変更されます。 • 選択肢：「64」「128」「256」「512」「1024」

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6 General Prefix（IPv6 汎用プレフィックス）

本項目では、VLAN インタフェース IPv6 汎用プレフィックスの設定、表示を行います。

L3 Features > IPv6 General Prefix をクリックし、以下の画面を表示します。

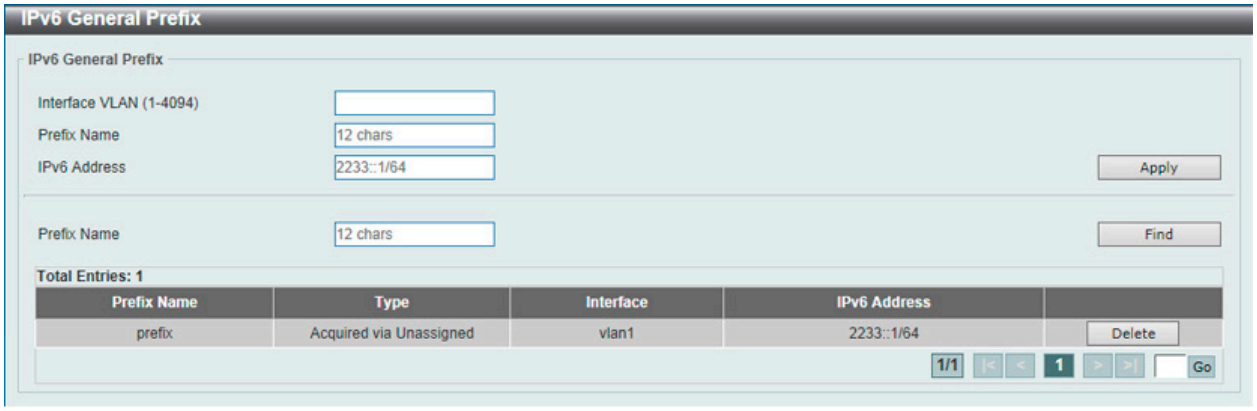


図 9-29　IPv6 General Prefix 画面

画面に表示される項目：

項目	説明
Interface VLAN	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Prefix Name	IPv6 汎用プレフィックスエントリ名を指定します。（12 文字以内）
IPv6 Address	IPv6 アドレスとプレフィックス長を指定します。IPv6 アドレスのプレフィックス長は VLAN インタフェースのローカルサブネットでもあります。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
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）（EI モードのみ）

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。

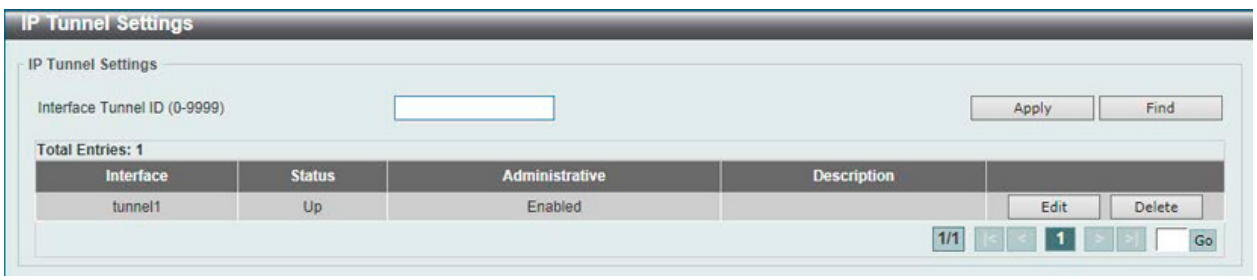


図 9-30　IP Tunnel Settings 画面

画面に表示される項目：

項目	説明
Interface Tunnel ID	IP トンネルのインタフェース ID を入力します。 • 設定可能範囲：0-9999

「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。

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

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。

エントリの編集

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。

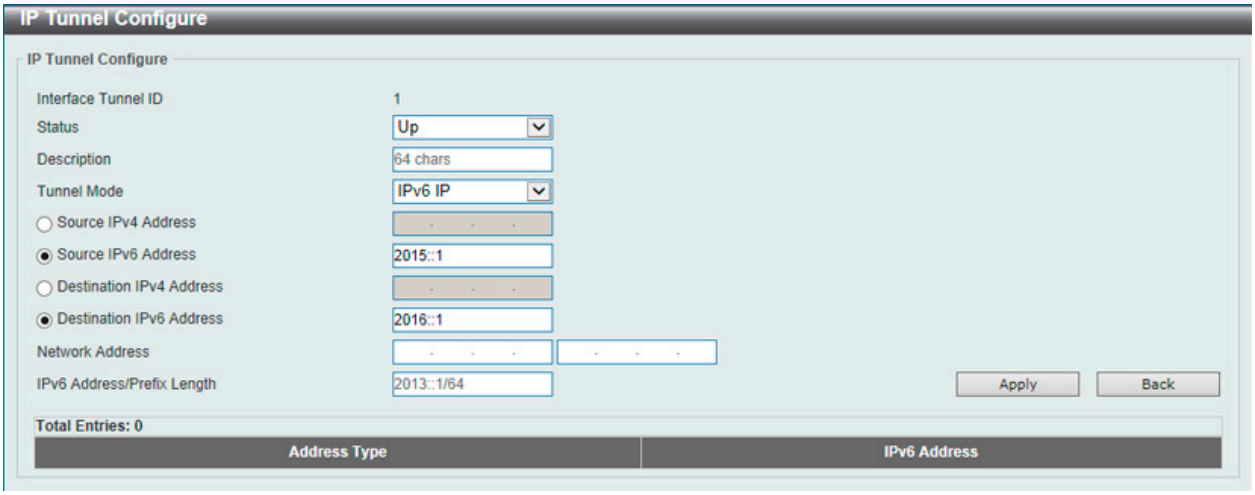


図 9-31　IP Tunnel Settings（Edit）- IP Tunnel Configure 画面

画面に表示される項目：

項目	説明
Status	IP トンネルインタフェースの状態を指定します。 • 選択肢：「Up」「Down」
Description	IP トンネルインタフェースの説明を指定します。（64 文字以内）
Tunnel Mode	トンネルモードを選択します。 • 「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。配信プロトコルは 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。配信プロトコルは IPv6 プロトコルです。
Source IPv4/IPv6 Address	インタフェースの送信元 IPv4/IPv6 アドレスを指定します。
Destination IPv4/IPv6 Address	インタフェースの送信先 IPv4/IPv6 アドレスを指定します。
Network Address	ネットワークアドレスを入力します。
IPv6 Address/Prefix Length	IPv6 アドレスとプレフィックス長を入力します。

項目を編集し、エントリの「Apply」ボタンをクリックします。

前の画面に戻るには、「Back」ボタンをクリックします。

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。ネットワーク上で攻撃を開始する一般的な方法の 1 つは、IPv4/IPv6 送信元アドレススプーフィングを利用することです。この方法では、ターゲットによって信頼されている / 既知の送信元アドレスを使用してトラフィックがネットワークに送信されます。保護が行われていない場合、組織のネットワークはトラフィックを許可し、様々な種類の攻撃にさらされる可能性があります。ユニキャスト RPF は、ルータを通過する不正な形式または偽造された IPv4/IPv6 送信元アドレスによって引き起こされる問題を軽減するのに役立ちます。

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。

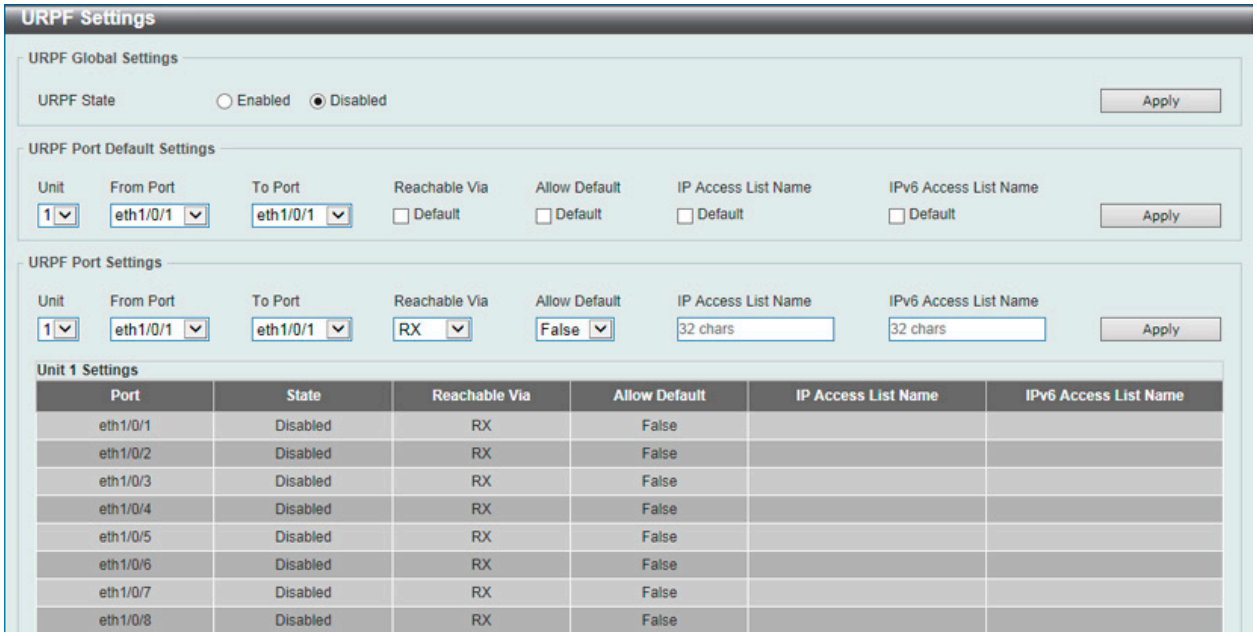


図 9-32　URPF Settings 画面

画面に表示される項目：

項目	説明
URPF Global Settings	
URPF State	URPF を有効 / 無効に設定します。 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、その後「Dynamic Inspection Protocol」（DIP）を使用した検出が必要になります。このプロセスでは、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、スイッチを再起動した後に有効になります。
URPF Port Default Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Reachable Via	デフォルトの到達可能な via 設定（RX）が使用されます。
Allow Default	デフォルトの許可設定（False）を使用します。
IP Access List Name	デフォルトの IP アクセスリスト設定を使用します。
IPv6 Access List Name	デフォルトの IPv6 アクセスリスト設定を使用します。
URPF Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
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認します。（Loose モード） • 「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、送信元と一致する受信インタフェースがパケットを受信するインタフェースを通して到達可能かを確認します。（Strict モード）
Allow Default	「Allow Default」のオプションを選択します。 • 「True」- ユニキャスト RPF 検証のデフォルトルートを使用します。 • 「False」- ユニキャスト RPF 検証のデフォルト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 文字以内）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 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

VRF（Virtual Routing and Forwarding）（EI 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 9-33　VRF Settings 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。（12 文字以内）

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

「Edit」ボタンをクリックすると、以下の画面が表示されます。

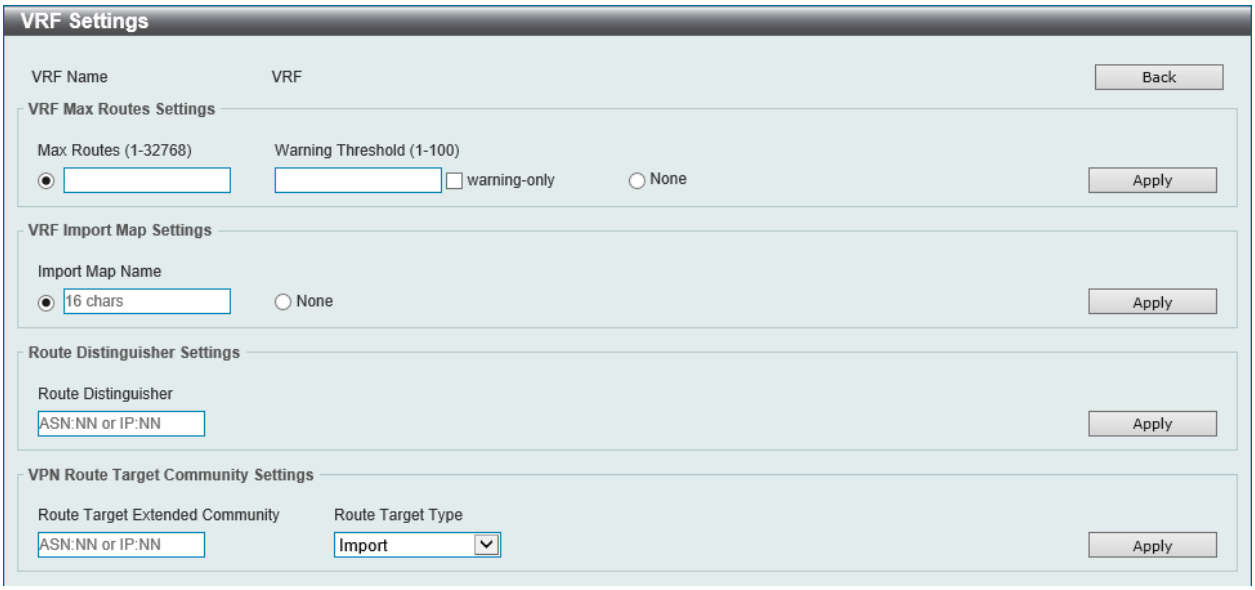


図 9-34　VRF Settings (Edit) 画面

画面に表示される項目：

項目	説明
VRF Max Routes Settings	
Max Routes	VRF 内の最大ルート数を入力します。 • 設定可能範囲：1-32768
Warning Threshold	警告しきい値を指定します。ルート数がしきい値に達し、ルートがハードウェアに書き込めなくなると、通知メッセージが送信されます。「warning-only」のオプションを選択すると、ルート数がしきい値を超えたときに通知メッセージが送信されますが、ルートは引き続きハードウェアに書き込むことができます。 • 設定可能範囲：1-100（%）
None	制限なしに設定するには、本オプションを指定します。

項目	説明
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。（16 文字以内）
None	VRF のインポートルートマップを無効にします。
Route Distinguisher Settings	
Route Distinguisher	VRF の Route Distinguisher (RD) を指定します。IPv4 プレフィックスの先頭に 8 バイト値を付加して VPN-IPv4 プレフィックスを作成するために使用されます。
VPN Route Target Community Settings	
Route Target Extended Community	ルートターゲット値を指定します。ルートターゲットは VPN のアプリケーションとして役に立ちます。1 つの VRF に対し複数のルートターゲットを設定することができます。
Route Target Type	ルートターゲットの種類を指定します。 • 「Import」- インポートルートターゲットを追加して、ターゲット VPN 拡張コミュニティからルーティング情報をインポートするように指定します。 • 「Export」- エクスポートルートターゲットを追加して、ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートするように指定します。 • 「Both」- インポートルート / エクスポートルートターゲットの両方を追加します。

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

「Show Detail」をクリックすると、以下の画面が表示されます。

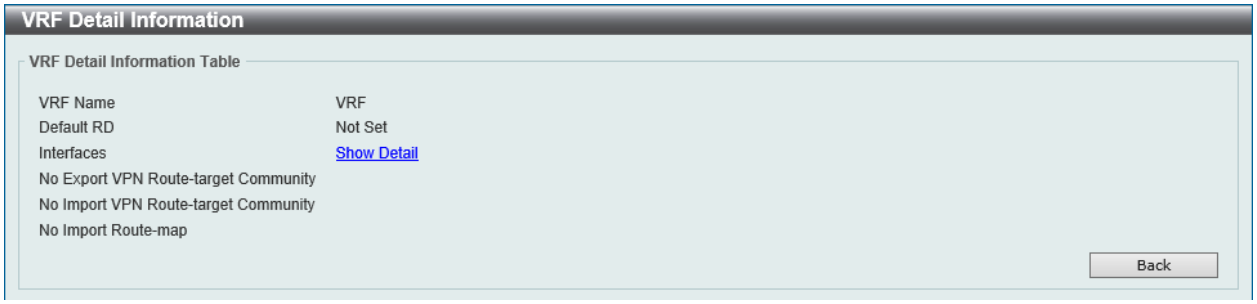


図 9-35　VRF Settings (Show Detail) - VRF Detail Information 画面

「VRF Detail Information」画面の Show Detail リンクをクリックすると、画面下部に情報が表示されます。

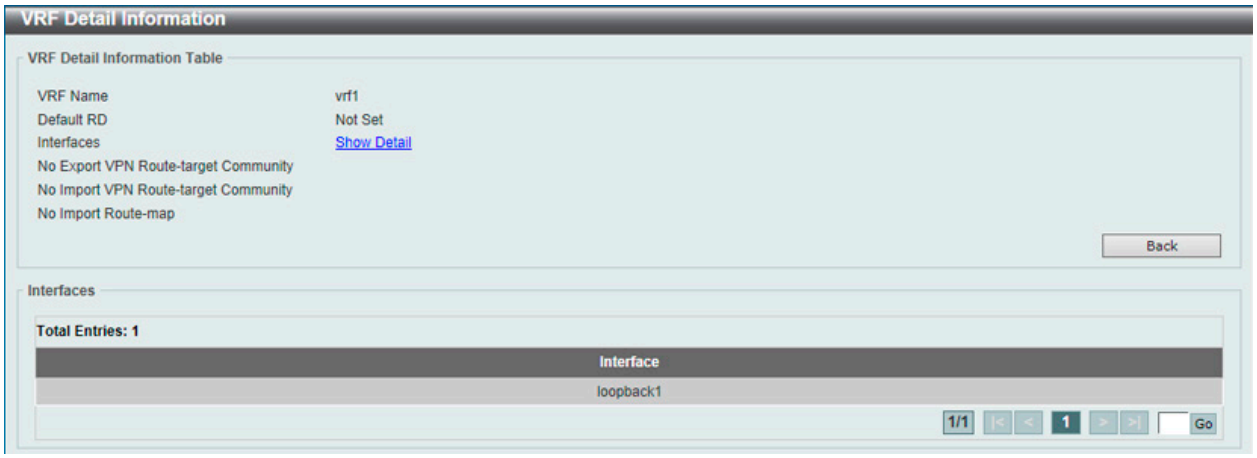


図 9-36　VRF Settings (Show Detail) - VRF Detail Information 画面

前の画面に戻るには、「Back」ボタンをクリックします。

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。

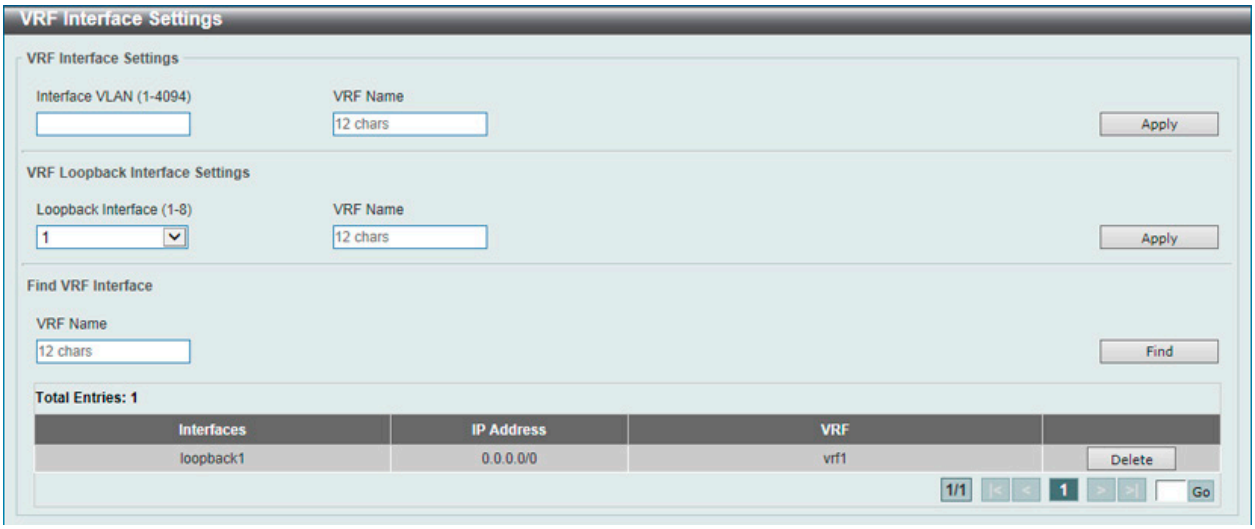


図 9-37　VRF Interface Settings 画面

画面に表示される項目：

項目	説明
VRF Interface Settings	
Interface VLAN	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
VRF Name	VRF インスタンス名を入力します。（12 文字以内）
VRF Loopback Interface Settings	
Loopback Interface	ループバックインタフェース ID を指定します。 • 設定可能範囲：1-8
VRF Name	VRF インスタンス名を入力します。（12 文字以内）
Find VRF Interface	
VRF Name	VRF インスタンス名を入力します。（12 文字以内）

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

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。

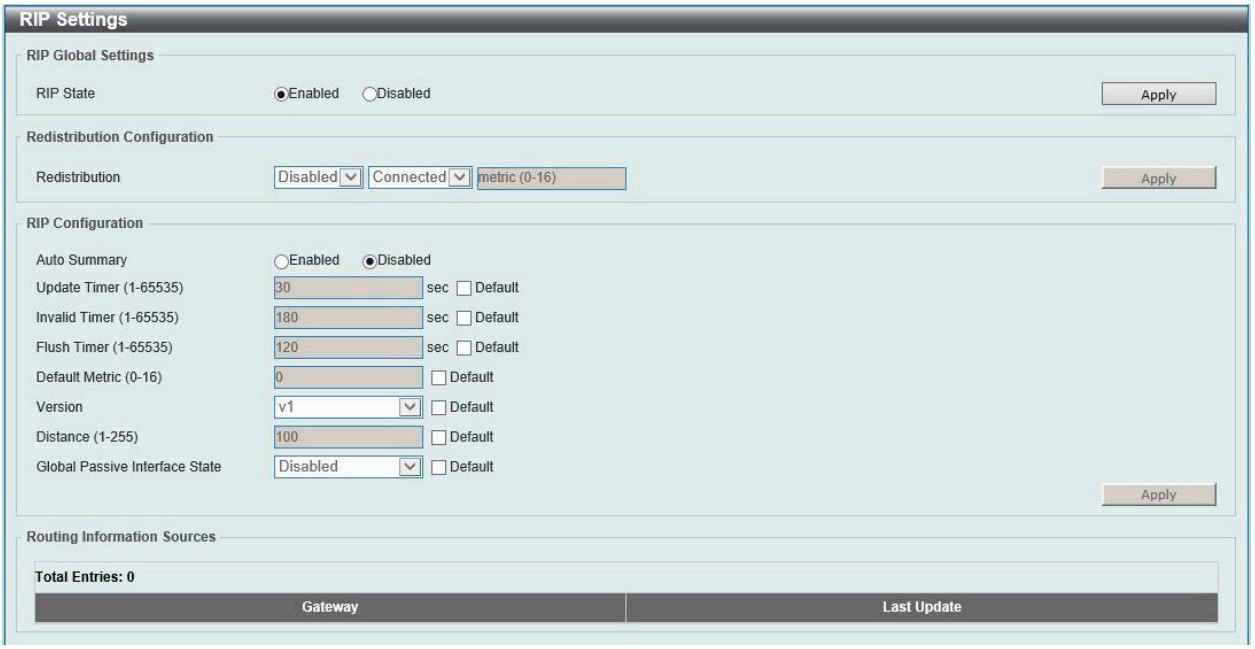


図 9-38　RIP Settings 画面（SI モード）

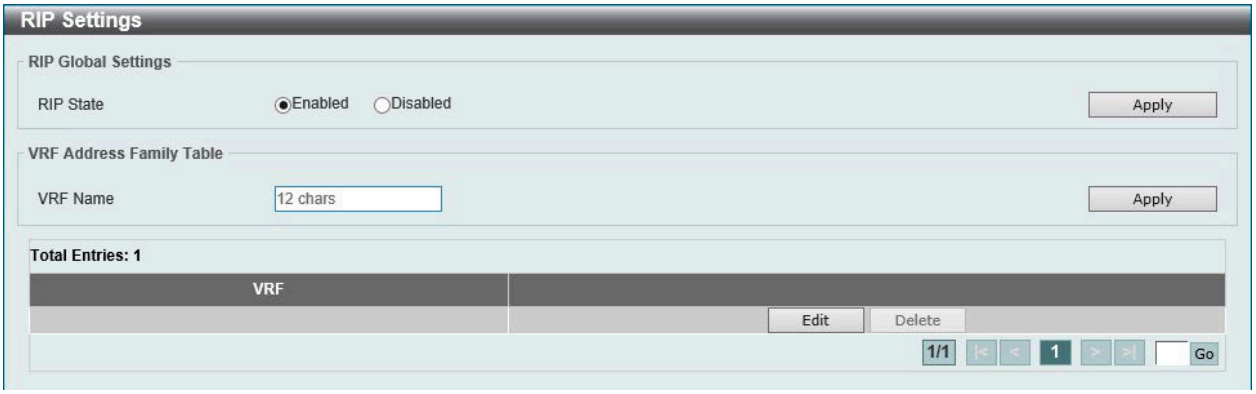


図 9-39　RIP Settings 画面（EI モード）

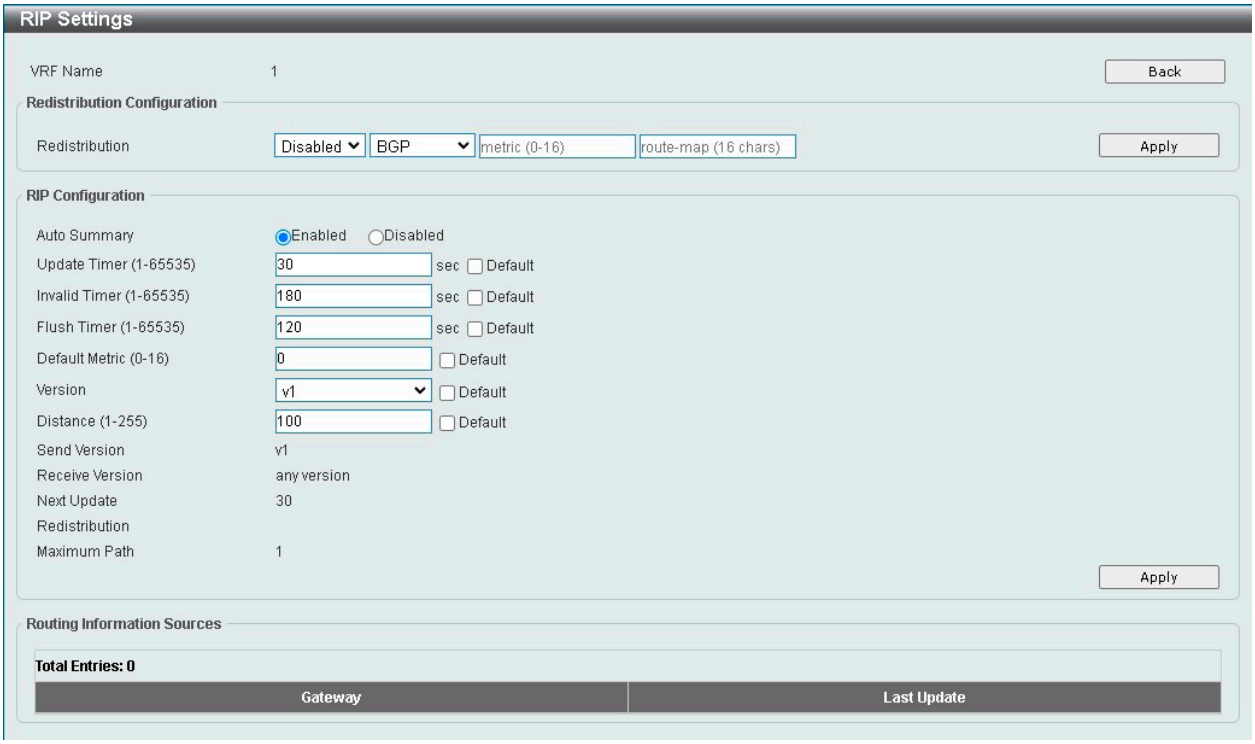


図 9-40　RIP Settings 画面（Edit）（EI モード）

画面に表示される項目：

項目	説明
RIP Global Settings	
RIP State	RIP 機能のグローバルステータスを有効 / 無効に設定します。
VRF Address Family Table	
VRF Name（EI モードのみ）	VRF インスタンスの名前を入力します。（12 文字以内）
Redistribution Configuration	
Redistribution	次の手順で指定します。 1. RIP Redistribution（RIP 再配布）機能を有効 / 無効に設定します。 2. RIP に再配布されるルーティングプロトコル（ドメイン）を指定します。「Static」は IP スタティックルートを再配布します。「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。 - 選択肢：「BGP（EI モードのみ）」「Connected」「OSPF」「Static」「ISIS（EI モードのみ）」 3. 再配布ルートのメトリック値を指定します。 - 設定可能範囲：0-16 4. 現在のルートプロトコルに再配布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。指定しない場合、全てのルートが再配布されます。
RIP Configuration	
Auto Summary	自動サマリ（集約）機能を有効 / 無効に設定します。
Update Timer	RIP アップデートメッセージを送信する間隔を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
Invalid Timer	Invalid タイマ値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：180（秒）
Flush Timer	Flush タイマ値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：120（秒）
Default Metric	初期メトリック値を指定します。他のルーティングプロトコルからのルートの再配布に使用されます。再配布されるルートは他のプロトコルに学習され、RIP との互換性がないメトリックになる場合があります。メトリックの指定により、メトリックを同期します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-16（秒） • 初期値：0（秒）
Version	すべてのインタフェースで初期バージョンとして使用されるグローバル RIP バージョンを指定します。「Default」を指定すると初期値を使用します。初期値では v1/v2 どちらも受信しますが、v1 のみ送信します。 • 選択肢：「v1（RIPv1）」「v2（RIPv2）」

項目	説明
Distance	RIPのアドミニストレーティブディスタンスを指定します。小さい値ほど適切なルートを意味します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-255 • 初期値：100

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

EI モードの場合、「Edit」ボタンをクリックすると、設定画面が表示されます。
前の画面に戻るには、「Back」ボタンをクリックします。

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。

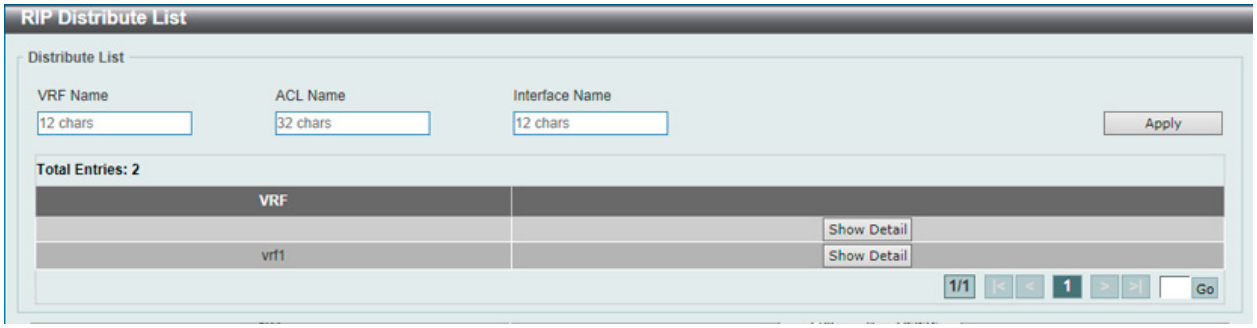


図 9-41　RIP Distribute List 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
ACL Name	アクセスリスト名を入力します。（32 文字以内）
Interface Name	インタフェース名を入力します。（12 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Show Detail」ボタンをクリックして、指定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 9-42　RIP Distribute List (Show Detail) 画面

前の画面に戻るには、「Back」ボタンをクリックします。

RIP Interface Settings（RIP インタフェース設定）

RIP インタフェースの設定を行います。

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

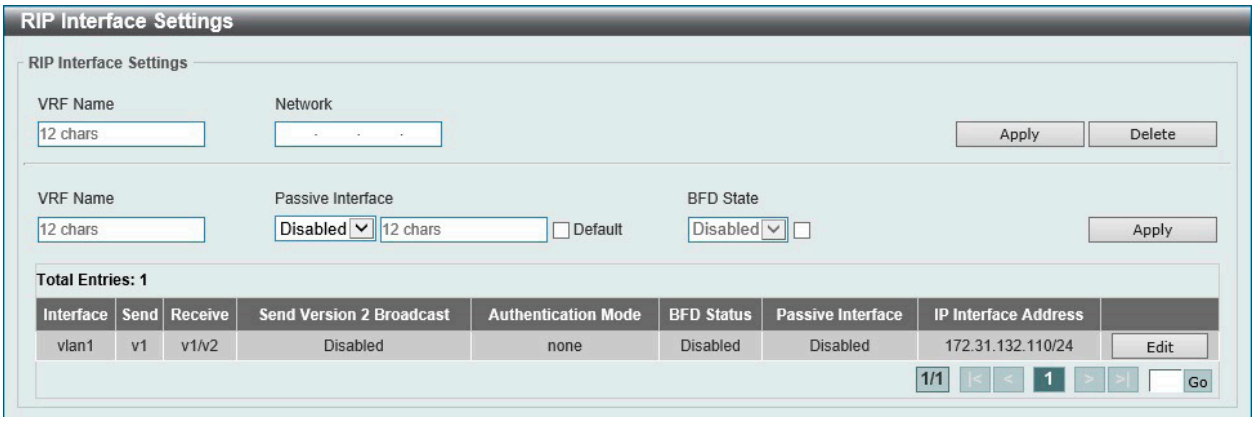


図 9-43　RIP Interface Settings 画面

画面に表示される項目：

項目	説明
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Network	RIP に使用される IPv4 ネットワーク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 / 無効に設定します。本機能は、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。ただし、本インタフェースで受信した他のルータからの RIP パケットは引き続き処理されます。表示される入力欄にパッシブインタフェースの名前（12 文字以内）を入力します。「Default」を指定すると、これがすべてのインタフェースの既定として使用されます。
BFD State	指定インタフェースの BFD 機能を有効 / 無効に設定します。BFD がインタフェースで有効な場合、ルータにより、インタフェースの現在の RIP ピアとともに BFD ピアが作成され、新しい RIP ピアが追加される際も 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 ルートもまた削除されます。

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

エントリの編集

「Edit」ボタンをクリックすると、以下の画面が表示されます。



図 9-44　RIP Interface Settings（Edit）- Configure RIP Interface 画面

画面に表示される項目：

項目	説明
Send Version	インタフェースで送信できる RIP パケットのバージョンを選択します。 • 選択肢：「v1」「v2」
Receive Version	インタフェースで受信できる RIP パケットのバージョンを選択します。 • 選択肢：「v1」「v2」「v1/v2」
Send v2-broadcast	RIP バージョン 2 の更新パケットを、マルチキャストパケットではなくブロードキャストパケットとして送信することを有効 / 無効に設定します。
Authentication Mode	認証モードを有効 / 無効に設定します。 • 「Disabled」- インタフェースで RIP 認証を無効にします。 • 「Text」- インタフェースで RIP 認証を有効にします。

項目	説明
BFD State	指定されたインタフェースで BFD 機能を有効 / 無効に設定します。
Authentication Text Password	インタフェースの RIP 認証を有効にした場合、本オプションを選択してパスワードを入力します。（16 文字以内） 空のパスワードを使用するには、「None」を選択します。

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

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（集約）されている場合、データベース内に表示されます。サマリアドレスの最後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

画面に表示される項目：

項目	説明
Network Address	ネットワークのサブネットプレフィックスとプレフィックス長を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）

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

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、ルートを計算するため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。

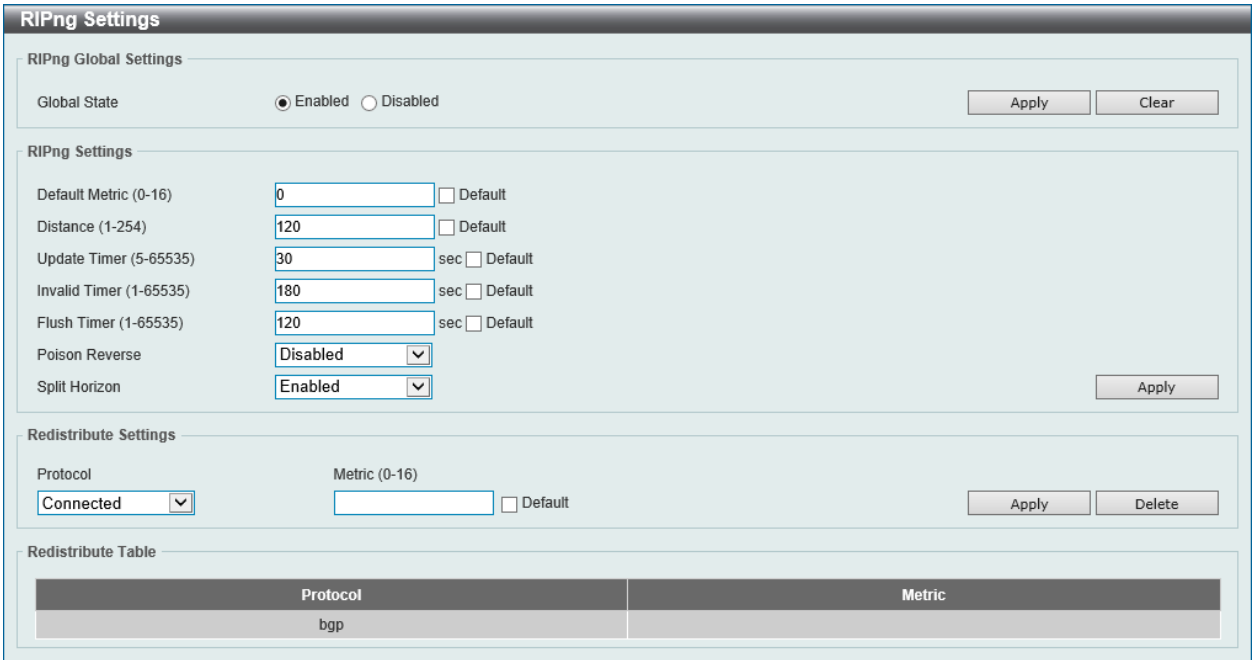


図 9-46　RIPng Settings 画面

画面に表示される項目：

項目	説明
RIPng Global Settings	
Global State	RIPng 機能のグローバルステータスを有効 / 無効に設定します。
RIPng Settings	
Default Metric	初期メトリック値を指定します。他のルーティングプロトコルからの再配布されたルートの初期メトリック値を指定します。再配布されるルートは他のプロトコルに学習され、RIPng との互換性がないメトリックになる場合があります。メトリックを再指定することにより、メトリックを同期させることができます。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-16 • 初期値：0
Distance	RIPng のアドミニストレーティブディスタンスを指定します。これは、ルートの信頼レートを意味します。小さい値ほど優先的なルートを意味します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-254 • 初期値：120
Update Timer	RIP アップデートメッセージを送信する間隔値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：5-65535（秒） • 初期値：30（秒）
Invalid Timer	Invalid タイマの値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：180（秒）
Flush Timer	Flush タイマの値を入力します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：120（秒）
Poison Reverse	「Poison Reverse」を有効 / 無効に設定します。本機能が有効の場合、インタフェースから学習したルートは到達不能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 / 無効に設定します。本機能が有効の場合、インタフェースから学習したルートは同じインタフェースに通知されません。

項目	説明
Redistribute Settings	
Protocol	ルートを再配布するプロトコルを指定します。「Static」は IPv6 スタティックルートを再配布します。「Connected」は IPv6 インタフェースの IP アドレス設定の際に自動的に構築するルートを意味します。 • 選択肢：「Connected」「Static」「OSPF」「BGP（EI モードのみ）」「ISIS（EI モードのみ）」
Metric	再配布されるルートのメトリックとして使用される値を指定します。「Default」は初期メトリック値を使用します。 • 設定可能範囲：0-16

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

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

画面に表示される項目：

項目	説明
Interface VLAN	RIPng 設定の VLAN インタフェース名を入力します。「All Interface」を選択すると、すべてのインタフェースに対して設定を適用します。 • 設定可能範囲：1-4094
State	指定の VLAN インタフェースで IPv6 RIP 機能を有効 / 無効に設定します。
Metric Offset	指定インタフェースで受信する IPv6 RIP ルートのメトリック値に本値を追加します。メトリックはホップ数を参照します。初期値では、IPv6 RIP ルートを受信すると、ルーティングテーブルに挿入される前にメトリック値「1」がルートに追加されます。この設定を使用すると、各インタフェースで受信するルートのメトリックおよびルートの優先度を調整することができます。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-16
BFD State	IPv6 RIP インタフェースの BFD 機能を有効 / 無効に設定します。
Passive Interface	パッシブインタフェースを有効 / 無効に設定します。本設定が無効になると、ルータはインタフェースを介して RIPng を送信しません。ただし、インタフェースで受信した他のルータからの RIPng パケットは、引き続き処理されます。

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

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

画面に表示される項目：

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、入力した情報に基づくエントリを検出します。

OSPF（OSPF 設定）

L3 Features > OSPF
OSPF の設定を行います。

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

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内） 「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Clear Process （EI モードのみ）	クリアするプロセスの名前を入力します。（12 文字以内） 「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。

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

「Edit」をクリックすると、以下の画面が表示されます。

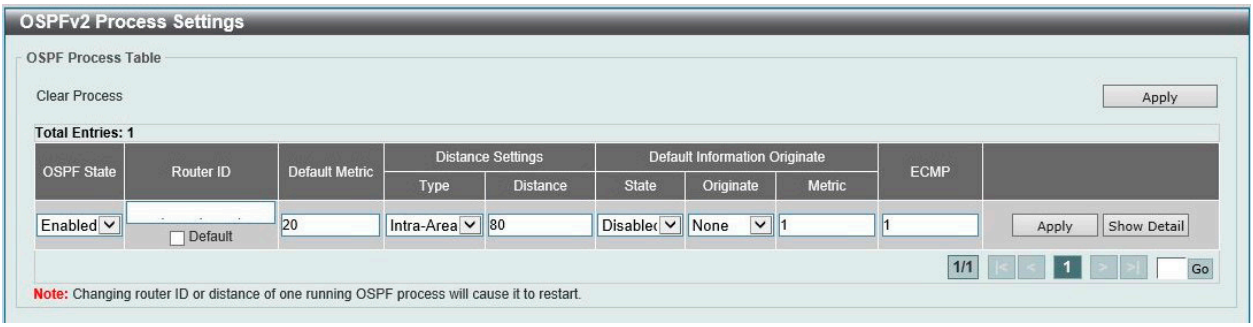


図 9-50　OSPFv2 Process Settings (Edit) 画面

画面に表示される項目：

項目	説明
OSPF State	OSPFv2 機能を有効 / 無効に設定します。
Router ID	IPv4 アドレス形式でルータ ID を指定します。ルータ ID は、OSPF プロトコルを実行する各ルータにアサインされる 32 ビットの数値であり、AS 内のルータを固有に識別します。AS 内で、各ルータは一意のルータ ID を持ちます。「Default」にチェックを入れると、デフォルトルータ ID を使用します。
Default Metric	初期メトリック値を指定します。 • 設定可能範囲：1-16777214
Type	ディスタンス設定の種類を指定します。 • 「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。 • 「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。 • 「External-1」-「type-1」のメトリックで、OSPF「external type-5」および「type-7」ルートのディスタンスを指定します。 • 「External-2」-「type-2」メトリックで、OSPF「external type-5」および「type-7」ルートのディスタンスを指定します。
Distance	アドミニストレーティブディスタンス値を指定します。 • 設定可能範囲：1-255
State	初期「Originate」情報を有効 / 無効に設定します。AS に向かう初期外部ルート (type-5 LSA) ネットワーク「0.0.0.0」の生成に使用されます。
Originate	「Originate」のオプションを指定します。「Always」を指定すると、ルーティングテーブルにデフォルトルートが存在していても、常にデフォルトルートを生成し続けます。 • 選択肢：「Always」「None」
Metric	生成されたデフォルトルートにかかるコストを入力します。指定しない場合、初期メトリックは「1」になります。 • 設定可能範囲：1-65535
ECMP	プロセスの ECMP 値を指定します。 • 設定可能範囲：1-64

「Apply」ボタンをクリックして、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。

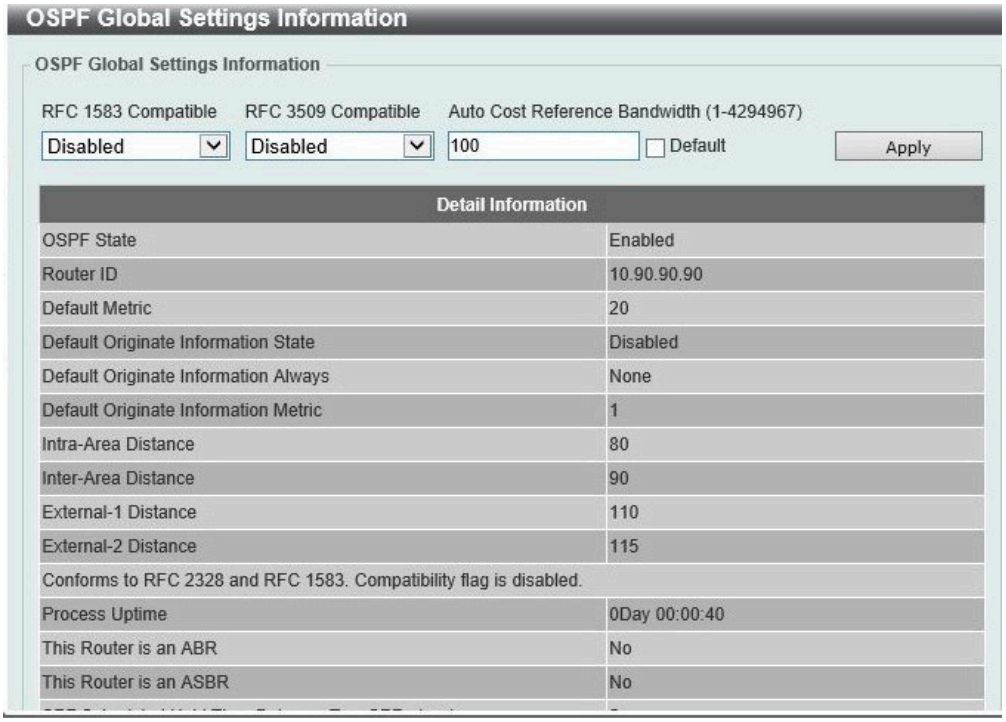


図 9-51　OSPFv2 Process Settings (Show Detail) - OSPF Global Settings Information 画面

画面に表示される項目：

項目	説明
RFC 1583 Compatible	RFC1583 の実装を有効 / 無効に設定します。
RFC 3509 Compatible	RFC3509 の実装を有効 / 無効に設定します。
Auto Cost Reference Bandwidth	自動コスト参照帯域幅の値を入力します。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：1-4294967

「Apply」ボタンをクリックして、設定内容を適用します。
「OK」をクリックし、画面を閉じます。

OSPFv2 Distribute List（OSPFv2 ディストリビュートリスト）

OSPFv2 ディストリビュートリストの設定、表示を行います。

L3 Features > OSPF > OSPFv2 > OSPFv2 Distribute List の順にメニューをクリックし、以下の画面を表示します。

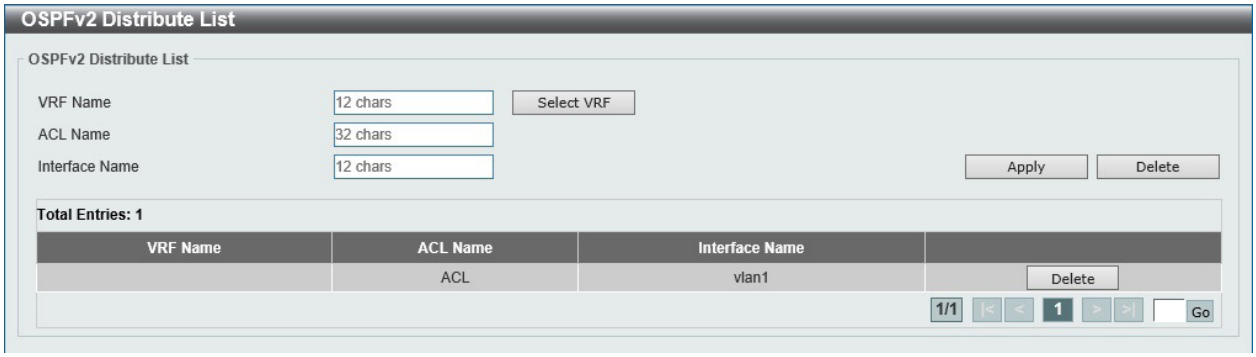


図 9-52　OSPFv2 Distribute List 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
ACL Name	アクセスリスト名を入力します。（32 文字以内）
Interface Name	インタフェース名を入力します。（12 文字以内）

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

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。

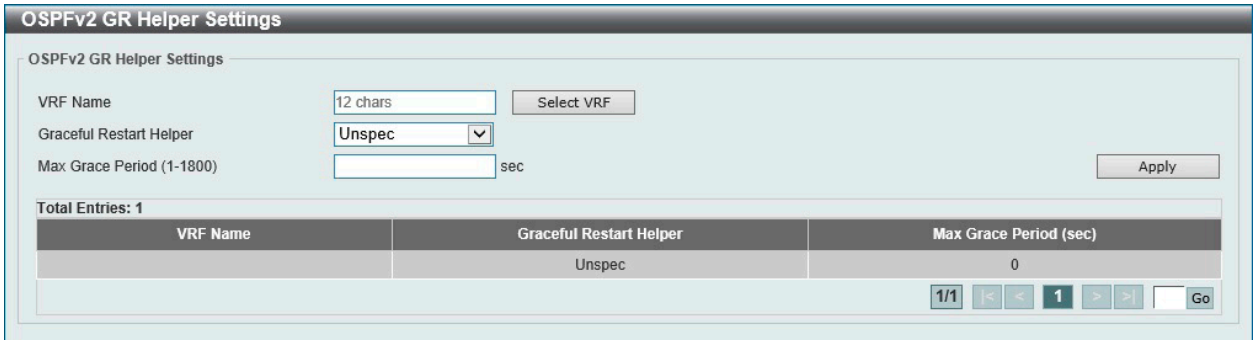


図 9-53　OSPFv2 GR Helper Settings 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
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を指定しません。 • 「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に対してのみ許可します。 • 「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に対してのみ許可します。
Max Grace Period	最大グレース期間を指定します。 • 設定可能範囲：1-1800（秒）

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

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。

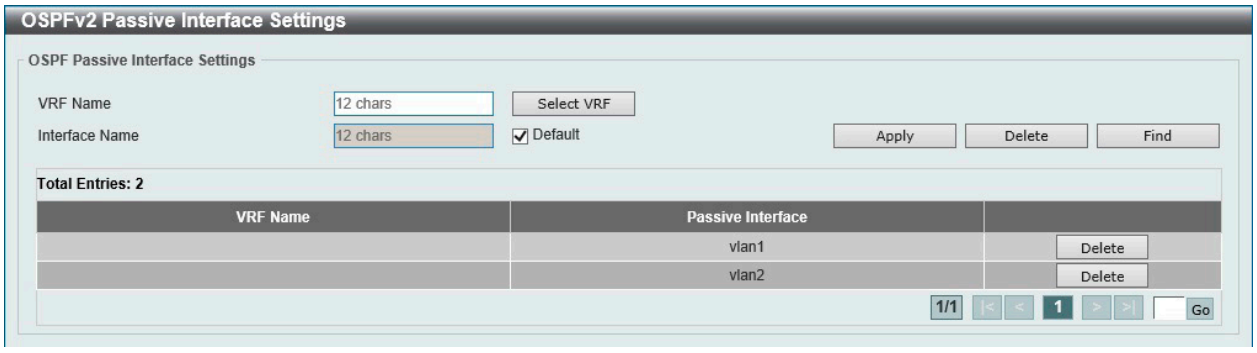


図 9-54　OSPFv2 Passive Interface Settings 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface Name	使用するインタフェース名（12 文字以内）を指定します。「Default」を選択するとすべての有効なインタフェースを指定します。

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

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。

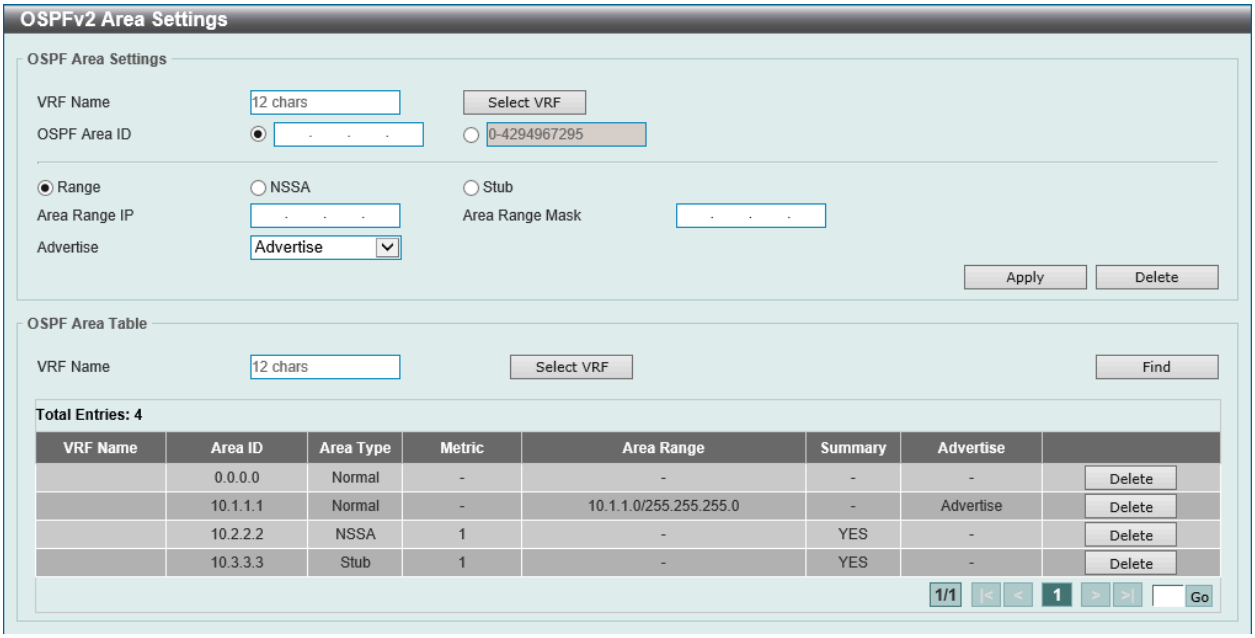


図 9-55　OSPFv2 Area Settings 画面

画面に表示される項目：

項目	説明
OSPFv2 Area Settings	
VRF Name (EI モードのみ)	VRF インスタンス名を入力します。(12 文字以内)「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
OSPF Area ID	OSPFv2 エリア識別子を選択して入力します。IP アドレス形式（xxx.xxx.xxx.xxx) または 10 進数値形式（0-4294967295）で指定できます。インタフェースで構成されたサブネットがここで指定されたネットワーク範囲内にある場合に、エリアはインタフェース上に作成されます。
Range	Area Border Router (ABR) で OSPF ルートを集約します。 • 「Area Range IP」- OSPF エリア範囲の IP アドレスを入力します。 • 「Area Range Mask」- OSPF エリア範囲のサブネットマスクを入力します。 • 「Advertise」- 通知オプションを選択します。 - 「Advertise」- 指定されたアドレス範囲の「Type-3 summary Link-State Advertisement (LSA)」を通知します。 - 「No-Advertise」-「Type-3 summary LSA」の通知を抑制します。コンポーネントのルートは存在しています。
NSSA	OSPF エリアを Not-So-Stubby Area (NSSA) として割り当てます。 • 「Default Cost」- デフォルトのコスト値を入力します。スタブエリアおよび Not-So-Stubby エリアに挿入される Type-3 デフォルトルートに関連するコストです。指定できる範囲は 0-65535 です。 • 「Default」- デフォルトのコスト値を使用します。 • 「No-Summary」- このエリアに集約ルートを挿入しません。
Stub	Stub エリアとして OSPF エリアを設定します。 • 「Default Cost」- デフォルトのコスト値を入力します。スタブエリアおよび Not-So-Stubby エリアに挿入される Type-3 デフォルトルートに関連するコストです。指定できる範囲は 0-65535 です。 • 「Default」- デフォルトのコスト値を使用します。 • 「No-Summary」- このエリアに集約ルートを挿入しません。
OSPF Area Table	
VRF Name (EI モードのみ)	VRF インスタンス名を入力します。(12 文字以内)「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。

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

テーブルのエントリをダブルクリックすると、以下の画面が表示されます。



図 9-56　OSPFv2 Area Settings（Process ID）- OSPF Area Settings 画面

「OK」ボタンをクリックして、画面を閉じます。
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。

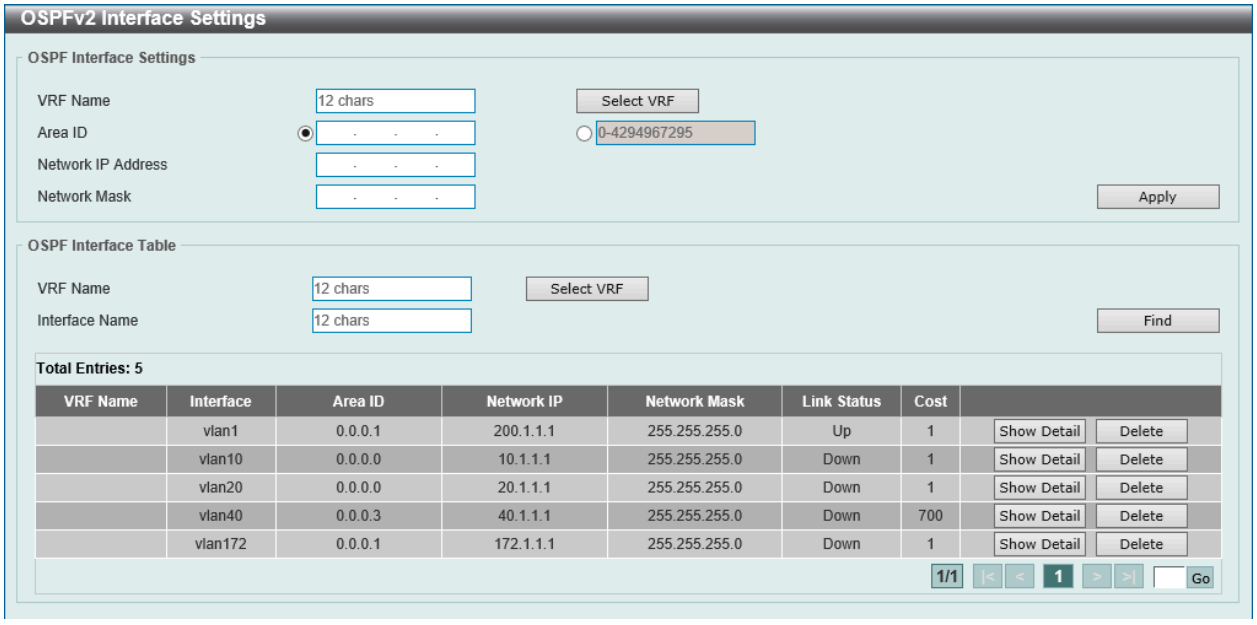


図 9-57　OSPFv2 Interface Settings 画面

画面に表示される項目：

項目	説明
OSPF Interface Settings	
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Area ID	OSPFv2 エリア識別子を選択して入力します。IP アドレス形式（xxx.xxx.xxx.xxx）または 10 進数値形式（0-4294967295）で指定できます。
Network IP Address	ネットワークの IPv4 アドレスを指定します。
Network Mask	ネットワークの IPv4 サブネットマスクを指定します。
OSPF Interface Table	
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface Name	インタフェース名を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

「Delete」ボタンをクリックして、指定のエントリを削除します。
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」ボタンをクリックして、指定エントリの詳細について表示します。

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。

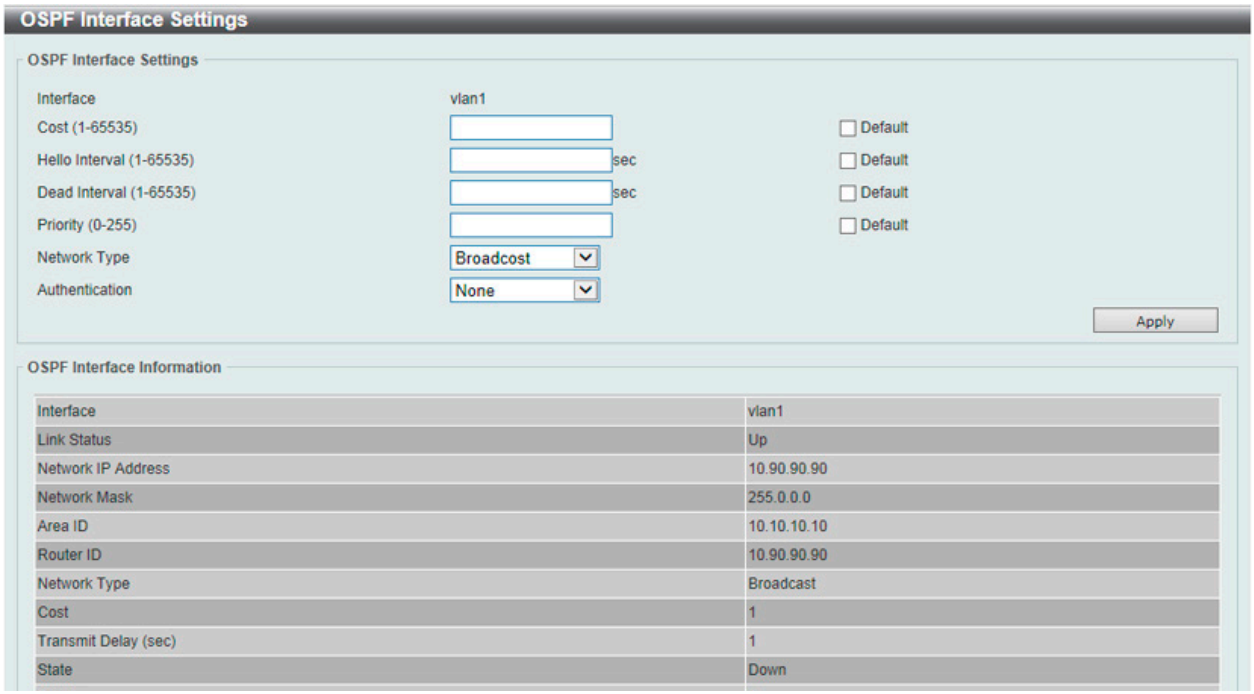


図 9-58　OSPFv2 Interface Settings (Show Detail) - OSPF Interface Settings 画面

画面に表示される項目：

項目	説明
Cost	コストの値を指定します。インタフェースのコストはインタフェース上のパケット送信のオーバーヘッドを反映します。コストはルータリンク通知の中でリンクコストとして通知されます。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535 • 初期値：1
Hello Interval	Hello インターバル値を指定します。Hello Interval は Hello パケット内で通知されます。同一ネットワーク内のすべてのルータに対し、同じ Hello Interval を設定してください。この間隔が短いと、トポロジ変更の検知が早くなりますが、ルーティングトラフィックが増加し、ルーティングが不安定になる可能性があります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead Interval	Dead インターバル値を指定します。この値は、隣接ルータが OSPF Hello パケットを受信してから、送信側のルータがダウンしたと判断するまでの時間です。本値には Hello Interval の倍数を指定します。この値は Hello パケット内で通知されます。同一ネットワーク内のすべてのルータに対し、同じ Dead Interval を設定してください。この間隔が短いと、トポロジ変更の検知が早くなりますが、ルーティングトラフィックが増加し、ルーティングが不安定になる可能性があります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
Priority	代表ルータ選出のプライオリティを指定します。OSPF ルータは、マルチアクセスネットワークにおいて代表ルータ（Designated Router/DR）を選出します。2 台のルータが代表ルータになろうとしている場合、高いプライオリティのルータが選出されます。同じプライオリティ値を持つ場合は、ルータ ID の高い方が優先されます。「0」の場合は代表ルータまたはバックアップ代表ルータ（BDR）として選出されません。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-255 • 初期値：1
Network Type	ネットワークタイプを指定します。 • 「Broadcast」- ネットワークタイプをブロードキャストとして指定します。ブロードキャストネットワークでは指定ルータ（DR）とバックアップ指定ルータ（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」- ネットワークタイプを「point-to-point」として指定します。「point-to-point」ネットワークでは、通信可能な 2 台のルータのみがネイバになることが可能です。

項目	説明
Authentication	認証方法を選択します。 • 選択肢：「None」「Simple Password」「MD5」
Password	「Authentication」で「Simple Password」を選択した場合、シンプルテキストのパスワードを入力します。（8 文字以内）パスワードにはスペースを含めることはできません。 このパスワード情報は、ルータがルーティングプロトコルパケットを送信する際の OSPF ヘッダに挿入されます。各インタフェースのそれぞれのネットワークに対し、パスワードを設定します。同じネットワーク上のルータには同じパスワードを設定し、OSPF ルーティングデータが交換できるようにします。同じルーティングドメインのルータには同じパスワードを設定してください。
MD5 Key ID	「Authentication」で「MD5」を選択した場合、パスワードの MD5 キー ID を入力します。 • 設定可能範囲：1-255
MD5	「Authentication」で「MD5」を選択した場合、MD5 キーを指定します。（16 文字以内）スペースなしの英数字文字列で指定します。 MD5 モードでは OSPF メッセージ送信者は送信メッセージのメッセージダイジェストキーを基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基に、メッセージ中のダイジェストを検証します。 ネイバルータ上の同じキー ID は、同じキー文字列で定義されている必要があります。 同じインタフェースのネイバルータに対しては同じキーを設定し、お互いに OSPF パケットが交換できるようにします。通常、同じインタフェースのすべてのネイバルータは同じキーを使用します。 MD5 ダイジェストモードでは、現在のメッセージ交換を中断することなく、ユーザは新しいキーにロールオーバーできます。 ルータが古いキーを使用して隣接ルータと OSPF パケットを交換している処理中の場合、ユーザが新しいキーを設定すると、ルータは古いキーと新しいキーの両方に重複したパケットを送信し、ロールオーバープロセスを開始します。ネットワーク上のすべてのルータが新しいキーを学習するまで、重複したパケットが送信されます。 ロールオーバープロセスが完了した後、ユーザは古いキーを削除して、ルータが古いキーを使用してルータと通信できないようにする必要があります。

「Apply」ボタンをクリックして、設定内容を適用します。

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 > OSPFv2 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

画面に表示される項目：

項目	説明
BFD State	「Edit」をクリックした後、指定インタフェースの BFD 機能を有効 / 無効に設定します。BFD がインタフェースで有効な場合、ルータは、このインタフェースの OSPF ネイバとの 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 セッションも削除されます。

「Apply」ボタンをクリックして、設定内容を適用します。
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 再配布設定）

本項目では OSPFv2 再配布（redistribution）について、設定、表示します。外部ルートは ASBR により、「Type-5」外部ルートとしてノーマルエリアに、「Type-7」外部ルートとして NSSA スタブエリアに再配布されます。
再配布外部ルートが「Type-1」の場合、メトリックは内部メトリックを意味します。再配布外部ルートが「Type-2」の場合、メトリックは外部メトリックを意味します。内部メトリックは、ルータ自身から再配布ルータまでのコストと、宛先に到達するためにアドバタイズされたコストを考慮します。外部メトリックは、宛先に到達するためにアドバタイズされたメトリックのみを認識します。初期メトリックとしてメトリック値が設定されていない場合、他のプロトコルから再配布されたルートはメトリック値 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。

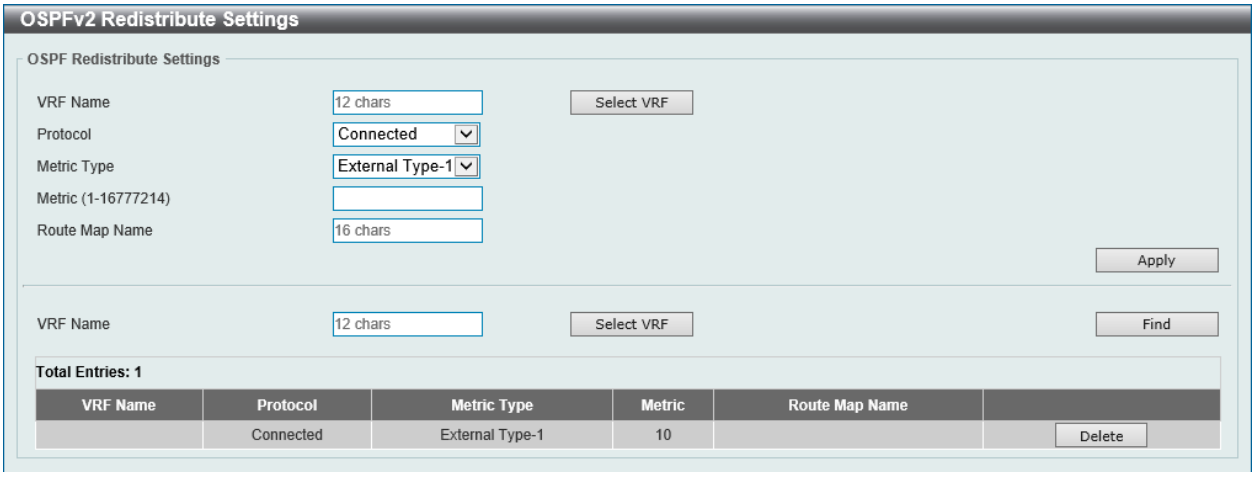


図 9-60　OSPFv2 Redistribute Settings 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Protocol	再配布される送信元プロトコルを指定します。OSPF などのルーティングプロトコルの場合、自律システムの外部として再配布されます。 • 選択肢：「Connected」「Static」「RIP」「BGP（EI モードのみ）」「ISIS（EI モードのみ）」
Metric Type	メトリックの種類を指定します。OSPF ルーティングドメインに再配布されるルートの外部リンクタイプを指定します。メトリックタイプが指定されていないと、スイッチは「Type-2」外部ルートを採用します。 • 選択肢：「External Type-1」「External Type-2」
Metric	再配布ルートのメトリックを指定します。 • 設定可能範囲：1-16777214
Router Map Name	送信元ルーティングプロトコルからインポートされたルートをフィルタするルートマップ名を指定します。 指定されない場合、すべてのルートが再配布されます。

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

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ゼロエリアに接続する必要があります。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。

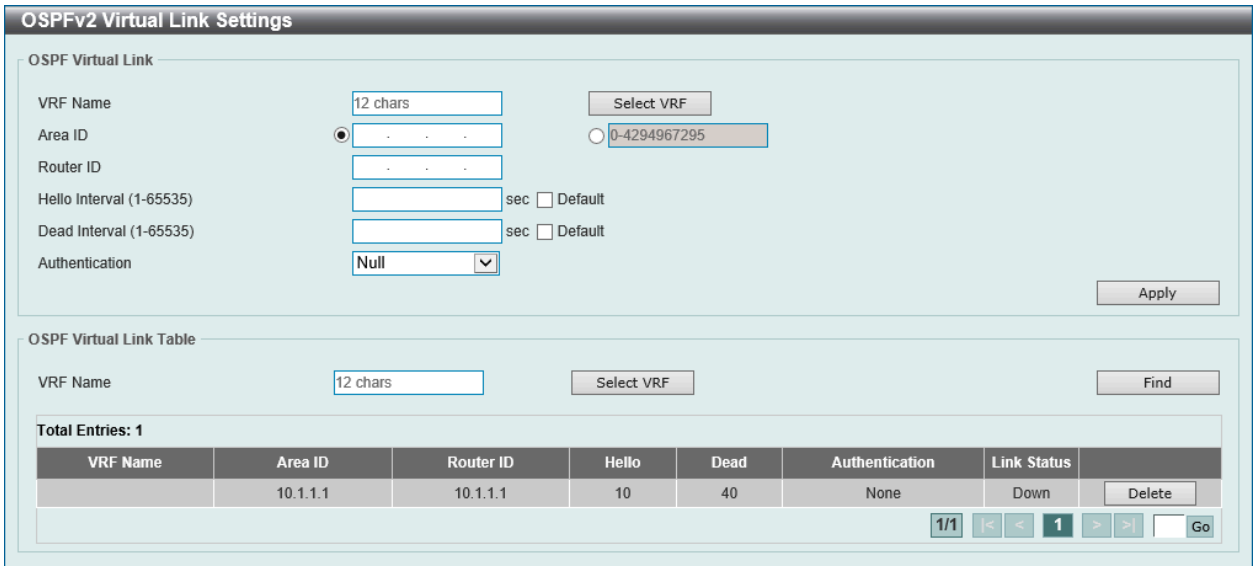


図 9-61　OSPF Virtual Link Settings 画面

画面に表示される項目：

項目	説明
OSPF Virtual Link	
VRF Name (EI モードのみ)	VRF インスタンス名を入力します。(12 文字以内)「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Area ID	OSPFv2 エリア識別子を選択して入力します。IP アドレス形式（xxx.xxx.xxx.xxx) または 10 進数値形式（0-4294967295）で指定できます。このエリアは、仮想リンクを確立するために使用されます。
Router ID	仮想リンクネイバのルータ ID を入力します。
Hello Interval	ルータが仮想リンクで送信する Hello パケットの送信間隔を指定します。「Default」オプションにチェックを入れると、初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead Interval	Hello パケットの最後の受信から、ネイバがオフラインになったと判断するまでの Dead インターバル を入力します。「Default」オプションにチェックを入れると、初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
Authentication	使用する認証を選択します。 • 選択肢：「Null」「Simple Password」「MD5」
Password	「Authentication」で「Simple Password」を選択した場合、パスワードを入力します。(8 文字以内)
MD5 Key ID	「Authentication」で「MD5」を選択した場合、MD5 認証キー ID を入力します。 • 設定可能範囲：1-255
MD5 Key	「Authentication」で「MD5」を選択した場合、MD5 認証キーを指定します。(16 文字以内)
OSPF Virtual Link Table	
VRF Name (EI モードのみ)	VRF インスタンス名を入力します。(12 文字以内)「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。

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

テーブル内のエントリをダブルクリックすると次の画面が表示されます。

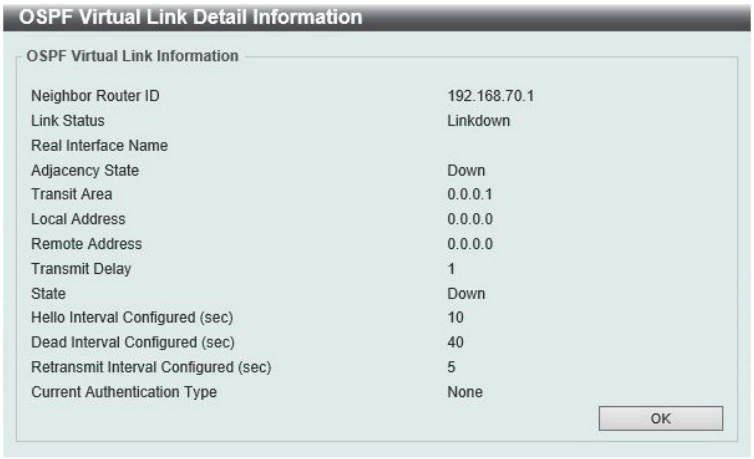


図 9-62　OSPFv2 Virtual Link Settings (Double Click) - OSPF Virtual Link Detail Information 画面

「OK」ボタンをクリックして、画面を閉じます。

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 の順にメニューをクリックし、以下の画面を表示します。

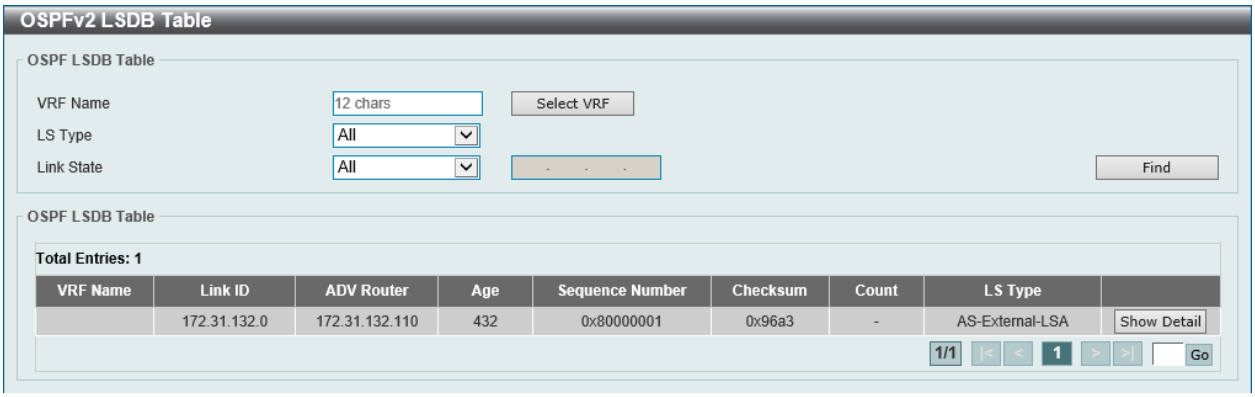


図 9-63　OSPFv2 LSDB Table 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
LS Type	表示する LSDB タイプを指定します。 • 選択肢：「All」「Router」「Network」「Summary」「ASBR Summary」「External」「Stub」「NSSA External」
Link State	表示するリンクステート情報を選択します。 • 「All」- 全ての OSPFv2 リンクステート情報を表示します。 • 「Link State ID」- 指定するリンクステート ID に関する情報を表示します。表示される入力欄にリンクステート ID を入力します。 • 「Self-Originate」- ローカルルータによって生成された LSA を表示します。 • 「Adv Router」- 通知ルータによって生成された全ての LSA を表示します。通知ルータ ID を空欄に入力します。

「Find」ボタンをクリックして、指定したエントリを検索します。
「Show Detail」ボタンをクリックして、指定エントリの詳細について表示します。
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 LSDB の詳細表示

「Show Detail」をクリックすると、以下の画面が表示されます。

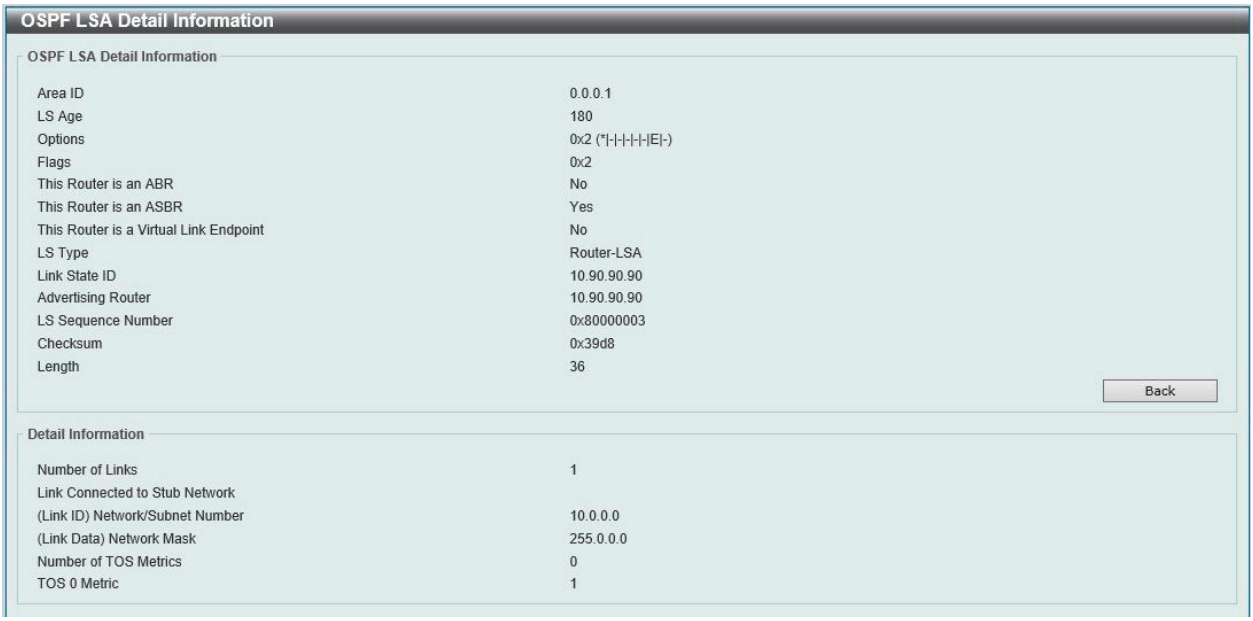


図 9-64　OSPFv2 LSDB Table（Show Detail）- OSPF LSA Detail Information 画面

前の画面に戻るには、「Back」ボタンをクリックします。

OSPFv2 Neighbor Table（OSPF Neighbor テーブル）

インタフェース毎の 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。

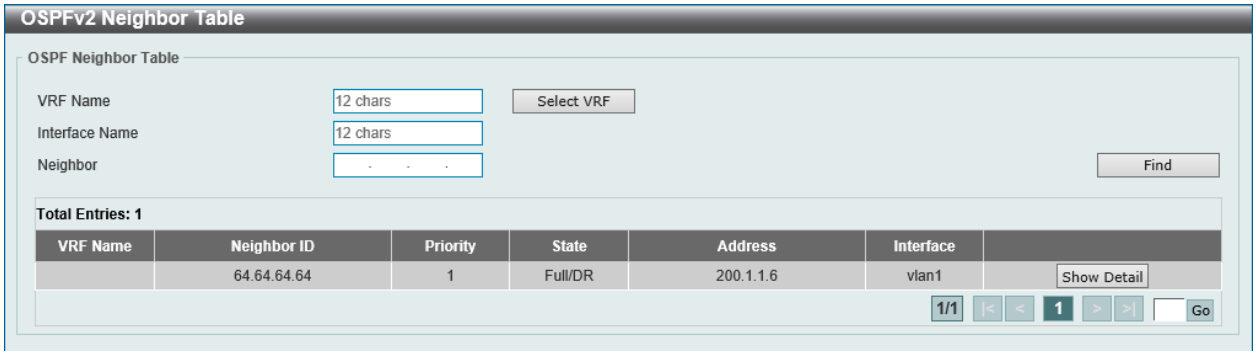


図 9-65　OSPFv2 Neighbor Table 画面

画面に表示される項目：

項目	説明
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface Name	表示するインタフェースを指定します。
Neighbor	ネイバ 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、指定した情報に基づくエントリを検索します。
「Show Detail」ボタンをクリックして、エントリの詳細を表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

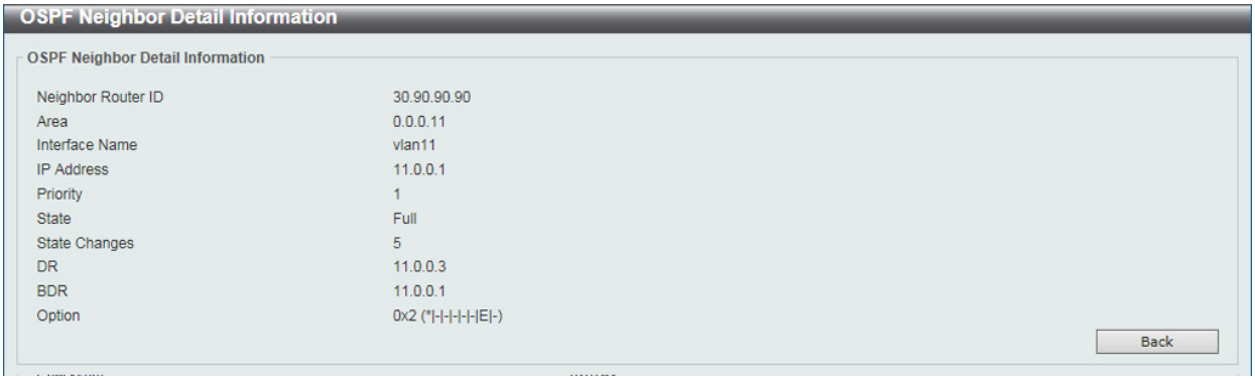


図 9-66　OSPFv2 Neighbor Table（Show Detail）- OSPF Neighbor Detail Information 画面

前の画面に戻るには、「Back」ボタンをクリックします。

OSPFv2 Host Route Settings（OSPFv2 ホストルート設定）

OSPFv2 ホストルート設定を行います。ルータは、Stub リンクのルータ LSA として特定のホストルートを通知します。

L3 Features > OSPF > OSPFv2 > OSPFv2 Host Route Settings の順にメニューをクリックし、以下の画面を表示します。

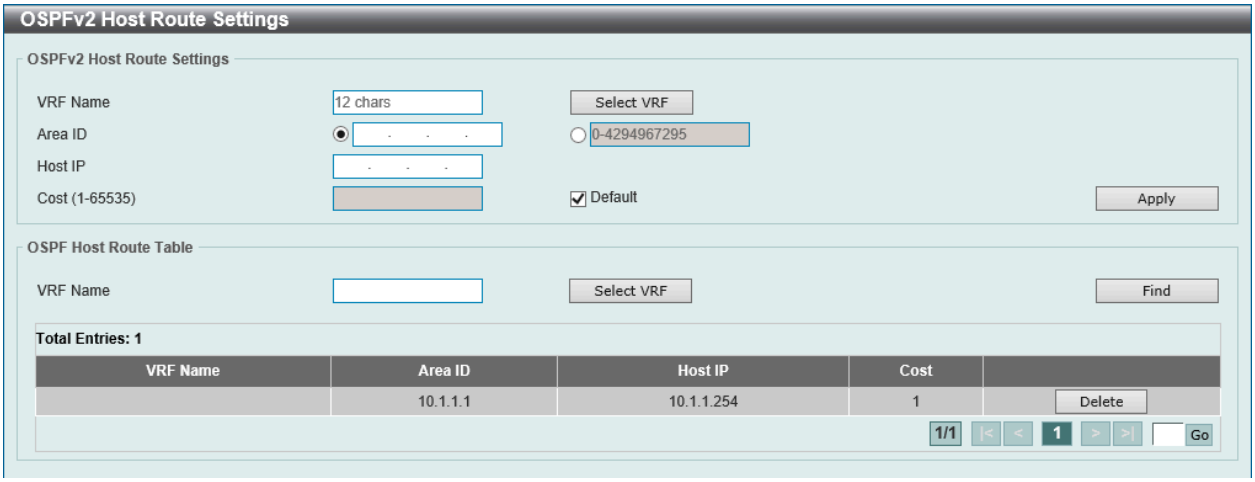


図 9-67　OSPFv2 Host Route Settings 画面

画面に表示される項目：

項目	説明
OSPFv2 Host Route Settings	
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Area ID	OSPFv2 エリア識別子を選択して入力します。IP アドレス形式（xxx.xxx.xxx.xxx）または 10 進数値形式（0-4294967295）で指定できます。このエリアは、仮想リンクを確立するために使用されます。
Host IP	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値を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535 • 初期値：1
OSPF Host Route Table	
VRF Name （EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。

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

OSPFv3

OSPFv3 Process Settings（OSPFv3 プロセス設定）

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。

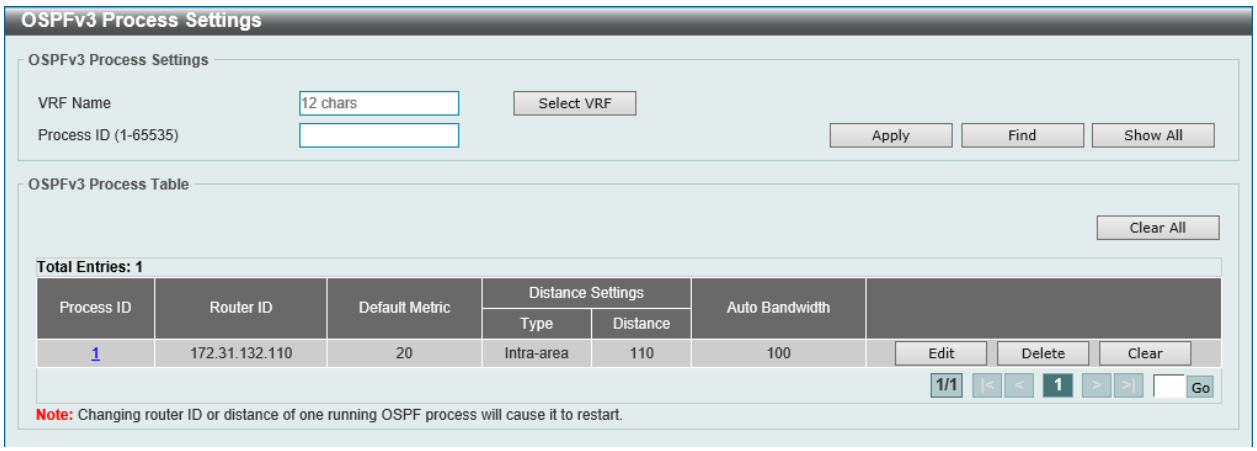


図 9-68　OSPFv3 Process Settings 画面

画面に表示される項目：

項目	説明
VRF Name (EI モードのみ)	VRF インスタンス名を入力します。(12 文字以内)「Select VRF」をクリックして、リストから VRF インスタンスを選択することも可能です。
Process ID	OSPFv3 のプロセス ID を指定します。 • 設定可能範囲：1-65535

エントリの作成・検出

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

エントリの編集・削除

「Delete」ボタンをクリックして、指定のエントリを削除します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Process ID」のリンクをクリックして、指定の OSPFv3 プロセスのへのアクセス、設定を行います。
「Clear」ボタンをクリックして、指定した OSPFv3 プロセスを再起動します。
「Clear All」ボタンをクリックして、すべての OSPFv3 プロセスを再起動します。

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。

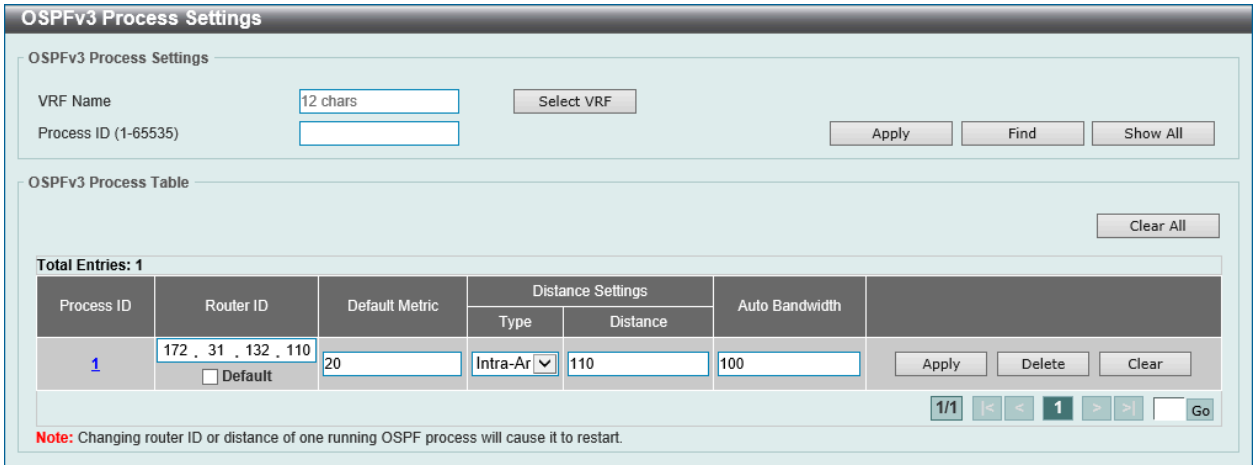


図 9-69　OSPFv3 Process Settings (Edit) 画面

画面に表示される項目：

項目	説明
Router ID	OSPF プロセスのルータ ID を入力します。デフォルトでは、ルータ ID が自動的に選択されます。 「Default」にチェックを入れると初期値に設定されます。
Default Metric	OSPF プロセスの初期メトリック値を指定します。この設定は、OSPFv3 再配布機能とともに使用され、現在のルーティングプロトコルを有効化してすべての再配布ルートに同じメトリック値を使用します。整合性のないメトリックを持つルートの再配布を行う場合、初期メトリックが役に立ちます。メトリックの直接変換ができない場合に、初期メトリックにより再配布が実行されます。 • 設定可能範囲：1-16777214 • 初期値：20
Type	ディスタンス設定種類を指定します。 •「Intra-Area」- OSPF 内エリアルートのディスタンスを指定します。 •「Inter-Area」- OSPF 間エリアルートのディスタンスを指定します。 •「External」- OSPF 外部ルートのディスタンスを指定します。
Distance	OSPF プロセスのディスタンス値を指定します。 • 設定可能範囲：1-254 • 初期値：110（全ての OSPF ルート）
Auto Bandwidth	自動帯域幅の値を指定します。インタフェースのメトリックの計算時に IPv6 OSPF が使用する参照値を制御するために使用されます。 • 設定可能範囲：1-4294967

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

「Process ID」のリンクを指定すると次の画面が表示されます。

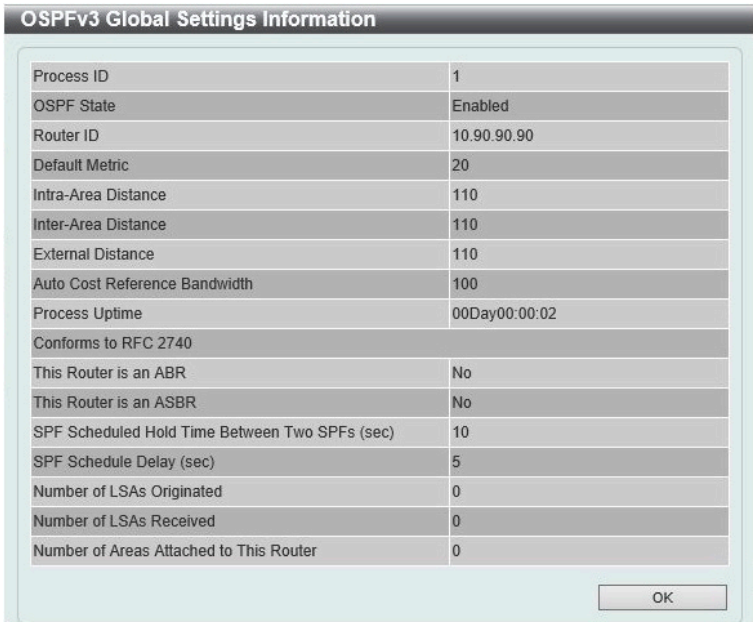


図 9-70　OSPFv3 Process Settings (Process ID) - OSPFv3 Global Settings Information 画面

「OK」ボタンをクリックして、画面を閉じます。

OSPFv3 Passive Interface Settings（OSPFv3 パッシブインタフェース設定）

OSPFv3 パッシブインタフェース設定を行います。インタフェースがパッシブ（受動）の場合、OSPF ルーティングアップデートパケットは指定のインタフェースを通じて送受信されなくなります。

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

画面に表示される項目：

項目	説明
Process ID	OSPFv3 のプロセス ID を指定します。 • 設定可能範囲：1-65535
Interface Name	パッシブインタフェース名（12 文字以内）を指定します。「Default」を選択すると、すべてのインタフェースがパッシブインタフェースとして指定されます。

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

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。

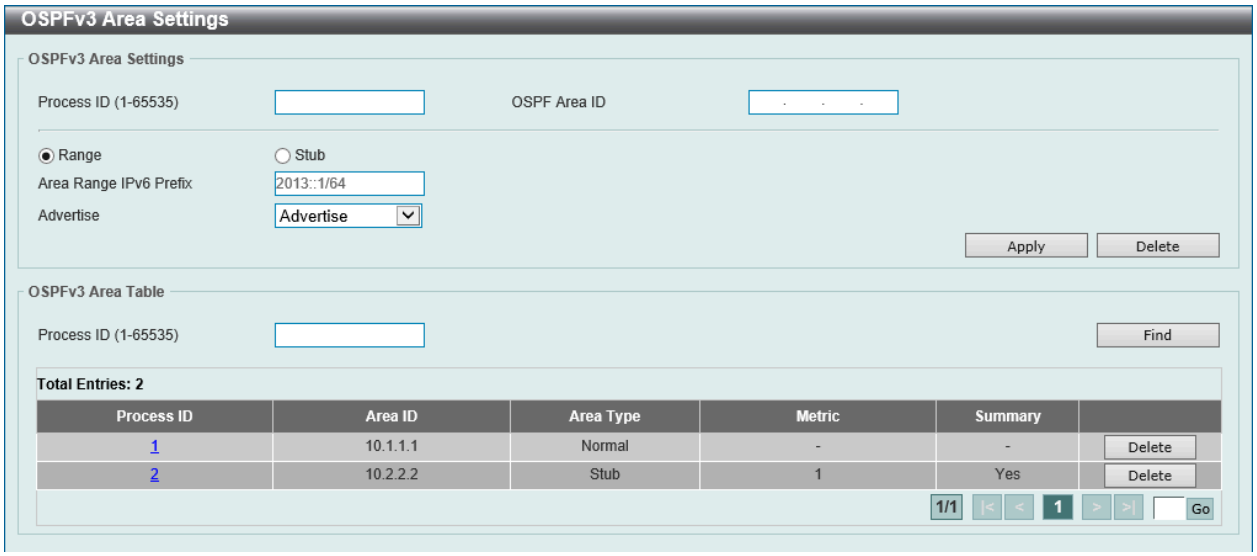


図 9-72　OSPFv3 Area Settings（Range）画面

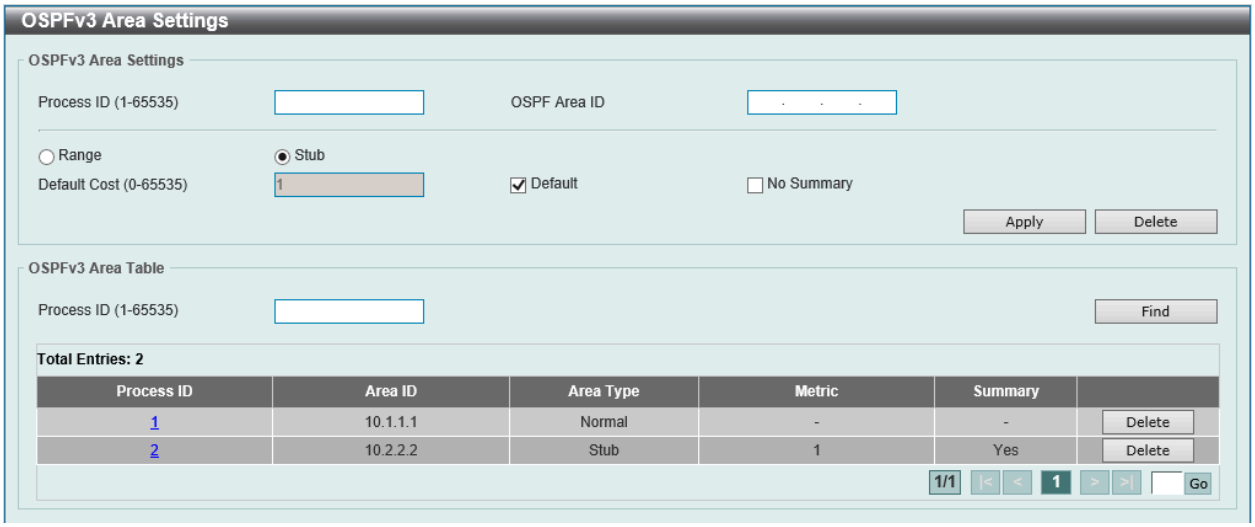


図 9-73　OSPFv3 Area Settings（Stub）画面

画面に表示される項目：

項目	説明
OSPFv3 Area Settings	
Process ID	OSPF のプロセス ID を指定します。 • 設定可能範囲：1-65535
OSPF Area ID	OSPF エリア ID を入力します。IPv4 アドレス形式で指定します。
Range	Area Border Router (ABR) で OSPF ルートを集約します。この機能は、ABR でのみ使用されます。エリアのルートが統合・集約され、1 つのサマリールートが ABR によって他のエリアにアドバタイズされます。ルーティング情報はエリア境界で集約されます。エリア外には、アドレス範囲ごとに 1 つのルートがアドバタイズされます。 • 「Area Range IPv6 Prefix」- OSPF エリア範囲 IPv6 プレフィックスとプレフィックス長を入力します。 • 「Advertise」- 通知オプションを選択します。 - 「Advertise」- 指定されたアドレス範囲のエリア間プレフィックス LSA をアドバタイズして生成します。 - 「No-Advertise」- 指定されたアドレス範囲のステータスを「Do-Not-Advertise」に設定します。エリア間プレフィックス LSA は抑制され、設定されたネットワークは他のネットワークから認識されない状態のままです。
Stub	エリアをスタブエリアとして定義します。 • 「Default Cost」- このエリアのデフォルトメトリック値（1）が使用されます。 • 「Default」- デフォルトのコスト値を使用します。 • 「No Summary」- ABR がエリア間プレフィックス LSA をスタブエリアに送信しないように設定します。
OSPFv3 Area Table	
Process ID	OSPF のプロセス ID を指定します。 • 設定可能範囲：1-65535

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「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。
「Process ID」のリンクをクリックして、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 9-74　OSPFv3 Area Settings 画面 - Stub

「OK」ボタンをクリックして、画面を閉じます。

「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。

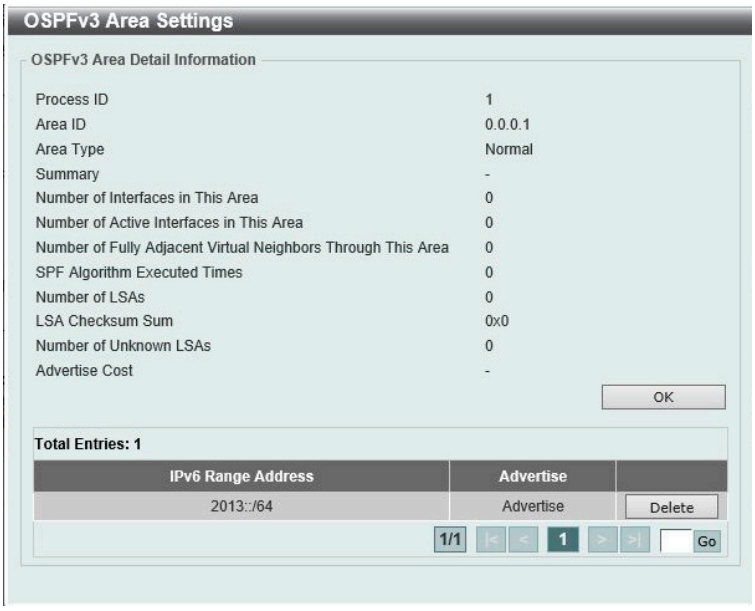


図 9-75　OSPFv3 Area Settings 画面 - Normal

「OK」ボタンをクリックして、画面を閉じます。
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。

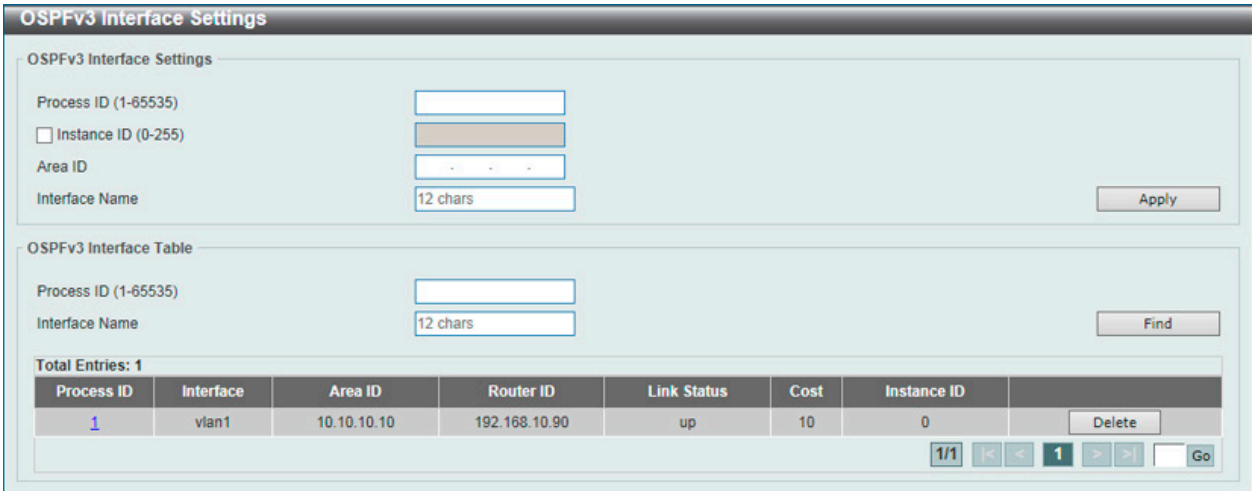


図 9-76　OSPFv3 Interface Settings 画面

画面に表示される項目：

項目	説明
OSPFv3 Interface Settings	
Process ID	IPv6 OSPF ルーティングのプロセス ID を指定します。 • 設定可能範囲：1-65535
Instance ID	インスタンス ID を指定します。 • 設定可能範囲：0-255 • 初期値：0
Area ID	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 文字以内）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 を指定します。 • 設定可能範囲：1-65535
Interface Name	インタフェース名を入力します。

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

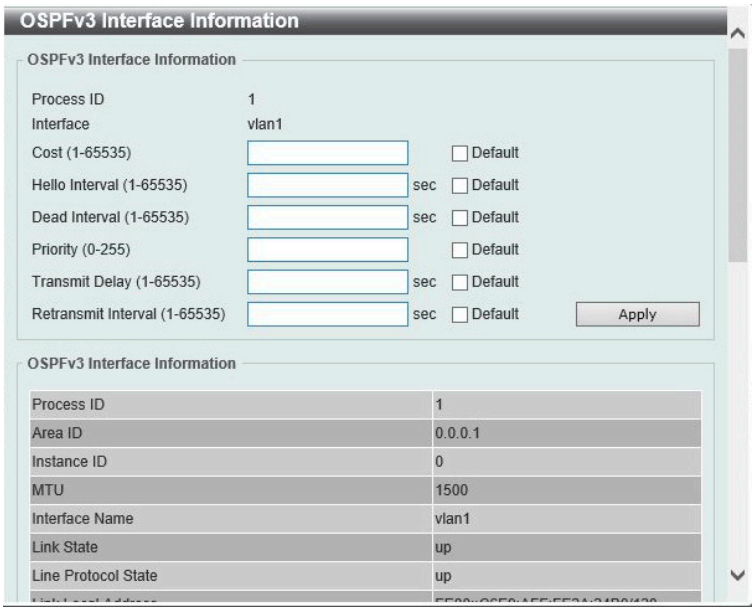


図 9-77　OSPFv3 Interface Settings 画面 - Process ID

「OK」ボタンをクリックして、画面を閉じます。

画面に表示される項目：

項目	説明
Cost	コストの値を指定します。リンク状態メトリックとして表される整数値です。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535 • 初期値：1
Hello Interval	Hello インターバル値を指定します。Hello Interval は Hello パケット内で通知されます。この間隔が短いほど、トポロジ変更の検知が早くなりますが、ルーティングトラフィックが増加します。対象ネットワーク上のすべてのルータとアクセスサーバで同じである必要があります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead Interval	Dead インターバル値を指定します。指定時間パケットが受信されない場合、ネイバがオフラインと認識されます。この値は Hello パケット内で通知されます。対象ネットワーク上のすべてのルータとアクセスサーバで同じである必要があります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
Priority	ルータのプライオリティを指定します。OSPF ルータは、ネットワークの代表ルータ（Designated Router/DR）を選出するために使用されます。2 台のルータがルータになろうとしている場合、高いプライオリティのルータが選出されます。同じプライオリティ値を持つ場合は、ルータ ID の高い方が優先されます。「0」の場合は代表ルータまたはバックアップ代表ルータ（BDR）として選出されません。（ポイントツーポイントではなく）マルチアクセスネットワークのみにルータプライオリティを設定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-255 • 初期値：1
Transmit Delay	Transmit Delay（送信遅延）の値を入力します。Link State Updates（LSU）は、その送信前に seconds 引数で指定された分を増加させます。設定する値は、インタフェースの伝送・伝播遅延を考慮する必要があります。 リンク上での送信の前に遅延時間が追加されない場合、LSA の伝播時間は考慮されません。この設定は、低速のリンクでは重要になります。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：1（秒）
Retransmit Interval	Retransmit Interval（再送信間隔）の値を指定します。ネイバに LSA を送信した後、ルータは Ack 応答を受信するまで LSA を保持します。指定時間（「Retransmit Interval」）ルータが応答を受信しなかった場合、LSA を再送信します。不要な再送信を減らすために、再送信間隔は控えめに指定することを推奨します。この間隔は、2 つのルータ間で予想される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。 • 設定可能範囲：1-65535（秒） • 初期値：5（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

OSPFv3 Redistribute Settings（OSPFv3 再配布設定）

OSPFv3 再配布について設定、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。

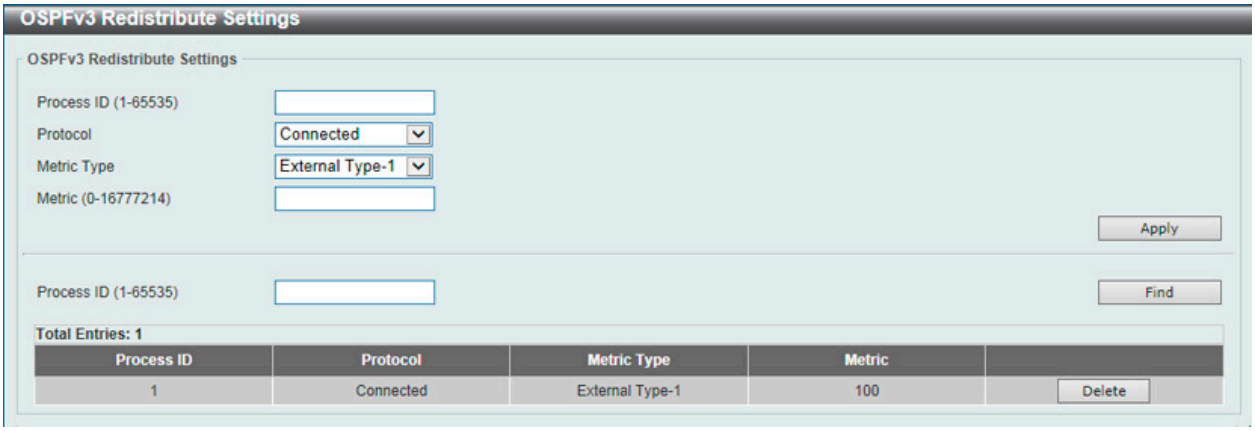


図 9-78　OSPFv3 Redistribute Settings 画面

画面に表示される項目：

項目	説明
Process ID	IPv6 OSPF ルーティングのプロセス ID を指定します。ローカルに割り当てられる値であり、ルータの IPv6 OSPF ルーティングプロセス毎に一意である必要があります。 • 設定可能範囲：1-65535
Protocol	再配布される送信元プロトコルを指定します。 • 選択肢：「Connected」「Static」「RIPng」「BGP（EI モードのみ）」「ISIS（EI モードのみ）」
Metric Type	IPv6 OSPF ルーティングドメインに通知されるデフォルトルートの外部リンクタイプを指定します。メトリックタイプを指定しない場合、スイッチは「Type-2」外部ルートを採用します。これは IPv6 OSPF のみに適用されます。 • 選択肢：「External Type-1」「External Type-2」
Metric	メトリック値を指定します。この設定は、他のプロセスを IPv6 OSPF プロセスに再配布する際に使用されます。 • 設定可能範囲：0-16777214 • 初期値：20

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

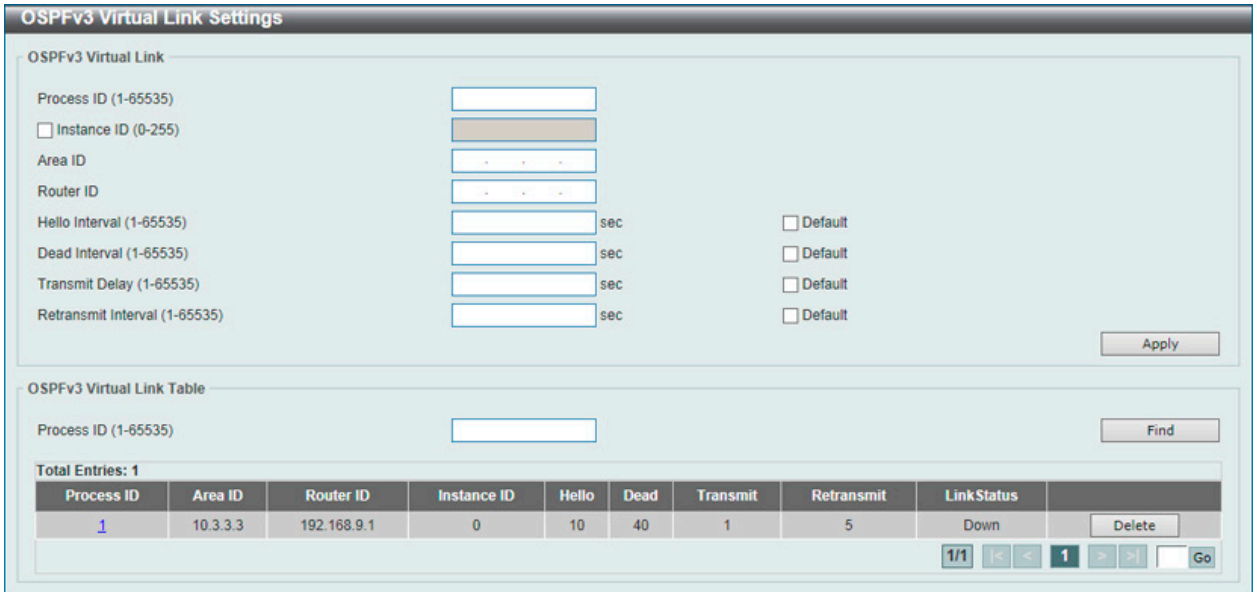


図 9-79　OSPFv3 Virtual Link Settings 画面

画面に表示される項目：

項目	説明
OSPFv3 Virtual Link	
Process ID	IPv6 OSPF ルーティングのプロセス ID を指定します。ローカルに割り当てられる値であり、ルータの IPv6 OSPF ルーティングプロセス毎に一意である必要があります。 • 設定可能範囲：1-65535
Instance ID	インスタンス ID を入力します。 • 設定可能範囲：0-255
Area ID	OSPF エリア ID を IPv4 アドレス形式で入力します。
Router ID	仮想リンクネイバのルータ ID を入力します。
Hello Interval	ルータがインタフェース上で送信する Hello パケットの送信間隔を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲： 1-65535（秒） • 初期値：10（秒）
Dead Interval	Dead インターバル値を指定します。指定時間パケットが受信されない場合、ネイバがオフラインと認識されます。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
Transmit Delay	ルータがパケットを送信するまでに待機する時間を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲： 1-65535（秒） • 初期値：1（秒）
Retransmit Interval	ルータがパケットを再送信するまでに待機する時間を指定します。「Default」にチェックを入れると初期値に設定されます。 • 設定可能範囲： 1-65535（秒） • 初期値：5（秒）
OSPFv3 Virtual Link Table	
Process ID	IPv6 OSPF ルーティングのプロセス ID を指定します。 • 設定可能範囲：1-65535

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

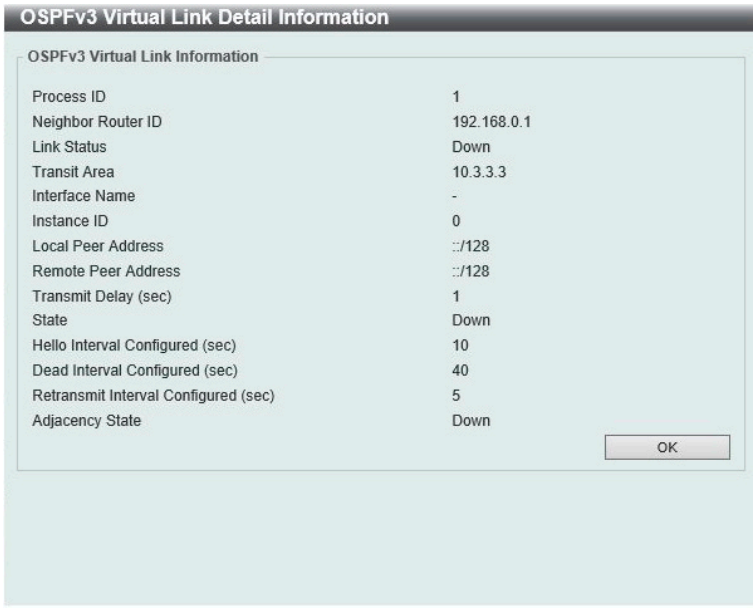


図 9-80　OSPFv3 Virtual Interface Settings（Edit）- OSPFv3 Virtual Link Detail Information 画面

「OK」ボタンをクリックして、画面を閉じます。

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。

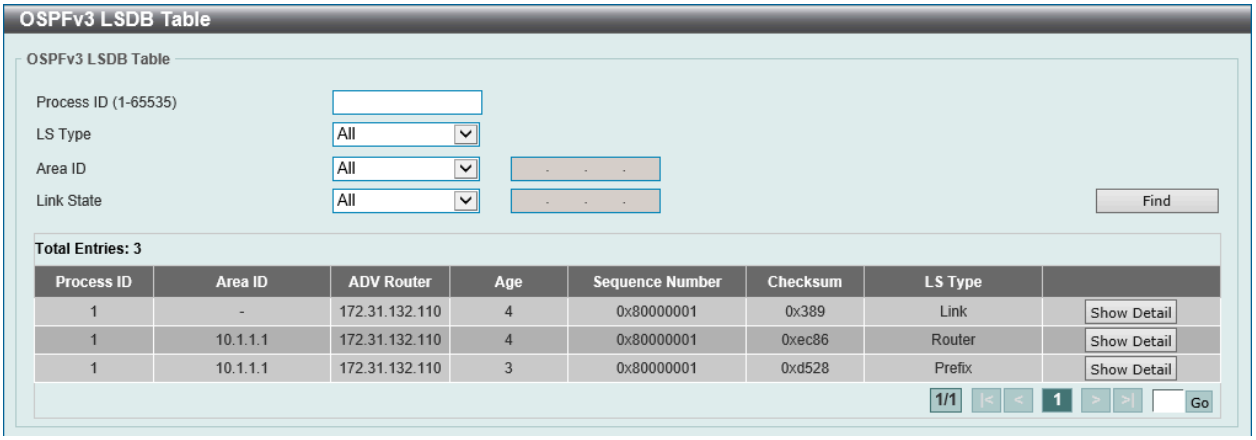


図 9-81　OSPFv3 LSDB Table 画面

画面に表示される項目：

項目	説明
Process ID	IPv6 OSPF ルーティングのプロセス ID を指定します。ローカルに割り当てられる値であり、ルータの IPv6 OSPF ルーティングプロセス毎に一意である必要があります。 • 設定可能範囲：1-65535
LS Type	表示する LSDB の種類を指定します。 • 「All」- すべての種類の LSDB 情報を表示します。 • 「Router LSA」- ルータ LSA の情報のみ表示します。 • 「Network LSA」- ネットワーク LSA の情報のみ表示します。 • 「Prefix」- エリア内プレフィックス LSA の情報を表示します。 • 「Link LSA」- リンク LSA の情報を表示します。 • 「Inter-Area Prefix LSA」- エリア間プレフィックス LSA に基づいた LSA の情報のみ表示します。 • 「Inter-Area Router LSA」- エリア間ルータ LSA に基づいた LSA の情報のみ表示します。 • 「AS-External-LSA」- 外部 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。指定されたエリアのすべての LSA を表示するには、「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。 • 選択肢：「All」「Area ID」

項目	説明
Link State	表示するリンクステート情報を選択します。 • 「All」- 全ての OSPFv2 リンクステート情報を表示します。 • 「Self-Originate」-（ローカルルータによって生成された）自己発信 LSA を表示します。 • 「Adv Router」- 通知ルータによって生成された全ての LSA を表示します。通知ルータ ID を IPv4 アドレス形式で空欄に入力します。

「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

「Show Detail」をクリックすると、以下の画面が表示されます。



図 9-82　OSPFv3 LSDB Router LSA Table（Show Detail）- OSPFv3 LSA Detail Information 画面

前の画面に戻るには、「Back」ボタンをクリックします。

OSPFv3 Neighbor Table（OSPFv3 ネイバテーブル）

OSPFv3 ネイバ情報を表示します。

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 9-83　OSPFv3 Neighbor Table 画面

画面に表示される項目：

項目	説明
Process ID	OSPFv3 プロセス ID を指定します。 • 設定可能範囲：1-65535
Interface VLAN	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Neighbor	OSPF ネイバ ID を入力します。IPv4 アドレスで指定します。

「Find」ボタンをクリックして、指定したエントリを検索します。

エントリの詳細表示

「Show Detail」をクリックすると、以下の画面が表示されます。



図 9-84　OSPFv3 Neighbor Table (Show Detail) - OSPFv3 Neighbor Detail Information 画面

前の画面に戻るには、「Back」ボタンをクリックします。

OSPFv3 Border Router Table（OSPFv3 境界ルータテーブル）

OSPFv3 境界ルータ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。

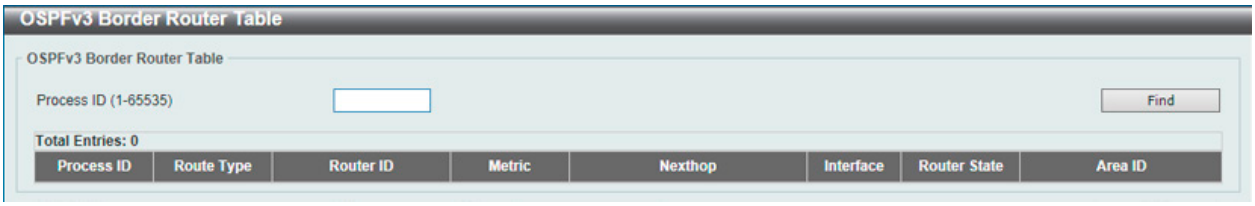


図 9-85　OSPFv3 Border Router Table 画面

画面に表示される項目：

項目	説明
Process ID	検索する OSPFv3 プロセス ID を指定します。 • 設定可能範囲：1-65535

「Find」ボタンをクリックして、入力した情報に基づくエントリを検索します。

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 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）

インタフェースごとに IGMP（Internet Group Management Protocol）設定を行います。

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。

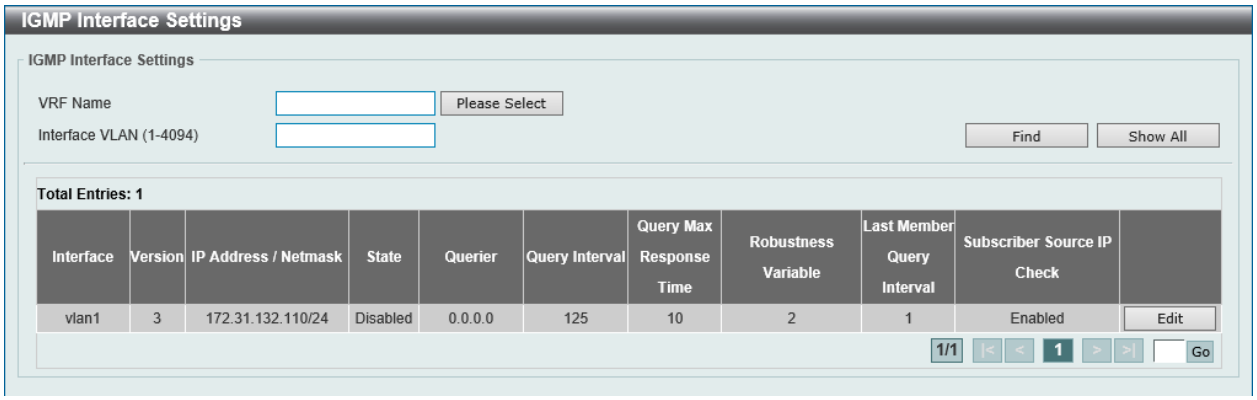


図 9-86　IGMP Interface Settings 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。（12 文字以内）「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface VLAN	本設定に使用するインタフェース VLAN を指定します。 • 設定可能範囲：1-4094

「Find」ボタンをクリックして、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
「Edit」ボタンをクリックして、以下の画面を表示します。

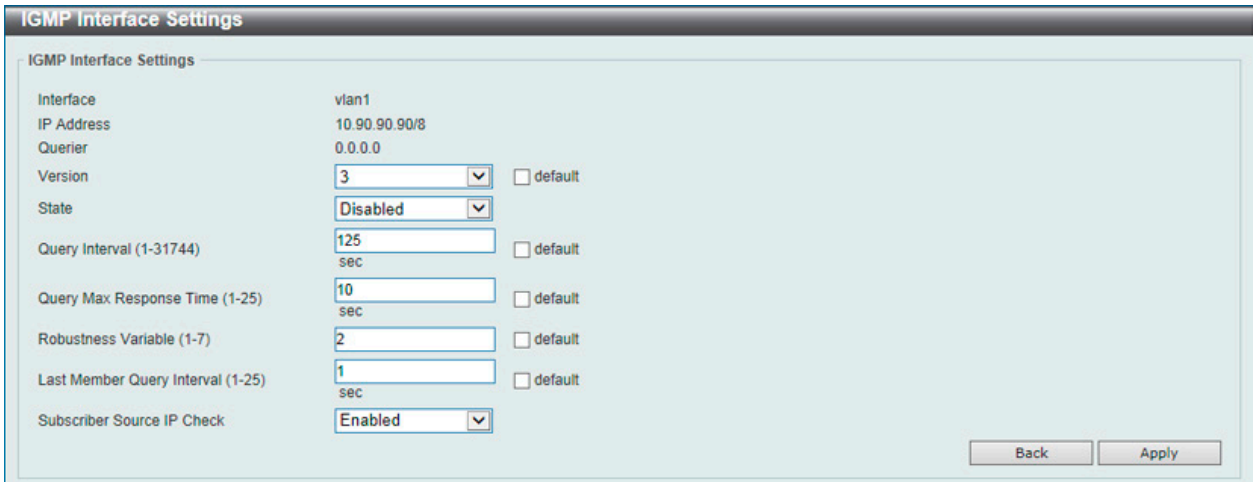


図 9-87　IGMP Interface Settings - Edit 画面

画面に表示される項目：

項目	説明
Version	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。 • 選択肢：「1」「2」「3」 • 初期値：「3」

項目	説明
State	インタフェースの IGMP ステータスを有効 / 無効に設定します。
Query Interval	IGMP クエリを送信する間隔を指定します。IGMP クエリアは、指定された間隔で IGMP クエリメッセージを送信し、マルチキャストグループへ参加しようとしているレシーバを検出します。この問い合わせに対し、ホストは参加するマルチキャストグループを示す IGMP レポートメッセージで応答します。「Default」を指定すると初期値を使用します。 • 設定可能範囲：1-31744（秒）
Query Max Response Time	グループメンバが IGMP クエリメッセージに対して応答可能な時間を指定します。この時間を超えると、ルータによりメンバシップが削除されます。「Default」を指定すると初期値を使用します。 • 設定可能範囲：1-25（秒）
Robustness Variable	ロバストネス変数の値を指定します。この値は、インタフェース上で予想されるパケット損失を許容するための調整に使用されます。「Default」を指定すると初期値を使用します。 • 設定可能範囲：1-7
Last Member Query Interval	Last Member Query Interval 値を入力します。ルータは、グループまたはチャネルを離れるための Leave メッセージをレシーバから受信すると、Group Specific Query または Group-Source Specific Query メッセージをレシーバインタフェースに送信します。IGMP Last Member Query Interval は、クエリメッセージでアドバタイズされ、レシーバに送信されます。本設定は、特定のグループまたはチャネルのレシーバからのレポートがない場合に、ルータが次の Group Specific Query または Group-Source Specific Query クエリメッセージを送信する期間を指定します。ルータは、最後のメンバクエリカウントを再試行します。再試行回数後にレポートメッセージが受信されない場合、インタフェースは特定のグループまたはチャネルからメンバシップを削除します。 「Default」を指定すると初期値を使用します。 • 設定可能範囲：1-25（秒）
Subscriber Source IP Check	サブスクライバ送信元 IP チェック機能を有効 / 無効に設定します。デフォルトでは、インタフェースで受信された IGMP レポートまたは Leave メッセージは、その送信元 IP がインタフェースと同じネットワーク内にあるかどうかチェックされます。同じネットワークに存在しない場合、メッセージ情報は IGMP プロトコルによって学習されません。

項目を編集後、「Apply」ボタンをクリックします。
前の画面に戻るには、「Back」ボタンをクリックします。

IGMP Static Group Settings（IGMP スタティックグループ設定）

IGMP スタティックグループを設定します。接続されたホストが IGMP プロトコルをサポートしていない場合、IGMP スタティックグループを作成します。設定が完了すると、グループメンバエントリが IGMP キャッシュに追加されます。

L3 Features > IP Multicast Routing Protocol > IGMP > IGMP 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。

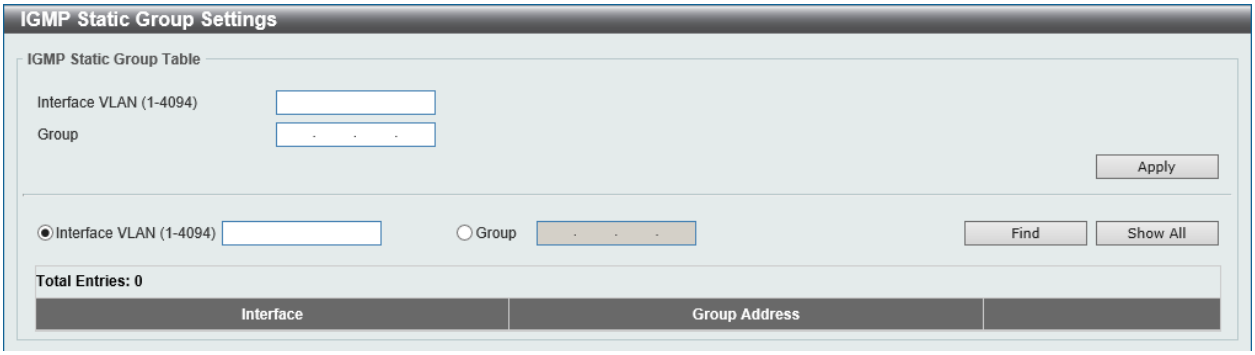


図 9-88　IGMP Static Group Settings 画面

画面に表示される項目：

項目	説明
Interface VLAN	本設定に使用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Group	IP マルチキャストグループアドレスを指定します。

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

IGMP Dynamic Group Table（IGMP ダイナミックグループテーブル）

IGMP ダイナミックグループ情報の表示、設定を行います。

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。

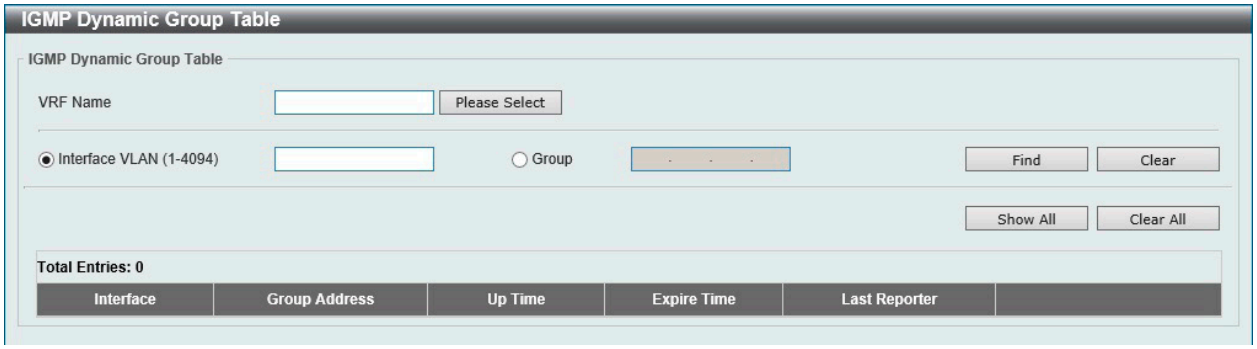


図 9-89　IGMP Dynamic Group Table 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。（12 文字以内）「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface VLAN	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Group	IP マルチキャスト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。
「Clear」ボタンをクリックして、入力した情報に基づきエントリをクリアします。
「Clear All」ボタンをクリックして、すべてのエントリをクリアします。
「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。

IGMP SSM Mapping Settings（IGMP SSM マッピング設定）

IGMP SSM マッピングの設定、表示を行います。Source Specific Multicast（SSM）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単に行うことができます。

SSM が有効な場合、ラストホップルータは、接続された IGMPv3 ホストから SSM 範囲に含まれる INCLUDE リクエスト（S,G）を受信すると、チャネル（S,G）の送信元ベースのツリーを構築します。

接続されたホストが(*,G)要求のみを発行する IGMPv1 または IGMPv2 ホストである場合があります。SSM マッピングでは、要求されているマルチキャストグループが SSM 範囲内にある場合、定義されているグループアドレスと送信元アドレスのマッピングに基づいて、ルータは（*,G）を（S,G）要求にマッピングできます。その後、ルータはマッピングされた(S,G)の送信元ベースのツリーを確立します。複数のアソシエーションが存在する場合、ルータは各 S に対して（S,G）送信元ベースのツリーを確立します。

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。

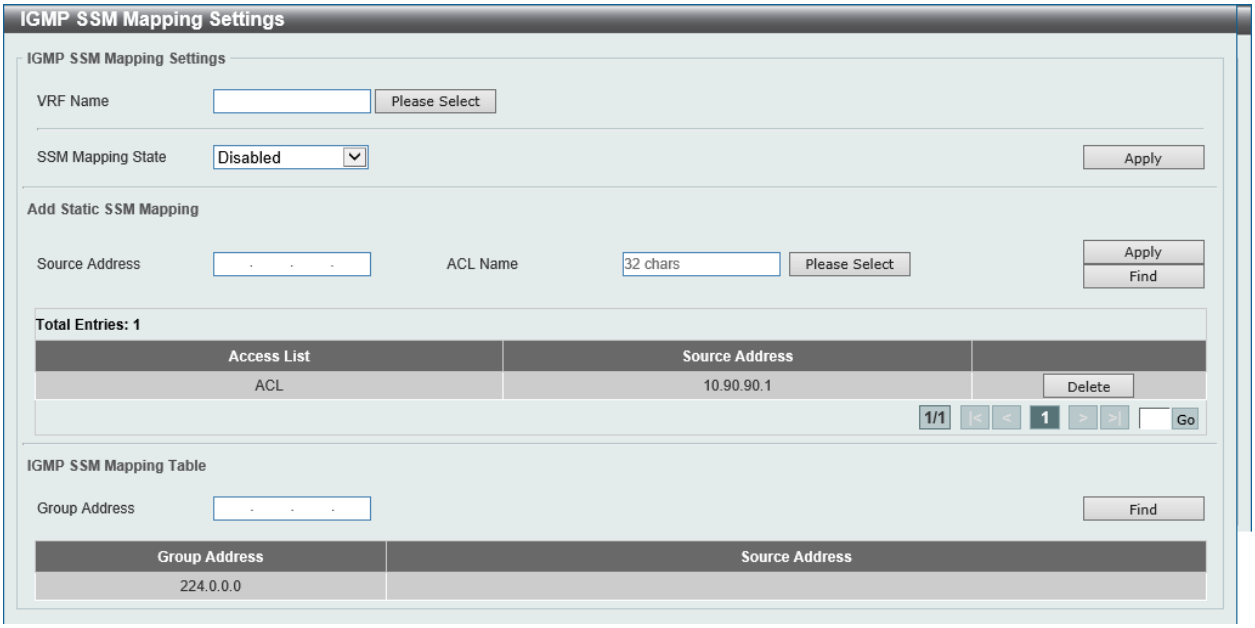


図 9-90　IGMP SSM Mapping Settings 画面

画面に表示される項目：

項目	説明
IGMP SSM Mapping Settings	
VRF Name	VRF インスタンス名を入力します。（12 文字以内）「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
SSM Mapping State	IGMPv1/IGMPv2 ホストの SSM マッピング機能を有効 / 無効に設定します。
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	マッピングす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」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
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 9-91　IGMP SSM Mapping Settings (Please Select) - ACL Access List 画面

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

MLD（MLD 設定）（EI モードのみ）

Multicast Listener Discovery（MLD）の設定を行います。

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。

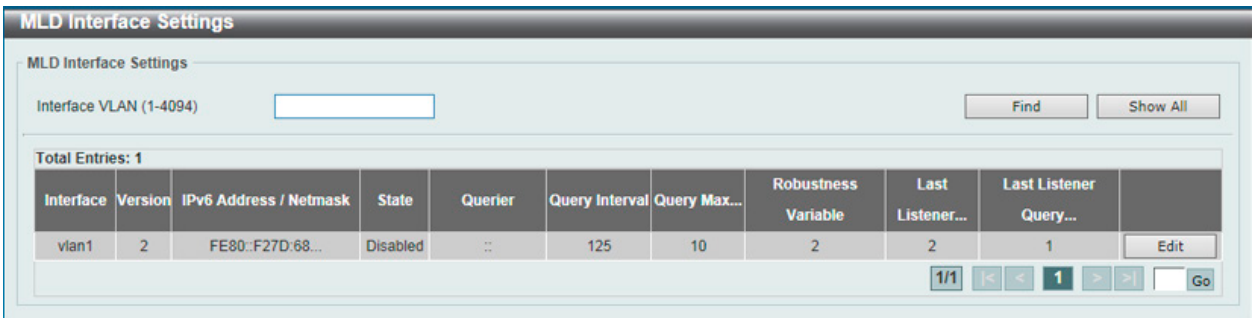


図 9-92　MLD Interface Settings 画面

画面に表示される項目：

項目	説明
Interface VLAN	インタフェース VLAN を指定します。 • 設定可能範囲：1-4094

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

■ エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

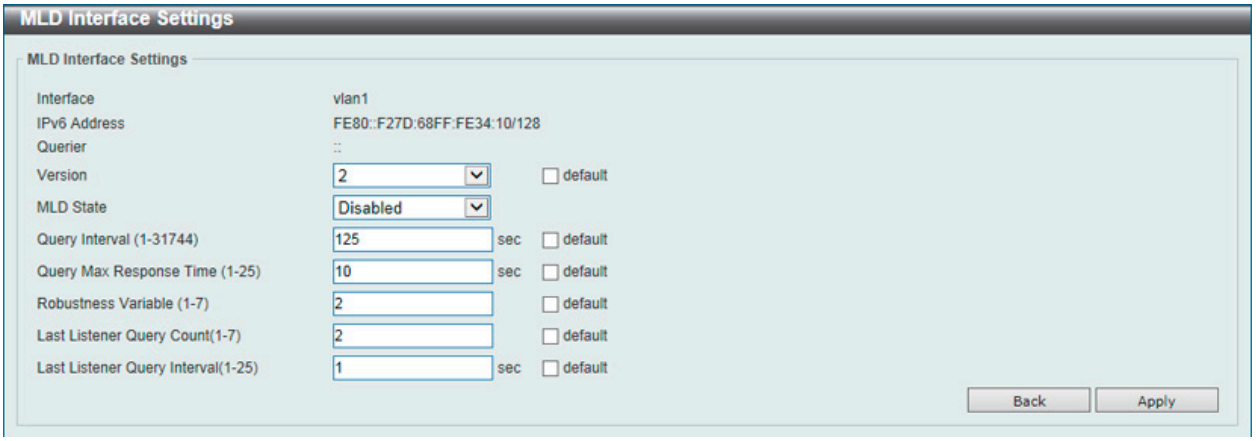


図 9-93　MLD Interface Settings（Edit）画面

画面に表示される項目：

項目	説明
Version	インタフェースで使用する MLD 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。 • 選択肢：「1」「2」 • 初期値：「2」
MLD State	インタフェースの MLD を有効 / 無効に設定します。
Query Interval	代表ルータが MLD General クエリメッセージを送信する間隔を指定します。General クエリを受信すると、MLD リスナはレポートパケットに応答して、指定されたマルチキャストグループへの参加を要求します。「Default」を指定すると初期値を使用します。 • 設定可能範囲：1-31744（秒） • 初期値：125（秒）
Query Max Response Time	クエリメッセージに対する最大応答時間を指定します。MLD クエリ内でアドバタイズされます。「Default」を指定すると初期値を使用します。 • 設定可能範囲：1-25（秒） • 初期値：10（秒）
Robustness Variable	ロバストネス変数の値を指定します。この値は、インタフェース上で予想されるパケット損失を許容するための調整に使用されます。「Default」を指定すると初期値を使用します。 • 設定可能範囲：1-7 • 初期値：2
Last Listener Query Count	「group-specific」または「group-source specific」クエリが指定回数送信されると、ルータはグループ内にローカルメンバがいないと判断します。ルータがタイムアウトまでにホストからレポートを受信しない場合、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を使用します。 • 設定可能範囲：1-7 • 初期値：2
Last Member Query Interval	Group Specific Query または Group-Source Specific Query メッセージのクエリ間隔を指定します。MLD クエリアは、グループまたはチャネルを離れるための Leave メッセージをレシーバから受信すると、Group Specific Query または Group-Source Specific Query メッセージをレシーバインタフェースに送信します。MLD クエリアがインタフェース上でパケットを受信すると、Leave タイマが開始されます。タイマが期限切れになるまでにインタエースでレポートパケットを受信しない場合、インタフェースのメンバシップは、離脱しているグループまたはチャネルから削除されます。「Default」を指定すると初期値を使用します。 • 設定可能範囲：1-25（秒） • 初期値：1（秒）

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

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。接続されたホストが MLD プロトコルをサポートしていない場合、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。

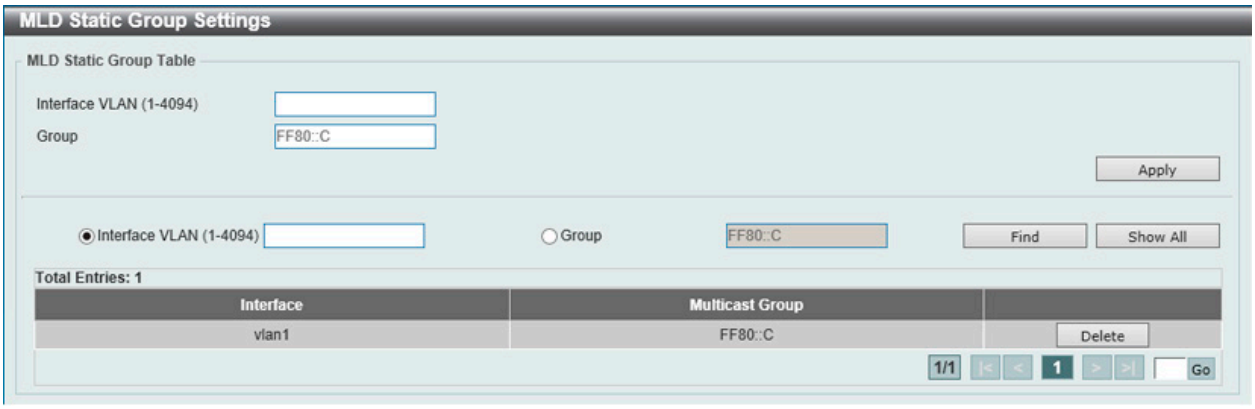


図 9-94　MLD Static Group Settings 画面

画面に表示される項目：

項目	説明
Interface VLAN	本設定に使用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Group	IPv6 マルチキャストグループアドレスを指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

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

MLD Group Table（MLD グループテーブル）

MLD 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 9-95　MLD Group Table 画面

画面に表示される項目：

項目	説明
Interface VLAN	検索する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Group	検索する IPv6 マルチキャスト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、入力した情報を基にエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

MLD SSM Mapping Settings（MLD SSM マッピング設定）

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。

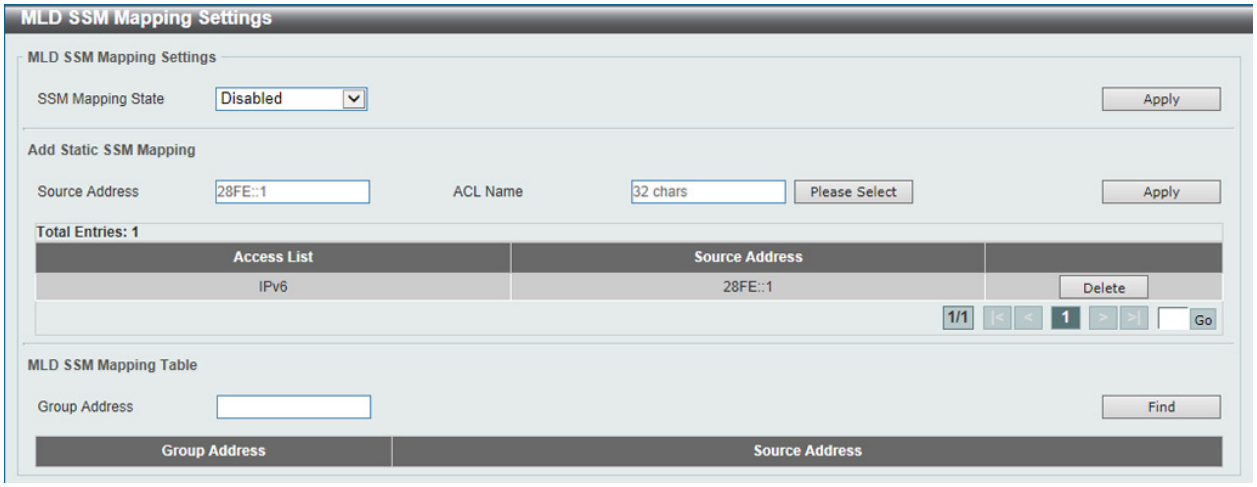


図 9-96　MLD SSM Mapping Settings 画面

画面に表示される項目：

項目	説明
MLD SSM Mapping Settings	
SSM Mapping State	MLD SSM マッピング機能を有効 / 無効に設定します。
Add Static SSM Mapping	
Source Address	グループの MLD メンバシップに関連付ける送信元アドレスを入力します。これは、アクセスリストによって識別されます。
ACL Name	標準 IPv6 アクセスリストの名前（32 文字以内）を指定します。「Please Select」を指定し、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」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
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 9-97　MLD SSM Mapping Settings (Please Select) - ACL Access List 画面

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

IGMP Proxy（IGMP プロキシ）（EI モードのみ）

IGMP プロキシ設定の表示と設定を行います。IGMP プロキシは、単純なツリートポロジでのみ機能します。ツリートポロジにプロキシデバイス以外のマルチキャストルータがないことを確認します。IGMP レポートパケットをダウンストリームインタフェースから受信すると、IGMP プロキシはメンバシップデータベースを更新します。このデータベースは、ダウンストリームインタフェースのすべてのサブスクリプションの統合により生成されます。データベースが変更されると、プロキシデバイスは Unsolicited レポートを送信するか、アップストリームインタフェースから離脱します。また、クエリを受信したときは、アップストリームインタフェースからメンバシップレポートを送信することもできます。

IGMP Proxy Settings（IGMP プロキシ設定）

IGMP プロキシを設定します。

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。

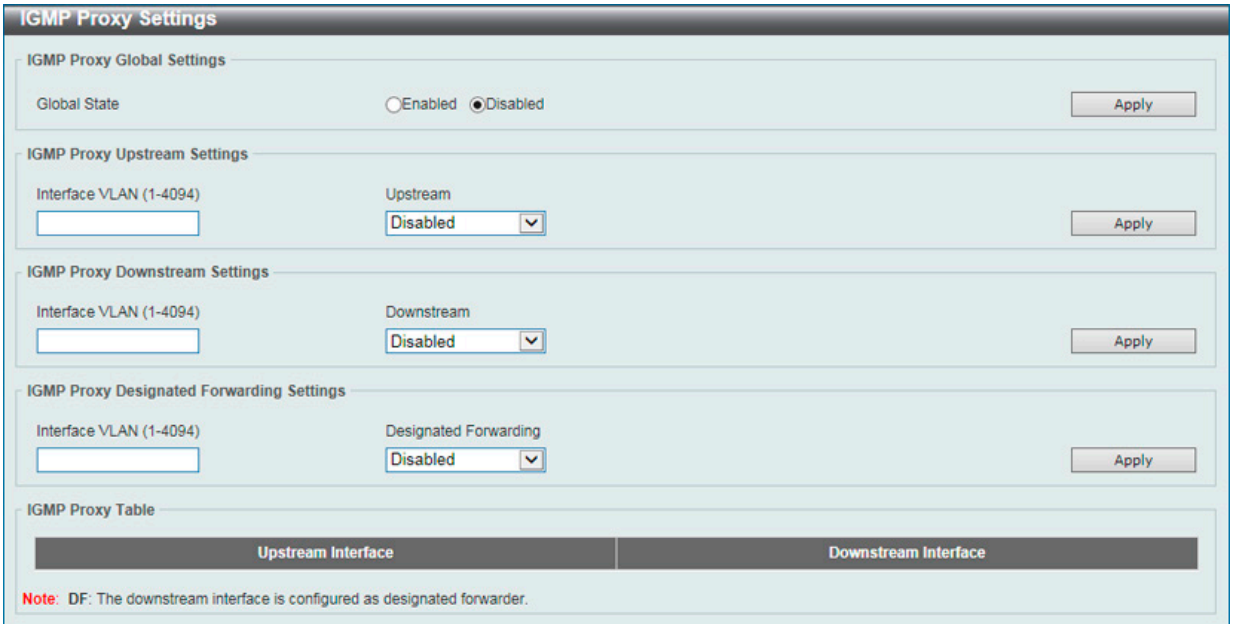


図 9-98　IGMP Proxy Settings 画面

画面に表示される項目：

項目	説明
IGMP Proxy Global Settings	
Global State	IGMP プロキシのグローバルステータスを有効 / 無効に設定します。
IGMP Proxy Upstream Settings	
Interface VLAN	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Upstream	アップストリーム IGMP プロキシとしてインタフェースを有効 / 無効に設定します。
IGMP Proxy Downstream Settings	
Interface VLAN	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094

項目	説明
Downstream	ダウンストリーム IGMP プロキシとしてインタフェースを有効 / 無効に設定します。
IGMP Proxy Designated Forwarding Settings	
Interface VLAN	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Designated Forwarding	非クエリア 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を有効 / 無効に設定します。複数の IGMP ベースのフォワーダによるダウンストリームリンクとみなされるリンクのローカルループと冗長トラフィックを回避するために、IGMP クエリアの選出を使用して、IGMP プロキシは LAN 上で単一のフォワーダを選択します。非クエリアデバイスをフォワーダにするには、このオプションを使用します。この機能は、インタフェースがダウンストリームインタフェースとして設定されていない場合、またはアップストリームインタフェースとして設定されている場合は有効になりません。

「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 プロキシグループを表示します。

L3 Features > IP Multicast Routing Protocol > 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。

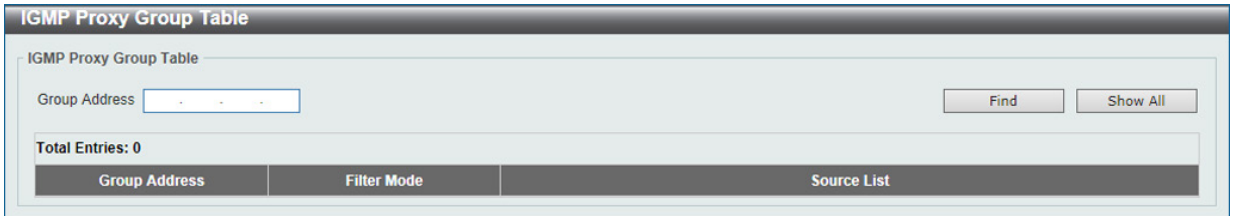


図 9-99　IGMP Proxy Group Table 画面

画面に表示される項目：

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

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。

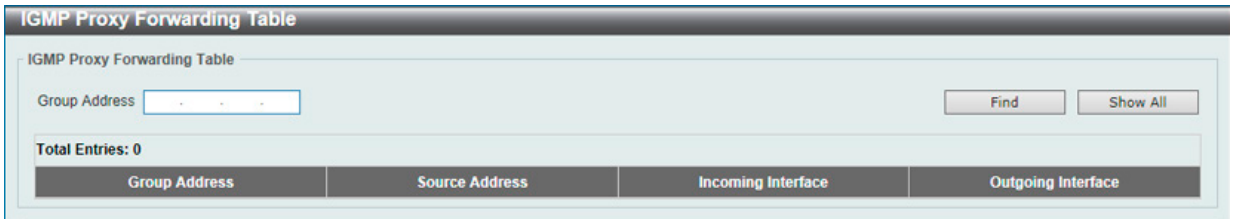


図 9-100　IGMP Proxy Forwarding Table 画面

画面に表示される項目：

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

MLD Proxy（MLD プロキシ）（EI モードのみ）

MLD プロキシ設定の表示と設定を行います。MLD プロキシは、単純なツリートポロジでのみ機能します。ツリートポロジにプロキシデバイス以外のマルチキャストルータがないことを確認します。MLD レポートパケットをダウンストリームインタフェースから受信すると、MLD プロキシはメンバシップデータベースを更新します。このパケットは、ダウンストリームインタフェースのすべてのサブスクリプションの統合により生成されます。データベースが変更されると、プロキシデバイスは Unsolicited レポートを送信するか、アップストリームインタフェースから離脱します。また、クエリを受信したときは、アップストリームインタフェースからメンバシップレポートを送信することもできます。

MLD Proxy Settings（MLD プロキシ設定）

MLD プロキシを設定します。

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。

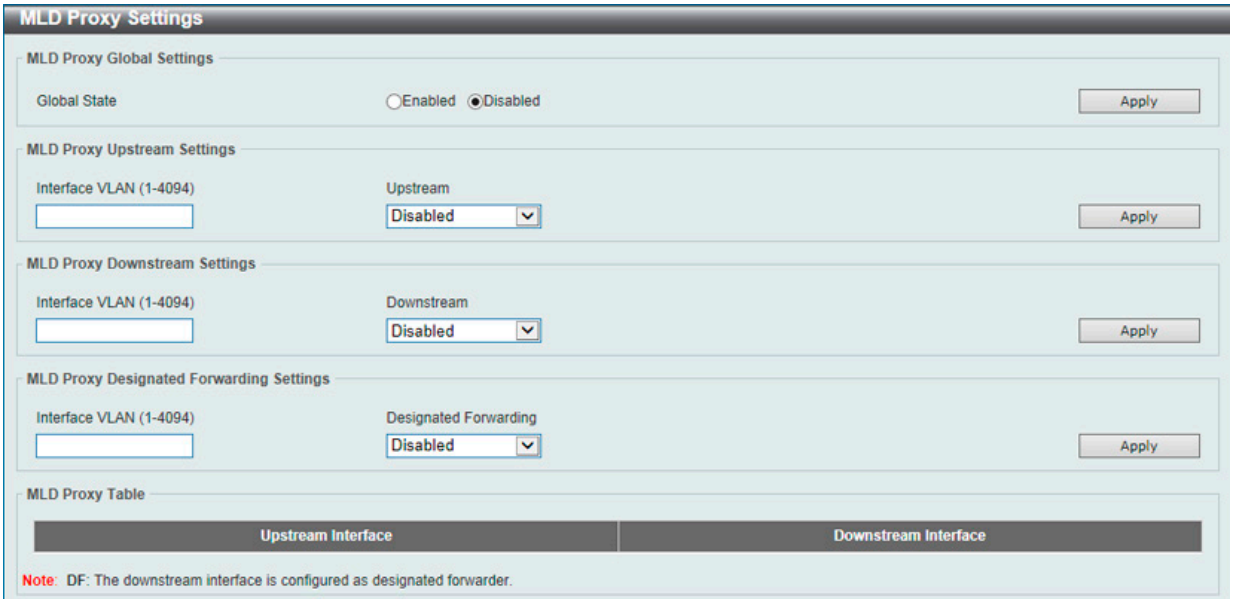


図 9-101　MLD Proxy Settings 画面

画面に表示される項目：

項目	説明
MLD Proxy Global Settings	
Global State	MLD プロキシのグローバルステータスを有効 / 無効に設定します。
MLD Proxy Upstream Settings	
Interface VLAN	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Upstream	アップストリーム MLD プロキシとしてインタフェースを有効 / 無効に設定します。 本機能は、インタフェースに IPv6 アドレスが設定されている場合にのみ有効になります。MLD プロキシデバイスに存在できるアップストリームインタフェースは 1 つだけです。
MLD Proxy Downstream Settings	
Interface VLAN	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Downstream	ダウンストリーム MLD プロキシとしてインタフェースを有効 / 無効に設定します。 本機能は、インタフェースに IPv6 アドレスが設定されている場合にのみ有効になります。MLD プロキシデバイスには、複数のダウンストリームインタフェースを設定できます。
MLD Proxy Designated Forwarding Settings	
Interface VLAN	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
Designated Forwarding	非クエリア 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を有効 / 無効に設定します。複数の MLD ベースのフォワーダによるダウンストリームリンクと見なされるリンクのローカルループと冗長トラフィックを回避するために、MLD プロキシは MLD クエリア選択を使用して LAN 上の単一のフォワーダを選択します。このオプションにより、非クエリアデバイスをフォワーダにすることができます。この機能は、インタフェースがダウンストリームインタフェースとして設定されていない場合、またはアップストリームインタフェースとして設定されている場合は有効になりません。

「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。

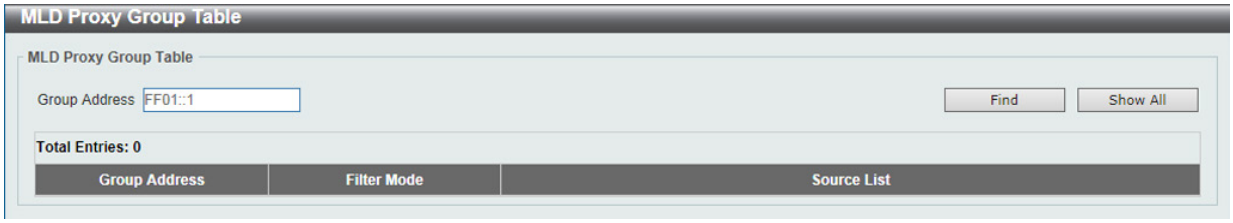


図 9-102　MLD Proxy Group Table 画面

画面に表示される項目：

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

MLD Proxy Forwarding Table（MLD フォワーディングテーブル）

MLD プロキシの転送情報を表示します。

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。

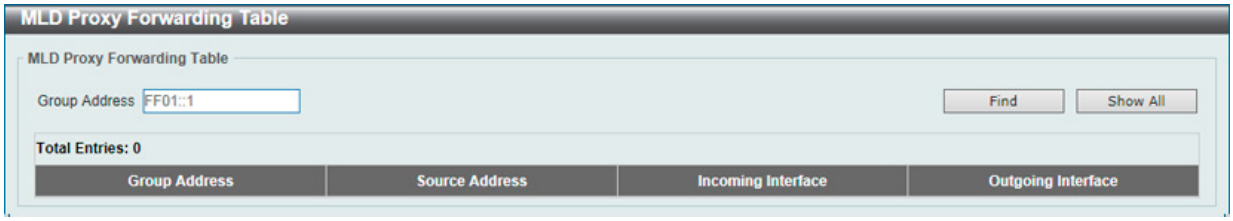


図 9-103　MLD Proxy Forwarding Table 画面

画面に表示される項目：

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

DVMRP（EI 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）

Distance Vector Multicast Routing Protocol（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 9-104　DVMRP Interface Settings 画面

画面に表示される項目：

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

エントリの編集

編集するエントリの「Edit」ボタンをクリックして以下の画面を表示します。

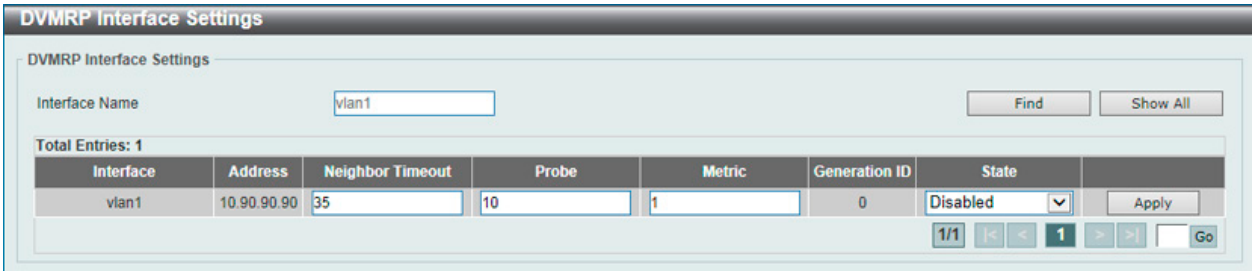


図 9-105　DVMRP Interface Settings（Edit）画面

画面に表示される項目：

項目	説明
Neighbor Timeout	ネイバの有効期間を指定します。指定時間までに、ルータがネイバからのプルーブメッセージを受信しない場合、ネイバはダウンしていると判断されます。 • 設定可能範囲：1-65535（秒） • 初期値：35（秒）
Probe	DVMRP プルーブ間隔の値を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Metric	メトリック値を指定します。報告された各送信元ネットワークに対し、報告されたルートにルートメトリックが関連付けられます。メトリックは、レポートを発信するルータ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合計です。DVMRP の場合、「32」の値は到達不能であることを意味します。DVMRP ネットワーク全体の幅を制限し、プロトコルの収束時間に上限を設けるために必要です。 • 設定可能範囲：1-32
State	指定インタフェースでの DVMRP 機能を有効 / 無効に設定します。

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）

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 9-106　DVMRP Routing Table 画面

画面に表示される項目：

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、すべてのエントリを表示します。

DVMRP Neighbor Table（DVMRP Neighbor テーブル）

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。

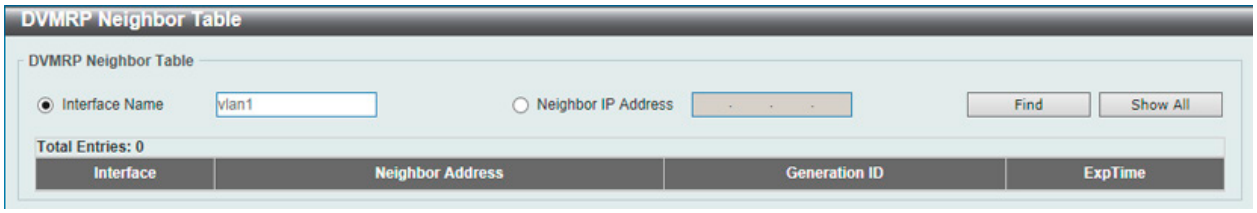


図 9-107　DVMRP Neighbor Table 画面

画面に表示される項目：

項目	説明
Interface Name	VLAN 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、すべてのエントリを表示します。

PIM（PIM 設定）（EI 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 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）をルートとする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、明示的にマルチキャストグループに属するルータに対してトラフィックを転送します。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から、送信元から受信したマルチキャスト情報を、ネットワーク内の要求ルータに対して返します。この方法により、RP をルートとして配送ツリーが作成されます。この配送ツリーには、PIM-SM が有効であるすべてのルータが含まれ、これらのルータから収集された情報は RP によって保持されます。

マルチアクセスネットワーク内に複数のルータが存在する場合、代表ルータ (DR) が選出されます。DR の主な機能は、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を持つルータが複数存在する場合、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することができますが、BSR メカニズムによって RP を決定することもできます。ネットワーク上には複数の Candidate BSR（C-BSR）を設定できますが、RP 情報を処理するために選出される BSR は 1 つのみです。BSR となる C-BSR が指定されていない場合、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）を発信し、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。選出された 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、コンパイルしてから、定期的なブートストラップメッセージ（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、データベースに保存します。

● マルチキャストグループの検出と参加

PIM-SM ルータは Hello パケットにより検出されますが、これらのルータは、DR と RP 間で交換される Join/Prune メッセージを介してのみ、マルチキャストグループへ参加または「Pruned（削除）」されます。Join/Prune メッセージは、どのインタフェースでマルチキャストデータを受信するか / しない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。ネットワーク上でこれらのメッセージが送信される頻度を設定することが可能です。また、Hello パケットが最初に受信されたルータに対してのみ有効です。Hello パケットは、ルータが存在すること、RP の配信ツリーの一部になる準備ができていることを単純に記載したものです。ルータが IGMP グループのメンバを受け入れ、PIM-SM が有効である場合、関連ルータは明示的な Join/Prune メッセージを RP に送信します。RP は送信元から関連ルータにマルチキャストデータをルーティングし、グループの単一方向の配布ツリーを生成します。その後、マルチキャストパケットがこれらのツリー上の全ノードに送信されます。RP の配布ツリーのメンバであるルータで Prune メッセージを受信すると、ルータは配布ツリーからインタフェースを破棄します。

● 配信ツリー

PIM-SM プロトコルには、Rendezvous-Point Tree（RPT）および最短経路ツリー（Shortest Path Tree：SPT）の 2 種類の配布ツリーがあります。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対し、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が、ルータが送信元の位置を決定すると、送信元と宛先間のホップ（RP など）を削除して、SPT を生成することができます。これは、マルチキャストデータ転送速度のしきい値により設定することができます。しきい値を越えると、データの経路は SPT に切り換わります。これにより、以前使用されていたホップを削除して、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することで、より近いリンクを送信元と宛先の間で作成することが可能となります。

● Register と Register-stop メッセージ

マルチキャストソースは、意図する受信グループに常に参加するとは限りません。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を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。これは、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 メッセージにより緩和されます。DR が受信した最初のマルチキャストパケットはカプセル化され、RP に送信されます。RP はこのカプセル化を解いて RP 配信ツリーにパケットを送信します。
ルートが確立すると、ルータをソースに直接接続するための SPT が作成されるか、マルチキャストトラフィックは DR から RP に送信されます。後者の場合、カプセル化されているパケットとカプセル化されていないパケットで、同じパケットが 2 回送信される可能性があります。RP がこの不備を検出すると、Register-stop メッセージを DR に返して、カプセル化されたパケットの送信を中止するように要求します。

● Assert メッセージ

PIM-SM 対応ネットワークにおいて、送信元から受信先へのパラレルパスが作成されることがあります。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ます。この状況を改善するために、受信デバイスから両方のマルチキャストソースに対して Assert メッセージが送信され、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。このメトリック値は 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。データトラフィックは、レシーバが明示的に参加しているマルチキャスト送信元のみからレシーバに送信されます。SSM 範囲のマルチキャストグループでは、送信元を指定したマルチキャスト配信ツリー (共有ツリーなし) のみ作成可能です。

IANA（Internet Assigned Numbers Authority）は SSM アプリケーションとプロトコル用に 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最適化されているため、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への定期的なマルチキャストメッセージのフラッディングに依存し、その後、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ブランチにマルチキャストメンバが存在しない旨を示す明示的な “Prune" メッセージを送信します。PIM-DM はその後マルチキャスト配信ツリーからこれらのブランチを削除（Prune）します。

マルチキャスト配信ツリーから刈り込まれたブランチ（枝）も、マルチキャスト配信グループへの参加を (将来的に) 希望す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、そのブランチ上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のキーポイントとなります。送信者が情報を送信するときに最初のホップに RP 情報がない場合、パケットを破棄し、何も実行しません。Sparse-Dense モードはこのようなケースで有用です。Sparse-Dense モードでは、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、RP が検出されない場合に pruning/joining（Prune/Graft）を使用して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、Sparse モードまたは Dense モードのいずれかで動作します。これは、マルチキャストグループがどのモードで動作するかによって異なります。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）

インタフェース毎に PIM（Protocol Independent Multicast）の設定、表示を行います。

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。

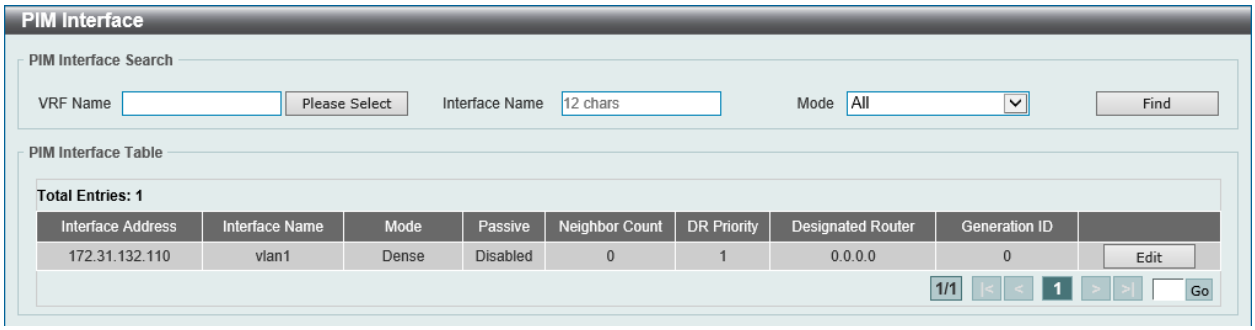


図 9-108　PIM Interface 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface Name	インタフェース名を指定します。
Mode	検出する PIM プロトコルのタイプを選択します。 • 選択肢：「Dense Mode」「Sparse Mode」「Spare-Dense Mode」「All」

「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

「Edit」ボタンをクリックして、以下の画面を表示します。

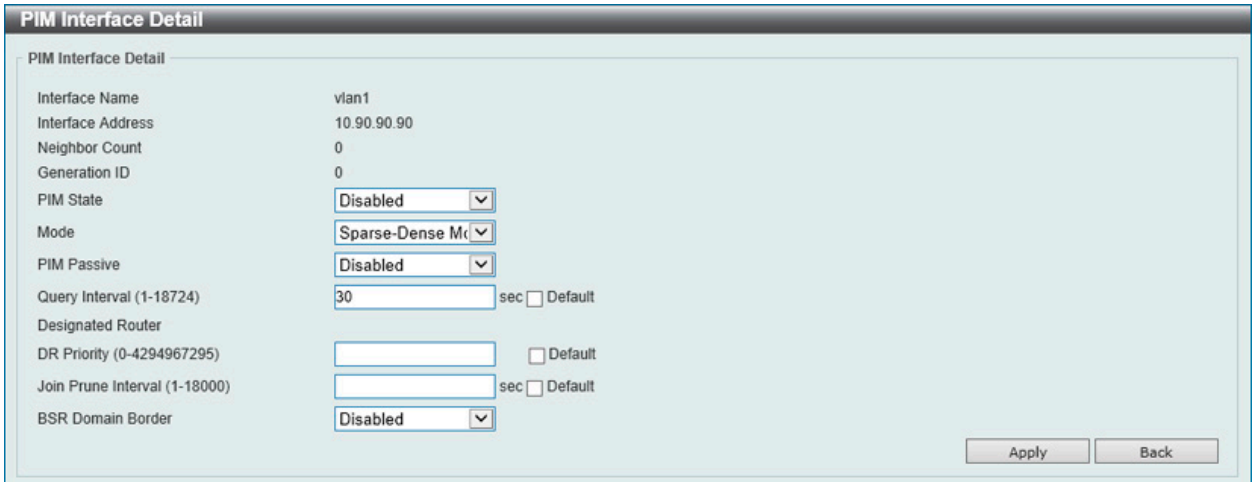


図 9-109　PIM Interface Settings（Edit）- PIM Interface Detail 画面

画面に表示される項目：

項目	説明
PIM State	インタフェースの PIM ステータスを有効 / 無効に設定します。
Mode	使用する PIM プロトコルの種類を指定します。 • 「Dense Mode」- PIM-DMは、送信元が送信を開始すると、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ていると想定します。最初に、マルチキャストデータストリームはすべての下流ルータと、グループ・メンバを持つインタフェースにフラッディングされます。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」- Sparse Mode のインタフェースでマルチキャストトラフィックを受信すると、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、トラフィックはマルチキャストルートエントリに基づいて転送されます。Sparse モードインタフェースは、ダウンストリームルータから Join メッセージを受信した場合、または Sparse モードのインタフェース上のグループメンバの場合にのみ、Multicast Route メンバのインタフェースとして設定されます。PIM ジョインプロセスにより共有ツリーまたはソースツリーが作成されます。 • 「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、インタフェースにより受信したマルチキャストグループは「sparse」/「dense」モードどちらでも動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 モードで動作します。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 / 無効に設定します。パッシブモードが有効の場合、インタフェースは PIM メッセージの送受信を行いません。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。この機能は、LAN に PIM ルータが 1 つしかない場合のみ使用してください。
Query Interval	Hello メッセージを送信する間隔を入力します。PIMv2 ルータは、PIM ハローメッセージを介して PIM ネイバを学習します。IP マルチキャスト用に設定されたルータは、PIM ルータを検出するために PIM ハローメッセージを送信します。SM の場合、Hello メッセージを使用して、各 LAN セグメントの指定ルータとして機能するルータも決定されます。設定されたクエリ間隔は、ホールド時間の値としても使用されます。間隔を短く設定すると、応答しないネイバーをより迅速に検出できるため、より効率的にフェイルオーバとリカバリを実行できます。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-18724（秒） • 初期値：30（秒）
DR Priority	「Sparse Mode 」または「Sparse-Dense Mode」を選択した場合、このパラメータを設定できます。指定ルータ（DR）の優先値を入力します。値が大きいほど、優先順位が高くなります。 Dense モード（DM）では、DR 優先オプションは Hello メッセージで伝送されません。プライオリティ値が最も高いルータが DR になります。複数のルータが同じプライオリティステータスの場合、IP アドレスが最も高いルータが DR になります。Hello メッセージ内の DR プライオリティをサポートしていないルータが LAN 上にある場合、LAN 上のすべてのルータは DR プライオリティを無視し、IP アドレスのみを使用して DR を選択します。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-4294967295 • 初期値：1
Join Prune Interval	「Sparse Mode 」または「Sparse-Dense Mode」を選択した場合、このパラメータを設定できます。Join/Prune メッセージの送信間隔を入力します。Join/Prune インターバルを設定するときは、設定された帯域幅や、接続されたネットワークやリンクで想定されるマルチキャストルートの平均エントリ数などの要素を考慮してください。Sparse モード（SM）の場合、ルータはこの指定間隔に基づいて定期的に Join メッセージを送信します。Join/Prune メッセージの hold-time は「Join Prune Interval 」の 3.5 倍です。受信ルータはこのホールド時間に基づいてタイマーを開始し、このインタフェースで Join メッセージが受信されなかった場合はインタフェースを削除します。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-18000（秒） • 初期値：60（秒）
BSR Domain Border	Bootstrap Router（BSR）ドメイン境界機能を有効 / 無効に設定します。この機能は、インタフェースで PIM が有効な場合にのみ有効になります。2 つのドメイン間での BSR メッセージの交換を回避するには、別のドメインと境界を結ぶインタフェースでこの機能を使用します。

項目を編集後、「Apply」ボタンをクリックします。
前の画面に戻るには、「Back」ボタンをクリックします。

■ PIM BSR Candidate（PIM BSR 候補設定）

PIM BSR 候補設定の表示と設定を行います。この機能は、インタフェースに IP アドレスが設定され、PIM Sparse モードになっている場合にのみ有効になります。

この機能により、ルータは Bootstrap メッセージを送信して、指定されたインタフェースの IP アドレスを CBSR アドレスとしてアナウンスします。ハッシュマスクは、ドメイン内のすべてのルータによって使用され、「グループ範囲 -RP」マッピングの一致するセットからランデブーポイント（RP）にグループをマッピングします（このセットは、すべて同じ最長のマスク長 / 最高のプライオリティを持ちます）。このアルゴリズムは、グループアドレスとマップからの候補 RP のアドレスを入力として取得し、使用する RP アドレスを出力として 1 つ指定します。

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。

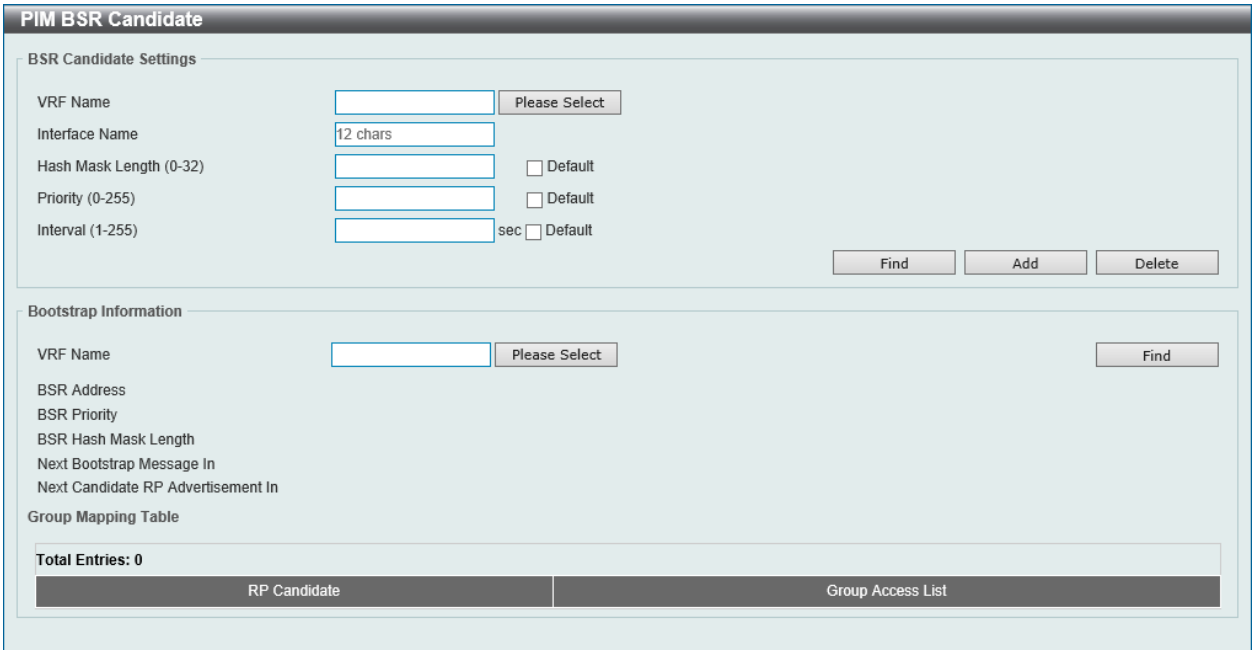


図 9-110　PIM BSR Candidate 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface Name	インタフェース名を入力します。
Hash Mask Length	RP 選出で使用するハッシュマスク長を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-32 • 初期値：30
Priority	「Candidate Bootstrap Router」(CBSR) の優先値を入力します。優先値が最も高い候補が優先されます。優先値が同じ場合は、IP アドレスが最も高いルータが優先されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：64
Interval	Bootstrap メッセージの送信間隔を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255（秒） • 初期値：60（秒）

「Add」ボタンをクリックして、入力した情報を基にエントリを追加します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報を基にエントリを検出します。

■ PIM RP Address（PIM RP アドレス設定）

スタティックマルチキャストグループから RP へのマッピングを表示、設定します。マルチキャストドメインでは、静的マルチキャストグループから RP へのマッピングを BSR と一緒に使用できます。ドメイン内のすべてのルータは、一貫したマルチキャストグループ - RP マッピングを持つ必要があります。レジスタメッセージを開始するファーストホップルータは、マッピングエントリを使用して、特定のグループ宛ての PIM レジスタメッセージを送信するための RP を決定します。Join メッセージを開始するラストホップルータは、マッピングエントリを使用して、特定のグループの Join および Prune メッセージを送信するための RP を決定します。ルータは、Join 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と、ルータがマルチキャストグループの正しい 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 を定義可能であり、それぞれ 1 つのアクセスリストを設定します。

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。

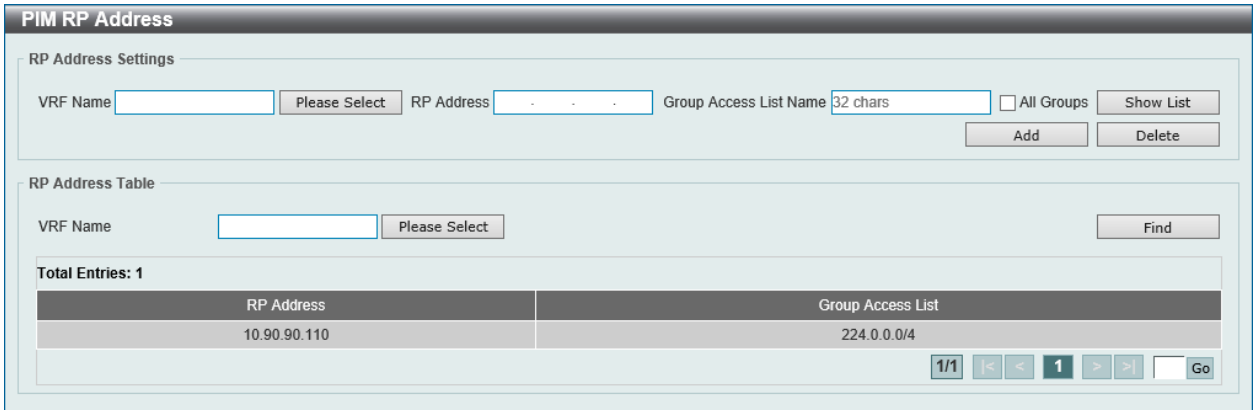


図 9-111　PIM RP Address 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
RP Address	RP IPv4 アドレスを入力します。
Group Access List Name	使用する標準アクセスリストを指定します。「Show List」をクリックすると、定義済みの 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ピングします。

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。

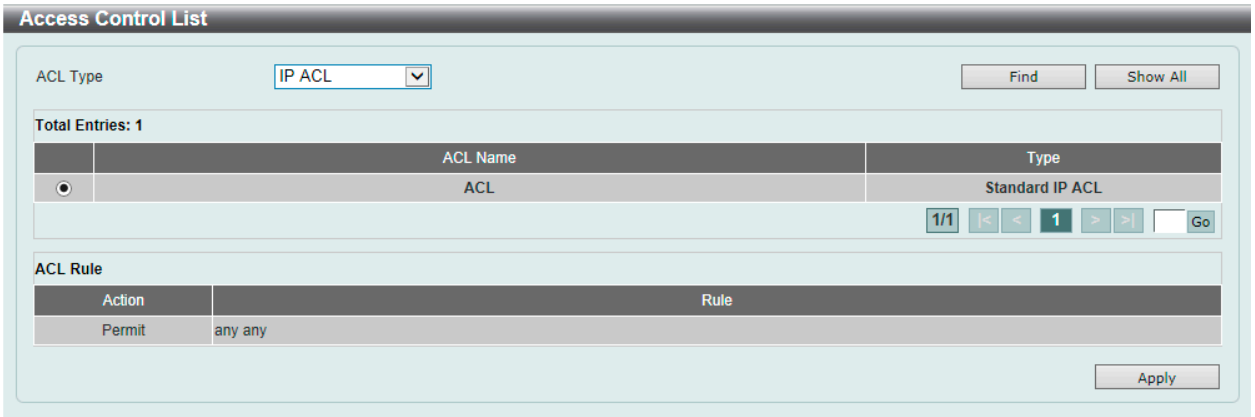


図 9-112　PIM RP Address (Show List) - Access Control List 画面

画面に表示される項目：

項目	説明
ACL Type	表示する ACL の種類を指定します。 • 選択肢：「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ACL List	使用するアクセスリストを指定します。

「Find」ボタンをクリックして、指定した種類のアクセスリストを検出します。

「Show All」ボタンをクリックして、すべてのアクセスリストを表示します。
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」ボタンをクリックして、選択したアクセスリストを使用します。

■ PIM RP Candidate（PIM RP Candidate 設定）

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。

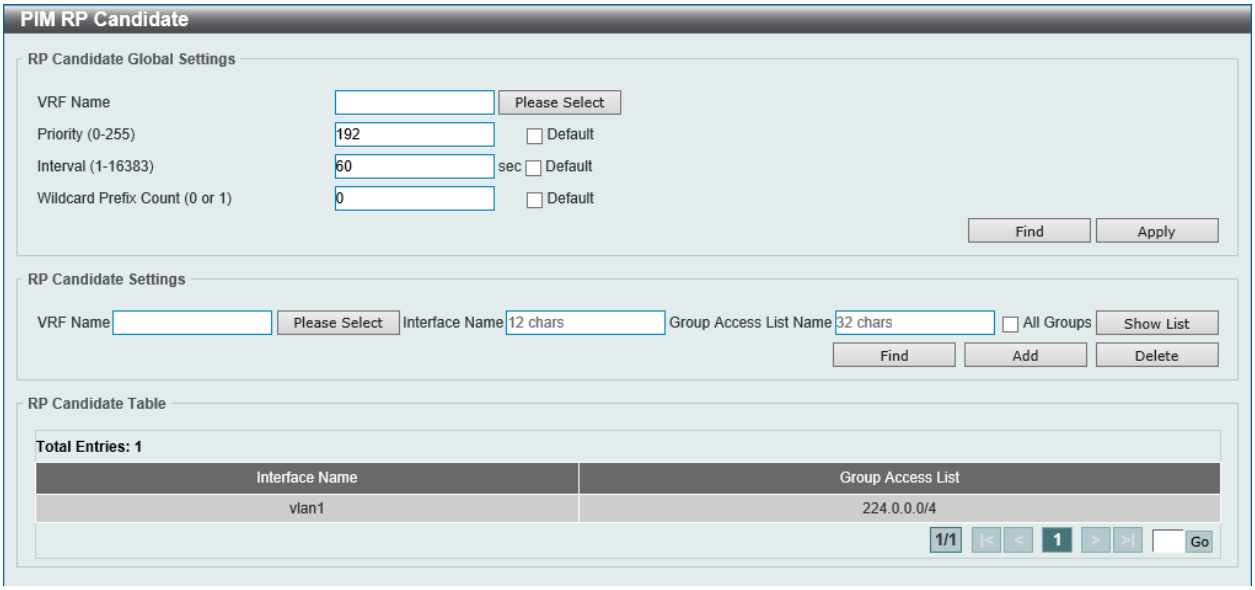


図 9-113　PIM RP Candidate 画面

画面に表示される項目：

項目	説明
RP Candidate Global Settings	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Priority	Candidate RP のプライオリティ値を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：192
Interval	Candidate RP のアドバタイズメント間隔をここに入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-16383（秒） • 初期値：60（秒）
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）プレフィックスカウント値を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-1 • 初期値：0
RP Candidate Settings	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface name	インタフェース名を入力します。
Group Access List Name	使用する標準アクセスリストを指定します。「Show List」をクリックすると、定義済みの 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ピングします。

「Apply」ボタンをクリックして、設定内容を適用します。

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。

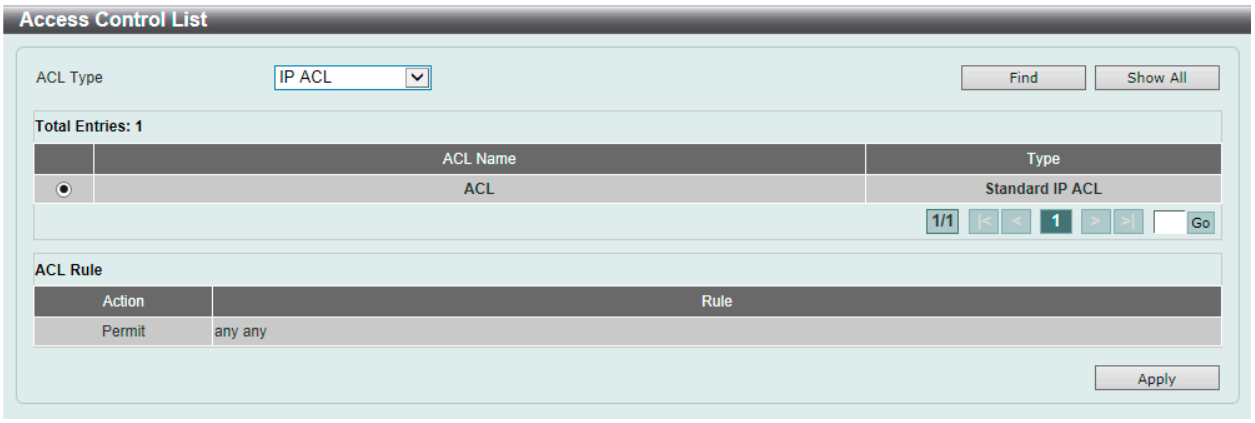


図 9-114　PIM RP Candidate (Show List) - Access Control List 画面

画面に表示される項目：

項目	説明
ACL Type	表示する ACL の種類を指定します。 • 選択肢：「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ACL List	使用するアクセスリストを指定します。

「Find」ボタンをクリックして、指定した種類のアクセスリストを検出します。
「Show All」ボタンをクリックして、すべてのアクセスリストを表示します。
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」ボタンをクリックして、選択したアクセスリストを使用します。

■ 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。

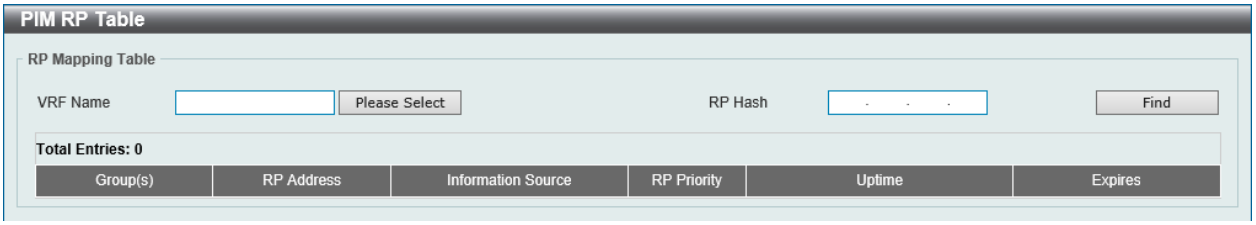


図 9-115　PIM RP Table 画面

以下の項目を使用します。

項目	説明
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
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」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 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。

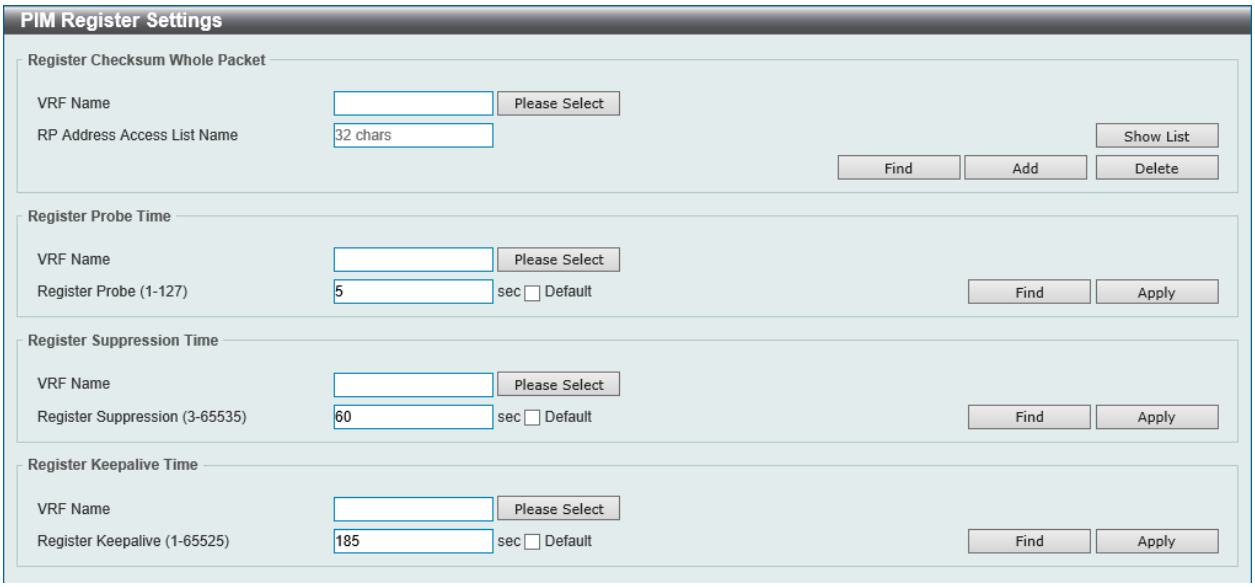


図 9-116　PIM Register Settings 画面

画面に表示される項目：

項目	説明
Register Checksum Whole Packet	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
RP Address Access List Name	使用する標準アクセスリストを指定します。「Show List」をクリックすると、定義済みの ACL リストを検出、選択することができます。
Register Probe Time	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Register Probe	Register Probe 時間を入力します。設定した時間が経過すると、レジスタストップタイマ（RST）が期限切れになり、DR が RP に Null-Register を送信して、RP により Register-Stop メッセージが再送信されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-127（秒） • 初期値：5（秒）
Register Suppression Time	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Register Suppression	Register Suppression のタイムアウト値を入力します。DR は、Register-Stop メッセージを受信すると、サプレッションタイマを開始します。抑制期間中、DR は RP への Register メッセージの送信を停止します。 ファーストホップルータでこの機能を使用してください。レジスタストップタイマの設定で負の値が発生しないようにするには、「Register Probe」時間の値が「Register Suppression」時間の半分未満である必要があります。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：3-65535（秒） • 初期値：60（秒）
Register Keepalive Time	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Register Keepalive	Register Keepalive の時間を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65525（秒） • 初期値：185（秒）

「Apply」ボタンをクリックして、設定内容を適用します。
「Add」ボタンをクリックして、入力した情報を基にエントリを追加します。
「Find」ボタンをクリックして、入力した情報を基に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。

「Show List」をクリックすると、以下の画面が表示されます。

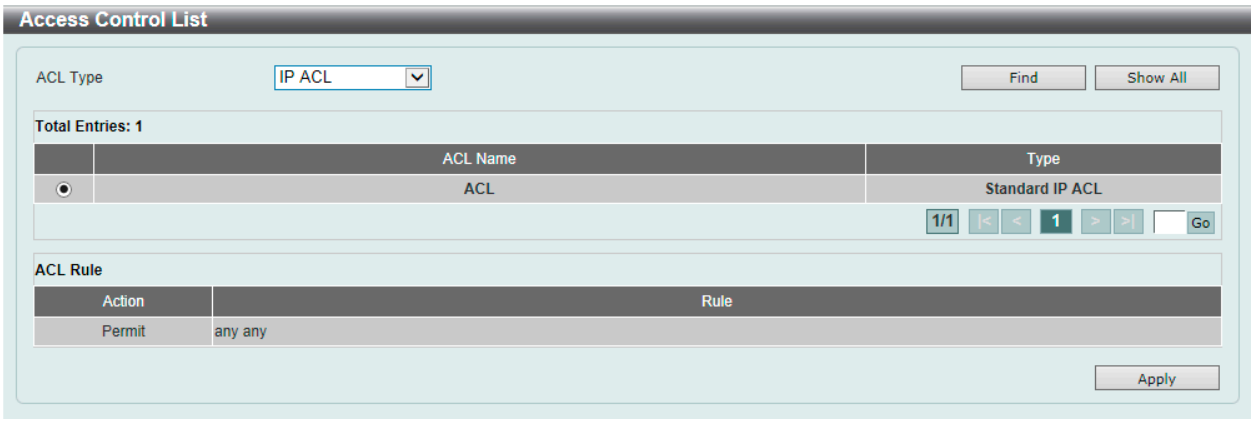


図 9-117　PIM Register Settings（Show List）- Access Control List 画面

画面に表示される項目：

項目	説明
ACL Type	表示する ACL の種類を指定します。 • 選択肢：「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ACL List	使用するアクセスリストを指定します。

「Find」ボタンをクリックして、指定した種類のアクセスリストを検出します。
「Show All」ボタンをクリックして、すべてのアクセスリストを表示します。
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」ボタンをクリックして、選択したアクセスリストを使用します。

■ PIM SPT Threshold Settings（PIM SPT しきい値設定）

PIM SPT しきい値を設定します。ルータのラストホップでこの機能を使用します。PIM-SM モードでは、最初、送信元からのマルチキャストトラフィックは RPT 共有ツリーに沿って受信側に送信されます。最初のパケットがラストホップルータに到着した後、トラフィックの各グループは次の 2 つのモードのいずれかで動作します。「Infinity」モードでは、トラフィックは引き続き共有ツリーに従います。「0」モードでは、ソースツリーが確立され、トラフィックはソースツリーへの切り替え（スイッチオーバ）が行われます。

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。

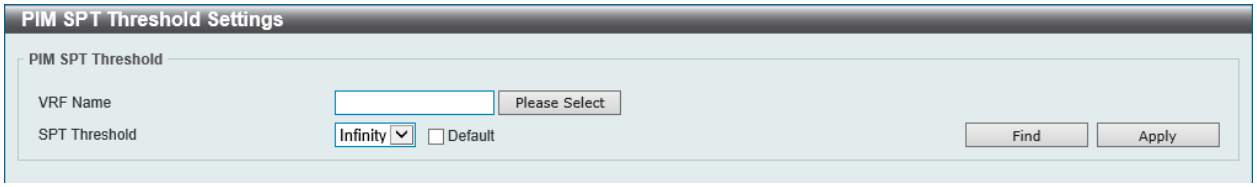


図 9-118　PIM SPT Threshold Settings 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
SPT Threshold	SPT しきい値を指定します。「Default」にチェックを入れると、初期値を使用します。 • 「Infinity」- 常に共有ツリーに従います。（初期値） • 「0」- 最初のパケットの到着時にソースツリーを確立します。

「Apply」ボタンをクリックして、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。この機能は、ルータのラストホップでのみ使用してください。SSMが有効な場合、ラストホップルータは、SSM 範囲に含まれる IGMPv3 Include（S,G）要求を接続されたホストから受信すると、チャネル（S,G）のソースベースツリーの確立を開始します。

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。

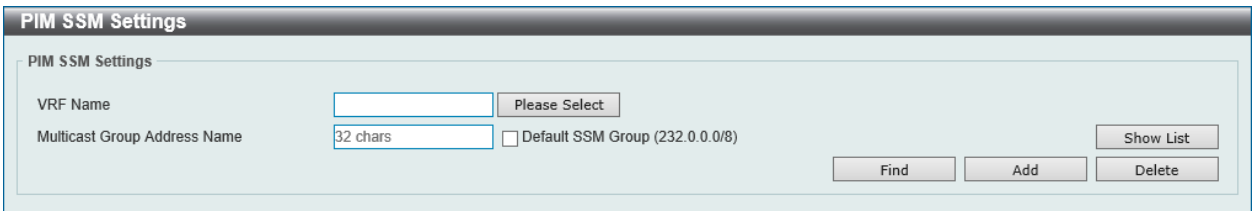


図 9-119　PIM SSM Settings 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Multicast Group Address Name	ユーザ指定の SSM グループアドレスを定義する標準 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)」オプションにチェックを入れると、初期値の SSM グループアドレス（232/8）を使用します。

「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。

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。

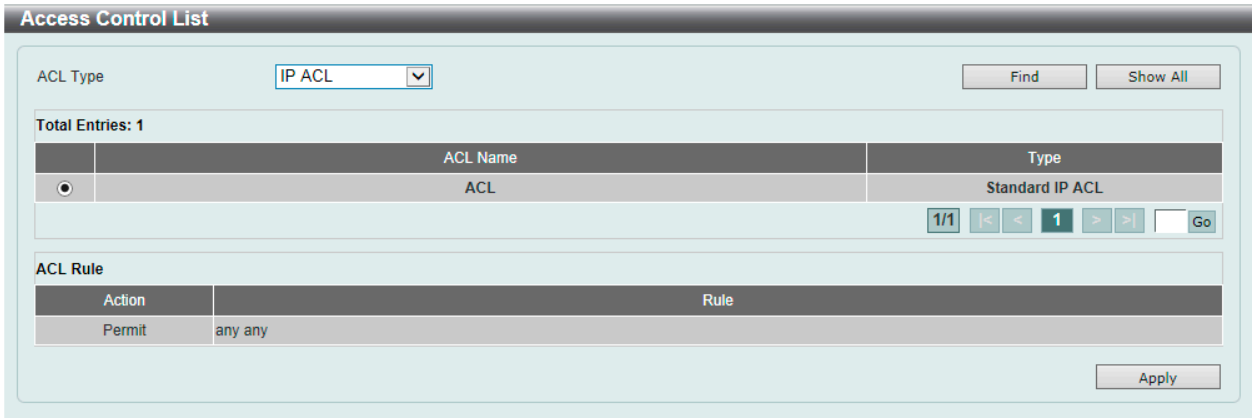


図 9-120　PIM SSM Settings（Show List）- Access Control List 画面

画面に表示される項目：

項目	説明
ACL Type	表示する ACL の種類を指定します。 • 選択肢：「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ACL List	使用するアクセスリストを指定します。

「Find」ボタンをクリックして、指定した種類のアクセスリストを検出します。
「Show All」ボタンをクリックして、すべてのアクセスリストを表示します。
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」ボタンをクリックして、選択したアクセスリストを使用します。

■ 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。

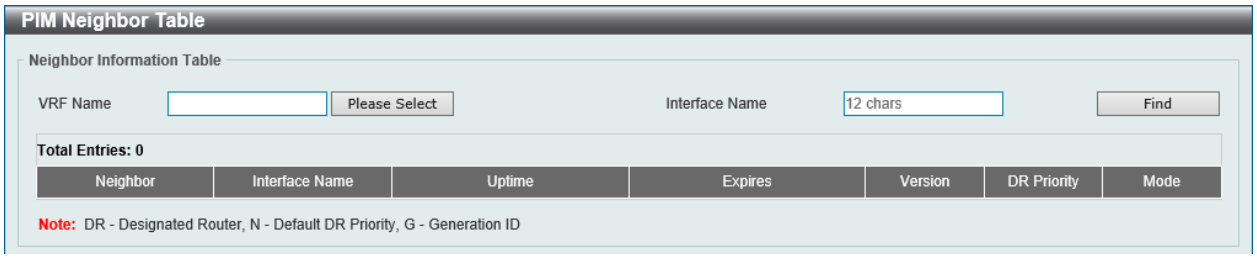


図 9-121　PIM Neighbor Table 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
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」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 for IPv6（IPv6 用 PIM の設定）

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6

IPv6 用 PIM Sparse モード（PIM-SMv6）および IPv6 用 PIM Dense モード（PIM-DMv6）に関する設定を行います。

■ 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。

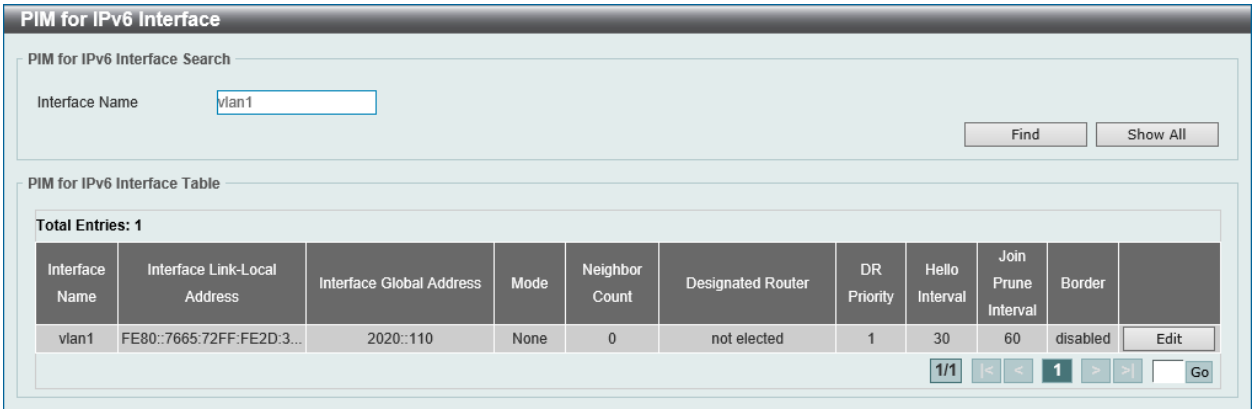


図 9-122　PIM for IPv6 Interface 画面

画面に表示される項目：

項目	説明
Interface Name	VLAN インタフェース名を指定します。

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

エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

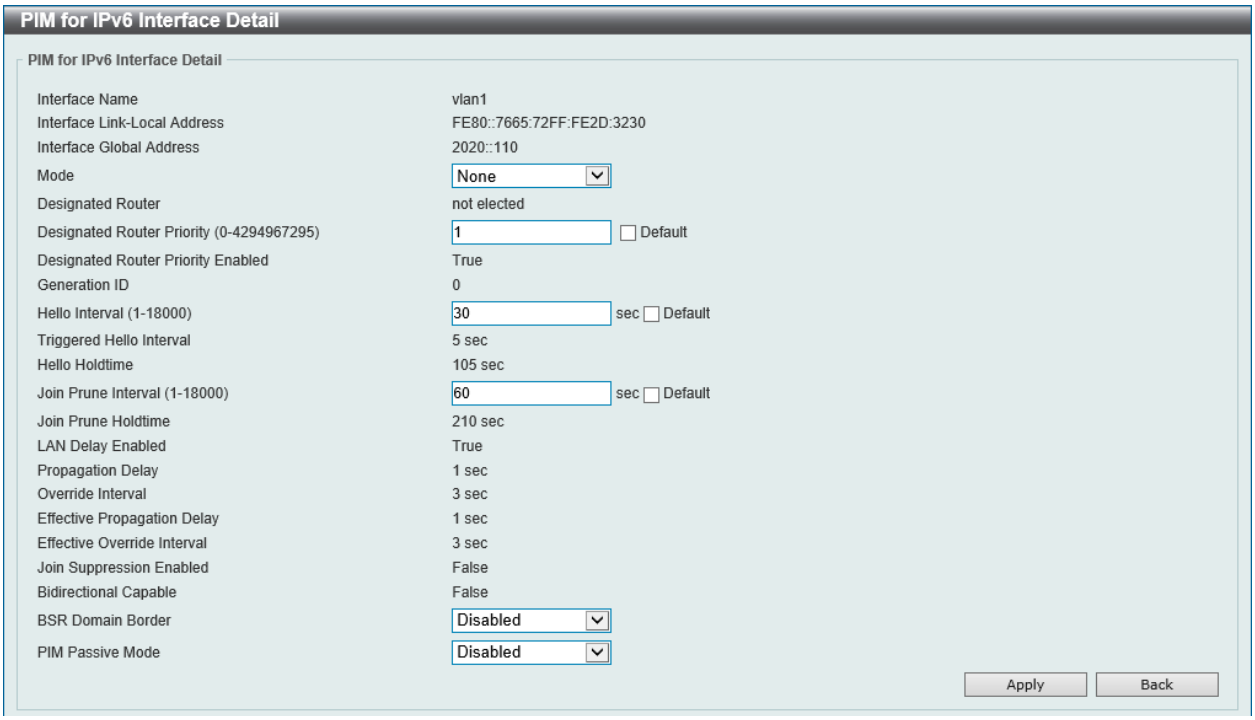


図 9-123　PIM for IPv6 Interface（Edit）- PIM for IPv6 Interface Detail 画面

画面に表示される項目：

項目	説明
Mode	このインタフェースで使用する IPv6 PIM プロトコルのタイプを選択します。 • 選択肢：「None」「Sparse Mode」
Designated Router Priority	DR プライオリティ値を入力します。値が大きいほど優先順位が高くなります。この機能は、VLAN インタフェースで PIM-SM モードが有効な場合にのみ有効になります。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-4294967295 • 初期値：1 DR 選出のプロセスは以下の通りです： - インタフェースに設定されている最も高いプライオリティ値を持つルータが DR として選択されます。複数のルータが同じ最高値のプライオリティを持つ場合、インタフェースに設定されている最も高い IPv6 アドレスを持つルータが DR として選出されます。 - ルータが Hello メッセージで優先値をアドバタイズしない場合、このルータは最も高いプライオリティを持つと見なされ、DR として選択されます。複数のルータが Hello メッセージに DR プライオリティオプションを含まない場合、最も高い IPv6 アドレスを持つルータが DR として選択されます。
Hello Interval	Hello メッセージの送信間隔を入力します。PIM ルータは、Hello メッセージを介して PIM ネイバを学習します。IP マルチキャスト用に設定されたルータは、PIM ルータを検出するために PIM Hello メッセージを送信します。SM の場合、Hello メッセージは、各 LAN セグメントの指定ルータとして選択されるルータを決定するためにも使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-18000（秒） • 初期値：30（秒）
Join Prune Interval	Join/Prune メッセージの送信間隔を入力します。Join/Prune インターバルを設定するときは、設定された帯域幅や、接続されたネットワークやリンクで想定されるマルチキャストルートの平均エントリ数などの要素を考慮してください。（例えば低速リンクや、多数のエントリを持つネットワークの中心に存在するルータでは、この期間は長くなります。）Sparse モード（SM）の場合、ルータはこの指定間隔に基づいて定期的に Join メッセージを送信します。Join/Prune メッセージの hold-time は「Join Prune Interval 」の 3.5 倍です。受信ルータはこのホールド時間に基づいてタイマを開始し、このインタフェースで Join メッセージが受信されなかった場合はインタフェースを削除します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-18000（秒） • 初期値：60（秒）
BSR Domain Border	Bootstrap Router（BSR）ドメイン境界機能を有効 / 無効に設定します。インタフェースが境界として設定されている場合、Bootstrap ルータ（BSR）メッセージが境界を介して送受信されないようにします。
PIM Passive Mode	インタフェースの PIM パッシブ機能を有効 / 無効に設定します。の機能は、インタフェースで IPv6 PIM が有効な場合にのみ有効になります。パッシブモードが有効の場合、インタフェースは PIM の送受信を行いません。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 上に PIM ルータが一つしかない場合にのみ使用してください。

項目を編集後、「Apply」ボタンをクリックします。
前の画面に戻るには、「Back」ボタンをクリックします。

■ PIM for IPv6 BSR Candidate Settings（PIM for IPv6 BSR Candidate 設定）

IPv6 PIM BSR Candidate（候補）を設定します。この機能は、PIM-SM 動作にのみ影響します。これにより、ルータは、指定されたインタフェースのアドレスを BSR アドレスとして、すべての PIM ネイバに Bootstrap メッセージを送信します。PIM-SM ドメインには、RP 情報の収集とアドバタイズを実行する一意の BSR（Bootstrap ルータ）が含まれて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。

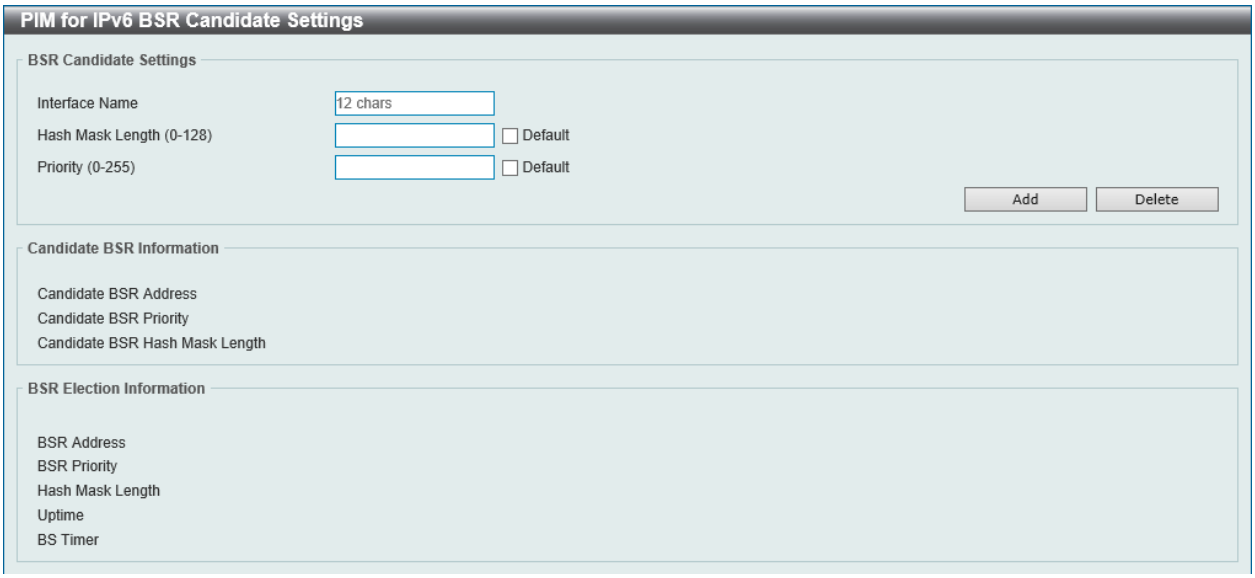


図 9-124　PIM for IPv6 BSR Candidate Settings 画面

画面に表示される項目：

項目	説明
Interface Name	インタフェース VLAN 名を入力します。
Hash Mask Length	RP 選出で使用するハッシュマスク長を入力します。ハッシュ関数を実行する前にグループアドレスと論理積をとるマスク（最大 128 ビット）です。同じシードハッシュを持つすべてのグループは、同じ RP に対応します。したがって、1 つの RP を複数のグループに派生させることができます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-128 • 初期値：126
Priority	BSR Candidate の優先値を入力します。優先値の高い BSR が優先されます。優先値が同じ場合、IPv6 アドレスが大きい方のルータが BSR になります。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：64

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

■ PIM for IPv6 BSR Table（PIM for IPv6 BSR テーブル）

「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 9-125　PIM for IPv6 BSR Table 画面

■ PIM for IPv6 RP Address（PIM for IPv6 RP アドレス）

IPv6 PIM RP アドレスの設定、表示を行います。この機能は、PIM-SM 動作にのみ影響します。この機能を使用して、Sparse モードで動作するマルチキャストグループの RP アドレスを静的に定義します。

複数のグループに 1 つの RP を使用します。アクセスリストで指定された条件により、RP を使用できるグループが決まります。複数の RP が定義可能で、各 RP は 1 つのアクセスリストを保持します。古い設定は新しい設定により上書きされます。

ドメイン内のすべてのルータは、一貫したマルチキャストグループ - RP マッピングを持つ必要があります。レジスタメッセージを開始するファーストホップルータは、マッピングエントリを使用して、特定のグループ宛ての PIM レジスタメッセージを送信するための RP を決定します。Join メッセージを開始するラストホップルータは、マッピングエントリを使用して、特定のグループの Join および Prune メッセージを送信するための RP を決定します。ルータは、Join 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と、ルータがマルチキャストグループの正しい RP でない場合、レジスタ停止メッセージが送信されます。

PIM ドメインが組み込み RP を使用している場合、その RP についてのみ、組み込み RP 範囲の RP として静的に設定する必要があります。他のルータは、IPv6 グループアドレスから RP アドレスを検出します。これらのルータが組み込み RP ではなくスタティック RP を選択する場合は、スタティック RP のアクセスリストで特定の組み込み RP グループ範囲を設定する必要があります。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > 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。

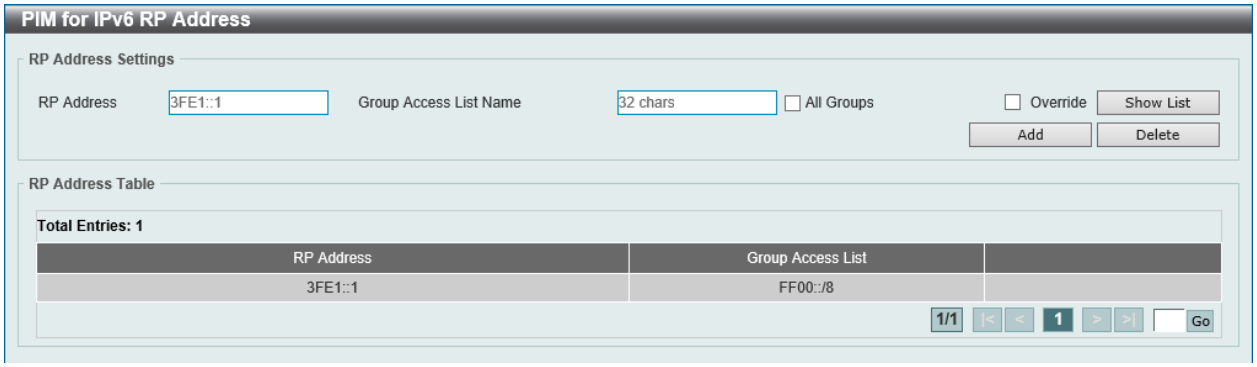


図 9-126　PIM for IPv6 RP Address 画面

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	使用する標準 IPv6 アクセスリストを指定します。「Show List」をクリックすると、定義済みの 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ピングします。
Override	このオプションを指定すると、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」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、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。

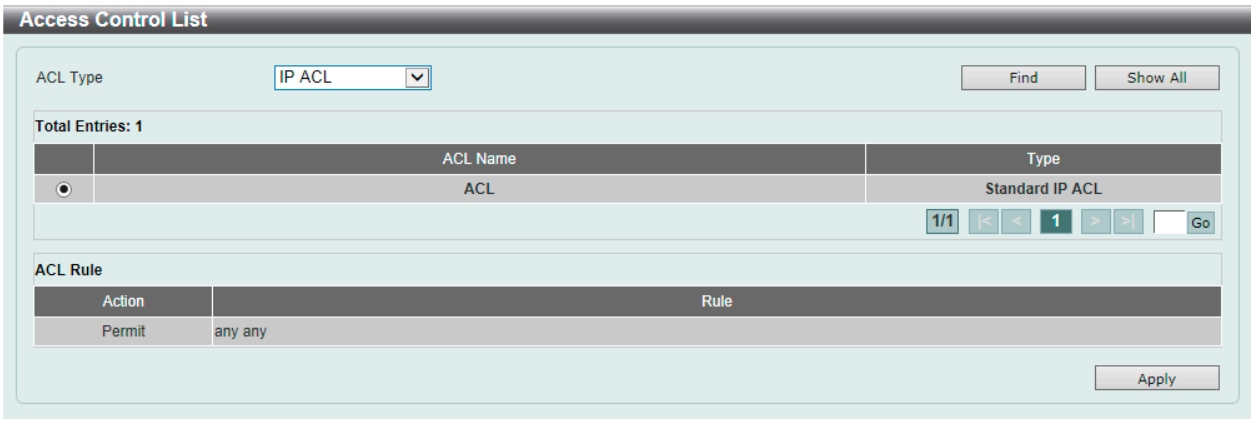


図 9-127　PIM for IPv6 RP Address（Show List）- Access Control List 画面

画面に表示される項目：

項目	説明
ACL Type	表示する ACL の種類を指定します。 • 選択肢：「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ACL List	使用するアクセスリストを指定します。

「Find」ボタンをクリックして、指定した種類のアクセスリストを検出します。
「Show All」ボタンをクリックして、すべてのアクセスリストを表示します。
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」ボタンをクリックして、選択したアクセスリストを使用します。

■ PIM for IPv6 RP Candidate（PIM for IPv6 RP Candidate 設定）

IPv6 PIM RP（Rendezvous Point）Candidate に関連する項目を設定します。インタフェース毎に 1 つのアクセスリストのみ指定可能です。古い設定は新しい設定に上書きされます。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。この設定により、ルータは自身を Candidate RP として通知する PIMv2 メッセージを BSR に送信します。

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。

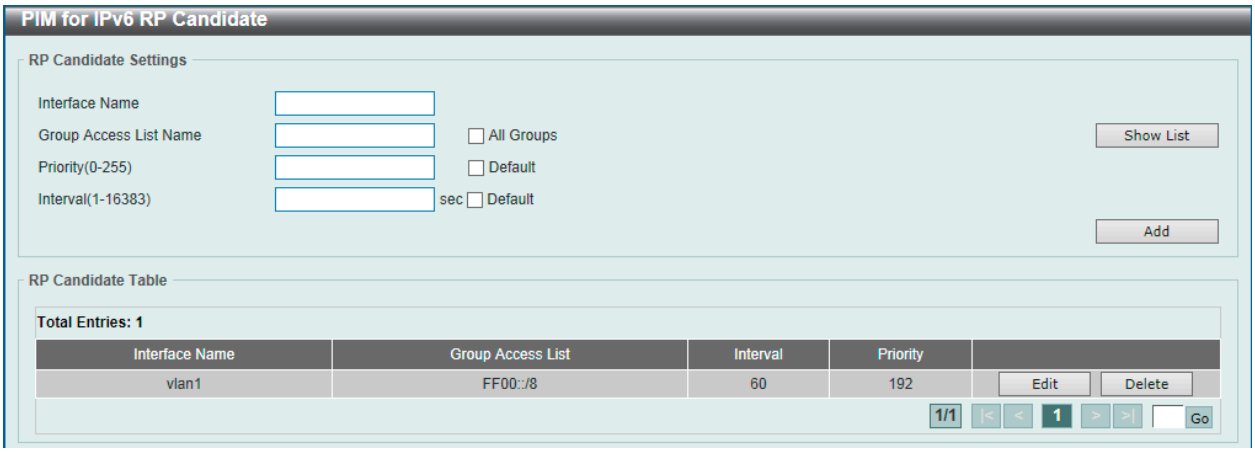


図 9-128　PIM for IPv6 RP Candidate 画面

画面に表示される項目：

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。このインタフェースの IPv6 アドレスが、Candidate RP（C-RP）としてアドバタイズされます。
Group Access List Name	使用する標準アクセスリストを指定します。「Show List」をクリックすると、定義済みの 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 Candidate RP を全マルチキャストグループにマッピングします。
Priority	RP 優先度の値を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：192
Interval	RP Candidate の通知間隔を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-16383（秒） • 初期値：60（秒）

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

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。

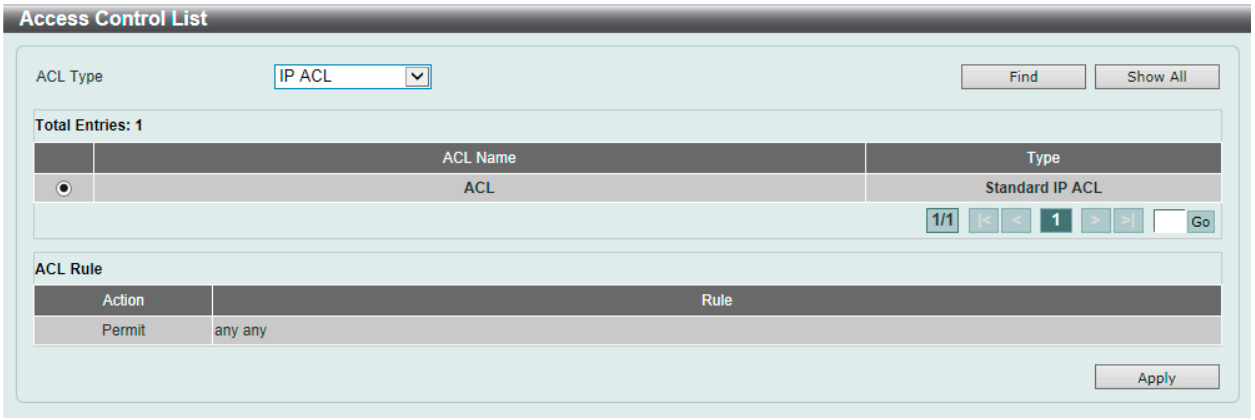


図 9-129　PIM for IPv6 RP Candidate（Show List）- Access Control List 画面

画面に表示される項目：

項目	説明
ACL Type	表示する ACL の種類を指定します。 • 選択肢：「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ACL List	使用するアクセスリストを指定します。

「Find」ボタンをクリックして、指定した種類のアクセスリストを検出します。
「Show All」ボタンをクリックして、すべてのアクセスリストを表示します。
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」ボタンをクリックして、選択したアクセスリストを使用します。

「Edit」をクリックすると、以下の画面が表示されます。

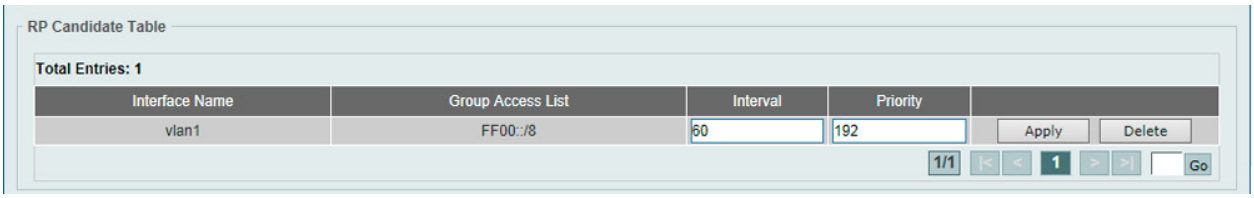


図 9-130　PIM for IPv6 RP Candidate (Edit) 画面

画面に表示される項目：

項目	説明
Interval	RP Candidate の通知間隔を指定します。 • 設定可能範囲：1-16383（秒）
Priority	RP 優先値を指定します。 • 設定可能範囲：0-255

「Apply」ボタンをクリックして、設定内容を適用します。

■ 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、スケーラブルなドメイン間マルチキャストの容易な展開が可能になり、ドメイン内マルチキャスト設定も簡素化されます。RP 情報が埋め込まれた IPv6 マルチキャストグループアドレスは、ff70::/12 で始まり、フラグ値 7 は埋め込み RP を意味します。

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。

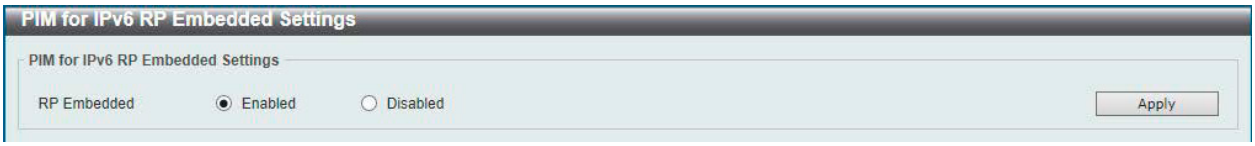


図 9-131　PIM for IPv6 RP Embedded Settings 画面

画面に表示される項目：

項目	説明
RP Embedded	RP 埋め込み機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

■ 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。

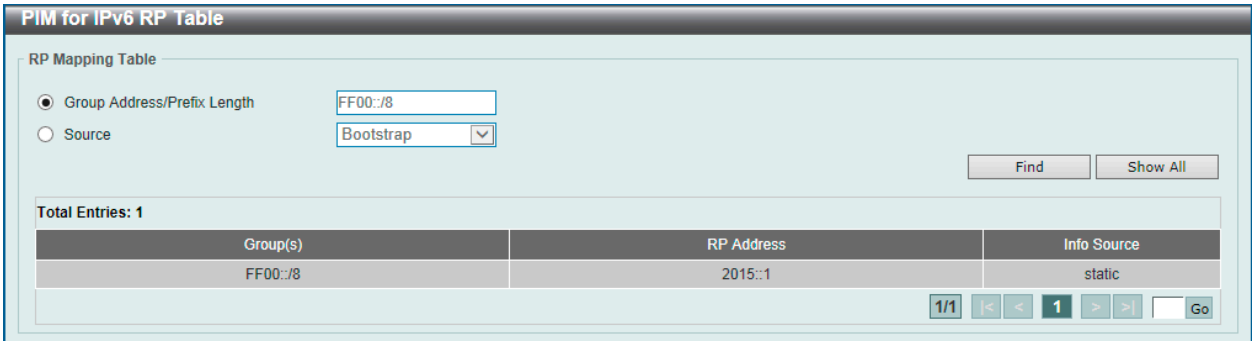


図 9-132　PIM for IPv6 RP Table 画面

画面に表示される項目：

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ックス長を指定します。
Source	表示するソースを指定します。 • 「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」- 手動設定で指定した範囲を表示します。

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

■ 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 IPv6 > 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。

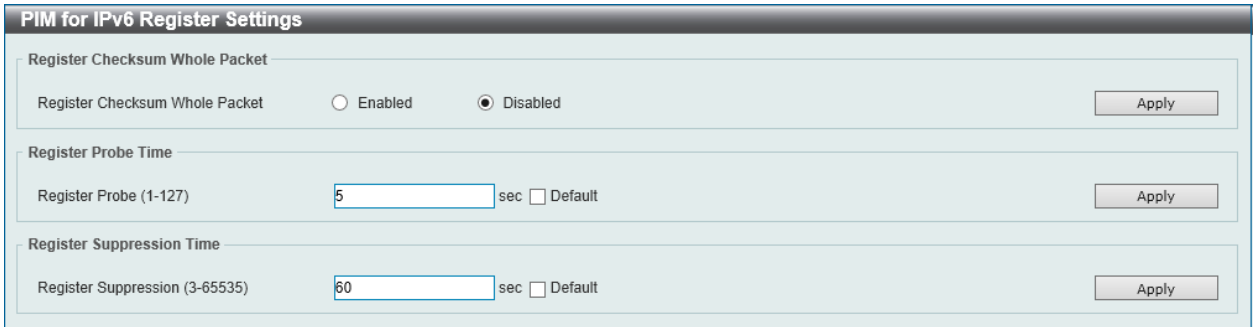


図 9-133　PIM for IPv6 Register Settings 画面

画面に表示される項目：

項目	説明
Register Checksum Whole Packet	
Register Checksum Whole Packet	全パケットのレジスタチェックサムを有効 / 無効に設定します。本設定を有効にした場合、ルータはデータ部分を含めた全 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。デフォルトでは、レジスタチェックサム方法は、レジスタメッセージのデータ部分を除いて、PIM RFC に準拠しています。
Register Probe Time	
Register Probe	Register Probe 時間を入力します。設定した時間が経過すると、レジスタストップタイマ（RST）が期限切れになり、DR が RP に Null-Register を送信して、RP により Register-Stop メッセージが再送信されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-127（秒） • 初期値：5（秒）
Register Suppression Time	
Register Suppression	Register Suppression のタイムアウト値を入力します。DR は、Register-Stop メッセージを受信すると、サプレッションタイマを開始します。抑制期間中、DR は RP への Register-encapsulated データの送信を停止します。指定ルータでこの機能を使用してください。レジスタストップタイマの設定で負の値が発生しないようにするには、「Register Probe」時間の値が「Register Suppression」時間の半分未満である必要があります。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：3-65535（秒） • 初期値：60（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

■ 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 IPv6 > 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。

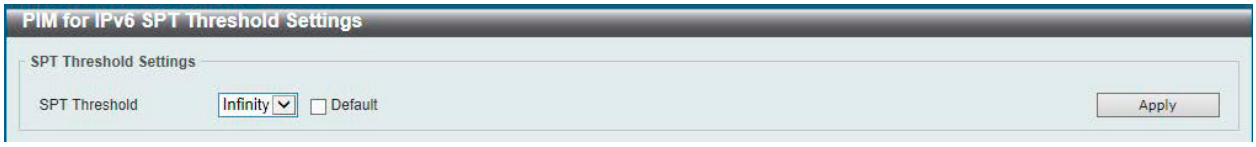


図 9-134　PIM for IPv6 SPT Threshold Settings 画面

画面に表示される項目：

項目	説明
SPT Threshold	SPT しきい値を指定します。「Default」にチェックを入れると、初期値を使用します。 • 「Infinity」- 常に共有ツリーに従います。（初期値） • 「0」- 最初のパケットの到着時にソースツリーを確立します。

「Apply」ボタンをクリックして、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 IPv6 > 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 9-135　PIM for IPv6 SSM Settings 画面

画面に表示される項目：

項目	説明
Multicast Group Address Name	ユーザ指定の SSM グループアドレスを定義するアクセスリストを指定します。「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）を使用します。

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。

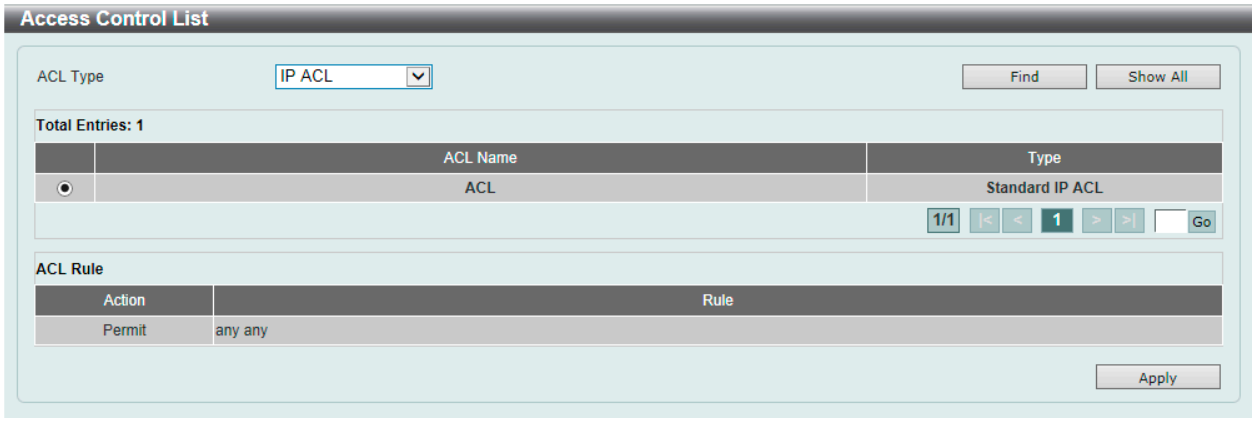


図 9-136　PIM for IPv6 SSM Settings（Show List）- Access Control List 画面

画面に表示される項目：

項目	説明
ACL Type	表示する ACL の種類を指定します。 • 選択肢：「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ACL List	使用するアクセスリストを指定します。

「Find」ボタンをクリックして、指定した種類のアクセスリストを検出します。
「Show All」ボタンをクリックして、すべてのアクセスリストを表示します。
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」ボタンをクリックして、選択したアクセスリストを使用します。

■ 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 IPv6 > 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。

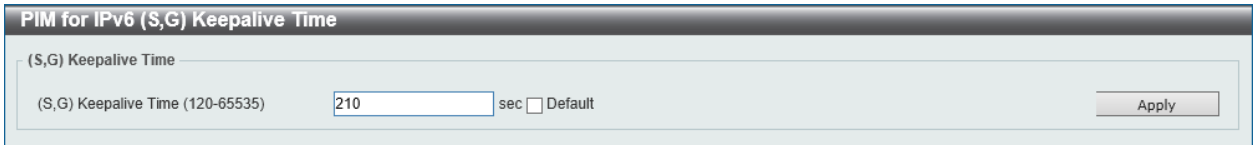


図 9-137　PIM for IPv6 (S,G) Keepalive Time 画面

画面に表示される項目：

項目	説明
(S,G) Keepalive Time	(S,G) キープアライブ時間を入力します。これは、明示的な (S,G) ローカルメンバーシップまたはそれを維持するために受信する (S,G) Join メッセージがない場合に、PIM ルータが (S,G) 状態を維持する期間です。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：120-65535（秒） • 初期値：210（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

■ PIM for IPv6 Multicast Route 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で見つかった宛先グループへの最適パスを使用します。

L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv6 > PIM for IPv6 Multicast 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。

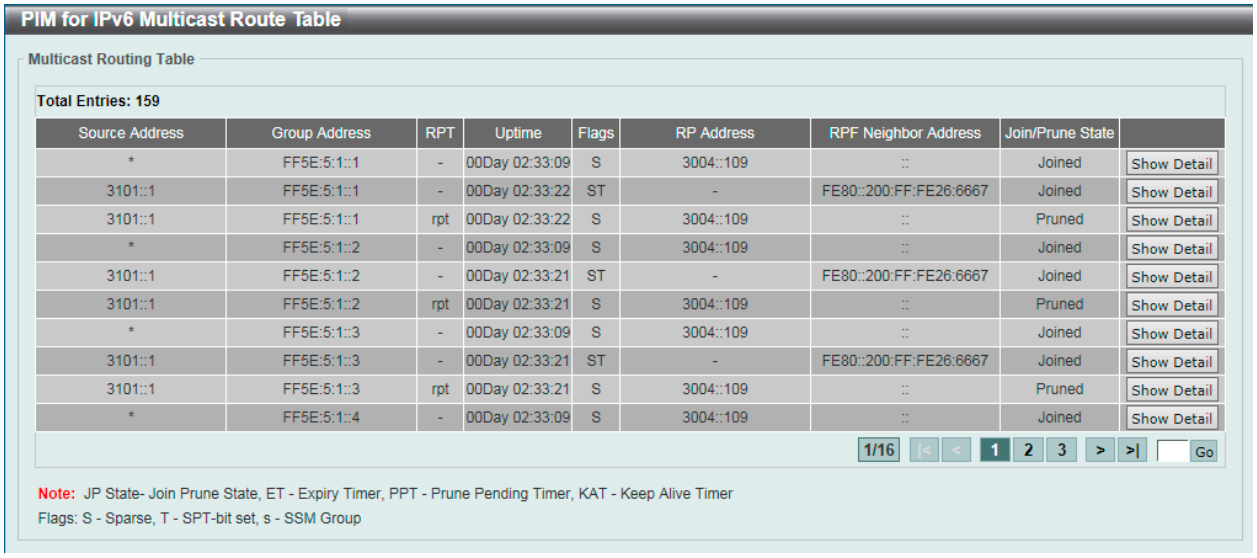


図 9-138　PIM for IPv6 Multicast Route Table 画面

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。

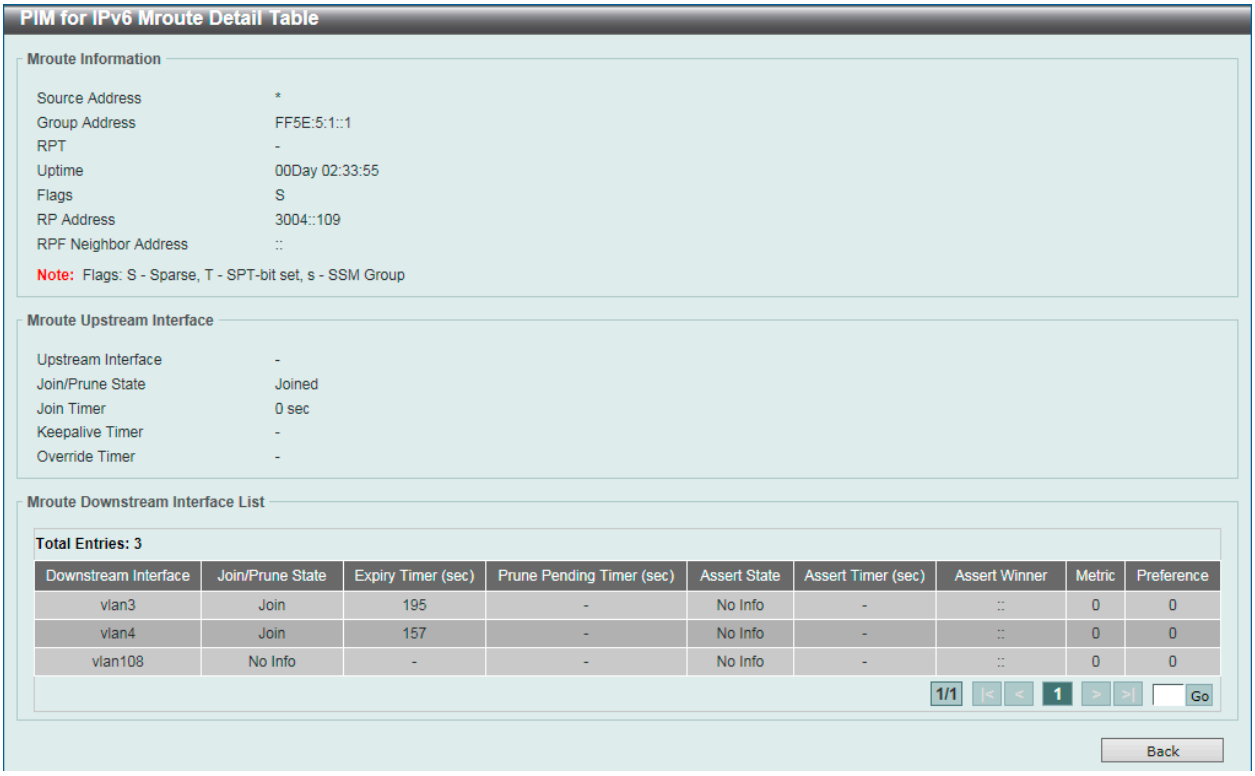


図 9-139　PIM for IPv6 Mroute Table (Show Detail) - PIM for IPv6 Mroute Detail Table 画面

前の画面に戻るには、「Back」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

■ PIM for IPv6 Neighbor Table（IPv6 PIM Neighbor テーブル）

IPv6 PIM ネイバ情報を表示します。

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。

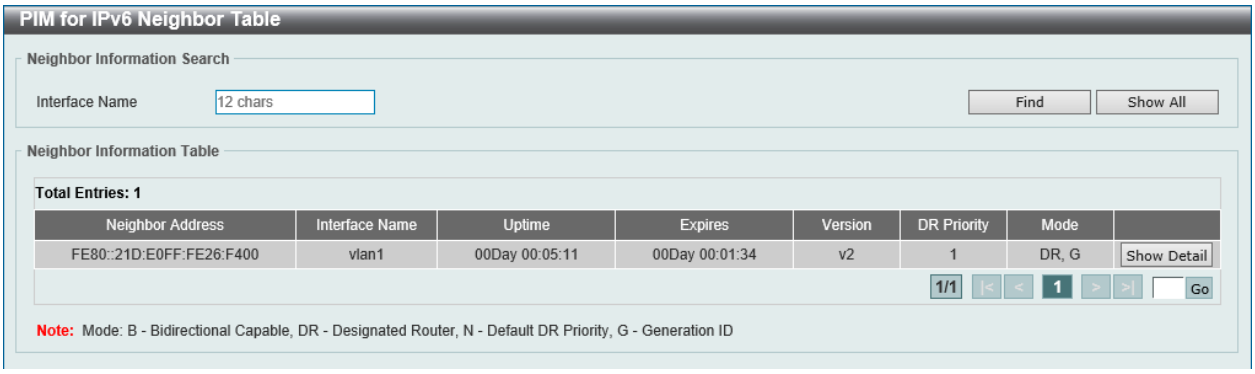


図 9-140　PIM for IPv6 Neighbor Table 画面

画面に表示される項目：

項目	説明
Interface Name	表示する VLAN インタフェース名を指定します。

「Find」ボタンをクリックして、入力した情報を基にエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。
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」ボタンをクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。



図 9-141　PIM for IPv6 Neighbor Table（Show Detail）- PIM for IPv6 Neighbor Detail Table 画面

前の画面に戻るには、「Back」ボタンをクリックします。

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。

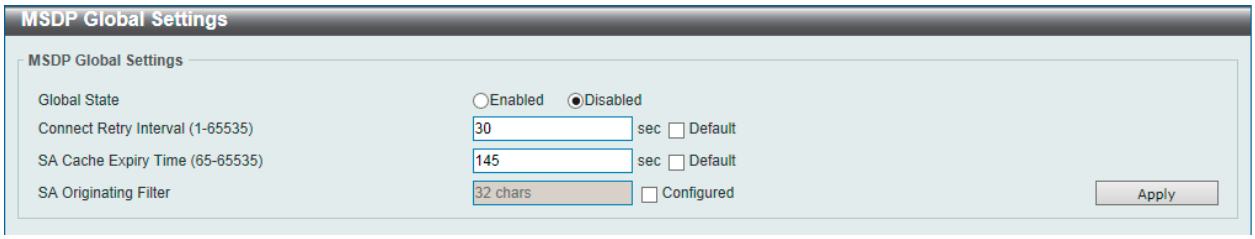


図 9-142　MSDP Global Settings 画面

画面に表示される項目：

項目	説明
Global State	MSDP のグローバルステータスを有効 / 無効に設定します。
Connect Retry Interval	接続再試行間隔を入力します。これは、ピア・セッションのリセットから再確立の試行までの間に、MSDP ピアが待機する時間を設定するために使用されます。時間間隔を大きくすると、ピア・セッションの再確立を試行するまでの時間が遅延します。最適な結果を得るには、1~60 秒の範囲で値を設定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
SA Cache Expiry Time	Source-Active（SA）キャッシュエントリの有効期限を入力します。SA の発信元の間隔は 60 秒であり、変更できません。SA キャッシュの有効期限により、ネットワーク上で予期されるパケット損失の暗黙的なチューニングが可能になります。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：65-65535（秒）
SA Originating Filter	「Configured」オプションを選択し、SA 発信フィルタ文字列を入力します（32 文字以内）。RP の設定により MSDP が実行され、この RP に登録するすべてのローカルソースの SA メッセージを発信します。リストを使用してフィルタを設定すると、RP は、標準 IP アクセスリストで定義されている（S,G）ペアに一致する指定されたグループに送信することによって、ローカルソースの SA メッセージのみを発信します。 「Configured」オプションを選択し、フィルタ文字列を指定しない場合、すべてのローカルソースの SA メッセージからの RP を防ぐことができます。

「Apply」ボタンをクリックして、設定内容を適用します。

■ 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。

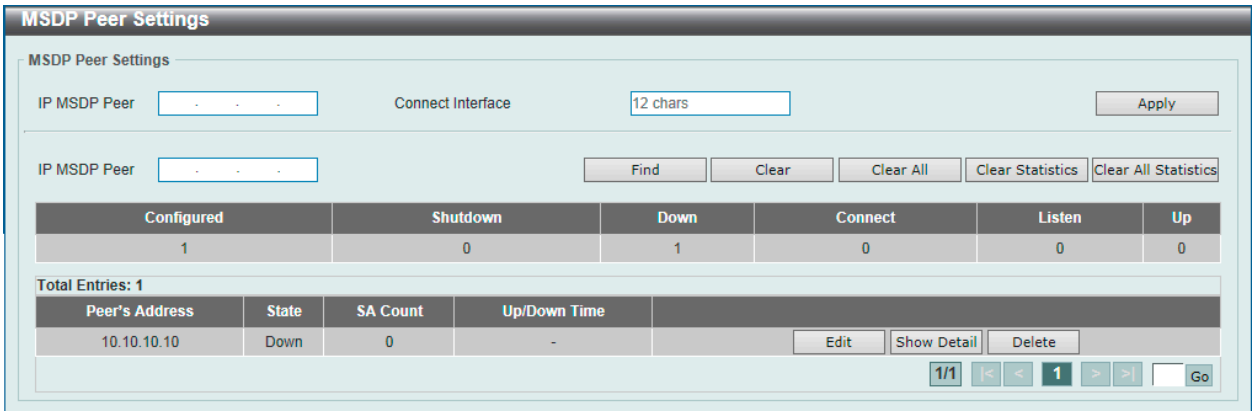


図 9-143　MSDP Peer Settings 画面

画面に表示される項目：

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 文字以内）を指定します。TCP 接続のソース IP アドレスとして使用するローカルインタフェースを指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

エントリ / 統計情報のクリア・検索

「Clear」ボタンをクリックして、入力したエントリをクリアします。
「Clear All」ボタンをクリックして、入力したエントリを全てクリアします。
「Clear Statistics」ボタンをクリックして、入力したエントリの統計情報をクリアします。
「Clear All Statistics」ボタンをクリックして、入力したエントリの統計情報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。

エントリの編集・詳細表示・削除

「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Show Detail」ボタンをクリックして、指定エントリの詳細について表示します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

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

「Edit」をクリックすると、以下の画面が表示されます。

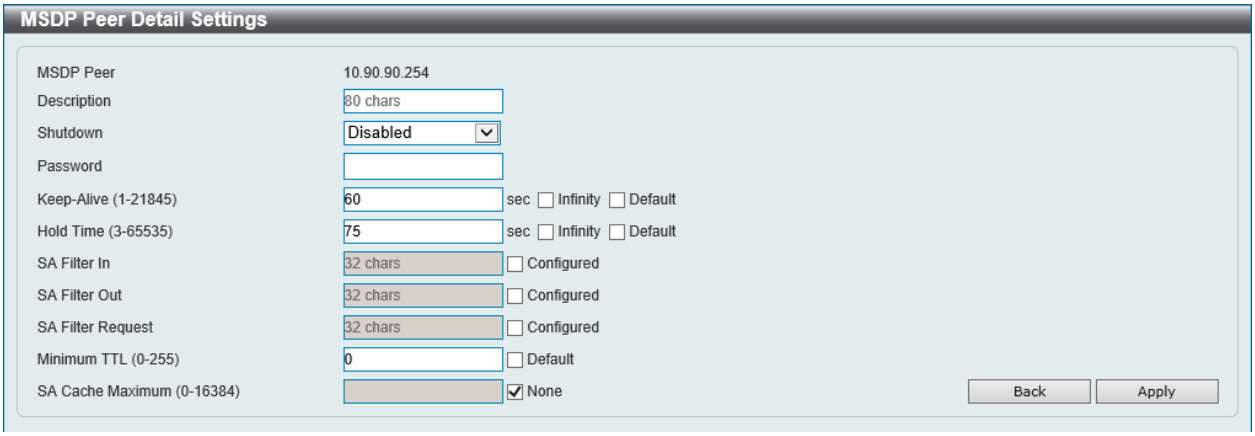


図 9-144　MSDP Peer Settings（Edit）- MSDP Peer Detail Settings 画面

画面に表示される項目：

項目	説明
Description	MSDP ピアの説明（80 文字以内）を入力します。

項目	説明
Shutdown	シャットダウン機能を有効 / 無効に設定します。シャットダウン状態は、既存の MSDP ピアで設定する必要があります。MSDP ピアがシャットダウン状態の場合、2 つのピア間の TCP 接続は確立されません。MSDP ピアが no shutdown 状態に変更された場合、2 つのピア間の TCP 接続は再確立を試みます。
Password	2 つのピア間の TCP 接続用の MD5 パスワードを入力します。MD5 認証は、両方の MSDP ピアで同じパスワードを使用する必要があります。パスワードが異なる場合、ピア間の接続を確立できません。
Keep-Alive	キープアライブの時間を入力します。キープアライブ間隔は、MSDP TCP 接続のリモート側で設定されたホールド時間より短くする必要があります。そうでない場合、MSDP Keep-Alive メッセージを受信する前に、MSDP TCP 接続のリモート側が切断される可能性があります。「Infinity」オプションを指定すると、キープアライブメッセージを送信しないように MSDP ピアを設定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-21845（秒） • 初期値：60（秒）
Hold Time	ホールドタイムの値を入力します。Hold Time インターバルは、MSDP TCP 接続のリモート側で設定されたキープアライブタイムよりも大きくなければなりません。そうでない場合、MSDP Keep-Alive メッセージを受信する前に MSDP TCP 接続が切断される可能性があります。2 つのピア間の接続が切断されないように指定するには、「Infinity」オプションを選択します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：3-65535（秒）
SA Filter In	「Configured」オプションを選択し、SA filter-in 文字列を入力します（32 文字以内）。ルータは、指定されたピアから送信されたすべての SA メッセージを受信します。この文字列を指定しないと、ルータは指定されたピアから送信されたすべての SA メッセージを無視します。この文字列を設定することで、ルータは、標準 IP アクセスリストで定義されている（S,G）ペアに一致する指定されたピアからの受信 SA メッセージのみを受信します。
SA Filter Out	「Configured」オプションを選択し、SA filter-Out 文字列を入力します（32 文字以内）。ルータは、すべての SA メッセージを MSDP ピアに転送します。この文字列を指定しないと、ルータは指定されたピアへの SA メッセージの転送を停止します。この文字列を指定することで、ルータは、標準 IP アクセスリストで定義されている（S,G）ペアに一致する SA メッセージのみを、指定されたピアに転送します。
SA Filter Request	「Configured」オプションを選択し、SA filter-Request 文字列を入力します（32 文字以内）。ルータは、指定されたピアからのすべての SA 要求メッセージを処理します。この文字列を指定しないと、ルータは指定されたピアからの Source-Active 要求メッセージの処理を停止します。この文字列を指定することで、ルータは、指定されたピアからの標準 IP アクセスリストで定義されているグループを要求する SA 要求メッセージのみを処理します。
Minimum TTL	最小 TTL 値を入力します。SA メッセージが MSDP ピアから送信されるときに、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）値が減少する際、減少した TTL 値が SA メッセージが送信された MSDP ピアの最小 TTL 値より小さいと、SA は送信されません。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：0
SA Cache Maximum	SA キャッシュの最大値を入力します。SA キャッシュエントリの最大値が 0 に設定されている場合、本スイッチはピアから SA キャッシュエントリを学習できません。SA キャッシュエントリの最大値が既存の SA キャッシュエントリより小さい場合、SA キャッシュエントリの数が最大値に等しくなるまで、古い既存の SA キャッシュエントリは削除されます。「None」オプションを指定すると、Source-Active キャッシュエントリの数に制限を適用しません。 • 設定可能範囲：0-16383

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

「Show Detail」をクリックすると、以下の画面が表示されます。

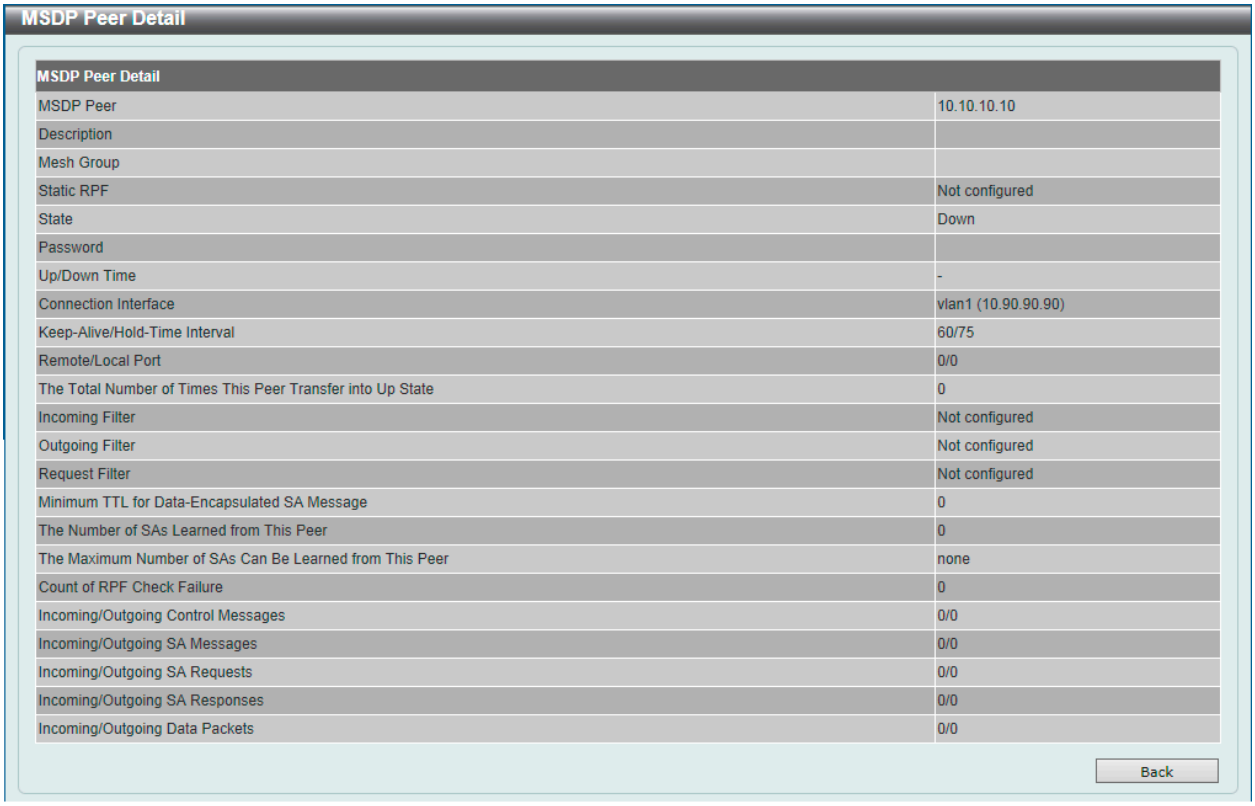


図 9-145　MSDP Peer Settings（Show Detail）- MSDP Peer Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

■ MSDP SA Cache（MSDP SA キャッシュ）

Multicast Source Discovery Protocol（MSDP）SA のキャッシュを表示、削除します。

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。

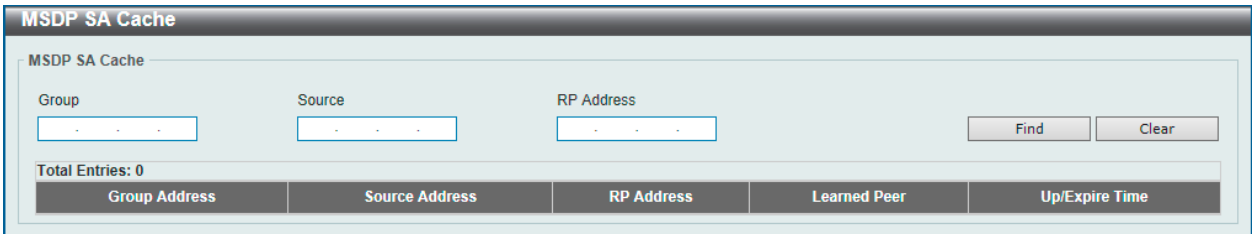


図 9-146　MSDP SA Cache 画面

画面に表示される項目：

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」ボタンをクリックして、入力した情報に基づくエントリをクリアします。
「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。

■ 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 プレフィックスリストが設定されると、ピアはプレフィックスリスト内の RP に対してのみスタティック RPF ピアになります。RP プレフィックスリストなしで複数のスタティック RPF ピアを指定した場合、アドレスが最も小さい接続ピアのみがアクティブなスタティック RPF ピアになります。MSDP ピアがスタティック RPF ピアとして複数設定されていると、最新の設定が有効になります。MSDP ピアが一つだけの場合、この MSDP ピアはスタティック RPF ピアとして動作します。

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。

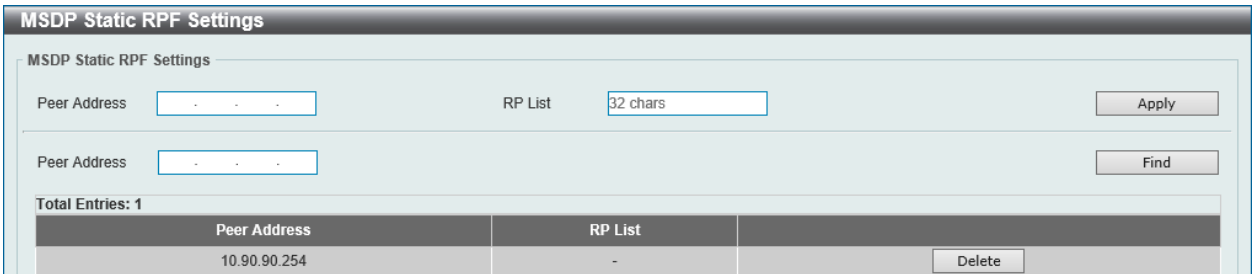


図 9-147　MSDP Static RPF Settings 画面

画面に表示される項目：

項目	説明
Peer Address	MSDP ピアアドレスを指定します。
RP List	RP プレフィックスリストを定義する標準 IP アクセスリスト（32 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、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。

■ 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。

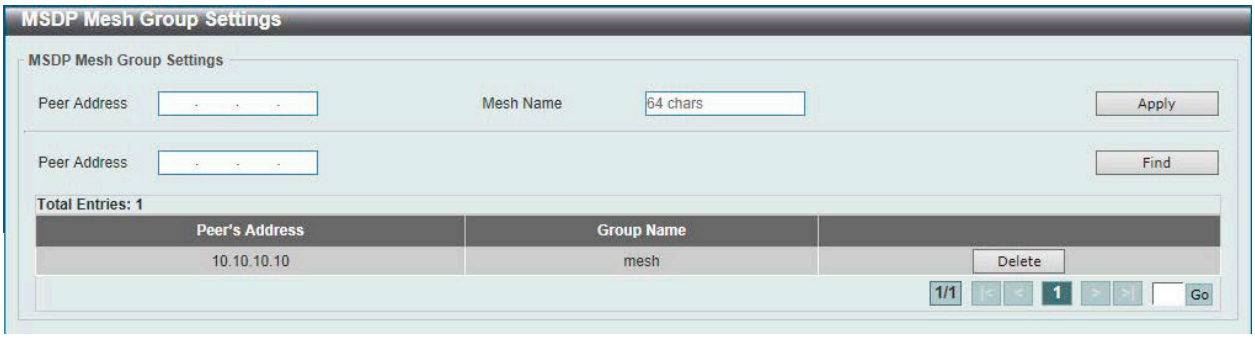


図 9-148　MSDP Mesh Group Settings 画面

画面に表示される項目：

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 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
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（IPMC）のグローバル設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Global Settings の順にメニューをクリックして、以下の画面を表示します。

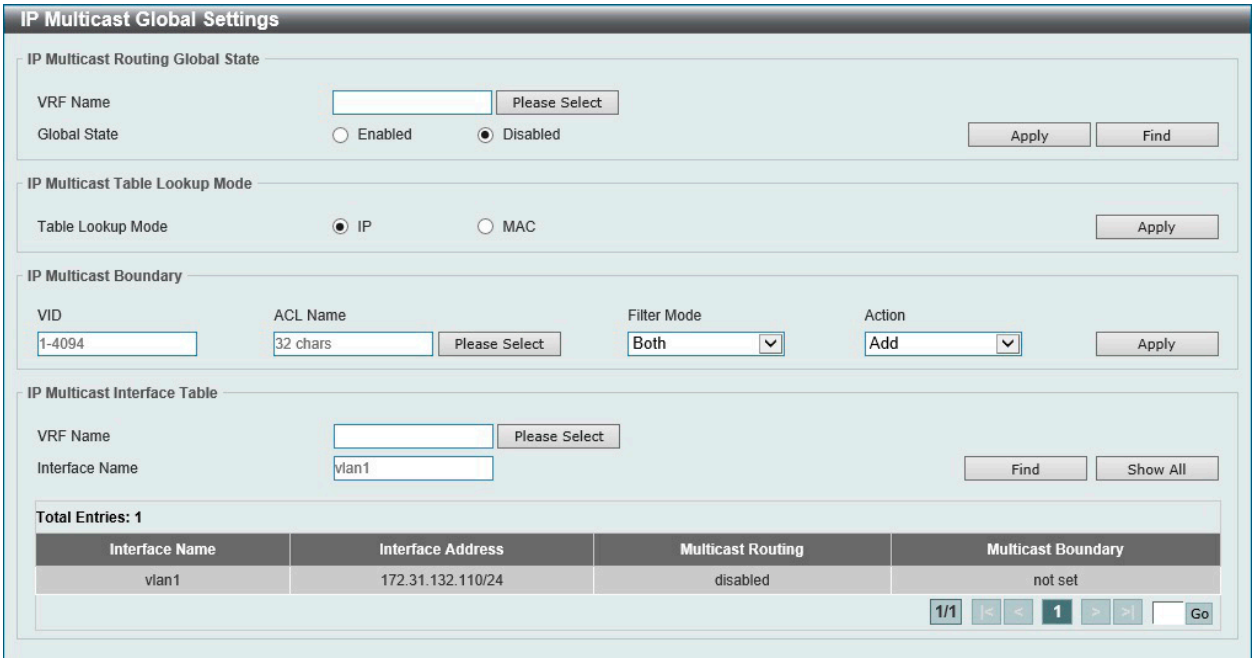


図 9-149　IP Multicast Global Settings 画面

画面に表示される項目：

項目	説明
IP Multicast Routing Global State（EI モードのみ）	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Global State	IP マルチキャストルーティングを有効 / 無効に設定します。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。
IP Multicast Table Lookup Mode	
Table Lookup Mode	IP マルチキャストフォワーディングのルックアップモードを指定します。 • 「IP」- IP アドレスに基づいてマルチキャストフォワーディングルックアップを行います。 • 「MAC」- MAC アドレスに基づいてマルチキャストフォワーディングルックアップを行います。
IP Multicast Boundary（EI モードのみ）	
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094
ACL Name	使用する標準 IP アクセスリスト名（32 文字以内）を指定します。「Please Select」をクリックし、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」- 受信 / 送信トラフィックの両方をフィルタします。 • 「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。これにより、特定のグループトラフィックまたは特定の送信元からの特定のグループのマルチキャストトラフィックがフィルタリングされます。
Action	実行するアクションを指定します。 • 選択肢：「Add」「Delete」
IP Multicast Interface Table（EI モードのみ）	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Interface Name	表示するインタフェース名を指定します。

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

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

「Please Select」をクリックすると、次の画面を表示します。



図 9-150　IP Multicast Global Settings（Please Select）- ACL Access List 画面

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

IP Multicast Route Settings（IP マルチキャストルート設定）（EI モードのみ）

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。

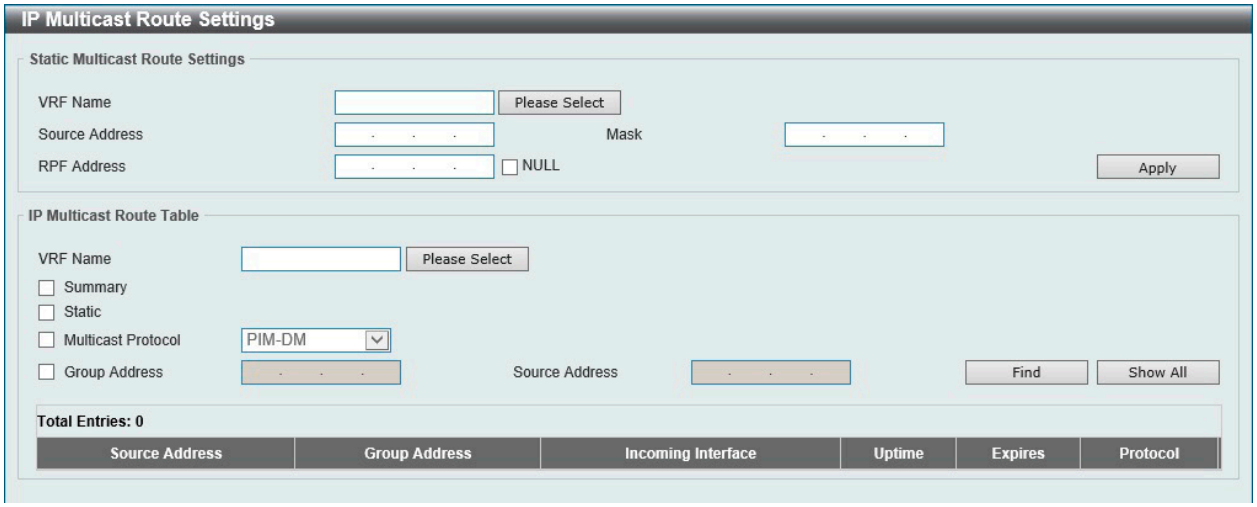


図 9-151　IP Multicast Route Settings 画面

画面に表示される項目：

項目	説明
Static Multicast Route Settings	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
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 チェックは常に失敗します。
IP Multicast Route Table	
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
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-DM ルートのみを表示します。 • 「PIM-SM」- PIM-SM ルートのみを表示します。 • 「DVMRP」- DVMRP ルートのみを表示します。
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	ソース IP アドレスを指定します

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

IP Multicast RPF Table（IP マルチキャスト RPF テーブル）（EI モードのみ）

ユニキャストホストアドレスの RPF（Reverse Path Forwarding）情報を表示します。

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。

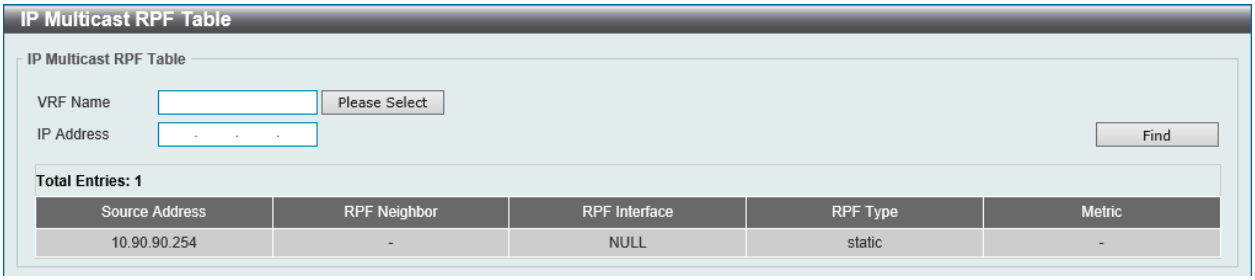


図 9-152　IP Multicast RPF Table 画面

画面に表示される項目：

項目	説明
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
IP Address	ユニキャスト IPv4 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。

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）データベースの表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast 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。

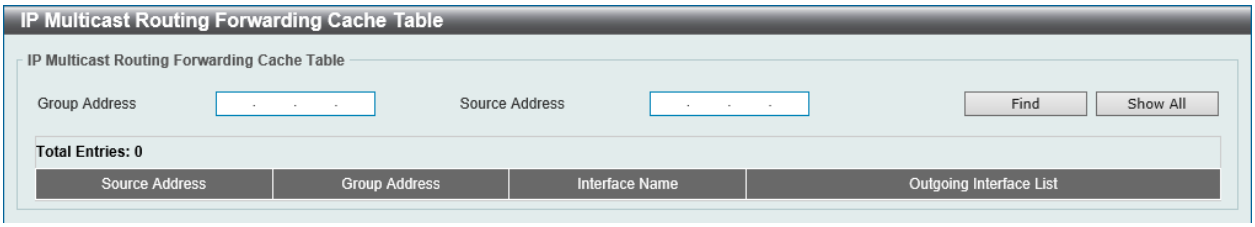


図 9-153　IP Multicast Forwarding Cache 画面

画面に表示される項目：

項目	説明
Group Address	マルチキャストグループ IP アドレスを指定します。
Source Address	ソース IP アドレスを指定します。

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

IP Multicast Protocol Statistics（IP マルチキャストプロトコル統計）（EI モードのみ）

IP Multicast Protocol Statistics（IP マルチキャストプロトコル統計）の表示、削除を行います。

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。

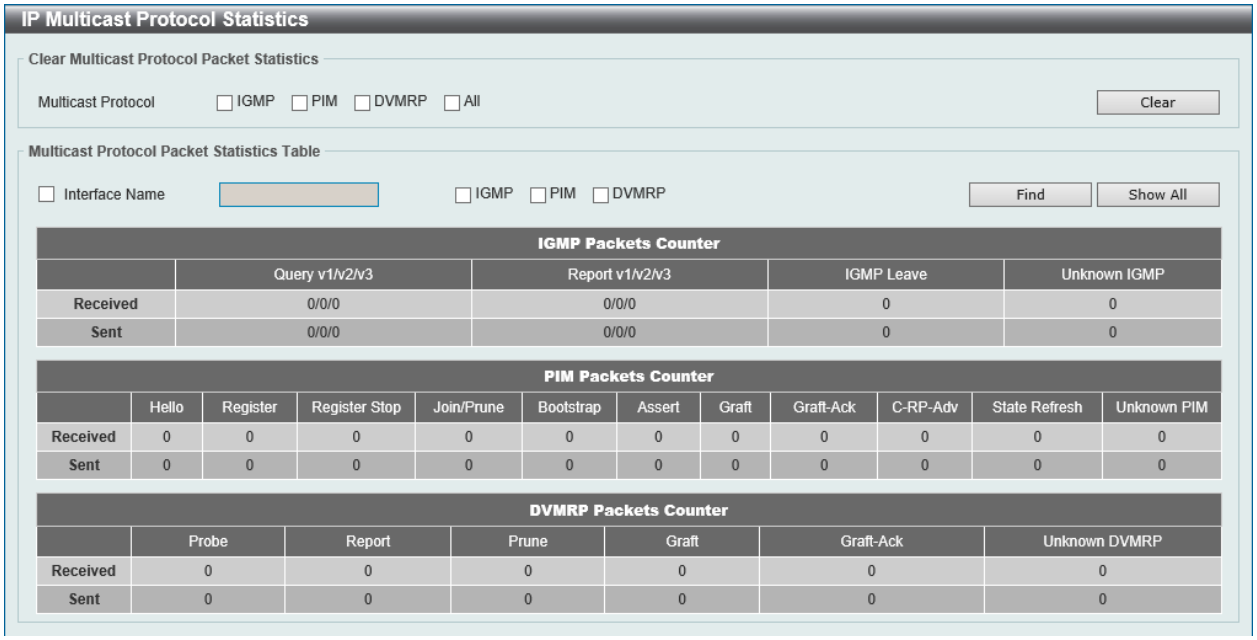


図 9-154　IP Multicast Protocol Statistics 画面

画面に表示される項目：

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。 • 選択肢：「IGMP」「PIM」「DVMRP」「All」
Multicast Protocol Packet Statistics Table	
Interface Name	表示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。 • 選択肢：「IGMP」「PIM」「DVMRP」

「Clear」ボタンをクリックして、入力情報に基づく統計をクリアします。
「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。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

Control Packet CPU Filtering（コントロールパケット CPU フィルタリング）

コントロールパケット CPU フィルタリングの表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > Control Packet CPU Filtering の順にメニューをクリックして、以下の画面を表示します。

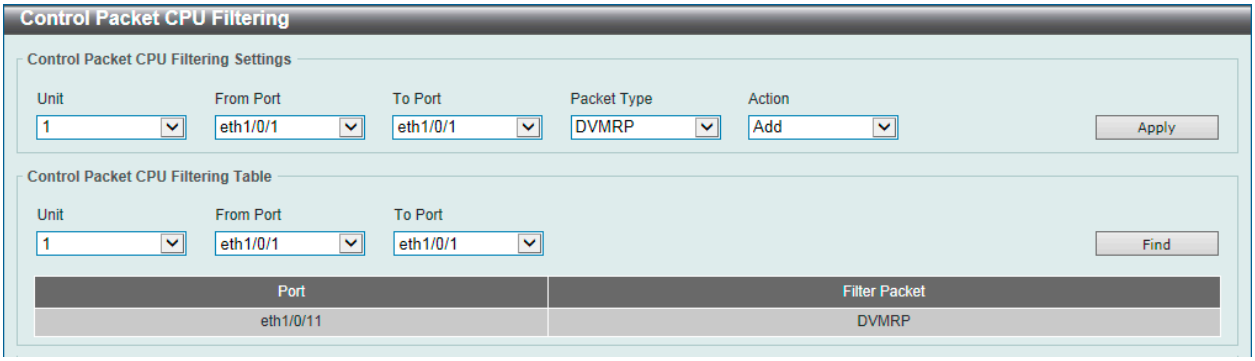


図 9-155　Control Packet CPU Filtering 画面

画面に表示される項目：

項目	説明
Control Packet CPU Filtering Settings	
Unit	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。
Packet Type	パケットの種類を指定します。 • 「DVMRP」- CPU に対して送信された「DVMRP L3 コントロールパケット」を破棄します。 • 「PIM」- CPU に対して送信された「PIM L3 コントロールパケット」を破棄します。 • 「IGMP Query」- CPU に対して送信された「IGMP Query L3 コントロールパケット」を破棄します。 • 「OSPF」- CPU に対して送信された「OSPF L3 コントロールパケット」を破棄します。 • 「RIP」- CPU に対して送信された「RIP L3 コントロールパケット」を破棄します。 • 「VRRP」- CPU に対して送信された「VRRP L3 コントロールパケット」を破棄します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Control Packet CPU Filtering Table	
Unit	表示するユニットを指定します。
From Port / To Port	表示するポートの始点 / 終点を設定します。

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

IPv6MC（IPv6 マルチキャスト設定）

L3 Features > IP Multicast Routing Protocol > IPv6MC

IPv6 Multicast Global Settings（IPv6 マルチキャストグローバル設定）（EI モードのみ）

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。

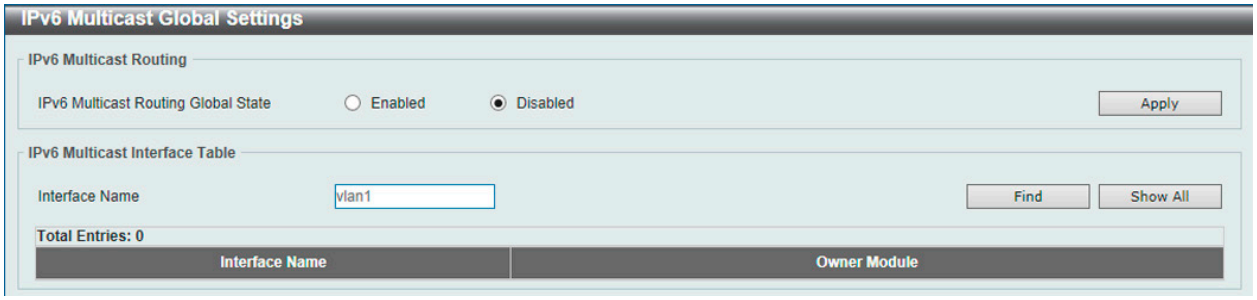


図 9-156　IPv6 Multicast Global Settings 画面

画面に表示される項目：

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機能のグローバルステータスを有効 / 無効に設定します。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のルーティングを停止します。
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」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv6 Static Multicast Route Settings（IPv6 スタティックマルチキャストルート設定）（EI モードのみ）

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 プロトコルには独自のルーティングテーブルはありませんが、ユニキャストルーティングテーブルを使用して、ネットワークに到達するためのリバースパス転送インタフェースを決定します。本画面では、ネットワークの RPF アドレスを指定するための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。

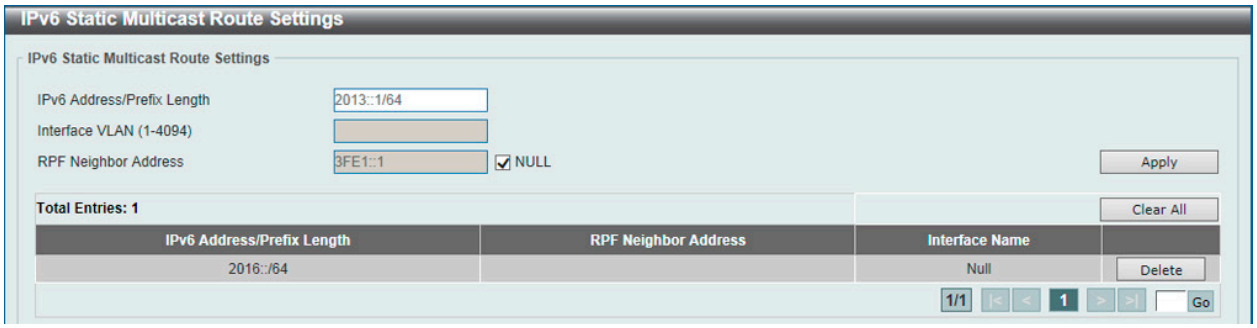


図 9-157　IPv6 Static Multicast Route Settings 画面

画面に表示される項目：

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レフィックス長を指定します。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビットの数を示す 10 進数値の前にスラッシュマークを付ける必要があります。
Interface VLAN	本設定に使用するインタフェース VLAN を指定します。 • 設定可能範囲：1-4094
RPF Neighbor Address	指定したネットワークに到達するために使用するネクストホップの IPv6 アドレスを入力します。「NULL」オプションを選択すると、RPF チェックは常に失敗となります。

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

IPv6 Multicast Routing Table（IPv6 マルチキャストルーティングテーブル）（EI モードのみ）

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 9-158　IPv6 Multicast Routing Table 画面

画面に表示される項目：

項目	説明
Group IPv6 Address	マルチキャストグループ IPv6 アドレスを指定します。
Source IPv6 Address	ソース IPv6 アドレスを指定します。
Summary	IPv6 マルチキャストルーティングテーブルのサマリが表示されます。

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

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（IPv6 マルチキャストフォワーディングキャッシュ）データベースを表示します。

L3 Features > IPv6 Multicast Routing Protocol > IPv6MC > IPv6 Multicast 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 9-159　IPv6 Multicast Forwarding Cache Table 画面

画面に表示される項目：

項目	説明
Group IPv6 Address	マルチキャストグループ IPv6 アドレスを指定します。
Source IPv6 Address	ソース IPv6 アドレスを指定します。

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

IPv6 RPF Table（IPv6 RPF テーブル）（EI モードのみ）

ユニキャストホストアドレスの RPF（Reverse Path Forwarding）情報の表示、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。

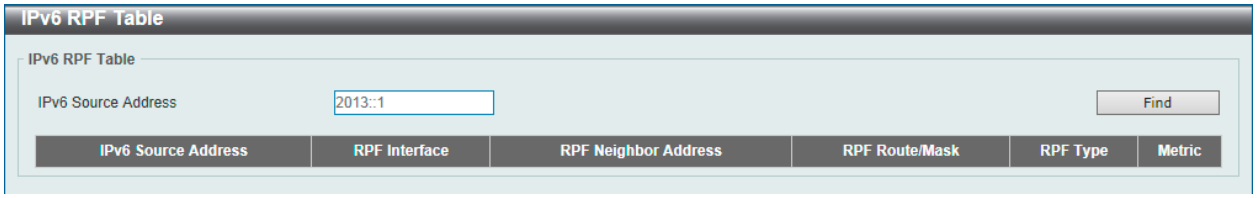


図 9-160　IPv6 RPF Table 画面

画面に表示される項目：

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」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。

BGP（Border Gateway Protocol）（EI モードのみ）

L3 Features > BGP

BGP（Border Gateway Protocol）の設定を行います。

注意　BGP を VRF-Lite で使用する場合の接続は eBGP に制限されます。

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。

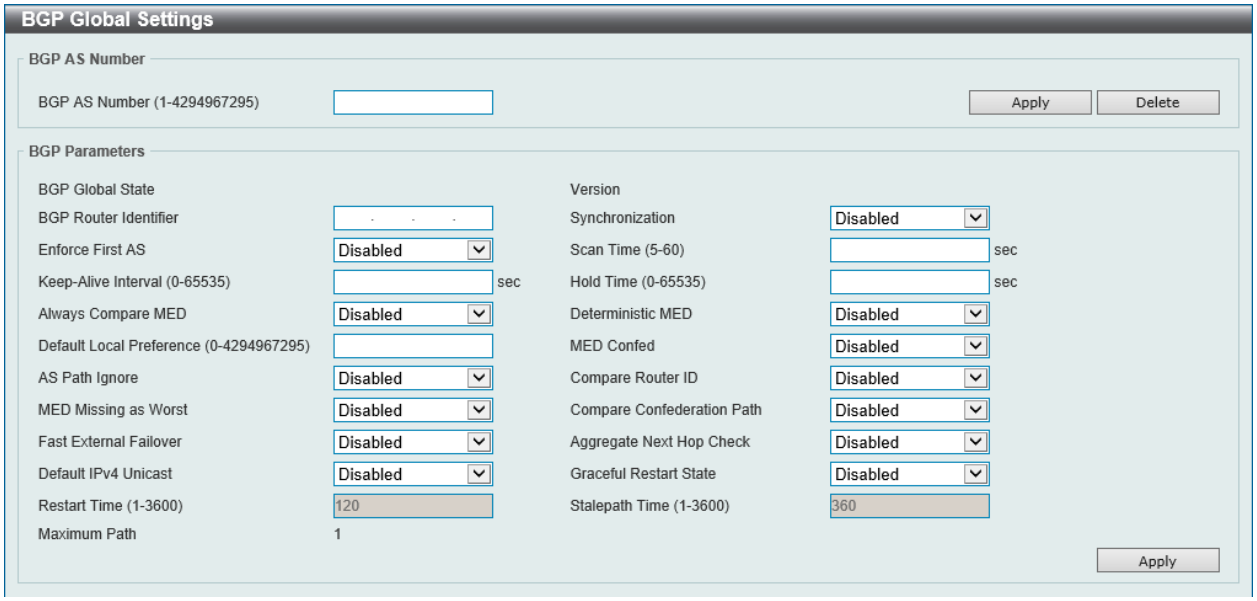


図 9-161　BGP Global Settings 画面

画面に表示される項目：

項目	説明
BGP AS Number	
BGP AS Number	BGP AS 番号を入力します。 • 設定可能範囲：1-4294967295
BGP AS Number	
BGP Router Identifier	BGP ルータ ID を IPv4 アドレス形式で指定します。
Synchronization	同期を有効/無効に設定します。同期を有効にすると、ルートがローカルルートであるか、BGP スピーカが IGP によってルートを学習しない限り、BGP スピーカは外部ネイバにルートをアドバタイズしません。

項目	説明
Enforce First AS	Enforced First AS 機能を有効 / 無効に設定します。このオプションは、eBGP ピアから受信したルートが、AS パスの最初の AS としてピアの AS 番号を持たなければならないことを強制するために使用されます。この機能は、誤って設定されたピアによるローカルルータに対するスプーフィングを回避するために使用されます。
Scan Time	スキャンタイムの値を入力します。ルータが BGP ルートのネクストホップのスキャンを有効にすると、ルータはルーティングテーブル内のネクストホップに到達するルートがあるかどうかを定期的にチェックします。 • 設定可能範囲：5-60（秒）
Keep-Alive Interval	キープアライブ間隔の値を入力します。これは、ソフトウェアが BGP ピアに keep-alive メッセージを送信するために使用する間隔です。 • 設定可能範囲：0-65535（秒）
Hold Time	ホールドタイム値を入力します。Keep Alive メッセージがタイムアウトする時間を指定します。ソフトウェアは、タイムアウト後に BGP ピアが Dead であると宣言します。 • 設定可能範囲：0-65535（秒）
Always Compare MED	Multi Exit Discriminator（MED）を常に比較する機能の有効 / 無効を選択します。有効にした場合、同じまたは異なる自律システムのいずれのネイバからアドバタイズされるパスであっても、ベストパス選択において MED を比較します。
Deterministic MED	Deterministic MED 機能を有効 / 無効に設定します。有効にした場合、最適なルート選択の選択で、同じ自律システム内から受信したすべてのパス間の MED 値を比較します。
Default Local Preference	デフォルトのローカル優先値を入力します。本設定は、ローカル AS から同じ宛先ネットワークへの優先出口ポイントを制御するために使用されます。ローカルプリファレンスは、iBGP ピアにアドバタイズされたルートとともに送信されます。外部ルートがローカルルータと iBGP ピアルータの両方を介して到達可能な場合、ローカルプリファレンス値によって、外部ルートに到達する優先出口ポイントが決定されます。 • 設定可能範囲：0-4294967295
MED Confed	MED コンフェデレーション機能の有効 / 無効を設定します。本設定を有効にすると、BGP プロセスはコンフェデレーションピアから受信したルートの MED を比較します。パスに外部 AS があるルートの場合、比較は行われません。
AS Path Ignore	AS Path Ignore 機能を有効 / 無効に設定します。本設定を有効にすると、最適パスの選択における識別要因として AS パスを無視します。
Compare Router ID	ルータ ID 比較機能を有効 / 無効に設定します。BGP プロセスにおいて、最適なパス選択でルータ ID がタイブレーカーとして使用されます。本設定を有効にすると、他のすべての属性が等しい場合に、ルータ ID が最も小さいパスが最適として選択されます。
MED Missing As Worst	MED Missing As Worst 機能を有効 / 無効に設定します。MED 属性が含まれていない場合、BGP プロセスによってルートに Infinity 値が割り当てられます。
Compare Confederation Path	コンフェデレーションパス比較機能を有効 / 無効に設定します。本設定を有効にすると、BGP プロセスはベストパス選択でコンフェデレーション AS パス長を比較します。コンフェデレーション AS パスの長さが短い方が優先されます。
Fast External Fallover	Fast External Failover 機能を有効 / 無効に設定します。直接接続された外部ピアの BGP セッションの Fast External Failover をグローバルに有効または無効にするために使用されます。本設定を有効にすると、リンクがダウンした場合、セッションはただちにリセットされます。無効にすると、セッションはデフォルトの保留タイマが期限切れになるまでリセットされません。
Aggregate Next Hop Check	Aggregate Next Hop Check 機能を有効 / 無効に設定します。BGP 集約ルートのネクストホップのチェックを有効にするために使用します。本設定が有効な場合、同じネクストホップ属性を持つルートのみ集約できます。
Default IPv4 Unicast	デフォルト IPv4 ユニキャスト機能を有効 / 無効に設定します。IPv4 ユニキャストルーティング情報の交換を有効にするために使用します。
Graceful Restart State	すべての BGP ネイバの BGP グレースフルリスタート機能を有効 / 無効に設定します。
Restart Time	グレースフルリスタートを有効にした場合、リスタート時間を入力します。ネイバが再起動するために必要な最大時間を指定します。 • 設定可能範囲：1-3600（秒）
Stalepath Time	グレースフルリスタートが有効な場合、stale-path time を入力します。ネイバが再起動してから古いパスを保持する最大時間を指定します。 • 設定可能範囲：1-3600（秒）

「Apply」ボタンをクリックして、各セクションで行った変更を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

BGP Aggregate Address Settings（BGP アグリゲートアドレス設定）

BGP 集約アドレスを設定します。ルート集約は、ルーティングエントリの数を減らすために使用されるメカニズムです。集約されたルートよりも具体的なルートエントリがある場合、集約ルートはルーティングテーブルに作成されます。集約ルートの特性は、そこに含まれる具体的なルートの特性の組み合わせになります。集約ルートは、ローカル AS からの着信として送信されます。アトミックアグリゲーションフラグは、それらのより具体的なルート情報の AS パス情報が、集約エントリから失われる可能性があること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。

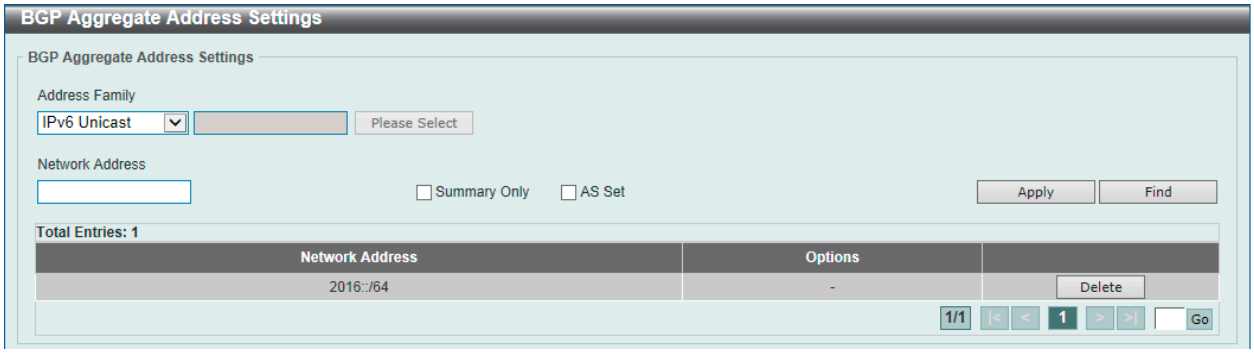


図 9-162　BGP Aggregate Address Settings 画面

画面に表示される項目：

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を使用します。 • 「IPv4 VRF」- VRF インスタンス（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリを使用します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
Network Address	IPv4/IPv6 集約アドレスとネットマスクを入力します。
Summary Only	本オプションにチェックを入れると、集約ルートのみを表示します。
AS Set	本オプションにチェックを入れると、自律システムセットのパス情報を生成します。

「Apply」ボタンをクリックして、設定内容を適用します。

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。

「Please Select」をクリックすると、次の画面が表示されます。

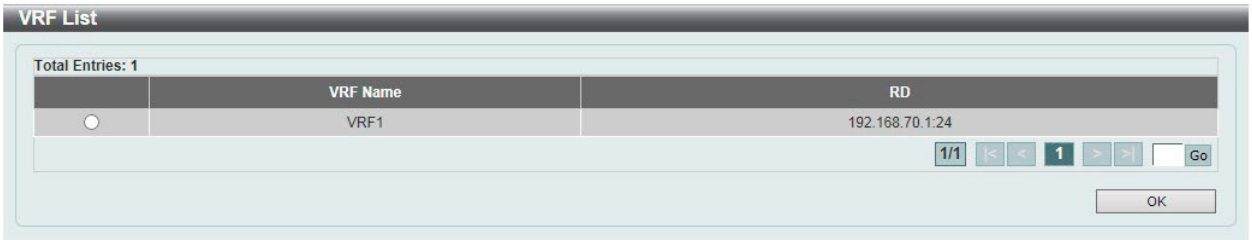


図 9-163　BGP Aggregate Address Settings（Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

BGP Network Settings（BGP ネットワーク設定）

BGP ネットワークを設定します。

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 9-164　BGP Network Settings 画面

画面に表示される項目：

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を使用します。 • 「IPv4 VRF」- VRF インスタンス（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリを使用します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
Network Address	BGP がアドバタイズする IPv4/IPv6 ネットワークアドレスとマスクを入力します。
Route Map Name	ルートマップ名（16 文字以内）を入力します。設定されたネットワークは、指定されたルートマップによってアドバタイズされることを許可される必要があります。

「Apply」ボタンをクリックして、設定内容を適用します。

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。

「Please Select」をクリックすると、次の画面が表示されます。

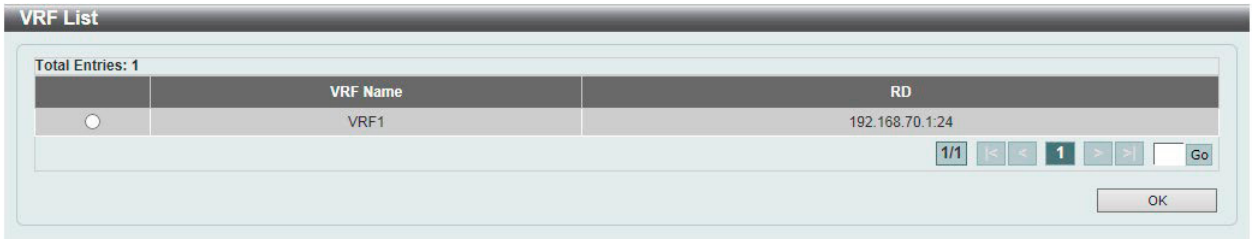


図 9-165　BGP Network Settings（Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

BGP Route Redistribution Settings（BGP ルート再配布設定）

BGP Route Redistribution Settings（BGP ルート再配布設定）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。

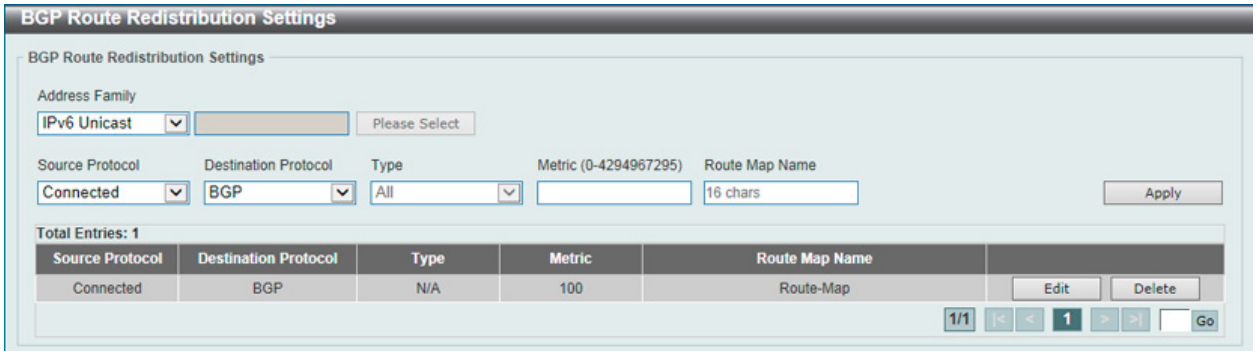


図 9-166　BGP Route Redistribution Settings 画面

画面に表示される項目：

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を使用します。 • 「IPv4 VRF」- VRF インスタンス（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリを使用します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
Source Protocol	送信元のプロトコルを選択します。 • 「Connected」- 接続されたルートを BGP に再配布します。 • 「Static」- スタティックルートを BGP に再配布します。 • 「RIP」- RIP ルートを BGP に再配布します。 • 「OSPF」- OSPF ルートを BGP に再配布します。 • 「ISIS」- ISIS ルートを BGP に再配布します。
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、OSPF タイプを選択します。 • 「All」- OSPF AS 内部ルートと OSPF AS 外部ルートの両方のルートを BGP に再配布します。 • 「External」- AS 外部ルートのみを BGP に再配布します。Type-1 ルートと Type-2 ルートが含まれます。 • 「Internal+E1」- OSPF AS 外部ルート Type-1 と OSPF AS 内部ルートのみを再配布します。 • 「Internal+E2」- OSPF AS 外部ルート Type-2 と OSPF AS 内部ルートのみを再配布します。 • 「Internal」- OSPF 内部ルートのみを再配布します。 • 「External Type1」- OSPF AS 外部ルート Type-1 のみを再配布します。 • 「External Type2」- OSPF AS 外部ルート Type-2 のみを再配布します。
Metric	再配布ルートの BGP メトリック値を入力します。 • 設定可能範囲：0-4294967295
Route Map Name	再配布するネットワークをフィルタリングするために使用されるルートマップ名を入力します。（16 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

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。

「Please Select」をクリックすると、次の画面が表示されます。

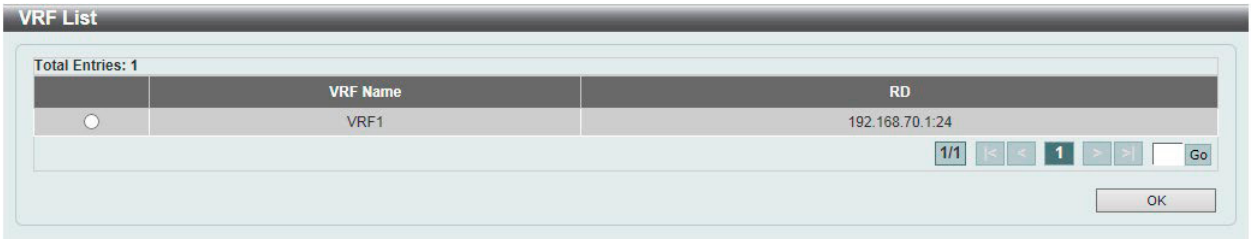


図 9-167　BGP Route Redistribution Settings（Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

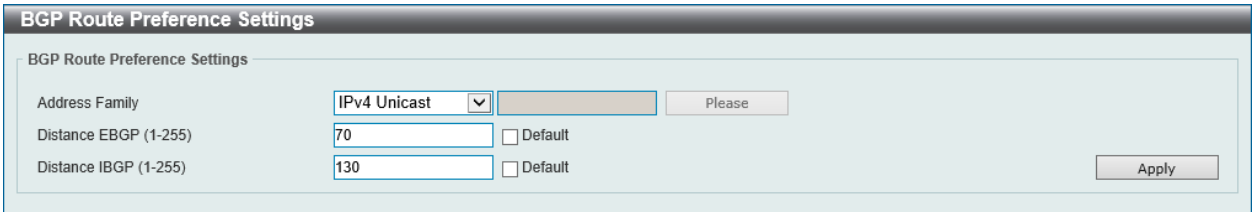


図 9-168　BGP Route Preference Settings 画面

画面に表示される項目：

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を使用します。 • 「IPv4 VRF」- VRF インスタンス（12 文字以内）を入力します。「Please」で既存の VRF インスタンスを選択することも可能です。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
Distance EGBP	ディスタンス eBGP ルート優先値を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255
Distance IBGP	ディスタンス iBGP ルート優先値を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255

「Apply」ボタンをクリックして、設定内容を適用します。

「Please」をクリックすると、次の画面が表示されます。



図 9-169　BGP Route Preference Settings（Please）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。本機能の目的は、不安定なルートのアドバタイズメントを削除して、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。

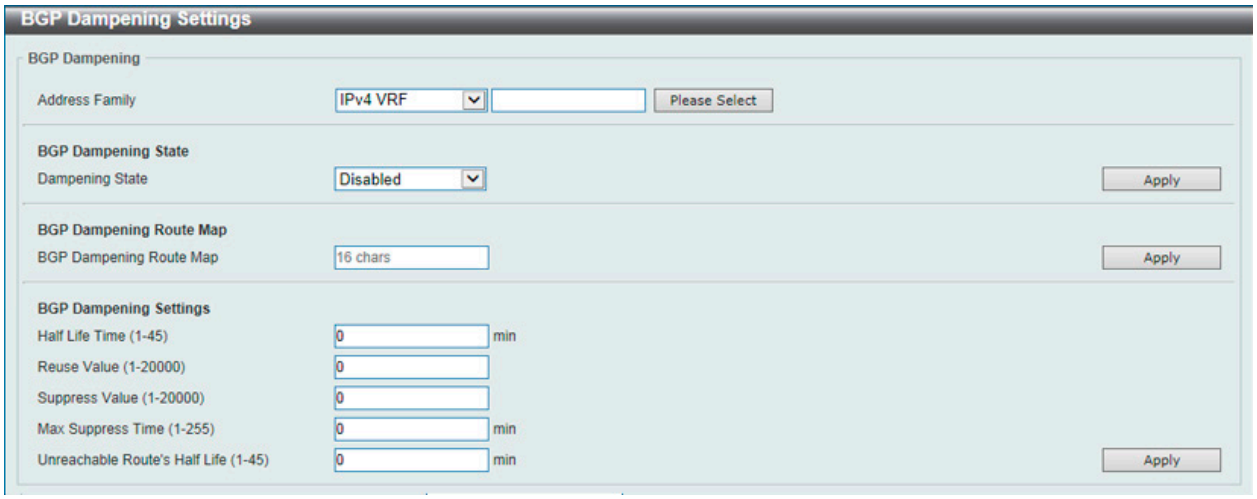


図 9-170　BGP Dampening Settings 画面

画面に表示される項目：

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を使用します。 • 「IPv4 VRF」- VRF インスタンス（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリを使用します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
BGP Dampening State	
Dampening State	BGP ダンプニング機能を有効 / 無効に設定します。
BGP Dampening Route Map	
BGP Dampening Route Map	BGP ダンプニングルートマップ名（16 文字以内）を入力します。
BGP Dampening Settings	
Half Life Time	Half Life Time 値を入力します。設定時間経過後、ルートの累積ペナルティが半分に減少します。 • 設定可能範囲：1-45（分）
Reuse Value	再利用値を入力します。ペナルティが減少し、再利用しきい値を下回ると、ルートは通常のルートとしてルーティングテーブルに再入力されます。 • 設定可能範囲：1-20000
Suppress Value	抑制値を入力します。ペナルティが増加し、抑制しきい値を超えると、ルートはダンプニングルートになりアドバタイズされません。 • 設定可能範囲：1-20000
Max Suppress Time	最大抑制値を入力します。この設定では、ルートがダンプニング状態となる最大時間を指定します。 • 設定可能範囲：1-255（分）
Unreachability Half Life	Unreachability Half Life 値をここに入力します。設定時間経過後、到達不能ルートのペナルティが半分になります。 • 設定可能範囲：1-45（分）

「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。

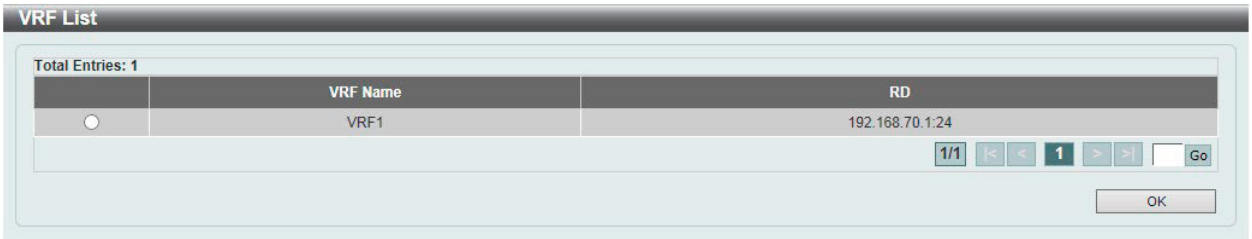


図 9-171　BGP Dampening Settings（Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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、クリアを行います。

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。

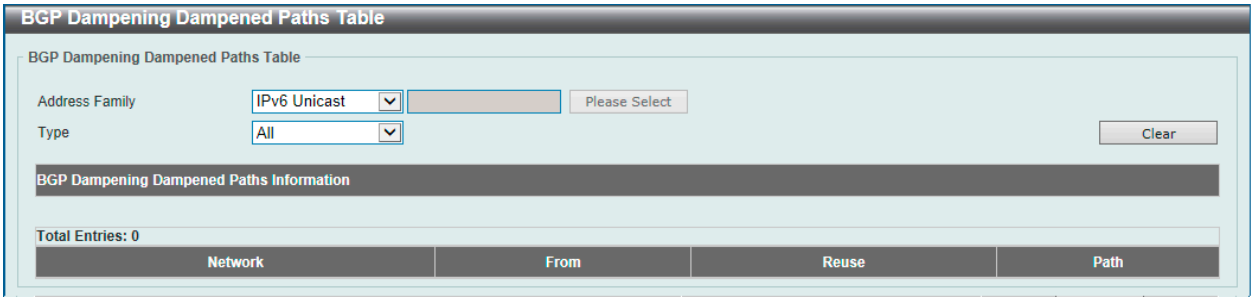


図 9-172　BGP Dampening Dampened Paths Table 画面

画面に表示される項目：

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を使用します。 • 「IPv4 VRF」- VRF インスタンス（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリを使用します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
Type	クリアオプションを指定します。 • 「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。表示される入力欄に IPv4 アドレスを入力します。 • 「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。表示される入力欄に IPv4 開始 / 終了アドレスを入力します。 • 「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。表示される入力欄に IPv6 アドレスを入力します。 • 「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。表示される入力欄に IPv6 アドレスとプレフィックス長を入力します。

「Clear」ボタンをクリックして、指定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 9-173　BGP Dampening Dampened Paths Table（Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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、クリアを行います。

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。

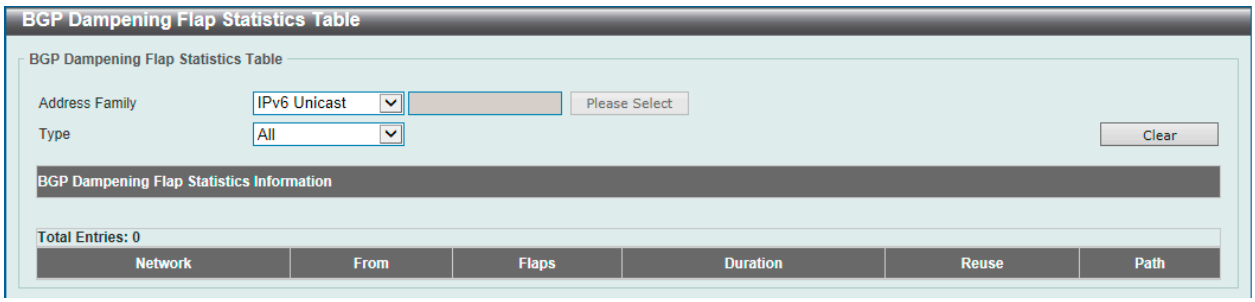


図 9-174　BGP Dampening Flap Statistics Table 画面

画面に表示される項目：

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を使用します。 • 「IPv4 VRF」- VRF インスタンス（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリを使用します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
Type	クリアオプションを指定します。 • 「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。表示される入力欄に IPv4 アドレスを入力します。 • 「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。表示される入力欄に IPv4 開始 / 終了アドレスを入力します。 • 「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。表示される入力欄に IPv6 アドレスを入力します。 • 「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。表示される入力欄に IPv6 アドレスとプレフィックス長を入力します。

「Clear」ボタンをクリックして、指定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。

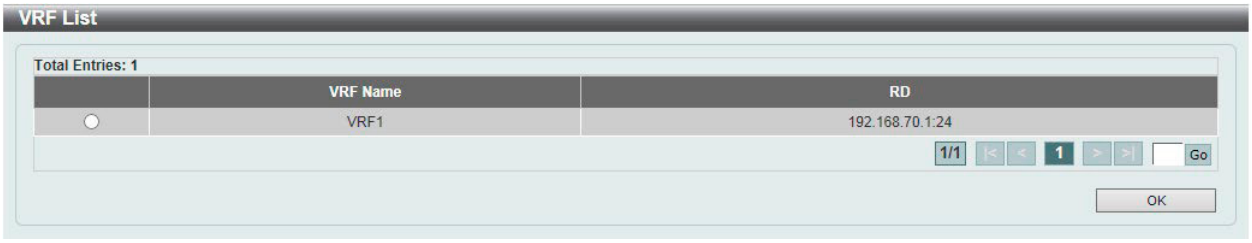


図 9-175　BGP Dampening Flap Statistics Table（Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

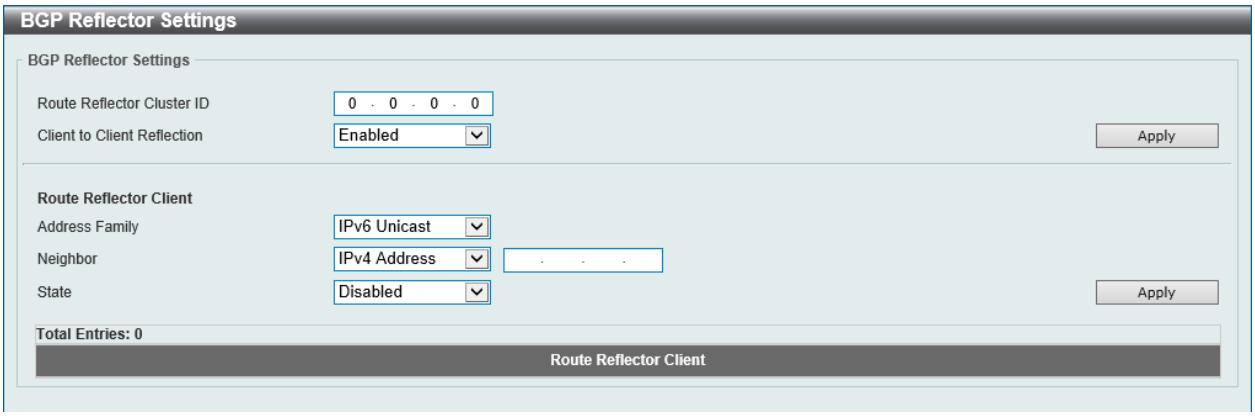


図 9-176　BGP Reflector Settings 画面

画面に表示される項目：

項目	説明
BGP Reflector Settings	
Route Reflector Cluster ID	ルートリフレクタのクラスタ ID 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 / 無効に設定します。
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を使用します。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリを使用します。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリを使用します。 • 「VPNv4」- VPNv4 アドレスファミリを使用します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
Neighbor	クライアントとなるネイバを指定します。 • 「IPv4 Address」- 隣接ルータの 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」- 隣接ルータの IPv6 アドレスを指定します。
State	BGP リフレクタクライアント機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、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。

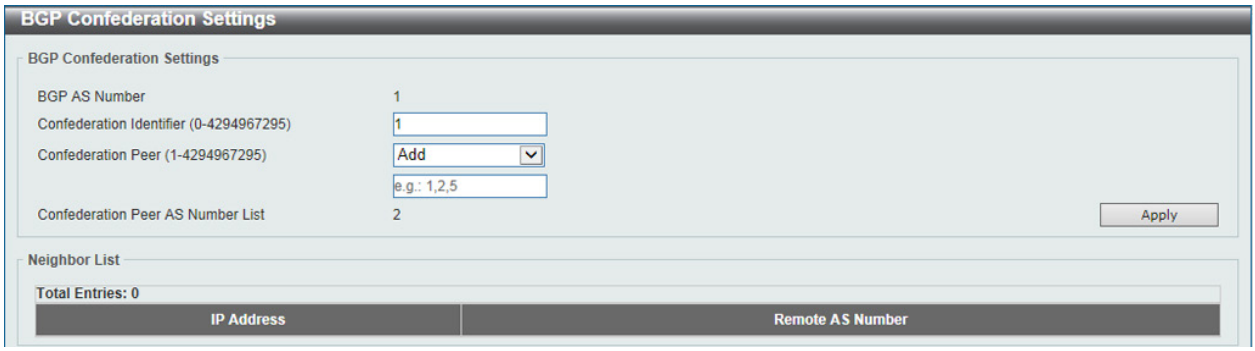


図 9-177　BGP Confederation Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Confederation Identifier	BGP コンフェデレーション ID を入力します。 • 設定可能範囲：0-4294967295
Confederation Peer	BGP コンフェデレーションピアを「Add」（追加）または「Delete」（削除）します。 BGP コンフェデレーションピア ID を入力します。 • 設定可能範囲：1-4294967295

「Apply」ボタンをクリックして、設定内容を適用します。

BGP AS Path Access List Settings（BGP AS パスアクセスリストリスト設定）

BGP 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。

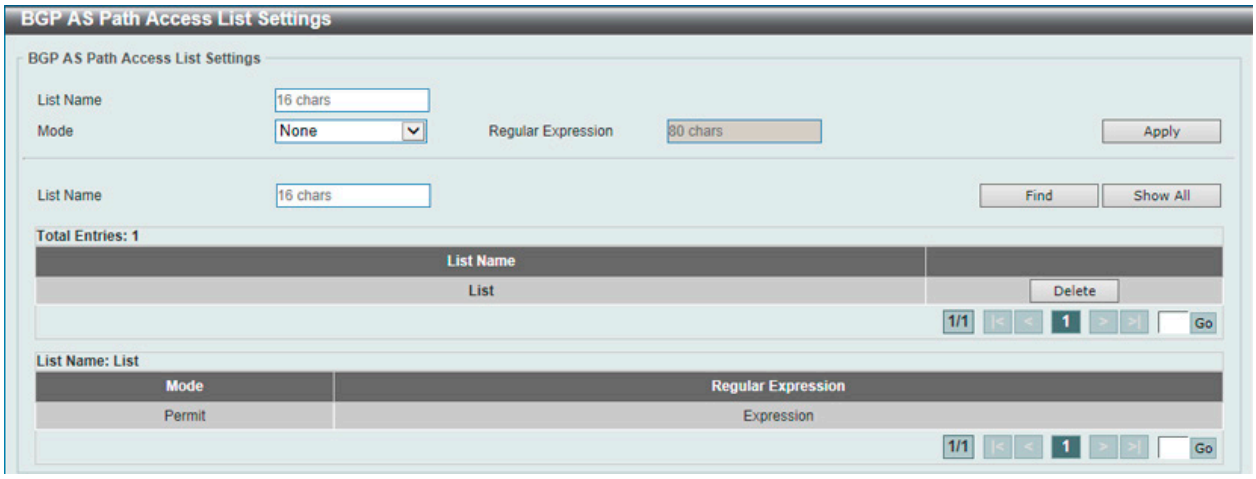


図 9-178　BGP AS Path Access List Settings 画面

画面に表示される項目：

項目	説明
List Name	AS パスアクセスリスト名を入力します。（16 文字以内）
Mode	動作モードを指定します。 •「Permit」- ルート一致条件が許可されます。 •「Deny」- ルート一致条件が拒否されます。 •「None」- アクションを実行しません。
Regular Expression	パスフィルタの正規表現（80 文字以内）を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

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。

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。

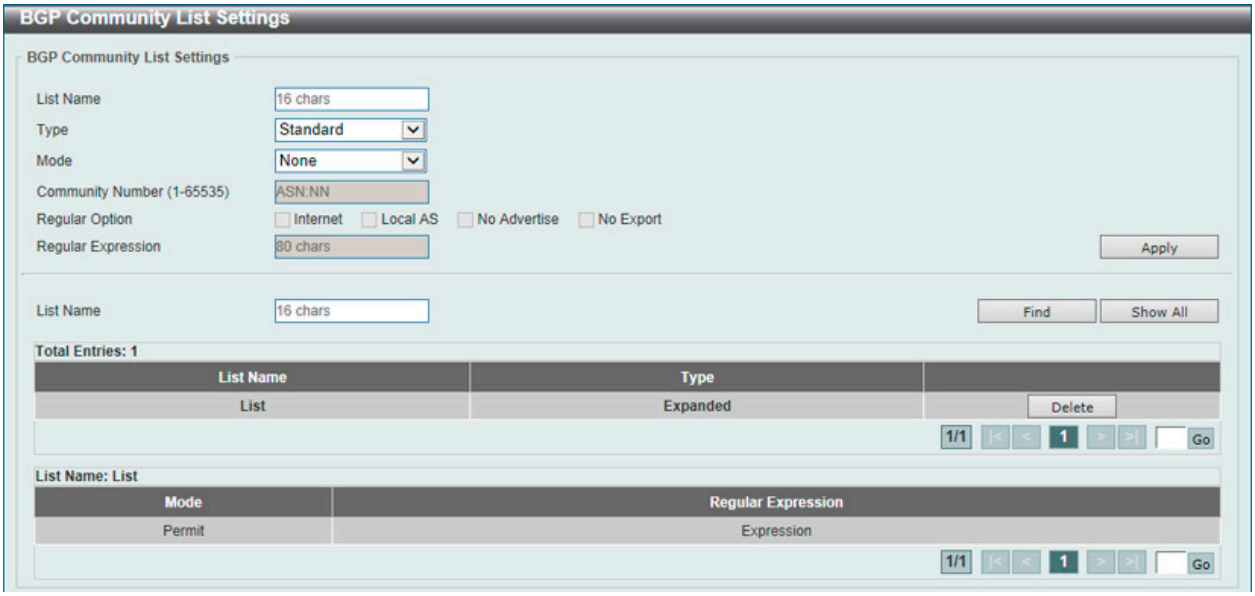


図 9-179　BGP Community List Settings 画面

画面に表示される項目：

項目	説明
List Name	コミュニティリスト名（16 文字以内）を入力します。
Type	タイプオプションを指定します。 • 「Standard」- 名前付き標準コミュニティリストを設定します。 • 「Expanded」- 名前付きの拡張コミュニティリストを設定します。
Mode	動作モードを指定します。 • 「Permit」- ルート一致条件が許可されます。 • 「Deny」- ルート一致条件が拒否されます。 • 「None」- アクションを実行しません。
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コミュニティ番号を指定します。スペースによって区切られた複数のコミュニティ番号を指定することも可能です。
Regular Option	標準オプションを選択します。 • 「Internet」- インターネットコミュニティを指定します。このコミュニティを持つルートはすべてのピアにアドバタイズされます。 • 「Local AS」- ローカル AS コミュニティを指定します。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のローカル AS またはサブ AS から送信されません。 • 「No Advertise」- No Advertise コミュニティを指定します。このコミュニティを持つルートは他の BGP ピアにアドバタイズされません。 • 「No Export」- No Export コミュニティを指定します。このコミュニティを持つルートは外部ピアにアドバタイズされません。
Regular Expression	正規表現を入力します。入力文字列と照合するパターンを指定するために使用されます。正規表現は、拡張されたコミュニティリストでのみ使用できます。（80 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

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。

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。

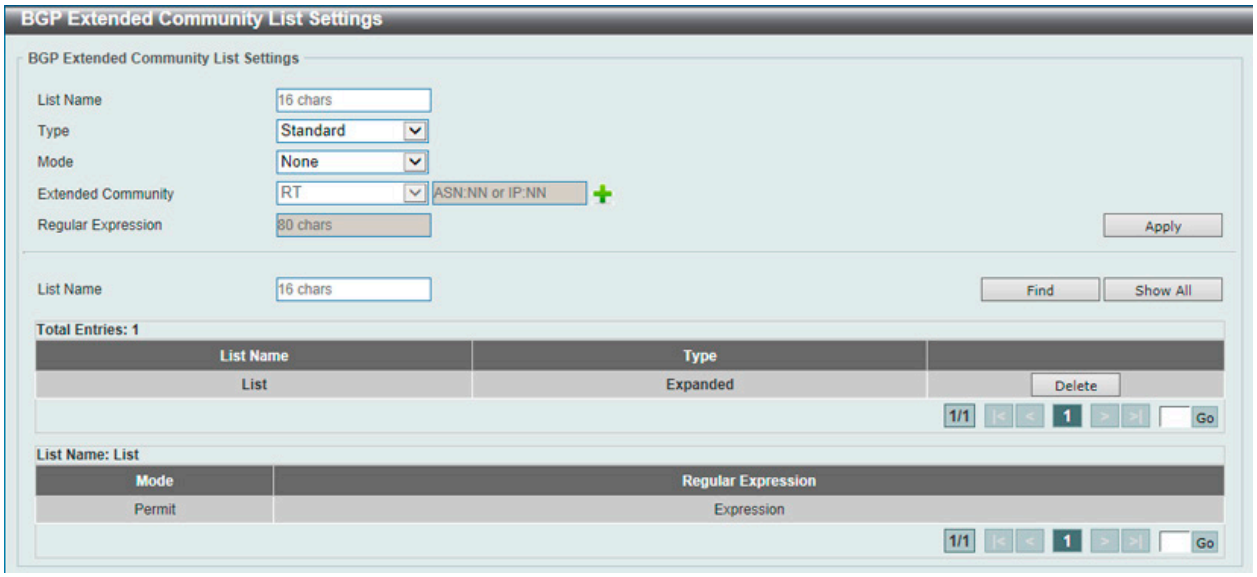


図 9-180　BGP Extended Community List Settings 画面

画面に表示される項目：

項目	説明
List Name	拡張コミュニティリスト名（16 文字以内）を入力します。スペースを含めることはできません。
Type	タイプオプションを指定します。 • 「Standard」- 名前付き標準拡張コミュニティリストを設定します。 • 「Expanded」- 名前付きの拡張コミュニティリストを設定します。
Mode	動作モードを指定します。 • 「Permit」- 拡張コミュニティリストを許可します。 • 「Deny」- 拡張コミュニティリストを拒否します。 • 「None」- アクションを実行しません。
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	正規表現を入力します。（80 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

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。

BGP Clear Settings（BGP クリア設定）

BGP クリア設定を行います。

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。

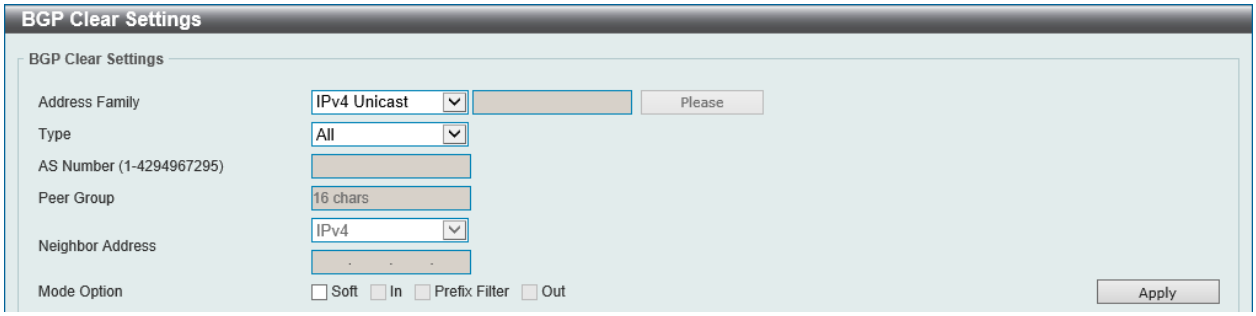


図 9-181　BGP Clear Settings 画面

画面に表示される項目：

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を使用します。 • 「IPv4 VRF」- VRF インスタンス（12 文字以内）を入力します。「Please」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリを使用します。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリを使用します。 • 「VPNv4」- VPNv4 アドレスファミリを使用します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリを使用します。
Type	BGP タイプを指定します。 • 「All」- 指定アドレスファミリ内のすべての BGP ピアセッションをクリアします。 • 「AS Number」- 指定した AS 内のすべての BGP ピアセッションをクリアします。 • 「Peer Group」- ピアグループ内のすべての BGP ピアセッションをクリアします。 • 「Neighbor Address」- ネイバアドレスに関連付けられているすべて BGP ピアセッションをクリアします。 • 「External」- ハード / ソフト再構成を使用してすべての BGP ピアセッションをクリアします。
AS Number	BGP ピアセッションがクリアされる AS 番号を入力します。 • 設定可能範囲：1-4294967295
Peer Group	BGP ピアセッションがクリアされるピアグループの名前を入力します。（16 文字以内）
Neighbor Address	BGP ピアセッションがクリアされるネイバの IPv4 アドレスまたは IPv6 アドレスを入力します。
Mode Option	モードオプションを指定します。 • 「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」- インバウンド再構成を開始します。In/Out のどちらも指定されていない場合、インバウンドセッションとアウトバウンドセッションの両方がクリアされます。 • 「Prefix Filter」- 既存の Outbound Route Filter (ORF) プレフィックスリストをクリアすることにより、新しいルートを更新を開始して、ピアルータからの ORF プレフィックスリストを更新します。 • 「Out」- アウトバウンド再構成を開始します。In/Out のどちらも指定されていない場合、インバウンドセッションとアウトバウンドセッションの両方がクリアされます。

「Apply」ボタンをクリックして、設定内容を適用します。

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。

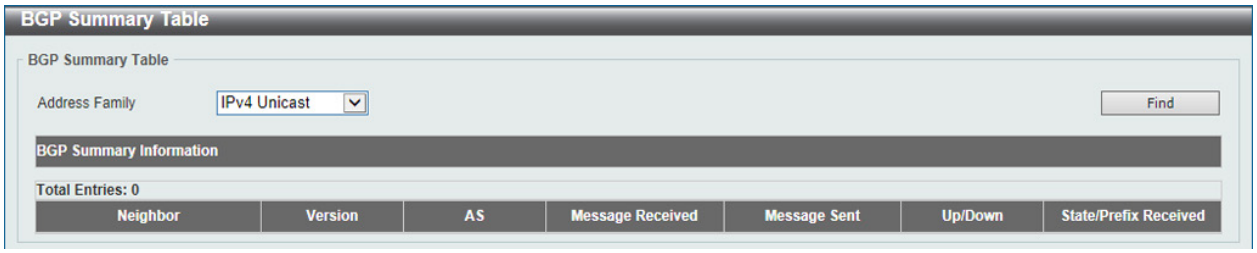


図 9-182　BGP Summary Table 画面

画面に表示される項目：

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に関連する BGP サマリ情報を表示します。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリに関連する BGP サマリ情報を表示します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリに関連する BGP サマリ情報を表示します。 • 「VPNv4 All」- VPNv4 アドレスファミリに関連するすべての BGP サマリ情報を表示します。 • 「VPNv4 RD」- VPNv4 アドレスファミリの Route Distinguisher (RD) に関連する BGP サマリ情報を表示します。表示されるフィールドに RD を入力します。 • 「VPNv4 VRF」- VPNv4 アドレスファミリの VRF インスタンスに関連する BGP サマリ情報を表示します。VRF インスタンスの名前（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリに関連する BGP サマリ情報を表示します。

「Find」ボタンをクリックして、指定 / 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。

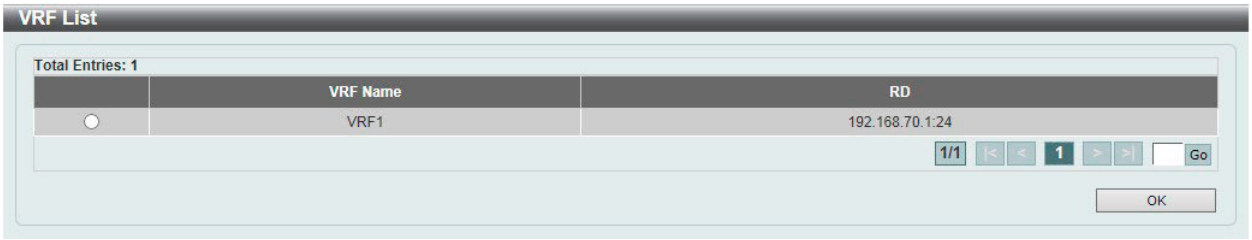


図 9-183　BGP Summary Table（VPNv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

BGP Routing Table（BGP ルーティングテーブル）

BGP ルーティングテーブルを表示します。

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 9-184　BGP Routing Table 画面

画面に表示される項目：

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に関連する BGP ルーティング情報を表示します。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリに関連する BGP ルーティング情報を表示します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリに関連する BGP ルーティング情報を表示します。 • 「VPNv4 All」- VPNv4 アドレスファミリに関連するすべての BGP ルーティング情報を表示します。 • 「VPNv4 RD」- VPNv4 アドレスファミリの Route Distinguisher (RD) に関連する BGP ルーティング情報を表示します。表示されるフィールドに RD を入力します。 • 「VPNv4 VRF」- VPNv4 アドレスファミリの VRF インスタンスに関連する BGP ルーティング情報を表示します。VRF インスタンスの名前（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「L2VPN VPLS All」- L2VPN VPLS アドレスファミリに関連するすべての BGP ルーティング情報を表示します。 • 「L2VPN VPLS RD」- L2VPNv4 アドレスファミリの Route Distinguisher (RD) に関連する BGP ルーティング情報を表示します。 • 「L2VPN VPLS VFI」- L2VPN VPLS アドレスファミリの VFI インスタンスに関連する BGP ルーティング情報を表示します。表示されるフィールドに VFI インスタンスの名前（12 文字以内）を入力します。
Type	タイプオプションを指定します。 • 「IP Address」- 指定した IPv4/IPv6 アドレスに関連する BGP ルーティング情報を表示します。 　- 「IP Address」- IPv4 アドレスを入力します。 　- 「IPv6 Address」- IPv6 アドレスを入力します。 • 「Network」- 指定されたネットワークに関連する BGP ルーティング情報を表示します。 　- 「Network」- ネットワーク範囲の開始 / 終了 IPv4 アドレスを入力します。「Longer Prefixes」オプションにチェックを入れると、指定されたルートと、すべてのより具体的なルートを表示します。 　- 「IPv6 Network」- IPv6 ネットワークアドレスとプレフィックス長を入力します。「Longer Prefixes」をオプションにチェックを入れると、指定プレフィックス長以上のプレフィックスを持つ IPv6 ルートを表示します。 • 「Route Map」- 指定されたルートマップに関連する BGP ルーティング情報を表示します。 　- 「Route Map Name」- ルートマップの名前を入力します。（16 文字以内） 　- 「L2VPN Prefix」- L2VPN プレフィックスを入力します。 • 「CIDR Only」- CIDR（Classless Inter-Domain Routing）ルートに関連する BGP ルーティング情報を表示します。 • 「Community」- 指定された BGP コミュニティに関連する BGP ルーティング情報を表示します。 　- 「Community Set」- BGP コミュニティの AS とコミュニティ番号を入力します。 　- 「Local AS」- コンフェデレーションのローカル AS またはサブ自律システムから送信しないように設定します。 　- 「No Advertise」- 他の BGP ピアにルートをアドバタイズしないように設定します。 　- 「No Export」- 外部ピアにアドバタイズしないように設定します。 　- 「Internet」- ルートはすべてのピアにアドバタイズされます。 　- 「Exact Match」- コミュニティは正確に一致する必要があります。 　- 「L2VPN Prefix」- L2VPN プレフィックスを入力します。 • 「Community List」- 指定された BGP コミュニティリストに関連する BGP ルーティング情報を表示します。 　- 「Community List」- BGP コミュニティリストの名前を入力します。（16 文字以内） 　- 「Exact Match」- 正確に一致するルートのみ表示します。 　- 「L2VPN Prefix」- L2VPN プレフィックスを入力します。 • 「Filter List」- 指定したフィルタリストに関連する BGP ルーティング情報を表示します。 　- 「Filter List Name」- フィルタリストの名前を入力します。（16 文字以内） 　- 「L2VPN Prefix」- L2VPN プレフィックスを入力します。 • 「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 BGP ルートを表示します。 　- 「L2VPN Prefix」- L2VPN プレフィックスを入力します。 • 「Quote Regexp」- 正規表現に一致する BGP ルートを表示します。 　- 「Regexp」- 正規表現を入力します。（80 文字以内） 　- 「L2VPN Prefix」- L2VPN プレフィックスを入力します。

「Find」ボタンをクリックして、指定 / 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。

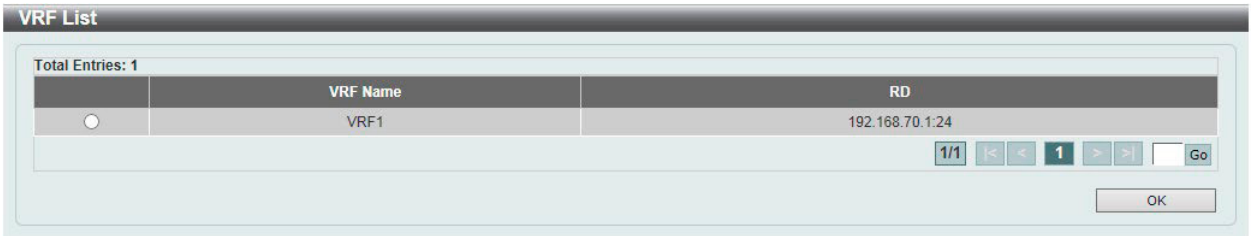


図 9-185　BGP Routing Table（VPNv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

BGP Labels Table（BGP ラベルテーブル）

BGP ラベルを表示します。

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。

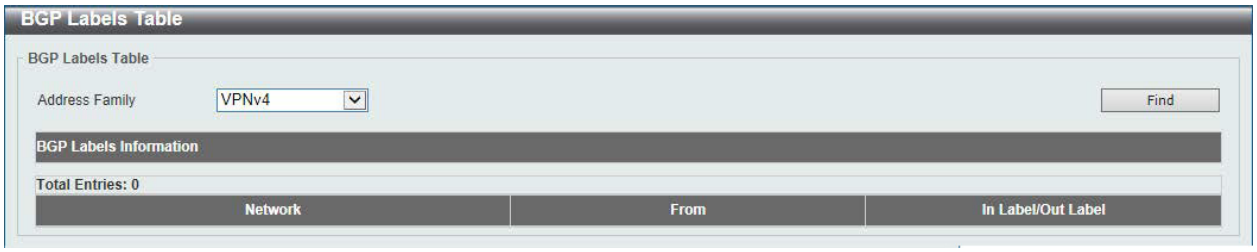


図 9-186　BGP Labels Table 画面

画面に表示される項目：

項目	説明
Address Family	アドレスファミリを選択します。 • 「VPNv4 All」- VPNv4 アドレスファミリに関連するすべての BGP ラベル情報を表示します。 • 「VPNv4 RD」- VPNv4 アドレスファミリの Route Distinguisher (RD) に関連する BGP ラベル情報を表示します。表示されるフィールドに RD を入力します。 • 「VPNv4 VRF」- VPNv4 アドレスファミリの VRF インスタンスに関連する BGP ラベル情報を表示します。VRF インスタンスの名前（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。

「Find」ボタンをクリックして、指定 / 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。

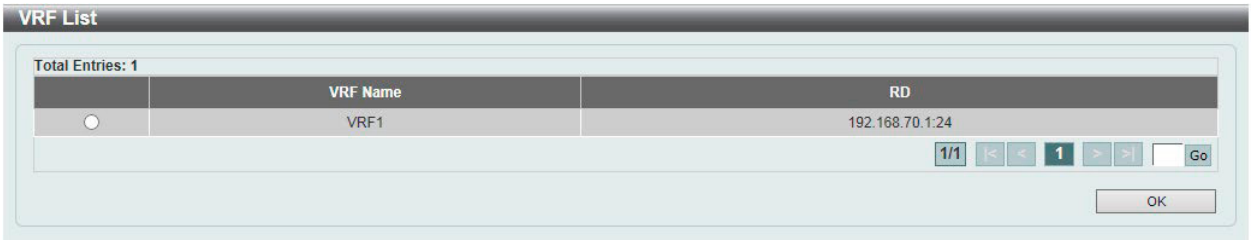


図 9-187　BGP Labels Table（Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

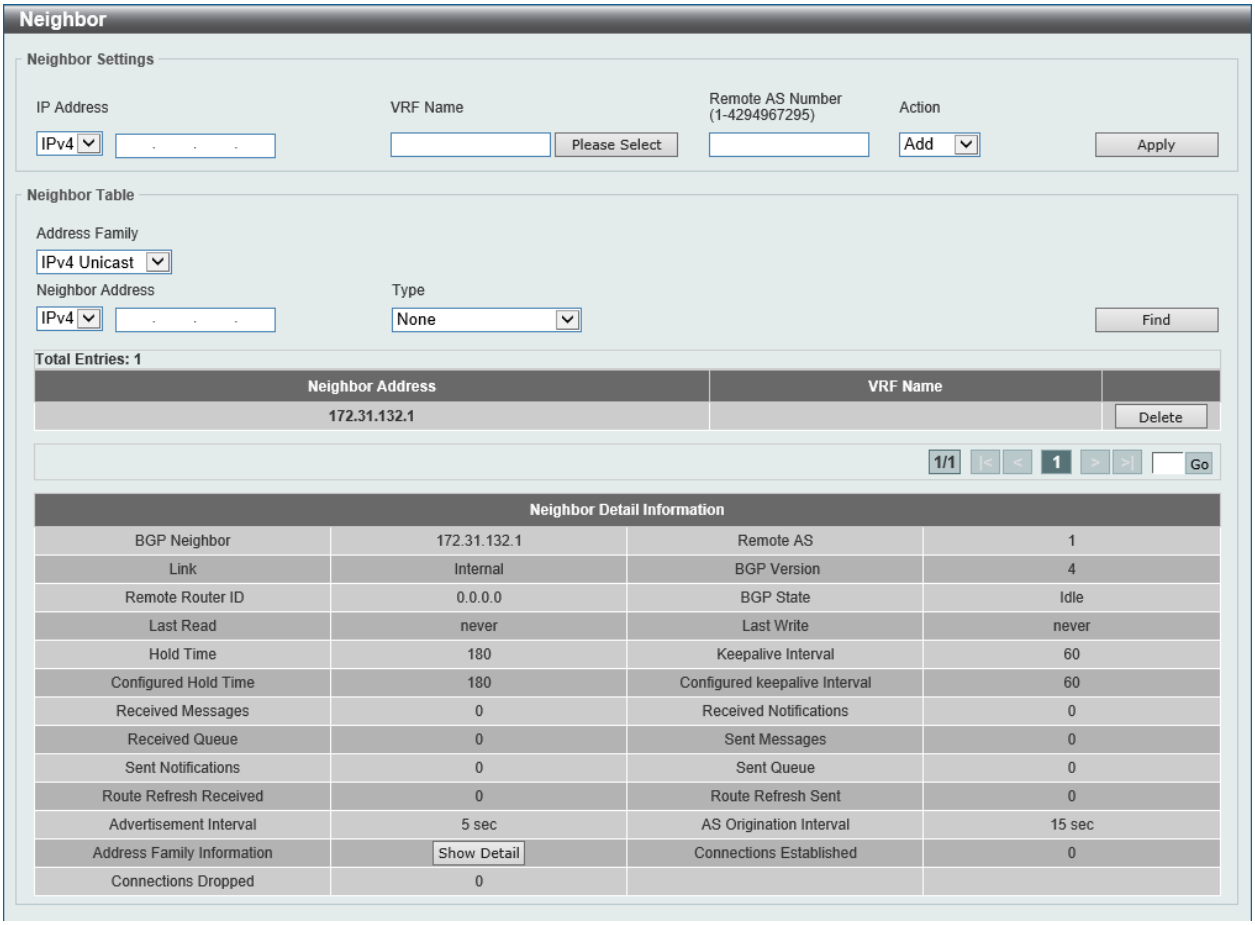


図 9-188　Neighbor 画面

画面に表示される項目：

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 インスタンス名を入力します（12 文字以内）。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Remote AS Number	リモート AS 番号を入力します。 • 設定可能範囲：1-4294967295
Action	実行するアクションを指定します。 • 選択肢：「Add」（追加）「Delete」（削除）
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に関連する BGP ネイバ情報を表示します。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリに関連する BGP ネイバ情報を表示します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリに関連する BGP ネイバ情報を表示します。 • 「VPNv4 All」- すべての VPNv4 アドレスファミリに関連する BGP ネイバ情報を表示します。 • 「VPNv4 RD」- VPNv4 アドレスファミリの Route Distinguisher (RD) に関連する BGP ネイバ情報を表示します。表示されるフィールドに RD を入力します。 • 「VPNv4 VRF」- VPNv4 アドレスファミリの VRF インスタンスに関連する BGP ネイバ情報を表示します。VRF インスタンスの名前（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリに関連する BGP ネイバ情報を表示します。
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	表示する情報の種類を選択します。 • 「None」- ネイバセッションの BGP および TCP 接続情報を表示します。 • 「Advertised Routes」- BGP ネイバに通知されたルートを表示します。 • 「Received Routes」- BGP ネイバから受信したルートを表示します。 • 「Routes」- BGP ネイバから受信し、受け入れられたルートを表示します。受け入れられたルートは、受信したルートのサブセットです。 • 「Received Prefix Filter」- 指定したネイバによって送信されたプレフィックスリストを表示します。

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

「Please Select」をクリックすると、次の画面が表示されます。

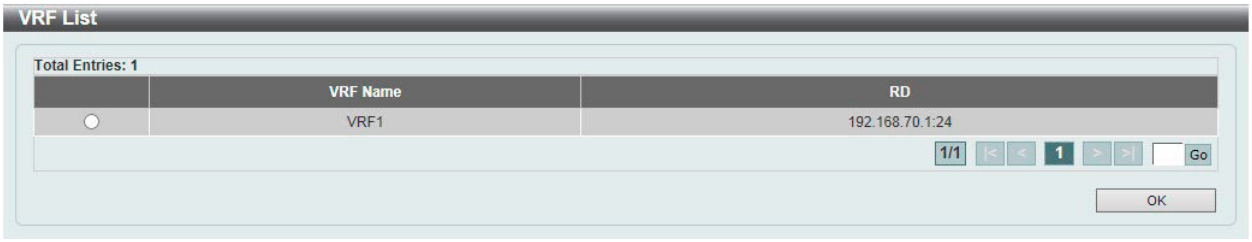


図 9-189　Neighbor（VPNv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

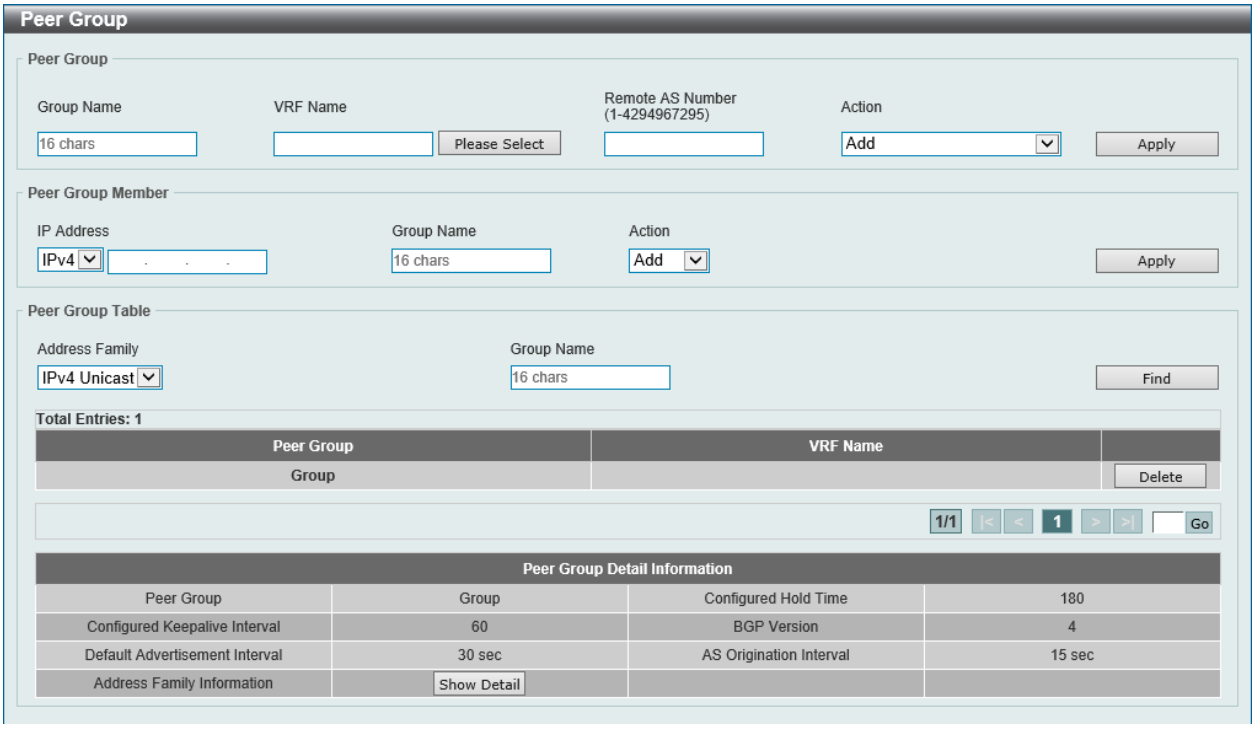


図 9-190　Peer Group 画面

画面に表示される項目：

項目	説明
Peer Group	
Group Name	BGP ピアグループ名（16 文字以内）を入力します。
VRF Name	VRF インスタンス名を入力します（12 文字以内）。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Remote AS Number	リモート AS 番号を入力します。 • 設定可能範囲：1-4294967295
Action	実行するアクションを指定します。 • 選択肢：「Add」「Delete Group」「Delete Group AS Number」
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 文字以内）を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add」（追加）「Delete」（削除）
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に関連する BGP ピアグループ情報を表示します。 • 「VPNv4 All」- すべての VPNv4 アドレスファミリに関連する BGP ピアグループ情報を表示します。 • 「VPNv4 RD」- VPNv4 アドレスファミリの Route Distinguisher (RD) に関連する BGP ピアグループ情報を表示します。表示されるフィールドに RD を入力します。 • 「VPNv4 VRF」- VPNv4 アドレスファミリの VRF インスタンスに関連する BGP ピアグループ情報を表示します。VRF インスタンスの名前（12 文字以内）を入力します。「Please Select」で既存の VRF インスタンスを選択することも可能です。
Group Name	BGP ピアグループ名（16 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
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」ボタンをクリックして、指定エントリの詳細について表示します。

「Please Select」をクリックすると、次の画面が表示されます。



図 9-191　Peer Group（VPNv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Show Detail」をクリックすると、次の画面が表示されます。

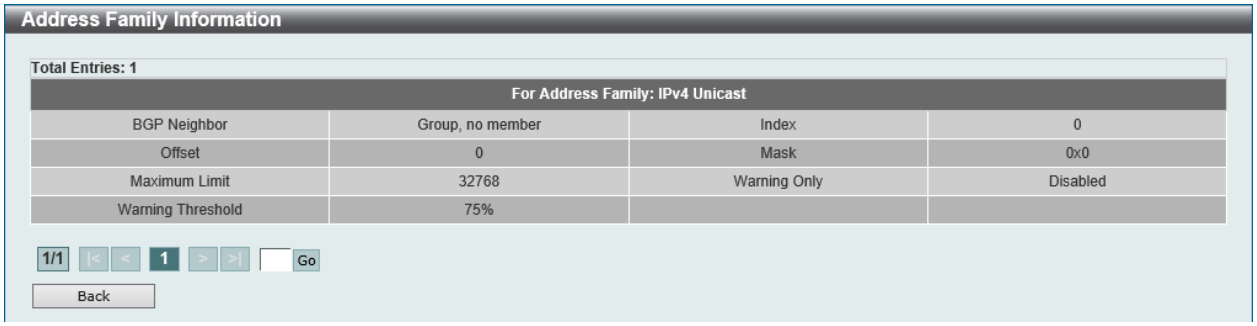


図 9-192　Peer Group（Show Detail）- Address Family Information 画面

前の画面に戻るには、「Back」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Neighbor Activate（ネイバ有効化）

Border Gateway Protocol (BGP) ネイバをアクティブ化、非アクティブ化します。

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 9-193　Neighbor Activate 画面

画面に表示される項目：

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に関連する BGP ネイバをアクティブ化 / 非アクティブ化します。 • 「IPv4 VRF」- IPv4 アドレスファミリの VRF インスタンスに関連する BGP ネイバをアクティブ化 / 非アクティブ化します。VRF インスタンスの名前（12 文字以内）を入力します。「Please」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリに関連する BGP ネイバをアクティブ化 / 非アクティブ化します。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリに関連する BGP ネイバをアクティブ化 / 非アクティブ化します。 • 「VPNv4」- VPNv4 アドレスファミリに関連する BGP ネイバをアクティブ化 / 非アクティブ化します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリに関連する BGP ネイバをアクティブ化 / 非アクティブ化します。
Neighbor	ネイバを選択します。 • 「IPv4 Address」- BGP ネイバの IPv4 アドレスを入力します。 • 「Peer Group」- BGP ネイバのピアグループ名を入力します。（16 文字以内） • 「IPv6 Address」- BGP ネイバの IPv6 アドレスを入力します。
Action	実行する動作を指定します。 • 選択肢：「Activate」（有効化）/「No Activate」（無効化）

「Apply」ボタンをクリックして、設定内容を適用します。

「Please」をクリックすると、次の画面が表示されます。



図 9-194　Neighbor Activate（IPv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

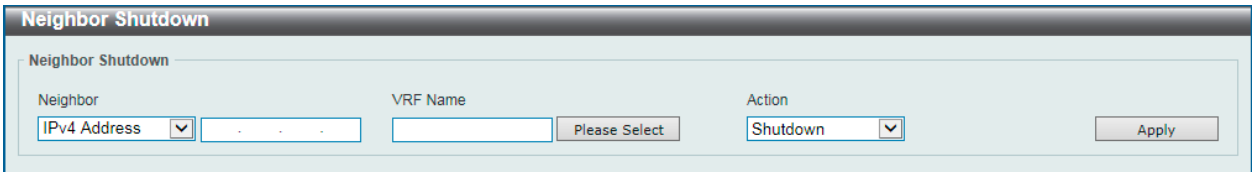


図 9-195　Neighbor Shutdown 画面

画面に表示される項目：

項目	説明
Neighbor	ネイバを選択します。 • 「IPv4 Address」- BGP ネイバの IPv4 アドレスを入力します。 • 「IPv6 Address」- BGP ネイバの IPv6 アドレスを入力します。 • 「Peer Group」- BGP ネイバのピアグループ名を入力します。（16 文字以内）
VRF Name	VRF インスタンス名を入力します（12 文字以内）。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。
Action	実行する動作を指定します。 • 選択肢：「Shutdown」「No Shutdown」

「Apply」ボタンをクリックして、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。

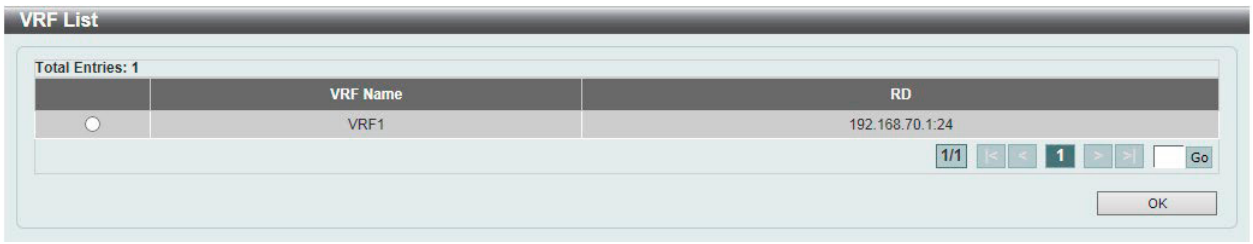


図 9-196　Neighbor Shutdown（Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Neighbor Map Settings（ネイバマップ設定）

Border Gateway Protocol (BGP) ネイバのマップを設定、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。

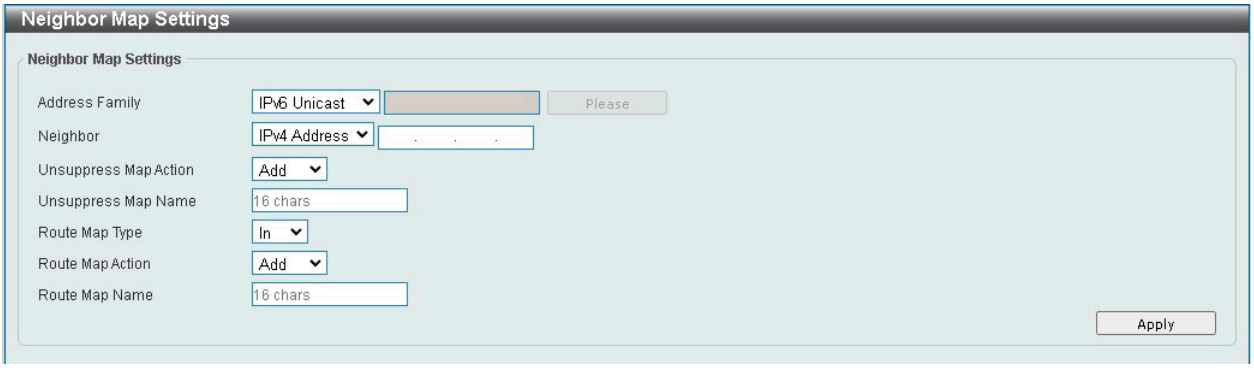


図 9-197　Neighbor Map Settings 画面

画面に表示される項目：

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に関連する BGP ネイバマップを設定します。 • 「IPv4 VRF」- IPv4 アドレスファミリの VRF インスタンスに関連する BGP ネイバマップを設定します。VRF インスタンスの名前（12 文字以内）を入力します。「Please」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリに関連する BGP ネイバマップを設定します。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリに関連する BGP ネイバマップを設定します。 • 「VPNv4」- VPNv4 アドレスファミリに関連する BGP ネイバマップを設定します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリに関連する BGP ネイバマップを設定します。
Neighbor	ネイバを選択します。 • 「IPv4 Address」- BGP ネイバの IPv4 アドレスを入力します。 • 「Peer Group」- BGP ネイバのピアグループ名を入力します。（16 文字以内） • 「IPv6 Address」- BGP ネイバの IPv6 アドレスを入力します。
Unsuppress Map Action	実行する非抑制アクションを選択します。集約アドレス機能によって抑制されたルートを選択的にアドバタイズするために使用されます。 • 選択肢：「Add」（追加）/「Delete」（削除）
Unsuppress Map Name	非抑制ルートマップの名前を入力します。（16 文字以内）
Route Map Type	ルートマップの種類を指定します。 • 「In」- ネイバからアドバタイズされたパスに適用されたルートマップを指定します。 • 「Out」- ネイバにアドバタイズされたパスに適用されたルートマップを指定します。
Route Map Action	ルートマップのアクションを指定します。 • 選択肢：「Add」（追加）/「Delete」（削除）
Route Map Name	ルートマップの名前をに入力します。（16 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

「Please」をクリックすると、次の画面が表示されます。

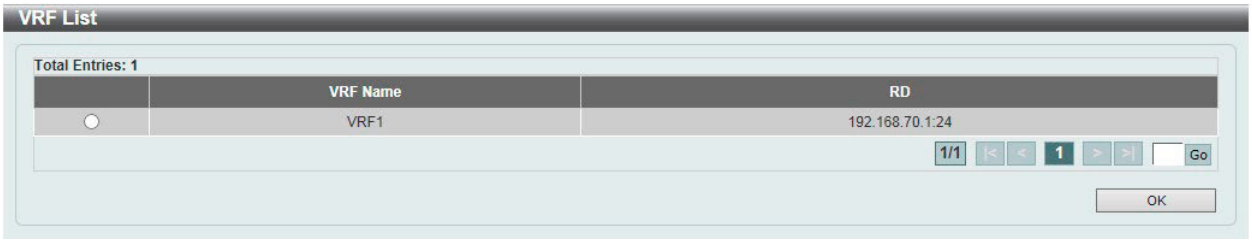


図 9-198　Neighbor Map Settings（IPv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

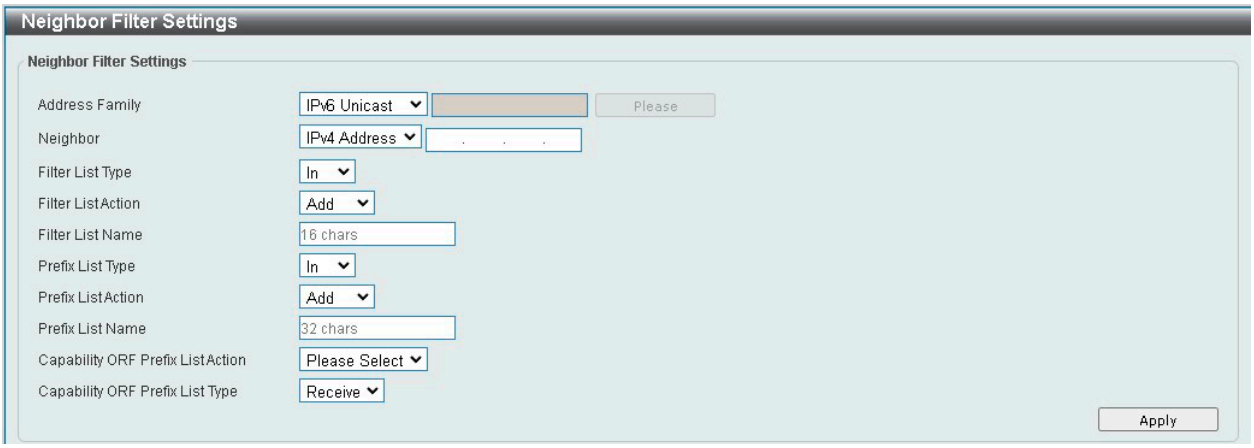


図 9-199　Neighbor Filter Settings 画面

画面に表示される項目：

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に関連する BGP ネイバフィルタを設定します。 • 「IPv4 VRF」- IPv4 アドレスファミリの VRF インスタンスに関連する BGP ネイバフィルタを設定します。VRF インスタンスの名前（12 文字以内）を入力します。「Please」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリに関連する BGP ネイバフィルタを設定します。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリに関連する BGP ネイバフィルタを設定します。 • 「VPNv4」- VPNv4 アドレスファミリに関連する BGP ネイバフィルタを設定します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリに関連する BGP ネイバフィルタを設定します。
Neighbor	ネイバを選択します。 • 「IPv4 Address」- BGP ネイバの IPv4 アドレスを入力します。 • 「Peer Group」- BGP ネイバのピアグループ名を入力します。（16 文字以内） • 「IPv6 Address」- BGP ネイバの IPv6 アドレスを入力します。
Filter List Type	フィルタリストの種類を選択します。 • 「In」- アクセスリストを内向きルートに適用します。 • 「Out」- アクセスリストを外向きルートに適用します。
Filter List Action	フィルタリストのアクションを指定します。 • 選択肢：「Add」（追加）/「Delete」（削除）
Filter List Name	AS パスアクセスリストの名前を入力します。（16 文字以内）
Prefix List Type	プレフィックスリストの種類を選択します。 • 「In」- ネイバからアドバタイズされるパスに適用するフィルタリストを指定します。 • 「Out」- ネイバにアドバタイズされるパスに適用するフィルタリストを指定します。
Prefix List Action	プレフィックスリストのアクションを指定します。 • 選択肢：「Add」（追加）/「Delete」（削除）
Prefix List Name	プレフィックスリストの名前を入力します。（32 文字以内）
Capability ORF Prefix List Action	ORF プレフィックスリスト機能を有効 / 無効に設定します。本機能は、ピアと交換されるプレフィックスの数を減らすために使用されます。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 / 双方向で動作可能です。
Capability ORF Prefix List Type	Capability ORF プレフィックスリストの種類を選択します。 • 選択肢：「Receive（受信）」「Send（送信）」「Both（送受信）」

「Apply」ボタンをクリックして、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。

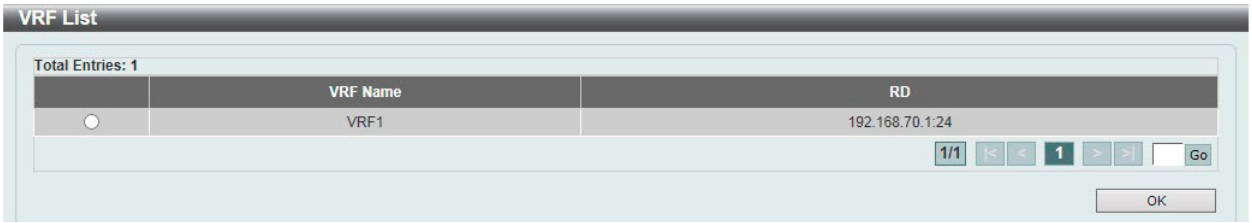


図 9-200　Neighbor Filter Settings（IPv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Neighbor Maximum Prefix Settings（ネイバ最大プレフィックス設定）

Border Gateway Protocol (BGP) ネイバの最大プレフィックスを設定、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ッ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。

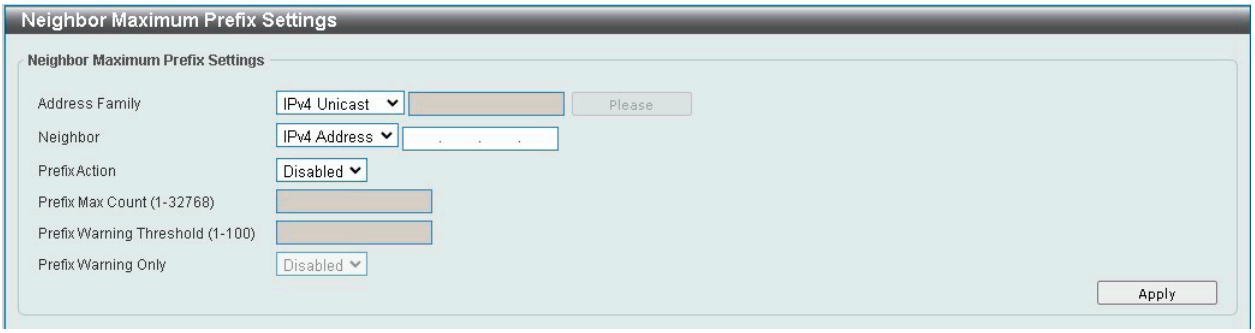


図 9-201　Neighbor Maximum Prefix Settings 画面

画面に表示される項目：

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に関連する BGP ネイバの最大プレフィックスを設定します。 • 「IPv4 VRF」- IPv4 アドレスファミリの VRF インスタンスに関連する BGP ネイバの最大プレフィックスを設定します。VRF インスタンスの名前（12 文字以内）を入力します。「Please」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリに関連する BGP ネイバの最大プレフィックスを設定します。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリに関連する BGP ネイバの最大プレフィックスを設定します。 • 「VPNv4」- VPNv4 アドレスファミリに関連する BGP ネイバの最大プレフィックスを設定します。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリに関連する BGP ネイバの最大プレフィックスを設定します。
Neighbor	ネイバを選択します。 • 「IPv4 Address」- BGP ネイバの IPv4 アドレスを入力します。 • 「Peer Group」- BGP ネイバのピアグループ名を入力します。（16 文字以内） • 「IPv6 Address」- BGP ネイバの IPv6 アドレスを入力します。
Prefix Action	プレフィックスアクションを有効 / 無効に設定します。
Prefix Max Count	指定されたネイバからの許可されるプレフィックスの最大数を指定します。 • 設定可能範囲：1-32768（IPv4 ユニキャスト、IPv4VRF、IPv4 マルチキャスト、L2VPN VPLS、VPNv4 アドレスファミリ） 1-16384（IPv6 ユニキャストアドレスファミリ）
Prefix Warning Threshold	プレフィックス警告しきい値として、最大プレフィックスのパーセンテージを指定します。このしきい値を超過すると、警告メッセージが生成されます。 • 設定可能範囲：1-100（%）
Prefix Warning Only	Prefix Warning Only 機能を有効 / 無効に設定します。 • 「Enabled」（有効）- しきい値を超えたときにシステムログメッセージの生成のみ行われます。 • 「Disabled」（無効）- しきい値を超えたときにピアリングセッションが終了します。

「Apply」ボタンをクリックして、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。

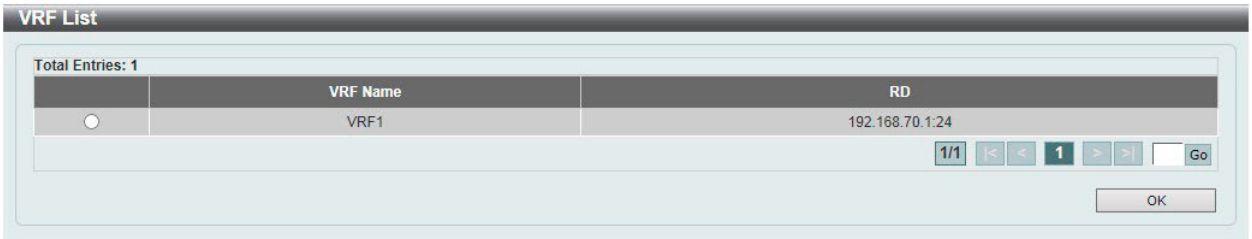


図 9-202　Neighbor Maximum Prefix Settings（IPv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

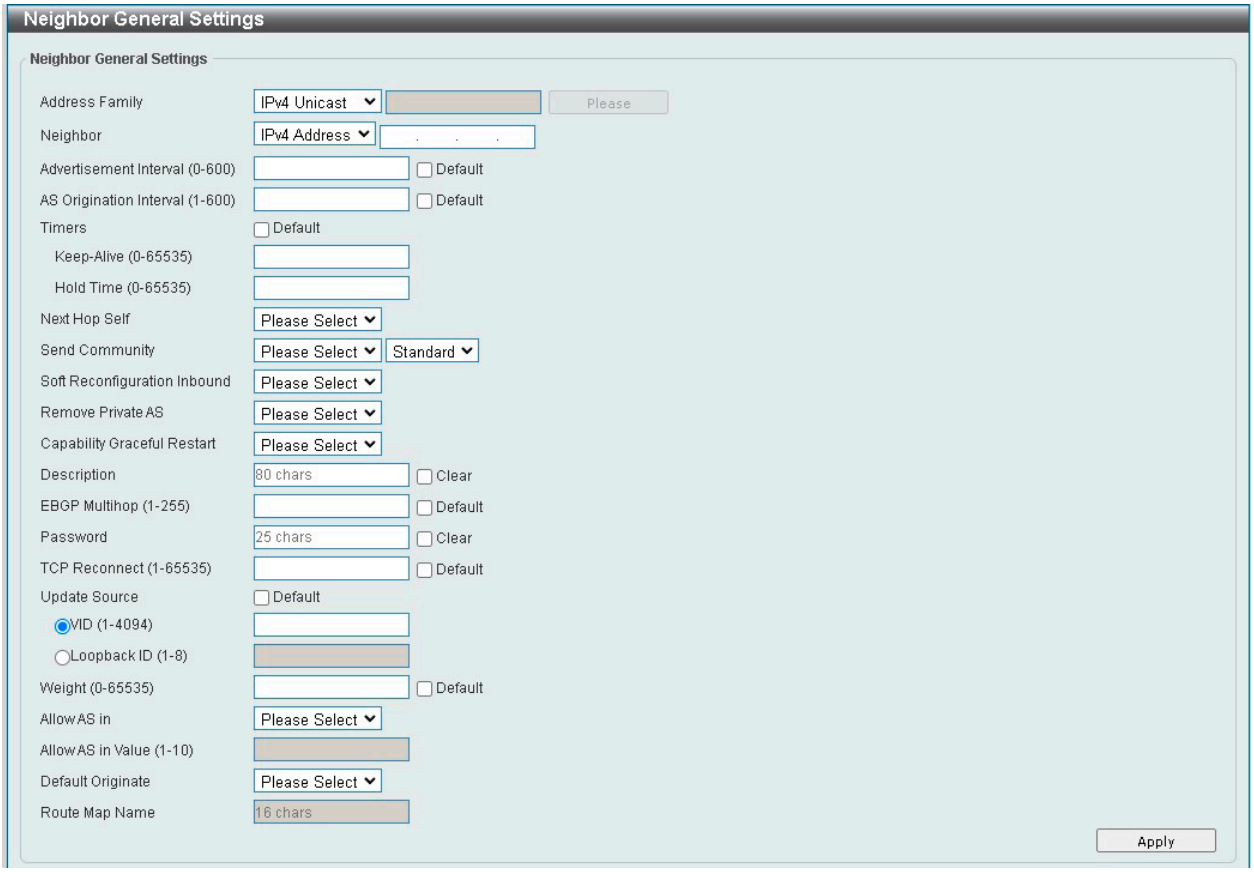


図 9-203　Neighbor General Settings 画面

画面に表示される項目：

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に関連する BGP 一般設定を行います。 • 「IPv4 VRF」- IPv4 アドレスファミリの VRF インスタンスに関連する BGP 一般設定を行います。VRF インスタンスの名前（12 文字以内）を入力します。「Please」で既存の VRF インスタンスを選択することも可能です。 • 「IPv4 Multicast」- IPv4 マルチキャストアドレスファミリに関連する BGP 一般設定を行います。 • 「L2VPN VPLS」- L2VPN VPLS アドレスファミリに関連する BGP 一般設定を行います。 • 「VPNv4」- VPNv4 アドレスファミリに関連する BGP 一般設定を行います。 • 「IPv6 Unicast」- IPv6 ユニキャストアドレスファミリに関連する BGP 一般設定を行います。
Neighbor	ネイバを選択します。 • 「IPv4 Address」- BGP ネイバの IPv4 アドレスを入力します。 • 「Peer Group」- BGP ネイバのピアグループ名を入力します。（16 文字以内） • 「IPv6 Address」- BGP ネイバの IPv6 アドレスを入力します。
Advertisement Interval	アドバタイズ間隔の値を入力します。BGP ルーティング UPDATE メッセージ間の最小間隔を設定するために使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-600
AS Origination Interval	AS Origination 間隔の値を入力します。AS の生成するルーティング更新の送信間隔の最小値を設定するために使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-600
Timers	タイマを指定します。「Default」にチェックを入れると、初期値を使用します。 • 「Keep-Alive」- keep-alive タイム値を入力します。指定したピアに keep-alive メッセージを送信する時間間隔です。 - 設定可能範囲：0-65535 • 「Hold Time」- hold-time 値を入力します。keep-alive メッセージがタイムアウトした場合に、hold-time 時間経過後にピアが Dead と宣言されます。 - 設定可能範囲：0-65535
Next Hop Self	ネクストホップセルフ機能を有効 / 無効に設定します。ルータを BGP スピーキングネイバまたはピアグループのネクストホップとして設定するために使用されます。

項目	説明
Send community	コミュニティ送信機能を有効 / 無効に設定します。指定されたタイプのコミュニティ属性を BGP ネイバに送信するように指定するために使用されます。「Standard」を使用します。標準コミュニティを送信するかどうかを指定します。
Soft Reconfiguration Inbound	ソフト再構成インバウンド機能を有効 / 無効に設定します。ネイバピアからのルート情報更新の保存を有効にするために使用されます。
Remove Private AS	プライベート AS 削除機能を有効 / 無効に設定します。アウトバウンド更新ルートの AS パスリストからプライベート AS 番号を削除するために使用されます。
Capability Graceful Restart	グレースフルリスタート機能を有効 / 無効に設定します。ネイバにグレースフルリスタート機能をアドバタイズできるようにするために使用されます。
Description	BGP ネイバの説明（80 文字以内）を指定します。説明を削除するには、「Clear」オプションを選択します。
EBGP Multihop	eBGP マルチホップ TTL 値を入力します。ルータがローカルピアに直接接続されていない eBGP ピアと BGP セッションを確立できるようにします。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255
Password	2 つの BGP ピア間で使用されるパスワードを入力します。（25 文字以内）。パスワードを削除するには、「Clear」オプションを選択します。
TCP Reconnect	TCP 再接続間隔を入力します。TCP 接続が失敗した後、BGP が TCP 接続要求をピアに送信するために使用する最小間隔を設定するために使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒） • 初期値：120（秒）
Update Source	更新元を指定します。BGP セッションが TCP 接続を開始するための送信元アドレスとして、運用インタフェースの IP アドレスを使用します。「Default」にチェックを入れると、初期値を使用します。 •「VID」- 使用する VLAN ID を入力します。 - 設定可能範囲：1-4094 •「Loopback ID」- 使用するループバックインタフェースの ID を入力します。 - 設定可能範囲：1-8
Weight	BGP ウェイト値を指定します。 指定ネイバからの受信するルートに割り当てるウェイトを指定します。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-65535
Allow AS in	Allow AS In 機能を有効 / 無効に設定します。これにより、受信 BGP パケット内にルータ自身の AS 番号が含まれることを許可します。
Allow AS in Value	Allow AS In 値を指定します。更新パケットの AS パス属性内に含まれるローカル AS の最大数を指定します。 • 設定可能範囲：1-10
Default Originate	Default Originate 機能を有効 / 無効に設定します。これによりネイバへのデフォルトルート生成を有効にします。
Route Map Name	ルートマップ名を指定します。（16 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

「Please Select」をクリックすると、次の画面が表示されます。

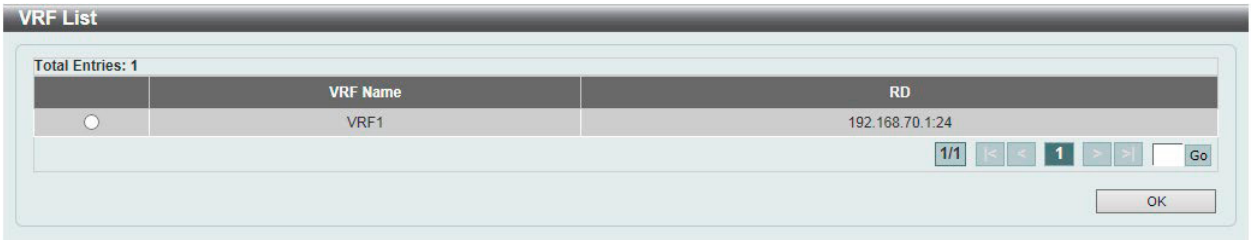


図 9-204　Neighbor General Settings（IPv4 VRF/Please Select）- VRF List 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

BFD（Bidirectional Forwarding Detection）

L3 Features > BFD

注意 BFD は VRF/VRF-Lite と併用できません。

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。

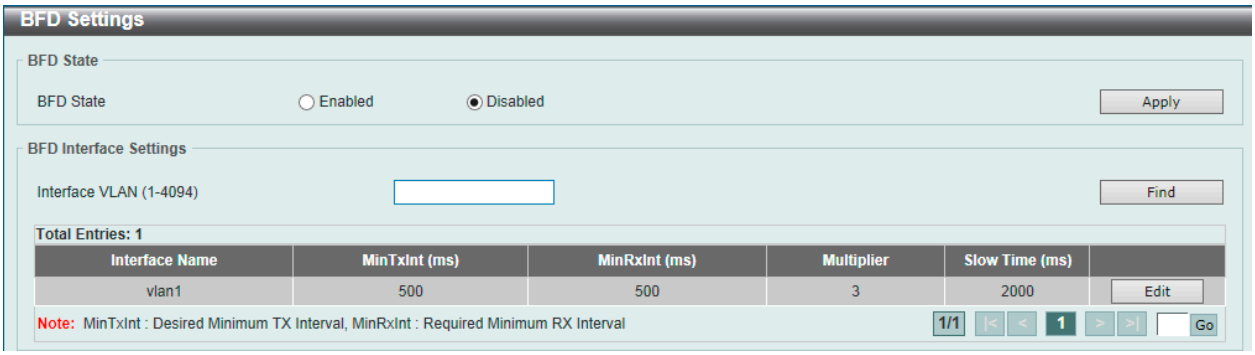


図 9-205　BFD Settings 画面

画面に表示される項目：

項目	説明
BFD State	
BFD State	BFD のグローバルステータスを有効 / 無効に設定します。
BFD Interface Settings	
Interface VLAN	VLAN インタフェースを入力します。

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

対象エントリで「Edit」をクリックすると次の画面が表示されます。

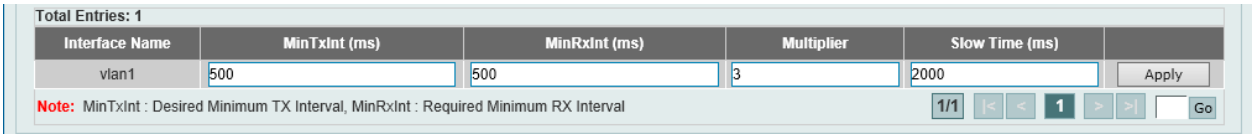


図 9-206　BFD Settings (Edit) 画面

画面に表示される項目：

項目	説明
MinTxInt	BFD 制御パケットを送信する最小間隔値を指定します。 • 設定可能範囲：10-1000（ミリ秒）
MinRxInt	システムがサポートする受信 BFD パケットの最小間隔値を指定します。 • 設定可能範囲：10-1000（ミリ秒）
Multiplier	BFD 検出時間乗算値を指定します。 • 設定可能範囲：3-99
Slow Time	BFD スロータイム値を指定します。 • 設定可能範囲：1000-3000（ミリ秒）

「Apply」ボタンをクリックして、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。

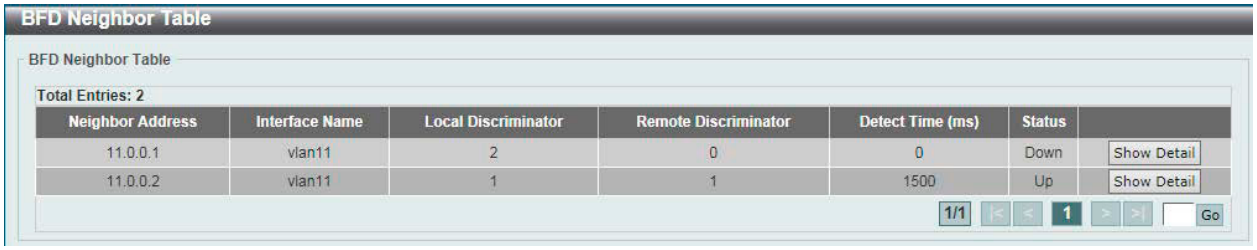


図 9-207　BFD Neighbor Table 画面

「Show Detail」ボタンをクリックして、指定エントリの詳細について表示します。
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。

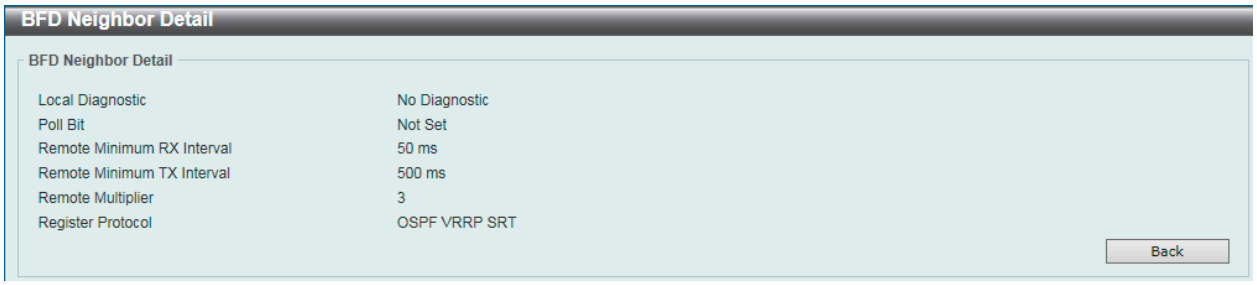


図 9-208　BFD Neighbor Table（Show Detail）- BFD Neighbor Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

ISIS（Intermediate System to Intermediate System）（EI 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。

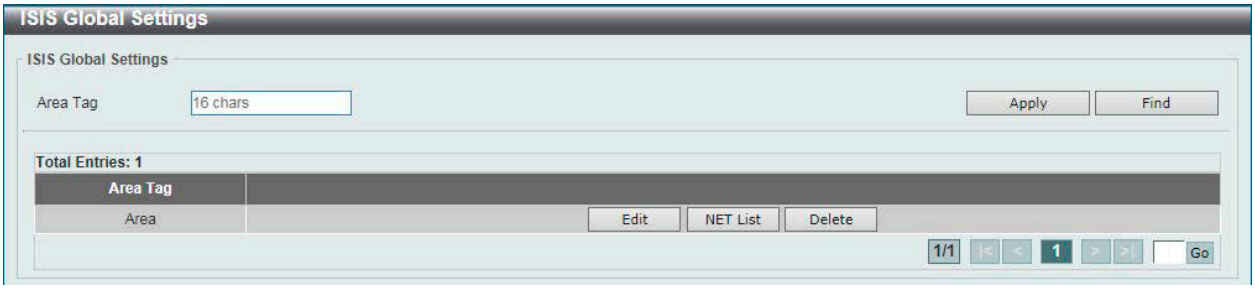


図 9-209　ISIS Global Settings 画面

画面に表示される項目：

項目	説明
Area Tag	ISIS エリアタグ（16 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、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」ボタンをクリックして、「NET Network Services Access Point (NSAP) 」アドレスを表示、設定します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Delete」ボタンをクリックして、指定のエントリを削除します。
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。

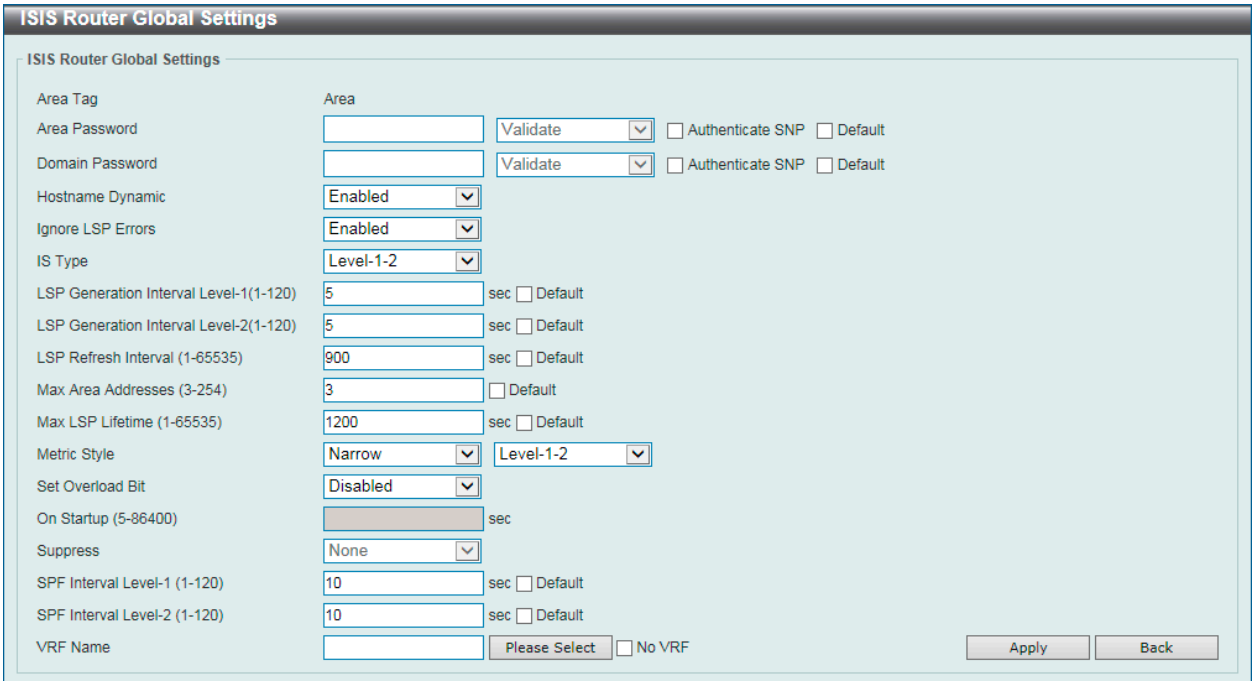


図 9-210　ISIS Global Settings (Edit) 画面

画面に表示される項目：

項目	説明
Area Password	ISIS エリア認証パスワードを入力します。エリアのすべてのスイッチについて、非認証のスイッチによって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が挿入されることを防止します。パスワードはプレーンテキストに変換されます。これは、現在サポートされている唯一の認証タイプです。 • 「Validate」- SNP にパスワードを挿入し、受信時に SNP でパスワードを確認するように設定します。 • 「Send Only」- SNP にパスワードを挿入しますが、受信時に SNP でパスワードを確認しません。 「Authenticate SNP」にチェックを入れると、パスワードを「sequence number PDU」(SNP) に挿入します。「Default」にチェックを入れると、初期値を使用します。
Domain Password	ISIS ルーティングドメイン認証パスワードを入力します。 • 「Validate」- SNP にパスワードを挿入し、受信時に SNP でパスワードを確認するように設定します。 • 「Send Only」- SNP にパスワードを挿入しますが、受信時に SNP でパスワードを確認しません。 「Authenticate SNP」にチェックを入れると、パスワードを「sequence number PDU」(SNP) に挿入します。「Default」にチェックを入れると、初期値を使用します。
Hostname Dynamic	ダイナミックホスト名の構成を有効 / 無効に設定します。ISIS のダイナミックホスト名マッピングを有効にするために使用されます。ダイナミックホスト名メカニズムでは、リンクステートプロトコル（LSP）フラッディングを使用して、ルータ名とシステム ID のマッピング情報をネットワーク全体に分散します。ネットワーク上のすべてのルータは、ルーティングテーブルにシステム ID とルータ名のマッピング情報をインストールしようと試みます。 ネットワーク上でダイナミックネーム Type、Length、Value（TLV）をアドバタイズしていたルータが、突然アドバタイズメントを停止した場合、最後に受信したマッピング情報は最大 1 時間ダイナミックホストマッピングテーブルに残り、ネットワーク管理者はネットワークに問題が発生したときにマッピングエントリテーブルにエントリを確認することができます。
Ignore LSP Errors	LSP エラー無視機能を有効 / 無効に設定します。不正チェックサムの link-state パケット（LSP）の無視を有効にするために使用されます。 ISIS プロトコル定義では、不正なデータリンクチェックサムをもつ受信 LSP がレシーバによって消去され、パケットのイニシエータに再生成させることを要求しています。しかし、ネットワークがデータ破損を引き起こすリンクを持ち、同時に正しいデータリンクチェックサムを持つ LSP を配信している場合、大量のパケットのパージと再生成が連続して発生する可能性があります。この状況ではネットワークが機能しなくなる可能性があるため、本機能を使用して、パケットをパージするのではなくこれらの LSP を無視するように設定します。
IS Type	IS タイプを指定します。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を設定するために使用されます。 • 「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 ルーティングは最も近いレベル 1-2 ルータで実行されます。 • 「Level-1-2」- レベル 1 とレベル 2 の両方の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 生成間隔のレベル 1 の値を入力します。レベル 1 のエリアのリンク状態パケット生成の間隔を設定するために使用されます。本設定により、ネットワークが不安定になっている間の LSP 生成のレートを下げることができます。これにより、ルータの CPU 負荷を軽減し、ISIS ネイバへの LSP 送信回数を減らすことができます。 • 設定可能範囲：1-120（秒） 「Default」にチェックを入れると、初期値を使用します。
LSP Generation Interval Level-2	LSP 生成間隔のレベル 2 の値を入力します。レベル 2 のエリアのリンク状態パケット生成の間隔を設定するために使用されます。本設定により、ネットワークが不安定になっている間の LSP 生成のレートを下げることができます。これにより、ルータの CPU 負荷を軽減し、ISIS ネイバへの LSP 送信回数を減らすことができます。 • 設定可能範囲：1-120（秒） 「Default」にチェックを入れると、初期値を使用します。
LSP Refresh Interval	LSP 更新間隔の値を入力します。link-state パケットの再生成間隔を設定するために使用されます。 LSP は、ライフタイムが終了する前に定期的に更新する必要があります。ここで設定する値は、「Max LSP Lifetime」パラメータの値より小さくする必要があります。そうでない場合、LSP は更新される前にタイムアウトします。LSP の期限を LSP の更新間隔に対して短く設定しすぎると、ソフトウェアによって LSP のリフレッシュ間隔が短くなり、LSP がタイムアウトしなくなります。 更新間隔を短くすると、リンク使用率は上がりますが、検出されないリンク状態データベースの破損が保持されることが多くなります。更新間隔を長くすると、更新されたパケットのフラッディングによって発生するリンク使用率は減らすことができます。 • 設定可能範囲：1-65535（秒） 「Default」にチェックを入れると、初期値を使用します。
Max Area Addresses	最大エリアアドレス値を指定します。追加の手動アドレスを設定することにより、ISIS エリアのサイズを最大化します。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：3-254

項目	説明
Max LSP Lifetime	LSP 有効期間の最大値を入力します。リンクステートパケットの最大有効期限を設定するために使用されます。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒）
Metric Style	メトリックスタイルを指定します。ISIS プロセスの生成とメトリックスタイルの受け入れを設定します。 • 「Narrow」- 古い形式のメトリック TLV を生成します。 • 「Wide」- 新しい形式のメトリック TLV を生成します。 • 「Narrow Transition」- 古い形式のメトリック TLV を生成し、新旧両形式のメトリック TLV を受け入れます。 • 「Wide Transition」- 新しい形式のメトリック TLV を生成し、新旧両形式のメトリック TLV を受け入れます。 • 「Transition」- 新旧両形式のメトリック TLV を生成します。各メトリック形式のレベルを指定します。 - 「Level-1」- レベル 1 ルーティングのみで有効にします。 - 「Level-1-2」- レベル 1/2 ルーティングで有効にします。 - 「Level-2」- レベル 2 ルーティングのみで有効にします。
Set Overload Bit	オーバーロードビット設定機能を有効 / 無効に設定します。ISIS プロセスによって非疑似ノード LSP のオーバーロードビットを設定するように指定します。通常、オーバーロードビットの設定は、ルータに問題が発生した場合にのみ許可されます。例えば、ルータで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により、ルーティングテーブルが不完全または不正確になっている可能性があります。LSP のオーバーロードビットをセットすることにより、ルータがその問題から回復するまで、他のルータは SPF 計算で信頼性の低いルータを無視できます。
On Startup	起動時のオーバーロードビット設定値を入力します。起動時にシステムのオーバーロードビットを設定するように指定します。指定された秒数の間、オーバーロードビットが設定された状態となります。 • 設定可能範囲：5-86400（秒）
Suppress	抑制オプションを指定します。後続のキーワード / キーワードによって識別される、抑制されるプレフィックスタイプを指定します。 • 「None」- 他の ISIS レベルおよび他のプロトコルから学習した IP プレフィックスのアドバタイズを妨げません。 • 「Interlevel」- 別の ISIS レベルから学習した IP プレフィックスがアドバタイズされないように設定します。 • 「External」- 他のプロトコルから学習した IP プレフィックスがアドバタイズされないように設定します。 • 「Both」- 別の ISIS レベルおよび他のプロトコルから学習した IP プレフィックスがアドバタイズされないよう設定します。
SPF Interval Level-1	SPF 間隔レベル 1 の値を指定します。レベル 1 エリアにのみ適用される SPF 計算の ISIS スロットルをカスタマイズするために使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-120（秒）
SPF Interval Level-2	SPF 間隔レベル 2 の値を指定します。レベル 2 エリアにのみ適用される SPF 計算の ISIS スロットルをカスタマイズするために使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-120（秒）
VRF Name	VRF インスタンス名を入力します。「Please Select」をクリックして、リストから VRF インスタンスを選択することも可能です。「No VRF」にチェックを入れると、VRF インスタンスは使用されません。

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

「Please Select」をクリックすると、次の画面が表示されます。



図 9-211　ISIS Global Settings（Please Select）- VRF Selection 画面

使用する VRF エントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「NET List」をクリックすると、次の画面が表示されます。



図 9-212　ISIS Global Settings (NET List) - NET List 画面

画面に表示される項目：

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 と呼ばれるアドレスによって識別されます。NSAP は「ISO10589」に規定されているように 3 つの部分に分割されます。「NET」は、最後のバイトが常に N セレクタで「0」となる NSAP です。「NET」の長さは 8 ～ 20 バイトです。複数の NET を設定して、エリアの分割、統合を行うことが可能です。この実装は IP ルーティングのみに適用されるため、「NET」はシステム ID とエリア ID を定義するように設定されている必要があります。

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

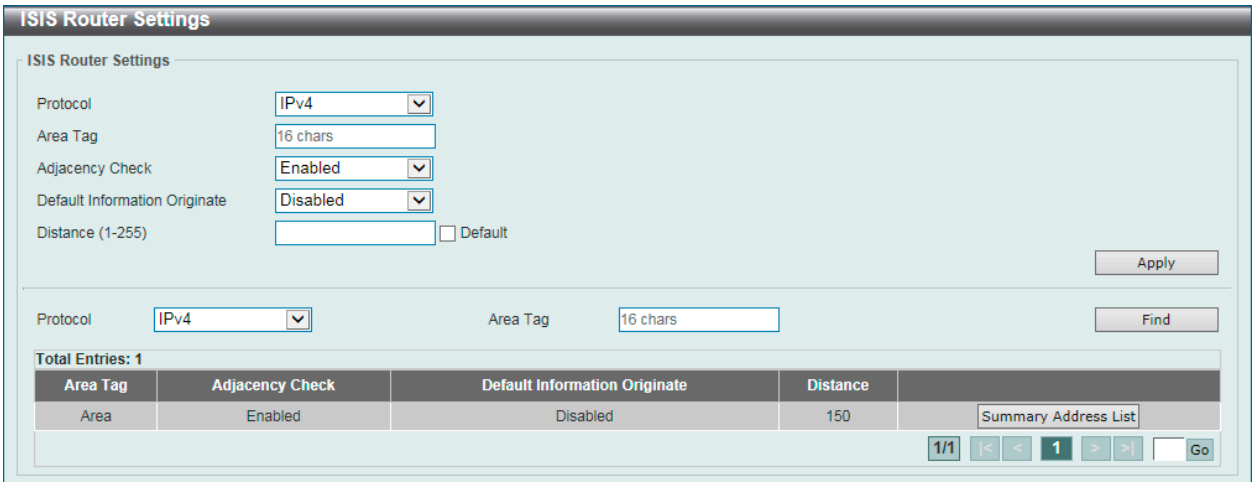


図 9-213　ISIS Router Settings（IPv4）画面

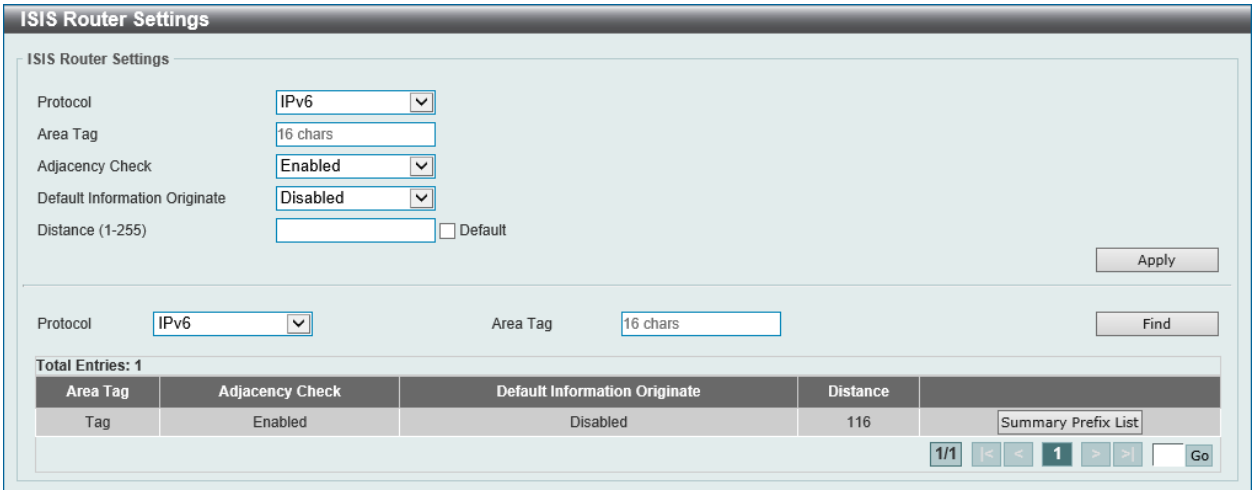


図 9-214　ISIS Router Settings（IPv6）画面

画面に表示される項目：

項目	説明
Protocol	プロトコルを指定します。 • 選択肢：「IPv4」「IPv6」
Area Tag	ISIS エリアタグ（16 文字以内）を指定します。これにより設定されるルーティングプロセスタグにおいて、IP インタフェースが有効になります。
Adjacency Check	Adjacency Check（隣接関係チェック）機能を有効 / 無効に設定します。ISIS は、Hello パケットに対して整合性チェックを実行し、同じプロトコル設定をサポートする隣接ルータとのみ隣接関係を形成します。
Default Information Originate	Default Information Originate 機能を有効 / 無効に設定します。本設定を有効にすると、ISIS は Level-2 Link-State Packets (LSP) でデフォルトルートの通知を生成します。
Distance	Distance 値を指定します。ISIS ルートのアドミニストレーティブディスタンスを定義します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Summary Address List」ボタンをクリックして、サマリアドレスリストを設定します。
「Summary Prefix List」ボタンをクリックして、サマリプレフィックスリストを設定します。
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。

「Summary Address List」をクリックすると、次の画面が表示されます。

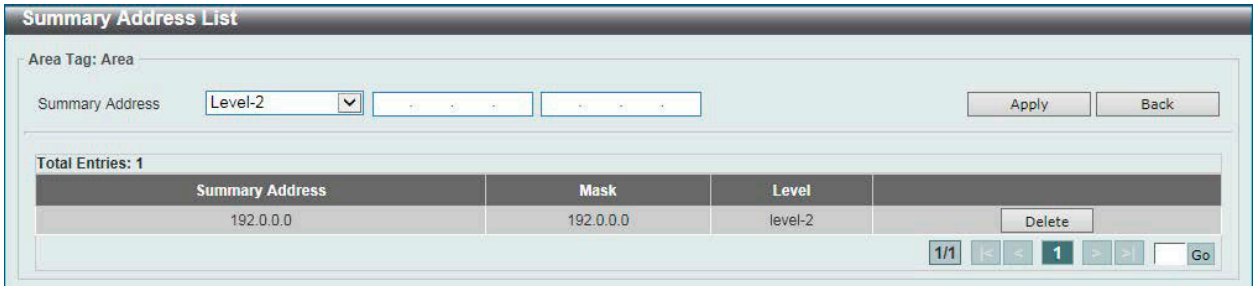


図 9-215　ISIS Router Settings (Summary Address List) - Summary Address List 画面

画面に表示される項目：

項目	説明
Summary Address	サマリアドレスとレベルを指定します。ISIS の集約アドレスを作成するために使用されます。 特定のレベルに対して複数のアドレスグループをまとめることができます。他のルーティングプロトコルから学習したルートも集約できます。サマリを通知するために使用されるメトリックは、より具体的なすべてのルートの最小メトリックです。本機能は、ルーティングテーブルのサイズを縮小することができます。また、リンクステートパケット（LSP）のサイズ、従ってリンクステートデータベース（LSDB）も削減することができます。サマリ通知は多くのより具体的なルートに依存するため、ネットワークの安定性にも役立ちます。多くの場合、単一ルートのフラップによってサマリ通知がフラップすることはありません。 集約アドレスの欠点としては、他のルートの方がより少ない情報ですべての個別の宛先に対して最適なルーティングテーブルを計算することができる可能性があるという点が挙げられます。 • 「Level-1」- レベル 1 に再配送されたルートのみが、設定された IP アドレスとマスク値で集約されます。 • 「Level-1-2」- エレベル 1 とレベル 2 の ISIS にルートを再配布するとき、およびレベル 2 の ISIS がそのエリアで到達可能としてレベル 1 のルートをアドバタイズするときに、集約ルートが適用されます。 • 「Level-2」- レベル 1 ルーティングによって学習されたルートが、設定された IP アドレスとマスク値でレベル 2 バックボーンに集約されます。レベル 2 の ISIS への再配布ルートも集約されます。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。
「Delete」ボタンをクリックして、指定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 9-216　ISIS Router Settings (Summary Prefix List) - Summary Prefix List 画面

画面に表示される項目：

項目	説明
Summary Prefix	レベルを選択し、集約プレフィックスを入力します。 • 「Level-1」- レベル 1 に再配送されたルートのみが、設定されたプレフィックス値で集約されます。 • 「Level-1-2」- エレベル 1 とレベル 2 の ISIS にルートを再配布するとき、およびレベル 2 の ISIS がそのエリアで到達可能としてレベル 1 のルートをアドバタイズするときに、集約ルートが適用されます。 • 「Level-2」- レベル 1 ルーティングによって学習されたルートが、設定されたプレフィックス値でレベル 2 バックボーンに集約されます。レベル 2 の ISIS への再配布ルートも集約されます。

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

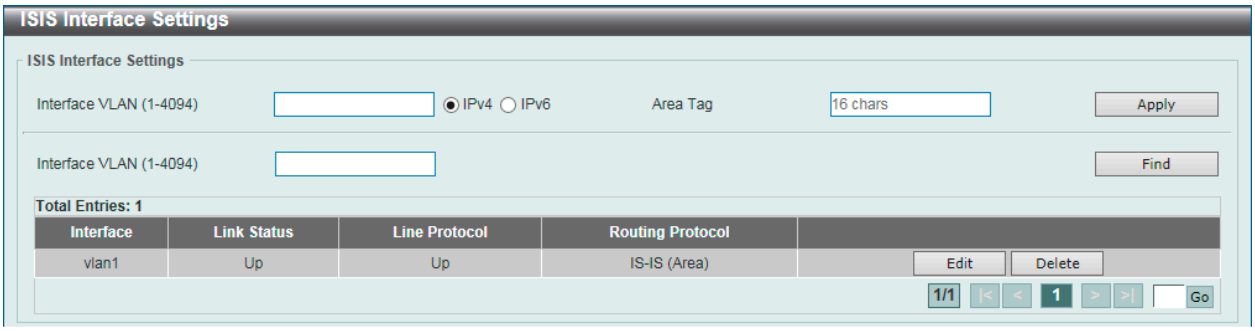


図 9-217　ISIS Interface Settings 画面

画面に表示される項目：

項目	説明
Interface VLAN	本設定に使用する VLAN ID を指定します。 • 設定可能範囲：1-4094
IPv4	指定インタフェースで IPv4 の ISIS ルーティングプロトコルを有効に指定します。
IPv6	指定インタフェースで IPv6 の ISIS ルーティングプロトコルを有効に指定します。
Area Tag	ISIS エリアタグ（16 文字以内）を指定します。

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

「Edit」をクリックすると、以下の画面が表示されます。

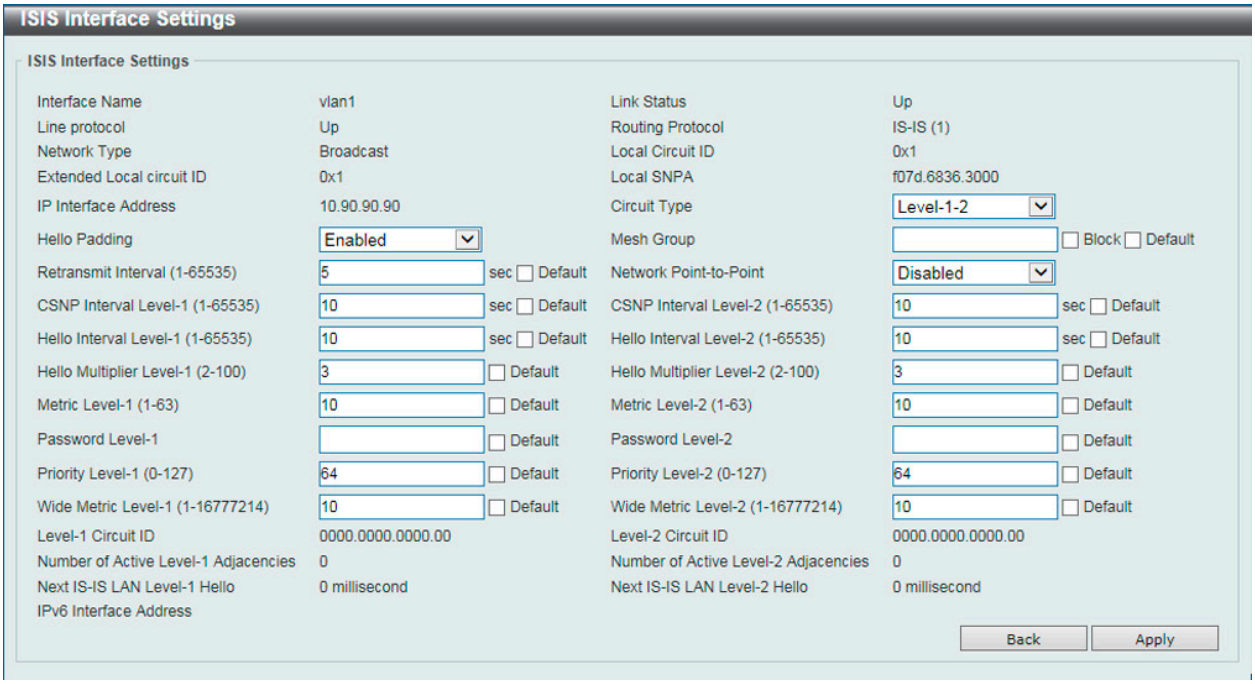


図 9-218　ISIS Interface Settings (Edit) 画面

画面に表示される項目：

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 隣接関係に対してのみスイッチを設定します。 • 「Level-1-2」- レベル 1/2 隣接関係に対してスイッチを設定します。 • 「Level-2」- レベル 2 隣接関係に対してのみスイッチを設定します。
Hello Padding	Hello パディング機能を有効 / 無効に設定します。ISIS ハローパケットは Maximum Transmission Unit（MTU）サイズまでパディングされます。ISIS Hello パケットをフル MTU までパディングすることで、大きいフレームの伝送によるエラーや、隣接関係のインタフェース上の MTU の不一致に起因するエラーといった問題の早期検出に有効です。両インタフェースの MTU が同じ場合にネットワーク帯域の消費を避けるためには、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) フラッディングを最適化するために使用します。 「Block」オプションを指定すると、インタフェースで LSP フラッディングは発生しません。「Default」にチェックを入れると、初期値を使用します。
Retransmit Interval	「Retransmit Interval」（再送信間隔）の値を指定します。Point-to-Point リンク上の各リンク状態パケットの送信間隔を設定するために使用されます。 • 設定可能範囲：1-65535（秒）
Network Point-to-Point	ネットワーク Point-to-Point 機能を有効 / 無効に設定します。ブロードキャストメディアを使用する 2 つのネットワークデバイスが動作するネットワークについて、統合 ISIS ルーティングプロトコルにおいて、ブロードキャストリンクではなく Point-to-Point リンクとして動作するように設定します。
CSNP Interval Level-1	レベル 1 CSNP の送信間隔を指定します。 宛先ルータに対してのみ有効です。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒）
CSNP Interval Level-2	レベル 2 CSNP の送信間隔を指定します。 宛先ルータに対してのみ有効です。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒）
Hello Interval Level-1	レベル 1 Hello パケットの送信間隔を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒）
Hello Interval Level-2	レベル 2 Hello パケットの送信間隔を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒）
Hello Multiplier Level-1	Hello Multiplier（レベル 1）の値を入力します。Hello Multiplier 時間と Hello 間隔は、ISIS Hello パケットで通知される Hold Time と等しくなります。Hello Multiplier の値を小さくすると、収束時間が早くなります。ただし、ルーティングは不安定になります。ネットワークの安定性が必要な場合は、Hello Multiplier の値を大きくします。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：2-100
Hello Multiplier Level-2	Hello Multiplier（レベル 2）の値を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：2-100
Metric Level-1	ISIS メトリック値を指定します。この設定はリンクに割り当てられ、ネットワーク内リンク経由の各ルータから他の宛先へのコストを計算するために使用されます。このメトリックは、レベル 1 ルーティングの SPF 計算で使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-63
Metric Level-2	ISIS メトリック値を指定します。この設定はリンクに割り当てられ、ネットワーク内リンク経由の各ルータから他の宛先へのコストを計算するために使用されます。このメトリックは、レベル 2 ルーティングの SPF 計算で使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-63
Password Level-1	レベル 1 ルーティングで使用する ISIS パスワード（16 文字以内）を入力します。パスワードを設定することにより、許可されていないルータと本ルータとの隣接関係の形成を防ぎ、ネットワークを侵入者から保護することができます。パスワードはプレーンテキストとして交換されるため、セキュリティには制限があります。「Default」にチェックを入れると、初期値を使用します。
Password Level-2	レベル 2 ルーティングで使用する ISIS パスワード（16 文字以内）を入力します。「Default」にチェックを入れると、初期値を使用します。
Priority Level-1	レベル 1 ルーティングで使用する優先値を入力します。本設定は、LAN 上で DIS となるルータの選出に使用されます。優先度は hello パケットでアドバタイズされます。最も高い優先度を持つデバイスが DIS になります。 ISIS では、バックアップ指定ルータはありません。優先度を 0 に設定すると、このシステムが DIS になる可能性は低くなりますが、完全に妨げるわけではありません。優先順位の高いシステムが起動すると、現在の DIS から役割が引き継がれます。優先順位が等しい場合、最大の MAC アドレス値を持つデバイスが優先されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-127
Priority Level-2	レベル 2 ルーティングで使用する優先値を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-127

項目	説明
Wide Metric Level-1	リンクに割り当てるワイドメトリック値を指定します。レベル 1 ルーティングについて、ネットワーク内リンク経由の他のルータから他の宛先へのコストを計算するために使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-16777214
Wide Metric Level-2	リンクに割り当てるワイドメトリック値を指定します。レベル 2 ルーティングについて、ネットワーク内リンク経由の他のルータから他の宛先へのコストを計算するために使用されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-16777214

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

ISIS Redistribute Settings（ISIS 再配布設定）

Intermediate System to Intermediate System (ISIS) 再配布の設定、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。

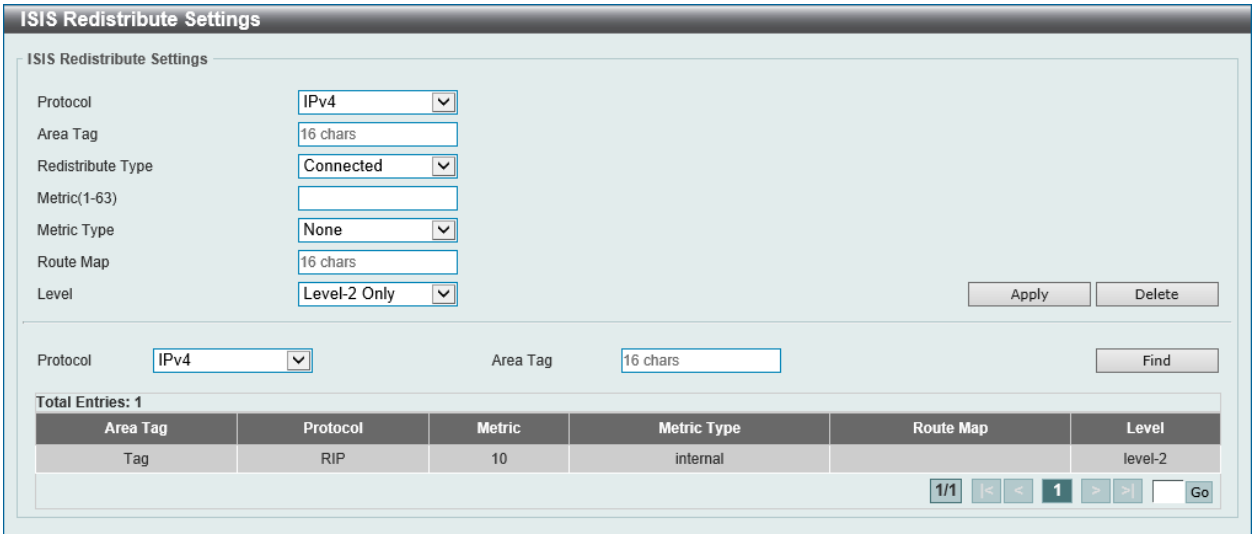


図 9-219　ISIS Redistribute Settings 画面

画面に表示される項目：

項目	説明
Protocol	プロトコルを指定します。 • 選択肢：「IPv4」「IPv6」
Area Tag	ISIS エリアタグ（16 文字以内）を指定します。
Redistribute Type	再配布のタイプを選択します。 • 「Connected」- 接続ルートを ISIS に再配布します。 • 「Static」- スタティックルートを ISIS に再配布します。 • 「RIP」- RIP ルートを ISIS に再配布します。 • 「OSPF」- OSPF ルートを ISIS に再配布します。 • 「BGP」- BGP ルートを ISIS に再配布します。
Metric	再配布ルートのメトリックを指定します。 • 設定可能範囲：1-63
Metric Type	再配布ルートのメトリックの種類を指定します。 • 「None」- メトリックタイプを指定しません。 • 「Internal」- 内部メトリックでアドバタイズされた再配布ルートを指定します。 • 「External」- 外部メトリックでアドバタイズされた再配布ルートを指定します。
Route Map	ルートマップ（16 文字以内）を指定します。
Level	ルーティングレベルを指定します。 • 選択肢：「Level-1」「Level-1-2」「Level-2 Only」

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

Intermediate System to Intermediate System (ISIS) 再配布 ISIS 設定、表示を行います。レベル 1 から 2（あるいはレベル 2 から 1）の ISIS ルート再配布に使用します。

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。

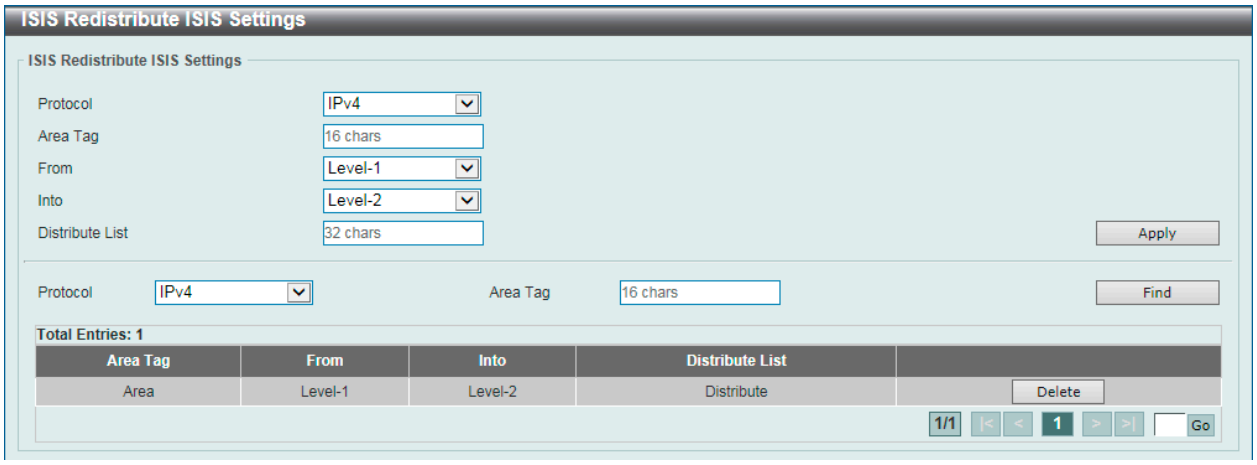


図 9-220　ISIS Redistribute ISIS Settings 画面

画面に表示される項目：

項目	説明
Protocol	プロトコルを指定します。 • 選択肢：「IPv4」「IPv6」
Area Tag	ISIS エリアタグ（16 文字以内）を指定します。
From	再配布されるルートのレベルを指定します。 • 選択肢：「Level-1」「Level-2」
Into	再配布先のルートのレベルを指定します。 • 選択肢：「Level-1」「Level-2」
Distribute List	配布リストの名前（32 文字以内）を指定します。

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

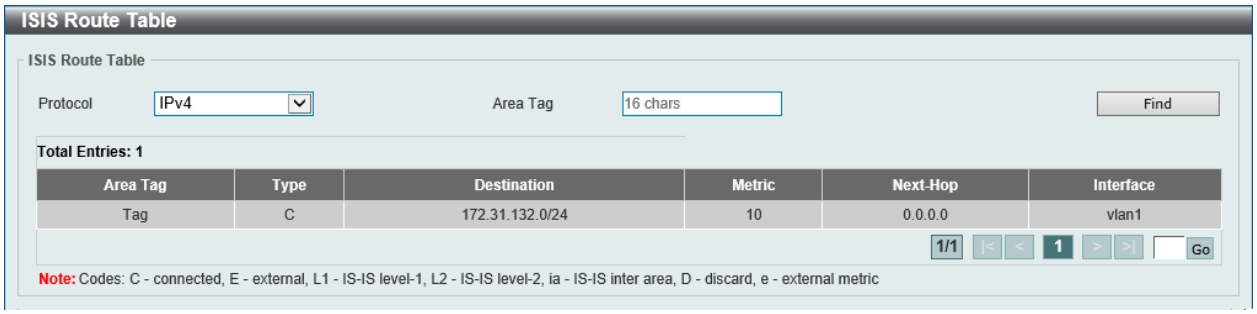


図 9-221　ISIS Route Table 画面

画面に表示される項目：

項目	説明
Protocol	表示するプロトコルを指定します。 • 「IPv4」- ISIS IPv4 ルーティングテーブル情報を表示します。 • 「IPv6」- ISIS IPv6 ルーティングテーブル情報を表示します。
Area Tag	ISIS エリアタグ（16 文字以内）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。
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。

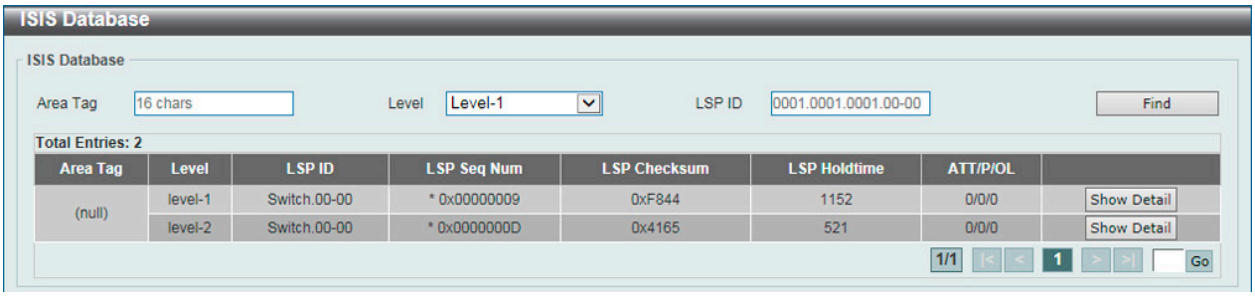


図 9-222　ISIS Database 画面

画面に表示される項目：

項目	説明
Area Tag	ISIS エリアタグ（16 文字以内）を指定します。
Level	ルーティングレベルを指定します。 • 選択肢：「Level-1」「Level-2」
LSP ID	LSP ID を指定します。ID 番号により、特定の LSP の内容を表示します。

「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。
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」ボタンをクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

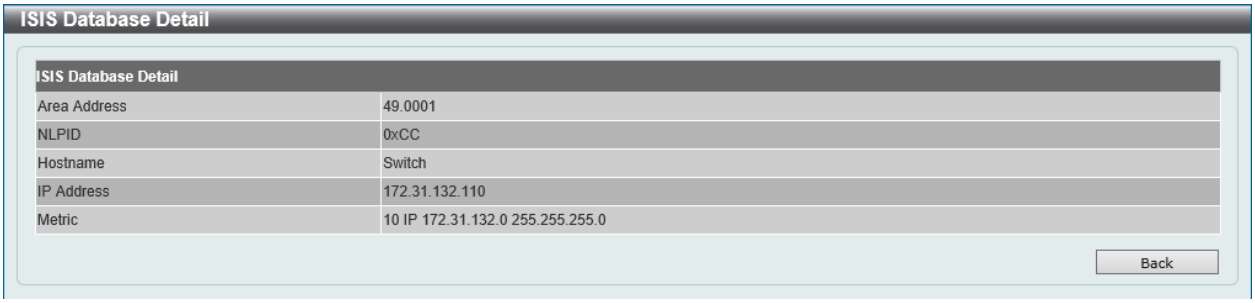


図 9-223　ISIS Database（Show Detail）- ISIS Database Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

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。

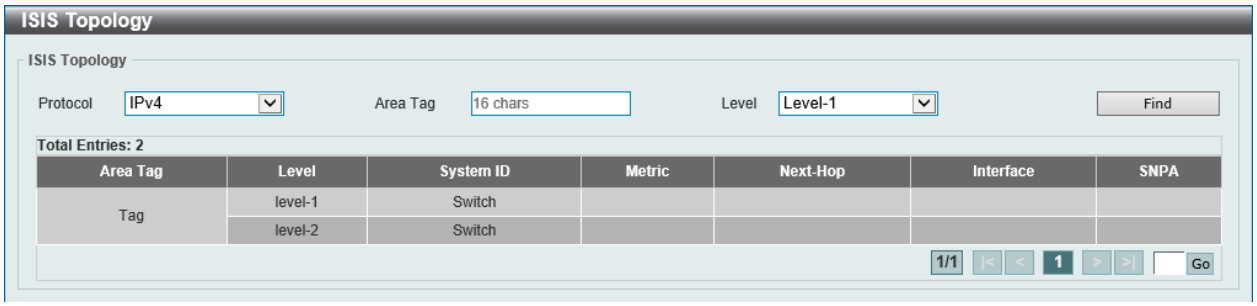


図 9-224　ISIS Topology 画面

画面に表示される項目：

項目	説明
Protocol	表示するプロトコルを指定します。 • 「IPv4」- ISIS IPv4 ルーティングテーブル情報を表示します。 • 「IPv6」- ISIS IPv6 ルーティングテーブル情報を表示します。
Area Tag	ISIS エリアタグ（16 文字以内）を指定します。
Level	ルートのレベルを指定します。 • 選択肢：「Level-1」「Level-2」

「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。

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 9-225　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。

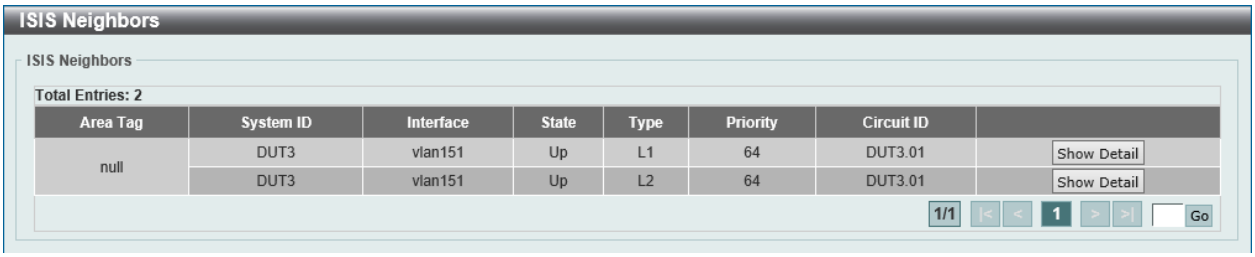


図 9-226　ISIS Neighbors 画面

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」ボタンをクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

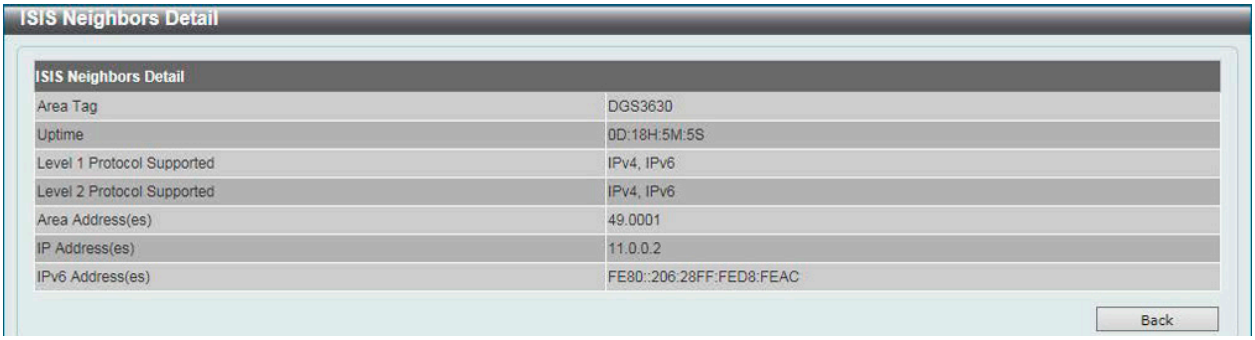


図 9-227　ISIS Neighbors (Show Detail) - ISIS Neighbors Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

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 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。

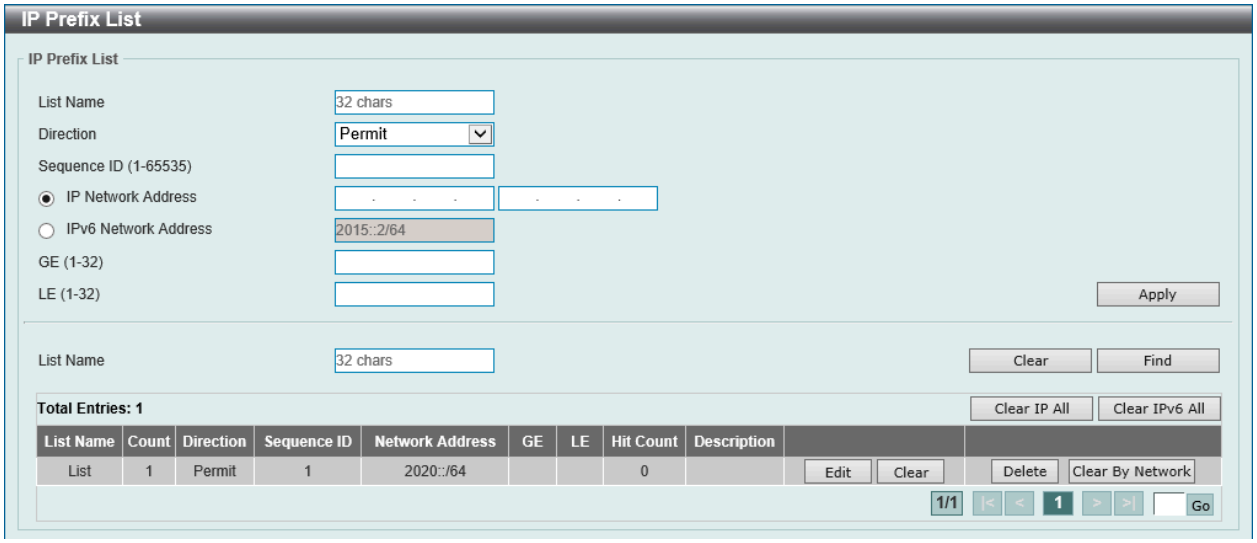


図 9-228　IP Prefix List 画面

画面に表示される項目：

項目	説明
List Name	プレフィックスリスト名（32 文字以内）を入力します。
Direction	ルールを選択します。 • 「Permit」- ルールエントリに一致するルートは許可されます。 • 「Deny」- ルールエントリに一致するルートは拒否されます。
Sequence ID	ルールのシーケンス番号を指定します。 • 設定可能範囲：1-65535
IP Network Address	IPv4 ネットワークアドレス（開始アドレス / 終了アドレス）を入力します。
IPv6 Network Address	IPv6 アドレスとプレフィックス長を入力します。
GE	照合するルートの最小プレフィックス長を入力します。 • 設定可能範囲：1-32（IPv4）、1-128（IPv6）
LE	照合するルートの最大プレフィックス長を入力します。 • 設定可能範囲：1-32（IPv4）、1-128（IPv6）

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、入力した IP プリフィックスリストに関連する情報をクリアします。
「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。

IP 情報のクリア

「Clear IP All」ボタンをクリックして、すべての IP プリフィックスリストに関連するすべての IP 情報をクリアします。
「Clear IPv6 All」ボタンをクリックして、すべての IP プリフィックスリストに関連するすべての IPv6 情報をクリアします。

エントリの編集・クリア

「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Clear」ボタンをクリックして、指定エントリの情報をクリアします。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Clear By Network」ボタンをクリックして、ネットワークに関連する情報をクリアします。

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

Route Map（ルートマップ設定）

ルートマップの作成を行います。

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 9-229　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（16 文字以内）を入力します。
Direction	ルールを選択します。 • 「Permit」- ルールエントリに一致するルートは許可されます。 • 「Deny」- ルールエントリに一致するルートは拒否されます。
Sequence ID	ルールのシーケンス番号を指定します。 • 設定可能範囲：1-65535

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

「Match Clause」の編集

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

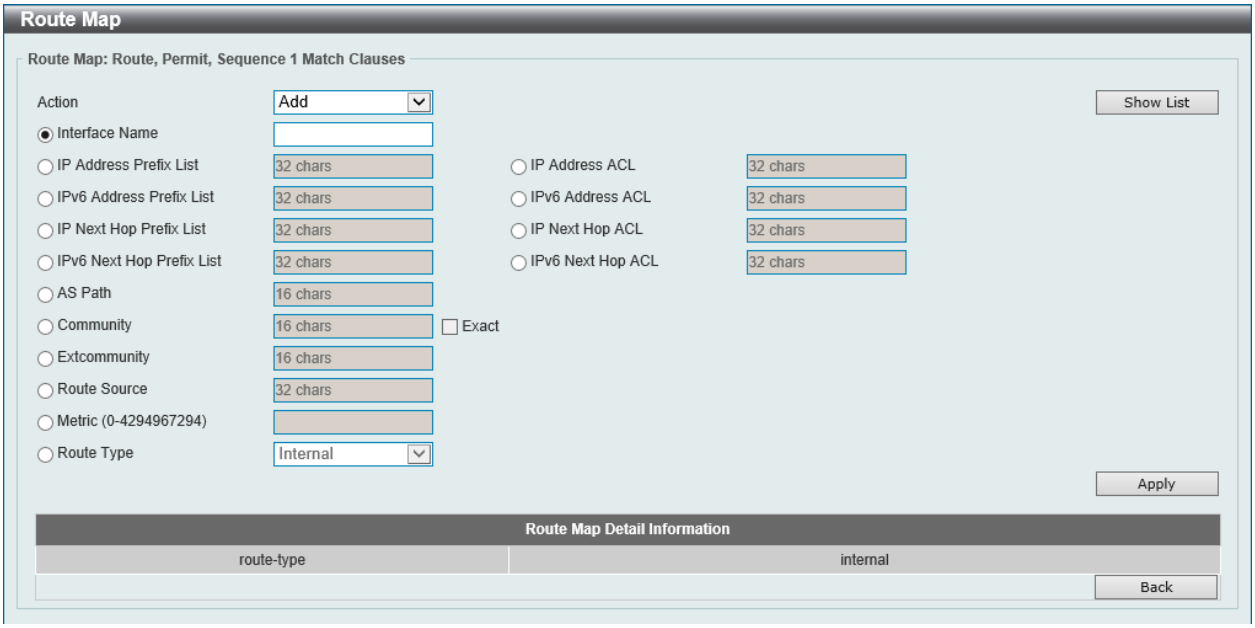


図 9-230　Route Map（Match Clauses）画面

画面に表示される項目：

項目	説明
Action	実行するアクションを指定します。 • 「Add」- 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」- 入力した情報に基づいてエントリを削除します。
Interface Name	インタフェース名を指定します。ルートの外向きインタフェースを照合するための条件を定義します。

項目	説明
IP Address Prefix List（EI モードのみ）	IP プレフィックスリスト名（32 文字以内）を指定します。IP プレフィックスリストに基づいてルートを照合します。
IP Address ACL	標準 / 拡張 IP アクセスリスト（32 文字以内）を指定します。標準 / 拡張 IP アクセスリストに基づいてルートを照合します。
IPv6 Address Prefix List（EI モードのみ）	IPv6 プレフィックスリスト（32 文字以内）を指定します。IPv6 プレフィックスリストに基づいてルートを照合します。
IPv6 Address ACL（EI モードのみ）	標準 / 拡張 IPv6 アクセスリスト（32 文字以内）を指定します。標準 / 拡張 IPv6 アクセスリストに基づいてルートを照合します。
IP Next Hop Prefix List（EI モードのみ）	IP ネクストホッププレフィックスリスト（32 文字以内）を指定します。IP ネクストホッププレフィックスリストに基づいてルートのネクストホップを照合します。
IP Next Hop ACL	標準 IP アクセスリスト（32 文字以内）を指定します。標準 IP アクセスリストに基づいてルートのネクストホップを照合します。
IPv6 Next Hop Prefix List（EI モードのみ）	IPv6 ネクストホッププレフィックスリスト（32 文字以内）を指定します。IPv6 ネクストホッププレフィックスリストに基づいてルートのネクストホップを照合します。
IPv6 Next Hop ACL（EI モードのみ）	標準 IPv6 アクセスリスト（32 文字以内）を指定します。標準 IPv6 アクセスリストに基づいてルートのネクストホップを照合します。
AS Path（EI モードのみ）	標準 / 拡張 IP/IPv6 アクセスリスト（16 文字以内）を指定します。標準 / 拡張 IP/IPv6 アクセスリストに基づいてルートの AS パスを照合します。
Community（EI モードのみ）	標準 / 拡張 IP/IPv6 アクセスリスト（16 文字以内）を指定します。標準 / 拡張 IP/IPv6 アクセスリストに基づいてルートのコミュニティを照合します。「Exact」オプションを指定すると、完全一致が必要となります。
Extcommunity（EI モードのみ）	標準 / 拡張 IP/IPv6 アクセスリスト（16 文字以内）を指定します。標準 / 拡張 IP/IPv6 アクセスリストに基づいてルートの拡張コミュニティを照合します。
Route Source	標準 / 拡張 IP/IPv6 アクセスリスト（16 文字以内）を指定します。標準 / 拡張 IP/IPv6 アクセスリストに基づいてルートソースを照合します。
Metric	ルートのメトリック値を指定します。ルートのメトリックの照合に使用されます。 • 設定可能範囲：0-4294967294
Route Type	ルートタイプを指定します。 • 「Internal」- Open Shortest Path First（OSPF）のエリア内ルートとエリア間ルートを指定します。 • 「External」- 自律システムの OSPF 外部ルートを指定します。Type-1 および Type-2 オプションが指定されていない場合、Type-1 および Type-2 外部ルートは含まれます。 • 「External Type1」- OSPF の Type-1 外部ルートを指定します。 • 「External Type2」- OSPF の Type-2 外部ルートを指定します。

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

「Set Clauses」の編集

「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。

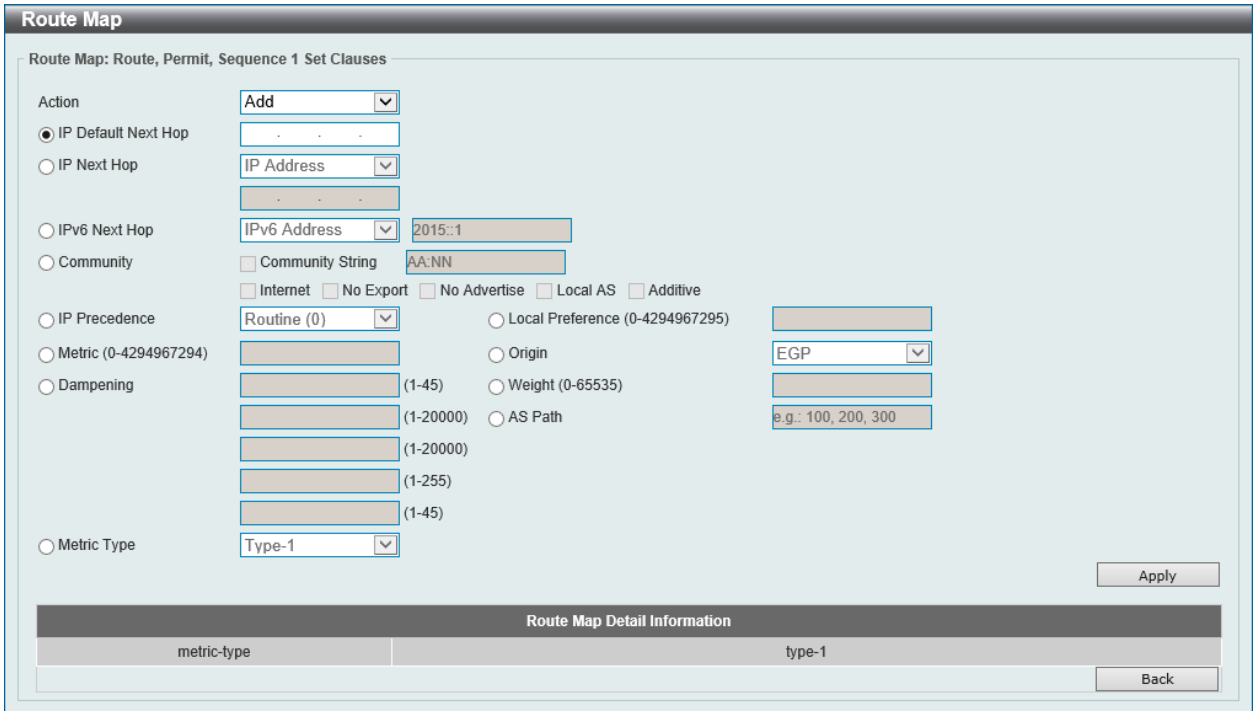


図 9-231　Route Map（Set Clauses）画面

画面に表示される項目：

項目	説明
Action	実行するアクションを指定します。 • 「Add」- 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」- 入力した情報に基づいてエントリを削除します。
IP Default Next Hop	パケットのルーティングに使用されるデフォルトのネクストホップ IP アドレスを入力します。この機能は、複数のデフォルトのネクストホップルータを指定するために使用できます。デフォルトのネクストホップがすでに設定されている場合は、後で設定されたデフォルトのネクストホップがデフォルトのネクストホップリストに追加されます。指定された最初のデフォルトのネクストホップルータがダウンしている場合、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ティングを試行します。最大 16 個のデフォルトのネクストホップ IP アドレスを設定できます。
IP Next Hop	IP ネクストホップの種類を選択します。この機能は、ルートマップシーケンスの一致条件に合致したパケットをルーティングするように、ネクストホップルータを設定します。 • 「IP Address」- パケットをルーティングするネクストホップの IP アドレスを指定します。入力欄にネクストホップ IP アドレスを入力します。最大 16 個のネクストホップ IP アドレスを設定できます。 • 「Peer Address」- BGP ピア・アドレスを次のホップとして指定します。（EI モードのみ） • 「Recursive」- ネクストホップルータとして再帰的な IP アドレスを指定します。入力欄に再帰的ネクストホップ IP アドレスを入力します。
IPv6 Next Hop （EI モードのみ）	IPv6 ネクストホップの種類を選択します。この機能は、ルートマップシーケンスの一致条件に合致したパケットをルーティングするように、ネクストホップルータを設定します。 • 「IPv6 Address」- パケットをルーティングするネクストホップの IPv6 アドレスを指定します。入力欄にネクストホップ IPv6 アドレスを入力します。
Community （EI モードのみ）	セット一致ルールで使用されるコミュニティオプションを選択します。 • 「Community String」- コミュニティ文字列を選択して入力します。「AA:NN」形式のユーザ指定の番号を設定します。AA（AS 番号）と NN（ユーザ指定のコミュニティ番号）から構成されます。カンマで区切った複数の数字を指定することが可能です。 • 「Internet」- ルートはすべてのピアにアドバタイズされます。 • 「No Export」- 外部ピアにアドバタイズしません。 • 「No Advertise」- 他の BGP ピアにルートをアドバタイズしません。 • 「Local AS」- コンフェデレーションのローカル AS またはサブ自律システムから送信しないように指定します。 • 「Additive」- 指定したコミュニティを既存のコミュニティに追加します。
IP Precedence	IP 優先オプションを指定します。IP ヘッダに含まれる優先値となります。このオプションは、ポリシールーティングが IPv4 パケットに関連する場合にのみ有効になります。 • 選択肢：「Routine」「Priority」「Immediate」「Flash」「Flash Override」「Critical」「Internet」「Network」
Local Precedence （EI モードのみ）	ローカルプリファレンス番号を入力します。本設定は、ローカル AS から同じ宛先ネットワークへの優先出口点を制御するために使用されます。 • 設定可能範囲：0-4294967295
Metric	メトリック値を入力します。 • 設定可能範囲：0-4294967294
Origin （EI モードのみ）	Origin オプションを選択します。 • 「IGP」- プレフィックス生成元を Interior Gateway Protocol（IGP）に指定します。 • 「EGP」- プレフィックス生成元を Exterior Gateway Protocol（EGP）に指定します。 • 「Incomplete」- プレフィックス生成元は不明なソースです。
Dampening （EI モードのみ）	ダンプニングの値を指定します。 • 「Half Life Time」- half-life time 値（1-45（分））を入力します。この設定時間を超えると、到達可能なルートのペナルティが半分減らされます。 • 「Reuse Value」- 再利用値（1-20000）を指定します。ルートのペナルティがこの値より低い場合、ルートは抑制されません。 • 「Suppress Value」- 抑制値（1-20000）を指定します。ルートのペナルティがこの値より高い場合、ルートは抑制されます。 • 「Maximum Suppress Time」- ルートの最大抑制時間の値（1-255（分））を指定します。 • 「Unreachable Route's Half Life」- 到達不能ルートのペナルティが半分に減らされるまでの unreachability half-life time の値（1-45/ 分）を指定します。
Weight （EI モードのみ）	Weight 値を入力します。 • 設定可能範囲：0-65535
AS Path （EI モードのみ）	AS パスの値を指定します。
Metric Type	メトリックタイプを選択します。 • 「Type-1」- OSPF 外部タイプ 1 メトリックを使用します。 • 「Type-2」- OSPF 外部タイプ 2 メトリックを使用します。

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

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。

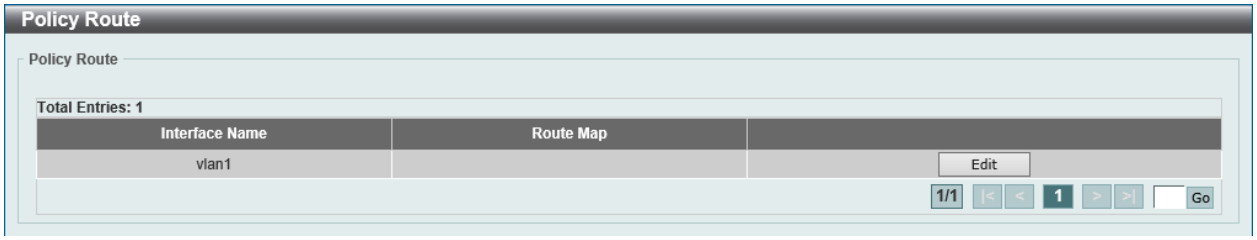


図 9-232　Policy Route 画面

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

エントリの編集
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。

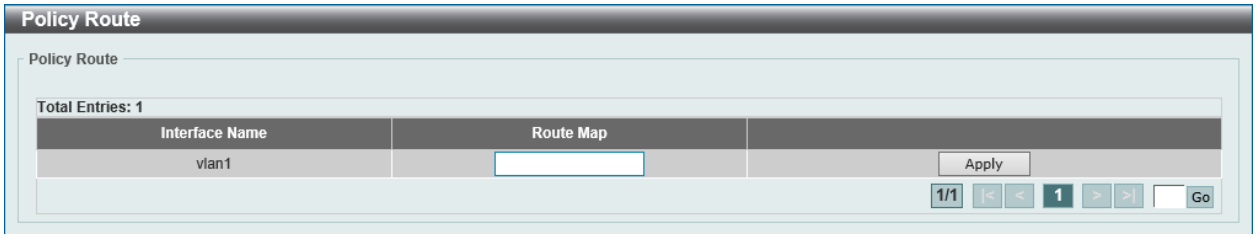


図 9-233　Policy Route（Edit）画面

画面に表示される項目：

項目	説明
Route Map	ポリシールートエントリで使用されるルートマップ名を入力します。

項目を編集し、エントリの「Apply」ボタンをクリックします。

注意　ポリシーベースルーティングと、STP（RST/MST を含む）、ERPS など L2 Loop free protocol とを併用した際に、Discarding Port においても対象トラフィックを転送します。

VRRP（VRRP 設定）

Virtual Router Redundancy Protocol（VRRP）設定の表示と設定に使用します。同じ VRRP グループ内のすべてのルータに、同じ仮想ルータ ID と IP アドレスを設定する必要があります。

仮想ルータグループは、仮想ルータ ID によって識別されます。仮想ルータの IP アドレスは、ホストに設定されているデフォルトルータです。仮想ルータの IP アドレスは、ルータに設定されている実際のアドレス、または未使用の IP アドレスに設定することができます。仮想ルータアドレスが実際に使用されている IP アドレスの場合、この IP アドレスを持つルータが IP アドレスオーナになります。

同じ仮想ルータをサポートするルータのグループ内で、マスタが選出されます。その他のルータはバックアップルータになります。マスタは、仮想ルータに送信されるパケットの転送を行います。

注意　VRRP は VRF/VRF-Lite と併用できません。

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。

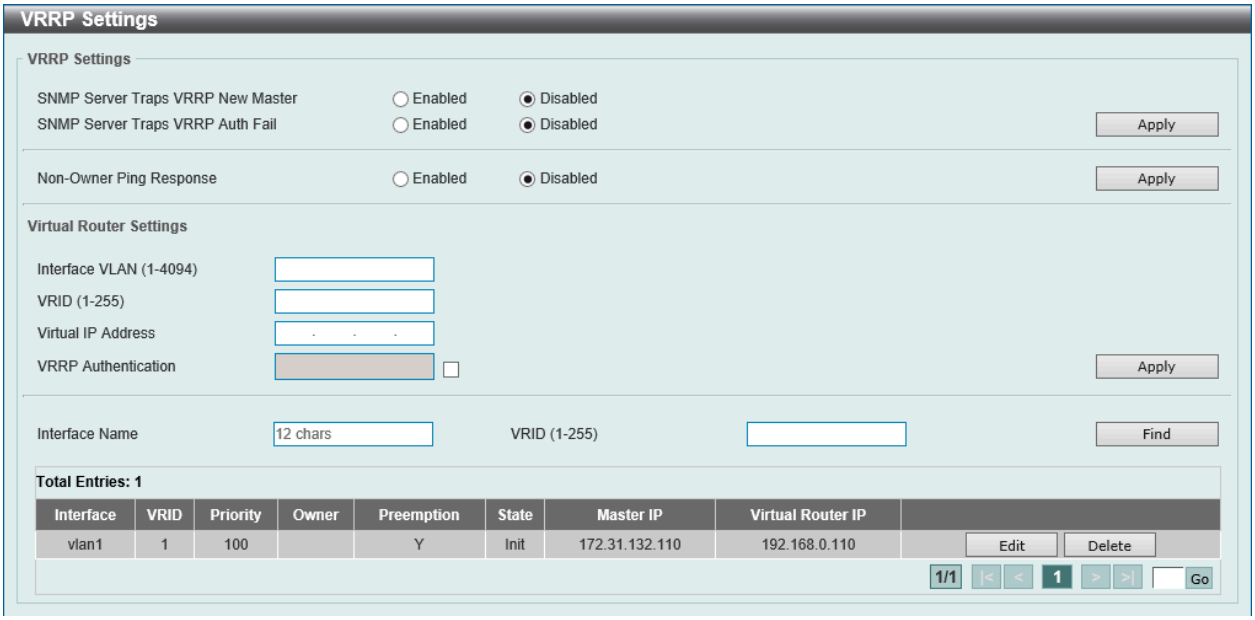


図 9-234　VRRP Settings 画面

画面に表示される項目：

項目	説明
VRRP Settings	
SNMP Server Traps VRRP New Master	新しい VRRP マスタの SNMP サーバトラップ機能を有効 / 無効に設定します。 本設定を有効にした場合、デバイスがマスタ状態に遷移したときに、トラップが送信されます。
SNMP Server Traps VRRP Auth Fail	認証失敗時の SNMP サーバトラップ機能を有効 / 無効に設定します。本設定を有効にした場合、受信したパケットの認証キーまたは認証タイプがこのルータのものと不一致であったときに、トラップが送信されます。
Non-Owner-Ping Response	「Non-Owner-Ping Response」（非オーナ Ping 応答）機能を有効 / 無効に設定します。この仮想ルータに関連付けられているものの非オーナである IP アドレスの ICMP エコー要求に対し、マスタ状態の仮想ルータが応答できるように設定します。
Virtual Router Settings	
Interface VLAN	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
VRID	作成する仮想ルータの ID を入力します。この ID は、VRRP グループ内の仮想ルータを識別するために使用されます。 • 設定可能範囲：1-255
Virtual IP Address	作成する仮想ルータグループの IPv4 アドレスを指定します。
VRRP Authentication	インタフェースで VRRP 認証のプレーンテキスト認証パスワードを有効にします。パスワードの文字列の長さは最大 8 文字です。認証はこのインタフェース上のすべての仮想ルータに適用されます。同じ VRRP グループ内のデバイスには、同じ認証パスワードが設定されている必要があります。
Interface Name	表示するインタフェース名（12 文字以内）を指定します。
VRID	表示する仮想ルータの ID を入力します。 • 設定可能範囲：1-255

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。

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

「Edit」をクリックすると、以下の画面が表示されます。

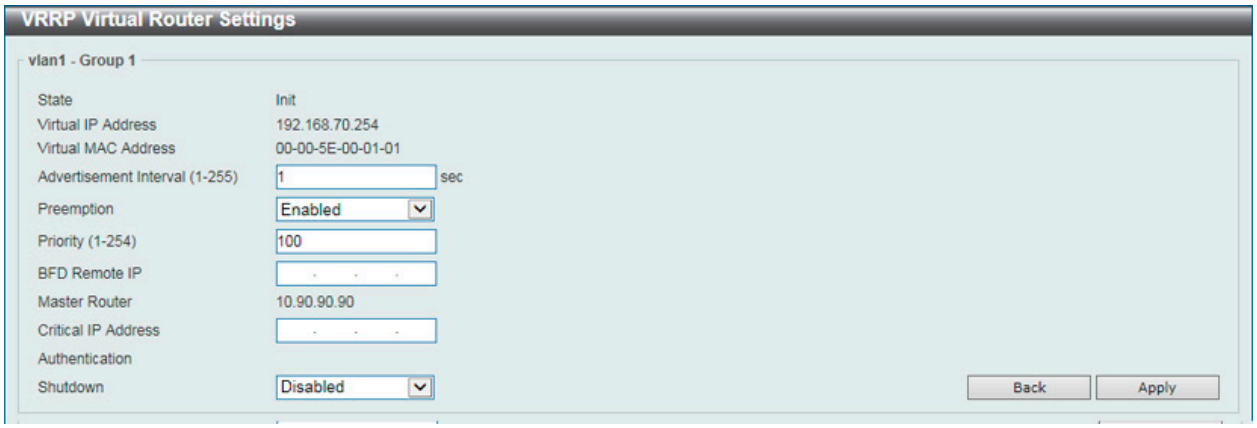


図 9-235　VRRP Settings（Edit）- VRRP Virtual Router Settings 画面

画面に表示される項目：

項目	説明
Advertisement Interval	マスタルータによる VRRP アドバタイズメントの送信間隔を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255（秒） • 初期値：1（秒）
Preemption	Preemption 機能を有効 / 無効に設定します。この機能は、現在のマスタよりも優先順位が高いルータが、マスタロールを引き継ぐことを許可するかどうかを指定します。
Priority	プライオリティ値を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-254
BFD Remote IP	Bidirectional Forwarding Detection（BFD）のリモート IP アドレスを入力します。この IP アドレスは、同じ VRRP 仮想グループ内のデバイスの実際の IP アドレスである必要があります。この VRRP ルータとピアの間に BFD セッションが作成されます。セッションがダウンすると、VRRP がバックアップ状態の場合、高速にマスタへの切り替えが行われます。
Critical IP Address	クリティカル IPv4 アドレスを入力します。仮想ルータに設定されているクリティカル IP アドレスが到達不能な場合、仮想ルータはアクティブ化されません。VRRP グループ毎に、1 つのクリティカル IP のみを追跡できます。
Shutdown	シャットダウン機能を有効 / 無効に設定します。インタフェース上の仮想ルータを無効にするために使用されます。他の非オーナルータをシャットダウンする前に IP アドレスのオーナルータをシャットダウンするミスを回避します。

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

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。

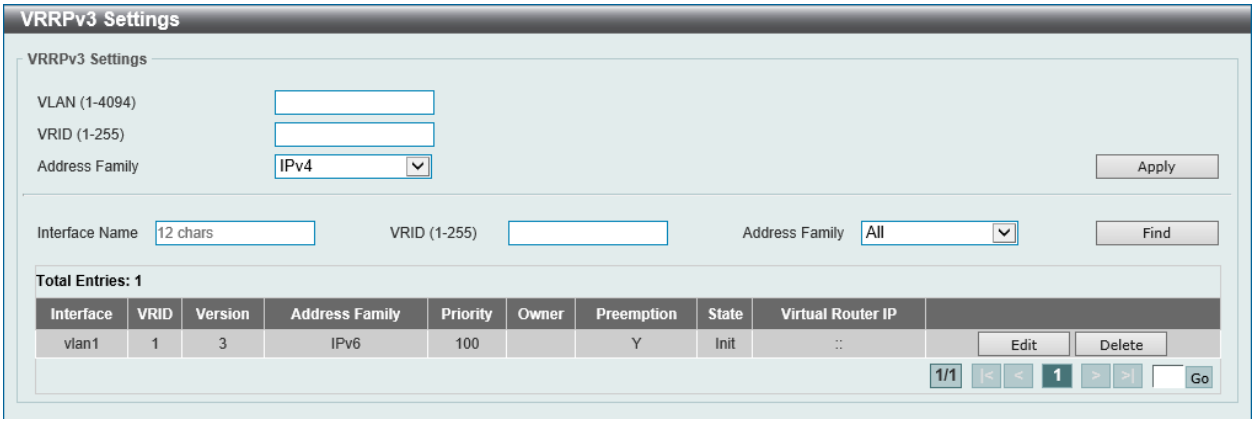


図 9-236　VRRPv3 Settings 画面

画面に表示される項目：

項目	説明
VRRPv3 Settings	
VLAN	VLAN インタフェースの ID を入力します。 • 設定可能範囲：1-4094
VRID	作成する仮想ルータの ID を入力します。 • 定可能範囲：1-255
Address Family	アドレスファミリを指定します。 • 「IPv4」- IPv4 仮想ルータを作成します。 • 「IPv6」- IPv6 仮想ルータを作成します。
VRRPv3 Settings テーブル	
Interface Name	表示するインタフェース名（12 文字以内）を指定します。
VRID	表示する仮想ルータの ID を入力します。 • 定可能範囲：1-255
Address Family	表示するアドレスファミリを指定します。 • 「All」- すべての仮想ルータを表示します。 • 「IPv4」- IPv4 仮想ルータのみ表示します。 • 「IPv6」- IPv6 仮想ルータのみ表示します。

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

「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。

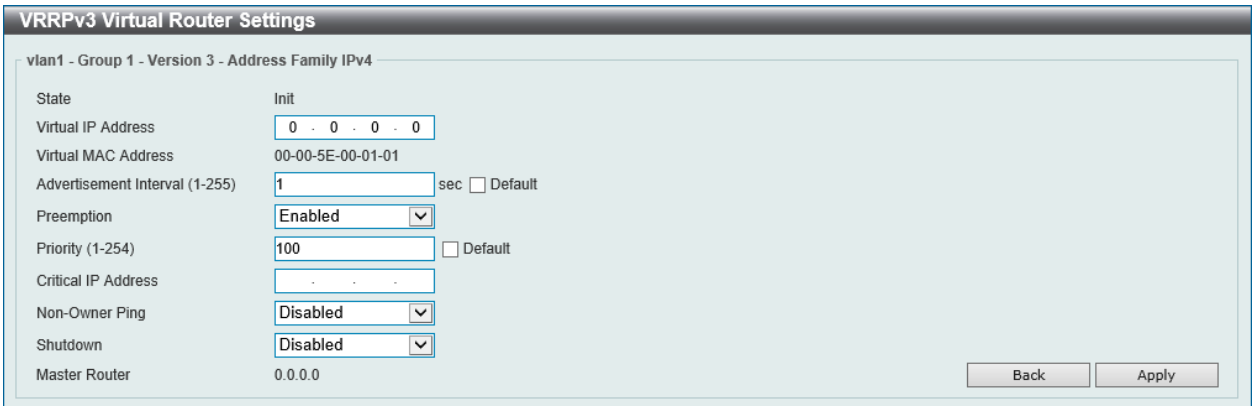


図 9-237　VRRPv3 Settings (Edit/IPv4 Address Family) - VRRPv3 Virtual Router Settings 画面

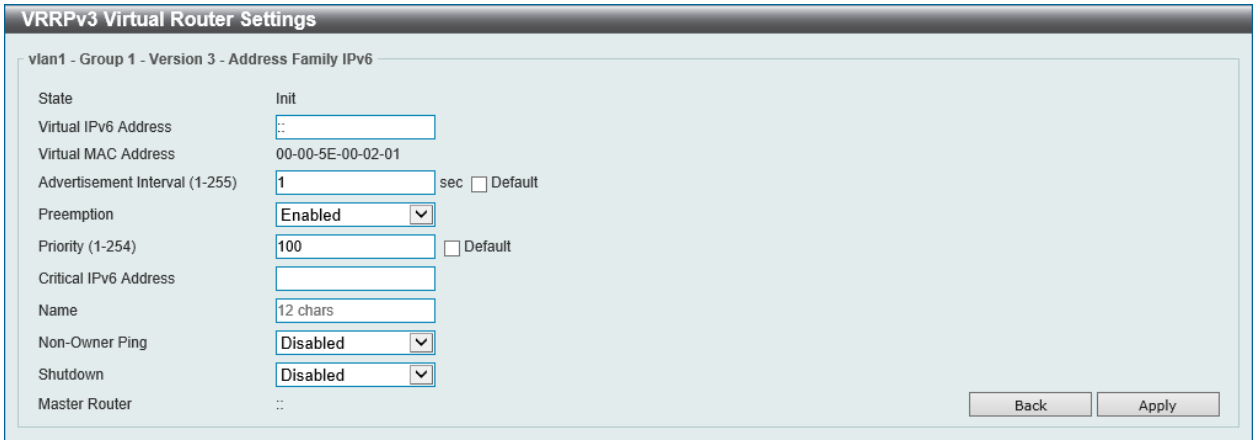


図 9-238　VRRPv3 Settings (Edit/IPv6 Address Family) - VRRPv3 Virtual Router Settings 画面

画面に表示される項目：

項目	説明
Virtual IP Address/ Virtual IPv6 Address	仮想 IPv4/IPv6 アドレスを入力します。同じ VRRP グループ内のすべてのルータに、同じ仮想ルータ ID と仮想アドレスを設定する必要があります。仮想ルータの IPv4/IPv6 アドレスは、ルータに設定されている実際のアドレスでも、未使用のアドレスでもかまいません。仮想アドレスがインタフェースの実際のアドレスと同じ場合、この仮想ルータは IPv4/IPv6 アドレスのオーナとなります。
Advertisement Interval	マスタルータによる VRRP アドバタイズメントの送信間隔を指定します。VRRP グループ内のすべての仮想ルータは、同じタイマ値を使用する必要があります。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255（秒）
Preemption	Preemption 機能を有効 / 無効に設定します。この機能は、現在のマスタよりも優先順位が高いルータが、マスタロールを引き継ぐことを許可するかどうかを指定します。
Priority	仮想ルータの優先値を指定します。VRRP グループのマスタは、この優先値に基づいて選択されます。優先値が最も高い仮想ルータがマスタになり、他の仮想ルータは VRRP グループのバックアップとして機能します。同じ優先値を持つルータが複数存在する場合、IPv4/IPv6 アドレスの値の大きい方がマスタになります。VRRP グループの IPv4/IPv6 アドレスオーナであるルータは、常に VRRP グループのマスタであり、最も高いプライオリティ「255」を持ちます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-254
Critical IP Address/ Critical IPv6 Address	クリティカル IPv4/IPv6 アドレスを入力します。仮想ルータに設定されているクリティカル IPv4/IPv6 アドレスが到達不能な場合、仮想ルータはアクティブ化されません。VRRP グループ毎に、1 つのクリティカル IPv4/IPv6 アドレスのみを追跡できます。
Name	IPv6 アドレスファミリの名前を入力します。（12 文字以内） IPv6 アドレスファミリエントリの画面にのみ表示されます。
Non-Owner Ping	「Non-Owner Ping」（非オーナ Ping）機能を有効 / 無効に設定します。マスタ状態の非 IPv4/IPv6 アドレスオーナ仮想ルータが IPv4/IPv6 アドレスの ICMP エコー要求に応答できるようにするために使用します。
Shutdown	シャットダウン機能を有効 / 無効に設定します。インタフェース上の仮想ルータを無効にするために使用されます。他の非オーナルータをシャットダウンする前に IPv4/IPv6 アドレスのオーナルータをシャットダウンするミスを回避します。

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

第 10 章　QoS（QoS 機能の設定）

本スイッチは、802.1p プライオリティキューイングの QoS（Quality of Service）機能をサポートしています。

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

サブメニュー	説明
Basic Settings（基本設定）	QoS の Basic Settings（基本設定）を行います。
Advanced Settings（アドバンス設定）	QoS の Advanced Settings（アドバンス設定）を行います。
QoS 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。

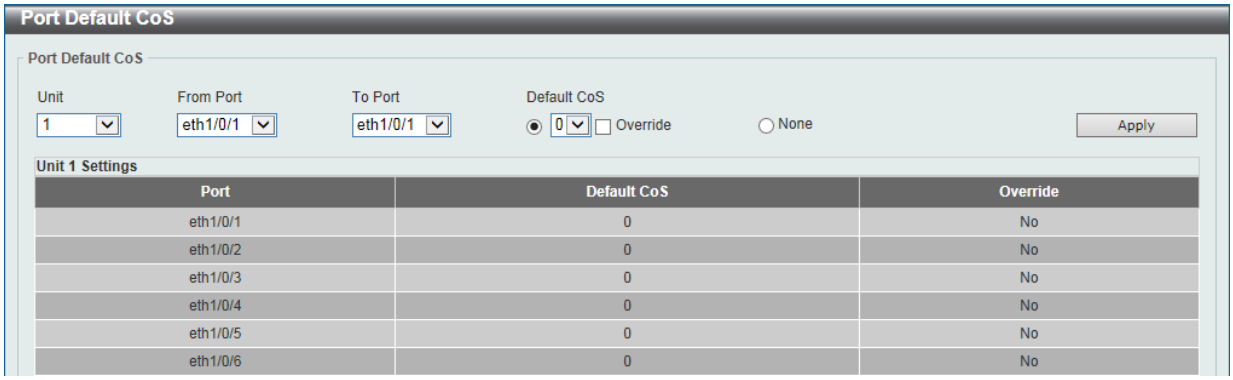


図 10-1　Port Default CoS 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Default CoS	ポートのデフォルト CoS を指定します。「Override」にチェックを入れると、パケットの CoS を上書きします。デフォルト CoS は、ポートで受信した全てのパケット（タグ付き / タグなしの両方）に適用されます。「None」を選択すると、タグ付きパケットの場合はパケットの CoS を使用し、タグなしパケットの場合はポートデフォルト CoS となります。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。

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

ポートスケジューラ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。

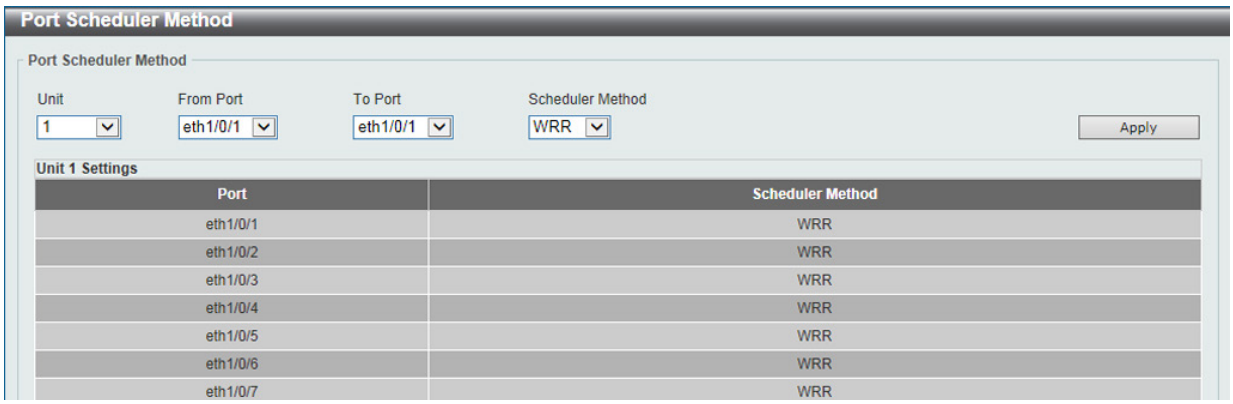


図 10-2　Port Scheduler Method 画面

画面に表示される項目：

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

項目	説明
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。 • 「SP」- すべてのキューは Strict Priority（絶対優先）スケジューリングを使用します。最も高い CoS 優先度のキューから絶対優先で送信されます。 • 「RR」- すべてのキューは Round-Robin スケジューリングを使用します。キューを順番に見ながら、均等な比率でパケットが処理されます。 • 「WRR」- Round-Robin 方式でパケットをキューに送出します。最初に、各キューは可変の重みをセットします。CoS キューからパケットが送信される度に、重み（Weight）の値から「1」が差し引かれ、次の CoS 優先度キューが処理されます。重みが「0」になると、重みが補充されるまでそのキューの処理は停止します。すべての CoS キューの重みが「0」に到達すると、キューの重みが補充されます。（初期値） • 「WDRR」- Round-Robin 方式で送信キューに蓄積された未処理のクレジットを処理します。最初に、各キューはクレジットカウンタを可変の数値にセットします。CoS キューからパケットが送信される度に、クレジットカウンタからパケットサイズが差し引かれ、次の CoS 優先度キューが処理されます。クレジットカウンタが「0」になると、クレジットが補充されるまでそのキューの処理は停止します。すべての CoS キューのクレジットカウンタが「0」に到達すると、クレジットカウンタが補充されます。クレジットカウンタが 0 またはマイナスになり、最後のパケット送信が完了するまで処理が行われます。その後、クレジットは補充されます。クレジットが補充されると、各 CoS キューのクレジットカウンタにクレジットのクオンタムが補充されます。各キューのクオンタムはユーザ定義により異なる場合があります。 特定の CoS キューを SP モードに設定する場合、それより優先度の高い CoS キューについても SP モードである必要があります。

「Apply」ボタンをクリックして、設定内容を適用します。

Queue Settings（QoS 設定）

キューを設定、表示します。

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

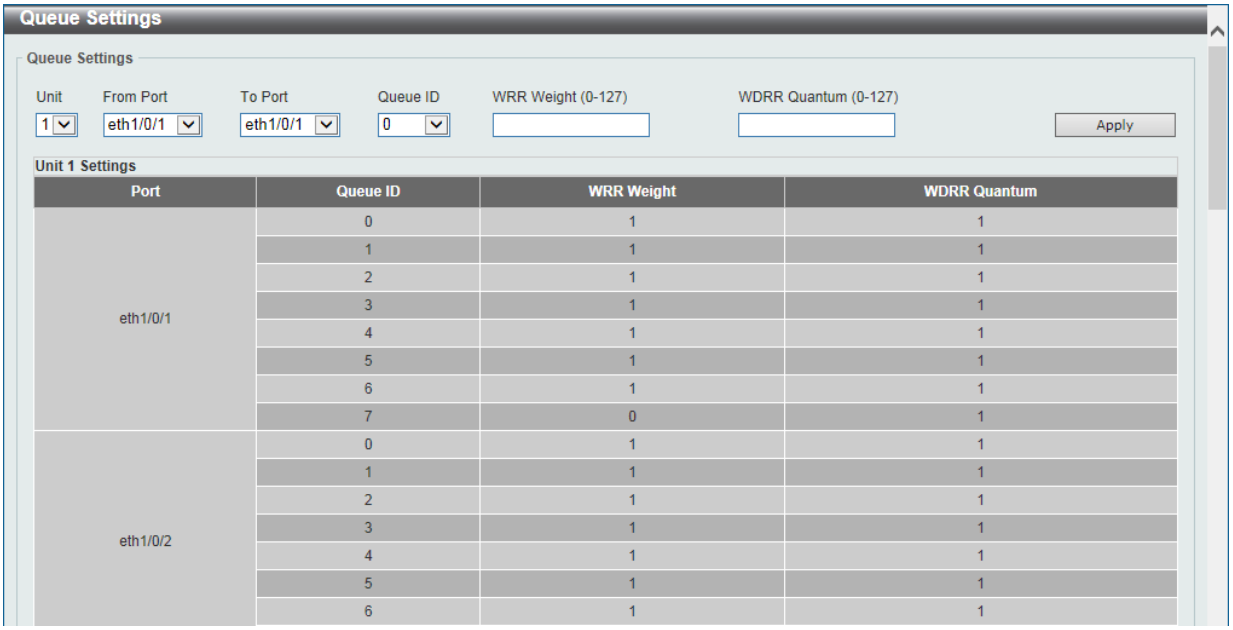


図 10-3　Queue Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Queue ID	キュー ID を指定します。 • 設定可能範囲：0-7
WRR Weight	WRR の値を入力します。「Expedited Forwarding」(EF) の動作要件を満たすには、最も優先度の高いキューが常に「Per-hop Behavior」(PHB) により選択され、キューのスケジュールモードが Strict プライオリティである必要があります。そのため、「Differentiate Service」がサポートされている場合、最後のキューの重みは 0 に設定する必要があります。 • 設定可能範囲：0-127
WDRR Quantum	「WDRR Quantum」の値を入力します。 • 設定可能範囲：0-127

「Apply」ボタンをクリックして、設定内容を適用します。

CoS to Queue Mapping（CoS キューマッピング設定）

CoS-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。

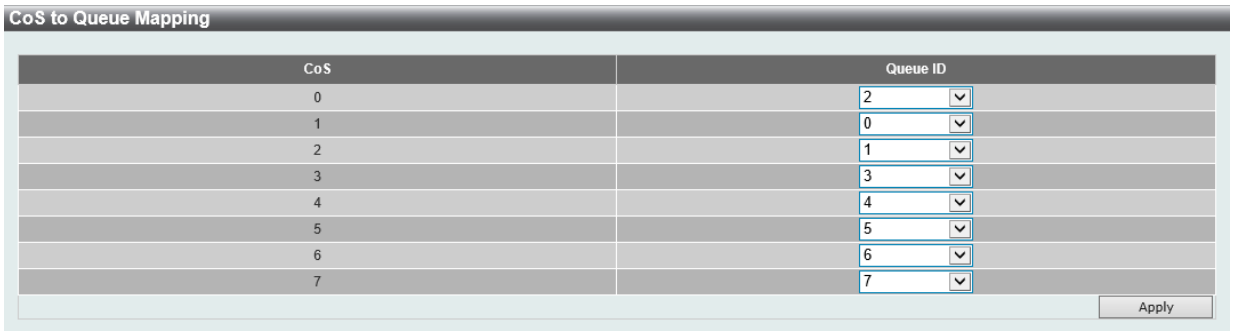


図 10-4　CoS to Queue Mapping 画面

画面に表示される項目：

項目	説明
Queue ID	各 CoS 値にマッピングされるキュー ID を指定します。 • 選択肢：0-7

「Apply」ボタンをクリックして、設定内容を適用します。

Port Rate Limiting（ポートレート制限設定）

ポートレート制限の設定を行います。

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

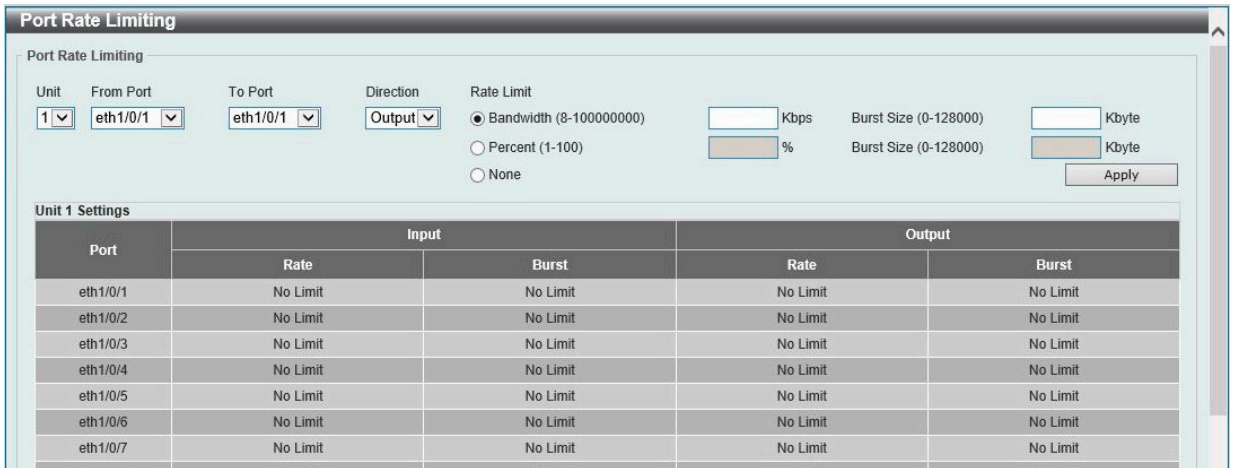


図 10-5　Port Rate Limiting 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Direction	レート制限の対象を指定します。「Output（イーグレス）」のみ指定可能です。送信パケットのレート制限が設定されます。
Rate Limit	レート制限の値を指定します。 指定された制限は、指定インタフェースの最大速度を超えることはできません。受信帯域幅制限については、受信トラフィックが制限を超えたときに、受信側は PAUSE フレームまたはフロー制御フレームを送信します。 • 「Bandwidth」- 受信 / 送信の帯域幅の値を入力欄に入力します。「Burst Size」に 0 を指定した場合、インタフェース上でレート制限は無効（制限なし）となります。 - 設定可能範囲：8-100000000（Kbps） - 「Burst Size」：0-128000（Kbytes） • 「Percent」- 受信 / 送信の帯域幅パーセンテージを入力欄に入力します。 - 設定可能範囲：1-100（%） - 「Burst Size」：0-128000（Kbytes） • 「None」- 指定ポートのレート制限を削除します。初期値では、すべてのポートの送受信に対し、このオプションが使用されます。

「Apply」ボタンをクリックして、設定内容を適用します。

Queue Rate Limiting（キューレート制限設定）

キューレートの制限設定をします。

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

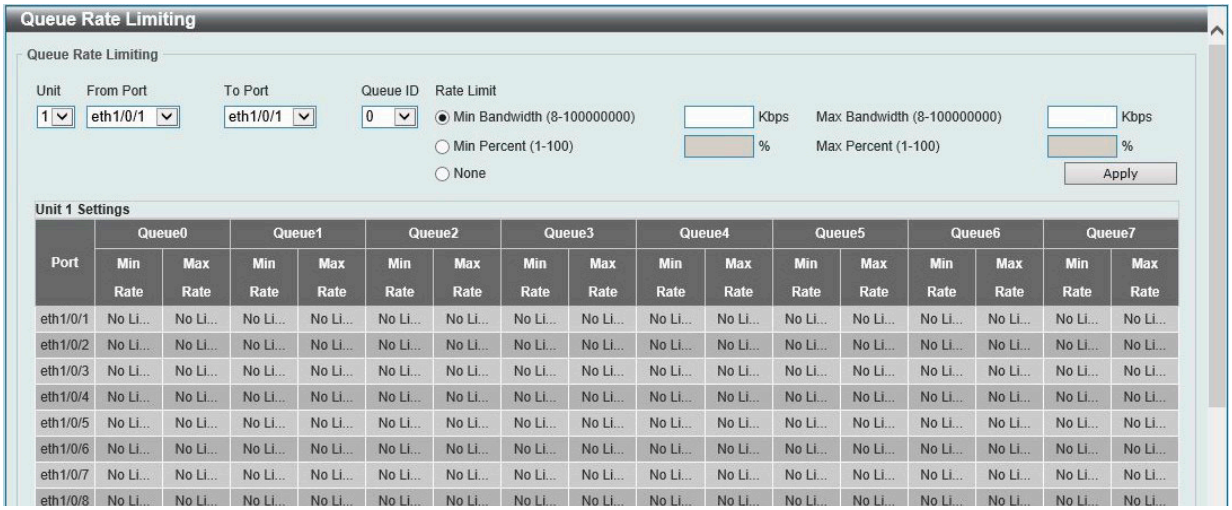


図 10-6　Queue Rate Limiting 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Queue ID	キュー ID を指定します。 • 選択肢：0-7
Rate Limit	キューレート制限の設定を行います。 • 「Min Bandwidth / Max Bandwidth」- 最小 / 最大のレート制限帯域値を入力します。 　- 設定可能範囲：8-100000000（Kbps） • 「Min Percent / Max Percent」- 最小 / 最大のレート制限パーセンテージを入力します。 　- 設定可能範囲：1-100（%） • 「None」- 指定ポートのレート制限を「なし」に設定します。初期値では、すべてのポートのすべてのキューに対し、このオプションが使用されます。 最小帯域の値により、キューから送信されるパケットが保証されます。また、帯域幅に余裕がある場合でも、キューからの送信パケットは最大帯域幅を超えることはありません。 各キューの最小帯域幅が保証されるようにするために、最小帯域幅の合計はインタフェース帯域幅の 75% 未満である必要があります。最も優先度の高い Strict プライオリティキューに対しては、最低保証帯域幅を設定する必要はありません。これは、すべてのキューの最小帯域幅が一杯である場合にはこのキューのトラフィックが最初に処理されるためです。1 つの CoS における最小保証帯域は、物理ポートにまたがって使用することはできないため、本設定は物理ポートにのみ設定可能であり、ポートチャネルに対しては設定できません。

「Apply」ボタンをクリックして、設定内容を適用します。

Advanced Settings（アドバンス設定）

QoS の Advanced Settings（アドバンス設定）を行います。

DSCP Mutation Map（DSCP 変更マップ設定）

本項目では「Differentiated Services Code Point」(DSCP) 変更マップ設定を行います。インタフェースでパケットを受信すると、QoS 関連の処理の前に、DSCP 変更マップに基づき受信 DSCP が他の DSCP に変更されます。DSCP 変更機能は、異なる DSCP 割り当てを持つドメインを統合する場合に役に立ちます。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。後続のすべての動作は変更 DSCP に基づいて行われます。

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

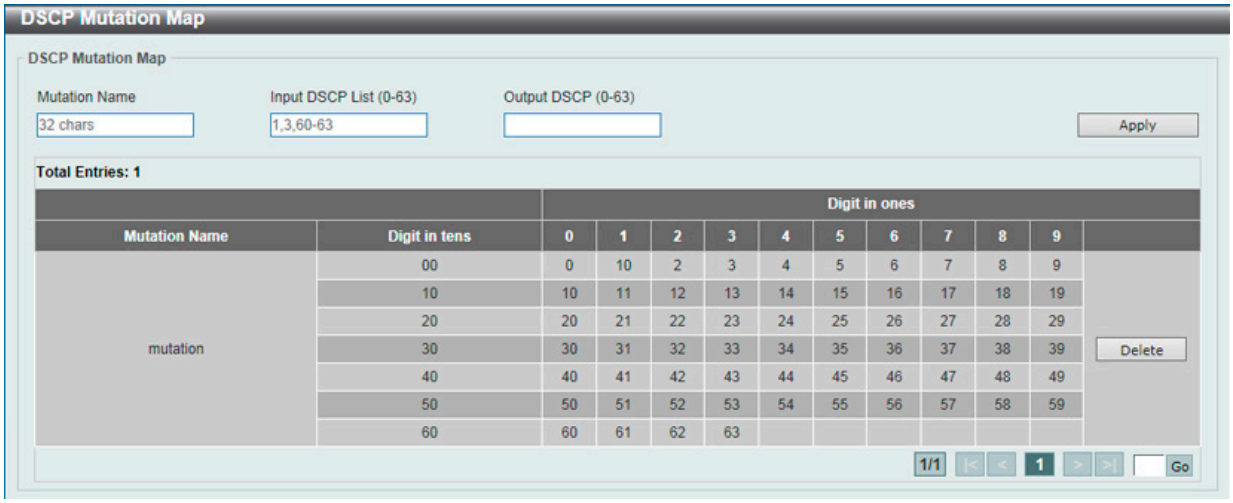


図 10-7　DSCP Mutation Map 画面

画面に表示される項目：

項目	説明
Mutation Name	DSCP 変更マップ名を指定します。（32 文字以内）
Input DSCP List	インプット DSCP リストの値を入力します。 • 設定可能範囲：0-63
Output DSCP	アウトプット DSCP リストの値を入力します。 • 設定可能範囲：0-63

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

Port Trust State and Mutation Binding（ポートトラスト設定 & 変更マップバインディング）

ポートトラスト設定、変更マップのバインディング設定を行います。

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

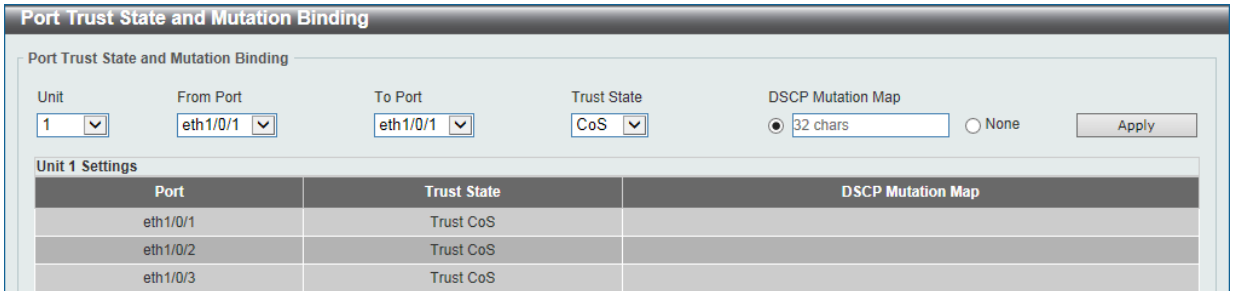


図 10-8　Port Trust State and Mutation Binding 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Trust State	ポートトラストのオプションを指定します。 • 選択肢：「CoS」「DSCP」

項目	説明
DSCP Mutation Map	DSCP 変更マップ名を入力します。（32 文字以内） 「None」を選択すると、DSCP 変更マップがポートに割り当てられません。

「Apply」ボタンをクリックして、設定内容を適用します。

DSCP CoS Mapping（DSCP CoS マップ設定）

本スイッチにおける DSCP CoS マップの設定と表示を行います。

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

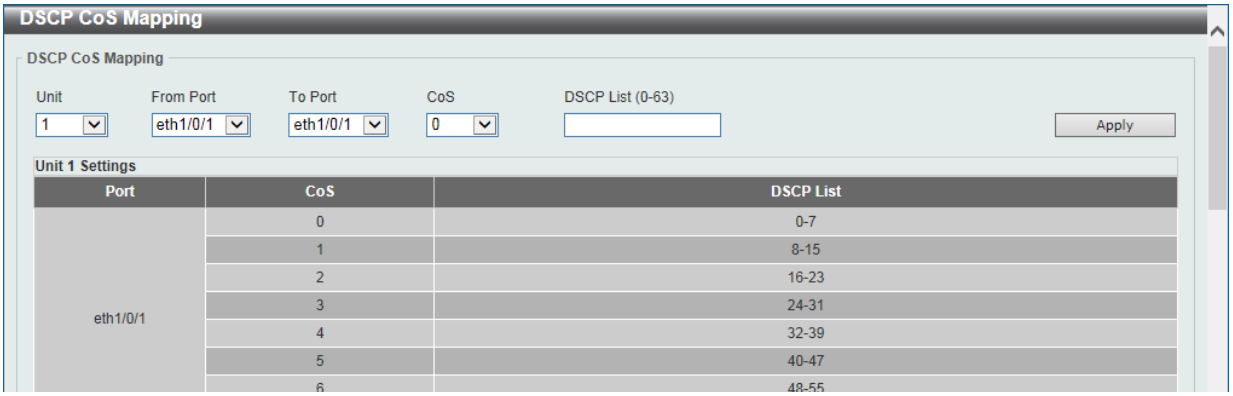


図 10-9　DSCP CoS Mapping 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
CoS	DSCP リストにマッピングする CoS 値を指定します。 • 設定可能範囲：0-7
DSCP List	CoS 値にマッピングする DSCP リストの値を入力します。 • 設定可能範囲：0-63

「Apply」ボタンをクリックして、設定内容を適用します。

CoS Color Mapping（CoS カラーマップ設定）

本スイッチにおける CoS カラーマップの設定と表示を行います。

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

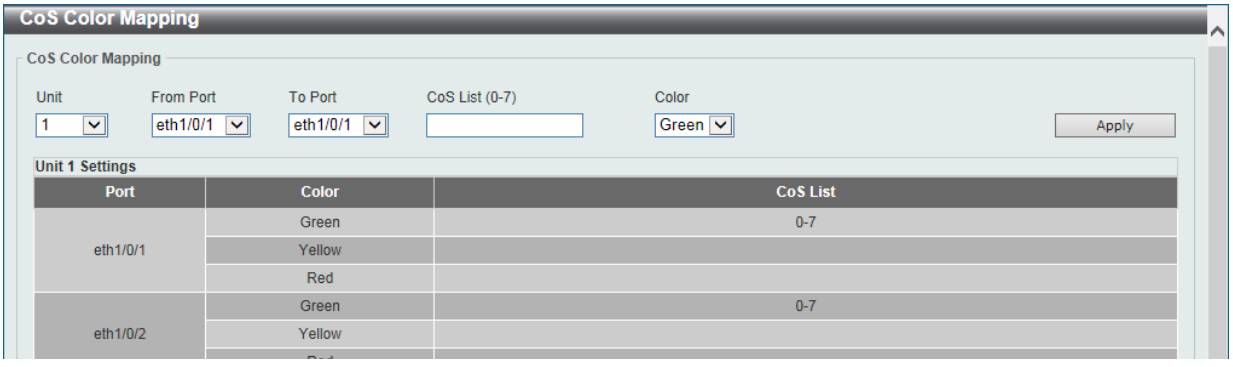


図 10-10　CoS Color Mapping 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
CoS List	カラーにマッピングされる CoS 値を指定します。 • 設定可能範囲：0-7
Color	CoS 値にマッピングされるカラーを指定します。 • 選択肢：「Green」「Yellow」「Red」

「Apply」ボタンをクリックして、設定内容を適用します。

DSCP Color Mapping（DSCP カラーマップ設定）

本スイッチにおける DSCP カラーマップの設定と表示を行います。

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

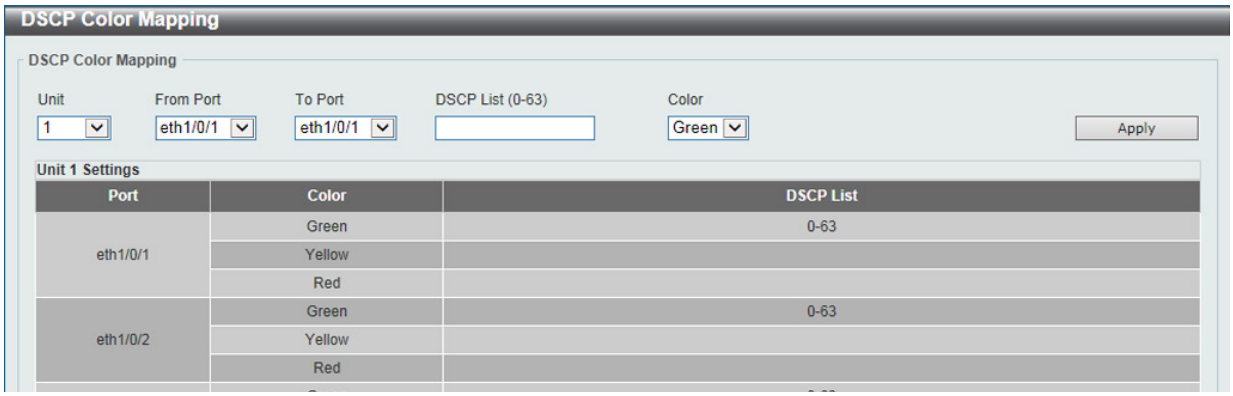


図 10-11　DSCP Color Mapping 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
DSCP List	カラーにマッピングされる DSCP リストを指定します。 • 設定可能範囲：0-63
Color	DSCP 値にマッピングされるカラーを指定します。 • 選択肢：「Green」「Yellow」「Red」

「Apply」ボタンをクリックして、設定内容を適用します。

Class Map（クラスマップ設定）

本スイッチにおけるクラスマップの設定と表示を行います。

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



図 10-12　Class Map 画面

画面に表示される項目：

項目	説明
Class Map Name	クラスマップ名を指定します。（32 文字以内）
Multiple Match Criteria	一致条件の種類を指定します。 • 選択肢：「Match All（すべて一致）」「Match Any（いずれかに一致）」

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

「Match」ボタンをクリックすると下記の画面が表示されます。

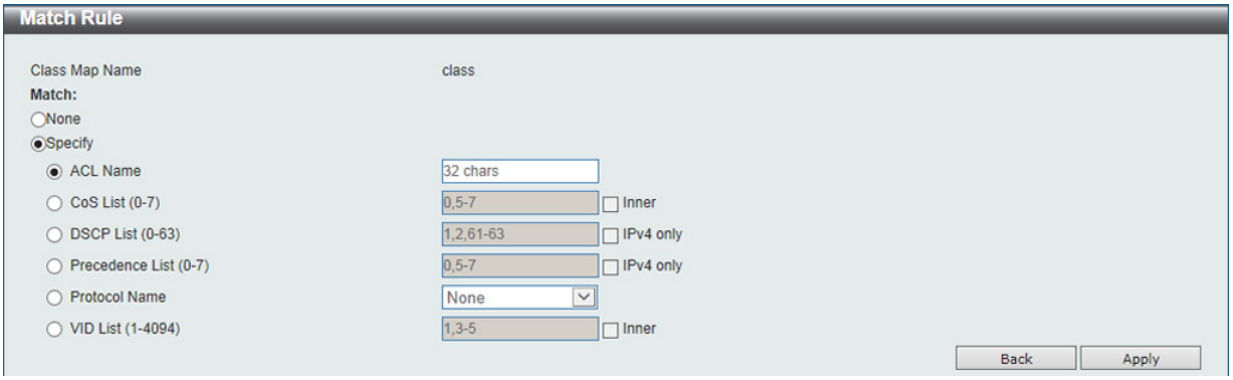


図 10-13　Class Map（Match）- Match Rule 画面

画面に表示される項目：

項目	説明
None	このクラスマップでは照合を行いません。
Specify	このクラスマップでは下記のいずれかのオプションで照合を行います。 • 「ACL Name」- クラスマップで照合するアクセスリスト名を指定します。（32 文字以内） • 「CoS List」- クラスマップで照合する CoS リスト値を指定します。「Inner」を指定すると、レイヤ 2 CoS マーキングの QinQ パケット内のインナモースト CoS を照合します。 - 設定可能範囲：0-7 • 「DSCP List」- クラスマップで照合する DSCP リスト値を指定します。「IPv4 only」にチェックを入れると、IPv4 パケットのみ照合します。チェックを入れない場合、IPv4/v6 両方のパケットを照合します。 - 設定可能範囲：0-63 • 「Precedence List」- クラスマップで照合する Precedence リスト値を指定します。「IPv4 only」にチェックを入れると、IPv4 パケットのみ照合します。チェックを入れない場合、IPv4/v6 両方のパケットを照合します。IPv6 パケットの場合、IPv6 ヘッダに含まれるトラフィッククラスの上位 3 ビットが Precedence になります。 - 設定可能範囲：0-7 • 「Protocol Name」- クラスマップで照合するプロトコル名を指定します。 - 選択肢：「None」「ARP」「BGP」「DHCP」「DNS」「EGP」「FTP」「IPv4」「IPv6」「NetBIOS」「NFS」「NTP」「OSPF」「PPPOE」「RIP」「RTSP」「SSH」「Telnet」「TFTP」 • 「VID List」- クラスマップで照合する VLAN リスト値を指定します。「Inner」を指定すると、802.1Q ダブルタグフレームのインナモースト VLAN ID と照合します。 - 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Aggregate Policer（アグリゲートポリサー設定）

本スイッチにおけるアグリゲートポリサーの設定と表示を行います。

QoS > Advanced Settings > Aggregate Policer の順にメニューをクリックし、以下の画面を表示します。

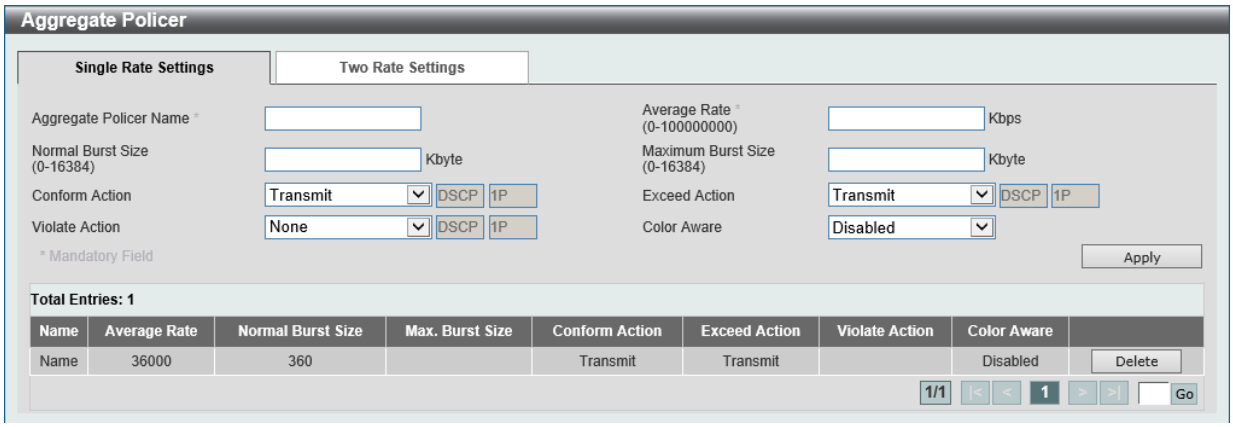


図 10-14　Aggregate Policer 画面 - Single Rate Settings タブ

画面に表示される項目：

項目	説明
Aggregate Policer Name	アグリゲートポリサー名を入力します。
Average Rate	平均レート値を入力します。 • 設定可能範囲：0-100000000（kbps）
Normal Burst Size	ノーマルバーストサイズを入力します。 • 設定可能範囲：0-16384（Kbytes）
Maximum Burst Size	最大バーストサイズを入力します。 • 設定可能範囲：0-16384（Kbytes）
Confirm Action	緑色パケットに対するアクションを指定します。 •「Drop」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p ユーザプライオリティ 値でパケットを送信します。 •「Transmit」- パケットはそのまま送信されます。（初期値） •「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Exceed Action	レート制限を超えたパケットに対するアクションを指定します。 •「Drop」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p ユーザプライオリティ 値でパケットを送信します。 •「Transmit」- パケットはそのまま送信されます。 •「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Violate Action	シングルレートポリシングにおけるノーマルおよび最大バーストサイズを超えたパケットに対するアクションを指定します。「CIR」や「PIR」を順守しないパケットの動作を指定します。 •「None」- アクションは実行されません。 •「Drop」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（ DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p ユーザプライオリティ 値で送信します。 •「Transmit」- パケットはそのまま送信されます。 •「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Color Aware	Color Aware オプションを有効 / 無効に指定します。 •「Enabled」- ポリサーは Color-Aware モードで動作します。 •「Disabled」- ポリサーは Color-Blind モードで動作します。（初期値）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

「Two Rate Setting」タブをクリックすると次のページが表示されます。

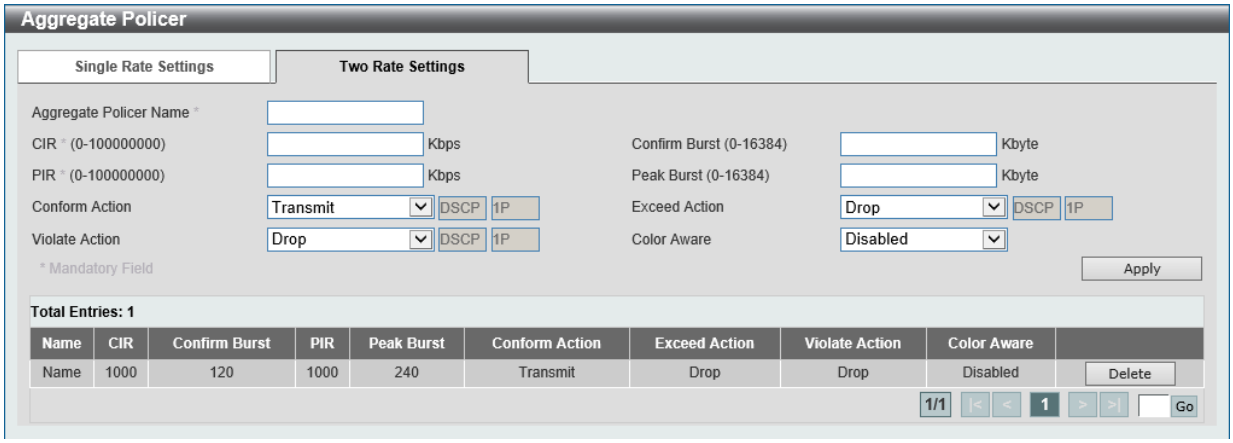


図 10-15　Aggregate Policer 画面 - Two Rate Settings タブ

画面に表示される項目：

項目	説明
Aggregate Policer Name	アグリゲートポリサー名を入力します。
CIR	CIR（Committed Information Rate）値を入力します。 • 設定可能範囲：0-100000000（kbps） この保証パケットレートは、２レートメータリングにおける最初のトークンバケットになります。
Confirm Burst	バーストサイズを入力します。 • 設定可能範囲：0-16384（Kbytes） Confirm Burst は、最初のトークンバケットのバーストサイズ（kbps）になります。
PIR	PIR（Peak Information Rate）値を入力します。 • 設定可能範囲：0-100000000（kbps） PIR は、２レートメータリングにおける二つ目のトークンバケットになります。
Peak Burst	ピークバースト値を入力します。 • 設定可能範囲：0-16384（Kbytes） ピークバーストサイズは、二つ目のトークンバケットのバーストサイズになります。
Confirm Action	ここでは緑色パケットに対するアクションを指定します。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。（初期値） • 「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Exceed Action	レート制限を超えたパケットに対するアクションを指定します。 • 「Drop」- パケットを破棄します。（初期値） • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Violate Action	シングルレートポリシングにおけるノーマルおよび最大バーストサイズを超えたパケットに対するアクションを指定します。「CIR」や「PIR」を順守しないパケットの動作を指定します。 • 「Drop」- パケットを破棄します。（初期値） • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値を設定して、新しい 802.1p ユーザプライオリティ 値で送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- IP DSCP 値と 802.1p ユーザプライオリティ 値を入力します。
Color Aware	Color Aware オプションを有効 / 無効に指定します。 • 「Enabled」- ポリサーは Color-Aware モードで動作します。 • 「Disabled」- ポリサーは Color-Blind モードで動作します。（初期値）

「Apply」ボタンをクリックして、設定内容を適用します。

Policy Map（ポリシーマップ設定）

本スイッチにおけるポリシーマップの設定と表示を行います。

QoS > Advanced Settings > Policy Map の順にメニューをクリックし、以下の画面を表示します。

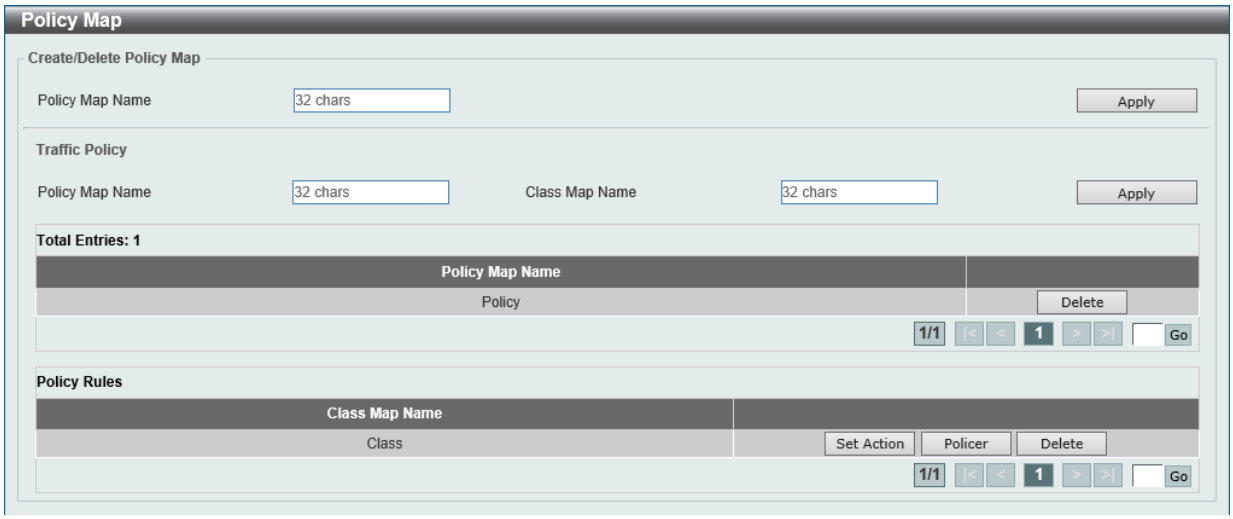


図 10-16　Policy Map 画面

本画面の「Create/Delete Policy Map」には以下の項目があります。

項目	説明
Create/Delete Policy Map	
Policy Map Name	作成 / 削除するポリシーマップ名を指定します。（32 文字以内）
Traffic Policy	
Policy Map Name	ポリシーマップ名を指定します。（32 文字以内）
Class Map Name	クラスマップ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

Class Map の編集

「Set Action」ボタンをクリックして、アクション設定を行います。
「Policer」ボタンをクリックして、ポリサー設定を行います。

ポリシーマップのエントリをクリックすると、画面下部にクラスマップが表示されます。「Set Action」ボタンをクリックし、以下の画面を表示します。

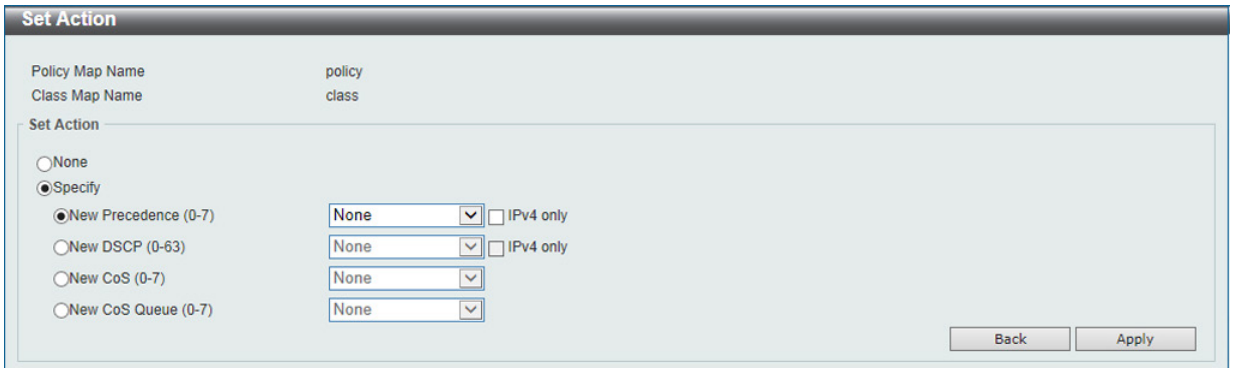


図 10-17　Policy Map（Set Action）画面

画面に表示される項目：

項目	説明
None	アクションを実行しません。

項目	説明
Specify	設定に基づきアクションを実行します。 • 「New Precedence」- 新しい Precedence 値を選択します。「IPv4 only」にチェックを入れると、IPv4 Precedence のみマークされます。チェックを入れない場合、IPv4/v6 両方の Precedence がマークされます。IPv6 パケットの場合、IPv6 ヘッダに含まれるトラフィッククラスの上位 3 ビットが Precedence になります。Precedence の設定は CoS キュー選択には影響しません。 - 選択肢：0-7 • 「New DSCP」- パケットの新しい DSCP 値を指定します。「IPv4 only」にチェックを入れると、IPv4 DSCP のみマークされます。チェックを入れない場合、IPv4/v6 両方の DSCP がマークされます。DSCP の設定は CoS キュー選択には影響しません。 - 選択肢：0-63 • 「New CoS」- パケットの新しい CoS 値を指定します。入力インタフェースにポリシーマップが適用されている場合、CoS 値の設定は CoS キュー選択に影響します。 - 選択肢：0-7 • 「New CoS Queue」- パケットの新しい CoS キュー値を指定します。元の CoS キュー選択は上書きされます。インタフェースの出力フローにポリシーマップが適用されている場合、CoS 値の設定は影響しません。 - 選択肢：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ポリシーマップのエントリをクリックすると、画面下部にクラスマップが表示されます。「Policer」ボタンをクリックし、以下の画面を表示します。

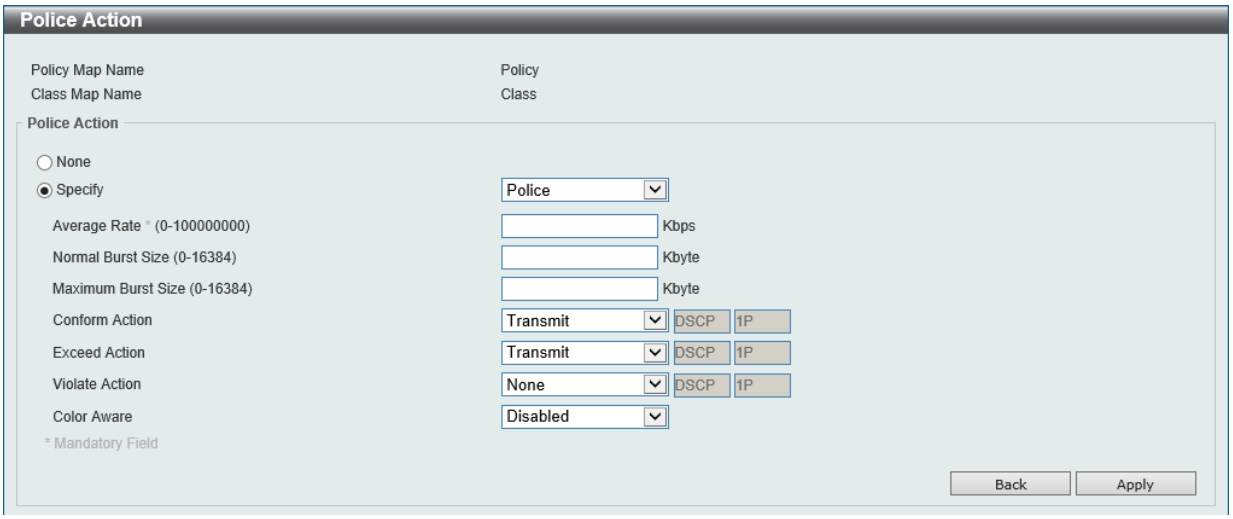


図 10-18　Policy Map（Police Action ）画面

画面に表示される項目：

項目	説明
None	このエントリにポリサー設定を指定しない場合に選択します。
Specify	このエントリにポリサー設定を指定する場合に選択します。 • 選択肢：「Police」「Police CIR」「Police Aggregate」
CIR	CIR 値を入力します。「Police CIR」を選択した場合に表示されます。
Confirm Burst	バーストサイズを入力します。「Police CIR」を選択した場合に表示されます。
PIR	PIR 値を入力します。「Police CIR」を選択した場合に表示されます。
Peak Burst	ピークバーストサイズを入力します。「Police CIR」を選択した場合に表示されます。
Average Rate	平均レート値を入力します。「Police」を選択した場合に表示されます。 • 設定可能範囲：0-100000000（Kbps）
Normal Burst Size	ノーマルバーストサイズを入力します。「Police」を選択した場合に表示されます。 • 設定可能範囲：0-16384（Kbyte）
Maximum Burst Size	最大バーストサイズを入力します。「Police」を選択した場合に表示されます。 • 設定可能範囲：0-16384（Kbyte）
Confirm Action	適合パケットに対するアクションを指定します。「Police」または「Police CIR」を選択した場合に表示されます。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値 を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- DSCP と 802.1p 値を設定して、新しい DSCP と 802.1p 値でパケットを送信します。

項目	説明
Exceed Action	超過パケットに対するアクションを指定します。「Police」または「Police CIR」を選択した場合に表示されます。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値 を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- DSCP と 802.1p 値を設定して、新しい DSCP と 802.1p 値でパケットを送信します。
Violate Action	違反パケットに対するアクションを指定します。「Police」または「Police CIR」を選択した場合に表示されます。 • 「None」- アクションを実行しません。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 802.1p ユーザプライオリティ 値 を設定して、新しい 802.1p 値でパケットを送信します。 • 「Transmit」- パケットはそのまま送信されます。 • 「Set-DSCP-1P」- DSCP と 802.1p 値を設定して、新しい DSCP と 802.1p 値でパケットを送信します。
Color Aware	Color Aware オプションを有効 / 無効に指定します。「Police」または「Police CIR」を選択した場合に表示されます。 • 「Enabled」- ポリサーは Color-Aware モードで動作します。 • 「Disabled」- ポリサーは Color-Blind モードで動作します。
Aggregate Policer Name	集約ポリサー名を入力します。「Police Aggregate」を選択した場合に表示されます。

「Apply」ボタンをクリックして、設定内容を適用します。

Policy Binding（ポリシーバインディング設定）

ポリシーバインディング設定を行います。

QoS > Advanced Settings > Policy Binding の順にメニューをクリックし、以下の画面を表示します。

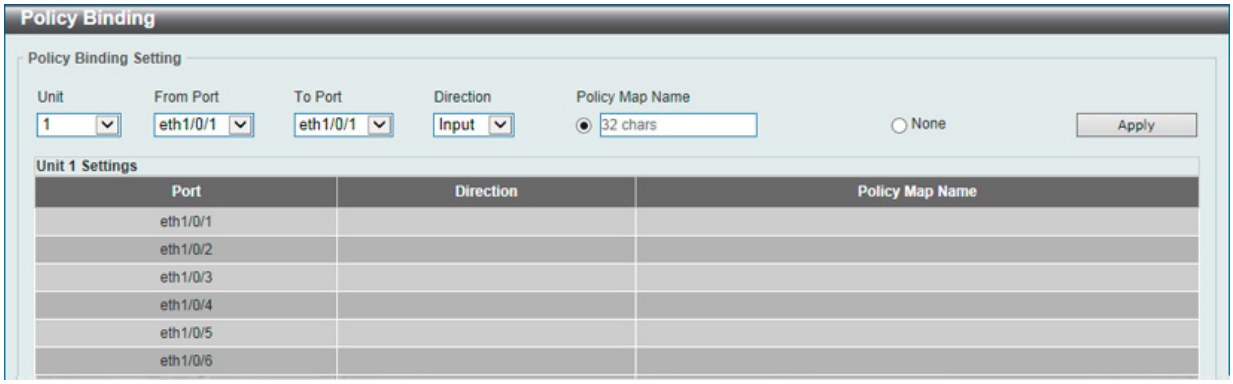


図 10-19　Policy Binding 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Direction	トラフィックの方向を指定します。 • 選択肢「Input（イングレス）」「Output（イーグレス）」
Policy Map Name	ポリシーマップ名を指定します。（32 文字以内）「None」を選択すると本エントリにポリシーマップは関連付けられません。

「Apply」ボタンをクリックして、設定内容を適用します。

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。

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。

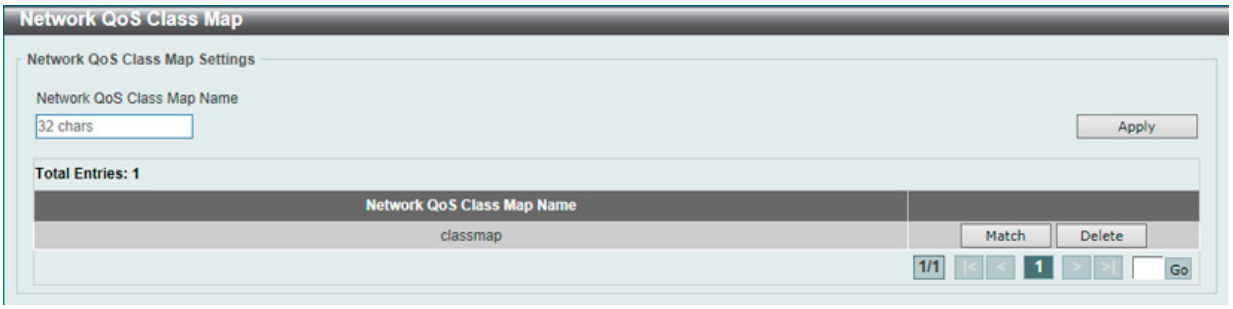


図 10-20　Network QoS Class Map 画面

画面に表示される項目：

項目	説明
Network QoS Class Map Name	トラフィックポリシーに適用するネットワーク QoS クラスマップ名（32 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Match」ボタンをクリックして、指定のエントリのマッチルール設定を行います。
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。

「Match」をクリックすると、以下の画面が表示されます。

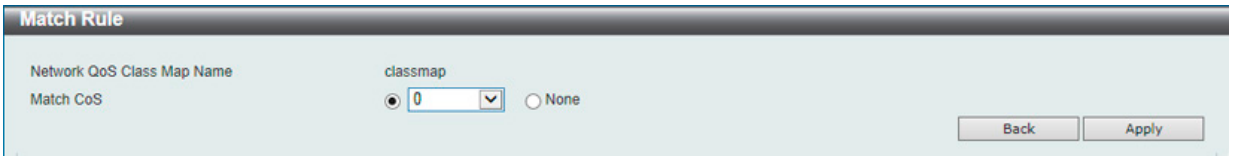


図 10-21　Network QoS Class Map (Match) - Match Rule 画面

画面に表示される項目：

項目	説明
Match CoS	照合する IEEE 802.1Q Class of Service (CoS) 値を指定します。パケットを受信すると、このパケットにインターナル CoS が付与されます。このインターナル CoS を使用して、CoS- キューマッピングに基づいた送信キューが選択されます。CoS キューの値が大きいほど、優先度が高くなります。「None」を選択すると、CoS 値による照合を無効にします。 • 選択肢：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Network QoS Policy Map（ネットワーク QoS ポリシーマップ）

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。

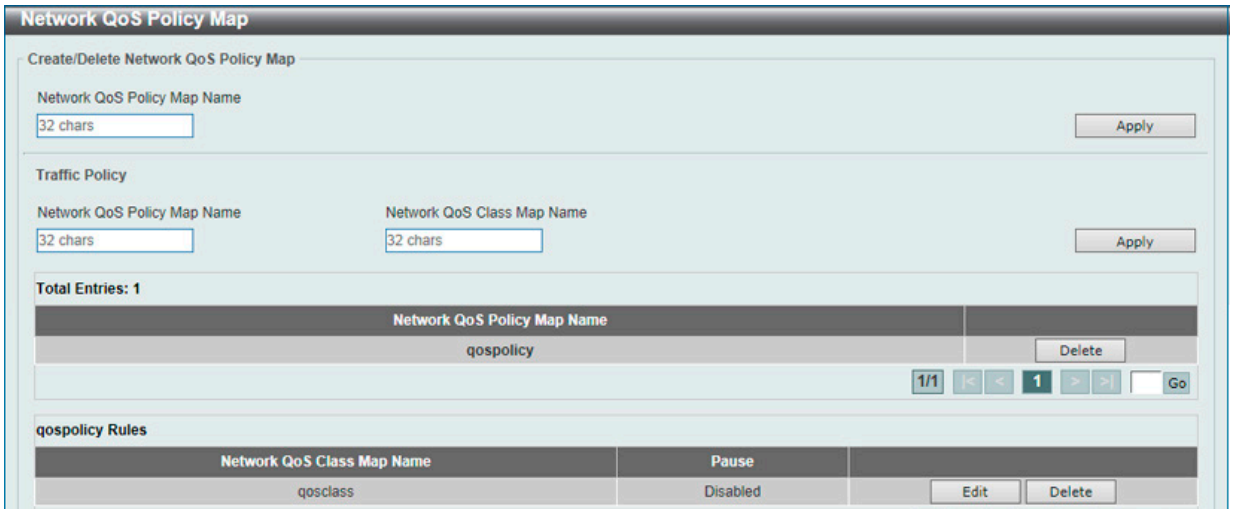


図 10-22　Network QoS Policy Map 画面

画面に表示される項目：

項目	説明
Create/Delete Network QoS Policy Map	
Network QoS Policy Map Name	作成 / 削除するネットワーク QoS ポリシーマップ名（32 文字以内）を指定します。
Traffic Policy	
Network QoS Policy Map Name	クラスマップに関連付けるネットワーク QoS ポリシーマップ名（32 文字以内）を指定します。
Network QoS Class Map Name	ポリシーマップに関連付けるネットワーク QoS クラスマップ名（32 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

ポリシーマップのエントリをクリックすると、画面下部にルールが表示されます。「Edit」をクリックし、以下の画面で指定エントリの編集を行います。

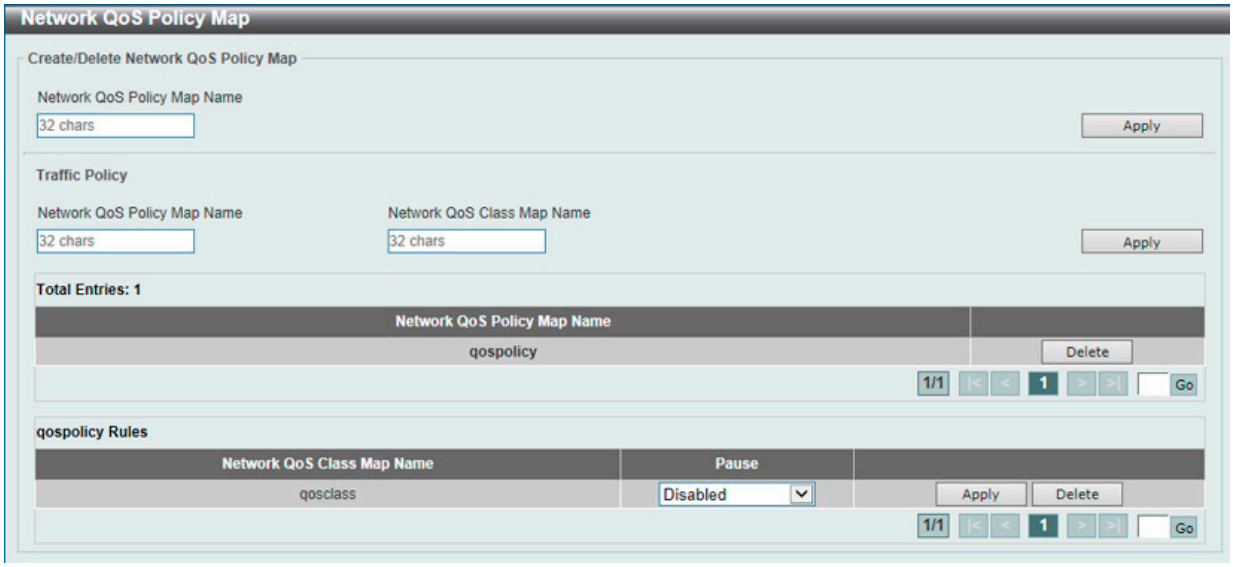


図 10-23　Network QoS Policy Map (Edit) 画面

画面に表示される項目：

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 ポリシーマップで参照されるクラスのPFC を有効にします。

「Apply」ボタンをクリックして、設定内容を適用します。

Network QoS Policy Binding（ネットワーク QoS ポリシーバインディング）

ネットワーク「Quality of Service」(QoS) ポリシーのバインディング設定、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。

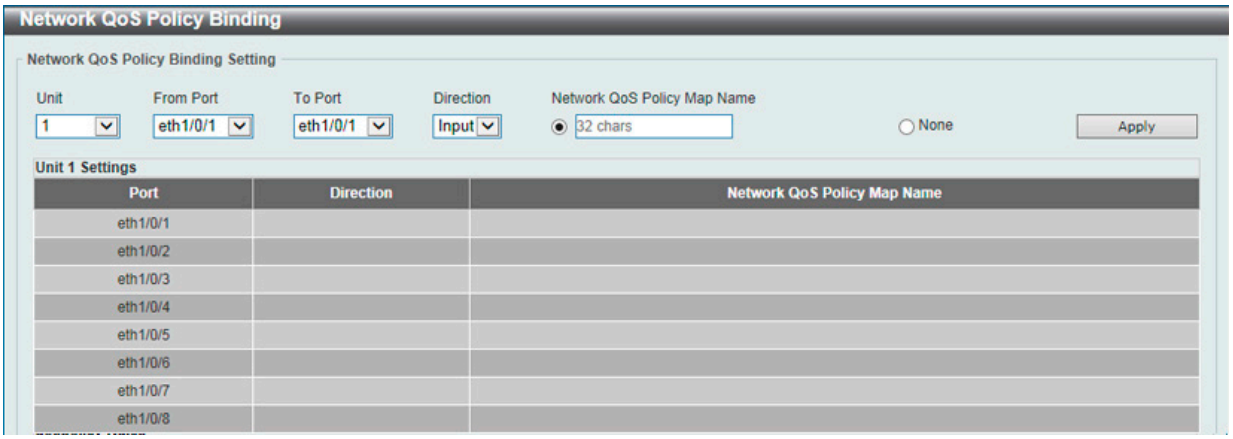


図 10-24　Network QoS Policy Binding 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Direction	「Input」を指定します。インタフェース上のイングレスフローに対してポリシーマップを適用します。
Network QoS Policy Map Name	ネットワーク QoS ポリシーマップ名 (32 文字以内) を指定します。「None」を選択すると、ネットワーク QoS ポリシーマップへの関連付けを行いません。

「Apply」ボタンをクリックして、設定内容を適用します。

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。

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。

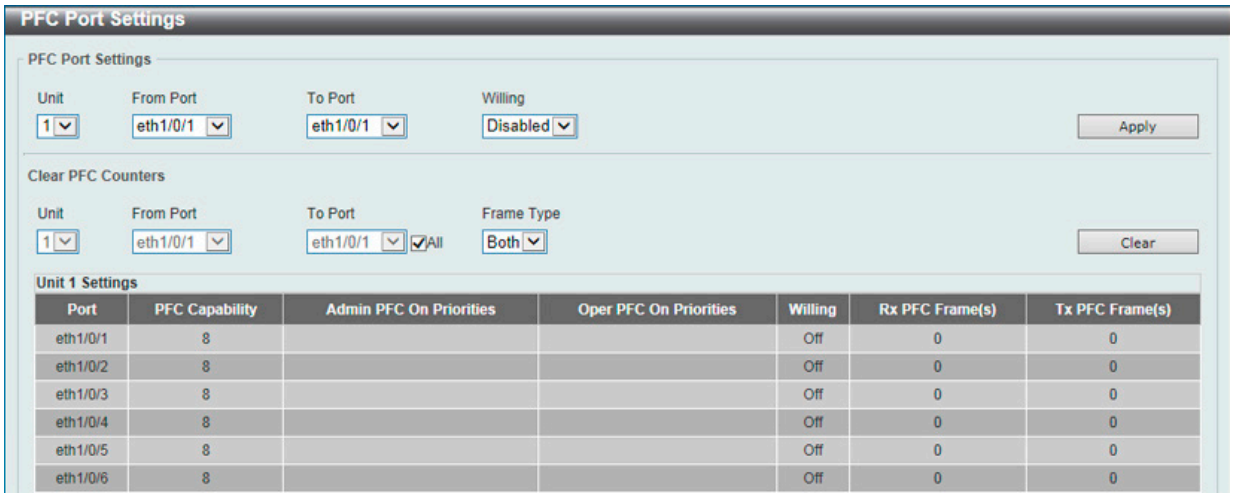


図 10-25　PFC Port Settings 画面

画面に表示される項目：

項目	説明
PFC Port Settings	
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Willing	「Willing」機能を有効/無効に指定します。「Data Center Bridging Exchange Protocol」(DCBX) PFC の 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	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Frame Type	クリアするフレームタイプを指定します。 • 「RX」- 受信した PFC フレームのカウンタをクリアします。 • 「TX」- 送信された PFC フレームのカウンタをクリアします。 • 「Both」- 送受信された PFC フレームのカウンタをクリアします。

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、指定した情報を基にカウンタをクリアします。

WRED（WRED 設定）

重み付けランダム早期検出（WRED）は、QoS キューの全体的なスループットを向上させる QoS 機能の 1 つです。この方式では、スイッチに設定された QoS の出力キューに基づいて、パケットと QoS キューを分析し、QoS キューに入るパケットにオーバーフローが発生しているかどうかを判断し、ランダムにパケットを破棄してキューへのパケットフローを最小化します。

WRED は、QoS キュー内の輻輳を回避する 2 つの方法を採用しています。

- 各 QoS キューには、パケットを受け入れる最小レベルと最大レベルが設定されます。キューの最大しきい値に達すると、スイッチはすべての入力パケットの破棄を開始します。これにより、QoS に割り当てられた帯域幅を最小化します。最小しきい値を下回ると、スイッチはすべての入力パケットを受け入れます。

- 入力パケットが最大キューと最小キューの範囲内にある場合、スイッチはスロープ確率関数を使用し、キューが最大しきい値に達した際の破棄確率を決める最大破棄レートに基づき、ランダムなパケット破棄方法を決定します。キューが最大しきい値に近い場合、スイッチはランダムパケットの廃棄を増やしてキューへのフローを均等にし、優先度の高いキューへのオーバーフローを回避します。

WRED Profile（WRED プロファイル設定）

WRED プロファイル設定を行います。

QoS > WRED > WRED Profile の順にメニューをクリックし、以下の画面を表示します。

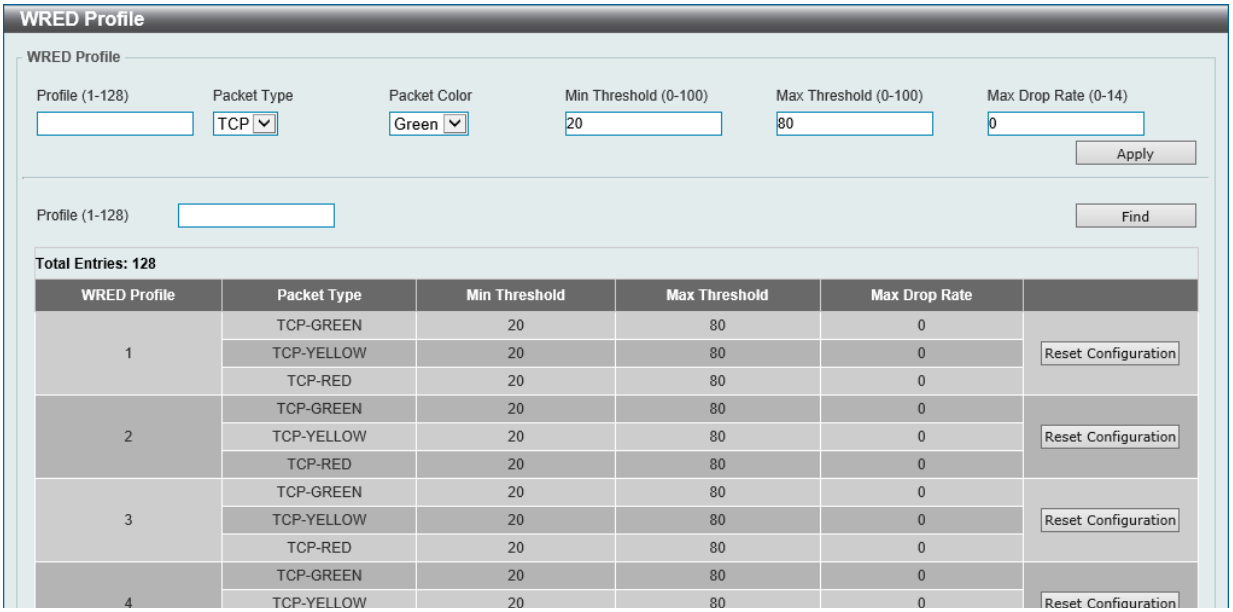


図 10-26　WRED Profile 画面

画面に表示される項目：

項目	説明
Profile	WRED プロファイル ID を入力します。 • 設定可能範囲：1-128
Packet Type	パケットタイプを TCP に指定します。
Packet Color	パケットカラーを選択します。 • 「Green」- 緑のパケットの WRED 破棄パラメータを設定します。 • 「Yellow」- 黄色のパケットの WRED 破棄パラメータを設定します。 • 「Red」- 赤のパケットの WRED 破棄パラメータを設定します。
Min Threshold	WRED 破棄を開始する最小しきい値を入力します。 • 設定可能範囲：0-100
Max Threshold	最大しきい値を入力します。このしきい値を超えると、WRED により、キュー宛てのすべてのパケットが破棄されます。 • 設定可能範囲：0-100
Max Drop Rate	破棄レートの最大値を入力します。平均キューサイズが最大しきい値に達したときの破棄レートを指定します。この値が「0」の場合、パケットは破棄されないか、ECN に対して再マーキングされません。 • 設定可能範囲：0-14

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Reset Configuration」ボタンをクリックして、指定エントリの設定をリセットします。

WRED Queue（WRED キュー設定）

WRED のキュー設定を行います。
WRED は指定のしきい値を超えた平均キューサイズに基づいてパケットを破棄します。「Explicit Congestion Notification」(ECN) は WRED の拡張機能であり、平均キューサイズが指定しきい値を超えた際に、パケットを破棄する代わりに ECN マークが付与されます。WRED ECN 機能を使用すると、ネットワークの輻輳とパケットの送信遅延を示す信号として、ルータやエンドホストによって ECN マークが使用されます。

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。

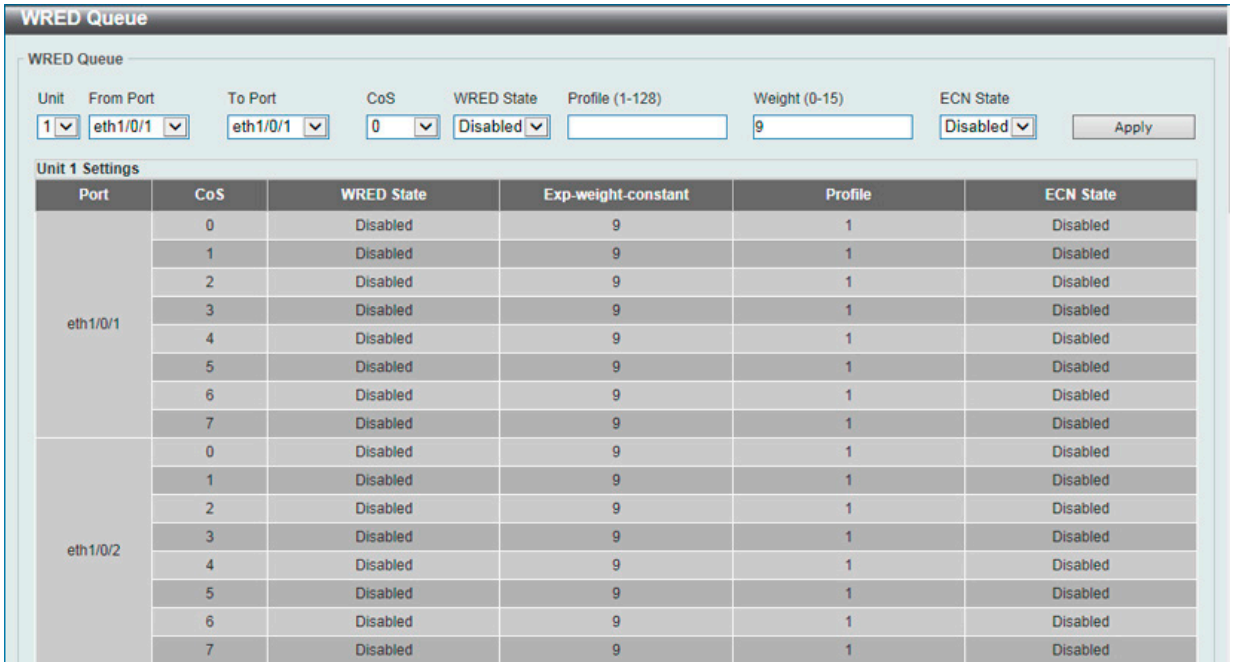


図 10-27　WRED Queue 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
CoS	CoS 値を指定します。 • 設定可能範囲：0-7
WRED State	指定ポートの WRED 機能を有効 / 無効に設定します。
Profile	WERD プロファイル ID を指定します。 • 設定可能範囲：1-128
Weight	平均キューサイズ計算に使用される WRED 重み係数を指定します。 • 設定可能範囲：0-15
ECN State	指定ポートの ECN 機能を有効 / 無効に指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

WRED Drop Counter（WRED ドロップカウンタ設定）

WRED のドロップカウンタを表示、クリアします。

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 10-28　WRED Drop Counter 画面

画面に表示される項目：

項目	説明
Unit	カウンタをクリアするユニットを指定します。
From Port / To Port	カウンタをクリアするポート範囲を指定します。

「Clear」ボタンをクリックして、指定ユニット / ポートのカウンタをクリアします。
「Clear All」ボタンをクリックして、すべてのカウンタをクリアします。

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 プロトコルを使用したパケットのスヌーピングによる、iSCSI セッションおよび通信の確立 / 終了の検出。
- 現在アクティブな iSCSI セッションおよび接続のデータベースの保持と、参加者に関するデータの保存。これにより、セッションのデータパケットに対し、目的の QoS 処理のためのルール分類が可能になります。
- iSCSI セッショントラフィックの必要に応じて分類子ルールセットを設定または削除します。
- セッション終了パケットが受信されない場合に、セッションエントリをエージアウトできるように、iSCSI セッションでのアクティビティを監視します。

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。

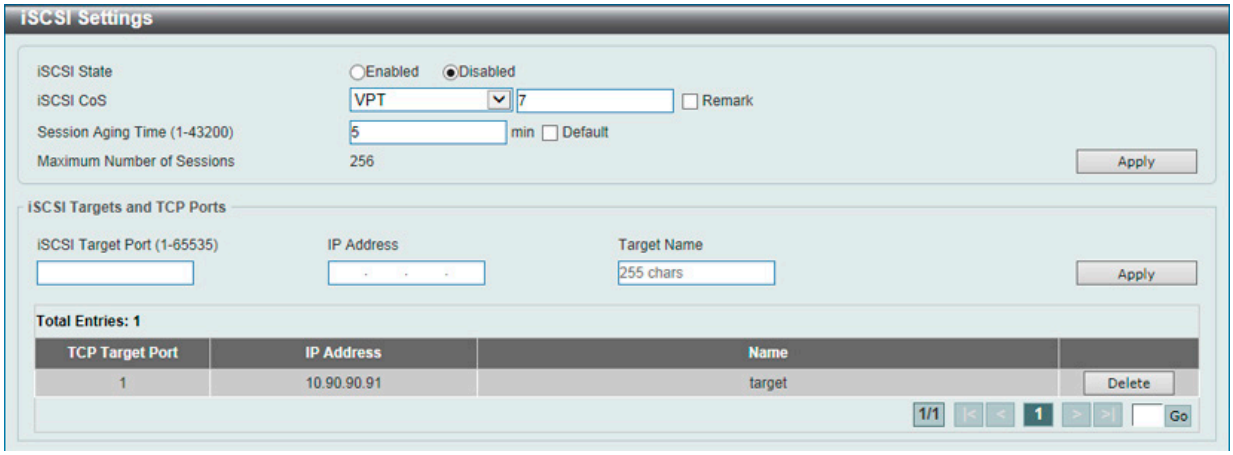


図 10-29　iSCSI Settings 画面

画面に表示される項目：

項目	説明
iSCSI State	
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への割り当てで使用する「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への割り当てで使用する「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。 「Remark」オプションを選択すると、イーグレスパケットについて、指定の VPT または DSCP を持つ iSCSI フレームをマークします。
Session Aging Time	セッションエージングタイム値を入力します。iSCSI セッションのエージングタイムを設定するために使用されます。エージングタイムを現在の設定より長く設定すると、現在のセッションはタイムアウトになり、新しいエージングタイムが使用されます。エージングタイムを現在の設定より短く設定すると、新しいエージングタイムより長いセッションは削除され、新しいエージングタイム以下のセッションは新しい設定で引き続き監視されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-43200（分） • 初期値：5（分）
iSCSI Targets and TCP Ports	
iSCSI Target Port	iSCSI ターゲットポート番号を指定します。 • 設定可能範囲：1-65535
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（255 文字以内）を指定します。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、新しいセッションまたは接続の最初のログイン要求で接続するために、iSCSI イニシエータ名と iSCSI ターゲット名の両方を提示する必要があります。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
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 のアクティブな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 10-30　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 設定ウィザードを使用して、アクセスプロファイルと ACL ルールの新規作成・更新を行います。
ACL Access List（ACL アクセスリスト）	ACL アクセスリストの設定を行います。
ACL Interface Access Group（ACL インタフェースアクセスグループ）	ACL インタフェースアクセスグループの設定を行います。
ACL VLAN Access Map（ACL VLAN アクセスマップ）	ACL VLAN アクセスマップの設定を行います。
ACL VLAN Filter（ACL VLAN フィルタ設定）	ACL VLAN フィルタの設定を行います。
CPU ACL（CPU ACL 設定）	CPU インタフェースフィルタリング機能の設定を行います。

ACL 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。

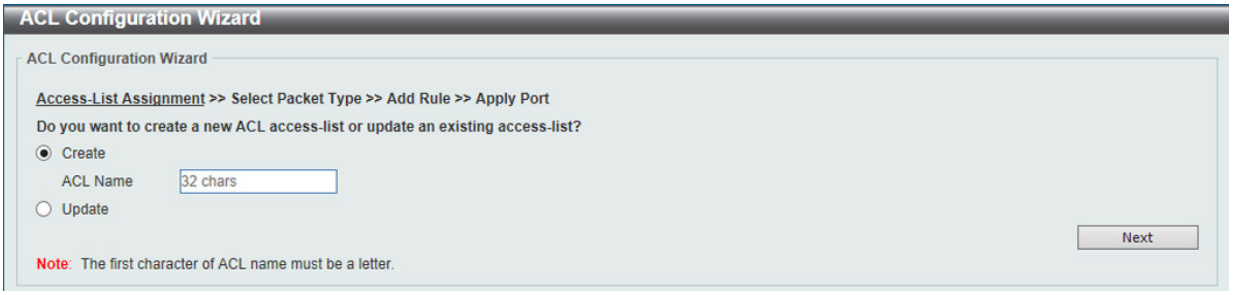


図 11-1　ACL Configuration Wizard（Access-List Assignment - Create) 画面

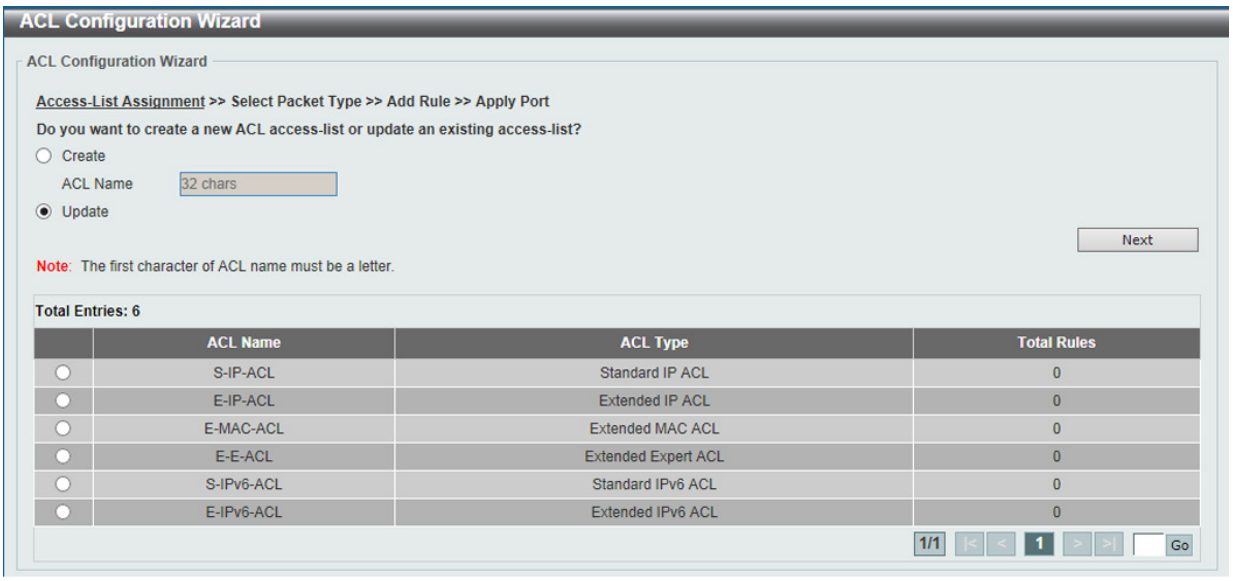


図 11-2　ACL Configuration Wizard（Access-List Assignment - Update) 画面

画面に表示される項目：

項目	説明
Create	新しいアクセスルールを作成する場合は、「Create」を選択します。
ACL Name	作成する ACL 名を指定します。（32 文字以内）
Update	既存の ACL アクセスリストを表示し、エントリを再設定する場合に選択します。

「Next」ボタンをクリックし、パケットタイプの選択を行います。

パケットタイプ選択（ACL 設定ウィザード）

「ACL Configuration Wizard」にて作成する ACL エントリ名を指定した後、パケットタイプを指定します。本画面は、新規作成時のみ表示されます。

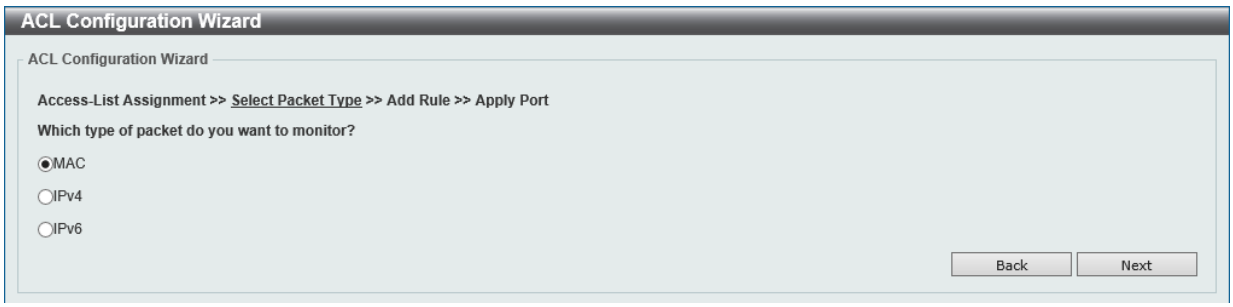


図 11-3　ACL Configuration Wizard（Select Packet Type) 画面

画面に表示される項目：

項目	説明
MAC	MAC ACL を作成します。
IPv4	IPv4 ACL を作成します。
IPv6	IPv6 ACL を作成します。

「Next」ボタンをクリックします。
選択したパケットの種類により次に表示される画面が異なります。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 ACL を作成・更新する場合、以下の画面が表示されます。

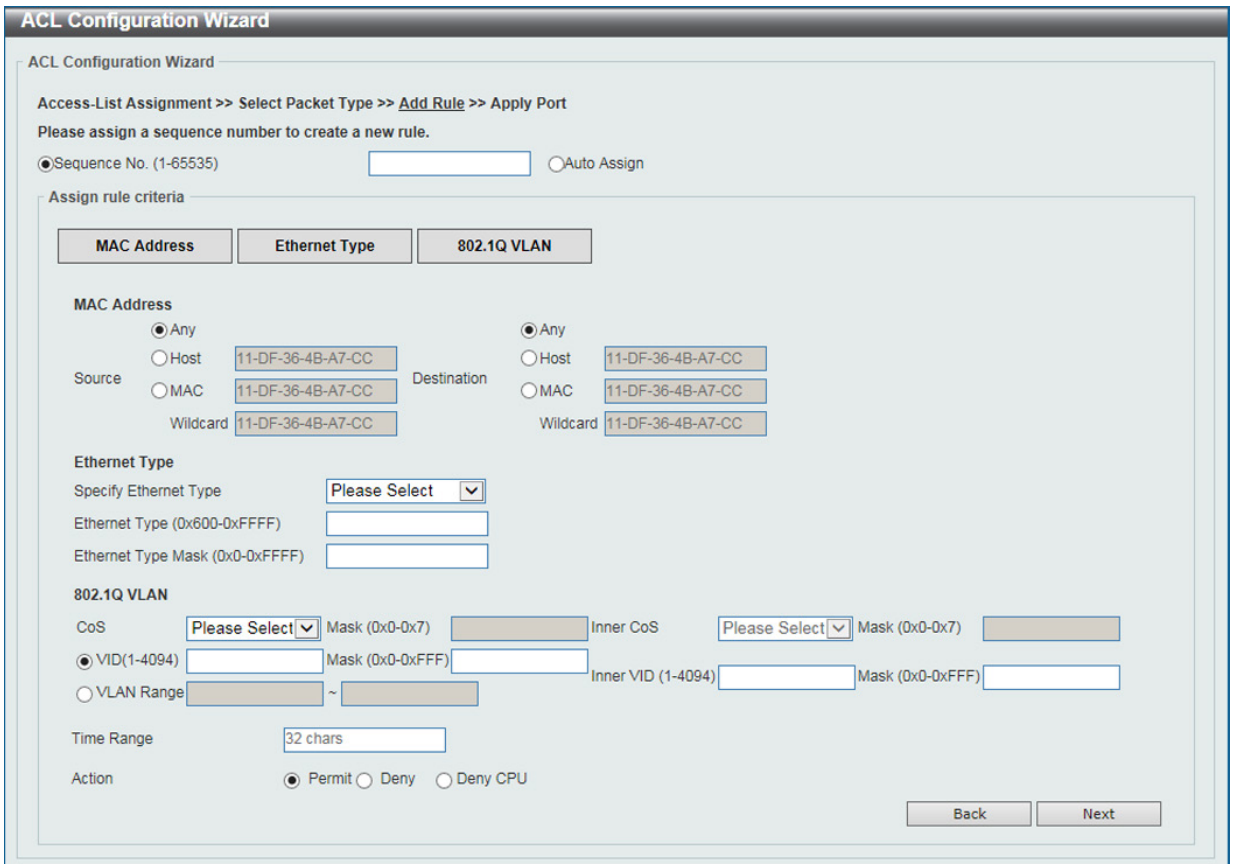


図 11-4　ACL Configuration Wizard 画面（Extended MAC ACL）

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Assign Rule Criteria（ルール条件の割り当て）	
MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力することができます。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
Ethernet Type	
Specify Ethernet Type	イーサネットタイプを選択します。 • 選択肢:「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
Ethernet Type	イーサネットタイプの 16 進数値を 0x0 から 0xFFFF の間で指定します。「Specify Ethernet Type」で指定したイーサネットタイプに基づき、自動的に適切な値が入力されます。
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。「Specify Ethernet Type」で指定したイーサネットタイプに基づき、自動的に適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
802.1Q VLAN	
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：CoS マスクを入力します。（0x0-0x7）
Inner CoS	CoS 値を指定後、Inner CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：Inner CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）
Inner VID	ACL ルールに紐づける Inner VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
VLAN Range	ACL ルールに紐づける VLAN 範囲を指定します。VLAN 範囲の開始 / 終了 VLAN を入力します。 • 設定可能範囲：1-4094
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」「Deny CPU（拒否 /CPU）」

「Next」ボタンをクリックします。
前の画面に戻るには、「Back」ボタンをクリックします。

IPv4 ACL Rule の設定

IPv4 ACL Rule を設定します。IPv4 ACL を作成・更新する場合、以下の画面が表示されます。

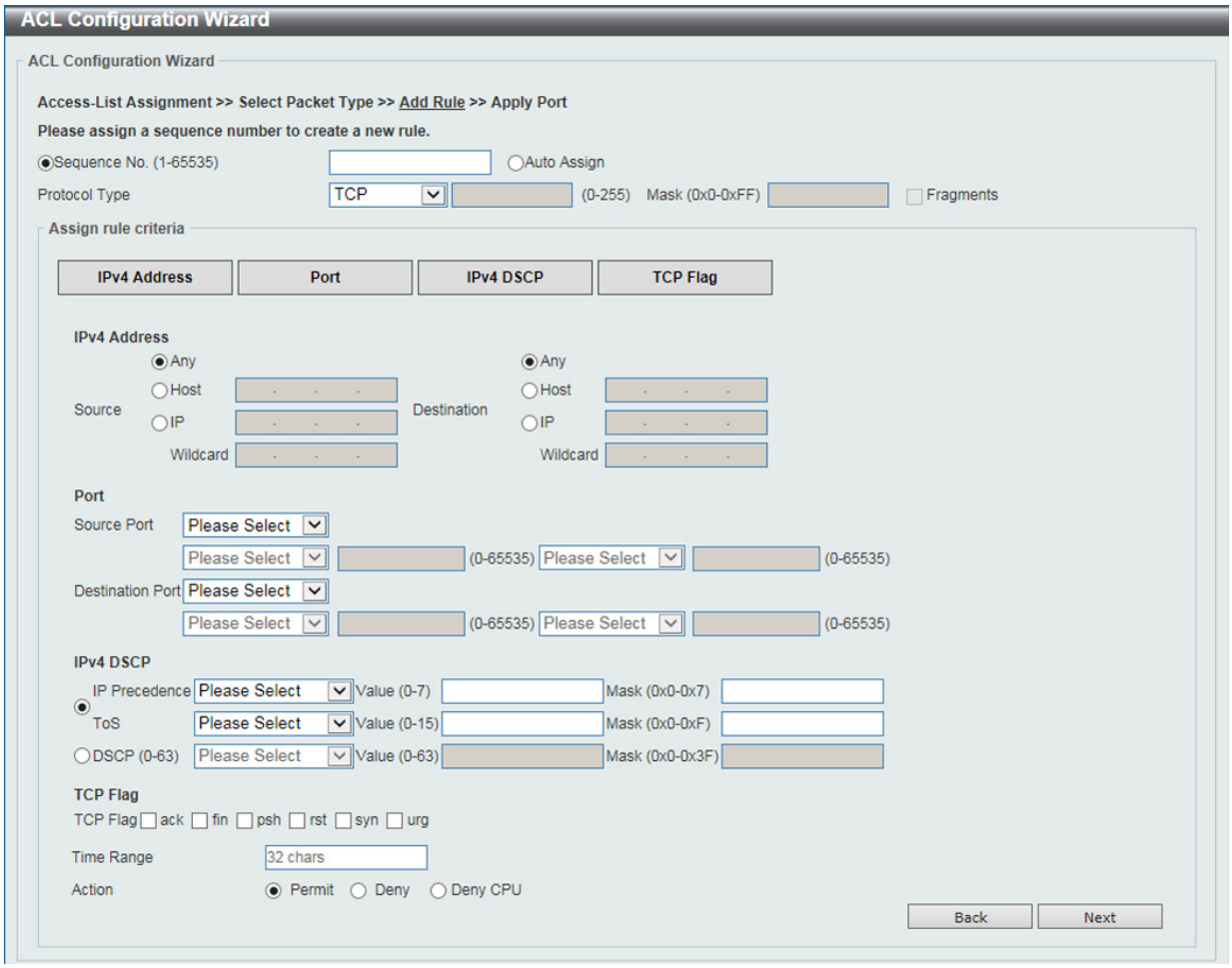


図 11-5　ACL Configuration Wizard 画面（Extended/Standard IPv4）

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Protocol Type（プロトコルタイプ）	
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（IPv4 ACL Rule）

項目	説明
IPv4 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「0 (routine)」「1 (priority)」「2（immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」 - 「Value」：IP 優先値を入力します。(0-7) - 「Mask」：IP 優先値マスクを入力します。(0x0-0x7)
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「4（max-throughput)」「8（min-delay)」 - 「Value」：ToS 値を入力します。(0-15) - 「Mask」：ToS マスクを入力します。(0x0-0xF)
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default（0)」「af11（10)」「af12（12)」「af13（14)」「af21（18)」「af22（20)」「af23（22)」「af31（26)」「af32（28)」「af33（30)」「af41（34)」「af42（36)」「af43（38)」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。(0-63) - 「Mask」：DSCP マスクを入力します。(0x0-0x3F)
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。(32 文字以内)
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可)」「Deny（拒否)」「Deny CPU（拒否 /CPU)」

「TCP」「UDP」選択時に表示される項目（IPv4 ACL Rule）

項目	説明
Port	
Source Port	送信元ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（IPv4 ACL Rule）

項目	説明
TCP Flag	
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（IPv4 ACL Rule）

項目	説明
ICMP	
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

IPv6 ACL Rule の設定

IPv6 ACL Rule を設定します。IPv6 ACL を作成・更新する場合、以下の画面が表示されます。

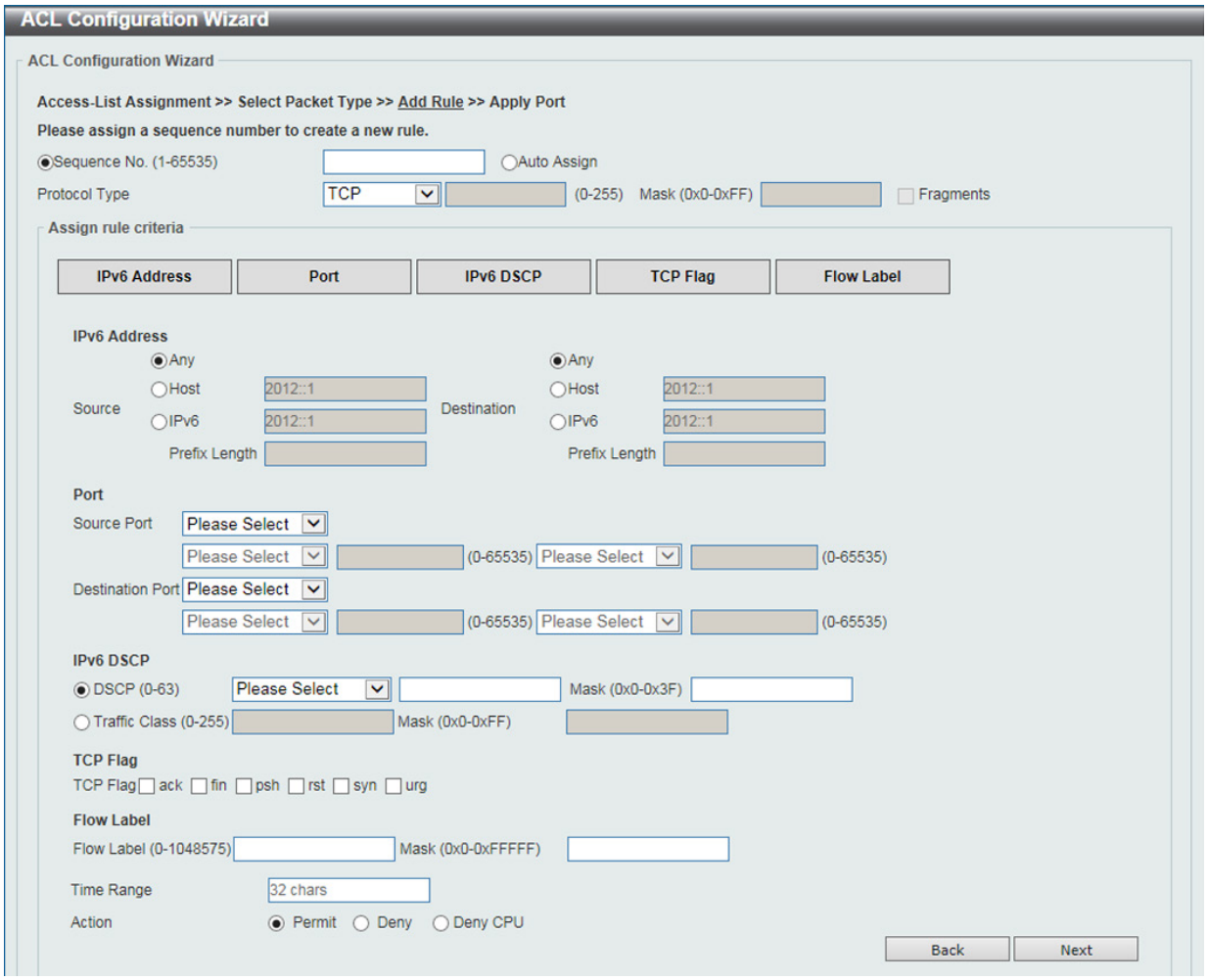


図 11-6　ACL Configuration Wizard 画面（Extended/Standard IPv6）

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Protocol Type（プロトコルタイプ）	
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「Protocol ID」「ESP」「RCP」「SCTP」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（IPv6 ACL Rule）

項目	説明
IPv6 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
IPv6 DSCP	
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。（0-63） - 「Mask」：DSCP マスクを入力します。（0x0-0x3F）
Traffic Class	トラフィッククラス値とトラフィッククラスのマスク値を入力します。 • 設定可能範囲：0-255 • 「Mask」：トラフィッククラスのマスクを入力します。（0x0-0xFF）
Flow Label	
Flow Label	フローラベルの値を入力します。 • 設定可能範囲：0-1048575 • 「Mask」：フローラベルマスクを入力します。（0x0-0xFFFFF）
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」「Deny CPU（拒否 /CPU）」

「TCP」「UDP」選択時に表示される項目（IPv6 ACL Rule）

項目	説明
Port	
Source Port	送信元ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（IPv6 ACL Rule）

項目	説明
TCP Flag	
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（IPv6 ACL Rule）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

Extended Expert ACL の設定

Extended Expert ACL Rule を設定します。Extended Expert ACL を更新する場合、以下の画面が表示されます。

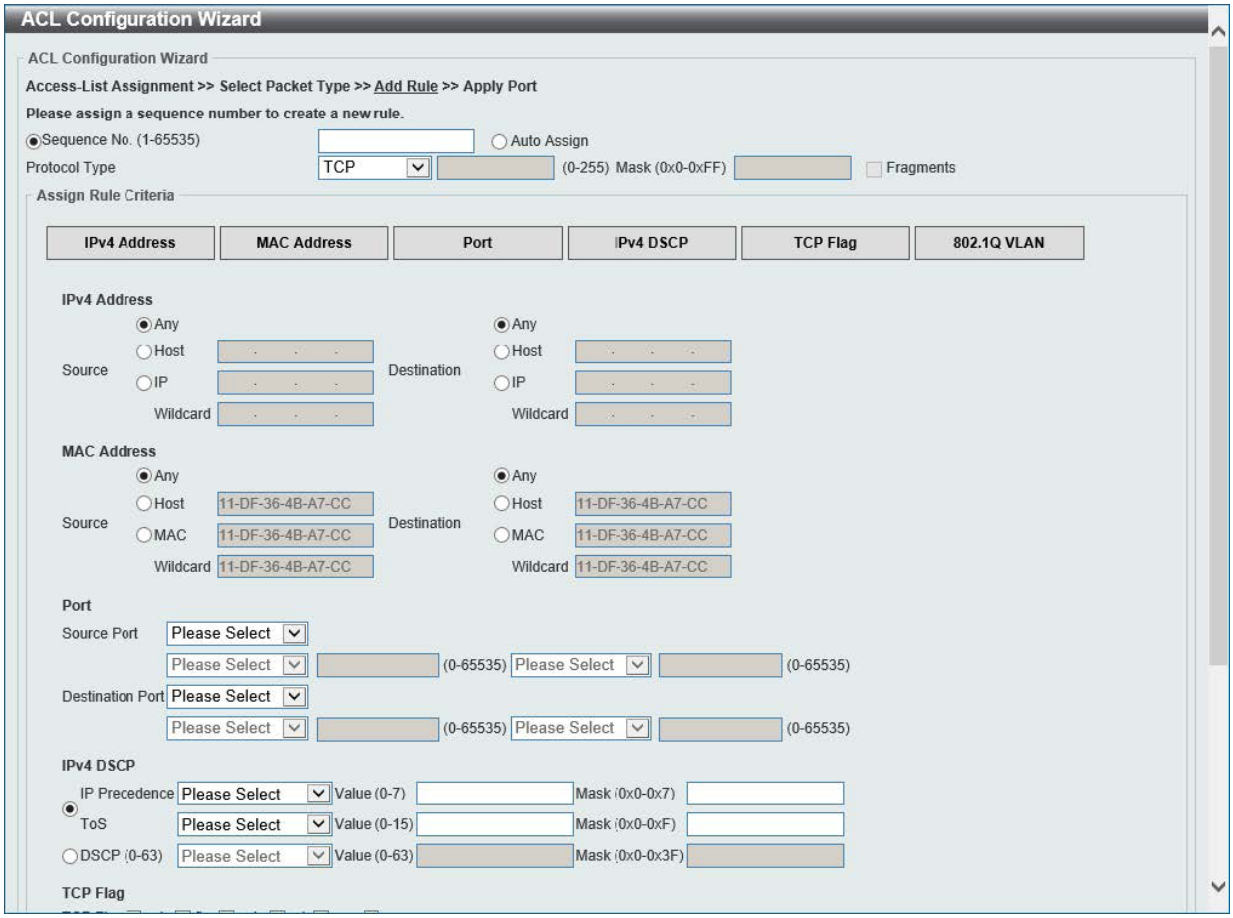


図 11-7　ACL Configuration Wizard（Extended Expert）画面

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Protocol Type（プロトコルタイプ）	
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「 Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

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
IPv4 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力することができます。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「0 (routine)」「1 (priority)」「2（immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」 - 「Value」：IP 優先値を入力します。(0-7) - 「Mask」：IP 優先値マスクを入力します。(0x0-0x7)
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「4（max-throughput)」「8（min-delay)」から指定できます。 - 「Value」：ToS 値を入力します。(0-15) - 「Mask」：ToS マスクを入力します。(0x0-0xF)
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。(0-63) - 「Mask」：DSCP マスクを入力します。(0x0-0x3F)
802.1Q VLAN	
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：CoS マスクを入力します。(0x0-0x7)
Inner CoS	Inner CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：Inner CoS マスクを入力します。(0x0-0x7)
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：VLAN ID マスクを入力します。(0x0-0xFFF)
Inner VID	ACL ルールに紐づける Inner VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：Inner VLAN ID マスクを入力します。(0x0-0xFFF)
VLAN Range	ACL ルールに紐づける VLAN 範囲（開始 VLAN/ 終了 VLAN）を入力します。 • 設定可能範囲：1-4094
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。(32 文字以内)
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可)」「Deny（拒否)」「Deny CPU（拒否 /CPU)」

「TCP」「UDP」選択時に表示される項目（Extended Expert ACL）

項目	説明
Source Port	送信元ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（Extended Expert ACL）

項目	説明
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（Extended Expert ACL）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

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。

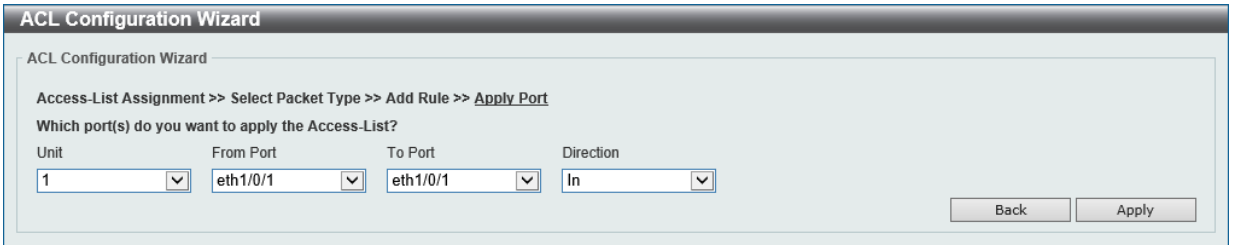


図 11-8　ACL Configuration Wizard (Apply Port) 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Direction	方向を指定します。 • 選択肢：「In」「Out」

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL Access List（ACL アクセスリスト）

アクセスコントロールリスト、ACL ルールの設定、表示を行います。

ACL > ACL Access List の順にメニューをクリックし、以下の画面を表示します。

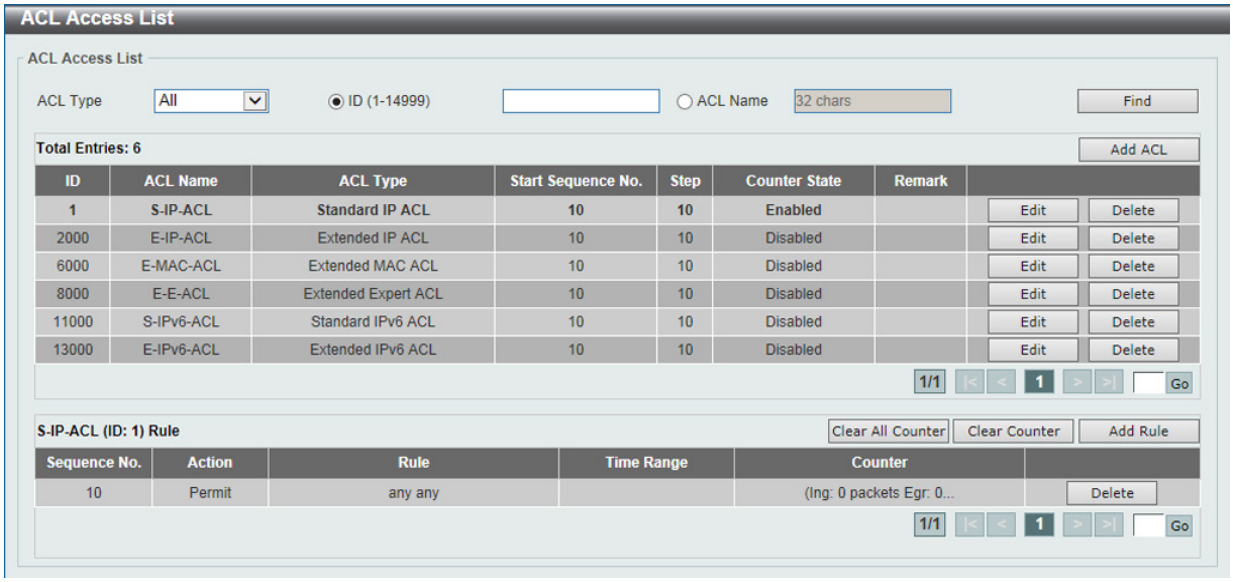


図 11-9　ACL Access List 画面

画面に表示される項目：

項目	説明
ACL Type	ACL プロファイルの種類を選択します。 • 選択肢：「All」「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」
ID	ACL ID を入力します。 • 設定可能範囲：1-14999
ACL Name	ACL 名を入力します。（32 文字以内）

「Find」ボタンをクリックし、入力した情報を基にエントリを検索します。
「Add ACL」ボタンをクリックして、新しい ACL プロファイルを作成します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Delete」ボタンをクリックして、指定のエントリを削除します。

ACL ルールの作成・カウンタ情報の削除
ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。
「Clear All Counter」ボタンをクリックして、表示されたすべてのカウンタ情報を消去します。
「Clear Counter」ボタンをクリックして、表示されたルールのカウンタ情報を消去します。

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」ボタンをクリックすると、以下の画面が表示されます。

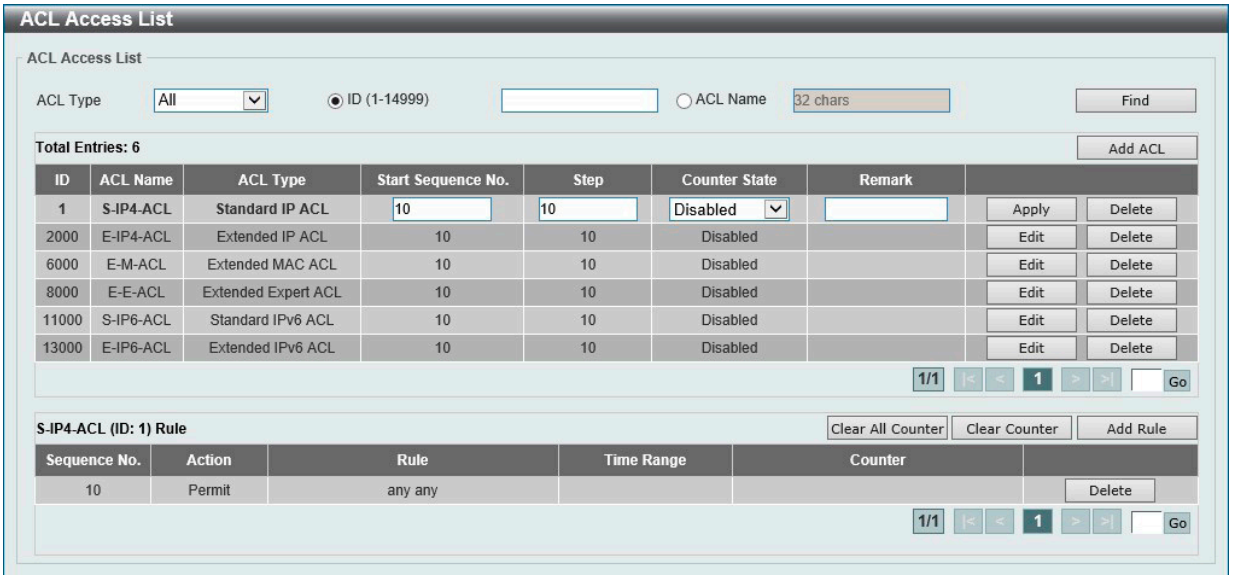


図 11-10　ACL Access List（Edit）画面

画面に表示される項目：

項目	説明
Start Sequence No.	シーケンスの開始番号を入力します。
Step	シーケンス番号のステップ（インクリメント）数を入力します。たとえば、シーケンスの開始番号が 20、ステップ値が 5 の場合、後続のシーケンス番号は 25、30、35、40 となります。 • 設定可能範囲：1-32 • 初期値：10
Counter State	カウンタ状態オプションを有効 / 無効に設定します。
Remark	ACL のオプション注釈を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

ACL プロファイルの作成

「Add ACL」ボタンをクリックすると、以下の画面が表示されます。

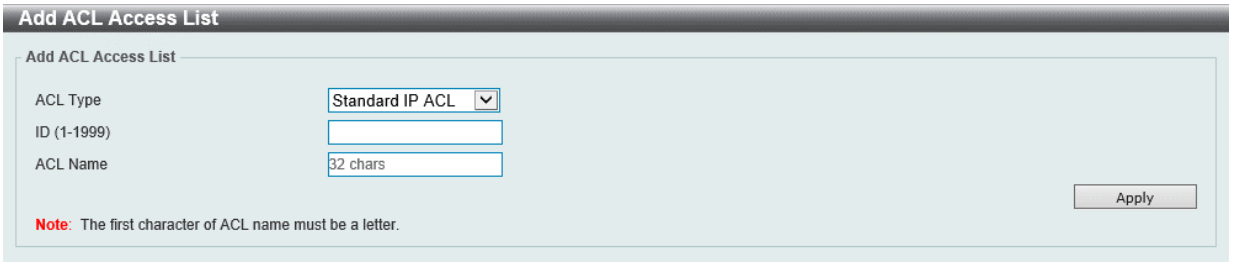


図 11-11　ACL Access List（Add ACL）- Add ACL Access List 画面

画面に表示される項目：

項目	説明
ACL Type	ACL プロファイルの種類を選択します。 • 選択肢：「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」
ID	ACL ID を入力します。 • 設定可能範囲：（Standard IP ACL）1-1999 （Extended IP ACL）2000-3999 （Standard IPv6 ACL）11000-12999 （Extended IPv6 ACL）13000-14999 （Extended MAC ACL）6000-7999 （Extended Expert ACL）8000-9999
ACL Name	ACL 名を入力します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

Standard IP ACL（通常 IP ACL）

ACL ルールの追加（Add Rule）（Standard IP ACL）

「ACL Access List」画面で「Standard IP ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

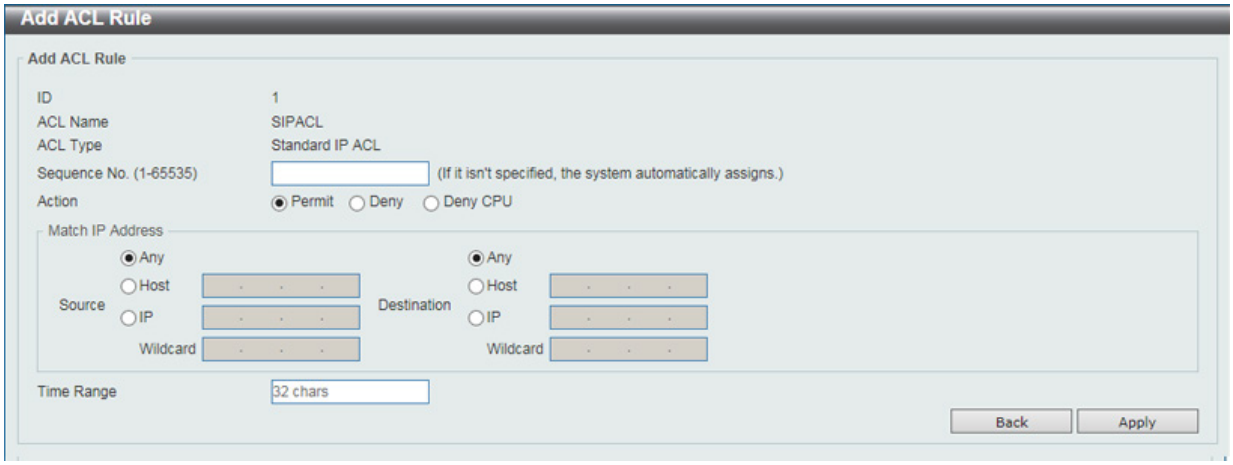


図 11-12　ACL Access List（Standard IP ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」「Deny CPU（拒否 /CPU）」
Match IP Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Extended IP ACL（拡張 IP ACL）

ACL ルールの追加（Add Rule）（Extended IP ACL）

「ACL Access List」画面で「Extended IP ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

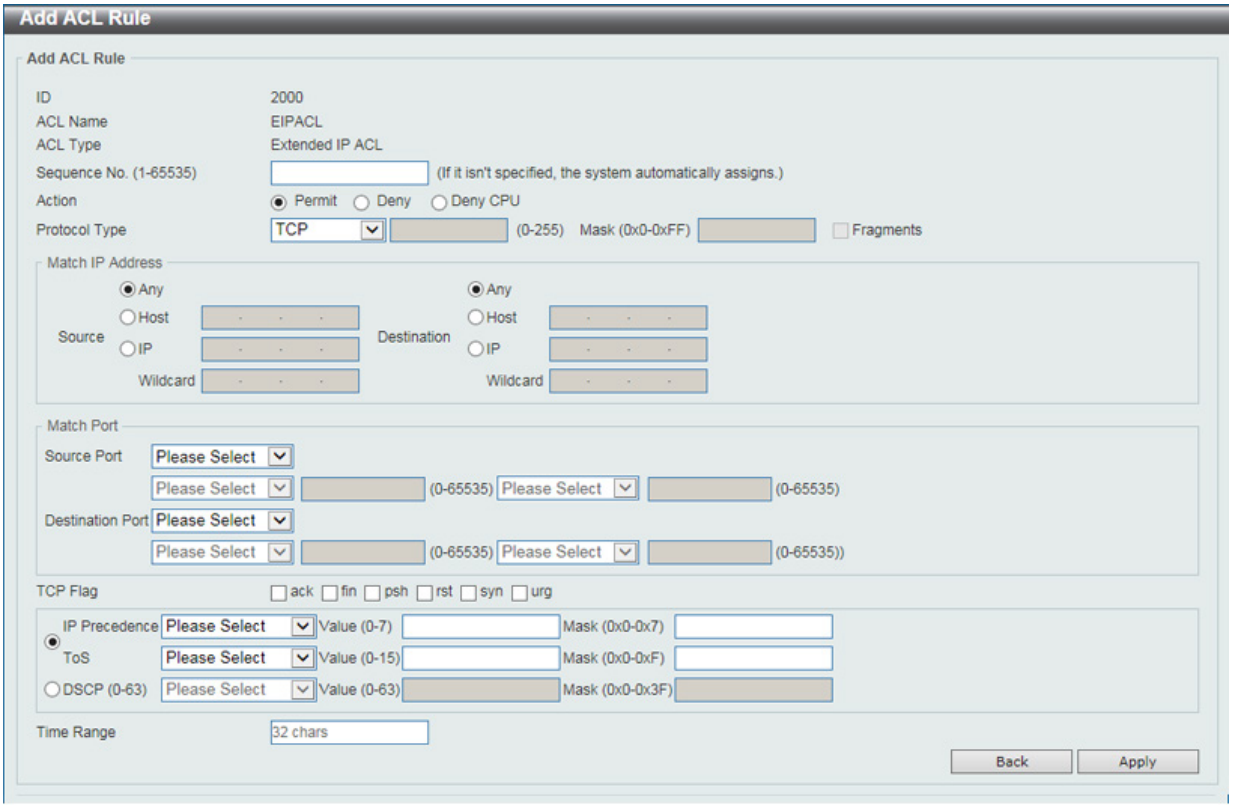


図 11-13　ACL Access List（Extended IP ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」「Deny CPU（拒否 /CPU）」
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「EIGRP (88)」「 ESP (50)」「 GRE (47)」「 IGMP (2)」「 OSPF (89)」「 PIM (103)」「 VRRP (112)」「 IP-in-IP (94)」「 PCP (108) 」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（Extended IP ACL）

項目	説明
Match IP Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。

項目	説明
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「0 (routine)」「1 (priority)」「2（immediate）」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」 - 「Value」：IP 優先値を入力します。（0-7） - 「Mask」に IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「4（max-throughput)」「8（min-delay)」 - 「Value」：ToS 値を入力します。（0-15） - 「Mask」：ToS マスクを入力します。（0x0-0xF）
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」：DSCP 値を入力します。（0-63） - 「Mask」：DSCP マスクを入力します。0x0-0x3F）
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「TCP」「UDP」選択時に表示される項目（Extended IP ACL）

項目	説明
Match Port	
Source Port	送信元ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（Extended IP ACL）

項目	説明
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（Extended IP ACL）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Standard IPv6 ACL（通常 IPv6 ACL）

ACL ルールの追加（Add Rule）（Standard IPv6 ACL）

「ACL Access List」画面で「Standard IPv6 ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

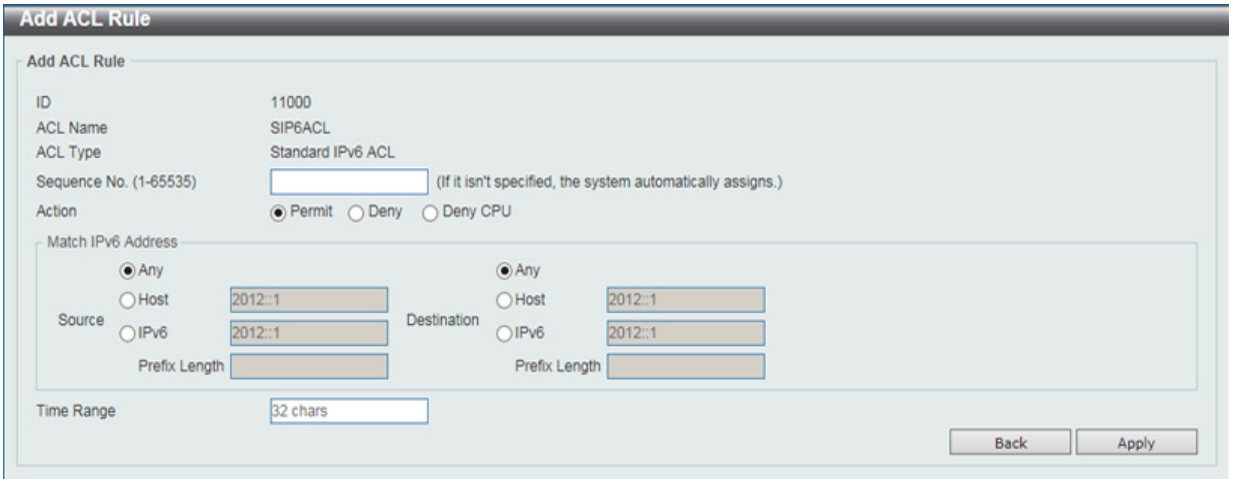


図 11-14　ACL Access List（Standard IPv6 ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」「Deny CPU（拒否 /CPU）」
Match IPv6 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Extended IPv6 ACL（拡張 IPv6 ACL）

ACL ルールの追加（Add Rule）（Extended IPv6 ACL）

「ACL Access List」画面で「Extended IPv6 ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

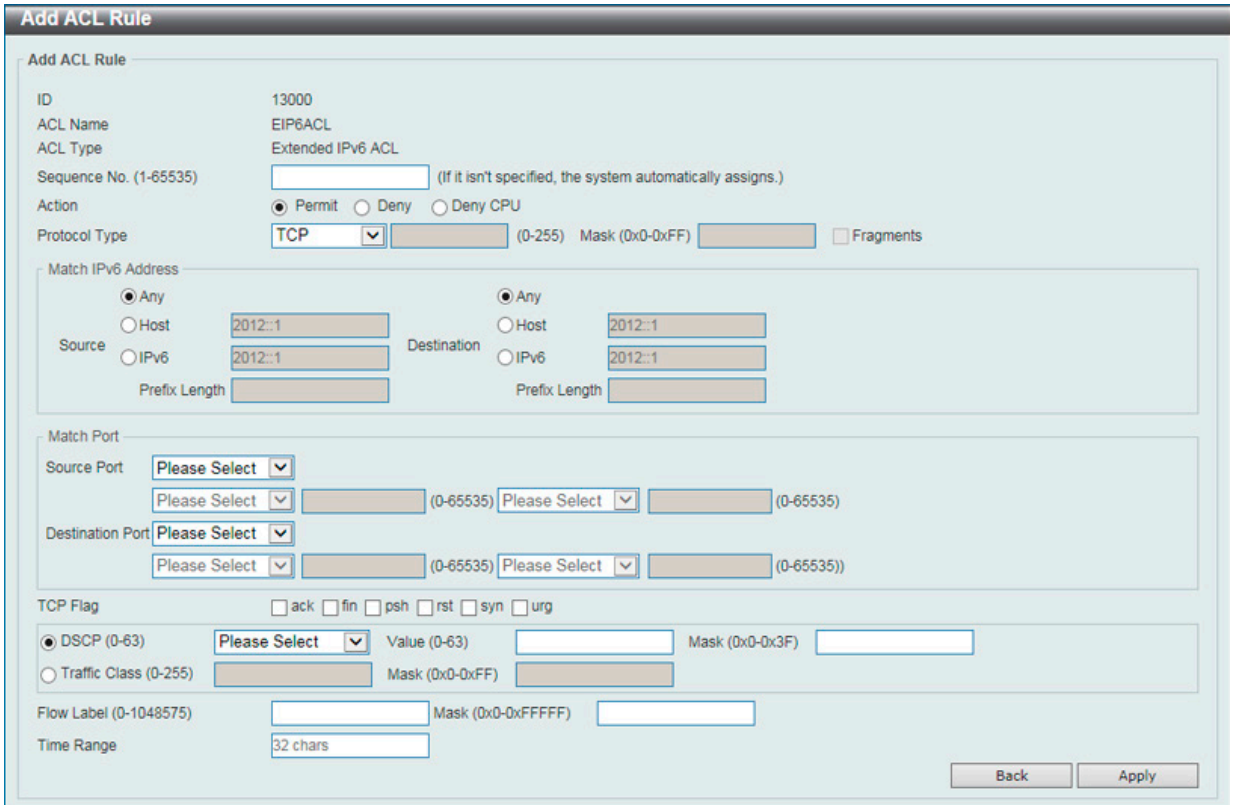


図 11-15　ACL Access List（Extended IPv6 ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」「Deny CPU（拒否 /CPU）」
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「Protocol ID」「ESP」「PCP」「SCTP」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（Extended IPv6 ACL）

項目	説明
Match IPv6 Address	
Source	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先のアドレスを指定します。 • 「Any - 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が選択可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
IPv6 DSCP	
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value：DSCP 値を入力します。（0-63） - 「Mask：DSCP マスクを入力します。（0x0-0x3F）
Traffic Class	トラフィッククラス値を入力します。 • 設定可能範囲：0-255 • 「Mask」：トラフィッククラスのマスク値を入力します。（0x0-0xFF）
Flow Label	
Flow Label	フローラベルの値を入力します。 • 設定可能範囲：0-1048575 • 「Mask」：フローラベルマスクを入力します。（0x0-0xFFFFF）
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「TCP」「UDP」選択時に表示される項目（Extended IPv6 ACL）

項目	説明
Match Port	
Source Port	送信元ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（Extended IPv6 ACL）

項目	説明
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（Extended IPv6 ACL）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。

項目	説明
ICMP Message Type	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定が可能範囲：0-255
Message Code	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定が可能範囲：0-255

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Extended MAC ACL（拡張 MAC ACL）

ACL ルールの追加（Add Rule）（Extended MAC ACL）

「ACL Access List」画面で「Extended MAC ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

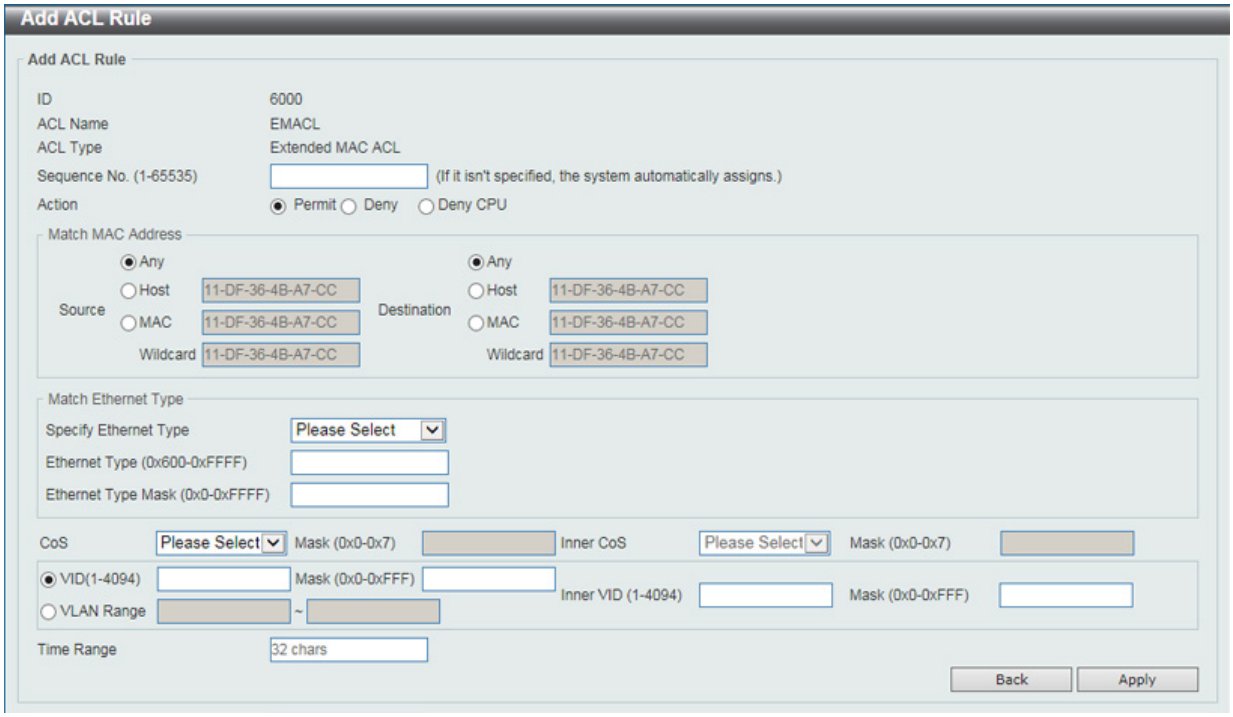


図 11-16　ACL Access List（Extended MAC ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」「Deny CPU（拒否 /CPU）」
Match MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。送信元 MAC アドレスとワイルドカードを指定します。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの MAC アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。宛先 MAC アドレスとワイルドカードを指定します。
Match Ethernet Type	
Specify Ethernet Type	イーサネットタイプを選択します。 • 設定可能範囲：「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
Ethernet Type	イーサネットタイプの 16 進数値を指定します。「Specify Ethernet Type」で指定したイーサネットタイプに基づき自動的に適切な値が入力されます。 • 設定可能範囲：0x600-0xFFFF

項目	説明
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。「Specify Ethernet Type」で指定したイーサネットタイプに基づき自動的に適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
802.1Q VLAN	
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 •「Mask」：CoS マスクを入力します。
Inner CoS	Inner CoS の値を入力します。 • 設定可能範囲：0-7 •「Mask」：Inner CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに適用する VLAN ID を入力します。 • 設定可能範囲：1-4094 •「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）
Inner VID	ACL ルールに適用する Inner VID を入力します。 • 設定可能範囲：1-4094 •「Mask」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
VLAN Range	ACL ルールに紐づける VLAN 範囲（開始 VLAN/ 終了 VLAN）を入力します。 • 設定可能範囲：1-4094
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Extended Expert ACL（拡張詳細 ACL）

ACL ルールの追加（Add Rule）（Extended Expert ACL）

「ACL Access List」画面で「Extended Expert ACL」エントリを選択し、「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

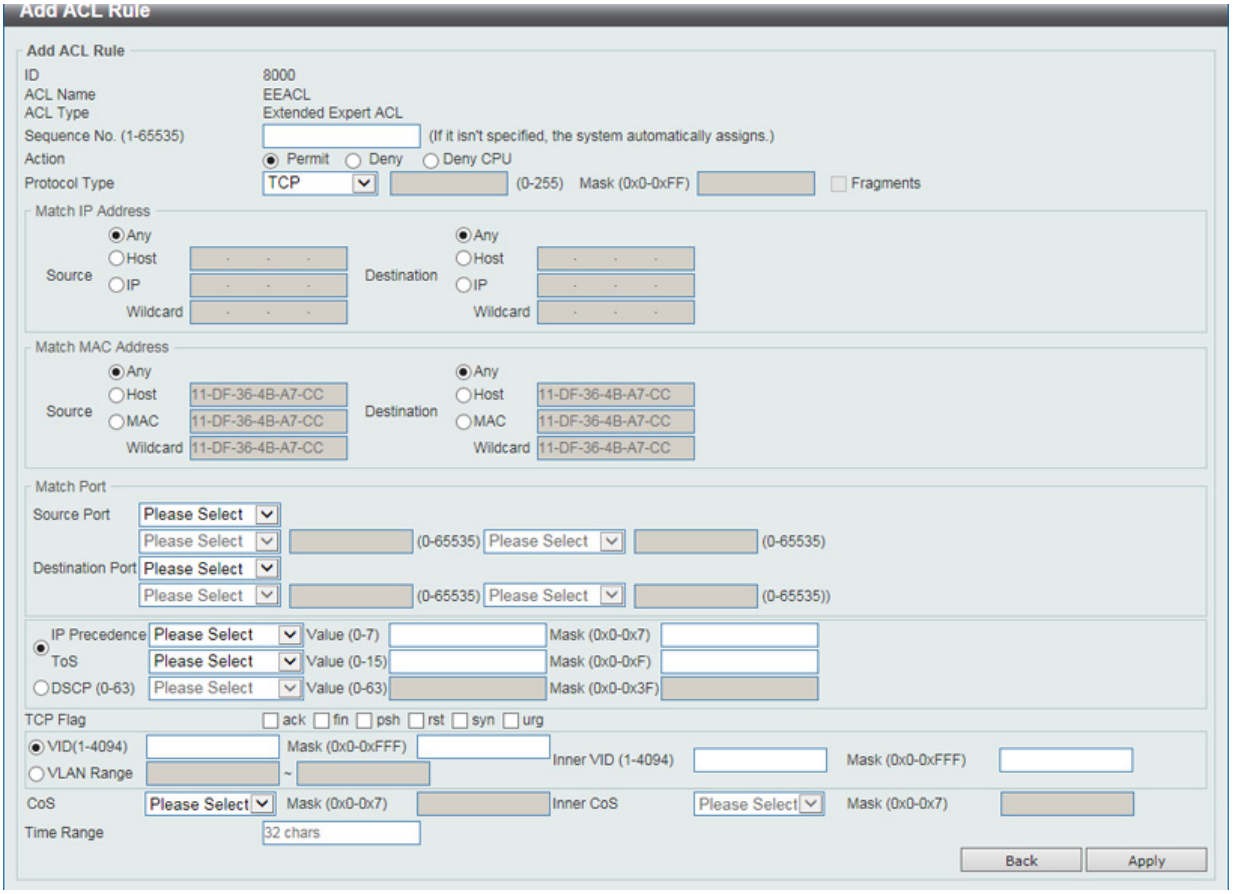


図 11-17　ACL Access List（Extended Expert ACL/Add Rule）- Add ACL Rule 画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」「Deny CPU（拒否 /CPU）」
Protocol Type	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「 Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（Extended Expert ACL）

項目	説明
Match IP Address	
Source	送信元のアドレスを指定します。 •「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 •「Host」- 送信元ホストの IP アドレスを入力します。 •「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 •「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 •「Host」- 宛先ホストの IP アドレスを入力します。 •「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Match MAC Address	
Source	送信元の MAC アドレスを指定します。 •「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 •「Host」- 送信元ホストの MAC アドレスを入力します。 •「MAC」-「Wildcard」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力することができます。
Destination	宛先の MAC アドレスを指定します。 •「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 •「Host」- 宛先ホストの MAC アドレスを入力します。 •「MAC」-「Wildcard」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
IPv4 DSCP	
IP Precedence	IP 優先値を指定します。 • 選択肢：「0 (routine)」「1 (priority)」「2（immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」 -「Value」：IP 優先値を入力します。（0-7） -「Mask」：IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「4（max-throughput)」「8（min-delay)」から指定できます。 -「Value」：ToS 値を入力します。（0-15） -「Mask」：ToS マスクを入力します。（0x0-0xF）
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 -「Value」：DSCP 値を入力します。（0-63） -「Mask」：DSCP マスクを入力します。（0x0-0x3F）
802.1Q VLAN	
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 •「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）

項目	説明
Inner VID	ACL ルールに紐づける Inner VLAN ID を入力します。 • 設定可能範囲：1-4094 •「Mask」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
VLAN Range	ACL ルールに紐づける VLAN 範囲（開始 VLAN/ 終了 VLAN）を入力します。 • 設定可能範囲：1-4094
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 •「Mask」：CoS マスクを入力します。（0x0-0x7）
Inner CoS	Inner CoS の値を入力します。 • 設定可能範囲：0-7 •「Mask」：Inner CoS マスクを入力します。（0x0-0x7）
スケジュール設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「TCP」「UDP」選択時に表示される項目（Extended Expert ACL）

項目	説明
Match MAC Address	
Source Port	送信元ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	宛先ポートの値を指定します。「=」「>」「<」「≠」「Range」から指定可能です。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（Extended Expert ACL）

項目	説明
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（Extended Expert ACL）

項目	説明
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。
ICMP Message Type	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

ACL Interface Access Group（ACL インタフェースアクセスグループ）

ACL インタフェースアクセスグループの設定、表示を行います。

ACL > ACL Interface Access Group の順にメニューをクリックし、以下の画面を表示します。

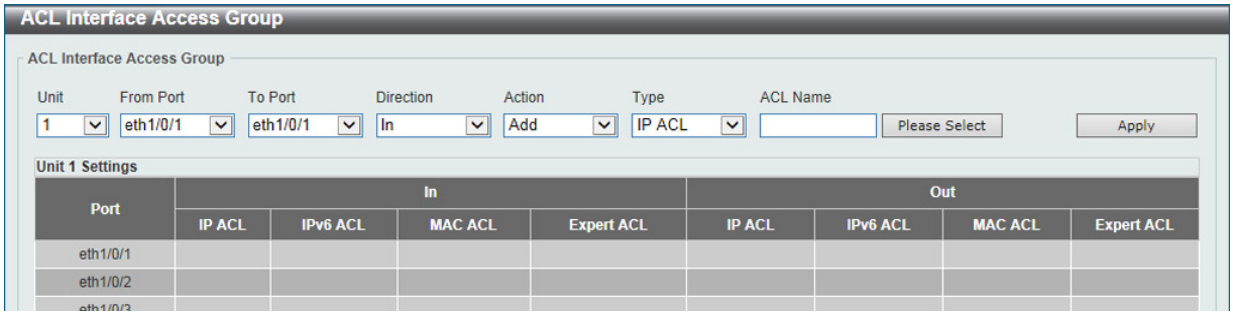


図 11-18　ACL Interface Access Group 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Direction	方向を指定します。 • 選択肢：「In」「Out」
Action	ACL インタフェースアクセスグループを追加 / 削除します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	ACL の種類を選択します。 • 選択肢：「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」
ACL Name	アクセスコントロールリスト名を入力します。「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定することも可能です。

「Apply」ボタンをクリックして、設定内容を適用します。

「Please Select」ボタンをクリックすると次の画面が表示されます。



図 11-19　ACL Interface Access Group（Please Select ）- ACL Access List 画面

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
設定するエントリを選択し「OK」ボタンをクリックします。

ACL VLAN Access Map（ACL VLAN アクセスマップ）

ACL VLAN アクセスマップの設定、表示を行います。

ACL > ACL VLAN Access Map の順にメニューをクリックし、以下の画面を表示します。

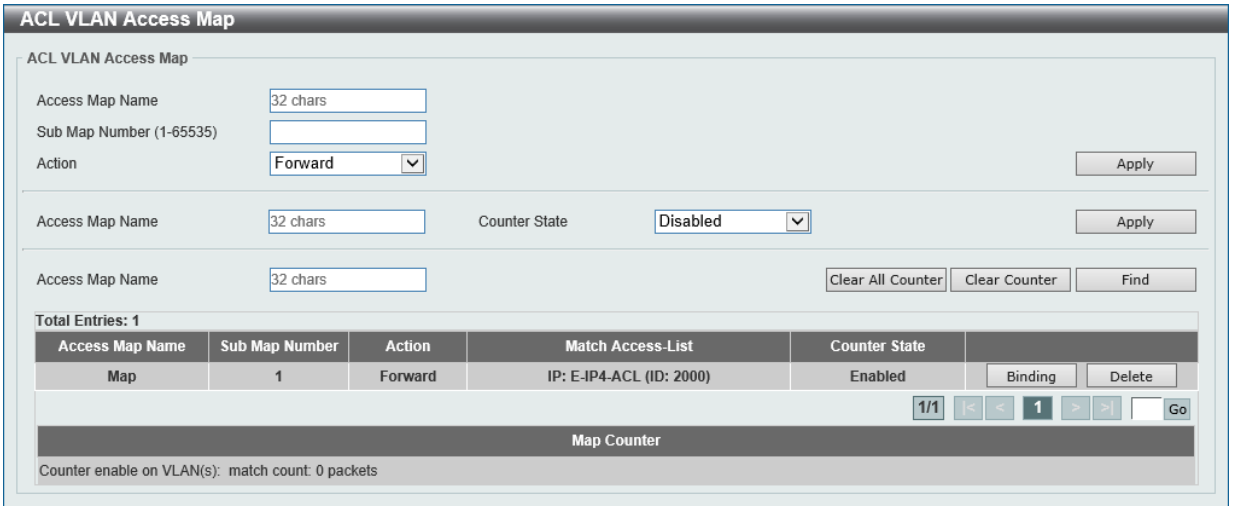


図 11-20　ACL VLAN Access Map 画面

画面に表示される項目：

項目	説明
Access Map Name	アクセスマップ名を入力します。（32 文字以内）
Sub Map Number	サイトマップ番号を入力します。 • 設定可能範囲：1-65535
Action	実行するアクションを選択します。「Redirect」を選択した場合、ドロップダウンリストからリダイレクトされるインタフェースを選択できます。 • 選択肢：「Forward」「Drop」「Redirect」
Counter State	カウンタの有効 / 無効を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

カウンタの検索・削除

「Clear All Counter」ボタンをクリックして、すべてのアクセスマップのカウンタ情報を消去します。
「Clear Counter」ボタンをクリックして、指定アクセスマップのカウンタ情報を消去します。
「Find」ボタンをクリックして、入力した情報を基に特定のエントリを検索します。

アクセスリストのバインディング・エントリの削除

「Binding」ボタンをクリックして、エントリにアクセスリストをバインディングします。
「Delete」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

アクセスマップエントリをクリックすると、画面下部に Map Counter テーブルが表示されます。

Match Access-List（照合アクセスリスト設定）

「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 11-21　ACL VLAN Access Map（Binding）- Match Access-List 画面

画面に表示される項目：

項目	説明
Match IP Access-List	照合する IP アクセスリストを指定します。 「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定することも可能です。
Match IPv6 Access-List	照合する IPv6 アクセスリストを指定します。 「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定することも可能です。
Match MAC Access-List	照合する MAC アクセスリストを指定します。 「Please Select」ボタンをクリックし、既存の ACL プロファイルを指定することも可能です。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

ACL の指定画面

「Please Select」ボタンをクリックすると次の画面が表示されます。



図 11-22　Match Access-List（Please Select）- ACL Access List 画面

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
設定するエントリを選択し「OK」ボタンをクリックします。

ACL VLAN Filter（ACL VLAN フィルタ設定）

ACL VLAN フィルタの設定、表示を行います。

ACL > ACL VLAN Filter の順にメニューをクリックし、以下の画面を表示します。

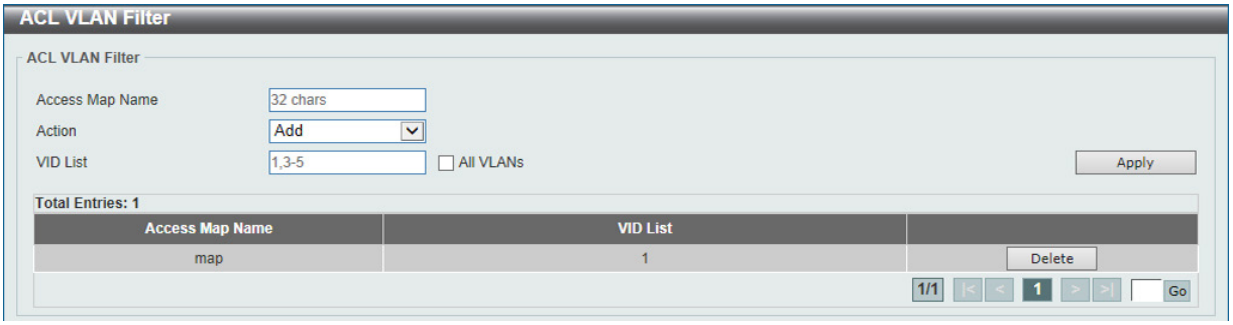


図 11-23　ACL VLAN Filter 画面

画面に表示される項目：

項目	説明
Access Map Name	アクセスマップ名を入力します。（32 文字以内）
Action	ACL VLAN フィルタを追加 / 削除します。 • 選択肢：「Add（追加）」「Delete（削除）」
VID List	使用する VLAN ID リストを入力します。「All VLANs」オプションにチェックを入れると、すべての VLAN に本設定を適用します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

CPU ACL（CPU ACL 設定）

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。

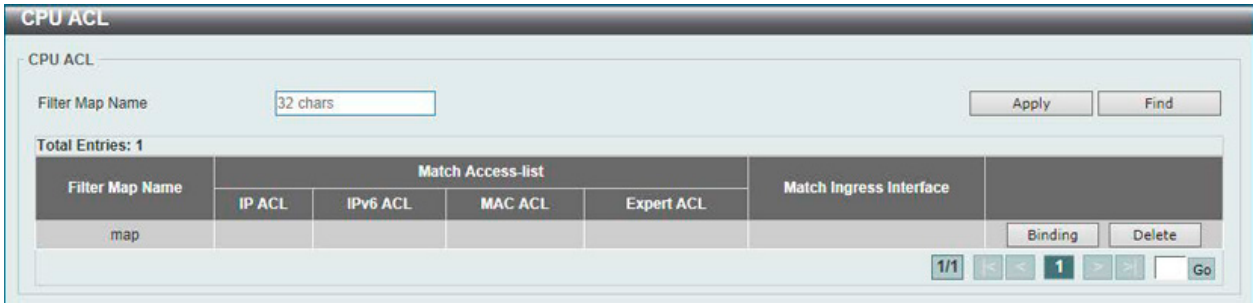


図 11-24　CPU ACL 画面

画面に表示される項目：

項目	説明
Filter Map Name	CPU ACL フィルタマップ名を指定します。（32 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックし、入力した情報を基に特定のエントリを検索します。
「Binding」ボタンをクリックし、エントリにアクセスリストをバインディングします。
「Delete」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

「Binding」ボタンをクリックすると以下の画面が表示されます。

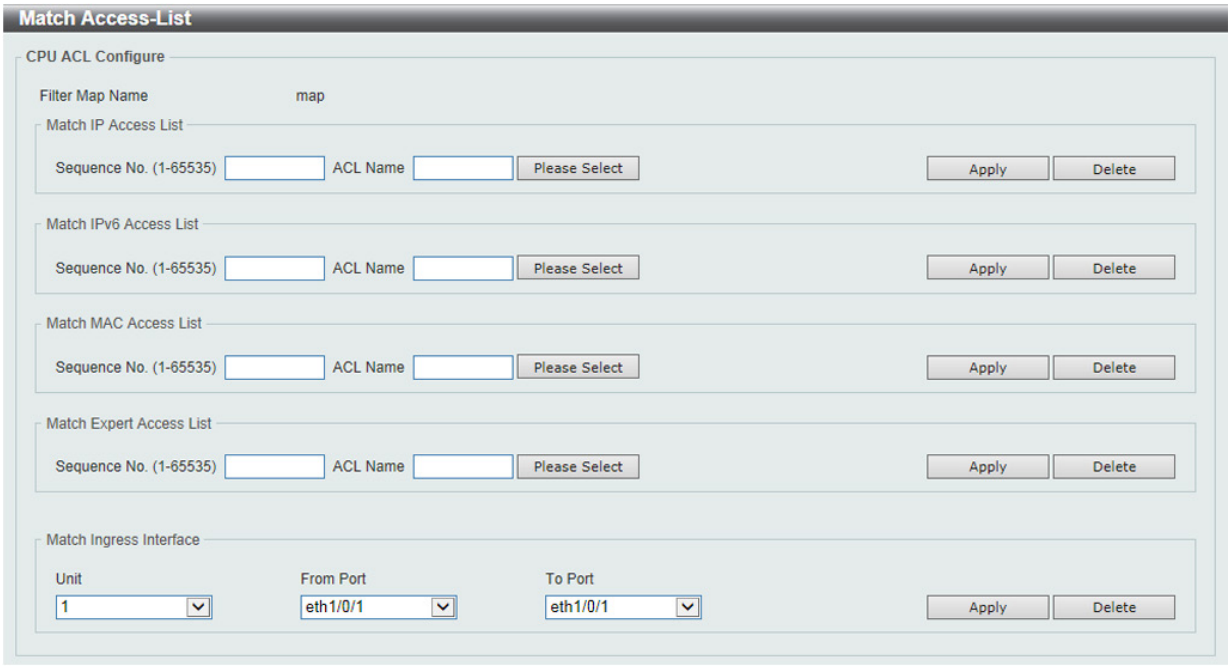


図 11-25　CPU ACL（Binding）- Match Access-List 画面

画面に表示される項目：

項目	説明
Match IP Access List	
Sequence No.	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL Name	照合する Standard または Extended IP アクセスリスト名を指定します。（32 文字以内） 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match IPv6 Access List	
Sequence No.	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535

項目	説明
ACL Name	照合する Standard または Extended IPv6 アクセスリスト名を指定します。（32 文字以内） 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match MAC Access List	
Sequence No.	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL Name	照合する Extended MAC アクセスリスト名を指定します。（32 文字以内） 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match Expert Access List	
Sequence No.	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL Name	照合する Extended Expert アクセスリスト名を指定します。（32 文字以内） 「Please Select」をクリックし、既存の ACL から選択することも可能です。
Match Ingress Interface	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

ACL 選択画面

「Please Select」ボタンをクリックすると次の画面が表示されます。



図 11-26　Match Access-List（Please Select）- ACL Access List 画面

設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。
設定するエントリを選択し「OK」ボタンをクリックします。

第 12 章　Security（セキュリティ機能の設定）

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

以下は Security サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
Port Security（ポートセキュリティ）	ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。
802.1X（802.1X 設定）	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。
AAA（AAA 設定）	AAA（Authentication、Authorization、Accounting）の設定を行います。
RADIUS（RADIUS 設定）	RADIUS の設定を行います。
TACACS+（TACACS+ 設定）	TACACS+ の設定を行います。
IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）	IP-MAC バインディングにより、スイッチにアクセスするユーザ数を制限します。
DHCP Server Screening（DHCP サーバスクリーニング設定）	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
ARP Spoofing Prevention（ARP スプーフィング防止設定）	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスと一致しなかった IP アドレスの ARP パケットをバイパスします。
BPDU Attack Protection（BPDU アタック防止設定）	スイッチのポートに BPDU 防止機能を設定します。
NetBIOS Filtering（NetBIOS フィルタリング設定）	NetBIOS フィルタリングの設定を行います。
MAC Authentication（MAC 認証）	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
Web-based Access Control（Web 認証）	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認証する機能です。
Network Access Authentication（ネットワークアクセス認証）	Network Access Authentication（ネットワークアクセス認証）の設定を行います。
Safeguard Engine（セーフガードエンジン）	セーフガードエンジンは、攻撃中にスイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。
Trusted Host（トラストホスト）	トラストホストの設定を行います。
Traffic Segmentation（トラフィックセグメンテーション）	トラフィックセグメンテーション機能はポート間のトラフィックの流れの制限を行います。
Storm Control Settings（ストームコントロール設定）	ストームコントロールの設定を行います。
DoS Attack Prevention Settings（DoS 攻撃防止設定）	各 DoS 攻撃に対して防御設定を行います。
SSH（Secure Shell）	SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。
SSL（Secure Socket Layer）	Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。
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。
Network Protocol Port Protect Settings（ネットワークプロトコルポート保護設定）	ネットワークプロトコルポートプロテクションの設定、表示を行います。

Port Security（ポートセキュリティ）

ポートセキュリティの設定を行います。ポートセキュリティ機能では、ソース MAC アドレスが未認証であるコンピュータについて、指定ポートからネットワークへアクセスすることを防ぐことができます。

Port Security Global Settings（ポートセキュリティグローバル設定）

ポートセキュリティのグローバル設定を行います。

Security > **Port Security** > **Port Security Global Settings** の順にクリックし、以下の画面を表示します。

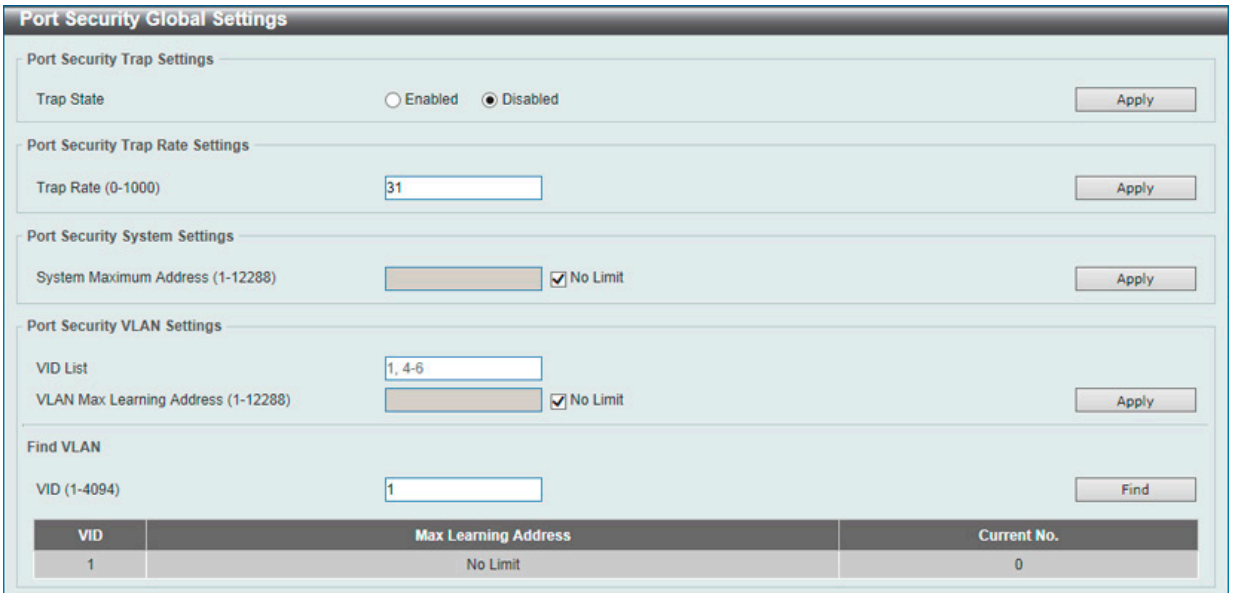


図 12-1　Port Security Global Settings 画面

画面に表示される項目：

項目	説明
Port Security Trap Settings	
Trap State	ポートセキュリティのトラップを有効 / 無効に設定します。
Port Security Trap Rate Settings	
Trap Rate	1 秒あたりのトラップ数を指定します。初期値の 31 では、すべてのセキュリティ違反に対して SNMP トラップが生成されます。 • 設定可能範囲：0-1000 • 初期値：31
Port Security System Settings	
System Maximum Address	許可される最大 MAC アドレス数を入力します。初期値では制限なしになります。「No Limit」オプションにチェックを入れると、セキュアな MAC アドレスの最大数が適用されます。 • 設定可能範囲：1-12288
Port Security VLAN Settings	
VID List	VLAN ID を指定します。
VLAN Max Learning Address	指定の VLAN が学習可能な MAC アドレスの最大数を指定します。「No Limit」オプションにチェックを入れると、セキュアな MAC アドレスの最大数が適用されます。 • 設定可能範囲：1-12288
Find VLAN	
VID	表示する VLAN ID を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。

Port Security Port Settings（ポートセキュリティポート設定）

ポートセキュリティのポート設定と設定内容の表示を行います。

Security > **Port Security** > **Port Security Port Settings** の順にメニューをクリックし、以下の画面を表示します。

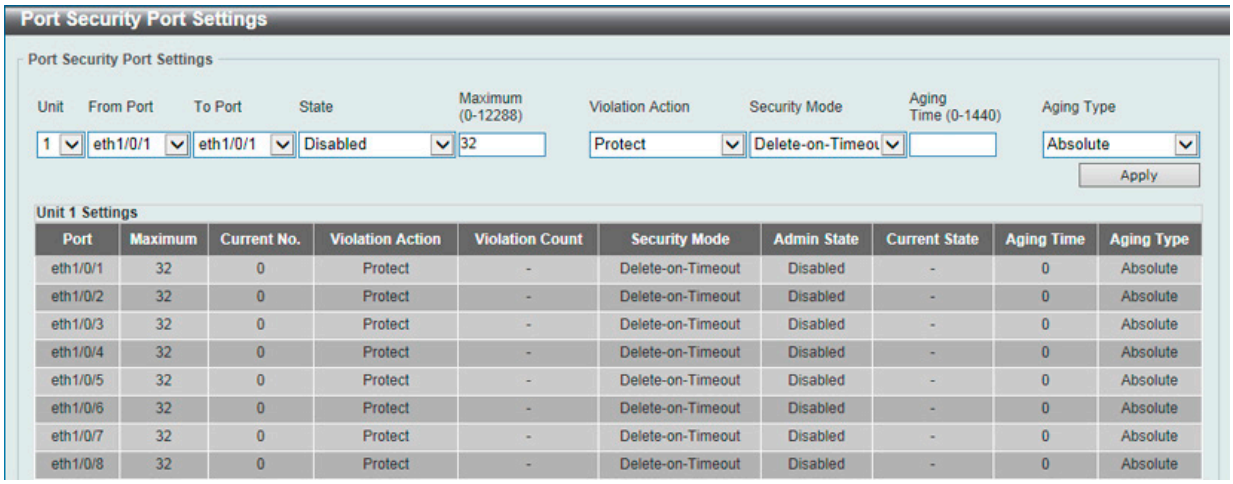


図 12-2　Port Security Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
State	指定ポートにおけるポートセキュリティ機能を有効 / 無効に設定します。
Maximum	指定ポートで許可されるセキュアな MAC アドレスの最大数を指定します。 • 設定可能範囲：0-12288 • 初期値：32
Violation Action	違反に対して実行するアクションを指定します。 • 「Protect」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反としてはカウントされません。 • 「Restrict」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントしてシステムログに記録します。 • 「Shutdown」- セキュリティ違反がある場合にポートをシャットダウンし、システムログに記録します。
Security Mode	セキュリティモードを選択します。 • 「Permanent」- すべての学習した MAC アドレスは、手動でエントリを削除しない限り削除されません。 • 「Delete-on-Timeout」- すべての学習した MAC アドレスは、タイムアウトにより自動的に削除されるか、手動により削除されます。
Aging Time	指定ポートで自動学習された安全なアドレスに使用するエージングタイムを入力します。 • 設定可能範囲：0-1440（分）
Aging Type	エージングの種類を指定します。 • 「Absolute」- ポート上のすべてのアドレスは、指定された時間を過ぎるとアドレスリストから削除されます。（初期値） • 「Inactivity」- ポート上のアドレスは、指定の期間そのアドレスからのトラフィックがない場合にエージアウトします。

「Apply」ボタンをクリックして、設定内容を適用します。

Port Security Address Entries（ポートセキュリティアドレスエントリ設定）

ポートセキュリティアドレスエントリの設定、表示を行います。

Security > Port Security > Port Security Address Entries の順にメニューをクリックし、以下の画面を表示します。

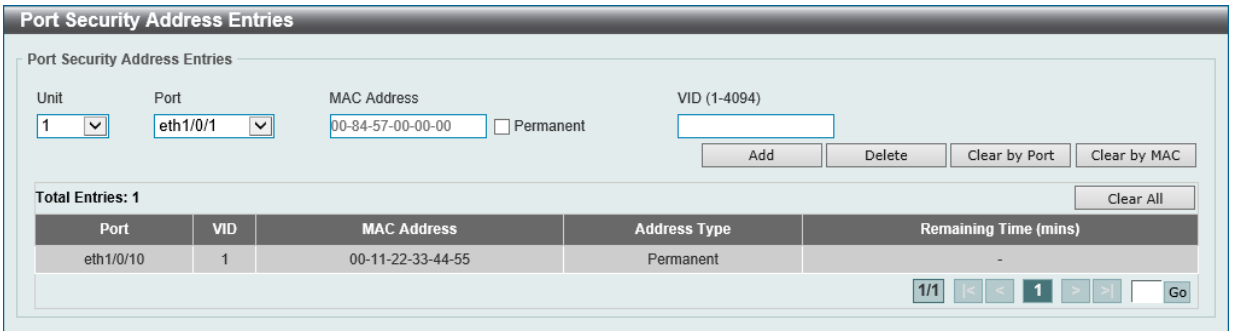


図 12-3　Port Security Address Entries 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port/To Port	本設定を適用するポート範囲を指定します。
MAC Address	MAC アドレスを入力します。「Permanent」オプションにチェックを入れると、すべての学習した MAC アドレスは、手動でエントリを削除しない限り削除されません。
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094

「Add」ボタンをクリックして、入力した情報に基づく新しいエントリを追加します。
「Delete」ボタンをクリックし、入力した情報に基づくエントリを削除します。
「Clear by Port」ボタンをクリックして、選択したポートに基づき情報を消去します。
「Clear by MAC」ボタンをクリックして、選択した MAC アドレスに基づき情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

802.1X（802.1X 設定）

802.1X（ポートベースおよびホストベースのアクセスコントロール）

IEEE 802.1X は、ユーザ認証を行うセキュリティの規格です。

クライアント / サーバベースのアクセスコントロールモデルを使用し、特定のローカルエリアネットワーク上の有線 / 無線デバイスへのアクセスを許可および認証するために使用します。この認証方法は、ネットワークへアクセスするユーザの認証に RADIUS サーバを使用し、EAPOL（Extensible Authentication Protocol over LAN）と呼ばれるパケットをクライアント / サーバ間でリレーして実現します。

以下の図は、基本的な EAPOL パケットの構成です。

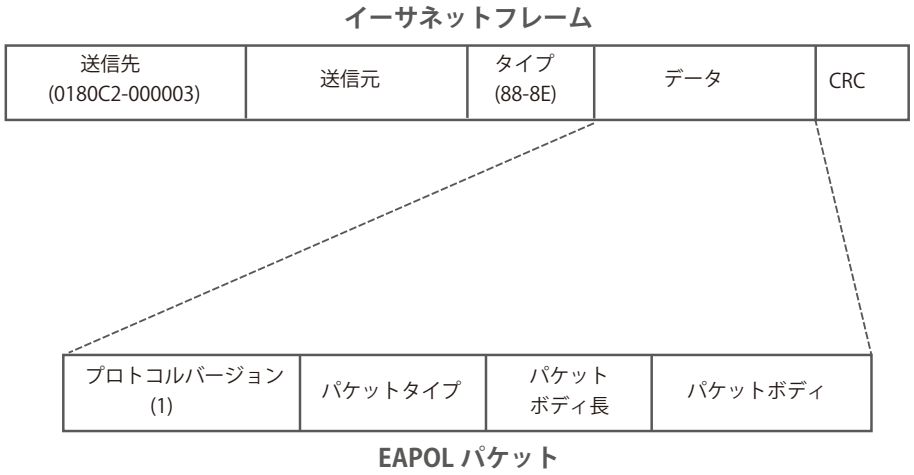


図 12-4　EAPOL パケット

IEEE 802.1X を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。
EAPOL パケットは、承認完了前でも指定ポート経由で送受信できる唯一のトラフィックです。

802.1X アクセスコントロールには認証サーバ、オーセンティケータ、クライアントの 3 つの役割があります。
それぞれがアクセスコントロールセキュリティの作成、状態の維持、動作のために重要です。

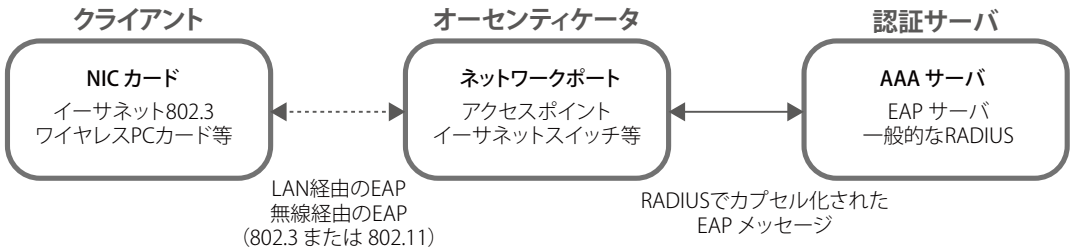


図 12-5　802.1X の 3 つの役割

以降の項目では、認証サーバ、オーセンティケータ、クライアントのそれぞれの役割について説明します。

認証サーバ

認証サーバは、クライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。

認証サーバ上で RADIUS サーバプログラムが実行され、認証サーバのデータがオーセンティケータ（スイッチ）に正しく登録されている必要があります。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを使用する前に、認証サーバ（RADIUS）によって認証される必要があります。

認証サーバの役割は、ネットワークにアクセスするクライアントの身元を証明することです。認証サーバ（RADIUS）とクライアントの間で EAPOL パケットによるセキュアな情報交換を行い、クライアントが「LAN やスイッチのサービスに対するアクセス許可があるか」をスイッチに通知します。

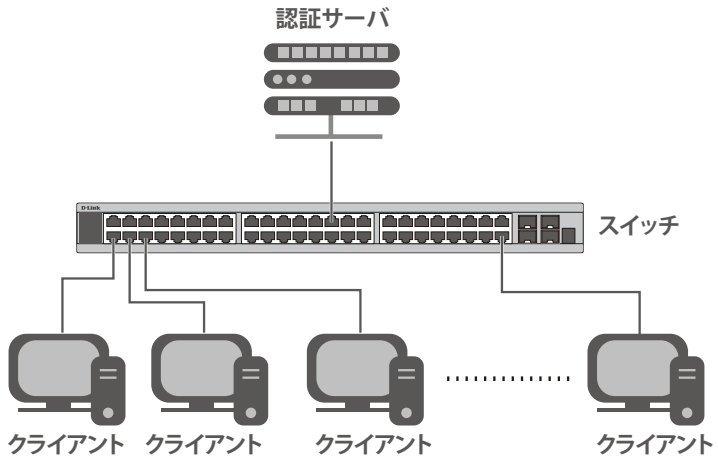


図 12-6　認証サーバ

オーセンティケータ

オーセンティケータ（スイッチ）は、認証サーバとクライアントの間を仲介します。

802.1X を使用する場合、オーセンティケータには 2 つの役割があります。

- 1 つ目の役割：
  クライアントに EAPOL パケットを通して認証情報を提出するよう要求することです。
  EAPOL パケットはクライアントにアクセスが許可される前にオーセンティケータを通過することのできる唯一の情報です。
- 2 つ目の役割：
  クライアントから収集した情報を認証サーバに確認してもらい、その結果をクライアントに伝達することです。

スイッチをオーセンティケータとして設定するには、以下の手順を実行します。

1. スイッチの 802.1X 機能を有効にします。（**Security > 802.1X > 802.1X Global Settings**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Port Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > RADIUS > RADIUS Server Settings**）

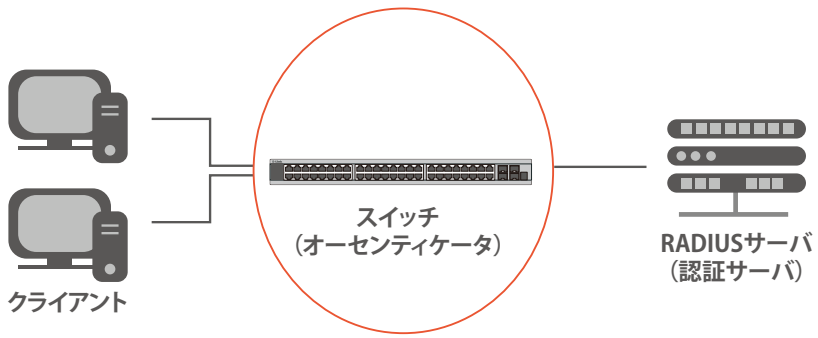


図 12-7　オーセンティケータ

クライアント

クライアントとは、LAN やスイッチが提供するサービスへアクセスしようとする端末です。

クライアントとなる端末では、802.1X プロトコルに準拠したソフトウェアが起動している必要があります。一部の Windows OS のように、OS 内に既にそのソフトウェアが組み込まれている場合がありますが、それ以外の OS をお使いの場合は、802.1X クライアントソフトウェアを別途用意する必要があります。

クライアントは EAPOL パケットを使用して LAN へのアクセスを要求し、スイッチからの要求に応答します。

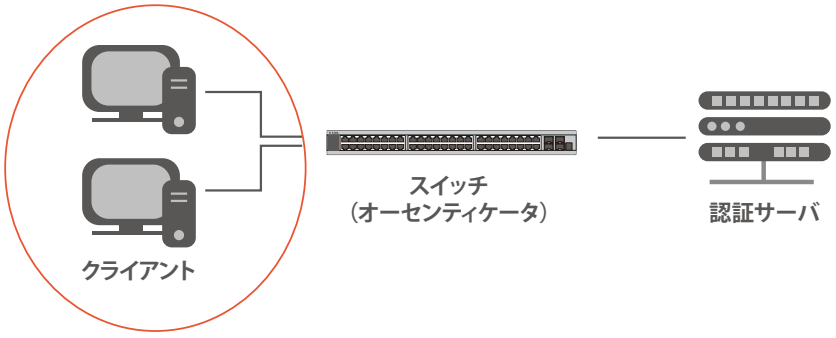


図 12-8　クライアント

認証プロセスについて

前述の「認証サーバ」「オーセンティケータ」「クライアント」により、802.1X プロトコルはネットワークへアクセスするユーザの認証を安定的かつ安全に行います。

認証完了前には EAPOL トラフィックのみが特定のポートの通過を許可されます。このポートは、有効なユーザ名とパスワード（802.1X の設定によっては MAC アドレスも）を持つクライアントがアクセス権を取得してポートのロックが解除されるまで、ロック状態を保ちます。ロックが解除されると、通常のトラフィックがポートを通過できるようになります。

本製品の 802.1X では、以下の 2 種類のアクセスコントロールが選択できます。

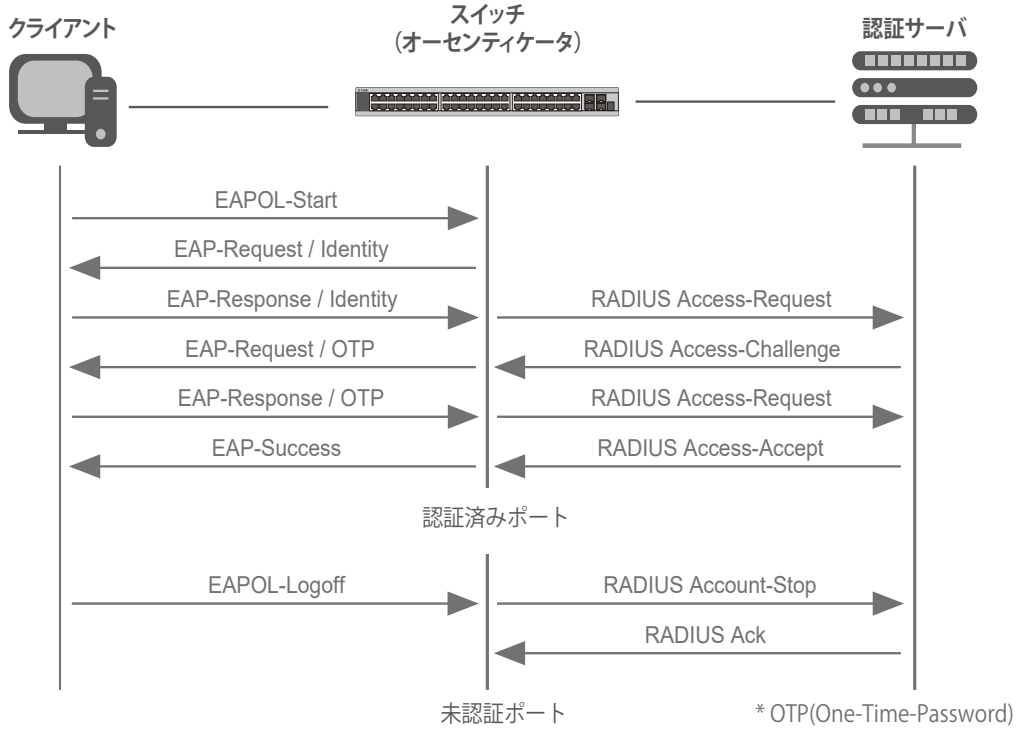


図 12-9　802.1X 認証プロセス

本製品の 802.1X 機能では、以下の 2 つのタイプのアクセスコントロールから選択することができます。

1. **ポートベースのアクセスコントロール**
   本方式では、リモート RADIUS サーバが、ポートごとに 1 人のユーザのみを認証することで、同じポート上の残りのユーザがネットワークにアクセスできるようにします。
2. **ホストベースのアクセスコントロール**
   本方式では、スイッチはポートで最大 4096 件までの MAC アドレスを自動的に学習してリストに追加します。
   スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に MAC アドレスごと（ユーザごと）の認証を行います。

802.X ポートベース / ホストベースのネットワークアクセスコントロールについて

802.1X は、元々は LAN 上で Point to Point プロトコルの特長を活用するために開発されました。

単一の LAN セグメントが 2 台より多くのデバイスを持たない場合、デバイスのどちらかがブリッジポートとなります。
ブリッジポートは、「リンクのリモートエンドにアクティブなデバイスが接続された」「アクティブなデバイスが非アクティブ状態になった」などのイベントを検知します。これらのイベントをポートの認証状態の制御に利用し、ポートの許可がされていない接続デバイスの認証プロセスを開始します。これをポートベースのアクセスコントロールと呼びます。

■ ポートベースネットワークアクセスコントロール

接続デバイスが認証に成功すると、ポートは「Authorized」（認証済み）の状態になります。ポートが未認証になるようなイベントが発生するまで、ポート上のすべてのトラフィックはアクセスコントロール制限の対象になりません。

そのため、ポートが複数のデバイスが所属する共有 LAN セグメントに接続される場合、接続デバイスの 1 つが認証に成功すると共有セグメント上のすべての LAN に対してアクセスを許可することになります。このような場合、ポートベースネットワークアクセスコントロールは脆弱であるといえます。

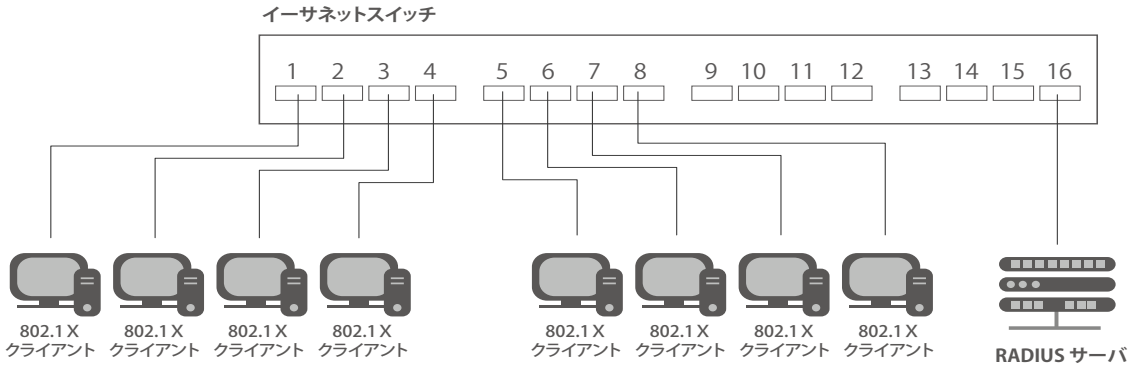


図 12-10　ポートベースアクセスコントロールのネットワーク構成例

■ ホストベースネットワークアクセスコントロール

共有 LAN セグメント内で 802.1X を活用するには、LAN へのアクセスを希望する各デバイスに論理ポートを定義する必要があります。

スイッチは、共有 LAN セグメントに接続する 1 つの物理ポートを異なる論理ポートの集まりであると認識し、それら論理ポートを EAPOL パケット交換と認証状態に基づいて別々に制御します。スイッチは接続する各デバイスの MAC アドレスを学習し、それらのデバイスがスイッチ経由で LAN と通信するための論理ポートを確立します。

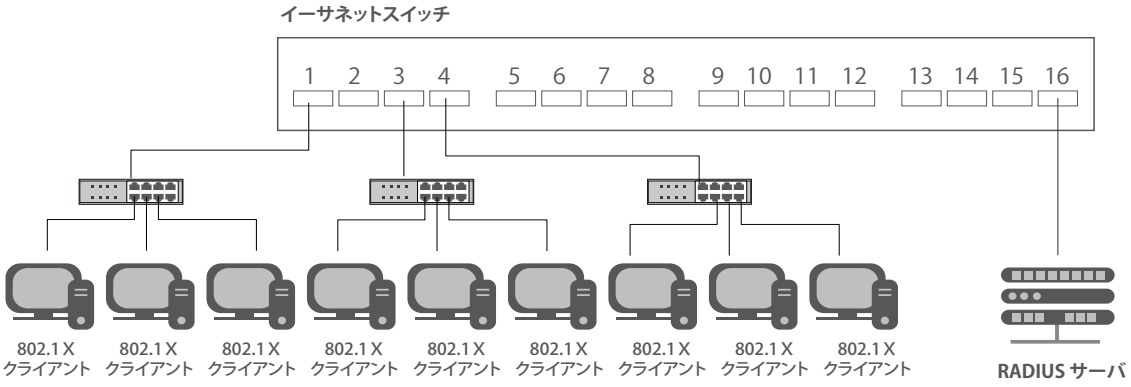


図 12-11　ホストベースアクセスコントロールのネットワーク構成例

802.1X Global Settings（802.1X グローバル設定）

本画面では 802.1X グローバル設定を行います。

802.1X 認証設定をするには、**Security > 802.1X > 802.1X Global Settings** の順にメニューをクリックします。



図 12-12　802.1X Global Settings 画面

画面に表示される項目：

項目	説明
802.1X State	802.1X 認証を有効 / 無効に設定します。
802.1X Trap State	802.1X トラップを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

802.1X Port Settings（802.1X ポート設定）

802.1X 認証ポートを設定します。

Security > 802.1X > 802.1X Port Settings の順にメニューをクリックします。

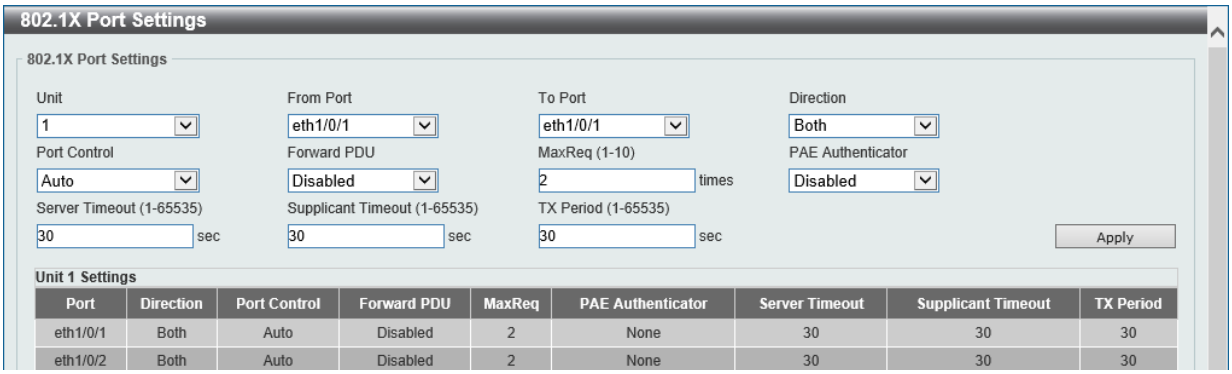


図 12-13　802.1X Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Direction	制御するトラフィックの方向を指定します。 • 「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（認証強制）」- 両方向の通信でポートは制御されません。 • 「Auto（自動）」- 制御対象の方向のポートへのアクセスは認証が必要になります。 • 「ForceUnauthorized（未認証強制）」- 制御対象の方向のポートへのアクセスはブロックされます。
Forward PDU	PDU 転送機能を有効 / 無効に設定します。
MaxReq	バックエンドの認証ステートマシンがクライアントに対して Extensible Authentication Protocol（EAP）リクエストフレームを再送する最大回数を指定します。本指定回数後、認証プロセスが再開されます。 • 設定可能範囲：1-10 • 初期値：2
PAE Authenticator	PAE Authenticator を有効 / 無効に設定します。 本設定により、特定ポートを IEEE 802.1X Port Access Entity（PAE）オーセンティケータとして指定します。
ServerTimeout	サーバのタイムアウト時間を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
SuppTimeout	サプリカント（クライアント）のタイムアウト状態となる時間を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）

項目	説明
TxPeriod	送信間隔を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

注意　定期的に EAP Request/Identity を送信する機能はありません。

Authentication Session Information（認証セッションの状態）

認証セッションの情報を表示します。

Security > 802.1X > Authentication Session Information の順にメニューをクリックし、以下の画面を表示します。

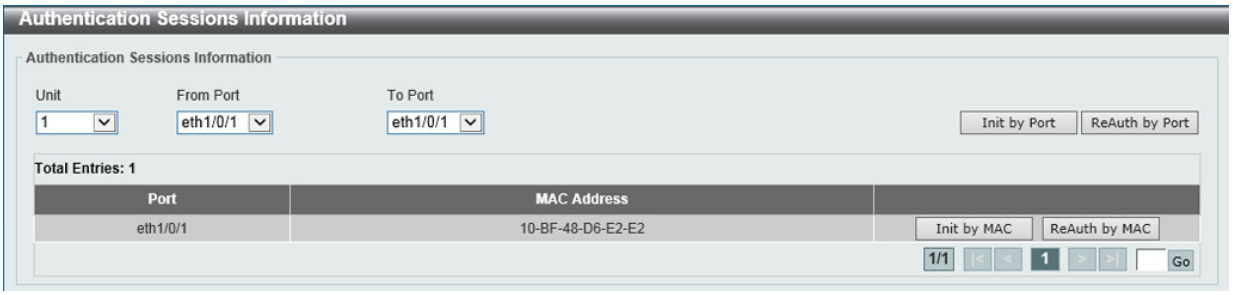


図 12-14　Authentication Session Information 画面

画面に表示される項目：

項目	説明
Unit	セッション情報の初期化 / 再認証を行うユニットを選択します。
From Port/To Port	セッション情報の初期化 / 再認証を行うポート範囲を指定します。

「Init by Port」ボタンをクリックして、指定ポートに基づくセッション情報の初期化を実行します。
「ReAuth by Port」ボタンをクリックして、指定ポートに基づくセッション情報の再認証（Re-Authenticate）を実行します。
「Init by MAC」ボタンをクリックして、指定 MAC アドレスに基づくセッション情報の初期化を実行します。
「ReAuth by MAC」ボタンをクリックして、指定 MAC アドレスに基づくセッション情報の再認証（Re-Authenticate）を実行します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Authenticator Statistics（オーセンティケータ統計情報）

オーセンティケータの統計情報を表示します。

Security > 802.1X > Authenticator Statistics の順にメニューをクリックし、以下の画面を表示します。

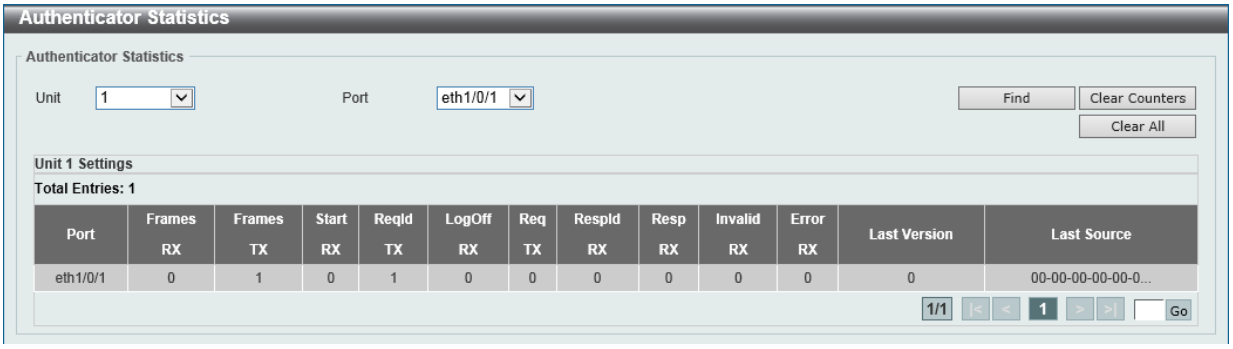


図 12-15　Authenticator Statics 画面

画面に表示される項目：

項目	説明
Unit	統計情報を表示 / クリアするユニットを選択します。
Port	統計情報を表示 / クリアするポート範囲を指定します。

「Find」ボタンをクリックし、指定ポートのエントリを検出します。
「Clear Counters」ボタンをクリックして、指定ポートの情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Authenticator Session Statistics（オーセンティケータセッション統計情報）

オーセンティケータセッションの統計情報を表示します。

Security > 802.1X > Authenticator Session Statistics の順にメニューをクリックし、以下の画面を表示します。



図 12-16　Authenticator Session Statistics 画面

画面に表示される項目：

項目	説明
Unit	統計情報を表示 / クリアするユニットを選択します。
Port	統計情報を表示 / クリアするポート範囲を指定します。

「Find」ボタンをクリックして、指定ポートのエントリを検出します。
「Clear Counters」ボタンをクリックして、指定ポートの情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。

Authenticator Diagnostics（オーセンティケータ診断）

オーセンティケータ診断情報を表示します。

Security > 802.1X > Authenticator Diagnostics の順にメニューをクリックし、以下の画面を表示します。

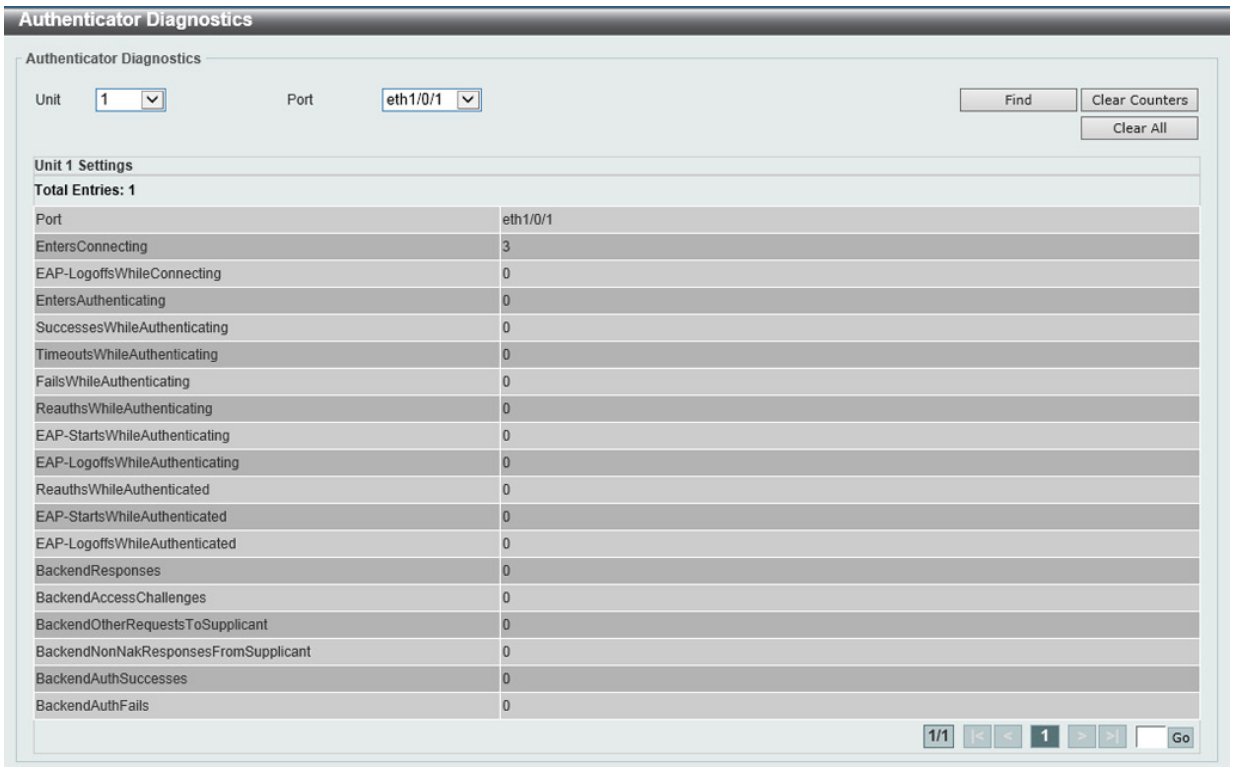


図 12-17　Authenticator Diagnostics 画面

画面に表示される項目：

項目	説明
Unit	診断情報を表示 / クリアするユニットを選択します。
Port	診断情報を表示 / クリアするポート範囲を指定します。

「Find」ボタンをクリックして、指定ポートのエントリを検出します。
「Clear Counters」ボタンをクリックして、指定ポートの情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

AAA（AAA 設定）

Security > AAA
本項目では AAA（Authentication、Authorization、Accounting）の設定を行います。

AAA Global Settings（AAA グローバル設定）

本項目では AAA（Authentication、Authorization、Accounting）のグローバル設定を行います。

Security > AAA > AAA Global Settings の順にメニューをクリックし、以下の画面を表示します。

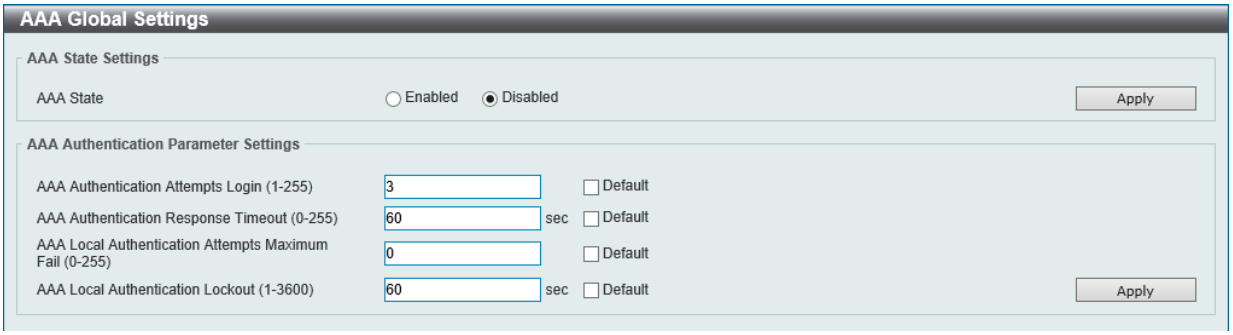


図 12-18　AAA Global Settings 画面

画面に表示される項目：

項目	説明
AAA State Settings	
AAA State	AAA のグローバルステータスを有効 / 無効に設定します。
AAA Authentication Parameter Settings	
AAA Authentication Attempts Login	許可される AAA 認証ログイン試行回数を入力します。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：1-255 • 初期値：3
AAA Authentication Response Timeout	AAA 認証応答のタイムアウト値を入力します。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：0-255（秒） • 初期値：60（秒）
AAA Local Authentication Attempts Maximum Fail	ローカル AAA 認証で許可される失敗の最大回数を入力します。この値が「0」の場合、本機能は無効となります。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：0-255 • 初期値：0
AAA Local Authentication Lockout	ローカル AAA 認証のロックアウト時間を入力します。「Default」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：1-3600（秒） • 初期値：60（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

Application Authentication Settings（アプリケーションの認証設定）

ログインする際に使用するスイッチの設定用アプリケーション（コンソール、Telnet、SSH、HTTP）を設定します。

Security > Access Authentication Control > Application Authentication Settings の順にクリックし、以下の画面を表示します。

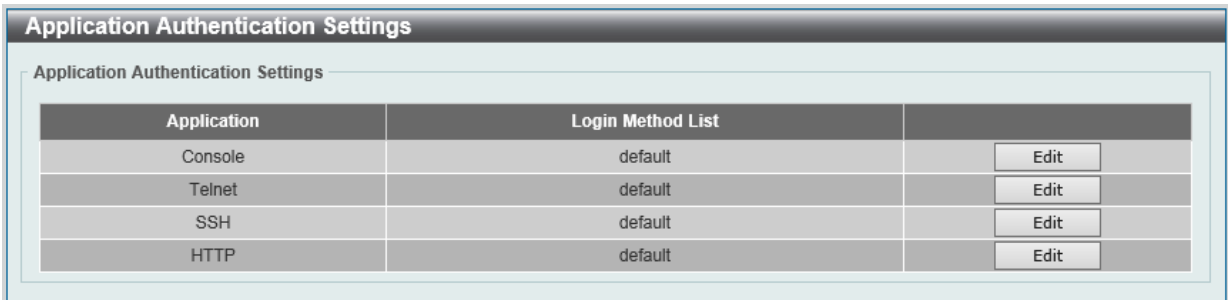


図 12-19　Application Authentication Settings 画面

指定エントリの「Edit」ボタンをクリックし編集を行います。

「Edit」をクリックすると、以下の画面が表示されます。

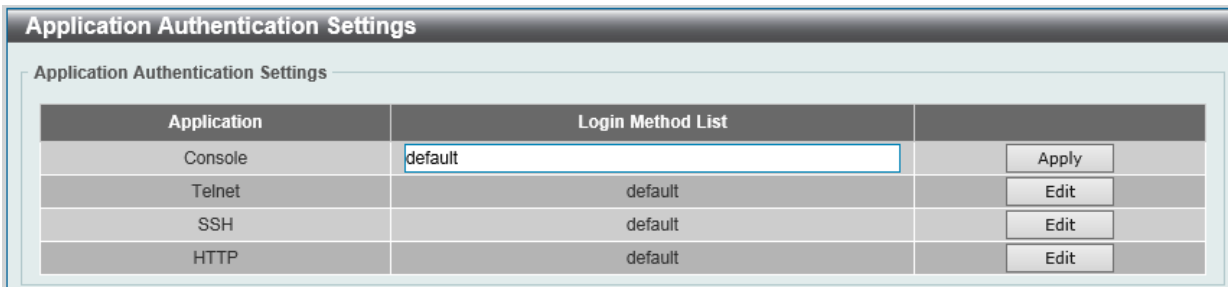


図 12-20　Application Authentication Settings (Edit) 画面

画面に表示される項目：

項目	説明
Login Method List	指定エントリの「Edit」ボタンをクリックし編集を行います。使用するログインメソッドリスト名を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。

Application Accounting Settings（アプリケーションアカウント設定）

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。

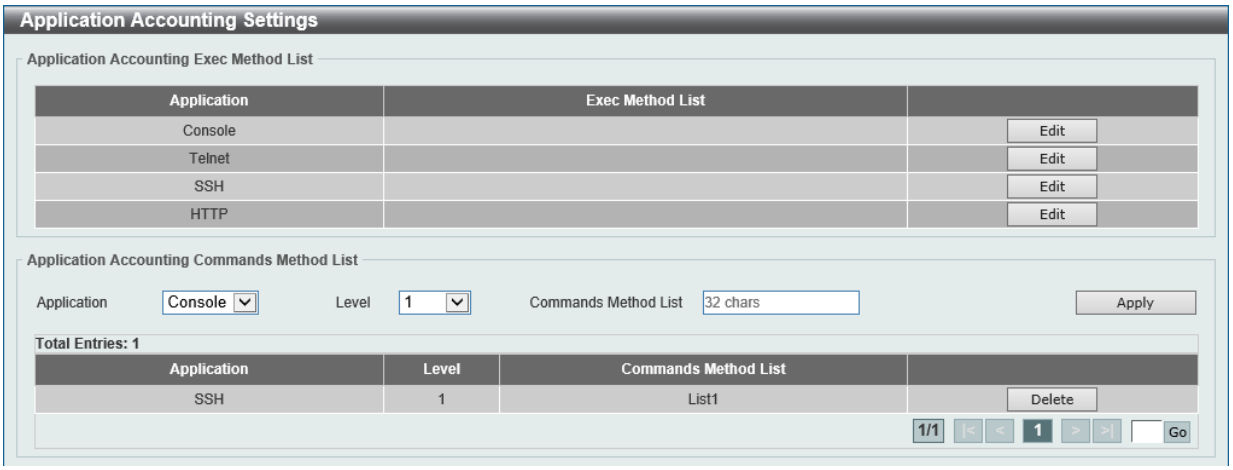


図 12-21　Application Accounting Settings 画面

「Edit」をクリックし、以下の画面で指定エントリの設定を行います。

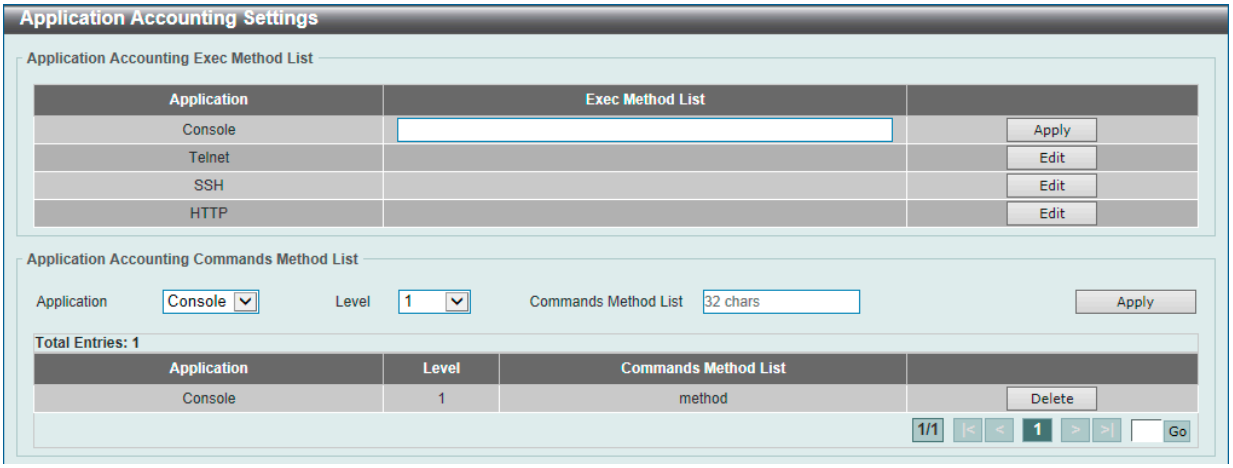


図 12-22　Application Accounting Settings (Edit) 画面

画面に表示される項目：

項目	説明
Application Accounting Exec Method List	
Exec Method List	「Edit」をクリックし、使用する EXEC メソッドリスト名を入力します。
Application Accounting Commands Method List	
Application	使用するアプリケーションを選択します。 • 選択肢：「Console」「Telnet」「SSH」
Level	権限レベルを指定します。 • 設定可能範囲：1-15
Commands Method List	使用するコマンドメソッドリスト名を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Authentication Settings（認証設定）

AAA ネットワークと EXEC 認証設定を行います。

Security > AAA > Authentication Settings の順にメニューをクリックし、以下の画面を表示します。

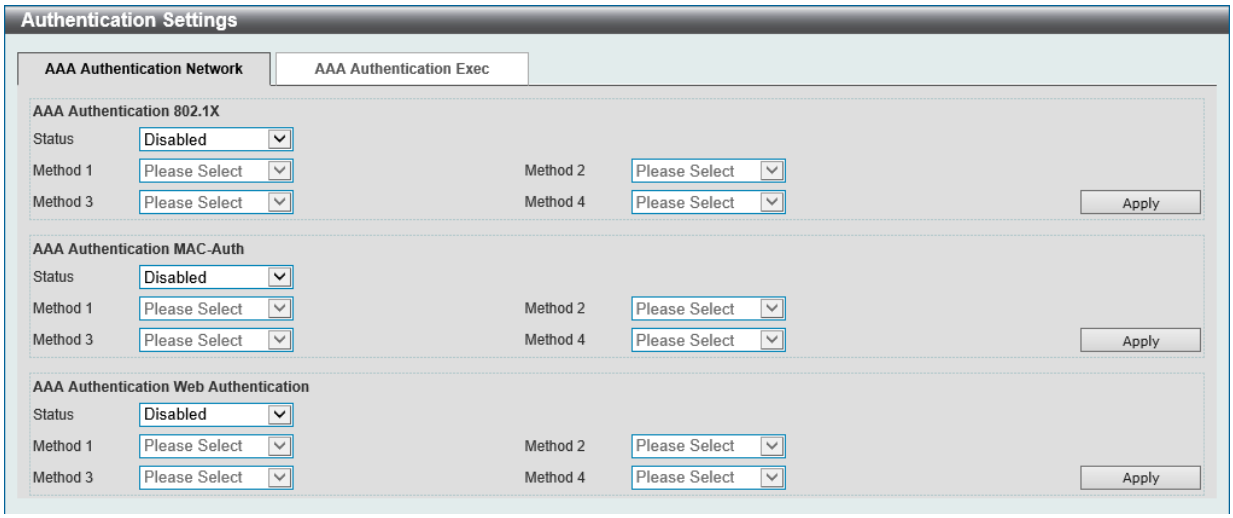


図 12-23　Authentication Settings 画面 -AAA Authentication Network タブ

「AAA Authentication Network」タブ

「AAA Authentication Network」タブ内の設定を行います。

画面に表示される項目：

項目	説明
AAA Authentication 802.1X	
Status	AAA 802.1X 認証ステータスを有効 / 無効に設定します。
Method 1 ～ 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- 認証にローカルデータベースを使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバ設定で定義されたサーバを使用します。
AAA Authentication MAC-Auth	
Status	AAA MAC 認証ステータスを有効 / 無効に設定します。
Method 1 ～ 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- 認証にローカルデータベースを使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。
AAA Authentication Web Authentication	
Status	AAA Web 認証ステータスを有効 / 無効に設定します。
Method 1 ～ 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- 認証にローカルデータベースを使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　802.1X 機能において、Local DB を指定した場合、EAP-MD5 のみをサポートします。

「AAA Authentication Exec」タブ

「AAA Authentication Exec」タブをクリックして、タブ内の設定を行います。

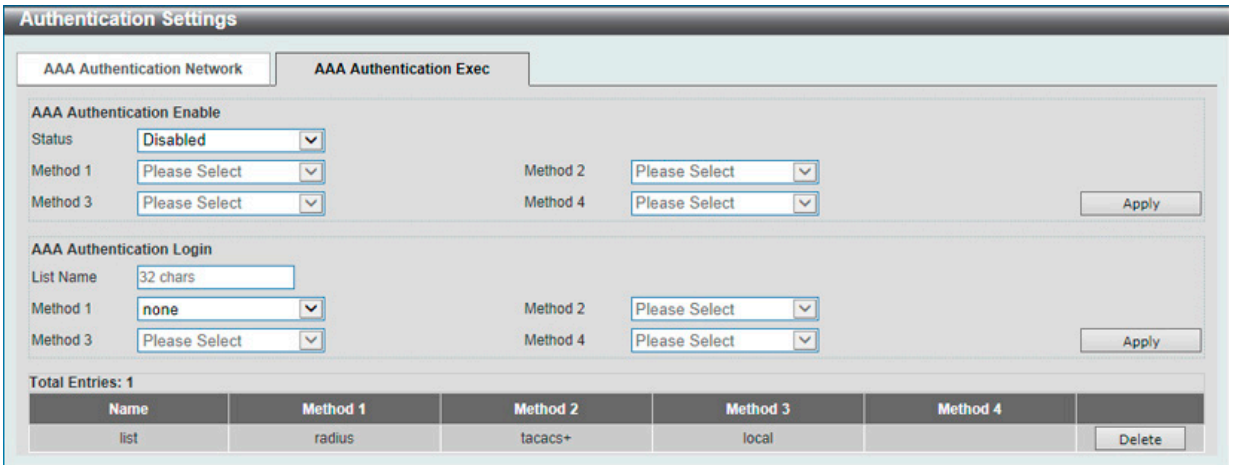


図 12-24　Authentication Settings 画面 -AAA Authentication Exec タブ

画面に表示される項目：

項目	説明
AAA Authentication Enable	
Status	AAA 認証 Enable ステータスを有効 / 無効に設定します。
Method 1 ～ 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「enable」- ローカル Enable パスワードを認証に使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。 • 「tacacs+」- TACACS+ サーバ設定で定義されたサーバを使用します。
AAA Authentication Login（AAA 認証ログイン）	
List Name	AAA 認証ログインオプションで使用するメソッドリスト名を入力します。
Method 1 ～ 4	使用するメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- ローカルデータベースを認証に使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。 • 「tacacs+」- TACACS+ サーバ設定で定義されたサーバを使用します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

Accounting Settings（アカウンティング設定）

アカウンティングの設定を行います。

Security > AAA > Accounting Settings の順にメニューをクリックします。

「AAA Accounting Network」タブ

「AAA Accounting Network」タブをクリックして、以下の画面を表示します。

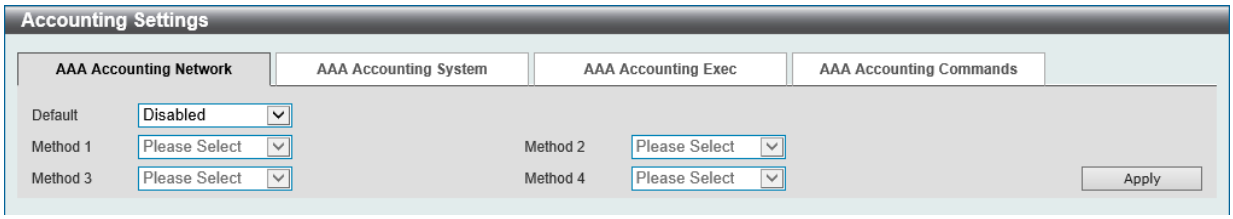


図 12-25　Accounting Settings 画面 - AAA Accounting Network タブ

画面に表示される項目：

項目	説明
Default	デフォルトのメソッドリストの使用を有効 / 無効に指定します。
Method 1 ～ 4	使用するメソッドリストを選択します。「None」オプションは「Method1」のみで設定可能です。 • 選択肢：「None」「Group」「RADIUS」「TACACS+」

「Apply」ボタンをクリックして、設定内容を適用します。

「AAA Accounting System」タブ

「AAA Accounting System」タブをクリックして、以下の画面を表示します。

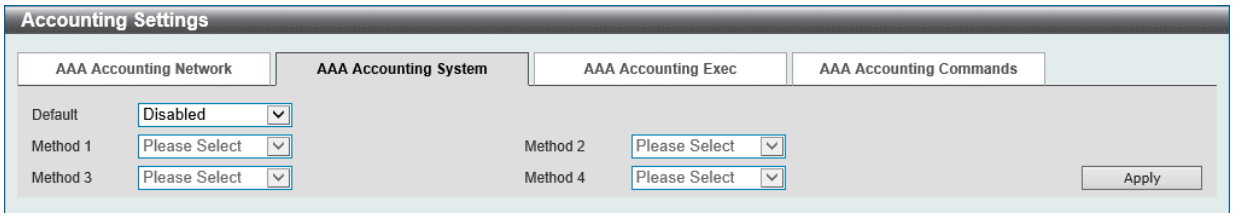


図 12-26　Accounting Settings 画面 - AAA Accounting System タブ

画面に表示される項目：

項目	説明
Default	デフォルトのメソッドリストの使用を有効 / 無効に指定します。
Method 1 ～ 4	使用するメソッドリストを選択します。「None」オプションは「Method1」のみで設定可能です。 • 選択肢：「None」「Group」「RADIUS」「TACACS+」

「Apply」ボタンをクリックして、設定内容を適用します。

「AAA Accounting Exec」タブ

「AAA Accounting Exec」タブをクリックして、以下の画面を表示します。

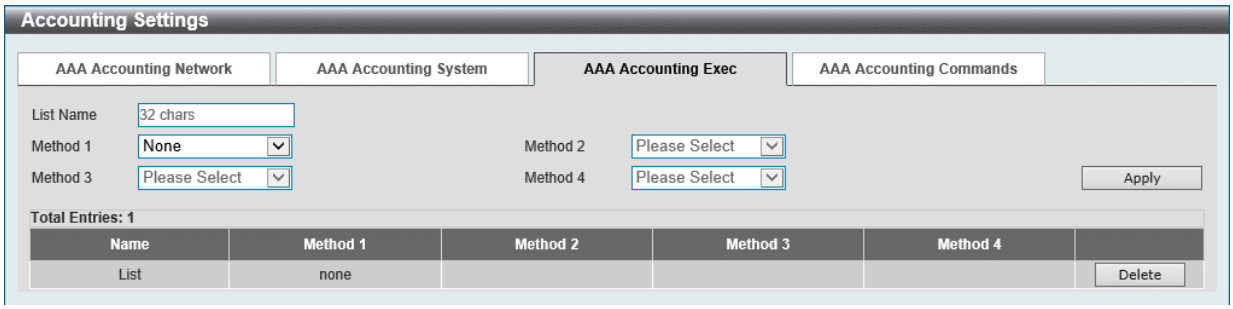


図 12-27　Accounting Settings 画面 - AAA Accounting Exec タブ

画面に表示される項目：

項目	説明
List Name	AAA アカウンティング EXEC オプションで使用するメソッドリスト名を入力します。
Method 1 ～ 4	使用するメソッドリストを選択します。「None」オプションは「Method1」のみで設定可能です。 • 選択肢：「None」「Group」「RADIUS」「TACACS+」

「Apply」ボタンをクリックして、設定内容を適用します。

「Delete」ボタンをクリックして、指定エントリを削除します。

「AAA Accounting Commands」タブ

「AAA Accounting Commands」タブをクリックして、以下の画面を表示します。

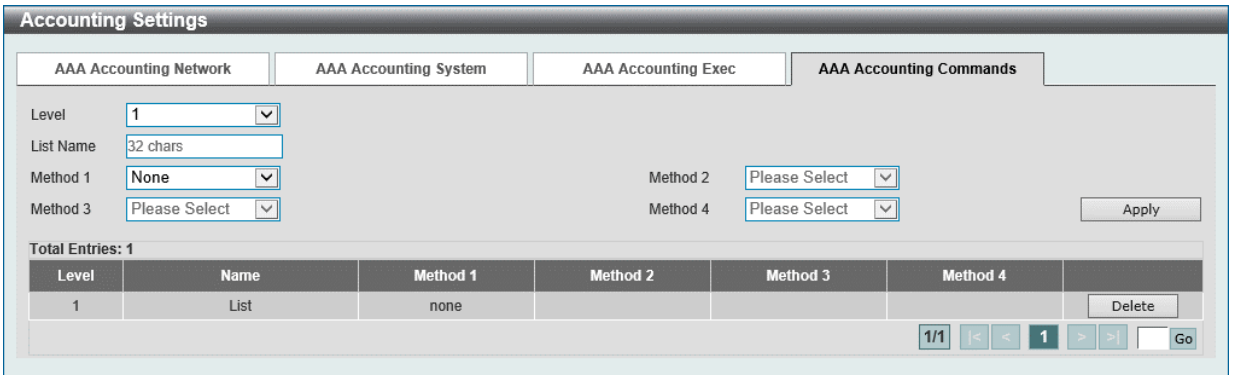


図 12-28　Accounting Settings 画面 - AAA Accounting Commands タブ

画面に表示される項目：

項目	説明
Level	権限レベルを指定します。 • 設定可能範囲：1-15
List Name	AAA アカウンティングコマンドオプションで使用するメソッドリスト名を入力します。
Method 1 ～ 4	使用するメソッドリストを選択します。「None」オプションは「Method1」のみで設定可能です。 • 選択肢：「None」「Group」「TACACS+」

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

RADIUS（RADIUS 設定）

RADIUS サーバの設定を行います。

RADIUS Global Settings（RADIUS グローバル設定）

RADIUS サーバのグローバルステータスを設定します。

Security > RADIUS > RADIUS Global Settings の順にメニューをクリックし、以下の画面を表示します。

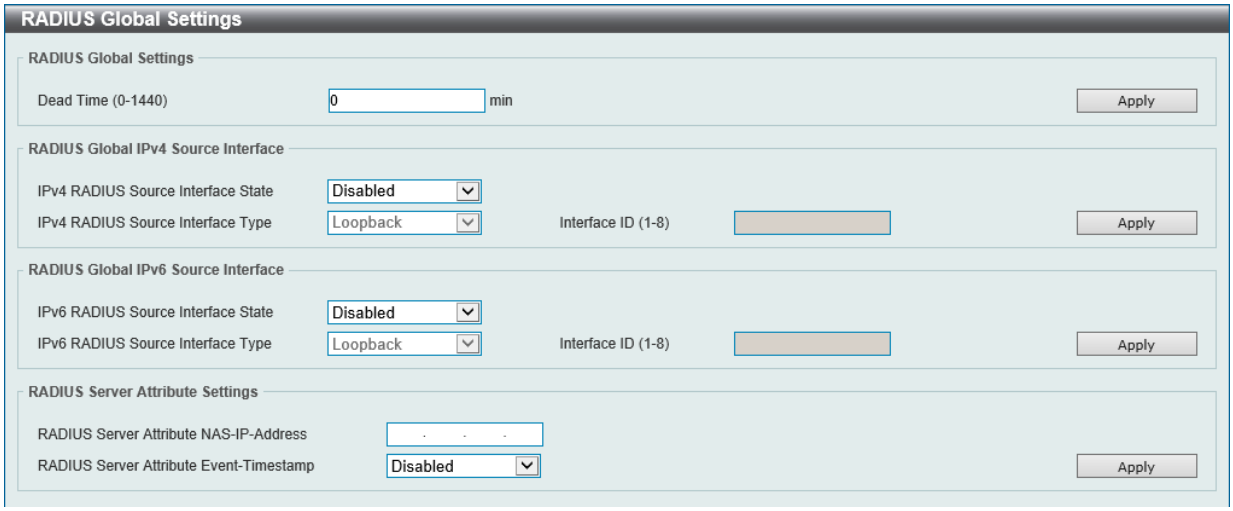


図 12-29　RADIUS Global Settings 画面

画面に表示される項目：

項目	説明
RADIUS Global Settings	
Dead Time	デッドタイムの設定を行います。0 に設定されている場合、応答しないサーバは「Dead」として認識されることはありません。本設定により、応答しないサーバホストのエントリはスキップされ、認証プロセス時間が改善されます。システムが認証サーバへ認証を行う際、一度に一台のサーバへの認証が試みられます。接続を試みたサーバが応答しない場合、システムは次のサーバに対して接続を試行します。応答しないサーバが検出されると、当該サーバはダウン状態として認識され、「デッドタイム」タイマが開始されます。それ以降のリクエスト認証はデッドタイム時間が経過するまでスキップされます。 • 設定可能範囲：0-1440（分） • 初期値：0（分）
RADIUS Global IPv4 Source Interface	
IPv4 RADIUS Source Interface State	IPv4 RADIUS 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv4 RADIUS Source Interface Type	IPv4 RADIUS 送信元インタフェースの種類を選択します。 •「Loopback」- IPv4 RADIUS 送信元インタフェースの種類をループバックに指定します。 •「MGMT」- IPv4 RADIUS 送信元インタフェースの種類を MGMT に指定します。 •「VLAN」- IPv4 RADIUS 送信元インタフェースの種類を VLAN に指定します。
Interface ID	IPv4RADIUS 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）
RADIUS Global IPv6 Source Interface	
IPv6 RADIUS Source Interface State	IPv6 RADIUS 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv6 RADIUS Source Interface Type	IPv6 RADIUS 送信元インタフェースの種類を選択します。 •「Loopback」- IPv6 RADIUS 送信元インタフェースの種類をループバックに指定します。 •「MGMT」- IPv6 RADIUS 送信元インタフェースの種類を MGMT に指定します。 •「VLAN」- IPv6 RADIUS 送信元インタフェースの種類を VLAN に指定します。
Interface ID	IPv6 RADIUS 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）
RADIUS Server Attribute Settings	
RADIUS Server Attribute NAS-IP-Address	RADIUS パケットに含まれる RADIUS サーバ属性 4（NAS-IP アドレス）を指定します。
RADIUS Server Attribute Event-Timestamp	RADIUS サーバ属性のイベントタイムスタンプ機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

RADIUS Server Settings（RADIUS サーバの設定）

RADIUS サーバ設定を行います。

Security > RADIUS > RADIUS Server Settings をクリックし、以下の画面を表示します。

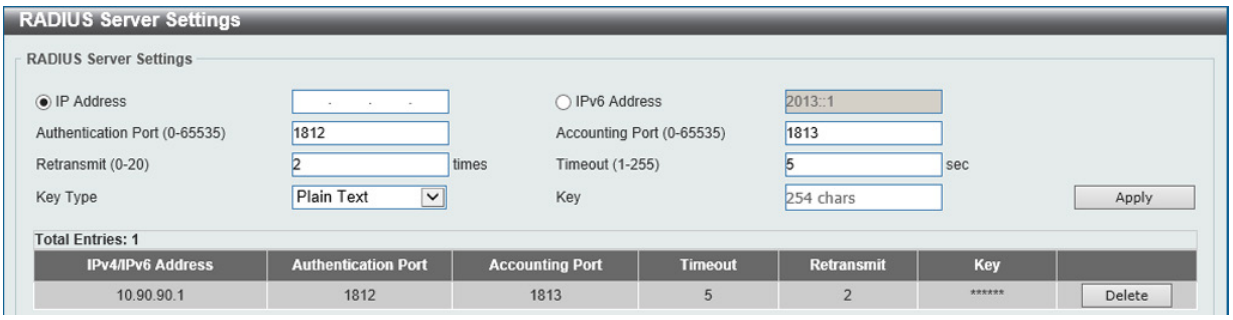


図 12-30　RADIUS Server Settings 画面

画面に表示される項目：

項目	説明
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。
Authentication Port	認証ポート番号を入力します。認証を使用しない場合は「0」を指定します。 • 設定可能範囲：0-65535 • 初期値：1812
Accounting Port	アカウンティングポート番号を入力します。アカウンティングを使用しない場合は「0」を指定します。 • 設定可能範囲：0-65535 • 初期値：1813
Retransmit	再送回数を設定します。このオプションを無効にする場合、「0」を指定します。 • 設定可能範囲：0-20（回） • 初期値：2（回）
Timeout	タイムアウト時間を設定します。 • 設定可能範囲：1-255（秒） • 初期値：5（秒）
Key Type	使用する鍵の種類を選択します。 • 選択肢：「Plain Text（平文）」「Encrypted（暗号化）」
Key	RADIUS サーバとの通信で使用する鍵を指定します。（254 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

RADIUS Group Server Settings（RADIUS グループサーバの設定）

RADIUS グループサーバの表示、設定を行います。

Security > RADIUS > RADIUS Group Server Settings をクリックし、以下の画面を表示します。



図 12-31　RADIUS Group Server Settings 画面

画面に表示される項目：

項目	説明
Group Server Name	RADIUS グループサーバ名を入力します。（32 文字以内）
IPv4 Address	RADIUS 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。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Show Detail」ボタンをクリックして、指定エントリの詳細について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

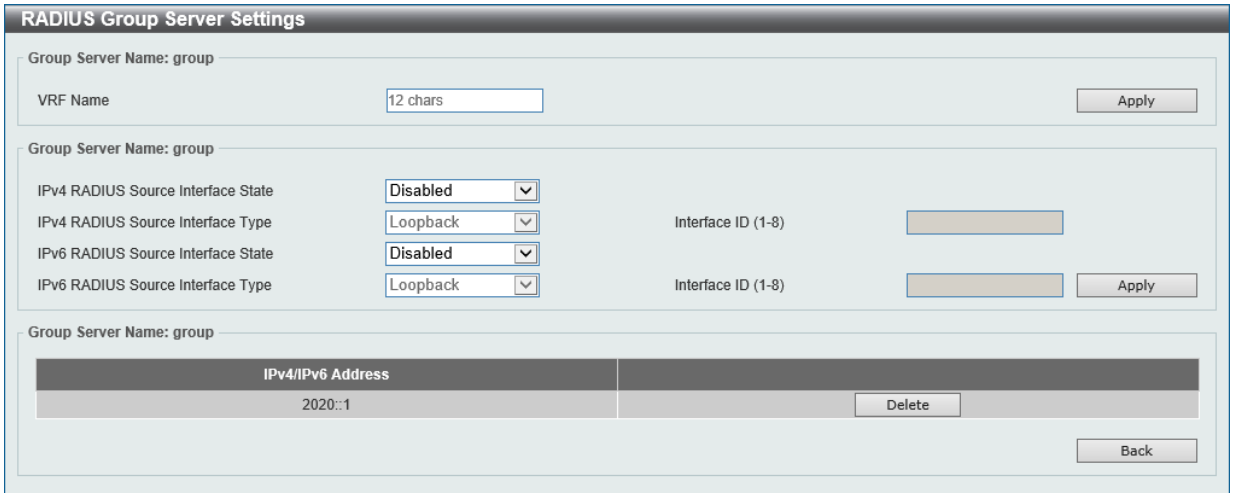


図 12-32　RADIUS Group Server Settings (Detail) 画面

画面に表示される項目：

項目	説明
Group Server Name: < グループサーバ名 >	
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Group Server Name: < グループサーバ名 >	
IPv4 RADIUS Source Interface State	IPv4 RADIUS 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv4 RADIUS Source Interface Type	IPv4 RADIUS 送信元インタフェースの種類を選択します。 • 「Loopback」- IPv4 RADIUS 送信元インタフェースの種類をループバックに指定します。 • 「MGMT」- IPv4 RADIUS 送信元インタフェースの種類を MGMT に指定します。 • 「VLAN」- IPv4 RADIUS 送信元インタフェースの種類を VLAN に指定します。
Interface ID	IPv4 RADIUS 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）
IPv6 RADIUS Source Interface State	IPv6 RADIUS 送信元インタフェースのステータスを有効 / 無効に設定します。

項目	説明
IPv6 RADIUS Source Interface Type	IPv6 RADIUS 送信元インタフェースの種類を選択します。 • 「Loopback」- IPv6 RADIUS 送信元インタフェースの種類をループバックに指定します。 • 「MGMT」- IPv6 RADIUS 送信元インタフェースの種類を MGMT に指定します。 • 「VLAN」- IPv6 RADIUS 送信元インタフェースの種類を VLAN に指定します。
Interface ID	IPv6 RADIUS 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
前の画面に戻るには、「Back」ボタンをクリックします。

RADIUS Statistic（RADIUS 統計情報）

RADIUS 統計情報を表示します。

Security > RADIUS > RADIUS Statistic をクリックし、以下の画面を表示します。

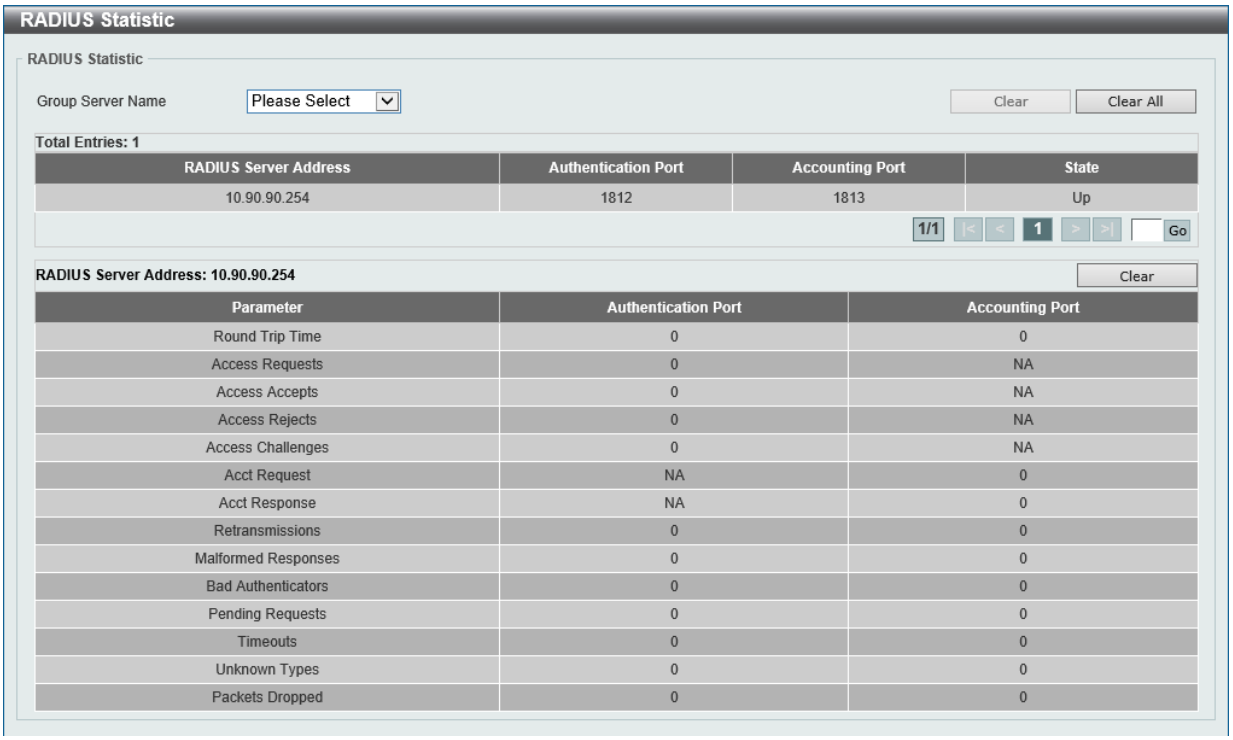


図 12-33　RADIUS Statistic 画面

画面に表示される項目：

項目	説明
Group Server Name	統計情報を削除する RADIUS グループサーバ名を選択します。

「Clear」ボタンをクリックして、選択に基づいて情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

TACACS+（TACACS+ 設定）

TACACS+ サーバの設定を行います。

TACACS+ Global Settings（TACACS+ サーバグローバル設定）

TACACS+ サーバのグローバルステータスを設定します。

Security > TACACS+ > TACACS+ Global Settings をクリックし、以下の画面を表示します。

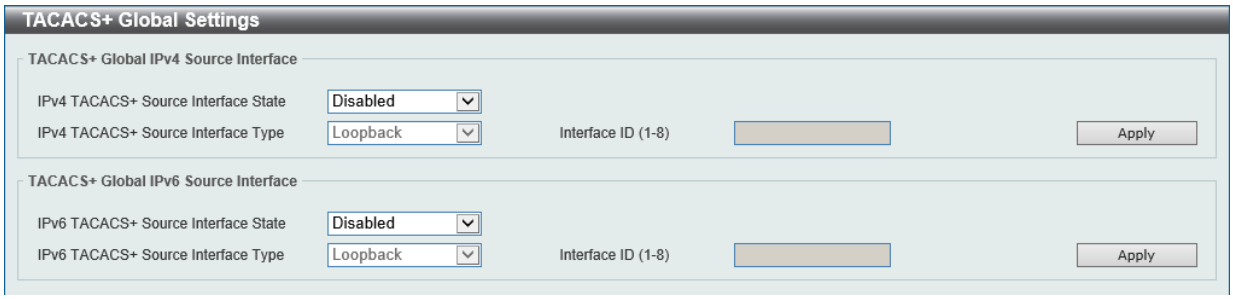


図 12-34　TACACS+ Global Settings 画面

画面に表示される項目：

項目	説明
TACACS+ Global IPv4 Source Interface	
IPv4 TACACS+ Source Interface State	IPv4 TACACS+ 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv4 TACACS+ Source Interface Type	IPv4 TACACS+ 送信元インタフェースの種類を選択します。 • 「Loopback」- IPv4 TACACS+ 送信元インタフェースの種類をループバックに指定します。 • 「MGMT」- IPv4 TACACS+ 送信元インタフェースの種類を MGMT に指定します。 • 「VLAN」- IPv4 TACACS+ 送信元インタフェースの種類を VLAN に指定します。
Interface ID	IPv4 TACACS+ 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）
TACACS+ Global IPv6 Source Interface	
IPv6 TACACS+ Source Interface State	IPv6 TACACS+ 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv6 TACACS+ Source Interface Type	IPv6 TACACS+ 送信元インタフェースの種類を選択します。 • 「Loopback」- IPv6 TACACS+ 送信元インタフェースの種類をループバックに指定します。 • 「MGMT」- IPv6 TACACS+ 送信元インタフェースの種類を MGMT に指定します。 • 「VLAN」- IPv6 TACACS+ 送信元インタフェースの種類を VLAN に指定します。
Interface ID	IPv6 TACACS+ 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）

「Apply」ボタンをクリックして、設定内容を適用します。

TACACS+ Server Settings（TACACS+ サーバの設定）

TACACS+ サーバの表示、設定を行います。

Security > TACACS+ > TACACS+ Server Settings をクリックし、以下の画面を表示します。

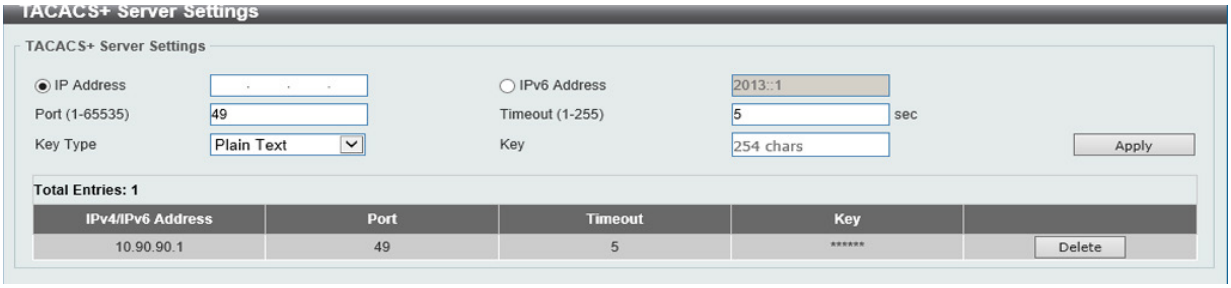


図 12-35　TACACS+ Server Settings 画面

画面に表示される項目：

項目	説明
IP Address	TACACS+ サーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ サーバの IPv6 アドレスを入力します。
Port	TACACS+ サーバのポート番号を入力します。 • 設定可能範囲：1-65535 • 初期値：49
Timeout	タイムアウト時間を設定します。 • 設定可能範囲：1-255（秒） • 初期値：5（秒）
Key Type	使用する鍵の種類を選択します。 • 選択肢：「Plain Text（平文）」「Encrypted（暗号化）」
Key	TACACS+ サーバとの通信で使用する鍵を指定します。（254 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

TACACS+ Group Server Settings（TACACS+ グループサーバの設定）

TACACS+ グループサーバの表示、設定を行います。

Security > TACACS+ > TACACS+ Group Server Settings をクリックし、以下の画面を表示します。

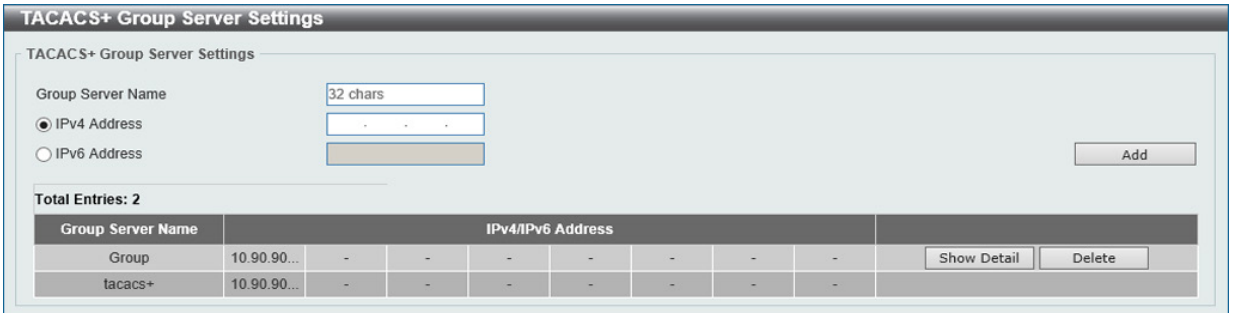


図 12-36　TACACS+ Group Server Settings 画面

画面に表示される項目：

項目	説明
Group Server Name	TACACS+ グループサーバ名を入力します。（32 文字以内）
IPv4 Address	TACACS+ グループサーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ グループサーバの IPv6 アドレスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Show Detail」ボタンをクリックして、TACACS+ グループサーバの詳細情報について表示します。

「Show Detail」をクリックすると、以下の画面が表示されます。

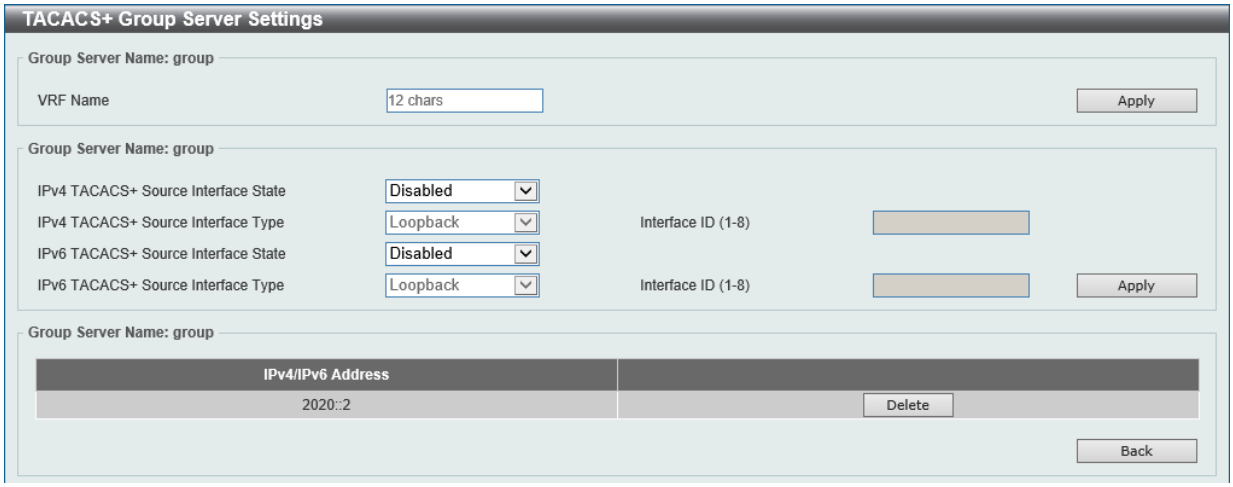


図 12-37　TACACS+ Group Server Settings（Show Detail）画面

画面に表示される項目：

項目	説明
Group Server Name: < グループサーバ名 >	
VRF Name（EI モードのみ）	VRF インスタンス名を入力します。（12 文字以内）
Group Server Name: < グループサーバ名 >	
IPv4 TACACS+ Source Interface State	IPv4 TACACS+ 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv4 TACACS+ Source Interface Type	IPv4 TACACS+ 送信元インタフェースの種類を選択します。 • 「Loopback」- IPv4 TACACS+ 送信元インタフェースの種類をループバックに指定します。 • 「MGMT」- IPv4 TACACS+ 送信元インタフェースの種類を MGMT に指定します。 • 「VLAN」- IPv4 TACACS+ 送信元インタフェースの種類を VLAN に指定します。
Interface ID	IPv4 TACACS+ 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）
IPv6 TACACS+ Source Interface State	IPv6 TACACS+ 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv6 TACACS+ Source Interface Type	IPv6 TACACS+ 送信元インタフェースの種類を選択します。 • 「Loopback」- IPv6 TACACS+ 送信元インタフェースの種類をループバックに指定します。 • 「MGMT」- IPv6 TACACS+ 送信元インタフェースの種類を MGMT に指定します。 • 「VLAN」- IPv6 TACACS+ 送信元インタフェースの種類を VLAN に指定します。
Interface ID	IPv6 TACACS+ 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（Loopback 選択時）、0（MGMT 選択時）、1-4094（VLAN 選択時）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
前の画面に戻るには、「Back」ボタンをクリックします。

TACACS+ Statistic（TACACS+ 統計情報）

TACACS+ 統計情報を表示します。

Security > TACACS+ > TACACS+ Statistic をクリックし、以下の画面を表示します。

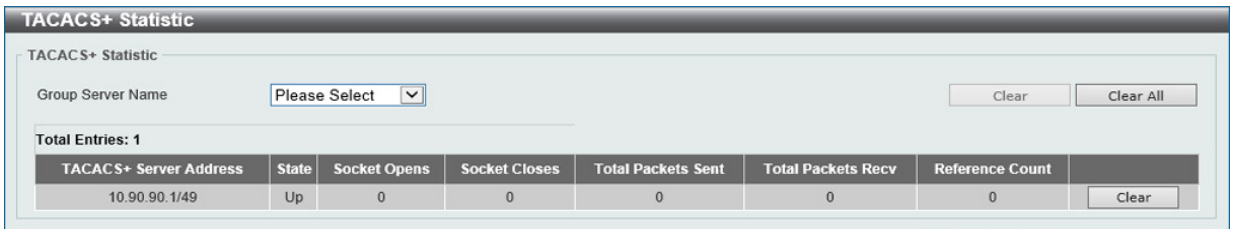


図 12-38　TACACS+ Statistic 画面

画面に表示される項目：

項目	説明
Group Server Name	統計情報を削除する TACACS+ グループサーバ名を選択します。

「Clear」ボタンをクリックして、選択に基づいて情報を消去します。
「Clear All」ボタンをクリックして、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びつけることにより、レイヤ間のデータ転送が可能になります。IP-MAC バインディングの主な目的は、スイッチにアクセスするユーザを制限することです。IP アドレスと MAC アドレスのペアについて、事前に設定したデータベースと比較を行い、認証クライアントのみがスイッチのポートアクセスできるようにします。もしくは DHCP スヌーピングが有効な場合において、スイッチがスヌーピング DHCP パケットから自動的に IP/MAC ペアを学習し、IMPB ホワイトリストに保存することで、認証クライアントのポートアクセスが可能になります。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。本機能はポートベースであるため、ポートごとに本機能を有効 / 無効にすることができます。

IPv4

DHCPv4 Snooping（DHCPv4 スヌーピング）

■ DHCP Snooping Global Settings（DHCP スヌーピンググローバル設定）

DHCP スヌーピングのグローバル設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings の順にクリックして、以下の画面を表示します。



図 12-39　DHCP Snooping Global Settings 画面

画面に表示される項目：

項目	説明
DHCP Snooping	DHCP スヌーピングのグローバルステータスを有効 / 無効に設定します。
Information Option Allow Untrusted	信頼されていないインタフェースにおけるリレーオプション 82 付き DHCP パケットの許可のグローバルステータスを有効 / 無効に設定します。
Source MAC Verification	クライアントのハードウェアアドレスと DHCP パケットの送信元 MAC アドレスが一致しているかどうかの検証を有効 / 無効に設定します。
Station Move Deny	DHCP スヌーピングの端末移動拒否（Station Move Deny）を有効 / 無効に設定します。 端末移動を有効（本機能を無効）にすると、指定ポート上で同じ VLAN ID と MAC アドレスを持つダイナミック DHCP バインディングエントリは、同じ VLAN ID と MAC アドレスに属する新しい DHCP プロセスが検出された場合、他のポートへ移動することが可能です。

「Apply」ボタンをクリックして、設定内容を適用します。

■ DHCP Snooping Port Settings（DHCP スヌーピングポート設定）

DHCP スヌーピングポートの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings の順にクリックして、以下の画面を表示します。

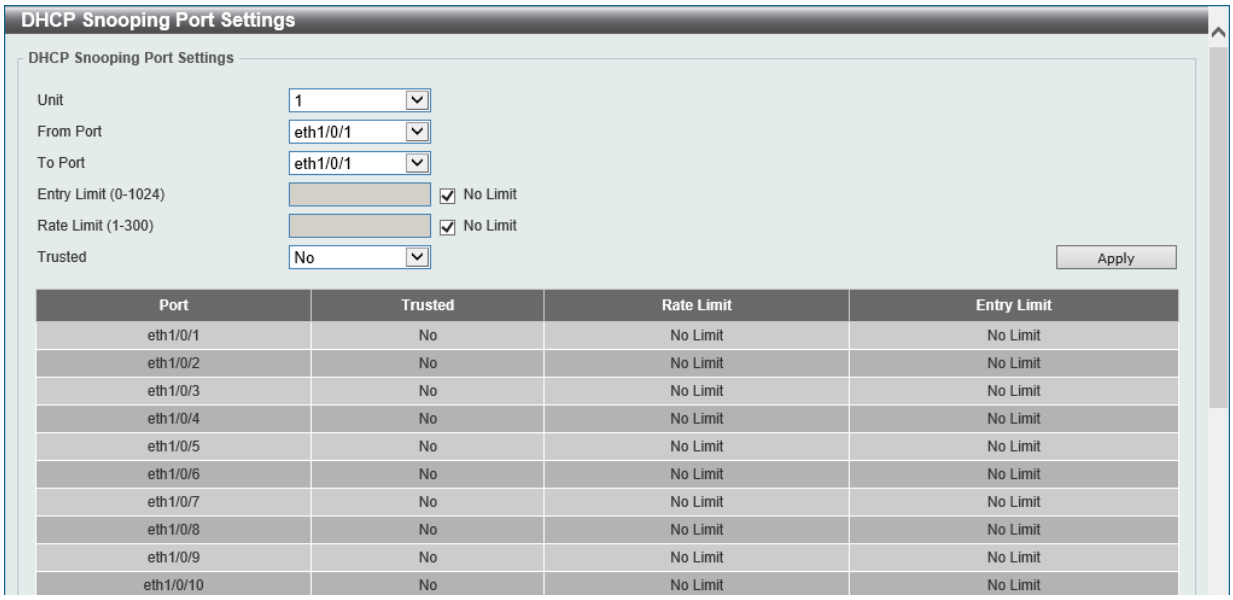


図 12-40　DHCP Snooping Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Entry Limit	エントリリミットの値を入力します。「No Limit」にチェックをすると、本機能は無効になります。 • 設定可能範囲：0-1024
Rate Limit	レートリミットの値を入力します。「No Limit」にチェックをすると、本機能は無効になります。 • 設定可能範囲：1-300
Trusted	信頼済みオプションを選択します。DHCP サーバや他のスイッチなどに接続しているポートは信頼済みインタフェースとして設定される必要があります。DHCP クライアントに接続しているポートは信頼されていないポートとして設定します。DHCP スヌーピングは DHCP サーバと信頼されていないインタフェースの間でファイアウォールとして動作します。 • 選択肢：「No」「Yes」

「Apply」ボタンをクリックして、設定内容を適用します。

DHCP Snooping VLAN Settings（DHCP スヌーピング VLAN 設定）

DHCP スヌーピング VLAN の設定、表示を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings の順にクリックして、以下の画面を表示します。

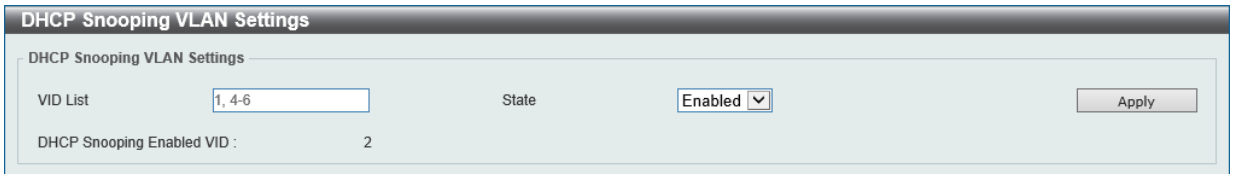


図 12-41　DHCP Snooping VLAN Settings 画面

画面に表示される項目：

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	DHCP スヌーピング VLAN を有効 / 無効に指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

■ DHCP Snooping Database（DHCP スヌーピングデータベース）

DHCP スヌーピングデータベースの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database の順にクリックして、以下の画面を表示します。

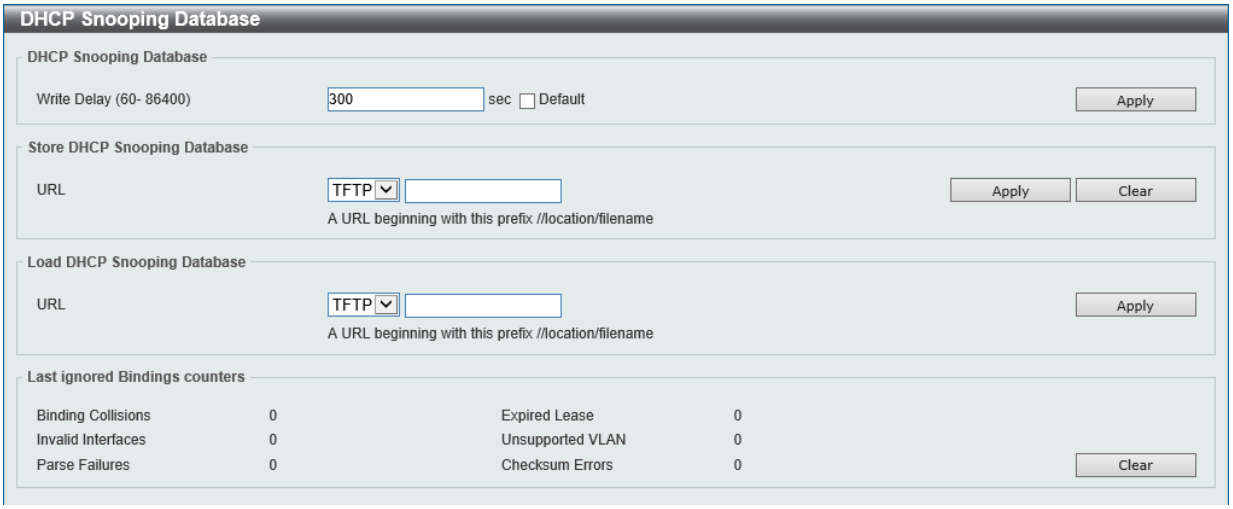


図 12-42　DHCP Snooping Database 画面

画面に表示される項目：

項目	説明
DHCP Snooping Database	
Write Delay	書き込み遅延時間の値を入力します。 • 設定可能範囲：60-86400（秒） • 初期値：300（秒）
Store DHCP Snooping Database	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースの保存先 URL を入力します。 • 選択肢：「TFTP」「FTP」「Flash」
Load DHCP Snooping Database	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースの読み込み元 URL を入力します。 • 選択肢：「TFTP」「FTP」「Flash」

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、カウンタ情報を消去します。

■ DHCP Snooping Binding Entry（DHCP スヌーピングバインディングエントリ設定）

DHCP スヌーピングバインディングエントリの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry の順にクリックして、以下の画面を表示します。

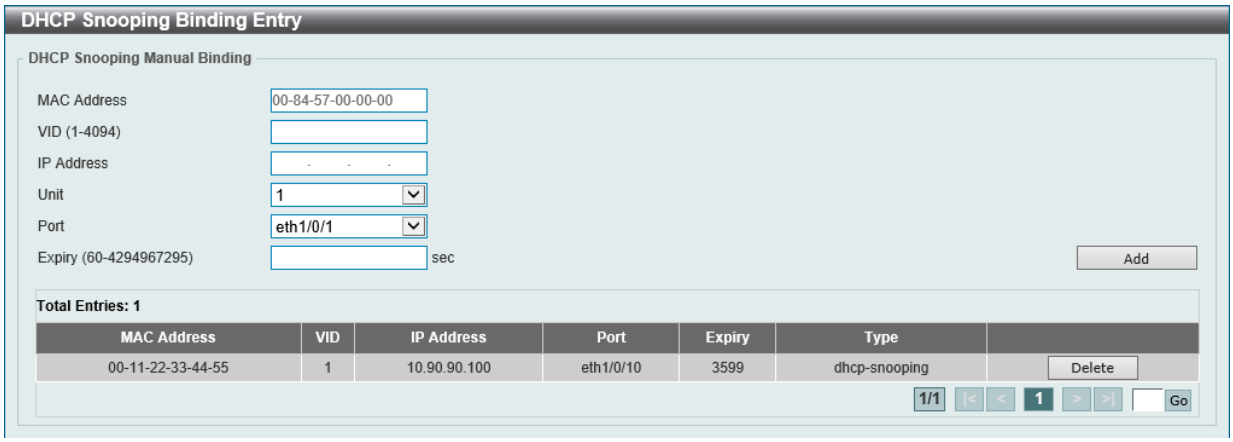


図 12-43　DHCP Snooping Binding Entry 画面

画面に表示される項目：

項目	説明
MAC Address	DHCP スヌーピングバインディングエントリの MAC アドレスを入力します。
VID	DHCP スヌーピングバインディングエントリの VLAN ID を入力します。 • 設定可能範囲：1-4094
IP Address	DHCP スヌーピングバインディングエントリの IP アドレスを入力します。
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Expiry	有効期限を入力します。 • 設定可能範囲：60-4294967295（秒）

「Add」ボタンをクリックして、入力した情報を基に新しいエントリを追加します。
「Delete」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Dynamic ARP Inspection（ダイナミック ARP インスペクション）

■ ARP Access List（ARP アクセスリスト）

ARP アクセスリストの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List の順にクリックして、以下の画面を表示します。

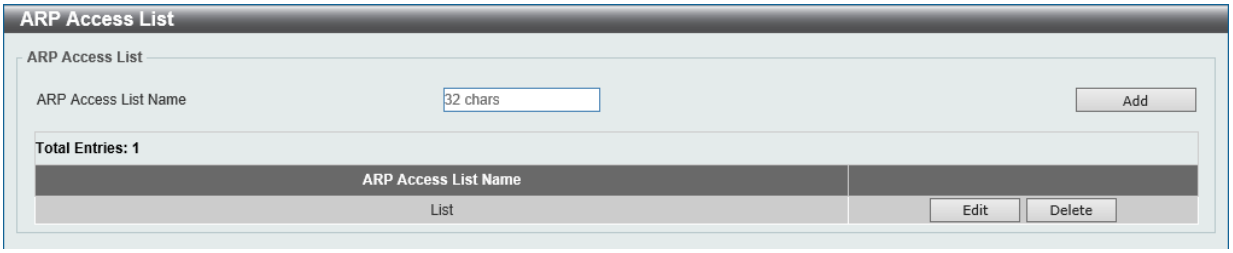


図 12-44　ARP Access List 画面

画面に表示される項目：

項目	説明
ARP Access List Name	ARP アクセスリスト名を入力します。（32 文字以内）

「Add」ボタンをクリックして、入力した情報を基に新しいエントリを追加します。
「Delete」ボタンをクリックして、指定エントリを削除します。

エントリの編集

「Edit」ボタンをクリックして指定のエントリを編集します。以下の画面が表示されます。

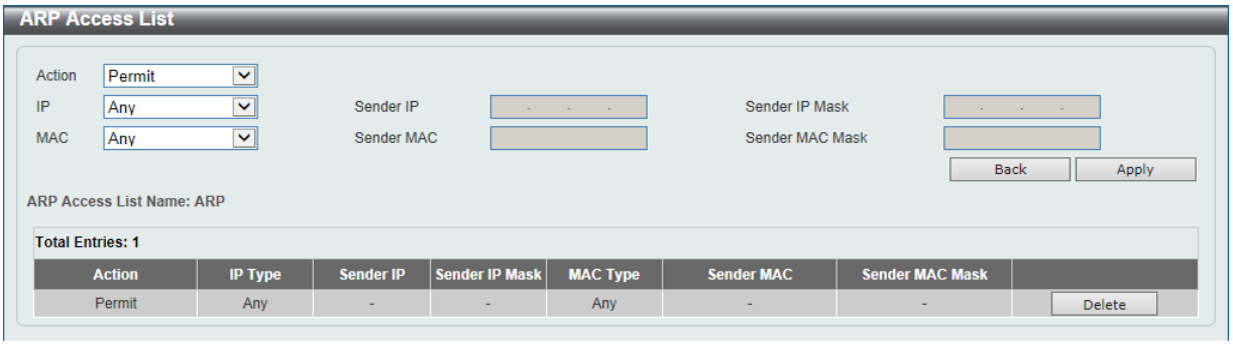


図 12-45　ARP Access List（Edit）画面

画面に表示される項目：

項目	説明
Action	実行するアクションを指定します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
IP	送信元 IP アドレスの種類を指定します。 • 選択肢：「Any」「Host」「IP with Mask」
Sender IP	IP アドレスの種類として「Host」「IP with Mask」を選択した場合、使用する送信元 IP アドレスを入力します。
Sender IP Mask	「IP with Mask」を選択した場合、使用する送信元 IP マスクを入力します。
MAC	送信元 MAC アドレスの種類を指定します。 • 選択肢：「Any」「Host」「MAC with Mask」
Sender MAC	MAC アドレスの種類として「Host」「MAC with Mask」を選択した場合、使用する送信元 MAC アドレスを入力します。
Sender MAC Mask	「MAC with Mask」を選択した場合、使用する送信元 MAC マスクを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。
「Delete」ボタンをクリックして、指定エントリを削除します。

■ ARP Inspection Settings（ARP インスペクション設定）

ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings の順にクリックして、以下の画面を表示します。

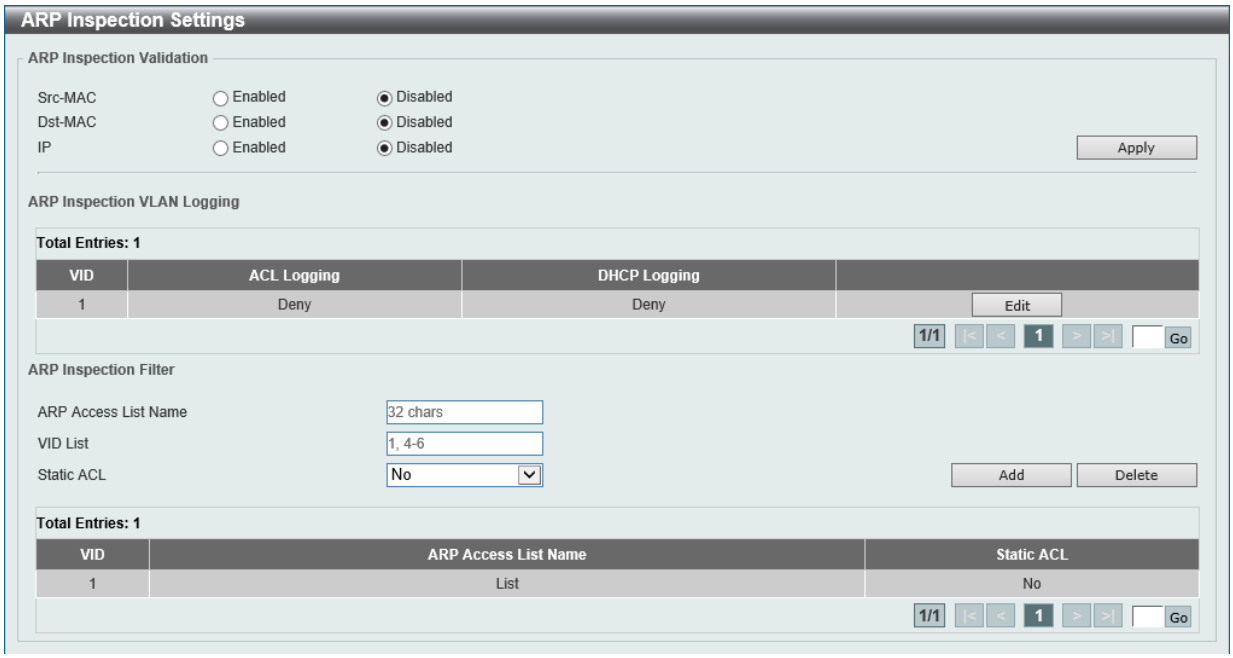


図 12-46　ARP Inspection Settings 画面

本画面の「ARP Inspection Validation」には以下の項目があります。

項目	説明
Src-MAC	送信元 MAC オプションについて有効 / 無効に設定します。本オプションを有効にすると、ARP リクエストおよび応答パケットをチェックし、ARP ペイロードに含まれる送信元 MAC アドレスに対してイーサネットヘッダ内の送信元 MAC アドレスの整合性を検証します。
Dst-MAC	宛先 MAC オプションについて有効 / 無効に設定します。本オプションを有効にすると、ARP 応答パケットをチェックし、ARP ペイロードに含まれる宛先 MAC アドレスに対してイーサネットヘッダ内の宛先 MAC アドレスの整合性を検証します。
IP	IP オプションについて有効 / 無効に設定します。本オプションを有効にすると、不正な IP アドレスや予期せぬ IP アドレスがないか ARP の body をチェックします。また、ARP ペイロードにおける IP アドレスの妥当性もチェックします。ARP リクエストとレスポンスの両方の送信元 IP、および ARP レスポンスのターゲット IP が検証されます。IP アドレス「0.0.0.0」「255.255.255.255」宛のパケットとすべての IP マルチキャストは破棄されます。送信元 IP アドレスはすべての ARP リクエストとレスポンスにおいてチェックされ、宛先 IP アドレスは ARP レスポンス内のみでチェックされます。

「Apply」ボタンをクリックして、設定内容を適用します。
「Edit」ボタンをクリックして、ACL/DHCP ロギングアクションを設定します。

本画面の「ARP Inspection Filter」には以下の項目があります。

項目	説明
ARP Access List Name	ARP アクセスリスト名を入力します。（32 文字以内）
VID List	使用する VLAN ID リストを指定します。
Static ACL	スタティック ACL を使用するか否かを選択します。

「Add」ボタンをクリックして、入力した情報を基に新しいエントリを追加します。
「Delete」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

■ ARP Inspection Port Settings（ARP インスペクションポート設定）

ポートでの ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings の順にクリックして、以下の画面を表示します。

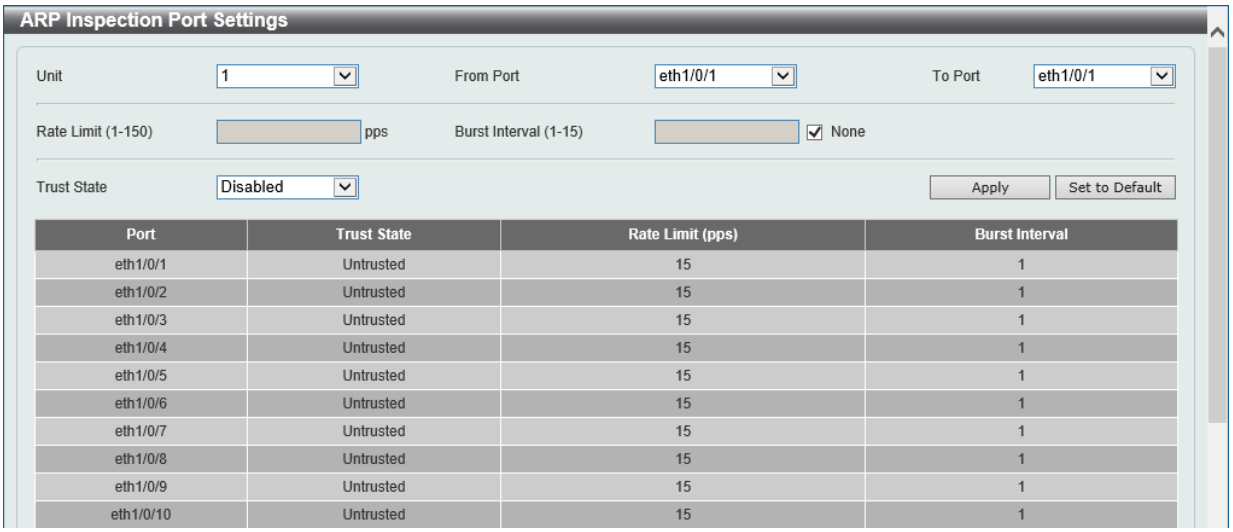


図 12-47　ARP Inspection Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Rate Limit	レート制限の値を入力します。 • 設定可能範囲：1- 150（パケット / 秒）
Burst Interval	バーストインターバルの値を入力します。「None」にチェックを入れるとオプションは無効になります。 • 設定可能範囲：1-15
Trust State	トラストステータスを有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

「Set to Default」ボタンをクリックすると、設定内容は初期値に変更されます。

■ ARP Inspection VLAN（ARP インスペクション VLAN 設定）

VLAN での ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN の順にクリックして、以下の画面を表示します。

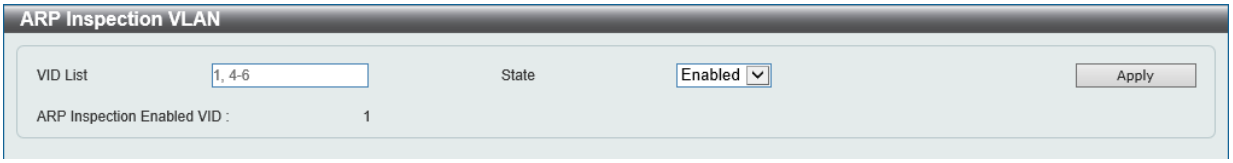


図 12-48　ARP Inspection VLAN 画面

画面に表示される項目：

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	指定 VLAN の ARP インスペクションについて有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

■ ARP Inspection Statistics（ARP インスペクション統計）

ARP インスペクションの統計情報の表示、消去を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics の順にクリックして、以下の画面を表示します。

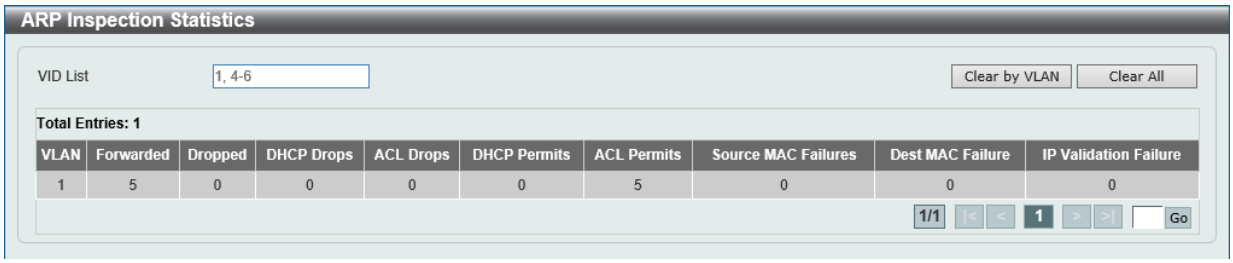


図 12-49　ARP Inspection Statistics 画面

画面に表示される項目：

項目	説明
VID List	統計情報を削除する VLAN ID リストを入力します。

「Clear by VLAN」ボタンをクリックして、入力した VLAN ID に基づき情報を消去します。
「Clear All」ボタンをクリックして、テーブルのすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

■ ARP Inspection Log（ARP インスペクションログ）

ARP インスペクションログ情報の表示、消去、設定を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log の順にクリックして、以下の画面を表示します。



図 12-50　ARP Inspection Log 画面

画面に表示される項目：

項目	説明
Log Buffer	使用するログバッファの値を入力します。 • 設定可能範囲：1-1024 • 初期値：32

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear Log」ボタンをクリックして、ログを消去します。

IP Source Guard（IP ソースガード）

IP Source Guard Port Settings（IP ソースガードポート設定）

IP ソースガード（IPSG）の表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings の順にクリックして、以下の画面を表示します。

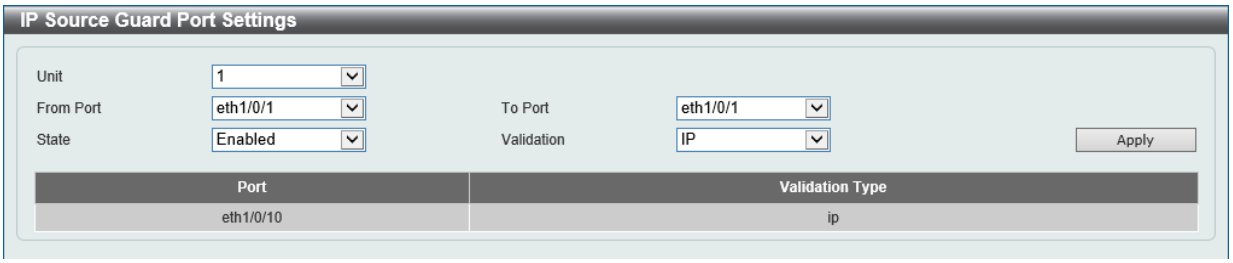


図 12-51　IP Source Guard Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポートを指定します。
State	指定ポートの IP ソースガードを有効 / 無効に設定します。
Validation	検証方法について選択します。 • 「IP」- 受信パケットの IP アドレスがチェックされます。 • 「IP-MAC」- 受信パケットの IP アドレスと MAC アドレスがチェックされます。

「Apply」ボタンをクリックして、設定内容を適用します。

■ IP Source Guard Binding（IP ソースガードバインディング）

IP ソースガードバインディングの表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding の順にクリックして、以下の画面を表示します。

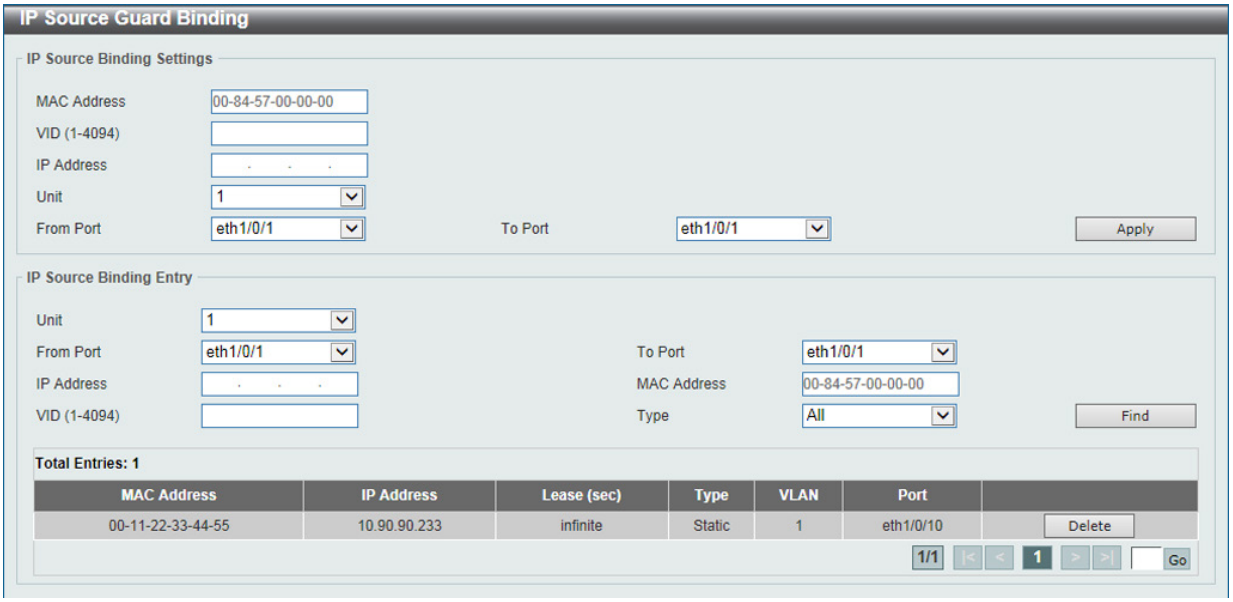


図 12-52　IP Source Guard Binding 画面

画面に表示される項目：

項目	説明
IP Source Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
IP Address	バインディングエントリの IP アドレスを入力します。
Unit	本設定を適用するユニットを指定します。
From Port/To Port	ポートの範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

項目	説明
IP Source Binding Entry	
Unit	バインディングエントリを検索するユニットを指定します。
From Port/To Port	バインディングエントリを検索するポートの範囲を指定します。
IP Address	バインディングエントリの IP アドレスを入力します。
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
Type	バインディングエントリの種類を選択します。 • 「All」- すべての DHCP バインディングエントリが表示されます。 • 「DHCP Snooping」- DHCP バインディングスヌーピングによって学習された IP ソースガードバインディングエントリが表示されます。 • 「Static」- 手動で設定した IP ソースガードバインディングエントリが表示されます。

「Find」ボタンをクリックして、入力した情報を基に指定のエントリを表示します。
「Delete」ボタンをクリックして、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

■ IP Source Guard HW Entry（IP ソースガードハードウェアエントリ）

IP ソースガードハードウェアエントリの表示を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry の順にクリックして、以下の画面を表示します。



図 12-53　IP Source Guard HW Entry 画面

画面に表示される項目：

項目	説明
Unit	検索対象のユニットを指定します。
From Port/To Port	検索対象のポート範囲を指定します。

「Find」ボタンをクリックして、指定した情報を基にエントリを表示します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Advanced Settings（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。

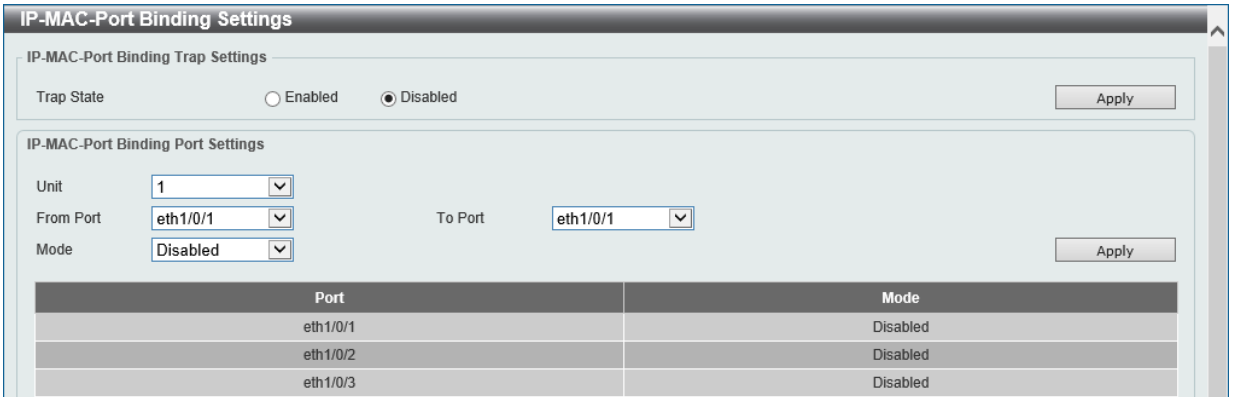


図 12-54　IP-MAC-Port Binding Settings 画面

画面に表示される項目：

項目	説明
IP-MAC-Port Binding Trap Settings	
Trap State	IP-MAC ポートバインディングのトラップ設定を有効 / 無効に指定します。
IP-MAC-Port Binding Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
Mode	アクセスコントロールのモードを選択します。 • 「Disabled」- 指定ポートで IP-MAC-Port バインディング機能が無効になります。 • 「Strict」- ホストが ARP/IP パケット送信後、それらのパケットがバインディングチェックを通過した後のみ、ポートへアクセスできます。有効な ARP/IP パケットが検出されるまで、L2 パケットはデフォルトでブロックされます。 • 「Loose」- ホストが ARP/IP パケット送信後、それらのパケットがバインディングチェックを通過しなかった場合にポートへのアクセスが拒否されます。不正な ARP/IP パケットが検出されるまで、L2 パケットはデフォルトで転送されます。 バインディングチェックを通過するには、送信元 IP アドレス / 送信元 MAC アドレス /VLAN ID/ 受信ポート番号が、IP ソースガードスタティックバインディングエントリ、または DHCP スヌーピングによって学習されたダイナミックバインディングエントリのいずれかのエントリに一致する必要があります。

「Apply」ボタンをクリックして、設定内容を適用します。

■ IP-MAC-Port Binding Blocked Entry（IP-MAC ポートバインディングブロックエントリ）

IP-MAC ポートバインディングブロックエントリの表示、消去を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry の順にクリックして、以下の画面を表示します。

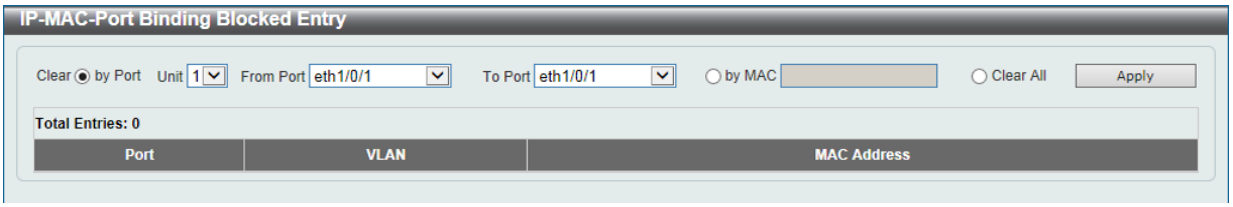


図 12-55　IP-MAC-Port Binding Blocked Entry 画面

画面に表示される項目：

項目	説明
Clear by Port	選択ポートに基づいたエントリテーブルをクリアします。
Unit	エントリを削除するユニットを指定します。
From Port/To Port	エントリを削除するポートを指定します。
Clear by MAC	指定した MAC アドレスに基づきエントリを消去します。項目欄に MAC アドレスを入力します。
Clear All	すべてのエントリを消去します。

「Apply」ボタンをクリックして、設定内容を適用します。

IPv6

IPv6 Snooping（IPv6 スヌーピング）

IPv6 スヌーピングについて表示、設定します。

Security > IMPB > IPv6 > IPv6 Snooping の順にクリックして、以下の画面を表示します。

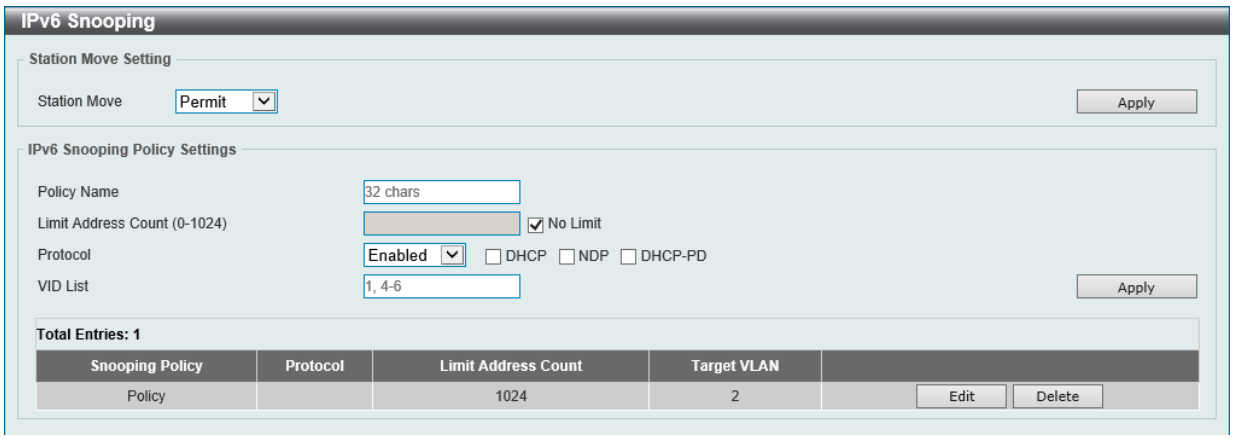


図 12-56　IPv6 Snooping 画面

画面に表示される項目：

項目	説明
Station Move Setting	
Station Move	ステーション移動について設定します。 • 「Permit（許可）」「Deny（拒否）」
IPv6 Snooping Policy Settings	
Policy Name	IPv6 スヌーピングポリシー名を入力します。（32 文字以内）
Limit Address Count	アドレスカウント制限の値を指定します。「No Limit」を指定するとアドレスカウント制限は無効になります。 • 設定可能範囲：0-1024 • 初期値：1024
Protocol	プロトコルステートを有効 / 無効に設定し、本ポリシーに対応するプロトコルを選択します。 • 「DHCP」- DHCPv6 パケットのアドレスがスヌーピングされます。 • 「NDP」- NDP パケットのアドレスがスヌーピングされます。 • 「DHCP-PD」- DHCPv6-PD パケットの IPv6 プレフィックスがスヌーピングされます。 DHCPv6 スヌーピング： アドレス割り当ての際に DHCPv6 クライアントとサーバ間の DHCPv6 パケットをスヌーピングします。DHCPv6 クライアントが有効な IPv6 アドレスを取得すると、DHCPv6 スヌーピングによってバインディングデータベースが作成されます。 ND スヌーピング： ステートレス自動設定による IPv6 アドレスと手動設定による IPv6 アドレスのための機能です。IPv6 アドレスを割り当てる前に、ホストは「Duplicate Address Detection」（DAD：重複アドレス検出）を実行する必要があります。ND スヌーピングは DAD メッセージ（DAD NS と DAD NA）を受信しバインディングデータベースを構築します。NDP パケット (NS と NA) は、ホストが到達可能かを判断しバインディングを削除するかどうかを決定するためにも使用されます。 DHCP-PD スヌーピング： Prefix Delegation（PD）の DHCPv6 スヌーピングを実行して、（IPv6 プレフィックスを割り当てられた）委任ルータと、対応する要求ルータの間のバインディングを設定します。このバインディングはパケット内の送信元プレフィックスを検証するために使用されます。
VID List	使用する VLAN ID リストを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」ボタンをクリックして、指定エントリを編集します。

IPv6 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。

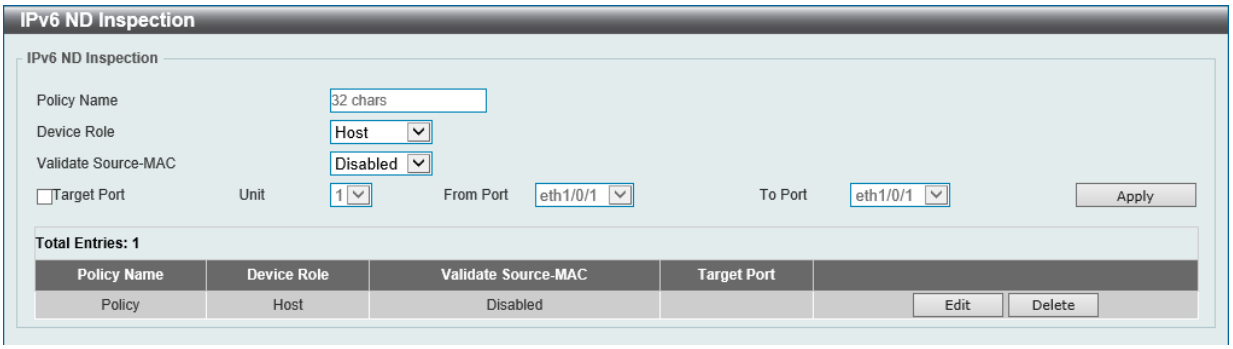


図 12-57　IPv6 ND Inspection 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 • 「Host」- デバイスの役割をホストに設定します。NS/NA メッセージに対するインスペクションが実行されます。（初期値） • 「Router」- デバイスの役割をルータに設定します。NS/NA に対するインスペクションは実行されません。 NS/NA インスペクションが実行されると、DHCP もしくは ND プロトコルから学習したダイナミックバインディングテーブルに対してメッセージの検証が行われます。
Validate Source-MAC	送信元 MAC アドレスオプションの検証を有効 / 無効に設定します。リンクレイヤアドレスを含む ND メッセージを受信した時に、リンクレイヤアドレスに対して送信元 MAC アドレスがチェックされます。リンクレイヤアドレスと MAC アドレスが異なる場合、パケットは破棄されます。
Target Port	チェックを入れターゲットポートを指定します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」ボタンをクリックして、指定エントリを編集します。

IPv6 RA Guard（IPv6 RA ガード）

IPv6 RA ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 RA Guard の順にクリックして、以下の画面を表示します。

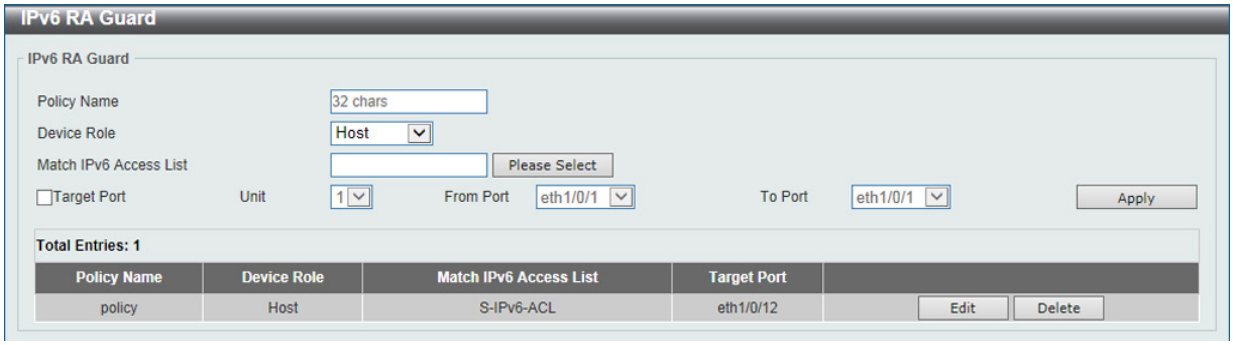


図 12-58　IPv6 RA Guard 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 • 「Host」- デバイスの役割をホストに設定します。RA パケットはすべてブロックされます。（初期値） • 「Router」- デバイスの役割をルータに設定します。RA パケットは、ポートに設定された ACL に従い転送されます。
Match IPv6 Access List	照合を行う IPv6 アクセスリストを入力します。「Please Select」をクリックすると、既存の ACL を選択することができます。
Target Port	チェックを入れターゲットポートを指定します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」ボタンをクリックして、指定エントリを編集します。

ACL 選択画面

「Please Select」をクリックすると次の画面が表示されます。



図 12-59　IPv6 RA Guard (Please Select) - ACL Access List 画面

設定するエントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv6 DHCP Guard（IPv6 DHCP ガード）

IPv6 DHCP ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 DHCP Guard の順にクリックして、以下の画面を表示します。

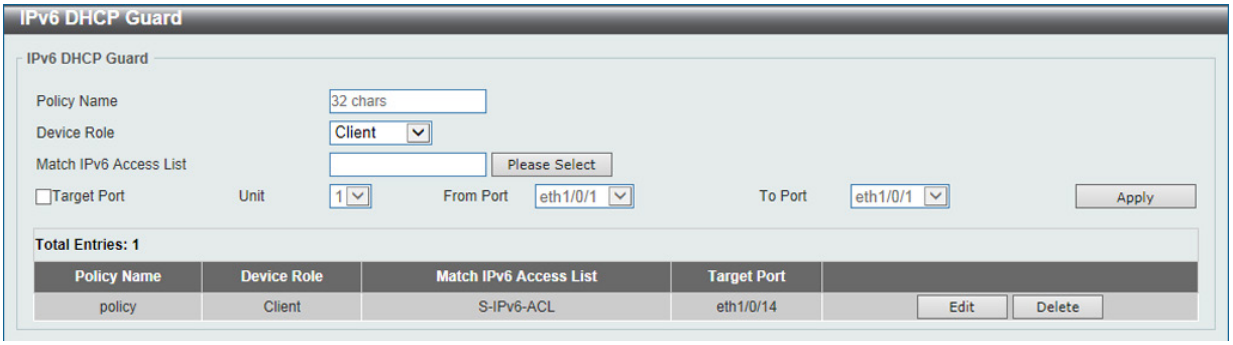


図 12-60　IPv6 DHCP Guard 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 • 「Client」- DHCPv6 サーバからの DHCPv6 パケットはすべてブロックされます。（初期値） • 「Server」- DHCPv6 サーバパケットはポートに設定された ACL に従い転送されます。
Match IPv6 Access List	照合する IPv6 アクセスリストを入力します。「Please Select」をクリックすると、既存のエントリから選択することができます。
Target Port	チェックを入れターゲットポートを指定します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Edit」ボタンをクリックして、指定エントリを編集します。

ACL 選択画面

「Please Select」をクリックすると次の画面が表示されます。



図 12-61　IPv6 DHCP Guard (Please Select) - ACL Access List 画面

設定するエントリを選択し、「OK」ボタンをクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

IPv6 Source Guard（IPv6 ソースガード）

■ IPv6 Source Guard Settings（IPv6 ソースガード設定）

IPv6 ソースガードの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings の順にクリックして、以下の画面を表示します。

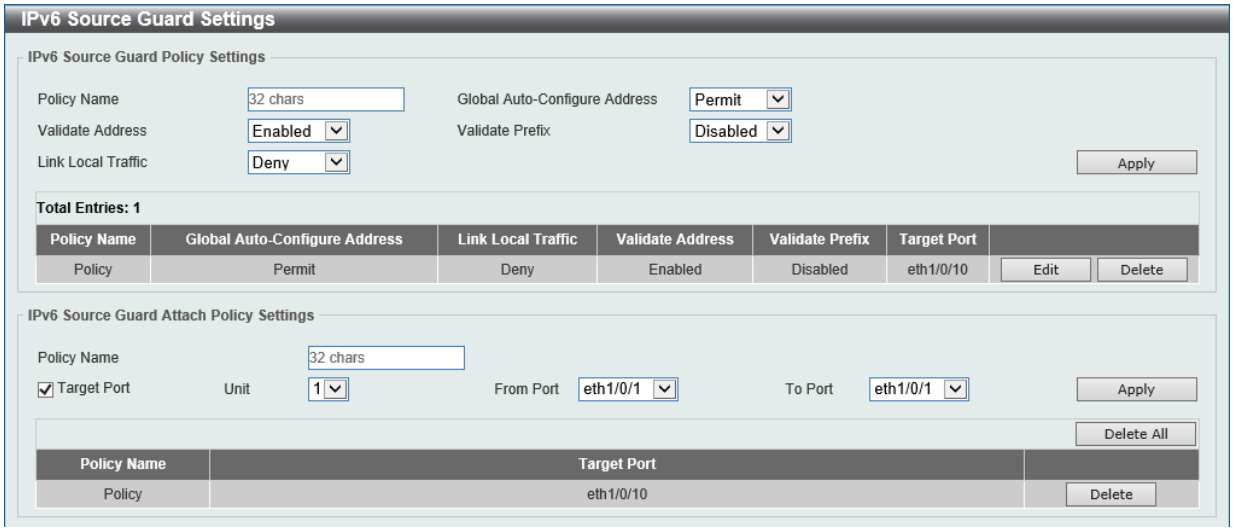


図 12-62　IPv6 Source Guard Settings 画面

画面に表示される項目：

項目	説明
IPv6 Source Guard Policy Settings	
Policy Name	ポリシー名を入力します。（32 文字以内）
Global Auto-Configure Address	自動設定グローバルアドレスからのデータトラフィックの許可 / 拒否を選択します。リンク上のすべてのグローバルアドレスが DHCP によって割り当てられていて、ホスト自身による設定アドレスからのトラフィック送信をブロックしたい場合に役に立ちます。 ・ 選択肢：「Permit（許可）」「Deny（拒否）」
Validate Address	アドレス検証機能を有効 / 無効に指定します。IPv6 ソースガードでアドレス検証機能を実行します。
Validate Prefix	プレフィックス検証機能を有効 / 無効に指定します。IPv6 ソースガードで IPv6 プレフィックスガード機能を実行します。
Link Local Traffic	ハードウェアによって許可されたリンクローカルアドレスからのデータトラフィックを許可 / 拒否します。 ・ 選択肢：「Permit（許可）」「Deny（拒否）」
IPv6 Source Guard Attach Policy Settings	
Policy Name	ポリシー名を入力します。（32 文字以内）
Target Port	ターゲットポートを指定します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Delete All」ボタンをクリックして、すべてのエントリを削除します。

■ IPv6 Neighbor Binding（IPv6 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。

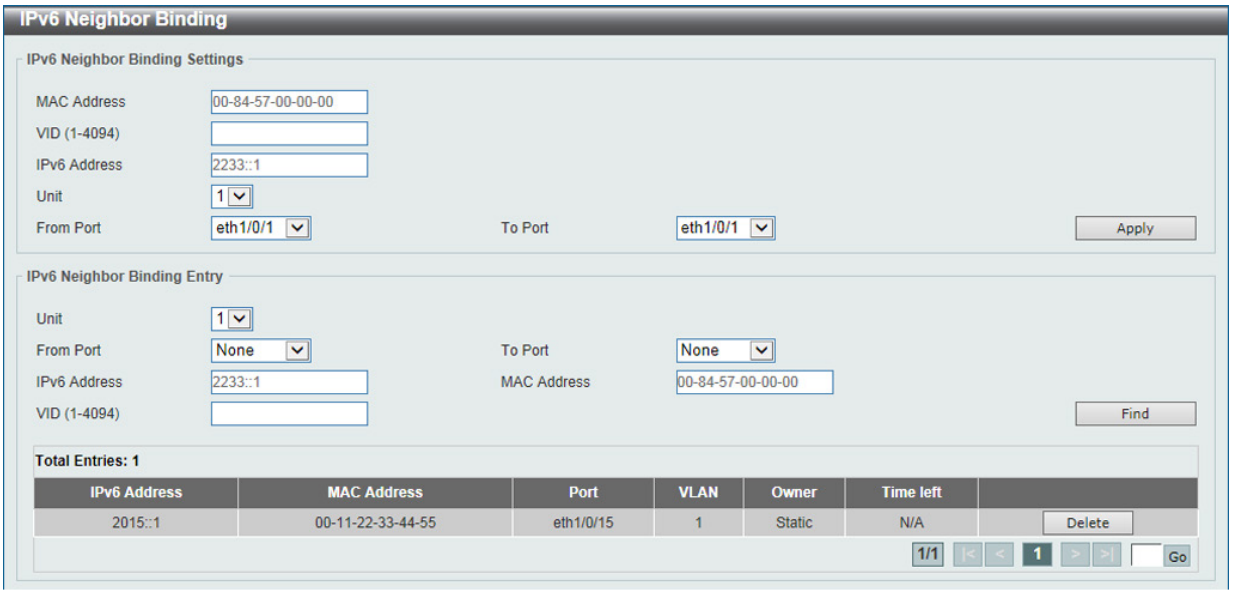


図 12-63　IPv6 Neighbor Binding 画面

画面に表示される項目：

項目	説明
IPv6 Neighbor Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。 • 設定可能範囲：1-4094
IPv6 Address	バインディングエントリの IPv6 アドレスを入力します。
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
IPv6 Neighbor Binding Entry	
Unit	バインディングエントリを表示するユニットを指定します。
From Port/To Port	バインディングエントリを表示するポートを指定します。
IPv6 Address	検索する IPv6 アドレスを入力します。
MAC Address	検索する MAC アドレスを入力します。
VID	検索する VLAN ID を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Find」ボタンをクリックして、入力した情報を基に指定のエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

DHCP Server Screening（DHCP サーバスクリーニング設定）

DHCP サーバパケットの制限や、DHCP クライアントが指定の DHCP サーバパケットを受信するように設定します。複数の DHCP サーバがネットワーク上に存在し、それぞれ異なる個別のクライアントグループに DHCP サービスを提供する場合に役立ちます。

ポートで DHCP サーバスクリーニング機能が有効になっている場合、このポートで受信したすべての DHCP サーバパケットは、ソフトウェアベースのチェックのために CPU にリダイレクトされます。 正当な DHCP サーバパケットは転送され、不正な DHCP サーバパケットは破棄されます。
DHCP サーバスクリーニング機能を有効にすると、すべての DHCP サーバパケットが特定のポートでフィルタリングされます。

DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）

DHCP サーバスクリーニングのグローバル設定を行います。

Security > DHCP Server Screening > DHCP Server Screening Global Settings の順にメニューをクリックして、以下の画面を表示します。

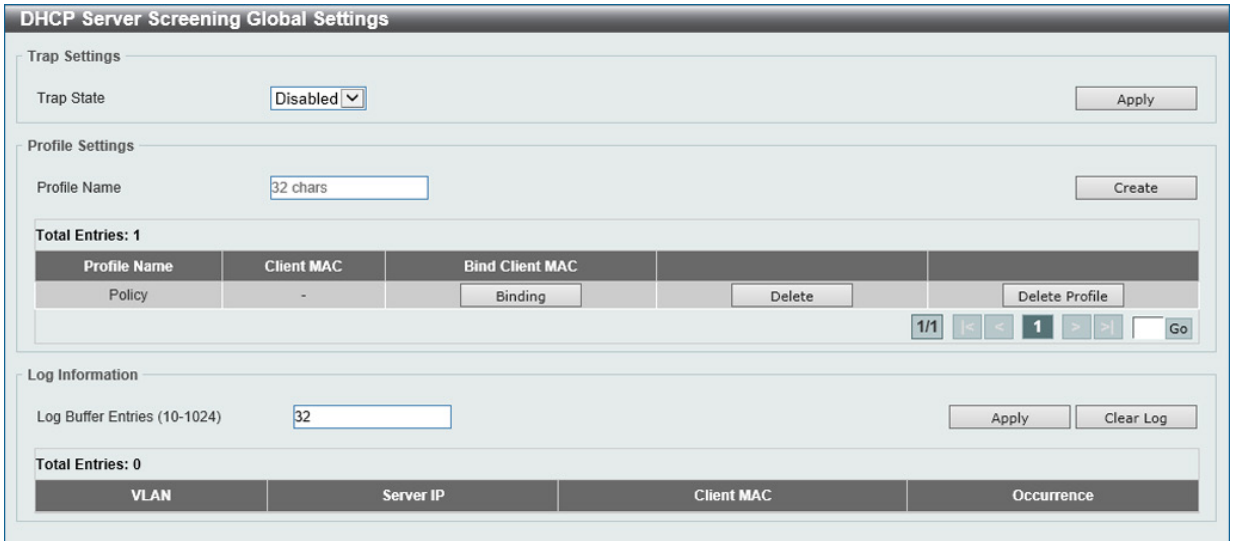


図 12-64　DHCP Server Screening Global Settings 画面

画面に表示される項目：

Trap Settings

項目	説明
Trap State	DHCP サーバスクリーニングのトラップ機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

Profile Settings

項目	説明
Profile Name	DHCP サーバスクリーニングのプロファイル名を入力します。（32 文字以内）

「Binding」ボタンをクリックして、プロファイルでクライアント MAC アドレスを設定します。
「Binding」画面で MAC アドレスを設定した後、「Apply」ボタンをクリックして設定内容を適用します。
「Delete」ボタンをクリックして、プロファイルから MAC アドレスの設定を削除します。
「Delete Profile」ボタンをクリックして、プロファイルを削除します。

Log Information

項目	説明
Log Buffer Entries	ログバッファエントリ数を入力します。 • 設定可能範囲：10-1024 • 初期値：32

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear Log」ボタンをクリックして、ログを削除します。

「Binding」ボタンをクリックすると以下の画面が表示されます。

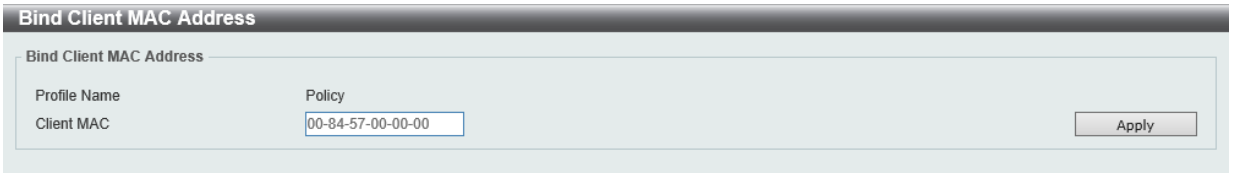


図 12-65　DHCP Server Screening Global Settings（Binding）- Bind Client MAC Address 画面

画面に表示される項目：

項目	説明
Client MAC	使用する MAC アドレスを指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

DHCP Server Screening Port Settings（DHCP サーバスクリーニングポート設定）

DHCP サーバスクリーニングポートの表示、設定を行います。

Security > DHCP Server Screening > DHCP Server Screening Port Settings の順にクリックし、以下の画面を表示します。

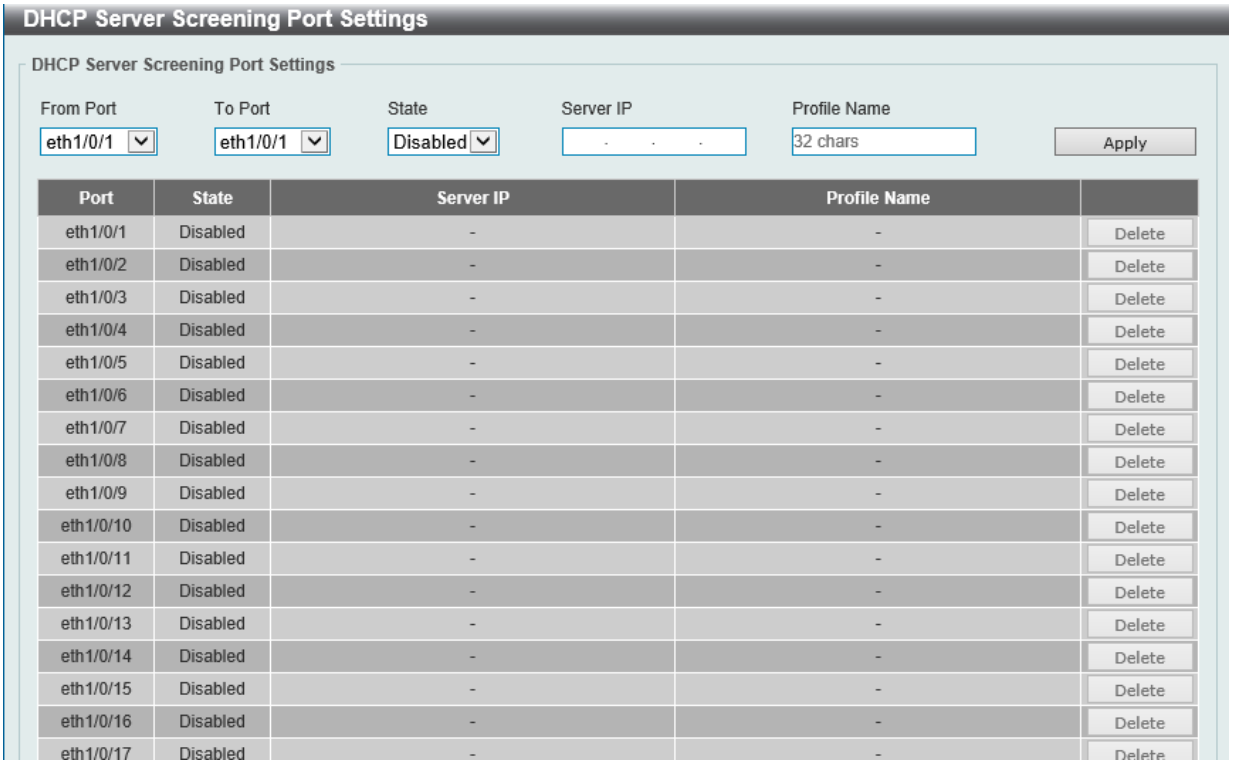


図 12-66　DHCP Server Screening Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
State	指定ポートでの DHCP サーバスクリーニング機能を有効 / 無効に設定します。
Server IP	DHCP サーバの IP アドレスを入力します。
Profile Name	ポートに設定する DHCP サーバスクリーニングプロファイル名を入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

ARP Spoofing Prevention（ARP スプーフィング防止設定）

ARP スプーフィング防止設定を表示および設定します。
エントリが作成されると、送信元 IP アドレスがエントリのゲートウェイ IP アドレスと一致するものの、送信元 MAC アドレスがエントリのゲートウェイ MAC アドレスと一致しない ARP パケットは、システムによって破棄されます。 送信元 IP アドレスがゲートウェイ IP アドレスと一致しない ARP パケットは、ASP によってバイパスされます。
ARP アドレスが設定済みのゲートウェイの IP アドレス、MAC アドレス、およびポートリストと一致する場合、受信ポートが ARP により信頼済みか否かにかかわらず、ダイナミック ARP インスペクション（DAI）チェックをバイパスします。

Security > ARP Spoofing Prevention の順にメニューをクリックし、以下の画面を表示します。



図 12-67　ARP Spoofing Prevention 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Gateway IP	ゲートウェイの IP アドレスを入力します。
Gateway MAC	ゲートウェイの MAC アドレスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

BPDU Attack Protection（BPDU アタック防止設定）

スイッチのポートにBPDU防止機能を設定します。通常、BPDU防止機能には2つの状態があります。1つは正常な状態で、もう1つはアタック状態です。アタック状態には、3つのモード（破棄、ブロックおよびシャットダウン）があります。BPDU 防止が有効なポートは、STP BPDU パケットを受信するとアタック状態に入ります。そして、設定に基づいてアクションを実行します。

BPDU 防止は、STP 機能における BPDU Forward 設定よりも高い優先度を持っています。つまり、ポートで BPDU Forward 設定が有効になっていても、BPDU 防止が有効である場合には、ポートは STP BPDU を転送しません。

また、BPDU 防止は BPDU トンネルポート設定よりも高い優先度を持っています。つまり、ポートが STP において BPDU トンネルポートとして設定されている場合、通常 STP BPDU を転送しますが、ポートで BPDU 防止が有効である場合には STP BPDU を転送しません。

Security > BPDU Attack Protection の順にメニューをクリックし、以下の画面を表示します。

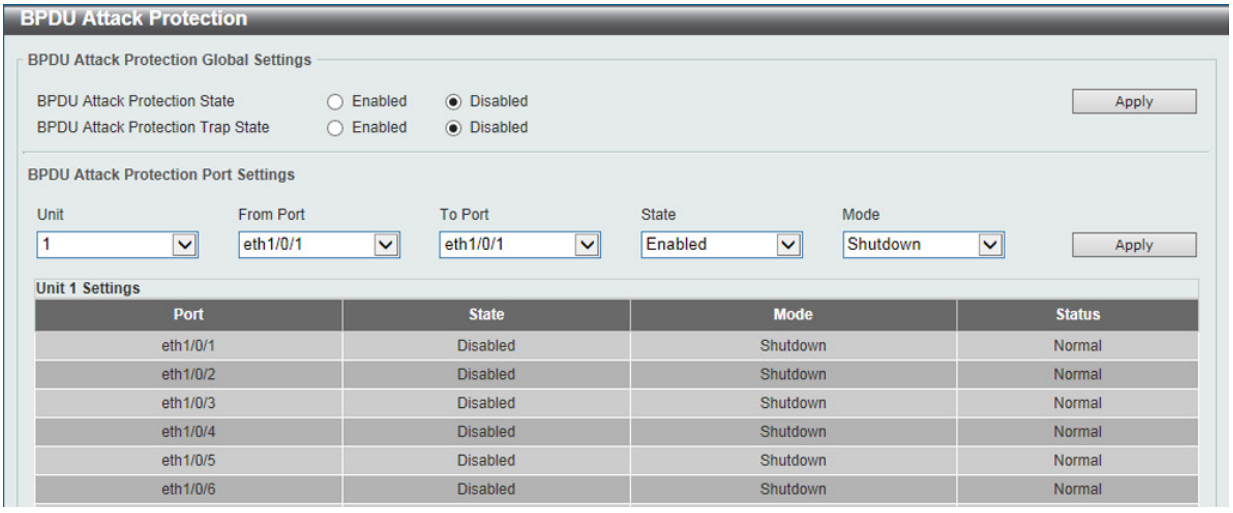


図 12-68　BPDU Attack Protection 画面

画面に表示される項目：

項目	説明
BPDU Attack Protection Global Settings	
BPDU Attack Protection State	BPDU アタック防止機能を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
BPDU Attack Protection Trap State	トラップの状態を有効 / 無効に設定します。
BPDU Attack Protection Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートに対して BPDU アタック防止機能を有効 / 無効に設定します。
Mode	BPDU 防止モードを指定します。 • 「Drop」- ポートがアタック状態に入ると、受信したすべての BPDU パケットを破棄します。 • 「Block」- ポートがアタック状態に入ると、すべてのパケット（BPDU と正常なパケットを含む）を破棄します。 • 「Shutdown」- ポートがアタック状態に入るとポートをシャットダウンします。

「Apply」ボタンをクリックして、設定内容を適用します。

NetBIOS Filtering（NetBIOS フィルタリング設定）

本項目では NetBIOS フィルタリングの設定、表示を行います。

Security > NetBIOS Filtering の順にメニューをクリックし、以下の画面を表示します。

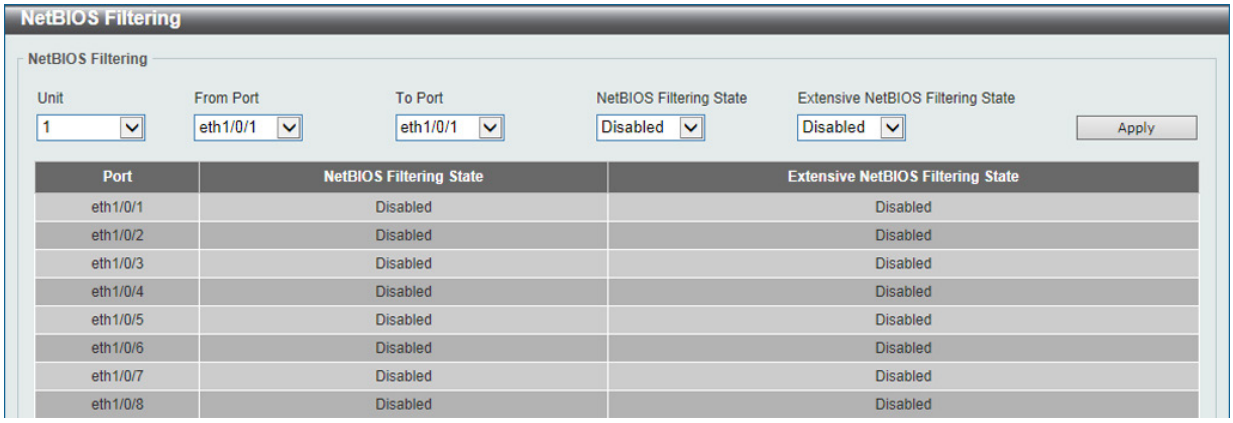


図 12-69　NetBIOS Filtering 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
NetBIOS Filtering State	指定ポートでの NetBIOS フィルタリングを有効 / 無効に設定します。 これにより物理ポートでの NetBIOS パケットが許可 / 拒否されます。
Extensive NetBIOS Filtering State	指定ポートでの Extensive NetBIOS フィルタリングを有効 / 無効に設定します。 これにより物理ポートでの 802.3 フレーム上の NetBIOS パケットが許可 / 拒否されます。

「Apply」ボタンをクリックして、設定内容を適用します。

MAC Authentication（MAC 認証）

MAC 認証機能は、MAC アドレスを使用してネットワークの認証を行う機能です。
本スイッチでは、ローカル認証方式、RADIUS サーバ認証方式の両方をサポートしています。
ローカルデータベースに基づいて認証を実行、または RADIUS クライアントとしてリモート RADIUS サーバとの間で RADIUS プロトコルを介して認証プロセスを実行します。

補足　RADIUS サーバを使った場合の MAC 認証の最大ユーザ数は 4,000 となります。

Security > MAC Authentication の順にメニューをクリックし、以下の画面を表示します。

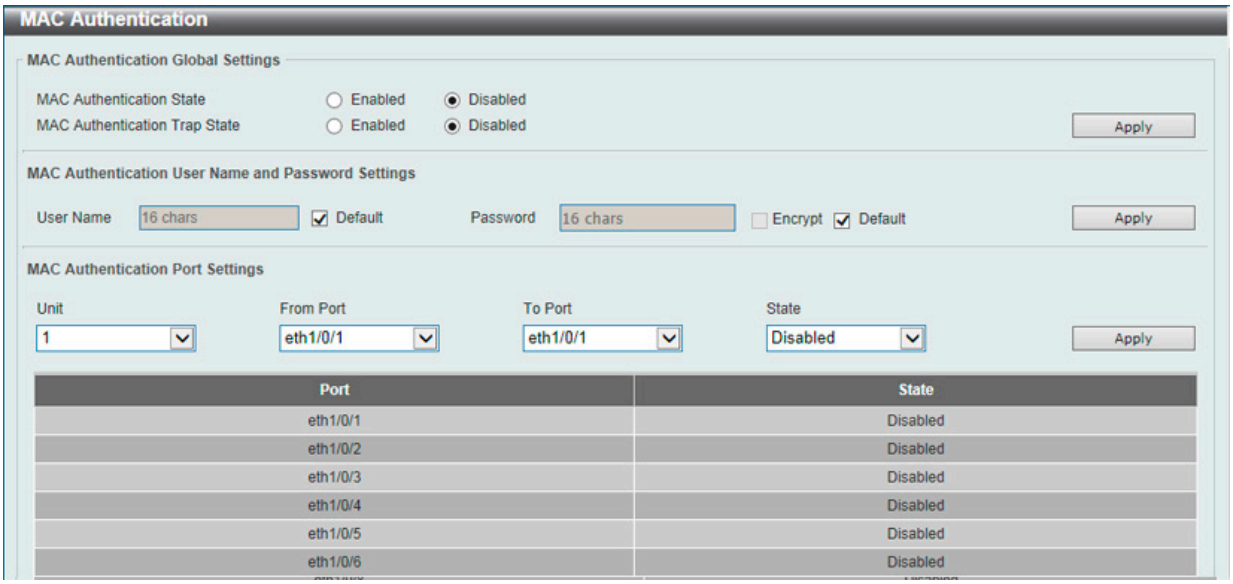


図 12-70　MAC Authentication 画面

画面に表示される項目：

項目	説明
MAC Authentication Global Settings	
MAC Authentication State	スイッチの MAC 認証のグローバルステータスを有効 / 無効に設定します。
MAC Authentication Trap State	MAC 認証のトラップのステータスを有効 / 無効に設定します。
MAC Authentication User Name and Password Settings	
User Name	MAC 認証のユーザ名を入力します。（16 文字以内）「Default」にチェックを入れると、クライアントの MAC アドレスがユーザ名として指定されます。
Password	MAC 認証のパスワードを入力します。「Encrypt」にチェックを入れると、パスワードを暗号化します。「Default」にチェックを入れると、クライアントの MAC アドレスがパスワードとして指定されます。
MAC Authentication Port Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定のポートに対し、MAC 認証を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

注意　MAC 認証において、Host Mode が Multi Auth モードの場合、Guest VLAN を使用する際に端末のポート間の移動を許可するには、”no ingress-checking” を設定する必要があります。

注意　ゲスト VLAN 使用時、認証された MAC アドレスはゲスト VLAN でログに記録されます。

注意　MAC 認証において、ゲスト VLAN はトランクモード、VLAN トンネルのインタフェースで動作しません。

Web-based Access Control（Web 認証）

Web-based Access Control（WAC）は、ユーザがスイッチを経由してインターネットにアクセスを試みる際に、ユーザを認証する機能です。認証処理にはHTTP/HTTPS プロトコルが使用されます。ユーザがWeb ブラウザ経由でWebページ(例 : http://www.dlink.com) を閲覧しようとすると、スイッチは認証段階に進みます。スイッチにより HTTP/HTTPS パケットが検出され、ポートが未認証である場合、ユーザは認証ページにリダイレクトされます。認証処理が完了するまで、ユーザはインターネットにアクセスすることはできません。

スイッチは、認証サーバとしてローカルデータベースに基づく認証を行うか、RADIUS クライアントとしてリモート RADIUS サーバ経由による RADIUS プロトコルを利用した認証処理を実行します。クライアントユーザが Web へのアクセスを試みると、WAC の認証処理が開始されます。

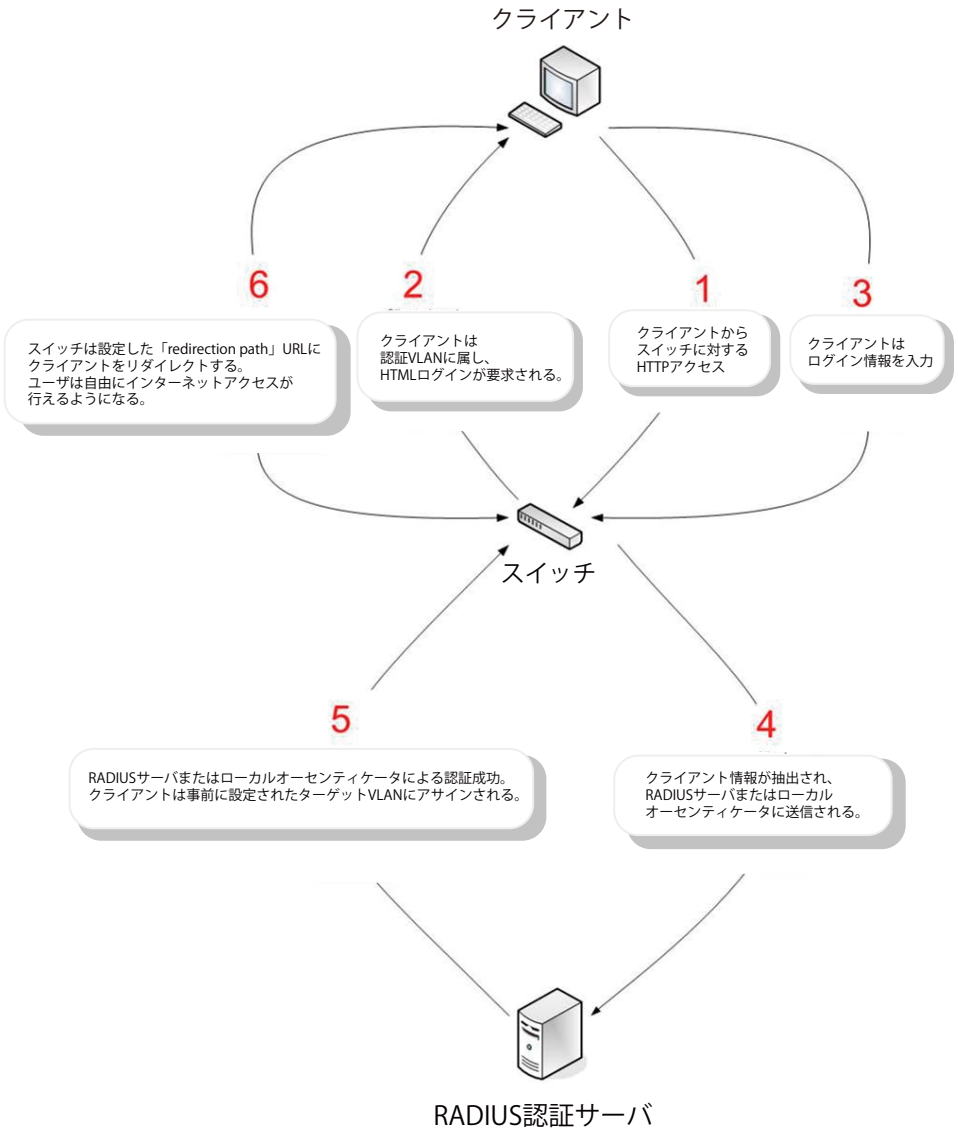
D-Link の WAC の実行には、WAC 機能が排他的に使用している仮想 IP が使用されます。この IP アドレスは、スイッチの他のモジュールには認識されません。スイッチの他の機能への影響を避けるため、WAC は仮想 IP アドレスのみを使用してホストとの通信を行います。従って、すべての認証要求は、スイッチの物理インタフェースの IP アドレスではなく仮想 IP アドレスに送信される必要があります。

ホスト PC が仮想 IP 経由で WAC スイッチと通信する場合、この仮想 IP は、スイッチの物理的な IPIF（IP インタフェース）アドレスに変換されて通信が可能になります。ホスト PC や他のサーバの IP 構成は WAC の仮想 IP に依存しません。また、仮想 IP は、ICMP パケットや ARP リクエストに応答しません。つまり、仮想 IP は、スイッチの IPIF（IP インタフェース）と同じサブネット、またはホスト PC のサブネットと同じサブネットに設定することはできません。

認証された / 認証中のホストからの仮想 IP へのすべてのパケットは、スイッチの CPU で処理されます。そのため、仮想 IP が他のサーバや PC の IP アドレスと同じ場合、WAC が有効なポートに接続するホストは、その IP アドレスを実際に使用しているサーバや PC とは通信ができません。ホストがそれらのサーバや PC にアクセスする必要がある場合、仮想 IP をサーバや PC のアドレスと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、認証が適切に実行されるように、PC のユーザはプロキシの例外設定に仮想 IP を追加する必要があります。

スイッチの WAC 機能では、HTTP または HTTPS プロトコルに対し、ユーザ定義の TCP ポート番号を設定することができます。HTTP または HTTPS 用の TCP ポートは、認証処理において CPU で処理される HTTP /HTTPS パケットを識別したり、ログインページにアクセスしたりするために使用されます。ポート番号を指定しない場合、HTTP のポート番号の初期値は 80、HTTPS のポート番号の初期値は 443 となります。

次の図は、Web ベースのアクセスコントロールにおいて、各ノードで行われる認証プロセスの基本の 6 つのステップを例示しています。



条件および制限

1. クライアントが IP アドレスの取得に DHCP を使用している場合、IP アドレスを取得できるように、認証 VLAN に DHCP サーバまたは DHCP リレー機能を設定する必要があります。
2. アクセスプロファイル機能などの一部のスイッチ機能では、HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
3. 認証に RADIUS サーバを使用する場合、スイッチで Web 認証を有効にする前に、RADIUS サーバに対して適切な構成（ユーザ情報やターゲット VLAN など）を行ってください。

Web Authentication（Web 認証設定）

スイッチの Web 認証設定を行います。

Security > Web-based Access Control > Web Authentication をクリックして、以下の画面から設定します。



図 12-71　Web Authentication 画面

画面に表示される項目：

項目	説明
Web Authentication State	Web 認証機能のグローバルステータスを有効 / 無効に設定します。
Trap State	Web 認証のトラップの状態を有効 / 無効に設定します。
Virtual IPv4	仮想 IP アドレスを入力します。このアドレスは WAC 機能のみで使用されます。すべての Web 認証のプロセスはこの IPv4 アドレスを使用して行われますが、仮想 IP は ICMP パケットや ARP リクエストには応答しません。そのため、仮想 IP はスイッチやホスト PC のインタフェースと同じサブネットに設定することはできません。同じサブネットに設定した場合、Web 認証は正しく動作しません。定義した URL は、仮想 IP アドレスが設定されている場合にのみ有効になります。ユーザは、仮想 IP アドレスを取得するために、DNS サーバに保存された FQDN URL を取得します。取得した IP アドレスは本項目で指定した仮想 IP アドレスと一致する必要があります。仮想 IPv4 アドレスが設定されていない場合、IPv4 接続で Web 認証を開始することができません。
Virtual IPv6	仮想 IPv6 アドレスを入力します。仮想 IPv6 アドレスが設定されていない場合、IPv6 接続で Web 認証を開始することができません。
Virtual URL	仮想 URL を指定します。（128 文字以内）
Redirection Path	リダイレクトパスを入力します。（128 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。

注意　WAC 未認証時、DNS Over TCP はブロックされます。

WAC Port Settings（Web 認証ポート設定）

ポート毎に WAC 機能のステータスを設定します。

Security > Web-based Access Control > WAC Port Settings をクリックし、以下の設定用画面を表示します。

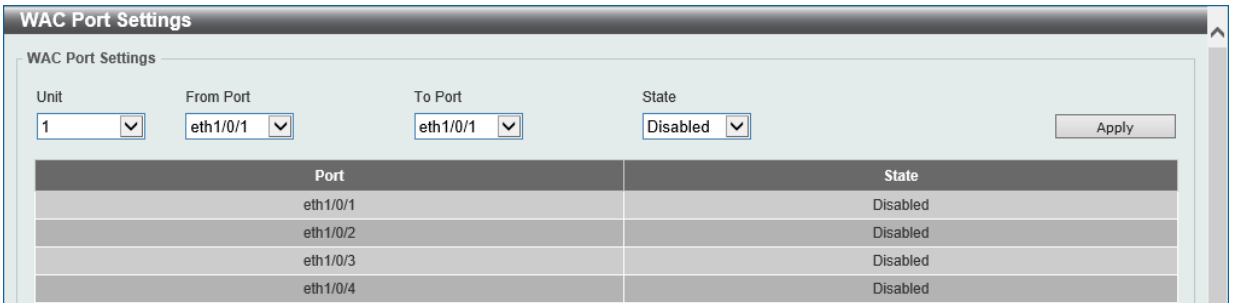


図 12-72　WAC Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	WAC 機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

WAC Customize Page（WAC カスタマイズページ設定）

認証ページの項目をカスタマイズします。

Security > Web-based Access Control > WAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

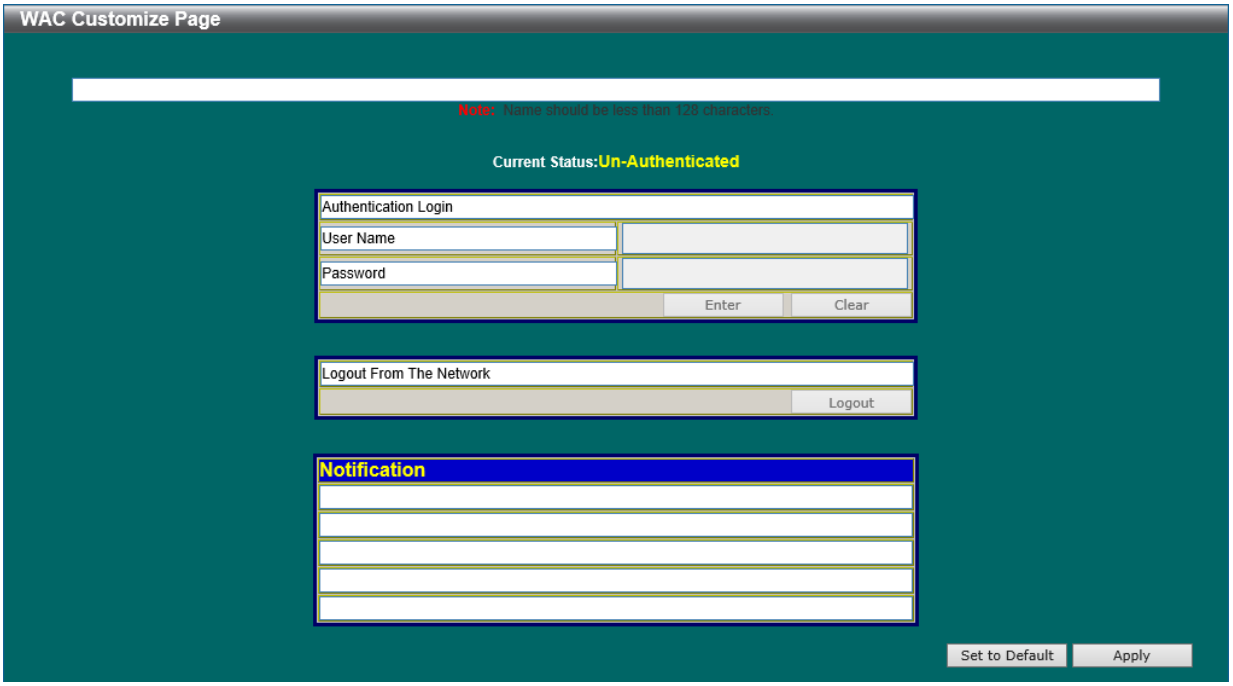


図 12-73　WAC Customize Page 画面

画面に表示される項目：

項目	説明
Page Title	ページのタイトルとなるメッセージを入力します。（128 文字以内）
Login window Title	ログイン画面のタイトルを入力します。（64 文字以内）
User Name Title	ユーザ名項目のタイトルを入力します。（32 文字以内）
Password Title	パスワード項目のタイトルを入力します。（32 文字以内）
Logout window Title	ログアウト画面のタイトルを入力します。（64 文字以内）
Notification	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。

WAC ページの設定を変更するには、本画面の WAC 認証情報をすべて入力して「Apply」ボタンをクリックし、変更を適用します。
「Set to Default」ボタンをクリックして、全項目を初期設定に戻します。

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。

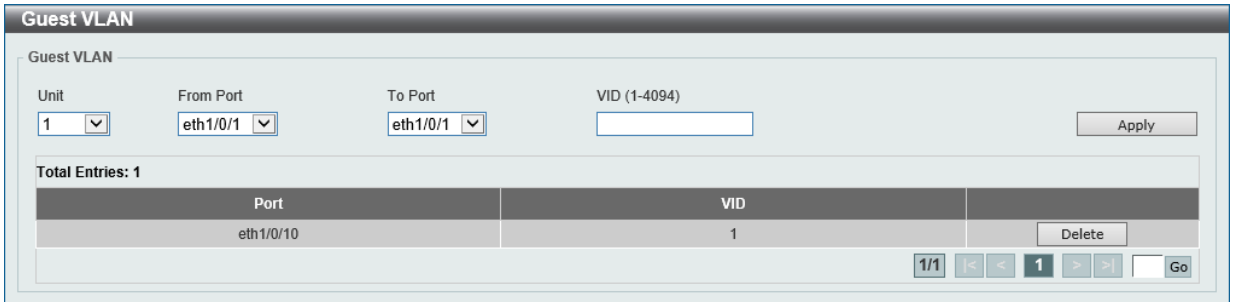


図 12-74　Guest VLAN 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
VID	設定する VLAN ID を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）

ネットワークアクセス認証のグローバルステータスを設定します。

Security > Network Access Authentication > Network Access Authentication Global Settings の順にメニューをクリックし、以下の画面を表示します。

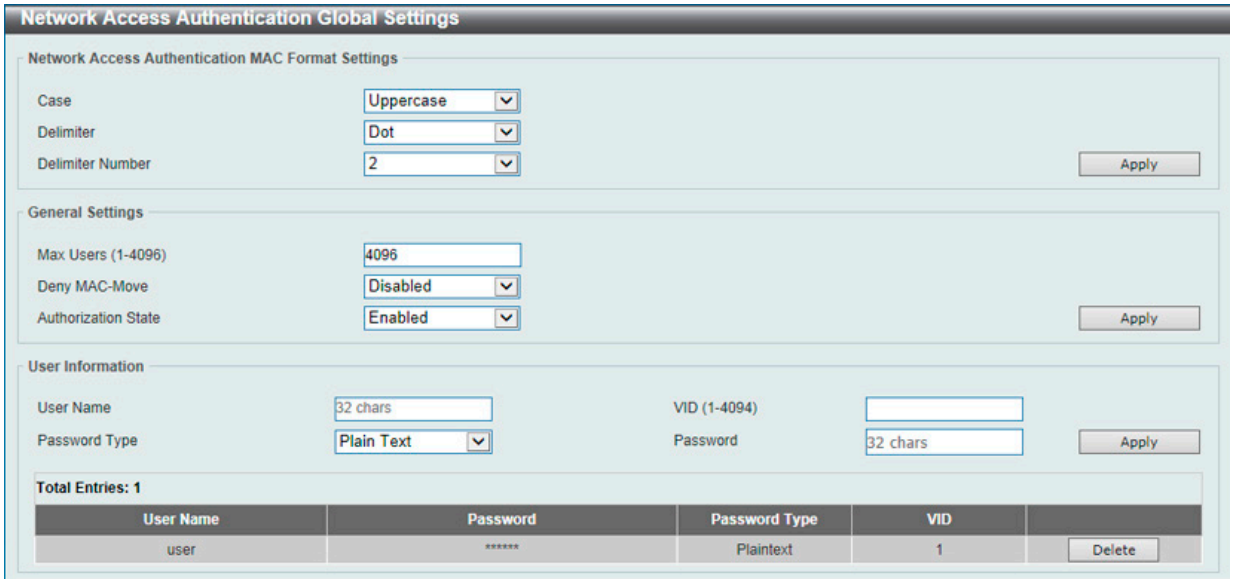


図 12-75　Network Access Authentication Global Settings 画面

画面に表示される項目：

項目	説明
Network Access Authentication MAC Format Settings	
Case	ネットワークアクセス認証に使用する MAC アドレスの形式を選択します。 • 選択肢：「Uppercase」（大文字）または「Lowercase」（小文字）
Delimiter	MAC アドレスを入力する際の区切りを選択します。 • 選択肢：「Hyphen（ハイフン）」「Colon（コロン）」「Dot（ドット）」「None（区切り文字なし）」

項目	説明
Delimiter Number	MAC アドレスにおける区切り数を選択します。 • 選択肢：「1」「2」「5」
General Settings	
Max Users	許可するユーザの最大数を指定します。 • 設定可能範囲：1-4096 • 初期値：4096
Deny MAC-Move	MAC 移動拒否機能の拒否を有効 / 無効に設定します。マルチ認証モードのポートで認証されたホストについて、別のポートへの移動を許可するかどうかを制御します。 ホストによる認証ポート間の移動には二つの状況が考えられます。次のルールに基づき、再認証が必要となるか、再認証を行うことなく新しいポートに直接移動します。 - 新しいポートの認証設定が元のポートと同じ場合、再認証は必要ありません。ホストは新しいポートに同じ承認属性を引き継ぎます。認証されたホストは、ポート 1 からポート 2 へのローミングを実行でき、再認証なしで承認属性を継承します。 - 新しいポートの認証設定が元のポートと異なる場合は、再認証が必要です。ポート 1 の認証済みホストは、ポート 2 に移動して再認証を行うことが可能です。新しいポートで認証方式が有効になっていない場合は、ステーションは新しいポートに直接移動します。元のポートとのセッションは削除されます。ポート 1 の認証済みホストは、ポート 2 に移動できます。 MAC 移動が無効（本機能が有効）になっていて、認証されたホストが別のポートに移動した場合、違反エラーとして認識されます。
Authorization State	承認について有効 / 無効に指定します。本オプションは、認証された設定を承認するかどうかを指定します。認証への承認が有効になると、RADIUS サーバにより付与される権限属性（VLAN, 802.1p default priority, bandwidth, ACL など）が許容されます。「Bandwidth」「ACL」はポートベースでアサインされます。マルチ認証モードの場合、「VLAN」と「802.1p」は各ホストベースでアサインされます。それ以外の場合、「Bandwidth」「ACL」は各ポートベースでアサインされます。
User Information	
User Name	ユーザ名を入力します。（32 文字以内）
VID	VLAN ID を入力します。
Password Type	パスワードの種類を選択します。 • 選択肢：「Plain Text（平文）」「Encrypted（暗号化）」
Password	パスワードを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

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。

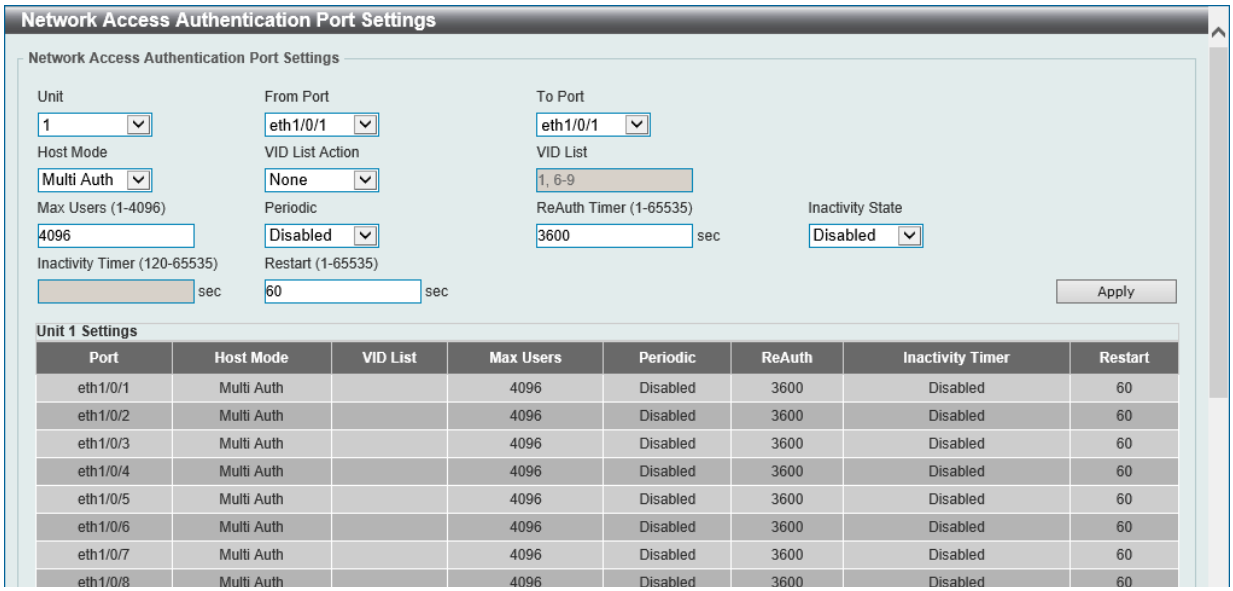


図 12-76　Network Access Authentication Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Host Mode	選択ポートに適用するホストモードを選択します。 • 「Multi Host」- ポートがマルチホストモードで動作している場合、一台のホストが認証されると、他のすべてのホストについてもポートへのアクセスが許可されます。802.1X 認証に従い、再認証失敗や認証ユーザのログオフなどが発生した場合、ポートはしばらくの間ブロックされます。一定の時間が過ぎると、EAPOL パケットの処理を元に戻します。 • 「Multi Auth」- ポートがマルチ認証モードで動作している場合、各ホストに対し、ポートへのアクセスに認証が必要になります。ホストは MAC アドレスによって識別され、認証されたホストのみポートへのアクセスが可能になります。
VID List Action	VLAN リストに対するアクションを設定します。 • 選択肢：「None（なし）」「Add（追加）」「Delete（削除）」
VID List	ホストモードでマルチ認証オプションを選択すると、パラメータが有効になります。使用する VLAN ID を入力します。この設定は、スイッチ上の各 VLAN に対して異なる認証要件が求められる場合に便利です。クライアントが認証された後、クライアントは他の VLAN から受信しても再認証は必要とされません。このオプションは、トランクポートが VLAN ごとの認証制御を行う場合に便利です。ポートの認証モードがマルチホストに変更された場合、ポート上の以前の認証 VLAN はクリアされます。
Max Users	最大ユーザ数を指定します。 • 設定可能範囲：1-4096
Periodic	選択ポートの定期的な再認証を有効 / 無効に設定します。802.1X プロトコルにのみ影響します。
ReAuth Timer	再認証タイマを指定します。 • 設定可能範囲：1-65535（秒） • 初期値：3600（秒）
Inactivity State	非アクティブ状態を有効 / 無効に指定します。
Inactivity Timer	非アクティブ状態を有効にした場合、非アクティブ時間の値を入力します。このパラメータは WAC の認証プロトコルにのみ影響します。 • 設定可能範囲：120-65535（秒）
Restart	リスタート時間を入力します。 • 設定可能範囲：1-65535（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）

ネットワークアクセス認証セッション情報の表示、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。

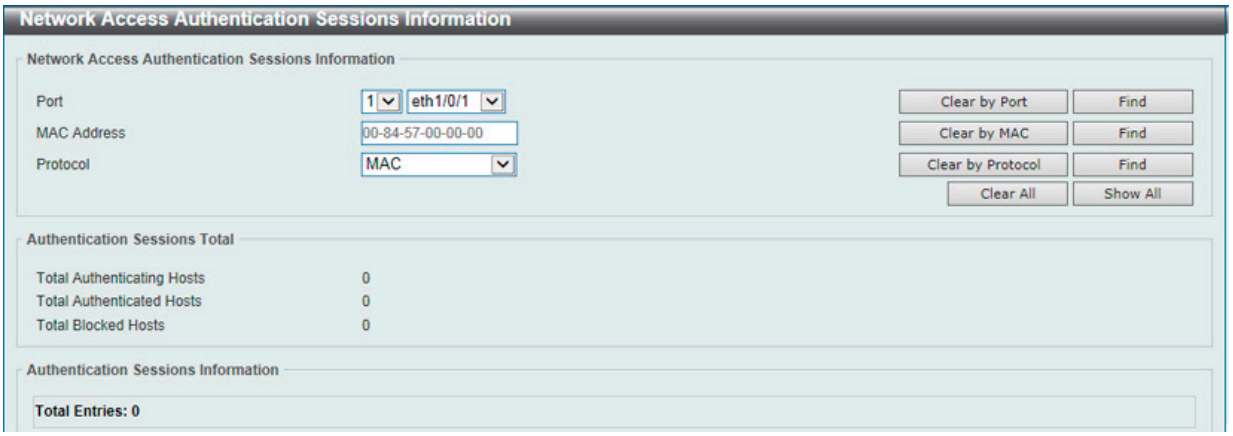


図 12-77　Network Access Authentication Sessions Information 画面

画面に表示される項目：

項目	説明
Port	表示 / クリアするユニットとポートを指定します。
MAC Address	表示 / クリアする MAC アドレスを指定します。
Protocol	プロトコルオプションを選択します。 • 選択肢：「MAC」「WAC」「DOT1X」

情報の消去

「Clear by Port」ボタンをクリックして、選択したポートに基づき情報を消去します。
「Clear by MAC」ボタンをクリックして、選択した MAC アドレスに基づき情報を消去します。
「Clear by Protocol」ボタンをクリックして、選択したプロトコルに基づき情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。

エントリの検出 / 表示

「Find」ボタンをクリックして、入力した情報を基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て、すべてのエントリを表示します。

Safeguard Engine（セーフガードエンジン）

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃により、スイッチの CPU 負荷は対応可能なキャパシティを超えて増大してしまう可能性があります。このような問題を軽減するために、本スイッチにはセーフガードエンジン機能が実装されています。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化してスイッチ全体の操作性を保ち、限られたリソース内で重要なパケットの送受信を可能にします。

CPU 負荷が上昇しきい値を超えると、セーフガードエンジン機能が作動し、スイッチは「Exhausted」モードに入ります。Exhausted モードでは、スイッチは ARP とブロードキャスト IP パケットで使用可能な帯域を制限します。CPU 負荷がしきい値を下回った場合、セーフガードエンジンは動作を停止し、スイッチは Exhausted モードを脱却して通常モードへ移行します。

CPU 宛に送信されるパケットは 3 つのグループに分類されます。サブインタフェースとしても知られるこれらのグループは、CPU が特定の種類のトラフィックを識別するために使用する論理的なインタフェースです。この 3 つのグループは「プロトコル」「管理」「ルート」に分類されています。通常、スイッチの CPU が受信パケットを処理する際、「プロトコル」グループが最も高い優先度でパケットを受信し、（スイッチの CPU は基本的にルーティングパケットの処理を行うため）「ルート」グループは最も低い優先度でパケットを受信します。「プロトコル」グループで処理されるパケットは、ルータによって識別されるプロトコルコントロールパケットです。「管理」グループで処理されるパケットは、Telnet や SSH などの対話型アクセスプロトコルを使用して、ルータやシステムネットワーク管理インタフェースへ送信されます。「ルート」グループで処理されるパケットは、一般にルータ CPU によって処理される通過ルーティングパケットとして認識されます。

以下の表は、プロトコルと対応するサブインタフェースの一覧です。

プロトコル名	サブインタフェース（グループ）	概要
802.1X	Protocol	Port-based Network Access Control（ポートベースアクセスコントロール）
ARP	Protocol	Address resolution Protocol (ARP)
BGP	Protocol	Border Gateway Protocol（BGP）
DHCP	Protocol	Dynamic Host Configuration Protocol（DHCP）
DNS	Protocol	Domain Name System（DNS）
DVMRP	Protocol	Distance Vector Multicast Routing Protocol（DVMRP）
GVRP	Protocol	GARP VLAN Registration Protocol（GVRP）
ICMPv4	Protocol	Internet Control Message Protocol（ICMP）
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol（NS/NA/RS/RA) 以外
IGMP	Protocol	Internet Group Management Protocol（IGMP）
LACP	Protocol	Link Aggregation Control Protocol（LACP）
NTP	Protocol	Network Time Protocol（NTP）
OSPF	Protocol	Open Shortest Path First（OSPF）
PIM	Protocol	Protocol Independent Multicast（PIM）
PPPoE	Protocol	Point-to-point protocol over Ethernet（PPPoE）
RIP	Protocol	Routing Information Protocol（RIP）
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（VRRP）
Web	Manage	Hypertext Transfer Protocol (HTTP) Hypertext Transfer Protocol Secure (HTTPS)

カスタマイズされたレートリミット（パケット / 毎秒）をセーフガードエンジンのサブインタフェースに対してまとめて割り当て、または管理インタフェースで指定した個々のプロトコルに対して割り当てることが可能です。本機能を使用して個々のプロトコルのレート制限をカスタマイズする場合、不適切なレート制限を設定すると、パケットの処理に異常が発生する可能性がありますのでご注意ください。

注意　エンジンガードが有効になっている場合、スイッチは FFP（高速フィルタプロセッサ）メータリングテーブルを使用して、様々なトラフィックフロー（ARP、IP）に帯域幅を割り当て、CPU 使用率とトラフィック制限を制御します。これにより、ネットワーク経由のトラフィックルーティング速度が制限される場合があります。

Safeguard Engine Settings（セーフガードエンジン設定）

スイッチにセーフガードエンジンの設定を行います。

Security > Safeguard Engine > Safeguard Engine Settings の順にクリックし、以下の画面を表示します。

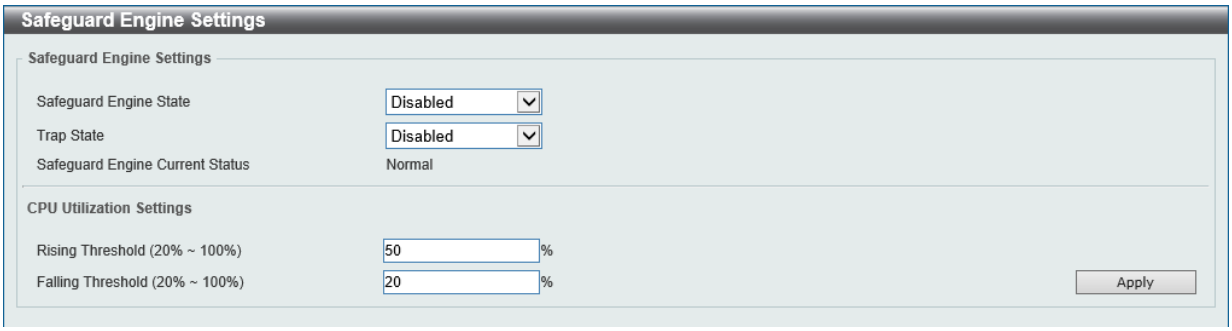


図 12-78　Safeguard Engine Settings 画面

画面に表示される項目：

項目	説明
Safeguard Engine Settings	
Safeguard Engine State	セーフガードエンジン機能を有効 / 無効に設定します。
Trap State	セーフガードエンジンのトラップを有効 / 無効に設定します。
Safeguard Engine Current Status	現在のセーフガードエンジンのステータスを表示します。
CPU Utilization Settings	
Rising Threshold	CPU 使用率の上限しきい値を設定します。CPU 使用率がこのしきい値に到達すると、設定値に基づいて Exhausted モードに入ります。 • 設定可能範囲：20-100（%）
Falling Threshold	CPU 使用率の下限しきい値を設定します。CPU 使用率がこのしきい値を下回ると、Safeguard Engine 状態から Normal モードに戻ります。 • 設定可能範囲：20-100（%）

「Apply」ボタンをクリックして、設定内容を適用します。

補足　セーフガード設定の CPU 使用率しきい値（「CPU Utilization Settings」）は、4 Core の平均値に対して適用されます。

CPU Protect Counters（CPU プロテクトカウンタ）

CPU プロテクションのカウンタ情報を表示、消去します。

Security > Safeguard Engine > CPU Protect Counters の順にクリックし、以下の画面を表示します。

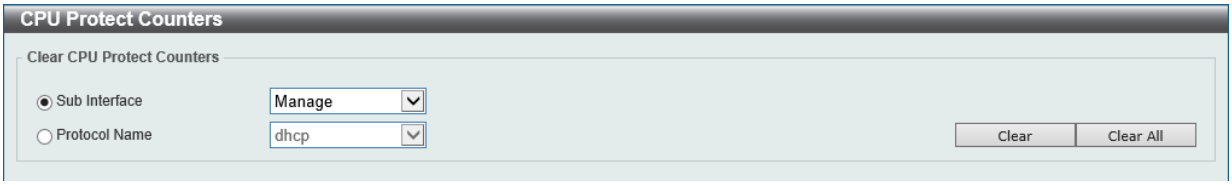


図 12-79　CPU Protect Counters 画面

画面に表示される項目：

項目	説明
Sub Interface	サブインタフェースのオプションを選択します。指定したサブインタフェースの CPU プロテクトカウンタをクリアします。 • 選択肢：「Manage」「Protocol」「Route」「All」
Protocol Name	プロトコル名のオプションを選択します。

「Clear」ボタンをクリックして、設定に基づいて情報を消去します。
「Clear All」ボタンをクリックして、すべての情報を消去します。

CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）

CPU プロテクションのサブインタフェースを設定、表示します。

Security > Safeguard Engine > CPU Protect Sub-Interface の順にクリックし、以下の画面を表示します。



図 12-80　CPU Protect Sub-Interface 画面

画面に表示される項目：

項目	説明
CPU Protect Sub-Interface	
Sub-Interface	サブインタフェースのオプションを選択します。 • 選択肢：「Manage」「Protocol」「Route」
Rate Limit	レートリミットの値を入力します。「No Limit」を指定するとレートリミットを無効にします。 • 設定可能範囲：0-1024（パケット / 秒）
Sub-Interface Information	
Sub-Interface	サブインタフェースのオプションを選択します。 • 選択肢：「Manage」「Protocol」「Route」

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定条件に基づくエントリを検出します。

CPU Protect Type（CPU プロテクトタイプ）

CPU プロテクションの種類の設定、表示します。

Security > Safeguard Engine > CPU Protect Type の順にクリックし、以下の画面を表示します。

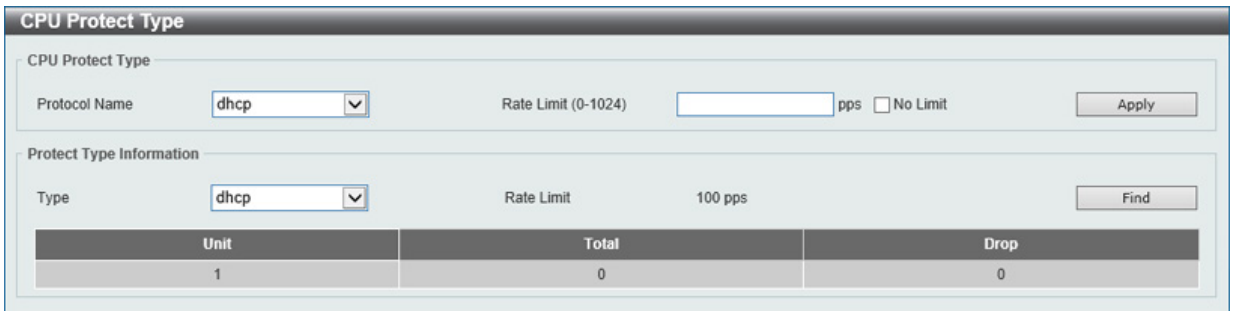


図 12-81　CPU Protect Type 画面

画面に表示される項目：

項目	説明
CPU Protect Type	
Protocol Name	プロトコル名のオプションを選択します。
Rate Limit	レートリミットの値を入力します。「No Limit」を指定するとレートリミットを無効にします。 • 設定可能範囲：0-1024（パケット / 秒）
Protect Type Information	
Type	プロトコルタイプを選択します。プロトコルタイプの選択後、レートリミットの値が表示されます。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報を基にエントリを検出します。

補足　CPU プロテクトタイプに関する設定は、セーフガードエンジン機能の有効 / 無効とは独立して動作します。

Trusted Host（トラストホスト）

トラストホストの設定、表示を行います。

Security > Trusted Host の順にクリックし、以下の画面を表示します。

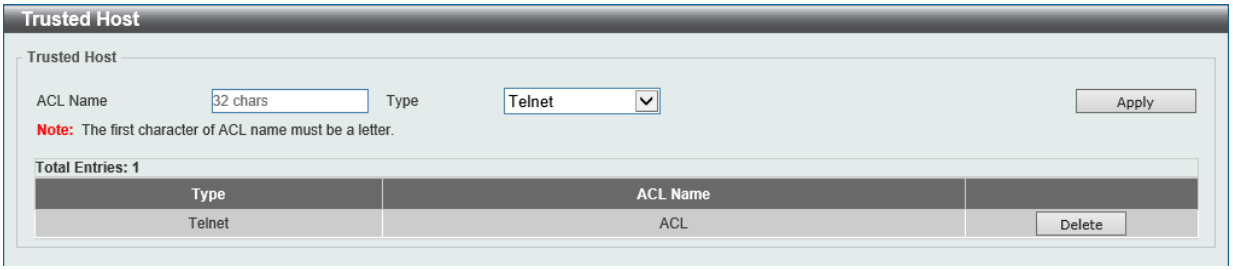


図 12-82　Trusted Host 画面

画面に表示される項目：

項目	説明
ACL Name	使用する ACL 名を入力します。（32 文字以内）
Type	トラストホストの種類を指定します。 • 選択肢：「Telnet」「SSH」「Ping」「HTTP」「HTTPS」

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

Traffic Segmentation（トラフィックセグメンテーション）

トラフィックセグメンテーションを設定します。 トラフィックセグメンテーション転送ドメインが指定されると、ポートで受信するパケットは、レイヤ 2 パケット転送においてドメイン内のインタフェースに制限されます。 ポートの転送ドメインが空の場合、ポートで受信したパケットのレイヤ 2 転送は制限されません。
トラフィックセグメンテーションのメンバリストは、同じ転送ドメインのポートとポートチャネルなど、異なるインタフェースタイプで構成できます。指定されたインタフェースにポートチャネルが含まれている場合、このポートチャネルのすべてのメンバポートが転送ドメインに含まれます。

Security > Traffic Segmentation Settings の順にメニューをクリックし、以下の画面を表示します。

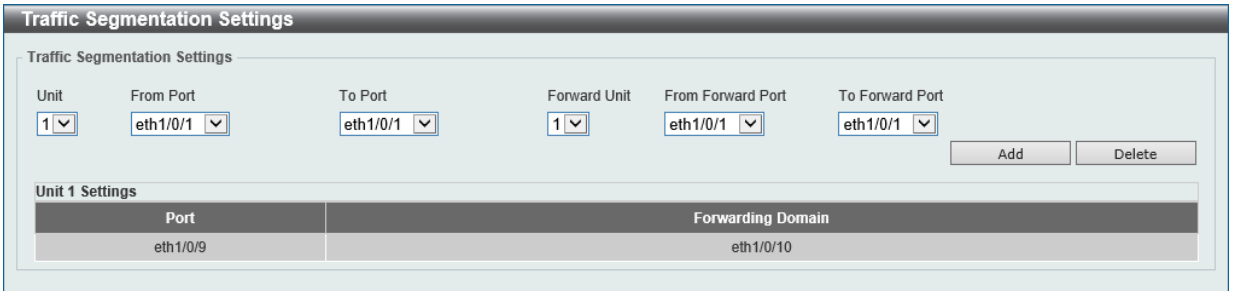


図 12-83　Traffic Segmentation 画面

画面に表示される項目：

項目	説明
Unit	設定する受信スイッチユニットを選択します。
From Port / To Port	設定する受信ポート範囲を指定します。
Forward Unit	設定する転送スイッチユニットを指定します。
From Forward Port / To Forward Port	設定する転送ポート範囲を指定します。

「Add」ボタンをクリックして、入力した情報を基に新しいエントリを追加します。
「Delete」ボタンをクリックして、入力した情報を基にエントリを削除します。

Storm Control Settings（ストームコントロール設定）

ストームコントロールの設定、表示を行います。

Security > Storm Control Settings の順にクリックします。

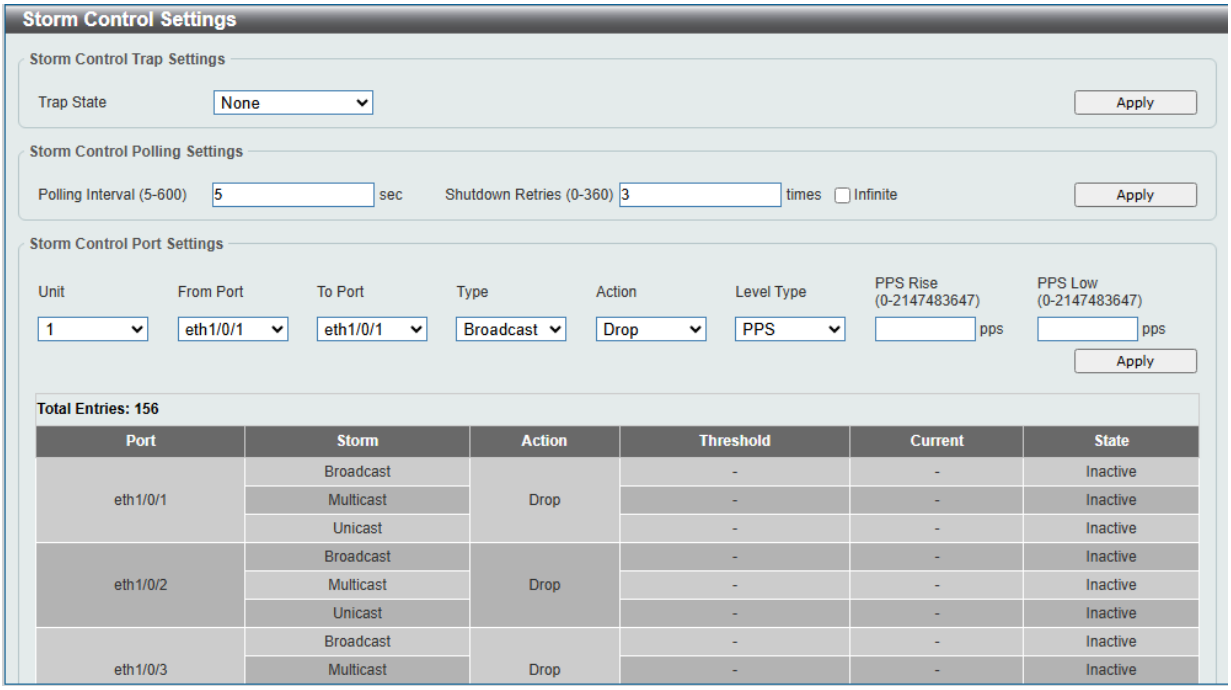


図 12-84　Storm Control Settings 画面

画面に表示される項目：

項目	説明
Storm Control Trap Settings	
Trap State	ストームコントロールトラップのオプションを指定します。 • 「None」- トラップは送信されません。 • 「Storm Occur」- ストームの発生を検出した時点でトラップが通知されます。 • 「Storm Clear」- ストームが解消された時点でトラップが通知されます。 • 「Both」- ストームの発生を検出、またはストームが解消された時点でトラップが通知されます。
Storm Control Polling Settings	
Polling Interval	ポーリング間隔の値を指定します。 • 設定可能範囲：5-600（秒） • 初期値：5（秒）
Shutdown Retries	シャットダウンの再試行回数を入力します。「Infinite」にチェックを入れると本機能は無効になります。 • 設定可能範囲：0-360（回） • 初期値：3（回）
Storm Control Port Setting	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Type	コントロールするストームの種類を選択します。 • 選択肢：「Broadcast」「Multicast」「Unicast」 シャットダウンモードに設定されている場合、ユニキャストは「Known」「Unknown」両方を参照します。つまり、既知または不明なユニキャストパケットが指定のしきい値に達すると、ポートはシャットダウンします。それ以外の設定では、ユニキャストは「Unknown」パケットのみを参照します。
Action	実行するアクション指定します。 • 「None」- ストームパケットをフィルタしません。 • 「Shutdown」- 指定したしきい値に達するとポートはシャットダウンされます。 • 「Drop」- 指定したしきい値に達するとパケットは破棄されます。
Level Type	レベルタイプを指定します。 • 選択肢：「PPS」「Kbps」「Level」
PPS Rise	1 秒あたりのパケット量について上限しきい値を指定します。 • 設定可能範囲：0-2147483647（パケット / 秒）

項目	説明
PPS Low	1 秒あたりのパケット量について下限しきい値を指定します。 • 設定可能範囲：0-2147483647（パケット / 秒） • 初期値：PPS Rise 値の 80%

「Apply」ボタンをクリックして、設定内容を適用します。

「Level Type」で「Kbps」を選択すると、以下の画面が表示されます。

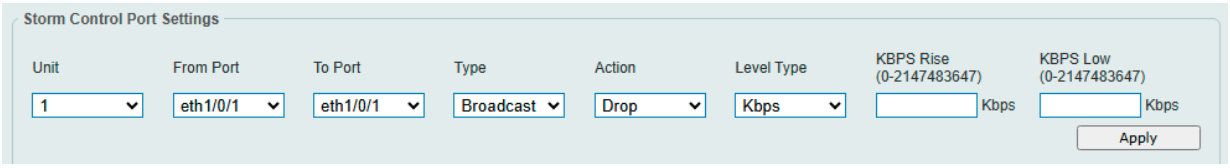


図 12-85　Storm Control Settings（Kbps）画面

画面に表示される項目：

項目	説明
KBPS Rise	上限 KBPS の値を指定します。ポートで受信するトラフィックの上限しきい値をキロビット / 秒で指定します。 • 設定可能範囲：0-2147483647（Kbps）
KBPS Low	下限 KBPS の値を指定します。ポートで受信するトラフィックの下限しきい値をキロビット / 秒で指定します。 • 設定可能範囲：0-2147483647（Kbps） • 初期値：KBPS Rise 値の 80%

「Apply」ボタンをクリックして、設定内容を適用します。

「Level Type」で「Level」を選択すると、以下の画面が表示されます。

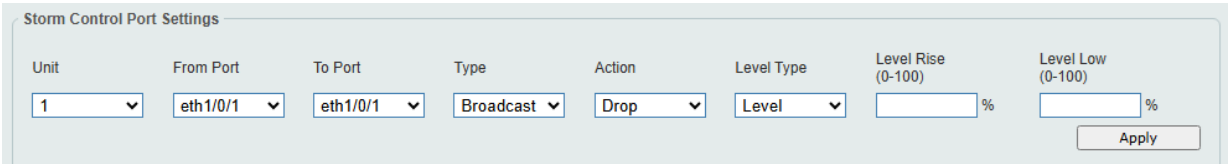


図 12-86　Storm Control Settings（Level）画面

画面に表示される項目：

項目	説明
Level Rise	上限レベルについて入力します。本オプションはポートで受信するトラフィックの総帯域の上限しきい値をパーセンテージとして指定します。 • 設定可能範囲：0-100（%）
Level Low	下限レベルについて入力します。本オプションはポートで受信するトラフィックの総帯域の下限しきい値をパーセンテージとして指定します。 • 設定可能範囲：0-100（%） • 初期値：Level Rise 値の 80%

「Apply」ボタンをクリックして、設定内容を適用します。

注意　ストームコントロール機能において、「Multicast」を指定した場合、IPv4、IPv6 の予約 MAC アドレス（VRRP、OSPF、IGMP、MLD など）に対して制限が適用されません。

DoS Attack Prevention Settings（DoS 攻撃防止設定）

各 DoS 攻撃に対して防御設定を行います。次のような既知の DoS 攻撃をスイッチで検出することができます。

- Land 攻撃：このタイプの攻撃には、送信元アドレスと宛先アドレスがターゲットデバイスのアドレスに設定されている IP パケットが使用されます。ターゲットデバイスが自身に対して継続的に応答してしまう可能性があります。
- Blat 攻撃：このタイプの攻撃は、ターゲットデバイスの宛先ポートと同じ TCP / UDP ソースポートでパケットを送信します。ターゲットデバイスが自身に対して応答してしまう可能性があります。
- TCP-Null：このタイプの攻撃には、シーケンス番号 0 でフラグを持たない特定のパケットを使用したポートスキャンが使用されます。
- TCP-Xmas：このタイプの攻撃には、シーケンス番号 0 で緊急（URG）、プッシュ（PSH）、および FIN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- TCP SYN-FIN：このタイプの攻撃には、SYN および FIN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- TCP SYN SrcPort Less 1024：このタイプの攻撃には、送信元ポート 0 ～ 1023 と SYN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- Ping of Death 攻撃：Ping of Death 攻撃は、コンピューターに対する攻撃の一種で、不正な形式の Ping または悪意のある Ping をコンピューターに送信します。 Ping のサイズは通常 64 バイトです（多くのコンピュータは、最大 IP パケットサイズである 65535 バイトより大きい Ping を処理できません）。このサイズの ping を送信すると、ターゲットコンピュータがクラッシュする可能性があります。従来、このバグは比較的簡単に悪用されていました。一般に、65536 バイトの Ping パケットを送信することはネットワークプロトコルの規定に違反しますが、断片化されている場合、このサイズのパケットが送信できてしまいます。ターゲットコンピュータがパケットを再構成すると、バッファオーバーフローが発生する可能性があり、システムクラッシュを引き起こすことがあります。
- TCP Tiny Fragment 攻撃：Tiny TCP Fragment 攻撃者は、IP フラグメンテーションを使用して非常に小さなフラグメントを作成し、TCP ヘッダ情報をパケットフラグメントに分割してルータのチェック機能を通過させ、攻撃を実行します。
- すべてのタイプ：上記のすべてのタイプ

Security > DoS Attack Prevention Settings の順にメニューをクリックし、以下の画面を表示します。

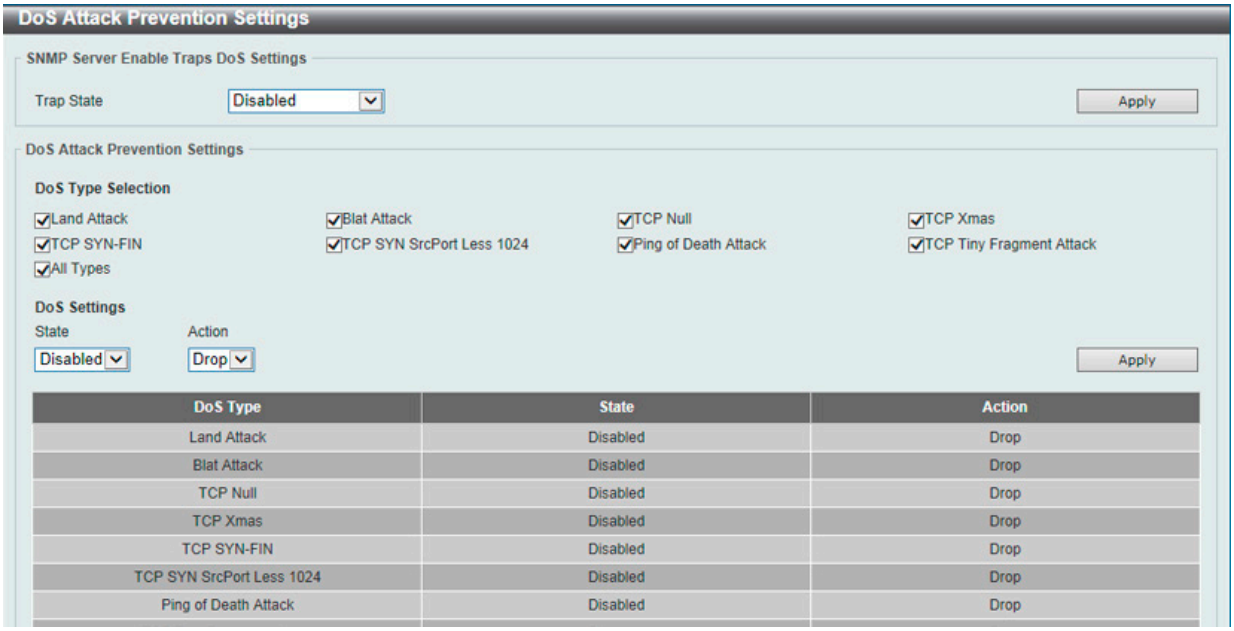


図 12-87　DoS Attack Prevention Settings 画面

画面に表示される項目：

項目	説明
SNMP Server Enable Traps DoS Settings	
Trap State	DoS 攻撃防止のトラップ状態を有効 / 無効に設定します。
DoS Attack Prevention Settings	
DoS Type Selection	DoS 攻撃防御のタイプを選択します。 • 「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 Xmas scan 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。

項目	説明
State	DoS 攻撃防止の状態を有効 / 無効に指定します。
Action	DoS 攻撃を検出したときに実行されるアクションを指定します。 • 「Drop」- 一致する DoS 攻撃パケットをすべて破棄します。

「Apply」ボタンをクリックして、設定内容を適用します。

SSH（Secure Shell）

SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。SSH は、リモートのホストコンピュータへの安全なログインや、リモートのエンドノードでの安全なコマンド実行メソッドを可能にし、信頼関係を結んでいないホスト間に暗号化と認証を利用した安全な通信を提供します。高度なセキュリティ機能を備えた SSH は、今日のネットワーク環境に必要不可欠なツールです。ネットワーク通信を脅かす数々のセキュリティハザードに対して、強力な監視者としての役割を担います。

リモート PC（SSH クライアント）とスイッチ（SSH サーバ）間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

1. 「User Accounts Settings」で管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに他の管理者レベルのユーザアカウントを作成する方法と同じであり、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
2. 「SSH User Settings」画面を使用して、ユーザアカウントを設定します。ここでは、スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「Host Based」、「Password」、「Public Key」の 3 つがあります。
3. 「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。

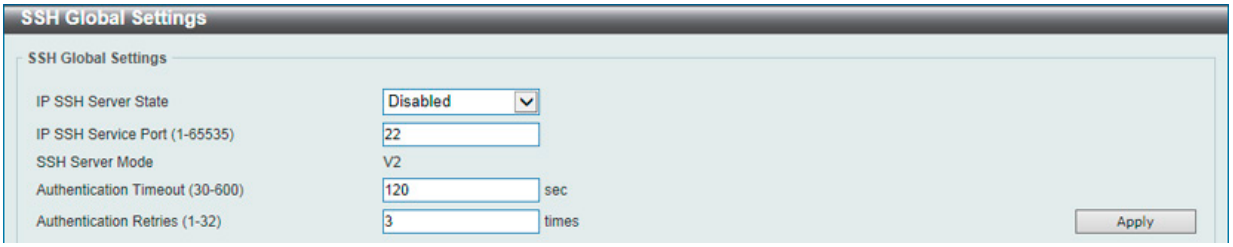


図 12-88　SSH Global Settings 画面

画面に表示される項目：

項目	説明
IP SSH Server State	グローバルに SSH 機能を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
IP SSH Service Port	SSH サービスポート番号を設定します。 • 設定可能範囲：1-65535 • 初期値：22
Authentication Timeout	認証のタイムアウト時間を指定します。 • 設定可能範囲：30-600（秒） • 初期値：120（秒）
Authentication Retries	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。指定した回数を超えると接続が切断され、ユーザは再度スイッチに接続する必要があります。 • 設定可能範囲：1-32 • 初期値：3

「Apply」ボタンをクリックして、設定内容を適用します。

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。

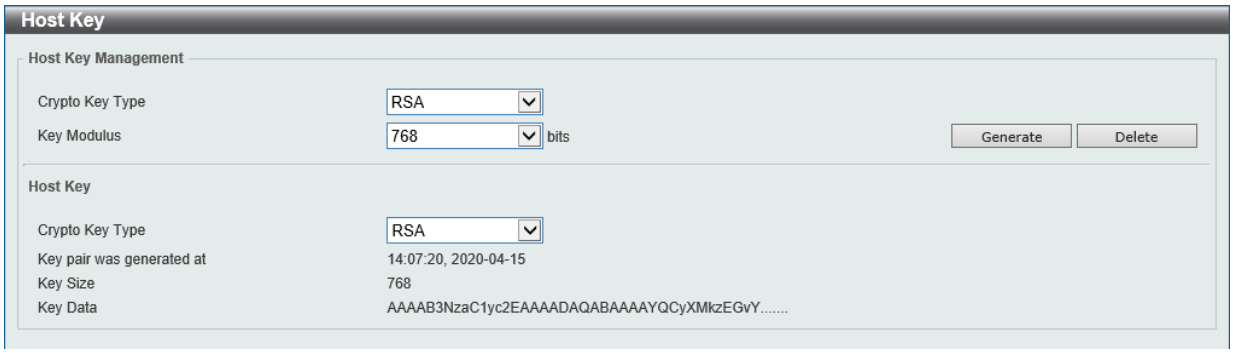


図 12-89　Host Key 画面

画面に表示される項目：

項目	説明
Host Key Management	
Crypto Key Type	暗号鍵の種類を選択します。 • 選択肢：「RSA（Rivest Shamir Adleman)」「DSA（Digital Signature Algorithm）」
Key Modulus	鍵係数の値を入力します。 • 選択肢：「360」「512」「768」「1024」「2048」（ビット）
Host Key	
Crypto Key Type	暗号鍵の種類を選択します。 • 選択肢：「RSA（Rivest Shamir Adleman)」「DSA（Digital Signature Algorithm）」

「Generate」ボタンをクリックして、指定したホスト鍵を生成します。
「Delete」ボタンをクリックして、指定したホスト鍵を削除します。

「Generate」ボタンをクリックすると次の画面が表示されます。

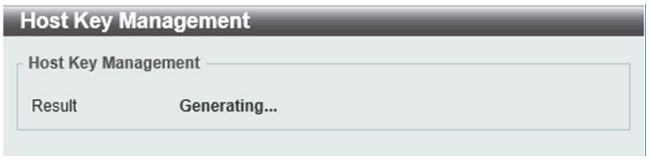


図 12-90　Host Key (Generating) 画面

鍵の生成が完了すると次の画面が表示されます。

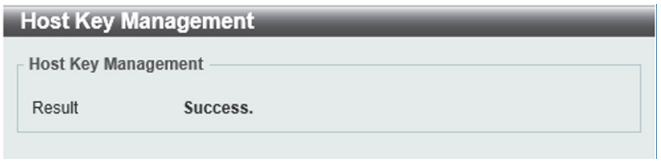


図 12-91　Host Key (Success) 画面

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。

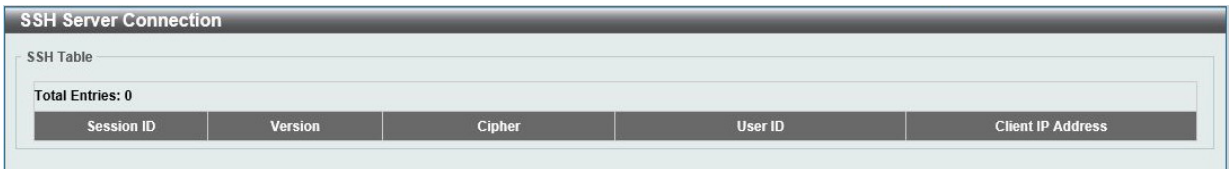


図 12-92　SSH Server Connection 画面

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 ユーザの設定を行います。

Security > SSH > SSH User Settings の順にメニューをクリックし、以下の画面を表示します。

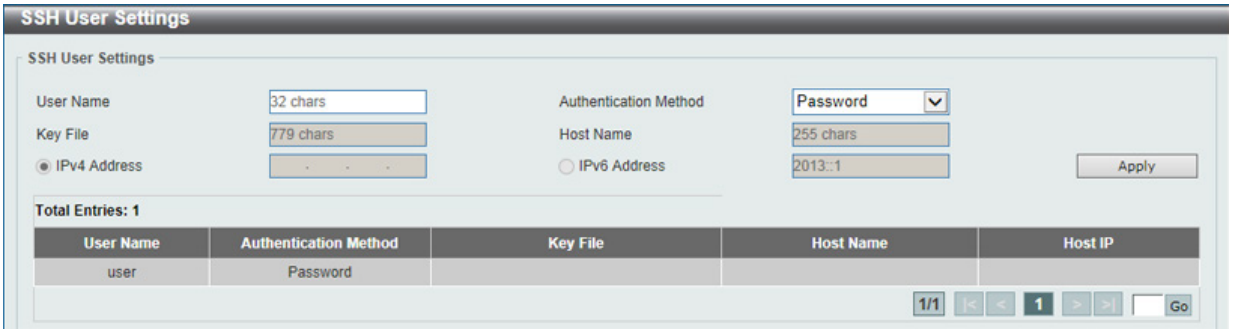


図 12-93　SSH User Settings 画面

画面に表示される項目：

項目	説明
User Name	SSH ユーザを識別するユーザ名を指定します。（半角英数字 32 文字以内）
Authentication Method	スイッチにアクセスを試みるユーザの認証モードを指定します。 • 選択肢：「Password」「Public Key」「Host-based」
Key File	「Public Key」または「Host-based」を選択した場合、公開鍵（Public Key）を入力します。
Host Name	「Host-based」を選択した場合、ホスト名を入力します。
IPv4 Address	「Host-based」を選択した場合、IPv4 アドレスを入力します。
IPv6 Address	「Host-based」を選択した場合、IPv6 アドレスを入力します。

「Apply」ボタンをクリックして、設定内容を適用します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

SSL（Secure Socket Layer）

Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、暗号スイートを使用して実現されます。暗号スイートは、認証セッションに使用される厳密な暗号化パラメータ、特定の暗号化アルゴリズムおよびキー長を決定するセキュリティ文字列であり、以下の 3 つの段階で構成されます。

1. 鍵交換（Key Exchange）
   暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DSA、ここでは DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。これはクライアントとホスト間の最初の認証プロセスであり、「鍵交換」を行って一致した場合、認証が受諾され、次のレベルで暗号化のネゴシエーションが行われます。
2. 暗号化（Encryption）
   暗号スイートの次の部分は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
   - ストリーム暗号（Stream Ciphers）– スイッチは 2 種類のストリーム暗号（40 ビット鍵での RC4 と、128 ビット鍵での RC4）に対応しています。これらの鍵はメッセージの暗号化に使用され、最適に利用するためにはクライアントとホスト間で一致させる必要があります。
   - CBC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、1 つ前の暗号化テキストのブロックを使用して、現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義される 3 DES EDE 暗号化コードと高度な暗号化規格（AES）をサポートし、暗号化されたテキストを生成します。
3. ハッシュアルゴリズム（Hash Algorithm）
   暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージと共に暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）、SHA-256 の 3 つのハッシュアルゴリズムをサポートします。

サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成するために、これら 3 つのパラメータの一意の組み合わせである 11 種類の暗号化スイートについてスイッチ上で設定が可能です。それぞれの暗号化スイートに対して有効 / 無効の設定を行うことが可能ですが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号化スイートに含まれる情報はスイッチには実装されていないため、サードソースから証明書ファイルをダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバやスイッチのファイルシステムを使用してスイッチにダウンロードできます。また、本スイッチは、TLSv1/v2/v3 をサポートしています。それ以外のバージョンは本スイッチとは互換性がない恐れがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する可能性があります。

SSL 機能が有効化されると、通常の HTTP 接続はできなくなります。SSL 機能を使用した Web ベースの管理を行うには、SSL 暗号化がサポートされた Web ブラウザにおいて、https:// で始まる URL を使用する必要があります（例 : https://10.90.90.90）。これらの条件を満たさない場合、エラーが発生し、Web ベースの管理機能への接続認証が行われません。

SSL 機能で使用する証明書ファイルは TFTP サーバからスイッチへダウンロードすることができます。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者や認証のための鍵、デジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバ側とクライアント側で整合性のある証明書ファイルを保持している必要があります。スイッチには初期状態で証明書がインストールされていますが、ユーザ環境に応じて追加のダウンロードが必要になる場合があるかもしれません。

SSL Global Settings（SSL グローバル設定）

SSL グローバル設定を行います。

Security > SSL > SSL Global Settings の順にメニューをクリックし、以下の画面を表示します。



図 12-94　SSL Global Settings 画面

画面に表示される項目：

項目	説明
SSL Global Settings	
SSL Status	SSL のグローバルステータスを有効 / 無効に設定します。
Service Policy	SSL ポリシー名を入力します。（32 文字以内）
Import File	
File Select	ロードされるファイルの種類を指定します。 • 選択肢：「Certificate」「Private Key」 ファイル種類を選択した後、「ファイルを選択」ボタンをクリックし、適切なファイルを選択してローカルコンピュータからロードします。
Destination File Name	宛先ファイル名を指定します。（32 文字以内）
SSL Self-signed Certificate	
Self-signed Certificate	「Generate」ボタンを選択すると、組み込みの自己署名証明書があるかどうかに関係なく、新しい自己署名証明書が生成されます。生成された証明書は、ユーザが所有する証明書には影響しません。

「Apply」ボタンをクリックして、設定内容を適用します。

補足　SSL 自己署名証明書は、キー長が 2048 ビットの自己署名 RSA 証明書のみをサポートします。

注意　F/W バージョン v1.00/1.01 系をご利用の場合、既定で SSL を有効にした際に正しく接続できません。SSL Service Policy を適切に設定して、SSL を有効にする必要があります。

注意　SSL を無効にしても、HTTP は有効になりません。**Management > Telnet/Web** から Web State を有効に変更して下さい。

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。

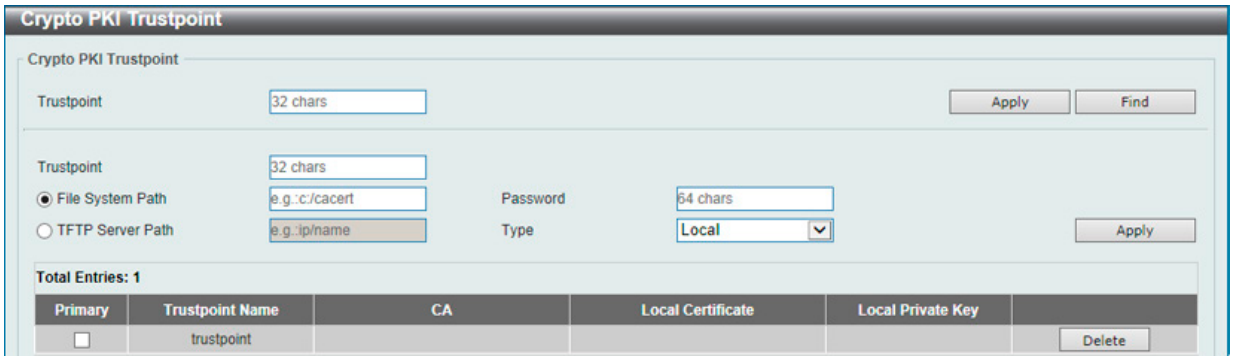


図 12-95　Crypto PKI Trustpoint 画面

画面に表示される項目：

項目	説明
Trustpoint	インポートした証明書と鍵ペアに対応するトラストポイント名を入力します。（32 文字以内）
File System Path	証明書と鍵ペアのファイルシステムパスを入力します。
Password	インポートしたプライベート鍵の暗号を解除する暗号パスフレーズを入力します。（64 文字以内）パスフレーズが指定されないと「NULL」文字列が使用されます。
TFTP Server Path	TFTP サーバのパスを指定します。
Type	インポートされる証明書の種類を指定します。 • 「Both」-「CA 証明書」「ローカル証明書と鍵ペア」をインポートします。 • 「CA」-「CA 証明書」のみインポートします。 • 「Local」-「ローカル証明書と鍵ペア」のみインポートします。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づいて指定エントリを検出します。
「Delete」ボタンをクリックして、指定エントリを削除します。

SSL Service Policy（SSL サービスポリシー）

SSL サービスポリシーの表示、設定を行います。

Security > SSL > SSL Service Policy の順にメニューをクリックし、以下の画面を表示します。

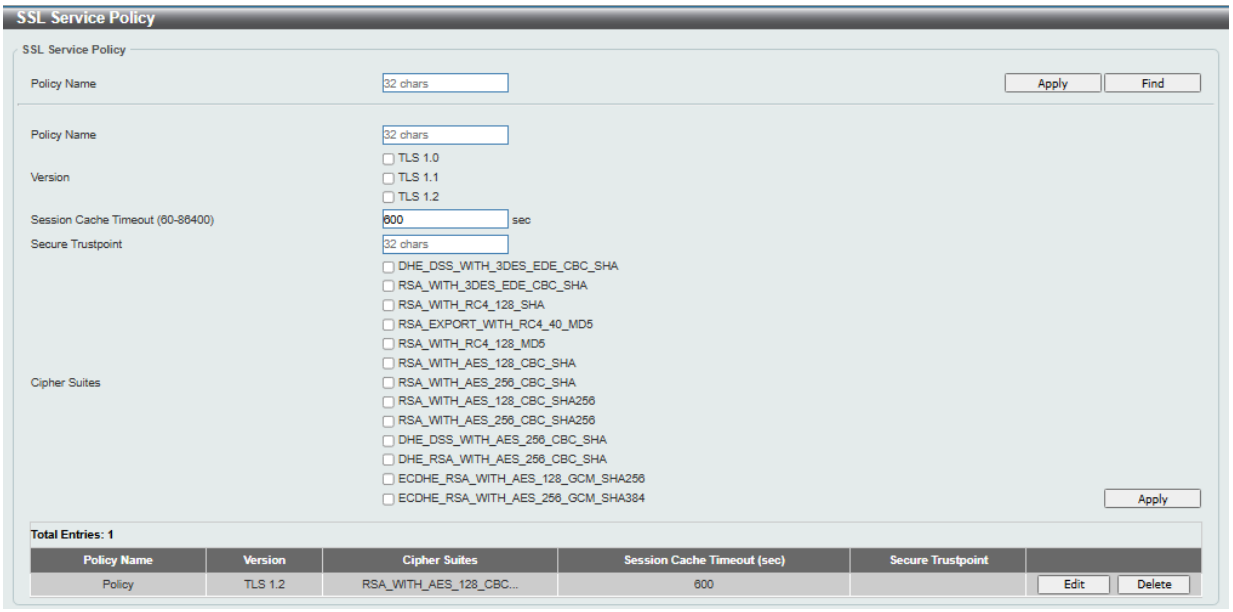


図 12-96　SSL Service Policy 画面

画面に表示される項目：

項目	説明
Policy Name	SSL サービスポリシー名を入力します。（32 文字以内）
Version	「Transport Layer Security」(TLS) のバージョンを指定します。 • 選択肢：「TLS 1.0」「TLS 1.1」「TLS 1.2」
Session Cache Timeout	セッションキャッシュタイムアウトの時間を指定します。 • 設定可能範囲：60-86400（秒） • 初期値：600（秒）
Secure Trustpoint	セキュアなトラストポイントの名前を入力します。（32 文字以内）
Cipher Suites	本プロファイルの暗号スイートを選択します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づいて指定エントリを検出します。
「Edit」ボタンをクリックして、指定エントリを編集します。
「Delete」ボタンをクリックして、指定エントリを削除します。

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。

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。

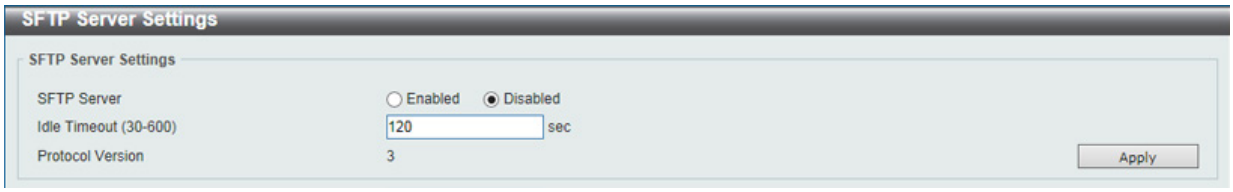


図 12-97　SFTP Server Settings 画面

画面に表示される項目：

項目	説明
SFTP Server	SFTP サーバを有効 / 無効に設定します。
Idle Timeout	アイドルタイムアウトの時間を設定します。指定したセッションアイドルタイマー後、SFTP サーバが動作を検出しない場合、SFTP セッションは終了します。 • 設定可能範囲：30-600（秒） • 初期値：120（秒）

「Apply」ボタンをクリックして、設定内容を適用します。

Network Protocol Port Protect Settings（ネットワークプロトコルポート保護設定）

本項目ではネットワークプロトコルポート保護の設定、表示を行います。

Security > Network Protocol Port Protect Settings の順にメニューをクリックし、以下の画面を表示します。



図 12-98　Network Protocol Port Protect Settings 画面

画面に表示される項目：

項目	説明
TCP Port Protection State	TCP ポート保護ステータスを有効 / 無効に指定します。
UDP Port Protection State	UDP ポート保護ステータスを有効 / 無効に指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)

以下は OAM サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
CFM（Connectivity Fault Management : 接続性障害管理）	CFM 機能を設定します。
Cable Diagnostics（ケーブル診断機能）	スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。
Ethernet OAM（イーサネット OAM）	ポートにイーサネット OAM モード、イベント、ログを設定します。
DDM（DDM 設定）	Digital Diagnostic Monitoring（DDM）機能を実行します。スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定（アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx（送信）電力しきい値設定、および Rx（受信）電力しきい値設定）を行うことができます。

CFM（Connectivity Fault Management : 接続性障害管理）

CFM は IEEE 802.1ag に定義されており、ネットワークにおける接続性故障の検出、隔離、およびレポートを行う標準規格です。

CFM Settings（CFM 設定）

CFM 機能を設定します。

OAM > CFM > CFM Settings の順にメニューをクリックし、以下の画面を表示します。

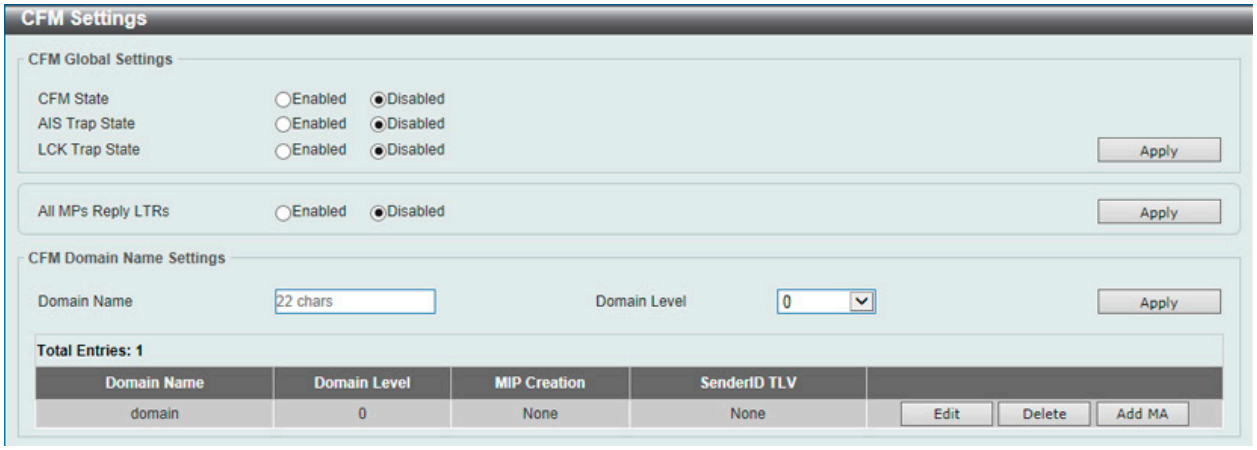


図 13-1　CFM Settings 画面

画面に表示される項目：

項目	説明
CFM Global Settings	
CFM State	CFM 機能を有効 / 無効に設定します。
AIS Trap State	「Alarm Indication Signal」(AIS) トラップ機能を有効 / 無効に設定します。有効にすると「ETH-AIS」イベント発生 / 解消時にトラップが送信されます。
LCK Trap State	「Locked Signal」(LCK) トラップ機能を有効 / 無効に設定します。有効にすると「ETH-LCK」イベント発生 / 解消時にトラップが送信されます。
All MPs Reply LTRs	すべての MP について、Link-Trace Reply (LTR) 機能を有効 / 無効に設定します。IEEE 802.1ag 標準では、ブリッジは Link-Trace Message (LTM) への応答として LTR を返します。本機能を設定すると、LTM のフォワーディングパス上のすべての MP が、ブリッジ上に存在するかどうかについて LTR で応答します。
CFM Domain Name Settings	
Domain Name	メンテナンスドメイン（MD）の名称を入力します。（22 文字以内）スペースを含めることはできません。サービスプロバイダまたはオペレータで使用される MD はそれぞれ固有の名前を持ちます。これにより、各メンテナンスドメインを管理する上で識別が容易になります。
Domain Level	メンテナンスドメインのレベルを選択します。MD レベルを割り当てることで、ドメイン間の階層関係を定義することができます。広い範囲のドメインには大きな値を設定します。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、各セクションで行った変更を適用します。

エントリの編集

編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

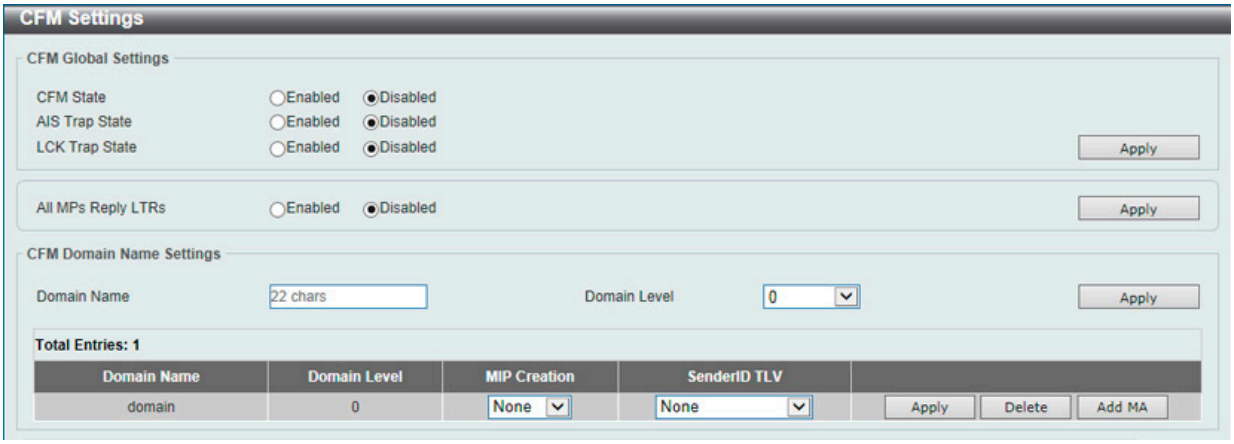


図 13-2　CFM Settings（Edit）画面

画面に表示される項目：

項目	説明
MIP Creation	Maintenance domain Intermediate Point（MIP）オプションを選択します。メンテナンスドメインにおける MIP の作成は、MIP 毎にリンクを追跡する上で役に立ちます。また、ユーザは MEP から MIP へのループバックを実行することもできます。列挙値に基づき、管理エンティティがメンテナンスドメインの MIP Half Functions（MHF）を作成できます。 • 「None」- メンテナンスドメインに MIP を作成しません。 • 「Auto」- 次の場合にこの MD のポートで MIP が作成されます。 - 本 MD レベル以上のアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されていない場合、かつ本レベルの次に低いレベルのアクティブな MD において同じ VID を持つ MA のポートで MEP が設定されている場合、または本 MD レベルより低いアクティブな MD レベルにおいて同じ VID を持つ MA が存在しない場合 • 「Explicit」- 次の場合にこの MD の MA のポートで MIP が作成されます。 - 本 MD レベル以上のアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されていない場合、かつ本レベルの次に低いレベルのアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されている場合 MA 内の中間スイッチには「Auto」を指定してデバイス上に MIP が作成されるようにします。
Sender ID TLV	MD 内の MP による SenderID TLV のデフォルト転送を設定します。 • 「None」- SenderID TLV を転送しません。 • 「Chassis」- シャーシ ID 情報を持つ SenderID TLV を転送します。 • 「Manage」- 管理アドレス情報を持つ SenderID TLV を転送します。 • 「Chassis_Manage」- シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。

「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。

「Delete」ボタンをクリックして、指定エントリを削除します。

Add MA（CFM MA Settings）

メンテナンスアソシエーションを設定します。

OAM > CFM > CFM Settings 画面で「Add MA」ボタンをクリックし、以下の画面を表示します。



図 13-3　CFM Settings（Add MA）- CFM MA Settings 画面

画面に表示される項目：

項目	説明
MA Name	メンテナンスアソシエーション（MA）のエントリ名（22 文字以内）を入力します。同一 MD 内の MA は、それぞれ異なる MA 名を持つ必要があります。別の MD に設定される MA には同じ MA 識別子が設定されていても問題ありません。MA エントリが削除されると設定も削除されます。
MA VID	メンテナンスアソシエーション（MA）エントリの VLAN ID を入力します。 • 設定可能範囲：1-4094

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、エントリを削除します。
前の画面に戻るには、「Back」ボタンをクリックします。
「Add MEP」ボタンをクリックして、MEP（Maintenance End Point）エントリを追加します。

エントリの編集

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。

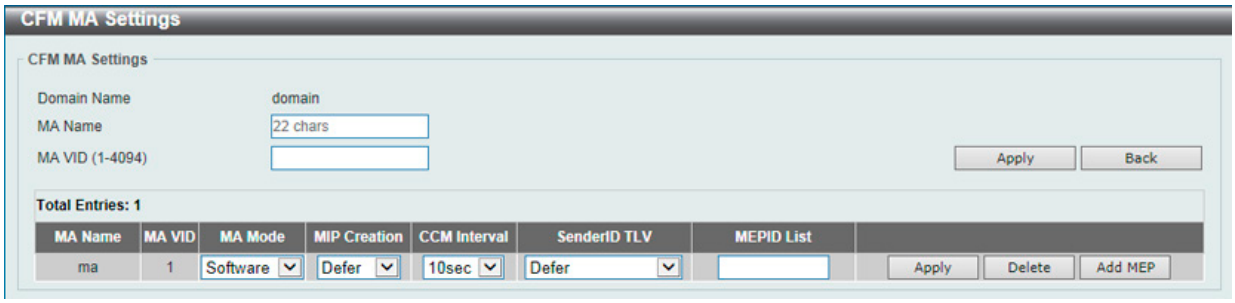


図 13-4　CFM Settings（Add MA）- CFM MA Settings 画面（Edit）

画面に表示される項目：

項目	説明
MIP Creation	MA に対する MIP の作成について設定します。 • 「None」- MA に MIP を作成しません。 • 「Auto」- 次のいずれかの場合にこの MA のポートで MIP が作成されます。 - 本 MD レベル以上のアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されていない場合、かつ本レベルの次に低いレベルのアクティブな MD において同じ VID を持つ MA のポートで MEP が設定されている場合、または本 MD レベルより低いアクティブな MD レベルにおいて同じ VID を持つ MA が存在しない場合 • 「Explicit」- 次の場合にこの MA のポートで MIP が作成されます。 - 本 MD レベル以上のアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されていない場合、かつ本レベルの次に低いレベルのアクティブな MD において同じ VID を持つ MA のポート上で MEP が設定されている場合 • 「Defer」- この MA が関連付けられているメンテナンスドメインの設定を継承します。（初期値） MA 内の中間スイッチには「Auto」を指定してデバイス上に MIP が作成されるようにします。

項目	説明
CCM Interval	Continuity Check Message（CCM）送信間隔を選択します。MEP が MA 内で定期的に CCM パケットを送信する間隔となります。 • 「100ms」- 100 ミリ秒 • 「1sec」- 1 秒 • 「10sec」- 10 秒 • 「1min」- 1 分 • 「10min」- 10 分
SenderID TLV	MA 内の MP による SenderID TLV の転送を制御します。 • 「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 が関連付けられているメンテナンスドメインの設定を継承します。（初期値）
MEPID List	MA に含まれる Maintenance association End Point（MEP）ID を指定します。 • 設定可能範囲：1-8191

項目設定後、「Apply」ボタンをクリックします。

Add MEP（CFM Settings）

MEP を追加します。

「CFM MA Settings」画面で「Add MEP」ボタンをクリックし、以下の画面を表示します。

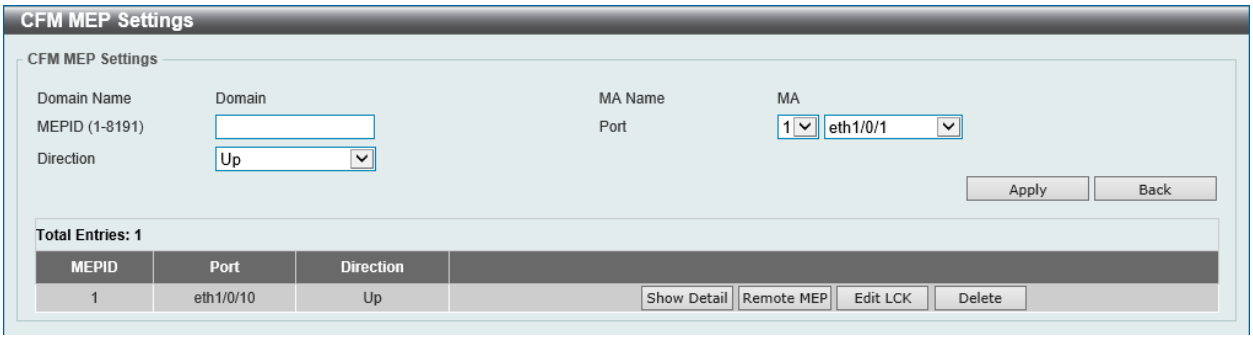


図 13-5　CFM Settings（Add MA, Add MEP）- CFM MEP Settings 画面

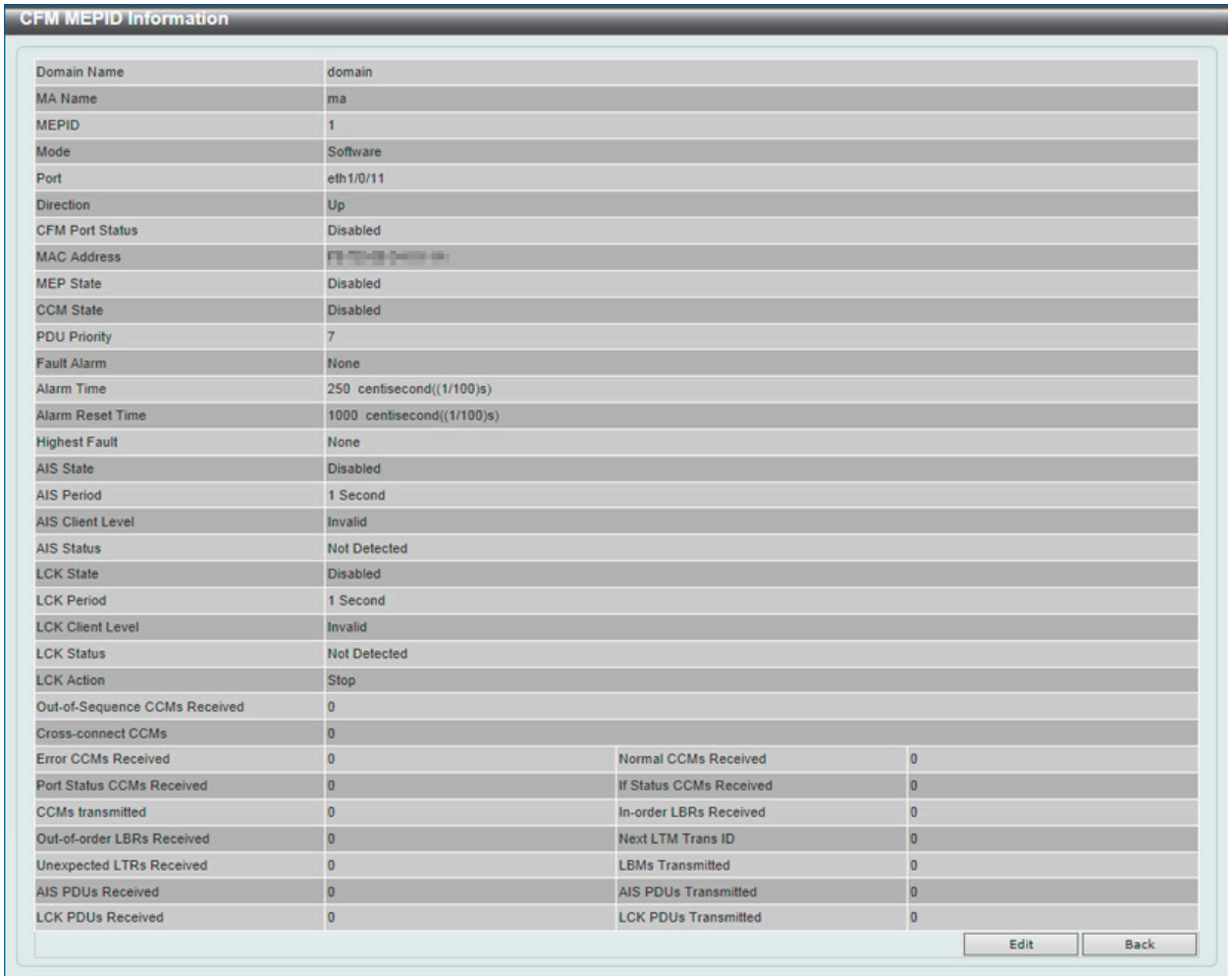
画面に表示される項目：

項目	説明
MEP ID	MEP ID を入力します。同一 MA 内に存在する MEP には、それぞれ固有の MEP ID を設定する必要があります。別の MA に設定される MEP には同じ MEP ID が設定されていても問題ありません。MEP を作成する前に、MA の MEP ID リストに MEP ID を設定しておく必要があります。 • 設定可能範囲：1-8191
Port	設定を適用するユニットとポートを指定します。
Direction	MEP の方向を指定します。 • 「Up」- 内向き（アップ）MEP を作成します。 • 「Down」- 外向き（ダウン）MEP を作成します。

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。
「Show Detail」ボタンをクリックして、指定した MEP の詳細情報を表示します。
「Remote MEP」ボタンをクリックして、Remote MEP テーブルを表示します。
「Edit LCK」ボタンを選択して、指定したエントリの LCK 設定を変更します。
「Delete」ボタンを選択して、指定したエントリを表示します。

詳細情報の参照（Show Detail）

「Show Detail」ボタンをクリックし、以下の画面を表示します。



CFM MEPID Information

Domain Name	domain		
MA Name	ma		
MEPID	1		
Mode	Software		
Port	eth1/0/11		
Direction	Up		
CFM Port Status	Disabled		
MAC Address	[redacted]		
MEP State	Disabled		
CCM State	Disabled		
PDU Priority	7		
Fault Alarm	None		
Alarm Time	250 centisecond((1/100)s)		
Alarm Reset Time	1000 centisecond((1/100)s)		
Highest Fault	None		
AIS State	Disabled		
AIS Period	1 Second		
AIS Client Level	Invalid		
AIS Status	Not Detected		
LCK State	Disabled		
LCK Period	1 Second		
LCK Client Level	Invalid		
LCK Status	Not Detected		
LCK Action	Stop		
Out-of-Sequence CCMs Received	0		
Cross-connect CCMs	0		
Error CCMs Received	0	Normal CCMs Received	0
Port Status CCMs Received	0	If Status CCMs Received	0
CCMs transmitted	0	In-order LBRs Received	0
Out-of-order LBRs Received	0	Next LTM Trans ID	0
Unexpected LTRs Received	0	LBMs Transmitted	0
AIS PDUs Received	0	AIS PDUs Transmitted	0
LCK PDUs Received	0	LCK PDUs Transmitted	0

Edit　Back

図 13-6　CFM Settings（Add MA, Add MEP, Show Detail）- CFM MEP ID Information 画面

「Edit」ボタンを選択して、指定したエントリを変更します。

前の画面に戻るには、「Back」ボタンをクリックします。

MEP の編集

「CFM MDP ID Information」画面で「Edit」ボタンをクリックすると、以下の画面が表示されます。

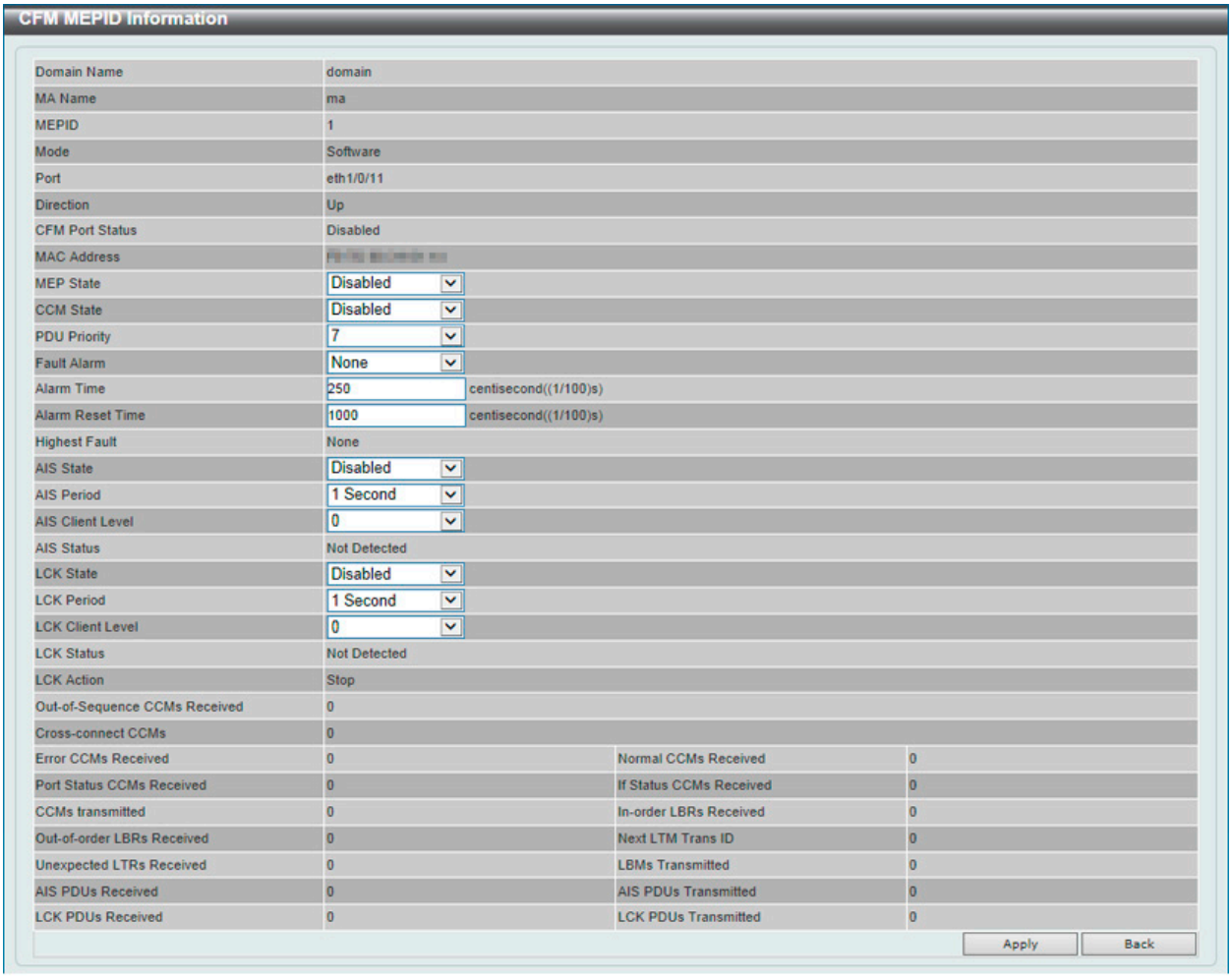


図 13-7　CFM Settings（Add MA, Add MEP, Show Detail）- CFM MEP ID Information 画面（Edit）

画面に表示される項目：

項目	説明
MEP State	インタフェースの MEP 管理状態を有効 / 無効に設定します。
CCM State	CCM 送信状態を有効 / 無効に設定します。
PDU Priority	PDU 優先度の値を設定します。MEP によって送信される CCM およびその他の CFM PDU にセットされる 802.1p プライオリティ値を定義します。 • 設定可能範囲：0-7
Fault Alarm	MEP によって送信される障害アラームのタイプを指定します。 • 「None」- 障害アラームは送信されません。 • 「All」- すべての障害アラームのタイプが送信されます。 • 「MAC-Status」- 優先度が「DefMACstatus」以上である障害アラームのみが送信されます。 • 「Remote-CCM」- 優先度が「DefRemoteCCM」以上である障害アラームのみが送信されます。 • 「Error-CCM」- 優先度が「DefErrorCCM」以上である障害アラームのみが送信されます。 • 「Xcon-CCM」- 優先度が「DefXconCCM」以上である障害アラームのみが送信されます。
Alarm Time	MEP で障害が検出された後、障害アラームが送信されるまでの時間を設定します。 • 設定可能範囲：250-1000（センチ秒） • 初期値：250（センチ秒）
Alarm Reset Time	MEP で検出されたすべての障害が取り除かれてから障害アラームがリセットされるまでの時間を設定します。 • 設定可能範囲：250-1000（センチ秒） • 初期値：1000（センチ秒）
AIS State	インタフェースにおける AIS 機能を有効 / 無効に設定します。
AIS Period	AIS PDU 送信間隔を選択します。 • 選択肢：「1 Second（1 秒）」「1 Minute（1 分）」 • 初期値：「1 Second（1 秒）」

項目	説明
AIS Client Level	MEP が AIS PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は、MIP と MEP が存在する最も近いクライアントレイヤの MD レベルです。 • 設定可能範囲：0-7
LCK State	インタフェースにおける LCK 機能を有効 / 無効に設定します。
LCK Period	LCK PDU 送信間隔を選択します。 • 選択肢：「1 Second（1 秒）」「1 Minute（1 分）」 • 初期値：「1 Second（1 秒）」
LCK Client Level	MEP が LCK PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は、MIP と MEP が存在する最も近いクライアントレイヤの MD レベルです。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

Remote MEP（CFM Settings）

Remote MEP を参照します。

「CFM MEP Settings」画面で「Remote MEP」ボタンをクリックします。

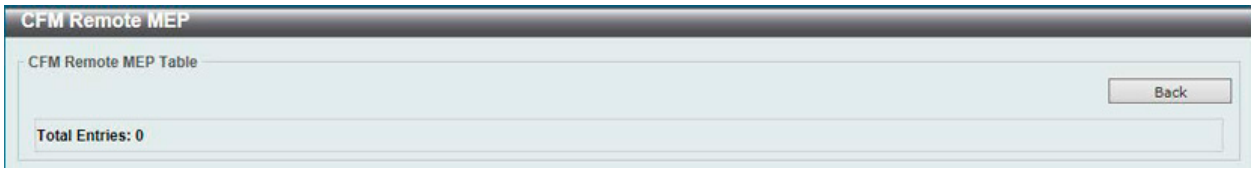


図 13-8　CFM Settings（Add MA, Add MEP, Remote MEP）- CFM Remote MEP 画面

前の画面に戻るには、「Back」ボタンをクリックします。

Edit LCK（CFM Settings）

LCK を編集します。

「CFM MEP Settings」画面で「Edit LCK」ボタンをクリックします。

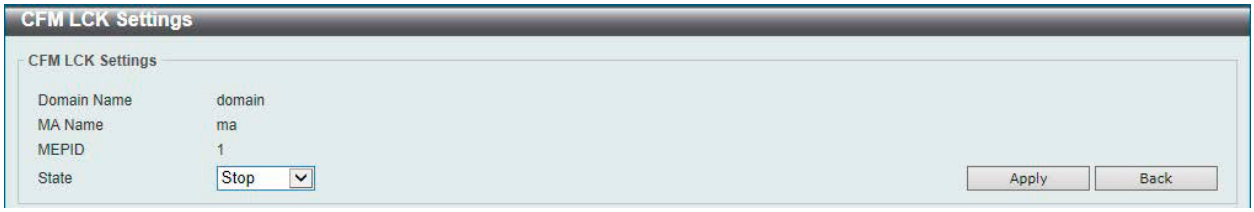


図 13-9　CFM Settings（Add MA, Add MEP, Edit LCK）- CFM LCK Settings 画面

画面に表示される項目：

項目	説明
State	管理ロック動作を指定します。MEP からクライアントレベル MEP に LCK PDU を送信します。 • 選択肢：「Start（開始）」「Stop（停止）」

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

CFM Port Settings（CFM ポート設定）

CFM ポート状態を有効または無効にします。

OAM > CFM > CFM Port Settings の順にメニューをクリックし、以下の画面を表示します。

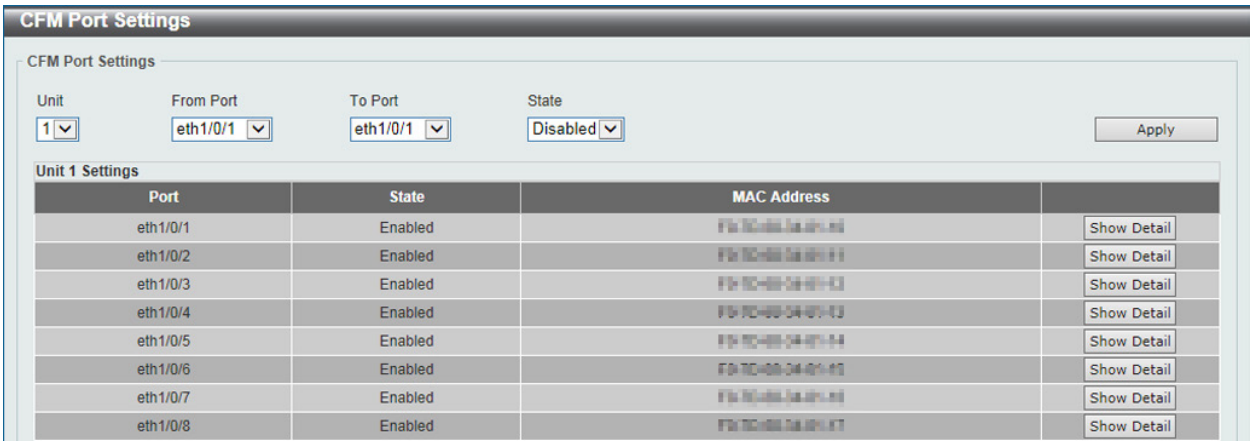


図 13-10　CFM Port Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
State	特定ポートの CFM 設定を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

詳細情報の表示

「Show Detail」ボタンをクリックし、以下の画面を表示します。



図 13-11　CFM Port Settings（Show Detail ）- CFM Port Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

CFM Loopback Test（CFM ループバックテスト）

CFM ループバックテストを設定します。

OAM > CFM > CFM Loopback Test の順にメニューをクリックし、以下の画面を表示します。

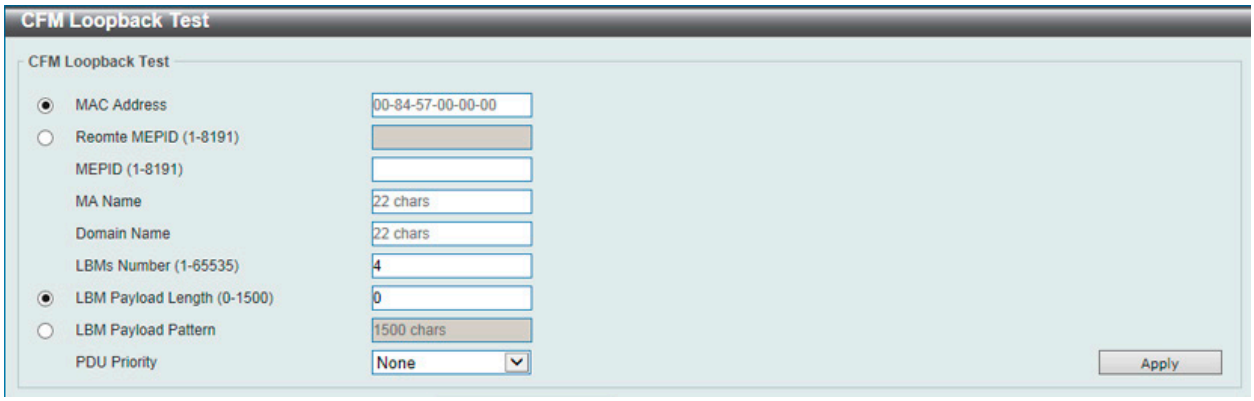


図 13-12　CFM Loopback Test 画面

画面に表示される項目：

項目	説明
MAC Address	宛先 MAC アドレスを入力します。
Remote MEPID	リモート MEP ID を入力します。 • 設定可能範囲：1-8191
MEP ID	ループバックテストを開始する MEP ID を入力します。 • 設定可能範囲：1-8191
MA Name	使用するメンテナンスアソシエーション名を指定します。（22 文字以内）
Domain Name	使用するメンテナンスドメイン名を指定します。（22 文字以内）
LBMs Number	送信する LBM 数を指定します。 • 設定可能範囲：1-65535 • 初期値：4
LBM Payload Length	送信される LBM のペイロード長を指定します。 • 設定可能範囲：0-1500 • 初期値：0
LBM Payload Pattern	LBM のペイロードパターンを指定します。Data TLV が含まれるかどうかの指定と、Data TLV に含まれる任意の数のデータを指定します。（1500 文字以内）スペースを含めることはできません。
PDU Priority	送信される LBM に設定される 802.1p プライオリティを指定します。指定しない場合、MA が送信した CCM と同じ優先度を使用します。 • 選択肢：0-7 • 初期値：「None」（なし）

「Apply」ボタンをクリックして、設定内容を適用します。

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。

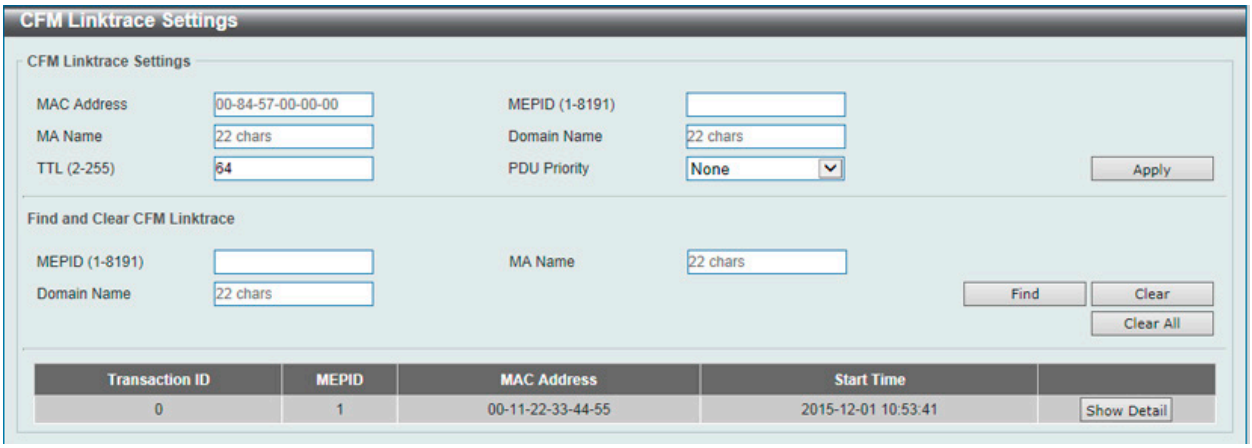


図 13-13　CFM Linktrace Settings 画面

画面に表示される項目：

項目	説明
CFM Linktrace Settings	
MAC Address	宛先 MAC アドレスを入力します。
MEP ID	リンクトレース機能を開始する MEP ID を指定します。 • 設定可能範囲：1-8191
MA Name	使用するメンテナンスアソシエーション名を指定します。（22 文字以内）
Domain Name	使用するメンテナンスドメイン名を指定します。（22 文字以内）
TTL	リンクトレースメッセージの TTL 値を指定します。 • 設定可能範囲：2-255 • 初期値：64
PDU Priority	送信される LTM に設定される 802.1p プライオリティを選択します。指定しない場合、MA が送信した CCM と同じ優先度を使用します。 • 選択肢：：0-7 • 初期値：「None」（なし）
Find and Clear CFM Linktrace	
MEPID	MEP ID を入力します。 • 設定可能範囲：1-8191
MA Name	使用するメンテナンスアソシエーション名を指定します。（22 文字以内）
Domain Name	使用するメンテナンスドメイン名を指定します。（22 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、入力した情報を基にエントリをクリアします。
「Clear All」ボタンをクリックして、すべてのエントリに紐づく情報をクリアします。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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。

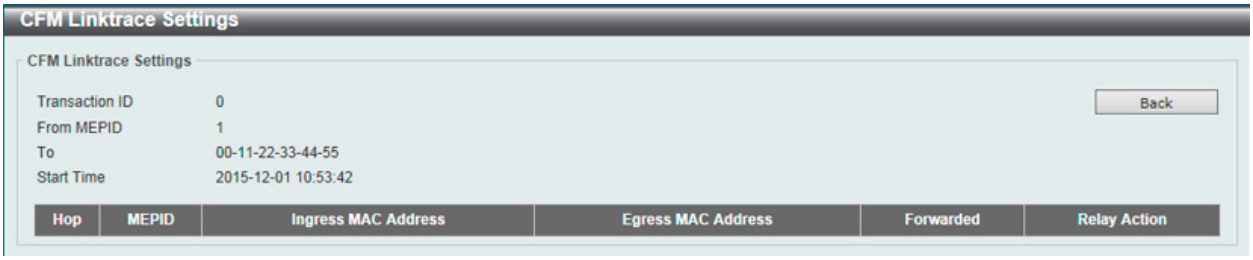


図 13-14　CFM Linktrace Settings（Show Detail）- CFM Linktrace Settings 画面

前の画面に戻るには、「Back」ボタンをクリックします。

CFM Packet Counter（CFM パケットカウンタ）

OSPF パケットカウンタ情報を表示します。

OAM > CFM > CFM Packet Counter の順にメニューをクリックし、以下の画面を表示します。

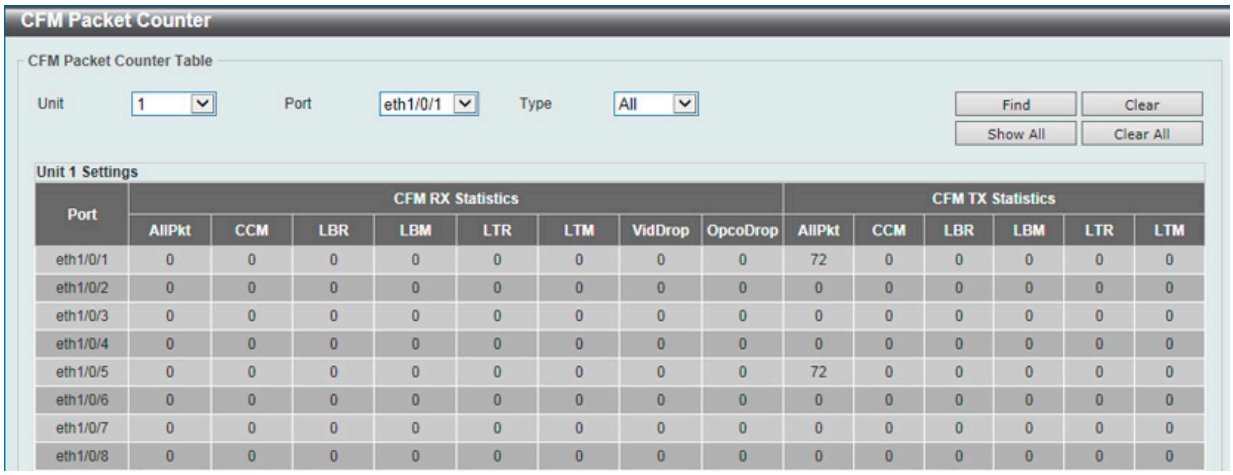


図 13-15　CFM Packet Counter 画面

画面に表示される項目：

項目	説明
Unit	カウンタを参照 / 削除するユニットを指定します。
Port	カウンタを参照 / 削除するポートを選択します。
Type	パケットの種類を選択します。 • 「RX」- 受信したすべての CFM パケットのカウンタ情報を表示 / 削除します。 • 「TX」- 送信したすべての CFM パケットのカウンタ情報を表示 / 削除します。 • 「All」- 送受信したすべての CFM パケットのカウンタ情報を表示 / 削除します。

「Find」ボタンをクリックして、指定条件に基づくカウンタ情報を検索 / 表示します。
「Show All」ボタンをクリックして、すべてのカウンタ情報を表示します。
「Clear」ボタンをクリックして、指定条件に基づいてカウンタ情報をクリアします。
「Clear All」ボタンをクリックして、すべてのカウンタ情報をクリアします。

CFM Counter CCM（CFM カウンタ CCM）

CFM カウンタ CCM 情報を表示します。

OAM > CFM > CFM Counter CCM の順にメニューをクリックし、以下の画面を表示します。



図 13-16　CFM Counter CCM 画面

「Clear」ボタンをクリックして、すべてのエントリに紐づくカウンタ情報をクリアします。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

CFM MIP CCM Table（CFM MIP CCM テーブル）

MIP CCM 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。

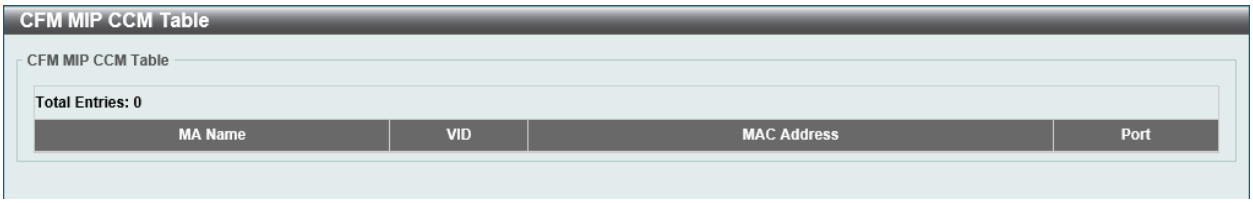


図 13-17　CFM MIP CCM Table 画面

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 13-18　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。

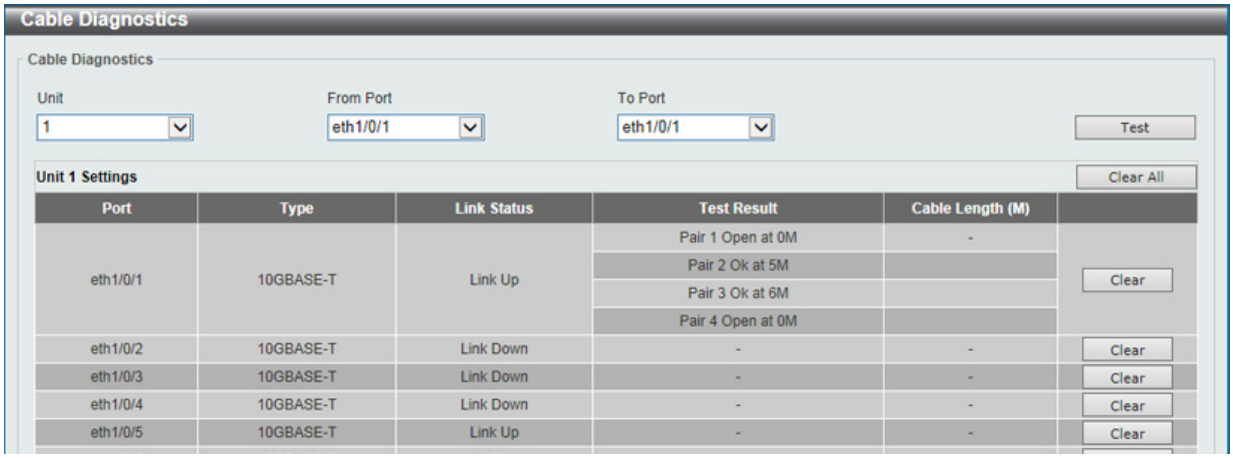


図 13-19　Cable Diagnostics 画面

画面に表示される項目：

項目	説明
Unit	診断を実行するユニットを選択します。
From Port / To Port	診断を実行するポート範囲を指定します。

「Test」ボタンをクリックして、指定ポートのケーブル診断を実行します。
「Clear」ボタンをクリックして、指定ポートの情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。

診断結果のメッセージは以下の通りです。

項目	説明
Test Result	ケーブル診断の結果が表示されます。 • OK - ケーブルの状態に問題はありません。 • Short - UTP ケーブルでショートが発生しています。 • Open - UTP ケーブルが断線しているか、接続が外れています。 • CrossTalk - UTP ケーブルと他のケーブルとのクロストークが発生しています。 • Unknown - ケーブルのステータスを取得できません。再試行してください。 • NA - ケーブルが見つかりませんでした。ケーブルが診断仕様外であるか、品質が悪い可能性があります。

注意　ケーブル診断機能は Copper ポートのみでサポートされます。

注意　より正確なテスト結果を得るには、RJ45 コネクタの TIA/EIA-568B ピン割り当てを使用します。

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。

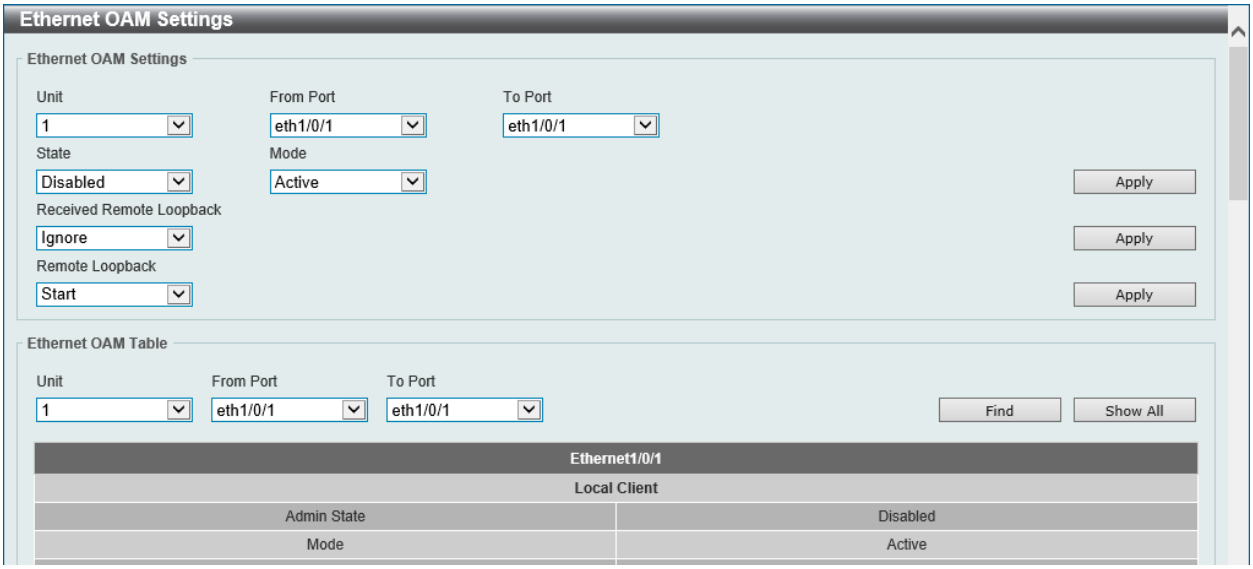


図 13-20　Ethernet OAM Settings 画面

画面に表示される項目：

項目	説明
Ethernet OAM Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	指定ポートで OAM 機能を有効 / 無効に設定します。 本機能を有効化すると、インタフェースで OAM ディスカバリが開始されます。OAM モードが「Active」の場合、ディスカバリが開始され、「Passive」の場合、ピアから受信したディスカバリに応答します。
Mode	イーサネット OAM モードを指定します。 • 選択肢：「Active」「Passive」 Active モードでは、次の 2 つのアクションが許可されます。Passive モードでは許可されません。 （1）OAM ディスカバリの開始 （2）リモートループバックの開始 / 停止
Received Remote Loopback	ピアからのイーサネット OAM リモートループバック要求に対する指定ポート上での動作を指定します。 • 「Ignore」- ピアからのリモートループバック要求を無視します。 • 「Process」- ピアからのリモートループバック要求を処理します。 リモートループバックモードでは、全てのユーザトラフィックは処理されません。受信したリモートループバックを無視することで、ポートがリモートループバックモードに移行することを回避することができます。
Remote Loopback	リモートループバックのアクションを選択します。 • 「Start」- リモートループバックモードに変更するようにピアに要求します。 • 「Stop」- 通常の操作モードに変更するようにピアに要求します。 リモートピアがリモートループバック要求を無視するように設定されている場合、要求を受信してもリモートループバックモードへの移行や離脱を行いません。リモートピアがリモートループバックモードへ移行するには、ローカルクライアントが Active モードかつ OAM 接続が確立されている必要があります。ローカルクライアントが既にリモートループバックモードの場合、本機能は適用されません。
Ethernet OAM Table	
Unit	表示するユニットを指定します。
From Port / To Port	表示するポート範囲を設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）

ポートにイーサネット OAM のイベントを設定します。

OAM > Ethernet OAM > Ethernet OAM Configuration Settings の順にメニューをクリックし、以下の画面を表示します。

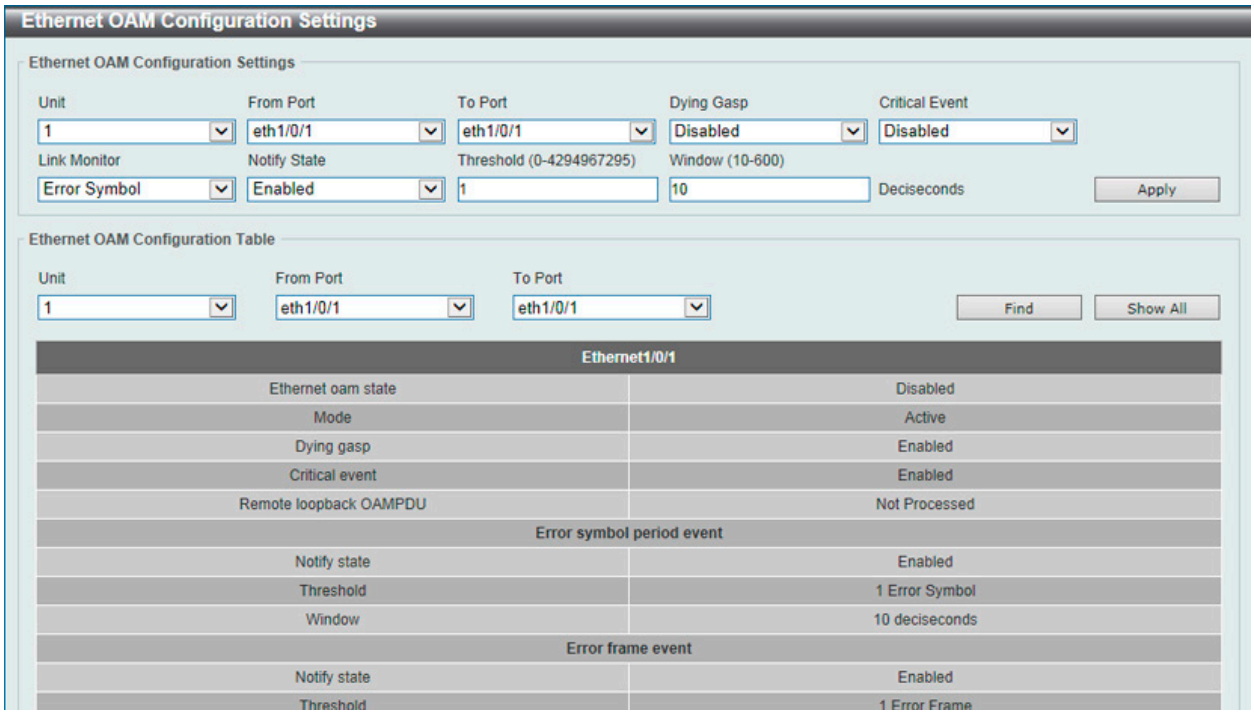


図 13-21　Ethernet OAM Configuration Settings 画面

画面に表示される項目：

項目	説明
Ethernet OAM Configuration Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Dying Gasp	「Dying Gasp」を有効 / 無効に設定します。電源障害など回復不可能なイベントの発生の検出について指定します。本機能が無効化されている場合、回復不可能なローカル障害が発生した際に、Dying Grasp イベントのビットを含む OAM PDU がポートから送信されません。
Critical Event	イーサネット OAM の重大イベント機能を有効 / 無効に設定します。本機能が無効化されている場合、指定されていない重大イベントが発生した際に、クリティカルイベントのビットを含む OAM PDU がポートから送信されません。
Link Monitor	リンクモニタ機能を設定します。 • 「Error Symbol」- イーサネット OAM エラーシンボルのイベント通知を有効化し、モニタリングのしきい値とウィンドウを設定します。 • 「Error Frame」- イーサネット OAM エラーフレームのイベント通知を有効化し、モニタリングのしきい値とウィンドウを設定します。 • 「Error Frame Seconds」- イーサネット OAM エラーフレーム秒のイベント通知を有効化し、モニタリングのしきい値とウィンドウを設定します。 • 「Error Frame Period」- イーサネット OAM エラーフレーム期間のイベント通知を有効化し、モニタリングのしきい値とウィンドウを設定します。
Notify State	イベント通知を有効 / 無効に設定します。
Threshold	しきい値を設定します。 • 「Error Symbol」選択時 - シンボルエラーの数を入力します。指定期間（Window）におけるシンボルエラーの数がしきい値を超えた場合、イベントが生成されます。0-4294967295 の範囲で指定します。 • 「Error Frame」選択時 - フレームエラーの数を入力します。指定期間（Window）におけるフレームエラーの数がしきい値を超えた場合、イベントが生成されます。0-4294967295 の範囲で指定します。 • 「Error Frame Seconds」選択時 - フレームエラーの秒数を入力します。指定期間（Window）におけるフレームエラーの秒数がしきい値を超えた場合、イベントが生成されます。1-900（秒）の範囲で指定します。 • 「Error Frame Period」選択時 - フレームエラーの数を入力します。指定フレーム数（Window）におけるフレームエラーがしきい値を超えた場合、イベントが生成されます。0-4294967295 の範囲で指定します。

項目	説明
Window	ウィンドウを設定します。 • 「Error Symbol」選択時 - この期間内でシンボルエラーの発生数がしきい値を超えた場合、イベント通知の OAM PDU が生成されます。これには、しきい値を超過したことを示すエラーシンボル期間イベント TLV が含まれます。10-600（デシ秒）の範囲で指定します。 • 「Error Frame」選択時 - この期間内でフレームエラーの発生数がしきい値を超えた場合、イベント通知の OAM PDU が生成されます。これには、しきい値を超過したことを示すエラーフレーム期間イベント TLV が含まれます。10-600（デシ秒）の範囲で指定します。 • 「Error Frame Seconds」選択時 - この期間内でフレームエラーの秒数がしきい値を超えた場合、イベント通知の OAM PDU が生成されます。これには、しきい値を超過したことを示すエラーフレーム秒サマリイベント TLV が含まれます。100-9000（デシ秒）の範囲で指定します。 • 「Error Frame Period」選択時 - この指定フレーム数で発生したフレームエラーがしきい値を超えた場合、イベント通知の OAM PDU が生成されます。これには、しきい値を超過したことを示すエラーフレーム期間イベント TLV が含まれます。下限値は、物理レイヤにおいて 100ms 内で受信可能な最小フレームサイズのフレーム数です。上限値は、物理レイヤにおいて 1 分内で受信可能な最小フレームサイズのフレーム数です。1488100-8928600000 の範囲で指定します。
Ethernet OAM Configuration Table	
Unit	設定を表示するユニットを選択します。
From Port / To Port	設定を表示するポート範囲を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

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。

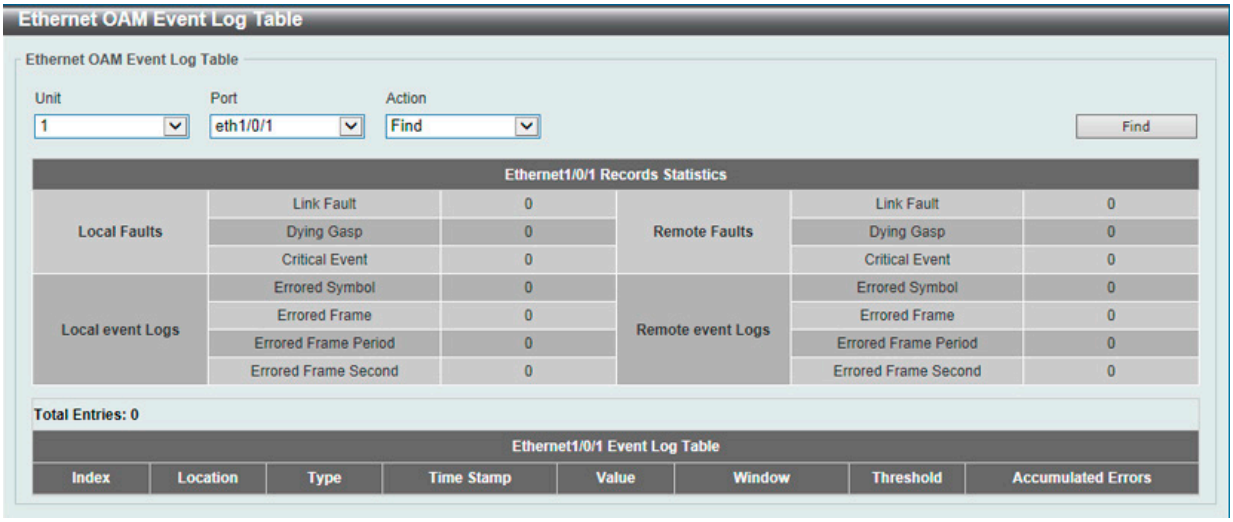


図 13-22　Ethernet OAM Event Log Table 画面

画面に表示される項目：

項目	説明
Unit	ログを参照 / 削除するユニットを指定します。
Port	ログを参照 / 削除するポート範囲を選択します。
Action	実行する動作を指定します。 • 「Find」- 指定ポートのログエントリを表示します。 • 「Clear」- 指定ポートのログエントリを削除します。

「Find」ボタンをクリックして、指定ポートのログエントリを表示します。
「Clear」ボタンをクリックして、指定条件に基づくエントリを削除します。

Ethernet OAM Statistics Table（イーサネット OAM 統計情報テーブル）

ポートのイーサネット OAM 統計情報を表示します。

OAM > Ethernet OAM > Ethernet OAM Statistics Table の順にメニューをクリックし、以下の画面を表示します。

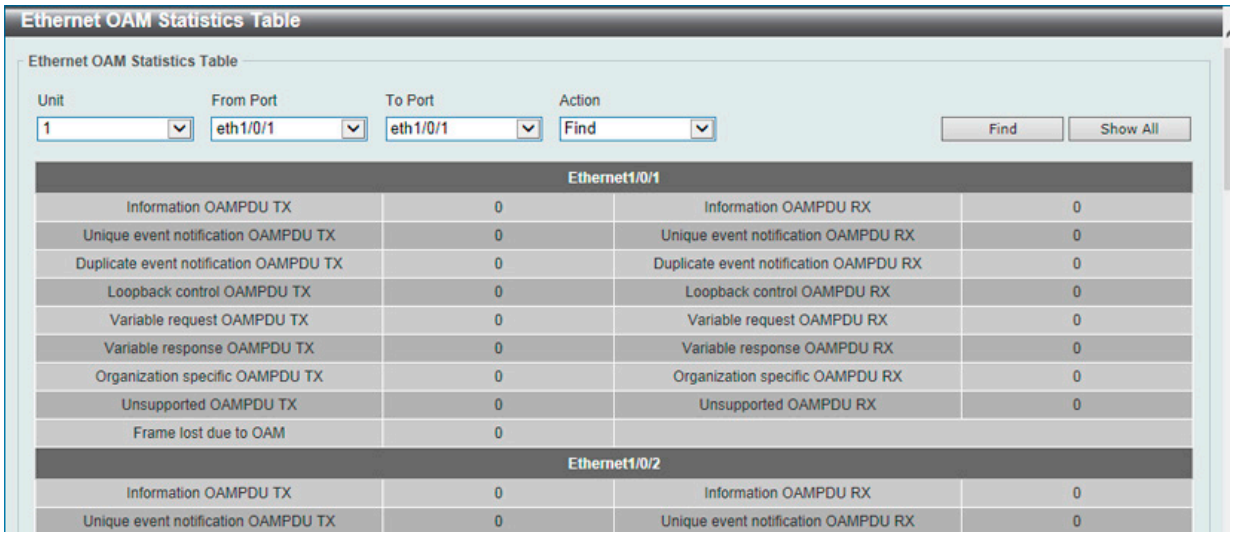


図 13-23　Ethernet OAM Statistics Table 画面

画面に表示される項目：

項目	説明
Unit	ログを参照 / 削除するユニットを指定します。
From Port / To Port	ログを参照 / 削除するポート範囲を選択します。
Action	実行する動作を指定します。 • 「Find」- 指定ポートの統計情報を表示します。 • 「Clear」- 指定ポートの統計情報を削除します。

「Find」ボタンをクリックして、指定条件に基づく統計情報を表示します。
「Show All」ボタンをクリックして、すべての統計情報を表示します。
「Clear」ボタンをクリックして、指定条件に基づく統計情報を削除します。
「Clear All」ボタンをクリックして、テーブル上のすべての統計情報を削除します。

Ethernet OAM DULD Settings（イーサネット OAM DULD 設定）

本項目ではイーサネット OAM「D-Link Unidirectional Link Detection」(DULD) の設定、表示を行います。DULD は、802.3ah イーサネット OAM の拡張機能です。PHY サポート外の単方向ポイントツーポイントイーサネットリンクの検出を行います。OAM ベンダ固有のメッセージが検出に使用されます。検出プロセスは、OAM ディスカバリの開始後に開始されますが、設定された検出時間内にはネゴシエーションは完了しません。

OAM > Ethernet OAM > Ethernet OAM DULD Settings の順にメニューをクリックし、以下の画面を表示します。

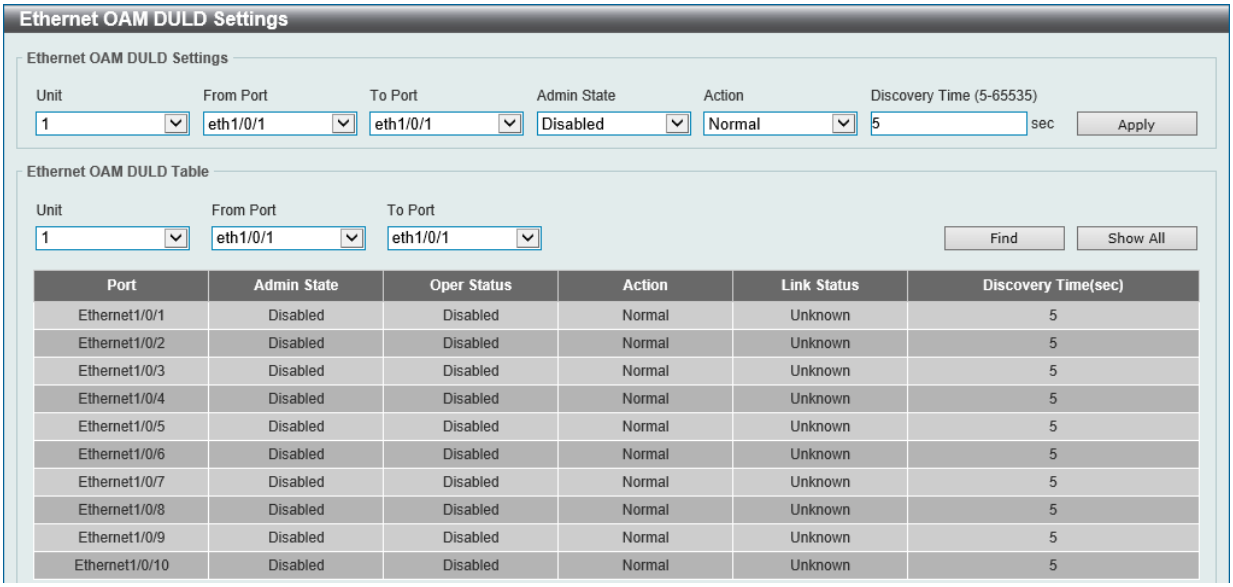


図 13-24　Ethernet OAM DULD Settings 画面

画面に表示される項目：

項目	説明
Ethernet OAM DULD Settings	
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Admin State	管理ステータスを有効 / 無効に設定します。指定ポートの単方向リンク検出状態を有効にするために使用されます。
Action	実行するアクションを選択します。 • 選択肢：「Normal」「Shutdown」
Discovery Time	検出時間を入力します。OAM ディスカバリによるネゴシエーションが正常に完了しないまま検出がタイムアウトになると、単方向リンク検出が開始します。 • 設定可能範囲：5-65535（秒） • 初期値：5（秒）
Ethernet OAM DULD Table	
Unit	設定を表示するユニットを指定します。
From Port / To Port	設定を表示するポート範囲を設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、指定した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。

DDM（DDM 設定）

Digital Diagnostic Monitoring（DDM）機能の設定を行います。スイッチに挿入した SFP/SFP+ モジュールの DDM 状態の参照、各種設定（アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx（送信）電力しきい値設定、Rx（受信）電力しきい値設定）を行うことができます。

DDM Settings（DDM 設定）

アラームしきい値や警告しきい値を超過するイベントが発生した際に、指定ポートで実行するアクションを設定します。

OAM > DDM > DDM Settings の順にメニューをクリックし、以下の画面を表示します。

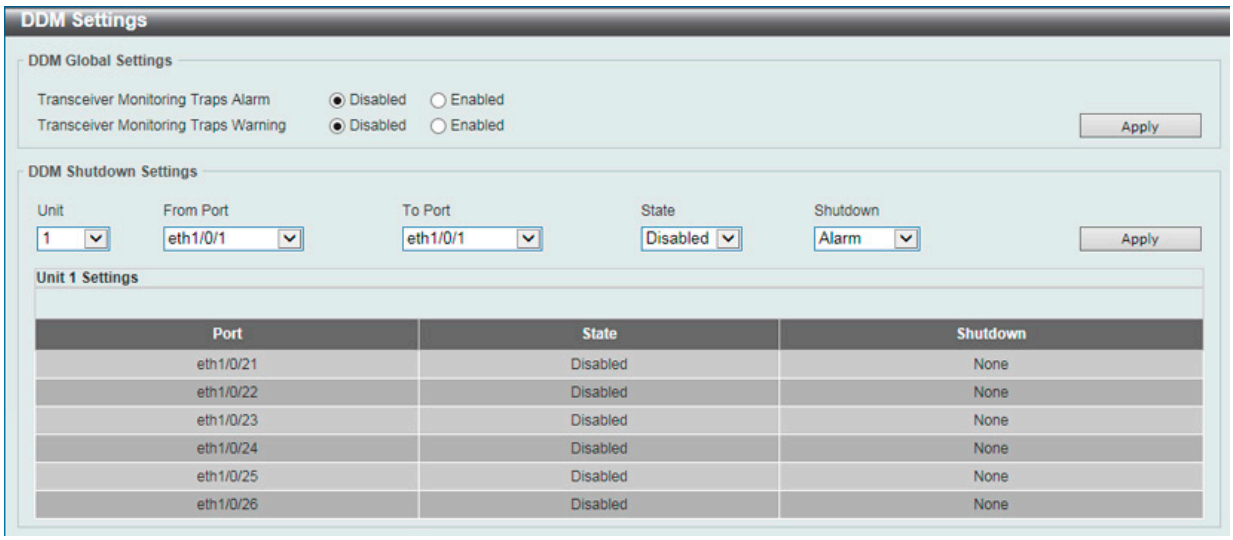


図 13-25　DDM Settings 画面

画面に表示される項目：

項目	説明
Transceiver Monitoring Traps Alarm	トランシーバモニタリングのトラップアラームを有効 / 無効に設定します。
Transceiver Monitoring Traps Warning	トランシーバモニタリングのトラップ警告を有効 / 無効に設定します。
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	DDM の状態を有効 / 無効に設定します。
Shutdown	動作パラメータが Alarm または Warning しきい値を超過した際に、ポートをシャットダウンするかどうかを指定します。 • 「Alarm」- Alarm しきい値を超過した場合にポートをシャットダウンします。 • 「Warning」- Warning しきい値を超過した場合にポートをシャットダウンします。 • 「None」- しきい値の超過に関わらずシャットダウンは実行されません。（初期値）

「Apply」ボタンをクリックして、設定内容を適用します。

DDM Temperature Threshold Settings（DDM 温度しきい値設定）

スイッチの特定ポートに DDM 温度しきい値設定を行います。

OAM > DDM > DDM Temperature Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

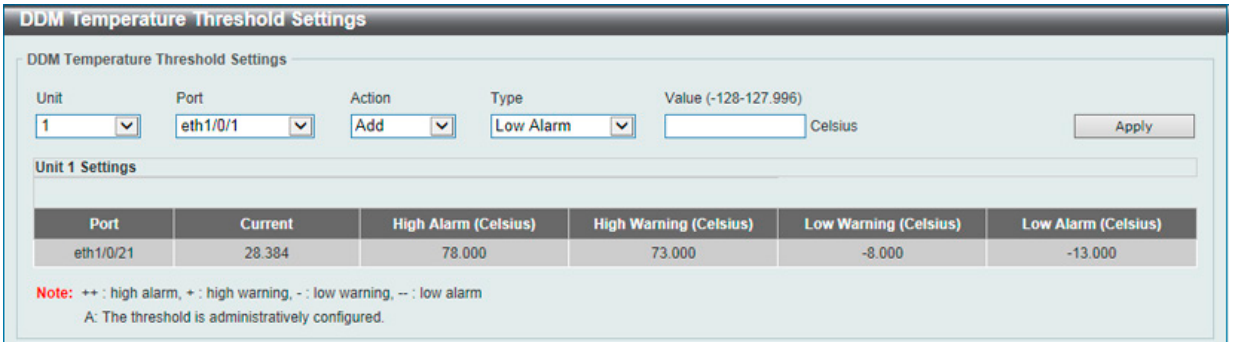


図 13-26　DDM Temperature Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	温度しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	温度しきい値の値について指定します。 • 設定可能範囲：-128 ～ 127.996（℃）

「Apply」ボタンをクリックして、設定内容を適用します。

DDM Voltage Threshold Settings（DDM 電圧しきい値設定）

スイッチの特定ポートに電圧しきい値を設定します。

OAM > DDM > DDM Voltage Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

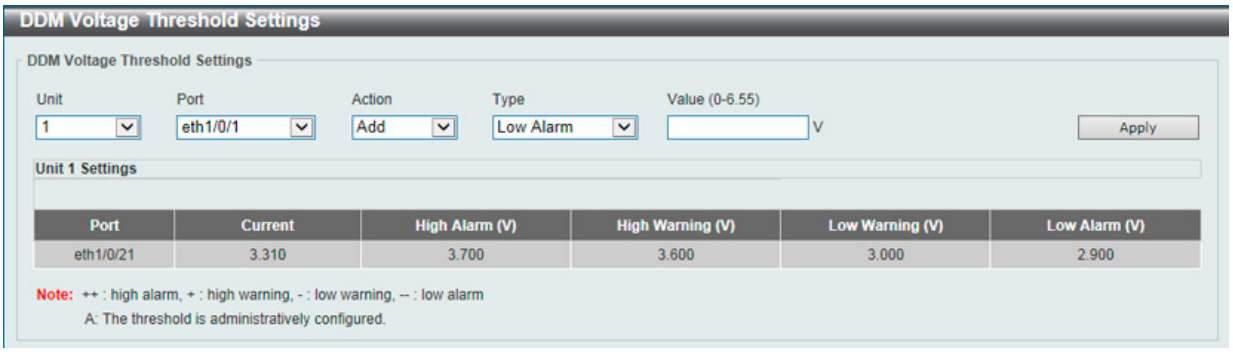


図 13-27　DDM Voltage Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	電圧しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	電圧しきい値の値について指定します。 • 設定可能範囲：0-6.55（V）

「Apply」ボタンをクリックして、設定内容を適用します。

DDM Bias Current Threshold Settings（DDM バイアス電流しきい値設定）

スイッチの特定ポートにバイアス電流しきい値を設定します。

OAM > DDM > DDM Bias Current Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

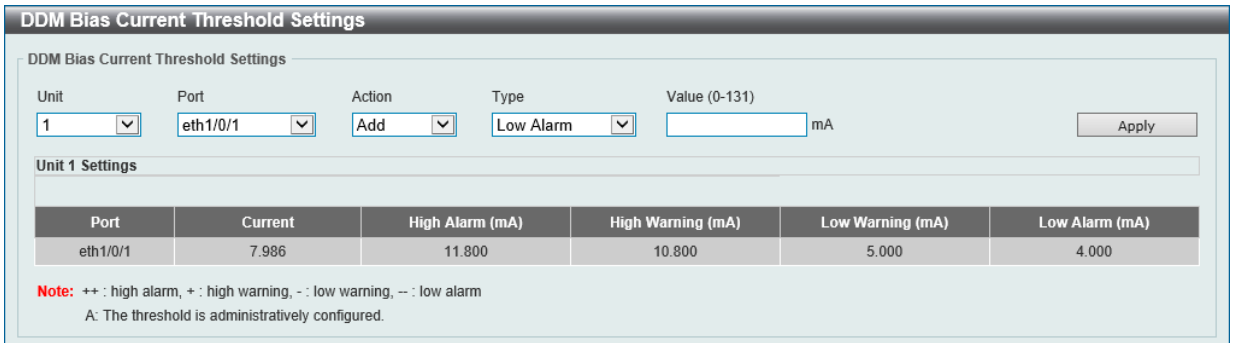


図 13-28　DDM Bias Current Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポートを指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	バイアス電流しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	バイアス電流しきい値の値について指定します。 • 設定可能範囲：0-131（mA）

「Apply」ボタンをクリックして、設定内容を適用します。

DDM TX Power Threshold Settings（DDM 送信電力しきい値設定）

スイッチの特定ポートに送信電力しきい値を設定します。

OAM > DDM > DDM TX Power Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

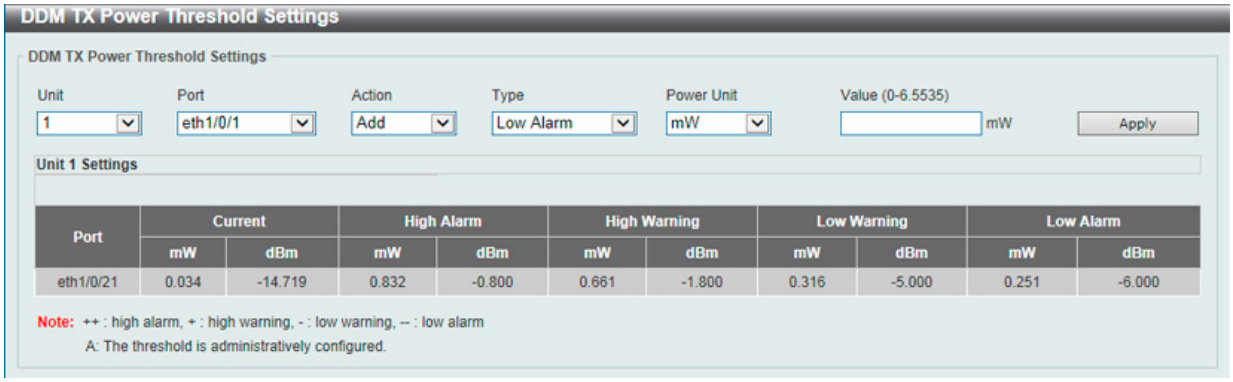


図 13-29　DDM TX Power Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	送信電力しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Power Unit	送信電力単位について指定します。 • 選択肢：「mW」「dBm」
Value	送信電力しきい値の値について指定します。 • 設定可能範囲：0-6.5535（mW） -40 ～ 8.1647（dBm）

「Apply」ボタンをクリックして、設定内容を適用します。

DDM RX Power Threshold Settings（DDM 受信電力しきい値設定）

スイッチの特定ポートに受信電力しきい値を設定します。

OAM > DDM > DDM RX Power Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

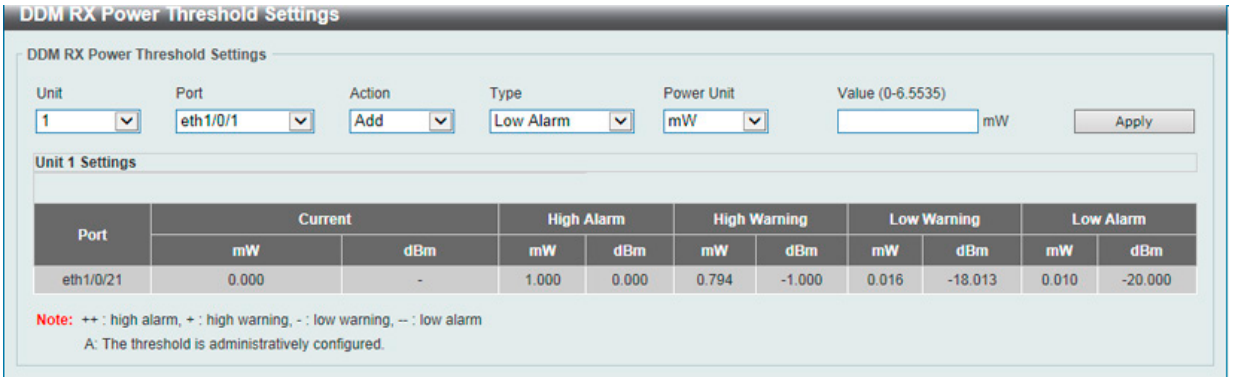


図 13-30　DDM RX Power Threshold Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Port	本設定を適用するポート範囲を指定します。
Action	実行するアクションを指定します。 • 選択肢：「Add（追加）」「Delete（削除）」
Type	受信電力しきい値の種類について指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Power Unit	受信電力単位について指定します。 • 選択肢：「mW」「dBm」
Value	受信電力しきい値の値について指定します。 • 設定可能範囲：0-6.5535（mW） -40 ～ 8.1647（dBm）

「Apply」ボタンをクリックして、設定内容を適用します。

DDM Status Table（DDM ステータステーブル）

指定ポートで現在動作中の DDM パラメータと SFP モジュールにおけるその値を表示します。

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。

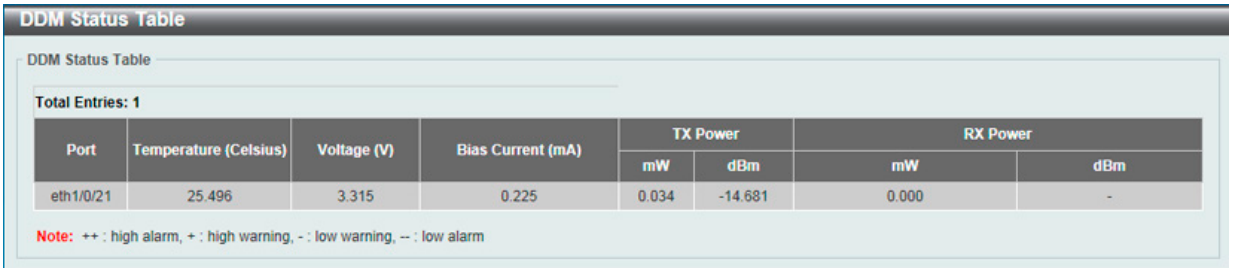


図 13-31図 13-8　　DDM Status Table 画面

画面に表示される項目：

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（EI 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）を表示します。
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）の設定を行います。
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、表示を行います。
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）を表示します。
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）を表示します。
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）を表示します。
MPLS QoS Settings（MPLS QoS 設定）	MPLS QoS Settings（MPLS QoS 設定）の設定、表示を行います。
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にホップごとの障害点特定に使用されます。

注意　MPLS については EI モードのみでサポートされます。

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。

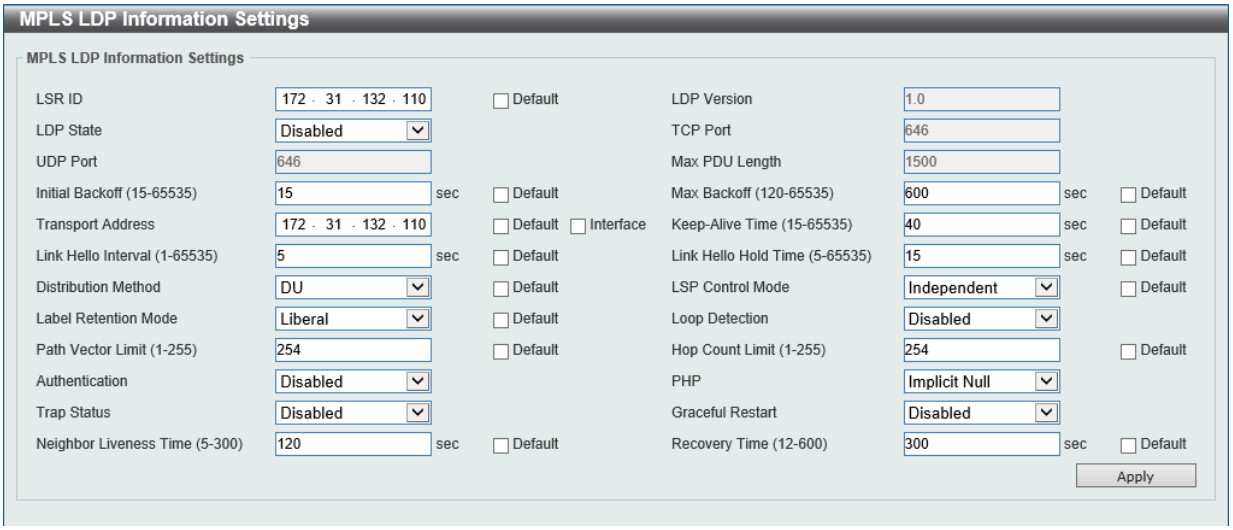


図 14-1　MPLS LDP Information Settings 画面

画面に表示される項目：

項目	説明
LSR ID	Label Switching Router（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 を識別するために使用されます。「Default」にチェックを入れると、初期値を使用します。
LDP Version	LDP バージョンが表示されます。
LDP State	LDP 機能を有効 / 無効に設定します。
TCP Port	LDP TCP ポート番号が表示されます。
UDP Port	LDP UDP ポート番号が表示されます。
Max PDU Length	LDP の最大 PDU 長が表示されます。
Initial Backoff	初期バックオフ遅延時間を入力します。LDP バックオフ遅延時間は、互換性のない設定を持つ 2 つの LSR 間で発生するセッション確立失敗を無限に繰り返すことを防止するメカニズムです。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：15-65535（秒） • 初期値：15（秒）
Max Backoff	バックオフ遅延の最大時間を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：120-65535（秒） • 初期値：600（秒）
Transport Address	トランスポートの IPv4 アドレスを入力します。トランスポートアドレスは、LDP TCP 接続を確立するために使用されます。「Default」にチェックを入れると、初期値を使用します。「Interface 」にチェックを入れると、対応するインタフェースの IP アドレスを各インタフェースのセッションの送信アドレスとして使用します。
Keep-Alive Time	Keep-Alive 時間を入力します。LDP は、ピアセッションごとに Keep-Alive ホールドタイマを保持します。ピアから LDP PDU を受信しないまま Keep-Alive ホールドタイマが期限切れになると、LDP は LDP セッションを終了します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：15-65535（秒） • 初期値：40（秒）
Link Hello Interval	Hello メッセージを送信する間隔を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒） • 初期値：5（秒）
Link Hello Hold Time	Hello の保持時間を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：5-65535（秒） • 初期値：15（秒）
Distribution Method	配布方式を選択します。「Default」にチェックを入れると、初期値を使用します。 • 「DU」- 配布モードを「Downstream-Unsolicited」に設定します。ルーティングテーブルでラベルが学習されると、ダウンストリーム LSR はラベルマッピングをアドバタイズします。（初期値） • 「DoD」- 配布モードを「Downstream-on-Demand」に設定します。アップストリーム接続が明示的な要求を行うと、ダウンストリーム LSR はラベルマッピングをアドバタイズします。

項目	説明
LSP Control Mode	Label-Switched Path（LSP）制御モードを選択します。「Default」にチェックを入れると、初期値を使用します。 • 「Independent」- 独立 LSP 制御モードでは、各 LSR はラベルを Forwarding Equivalence Class（FEC：転送等価クラス）に個別にバインドし、ラベル配布ピアにこの割り当てを配布します。（初期値） • 「Ordered」- 順次 LSP 制御モードでは、FEC がイーグレス LSR である場合、または FEC のネクストホップから FEC のラベル割り当てを既に受信している場合にのみ、LSR はラベルを FEC にバインドします。
Label Retention Mode	ラベル保存モードを選択します。「Default」にチェックを入れると、初期値を使用します。 • 「Conservative」- ラベル配布方法が Downstream-Unsolicited で、ラベル保持モードが「Conservative」である場合、LSR が FEC のネクストホップではない LSR からラベル割り当てを受信すると、この割り当ては破棄されます。 • 「Liberal」- ラベル保持モードが「Liberal」の場合、このような割り当ては保持されます。ネクストホップが変更された場合に、LSP のセットアップを高速化するのに役立ちます。（初期値）
Loop Detection	ループ検知機能を有効 / 無効に設定します。本機能は、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る Path Vector と Hop Count TLV を利用し、LDP メッセージのループを防ぎます。有効にした場合、LDP はパスベクタチェックまたはホップカウントチェックに違反する LDP メッセージをネクストホップに送信しません。
Path Vector Limit	Path Vector 制限値を入力します。ループ検知が有効な場合、ラベルマッピングメッセージ、ラベル要求メッセージ、または Path Vector 長の Path Vector リストにある LDR ID が最大長を超えていると、ループが発生したとみなされます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255 • 初期値：254
Hop Count Limit	LSP 確立で許可される最大ホップ数を設定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255 • 初期値：254
Authentication	認証機能を有効 / 無効に設定します。LDP MD5 認証が有効な場合、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 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 ダイジェストと一緒に TCP セグメントを受信すると、MD5 ダイジェストを計算（自身のパスワードレコードを使用）してセグメントの妥当性を確認し、計算されたダイジェストと受信ダイジェストを比較します。比較が失敗した場合、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 メッセージを無視します。
PHP	Penultimate Hop Popping（PHP）の動作を選択します。 • 選択肢：「Implicit Null」「Explicit Null」 イーグレスルータが Implicit Null ラベルをアドバタイズする場合、アップストリームは PHP を実行します。イーグレスルータが Explicit Null ラベルをアドバタイズする場合、アップストリームはポップ（ラベル削除）せずに外側のラベルを保持します。
Trap Status	LDP トラップ機能を有効 / 無効に設定します。
Graceful Restart	「Graceful Restart」を有効 / 無効に設定します。LDP グレースフルリスタートは、Label Switching Router（LSR）の制御プレーンの再起動によって生じる MPLS トラフィックへの悪影響を最小限に抑えるために役立つメカニズムです。LDP セッションのリカバリ中に MPLS フォワーディング状態を保持し、データプレーンに影響を与えないようにします。グレースフルリスタートは、ローカルとピアの両方が有効になっている場合にのみ、LDP セッションによって使用されます。
Neighbor Liveness Time	ネイバ保持時間を入力します。ネイバとの LDP セッションがダウンしたことを検出すると、デバイスは再接続時間内にネイバとの LDP 通信を再確立しようとします。再接続時間は、ネイバによって通知された FT 再接続タイムアウト値とローカルの「Neighbor Liveness Time」のうち、小さい方に応じて設定されます。再接続時間内に LDP セッションを確立できない場合、関連するすべての古いラベル転送エントリが削除されます。LDP グレースフルリスタートが有効な場合、通知された FT 再接続タイムアウトは、「Neighbor Liveness Time」値に従って設定されます。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：5-300（秒）
Recovery Time	リカバリ時間を入力します。LDP グレースフルリスタートが有効で、LDP セッションが再確立された場合、デバイスはリカバリ時間内にネイバとのラベルマッピング情報の交換を完了します。リカバリタイマが終了すると、デバイスは古いとマークされたすべてのラベル転送エントリを削除します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：12-600（秒）

「Apply」ボタンをクリックして、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、MPLS Label-Switched（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 確立のトリガとなる 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。

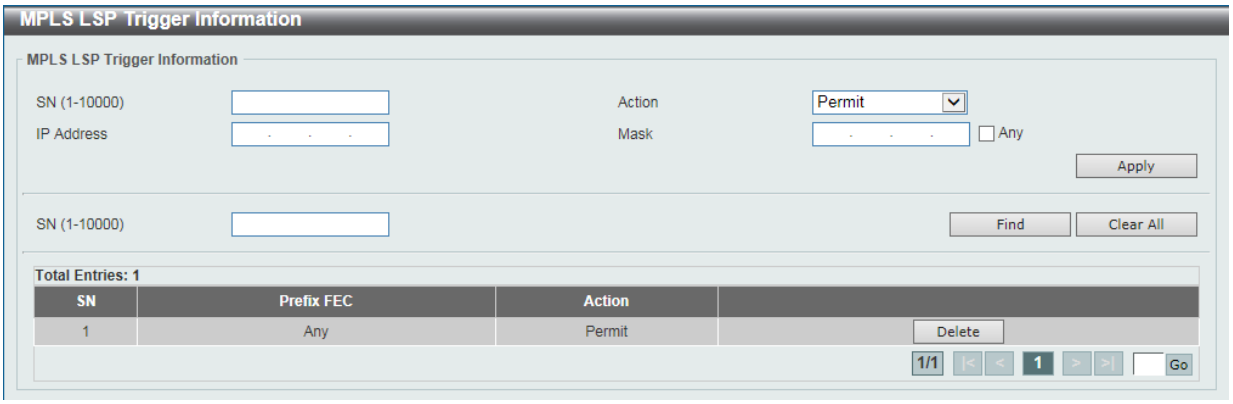


図 14-2　MPLS LSP Trigger Information 画面

画面に表示される項目：

項目	説明
SN	LSP トリガフィルタルールのシーケンス番号を指定します。新しいルールを作成する際に本パラメータを指定しない場合、SN は 10 から始まり、10 ずつ増加します。 • 設定可能範囲：1-10000
Action	実行するアクションを指定します。 • 「Permit」- LSP を確立する際に、IP プレフィックス FEC に従うことを許可します。 • 「Deny」- LSP を確立する際に、IP プレフィックス FEC に従うことを許可しません。
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」にチェックを入れると、すべての IP プレフィックス FEC に適用されます。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Clear All」ボタンをクリックして、入力した SN に関連するすべての情報をクリアします。
「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。
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) に分類された受信パケットは MPLS ラベルでプッシュされ、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、受信ラベルに一致した受信 MPLS パケットは、設定された ILM アクションに基づき処理されます。ラベル操作としては、内向きトップラベルが指定外向きラベルへ変換されてパケットがネクストホップに転送されるか、あるいはトップラベルが外されてパケットが転送されます。

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。

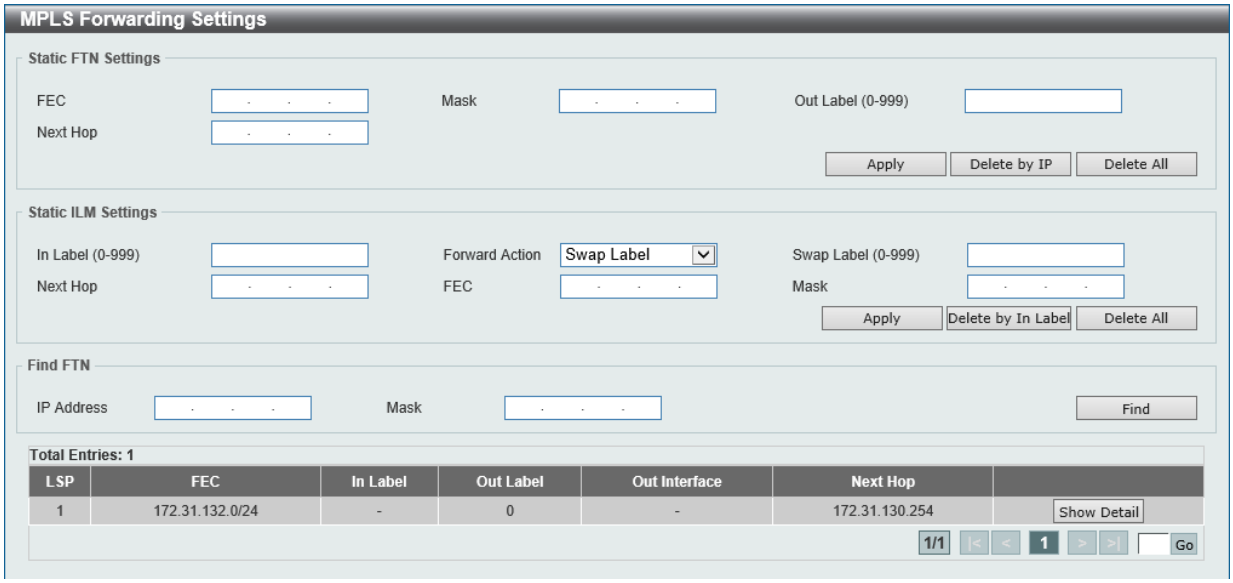


図 14-3　MPLS Forwarding Settings 画面

画面に表示される項目：

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 の出力ラベル値を指定します。 • 設定可能範囲：0-999
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 の入力ラベルを指定します。 • 設定可能範囲：0-999
Forward Action	実行する転送アクション指定します。 • 選択肢：「Swap Label」「Pop」
Swap Label	「Swap Label」を選択後、交換ラベルの値を指定します。 • 設定可能範囲：0-999
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 に関連付ける FEC IPv4 アドレスを指定します。
Mask	ILM に関連付ける 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」ボタンをクリックして、設定内容を適用します。
「Delete by IP」ボタンをクリックして、入力した IP アドレスに基づき指定のエントリを削除します。
「Delete by In Label」ボタンをクリックして、入力した「In Label」に基づき指定のエントリを削除します。
「Delete All」ボタンをクリックして、すべてのエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show Detail」ボタンをクリックすると、以下の画面が表示されます。



図 14-4　MPLS Forwarding Settings（Show Detail）- MPLS Forwarding Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

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 認証が有効である時、LSR はピアと同じパスワードを交換する場合にセッションを確立します。パスワードの設定はリンクネイバやターゲットネイバとのネゴシエーションに適用されます。

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 14-5　MPLS LDP Neighbor Password Settings 画面

画面に表示される項目：

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」にチェックを入れると、初期値（空欄）を使用します。

「Apply」ボタンをクリックして、設定内容を適用します。
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、設定された間隔でターゲットの Hello メッセージを送信してネイバを検出します。検出されたネイバについて、LDP は Hold タイマを保持します。ネイバからの Hello メッセージを受信せずにタイマが期限切れになると、ネイバがタイムアウトします。

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。

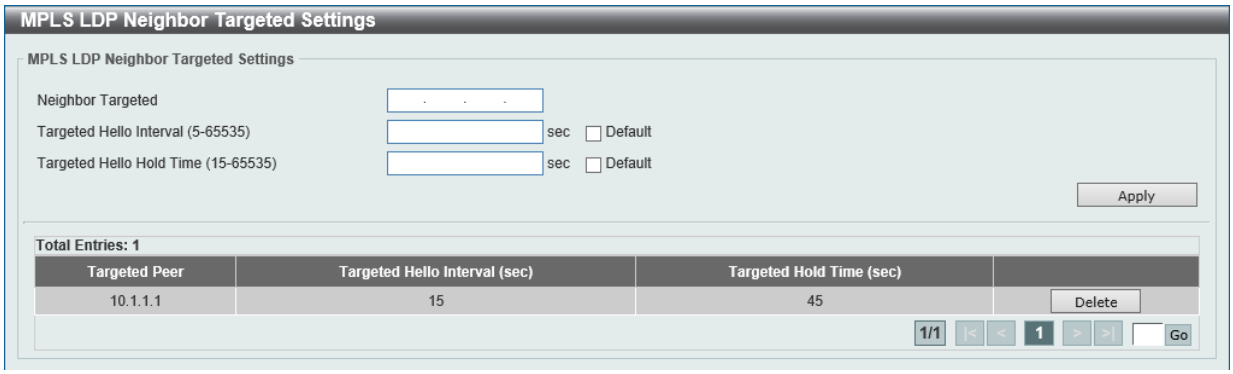


図 14-6　MPLS LDP Neighbor Targeted Settings 画面

画面に表示される項目：

項目	説明
Neighbor Targeted	ターゲットピアの IP アドレスを入力します。ターゲットピアは、直接接続されていないネイバとの LDP セッションを確立するために使用されます
Targeted Hello Interval	拡張ピアとのセッションに対する Hello メッセージの間隔を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：5-65535（秒）
Targeted Hello Hold Time	拡張ピアとのセッションに対する Hold 時間を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：15-65535（秒）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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）の表示とクリアを行います。

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。

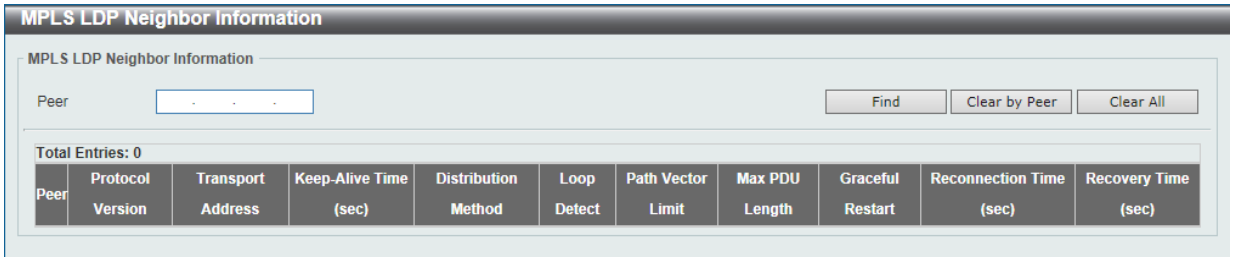


図 14-7　MPLS LDP Neighbor Information 画面

画面に表示される項目：

項目	説明
Peer	ピア LSR ID（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。
「Clear by Peer」ボタンをクリックして、入力したピアの情報をクリアします。
「Clear All」ボタンをクリックして、すべての MPLS LDP ネイバ情報をクリアします。

MPLS Global Settings（MPLS グローバル設定）

本項目では、MPLS のグローバルステータスを設定、表示します。

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。

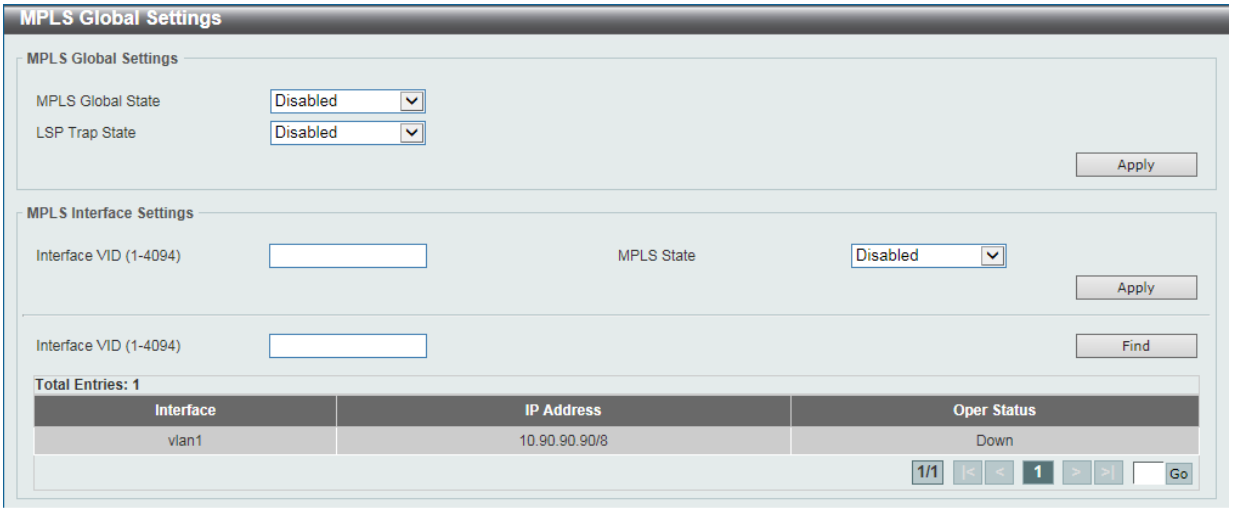


図 14-8　MPLS Global Settings 画面

画面に表示される項目：

項目	説明
MPLS Global Settings	
MPLS Global State	MPLS 機能のグローバルステータスを有効 / 無効に設定します。
LSP Trap State	MPLS LSP トラップを有効 / 無効に設定します。
MPLS Interface Settings	
Interface VID	インタフェース VLAN ID を指定します。 • 設定可能範囲：1-4094
MPLS State	指定インタフェースの MPLS 機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「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。

MPLS LDP Interface Settings（MPLS LDP インタフェース設定）

本項目では、MPLS LDP インタフェースの設定、表示を行います。

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。

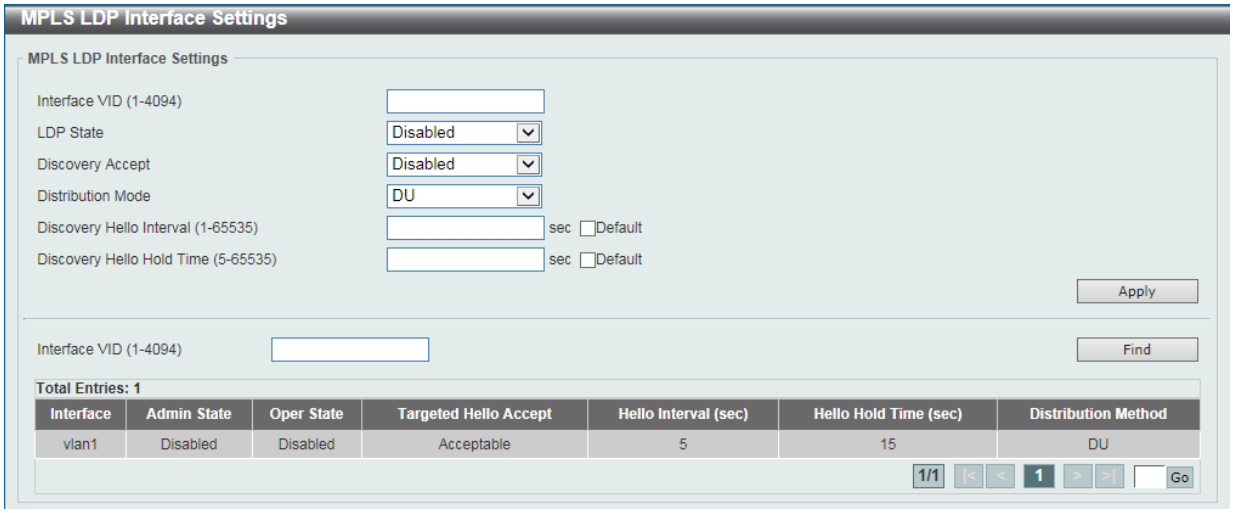


図 14-9　MPLS LDP Interface Settings 画面

画面に表示される項目：

項目	説明
Interface VID	インタフェース VLAN ID を指定します。 • 設定可能範囲：1-4094
LDP State	指定インタフェースで LDP 機能を有効 / 無効に設定します。
Discovery Accept	検出受け入れ機能を有効 / 無効に設定します。ターゲット Hello メッセージの受け入れが無効であり、受信したターゲット Hello メッセージ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。ターゲット Hello メッセージの受け入れが有効の場合、LSR は全てのネイバから受信したターゲット Hello メッセージ を受け入れます。
Distribution Mode	配布方式を選択します。 •「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。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒）
Discovery Hello Hold Time	Discovery Hello の保持時間を入力します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：5-65535（秒）

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
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、表示を行います。

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。

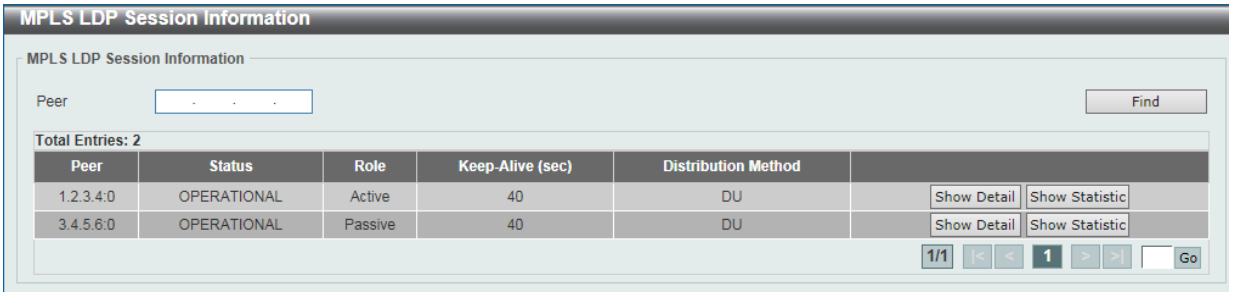


図 14-10　MPLS LDP Session Information 画面

画面に表示される項目：

項目	説明
Peer	ピア LSR ID として使用される 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 Statistics」ボタンをクリックして、統計情報を表示します。
「Show Detail」ボタンをクリックして、指定エントリの詳細について表示します。
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。

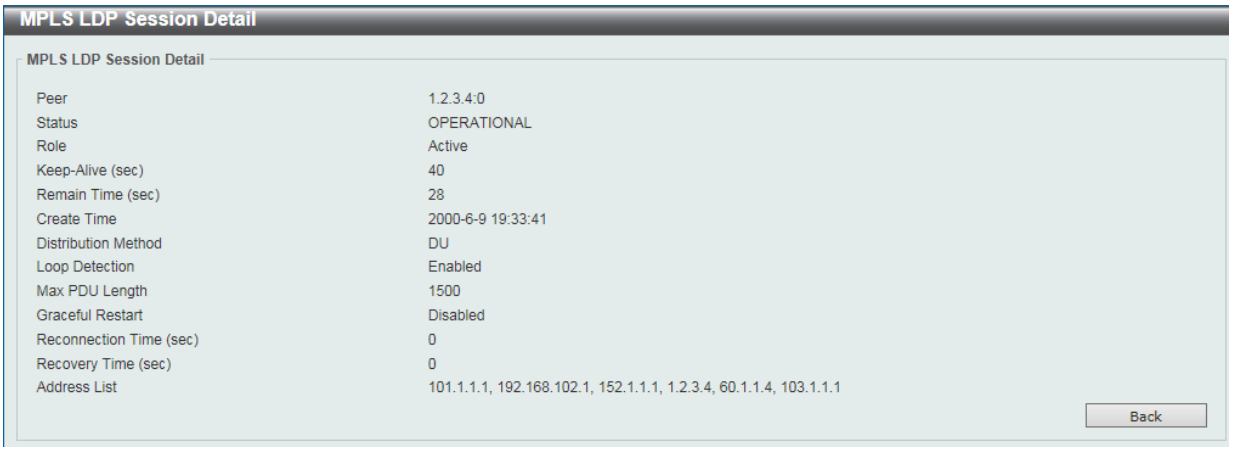


図 14-11　MPLS LDP Session Information（Show Detail）- MPLS LDP Session Detail 画面

前の画面に戻るには、「Back」ボタンをクリックします。

「Show Statistics」をクリックすると、以下の画面が表示されます。

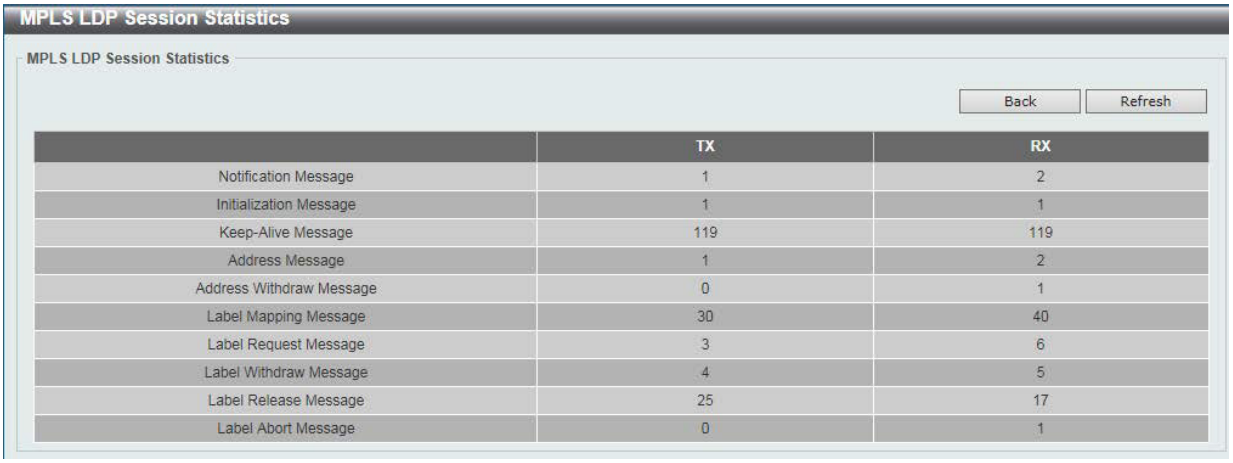


図 14-12　MPLS LDP Session Information（Show Statistics）- MPLS LDP Session Statistics 画面

前の画面に戻るには、「Back」ボタンをクリックします。

MPLS LDP Statistic（MPLS LDP スタティスティック）

本項目では、MPLS LDP Statistic（MPLS LDP 統計）の表示を行います。

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 14-13　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）の表示を行います。

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 14-14　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）の表示を行います。

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。

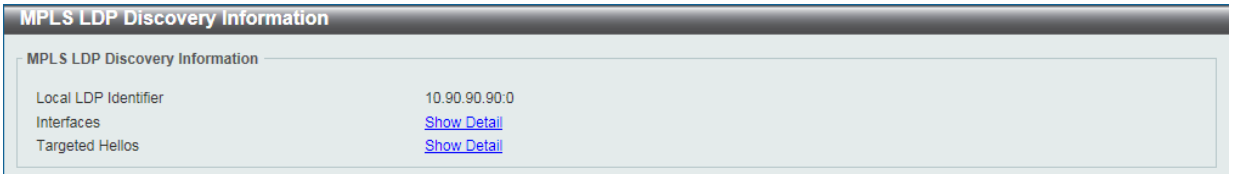


図 14-15　MPLS LDP Discovery Information 画面

「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。

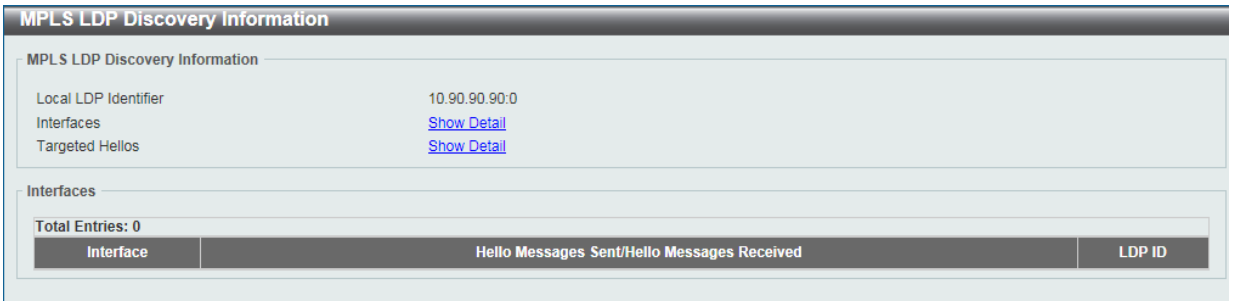


図 14-16　MPLS LDP Discovery Information (Show Detail) 画面

「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。

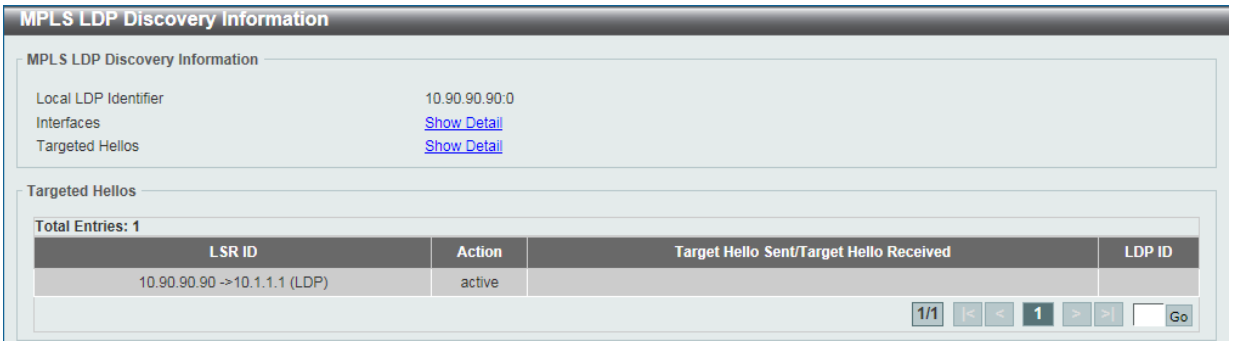


図 14-17　MPLS LDP Discovery Information (Show Detail - Targeted Hellos) 画面

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、表示を行います。

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。

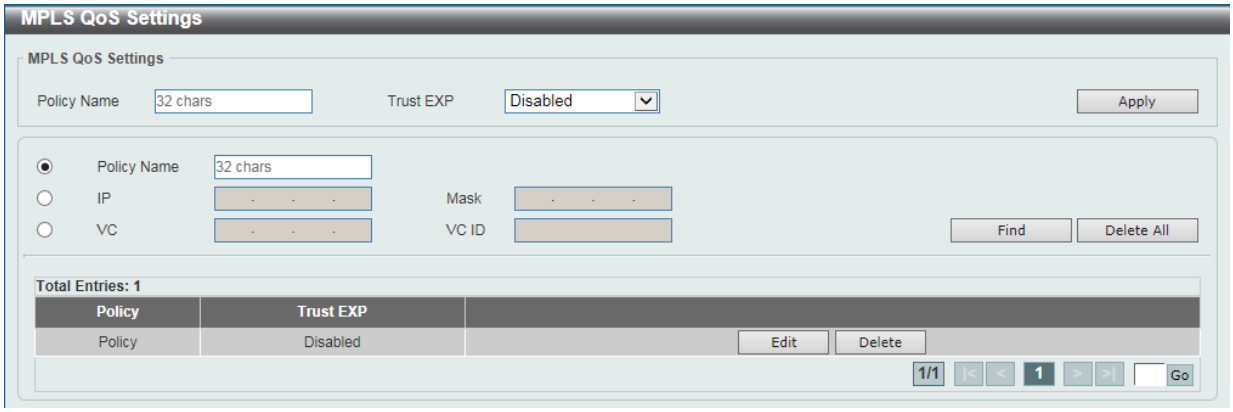


図 14-18　MPLS QoS Settings 画面

画面に表示される項目：

項目	説明
Policy Name	MPLS QoS ポリシー名（32 文字以内）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 / 無効に設定します。 EXP が信頼されている場合、一致したパケットは、MPLS QoS ポリシーのプライオリティマッピングに対する EXP に従ってスケジュールされます。そうでない場合、パケットは 802.1p のプライオリティに従ってスケジューリングされます。
IP	QoS ポリシーに関連付ける FEC IP アドレスを指定します。
Mask	QoS ポリシーに関連付ける FEC サブネットマスクを指定します。
VC	QoS ポリシーに関連付ける FEC VC アドレスを指定します。
VC ID	QoS ポリシーに関連付ける FEC VC ID を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Delete All」ボタンをクリックして、指定 / 入力した情報に基づくすべてのエントリを削除します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定し「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。

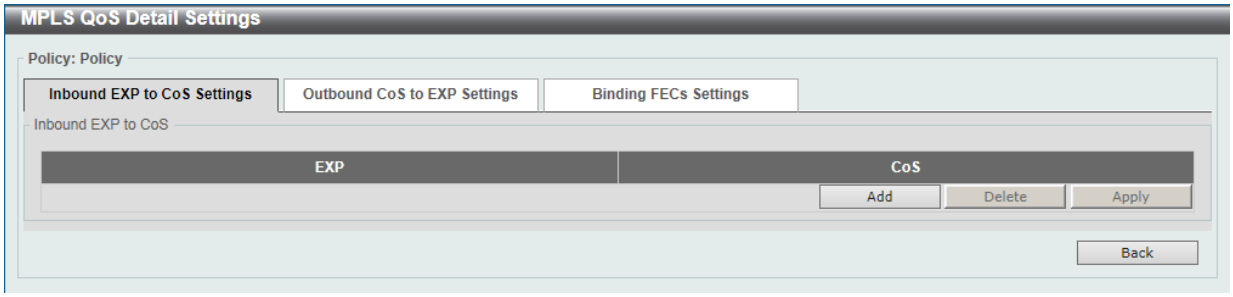


図 14-19　MPLS QoS Settings（Edit）- MPLS QoS Detail Settings 画面 - Inbound EXP to CoS Settings タブ

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Add」ボタンをクリックして、エントリを追加します。

前の画面に戻るには、「Back」ボタンをクリックします。

「Add」をクリックすると、以下の画面が表示されます。

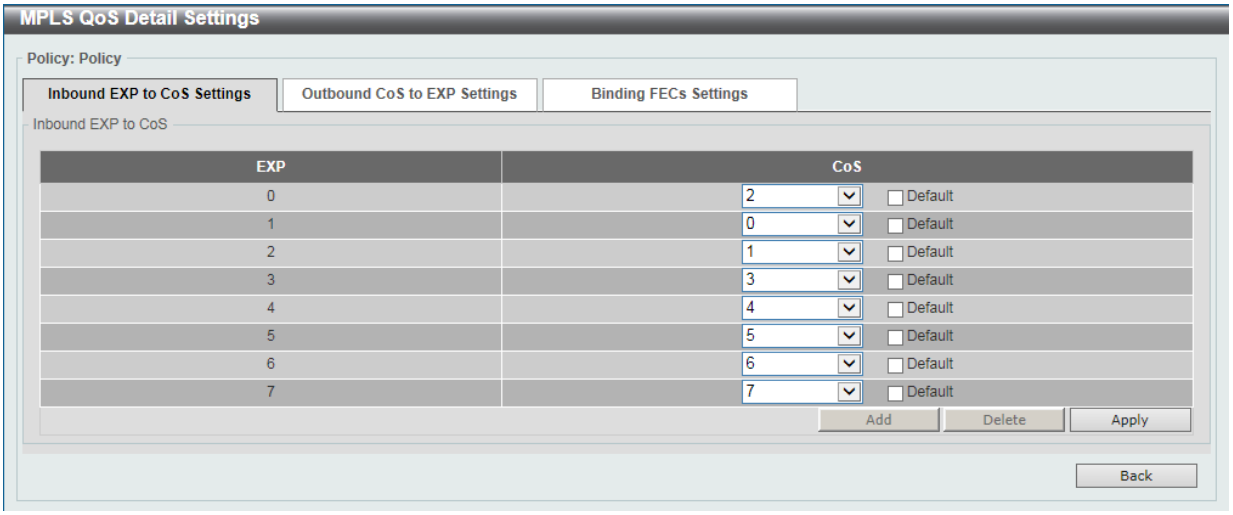


図 14-20　MPLS QoS Settings（Edit）- MPLS QoS Detail Settings 画面 - Inbound EXP to CoS Settings タブ（Add）

画面に表示される項目：

項目	説明
CoS	EXP 値にマッピングする CoS 値を選択します。ポリシーにおいて、サービスクラス（CoS）を Experimental ビット（EXP）にマッピングします。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

「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。

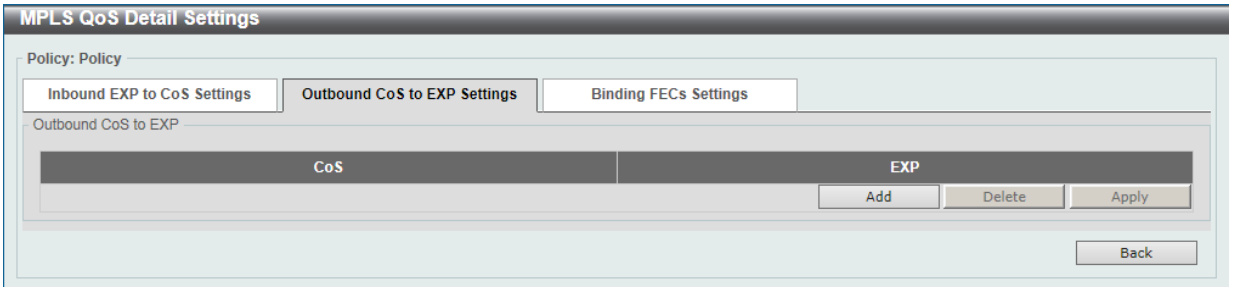


図 14-21　MPLS QoS Settings（Edit）- MPLS QoS Detail Settings 画面 - Outbound CoS to EXP Settings タブ

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Add」ボタンをクリックして、エントリを追加します。
前の画面に戻るには、「Back」ボタンをクリックします。

「Add」をクリックすると、以下の画面が表示されます。

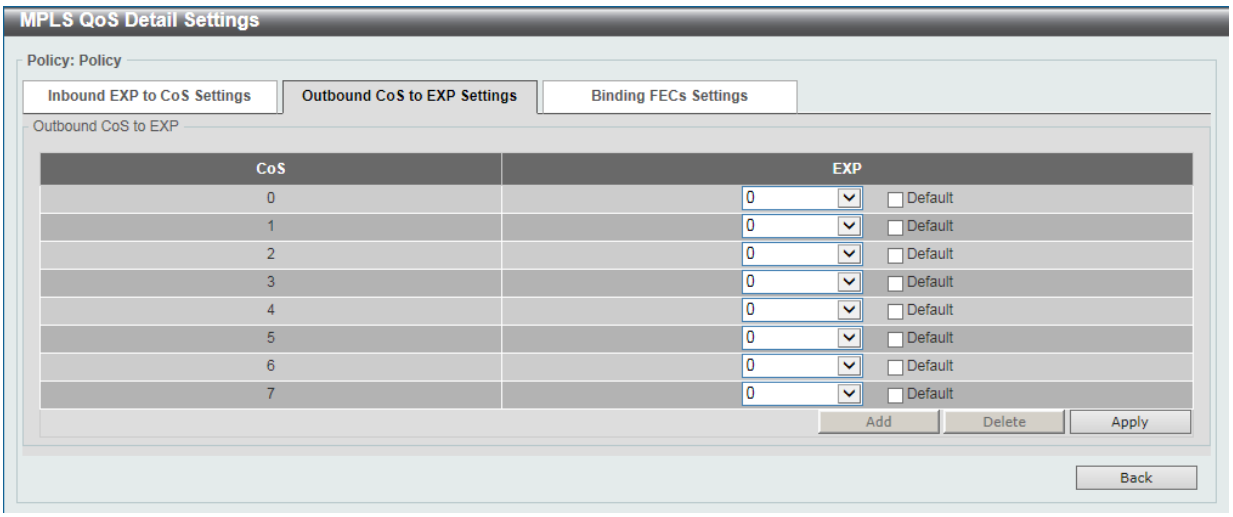


図 14-22　MPLS QoS Settings（Edit）- MPLS QoS Detail Settings 画面 - Outbound CoS to EXP Settings タブ（Add）

画面に表示される項目：

項目	説明
EXP	CoS 値にマッピングする EXP 値を選択します。ポリシーにおいて、クラス EXP を CoS にマッピングします。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-7

「Apply」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

「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。

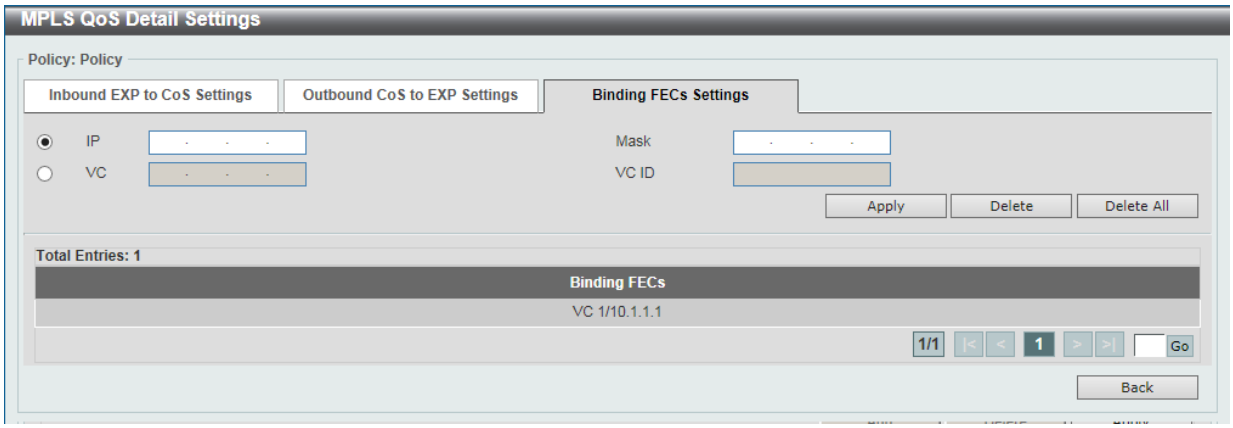


図 14-23　MPLS QoS Settings（Edit）- MPLS QoS Detail Settings 画面 - Binding FECs Settings タブ

画面に表示される項目：

項目	説明
IP	FEC IP アドレスを入力します。本設定により、MPLS QoS ポリシーを FEC に適用します。QoS ポリシーは、FEC のすべての MPLS パケットに適用されます。FEC は、最大で 1 つのポリシーにのみバインドできます。
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」ボタンをクリックして、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

「Delete」ボタンをクリックして、指定のエントリを削除します。
「Delete All」ボタンをクリックして、すべてのエントリを削除します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

Ping MPLS

本項目では、指定 FEC の LSP の接続性を確認します。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、指定 FEC の LSP と一緒に MPLS Echo Request メッセージが送信されます。イーグレス LSR がリクエストメッセージを受信した場合、MPLS Echo Reply 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。

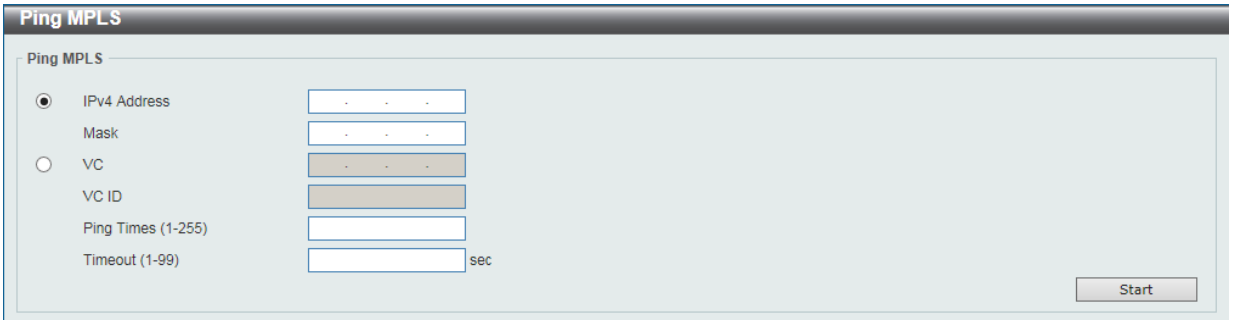


図 14-24　Ping MPLS 画面

画面に表示される項目：

項目	説明
IPv4 Address	LSP 接続性をチェックする 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 の回数を指定します。送信される Ping パケットの回数です。 • 設定可能範囲：1-255（回）
Timeout	Ping タイムアウト値を指定します。 • 設定可能範囲：1-99（秒）

「Start」ボタンをクリックして、MPLS Ping を開始します。

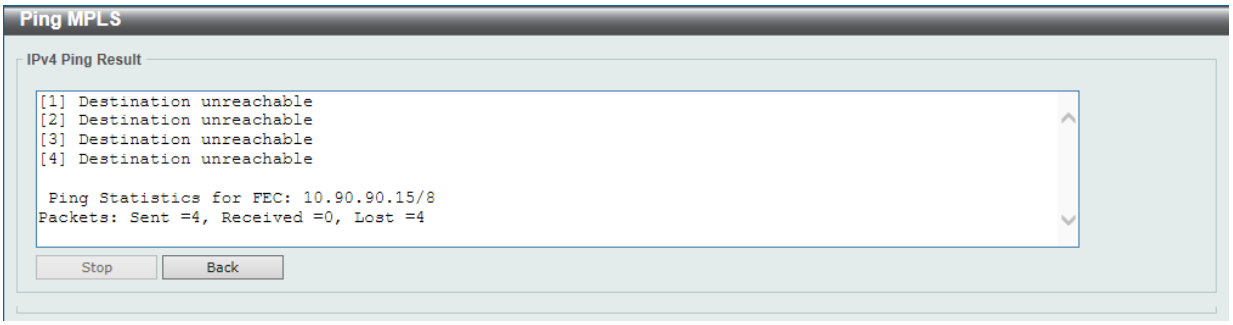


図 14-25　Ping MPLS (Start) 画面

「Stop」ボタンをクリックして、MPLS Ping を停止します。
前の画面に戻るには、「Back」ボタンをクリックします。

Traceroute MPLS IPv4（トレースルート MPLS IPv4）

本機能は、指定 FEC の LSP パストレースのようにホップごとの障害点特定に使用されます。
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、指定 FEC の LSP と一緒に MPLS エコー要求メッセージが送信されます。 MPLS エコー要求の最遠ラベル内の TTL は 1、 2、 3 ... というように連続した値で設定されます。これにより、LSP を持つ各 LSR でエコー要求が期限切れとなります。LSR は MPLS エコー応答を返します。タイムアウト前に送信側で応答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 14-26　Traceroute MPLS IPv4 画面

画面に表示される項目：

項目	説明
IPv4 Address	LSP 接続性をチェックする 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	トレースルートのタイムアウト値を指定します。 • 設定可能範囲：1-99（秒）

「Start」ボタンをクリックして、MPLS トレースルートを開始します。

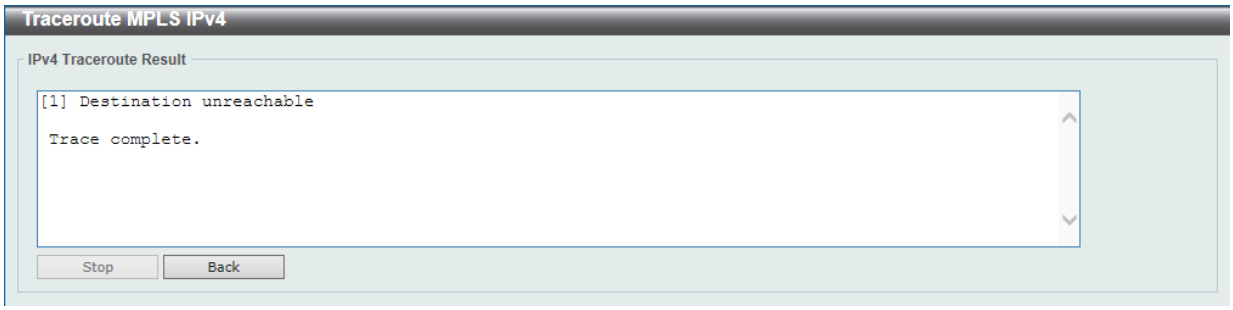


図 14-27　Traceroute MPLS IPv4 (Start) 画面

「Stop」ボタンをクリックして、MPLS ルートトレースを停止します。
前の画面に戻るには、「Back」ボタンをクリックします。

第 15 章　MPLS L2VPN（EI 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) の設定を行います。
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）の設定を行います。
VPLS Settings（VPLS 設定）	「Virtual Private LAN Service」(VPLS) の設定を行います。
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）を表示します。

注意　MPLS L2VPN については EI モードのみでサポートされます。

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。

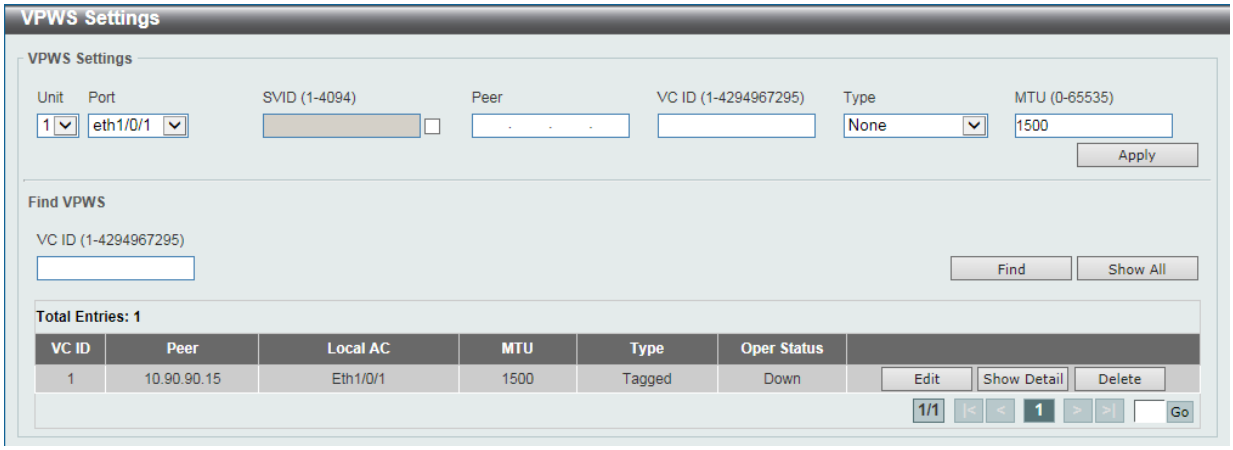


図 15-1　VPWS Settings 画面

画面に表示される項目：

項目	説明
VPWS Settings	
Unit	本設定を適用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。
SVID	カプセル化された VLAN ID を指定します。 • 設定可能範囲：1-4094
Peer	他エンドの Provider Edge（PE）を識別するために使用されるピア IP アドレスを入力します。
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。VPWS を一意に識別するために使用される値であり、両方の PE で一意である必要があります。 • 設定可能範囲：1-4294967295
Type	タイプを選択します。 • 選択肢：「None」「Manual」「Raw」「Tagged」「Manual Raw」「Manual Tagged」 Raw モードで動作している場合、S- タグは PW を介して送信されません。Tagged モードで動作している場合、S- タグは PW を介して送信されます。初期値では PW タイプは Ethernet タグモードになっています。
MTU	リモートピアに通知されるローカル 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 MTU を通知しません。MTU はローカル / リモートデバイスの両方で同じである必要があります。 • 設定可能範囲：0-65535（Bytes） • 初期値：1500（Bytes）
Find VPWS	
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。 • 設定可能範囲：1-4294967295

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「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」ボタンをクリックして、指定エントリの詳細について表示します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、以下の画面が表示されます。

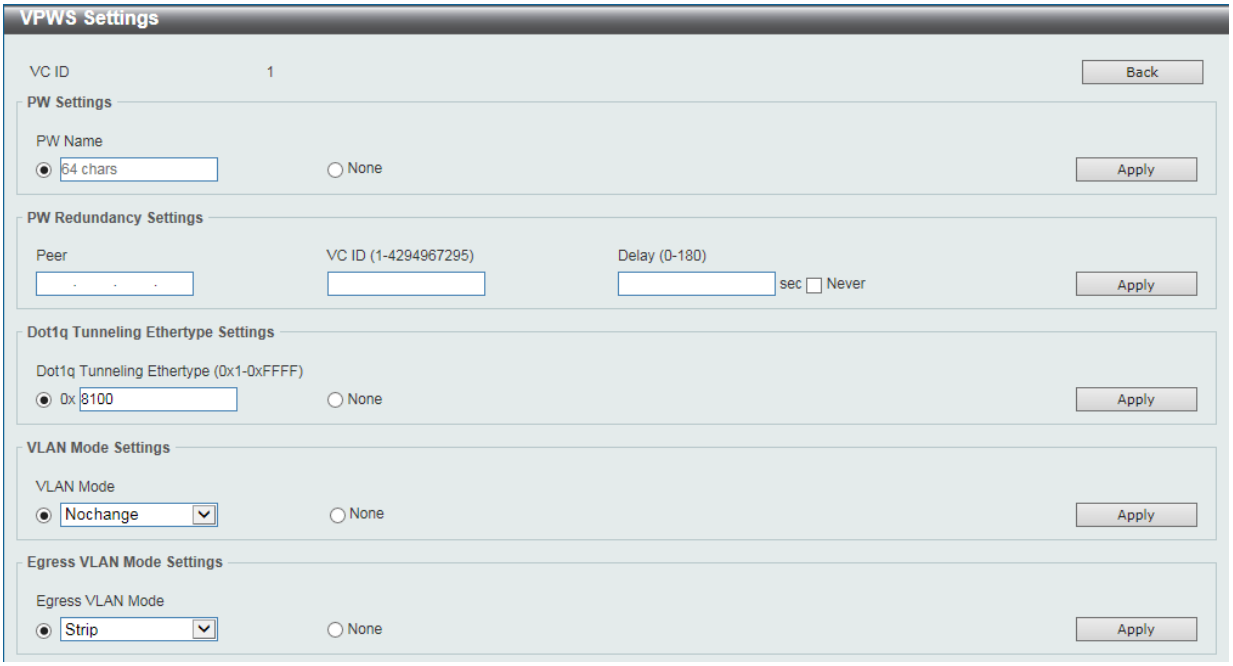


図 15-2　VPWS Settings（Edit）画面

前の画面に戻るには、「Back」ボタンをクリックします。

画面に表示される項目：

項目	説明
PW Settings	
PW Name	Pseudo-Wire (PW) 名（64 文字以内）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	他エンドの Provider Edge（PE）を識別するために使用されるピア LSR ID を入力します。
VC ID	Pseudo-Wire (PW) サービスインスタンス ID を入力します。 • 設定可能範囲：1-4294967295
Delay	遅延時間の値を指定します。指定の遅延時間の後にプライマリ PW に戻ります。 「Never」にチェックを入れると、プライマリ PW へ戻る事はありません（初期値）。 • 設定可能範囲：0-180（秒）
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。「None」を指定すると、本機能は無効になります。 • 設定可能範囲：0x1-0xFFFF（16 進数形式）
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 にのみ適用可能です。 • 「Add VLAN」- イングレスパケットに 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。イーサネットベース / イーサネット VLAN ベース AC に適用可能です。 • 「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 にのみ適用可能です。 「None」を指定すると初期値を使用します。 本設定は、スタンドアロンスイッチにのみ適用できます。
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 で送信される際に、パケットのアウタタグを取り外します。 • 「Change VLAN」- AC で送信される際に、パケットのアウタタグを AC の VLAN ID に変更します。イーサネット VLAN ベース AC にのみ適用可能です。 「None」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、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）- VPWS Detail Information 画面

L2VC Interface Description（L2VC インタフェース概要）

本項目では、Layer 2 Virtual Circuit（L2VC）インタフェースの説明を設定します。

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。

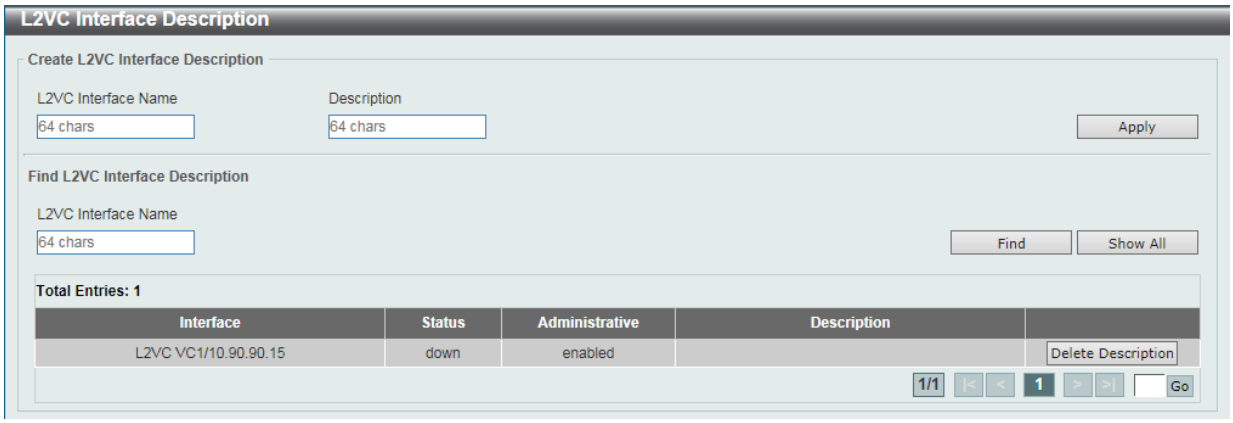


図 15-4　L2VC Interface Description 画面

画面に表示される項目：

項目	説明
Create L2VC Interface Description	
L2VC Interface Name	L2VC インタフェース名（64 文字以内）を指定します。
Description	L2VC インタフェースの説明（64 文字以内）を指定します。
Find L2VC Interface Description	
L2VC Interface Name	L2VC インタフェース名（64 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete Description」ボタンをクリックして、指定のエントリの概要を削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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。

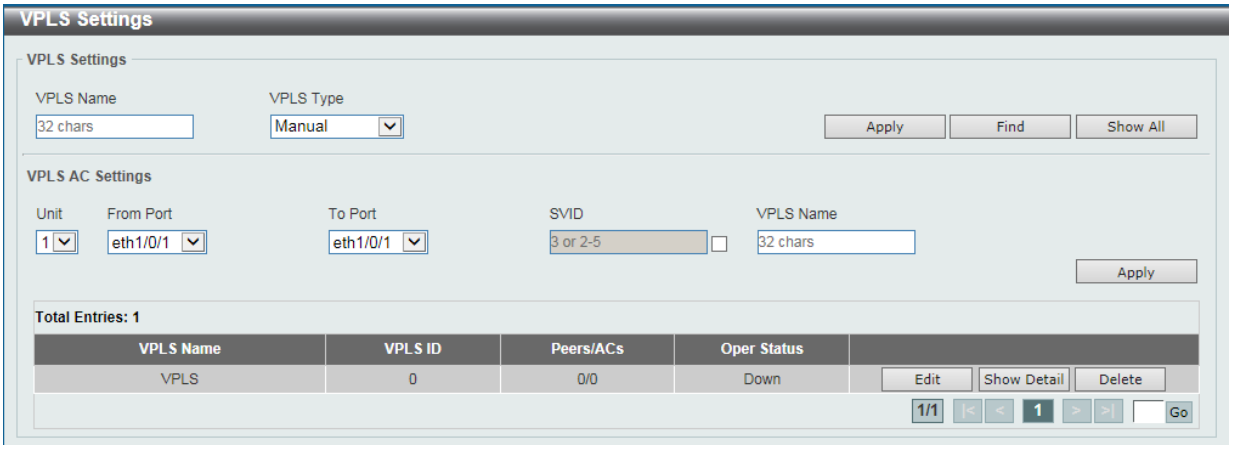


図 15-5　VPLS Settings 画面

画面に表示される項目：

項目	説明
VPLS Settings	
VPLS Name	VPLS 名（32 文字以内）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、シグナリングに LDP を使用します。 • 「Auto Discovery」- 自動検出とシグナリングに BGP を使用します。
VPLS AC Settings	
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
SVID	SVID を指定します。 • 設定可能範囲：1-4094
VPLS Name	VPLS インスタンス名（32 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。
「Show Detail」ボタンをクリックして、指定エントリの詳細について表示します。
「Edit」ボタンをクリックして、指定エントリの編集を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

「Edit」をクリックすると、設定画面が表示されます。表示される画面は「VPLS Type」で選択した VPLS タイプによって異なります。

VPLS タイプで「Manual」を選択した場合

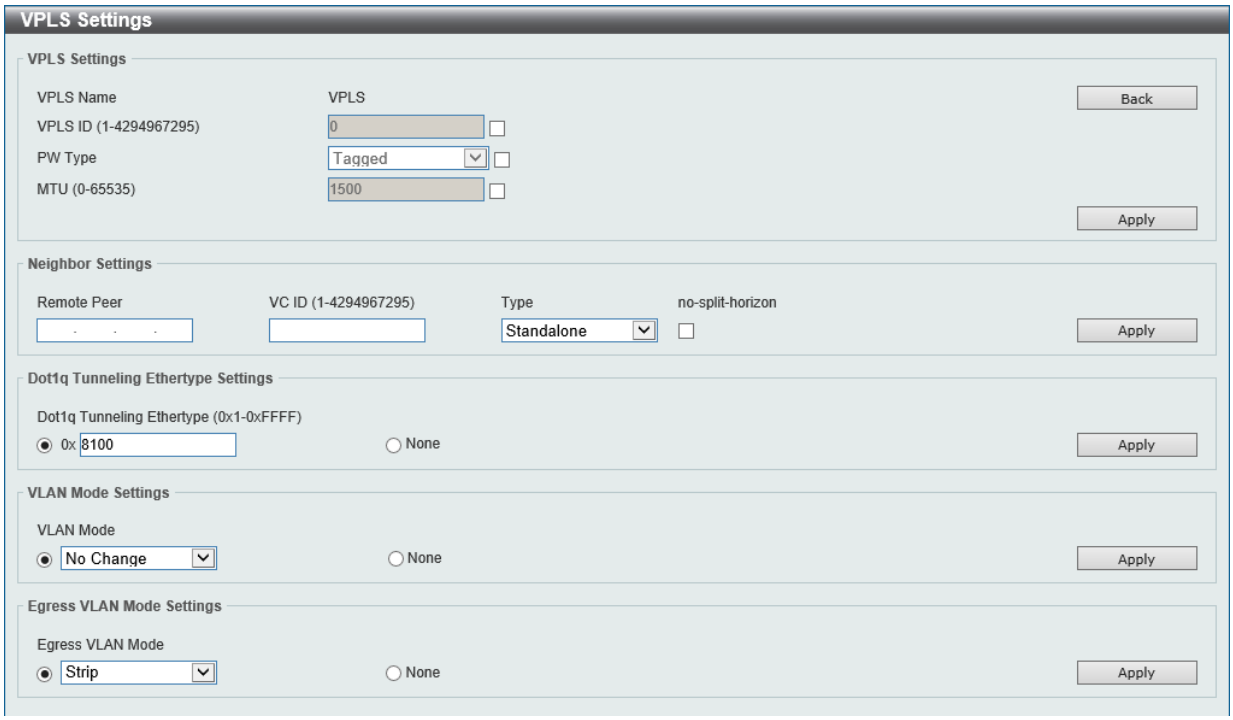


図 15-6　VPLS Settings（Edit）画面 - VPLS タイプで「Manual」選択時

画面に表示される項目：

項目	説明
VPLS Settings	
VPLS ID	VPLS インスタンス ID を入力します。 • 設定可能範囲：1-4294967295
PW Type	PW タイプを選択します。 • 「Raw」- サービスタイプをイーサネット Raw モードに指定します。VPLS 内のすべての 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」- サービスタイプをイーサネット Tagged モードに指定します。VPLS 内のすべての 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 AC リンクの MTU 値を入力します。PW を確立するには、ローカルサイトとリモートサイトの両方で MTU 値が同じである必要があります。MTU が 0 に指定されている場合、ローカル MTU は VPLS 内のリモートピアに通知されません。 • 設定可能範囲：0-65535（Bytes） • 初期値：1500（Bytes）
Neighbor Settings	
Remote Peer	ピアが所属している PE を識別するために使用する LSR ID を指定します。
VC ID	PW VC ID を入力します。VPLS のピアを一意に識別するために、IP アドレスと一緒に使用されます。指定しない場合、PW ID はこの VPLS の VPN ID によって設定されます。 • 設定可能範囲：1-4294967295
Type	タイプを選択します • 選択肢：「Backup」「Standalone」 「Backup」を選択した場合、H-VPLS の PW 冗長性のためのバックアップピアが作成されます。
no-split-horizon	本項目にチェックを入れると、ピアがスポーク PW として使用されます。VPLS 内の他の 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 内の他の PW に転送されます。このオプションを指定しない場合、ピアはネットワーク PW として使用されます。VPLS 内の他のネットワーク PW からのパケットはこの PW に転送されず、この PW からのパケットは VPLS 内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。「None」を指定すると、本機能は無効になります。 • 設定可能範囲：0x1-0xFFFF（16 進数形式）

項目	説明
VLAN Mode Settings	
VLAN Mode	VPLS の VLAN モードを指定します。VLAN モードは、この VPLS に属するすべての PW のカプセル化パケットの VLAN 処理に影響します。 • 「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 ベースの AC にのみ適用できます。 • 「Add VLAN」- イングレスパケットに指定 VLAN を追加します。ポートベース AC の初期動作では、VLAN ID「0」を追加します。イーサネットベースおよびイーサネット VLAN ベース AC の両方に適用できます。 • 「Change VLAN」- イングレスパケットの VLAN タグを指定 VLAN ID に変更します。イーサネット VLAN ベースの AC にのみ適用できます。 「None」を指定すると初期値を使用します。 本設定はスタンドアロンスイッチにのみ適用できます。
Egress VLAN Mode Settings	
Egress VLAN Mode	VPLS のイーグレス VLAN モードを指定します。イーグレス VLAN モードは、この VPLS に属する AC でカプセル化が解除されたパケットを送信する前に、アウタ VLAN タグの処理に影響します。 • 「Strip」- AC で送信される際に、パケットのアウタタグを取り外します。 • 「Change VLAN」- AC で送信される際に、パケットのアウタタグを AC の VLAN ID に変更します。イーサネット VLAN ベース AC にのみ適用可能です。 「None」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、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

VPLS タイプで「Auto Discovery」を選択した場合

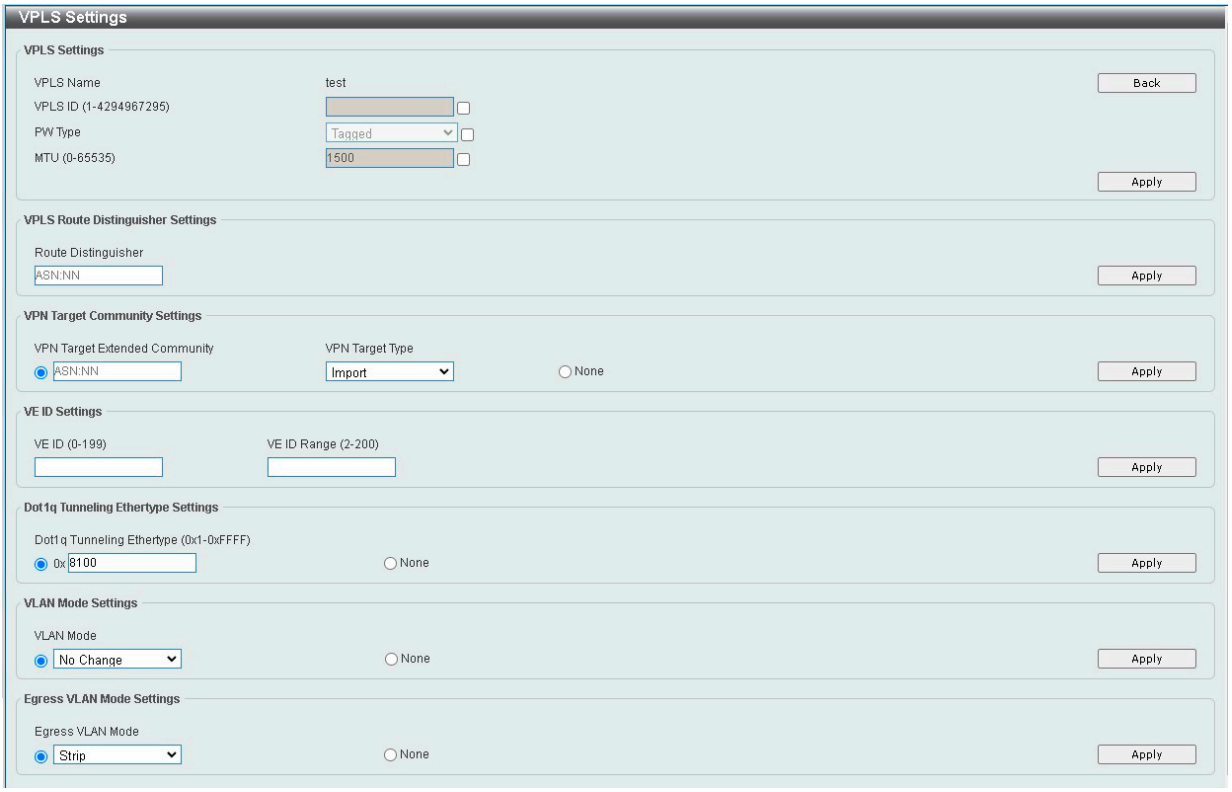


図 15-7　VPLS Settings（Edit）画面 - VPLS タイプで「Auto Discovery」選択時

画面に表示される項目：

項目	説明
VPLS Settings	
VPLS ID	VPLS インスタンス ID を入力します。 • 設定可能範囲：1-4294967295
PW Type	PW タイプを選択します。 • 「Raw」- サービスタイプをイーサネット Raw モードに指定します。VPLS 内のすべての 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」- サービスタイプをイーサネット Tagged モードに指定します。VPLS 内のすべての PW のカプセル化はイーサネット Tagged モードで行われます。

項目	説明
MTU	リモートピアに通知される VPLS のローカル AC リンクの MTU 値を入力します。PW を確立するには、ローカルサイトとリモートサイトの両方で MTU 値が同じである必要があります。MTU が 0 に指定されている場合、ローカル MTU は VPLS 内のリモートピアに通知されません。 • 設定可能範囲：0-65535（Bytes） • 初期値：1500（Bytes）
VPLS Route Distinguisher Settings	
Route Distinguisher	Auto Discovery で VRF を識別するために使用する RD（Route Distinguisher）を指定します。 RD の値は 1 つの PE 内の VPLS に対し一意である必要があります。RD の値は設定後に修正できません。
VPN Target Community Settings	
VPN Target Extended Community	VPN ターゲット拡張コミュニティを指定します。
VPN Target Type	VPN ターゲットタイプを選択します。 • 選択肢：「Important」「Export」「Both」 「None」を指定すると、本機能は無効になります。
VE ID Settings	
VE ID	Auto Discovery VRF の VE ID を入力します。 • 設定可能範囲：0-199
VE ID Range	Auto Discovery VRF の VE ID 範囲を入力します。 • 設定可能範囲：2-200
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。「None」を指定すると、本機能は無効になります。 • 設定可能範囲：0x1-0xFFFF（16 進数形式）
VLAN Mode Settings	
VLAN Mode	VPLS の VLAN モードを指定します。VLAN モードは、この VPLS に属するすべての PW のカプセル化パケットの VLAN 処理に影響します。 • 「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 ベースの AC にのみ適用できます。 • 「Add VLAN」- イングレスパケットに指定 VLAN を追加します。ポートベース AC の初期動作では、VLAN ID「0」を追加します。イーサネットベースおよびイーサネット VLAN ベース AC の両方に適用できます。 • 「Change VLAN」- イングレスパケットの VLAN タグを指定 VLAN ID に変更します。イーサネット VLAN ベースの AC にのみ適用できます。 「None」を指定すると初期値を使用します。 本設定はスタンドアロンスイッチにのみ適用できます。
Egress VLAN Mode Settings	
Egress VLAN Mode	VPLS のイーグレス VLAN モードを指定します。イーグレス VLAN モードは、この VPLS に属する AC でカプセル化が解除されたパケットを送信する前に、アウタ VLAN タグの処理に影響します。 • 「Strip」- AC で送信される際に、パケットのアウタタグを取り外します。 • 「Change VLAN」- AC で送信される際に、パケットのアウタタグを AC の VLAN ID に変更します。イーサネット VLAN ベース AC にのみ適用可能です。 「None」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、設定内容を適用します。
前の画面に戻るには、「Back」ボタンをクリックします。

「Show Detail」をクリックすると、以下の画面が表示されます。

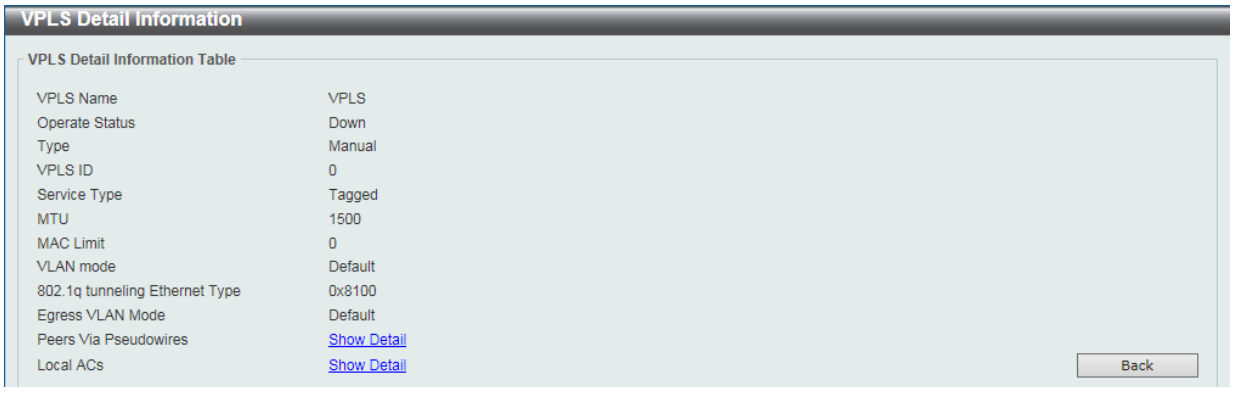


図 15-8　VPLS Settings（Show Detail）- VPLS Detail Settings 画面（「Manual」選択時）

前の画面に戻るには、「Back」ボタンをクリックします。
各項目の「Show Detail」をクリックすると、該当項目の詳細情報が表示されます。

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）の表示、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。

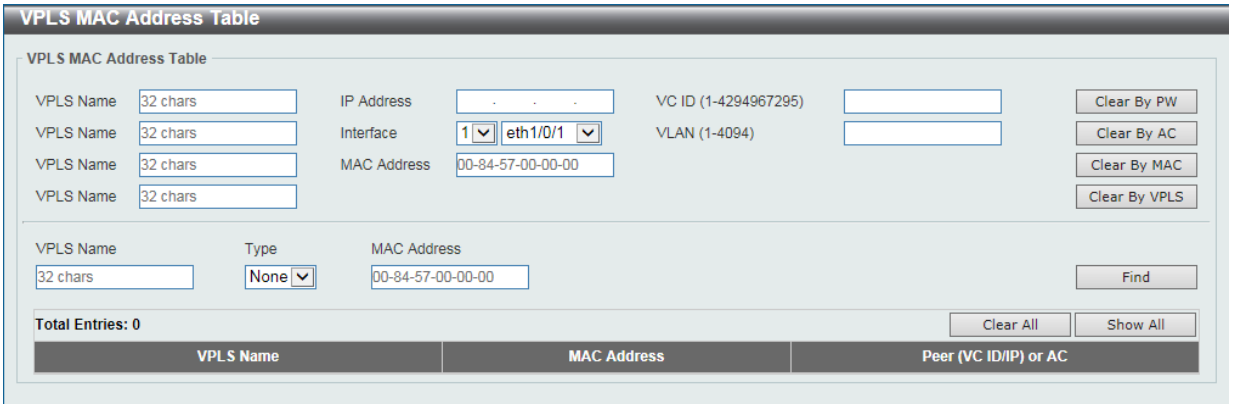


図 15-9　VPLS MAC Address Table 画面

画面に表示される項目：

項目	説明
VPLS Name	VPLS インスタンス名（32 文字以内）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 を指定します。 • 設定可能範囲：1-4294967295
Interface	設定を行うユニット / ポートを指定します。
VLAN	サービス VLAN ID を指定します。 • 設定可能範囲：1-4094
MAC Address	MAC アドレスを指定します。
Type	検索クエリで指定する情報のタイプを選択します。 • 選択肢：「None」「Peer」「AC」

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Show All」ボタンをクリックして、すべてのエントリを表示します。
「Clear All」ボタンをクリックして、テーブルのすべてのエントリをクリアします。
「Clear By PW」ボタンをクリックして、指定した「PW」に関連する情報をクリアします。
「Clear By AC」ボタンをクリックして、指定した「AC」に関連する情報をクリアします。
「Clear By MAC」ボタンをクリックして、指定した「MAC」に関連する情報をクリアします。
「Clear By VPLS」ボタンをクリックして、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確認することができます。

以下は Monitoring サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
VLAN Counter（VLAN カウンタ）	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを作成します。
Utilization（利用分析）	スイッチの Utilization（利用分析）を表示します。
Statistics（統計情報）	スイッチの Statistics（統計情報）を表示します。
Mirror Settings（ミラー設定）	ミラーリング機能の設定を行います。対象ポートで送受信するフレームをコピーし、フレームの出力先を他のポートに変更する機能（ポートミラーリング）です。
sFlow（sFlow 設定）	sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。
Device Environment（機器環境確認）	Device Environment（機器環境確認）ではスイッチの内部の温度状態を表示します。

VLAN Counter（VLAN カウンタ）

本画面では、VLAN カウンタの設定、表示を行います。指定の L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを作成します。

Monitoring > VLAN Counter の順にメニューをクリックし、以下の画面を表示します。

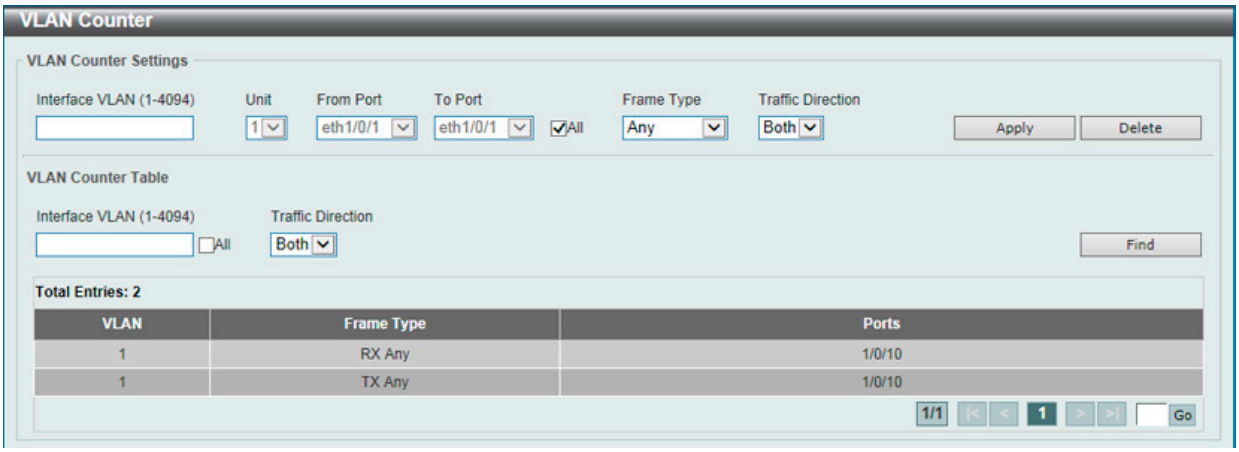


図 16-1　VLAN Counter 画面

画面に表示される項目：

項目	説明
VLAN Counter Settings	
Interface VLAN	インタフェース VLAN を指定します。 • 設定可能範囲：1-4094
Unit	本設定を適用するユニットを指定します。
From Port / To Port	本設定を適用するポート範囲を指定します。
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 を指定します。「All」を指定すると全 VLAN を指定します。 • 設定可能範囲：1-4094
Traffic Direction	トラフィックの向きを指定します。 • 「RX」- イングレストラフィックの設定を表示します。 • 「TX」- イーグレストラフィックの設定を表示します。 • 「Both」- 両方のトラフィックの設定を表示します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Find」ボタンをクリックして、入力した情報を基に指定のエントリを検出します。
「Delete」ボタンをクリックして、指定した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。

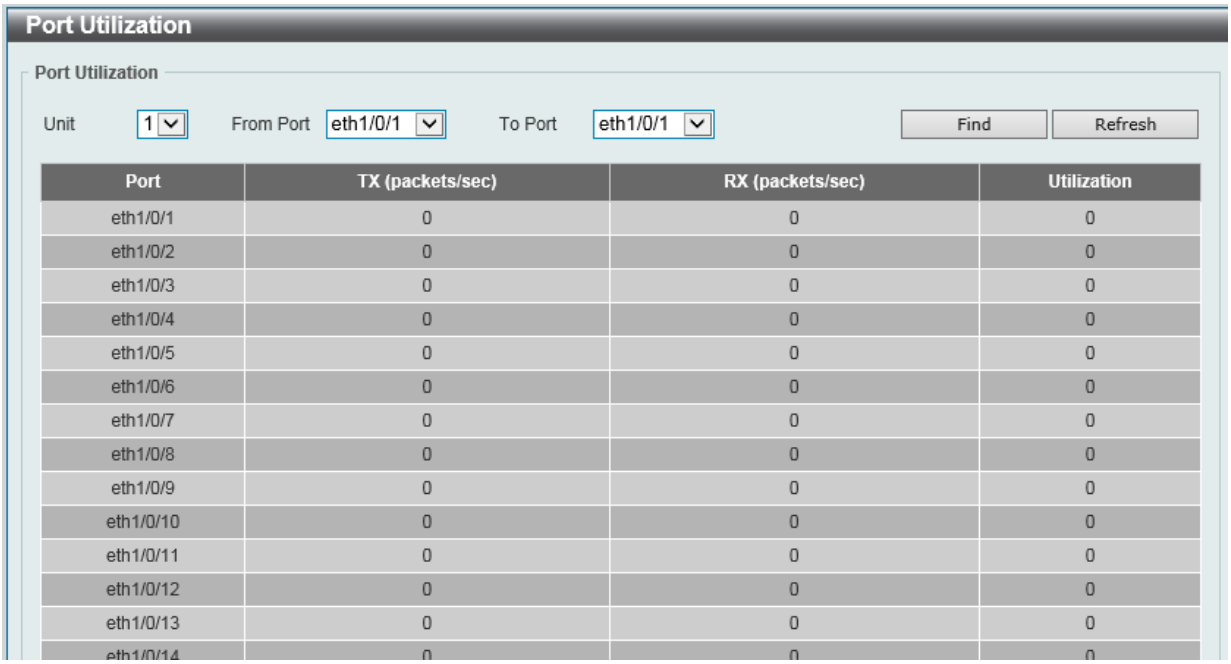


図 16-2　Port Utilization 画面

画面に表示される項目：

項目	説明
Unit	ポート使用率を表示するユニットを指定します。
From Port / To Port	ポート使用率を表示するポート範囲を指定します。

「Find」ボタンをクリックして、指定ポートのエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。

History Utilization（使用履歴）

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

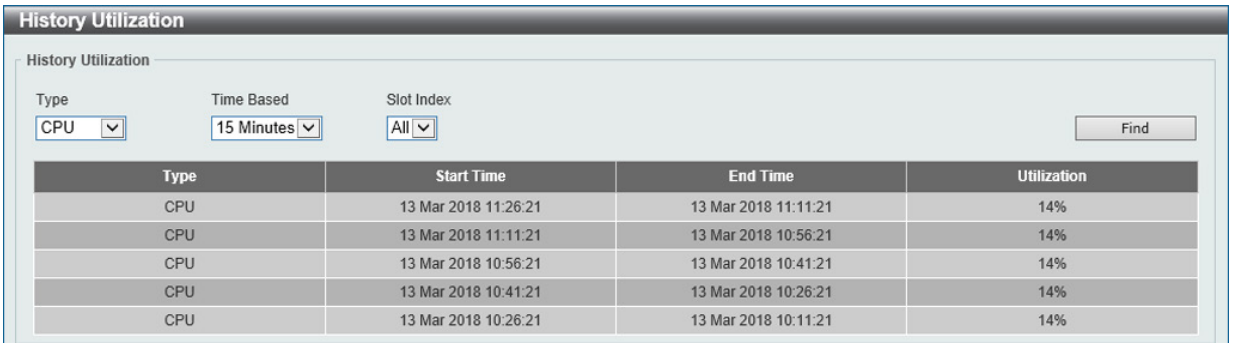


図 16-4　History Utilization (CPU) 画面

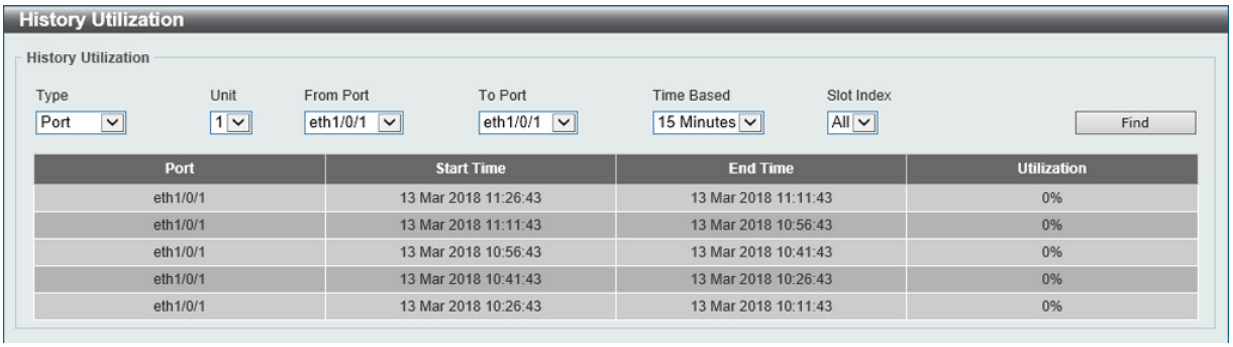


図 16-5　History Utilization (Port) 画面

画面に表示される項目：

項目	説明
Type	表示する使用履歴の種類を指定します。 • 「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	使用履歴を表示するユニットを指定します。
From Port / To Port	使用履歴を表示するポート範囲を指定します。
Time Based	表示する統計情報の期間を指定します。 • 「15 Minutes」- 15 分間単位の使用情報を表示します。 • 「1 Day」- 1 日単位の使用情報を表示します。 「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1Day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。
Slot Index	スロットのインデックスを指定します。 • 選択肢：「All」「1」「2」「3」「4」「5」（「15 Minutes」選択時） 「All」「1」「2」（「1 Day」選択時）

「Find」ボタンをクリックして、指定した情報を基に特定のエントリを検出します。

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。

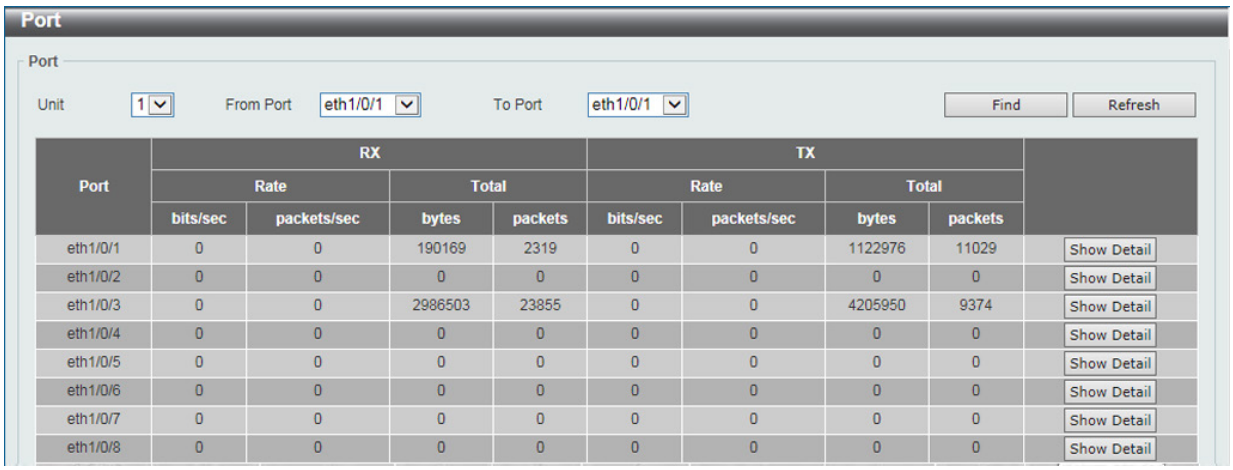


図 16-6　Port 画面

画面に表示される項目：

項目	説明
Unit	統計情報を表示するユニットを選択します。
From Port / To Port	統計情報を表示するポート範囲を指定します。

「Find」ボタンをクリックして、指定ポートのエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Show Detail」ボタンをクリックして、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

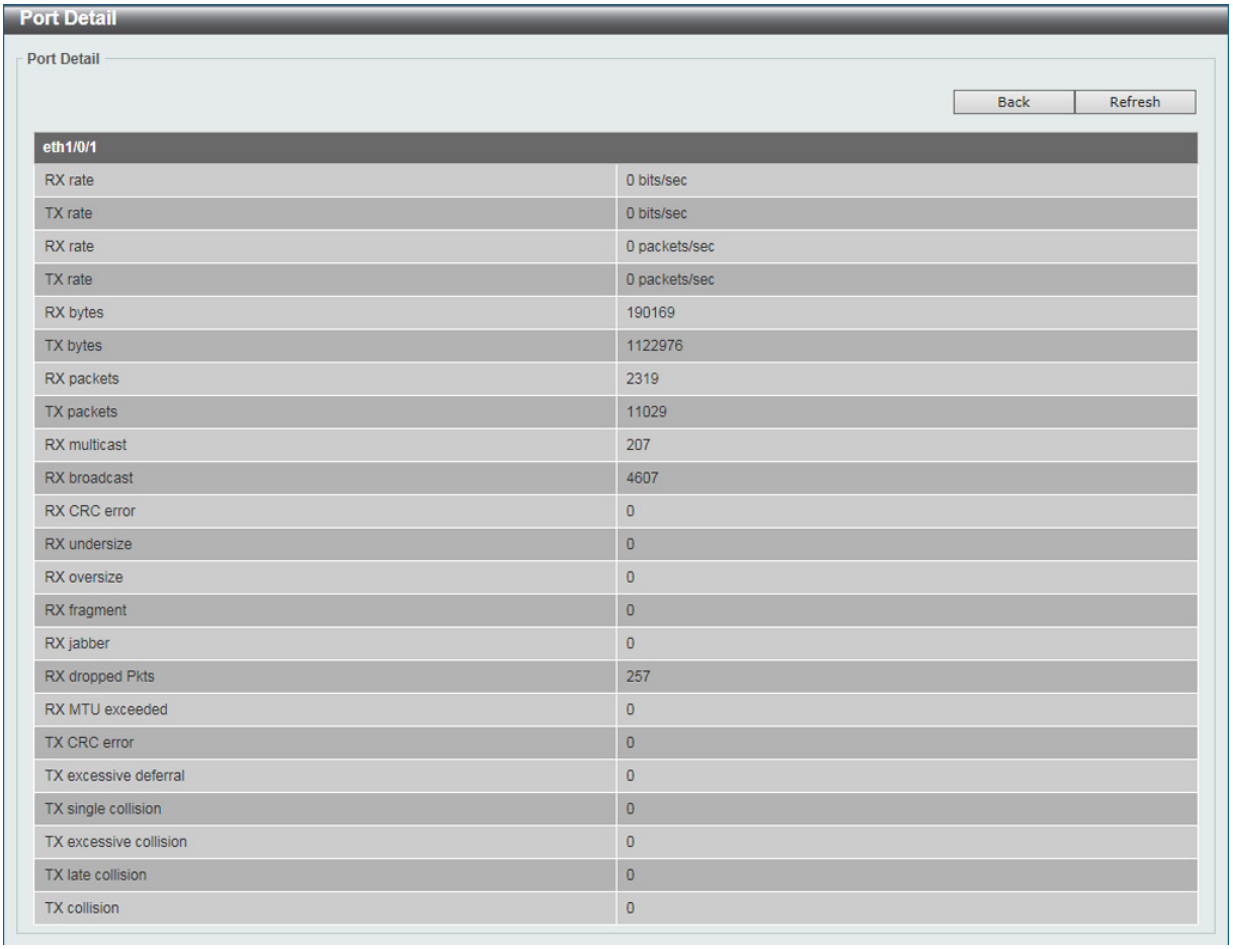


図 16-7　Port（Show Detail）- Port Detail 画面

「Refresh」ボタンをクリックし、テーブルの情報を更新します。
前の画面に戻るには、「Back」ボタンをクリックします。

注意　受信パケットサイズが 1518 ～ 1536Bytes の場合、rxOversizedPkts の数値が増加し、それより大きい場合は rxMTUDropPkts、dot3StatsFrameTooLongs の数値が増加します。

CPU Port（CPU ポート）

CPU の統計情報について表示します。

Monitoring > Statistics > CPU Port の順にメニューをクリックし、以下の画面を表示します。

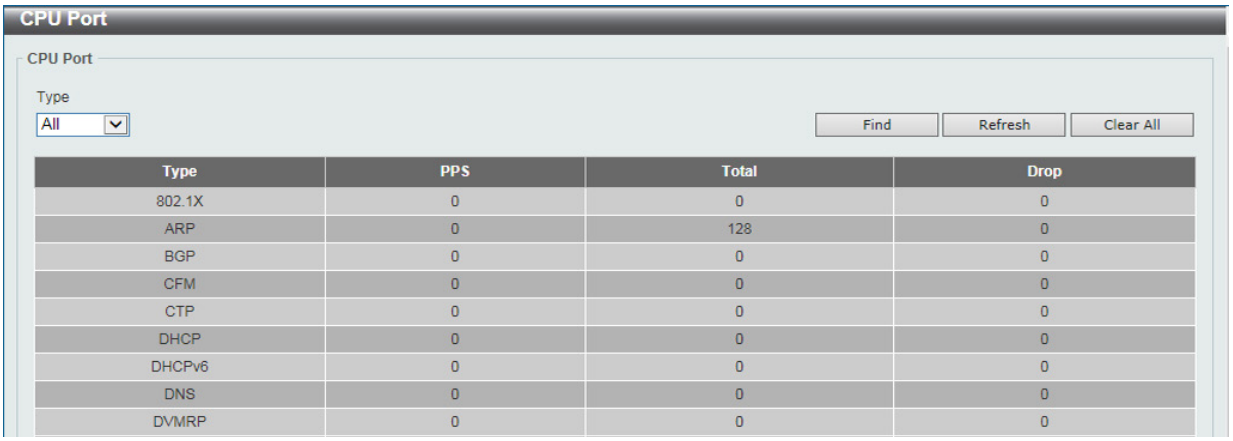


図 16-8　CPU Port 画面

画面に表示される項目：

項目	説明
Type	表示する情報のタイプを指定します。 • 選択肢：「All」「L2」「L3」「Protocol」

「Find」ボタンをクリックして、指定した情報を基に特定のエントリを検出します。

「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。

Interface Counters（インタフェースカウンタ）

インタフェースカウンタ情報について表示します。

Monitoring > Statistics > Interface Counters の順にメニューをクリックし、以下の画面を表示します。

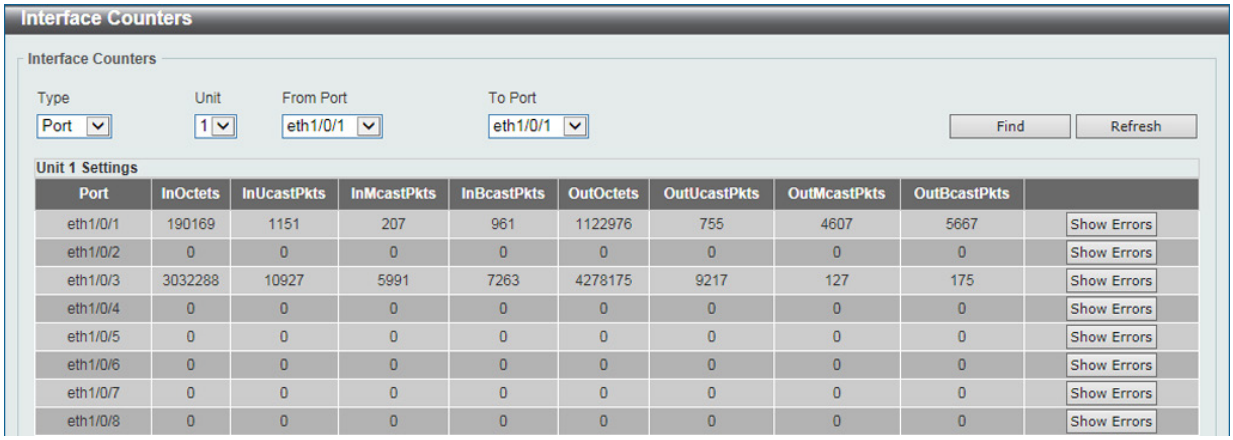


図 16-9　Interface Counters 画面

画面に表示される項目：

項目	説明
Type	表示する情報のタイプを指定します。 • 選択肢：「Port」「VLAN」
Unit	インタフェースカウンタを表示するユニットを指定します。
From Port / To Port	インタフェースカウンタを表示するポート範囲を指定します。

「Find」ボタンをクリックして、指定した情報を基に指定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Show Errors」ボタンをクリックして、指定ポートのエラー情報について表示します。

「Show Errors」ボタンをクリックすると、次の画面が表示されます。

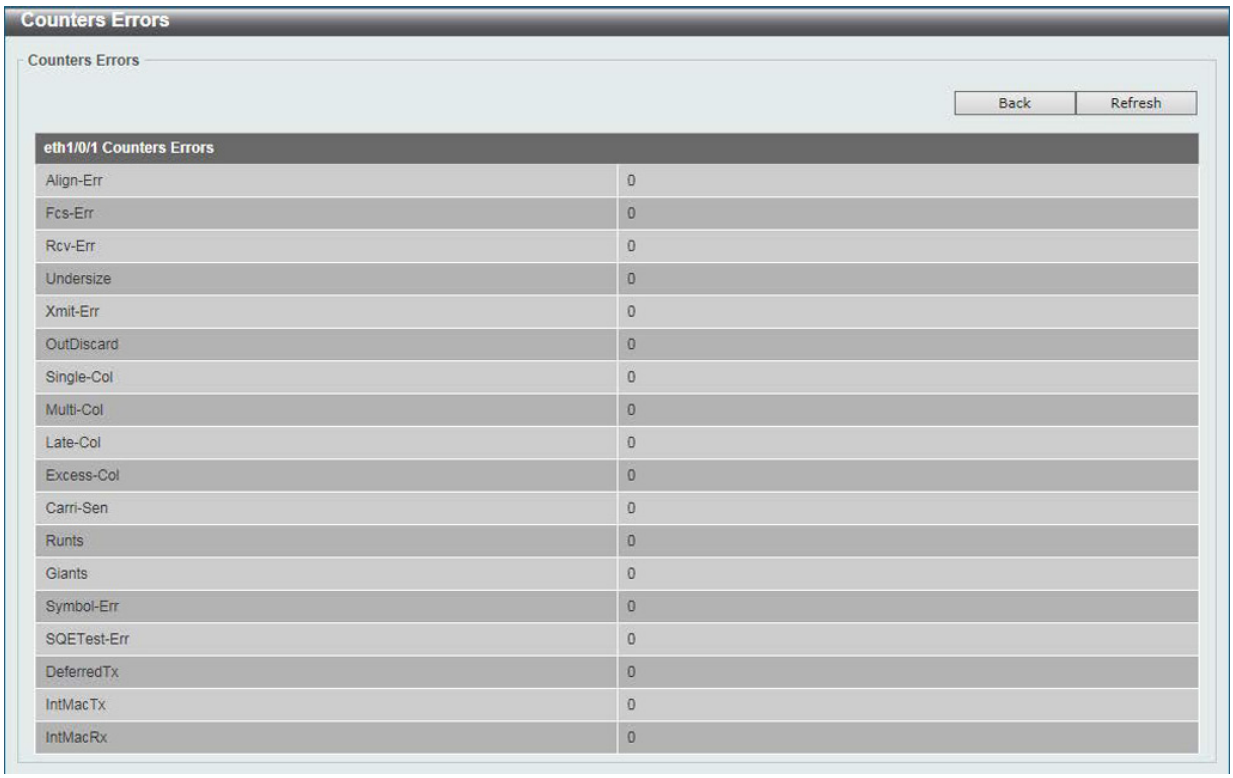


図 16-10　Interface Counters (Show Errors) 画面

前の画面に戻るには、「Back」ボタンをクリックします。
「Refresh」ボタンをクリックし、テーブルの情報を更新します。

「Type」で「VLAN」を選択すると、次の画面が表示されます。

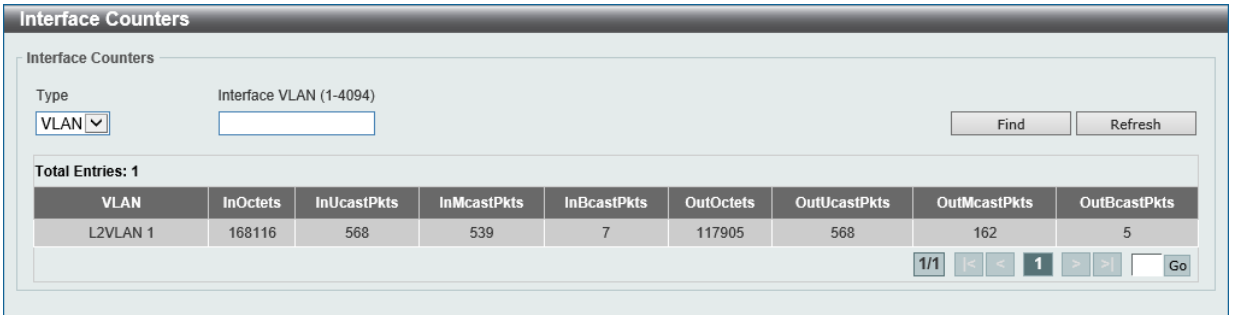


図 16-11　Interface Counters (VLAN) 画面

画面に表示される項目：

項目	説明
Type	表示するタイプを指定します。 • 選択肢：「Port」「VLAN」
Interface VLAN	インタフェースカウンタを表示する VLAN ID を指定します。

「Find」ボタンをクリックして、入力した情報を基に指定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。

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。

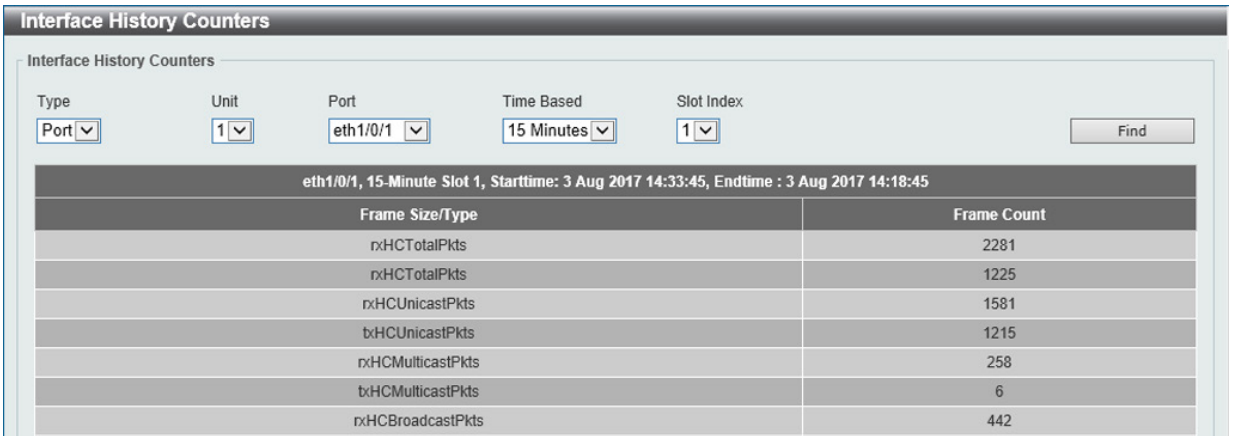


図 16-12　Interface History Counters 画面

画面に表示される項目：

項目	説明
Type	表示する情報のタイプを指定します。
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。
Time Based	表示する統計情報の期間を指定します。 • 「15 Minutes」- 15 分間単位の使用情報を表示します。 • 「1 Day」- 1 日単位の使用情報を表示します。 「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1Day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。
Slot Index	スロットのインデックスを指定します。 • 選択肢：「1」「2」「3」「4」「5」（「15 Minutes」選択時） 「1」「2」（「1 Day」選択時）

「Find」ボタンをクリックして、指定した情報を基に特定のエントリを検出します。

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。

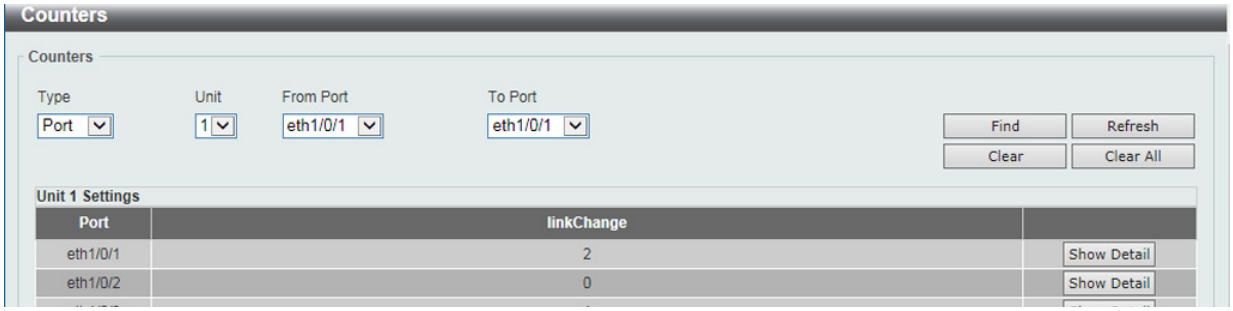


図 16-13　Counters 画面（Port 選択時）

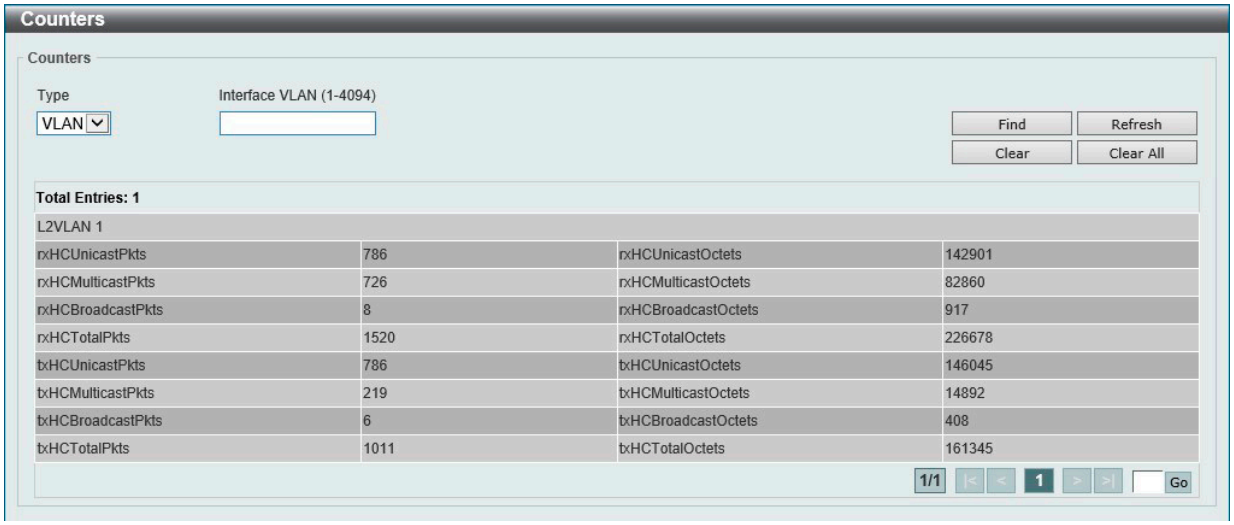


図 16-14　Interface Counters 画面（VLAN 選択時）

画面に表示される項目：

項目	説明
Type	表示するタイプを指定します。 • 「Port」- ポート毎のカウンタを表示します。 • 「VLAN」- VLAN 毎のカウンタを表示します。
Unit	「Port」を選択した場合、表示するユニットを選択します。
From Port / To Port	「Port」を選択した場合、表示するポート範囲を指定します。
Interface VLAN	「VLAN」を選択した場合、表示するインタフェース VLAN ID を指定します。

「Find」ボタンをクリックして、指定 / 入力した情報を基に特定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルの情報を更新します。
「Clear」ボタンをクリックして、指定ポートの情報を消去します。
「Clear All」ボタンをクリックして、テーブル上のすべての情報を消去します。
「Show Detail」ボタンをクリックして、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

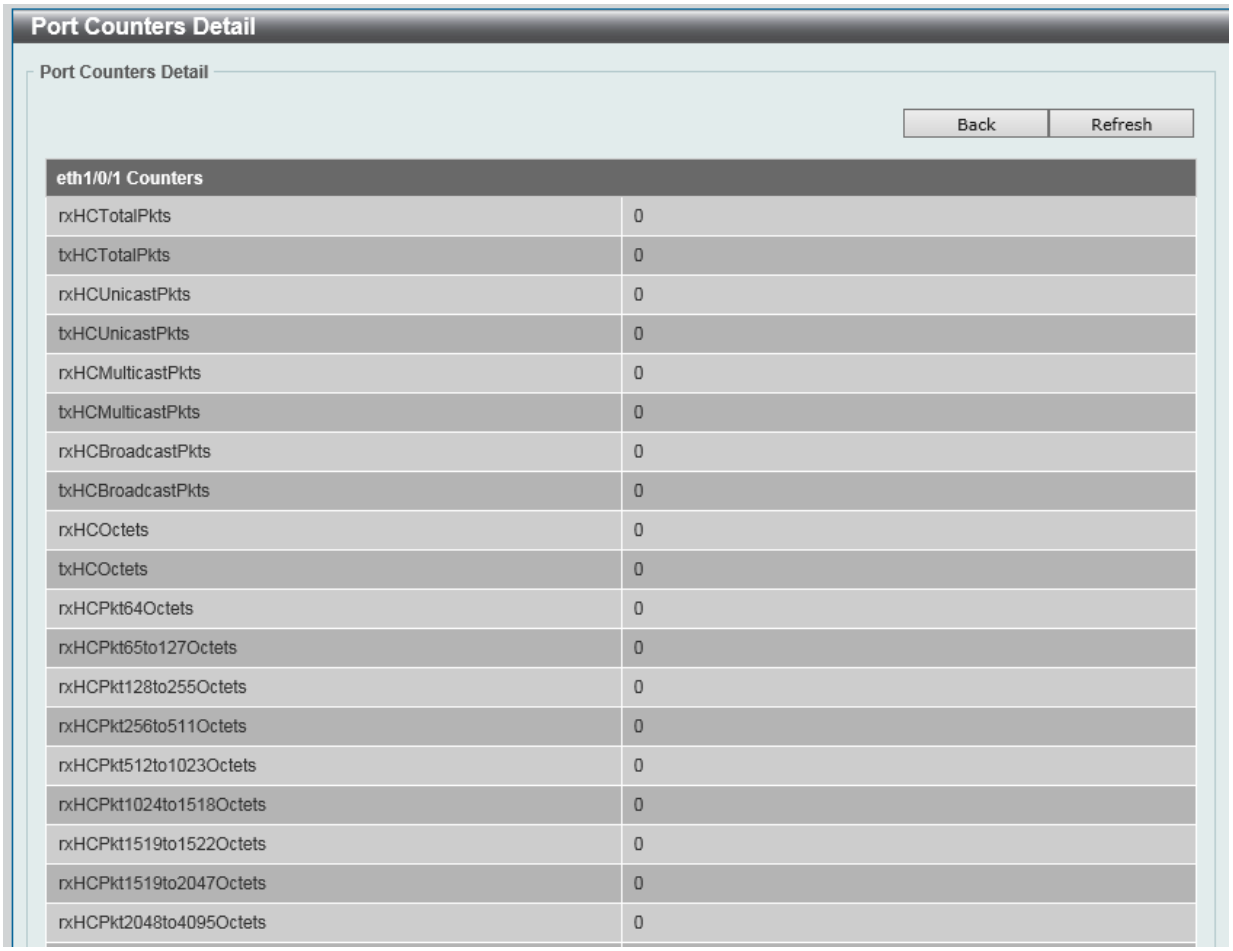


図 16-15　Interface Counters（Show Detail）- Port Counters Detail 画面

「Refresh」ボタンをクリックし、テーブルの情報を更新します。
前の画面に戻るには、「Back」ボタンをクリックします。

Mirror Settings（ミラー設定）

ミラーリング機能についての設定、表示を行います。本スイッチは、対象ポートで送受信するフレームをコピーして、そのコピーしたフレームの出力先を他のポートに変更する機能（ポートミラーリング）を持っています。ミラーリングポートに監視機器（スニファや RMON probe など）を接続し、最初のポートを通したパケットの詳細を確認することができます。トラブルシューティングやネットワーク監視の目的に適しています。

Monitoring > Mirror Settings をクリックします。

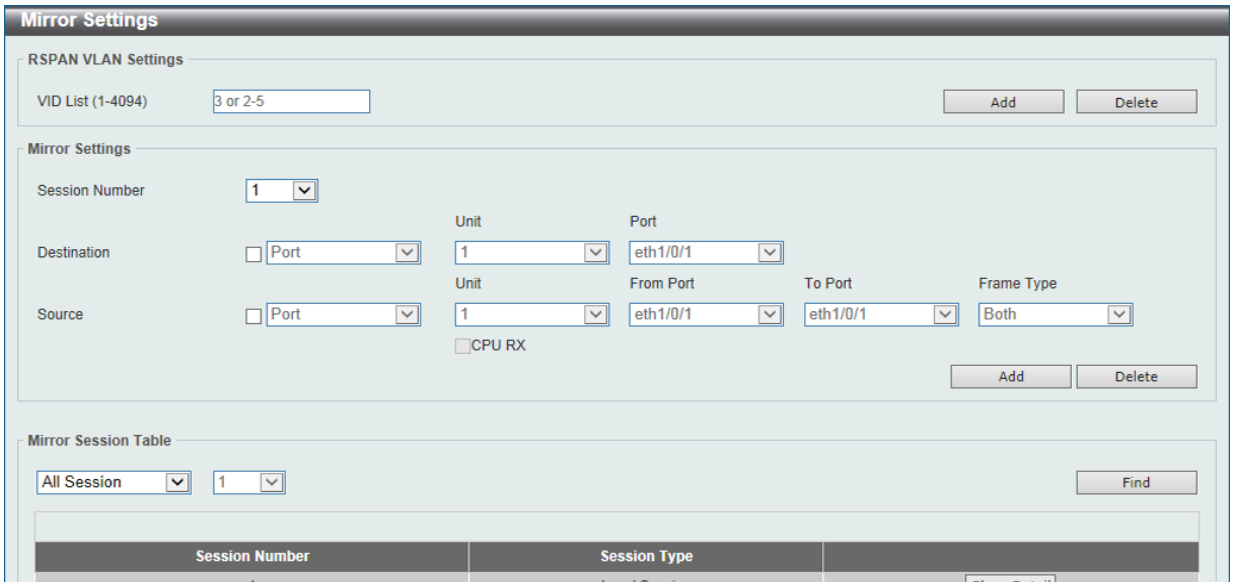


図 16-16　Mirror Settings 画面

画面に表示される項目：

項目	説明
RSPAN VLAN Settings	
VID List	VLAN ID のリストを指定します。
Mirror Settings	
Session Number	このエントリのセッション番号を指定します。 • 設定可能範囲：1-4
Destination	チェックボックスにチェックを入れ、ポートミラーエントリの宛先タイプを設定します。 • 「Port」-「Port」を選択した後に、宛先ユニットとポート番号を指定します。 • 「Remote VLAN」-「Remote VLAN」を選択した後に、宛先ユニットとポート番号を指定し、「VID」（2-4094）を指定します。 • 「Replace」-「Replace」を選択した後に、ACL 名と VID（2-4094）を指定します。
Source	チェックボックスにチェックを入れ、ポートミラーエントリの送信元タイプを設定します。 • 「Port」-「Port」を選択した後に、ユニット ID と「From Port」および「To Port」の番号を指定します。また、「Frame Type」オプションを指定します。「Frame Type」で指定可能なオプションは「Both」「RX」「TX」「TX Forwarding」です。「Both」を選択すると送受信両方のトラフィックがミラーされます。「RX」の場合、受信トラフィックのみミラーされ、「TX」は送信トラフィックのみミラーされます。「CPU RX」オプションにチェックを入れると、CPU RX トラフィックを監視します。 • 「ACL」- ACL 名を入力します。 • 「VLAN」-「VLAN」を選択した後に、「VID List」を指定し、Frame Type を選択します。「RX」のみサポートされます。 • 「Remove VLAN」-「Remote VLAN」を選択した後に VID（2-4094）を指定します。
Mirror Session Table	
Mirror Session Type	表示する情報のミラーセッションタイプを選択します。 • 選択肢：「All Session」「Session Number」「Remote Session」「Local Session」 「Session Number」を選択した後、ドロップダウンメニューからセッション番号（1-4）を選択します。

「Add」ボタンをクリックして、指定 / 入力した情報に基づき新規のミラーエントリを追加します。
「Delete」ボタンをクリックして、指定 / 入力した情報に基づき既存のミラーエントリを削除します。
「Find」ボタンをクリックして、指定した情報に基づいたエントリを検出します。

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、宛先ポートへのミラーリングが行われます。

「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）- Mirror Session Detail 画面

sFlow（sFlow 設定）

sFlow は、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。

sFlow Agent Information（sFlow エージェント情報）

sFlow エージェント情報を表示します。

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。

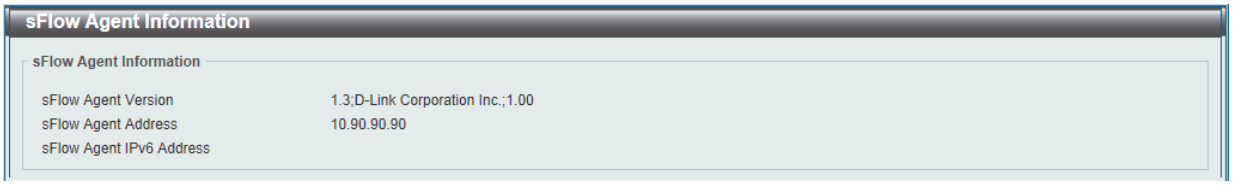


図 16-18　sFlow Agent Information 画面

sFlow Receiver Settings（sFlow レシーバ設定）

sFlow エージェントのレシーバを設定、表示します。レシーバは sFlow エージェントから削除したり追加したり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。

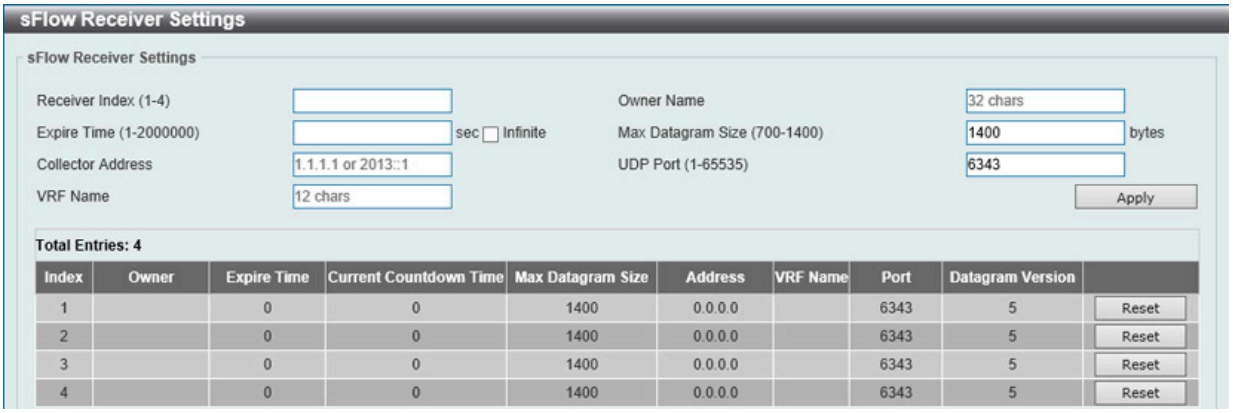


図 16-19　sFlow Receiver Settings 画面

画面に表示される項目：

項目	説明
Receiver Index	追加する sFlow レシーバの識別子を指定します。 • 設定可能範囲：1-4
Owner Name	sFlow レシーバのオーナ名を指定します。（32 文字以内）
Expire Time	エントリの有効期限を指定します。期限になるとエントリのパラメータはリセットされます。「Infinite」を設定するとエントリはタイムアウトしません。 • 設定可能範囲：1-2000000（秒）
Max Datagram Size	sFlow データ 1 つあたりの最大データバイト数を指定します。 • 設定可能範囲：700-1400（Bytes） • 初期値：1400（Bytes）

項目	説明
Collector Address	リモート sFlow コレクタの IPv4/IPv6 アドレスを指定します。
UDP Port	リモート sFlow コレクタの UDP ポート番号を指定します。 • 設定可能範囲：1-65535 • 初期値：6343
VRF Name （EI モードのみ）	VRF インスタンスの名前を入力します。（12 文字以内）

「Apply」ボタンをクリックして、設定内容を適用します。
「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行います。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

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Instance	インタフェースに複数のサンプラを設定する場合、インスタンスのインデックス番号を指定します。 • 設定可能範囲：1-65535
Receiver	レシーバの識別番号を指定します。何も指定しない場合、値は「0」になります。 • 設定可能範囲：1-4
Mode	モードを指定します。 •「Inbound」- 受信パケットをサンプリングします。（初期値） •「Outbound」- 送信パケットをサンプリングします。
Sampling Rate	パケットサンプリングのレートを設定します。指定しない場合、初期値の「0」となります。 • 設定可能範囲：0-65536 • 初期値：0（サンプリング無効）
MAX Header Size	サンプリングパケットからコピーすることができる最大バイト数を設定します。 • 設定可能範囲：18-256（Bytes） • 初期値：128（Bytes）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

sFlow Poller Settings（sFlow ポーラ設定）

スイッチのポーラ設定を行います。

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

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Instance	インタフェースで複数のサンプラを設定する場合、インスタンスの識別番号を指定します。 • 設定可能範囲：1-65535
Receiver	レシーバの識別番号を指定します。 • 設定可能範囲：1-4
Interval	ポーリングサンプリングの間隔を設定します。「0」を入力すると機能は無効になります。 • 設定可能範囲：0-120（秒） • 初期値：0（秒）

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定エントリを削除します。

Device Environment（機器環境確認）

本画面ではスイッチの内部温度状態を表示します。

Monitoring > Device Environment をクリックして次の画面を表示します。

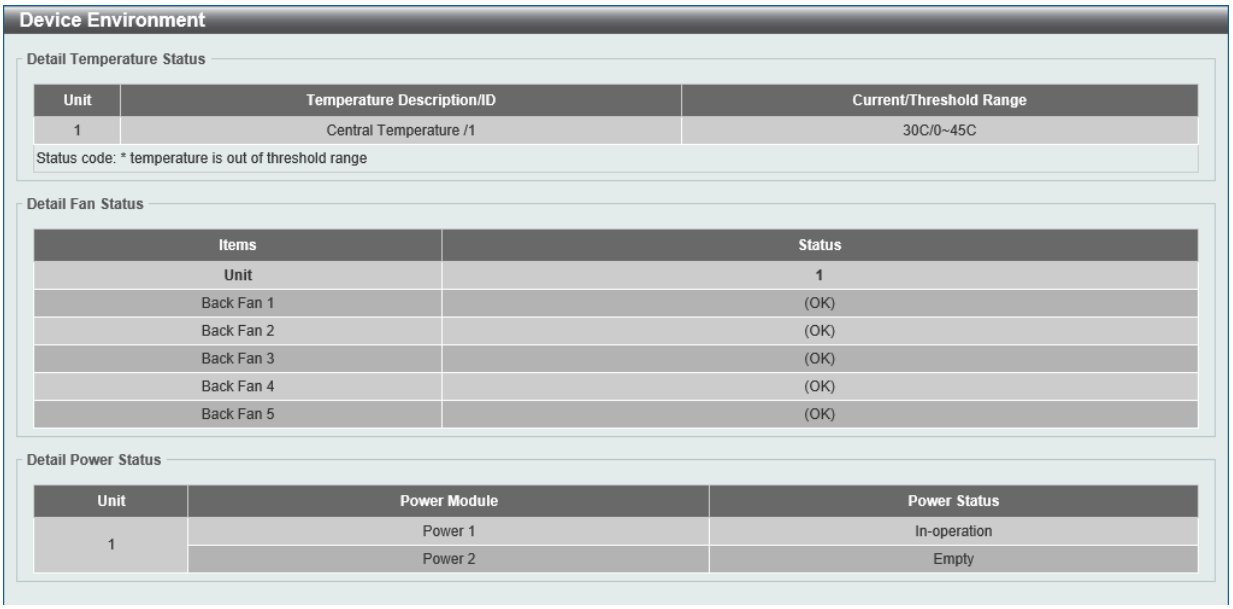


図 16-22　Device Environment 画面

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

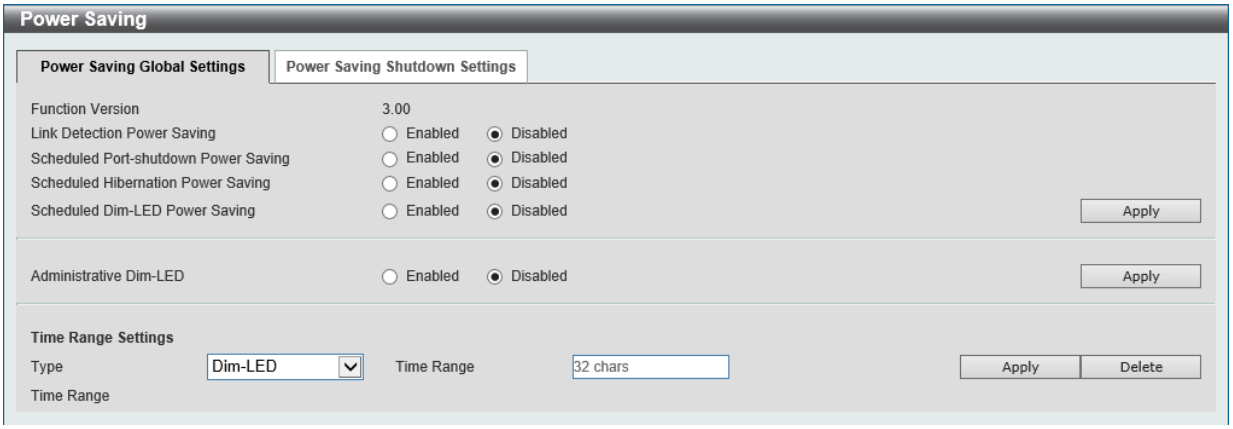


図 17-1　Power Saving 画面 - Power Saving Global Settings タブ

画面に表示される項目：

項目	説明
Link Detection Power Saving	「リンク検出」を有効 / 無効に設定します。本設定を有効にすると、リンクダウンしているポートへの電力供給が停止し、スイッチの消費電力を抑えます。リンクアップしているポートへの影響はありません。
Scheduled Port-shutdown Power Saving	スケジュールによるポートシャットダウン機能の有効 / 無効を指定します。
Scheduled Hibernation Power Saving	スケジュールによるスイッチ休止の有効 / 無効を指定します。
Scheduled Dim-LED Power Saving	スケジュールによる減光 LED の有効 / 無効を指定します。
Administrative Dim-LED	ポート LED 機能の有効 / 無効を指定します。
Time Range Settings	
Type	省電力モードの種類を指定します。 • 選択肢：「Dim-LED」
Time Range	上記省電力機能に適用するスケジュールを指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

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

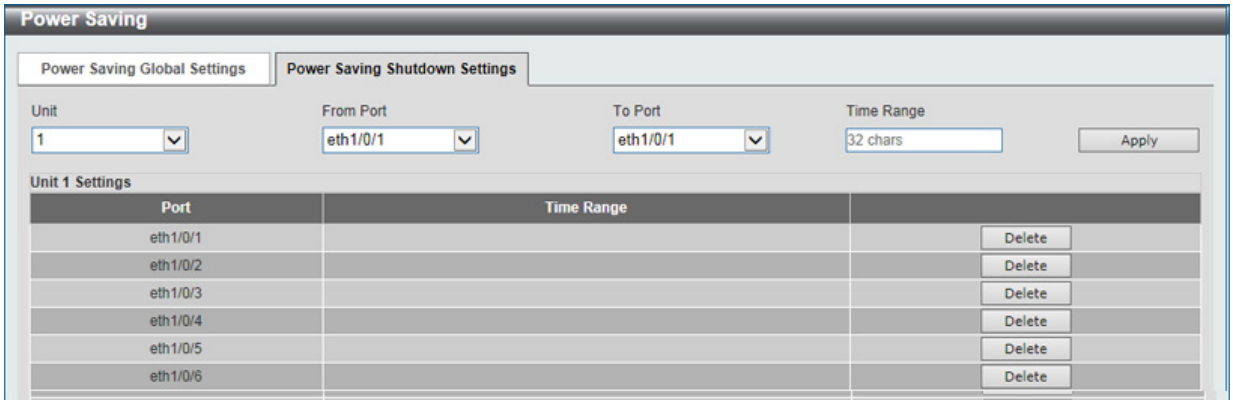


図 17-2　Power Saving 画面 - Power Saving Shutdown Settings タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
Time Range	ポートに適用するスケジュール名を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

EEE（Energy Efficient Ethernet/ 省電力イーサネット）

「Energy Efficient Ethernet」(EEE/ 省電力イーサネット) は「IEEE 802.3az」によって定義されています。リンク上でパケットの送受信が発生していない場合、電力消費を抑えることができます。

Green > EEE メニューをクリックし、以下の画面を表示します。

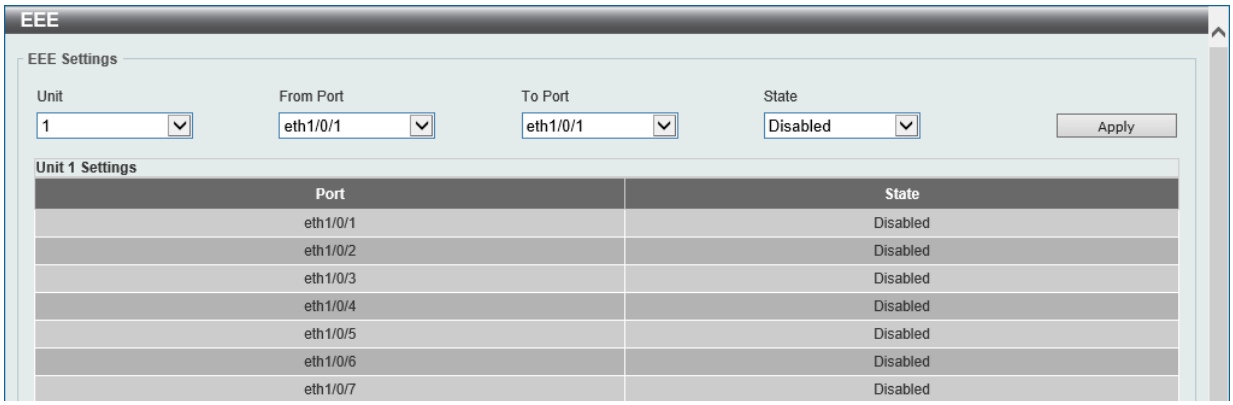


図 17-3　EEE 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port / To Port	本設定を適用するポート範囲を指定します。
State	本機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

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 コントローラ側で同じプロトコルバージョンがサポートされていることをご確認下さい。

OpenFlow Settings（OpenFlow 設定）

OpenFlow > OpenFlow Settings メニューでは、OpenFlow の設定を行います。

OpenFlow Global Settings タブ

OpenFlow > OpenFlow Settings > OpenFlow Global Settings タブをクリックし、以下の画面を表示します。

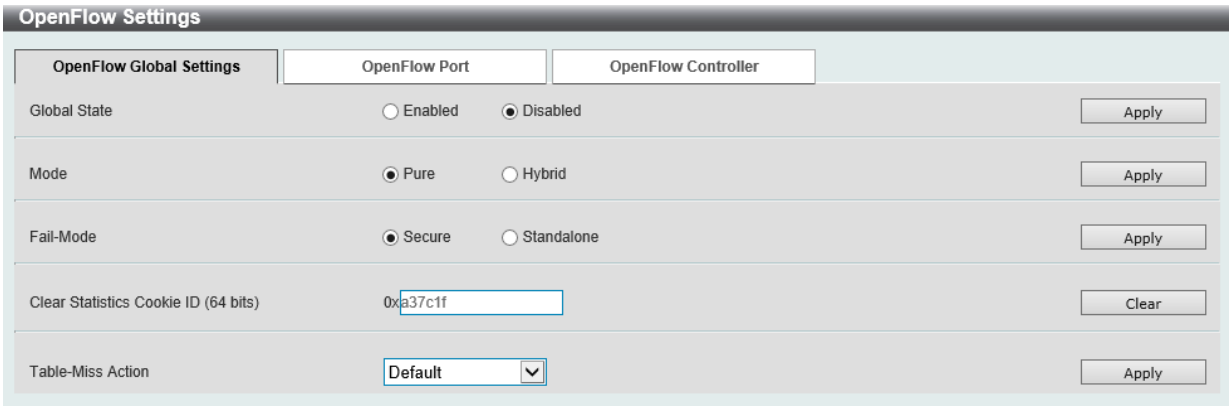


図 18-1　OpenFlow Settings 画面 - OpenFlow Global Settings タブ

画面に表示される項目：

項目	説明
Global State	OpenFlow をグローバルで有効 / 無効に設定します。
Mode	OpenFlow のモードを指定します。 • 「Pure」- すべてのポートが OpenFlow パイプラインにあることを指定します。 • 「Hybrid」- 一部のポートが OpenFlow パイプラインにあり、一部が通常のパイプラインにあることを指定します。
Fail-Mode	Fail モードを指定します。 • 「Secure」- スイッチはコントローラへのパケットとメッセージの送信を停止します。フローエントリは、引き続きタイムアウトに従って期限切れになります。 • 「Standalone」- スイッチはコントローラへのパケットとメッセージの送信を停止します。フローエントリは削除されます。レガシー機能は、既存の通常ポートで引き続き機能します。このモードは、ハイブリッドスイッチでのみ使用できます。
Clear Statistics Cookie ID	フローエントリの Cookie ID を入力します。指定したフローエントリに関する統計情報がクリアされます。
Table-Miss Action	Table-Miss アクションを指定します。 • 「Default」- デフォルトアクションを使用します。 • 「Drop」- Table-Miss エントリをクリアし、不明なパケットを破棄します。 • 「Controller」- Table-Miss エントリにアクションを適用します。設定されるアクションは、コントローラへの送信です。不明なパケットはコントローラに送信されます。

「Apply」ボタンをクリックして、設定内容を適用します。
「Clear」ボタンをクリックして、指定の統計を削除します。

OpenFlow Port タブ

OpenFlow > OpenFlow Settings > OpenFlow Port タブをクリックし、以下の画面を表示します。

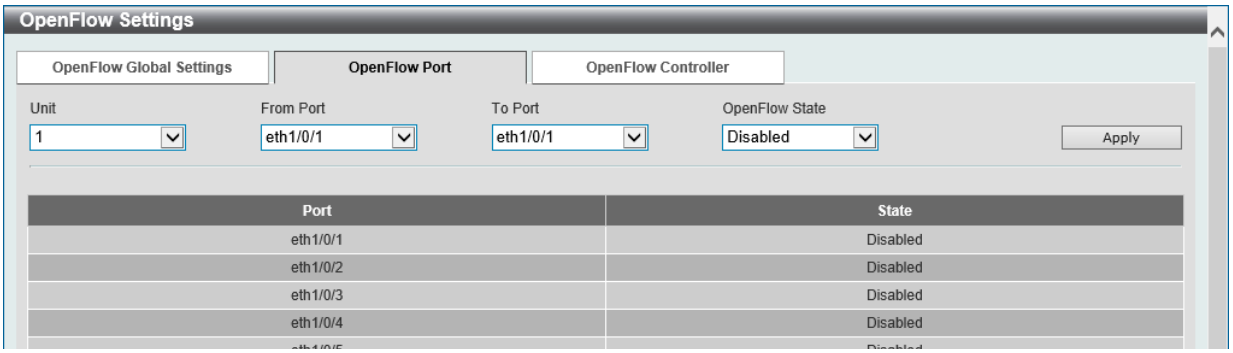


図 18-1　OpenFlow Settings 画面 - OpenFlow Port タブ

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を指定します。
OpenFlow State	指定ポートの OpenFlow 機能を有効 / 無効に設定します。

「Apply」ボタンをクリックして、設定内容を適用します。

OpenFlow Controller タブ

OpenFlow > OpenFlow Settings > OpenFlow Controller タブをクリックし、以下の画面を表示します。

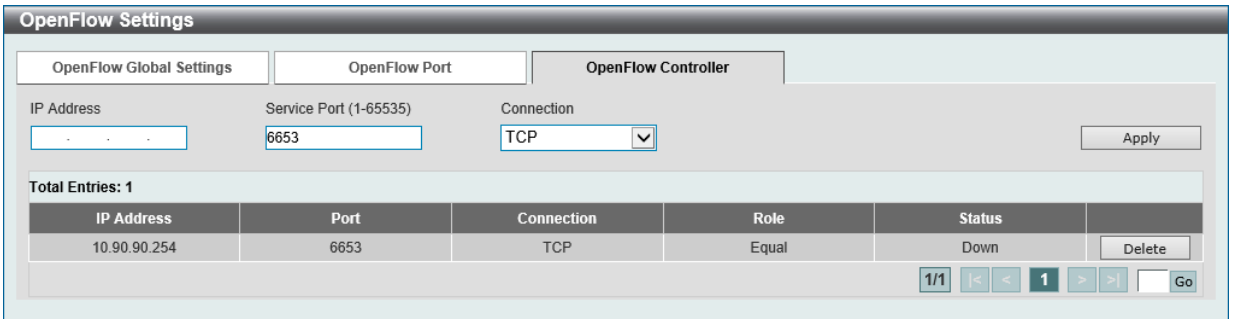


図 18-2　OpenFlow Settings 画面 - OpenFlow Controller タブ

画面に表示される項目：

項目	説明
IP Address	OpenFlow コントローラの IPv4 アドレスを入力します。
Service Port	コントローラへの接続に使用する TCP ポート番号を入力します。 • 設定可能範囲：1-65535 • 初期値：6653
Connection	接続方法を選択します。 • 選択肢：「TCP」「TLS」

「Apply」ボタンをクリックして、設定内容を適用します。
「Delete」ボタンをクリックして、指定のエントリを削除します。

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（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

現在実行中のコンフィグレーションをブートコンフィグとしてスイッチに保存します。電源が落ちた場合にコンフィグレーションが失われることを防ぎます。

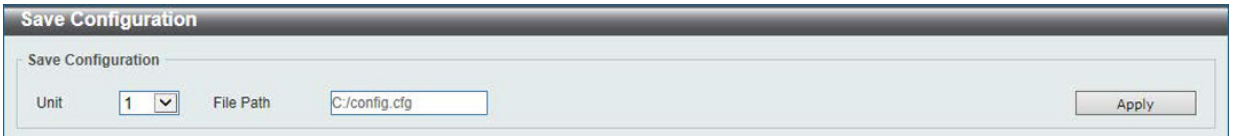


図 19-1　Save - Configuration 画面

以下の項目が表示されます。

項目	説明
Unit	保存先のユニットを選択します。
File Path	保存先のファイルパスおよびファイル名を指定します。

「Apply」ボタンをクリックして、コンフィグレーションを保存します。

Tools（Tools メニュー）

ファームウェアアップグレード＆バックアップ、コンフィグレーションリストア＆バックアップ、ログファイルのバックアップ、Ping、トレースルート、リセット、システム再起動、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。

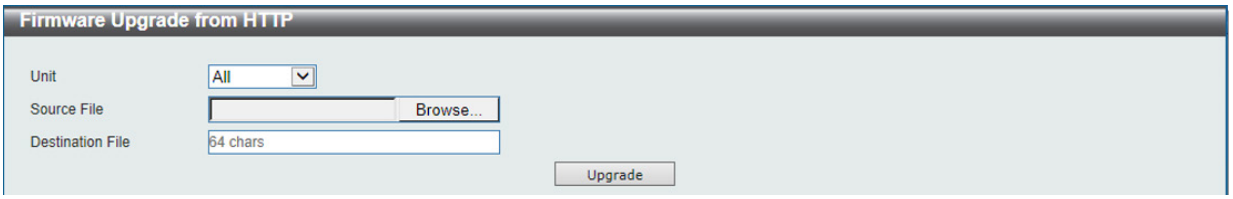


図 19-2　Firmware Upgrade from HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定します。
Destination File	ファームウェアが保存されるスイッチの場所を指定します。（64 文字以内）

「Upgrade」ボタンをクリックして、アップグレードを開始します。

Firmware Upgrade from TFTP（TFTP を使用したファームウェアアップグレード）

TFTP を使用してファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP をクリックし、設定画面を表示します。

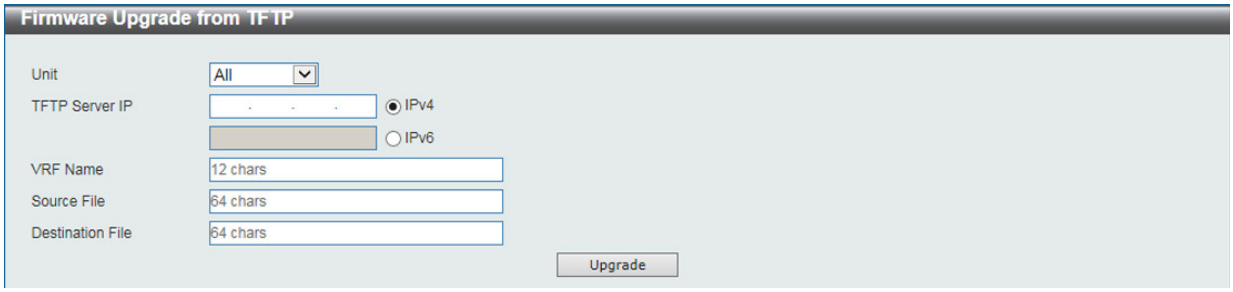


図 19-3　Firmware Upgrade from TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	TFTP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内）
Destination File	ファームウェアが保存されるスイッチの場所を指定します。（64 文字以内）

「Upgrade」ボタンをクリックして、アップグレードを開始します。

Firmware Upgrade from 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。

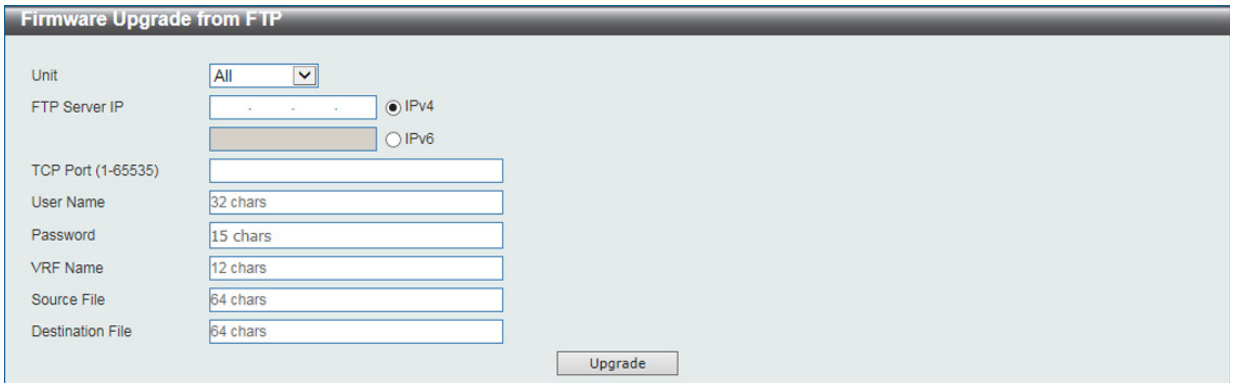


図 19-4　Firmware Upgrade from FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	FTP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内）
Destination File	ファームウェアが保存されるスイッチの場所を指定します。（64 文字以内）

「Upgrade」ボタンをクリックして、アップグレードを開始します。

Firmware Upgrade from 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。

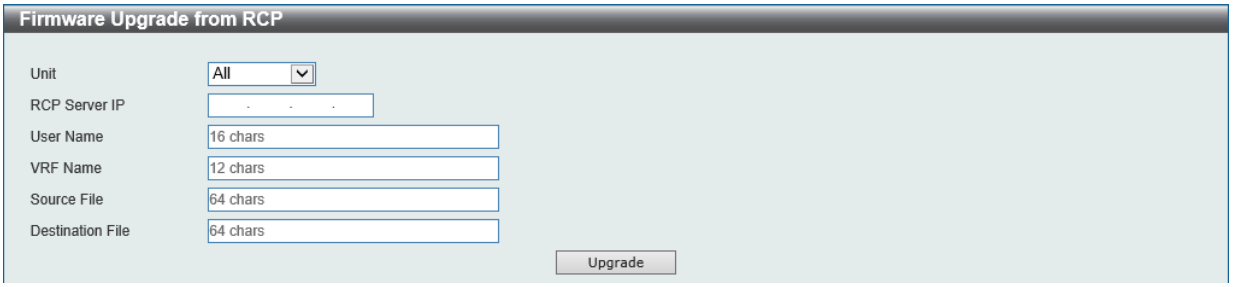


図 19-5　Firmware Upgrade from RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（16 文字以内）を指定します。
VRF Name （EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	RCP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内）
Destination File	ファームウェアが保存されるスイッチの場所を指定します。（64 文字以内）

「Upgrade」ボタンをクリックして、アップグレードを開始します。

Firmware Backup to HTTP（HTTP を使用したファームウェアバックアップ）

HTTP を使用して、ローカル PC へファームウェアバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP をクリックし、設定画面を表示します。

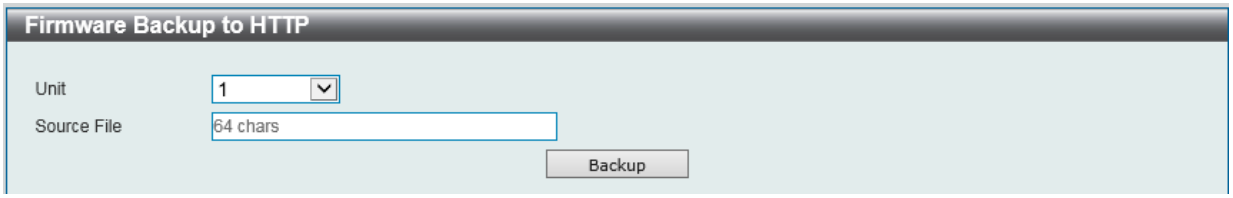


図 19-6　Firmware Backup to HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	スイッチ上でファームウェアが保存されているファイルパスとファイル名を入力します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Firmware Backup to TFTP（TFTP を使用したファームウェアバックアップ）

TFTP サーバにファームウェアバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP をクリックし、設定画面を表示します。

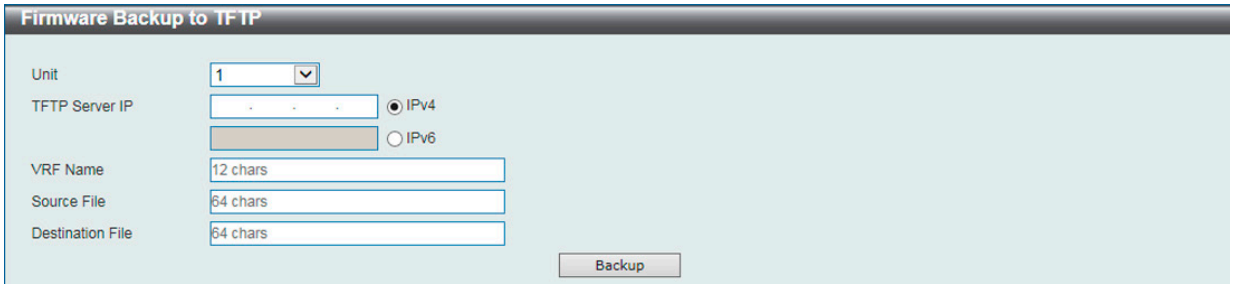


図 19-7　Firmware Backup to TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	スイッチ上でファームウェアが保存されているファイルパスとファイル名を入力します。（64 文字以内）
Destination File	ファームウェアファイルがバックアップされる TFTP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Firmware Backup to FTP（FTP を使用したファームウェアバックアップ）

FTP サーバにファームウェアバックアップを行います。

Tools > Firmware Backup & Backup > firmware Backup to FTP をクリックし、設定画面を表示します。

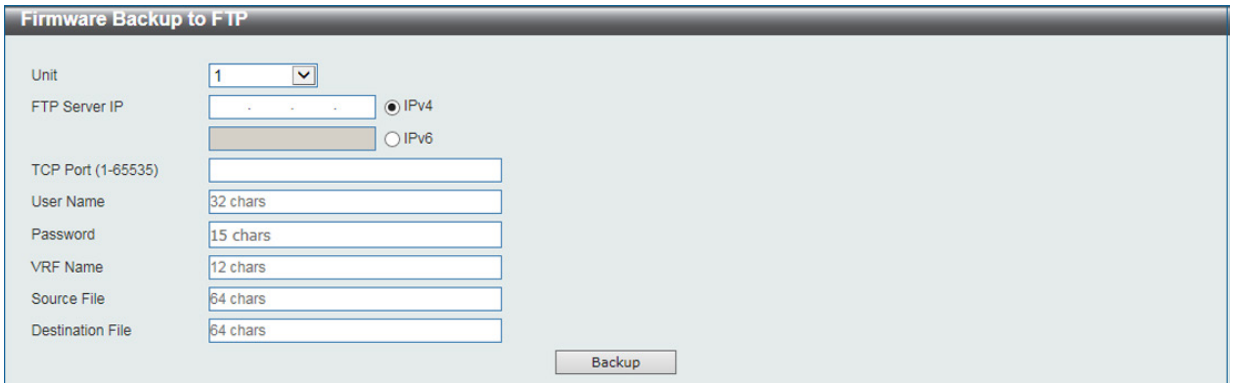


図 19-8　Firmware Backup to FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	スイッチ上でファームウェアが保存されているファイルパスとファイル名を入力します。（64 文字以内）
Destination File	ファームウェアファイルがバックアップされる FTP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Firmware Backup to RCP（RCP を使用したファームウェアバックアップ）

RCP サーバへファームウェアバックアップを行います。

Tools > Firmware Backup & Backup > firmware Backup to RCP をクリックし、設定画面を表示します。

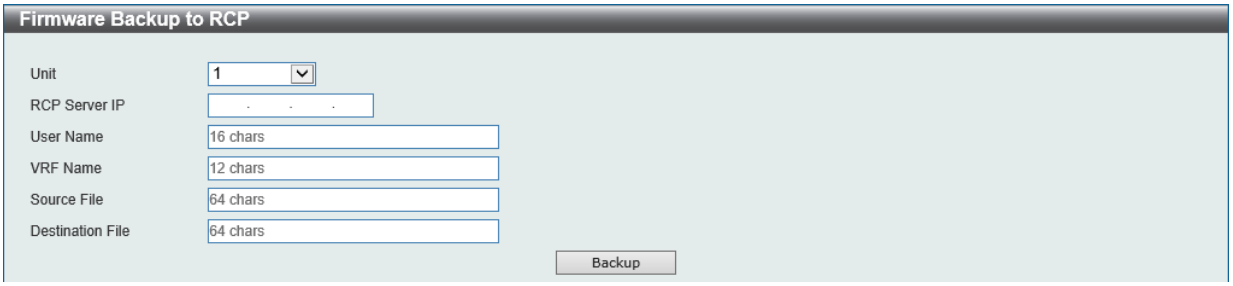


図 19-9　Firmware Backup to RCP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（16 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	スイッチ上でファームウェアが保存されているファイルパスとファイル名を入力します。（64 文字以内）
Destination File	ファームウェアファイルがバックアップされる RCP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）

Configuration Restore from HTTP（HTTP サーバからコンフィグレーションのリストア）

HTTP を使用してローカル PC からコンフィグレーションをリストアします。

Tools > Configuration Restore & Backup > Configuration Restore from HTTP をクリックし、設定画面を表示します。



図 19-10　Configuration Restore from HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	「Browse/ 参照」ボタンをクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定します。
Destination File	コンフィグレーションファイルが保存されるスイッチの場所を指定します。（64 文字以内） 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストア＆上書きされます。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルがリストア＆上書きされます。
Replace	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

「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。

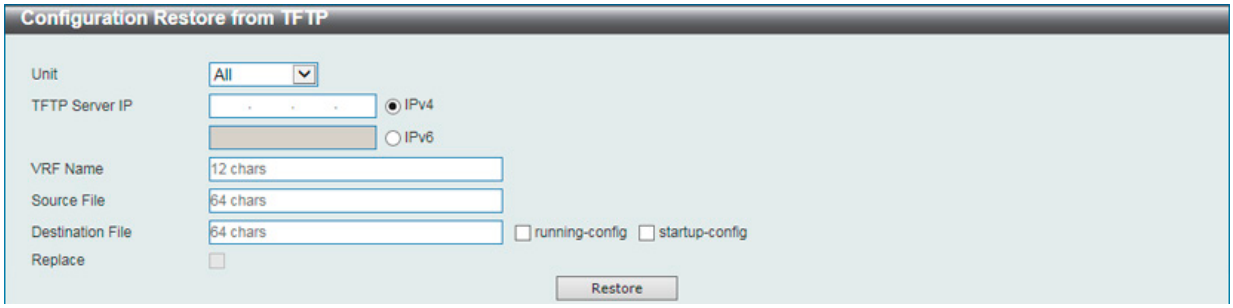


図 19-11　Configuration Restore from TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	TFTP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。（64 文字以内）
Destination File	コンフィグレーションファイルが保存されるスイッチの場所を指定します。（64 文字以内） 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストア＆上書きされます。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルがリストア＆上書きされます。
Replace	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

「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。

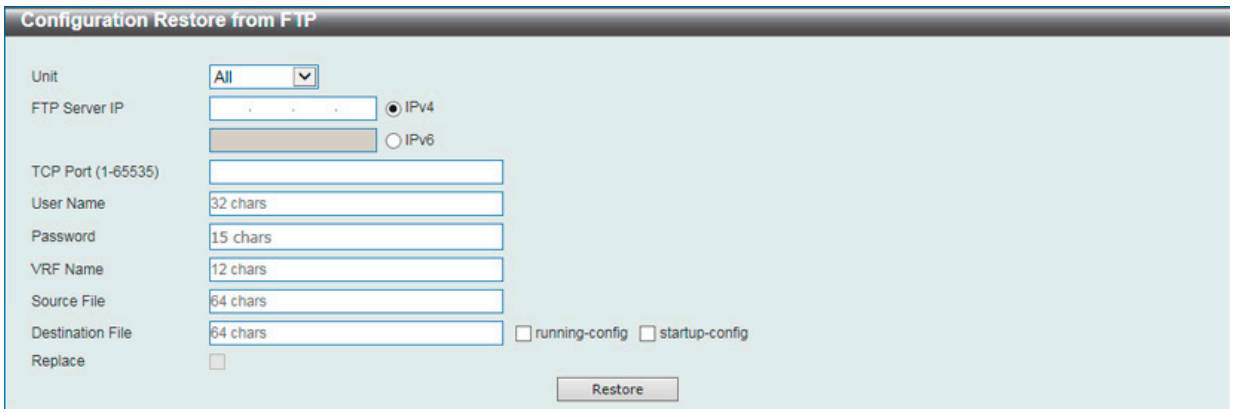


図 19-12　Configuration Restore from FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。

項目	説明
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	FTP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。（64 文字以内）
Destination File	コンフィグレーションファイルが保存されるスイッチの場所を指定します。（64 文字以内） 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストア＆上書きされます。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルがリストア＆上書きされます。
Replace	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

「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。

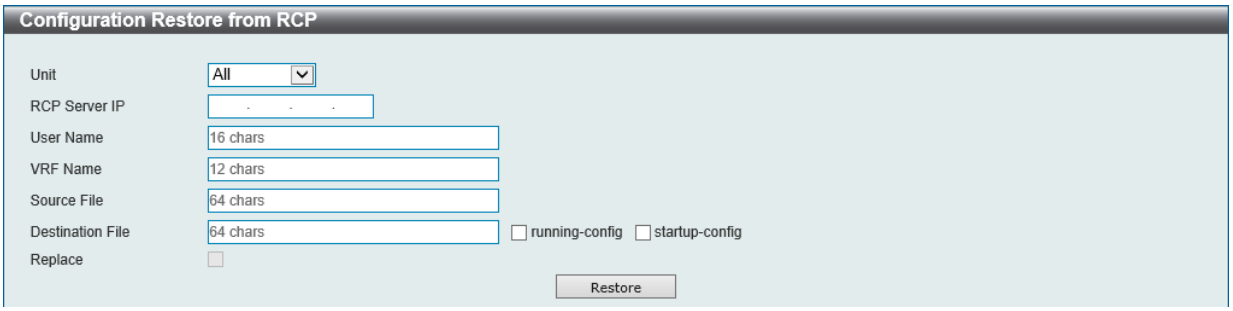


図 19-13　Configuration Restore from RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。 • 「IPv4」- RCP サーバの IPv4 アドレスを入力します。 • 「IPv6」- RCP サーバの IPv6 アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（16 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	RCP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。（64 文字以内）
Destination File	コンフィグレーションファイルが保存されるスイッチの場所を指定します。（64 文字以内） 「running-config」オプションを選択すると、ランニングコンフィグレーションファイルがリストア＆上書きされます。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルがリストア＆上書きされます。
Replace	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

「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 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。

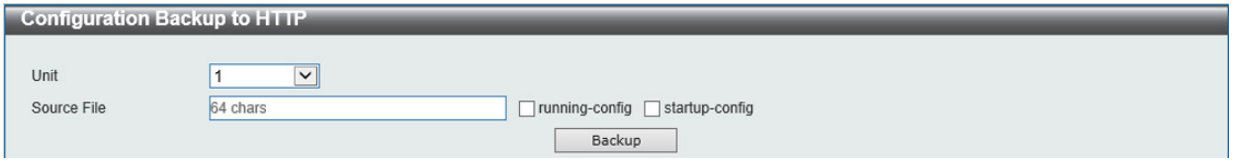


図 19-14　Configuration Backup to HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	スイッチ上でコンフィグレーションが保存されているパスとファイル名を入力します。（64 文字以内） 「running-config」オプションを選択すると、実行中のコンフィグレーションファイルがバックアップされます。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルがバックアップされます。

「Backup」ボタンをクリックして、バックアップを開始します。

Configuration Backup to TFTP（TFTP を使用したコンフィグレーションバックアップ）

TFTP サーバにコンフィグレーションバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to TFTP をクリックし、設定画面を表示します。

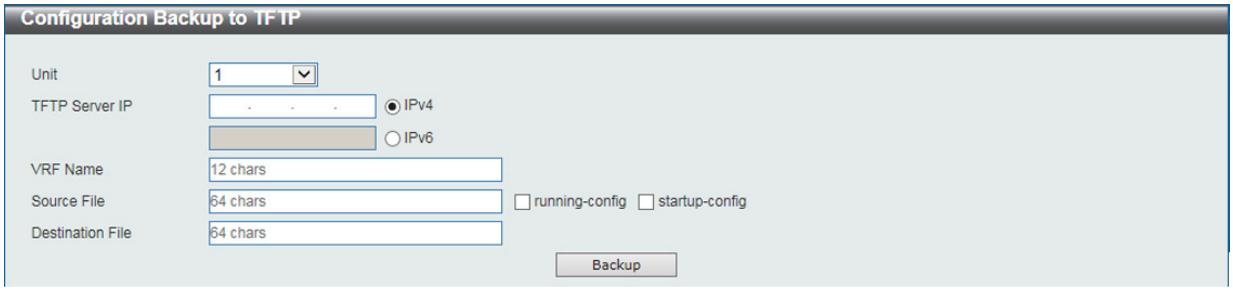


図 19-15　Configuration Backup to TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	スイッチ上でコンフィグレーションが保存されているパスとファイル名を入力します。（64 文字以内） 「running-config」オプションを選択すると、実行中のコンフィグレーションファイルがバックアップされます。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルがバックアップされます。
Destination File	コンフィグレーションファイルが保存される TFTP サーバの場所を指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

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。

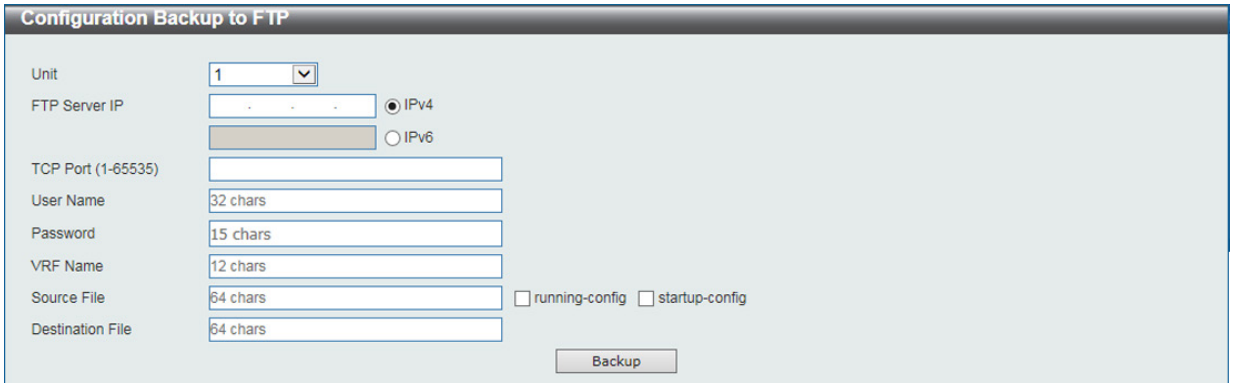


図 19-16　Configuration Backup to FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。

項目	説明
Source File	スイッチ上でコンフィグレーションが保存されているパスとファイル名を入力します。（64 文字以内） 「running-config」オプションを選択すると、実行中のコンフィグレーションファイルがバックアップされます。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルがバックアップされます。
Destination File	コンフィグレーションファイルが保存される FTP サーバの場所を指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

注意　copy running-config ftp: コマンドでエラーが発生する場合、no network-protocol-port protect tcp コマンドを実行してください。

Configuration Backup to RCP（RCP を使用したコンフィグレーションバックアップ）

RCP サーバにコンフィグレーションバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to RCP をクリックし、設定画面を表示します。

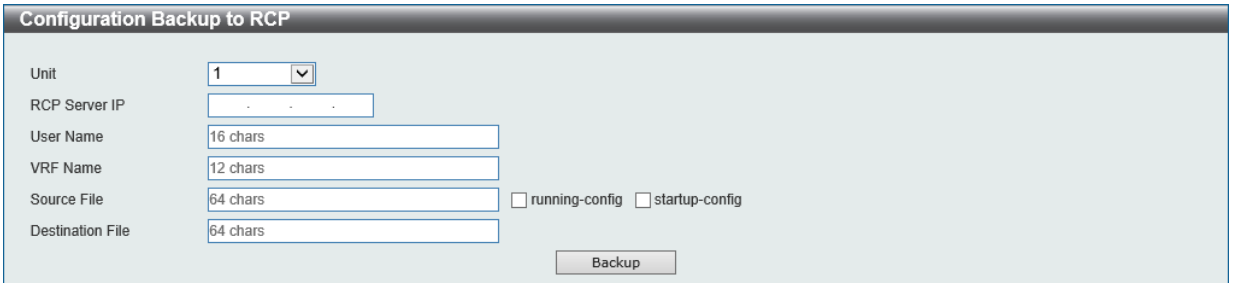


図 19-17　Configuration Backup to RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（16 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	スイッチ上でコンフィグレーションが保存されているパスとファイル名を入力します。（64 文字以内） 「running-config」オプションを選択すると、実行中のコンフィグレーションファイルがバックアップされます。 「startup-config」オプションを選択すると、スタートアップコンフィグレーションファイルがバックアップされます。
Destination File	コンフィグレーションファイルが保存される RCP サーバの場所を指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Certificate & Key Restore & Backup（証明書 / 鍵リストア＆バックアップ）

Certificate & Key Restore from HTTP（HTTP を使用した証明書 / 鍵リストア）

HTTP を使用してローカル PC から証明書 / 鍵のリストアを実行します。

Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from HTTP をクリックし、設定画面を表示します。

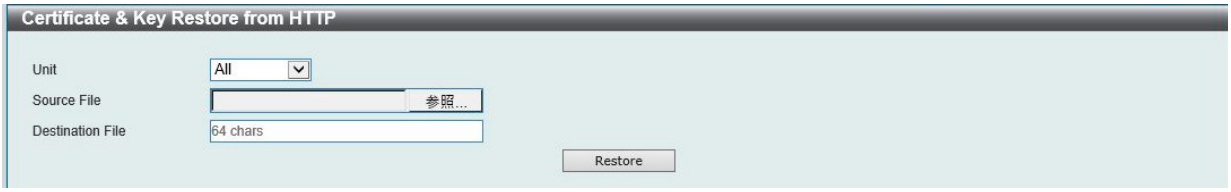


図 19-18　Certificate & Key Restore from HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	「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します。
Destination File	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「Restore」ボタンをクリックして、リストアを開始します。

Certificate & Key Restore from TFTP（TFTP を使用した証明書 / 鍵リストア）

TFTP サーバからの証明書 / 鍵リストアを実行します。

Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from TFTP をクリックし、設定画面を表示します。

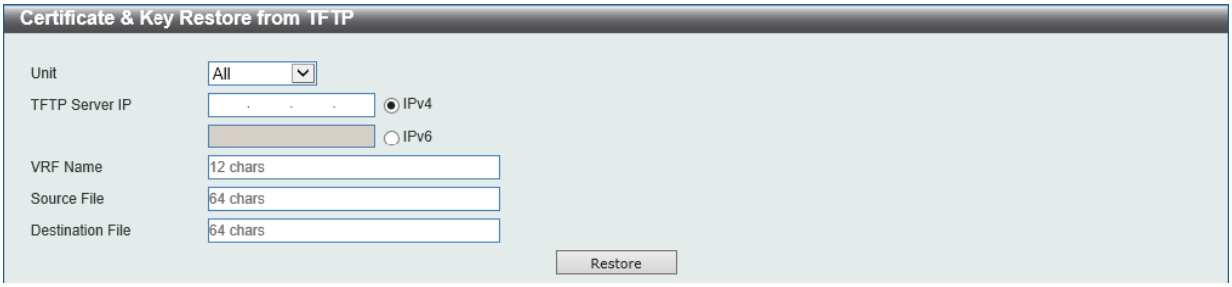


図 19-19　Certificate & Key Restore from TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	TFTP サーバ上に保存されている証明書 / 鍵のパスとファイル名を入力します。（64 文字以内）
Destination File	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「Restore」ボタンをクリックして、リストアを開始します。

Certificate & Key Restore from FTP（FTP を使用した証明書 / 鍵リストア）

FTP サーバからの証明書 / 鍵リストアを実行します。

Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from FTP をクリックし、設定画面を表示します。

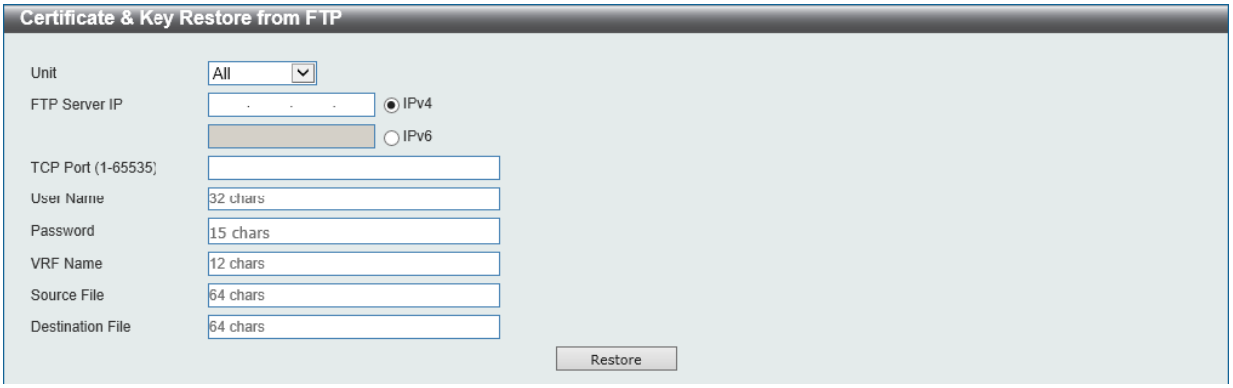


図 19-20　Certificate & Key Restore from FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	FTP サーバ上に保存されている証明書 / 鍵のパスとファイル名を入力します。（64 文字以内）
Destination File	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「Restore」ボタンをクリックして、リストアを開始します。

Certificate & Key Restore from RCP（RCP を使用した証明書 / 鍵リストア）

RCP サーバからの証明書 / 鍵リストアを実行します。

Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from RCP をクリックし、設定画面を表示します。



図 19-21　Certificate & Key Restore from RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（16 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	RCP サーバ上に保存されている証明書 / 鍵のパスとファイル名を入力します。（64 文字以内）
Destination File	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「Restore」ボタンをクリックして、リストアを開始します。

Public Key Backup to HTTP（HTTP を使用した公開鍵バックアップ）

HTTP を使用してローカル PC へ公開鍵バックアップを行います。

Tools > Certificate & Key Restore & Backup > Public Key Backup to HTTP をクリックし、設定画面を表示します。

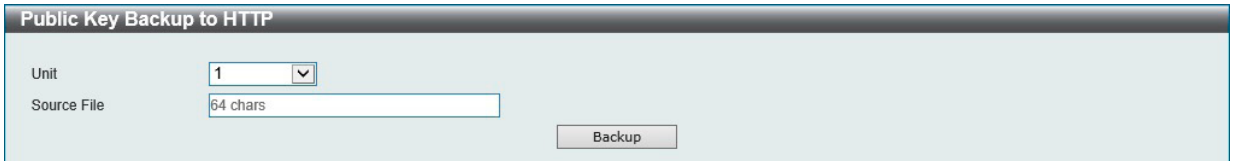


図 19-22　Public Key Backup to HTTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
Source File	スイッチに保存されている証明書 / 鍵ファイルのパスとファイル名を入力します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Public Key Backup to TFTP（TFTP を使用した公開鍵バックアップ）

TFTP サーバに公開鍵バックアップを行います。

Tools > Certificate & Key Restore & Backup > Public Key Backup to TFTP をクリックし、設定画面を表示します。



図 19-23　Public Key Backup to TFTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	スイッチに保存されている証明書 / 鍵ファイルのパスとファイル名を入力します。（64 文字以内）
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 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Public Backup to FTP（FTP を使用した公開鍵バックアップ）

FTP サーバへの公開鍵バックアップを実行します。

Tools > Certificate & Key Restore & Backup > Public Key Backup to FTP をクリックし、設定画面を表示します。

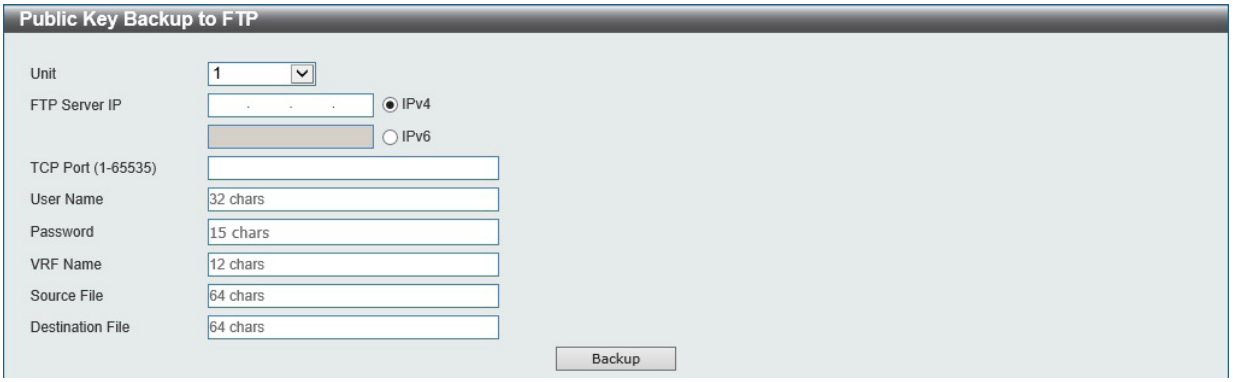


図 19-24　Public Key Backup to FTP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
FTP Server IP	FTP サーバの IP アドレスを入力します。 • 「IPv4」- FTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- FTP サーバの IPv6 アドレスを入力します。
TCP Port	FTP 接続に使用する TCP ポート番号を指定します。 • 設定可能範囲：1-65535
User Name	FTP 接続に使用するユーザ名（32 文字以内）を指定します。
Password	FTP 接続に使用するパスワード（15 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	スイッチに保存されている証明書 / 鍵ファイルのパスとファイル名を入力します。（64 文字以内）
Destination File	証明書 / 鍵ファイルがバックアップされる FTP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

Public Key Backup to RCP（RCP を使用した公開鍵バックアップ）

RCP サーバへの公開鍵バックアップを実行します。

Tools > Certificate & Key Restore & Backup > Public Key Backup to RCP をクリックし、設定画面を表示します。

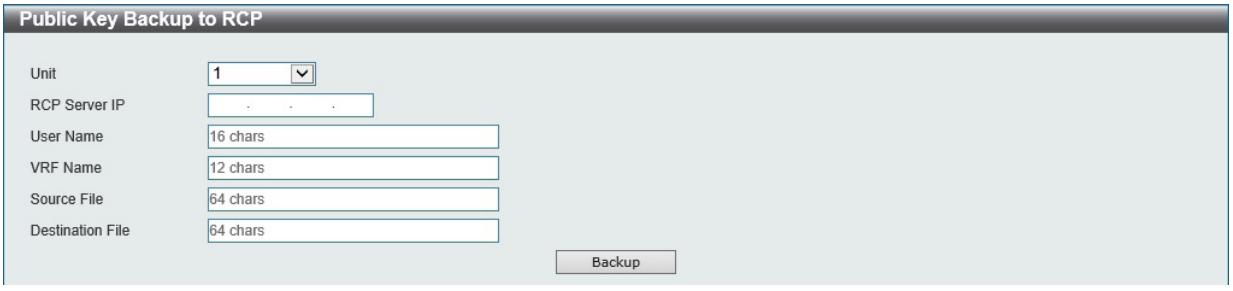


図 19-25　Public Key Backup to RCP 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを選択します。
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（16 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Source File	スイッチに保存されている証明書 / 鍵ファイルのパスとファイル名を入力します。（64 文字以内）
Destination File	証明書 / 鍵ファイルがバックアップされる RCP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「Backup」ボタンをクリックして、バックアップを開始します。

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。

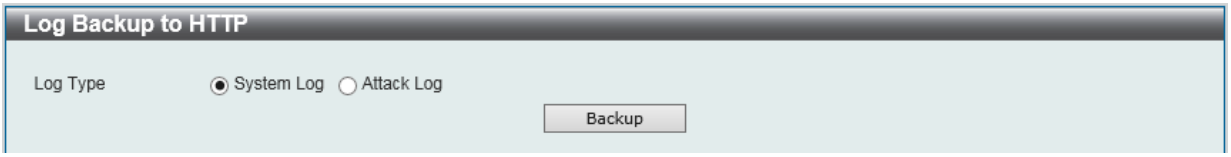


図 19-26　Log Backup to HTTP 画面

画面に表示される項目：

項目	説明
Log Type	HTTP を使用してローカル PC にバックアップするログの種類を選択します。 • 「System Log」- システムログをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「Backup」ボタンをクリックして、バックアップを開始します。

Log Backup to TFTP（TFTP サーバを使用したログファイルのバックアップ）

TFTP サーバへのシステムログのバックアップを行います。

Tools > Log Backup > Log Backup to TFTP をクリックし、設定画面を表示します。

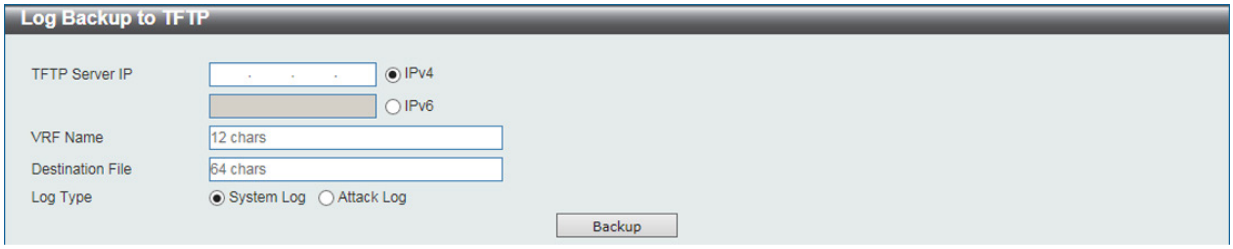


図 19-27　Log Backup to TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Destination File	ログファイルが保存される TFTP サーバの場所を指定します。（64 文字以内）
Log Type	バックアップするログの種類を選択します。 • 「System Log」- システムログエントリをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「Backup」ボタンをクリックして、バックアップを開始します。

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。

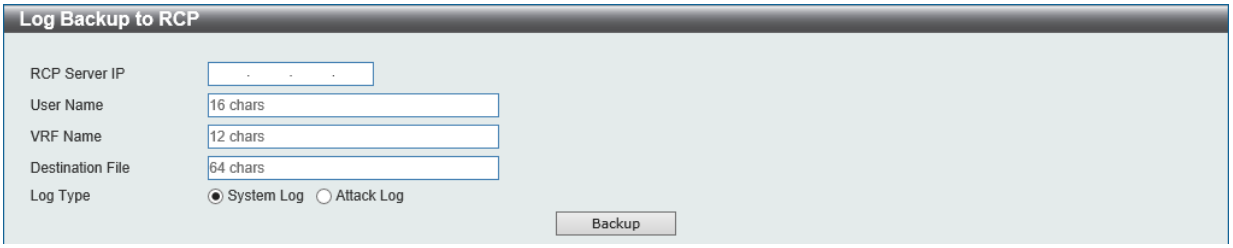


図 19-28　Log Backup to RCP 画面

画面に表示される項目：

項目	説明
RCP Server IP	RCP サーバの IP アドレスを入力します。
User Name	RCP 接続に使用するユーザ名（16 文字以内）を指定します。
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Destination File	ログファイルが保存される RCP サーバの場所を指定します。（64 文字以内）
Log Type	バックアップするログの種類を選択します。 • 「System Log」- システムログエントリをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「Backup」ボタンをクリックして、バックアップを開始します。

Ping

「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。宛先の機器はスイッチから送信された "echoes" に応答します。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。

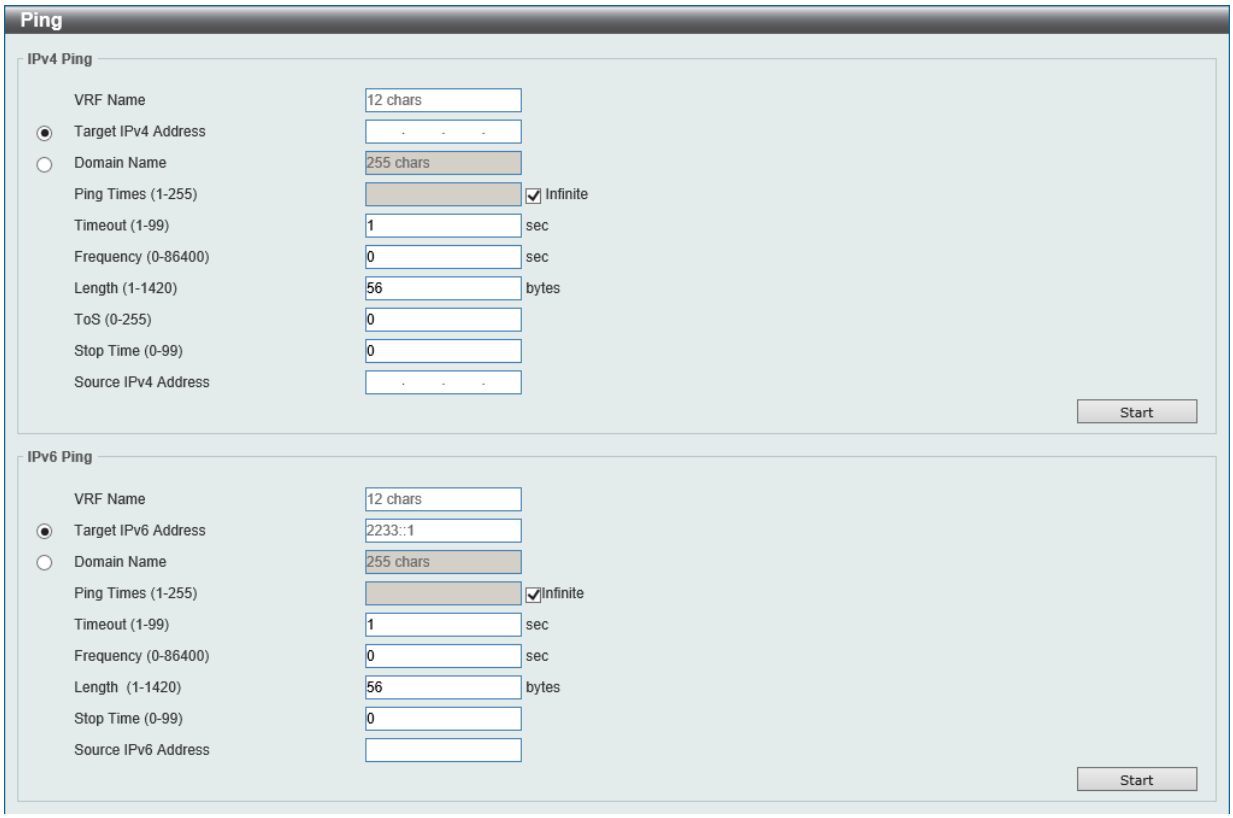


図 19-29　Ping 画面

画面に表示される項目：

項目	説明
IPv4 Ping	
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Target IPv4 Address	Ping の送信先となる IPv4 アドレスを入力します。
Domain Name	検出するシステムのドメイン名を入力します。
Ping Times	Ping の試行回数を入力します。「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。 • 設定可能範囲：1-255
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。 • 設定可能範囲：1-99（秒）
Frequency	Ping 頻度を指定します。 • 設定可能範囲：0-86400（秒）
Length	Ping 長を指定します。送信データバイト数になります。初期値の 56 バイトに ICMP ヘッダデータの 8 バイトが組み合わさると、64 バイトの ICMP データになります。VLAN（IEEE 802.1Q）タグ長は含まれません。 • 設定可能範囲：1-1420（Bytes） • 初期値：56（Bytes）
ToS	ToS 値を指定します。ICMP データグラムの QoS として使用されます。 • 設定可能範囲：0-255
Stop Time	停止回数を指定します。指定の Ping 回数を過ぎると Ping が停止します。「0」に指定した場合、「Stop」をクリックするまで Ping が実行されます。自動的には停止しません。 • 設定可能範囲：0-99
Source IPv4 Address	送信元 IPv4 アドレスを入力します。スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。入力した IPv4 アドレスは、リモートホストに送信されるパケットの送信元 IP アドレスまたはプライマリ IP アドレスとして使用されます。

項目	説明
IPv6 Ping	
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
Target IPv6 Address	Ping する IPv6 アドレスを入力します。
Domain Name	検出するシステムのドメイン名を入力します。
Ping Times	Ping の試行回数を入力します。「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。 • 設定可能範囲：1-255
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。 • 設定可能範囲：1-99（秒）
Frequency	Ping 頻度を指定します。 • 設定可能範囲：0-86400
Length	Ping 長を指定します。送信データバイト数になります。初期値の 56 バイトに ICMP ヘッダデータの 8 バイトが組み合わさると、64 バイトの ICMP データになります。VLAN（IEEE 802.1Q）タグ長は含まれません。 • 設定可能範囲：1-1420（Bytes） • 初期値：56（Bytes）
Stop Time	停止回数を指定します。指定の Ping 回数を過ぎると Ping が停止します。「0」に指定した場合、「Stop」をクリックするまで Ping が実行されます。自動的には停止しません。 • 設定可能範囲：0-99
Source IPv6 Address	送信元 IPv6 アドレスを入力します。スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。入力した IPv6 アドレスは、リモートホストに送信されるパケットの送信元 IP アドレスまたはプライマリ IP アドレスとして使用されます。

「Start」ボタンをクリックして、各個別セクションでの Ping テストを実行します。

「IPv4 Ping」セクションで「Start」ボタンをクリックすると、以下の「IPv4 Ping Result」画面が表示されます。

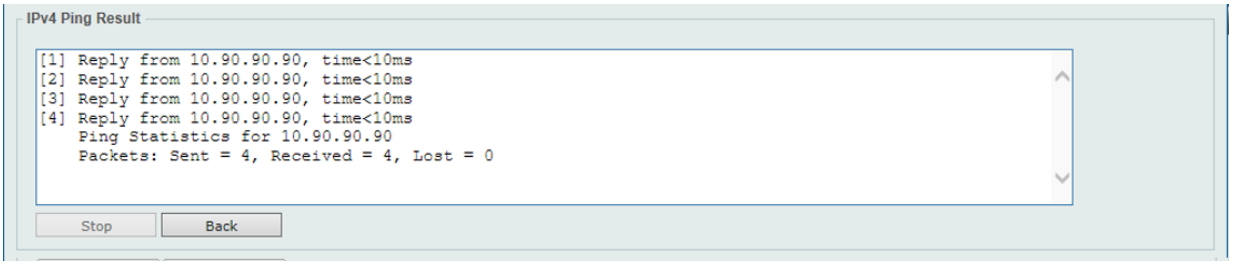


図 19-30　IPv4 Ping Result 画面

「IPv6 Ping」セクションで「Start」ボタンをクリックすると、以下の「IPv6 Ping Result」画面が表示されます。

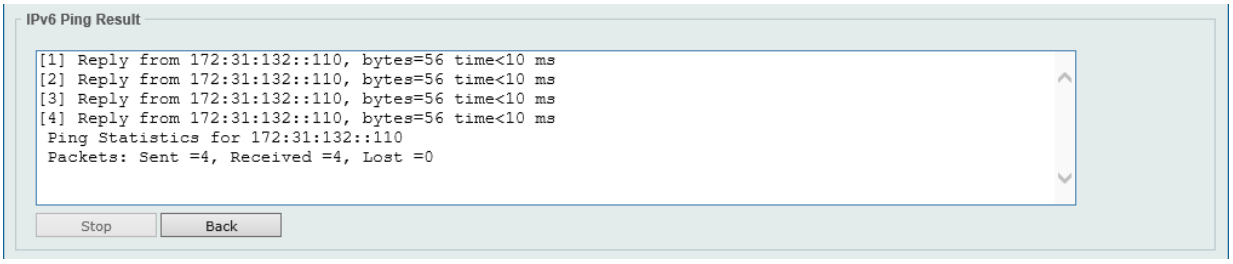


図 19-31　IPv6 Ping Result 画面

「Stop」ボタンをクリックして、Ping テストを停止します。
「Back」ボタンをクリックして、前の画面に戻ります。

Trace Route（トレースルート）

ネットワークとホスト間のルートをトレースします。

Tools > Trace Route の順にメニューをクリックし、以下の画面を表示します。

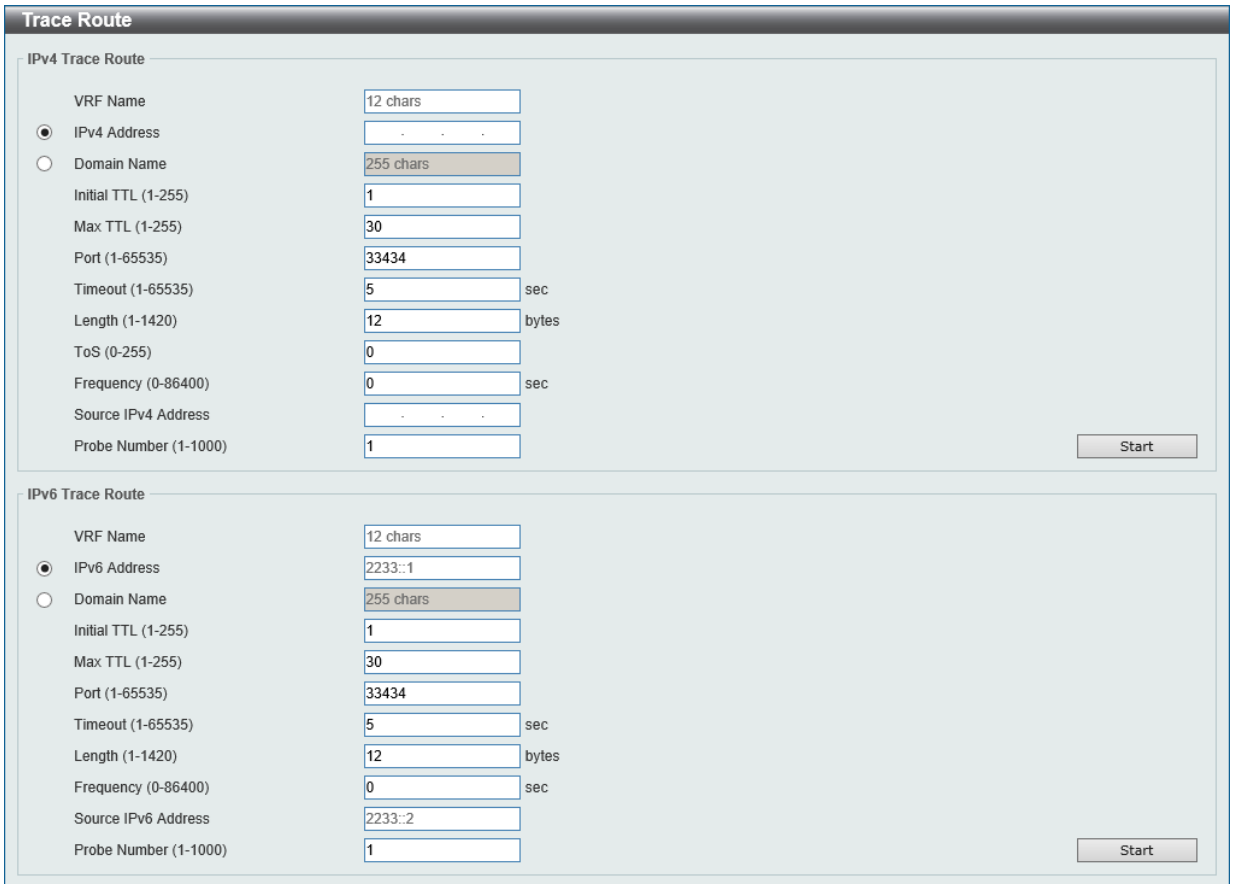


図 19-32　Trace Route 画面

画面に表示される項目：

項目	説明
IPv4 Trace Route	
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
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	初期 TTL（Time-To-Live）値を入力します。 • 設定可能範囲：1-255
Max TTL	トレースルートリクエストの Time-To-Live (TTL) 値を入力します。トレースルートパケットが通過できるルータの最大数となります。2 台のデバイス間でネットワークパスを検出する際に、このトレースルートオプションを使用します。 • 設定可能範囲：1-255
Port	ポート番号を指定します。 • 設定可能範囲：1-65535
Timeout	リモートデバイスからのレスポンスを待機する時間を指定します。この時間を過ぎるとタイムアウトになります。 • 設定可能範囲：1-65535（秒） • 初期値：5（秒）
Length	送信データグラムのバイト数を指定します。 • 設定可能範囲：1-1420（Bytes）
ToS	ToS 値を指定します。送信データグラムの IP ヘッダにセットされる値です。 • 設定可能範囲：0-255
Frequency	トレースルートの頻度を指定します。 • 設定可能範囲：0-86400（秒）
Source IPv4 Address	送信元 IPv4 アドレスを入力します。スイッチに設定された IPv4 アドレスのいずれかを指定します。
Probe Number	プローブ数を指定します。 • 設定可能範囲：1-1000 • 初期値：1

項目	説明
IPv6 Trace Route	
VRF Name（EI モードのみ）	VRF インスタンス名（12 文字以内）を入力します。
IPv6 Address	宛先 IPv6 アドレスを入力します。
Domain Name	宛先のドメイン名を入力します。
Initial TTL	初期 TTL（Time-To-Live）値を入力します。 • 設定可能範囲：1-255
Max TTL	トレースルートリクエストの Time-To-Live (TTL) 値を入力します。トレースルートパケットが通過できるルータの最大数となります。2 台のデバイス間でネットワークパスを検出する際に、このトレースルートオプションを使用します。 • 設定可能範囲：1-255
Port	ポート番号を指定します。 • 設定可能範囲：1-65535
Timeout	リモートデバイスからのレスポンスを待機する時間を指定します。この時間を過ぎるとタイムアウトになります。 • 設定可能範囲：1-65535（秒）
Length	送信データグラムのバイト数を指定します。 • 設定可能範囲：1-1420（Bytes）
Frequency	トレースルートの頻度を指定します。 • 設定可能範囲：0-86400
Source IPv6 Address	送信元 IPv6 アドレスを入力します。スイッチに設定された IPv6 アドレスのいずれかを指定します。
Probe Number	プローブ数を指定します。 • 設定可能範囲：1-1000 • 初期値：1

「Start」ボタンをクリックし、Traceroute プログラムを開始します。

以下の結果画面が表示されます。

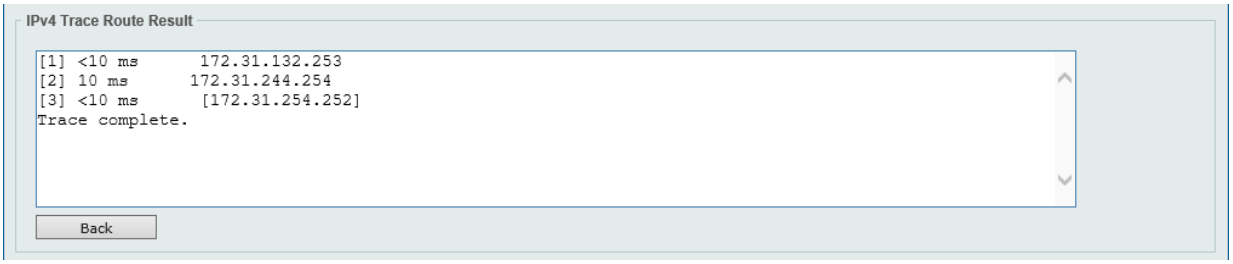


図 19-33　IPv4 Trace Route Result 画面

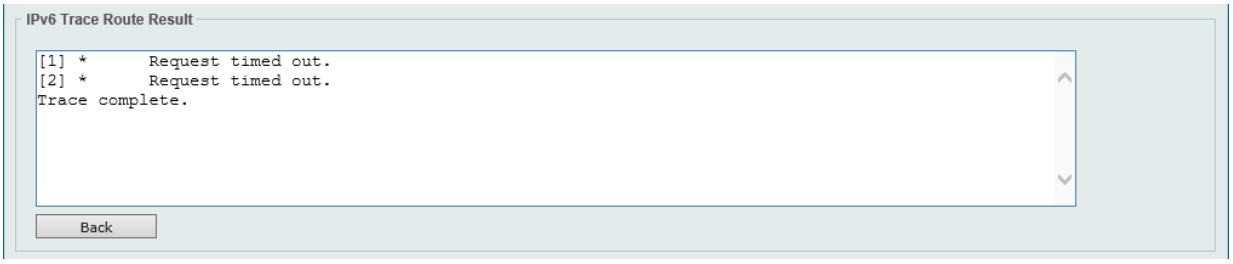


図 19-34　IPv6 Trace Route Result 画面

「Back」ボタンをクリックして、前の画面に戻ります。

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。

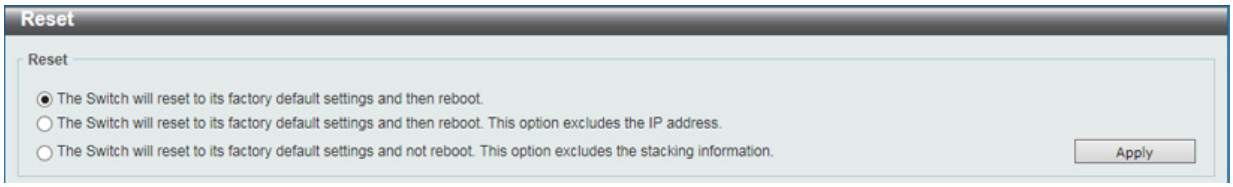


図 19-35　Reset 画面

画面に表示される項目：

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 System をクリックし、以下の設定画面を表示します。

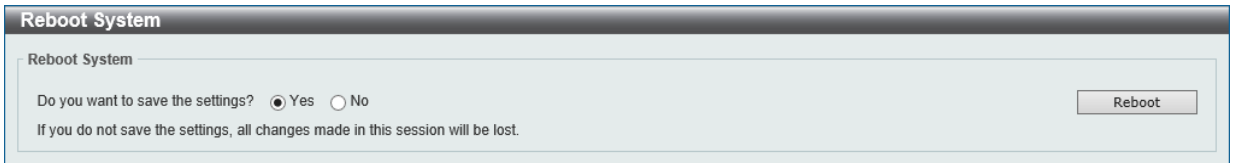


図 19-36　Reboot System 画面

画面に表示される項目：

項目	説明
Do you want to save the settings?	再起動オプションを指定します。 • 「Yes」- スイッチは再起動する前に現在の設定を保存します。 • 「No」- スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使用されます。

「Reboot」ボタンをクリックして、再起動を開始します。

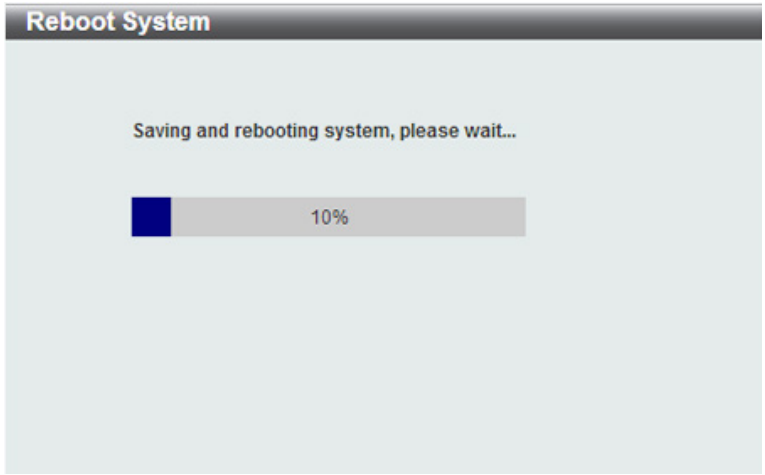


図 19-37　System Rebooting 画面

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。
ライセンスの種類により、スイッチで利用できる機能が異なります。ライセンスキーは購入する必要があります。物理的なパッケージに印刷されているか、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。（ライセンスキーではなく）適切なアクティベーションコードをインストールし、機能のアクティブ化 / ロックを行います。アクティベーションコードが正常にインストールされたら、スイッチを再起動してライセンスをアクティブ化します。

Tools > DLMS Settings をクリックし、次の設定画面を表示します。



図 19-38　DLMS Settings 画面

画面に表示される項目：

項目	説明
Unit	本設定を適用するユニットを指定します。
DLMS Activation Code	DLMS アクティベーションコード（25 文字以内）を指定します。

「Apply」ボタンをクリックして、設定内容を適用します。

付録

付録 A パスワードリカバリ手順

本スイッチシリーズのパスワードのリセット手順について説明します。

ネットワークにアクセスを試みるすべてのユーザに対し、認証を行うことが必要かつ重要です。権限のあるユーザを受け入れるために使用される基本的な認証方法は、ユーザ名とパスワードを使用したローカルログイン認証です。ネットワーク管理者は、パスワードを忘れた場合や破棄された場合などに、パスワードのリセットを行う必要があります。

本セクションでは、スイッチのパスワードリカバリ機能を使用して、パスワードを簡単に復旧する方法について説明します。
パスワードをリセットするには、次の手順を実行します。

1. セキュリティの理由により、パスワードリカバリ機能では物理的にデバイスにアクセスする必要があります。したがって、本機能は、デバイスのコンソールポートへ直接接続している場合にのみ利用することができます。本スイッチのコンソールポートに、端末または端末エミュレーションを搭載した PC を接続する必要があります。
2. スイッチの電源をオンにします。パスワードリカバリモードに入るためには、「UART init」が 100% までロードされた後 2 秒以内に、ホットキー「 ^ 」を押します。「Password Recovery Mode」に入ると、スイッチのすべてのポートが無効になります。

```
Boot Procedure                                          V1.00.007
-------------------------------------------------------------------------------

Power On Self Test ..................................... 100 %

MAC Address    : 80-26-89-15-28-00
H/W Version    : A1

Please Wait, Loading 1.00.026 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	実行中の設定を工場出荷時の設定に戻し、スイッチを再起動します。
show running-config	実行中の設定を表示します。
show username	ローカルユーザアカウント情報を表示します。

付録 B システムログエントリ

スイッチのシステムログに出力されるログイベントとそれらの意味を以下に示します。

Critical（重大）、Warning（警告）、Informational（報告）、Notice（通知）

ログの内容	緊急度	イベントの説明
802.1X		
802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) **パラメータ説明：** • reason: 認証失敗の理由 • username：認証されるユーザ名 • interface-id：インタフェース名 • mac-address：認証されるデバイスの 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-address：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。
802.1X cannot work correctly because ACL rule resource is not available	Alert	ACL ハードウェアの枯渇により 802.1X 認証を実行できません。
AAA		
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。
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	リモートサーバが認証リクエストに応答しません。

ログの内容	緊急度	イベントの説明
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。
RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface -id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • direction:：帯域幅制御の方向（例：ingress または egress.） • threshold: サーバから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 priority: <priority> to port < interface -id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • priority：RADIUS サーバから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。

ログの内容	緊急度	イベントの説明
User <username> locked out on authentication failure **パラメータ説明：** • username：ロックアウトされたユーザ名	Notification	ローカルユーザがロックアウトされました。
User <username> unlocked. **パラメータ説明：** • username：ロックが解除されたユーザ名	Notification	ローカルユーザのロックが解除されました。
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：デバイスと重複する IP アドレス • macaddr：重複する IP アドレスを持つデバイスの MAC アドレス • unitID：ユニット番号 • portNum：ポート番号 • ipif_name：重複する IP アドレスを持つスイッチの IP インタフェース名	Warning	Gratuitous ARP は重複した IP を検出しました。
Auto image		
The downloaded firmware was successfully executed by DHCP Auto image update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：TFTP サーバの IP アドレス	Informational	DHCP 自動イメージによるファームウェア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：TFTP サーバの IP アドレス	Informational	DHCP 自動イメージによるファームウェア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：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	DDP の設定情報が自動で保存されました。
Auto Surveillance VLAN		
New surveillance device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface–id：インタフェース名 • mac-address：監視デバイスの MAC アドレス	Informational	インタフェースで新しい監視デバイスが検出されました。
<interface-id> add into surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名 • vid：VLAN ID	Informational	サーベイランス VLAN が有効のインタフェースが自動的にサーベイランス VLAN に追加されました。
<interface-id> remove from surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名 • vid：VLAN ID	Informational	インタフェースがサーベイランス VLAN から離脱し、エージング期間内に当該インタフェースに監視デバイスが検出されませんでした。ログメッセージが出力されました。
BGP		
[BGP(1):] BGP connection is successfully established (Peer:<ipaddr>) **パラメータ説明：** • ipaddr：BGP ピアの IP アドレス	Informational	ピアとの BGP FSM の構築に成功しました。

ログの内容	緊急度	イベントの説明
[BGP(2):] BGP connection is normally closed(Peer:<ipaddr>) **パラメータ説明：** • ipaddr：BGP ピアの IP アドレス	Informational	BGP 接続が正常に閉じました。
[BGP(3):] BGP connection is closed due to error (Code:<num> Sub-code:<num> Field:<field> Peer:<ipaddr>) **パラメータ説明：** • num：RFC4271 で定義されたエラーコード / サブコード • filed：エラー発生場所 • ipaddr：BGP ピアの 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、データフィールドは RFC 参照）
[BGP(4):] BGP Notify: unknown Error code(num), Sub Error code(num), Peer:<ipaddr> **パラメータ説明：** • num：RFC4271 で定義されたエラーコード / サブコード • ipaddr：BGP ピアの IP アドレス	Warning	RFC4271 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(5):] BGP Update Attr NHop: Erroneous NHop <ipaddr> Peer:<ipaddr> **パラメータ説明：** • ipaddr：BGP ピアの IP アドレス	Warning	BGP アップデートパケットを受信しましたが、ネクストホップがローカルインタフェースです。
[BGP(6):] 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：BGP ピアの 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 参照）
[BGP(7):] BGP connection is closed due to Notify: Code <num> Sub-code <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：BGP ピアの IP アドレス	Warning	通知パケットの受信による BGP 接続の切断（エラーコード / エラーサブコードは RFC 参照）
[BGP(8):] The number of prefix received reaches <num>, max <limit> (Peer <ipaddr>) **パラメータ説明：** • num：受信したプレフィックス番号 • limit：受信可能なプレフィックスの最大値 • ipaddr：BGP ピアの IP アドレス	Informational	ネイバから受信した BGP のプレフィックスが最大しきい値に到達しました。
[BGP(9):] The total number of prefix received reaches max prefix limit	Informational	受信 BGP プレフィックスの総数が上限を超えました。
[BGP(10):] 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(11):] 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(12):] 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」または「AS_CONFED_SET」パスセグメントタイプを受信しました。
[BGP(13):] 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。

ログの内容	緊急度	イベントの説明
[BGP(14):] 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「AGGREGATOR」属性を受信しました。
BPDU Protection		
<interface-id> enter STP BPDU under protection state (mode: <mode>) **パラメータ説明：** • interface–id：STP BPDU アタックが検出されたインタフェース • mode：インタフェースの BPDU プロテクションモード（drop, block, shutdown）	Informational	BPDU アタックが発生しました。
<interface-id> recover from BPDU under protection state **パラメータ説明：** • interface–id：STP BPDU アタックが検出されたインタフェース	Informational	STP BPDU 攻撃から回復しました。
CFM		
CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース • mepdirection：MEP の方向。（「inward」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。	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。	Warning	エラー CFM CCM パケットが検出されました。
CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) **パラメータ説明：** • vlanid：MEP の VLAN ID • mdlevel：MEP の MD レベル • interface-id：MEP のインタフェース • mepdirection：MEP の方向。（「inward」または「outward」）	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」）	Warning	リモート MEP の MAC がエラー状態です。

ログの内容	緊急度	イベントの説明
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」）	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
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

ログの内容	緊急度	イベントの説明
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。
[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。

ログの内容	緊急度	イベントの説明
[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。
[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>,]Configuration saved to flash by console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のログインユーザ名	Informational	コンソール上でコンフィグレーションがフラッシュに保存されました。
[Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • unitID：ユニット ID • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	リモートでコンフィグレーションがフラッシュに保存されました。
[Unit <unitID>,] Log message uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) **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	Informational	ログメッセージのアップロードが成功しました。

ログの内容	緊急度	イベントの説明
[Unit <unitID>,] Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) **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	Warning	ログメッセージのアップロードが失敗しました。
[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。
• ユーザのセッションは Console、Web、SNMP、Telnet、SSH のいずれかです。 • スイッチがスタンドアロン状態の場合、ユイット ID はログ出力されません。 • コンソール経由でのコンフィグレーション / ファームウェアの更新では、IP や MAC 情報はログ出力されません。		
DAD		
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 が重複アドレスを含む「Neighbor Solicitation」(NS) メッセージを受信しました。
Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages **パラメータ説明：** • ipv6address：NA メッセージの IPv6 アドレス • interface-id：ポートインタフェース ID	Warning	DAD の間に DUT が重複アドレスを含む「Neighbor Advertisement」(NA) メッセージを受信しました。
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いずれかです。 - temperature - supply voltage - bias current - TX power - RX power • high-low：High または Low	Warning	SFP パラメータのいずれが警告しきい値を超えました。

ログの内容	緊急度	イベントの説明
Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded **パラメータ説明：** • interface-id：ポートインタフェース ID • component：DDM のしきい値タイプ。しきい値タイプは以下のいずれかです。 - temperature - supply voltage - bias current - TX power - RX power • high-low：High または Low	Critical	SFP パラメータのいずれかがアラームしきい値を超えました。
Optical transceiver <interface-id> <component> back to normal **パラメータ説明：** • interface-id：ポートインタフェース ID • component：DDM のしきい値タイプ。しきい値タイプは以下のいずれかです。 - temperature - supply voltage - bias current - TX power - RX power	Warning	SFP パラメータのいずれかが警告しきい値から回復しました。
DHCPv6 Client		
DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] **パラメータ説明：** • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 クライアントインタフェース管理者ステートが変更されました。
DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name> **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 クライアントが DHCPv6 サーバから ipv6 アドレスを取得しました。
The IPv6 address <ipv6address> on interface <ipif-name> starts renewing **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得した IPv6 アドレスが更新を開始します。
The IPv6 address <ipv6address> on interface <ipif-name> renews success **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスの更新に成功しました。
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。
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。

ログの内容	緊急度	イベントの説明
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。
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不正です。
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。

ログの内容	緊急度	イベントの説明
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。
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。
DNS Resolver		
Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> **パラメータ説明：** • domainname：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	ポートで単一方向リンクを検出しました。
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 リクエストまたは応答を示します。 • 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 リクエストまたは応答を示します。 • 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	「Manual Switch」が発行されました。

ログの内容	緊急度	イベントの説明
Signal fail detected on node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	シグナル失敗が検出されました。
Signal fail cleared on node(MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	シグナル失敗が解消されました。
Force Switch is issued on node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	「Force Switch」が発行されました。
Clear command is issued on node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	「Clear」コマンドが発行されました。
RPL owner conflicted on the node (MAC: <macaddr>, instance <InstanceID>) **パラメータ説明：** • mac-address：MAC アドレス • InstanceID：インスタンス ID	Warning	RPL オーナが競合しています。
ErrDisable		
Port <interface-id> enters error disable state due to <reason-id> **パラメータ説明：** • interface-id：ポート番号 • reason-id：「Loopback Detection」「Port Security Violation」「Storm Control」「BPDU Protect」「ARP Rate Limit」「DHCP Rate Limit」「L2 Protocol Tunneling」「Digital Diagnostics Monitoring」「Scheduled Port-shutdown by Power Saving」「Scheduled Hibernation by Power Saving」「D-LINK Unidirectional Link Detection」	Warning	ポートがエラーディセーブル状態に移行しました。
Port <interface-id> leaves the error disable state which is previously caused by <reason-id> **パラメータ説明：** • interface-id：ポート番号 • reason-id：「Loopback Detection」「Port Security Violation」「Storm Control」「BPDU Protect」「ARP Rate Limit」「DHCP Rate Limit」「L2 Protocol Tunneling」「Scheduled Port-shutdown by Power Saving」「Scheduled Hibernation by Power Saving」「D-LINK Unidirectional Link Detection」	Warning	ポートがエラーディセーブル状態から元の状態に戻りました。
Port <interface-id> VLAN <vid> enters error disable state due to <reason-id> **パラメータ説明：** • interface-id：ポート番号 • reason-id：「Loopback Detection」「Port Security Violation」「Storm Control」「BPDU Protect」「L2 Protocol Tunneling」「Scheduled Port-shutdown by Power Saving」「Scheduled Hibernation by Power Saving」 • vid：VLAN ID	Warning	ポートがエラーディセーブル状態に移行しました。

ログの内容	緊急度	イベントの説明
Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id> **パラメータ説明：** • interface-id：ポート番号 • reason-id：「Loopback Detection」「Port Security Violation」「Storm Control」「BPDU Protect」「L2 Protocol Tunneling」「Scheduled Port-shutdown by Power Saving」「Scheduled Hibernation by Power Saving」 • vid：VLAN ID	Warning	ポートがエラーディセーブル状態から元の状態に戻りました。
Ethernet OAM		
OAM dying gasp event received (Port<interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートで「Dying gasp」イベントが発生しました。
Device encountered an OAM dying gasp event	Warning	ローカルで「Dying gasp」イベントが発生しました。
OAM critical event received (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでクリティカルなイベントが発生しました。
Device encountered an OAM critical event (Port <interface-id>, <condition>) **パラメータ説明：** • interface-id：インタフェース ID • condition：クリティカル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	ローカルでクリティカルなイベントが発生しました。
Error symbol period event received (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでエラーシンボル期間イベントが発生しました。
Error frame event received(Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでエラーフレームイベントが発生しました。
Error frame period event received(Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでエラーフレーム期間イベントが発生しました。
Error frame seconds summary event received (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートでエラーフレーム秒サマリイベントが発生しました。
OAM Remote loopback started (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートループバックが開始しました。
OAM Remote loopback stopped (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	リモートループバックが停止しました。
Device encountered an error symbol period event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	ローカルでエラーシンボル期間イベントが発生しました。
Device encountered an error frame event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	ローカルでエラーフレームイベントが発生しました。

ログの内容	緊急度	イベントの説明
Device encountered an error frame period event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	ローカルでエラーフレーム期間イベントが発生しました。
Device encountered an error frame seconds summary event (Port <interface-id>) **パラメータ説明：** • interface-id：インタフェース ID	Warning	ローカルでエラーフレーム秒サマリイベントが発生しました。
Interface		
<interface-id> link up, <link state> **パラメータ説明：** • interface-id：インタフェース ID • 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。
<interface-id> link down **パラメータ説明：** • interface-id：インタフェース ID	Informational	ポートがリンクダウンしました。
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	特定サブネットにおいて IP ダイレクトブロードキャストレートが毎秒 50 パケットを超えました。
IP Directed Broadcast rate is high.	Informational	IP ダイレクトブロードキャストレートが毎秒 100 パケットを超えました。
IP Source Guard（IPSG）		
Failed to set IPSG entry due to no hardware rule resource. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>) **パラメータ説明：** • IPADDR：IP アドレス • MACADDR：MAC アドレス • VLANID：VLAN ID • INTERFACE-ID：インタフェース ID	Warning	ハードウェアルールのリソースが枯渇しているため、DHCP スヌーピングエントリを ISPG テーブルにセットできません。
IPv6 Source Guard		
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：** • IPADDR：IP アドレス • MACADDR：MAC アドレス • VLANID：VLAN ID • INTERFACE-ID：インタフェース ID	Warning	ハードウェアルールのリソースが枯渇しているため、IPv6SG エントリを ISPG テーブルにセットできません。
LACP		
Link Aggregation Group <group-id> link up **パラメータ説明：** • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクアップします。
Link Aggregation Group <group-id> link down **パラメータ説明：** • group-id：リンクダウン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：ポートがアタッチするアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループにアタッチします。

ログの内容	緊急度	イベントの説明
<ifname> detach from Link Aggregation Group <group-id> **パラメータ説明：** • ifname：アグリゲーショングループからデタッチするポートのインタフェース名 • group-id：ポートがデタッチする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）		
<interface-id> LBD loop occurred **パラメータ説明：** • interface-id：ループが検出されたインタフェース	Critical	ポートベースモードでループバックが検出されました。
<interface-id> VLAN <vlan-id> LBD loop occurred **パラメータ説明：** • interface-id：ループが検出されたインタフェース • vlan-id：ループが検出された VLAN ID	Critical	VLAN ベースモードでループバックが検出されました。
<interface-id> LBD loop recovered **パラメータ説明：** • interface-id：ループが検出されたインタフェース	Critical	ポートベースモードでループバックから回復しました。
<interface-id> VLAN <vlan-id> LBD loop recovered **パラメータ説明：** • interface-id：ループが検出されたインタフェース • vlan-id：ループが検出された VLAN ID	Critical	VLAN ベースモードでループバックからポートが回復しました。
Loop VLAN numbers overflow	Critical	ループバックが発生した VLAN の数が予約数に達しました。
LLDP-MED		
LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notice	LLDP-MED トポロジの変更が検出されました。

ログの内容	緊急度	イベントの説明
Conflict LLDP-MED device type detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notice	LLDP-MED デバイスタイプの重複が検出されました。
Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notice	LLDP-MED TLV の非互換性が検出されました。

ログの内容	緊急度	イベントの説明
Login/Logout CLI		
[Unit <unitID>,]Successful login through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のログインユーザ名	Informational	コンソール経由のログインに成功しました。
[Unit <unitID>,] Login failed through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のログインユーザ名	Warning	コンソール経由のログインに失敗しました。
[Unit <unitID>,] Console session timed out (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のログインユーザ名	Informational	コンソールのセッションはタイムアウトしました。
[Unit <unitID>,] Logout through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のログインユーザ名	Informational	コンソール経由でログアウトしました。
Successful login through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由のログインに成功しました。
Login failed through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス • 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>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	Telnet のセッションはタイムアウトしました。
Logout through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由でログアウトしました。
Successful login through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	SSH 経由のログインに成功しました。
Login failed through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Critical	SSH 経由のログインに失敗しました。
SSH session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	SSH のセッションはタイムアウトしました。

ログの内容	緊急度	イベントの説明
Logout through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	SSH 経由でログアウトしました。
MAC-based Access Control（MAC 認証）		
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上限数に達しました。
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一定期間、上限数を下回りました。
<interface-id> enters MAC-based Access Control stop learning state **パラメータ説明：** • interface-id：ホストが認証されたインタフェース	Warning	インタフェースで認証されたユーザ数が上限数に達しました。
<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一定期間、上限数を下回りました。
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. version is different：MLAG バージョンがピアデバイスと異なります。 2. domain is different：ドメインがピアデバイスと異なります。 3. device id is same：デバイス ID がピアスイッチと同じです。 4. hello interval is different：hello 間隔がピアスイッチと異なります。 5. MLAG found third device：3 つ目のデバイスが MLAG に接続されました。 6. 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。 7. device id is not set：MLAG デバイスが設定されていません。	Informational	MLAG 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モードが異なります。 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：確立された LSP ID	Informational	LSP がアップしました。
LSP <lsp-id> is down **パラメータ説明：** • lsp-id：削除された LSP ID	Informational	LSP がダウンしました。
MSTP Debug		
Topology changed [([Instance:<InstanceID>],port:<portNum>,MAC: <macaddr>)] **パラメータ説明：** • InstanceID：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：** • InstanceID：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
New root port selected [([Instance:<InstanceID>], port:<portNum>)] **パラメータ説明：** • InstanceID：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。

ログの内容	緊急度	イベントの説明
Spanning Tree port status change [([Instance:<InstanceID>], port:<portNum>)] <old-status> -> <new-status> **パラメータ説明：** • InstanceID：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>], port:<[portNum>)] <old-role> -> <new-role> **パラメータ説明：** • InstanceID：インスタンス ID • portNum：ポート番号 • old-role：旧ロール • new-role：新ロール	Informational	スパニングツリーポートのロールが変更されました。
Spanning Tree instance create. Instance:<InstanceID> **パラメータ説明：** • InstanceID：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 delete. Instance:<InstanceID> **パラメータ説明：** • InstanceID：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：新しい名前 • revision-level：新しいリビジョンレベル	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: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • InstanceID：インスタンス ID • startvlanid：削除される VLAN 範囲の開始 VID • endvlanid：削除される 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：** • InstanceID：インスタンス ID • startvlanid：追加される VLAN 範囲の開始 VID • endvlanid：追加される 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。
Spanning Tree port role change (Instance: <InstanceID>, <portNum>) to alternate port due to the guard root **パラメータ説明：** • InstanceID：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：** • InstanceID：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。

ログの内容	緊急度	イベントの説明
OpenFlow		
<connection-type> session is successfully connected with the controller <ipaddr>:<port> **パラメータ説明：** • connection-type：TCP または TLS 接続 • ipaddr：コントローラの IP アドレス • port：L4 ポート番号	Informational	OpenFlow コントローラとの間で TCP/TLS セッションが正常に確立しました。
<connection-type> session is disconnected from the controller <ipaddr>:<port> **パラメータ説明：** • connection-type：TCP または TLS 接続 • ipaddr：コントローラの IP アドレス • port：L4 ポート番号	Informational	OpenFlow コントローラとの間で TCP/TLS セッションが切断されました。
Flow entry (cookie is <cookie>) setting <set-type> from the controller is failed **パラメータ説明：** • cookie：フローインストール時にコントローラによって指定されるクッキー • set-type：フローエントリ設定 - OFPFC_ADD - OFPFC_MODIFY - OFPFC_MODIFY_STRICT - OFPFC_DELETE - OFPFC_DELETE_STRICT	Error	コントローラからのフロー設定が失敗しました。
Flow entry cookie <cookie> is deleted by controller <ipaddr>:<port> **パラメータ説明：** • cookie：フローインストール時にコントローラによって指定されるクッキー • ipaddr：コントローラの IP アドレス • port：L4 ポート番号	Warning	log will be generated when the flow entry is deleted by controller コントローラによってフローエントリが削除されました。
Flow entry cookie <cookie> is deleted because of <delete-reason> **パラメータ説明：** • cookie：フローインストール時にコントローラによって指定されるクッキー • delete-reason：フローエントリ削除の理由。<duration> はタイムアウト値を示します。 - "idle timeout (<duration> seconds)" - "hard timeout (<duration> seconds)" - "FLOW_MOD request" - "overwrite"	Warning	アイドルタイム / ハードタイムアウトの期限切れ、Flow-Mod リクエスト、上書きによってフローエントリが削除されました。
An error <error-type> occurs with the controller <ipaddr> **パラメータ説明：** • error-type：スイッチとコントローラ間で発生したエラーの種類 - OFPET_BAD_REQUEST - OFPET_FLOW_MOD_FAILED - OFPET_GROUP_MOD_FAILED - OFPET_ROLE_REQUEST_FAILE - OFPET_METER_MOD_FAILED • ipaddr：コントローラの IP アドレス	Error	コントローラからのフロー設定が失敗しました。
OSPFv2		
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。

ログの内容	緊急度	イベントの説明
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。
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。
OSPF state changed to Enabled	Informational	OSPF 有効化
OSPF state changed to Disabled	Informational	OSPF 無効化
Peripheral		
Unit <id> Back Fan <id> back to normal **パラメータ説明：** • Fan <id>：ファン ID • Unit <id>：ユニット ID	Critical	ファンが回復しました。
Unit <id> Back Fan <id> failed **パラメータ説明：** • Fan <id>：ファン ID • Unit <id>：ユニット ID	Critical	ファンの故障
[Unit <unitID>] Sensor: <sensorID> detects abnormal temperature <temperature_value> **パラメータ説明：** • unitID：ユニット ID • sensorID：センサ ID • temperature_value：現在のセンサ温度	Critical	温度センサが異常を検知しました。

ログの内容	緊急度	イベントの説明
[Unit <unitID>] sensor: <sensorID> temperature back to normal **パラメータ説明：** • unitID：ユニット ID • sensorID：センサ ID	Critical	温度が通常に戻りました。
Unit <unitID>, Power <powerID> failed **パラメータ説明：** • unitID：ユニット ID • powerID：電源 ID	Critical	電源故障
Unit <unitID>, Power <powerID> empty **パラメータ説明：** • unitID：ユニット ID • powerID：電源 ID	Critical	電源モジュールが切断されました。
Unit <unitID> Power <powerID> back to normal **パラメータ説明：** • unitID：ユニット ID • powerID：電源 ID	Critical	電源回復
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上限に達しました。
Limit on system entry number has been exceeded	Warning	システム上のアドレスが上限に達しました。
PTP		
PTP port <interface-id> role changed to <ptp-role> **パラメータ説明：** • interface-id：スイッチのインタフェース ID • ptp-role：変更後の PTP ロール - INITIALIZING - FAULTY - DISABLED - LISTENING - PRE_MASTER - MASTER - PASSIVE - UNCALIBRATED - SLAVE.	Informational	特定ポートの PTP ロールが変更されました。
The boundary clock synchronized to its master, the offset value is <offset> second(s) **パラメータ説明：** • offset：スレーブ / マスタ間のオフセット値	Informational	境界クロックがマスタと同期されました。
Reboot Schedule		
Reboot scheduled in 5 minutes	Warning	5 分以内に再起動します。
Reboot scheduled in 1 minute	Critical	1 分以内に再起動します。
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	スイッチは「exhausted」モードに移行します。

ログの内容	緊急度	イベントの説明
Unit <unit-id>, Safeguard Engine enters NORMAL mode **パラメータ説明：** • unit-id：ユニット ID	Informational	スイッチはノーマルモードに移行します。
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文字列を受信しました。
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異なる SRM モードのスレーブが検出されました。
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：ボックス 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：ボックス ID • macaddr：MAC アドレス ID	Informational	デバイスが削除されました。
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：重複するボックスの 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

ログの内容	緊急度	イベントの説明
System		
[Unit <unitID>,]System warm start **パラメータ説明：** • unitID：ユニット ID スイッチがスタンドアロンモードの場合、ユニット ID は含まれません。	Critical	システムがウォームスタートしました。
[Unit <unitID>,]System cold start **パラメータ説明：** • unitID：ユニット ID スイッチがスタンドアロンモードの場合、ユニット ID は含まれません。	Critical	システムがコールドスタートしました。
[Unit <unitID>,]System started up. **パラメータ説明：** • unitID：ユニット ID スイッチがスタンドアロンモードの場合、ユニット ID は含まれません。	Critical	システムが起動しました。
Telnet		
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
TFTP Client		
[TFTP(1):] Unit <unitID>, Firmware upgraded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **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 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Informational	ファームウェアのアップグレードが成功しました。
[TFTP(2):] Unit <unitID>, Firmware upgraded by <session> unsuccessfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **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 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	warning	ファームウェアのアップグレードが失敗しました。

ログの内容	緊急度	イベントの説明
[TFTP(3):] Unit <unitID>, Firmware uploaded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **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 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Informational	ファームウェアのアップロードが成功しました。
[TFTP(4):] Unit <unitID>, Firmware uploaded by <session> unsuccessfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **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 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	warning	ファームウェアのアップロードが失敗しました。
[TFTP(5):] Unit <unitID>, Configuration downloaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **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 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Informational	コンフィグレーションのダウンロードが成功しました。
[TFTP(6):] Unit <unitID>, Configuration downloaded by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **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 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	warning	コンフィグレーションのダウンロードが失敗しました。
[TFTP(7):] Unit <unitID>, Configuration uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **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 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Informational	コンフィグレーションのアップロードが成功しました。
[TFTP(8):] Unit <unitID>, Configuration uploaded by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **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 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	warning	コンフィグレーションのアップロードが失敗しました。

ログの内容	緊急度	イベントの説明
[TFTP(9):]Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Informational	ログメッセージのアップロードが成功しました。
[TFTP(10):]Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	warning	ログメッセージのアップロードが失敗しました。
• ユーザのセッションは Console、Web、SNMP、Telnet、SSH のいずれかです。 • コンソール経由でのファームウェアの更新では、IP や MAC 情報はログ出力されません。 • SNMP 経由でのファームウェアの更新では、ユーザ名はログ出力されません。		
Traffic 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）によりストーム発生 • Multicast：マルチキャストパケットによりストームが発生（不明 / 既知の L2 マルチキャスト、不明 / 既知の IP マルチキャストを含む） • Unicast：ユニキャストパケットによりストーム発生（不明 / 既知のユニキャストパケットを含む） • interface-id：ストームが発生したインタフェース ID	Warning	ブロードキャストストームが発生
<Broadcast | Multicast | Unicast> storm is cleared on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストストームが解消しました。 • Multicast：マルチキャストストームが解消しました。 • Unicast：ユニキャストストームが解消しました。 • interface-id：ストームが解消したインタフェース ID	Informational	ブロードキャストストームが解消
<interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm **パラメータ説明：** • interface-id：ストームにより error-disabled 状態のインタフェース ID • Broadcast：インタフェースはブロードキャストストームにより無効です。 • Multicast：インタフェースはマルチキャストストームにより無効です。 • Unicast：インタフェースはユニキャストストームにより無効です。	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
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：音声デバイスの MAC アドレス	Informational	インタフェースで音声デバイスが検出されました。
<interface-id> add into voice VLAN <vid> **パラメータ説明：** • interface-id：インタフェース ID • vid：VLAN ID	Informational	自動音声 VLAN モードのインタフェースが音声 VLAN に追加されました。

ログの内容	緊急度	イベントの説明
<interface-id> remove from voice VLAN <vid> **パラメータ説明：** • interface-id：インタフェース ID • vid：VLAN ID	Informational	インタフェースが音声 VLAN から離脱し、エージング期間内に音声デバイスがインタフェースで検出されませんでした。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		
Pseudo-wire ID <vc-id> peer ip <ipaddr> link down **パラメータ説明：** • vc-id：pseudowire ID • ipaddr：リンクダウン pseudo-wire のピア IP アドレス	Informational	Pseudowire がリンクダウン
Pseudo-wire id <vc-id> peer ip <ipaddr> link up **パラメータ説明：** • vc-id：pseudowire ID • ipaddr：リンクアップ pseudo-wire のピア IP アドレス	Informational	Pseudowire がリンクアップ
Pseudo-wire id <vc-id> peer ip <ipaddr> is deleted **パラメータ説明：** • vc-id：削除された pseudowire ID • ipaddr：削除された pseudo-wire のピア IP アドレス	Informational	Pseudowire が削除
Pseudo-wire id <vc-id> peer ip <ipaddr> link standby **パラメータ説明：** • vc-id：pseudowire ID • ipaddr：リンクスタンバイ pseudo-wire のピア IP アドレス	Informational	Pseudowire リンクがスタンドバイ
VRRP Debug		
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	仮想ルータがマスタに移行しました。
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	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	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。

ログの内容	緊急度	イベントの説明
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。
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。

ログの内容	緊急度	イベントの説明
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 アドレスがベースにしているインタフェース	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 アドレスのスタックボックス ID	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。
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。
Web		
Successful login through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP サーバへのログインに使用されるユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web 経由でのログインに成功しました。
Login failed through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP サーバへのログインに使用されるユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Warning	Web 経由でのログインに失敗しました。
Web session timed out (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP サーバへのログインに使用されるユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web セッションがタイムアウトしました。
Logout through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP サーバへのログインに使用されるユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web 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 Web (SSL) (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：HTTPS サーバへのログインに使用されるユーザ名 • ipaddr：HTTPS クライアントの IP アドレス	Informational	Web（SSL）経由でのログインに成功しました。
Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTPS サーバへのログインに使用されるユーザ名 • ipaddr：HTTPS クライアントの IP アドレス	Warning	Web（SSL）経由でのログインに失敗しました。
Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTPS サーバへのログインに使用されるユーザ名 • ipaddr：HTTPS クライアントの IP アドレス	Informational	Web（SSL）セッションがタイムアウトしました。
Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTPS サーバへのログインに使用されるユーザ名 • ipaddr：HTTPS クライアントの IP アドレス	Informational	Web（SSL）経由でログアウトしました。
Web Authentication		
Web-Authentication host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, Port: <interface-id>, VID: <vlan-id>) **パラメータ説明：** • string：ホストのユーザ名 • ipaddr：ホストの IP アドレス • ipv6address：ホストの IPv6 アドレス • 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	クライアントホストが認証に成功しました。
Web-Authentication host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, Port: <interface-id>, VID: <vlan-id>) **パラメータ説明：** • string：ホストのユーザ名 • ipaddr：ホストの IP アドレス • ipv6address：ホストの IPv6 アドレス • mac-address：ホストの MAC アドレス • interface-id：ホストが認証されるインタフェース • vlan-id：ホストが存在する VLAN ID	Critical	クライアントホストが認証に失敗しました。
Web-Authentication enters stop learning state	Warning	デバイス全体において認証ユーザ数が最大値に達しました。
Web-Authentication recovers from stop learning state	Warning	デバイス全体において認証ユーザ数が一定期間最大値を下回りました。
Web-Authentication cannot work correctly because ACL rule resource is not available	Alert	ハードウェア ACL リソースが不足しています。

付録 C トラップログエントリ

スイッチのトラップログエントリとその説明を以下に示します。

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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	エージェントロールで動作する SNMPv2 エントリが、正しく認証されていないプロトコルメッセージを受信したことを示します。SNMPv2 の実装ではこのトラップを生成できることを規定していますが、このトラップが生成されるかどうかは snmpEnableAuthenTraps オブジェクトにより指定されます。	1.3.6.1.6.3.1.1.5.5
BPDU 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 14.47.0.2

カテゴリ	トラップ名	説明	OID
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
	swCFMExtAISOccurred	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) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171. 14.86.0.1
	swCFMExtAISCleared	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) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171. 14.86.0.2
	swCFMExtLockOccurred	ローカル MEP がロックステータスになった場合、生成されます。 関連オブジェクト : (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171. 14.86.0.3
	swCFMExtLockCleared	ローカル MEP のロックステータスが解除された場合、生成されます。 関連オブジェクト : (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171. 14.86.0.4
DDM	dDdmAlarmTrap	異常なアラームが発生、または正常な状態に回復した際に通知されます。現在の値 > low warning または現在の値 < high warning になったときにのみリカバトラップを送信します。 関連オブジェクト : (1) dDdmNotifyInfoIfIndex (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 14.133.0.1
DoS 防止	dDosPreveAttackDetectedPacket	DoS アタックを検出したときに送信されます。 関連オブジェクト : (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171. 14.59.0.2

カテゴリ	トラップ名	説明	OID
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
Gratuitous ARP	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	1.3.6.1.4.1.171.14.75.0.1
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	1.3.6.1.4.1.171.14.22.0.1
LACP	linkUp	「linkUp」トラップは、エージェントロールで動作している SNMP エンティティにより、コミュニケーションリンクの 1 つにおいて、ifOperStatus が「down」ステートから他のステート（「notPresent」以外）に移行したことを検出した場合に送信されます。移行後のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
	linkDown	「linkDown」トラップは、エージェントロールで動作している SNMP エンティティにより、コミュニケーションリンクの 1 つにおいて、ifOperStatus が他のステート（「notPresent」以外）から「down」ステートに移行しようとしていることを検出した場合に送信されます。移行前のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

カテゴリ	トラップ名	説明	OID
LBD	dLbdLoopOccurred	インタフェースにループが発生したときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171. 14.46.0.1
	dLbdLoopRestart	指定時間後、インタフェースのループが再スタートしたときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171. 14.46.0.2
	dLbdVlanLoopOccurred	インタフェースに VID ループが発生したときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171. 14.46.0.3
	dLbdVlanLoopRestart	指定時間後、VID のインタフェースループが再スタートしたときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171. 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)」ステートから離脱した際に送信されます。	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	1.0.8802. 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	1.3.6.1.4.1.171.14.153.0.1
	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	1.3.6.1.4.1.171.14.153.0.2
	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	1.3.6.1.4.1.171.14.153.0.3
MAC Notification	swL2macNotification	本トラップはアドレステーブルの MAC アドレスに変更が生じたことを意味します。 関連オブジェクト : (1) swL2macNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
	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	1.3.6.1.4.1.171.14.3.0.2
MPLS	mplsXCUp	「mplsXCTable」のエントリの「mplsXCOperStatus」オブジェクトが、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	「mplsXCTable」のエントリの「mplsXCOperStatus」オブジェクトが、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（Topology Change Timer の期限切れなどに伴い）すぐにブリッジによって送信されます。 本トラップの実装はオプションです。	1.3.6.1.2.1.17.0.1
	topologyChange	topologyChange トラップは、いずれかの構成ポートが Learning 状態から Forwarding 状態に、または Forwarding 状態から Blocking 状態に遷移する場合にブリッジによって送信されます。同様の変更に対して newRoot トラップが送信される場合には、本トラップは送信されません。 本トラップの実装はオプションです。	1.3.6.1.2.1.17.0.2

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」が「fault」）または回復（「dEntityExtEnvFanStatus」が「ok」）） 関連オブジェクト： (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.171. 14.5.1
	dEntityExtThermalStatusChg	温度状態の変更通知 （温度警告（「dEntityExtEnvTempStatus」が「abnormal ）または回復（「dEntityExtEnvTempStatus」が「ok)） 関連オブジェクト： (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.171. 14.5.2
	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	1.3.6.1.4.1.171. 14.5.3

カテゴリ	トラップ名	説明	OID
PIM6-SM	pimNeighborLoss	「pimNeighborLoss」通知は、ネイバとの隣接関係を失った際に送信されます。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「pimNieghborLossNotificationsPeriod」によってレートリミットが指定されている場合、カウンタ「pimNeighborLossCount」が増加するときにも起動します。 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「pimInvalidRegisterNotificationPeriod」によってレートリミットが指定されている場合、カウンタ「pimInvalidRegisterMsgsRcvd」が増加するときにも起動します。 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「pimInvalidJoinPruneNotificationPeriod」によってレートリミットが指定されている場合、カウンタ「pimInvalidJoinPruneMsgsRcvd」が増加するときにも起動します。 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」通知はデバイスでアクティブな RP マッピングに変更があった場合に起動します。 本通知は「pimRPMappingChangeNotificationPeriod」によってレートリミットが指定されている場合、カウンタ「pimRPMappingChangeCount」が増加するときにも起動します。 関連オブジェクト : (1) pimGroupMappingPimMode (2) pimGroupMappingPrecedence	1.3.6.1.2.1.157.0.4
	pimInterfaceElection	「pimInterfaceElection」通知はネットワークで新しい DR または DF が選出された場合に起動します。 本通知は「pimInterfaceElectionNotificationPeriod」によってレートリミットが指定されている場合、カウンタ「pimInterfaceElectionWinCount」が増加するときにも起動します。 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
Port	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) ifOperStatus	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) ifOperStatus	1.3.6.1.6.3.1 1.5.3
Port Security	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 アドレスがトリガとなり送信されるトラップメッセージです。 関連オブジェクト : (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.171. 14.8.0.1
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
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、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) alarmFallingThreshold	1.3.6.1.2.1.16.0.2
Safeguard	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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 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	1.3.6.1.4.1.171. 12.8.6.0.17

カテゴリ	トラップ名	説明	OID
Stack	dStackInsertNotification	ユニットのホットインサート（活線挿入）の通知です。 関連オブジェクト： (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.1
	dStackRemoveNotification	ユニットのホットリムーブ（活線抜出）の通知です。 関連オブジェクト： (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.2
	dStackFailureNotification	ユニットのスタック失敗の通知です。 関連オブジェクト： (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	coldStart	coldStart トラップは、エージェントロールで動作する SNMPv2 エンティティが、自身を再初期化したことを示します。設定が変更された可能性があります。	1.3.6.1.6.3.1.1.5.1
	warmStart	warmStart トラップは、エージェントロールで動作する SNMPv2 エンティティが、自身を再初期化したことを示します。設定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	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	1.3.6.1.4.1.171.14.25.0.1
	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	1.3.6.1.4.1.171.14.25.0.2
System File	dsfUploadImage	イメージファイルのアップロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.1
	dsfDownloadImage	イメージファイルのダウンロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.2
	dsfUploadCfg	コンフィグレーションファイルのアップロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.3
	dsfDownloadCfg	コンフィグレーションファイルのダウンロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.4
	dsfSaveCfg	コンフィグレーションファイルの保存に成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.5

カテゴリ	トラップ名	説明	OID
VRRP	vrrpTrapNewMaster	送信エージェントが「Master」ステートに変更された場合、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
Web Authentication	dWebAuthLoggedSuccess	クライアントが Web 認証をパスしてログインに成功したときに送信されます。 関連オブジェクト : (1) ifIndex (2) dnaSessionAuthVlan (3) dnaSessionClientMacAddress (4) dnaSessionClientAddrType (5) dnaSessionClientAddress (6) dnaSessionAuthUserName	1.3.6.1.4.1.171.14.154.0.1
	dWebAuthLoggedFail	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) ifIndex (2) dnaSessionAuthVlan (3) dnaSessionClientMacAddress (4) dnaSessionClientAddrType (5) dnaSessionClientAddress (6) dnaSessionAuthUserName	1.3.6.1.4.1.17 1.14.154.0.2

付録 D RADIUS 属性割り当て

本スイッチでは次のモジュールに対し、RADIUS 属性割り当てが使用されます。
- 「コンソール」「Telnet」「SSH」「Web」「802.1X」「MAC ベースアクセスコントロール」「WAC」

以下の RADIUS 属性割り当てタイプについて説明します。
- 特権レベル
- イングレス / イーグレス帯域幅
- 802.1p デフォルトプライオリティ
- VLAN
- ACL

■ 特権レベル

RADIUS サーバで特権レベルを割り当てるには、適切なパラメータが RADIUS サーバで設定されている必要があります。特権レベルのパラメータは以下の通りです。

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	1	必須
Attribute-Specific Field	スイッチを操作するユーザの特権レベルの割り当てに使用します。	範囲（1-15）	必須

ユーザが RADIUS サーバの特権レベル属性（例えば、レベル 15）を設定し、コンソール、Telnet、SSH、Web 認証が成功した場合、デバイスは、このアクセスユーザに（RADIUS サーバに基づく）特権レベルを割り当てます。ユーザが特権レベル属性を設定せず、認証に成功した場合、デバイスはアクセスユーザに特権レベルを割り当てません。特権レベルが最小サポート値よりも小さい場合、または最大サポート値よりも大きい場合、特権レベルは無視されます。

■ イングレス / イーグレス帯域幅

RADIUS サーバにより Ingress/Egress 帯域を割り当てるには、適切なパラメータが RADIUS サーバに設定されている必要があります。帯域幅のパラメータは以下の通りです。

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	2（イングレス帯域幅） 3（イーグレス帯域幅）	必須
Attribute-Specific Field	ポートの帯域幅の割り当てに使用します。	ユニット (Kbits)	必須

ユーザが RADIUS サーバの帯域属性（例えば、イングレス帯域 1000Kbps）を設定し、802.1X 認証に成功した場合、デバイスはポートへ（RADIUS サーバに基づく）帯域を割り当てます。ユーザが帯域属性を設定せず、認証に成功した場合、デバイスはポートに帯域を割り当てません。RADIUS サーバ上で帯域属性が "0" の値で設定されている場合、実効的な帯域は、"no_limited" に設定されます、また、帯域が "0" より小さい場合、または最大サポート値よりも大きい場合、帯域は無視されます。

■ 802.1p デフォルトプライオリティ

RADIUS サーバにより 802.1p デフォルトプライオリティを割り当てるには、適切なパラメータが RADIUS サーバに設定されている必要があります。802.1p デフォルトプライオリティのパラメータは以下の通りです。

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	4	必須
Attribute-Specific Field	802.1p デフォルトプライオリティの割り当てに使用します。	0-7	必須

ユーザは、RADIUS サーバの 802.1p デフォルトプライオリティ（例えば、優先度 7）を設定し、802.1X 認証や MAC ベース認証に成功した場合、デバイスはポートに（RADIUS サーバに基づく）802.1p デフォルトプライオリティを割り当てます。ユーザがプライオリティ属性を設定せず、認証が成功した場合、デバイスはこのポートにプライオリティを割り当てません。RADIUS サーバで設定されたプライオリティ属性が、範囲外の値（7 よりも大きい値）である場合、デバイスに設定しません。

■ VLAN

RADIUS サーバにより VLAN を割り当てるには、適切なパラメータが RADIUS サーバに設定されている必要があります。VLAN 割り当てを使用するために、RADIUS パケット内の以下のトンネル属性が RFC3580 により定義されています。

VLAN のパラメータ

RADIUS トンネル属性	説明	値	使用法
Tunnel-Type	この属性は、（トンネルイニシエータの場合）使用されるトンネリングプロトコル、もしくは、（トンネルターミネータの場合）使用中のトンネリングプロトコルを示します。	13 (VLAN)	必須
Tunnel-Medium-Type	使用されるトランスポートミディアムタイプ	6（802）	必須
Tunnel-Private-Group-ID	特定のトンネルセッションのグループ ID	String 値（VID）	必須

トンネルプライベートグループ ID 属性形式の概要

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Length     |     Tag       |  String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

タグフィールドの定義（RFC 2868 と異なる）

タグフィールド値	文字列のフィールド形式
0x01	VLAN 名（ASCII）
0x02	VLAN ID（ASCII）
その他 (0x00, 0x03 ~ 0x1F, >0x1F)	スイッチが VLAN 設定の文字列を受信すると、最初に VLAN ID と認識します。つまり、スイッチはすべての既存 VLAN ID を確認し、一致するものがあるかどうかを確認します。一致するものを検出できた場合はその VLAN に移動し、検出できなかった場合は VLAN 設定文字列を VLAN 名と判断し、一致する VLAN 名を検出します。

注意 0x1F より大きなタグフィールドは次に続くフィールドの初めのオクテットとして判断されます。

ユーザが RADIUS サーバの VLAN 属性（VID3 など）を設定し、802.1X、MAC ベースアクセスコントロール、または WAC 認証に成功した場合、ポートは VLAN3 が割り当てられます。ユーザが VLAN 属性を設定していない場合、ポートがゲスト VLAN メンバではないときは、現在の認証 VLAN にとどまり、ポートがゲスト VLAN メンバであるときは、元々の VLAN に割り当てられます。

■ ACL

RADIUS サーバで ACL を割り当てるには、適切なパラメータが RADIUS サーバで設定されている必要があります。ACL のパラメータは以下の通りです。

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	14 (ACL スクリプト)	必須
Attribute-Specific Field	ACL スクリプトの割り当てに使用します。 形式は Access Control List (ACL) コマンドに基づきます。	ACL スクリプト 例： ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;	必須

ユーザが RADIUS サーバの ACL 属性を設定（例：ACL スクリプト：ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;）し、802.1X、MAC ベースアクセスコントロール、または WAC に成功した場合、デバイスは RADIUS サーバによる ACL スクリプトを割り当てます。アクセスリストコンフィグモードへの移行 / 終了は対になっている必要があります。そのように設定されていない場合、ACL スクリプトは拒否されます。

付録 E IETF RADIUS 属性サポート

リモート認証ダイヤルインユーザサービス（RADIUS）属性を使用すると、リクエストや応答の中で認証、承認、情報、設定詳細などをやり取りすることができます。

本付録では、スイッチによりサポートされる RADIUS 属性一覧を記載しています。

RADIUS 属性は、IETF 規格やベンダ特定属性（VSA) によりサポートされます。VSA により、ベンダは固有の RADIUS 属性を定義することができます。D-Link VSA についての詳しい情報は、「付録 D RADIUS 属性割り当て」を参照してください。

IETF 規格 RADIUS 属性は、RFC2865 リモート認証ダイヤルインユーザサービス（RADIUS)、RFC2866 RADIUS アカウンティング、RFC2868 トンネルプロトコルに対する RADIUS 属性、RFC2869 RADIUS 拡張で定義されています。
以下のリストは、D-Link スイッチでサポートされている IETF RADIUS 属性です。

RADIUS 認証属性

ナンバー	IETF 属性
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

RADIUS アカウンティング属性

ナンバー	IETF 属性
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

付録 F 機能設定例

本項では、一般によく使う機能についての設定例を記載します。実際に設定を行う際の参考にしてください。

- Traffic Segmentation（トラフィックセグメンテーション）
- VLAN
- Link Aggregation（リンクアグリゲーション）
- Access List（アクセスリスト）
- Loopback Detection（LBD）（ループ検知）

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DXS-3610

Traffic Segmentation（トラフィックセグメンテーション）

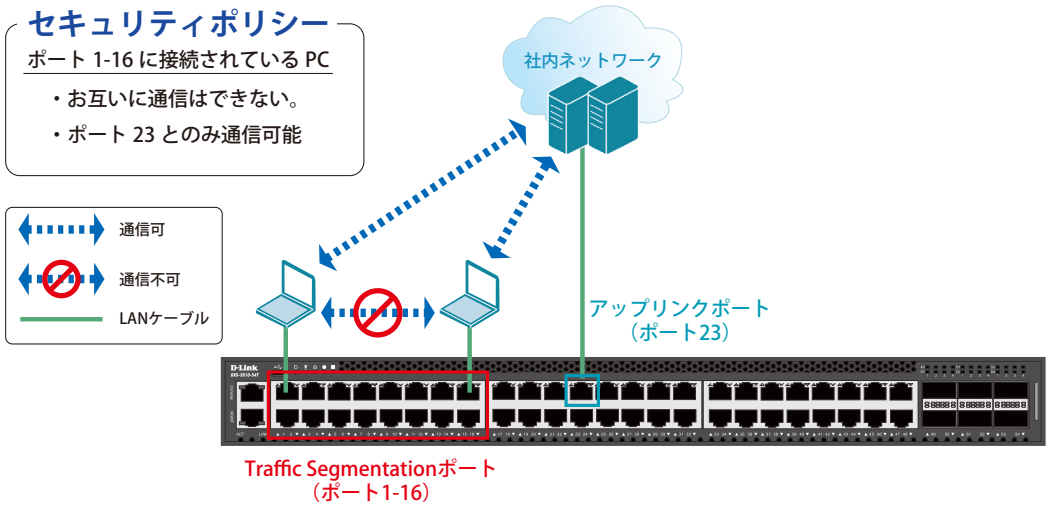


図 20-1　Traffic Segmentation（DXS-3610-54T）

概要

ポート 1 ～ 16 に対し、トラフィックセグメンテーションを設定します。1 ～ 16 のポート間ではお互いに通信ができないようにし、ポート 1 ～ 16 は、アップリンクポートとして使用するポート 23 とのみ通信ができるようにします。

設定手順

1. ポート（1-16）のトラフィックセグメンテーション設定を行います。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#traffic-segmentation forward interface ethernet 1/0/23
Switch(config-if-range)#end
```

2. 情報確認

```
Switch#show traffic-segmentation forward
```

注意　本機能を利用する場合、送信先 MAC アドレスが不明な Unknown ユニキャストについて、スイッチの全ポートにフラッドされます。

3. 設定を保存します。

```
Switch#copy running-config startup-config
```

VLAN

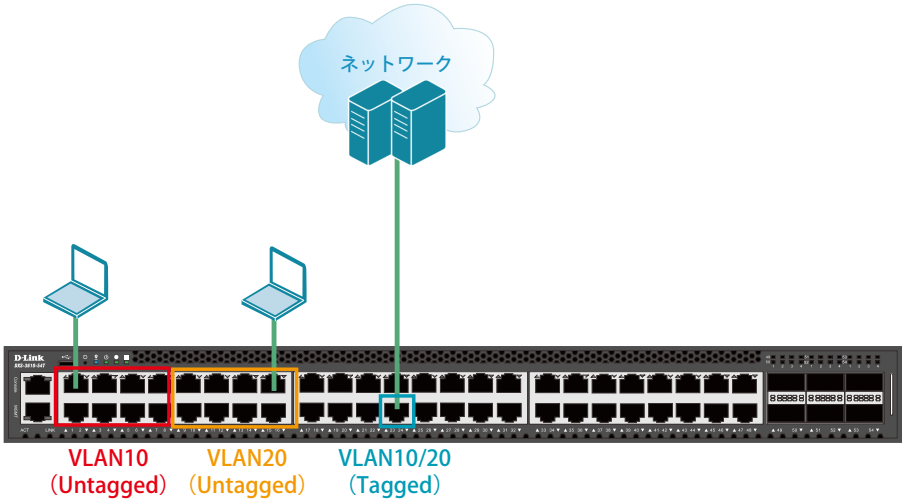


図 20-2　VLAN（DXS-3610-54T）

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）

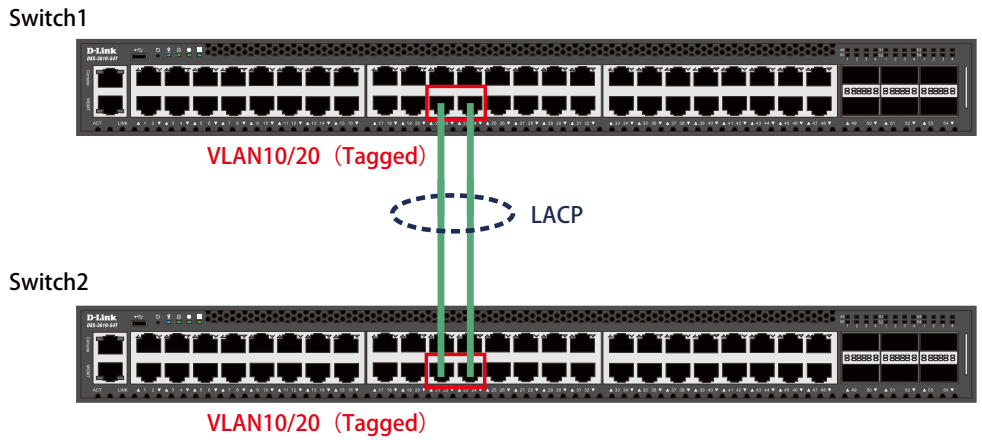


図 20-3　Link Aggregation（DXS-3610-54T）

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、各物理インタフェース上では設定せず、Port-channel インタフェース上で VLAN の設定を行います。

```
Switch(config)#interface port-channel 1
Switch(config if)#switchport mode trunk
Switch(config if)#switchport trunk native vlan 1
Switch(config if)#switchport trunk allowed vlan 1,10,20
Switch(config if)#exit
Switch(config)#exit
```

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）

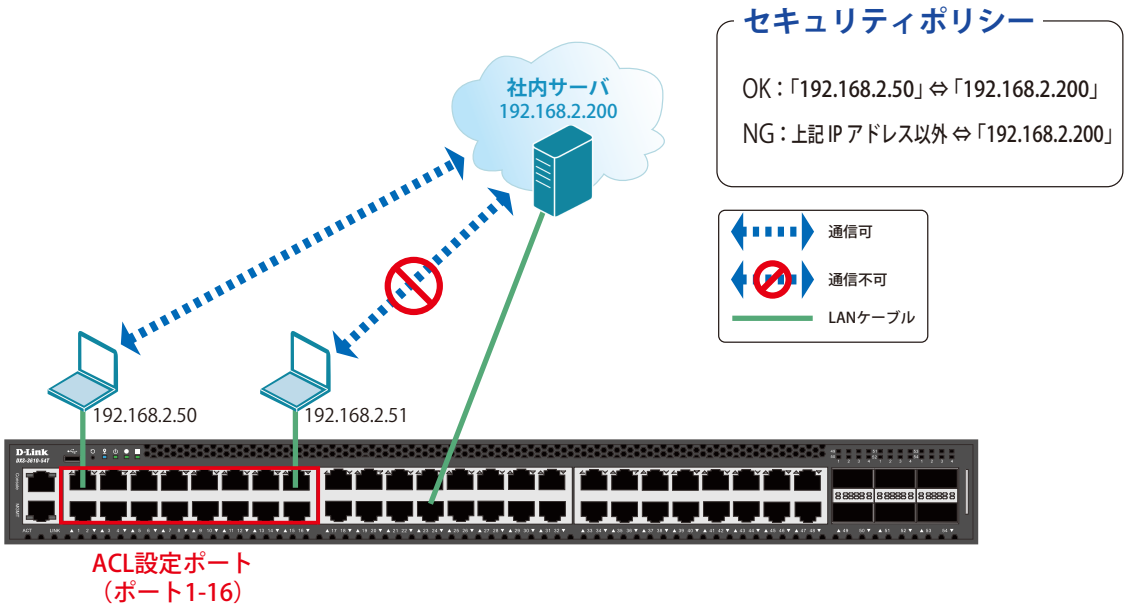


図 20-4　Access List（DXS-3610-54T）

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）

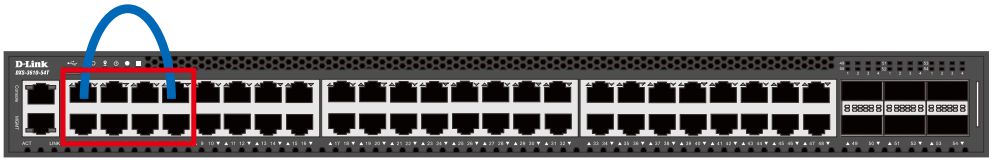


図 20-5　Loopback Detection（DXS-3610-54T）

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、インタフェースモードにて「no shutdown」コマンドを投入する必要があります。

4. ポート 1-8 でループバック検知機能を有効にします。

```
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#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、設定するインタフェースの「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、各インタフェースでは「enable」となっています。各インタフェースにて「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の有効 / 無効、確認間隔を表示します。）