D-Link DXS-1100 シリーズ

10 Gigabit Layer2 Easy Smart Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

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

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

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

ご使用上の注意

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

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

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

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

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

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

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

目次

安全にお使いいただくために 2
ご使用上の注意 4
静電気障害を防止するために 4
電源の異常 4

はじめに 10

本マニュアルの対象者 11
表記規則について 11
製品名 / 品番一覧 11

第 1 章　本製品のご利用にあたって 12

スイッチ概要 12
SFP について 12
前面パネル 13
LED 表示 13
背面パネル 14
側面パネル 15
　スマートファンについて 15

第 2 章　スイッチの設置 16

パッケージの内容 16
ネットワーク接続前の準備 16
ゴム足の取り付け（19 インチラックに設置しない場合） 16
19 インチラックへの取り付け 17
SFP+ スロットの設置 18
電源抜け防止クリップの装着 18
電源の投入 20
電源の異常 20

第 3 章　スイッチの接続 21

エンドノードと接続する 21
バックボーンまたはサーバと接続する 21

第 4 章　スイッチ管理について 22

管理オプション 22
　SNMP ベースの管理 22
　Web ベースの管理インタフェース 22
SNMP 設定 22
　トラップ 23
　MIB 23
　DNA (D-Link Network Assistant) について 23

第 5 章　Web ベースのスイッチ管理 24

Web ベースの管理について 24
Web マネージャへのログイン 24
Smart Wizard 設定 26
Web ベースのユーザインタフェース 29
　ユーザインタフェース内の各エリア 29
Web マネージャのメニュー構成 30

第 6 章　System（システム設定） 31

Device Information（デバイス情報） 32
System Information Settings（システム情報） 33
Peripheral Settings（環境設定） 33
Port Configuration（ポート設定） 34
　Port Settings（ポート設定） 34
　Port Status（ポートステータス） 35
　Error Disabled Settings（エラー無効設定） 36
　Jumbo Frame（ジャンボフレーム設定） 36
System Log（システムログ） 37
　System Log Settings（システムログ設定） 37
　System Log Discriminator Settings（システムログディスクリミネーター設定） 38
　System Log Server Settings（システムログサーバの設定） 38
　System Log（システムログの設定） 39
　System Attack Log（システムアタックログ） 39

Time and SNTP（時間設定・SNTP 設定）..... 40
Clock Settings（時間設定）..... 40
Time Zone Settings（タイムゾーン設定）..... 40
SNTP Settings（SNTP 設定）..... 42
Time Range（タイムレンジ設定）..... 43

第 7 章　Management（スイッチの管理）　44

User Accounts Settings（ユーザアカウント設定）..... 45
Password Encryption（パスワード暗号化）..... 46
SNMP（SNMP 設定）..... 46
SNMP Global Settings（SNMP グローバル設定）..... 47
SNMP Linkchange Traps Settings（SNMP リンクチェンジトラップ設定）..... 48
SNMP View Table Settings（SNMP ビューテーブル）..... 48
SNMP Community Table Settings（SNMP コミュニティテーブル設定）..... 49
SNMP Group Table Settings（SNMP グループテーブル設定）..... 50
SNMP Engine ID Local Settings（SNMP エンジン ID ローカル設定）..... 50
SNMP User Table Settings（SNMP ユーザテーブル設定）..... 51
SNMP Host Table Settings（SNMP ホストテーブル設定）..... 52
RMON（RMON 設定）..... 53
RMON Global Settings（RMON グローバル設定）..... 53
RMON Statistics Settings（RMON 統計情報）..... 53
RMON History Settings（RMON ヒストリ設定）..... 54
RMON Alarm Settings（RMON アラーム設定）..... 55
RMON Event Settings（RMON イベント設定）..... 56
Web Settings（Web 設定）..... 57
Session Timeout（セッションタイムアウト）..... 57
File System（ファイルシステム）..... 58
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）..... 59

第 8 章　L2 Features（レイヤ 2 機能の設定）　60

FDB（FDB 設定）..... 61
Static FDB（スタティック FDB 設定）..... 61
MAC Address Table Settings（MAC アドレステーブル設定）..... 62
MAC Address Table（MAC アドレステーブル）..... 63
MAC Notification（MAC 通知設定）..... 64
VLAN（VLAN 設定）..... 65
802.1Q VLAN Settings（802.1Q VLAN 設定）..... 65
Asymmetric VLAN（Asymmetric VLAN 設定）..... 66
VLAN Interface（VLAN インタフェース設定）..... 66
Auto Surveillance VLAN（自動サーベイランス VLAN）..... 68
Voice VLAN（音声 VLAN）..... 70
Spanning Tree（STP/ スパニングツリーの設定）..... 73
802.1Q-2005 MSTP..... 73
802.1D-2004 Rapid Spanning Tree..... 73
ポートの状態遷移..... 73
STP Global Settings（STP グローバル設定）..... 74
STP Port Settings（STP ポートの設定）..... 75
STP Global Information（STP グローバル情報）..... 76
STP Port Information（STP ポート情報）..... 76
Loopback Detection（ループバック検知設定）..... 77
Link Aggregation（リンクアグリゲーション）..... 78
L2 Multicast Control（L2 マルチキャストコントロール）..... 80
IGMP Snooping（IGMP スヌーピング）..... 80
MLD Snooping Settings（MLD スヌーピング）..... 84
Multicast Filtering（マルチキャストフィルタリング）..... 89
LLDP（LLDP 設定）..... 89
LLDP Global Settings（LLDP グローバル設定）..... 90
LLDP Port Settings（LLDP ポート設定）..... 91
LLDP Management Address List（LLDP 管理アドレスリスト）..... 92
LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）..... 92
LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）..... 93
LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）..... 93
LLDP-MED Port Settings（LLDP-MED ポート設定）..... 94
LLDP Statistics Information（LLDP 統計情報）..... 94
LLDP Local Port Information（LLDP ローカルポート情報）..... 95
LLDP Neighbor Port Information（LLDP ネイバポート情報）..... 96

第 9 章　L3 Features（レイヤ 3 機能）　97

IPv4 Interface（IPv4 インタフェース）....98
IPv6 Interface（IPv6 インタフェース）....99
IPv6 Neighbor（IPv6 Neighbor 設定）....100
IPv6 Route Table（IPv6 ルートテーブル）....101

第 10 章　QoS（QoS 機能の設定）　102

Basic Settings（基本設定）....102
　Port Default CoS（ポートデフォルト CoS 設定）....102
　Port Scheduler Method（ポートスケジューラーメソッド設定）....103
　Queue Settings（QoS 設定）....103
　CoS to Queue Mapping（CoS キューマッピング設定）....104
　Port Rate Limiting（ポートレート制限設定）....104
Advanced Settings（アドバンス設定）....105
　Port Trust State（ポートトラスト設定）....105
　DSCP CoS Mapping（DSCP CoS マップ設定）....105

第 11 章　Security（セキュリティ機能の設定）　106

Port Security（ポートセキュリティ）....107
　Port Security Global Settings（ポートセキュリティグローバル設定）....107
　Port Security Port Settings（ポートセキュリティポート設定）....107
　Port Security Address Entries（ポートセキュリティアドレスエントリ設定）....108
ARP Spoofing Prevention（ARP スプーフィング防止設定）....109
Safeguard Engine Settings（セーフガードエンジン）....110
Traffic Segmentation Settings（トラフィックセグメンテーション）....111
Storm Control（ストームコントロール）....111
DoS Attack Prevention Settings（DoS 攻撃防止設定）....113
SSL（Secure Socket Layer）....114
　SSL Global Settings（SSL グローバル設定）....115
　Crypto PKI Trustpoint（暗号 PKI トラストポイント）....115
　SSL Service Policy（SSL サービスポリシー）....116

第 12 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)　117

Cable Diagnostics（ケーブル診断機能）....117

第 13 章　Monitoring（スイッチのモニタリング）　118

Utilization（利用分析）....118
　Port Utilization（ポート使用率）....118
Statistics（統計情報）....119
　Port（ポート統計情報）....119
　Port Counters（ポートカウンタ）....120
　Counters（カウンタ）....122
Mirror Settings（ミラー設定）....123
Device Environment（機器環境確認）....124

第 14 章　Green（省電力テクノロジー）　125

Power Saving（省電力）....125
　Power Saving Global Settings タブ....125
　Power Saving Shutdown Settings タブ....126
EEE（Energy Efficient Ethernet/ 省電力イーサネット）....126

第 15 章　Save and Tools（Save と Tools メニュー）　127

Save（Save メニュー）....127
　Save Configuration（コンフィグレーションの保存）....127
Tools（ツールメニュー）....127
　Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）....127
　Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）....129
　Log Backup（ログファイルのバックアップ）....131
　Ping....132
　Reset（リセット）....133
　Reboot System（システム再起動）....133

付録 A ケーブルとコネクタ 134

付録 B ケーブル長 134

付録 C 用語解説 135

付録 D 機能設定例 137

対象機器について 137
Traffic Segmentation（トラフィックセグメンテーション） 138
VLAN 139
Link Aggregation（リンクアグリゲーション） 141

はじめに

DXS-1100 シリーズユーザマニュアルは、本スイッチのインストールおよび操作方法を例題と共に記述しています。

第 1 章 本製品のご利用にあたって
- 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、各種管理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方法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、ユーザアカウントの設定、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、パスワード暗号化、SNMP 設定、RMON 設定、Web 設定、セッションタイムアウト、ファイルシステム、D-Link ディスカバリプロトコル設定など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、リンクアグリゲーション、L2 マルチキャストコントロール、LLDP 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）
- IPv4/IPv6 インタフェース、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）
- 802.1p 設定、CoS、QoS 設定について説明します。

第 11 章 Security（セキュリティ機能の設定）
- ポートセキュリティ、ARP スプーフィング防止設定、セーフガードエンジン、トラフィックセグメンテーション、ストームコントロール、DoS 攻撃防止設定、SSL などのセキュリティの設定について解説します。

第 12 章 OAM（Object Access Method : オブジェクトアクセス方式）
- ケーブル診断機能設定について解説します。

第 13 章 Monitoring（スイッチのモニタリング）
- 本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報について表示します。

第 14 章 Green（グリーンテクノロジー）
- 本スイッチの省電力、EEE について設定、表示します。

第 15 章 Save and Tools（Save と Tools メニュー）
- Web インタフェース画面左上部の「Save」「Tools」メニューを使用してスイッチの管理、設定を行います。

付録 A ケーブルとコネクタ
- スイッチに使用されるケーブルとコネクタ形状について説明します。

付録 B ケーブル長
- スイッチに使用されるケーブル長の最大値について説明します。

付録 C 用語解説
- 本マニュアルに使用される用語の定義を示します。

付録 D 機能設定例
- 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。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

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

製品名 / 品番一覧

製品名	品番
DXS-1100-10TS	DXS-1100-10TS
DXS-1100-16TC	DXS-1100-16TC
DXS-1100-16SC	DXS-1100-16SC

第 1 章　本製品のご利用にあたって

- スイッチ概要
- SFP について
- 前面パネル
- LED 表示
- 背面パネル
- 側面パネル

DXS-1100 シリーズは、10 ギガビットの高速通信を実現するサーバファーム、ネットワークエッジとして理想的な製品で、小、中規模のビジネスシーンに適した Easy スマートレイヤー 2 10 ギガビットイーサネットスイッチです。本製品は「Easy Smart スイッチ」に位置付けられ、Web UI でのみ設定が可能です。802.1Q やリンクアグリゲーションなどエッジでも必須となる機能を実装し、Web UI で直感的に設定が可能です。また、D-Link Green に対応し、環境にも配慮や運用コストの削減を提供します。

本マニュアルでは、DXS-1100-10TS、DXS-1100-16TC、DXS-1100-16SC を含む D-Link DXS-1100 シリーズの設置、管理および設定の方法について記述しています。本シリーズは機能設定やハードウェア構成は一部機能を除き同じであるため、本マニュアルの情報をすべての種類にほぼ適用できます。Web による管理画面例は、上に記載したいずれかの機種のものですが、一部機能、ポート数を除き設定内容はほぼ同じです。

スイッチ概要

DXS-1100 シリーズは以下の製品で構成されるギガビット L2 Web スマートスイッチです。:

- DXS-1100-10TS：100/1000/10G BASE-T x 8 ポート、10G SFP+ x 2 スロット搭載
- DXS-1100-16TC：100/1000/10G BASE-T x 14 ポート、10G SFP+ x 2 コンボスロット 10G SFP+ x 2 スロット搭載
- DXS-1100-16SC：10G SFP+ x 16 スロット、100/1000/10G BASE-T x 2 コンボポート搭載

注意　DXS-1100 シリーズのすべての機種について、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-1100” と記載します。

ケーブルについて

本製品で 10G ビットイーサネットを使用するには、以下のケーブルを使用してください。

- IEEE 802.3an 10GBASE-T：UTP/STP ケーブル（Cat6A 以上）

SFP について

本スイッチには PC やハブ、他のスイッチなど、様々なアップリンクネットワークデバイスとの全二重モードでの接続に使用される 10G BASE-T ポートと SFP+ スロットがあります。SFP（Small Form-Factor Pluggable）ポートは光ファイバトランシーバ用のケーブル配線に使用され、ギガビットデータの長距離伝送が可能なネットワークデバイスと通信を行います。これらの SFP スロットは、全二重モードをサポートして、次のトランシーバと共に使用が可能です。

DXS-1100 シリーズスイッチ対応オプションモジュール

種別	製品名
SFP+(10Giga)	DEM-431XT
	DEM-432XT
	DEM-433XT
	DEM-434XT
	DEM-436XT-BXU
	DEM-436XT-BXD
Copper SFP+(10Giga)	DEM-410T※
WDM 対応 1 芯 SFP(1Giga)	DEM-330T
	DEM-330R
	DEM-331T
	DEM-331R
2 芯 SFP(1Giga)	DEM-310GT
	DEM-311GT
	DEM-312GT2
	DEM-314GT
	DEM-315GT
Copper SFP(1Giga)	DGS-712※

※ SFP コンボスロットでは使用できません。

前面パネル

スイッチの前面パネルには、ポート、スロットおよび Reset ボタンの他、電源、および各ポートの Link/Act を示す各ポート、SPF+ スロット用の LED が配置されています。

DXS-1100-10TS

図 1-1　DXS-1100-10TS の前面パネル

DXS-1100-16TC

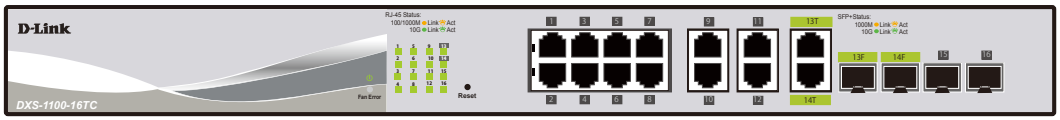

図 1-2　DXS-1100-16TC の前面パネル

DXS-1100-16SC

図 1-3　DXS-1100-16SC の前面パネル

LED 表示

スイッチは、Power、ファン、およびポート / スロットについての LED をサポートしています。

DXS-1100-10TS

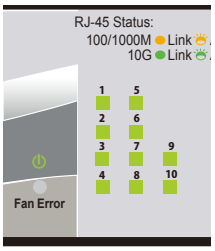

図 1-4　DXS-1100-10TS の前面 LED

DXS-1100-16TC

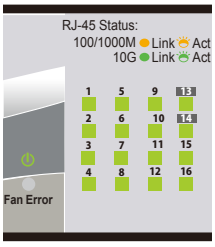

図 1-5　DXS-1100-16TC の前面 LED

DXS-1100-16SC

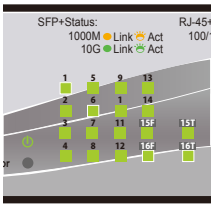

図 1-6　DXS-1100-16SC の前面 LED

以下の表に LED の状態が意味するスイッチの状態を示します。

LED	色	状態	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。
	ー	消灯	電源が供給されていません。
Fan Err	赤	点灯	ファンのいずれかが故障しています。
	緑	点灯	ファンは正常に動作しています。
100/1000/10G ポート LED			
Link/Act/Speed	緑	点灯	10Gbps でリンクが確立しています。
		点滅	10Gbps でデータを送受信しています。
	橙	点灯	100/1000Mbps でリンクが確立しています。
		点滅	100/1000Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
SFP+ スロット LED			
Link/ACT	緑	点灯	10Gbps でリンクが確立しています。
		点滅	10Gbps でデータを送受信しています。
	橙	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。

背面パネル

DXS-1100-10TS

接地コネクタ、AC 電源コネクタ、電源抜け防止クリップ挿入口、セキュリティスロットが配備されています。

図 1-7　DXS-1100-10TS の背面パネル

DXS-1100-16TC

接地コネクタ、AC 電源コネクタ、電源抜け防止クリップ挿入口、セキュリティスロットが配備されています。

図 1-8　DXS-1100-16TC の背面パネル

DXS-1100-16SC

接地コネクタ、AC 電源コネクタ、電源抜け防止クリップ挿入口、セキュリティスロットが配備されています。

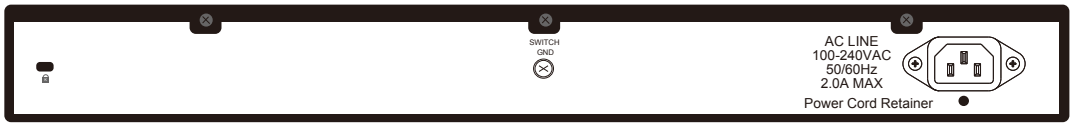

図 1-9　DXS-1100-16SC の背面パネル

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

警告 システムの通気口が両側面にあります。通気口はスイッチが持つ熱を放出する役割がありますので、これらをふさがないようにご注意ください。スイッチの適切な通気のためには、必ず 16cm 以上のスペースを確保してください。最適な熱放出、空気の循環をしないとシステム障害や部品の激しい損傷を引き起こす場合がありますのでご注意ください。

DXS-1100-10TS、DXS-1100-16TC、DXS-1100-16SC

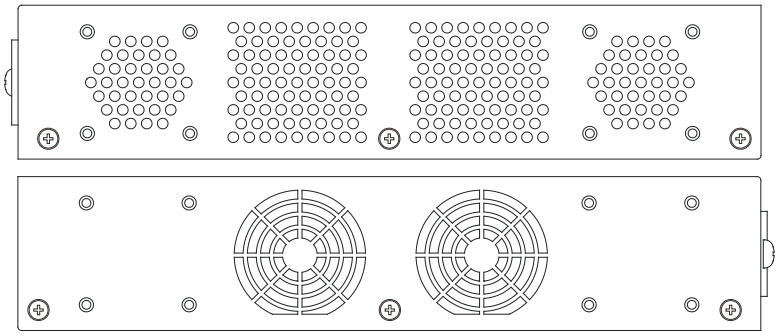

図 1-10　DXS-1100-10TS、DXS-1100-16TC、DXS-1100-16SC の側面パネル

スマートファンについて

DXS-1100 シリーズスイッチ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。スピード調整には 2 つの状態があり「低スピード回転」「高スピード回転」になっています。

以下が各機種のスマートファンによるスピード調整の基準になります。

DXS-1100-10TS、16TC
内部温度が 40℃以上になった場合、ファンは「高スピード回転」に移行します。
内部温度が 36 度以下になった場合、ファンは「低スピード回転」に移行します。

DXS-1100-16SC
内部温度が 56℃以上になった場合、ファンは「高スピード回転」に移行します。
内部温度が 46℃以下になった場合、ファンは「低スピード回転」に移行します。

第 2 章　スイッチの設置

- パッケージの内容
- ネットワーク接続前の準備
- ゴム足の取り付け（19 インチラックに設置しない場合）
- 19 インチラックへの取り付け
- SFP スロットの設置
- 電源抜け防止クリップの装着
- 電源の投入
- 電源の異常

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
- 電源ケーブル　x　1
- 19 インチラックマウントキット 1 式
- ゴム足（貼り付けタイプ）　x　4
- 電源抜け防止クリップ　x　1
- クイックインストールガイド
- CD-ROM　x　1
- PL シート　x　1

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最低 3 キロ以上の耐荷重性のある場所に設置してください。また、スイッチの上に重いものを置かないでください。
- 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本スイッチの周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後 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たゴム製足をスイッチの裏面の四隅に取り付けます。スイッチの周囲に十分な通気を確保するようにしてください。

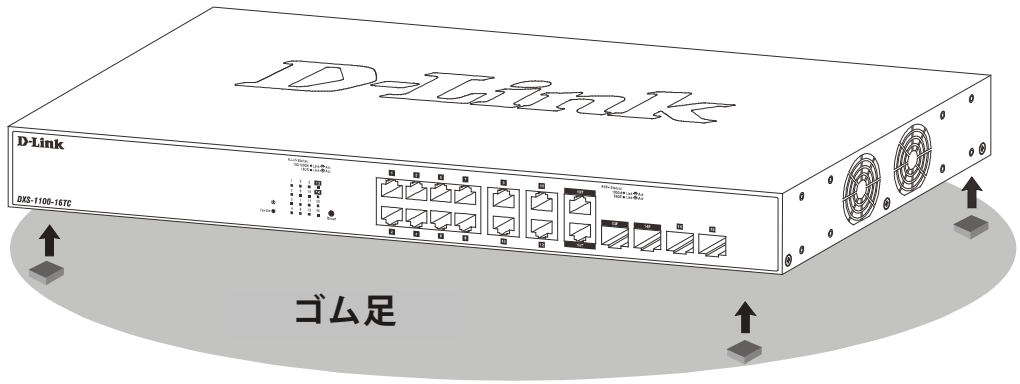

図 2-1　　机や棚の上に設置する場合の準備（DXS-1100-16TC）

19 インチラックへの取り付け

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

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

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シャーシ、拡張モジュールに接続していないことを確認します。
2. 付属のネジで、スイッチ両側面にブラケットを取り付けます。

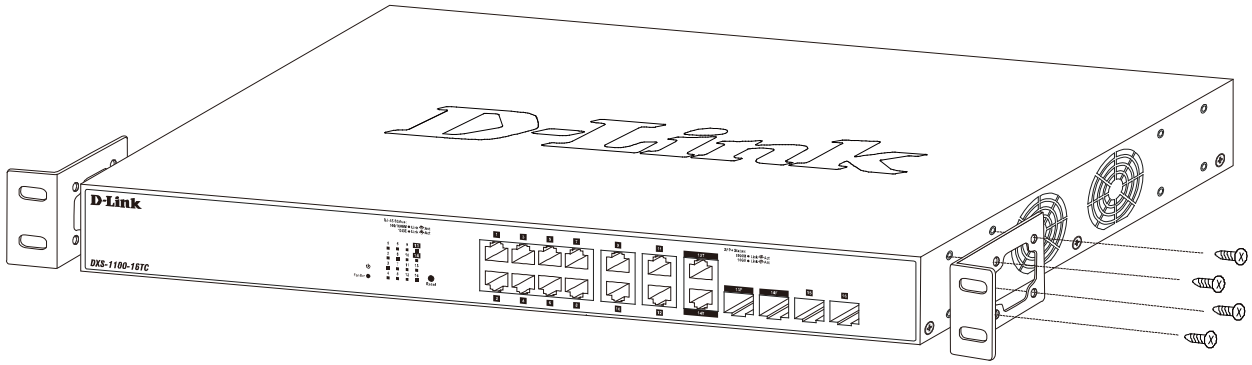

図 2-2　ブラケットの取り付け

3. 19 インチラックに付属のネジを使用し、シャーシをラックに固定します。

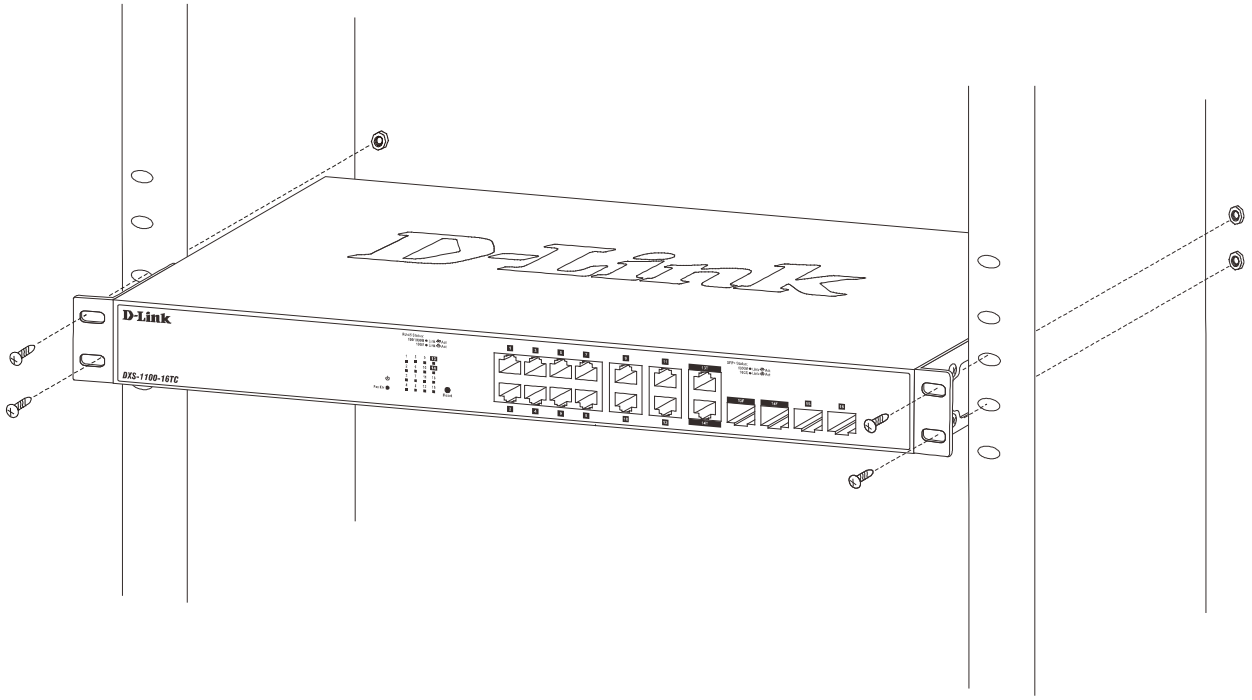

図 2-3　19 インチラックへの設置

SFP+ スロットの設置

スイッチの前面パネルに SFP スロットまたは SFP+ スロットを装備しています。以下に、スイッチに SFP/SFP+ スロットモジュールを挿入した図を示します。

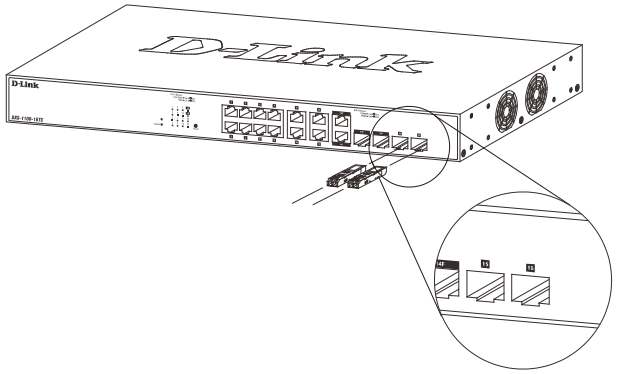

図 2-5　SFP ポートにモジュールを挿入

電源抜け防止クリップの装着

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

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

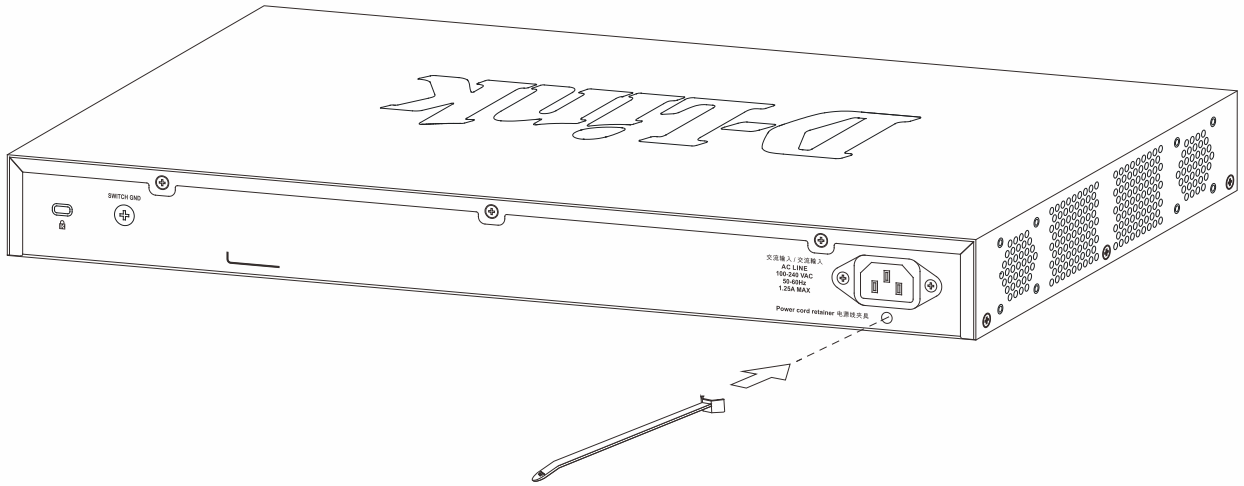

図 2-6　　タイラップの挿し込み

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。

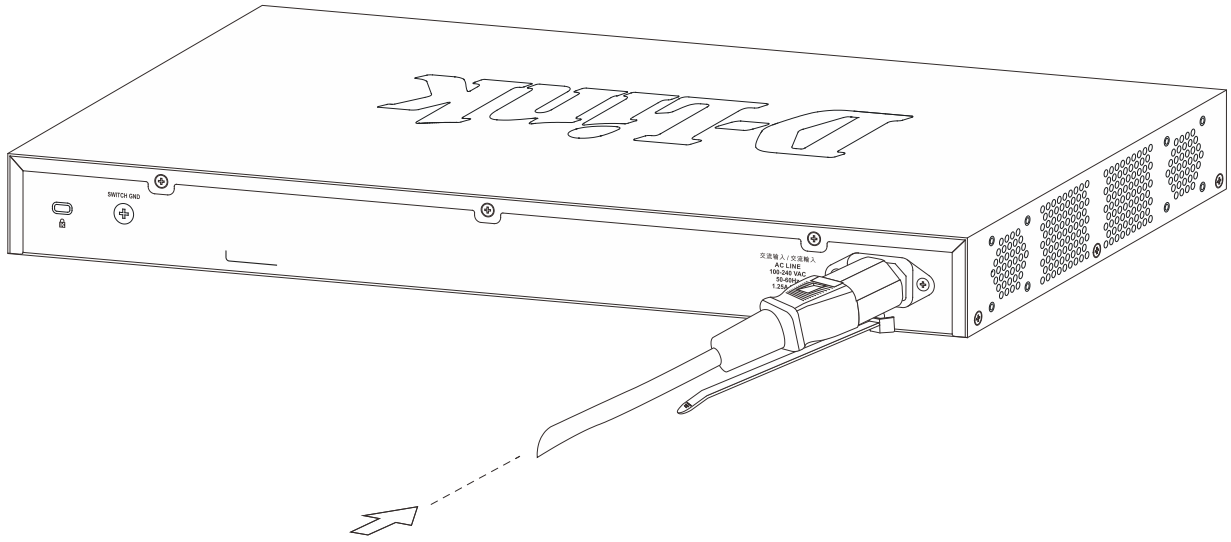

図 2-7　　電源コード挿し込み

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。

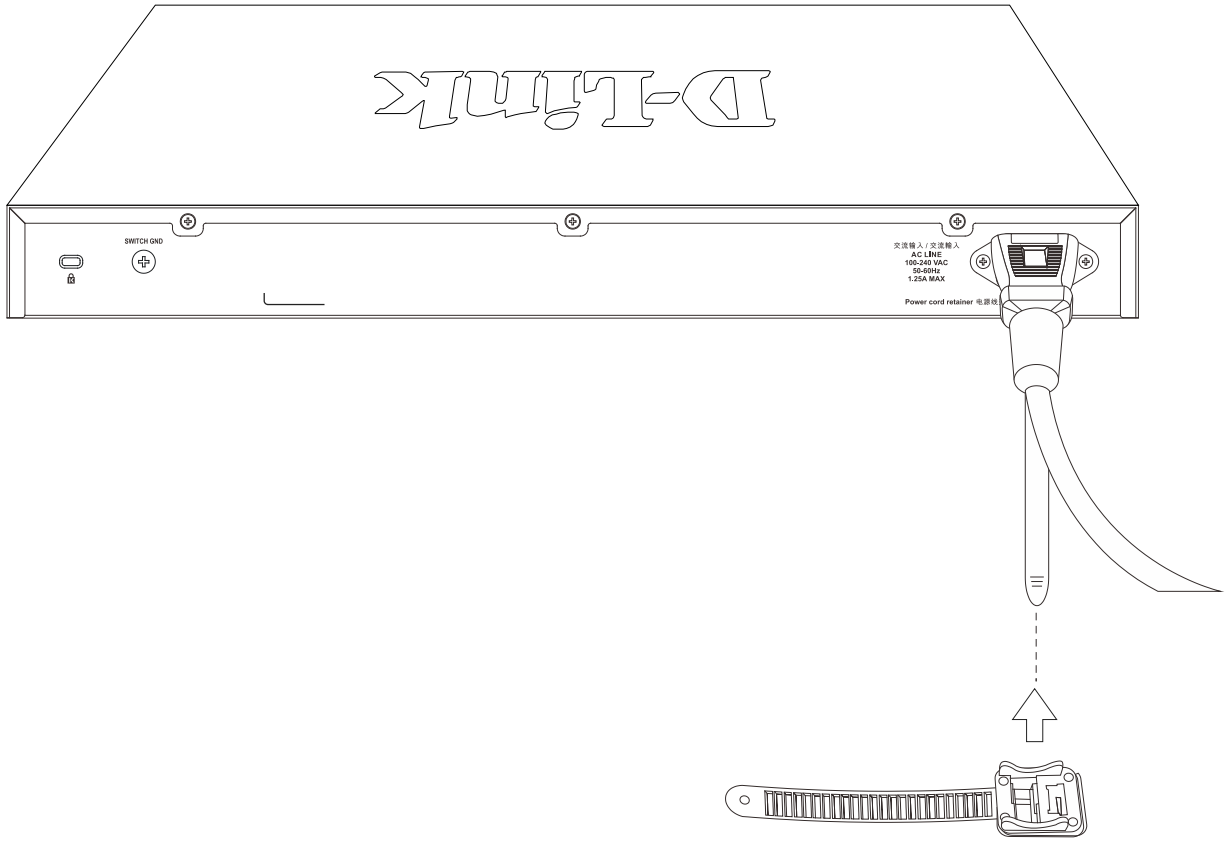

図 2-8　リテイナー（固定具）のスライド

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。

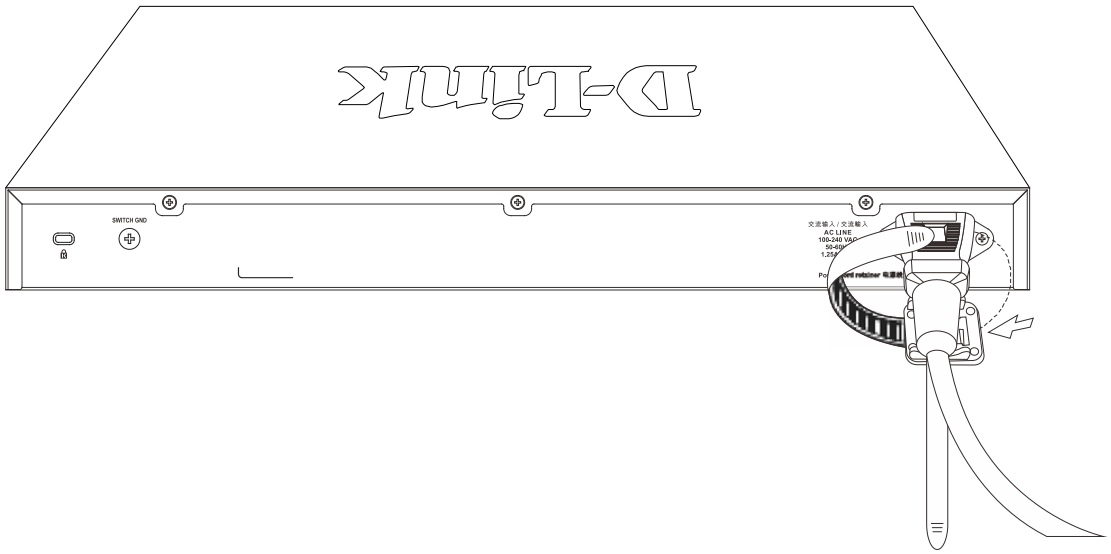

図 2-9　リテイナーの巻き付け、固定

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

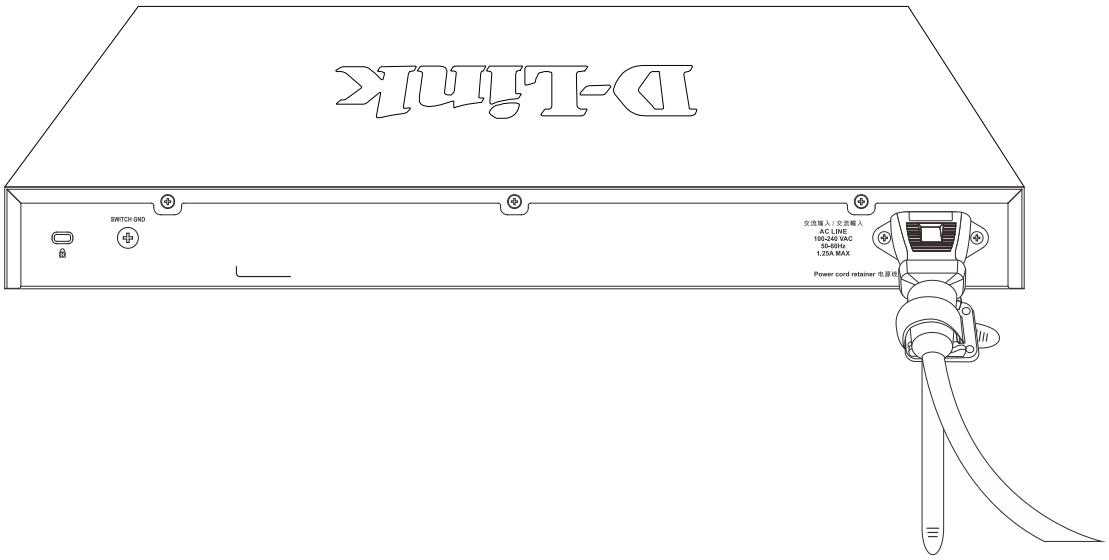

図 2-10　電源抜け防止クリップの固定確認

電源の投入

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

電源の異常

AC 電源に異常が発生した場合（停電等）、スイッチとの接続を解除してください。電力の回復後に再接続します。

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。

第 3 章　スイッチの接続

- エンドノードと接続する
- バックボーンまたはサーバと接続する

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本スイッチの 1000BASE-T ポートとエンドノードを接続します。
エンドノードとは、RJ-45 コネクタ対応 10/100/1000Mbps イーサネットネットワークインタフェースカードを装備した PC やルータを指しています。
さらにエンドノードとスイッチ間も UTP ケーブルで接続できます。エンドノードへの接続はスイッチ上の 100/1000/10G BASE-T ポートから行えます。
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。

バックボーンまたはサーバと接続する

SFP ＋ポートは、ネットワークバックボーンやサーバとのアップリンク接続に適しています。RJ-45 ポートは、全二重モード時において 100/1000/10Gbps の速度を提供し、SFP ＋ポートは、全二重モード時において 10Gbps の速度を提供します。
ギガビットイーサネットポートとの接続はポートのタイプによって光ファイバケーブルまたはエンハンスドカテゴリ 5 以上のケーブルを使用します。正しくリンクが確立すると Link LED が点灯します。

第 4 章　スイッチ管理について

- 管理オプション
- SNMP 設定

管理オプション

本システムは Web ブラウザを使用した Web ベース管理と SNMP ベースでの管理を行うことができます。さらに同梱のソフトウェア「DNA」(D-Link Network Assistant) を使用した管理も行うことが可能です。

SNMP ベースの管理

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

Web ベースの管理インタフェース

本スイッチの設置完了後、Microsoft® Internet Explorer（バージョン 7 以上）、Mozilla Firefox (最新バージョン)、Safari (最新バージョン) および Google Chrome (最新バージョン) によって本スイッチの設定、LED のモニタ、および統計情報をグラフィカルに表示することができます。

SNMP 設定

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

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

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

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

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

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

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

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

個別のユーザや SNMP マネージャグループに SNMP バージョン 3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。そのような管理機能の可否は各 MIB に関連付けられる OID（Object Identifier）を使用して定義します。SNMP バージョン 3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。スイッチでの SNMP バージョン 3 の設定方法については「SNMP（SNMP 設定）」（46 ページ）をご参照ください。

トラップ

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

MIB

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

DNA (D-Link Network Assistant) について

DNA（D-Link Network Assistant）は PC に接続している同じ L2 ネットワークセグメント内の Smart スイッチを検出、管理するためのプログラムです。DNA（D-Link Network Assistant）のインストール手順や使用方法については、弊社 Web よりマニュアルをダウンロードして参照してください。

注意 最新の DNA をインストールする前に既存の DNA を必ずアンインストールしてください。

注意 DXS-1100-16SC は未サポートです。

第 5 章　Web ベースのスイッチ管理

- Web ベースの管理について
- Web マネージャへのログイン
- Smart Wizard 設定
- Web ベースのユーザインタフェース
- Web マネージャのメニュー構成

Web ベースの管理について

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

Web 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）。この接続においてはプロキシ設定を無効とする必要があります。

ここでは D-Link の Web ベースインタフェースの利用方法について説明します。

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。ブラウザのポップアップブロックが無効になっていることを確認してください。ポップアップブロックが有効な場合、画面が開けない場合があります。

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。

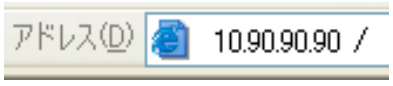

図 5-1　URL の入力

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」が設定されています。端末側の IP インタフェースを本スイッチに合わせるか、本スイッチを端末側の IP インタフェースに合わせてください。

3. 以下のユーザ認証画面が表示されます。

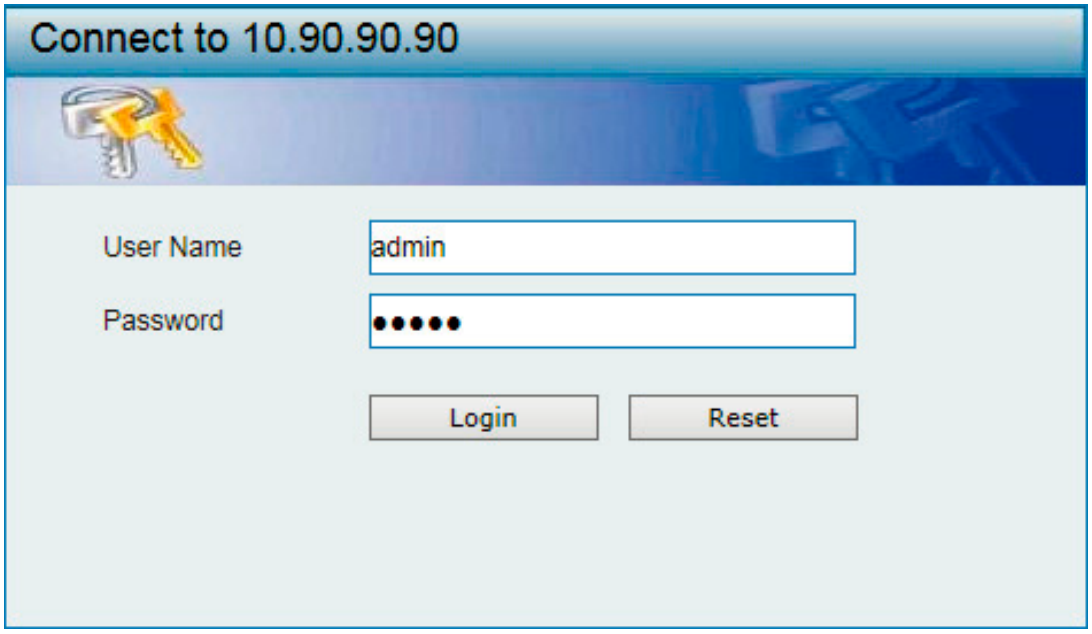

図 5-2　ユーザ認証画面

「ユーザー名」および「パスワード」欄を入力し、「OK」ボタンをクリックし、Web ベースユーザインタフェースに接続します。Web ブラウザで使用可能な機能を以下で説明します。
ご購入後、はじめてログインする場合は、「ユーザー名」、「パスワード」は「admin」と入力、「OK」ボタンをクリックします。

4. スマートウィザード画面が表示されます。

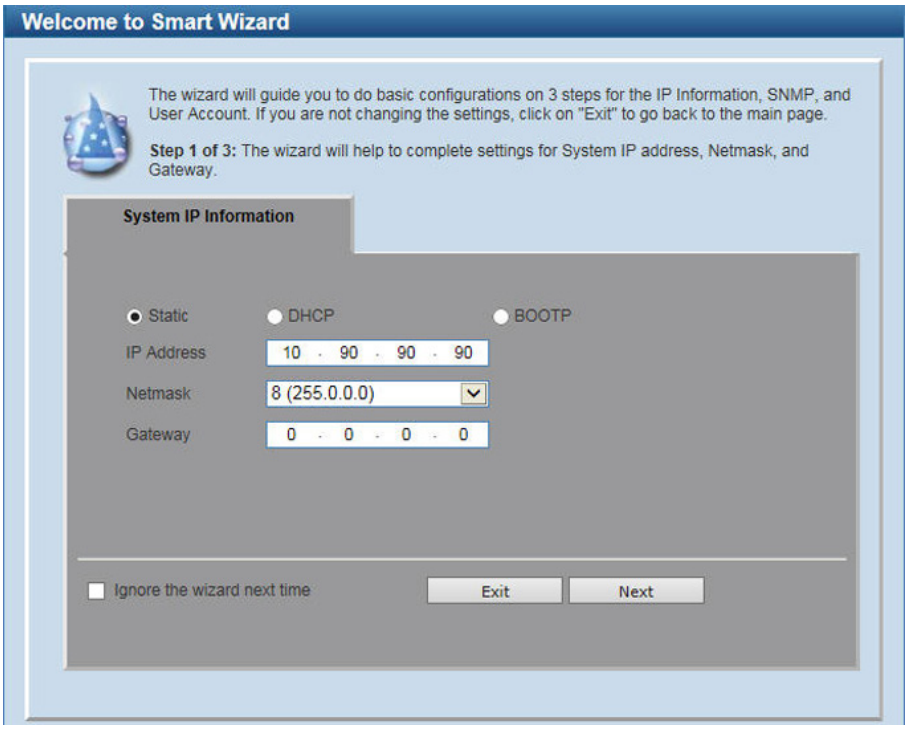

図 5-3　Smart Wizard 画面

ウィザード画面では、システム IP アドレス・ユーザアカウント / 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。

注意 Smart Wizard では、IPv4 アドレスのみ設定可能です。

注意 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。

注意 「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。

1. IP アドレスの設定を行います。

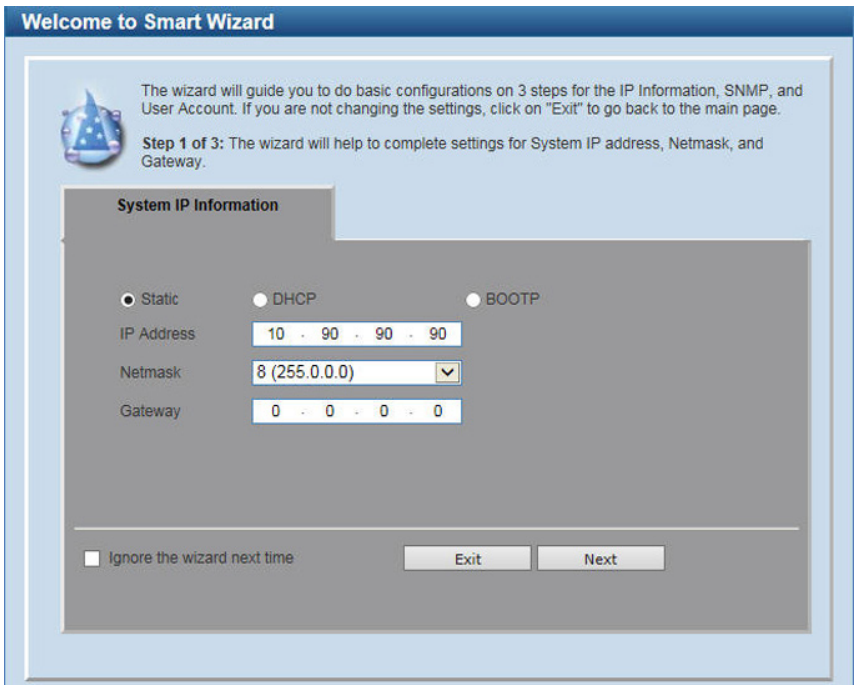

図 5-4　IP Information 設定画面

1. 「Static」「DHCP」「BOOTP」のいずれかをクリックします。
   - 「Static」：固定設定
   - 「DHCP」：DHCP による自動取得
   - 「BOOTP」：BOOTP による自動取得

   「Static」を選択した場合は、「IP Address」「Netmask」「Gateway」を入力します。
2. 「Next」をクリックします。

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

2. ユーザアカウントの設定を行います。

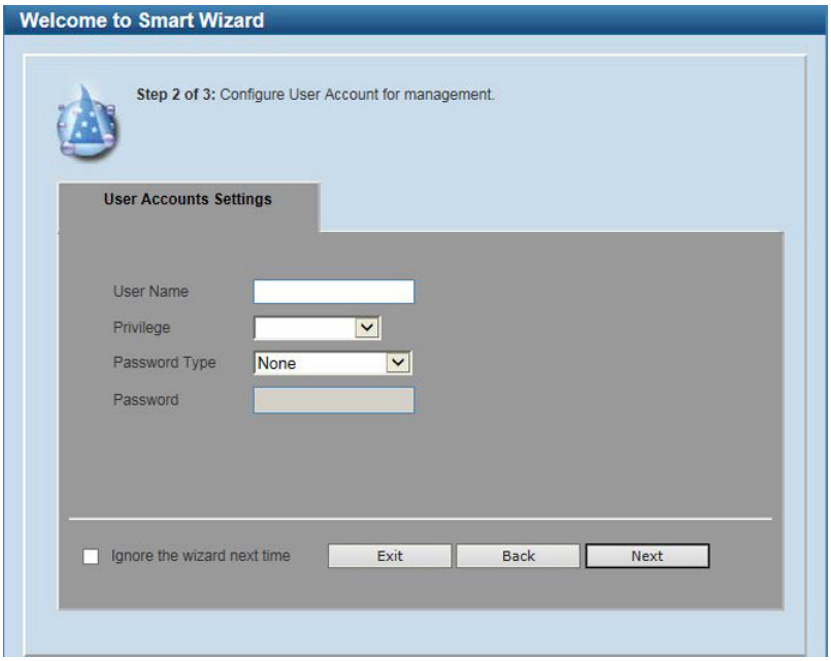

図 5-5　ユーザアカウント設定画面

以下の項目が表示されます。

項目	説明
User Name	ユーザアカウントに使用するユーザ名を入力します。
Privilege	ユーザアカウントの権限を指定します。 「User」（ユーザ）または「Administrator」（管理者）から指定できます。
Password Type	パスワードの種類を指定します。「None」「Plain Text」「Encrypted」から指定できます。 「Encrypted」を選択した場合のみ、「SHA-1」で 35 文字の暗号パスワードを入力することができます。これは入力時に暗号化されていない「プレーンテキスト」パスワードは、「暗号化フォーマット」へ暗号化することができないことを意味します。「Password Encryption」については「パスワード暗号化」を参照ください。
Password	パスワードの種類で「Plain Text」「Encrypted」をした場合本項目は指定可能になります。ユーザアカウントのパスワードを入力します。

ユーザアカウント設定手順

1. 「User Name」欄に設定するユーザアカウントを入力します。
2. 「Privilege」でアカウントの権限を指定します。
3. 「Password Type」でパスワードの種類を指定します。
4. 「Password」でパスワードを指定します。
5. 「Apply」をクリックします。
6. Web マネージャ画面が表示されます。

3. SNMP の設定を行います

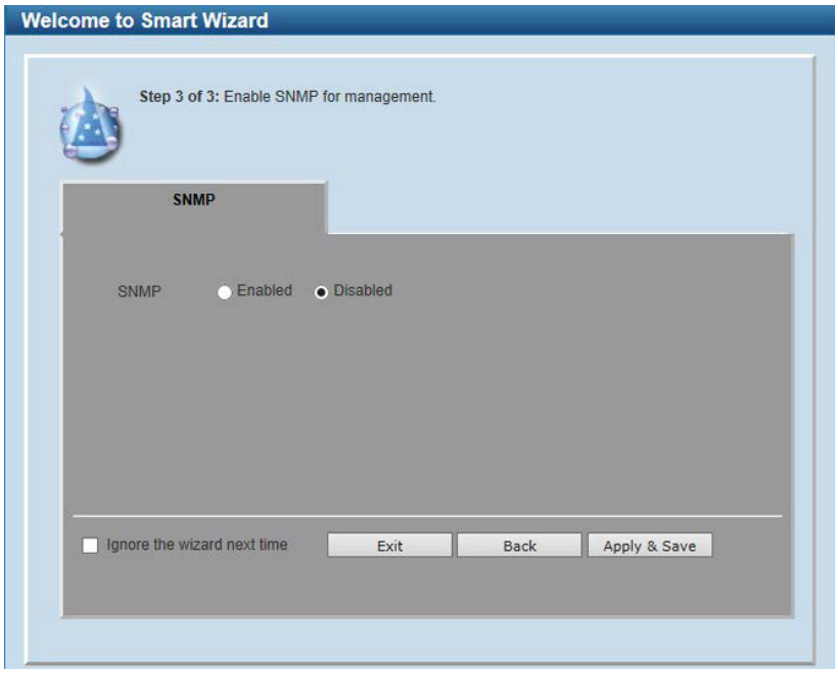

図 5-6　SNMP 設定画面

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。

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、管理画面にアクセスし、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。

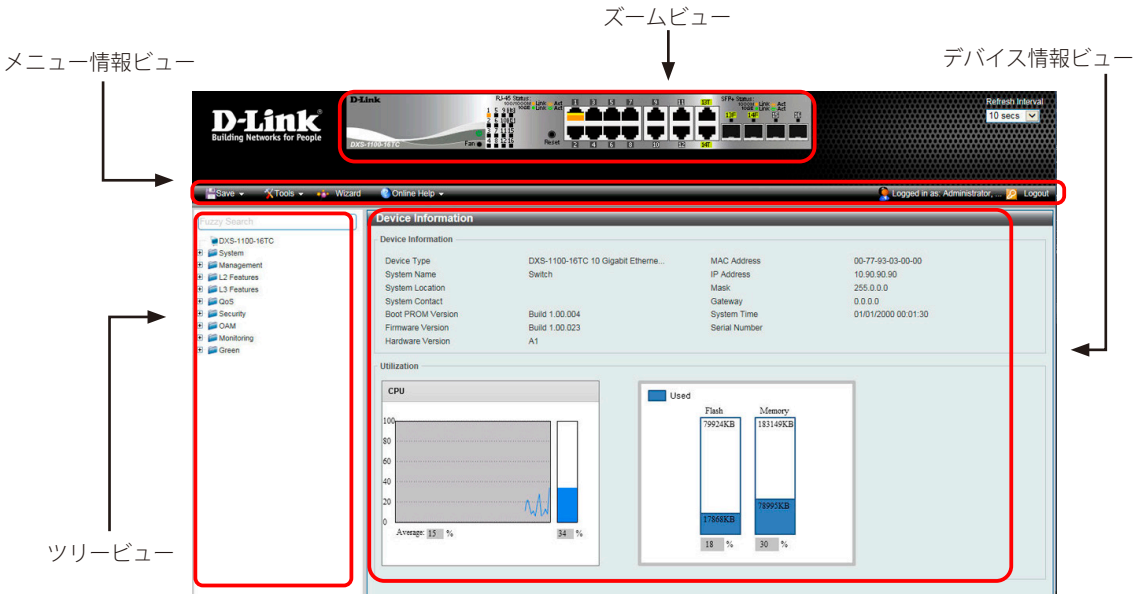

図 5-7　Device Information 画面

次の表では「Device Information」画面の主要な 4 つの領域について説明します。

表 5-1　メイン領域

ビュー	説明
ツリービュー	システムの機能、設定オプションごとに分類して表示します。 表示されているフォルダか画面を選択します。フォルダアイコンを開くことにより、ハイパーリンクメニューボタンやさらにその下のサブフォルダを表示することができます。
ズームビュー	ホームページの最上部に位置し、スイッチの前面パネル上のポートについて、ポート LED の状態をリアルタイムに近いグラフィック表示で提供します。この領域はスイッチのポートや拡張モジュールを表示し、設定したポートの動作、デュプレックスモード、フロー制御に従って表示します。 このグラフィックのさまざまな部分は、設定を含む管理機能を使用するために選択することができます。
メニュー情報ビュー	ズームビューの下で「Save」、「Tools」メニューや、「Wizard」、「Online Help」、「Logout」ボタンを提供します。 また、言語情報やログインユーザ名も表示します。
デバイス情報ビュー	ホームページの主となる部分にあり、デバイス情報ビューはスイッチの情報、テーブル、設定について表示します。

注意　スイッチ設定を変更した場合、以下で説明する Web ブラウザの「Apply」にて保存する必要があります。

注意　「Logout」をクリックせずに Web ブラウザを終了した場合、ログインセッションが残ったままになります。

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
Device Information（製品名）	—	スイッチの主な設定情報を表示します。
System	System Information Settings	スイッチの基本情報を表示します。
	Peripheral Settings	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。
	System Log	スイッチのシステムログ設定を行います。
	Time and SNTP	スイッチの時間設定を行います。
	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	パスワードの暗号を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。
	Web	スイッチの Web 設定をします。
	Session Timeout	セッションタイムアウトの設定をします。
	File System	フラッシュファイルシステムを設定します。
	D-Link Discovery Protocol	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	VLAN 表示、設定を行います。
	STP	スパニングツリーの設定を行います。
	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	IPv4 Interface	IPv4 アドレスのインタフェースの設定を行います。
	IPv6 Interface	IPv6 アドレスの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 Route Table	IPv6 のルートテーブルの設定を行います。
QoS	Basic Settings	QoS、CoS キューマッピングなどの設定を行います。
	Advanced Settings	DSCP/CoS のマップ設定などを行います。
Security	Port Security	ポートセキュリティの設定を行います。
	ARP Spoofing Prevention	ARP スプーフィング防止設定を行います。
	Safeguard Engine	セーフガードエンジン設定を行います。
	Traffic Segmentation	トラフィックセグメンテーション設定を行います。
	Storm Control	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。
	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。
Monitoring	Utilization	CPU 使用率、ポートの帯域使用率を表示します。
	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。
	Device Environment	機器環境の設定、表示を行います。
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。
Save and Tools	Save	コンフィグレーションの保存などを行います。
	Tools	ファームウエ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。

第 6 章　System（システム設定）

本章ではデバイス情報の確認、IP アドレスの設定、スタックの管理、ポートパラメータの設定、ユーザアカウントの設定、システムログの設定と管理、システム時刻の設定、SNMP システム管理について説明します。

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	参照ページ
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。	32
System Information Settings（システム情報）	スイッチの基本情報を表示します。	33
Peripheral Settings（環境設定）	スイッチの環境設定を行います。	33
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。以下のメニューがあります。 Port Status（ポートステータス）、Error Disabled Settings（エラー無効設定）、Jumbo Frame（ジャンボフレーム設定）	34
System Log（システムログ構成）	フラッシュメモリにスイッチのログを保存する方法、Syslog サーバの設定を行います。以下のメニューがあります。 System Log Settings（システムログ設定）、System Log Discriminator Settings（システムログディスクリミネーター設定）、System Log Server Settings（システムログサーバの設定）、System Log（システムログの設定）、System Attack Log（システムアタックログ）	37
Time and SNTP（時刻と SNTP 設定）	スイッチに時刻を設定します。	40
Time Range（タイムレンジ設定）	アクセスプロファイル機能を実行する期間を決定します。	43

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主な機能の設定内容です。他の画面から「Device Information」画面に戻るためには、「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として設定する項目があります。これには、システム名、場所、接続、システム MAC アドレス、システム稼働時間、IP アドレス、ファームウェア、ブート、およびハードウェアのバージョン情報などが含まれます。

ツリービューの製品名をクリックし、以下の画面を表示します。

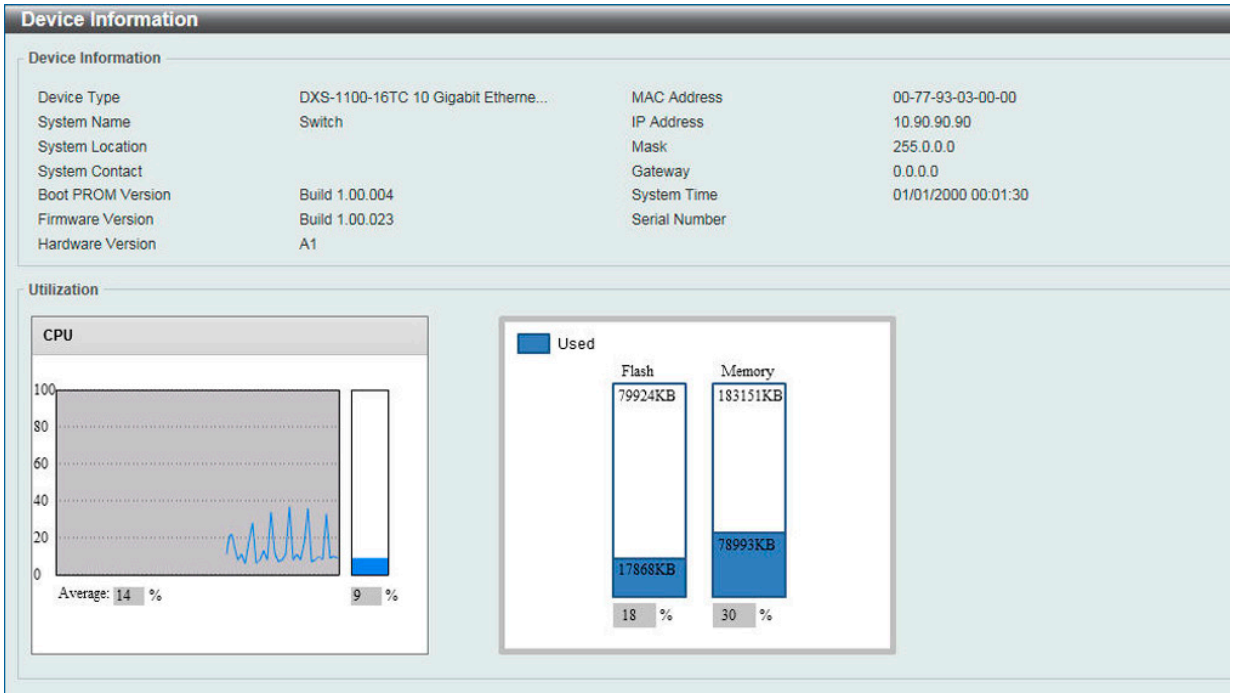

図 6-1　Device Information 画面

「Device Information」画面には以下の項目があります。

項目	説明
Device Information	
Device Type	工場にて定義した機種名と型式を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。（半角英数字 255 文字以内）
System Contact	担当者名を表示します。（半角英数字 255 文字以内）
Boot PROM Version	デバイスのブート /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。
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	システムの日付を表示します。日 / 月 / 年で表示します。
Serial Number	デバイスのシリアル番号を表示します。

System Information Settings（システム情報）

システム情報を提供します。

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

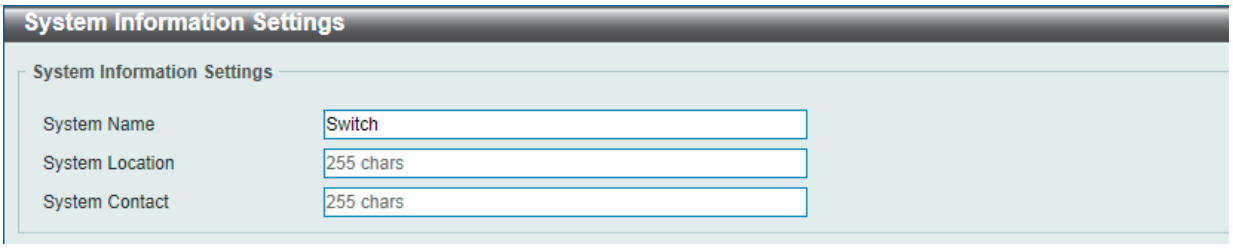

図 6-2　System Information Settings 画面

画面には以下の項目があります。

項目	説明
System Name	ユーザが定義するシステム名を設定します。 最大 64 文字、システム名の最初は英字、最後は英字もしくは数字を使用可能です。ハイフンはシステム名の最初と最後の文字以外の個所に使用可能です。10 文字以下での設定を推奨します。
System Location	システムが現在動作している場所を定義します。（半角英数字 255 文字以内）
System Contact	担当者名を表示します。（半角英数字 255 文字以内）

「Apply」ボタンをクリックすると設定が更新されます。

Peripheral Settings（環境設定）

システムの警告温度や環境トラップの設定を行います

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

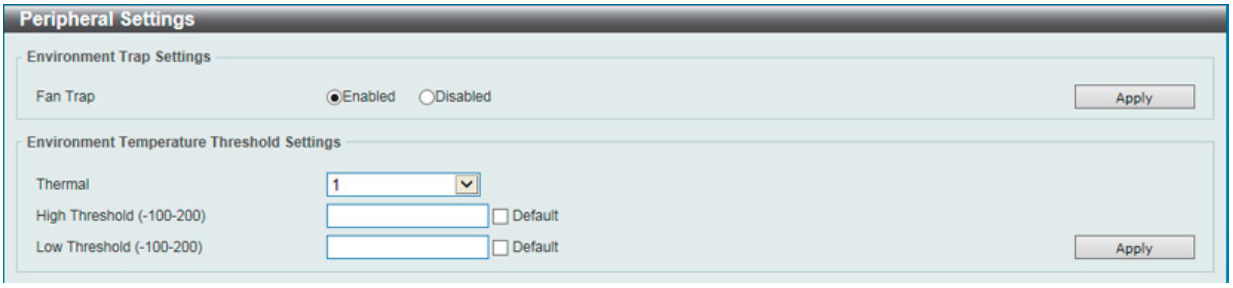

図 6-3　Peripheral Settings 画面

画面には以下の項目があります。

項目	説明
Environment Trap Settings	
Fan Trap	ファン警告設定のトラップを有効 / 無効に設定します。
Environment Temperture Threshold Settings	
Thermal	温度センサ ID を選択します。
High Threshold	高温警告しきい値を指定します。-100℃から 200℃の間で指定できます。「Default」をチェックすると初期値に戻ります。
Low Threshold	低温警告しきい値を指定します。-100℃から 200℃の間で指定できます。「Default」をチェックすると初期値に戻ります。

「Apply」ボタンをクリックすると設定が更新されます。

Port Configuration（ポート設定）

各ポートの設定を行います。

Port Settings（ポート設定）

デバイスのポートの詳細説明を設定します。

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

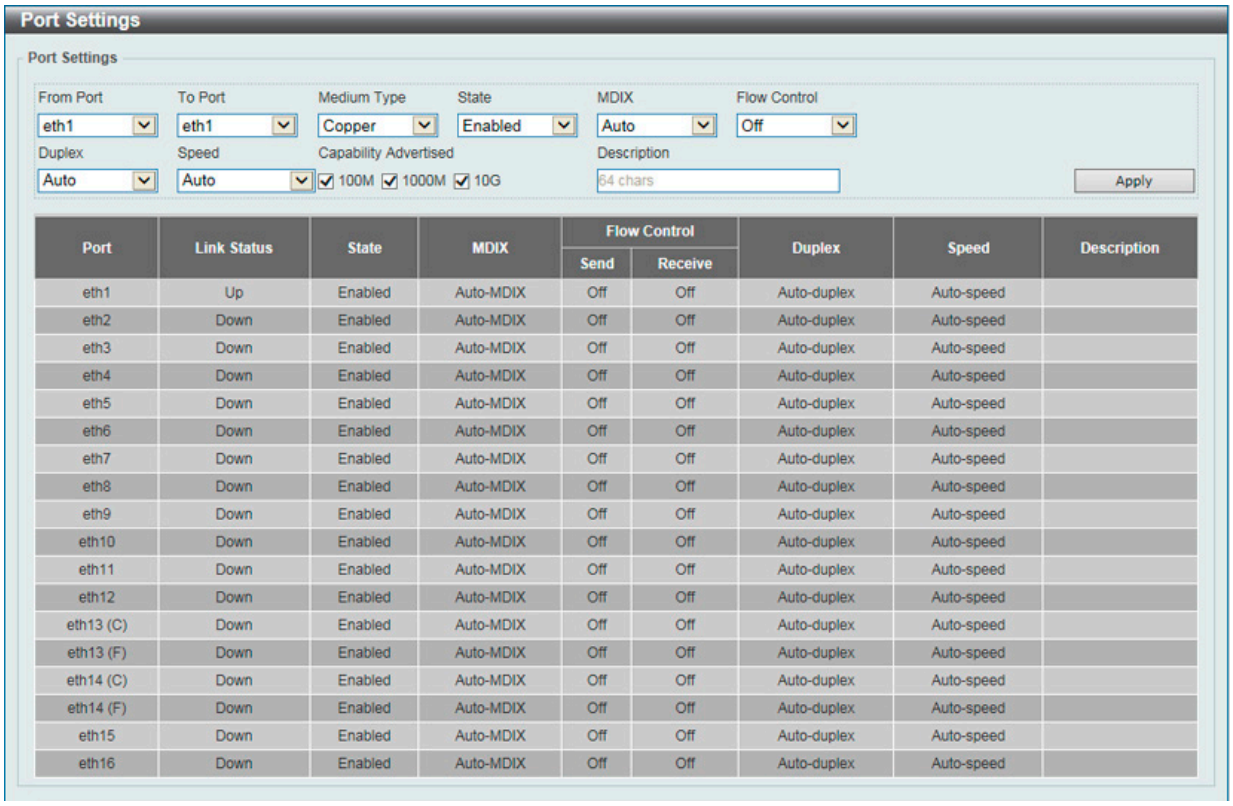

図 6-4　Port Settings 画面

画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート範囲を設定します。
Medium Type	コンボポートを使用する場合、使用するポートメディアを指定します。
State	物理ポートの有効 / 無効を指定します。 • Enabled - 選択した物理ポートが有効です。 • Disabled - 選択した物理ポートが無効です。
MDIX	• Auto - 最適なケーブル接続を自動的に設定します。 • Normal - ケーブル接続に Normal を選択します。 • Cross - ケーブル接続に Cross を選択します。 「Normal」を選択すると、MDI モードにあるポートはストレートケーブルを通して PC のネットワークボード、またはクロスケーブルで別のスイッチのポート（MDI モード）に接続することができます。「Cross」を選択すると、MDIX モードにあるポートはストレートケーブルで別のスイッチのポート (MDI モード) に接続することができます。
Flow Control	Full-Duplex では 802.3x フローコントロールを、Half-Duplex ではバックプレッシャーによる制御を自動で行います。「Enabled」（フロー制御あり）または「Disabled」（フロー制御なし）を選択します。「Auto」は自動的にいずれかを使用します。
Duplex	全二重 / 半二重モードの選択を行います。「Auto」「Full」から選択します。

項目	説明
Speed	「Speed」欄でポートの速度を選択します。ここでは指定したポートを指定した速度のみで接続するように手動で設定します。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 オプションには「Auto」「100M」「1000M」「1000M Master」「1000M Slave」、および「10G」があります。「Auto」以外のオプションのポート設定は固定となります。 スイッチは 2 つのタイプ（「1000M Master」および「1000M Slave」）のギガビット接続設定ができます。 マスタ設定 (1000M Master) によりポートはデュプレックス、さらに 2 つの接続している物理レイヤ間のマスタおよびスレーブを決定します。この関係は 2 つの物理レイヤ間のタイミングコントロールを確立するために必要です。タイミング制御は、ローカルソースによってマスタの物理層に設定されます。スレーブ設定 (1000M Slave) はループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わせます。一方の接続に「1000M Master」を設定すると、他方の接続は「1000M Slave」とする必要があります。その他の設定は両ポートのリンクダウンを引き起こします。
Capability Advertised	上記「Speed」が「Auto」に設定されている場合、オートネゴシエーションの間、本機能は有効になります。
Description	関連のポートについて 64 文字以内に概要を指定します。

「Apply」ボタンをクリックすると設定が更新されます。

Port Status（ポートステータス）

ポートの状態、設定について表示します。

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

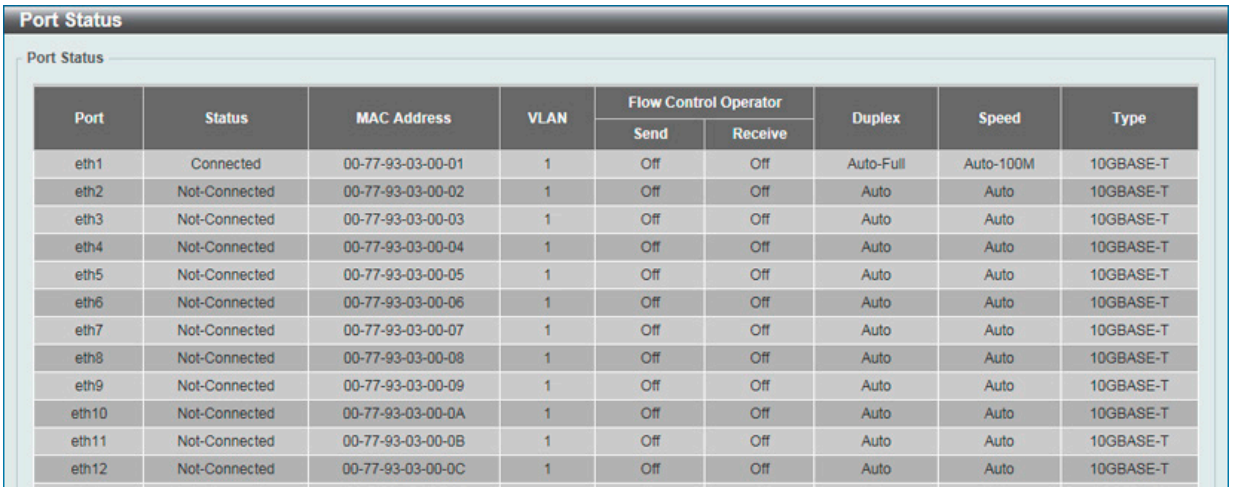

図 6-5　Port Status 画面

Error Disabled Settings（エラー無効設定）

エラー無効発生時の SNMP 通知送信について設定します。

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

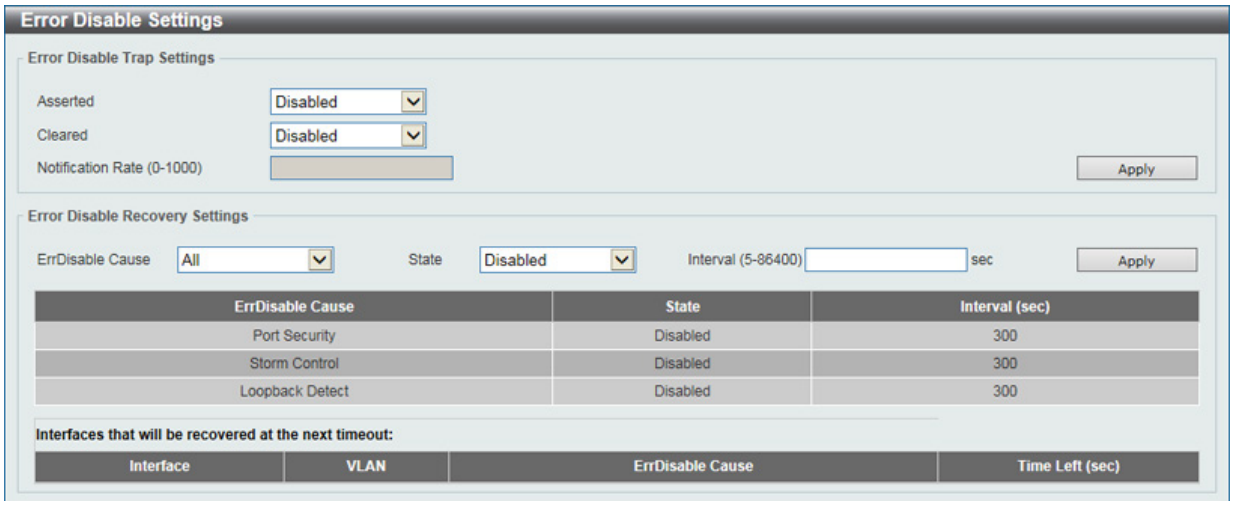

図 6-6　Error Disabled Settings 画面

画面には以下の項目があります。

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

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

「Apply」ボタンをクリックすると設定が更新されます。

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

項目	説明
ErrDisable Cause	エラー無効の原因を次から選択します。 「ALL」「Port Security」「Storm Control」「Loopback Detect」
State	指定した原因によるエラー無効ポートのの自動リカバリ機能を有効 / 無効にします。
Interval	ポートリカバリ実行の間隔時間を 5 から 86400（秒）で指定します。

「Apply」ボタンをクリックすると設定が更新されます。

Jumbo Frame（ジャンボフレーム設定）

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。ジャンボフレームは、1518 バイト以上のペイロードを持つイーサネットフレームです。本スイッチは最大 9216 バイトまでのジャンボフレームをサポートします。「Jumbo Frame Settings」画面では、スイッチでジャンボフレームを扱うことを可能にします。これによりオーバヘッド、処理時間、割り込みを確実に減らすことができます。

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

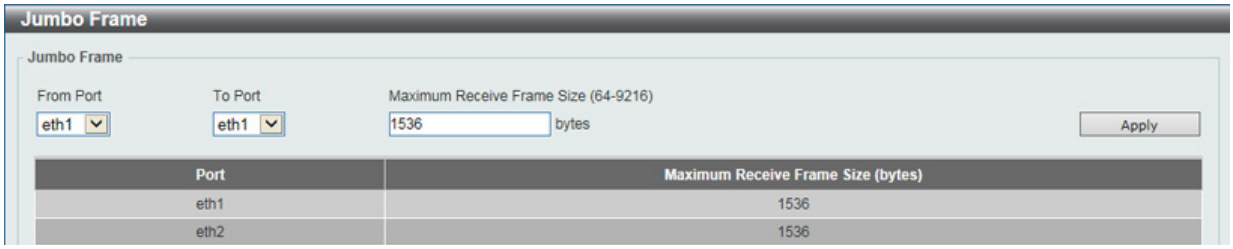

図 6-7　Jumbo Frame 画面

画面には以下の項目があります。

項目	説明
From Port/To Port	本設定を適用するポート範囲を設定します。
Maximum Receive Frame Size	スイッチのジャンボフレーム機能の最大値を指定します。 64 から 9216（バイト）まで指定可能で、初期値は 1536 バイトです。

「Apply」ボタンをクリックすると設定が更新されます。

System Log（システムログ）

System Log Settings（システムログ設定）

スイッチのシステムログ設定を行います。

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

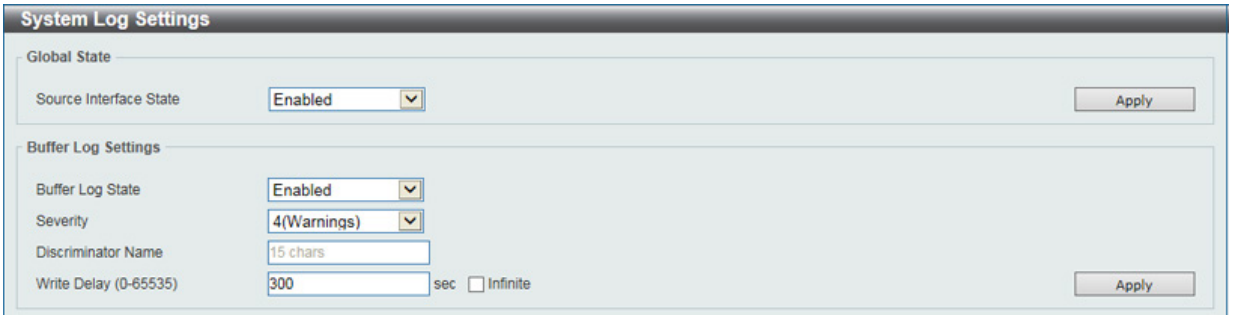

図 6-8　System Log Settings 画面

System Log Settings 画面には次の項目があります。

Global State（グローバルステート）

項目	説明
Source Interface State	ソースインタフェースをグローバルに有効 / 無効に指定します。

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

Buffer Log Settings（バッファログ設定）

項目	説明
Buffer Log State	「Enable」「Disabled」「Default」から選択します。 「Default」を選択するとバッファログのグローバルステートは初期設定のまま動作します。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。
Write Delay	フラッシュにロギングバッファを定期的に書き込む間隔を指定します。0 から 65535（秒）の間で指定できます。初期値は 300 秒です。「Infinite」にチェックを入れると本機能は無効になります。

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

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

システムログディスクリミネーターの設定、設定内容の表示を行います。

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

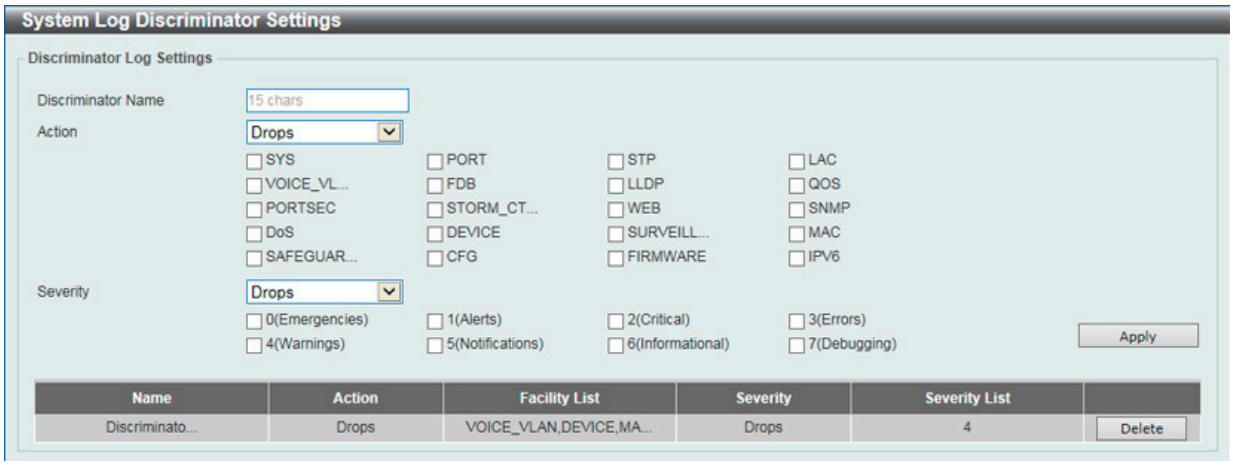

図 6-9　System Log Discriminator Settings 画面

本画面には次の項目があります。

項目	説明
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。
Action	機能が実行する動作内容と選択した動作に関連する機能の種類を選択します。「Drops」「Includes」から選択します。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。

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

「Delete」ボタンをクリックすると指定のエントリが削除されます。

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

システムログはイベントの記録と管理、エラーと情報のメッセージをレポートします。

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

図 6-10　System Log Server 画面

本画面には次の項目があります。

項目	説明
Host IPv4 Address	ログを記録するサーバの IPv4 アドレスを設定します。
Host IPv6 Address	ログを記録するサーバの IPv6 アドレスを設定します。
UDP Port	ログを送信するサーバの UDP ポートを設定します。初期値は 514 です。 値は「514」、または「1024」から「65535」で指定します。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。
Facility	プルダウンメニューを使用して「0」から「23」までの間を選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。

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

「Delete」ボタンをクリックすると指定のエントリが削除されます。

System Log（システムログの設定）

システムログの閲覧 / 消去を行います。本テーブルに表示される最大エントリ数は 1,000 件になります。インデックス番号は 90,000 まで割り当てられます。このログが最大値に達すると古いエントリから削除されていきます。

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

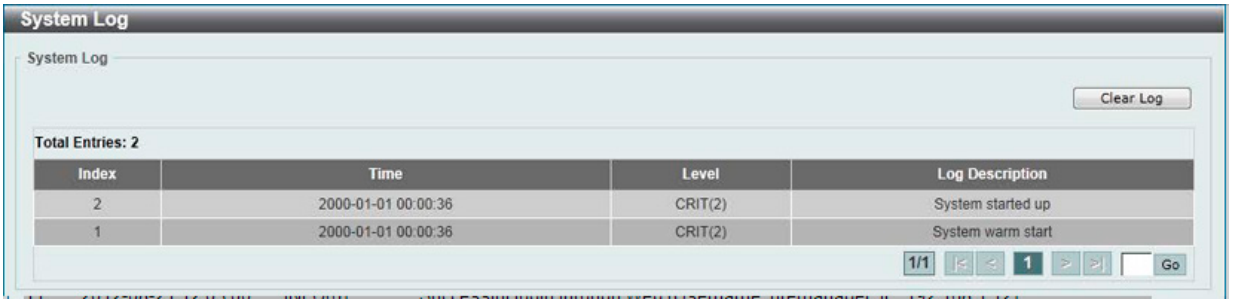

図 6-11　System Log 画面

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

System Attack Log（システムアタックログ）

攻撃を受けたシステムログの閲覧 / 消去を行います。本テーブルに表示される最大エントリ数は 1,000 件になります。インデックス番号は 90,000 まで割り当てられます。このログが最大値に達すると古いエントリから削除されていきます。

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

図 6-12　System Attack Log 画面

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

Time and SNTP（時間設定・SNTP 設定）

SNTP（Simple Network Time Protocol）は、コンピュータのクロックにスイッチを同期させるために使用されます。
地域時刻を提供するサービスへアクセスし、SNTP サーバのサブネットとクライアントを管理、各々のシステム時刻の調整を行う総合的なメカニズムになります。

Clock Settings（時間設定）

スイッチの時間設定を行います。

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。

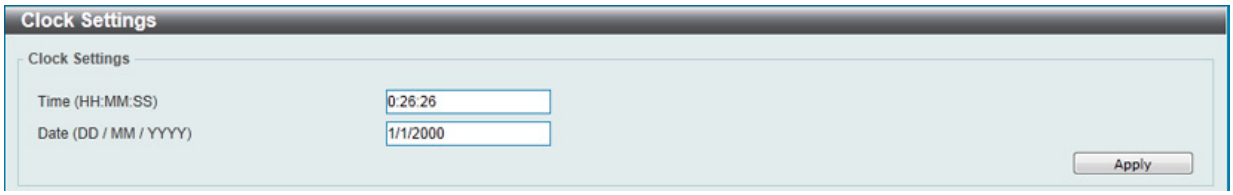

図 6-13　Clock Settings 画面

画面には以下の項目があります。

項目	説明
Time (HH:MM:SS)	現在時刻を入力します。（時 / 分 / 秒）
Date (DD / MM / YYYY)	現在の日付を入力します。（日 / 月 / 年）

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

Time Zone Settings（タイムゾーン設定）

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

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

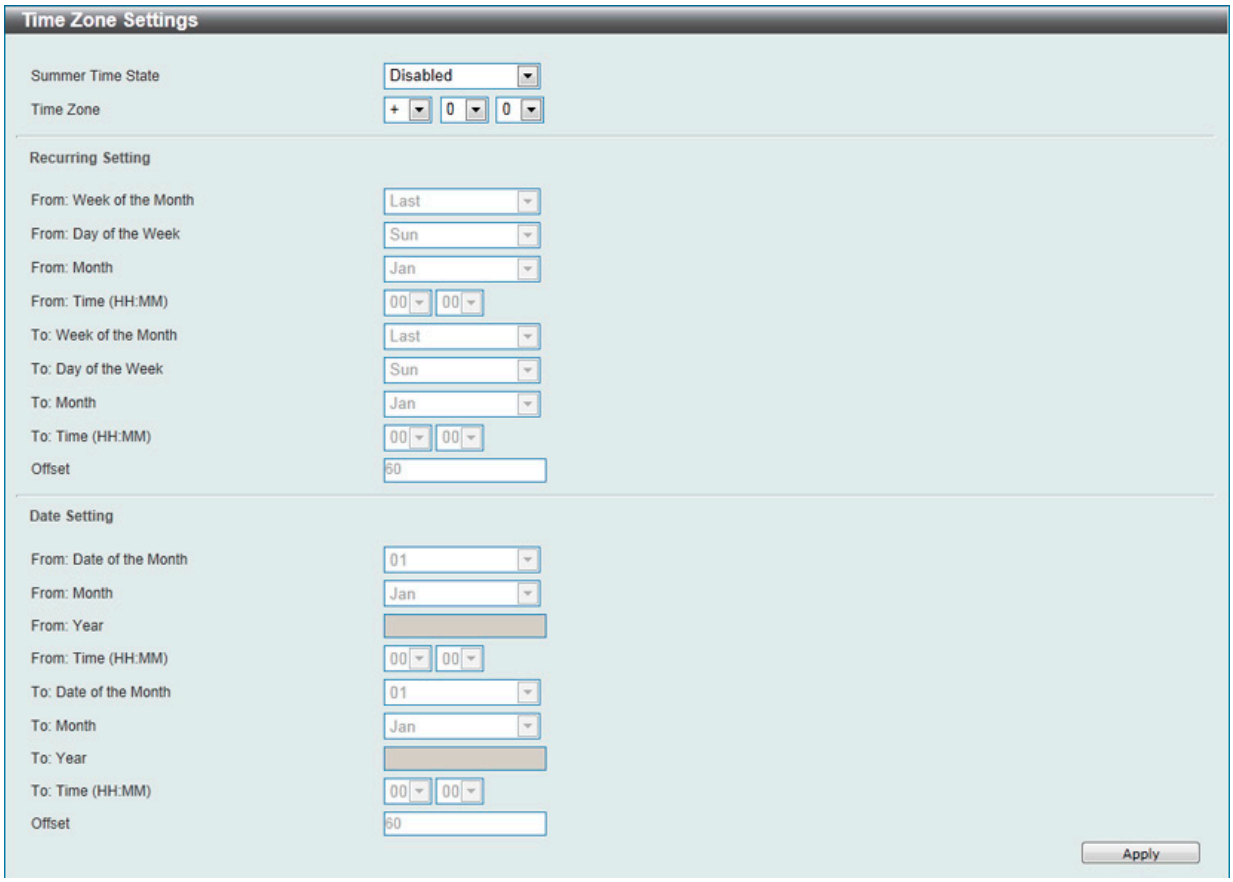

図 6-14　Time Zone Settings 画面

以下に、画面の各項目を示します。

項目	説明
Summer Time State	デバイスに設定するサマータイムの種類を設定します。 • Disabled - サマータイムを無効にします。（初期値） • Recurring Setting - サマータイムを周期的に有効にします。このオプションでは開始と終了のタイミングを指定月の指定週で設定する必要があります。 • Date Setting - サマータイムを日付指定で有効にします。このオプションでは開始と終了の日付を設定する必要があります。
Time Zone	タイムゾーンを設定します。 UTC（世界標準時刻）との時差を以下のドロップダウンリストから選択してください。 • 左側のドロップダウンリスト： UTC と比較して進んでいる場合は「+」、遅れている場合は「-」を選択します。 • 中央のドロップダウンリスト： UTC と比較して進んでいるまたは遅れている「時間」を選択します。 • 右側のドロップダウンリスト： UTC と比較して進んでいるまたは遅れている「分」を選択します。 （例）UTC と比較して 9 時間 00 分進んでいる場合は、左から順に「+」「9」「0」を選択します。
Recurring Setting	
Recurring Setting モードを使用すると、サマータイムの設定を指定した期間で自動的に調整できるようになります。例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。	
From: Week Of The Month	月の第何週から DST が始まるかを設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
From: Day Of Week	サマータイムが開始する曜日を指定します。Sun、Mon、Tue、Web、Tues、Fri、Sat
From: Month	サマータイムが開始する月を指定します。Jan、Feb、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec
From: Time (HH:MM)	サマータイムが開始する時間を指定します。
To: Week Of The Month	月の第何週でサマータイムが終わるかを設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
To: Day Of Week	サマータイムが終了する曜日を指定します。
To: Month	サマータイムが終了する月を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。初期値は 60（分）です。オフセットの範囲は「30」「60」「90」「120」から選択可能です。
Date Setting	
From: Date of the Month	サマータイムが始まる月日を指定します。
From: Month	サマータイムが開始する月を指定します。（毎年）
From: Day	サマータイムが開始する日を指定します。（毎年）
From: Time In HH MM	サマータイムが開始する時間を指定します。（毎年）
To: Date of the Month	サマータイムが修了する月日を指定します。
To: Month	サマータイムが終了する月を指定します。（毎年）
To: Day	サマータイムが終了する日を指定します。（毎年）
To: Time In HH MM	サマータイムが終了する時間を指定します。（毎年）
Offset	サマータイムに追加する時間を指定します。初期値は 60（分）です。オフセットの範囲は「30」「60」「90」「120」から選択可能です。

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

SNTP Settings（SNTP 設定）

スイッチに時刻を設定します。

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。

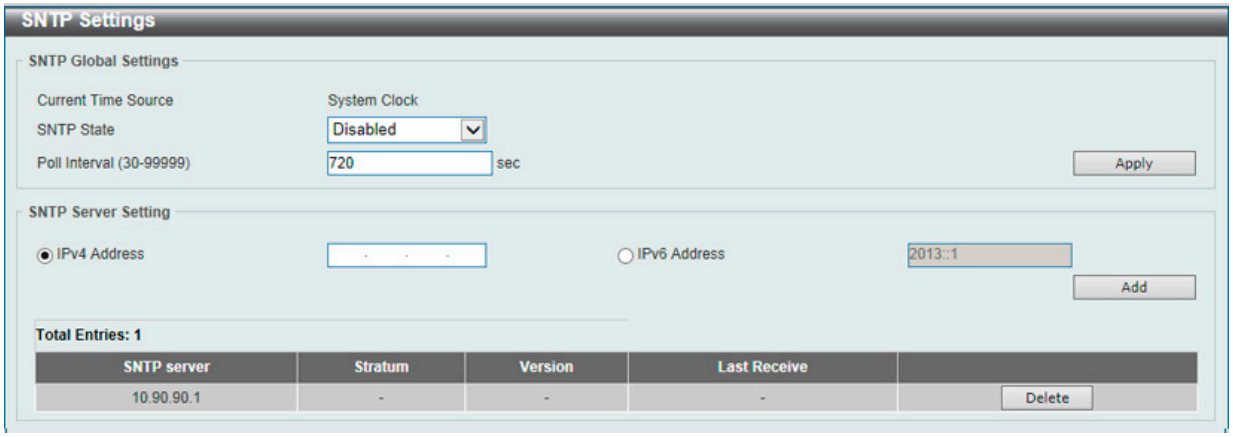

図 6-15　SNTP Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
SNTP Global Settings	
Current Time Source	現在の日付と時刻の情報源を表示します。
SNTP State	SNTP を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Poll Interval	同期する間隔（秒）を指定します。 「30」から「99999」（秒）で指定します。 初期値は「720 秒」です。
SNTP Server Settings	
IPv4 Address	SNTP 情報の取得元であるサーバの IP アドレスを設定します。
IPv6 Address	SNTP 情報の取得元であるサーバの IPv6 アドレスを設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Add」をクリックして SNTP サーバを追加します。
「Delete」をクリックして指定のエントリを削除します。

Time Range（タイムレンジ設定）

スイッチのタイムレンジを設定します。

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

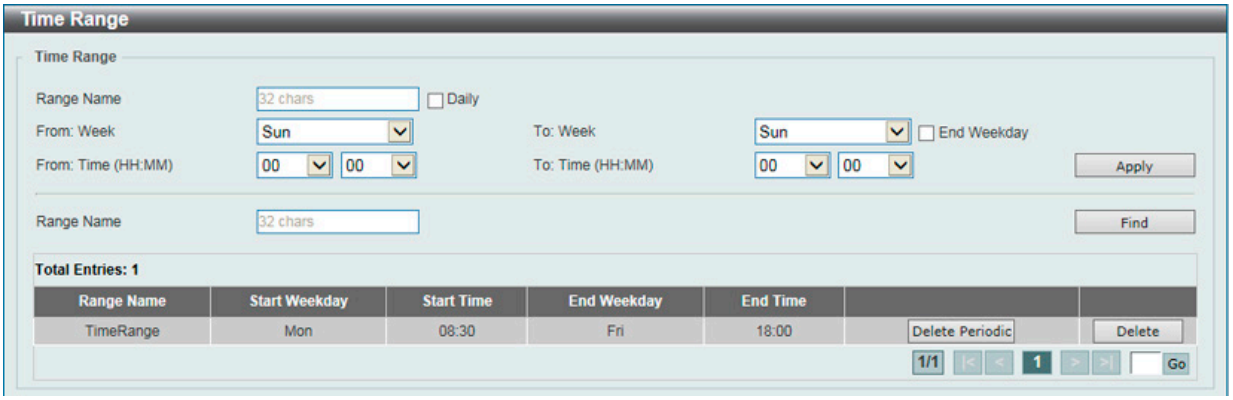

図 6-16　Time Range 画面

以下の項目を設定することができます。

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

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

エントリの削除

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

第 7 章　Management（スイッチの管理）

本章でスイッチの管理を行います。

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	参照ページ
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。	45
Password Encryption（パスワード暗号化）	パスワードの暗号を設定ファイルに保存します。	46
SNMP Settings（SNMP 設定）	SNMP を利用してゲートウェイ、ルータ、およびその他のネットワークデバイスの設定状態を確認または変更します。また、SNMP を利用してスイッチやスイッチ群、またはネットワークに対し、正常な動作を行うためのシステム設定、パフォーマンスの監視、問題の検出を行います。	46
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。	53
Web Settings（Web 設定）	スイッチの Web ベースマネジメントに使用される TCP ポート番号を指定します。	57
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します。	57
File System（ファイルシステム）	フラッシュファイルシステムの設定を行います。	58
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）	D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。	59

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。

注意 初期値ではユーザアカウントとして「admin」（パスワード：admin）が設定されています。

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

- User（基本ユーザ）- ユーザアカウントの中で低い優先値になります。このアカウントの目的は基本的なシステムのチェックになります。
- Administrator - システム情報を含むすべての設定に関する閲覧、変更の権限があります。

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

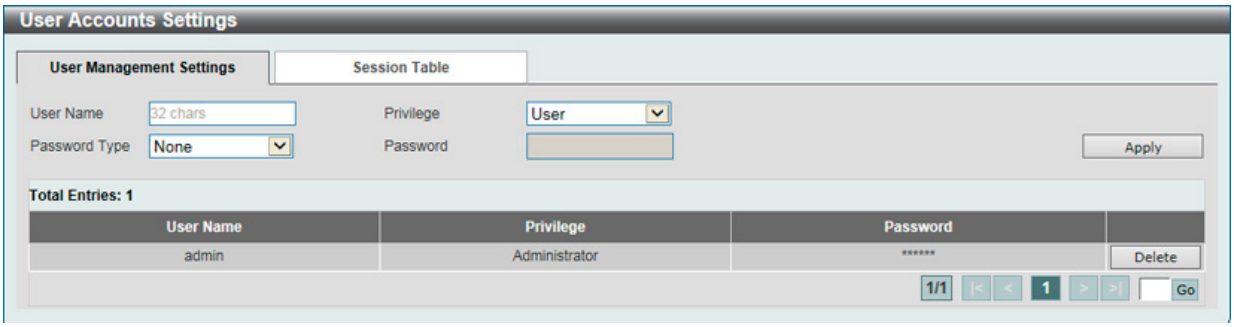

図 7-1　User Accounts Settings - User Management Settings 画面

画面には次の項目があります。

項目	説明
User Name	ユーザ名を定義します。（半角英数字 32 文字以内）
Privilege	アカウントの権限レベルを指定します。
Password Type	アカウントで使用する暗号化の方法を「None」「Plain Text」「Encrypted」から選択します。 「Encrypted」を選択した場合のみ、「SHA-1」で 35 文字の暗号パスワードを入力することができます。これは入力時に暗号化されていない「プレーンテキスト」パスワードは、「暗号化フォーマット」へ暗号化することができないことを意味します。 「Password Encryption」については「パスワード暗号化」を参照ください。
Password	アカウントで使用するパスワードを入力します。

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

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

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

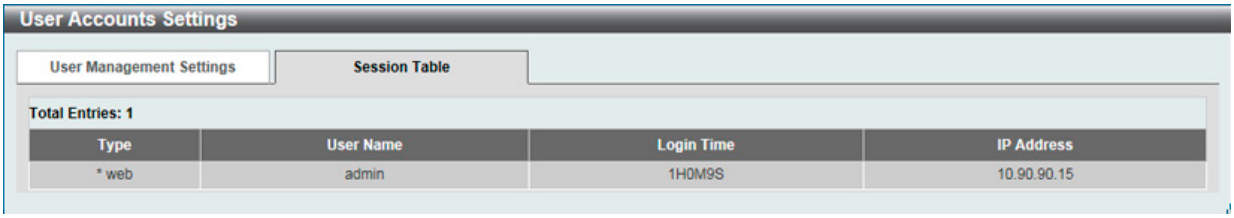

図 7-2　User Accounts Settings - Session Table 画面

Password Encryption（パスワード暗号化）

パスワードの暗号を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。

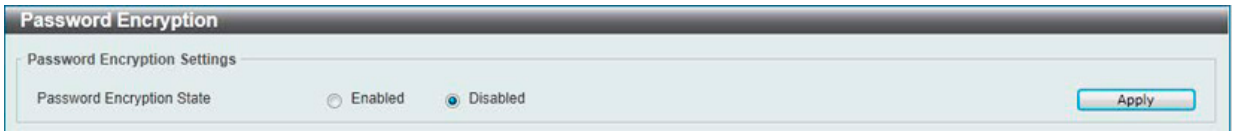

図 7-3　Password Encryption 画面

画面には次の項目があります。

項目	説明
Password Encryption State	パスワードの暗号化のコンフィグファイル保存ついての有効 / 無効を設定します。

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

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、ネットワークデバイスの管理や監視を行います。ネットワーク管理デバイスは、SNMP を利用してゲートウェイ、ルータ、およびその他のネットワークデバイスの設定状態を確認または変更します。また、SNMP を利用してスイッチやスイッチ群、またはネットワークに対し、正常な動作を行うためのシステム設定、パフォーマンスの監視、問題の検出を行います。

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

本スイッチは、SNMP バージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）をサポートしています。初期設定では SNMP 機能は無効になっているため、有効にする必要があります。SNMP 機能を有効にしたら、スイッチの監視と制御に使用する SNMP バージョンを選択します。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

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

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

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

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

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

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

トラップ

トラップとは、スイッチ上で発生したイベントを、ネットワーク管理者に警告するためのメッセージです。イベントには、再起動（誰かが誤ってスイッチの電源を切ってしまった）などの重大なものから、ポートの状態変化を知らせる軽微なものまで幅広い種類があります。スイッチはトラップを生成してトラップ受信者（またはネットワークマネージャ）に送信します。

MIB

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

DXS-1100 シリーズは、スイッチの環境に合わせた柔軟性のある SNMP 管理機能を採用しています。SNMP 管理機能は、ネットワークの要求やネットワーク管理者の好みに合わせてカスタマイズすることができます。SNMP バージョンの選択は、「SNMP Group Table」で行うことができます。DXS-1100 シリーズは、SNMP バージョン 1、2c、および 3 をサポートします。管理者は、スイッチの監視と制御にどの SNMP バージョンを使用するかを指定できます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

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

SNMP Global Settings（SNMP グローバル設定）

SNMP グローバル設定とトラップ設定を行います。

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

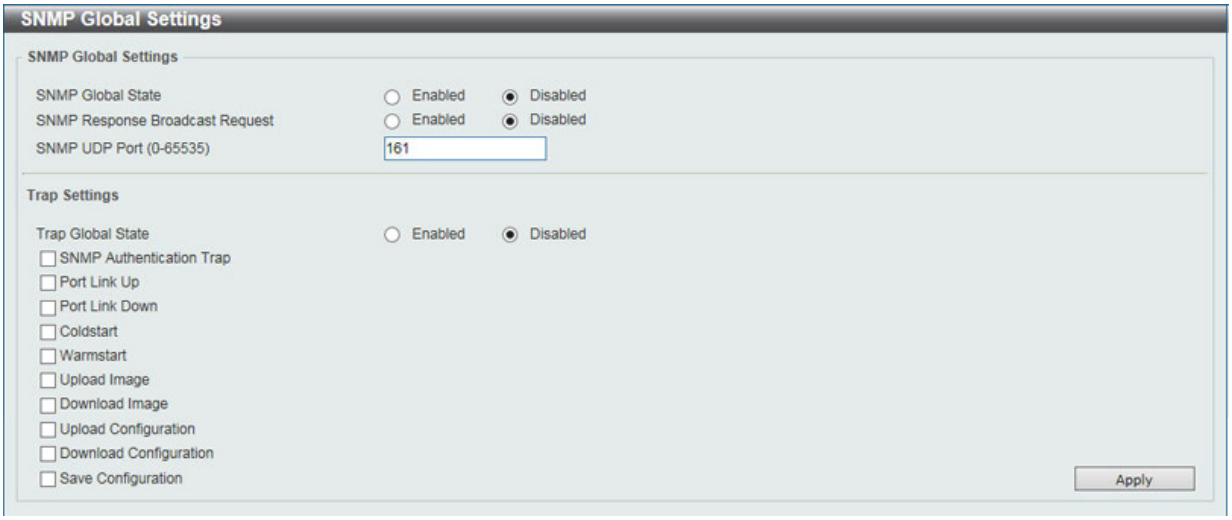

図 7-4　SNMP Global Settings 画面

以下の項目が使用されます。

SNMP Global Settings（SNMP グローバル設定）

項目	説明
SNMP Global State	「SNMP」機能の有効 / 無効を選択します。
SNMP Response Broadcast Request	「SNMP GetRequest」パケットのブロードキャストに対応するサーバを有効 / 無効に指定します。
SNMP UDP Port	SNMP UDP ポート番号を指定します。

Trap Settings（トラップ設定）

項目	説明
Trap Global State	「SNMP」トラップを有効 / 無効にします。
SNMP Authentication Trap	SNMP 認証失敗の通知送信の設定を行います。認証失敗トラップは、機器が正しく認証されていない SNMP メッセージを受信した時に実行されます。認証方法は使用している SNMP のバージョンによります。SNMPv1 または SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。SNMPv3 の場合は、間違った SHA/MD5 キーによってパケットが構成されている時に認証に失敗します。
Port Link Up	ポートリンクアップ通知送信の設定を行います。リンクアップトラップは機器がリンクアップを認識すると実行します。
Port Link Down	ポートリンクダウン通知送信の設定を行います。リンクダウントラップは機器がリンクダウンを認識すると実行します。
Coldstart	「Coldstart Traps」を有効 / 無効にします。
Warmstart	「Warmstart Traps」を有効 / 無効にします。
Upload Image	イメージアップロードが成功した時に通知を送信します。
Download Image	イメージダウンロードが成功した時に通知を送信します。
Upload Configuration	コンフィグアップロードが成功した時に通知を送信します。
Download Configuration	コンフィグダウンロードが成功した時に通知を送信します。
Save Configuration	コンフィグが保存された時に通知を送信します。

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

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

スイッチの SNMP リンクチェンジトラップを有効または無効にします。

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

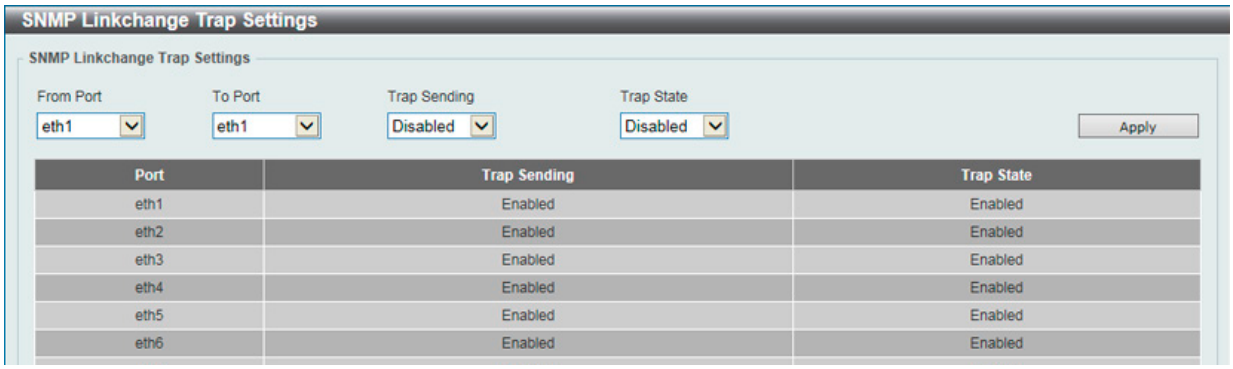

図 7-5　SNMP Linkchange Traps Settings 画面

以下の項目が使用されます。

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

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

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

コミュニティ名に対しビュー（アクセスできる MIB オブジェクトの集合）を割り当て、リモート SNMP マネージャがどの MIB オブジェクトにアクセスするかを定義するために使用します。SNMP ユーザ（「SNMP User Table」で設定）と本画面で登録するビューは、「SNMP Group Table」によって作成する SNMP グループによって関連付けます。

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

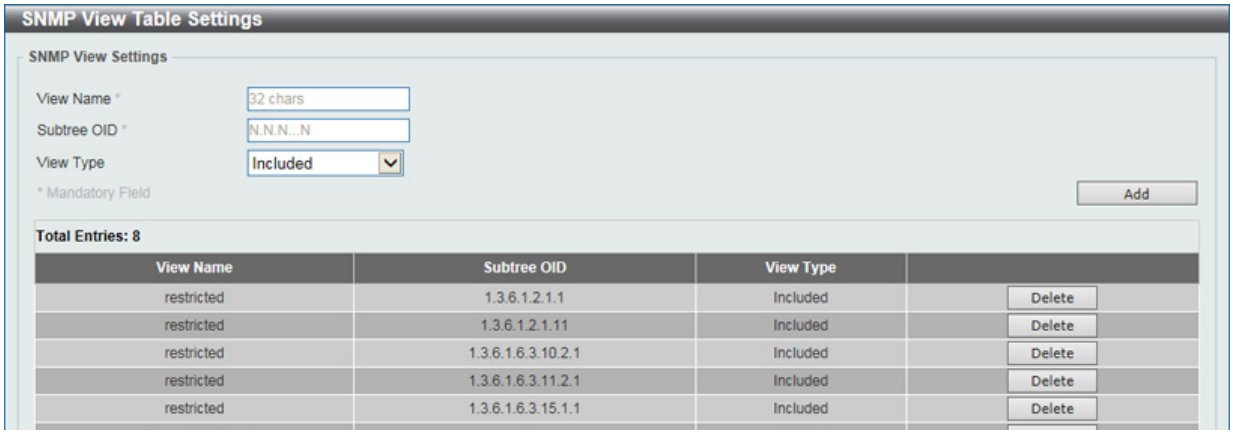

図 7-6　SNMP View Table 画面

エントリの削除

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

エントリの作成

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

以下の項目が使用されます。

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

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

「SNMP Community Table」は、SNMP コミュニティ名を登録し、SNMP マネージャとエージェントの関係を定義するために使用します。コミュニティ名は、スイッチ上のエージェントへのアクセスを行う際のパスワードの役割をします。以下の特性はコミュニティ名と関係します。

- コミュニティ名を使用して、スイッチ上の SNMP エージェントにアクセスを行う SNMP マネージャの IP アドレスが掲載されるアクセスリスト。
- MIB オブジェクトのすべてのサブセットを定義する MIB ビューは SNMP コミュニティにアクセス可能である。
- SNMP コミュニティにアクセス可能な MIB オブジェクトが Read/Write または Read-only レベルである。

コミュニティエントリを設定するためには、**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 7-7　SNMP Community Table 画面

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

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

エントリの作成

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

エントリの削除

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

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

SNMP ユーザ（「SNMP User Table」で設定）のテーブルマップで構成された SNMP グループを表示します。

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

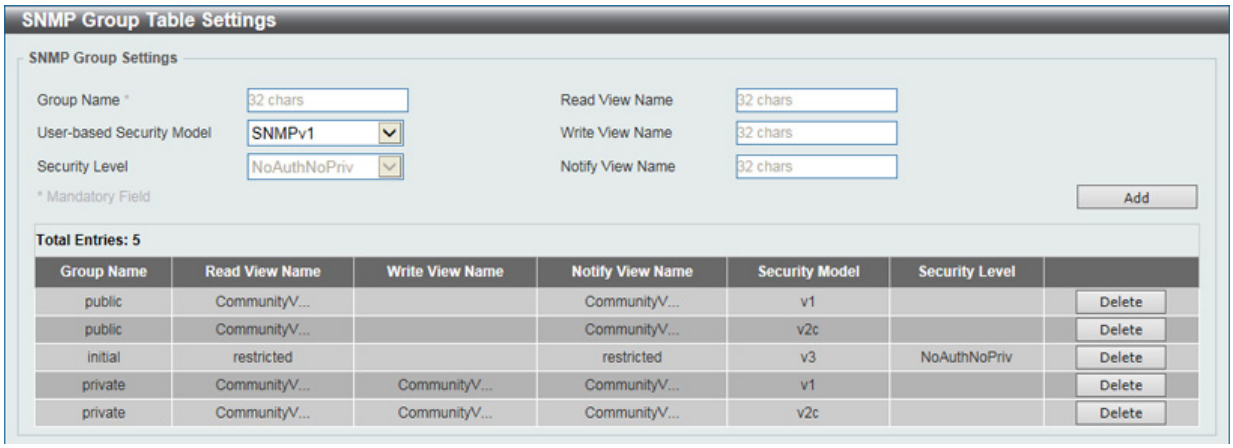

図 7-8　SNMP Group Table 画面

「SNMP Group Table」画面のエントリの削除

エントリの行の「Delete」ボタンをクリックします。

「SNMP Group Table」画面への新規エントリの追加

上記画面に情報を入力し、「Add」ボタンをクリックします。

以下の項目が使用されます。

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

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

エンジン ID は、SNMP バージョン 3 で使用される場合に定義される固有の識別名です。識別名は半角英数字の文字列で表記され、スイッチ上の SNMP エンジン（エージェント）を識別するために使用します。

スイッチの SNMP エンジン ID を表示します。

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

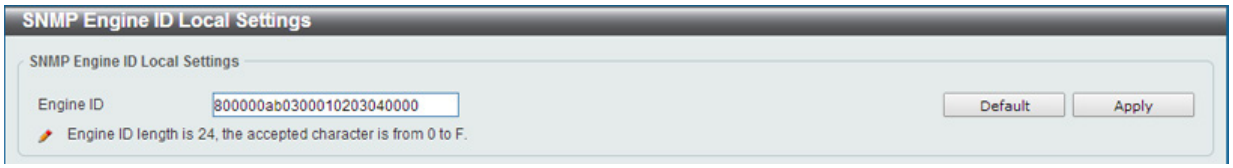

図 7-9　SNMP Engine ID 画面

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

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

スイッチに現在設定されているすべての SNMP ユーザが表示されます。

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

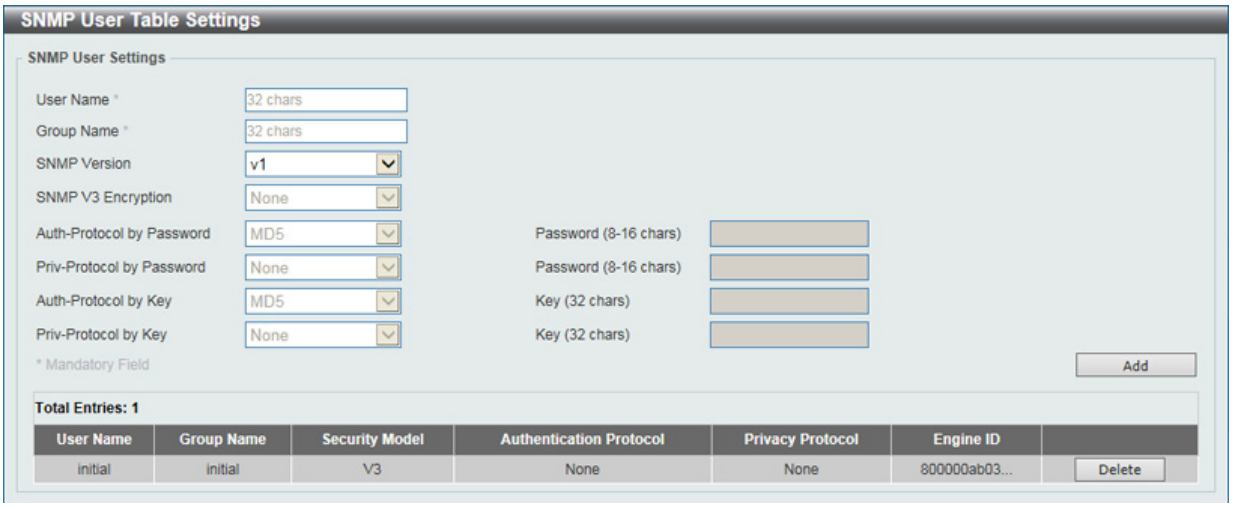

図 7-10　SNMP User Table 画面

エントリの削除

エントリの行の「Delete」ボタンをクリックします。

エントリの新規登録

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

上記画面中の項目を以下に示します。

項目	説明
User Name	32 文字までの半角英数字。SNMP ユーザを識別します。
Group Name	作成した SNMP グループが SNMP メッセージを要求するために使用される名前です。
SNMP Version	• v1 - SNMP バージョン 1 が使用されています。 • v2c - SNMP バージョン 2 が使用されています。 • v3 - SNMP バージョン 3 が使用されています。
SNMP v3 Encryption	SNMP v3 に対して暗号化を有効にします。本項目は「SNMP Version」で「v3」を選択した場合に有効になります。 • None - ユーザ認証は使用しません。 • Key - HMAC-MD5 アルゴリズムまたは HMAC-SHA-96 アルゴリズムレベルのユーザ認証を行います。 • Password - HMAC-SHA-96 アルゴリズムレベルのパスワードか HMAC-MD5-96 パスワードによる認証を行います。
Auth-Protocol	本項目は「SNMP Version」で「v3」が選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。本項目を選択後、「Password」/「Key」にパスワードを入力します。 • MD5 - HMAC-MD5-96 認証レベルが使用されます。 • SHA - HMAC-SHA 認証プロトコルが使用されます。
Priv-Protocol	本項目は「SNMP Version」で「v3」が選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 • None - 認証プロトコルは使用されていません。 • DES - CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されています。本項目を選択後、「Password」/「Key」にパスワード（半角英数字 8-16 文字）を入力します。

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

SNMP トラップの送信先を登録します。

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

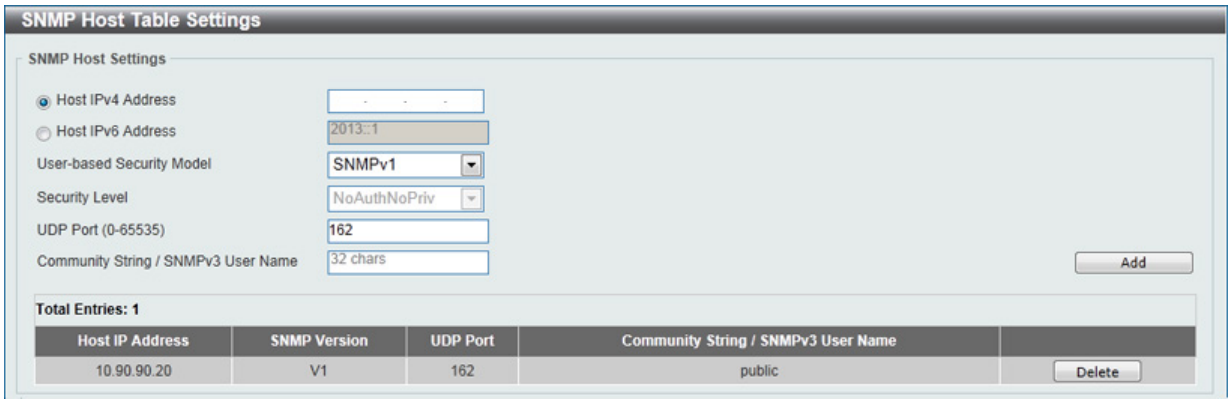

図 7-11　SNMP Host Table 画面

エントリの新規登録

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

以下の項目を設定します。

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv6 アドレスを入力します。
User-based Security Model	• SNMPv1 : SNMP バージョン 1 が使用されます。 • SNMPv2c : SNMP バージョン 2c が使用されます。 • SNMPv3 : SNMP バージョン 3 が使用されます。
Security Level	• NoAuthNoPriv : NoAuth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。 • AuthNoPriv : V3-Auth-NoPriv セキュリティレベルの SNMP バージョン 3 が使用されます。 • AuthPriv : V3-Auth-Priv セキュリティレベルの SNMP バージョン 3 が使用されます。
UDP Port	UDP ポート番号を入力します。UDP ポート番号の初期トラップは 162 です。UDP ポート範囲は 0 から 65535 です。いくつかのポート番号は他のプロトコルと衝突する可能性があります。
Community String/ SNMPv3 User Name	コミュニティ名または SNMPv3 ユーザ名を入力します。

エントリの削除

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

RMON（RMON 設定）

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

RMON Global Settings（RMON グローバル設定）

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

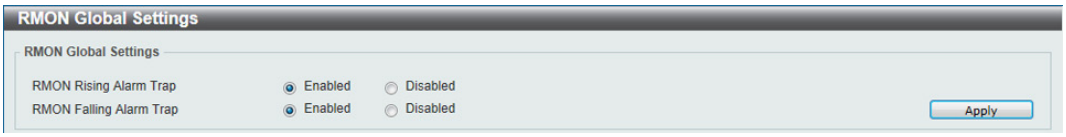

図 7-12　RMON Global Settings 画面

以下の項目が使用されます。

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

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

RMON Statistics Settings（RMON 統計情報）

RMON 統計情報を表示、設定します。

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

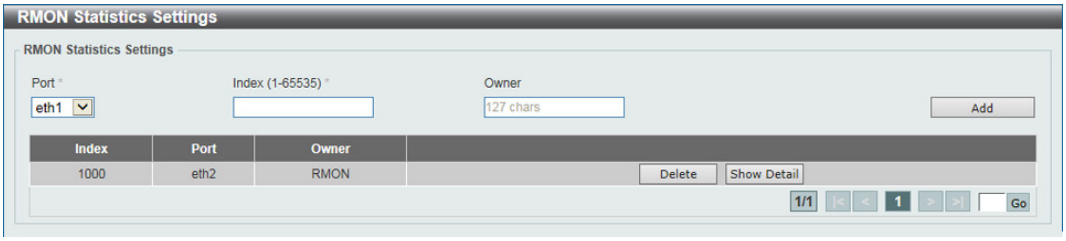

図 7-13　RMON Statistics Settings 画面

以下の項目が使用されます。

項目	説明
Port	RMON 情報を取得したポートを指定します。
Index (1 - 65535)	RMON イーサネット統計情報エントリの番号を指定します。
Owner	RMON 情報を要求した RMON ステーションまたはユーザを表示します。

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

統計情報の登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

統計情報の削除を行う場合

「Delete」をクリックします。

指定ポートの統計情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

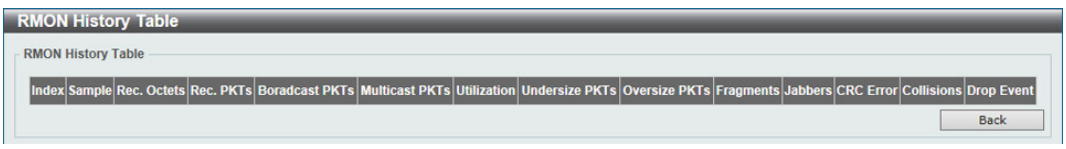

図 7-14　RMON Statistics Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

RMON History Settings（RMON ヒストリ設定）

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

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

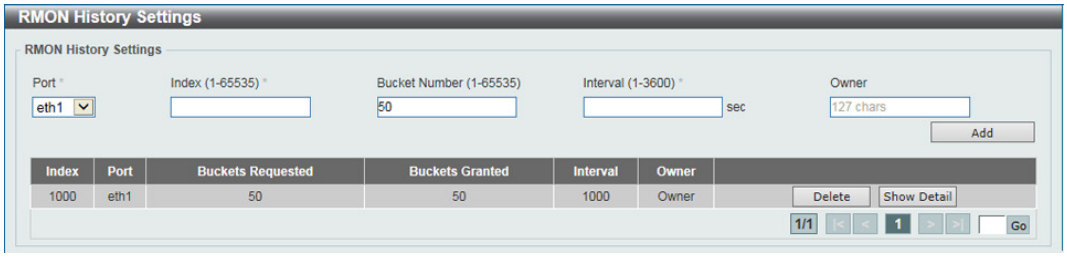

図 7-15　RMON History Settings 画面

以下の項目が使用されます。

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

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

履歴情報の登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

履歴情報の削除を行う場合

「Delete」をクリックします。

指定ポートの履歴情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

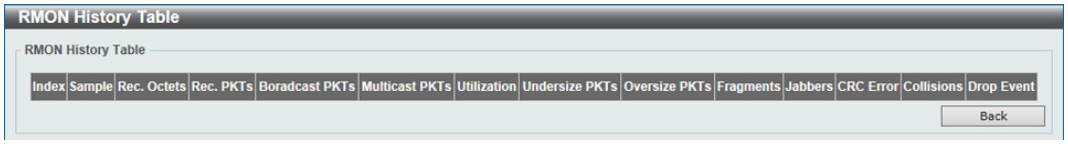

図 7-16　RMON History Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

RMON Alarm Settings（RMON アラーム設定）

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

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

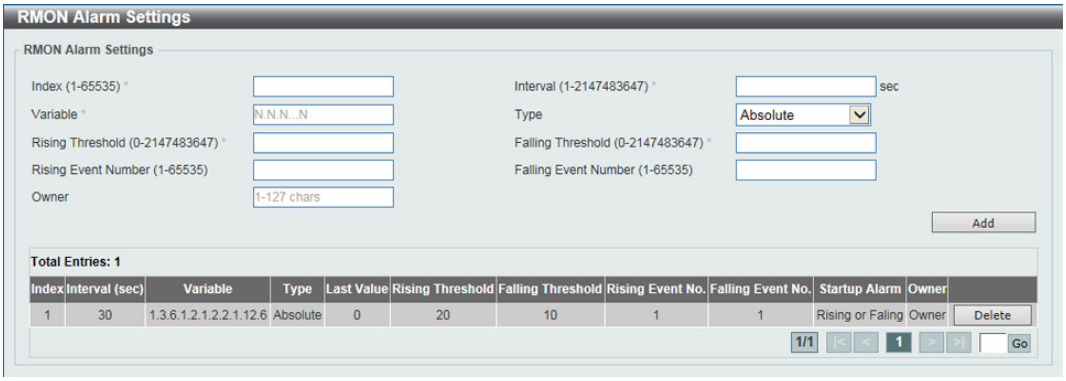

図 7-17　RMON Alarm Settings 画面

以下の項目が使用されます。

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

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

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

「Delete」をクリックします。

RMON Event Settings（RMON イベント設定）

RMON イベント統計情報の定義、編集、および参照を行います。

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

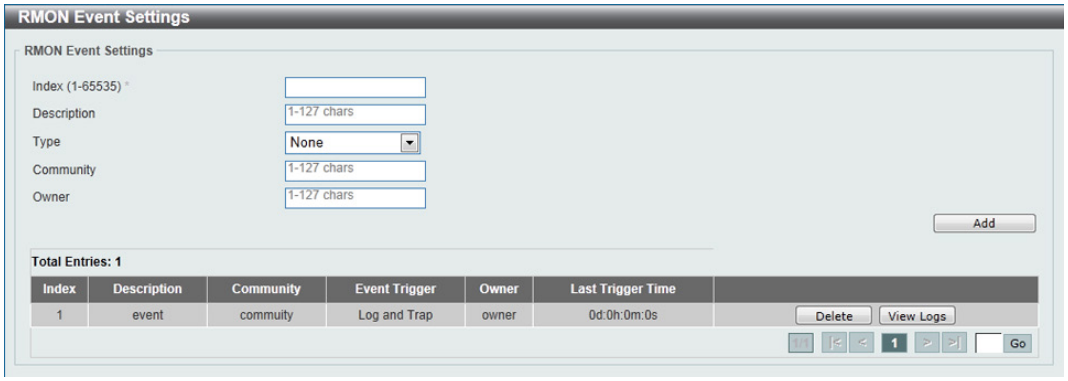

図 7-18　RMON Event Settings 画面

以下の項目が使用されます。

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

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

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

「Delete」をクリックします。

指定エントリのログ情報を表示する場合

「View Logs」をクリックします。以下の画面が表示されます。

図 7-19　Event Logs Table 画面

「Back」をクリックすると前ページへ移動します。

Web Settings（Web 設定）

スイッチの Web 設定をします。

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

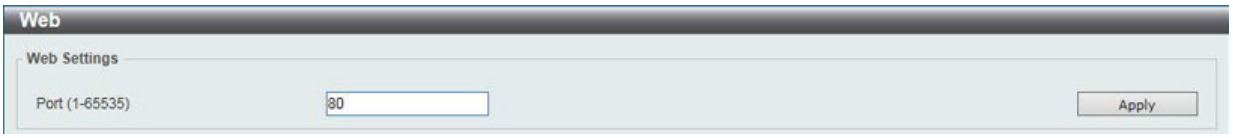

図 7-20　Web Settings 画面

以下の項目が使用されます。

Web 設定

項目	説明
Port (1-65535)	スイッチの Web ベースマネジメントに使用される TCP ポート番号。Web プロトコルに通常使用される TCP ポートは 80 です。

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

Session Timeout（セッションタイムアウト）

セッションタイムアウトの設定をします。

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

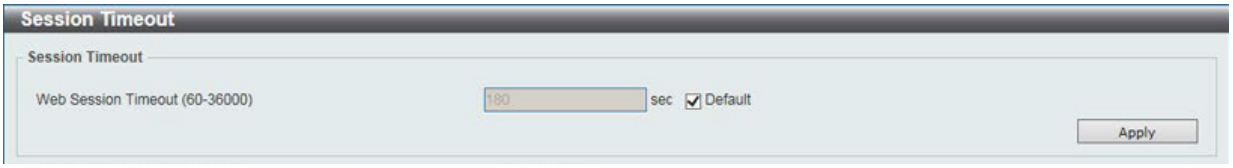

図 7-21　Session Timeout 画面

以下の項目が使用されます。

項目	説明
Web Session Timeout	Web セッションのタイムアウト時間（秒）を設定します。「Default」にチェックを入れると初期値に戻ります。60 から 36000（秒）で設定可能です。初期値は 180 秒です。

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

File System（ファイルシステム）

フラッシュファイルシステムを使用する理由

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

使用するシステムにおけるフラッシュファイルシステム

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

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

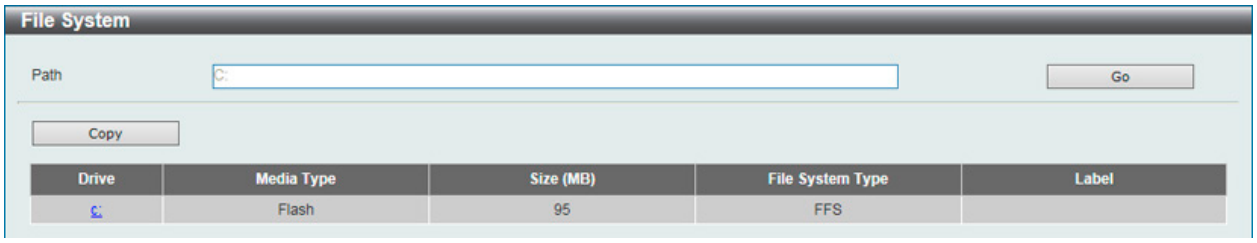

図 7-22　File System 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Path	パスの文字列を入力します。

「Path」に現在のパスを入力し、「Go」ボタンをクリックすると入力したパスに遷移します。
「C:」リンクをクリックすると、「C:」ドライブに遷移します。

「C:」リンクをクリックした後、次の画面が表示されます。

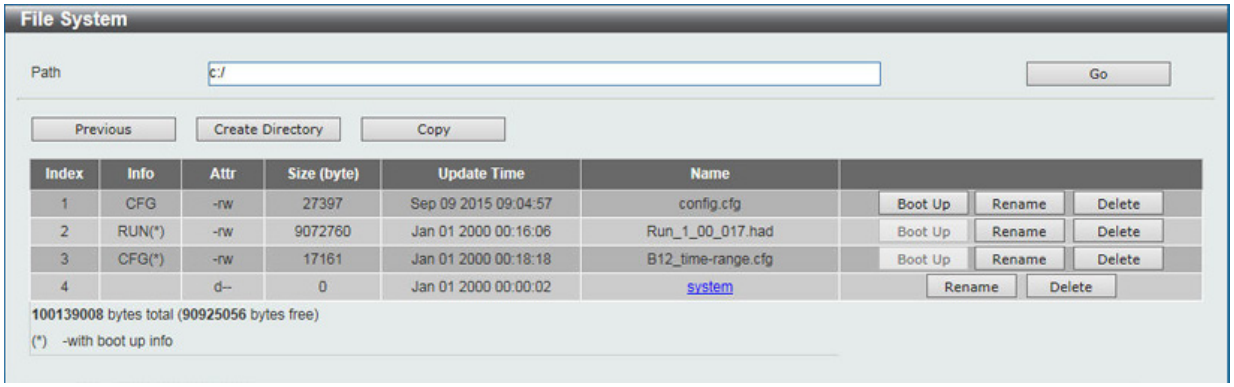

図 7-23　Flash File System Setting – Search for Drive 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Previous	前のページに戻ります。
Create Directory	スイッチのファイルシステムに新しいディレクトリを作成します。
Copy	指定ファイルをスイッチにコピーします。
Boot Up	起動用のブートアップイメージとして指定したランタイムイメージを設定します。
Rename	指定ファイルを変更します。
Delete	ファイルシステムから指定ファイルを削除します。

ファイルのコピー

1. 「Copy」ボタンをクリックすると、以下の画面が表示されます。

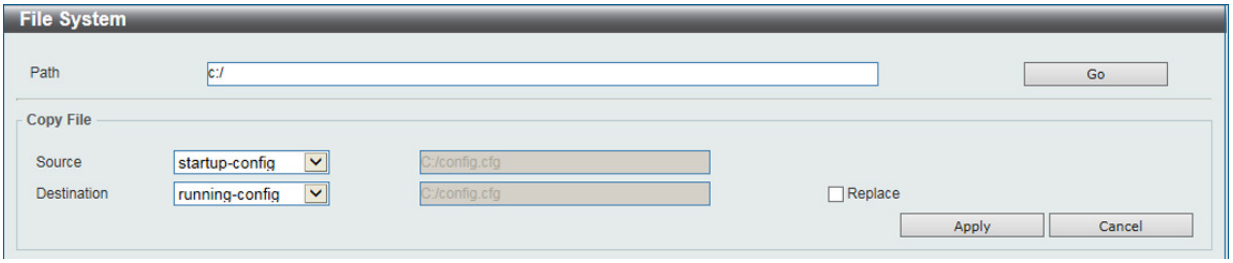

図 7-24　Flash File System Settings 画面 - Copy

2. スイッチのファイルシステムにファイルをコピーする時、送信元（Source）/ 宛先（Destination）のパスを入力します。

3. 「Apply」ボタンをクリックして、コピーを開始します。「Cancel」ボタンをクリックすると処理は破棄されます。「Replace」にチェックを入れると、言外の設定内容から設定ファイルの内容に変更されます。

注意　「**/\:*?"<>**」とスペースはファイル名には使用できません。

注意　ファイル名またはフォルダ名を変更、またはディレクトリを変更する場合、「/」はファイル、フォルダを識別するために使用され、ファイル名に使用されているとパス内で「ファイル名の終わり」と認識されてしまうため、使用することはできません。

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

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

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

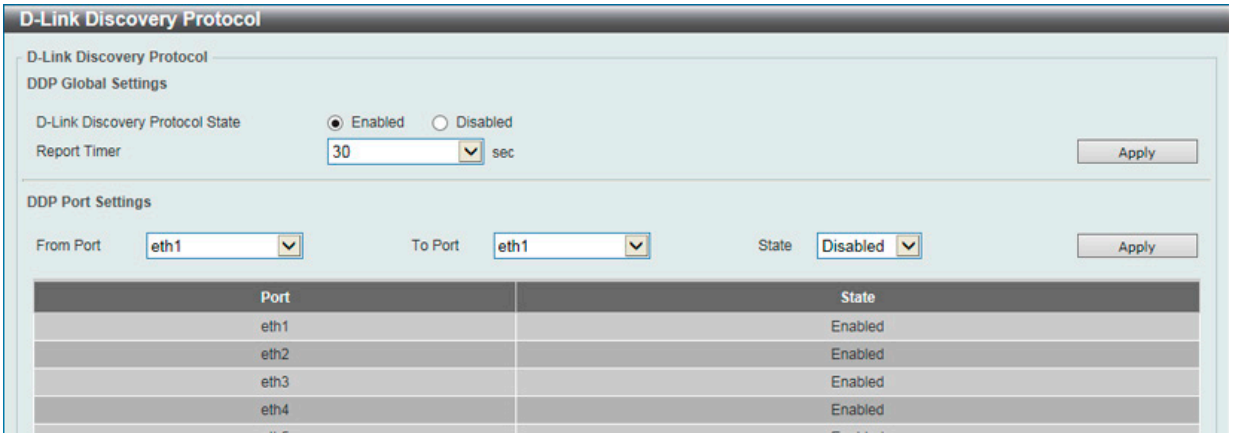

図 7-25　D-Link Discovery Protocol 画面

設定には以下の項目を使用します。

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

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

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	参照ページ
FDB（FDB 設定）	スタティック FDB、MAC アドレステーブルなどを設定します。	61
VLAN（VLAN 設定）	VLAN 表示、設定を行います。	65
STP（スパニングツリーの設定）	スパニングツリーの設定を行います。	73
Loopback Detection（ループバック検知設定）	ループバック検知設定を行います。	77
Link Aggregation（リンクアグリゲーション）	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。	78
L2 Multicast Control（L2 マルチキャストコントロール）	L2 マルチキャストコントロールの設定を行います。	80
LLDP（LLDP 設定）	LLDP（Link Layer Discovery Protocol）の設定を行います。	89

FDB（FDB 設定）

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）

スタティックユニキャスト転送の設定を行います。

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。

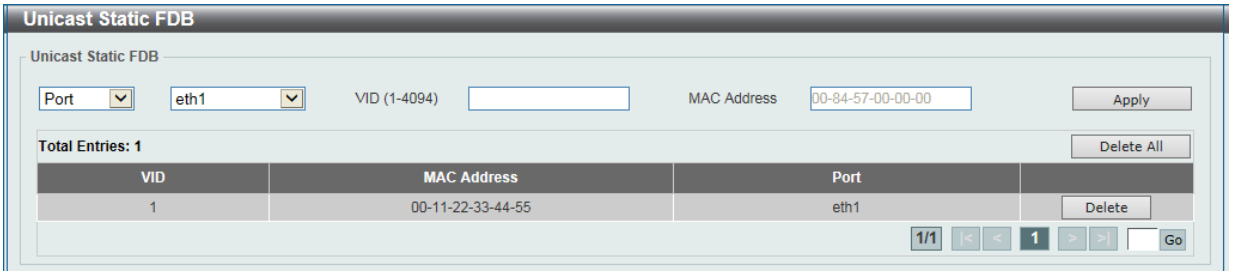

図 8-1　Unicast Static FDB 設定

画面には以下の項目があります。

項目	説明
Port/Drop	上記で入力した MAC アドレスの存在する、ポート番号の選択を行います。このオプションは同時にユニキャストスタティック FDB からの MAC アドレスを破棄するのに使用されます。ポート番号を項目に入力します。 入力形式は次の通りです。 「ポート番号」（例：5）
Port Number	設定するポートを選択します。
VID	ラジオボタンをクリックしてユニキャスト MAC アドレスのある VLAN リストを入力します。
MAC Address	パケットが手動で転送される MAC アドレスを指定します。これはユニキャスト MAC アドレスです。

項目を設定後、「Apply」ボタンをクリックし、デバイスに設定を適用します。
「Delete」をクリックすると指定のエントリを、「Delete All」ですべてのエントリを削除します。

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

スタティックマルチキャスト転送の設定を行います。

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

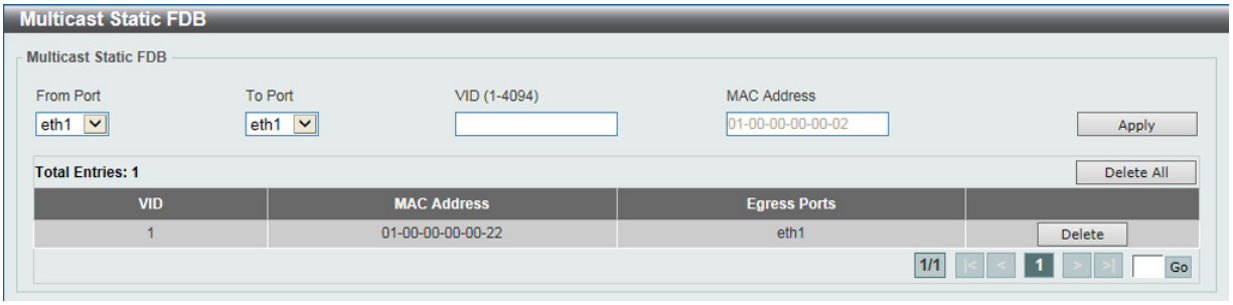

図 8-2　Multicast Static FDB 設定

画面には以下の項目があります。

項目	説明
From Port / To Port	ポートの始点 / 終点を設定します。
VID	関連の MAC アドレスが属する VLAN の VLAN ID です。
MAC Address	スタティックフォワーディングテーブルに追加するマルチキャスト MAC アドレスを入力します。

項目を設定後、「Apply」ボタンをクリックし、デバイスに設定を適用します。
「Delete」をクリックすると指定のエントリを、「Delete All」ですべてのエントリを削除します。

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

スイッチに MAC アドレスエージングタイムを設定します。

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

Global Settings（グローバル設定タブ）

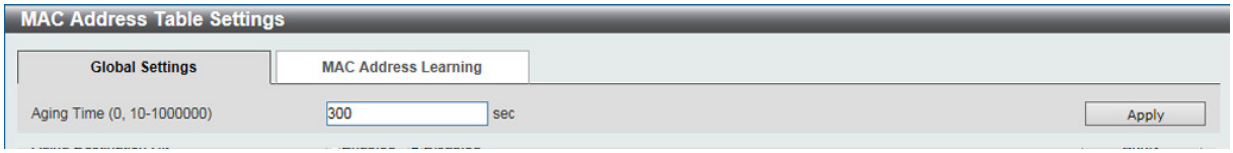

図 8-3　MAC Address Table Settings (Global Settings) 画面

以下の項目を使用して設定を行います。

項目	説明
Aging Time (10-1000000)	学習した MAC アドレスが、アクセスされないでフォワーディングテーブルに保持される（つまりどれくらい学習した MAC アドレスが、アイドル状態を続けることが許可される）時間（10-1000000）を指定します。これを変更するためには、現在の MAC アドレスが破棄される時間（秒）とは異なる値を入力します。初期値は 300（秒）。

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

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

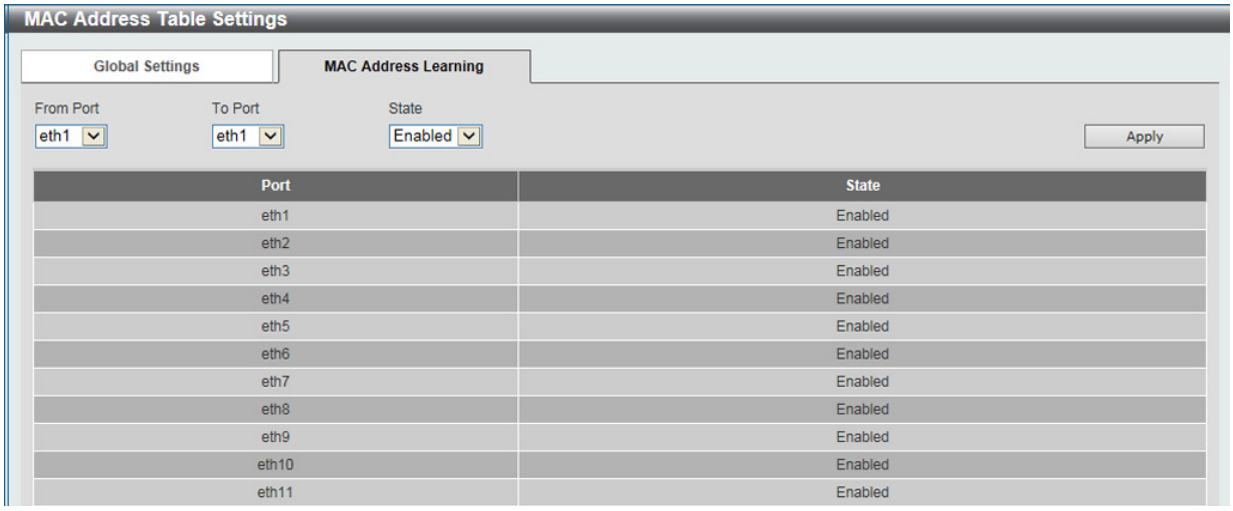

図 8-4　MAC Address Table Settings (MAC Address Learning) 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
From Port / To Port	ポートの始点 / 終点を設定します。
State	MAC アドレスラーニングを有効 / 無効にします。

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

MAC Address Table（MAC アドレステーブル）

MAC アドレステーブル内のエントリリストの表示を行います。

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。

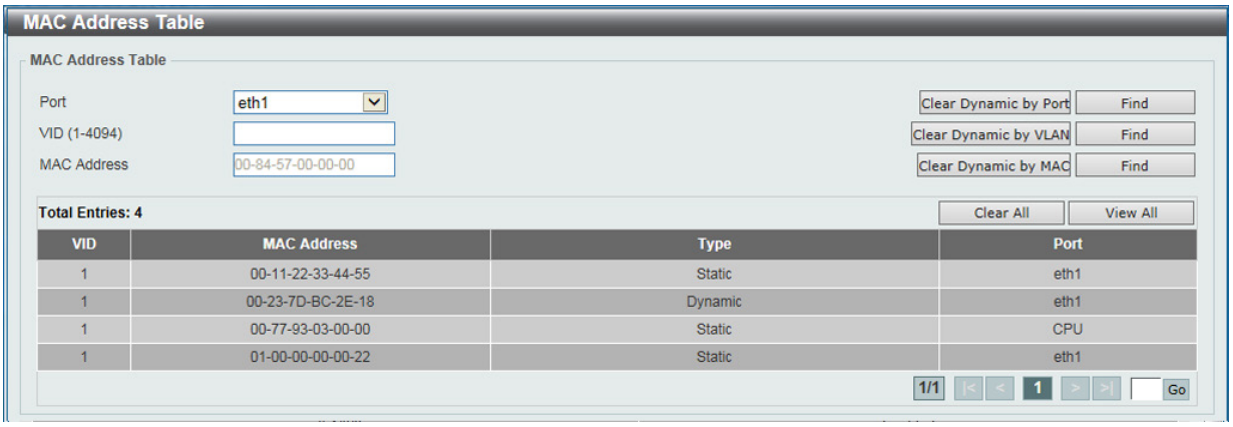

図 8-5　MAC Address Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	MAC アドレスと関連付けられるポートを表示します。
VLAN ID	表示する VLAN ID を入力します。
MAC Address	表示する MAC アドレスを入力します。

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

エントリの検索

「Find」ボタンをクリックして、指定したポート、VLAN または MAC アドレスをキーとして検索します。

ダイナミックエントリの削除

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

エントリの表示

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

全エントリの削除

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

エントリの追加

「Add to Static MAC table」ボタンをクリックして、スタティックテーブルに指定エントリを追加します。

MAC Notification（MAC 通知設定）

MAC Notification（通知）の表示、設定を行います。

注意 本機能をご使用になる場合、NMS（ネットワーク管理システム）側で「MAC NotificationTrap」を受信できる環境が必要になります。Email や Syslog での通知には対応しておりません。

MAC 通知を行うためには、**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。

MAC Notification Settings タブ

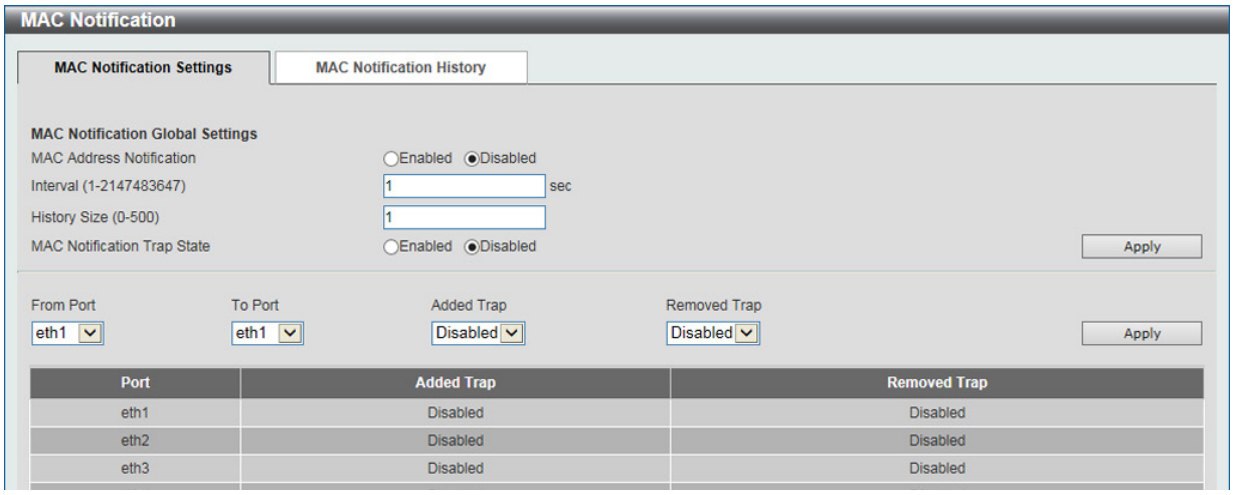

図 8-6　MAC Notification Settings 画面

以下の項目を使用して設定を行います。

項目	説明
MAC Address Notification	スイッチ上の MAC 通知をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
Interval (1-2147483647 sec)	通知を行う間隔（秒）。初期値 : 1（秒）
History Size (0-500)	通知用に使用するヒストリログの最大エントリ数（最大 500 エントリ）。初期値 : 1
MAC Notification Trap State	MAC 通知トラップを有効 / 無効に設定します。
From Port /To Port	プルダウンメニューから、MAC 通知設定を有効または無効にするポートを指定します。
Added Trap	選択したポートの追加トラップを有効 / 無効に設定します。
Removed Trap	選択したポートの削除トラップを有効 / 無効に設定します。

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

MAC Notification History タブ

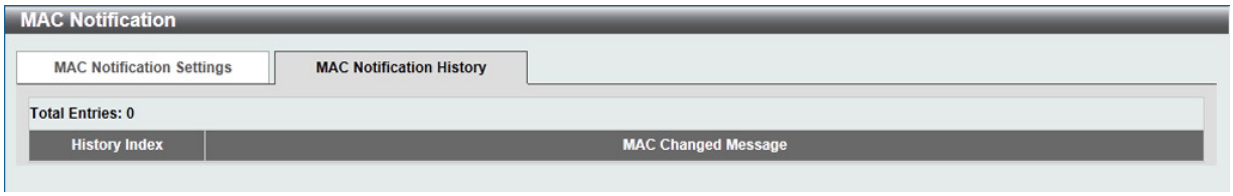

図 8-7　MAC Notification History 画面

MAC 通知メッセージの履歴が表示されます。

VLAN（VLAN 設定）

802.1Q VLAN Settings（802.1Q VLAN 設定）

VLAN 表示、設定を行います。

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

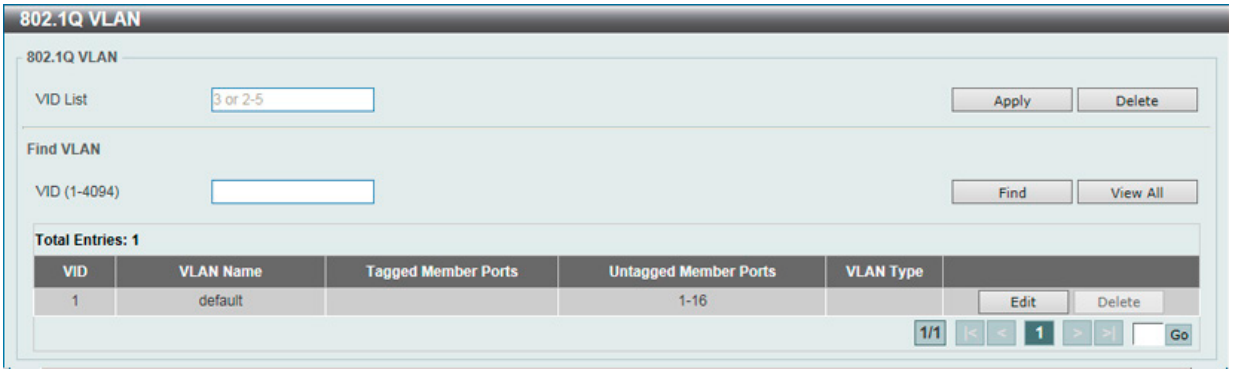

図 8-8　802.1Q VLAN 画面

以下の項目が含まれます。

項目	内容
VID List	追加、削除する VLAN ID リストを入力します。
VID	表示する VLAN ID を入力します。

「Apply」ボタンをクリックし、設定を適用します。

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

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

VLAN の検索

「Find VLAN」に VLAN ID を入力して「Find」ボタンをクリックします。「View All」をクリックするとすべて表示されます。

VLAN の編集

該当エントリの横で「Edit」ボタンをクリックします。

Asymmetric VLAN（Asymmetric VLAN 設定）

Asymmetric VLAN の設定を行います。

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

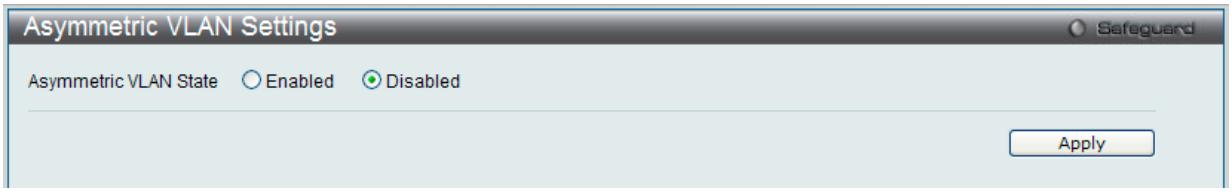

図 8-9　Asymmetric VLAN 画面

項目	説明
Asymmetric VLAN State	Asymmetric VLAN を有効にするかを設定します。 • Enabled - Asymmetric VLAN を有効にします。 • Disabled - Asymmetric VLAN を無効にします。（初期値）

「Apply」ボタンをクリックし、設定を適用します。

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

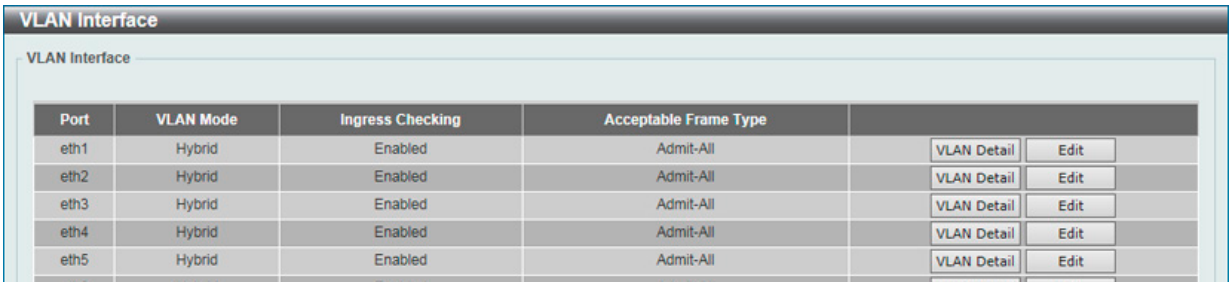

図 8-10　VLAN Interface 画面

VLAN 詳細情報の表示

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

エントリの編集

「Edit」ボタンをクリックして、指定エントリの編集をします。「**VLAN Mode**」を変更すると画面の内容が変化します。

VLAN Deteil（VLAN 詳細情報の表示）

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

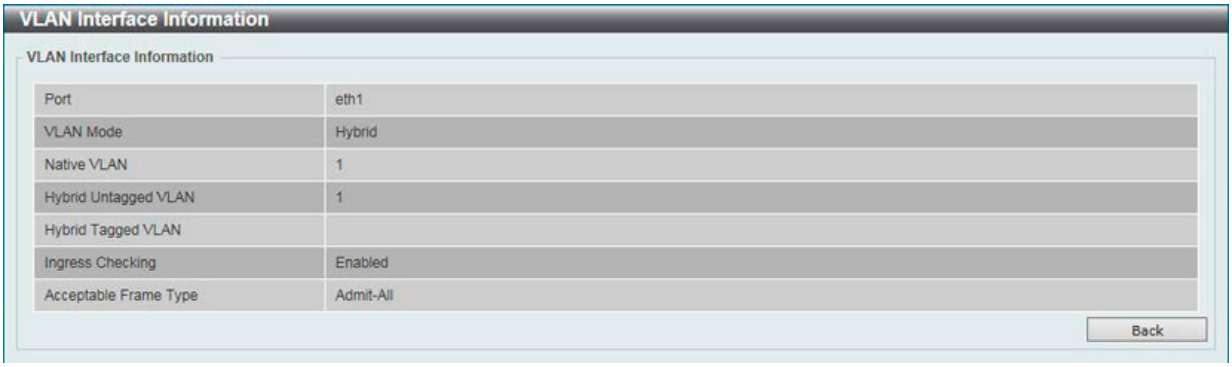

図 8-11　VLAN Interface Information 画面

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

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

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

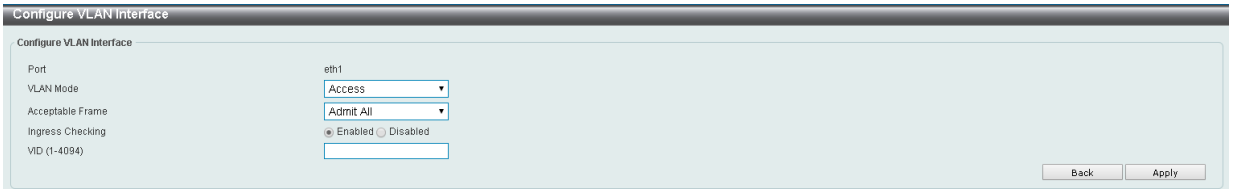

図 8-12　Configure VLAN Interface - Access 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
VID	設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。

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

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

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

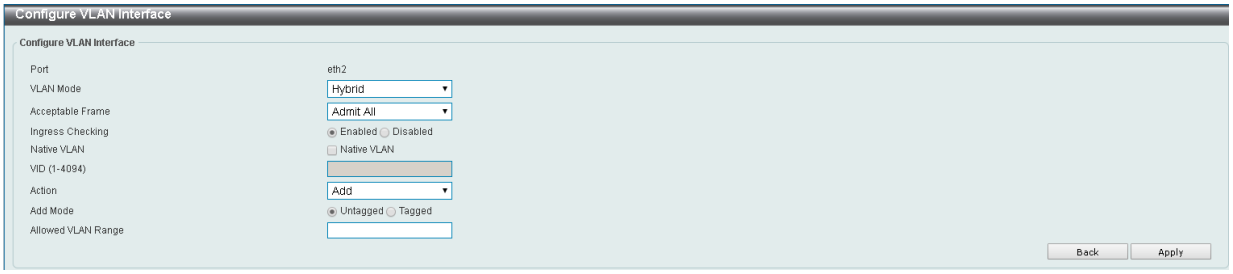

図 8-13　Configure VLAN Interface - Hybrid 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	チェックを入れるとネイティブ VLAN 機能が有効になります。
VID	「VLAN ID」を指定します。1 から 4094 で指定可能です。（Native VLAN にチェックを入れると有効になります。）
Action	実行する動作を「Add」「Remove」「Tagged」「Untagged」から選択します。
Add Mode	Action を「Add」に指定した際に追加する VLAN を「Tagged」「Untagged」から選択します。
Allowed VLAN Range	許可する VLAN 範囲情報を指定します。

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

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

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

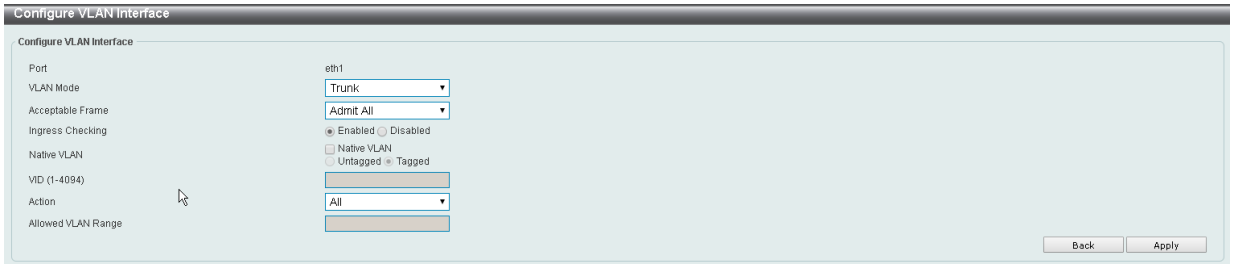

図 8-14　Configure VLAN Interface - Trunk 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	チェックを入れるとネイティブ VLAN 機能が有効になります。 「Tagged」「Untagged」のどちらかを選択します。
VID	「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「All」「Add」「Remove」「Except」「Replace」から選択します。
Allowed VLAN Range	許可する VLAN 範囲情報を指定します。

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

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

自動サーベイランス VLAN は、IP サーベイランスサービスを強化するための機能です。音声 VLAN と同様、D-Link IP カメラからのビデオトラフィックに対して自動的に VLAN をアサインします。優先度が高いこと、また個別の VLAN を使用することで、サーベイトラフィックの品質とセキュリティを保証します。

Auto Surveillance Properties（自動サーベイランスプロパティ）

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

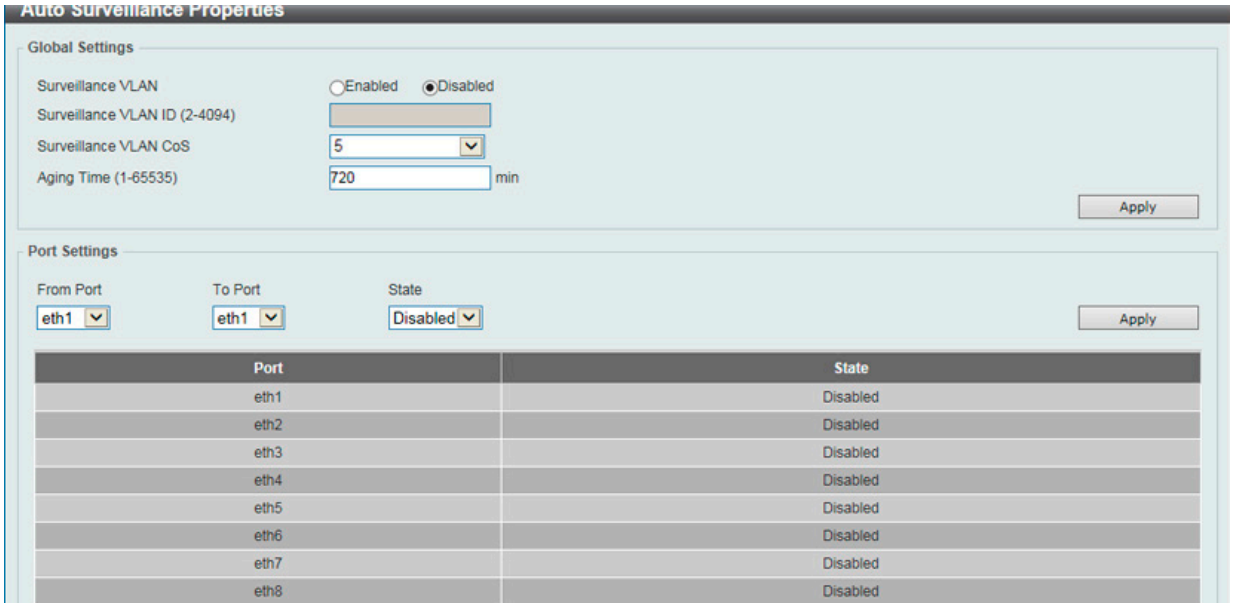

図 8-15　Auto Surveillance Properties 画面

画面には次の項目があります。

項目	説明
Surveillance VLAN	サーベイランス VLAN を有効 / 無効に設定します。
Surveillance VLAN ID	サーベイランス VLAN の VLAN ID を指定します。2 から 4094 で指定できます。
Surveillance VLAN CoS	サーベイランス VLAN の優先値を指定します。0 から 7 で指定できます。
Aging Time	エージングタイム（1-65535 分）。 初期値は 720（分）です。 エージングタイムは、ポートがオートサーベイランス VLAN メンバである場合にサーベイランス VLAN からポートを削除するために使用されます。最後のサーベイランスデバイスが、トラフィックの送信を止めて、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。 サーベイランストラフィックがエージングタイム内に再開すると、エージングタイマは停止し、リセットされます。

「Apply」ボタンをクリックし、設定を適用します。

Auto Surveillance VLAN Port Settings（自動サーベイランス VLAN ポート設定）

自動サーベイランス VLAN 情報のポート設定を行います。

以下の項目を使用して、設定します。

項目	説明
From Port / To Port	表示するポート範囲を指定します。
State	ポートの状態を有効または無効にします。

「Apply」ボタンをクリックし、設定を適用します。

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

ユーザ定義のサーベイランストラフィックの OUI を設定します。

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

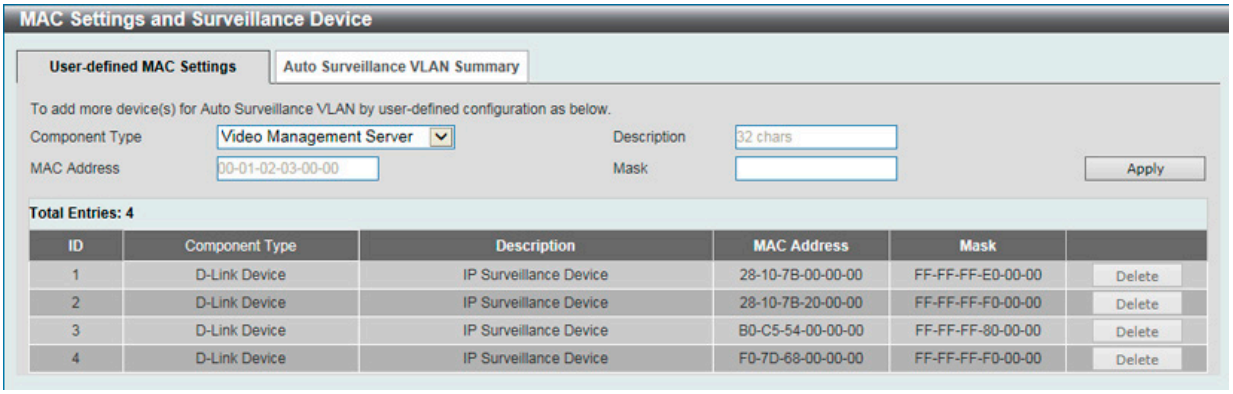

図 8-16　User -defined MAC Settings 画面

以下の項目を使用して設定します。

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

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

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

自動サーベイランス VLAN サマリの表示

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

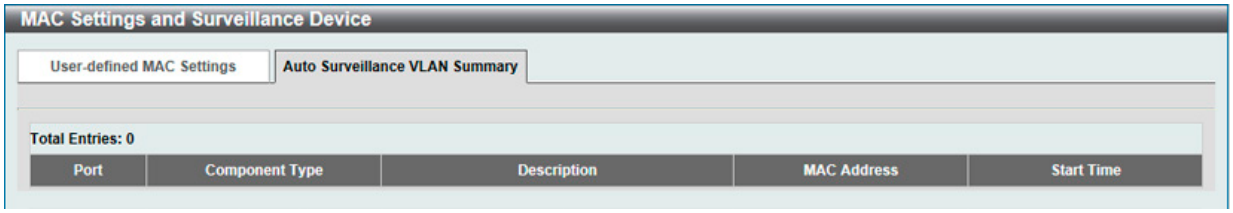

図 8-17　Auto Surveillance VLAN Summary 画面

Voice VLAN（音声 VLAN）

Voice VLAN は IP 電話からの音声トラフィックを送信する上で使用される VLAN です。IP 電話の音声品質が劣化するなどの理由から音声トラフィックの QoS を通常のトラフィックより優先的に送信されるように設定します。

送信元の MAC アドレスから受信したパケットが音声パケットであると判断します。パケットの送信元 MAC アドレスが OUI アドレスだとシステムが認識した場合、パケットは音声 VLAN に送信された音声パケットであると判断されます。

Voice VLAN Global（音声 VLAN グローバル設定）

音声 VLAN をグロバールに有効 / 無効にします。

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

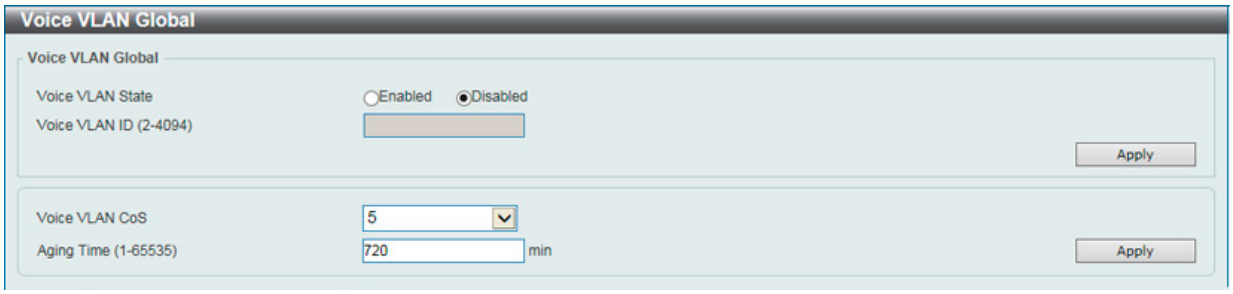

図 8-18　Voice VLAN Global 画面

以下の項目を使用して、設定します。

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

「Apply」ボタンをクリックし、設定を適用します。

Voice VLAN Port（音声 VLAN ポート設定）

音声 VLAN のポート設定を行います。

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

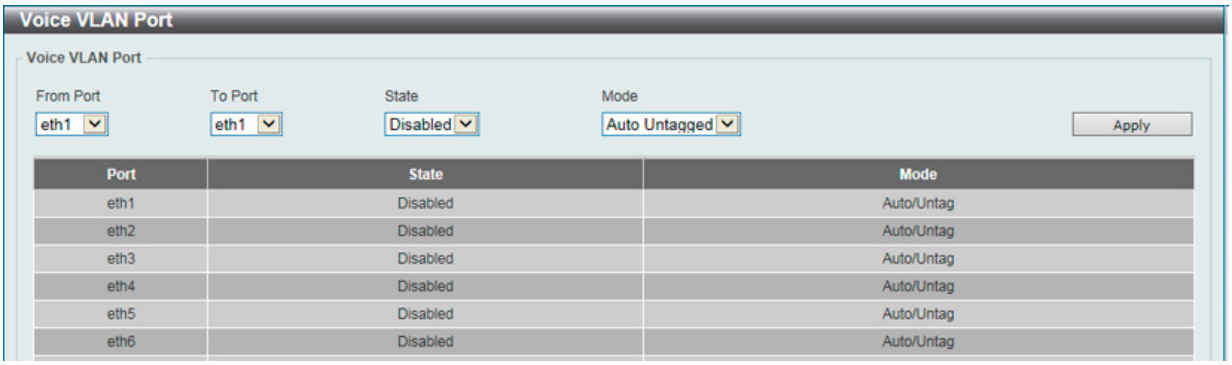

図 8-19　Voice VLAN Port 画面

以下の項目を使用して、設定します。

項目	説明
From Port / To Port	音声 VLAN を設定するポートの範囲を設定します。
State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Mode	「Auto Untagged」「Auto Tagged」「Manual」で設定します。受信パケットの「Auto Untagged」（タグなし）、「Auto Tagged」（タグ付き）が一致した場合、ポートは自動的に音声 VLAN の一部であると認識され設定されます。「Manual」モードに設定した場合、802.1Q VLAN 設定コマンドを使用して、ポートは手動で音声 VLAN の一部として追加 / 削除する必要があります。

「Apply」ボタンをクリックし、設定を適用します。

Voice VLAN OUI（音声 VLAN OUI 設定）

ユーザ設定音声トラフィックの OUI を設定します。OUI は事前に設定済みのものがありますので、ユーザが手動で OUI を設定する場合、事前に設定されている下記の OUI は避けて設定する必要があります。

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

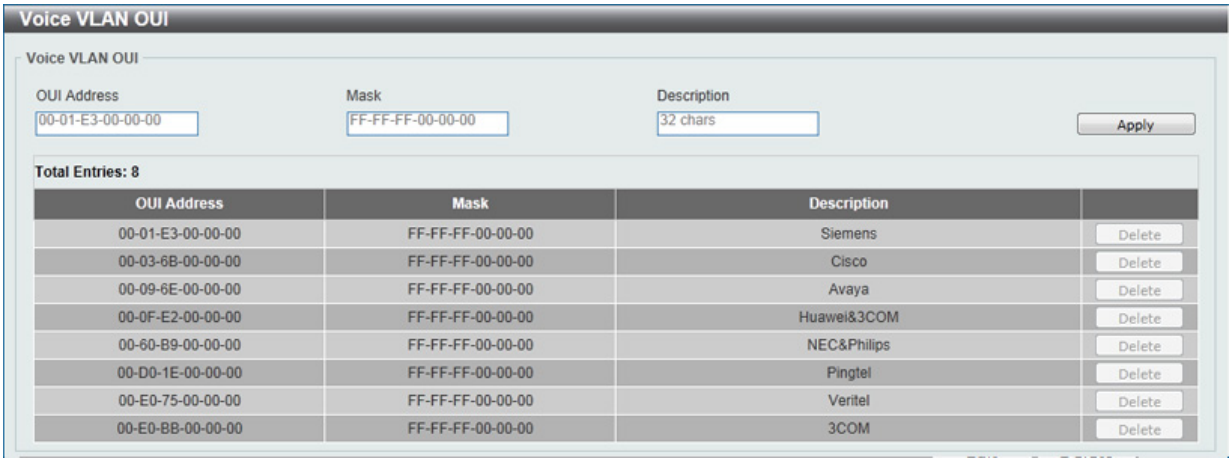

図 8-20　Voice VLAN OUI 画面

以下の項目を使用して、設定します。

項目	説明
OUI Address	OUI MAC アドレスを入力します。
Mask	OUI MAC アドレスマスクを入力します。
Description	設定する OUI についての説明を入力します。

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

Voice VLAN Device（音声 VLAN 機器）

各スイッチポートに接続中の音声 VLAN が使用可能なデバイスを表示します。

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

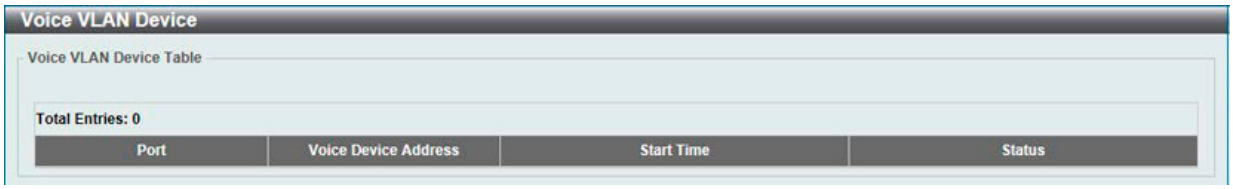

図 8-21　Voice VLAN Device 画面

Voice VLAN LLDP-MED Voice Device（音声 VLAN LLDP-MED 音声機器）

LLDP-MED で検出された音声バイスを表示します。

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

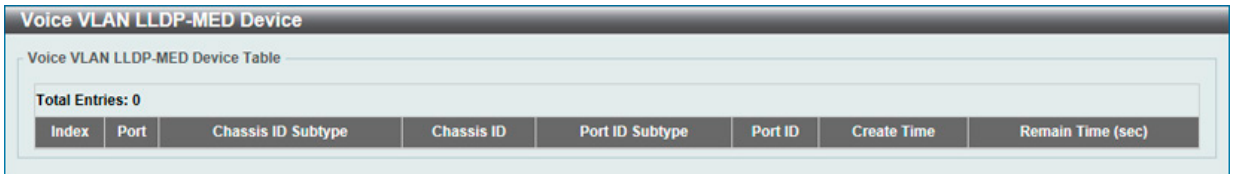

図 8-22　Voice VLAN LLDP-MED Voice Device 画面

Spanning Tree（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（802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。ネットワーキング管理者間では 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ると思います。しかし、D-Link のマネジメントスイッチにも 802.1D-2004 RSTP と 802.1Q-2005 MSTP は導入されており、それらの技術について、以下に簡単に紹介します。また、802.1D-1998 STP、802.1D-2004 Rapid STP、802.1Q-2005 MSTP それぞれの設定方法についても、本章中に記述します。

802.1Q-2005 MSTP

MSTP（Multiple Spanning Tree 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、ネットワーク中に複数の経路を提供します。また、ロードバランシングを可能にし、 1 つのインスタンスに障害が発生した場合でも、広い範囲で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を素早く収束します。これら VLAN 用のフレームは、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て、素早く適切に相互接続されたブリッジを通して処理されます。

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します。MSTP では、複数のスパニングツリーを CIST（Common and Internal Spanning Tree）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決定し、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、異なる VLAN を割り当てられたフレームは、ネットワーク上の管理用に設定されたリージョン中の異なるデータ経路を通ります。

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

1. 32 文字までの半角英数字で定義された「Configuration 名」。「MST Configuration Identification」画面中の「Configuration Name」で設定します。
2. 「Configuration Revision 番号」（「MST Configuration Identification」画面内の「Revision Level」）。
3. 4096 エレメントテーブル（「MST Configuration Identification」画面内の「VID List」）。スイッチがサポートする 4096 件までの VLAN とインスタンスとの関連付けです。

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

1. スイッチに MSTP 設定を行います。（「STP Bridge Global Settings」画面の「STP Version」で設定）
2. MSTP インスタンスに適切なスパニングツリープライオリティを設定します。（「STP Instance Settings」画面の「Priority」で設定）
3. 共有する VLAN を MSTP Instance ID に追加します。（「MST Configuration Identification」画面の「VID List」で設定）

802.1D-2004 Rapid Spanning Tree

本スイッチには、IEEE 802.1Q-2005 に定義される MSTP（Multiple Spanning Tree Protocol）、IEEE 802.1D-2004 に定義される RSTP（Rapid Spanning Tree Protocol）、および 802.1D-1998 で定義される STP（Spanning Tree Protocol）の 3 つのプロトコルを実装しています。RSTP は IEEE 802.1D-1998 をサポートするレガシー機器との併用が可能ですが、その場合 RSTP を使用する利点は失われます。

RSTP は 802.1D-1998 STP 標準の進化型です。RSTP は、STP を使用する上での制限を克服する目的で開発されました。制限とは、特に今日イーサネットスイッチに取り入れられているレイヤ 3 の諸機能を妨害するものを指しています。RSTP の基本的な機能や用語の多くは STP と同じであると言えます。STP 用の設定項目の多くも RSTP で同じように使用されます。本項では、スパニングツリーの新しいコンセプトと、これら 2 つのプロトコル間の主な違いについて記述します。

ポートの状態遷移

3 つのプロトコル間の根本的な相違は、ポートがフォワーディング状態に遷移する方法と、この遷移とトポロジの中でのポートの役割（Forwarding/ Not Forwarding）の関連性にあります。MSTP と RSTP では、802.1D-1998 で使用されていた 3 つの状態、「Disabled」、「Blocking」、「Listening」が、「Discarding」という 1 つの状態に統合されました。どちらのケースにおいて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中では「アクティブではない状態」であり、機能の差はありません。以下の表にポートの状態遷移における 3 つのプロトコルの差を示しています。

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 1 つのパスがあります。すべてのブリッジは BPDU パケットをリッスンします。しかし、BPDU パケットは、さらに Hello パケット送信ごと送信されます。
BPDU パケットは、受信されないことがあっても送信されます。そのため、ブリッジ間のリンクはリンクの状態に反応します。結果として、この違いがリンク断の素早い検出とトポロジの調整に繋がるのです。802.1D-1998 の欠点は隣接するブリッジからの即時のフィードバックがないことです。

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、タイマの設定への依存をやめ、フォワーディング状態への急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からのフィードバックに反応するようになりました。ポートは、フォワーディング状態の遷移の間トポロジが安定するまで待つ必要がなくなりました。この急速な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）が使用されます。

Edge Port

エッジポートは、ループを作成できないセグメントに直接接続しているポートに指定するものです。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、直接 forwarding に遷移し、listening および learning の段階は飛ばしてしまいます。エッジポートは BPDU パケットを受け取った時点で、通常のスパニングツリーポートに変わります。

P2P Port

P2P ポートでも急速な遷移が可能になっています。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、全二重モードで動作しているすべてのポートは、特に設定を変えられていない限り、P2P ポートと見なされます。

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

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。しかし、802.1D-1998 STP を使用しているセグメントでは、MSTP や RSTP の利点である迅速な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。それらのプロトコルは、セグメント上でレガシー機器が RSTP や MSTP を使用するためにアップデートを行う場合などの、マイグレーションに使用する変数を用意しています。

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。

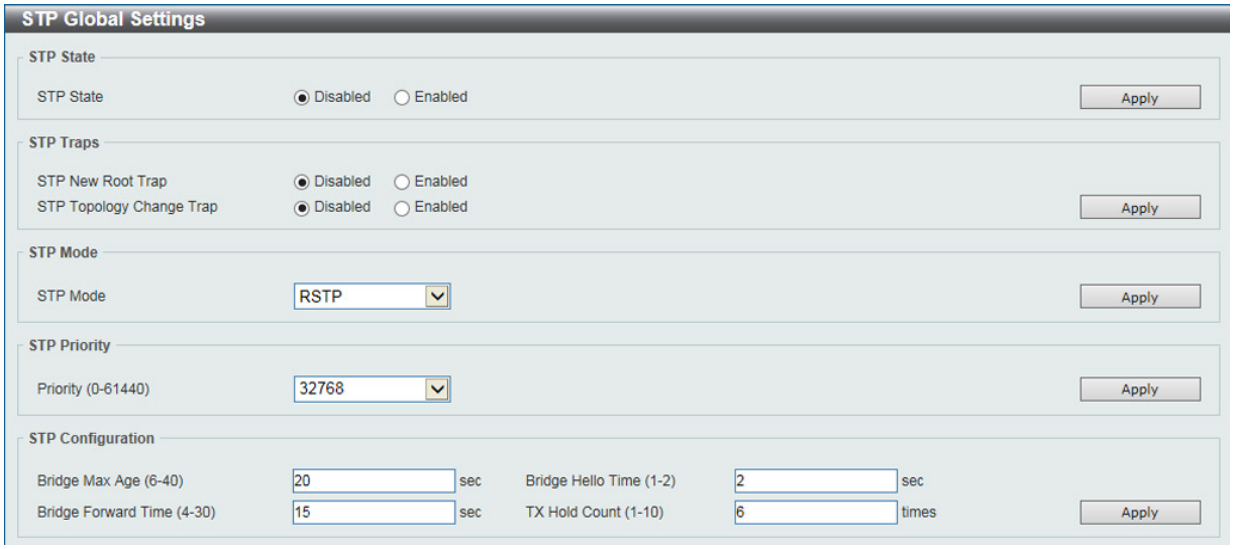

図 8-23　STP Global Settings 画面

設定には以下の項目が使用されます。

項目	説明
STP State	
STP State	STP をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。初期値は Disabled です。
STP Trap	
STP New Root Trap	新しいルートトラップ送信の有効 / 無効を設定します。初期値は Disabled です。
STP Topology Change Trap	トポロジ変更トラップ送信の有効 / 無効を設定します。初期値は Disabled です。
STP Mode	
STP Mode	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。 • MSTP - スイッチ上で MSTP がグローバルに使用されます。
STP Priority	
Priority	STP 優先値を指定します。0 から 61440 までで指定可能です。初期値は 32768 です。低い方が優先値は高いです。
STP Configuration	
Bridge Max Age (6-40)	本項目は、古い情報がネットワーク内の冗長パスをずっと循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40（秒）の範囲から値を指定します。初期値では 20（秒）が指定されています。
Bridge Hello Time (1-2)	ブリッジの「Hello Time」の値を入力します。1-2（秒）の値を入力できます。初期値は「2」です。この値は他のすべてのスイッチにルートブリッジを認識させるため、ルートブリッジから送信される BDPU パケットの送信間隔です。
Bridge Forward Time (4-30)	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間に本値で指定した時間 Listening 状態を保ちます。4-30（秒）の範囲から指定します。初期値は 15（秒）です。
Tx Hold Count (1-10)	Hello パケットの最大送信回数を指定します。1-10 の範囲から指定します。初期値は 6 です。

「Apply」ボタンをクリックし、設定を適用します。

STP Port Settings（STP ポートの設定）

本項目では個別ポート / ポート範囲での STP パラメータの設定について説明します。
スイッチレベルでのスパニングツリー設定のほかに、ポートをグループ分けして、各ポートグループに対してスパニングツリーの設定を行うことも可能です。STP グループ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様の働きをしますが、ルートブリッジの概念はルートポートに置き換えられて考えることができます。グループ内のルートポートは、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、ネットワークとグループを接続する役割を果たします。スイッチレベルの場合と同様に、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（または同様のネットワークデバイス）の冗長リンクをブロックし、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。
STP グループと VLAN グループを関連付けて定義することを推奨します。

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。

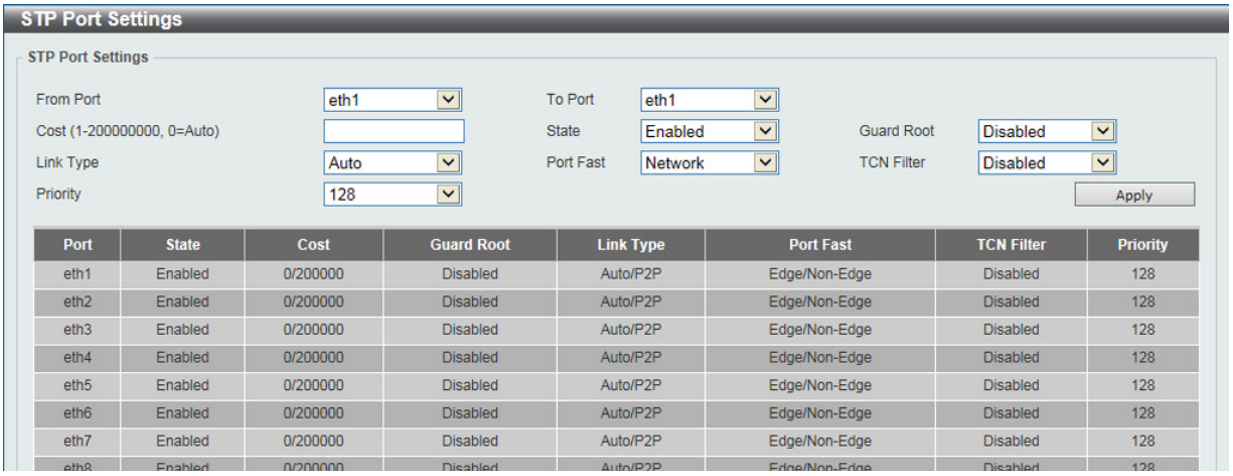

図 8-24　STP Port Setting 画面

本画面には以下の項目があります。

項目	説明
From Port	連続するポートグループの最初の番号を設定します。
To Port	連続するポートグループの最後の番号を設定します。
Cost (1-200000000, 0=Auto)	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。ポートのコストは自動か、メトリックの値で設定します。初期値は 0（Auto）です。 • 0（Auto）- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。 ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。 • 値 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほどパケット転送は頻繁に行われるようになります。
State	ポートグループでの STP の「Enabled」（有効）/「Disabled」（無効）を設定します。初期値は「Enabled」です。
Guard Root	Guard Root の「Enabled」（有効）/「Disabled」（無効）を設定します。
Link Type	リンクの種類を設定します。初期値は「Auto」です。 • P2P - P2P ポートとしてリンクを共有します。P2P ポートは全二重でなくてはならないという制限があります。 • Shared - 半二重ポートとして認識されます。 • Auto - 可能であれば常に P2P となるように設定します。ポートが、例えば強制的に半二重になるなど状態を維持できない場合には、Shared と同様の状態になります。
Port Fast	ポートファストオプションを指定します。 「Network」「Disabled」「Edge」から選択します。「Network」モデム内だとポートは 3 秒だけ非ポートファスト状態に残ります。ポートは BPDU が受信されず、転送状態に変更されるとポートファスト状態に変更します。のちに BPDU を受信すると非ポートファストへ戻ります。「Disable」モードではポートは常に非ポートファスト状態です。常に転送状態への変化のために「forward-time delay」を待ちます。「Edge」モードではポートは「forward-time delay」を待たずに直接 STP 転送状態に変化します。インタフェースが「BPDU」を受信すると非ポートファストへ移行します。初期値では「Network」になります。
TCN Filter	TCN（Topology Change Notification）フィルタを有効 / 無効に設定します。 ポートの TCN フィルタリングを有効にすると、域内のアドレスフラッシングを発生させるネットワークのコア域への外部ブリッジを ISP により防ぐために有効です。 こういったブリッジは管理者のコントロール下で構築されることはないためです。ポートが TCN フィルタモードに設定されると、ポートは無視されることにより TC イベントは受信されます。初期値は無効です。
Priority	優先値を指定します。0 から 240 で指定可能です。初期値は 128 です。少ない方が優先値は高くなります。

「Apply」ボタンをクリックし、設定を適用します。

STP Global Information（STP グローバル情報）

STP のグローバル情報について表示します。

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

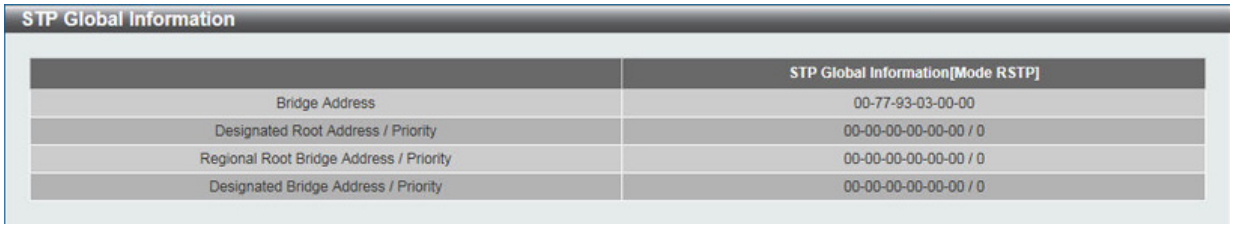

図 8-25　STP Global Information 画面

STP Port Information（STP ポート情報）

現在の STP ポート情報を表示します。

L2 Features > STP > STP 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 8-26　STP Port Information 画面

本画面には以下の情報があります。

項目	説明
Port	プルダウンメニューを使用して、ポートを選択します。

「Clear Detected Protocol」ボタンをクリックし、選択したポートの検出したプロトコル設定をクリアします。

指定ポートの STP 設定の参照
特定ポートの STP 設定を参照するためには、プルダウンメニューでポート番号を選択し、「Find」ボタンをクリックします。

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。
該当エントリの横で「Edit」ボタンをクリックし設定の編集を行います。

Loopback Detection（ループバック検知設定）

ループバック検知機能は、特定のポートによって生成されるループを検出するために使用されます。
本機能は、CTP（Configuration Testing Protocol）パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN から受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。ループバック検知機能はポート範囲に実行されます。プルダウンメニューを使用し、機能を「Enabled」（有効）/「Disabled」（無効）にします。

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

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。

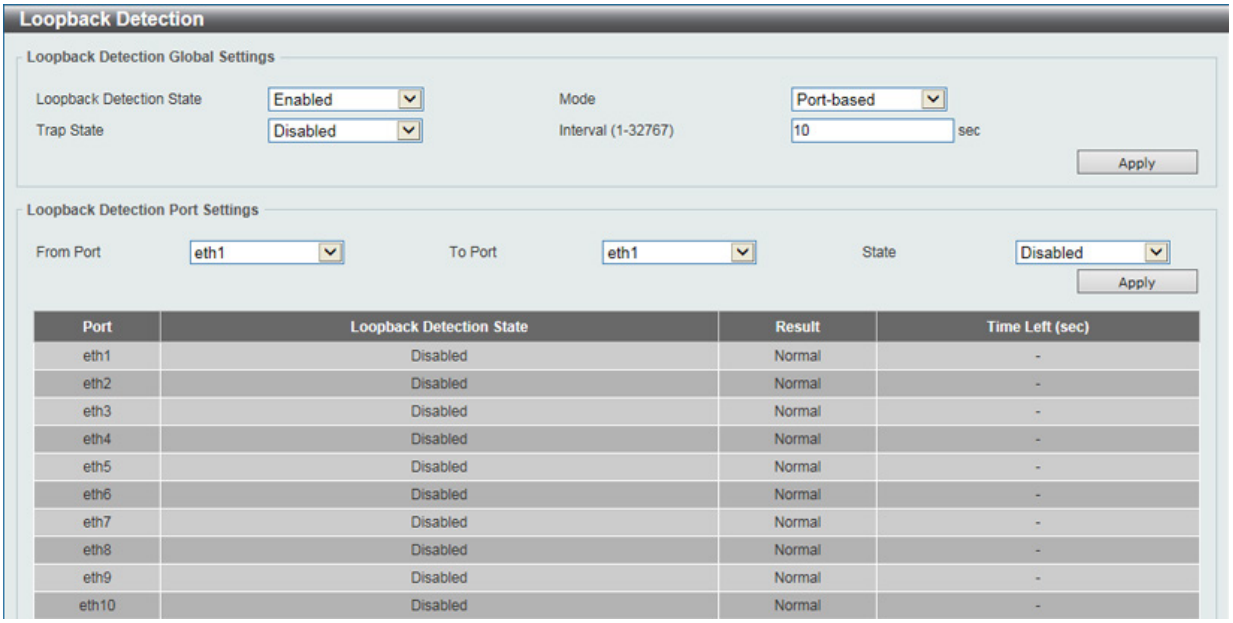

図 8-27　Loopback Detection Settings 画面

項目	説明
Loopback Detection State	ループバック検知機能を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Mode	プルダウンメニューで「Port Based」を選択します。
Traps State	トラップを有効 / 無効に設定します。
Interval (1-32767)	ループ検知間隔を設定します。（1-32767 秒）
From Port	プルダウンメニューで開始ポートを選択します。
To Port	プルダウンメニューで終了ポートを選択します。
State	「Enabled」（有効）または「Disabled」（無効）を指定します。

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

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。DXS-1100-10TS は 1 から 4 のポートを束ねた 5 個までのトランクグループをサポートします。DXS-1100-16TC/16SC は 1 から 8 のポートを束ねた 8 個までのトランクグループをサポートします。

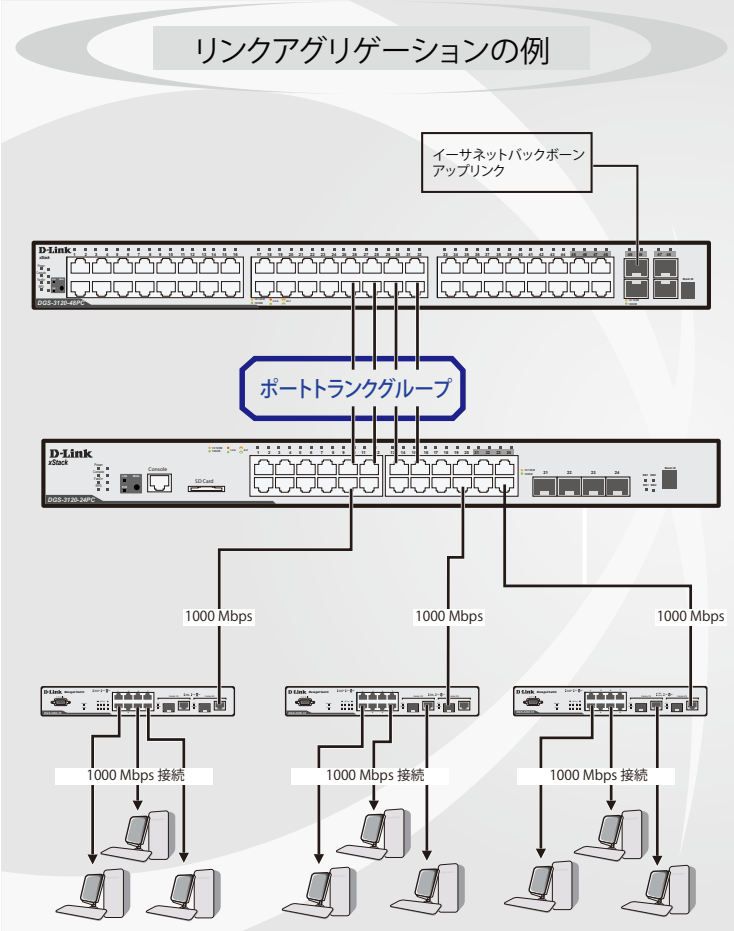

図 8-28　ポートトランクグループの例

スイッチはトランクグループ内のすべてのポートを 1 つのポートと見なします。あるホスト（宛先アドレス）へのデータ転送は、トランクグループ内のいつも同じポートから行われます。これにより、データが送信された順に受け取られるようになります。

注意 トランクグループ内のある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他のリンクアグリゲーション（集約）グループ内の他のポート間でロードシェアされます。

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

リンクアグリゲーション機能により、 1 つのグループとして束ねられたポートは、1 つのリンクの働きをします。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、サーバやバックボーンなど、広帯域を必要とするネットワークデバイスにおいて広く利用されています。

DXS-1100-10TS では、1 から 4 のリンク（ポート）で構成する最大 5 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。
DXS-1100-16TC/16SC では、1 から 8 のリンク（ポート）で構成する最大 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。各ポートにつき 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。

1 つのグループ内のポートはすべて同じ VLAN に属し、それぞれのスパニングツリープロトコル（STP）ステータス、スタティックマルチキャスト、トラフィックコントロール、トラフィックセグメンテーション、および 802.1p デフォルトプライオリティの設定は同じである必要があります。
また、ポートロッキング、ポートミラーリング、および 802.1X は無効にする必要があります。さらに、集約するリンクはすべて同じ速度で、全二重モードで設定されている必要があります。

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によって発生するネットワークトラフィックは、グループ内の他のリンクに振り分けられます。

スパニングツリープロトコル（STP）は、スイッチレベルにおいて、リンクアグリゲーショングループを 1 つのリンクとしてとらえます。ポートレベルでは STP はマスタポートのパラメータを使用してポートコストを計算し、リンクアグリゲーショングループの状態を決定します。スイッチ上に 2 つのリンクアグリゲーショングループが冗長して設定された場合、STP は冗長リンクを持つポートのブロックを行うのと同様に、 1 つのポートをブロックします。

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

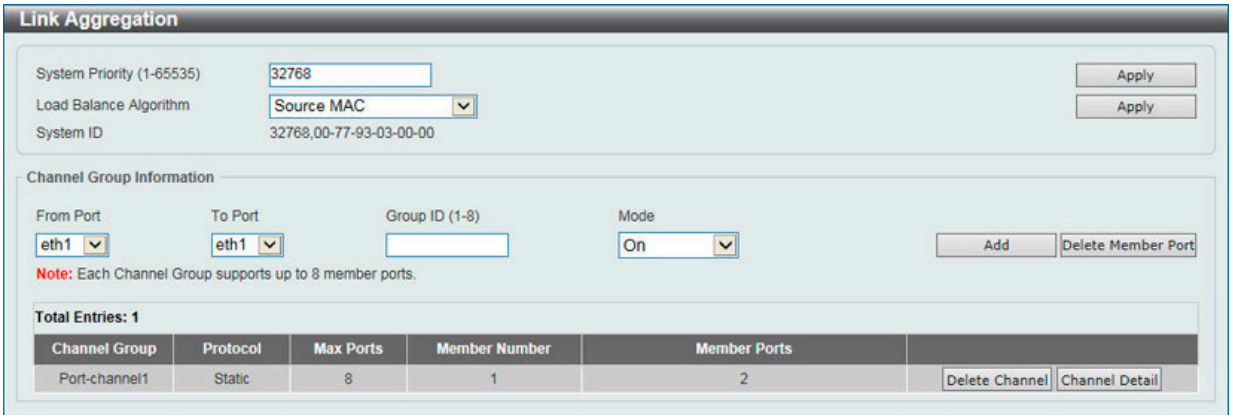

図 8-29　Link Aggregation 画面

本画面には次の項目があります。

項目	説明
System Priority	システム優先値を指定します。1 から 65535 の間で指定できます。初期値は 32768 です。システム優先値はどのポートがポートチャネルに属するか、そしてポートがスタンドアロンモードに入るかを決定します。低い値の方が高い優先値を示します。二つ以上のポートで同じ優先値を与えられた場合、ポート番号で優先値が決まります。
Load Balance Algorithm	ポートトランクグループを構成するポートのロードバランスに使用するアルゴリズムを選択します。「Source MAC」、「Destination MAC」、「Source Destination MAC」、「Source IP」、「Destination IP」、「Source Destination IP」から指定してください。初期値は「Source MAC」です。
From Port / To Port	設定するポートの範囲を設定します。
Group ID (1-8)	グループの ID 番号（1-8）を設定します。
Mode	モードを指定します。「On」「Active」「Passive」から指定できます。 • On - チャネルグループタイプは固定です。 • Active - Active ポートは LACP 制御フレームの処理と送信を行います。これにより LACP 準拠のデバイス同士はネゴシエーションとリンクの集約を行い、グループは必要に応じて動的に変更されます。グループへのポート追加、または削除などのグループの変更を行うためには、少なくともどちらかのデバイスで LACP ポートを Active に設定する必要があります。また、両方のデバイスは LACP をサポートしている必要があります。 • Passive - Passive ポートは自分から LACP 制御フレームの送信を行いません。リンクするポートグループがネゴシエーションを行い、動的にグループの変更を行うためには、コネクションのどちらか一端が Active な LACP ポートである必要があります。（初期値）

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

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

ポートトランクグループの編集
チャネルについてのより詳細な情報の確認には「Channel Detail」をクリックします。

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

IGMP Snooping（IGMP スヌーピング）

IGMP（Internet Group Management Protocol）Snooping 機能を利用すると、スイッチはネットワークステーションまたはデバイスと IGMP ホスト間で送信される IGMP クエリと IGMP レポートを認識するようになります。また、スイッチを通過する IGMP メッセージの情報に基づいて、指定したデバイスに接続するポートを追加 / 削除できるようになります。

IGMP Snooping Settings（IGMP スヌーピング設定）

IGMP Snooping 設定を有効または無効にします。

IGMP Snooping 機能を利用するためには、まず、画面上部の「IGMP Global Settings」セクションでスイッチ全体に機能を有効にします。IGMP Snooping を有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバに接続するポートを開閉できるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストがもう存在していないと判断すると、マルチキャストパケットの送信を停止します。

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

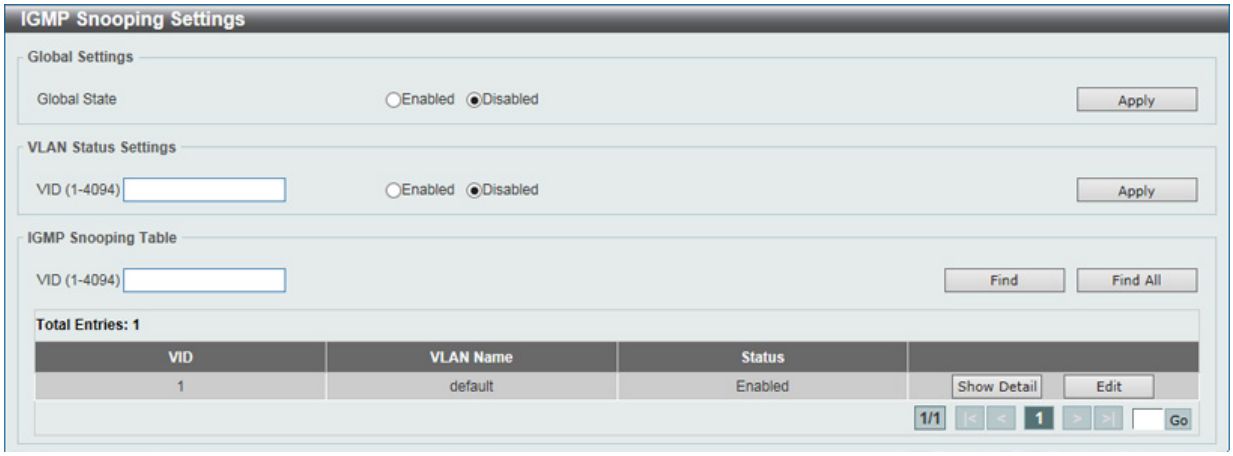

図 8-30　IGMP Snooping Settings 画面

画面には以下の項目があります。

項目	説明
Global Setting	
Global State	IGMP Snooping の有効 / 無効を設定します。 • Enabled - デバイスで IGMP Snooping を有効にします。 • Disabled - デバイスで IGMP Snooping を無効に設定します。（初期値）
VLAN Status Settings	
VID	VLAN 上の IGMP Snooping を有効 / 無効にし、VLAN を識別する VLAN ID を指定します。 • Enabled - VLAN を有効にします。 • Disabled - VLAN を無効に設定します。（初期値）
IGMP Snooping Table	
VID	IGMP Snooping Table 上の VLAN を表示させるための VLAN ID を指定します。 • Find - 指定の VLAN ID を入力して指定のエントリを表示します。 • Find All - IGMP Snooping Table 上のすべてのエントリを表示します。

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。
「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。

IGMP Snooping VLAN の詳細情報表示

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

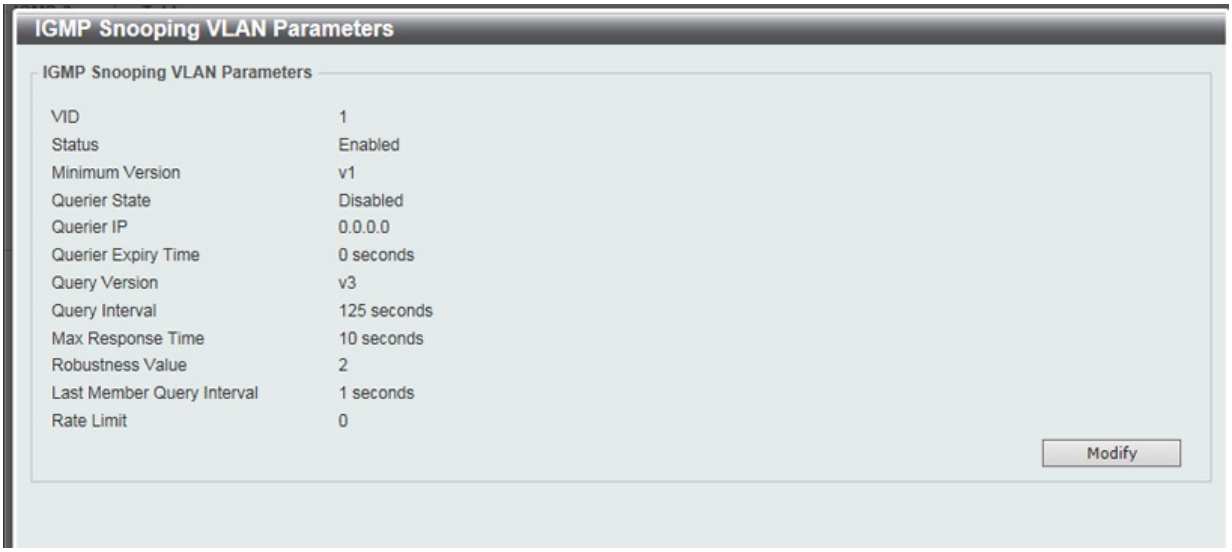

図 8-31　IGMP Snooping VLAN Parameters 画面

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 VLAN Settings）

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

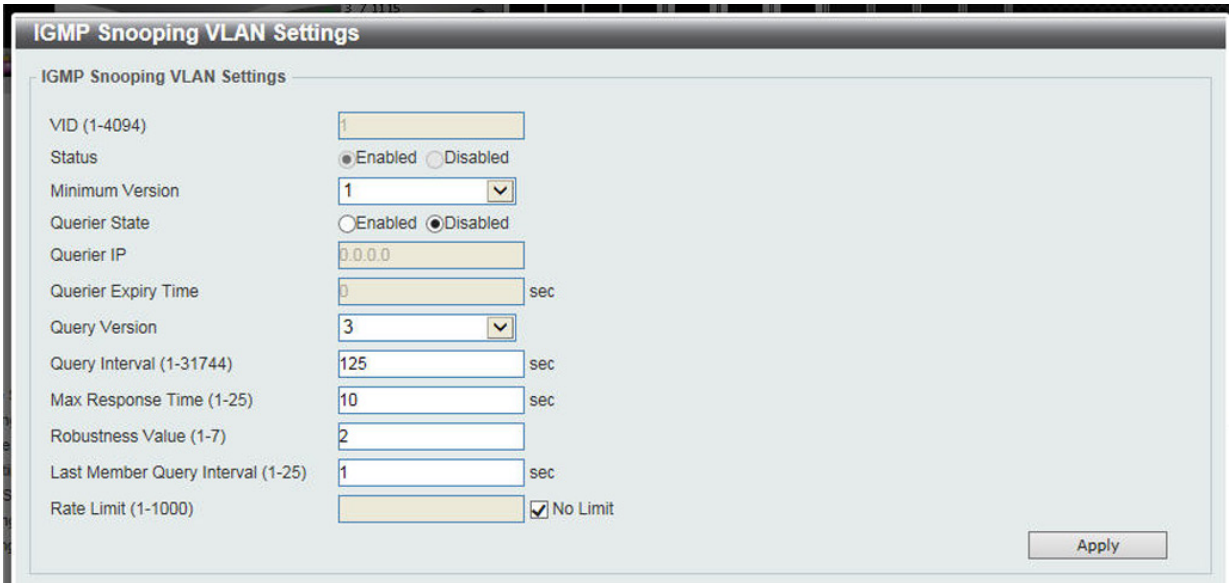

図 8-32 IIGMP Snooping VLAN Settings 画面

以下の項目が表示、または設定変更に使用できます。

項目	説明
VID（1-4094）	IGMP Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
Status	指定した VLAN への IGMP Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。
Minimum Version	VLAN に許可された IGMP ホストの最小バージョンを選択します。
Querier State	「Enabled」（有効）にすると IGMP Query パケットを送信可能になります。初期値は「Disabled」（無効）です。
Query Version	IGMP スヌーピングクエリアに送信されるクエリパケットのバージョンを選択します。「1」「2」「3」から選択可能です。
Query Interval	IGMP query 送信間隔（秒）。1-31744 の範囲から指定します。初期値は 125 です。
Max Response Time (1-25)	IGMP response report を送信するまでの最大時間（秒）。1-25 の範囲から指定します。初期値は 10（秒）です。
Robustness Value (1-7)	パケットロスへの抵抗力を示します。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。1-255 の範囲から指定します。初期値は 2 です。
Last Member Query Interval (1-25)	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の Max Response Time 欄に設定する値（Last Member Query Interval）。また、同 Query の送信間隔でもあります。初期値は 1 です。
Rate Limit	使用する IGMP Snooping の Rate Limit を指定します。「No Limit」にチェックを入れるとリミットは無視されます。

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

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

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

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

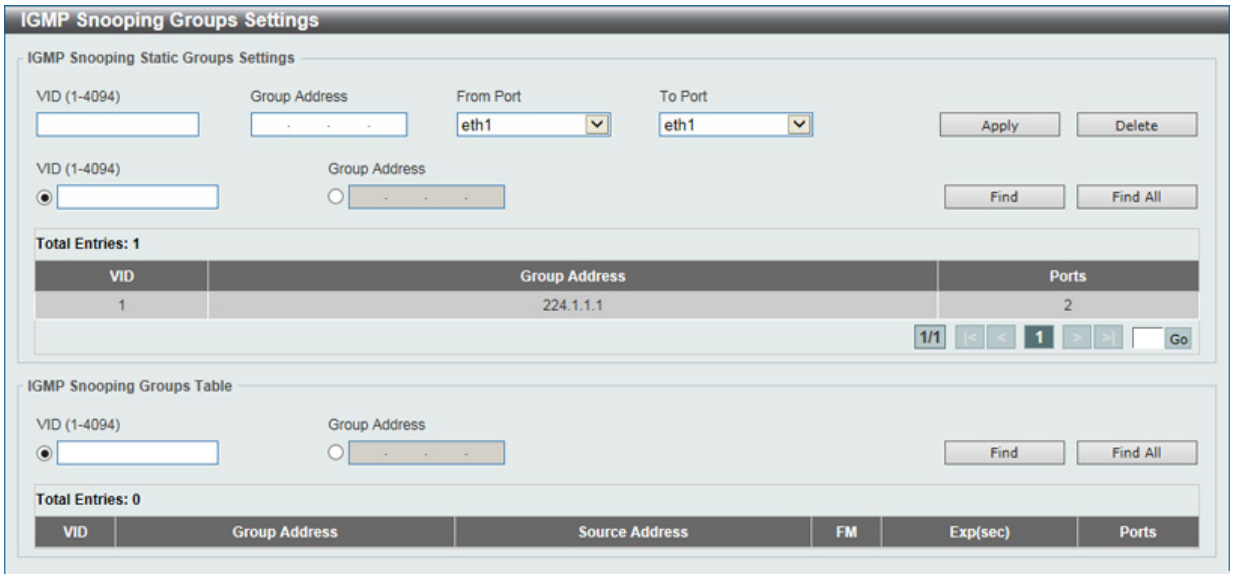

図 8-33　IGMP Snooping Group Settings 画面

以下の項目を使用して、設定します。

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

項目	説明
IGMP Snooping Static Groups Settings	
VID	登録または削除するマルチキャストグループの VLAN ID。
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。
From Port / To Port	設定するポートの範囲を設定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Find All」ボタンをクリックして、すべての定義済みエントリを表示します。

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

項目	説明
IGMP Snooping Groups Table	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。

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

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

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

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

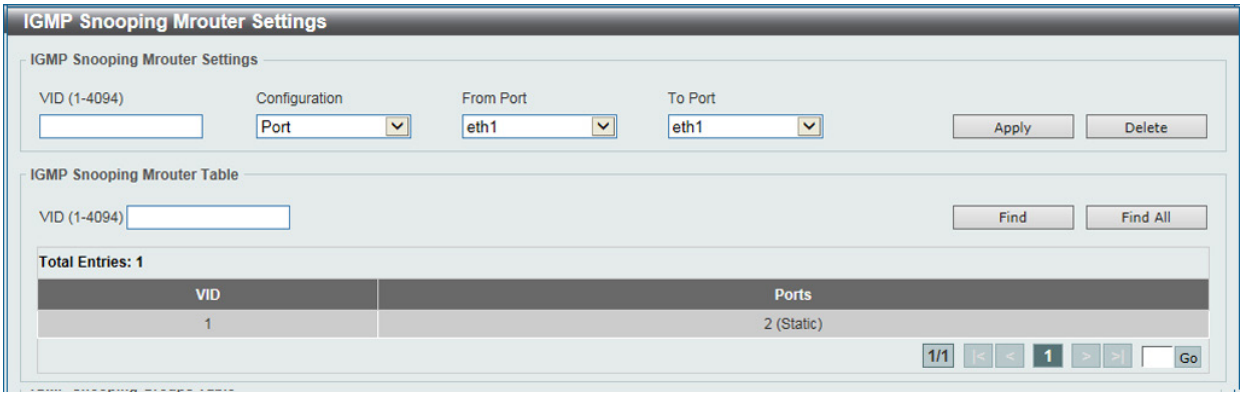

図 8-34　IGMP Snooping Mrouter Settings 画面

画面には以下の項目があります。

IGMP Snooping Mrouter Settings（IGMP スヌーピングマルチキャストルータ設定）

項目	説明
IGMP Snooping Mrouter Settings	
VID	VLAN ID を入力します。
Configuration	ポートの設定を行います。「Port」「Forbidden Port」から選択します。 • Port - マルチキャストが有効なルータと接続するポート範囲を設定します。プロトコルに関係なくマルチキャスト有効ルータに全てのパケットが届くことを確実にします。 • Forbidden Router Port - マルチキャストが有効なルータと接続しないポート範囲を設定します。禁止されたルータポートはルーティングパケットを送信しません。
From Port / To Port	設定するポートの範囲を設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

IGMP Snooping Mrouter Table（IGMP スヌーピングマルチキャストルータテーブル）

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

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

IGMP Snooping Statistics Settings（IGMP Snooping 統計設定）

現在の IGMP Snooping の統計情報を表示します。

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

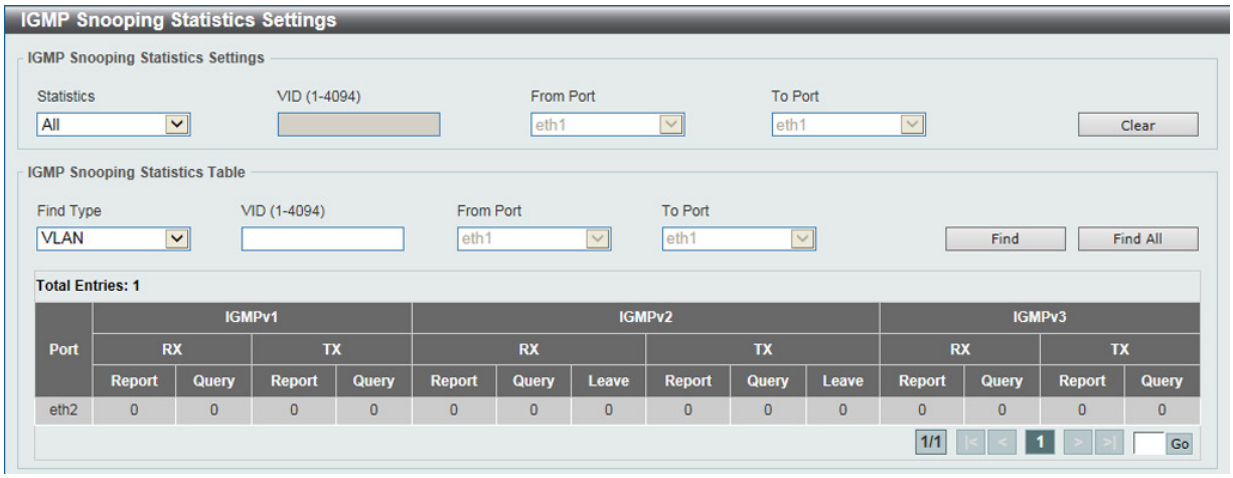

図 8-35　IGMP Snooping Statistics Settings 画面

以下の項目が表示されます。

IGMP Snooping Statistics Settings（IGMP スヌーピング統計設定）

項目	説明
Statistics	インタフェースを選択します。「All」「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Statistics」で「VLAN」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Statistics」で「Port」を選択すると設定可能になります。

「Clear」をクリックすると表示された統計情報がクリアされます。

IGMP Snooping Statistics Table（IGMP スヌーピング統計テーブル）

項目	説明
Find Type	インタフェースを選択します。「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Find Type」で「VLAN」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Find Type」で「Port」を選択すると設定可能になります。

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

注意　「IPv4 IGMP Snooping」、「IPv6 MLD Snooping」機能において「Router Port」へ「Multicast Stream」を「Flooding」する機能はありません。

MLD Snooping Settings（MLD スヌーピング）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じように使用される IPv6 機能です。マルチキャストデータを要求する VLAN に接続しているポートを検出するために使用されます。選択した VLAN 上のすべてのポートにマルチキャストトラフィックが流れる替わりに、MLD Snooping は、リクエストポートとマルチキャストの送信元によって生成する MLD クエリと MLD レポートを使用してデータを受信したいポートにのみマルチキャストデータを転送します。

MLD Snooping は、エンドノードと MLD ルータ間で交換される MLD コントロールパケットのレイヤ 3 部分を調査することで実行されます。ルータがマルチキャストトラフィックをリクエストしていることをスイッチが検出すると、該当ポートを IPv6 マルチキャストテーブルに直接追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のこのエントリは該当ポート、その VLAN ID、および関連する IPv6 マルチキャストグループアドレスを記録し、このポートをアクティブな Listening ポートと見なします。アクティブな Listening ポートはマルチキャストグループデータの受信だけをします。

MLD コントロールメッセージ

MLD Snooping を使用するデバイス間で 3 つのタイプのメッセージを交換します。これらのメッセージは、130、131、132 および 143 にラベル付けされた 4 つの ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query – IPv4 の IGMPv2 Host Membership Query（HMQ）と類似のものです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query は全マルチキャストアドレスに Listening ポートすべてにマルチキャストデータを送信する準備が整ったことを通知するために使用します。また、Multicast Specific query は特定のマルチキャストアドレスに送信準備が整ったことを通知するために使用します。 2 つのメッセージタイプは IPv6 ヘッダ内のマルチキャスト終点アドレス、および Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別します。
2. Multicast Listener Report – IGMPv2 の Host Membership Report（HMR）と類似のものです。Listening ホストは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。
3. Multicast Listener Done – IGMPv2 の Leave Group Message と類似のものです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからマルチキャストデータを受信せず、このアドレスからのマルチキャストデータとともに”done”（完了）した旨を伝えます。スイッチは本メッセージを受信すると、この Listening ホストには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しません。
4. Multicast Listener Report Version2 – IGMPv3 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

MLD Snooping Settings（MLD スヌーピング設定）

MLD Snooping 設定を有効または無効にします。

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

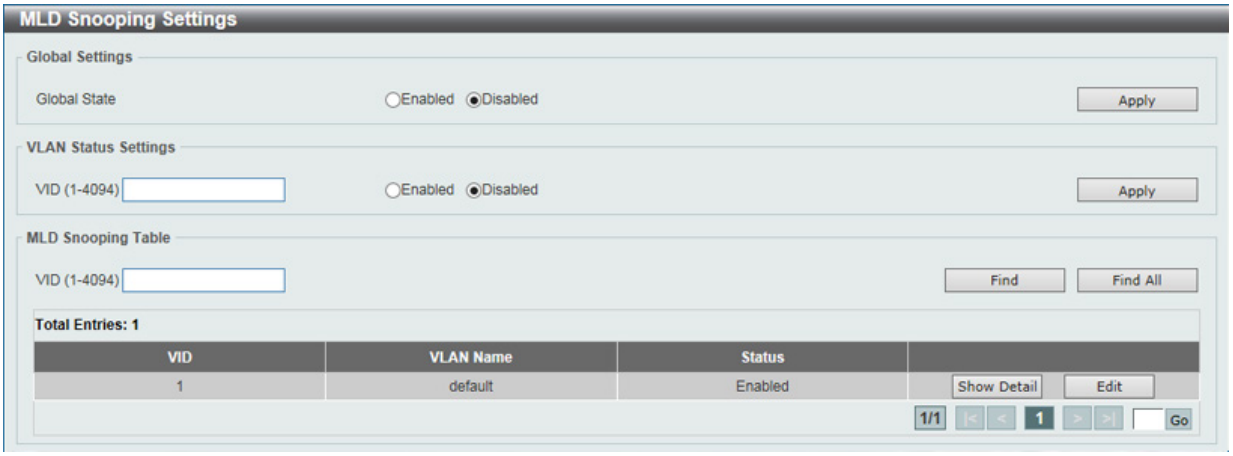

図 8-36　MLD Snooping Settings 画面

画面には以下の項目があります。

項目	説明
Global Setting	
Global State	MLD Snooping の有効 / 無効を設定します。 • Enabled - デバイスで MLD Snooping を有効にします。 • Disabled - デバイスで MLD Snooping を無効に設定します。（初期値）
VLAN Status Settings	
VID	VLAN 上の MLD Snooping を有効 / 無効にし、VLAN を識別する VLAN ID を指定します。 • Enabled - VLAN を有効にします。 • Disabled - VLAN を無効に設定します。（初期値）
MLD Snooping Table	
VID	MLD Snooping Table 上の VLAN を表示させるための VLAN ID を指定します。 • Find - 指定の VLAN ID を入力して指定のエントリを表示します。 • Find All - MLD Snooping Table 上のすべてのエントリを表示します。

「Find」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。
「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。

MLD Snooping VLAN の詳細情報表示

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

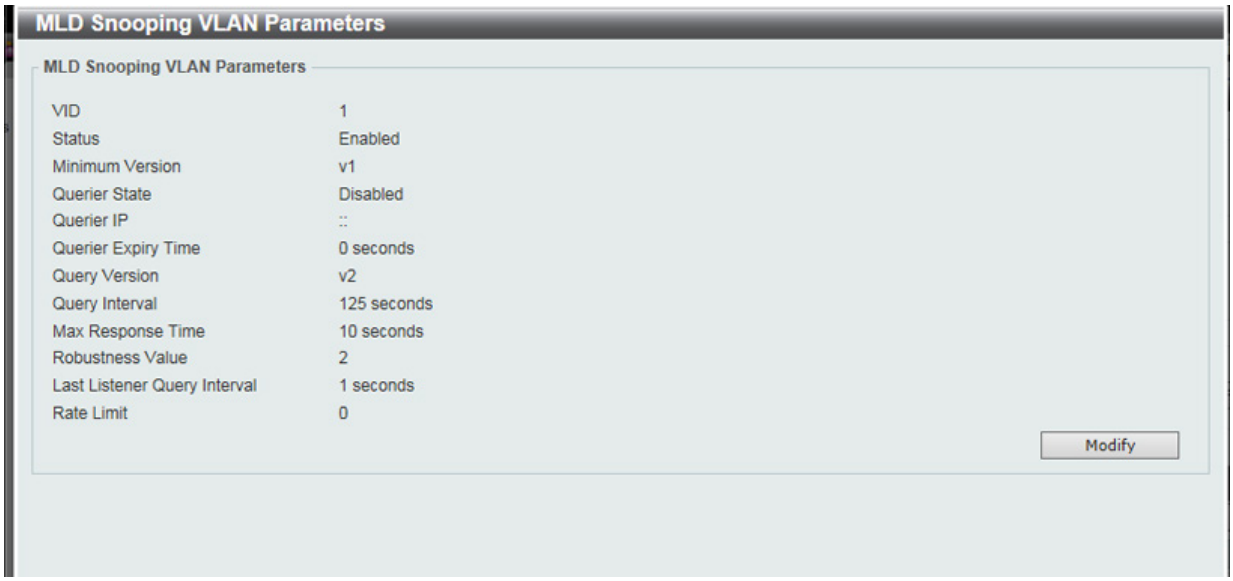

図 8-37　MLD Snooping VLAN Parameters 画面

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 VLAN の詳細設定

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

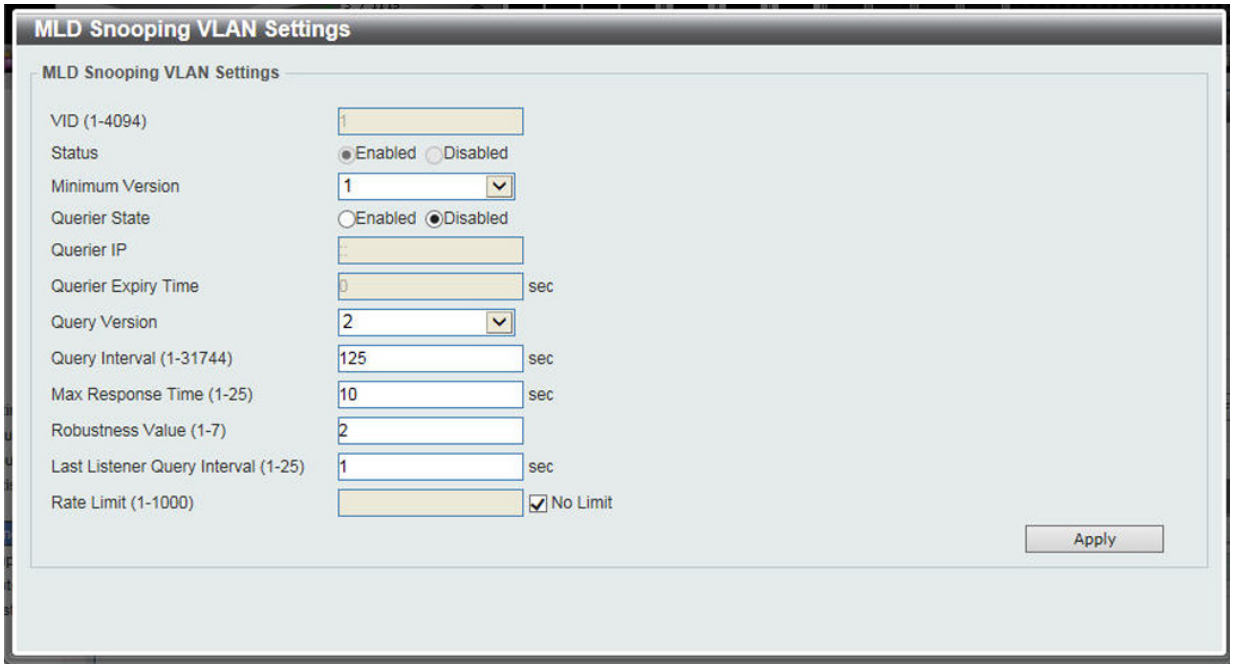

図 8-38 MLD Snooping VLAN Settings 画面

以下の項目が表示、または設定変更に使用できます。

項目	説明
VID	MLD Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
Status	指定した VLAN への MLD Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。
Minimum Version	VLAN に許可された MLD ホストの最小バージョンを選択します。
Querier State	「Enabled」（有効）にすると MLD Query パケットを送信可能になります。初期値は「Disabled」（無効）です。
Query Version	MLD スヌーピングクエリアに送信されるクエリパケットのバージョンを選択します。「1」「2」から選択可能です。
Query Interval	MLD query 送信間隔（秒）。1-31744 の範囲から指定します。初期値は 125 です。
Max Response Time (1-25)	MLD response report を送信するまでの最大時間（秒）。1-25 の範囲から指定します。初期値は 10（秒）です。

項目	説明
Robustness Value (1-7)	パケットロスへの抵抗力を示します。予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を取ります。1-255 の範囲から指定します。初期値は 2 です。
Last Listener Query Interval	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の Max Response Time 欄に設定する値（Last Listener Query Interval）。また、同 Query の送信間隔でもあります。初期値は 1 です。
Rate Limit	使用する MLD Snooping の Rate Limit を指定します。「No Limit」にチェックを入れるとリミットは無視されます。

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

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

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

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

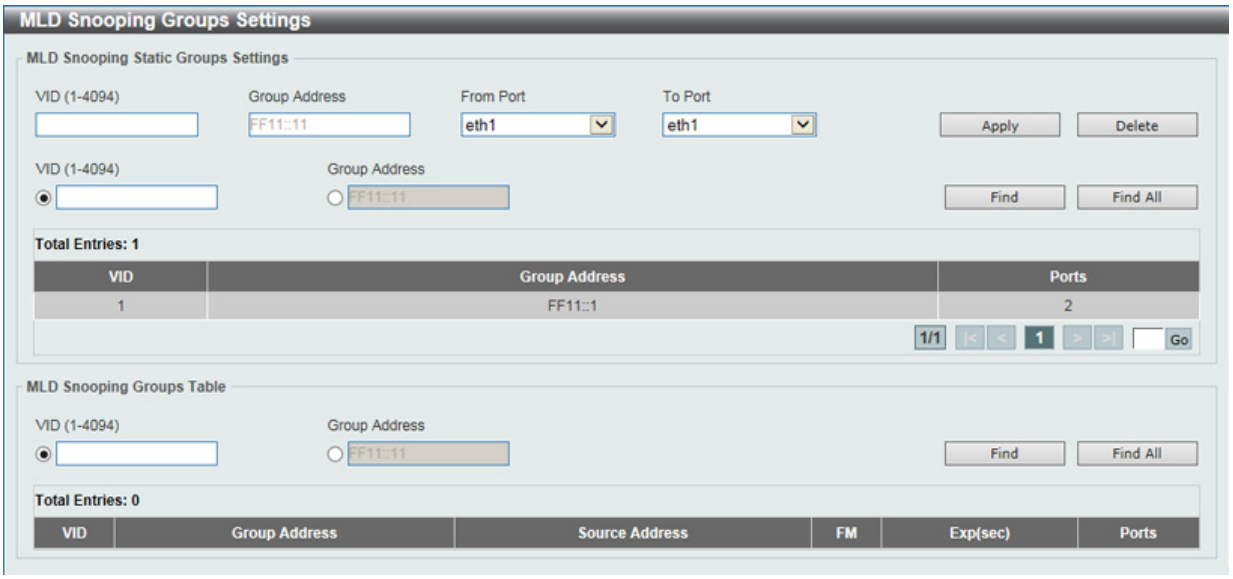

図 8-39　MLD Snooping Group Settings 画面

以下の項目を使用して、設定します。

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

項目	説明
MLD Snooping Static Groups Settings	
VID	登録または削除する IPv6 マルチキャストグループの VLAN ID。
Group Address	登録または削除する IPv6 マルチキャストグループの IP アドレス。
From Port / To Port	設定するポートの範囲を設定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「Find All」ボタンをクリックして、すべての定義済みエントリを表示します。

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

項目	説明
MLD Snooping Groups Table	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。
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。

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

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

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

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

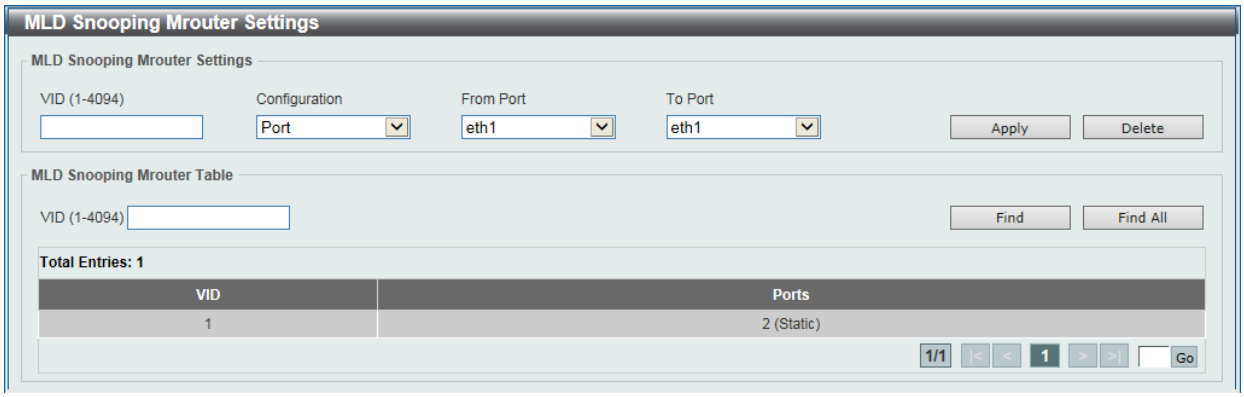

図 8-40　MLD Snooping Mrouter Settings 画面

画面には以下の項目があります。

MLD Snooping Mrouter Settings（MLD スヌーピングマルチキャストルータ設定）

項目	説明
MLD Snooping Mrouter Settings	
VID	VLAN ID を入力します。
Configuration	ポートの設定を行います。「Port」「Forbidden Port」「Learn pimv6」から選択します。 • Port - マルチキャストが有効なルータと接続するポート範囲を設定します。プロトコルに関係なくマルチキャスト有効ルータに全てのパケットが届くことを確実にします。 • Forbidden Port - マルチキャストが有効なルータと接続しないポート範囲を設定します。禁止されたルータポートはルーティングパケットを送信しません。
From Port / To Port	設定するポートの範囲を設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用します。
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

MLD Snooping Mrouter Table（MLD スヌーピングマルチキャストルータテーブル）

項目	説明
MLD Snooping Mrouter Table	
VID	VLAN ID を入力します。

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

MLD Snooping Statistics Settings（MLD Snooping 統計設定）

現在の MLD Snooping の統計情報を表示します。

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

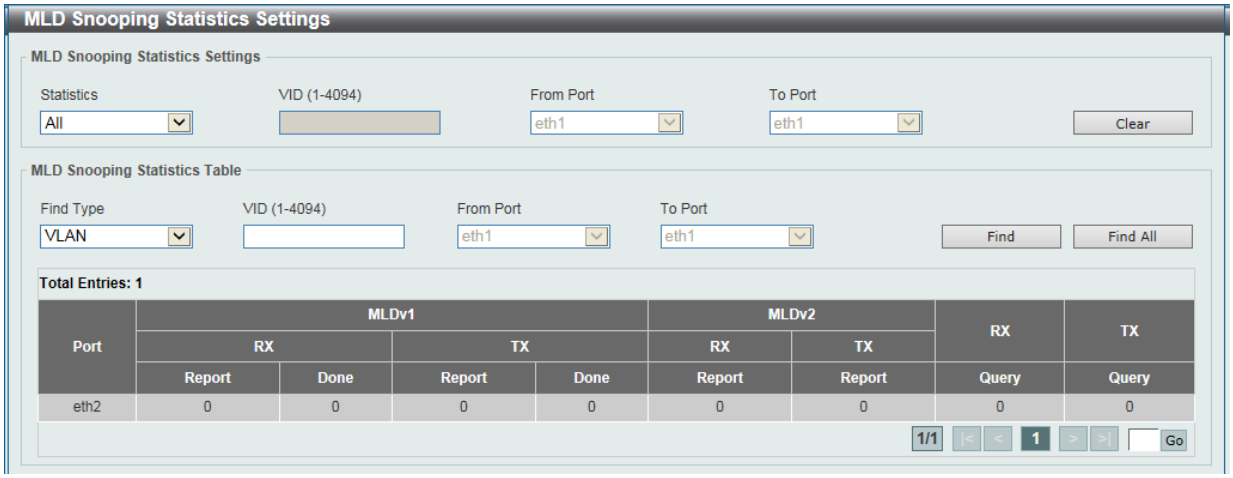

図 8-41　MLD Snooping Statistics Settings 画面

以下の項目が表示されます。

MLD Snooping Statistics Settings（MLD スヌーピング統計設定）

項目	説明
Statistics	インタフェースを選択します。「All」「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Statistics」で「VLAN」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Statistics」で「Port」を選択すると設定可能になります。

「Clear」をクリックすると表示された統計情報がクリアされます。

MLD Snooping Statistics Table（MLD スヌーピング統計テーブル）

項目	説明
Find Type	インタフェースを選択します。「VLAN」「Port」から選択します。
VID	VLAN ID1 から 4094 の間で指定します。「Find Type」で「VLAN」を選択すると設定可能になります。
From Port / To Port	設定するポートの範囲を設定します。「Find Type」で「Port」を選択すると設定可能になります。

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

Multicast Filtering（マルチキャストフィルタリング）

プロファイルを追加し、指定したスイッチポートに受信するマルチキャストアドレスレポートを設定します。

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

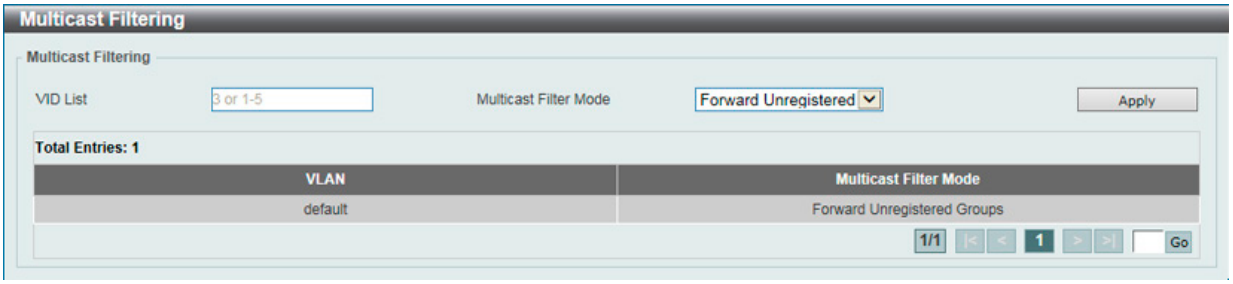

図 8-42　Multicast Filtering 画面

以下の項目を使用して、設定します。

項目	説明
VID List	設定する VLAN の VLAN ID リストを入力します。
Multicast Filter Mode	マルチキャストフィルタモードを選択します。 「Forward Unregistered」「Forward All」「Filter Unregistered」から選択可能です。 • 「Forward Unregistered」- 選択すると登録されたマルチキャストパケットはフォワーディングテーブルに基づいて転送され、登録されていないマルチキャストパケットは VLAN ドメインに基づきフラッドします。 • 「Forward All」- 選択するとすべてのマルチキャストパケットは VLAN ドメインに基づきフラッドします。 • 「Filter Unregistered」- 選択すると登録されたマルチキャストパケットはフォワーディングテーブルに基づき転送され、登録されていないマルチキャストパケットはフィルタされます。

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

LLDP（LLDP 設定）

本スイッチは IEEE 802.1AB に準拠した LLDP（Link Layer Discovery Protocol）に準拠しており、隣接する LLDP デバイスにそれぞれの情報を通知し、お互いを認識します。本プロトコルによって送信される情報は、受信先によって標準の管理情報ベース（MIB）に格納されるので、SNMP（Simple Network Management Protocol）などの管理プロトコル使ったネットワーク管理システム（NMS）からその情報にアクセスできるようになります。

LLDP Global Settings（LLDP グローバル設定）

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

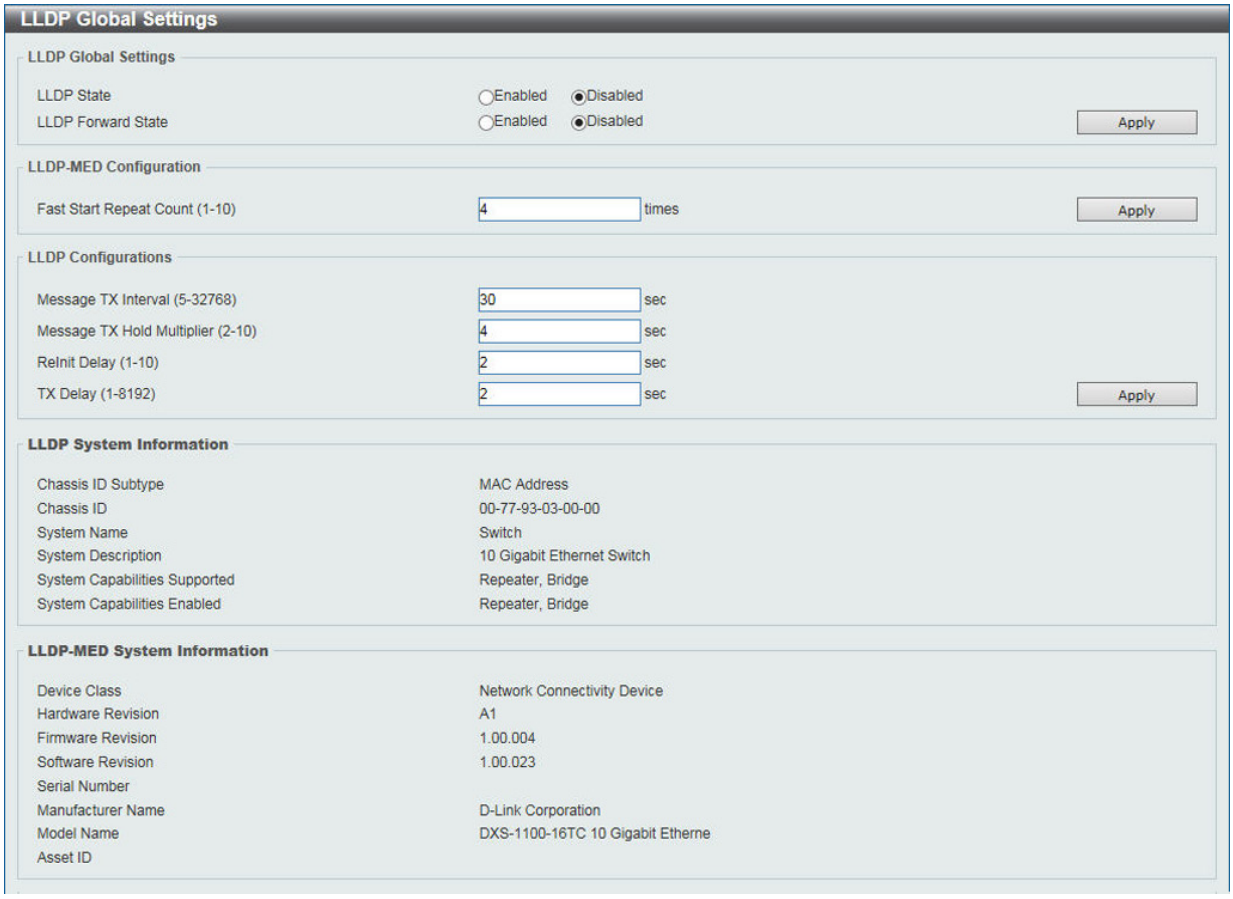

図 8-43　LLDP Global Settings 画面

以下の項目を設定できます。

項目	説明
LLDP State	スイッチにおける LLDP 機能を「Enabled」（有効）または「Disabled」（無効）にします。
LLDP Forward State	同じ IEEE 802 ネットワークに割り当てられた他のステーションに通知するために LLDP 機能のメッセージ転送を「Enabled」（有効）または「Disabled」（無効）にします。 「LLDP」が 無効で「LLDP Forward Sate」が有効の場合、受信した「LLDPDU」パケットは転送されます。
Fast Start Repeat Count	「LLDP-MED」ファストスタートリピートカウント値を指定します。1 から 10 の間で指定できます。
Message TX Interval (5-32768)	アクティブなポートが通知を再送する方法を制御します。パケット伝送間隔を変更するために、5-32768（秒）の範囲で値を入力します。
Message TX Hold Multiplier (2-10)	LLDP スイッチに使用される乗数を変更することで LLDP Neighbor に LLDP 通知を作成して送信する有効期間（TTL : Time-to-Live）を計算します。指定通知の TTL（Time-to-Live）の期限が来ると、通知データは Neighbor スイッチの MIB から削除されます。
ReInit Delay (1-10)	LLDP ポートが LLDP 無効にするコマンドを受け取った後、再初期化を行う前に待機する最小時間です。LLDP Reinit Delay を変更するために、1-10（秒）から値を入力します。
TX Delay (1-8192)	LLDP MIB のコンテンツ変更のために、LLDP ポートが連続した LLDP 通知の送信を遅らせる最短時間（遅延間隔）を変更します。LLDP TX Delay を変更するために、1-8192（秒）から値を入力します。

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

LLDP Port Settings（LLDP ポート設定）

LLDP ポートパラメータを設定します。

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

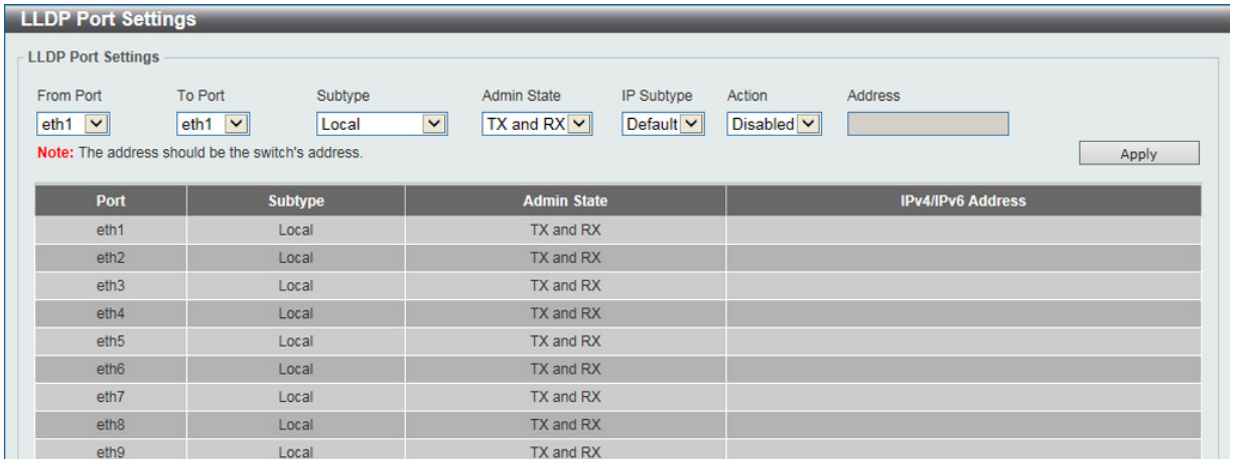

図 8-44　LLDP Port Settings 画面

以下の項目を設定できます。

項目	説明
From Port/To Port	プルダウンメニューを使用して設定するポート範囲を指定します。
Subtype	プルダウンメニューを使用して LLDP TLV(s) のサブタイプを選択します。「MAC Address」「Local」から選択可能です。
Admin State	プルダウンメニューを通知のステータスを選択します。: Tx（送信のみ）、Rx（受信のみ）、Tx And Rx（送受信）または「Disabled」（無効）。 TX - ローカル LLDP エージェントは LLDP フレーム送信のみします。 RX - ローカル LLDP エージェントは LLDP フレーム受信のみします。 TX and RX - ローカル LLDP エージェントは LLDP フレームの送受信をします。 Disabled - ローカル LLDP エージェントは LLDP フレームの送受信をしません。 初期値は TX and RX です。
IP Subtype	プルダウンメニューを使用して送信する IP アドレスの種類を選択します。
Address	通知するエンティティの管理アドレスを入力します。
Action	ポートベースの管理アドレス機能を「Enabled」（有効）または「Disabled」（無効）にします。

「Apply」ボタンをクリックし、変更を有効にします。

注意　入力する IPv4/IPv6 アドレスは、既存の LLDP 管理 IP アドレスである必要があります。

LLDP Management Address List（LLDP 管理アドレスリスト）

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 8-45　LLDP Management Address List 画面

以下の項目を設定できます。

項目	説明
All/IPv4/IPv6	通知するエンティティの管理 IP アドレスを選択します。

「Find」ボタンをクリックし、LLDP 管理情報を検索します。

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

TLV（Type-length-value）は、LLDP パケット内の TLV エレメントとして特定の送信情報を許可します。本スイッチにおけるベーシック TLV 設定を有効にします。スイッチのアクティブな LLDP ポートは、通常その外向き通知にいつも必須データを含んでいます。外向き LLDP 通知からこれらのデータタイプの 1 個以上を除外するために、個別のポートまたはポートグループに設定できる 4 つのオプションデータがあり、必須データタイプには、4 つの基本的な情報タイプ（end f LLDPDU TLV、chassis ID TLV、port ID TLV および Time to Live TLV）があります。必須データタイプは無効にすることができません。さらに、オプションで選択可能な 4 つのデータタイプ（Port Description、System Name、System Description および System Capability）があります。
本スイッチにおけるベーシック TLV 設定を有効にします。

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

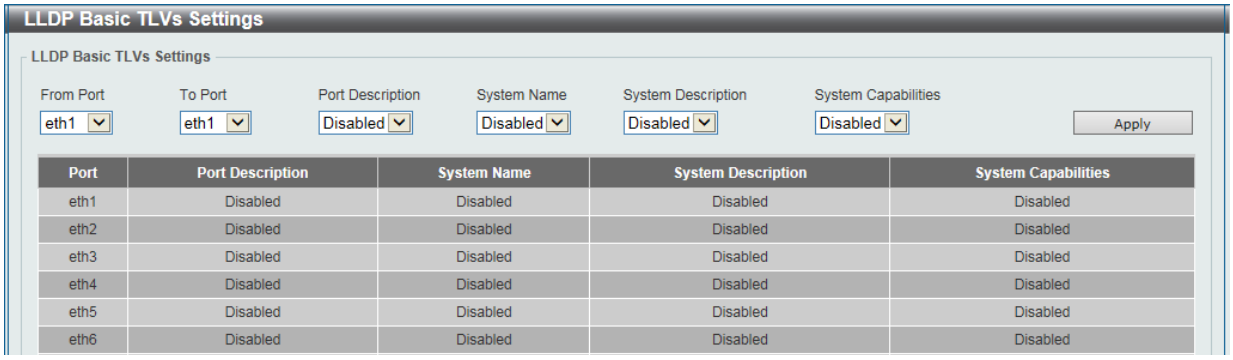

図 8-46　LLDP Basic TLVs Settings 画面

プルダウンメニューを使用してベーシック TLV 設定を「Enabled」（有効）/「Disabled」（無効）にします。

以下の項目を設定できます。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
Port Description	ポート説明を「Enabled」（有効）/「Disabled」（無効）にします。
System Name	システム名を「Enabled」（有効）/「Disabled」（無効）にします。
System Description	システム説明を「Enabled」（有効）/「Disabled」（無効）にします。
System Capabilities	システム能力を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

LLDP Dot1 TLV は、IEEE 802.1 によって組織的に定義されている TLV で、送信する LLDP 通知から IEEE 802.1 規定のポート VLAN ID の TLV データタイプを除外するようにポートやポートグループを設定する時に使用します。

L2 Features > LLDP > LLDP Dot1 TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

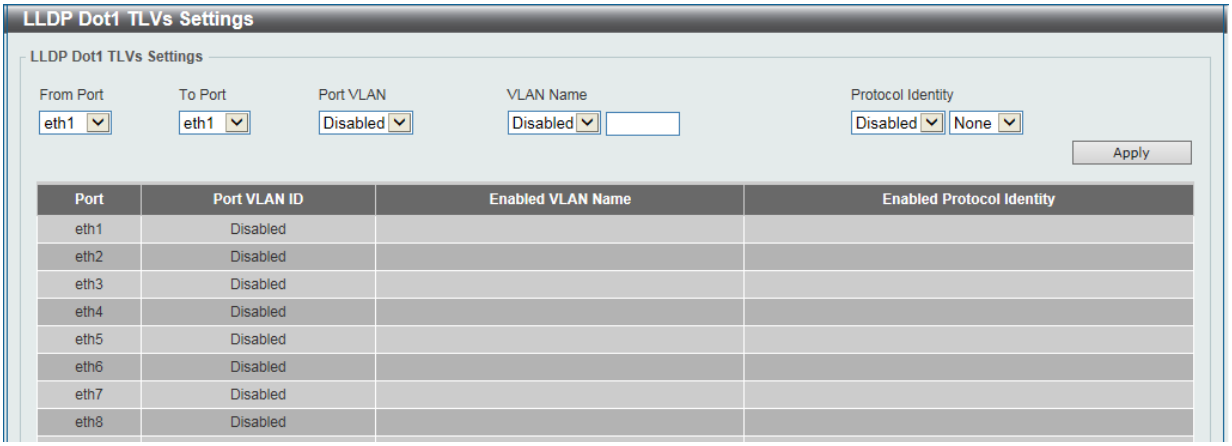

図 8-47　LLDP Dot1 TLVs Settings 画面

以下の項目が使用できます。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
Port VLAN	ポート VLAN ID TLV の通知を「Enabled」（有効）/「Disabled」（無効）にします。 「ポート VLAN ID TLV」は VLAN ブリッジポートにタグなし・タグ付きフレームの PVID の通知を許可するオプションのフィックス長 TLV です。
VLAN Name	VLAN 名の通知を「Enabled」（有効）/「Disabled」（無効）にします。 対象となるプロトコル VLAN を右の欄で VLAN ID で指定します。
Protocol Identity	プロトコル識別子の通知を「Enabled」（有効）/「Disabled」（無効）にします。 次に対象とするプロトコルを None、LACP、STP または All から選択します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

個別のポートやポートグループが送信する LLDP 通知から IEEE 802.3 規定のポート VLAN ID TLV データタイプを除外するように設定します。

L2 Features > LLDP > LLDP Dot3 TLVs Settings の順にメニューをクリックし、以下の画面を表示します。

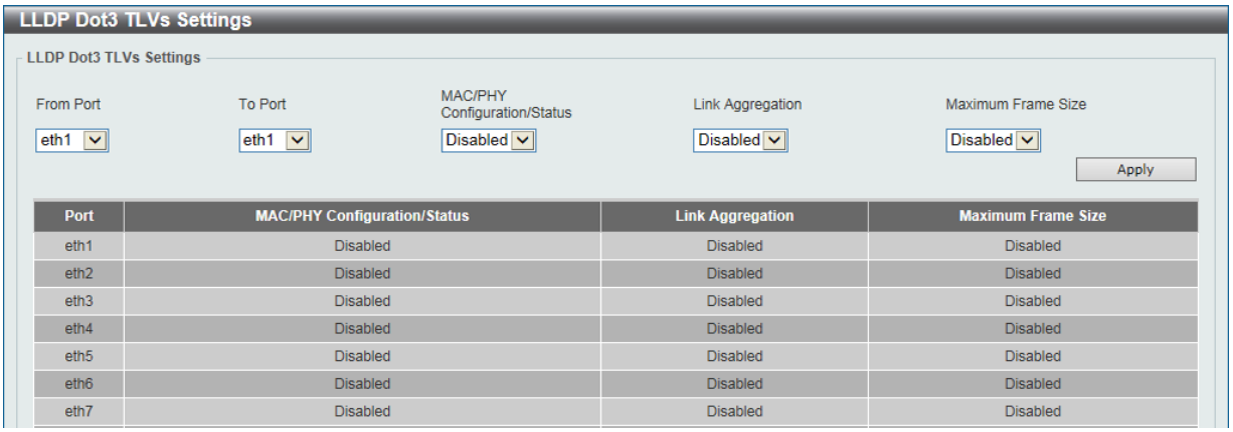

図 8-48　LLDP Dot3 TLVs Settings 画面

以下の項目を設定できます。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
MAC/PHY Configuration Status	スイッチの MAC または PHY 状態の通知を「Enabled」（有効）/「Disabled」（無効）にします。
Link Aggregation	スイッチのリンクアグリゲーション状態の通知を「Enabled」（有効）/「Disabled」（無効）にします。
Maximum Frame Size	最大フレームサイズの通知を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、変更を有効にします。

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

LLDP-MED TLV の送信を有効または無効にします。

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

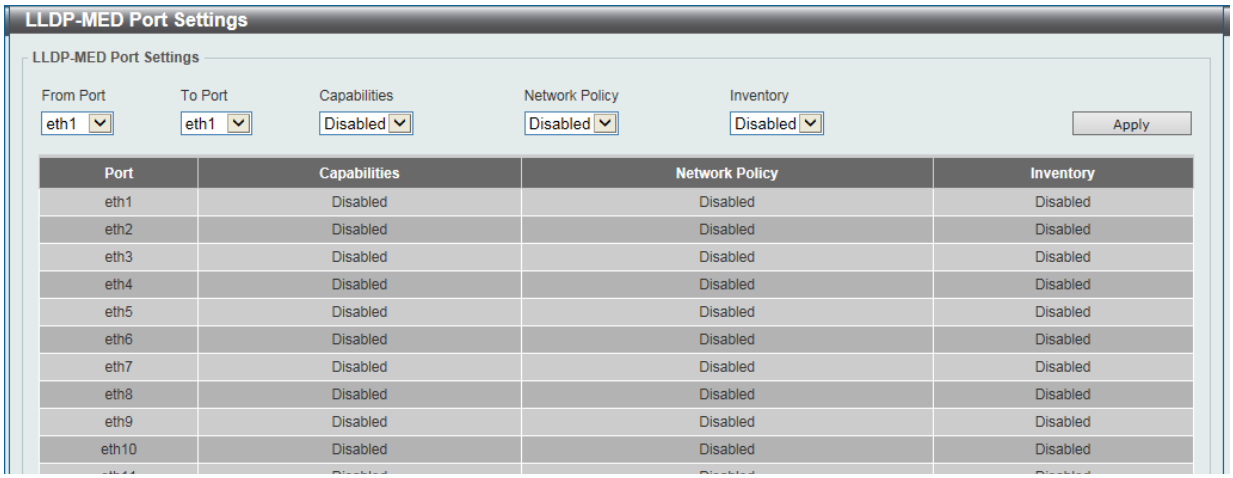

図 8-49　LLDP-MED Port Settings 画面

以下の項目が使用できます。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Capabilities	「LLDP-MED capabilities TLV」の送信を有効 / 無効にします。
Network Policy	「LDP-MED network policy TLV」の送信を有効 / 無効にします。
Inventory	「LLDP-MED inventory TLV」の送信を有効 / 無効にします。

「Apply」ボタンをクリックして変更を適用します。

LLDP Statistics Information（LLDP 統計情報）

スイッチにおける LLDP 統計情報と各ポートの設定を参照できます。

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

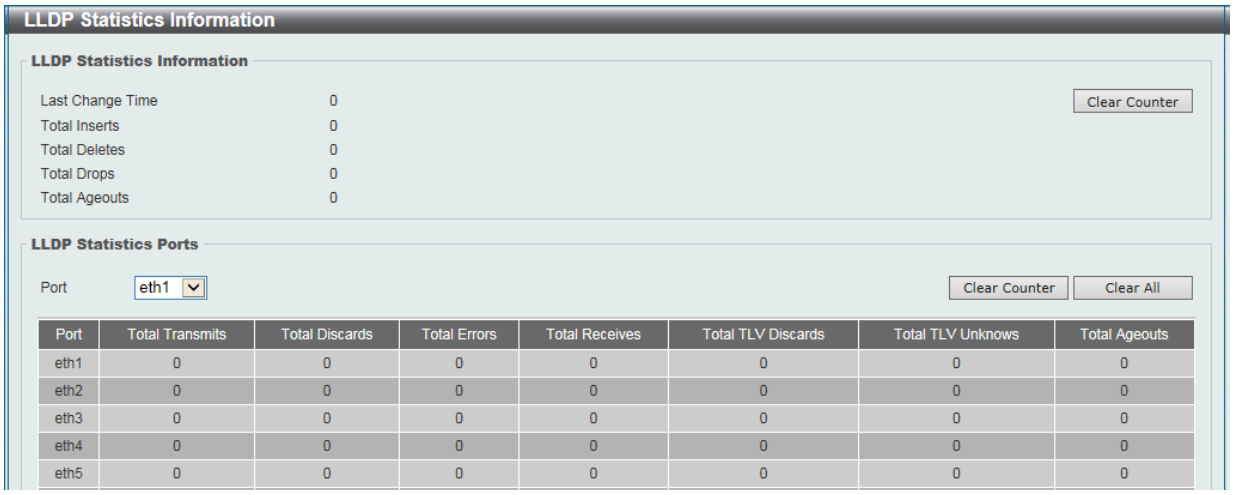

図 8-50　LLDP Statistics Information 画面

以下の項目が使用できます。

項目	説明
Port	表示するポートを指定します。

「Clear Counter」をクリックして統計情報のカウンタ数をクリアします。
「Clear All」をクリックしてすべてのカウンタ数をクリアします。

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

以下のローカルポートの要約テーブルにポートベースの情報を表示します。

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

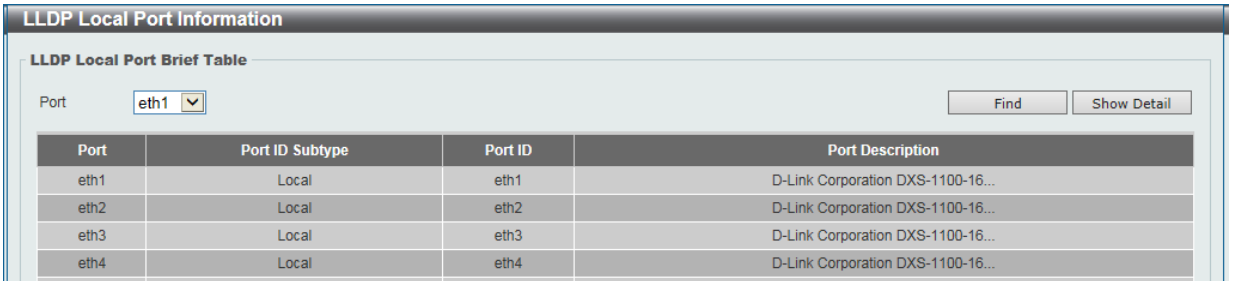

図 8-51　LLDP Local Port Information 画面

以下の項目が使用できます。

項目	説明
Port	表示するポートを指定します。

ポートを選択し、「Find」ボタンをクリックします。情報が画面下半分に表示されます。

各パラメータの詳細の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。

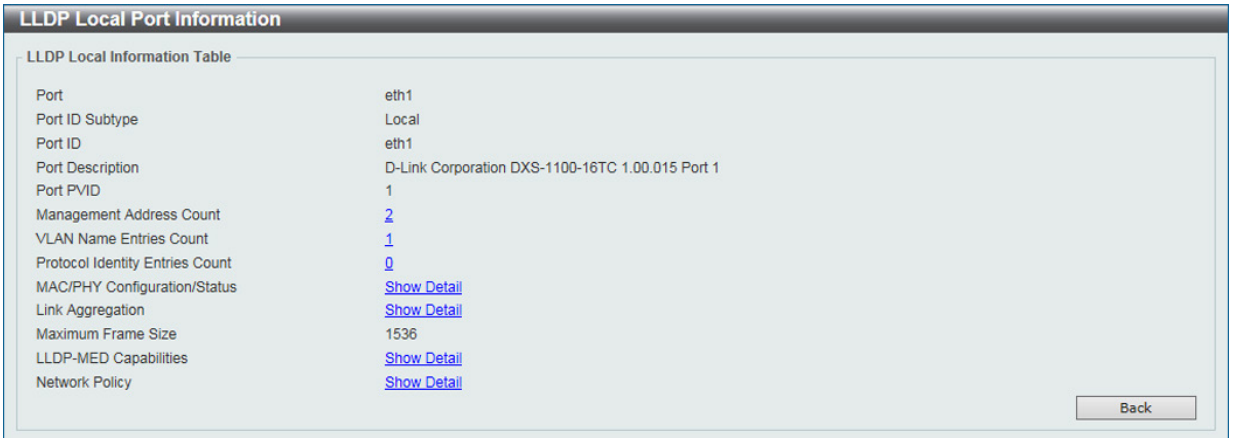

図 8-52　LLDP Local Port Information（Show Detail）画面

「MAC/PHY Configuration/Status」情報の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。

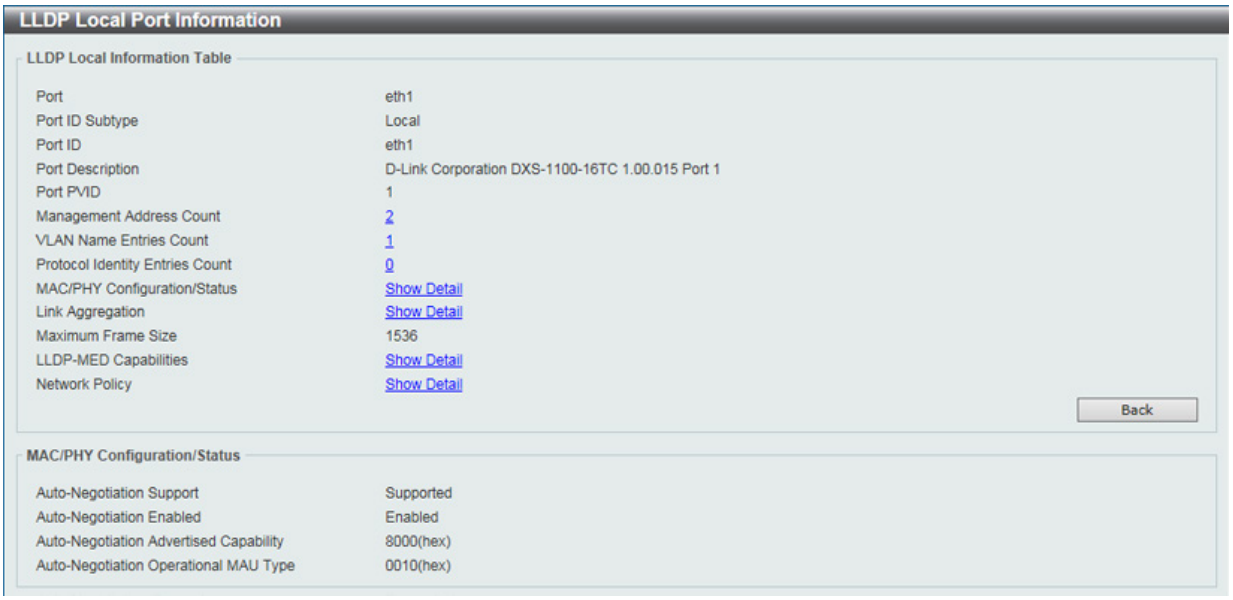

図 8-53　LLDP Local Port Information - MAC/PHY Configuration/Status 画面

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

Neighbor から学習したポート情報を表示します。

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

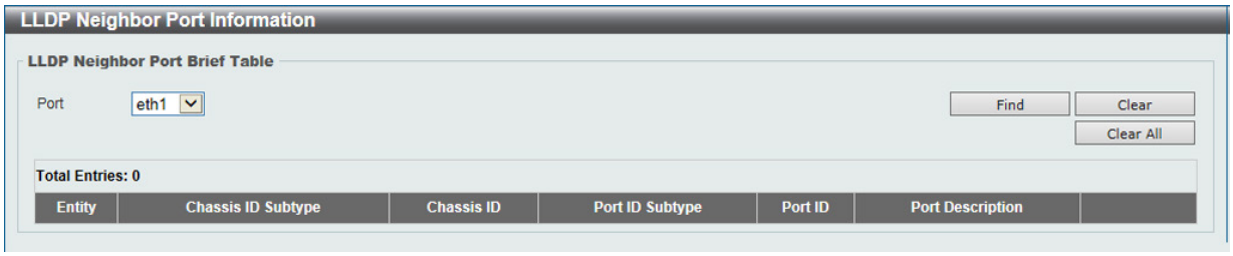

図 8-54　LLDP Neighbor Port Information 画面

以下の項目が使用できます。

項目	説明
Port	表示するポートを指定します。

ポートを選択し、「Find」ボタンをクリックします。情報が画面下半分に表示されます。
「Clear」をクリックしてポート情報をクリアします。
表示されているすべてのポート情報を削除するには、「Clear All」ボタンをクリックします。

第 9 章　L3 Features（レイヤ 3 機能）

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	参照ページ
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。	98
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。	99
IPv6 Neighbor（IPv6 Neighbor 設定）	IPv6 ネイバの設定を行います。	100
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。	101

IPv4 Interface（IPv4 インタフェース）

IP インタフェースの設定を行う場合は **L3 Features > IPv4 Interface** から設定を行います。

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

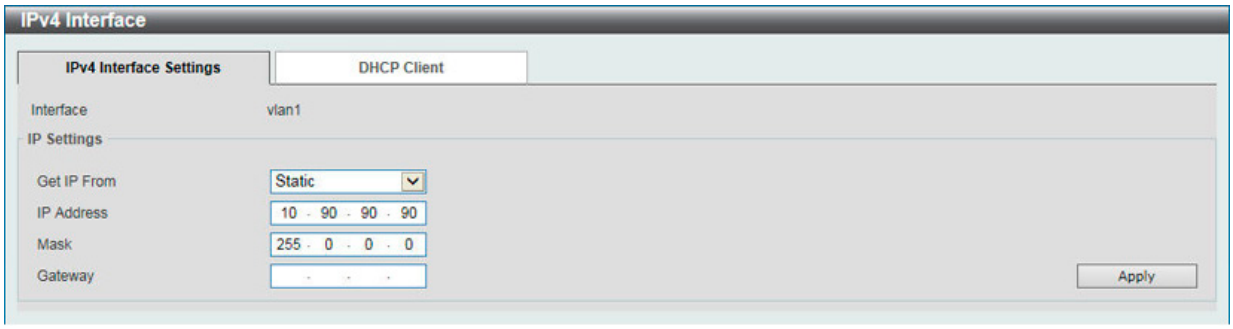

図 9-1　IPv4 Interface 画面

以下の項目を使用して設定を行います。

項目	説明
Interface	設定、表示するインタフェースの VLAN ID です。
Get IP From	IPv4 アドレス、サブネットマスク、デフォルトゲートウェイに設定する「Static」「DHCP」「BOOTP」プロトコルを選択します。
IP Address	IPv4 インタフェースに割り当てる IPv4 アドレスを入力します。
Mask	IPv4 インタフェースに割り当てるサブネットマスクを入力します。
Gateway	IPv4 インタフェースに割り当てるゲートウェイを入力します。

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

IPv4 インタフェースの編集（DHCP Client）

「IPv4 Interface」の「DHCP Client」タブをクリックして以下の画面を表示します。

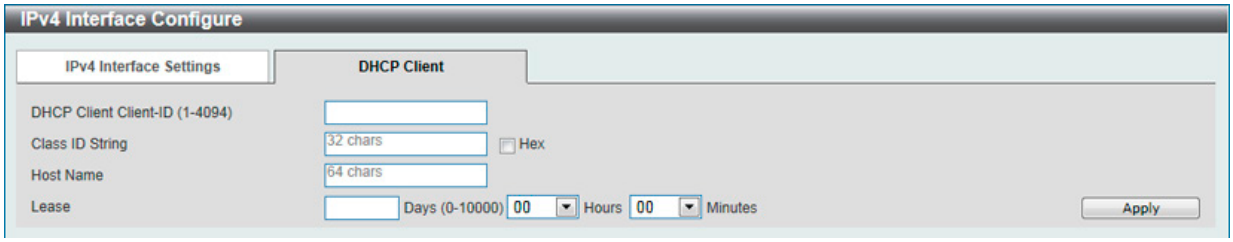

図 9-2　DHCP Client 画面

画面には以下の項目が表示されます。

項目	説明
DHCP Client Client-ID	VLAN インタフェースをです。
Class ID String	最大 32 文字を使用してベンダクラス識別名を入力します。「Hex」にチェックを入れると 16 進数方式になります。
Host Name	ホスト名を入力します。最大 64 文字で入力可能です。ホスト名はアルファベットで始まり、アルファベットまたは数字で終わるようにします。
Lease	DHCP サーバから割り振られる IP アドレスのリース時間（時間 / 分）を指定します。

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

注意　IPv4/IPv6 インタフェースは VLAN1 にのみ設定可能です。

IPv6 Interface（IPv6 インタフェース）

IPv6 インタフェースの設定を行う場合は **L3 Features > IPv6 Interface** から設定を行います。

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

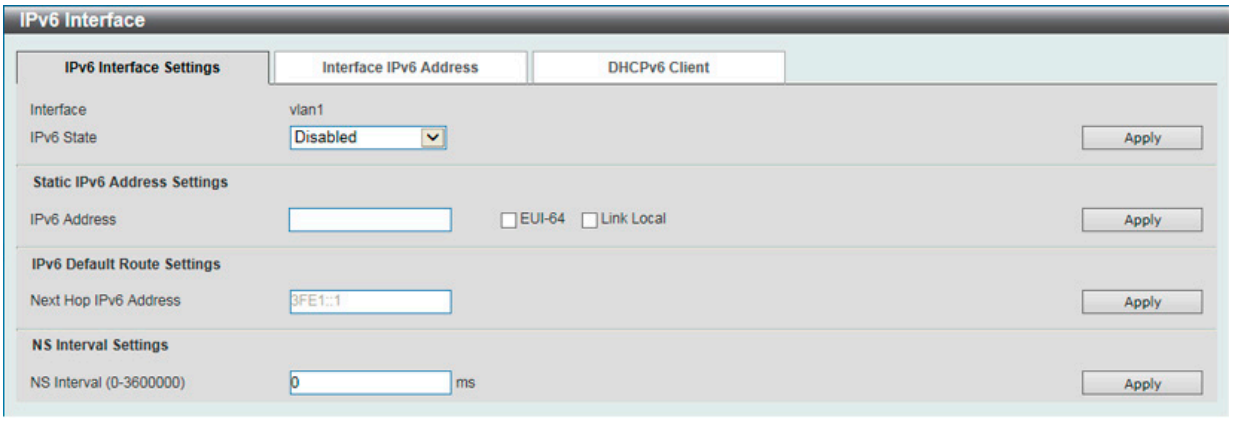

図 9-3　IPv6 Interface 画面

以下の項目を使用して設定を行います。

項目	説明
Interface	設定、表示するインタフェースの VLAN ID です。
IPv6 State	該当エントリの IPv6 インタフェースをグローバルに有効 / 無効にします。
IPv6 Address	IPv6 インタフェースに割り当てる IPv6 アドレスを入力します。 「EUI-64」- EUI-64 インタフェース ID を使用してインタフェースの IPv6 アドレスを設定します。 「Link Local」- IPv6 インタフェースにリンクローカルアドレスを使用します。
Next Hop IPv6 Address	Next Hop IPv6 アドレスを入力します。
NS Interval	NS Interval を 0 から 3600000 ミリ秒で設定します。

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

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

「Interface IPv6 Address」タブをクリックして以下の画面を表示します。

図 9-4　Interface IPv6 Address 画面

エントリの削除

対象のエントリの「Delete」ボタンをクリックします。

IPv6 インタフェースの編集（DHCPv6 Client）

「DHCPv6 Client」タブをクリックして以下の画面を表示します。

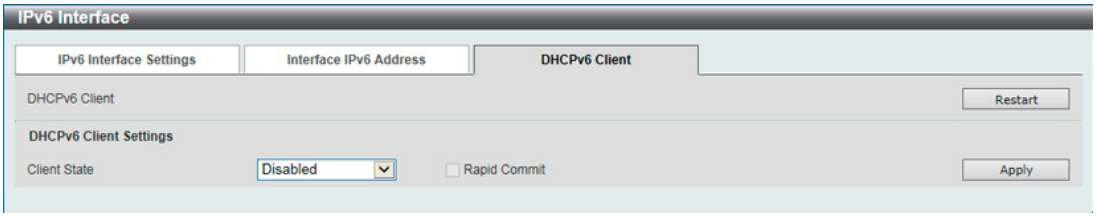

図 9-5　DHCPv6 Client 画面

画面には以下の項目が表示されます。

項目	説明
DHCPv6 Client	「Restart」をクリックするとインタフェースの DHCPv6 クライアントはリスタートします。
Client State	DHCPv6 クライアントを有効 / 無効に指定します。「Rapid Commit」にチェックを入れると、プリフィクス委任のメッセージ交換を実行します。

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

注意　IPv4/IPv6 インタフェースは VLAN1 にのみ設定可能です。

IPv6 Neighbor（IPv6 Neighbor 設定）

IPv6 Neighbor は、IPv6 デバイスして検出された Link-Local ネットワーク上のデバイスです。これらのデバイスは、パケットを転送し、ネットワーク上のノードの Link-Layer アドレスに変更が発生しているか、または同一のユニキャストアドレスがローカルリンク上に存在するかなどルータの到達性を絶えずモニタしています。以下の 2 つの画面では、IPv6 Neighbor の追加と参照、または Neighbor キャッシュからの削除を行います。

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。

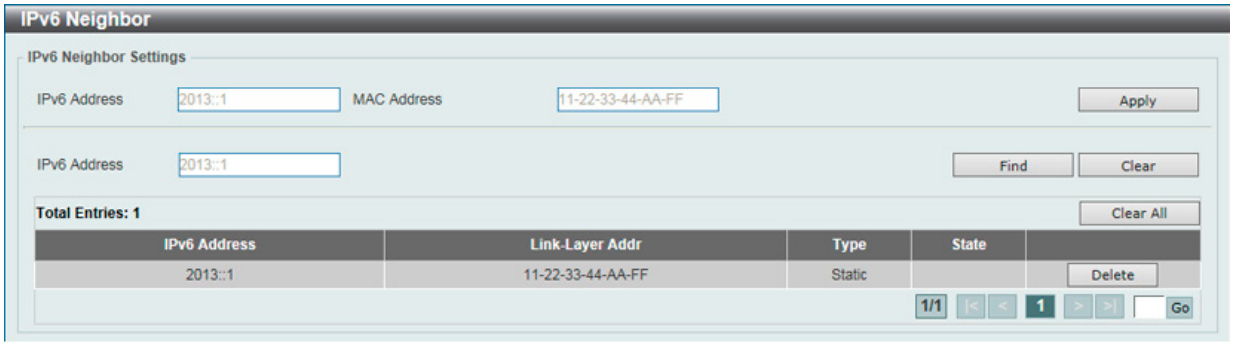

図 9-6　IPv6 Neighbor 画面

「IPv6 Neighbor」画面には次の項目があります。

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

IPv6 Neighbor の新規登録
画面上段の「IPv6 Address」および「MAC Address」を入力し、「Apply」ボタンをクリックします。

エントリの検索
画面中央の「IPv6 Address」を入力し「Find」ボタンをクリックします。

検索結果の削除
検索結果を削除するには、「Clear」、表示されているすべてのエントリを削除するには、「Clear All」ボタンをクリックします。

エントリの削除
該当エントリの「Delete」ボタンをクリックします。

IPv6 Route Table（IPv6 ルートテーブル）

現在の IPv6 ルーティングテーブルを表示します。

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

図 9-7　IPv6 Route Table 画面

第 10 章　QoS（QoS 機能の設定）

本スイッチは、802.1p キューイング QoS（Quality of Service）をサポートしています。QoS メニューを使用し、本スイッチにセキュリティ機能を設定することができます。

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

サブメニュー	説明	参照ページ
Basic Settings（基本設定）	QoS、CoS キューマッピングなどの設定を行います。	102
Advanced Settings（アドバンス設定）	DSCP/CoS のマップ設定などを行います。	105

Basic Settings（基本設定）

Port Default CoS（ポートデフォルト CoS 設定）

各ポートにデフォルト CoS の設定を行います。

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

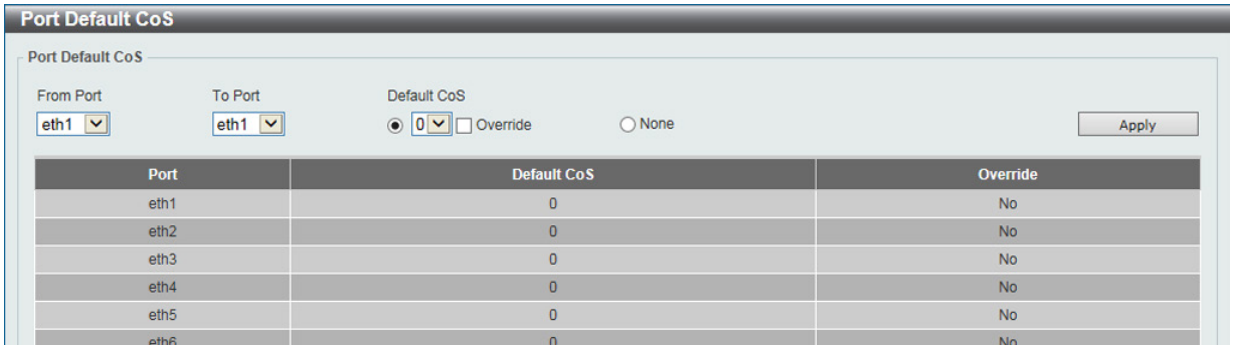

図 10-1　Port Default CoS 画面

本画面には以下の項目があります。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
Default CoS	ポートに初期 CoS を指定します。0 から 7 の間で指定可能です。「Override」にチェックを入れるとポートに受信したすべてのパケット（タグありなし関わらず）にポートの CoS が適用されます。「None」を選択すると、初期設定を有効にします。プライオリティを割り当てるクラス（キュー）を設定します。「Class-0」（クラス 0）は最も低い優先度のキューで、「Class-7」（クラス 7）が最も高くなります。

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

Port Scheduler Method（ポートスケジューラーメソッド設定）

ポートスケジューラーメソッドを設定します。

QoS > Basic Settings > Port Scheduler Method の順にクリックし、以下の画面を表示します。

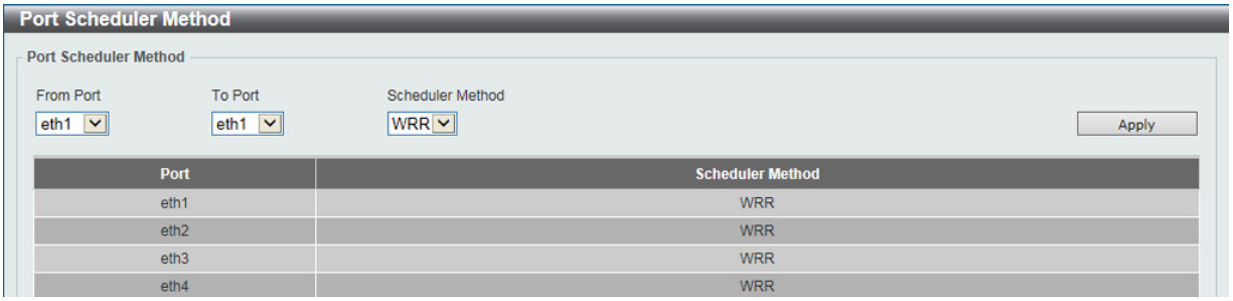

図 10-2　Port Scheduler Method 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	設定するポート / ポート範囲を入力します。
Scheduler Method	指定ポートに対するスケジューリングの方法を設定します。 「Strict Priority」(SP)、「Weighted Round-Robin」(WRR) から指定できます。初期値では出力キュースケジューリングアルゴリズムは「WRR」です。 • SP：SP モードで CoS キューを設定するには、より高いプライオリティの CoS キューも SP モードになっている必要があります。 • WRR - WRR は送信キュー内のパケットをラウンドロビンで転送していきます。最初、各キューは、設定可能な重みで重みづけを設定します。高いプライオリティの CoS キューからパケットが送信されるたびに、重みづけが 1 ずつ減算され、次に低い CoS キュー内のパケットが処理されます。CoS キューの重みづけがゼロに達すると、キューは、重みづけが戻るまで処理されません。すべての CoS キューの重みづけが 0 に達すると、重みづけは補完されます。

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

Queue Settings（QoS 設定）

キューを設定、表示します。

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

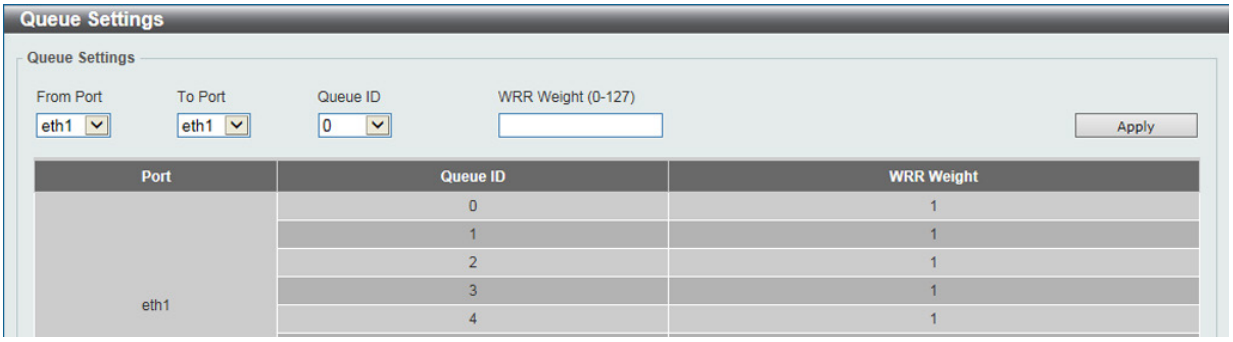

図 10-3　Queue Settings 画面

本画面には以下の項目があります。

項目	説明
From Port / To Port	設定するポート / ポート範囲を入力します。
Queue ID	キュー ID を指定します。0 から 7 の間で指定可能です。
WRR Weight	WRR の値を入力します。0 から 127 の間で指定可能です。「Expedited Forwarding」(EF) の要件を満たすには最高のキューは常に「Per-hop Behavior」(PHB) により選択されキューのスケジュールモードはストリクトプライオリティである必要があります。そのため最後のキューの重みは「Differentiate Service」がサポートされている間は 0 に設定する必要があります。

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

CoS to Queue Mapping（CoS キューマッピング設定）

CoS-to-Queue マッピングの表示、設定を行います。

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

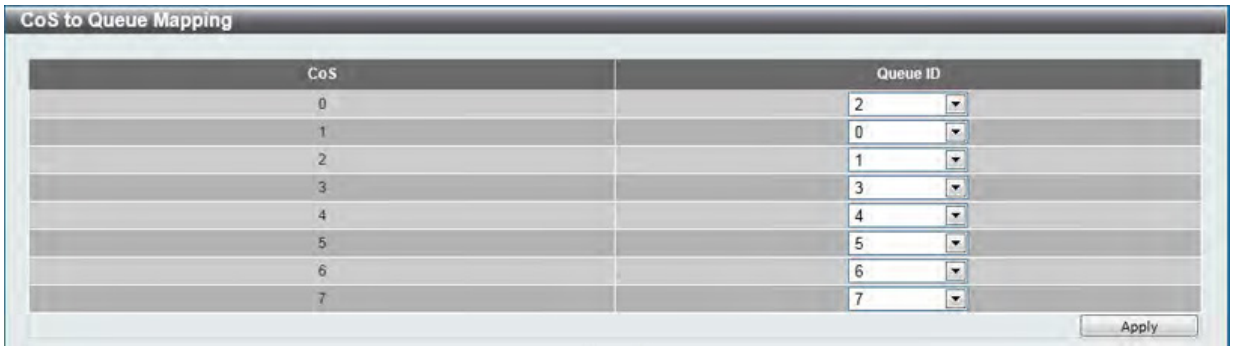

図 10-4　CoS to Queue Mapping 画面

本画面には以下の項目があります。

項目	説明
Queue ID	プライオリティを割り当てるクラス（キュー）を設定します。「0」（クラス 0）は最も低い優先度のキューで、「7」（クラス 7）が最も高くなります。

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

Port Rate Limiting（ポートレート制限設定）

ポートレート制限の設定を行います。

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

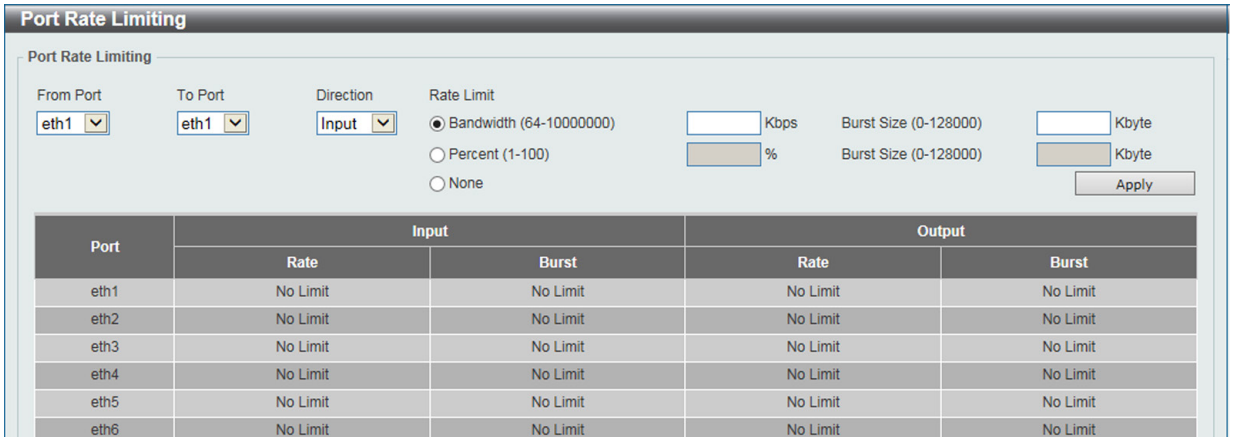

図 10-5　Port Rate Limiting 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	設定するポート / ポート範囲を入力します。
Direction	レート制限の対象を Input（イングレス）、Output（イーグレス）から選択します。
Rate Limit	レート制限の値を指定します。 • 「Bandwidth」-「Bandwidth」を選択し、受信 / 送信の帯域値を入力欄に入力します。この値は 64 から 10000000 Kbps で指定できます。また「Burst Size」の値も 0 から 128000Kbytes で指定可能です。 • 「Percent」-「Percent」を選択し、受信 / 送信の帯域パーセントを入力欄に入力します。この値は 1 から 100%で指定できます。また「Burst Size」の値も 0 から 128000 kilobytes で指定可能です。 • 「None」-「None」を選択すると指定ポートのレート制限を削除します。指定の制限はインタフェースの最大スピードを超えません。イングレスは受信したトラフィックが制限を超えた場合、フレーム、またはフローコントロールフレームを停止します。

「Apply」ボタンをクリックして行った変更を適用します。

Advanced Settings（アドバンス設定）

Port Trust State（ポートトラスト設定）

本スイッチにおけるポートトラスト設定と表示を行います。

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

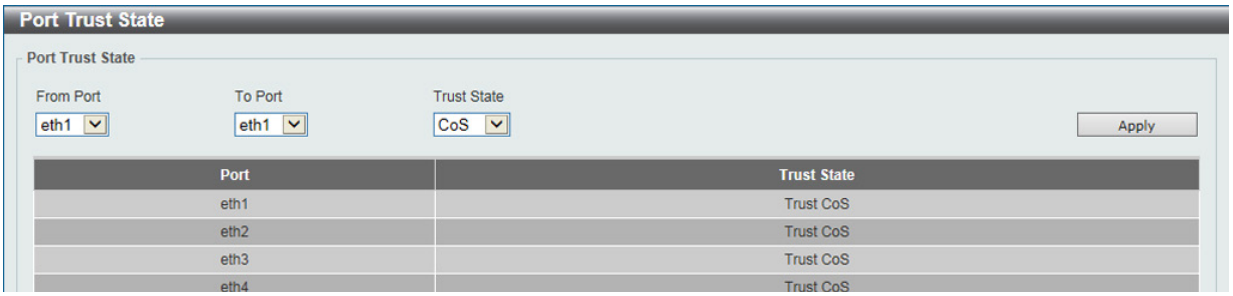

図 10-6　Port Trust State 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	設定するポート / ポート範囲を入力します。
Trust State	ポートトラストの設定をします。「CoS」「DSCP」から選択可能です。

「Apply」ボタンをクリックして行った変更を適用します。

DSCP CoS Mapping（DSCP CoS マップ設定）

本スイッチにおける DSCP CoS マップの設定と表示を行います。

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

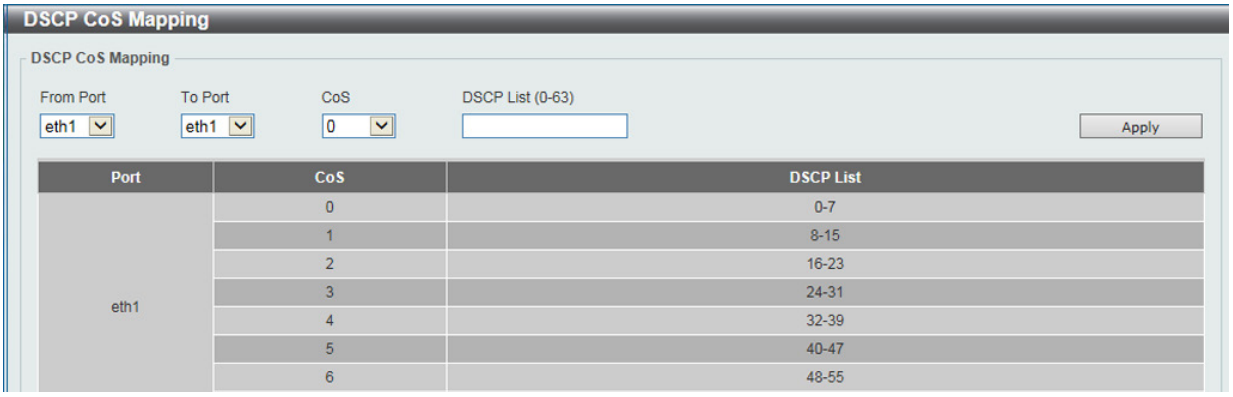

図 10-7　DSCP CoS Mapping 画面

本画面には以下の項目があります。

項目	説明
From Port/To Port	設定の対象となるポートを指定します。
CoS	CoS の値を指定します。0 から 7 の間で指定可能です。
DSCP List (0-63)	DSCP リストの値を入力します。0 から 63 の範囲で設定します。

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

第 11 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	参照ページ
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。	107
ARP Spoofing Prevention（ARP スプーフィング防止設定）	ARP スプーフィング防止設定を行います。	109
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。	110
Traffic Segmentation（トラフィックセグメンテーション）	トラフィックセグメンテーション設定を行います。	111
Storm Control（ストームコントロール）	ストームコントロールの設定を行います。	111
DoS Attack Prevention Settings（DoS 攻撃防止設定）	DoS 攻撃防止設定を行います。	113
SSL（Secure Socket Layer）	SSL（Secure Socket Layer）の設定を行います。	114

Port Security（ポートセキュリティ）

Port Security Global Settings（ポートセキュリティグローバル設定）

ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

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

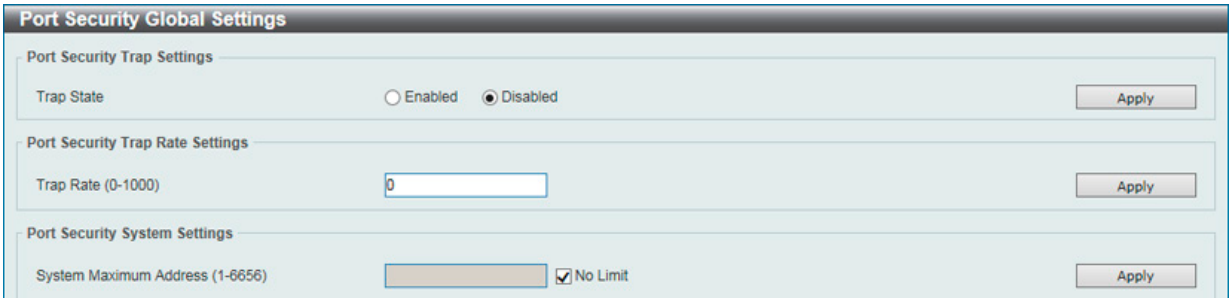

図 11-1　Port Security Global Settings 画面

本画面には以下の項目があります。

項目	説明
Trap State	ポートセキュリティトラップ設定を「Enabled」（有効）または「Disabled」（無効）にします。
Trap Rate	毎秒のトラップ数を指定します。0 から 1000 までの間で指定できます。初期値の 0 は SNMP トラップがあらゆるセキュリティ違反に対して動作することを意味します。
System Maximum Address	システムの最大 MAC アドレス数を入力します。1 から 6656 まで指定可能です。指定しない場合、または「No Limit」にチェックを入れた場合、初期値の「No Limit」となり、スイッチに MAC アドレス最大数が適用されます。

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

Port Security Port Settings（ポートセキュリティポート設定）

ポートセキュリティのポート設定と設定内容の表示をお行います。

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

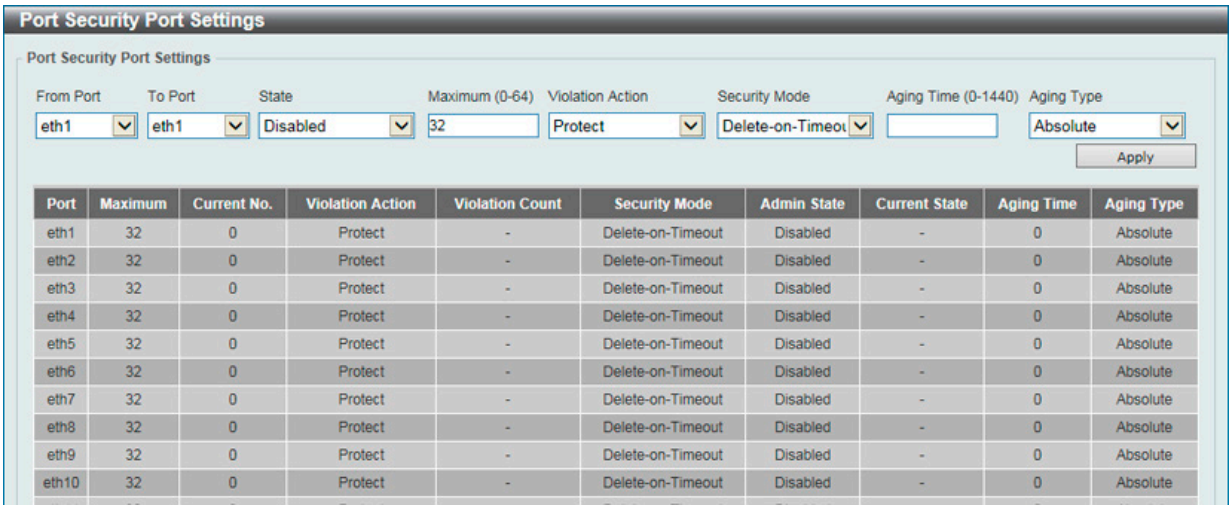

図 11-2　Port Security Port Settings 画面

本画面には以下の項目があります。

項目	説明
From Port/To Port	設定の対象となるポートを指定します。
State	指定ポートへのポートセキュリティ機能を有効 / 無効にします。
Maximum	指定ポートで許可される安全な MAC アドレスの最大数を指定します。0 から 64 まで指定可能で初期値は 32 です。
Violation Action	違反に対する動作を指定します。「Protect」「Restrict」「Shutdown」から指定可能です。 「Protect」を選択すると、ポートセキュリティレベルで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反カウントとしては数えられません。 「Restrict」を選択すると、ポートセキュリティレベルで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントされシステムログに記録されます。 「Shutdown」を選択すると、セキュリティ違反があるとポートをシャットダウンし、システムログに記録されます。

項目	説明
Security Mode	セキュリティモードを選択します。「Permanent」「Delete-on-Timeout」から選択可能です。「Permanent」を選択するとすべての学習した MAC アドレスは手動でエントリを削除しない限り削除されません。「Delete-on-Timeout」を選択するとすべての学習した MAC アドレスはタイムアウトにより自動的に削除されるか、手動でエントリを削除します。
Aging Time	指定ポートの自動取得アドレスに使用するエージングタイムです。0 から 1440 分の間で指定可能です。
Aging Type	エージングの種類を指定します。「Absolute」「Inactivity」から指定します。「Absolute」を指定するとポート上のすべてのアドレスは指定された時間を過ぎるとアドレスリストから削除されます。初期値になります。「Inactivity」を指定すると指定の期間安全なアドレスからのトラフィックがない場合、エージアウトしません。

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

Port Security Address Entries（ポートセキュリティアドレスエントリ設定）

ポートセキュリティアドレスエントリの設定、表示を行います。

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

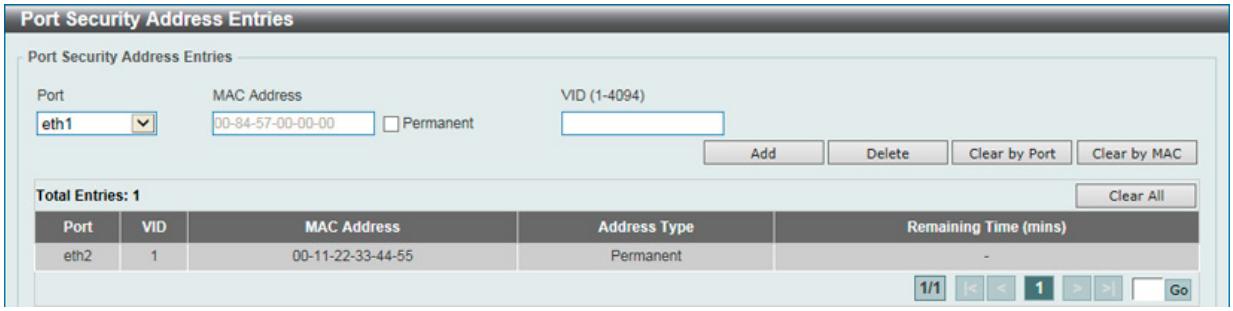

図 11-3　Port Security Address Entries 画面

本画面には以下の項目があります。

項目	説明
Port	設定の対象となるポートを指定します。
MAC Address	MAC アドレスを入力します。Permanent にチェックを入れると、エントリ自体が手動で削除されるまで学習した MAC アドレスが削除されることはありません。
VID	VLAN ID を指定します。1 から 4094 の間で指定できます。

「Add」ボタンをクリックして、入力した情報に基づく新しいエントリを追加します。
「Delete」ボタンをクリックし、入力した情報に基づく新しいエントリを削除します。
「Clear by Port」ボタンをクリックし、選択したポートに基づく情報を消去します。
「Clear by MAC」ボタンをクリックし、選択した MAC アドレスに基づく情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ARP Spoofing Prevention（ARP スプーフィング防止設定）

ユーザは保護されたゲートウェイに対し、MAC のスプーフィングを防ぐためにスプーフィング防止を設定することができます。エントリーが作成された場合に、送信先 ARP パケットはエントリのゲートウェイ IP にマッチしているが、送信先 MAC フィールドもしくは送信元 MAC フィールドのどちらかがエントリのゲートウェイ MAC と合致しない場合はシステムにより破棄されます。
ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスとマッチしなかった IP アドレスの ARP パケットをバイパスします。もし ARP アドレスが設定したゲートウェイの IP アドレス、MAC アドレスそしてポートリストなどとマッチする場合、受信ポートが ARP トラストかどうかは関係なく Dynamic ARP Inspection (DAI) チェックをバイパスします。

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

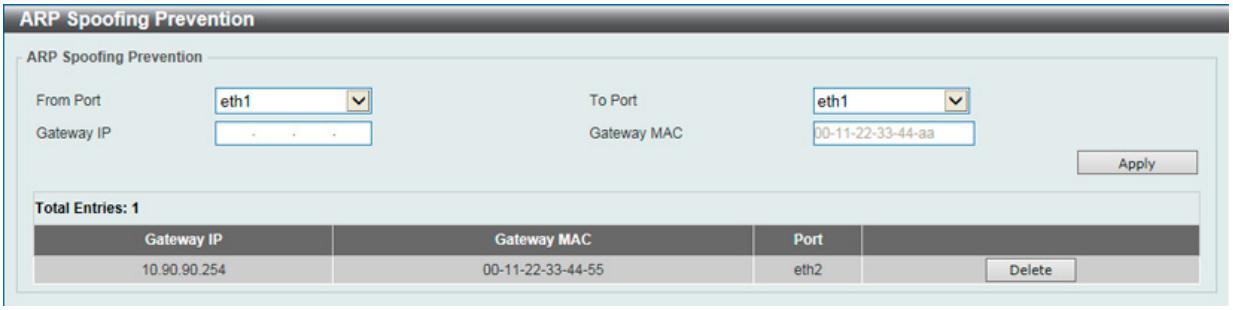

図 11-4　ARP Spoofing Prevention 画面

以下の項目を使用して、設定します。

項目	説明
From Port / To Port	選択したポートから連続した複数のポートを設定できます。
Gateway IP	ゲートウェイの IP アドレスを入力します。
Gateway MAC	ゲートウェイの MAC アドレスを入力します。

「Apply」ボタンをクリックし、変更を有効にします。
「Delete」ボタンをクリックして、指定エントリを削除します。

Safeguard Engine Settings（セーフガードエンジン）

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃によりスイッチの CPU はその対応量を超えて増加してしまう可能性があります。このような問題を軽減するために、本スイッチのソフトウェアにセーフガードエンジン機能を付加しました。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。省パワーモード（exhausted mode）の場合、スイッチは ARP と IP パケットのための帯域を制限します。もし CPU の稼働がしきい値以下に下がった場合、セーフガードエンジンは動作を停止しスイッチは省パワーモードを脱却し通常モードへ移行します。

注意 エンジンガードが有効になっている場合、CPU 使用率とトラフィック制限を制御するために、スイッチは FFP（高速フィルタプロセッサ）メータリングテーブルを使用して、さまざまなトラフィックフロー（ARP、IP）に帯域幅を割り当てます。これはネットワークを介してトラフィックをルーティングするスピードが制限される場合があります。

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

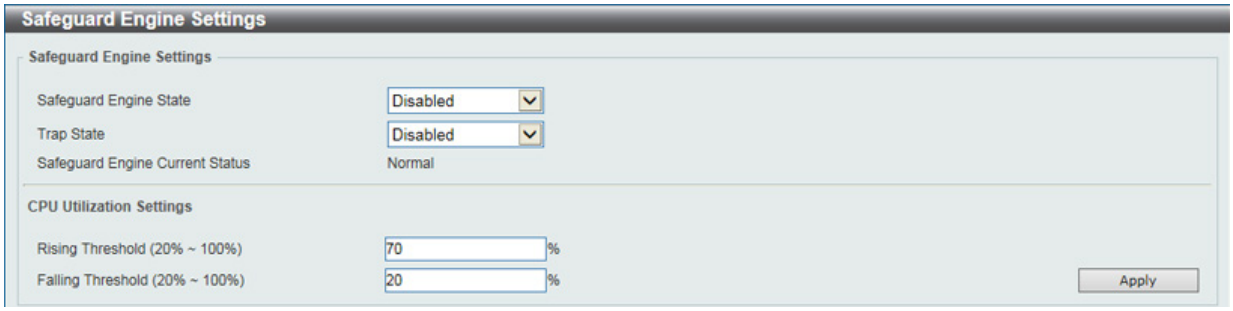

図 11-5　Safeguard Engine Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Safeguard Engine Settings	
Safeguard Engine State	セーフガードエンジン機能を「Enabled」（有効）/「Disabled」（無効）にします。
Trap State	セーフガードエンジントラップを「Enabled」（有効）/「Disabled」（無効）にします。
Safeguard Engine Current Status	現在のセーフガードエンジンの状態を表示します。
CPU Utilization Settings	
Rising Threshold (20% ~ 100%)	Safeguard Engine を有効にする前に許容可能な CPU 使用率のレベルを設定します。CPU 使用率がこのしきい値に到達すると、ここで設定した項目に基づいて、Exhausted モードに入ります。
Falling Threshold (20% ~ 100%)	許容可能な CPU 使用率のレベルを設定します。スイッチは CPU 使用率がこのしきい値に到達すると Safeguard Engine 状態から Normal モードに戻ります。

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

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

トラフィックセグメンテーション機能は、（単一 / 複数）ポート間のトラフィックの流れを制限するために使用します。「トラフィックフローの分割」という方法は、「VLAN によるトラフィック制限」に似ていますが、さらに制限的です。本機能によりマスタスイッチ CPU のオーバヘッドを増加させないようにトラフィックを操作することが可能です。

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

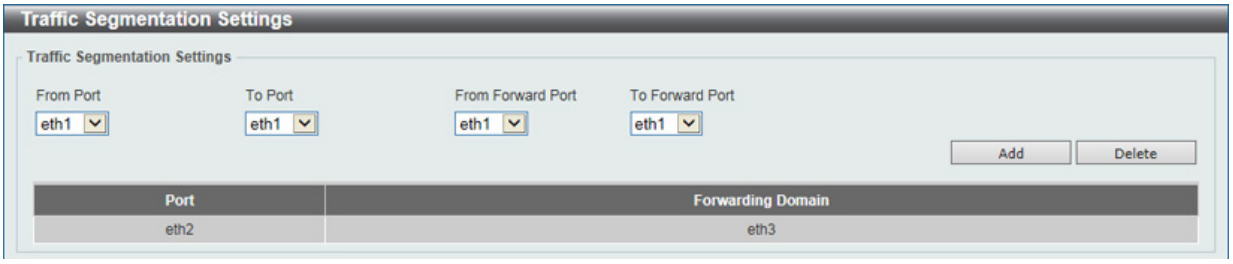

図 11-6　Traffic Segmentation 画面

以下の項目を使用して設定を行います。

項目	説明
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。

「Add」ボタンをクリックすると、入力した情報を元に新しいエントリを追加します。
「Delete」ボタンをクリックすると、入力した情報を元にエントリを削除します。

Storm Control（ストームコントロール）

ストームコントロールの設定、表示を行います。**Security > Storm Control** の順にクリックします。

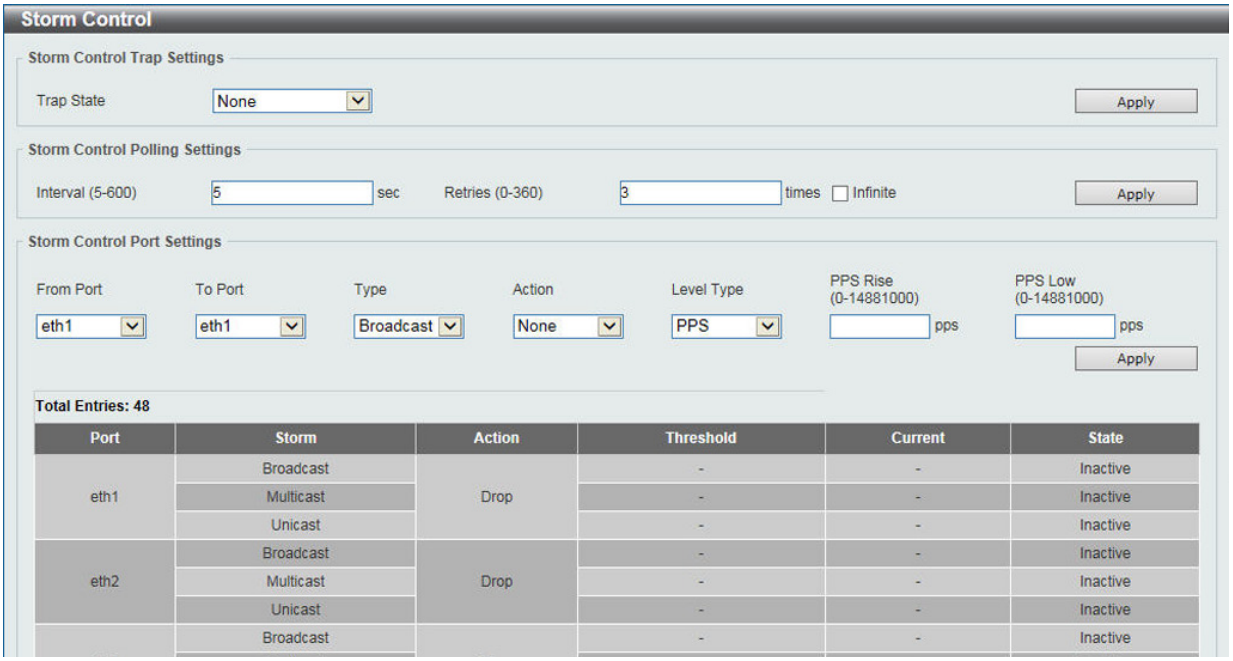

図 11-7　Storm Control 画面

以下の項目を使用して、設定を行います。

項目	説明
Storm Control Trap Settings（ストームコントロールトラップ設定）	
Trap State	ストームコントロールトラップのオプションを指定します。「None」「Storm Occur」「Storm Clear」「Both」から指定できます。「None」が選択されるとトラップは送信されません。「Storm Occur」が選択されると、ストームの発生を検出した時点でトラップは通知されます。「Storm Clear」が選択されるとストームが解消された時点でトラップは通知されます。

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

項目	説明
Storm Control Polling Settings（ストームコントロールポーリング設定）	
Interval	インターバルの値を指定します。5 から 600（秒）で指定できます。初期値は 5 秒です。
Retries	再試行の値を入力します。0 から 360 で指定できます。初期値は 3 です。「Infinite」にチェックを入れると本機能は無効になります。

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

項目	説明
Storm Control Port Settings（ストームコントロールポート設定）	
From Port / To Port	設定するポート範囲を指定します。
Type	コントロールするストームの種類を選択します。「Broadcast」「Multicast」「Unicast」から指定できます。シャットダウンモードで選択すると、ユニキャストは「Known」「Unknown」両方が設定してある場合、どちらにも対応しポートはシャットダウンします。そうでない場合は「Unknown」にのみ対応します。
Action	動作について指定します。「None」「Shutdown」「Drop」から指定します。「None」を指定するとストームパケットをフィルタしません。「Shutdown」は選択すると、指定したしきい値に達するとポートはシャットダウンされます。「Drop」を選択すると指定したしきい値に達するとパケットを破棄します。
Level Type	レベルタイプを指定します。「PPS」「Kbps」「Level」から選択します。
PPS Rise	毎秒のパケット増加の上限値について指定します。毎秒増加するパケットの量について上限しきい値を指定します。0 から 14881000 パケット毎秒で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。
PPS Low	毎秒のパケット減少の下限値について指定します。毎秒減少するパケットの量について下限しきい値を指定します。0 から 14881000 パケット毎秒で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。

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

「Level Type」で「Kbps」を選択すると、以下の画面が表示されます。

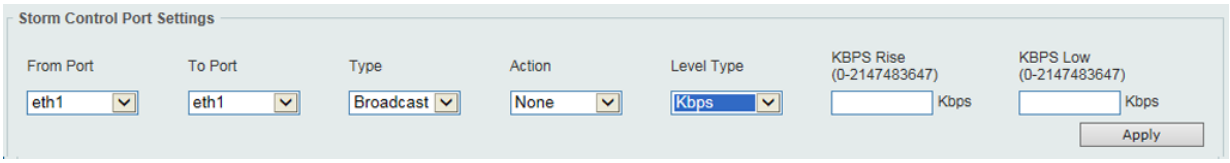

図 11-8　Storm Control (Kbps) 画面

項目	説明
KBPS Rise	上限 KBPS の値を指定します。ポートに受信するトラフィックの上限しきい値をキロビット / 毎秒で指定します。0 から 2147483647 Kbps の間で指定できます。
KBPS Low	下限 KBPS の値を指定します。ポートに受信するトラフィックの下限しきい値をキロビット / 毎秒で指定します。0 から 2147483647 Kbps の間で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。

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

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

各 DoS 攻撃に対して防御設定を行います。

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

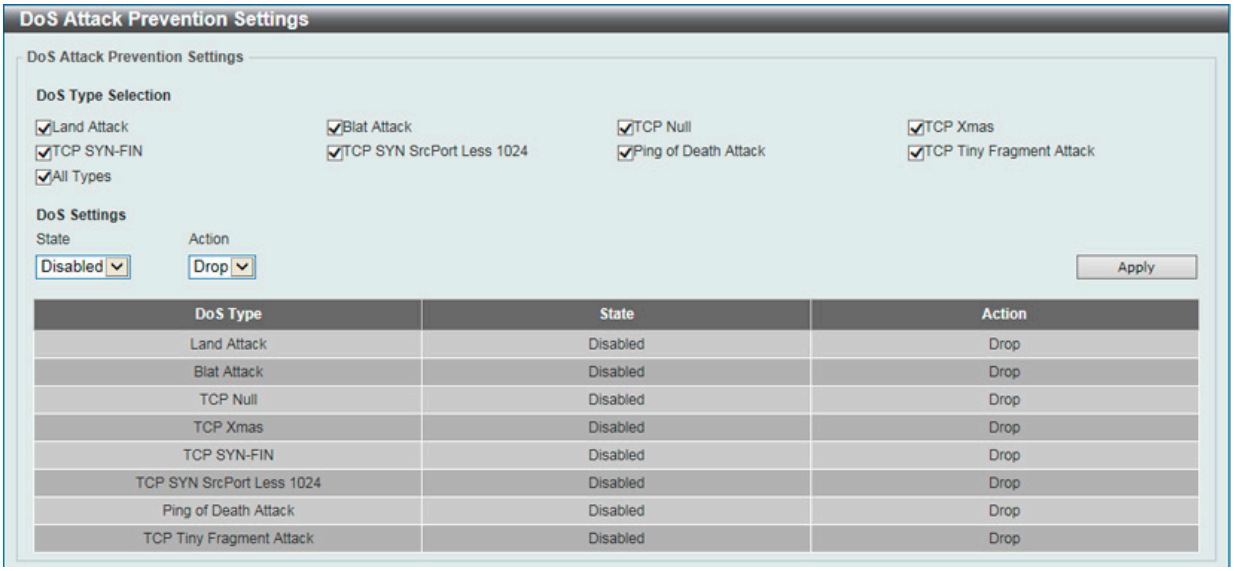

図 11-9　DoS Attack Prevention Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
DoS Attack Prevention Settings	
DoS Type Selection	適切な DoS 攻撃防御のタイプを選択します。 • Land Attack - DoS 攻撃防止タイプに LAND 攻撃を指定します。 • Blat Attack - DoS 攻撃防止タイプに BLAT 攻撃を指定します。 • TCP Null - DoS 攻撃防止タイプに TCP Null Scan 攻撃を指定します。 • TCP Xmas - DoS 攻撃防止タイプに TCP Xmascan 攻撃を指定します。 • TCP SYN-FIN - DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。 • TCP SYN SrcPort Less 1024 - DoS 攻撃防止タイプに TCP SYN Source Port Less 1024 攻撃を指定します。 • Ping of Death Attack - DoS 攻撃防止タイプに Ping Death Attack 攻撃を指定します。 • TCP Tiny Fragment Attack - DoS 攻撃防止タイプに TCP Tiny Frag 攻撃を指定します。 • All Types - DoS 攻撃防止タイプにすべての攻撃を指定します。
State	DoS 攻撃防止の状態を指定します。 • Enabled - DoS 攻撃防止の状態を有効にします。 • Disabled - DoS 攻撃防止の状態を無効にします。
Action	DoS 攻撃防止機能により行われる操作を無効にします。 • Drop - 一致する DoS 攻撃パケットをすべて破棄します。

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

SSL（Secure Socket Layer）

Secure Sockets Layer（ SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、暗号スイートを使用して実現されます。暗号スイートは、認証セッションに使用される特定の暗号化アルゴリズムおよびキー長を決定するセキュリティ文字列であり、以下の 3 つの段階で構成されます。

1. 鍵交換（Key Exchange）
暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DSA、ここでは DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。これはクライアントとホスト間の最初の認証プロセスであり、「鍵交換」を行って一致した場合、認証が受諾され、以下のレベルで暗号化のネゴシエーションが行われます。

2. 暗号化（Encryption）
暗号スイートの次の部分は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
-- ストリーム暗号（Stream Ciphers）– スイッチは 2 種類のストリーム暗号（40 ビット鍵での RC4 と、128 ビット鍵での RC4）に対応しています。これらの鍵はメッセージの暗号化に使用され、最適に利用するためにはクライアントとホスト間で一致させる必要があります。
-- CBC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、1 つ前の暗号化テキストのブロックを使用して、現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義される 3 DES EDE 暗号化コードと高度な暗号化規格（AES）をサポートし、暗号化されたテキストを生成します。

3. ハッシュアルゴリズム（Hash Algorithm）
暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージと共に暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）、SHA-256 の 3 つのハッシュアルゴリズムをサポートします。

サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成するために、これら 3 つのパラメータの一意の組み合わせである 5 種類の暗号化スイートについてスイッチ上で設定が可能です。それぞれの暗号化スイートに対して有効 / 無効の設定を行うことが可能ですが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。また、本スイッチは、SSLv3 および TLS1.0/1.1 をサポートしています。それ以外のバージョンは本スイッチとは互換性がない恐れがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する可能性があります。

「SSL Global Settings」および「SSL Service Policy」画面では、スイッチで SSL を有効にして各種暗号スイートのステータスを設定することができます。暗号スイートは、認証セッションに使用される正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定するセキュリティ文字列です。スイッチには 5 個の暗号スイート設定が用意されており、初期設定ではすべて有効になっています。特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

SSL 機能が有効化されると、通常の HTTP 接続はできなくなります。SSL 機能を使用した Web ベースの管理を行うには、SSL 暗号化がサポートされた Web ブラウザにおいて、https:// で始まる URL を使用する必要があります（例 : https://10.90.90.90）。これらの条件を満たさない場合、エラーが発生し、Web ベースの管理機能への接続認証が行われません。

SSL 機能で使用する証明書ファイルは TFTP サーバからスイッチへダウンロードすることができます。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者や認証のための鍵、デジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバ側とクライアント側で整合性のある証明書ファイルを保持している必要があります。スイッチには初期状態で証明書がインストールされていますが、ユーザ環境に応じて追加のダウンロードが必要になる場合があるかもしれません。

SSL Global Settings（SSL グローバル設定）

SSL グローバル設定を行います。

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

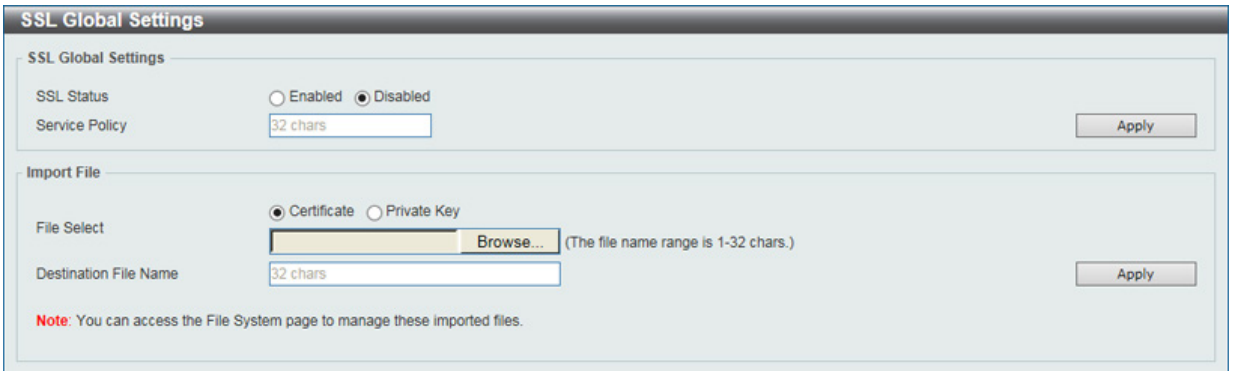

図 11-10　SSL Global Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
SSL Global Settings	
SSL Status	SSL をグローバルに「Enabled」（有効）、「Disabled」（無効）に設定します。初期値は「Disabled」です。
Service Policy	SSL ポリシー名を入力します。32 文字まで指定できます。

項目	説明
Import File	
File Select	ロードされるファイル種類を指定します。「Certificate」「Private Key」から指定可能です。ファイル種類を選択した後、「Browse/ 参照」ボタンをクリックして、適切なファイルを選択しローカルコンピュータにロードします。
Destination File Name	宛先ファイル名を指定します。32 文字まで指定可能です。

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

Crypto PKI Trustpoint（暗号 PKI トラストポイント）

暗号 PKI トラストポイントの表示、設定を行います。

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

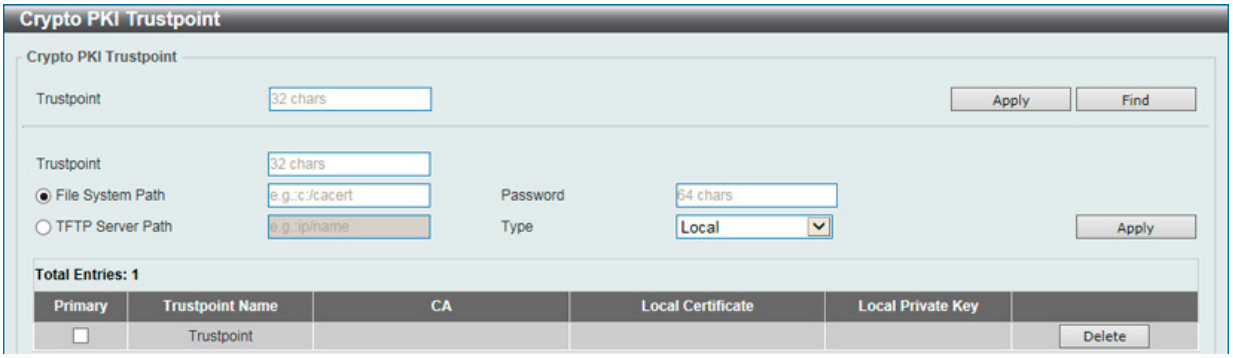

図 11-11　Crypto PKI Trustpoint 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
Trustpoint	インポートした証明書と鍵ペアに対応するトラストポイント名を入力します。32 文字まで指定できます。
File System Path	証明書と鍵ペアのファイルシステムパスを入力します。
Password	インポートしたプライベート鍵の暗号を解除する暗号パスフレーズを入力します。パスフレーズは 64 文字まで指定可能です。パスフレーズが指定されないと「NULL」文字列が使用されます。
TFTP Server Path	TFTP サーバのパスを指定します。
Type	インポートされる証明書の種類を指定します。「Both」「CA」「Local」。「Both」を選択すると「CA 証明書」「ローカル証明書の鍵ペア」をインポートします。「CA」を選択すると「CA 証明書」のみインポートします。「Local」を選択すると「ローカル証明書の鍵ペア」のみインポートします。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、入力した情報に基づいて指定エントリを検出します。

「Delete」ボタンをクリックして、指定エントリを削除します。

SSL Service Policy（SSL サービスポリシー）

SSL サービスポリシーの表示、設定を行います。

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

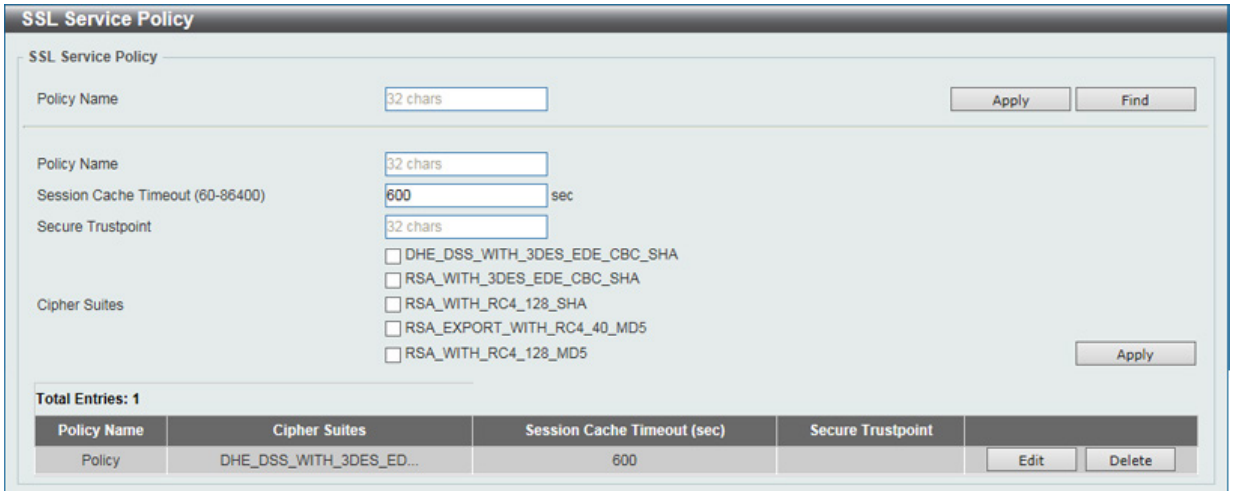

図 11-12　SSL Service Policy 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
Policy Name	SSL サービスポリシー名を入力します。32 文字まで指定可能です。
Session Cache Timeout	セッションキャッシュタイムアウトの時間を指定します。初期値は 600（秒）です。
Secure Trustpoint	セキュアなトラストポイントの名前を入力します。32 文字まで指定可能です。
Cipher Suites	本プロファイルの暗号一式を選択します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、入力した情報に基づいて指定エントリを検出します。
「Edit」ボタンをクリックして、指定エントリを編集します。
「Delete」ボタンをクリックして、指定エントリを削除します。

第 12 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)

故障診断機能を設定します。

以下は、OAM のサブメニューです。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	参照ページ
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。	117

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主に管理者とカスタマサービス担当者が UTP ケーブルを検査、テスト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即座に診断します。

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。

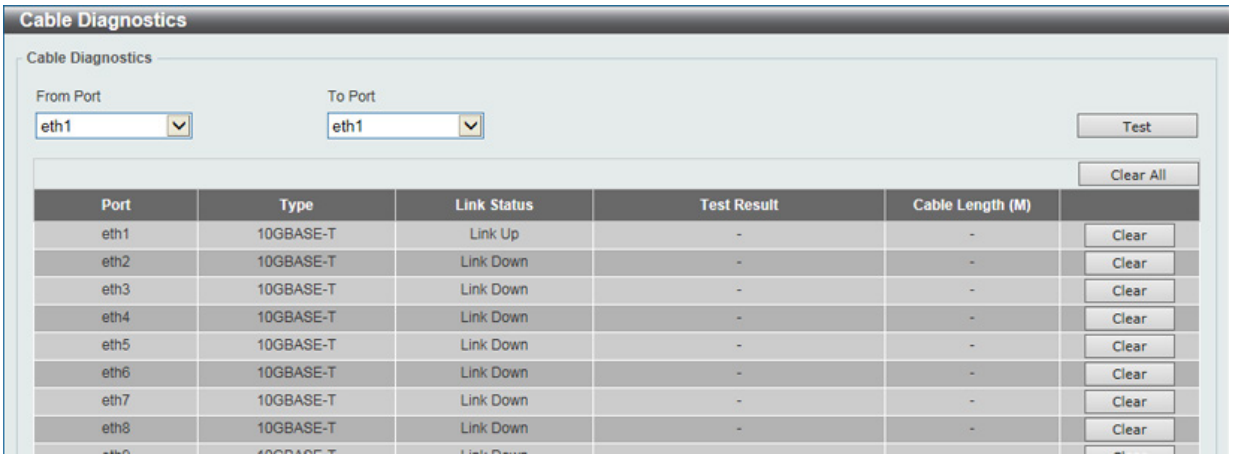

図 12-1　Cable Diagnostics 画面

特定のポートに対するケーブル診断を表示するためには、プルダウンメニューを使用して設定するポートを選択し、「Test」ボタンをクリックします。情報が画面に表示されます。
「Clear」ボタンをクリックし、指定ポートの情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

第 13 章　Monitoring（スイッチのモニタリング）

Monitoring メニューを使用し、本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報を提供することができます。

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

サブメニュー	説明	参照ページ
Utilization（利用分析）	CPU 使用率、ポートの帯域使用率を表示します。	118
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。	119
Mirror Settings（ミラー設定）	ポートミラーリングの設定を行います。	123
Device Environment（機器環境確認）	機器環境の設定、表示を行います。	124

Utilization（利用分析）

Port Utilization（ポート使用率）

本画面では、ポートの帯域使用率を表示します。

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

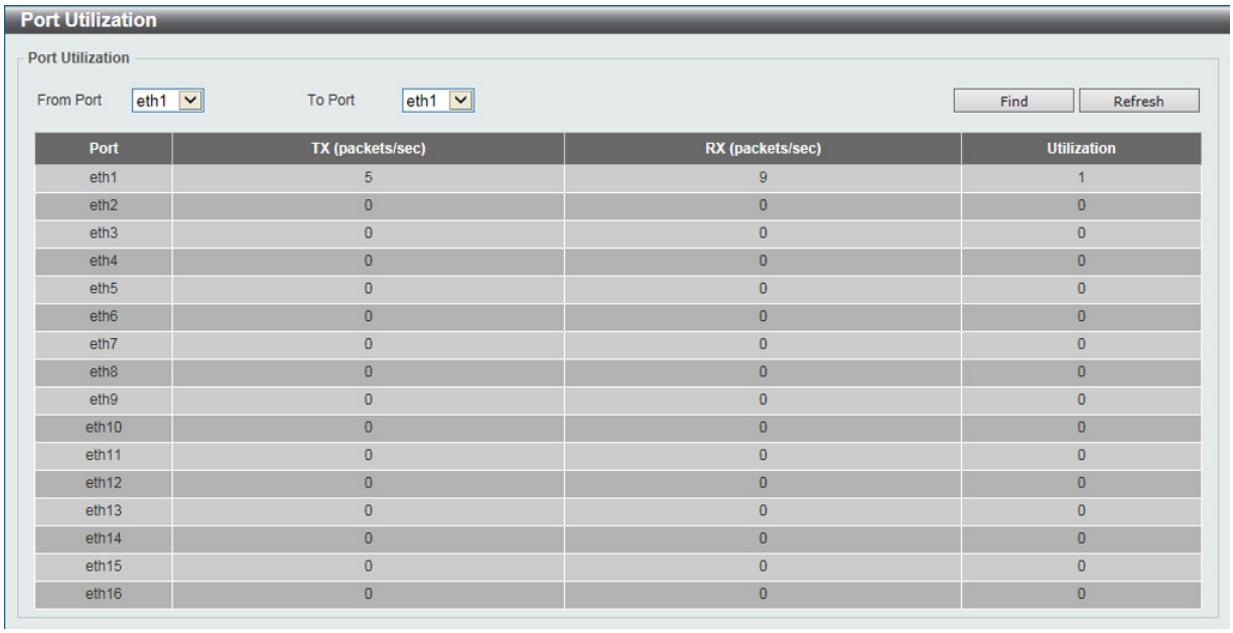

図 13-1　Port Utilization 画面

以下の設定項目が使用できます。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。

Statistics（統計情報）

Port（ポート統計情報）

ポートのパケット情報を表示します。

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

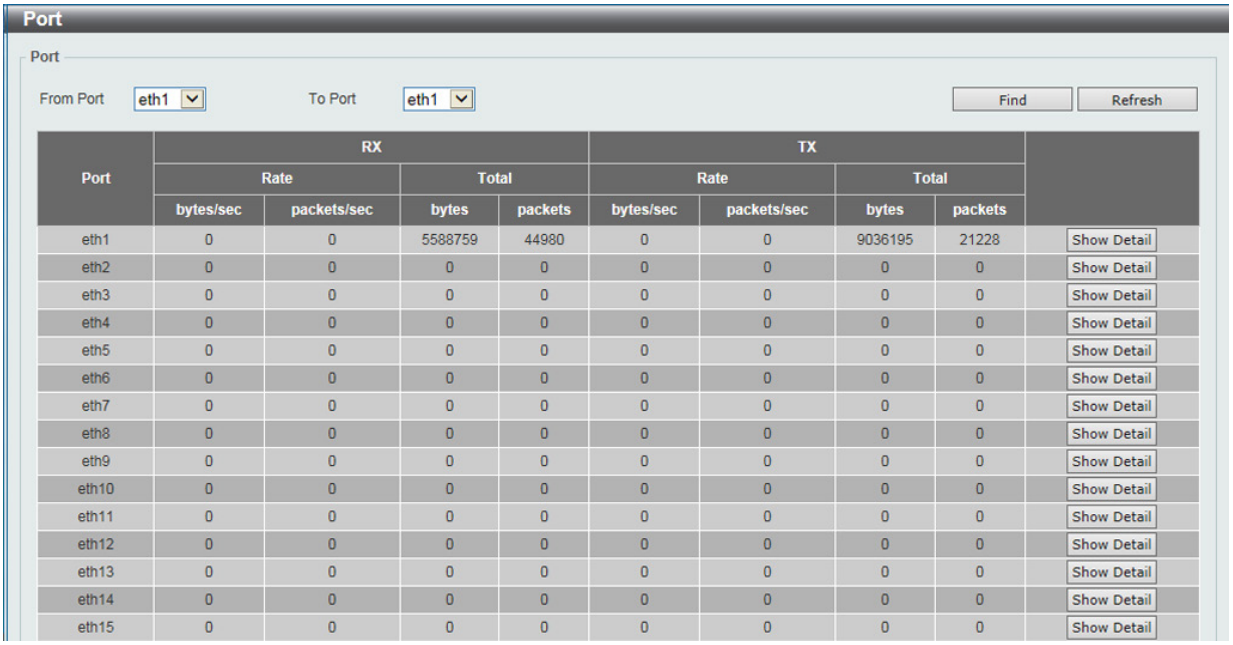

図 13-2　Port Statistics 画面

以下の設定項目を使用して、設定および表示を行います。

項目	説明
From Port / To Port	表示するポート範囲を指定します。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを更新します。
「Show Detail」ボタンをクリックし、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

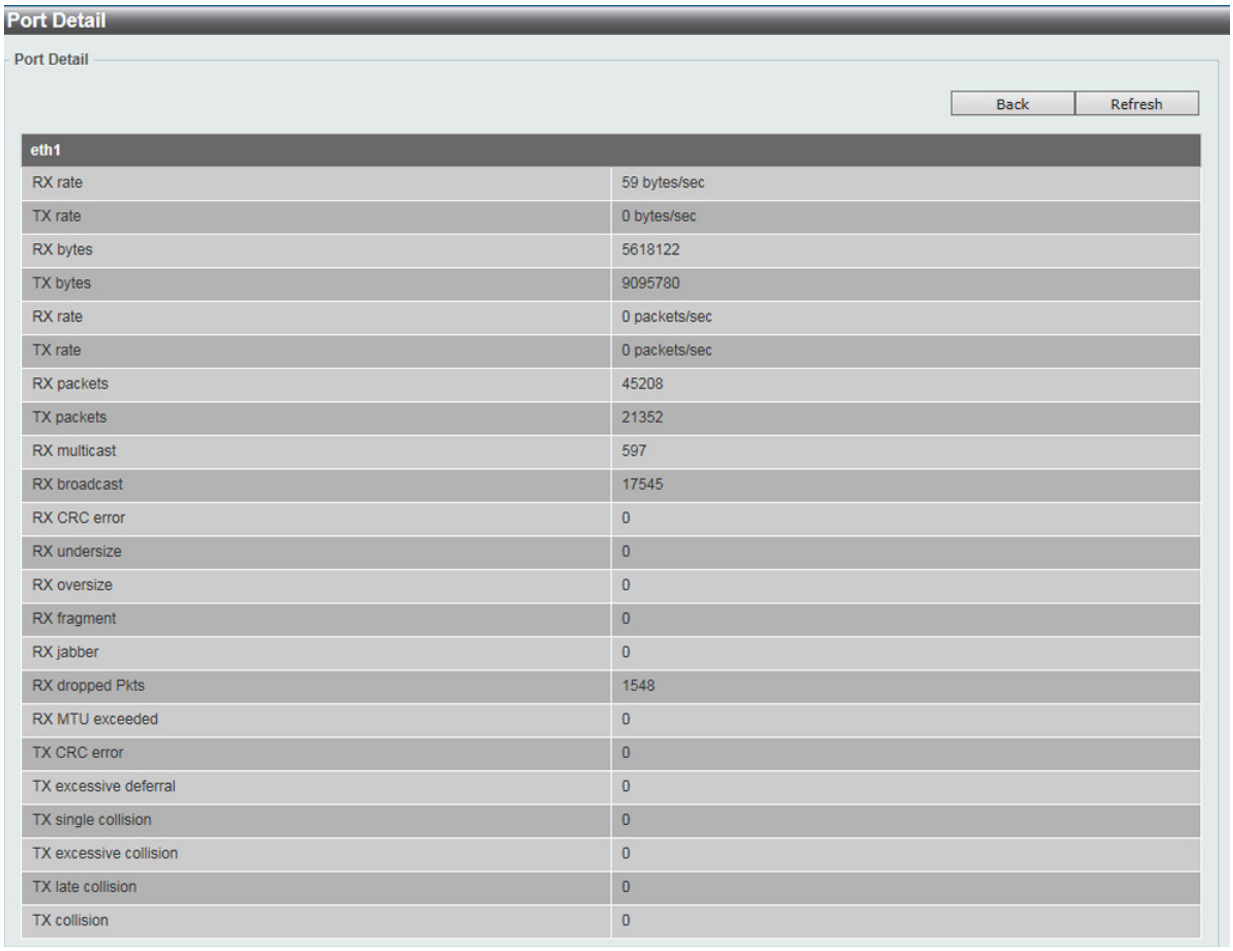

図 13-3　Port Statistics - Show Detail 画面

「Refresh」ボタンをクリックし、テーブルを再起動します。
「Back」ボタンをクリックし、前の画面に戻ります。

Port Counters（ポートカウンタ）

ポートのカウンタ情報を表示します。

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。

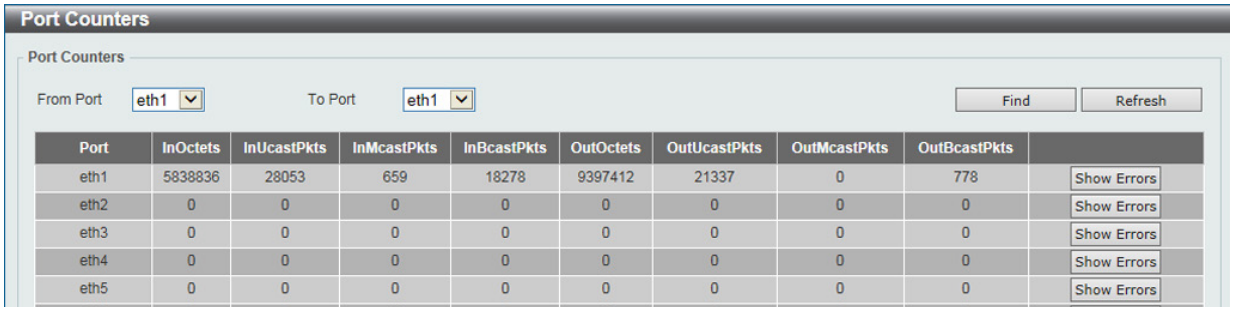

図 13-4　Port Counters 画面

以下の設定項目を使用して、設定および表示を行います。

項目	説明
From Port / To Port	表示するポート範囲を指定します。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。
「Show Errors」ボタンをクリックし、指定ポートのエラー情報について表示します。

「Show Errors」ボタンをクリックすると以下の画面が表示されます。

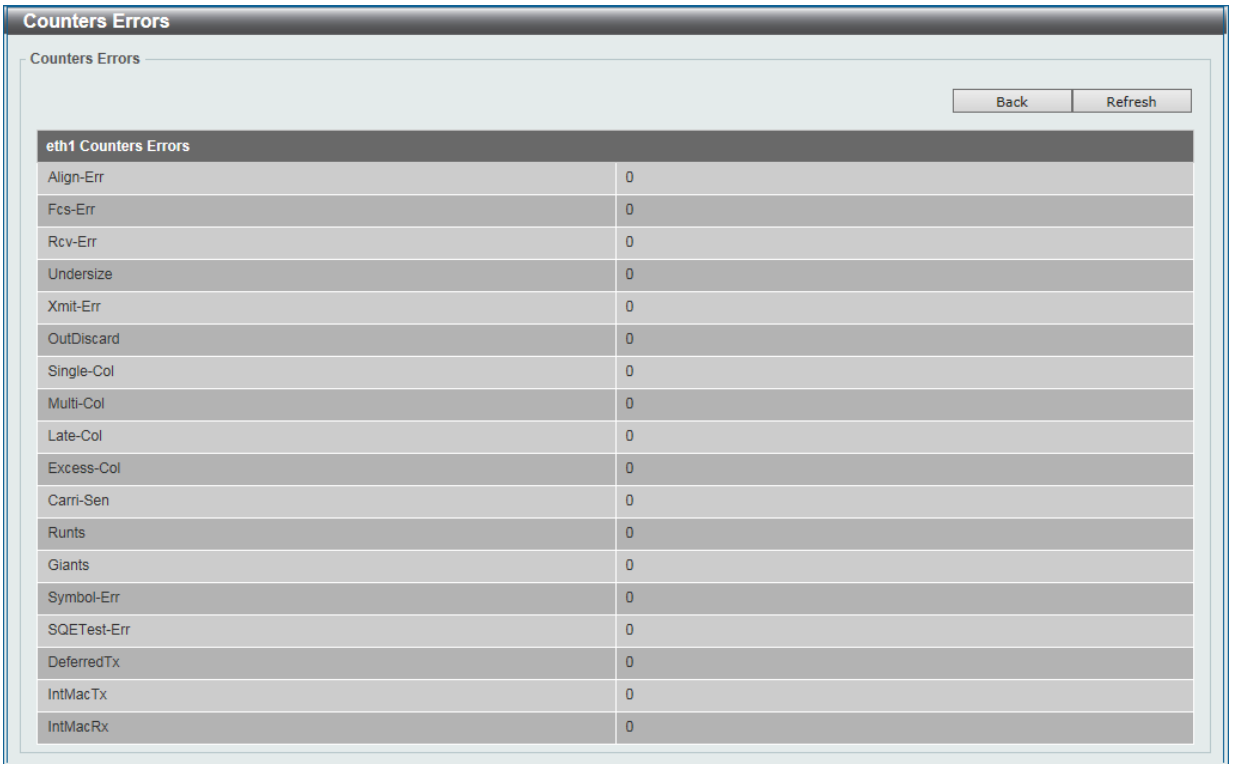

図 13-5　Port Statistics - Show Errors 画面

「Refresh」ボタンをクリックし、テーブルを再起動します。
「Back」ボタンをクリックし、前の画面に戻ります。

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。

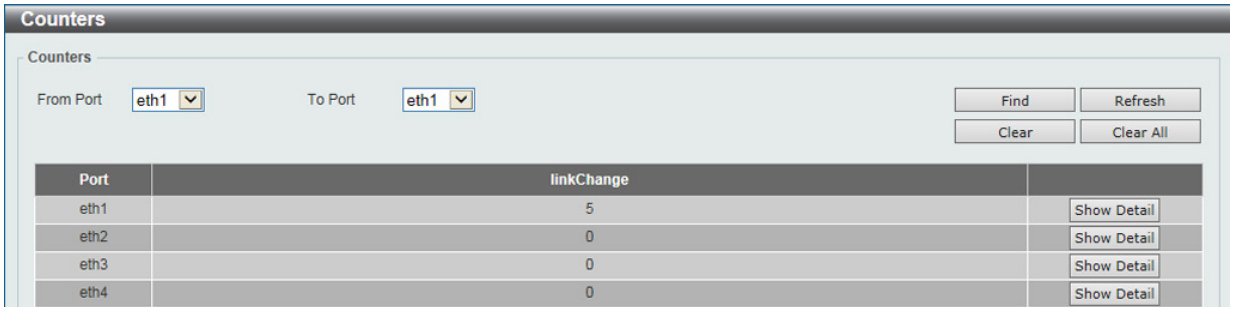

図 13-6　Counters 画面

以下の設定項目を使用して、設定および表示を行います。

項目	説明
From Port / To Port	表示するポート範囲を指定します。

「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「Refresh」ボタンをクリックし、テーブルを再起動します。
「Clear」ボタンをクリックし、指定ポートの情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。
「Show Detail」ボタンをクリックし、指定ポートの詳細情報について表示します。

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

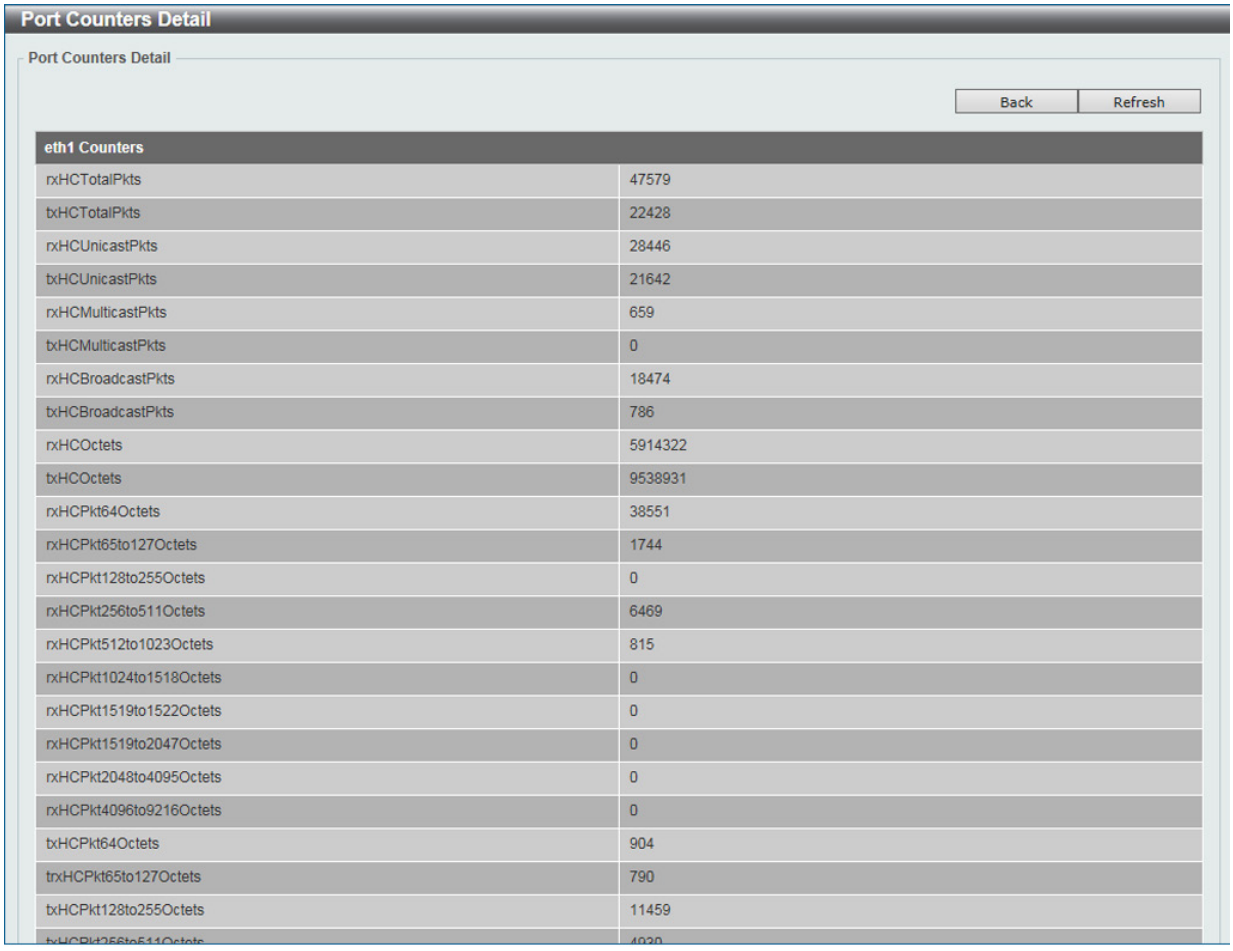

図 13-7　Port Counters Detail 画面

「Refresh」ボタンをクリックし、テーブルを再起動します。
「Back」ボタンをクリックし、前の画面に戻ります。

Mirror Settings（ミラー設定）

ミラーリング機能についての設定、表示を行います。本スイッチは対象ポートで送受信するフレームをコピーして、そのコピーしたフレームの出力先を他のポートに変更する機能（ポートミラーリング）を持っています。ミラーリングポートに監視機器（スニファや RMON probe など）を付随させて初期ポートを通したパケットの詳細を表示します。トラブルシューティングやネットワーク監視の目的において適しています。

Monitoring > Mirror Settings をクリックします。

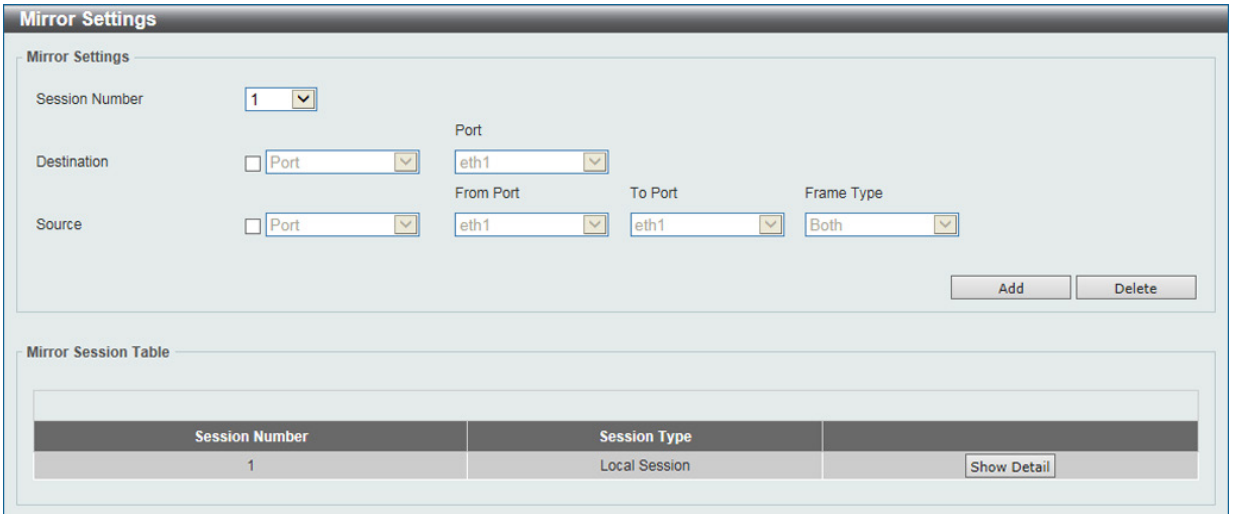

図 13-8　Mirror Settings 画面

以下の情報が表示されます。

項目	説明
Mirror Settings	
Session Number	該当エントリのセッション番号を指定します。
Destination	チェックボックスにチェックを入れポートミラーエントリの宛先について設定します。 宛先タイプオプションとして「Port」を選択します。「Port」を選択した後に、宛先ポート番号を指定します。
Source	チェックボックスにチェックを入れポートミラーエントリの送信元について設定します。 送信元タイプオプションとして「Port」または「ACL」を選択します。「Port」を選択した後に、「From Port」と「To Port」の番号を指定します。最後に「Frame Type」オプションを指定します。「Frame Type」で指定可能なオプションは「Both」「RX」「TX」「TX Forwarding」です。「Both」を選択すると送受信どちらのトラフィックもミラーされます。「RX」の場合、受信トラフィックのみミラーされ、「TX」は送信トラフィックのみミラーされます。

「Add」ボタンをクリックして、入力した情報に基づいた新規のミラーエントリを追加します。
「Delete」ボタンをクリックして、入力した情報に基づいた既存のミラーエントリを削除します。

注意　ミラー機能において、TX を設定している場合、Source Port が STP などにより、Block の状態のために実際には送信していない場合でも、宛先ポートにモニタします。

「Mirror Session Table」の「Show Detail」リンクをクリックし、以下の画面を表示します。

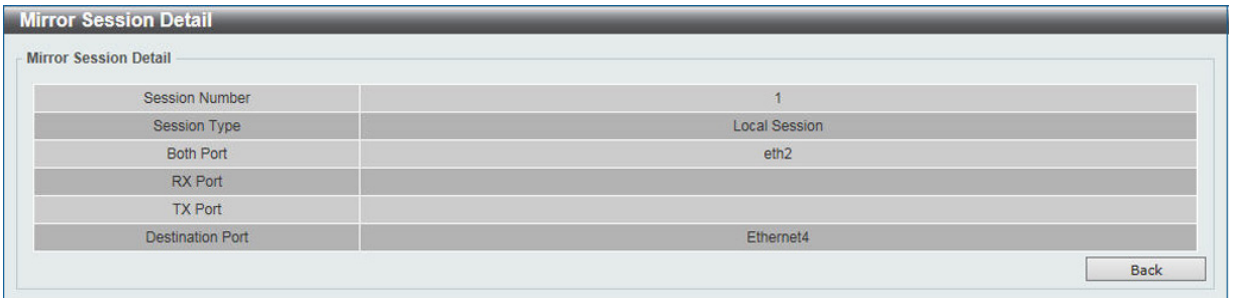

図 13-9　Mirror Settings - Show Detail 画面

Device Environment（機器環境確認）

本画面ではスイッチの内部温度状態を表示します。

Monitoring > Device Environment をクリックして次の画面を表示します。

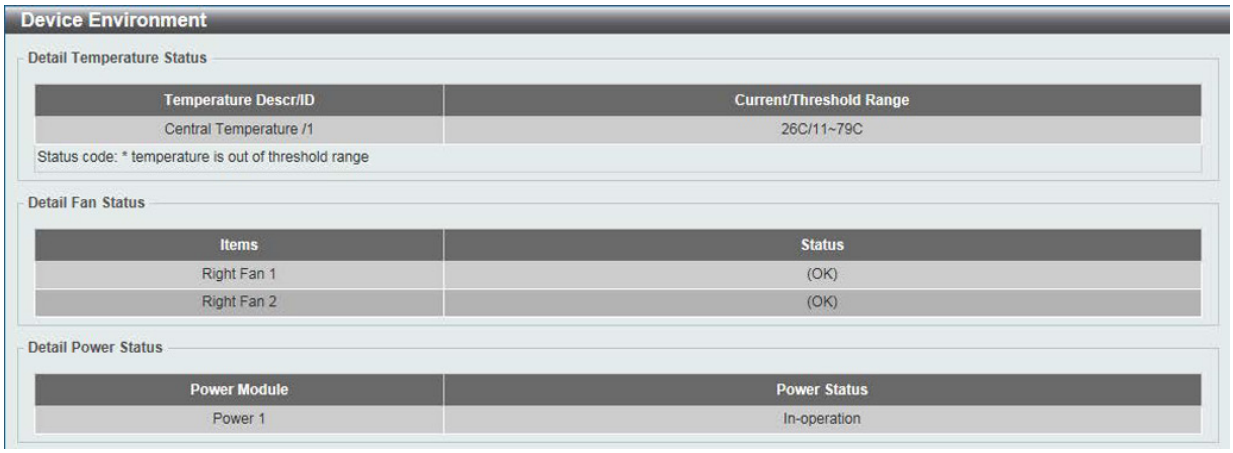

図 13-10　Device Environment 画面

第 14 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	参照ページ
Power Saving（省電力）	機器の省電力設定を行います。	125
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。	126

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

「リンクダウン」や「ケーブル長」など様々な状況下でのスイッチの電力消費を抑えます。

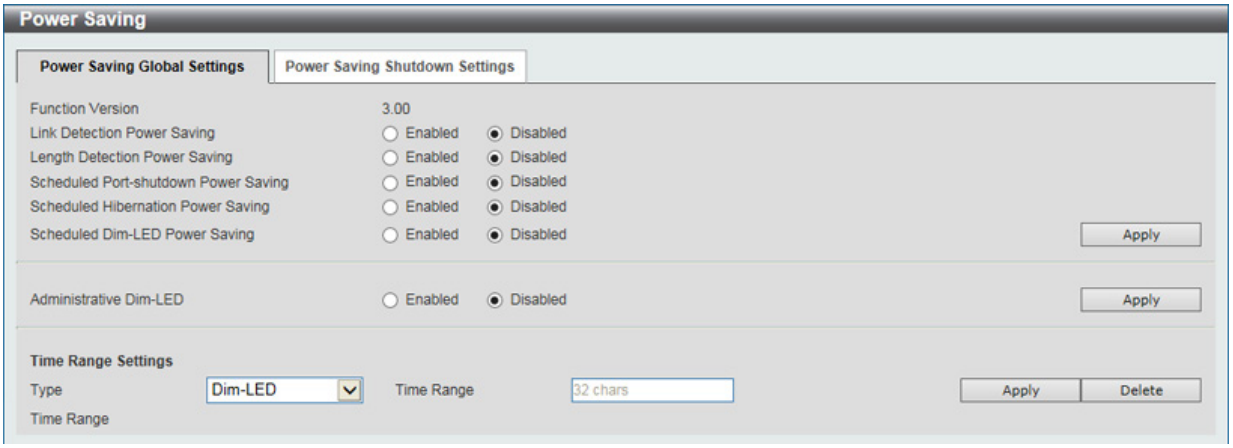

図 14-1　Power Saving - Power Saving Global Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Global Settings タブ	
Link Detection Power Saving	「リンク検出」を有効 / 無効に指定します。有効にするとリンクダウンしているポートへの電力供給は止められ、スイッチの消費電力を抑えます。これによりリンクアップしているポートへの影響はありません。
Length Detection Power Saving	「ケーブル長検出」を有効 / 無効に指定します。有効にすると 10 メートル以下のケーブルへの電力消費は抑えられ、スイッチの消費電力を抑えます。
Scheduled Port-shutdown Power Saving	スケジュールによるポートシャットダウン機能の有効 / 無効を指定します。
Scheduled Hibernation Power Saving	スケジュールにより休止省電力機能を有効 / 無効に指定します。有効にすると、スイッチは設定期間休止状態（アイドル状態）になり電力消費を抑えます。スイッチの LED は全て消え、コンソールを除くネットワーク機能も無効になります。スイッチが PoE 給電機能を有していた場合、電力の供給も行わなくなります。
Scheduled Dim-LED Power Saving	スケジュールによりスイッチの LED 照明を消すことで、消費電力を抑えます。
Administrative Dim-LED	ポート LED 機能の有効 / 無効を指定します。
Type	省電力モードの種類を指定します。「Dim-LED」「Hibernation」から指定できます。
Time Range	上記省電力機能に対応するスケジュールを指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。
「Delete」ボタンをクリックし指定のエントリを削除します。

Power Saving Shutdown Settings タブ

事前に指定したスケジュールに基づき、シャットダウンするポート範囲を指定します。

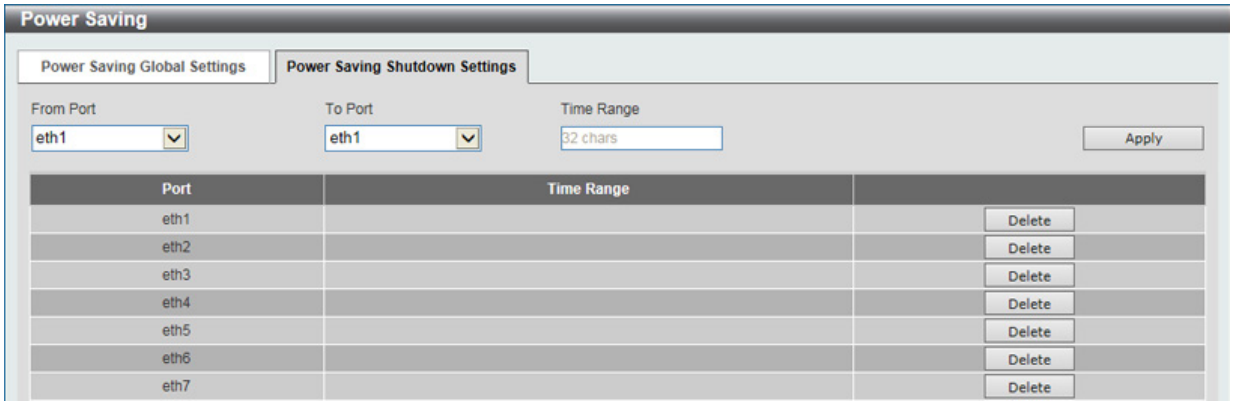

図 14-2　Power Saving - Power Saving Shutdown Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Shutdown Settings タブ	
From Port / To Port	設定するポート範囲を指定します。
Time Range	ポートに対応するスケジュール名を指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。
「Delete」ボタンをクリックし指定のエントリを削除します。

EEE（Energy Efficient Ethernet/ 省電力イーサネット）

「Energy Efficient Ethernet」(EEE/ 省電力イーサネット) は「IEEE 802.3az」によって定義されています。パケットの送受信がリンクに発生していない場合の電力消費を抑える目的で設計されています。

Green > EEE メニューをクリックし、以下の画面を表示します。

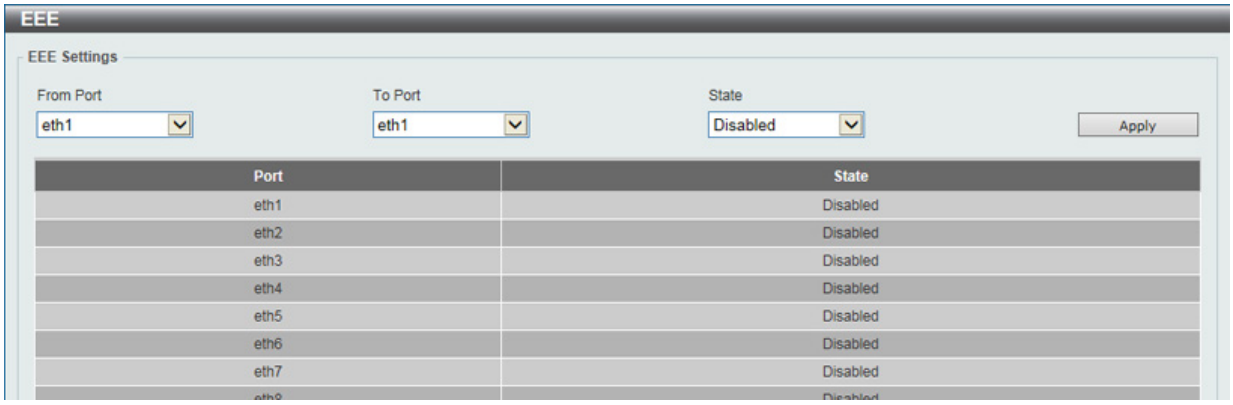

図 14-3　EEE 画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Shutdown Settings タブ	
From Port / To Port	設定するポート範囲を指定します。
State	本機能を有効 / 無効に指定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。

注意　本機能を使用するには、接続する対向の機器も EEE に対応している必要があります。

第 15 章　Save and Tools（Save と Tools メニュー）

Web インタフェース画面左上部の「Save」「Tools」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	参照ページ
Save（Save メニュー）		
Save Configuration（コンフィグレーションの保存）	コンフィグレーションをスイッチに保存します。	127
Tools（ツールメニュー）		
Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）	ファームウエアのアップグレードとバックアップをします。	127
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します。	129
Log Backup（ログファイルのバックアップ）	ログファイルのバックアップをします。	131
Ping	Ping を実行します。	132
Reset（リセット）	機器をリセットします。	133
Reboot System（システム再起動）	システムの再起動を行います。	133

Save（Save メニュー）

Save Configuration（コンフィグレーションの保存）

Web マネージャ先頭の **Save > Save Configuration / Log** をクリックし、以下の画面を表示します。

コンフィグレーションの保存

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Type」プルダウンメニューの「Configuration」を選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。

図 15-1　Save - Configuration 画面

Tools（ツールメニュー）

Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）

Tools > Firmware Upgrade & Backup では、ファームウェアの保存とファームウェアファイルのスイッチへのアップロードを実行できます。

本製品がファイルシステムに保存できるファームウェアファイルは最大 2 つです。
ファームウェアを正常にアップグレードするには、Management > File System 画面で、ファームウェアファイルが 1 つであることを確認の上、アップグレードを実施して下さい。2 つ以上ファームウェアファイルがある場合は、古いファームウェアファイルを削除して下さい。

ファームウェアの保存およびアップロードは、「HTTP」または「TFTP」経由で行います。

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。

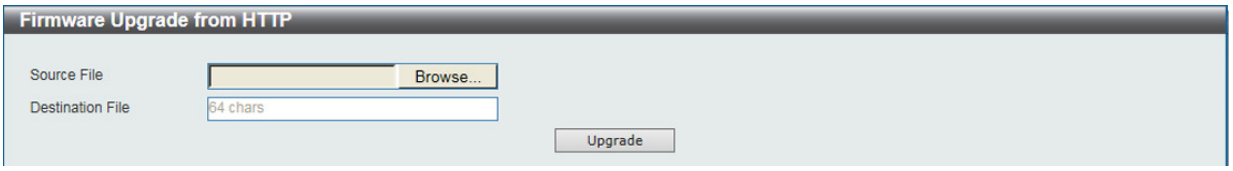

図 15-2　Firmware Upgrade from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

Firmware Upgrade from TFTP（TFTP を使用したファームウェアアップグレード）

TFTP を使用してファームウェアアップグレードを実行します。

Tools > Firmware Upgrade & Backup > firmware Upgrade from TFTP をクリックし、設定画面を表示します。

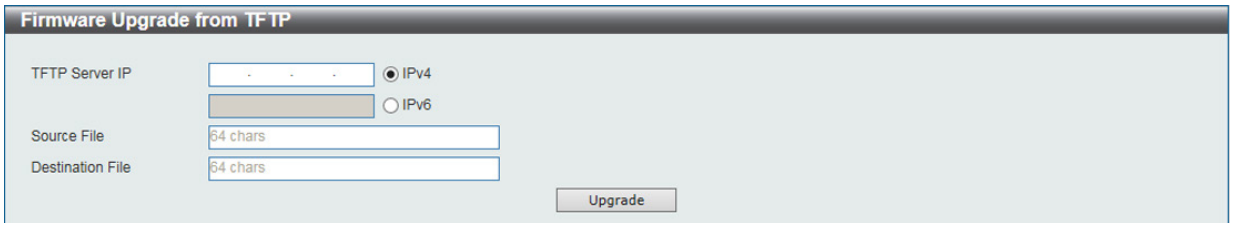

図 15-3　Firmware Upgrade from TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

Firmware Backup to HTTP（HTTP を使用したファームウェアバックアップ）

HTTP サーバにファームウェアバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP をクリックし、設定画面を表示します。

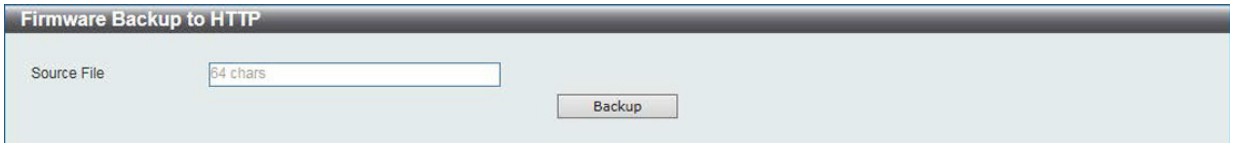

図 15-4　Firmware Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。

「Backup」ボタンをクリックしてバックアップを開始します。

Firmware Backup to TFTP（TFTP を使用したファームウェアバックアップ）

TFTP サーバにファームウェアバックアップを行います。

Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP をクリックし、設定画面を表示します。

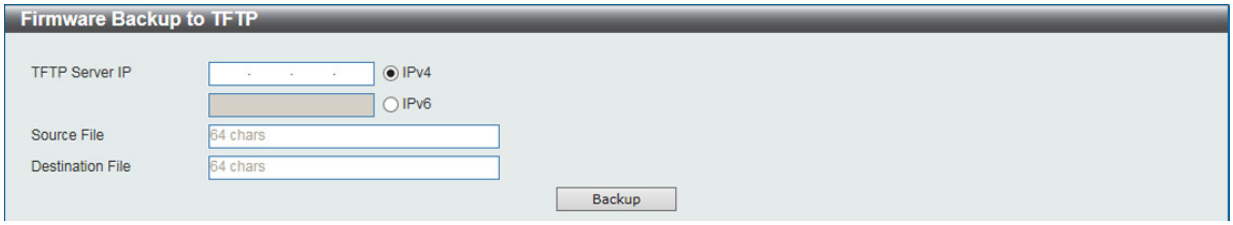

図 15-5　Firmware Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。
Destination File	ファームウェアファイルがバックアップされる TFTP サーバの場所（パス / ファイル名）を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）

Configuration Restore from HTTP（HTTP サーバからコンフィグレーションのリストア）

HTTP サーバを使用してローカル PC からコンフィグレーションをリストアします。

Tools > Configuration Restore & Backup > Configuration Restore from HTTP をクリックし、設定画面を表示します。

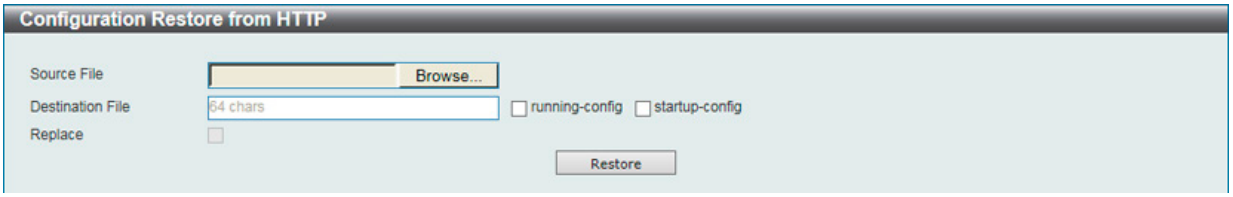

図 15-6　Configuration Restore from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source File	ローカル PC にあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。 「Browse/ 参照」ボタンをクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定できます。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

Configuration Restore from TFTP（TFTP サーバからコンフィグレーションのリストア）

TFTP サーバを使用してローカル PC からコンフィグレーションをリストアします。

Tools > Configuration Restore & Backup > Configuration Restore from TFTP をクリックし、設定画面を表示します。

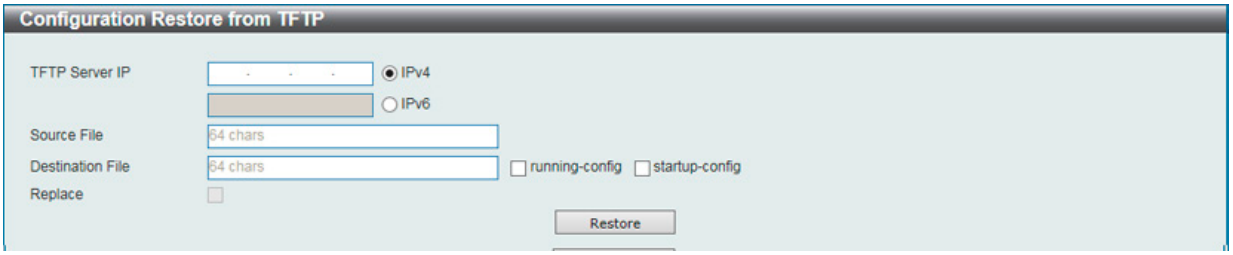

図 15-7　Configuration Restore from TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

Configuration Backup to HTTP（HTTP を使用したコンフィグレーションバックアップ）

HTTP サーバを使用してローカル PC にコンフィグレーションバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to HTTP をクリックし、設定画面を表示します。

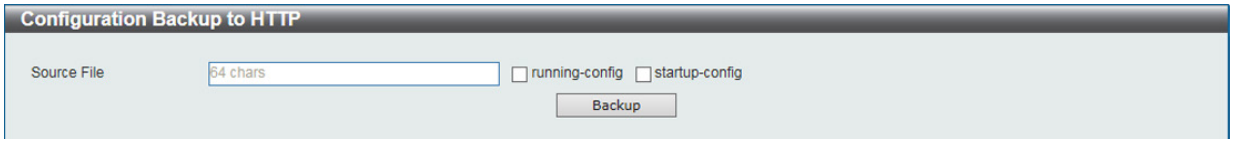

図 15-8　Configuration Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup-config」オプションを選択すると起動時のコンフィグレーションファイルがバックアップされます。

「Backup」ボタンをクリックしてバックアップを開始します。

Configuration Backup to TFTP（TFTP を使用したコンフィグレーションバックアップ）

TFTP サーバにコンフィグレーションバックアップを行います。

Tools > Configuration Restore & Backup > Configuration Backup to TFTP をクリックし、設定画面を表示します。

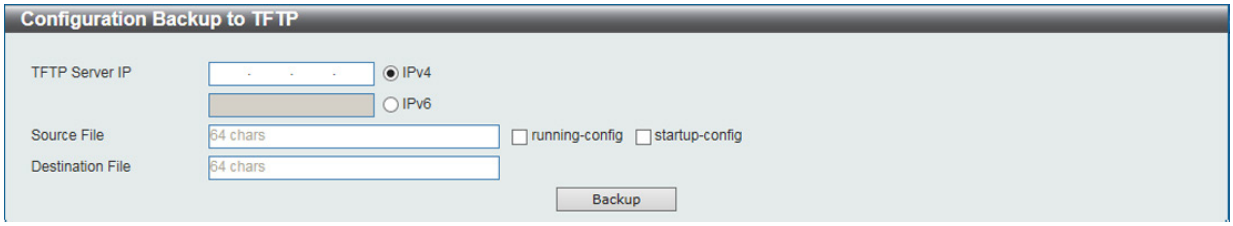

図 15-9　Configuration Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup-config」オプションを選択すると起動時のコンフィグレーションファイルがバックアップされます。
Destination File	コンフィグレーションファイルがストアされる TFTP サーバの場所を指定します。64 文字までで指定できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Log Backup（ログファイルのバックアップ）

Log Backup to HTTP（HTTP サーバを使用したログファイルのバックアップ）

HTTP サーバを使用してローカル PC へのシステムログのバックアップを行います。

Tools > Log Backup > Log Backup to HTTP をクリックし、設定画面を表示します。

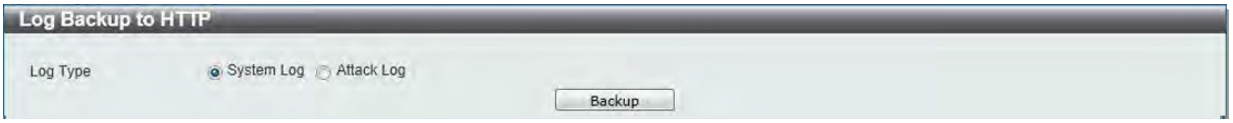

図 15-10 Log Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Log Type	HTTP を使用してローカル PC にバックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップします。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。

「Backup」ボタンをクリックしてバックアップを開始します。

Log Backup to TFTP（TFTP サーバを使用したログファイルのバックアップ）

TFTP サーバへのシステムログのバックアップを行います。

Tools > Log Backup > Log Backup to TFTP をクリックし、設定画面を表示します。

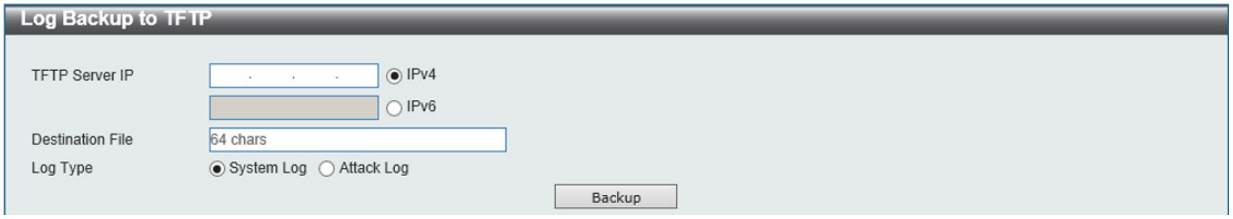

図 15-11 Log Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Destination File	ログファイルがストアされる TFTP サーバの場所を指定します。64 文字までで指定できます。
Log Type	バックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップします。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。

「Backup」ボタンをクリックしてバックアップを開始します。

Ping

「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。宛先の機器はスイッチから送信された "echoes" に応答します。これはネットワーク上のスイッチと機器の接続状況を確認するうえで非常に有効です。

Tools > Ping をクリックし、設定画面を表示します。

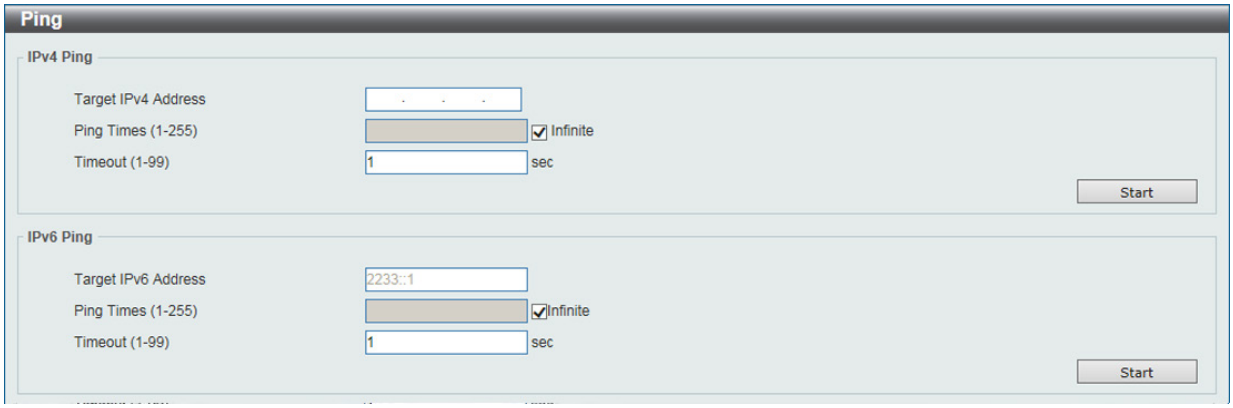

図 15-12 Ping 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
IPv4 Ping	
Target IPv4 Address	Ping する IPv4 アドレスを入力します。
Ping Times	繰り返し行う Ping の回数を入力します。1 から 255 の間でしてできます。「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99（秒）までの間で指定できます。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。
IPv6 Ping	
Target IPv6 Address	Ping する IPv6 アドレスを入力します。
Ping Times	繰り返し行う Ping の回数を入力します。1 から 255 の間でしてできます。 「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99（秒）までの間で指定できます。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。

「Start」ボタンをクリックして、各個別セクションでの Ping テストを実行します。

「IPv4 Ping」セクションで「Start」をクリックすると以下の「IPv4 Ping Result」画面が表示されます。

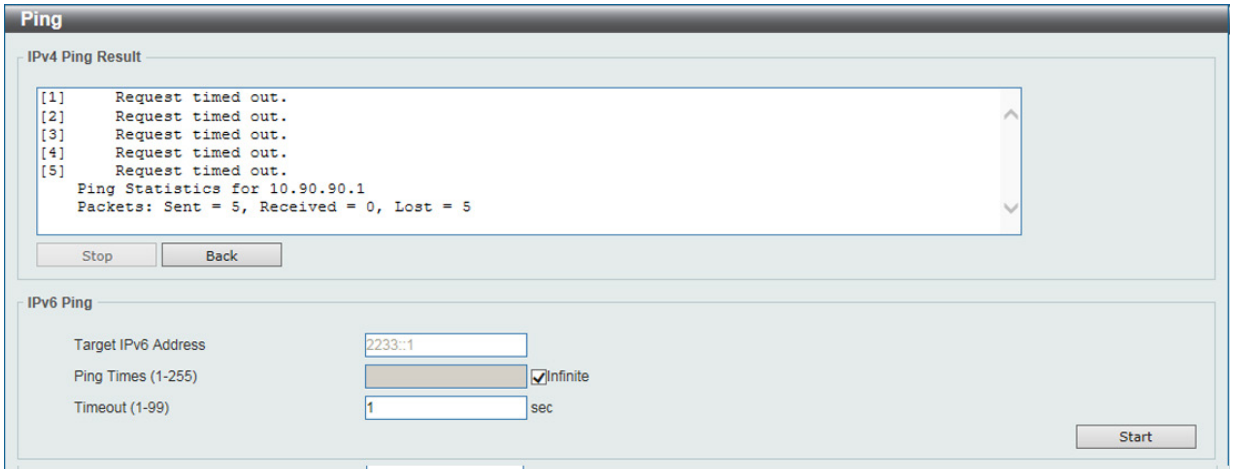

図 15-13 IPv4 Ping Result 画面

「Stop」ボタンをクリックして、Ping テストを停止します。
「Back」ボタンをクリックして、前の画面に戻ります。

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。

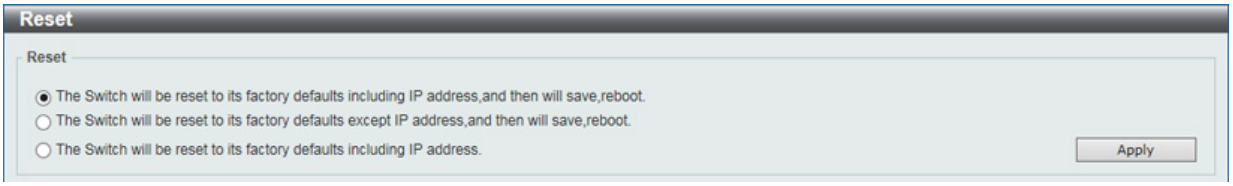

図 15-14　Reset System 画面

項目	説明
The Switch will be reset to its factory defaults including IP address, and then will save, reboot.	IP アドレスを含む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。
The Switch will be reset to its factory defaults except IP address, and then will save, reboot	IP アドレスを除くスイッチを工場出荷時の設定に戻し、保存、再起動を実行します。
The Switch will be reset to its factory defaults including IP address	IP アドレスを含むスイッチを工場出荷時設定にリセットしますが、再起動は行いません。

「Apply」ボタンをクリックして、リセット操作を開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

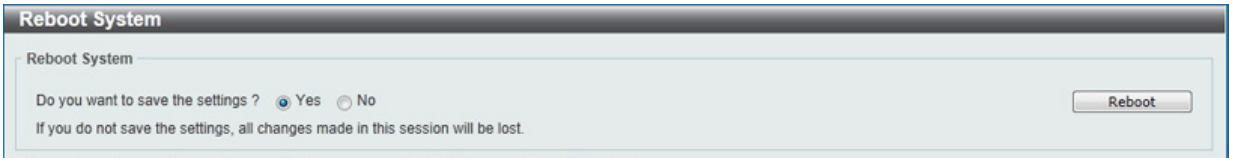

図 15-15　Reboot System 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Yes	スイッチは再起動する前に現在の設定を保存されます。
No	スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。
Reboot	スイッチは再起動します。

「Reboot」をクリックして再起動を開始します。

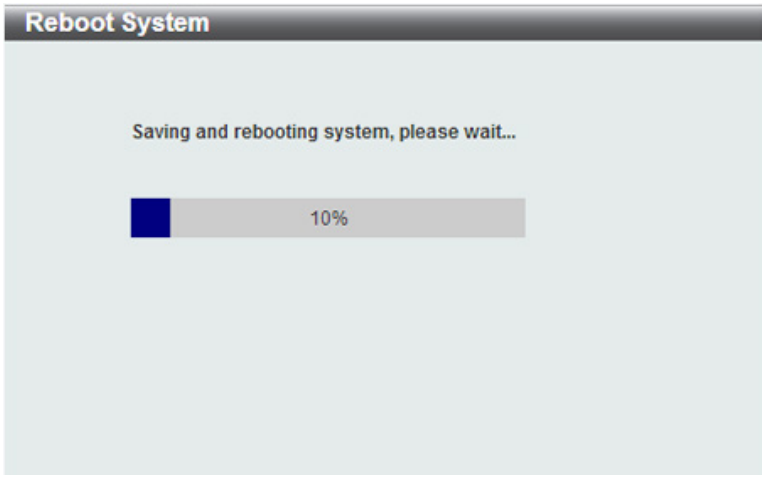

図 15-16　System Rebooting 画面

付録 A ケーブルとコネクタ

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。
以下の図と表は標準の RJ-45 プラグ / コネクタとピンアサインです。

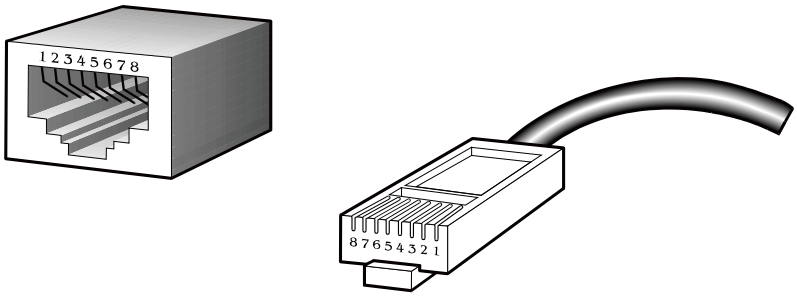

図 A-1　標準的な RJ-45 プラグとコネクタ

表 A-1　標準的な RJ-45 ピンアサイン

RJ-45 ピンアサイン		
コンタクト（ピン番号）	MDI-X 信号	MDI-II 信号
1	RD+（受信）	TD+（送信）
2	RD-（受信）	TD-（送信）
3	TD+（送信）	RD+（受信）
4	未使用	未使用
5	未使用	未使用
6	TD-（送信）	RD-（受信）
7	未使用	未使用
8	未使用	未使用

付録 B ケーブル長

以下の表は各規格に対応するケーブル長（最大）です。

規格	メディアタイプ	最大伝送距離
SFP	1000BASE-LX、シングルモードファイバモジュール 1000BASE-SX、マルチモードファイバモジュール 1000BASE-LH、シングルモードファイバモジュール 1000BASE-ZX、シングルモードファイバモジュール	10 km 550 m 40 km 80 km
1000BASE-T	エンハンスドカテゴリ 5 UTP ケーブル カテゴリ 5 UTP ケーブル（1000 Mbps）	100 m
100BASE-TX	カテゴリ 5 UTP ケーブル（100 Mbps）	100 m
10BASE-T	カテゴリ 3 UTP ケーブル（10 Mbps）	100 m

付録 C 用語解説

用語	説明
1000BASE-LX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。長い光波長で長距離伝送用に使用されます。伝送距離（最大）はシングルモード光ファイバを使用した場合で 10km。
1000BASE-SX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。短い光波長でマルチモード光ファイバを使用した場合伝送距離（最大）は 550m。
100BASE-FX	光ファイバを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
100BASE-TX	カテゴリ 5 以上の UTP ケーブルを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
10BASE-T	IEEE 802.3 準拠でカテゴリ 3 以上の UTP ケーブルを使用する最大伝送速度 10Mbps の Ethernet の規格のひとつ。
エージング	タイムアウトし、無効のスイッチのダイナミックデータベースを自動的に消去します。
ATM	非同期転送モード。セルと呼ばれる固定長のセル（パケット）ベースで転送するプロトコル。ATM は音声、データおよびビデオ信号を含むユーザトラフィックの完全な列を転送するために開発されたものです。
オートネゴシエーション	スピード、デュプレックスおよびフローコントロールを自動的に認識する機能。オートネゴシエーションをサポートする端末と接続すると、リンクは自動的に最適なリンク条件に設定されます。
バックボーンポート	デバイスのアドレスを学習せず不明なアドレスを持つすべてのフレームを受信するポート。バックボーンポートは通常ご使用のネットワークのバックボーンにスイッチを接続するために使用されるポートです。バックボーンポートは以前はダウンリンクポートとして知られていました。
バックボーン	ネットワークセグメント間でトラフィックが転送される場合に優先パスとして使用されるネットワークの一部分。
帯域	1 秒あたりのビット数で計算される 1 チャンネルが転送できる情報量。イーサネットの帯域は 10Mbps、ファーストイーサネットは 100Mbps。
ボーレート	ラインのスイッチングスピード。ネットワークセグメント間のラインスピードとして知られています。
BOOTP	BOOTP プロトコルはデバイスが起動するたびに IP アドレスを MAC アドレスに自動マッピングします。さらにデバイスにサブネットマスク、デフォルトゲートウェイを割り当てます。
ブリッジ	たとえ高いレベルのプロトコルが関連してもローカルまたはリモートネットワークを相互接続するデバイス。ブリッジはネットワーク管理を中央に集めて 1 個の論理ネットワークを形成します。
ブロードキャスト	ネットワーク上のすべての終点デバイスに送信されるメッセージ。
ブロードキャストストーム	が主として可能なネットワーク帯域を奪い、ネットワークエラーを引き起こす Multiple simultaneous ブロードキャスト。
コンソールポート	端末またはモデムコネクタと接続可能なスイッチ上のポート。コンピュータ内でパラレル配列のデータをデータ転送リンクで使用されるシリアル形式に変換します。このポートはほとんどの場合ローカル管理のために使用されます。
CSMA/CD	イーサネットと IEEE 802.3 標準によって使用されるチャンネルアクセス方法で検索したデータチャンネルが一定期間後クリアされた後にだけデバイスに転送します。2 つのデバイスが同時に転送する場合、コリジョンが発生し、コリジョンを発生したデバイスは任意の時間再転送を遅らせます。
データセンタースイッチング	スイッチがサーバファームへの高パフォーマンスアクセス、高速バックボーン接続、およびネットワーク管理とセキュリティのためのコントロールポイントを提供するコーポレートネットワーク内のアグリゲーションポイント
イーサネット	Xerox、Intel および DEC が共同で開発した LAN 仕様。イーサネットネットワークは CSMA/CD を使用して 10Mbps で処理を行います。
ファーストイーサネット	Ethernet/CD ネットワークアクセス方法をベースにした 100Mbps 技術。
フローコントロール	(IEEE 802.3x) 端末に接続した転送ポートへのパケットを抑止します。受信バッファがあふれそうになった場合にパケットロスを防ぎます。
フォワーディング	中間のネットワークデバイスによりパケットを到達点に向けて送信するプロセス。
フルデュプレックス	同時にパケットの送受信を可能とし、スループットを 2 倍にするシステム。
ハーフデュプレックス	パケットの送受信を行うが、同時には行えないシステム。
IP アドレス	Internet Protocol アドレス。TCP/IP を使用するネットワークに付属するデバイスの固有な識別子。IPv4 アドレスは 8 ビットずつピリオドで区切られ、ネットワークセクション、サブネットセクション、ホストセクションで構成されます。
IPX（Internetwork Packet Exchange）	ネットワーク通信で使用するプロトコル。
LAN – ローカルエリアネットワーク	通常フロアもしくはビルのような規模の小さいエリアで PC、プリンタ、サーバのようなコンピュータリソースを接続するネットワーク。高速で低エラー率が特長です。
レイテンシ	デバイスがパケットを受信する時間とパケットが到達点ポートに転送される時間の遅延。
ラインスピード	ボーレートを参照。
メインポート	通常の操作条件でデータトラフィックを送信する Resilient リンク内のポート。

用語	説明
MDI（Medium Dependent Interface）	1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。
MDI-X（Medium Dependent Interface Cross-over）	接続送受信のラインが交差しているイーサネットポート接続。
MIB（Management Information Base）	デバイスの管理特性とパラメータを保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。
マルチキャスト	シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。
プロトコル	ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。
Resilient link	他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。
RJ-45	10BASE-T や 100BASE-TX などで使用する標準 8 線コネクタ
RMON	リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。
RPS（リダンダント電源システム）	スイッチに接続されて、バックアップ電源を供給するデバイス。
サーバファーム	大量のユーザにサービスを提供する中央に位置するサーバグループ。
SLIP（Serial Line Internet Protocol）	IP がシリアルライン接続を経由して動作することが可能なプロトコル。
SNMP（Simple Network Management Protocol）	当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。
スパニングツリープロトコル (STP)	ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。
スタック	1 個の論理的なデバイスの形をとするために統合されたネットワークデバイスのグループ。
スタンバイポート	リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。
スイッチ	パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。
TCP/IP	Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。
telnet	仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。
TFTP（Trivial File Transfer Protocol）	スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する（ソフトウェアアップグレードなど）ことができます。
UDP（User Datagram Protocol）	インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。
VLAN（Virtual LAN）	物理的に接続した LAN のように通信する位置やトポロジが独立しているデバイスのグループ。
VLT（Virtual LAN Trunk）	各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。
VT100	ASCII コードを使用するターミナルタイプ。 VT100 画面はテキストベースの表示をします。

付録 D 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）

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-1100 シリーズ

Traffic Segmentation（トラフィックセグメンテーション）

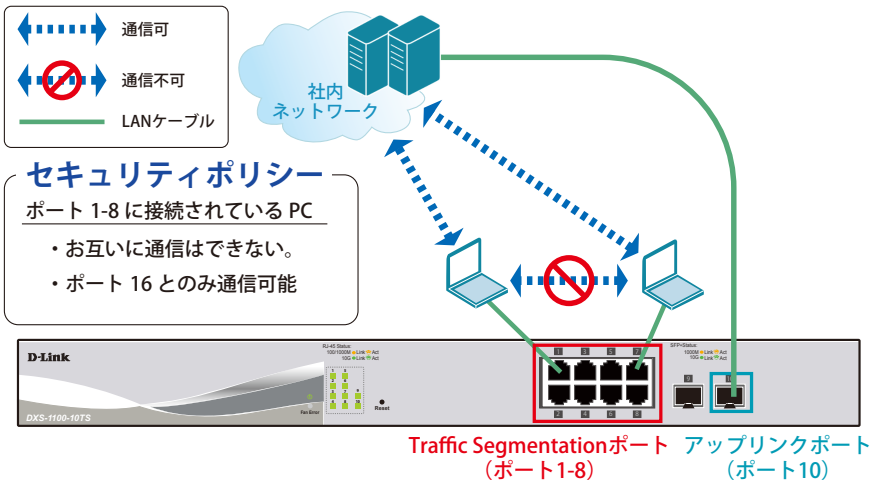

図 1-1　Traffic Segmentation（DXS-1100-10TS）

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 10 とのみ通信ができるようにします。

設定手順

1. **Security > Traffic Segmentation Settings** で「Traffic Segmentation」の適応ポート範囲を設定します。
「From / To Port」で「Traffic Segmentation」の適応ポート範囲を、「From / To Forward Port」で通信可能なアップリンクポートを指定します。

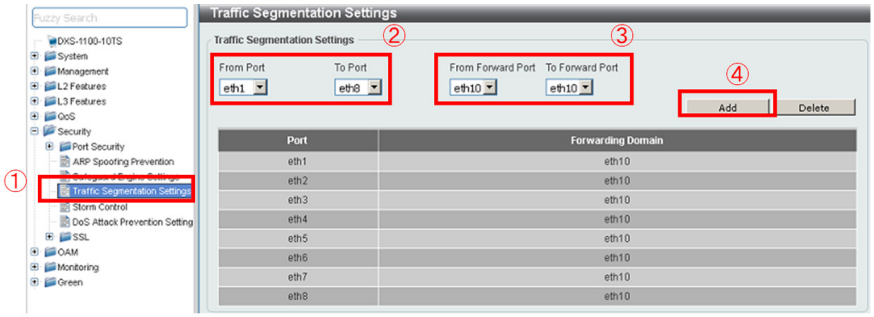

図 1-2　Traffic Segmentation（DXS-1100-10TS）

注意　本機能を利用する場合、Unknown ユニキャストについては全ポートにブロードキャストされます。各 PC 間のユニキャストを閾値 0 にすることにより制限することができます。

2. **Security > Storm Control** で「Storm Control」機能を「Unknown」ユニキャストを設定、「Action」を「Drop」にし、閾値を「0」に設定します。

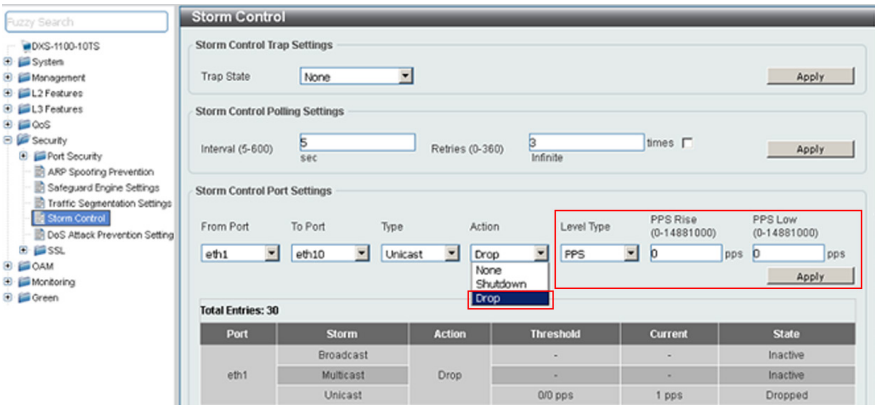

図 1-3　Storm Control（DXS-1100-10TS）

3. **Save > Save Configuration** で設定を保存します。「Apply」をクリックします。

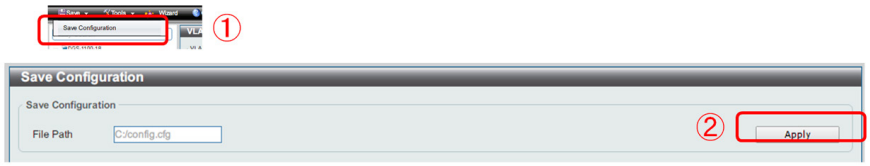

図 1-4　Save Configuration（DXS-1100-10TS）

VLAN

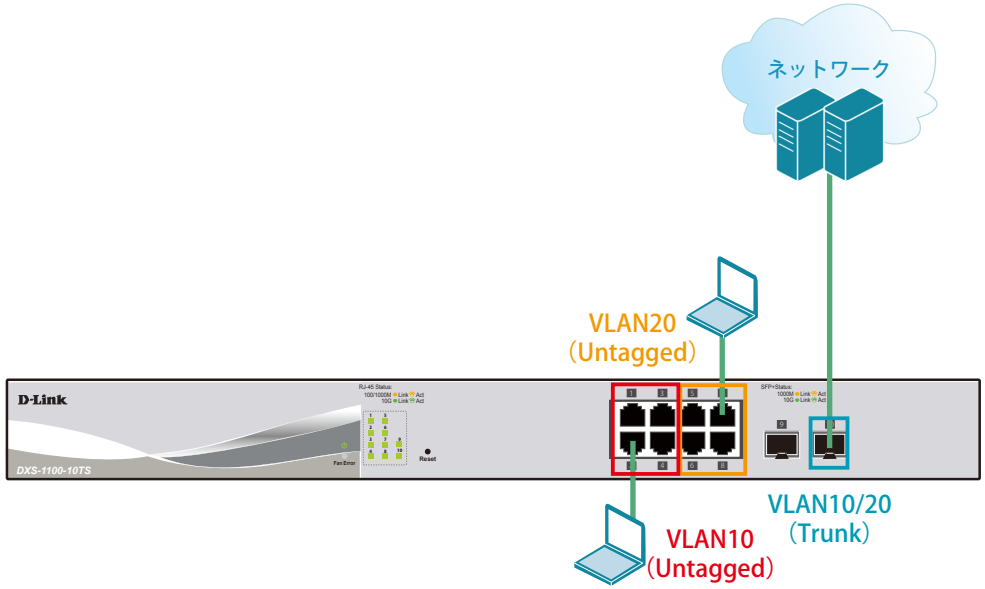

図 1-5　VLAN（DXS-1100-10TS）

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 10 において、VLAN10 と VLAN20 を「Tagged」で割り当てます。

設定手順

1. VLAN10 と VLAN20 を作成します。**L2 Features > VLAN > 802.1Q VLAN** で VLAN10 を作成します。

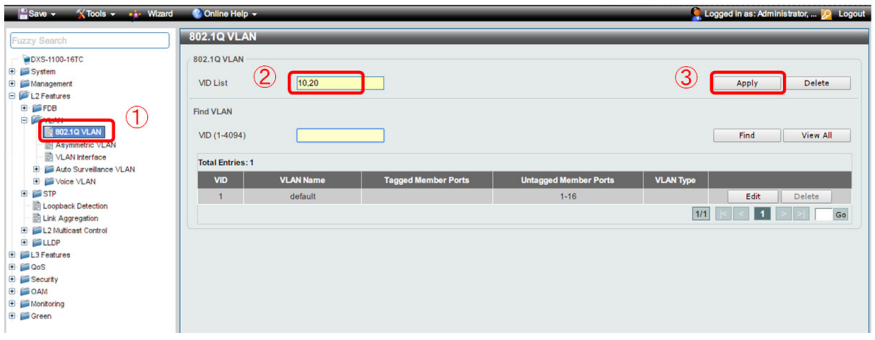

図 1-6　VLAN 作成（DXS-1100-10TS）

2. ポート 1 ～ 4 に VLAN10、ポート 5 ～ 8 に VLAN20 を割り当て、ポート 10 に VLAN10、20 を「Tagged」で割当てします。
L2 Features > VLAN > VLAN Interface でポート 1 から順に 4 まで VLAN10（VID10）を「Untagged」で割り当てます。

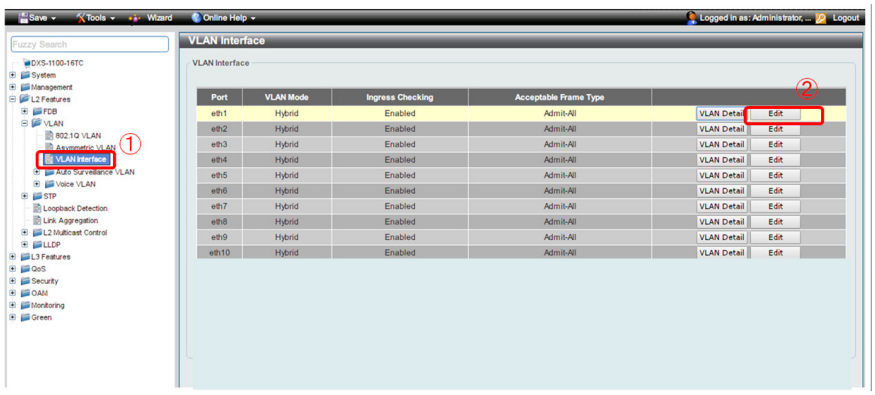

図 1-7　VLAN 編集（DXS-1100-10TS）

3. ポート 1 において下図のように設定し、「Apply」をクリックします。ポート 2，3，4 においても同様の設定を行います。

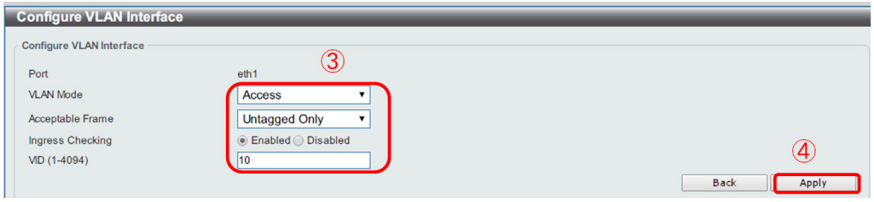

図 1-8　VLAN インタフェース設定（ポート 1）（DXS-1100-10TS）

VLAN Mode	Access
Acceptable Frame	Untagged Only
VID	10

4.「ポート 5 ～ 8」においては「VLAN20」を上記、同様の手順で割当てます。

5.「ポート 10」に「VLAN10」と「VLAN20」をトランクで割当てます。
①の項目で下図のように設定し、「Apply」をクリックします。

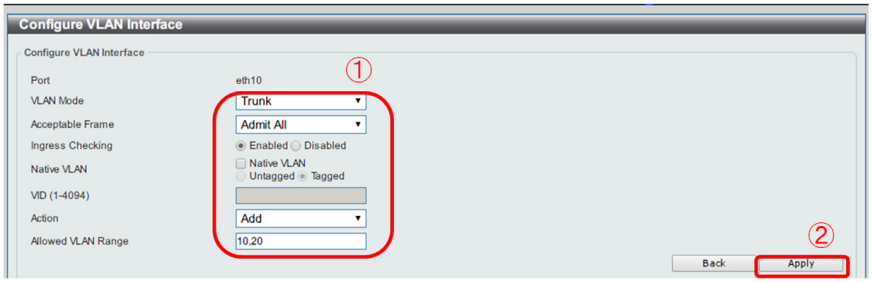

図 1-9　VLAN インタフェース設定（ポート 10）（DXS-1100-10TS）

VLAN Mode	Trunk
Action	Add
VID	10、20

注意　作成した VLAN でトランクしたくない VLAN は「Remove」を選択して削除してください。

6. **Save > Save Configuration** で設定を保存します。「Apply」をクリックします。

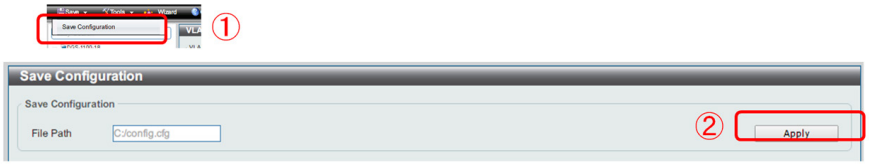

図 1-10　Save Configuration（DXS-1100-10TS）

Link Aggregation（リンクアグリゲーション）

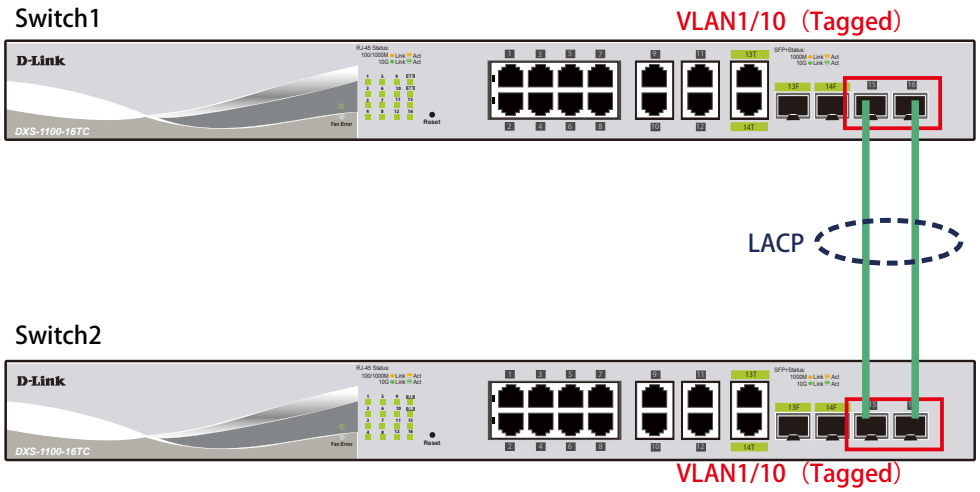

図 1-11　Link Aggregation（DXS-1100-16TC）

概要

VLAN1 と 10 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 15 と 16 に VLAN1 と VLAN10 を Tagged で割当て、ポート 15 と 16 をグループとして 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

1. VLAN10 を作成します。**L2 Features > VLAN > 802.1Q VLAN** を開き、「VID List」に 10 を設定して「Apply」をクリックします。

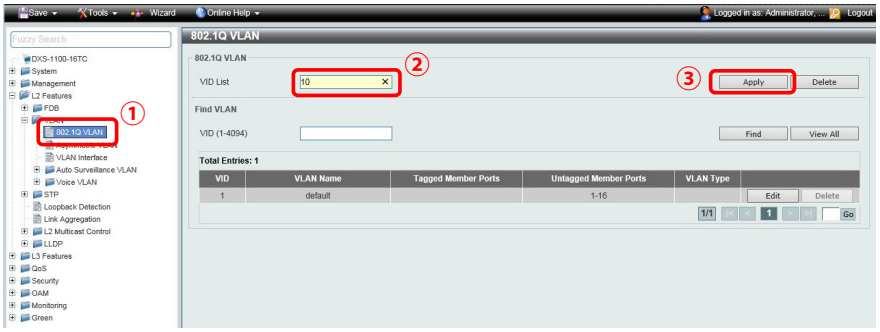

図 1-12　VLAN 作成（DXS-1100-16TC）

2. **L2 Features > Link Aggregation** でポート 15 ～ 16 を LACP に設定します。
②の項目で対象ポートを「eth15 ～ 16」に指定し「Group ID」「Mode」を下図のように設定します。「Add」をクリックします。

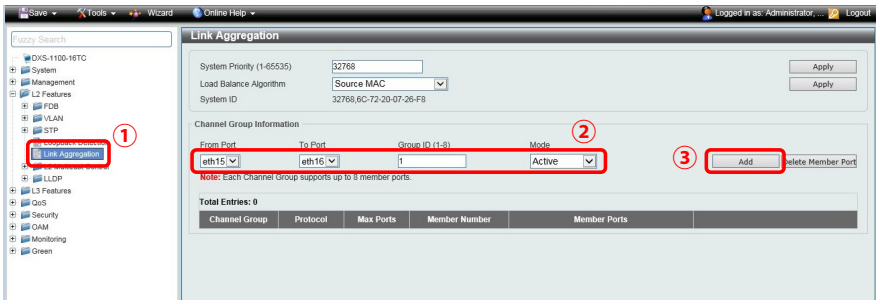

図 1-13　Link Aggregation 設定（DXS-1100-16TC）

From Port	eth15
To Port	eth16
Group ID	1
Mode	Active

3. リンクアグリゲーションをポート 15、16 に設定します。**L2 Features > VLAN > VLAN Interface** に移動し、Port-channel1 行上の「Edit」ボタンをクリックします。

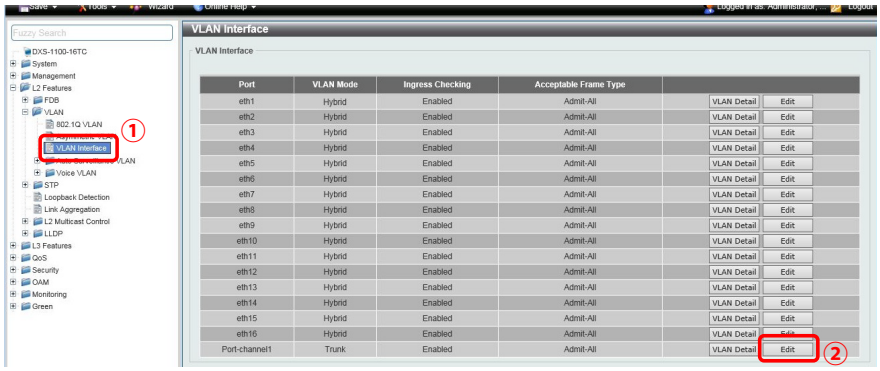

図 1-14　VLAN 編集 設定（DXS-1100-16TC）

4. 下図のように設定し、「Apply」をクリックします。

図 1-15　VLAN インタフェース設定（Port-channel1）（DXS-1100-16TC）

VLAN Mode	Trunk
Native VLAN	チェック
Native VLAN	Untagged
VID	1
Action	Replace
Allowed VLAN Range	1,10

5. **Save > Save Configuration** で設定を保存します。「Apply」をクリックします。

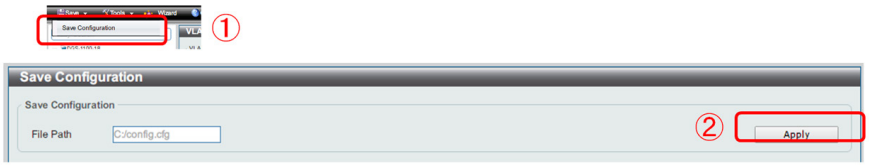

図 1-16　Save Configuration（DXS-1100-16TC）