D-Link DXS-1210-10TS/10MP/12TS/12SC

10 Gigabit Layer 2 Smart Managed Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

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

⃠ 禁止　ぬれた手でさわらない
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

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

VCCI - A

ご使用上の注意

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

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

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

計画停電前や電源設備に異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

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

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

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

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

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

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

目次

はじめに

DXS-1210 ユーザマニュアルは、本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　本製品のご利用にあたって
  - 本スイッチの概要と前面、背面、側面の各パネル、LED 表示について説明します。
- 第 2 章　スイッチの設置
  - システムの基本的な設置方法および電源接続の方法について紹介します。
- 第 3 章　スイッチの接続
  - スイッチをご使用のイーサネット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、IP アドレス割り当て、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（システム設定）
  - デバイス情報の確認、環境設定、ポートの設定、システムログの設定と管理、システム時刻の設定について説明します。
- 第 7 章　Management（スイッチの管理）
  - ユーザアカウント設定など、スイッチの管理について説明します。
- 第 8 章　L2 Features（レイヤ 2 機能の設定）
  - FDB 設定、VLAN 設定、スパニングツリーの設定、ループバック検知設定など L2 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、IPv4/IPv6 インタフェース、IPv4/IPv6 ルート設定などの L3 機能について説明します。
- 第 10 章　QoS（QoS 機能の設定）
  - QoS 機能について説明します。帯域制御、QoS スケジューリング、802.1p デフォルトプライオリティなどの機能を含みます。
- 第 11 章　ACL（ACL 機能の設定）
  - アクセスコントロールリスト（ACL）関連の設定について説明します。
- 第 12 章　Security（セキュリティ機能の設定）
  - ポートセキュリティ、802.1X 認証、AAA、RADIUS 設定などのセキュリティの設定について説明します。
- 第 13 章　OAM（Operations, Administration, Maintenance：運用・管理・保守）
  - ケーブル診断、DDM 機能について説明します。
- 第 14 章　Monitoring（スイッチのモニタリング）
  - 本スイッチのパケット統計、パケットエラーなどの情報について表示します。
- 第 15 章　Green（省電力テクノロジー）
  - 本スイッチの省電力について設定、表示します。
- 第 16 章　Toolbar（ツールバー）
  - Web インタフェース画面上部のツールバーにあるメニューを使用してスイッチの管理・設定を行います。また、設定の保存、再起動などスイッチのユーティリティ機能について説明します。
- 【付録 A】システムログエントリ
  - ログエントリとそれらの意味について説明します。
- 【付録 B】トラップログエントリ
  - トラップログとそれらの意味について説明します。
- 【付録 C】RADIUS 属性の割り当て指定
  - スイッチの RADIUS 属性の割り当てについて説明します。
- 【付録 D】IETF RADIUS 属性のサポート
  - 本スイッチがサポートする RADIUS 属性一覧です。
- 【付録 E】ERPS 情報
  - ERPS 情報ついて説明します。
- 【付録 F】機能設定例
  - 機能設定例ついて説明します。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、使用にあたっての注意事項について説明します。

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

補足 補足では、特長や技術についての詳細情報について説明します。

参照 参照では、別項目での説明へ誘導します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "（13 ページ）をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
courier 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
courier 斜体	コマンド項目（可変または固定）。	*value*
< >	可変項目。< > にあたる箇所に値または文字を入力します。	<*value*>
[ ]	任意の固定項目。	[*value*]
[< >]	任意の可変項目。	[<*value*>]
{ }	{ } 内の選択肢から 1 つ選択して入力する項目。	{*choice1* | *choice2*}
|（垂直線）	相互排他的な項目。	*choice1* | *choice2*
Menu Name > Menu Option	メニュー構造を示します。	Device > Port > Port Properties は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。

製品名 / 品番一覧

製品名	HW バージョン	品番
DXS-1210-10TS	B1	DXS-1210-10TS/B1
DXS-1210-10MP	B1	DXS-1210-10MP/B1
DXS-1210-12TC	B1	DXS-1210-12TC/B1
DXS-1210-12SC	B1	DXS-1210-12SC/B1

第 1 章　本製品のご利用にあたって

スイッチ概要

DXS-1210シリーズは、プラグアンドプレイのシンプルさと優れた価値、さらに中小企業（SMB）ネットワーキング向けの信頼性を兼ね備えています。本シリーズの筐体はラックマウント型の金属ケースで、前面パネルに各種ステータス LED が付いています。また、ネットワークセキュリティ、トラフィックセグメンテーション、QoS、多彩な管理機能など、高度な機能を提供します。

柔軟なポート設定
DXS-1210 シリーズでは、10GBASE-T × 8/10 ポート、または SFP+ × 12 ポートを搭載したモデルを提供します。本シリーズは、直感的で機能豊富なソフトウェアを有しており、見やすく簡素化された Web GUI を使用して、Web ブラウザを介してあらゆる場所からスイッチにアクセスし、設定可能です。10GBASE-T ポートは、Cat6/6A/7 の UTP または STP ツイストペアケーブルを使用すると、100/1000Mbps から 10Gbps に透過的にアップグレード可能な下位互換性を提供します。10G SFP+ スロットの利点は、消費電力が低く、長距離伝送に対応、レイテンシ性能が優れていることです。ダイレクトアタッチケーブル（DAC）を使用すると、近接スイッチ同士で 10Gbps 接続する際にコストを抑えることができます。

D-Link Green テクノロジ
D-Link Green 技術に対応した製品は、パフォーマンスを損なうことなく環境にやさしい省電力機能を使用することができます。LED オフ、ポートシャットダウン、システムスリープ、および EEE による省電力機能により、スイッチのエネルギー消費を削減することが可能です。

多様な 2 機能
本シリーズには、IGMP スヌーピング、ポートミラーリング、スパニングツリー、ERPS、802.3ad LACP、SNTP、LLDP、ループバック検出などの L2 スイッチとしての機能が実装されています。パフォーマンスとネットワークの信頼性を強化します。

レイヤ 3 機能
本シリーズには、IP インタフェース、スタティックルート、IPv6 スタティックルート、ARP などの L3 機能も含まれます。

QoS
本スイッチは帯域幅制御や 802.1p プライオリティキューをサポートしており、音声や動画などのデータ遅延に影響を受けやすいアプリケーションをネットワーク上で実行する場合にも最適なネットワーク設定が可能です。これらの機能は、VLAN、802.1p トラフィックとシームレスに機能し、ネットワーク上のトラフィックを優先することができます。

ネットワークセキュリティ
D-Link のセーフガードエンジン機能は、ウィルス攻撃によるトラフィックフラッディングからスイッチを保護します。ストームコントロールなどの追加機能は、異常なトラフィックによってネットワークが圧迫されないようにするのに役立ちます。ポートセキュリティは、ネットワークデバイスの整合性を維持するための、シンプルかつ便利な認証方法です。そのほか、DHCP サーバスクリーニング、SSL、IP-MAC ポートバインディング機能もサポートされています。

様々な管理機能
本シリーズは、Web ベースのシンプルで簡単な管理を提供します。管理者は管理インタフェースを使用して、リモートからポートレベルの設定・管理が可能です。また、コマンドラインインタフェース管理用に、RJ-45 コンソールポートが搭載されています。本デバイスの前面パネルのコンソールポートを使用して、スイッチを帯域外で管理できます。または、スイッチの任意の LAN ポートに Telnet 接続して、帯域内でスイッチを管理することもできます。コマンドラインインタフェースは、すべてのスイッチ管理機能にアクセスすることができます。

また、SNMP MIB（Management Information Base）を利用して、スイッチにステータス情報をポーリングしたり、異常イベントのトラップを送信したりできます。SNMP サポートにより、ス他のサードパーティ製デバイスとの統合管理が可能です。

搭載ポート

DXS-1210 シリーズは以下のポートを搭載しています。

- DXS-1210-10TS：100/1000/2.5G/5G/10G BASE-T ポート x 8 ポート、10G SFP+ スロット x 2 ポート
- DXS-1210-10MP：100/1000/2.5G/5G/10G BASE-T（PoE）ポート x 8 ポート、10G SFP+ スロット x 2 ポート
- DXS-1210-12TC：100/1000/2.5G/5G/10G BASE-T ポート x 10 ポート、10G SFP+ スロット x 2 ポート、10G SFP+ コンボスロット x 2 ポート
- DXS-1210-12SC：100/1000/2.5G/5G/10G BASE-T ポート x 2 ポート、10G SFP+ スロット x 10 ポート、10G SFP+ コンボスロット x 2 ポート

注意 DXS-1210-10TS/10MP/12TC/12SC について、区別する必要がある場合を除き、本マニュアル上では単に“スイッチ”あるいは“DXS-1210”と記載します。

オプションモジュール（光トランシーバ / ダイレクトアタッチケーブル）

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

光トランシーバ

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

※1 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。

※ 2 DEM-410T の取り付けは、スイッチ 1 台に対し最大 2 個までとなります。

※ スイッチ /SFP モジュールのハードウェア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 モジュールのハードウェア 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

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

DXS-1210 シリーズの前面パネルの各部名称は以下のとおりです。

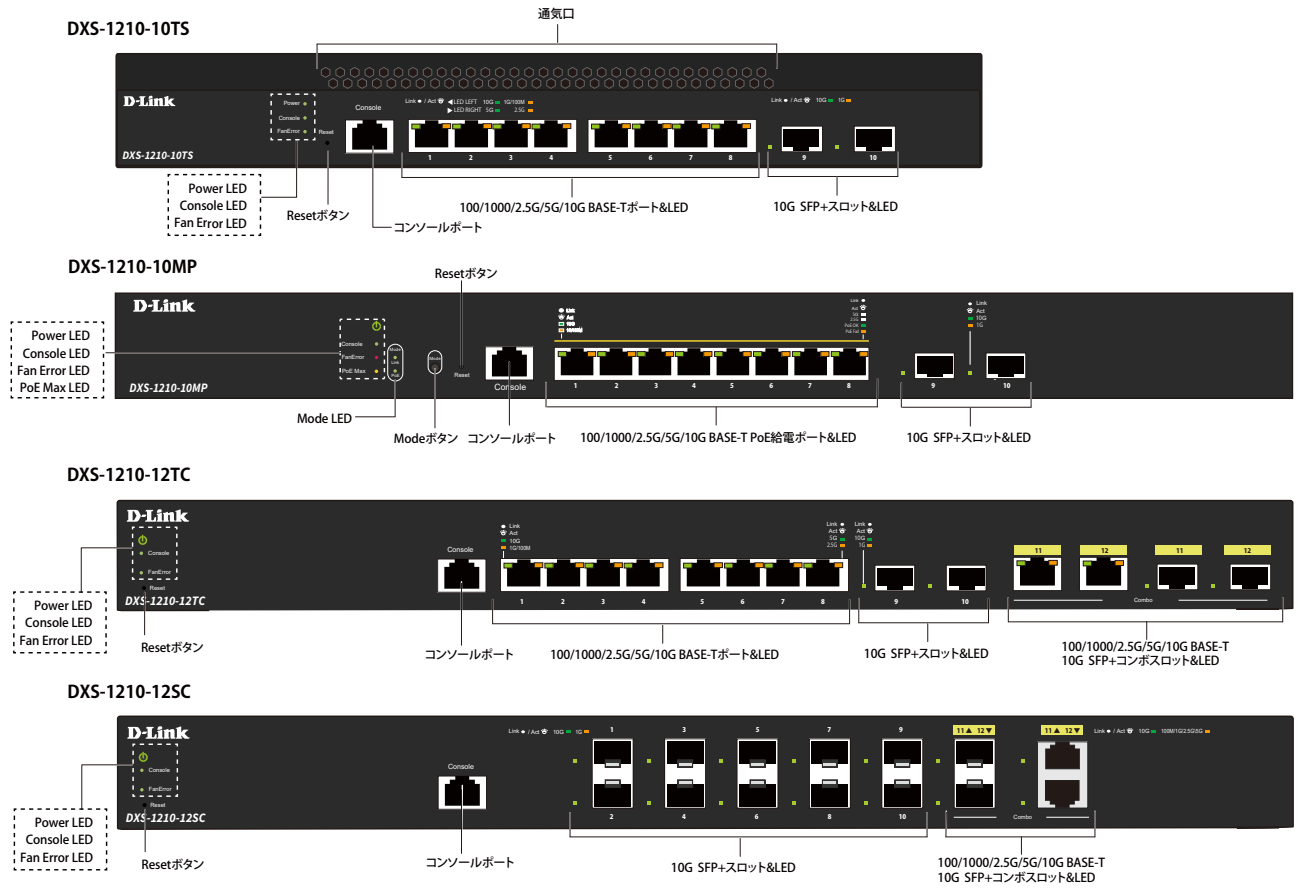


図 1-1　DXS-1210 シリーズ前面パネル

Reset（リセットボタン）

スイッチの前面パネルにはリセットボタン（Reset）があり、工場出荷時の値へのリセットを行うことができます。

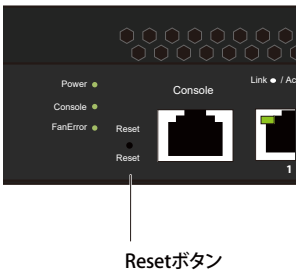


図 1-2　リセットボタン（DXS-1210-10TS）

リセットボタンを使用した再起動 / リセット方法

- リセットボタンを 1-5 秒押下すると、スイッチは再起動されます。
- リセットボタンを 6-10 秒押下すると、スイッチの設定内容は工場出荷時の値へリセットされます。

Mode（Mode ボタン）

DXS-1210-10MP の前面パネルには Mode ボタンがあります。
Mode ボタンを押下することにより、LED ステータスが異なる以下の 2 つのモードの切り替えを行うことができます。

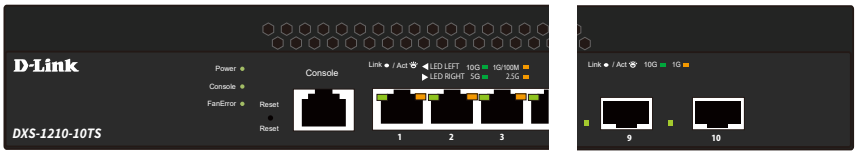
- Link/Act/Speed モード
- PoE モード

各モードにより、LED の点灯状態が異なります。詳細は「LED 表示」の説明をご確認ください。

LED 表示

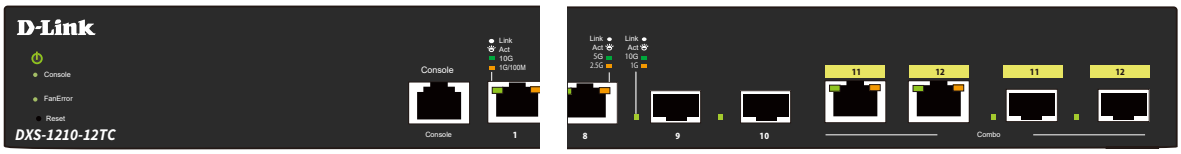
前面パネルに搭載されている LED 表示について説明します。

DXS-1210-10TS



DXS-1210-10MP

DXS-1210-12TC



DXS-1210-12SC

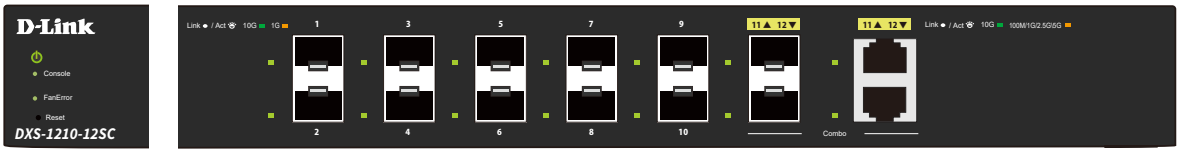


図 1-3　DXS-1210 シリーズの LED 配置図

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。

LED	位置	色	状態	内容
システム LED				
Power	—	緑	点灯	電源が供給され正常に動作しています。
		—	消灯	電源が供給されていません。
Console	—	緑	点灯	コンソールポートに接続しています。
		—	消灯	コンソールポートに接続していません。
Fan Error	—	赤	点灯	ファンは故障のため停止しています。
		—	消灯	ファンは正常に動作しています。
PoE Max （DXS-1210-10MP）	—	橙	点灯	受電デバイスに供給している電力が PoE の最大供給電力に近づき、Power Guard Band（電力保護帯域）に到達しています。 • 電力保護帯域は、最大供給電力のうち 7W 確保されています。（初期値） • 最大供給電力は最大 370W です。（初期値）
		—	消灯	PoE 供給電力が十分あり、Power Guard Band（電力保護帯域）を下回っています。
Mode （DXS-1210-10MP）	Link	緑	点灯	Link/Act/Speed モードに設定されています。 ポート LED は各ポートの Link/Act/Speed ステータスを表示します。
	PoE	緑	点灯	PoE モードに設定されています。 ポート LED は各ポートの PoE ステータスを表示します。 補足 PoE モードでは、ポート LED はポート 1-8 のみ点灯します。

LED	位置	色	状態	内容
ポート LED（Link/Act/Speed モード）				
100/1000/2.5G/5G/10GBASE-T ポート（DXS-1210-10TS/10MP/12TC）	ポート左側	緑	点灯	10 Gbps でリンクが確立しています。
			点滅	10 Gbps でデータを送受信しています。
		橙	点灯	100/1000 Mbps でリンクが確立しています。
			点滅	100/1000 Mbps 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。
	ポート右側	緑	点灯	5 Gbps でリンクが確立しています。
			点滅	5 Gbps でデータを送受信しています。
		橙	点灯	2.5 Gbps でリンクが確立しています。
			点滅	2.5 Gbps 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。
100/1000/2.5G/5G/10GBASE-T ポート（DXS-1210-12SC）	ー	緑	点灯	10 Gbps でリンクが確立しています。
			点滅	10 Gbps でデータを送受信しています。
		橙	点灯	100M/1000M/2.5G/5Gbps でリンクが確立しています。
			点滅	100M/1000M/2.5G/5Gbps 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。
10G SFP+ スロット	ー	緑	点灯	10 Gbps でリンクが確立しています。
			点滅	10 Gbps でデータを送受信しています。
		橙	点灯	1 Gbps でリンクが確立しています。
			点滅	1 Gbps 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。
ポート LED（PoE モード）				
100/1000/2.5G/5G/10GBASE-T ポート（DXS-1210-10MP）	ー	緑	点灯	PoE 受電機器が接続され、電力が供給されています。
		橙	点灯	PoE 受電機器が接続されていますが、電力を供給できません。 （PD 側のエラー、過電流、給電容量の不足といった理由が考えられます。）
		ー	消灯	PoE ポートが無効状態、または PoE 受電機器が接続されていません。

背面パネル

背面パネルの各部名称について説明します。
接地コネクタ、電源コネクタ、電源抜け防止器具挿入口、セキュリティスロットが配備されています。DXS-1210-10TS には通気口があります。

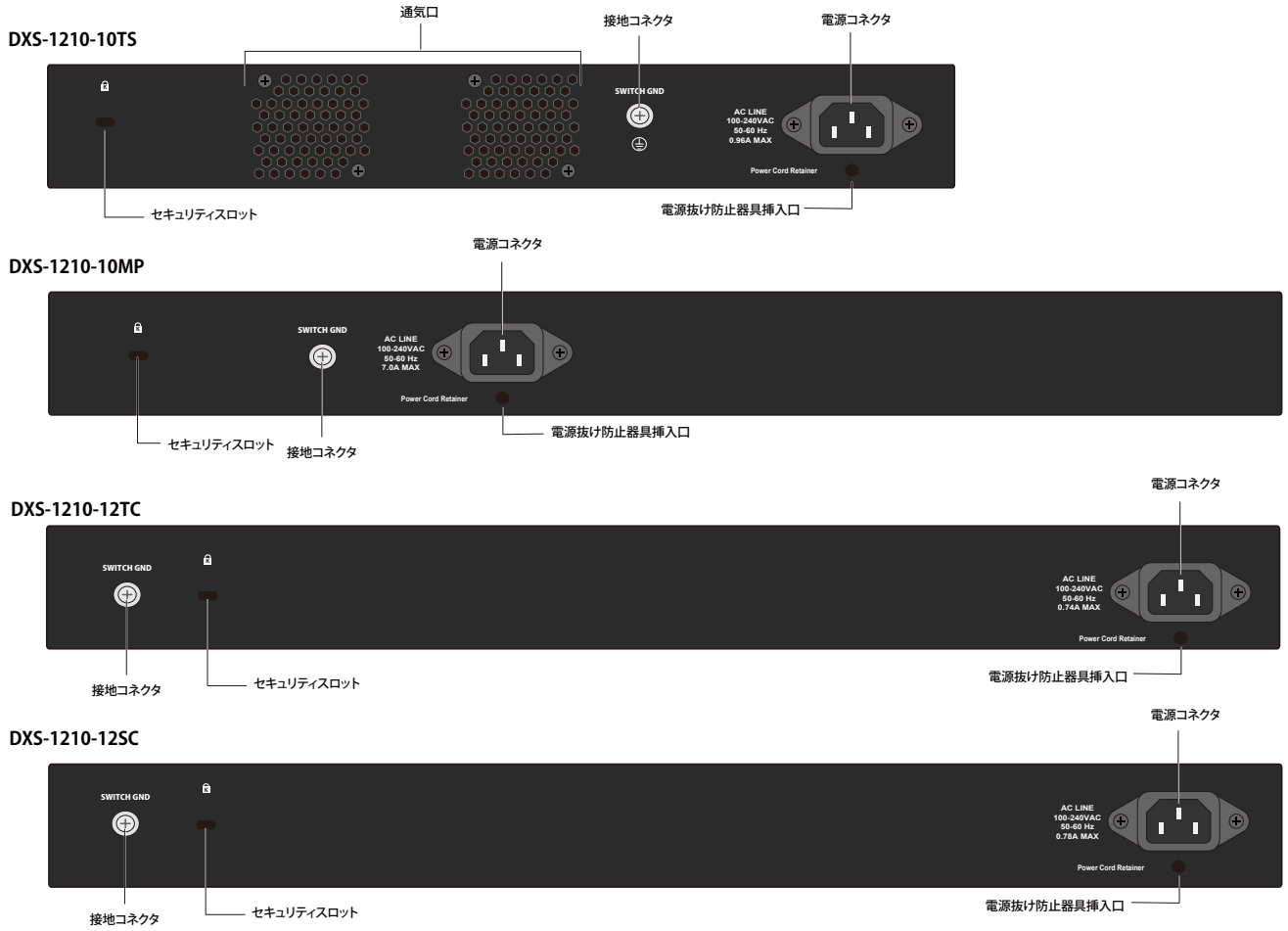


図 1-4　DXS-1210-10TS/10MP/12TC/12SC 背面パネル

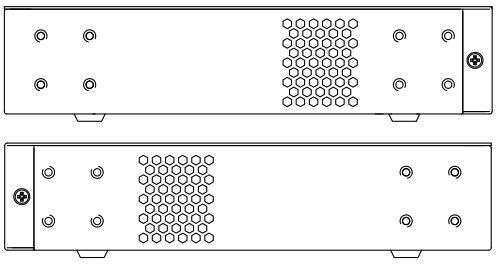
AC 電源コネクタは標準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ～ 240VAC 内の電圧に調整されます。

側面パネル

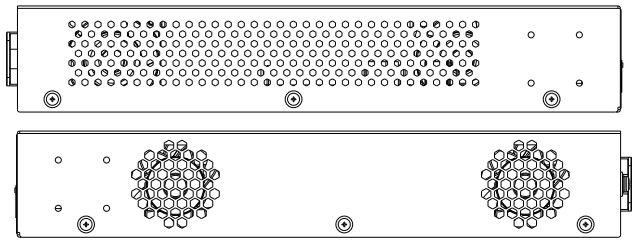
側面パネルには、通気口、ファン、ラック取り付けネジ穴などがあります。

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

DXS-1210-10TS 側面パネル



DXS-1210-10MP 側面パネル



DXS-1210-12TC/12SC 側面パネル

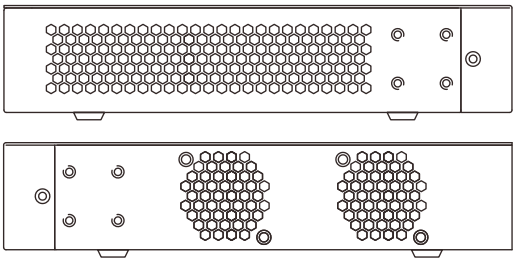


図 1-5　DXS-1210 シリーズ側面パネル

スマートファンについて

本シリーズは、ハードウェアに内蔵されたセンサによってスイッチ内部の温度を検出し、自動的にファンのスピードを調整する「スマートファン」を搭載しています。

本シリーズのスマートファンの回転スピードは、温度によって 5 段階（30%～ 70%）で調整されます。
各機種のスマートファンにおけるスピード調整の基準は、以下の通りです。

DXS-1210-10TS
- 温度上昇時：46℃未満の状態では低速、温度上昇により段階的にファンスピードが速くなり、59℃以上で高速になります。
- 温度下降時：54℃までの状態では高速、温度下降により段階的にファンスピードが遅くなり、29℃未満で低速になります。

DXS-1210-10MP
- 温度上昇時：61℃未満の状態では低速、温度上昇により段階的にファンスピードが速くなり、73℃以上で高速になります。
- 温度下降時：68℃までの状態では高速、温度下降により段階的にファンスピードが遅くなり、56℃未満で低速になります。

DXS-1210-12TC
- 温度上昇時：47℃未満の状態では低速、温度上昇により段階的にファンスピードが速くなり、69℃以上で高速になります。
- 温度下降時：64℃までの状態では高速、温度下降により段階的にファンスピードが遅くなり、25℃未満で低速になります。

DXS-1210-12SC
- 温度上昇時：31℃未満の状態では低速、温度上昇により段階的にファンスピードが速くなり、60℃以上で高速になります。
- 温度下降時：55℃までの状態では高速、温度下降により段階的にファンスピードが遅くなり、25℃未満で低速になります。

ファンモード（DXS-1210-10MP のみ）

DXS-1210-10MP は、以下の 2 種類のファンモードに対応しています。

ファンモード	説明
Normal（ノーマル）モード	ファンは温度によって自動的にスピード調整されます。（初期値 / 上記参照）
Quiet（静音）モード	ファンは 低速（Ultra Low、30%）で動作します。 温度や PoE の基準値を超えた場合、「Normal」モードに戻ります。 ※「Normal」モードに変更されると、「Quiet」モードには戻りません。 • PoE 供給電力が 240W を超えた場合、「Normal」モードに自動的に戻ります。 • リンクアップポートが 6 ポートを超えた場合、「Normal」モードに自動的に戻ります。 • 内部温度が 70℃を超えた場合、「Normal」モードに自動的に戻ります。

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

第 2 章　スイッチの設置

パッケージの内容

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

- 本体　x　1
- AC 電源ケーブル（100V 用）　x　1
- RJ-45/RS-232C コンソールケーブル　x　1
- 19 インチラックマウントキット 1 式
- 電源抜け防止器具　x　1
- ゴム足　x　4
- 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。
- 電源ケーブルが電源コネクタ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 10cm 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。

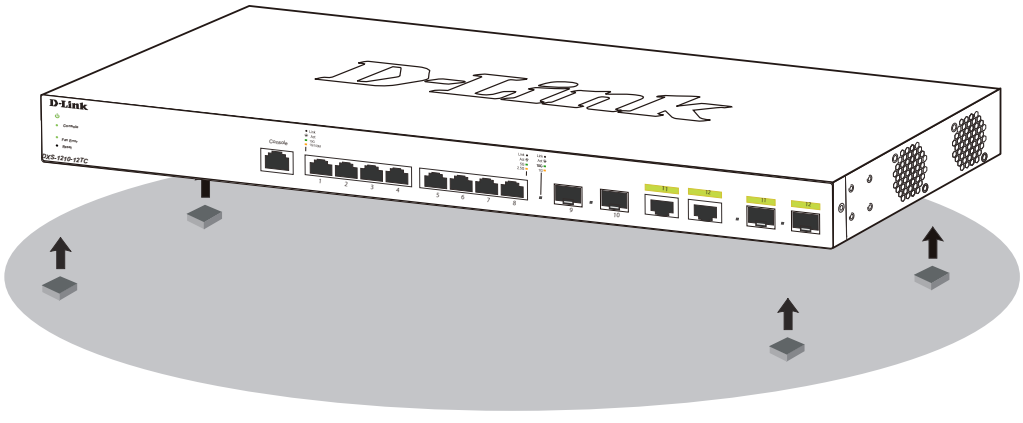


図 2-1　　机や棚の上に設置する場合の準備

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。

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

1. 電源ケーブルおよびケーブル類が本体に接続されていないことを確認します。
2. 付属のネジで、スイッチ両側面にブラケットを取り付けます。

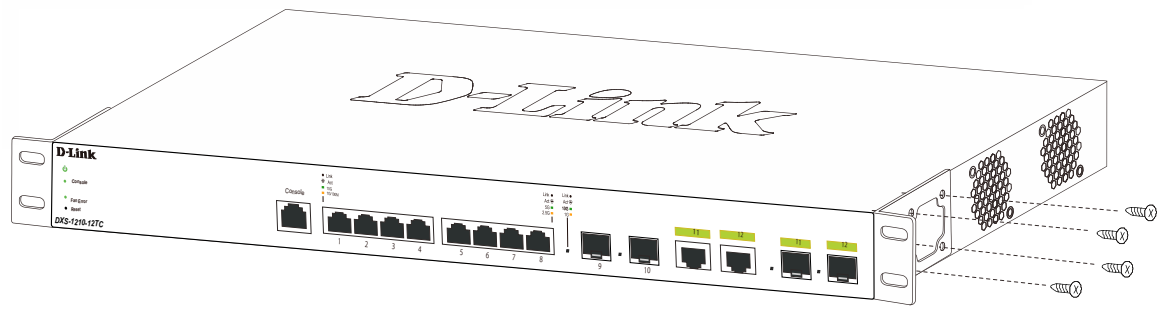


図 2-2　ブラケットの取り付け

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

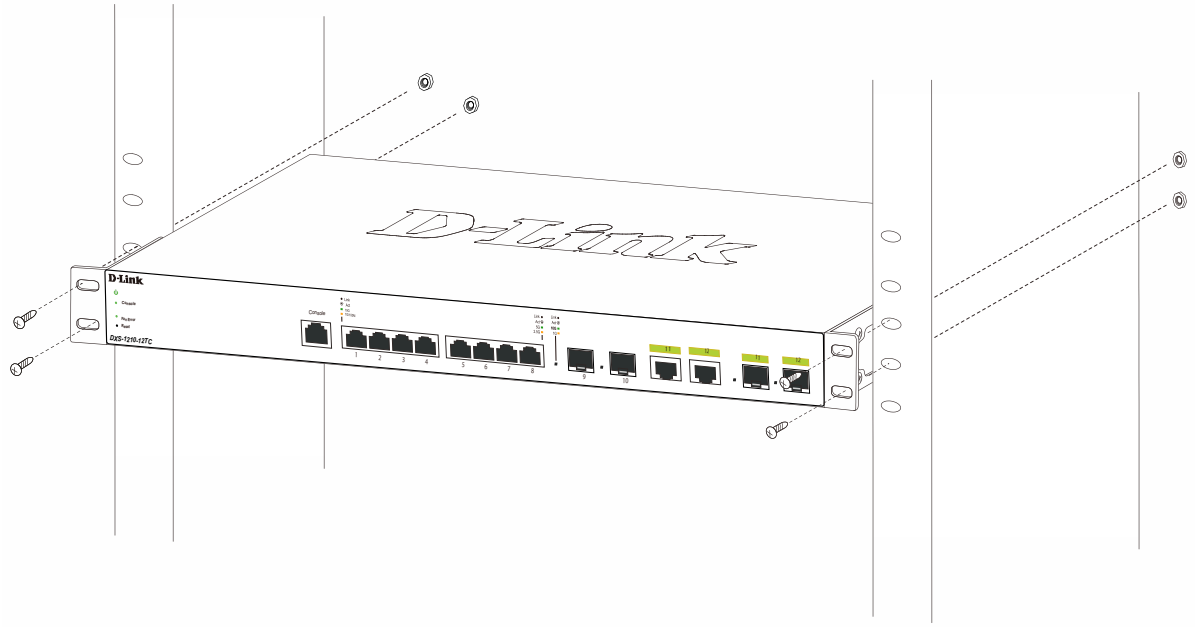


図 2-3　19 インチラックへの設置

光トランシーバの接続

本シリーズには SFP+ スロットが搭載されており、光トランシーバを接続できます。

■ SFP+ スロットに光トランシーバを挿入

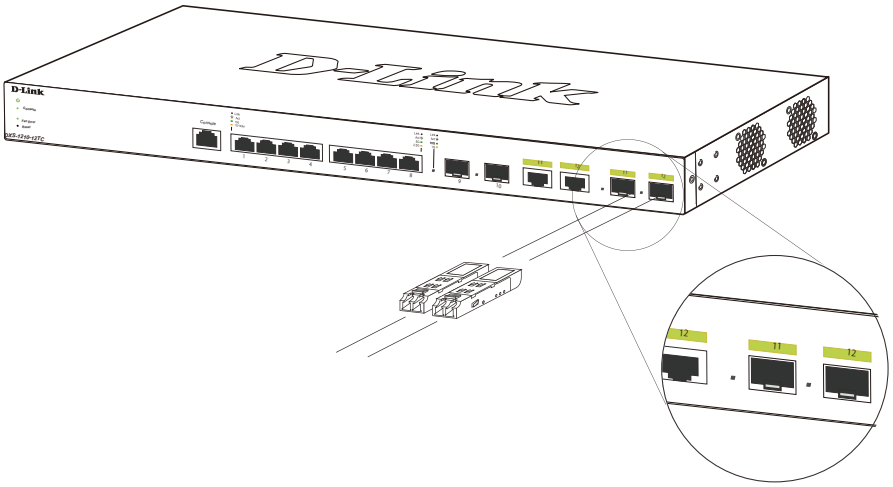


図 2-4　SFP+ スロットにモジュールを挿入

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

注意 光トランシーバを素早く抜き差しした場合、コンソール上でエラーログが表示される場合があります。

電源抜け防止器具の装着

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

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

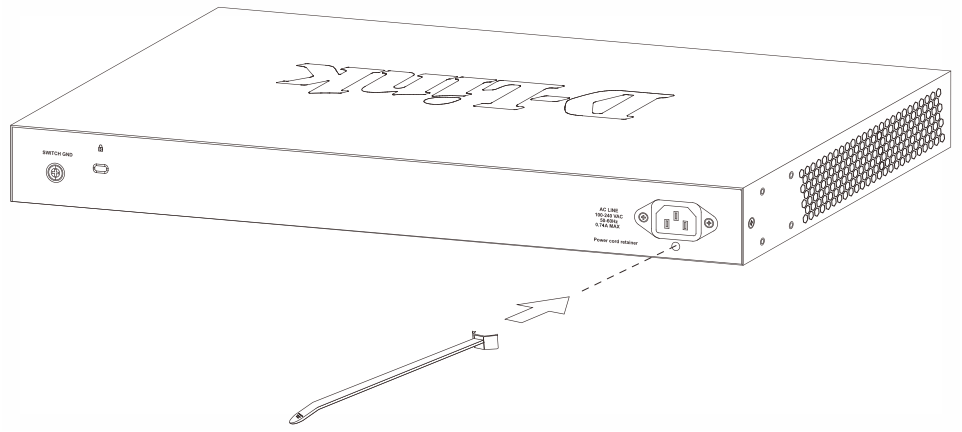


図 2-5　タイラップの挿し込み

2. AC 電源コードをスイッチの電源プラグに挿し込みます。

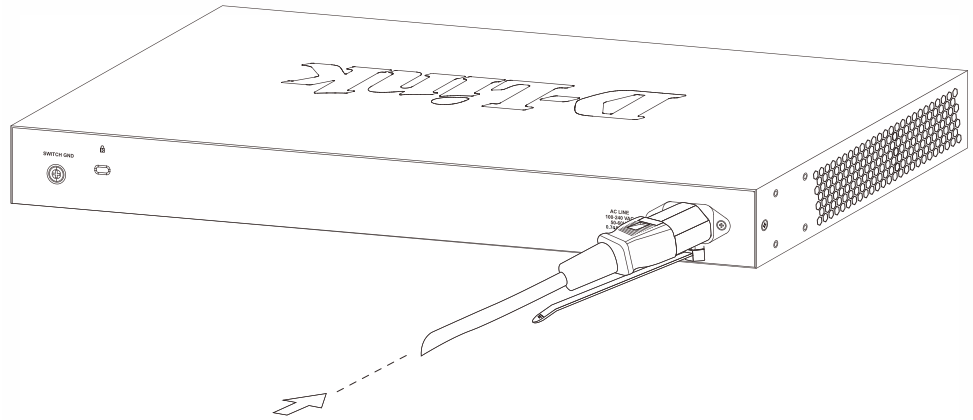


図 2-6　電源コード挿し込み

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

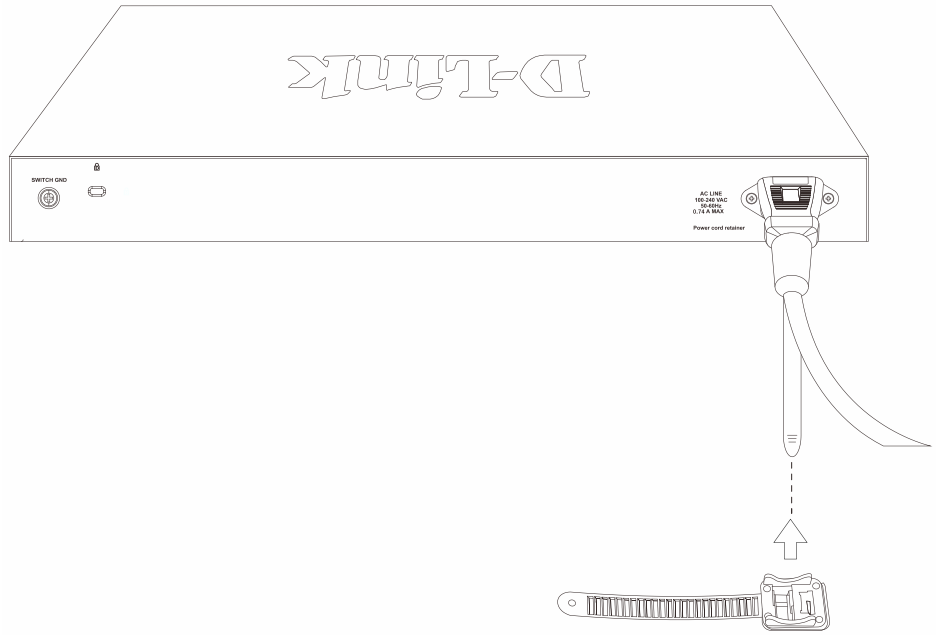


図 2-7　リテイナー（固定具）のスライド

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

図 2-8　　リテイナーの巻き付け、固定

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

図 2-9　　電源抜け防止器具の固定確認

スイッチの接地

本スイッチを接地する方法について説明します。

注意　スイッチの電源をオンにする前に、本手順を完了する必要があります。

接地に必要なツールと機器

- 接地ネジ（M4 x 6mm のパンヘッドネジ）1 個
- リング型ラグ端子付接地線
- ドライバ

注意　接地ネジ / リング型ラグ端子付接地線 / ドライバは、本製品の同梱物には含まれていません。

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

以下の手順でスイッチを保安用接地に接続します。

1. システムの電源がオフであることを確認します。
2. 接地ケーブルを使用して、以下の図のように、オープン状態の接地ネジ穴の上に # 8 リング型ラグ端子を置きます。
3. 接地ネジ穴に接地端子を挿入します。
4. ドライバを使用して、接地ネジをしめて、スイッチに接地ケーブルを固定します。
5. スイッチが設置されるラック上の適切な設置スタッドまたはボルトに接地線の一端にあるリング型ラグ端子を取り付けます。
6. スイッチとラック上の設置コネクタの接続がしっかりと行われていることを確認します。

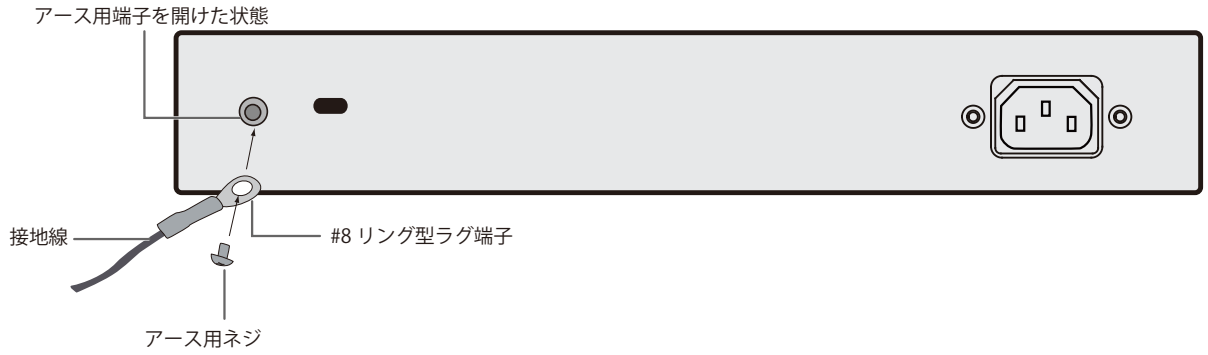


図 2-10　スイッチへのラグ端子の接続

電源の投入

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

電源の異常

AC 電源に異常が発生した / する場合（停電等）、スイッチから電源ケーブルを抜いてください。電力の回復後に再接続します。

第 3 章　スイッチの接続

参照　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

UTP ケーブルを使用してスイッチとエンドノードを接続します。エンドノードとは、RJ45 ネットワークポートを搭載した PC やルータの総称です。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。

下図は、スイッチに接続されている一般的なエンドノードを示しています。

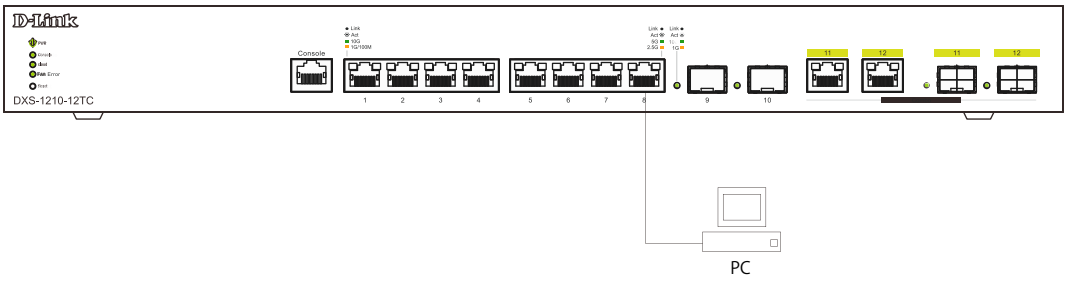


図 3-1　エンドノードとの接続図

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

ハブまたはスイッチと接続する

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 5/5e/6/6a/7 の UTP/STP ケーブル : 100/1000/2.5G/5G/10G BASE-T スイッチポートと接続します。
  - 10GBASE-T 通信用には、カテゴリ 6/6a/7 の UTP/STP ケーブルを使用します。
- 光ファイバケーブル : SFP+ スロット経由で光ファイバをサポートするスイッチにアップリンクします。

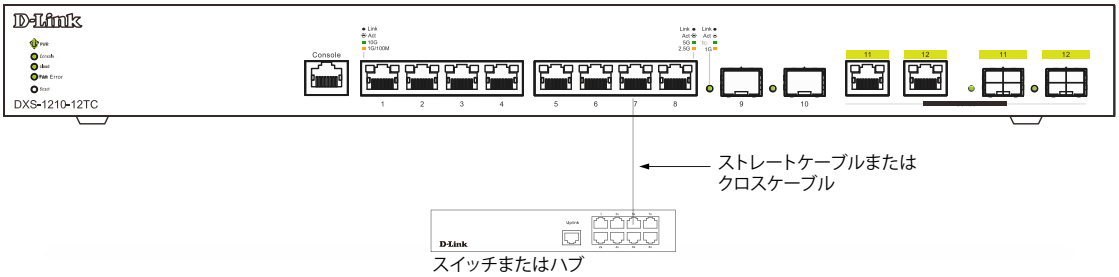


図 3-2　ハブまたはスイッチとの接続図

バックボーンまたはサーバと接続する

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

各ポートは以下の速度で動作します。
- RJ45 ポート：100Mbps および 1/2.5/5/10Gbps
- SFP+ スロット：1/10Gbps

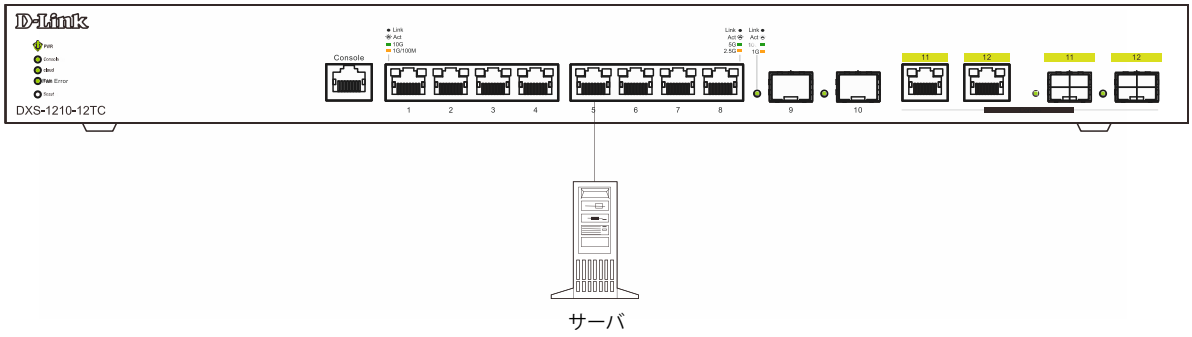


図 3-3　サーバとの接続図

第 4 章　スイッチ管理について

Web GUI による管理

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

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

SNMP による管理

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

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

CLI による管理

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

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

注意　本製品の CLI の使用に関して、以下の制限があります。

- CLI でコマンドのオプション候補を表示する（? を入力）際に、文字を省略して入力し、複数のコマンド候補がある場合は、すべての該当コマンドのオプションが表示されます。
- “configure” と” clear running-config” コマンドを繰り返し実行した場合、ポートのリンクダウン / リンクアップが発生します。
- コンフィグの流し込みとリセットを繰り返し実施した場合、Web が正常に表示されなくなる場合があります。

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「ユーザアカウント / パスワードの設定」を参照してください。
CLI の詳細及びコマンドリストについては、CLI マニュアルを参照してください。

5. ログアウトする場合は、logout コマンド使用するか、ターミナルソフトを終了します。

ユーザアカウント / パスワードの設定

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

注意 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 NewUser password 12345
Switch(config)# username NewUser privilege 15
Switch(config)# line console
Switch(config-line)#
```

1. ログインユーザの権限がレベル 15 以外の場合、「enable」コマンドを入力し、Privileged EXEC モードにアクセスします。
2. 「configure terminal」コマンドを入力し、Global Configuration モードにアクセスします。
3. 「username NewUser password 12345」コマンドを入力し、ユーザ名「NewUser」、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」コマンドを入力すると、LINE Configuration モードにアクセスできます。

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。詳しくは DXS-1210 の CLI マニュアルを参照してください。

IP アドレスの設定

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

- IP アドレスの初期値：10.90.90.90/8

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

1. ログインユーザの権限がレベル 15 以外の場合、「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

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

本スイッチのすべてのソフトウェア機能は、実装されている Web ベース（HTML）インタフェース経由で管理、設定およびモニタできます。標準的なブラウザを使用して、ネットワーク上のリモートステーションから本スイッチを管理できます。

最大 4 人のユーザが Web ベース管理に同時にアクセスできます。

サポートされるブラウザ

- Microsoft Edge
- Google Chrome
- Firefox
- Safari
- Opera

ブラウザの仕様により互換性が確保されない場合があります。

スイッチへの接続

デバイスの Web ベース管理を開始するには、次の準備が必要です。
- RJ-45 イーサネット接続のある PC
- 標準イーサネットケーブル

イーサネットケーブルを、スイッチの前面パネルの任意のポートと PC のイーサネットポートに接続します。

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）。

Web ベースユーザインタフェースに接続する :

1. Web ブラウザを開きます。

2. アドレスバーに本スイッチの IP アドレスを入力し、「Enter」キーを押下します。

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」、デフォルトゲートウェイ「0.0.0.0」が設定されています。
Web マネージャへログインするには、PC の IP アドレスを本スイッチに合わせるか、本スイッチを PC の IP アドレスに合わせてください。
【例】スイッチの IP アドレスが 10.90.90.90 の場合 :
以下の通りに設定します。
管理 PC のアドレス：10.x.y.z（x/y は 0 ～ 254 の間の整数、z は 1 ～ 254 の間の整数）
サブネットマスク：255.0.0.0

3. 以下のユーザ認証画面が表示されます。

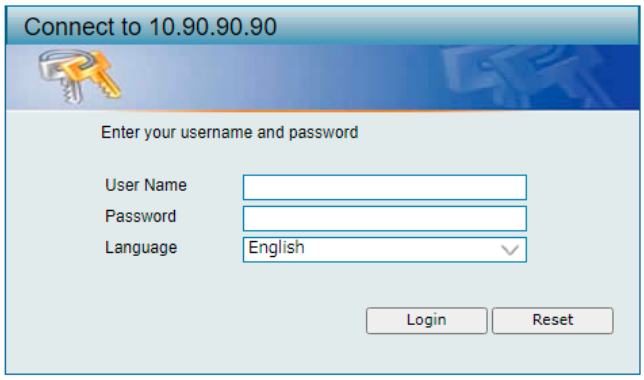


図 5-2　ユーザ認証画面

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

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

補足　入力値は ASCII 文字のみをサポートします。

4. スマートウィザード画面が表示されます。

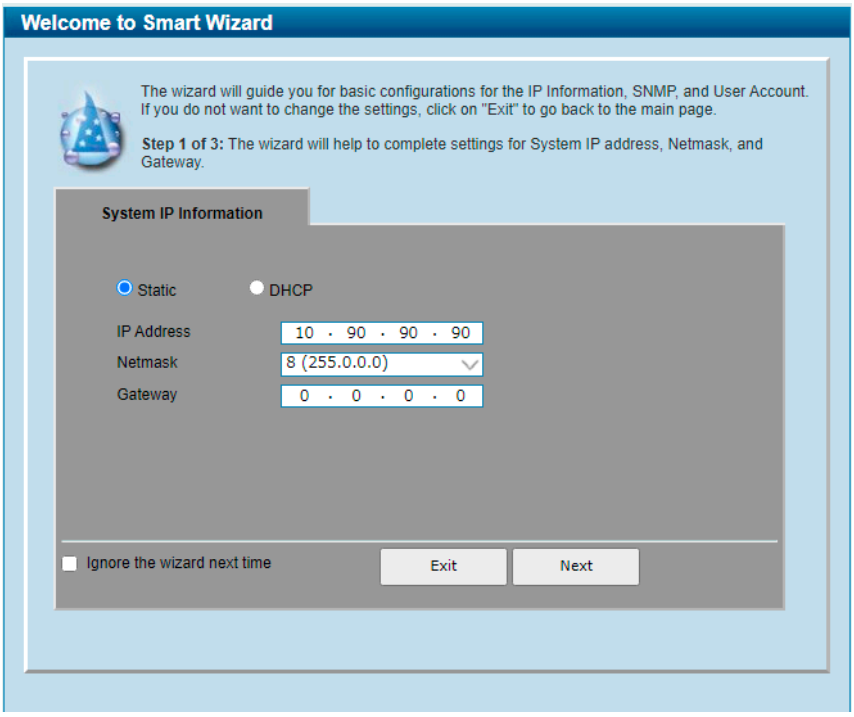


図 5-3　Smart Wizard 画面

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

5. ウィザードを使用しない場合は、「Exit」をクリックします。

Smart Wizard 設定

「Smart Wizard」で基本的なシステム設定（IP アドレス、パスワード、SNMP）を行います。

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

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

IP アドレスの設定（Smart Wizard）

1. IP アドレスの設定を行います。

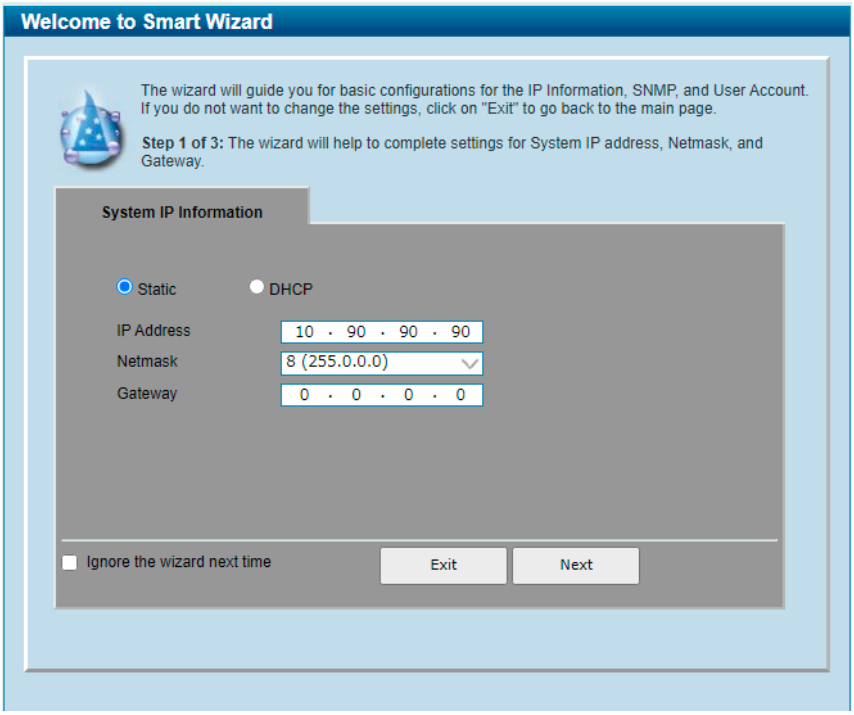


図 5-4　IP Information 設定画面

1. 「Static」「DHCP」のいずれかを選択します。
   - 「Static」：固定 IP アドレスを手動で設定します。
   - 「DHCP」：DHCP サーバから IPv4 アドレスを自動的に取得します。

   「Static」を選択した場合は、「IP Address」「Netmask」「Gateway」を入力します。
   「DHCP」を選択した場合は「DHCP Retry Times」を指定します。

2. 「Next」をクリックします。

設定内容、変更を破棄し Web GUI へ戻る場合は、「Exit」をクリックします。

補足　スマートウィザードでは IPv4 アドレスのみ設定可能です。

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

SNMP の設定（Smart Wizard）

2. SNMP の設定を行います。

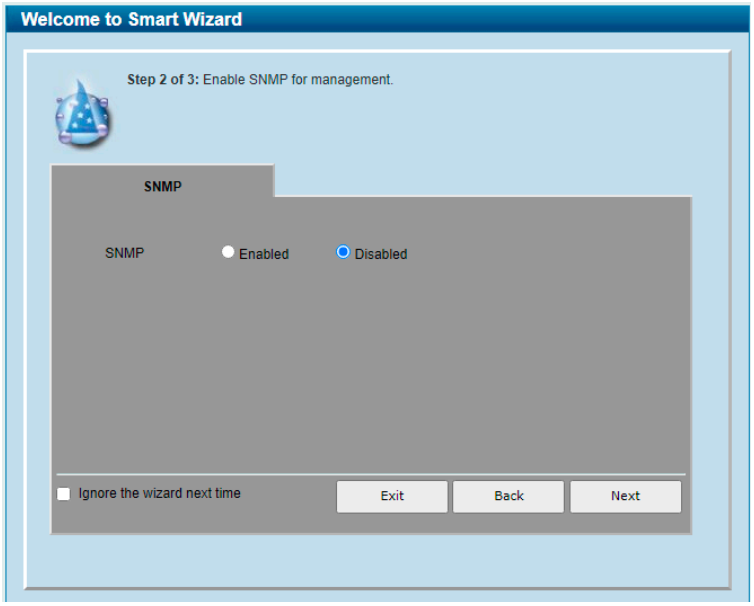


図 5-5　SNMP 設定画面

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

設定内容、変更を破棄し Web GUI へ戻る場合は、「Exit」をクリックします。
前のページへ戻る場合は、「Back」をクリックします。

ユーザアカウントの設定（Smart Wizard）

3. ユーザアカウントの設定を行います。

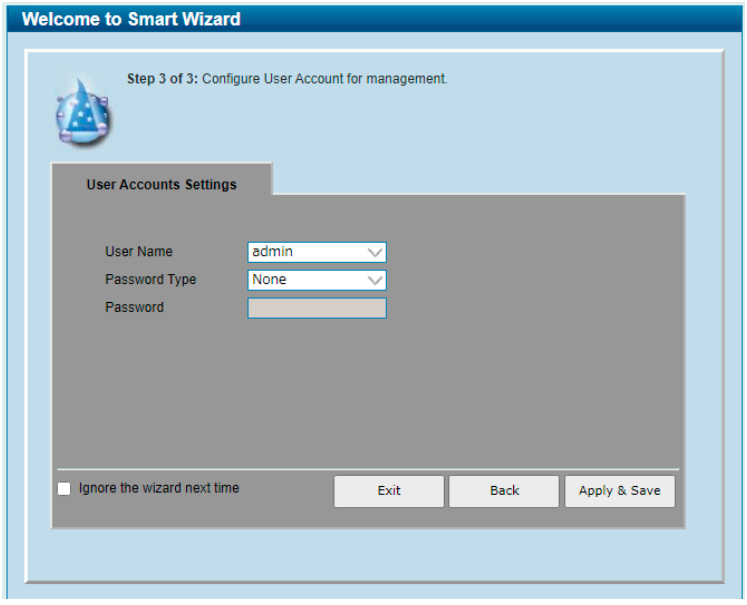


図 5-6　ユーザアカウント設定画面

1. 以下の項目を設定します。
   - 「User Name」：設定を行うユーザアカウントを選択します。
   - 「Password Type」：パスワード暗号化の種類を指定します。
   - 「Password」：ユーザアカウントのパスワードを入力します。

2. 「Apply & Save」をクリックします。

設定内容、変更を破棄し Web GUI へ戻る場合は、「Exit」をクリックします。
前のページへ戻る場合は、「Back」をクリックします。

Web ベースのユーザインタフェース

Web ユーザインタフェースではスイッチの設定を行うほか、パフォーマンス状況やシステム状態をグラフィック表示で参照できます。

ユーザインタフェース内の各エリア

Web ベースインタフェースの「Device Information」画面では以下の情報を参照することができます。

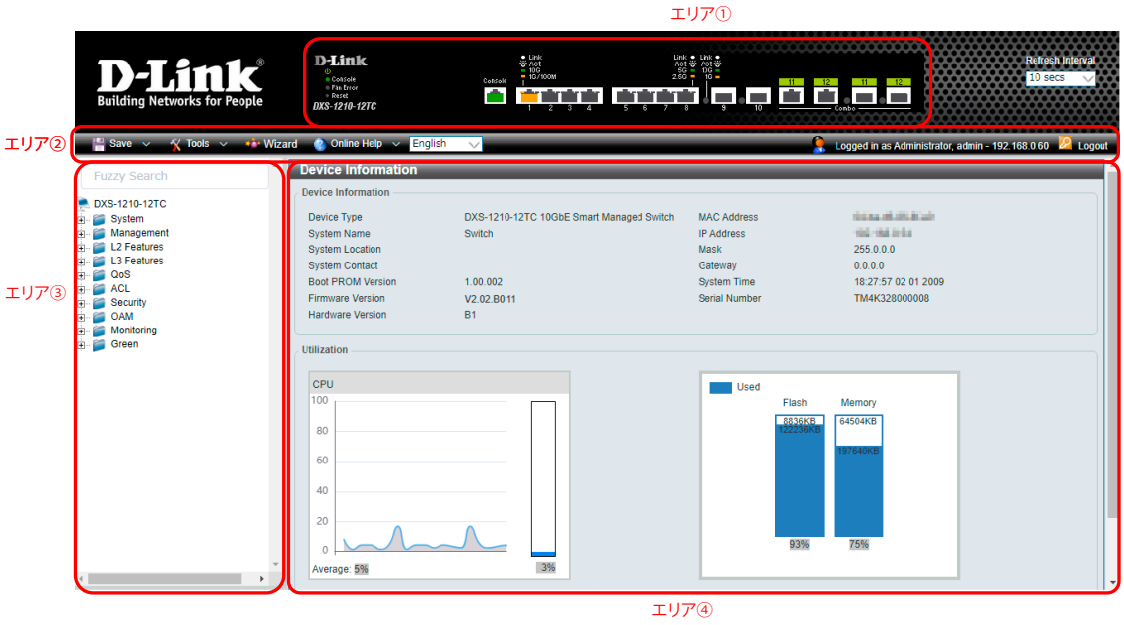


図 5-7　Device Information 画面

エリア	説明
エリア①	本エリアではスイッチの前面パネルの状態がほぼリアルタイムにグラフィカル表示されます。 スイッチのポート、拡張モジュールが表示されます。 「D-Link」ロゴをクリックすると D-Link Web サイト（英語）へ移動します。
エリア②	スイッチの再起動、コンフィグレーションのバックアップとリストア、ファームウェアの更新、設定の初期化などを行う「Tools」メニューと、設定の保存を行う「Save」メニューがあります。 ツールバーの右側には、現在接続中のユーザ名とスイッチの IP アドレス、ログアウトボタンが表示されます。
エリア③	Web GUI 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	エリア③の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。

注意　スイッチ設定を変更した場合、Web GUI ツールバーの「Save」メニューで設定を保存する必要があります。

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

Web マネージャのメニュー構成

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

メイン メニュー	サブメニュー	説明
System	Device Information	スイッチの主な設定情報を表示します。
	System Information	スイッチの基本情報を表示します。
	Peripheral	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、ジャンボフレーム設定などを行います。
	PoE	PoE 設定を行います。
	System Log	スイッチのシステムログ設定を行います。
	Time and SNTP	スイッチの時刻設定を行います。
	Time Range	スイッチのタイムレンジを設定します。
Management	User Accounts Settings	ユーザアカウントの作成と設定を行います。有効なユーザアカウントを表示可能です。
	Password Encryption	パスワードを暗号化し設定ファイルに保存します。
	SNMP	SNMP を使用してスイッチを管理します。
	RMON	スイッチの SNMP 機能に対するリモートモニタリング（RMON）ステータスを有効または無効にします。
	DHCP Auto Configuration	DHCP 自動設定機能の設定を行います。
	Telnet/Web	スイッチの Telnet 設定と Web 設定を行います。
	Session Timeout	セッションタイムアウトの設定を行います。
	D-Link Discovery Protocol Settings	D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。
L2 Features	FDB	スタティック FDB、MAC アドレステーブルなどを設定します。
	VLAN Configuration Wizard	ウィザードを使用して VLAN の設定を行います。
	802.1Q VLAN	802.1Q VLAN の設定を行います。
	Asymmetric VLAN	Asymmetric VLAN の設定を行います。
	VLAN Interface	VLAN インタフェースの設定を行います。
	GVRP	GVRP（GARP VLAN Registration Protocol）の設定を行います。
	Auto Surveillance VLAN	自動サーベイランス VLAN の設定を行います。
	Voice VLAN	音声 VLAN の設定を行います。
	STP	スパニングツリーの設定を行います。
	ERPS (G.8032)	「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を行います。
	Link Aggregation	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します。
	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	LLDP（Link Layer Discovery Protocol）の設定を行います。
L3 Features	ARP	ARP の設定、編集を行います。
	IPv4 Interface	IPv4 インタフェースの設定を行います。
	IPv4 Static/Default Route	IPv4 スタティック / デフォルトルートの設定を行います。
	IPv4 Route Table	IPv4 ルートテーブルの設定を行います。
	IPv6 Interface	IPv6 インタフェースの設定を行います。
	IPv6 Neighbor	IPv6 ネイバの設定を行います。
	IPv6 Static/Default Route	IPv6 スタティック / デフォルトルートの設定を行います。
	IPv6 Route Table	IPv6 ルートテーブルの設定を行います。
	DNS Server Settings	DNS サーバの設定を行います。
QoS	Port Default CoS	各ポートにデフォルト CoS の設定を行います。
	Port Scheduler Method	ポートスケジューラメソッドを設定します。
	Queue Settings	キューを設定、表示します。
	CoS to Queue Mapping	CoS-to-Queue マッピングの表示、設定を行います。
	Port Rate Limiting	ポートレート制限の設定を行います。
	Queue Rate Limiting	キューレートの制限設定をします。
	Port Trust State	ポートトラスト設定を行います。
	DSCP CoS Mapping	DSCP CoS マップの設定と表示を行います。

メイン メニュー	サブメニュー	説明
ACL	ACL Configuration Wizard	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します。
	ACL Access List	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の設定を行います。
Security	Port Security	ポートセキュリティの設定を行います。
	802.1X	802.1X 認証設定を行います。
	AAA	AAA の設定を行います。
	RADIUS	RADIUS サーバの設定を行います。
	TACACS	TACACS サーバの設定を行います。
	IMPB	IP-MAC ポートバインディングの設定を行います。
	Network Access Authentication	ネットワークアクセス認証設定を行います。
	DHCP Server Screening	DHCP サーバスクリーニングの設定を行います。
	Safeguard Engine	セーフガードエンジン設定を行います。
	Trusted Host	トラストホスト設定を行います。
	Traffic Segmentation Settings	トラフィックセグメンテーション設定を行います。
	Storm Control Settings	ストームコントロールの設定を行います。
	DoS Attack Prevention Settings	DoS 攻撃防止設定を行います。
	SSH	SSH（Secure Shell）の設定を行います。
	SSL	SSL（Secure Socket Layer）の設定を行います。
OAM	Cable Diagnostics	ケーブル診断を行います。
	DDM	Digital Diagnostic Monitoring（DDM）機能を設定します。
Monitoring	Statistics	パケット統計情報とエラー統計情報を表示します。
	Mirror Settings	ポートミラーリングの設定を行います。
Green	Power Saving	機器の省電力設定を行います。
	EEE	Energy Efficient Ethernet/ 省電力イーサネットの設定を行います。
Toolbar	Save	コンフィグレーションの保存などを行います。
	Tools	ファームウェアアップグレードやバックアップ、コンフィグレーションのリストア、バックアップなどを行います。
	Wizard	スマートウィザードを開始します。
	Online Help	D-Link のサポート Web サイト（英語）/ またはユーザガイド（英語版）を表示します。インターネット接続が必要です。
	Logout	Web GUI からログアウトします。

第 6 章　System（システム設定）

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（システム情報）	スイッチの基本情報を表示します。
Peripheral（環境設定）	スイッチの環境設定を行います。
Port Configuration（ポート設定）	ポート設定、ジャンボフレーム設定などを行います。
PoE（PoE 設定）（DXS-1210-10MP）	PoE の設定を行います。（DXS-1210-10MP のみ）
System Log（システムログ）	システムログの設定を行います。
Time and SNTP（時刻・SNTP 設定）	スイッチに時刻を設定します。
Time Range（タイムレンジ設定）	スイッチの ACL 機能などで使用するスケジュールを定義します。

Device Information（デバイス情報）

ログイン時に自動的に表示されるスイッチのシステム情報です。
他の画面から「Device Information」画面に戻る場合は、製品名をクリックします。
「Device Information」画面にはデバイスの一般的な情報（システム名、場所、システム MAC アドレス、システム時刻、IP アドレス、ファームウェア、およびハードウェアのバージョン情報など）が表示されます。

ツリービューの製品名（DXS-1210-10TS/10MP/12TC/12SC）をクリックし、以下の画面を表示します。

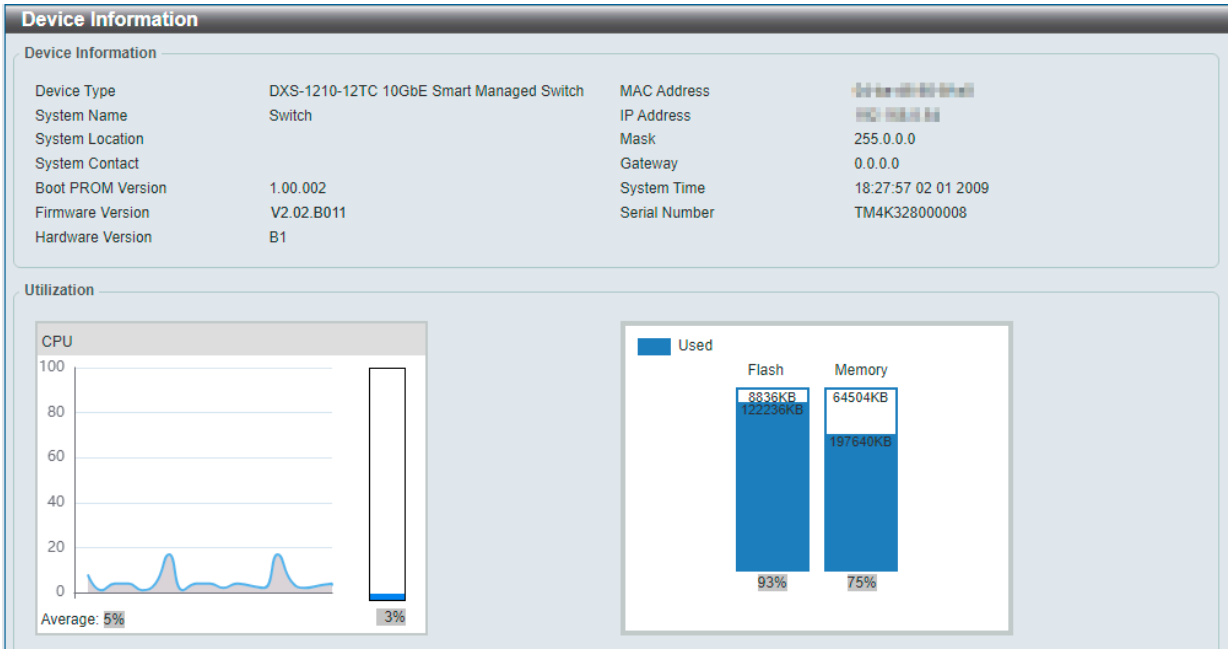


図 6-1　Device Information 画面

「Device Information」画面に表示される項目：

項目	説明
Device Information	
Device Type	工場で定義された機種名と型式を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。
System Contact	担当者名を表示します。
Boot PROM Version	起動 PROM バージョンを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
Hardware Version	デバイスのハードウェアバージョンを表示します。
MAC Address	デバイスに割り当てられた MAC アドレスを表示します。
IP Address	デバイスに割り当てられた IP アドレスを表示します。
Mask	デバイスに割り当てられたサブネットマスクを表示します。

項目	説明
Gateway	デバイスに割り当てられたデフォルトゲートウェイを表示します。
System Time	システムの時刻および日付を表示します。時刻 / 日 / 月 / 年の順で表示します。
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	フラッシュの使用率を表示します。
Memory	メモリの使用率を表示します。

System Information（システム情報）

システム情報画面では、基本的なシステム情報の設定を行います。

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

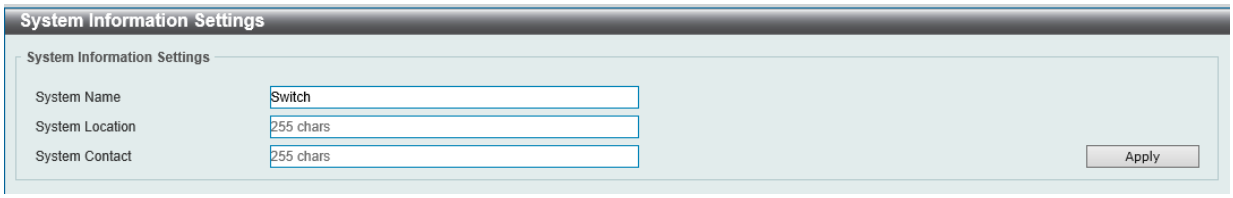


図 6-2　System Information Settings 画面

画面に表示される項目：

項目	説明
System Name	必要に応じて、スイッチのシステム名を変更します。ネットワーク内での識別名となります。
System Location	必要に応じて、システムが稼働している場所を定義します。
System Contact	必要に応じて、スイッチの管理者情報を入力します。

「Apply」をクリックして、設定内容を適用します。

Peripheral（環境設定）

システムの温度やファンのトラップ設定を行います。

System > Peripheral 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（DXS-1210-10TS/12TC/12SC）

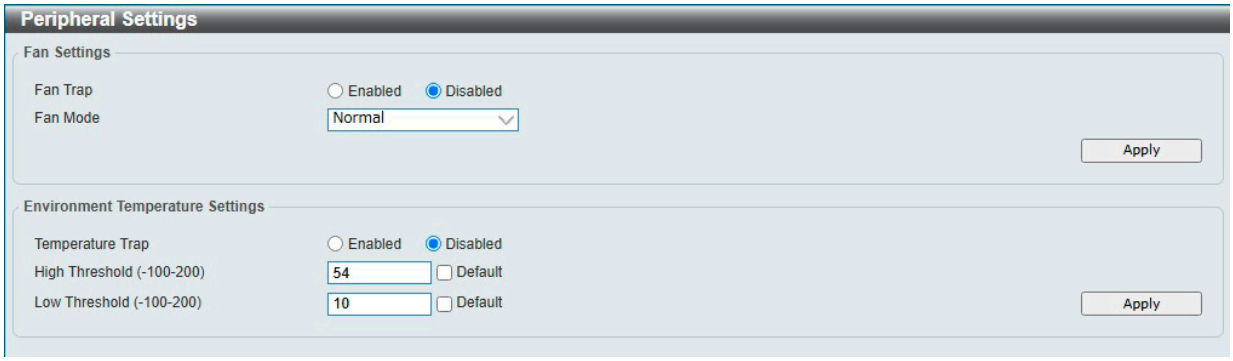


図 6-4　Peripheral Settings 画面（DXS-1210-10MP）

画面に表示される項目（DXS-1210-10TS/12TC/12SC）：

項目	説明
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。
Fan Mode （DXS-1210-10MP のみ）	ファン制御のモードを選択します。 • 選択肢：「Normal（ノーマル）」「Quiet（静音）」
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。
High Threshold	高温警告しきい値を指定します。 • 設定可能範囲：「-100℃」-「200℃」 「Default」にチェックを入れると初期値に戻ります。
Low Threshold	低温警告しきい値を指定します。 • 設定可能範囲：「-100℃」-「200℃」 「Default」にチェックを入れると初期値に戻ります。

「Apply」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（ポート設定）

ポートの詳細を設定します。

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

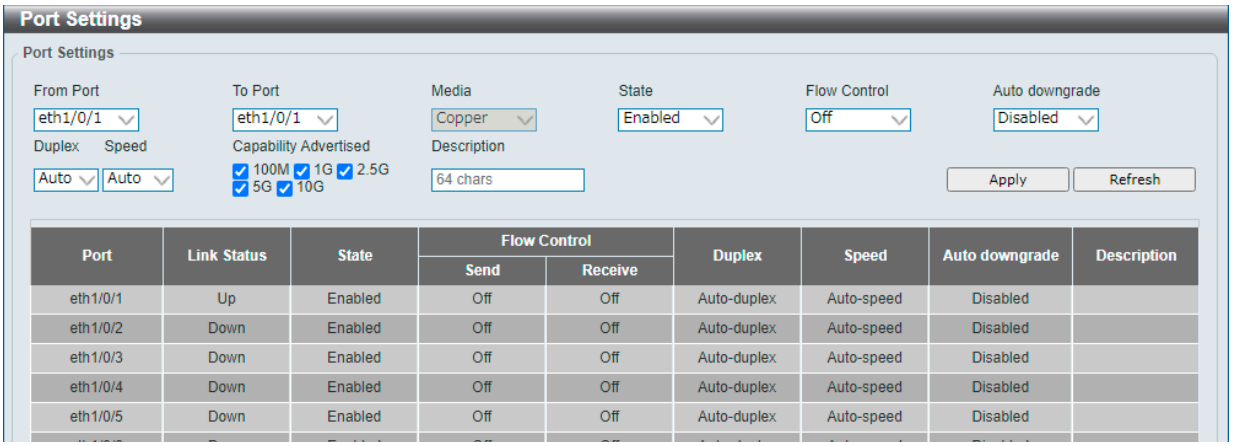


図 6-5　Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Media	コンボポートの場合、設定するポートを選択します。 • 選択肢：「Copper」「Fiber」
State	物理ポートのステータスを有効 / 無効に設定します。
Flow Control	「On」（フロー制御あり）または「Off」（フロー制御なし）を選択します。 Full-Duplex のポートでは 802.3x フローコントロールによる制御を行い、半二重ポートではバックプレッシャーによるフロー制御を行います。「Auto」のポートは自動的にいずれかの方式を使用します。
Auto downgrade	利用可能な速度でリンクを確立できない場合に、アドバタイズ速度の自動ダウングレードを有効 / 無効に設定します。
Duplex	Duplex モードの設定を以下から選択します。 • 「Auto」「Full」
Speed	ポートの速度を選択します。 • 「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 • 「100M」- ポート速度を 100 Mbps に指定します。（Copper ポートのみ） • 「1G」- ポート速度を 1 Gbps に指定します。 • 「2.5G」- ポート速度を 2.5 Gbps に指定します。（Copper ポートのみ） • 「5G」- ポート速度を 5 Gbps に指定します。（Copper ポートのみ） • 「10G」- ポート速度を 10 Gbps に指定します。

項目	説明
Capability Advertised	「Speed」を「Auto」に設定した場合、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」をクリックして、設定内容を適用します。

注意　本シリーズは、10Mbps をサポートしていません。

注意　手動による 100M Half モードの設定はサポートされません。オートネゴシエーションの場合、Full/Half は自動的に調整されます。

注意　4 芯 2 対のツイストペアケーブル（UTP）を使用した場合、オートネゴシエーションの設定ではリンクアップしません。

注意　SFP+ スロットはリンクパートナーの状態に関わらず、フローコントロールは常にオフです。Copper ポートはリンクパートナーの状態に関わらず、フローコントロールは常にオンです。

注意　AIR-AP1242AG-A-K9 を接続する場合、PHY 互換性の問題により速度設定を 100M に設定する必要があります。

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 の順にクリックし、以下の画面を表示します。

図 6-6　Port Status 画面

Port GBIC（ポート GBIC）

スイッチの各物理ポートの GBIC 情報について表示します。

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

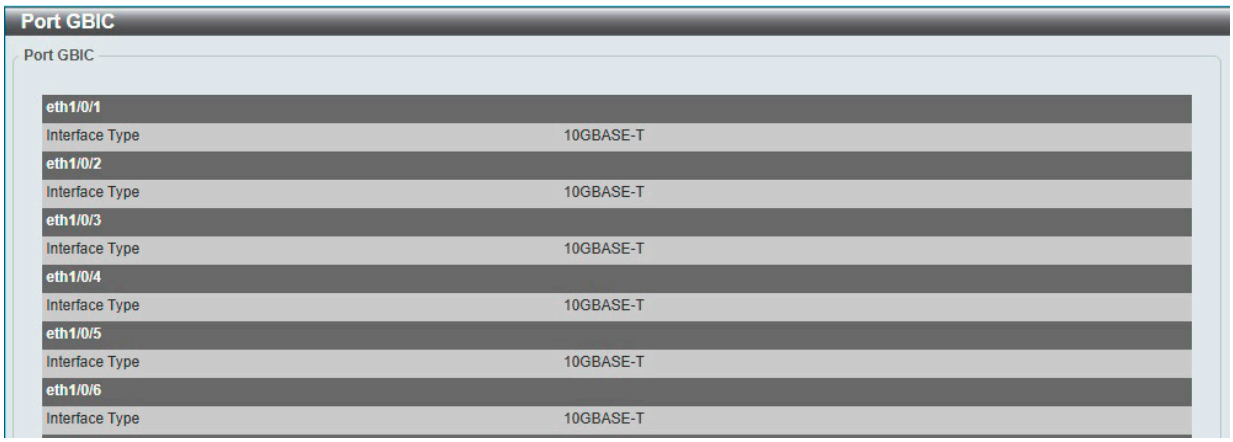


図 6-7　Port GBIC 画面

Error Disable Settings（エラーディセーブル設定）

エラー Disable は、ループバック検出などのエラーが発生したポートを Disable（無効）状態にする機能です。
本画面では、エラーの原因や Disable 状態のポートのリカバリ間隔の設定などを行います。

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

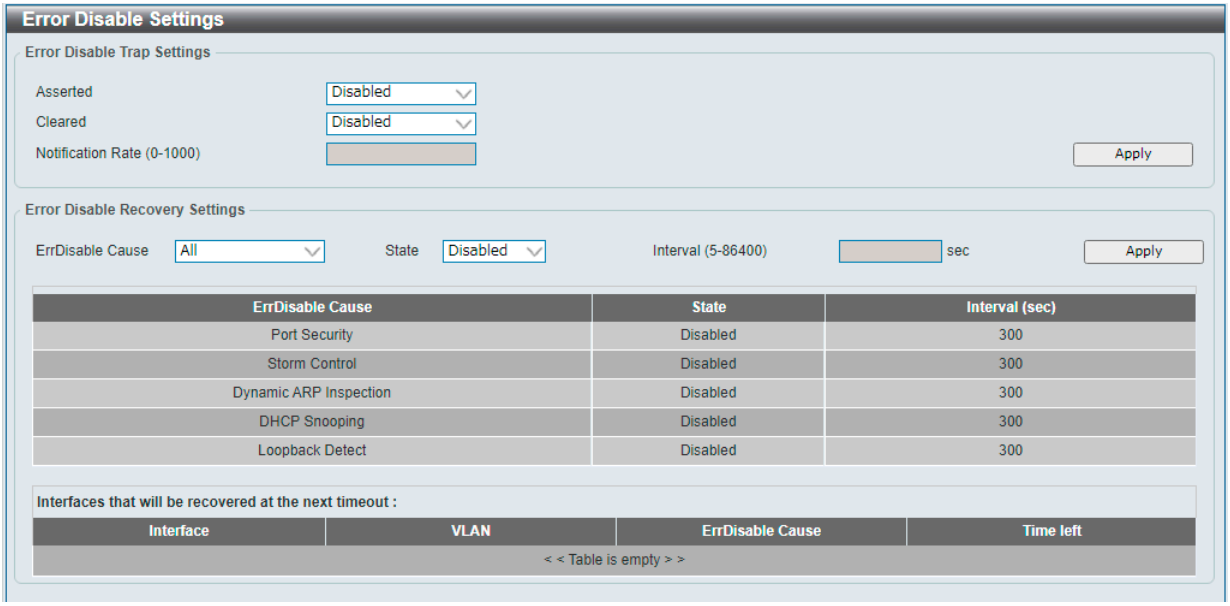


図 6-8　Error Disable Settings 画面

画面に表示される項目：

項目	説明
Error Disable Trap Settings	
Asserted	エラーディセーブル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	エラーディセーブル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	エラーディセーブルの原因を次から選択します。 • 選択肢：「All」「Port Security」「Storm Control」「Dynamic ARP Inspection」「DHCP Snooping」「Loopback Detect」
State	指定した原因によるエラーディセーブルポートの自動リカバリ機能を有効 / 無効にします。
Interval	ポートリカバリを実行する間隔を設定します。 • 設定可能範囲：5 - 86400（秒）

「Apply」をクリックして、設定内容を適用します。

Jumbo Frame（ジャンボフレーム設定）

ジャンボフレームは、1,518Byte を超えるフレームサイズを意味します。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。本シリーズでは、最大フレームサイズが 10,240 バイトまでのジャンボフレームをサポートしています。

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

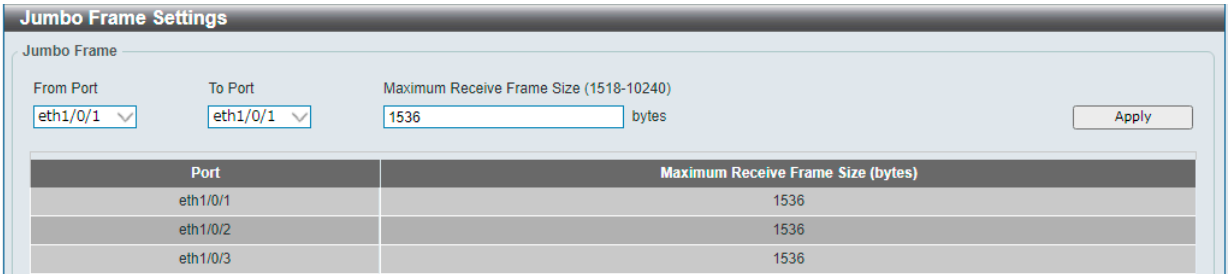


図 6-9　Jumbo Frame Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Maximum Receive Frame Size	スイッチのジャンボフレーム機能の最大値を指定します。 • 設定可能範囲：1518 - 10240（bytes） • 初期値：1536（bytes）

「Apply」をクリックして、設定内容を適用します。

注意 VLAN インタフェース経由で送信されるパケットにはジャンボフレームの設定が適用されません。

注意 802.1Q タグが含まれるパケットは、ジャンボフレームの最大値が使用されます。

PoE（PoE 設定）（DXS-1210-10MP）

DXS-1210-10MP は、IEEE802.3af/at/bt 規格の PoE 機能をサポートしています。

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

PSE 供給電力 /PD 受電電力の一覧（シングルシグネチャ）

クラス	タイプ	PSE の供給電力	PD の受電電力
0	Default, Type 1	15.4W	0.44 ～ 12.95 W
1	Type 1	4.0W	0.44 ～ 3.84 W
2	Type 1	7.0W	3.84 ～ 6.49 W
3	Type 1	15.4W	6.49 ～ 12.95 W
4（802.3at）	Type 2	30W	12.95 ～ 25.5 W
5（802.3bt）	Type 3	45W	40W
6（802.3bt）	Type 3	60W	51W

PSE 供給電力 /PD 受電電力の一覧（デュアルシグネチャ）

クラス	タイプ	PSE の供給電力	PD の受電電力
1	Type 1	8W	7.68W
2	Type 1	14W	12.98W
3（802.3at）	Type 1	30W	26W
4（802.3bt）	Type 2	60W	51W

※ 802.3bt では、シングルシグネチャとデュアルシグネチャと呼ばれる 2 種類の PD シグネチャ構成をサポートしています。PD に応じて、シングルシグネチャまたはデュアルシグネチャで動作します。
※上記の表は、100m のケーブルの場合の電力損失を考慮したものであり、ケーブル長が短い場合は受信可能電力が大きくなる場合があります。

PoE System（PoE システム設定）

デバイスの PoE 情報を参照および変更します。

PoE System Settings

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

図 6-10　PoE System 画面 - PoE System Settings タブ

画面に表示される項目：

項目	説明
PoE Perpetual	Perpetual PoE 機能を有効または無効に設定します。本機能を有効にすると、スイッチの再起動時にも受電デバイスへの PoE 供給が中断されません。
Power Budget	本スイッチの PoE 給電可能電力（総計値）を設定します。 • 初期値：370000（mw）
Usage Threshold	総使用電力のしきい値を指定します。設定したしきい値を超えた場合、SNMP トラップが送信されます。 • 設定可能範囲：1 - 99（%）
Guard Band	PoE ガードバンド（PoE 保護帯域）の設定を行います。保護帯域を確保することで、PD の電力スパイクから保護することができます。 • 設定可能範囲：0 - 15400（mw）
Policy Preempt	ポリシープリエンプトを有効 / 無効にします。 ポリシープリエンプトは、電力が不足している状態で新しくデバイスを接続した場合に、優先度の低いデバイスを切断して、新規の優先度の高いデバイスに供給する電力を確保する機能です。
Trap State	PoE イベントの通知送信を有効 / 無効にします。

「Apply」をクリックして、設定内容を適用します。

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

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

PoE System Parameters

「PoE System Parameters」タブをクリックし、以下の画面を表示します。

図 6-11　PoE System 画面 - PoE System Parameters タブ

PoE Status（PoE ステータス）

各ポートの PoE ステータスを表示します。

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

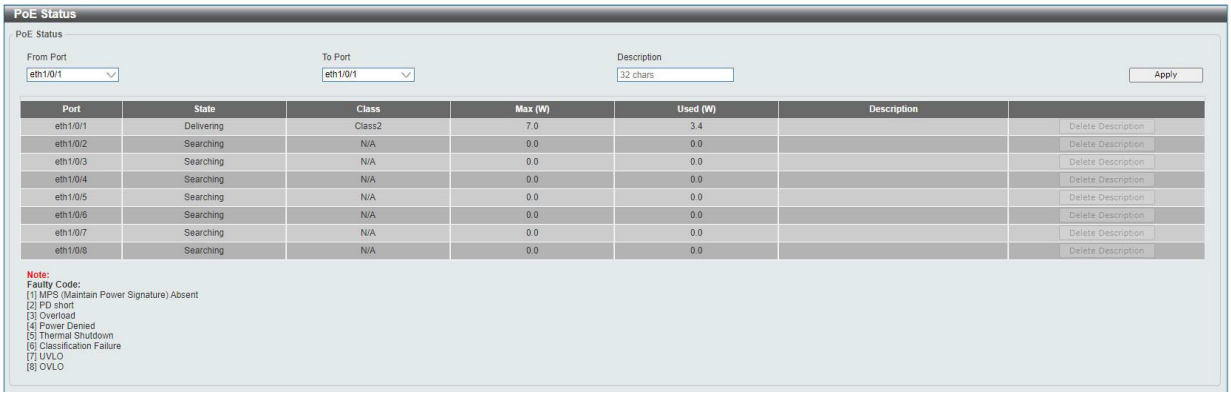


図 6-12　PoE Status 画面

以下の項目を設定します。

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Description	PoE インタフェースに接続されている PD（受電デバイス）についての説明を入力します。（32 文字以内）

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

テーブルには、以下の項目が表示されます。

項目	説明
Port	PoE 対応のインタフェースを表示します。
Status	インタフェースの現在の状態を表示します。 • ステータス：「Disabled」「Searching」「Requesting」「Delivering」「Time-based Off」「Failure（障害の内容）」

項目	説明
Class	現在の PD クラス分類を表示します。IEEE 802.3af/at/bt PoE 規格に準拠したスイッチでは Class 0 ～ 6 に対応しています。
Max (W)	クラス分類に基づく最大電力を表示します。
Used (W)	インタフェースの現在の電力使用量を表示します。
Description	設定した説明文を表示します。

PoE Configuration（PoE 設定）

PoE ポートの優先度、電力量、タイムレンジなどの設定を行います。

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

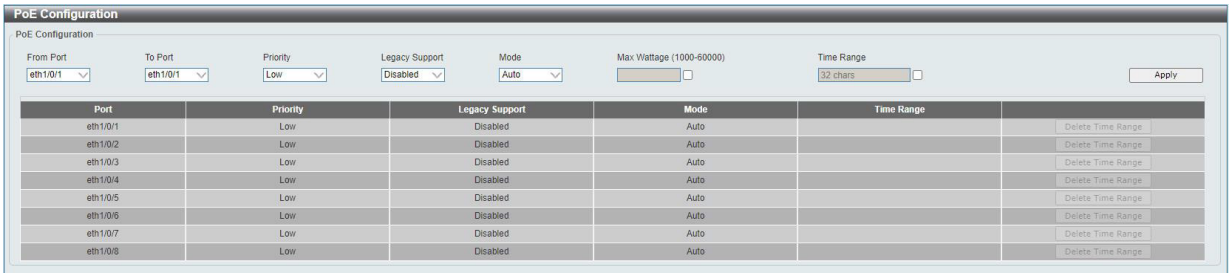


図 6-13　PoE Configuration 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Priority	ポートの優先度を指定します。ポート優先度はシステムがどのポートに優先的に電力供給を行うかを設定します。 • 選択肢：「Critical」「High」「Low」
Legacy Support	レガシー PD（受電機器）のサポートを有効 / 無効にします。
Mode	PoE ポートの電力管理モードを選択します。 • 選択肢：「Auto」「Never」
Max Wattage	本項目は「Mode」で「Auto」を選択した場合に表示されます。チェックボックスにチェックを入れ、自動検出 PD へ供給する最大電力を指定します。数値を設定しない場合、PD のクラスによって、供給可能な電力が自動的に決定されます。 • 設定可能範囲：1000 - 60000（mw）
Time Range	本項目は「Mode」で「Auto」を選択した場合に表示されます。チェックボックスにチェックを入れ、タイムレンジを入力します。タイムレンジは、ポートの PoE 機能を有効にする時間を指定します。

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

注意　「Time Range」の時間範囲外の再起動において、起動処理中は一時的に給電されます。

注意　「Priority」、「Legacy Support」、「MAX Wattage」を変更すると、PoE による給電が一度停止します。

PoE Statistics（PoE 統計）

PoE の統計情報を表示します。

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

図 6-14　PoE Statistics 画面

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

注意　未給電時は「Invalid Signature」の値が上昇し続けます。

PoE Measurement（PoE 計測）

PoE の計測情報を表示します。

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

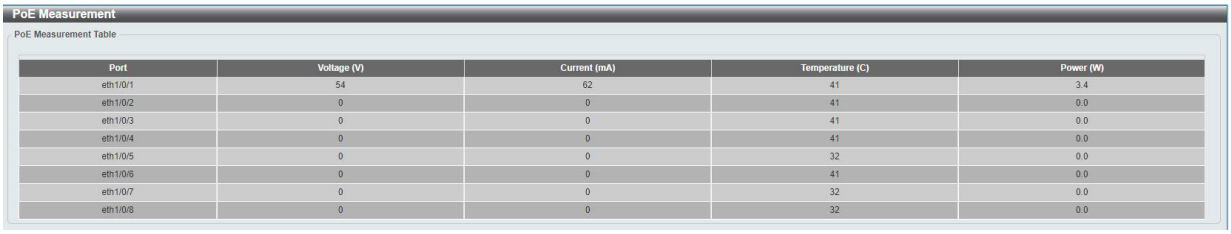


図 6-15　PoE Measurement 画面

PD Alive（PD アライブ）

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

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

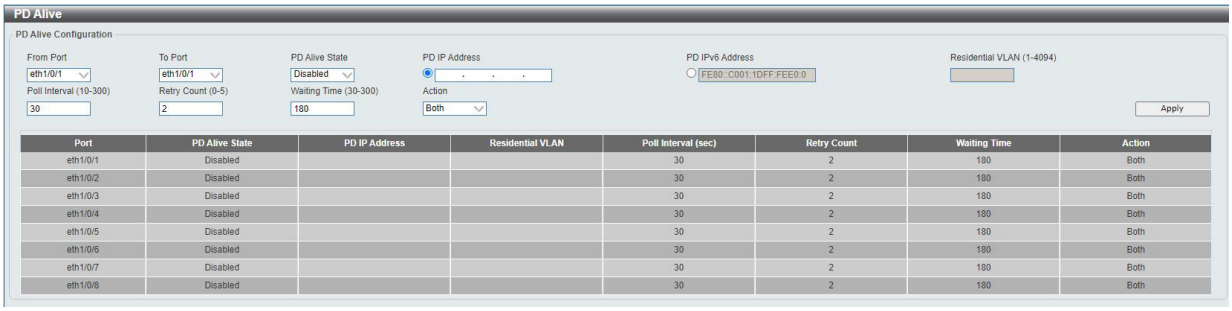


図 6-16　PD Alive 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
PD Alive State	PD アライブ機能を有効 / 無効にします。
PD IP Address	PD の IPv4 アドレスを指定します。
PD IPv6 Address	PD の IPv6 アドレスを指定します。
Residential VLAN	IPv6 リンクローカル宛先の VLAN ID を入力します。
Poll Interval	ポーリング間隔を指定します。ポーリング間隔は、指定の PD の状況を確認するために Ping を送信する間隔です。 • 設定可能範囲：10 - 300（秒） • 初期値：30（秒）
Retry Count	リトライ回数を指定します。リトライ回数は、指定の PD から応答がなかった際に Ping を再送信する回数です。 • 設定可能範囲：0 - 5 • 初期値：2
Waiting Time	待機時間を指定します。待機時間は、リセットアクションが実行された後、その PD に ping メッセージを送信する前にシステムが待機する時間です。 • 設定可能範囲：30 - 300（秒） • 初期値：180（秒）
Action	実行する動作を指定します。 • 「Reset」- PoE ポートをリセットします。（一旦 PoE をオフにし、再度オンにします。） • 「Notify」- 管理者に通知するログとトラップを送信します。 • 「Both」- 管理者に通知するログとトラップを送信し、PoE ポートをリセットします。（一旦 PoE をオフにし、再度オンにします。）

「Apply」をクリックして、設定内容を適用します。

System Log（システムログ）

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 の順にクリックし、以下の画面を表示します。

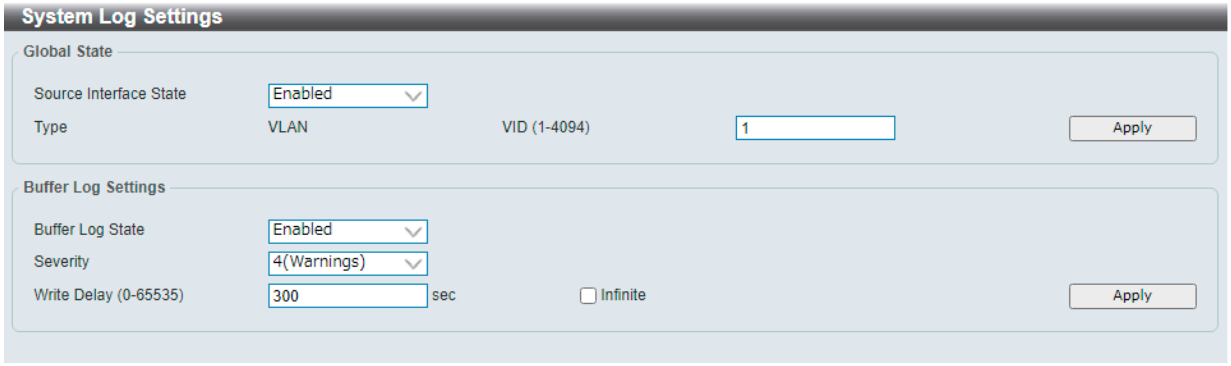


図 6-17　System Log Settings 画面

画面に表示される項目：

項目	説明
Global State	
Source Interface State	送信元インタフェースのステータスを有効 / 無効に指定します。
Type	インタフェースの種類が表示されます。
VID	VLAN ID を指定します。 • 設定可能範囲：1 - 4094
Buffer Log Settings	
Buffer Log State	バッファログのステータスを指定します。 • 選択肢：「Enabled」「Disabled」
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）
Write Delay	フラッシュにロギングバッファを定期的に書き込む間隔を指定します。 「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 - 65535（秒） • 初期値：300（秒）

「Apply」をクリックして、設定内容を適用します。

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

システムログサーバの設定を行います。

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

図 6-18　System Log Server Settings 画面

画面に表示される項目：

項目	説明
IPv4 Address	システムログサーバの IPv4 アドレスを設定します。
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： 「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）
Facility	ログ出力されるファシリティの番号を選択します。 • 設定可能範囲：0 - 23

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

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックすると指定のエントリが削除されます。

System Log（システムログ）

システムログの閲覧 / 消去を行います。

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

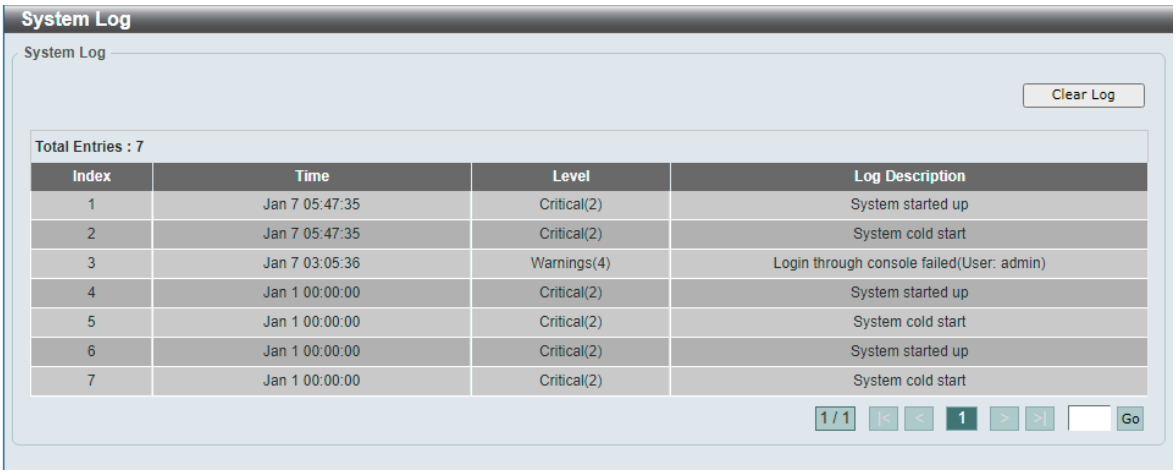


図 6-19　System Log 画面

「Clear Log」をクリックし、表示画面内のすべてのエントリをクリアします。
複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

Time and SNTP（時刻・SNTP 設定）

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（時刻設定）

スイッチの時刻設定を行います。

注意　本シリーズはリアルタイムクロック（RTC）を持っていないため、手動で設定する場合は、再起動後時刻を再設定する必要があります。

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。

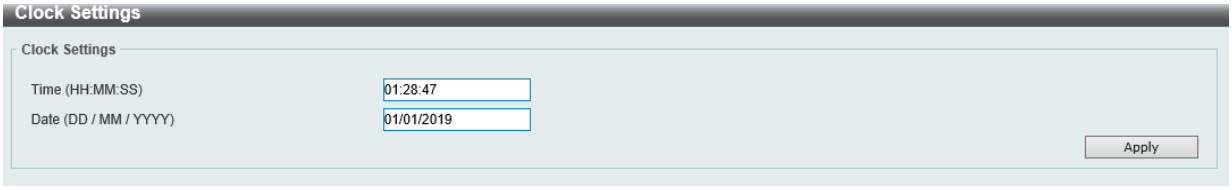


図 6-20　Clock Settings 画面

画面に表示される項目：

項目	説明
Time	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	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」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 の順にクリックし、以下の設定画面を表示します。

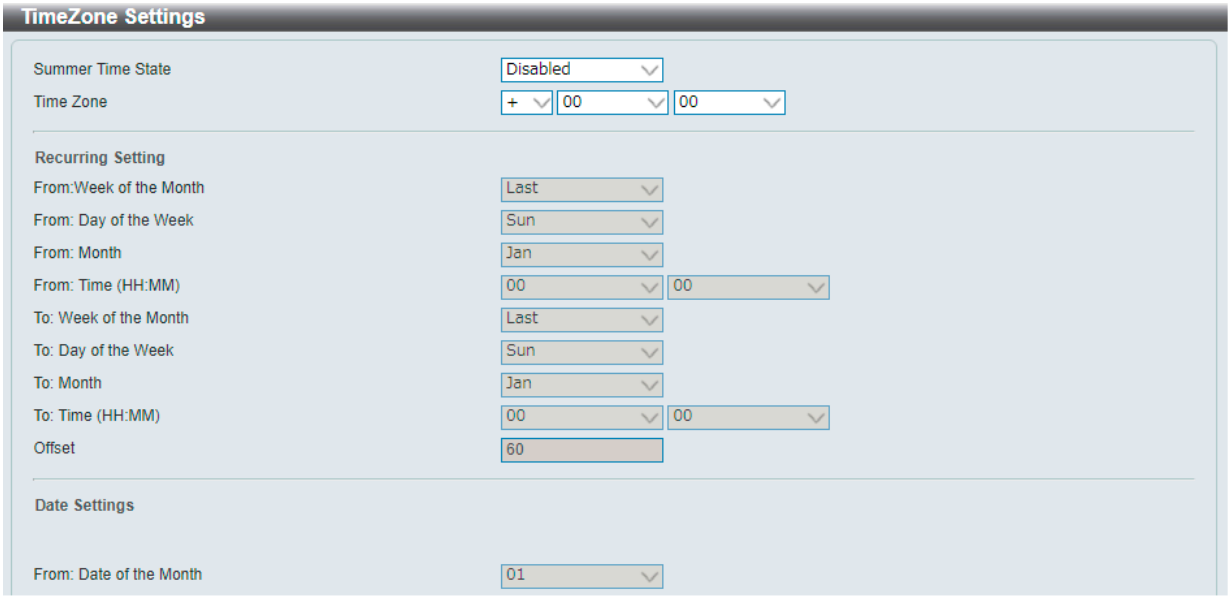


図 6-21　Time Zone Settings 画面

画面に表示される項目：

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）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に指定	
From: Week of the Month	月の第何週からサマータイムを開始するかを設定します。
From: Day of the Week	サマータイムを開始する曜日を指定します。 • 選択肢：「Sun」「Mon」「Tue」「Wed」「Tue」「Fri」「Sat」
From: Month	サマータイムを開始する月を指定します。 • 選択肢：「Jan」「Feb」「Mar」「Apr」「May」「Jun」「Jul」「Aug」「Sep」「Oct」「Nov」「Dec」
From: Time (HH:MM)	サマータイムを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。
To: Day of the Week	サマータイムを終了する曜日を指定します。
To: Month	サマータイムを終了する月を指定します。
To: Time (HH:MM)	サマータイムを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	
サマータイムの開始 / 終了月日を指定します。	
From: Date of the Month	サマータイムを開始する日にちを指定します。
From: Month	サマータイムを開始する月を指定します。
From: Year	サマータイムを開始する年を指定します。
From: Time (HH:MM)	サマータイムを開始する時間を指定します。
To: Date of the Month	サマータイムを終了する日にちを指定します。
To: Month	サマータイムを終了する月を指定します。
To: Year	サマータイムを終了する年を指定します。

項目	説明
To: Time (HH:MM)	サマータイムを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」をクリックして、設定内容を適用します。

SNTP Settings（SNTP 設定）

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

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

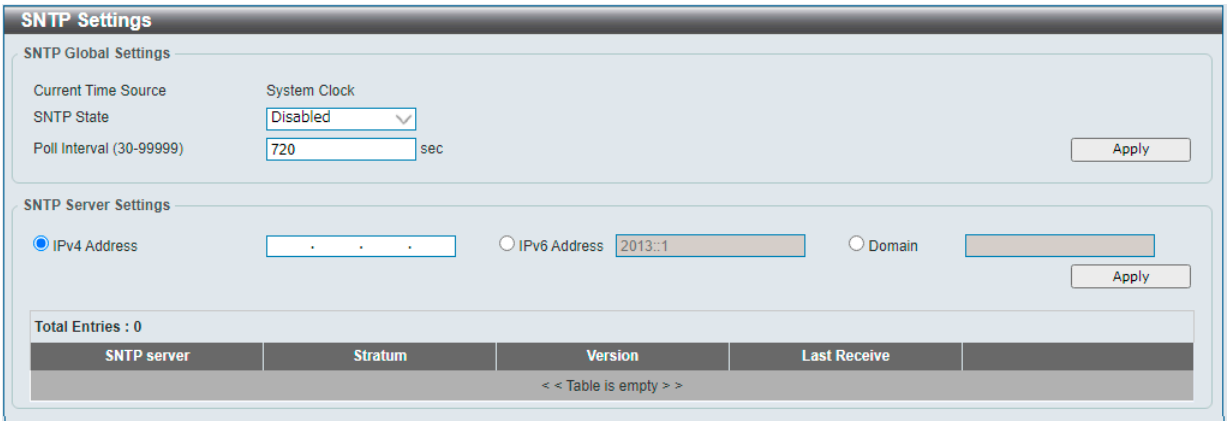


図 6-22　SNTP Settings 画面

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 を有効 / 無効にします。
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 SNTP 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 SNTP サーバの IPv6 アドレスを設定します。
Domain	SNTP 情報の取得元である SNTP サーバのドメイン名を設定します。

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

注意　「Poll Interval」は、正常応答時に適用されます。正常な応答がない場合、RFC4330 に従い、exponential-backoff algorithm に基づき再送間隔を伸ばします。

注意　SNTP の設定について、DNS を使用し、FQDN で SNTP サーバを指定する場合、AAAA レコードはサポートされません。

注意　リアルタイムクロックを内蔵していないため、起動もしくは再起動した後、時刻同期を再開します。

Time Range（タイムレンジ設定）

スイッチのタイムレンジを設定します。

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

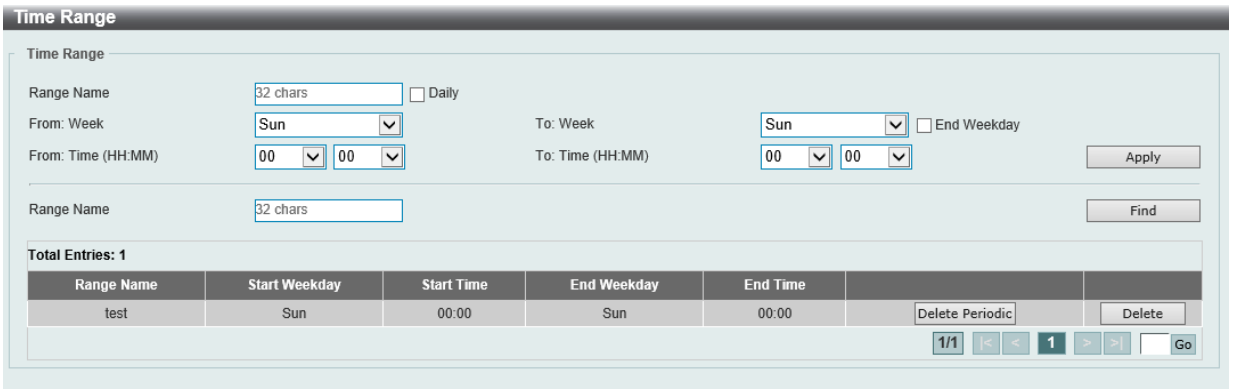


図 6-23　Time Range 画面

画面に表示される項目：

項目	説明
Range Name	タイムレンジのプロファイル名を入力します。（32 文字以内）
From: Week /To: Week	タイムレンジに使用する「始まり」と「終わり」の曜日を指定します。 「Daily」にチェックを入れると「毎日」がタイムレンジとして指定されます。 「End Weekday」にチェックを入れると「始まり」に指定された日から週の最後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」をクリックして、設定内容を適用します。

関連情報を入力して「Find」をクリックすると指定のエントリを検索できます。

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

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

第 7 章　Management（スイッチの管理）

以下は、Management サブメニューです。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
User Accounts Settings（ユーザアカウント設定）	ユーザアカウントの作成と設定を行います。有効なユーザアカウントを表示可能です。
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。
SNMP（SNMP 設定）	SNMP を使用してスイッチを管理します。
RMON（RMON 設定）	スイッチの SNMP 機能に対するリモートモニタリング（RMON）の設定を行います。
DHCP Auto Configuration（DHCP 自動コンフィグ設定）	DHCP 自動設定機能の設定を行います。
Telnet / Web（Telnet /Web 設定）	スイッチの Telnet 設定と Web 設定を行います。
Session Timeout（セッションタイムアウト）	セッションタイムアウトの設定を行います。
D-Link Discovery Protocol Settings（D-Link ディスカバリプロトコル設定）	D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

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

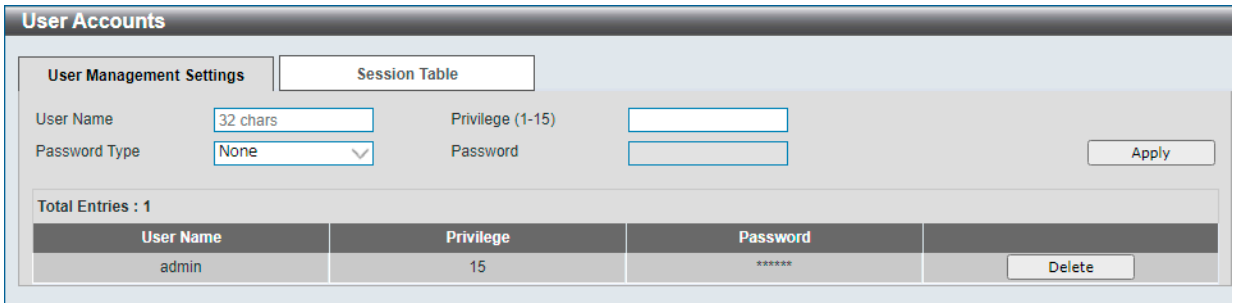


図 7-1　User Accounts - User Management Settings 画面

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	このアカウントの権限レベルを選択します。 • 設定可能範囲：1 - 15 本スイッチでは、以下のユーザアカウント権限レベルがサポートされています。 • Basic User（基本ユーザ）：本項目の設定値を「1」にした場合、基本的なシステムの設定・表示が可能です。 • Operator（オペレータ）：本項目の設定値を「12」にした場合、ユーザアカウントや SNMP アカウント設定以外のシステム設定・表示が可能です。 • Administrator（管理者）：本項目の設定値を「15」にした場合、すべてのシステム設定・表示が可能です。
Password Type	アカウントで使用するパスワードの暗号化の方法を選択します。 • 「None」- ユーザアカウントにパ Encrypted スワードを指定しません。 • 「Plain Text」- プレーンテキストでパスワードを指定します。 • 「Encrypted-SHA1」- SHA1 暗号化形式でパスワードを指定します。 • 「Encrypted-MD5」- MD5 暗号化形式でパスワードを指定します。
Password	パスワードタイプで「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」を選択した場合、ユーザアカウントで使用するパスワードを入力します。

「Apply」をクリックして、設定内容を適用します。
削除するエントリ横の「Delete」をクリックすると該当エントリは削除されます。

注意　ユーザ名に” root” を設定することはできません。

■ **Session Table**

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

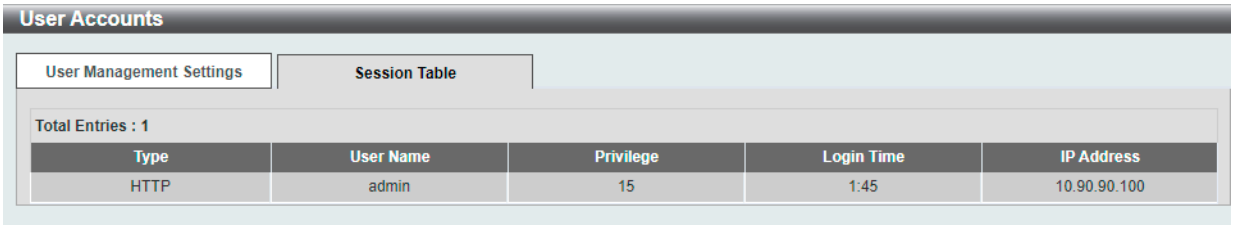


図 7-2　User Accounts - Session Table 画面

Password Encryption（パスワード暗号化）

パスワードを暗号化して設定ファイルに保存します。

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

図 7-3　Password Encryption 画面

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。

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 グローバル設定とトラップ設定を行います。

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

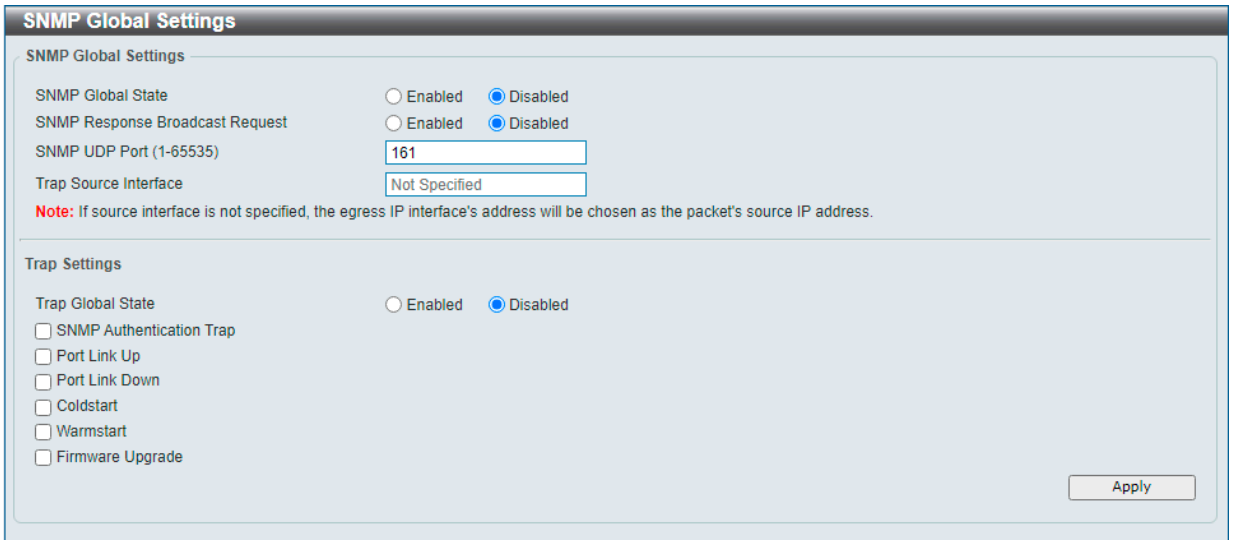


図 7-4　SNMP Global Settings 画面

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	ブロードキャストの SNMP GetRequest パケットに対するサーバの応答を有効 / 無効に指定します。
SNMP UDP Port	SNMP UDP ポート番号を指定します。 • 設定可能範囲：1 - 65535 • 初期値：161
Trap Source Interface	SNMP トラップパケットの送信元インタフェースを指定します。このインタフェースの IP アドレスがトラップの送信元アドレスとして使用されます。
Trap Settings	
Trap Global State	SNMP トラップを有効 / 無効にします。
SNMP Authentication Trap	SNMP 認証失敗の通知を有効 / 無効に設定します。 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。SNMPv3 の場合、不正な SHA/MD5 認証キーでパケットが構成されている時に認証に失敗します。
Port Link Up	ポートリンクアップ通知を有効 / 無効に設定します。 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 / 無効に設定します。 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 / 無効に設定します。
Warmstart	warmStart 通知を有効 / 無効に設定します。
Firmware Upgrade	ファームウェアのアップグレード通知を有効 / 無効に設定します。

「Apply」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できるかを定義するために使用します。

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

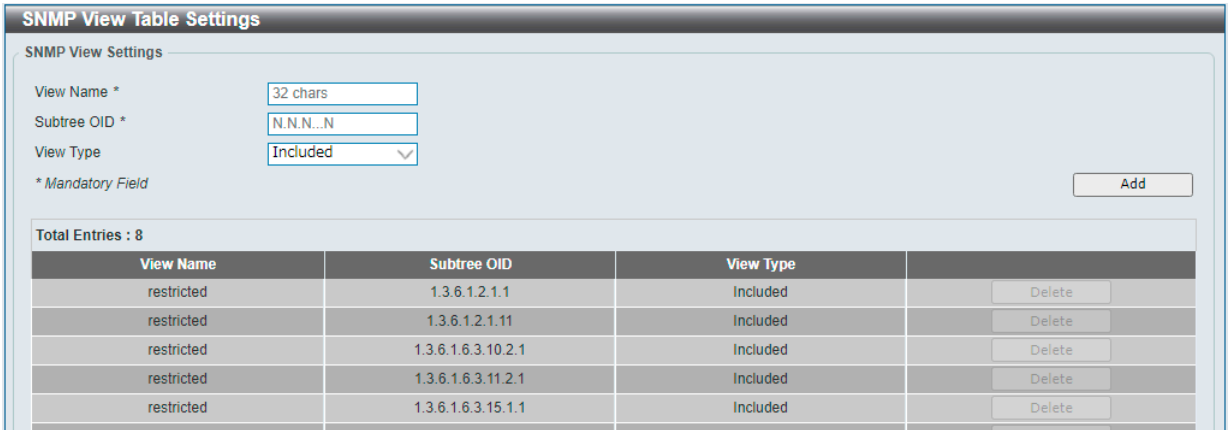


図 7-5　SNMP View Table Settings 画面

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 により、SNMP マネージャによってアクセス可能なオブジェクトツリー（MIB ツリー）範囲かどうかを識別します。
View Type	「Subtree OID」で指定した OID が、SNMP マネージャがアクセス可能な範囲であるかを指定します。 • 「Included」- SNMP マネージャがアクセスできるオブジェクトのリストにこのオブジェクトを含めます。 • 「Excluded」- SNMP マネージャがアクセスできるオブジェクトのリストにこのオブジェクトを含めません。

「Add」をクリックして SNMP ビューを追加します。
「Delete」をクリックすると指定のエントリが削除されます。

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

SNMP コミュニティ名を設定します。
コミュニティ名は、スイッチの SNMP 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。

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 7-6　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。

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） 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 Settings」で定義されている必要があります。
Access Right	アクセス権を以下から選択します。 • 「Read Only」- 指定したコミュニティ名を使用する 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です。 • 「Read Write」- 指定したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りおよび書き込みが可能です。
IP Access-List Name	ユーザを制限するために使用するアクセスリストの名前を入力します。 許可されるユーザは、コミュニティ文字列を使用して SNMP にアクセスすることができます。

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

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

SNMP グループを登録します。
本グループは、SNMP ユーザ（「SNMP User Table Settings（SNMP ユーザテーブル設定）」）と SNMP ビューテーブル（「SNMP View Table Settings（SNMP ビューテーブル設定）」）で設定するビューを関連付けます。

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

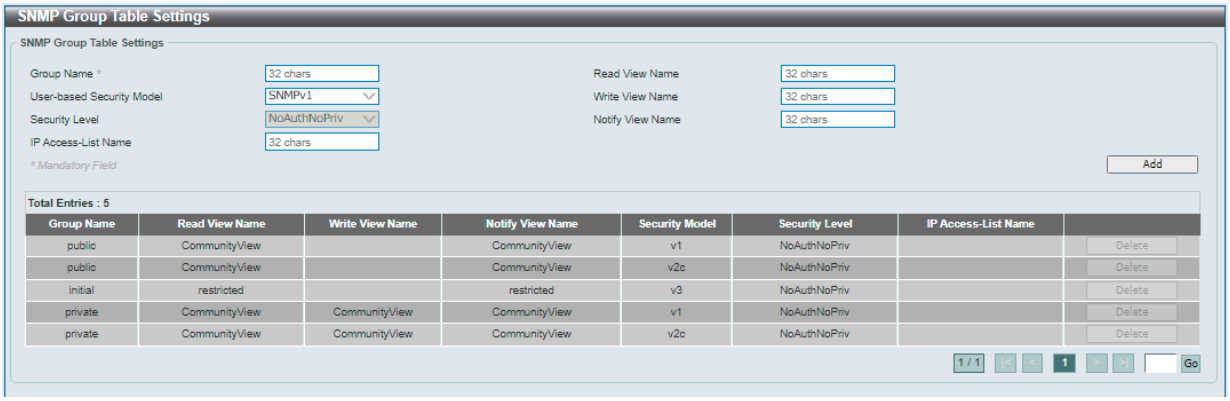


図 7-7　SNMP Group Table Settings 画面

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。（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	SNMP バージョン 3 を選択した場合に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は認証も暗号化もされません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、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、認証と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 ビュー名を入力します。
Write View Name	グループのユーザがアクセス可能な Write ビュー名を入力します。
Notify View Name	グループのユーザがアクセス可能な Notify ビュー名を入力します。 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。

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

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

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 の順にクリックし、以下の画面を表示します。

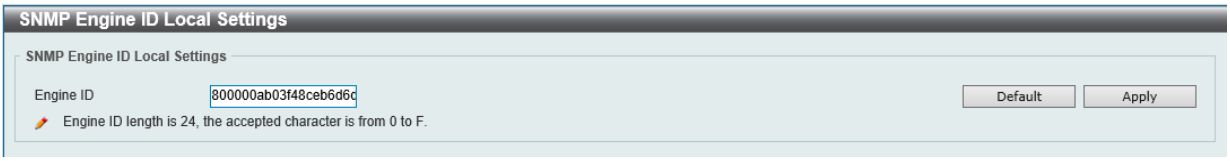


図 7-8　SNMP Engine ID Local Settings 画面

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」をクリックします。
「Default」をクリックすると、エンジン ID は初期値に戻ります。

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

SNMP ユーザの登録、表示を行います。

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

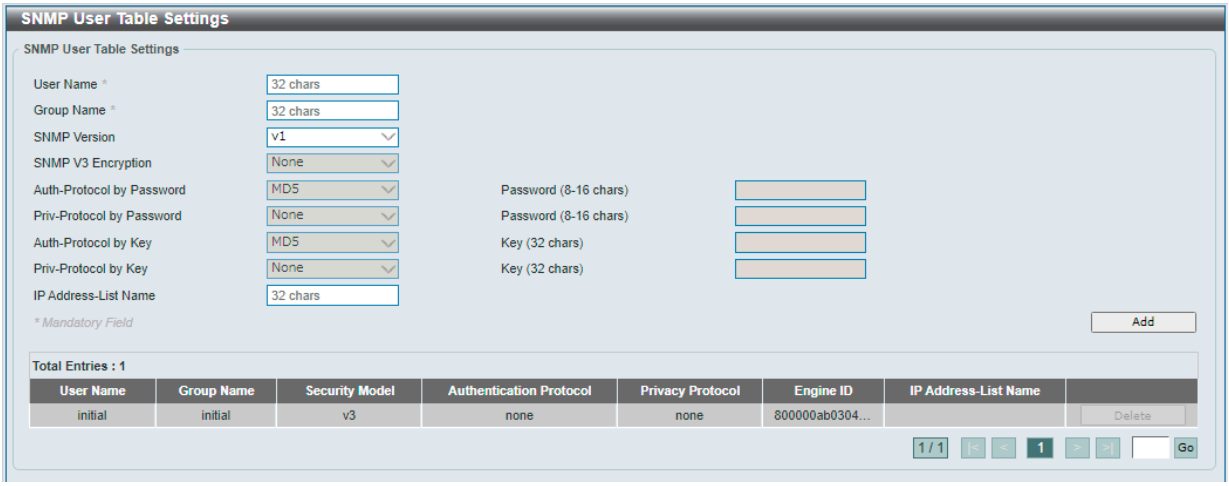


図 7-9　SNMP User Table Settings 画面

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 バージョンを選択します。 • 選択肢：「v1」「v2c」「v3」
SNMP V3 Encryption	SNMP バージョンで「v3」を選択した場合、SNMP v3 の暗号化の設定を行います。 • 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。 以下から認証プロトコルを選択後、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。（パスワード：8-16 文字以内） • 「SHA」- HMAC-SHA 認証プロトコルが使用されます。（パスワード：8-20 文字以内）
Priv-Protocol by Password	「SNMP V3 Encryption」で「Password」を選択した場合に有効になります。 以下からプライバシープロトコルを選択後、パスワードを入力します。 • 「None」- 認証プロトコルは使用されません。 • 「DES56」- CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されます。（パスワード：8-16 文字以内）
Auth-Protocol by Key	「SNMP V3 Encryption」で「Key」を選択した場合に有効になります。 以下から認証プロトコルを選択後、キーを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。（キー：32 文字） • 「SHA」- HMAC-SHA 認証プロトコルが使用されます。（キー：40 文字）

項目	説明
Priv-Protocol by Key	「SNMP V3 Encryption」で「Key」を選択した場合に有効になります。 以下からプライバシープロトコルを選択後、キーを入力します。 • 「None」- 認証プロトコルは使用されません。 • 「DES56」- CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されます。（キー：32 文字）
IP Access-List Name	ユーザに関連付ける標準 IP アクセスコントロールリストの名前を入力します。

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

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

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

SNMP トラップの送信先を登録します。

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

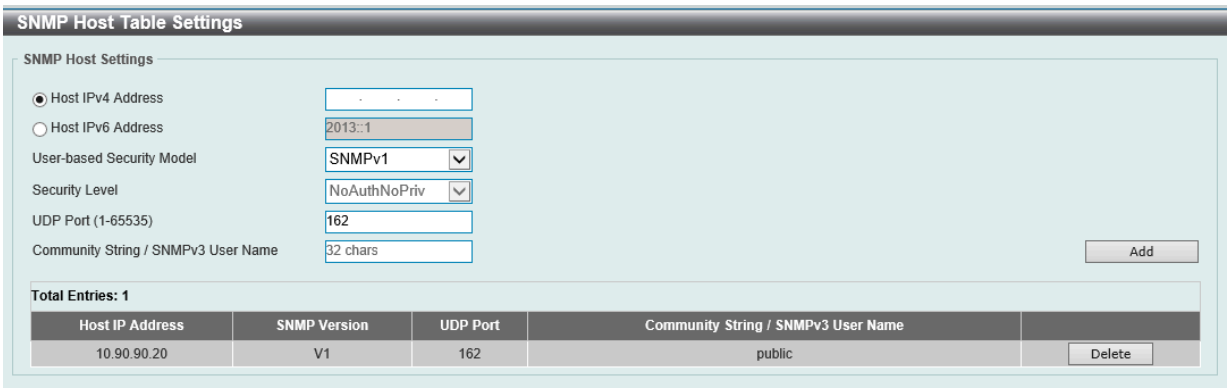


図 7-10　SNMP Host Table Settings 画面

画面に表示される項目：

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv6 アドレスを入力します。
User-based Security Model	管理ホストの 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	SNMP バージョンで「SNMPv3」を指定した場合、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」をクリックしてエントリを追加します。
「Delete」をクリックしてエントリを削除します。

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 の順にクリックし、以下の画面を表示します。

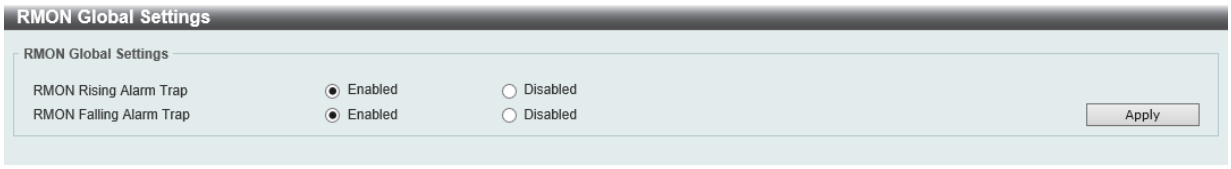


図 7-11　RMON Global Settings 画面

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」をクリックして、設定内容を適用します。

RMON Statistics Settings（RMON 統計設定）

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。

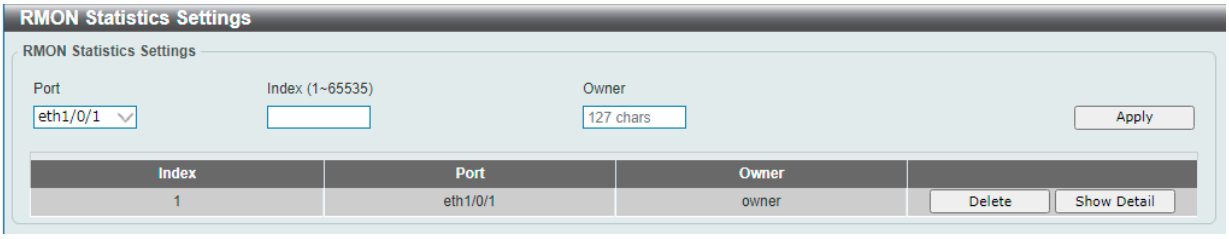


図 7-12　RMON Statistics Settings 画面

画面に表示される項目：

項目	説明
Port	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	オーナ名を入力します。（127 文字以内） RMON 情報を要求する RMON ステーションまたはユーザを入力します。

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

指定ポートの統計情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

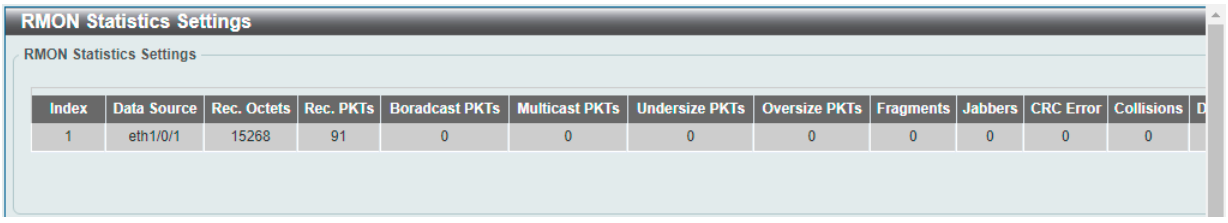


図 7-13　RMON Statistics Settings - Show Detail 画面

前の画面に戻るには、「Back」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 の順にクリックし、以下の画面を表示します。

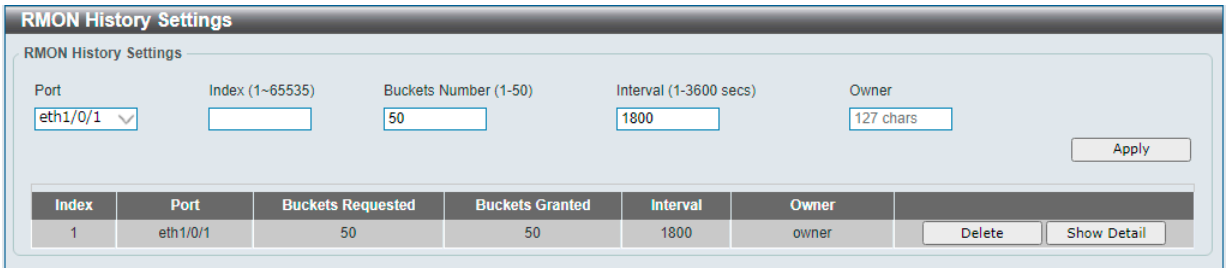


図 7-14　RMON History Settings 画面

画面に表示される項目：

項目	説明
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
Buckets 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 - 50 • 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） • 初期値：1800（秒）
Owner	オーナの文字列を入力します。（127 文字以内） RMON 情報を要求する RMON ステーションまたはユーザを入力します。

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

指定ポートの履歴情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

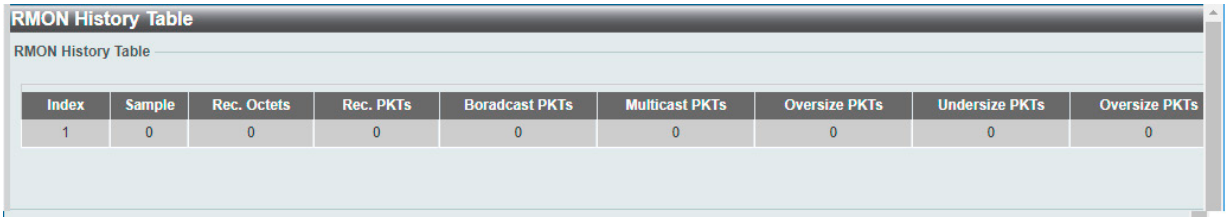


図 7-15　RMON History Table 画面

前の画面に戻るには、「Back」をクリックします。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

RMON Alarm Settings（RMON アラーム設定）

インタフェースをモニタするためのアラームエントリを表示、設定します。
ネットワークアラームは、ネットワークの問題またはイベントが検出されたときに発生します。

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

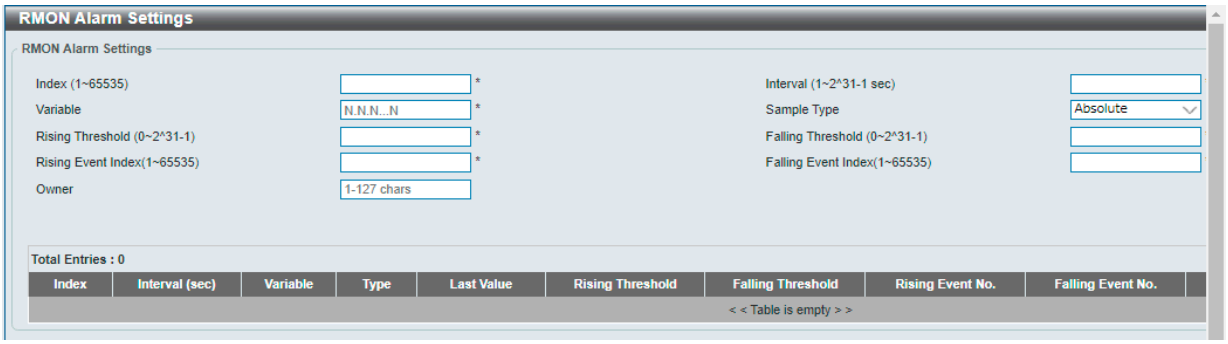


図 7-16　RMON Alarm Settings 画面

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	サンプリングする変数のオブジェクト識別子を入力します。
Sample Type	モニタリングのタイプを選択します。 •「Absolute」- サンプリング値がしきい値と直接比較されます。 •「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。
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 Index	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、上昇しきい値を超えてもアクションを実行しません。
Falling Event Index	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、下降しきい値を下回ってもアクションを実行しません。
Owner	オーナ名を入力します。（127 文字以内）

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

RMON Event Settings（RMON イベント設定）

RMON イベントの設定を行います。

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

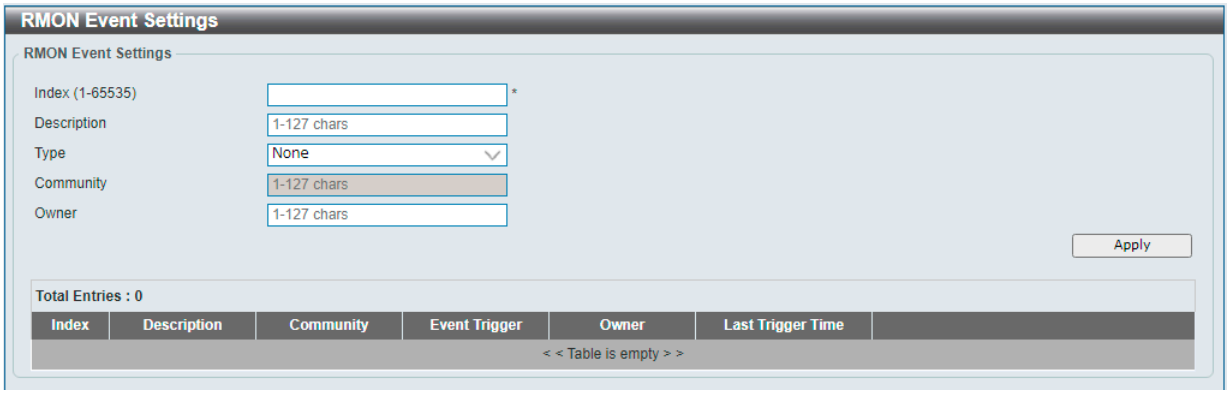


図 7-17　RMON Event Settings 画面

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。 • 「SNMP Trap」- トラップを送信します。 • 「Log and Trap」- ログを出力し、トラップを送信します。
Community	イベントタイプで「SNMP Trap」または「Log and Trap」を指定した場合、イベントが属する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）

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

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。

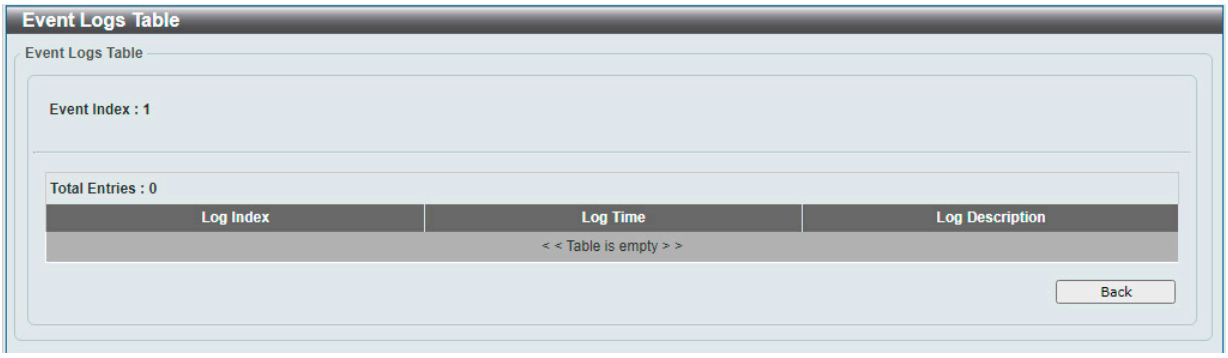


図 7-18　Event Logs Table 画面

前の画面に戻るには、「Back」をクリックします。

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 サーバからの設定ファイルの自動ダウンロードを有効または無効にすることができます。再起動時に、DHCP 自動設定が有効になっている場合、デバイスは TFTP サーバの設定ファイルを取得します。

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。

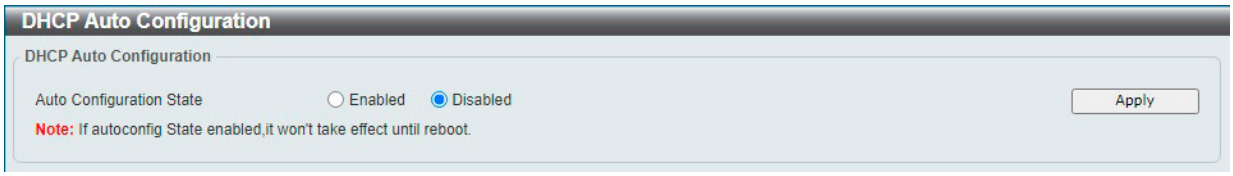


図 7-19　DHCP Auto Configuration 画面

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。

Telnet / Web（Telnet /Web 設定）

スイッチの Telnet/Web 設定を行います。

Management > Telnet/Web の順にクリックし、以下の画面を表示します。

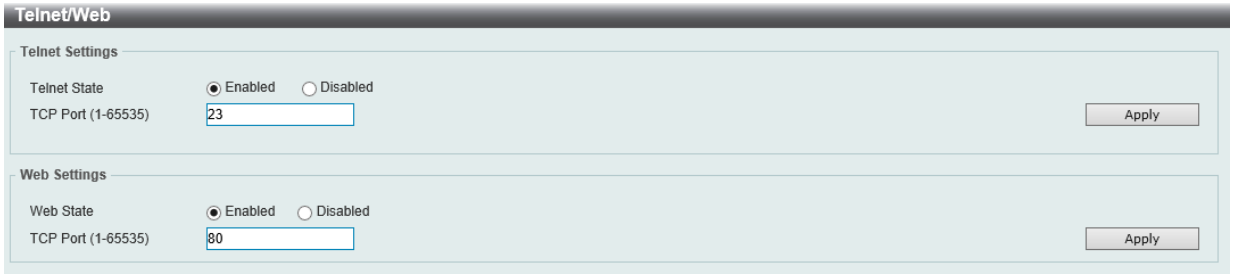


図 7-20　Telnet/Web 画面

画面に表示される項目：

項目	説明
Telnet Settings	
Telnet State	Telnet 経由での設定を有効 / 無効に設定します。
TCP Port	スイッチの Telnet 管理に使用する TCP ポート番号を入力します。Telnet プロトコルに通常使用される TCP ポートは 23 です。 • 設定可能範囲：1 - 65535
Web Settings	
Web State	Web ベースでの設定を有効 / 無効に設定します。
Port	スイッチの Web 管理に使用される TCP ポート番号を指定します。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」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、コンソール、Telnet）のタイムアウトの設定をします。

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

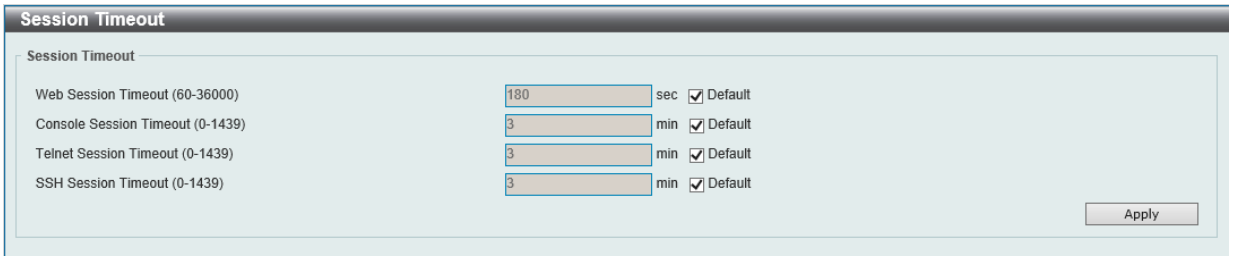


図 7-21　Session Timeout 画面

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（秒）を設定します。 「Default」にチェックを入れると初期値に戻ります。 • 設定可能範囲：60 - 36000（秒） • 初期値：180（秒）
Console Session Timeout	コンソールセッションのタイムアウト時間（分）を設定します。 「Default」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 - 1439（分） • 初期値：30（分）
Telnet Session Timeout	Telnet セッションのタイムアウト時間（分）を設定します。 「Default」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 - 1439（分） • 初期値：30（分）
SSH Session Timeout	SSH セッションのタイムアウト時間（分）を設定します。 「Default」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 - 1439（分） • 初期値：30（分）

「Apply」をクリックして、設定内容を適用します。

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

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

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

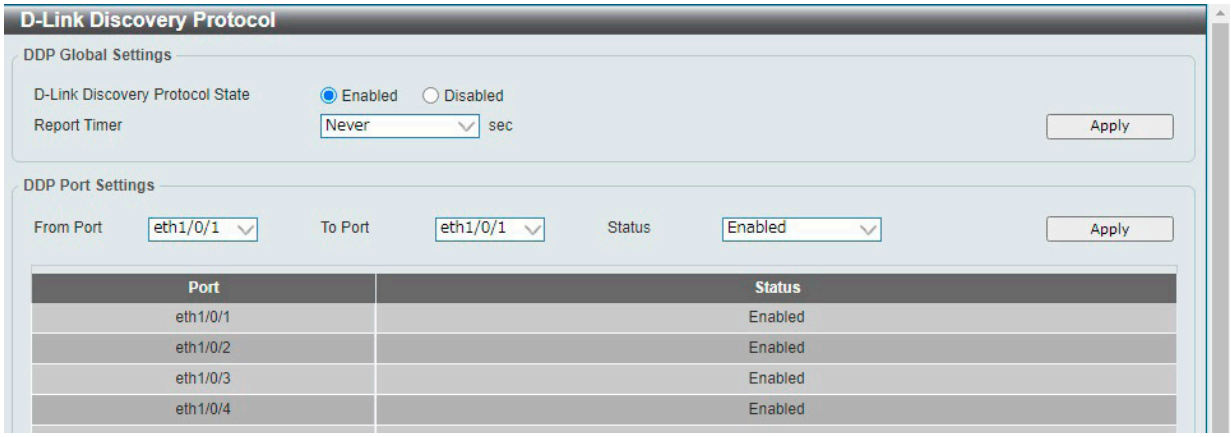


図 7-22　D-Link Discovery Protocol 画面

画面に表示される項目：

項目	説明
DDP Global Settings	
D-Link Discovery Protocol State	DDP のグローバルステータスを有効 / 無効に設定します。
Report Timer	DDP レポートメッセージの送信間隔を以下から指定します。 • 選択肢：「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	
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。

第 8 章　L2 Features（レイヤ 2 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 Configuration Wizard（VLAN 設定ウィザード）	ウィザードを使用して VLAN の設定を行います。
802.1Q VLAN（802.1Q VLAN 設定）	802.1Q VLAN の設定を行います。
Asymmetric VLAN（Asymmetric VLAN 設定）	Asymmetric VLAN の設定を行います。
VLAN Interface（VLAN インタフェース設定）	VLAN インタフェースの設定を行います。
GVRP（GVRP の設定）	GVRP（GARP VLAN Registration Protocol）の設定を行います。
Auto Surveillance VLAN（自動サーベイランス VLAN）	自動サーベイランス VLAN の設定を行います。
Voice VLAN（音声 VLAN）	音声 VLAN の設定を行います。
STP（スパニングツリーの設定）	スパニングツリープロトコル（STP）設定を行います
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。
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（LLDP 設定）	LLDP（Link Layer Discovery Protocol）の設定を行います。

FDB（FDB 設定）

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

補足　FDB で登録可能な MAC アドレス数は 32K です。

注意　"no mac-address-table static" コマンドを使用した際に、MAC アドレス形式が不正（区切りなし）によりエントリを削除できない場合でも、エラーメッセージが表示されませんのでご注意ください。

Static FDB（スタティック FDB 設定）

Unicast Static FDB（ユニキャストスタティック FDB 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 の順にクリックし、以下の画面を表示します。

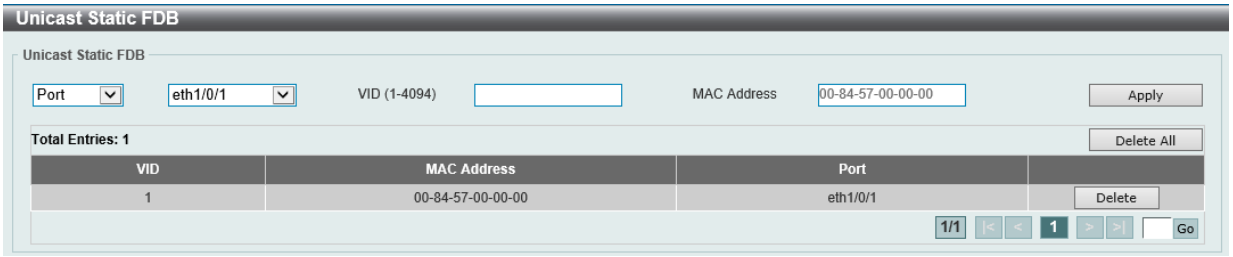


図 8-1　Unicast Static FDB 設定

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。
Port Number	「Port」を選択した場合、ポート番号を入力します。
VID	指定のユニキャスト MAC アドレスが所属する VLAN ID を入力します。 • 設定可能範囲：1 - 4094

項目	説明
MAC Address	ユニキャストパケットが送信される宛先の MAC アドレスを入力します。または、破棄する MAC アドレスを入力します。 ユニキャスト MAC アドレスを指定する必要があります。

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

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

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

スイッチにスタティックなマルチキャストフォワーディングを設定します。

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

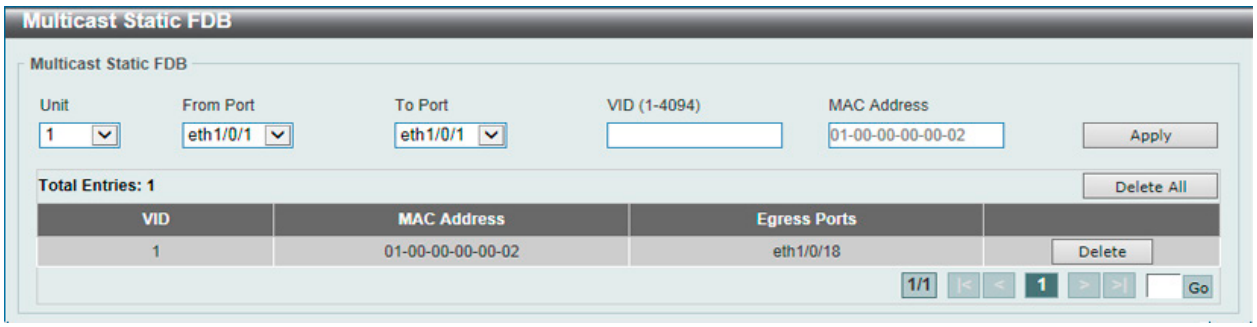


図 8-2　Multicast Static FDB 画面

画面に表示される項目：

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。
VID	指定のマルチキャスト MAC アドレスが所属する VLAN の VLAN ID を入力します。 • 設定可能範囲：1 - 4094
MAC Address	マルチキャストパケットが送信される宛先の MAC アドレスを入力します。マルチキャスト MAC アドレスを指定する必要があります。宛先 MAC アドレスのフォーマットは「01-XX-XX-XX-XX-XX」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。
「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。

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）

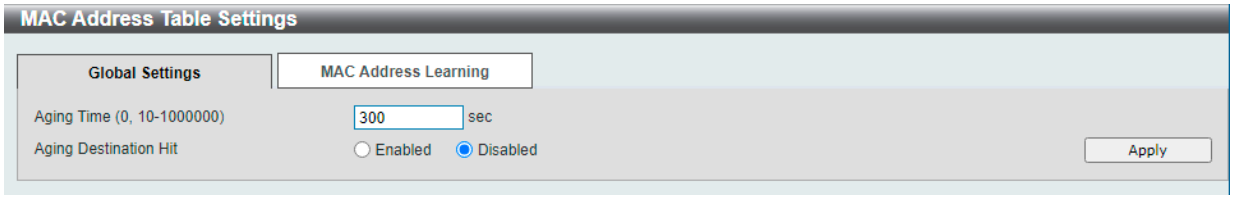


図 8-3　MAC Address Table Settings - Global Settings タブ画面

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。 設定した時間内にアクセスのない端末について、学習した MAC アドレスを MAC アドレステーブルから削除します。 • 設定可能範囲：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。

項目	説明
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」をクリックして、設定内容を適用します。

Address Learning（MAC アドレスラーニングタブ）

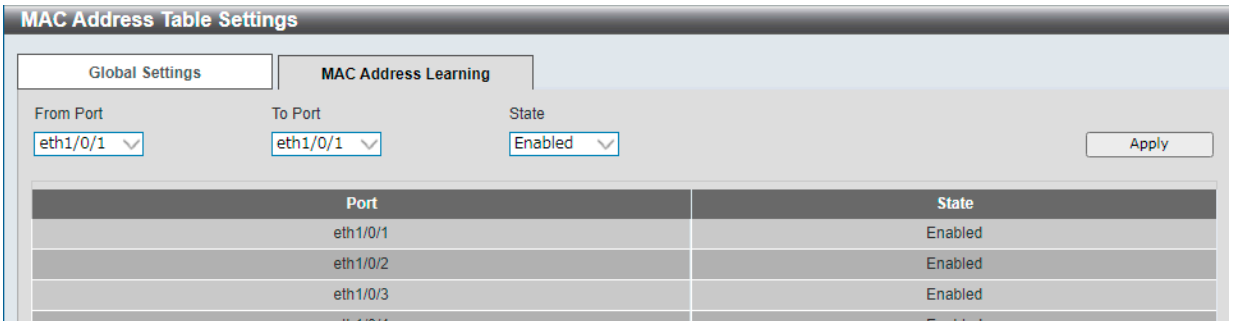


図 8-4　MAC Address Table Settings - MAC Address Learning タブ画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Status	指定したポートの MAC アドレス学習機能を有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

注意　多数の異なる MAC アドレスの学習が発生する状況において、アドレス更新キューの輻輳が発生し、一部 MAC アドレスの学習が行われない場合があります。

注意　MAC アドレス学習が無効の場合、学習済み MAC アドレスは即時削除、未登録 MAC アドレスからの通信は遮断されます。

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。

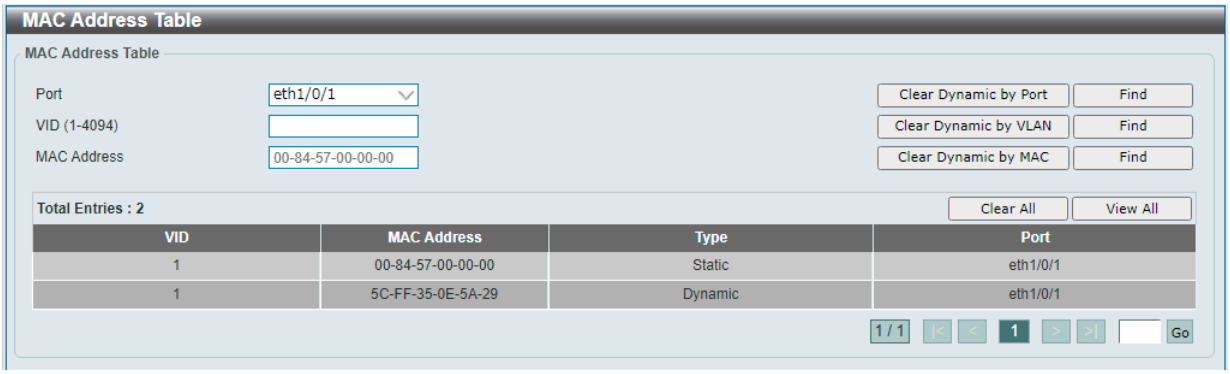


図 8-5　MAC Address Table 画面

画面に表示される項目：

項目	説明
Port	表示またはクリアするエントリのポート番号を指定します。
VID	表示またはクリアするエントリの VLAN ID を入力します。
MAC Address	表示またはクリアするエントリの MAC アドレスを入力します。

エントリの検索 / 表示

「Find」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。
「View All」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/VLAN/MAC）」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」をクリックして、アドレステーブルのすべてのエントリを削除します。

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

注意　MAC アドレステーブルには自身の VLAN インタフェースの MAC アドレスは表示されません。

注意　Asymmetric VLAN 有効時、MAC アドレステーブルの VID は N/A 表示となります。

注意　CLI 上で、FDB テーブル上の VLAN 情報が正しく表示されない場合があります。

MAC Notification（MAC 通知設定）

MAC Notification（MAC 通知）の表示、設定を行います。MAC エントリが学習または削除されたときに通知します。

MAC Notification Settings タブ

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

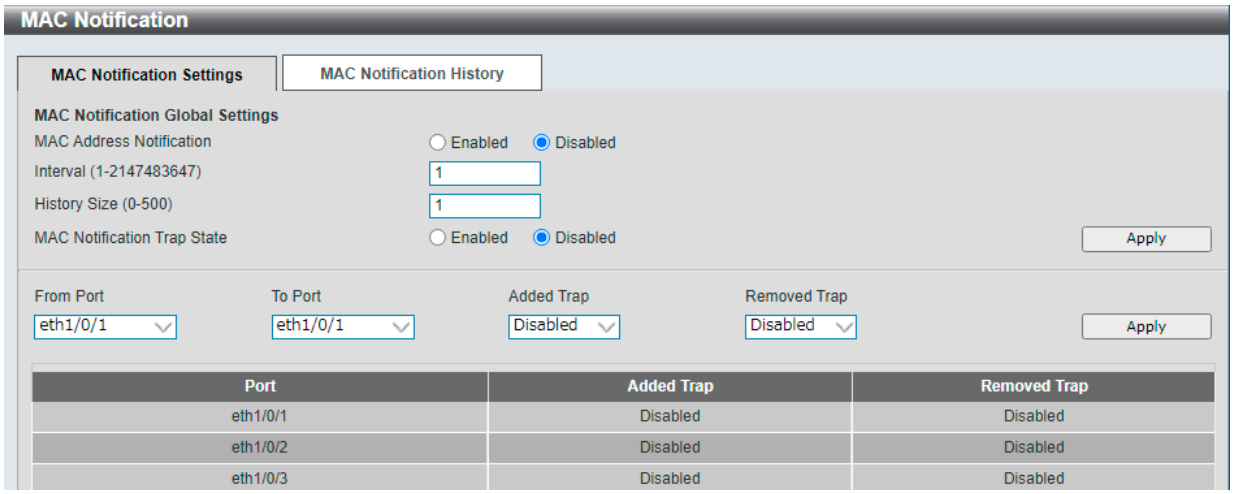


図 8-6　MAC Notification - MAC Notification Settings 画面

画面に表示される項目：

項目	説明
MAC Address Notification	スイッチ上の MAC 通知を有効 / 無効に設定します。
Interval	通知を行う間隔を設定します。 • 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設定します。 • 設定可能範囲：0 - 500 • 初期値 : 1
MAC Notification Trap State	MAC 通知トラップを有効 / 無効に設定します。
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	選択したポートで MAC エントリが追加された際のトラップを有効 / 無効に設定します。
Removed Trap	選択したポートで MAC エントリが削除された際のトラップを有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

MAC Notification History タブ

右側の「MAC Notification History（MAC 通知履歴）タブをクリックします。

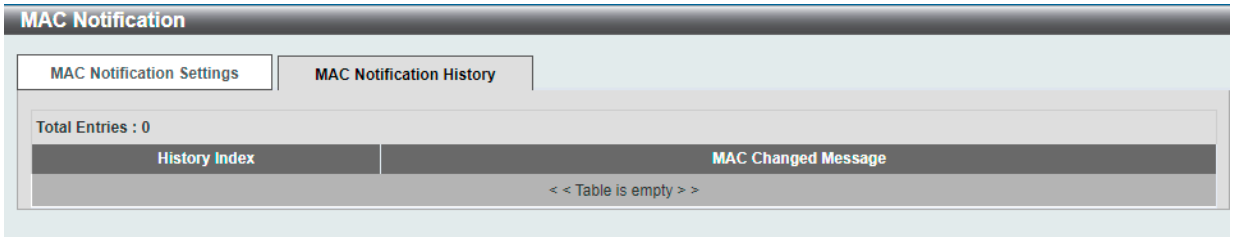


図 8-7　MAC Notification - MAC Notification History 画面

MAC 通知メッセージの履歴が表示されます。

VLAN について

IEEE 802.1p プライオリティについて

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

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

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

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

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

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

VLAN とは

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

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

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

本スイッチシリーズにおける VLAN について

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

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

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

IEEE 802.1Q VLAN

用語の説明

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

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

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

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

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

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

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

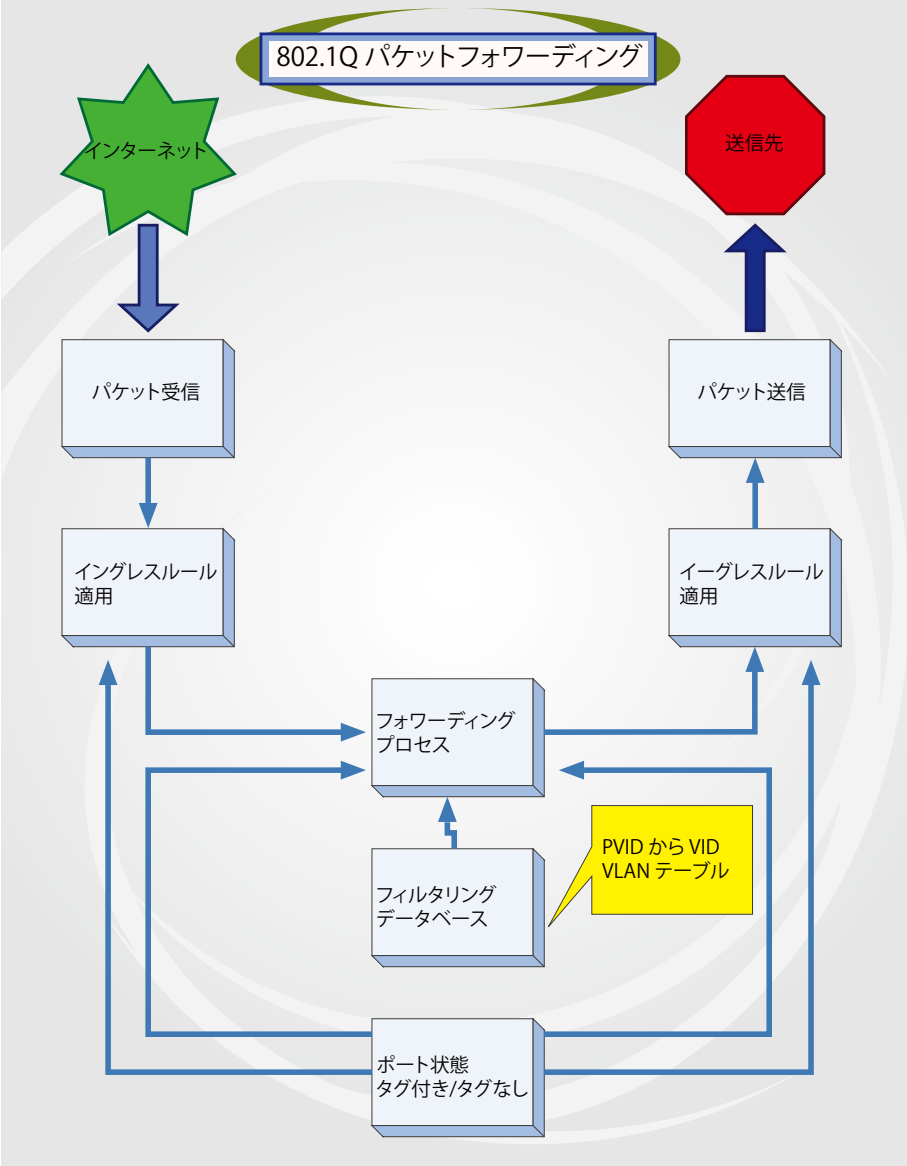


図 8-1　IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

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

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

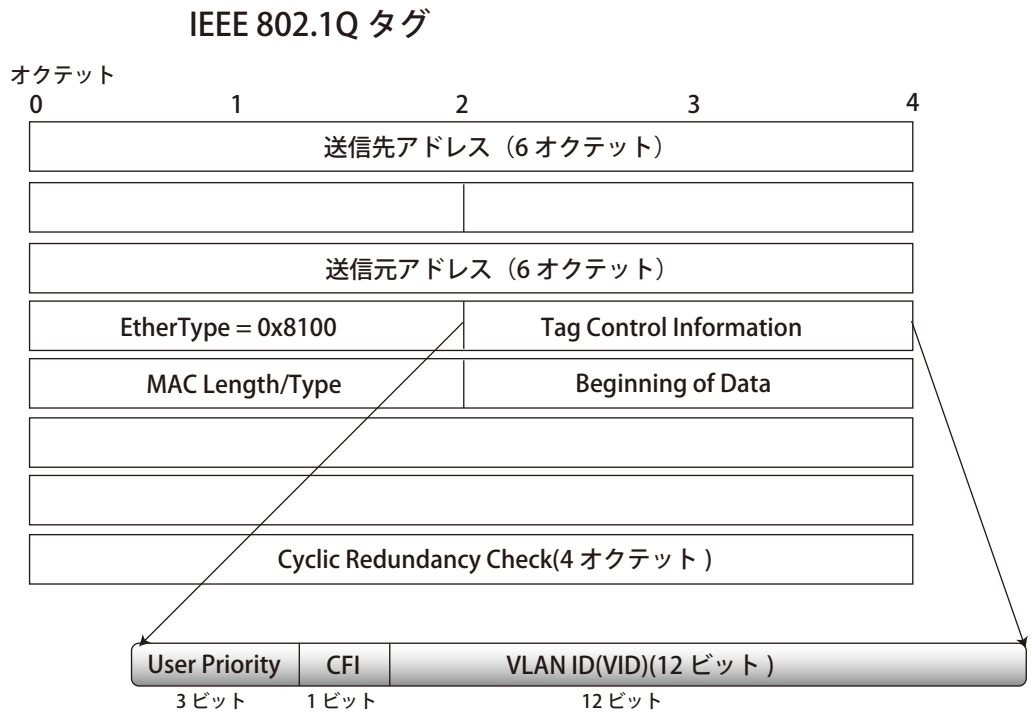


図 8-2　IEEE 802.1Q タグ

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

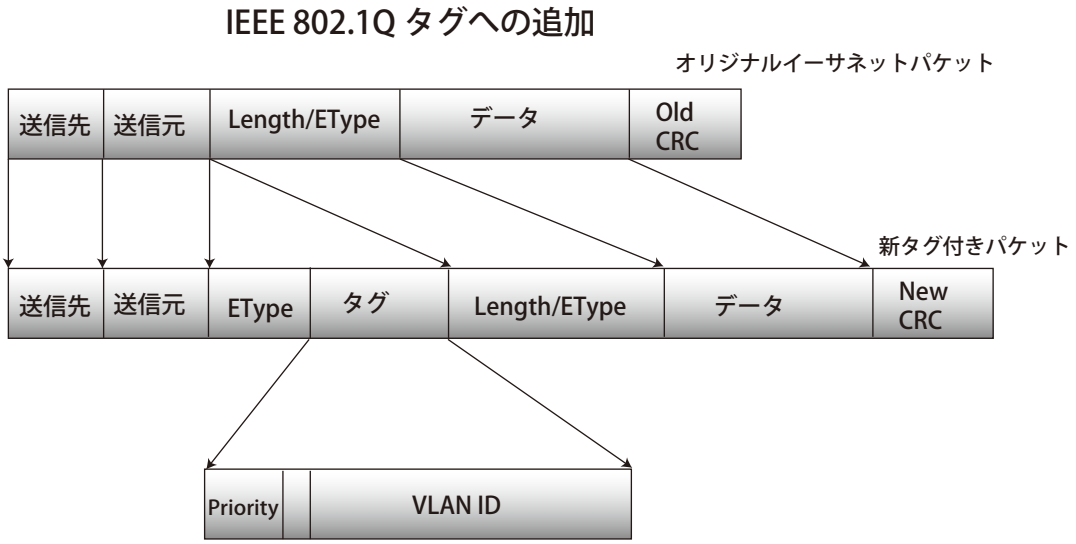


図 8-3　IEEE 802.1Q タグの挿入

ポート VLAN ID

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

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

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

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

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

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

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

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

タグ付きとタグなし

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

イングレスフィルタリング

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

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

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

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

デフォルト VLAN

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

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

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

VLAN の設定例を以下に示します。

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

ポートベース VLAN

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

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

VLAN セグメンテーション

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

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

図 8-4　VLAN Configuration Wizard 画面

画面に表示される項目：

項目	内容
Create VLAN	新しく VLAN を作成する場合に選択します。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。

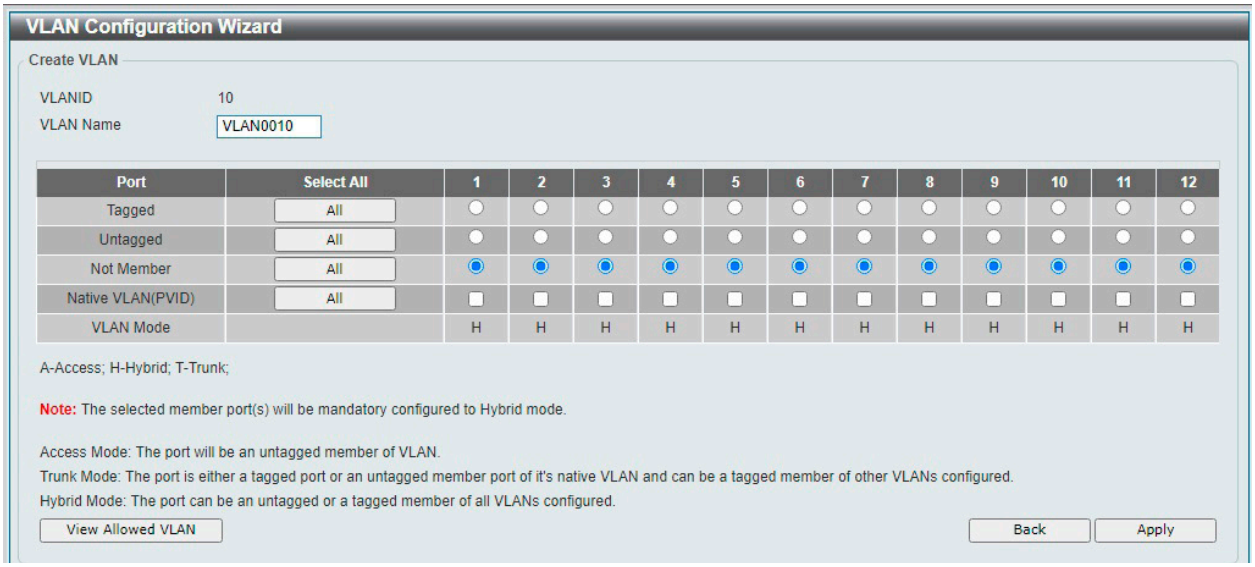


図 8-5　VLAN Configuration Wizard 画面

画面に表示される項目：

項目	内容
VID	選択した VID が表示されます。
VLAN Name	VLAN 名を入力します。
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。
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。

「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。

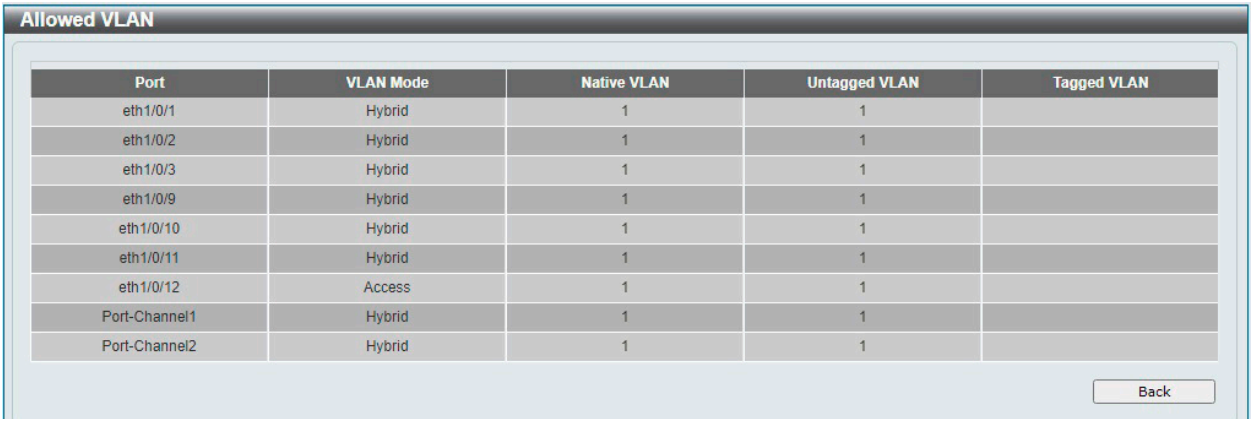


図 8-6　Allowed VLAN 画面

802.1Q VLAN（802.1Q VLAN 設定）

802.1Q VLAN を設定します。

L2 Features > 802.1Q VLAN の順にクリックし、次の画面を表示します。

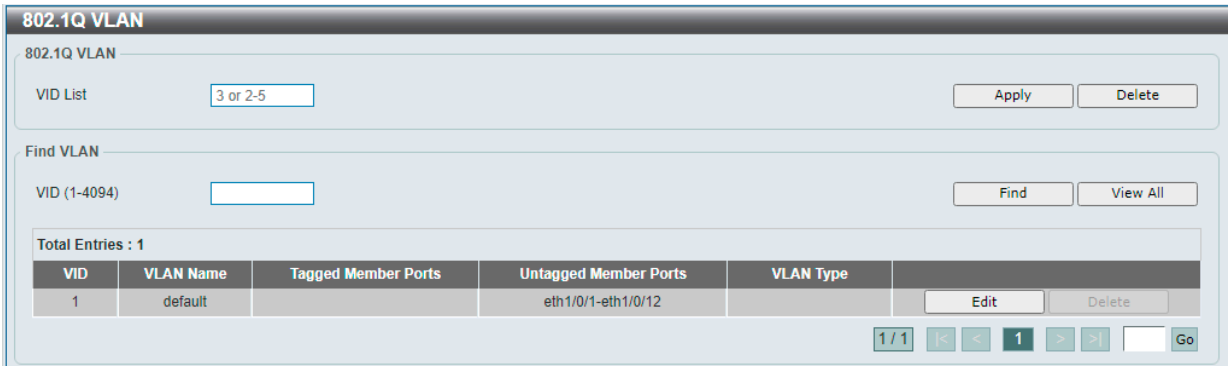


図 8-7　802.1Q VLAN 画面

画面に表示される項目：

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

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

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

Asymmetric VLAN（Asymmetric VLAN 設定）

Asymmetric VLAN（非対称 VLAN）の設定を行います。
非対称 VLAN は、それぞれ異なった VLAN に所属するクライアントから、サーバやファイアウォールなどのリソースを共有させる機能です。

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

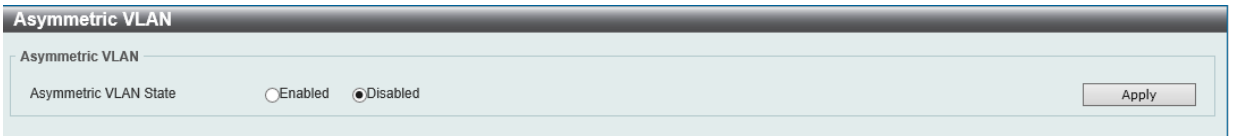


図 8-8　Asymmetric VLAN 画面

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

「Apply」をクリックして、設定内容を適用します。

VLAN Interface（VLAN インタフェース設定）

VLAN インタフェースの設定を行います。

L2 Features > VLAN 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、および編集を実行できます。

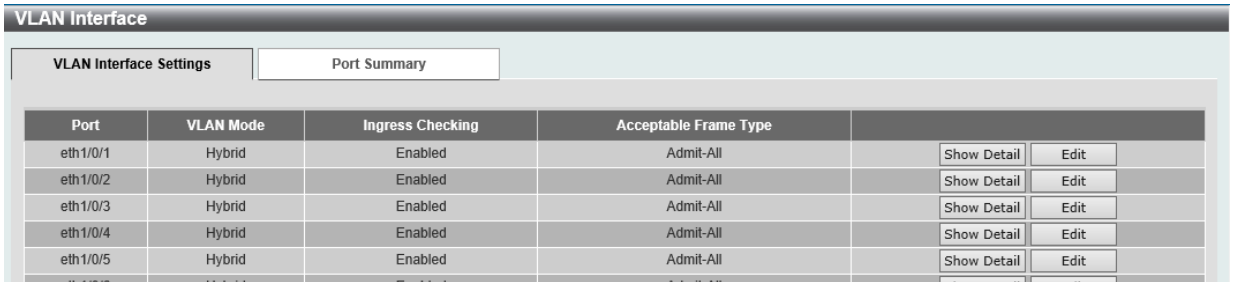


図 8-9　VLAN Interface 画面

「VLAN Detail」をクリックして、指定インタフェースの VLAN について詳細情報を表示します。
「Edit」をクリックして、指定エントリの編集をします。

■ VLAN 詳細情報の表示

「VLAN Detail」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 8-10　VLAN Interface Information 画面

「Back」をクリックすると前画面に戻ります。

■ 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 モードは以下です。

- 「Access」「Hybrid」「Trunk」

● **VLAN モード「Access」を選択した場合：**

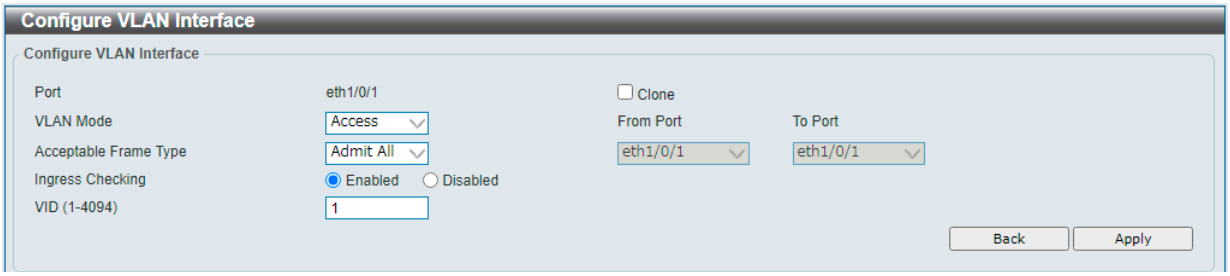


図 8-11　Configure VLAN Interface - Access 画面

画面に表示される項目：

項目	説明
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを選択します。ここでは「Access」を選択します。
Acceptable Frame Type	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
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。
From Port / To Port	設定内容をコピーするポートの範囲を指定します。

「Apply」をクリックして、設定内容を適用します。
「Back」をクリックすると前画面に戻ります。

● **VLAN モード「Hybrid」を選択した場合：**

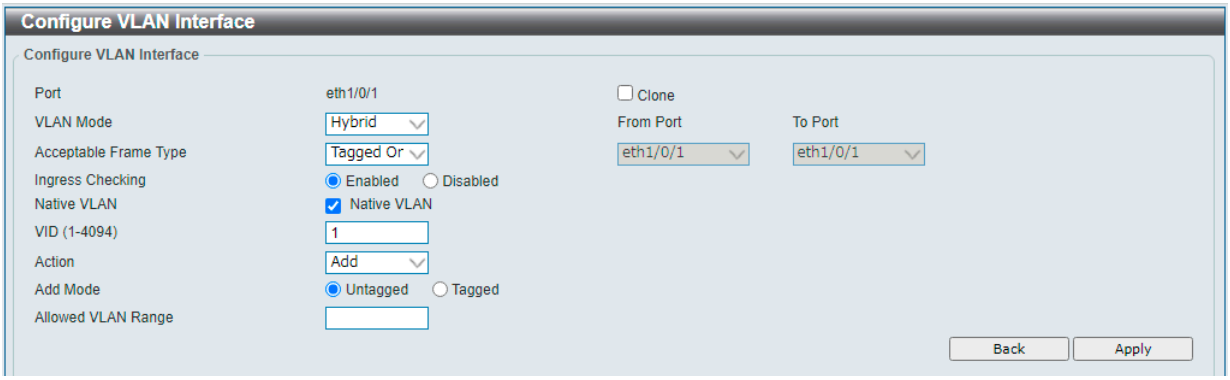


図 8-12　Configure VLAN Interface - Hybrid 画面

画面に表示される項目：

項目	説明
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを選択します。ここでは「Hybrid」を選択します。
Acceptable Frame Type	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	Native VLAN を有効にします。
VID	Native VLAN を有効にした場合は、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	「Action」で「Add」を選択した場合、「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。
From Port / To Port	設定内容をコピーするポートの範囲を指定します。

「Apply」をクリックして、設定内容を適用します。
「Back」をクリックすると前画面に戻ります。

● **VLAN モード「Trunk」を選択した場合：**

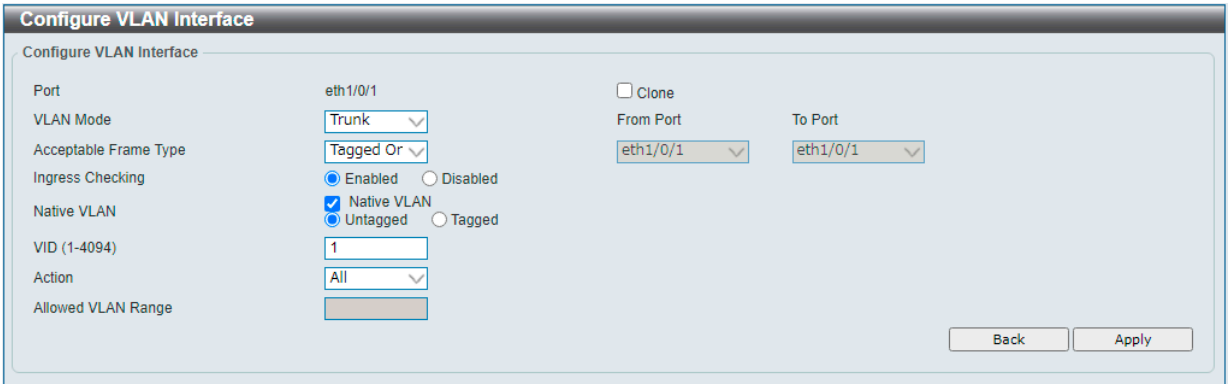


図 8-13　Configure VLAN Interface - Trunk 画面

画面に表示される項目：

項目	説明
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを選択します。ここでは「Trunk」を選択します。
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
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：「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。
From Port / To Port	設定内容をコピーするポートの範囲を指定します。

「Apply」をクリックして、設定内容を適用します。
「Back」をクリックすると前画面に戻ります。

Port Summary（ポートサマリ）

「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。

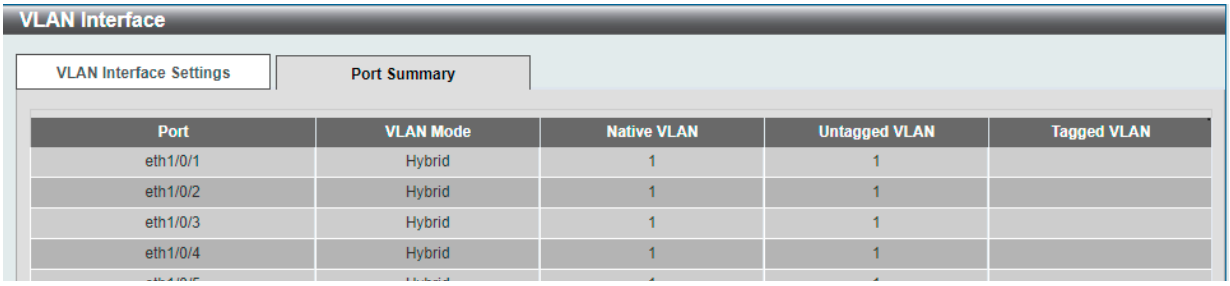


図 8-14　VLAN Interface - Port Summary 画面

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。
本機能では、スイッチが他の GARP VLAN Registration Protocol（GVRP）対応スイッチと VLAN コンフィグレーション情報を共有するかどうかを設定できます。さらに、Ingress Checking を使用して、PVID がポートの PVID と一致しない受信パケットをフィルタリングすることで、トラフィックを制限できます。

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

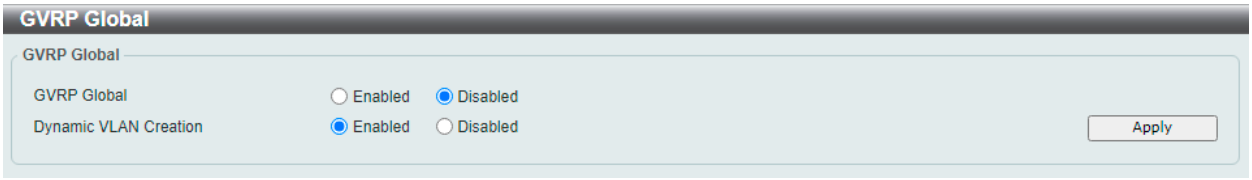


図 8-15　GVRP Global 画面

画面に表示される項目：

項目	説明
GVRP Global	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。

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

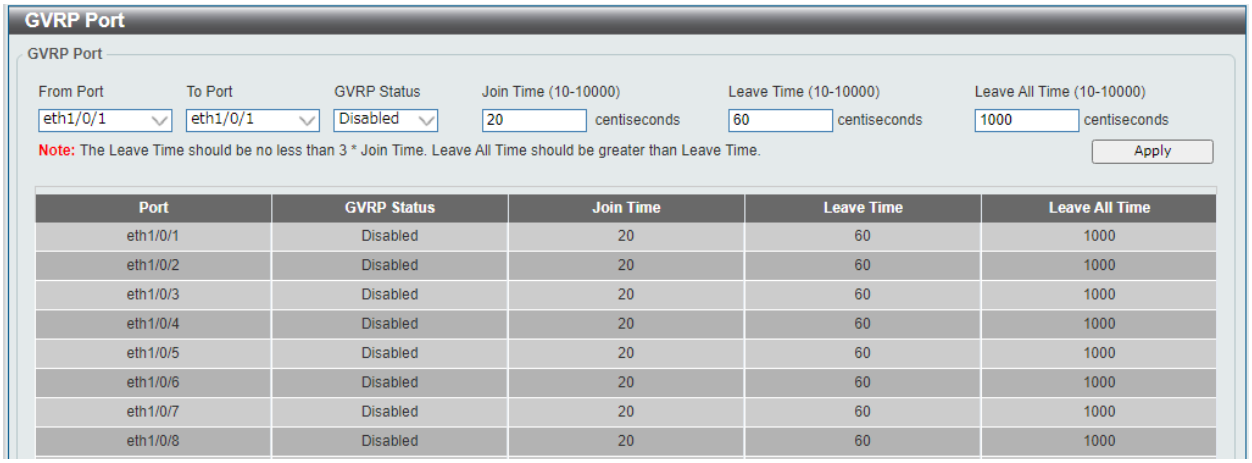


図 8-16　GVRP Port 画面

画面に表示される項目：

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。
GVRP Status	ポートの GVRP ステータスを有効 / 無効に設定します。「Hybrid」または「Trunk」モードの場合に利用可能です。 • 初期値：「Disabled（無効）」
Join Time	PDU が送信される間隔を設定します。 • 設定可能範囲：10 - 10000（センチ秒） • 初期値：20
Leave Time	デバイスが GARP 状態から抜けるまでに待機する時間を設定します。Leave Time は、Leave All メッセージの送受信によって有効化され、Join メッセージによってキャンセルされます。 • 設定可能範囲：10 - 10000（センチ秒） • 初期値：60
Leave All Time	VLAN 内のポートを確認するために使用されるメッセージの送信間隔を指定します。 • 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 でアドバタイズされる VLAN ID の設定、表示を行います。

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

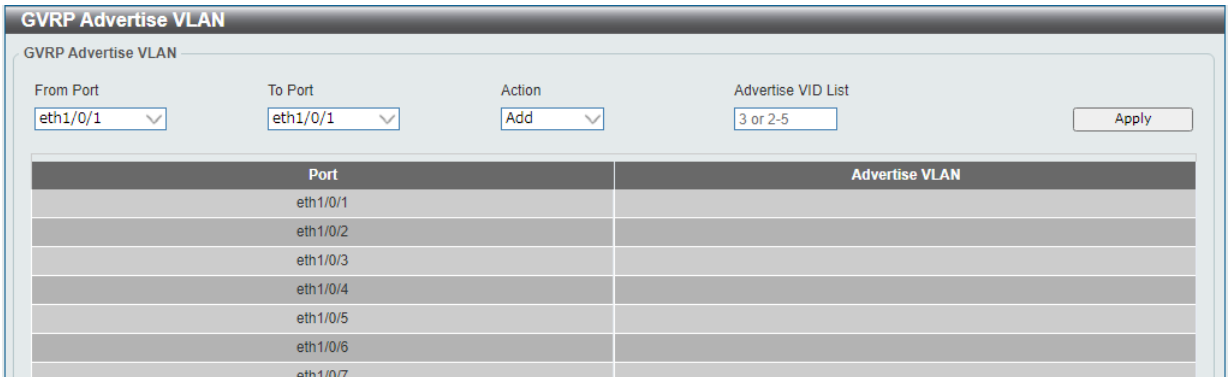


図 8-17　GVRP Advertise VLAN 画面

画面に表示される項目：

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 VLAN ID を追加します。 • 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。

注意　gvrp advertise、gvrp forbidden コマンドの実行において、add/remove パラメータを指定しない場合、既存の VLAN リストの上書きではなく、指定 VLAN が追加されます。

GVRP Forbidden VLAN（GVRP Forbidden VLAN 設定）

GVRP で登録が禁止される VLAN ID の設定、表示を行います。

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

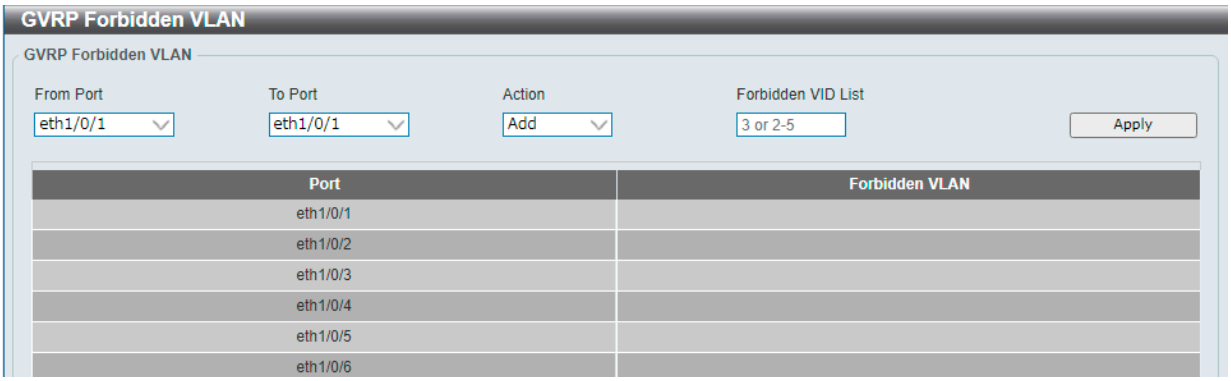


図 8-18　GVRP Forbidden VLAN 画面

画面に表示される項目：

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	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 VLAN ID を追加します。 • 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。

注意　gvrp advertise、gvrp forbidden コマンドの実行において、add/remove パラメータを指定しない場合、既存の VLAN リストの上書きではなく、指定 VLAN が追加されます。

GVRP Statistics Table（GVRP 統計テーブル）

GVRP の統計カウンタを表示します。

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

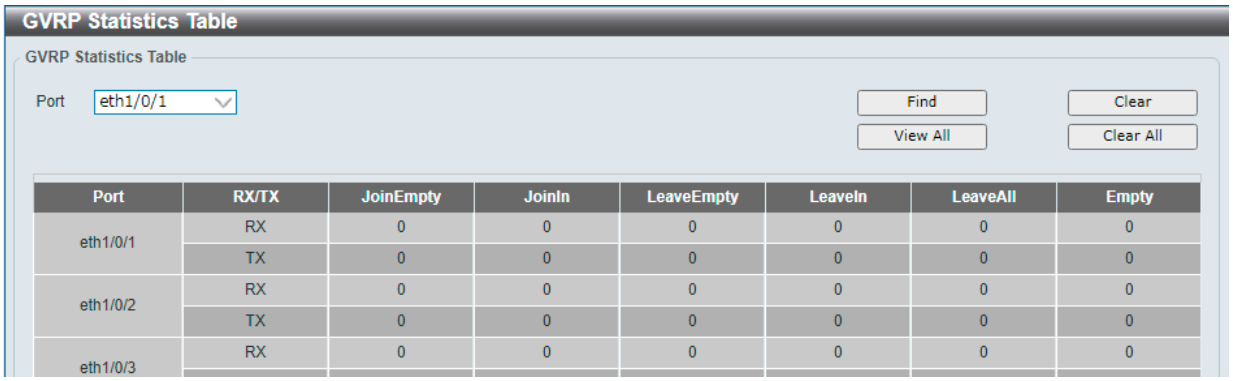


図 8-19　GVRP Statistics Table 画面

画面に表示される項目：

項目	説明
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。
「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。

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。

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 > Auto Surveillance VLAN > Auto Surveillance Properties の順にクリックし、次の画面を表示します。

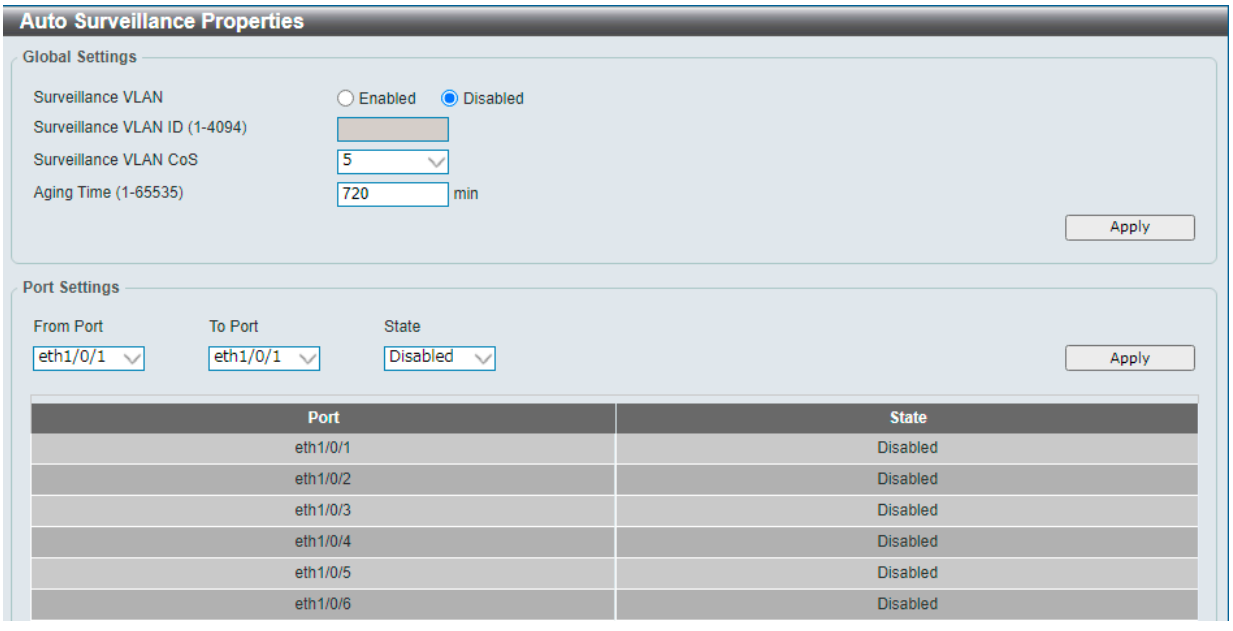


図 8-20　Auto Surveillance Properties 画面

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：1 - 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） • 初期値：720（分）
Port Settings	
From Port / To Port	設定するポートの範囲を指定します。
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」をクリックして、設定内容を適用します。

注意　自動サーベイランスの帯域が同じキュー内で同等になりません。

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

ユーザ定義のサーベイランスデバイス OUI の設定や、サーベイランス VLAN 情報の表示を行います。

User-defined MAC Settings（ユーザ定義 MAC 設定）

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

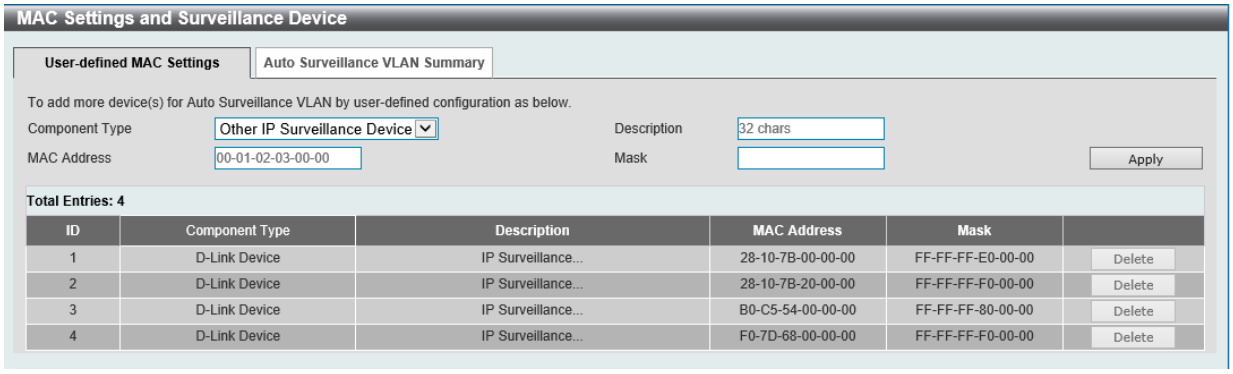


図 8-21　MAC Settings and Surveillance Device - User-defined MAC Settings 画面

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： 「Vms」「VmsClient」「VideoEncoder」「NetworkStorage」「Other」
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。

項目	説明
Mask	ユーザ定義の OUI MAC アドレスマスクを入力します。

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

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

「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 8-22　MAC Settings and Surveillance Device - Auto Surveillance VLAN Summary 画面

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。
音声 VLAN は、IP フォンから音声トラフィックを伝送するために使用される VLAN です。Voice over IP の音質は遅延の影響を受けやすいため、音声トラフィックの QoS（Quality of Service）を設定して、音声トラフィックがより高い優先順位で処理されるようにする必要があります。
スイッチは、受信したパケットが音声パケットであるかどうかを、その送信元 MAC アドレスをチェックすることによって判断します。パケットの送信元 MAC アドレスが、システムによって設定された組織的に一意な識別子（OUI）アドレスに準拠している場合、パケットは音声パケットとして識別され、音声 VLAN で送信されます。

L2 Features > 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。

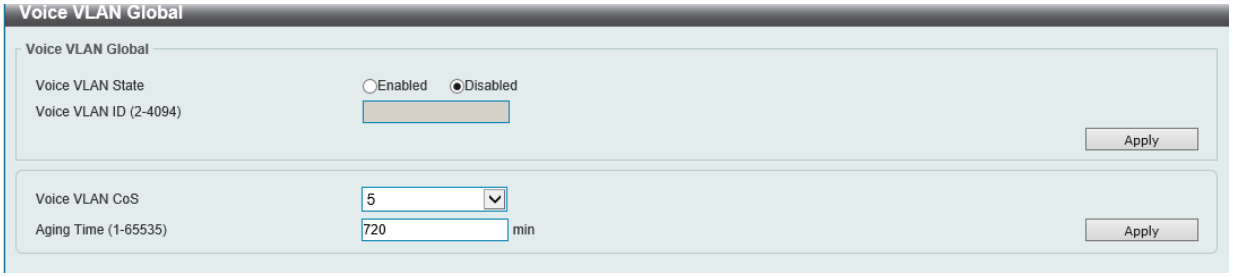


図 8-23　Voice VLAN Global 画面

画面に表示される項目：

項目	説明
Voice VLAN State	音声 VLAN 機能を有効 / 無効に設定します。
Voice VLAN ID	音声 VLAN の VLAN ID を入力します。指定する VLAN は事前に作成しておく必要があります。 • 設定可能範囲：2 - 4094
Voice VLAN CoS	音声 VLAN の優先度を設定します。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	音声 VLAN からポートを削除するエージングタイム 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） • 初期値：720（分）

「Apply」をクリックして、設定内容を適用します。

注意　音声 VLAN で処理されるトラフィックにおいて、最初のパケットは音声 VLAN から除外されます。

Voice VLAN Port（音声 VLAN ポート設定）

ポートの音声 VLAN 設定を行います。

L2 Features > 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。

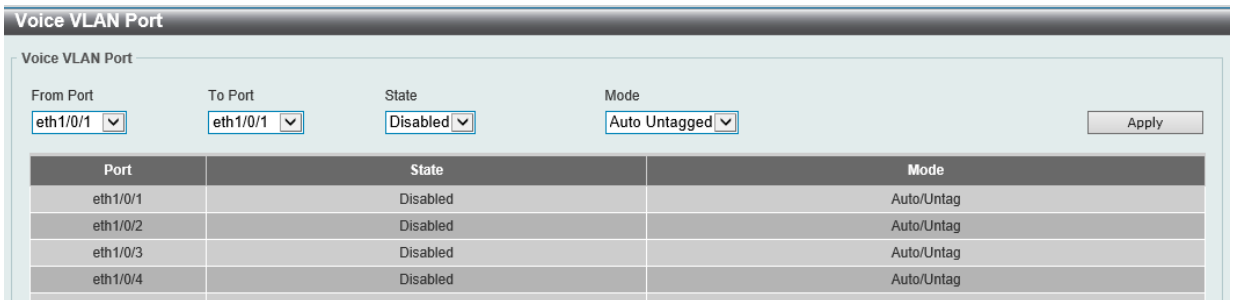


図 8-24　Voice VLAN Port 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
State	指定ポートの音声 VLAN 機能を有効 / 無効に設定します。 音声 VLAN が有効になると、受信した音声パケットは音声 VLAN として送信されます。受信した音声 VLAN パケットの送信元 MAC アドレスが OUI アドレスに一致すると、音声 VLAN と認識されます。
Mode	モードを選択します。 • 「Auto Untagged」- タグなしの音声 VLAN 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」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。事前定義済みの OUI の他に、必要に応じてユーザ定義の OUI を設定できます。
ユーザ定義 OUI は定義済みの OUI と同じとすることはできません。また、定義済み OUI の削除はできません。

L2 Features > 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。

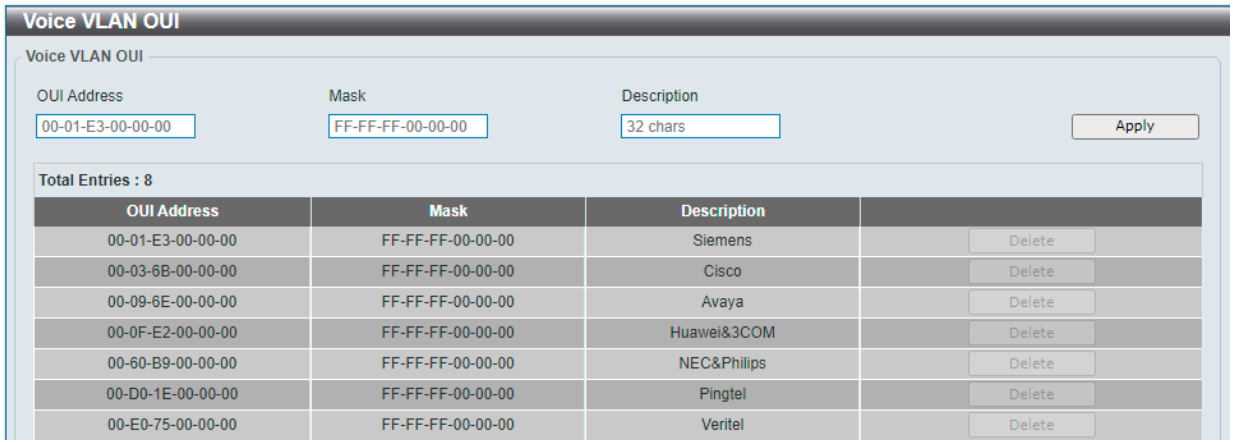


図 8-25　Voice VLAN OUI 画面

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 に関する説明を入力します。（32 文字以内）

「Apply」をクリックし、デバイスに設定を適用します。
「Delete」をクリックして、指定エントリを削除します。

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。
「Start Time」はデバイスがポートで検出された時間、「Status」はポートの音声 VLAN ステータスを表示します。

L2 Features > 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 8-26　Voice VLAN Device 画面

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 音声デバイスを表示します。

L2 Features > Voice VLAN > Voice VLAN LLDP-MED 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。

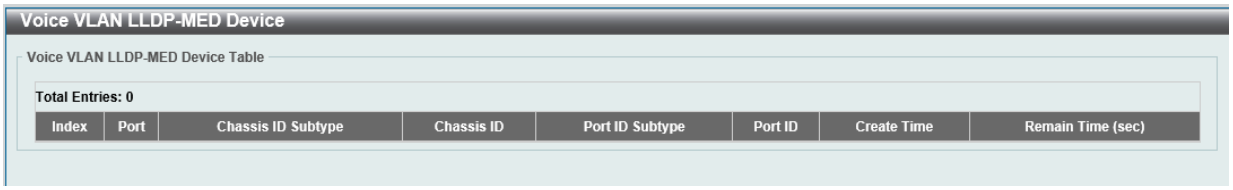


図 8-27　Voice VLAN LLDP-MED Device 画面

STP（スパニングツリーの設定）

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 Spanning Tree

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。本項では、スパニングツリーの新しいコンセプトと、これらのプロトコル間の主な違いについて説明します。

ポートの状態遷移

3 つのプロトコル間の根本的な相違点は、ポートがどのように Forwarding 状態に遷移するかという点と、この状態遷移がトポロジ内でのポートの役割（Forwarding/Not Forwarding）にどのように対応するかという点にあります。802.1D-1998 規格で使用されていた 3 つの状態「Disabled」「Blocking」「Listening」が、MSTP 及び RSTP では「Discarding」という 1 つの状態に統合されました。いずれの場合も、ポートはパケットの送信を行わない状態です。STP の「Disabled」「Blocking」「Listening」であっても、RSTP/MSTP の「Discarding」であっても、ネットワークトポロジ内では「非アクティブ状態」であり、機能の差はありません。以下の表では、3 つのプロトコルにおけるポートの状態遷移の違いを示しています。

トポロジの計算については、3 つのすべてのプロトコルにおいて同様に行われます。各セグメントにはルートブリッジへのパスが 1 つ存在し、すべてのブリッジで BPDU パケットをリッスンします。RSTP/MSTP では、ルートブリッジから BPDU を受信しなくても BPDU パケットが Hello パケット送信毎に送信されます。ブリッジ間の各リンクはリンクの状態を素早く検知することができるため、リンク断絶時の素早い検出とトポロジの調整が可能となります。802.1D-1998 規格では、隣接するブリッジ間においてこのような素早い状態検知が行われません。

ポート状態の比較

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	不可能	不可能
Discarding	Discarding	Blocking	不可能	不可能
Discarding	Discarding	Listening	不可能	不可能
Learning	Learning	Learning	不可能	可能
Forwarding	Forwarding	Forwarding	可能	可能

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

Edge Port

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

P2P Port

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

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

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

2 つのレベルで動作するスパニングツリープロトコル

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

STP Global Settings（STP グローバル設定）

STP をグローバルに設定します。

L2 Features > STP > 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。

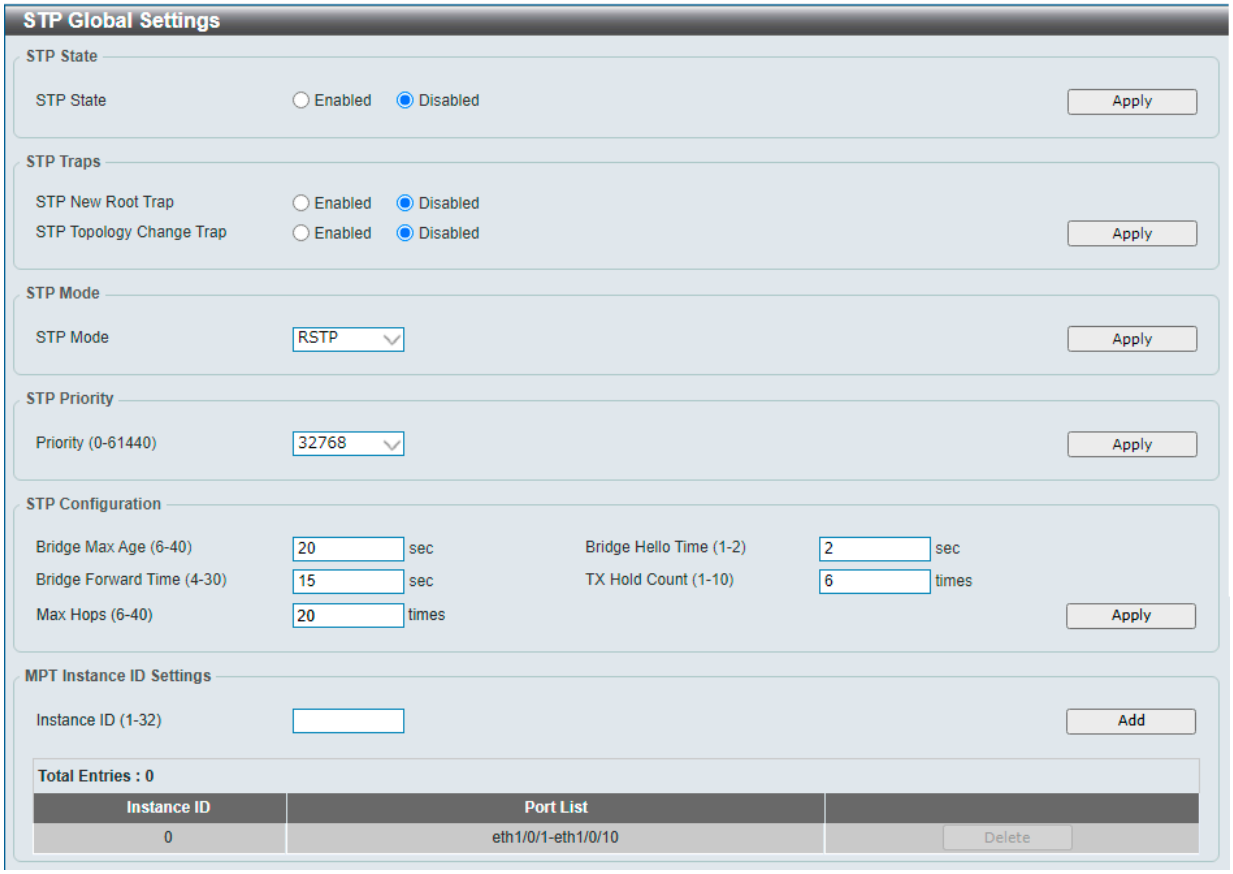


図 8-28　STP Global Settings 画面

補足　STP 機能は、ERPS、LBD 機能と併用することはできません。

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 Trap	
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します。 • 設定可能範囲：6 - 40（秒） • 初期値：20（秒）

項目	説明
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。（次のセクションの「STP Port Setting」を参照してください。） • 設定可能範囲：1 - 2（秒） • 初期値：2（秒）
Bridge Forward Time	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	BPDU の転送保留カウント値を指定します。カウンタは BPDU 送信毎に増加し、1 秒経過すると減少します。指定カウントに到達すると 1 秒間送信を停止します。 • 設定可能範囲：1 - 10（回） • 初期値：6（回）
Max Hops	スパニングツリー範囲のデバイス間で、スイッチが送信した BPDU パケットが破棄されるまでのホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。0 に到達すると、BPDU パケットが破棄され、ポートに保持していた情報は解放されます。 • 設定可能範囲：6 - 40 • 初期値：20
MPT Instance ID Settings	
Instance ID	Multi-Process RSTP のインスタンスを入力します。 • 設定可能範囲：1 - 32

「Apply」をクリックして、設定内容を適用します。
「Add」をクリックして、インスタンスを追加します。
「Delete」をクリックして、エントリを削除します。

STP Port Settings（STP ポートの設定）

スイッチ全体での STP パラメータの設定に加えて、ポート毎の設定も可能です。
ポートグループにはそれぞれ STP インスタンスや構成が設定されています。

ポートレベルのスパニングツリーはスイッチレベルのスパニングツリーと同じように機能しますが、ルートブリッジはルートポートに置き換えられます。ルートポートはポートプライオリティとポートコストに基づいて選出され、STP グループにおけるネットワークへの接続部となります。

スイッチレベルで冗長リンクがブロックされるのと同様に、ポートレベルにおいても冗長リンクはブロックされます。スイッチレベルの STP は、スイッチ間の冗長リンクをブロックします。ポートレベルの STP は、STP グループ内の冗長リンクをブロックします。

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。

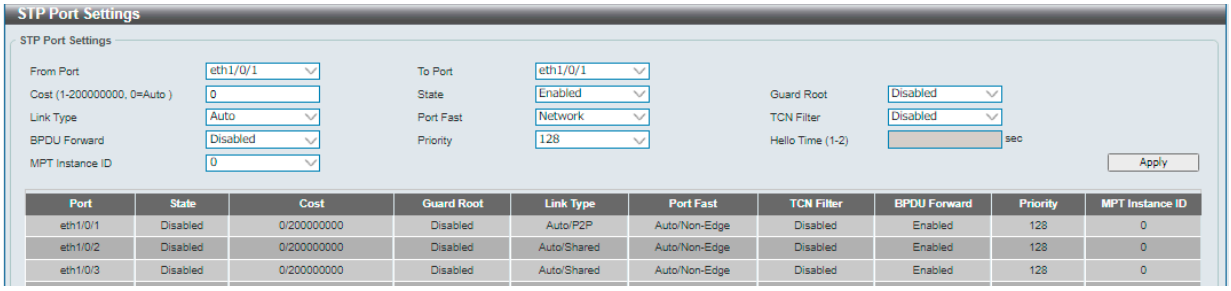


図 8-29　STP Port Settings 画面　更新

本画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Cost （1-200000000, 0=Auto）	指定ポートへパケットを転送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 = 200,000、1 Gbps = 20,000、2.5G = 8,000、5G = 4,000、10G = 2,000 • 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。

項目	説明
Guard Root	Guard Root を有効 / 無効に設定します。
Link Type	リンクの種類を設定します。全二重ポートは P2P ポートとして判別されます。半二重ポートは、共有接続があると見なされます。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：「P2P」「Shared」「Auto」 • 初期値：「Auto」
Port Fast	ポートファストオプションを指定します。 • 「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。 • 「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 • 「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）
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、ポートで受信したトポロジ変更イベントは無視されます。管理者の完全な制御下にない外部ネットワークに接続する場合、本機能が有用です。 • 初期値：「Disabled」（無効）
BPDU Forward	BPDU パケットの転送を有効 / 無効にします。 有効にすると、受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。 • 「Enabled」：ポートで BPDU 転送が有効です（STP を無効にする必要があります）。 • 「Disabled」（無効 / 初期値）：ポートで BPDU フィルタリングが有効です。 2 つのリージョンがブリッジで接続され、各リージョンが個別のスパニングツリーで構成されている場合に本機能が役に立ちます。
Priority	優先値を指定します。値が小さい方が優先度は高くなり、ポートがルートポートとして選択される確率が高くなります。 • 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。BPDU パケットの送信間隔となります。 本項目は、「STP Global Settings」画面の「STP Mode」で「MSTP」を選択した場合のみ設定可能です。 • 設定可能範囲：1 - 2（秒）
MPT Instance ID	MPT インスタンス ID を指定します。

「Apply」をクリックして、設定内容を適用します。

MST Configuration Identification（MST の設定）

マルチプルスパニングツリー（MSTP）は、複数の VLAN を単一のスパニングツリーインスタンスにマッピングし、ネットワーク全体に複数のパスを提供することで、さまざまなロードバランシングシナリオを提供します。たとえば、ポート A が特定の STP インスタンスでブロックされている間、このポートは別の STP インスタンスでフォワーディング状態になることができます。

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

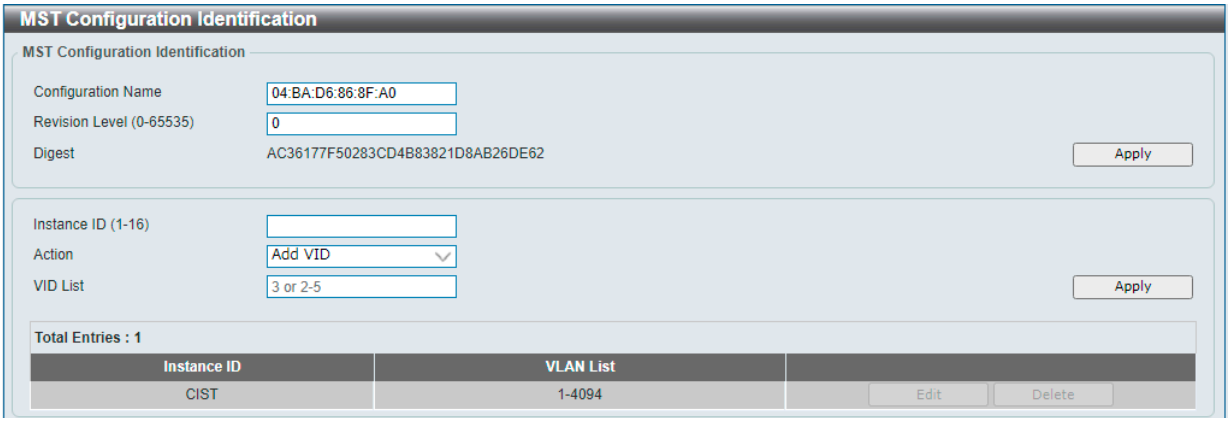


図 8-30　MST Configuration Identification 画面

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

項目	説明
Instance ID Settings	
Instance ID	VID List に関連付ける Instance ID を設定します。 • 設定可能範囲：1 - 16
Action	MSTI 対して行う変更を選択します。 •「Add VID」- VID List 項目に指定された VID を MSTI ID に追加します。 •「Remove VID」- VID List 項目に指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、指定のエントリを削除します。
「Edit」をクリックして、指定エントリの編集を行います。

STP Instance（STP インタンス設定）

STP インスタンスの設定を変更します。

L2 Features > STP > STP Instance をクリックし、以下の画面を表示します。

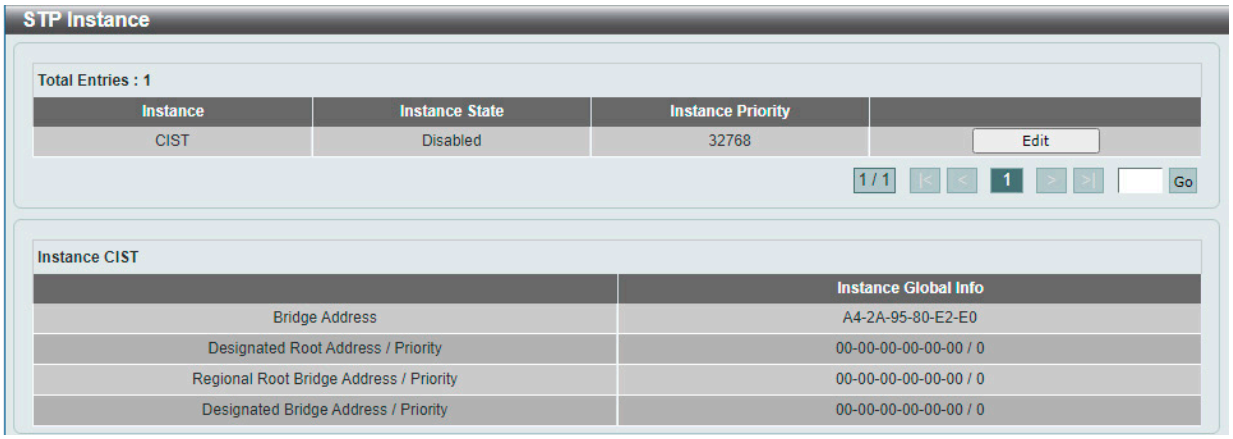


図 8-31　STP Instance 画面

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ためのプライオリティを設定します。 • 設定可能範囲：0 - 61440

「Edit」をクリックして指定エントリの編集を行い、「Apply」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、設定を行います。

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

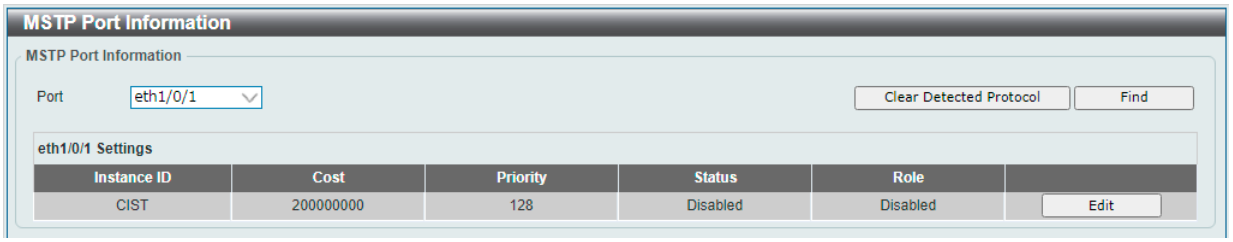


図 8-32　MSTP Port Information 画面

画面に表示される項目：

項目	説明
Port	エントリを表示 / 削除するポートを選択します。
Cost	「Edit」を選択後、パケットを転送するコストを設定します。 • 設定可能範囲：1 - 200000000

項目	説明
Priority	「Edit」を選択後、優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0 - 224 • 初期値：128

「Clear Detected Protocol」をクリックし、選択したポートの検出したプロトコル設定をクリアします。
「Find」をクリックして、特定ポートの MSTP 設定を参照します。
「Edit」を選択して、特定のエントリを再設定し、「Apply」をクリックして設定内容を適用します。

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。

リング内の 1 つのリンクが、ループ（RPL : Ring Protection Link）を回避するためにブロックされます。障害が発生すると、保護スイッチングは障害のあるリンクをブロックして RPL のブロックを解除します。障害が解決すると、保護スイッチングは再度 RPL をブロックして、障害が解決したリンクのブロックを解除します。

参照　各製品の処理方法については、「【付録 E】ERPS 情報」をご確認ください。

ERPS

スイッチの ERPS 機能を有効にします。

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。

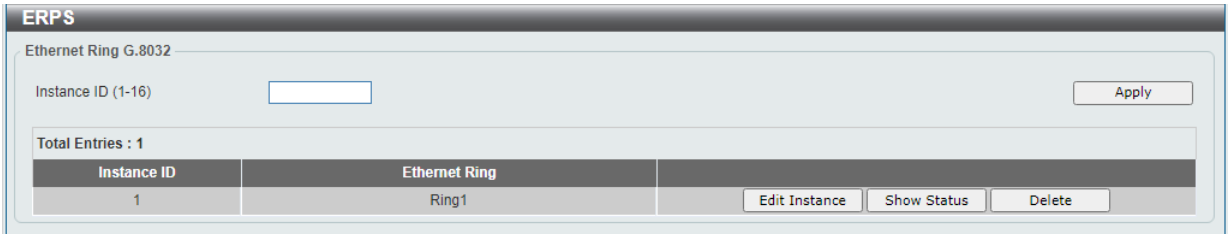


図 8-33　ERPS 画面

上記画面には以下の項目が含まれます。

項目	説明
Instance ID	作成するインスタンス ID を指定します。 • 設定可能範囲：1 - 16

「Apply」をクリックして「ITU-T G.8032 ERP リング」を作成します。
「Edit Instance」をクリックして ERP インスタンスを編集します。
「Show Status」をクリックして「ITU-T G.8032 ERP リング」の情報について表示します。
「Delete」をクリックして指定の「ITU-T G.8032 ERP リング」を削除します。

補足　ERPS 機能は、STP、LBD 機能と併用することはできません。

Instance の編集

「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。

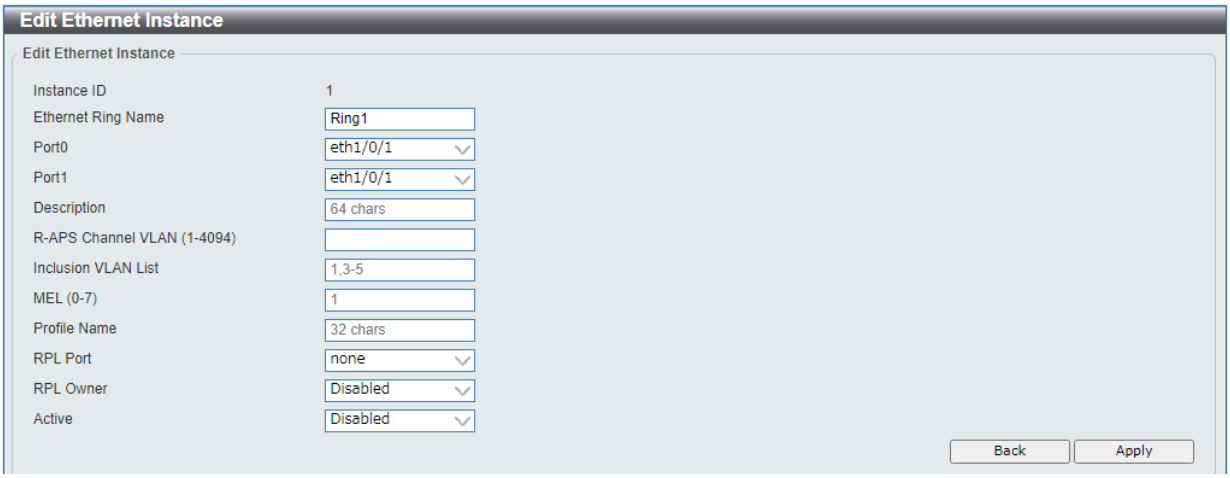


図 8-34　ERPS 画面 - Instance

設定対象となる項目は以下の通りです。

項目	説明
Ethernet Ring Name	指定インスタンスの Ethernet リング名を入力します。
Port0	ポートを最初のリングポートとして指定し、使用される仮想ポートチャネルを指定します。
Port1	ポートを 2 番目のリングポートとして指定し、使用される仮想ポートチャネルを指定します。
Description	インスタンスの説明を入力します。
R-APS Channel VLAN	ERP インスタンスの R-APS チャネルを指定します。 • 設定可能範囲：1 - 4094
Inclusion VLAN List	インスタンスに含まれる VLAN リストを指定します。指定された VLAN は ERP のメカニズムで保護されます。
MEL	R-APS 機能のリング MEL を指定します。 • 初期値：1
Profile Name	イーサネットインスタンスのプロファイル名を指定します。
RPL Port	使用する RPL ポートを指定します。 • 選択肢：「None」「Port0」「Port1」
RPL Owner	RPL オーナノードを有効 / 無効に設定します。
Active	ERP インスタンスをアクティブにするかどうかを指定します。

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

ステータスの表示

「Show Status」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。

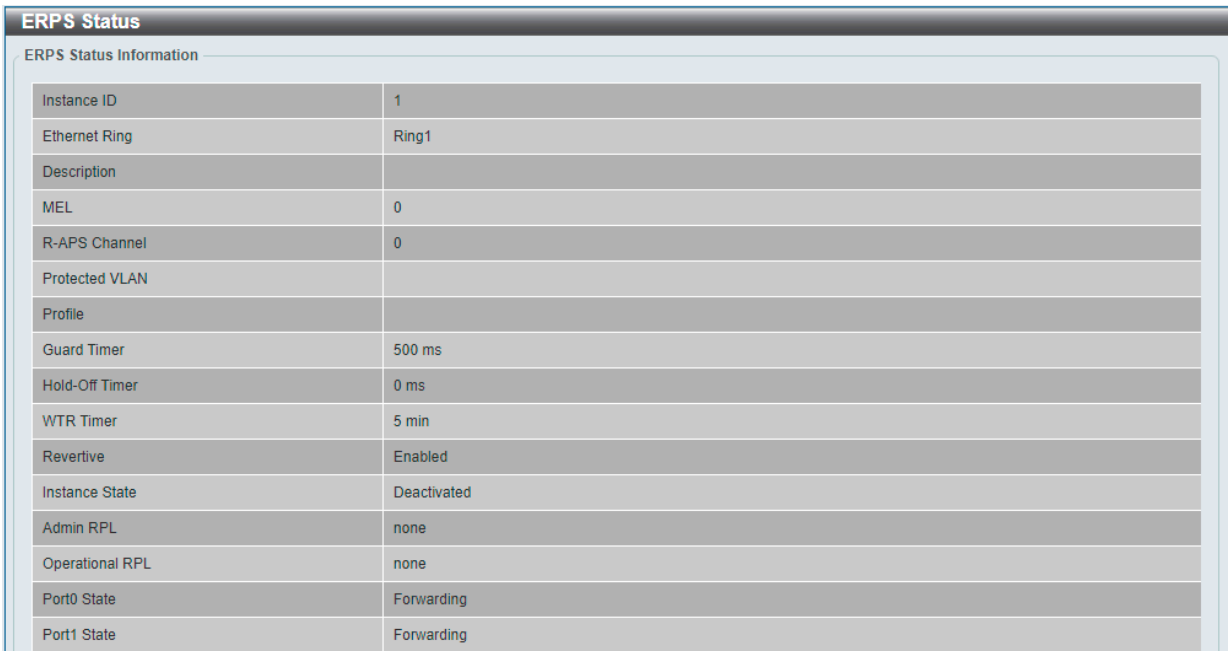


図 8-35　ERPS Status 画面

「Back」をクリックすると前画面に戻ります。

ERPS Profile（ERPS プロファイル）

ERPS プロファイル設定を行います。

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

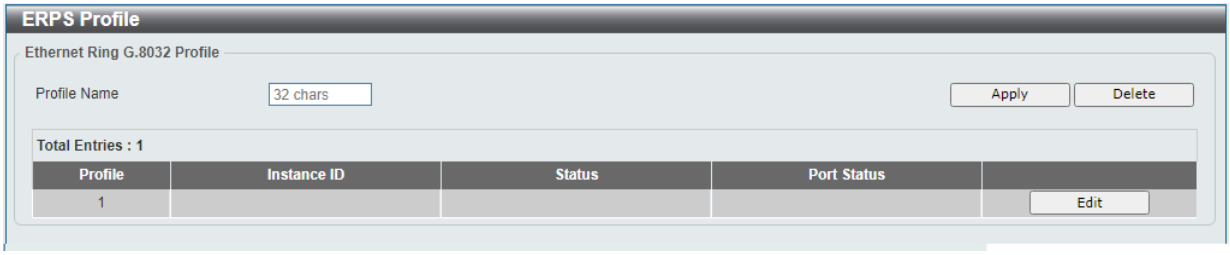


図 8-36　ERPS Profile 画面

設定対象となる項目は以下の通りです。

項目	説明
Profile Name	プロファイル名を指定します。

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

「G.8032」プロファイルの編集

「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。

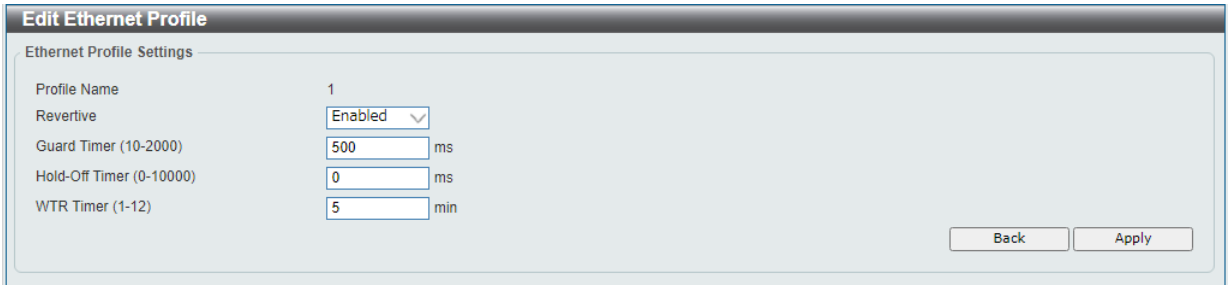


図 8-37　「G.8032」プロファイル画面 - Edit

設定対象となる項目は以下の通りです。

項目	説明
Revertive	RPL がブロックされた場合など、障害発生後に元の状態を有効にするか無効にするかを指定します。
Guard Timer	R-APS 機能のガードタイムを指定します。 • 設定可能範囲：10 - 2000（ミリ秒） • 初期値：500（ミリ秒）
Hold-Off Timer	R-APS 機能のホールドオフ時間を指定します。 • 設定可能範囲：0 - 10000（ミリ秒） • 初期値：0（ミリ秒）
WTR Timer	R-APS 機能の WTR 時間を指定します。 • 設定可能範囲：1 - 12（分） • 初期値：5（分）

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

Loopback Detection（ループバック検知設定）

ループバック検出機能は、STP を使用しない環境において、ポートで生成されるループを検出するために使用されます。ループが検出されると、スイッチは自動的にポートをシャットダウンし、管理者にトラップを送信します。ループバック検知ポートは、「Error Disable Recovery Setting」がタイムアウトするとアンロックされます。

補足 LBD 機能は、STP、ERPS と併用することはできません。また、ポートチャネルに対しては適用できません。

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。

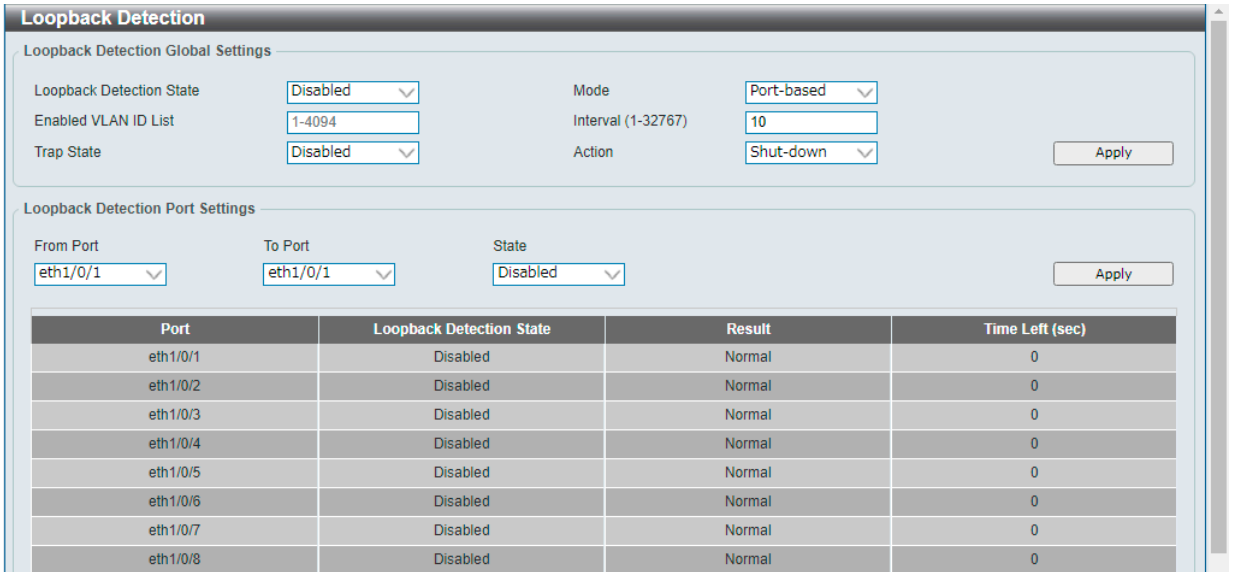


図 8-38　Loopback Detection 画面

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-based」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。 • 設定可能範囲：1 - 32767（秒） • 初期値：10（秒）
Traps State	ループバック検知トラップを有効 / 無効に設定します。
Action	動作モードを指定します。 • 「Shut-down」- ループ検出時にポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックします。 • 「None」- ループ検出時でもポートをシャットダウンや VLAN トラフィックのブロックは行いません。
Loopback Detection Port Settings	
From Port/To Port	設定を適用するポートの範囲を指定します。
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」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に、同時に検出可能な VLAN 数は検出順に 8 までに制限されます。

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 8 個まで作成可能であり、各グループには最大 8 個までの物理ポートを割り当てることができます。

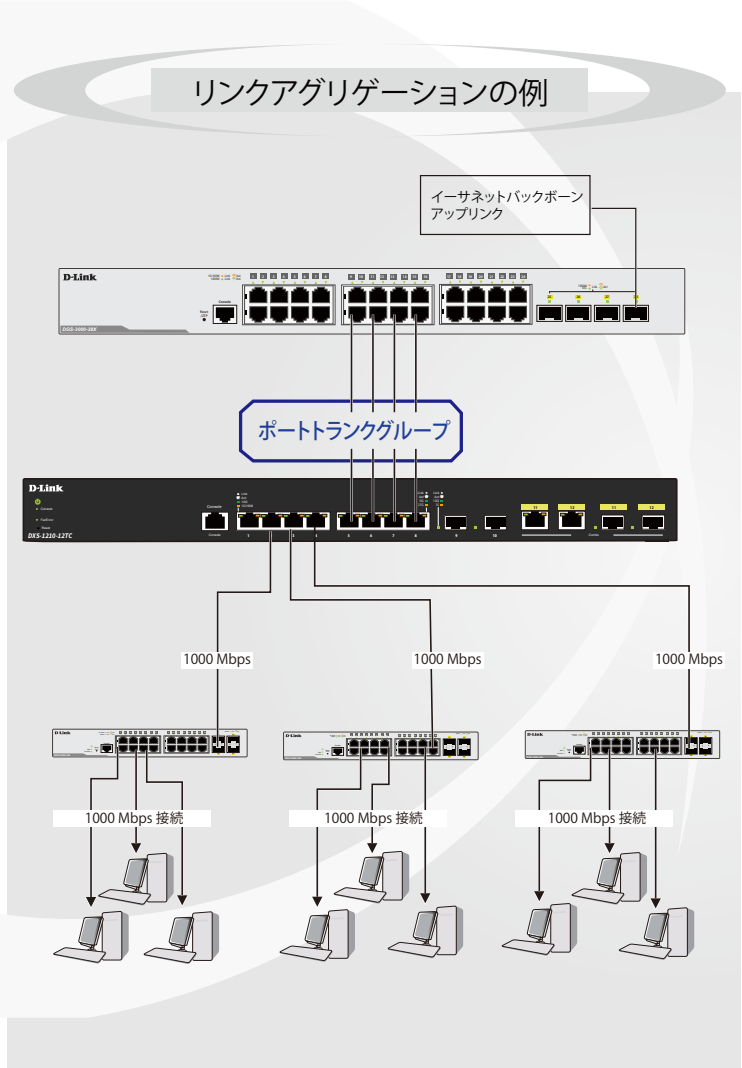


図 8-39　ポートトランクグループの例

トランクグループ内のすべてのポートは 1 つのポートと見なされます。あるホスト（宛先アドレス）へデータ転送が行われる際には、常にトランクグループ内の特定のポートが使用されるため、データは送信された順で宛先ホスト側に到着します。

リンクアグリゲーション機能により複数のポートが 1 つのグループとして束ねられ、1 つのリンクとして動作します。この時、1 つのリンクの帯域は束ねられたポート分拡張されます。

リンクアグリゲーションは、サーバなどの広帯域を必要とするネットワークデバイスをバックボーンネットワークに接続する際に広く利用されています。

本スイッチでは、8 個のリンク（ポート）から構成される最大 8 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はブロックされます（冗長リンクを持つポートがブロックされるケースと同様）。

注意　トランクグループ内のいずれかのポートが接続不可になると、そのポートが処理するパケットはリンクアグリゲーション（集約）グループ内の他のポート間でロードシェアされます。

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

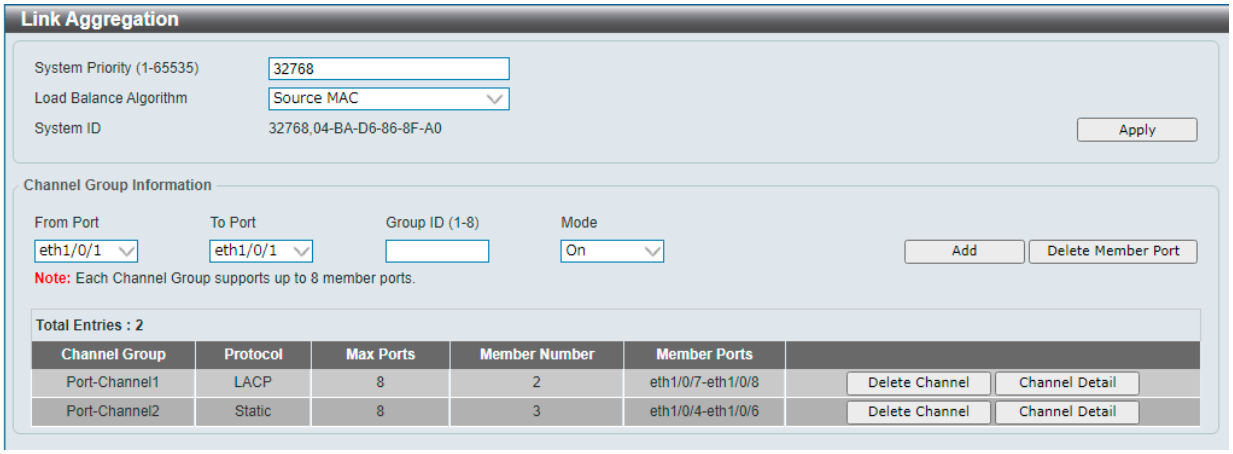


図 8-40　Link Aggregation 画面

画面に表示される項目：

項目	説明
System Priority	システムプライオリティを指定します。 本値により、接続するスイッチ間で「Actor」となるシステムが決定され、そのシステムのポートプライオリティが使用されます。値の小さい方が高い優先度を示します。システムプライオリティが同じ値の場合、MAC ID の小さいシステムが選出されます。その後、「Actor」スイッチのポートプライオリティの値により、ポートチャネルに属するかスタンドアロンモードになるかが決定します。ポートプライオリティが同じ値の場合、ポート番号で優先値が決まります。 • 設定可能範囲：1 - 65535 • 初期値：32768
Load Balance Algorithm	ロードバランスに使用するアルゴリズムを選択します。 • 選択肢：「Source MAC」「Destination MAC」「Source Destination MAC」「Source IP」「Destination IP」「Source Destination IP」 • 初期値：「Source MAC」
Channel Group Information	
From Port / To Port	設定するポートの範囲を指定します。
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 - 8
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。

「Apply」ボタンをクリックして、設定内容を適用します。
各項目を入力後、「Add」をクリックし、チャネルグループを作成します。
「Delete Channel」をクリックして、チャネルを削除します。
「Delete Member Port」をクリックして、特定のグループメンバポートを削除します。
「Channel Detail」をクリックすると、チャネルの詳細情報が表示されます。

補足　リンクアグリゲーション設定は、LBD 機能を有効化したポートに適用することはできません。

注意　「Load Balance Algorithm」が「Source Destination MAC」または「Source Destination IP」に設定されている場合、適切に負荷分散されません。

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「Channel Detail」をクリックします。

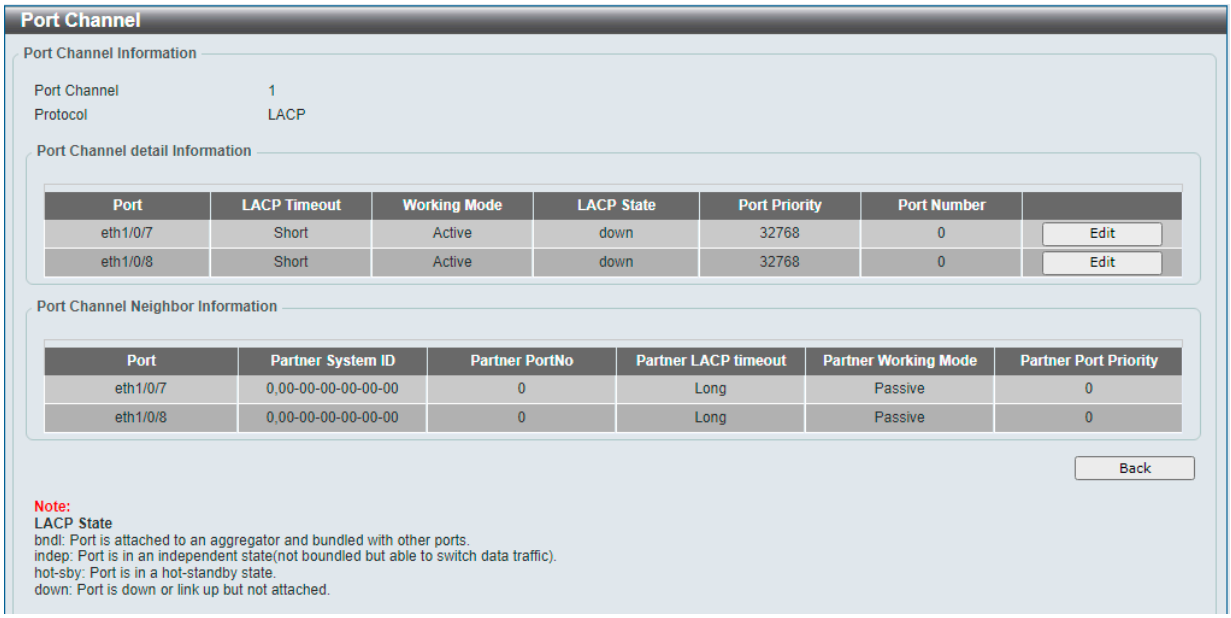


図 8-41　Link Aggregation（Channel Detail）画面

画面に表示される項目：

項目	説明
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」をクリックしてパラメータを設定後、「Apply」をクリックして設定内容を適用します。

「Back」をクリックして前の画面に戻ります。

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

IGMP（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 スヌーピング）

GMP（Internet Group Management Protocol）Snooping 機能を有効にすると、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。
適切にマルチキャストパケットを転送することにより、無駄なトラフィックの発生を抑えることができます。

注意　IGMP スヌーピングおよび STP 有効時、トポロジが変更されても IGMP クエリが送信されません。

IGMP Snooping Settings（IGMP スヌーピング設定）

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」をクリックして、各 VLAN に詳細な設定を行います。

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

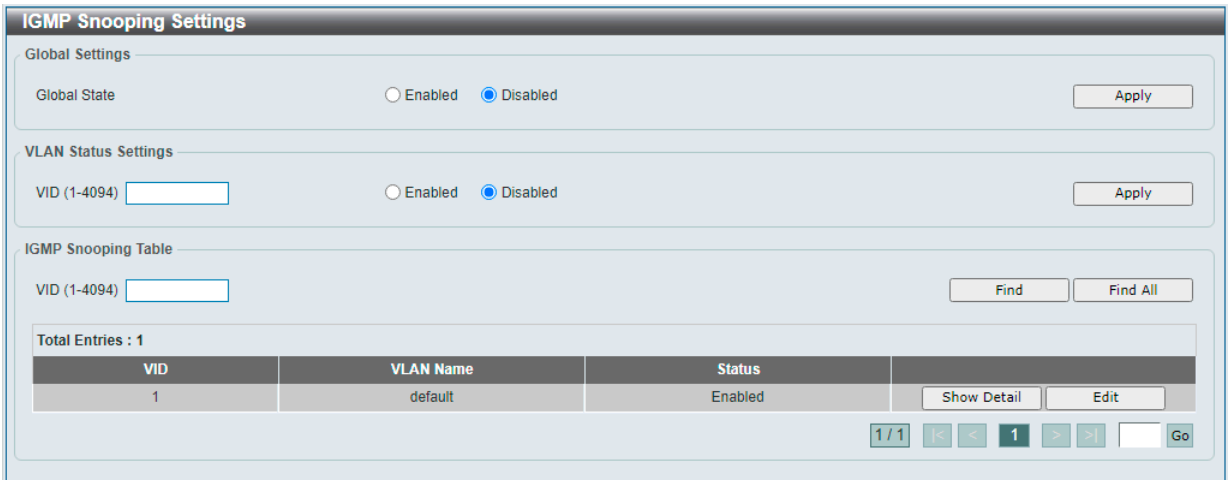


図 8-42　IGMP Snooping Settings 画面

画面に表示される項目：

項目	説明
Global Settings	
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」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。
「Find All」をクリックして IGMP Snooping Table 上のすべてのエントリを表示します。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

注意　IGMP Snooping 機能では、Router Port へ Multicast Stream をフラッディングしません。

IGMP Snooping VLAN の詳細情報表示

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

図 8-43　IGMP Snooping VLAN Parameters 画面

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

■ IGMP Snooping 機能の詳細設定

「IGMP Snooping Settings」で関連する VLAN エントリの「Edit」をクリック、または詳細情報画面の「Modify」をクリックし、以下の画面で各 VLAN に対して詳細な設定を行います。

図 8-44 IGMP Snooping VLAN Settings（Edit/Modify）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。
State	VLAN の IGMP Snooping 機能の有効 / 無効ステータスが表示されます。
Fast Leave	Fast Leave 機能を有効 / 無効に設定します。 本機能が有効な場合、システムで IGMP done メッセージを受信すると、Group Specific または Group-Source Specific クエリを送信せずに、メンバシップが直ちに削除されます。
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入力します。 • 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。 • 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）

「Apply」をクリックして、設定内容を適用します。
「Back」をクリックして前の画面に戻ります。

注意　IGMP Snooping は IGMPv1/v2 のみサポートします。

IGMP Snooping Group 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、以下の画面を表示します。

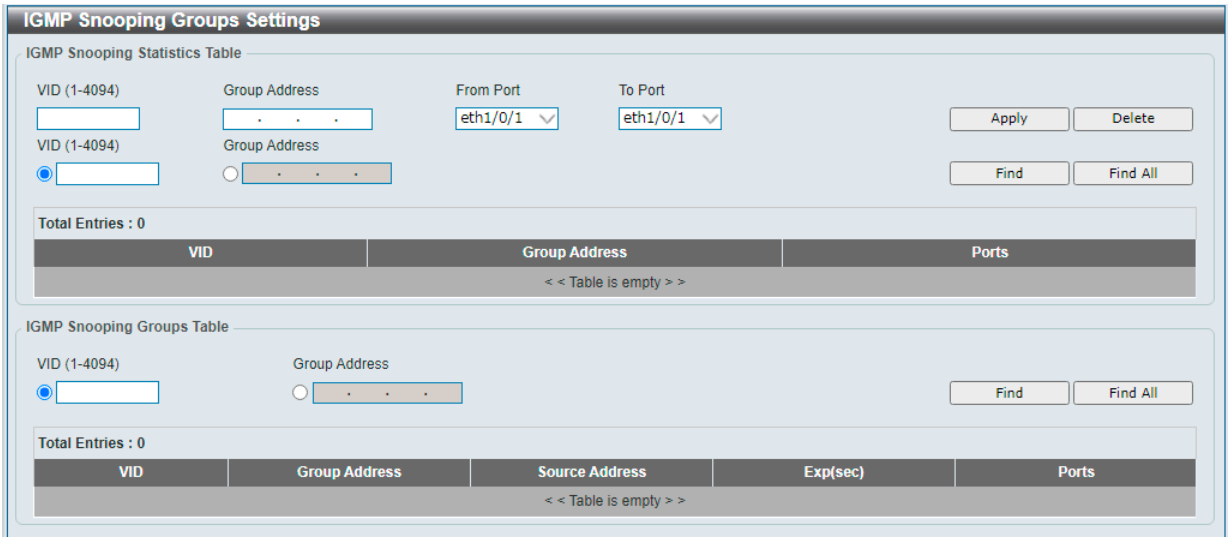


図 8-45　IGMP Snooping Group Settings 画面

画面に表示される項目：

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。
From Port / To Port	設定するポートの範囲を指定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 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。
IGMP Snooping Groups Table	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 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。

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、入力した情報に基づいて指定エントリを削除します。

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

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

IGMP Snooping マルチキャストルータポートの設定を行います。

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

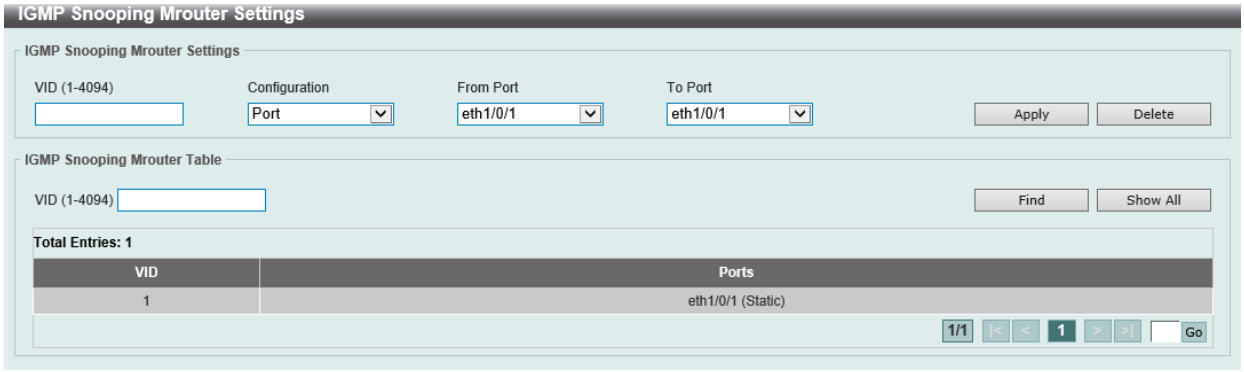


図 8-46　IGMP Snooping Mrouter Settings 画面

画面に表示される項目：

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 Port 」- ポートを非マルチキャストポートに指定します。
From Port / To Port	設定するポートの範囲を指定します。
IGMP Snooping Mrouter Table	
VID	VLAN ID を入力します。 • 設定可能範囲：1 - 4094

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、入力した情報に基づいて指定エントリを削除します。

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

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

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。

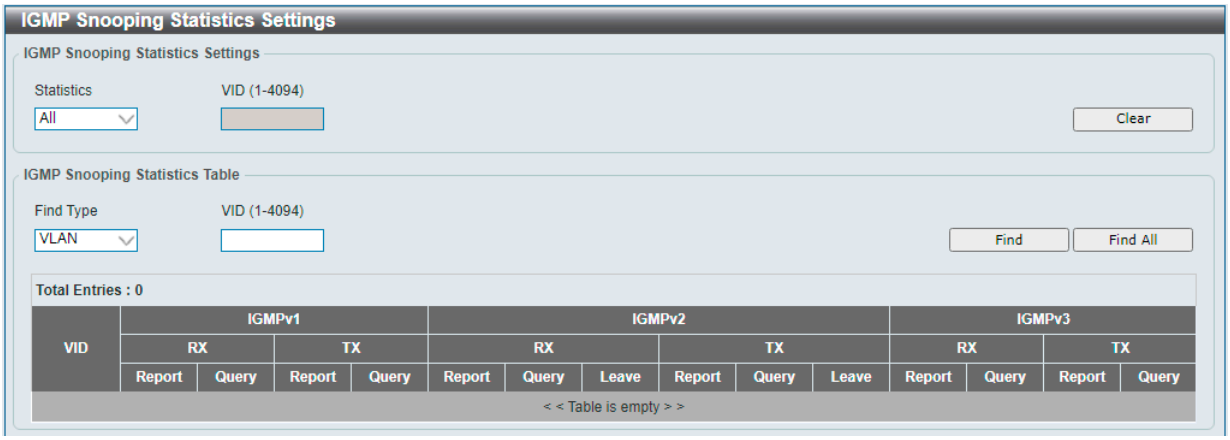


図 8-47　IGMP Snooping Statistics Settings 画面

画面に表示される項目：

項目	説明
IGMP Snooping Statistics Settings	
Statistics	インタフェースを選択します。 • 選択肢：「All」「VLAN」
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
IGMP Snooping Statistics Table	
Find Type	インタフェースを選択します。 • 選択肢：「VLAN」
VID	VLAN ID を指定します。 • 設定可能範囲：1 - 4094

「Clear」をクリックして、指定したエントリの統計情報をクリアします。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Find All」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 Snooping Settings（MLD スヌーピング設定）

MLD Snooping の設定を行います。

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。

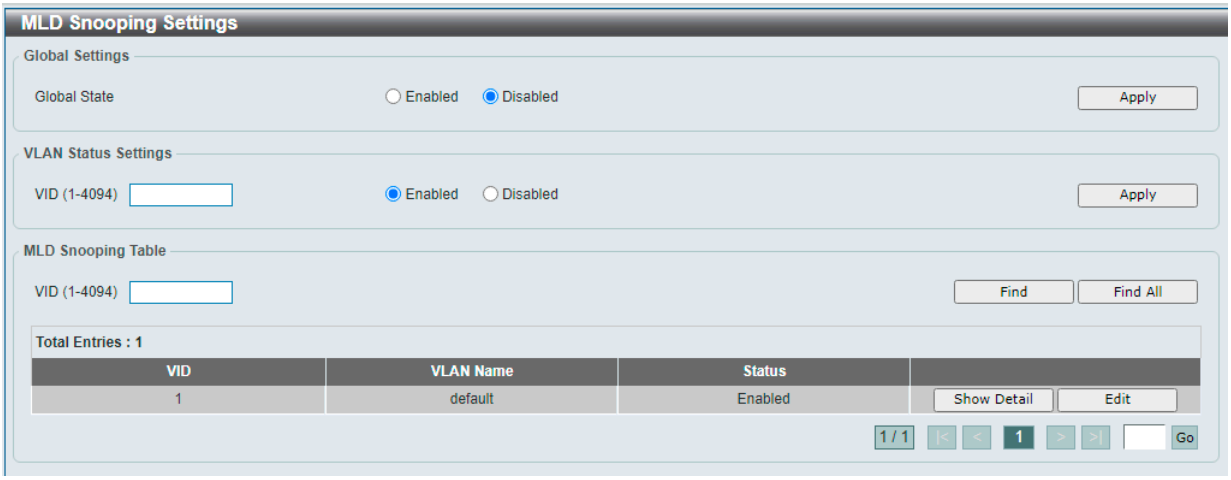


図 8-48　MLD Snooping Settings 画面

画面に表示される項目：

項目	説明
Global Settings	
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
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」をクリックして、設定内容を適用します。

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

「Edit」をクリックしてエントリを編集します。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

注意　MLD Snooping 機能では、Router Port へ Multicast Stream を フラッディングしません。

LD Snooping VLAN の詳細情報表示

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

図 8-49　MLD Snooping VLAN Parameters 画面

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

MLD Snooping 機能の詳細設定

「MLD Snooping Settings」で関連する VLAN エントリの「Edit」をクリック、または詳細情報画面の「Modify」をクリックし、以下の画面で各 VLAN に対して詳細な設定を行います。

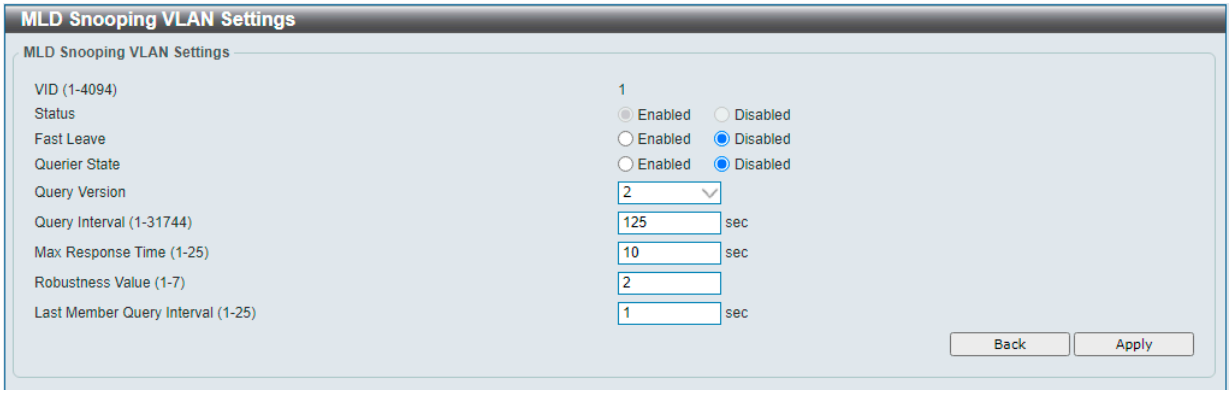


図 8-50 MLD Snooping VLAN Settings（Edit/Modify）画面

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	指定した VLAN の MLD Snooping 機能の有効 / 無効ステータスを表示します。
Fast Leave	Fast Leave 機能の有効 / 無効を設定します。 本機能が有効な場合、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。
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） • 初期値：125（秒）
Max Response Time	MLD スヌーピングクエリでアドバタイズされる最大応答時間を指定します。 • 設定可能範囲：1 - 25（秒） • 初期値：10（秒）
Robustness Value	MLD スヌーピングで使用する、パケットロスに対するロバストネス変数を指定します。 • 設定可能範囲：1 - 7
Last Listener Query Interval	MLD スヌーピングクエリアが MLD Group-Specific クエリまたは Group-Source-Specific（Channel）クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1 - 25（秒）

「Apply」をクリックして、設定内容を適用します。
「Back」をクリックして前の画面に戻ります。

注意　MLD Snooping 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、以下の画面を表示します。

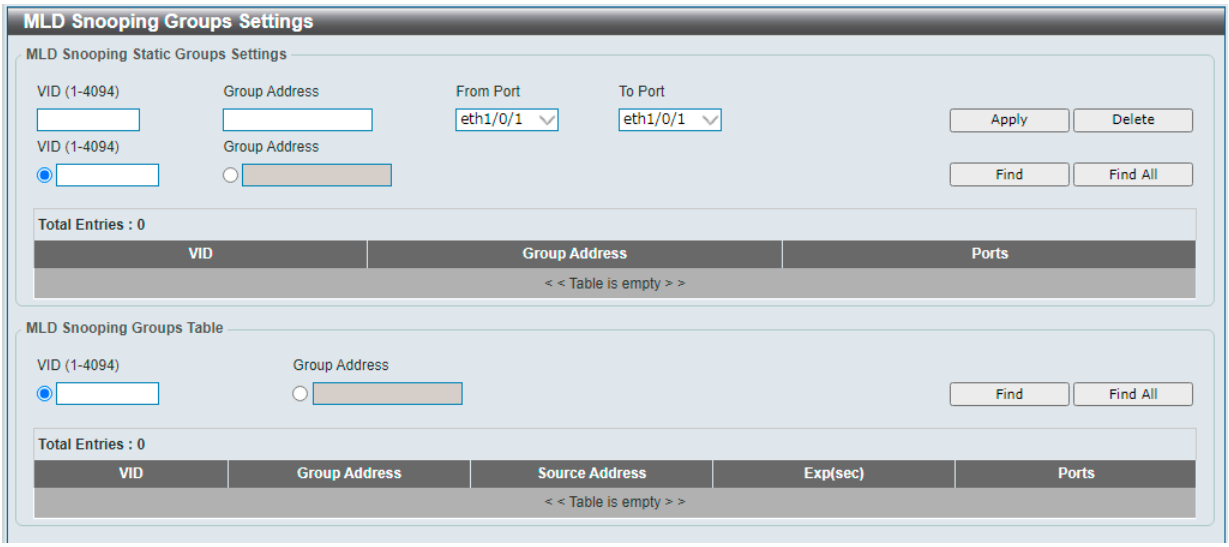


図 8-51　MLD Snooping Groups Settings 画面

画面に表示される項目：

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。
From Port / To Port	設定するポートの範囲を指定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 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。
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 IP アドレスを入力します。

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

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

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

VLAN インタフェースでマルチキャストルータポートの設定を行います。

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings をクリックし、以下の画面を表示します。

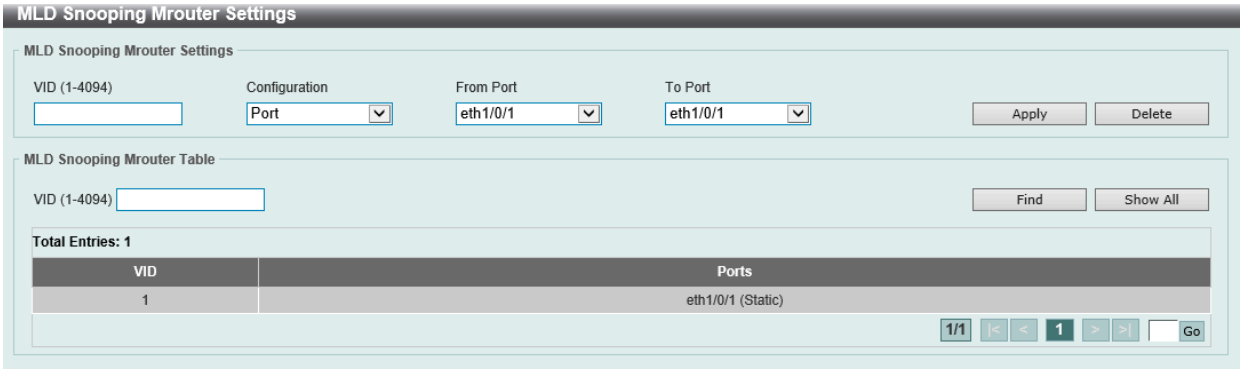


図 8-52　MLD Snooping Mrouter Settings 画面

画面に表示される項目：

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	ポートの設定を以下から選択します。 • 「Port」- マルチキャストが有効なルータと接続するポート範囲を設定します。 • 「Forbidden Port」- マルチキャストが有効なルータと接続しないポート範囲を設定します。
From Port / To Port	設定するポートの範囲を指定します。
MLD Snooping Mrouter Table	
VID	VLAN ID を入力します。 • 設定可能範囲：1 - 4094

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

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

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

MLD Snooping Statistics Settings（MLD Snooping 統計設定）

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。

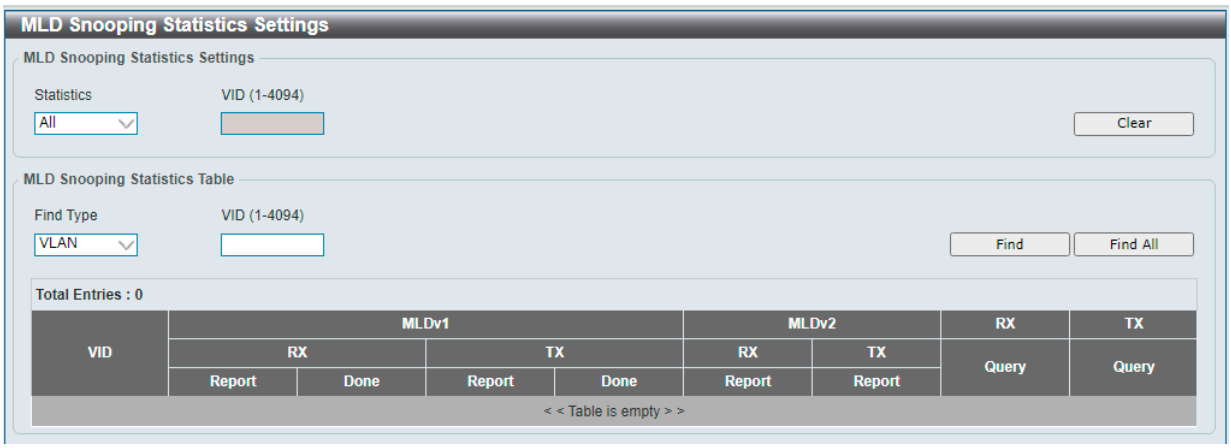


図 8-53　MLD Snooping Statistics Settings 画面

画面に表示される項目：

項目	説明
MLD Snooping Statistics Settings	
Statistics	インタフェースを選択します。 • 選択肢：「All」「VLAN」
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
MLD Snooping Statistics Table	
Find Type	インタフェースのタイプを選択します。 • 選択肢：「VLAN」
VID	VLAN ID を指定します。 • 設定可能範囲：1 - 4094

「Clear」をクリックして、指定したエントリの統計情報をクリアします。

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

Multicast Filtering（マルチキャストフィルタリング）

L2 マルチキャストフィルタリング設定を行います。

L2 Features > L2 Multicast Control > Multicast Filtering をクリックし、以下の画面を表示します。

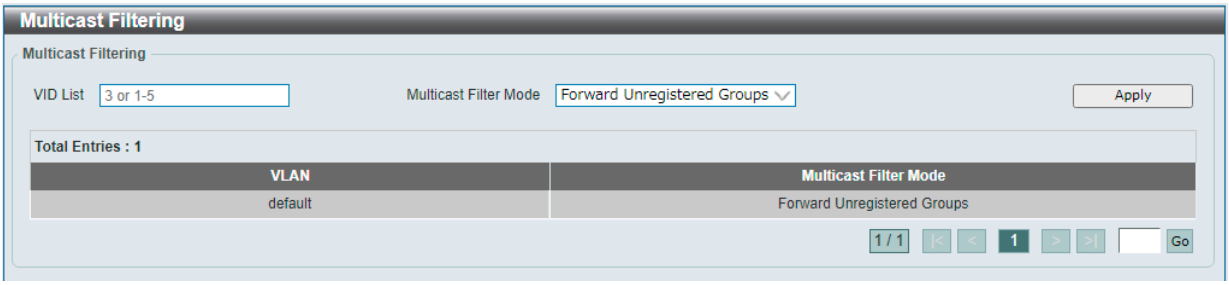


図 8-54　Multicast Filtering 画面

画面に表示される項目：

項目	説明
VID List	設定する VLAN の VLAN ID リストを入力します。
Multicast Filtering Mode	マルチキャストフィルタリングモードを選択します。 • 「Forward Unregistered Groups」- 登録されたマルチキャストパケットはフォワーディングテーブルに基づいて転送され、登録されていないマルチキャストパケットは VLAN ドメインにフラッドします。 • 「Filter Unregistered Groups」- 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。 • 「Forward All Groups」- 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。

「Apply」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（LLDP 設定）

LLDP（Link Layer Discovery Protocol）は、近隣ノードの情報を収集するための IEEE 802.1AB 準拠のプロトコルです。
隣接機器に自分の機器情報をアドバタイズ、または隣接機器の情報を学習します。
SNMP ユーティリティで LLDP デバイスの MIB 情報を取得することにより、ネットワークトポロジ情報を収集することができます。

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。

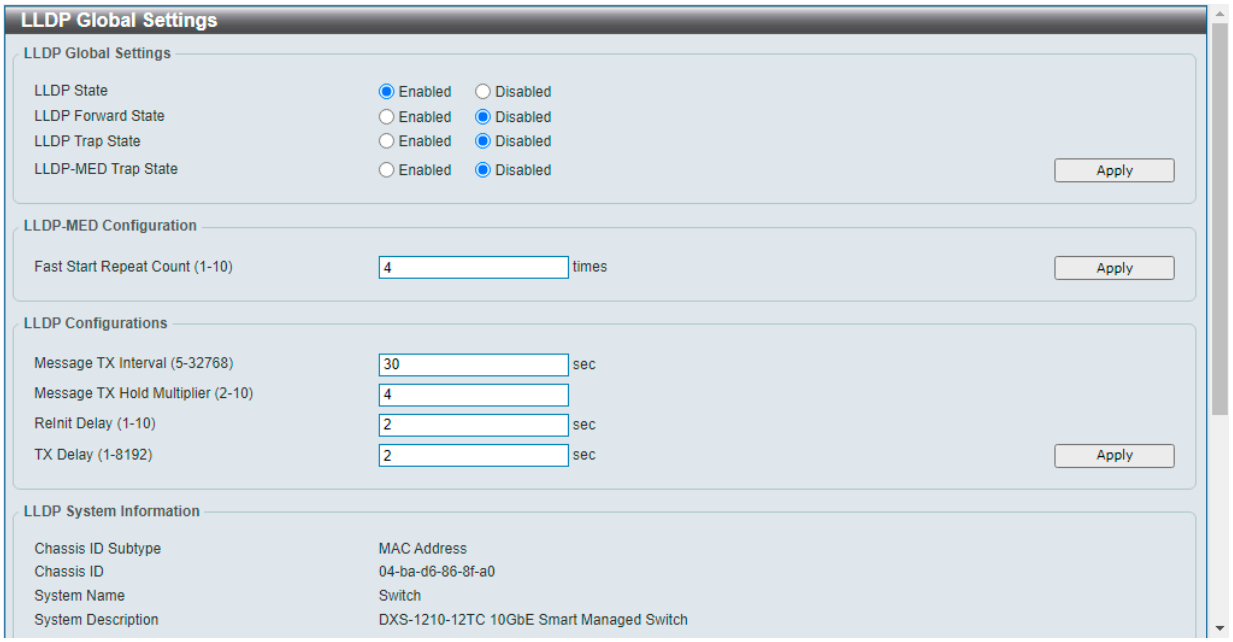


図 8-55　LLDP Global Settings 画面

画面に表示される項目：

項目	説明
LLDP Global Settings	
LLDP State	スイッチの LLDP 機能を有効 / 無効に設定します。 有効にした場合、スイッチは LLDP パケットの送受信、処理を行います。
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。 • 設定可能範囲：1 - 10
LLDP Configurations	
Message TX Interval	物理インタフェースの LLDP アドバタイズメント送信間隔を設定します。 • 設定可能範囲：5 - 32768（秒） • 初期値：30（秒）
Message TX Hold Multiplier	LLDPDU の TTL 値を計算するために使用される、LLDPDU 転送間隔に対する乗数を指定します。 • 設定可能範囲：2 - 10 • 初期値：4
Relnit Delay	管理ステータスが無効化されてから 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。 • 設定可能範囲：1 - 10（秒） • 初期値：2（秒）
TX Delay	インタフェースで LLDPDU を送信するまでの待機時間を指定します。転送間隔の数値の 1/4 より大きくすることはできません。 • 設定可能範囲：1 - 8192（秒） • 初期値：2（秒）

「Apply」をクリックして、設定内容を適用します。

画面下部の「LLDP System Information」「LLDP-MED System Information」セクションには、本スイッチの LLDP 構成情報が表示されます。

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。

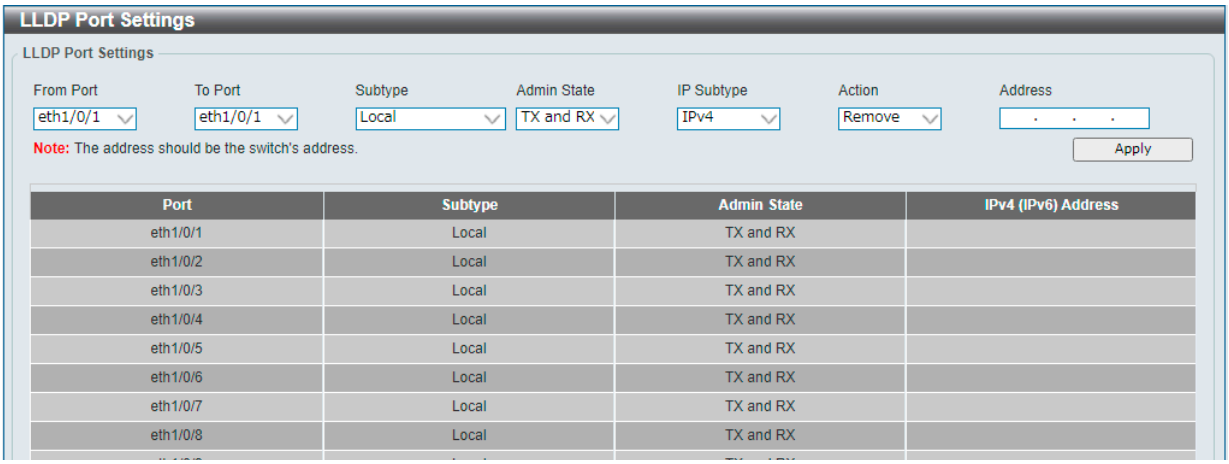


図 8-56　LLDP Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Subtype	LLDP TLV のサブタイプを選択します。 • 選択肢：「Local」「MAC Address」
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 フレームの送信のみ行います。 • 「RX」- ローカル LLDP エージェントは LLDP フレームの受信のみ行います。 • 「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：「IPv4」「IPv6」
Action	実行する動作を選択します。 • 選択肢：「Remove」「Add」
Address	送信する IP アドレスを入力します。

「Apply」をクリックして、設定内容を適用します。

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 8-57　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」をクリックし、LLDP 管理情報を検索します。

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

隣接デバイスに送信する LLDP の Type-Length-Value（TLV）設定を行います。
本画面では、基本情報セットのオプション項目を設定します。

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

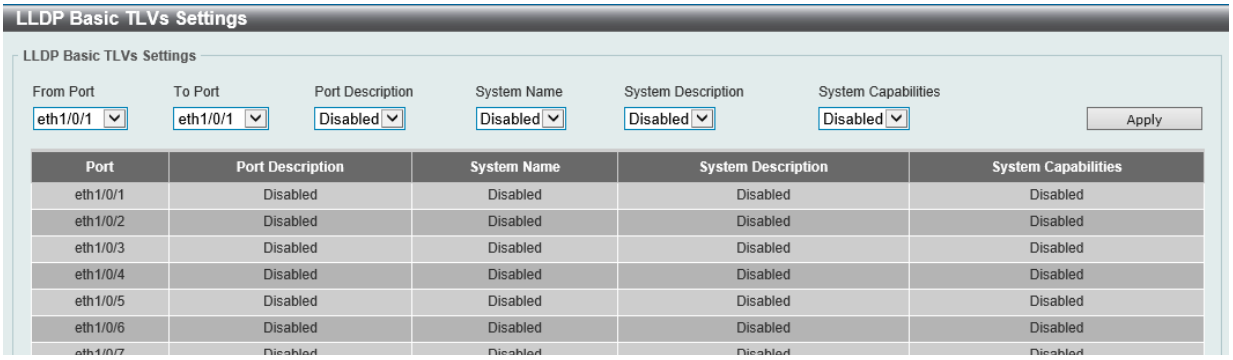


図 8-58　LLDP Basic TLVs Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
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」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）

LLDP で送信する IEEE802.1 Organizationally Specific TLV のオプション項目を設定します。

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。

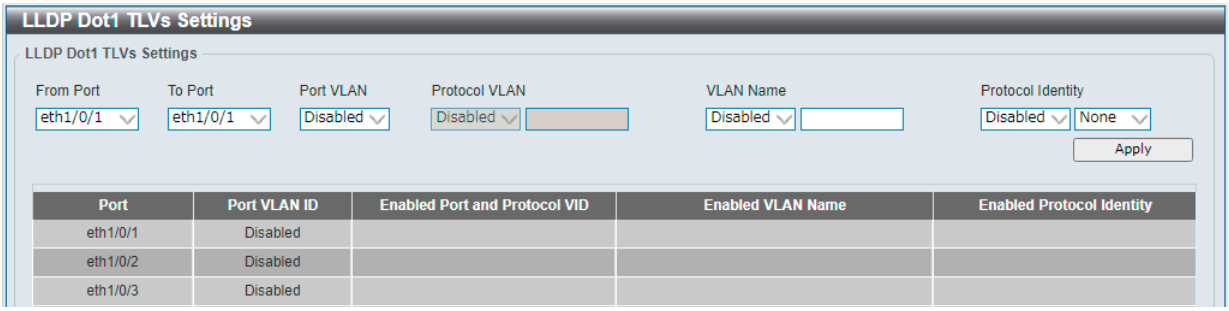


図 8-59　LLDP Dot1 TLVs Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Port VLAN	ポート VLAN ID TLV の送信を有効 / 無効に設定します。 ポート VLANID TLV は、オプションの固定長 TLV です。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」付きフレームに紐づくポート VLAN ID（PVID）を通知できます。
Protocol VLAN	本項目の設定は未サポートです。（デフォルトで無効）
VLAN Name	VLAN 名 TLV の送信を有効 / 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 の送信を有効 / 無効に設定します。 対象とするプロトコルを以下から選択します。 • 選択肢：「None」「EAPOL」「LACP」「GVRP」「STP」「All」

「Apply」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）

LLDP で送信する IEEE 802.3 Organizationally Specific TLV のオプション項目を設定します。

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。

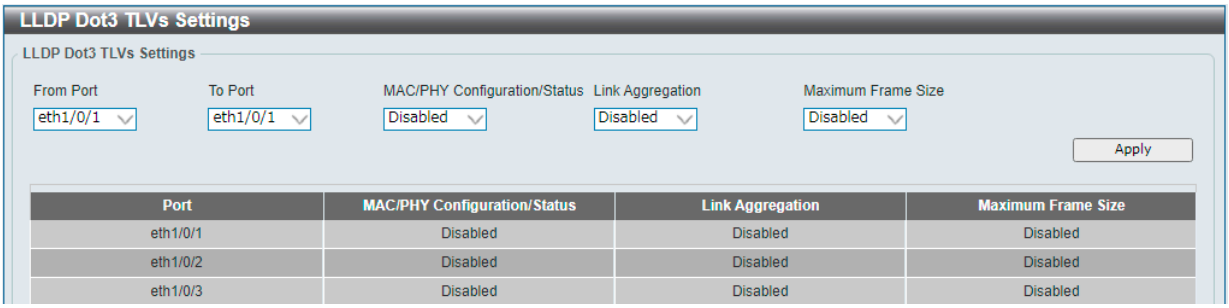


図 8-60　LLDP Dot3 TLVs Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
MAC/PHY Configuration/Status	MAC/PHY Configuration/Status TLV の通知を有効 / 無効に設定します。 MAC/PHY Configuration/Status TLV には以下の情報が含まれます。 （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
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、実装されている MAC/PHY の最大フレームサイズ Capability を示します。

項目	説明
Power Via MDI （DXS-1210-10MP のみ）	power via MDI TLV の通知を有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

注意　LLDP を使用する PoE 給電において、クラス 6 ネゴシエーションはサポートされません。

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

LLDP で送信する LLDP-MED TLV のオプション項目を設定します。

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

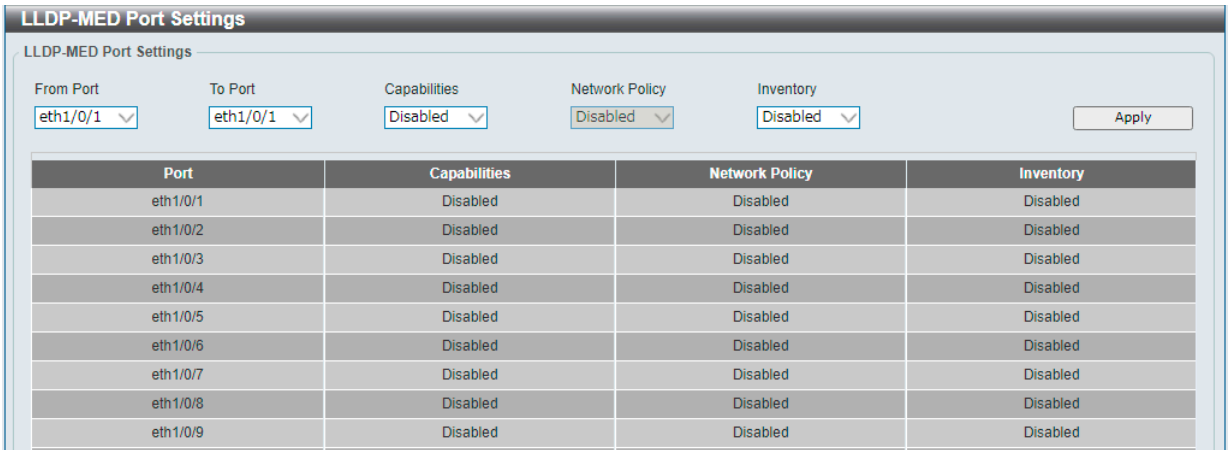


図 8-61　LLDP-MED Port Settings 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Capabilities	「LLDP-MED capabilities TLV」の送信を有効 / 無効に設定します。
Network Policy	本項目の設定は未サポートです。（デフォルトで無効）
Inventory	「LLDP-MED inventory TLV」の送信を有効 / 無効に設定します。

「Apply」をクリックし、変更を適用します。

LLDP Statistics Information（LLDP 統計情報）

スイッチにおける LLDP 統計情報を参照できます。

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

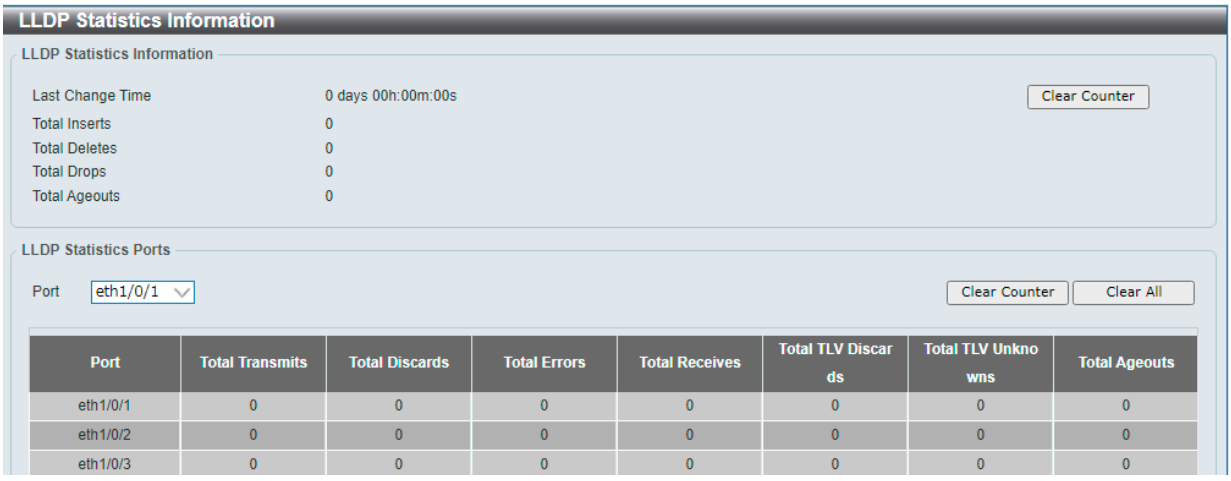


図 8-62　LLDP Statistics Information 画面

画面に表示される項目：

項目	説明
LLDP Statistics Information	

項目	説明
Last Change Time	リモートテーブルへの変更が検出されてからの経過時間が表示されます。
Total Inserts	スイッチを再起動してから新しく追加されたエントリの数を表示します。
Total Deletes	スイッチを再起動してから新しく削除されたエントリの数を表示します。
Total Drops	管理テーブルの空き容量不足により破棄された LLDP フレームの数を表示します。
Total Ageouts	Time-To-Live の有効期限切れにより削除されたエントリの数を表示します。
LLDP Statistics Ports	
Port	カウンタをクリアするポートを指定します。
Total Transmits	ポートで送信された LLDP フレームの総数を表示します。
Total Discards	ポートで受信した LLDP フレームの総廃棄フレーム数を表示します。
Total Errors	ポートで受信した LLDP フレームのエラーフレーム数を表示します。
Total Receives	ポートで受信した LLDP フレームの総数を表示します。
Total TLV Discards	各 LLDP フレームには、TLV と呼ばれる複数の情報を含めることができます。TLV の形式が不正な場合は、カウントされて破棄されます。
Total TLV Unknowns	ポートで受信した未知の情報（TLV）の数を表示します。
Total Ageouts	各 LLDP フレームには、LLDP 情報の有効期間に関する情報が含まれます。エージアウト時間内に新しい LLDP フレームが受信されない場合、LLDP 情報は削除され、Age-Out カウンタが増加します。

「LLDP Statistics Information」セクションの「Clear Counter」をクリックして、当該セクションの統計情報をクリアします。
「LLDP Statistics Ports」セクションの「Clear Counter」をクリックして、指定したポートの統計情報のカウンタ数をクリアします。
「Clear All」をクリックしてすべてのカウンタ数をクリアします。

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

LLDP ローカルポート情報を表示します。

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

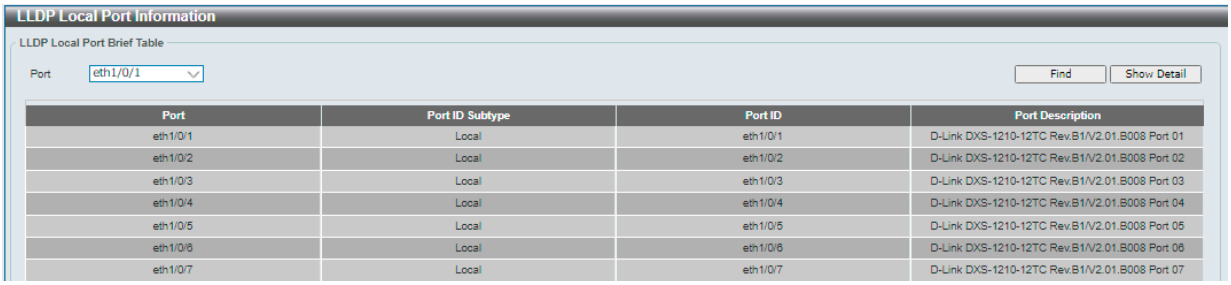


図 8-63　LLDP Local Port Information 画面

画面に表示される項目：

項目	説明
Port	表示するポートを指定します。
表示項目	
Port	ポート番号を表示します。
Port ID Subtype	ポート ID サブタイプを表示します。
Port ID	ポート ID（ユニット番号 / ポート番号）を表示します。
Port Description	ポートの説明を表示します。

「Find」をクリックし、指定ポートの情報を表示します。

■ **詳細情報の参照**

「Show Detail」をクリックし、以下の画面を表示します。

図 8-64　LLDP Local Port Information（Show Detail）画面

各項目の「Show Detail」をクリックすると、関連する詳細情報が表示されます。
「Back」をクリックすると前画面に戻ります。

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

ネイバ から学習した LLDP 情報を表示します。
スイッチはリモートステーションからパケットを受信し、その情報をローカルに保存します。

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 8-65　LLDP Neighbor Port Information 画面

画面に表示される項目：

項目	説明
Port	表示するポートを指定します。

「Find」をクリックし、指定ポートの情報を表示します。
「Clear」をクリックしてポート情報をクリアします。
「Clear All」をクリックして、アドレステーブルのすべての情報をクリアします。

「Show Detail」をクリックすると該当ポートの詳細が表示されます。

図 8-66　LLDP Neighbor Port Information 画面

各項目の「Show Detail」をクリックすると、関連する詳細情報が表示されます。
「Back」をクリックすると前画面に戻ります。

第 9 章　L3 Features（レイヤ 3 機能の設定）

L3 Features メニューを使用し、本スイッチにレイヤ 3 機能を設定することができます。

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

サブメニュー	説明
ARP（ARP 設定）	ARP の設定、編集を行います。
IPv4 Interface（IPv4 インタフェース）	IPv4 アドレスのインタフェースの設定を行います。
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート）	IPv4 アドレスのスタティック / 初期ルートの設定を行います。
IPv4 Route Table（IPv4 ルートテーブル）	IPv4 のルートテーブルの設定を行います。
IPv6 Interface（IPv6 インタフェース）	IPv6 アドレスのインタフェースの設定を行います。
IPv6 Neighbor（IPv6 Neighbor 設定）	IPv6 ネイバ設定を行います。
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート）	IPv6 アドレスのスタティック / 初期ルートの設定を行います。
IPv6 Route Table（IPv6 ルートテーブル）	IPv6 のルートテーブルの設定を行います。
DNS Server Settings（DNS サーバ設定）	DNS サーバの設定を行います。

注意　トラフィックが大量に発生した際に、スイッチの接続が一時的に切断しパケットがルーティングされない場合があります。

ARP（ARP 設定）

ARP（Address Resolution Protocol）は、IP アドレスによってネットワーク上のホストの MAC アドレスを得るためのアドレス解決プロトコルです。
特定のデバイスに対する ARP 情報を参照、編集および削除することができます。

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 9-1　ARP Aging Time 画面

画面に表示される項目：

項目	説明
Timeout	「Edit」をクリックして、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。 • 設定可能範囲：0 - 65535（分）

「Edit」ボタンを選択して特定エントリの値を編集し、「Apply」をクリックして適用します。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

補足　ARP エントリ数は最大 768 です。

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。

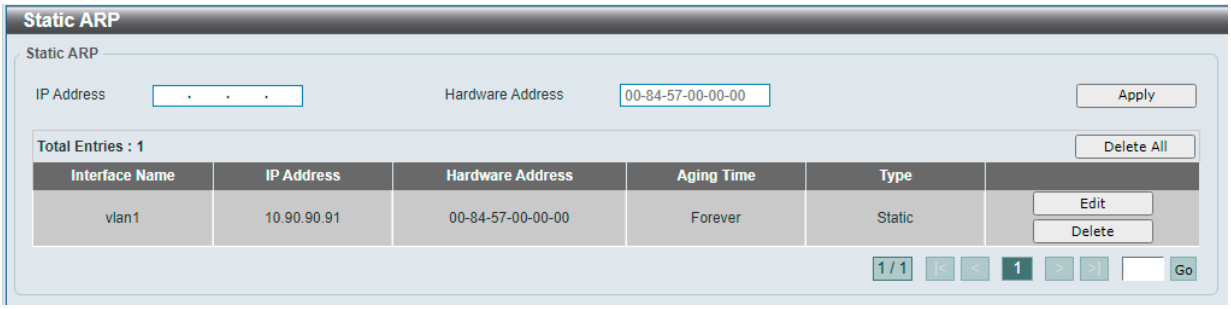


図 9-2　Static ARP 画面

画面に表示される項目：

項目	説明
IP Address	MAC アドレスと紐づける IP アドレスを設定します。
Hardware Address	IP アドレスと紐づける MAC アドレスを設定します。

「Apply」をクリックして、設定内容を適用します。
「Edit」をクリックして、指定エントリの編集を行います。
「Delete」をクリックして、エントリを削除します。
「Delete All」をクリックして、すべてのエントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

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 の順にクリックし、以下の画面を表示します。

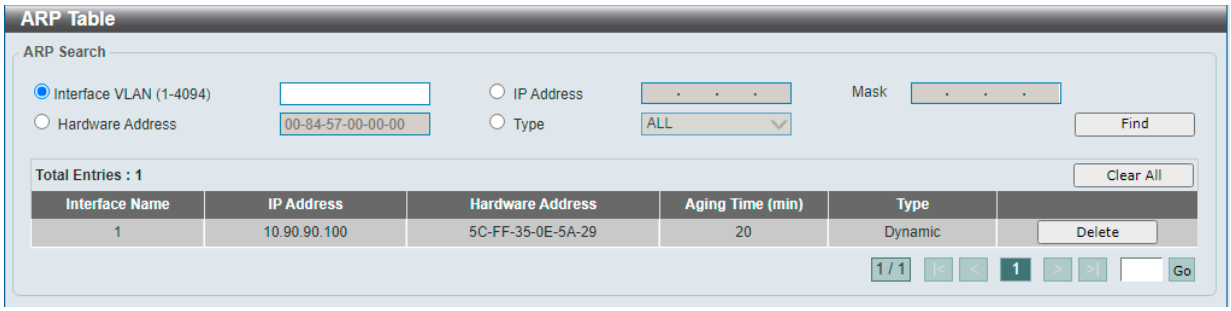


図 9-3　ARP Table 画面

画面に表示される項目：

項目	説明
Interface VLAN	表示するインタフェースの VLAN ID を入力します。 • 設定可能範囲：1 - 4094
IP Address	表示する IP アドレスを入力します。
Mask	上記 IP アドレスのマスクを指定します。
Hardware Address	表示する MAC アドレスを入力します。
Type	表示する ARP の種類を指定します。 • 選択肢：「ALL」「Dynamic」

「Find」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」をクリックするとテーブル上のエントリが全て消去されます。
削除するエントリの「Delete」をクリックするとエントリが削除されます。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

補足　Gratuitous ARP による ARP テーブルの更新には対応していません。

補足　ARP エントリは、対応する MAC アドレステーブルのエージングアウト契機により削除されます。

IPv4 Interface（IPv4 インタフェース）

IPv4 インタフェースの設定を行います。

補足　設定可能な IPv4 インタフェースは最大 8 つまでです。

補足　DHCP Relay をサポートしていません。

L3 Features > IPv4 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。

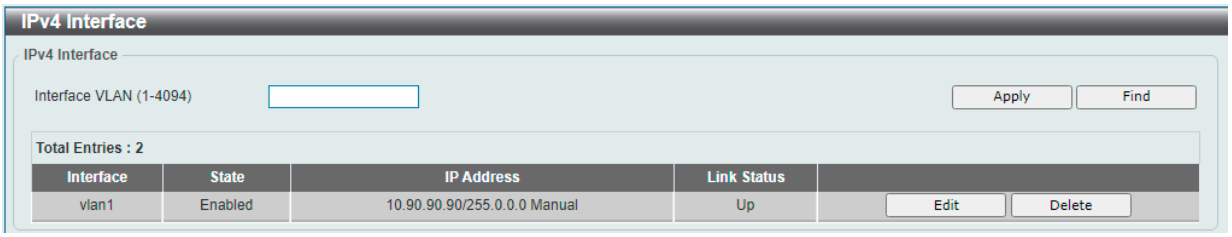


図 9-4　IPv4 Interface 画面

画面に表示される項目：

項目	説明
Interface VLAN	設定、表示するインタフェースの VLAN ID を入力します。 • 設定可能範囲：1 - 4094

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

設定するエントリの「Edit」をクリックして、以下の画面を表示します。

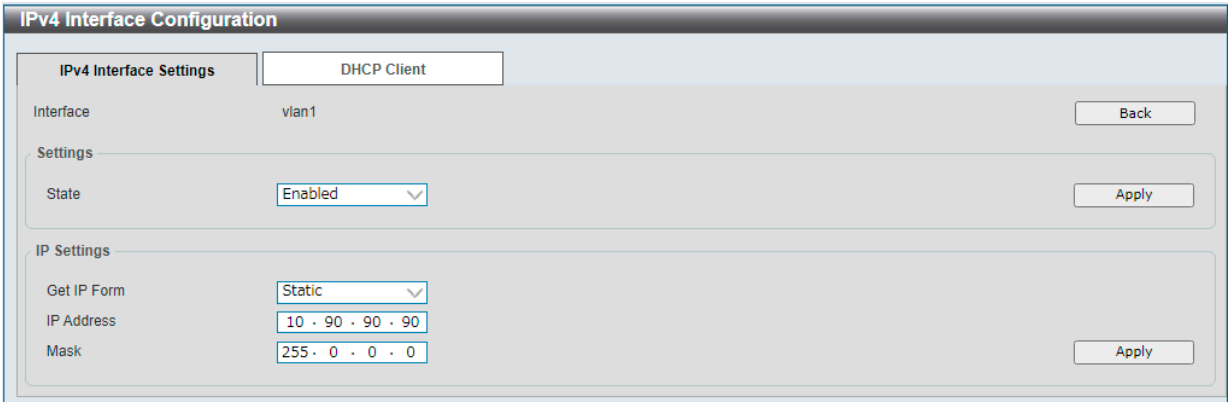


図 9-5　IPv4 Interface Configuration - IPv4 Interface Settings 画面

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 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。

「Apply」をクリックして、設定内容を適用します。

IPv4 インタフェースの編集（DHCP Client タブ）

設定するエントリの「Edit」をクリック →「IPv4 Interface Configuration」画面の「DHCP Client」タブをクリックして以下の画面を表示します。

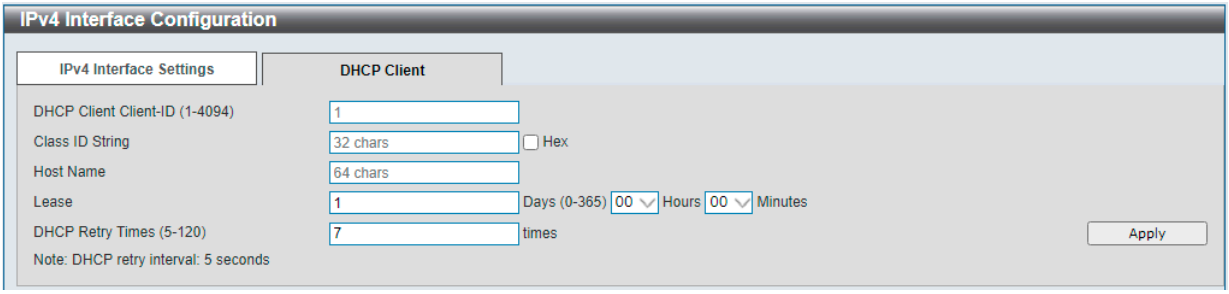


図 9-6　IPv4 Interface Configuration - DHCP Client タブ 画面

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 進数方式になります。（64 文字以内） DHCP DISCOVER メッセージと一緒に送信されるオプション 60 のベンダクラス識別子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。リース日数、時間と分を指定することができます。 • 設定可能範囲：0 - 365（日）
DHCP Retry Times	DHCP 再試行回数を入力します • 設定可能範囲：5 - 120（回） • 初期値：7（回）

「Apply」をクリックして、設定内容を適用します。

IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート）

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。

L3 Features > IPv4 Static/Default Route 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 9-7　IPv4 Static/Default Route 画面

画面に表示される項目：

項目	説明
IP Address	スタティックルートに割り当てる IPv4 アドレスを入力します。 デフォルトルートとして設定するには、「Default Route」にチェックを入れます。
Mask	このルートのサブネットマスクを入力します。
Gateway	このルートのゲートウェイ IP アドレスを入力します。 デフォルトルートの場合、これがデフォルトゲートウェイになります。

項目	説明
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。 各ネットワークには 1 つのプライマリルートのみ設定可能です。他のルートはバックアップ状態に割り当てる必要があります。本スイッチは、プライマリルートに障害が発生した場合のバックアップとして、フローティングスタティックルートがサポートされており、別のネクストホップへの代替スタティックルートを作成できます。このセカンダリネクストホップデバイスルートは、プライマリスタティックルートがダウンしている場合、バックアップスタティックルートと見なされます。プライマリルートが失われると、バックアップルートがアクティブになります。

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、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」をクリックして、特定のページへ移動することができます。

IPv4 Route Table（IPv4 ルートテーブル）

IPv4 ルートテーブルの設定を行います。

L3 Features > IPv4 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。

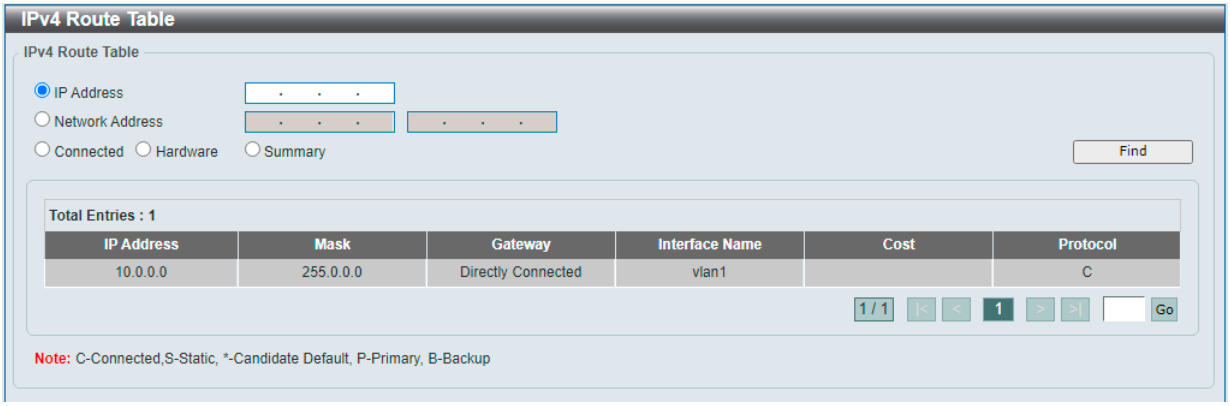


図 9-8　IPv4 Route Table 画面

画面に表示される項目：

項目	説明
IP Address	表示するルートの宛先 IP アドレスを指定します。
Network Address	表示するルートの宛先ネットワークアドレスを指定します。
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	アクティブなルーティングエントリのサマリが表示されます。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

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 Interface（IPv6 インタフェース）

IPv6 インタフェースの設定を行います。

補足　IPv6 インタフェースは最大 8 つまで作成可能です。

補足　/64 より長い Prefix 長に対応します。

L3 Features > Interface > 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 9-9　IPv6 Interface 画面

画面に表示される項目：

項目	説明
Interface VLAN	設定、表示する 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」をクリックして、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Detail」をクリックして、IPv6 インタフェースエントリの詳細設定を行います。

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

設定するエントリの「Detail」をクリックして、「IPv6 Interface Settings」タブを表示します。

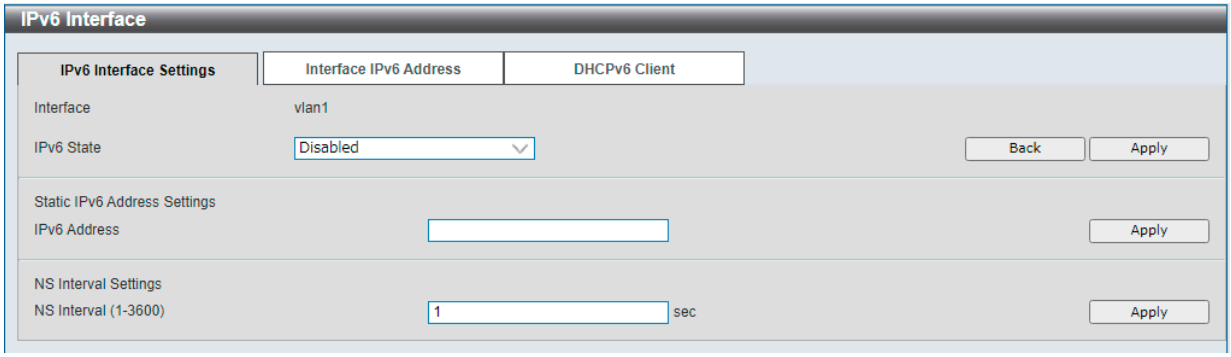


図 9-10　IPv6 Interface - IPv6 Interface Settings 画面

画面に表示される項目：

項目	説明
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。
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。
NS Interval Settings	
NS Interval	Neighbor Solicitation（NS）間隔を指定します。 • 設定可能範囲：1 - 3600（秒）

「Apply」をクリックして、設定内容を適用します。

注意　IPv6 RA の送信、Managed Flag、Other Flag には対応していません。

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

設定するエントリの「Detail」をクリックして、「Interface IPv6 Address」タブを表示します。

図 9-11　IPv6 Interface - Interface IPv6 Address 画面

「Delete」をクリックして、エントリを削除します。

IPv6 インタフェースの編集（DHCPv6 Client タブ）

設定するエントリの「Detail」をクリックして、「DHCPv6 Client」タブを表示します。

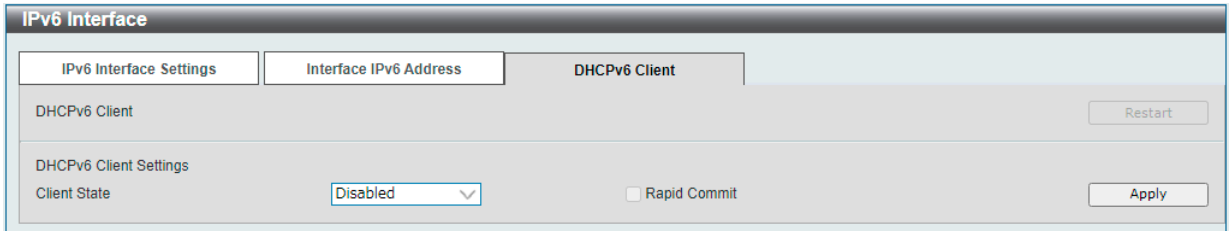


図 9-12　IPv6 Interface - DHCPv6 Client 画面

画面に表示される項目：

項目	説明
DHCPv6 Client	「Restart」をクリックすると、DHCPv6 クライアントサービスを再起動します。
Client State	DHCPv6 クライアントを有効 / 無効に設定します。 「Rapid Commit」オプションにチェックを入れると、アドレス委任の際、4 つのメッセージ交換の代わりに 2 つのメッセージ交換を実行します。Solicit メッセージには、2 つのメッセージのハンドシェイクを要求するための Rapid Commit オプションが含まれます。

「Apply」をクリックして、設定内容を適用します。

IPv6 Neighbor（IPv6 Neighbor 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て、以下の画面を表示します。

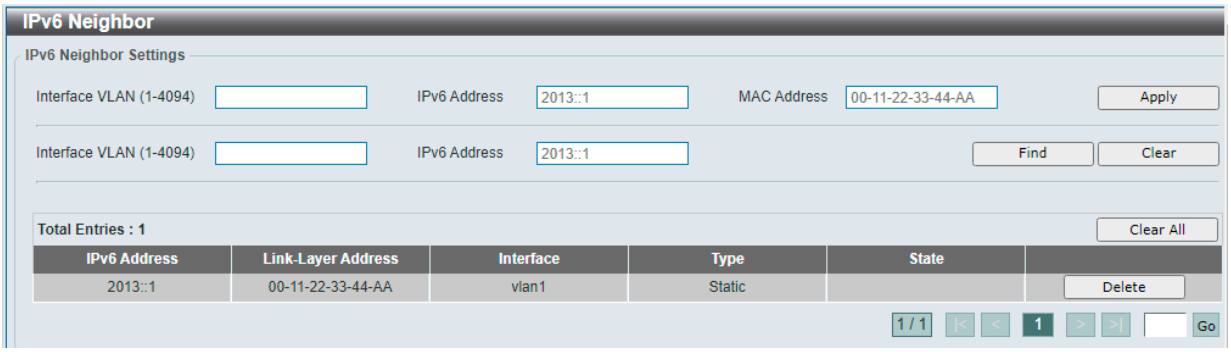


図 9-13　IPv6 Neighbor 画面

画面に表示される項目：

項目	説明
Interface VLAN	IPv6 ネイバのインタフェース VLAN を指定します。 • 設定可能範囲：1 - 4094
IPv6 Address	ネイバ IPv6 アドレスを入力します。
MAC Address	MAC アドレスを指定します。

「Apply」をクリックして、設定内容を適用します。
「Find」をクリックして、入力内容を基にエントリを検索します。

「Clear」をクリックして、指定のインタフェースの情報を削除します。
「Clear All」をクリックして、テーブルのすべての情報をクリアします。

「Delete」をクリックして、指定のエントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート）

IPv6 スタティック / デフォルトルートを表示、設定します。

L3 Features > IPv6 Static/Default Route 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。

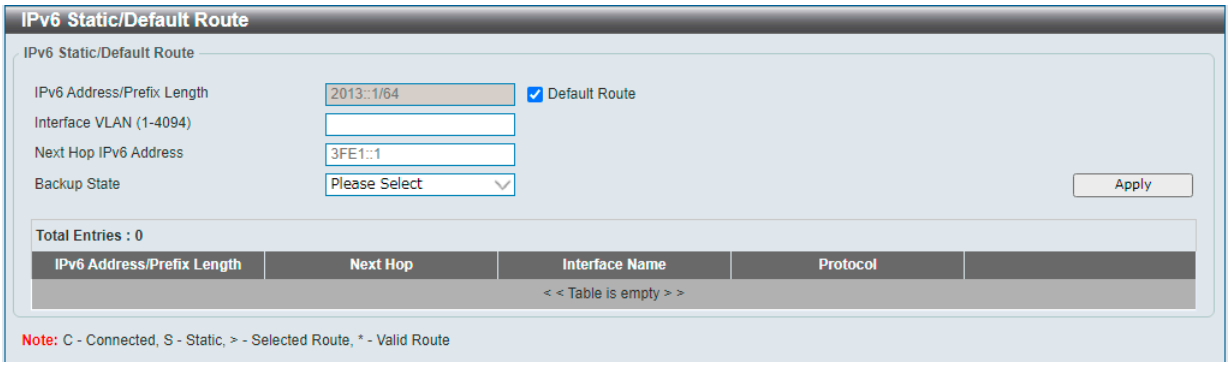


図 9-14　IPv6 Static/Default Route 画面

画面に表示される項目：

項目	説明
IPv6 Address/Prefix Length	ルートの IPv6 アドレスとプレフィックス長を入力します。デフォルトルートとして割り当てるには、「Default Route」オプションを選択します。
Interface VLAN	このルートに関連付けるインタフェース VLAN ID を入力します。
Next Hop IPv6 Address	ネクストホップ IPv6 アドレスを入力します。

項目	説明
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設定されます。 • 「Backup」- 宛先へのバックアップルートとして設定されます。

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

IPv6 Route Table（IPv6 ルートテーブル）

現在の IPv6 ルーティングテーブルを表示します。

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

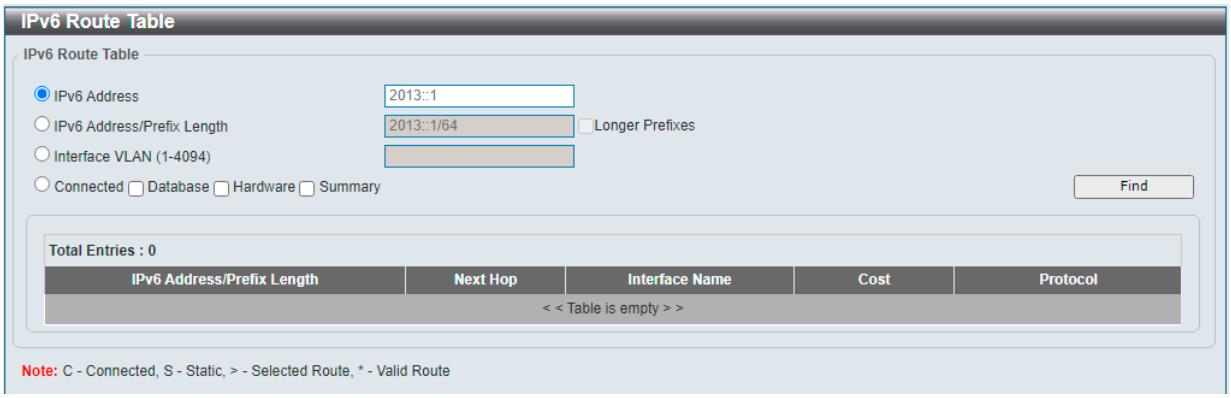


図 9-15　IPv6 Route Table 画面

画面に表示される項目：

項目	説明
IPv6 Address	表示するルートの宛先 IP アドレスを指定します。
IPv6 Address/Prefix Length	表示するルートの IPv6 アドレスとプレフィックス長を入力します。 「Longer Prefixes」を選択すると、指定プレフィックス長以上の IPv6 ルートを表示します。
Interface VLAN	表示するインタフェース VLAN ID を入力します。
Connected	接続されたルートのみ表示します。
Database	ルーティングデータベースのエントリをすべて表示します。
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	アクティブなルーティングエントリのサマリが表示されます。

「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。

DNS Server Settings（DNS サーバ設定）

DNS サーバを設定します。

L3 Features > DNS Server 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。

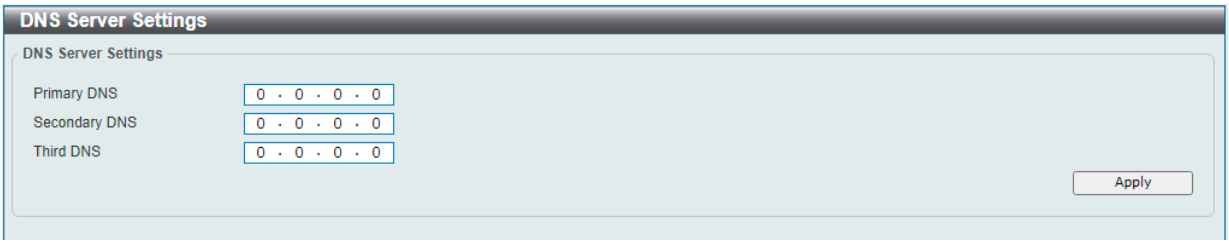


図 9-16　DNS Server Settings 画面

画面に表示される項目：

項目	説明
Primary DNS	プライマリ DNS を入力します。
Secondary DNS	セカンダリ DNS を入力します。
Third DNS	ターシャリ DNS を入力します。

「Apply」をクリックして、設定内容を適用します。

第 10 章　QoS（QoS 機能の設定）

本スイッチは、802.1p キューイング QoS（Quality of Service）をサポートしています。

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

サブメニュー	説明
Port Default CoS（ポートデフォルト CoS 設定）	各ポートにデフォルト CoS の設定を行います。
Port Scheduler Method（ポートスケジューラメソッド設定）	ポートスケジューラメソッドを設定します。
Queue Settings（QoS 設定）	キューを設定、表示します。
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。
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。
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。
Port Trust State（ポートトラスト設定）	ポートトラスト設定を行います。
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。

Port Default CoS（ポートデフォルト CoS 設定）

各ポートにデフォルト CoS の設定を行います。

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

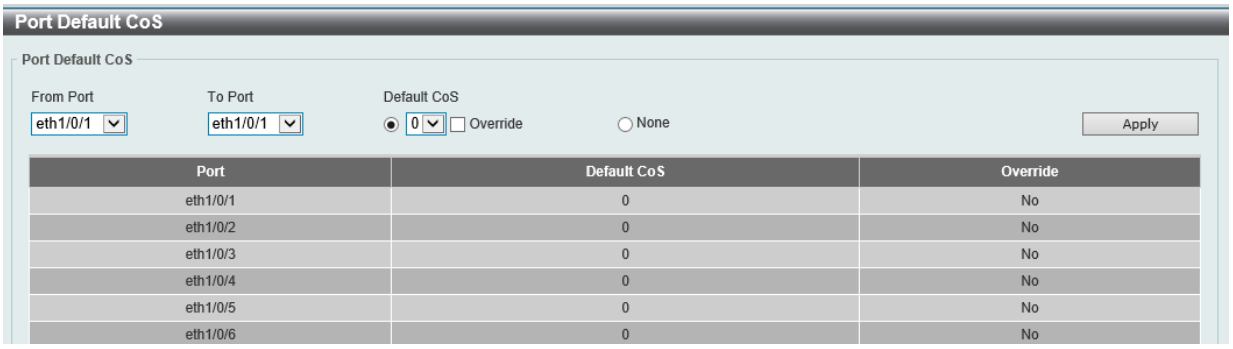


図 10-1　Port Default CoS 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Default CoS	ポートのデフォルト CoS を指定します。 「Override」にチェックを入れない場合、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。「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」を指定した場合、初期値に戻ります。 • 設定可能範囲：0 - 7

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

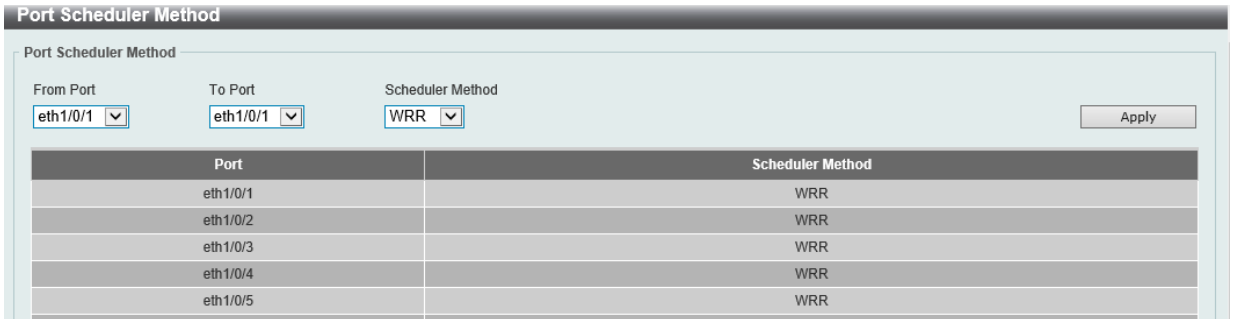


図 10-2　Port Scheduler Method 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Scheduler Method	指定ポートに対するスケジューリングの方法を設定します。 • 「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） • 「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。

「Apply」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 > 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
From Port / To Port	設定するポートの範囲を指定します。
Queue ID	キュー ID を指定します。 • 設定可能範囲：0 - 7
WRR Weight	WRR の値を入力します。 • 設定可能範囲：0 - 127

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

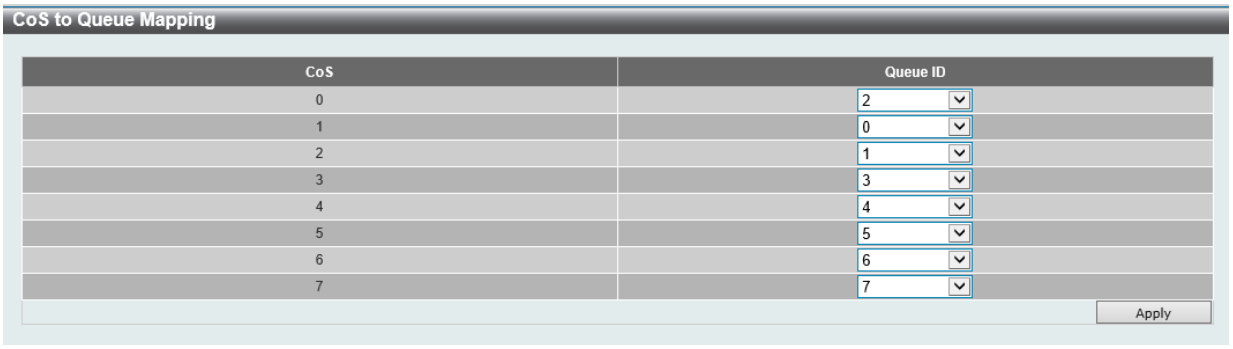


図 10-4　CoS to Queue Mapping 画面

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」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 > 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。

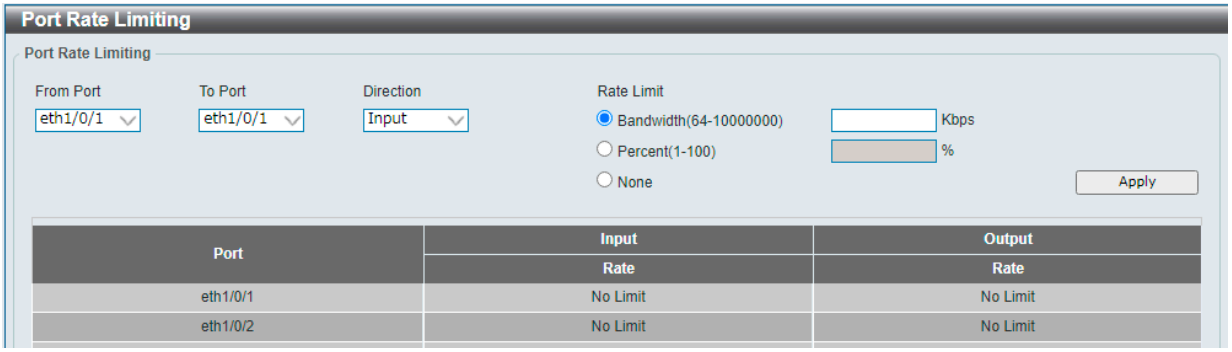


図 10-5　Port Rate Limiting 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Direction	レート制限の対象を指定します。 • 「Input」- イングレスパケットに対してレート制限を行います。 • 「Output」- イーグレスパケットに対してレート制限を行います。
Rate Limit	レート制限の値を指定します。 受信トラフィックがイングレス帯域幅の設定値を超えると、受信側は PAUSE フレームまたはフロー制御フレームを送信する場合があります。 • 「Bandwidth」- 受信 / 送信の帯域幅の値を入力欄に入力します。 - 設定可能範囲：64 - 10000000（Kbps） • 「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（%）） • 「None」- 指定ポートのレート制限を削除します。

「Apply」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 > 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。

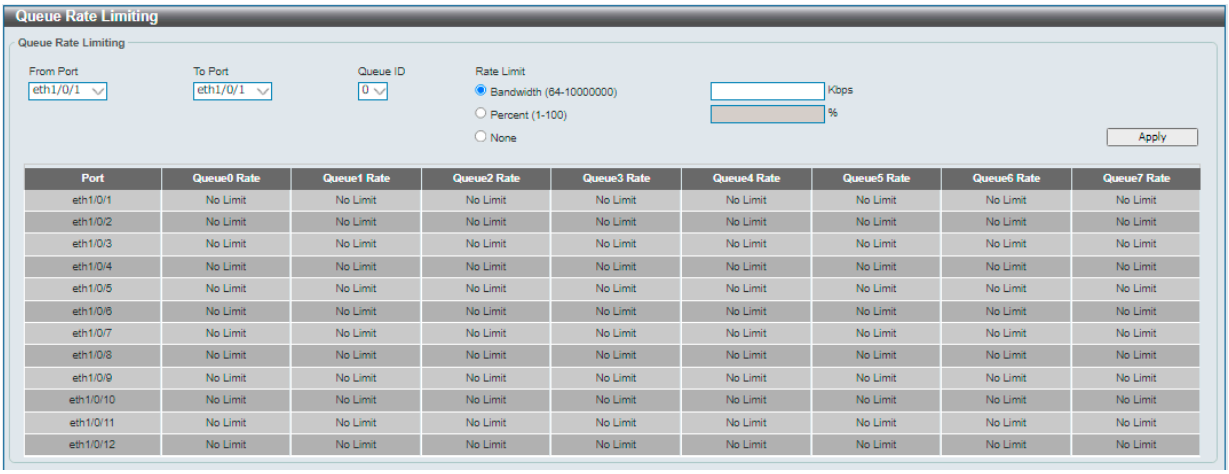


図 10-6　Queue Rate Limiting 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
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。 •「Bandwidth」- 帯域レート制限値を入力します。 - 設定可能範囲：64-10000000（Kbps） •「Percent」- 帯域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。

「Apply」をクリックして、設定内容を適用します。

Port Trust State（ポートトラスト設定）

ポートトラスト設定を行います。

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

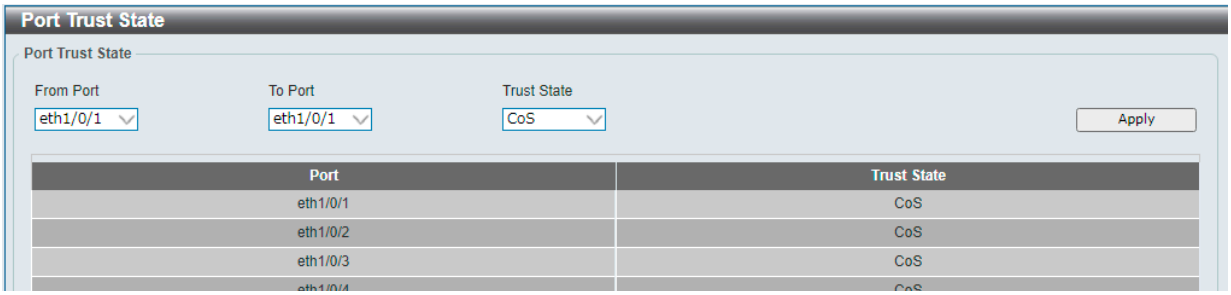


図 10-7　Port Trust State 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Trust State	ポートトラストのオプションを指定します。 • 選択肢：「CoS」「DSCP」

「Apply」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 > 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。

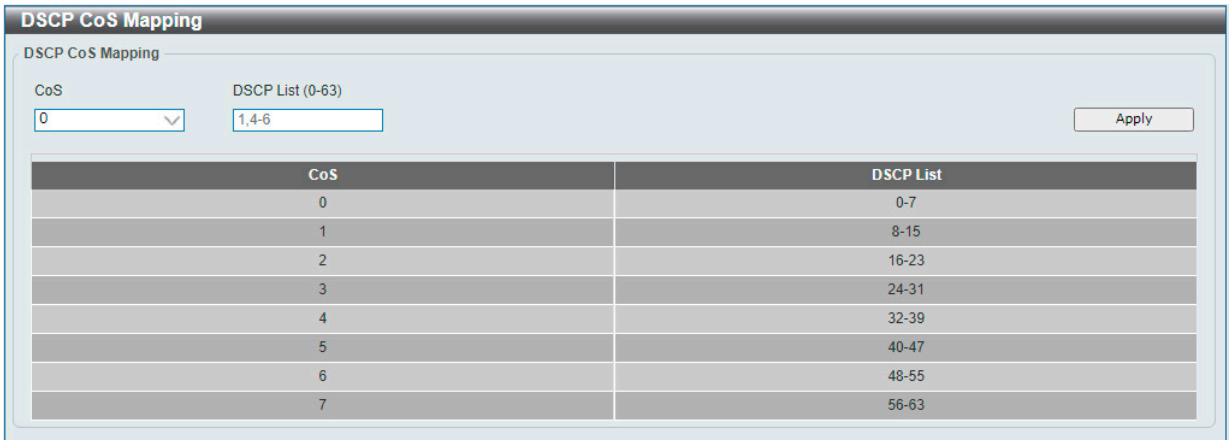


図 10-8　DSCP CoS Mapping 画面

画面に表示される項目：

項目	説明
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 値をマッピングする DSCP リストの値を入力します。 • 設定可能範囲：0 - 63

「Apply」をクリックして、設定内容を適用します。

第 11 章　ACL（ACL 機能の設定）

ACL メニューを使用し、本スイッチにアクセスプロファイルおよびルールの設定を行うことができます。

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

サブメニュー	説明
ACL Configuration Wizard（ACL 設定ウィザード）	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します。
ACL Access List（ACL アクセスリスト）	ACL アクセスリストの設定を行います。
ACL Interface Access Group（ACL インタフェースアクセスグループ）	ACL インタフェースアクセスグループの設定を行います。

注意　GVRP、STP 制御パケットは、ACL の拒否ルールよりも優先されます。

ACL Configuration Wizard（ACL 設定ウィザード）

ウィザードを使用してアクセスプロファイルとルールを作成・更新します。

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 ルールの編集、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。

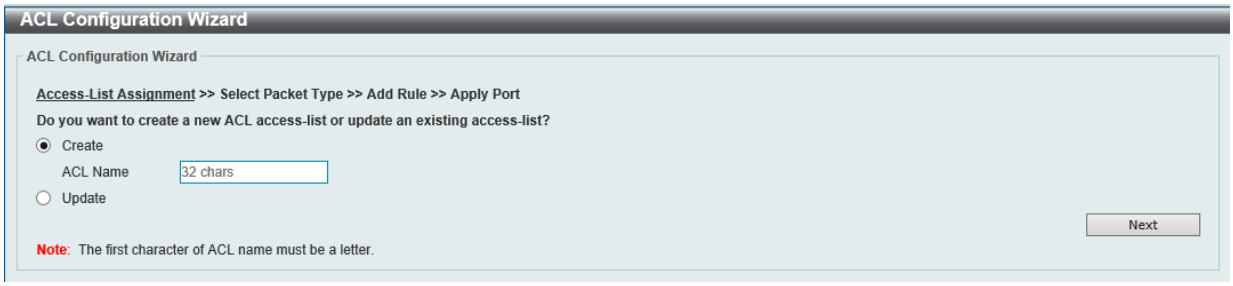


図 11-9　ACL Configuration Wizard 画面（Create）

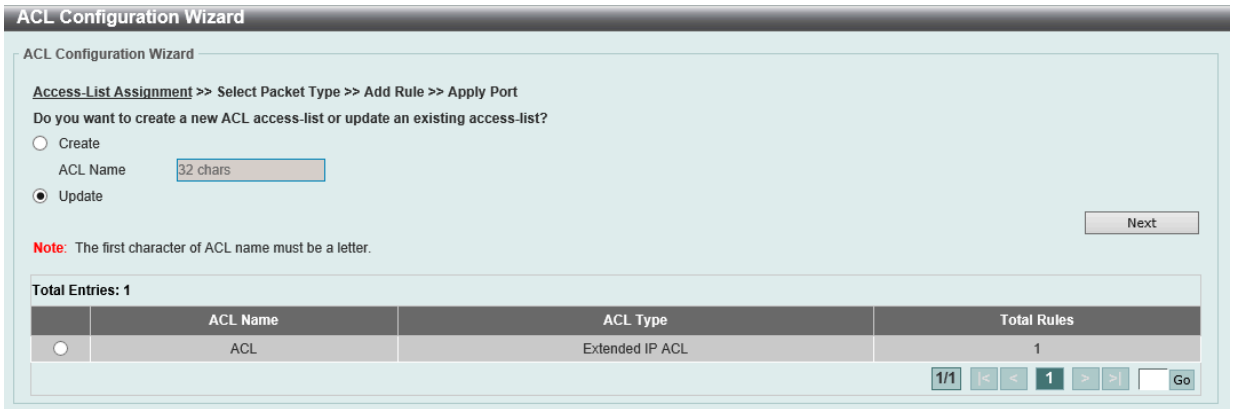


図 11-10　ACL Configuration Wizard 画面（Update）

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」をクリックし、パケットタイプの選択を行います。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

パケットタイプ選択（ACL 設定ウィザード）

「ACL Configuration Wizard」にて設定する ACL エントリを指定した後、パケットタイプを指定します。

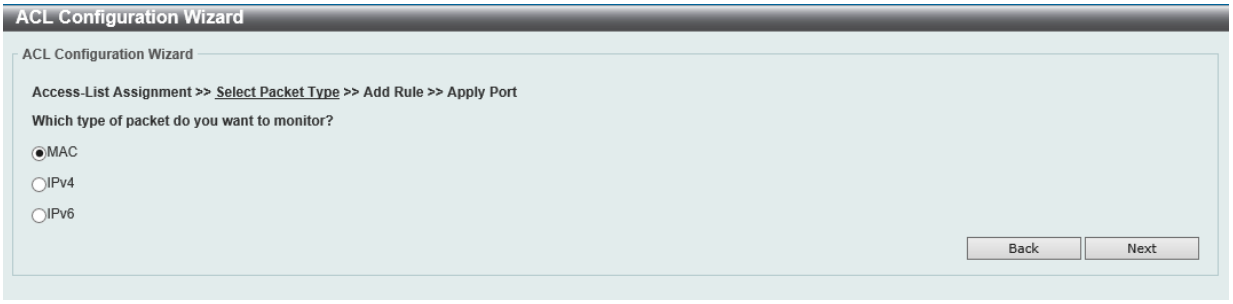


図 11-11　ACL Configuration Wizard（Select Packet Type）画面

画面に表示される項目：

項目	説明
MAC	MAC ACL を選択します。以降の設定は「MAC ACL の設定」を参照してください。
IPv4	IPv4 ACL を選択します。以降の設定は「IPv4 ACL Rule の設定」を参照してください。
IPv6	IPv6 ACL を選択します。以降の設定は「IPv6 ACL Rule の設定」を参照してください。

「Next」をクリックします。
選択したパケットの種類により、次に表示される画面が異なります。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 の設定

MAC ACL Rule を設定します。「MAC」を選択 →「Next」をクリックし、以下の画面で設定を行います。

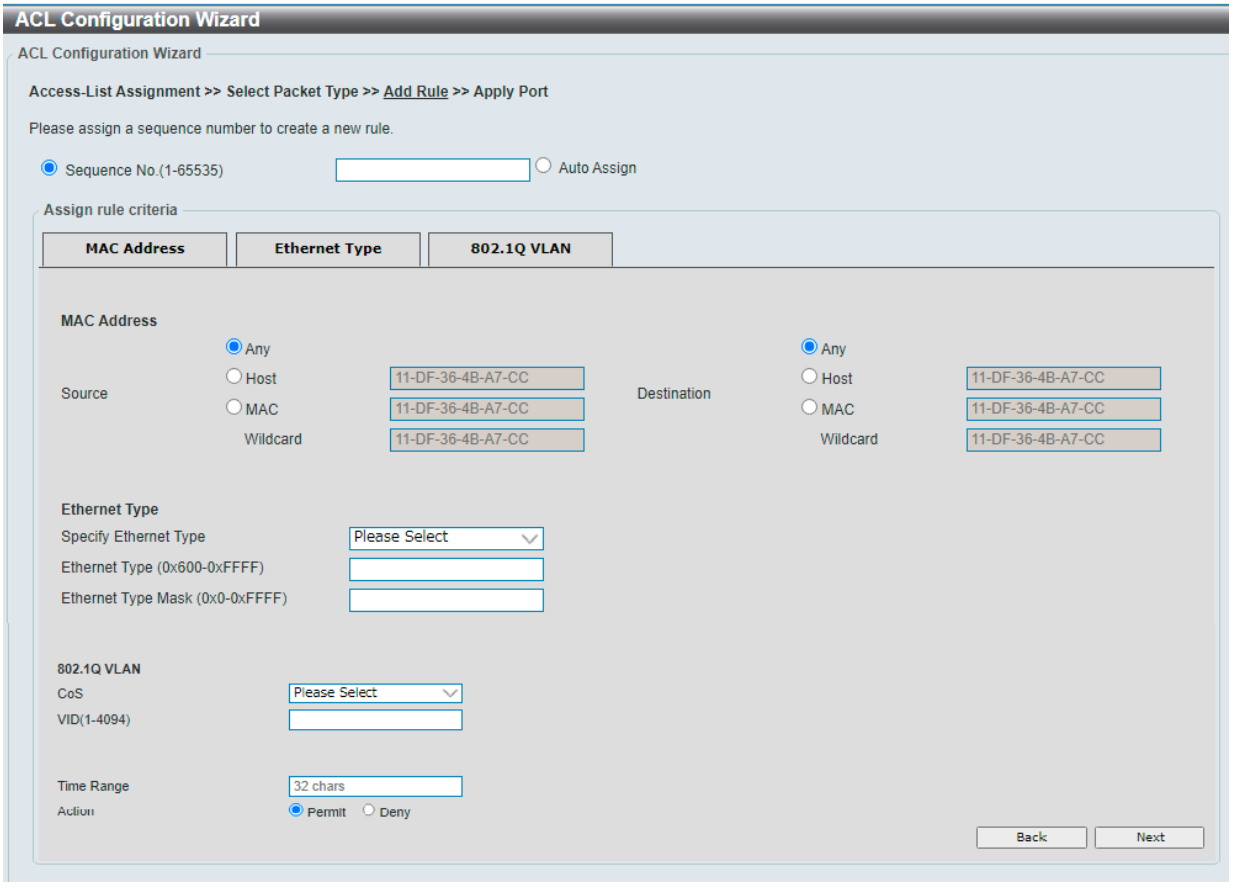


図 11-12　ACL Configuration Wizard 画面（Extended MAC ACL）

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」オプションが利用可能になり、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」オプションが利用可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
Ethernet Type	
Specify Ethernet Type	イーサネットタイプを選択します。 • 選択肢:「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
Ethernet Type	イーサネットタイプの 16 進数値を指定します。 「Specify Ethernet Type」ドロップダウンリストでイーサネットタイププロファイルを選択すると、適切な 16 進数値が自動的に入力されます。 • 設定可能範囲：0x0 - 0xFFFF
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。 「Specify Ethernet Type」ドロップダウンリストでイーサネットタイププロファイルを選択すると、適切な 16 進数値が自動的に入力されます。 • 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
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
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」

「Next」をクリックします。
「Back」をクリックすると前のページに戻ります。

注意　MAC ACL で「Ethernet Type」に「86DD (IPv6 プロトコル)」を指定した場合、レイヤ 3 IP パケットがブロックされます。

IPv4 ACL Rule の設定

IPv4 ACL Rule を設定します。「IPv4」を選択 →「Next」をクリックし、以下の画面で設定を行います。

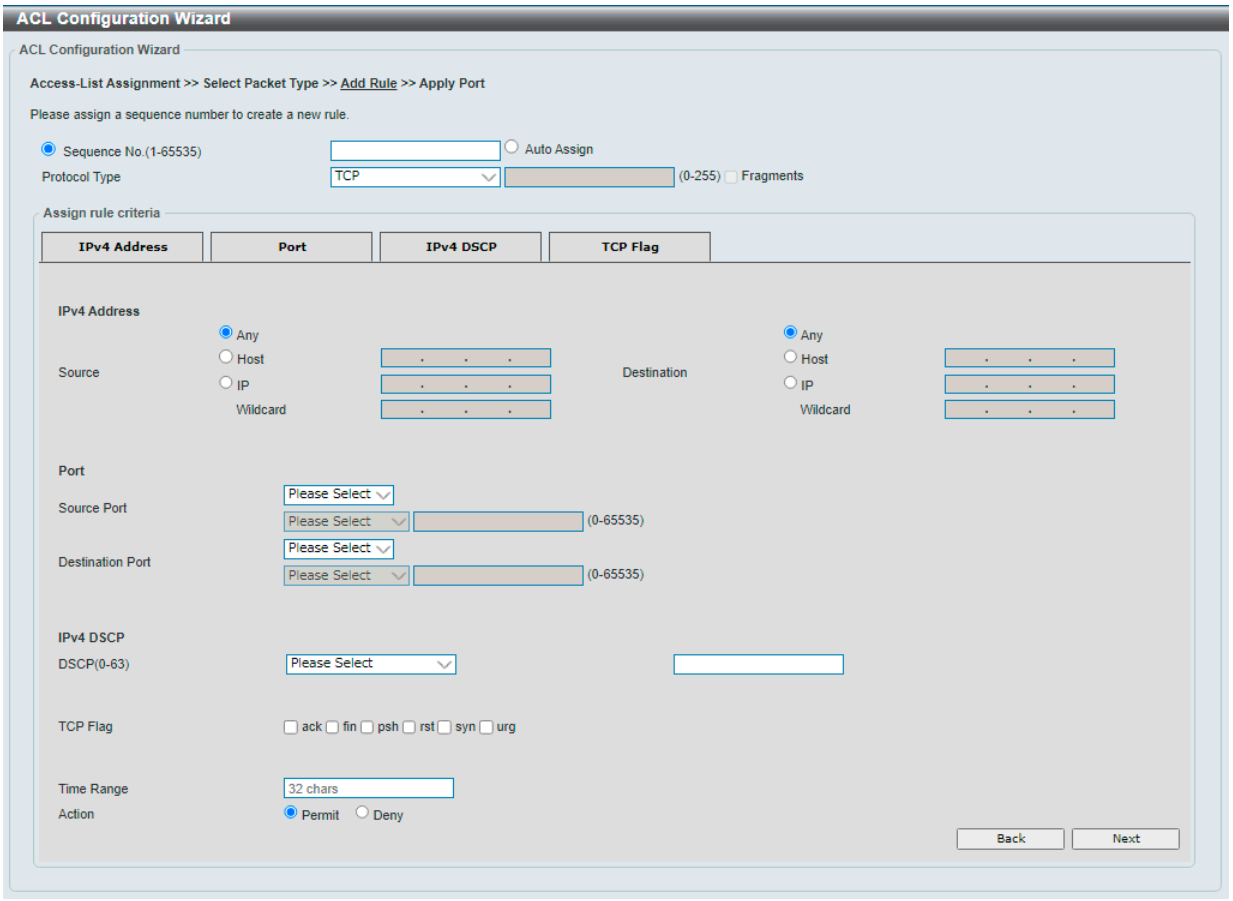


図 11-13　ACL Configuration Wizard 画面（Extended IPv4 ACL）

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1 - 65535
Protocol Type（プロトコルタイプ）	
Protocol Type	プロトコルの種類を以下から選択します。 • 「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。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

項目	説明
Assign rule criteria（ルール条件の割り当て）	
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」オプションが利用可能になります。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」オプションが利用可能になります。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
Port	
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 ・「=」- 指定のポート番号が使用されます。 ・「>」- 指定ポートよりも大きいポートが使用されます。 ・「<」- 指定ポートより小さいポートが使用されます。 ・「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 ・「=」- 指定のポート番号が使用されます。 ・「>」- 指定ポートよりも大きいポートが使用されます。 ・「<」- 指定ポートより小さいポートが使用されます。 ・「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 ・ 設定可能範囲：0 - 255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 ・ 設定可能範囲：0 - 255
IPv4 DSCP	
DSCP	使用する DSCP 値を選択します。 ・「default (0)」「10 (af11)」「12 (af12)」「14 (af13)」「18 (af21)」「20 (af22)」「22 (af23)」「26 (af31)」「28 (af32)」「30 (af33)」「34 (af41)」「36 (af42)」「38 (af43)」「8 (cs1)」「16 (cs2)」「24 (cs3)」「32 (cs4)」「40 (cs5)」「48 (cs6)」「56 (cs7)」「46 (ef)」 - 「Value」- DSCP 値を入力します。（0-63）
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 ・ 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 ・ 選択肢：「Permit（許可）」「Deny（拒否）」

「Next」をクリックします。
「Back」をクリックすると前のページに戻ります。

IPv6 ACL Rule の設定

IPv6 ACL Rule を設定します。「IPv6」を選択 →「Next」をクリックし、以下の画面で設定を行います。

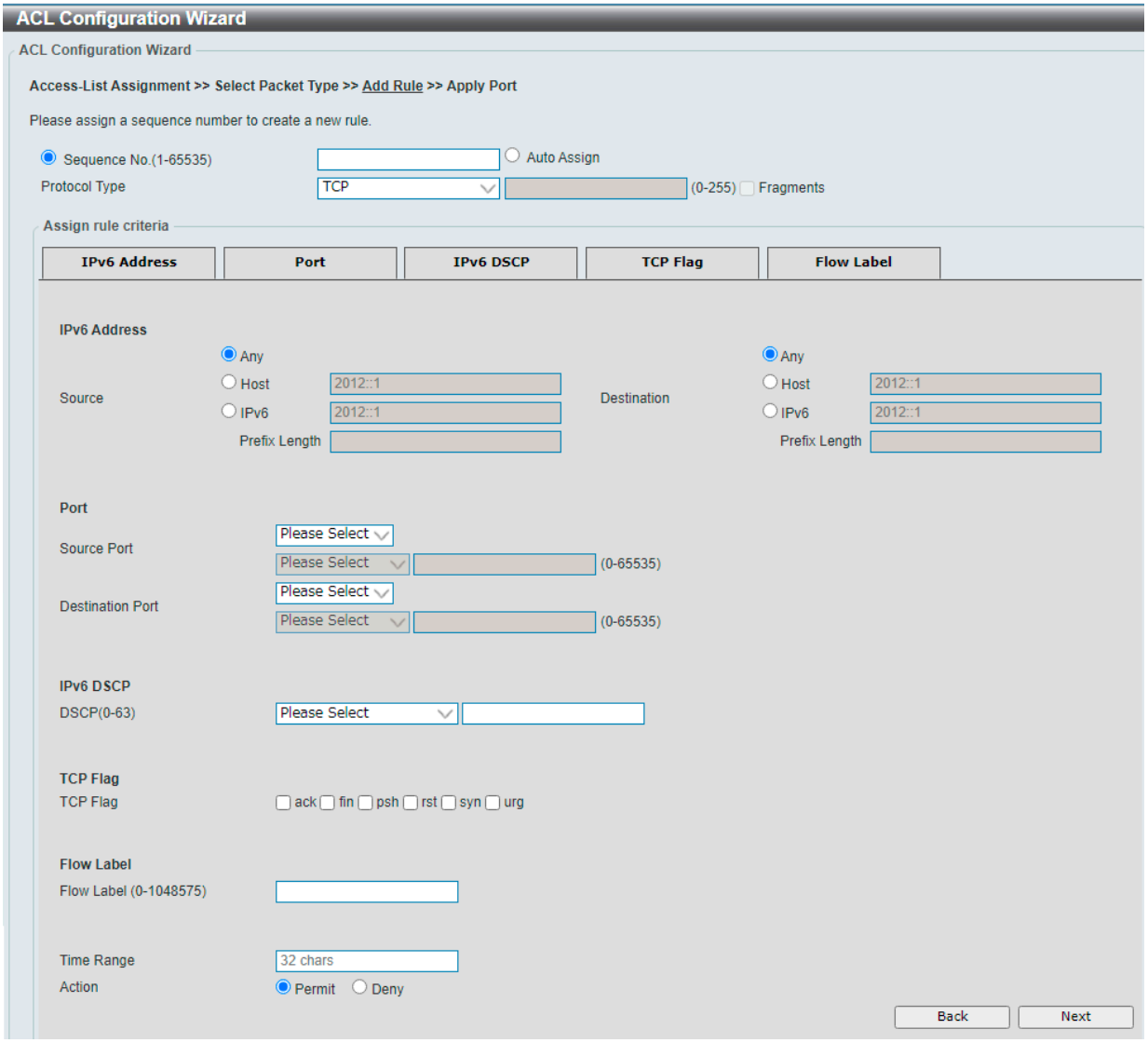


図 11-14　ACL Configuration Wizard 画面（Extended IPv6 ACL）

画面に表示される項目：

項目	説明
Assign sequence number（シーケンス番号の指定）	
Sequence No.	シーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1 - 65535
Protocol Type（プロトコルタイプ）	
Protocol Type	プロトコルの種類を以下から選択します。 • 「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。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

項目	説明
Assign rule criteria（ルール条件の割り当て）	
IPv6 Address	
Source	送信元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」が指定可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。

項目	説明
Destination	宛先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」が指定可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
Port	
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 ・「=」- 指定のポート番号が使用されます。 ・「>」- 指定ポートよりも大きいポートが使用されます。 ・「<」- 指定ポートより小さいポートが使用されます。 ・「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 ・「=」- 指定のポート番号が使用されます。 ・「>」- 指定ポートよりも大きいポートが使用されます。 ・「<」- 指定ポートより小さいポートが使用されます。 ・「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 ・ 設定可能範囲：0 - 255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 ・ 設定可能範囲：0 - 255
IPv6 DSCP	
DSCP	使用する DSCP 値を選択します。 ・「default (0)」「10 (af11)」「12 (af12)」「14 (af13)」「18 (af21)」「20 (af22)」「22 (af23)」「26 (af31)」「28 (af32)」「30 (af33)」「34 (af41)」「36 (af42)」「38 (af43)」「8 (cs1)」「16 (cs2)」「24 (cs3)」「32 (cs4)」「40 (cs5)」「48 (cs6)」「56 (cs7)」「46 (ef)」 - 「Value」- DSCP 値を入力します。（0 - 63）
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 ・ 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Flow Label	
Flow Label	フローラベルの値を入力します。 ・ 設定可能範囲：0 - 1048575
アクション設定	
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 ・ 選択肢：「Permit（許可）」「Deny（拒否）」

「Next」をクリックします。
「Back」をクリックすると前のページに戻ります。

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。

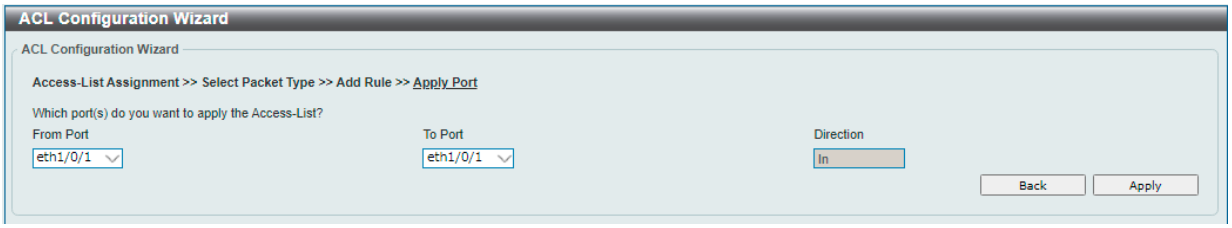


図 11-15　ACL Configuration Wizard 画面（Apply Port）

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Direction	方向を指定します。 • 選択肢：「In」

「Apply」をクリックして、設定内容を適用します。

ACL Access List（ACL アクセスリスト）

ACL アクセスリストの設定、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 11-16　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」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」をクリックし、新しい ACL プロファイルを作成します。
「Edit」をクリックして、指定エントリの編集を行います。
「Delete」をクリックすると指定のエントリを削除します。

ACL ルールの作成・カウンタの削除

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」をクリックします。
「Clear All Counter」をクリックし、表示されたすべてのカウンタ情報を消去します。
「Clear Counter」をクリックし、表示された指定ルールのカウンタ情報を消去します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

注意　別の ACL で作成されたルールと同じ内容のルールを異なる ACL に対して作成できません。

注意　CLI で ACL を作成する際、ACL 名の文字数上限に達した場合のエラーメッセージは「Invalid Command」と表示されます。

ACL の編集

既存の ACL を編集する場合は、アクセスリストの「Edit」をクリックし、以下の画面で編集を行います。

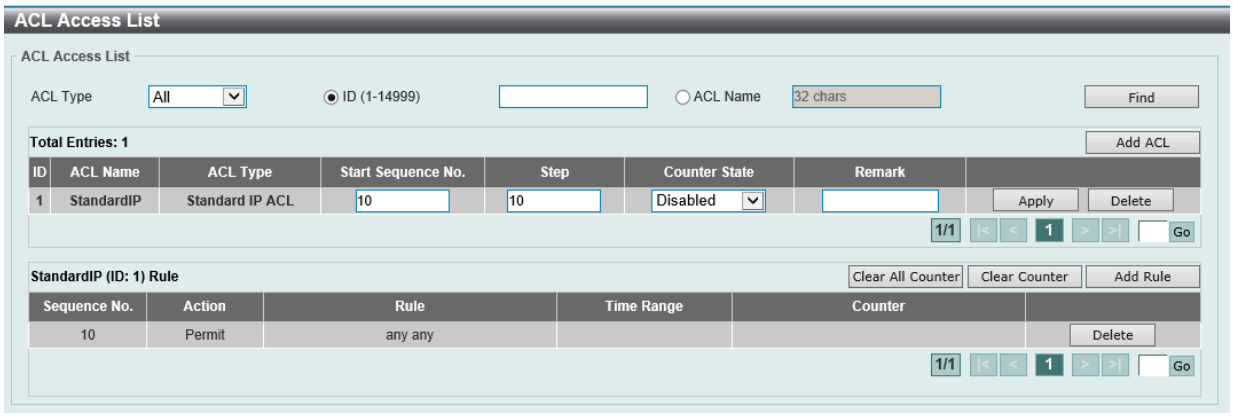


図 11-17　ACL Access List（Edit）画面

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」をクリックし、設定を適用します。

ACL プロファイルの作成

「Add ACL」をクリックすると、以下の画面が表示されます。

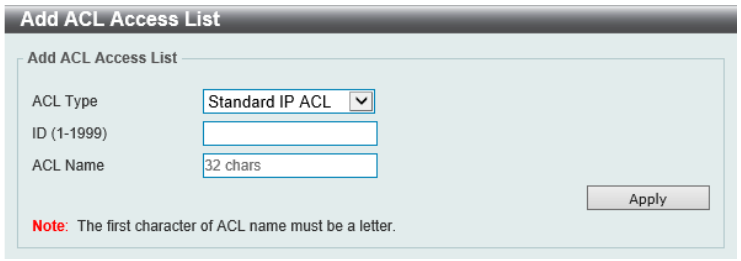


図 11-18　Add ACL Access List 画面

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:「Extended MAC ACL」「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended Expert ACL」
ID	ACL ID を入力します。 • Extended MAC ACL の場合：6000 - 7999 • Standard IP ACL の場合：1 - 1999 • Extended IP ACL の場合：2000 - 3999 • Standard IPv6 ACL の場合：11000 - 12999 • Extended IPv6 ACL の場合：13000 - 14999 • Extended Expert ACL の場合：8000 - 9999
ACL Name	ACL 名を入力します。（32 文字以内）

「Apply」をクリックして、設定内容を適用します。

Extended MAC ACL（拡張 MAC ACL）の設定

ACL プロファイルで「Extended MAC ACL」を選択した場合の設定について説明します。

ACL > ACL Access List 画面で、Extended MAC ACL のエントリを選択し、「Add Rule」をクリックします。

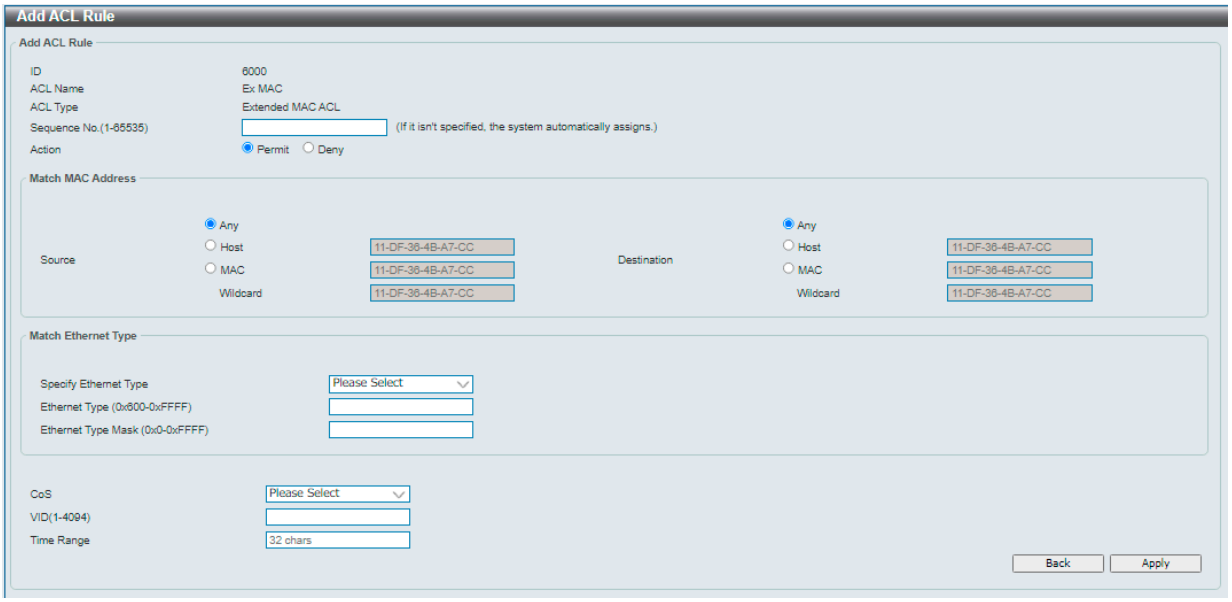


図 11-19　Add ACL Rule (Extended MAC ACL）画面

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1 - 65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Match MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが利用可能になり、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」オプションが利用可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
Match 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
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
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」をクリックして、設定を適用します。

Standard IP ACL（通常 IP ACL）の設定

ACL プロファイルで「Standard IP ACL」を選択した場合の設定について説明します。

ACL > ACL Access List 画面で、Standard IP ACL エントリの「Add Rule」をクリックします。

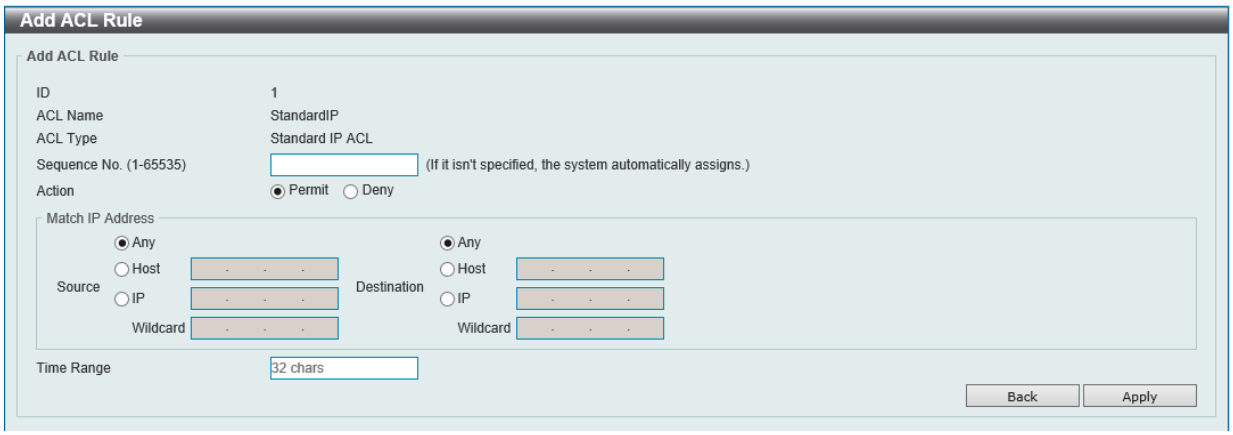


図 11-20　Add ACL Rule (Standard IP ACL）画面

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）」
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」オプションが利用可能になります。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」オプションが利用可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」をクリックして、設定を適用します。

Extended IP ACL（拡張 IP ACL）の設定

ACL プロファイルで「Extended IP ACL」を選択した場合の設定について説明します。

ACL > ACL Access List 画面で、Extended IP ACL のエントリの「Add Rule」をクリックします。

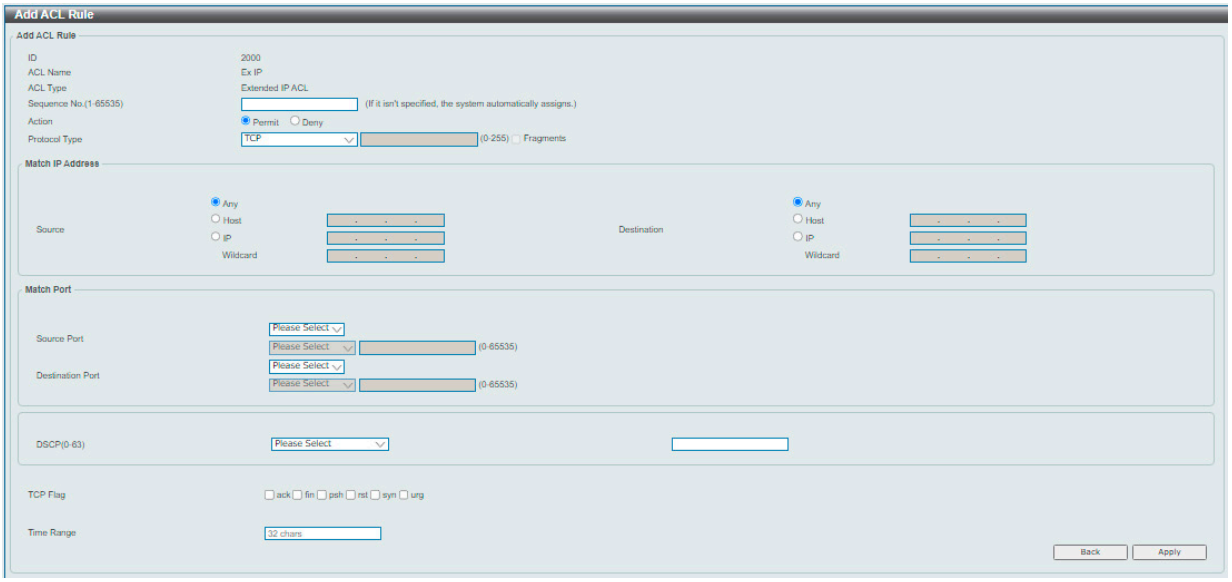


図 11-21　Add ACL Rule (Extended IP ACL）画面

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1 - 65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Protocol Type	プロトコルの種類を以下から選択します。 • 「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。 - 「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。

画面に表示される項目：

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」オプションが利用可能になります。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」オプションが利用可能になります。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 Port	
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。

項目	説明
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
Match ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0 - 255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0 - 255
IPv4 DSCP	
DSCP	使用する DSCP 値を選択します。 • 「default (0)」「10 (af11)」「12 (af12)」「14 (af13)」「18 (af21)」「20 (af22)」「22 (af23)」「26 (af31)」「28 (af32)」「30 (af33)」「34 (af41)」「36 (af42)」「38 (af43)」「8 (cs1)」「16 (cs2)」「24 (cs3)」「32 (cs4)」「40 (cs5)」「48 (cs6)」「56 (cs7)」「46 (ef)」 - 「Value」- DSCP 値を入力します。（0 - 63）
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Time Range	
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」をクリックして、設定を適用します。

Standard IPv6 ACL（標準 IPv6 ACL）の設定

ACL プロファイルで「Standard IPv6 ACL」を選択した場合の設定について説明します。

ACL > ACL Access List 画面で、Standard IPv6 ACL のエントリの「Add Rule」をクリックします。

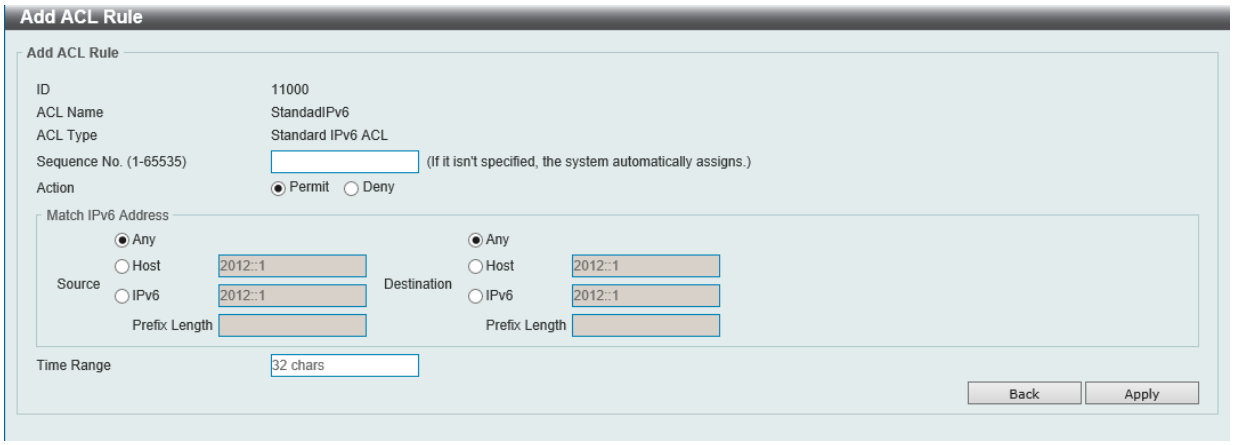


図 11-22　Add ACL Rule (Standard IPv6 ACL）画面

画面に表示される項目：

項目	説明
Sequence No.	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）」

項目	説明
Source	送信元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」が指定可能になります。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」が指定可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」をクリックして、設定内容を適用します。

Extended IPv6 ACL（拡張 IPv6 ACL）の設定

ACL プロファイルで「Extended IPv6 ACL」を選択した場合の設定について説明します。

ACL > ACL Access List 画面で、Extended IPv6 ACL のエントリの「Add Rule」をクリックします。

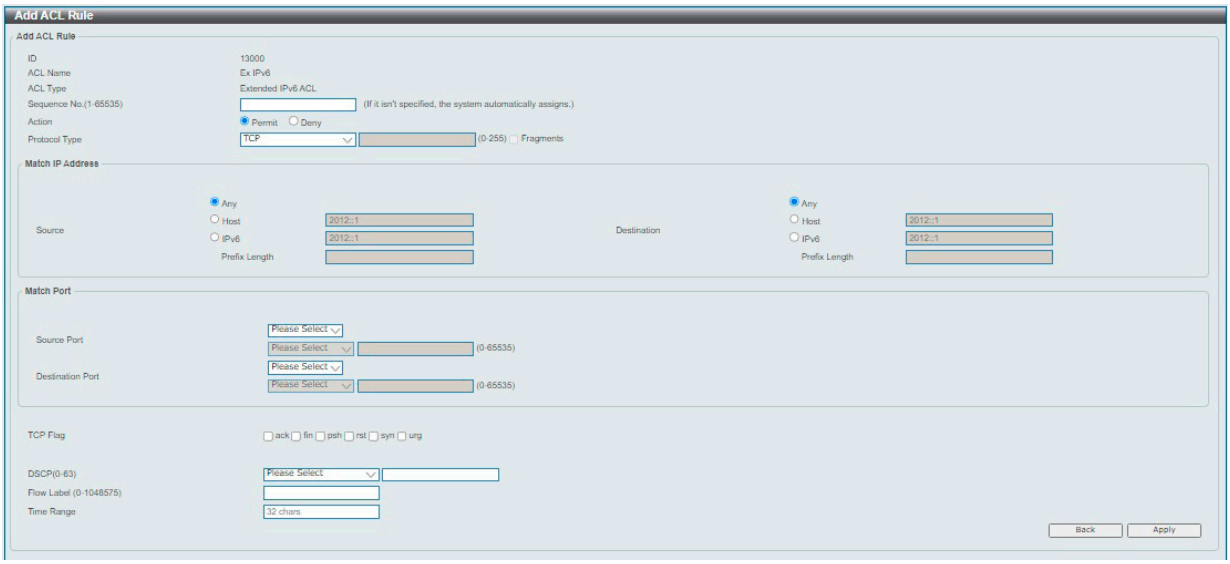


図 11-23　Add ACL Rule (Extended IPv6 ACL）画面

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1 - 65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Protocol Type	プロトコルの種類を以下から選択します。 • 「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。 - 「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。

画面に表示される項目：

項目	説明
Match IPv6 Address	
Source	送信元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」が指定可能になります。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」が指定可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。

項目	説明
Port	
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 ・「=」- 指定のポート番号が使用されます。 ・「>」- 指定ポートよりも大きいポートが使用されます。 ・「<」- 指定ポートより小さいポートが使用されます。 ・「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 ・「=」- 指定のポート番号が使用されます。 ・「>」- 指定ポートよりも大きいポートが使用されます。 ・「<」- 指定ポートより小さいポートが使用されます。 ・「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 ・ 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Match ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 ・ 設定可能範囲：0 - 255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 ・ 設定可能範囲：0 - 255
IPv6 DSCP	
DSCP	使用する DSCP 値を選択します。 ・「default (0)」「10 (af11)」「12 (af12)」「14 (af13)」「18 (af21)」「20 (af22)」「22 (af23)」「26 (af31)」「28 (af32)」「30 (af33)」「34 (af41)」「36 (af42)」「38 (af43)」「8 (cs1)」「16 (cs2)」「24 (cs3)」「32 (cs4)」「40 (cs5)」「48 (cs6)」「56 (cs7)」「46 (ef)」 - 「Value」- DSCP 値を入力します。（0 - 63）
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
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」をクリックして、設定を適用します。

Extended Expert ACL（拡張詳細 ACL）の設定

ACL プロファイルで「Extended Expert ACL」を選択した場合の設定について説明します。

ACL > ACL Access List 画面で、Extended Exprt ACL のエントリの「Add Rule」をクリックします。

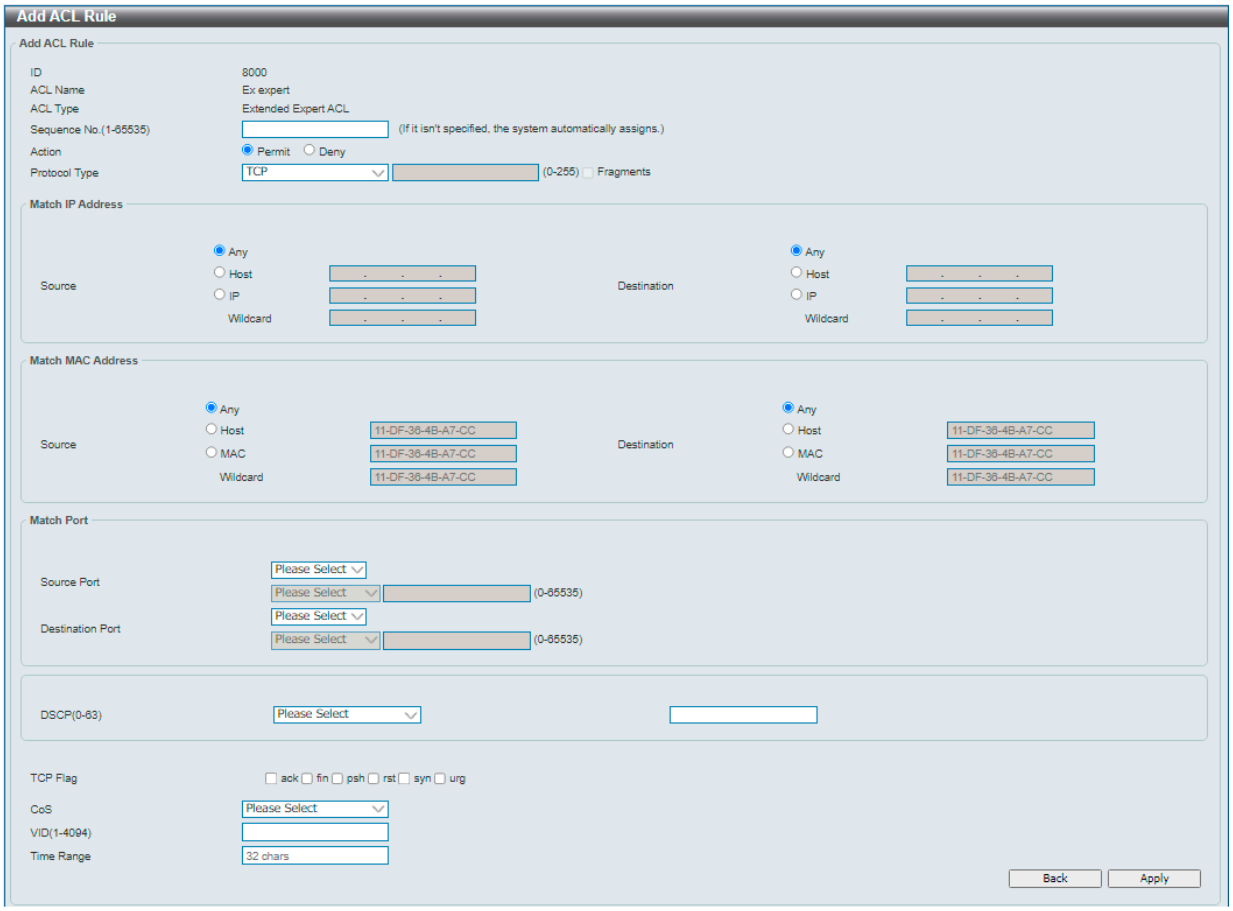


図 11-24　Add ACL Rule (Extended Exprt ACL）画面

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1 - 65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit（許可）」「Deny（拒否）」
Protocol Type	プロトコルの種類を以下から選択します。 • 「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。 - 「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。

画面に表示される項目：

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」オプションが利用可能になります。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」オプションが利用可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。

項目	説明
Match MAC Address	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが利用可能になり、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」オプションが利用可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
Match Port	
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。
Match ICMP	
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0 - 255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0 - 255
IPv4 DSCP	
DSCP	使用する DSCP 値を選択します。 • 「default (0)」「10 (af11)」「12 (af12)」「14 (af13)」「18 (af21)」「20 (af22)」「22 (af23)」「26 (af31)」「28 (af32)」「30 (af33)」「34 (af41)」「36 (af42)」「38 (af43)」「8 (cs1)」「16 (cs2)」「24 (cs3)」「32 (cs4)」「40 (cs5)」「48 (cs6)」「56 (cs7)」「46 (ef)」 - 「Value」- DSCP 値を入力します。（0 - 63）
TCP Flag	
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
802.1Q VLAN	
CoS	CoS の値を入力します。 • 設定可能範囲：0 - 7
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
Time Range	
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」をクリックして、設定を適用します。

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。

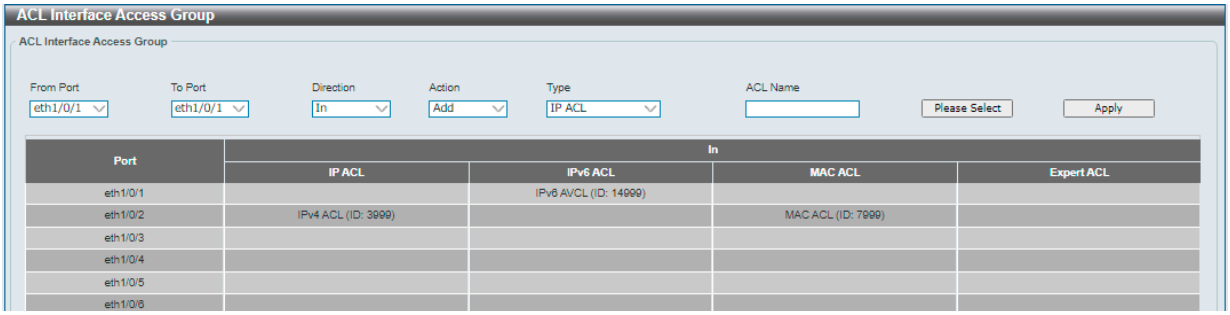


図 11-25　ACL Interface Access Group 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Direction	方向を指定します。 • 選択肢：「In」
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」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」をクリックして、設定を適用します。

「Please Select」をクリック すると次の画面が表示されます。作成した ACL プロファイルを選択します。

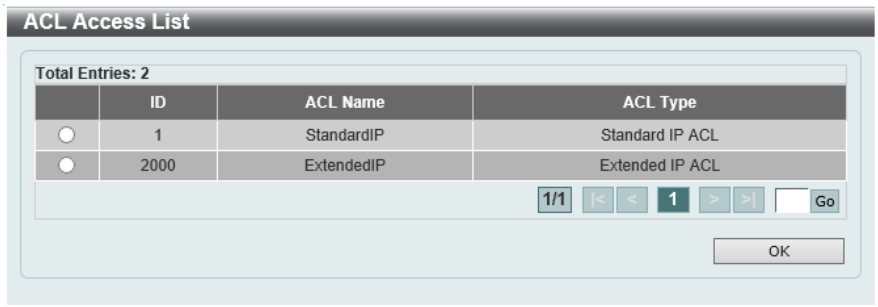


図 11-26　ACL Access List 面

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

第 12 章　Security（セキュリティ機能の設定）

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

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

サブメニュー	説明
Port Security（ポートセキュリティ）	ポートセキュリティの設定を行います。
802.1X（802.1X 認証設定）	802.1X 認証設定を行います。
AAA（AAA 設定）	AAA の設定を行います。
RADIUS（RADIUS 設定）	RADIUS サーバの設定を行います。
TACACS（TACACS 設定）	TACACS サーバの設定を行います。
IMPB（IP-MAC-Port Binding / IP-MAC ポートバインディング）	IP-MAC ポートバインディングの設定を行います。
Network Access Authentication（ネットワークアクセス認証）	ネットワークアクセス認証設定を行います。
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設定を行います。
Trusted Host（トラストホスト）	トラストホスト設定を行います。
Traffic Segmentation Settings（トラフィックセグメンテーション設定）	トラフィックセグメンテーション設定を行います。
Storm Control Settings（ストームコントロール設定）	ストームコントロールの設定を行います。
DoS Attack Prevention Settings（DoS 攻撃防止設定）	DoS 攻撃防止設定を行います。
SSH（Secure Shell の設定）	SSH（Secure Shell）の設定を行います。
SSL（Secure Socket Layer）	SSL（Secure Socket Layer）の設定を行います。

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、送信元 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。

注意　ポートセキュリティと IMPB 機能は同時に有効化しないでください。

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ル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。

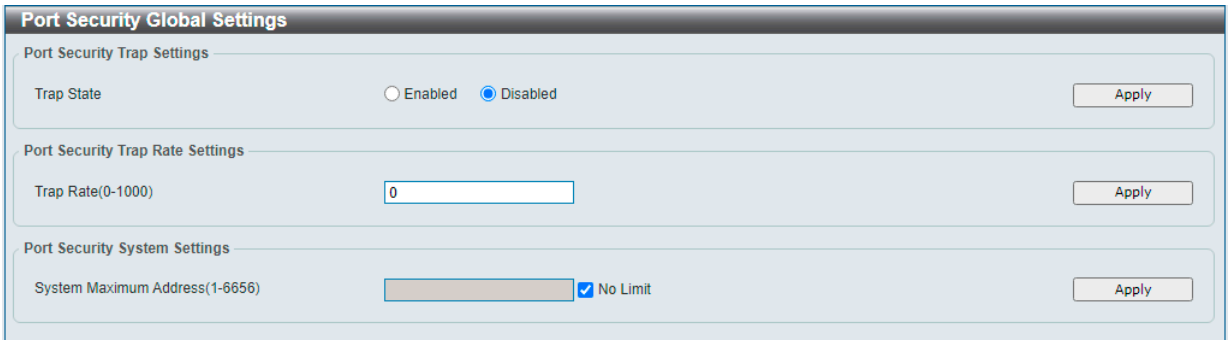


図 12-1　Port Security Global Settings 画面

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。 • 設定可能範囲：0 - 1000 • 初期値：0

項目	説明
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。 「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：0 - 6656 • 初期値：「No Limit（制限なし / 最大値）」

「Apply」をクリックして、設定内容を適用します。

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て、以下の画面を表示します。

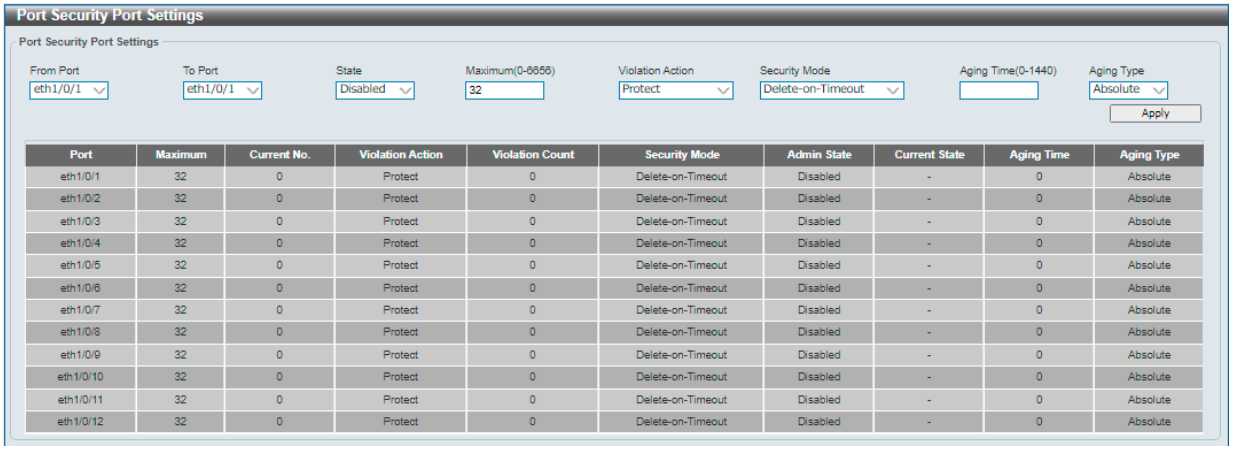


図 12-2　Port Security Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
State	指定ポートにおけるポートセキュリティ機能を有効 / 無効に設定します。
Maximum	指定ポートで許可されるセキュアな MAC アドレスの最大数を指定します。 • 設定可能範囲：0 - 6656 • 初期値：32
Violation Action	違反に対して実行するアクションを指定します。 • 「Protect」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反としてはカウントされません。 • 「Restrict」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントしてシステムログに記録します。 • 「Shutdown」- セキュリティ違反がある場合にポートをシャットダウンし、システムログに記録します。
Security Mode	セキュリティモードを選択します。 • 「Permanent」- すべての学習した MAC アドレスは手動でエントリを削除しない限り削除されません。 • 「Delete-on-Timeout」- すべての学習した MAC アドレスはタイムアウトにより自動的に削除されるか、手動により削除されます。
Aging Time	指定ポートで自動学習された安全なアドレスに使用するエージングタイムを入力します。 • 設定可能範囲：0 - 1440（分）
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」をクリックして、設定内容を適用します。

注意　「Delete-on-Timeout」モードは未サポートです。

注意　「Inactivity」モードは未サポートです。

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て、以下の画面を表示します。

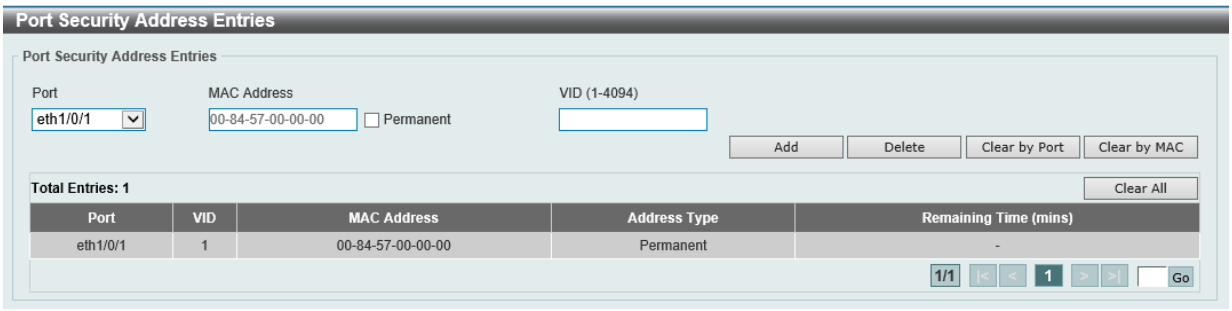


図 12-3　Port Security Address Entries 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
MAC Address	MAC アドレスを入力します。
VID	VLAN ID を指定します。 • 設定可能範囲：1 - 4094

「Add」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」をクリックして、入力した情報に基づくエントリを削除します。

「Clear by Port」をクリックして、選択したポートに基づく情報を消去します。
「Clear by MAC」をクリックして、選択した MAC アドレスに基づく情報を消去します。
「Clear All」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」をクリックして、特定のページへ移動することができます。

注意　VLAN 削除後、ポートセキュリティのアドレスエントリの番号が正しく表示されない場合があります。

802.1X（802.1X 認証設定）

802.1X（ポートベースおよびホストベースのアクセスコントロール）

IEEE 802.1X 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。

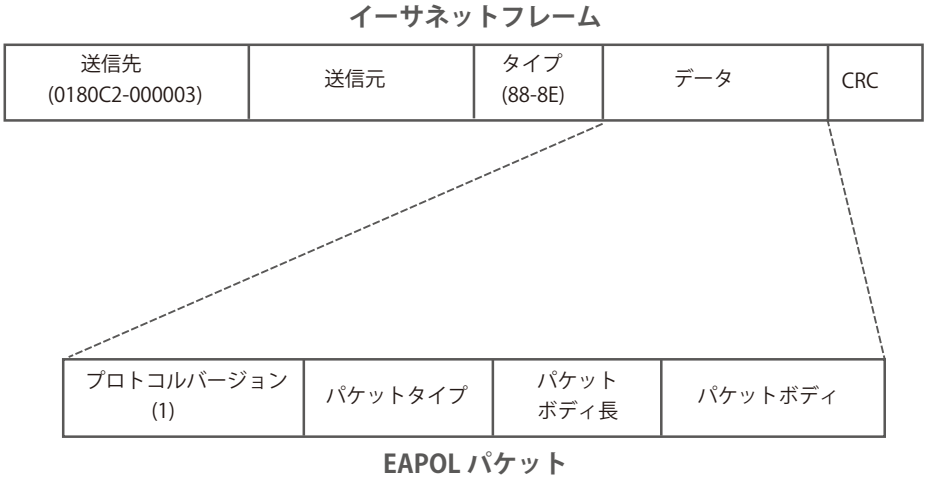


図 12-4　EAPOL パケット

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。

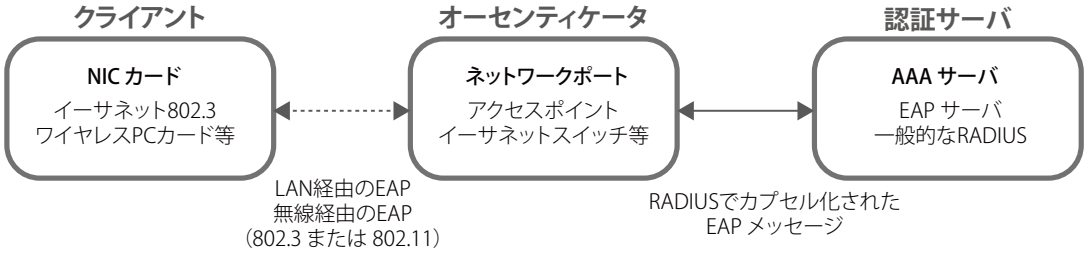


図 12-5　802.1X の 3 つの要素

以下の項では、クライアント、オーセンティケータ、および認証サーバのそれぞれの役割について詳しく説明します。

認証サーバ

認証サーバは、クライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。

認証サーバ上で 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。

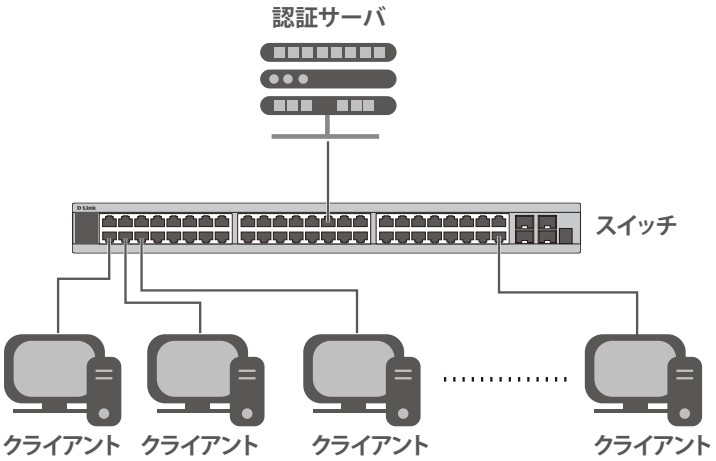


図 12-6　認証サーバ

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**）

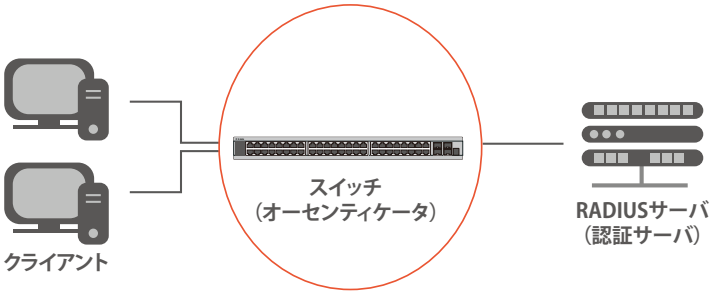


図 12-7　オーセンティケータ

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。

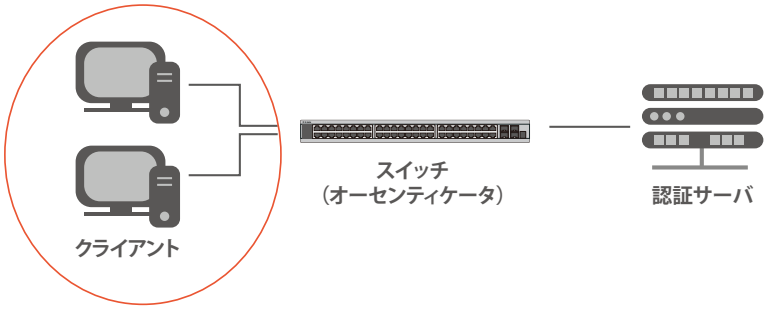


図 12-8　クライアント

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。

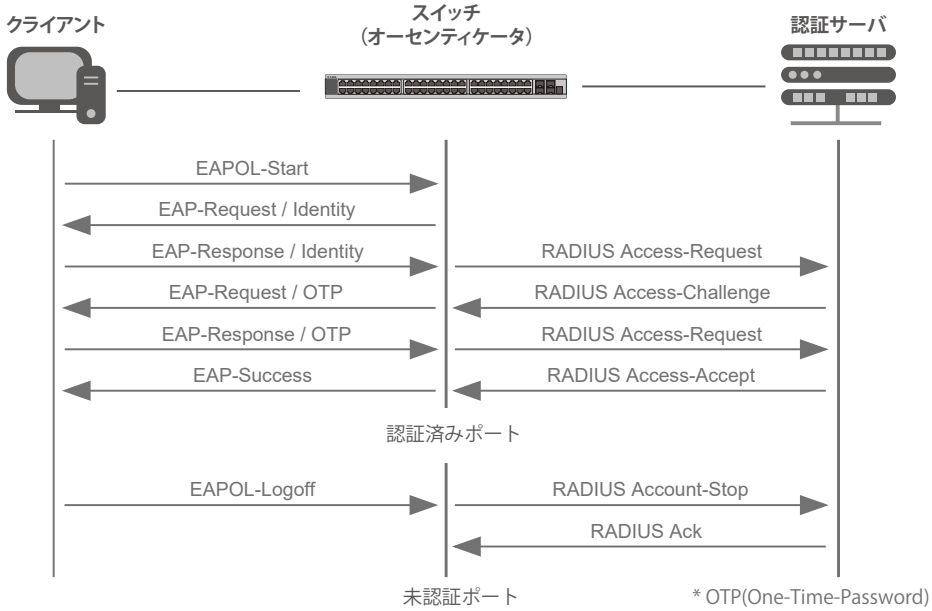


図 12-9　802.1X 認証プロセス

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 256 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。

ポートベースのネットワークアクセスコントロール

802.1X 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。

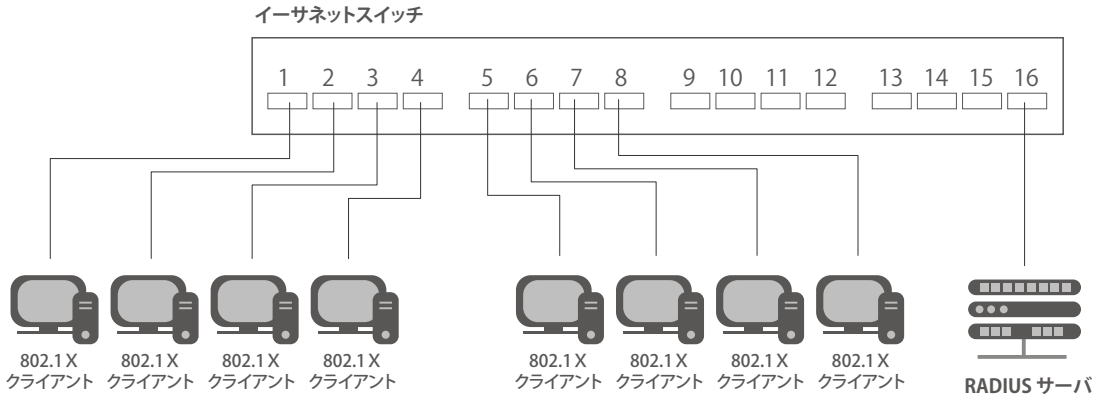


図 12-10　ポートベースアクセスコントロールのネットワーク構成例

■ 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。

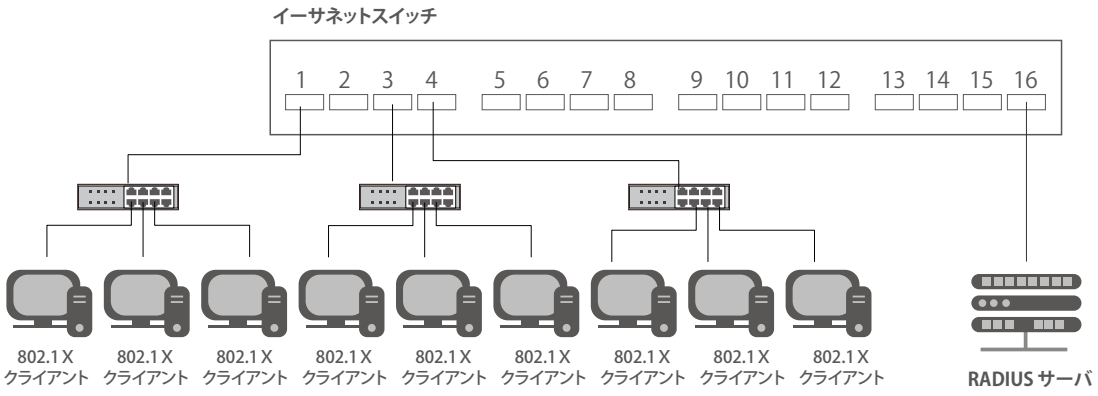


図 12-11　ホストベースアクセスコントロールのネットワーク構成例

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。

Security > 802.1X > 802.1X Global Settings の順にメニューをクリックします。

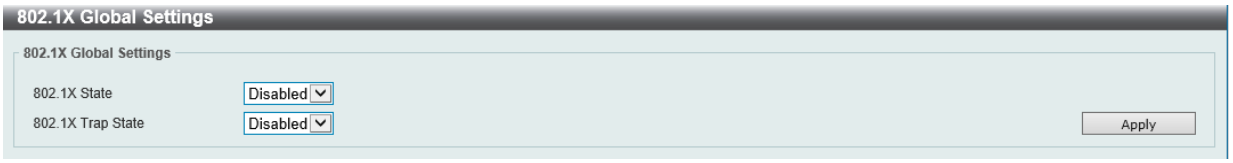


図 12-12　802.1X Global Settings 画面

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」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。

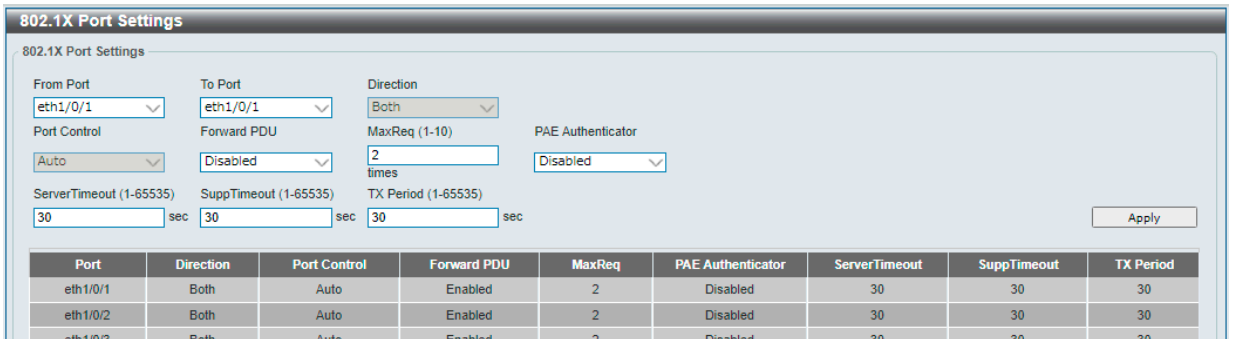


図 12-13　802.1X Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Direction	制御するトラフィックの方向を指定します。 • 「Both」- ポートが受信 / 送信する両方向のトラフィックについて処理します。
Port Control	ポートの認証状態の制御方法を指定します。 • 「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。最初の状態では、ポートは 802.1X 未認証の状態であり、EAPOL フレームのみ送受信可能です。リンクアップした際、または EAPOL-Start フレームを受信した場合に認証プロセスが開始されます。その後、スイッチはクライアントの識別情報を要求し、クライアントと認証サーバ間の認証メッセージの中継を開始します。（初期値）
Forward PDU	PDU 転送機能を有効 / 無効に設定します。
MaxReq	スイッチがクライアントに対して EAP Request フレームを再送する最大回数を指定します。指定回数に達すると、認証セッションがタイムアウトします。 • 設定可能範囲：1 - 10 • 初期値：2
PAE Authenticator	PAE Authenticator を有効 / 無効に指定します。 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	認証サーバから応答を待つ時間を指定します。指定時間が経過すると、オーセンティケータからクライアントに EAP リクエストパケットが送信されます。 • 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）から応答を待つ時間を指定します。指定時間が経過すると、EAP リクエスト ID 以外のサプリカントメッセージがタイムアウトします。 • 設定可能範囲：1 - 65535（秒） • 初期値：30（秒）

項目	説明
TX Period	オーセンティケータ PAE ステートマシンの TxPeriod を指定します。クライアントに送信される EAP Request/Identity パケットを再送信するまでの時間となります。 • 設定可能範囲：1 - 65535（秒） • 初期値：30（秒）

「Apply」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、定期的に EAP Request/Identity を送信する機能はありません。

注意　802.1X の機能において、Tag 付き EAP/EAPOL に対応しません。

Authentication Session Information（認証セッションの状態）

認証セッションの状態を表示します。

Security > 802.1X > Authentication Session Information の順にメニューをクリックして、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
From Port/To Port	セッションに関する処理を実行するポートの範囲を指定します。

「Init by Port」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」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。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

注意　"show authentication sessions" コマンド実行時、認証開始前の Multi-Host ポートにおいて、MAC アドレスが「00-00-00-00-00-00」と表示されます。

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て、以下の画面を表示します。

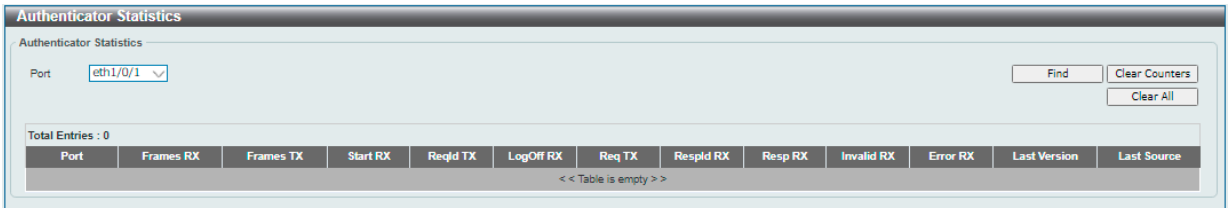


図 12-15　Authenticator Statistics 画面

画面に表示される項目：

項目	説明
Port	統計情報を表示 / クリアするポートを指定します。

「Find」をクリックして、指定した情報に基づくエントリを検出します。
「Clear Counters」をクリックして、選択に基づく情報を消去します。
「Clear All」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」をクリックして、特定のページへ移動することができます。

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て、以下の画面を表示します。

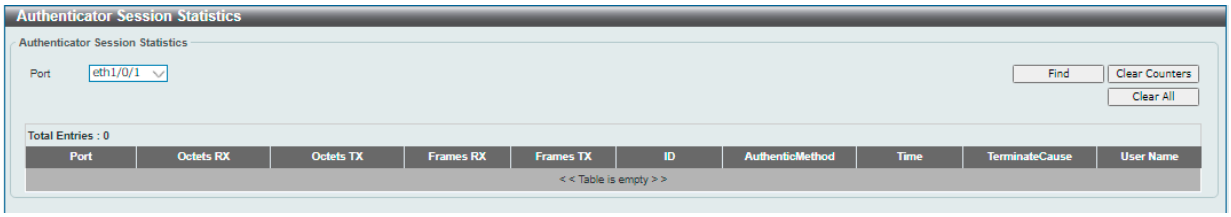


図 12-16　Authenticator Session Statistics 画面

画面に表示される項目：

項目	説明
Port	統計情報を表示 / クリアするポートを指定します。

「Find」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」をクリックして、指定ポートの情報を消去します。
「Clear All」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て、以下の画面を表示します。

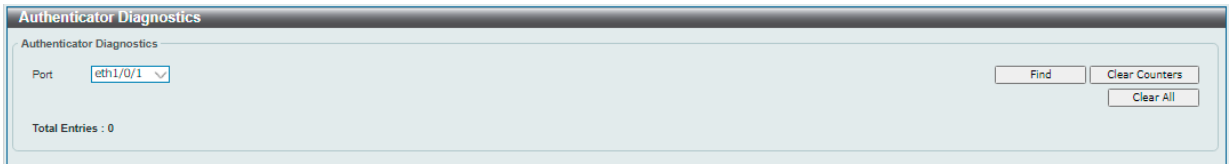


図 12-17　Authenticator Diagnostics 画面

画面に表示される項目：

項目	説明
Port	診断情報を表示 / クリアするポートを指定します。

「Find」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」をクリックして、指定ポートの情報を消去します。
「Clear All」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」をクリックして、特定のページへ移動することができます。

AAA（AAA 設定）

AAA（Authentication、Authorization、Accounting）の設定を行います。
本機能では、スイッチへのアクセスに対して管理者定義の認証ポリシーを有効にします。ユーザ認証の際、所定の Login Method List（ログイン認証方式リスト）が使用されます。

AAA Global Settings（AAA グローバル設定）

AAA（Authentication、Authorization、Accounting）をグローバルに有効 / 無効に設定します。

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

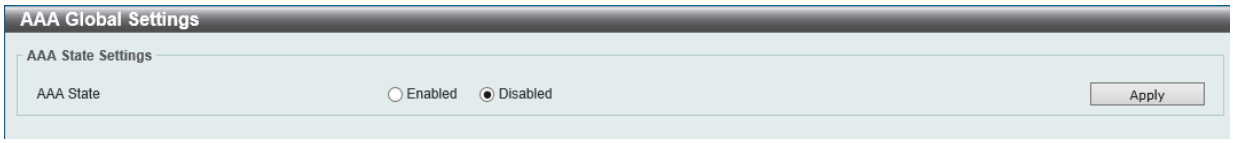


図 12-18　AAA Global Settings 画面

画面に表示される項目：

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

「Apply」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）に対し、ログイン方式リストを設定します。

Security > AAA > Application Authentication Settings の順にクリックし、以下の画面を表示します。

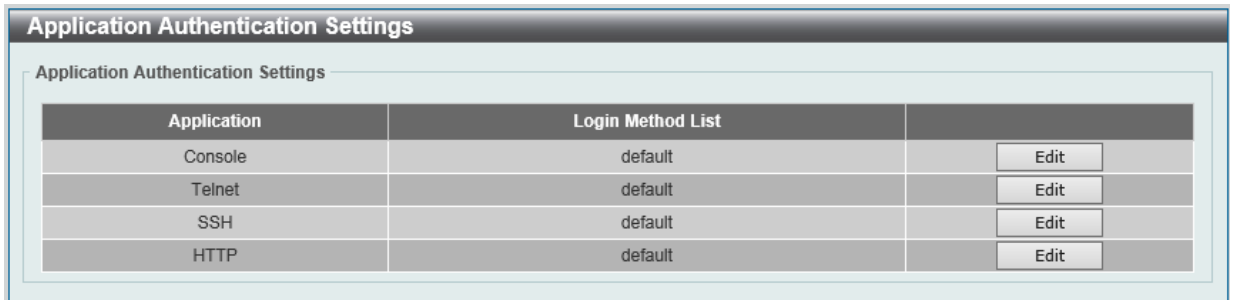


図 12-19　Application Authentication Settings 画面

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。

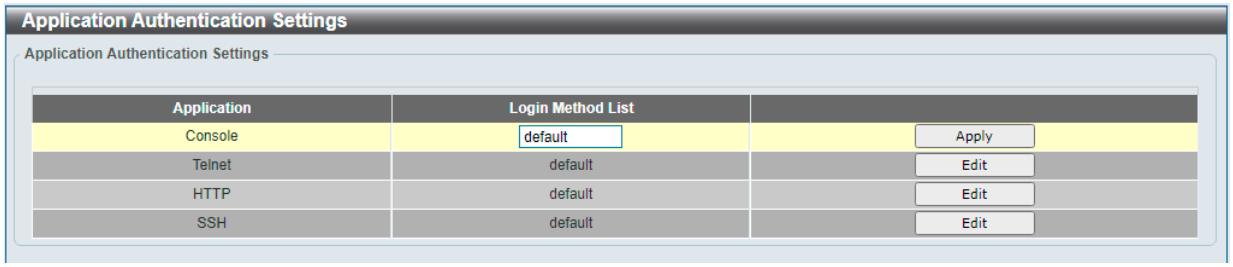


図 12-20　Application Authentication Settings (Edit) 画面

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。使用するログイン方式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。

補足　Telnet/SSH のセッション数は、それぞれ最大 4 となります。

Authentication Settings（認証設定）

ネットワークと EXEC の認証方式の設定を行います。

「AAA Authentication Network」タブ

「AAA Authentication Network」タブ内の設定を行います。

Security > AAA > Authentication 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。

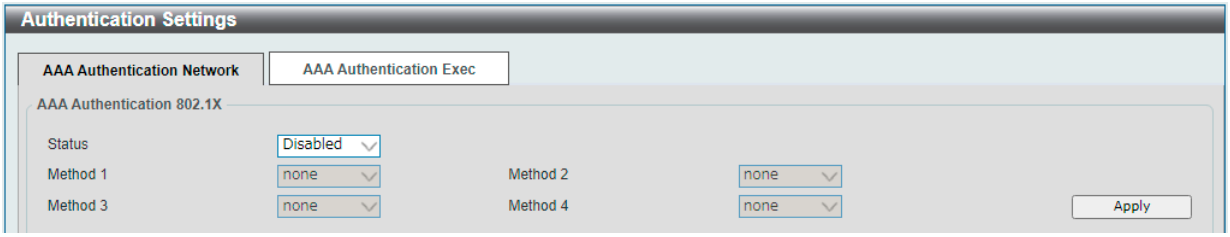


図 12-21　Authentication Settings 画面 -AAA Authentication Network タブ

画面に表示される項目：

項目	説明
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	方式 1 ～ 4 の順番で認証アルゴリズムが試行されます。1 つ以上の方式を指定します。 • 「none」- 通常、このオプションは最後の方式として指定します。1 つ前の認証方式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。 • 「tacacs+」- TACACS+ サーバ設定で定義されたサーバを使用します。

「Apply」をクリックして、設定内容を適用します。

注意　802.1X の機能において、認証にローカルデータベースを指定した場合、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。

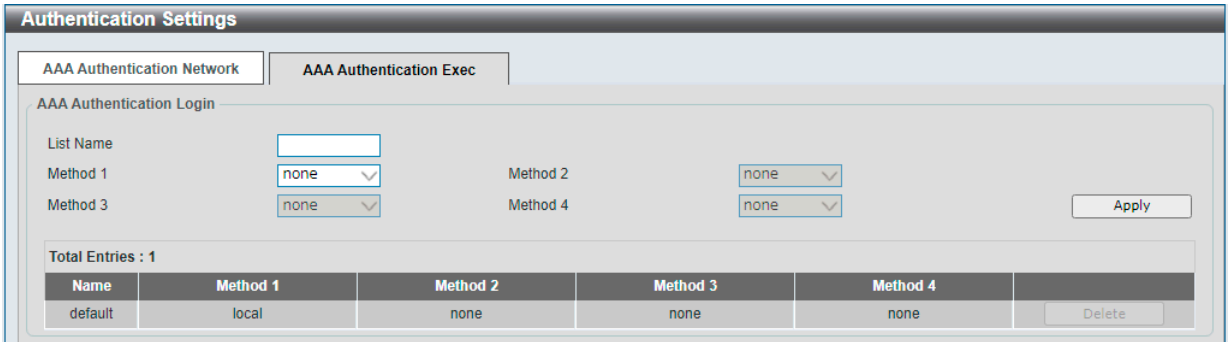


図 12-22　Authentication Settings 画面 -AAA Authentication Exec タブ

画面に表示される項目：

項目	説明
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	方式 1 ～ 4 の順番で認証アルゴリズムが試行されます。1 つ以上の方式を指定します。 • 「none」- 通常、このオプションは最後の方式として指定します。1 つ前の認証方式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。 • 「tacacs+」- TACACS+ サーバ設定で定義されたサーバを使用します。

「Apply」をクリックして、設定内容を適用します。

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て、以下の画面を表示します。

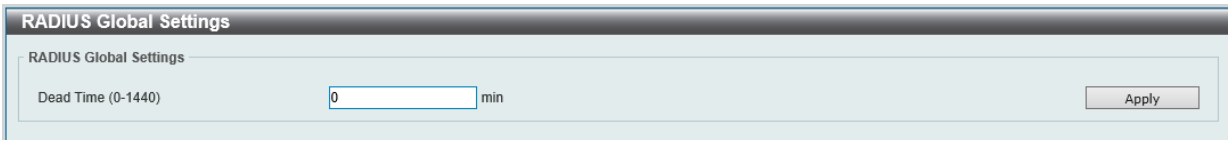


図 12-23　RADIUS Global Settings 画面

画面に表示される項目：

項目	説明
DeadTime	デッドタイムの設定を行います。 0 に設定した場合、応答しないサーバは「Dead」として認識されることはありません。この設定により、応答しないサーバホストのエントリはスキップされ、認証プロセス時間が改善されます。 システムが認証サーバへ認証を行う際、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）

「Apply」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。RADIUS サーバを利用することで、認証の一元化や強固なセキュリティを実現します。

Security > RADIUS > RADIUS Server Settings をクリックして、以下の画面を表示します。

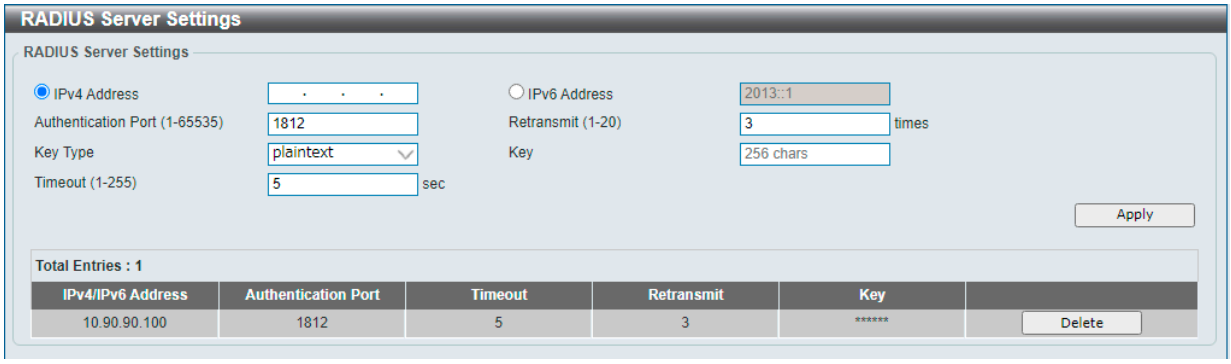


図 12-24　RADIUS Server Settings 画面

画面に表示される項目：

項目	説明
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。
Authentication Port	認証ポート番号を入力します。 • 設定可能範囲：1 - 65535 • 初期値：1812
Retransmit	再送信回数を設定します。 • 設定可能範囲：1 - 20（回） • 初期値：3（回）
Key Type	使用する鍵の種類を選択します。 • 選択肢：「plaintext（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。

項目	説明
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）

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

RADIUS Group Server Settings（RADIUS グループサーバ設定）

RADIUS グループサーバの表示、設定を行います。

Security > RADIUS > RADIUS Group Server Settings をクリックして、以下の画面を表示します。

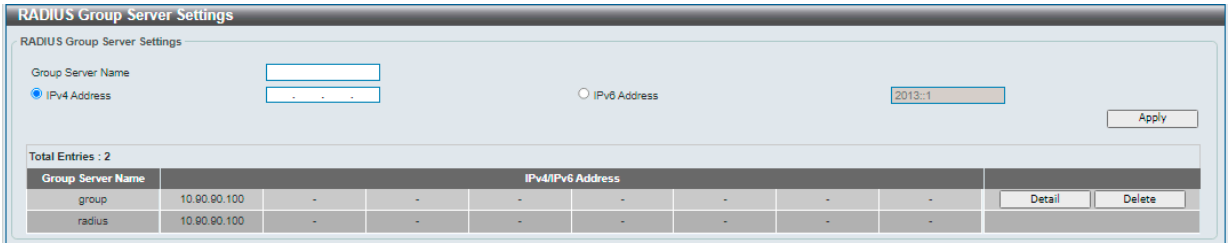


図 12-25　RADIUS Group Server Settings 画面

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。（15 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」をクリックして、エントリを追加します。
「Delete」をクリックして指定エントリを削除します。

エントリの詳細を表示

「Detail」をクリックすると RADIUS グループサーバの詳細情報について表示されます。

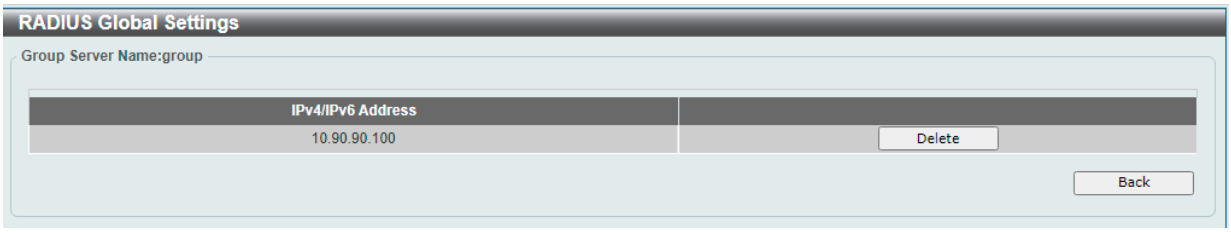


図 12-26　RADIUS Group Server Settings - Detail 画面

「Delete」をクリックして指定エントリを削除します。
「Back」をクリックして以前の画面に戻ります。

RADIUS Statistic（RADIUS 統計情報）

RADIUS 統計情報を表示します。

Security > RADIUS > RADIUS Statistic をクリックして、以下の画面を表示します。

図 12-27　RADIUS Statistic 画面

テーブル上のエントリをクリックすると、画面下部にそのサーバの統計情報が表示されます。

画面に表示される項目：

項目	説明
Group Server Name	統計情報をクリアする RADIUS グループサーバ名を選択します。

「Clear」をクリックして、選択に基づいて表示した情報を消去します。
「Clear All」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」をクリックして、特定のページへ移動することができます。

TACACS（TACACS 設定）

TACACS サーバの設定を行います。

TACACS Server Settings（TACACS サーバの設定）

TACACS サーバ設定を行います。TACACS サーバを利用することで、認証の一元化や強固なセキュリティを実現します。

Security > TACACS > TACACS Server Settings をクリックして、以下の画面を表示します。

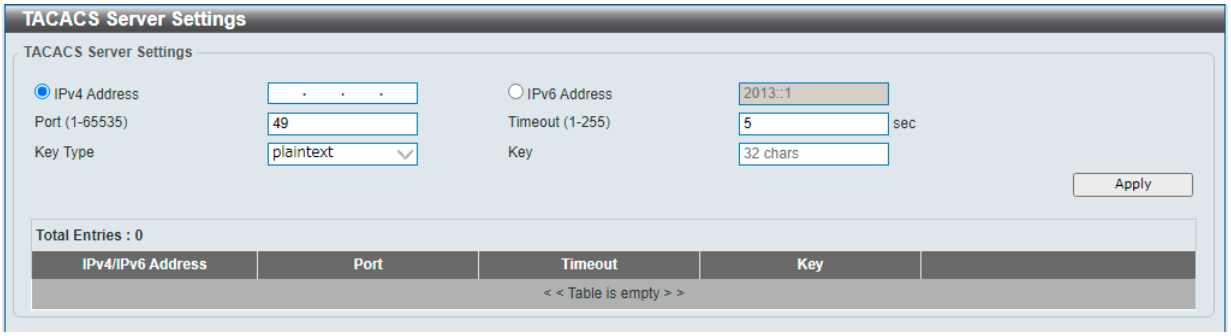


図 12-28　TACACS Server Settings 画面

画面に表示される項目：

項目	説明
IPv4 Address	TACACS サーバの IPv4 アドレスを入力します。

項目	説明
IPv6 Address	TACACS サーバの IPv6 アドレスを入力します。
Port	認証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：「plaintext（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。

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

TACACS Group Server Settings（TACACS グループサーバ設定）

TACACS グループサーバの表示、設定を行います。

Security > TACACS > TACACS Group Server Settings をクリックして、以下の画面を表示します。

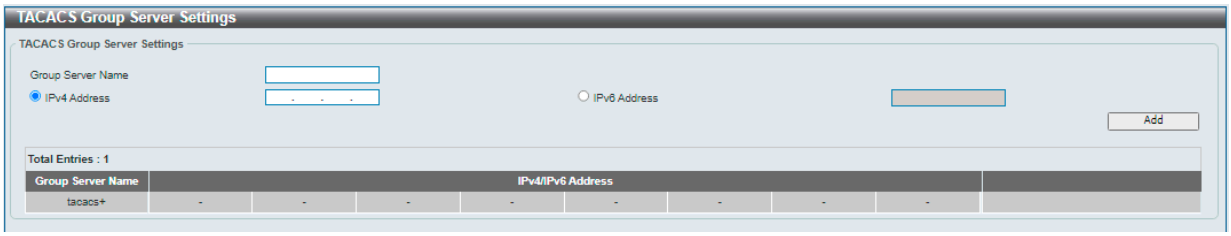


図 12-29　TACACS Group Server Settings 画面

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。（15 文字以内）
IPv4 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。

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

エントリの詳細を表示

「Detail」をクリックすると TACACS グループサーバの詳細情報について表示されます。

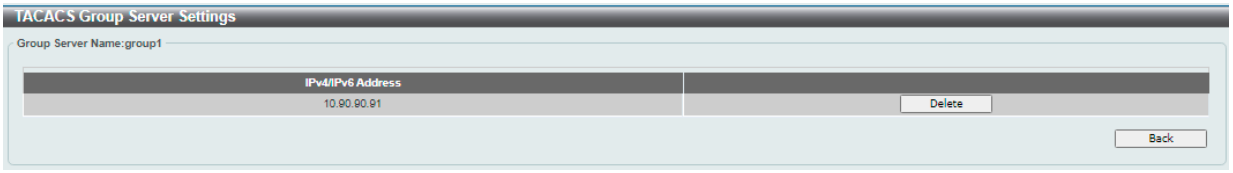


図 12-30　TACACS Group Server Settings - Detail 画面

「Delete」をクリックして指定エントリを削除します。
「Back」をクリックして以前の画面に戻ります。

TACACS Statistic（TACACS 統計情報）

TACACS 統計情報を表示します。

Security > TACACS > TACACS Statistic をクリックして、以下の画面を表示します。

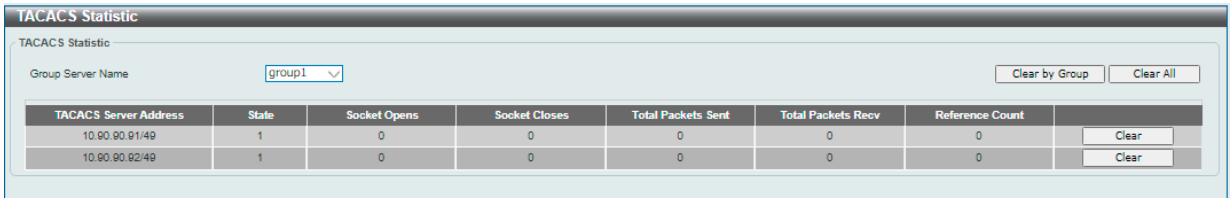


図 12-31　TACACS Statistic 画面

画面に表示される項目：

項目	説明
Group Server Name	統計情報をクリアする TACACS グループサーバ名を選択します。

「Clear by Group」をクリックして、選択に基づいて表示した情報を消去します。
「Clear All」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）

IMPB（IP-MAC-Port Binding) の設定を行います。
IP-MAC バインディングにより、スイッチにアクセスするユーザを制限することができます。

注意　ポートセキュリティと IMPB 機能は同時に有効化しないでください。

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、以下の画面を表示します。

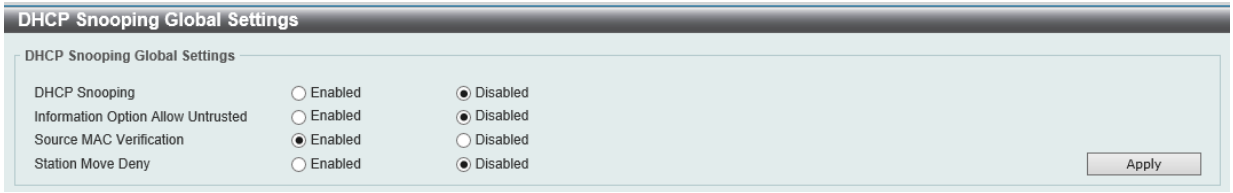


図 12-32　DHCP Snooping Global Settings 画面

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。 本機能を有効にすると、スイッチは DHCP サーバおよびクライアントから送信されたパケットをスヌーピングします。
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、ポート上の同じ VLAN ID と MAC アドレスを持つダイナミック DHCP バインディングエントリは、新しい DHCP プロセスが同じ VLAN ID と MAC アドレスに属している事を検出した場合、他のポートへ移動することが可能です。

「Apply」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、以下の画面を表示します。

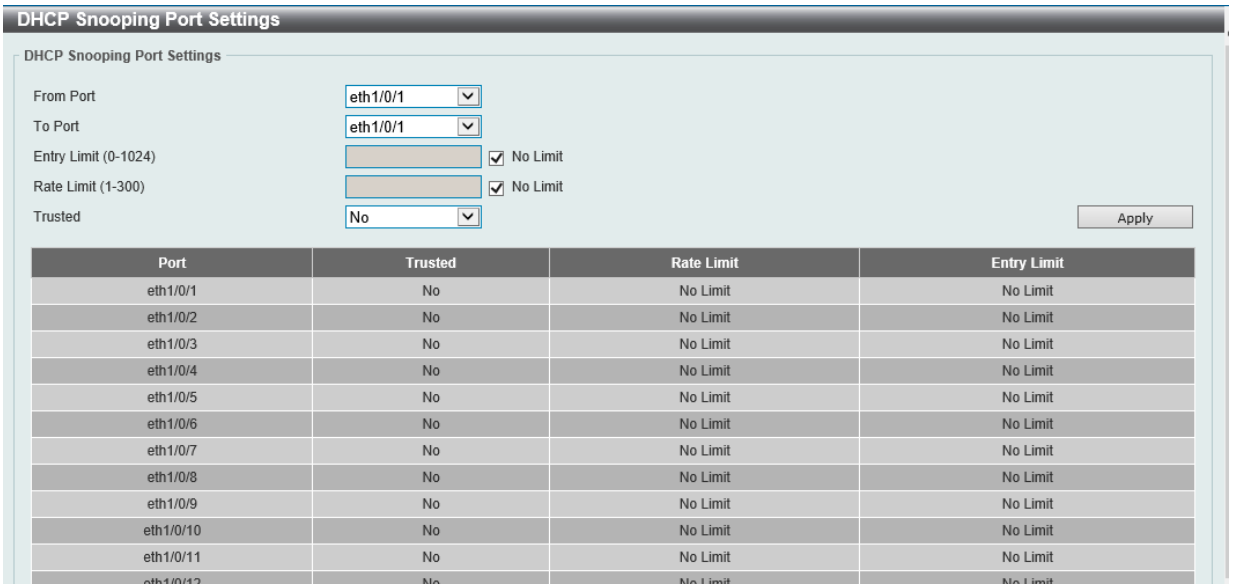


図 12-33　DHCP Snooping Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Entry Limit	エントリ制限の値を入力します。「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	レート制限の値を入力します。「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」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、以下の画面を表示します。

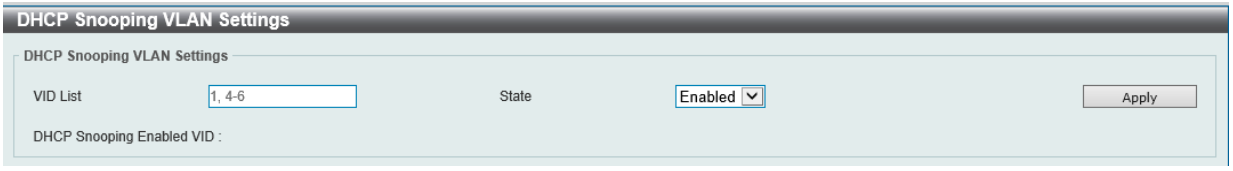


図 12-34　DHCP Snooping VLAN Settings 画面

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 / 無効に設定します。

「Apply」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、以下の画面を表示します。

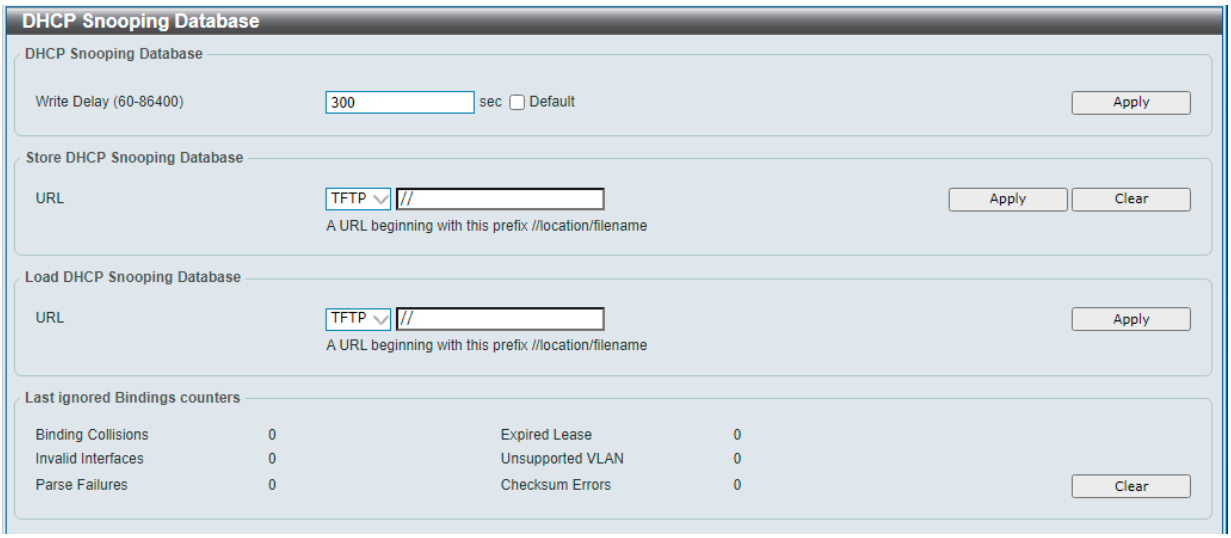


図 12-35　DHCP Snooping Database 画面

画面に表示される項目：

項目	説明
DHCP Snooping Database	
Write Delay	書き込み遅延時間の値を入力します。「Default」にチェックを入れると初期値を使用します。 • 設定可能範囲：60 - 86400（秒） • 初期値：300（秒）
Store DHCP Snooping Database	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースの保存先 URL を入力します。 • 選択肢：「TFTP」
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」

「Apply」をクリックして、設定内容を適用します。
「Store DHCP Snooping Database」セクションで「Clear」をクリックして、設定値をリセットします。
「Last ignored Bindings Counters」セクションで「Clear」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 バインディングポートエントリの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry の順にクリックして画面を表示します。

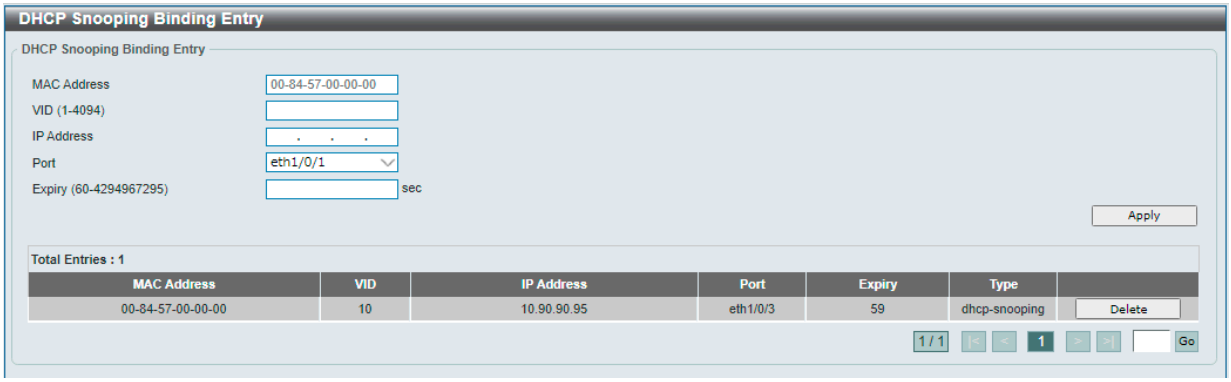


図 12-36　DHCP Snooping Binding Entry 画面

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。
Port	設定するポートを指定します。
Expiry	有効期限を入力します。 • 設定可能範囲：60 - 4294967295（秒）

「Apply」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」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」をクリックして、特定のページへ移動することができます。

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、以下の画面を表示します。

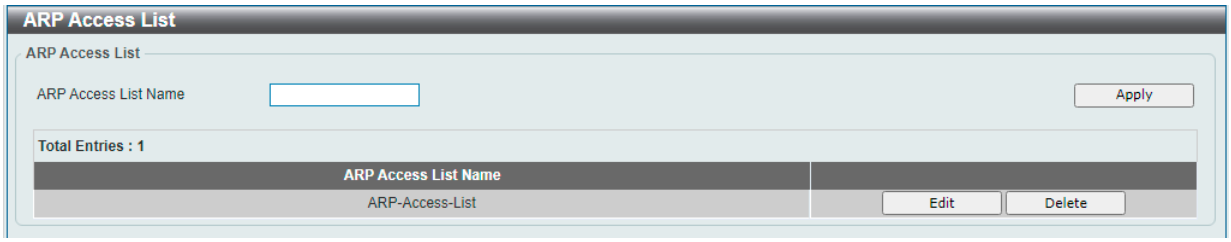


図 12-37　ARP Access List 画面

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）

「Apply」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」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」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。

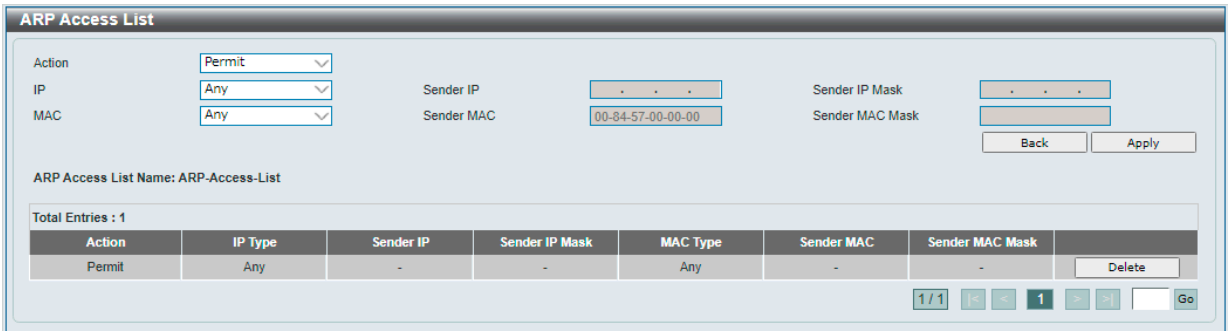


図 12-38　ARP Access List - Edit 画面

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	送信元 IP アドレスを「Host」または「IP with Mask」に設定した場合、使用する送信元 IP アドレスを入力します。
Sender IP Mask	送信元 IP アドレスを「IP with Mask」に設定した場合、使用する送信元 IP マスクを入力します。
MAC	送信元 MAC アドレスの種類を指定します。 • 選択肢：「Any」「Host」「MAC with Mask」
Sender MAC	送信元 MAC アドレスを「Host」または「MAC with Mask」に設定した場合、使用する送信元 MAC アドレスを入力します。
Sender MAC Mask	送信元 IP アドレスを「MAC with Mask」に設定した場合、使用する送信元 MAC マスクを入力します。

「Back」をクリックすると前のページに戻ります。
「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

■ 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、以下の画面を表示します。

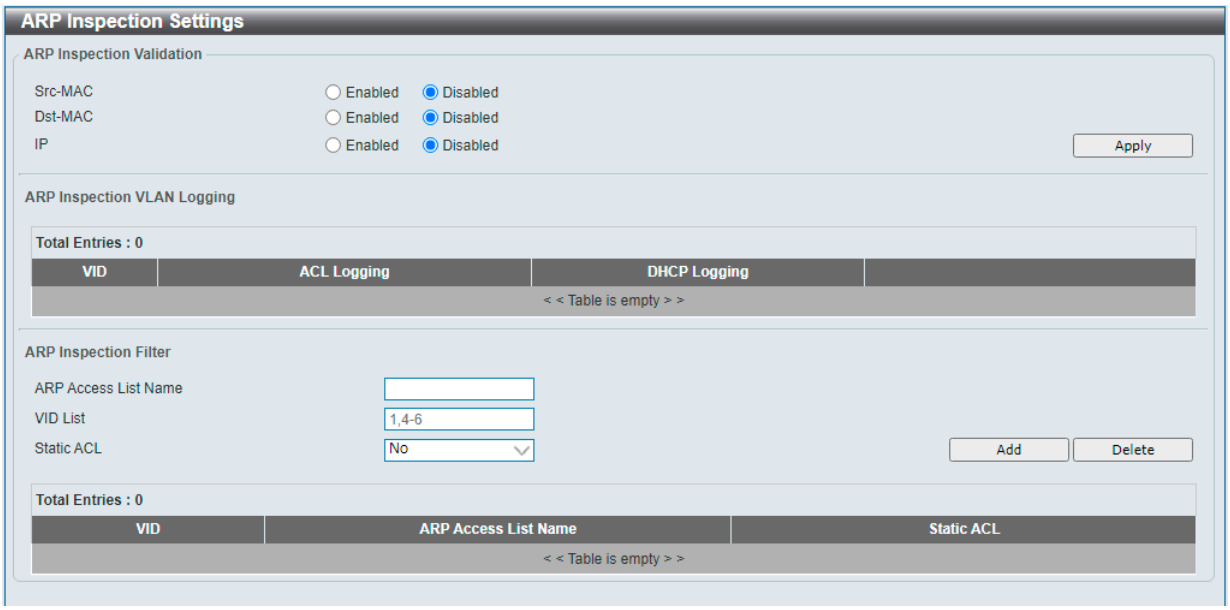


図 12-39　ARP Inspection Settings 画面

画面に表示される項目：

項目	説明
ARP Inspection Validation	
Src-MAC	送信元 MAC オプションについて有効 / 無効に設定します。 本オプションを有効にすると、ARP リクエストおよび応答パケットをチェックし、ARP ペイロードに含まれる送信元 MAC アドレスに対してイーサネットヘッダ内の送信元 MAC アドレスの整合性を検証します。
Dst-MAC	宛先 MAC オプションについて有効 / 無効に設定します。 本オプションを有効にすると、ARP 応答パケットをチェックし、ARP ペイロードに含まれる宛先 MAC アドレスに対してイーサネットヘッダ内の宛先 MAC アドレスの整合性を検証します。
IP	IP オプションについて有効 / 無効に設定します。 本オプションを有効にすると、不正な IP アドレスや予期せぬ IP アドレスがないか ARP の body をチェックします。また、ARP ペイロードにおける IP アドレスの妥当性もチェックします。 ARP リクエストとレスポンスの両方の送信元 IP、および ARP レスポンスのターゲット IP が検証されます。IP アドレス「0.0.0.0」「255.255.255.255」宛のパケットと、すべての IP マルチキャストアドレス宛てのパケットは破棄されます。送信元 IP アドレスはすべての ARP リクエストとレスポンスにおいてチェックされ、宛先 IP アドレスは ARP レスポンス内のみでチェックされます。
ARP Inspection VLAN Logging	
ACL Logging	「Edit」をクリックして、ACL ロギングの動作を選択します。 • 選択肢：「Deny」「Permit」「All」「None」
DHCP Logging	「Edit」をクリックして、DHCP ロギングの動作を選択します。 • 選択肢：「Deny」「Permit」「All」「None」
ARP Inspection Filter	
ARP Access List Name	ARP アクセスリスト名を入力します。（32 文字以内）
VID List	使用する VLAN ID リストを指定します。
Static ACL	スタティック ACL を使用する場合は「Yes」、使用しない場合は「No」を選択します。

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

■ 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、以下の画面を表示します。

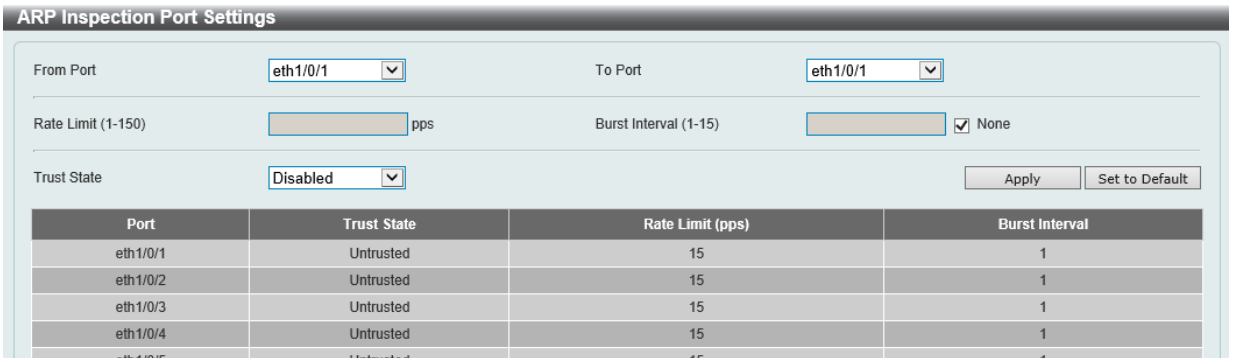


図 12-40　ARP Inspection Port Settings 画面

画面に表示される項目：

項目	説明
From Port/ To Port	設定するポートの範囲を指定します。
Rate Limit	レート制限の値を入力します。「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 - 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（信頼済み）ステータスを有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。
「Set to Default」をクリックすると、設定内容は初期値になります。

■ ARP Inspection VLAN（ARP インスペクション VLAN 設定）

VLAN での ARP インスペクションの設定、表示を行います。

Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN の順にクリックし、以下の画面を表示します。

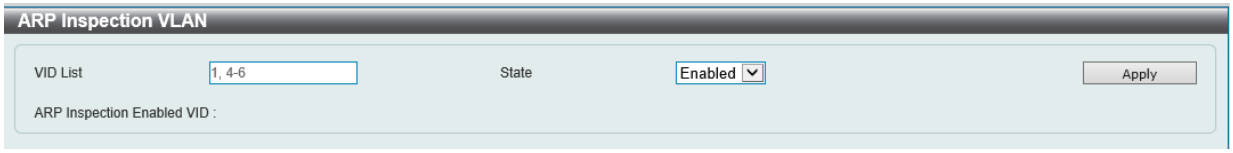


図 12-41　ARP Inspection VLAN 画面

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」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、以下の画面を表示します。

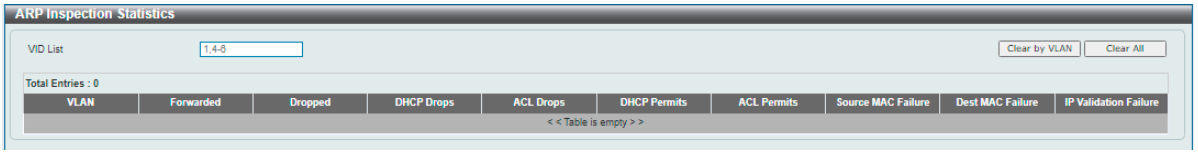


図 12-42　ARP Inspection Statistics 画面

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」をクリックして、入力した VLAN ID についての情報を消去します。
「Clear All」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」をクリックして、特定のページへ移動することができます。

■ 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、以下の画面を表示します。

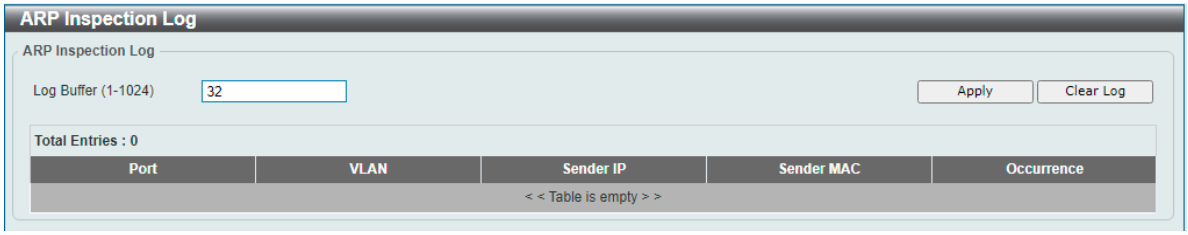


図 12-43　ARP Inspection Log 画面

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」をクリックして、設定内容を適用します。
「Clear Log」をクリックして、ログを消去します。

Network Access Authentication（ネットワークアクセス認証）

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て、以下の画面を表示します。

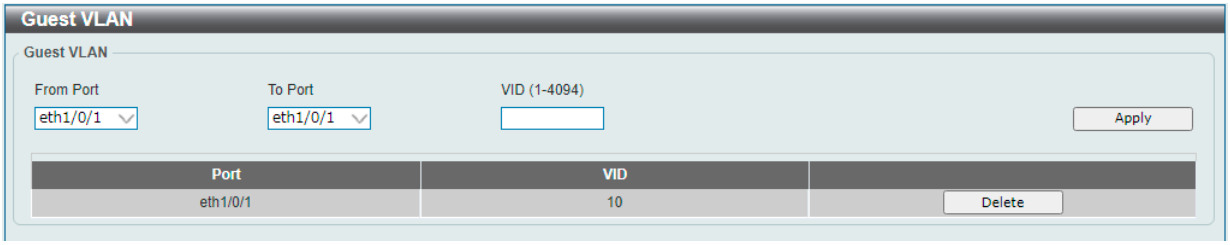


図 12-44　Guest VLAN 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
VID	設定する VLAN ID を入力します。 • 設定可能範囲：1 - 4094

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

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て、以下の画面を表示します。

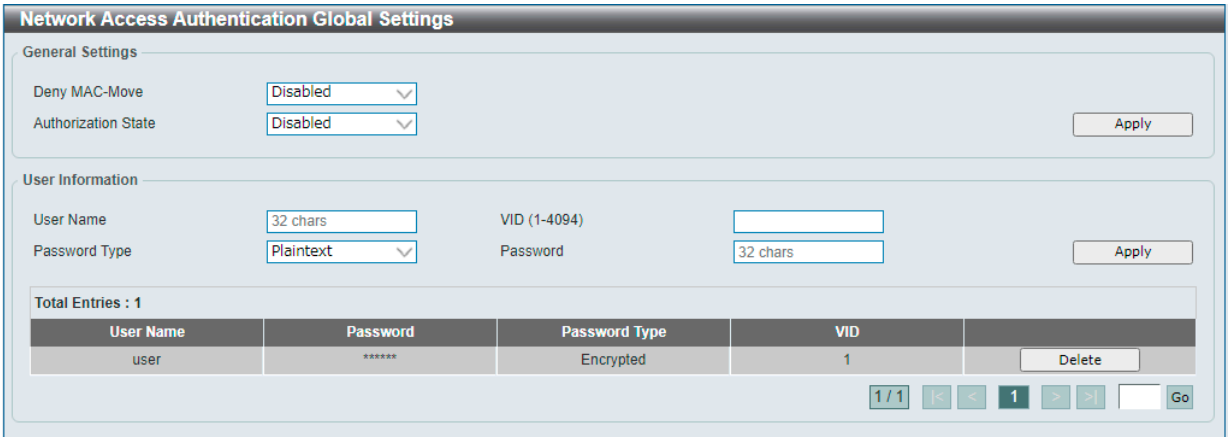


図 12-45　Network Access Authentication Global Settings 画面

画面に表示される項目：

項目	説明
General Settings	
Deny MAC-Move	MAC 移動拒否機能を有効 / 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、再認証の際に別のポートへの移動が許可されるかどうかを制御します。 本機能が有効の場合、認証ホストはスイッチの他のポートへの移動が許可されません。 本機能が無効の場合、認証ホストはスイッチの他のポートへの移動が許可されます。 移動が許可されているホストは、移動先のポートの設定に応じて、再認証が必要になるか、再認証なしで移動することができます。 - 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。 - 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。 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。

項目	説明
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」はポートごとに割り当てられます。ホストモードがマルチ認証モードの場合、「VLAN」と「802.1p」はホストごとに割り当てられます。
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：「Plaintext」（平文）」「Encrypted（暗号化）」
Password	パスワードを入力します。

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

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

注意 802.1X の機能において、ダイナミック VLAN を使用する場合、「Authorization State」を有効化、または”no authorization disable”コマンドを実行し、認証への承認（VLAN の割り当て）を有効化してください。

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て、以下の画面を表示します。

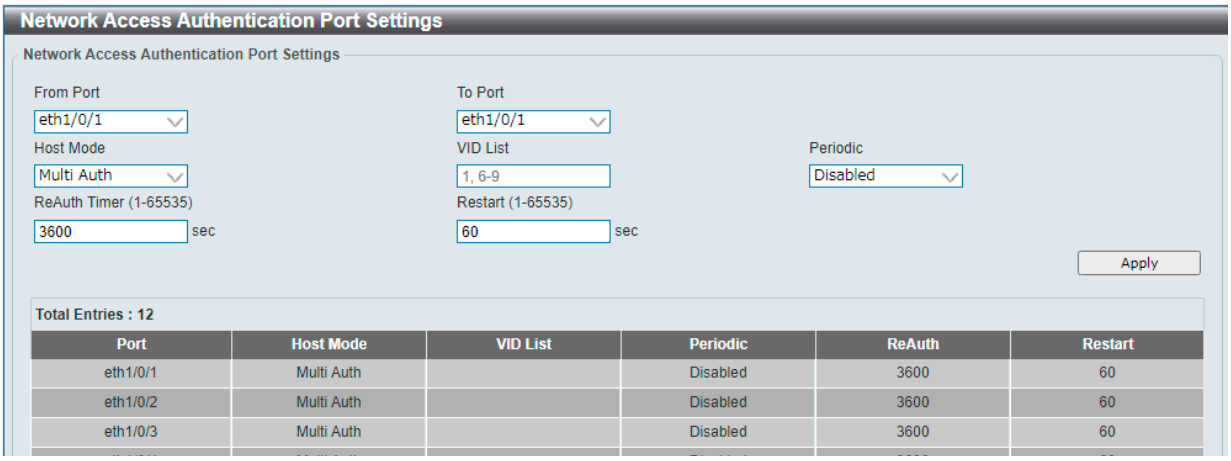


図 12-46　Network Access Authentication Port Settings 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
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、ポートは指定された時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。（初期値）
VID List	ホストモードとして「Multi Auth（マルチ認証）」オプションを選択した場合、認証を有効にする VLAN ID を入力します。認証済みのクライアントは、送信元 VLAN に関わらず再認証は行われません。ポートがマルチホストモードに変更された場合、そのポートの認証 VLAN はクリアされます。
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。 • 初期値：「Disabled」（無効）
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）

項目	説明
Restart	再起動時間を入力します。 • 設定可能範囲：1 - 65535（秒） • 初期値：60（秒）

「Apply」をクリックして、設定内容を適用します。

注意 802.1X の機能において、ダイナミック VLAN は “multi-host” のみサポートされます。

Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）

ネットワークアクセス認証セッションの情報表示、クリアを行います。

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

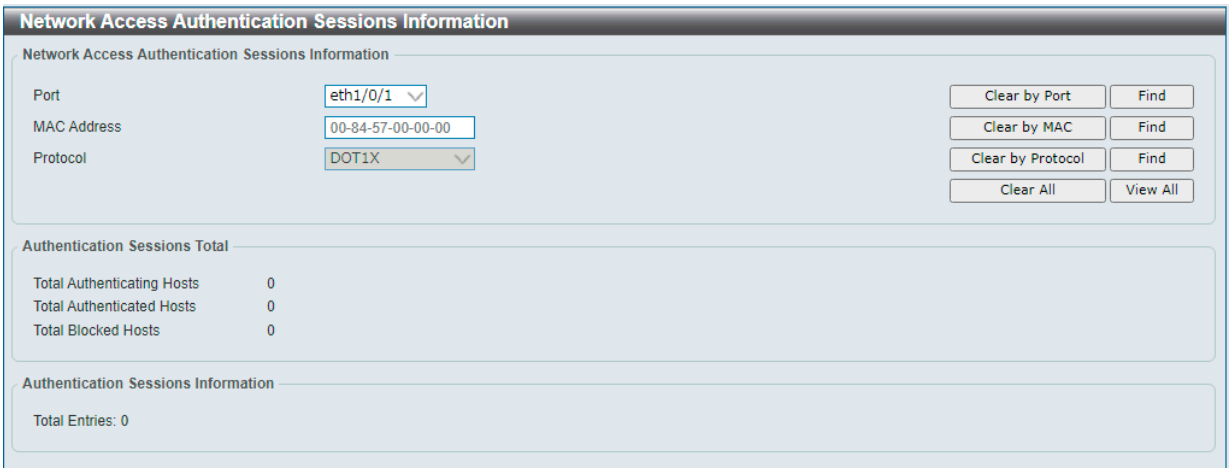


図 12-47　Network Access Authentication Sessions Information 画面

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：「DOT1X」

情報の消去

「Clear by Port」をクリックして、指定したポートに基づく情報を消去します。
「Clear by MAC」をクリックして、指定した MAC アドレスに基づく情報を消去します。
「Clear by Protocol」をクリックして、指定したプロトコルに基づく情報を消去します。
「Clear All」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」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。
「View All」をクリックして、すべてのエントリを表示します。

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。

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画面を表示します。

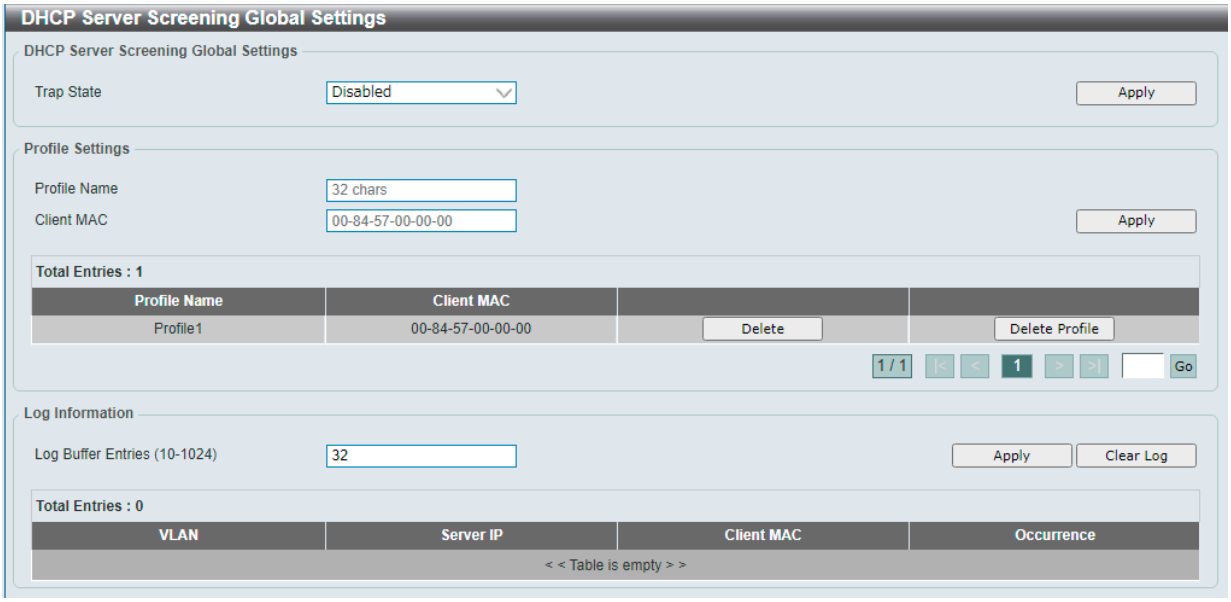


図 12-48　DHCP Server Screening Global Settings 画面

画面に表示される項目：

項目	説明
DHCP Server Screening Global Settings	
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。
Profile Settings	
Profile Name	DHCP サーバスクリーニングのプロファイル名を入力します。（32 文字以内）
Client MAC	MAC アドレスを入力します。
Log Information	
Log Buffer Entries	ログバッファエントリ数を入力します。 • 設定可能範囲：10 - 1024 • 初期値：32

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして指定エントリを削除します。
「Delete Profile」をクリックして指定プロファイルを削除します。
「Clear Log」をクリックしてログを消去します。

複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動することができます。

DHCP Server Screening Port Settings（DHCP サーバスクリーニングポート設定）

DHCP サーバスクリーニングポートの表示、設定を行います。

Security > DHCP Server Screening > DHCP Server Screening Port Settings の順にクリックし、画面を表示します。

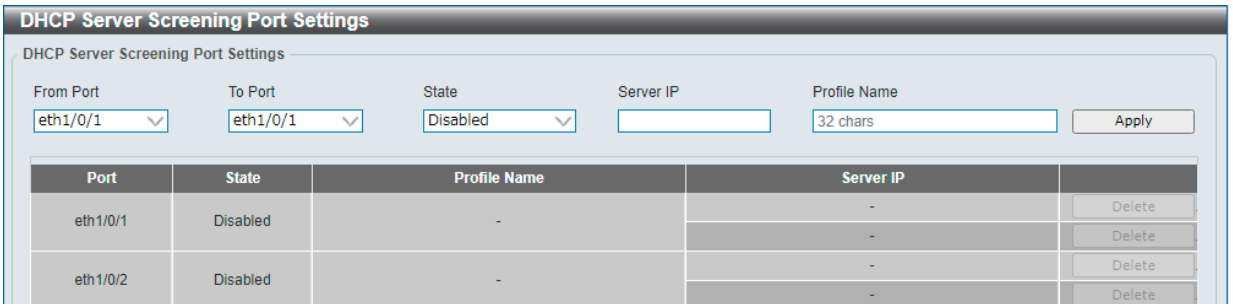


図 12-49　DHCP Server Screening Port Settings 画面

画面に表示される項目：

項目	説明
From Port/ To Port	設定するポートの範囲を指定します。
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 IPv4 アドレスまたは IPv6 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」をクリックして、設定内容を適用します。
「Delete」をクリックして、指定エントリを削除します。

Safeguard Engine（セーフガードエンジン）

セーフガードエンジンは、パケットフラッディングによるスイッチの CPU への影響を自動的に抑制する機能です。
悪意のあるウィルスやワームによる攻撃が スイッチの動作に影響を与えないように保護を行います。

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

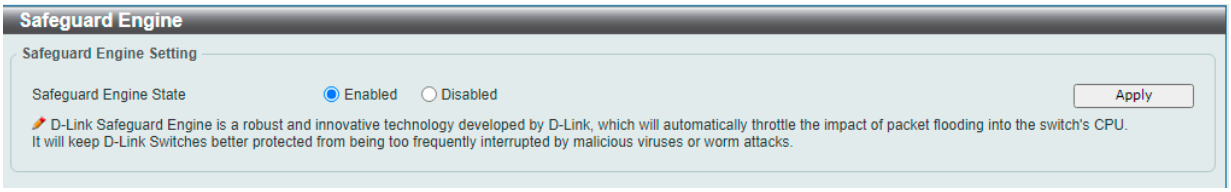


図 12-50　Safeguard Engine 画面

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。

「Apply」をクリックして、設定内容を適用します。

Trusted Host（トラストホスト）

トラストホストの設定、表示を行います。

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

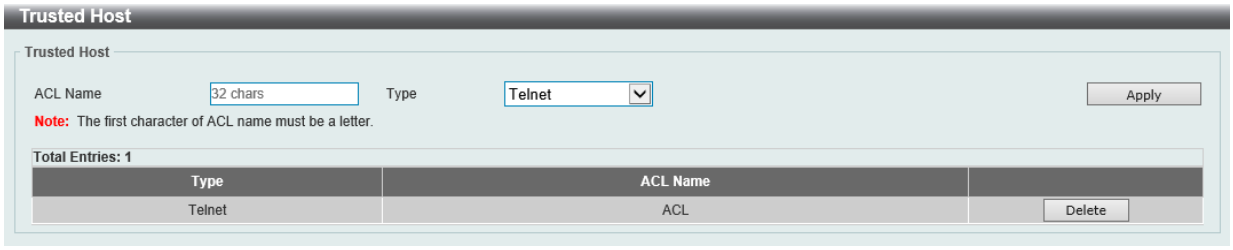


図 12-51　Trusted Host 画面

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」「Ping」「HTTP」「HTTPS」「SSH」

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

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

レイヤ 2 パケット転送において、ポートで受信するパケットのフローを指定した転送ドメインに制限することができます。トラフィックの制限機能として VLAN を使用する方法もありますが、本機能ではトラフィックフローがより制限されます。

Security > Traffic Segmentation 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。

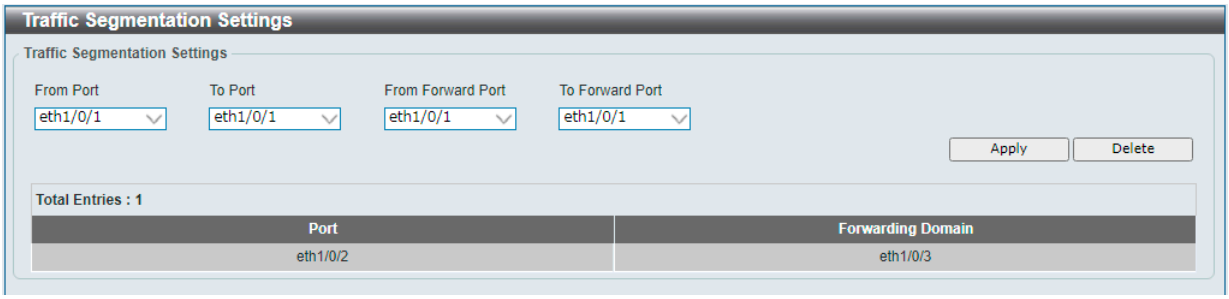


図 12-52　Traffic Segmentation Settings 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定する受信ポート範囲を指定します。
From Forward Port / To Forward Port	設定する転送ポート範囲を指定します。

「Apply」をクリックして、指定した情報を基に新しいエントリを追加します。
「Delete」をクリックして、指定した情報を基にエントリを削除します。

Storm Control Settings（ストームコントロール設定）

ストームコントロールの設定、表示を行います。

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

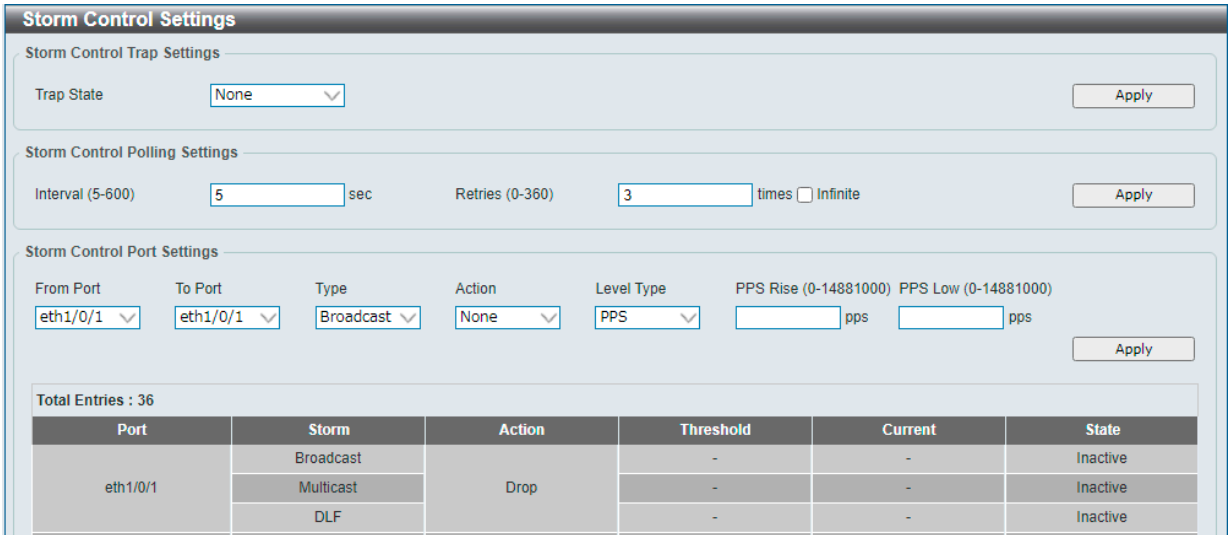


図 12-53　Storm Control Settings 画面

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	
Interval	受信パケットカウントのポーリング間隔を指定します。 • 設定可能範囲：5 - 600（秒） • 初期値：5（秒）
Retries	アクションが「Shutdown」に設定されている場合、指定回数ストームを検知すると、エラー無効状態に移行します。 「0」を指定した場合、ストームを検出するとすぐにエラー無効状態に移行します。 「Infinite」にチェックを入れると、ストームを検知してもエラー無効状態に移行しません。 • 定可能範囲：0 - 360 • 初期値：3
Storm Control Port Settings	
From Port / To Port	設定するポートの範囲を指定します。
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」「DLF（Destination Lookup Failure/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」の両方が参照されます。 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を指定します。 • 「None」- ストームパケットをフィルタしません。 • 「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。 • 「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。
Level Type	レベルタイプを指定します。 • 選択肢：「PPS」「Kbps」
PPS Rise	レベルタイプで「PPS」を選択した場合、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 - 14881000（パケット / 秒）
PPS Low	レベルタイプで「PPS」を選択した場合、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 - 14881000（パケット / 秒）

項目	説明
Kbps Rise	レベルタイプで「Kbps」を選択した場合、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 - 10000000（Kbps）
Kbps Low	レベルタイプで「Kbps」を選択した場合、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 - 10000000（Kbps）

「Apply」をクリックして、設定内容を適用します。

注意　ブロードキャスト、マルチキャスト、ユニキャストにはそれぞれ異なるしきい値を設定することができません。最新の設定値がすべての種類のパケットに適用されます。

注意　コントロールするストームの種類に「Multicast」を指定した場合、予約 MAC アドレス（VRRP、OSPF、IGMP、MLD など）に対する制限は適用されません。

注意　ストームコントロール機能について、ポートチャネルには適用できません。

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

Denial-of-Service（DoS）攻撃防止の設定を行います。

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

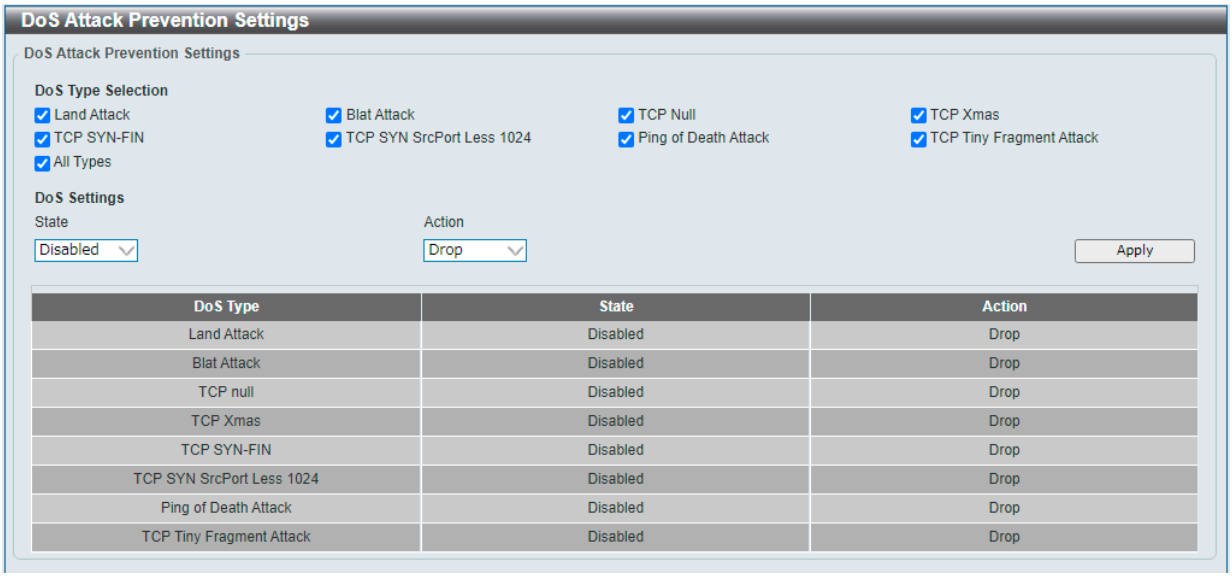


図 12-54　DoS Attack Prevention Settings 画面

画面に表示される項目：

項目	説明
DoS Attack Prevention Settings	
DoS Type Selection	DoS 攻撃防止のタイプを選択します。
DoS Settings	
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」をクリックして、設定内容を適用します。

注意　Direct Method を使用した「TCP Tiny Fragment Attack」の破棄はサポートされません。

SSH（Secure Shell の設定）

SSH（Secure Shell）は、リモートネットワーク間で安全性の高い、暗号化された通信を実現します。SSH は、平文の通信（Telnet）に比べてより安全な通信です。

SSH Global Settings（SSH グローバル設定）

SSH グローバル設定を行います。

Security > SSH > SSH Global Settings の順にメニューをクリックします。

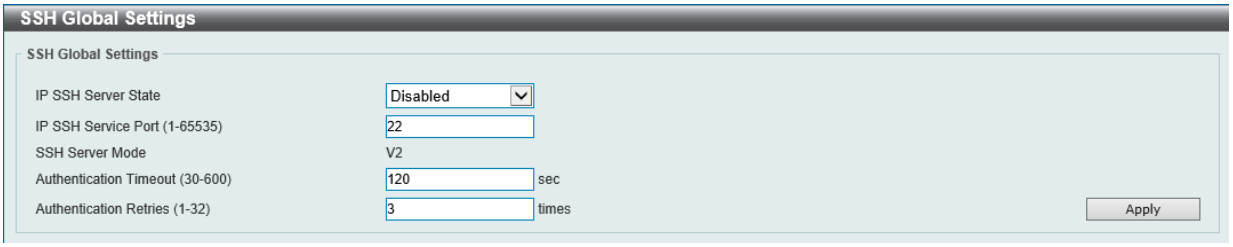


図 12-55　SSH Global Settings 画面

画面に表示される項目：

項目	説明
IP SSH Server State	SSH 機能のグローバルステータスを有効 / 無効にします。
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スイッチは接続を切断し、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」をクリックして、設定内容を適用します。

Host Key（Host Key 設定）

SSH ホスト鍵の設定を行います。

Security > SSH > Host Key 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。

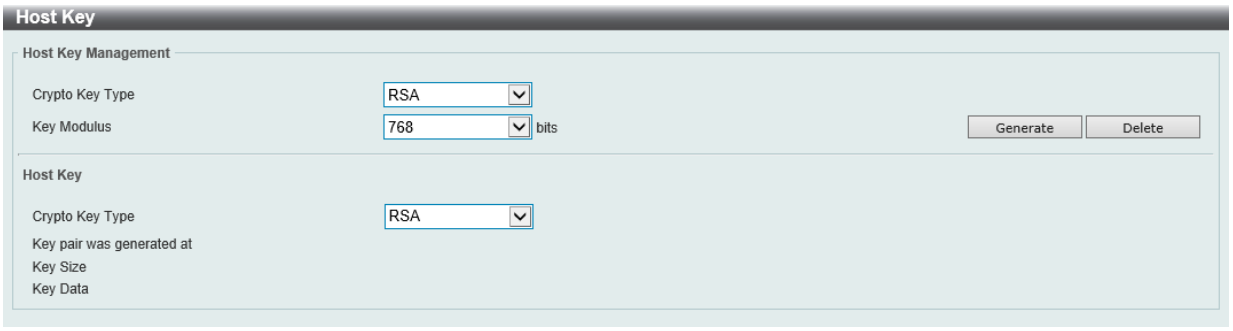


図 12-56　Host Key 画面

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。 • 「RSA（Rivest Shamir Adleman）」「DSA（Digital Signature Algorithm）」
Key Modulus	鍵長を選択します。「DSA」を選択した場合、1024 ビット固定になります。 • 選択肢：「1024」「2048」（ビット）

項目	説明
Host Key	
Crypto Key Type	表示する暗号鍵の種類を選択します。 • 「RSA（Rivest Shamir Adleman）」「DSA（Digital Signature Algorithm）」

「Generate」をクリックして、指定したホスト鍵を生成します。
「Delete」をクリックして、指定したホスト鍵を削除します。

「Generate」をクリックすると鍵の生成が開始されます。
鍵の生成が完了すると次のメッセージが表示されます。

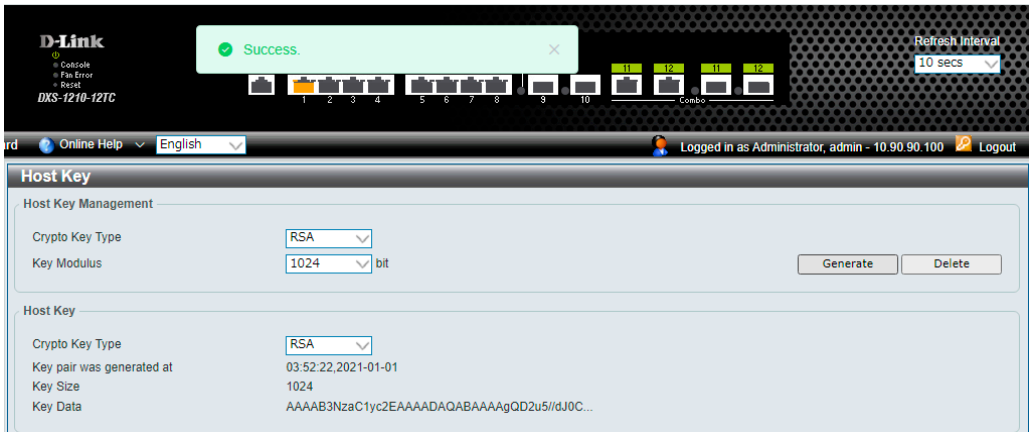


図 12-57　Success メッセージ

注意　既知の問題により、SSH ホスト鍵の設定において、DSA および RSA キーを生成し、システムを再起動後、再度 DSA および RSA キーを生成し直した場合にシステムがクラッシュする場合がありますので、この操作を行わないようにしてください。

SSH Server Connection（SSH サーバ接続）

SSH サーバ接続テーブルを表示します。

Security > SSH > SSH Server Connection 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。

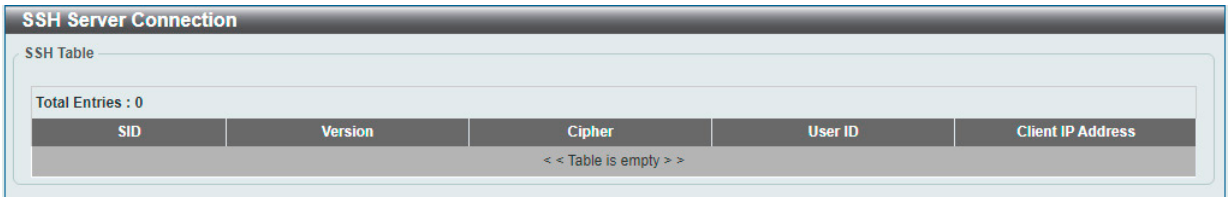


図 12-58　SSH Server Connection 画面

SSH User Authentication List（SSH ユーザ認証リスト）

SSH ユーザを表示、設定します。

Security > SSH > SSH Authentication Lists 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。

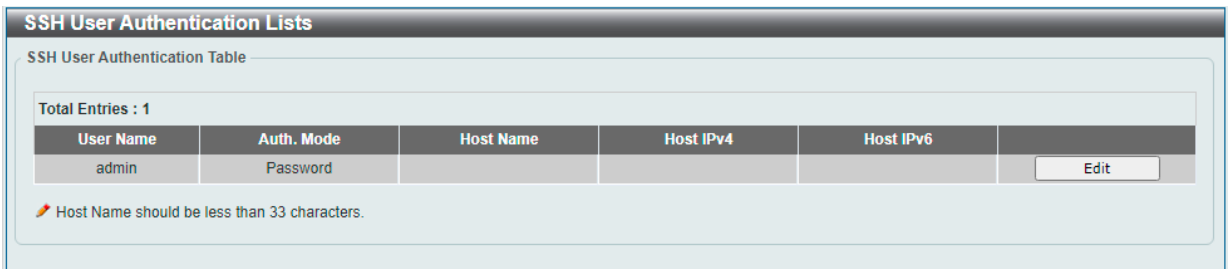


図 12-59　SSH User Authentication List 画面

■ ユーザ設定の編集

指定エントリの「Edit」をクリックして、以下の画面を表示します。

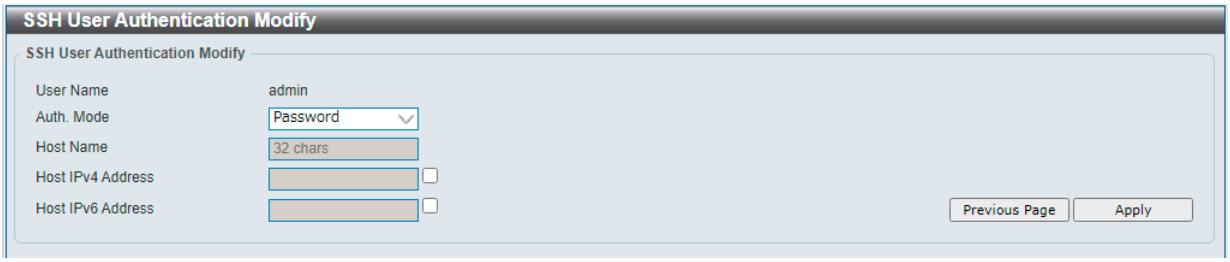


図 12-60　SSH User Authentication Modify 画面

画面に表示される項目：

項目	説明
User Name	SSH ユーザ名が表示されます。
Auth Mode	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：「Public Key」「Password」「Host based」
Host Name	認証モードで「Host based」を選択した場合、ホスト名を入力します。
Host IPv4 Address	認証モードで「Host based」を選択した場合、IPv4 アドレスを入力します。
Host IPv6 Address	認証モードで「Host based」を選択した場合、IPv6 アドレスを入力します。

「Apply」をクリックして、設定内容を適用します。

SSH Public Key Settings（SSH 公開鍵設定）

SSH 公開鍵を設定します。

Security > SSH > SSH Public Key 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。

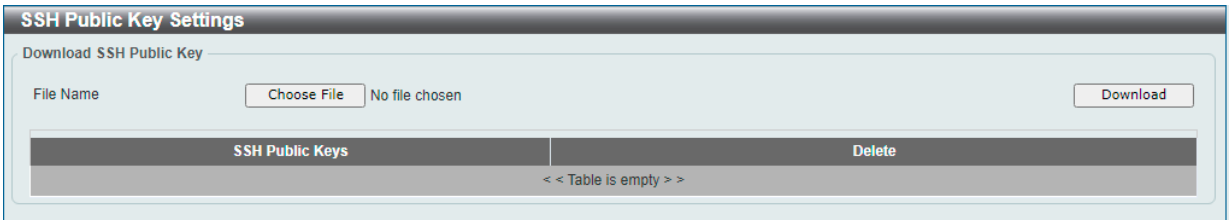


図 12-61　SSH Public Key Settings 画面

画面に表示される項目：

項目	説明
File Name	「Choose File」をクリックして、ローカルフォルダに保存した公開鍵ファイルを指定します。

「Download」ボタンをクリックして、スイッチに公開鍵をダウンロードします。

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により構成されます。

SSL Global Settings（SSL グローバル設定）

SSL グローバル設定を行います。

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

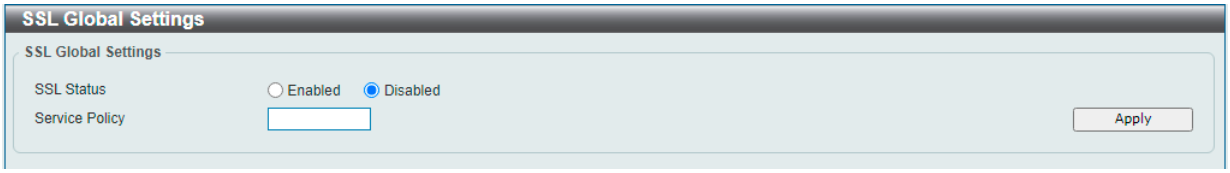


図 12-62　SSL Global Settings 画面

画面に表示される項目：

項目	説明
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。

「Apply」をクリックして、設定内容を適用します。

注意　SSL を無効にしても、HTTP は有効になりません。HTTP を有効にする場合は、**Management > Telnet/Web** 画面で「Web State」を「Enabled」に変更して下さい。

注意　SSL が有効である場合、暗号化により Web を開く際に通常よりも長い時間がかかります。コンフィグレーションの保存後、システムのサマリページの表示まで 10 秒ほどお待ちください。

SSL Service Policy（SSL サービスポリシー）

SSL サービスポリシーの表示、設定を行います。

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

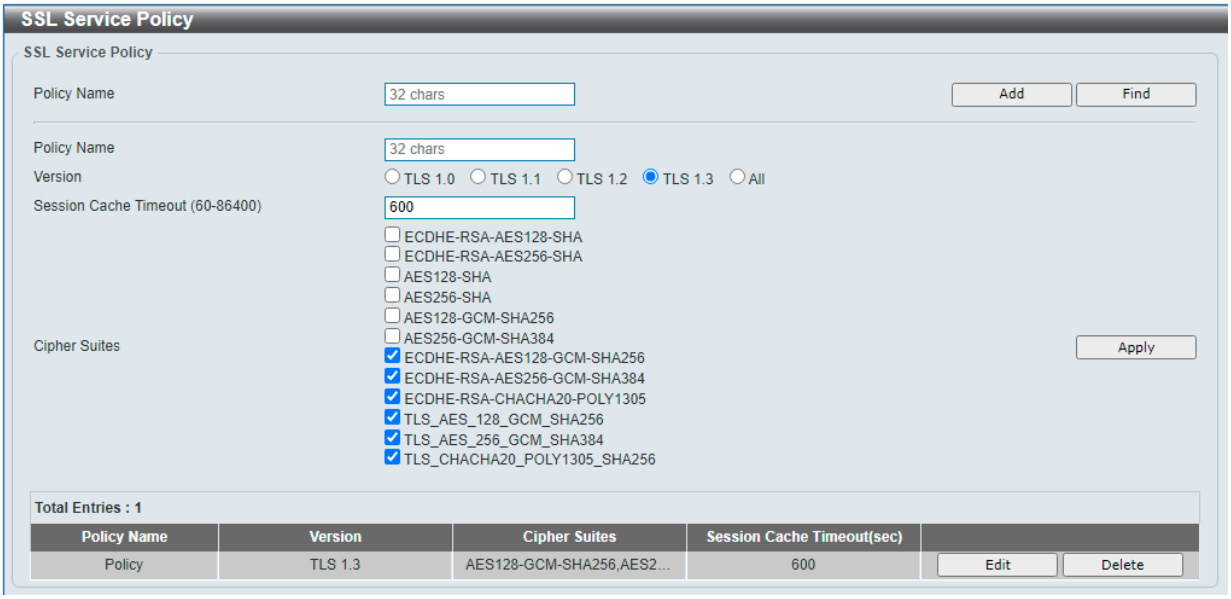


図 12-63　SSL Service Policy 画面

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」「TLS 1.3」「All（全て）」
Session Cache Timeout	セッションキャッシュの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）
Cipher Suites	本プロファイルの暗号スイートを選択します。

「Add」をクリックして、プロファイルを作成します。
「Apply」をクリックして、設定内容を適用します。
「Find」をクリックして、入力した情報に基づいて指定エントリを検出します。
「Edit」をクリックして、指定エントリを編集します。
「Delete」をクリックして、指定エントリを削除します。

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
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。
DDM（DDM 設定）	Digital Diagnostic Monitoring（DDM）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。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。

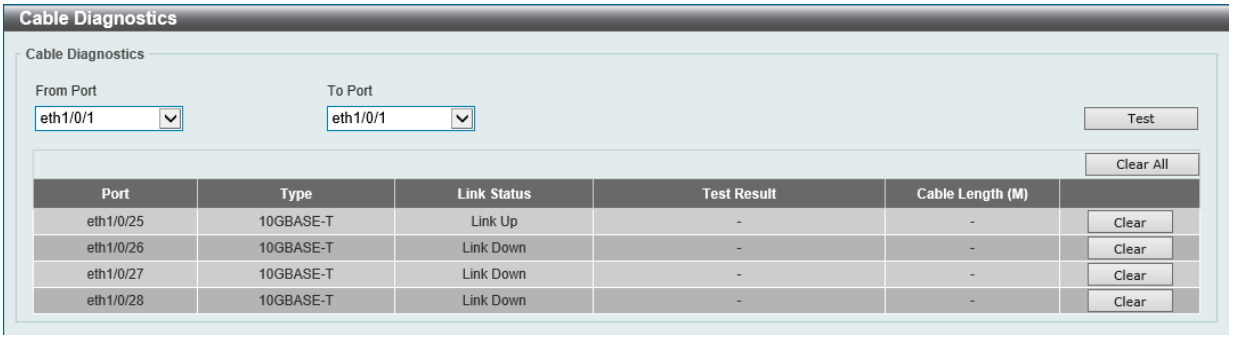


図 13-1　Cable Diagnostics 画面

■ ケーブル診断の手順

1. 「From Port」「To Port」で診断するポートを選択します。
2. 「Test」をクリックします。情報が画面に表示されます。

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

注意　ケーブル診断は SFP+ スロットではサポートされません。

注意　ケーブル診断のテスト結果に関して、以下の制限があります。

- 1m 未満のケーブルをご利用の場合、標準の Copper ポート（非コンボポート）におけるテスト結果が N/A と表示されます。
- ケーブルが接続されていないポートについて、" No Cable" ではなくエラー表示となる場合があります。
- 最初のテスト結果が「Link Down」と表示される場合があります。ページの更新により「Link UP」と表示されます。
- 電源オフのリンクパートナーが接続されているポートについて、診断結果が OK となる場合があります。

■ 情報の消去

「Clear」をクリックし、当該ポートの情報を消去します。
「Clear All」をクリックし、テーブル上のすべての情報を消去します。

■ 障害メッセージ

- Open - エラーペアのケーブルが示された位置で接続されていません。
- Short - エラーペアのケーブルは、示された位置でショート（短絡）しています。
- Open or Short - ケーブルにオープン（断線）またはショート（短絡）の問題がありますが、PHY にはそれらを区別する機能がありません。
- Crosstalk - エラーペアのケーブルは、示された位置でクロストークの問題があります。
- Shutdown - リモートパートナーの電源がオフです。
- Unknown - テストのステータスが不明です。
- OK - ペアやケーブルに問題はありません。
- No cable - ポートには、リモートパートナーへのケーブル接続がありません。

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、アラーム / 警告設定、温度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。

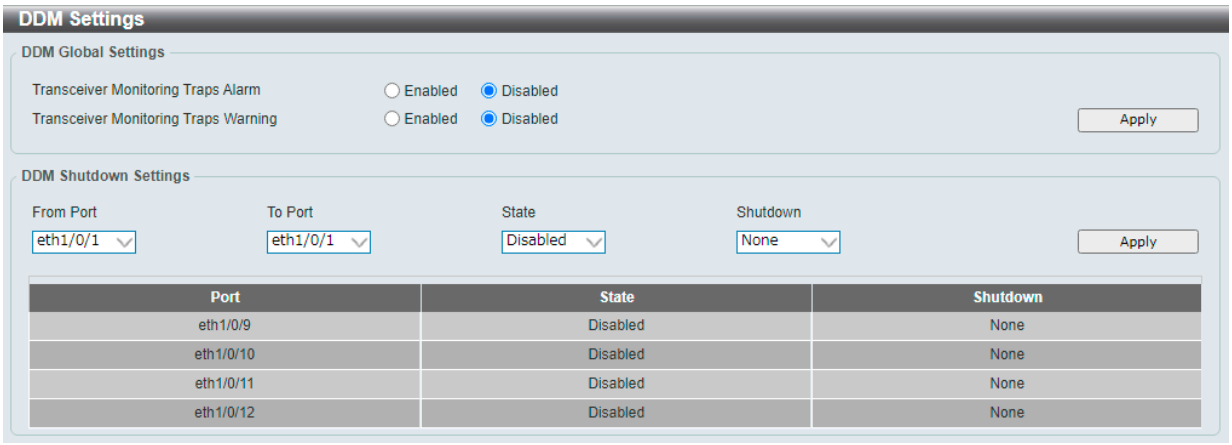


図 13-2　DDM Settings 画面

画面に表示される項目：

項目	説明
DDM Global Settings	
Transceiver Monitoring Traps Alarm	トランシーバモニタリングのアラームレベルのトラップ通知を有効 / 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警告レベルのトラップ通知を有効 / 無効に設定します。
DDM Shutdown Settings	
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。 • 「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） • 「Alarm」- Alarm（アラーム）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（警告）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。

「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。

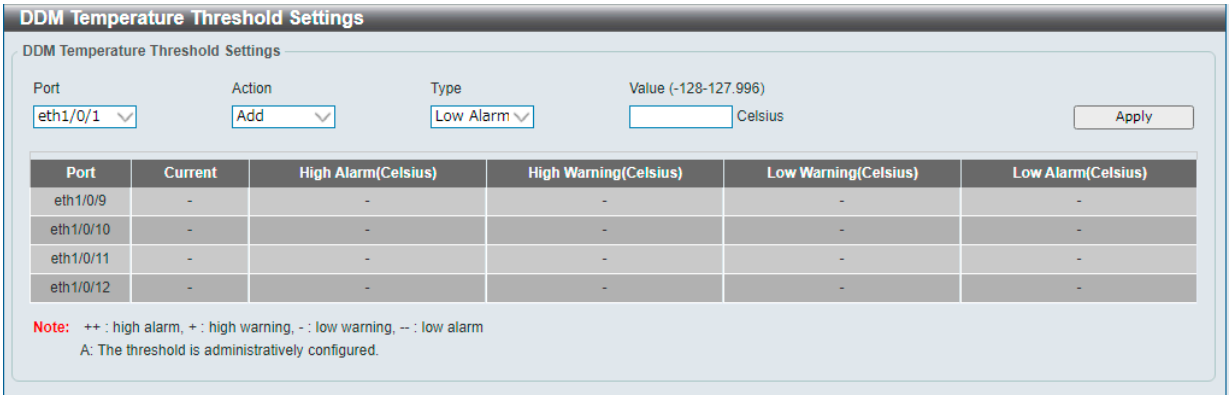


図 13-3　DDM Temperature Threshold Settings 画面

画面に表示される項目：

項目	説明
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を指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	温度しきい値の値を指定します。 • 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。

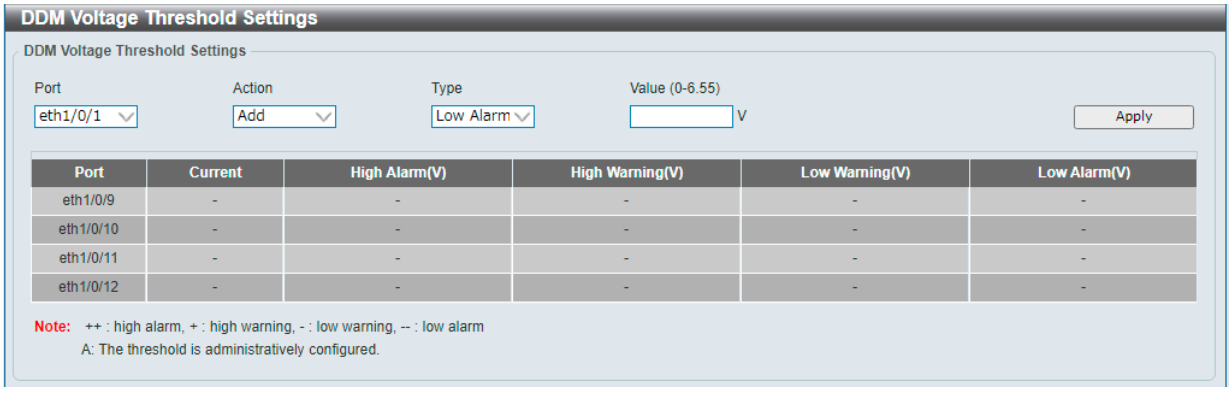


図 13-4　DDM Voltage Threshold Settings 画面

画面に表示される項目：

項目	説明
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を指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	電圧しきい値の値を指定します。 • 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。

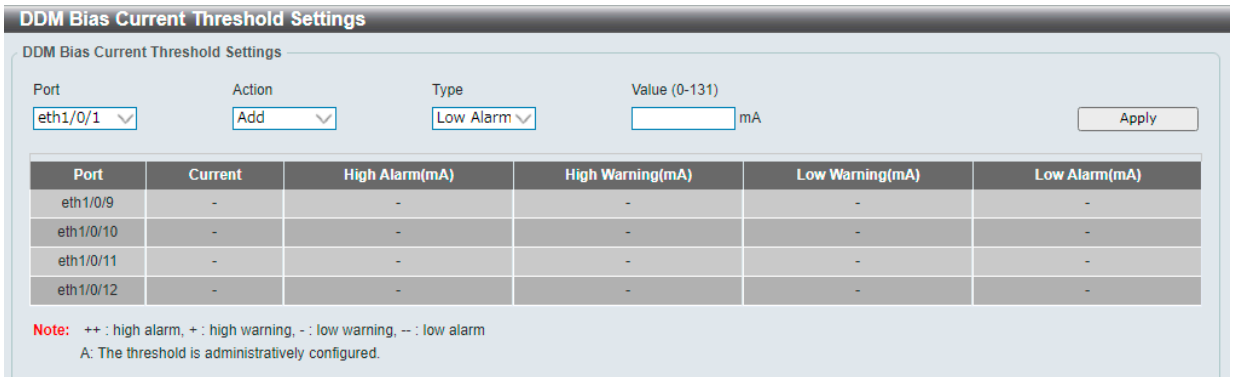


図 13-5　DDM Bias Current Threshold Settings 画面

画面に表示される項目：

項目	説明
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を指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Value	バイアス電流しきい値の値を指定します。 • 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。

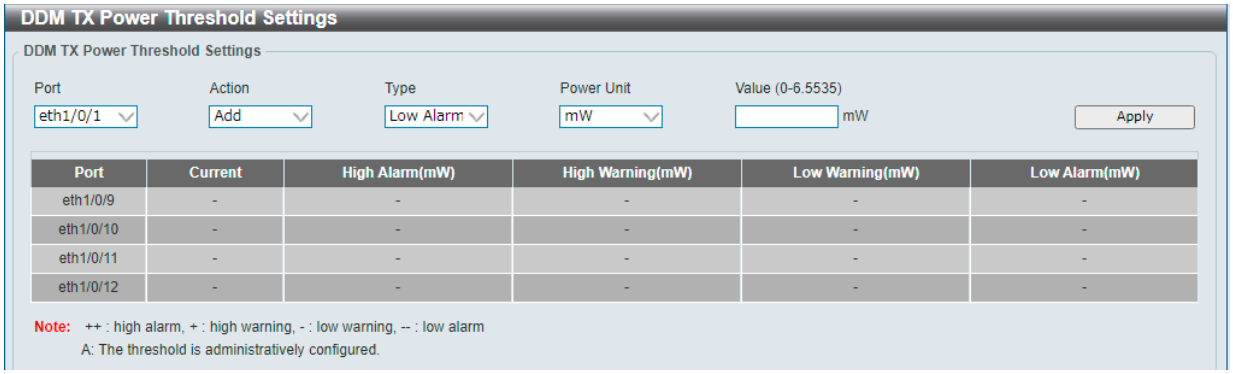


図 13-6　DDM TX Power Threshold Settings 画面

画面に表示される項目：

項目	説明
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を指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Power Unit	送信電力の単位を指定します。 • 選択肢：「mW」「dBm」
Value	送信電力しきい値の値を指定します。 • 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。

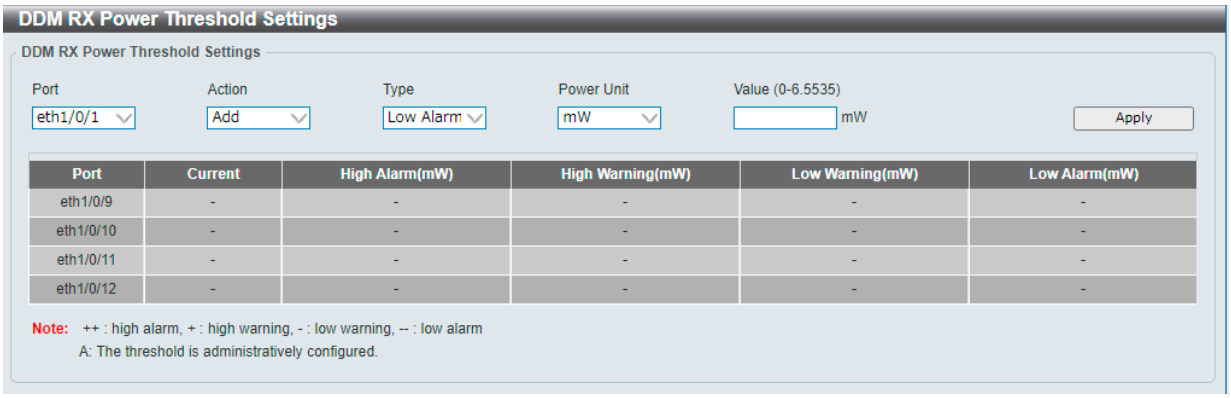


図 13-7　DDM RX Power Threshold Settings 画面

画面に表示される項目：

項目	説明
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を指定します。 • 選択肢：「Low Alarm」「Low Warning」「High Alarm」「High Warning」
Power Unit	受信電力の単位を指定します。 • 選択肢：「mW」「dBm」
Value	受信電力しきい値の値を指定します。 • 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 診断ステータスを表示します。

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。

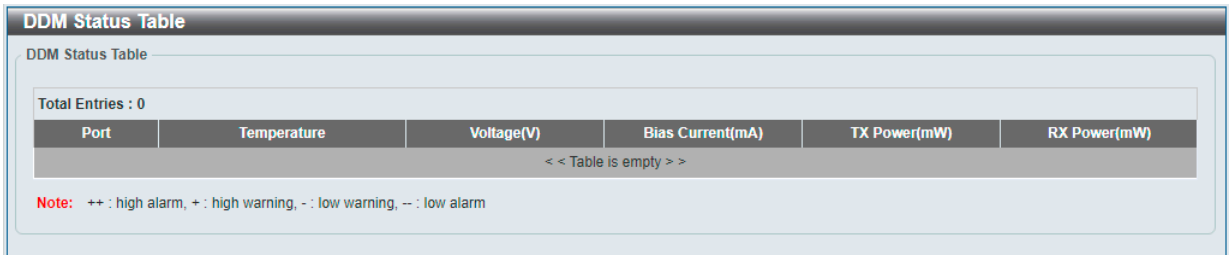


図 13-8図 13-8　　DDM Status Table 画面

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　Monitoring（スイッチのモニタリング）

Monitoring メニューを使用し、本スイッチのパケット統計、パケットエラーおよびパケットサイズ等の情報を提供することができます。

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

サブメニュー	説明
Statistics（統計情報）	パケット統計情報とエラー統計情報を表示します。
Mirror Settings（ミラー設定）	ポートミラーリングの設定を行います。

Statistics（統計情報）

スイッチの統計情報を表示します。

Port（ポート統計情報）

ポートのパケット統計を表示します。

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

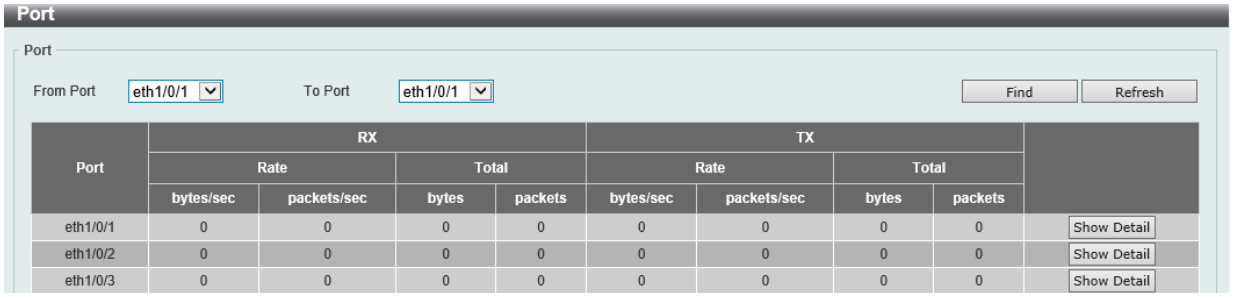


図 14-9　Port 画面

画面に表示される項目：

項目	説明
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」をクリックし、指定ポートの情報を表示します。
「Refresh」をクリックし、テーブルの情報を更新します。
「Show Detail」をクリックし、指定ポートの詳細情報について表示します。

「Show Detail」をクリックすると以下の画面が表示されます。

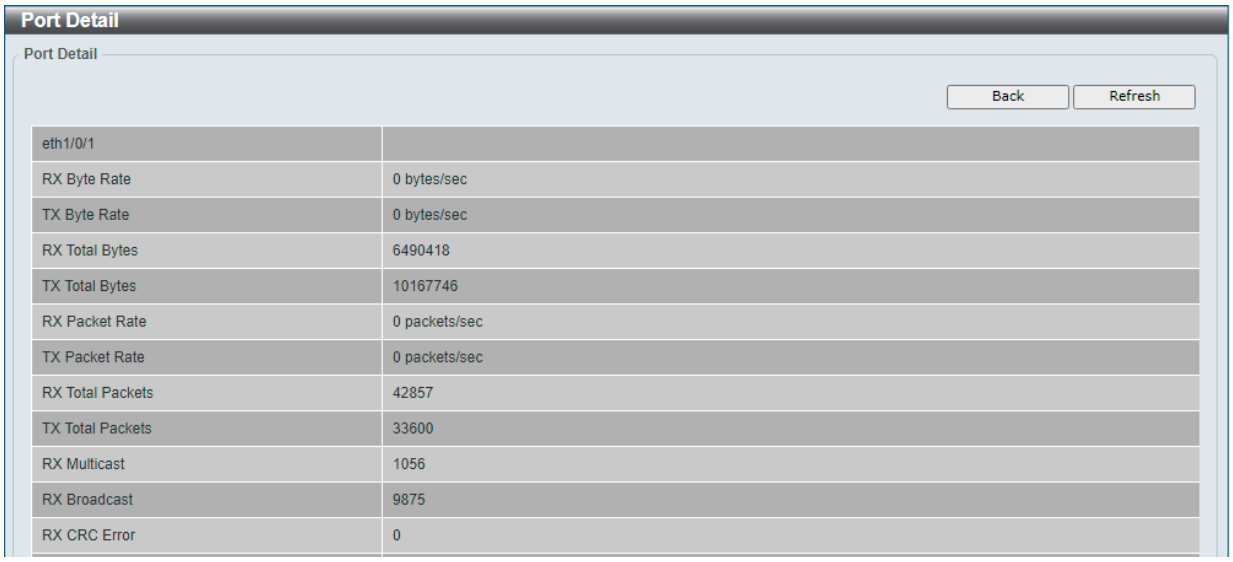


図 14-10　Port Detail 画面

「Refresh」をクリックし、テーブルを更新します。
「Back」をクリックし、前の画面に戻ります。

注意　RX CRC Error の表示はサポートされません。

Port Counters（ポートカウンタ）

ポートカウンタ情報について表示します。

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

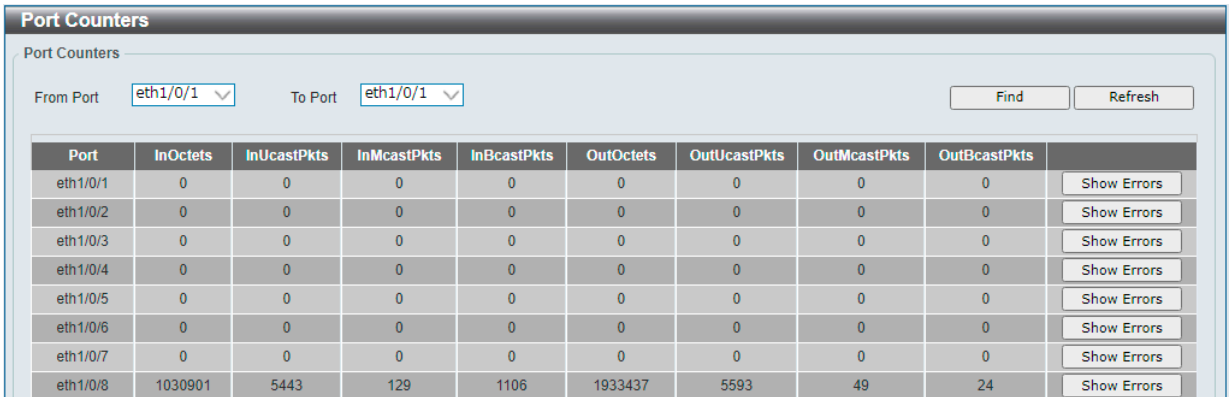


図 14-11　Port Counters 画面

画面に表示される項目：

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

「Find」をクリックし、指定ポートの情報を表示します。
「Refresh」をクリックし、テーブルを更新します。

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

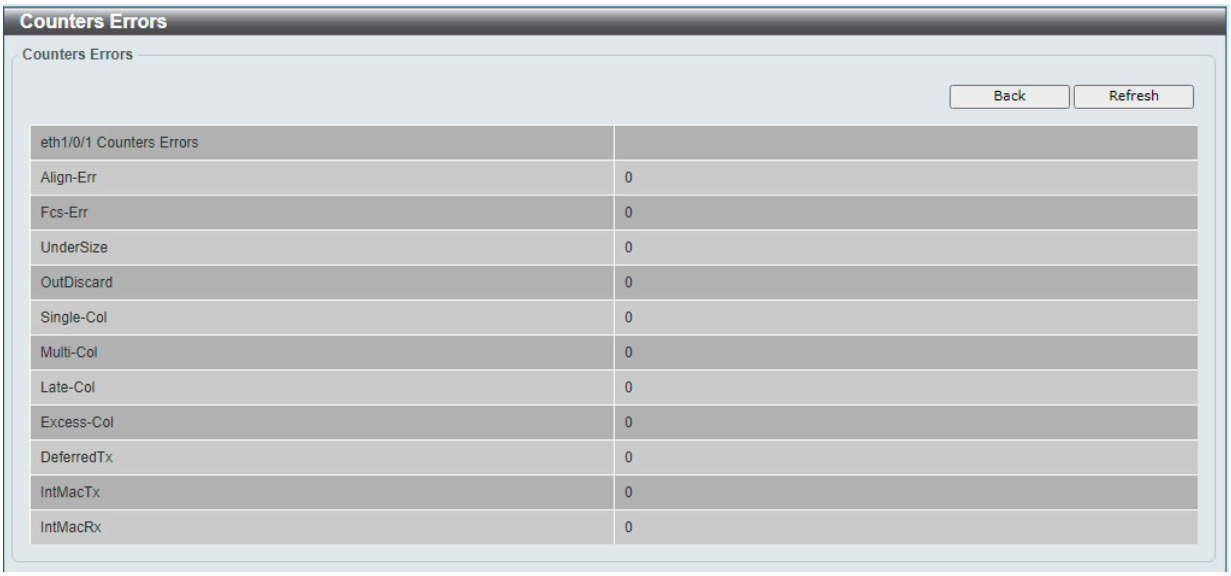


図 14-12　Counters Errors 画面

「Refresh」をクリックし、テーブルを更新します。
「Back」をクリックし、前の画面に戻ります。

Counters（カウンタ）

すべてのポートのカウンタ情報を表示、消去します。

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

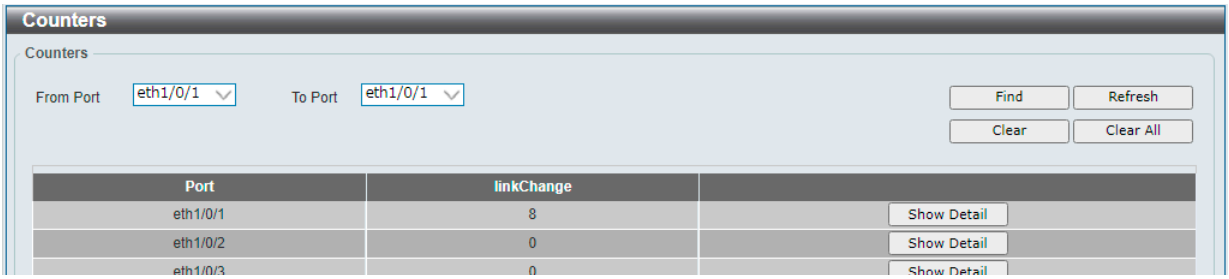


図 14-13　Counters 画面

画面に表示される項目：

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

「Find」をクリックし、指定ポートの情報を表示します。
「Refresh」をクリックし、テーブルを更新します。
「Clear」をクリックし、指定ポートの情報を消去します。
「Clear All」をクリックし、テーブル上のすべての情報を消去します。

詳細を表示

「Show Detail」をクリックし、指定ポートの詳細情報について表示します。

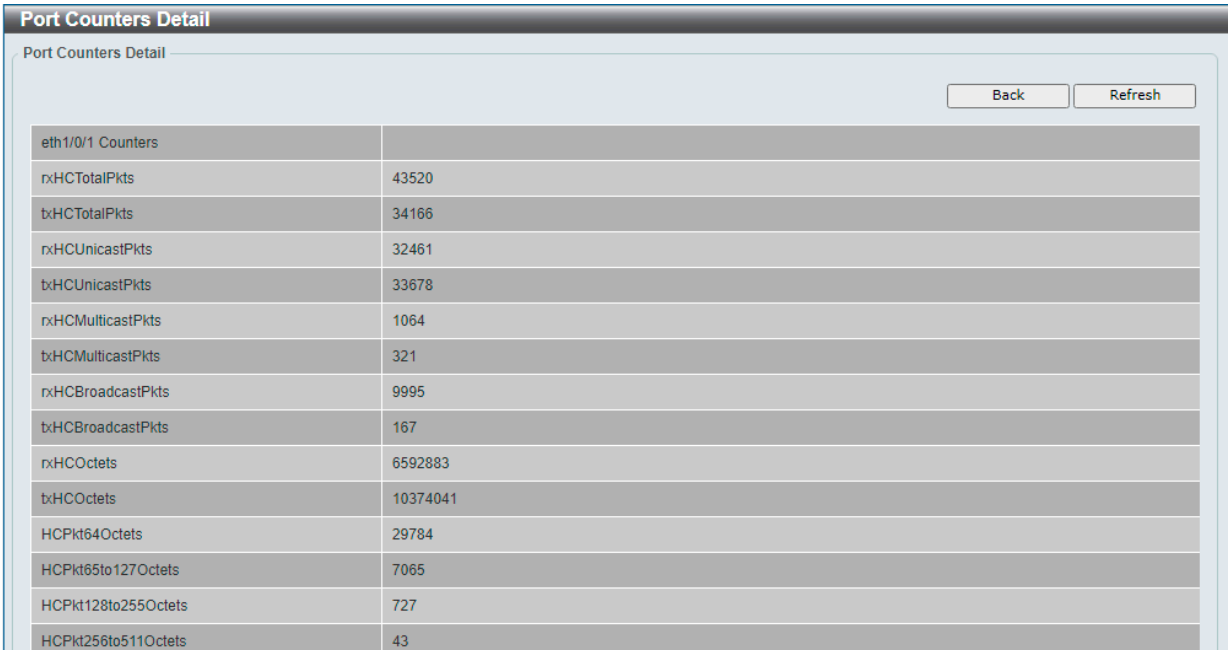


図 14-14　Port Counters Detail 画面

「Refresh」をクリックし、テーブルを更新します。
「Back」をクリックし、前の画面に戻ります。

注意　rxCRCAlignErrrors の表示はサポートされません。

Mirror Settings（ミラー設定）

ミラーリング機能の設定を行います。
本スイッチは、対象ポートで送受信するフレームをコピーして、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、最初のポートを通過したパケットの詳細を確認することができます。トラブルシューティングやネットワーク監視の目的に適しています。

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

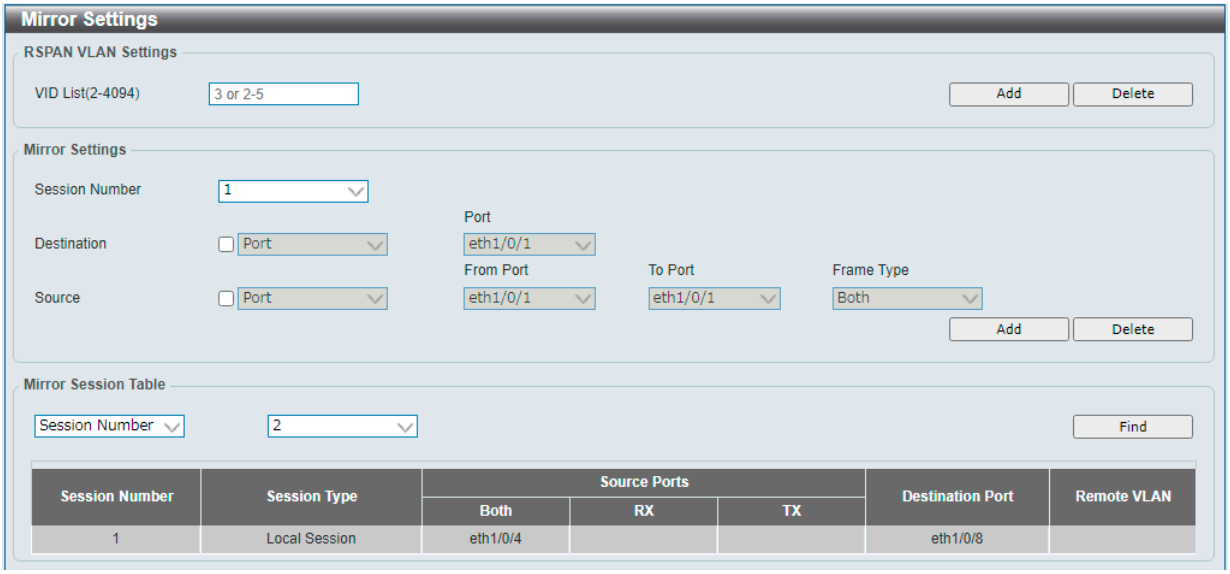


図 14-15　Mirror Settings 画面

画面に表示される項目：

項目	説明
RSPAN VLAN Settings	
VID List	VLAN ID 範囲を入力します。 • 設定可能範囲：2 - 4094
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 - 2
Destination	チェックボックスを選択して、ポートミラーエントリの宛先を設定します。 • 宛先タイプオプションの選択肢：「Port」「Remote VLAN」 - 「Remote VLAN」：宛先タイプオプションとして「Remote VLAN」を選択した場合、VLAN ID を指定します。 - 「Port」：ポート番号を指定します。
Source	チェックボックスを選択して、このポートミラーエントリの送信元を設定します。 • 送信元タイプオプションの選択肢：「Port」「Remote VLAN」 - 「Remote VLAN」：宛先タイプオプションとして「Remote VLAN」を選択した場合、VLAN ID を指定します。 - 「From Port / To Port」：宛先タイプオプションとして「Port」を選択した場合、ポート範囲を指定します。 - 「Frame Type」：宛先タイプオプションとして「Port」を選択した場合、フレームの種類を「Both」（両方）、「RX」（受信データ）、「TX」（送信データ）から指定します。
Mirror Session Table	
表示するエントリのタイプ、セッション番号を指定します。 • 「All Session」- テーブル内のすべてのミラーセッションを表示します。 • 「Session Number」- 指定したミラーセッションのみを表示します。ミラーセッション番号（1-2）を選択します。	

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

第 15 章　Green（省電力テクノロジー）

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）	スイッチの省電力設定を行います。
EEE（Energy Efficient Ethernet/ 省電力イーサネット）	Energy Efficient Ethernet/ 省電力イーサネットの設定を行います。

Power Saving（省電力）

スイッチの省電力機能を設定、表示します。

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

■ Power Saving Global Settings タブ

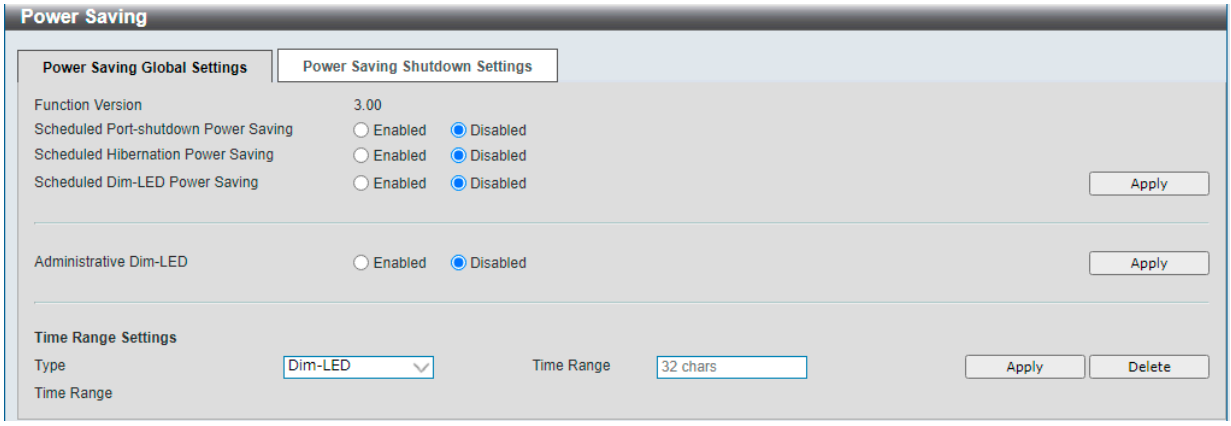


図 15-1　Power Saving 画面 - Power Saving Global Settings タブ

画面に表示される項目：

項目	説明
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を有効 / 無効に設定します。
Scheduled Hibernation Power Saving	スケジュールによるシステムスリープ機能を有効 / 無効に設定します。 システムが休止モードになると、スイッチは低電力状態になり、アイドル状態になります。すべてのポートと LED がシャットダウンし、すべてのネットワーク機能が無効になります。
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	LED 減光機能の有効 / 無効を指定します。
Time Range Settings	
Type	省電力モードの種類を指定します。 • 選択肢：「Dim-LED」「Hibernation」
Time Range	上記省電力機能に適用するスケジュールを指定します。

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

■ Power Saving Shutdown Settings タブ

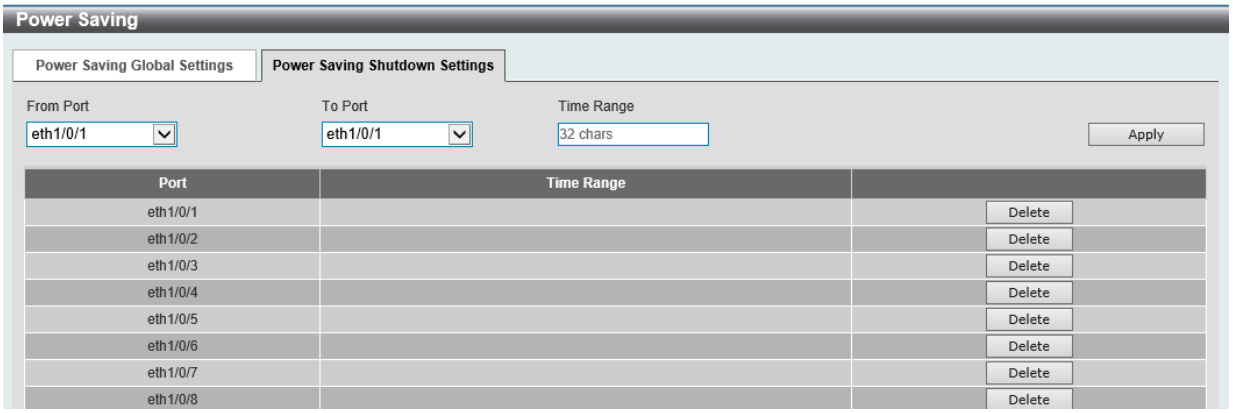


図 15-2　Power Saving - Power Saving Shutdown Settings タブ画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Time Range	ポートに適用するスケジュール名を指定します。

「Apply」をクリックして、設定内容を適用します。画面は自動的に更新されます。
「Delete」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 の順にクリックし、以下の設定画面を表示します。

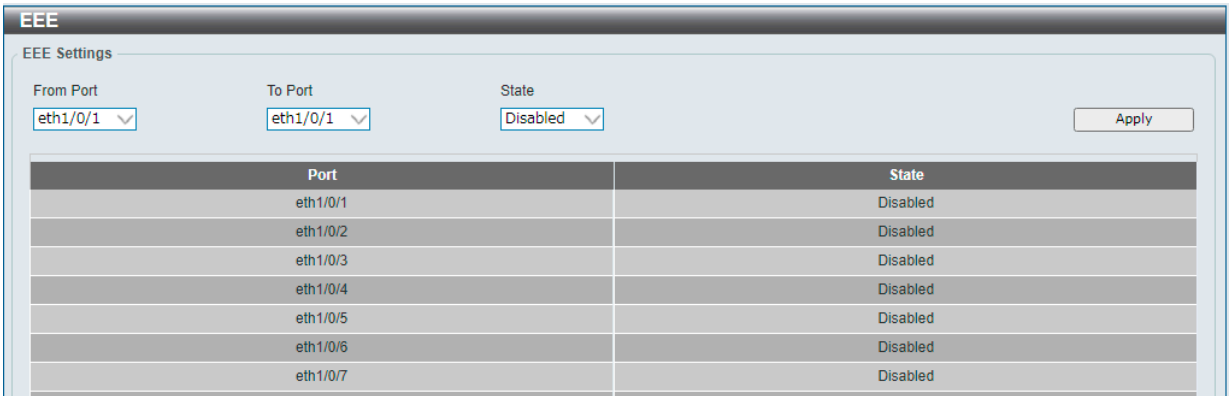


図 15-3　EEE 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポート範囲を指定します。
State	本機能を有効 / 無効に指定します。

「Apply」をクリックし、設定を適用します。

注意　EEE 有効化 / 無効化時、一時的にポートがリンクダウンします。

注意　SFP+ スロットでは利用できません。

注意　オートネゴシエーションが無効のポートでは、EEE はサポートされません。

第 16 章　Toolbar（ツールバー）

Web インタフェース画面上部のツールバーにある「Save」「Tools」「Wizard」「Online Help」「Logout」メニューを使用してスイッチの管理・設定を行います。

以下は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。

メニュー	サブメニュー	説明
Save（保存）	—	コンフィグレーションをスイッチに保存します。
Tools（ツール）	Firmware Information	ファームウェア情報を表示します。
	Configuration Information	コンフィグレーション情報を表示します。
	Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）	ファームウェアのアップグレードとバックアップを行います。
	Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）	コンフィグレーションのリストアとバックアップを行います。
	Log Backup（ログのバックアップ）	ログファイルのバックアップをします。
	Ping	Ping を実行します。
	Trace Route（トレースルート）	トレースルートを実行します。
	Reboot System（システム再起動）	システムの再起動を行います。
	Nuclias Connect Setting（Nuclias Connect 設定）	Nuclias Connect の設定を行います。
	Upload Nuclias Connect File（Nuclias Connect ファイルのアップロード）	Nuclias Connect のファイルをアップロードします。
Wizard（ウィザード）	—	スマートウィザードを開始します。
Online Help（オンラインヘルプ）	D-Link Support Site（D-Link サポート Web サイト（英語））	D-Link サポートサイト（英語版）を表示します
	User Guide（ユーザガイド（英語版））	ユーザガイド（英語版）を表示します。
Logout（ログアウト）	—	ログアウトします。

図 16-1　Toolbar

Save（保存）

現在のコンフィグレーションを保存します。

Save Configuration（コンフィグレーションの保存）

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

コンフィグレーションの保存

現在実行中のコンフィグレーションをブートコンフィグとしてスイッチに保存します。
電源が落ちた場合にコンフィグレーションが失われることを防ぎます。

図 16-2　Save Configuration 画面

画面に表示される項目：

項目	説明
Destination	コンフィグレーションの保存先を指定します。 • 選択肢：「Config 1」「Config 2」 「startup-config」にチェックを入れると、保存先としてブートコンフィグが指定されます。

「Apply」をクリックしてコンフィグレーションを保存します。

Tools（ツール）

Firmware Information（ファームウェア情報）

2 つのファームウェアイメージを表示します。起動中のイメージと、次回の起動用に選択されたイメージを確認することができます。

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

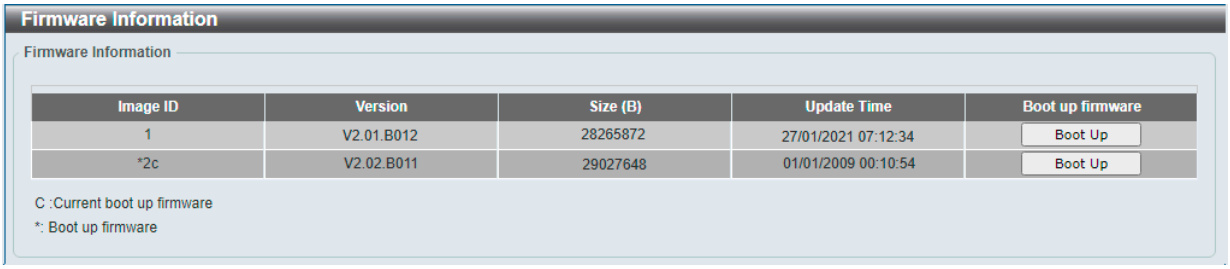


図 16-3　Firmware Information 画面

「Boot Up」をクリックして、次回の起動時に適用するイメージに指定します。

注意　"show boot" コマンドは、現在の起動ファイルを表示します。起動ファイルを変更した場合、このコマンドでは設定変更後のファイルを確認することはできません。

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

スイッチのコンフィグレーション情報を表示します。現在のコンフィグレーションと、次回の起動用に選択されたコンフィグレーションを確認することができます。

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

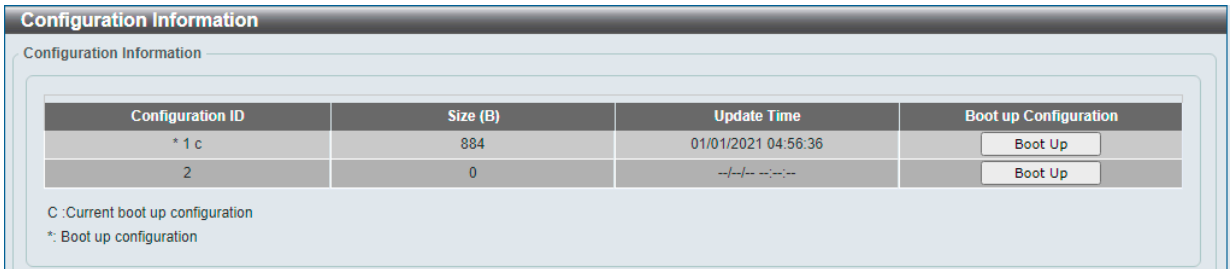


図 16-4　Configuration Information 画面

「Boot Up」をクリックして、次回の起動時に適用するコンフィグレーションに指定します。

注意　"show boot" コマンドは、現在の起動ファイルを表示します。起動ファイルを変更した場合、このコマンドでは設定変更後のファイルを確認することはできません。

注意　"show running configuration" コマンドで表示されるファイルサイズが実際のサイズとは異なる場合があります。

注意　本画面の「Configuration Information」で表示されるサイズは圧縮ファイルのサイズとなり、ダウンロード時のファイルサイズとは異なります。

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

Firmware Upgrade from HTTP（HTTP を使用したファームウェアアップグレード）

HTTP を使用してローカル PC からファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP をクリックし、設定画面を表示します。

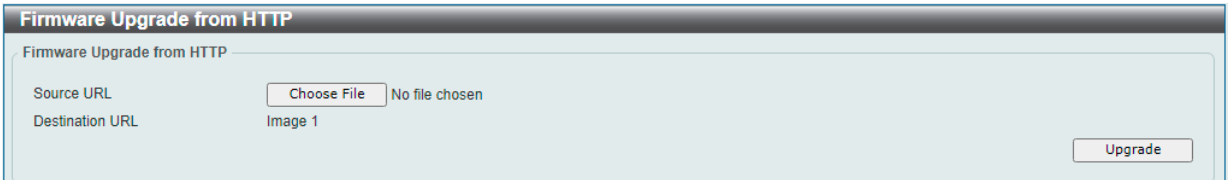


図 16-5　Firmware Upgrade from HTTP 画面

画面に表示される項目：

項目	説明
Source URL	「Choose File」をクリックし、ローカル PC 上のファームウェアファイルを指定します。

「Upgrade」をクリックしてアップグレードを開始します。

注意　アップロードしたファームウェアを適用するには、Bootup に指定し、再起動する必要があります。

Firmware Upgrade from TFTP（TFTP を使用したファームウェアアップグレード）

TFTP サーバを使用してファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP をクリックし、設定画面を表示します。

図 16-6　Firmware Upgrade from 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。
Source URL	TFTP サーバ上にあるファームウェアのファイル名を入力します。（64 文字以内）

「Upgrade」をクリックしてアップグレードを開始します。

注意　アップロードしたファームウェアを適用するには、Bootup に指定し、再起動する必要があります。

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

HTTP を使用して、ローカル PC へファームウェアのバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP をクリックし、設定画面を表示します。

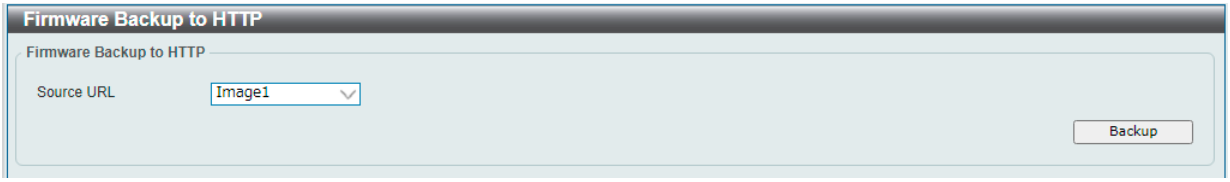


図 16-7　Firmware Backup to HTTP 画面

画面に表示される項目：

項目	説明
Source URL	ローカル PC にバックアップするファームウェアを選択します。 • 選択肢：「Image1」「Image2」

「Backup」をクリックしてバックアップを開始します。

注意　HTTPS 接続による WebUI 経由のファームウェアバックアップは未サポートです。

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

TFTP サーバにファームウェアバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP をクリックし、設定画面を表示します。

図 16-8　Firmware Backup to TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source	TFTP サーバにバックアップするファームウェアを選択します。 • 選択肢：「Image 1」「Image 2」
Destination URL	ここで指定したファイル名で TFTP サーバに保存されます。（64 文字以内）

「Backup」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 からコンフィグレーションのリストア）

HTTP を使用してローカル PC からコンフィグレーションをリストアします。

Tools > Configuration Restore & Backup > Configuration Restore from HTTP をクリックし、設定画面を表示します。

図 16-9　Configuration Restore from HTTP 画面

画面に表示される項目：

項目	説明
Source URL	「Choose File」をクリックし、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	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。 • 「Config 1」-「Configuration 1」を指定します。 • 「Config 2」-「Configuration 2」を指定します。 「startup-config」にチェックを入れると、スタートアップコンフィグレーションファイルが上書きされます。

「Restore」をクリックしてコンフィグレーションのリストアを開始します。

注意　コンフィグレーションのリストア時、WebUI/CLI 共に「running-config」を指定することはできません。

- 現在のコンフィグとは別の ID を指定してリストアを実施した場合、次回のブート ID を指定し直す必要があります。
- システム再起動時に、現在の設定を保存するオプションを指定せずに再起動すると、リストアした設定が適用されます。

Configuration Restore from TFTP（TFTP サーバからコンフィグレーションのリストア）

TFTP サーバからコンフィグレーションをリストアします。

Tools > Configuration Restore & Backup > Configuration Restore from TFTP をクリックし、設定画面を表示します。

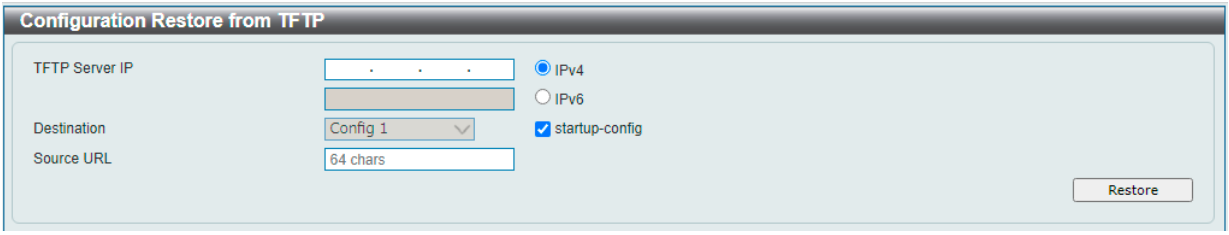


図 16-10　Configuration Restore from TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Destination	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 / ファイル名を指定します。 • 「Config 1」-「Configuration 1」を指定します。 • 「Config 2」-「Configuration 2」を指定します。 「startup-config」にチェックを入れると、スタートアップコンフィグレーションファイルが上書きされます。
Source URL	TFTP サーバに保存されているコンフィグレーションのファイル名を入力します。（64 文字以内）

「Restore」をクリックしてコンフィグレーションのリストアを開始します。

注意　コンフィグレーションのリストア時、WebUI/CLI 共に「running-config」を指定することはできません。

- 現在のコンフィグとは別の ID を指定してリストアを実施した場合、次回のブート ID を指定し直す必要があります。
- システム再起動時に、現在の設定を保存するオプションを指定せずに再起動すると、リストアした設定が適用されます。

Configuration Backup to HTTP（HTTP を使用したコンフィグレーションバックアップ）

HTTP を使用して、ローカル PC へコンフィグレーションバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to HTTP をクリックし、設定画面を表示します。

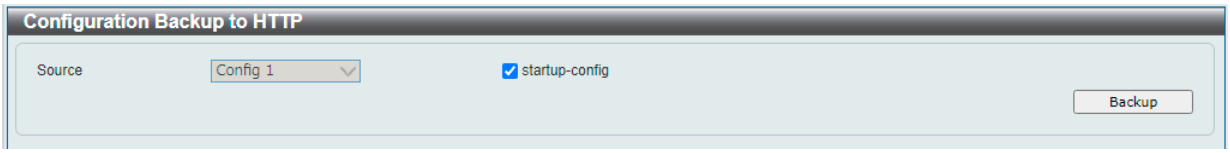


図 16-11　Configuration Backup to HTTP 画面

画面に表示される項目：

項目	説明
Source File	ローカル PC にバックアップするコンフィグレーションファイルを選択します。 • 「Config 1」-「Configuration 1」を指定します。 • 「Config 2」-「Configuration 2」を指定します。 「startup-config」にチェックを入れると、スタートアップコンフィグレーションファイルが指定されます。

「Backup」をクリックしてバックアップを開始します。

注意 コンフィグレーションのバックアップ時、WebUI では「running-config」を指定することはできません（CLI は可）。設定を変更した場合は「Save Configuration」から設定の保存を行ってください。

Configuration Backup to TFTP（TFTP を使用したコンフィグレーションバックアップ）

TFTP サーバにコンフィグレーションバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to TFTP をクリックし、設定画面を表示します。

図 16-12　Configuration 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。
Source	TFTP サーバにバックアップするコンフィグレーションファイルを選択します。 • 「Configuration 1」-「Config 1」を指定します。 • 「Configuration 2」-「Config 2」を指定します。 「startup-config」にチェックを入れると、スタートアップコンフィグレーションファイルが指定されます。
Destination URL	ここで指定したファイル名で TFTP サーバに保存されます。（64 文字以内）

「Backup」をクリックしてバックアップを開始します。

注意 コンフィグレーションのバックアップ時、WebUI では「running-config」を指定することはできません（CLI は可）。設定を変更した場合は「Save Configuration」から設定の保存を行ってください。

Log Backup（ログのバックアップ）

Log Backup to HTTP（HTTP を使用したログのバックアップ）

HTTP を使用してローカル PC へのシステムログのバックアップを行います。

Tools > Log Backup > Log Backup to HTTP をクリックし、設定画面を表示します。

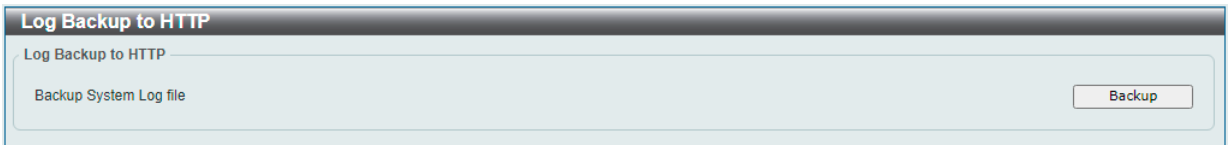


図 16-13　Log Backup to HTTP 画面

「Backup」をクリックしてバックアップを開始します。

Log Backup to TFTP（TFTP を使用したログのバックアップ）

TFTP サーバへのシステムログのバックアップを行います。

Tools > Log Backup > Log Backup to TFTP をクリックし、設定画面を表示します。

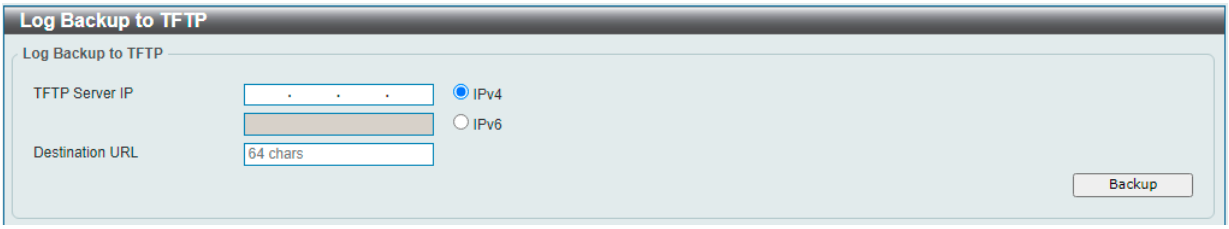


図 16-14　Log Backup to TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Destination URL	ここで指定したファイル名で TFTP サーバに保存されます。（64 文字以内）

「Backup」をクリックしてバックアップを開始します。

注意　TFTP のログバックアップにおいて、送信エラーになる場合があります。

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。ネットワーク上のスイッチと機器の接続状況を確認するうえで非常に有効です。

Tools > Ping をクリックし、設定画面を表示します。

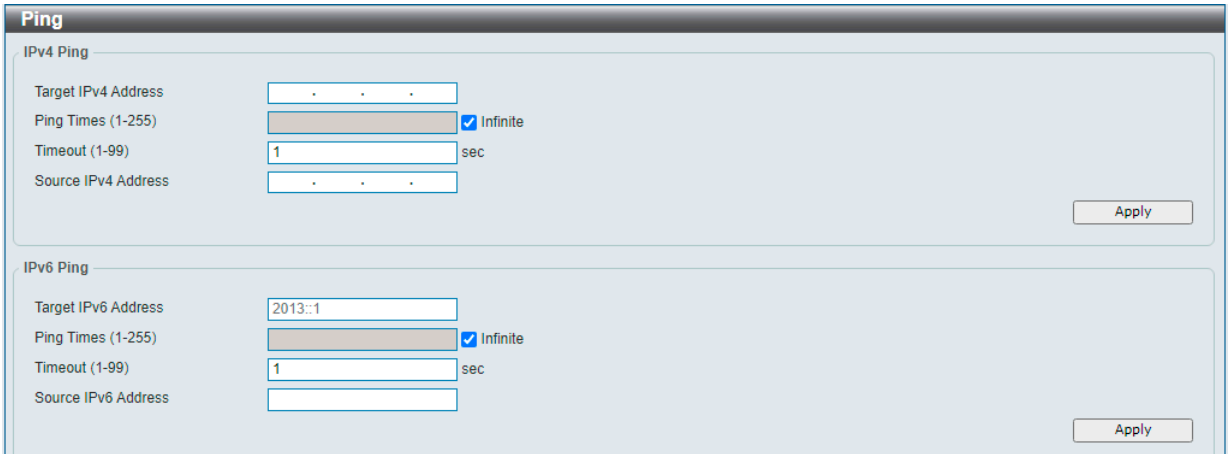


図 16-15　Ping 画面

画面に表示される項目：

項目	説明
IPv4 Ping	
Target IPv4 Address	Ping の送信先となる IPv4 アドレスを入力します。
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）
Source IPv4 Address	送信元 IPv4 アドレスを入力します。 スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。入力した IPv4 アドレスは、リモートホストに送信されるパケットの送信元 IP アドレスまたはプライマリ IP アドレスとして使用されます。
IPv6 Ping	
Target IPv6 Address	Ping の送信先となる IPv6 アドレスを入力します。
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）
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。

「Apply」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。

以下のように結果が表示されます。

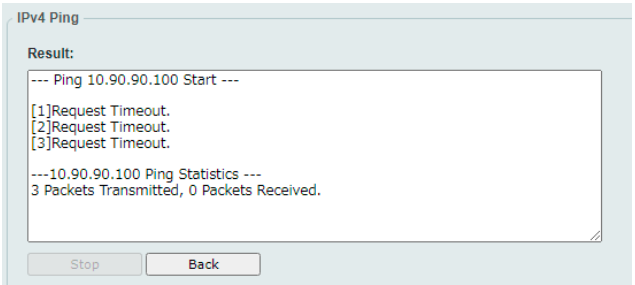


図 16-16　IPv4 Ping Result 画面

「Stop」をクリックして、Ping テストを停止します。
「Back」をクリックして、前の画面に戻ります。

Trace Route（トレースルート）

ネットワークとホスト間のルートをトレースします。

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

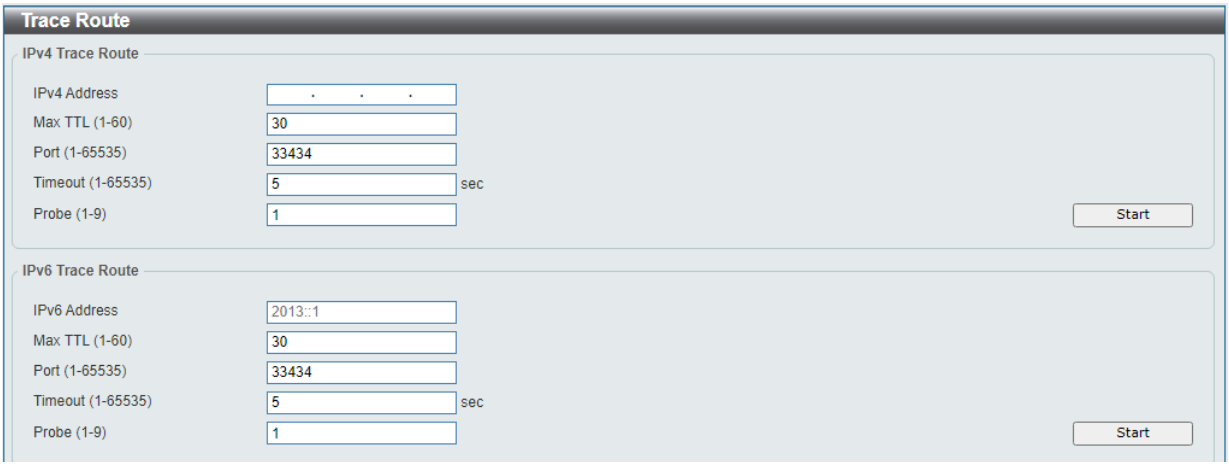


図 16-17　Trace Route 画面

画面に表示される項目：

項目	説明
IPv4 Trace Route	
IPv4 Address	宛先 IPv4 アドレスを入力します。
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 - 60
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）
Probe Number	プローブ数を指定します。 • 設定可能範囲：1 - 9
IPv6 Trace Route	
IPv6 Address	宛先 IPv6 アドレスを入力します。
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 - 60
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）
Probe Number	プローブ数を指定します。 • 設定可能範囲：1 - 9

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

以下の結果画面が表示されます。

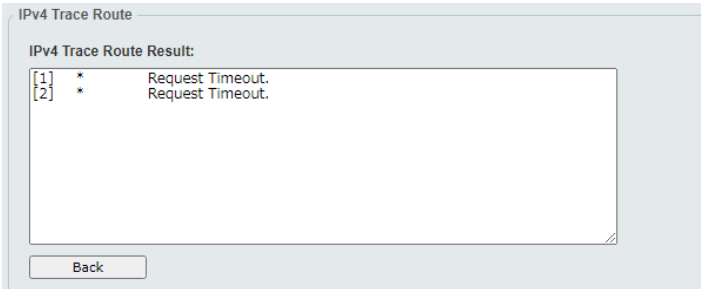


図 16-18　IPv4 Trace Route Result 画面

「Back」ボタンをクリックして、前の画面に戻ります。

注意　ARP パケットを多数受信した際にトレースルートの結果が正しく表示されない場合があります。

Reset（リセット）

スイッチの設定内容を工場出荷時状態に戻します。

Tools > Reset をクリックし、次の設定画面を表示します。

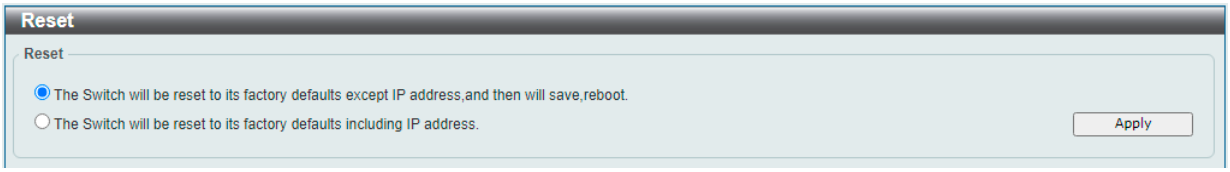


図 16-19　Reset 画面

画面に表示される項目：

項目	説明
The Switch will be reset to its factory defaults except IP address,and then will save,reboot.	スイッチを工場出荷時設定にリセットして、保存、再起動を実行します。（IP アドレスは除く）
The Switch will be reset to its factory defaults including IP address.	スイッチを工場出荷時設定にリセットして、保存、再起動を実行します。（IP アドレスを含む）

「Apply」をクリックして、リセットを開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

図 16-20　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?	スイッチが再起動する前に現在の設定を保存するかどうかを指定します。 • 「Yes」- 再起動する前に現在の設定を保存します。 • 「No」- 再起動する前に現在の設定を保存しません。保存していない設定は破棄され、最後に保存した時の設定が使われます。
Destination	コンフィグレーションの保存先を選択します。 「startup-config」にチェックを入れると、スタートアップコンフィグレーションファイルが指定されます。

「Reboot」をクリックして再起動を開始します。

再起動後、ログイン画面が表示されます。

Nuclias Connect Setting（Nuclias Connect 設定）

Nuclias Connect は、中小企業向けの D-Link の一元管理ソリューションです。Nuclias Connect を使用することで、ネットワークの分析、自動化、設定、最適化、拡張、セキュリティ保護が容易になり、企業ネットワークの包括的な管理ソリューションを実現します。

注意　Nuclias Connect によるスイッチ管理は未サポートです。

Tools > Nuclias Connect Setting をクリックし、以下の設定画面を表示します。

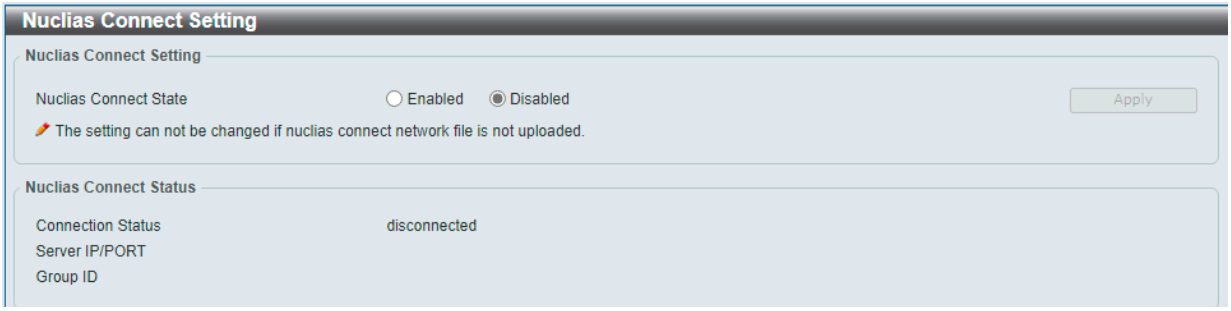


図 16-21　Nuclias Connect Setting 画面

画面に表示される項目：

項目	説明
Nuclias Connect Setting	
Nuclias Connect State	Nuclias Connect ステータスを有効 / 無効に設定します。
Nuclias Connect Status	
Connection Status	Nuclias Connect との接続ステータスが表示されます。
Server IP/PORT	サーバ IP およびポートが表示されます。
Group ID	グループ ID が表示されます。

「Apply」をクリックして、設定内容を適用します。

Upload Nuclias Connect File（Nuclias Connect ファイルのアップロード）

Nuclias Connect でエクスポートしたプロファイルをアップロードすることで、アクセスポイントを Nuclias Connect の管理対象として追加することができます。

注意　Nuclias Connect によるスイッチ管理は未サポートです。

Tools > Upload Nuclias Connect Network File をクリックし、以下の設定画面を表示します。

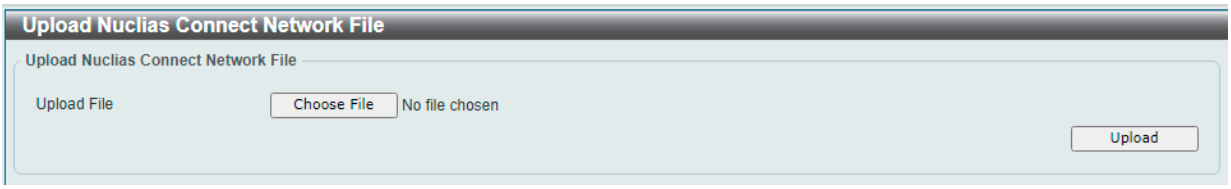


図 16-22　Upload Nuclias Connect Network File 画面

画面に表示される項目：

項目	説明
Upload File	「Choose File」をクリックし、アップロードする Nuclias Connect ネットワークファイルを指定します。

「Upload」をクリックして、ファイルをアップロードします。

Wizard（ウィザード）

クリックするとスマートウィザードを開始します。詳しくは「Smart Wizard 設定」を参照ください。

Online Help（オンラインヘルプ）

D-Link Support Site（D-Link サポート Web サイト（英語））

クリックすると D-Link のサポート Web サイト（英語）へ接続します。インターネット接続が必要です。

User Guide（ユーザガイド（英語版））

ユーザガイド（英語版）を表示します。インターネット接続が必要です。

Logout（ログアウト）

クリックするとログアウトします。

【付録 A】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のメッセージについて説明します。

Critical（重大）、Warning（警告）、Informational（情報）

ログの内容		緊急度	イベントの説明
802.1X			
1	802.1X authentication fails from (Username: <username>, Port: <interface-id>, MAC: <mac-address>) **パラメータ説明：** • username：認証ユーザ名 • interface-id：インタフェース番号 • mac-address：認証デバイスの MAC アドレス	Warning	802.1X 認証に失敗しました。
2	802.1X authentication succeeds from (Username: <username>, Port: <interface-id>, MAC: <mac-address>) **パラメータ説明：** • username：認証ユーザ名 • interface-id：インタフェース番号 • mac-address：認証デバイスの MAC アドレス	Informational	802.1X 認証に成功しました。
AAA			
1	Invalid VLAN assignment by radius with VLAN <vid>, port <interface-id> **パラメータ説明：** • vid：RADIUS サーバにより認証された不正な 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	Warning	RADIUS が不正な VLAN ID 属性を割り当てました。
2	Invalid port default 802.1p assignment by RADIUS with 802.1p: <priority>, port < interface -id> **パラメータ説明：** • priority：RADIUS サーバにより認証された不正なプライオリティ割り当て • interface–id：認証されたクライアントのポート番号	Warning	RADIUS が不正なプライオリティ属性を割り当てました。
3	Invalid bandwidth assignment by RADIUS with type <direction> rate <threshold>, port <interface -id> **パラメータ説明：** • direction：帯域制御の方向（TX/RX） • threshold：RADIUS サーバにより認証された不正な帯域しきい値割り当て • interface–id：認証されたクライアントのポート番号	Warning	RADIUS が不正な帯域属性を割り当てました。
4	The port <interface -id> is set to 802.1X mac based. It does not support radius assignment. **パラメータ説明：** • interface–id：ホストモードがマルチ認証モードのポート番号	Warning	802.1X MAC ベース（ホストモードがマルチ認証）のポートに対して RADIUS 割り当てが要求されました。
5	The port ethernet <interface -id> is set to a router port of IGMP snooping. it does not support radius assignment. **パラメータ説明：** • interface–id：IGMP スヌーピングルータポートのポート番号	Warning	IGMP スヌーピングルータポートに対して RADIUS 割り当てが要求されました。
Configuration/Firmware/Log			
1	Firmware upgraded successfully via <session>! **パラメータ説明：** • session：ユーザのセッション	Informational	ファームウェアのアップグレードに成功しました。
2	Firmware upgrade failure via <session>! **パラメータ説明：** • session：ユーザのセッション	Warning	ファームウェアのアップグレードに失敗しました。

ログの内容		緊急度	イベントの説明
3	Firmware backup successful via <session> **パラメータ説明：** • session：ユーザのセッション	Informational	ファームウェアのバックアップに成功しました。
4	Firmware backup failure via <session>! **パラメータ説明：** • session：ユーザのセッション	Warning	ファームウェアのバックアップに失敗しました。
5	Configuration restore successful via <session> **パラメータ説明：** • session：ユーザのセッション	Informational	コンフィグレーションのリストアに成功しました。
6	Configuration restore failure via <session>! **パラメータ説明：** • session：ユーザのセッション	Warning	コンフィグレーションのリストアに失敗しました。
7	Configuration backup successful via <session>. **パラメータ説明：** • session：ユーザのセッション	Informational	コンフィグレーションのバックアップに成功しました。
8	Configuration backup failure via <session>! **パラメータ説明：** • session：ユーザのセッション	Warning	コンフィグレーションのバックアップに失敗しました。
9	Configuration save successful.	Informational	コンフィグレーションの保存に成功しました。
10	Configuration save failure.	Warning	コンフィグレーションの保存に失敗しました。
11	System log backup successful via <session>. **パラメータ説明：** • session：ユーザのセッション	Informational	システムログのバックアップに成功しました。
12	System log backup failure via <session>! **パラメータ説明：** • session：ユーザのセッション	Warning	システムログのバックアップに失敗しました。
	Interface		
1	Port <port-type>< interface-id> link down. **パラメータ説明：** • port-type：ポートタイプ • interface-id：インタフェース名	Informational	ポートがリンクダウンしました。
2	Port <port-type>< interface-id> link up, <link-speed>. **パラメータ説明：** • port-type：ポートタイプ • interface-id：インタフェース名 • link-speed：ポートのリンクスピード	Informational	ポートがリンクアップしました。
	LACP		
1	Trunk group< group_id > link up. **パラメータ説明：** • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクアップしました。
2	Trunk group< group_id > link down. **パラメータ説明：** • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクダウンしました。

ログの内容		緊急度	イベントの説明
3	Port <port_id> attach to Trunk group<group_id >. **パラメータ説明：** • port_id：アグリゲーショングループにアタッチされたポート ID • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループにアタッチしました。
4	Port <port_id> detach from Trunk group< group_id >. **パラメータ説明：** • port_id：アグリゲーショングループからデタッチされたポート ID • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループからデタッチしました。
LBD（ループバック検知）			
1	Port <interface-id> LBD loop occurred. Port blocked. **パラメータ説明：** • interface-id：ループが検知されたインタフェース	Critical	ポートベースモードでループバックが検出されました。
2	Port <interface-id> LBD loop occurred. Port blocked at VID <vlan-id>. **パラメータ説明：** • interface-id：ループが検知されたインタフェース • vlan-id：ループが検知された VLAN	Critical	VLAN ベースモードでループバックが検出されました。
3	Port <interface-id> LBD loop recovered. Loop detection restarted. **パラメータ説明：** • interface-id：ループから回復したインタフェース	Informational	ポートベースモードでループバックから回復しました。
4	Port <interface-id> LBD Port at VID <vlan-id> recovered. Loop detection restarted. **パラメータ説明：** • interface-id：ループから回復したインタフェース • vlan-id：ループから回復した VLAN	Informational	VLAN ベースモードでループバックからポートが回復しました。
5	Port <interface-id> LBD loop occurred. Port not blocked as a result of NONE action mode. **パラメータ説明：** • interface-id：ループが検知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が、アクションが「None」に設定されているためポートはブロックされません。
6	Port <interface-id> LBD port VID <vlan-id> loop occurred. Port not blocked as a result of NONE action mode. **パラメータ説明：** • interface-id：ループが検知されたインタフェース • vlan-id：ループが検知された VLAN	Critical	VLAN ベースモードでループバックが検出されましたが、アクションが「None」に設定されているためポートはブロックされません。
Login/Logout CLI			
1	Successful login through Telnet (User: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由のログインに成功しました。
2	Login failed through Telnet (IP: <ipaddr>) **パラメータ説明：** • ipaddr：クライアントの IP アドレス	Warning	Telnet 経由のログインに失敗しました。
3	Telnet session timed out (IP: <ipaddr>) **パラメータ説明：** • ipaddr：クライアントの IP アドレス	Informational	Telnet のセッションがタイムアウトしました。
4	Logout through Telnet (IP: <ipaddr>) **パラメータ説明：** • 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。

	ログの内容	緊急度	イベントの説明
	MSTP Debug Enhancement		
1	Spanning Tree Protocol is enabled.	Informational	スパニングツリープロトコル有効化
2	Spanning Tree Protocol is disabled.	Informational	スパニングツリープロトコル無効化
3	Topology changed (Instance: < Instance-id >, port: <interface_id>) **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンス（CIST）を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号	Informational	MSTP インスタンスのトポロジに変更がありました。
4	New Root bridge selected (MAC: <macaddr> Priority :< priority>) **パラメータ説明：** • macaddr：ブリッジの MAC アドレス • priority：ブリッジの優先値。4096 で割り切れる数値です。	Informational	新しいルートブリッジが選定されました。
5	Topology changed (port : <interface_id>) **パラメータ説明：** • interface-id：イベントを検知したポート番号	Informational	STP/RSTP のトポロジに変更がありました。
	Peripheral（周辺機器）		
1	Right Fan <fan-descr> back to normal. **パラメータ説明：** • fan-descr：ファンの ID と場所	Critical	ファンが回復しました。
2	Right Fan <fan-descr> failed. **パラメータ説明：** • fan-descr：ファンの ID と場所	Critical	ファンに異常があります。
3	Temperature exceeds the thresholds.	Critical	温度センサがアラーム状態に入りました。
4	Temperature recovered.	Critical	温度が正常な状態に回復しました。
	PoE		
1	PoE power usage threshold is exceed!	Informational	総電力の使用率がしきい値を超えました。
2	PoE Port {PORT} power short circuit! **パラメータ説明：** • {PORT}：イベントが発生したポート番号	Warning	ケーブルの短絡が検出されました。
3	PoE Port {PORT} power over load! **パラメータ説明：** • {PORT}：イベントが発生したポート番号	Warning	オーバーロードが検出されました。
4	PoE Port {PORT} power denied! **パラメータ説明：** • {PORT}：イベントが発生したポート番号	Warning	不具合により電力の供給が停止しました。
5	PoE Port {PORT.1} power thermal shutdown! **パラメータ説明：** • {PORT}：イベントが発生したポート番号	Warning	オーバーヒートにより電力の供給が停止しました。
6	PoE Port {PORT} power on! **パラメータ説明：** • {PORT}：イベントが発生したポート番号	Informational	PD への電力供給が開始されました。

ログの内容		緊急度	イベントの説明
7	PoE Port {PORT} power off! **パラメータ説明：** • {PORT}：イベントが発生したポート番号	Informational	PD への電力供給が停止されました。
8	PoE Port {PORT} classfication failed! **パラメータ説明：** • {PORT}：イベントが発生したポート番号	Informational	PD の識別ができません。
9	PoE over max power budget!	Informational	総使用電力が供給可能電力を超えました。
	Port Security		
1	Port security violation (Port:<interface-id>). **パラメータ説明：** • interface-id：インタフェース名	Warning	ポート上のアドレス最大数を超過しています。
2	The limit on system entry number has been exceeded.	Warning	システム上のアドレス最大数を超過しています。
	SNMP		
1	SNMP request received with invalid <string>. **パラメータ説明：** • string:：無効なコミュニティ名またはセキュリティモデル	Warning	SNMP リクエストで無効なコミュニティ文字列を受信しました。
	Storm Control		
1	<broadcast | multicast | unicast> storm is occurring on <interface-id>. **パラメータ説明：** • broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • multicast：未知 / 既知の L2 マルチキャスト、未知 / 既知の IP マルチキャストを含むマルチキャストパケットによるストーム • unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストームが発生しているインタフェース ID	Warning	ストームが発生しました。
2	<interface-id> is currently shutdown due to the <broadcast | multicast | unicast> storm. **パラメータ説明：** • interface-id：ストームによりエラー無効状態になったインタフェース ID • broadcast：ブロードキャストストームによるエラー無効状態 • multicast：マルチキャストストームによるエラー無効状態 • unicast:ユニキャストストーム（既知と未知のユニキャスト（DLF）パケットを含む）によるエラー無効状態	Warning	パケットストームによりポートがシャットダウンしました。
	Telnet		
1	Successful login through Telnet (User: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet サーバへのログインユーザ名 • ipaddr：Telnet クライアントの IP アドレス	Informational	Telnet 経由のログインに成功しました。
2	Login failed through Telnet (IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス	Warning	Telnet 経由のログインに失敗しました。
3	Logout through Telnet (IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントのアドレス	Informational	Telnet からログアウトしました。
4	Telnet session timed out (IP: <ipaddr>). **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス	Informational	Telnet セッションがタイムアウトしました。

	ログの内容	緊急度	イベントの説明
	Web		
1	Successful login through Web (IP: <ipaddr>). **パラメータ説明：** • 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。
2	Login failed through Web (IP: <ipaddr>). **パラメータ説明：** • 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。
3	Logout through Web (IP: <ipaddr>). **パラメータ説明：** • 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。

【付録 B】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について説明します。

	トラップ名	説明	OID
802.1X			
1	pnacAuthNotifyAuthSuccess	ホストが 802.1X 認証に成功したときにトラップが送信されます。（ログインに成功） 関連オブジェクト： (1) networkPortAuthPortNumber (2) networkPortAuthVlan (3) networkPortAuthMac (4) networkPortAuthUserName	1.3.6.1.4.1.171.10.139.1.1.8.2.7.0.1
2	pnacAuthNotifyAuthFailure	ホストが 802.1X 認証に失敗したときにトラップが送信されます。（ログインに失敗） 関連オブジェクト： (1) networkPortAuthPortNumber (2) networkPortAuthVlan (3) networkPortAuthMac (4) networkPortAuthUserName (5) networkPortAuthFailReason	1.3.6.1.4.1.171.10.139.1.1.8.2.7.0.2
DHCP Server Screen Prevention			
1	dhcpSerScrAttackDetect	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、攻撃パケット受信時にイベントをトラップ検知します。 関連オブジェクト： (1) dhcpSerScrLogVlanID (2) dhcpSerScrLogIPAddr (3) dhcpSerScrLogMacAddr (4) dhcpSerScrLogOccurrence	1.3.6.1.4.1.171.10.139.1.1.8.7.3.0.1
ErrDisable			
1	errDisNotifyPortDisabledAssert	ポートがエラー無効モードになったときにトラップが送信されます。 関連オブジェクト： (1) errDisIfStatusPortIndex (2) errDisIfStatusVlanIndex (3) errDisPortReason	1.3.6.1.4.1.171.10.139.1.1.2.13.8.0.1
2	errDisNotifyPortDisabledClear	指定時間後にポートが復旧したときにトラップが送信されます。 関連オブジェクト： (1) errDisIfStatusPortIndex (2) errDisIfStatusVlanIndex (3) errDisPortReason	1.3.6.1.4.1.171.10.139.1.1.2.13.8.0.2
3	errDisNotifyVlanDisabledAssert	指定 VID のポートでループが発生したときにトラップが送信されます。 関連オブジェクト： (1) errDisIfStatusPortIndex (2) errDisIfStatusVlanIndex (3) errDisPortReason	1.3.6.1.4.1.171.10.139.1.1.2.13.8.0.3
4	errDisNotifyVlanDisabledClear	指定 VID のポートが再起動したときにトラップが送信されます。 関連オブジェクト： (1) errDisIfStatusPortIndex (2) errDisIfStatusVlanIndex (3) errDisPortReason	1.3.6.1.4.1.171.10.139.1.1.2.13.8.0.4

	トラップ名	説明	OID
		LACP	
1	linkUp	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、トラップが送信されます。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) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	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、トラップが送信されます。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) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3
		LBD	
1	lbdLoopOccur	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) lbdportIndex	1.3.6.1.4.1.171.10.139.1.1.4.4.4.0.1
2	lbdLoopRecover	指定時間後、インタフェースのループが解消したきに送信されます。 関連オブジェクト : (1) lbdportIndex	1.3.6.1.4.1.171.10.139.1.1.4.4.4.0.2
		LLDP/LLDP-MED Trap Name	
1	lldpRemoteTableChanged	「lldpStatsRemTableLastChangeTime」の値が変更された時にトラップが送信されます。NMS が LLDP リモートシステムテーブルのメンテナンスポーリングをトリガする際に使用することができます。 関連オブジェクト : (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.1
2	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トラップが送信されます。 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
3	lldpChasisIdMatched	設定された chasisID と隣接デバイスから受信した chasisID が同一の場合にトラップが送信されます。	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.2
4	lldpSystenameMatched	設定されたシステム名と隣接デバイスから受信したシステム名が同一の場合にトラップが送信されます。 関連オブジェクト : (1) lldpRemSysName	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.3
5	lldpManagementaddressMatched	設定された管理アドレスと隣接デバイスから受信した管理アドレスが同一の場合にトラップが送信されます。受信した重複アドレスは OID と一緒に送信されます。Value フィールドで「lldpRemManAddrIfId」が送信されます。 関連オブジェクト : (1) lldpRemManAddr	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.4

	トラップ名	説明	OID
6	lldpPVIDNotMatched	同じリンクに接続する２つのシステムのポート VLAN ID が異なる場合にトラップが送信されます。 関連オブジェクト : (1) lldpXdot1RemPortVlanId	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.5
7	lldpVlannameNotMatched	同じリンクに接続する２つのシステムの VLAN 名が異なる場合にトラップが送信されます。 関連オブジェクト : (1) lldpXdot1RemVlanName	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.6
8	lldpProtocolIDNotMatched	同じリンクに接続する２つのシステムのプロトコル識別情報（スパニングツリープロトコル、リンクアグリゲーションプロトコル、ベンダ固有プロトコルなど）が異なる場合にトラップが送信されます。 関連オブジェクト : (1) lldpXdot1RemProtocolId	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.7
9	lldpLAstatusNotMatched	同じリンクに接続する２つのシステムのリンクアグリゲーション構成が異なる場合にトラップが送信されます。 関連オブジェクト : (1) lldpXdot3RemLinkAggStatus	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.8
10	lldpMaxFrameSizeNotMatched	同じリンクに接続する２つのシステムの最大フレームサイズ設定が異なる場合にトラップが送信されます。 関連オブジェクト : (1) lldpXdot3RemMaxFrameSize	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.9
11	lldpMAUTypeNotMatched	同じリンクに接続する２つのシステムの Operational MauType が異なる場合にトラップが送信されます。 関連オブジェクト : (1) lldpXdot3RemPortOperMauType	1.3.6.1.4.1.171.10.139.1.1.4.7.12.0.10
		MSTP	
1	stpNewRootTrap	本トラップは、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、（Topology Change Timer の期限切れなどに伴い）新しいルートとして選出された後すぐにブリッジによって送信されます。 本トラップの実行はオプションです。 関連オブジェクト : (1) deviceInfoMACAddress (2) mstMstiBridgeRegionalRoot	1.3.6.1.4.1.171.10.139.1.1.4.3.6.0.1
2	stpTopologyChgTrap	本トラップは、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 stpNewRootTrap トラップが送信される場合には、本トラップは送信されません。 本トラップの実行はオプションです。 関連オブジェクト : (1) deviceInfoMACAddress (2) mstMstiTopChanges	1.3.6.1.4.1.171.10.139.1.1.4.3.6.0.2
		Peripheral	
1	envTrapFanFailed	ファンにエラーが発生したことを示します。 関連オブジェクト : (1) environmentFanId	1.3.6.1.4.1.171.10.139.1.1.2.2.6.0.1

トラップ名		説明	OID
2	envTrapFanRecover	ファンが回復したことを示します。 関連オブジェクト : (1) environmentFanId	1.3.6.1.4.1.171.10.139.1.1.2.2.6.0.2
3	envTrapTemperatureExceed	温度がしきい値を超えたことを示します。 関連オブジェクト : (1) environmentTempCurrent	1.3.6.1.4.1.171.10.139.1.1.2.2.6.0.3
4	envTrapTemperatureRecover	温度が回復したことを示します。 関連オブジェクト : (1) environmentTempCurrent	1.3.6.1.4.1.171.10.139.1.1.2.2.6.0.4
Port			
1	linkUp	ポートがリンクアップしたときに生成されます。 関連オブジェクト : (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	ポートがリンクダウンしたときに生成されます。 関連オブジェクト : (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3
Port Security			
1	portSecurityVioAction	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) portSecurityPort (2) portSecurityVioCount	1.3.6.1.4.1.171.10.139.1.1.8.1.2.1.1.4
RMON			
1	risingAlarm	SNMP トラップは、アラームエントリが上昇しきい値を超える時に生成され、イベントの設定に応じてトラップが送信されます。 関連オブジェクト : (1)alarmIndex (2)eventDescription (3)alarmVariable (4)alarmSampleType (5)alarmValue (6)alarmRisingThreshold	1.3.6.1.2.1.16.0.1
2	fallingAlarm	SNMP トラップは、アラームエントリが下降しきい値を下回るときに生成され、イベントの設定に応じてトラップが送信されます。 関連オブジェクト : (1)alarmIndex (2)eventDescription (3)alarmVariable (4)alarmSampleType (5)alarmValue (6)alarmFallingThreshold	1.3.6.1.2.1.16.0.2
Start			
1	coldStart	coldStart トラップは、エージェントロールで動作する SNMPv2 エンティティが、自身を再初期化したことを示します。設定が変更された可能性があります。	1.3.6.1.6.3.1.1.5.1
2	warmStart	warmStart トラップは、エージェントロールで動作する SNMPv2 エンティティが、自身を再初期化したことを示します。設定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

	トラップ名	説明	OID
Storm Control			
1	stormCtrlTrapsStormOccur	ストームが発生 / 検知されたときにトラップが送信されます。 関連オブジェクト : (1) stormCtrlIndex	1.3.6.1.4.1.171.10.139.1.1.8.16.1.1.6.0.1
2	stormCtrlTrapsStormClear	ポートでストームが解消したときにトラップが送信されます。 関連オブジェクト : (1) stormCtrlIndex	1.3.6.1.4.1.171.10.139.1.1.8.16.1.1.6.0.2

【付録 C】RADIUS 属性の割り当て指定

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」

以下の RADIUS 属性割り当てタイプについて説明します。
- 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

■ イングレス / イーグレス帯域幅

RADIUS サーバにより Ingress/Egress 帯域を割り当てるには、適切なパラメータが RADIUS サーバに設定されている必要があります。帯域幅のパラメータは以下の通りです。

ベンダ固有属性のパラメータ

ベンダ固有属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	2（イングレス帯域幅） 3（イーグレス帯域幅）	必須
Attribute-Specific Field	ポートの帯域幅の割り当てに使用します。	単位 (Kbits)	必須

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。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	ポートの 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

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。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、デバイスに設定されません。

■ 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	使用されるデータ転送媒体	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	ASCII（VID）	必須

【付録 D】IETF RADIUS 属性のサポート

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。

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 C】RADIUS 属性の割り当て指定」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、本スイッチでサポートされている IETF RADIUS 属性の一覧です。

RADIUS 認証属性

番号	IETF 属性
1	User-Name
2	User-Password
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
64	Tunnel-Type
65	Tunnel-Medium-Type
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID

【付録 E】ERPS 情報

本シリーズはソフトウェアベースの ERPS をサポートしています。（Fast Link Drop Interrupt 機能はサポートしていません）

製品名	ERPS	ポート 1-8	ポート 9-10
DXS-1210-10TS	ハードウェアベース	—	—
	ソフトウェアベース	○	○

製品名	ERPS	ポート 1-8	ポート 9-10
DXS-1210-10MP	ハードウェアベース	—	—
	ソフトウェアベース	○	○

製品名	ERPS	ポート 1-8	ポート 9-12
DXS-1210-12TC	ハードウェアベース	—	—
	ソフトウェアベース	○	○

製品名	ERPS	ポート 1-8	ポート 9-12
DXS-1210-12SC	ハードウェアベース	—	—
	ソフトウェアベース	○	○

【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-1210/B1

Traffic Segmentation（トラフィックセグメンテーション）

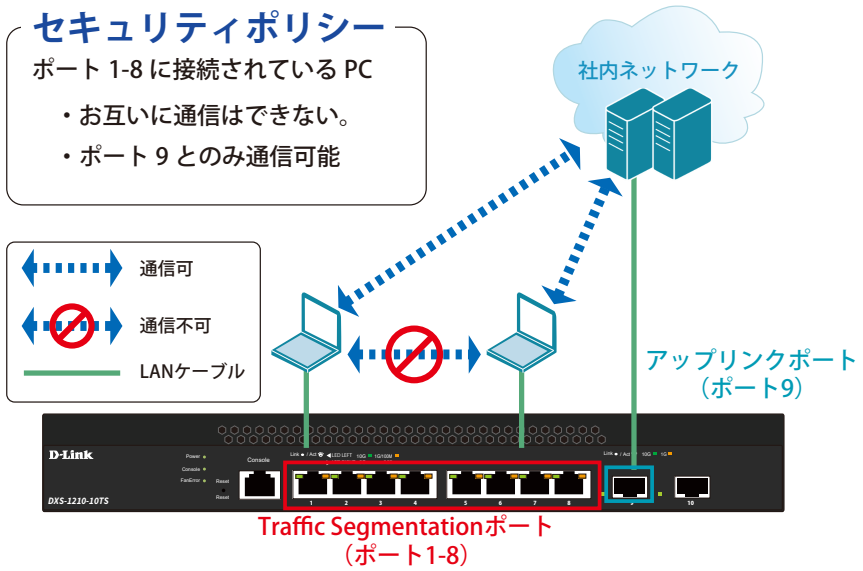


図 17-1　Traffic Segmentation（DXS-1210-10TS）

概要

ポート 1 - 8 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 - 8 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 - 8 は、アップリンクポートとして使用するポート 9 とのみ通信ができるようにします。

設定手順

1. ポート（1-8）のセキュリティ設定をします。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#traffic-segmentation forward interface ethernet 1/0/9
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。他ポートへのフラッディングを回避するために、ダウンリンクポートを対象に、ストームコントロール機能を用いて宛先 MAC アドレス不明の unknown ユニキャストパケットをドロップするよう設定を追加します。

3. （必要に応じて）ストームコントロール機能により、Unknown ユニキャストに閾値「0」を設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-10
Switch(config-if-range)#storm-control DLF level kbps 0
Switch(config-if-range)#storm-control action drop
Switch(config-if-range)#end
```

4. 設定を保存します。

```
Switch#copy running-config startup-config
Destination filename startup-config? [y/n]:y
```

5. 情報確認（ポート 1-8 の storm-control の unicast の設定と閾値を表示します。）

```
Switch#show storm-control interface ethernet 1/0/1-8 DLF
```

VLAN

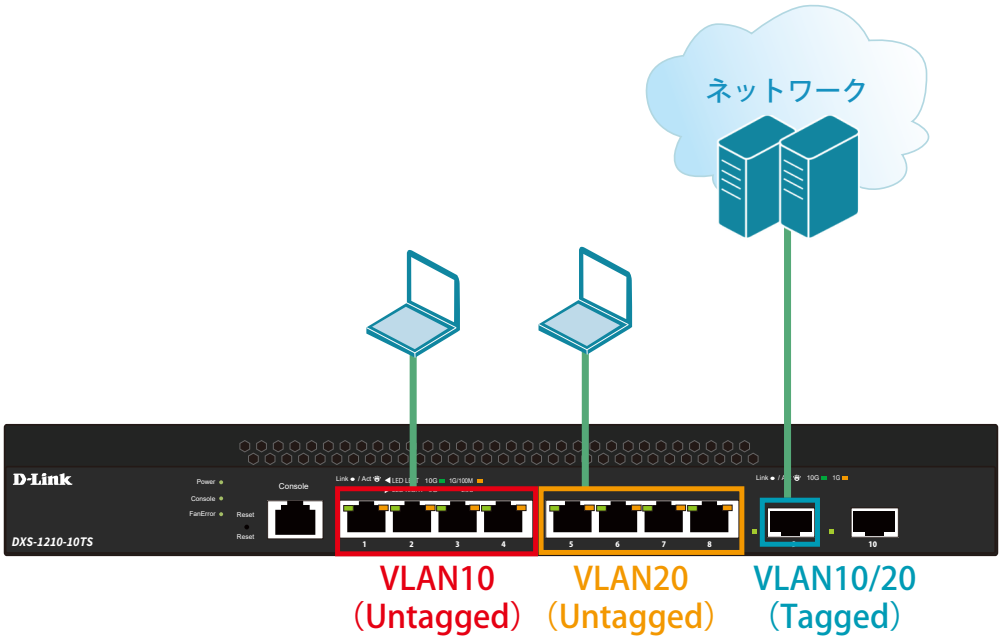


図 17-2　VLAN（DXS-1210-10TS）

概要

VLAN を設定します。ポート 1 - 4 に VLAN10 を「Untagged」で割り当て、ポート 5 ～ 8 に VLAN20 を「Untagged」で割り当て、ポート 9 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)#end
```

2. ポート 1-4 に VLAN10、ポート 5-8 に VLAN20 を 割り当てます。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#

Switch(config)#interface range ethernet 1/0/5-8
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 9 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 1/0/9
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 1/0/9
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
Destination filename startup-config? [y/n]:y
```

5. 情報確認

```
Switch#show vlan
```

（作成した VLAN と各ポートに割り当てられている VLAN が表示されます。）

```
Switch#show vlan int ethernet 1/0/xx
```

（ポートに紐づいている VLAN 情報が表示されます。）

Link Aggregation（リンクアグリゲーション）

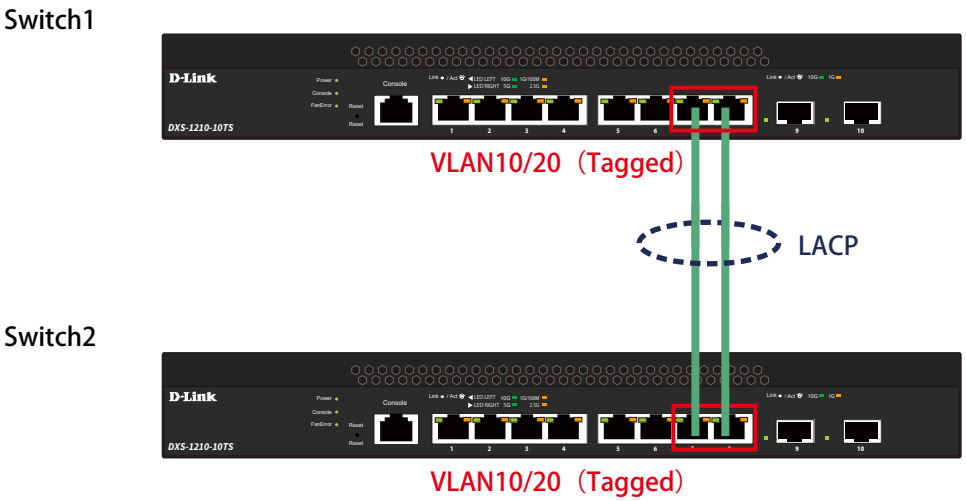


図 17-3　Link Aggregation（DXS-1210-10TS）

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 7 と 8 に VLAN10 と VLAN20 を「Tagged」で割り当て、ポート 7 と 8 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 range ethernet 1/0/7-8
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
```

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）

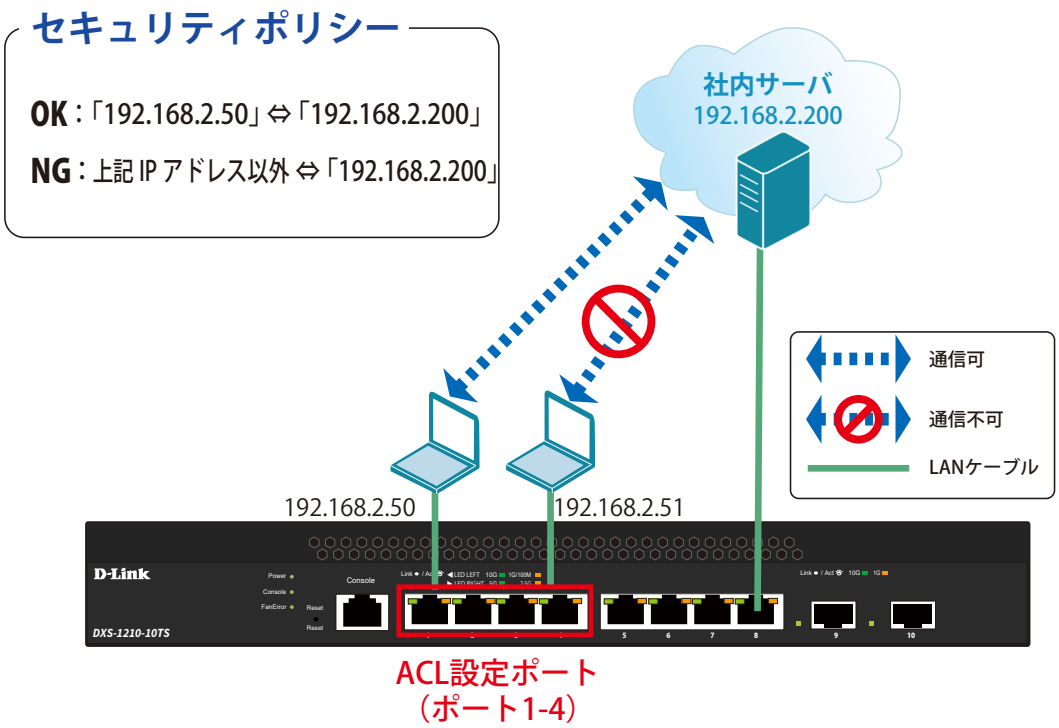


図 17-4　Access List（DXS-1210-10TS）

概要

ポート 1 - 4 に対し、アクセスリストを設定します。ポート 1 - 4 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)#rule permit 192.168.2.50 0.0.0.0 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#rule 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 - 4 へ設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-4
Switch(config-if-range)#ip access-group ACL in
Switch(config-if-range)#end
```

3. 設定を保存します。

```
Switch#copy running-config startup-config
```

4. 情報確認

```
Switch#show access-list
Switch#show access-list ip
Switch#show access-group
```

Loopback Detection（LBD）（ループ検知）

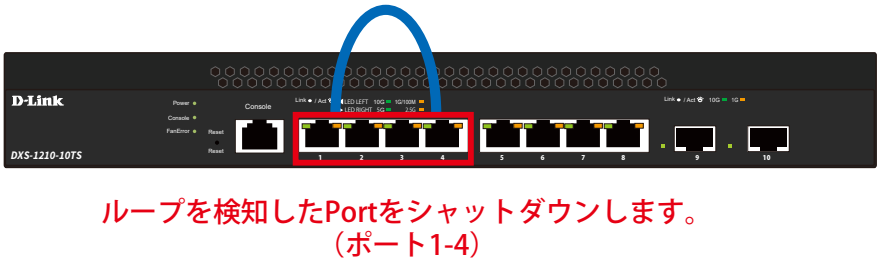


図 17-5　Loopback Detection（DXS-1210-10TS）

概要

ポート 1~4 に対しループバック検知を設定します。ポート 1~4 でループを検知した際、ポートをシャットダウンするように設定します。

設定手順

1. ポートベースでループ検知機能を動作させ、ループ検知後はポートをシャットダウンする設定をします。

```
Switch#configure terminal
Switch(config)#loopback-detection
Switch(config)#loopback-detection mode port-based
```

2. ループ発生を確認する間隔を 20 秒に設定します。

```
Switch(config)#loopback-detection interval 20
```

3. （必要に応じて）ループ発生後のループ解消確認間隔を 20 秒に設定し、ループ解消確認後、自動で Port 開放するように設定します。

```
Switch(config)#errdisable recovery cause loopback-detect interval 20
```

注意 この設定をしない場合、永続的にポートが「shutdown」状態となります。ポートを開放する場合、該当のポートに対し、インタフェースモードにて「no shutdown」コマンドを投入する必要があります。

4. ポート 1-8 でループバック検知機能を有効にします。

```
Switch(config)#interface range ethernet 1/0/1-4
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。

7. 設定を保存します。

```
Switch#copy running-config startup-config
```

8. 情報確認

```
Switch#show loopback-detection
```

（ループ検知の有効 / 無効、各ポートのループ状態等を表示します。）

```
Switch#show errdisable recovery
```

（ループ解消後の自動ポート解放設定の有効 / 無効、確認間隔を表示します。）