D-Link DXS-1210-28T/28S

10 Gigabit Layer 2 Smart Managed Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

⚠危険	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
⚠警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、間違った使い方をすると、傷害または物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ラベルや「Warranty Void Sticker」（シール）をはがさないでください。はがしてしまうとサポートを受けられなくなります。

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。
このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

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

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

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

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

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

目次

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 5

はじめに 12

本マニュアルの対象者 13
表記規則について 13
製品名 / 品番一覧 13

第 1 章　本製品のご利用にあたって 14

スイッチ概要 14
SFP について 15
ダイレクトアタッチケーブル 15
前面パネル 16
　Reset（リセットボタン） 16
LED 表示 17
背面パネル 18
側面パネル 18
　スマートファンについて 18

第 2 章　スイッチの設置 19

パッケージの内容 19
ネットワーク接続前の準備 19
ゴム足の取り付け（19 インチラックに設置しない場合） 19
19 インチラックへの取り付け 20
光トランシーバの接続 21
電源抜け防止クリップの装着 22
スイッチの接地 24
　接地に必要なツールと機器 24
電源の投入 24
電源の異常 24

第 3 章　スイッチの接続 25

エンドノードと接続する 25
ハブまたはスイッチと接続する 25
バックボーンまたはサーバと接続する 26

第 4 章　スイッチ管理について 27

Web GUI による管理 27
SNMP による管理 27
CLI による管理 27
コンソールポートの接続 28
　端末をコンソールポートに接続する 28
　ユーザアカウント / パスワードの設定 29
　IP アドレスの設定 29

第 5 章　Web ベースのスイッチ管理 30

Web ベースの管理について 30
Web マネージャへのログイン 30
Smart Wizard 設定 32
　Web モードの選択（Smart Wizard） 32
　IP アドレスの設定（Smart Wizard） 33
　ユーザアカウントの設定（Smart Wizard） 34
　SNMP の設定（Smart Wizard） 35
Web ベースのユーザインタフェース 36
　ユーザインタフェース内の各エリア（スタンダードモード） 36
　ユーザインタフェース内の各エリア（サーベイランスモード） 37
Web マネージャのメニュー構成 38

第 6 章　System（システム設定）　40

Device Information（デバイス情報）....41
System Information Settings（システム情報）....42
Peripheral Settings（環境設定）....42
Port Configuration（ポート設定）....43
Port Settings（ポート設定）....43
Port Status（ポートステータス）....44
Port Auto Negotiation（ポートオートネゴシエーション）....44
Error Disabled Settings（エラーディセーブル設定）....45
Jumbo Frame（ジャンボフレーム設定）....46
Interface Description（インタフェース概要）....46
System Log（システムログ）....47
System Log Settings（システムログ設定）....47
System Log Discriminator Settings（システムログ識別設定）....48
System Log Server Settings（システムログサーバの設定）....49
System Log（システムログ）....50
System Attack Log（システム攻撃ログ）....50
Time and SNTP（時刻・SNTP 設定）....51
Clock Settings（時刻設定）....51
Time Zone Settings（タイムゾーン設定）....51
SNTP Settings（SNTP 設定）....53
Time Range（タイムレンジ設定）....54

第 7 章　Management（スイッチの管理）　55

User Accounts Settings（ユーザアカウント設定）....56
SNMP（SNMP 設定）....57
トラップ....57
MIB....57
SNMP Global Settings（SNMP グローバル設定）....58
SNMP Linkchange Traps Settings（SNMP リンクチェンジトラップ設定）....59
SNMP View Table Settings（SNMP ビューテーブル）....59
SNMP Community Table Settings（SNMP コミュニティテーブル設定）....60
SNMP Group Table Settings（SNMP グループテーブル設定）....61
SNMP Engine ID Local Settings（SNMP エンジン ID ローカル設定）....61
SNMP User Table Settings（SNMP ユーザテーブル設定）....62
SNMP Host Table Settings（SNMP ホストテーブル設定）....63
RMON（RMON 設定）....64
RMON Global Settings（RMON グローバル設定）....64
RMON Statistics Settings（RMON 統計設定）....64
RMON History Settings（RMON ヒストリ設定）....65
RMON Alarm Settings（RMON アラーム設定）....66
RMON Event Settings（RMON イベント設定）....67
Telnet / Web（Telnet /Web 設定）....68
Session Timeout（セッションタイムアウト）....69
DHCP（DHCP 設定）....70
Service DHCP（DHCP サービス）....70
DHCP Class Settings（DHCP クラス設定）....70
DHCP Relay（DHCP リレー）....71
DHCPv6 Relay（DHCPv6 リレー）....75
DHCP Auto Configuration（DHCP 自動設定）....79
DHCP Auto Image Settings（DHCP 自動イメージ設定）....79
DNS（ドメインネームシステム）....80
DNS Global Settings（DNS グローバル設定）....80
DNS Name Server Settings（DNS ネームサーバ設定）....80
DNS Host Settings（DNS ホスト設定）....81
File System（ファイルシステム）....82
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）....84
DDP Settings（DDP 設定）....84
DDP Neighbors（DDP 隣接機器）....84

第 8 章　L2 Features（レイヤ 2 機能の設定）　85

FDB（FDB 設定）....86
Static FDB（スタティック FDB 設定）....86
MAC Address Table Settings（MAC アドレステーブル設定）....86
MAC Address Table（MAC アドレステーブル）....87
MAC Notification（MAC 通知設定）....88
VLAN について....89
IEEE 802.1p プライオリティについて....89
VLAN とは....89
IEEE 802.1Q VLAN....89
VLAN（VLAN 設定）....94
VLAN Configuration Wizard（VLAN 設定ウィザード）....94
802.1Q VLAN（802.1Q VLAN 設定）....95
VLAN Interface（VLAN インタフェース設定）....96
Asymmetric VLAN（Asymmetric VLAN 設定）....99
L2VLAN Interface Description（L2 VLAN インタフェース概要）....99
Auto Surveillance VLAN（自動サーベイランス VLAN）....100
Voice VLAN（音声 VLAN）....104
STP（スパニングツリーの設定）....107
802.1Q-2005 MSTP....107
802.1D-2004 Rapid Spanning Tree....107
ポートの状態遷移....108
STP Global Settings（STP グローバル設定）....109
STP Port Settings（STP ポートの設定）....110
MST Configuration Identification（MST の設定）....111
STP Instance（STP インタンス設定）....111
MSTP Port Information（MSTP ポート情報）....112
Loopback Detection（ループバック検知設定）....113
Link Aggregation（リンクアグリゲーション）....114
ポートトランクグループについて....114
L2 Multicast Control（L2 マルチキャストコントロール）....117
IGMP Snooping（IGMP スヌーピング）....117
MLD Snooping（MLD スヌーピング）....122
Multicast Filtering（マルチキャストフィルタリング）....127
LLDP（LLDP 設定）....128
LLDP Global Settings（LLDP グローバル設定）....128
LLDP Port Settings（LLDP ポート設定）....129
LLDP Management Address List（LLDP 管理アドレスリスト）....130
LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）....130
LLDP-MED Port Settings（LLDP-MED ポート設定）....132
LLDP Statistics Information（LLDP 統計情報）....133
LLDP Local Port Information（LLDP ローカルポート情報）....133
LLDP Neighbor Port Information（LLDP ネイバポート情報）....134

第 9 章　L3 Features（レイヤ 3 機能の設定）　136

ARP（ARP 設定）....136
ARP Aging Time（ARP エージングタイム設定）....136
Static ARP（スタティック ARP 設定）....137
ARP Table（ARP テーブルの参照）....137
Gratuitous ARP（Gratuitous ARP 設定）....138
IPv6 Neighbor（IPv6 Neighbor 設定）....139
Interface（インタフェース設定）....140
IPv4 Interface（IPv4 インタフェース）....140
IPv6 Interface（IPv6 インタフェース）....141
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート）....144
IPv4 Route Table（IPv4 ルートテーブル）....145
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート）....146
IPv6 Route Table（IPv6 ルートテーブル）....147
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル設定）....148
IPMC（IPMC 設定）....148
IPv6MC（IPv6MC 設定）....148

第 10 章　QoS（QoS 機能の設定）　149

Basic Settings（基本設定）....149
Port Default CoS（ポートデフォルト CoS 設定）....149
Port Scheduler Method（ポートスケジューラメソッド設定）....149
Queue Settings（QoS 設定）....150
CoS to Queue Mapping（CoS キューマッピング設定）....151
Port Rate Limiting（ポートレート制限設定）....151
Queue Rate Limiting（キューレート制限設定）....152
Advanced Settings（詳細設定）....153
DSCP Mutation Map（DSCP 変更マップ設定）....153
Port Trust State and Mutation Binding（ポートトラスト設定 & 変更マップバインディング）....153
DSCP CoS Mapping（DSCP CoS マップ設定）....154
Class Map（クラスマップ設定）....154
Policy Map（ポリシーマップ設定）....156
Policy Binding（ポリシーバインディング設定）....157

第 11 章　ACL（ACL 機能の設定）　158

ACL Configuration Wizard（ACL 設定ウィザード）....158
ACL Configuration Wizard（ACL 設定ウィザードの開始）....158
パケットタイプ選択（ACL 設定ウィザード）....159
ルール追加（ACL 設定ウィザード）....159
ポート設定（ACL 設定ウィザード）....165
ACL Access List（ACL アクセスリスト）....166
Standard IP ACL（通常 IP ACL）の設定....167
Extended IP ACL（拡張 IP ACL）の設定....168
Standard IPv6 ACL（標準 IPv6 ACL）の設定....170
Extended IPv6 ACL（拡張 IPv6 ACL）の設定....171
Extended MAC ACL（拡張 MAC ACL）の設定....173
ACL Interface Access Group（ACL インタフェースアクセスグループ）....174

第 12 章　Security（セキュリティ機能の設定）　175

Port Security（ポートセキュリティ）....176
Port Security Global Settings（ポートセキュリティグローバル設定）....176
Port Security Port Settings（ポートセキュリティポート設定）....177
Port Security Address Entries（ポートセキュリティアドレスエントリ設定）....178
802.1X（802.1X 認証設定）....179
802.1X Global Settings（802.1X グローバル設定）....183
802.1X Port Settings（802.1X ポート設定）....183
Authentication Session Information（認証セッションの状態）....184
Authenticator Statistics（オーセンティケータ統計情報）....184
Authenticator Session Statistics（オーセンティケータセッション統計情報）....185
Authenticator Diagnostics（オーセンティケータ診断）....185
AAA（AAA 設定）....186
AAA Global Settings（AAA グローバル設定）....186
Authentication Settings（認証設定）....186
RADIUS（RADIUS 設定）....187
RADIUS Global Settings（RADIUS グローバル設定）....187
RADIUS Server Settings（RADIUS サーバの設定）....187
RADIUS Group Server Settings（RADIUS グループサーバ設定）....188
RADIUS Statistic（RADIUS 統計情報）....189
IMPB（IP-MAC-Port Binding / IP-MAC ポートバインディング）....190
IPv4....190
IPv6....200
DHCP Server Screening（DHCP サーバスクリーニング設定）....205
DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）....205
DHCP Server Screening Port Settings（DHCP サーバスクリーニングポート設定）....206
ARP Spoofing Prevention（ARP スプーフィング防止設定）....207
Network Access Authentication（ネットワークアクセス認証）....208
Guest VLAN（ゲスト VLAN 設定）....208
Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）....208
Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）....209
Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）....210

Safeguard Engine（セーフガードエンジン）.....211
Safeguard Engine Settings（セーフガードエンジン設定）.....212
CPU Protect Counters（CPU プロテクトカウンタ）.....212
CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）.....213
CPU Protect Type（CPU プロテクトタイプ）.....213
Trusted Host（トラストホスト）.....214
Traffic Segmentation Settings（トラフィックセグメンテーション設定）.....214
Storm Control Settings（ストームコントロール設定）.....215
DoS Attack Prevention Settings（DoS 攻撃防止設定）.....217
SSH（Secure Shell の設定）.....218
SSH Global Settings（SSH グローバル設定）.....218
Host Key（Host Key 設定）.....219
SSH Server Connection（SSH サーバ接続）.....219
SSH User Settings（SSH ユーザ設定）.....220
SSL（Secure Socket Layer）.....221
SSL Global Settings（SSL グローバル設定）.....221
Crypto PKI Trustpoint（暗号 PKI トラストポイント）.....222
SSL Service Policy（SSL サービスポリシー）.....223
Network Protocol Port Protection Settings（ネットワークプロトコルポート保護設定）.....224

第 13 章　OAM（Operations, Administration, Maintenance：運用・管理・保守）　225

Cable Diagnostics（ケーブル診断機能）.....225

第 14 章　Monitoring（スイッチのモニタリング）　226

Utilization（利用分析）.....226
Port Utilization（ポート使用率）.....226
Statistics（統計情報）.....227
Port（ポート統計情報）.....227
Interface Counters（インタフェースカウンタ）.....228
Counters（カウンタ）.....229
Mirror Settings（ミラー設定）.....230
Device Environment（機器環境確認）.....231

第 15 章　Green（省電力テクノロジー）　232

Power Saving（省電力）.....232
EEE（Energy Efficient Ethernet/ 省電力イーサネット）.....233

第 16 章　Toolbar（ツールバー）　234

Save（保存）.....234
Save Configuration（コンフィグレーションの保存）.....234
Tools（ツール）.....235
Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）.....235
Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）.....237
Certificate & Key Restore & Backup（証明書と鍵のリストア＆バックアップ）.....239
Log Backup（ログのバックアップ）.....240
Ping.....241
Language Management（言語管理）.....242
Reset（リセット）.....243
Reboot System（システム再起動）.....243
Wizard（ウィザード）.....244
Online Help（オンラインヘルプ）.....244
D-Link Support Site（D-Link サポート Web サイト（英語））.....244
User Guide（ユーザガイド（英語版））.....244
Surveillance Mode（サーベイランスモードへの変更）.....244
Logout（ログアウト）.....244

第 17 章　サーベイランスモード 245

Surveillance Overview（サーベイランスモード概要）....246
Surveillance Topology（サーベイランストポロジ）....246
Device Information（デバイス情報）....247
Port Information（ポート情報）....248
IP-Camera Information（IP-Camera 情報）....250
NVR Information（NVR 情報）....251
Management（管理）....252
File System（ファイルシステム）....252
Time（時刻設定）....254
Clock Settings（時刻設定）....254
SNTP Settings（SNTP 設定）....254
Surveillance Settings（サーベイランス設定）....255
Surveillance Log（サーベイランスログ）....256
Health Diagnostic（正常性診断）....257
Toolbar（ツールバー）（サーベイランスモード）....258
Wizard（ウィザード）....258
Tools（ツール）....258
Save（保存）....261
Help（ヘルプ画面）....261
Online Help（オンラインヘルプ）....262
Standard Mode（スタンダードモード）....262
Logout（ログアウト）....262

【付録 A】システムログエントリ 263

【付録 B】トラップログエントリ 278

【付録 C】RADIUS 属性の割り当て指定 283

【付録 D】IETF RADIUS 属性のサポート 284

【付録 E】機能設定例 285

対象機器について....285
Traffic Segmentation（トラフィックセグメンテーション）....285
VLAN....286
Link Aggregation（リンクアグリゲーション）....288
Access List（アクセスリスト）....289
Loopback Detection（LBD）（ループ検知）....290

はじめに

DXS-1210-28T/28S 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、IP アドレス割り当て、および各種デバイスからの本スイッチへの接続など基本的なスイッチの管理について説明します。
- 第 5 章　Web ベースのスイッチ管理
  - Web ベースの管理機能への接続方法および使用方法について説明します。
- 第 6 章　System（システム設定）
  - デバイス情報の確認、環境設定、ポートの設定、システムログの設定と管理、システム時刻の設定について説明します。
- 第 7 章　Management（スイッチの管理）
  - ユーザアカウント設定など、スイッチの管理について説明します。
- 第 8 章　L2 Features（レイヤ 2 機能の設定）
  - FDB 設定、VLAN 設定、スパニングツリーの設定、ループバック検知設定など L2 機能について説明します。
- 第 9 章　L3 Features（レイヤ 3 機能の設定）
  - ARP 設定、IPv4/IPv6 インタフェース、IPv4/IPv6 ルート設定などの L3 機能について説明します。
- 第 10 章　QoS（QoS 機能の設定）
  - 802.1p 設定、DSCP、CoS、QoS 設定について説明します。
- 第 11 章　ACL（ACL 機能の設定）
  - アクセスコントロールリスト（ACL）関連の設定について説明します。
- 第 12 章　Security（セキュリティ機能の設定）
  - ポートセキュリティ、802.1X 認証、AAA、RADIUS 設定などのセキュリティの設定について説明します。
- 第 13 章　OAM（Operations, Administration, Maintenance：運用・管理・保守）
  - ケーブル診断機能について解説します。
- 第 14 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 15 章　Green（省電力テクノロジー）
  - 本スイッチの省電力、EEE について設定、表示します。
- 第 16 章　Toolbar（ツールバー）
  - Web インタフェース画面上部のツールバーにあるメニューを使用してスイッチの管理・設定を行います。また、設定の保存、リブートなどスイッチのユーティリティ機能について説明します。
- 第 17 章　サーベイランスモード
  - サーベイランスモードによる WebGUI の表示・操作について説明します。
- 【付録 A】システムログエントリ
  - ログエントリとそれらの意味について説明します。
- 【付録 B】トラップログエントリ
  - システムに表示される可能性のあるトラップログとそれらの意味について説明します。
- 【付録 C】RADIUS 属性の割り当て指定
  - DXS-1210-28T/28S における RADIUS 属性の割り当てについて説明します。
- 【付録 D】IETF RADIUS 属性のサポート
  - RADIUS 属性は IETF 標準と VSA（Vendor-Specific Attribute: ベンダ固有属性）によってサポートされており、本スイッチがサポートする RADIUS 属性を示します。
- 【付録 E】機能設定例
  - 機能設定例ついて説明します。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、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	HW バージョン	品番
DXS-1210-28T	A1	DXS-1210-28T/A1
DXS-1210-28S	A1	DXS-1210-28S/A1

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
- ダイレクトアタッチケーブル
- 前面パネル
- LED 表示
- 背面パネル
- 側面パネル

DXS-1210 シリーズは、様々な規模のネットワーク環境に柔軟に対応可能な 10 ギガビットスマートスイッチです。

DXS-1200-28T は 100/1000/10GBASE-T ポートを 24 ポート、25G SFP28 スロットを 4 ポート搭載し、DXS-1210-28S は 10G SFP+ スロットを 24 ポート、1000/10GBASE-T ポートを 4 ポート搭載しています。

SMB ネットワークのエッジ集約スイッチとしての使用のほか、エンタープライズネットワークでのエッジや集約スイッチとしても使用できます。

本マニュアルでは、DXS-1210-28T/28S 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-1210-28T/28S は、以下のポートを搭載した 10 ギガビット L2 スマートスイッチです。

- DXS-1210-28T：100/1000/10GBASE-T ポート x 24 ポート、25G SFP28 スロット x 4 ポート
- DXS-1210-28S：10G SFP+ スロット x 24 ポート、100/1000/10G BASE-T x 4 ポート

注意　DXS-1210-28T/28S について、区別する必要がある場合を除き、本マニュアル上では単に “スイッチ” あるいは “DXS-1210” と記載します。

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 100/1000/10GBASE-T ポートと 25G SFP28 スロット、10G 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おり、以下のオプション光トランシーバと共に使用が可能です。

種別	製品名
SFP28（25Giga）	DEM-S2801SR※1
	DEM-S2810LR※1
SFP+(10Giga)	DEM-431XT
	DEM-432XT
Copper SFP+（10Giga）	DEM-410T※2※4
WDM 対応 1 芯 SFP(1Giga)	DEM-330T※3※4
	DEM-330R※3※4
2 芯 SFP(1Giga)	DEM-310GT※4
	DEM-311GT※4
	DEM-314GT※4
Copper SFP(1Giga)	DGS-712※4

※ 1：SFP28 スロットでのみ使用可能です。
※ 2：DEM-410T/A2 を使用する場合、環境温度（室温）が 40℃までの環境での利用のみをサポートします。そのため、この場合のスイッチの動作温度範囲も 0~40℃までとなりますので、十分にご注意ください。また、DEM-410T の取り付けは、スイッチ 1 台に対し最大 2 個までとなります。
※ 3：DEM-330T と DEM-330R は対向でご使用下さい。
※ 4：SFP28 スロットでは使用できません。
※ スイッチ /SFP モジュールの H/W バージョンの組み合わせによっては、接続できない場合があります。サポートされる SFP モジュールの H/W バージョンについては、弊社 Web ページで公開されている「光トランシーバ対応製品一覧」をご確認ください。

ダイレクトアタッチケーブル

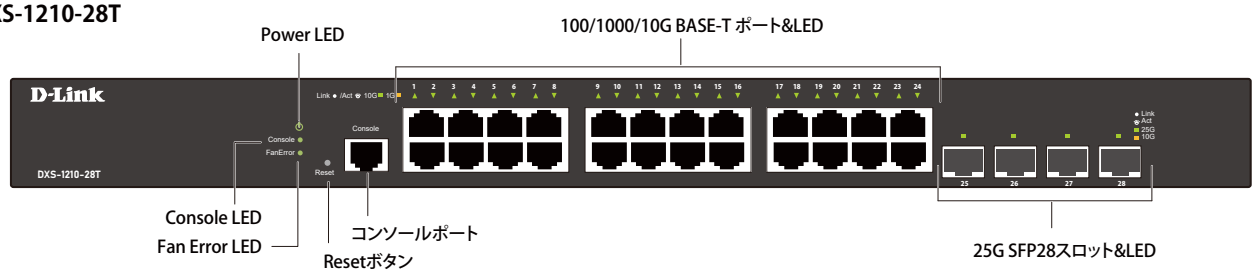
DXS-1210-28T/28S では以下のダイレクトアタッチケーブルを使用できます。

種別	製品名
SFP+ ダイレクトアタッチケーブル	DEM-CB100S
	DEM-CB300S
SFP28 ダイレクトアタッチケーブル	DEM-CB100S28

前面パネル

DXS-1210-28T/28S の前面パネルの各部名称は以下のとおりです。

DXS-1210-28T



DXS-1210-28S

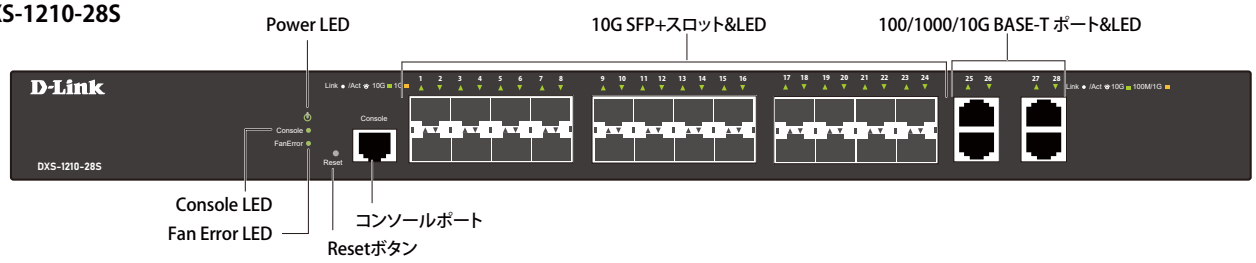


図 1-1　DXS-1210-28T/28S 前面パネル

Reset（リセットボタン）

スイッチの前面パネルにはリセットボタン（Reset）があり、押下する秒数により、再起動、または工場出荷値へのリセットが実行されます。

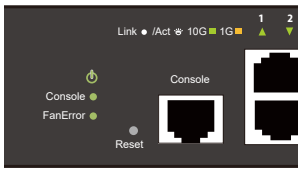


図 1-2　リセットボタン（DXS-1210-28T）

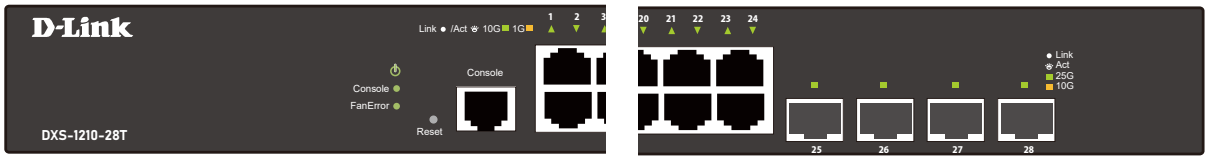
リセットボタンを使用したリセット方法（再起動方法）

- リセットボタンを 5 秒未満押下する（5 秒経過する前にボタンを離す）とスイッチは再起動されます。
  保存していない設定は破棄されます。
- リセットボタンを 5 秒以上押下する（5 秒経過後にボタンを離す）と、スイッチの設定内容を工場出荷値へリセットします。
  全てのポート LED が「橙」に点灯（2 秒間）し、リセットが開始されます。

LED 表示

前面パネルに搭載されている LED 表示について説明します。

DXS-1210-28T



DXS-1210-28S

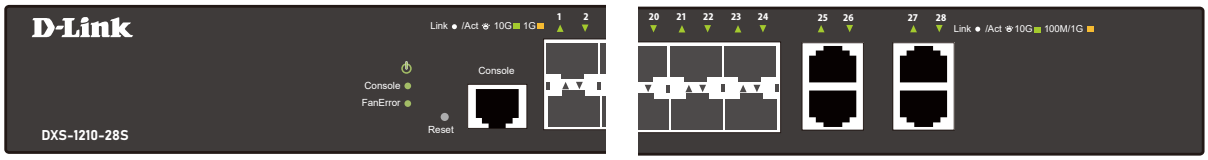


図 1-3　DXS-1210-28T/28S の LED 配置図

以下の表に LED の状態が意味するスイッチの状態を示します。

LED	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。
	緑	点滅	システムセルフテスト中です。
	ー	消灯	電源が供給されていません。
Console	緑	点灯	コンソール経由で本製品にログインしています。
	ー	消灯	コンソール経由で本製品にログインしていません。
FanError	赤	点灯	ファンは故障のため停止しています。
	ー	消灯	ファンは正常に動作しています。
ポート LED			
Link/Act （100/1000/10GBASE-T ポート）	緑	点灯	10 Gbps でリンクが確立しています。
		点滅	10 Gbps でデータを送受信しています。
	橙	点灯	100/1000 Mbps でリンクが確立しています。
		点滅	100/1000 Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
Link/Act （10G SFP+ スロット） ※ DXS-1210-28S のみ	緑	点灯	10 Gbps でリンクが確立しています。
		点滅	10 Gbps でデータを送受信しています。
	橙	点灯	1 Gbps でリンクが確立しています。
		点滅	1 Gbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
Link/Act （25G SFP28 スロット） ※ DXS-1210-28T のみ	緑	点灯	25 Gbps でリンクが確立しています。
		点滅	25 Gbps でデータを送受信しています。
	橙	点灯	10 Gbps でリンクが確立しています。
		点滅	10 Gbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。

背面パネル

背面パネルの各部名称について説明します。
接地コネクタ、電源コネクタ、電源抜け防止クリップ挿入口、セキュリティスロットが配備されています。

DXS-1210-28ST / DXS-1210-28S

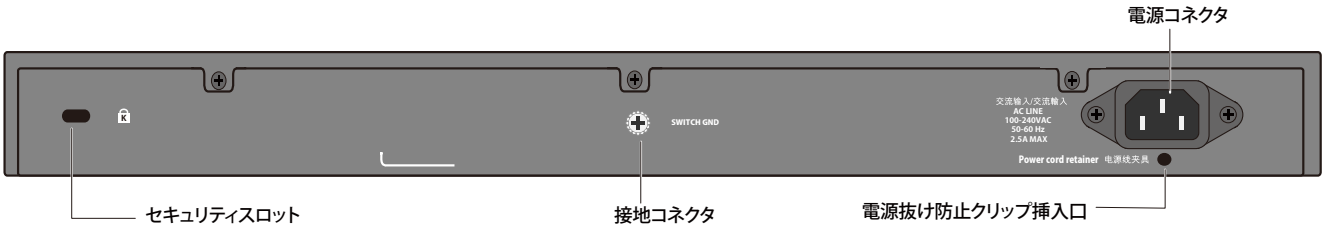


図 1-4　DXS-1210-28T/28S 背面パネル

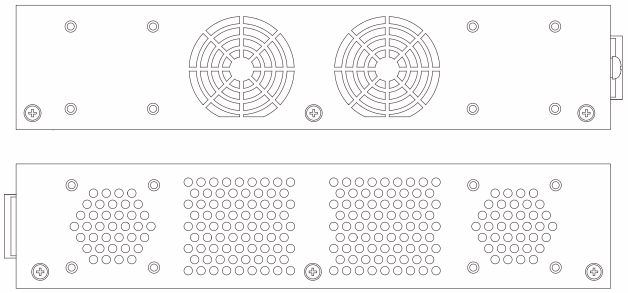
AC 電源コネクタは標準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ～ 240VAC 内の電圧に調整されます。

側面パネル

側面パネルには、通気口、ファン、ラック取り付けネジ穴などがあります。

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

DXS-1210-28T 側面パネル



DXS-1210-28S 側面パネル

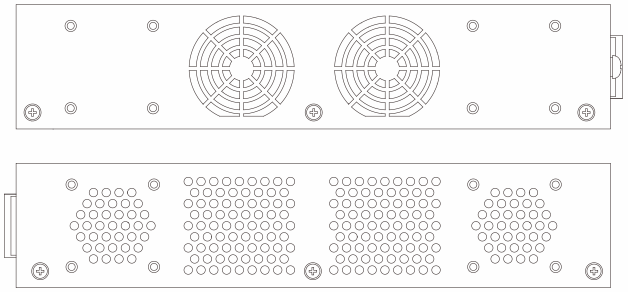


図 1-5　DXS-1210-28T/28S 側面パネル

スマートファンについて

DXS-1210-28T/28S 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。スピードには「低スピード回転」と「高スピード回転」の 2 つの状態があります。
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-1210-28T
内部温度が 33℃より高温になった場合、ファンは「高スピード回転」に移行します。
内部温度が 28℃より低温になった場合、ファンは「低スピード回転」に移行します。

DXS-1210-28S
内部温度が 31℃より高温になった場合、ファンは「高スピード回転」に移行します。
内部温度が 26℃より低温になった場合、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
- 光トランシーバの接続
- 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
- AC 電源ケーブル（100V 用）　x　1
- RJ-45/RS-232C コンソールケーブル　x　1
- 19 インチラックマウントキット 1 式
- 電源抜け防止クリップ　x　1
- ゴム足　x　4
- マニュアル　x　1
- PL シート　x　1
- GPL Code Statement　x　1

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

ネットワーク接続前の準備

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

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

ゴム足の取り付け（19 インチラックに設置しない場合）

机や棚の上に設置する場合は、まずスイッチに同梱されてい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。

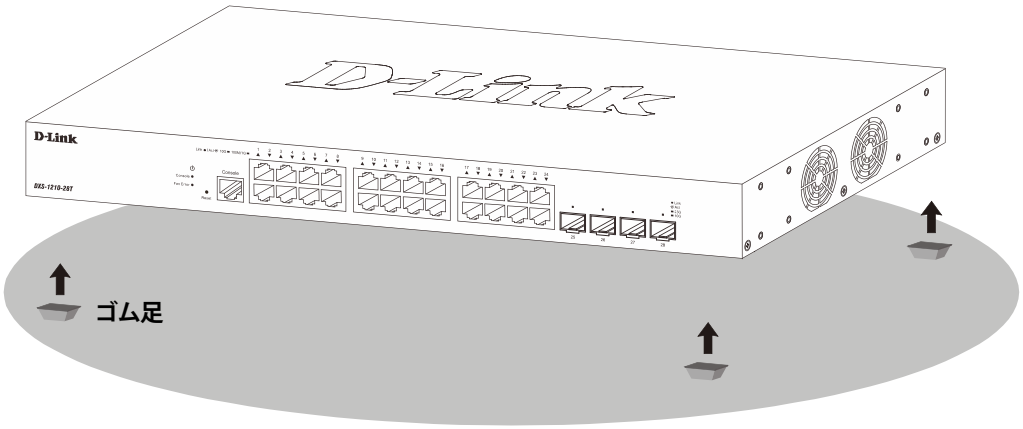


図 2-1　　机や棚の上に設置する場合の準備（DXS-1210-28T）

19 インチラックへの取り付け

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

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

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

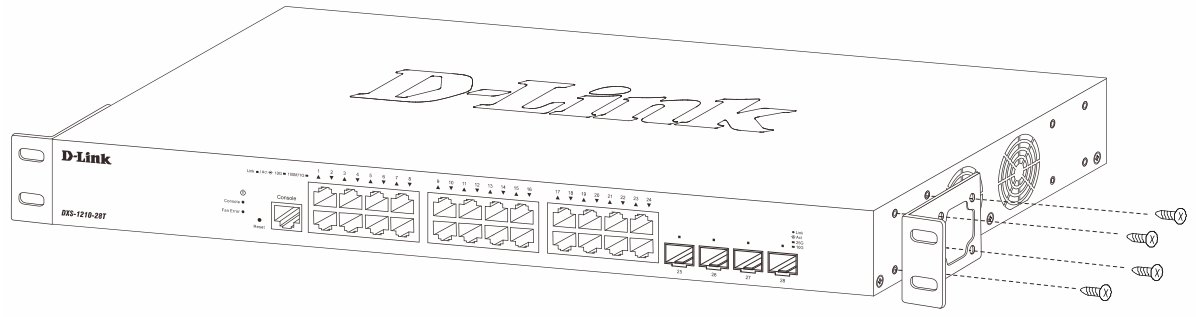


図 2-2　ブラケットの取り付け

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

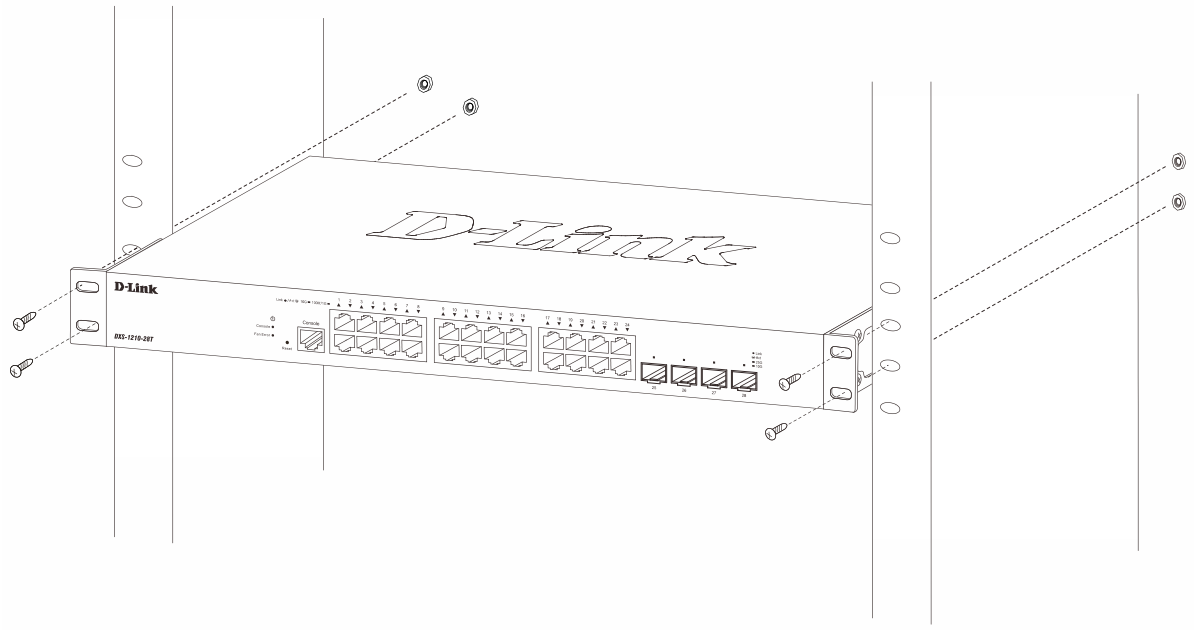


図 2-3　19 インチラックへの設置

光トランシーバの接続

DXS-1210-28S には SFP+ スロット、DXS-1210-28T には SFP28 ポートが搭載されており、光トランシーバを接続できます。

■ SFP+ スロットに光トランシーバを挿入

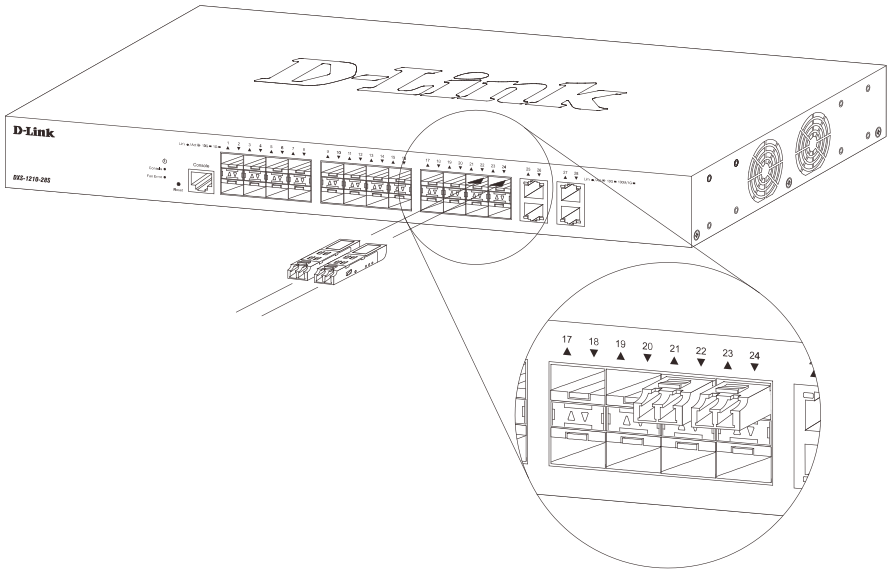


図 2-4　SFP+ スロットにモジュールを挿入（DXS-1210-28S）

■ SFP28 スロットに光トランシーバを挿入

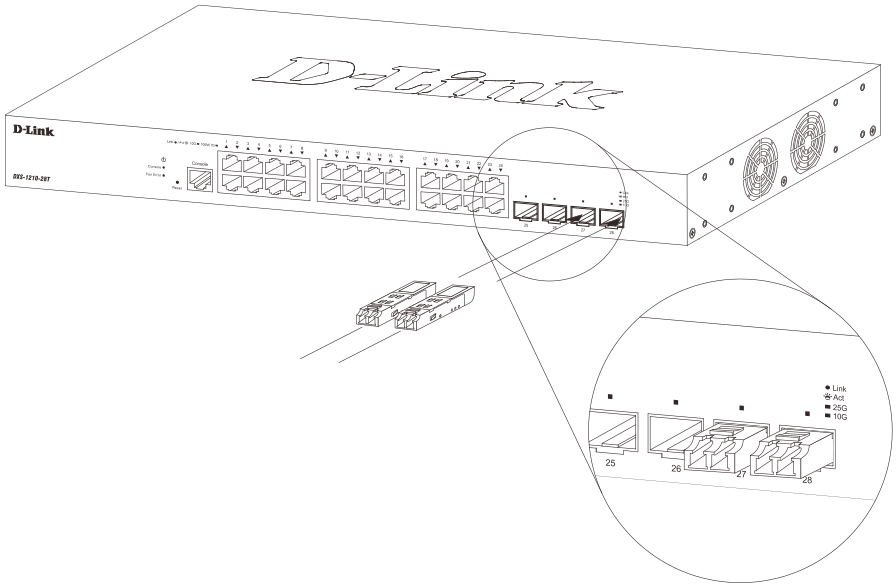


図 2-5　SFP28 スロットに光トランシーバを挿入（DXS-1210-28T）

注意　サポートしている光トランシーバについては、「SFP について」を参照してください。

注意　25G SFP28 スロットでは FEC 機能をサポートしていません。
DXS-1210-28T と DXS-1210 シリーズ以外のスイッチを接続した際に、25G bps SFP28 で接続が確立できない場合は、他のスイッチの FEC 機能を無効にしてください。

注意　光トランシーバ及びダイレクトアタッチケーブルは、クラス 1 レーザ製品に該当するものをご使用ください。

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。

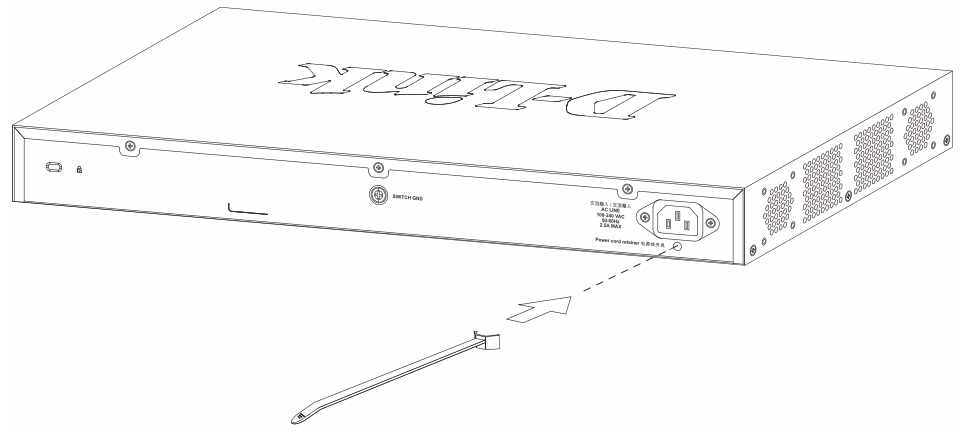


図 2-6　タイラップの挿し込み

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。

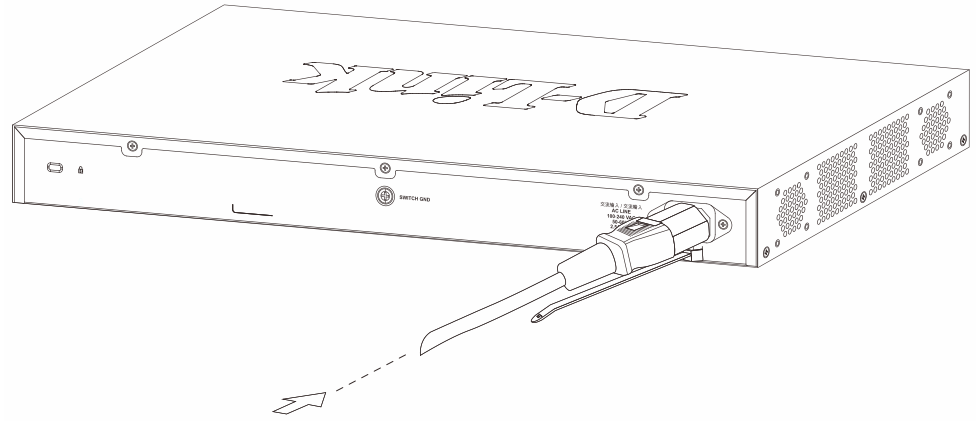


図 2-7　電源コード挿し込み

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。

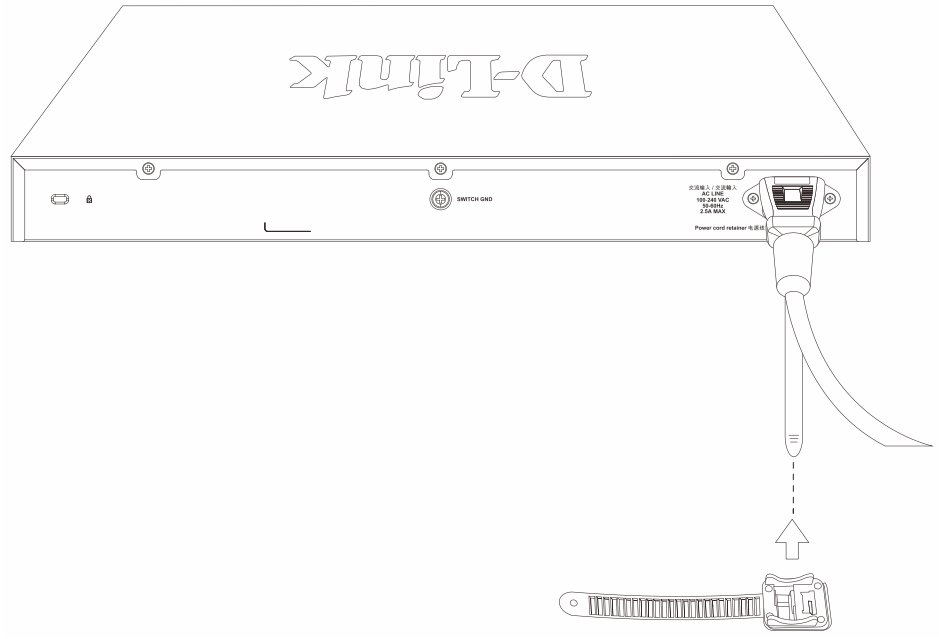


図 2-8　リテイナー（固定具）のスライド

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。

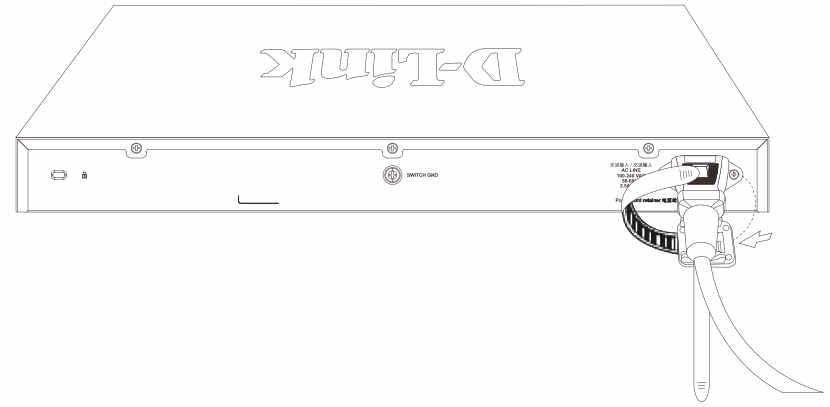


図 2-9　　リテイナーの巻き付け、固定

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

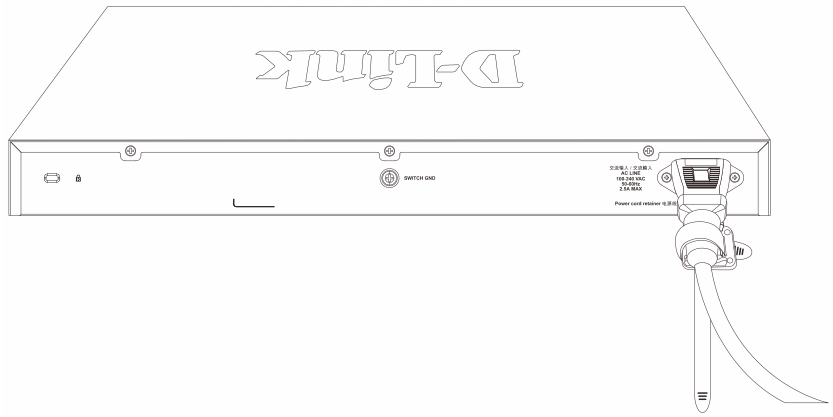


図 2-10　電源抜け防止クリップの固定確認

スイッチの接地

本スイッチを接地する方法について説明します。

注意　スイッチの電源をオンにする前に、本手順を完了する必要があります。

接地に必要なツールと機器

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

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

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

以下の手順でスイッチを保安用接地に接続します。

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

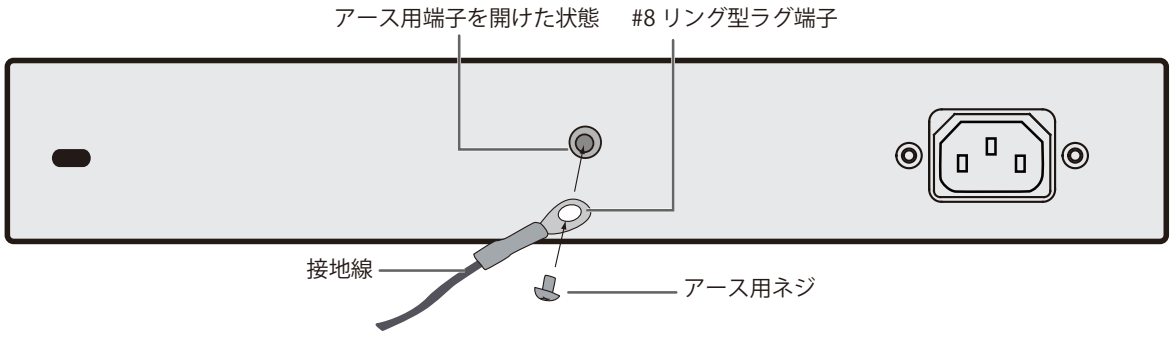


図 2-11　スイッチへのラグ端子の接続

電源の投入

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

電源の異常

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

第 3 章　スイッチの接続

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

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 DXS-1210-28T/28S とエンドノードを接続します。エンドノードとは、RJ45 ネットワークポートを装備した PC やルータの総称です。接続が正常に確立されると、対応するポートライトが点灯・点滅し、そのポートでデータの送受信が行われていることを示します。

下図は、本装置に接続されている一般的なエンドノードを示しています。

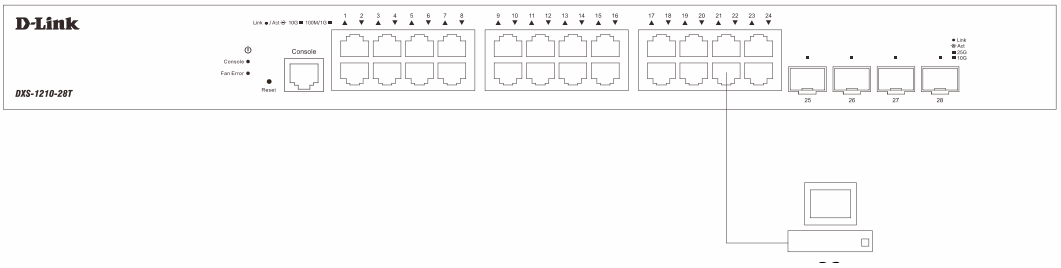


図 3-1　エンドノードとの接続図

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

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- カテゴリ 5 の UTP/STP ケーブル : 100BASE-TX スイッチポートと接続します。
- カテゴリ 5e の UTP/STP ケーブル : 1000BASE-T スイッチポートと接続します。
- カテゴリ 6/6a/7 の UTP/STP ケーブル : 10GBASE-T スイッチポートと接続します。
- 光ファイバケーブル : SFP+/SFP28 ポート経由で光ファイバをサポートするスイッチにアップリンクします。

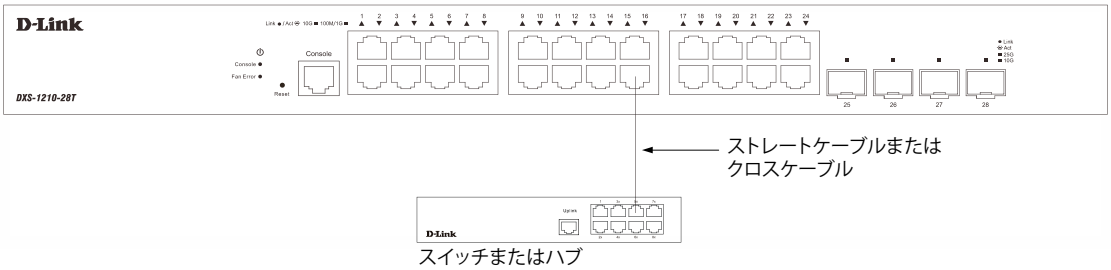
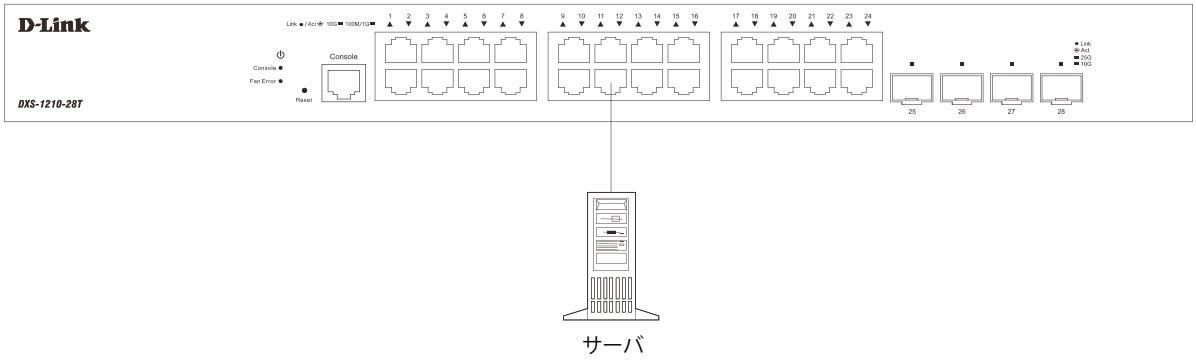


図 3-2　ハブまたはスイッチとの接続図

バックボーンまたはサーバと接続する

DXS-1210-28T/28S は、ネットワークバックボーン、サーバ、サーバファームへ接続できます。
各ポートは以下の速度で動作します。

- RJ45 ポート：100Mbps および 1/10Gbps
- SFP+ スロット：1/10Gbps
- SFP28 スロット：10/25Gbps



サーバ

図 3-3　サーバとの接続図

第 4 章　スイッチ管理について

- Web GUI による管理
- SNMP による管理
- CLI による管理
- コンソールポートの接続

Web GUI による管理

本スイッチの設置完了後、Microsoft® Internet Explorer（バージョン 11 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。

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

SNMP による管理

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

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

CLI による管理

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

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

コンソールポートの接続

スイッチのモニタリングと設定のために、RJ-45 コンソールポートを搭載しています。コンソールポートを使用するためには、以下をご用意ください。
- ターミナルソフトを操作するシリアルポート搭載の端末またはコンピュータ
- 同梱の RJ-45/RS-232C 変換ケーブル

端末をコンソールポートに接続する

ケーブルの接続

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

ターミナルソフトの設定

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

ログインとログアウト

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

注意　パスワードの大文字と小文字は区別されます。

4. コマンドを入力し、必要な設定を行います。

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

ユーザアカウント / パスワードの設定

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

注意 工場出荷時のユーザアカウントおよびパスワードは「admin」です。
はじめてログインした際は、本スイッチに対する不正アクセスを防ぐために、ユーザ名に対して必ず新しいパスワードを設定してください。
このパスワードは忘れないように記録しておいてください。

```
Switch# configure terminal
Switch(config)# username NewUser password 12345
Switch(config)#
```

1. 「configure terminal」コマンドを入力し、Global Configuration モードにアクセスします。
2. 「username NewUser password 12345」コマンドを入力し、ユーザ名「NewUser」、パスワード「12345」を指定します。

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

注意 CLI の設定コマンドは実行中の設定ファイルの編集でありスイッチが再起動した場合、設定は保存されません。
設定内容変更の安全な保存については、「copy running-config startup-config」コマンドを使用して、実行中の設定ファイルをスタート時の設定ファイルとしてコピーする必要があります。詳しくは DXS-1210-28T/28S の CLI マニュアルを参照してください。

注意 既定のアカウント「admin」は削除できません。

IP アドレスの設定

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

- IP アドレスの初期値：10.90.90.90/8

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

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

第 5 章　Web ベースのスイッチ管理

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

Web マネージャへのログイン

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

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。

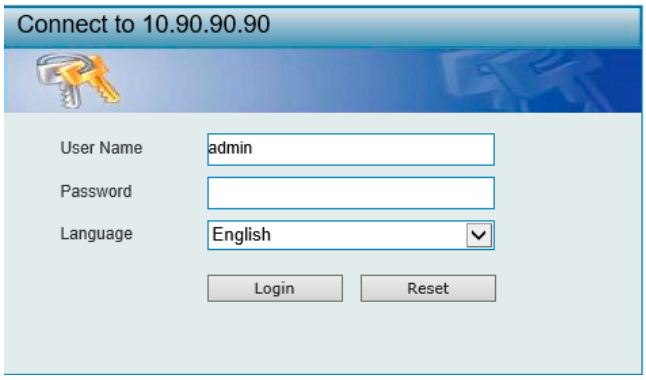


図 5-2　ユーザ認証画面

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

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

補足　入力値は ASCII 文字のみをサポートします。

注意　英語以外の言語で Web GUI を使用する場合は、**Tools > Language Management** 画面で言語ファイルを再インストールしてください。

4. スマートウィザード画面が表示されます。

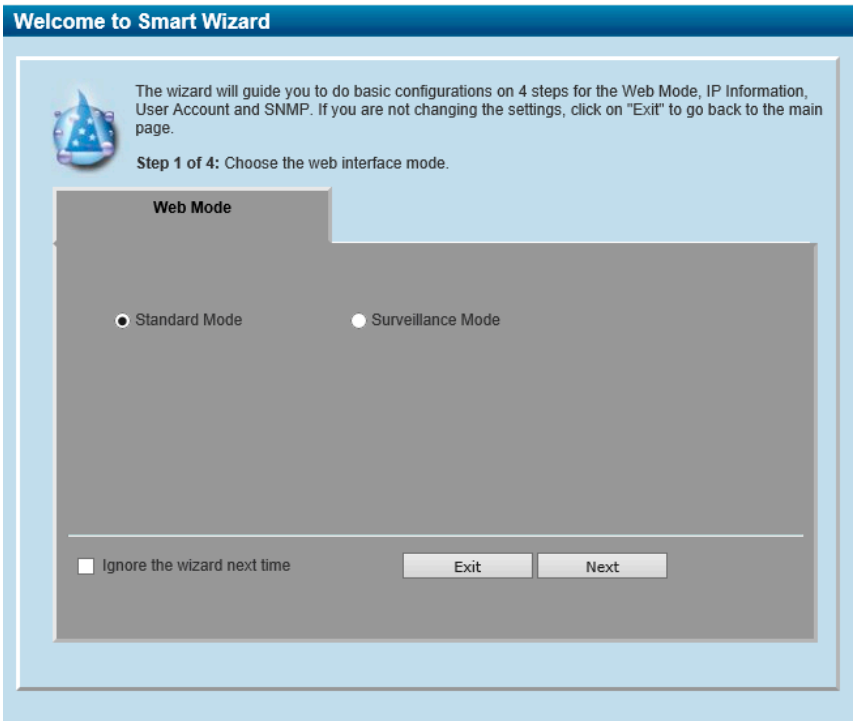


図 5-3　Smart Wizard 画面

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

5. ウィザードを使用しない場合は、「Exit」をクリックします。

Smart Wizard 設定

「Smart Wizard」で Web モードの選択や基本的なシステム設定（IP アドレス、パスワード、SNMP）を行います。

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

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

Web モードの選択（Smart Wizard）

本スイッチは「Standard Mode」（スタンダードモード）と「Surveillance Mode」（サーベイランスモード）をサポートしています。
スタンダードモードではソフトウェア機能の設定、管理、機能のモニタリングなどを行います。
サーベイランスモードは本スイッチでサポートしている監視機能に関する設定に特化したモードです。

注意　Web モードの変更は Web GUI へのログインが 1 ユーザの場合にのみ可能です。

1. Web モードを選択します。

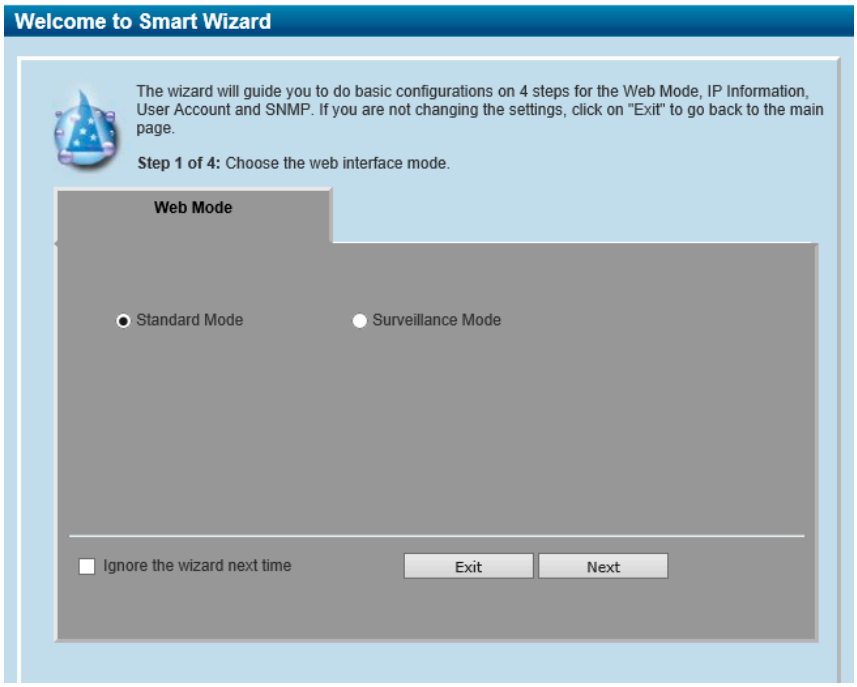


図 5-4　Web モード選択

1. 「Standard Mode」（スタンダードモード）または「Surveillance Mode」（サーベイランスモード）を選択します。
2. 「Next」をクリックします。

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

IP アドレスの設定（Smart Wizard）

2. IP アドレスの設定を行います。

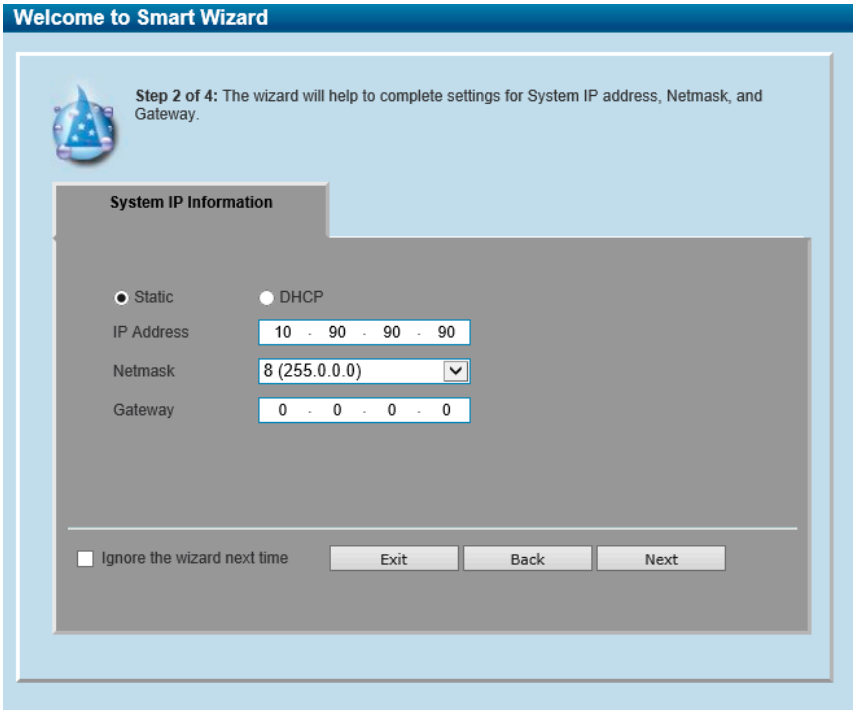


図 5-5　IP Information 設定画面

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

   「Static」を選択した場合は、「IP Address」「Netmask」「Gateway」を入力します。
   IPv4 アドレスのみ設定可能です。

2. 「Next」をクリックします。

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

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。

注意　スイッチはサーベイランスデバイスの確認を 30 秒毎で行います。サーベイランスデバイスがスイッチと同じサブネットにない場合、自動的に検出はされません。ONVIF カメラなどサーベイランス機器をサーベイランスモード Web GUI に自動的に追加するためには、スイッチ管理 IP アドレスをそれらの機器と同じサブネットにする必要があります。

ユーザアカウントの設定（Smart Wizard）

3. ユーザアカウントの設定を行います。

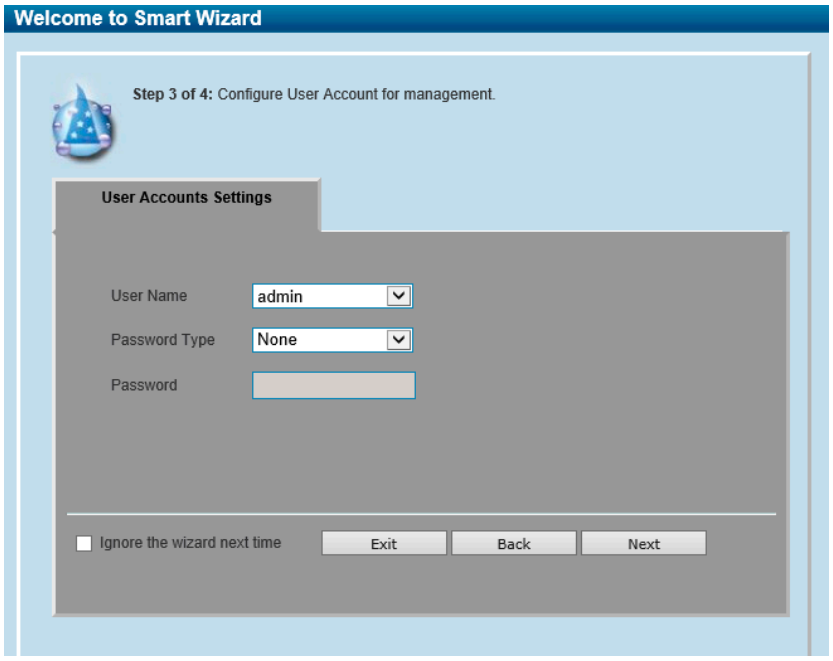


図 5-6　ユーザアカウント設定画面

画面に表示される項目：

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。
Password Type	パスワードタイプを指定します。 • 「None」- ユーザアカウントにパスワードを指定しません。 • 「Plain Text 」- プレーンテキストでパスワードを指定します。
Password	パスワードの種類で「Plain Text」をした場合に、ユーザアカウントのパスワードを入力します。

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

SNMP の設定（Smart Wizard）

4. SNMP の設定を行います。

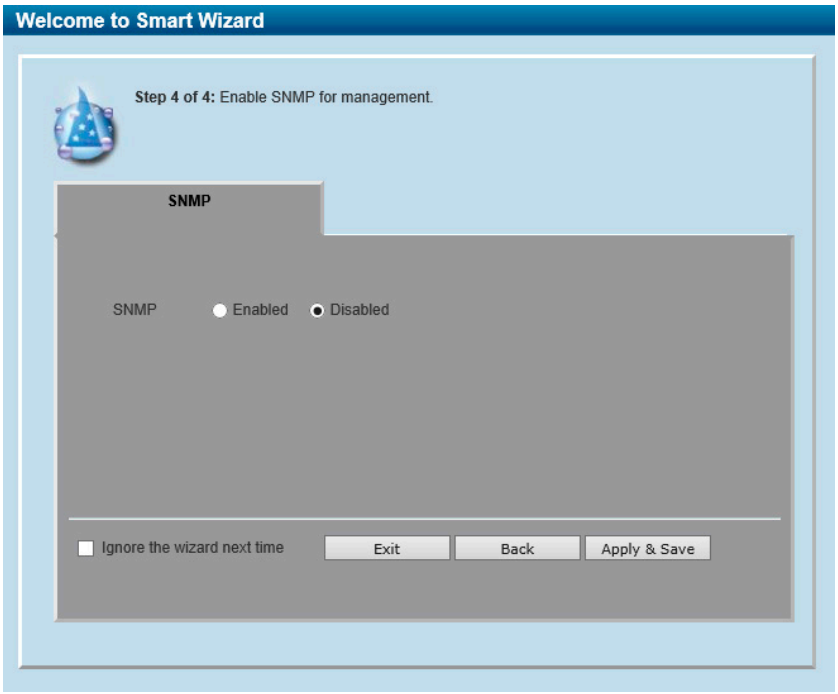


図 5-7　SNMP 設定画面

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

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

Web ベースのユーザインタフェース

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

ユーザインタフェース内の各エリア（スタンダードモード）

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。

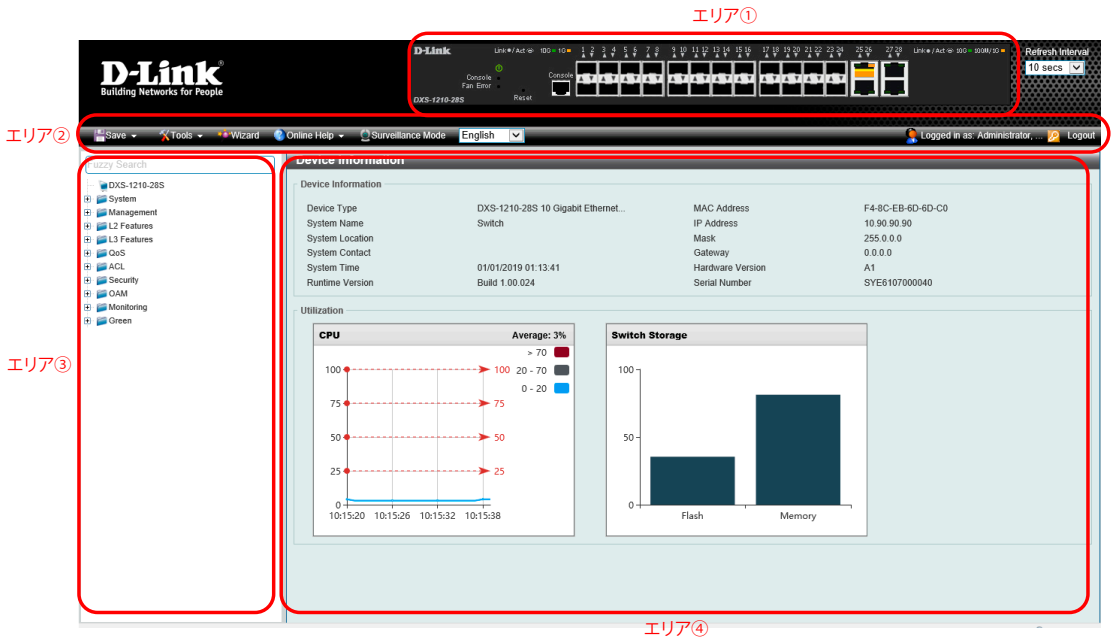


図 5-8　Device Information 画面

エリア	説明
エリア①	本エリアではスイッチの前面パネルの状態がほぼリアルタイムにグラフィカル表示されます。 スイッチのポート、拡張モジュールが表示されます。ポートモニタなどの管理機能はここからアクセスする事も可能です。 「D-Link」ロゴをクリックすると D-Link Web サイト（英語）へ移動します。
エリア②	スイッチの再起動、コンフィグレーションのバックアップとリストア、ファームウェアの更新、サーベイランスモードへの移行、設定の初期化などを行う「Tool」メニューと、設定の保存を行う「Save」メニューがあります。 ツールバーの右側には、現在接続中のユーザ名とスイッチの IP アドレス、ログアウトボタンが表示されます。
エリア③	Web GUI を使用して設定可能な機能のツリービューが表示されます。ツリー項目をクリックして各機能の設定画面に移動します。製品名をクリックすると、デバイス情報画面が表示されます。 また、メニュー項目をキーワードで検索するための検索フィールドも用意されています。
エリア④	エリア③のツリービューで選択した各機能の設定画面が表示されます。

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

補足　Web GUI を表示するための最適な画面解像度は、1280 x 1024 ピクセルです。

ユーザインタフェース内の各エリア（サーベイランスモード）

サーベイランスモードで Web GUI にアクセスした場合は、以下の画面が表示されます。

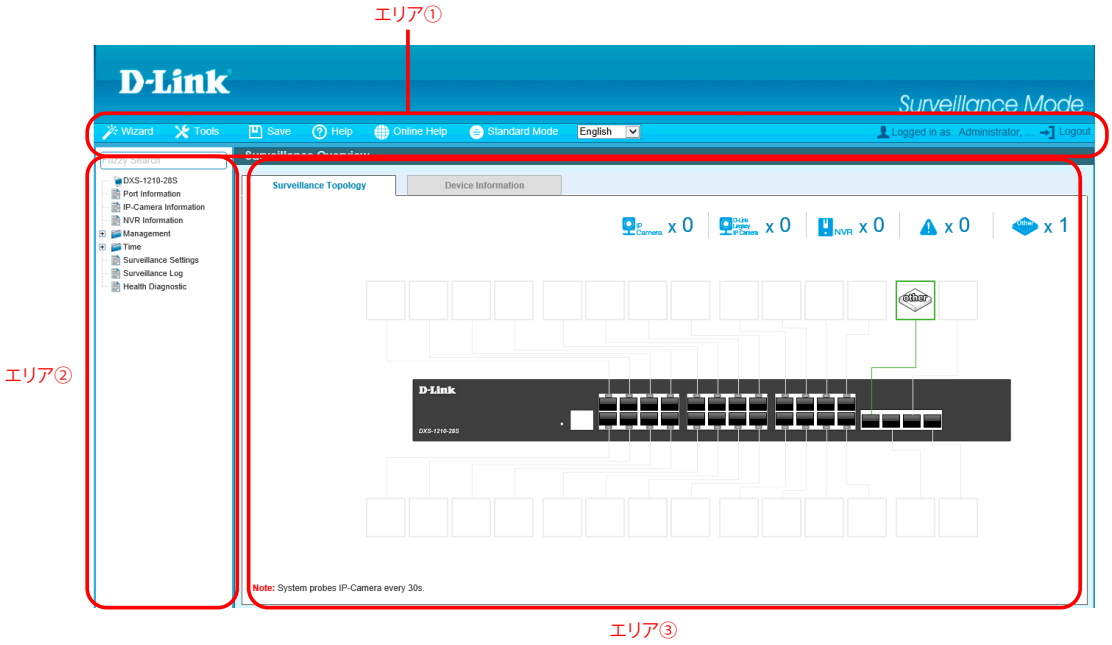


図 5-9　サーベイランスモード初期画面

エリア	説明
エリア①	スイッチの再起動、コンフィグレーションのバックアップとリストア、ファームウェアの更新、スタンダードモードへの移行、設定の初期化などを行う「Tool」メニューと設定の保存を行う「Save」メニューがあります。 ツールバーの右側には、現在接続中のユーザ名とスイッチの IP アドレス、ログアウトボタンが表示されます。
エリア②	サーベイランスモードで設定可能な機能のツリービューが表示されます。 ツリー項目をクリックして各機能の設定画面に移動します。また、メニュー項目をキーワードで検索するための検索フィールドも用意されています。
エリア③	エリア②のツリービューで選択した各機能の設定画面が表示されます。

Web マネージャのメニュー構成

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

メイン メニュー	サブメニュー	説明
System	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。
	Interface Description	各ポートのステータス、管理ステータスや概要を表示します。
	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。
	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。
	Telnet / Web	スイッチに Telnet 設定と 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。
	DHCP	スイッチの DHCP リレーサービスについて設定します。
	DHCP Auto Configuration	DHCP 自動設定機能の設定を行います。
	DHCP Auto Image Settings	DHCP 自動イメージ機能の設定を行います。
	DNS	スイッチの DNS サービスについて設定します。
	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	ARP	ARP の設定、編集を行います。
	Gratuitous ARP	Gratuitous ARP の設定、編集を行います。
	IPv6 Neighbor	IPv6 ネイバの設定を行います。
	Interface	IPv4/IPv6 アドレスのインタフェースの設定を行います。
	IPv4 Static/Default Route	IPv4 アドレスのスタティック / 初期ルートの設定を行います。
	IPv4 Route Table	IPv4 のルートテーブルの設定を行います。
	IPv6 Static/Default Route	IPv6 アドレスのスタティック / 初期ルートの設定を行います。
	IPv6 Route Table	IPv6 のルートテーブルの設定を行います。
	IP Multicast Routing Protocol	IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）の設定を行います。
QoS	Basic Settings	QoS の基本設定を行います。
	Advanced Settings	QoS の詳細設定を行います。
ACL	ACL Configuration Wizard	ウィザードを使用してアクセスプロファイルとルールを作成します。
	ACL Access List	ACL アクセスリストの設定をします。
	ACL Interface Access Group	ACL インタフェースアクセスグループの設定を行います。

メイン メニュー	サブメニュー	説明
Security	Port Security	ポートセキュリティの設定を行います。
	802.1X	802.1X 認証設定を行います。
	AAA	AAA の設定を行います。
	RADIUS	RADIUS の設定を行います。
	IMPB	IP-MAC ポートバインディングの設定を行います。
	DHCP Server Screening	DHCP サーバスクリーニングの設定を行います。
	ARP Spoofing Prevention	ARP スプーフィング防止設定を行います。
	Network Access Authentication	ネットワークアクセス認証設定を行います。
	Safeguard Engine	セーフガードエンジン設定を行います。
	Trusted Host	トラストホスト設定を行います。
	Traffic Segmentation Settings	トラフィックセグメンテーション設定を行います。
	Storm Control Settings	ストームコントロールの設定を行います。
	DoS Attack Prevention Settings	DoS 攻撃防止設定を行います。
	SSH	SSH（Secure Shell）の設定を行います。
	SSL	SSL（Secure Socket Layer）の設定を行います。
	Network Protocol Port Protect Settings	TCP/UDP ポートのネットワークプロトコルポート保護設定を行います。
OAM	Cable Diagnostics	ケーブル診断を行います。
Monitoring	Utilization	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。
Toolbar	Save	コンフィグレーションの保存などを行います。
	Tools	ファームウェアアップグレードやバックアップ、コンフィグレーションのリストア、バックアップなどを行います。
	Wizard	スマートウィザードを開始します。
	Online Help	D-Link のサポート Web サイト（英語）/ またはユーザガイド（英語版）を表示します。インターネット接続が必要です。
	Surveillance Mode	Web モードをスタンダードモードからサーベイランスモードに移行します。
	Logout	Web GUI からログアウトします。

第 6 章　System（システム設定）

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

サブメニュー	説明
Device Information（デバイス情報）	スイッチの主な設定情報を表示します。
System Information Settings（システム情報）	スイッチの基本情報を表示します。
Peripheral Settings（環境設定）	スイッチの環境設定を行います。
Port Configuration（ポート設定）	ポート設定、ジャンボフレーム設定などを行います。
Interface Description（インタフェース概要）	各ポートのステータス、管理ステータスや概要を表示します。
System Log（システムログ）	システムログの設定を行います。
Time and SNTP（時刻・SNTP 設定）	スイッチに時刻を設定します。
Time Range（タイムレンジ設定）	スイッチの ACL 機能などで使用するスケジュールを定義します。

Device Information（デバイス情報）

ログイン時に自動的に表示されるスイッチの主な機能の設定内容です。
他の画面から「Device Information」画面に戻る場合は、製品名（DXS-1210-28T、DXS-1210-28S）をクリックします。
「Device Information」画面にはデバイスの一般的な情報（システム名、場所、システム MAC アドレス、システム時刻、IP アドレス、ファームウェア、およびハードウェアのバージョン情報など）が表示されます。

ツリービューの製品名（DXS-1210-28T、DXS-1210-28S）をクリックし、以下の画面を表示します。

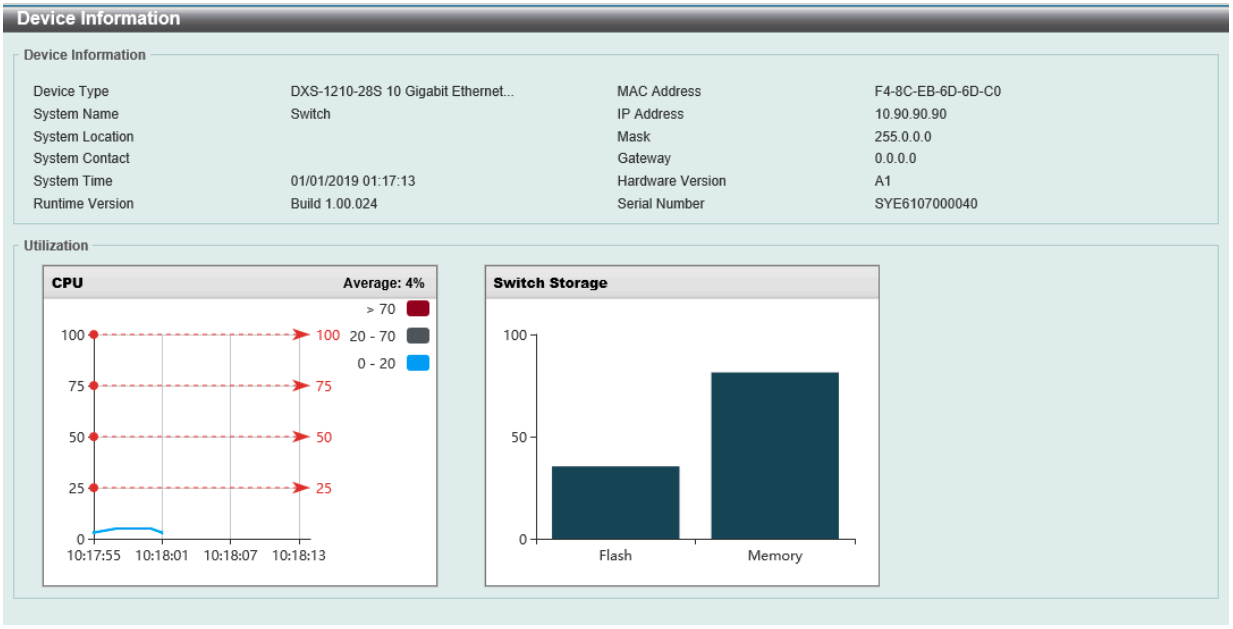


図 6-1　Device Information 画面

「Device Information」画面に表示される項目：

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

System Information Settings（システム情報）

システム情報設定画面では、システム情報の設定を行います。

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

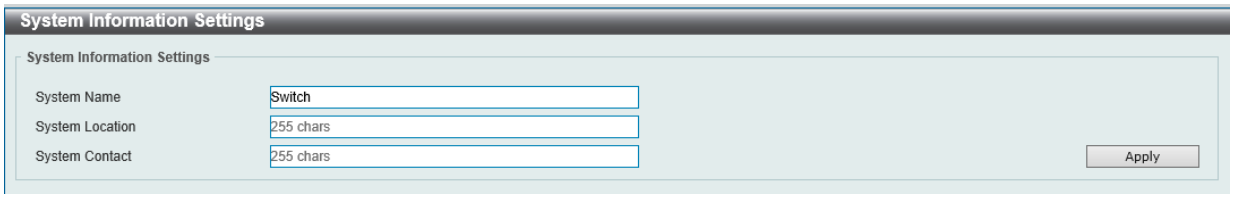


図 6-2　System Information Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

Peripheral Settings（環境設定）

システムの警告温度や環境トラップの設定を行います。

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

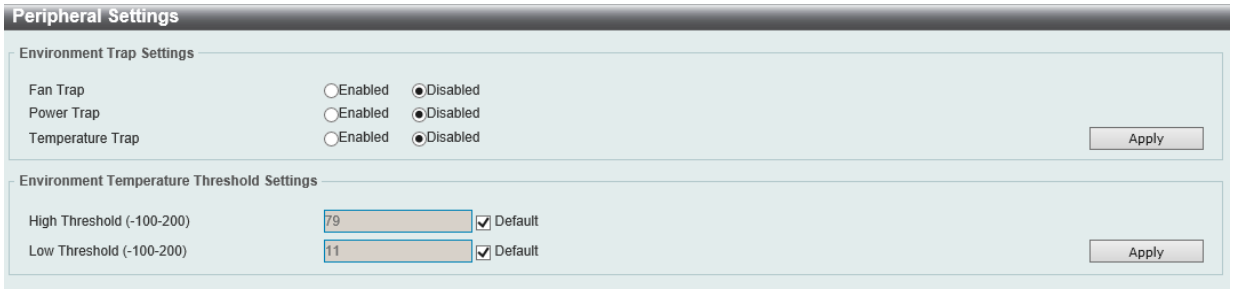


図 6-3　Peripheral Settings 画面

画面に表示される項目：

項目	説明
Environment Trap Settings	
Fan Trap	ファン警告イベント（ファンエラーまたは回復）のトラップを有効 / 無効に設定します。
Power Trap	電源警告イベント（電源エラーまたは回復）のトラップを有効 / 無効に設定します。
Temperature Trap	温度警告イベント（温度しきい値の超過または回復）のトラップを有効 / 無効に設定します。
Environment Temperature Threshold Settings	
High Threshold	高温警告しきい値を指定します。 • 設定可能範囲：「-100℃」-「200℃」 • 初期値：79℃ 「Default」をチェックすると初期値に戻ります。
Low Threshold	低温警告しきい値を指定します。 • 設定可能範囲：「-100℃」-「200℃」 • 初期値：11℃ 「Default」をチェックすると初期値に戻ります。

「Apply」をクリックして、設定内容を適用します。

Port Configuration（ポート設定）

各ポートの設定を行います。

Port Settings（ポート設定）

ポートの詳細を設定します。

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

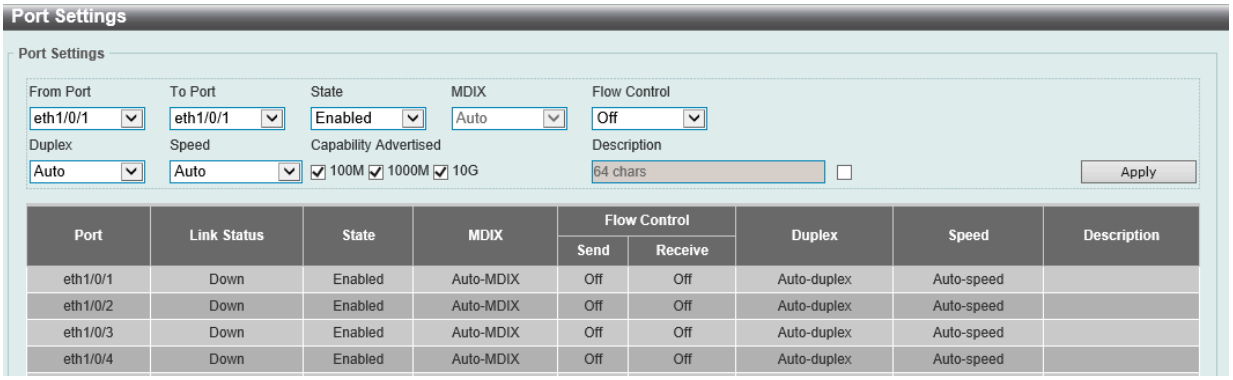


図 6-4　Port Settings (DXS-1210-28S) 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
State	物理ポートのステータスを有効 / 無効に設定します。
MDIX	MDIX の設定を以下から選択します。 • 「Auto」- 最適なケーブル接続を自動的に設定します。 • 「Normal」- 通常のケーブル接続の場合は、このオプションを選択します。このオプションを選択すると、ポートは MDIX モードになり、ストレートケーブルを使用して PC の NIC に接続するか、クロスケーブルを介して別のスイッチのポート（MDI モード）に接続できます。 • 「Cross」- ポートは MDI モードとなり、ストレートケーブルで別のスイッチのポート (MDIX モード) に接続することができます。
Flow Control	「On」（フロー制御あり）または「Off」（フロー制御なし）を選択します。 Full-Duplex のポートでは 802.3x フローコントロールによる制御を行います。「Auto」のポートは自動的にいずれかを使用します。
Duplex	Duplex モードの設定を以下から選択します。半二重モードはサポートされていません • 「Auto」「Full」
Speed	ポートの速度を選択します。 選択肢： • 「Auto」- Copper ポートの場合、オートネゴシエーションを開始してリンクパートナーと速度、フローコントロールの調整を行います。光ファイバポートの場合、オートネゴシエーションを開始してリンクパートナーとクロック、フローコントロールの調整を行います • 「100M」- ポート速度を 100Mbps に指定します。このオプションは、100Mbps の Copper 接続でのみ使用できます。 • 「1000M」- ポート速度を 1 Gbps に指定します。 • 「10G」- ポート速度を 10 Gbps に指定します。 • 「25G」- ポート速度を 25 Gbps に指定します。 注意　DXS-1210-28T の場合、ポート 25 - 28 は同じ速度で動作する必要があります。
Capability Advertised	「Speed」を「Auto」に設定した場合、指定した項目がオートネゴシエーションの間にアドバタイズされます。
Description	ポートの説明を入力します。（64 文字以内）

「Apply」をクリックして、設定内容を適用します。

注意　25G SFP28 スロットでは FEC 機能をサポートしていません。
DXS-1210-28T と DXS-1210 シリーズ以外のスイッチを接続した際に、25G bps SFP28 で接続が確立できない場合は、他のスイッチの FEC 機能を無効にしてください。

注意　DXS-1210-28T/28S は、オートネゴシエーションのみサポートしています。以下の場合はリンクアップしません。
・対向がオートセンシングのみ場合（速度固定を含む）
・対向がオートネゴシエーションで Half-Duplex のみをアドバタイズする場合

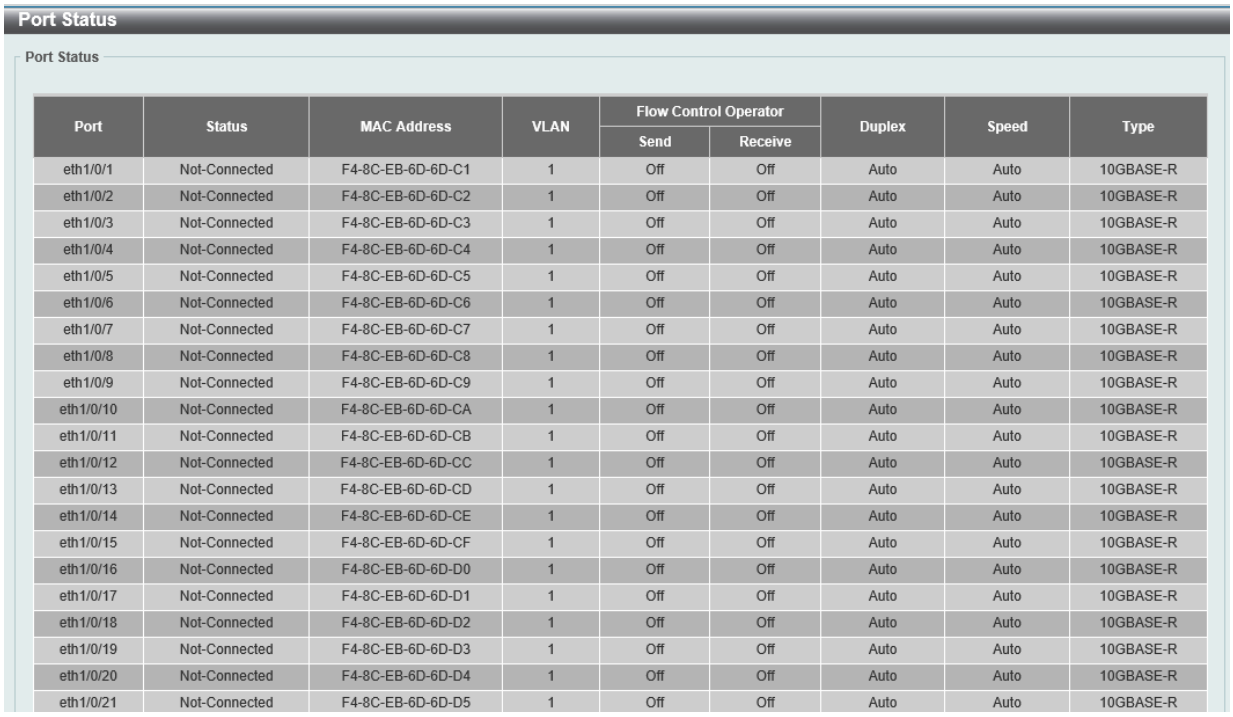
注意　DXS-1210-28T/28S は、10Mbps をサポートしていません。

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

Port Status（ポートステータス）

ポートの状態、設定について表示します。

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



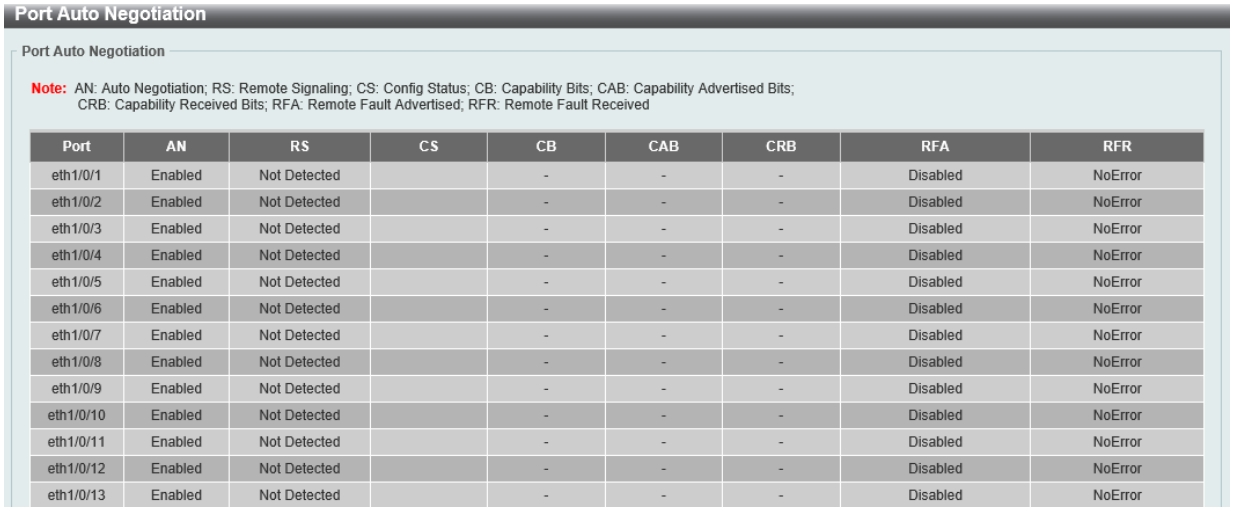
Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	Not-Connected	F4-8C-EB-6D-6D-C1	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/2	Not-Connected	F4-8C-EB-6D-6D-C2	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/3	Not-Connected	F4-8C-EB-6D-6D-C3	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/4	Not-Connected	F4-8C-EB-6D-6D-C4	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/5	Not-Connected	F4-8C-EB-6D-6D-C5	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/6	Not-Connected	F4-8C-EB-6D-6D-C6	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/7	Not-Connected	F4-8C-EB-6D-6D-C7	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/8	Not-Connected	F4-8C-EB-6D-6D-C8	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/9	Not-Connected	F4-8C-EB-6D-6D-C9	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/10	Not-Connected	F4-8C-EB-6D-6D-CA	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/11	Not-Connected	F4-8C-EB-6D-6D-CB	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/12	Not-Connected	F4-8C-EB-6D-6D-CC	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/13	Not-Connected	F4-8C-EB-6D-6D-CD	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/14	Not-Connected	F4-8C-EB-6D-6D-CE	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/15	Not-Connected	F4-8C-EB-6D-6D-CF	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/16	Not-Connected	F4-8C-EB-6D-6D-D0	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/17	Not-Connected	F4-8C-EB-6D-6D-D1	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/18	Not-Connected	F4-8C-EB-6D-6D-D2	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/19	Not-Connected	F4-8C-EB-6D-6D-D3	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/20	Not-Connected	F4-8C-EB-6D-6D-D4	1	Off	Off	Auto	Auto	10GBASE-R
eth1/0/21	Not-Connected	F4-8C-EB-6D-6D-D5	1	Off	Off	Auto	Auto	10GBASE-R

図 6-5　Port Status 画面

Port Auto Negotiation（ポートオートネゴシエーション）

オートネゴシエーションの詳細情報を表示します。

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



Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
eth1/0/1	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/2	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/3	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/4	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/5	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/6	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/7	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/8	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/9	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/10	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/11	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/12	Enabled	Not Detected		-	-	-	Disabled	NoError
eth1/0/13	Enabled	Not Detected		-	-	-	Disabled	NoError

図 6-6　Port Auto Negotiation 画面

Error Disabled Settings（エラーディセーブル設定）

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

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

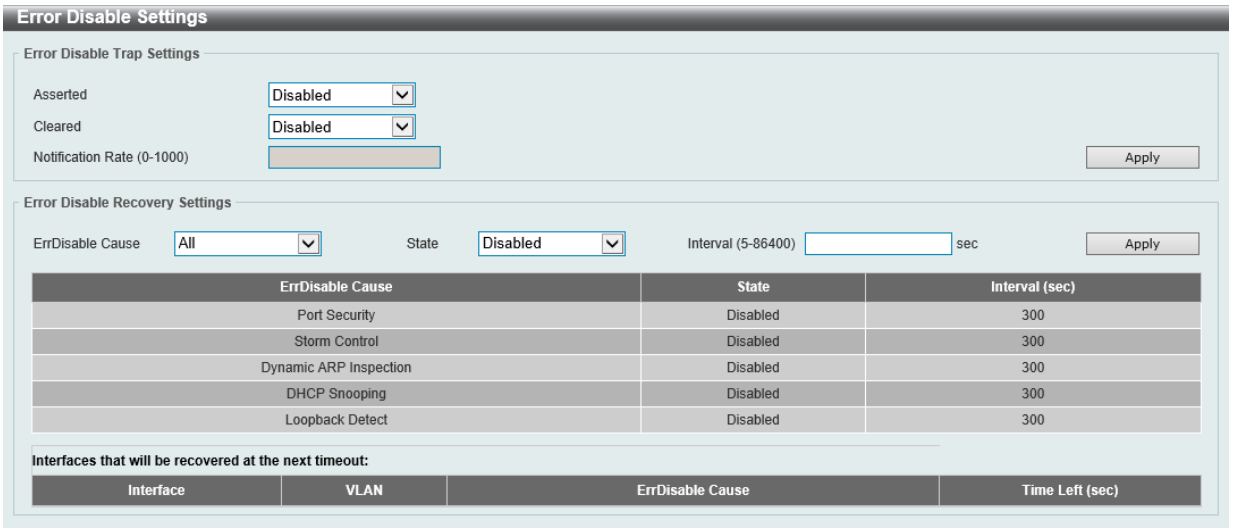


図 6-7　Error Disabled Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

Jumbo Frame（ジャンボフレーム設定）

ジャンボフレームは、1,518Byte を超えるフレームサイズを意味します。ジャンボフレームにより、同じデータを少ないフレームで転送することができます。DXS-1210-28T/28S では、最大フレームサイズが 12,288 バイトまでのジャンボフレームをサポートしています。

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

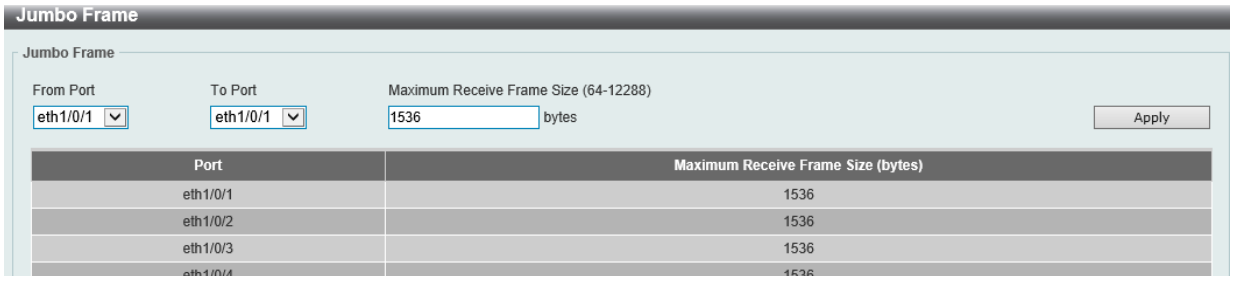


図 6-8　Jumbo Frame 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Maximum Receive Frame Size	スイッチのジャンボフレーム機能の最大値を指定します。 • 設定可能範囲：64 - 12288（bytes） • 初期値：1536（bytes）

「Apply」をクリックして、設定内容を適用します。

補足　フレームサイズには FCS（Frame Check Sequence）が含まれます。

Interface Description（インタフェース概要）

各ポートのステータス、管理ステータスや概要を表示します。

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

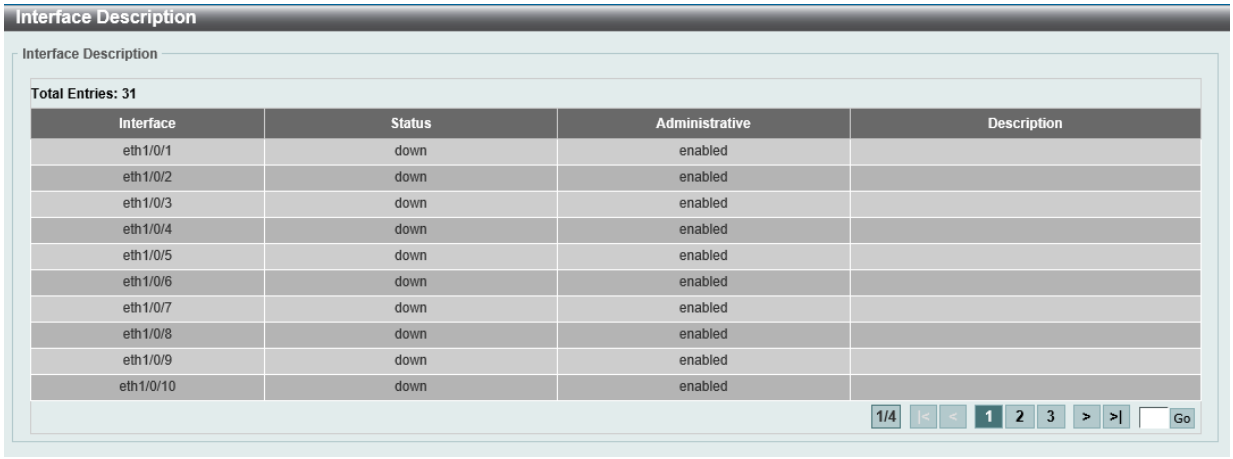


図 6-9　Interface Description 画面

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

System Log（システムログ）

システムログの設定を行います。

System Log Settings（システムログ設定）

システムログ機能のステータスや、ログの保存方法などを設定します。

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

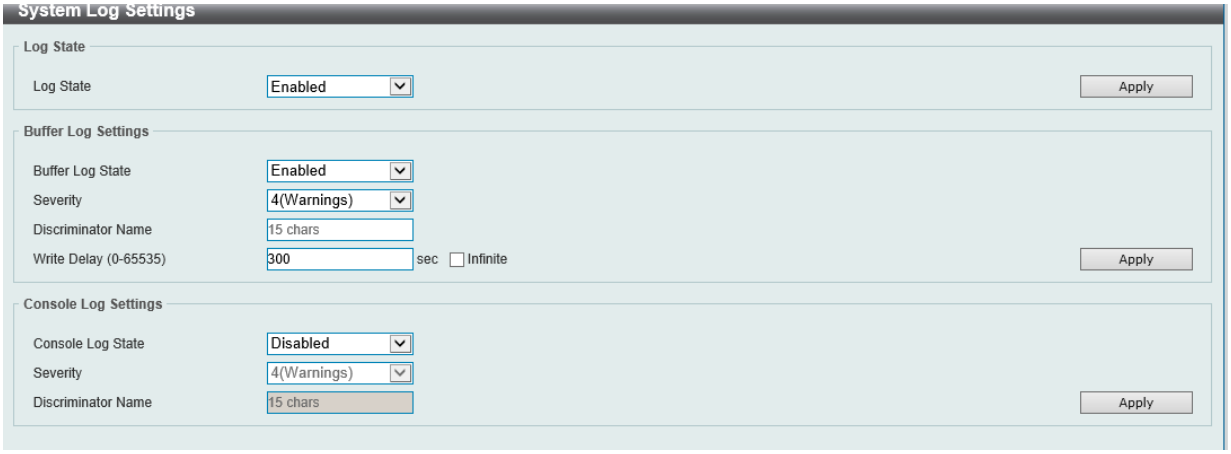


図 6-10　System Log Settings 画面

画面に表示される項目：

項目	説明
Log State	
Log State	シスログのグローバルステータスを有効 / 無効に指定します。
Buffer Log Settings	
Buffer Log State	バッファログのグローバルステータスを指定します。 • 選択肢：「Enable」「Disabled」「Default」 「Default」を選択するとバッファログのグローバルステートは初期設定のまま動作します。
Severity	ログされる情報のレベルを選択します。 • 選択肢：「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Discriminator Name	識別名を入力します。（15 文字以内）
Write Delay	フラッシュにロギングバッファを定期的に書き込む間隔を指定します。 「Infinite」にチェックを入れると本機能は無効になります。 • 設定可能範囲：0 - 65535（秒） • 初期値：300（秒）
Console Log Settings	
Console Log State	コンソールログのグローバルステータスを有効 / 無効にします。
Severity	ログされる情報のレベルを選択します。 • 選択肢：「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Discriminator Name	識別名を入力します。（15 文字以内）

「Apply」をクリックして、設定内容を適用します。

注意　Syslog が原因で定期的に CPU 負荷が 100%になる場合、「Write Delay」で「Infinite」を選択するか、60 秒など初期値より短い時間を指定してください。

System Log Discriminator Settings（システムログ識別設定）

システムログ識別名の設定、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。

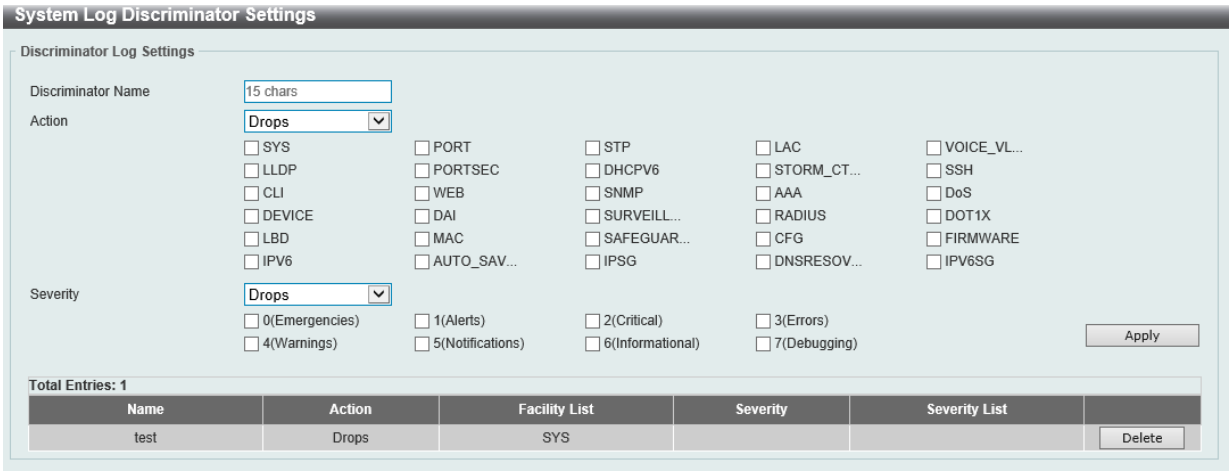


図 6-11　System Log Discriminator Settings 画面

画面に表示される項目：

項目	説明
Discriminator Name	識別名を入力します。（15 文字以内）
Action	動作を「Drops」（破棄）、「Includes」（含む）から選択します。 動作に関連づけるファシリティタイプのチェックボックスを選択します。
Severity	セベリティ（重要度）の動作を「Drops」（破棄）、「Includes」（含む）から選択します。 ログに記録される情報の種類をチェックボックスで選択します。 • 選択肢： 「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）

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

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

システムログサーバの設定を行います。

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

図 6-12　System Log Server Settings 画面

画面に表示される項目：

項目	説明
Host IPv4 Address	システムログサーバの IPv4 アドレスを設定します。
Host IPv6 Address	システムログサーバの IPv6 アドレスを設定します。
UDP Port	システムログサーバの UDP ポートを設定します。 • 設定可能範囲：514、1024 - 65535 • 初期値：514
Severity	ログ出力される情報のレベルを選択します • 選択肢： 「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）
Facility	ログ出力されるファシリティの番号を選択します。 • 設定可能範囲：0 - 23
Discriminator Name	識別名を入力します。（15 文字以内）

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

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

System Log（システムログ）

システムログの閲覧 / 消去を行います。

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

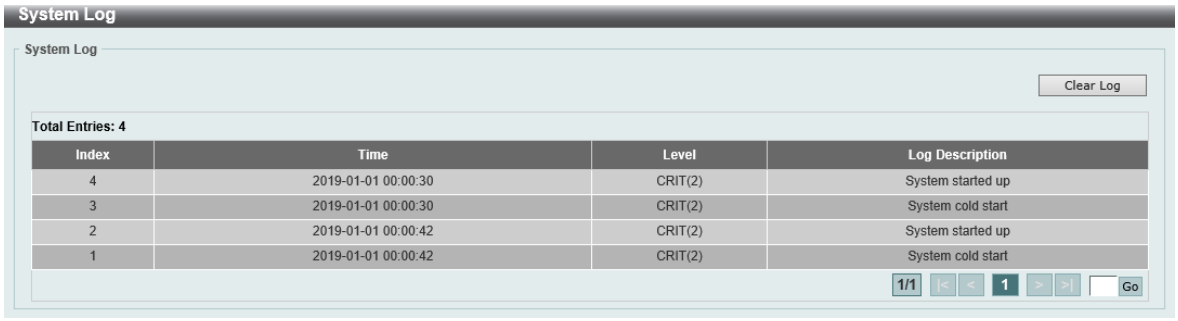


図 6-13　System Log 画面

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

System Attack Log（システム攻撃ログ）

システム攻撃ログの閲覧、消去を行います。

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

図 6-14　System Attack Log 画面

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

Time and SNTP（時刻・SNTP 設定）

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

Clock Settings（時刻設定）

スイッチの時間設定を行います。

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。

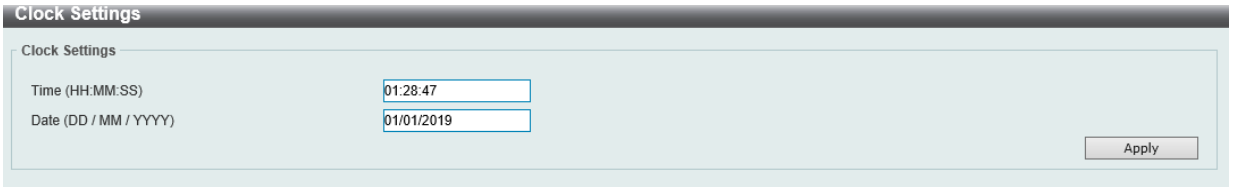


図 6-15　Clock Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

Time Zone Settings（タイムゾーン設定）

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

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

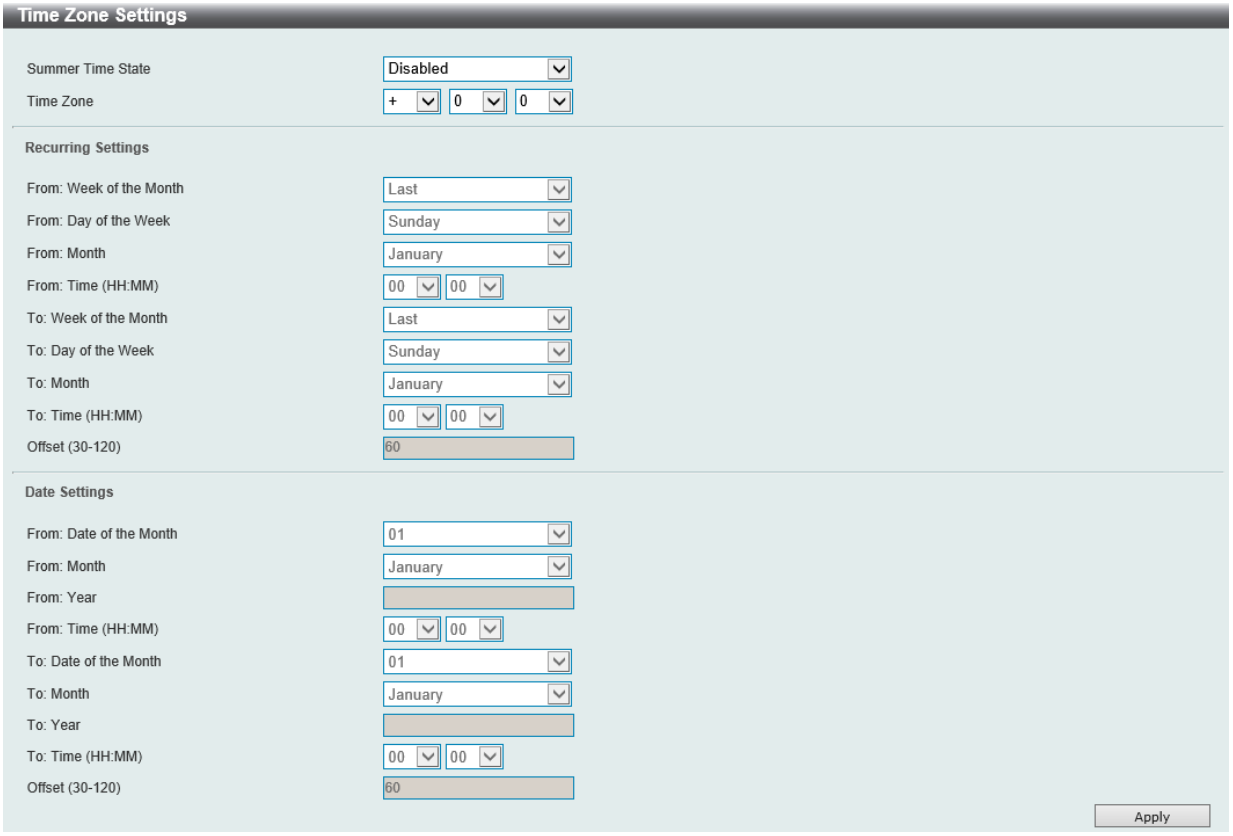


図 6-16　Time Zone Settings 画面

画面に表示される項目：

項目	説明
Summer Time State	デバイスに設定するサマータイムの種類を設定します。 • 「Disabled」- サマータイムを無効にします。（初期値） • 「Recurring Setting」- サマータイムを周期的に有効にします。このオプションでは、指定月の指定曜日にサマータイムが開始 / 終了します。 • 「Date Setting」- サマータイムを日付指定で有効にします。このオプションでは、指定年月日にサマータイムが開始 / 終了します。
Time Zone	ローカルタイムゾーンの UTC からのオフセットを指定します。
Recurring Setting	
Recurring Setting モードを使用すると、サマータイムの設定を指定した期間で自動的に調整できるようになります。 （例）サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までに指定	
From: Week of the Month	月の第何週からサマータイムを開始するかを設定します。
From: Day of the Week	サマータイムを開始する曜日を指定します。 • 選択肢：「Sun」「Mon」「Tue」「Web」「Tues」「Fri」「Sat」
From: Month	サマータイムを開始する月を指定します。 • 選択肢：「Jan」「Feb」「Mar」「Apr」「May」「Jun」「Jul」「Aug」「Sep」「Oct」「Nov」「Dec」
From: Time (HH:MM)	サマータイムを開始する時間を指定します。
To: Week of The Month	月の第何週でサマータイムが終わるかを設定します。
To: Day of the Week	サマータイムを終了する曜日を指定します。
To: Month	サマータイムを終了する月を指定します。
To: Time (HH:MM)	サマータイムを終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。 • 選択肢：「30」「60」「90」「120」（分） • 初期値：60（分）
Date Setting	
サマータイムの開始 / 終了月日を指定します。	
From: Date of the Month	サマータイムを開始する月日を指定します。
From: Month	サマータイムを開始する月を指定します。
From: Year	サマータイムを開始する年を指定します。
From: Time (HH:MM)	サマータイムを開始する時間を指定します。
To: Date of the Month	サマータイムを終了する月日を指定します。
To: Month	サマータイムを終了する月を指定します。
To: Year	サマータイムを終了する年を指定します。
To: Time (HH:MM)	サマータイムを終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。 • 選択肢：「30」「60」「90」「120」（分） • 初期値：60（分）

「Apply」をクリックして、設定内容を適用します。

SNTP Settings（SNTP 設定）

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

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

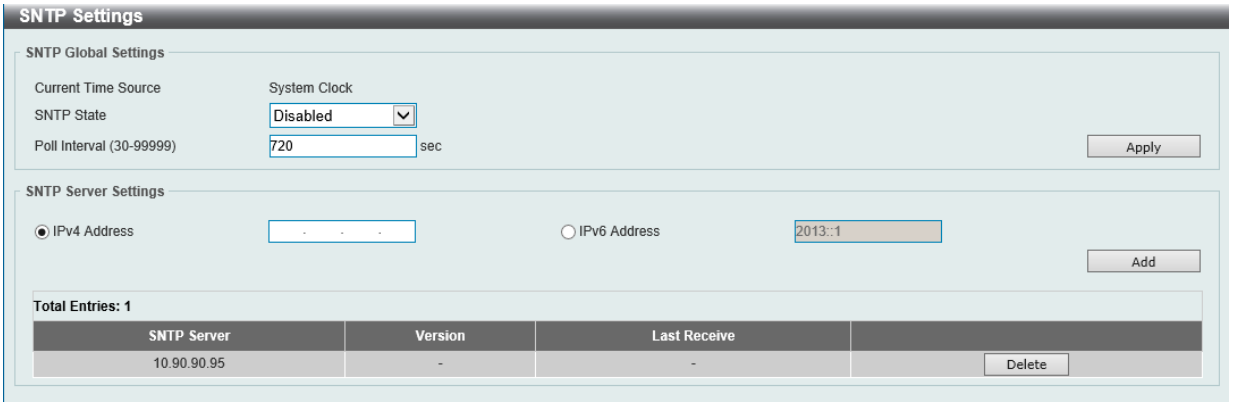


図 6-17　SNTP Settings 画面

画面に表示される項目：

項目	説明
SNTP Global Settings	
Current Time Source	現在の日付と時刻の提供元を表示します。
SNTP State	SNTP を有効 / 無効にします。
Poll Interval	同期する間隔を指定します。 • 設定可能範囲：30 - 99999（秒） • 初期値：720 秒
SNTP Server Settings	
IPv4 Address	SNTP 情報の取得元である SNTP サーバの IPv4 アドレスを設定します。
IPv6 Address	SNTP 情報の取得元である SNTP サーバの IPv6 アドレスを設定します。

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

注意　「Poll Interval」が 99999 秒に設定されている場合、ポーリング間隔の後に SNTP モードクライアントパケットを送信しません。

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。

注意　DXS-1210-28T/28S はリアルタイムクロック を持っていないため、タイムレンジの設定は時刻の同期後に行ってください。

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

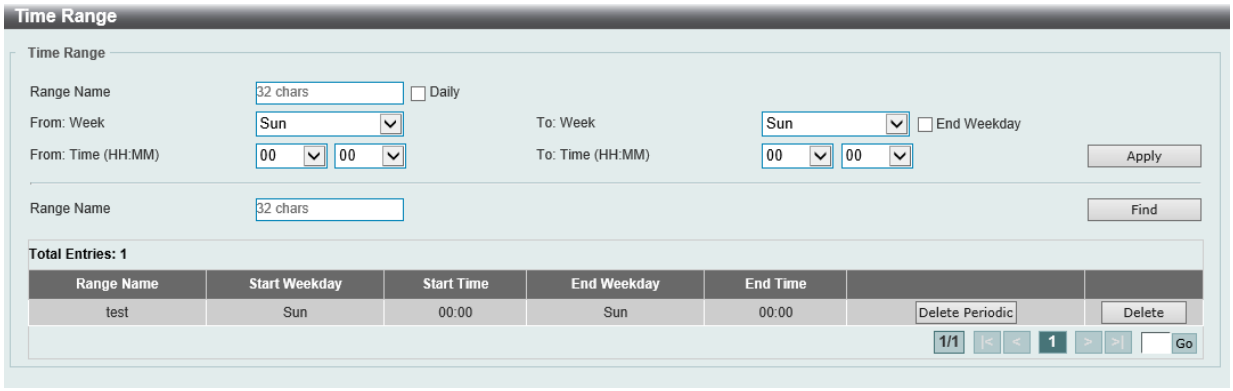


図 6-18　Time Range 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

設定エントリページが複数ページある場合、ページ番号を指定して「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」をクリックすると指定のエントリを検索できます。

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

第 7 章　Management（スイッチの管理）

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

サブメニュー	説明
User Accounts Settings（ユーザアカウント設定）	ユーザアカウントの作成と設定を行います。有効なユーザアカウントを表示可能です。
SNMP（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。
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。
Telnet / Web（Telnet /Web 設定）	Telnet 設定と Web 設定をします。
Session Timeout（セッションタイムアウト）	セッションタイムアウトの設定をします。
DHCP（DHCP 設定）	DHCP リレーサービスの設定を行います。
DHCP Auto Configuration（DHCP 自動設定）	DHCP 自動設定機能の設定を行います。
DHCP Auto Image Settings（DHCP 自動イメージ設定）	DHCP 自動イメージの設定を行います。
DNS（ドメインネームシステム）	DNS の設定を行います。
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。
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。

User Accounts Settings（ユーザアカウント設定）

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

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

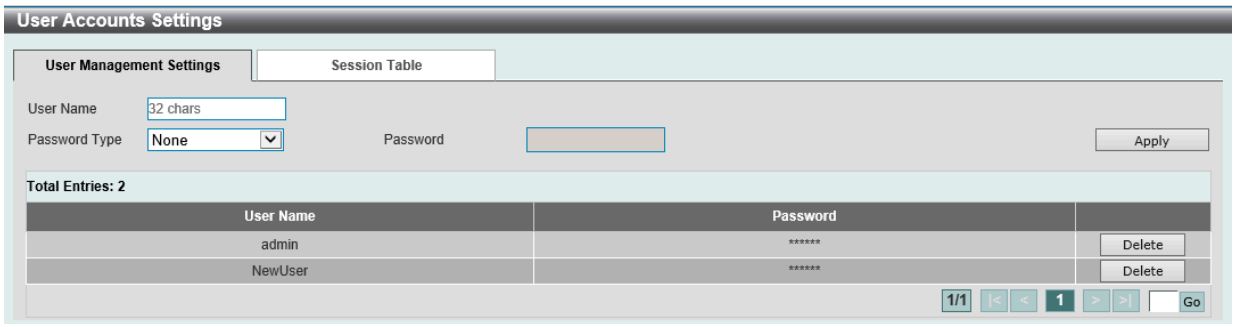


図 7-1　User Accounts Settings - User Management Settings 画面

画面に表示される項目：

項目	説明
User Name	ユーザ名を定義します。（32 文字以内）
Password Type	アカウントで使用する暗号化の方法を選択します。 • 「None」- ユーザアカウントにパスワードを指定しません。 • 「Plain Text」- プレーンテキストでパスワードを指定します。
Password	パスワードタイプで「Plain Text」を選択した場合、ユーザアカウントで使用するパスワードを入力します。

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

複数のページが存在する場合、ページ番号を指定して「Go」をクリックすることで特定のページへ移動できます。

■ 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。

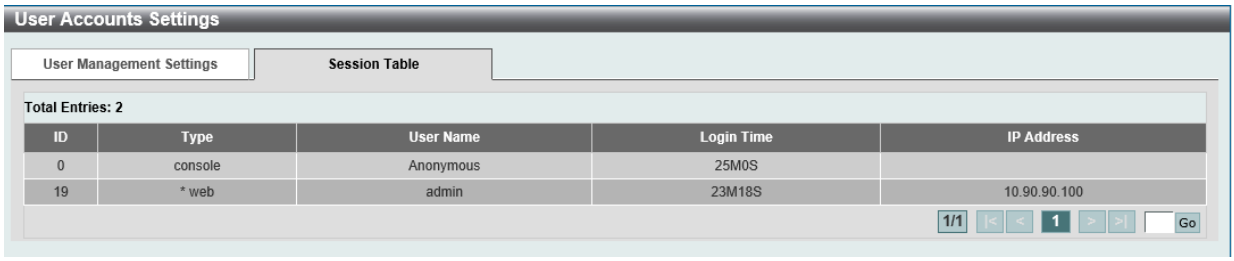


図 7-2　User Accounts Settings - Session Table 画面

複数のページが存在する場合、ページ番号を指定して「Go」をクリックすることで特定のページへ移動できます。

SNMP（SNMP 設定）

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

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

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

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

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

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

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

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

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

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

トラップ

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

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

MIB

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

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

SNMP Global Settings（SNMP グローバル設定）

SNMP グローバル設定とトラップ設定を行います。

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

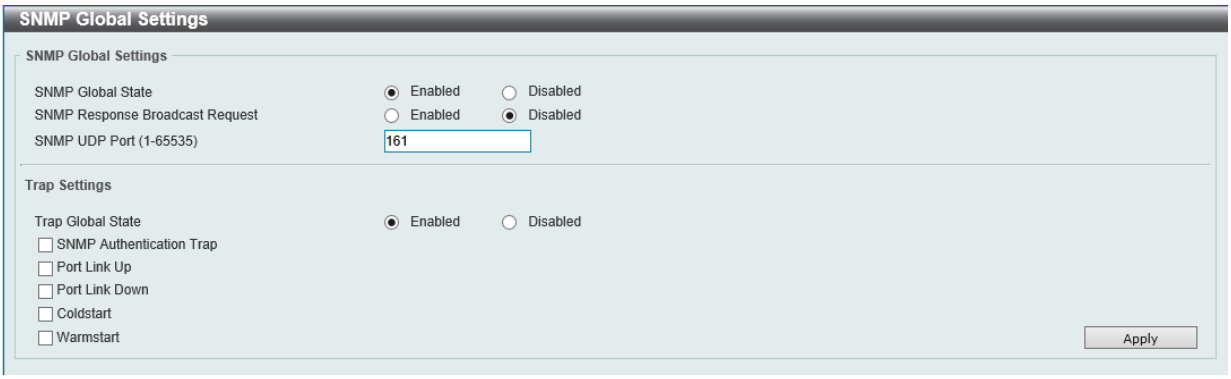


図 7-3　SNMP Global Settings 画面

画面に表示される項目：

項目	説明
SNMP Global Settings	
SNMP Global State	SNMP 機能を有効 / 無効に設定します。
SNMP Response Broadcast Request	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。 • 設定可能範囲：1-65535 • 初期値：161
Trap Settings	
Trap Global State	SNMP トラップを有効 / 無効にします。
SNMP Authentication Trap	SNMP 認証失敗の通知を有効 / 無効に設定します。 機器が正しく認証されていない SNMP メッセージを受信すると、authenticationFailuretrap トラップが生成されます。 認証方法は使用している SNMP のバージョンによって異なります。SNMPv1 または SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。
Port Link Up	ポートリンクアップ通知送信の設定を行います。 通信リンクのいずれかが起動すると、linkUp トラップが生成されます。
Port Link Down	ポートリンクダウン通知送信の設定を行います。 通信リンクのいずれかがダウンすると、linkDown トラップが生成されます。
Coldstart	coldStart 通知の設定を行います。
Warmstart	warmStart 通知の設定を行います。

「Apply」をクリックして、設定内容を適用します。

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

SNMP リンクチェンジトラップを設定します。

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

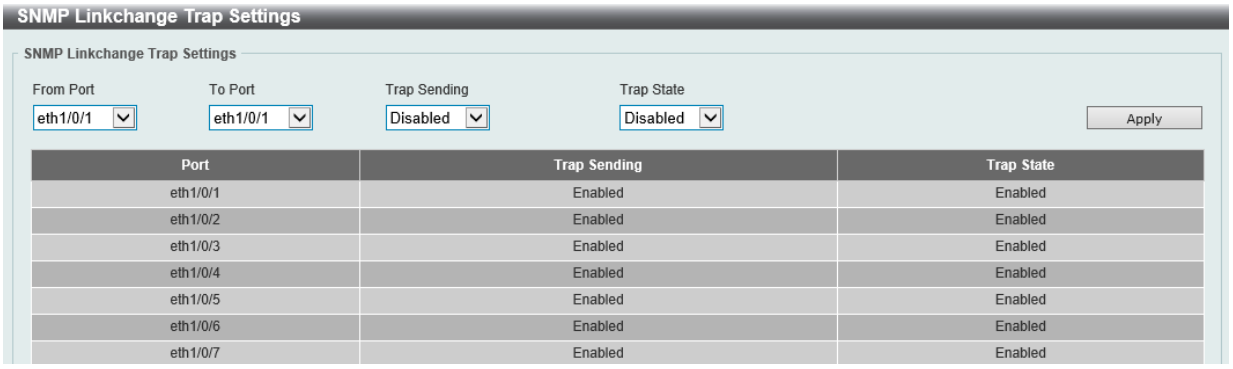


図 7-4　SNMP Linkchange Traps Settings 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
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 linkChange トラップを有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

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

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

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

図 7-5　SNMP View Table Settings 画面

画面に表示される項目：

項目	説明
View Name	ビュー名を入力します。（半角英数字 32 文字以内） SNMP ビューを識別する際に使用します。
Subtree OID	ビューの OID（Object Identifier）サブツリーを入力します。 OID 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」- SNMP マネージャがアクセスできるオブジェクトのリストにこのオブジェクトを含めます。 • 「Excluded」- SNMP マネージャがアクセスできるオブジェクトのリストにこのオブジェクトを含めません。

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

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

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

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

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

図 7-6　SNMP Community Table Settings 画面

画面に表示される項目：

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

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

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

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

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

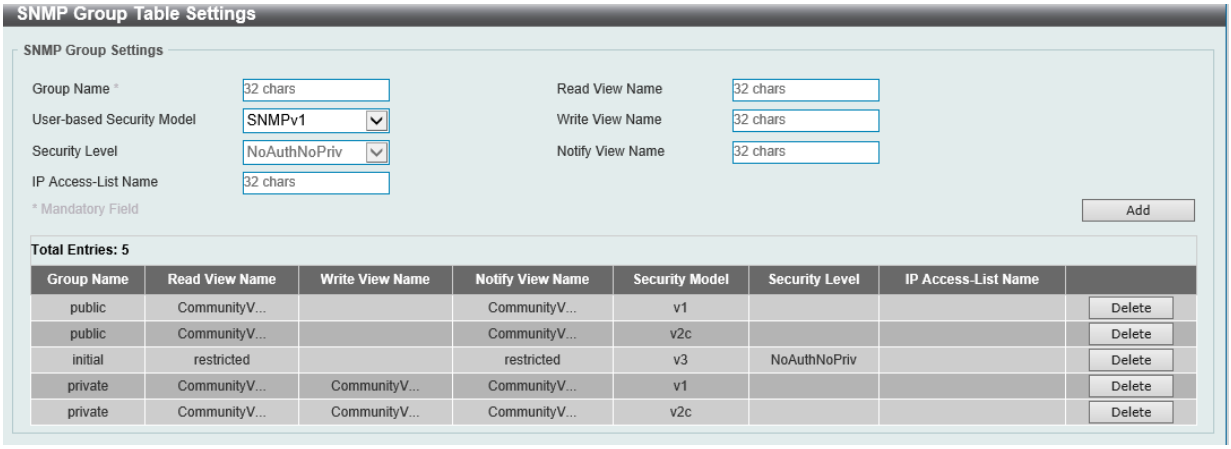


図 7-7　SNMP Group Table Settings 画面

画面に表示される項目：

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

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

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

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

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

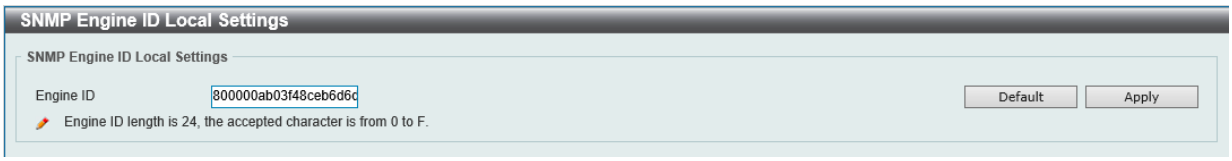


図 7-8　SNMP Engine ID Local Settings 画面

画面に表示される項目：

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

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

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

SNMP ユーザの登録、表示を行います。

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

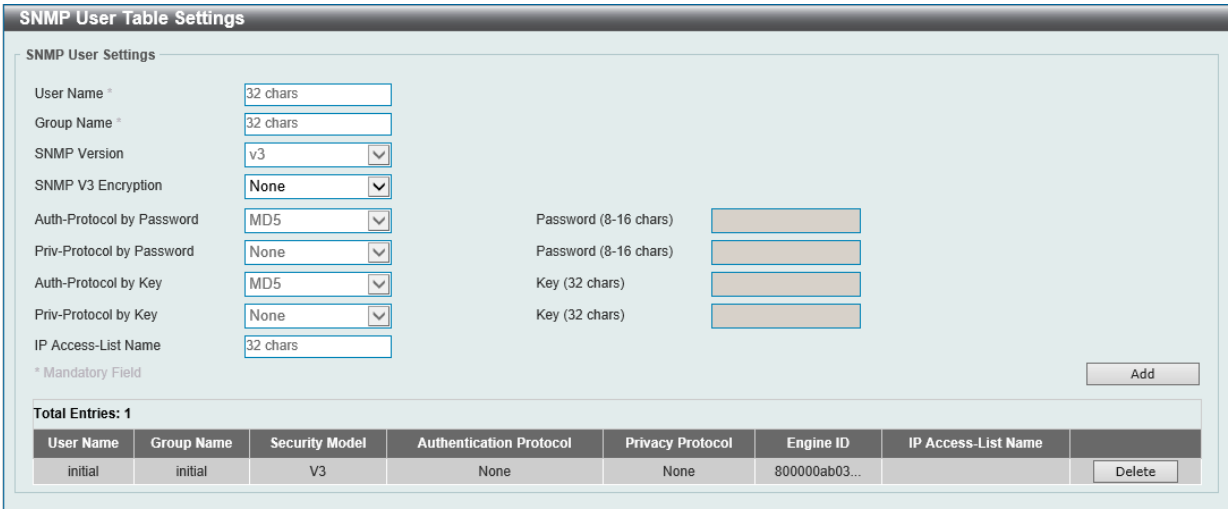


図 7-9　SNMP User Table Settings 画面

画面に表示される項目：

項目	説明
User Name	SNMP ユーザ名を入力します。（32 文字以内）
Group Name	ユーザが属する SNMP グループ名を入力します。（32 文字以内）
SNMP Version	SNMPv3 が選択されています。
SNMP V3 Encryption	SNMP v3 の暗号化の設定を行います。 • 選択肢：「None」「Key」「Password 」
Auth-Protocol by Password	「SNMP V3 Encryption」で「Password」を選択した場合に有効になります。 以下から認証プロトコルを選択後、パスワードを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。（パスワード：8-16 文字以内） • 「SHA」- HMAC-SHA 認証プロトコルが使用されます。（パスワード：8-20 文字以内）
Priv-Protocol by Password	「SNMP V3 Encryption」で「Password」を選択した場合に有効になります。 以下からプライバシープロトコルを選択後、パスワードを入力します。 • 「None」- 認証プロトコルは使用されません。 • 「DES56」- CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されます。（パスワード：8-16 文字以内）
Auth-Protocol by Key	「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 以下から認証プロトコルを選択後、キーを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。（キー：32 文字以内） • 「SHA」- HMAC-SHA 認証プロトコルが使用されます。（キー：40 文字以内）
Priv-Protocol by Key	「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 以下からプライバシープロトコルを選択後、キーを入力します。 • 「None」- 認証プロトコルは使用されません。 • 「DES56」- CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されます。（キー：32 文字以内）
IP Access-List Name	ユーザに関連付ける標準 IP アクセスコントロールリストの名前を入力します。

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

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

SNMP トラップの送信先を登録します。

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

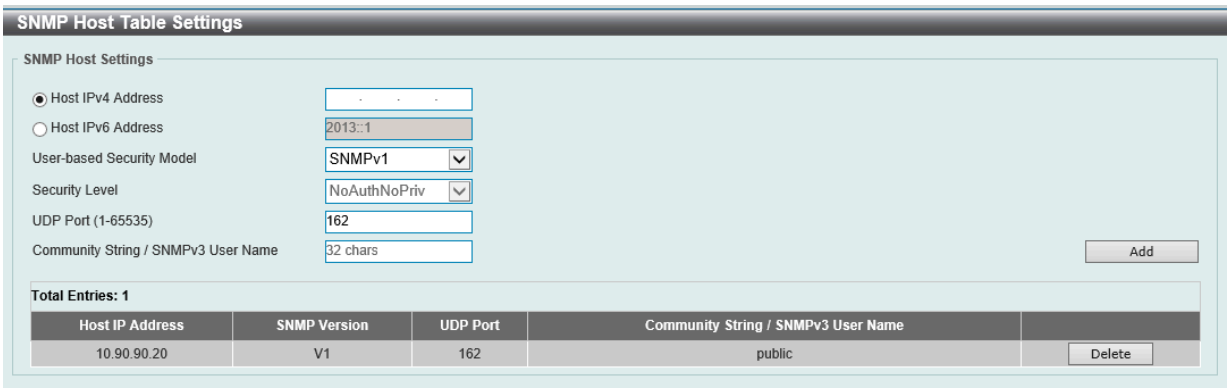


図 7-10　SNMP Host Table Settings 画面

画面に表示される項目：

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv6 アドレスを入力します。
User-based Security Model	SNMP バージョンを選択します。 • 「SNMPv1」- SNMP バージョン 1 を使用します。 • 「SNMPv2c」- SNMP バージョン 2c を使用します。 • 「SNMPv3」- SNMP バージョン 3 を使用します。
Security Level	「SNMPv3」を指定した場合、セキュリティレベルを設定します。 • 「NoAuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証も暗号化も行われません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証は行われますが暗号化は行われません。 • 「AuthPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証 / 暗号化が行われます。
UDP Port	UDP ポート番号を入力します。ポート番号によっては他のプロトコルと競合する可能性があります。 • 設定可能範囲：1 - 65535 • 初期値：162
Community String / SNMPv3 User Name	コミュニティ名または SNMP v3 ユーザ名を入力します。

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

RMON（RMON 設定）

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

RMON Global Settings（RMON グローバル設定）

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

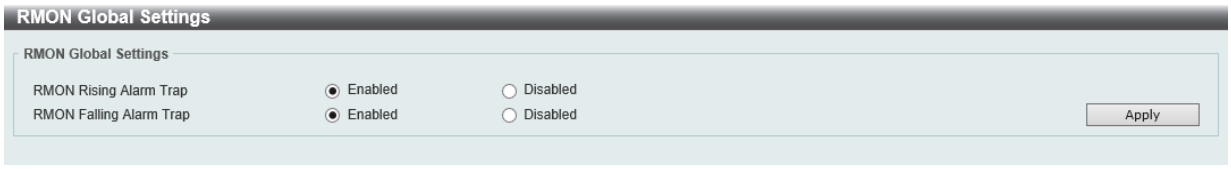


図 7-11　RMON Global Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

RMON Statistics Settings（RMON 統計設定）

RMON 統計情報を表示、設定します。

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

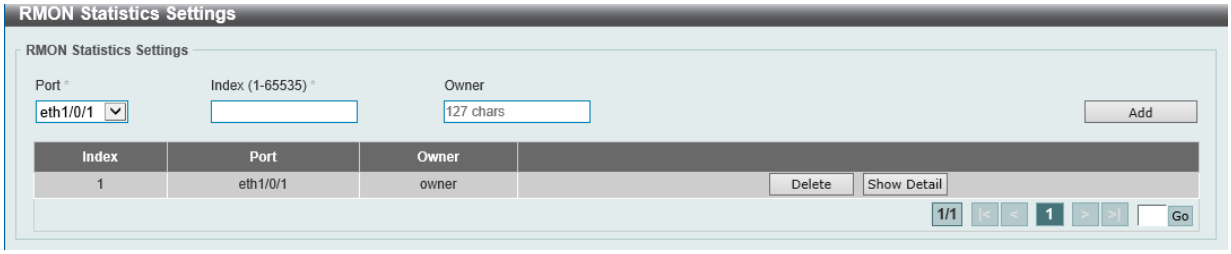


図 7-12　RMON Statistics Settings 画面

画面に表示される項目：

項目	説明
Port	ポートを指定します。
Index	RMON テーブルインデックスを入力します。 • 設定可能範囲：1 - 65535
Owner	オーナ名を入力します。（127 文字以内）

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

指定ポートの統計情報を表示する場合
「Show Detail」をクリックします。以下の画面が表示されます。

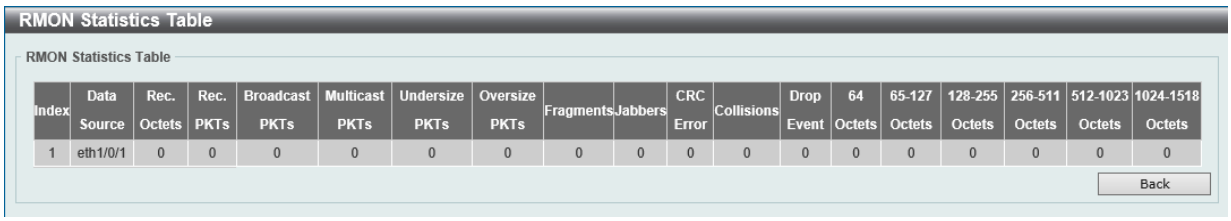


図 7-13　RMON Statistics Settings - Show Detail 画面

前の画面に戻るには、「Back」をクリックします。

RMON History Settings（RMON ヒストリ設定）

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

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

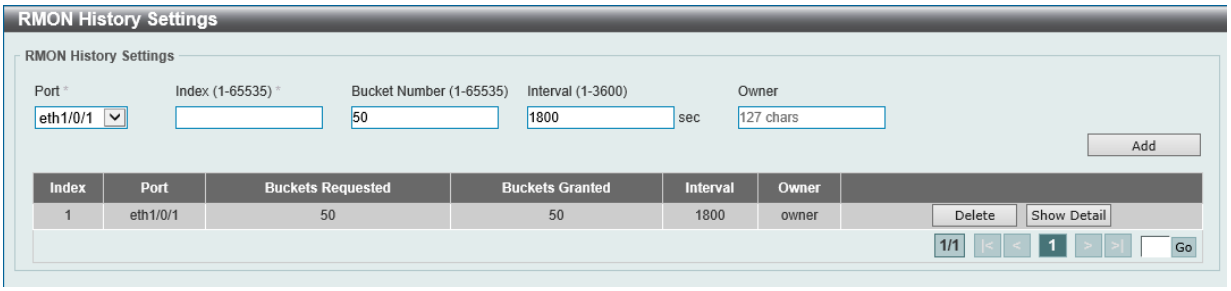


図 7-14　RMON History Settings 画面

画面に表示される項目：

項目	説明
Port	本設定を適用するポートを指定します。
Index	ヒストリグループテーブルのインデックス番号を指定します。 • 設定可能範囲：1-65535
Bucket Number	統計における RMON 収集ヒストリグループのバケット数を指定します。 • 設定可能範囲：1-65535 • 初期値：50
Interval	ポーリング間隔を設定します。 • 設定可能範囲：1-3600（秒） • 初期値：1800（秒）
Owner	オーナの文字列を入力します。（127 文字以内）

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

指定ポートの履歴情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

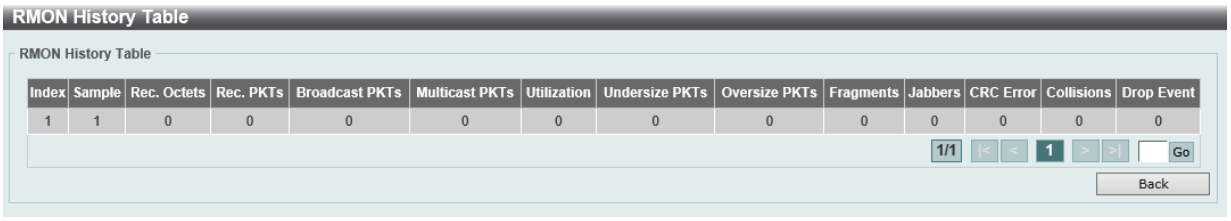


図 7-15　RMON History Settings - Show Detail 画面

前の画面に戻るには、「Back」をクリックします。

RMON Alarm Settings（RMON アラーム設定）

インタフェースをモニタするためのアラームエントリを表示、設定します。

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

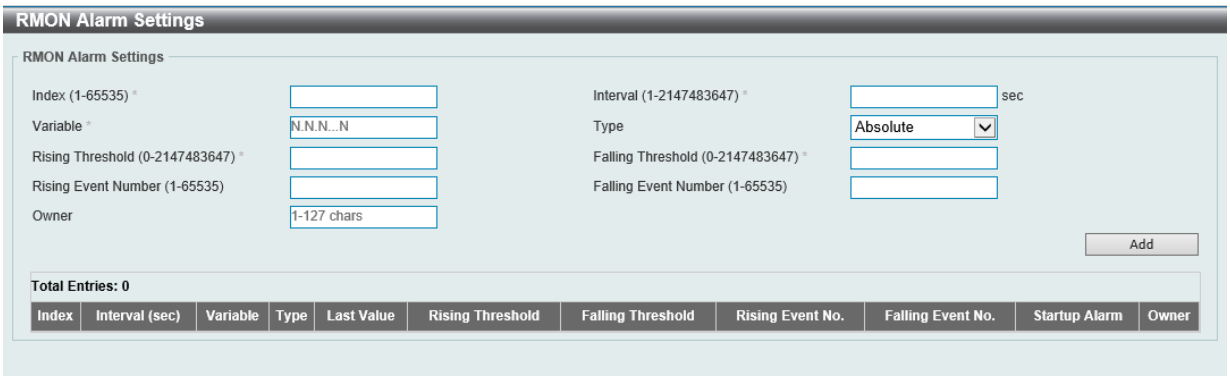


図 7-16　RMON Alarm Settings 画面

画面に表示される項目：

項目	説明
Index	アラームのインデックス番号を指定します。 • 設定可能範囲：1 - 65535
Interval	変数のサンプリングおよびしきい値に対するチェックの間隔を定義します。 • 設定可能範囲：1 - 2147483647（秒）
Variable	サンプリングする変数のオブジェクト識別子を入力します。
Type	モニタリングのタイプを選択します。 •「Absolute」- サンプリング値がしきい値と直接比較されます。 •「Delta」-2 つの連続したサンプル値の差分がしきい値と比較されます。
Rising Threshold	上昇しきい値を設定します。 • 設定可能範囲：0 - 2147483647
Falling Threshold	下降しきい値を設定します。 • 設定可能範囲：0 - 2147483647
Rising Event Number	上昇しきい値を超えたときに開始するイベントのインデックス番号を指定します。 • 設定可能範囲：1 - 65535 指定しない場合、上昇しきい値を超えてもアクションを実行しません。
Falling Event Number	下降しきい値を超えたときに開始するイベントのインデックス番号を指定します。 • 設定可能範囲：1 - 65535 指定しない場合、下降しきい値を下回ってもアクションを実行しません。
Owner	オーナ名を入力します。（127 字以内）

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

RMON Event Settings（RMON イベント設定）

RMON イベントの設定を行います。

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

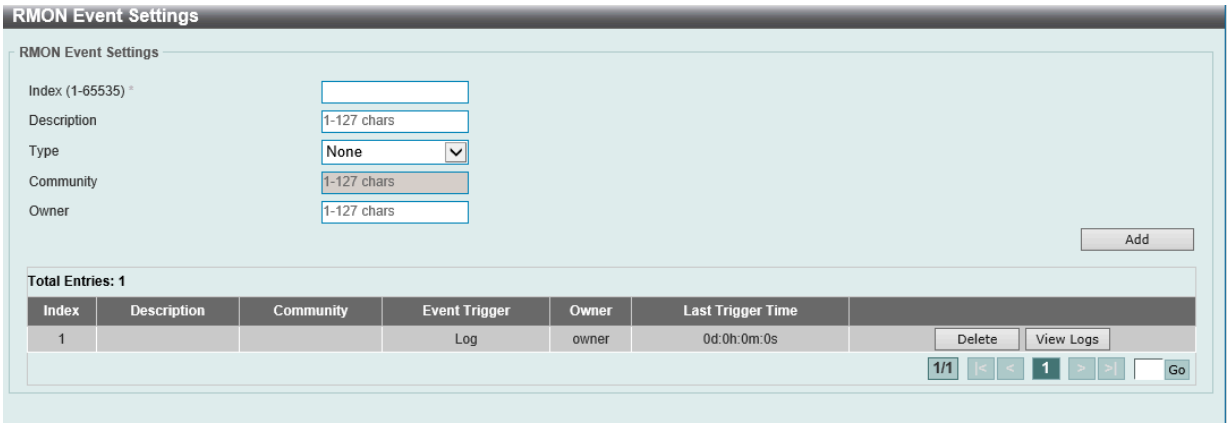


図 7-17　RMON Event Settings 画面

画面に表示される項目：

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

「Add」をクリックしてエントリを追加します。
「Delete」をクリックしてエントリを削除します。
複数のページが存在する場合、ページ番号を指定して「Go」をクリックすることで、特定のページへ移動できます。

指定エントリのログ情報を表示する場合

「View Logs」をクリックすると、以下の画面が表示されます。

図 7-18　Event Logs Table 画面

前の画面に戻るには、「Back」をクリックします。

Telnet / Web（Telnet /Web 設定）

スイッチの Telnet/Web 設定を行います。

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

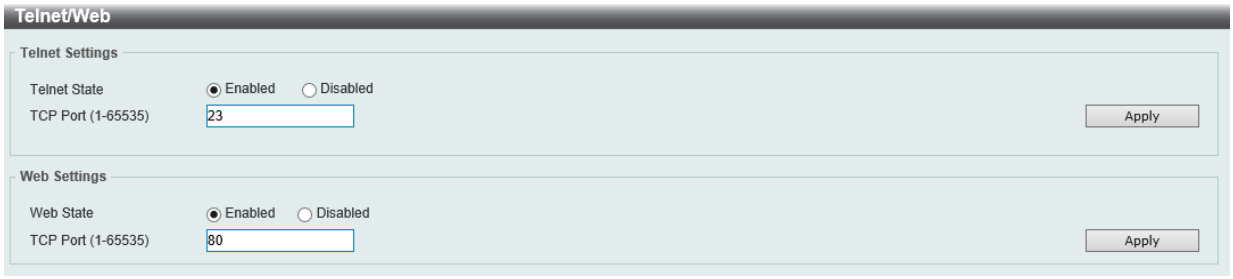


図 7-19　Telnet/Web 画面

画面に表示される項目：

項目	説明
Telnet Settings	
Telnet State	Telnet サーバ機能を有効 / 無効に設定します。
TCP Port	スイッチの Telnet 管理に使用する TCP ポート番号を入力します。Telnet プロトコルに通常使用される TCP ポートは 23 です。 • 設定可能範囲：1 - 65535
Web Settings	
Web State	Web ベースマネジメントの有効 / 無効を設定します。
Port	スイッチの Web マネジメントに使用される TCP ポート番号を指定します。 Web プロトコルに通常使用される TCP ポートは 80 です。 • 設定可能範囲：1 - 65535

「Apply」をクリックして、設定内容を適用します。

Session Timeout（セッションタイムアウト）

各セッション（Web、コンソール、Telnet、SSH）のタイムアウトの設定をします。

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

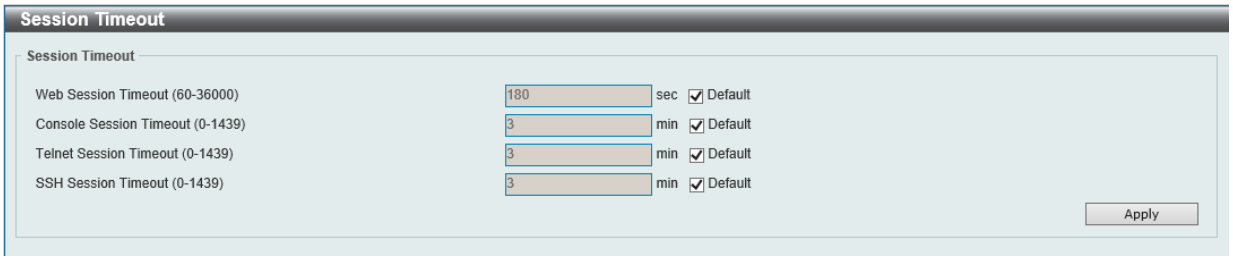


図 7-20　Session Timeout 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

DHCP（DHCP 設定）

Service DHCP（DHCP サービス）

スイッチの DHCP サービスについて設定します。

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

図 7-21　Service DHCP 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

DHCP Class Settings（DHCP クラス設定）

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

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

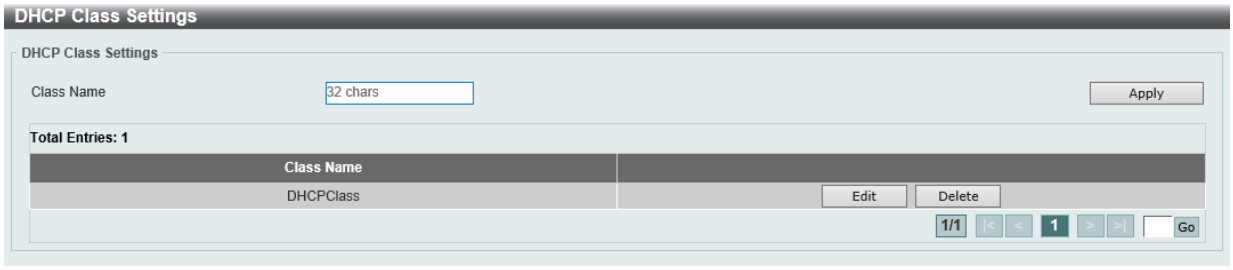


図 7-22　DHCP Class Settings 画面

画面に表示される項目：

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

「Apply」をクリックし、設定内容を適用します。
複数のページが存在する場合、ページ番号を指定して「Go」をクリックすることで特定のページへ移動できます。
「Delete」をクリックしてエントリを削除します。

指定エントリの編集を行う場合

「Edit」をクリックします。以下の画面が表示されます。

図 7-23　DHCP Class Option Settings 画面

画面に表示される項目：

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

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

前の画面に戻るには、「Back」をクリックします。

DHCP Relay（DHCP リレー）

DHCP リレーエージェントのスマートリレー機能を設定します。

注意　DHCP リレーが有効な場合、DISCOVER パケットは対象 VLAN 内にフラッディングされません。

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

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

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

図 7-24　DHCP Relay Pool Settings 画面

画面に表示される項目：

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

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

■ 各プールエントリの編集を行う

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

● 「Source」の編集を行う場合

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

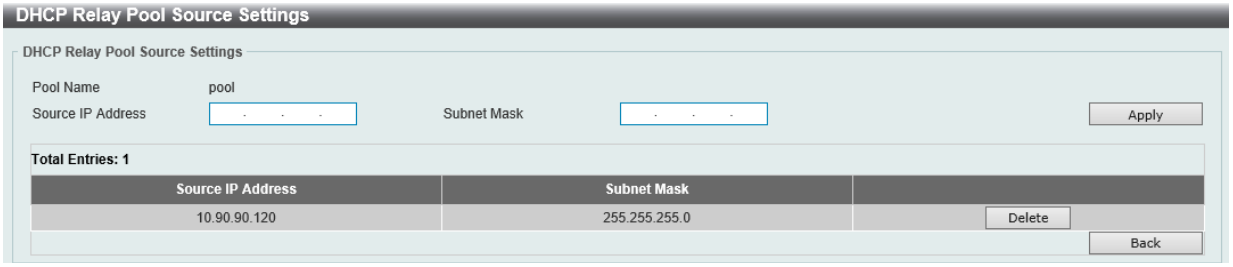


図 7-25　DHCP Relay Pool Source Settings 画面

画面に表示される項目：

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

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックして、エントリを削除します。
「Back」をクリックすると前の画面へ戻ります。

● 「Destination」の編集を行う場合

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

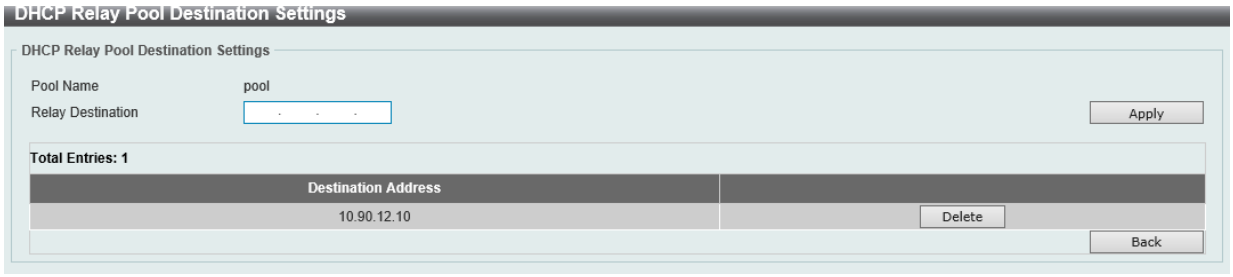


図 7-26　DHCP Relay Pool Destination Settings 画面

画面に表示される項目：

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

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックして、エントリを削除します。
「Back」をクリックすると前の画面へ戻ります。

● 「Class」の編集を行う場合

「Class」下の「Edit」をクリックします。以下の画面が表示されます。

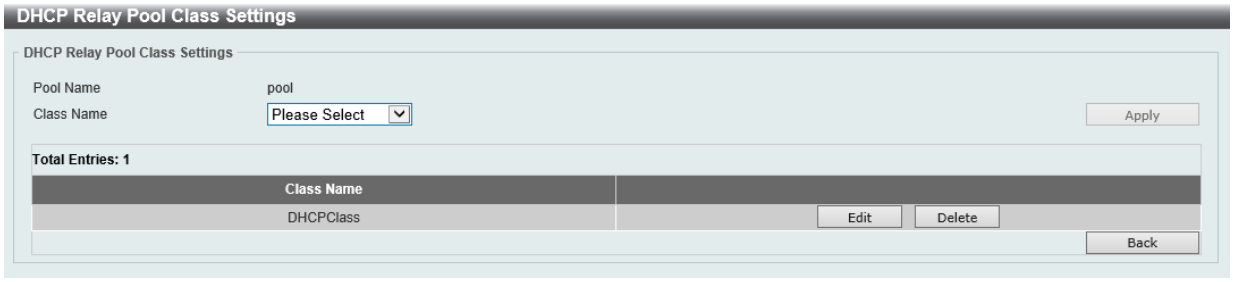


図 7-27　DHCP Relay Pool Class Settings 画面

画面に表示される項目：

項目	説明
Class Name	DHCP クラスの名前を選択します。

「Apply」をクリックし、設定内容を適用します。
「Delete」をクリックして、エントリを削除します。
「Back」をクリックすると前の画面へ戻ります。

クラス名の横の「Edit」をクリックすると以下の画面が表示されます。

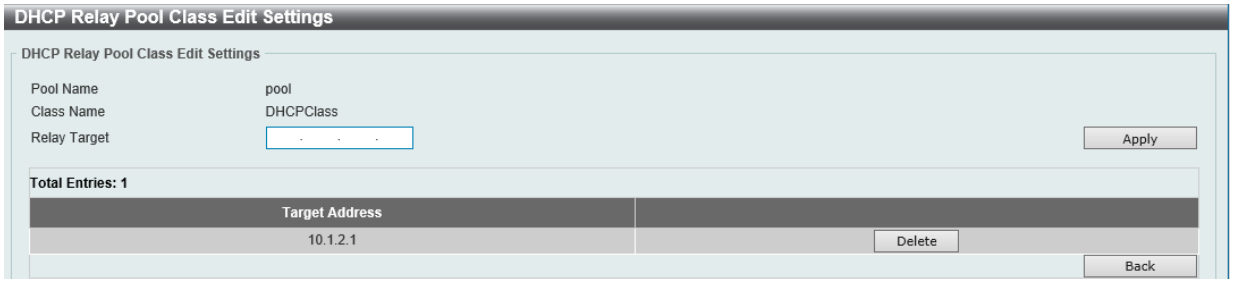


図 7-28　DHCP Relay Pool Class Edit Settings 画面

画面に表示される項目：

項目	説明
Relay Target	DHCP クラスで設定したオプションの値パターンと一致するパケットをリレーする DHCP リレーターゲットを入力します。

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、エントリを削除します。
「Back」をクリックすると前の画面へ戻ります。

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

DHCP リレー情報の設定を行います。

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

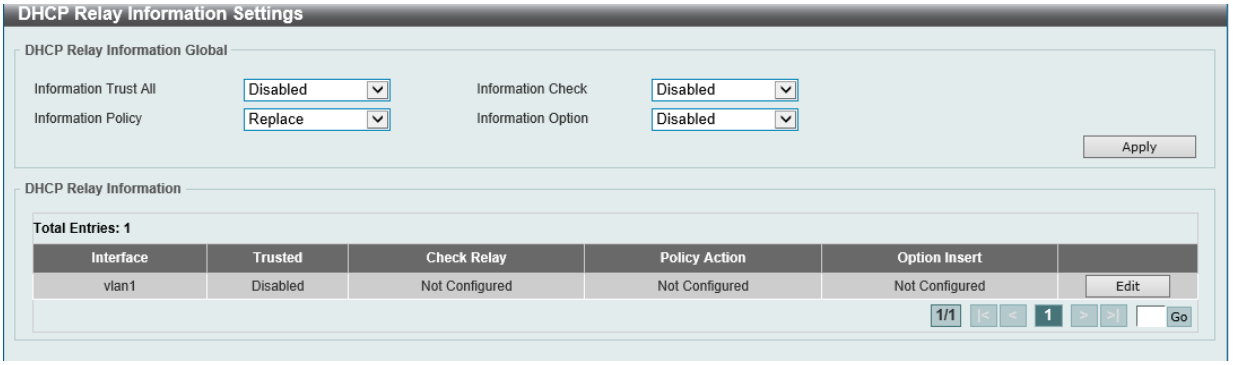


図 7-29　DHCP Relay Information Settings 画面

画面に表示される項目：

項目	説明
Information Trust All	すべてのインタフェースで DHCP リレーエージェントによる IP DHCP リレーインフォメーションへの信頼を有効 / 無効に設定します。
Information Check	DHCP リレーエージェントによる、受信した DHCP リレーパケットに含まれるリレーエージェントインフォメーションの検証と破棄を有効 / 無効に設定します。
Information Policy	DHCP リレーエージェントのオプション 82 再転送ポリシーを選択します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。 • 「Replace」- DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。
Information Option	DHCP リクエストパケットがリレーされる間のリレーエージェント情報（Option82）の挿入を有効 / 無効に設定します。

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

複数のページが存在する場合、ページ番号を指定して「Go」をクリックすることで特定のページへ移動できます。

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

DHCP 情報フォーマットの表示、設定を行います。

Management > DHCP > DHCP Relay > DHCP Relay Information Option Format Settings の順にクリックし、以下の画面を表示します。

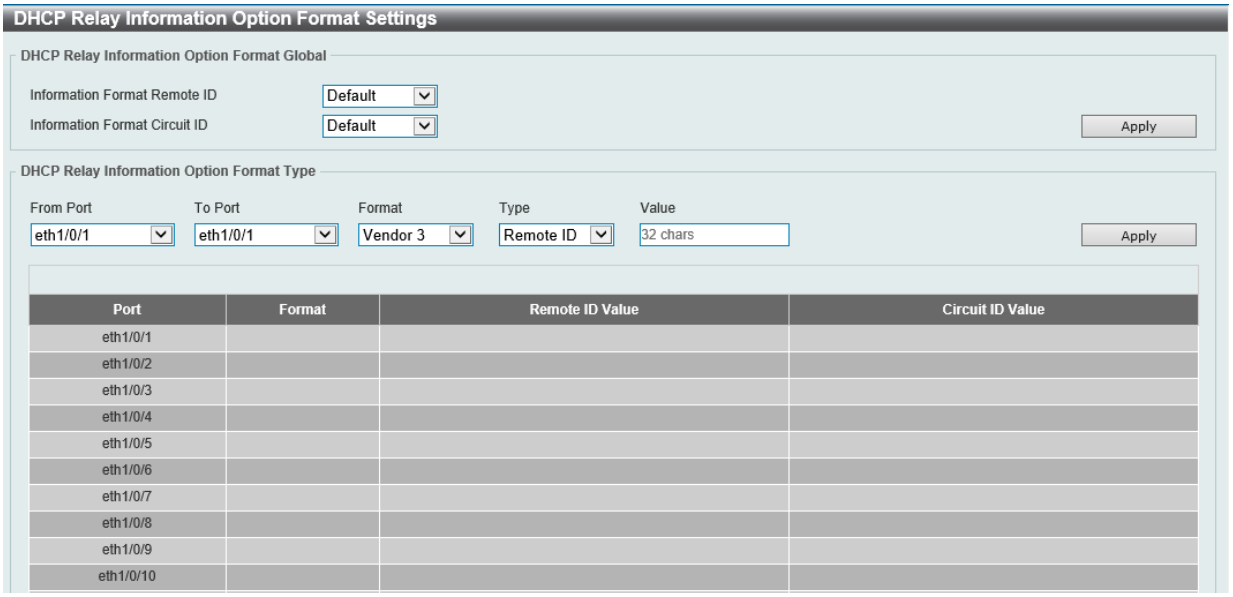


図 7-30　DHCP Relay Information Option Format Settings 画面

画面に表示される項目：

項目	説明
DHCP Relay Information Option Format Global	
Information Format Remote ID	「DHCP information remote ID」のサブオプションを選択します。 • 「Default」- リモート ID としてスイッチのシステム MAC アドレスを使用します。（初期値） • 「User Define」- リモート ID としてユーザ定義の文字列を使用します。（32 文字以内） • 「Vendor2」- リモート ID としてベンダ 2 を使用します。 • 「Vendor3」- リモート ID としてベンダ 3 を使用します。
Information Format Circuit ID	「DHCP information circuit ID」のサブオプションを選択します。 • 「Default」- 初期値のサーキット ID を使用します。（初期値） • 「User Define」- ユーザ定義のサーキット ID を使用します。（32 文字以内） • 「Vendor1」- サーキット ID としてベンダ 1 を使用します。 • 「Vendor2」- サーキット ID としてベンダ 2 を使用します。 • 「Vendor3」- サーキット ID としてベンダ 3 を使用します。 • 「Vendor4」- サーキット ID としてベンダ 4 を使用します。 • 「Vendor5」- サーキット ID としてベンダ 5 を使用します。 • 「Vendor6」- サーキット ID としてベンダ 6 を使用します。
DHCP Relay Information Option Format Type	
From Port / To Port	設定するポートの範囲を指定します。
Format	「Vendor3」フォーマットを指定します。
Type	リレー情報オプションの種類を選択します。 • 選択肢：「Remote ID」「Circuit ID」
Value	オプション 82 情報として、リモート / サーキット ID サブオプションに含まれるベンダ定義の文字列を入力します。（32 文字以内）

「Apply」をクリックして、設定内容を適用します。

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

VLAN、またはグループ VLAN のローカルリレー設定を行います。

Management > DHCP > DHCP Relay > DHCP Local Relay VLAN の順にクリックし、以下の画面を表示します。

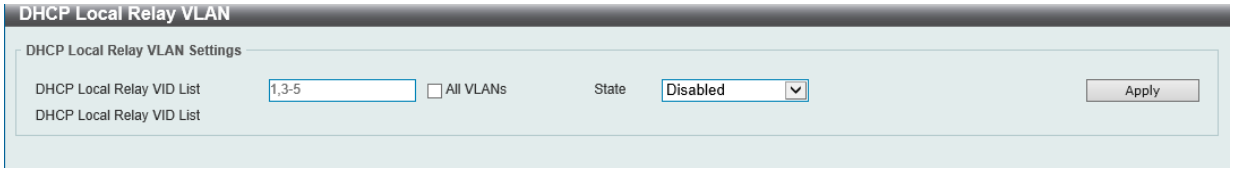


図 7-31　DHCP Local Relay VLAN 画面

画面に表示される項目：

項目	説明
DHCP Local Relay VID List	DHCP ローカルリレーを適用する VLAN ID を入力します。 「All VLANs」にチェックを入れると、すべての VLAN が対象になります。
State	指定した VLAN の DHCP ローカルリレー機能を有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

DHCPv6 Relay（DHCPv6 リレー）

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

スイッチの DHCPv6 リレー機能を設定します。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings の順にクリックし、以下の画面を表示します。

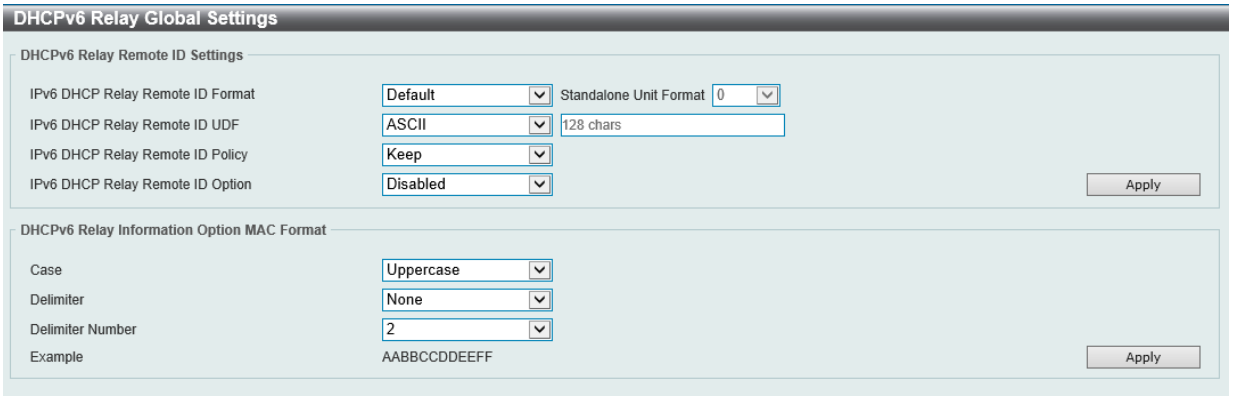


図 7-32　DHCPv6 Relay Global Settings 画面

画面に表示される項目：

項目	説明
IPv6 DHCP Relay Remote ID Format	IPv6 DHCP リレーリモート ID フォーマットを選択します。 • 選択肢：「Default」「CID With User Define」「User Define」「Expert UDF」
Standalone Unit Format	「Expert UDF」を選択した場合、スタンドアロンユニットのフォーマットを選択します。 • 選択肢：「0」「1」
IPv6 DHCP Relay Remote ID UDF	リモート ID のユーザ定義項目 (UDF) の入力形式 を選択します。 • 「None」- リモート ID の UDF を空のままにします。 • 「ASCII」- ASCII 文字列で入力します。（128 文字以内） • 「HEX」- 16 進数文字列で入力します。（256 文字以内）
IPv6 DHCP Relay Remote ID Policy	DHCPv6 リレーエージェントのオプション 37 フォワーディングポリシーを選択します。 • 「Keep」- DHCP クライアントから受信したパケット内の既存のオプション 37 リレー情報を保持します。 • 「Drop」- DHCP クライアントから受信したパケット内に既にオプション 37 リレー情報があった場合はそのパケットを破棄します。
IPv6 DHCP Relay Remote ID Option	DHCP IPv6 リクエストパケットのリレーの間のリレーエージェント情報（Option37）の挿入を有効 / 無効に設定します。
DHCPv6 Relay Information Option MAC Format	
Case	MAC アドレスの形式を選択します。 • 「Lowercase」- 小文字を使用します。（例：aa-bb-cc-dd-ee-ff） • 「Uppercase」- 大文字を使用します。（例：AA-BB-CC-DD-EE-FF）
Delimiter	MAC アドレスを入力する際の区切りを選択します。区切り文字を持たない場合には「None」を選択します。各項目の例は次の通りです。 • 「Hyphen」（ハイフン）-「AA-BB-CC-DD-EE-FF」 • 「Colon」（コロン）-「AA:BB:CC:DD:EE:FF」 • 「Dot」（ドット）-「AA.BB.CC.DD.EE.FF」 • 「None」（なし）-「AABBCCDDEEFF」
Delimiter Number	MAC アドレスにおける区切り数を選択します。各項目の例は次の通りです。 • 「1」-「AABBCC.DDEEFF」 • 「2」-「AABB.CCDD.EEFF」 • 「5」-「AA.BB.CC.DD.EE.FF」

「Apply」をクリックして、設定内容を適用します。

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

DHCPv6 リレーインタフェースの設定を行います。

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface Settings の順にクリックし、以下の画面を表示します。

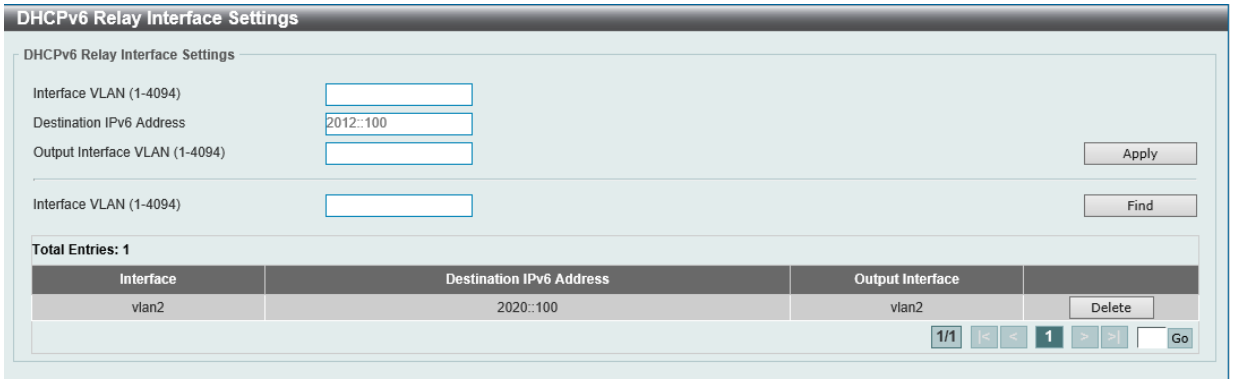


図 7-33　DHCPv6 Relay Interface Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。
「Find」をクリックして、入力した情報に基づく特定のエントリを検出します。
「Delete」をクリックして、特定のエントリを削除します。
複数のページが存在する場合、ページ番号を指定して「Go」をクリックすることで特定のページへ移動できます。

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

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

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Remote ID Profile Settings の順にクリックし、以下の画面を表示します。

図 7-34　DHCPv6 Relay Remote ID Profile Settings 画面

画面に表示される項目：

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

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

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

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

Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Format Type Settings の順にクリックし、以下の画面を表示します。

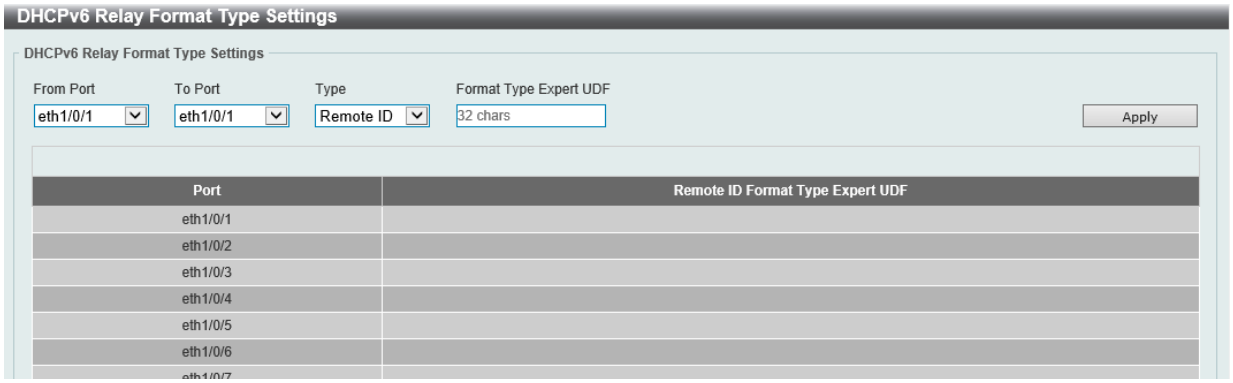


図 7-35　DHCPv6 Relay Format Type Settings 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Type	以下からタイプを指定します。 • 「Remote ID」-「expert UDF」フォーマットタイプ文字列を DHCPv6 オプション 37 で指定します。
Format Type Expert UDF	指定ポートで使用する「expert UDF」文字列のフォーマットを設定します。

「Apply」をクリックして、設定内容を適用します。

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

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

Management > DHCP > DHCPv6 Relay > DHCPv6 Local Relay VLAN の順にクリックし、以下の画面を表示します。

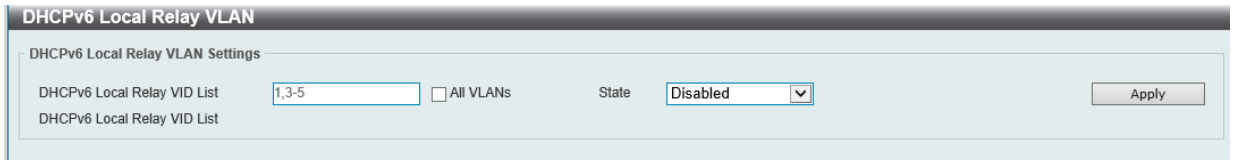


図 7-36　DHCPv6 Local Relay VLAN 画面

画面に表示される項目：

項目	説明
DHCPv6 Local Relay VID List	DHCPv6 ローカルリレー VLAN ID を入力します。1 つ以上の VLAN ID が入力可能です。 「All VLANs」オプションを指定すると、すべての VLAN が対象になります。
State	指定 VLAN の DHCPv6 ローカルリレー機能を有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

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

DHCP Auto Configuration（DHCP 自動設定）

DHCP 自動コンフィグ機能の設定を行います。

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

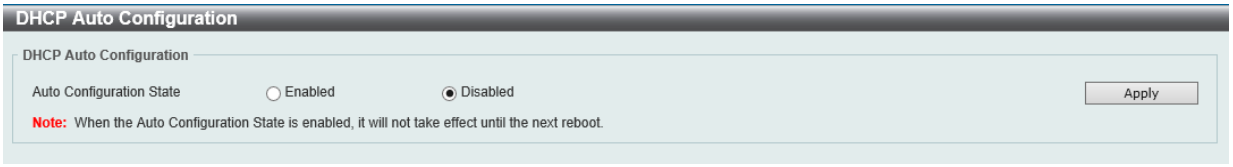


図 7-37　DHCP Auto Configuration 画面

画面に表示される項目：

項目	説明
Auto Configuration State	DHCP 自動設定を有効 / 無効にします。

「Apply」をクリックして、設定内容を適用します。

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

ここでは DHCP 自動イメージ設定を行います。
本機能は、スイッチの起動時に外部 TFTP サーバからイメージファイルを取得する機能です。この TFTP サーバの IP アドレスとファイル名は、DHCP サーバからの「DHCP OFFER」メッセージに含まれています。システムはこのイメージファイルを起動イメージとして使用します。システムが起動し、自動イメージ機能が有効になると、本スイッチは自動的に DHCP クライアントになります。
DHCP クライアントがアクティブになると、DHCP サーバからネットワーク設定を取得します。DHCP サーバからのメッセージには、TFTP サーバの IP アドレスとイメージファイル名が含まれています。スイッチがこの情報を受信した後、指定した TFTP サーバからの TFTP ダウンロード機能を起動します。このタイミングで、ダウンロード設定パラメータがコンソールに表示されます。レイアウトは download firmware コマンドを使用した場合と同じです。ファームウェアのダウンロードが完了すると、スイッチはすぐに再起動します。

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

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

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

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

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

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

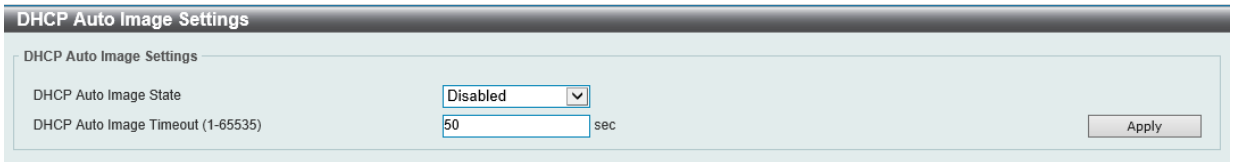


図 7-38　DHCP Auto Image Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

DNS（ドメインネームシステム）

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

DNS Global Settings（DNS グローバル設定）

DNS のグローバル設定を行います。

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

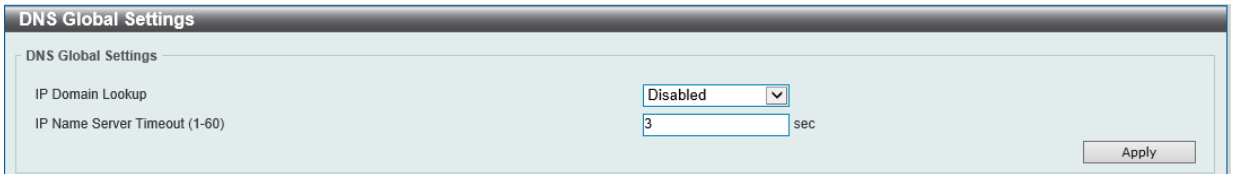


図 7-39　DNS Global Settings 画面

画面に表示される項目：

項目	説明
IP Domain Lookup	IP ドメインルックアップを有効 / 無効に設定します。
IP Name Server Timeout	指定ネームサーバからの回答を待つ待機時間を指定します。 • 設定可能範囲：1-60（秒）

「Apply」をクリックして、設定内容を適用します。

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

スイッチに DNS の IP アドレスを設定します。

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

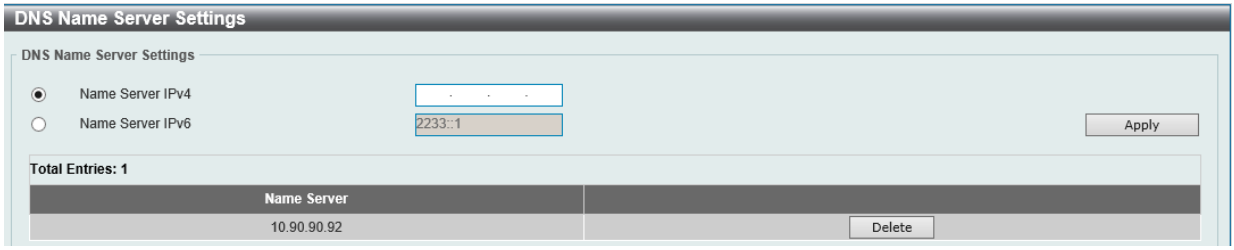


図 7-40　DNS Name Server Settings 画面

画面に表示される項目：

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

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

DNS Host Settings（DNS ホスト設定）

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

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

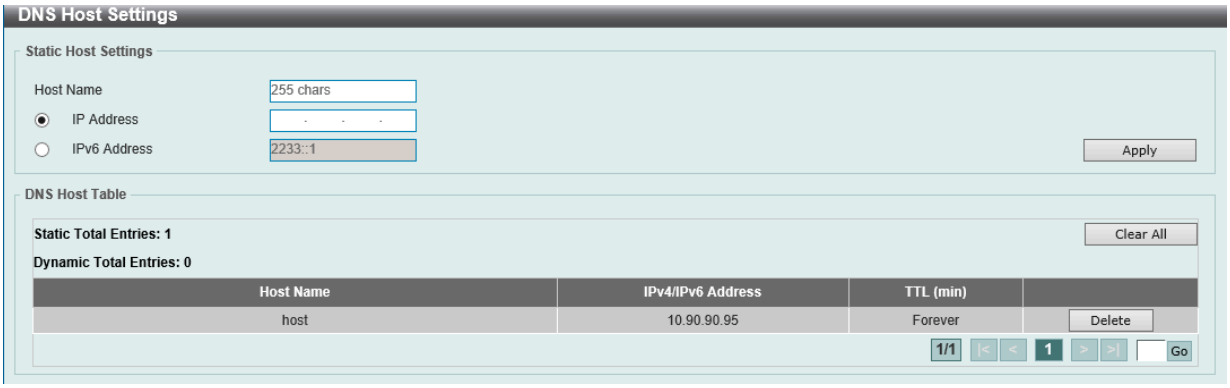


図 7-41　DNS Host Settings 画面

画面に表示される項目：

項目	説明
Host Name	ホスト名を入力します。
IP Address	ホストの IPv4 アドレスを入力します。
IPv6 Address	ホストの IPv6 アドレスを入力します。

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、指定エントリを削除します。
「Clear All」をクリックすると入力したエントリを全てクリアします。

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

File System（ファイルシステム）

スイッチのファイルシステムを閲覧、管理および設定します。

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

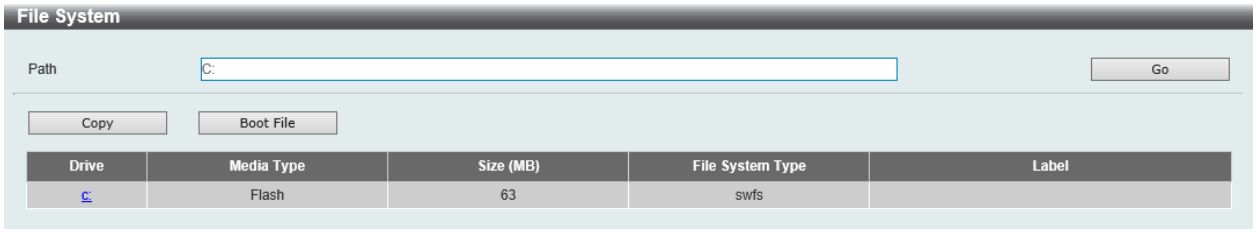


図 7-42　File System 画面

画面に表示される項目：

項目	説明
Path	パスの文字列を入力します。

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

「C:」リンクをクリックすると、以下の画面が表示されます。

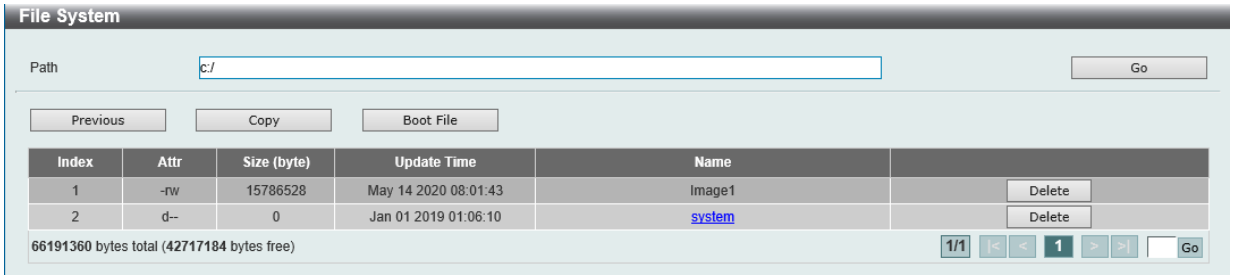


図 7-43　File System – Drive 画面

注意　ブートコンフィグレーションファイルが破損している場合、スイッチは自動的に初期設定に戻ります。

注意　ブートイメージファイルが破損している場合、スイッチは自動的にバックアップイメージファイルを次のブートアップ時に使用します。

画面に表示される項目：

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

注意　初期設定では起動用のコンフィグレーションに「config.cfg」が設定されています。
起動用のコンフィグレーションを指定する場合に選択できるのは「Config1」及び「Config2」です。

ファイルのコピー

「Copy」をクリックすると、以下の画面が表示されます。

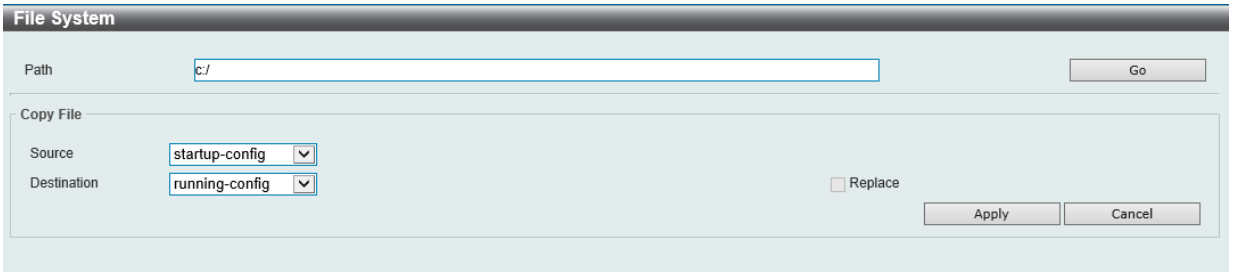


図 7-44　File System – Copy 画面

画面に表示される項目：

項目	説明
Source	コピー元のファイルの種類を選択します。 • 選択肢：「startup-config」「Image 1」「Image 2」「Configuration 1」「Configuration 2」
Destination	コピー先のファイルの種類を選択します。「Replace」にチェックを入れると、現在実行中のコンフィグファイルを指定のコンフィグファイルと差し替えます。 • 選択肢：「running-config」「startup-config」「Image 1」「Image 2」「Configuration 1」「Configuration 2」

「Apply」をクリックして、コピーを開始します。

「Cancel」をクリックすると処理は破棄されます。

起動ファイルの指定

「Boot File」をクリックすると、以下の画面が表示されます。

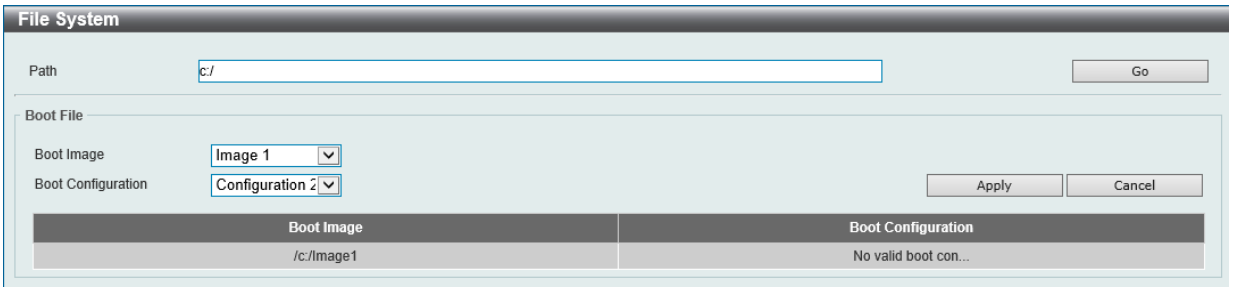


図 7-45　File System – Boot File 画面

画面に表示される項目：

項目	説明
Boot Image	ブートイメージファイルを選択します。 • 選択肢：「Image 1」「Image 2」
Boot Configuration	ブートコンフィグファイルを選択します。 • 選択肢：「Configuration 1」「Configuration 2」

「Apply」をクリックして、設定を適用します。

「Cancel」をクリックすると入力内容は破棄されます。

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

DDP Settings（DDP 設定）

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

Management > D-Link Discovery Protocol > DDP Settings の順にクリックし、以下の画面を表示します。

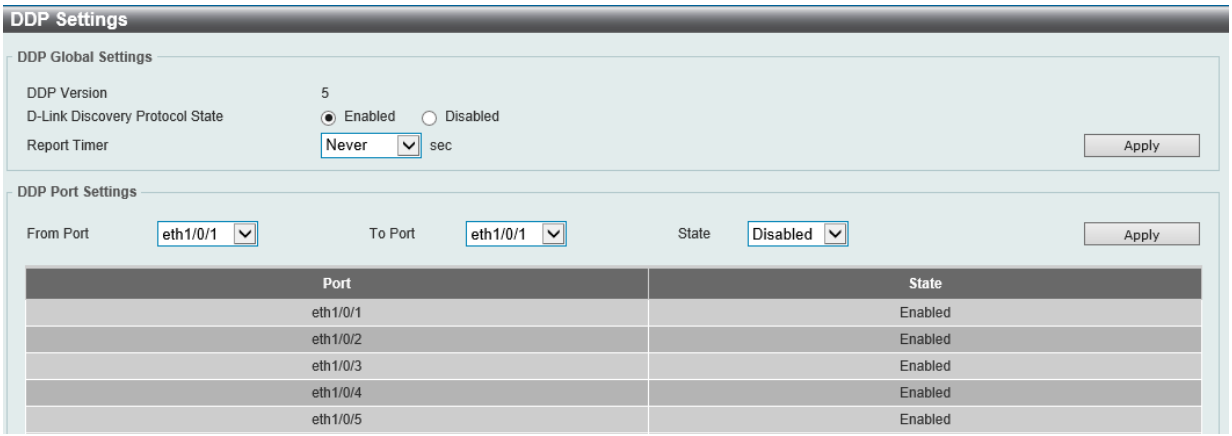


図 7-46　DDP Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

DDP Neighbors（DDP 隣接機器）

DDP 隣接機器の表示を行います。

Management > D-Link Discovery Protocol > DDP Neighbors の順にクリックし、以下の画面を表示します。

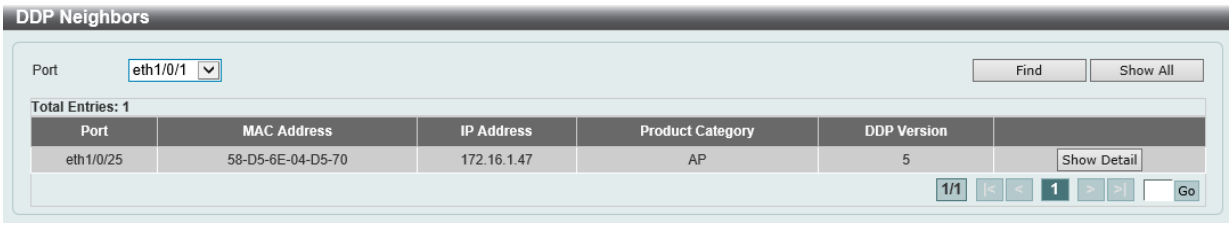


図 7-47　DDP Neighbors 画面

画面に表示される項目：

項目	説明
Port	検出対象のポートを選択します。

「Find」をクリックすると、指定したポートを介して接続している DDP 隣接機器が表示されます。
「Show All」をクリックすると、本スイッチに接続しているすべての DDP 隣接機器が表示されます。
「Show Detail」をクリックすると、エントリの詳細情報が表示されます。

第 8 章　L2 Features（レイヤ 2 機能の設定）

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

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

サブメニュー	説明
FDB（FDB 設定）	FDB（Forwarding DataBase）フォワーディングデータベースの設定を行います。
VLAN（VLAN 設定）	VLAN の表示、設定を行います。
STP（スパニングツリーの設定）	スパニングツリープロトコル（STP）設定を行います
Loopback Detection（ループバック検知設定）	ループバック検知（LBD）機能の設定を行います。
Link Aggregation（リンクアグリゲーション）	Link Aggregation（リンクアグリゲーション / ポートトランキング機能）の設定を行います。
L2 Multicast Control（L2 マルチキャストコントロール）	IGMP（Internet Group Management Protocol）Snooping 機能始めとした L2 Multicast Control（L2 マルチキャストコントロール）の設定を行います。
LLDP（LLDP 設定）	LLDP（Link Layer Discovery Protocol）の設定を行います。

FDB（FDB 設定）

補足　FDB で登録可能な MAC アドレス数は 32K です。

Static FDB（スタティック FDB 設定）

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

スイッチにスタティックなユニキャストフォワーディングを設定します。

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

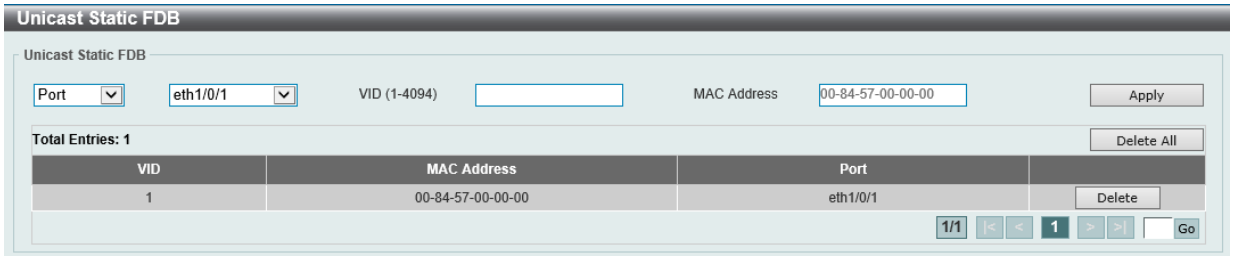


図 8-1　Unicast Static FDB 設定

画面に表示される項目：

項目	説明
Port/Drop	指定 MAC アドレスのあるポート番号を指定します。 また、本オプションはユニキャストのスタティック FDB から MAC アドレスを削除することもできます。 • 「Port」- 指定 MAC アドレスのあるポート番号を指定します。 • 「Drop」- ユニキャストのスタティック FDB から MAC アドレスを破棄します。
Port Number	「Port」を選択した場合、ポート番号を入力します。
VID	関連するユニキャスト MAC アドレスが存在する VLAN ID を入力します。
MAC Address	パケットがスタティックに送信される宛先の MAC アドレスを入力します。ユニキャスト MAC アドレスを指定します。

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

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

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

スイッチの MAC アドレステーブルの設定を行います。

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

Global Settings（グローバル設定タブ）

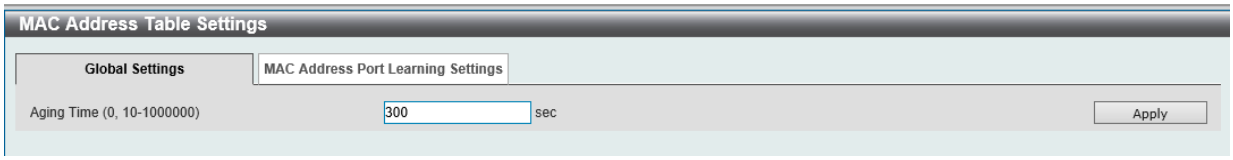


図 8-2　MAC Address Table Settings - Global Settings タブ画面

画面に表示される項目：

項目	説明
Aging Time	MAC アドレステーブルのエージングタイムを入力します。 設定した時間中にアクセスのない端末について、学習した MAC アドレスを MAC アドレステーブルから削除します。 • 設定可能範囲：10-1000000（秒） • 初期値：300（秒） 0 に設定した場合、学習した MAC アドレスは削除されません。

「Apply」をクリックして、設定内容を適用します。

MAC Address Port Learning（MAC アドレスポートラーニングタブ）

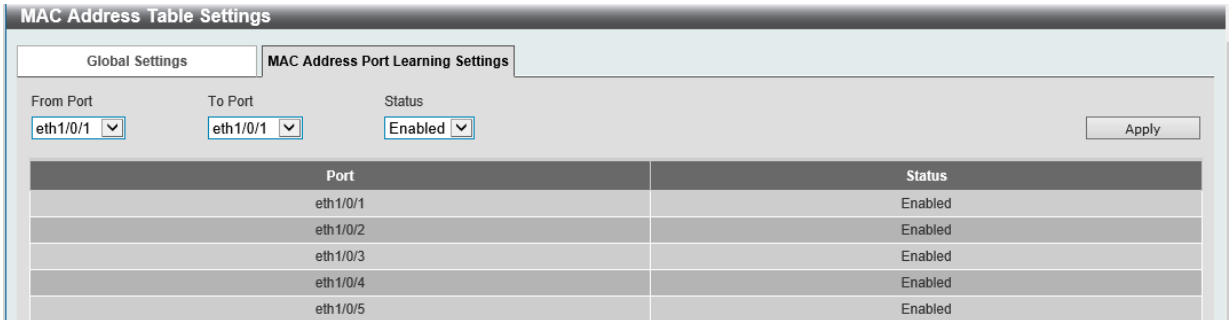


図 8-3　MAC Address Table Settings - MAC Address Port Learning タブ画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Status	指定したポートの MAC アドレスラーニングを有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

注意　MAC アドレスポートラーニングが無効の場合、未学習の送信元 MAC アドレスのパケットはフラッディングされます。学習済みの MAC アドレスはエージアウトまで保持されます。

MAC Address Table（MAC アドレステーブル）

スイッチの MAC アドレスフォワーディングテーブルを参照します。

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

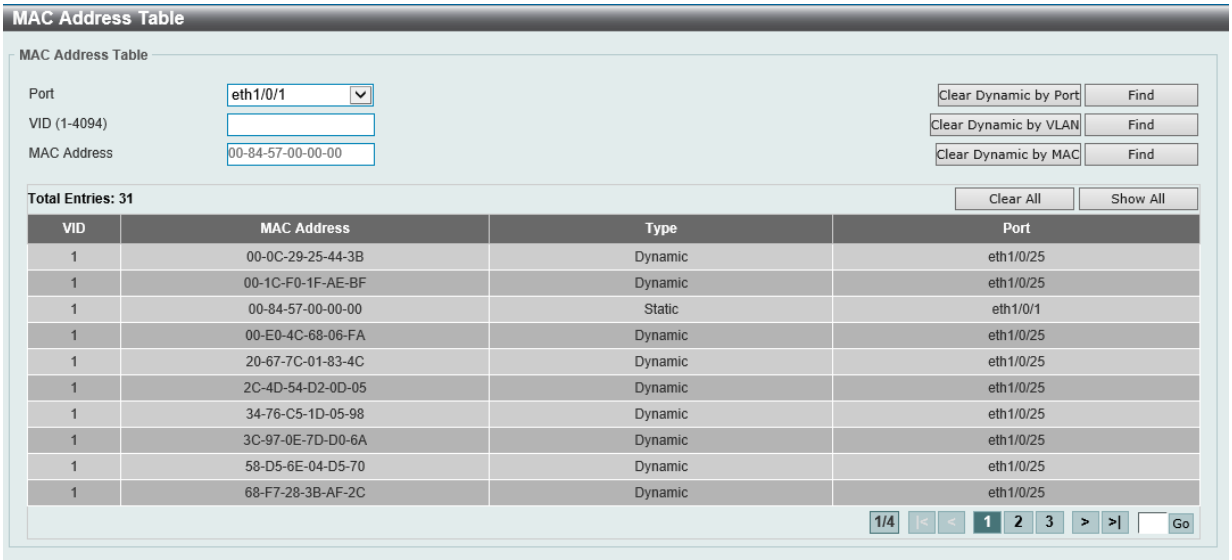


図 8-4　MAC Address Table 画面

画面に表示される項目：

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

エントリの検索 / 表示

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

ダイナミックエントリの削除

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

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

MAC Notification（MAC 通知設定）

MAC Notification（通知）の表示、設定を行います。

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

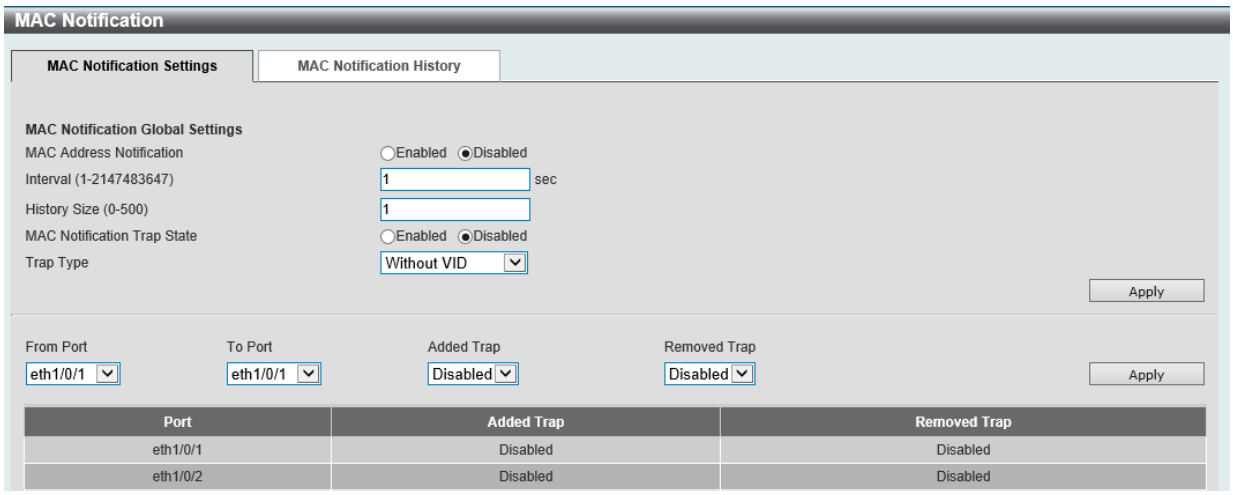


図 8-5　MAC Notification - MAC Notification Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

MAC Notification History タブ

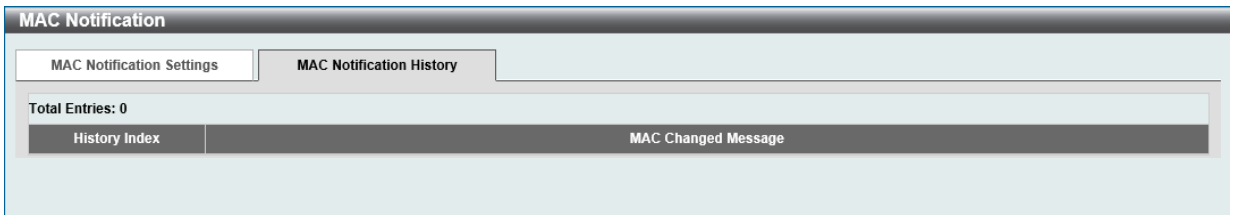


図 8-6　MAC Notification - MAC Notification History 画面

MAC 通知メッセージの履歴が表示されます。

VLAN について

IEEE 802.1p プライオリティについて

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

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

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

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

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

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

VLAN とは

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

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

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

本スイッチシリーズにおける VLAN について

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

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

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

IEEE 802.1Q VLAN

用語の説明

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

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

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

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

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

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

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

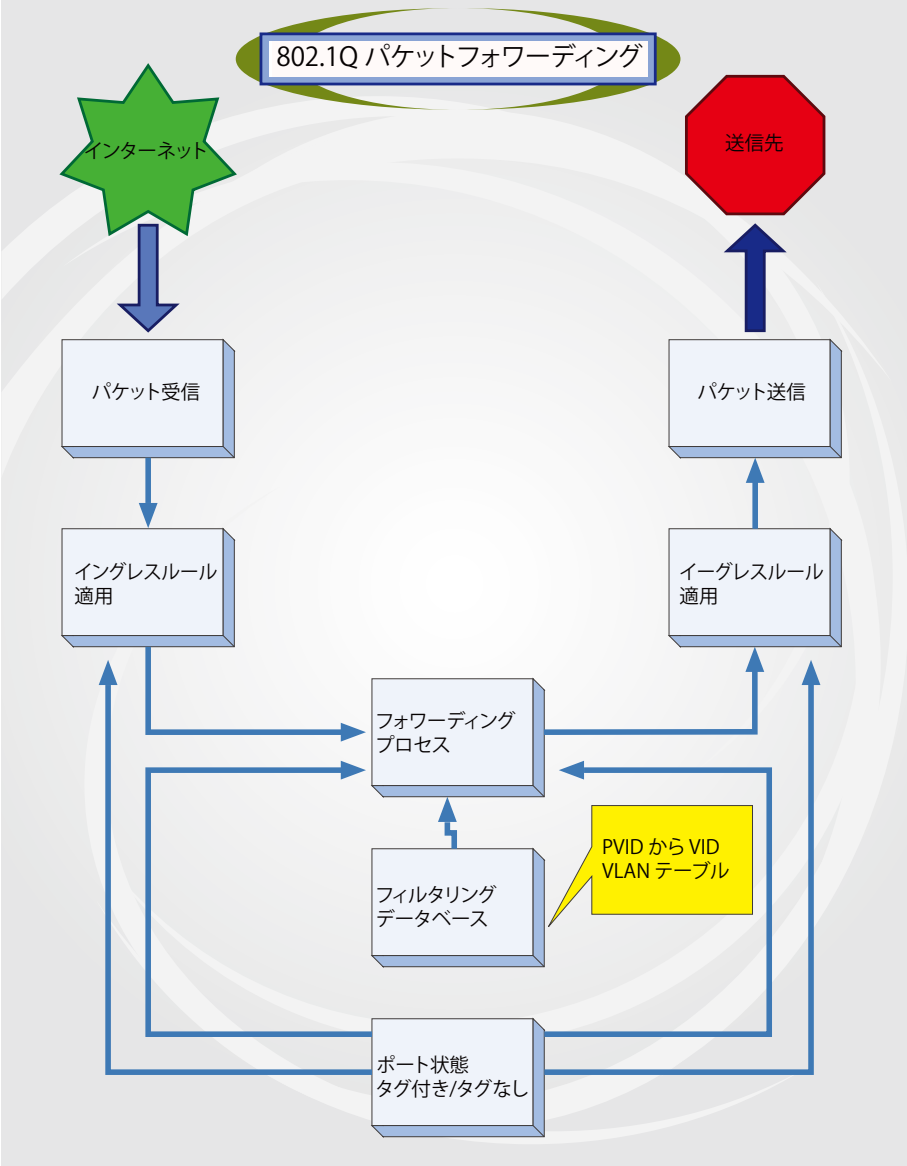


図 8-1　IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

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

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

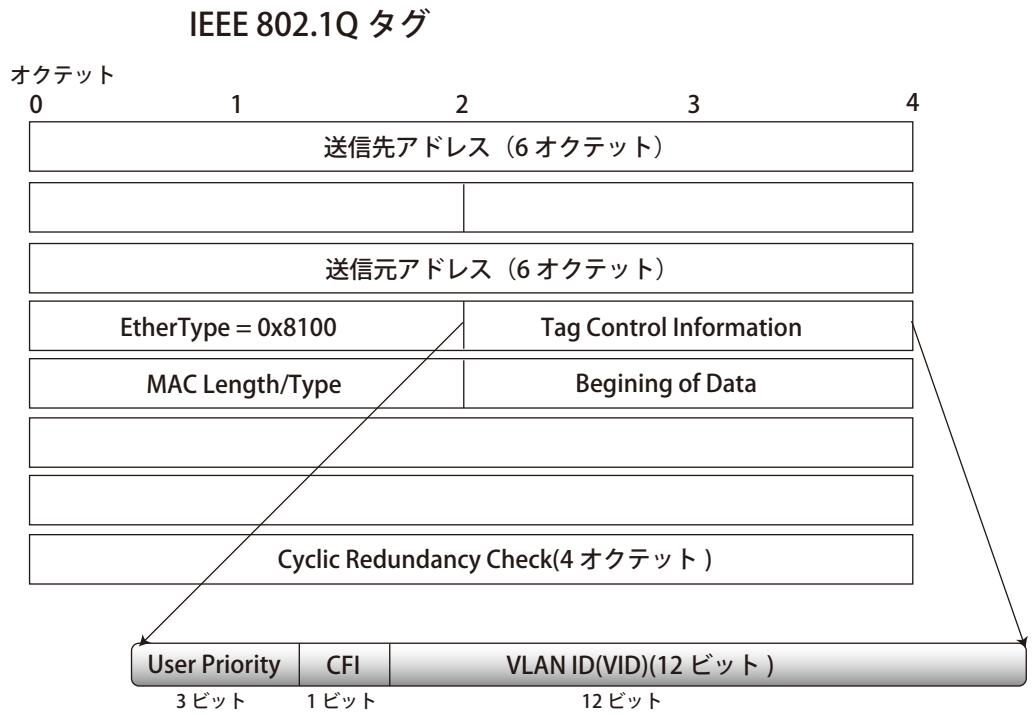


図 8-2　IEEE 802.1Q タグ

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

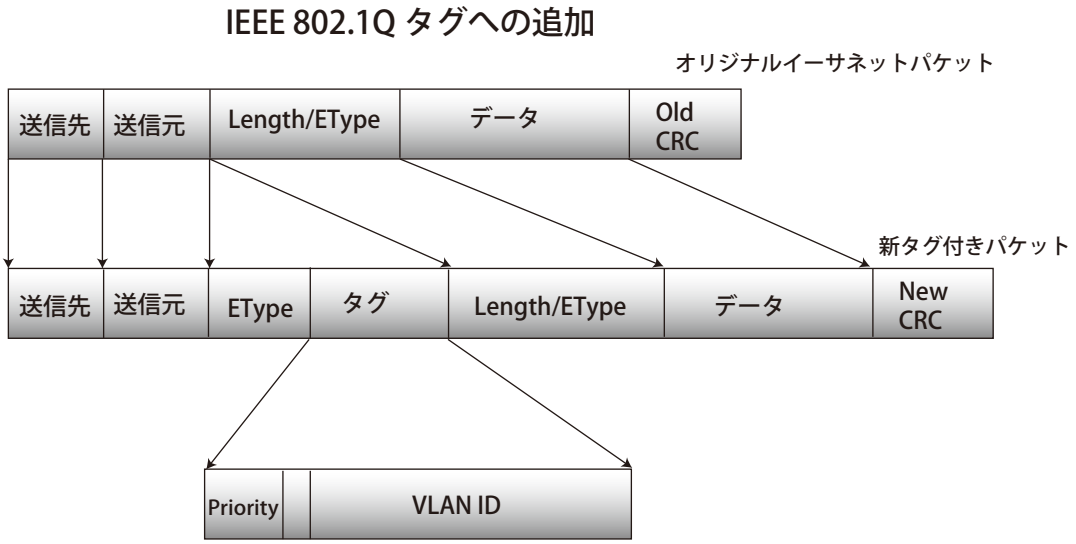


図 8-3　IEEE 802.1Q タグの挿入

ポート VLAN ID

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

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

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

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

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

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

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

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

タグ付きとタグなし

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

イングレスフィルタリング

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

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

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

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

デフォルト VLAN

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

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

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

VLAN の設定例を以下に示します。

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

ポートベース VLAN

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

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

VLAN セグメンテーション

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

VLAN（VLAN 設定）

スイッチの VLAN 設定を行います。

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

ウィザードを使用して VLAN の作成と設定を行います。

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

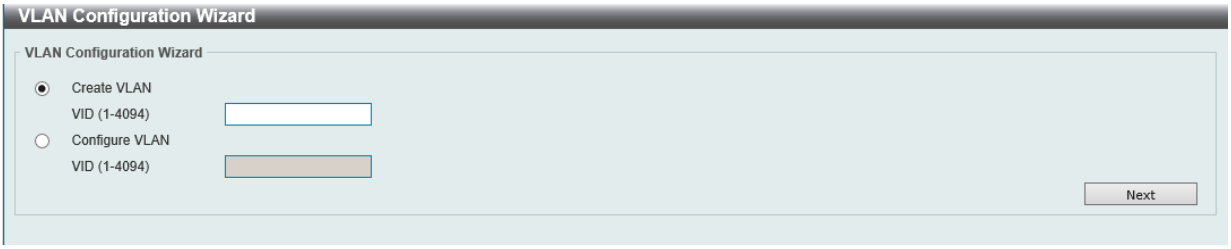


図 8-4　VLAN Configuration Wizard 画面

画面に表示される項目：

項目	内容
Create VLAN	新しく VLAN を作成する場合に選択します。 • 設定可能範囲：2-4094 VID 1 は default VLAN に設定されているため、本項目では入力できません。
Configure VLAN	作成済みの VLAN を設定する場合に選択します。 • 設定可能範囲：1-4094

「Next」をクリックし、以下の画面で設定を行います。

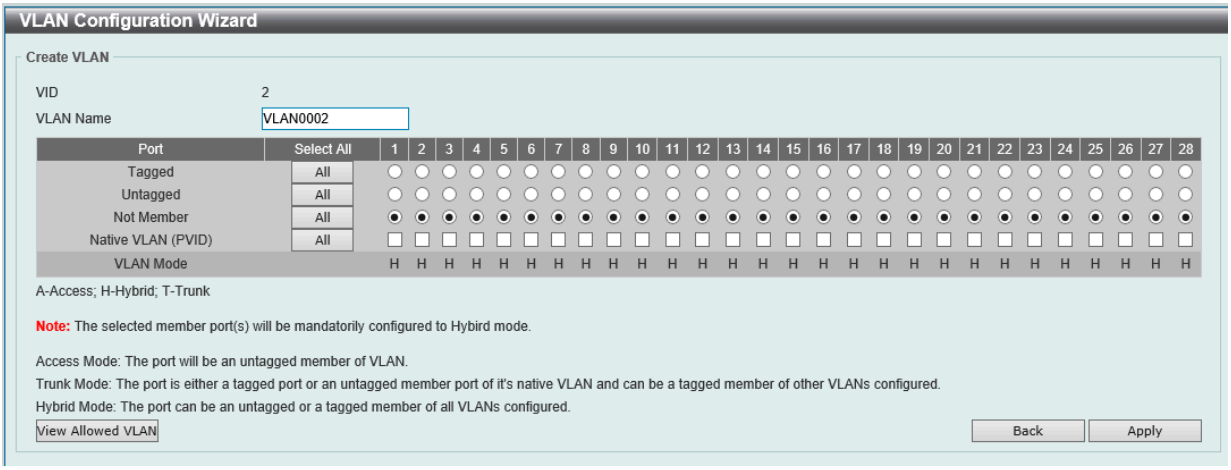


図 8-5　VLAN Configuration Wizard 画面

画面に表示される項目：

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

項目	内容
VLAN Mode	各ポートの VLAN モードが表示されます。 アルファベットの表示は以下のモードを表します。 • A：Access モード ポートは VLAN のタグなしメンバになります。 • H：Hybrid モード ポートは設定されているすべての VLAN のタグなしまたはタグ付きメンバにすることができます。 • T：Trunk モード ポートはネイティブ VLAN のタグ付きポートまたはタグなしメンバポートのいずれかであり、設定されている他の VLAN のタグ付きメンバにすることができます。
View Allowed VLAN	許可された VLAN の一覧が別ウィンドウで表示されます。

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

802.1Q VLAN（802.1Q VLAN 設定）

802.1Q VLAN を設定します。

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

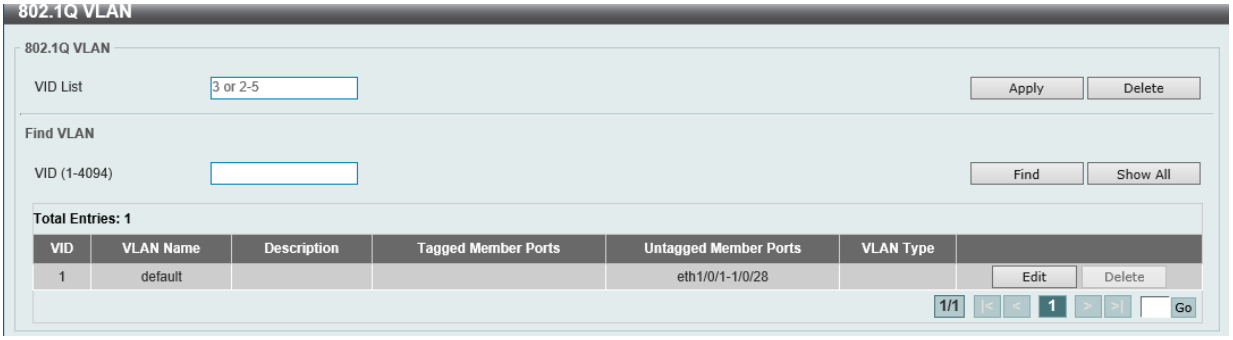


図 8-6　802.1Q VLAN 画面

画面に表示される項目：

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

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

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

VLAN Interface（VLAN インタフェース設定）

VLAN インタフェースの設定を行います。

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

VLAN Interface（VLAN インタフェース設定）

「VLAN Interface Settings」タブでは、各ポートの VLAN インタフェース設定の確認、および編集を実行できます。

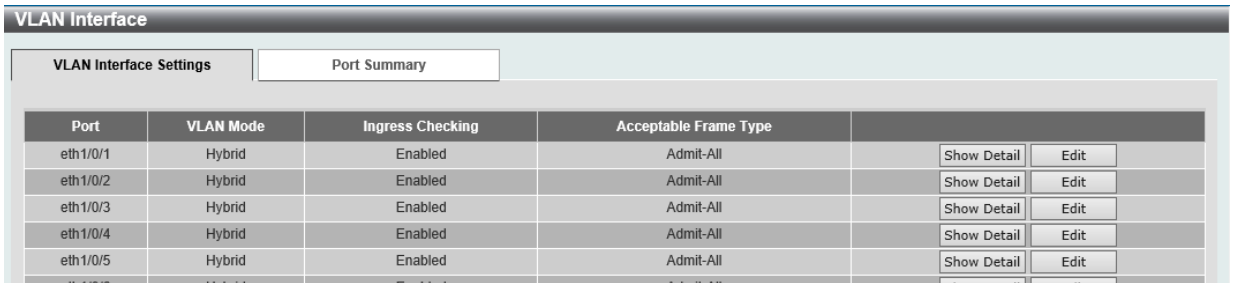


図 8-7　VLAN Interface 画面

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

■ VLAN 詳細情報の表示

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

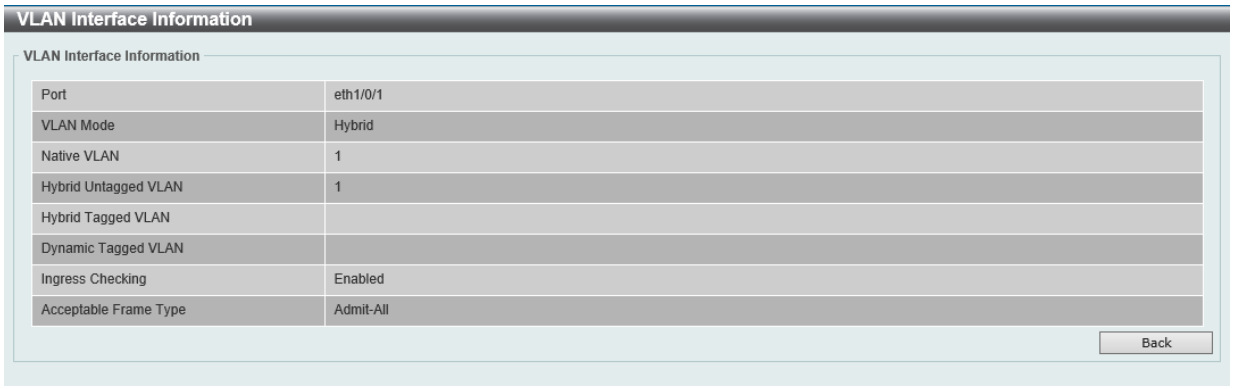


図 8-8　VLAN Interface Information 画面

「Back」をクリックすると前画面に戻ります。

■ Edit（VLAN インタフェース設定の編集）

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

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

- 「Access」「Hybrid」「Trunk」

● VLAN モード「Access」を選択した場合：

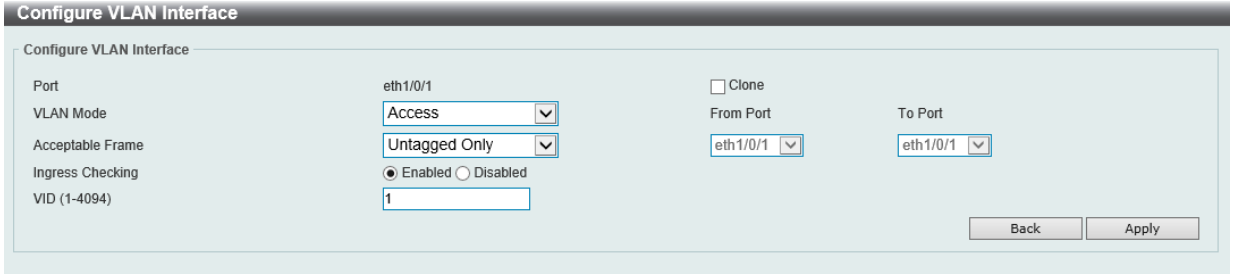


図 8-9　Configure VLAN Interface - Access 画面

画面に表示される項目：

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

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

● **VLAN モード「Hybrid」を選択した場合：**

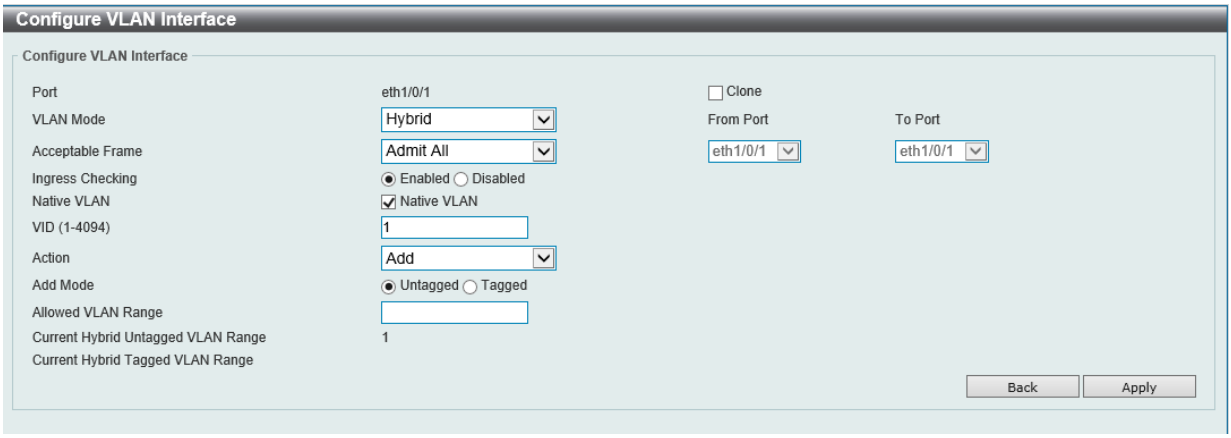


図 8-10　Configure VLAN Interface - Hybrid 画面

画面に表示される項目：

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

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

● **VLAN モード「Trunk」を選択した場合：**

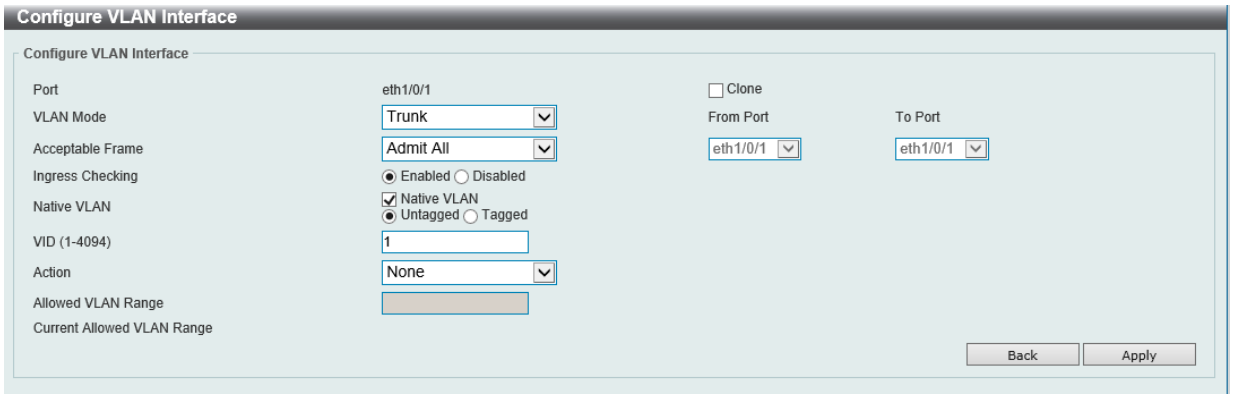


図 8-11　Configure VLAN Interface - Trunk 画面

画面に表示される項目：

項目	説明
Port	選択したポートが表示されます。
VLAN Mode	VLAN モードを選択します。ここでは「Trunk」を選択します。
Acceptable Frame	許可するフレームの種類を選択します。 • 選択肢：「Tagged Only」「Untagged Only」「Admit All」
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	Native VLAN を有効にします。「Untagged」または「Tagged」フレームを選択します。
VID	Native VLAN を有効にした場合は、設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
Action	実行する動作を選択します。 • 選択肢：「All」「Add」「Remove」「Except」「Replace」
Allowed VLAN Range	許可される VLAN 範囲を指定します。
Clone	クローン機能を有効にして、設定内容を他のポートにコピーします。
From Port / To Port	設定内容をコピーするポートの範囲を指定します。

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

Port Summary（ポートサマリ）

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

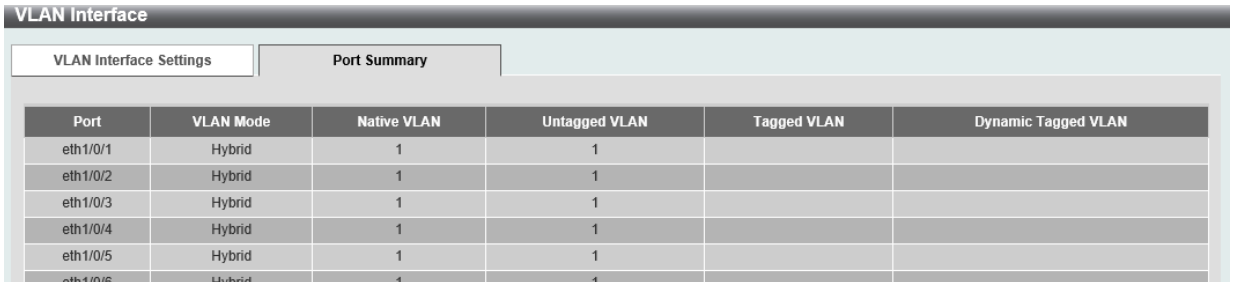


図 8-12　VLAN Interface - Port Summary 画面

Asymmetric VLAN（Asymmetric VLAN 設定）

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

補足　Asymmetric VLAN は、重複する全 VLAN に学習した MAC アドレスを乗せる事により、異なる Native VLAN 間の フラッディングを抑止します。

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

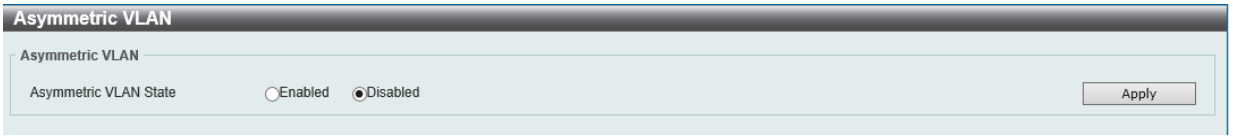


図 8-13　Asymmetric VLAN 画面

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

「Apply」をクリックして、設定内容を適用します。

L2VLAN Interface Description（L2 VLAN インタフェース概要）

L2 VLAN インタフェースについて表示、設定を行います。

L2 Features > VLAN > L2VLAN Interface Description の順にクリックし、次の画面を表示します。

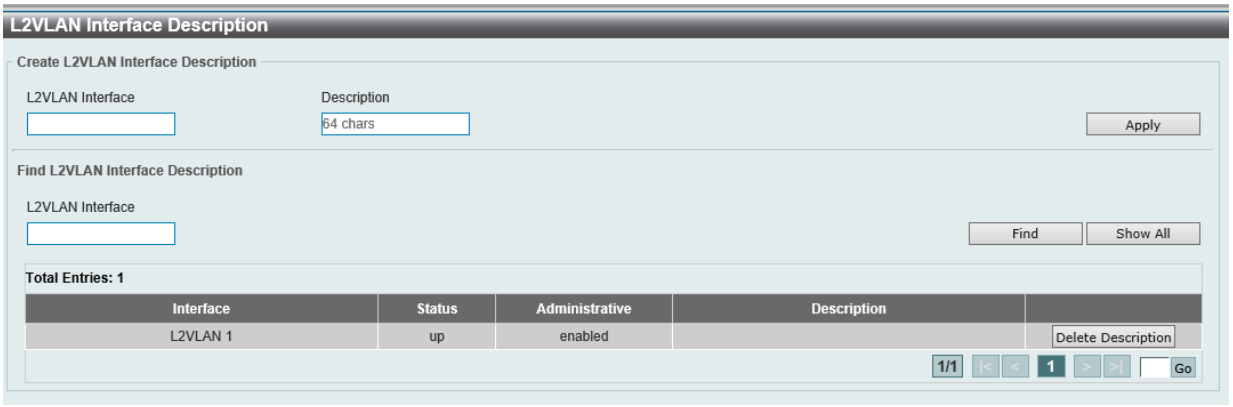


図 8-14　L2VLAN Interface Description 画面

画面に表示される項目：

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

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

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

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

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

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

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

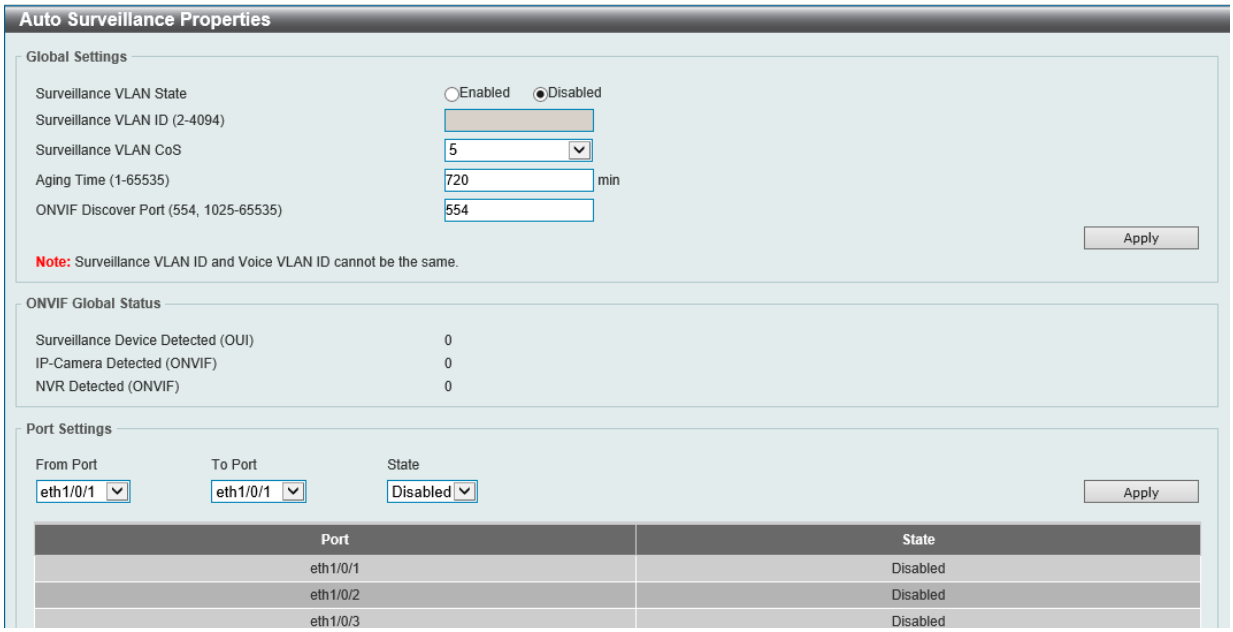


図 8-15　Auto Surveillance Properties 画面

画面に表示される項目：

項目	説明
Global Settings	
Surveillance VLAN State	サーベイランス VLAN を有効 / 無効に設定します。
Surveillance VLAN ID	サーベイランス VLAN の VLAN ID を指定します。 VLAN をサーベイランス VLAN に割り当てる前に、通常の VLAN として作成する必要があります。 • 設定可能範囲：2 - 4094
Surveillance VLAN CoS	サーベイランス VLAN の優先値を指定します。 サーベイランス VLAN が有効化されたポートで受信したサーベイランスパケットは、この CoS 値でマークされます。これにより、QoS データトラフィックとは区別されます。 • 設定可能範囲：0 - 7
Aging Time	エージングタイムを設定します。 本機能は、サーベイランス VLAN ダイナミックメンバポートのエージングタイムを設定するために使用されます。サーベイランスデバイスがトラフィックの送信を停止し、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。 サーベイランストラフィックがエージングタイム内に再開すると、エージングタイマはキャンセルされます。 • 設定可能範囲：1-65535（分）
ONVIF Discover Port	ONVIF Discover ポートを設定します。 • 設定可能範囲：554、1025-65535
Port Settings	
From Port / To Port	設定するポートの範囲を指定します。
State	指定したポートでサーベイランス VLAN を有効 / 無効に設定します。 サーベイランス VLAN が有効な場合、ポートはアンタグのサーベイランス VLAN メンバとして自動的に学習され、受信したアンタグのサーベイランスパケットはサーベイランス VLAN に転送されます。受信したパケットの送信元 MAC アドレスが OUI（Organizationally Unique Identifier）アドレスに一致している場合、そのパケットはサーベイランスパケットとして認識されます。

「Apply」をクリックして、設定内容を適用します。

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

サーベイランスデバイスの表示と MAC アドレスの設定を行います。

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

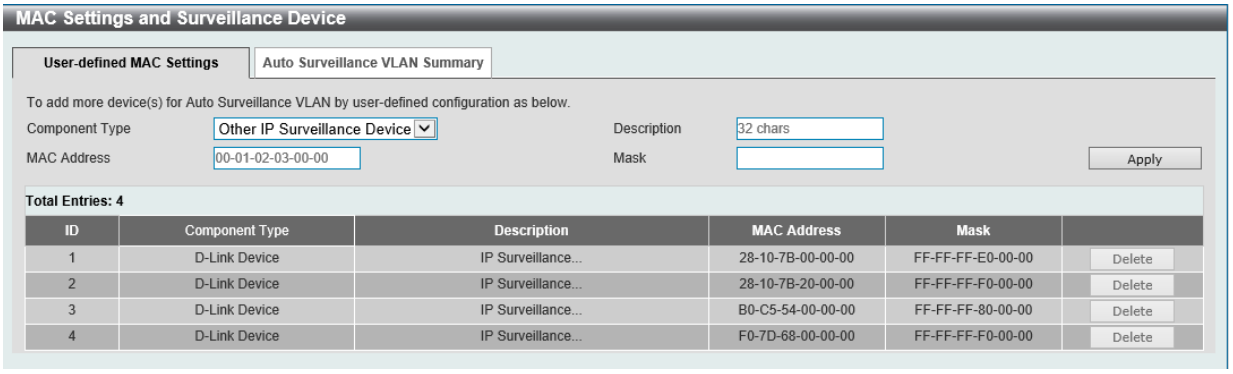


図 8-16　MAC Settings and Surveillance Device - User-defined MAC Settings 画面

画面に表示される項目：

項目	説明
Component Type	サーベイランス VLAN が自動検出可能なサーベイランスコンポーネントを選択します。 • 選択肢： 「Video Management Server」「VMS Client/Remote Viewer」「Video Encoder」「Network Storage」 「Other IP Surveillance Device」
Description	ユーザ定義の OUI に関する説明を入力します。（32 文字以内）
MAC Address	ユーザ定義の OUI MAC アドレスを入力します。 受信パケットの MAC アドレスが OUI パターンにいずれかと一致すると、そのパケットはサーベイランスパケットとして識別されます。
Mask	ユーザ定義の OUI MAC アドレスマスクを入力します。

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

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。

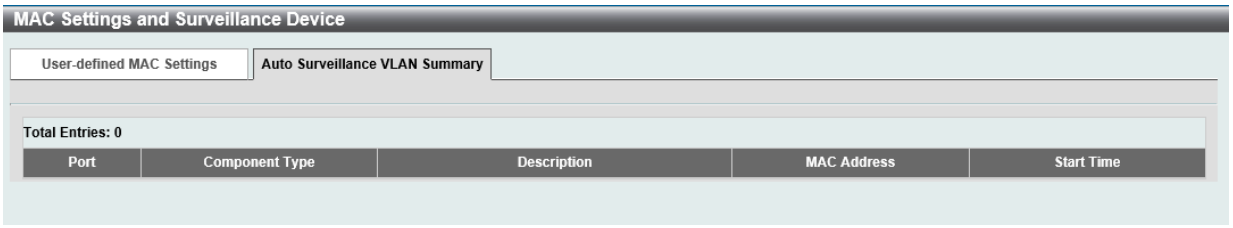


図 8-17　MAC Settings and Surveillance Device - Auto Surveillance VLAN Summary 画面

ONVIF IP-Camera Information（ONVIF IP カメラ情報）

ONVIF IP カメラの情報を表示します。

L2 Features > VLAN > Auto Surveillance VLAN > ONVIF IP-Camera Information をクリックし、以下の画面を表示します。

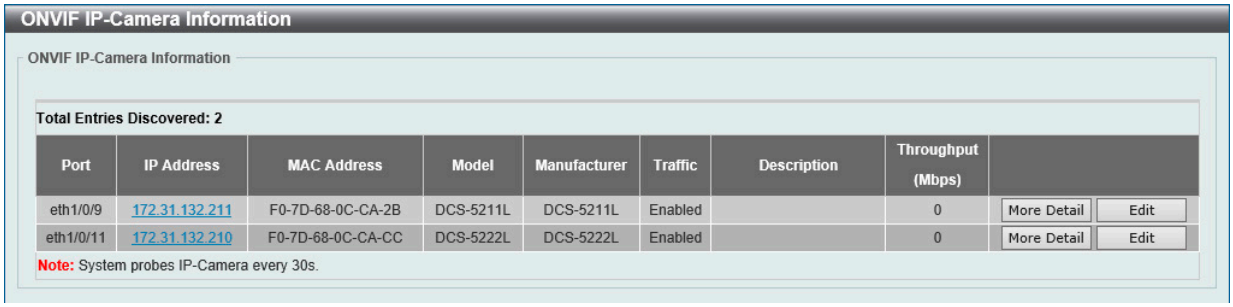


図 8-18　ONVIF IP-Camera Information 画面

「More Detail」をクリックすると接続している IP カメラについてより詳しい情報を表示します。
「Edit」をクリックすると該当の IP カメラの有効 / 無効と、説明を設定できます。

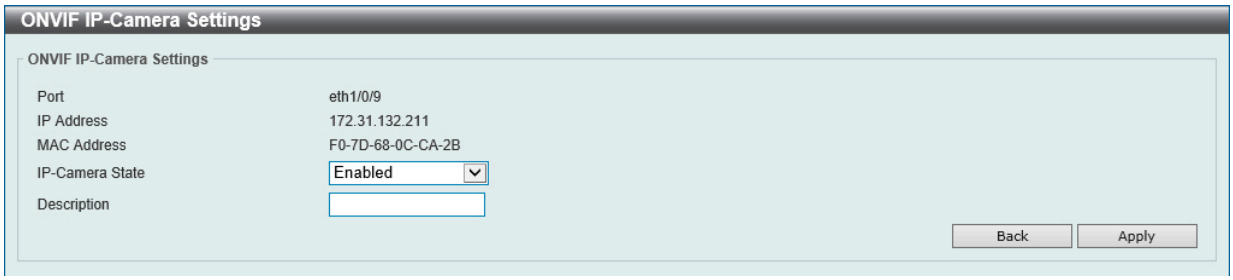


図 8-19　ONVIF IP-Camera Information（Edit）画面

画面に表示される項目：

項目	説明
IP-Camera State	IP カメラを有効 / 無効に指定します。
Description	IP カメラの概要を入力します。

「Apply」をクリックして、設定内容を適用します。
「Back」をクリックし、前画面にもどります。

「More Detail」をクリックするとより詳細な情報が表示されます。

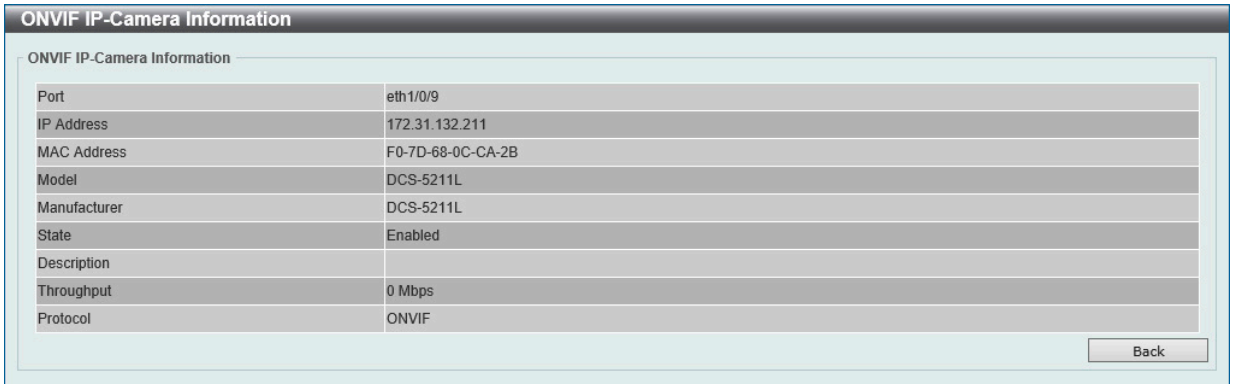


図 8-20　ONVIF IP-Camera Information（More Detail）画面

ONVIF NVR Information（ONVIF NVR 情報）

ONVIF VLAN で検出された NVR（Network Video Recorder）機器を表示します。

L2 Features > VLAN > Auto Surveillance VLAN > ONVIF NVR Information をクリックし、以下の画面を表示します。

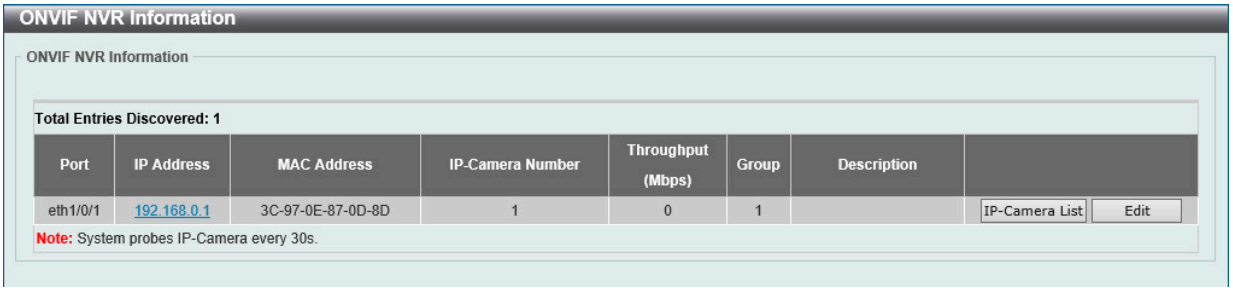


図 8-21　ONVIF NVR Information 画面

NVR の IP アドレスをクリックすると接続している NVR の Web インタフェースを表示します。
「IP-Camera List」をクリックすると NVR に接続している IP カメラのリストを表示します。

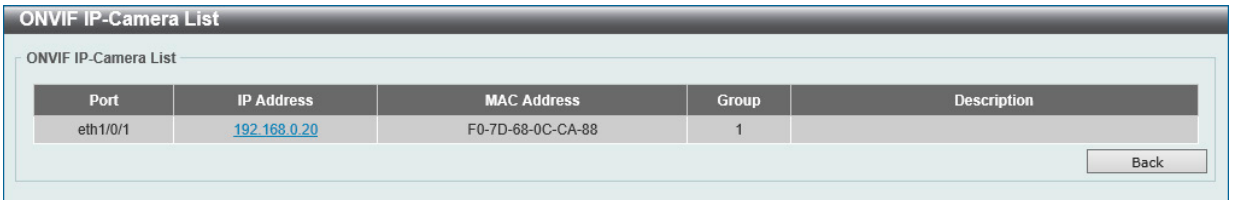


図 8-22　ONVIF NVR Information（IP-Camera List）画面

IP カメラの IP アドレスをクリックするとカメラの Web インタフェースを表示します。
「Back」をクリックし、前画面にもどります。

「Edit」をクリックすると該当の NVR についての設定を行います。

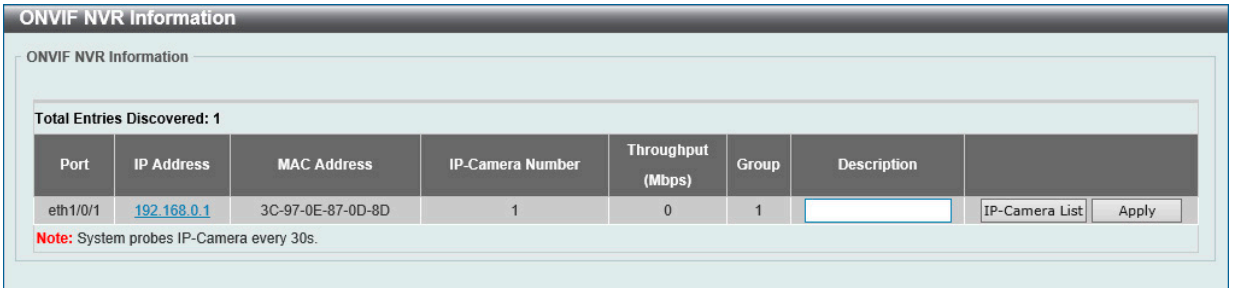


図 8-23　ONVIF NVR Information（Edit）画面

画面に表示される項目：

項目	説明
Description	NVR の概要を入力します。

「Apply」をクリックして、設定内容を適用します。

Voice VLAN（音声 VLAN）

Voice VLAN Global（音声 VLAN グローバル設定）

音声 VLAN の設定を行います。本スイッチの音声 VLAN は 1 つのみです。

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

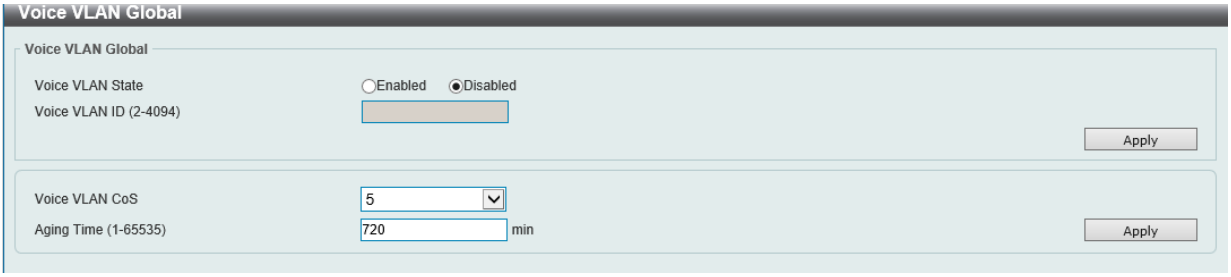


図 8-24　Voice VLAN Global 画面

画面に表示される項目：

項目	説明
Voice VLAN State	音声 VLAN 機能を有効 / 無効に設定します。
Voice VID	音声 VLAN の VLAN ID を入力します。指定する VLAN は事前に作成しておく必要があります。 • 設定可能範囲：2-4094
Voice VLAN CoS	音声 VLAN の優先度を設定します。音声 VLAN が有効化されたポートで受信した音声パケットは、この CoS 値でマークされます。これにより、QoS データトラフィックとは区別されます。 • 設定可能範囲：0-7
Aging Time	自動学習された音声デバイスと音声 VLAN 情報のエージングタイム を設定します。 音声デバイスがトラフィックの送信を停止し、この音声デバイスの MAC アドレスがエージングタイムに到達すると、音声 VLAN エージングタイマが開始されます。 ポートは音声 VLAN のエージングタイム経過後に音声 VLAN から削除されます。音声トラフィックがエージングタイム内に再開すると、エージングタイマはキャンセルされます。 • 設定可能範囲：1-65535（分）

「Apply」をクリックして、設定内容を適用します。

Voice VLAN Port（音声 VLAN ポート設定）

ポートの音声 VLAN 設定を行います。

L2 Features > 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。

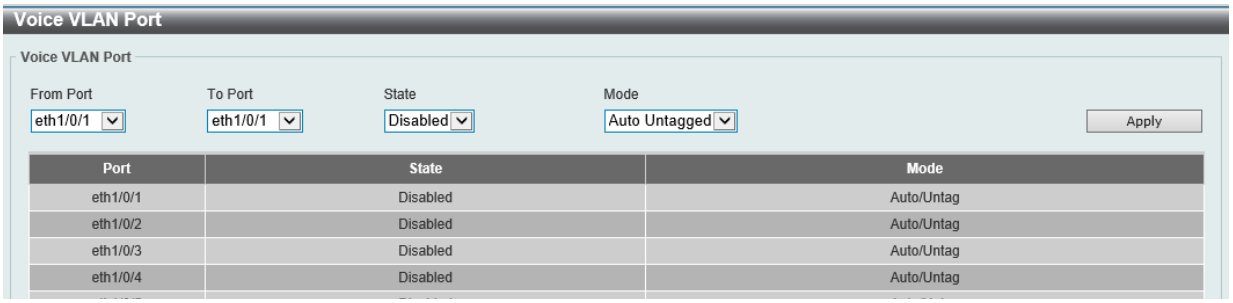


図 8-25　Voice VLAN Port 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
State	指定ポートの音声 VLAN 機能を有効 / 無効に設定します。 音声 VLAN が有効になると、受信した音声パケットは音声 VLAN として送信されます。受信した音声 VLAN パケットの送信元 MAC アドレスが OUI アドレスに一致すると、音声 VLAN と認識されます。
Mode	モードを選択します。 • 「Auto Untagged」- タグなしの音声 VLAN メンバシップが自動的に学習されます。 • 「Auto Tagged」- タグ付きの音声 VLAN メンバシップが自動的に学習されます。 • 「Manual」- 音声 VLAN メンバシップを手動で設定します。 指定ポートで自動学習が有効化されている場合、音声 VLAN メンバは自動的に学習され、エージアウトします。 「Auto Tagged」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、タグ付きメンバとして音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなしパケットは Port VLAN ID（PVID）で転送されます。 「Auto Untagged」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、タグなしメンバとして音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなしパケットは音声 VLAN で転送されます。 スイッチが LLDP-MED パケットを受信した場合、VLAN ID、Tagged フラグ、優先度フラグがチェックされます。スイッチは Tagged フラグ、優先度フラグに従います。

「Apply」をクリックして、設定内容を適用します。

Voice VLAN OUI（音声 VLAN OUI 設定）

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

L2 Features > 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。

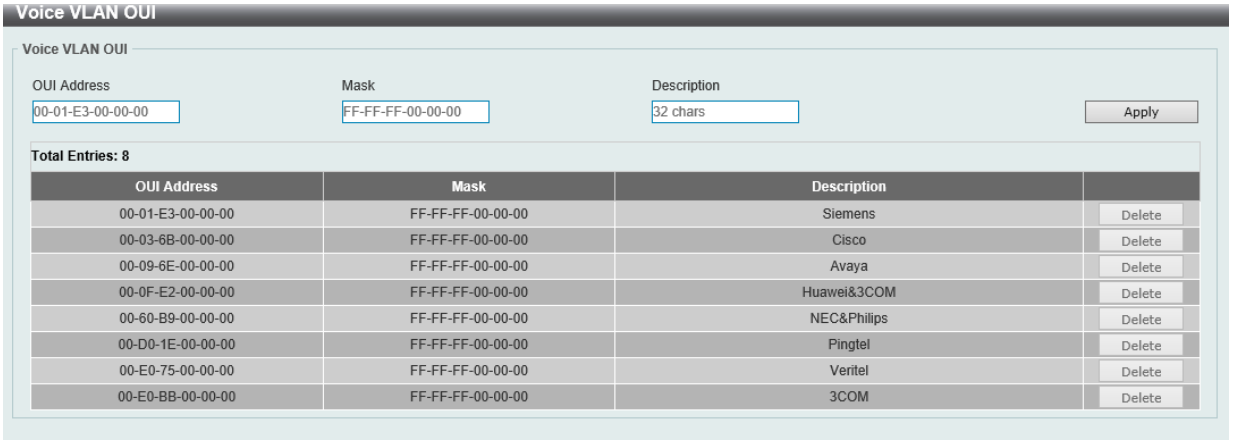


図 8-26　Voice VLAN OUI 画面

画面に表示される項目：

項目	説明
OUI Address	ユーザ定義の OUI MAC アドレスを入力します。
Mask	ユーザ定義の OUI MAC アドレスマスクを入力します。
Description	ユーザ定義の OUI に関する説明を入力します。（32 文字以内）

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

Voice VLAN Device（音声 VLAN デバイス）

ポートに接続する音声デバイスを表示します。

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。

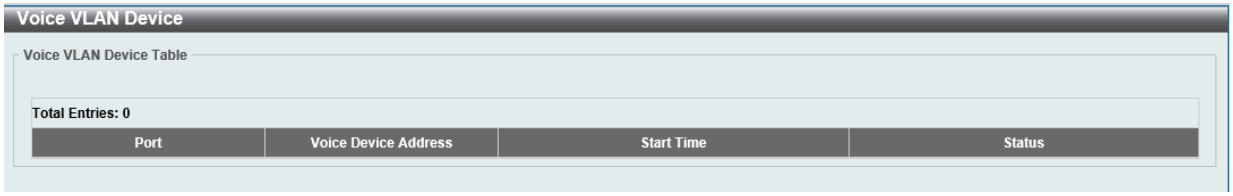


図 8-27　Voice VLAN Device 画面

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

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

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

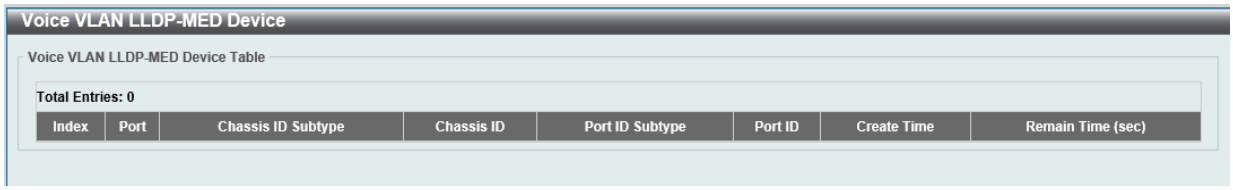


図 8-28　Voice VLAN LLDP-MED Device 画面

STP（スパニングツリーの設定）

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

802.1Q-2005 MSTP

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

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

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

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

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

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

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

802.1D-2004 Rapid Spanning Tree

本スイッチは、IEEE 802.1Q-2005 に定義される MSTP（Multiple STP Protocol）、IEEE 802.1D-2004 に定義される RSTP（Rapid STP Protocol）、および 802.1D-1998 で定義される STP（STP Protocol）の 3 つのプロトコルを実装しています。RSTP は IEEE 802.1D-1998 をサポートするレガシー機器との併用が可能ですが、その場合 RSTP を使用する利点は失われます。本項では、スパニングツリーの新しいコンセプトと、これらのプロトコル間の主な違いについて説明します。

ポートの状態遷移

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

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

ポート状態の比較

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

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

Edge Port

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

P2P Port

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

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

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

2 つのレベルで動作するスパニングツリープロトコル

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

STP Global Settings（STP グローバル設定）

STP をグローバルに設定します。

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

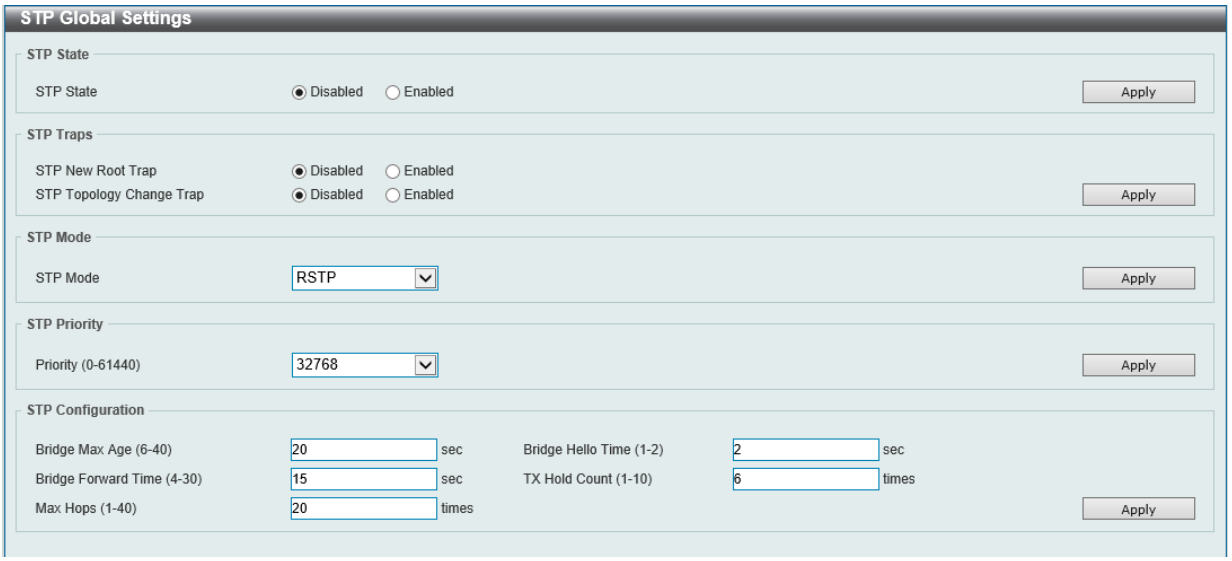


図 8-29　STP Global Settings 画面

画面に表示される項目：

項目	説明
STP State	
STP State	STP のグローバルステータスを有効 / 無効に設定します。
STP Trap	
STP New Root Trap	新しいルートトラップ送信を有効 / 無効に設定します。
STP Topology Change Trap	トポロジ変更トラップ送信を有効 / 無効に設定します。
STP Mode	
STP Mode	スイッチで使用する STP のバージョンを選択します。 • 「STP」- スイッチ上で STP がグローバルに使用されます。 • 「RSTP」- スイッチ上で RSTP がグローバルに使用されます。 • 「MSTP」- スイッチ上で MSTP がグローバルに使用されます。
STP Priority	
Priority	STP 優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0 - 61440 • 初期値：32768
STP Configuration	
Bridge Max Age	ブリッジの最大エージタイマを設定します。本項目は、古い情報がネットワーク内の冗長パスを無限に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。この値はルートブリッジによりセットされ、ブリッジで相互接続された LAN 内のデバイスと本スイッチの STP 設定値が整合性を持っていることを確認します。 • 設定可能範囲：6-40（秒） • 初期値：20（秒）
Bridge Hello Time	Bridge Hello タイムを入力します。ルートブリッジは、他のスイッチに自身がルートブリッジであることを示すために BPDU パケットを送信します。本値は、BPDU パケットの送信間隔です。「STP Mode」で STP または RSTP が選択された場合にのみ本項目が表示されます。MSTP については、Hello Time はポートごとに設定される必要があります。 • 設定可能範囲：1 - 2（秒） • 初期値：2（秒）
Bridge Forward Time	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間、本値で指定した時間 Listening 状態を保ちます。 • 設定可能範囲：4 - 30（秒） • 初期値：15（秒）
TX Hold Count	Hello パケットの最大送信回数を指定します。 • 設定可能範囲：1-10（回） • 初期値：6（回）

項目	説明
Max Hops	スパニングツリー範囲のデバイス間で、スイッチが送信した BPDU パケットが破棄されるまでのホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。0 に到達すると、BPDU パケットが破棄され、ポートに保持していた情報は解放されます。 • 設定可能範囲：1 - 40 • 初期値：20

「Apply」をクリックして、設定内容を適用します。

STP Port Settings（STP ポートの設定）

STP をポートごとに設定します。

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

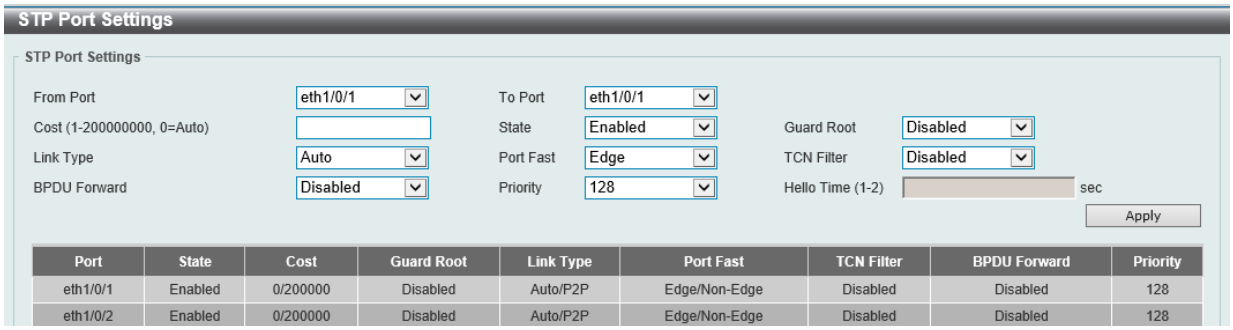


図 8-30　STP Port Setting 画面

本画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Cost （1-200000000, 0=Auto）	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。 ポートのコストは自動か、メトリックの値で設定します。 • 0（Auto）- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。（初期値） ポートコストの初期値 : 100Mbps = 200000、1 Gbps = 20000、10 Gbps = 2000、25 Gbps = 800 • 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。 数字が小さいほどパケット転送は頻繁に行われるようになります。
State	指定ポートでの STP を有効 / 無効に設定します。
Guard Root	Guard Root を有効 / 無効に設定します。
Link Type	リンクの種類を設定します。全二重ポートは P2P ポートとして判別されます。Shared 設定の場合、ポートは即時に Forwarding 状態にはなりません。 • 選択肢：「Auto」「P2P」「Shared」 • 初期値：「Auto」
Port Fast	ポートファストオプションを指定します。 • 「Network」- ポートは 3 秒だけ非ポートファスト状態に残ります。BPDU が受信されず、転送状態に移行した場合、ポートファスト状態になります。その後、BPDU を受信すると非ポートファスト状態へ戻ります。 • 「Disable」- ポートは常に非ポートファスト状態です。常に「forward-time delay」の時間待機し、転送状態へ移行します • 「Edge」- ポートは「forward-time delay」の時間を待たずに直接 STP 転送状態に移行します。インタフェースが「BPDU」を受信すると非ポートファストへ移行します。（初期値）
TCN Filter	TCN（Topology Change Notification）フィルタを有効 / 無効に設定します。 本オプションが有効な場合、ポートで受信した TC イベントは無視されます。 • 初期値：「Disabled」（無効）
BPDU Forward	BPDU パケットの転送を有効 / 無効にします。 有効にすると、受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。 • 初期値：「Disabled」（無効）
Priority	優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0 - 240 • 初期値：128
Hello Time	ハロータイムの値を指定します。この設定は指定ポートによる各設定メッセージの定期的な送信の間隔となります。 • 設定可能範囲：1- 2（秒）

「Apply」をクリックして、設定内容を適用します。

MST Configuration Identification（MST の設定）

スイッチ上に MST インスタンスの設定を行います。本設定は MSTI（マルチプルスパニングツリーインスタンス）を識別するためのものです。
スイッチは初期状態で 1 つの CIST（Common Internal Spanning Tree）を持ちます。
ユーザはパラメータを変更できますが、MSTI ID の変更 / 削除はできません。

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

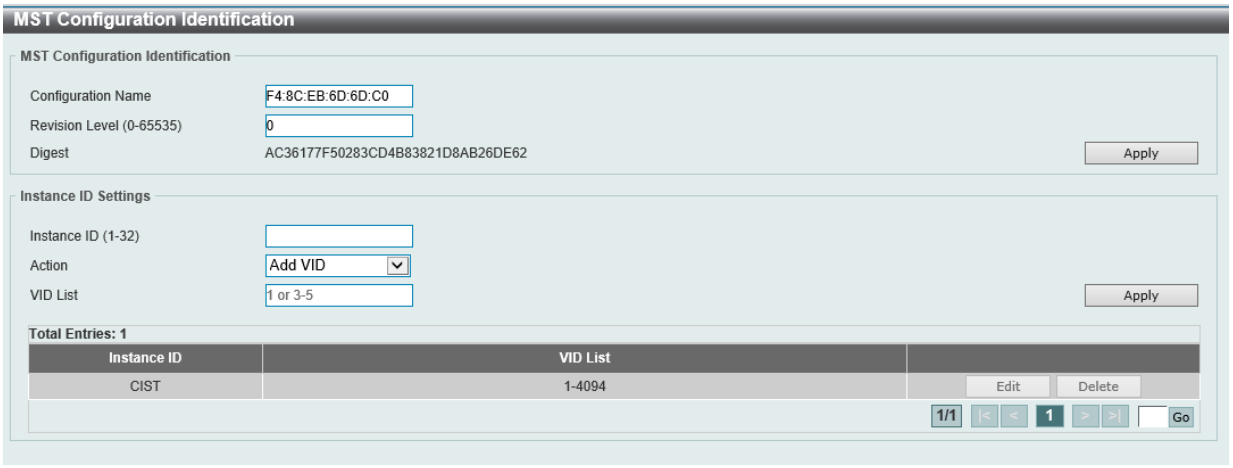


図 8-31　MST Configuration Identification 画面

画面に表示される項目：

項目	説明
MST Configuration Identification	
Configuration Name	MSTI（Multiple Spanning Tree Instance）を識別するための名前を設定します。 名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level	MST リージョンの値を設定します。 Configuration Name とともに、スイッチ上の MSTP リージョンを識別するために使用します。 • 設定可能範囲：0 - 65535 • 初期値：0
Instance ID Settings	
Instance ID	スイッチに Instance ID を設定します。 • 設定可能範囲：1-32
Action	MSTI に行う変更を選択します。 •「Add VID」- VID List 項目に指定された VID を MSTI ID に追加します。 •「Remove VID」- VID List 項目に指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

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

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

STP Instance（STP インタンス設定）

STP インスタンスの設定を変更します。

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

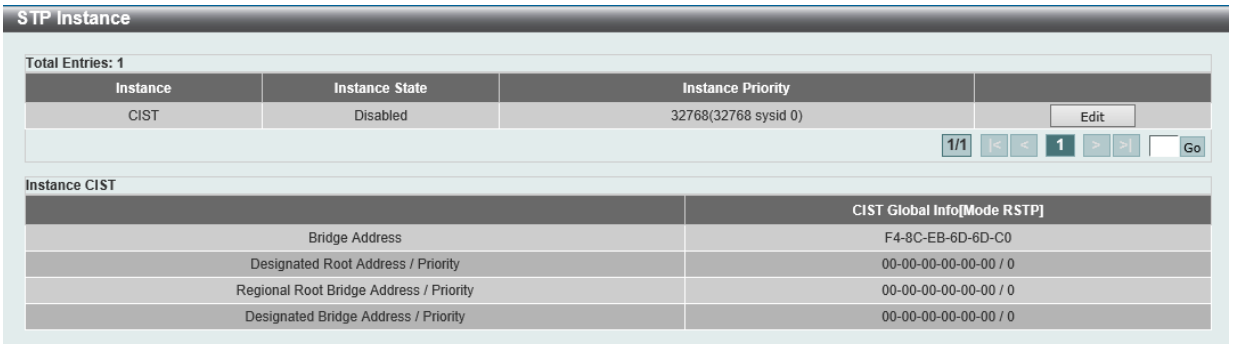


図 8-32　STP Instance 画面

画面に表示される項目：

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

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

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

MSTP Port Information（MSTP ポート情報）

現在の MSTP ポート情報の表示、設定を行います。

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

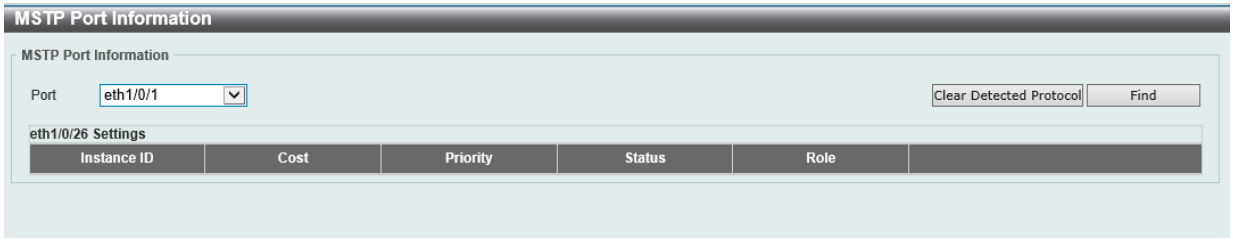


図 8-33　MSTP Port Information 画面

画面に表示される項目：

項目	説明
Port	エントリを表示 / 削除するポートを選択します。
Cost	「Edit」を選択後、パケットを転送するコストを設定します。 • 設定可能範囲：1 - 200000000
Priority	「Edit」を選択後、優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0 - 240 • 初期値：128

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

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

Loopback Detection（ループバック検知設定）

ループバック検知（LBD）機能は、特定のポートに生成されるループを検出するために使用されます。
本機能は、CTP（Configuration Testing Protocol）パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN で受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートは再起動（Normal 状態へ遷移）を行います。

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

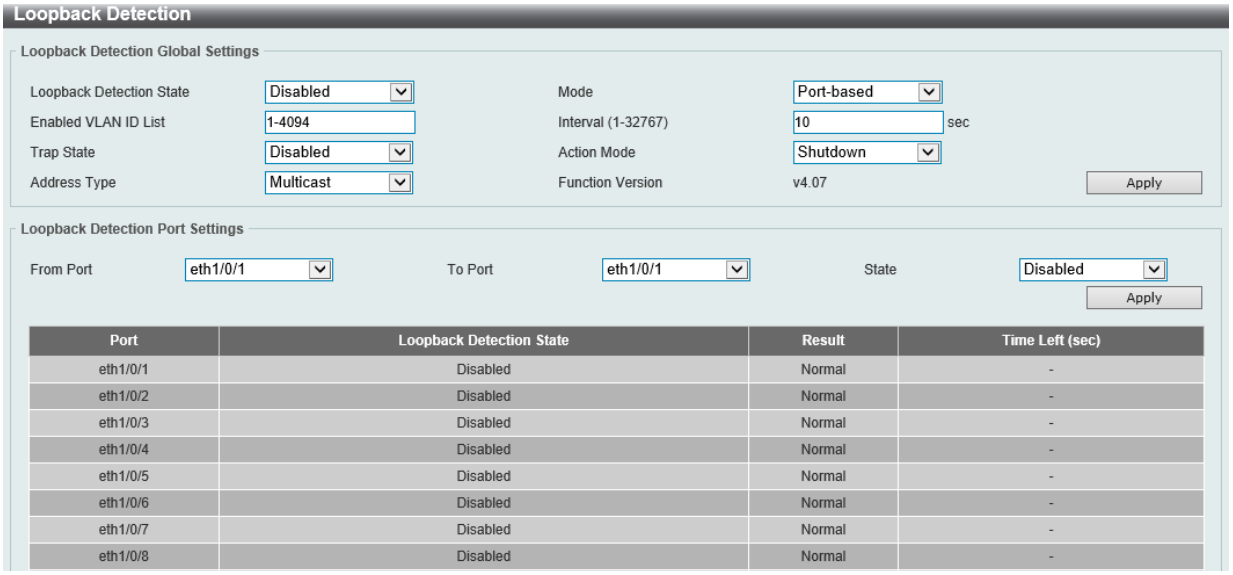


図 8-34　Loopback Detection 画面

画面に表示される項目：

項目	説明
Loopback Detection Global Settings	
Loopback Detection State	ループバック検知機能を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
Mode	ループ検知のモードを選択します。 • 選択肢：「Port-based」「VLAN-based」
Enable VLAN ID List	「Mode」で「VLAN Based」を選択した場合、VLAN ID のリストを入力します。
Interval	ループ検知間隔を設定します。 本設定の間隔で Configuration Test Protocol（CTP）パケットが送信され、ループバックイベントを検知します。 • 設定可能範囲：1 - 32767（秒） • 初期値：10（秒）
Traps State	ループバック検知トラップを有効 / 無効に設定します。
Action Mode	動作モードを指定します。 • 「Shutdown」- ループ検出時にポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックします。 • 「None」- ループ検出時でもポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックしません。
Address Type	アドレスタイプを選択します。 • 選択肢：「Multicast」「Broadcast」
Loopback Detection Port Settings	
From Port/To Port	設定を適用するポートの範囲を指定します。
State	ポートのループバック検知ステータスを有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

注意　VLAN モードで使用した場合、CTP パケットは 100VLANs/Port/Interval ずつ送信されます。CTP は 100VLANs を検出後、該当の VLAN のみに送出されます。

注意　ループバック検知とリンクアグリゲーションを設定している場合、ループ検知のモードは「Port-based」になります。

Link Aggregation（リンクアグリゲーション）

ポートトランクグループについて

ポートトランクグループは、複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。トランクグループは最大 8 個まで作成可能であり、各グループには最大 8 個までの物理ポートを割り当てることができます。

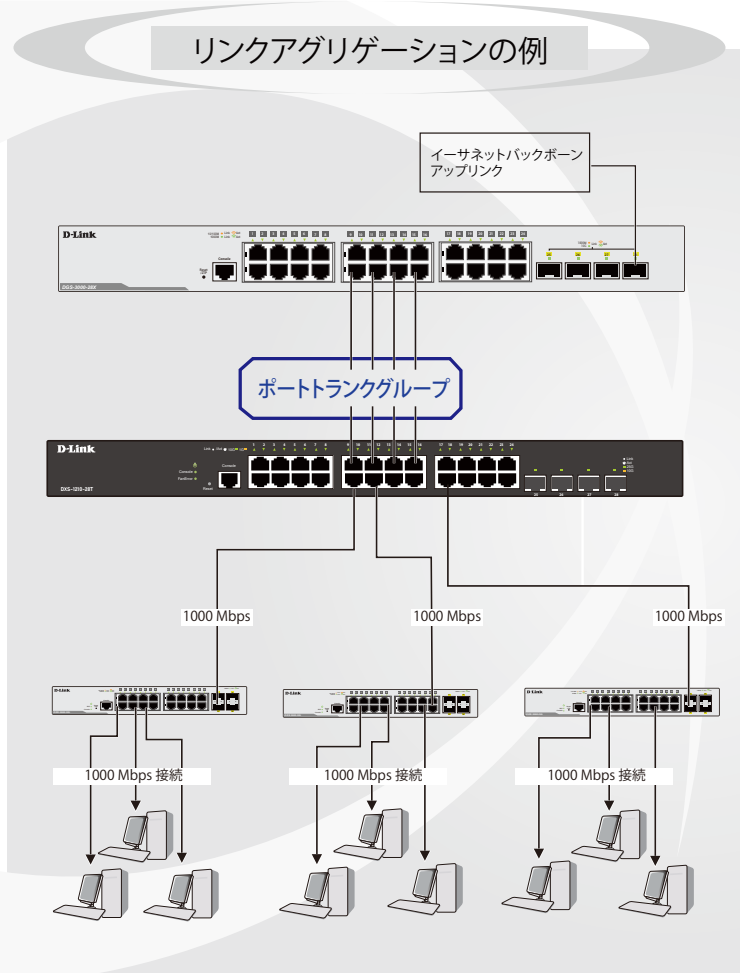


図 8-35　ポートトランクグループの例

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

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

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

本スイッチでは、8 個のリンク（ポート）から構成される最大 8 個のリンクアグリゲーショングループの構築が可能です。各ポートは 1 つのリンクアグリゲーショングループにのみ所属することができます。グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断が発生した場合、ネットワークトラフィックはグループ内の他のリンクに振り分けられます。

スパニングツリープロトコル（STP）は、リンクアグリゲーショングループを 1 つのリンクとして扱います。
スイッチに冗長化された 2 つのリンクアグリゲーショングループが設定されている場合、STP において片方のグループはブロックされます（冗長リンクを持つポートがブロックされるケースと同様）。

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

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

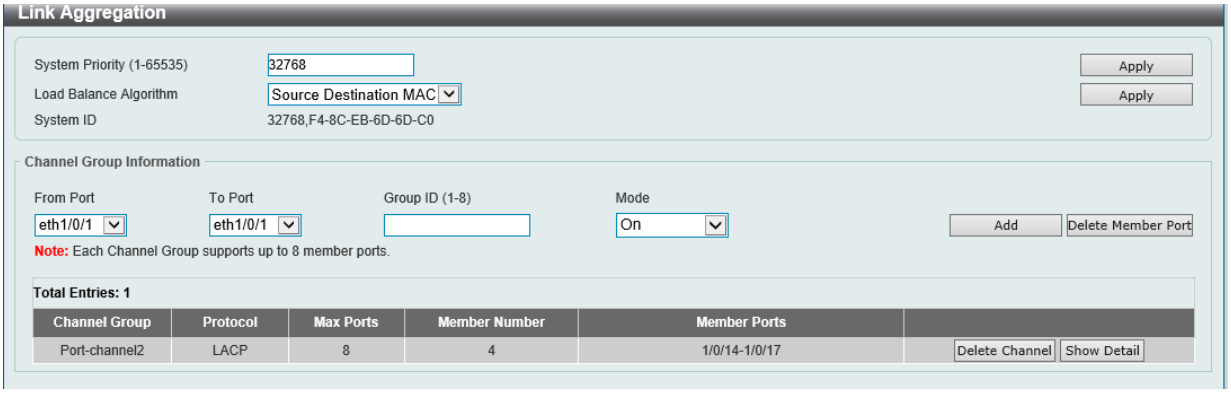


図 8-36　Link Aggregation 画面

画面に表示される項目：

項目	説明
System Priority	システム優先値を指定します。 システム優先値はどのポートがポートチャネルに属するか、そしてどのポートがスタンドアロンモードに入るかを決定します。値の小さい方が高い優先度を示します。二つ以上のポートで同じ優先値を与えられた場合、ポート番号で優先値が決まります。 • 設定可能範囲：1 - 65535 • 初期値：32768
Load Balance Algorithm	ロードバランスに使用するアルゴリズムを選択します。 • 選択肢： 「Source MAC」「Destination MAC」「Source Destination MAC」「Source IP」「Destination IP」「Source Destination IP」 • 初期値：「Source Destination MAC」
Channel Group Information	
From Port / To Port	設定するポートの範囲を指定します。
Group ID	グループの ID 番号を設定します。ポートが初めてチャネルグループに参加すると、自動的にポートチャネルが作成されます。各インタフェースは複数のチャネルグループに参加することはできません。 • 設定可能範囲：1-8
Mode	動作モードを指定します。 • 選択肢：「On」「Active」「Passive」 「On 」を選択した場合、チャネルグループタイプはスタティック（固定）になります。 「Active」または「Passive」が指定されている場合、チャネルグループタイプは LACP です。 チャネルグループは、固定もしくは LACP メンバのどちらかのみで構成されます。チャネルグループが決定すると、他のタイプのインタフェースはそのチャネルグループに参加できません。

各項目を入力後、「Add」をクリックし、チャネルグループを作成します。
「Delete Channel」をクリックして、チャネルを削除します。
「Delete Member Port」をクリックして、特定グループのメンバポートを削除します。
「Show Detail」をクリックすると、チャネルの詳細情報が表示されます。

ポートトランキンググループの編集

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

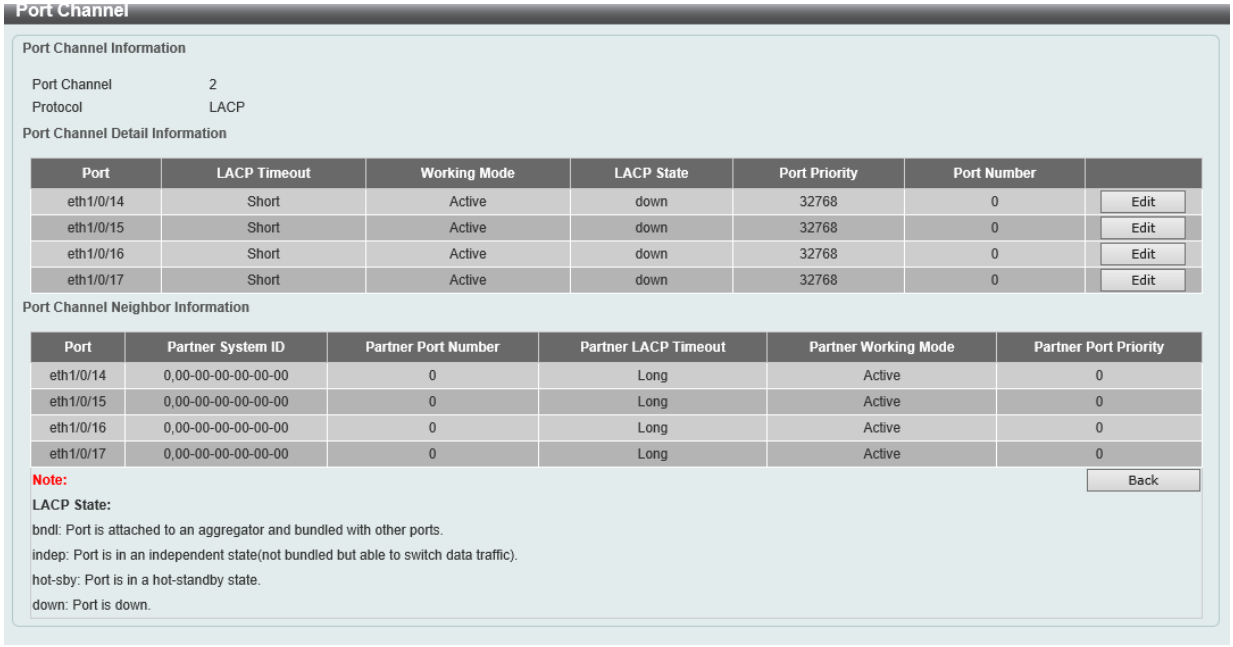


図 8-37　Link Aggregation（Channel Detail）画面

画面に表示される項目：

項目	説明
LACP Timeout	LACP タイムアウトを設定します。 • 選択肢：「Short」「Long」
Working Mode	動作モードを指定します。 • 「Active」- LACP パケットを送信してネゴシエーションを開始します。 • 「Passive」- LACP パケットへの応答のみ行います。
Port Priority	ポートプライオリティを設定します。

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

「Back」をクリックし前の画面に戻ります。

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

IGMP（Internet Group Management Protocol）Snooping 機能を始めとした L2 Multicast Control（L2 マルチキャストコントロール）の設定を行います。

IGMP Snooping（IGMP スヌーピング）

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。

IGMP Snooping Settings（IGMP スヌーピング設定）

IGMP Snooping 設定をグローバルに有効または無効にします。
IGMP Snooping 機能を利用するためには、まず本機能をスイッチ全体で有効にする必要があります。その後、対応する「Edit」をクリックして、各 VLAN に詳細な設定を行います。IGMP Snooping を有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバに接続するポートをオープンまたはクローズできるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストが存在しなくなった場合、マルチキャストパケットの送信を停止します。

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

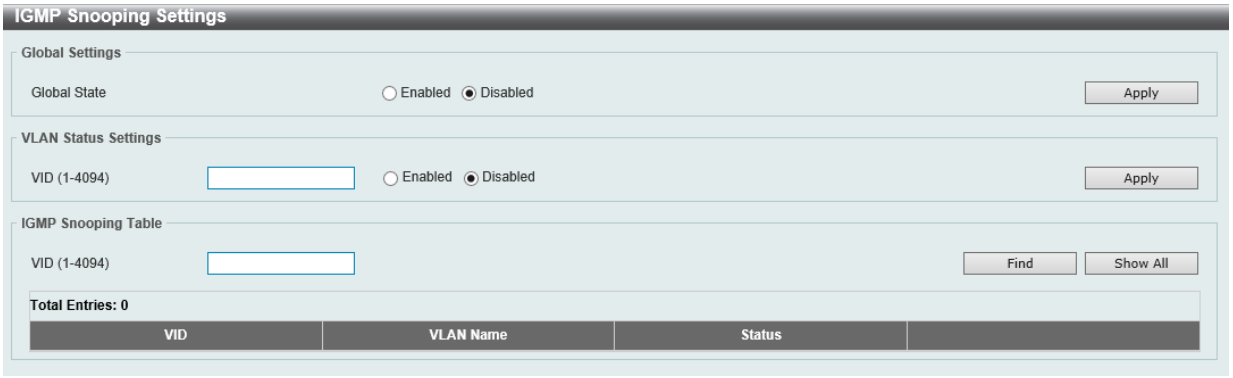


図 8-38　IGMP Snooping Settings 画面

画面に表示される項目：

項目	説明
Global Setting	
Global State	IGMP Snooping のグローバルステータスを有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
VLAN Status Settings	
VID	VLAN を識別する VLAN ID を入力し、指定 VLAN 上の IGMP Snooping を有効 / 無効に設定します。 • 設定可能範囲：1-4094
IGMP Snooping Table	
VID	IGMP Snooping テーブルに表示する VLAN の VLAN ID を指定します。 • 設定可能範囲：1-4094

「Apply」をクリックして、設定内容を適用します。

「Find」ボタンをクリックして、指定した VLAN ID のエントリを表示します。
「Show All」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。

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

IGMP Snooping VLAN の詳細情報表示

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

図 8-39　IGMP Snooping VLAN Parameters 画面

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

■ IGMP Snooping 機能の詳細設定

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

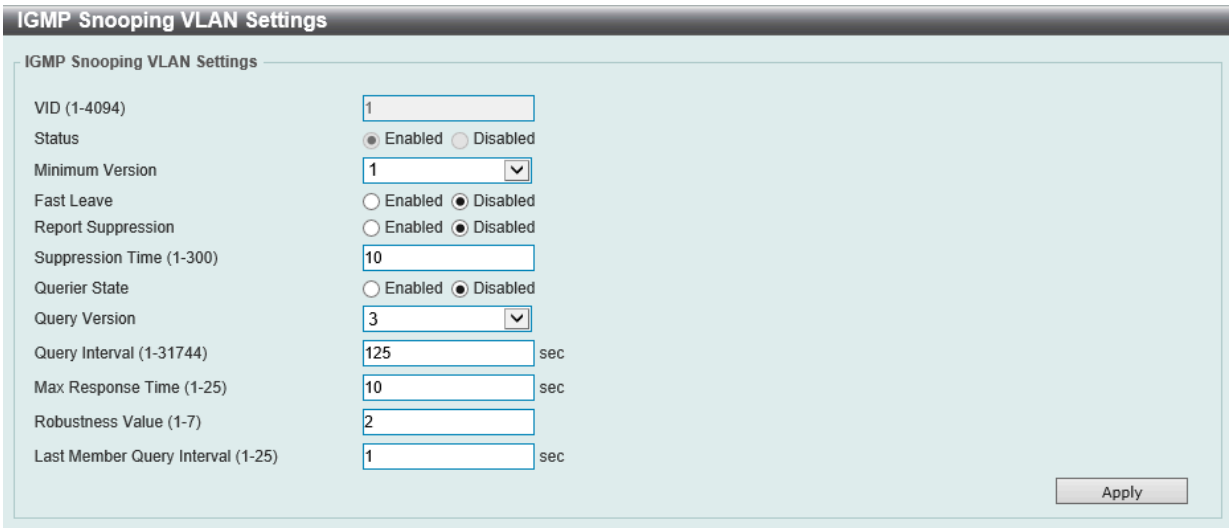


図 8-40 IGMP Snooping VLAN Settings（Edit）画面

画面に表示される項目：

項目	説明
VID	IGMP Snooping 設定を変更する VLAN を識別する VLAN ID が表示されます。
State	VLAN の IGMP Snooping 機能の有効 / 無効ステータスが表示されます。
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。 • 選択肢：「1」「2」「3」
Fast Leave	Fast Leave 機能を有効 / 無効に設定します。 有効の場合、システムが IGMP done メッセージを受信すると、メンバシップが直ちに削除されます。また、スイッチは Specific クエリを生成しません。 無効の場合、スイッチは Specific クエリを生成します。
Report Suppression	特定の VLAN への IGMP スヌーピングレポートの抑制を有効 / 無効にします。 レポート抑制機能は「IGMPv1」「IGMPv2」トラフィックでのみ機能します。 本機能を有効にした場合、ホストから送信される重複レポートを抑制します。抑制は抑制時間（Suppression Time）を過ぎるまで続きます。同じグループに対する Report/Leave メッセージは、1 つのメッセージのみが送信され、残りのメッセージは抑制されます。
Suppression Time	レポート抑制を行う時間を指定します。 • 設定可能範囲：1 - 300（秒）
Querier State	クエリア機能を有効 / 無効に設定します。
Query Version	IGMP スヌーピングクエリアで送信されるクエリパケットのバージョンを選択します。 • 選択肢：「1」「2」「3」

項目	説明
Query Interval	IGMP スヌーピングクエリアが General クエリを送信する間隔を指定します。 • 設定可能範囲：1 - 31744
Max Response Time	IGMP スヌーピングクエリでアドバタイズされる最大応答時間を入力します。 • 設定可能範囲：1 - 25（秒）
Robustness Value	パケットロスに対するロバストネス変数を指定します。 • 定可能範囲：1 - 7
Last Member Query Interval	IGMP スヌーピングクエリアが IGMP Group-Specific クエリまたは Group-Source-Specific（Channel）クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1 - 25（秒）

「Apply」をクリックして、設定内容を適用します。

注意　IGMP Snooping について、Fast Leave は IGMPv2 のみサポートします。

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

IGMP スヌーピングスタティックグループの表示と設定、IGMP スヌーピンググループの表示を行います。

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

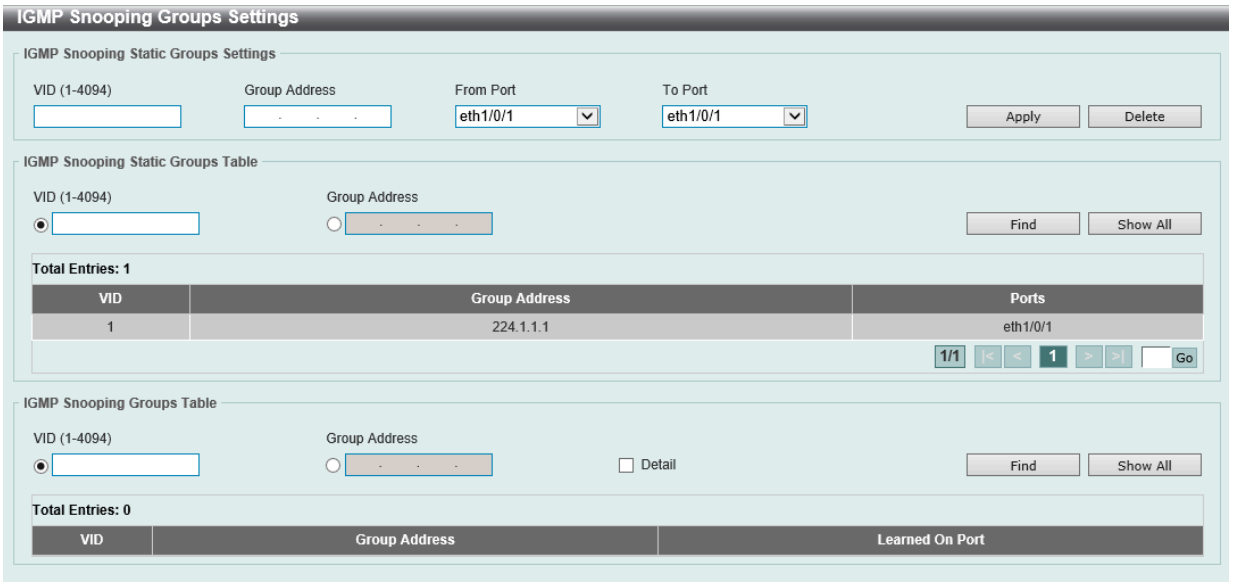


図 8-41　IGMP Snooping Group Settings 画面

画面に表示される項目：

項目	説明
IGMP Snooping Static Groups Settings	
VID	登録または削除するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	登録または削除するマルチキャストグループの IP アドレスを入力します。
From Port / To Port	設定するポートの範囲を指定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。
IGMP Snooping Groups Table	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。
Detail	チェックを入れ、IGMP グループの詳細情報を表示します。

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

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

IGMP Snooping マルチキャストルータの設定を行います。

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

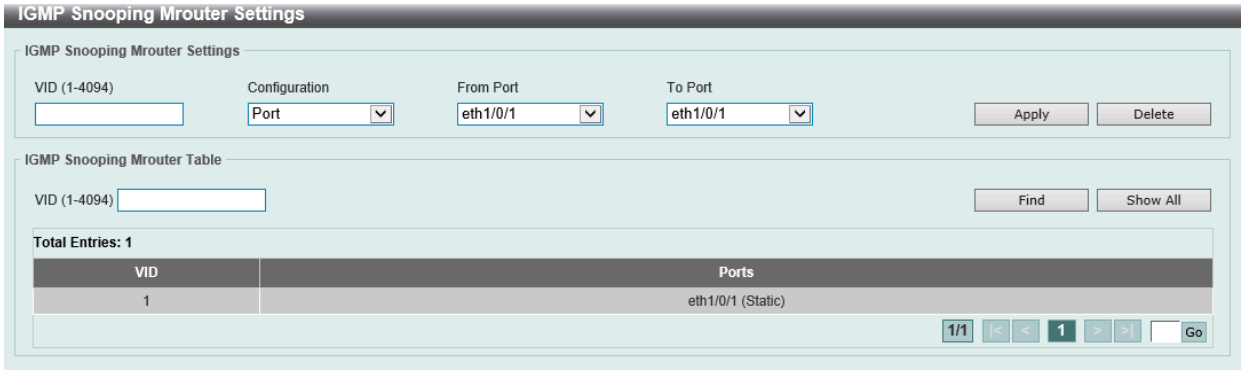


図 8-42　IGMP Snooping Mrouter Settings 画面

画面に表示される項目：

項目	説明
IGMP Snooping Mrouter Settings	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094
Configuration	ポートの設定を行います。 •「Port」- ポートをマルチキャストルータポートに指定します。 •「Forbidden Port 」- ポートを非マルチキャストポートに指定します。
From Port / To Port	設定するポートの範囲を指定します。
IGMP Snooping Mrouter Table	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094

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

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

IGMP Snooping Statistics Settings（IGMP Snooping 統計設定）

IGMP Snooping の統計情報を表示します。

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

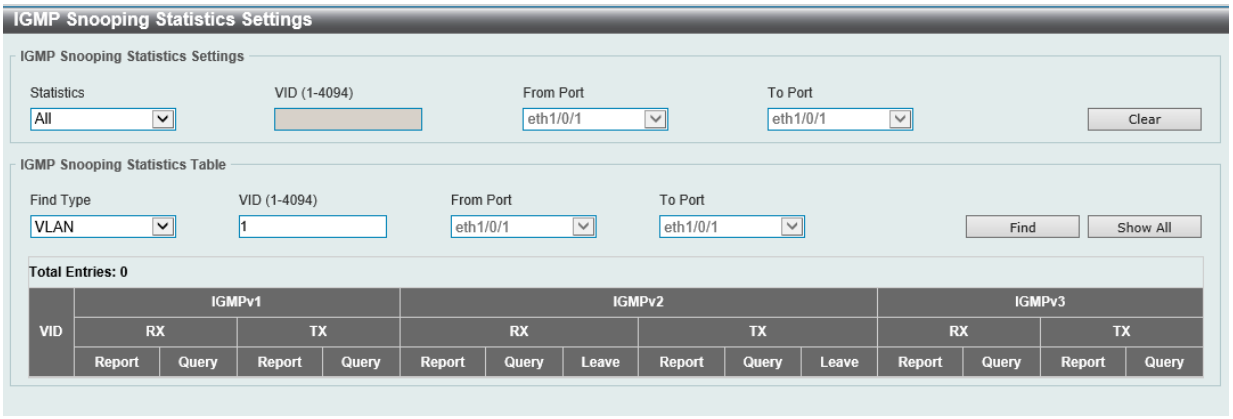


図 8-43　IGMP Snooping Statistics Settings 画面

画面に表示される項目：

項目	説明
IGMP Snooping Statistics Settings	
Statistics	インタフェースを選択します。 • 選択肢：「All」「VLAN」「Port」
VID	VLAN ID を指定します。「Statistics」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
From Port / To Port	設定するポートの範囲を指定します。「Statistics」で「Port」を選択すると設定可能になります。
IGMP Snooping Statistics Table	
Find Type	インタフェースを選択します。 • 選択肢：「VLAN」「Port」
VID	VLAN ID を指定します。「Find Type」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
From Port / To Port	表示するポートの範囲を指定します。「Find Type」で「Port」を選択すると設定可能になります。

「Clear」をクリックすると表示された統計情報がクリアされます。

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

MLD Snooping（MLD スヌーピング）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じ機能を持つ、IPv6 用のマルチキャストトラフィック制御機能です。VLAN 上でマルチキャストデータを要求するポートを検出するために使用されます。MLD Snooping では、所定の VLAN 上のすべてのポートにマルチキャストトラフィックを流すのではなく、要求元ポートとマルチキャストの送信元によって生成される MLD クエリと MLD レポートを使用して、データを受信したいポートに対してのみ、マルチキャストデータを転送します。
MLD Snooping は、エンドノードと MLD ルータとの間で交換される MLD 制御パケットのレイヤ 3 部分を調べることでパケットを処理します。スイッチは、ルートがマルチキャストトラフィックをリクエストしていることを検出すると、そのルートに直接接続されているポートを IPv6 マルチキャストテーブルに追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のエントリには、該当ポートや VLAN ID、関連する IPv6 マルチキャストグループアドレスが記録され、このポートはアクティブな Listening ポートと見なされます。アクティブな Listening ポートのみがマルチキャストグループデータを受信します。

MLD コントロールメッセージ

MLD Snooping を使用するデバイス間で以下の MLD コントロールメッセージが交換されます。これらのメッセージは、130、131、132 および 143 でラベル付けされた 4 つの ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query – IPv4 の IGMPv2 Host Membership Query（HMQ）に相当するメッセージです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query はリンク上のすべての Listening ポートに対し送信され、Multicast Specific Query は、特定のマルチキャストアドレスに対して送信されます。この 2 種類のメッセージは、IPv6 ヘッダ内のマルチキャスト宛先アドレス及び Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別されます。
2. Multicast Listener Report – IGMPv2 の Host Membership Report（HMR）に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。
3. Multicast Listener Done – IGMPv2 の Leave Group Message に相当するメッセージです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからのマルチキャストデータの受信を停止すること、つまり、このアドレスからのマルチキャストデータが "done"（完了）となった旨を伝えます。スイッチが本メッセージを受信すると、この Listening ホストには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しなくなります。
4. Multicast Listener Report Version2 – IGMPv3 の Host Membership Report（HMR）に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

MLD Snooping Settings（MLD スヌーピング設定）

MLD Snooping の設定を行います。

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

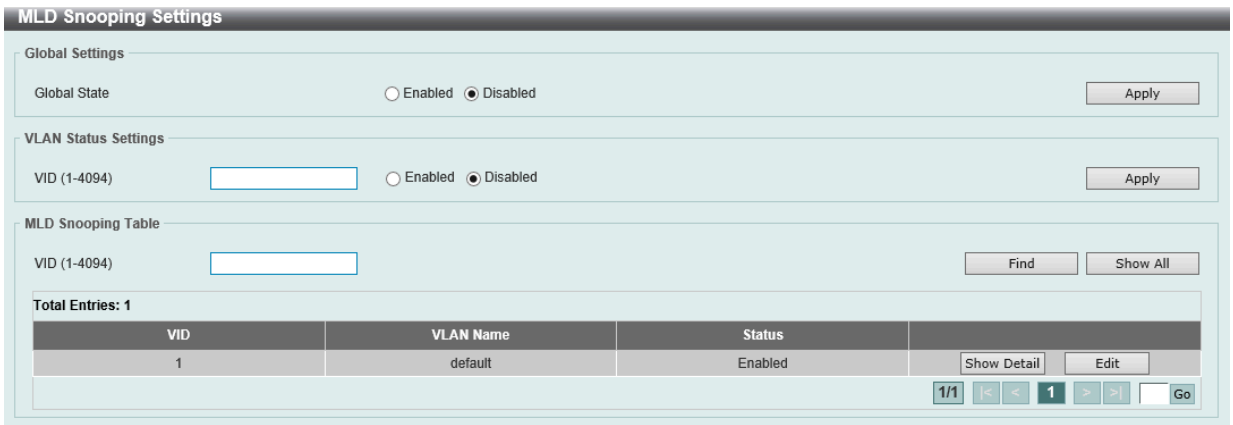


図 8-44　MLD Snooping Settings 画面

画面に表示される項目：

項目	説明
Global Setting	
Global State	MLD Snooping のグローバルステータスを有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
VLAN Status Settings	
VID	VLAN を識別する VLAN ID を入力し、指定 VLAN 上の MLD Snooping を有効 / 無効に設定します。 • 設定可能範囲：1-4094
MLD Snooping Table	
VID	MLD Snooping テーブルに表示する VLAN の VLAN ID を指定します。 • 設定可能範囲：1-4094

「Apply」をクリックして、設定内容を適用します。

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

「Edit」をクリックしてエントリを編集します。

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

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

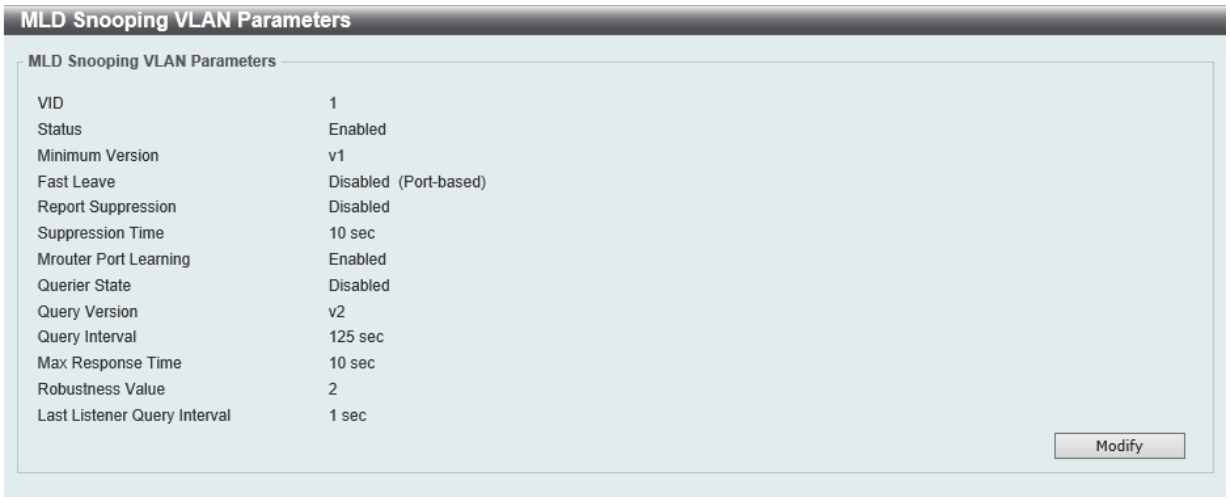


図 8-45　MLD Snooping VLAN Parameters 画面

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

MLD Snooping 機能の詳細設定
「MLD Snooping Settings」で関連する VLAN エントリの「Modify」をクリックし、以下の画面で各 VLAN に対して詳細な設定を行います。

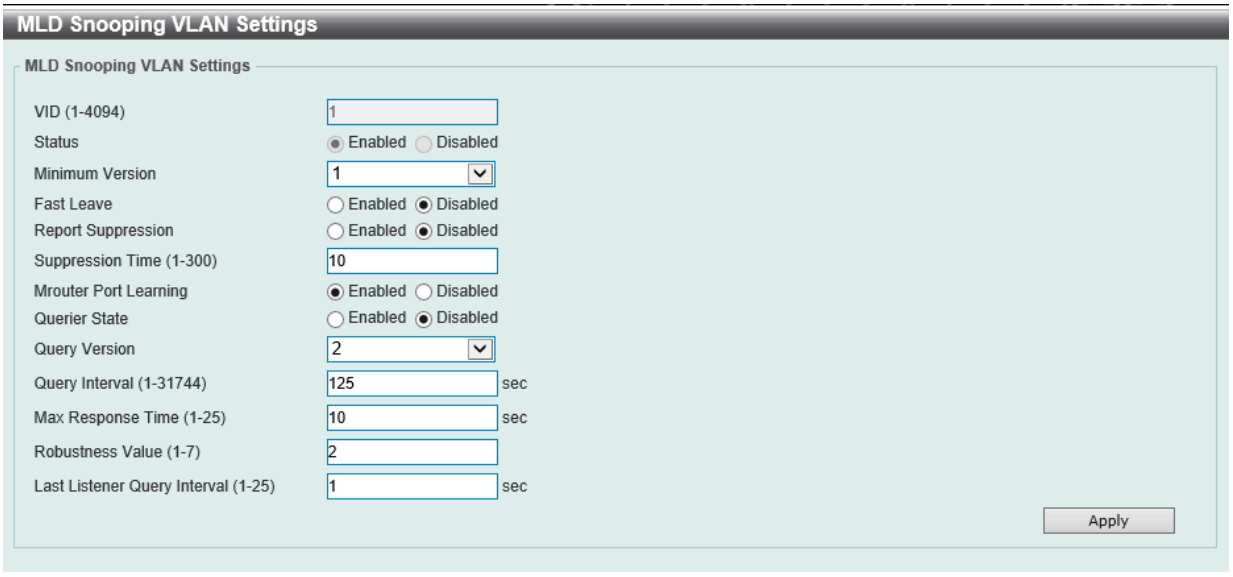


図 8-46 MLD Snooping VLAN Settings（Modify）画面

画面に表示される項目：

項目	説明
VID	MLD Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
Status	指定した VLAN の MLD Snooping 機能の有効 / 無効ステータスを表示します。
Minimum Version	VLAN に許可された MLD ホストの最小バージョンを選択します。 • 選択肢：「1」「2」
Fast Leave	Fast Leave 機能の有効 / 無効を設定します。 本機能が有効の場合、スイッチが MLD Leave メッセージを受信すると、マルチキャストグループのメンバは直ちにグループから脱退します。
Report Suppression	特定の VLAN への MLD スヌーピングレポートの抑制を有効 / 無効に設定します。 本機能を有効にした場合、ホストから送信される重複レポートを抑制します。
Suppression Time	レポート抑制を行う時間を指定します。 • 設定可能範囲：1 - 300（秒）
Mrouter Port Learning	Mrouter ポート学習機能を有効 / 無効に設定します。
Querier State	MLD クエリア機能を有効 / 無効に設定します。
Query Version	MLD スヌーピングクエリアによって送信される General クエリパケットのバージョンを選択します。 • 選択肢：「1」「2」
Query Interval	MLD スヌーピングクエリアが MLD General クエリメッセージを送信する間隔を入力します。 • 設定可能範囲：1 - 31744（秒） • 初期値：125（秒）
Max Response Time	MLD スヌーピングクエリでアドバタイズされる最大応答時間を指定します。 • 設定可能範囲：1 - 25（秒） • 初期値：10（秒）
Robustness Value	MLD スヌーピングで使用する、パケットロスに対するロバストネス変数を指定します。 • 設定可能範囲：1 - 7
Last Listener Query Interval	MLD スヌーピングクエリアが MLD Group-Specific クエリまたは Group-Source-Specific（Channel）クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1 - 25（秒）

「Apply」をクリックして、設定内容を適用します。

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

MLD スヌーピングスタティックグループの表示と設定、および MLD スヌーピンググループの表示を行います。

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

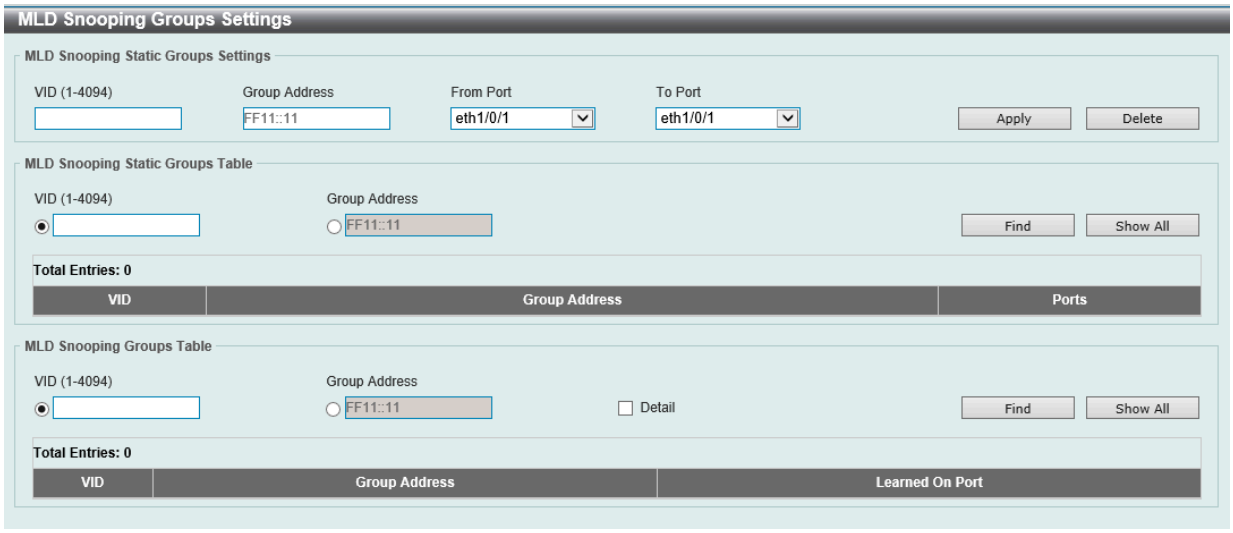


図 8-47　MLD Snooping Groups Settings 画面

画面に表示される項目：

項目	説明
MLD Snooping Static Groups Settings	
VID	登録または削除する IPv6 マルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	登録または削除する IPv6 マルチキャストグループの IPv6 アドレスを入力します。
From Port / To Port	設定するポートの範囲を指定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。
MLD Snooping Groups Table	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID（1-4094）を入力します。 • 設定可能範囲：1-4094
Group Address	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。
Detail	チェックを入れ、マルチキャストグループの詳細情報を表示します。

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

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

VLAN インタフェースでマルチキャストルータポートを指定します。

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

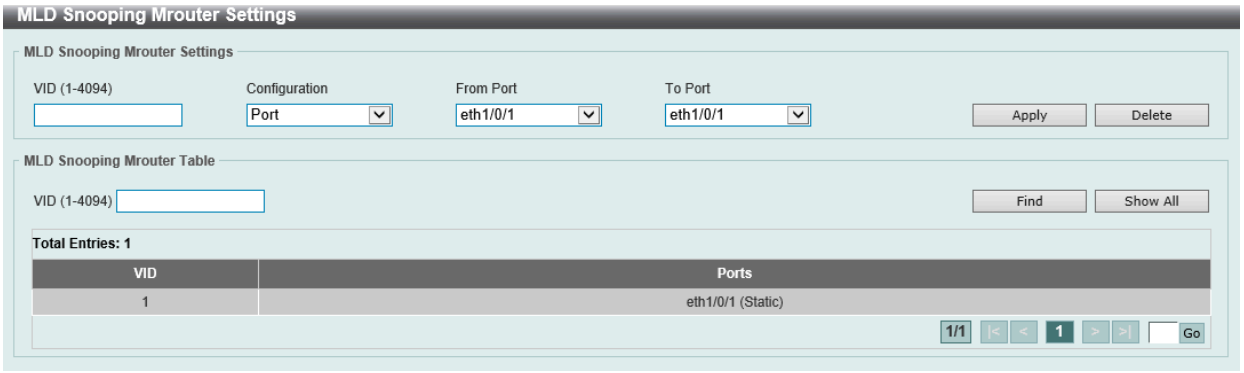


図 8-48　MLD Snooping Mrouter Settings 画面

画面に表示される項目：

項目	説明
MLD Snooping Mrouter Settings	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094
Configuration	ポートの設定を以下から選択します。 • 「Port」- マルチキャストが有効なルータと接続するポート範囲を設定します。 • 「Forbidden Port」- マルチキャストが有効なルータと接続しないポート範囲を設定します。 • 「Learn PIMv6」- 指定した VLAN において、マルチキャストルータポートの自動取得を有効にします。
From Port / To Port	設定するポートの範囲を指定します。
MLD Snooping Mrouter Table	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094

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

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

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。

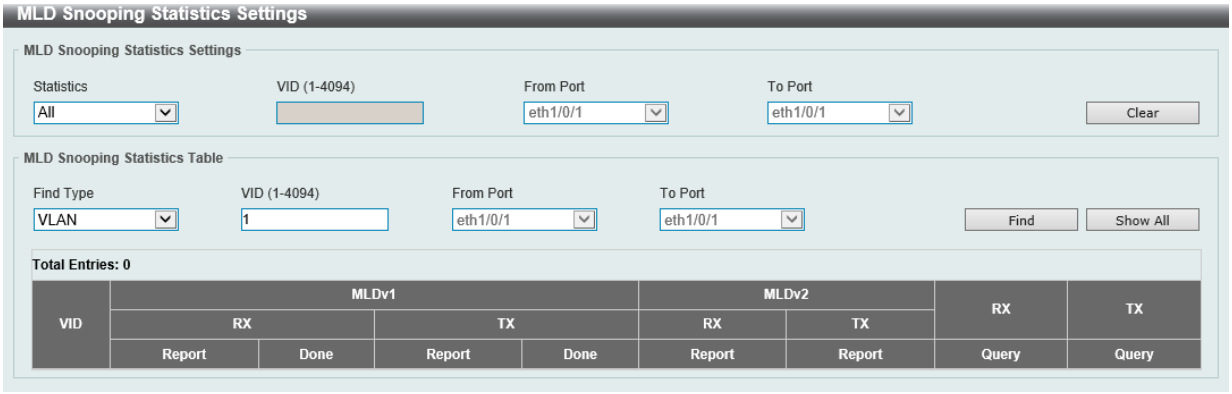


図 8-49　MLD Snooping Statistics Settings 画面

画面に表示される項目：

項目	説明
MLD Snooping Statistics Settings	
Statistics	インタフェースを選択します。 • 選択肢：「All」「VLAN」「Port」
VID	VLAN ID を指定します。「Statistics」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
From Port / To Port	設定するポートの範囲を指定します。「Statistics」で「Port」を選択すると設定可能になります。
MLD Snooping Statistics Table	
Find Type	インタフェースのタイプを選択します。 • 選択肢：「VLAN」「Port」
VID	VLAN ID を指定します。「Find Type」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
From Port / To Port	設定するポートの範囲を指定します。「Find Type」で「Port」を選択すると設定可能になります。

「Clear」をクリックすると表示された統計情報がクリアされます。

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

L2 マルチキャストフィルタリング設定を行います。

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

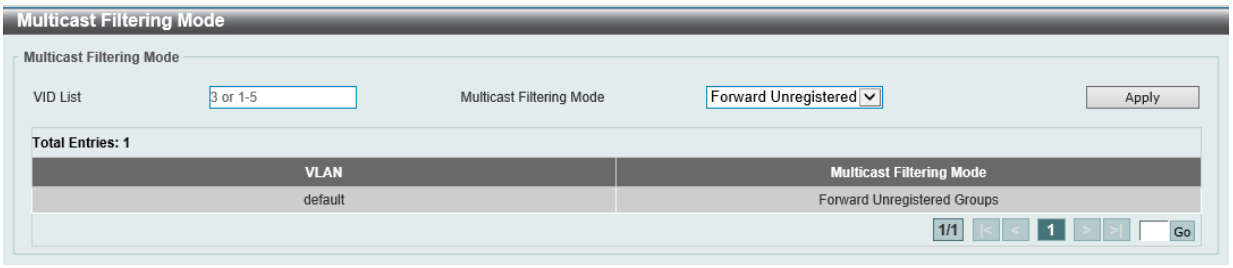


図 8-50　Multicast Filtering Mode 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

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

LLDP（LLDP 設定）

LLDP（Link Layer Discovery Protocol）は、隣接する機器の情報を収集するためのプロトコルです。
IEEE 802 ネットワークに接続している他の機器に対し、自分の機器情報をアドバタイズします。

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。

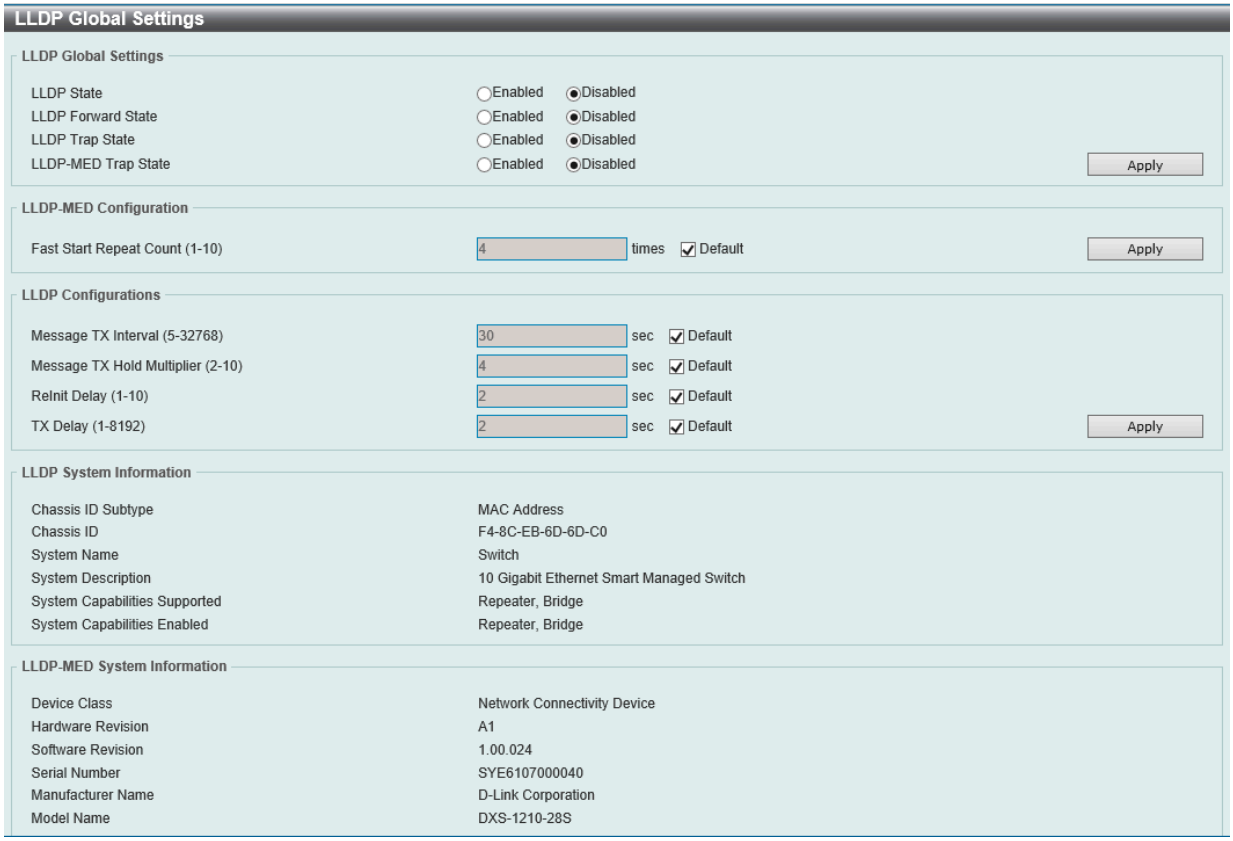


図 8-51　LLDP Global Settings 画面

画面に表示される項目：

項目	説明
LLDP Global Settings	
LLDP State	スイッチの LLDP 機能を有効 / 無効に設定します。
LLDP Forward State	LLDP 転送ステータスを有効 / 無効に設定します。 「LLDP Status」が 無効で「LLDP Forward Sate」が有効の場合、受信した「LLDPDU」パケットは転送されます。
LLDP Trap State	LLDP トラップを有効 / 無効に設定します。
LLDP-MED Trap State	LLDP-MED トラップを有効 / 無効に設定します。
LLDP-MED Configuration	
Fast Start Repeat Count	「LLDP-MED」ファストスタートリピートカウント値を指定します。 • 設定可能範囲：1 - 10
LLDP Configurations	
Message TX Interval	物理インタフェースの LLDP アドバタイズメント送信間隔を設定します。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：5 - 32768（秒）
Message TX Hold Multiplier	LLDPDU の TTL 値を計算するために使用される、LLDPDU 転送間隔に対する乗数を指定します。 「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：2 - 10
ReInit Delay	LLDP ポートが再初期化を行うまでの待機時間を指定します。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1 - 10（秒）
TX Delay	インタフェースで LLDPDU を送信するまでの待機時間を指定します。転送間隔の数値の 1/4 より大きくすることはできません。「Default」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-8192（秒）

「Apply」をクリックして、設定内容を適用します。

LLDP Port Settings（LLDP ポート設定）

LLDP ポートパラメータを設定します。

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

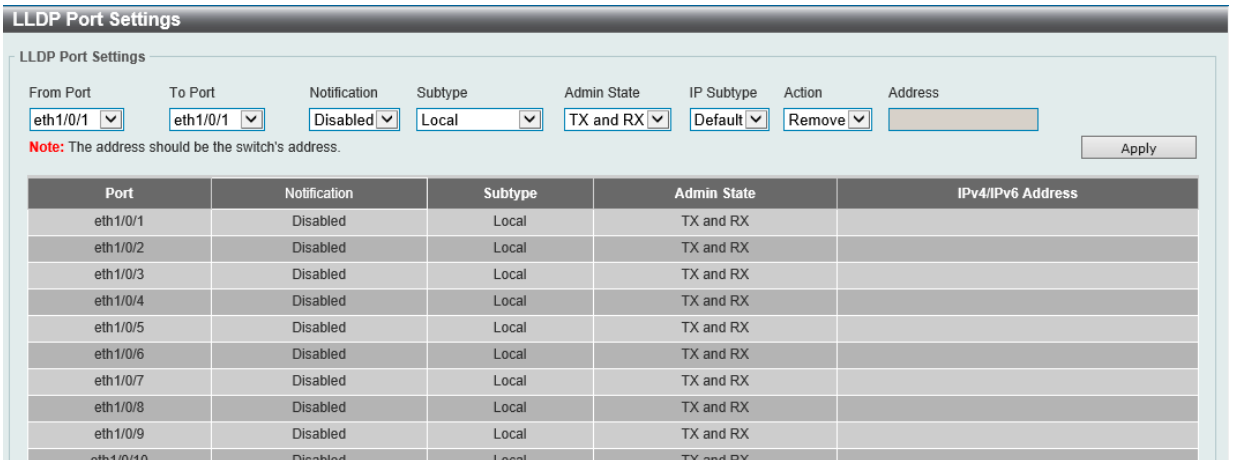


図 8-52　LLDP Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Notification	LLDP 通知を有効 / 無効に設定します。
Subtype	LLDP TLV のサブタイプを選択します。 • 選択肢：「MAC Address」「Local」
Admin State	LLDP フレームの送受信オプションを選択します。 • 「TX」- ローカル LLDP エージェントは LLDP フレームの送信のみ行います。 • 「RX」- ローカル LLDP エージェントは LLDP フレームの受信のみ行います。 • 「TX and RX」- ローカル LLDP エージェントは LLDP フレームの送受信を行います。（初期値） • 「Disabled」- ローカル LLDP エージェントは LLDP フレームの送受信を行いません。
IP Subtype	送信する IP アドレスの種類を選択します。 • 選択肢：「Default」「IPv4」「IPv6」
Action	実行する動作を選択します。 • 選択肢：「Remove」「Add」
Address	送信する IP アドレスを入力します。

「Apply」をクリックして、設定内容を適用します。

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

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

LLDP 管理アドレスリストを表示します。

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

図 8-53　LLDP Management Address List 画面

画面に表示される項目：

項目	説明
Subtype	表示する LLDP 管理アドレスのサブタイプを選択します。 • 「All」- すべてのエントリを表示します。 • 「IPv4」- IPv4 アドレスを入力します。 • 「IPv6」- IPv6 アドレスを入力します。

「Find」をクリックし、LLDP 管理情報を検索します。

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

LLDP の Type-Length-Value（TLV）設定を行います。TLV により、LLDP パケット内で特定の情報を送信できます。
スイッチのアクティブな LLDP ポートには、通常、その外向き通知に必須データが含まれています。
必須のデータタイプには、以下の 4 タイプの TLV が含まれます。必須のデータタイプを無効にすることはできません。

- end of LLDPDU TLV
- chassis ID TLV
- port ID TLV
- TTL TLV

さらに、オプションで選択可能な 4 つのデータタイプがあります。

- ポート説明（Port Description）
- システム名（System Name）
- システム説明（System Description）
- システム機能（System Capability）

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。

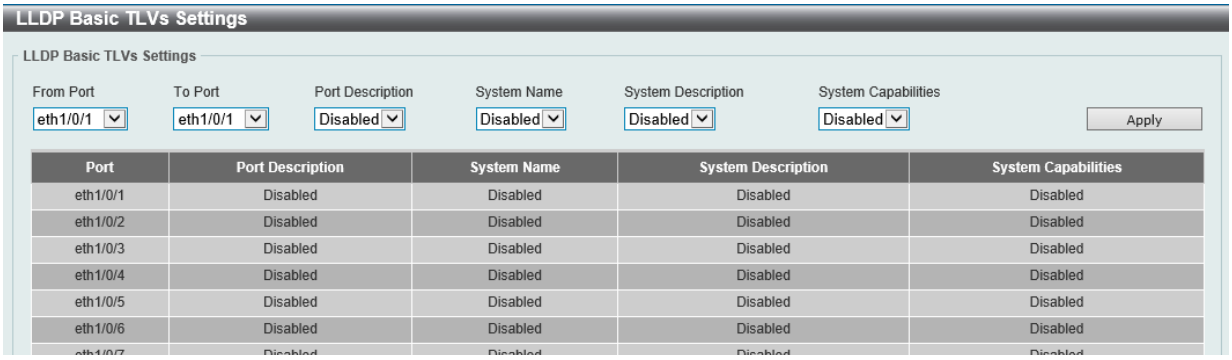


図 8-54　LLDP Basic TLVs Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Port Description	ポート説明オプションを有効 / 無効に設定します。
System Name	システム名オプションを有効 / 無効に設定します。
System Description	システム説明オプションを有効 / 無効に設定します。
System Capabilities	システム能力オプションを有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

VLAN 関連の TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

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

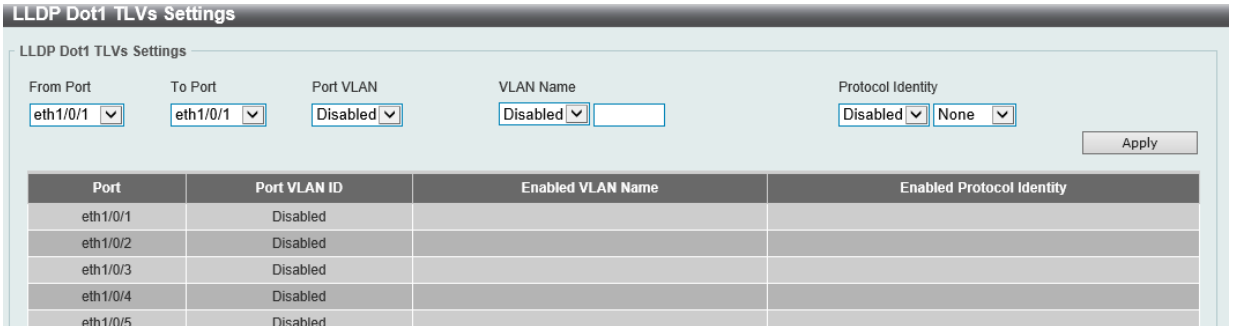


図 8-55　LLDP Dot1 TLVs Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Port VLAN	ポート VLAN ID TLV の通知を有効 / 無効に設定します。 ポート VLANID TLV は、オプションの固定長 TLV です。VLAN ブリッジポートにより、「アンタグ」または「プライオリティタグ」付きフレームに紐づくポート VLAN ID（PVID）を通知できます。
VLAN Name	VLAN 名 TLV の通知を有効 / 無効に設定します。右の欄に VLAN 名 TLV の VLANID を入力します。
Protocol Identity	プロトコル識別子 TLV およびプロトコル名の通知を有効 / 無効に設定します。 対象とするプロトコルを以下から選択します。 • 選択肢：「None」「EAPOL」「LACP」「STP」「All」

「Apply」をクリックして、設定内容を適用します。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

イーサネット関連の TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

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

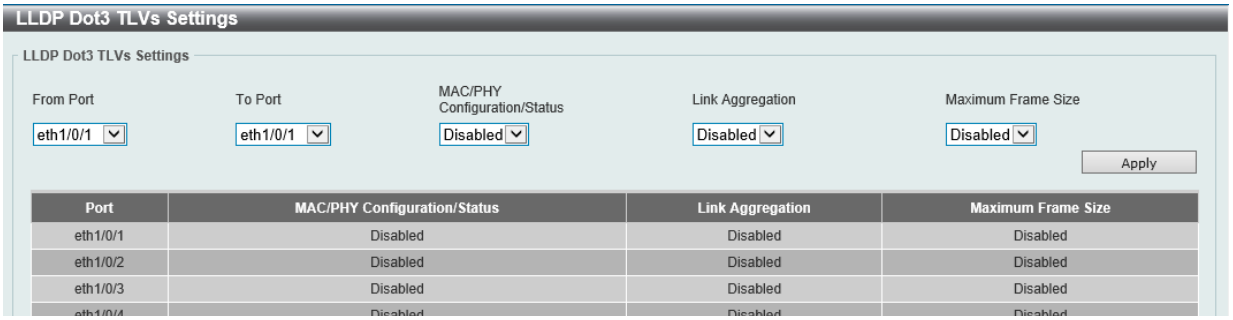


図 8-56　LLDP Dot3 TLVs Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
MAC/PHY Configuration/Status	MAC/PHY Configuration/Status TLV の通知を有効 / 無効に設定します。 MAC/PHY Configuration/Status TLV は以下を判別します。 （1）送信 IEEE 802.3 LAN ノードの Duplex およびビットレートの Capability （2）送信 IEEE 802.3 LAN ノードの現在の Duplex およびビットレート設定
Link Aggregation	リンクアグリゲーション TLV の通知を有効 / 無効に設定します。 リンクアグリゲーション TLV には以下の情報が含まれます。 - リンクはリンクアグリゲーション可能かどうか - リンクは現在リンクアグリゲーションに設定されているか - 集約ポートのチャンネル ID ポートがリンクアグリゲーションに設定されていない場合、ID は 0 となります。
Maximum Frame Size	最大フレームサイズ TLV の通知を有効 / 無効に設定します。 この TLV は、実装された MAC/PHY の最大フレームサイズ Capability を示します。

「Apply」をクリックして、設定内容を適用します。

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

LLDP-MED TLV の送信を有効または無効に設定します。

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

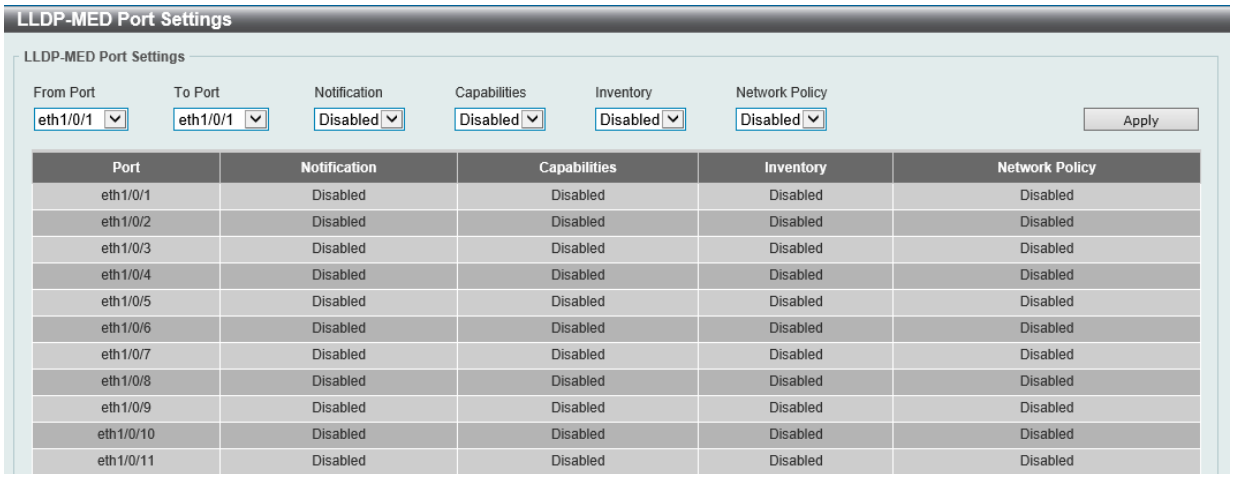


図 8-57　LLDP-MED Port Settings 画面

画面に表示される項目：

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

「Apply」をクリックし、変更を適用します。

LLDP Statistics Information（LLDP 統計情報）

スイッチにおける LLDP 統計情報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。

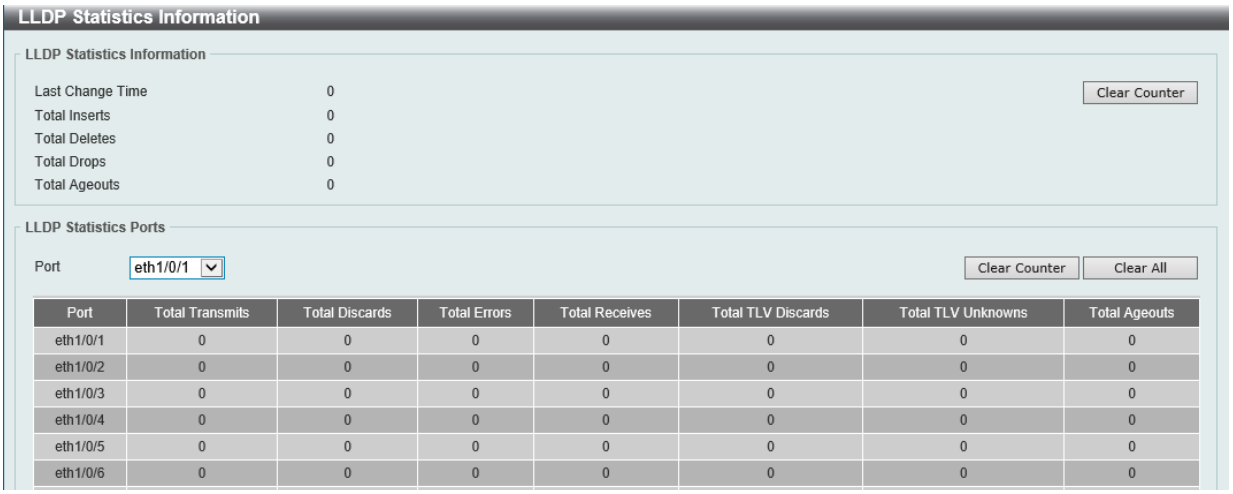


図 8-58　LLDP Statistics Information 画面

画面に表示される項目：

項目	説明
Port	表示するポートを指定します。

「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）

外向きの LLDP 通知に含まれる情報を表示します。

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

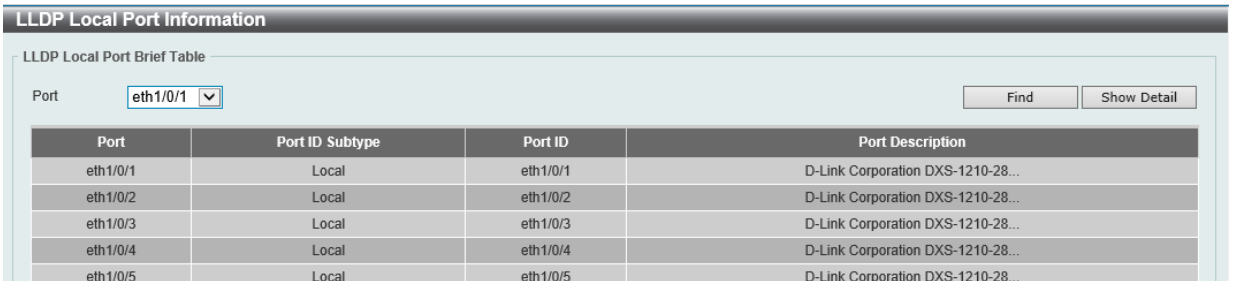


図 8-59　LLDP Local Port Information 画面

画面に表示される項目：

項目	説明
Port	表示するポートを指定します。

「Find」をクリックし、情報を表示します。

■ **詳細情報の参照**

「Show Detail」をクリックし、以下の画面を表示します。

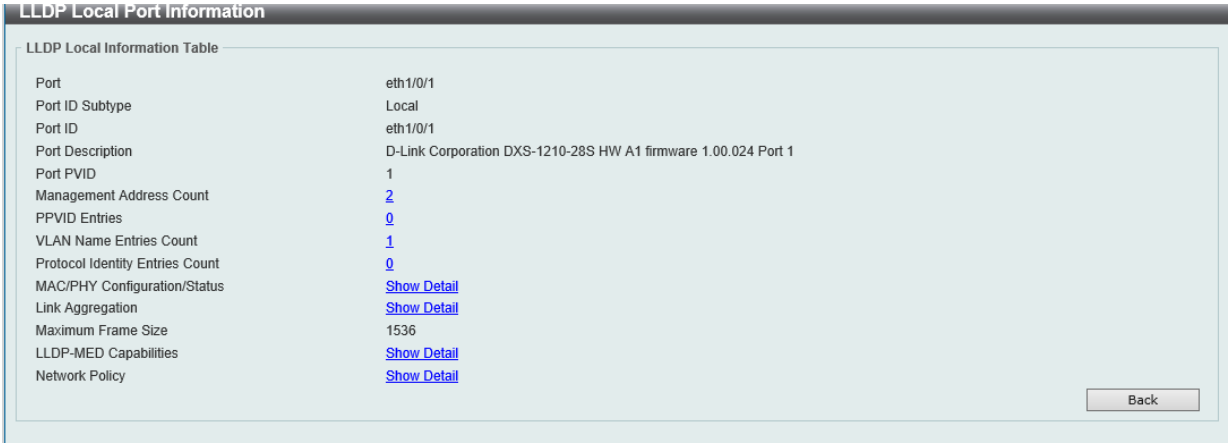


図 8-60　LLDP Local Port Information（Show Detail）画面

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

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

ネイバから学習した LLDP 情報を表示します。

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。

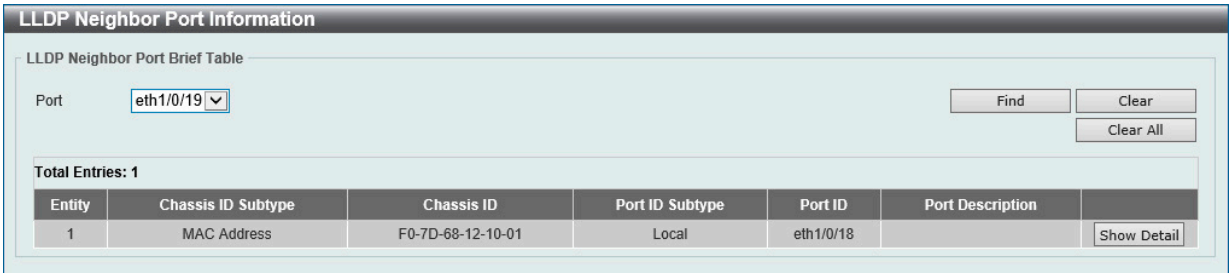


図 8-61　LLDP Neighbor Port Information 画面

画面に表示される項目：

項目	説明
Port	表示するポートを指定します。

ポートを選択し、「Find」をクリックします。情報が画面下半分に表示されます。
「Clear」をクリックしてポート情報をクリアします。
「Clear All」をクリックして、アドレステーブルのすべての情報をクリアします。

「Show Detail」をクリックすると該当ポートの詳細が表示されます。

図 8-62　LLDP Neighbor Port Information 画面

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

第 9 章　L3 Features（レイヤ 3 機能の設定）

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

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

サブメニュー	説明
ARP（ARP 設定）	ARP の設定、編集を行います。
Gratuitous ARP（Gratuitous ARP 設定）	Gratuitous ARP の設定、編集を行います。
IPv6 Neighbor（IPv6 Neighbor 設定）	IPv6 ネイバ設定を行います。
Interface（インタフェース設定）	IPv4/IPv6 アドレスのインタフェースの設定を行います。
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート）	IPv4 アドレスのスタティック / 初期ルートの設定を行います。
IPv4 Route Table（IPv4 ルートテーブル）	IPv4 のルートテーブルの設定を行います。
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート）	IPv6 アドレスのスタティック / 初期ルートの設定を行います。
IPv6 Route Table（IPv6 ルートテーブル）	IPv6 のルートテーブルの設定を行います。
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル設定）	IP マルチキャストルーティングプロトコルの設定を行います。

ARP（ARP 設定）

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

ARP Aging Time（ARP エージングタイム設定）

ARP エージングタイムの設定を行います。

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

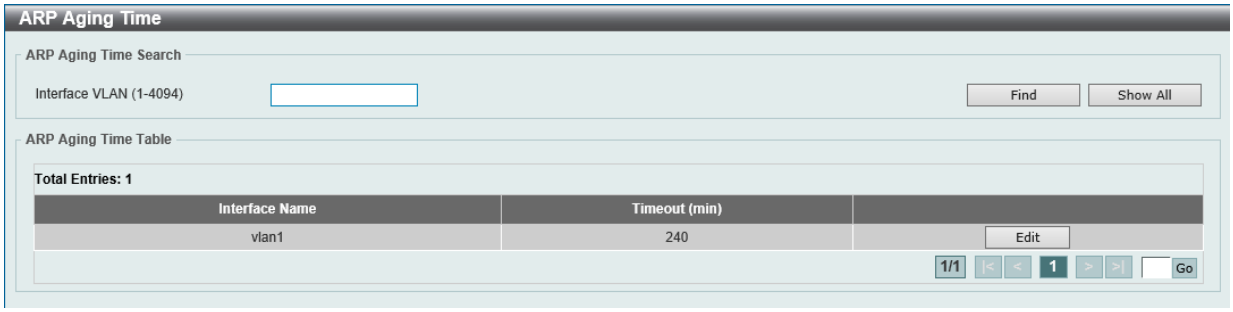


図 9-1　ARP Aging Time 画面

画面に表示される項目：

項目	説明
Interface VLAN	インタフェース VLAN ID を入力します。 • 設定可能範囲：1-4094
Timeout	「Edit」をクリックして、ARP エイジングタイムアウト値（分）を入力します。 この時間が経過すると、エントリはテーブルから削除されます。 • 設定可能範囲：0 - 65535（分） 「0」に設定した場合、タイムアウトしません。

「Find」をクリックして、指定 VLAN に基づいてエントリが検索します。
「Show All」をクリックして、すべての ARP エージングタイムエントリを表示します。

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

補足　ダイナミック ARP の最大エントリ数は 1500 です。

Static ARP（スタティック ARP 設定）

スタティックエントリを ARP テーブルに定義します。

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

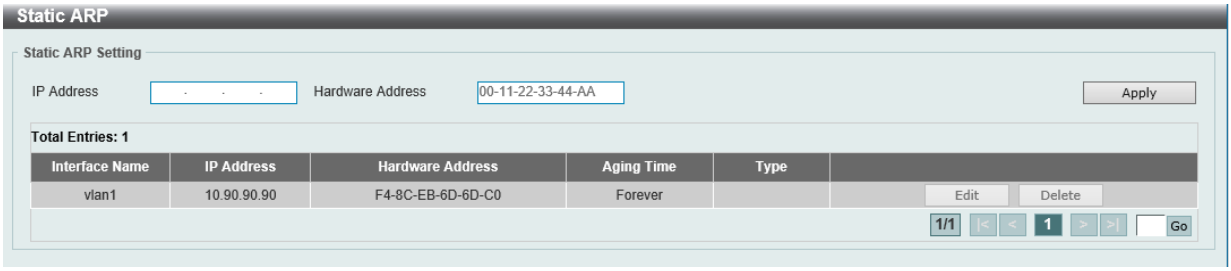


図 9-2　Static ARP 画面

画面に表示される項目：

項目	説明
IP Address	MAC アドレスとスタティックに結びつける IP アドレスを設定します。
Hardware Address	ARP テーブルで IP アドレスとスタティックに結びつける MAC アドレスを設定します。

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

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

ARP Table（ARP テーブルの参照）

スイッチ上の現在の ARP エントリを表示します。

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

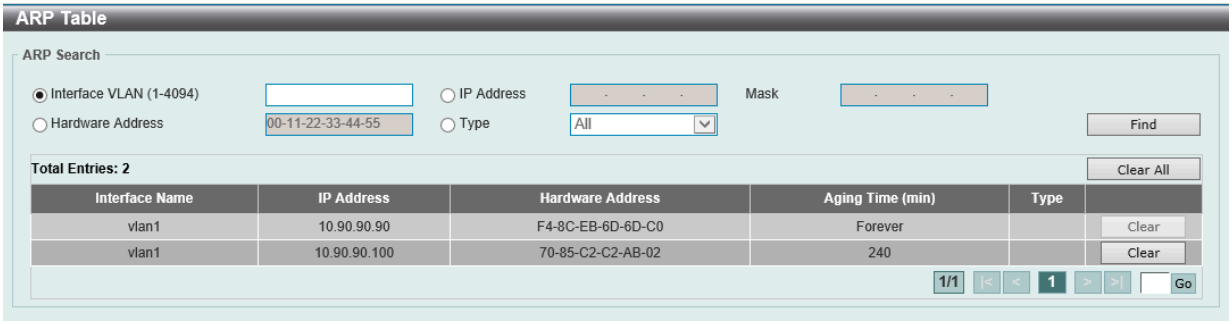


図 9-3　ARP Table 画面

画面に表示される項目：

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

「Find」をクリックして、入力した情報に基づく指定のエントリを検索します。
「Clear All」をクリックするとテーブル上のエントリが全て消去されます。
削除するエントリの「Clear」をクリックするとエントリが削除されます。

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

Gratuitous ARP（Gratuitous ARP 設定）

Gratuitous ARP リクエストパケットは、送信元 / 宛先 IP アドレスが送信元デバイスのアドレスに設定され、宛先 MAC アドレスがブロードキャストアドレスとなっている ARP リクエストパケットです。通常、Gratuitous ARP リクエストパケットを使用して、IP アドレスが他のデバイスと競合していないかを検出したり、インタフェースに接続されたホストの ARP キャッシュエントリを事前ロードまたは再構成したりします。

L3 Features > Gratuitous ARP の順にメニューをクリックして以下の画面を表示します。

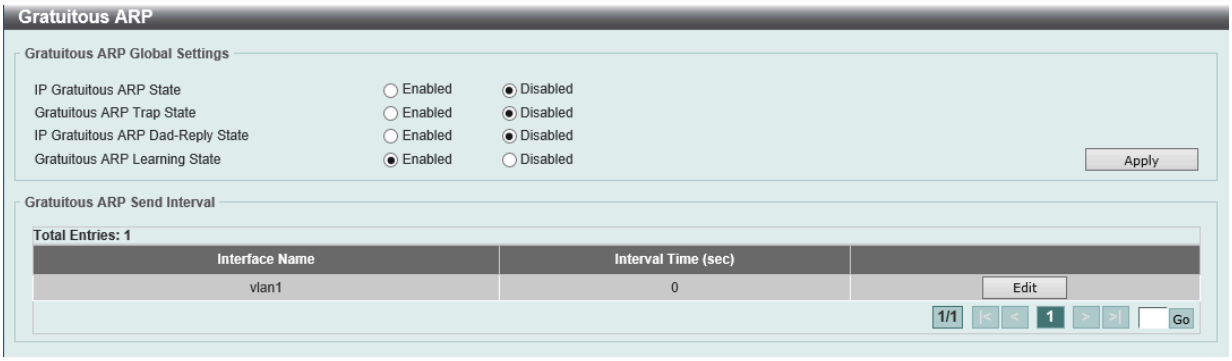


図 9-4　Gratuitous ARP 画面

画面に表示される項目：

項目	説明
IP Gratuitous ARP State	ARP キャッシュテーブルの Gratuitous ARP パケットの学習を有効 / 無効に設定します。
Gratuitous ARP Trap State	Gratuitous ARP トラップ を有効 / 無効に設定します。
IP Gratuitous ARP Dad-Reply State	IP Gratuitous ARP Dad-reply を有効 / 無効に設定します。
Gratuitous ARP Learning State	Gratuitous ARP 学習を有効 / 無効に設定します。 システムは通常、ARP 応答パケットや、スイッチの IP アドレスに対応する MAC アドレスを問い合せるために使用する、通常の ARP リクエストパケットからのみ ARP エントリを学習します。 Gratuitous ARP 学習を有効すると、受信した Gratuitous ARP パケットからの ARP エントリの学習が可能になります。Gratuitous ARP パケットは、送信元アドレスと問合せ IP アドレスが同一のパケットです。

「Apply」をクリックして、設定内容を適用します。
「Edit」をクリックして、「Interval Time」で Gratuitous ARP を送信する間隔（秒）を編集します。

IPv6 Neighbor（IPv6 Neighbor 設定）

スイッチの IPv6 ネイバ設定を行います。

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

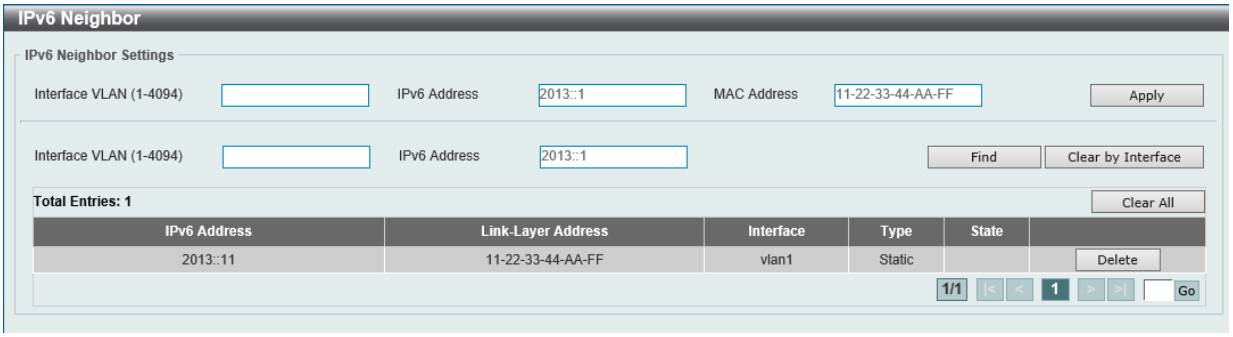


図 9-5　IPv6 Neighbor 画面

画面に表示される項目：

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

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

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

「Delete」をクリックして、指定のエントリを削除します。

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

Interface（インタフェース設定）

スイッチの IP インタフェース設定を行います。

IPv4 Interface（IPv4 インタフェース）

IPv4 インタフェースの設定を行います。

補足　設定可能な IPv4 インタフェースは最大 4 つまでです。

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

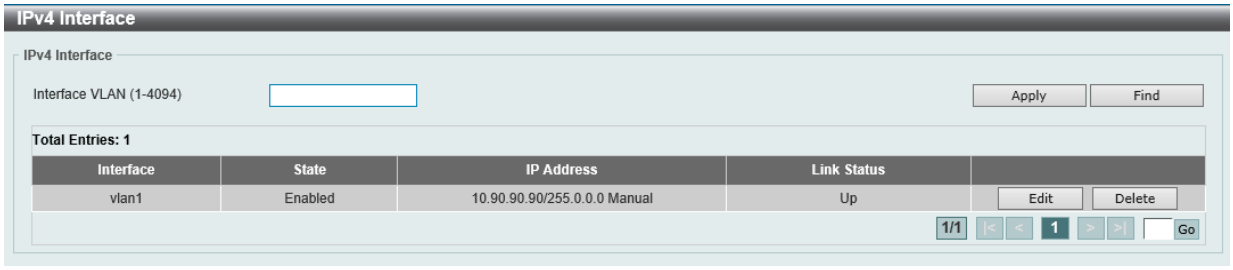


図 9-6　IPv4 Interface 画面

画面に表示される項目：

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

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

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

指定エントリの「Edit」をクリックして、以下の画面を表示します。

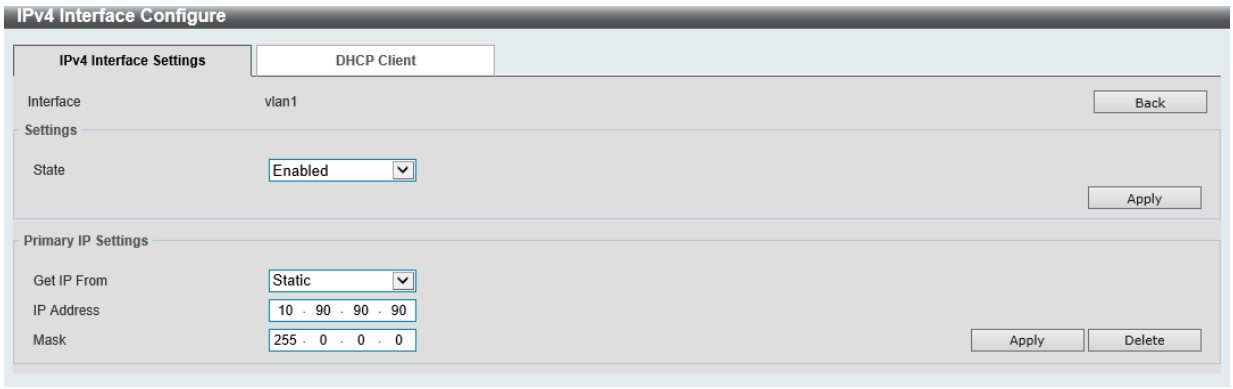


図 9-7　IPv4 Interface Configure - IPv4 Interface Settings 画面

画面に表示される項目：

項目	説明
Settings	
State	該当エントリの IPv4 インタフェースをグローバルに有効 / 無効にします。
Primary IP Settings	
Get IP From	IP アドレスの設定方法を選択します。 •「Static」- インタフェースに設定する IPv4 アドレスを手動で設定します。 •「DHCP」- ローカルネットワーク上の DHCP サーバから自動的に IPv4 情報を取得します。
IP Address	IPv4 インタフェースに割り当てる IPv4 アドレスを入力します。
Mask	IPv4 インタフェースに割り当てるサブネットマスクを入力します。

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

■ IPv4 インタフェースの編集（DHCP Client）

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

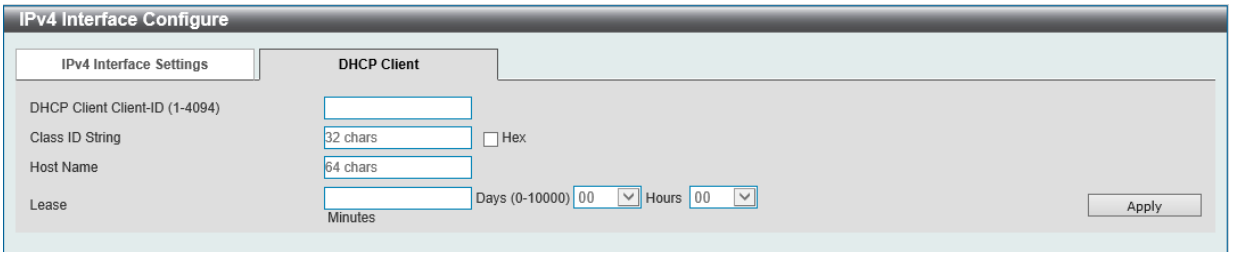


図 9-8　IPv4 Interface Configure - DHCP Client タブ 画面

画面に表示される項目：

項目	説明
DHCP Client Client-ID	DHCP クライアント ID を入力します。この ID は VLAN インタフェースを指定します。 該当インタフェースの 16 進数 MAC アドレスは、DISCOVER メッセージと一緒に送信されるクライアント ID として使用されます。 • 設定可能範囲：1-4094
Class ID String	クラス識別名を入力します。（32 文字以内） 「Hex」にチェックを入れると 16 進数方式になります。（64 文字以内） DHCP DISCOVER メッセージに含まれるオプション 60 の値として使用されます。
Host Name	ホスト名を入力します。（64 文字以内） DHCP DISCOVER メッセージと一緒に送信されるホスト名オプションの値です。
Lease	DHCP サーバから割り振られる IP アドレスのリース時間を指定します。オプションで時間と分を指定することもできます。 • 設定可能範囲：0-10000（日）

「Apply」をクリックして、設定内容を適用します。

IPv6 Interface（IPv6 インタフェース）

IPv6 インタフェースの設定を行います。

補足　設定可能な IPv6 インタフェースは最大 4 つまでです。

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

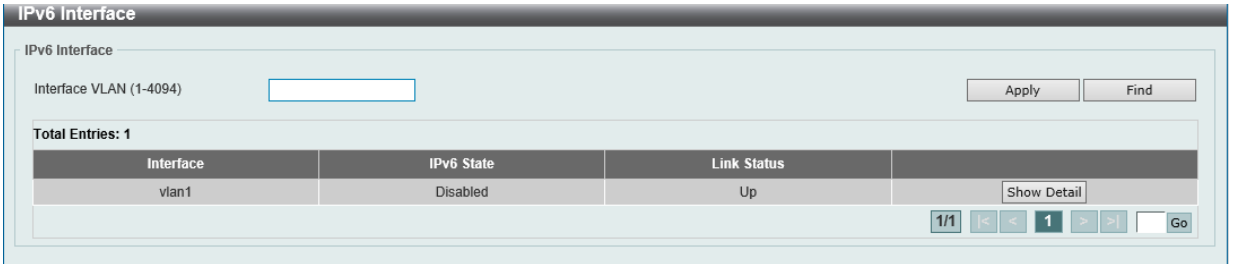


図 9-9　IPv6 Interface 画面

画面に表示される項目：

項目	説明
Interface VLAN	設定、表示する IPv6 インタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094

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

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

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

指定エントリの「Show Detail」をクリックして、「IPv6 Interface Settings」タブを表示します。

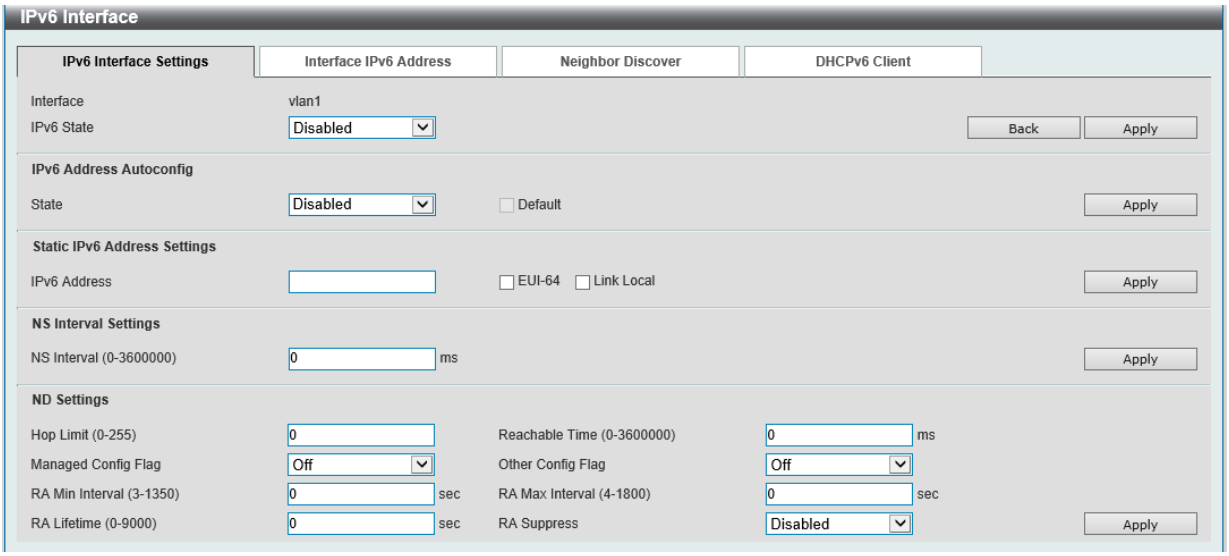


図 9-10　IPv6 Interface - IPv6 Interface Settings 画面

画面に表示される項目：

項目	説明
IPv6 State	該当エントリの IPv6 インタフェースをグローバルに有効 / 無効にします。
IPv6 Address Autoconfig	
State	ステートレス自動設定を使用した IPv6 アドレスの自動設定を有効 / 無効に設定します。 「Default」に指定すると、このインタフェースでデフォルトルータが選択されている場合、そのデフォルトルータを使用してデフォルトルートがインストールされます。このオプションは 1 つのインタフェースのみで指定可能です。
Static IPv6 Address Settings	
IPv6 Address	IPv6 インタフェースに割り当てる IPv6 アドレスを入力します。 • 「EUI-64」- EUI-64 インタフェース ID を使用してインタフェースの IPv6 アドレスを設定します。 • 「Link Local」- IPv6 インタフェースにリンクローカルアドレスを使用します。
NS Interval Settings	
NS Interval	Neighbor Solicitation（NS）間隔を指定します。 0 に指定した場合、1 秒間隔となり、RA メッセージには 0（未指定）の値がアドバタイズされます。 • 設定可能範囲：0-3600000（ミリ秒）（1000 の倍数）
ND Settings	
Hop Limit	ホップリミットを指定します。 システムから送信される IPv6 パケットも、最初のホップリミット値としてこの値を使用します。 • 設定可能範囲：0-255
Reachable Time	到達可能時間を指定します。 「0」に指定すると、1200 秒となり、RA メッセージでは 0（未指定）の値がアドバタイズされます。到達可能時間は、IPv6 ノードが、隣接しているノードの到達可否を判断する時間です。 • 設定可能範囲：0-3600000（ミリ秒）
Managed Config Flag	Managed Config Flag オプションを有効 / 無効に設定します。このフラグが有効な RA を受信すると、ネイバホストはステートフル設定プロトコルを使用して IPv6 アドレスを取得します。
Other Config Flag	Other Config Flag オプションを有効 / 無効に設定します。本設定を有効にすると、接続ホストはステートフル設定プロトコルを使用して、IPv6 アドレス以外の自動設定情報を取得します。
RA Min Interval	RA メッセージの再送信間隔の最小値を指定します。 • 設定可能範囲：3 - 1350（秒）。最大値の 75%未満である必要があります。
RA Max Interval	RA 通知の送信間隔の最大時間 を入力します。 • 設定可能範囲：4 - 1800（秒）
RA Lifetime	RA の有効期間を指定します。ホストは受信した RA に含まれる有効期間の値に基づき、送信元ルータをデフォルトルータとして使用します。 • 設定可能範囲：0-9000（秒）
RA Suppress	RA 抑制機能を有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

注意　IPv6 Intrface について、/64 より長い Prefix 長は付与できません。

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

指定エントリの「Show Detail」をクリックして、「Interface IPv6 Address」タブを表示します。

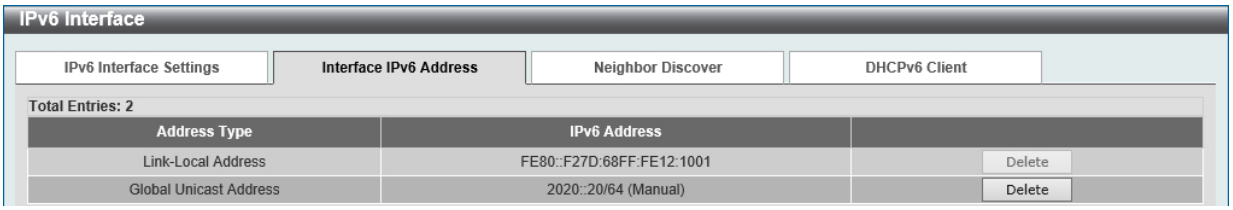


図 9-11　IPv6 Interface - Interface IPv6 Address 画面

「Delete」をクリックして、エントリを削除します。

IPv6 インタフェースの編集（Neighbor Discover タブ）

指定エントリの「Show Detail」をクリックして、「Neighbor Discover」タブを表示します。

図 9-12　IPv6 Interface - Neighbor Discover 画面

対象のエントリの「Edit」をクリックし、編集を行います。

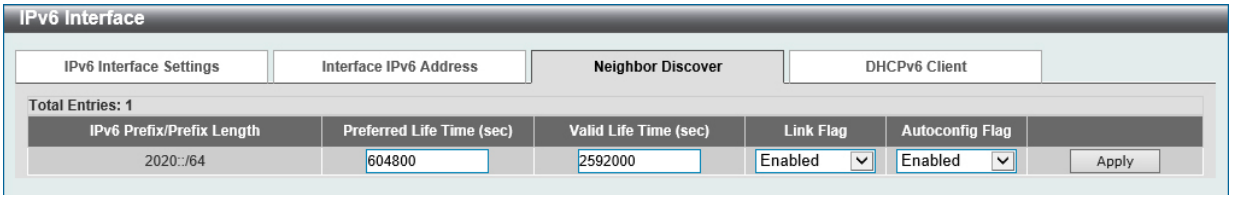


図 9-13　IPv6 Interface - Neighbor Discover 画面

画面に表示される項目：

項目	説明
Preferred Life Time	推奨有効期間を入力します。 • 設定可能範囲：0 - 4294967295（秒） • 初期値：604800（秒）＝（7 日）
Valid Life Time	有効期間を入力します。 • 設定可能範囲：0 - 4294967295（秒） • 初期値：2592000（秒）＝（30 日）
Link Flag	リンクフラグ機能の有効 / 無効を選択します。
Autoconfig Flag	自動設定フラグ機能の有効 / 無効を選択します。

「Apply」をクリックして、設定内容を適用します。

IPv6 インタフェースの編集（DHCPv6 Client タブ）

指定エントリの「Show Detail」をクリックして、「DHCPv6 Client」を表示します。

図 9-14　IPv6 Interface - DHCPv6 Client 画面

画面に表示される項目：

項目	説明
DHCPv6 Client	「Restart」をクリックすると、DHCPv6 クライアントサービスを再始動します。
Client State	DHCPv6 クライアントを有効 / 無効に設定します。 「Rapid Commit」を選択して、アドレス委任の 2 つのメッセージ交換を続行します。 「Rapid Commit」オプションは、2 メッセージのハンドシェイクを要求するための Solicit メッセージに含まれます。

「Apply」をクリックして、設定内容を適用します。

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

IPv4 スタティックおよびデフォルトルートの設定を行います。IPv4 には最大 128 個のスタティックルートエントリを作成することできます。

IPv4 スタティックルートが設定されると、スイッチによってネクストホップルータに ARP リクエストパケットが送信されます。スイッチに対しネクストホップから ARP の応答が返されると、ルートが有効になります。ただし、ARP エントリが既に存在している場合には、ARP 要求は送信されません。

スイッチはフローティングスタティックルートをサポートしています。ユーザは、異なるネクストホップを持つ代替のスタティックルートを作成することができます。この 2 個目のネクストホップデバイスのルートは、プライマリスタティックルートがダウンした場合のバックアップ用スタティックルートであると見なされます。プライマリルートが失われた場合、バックアップルートがアクティブになり、トラフィックの転送を開始します。

本スイッチのフォワーディングテーブル内のエントリは、IP アドレス、サブネットマスクおよびゲートウェイを使用して作成します。

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

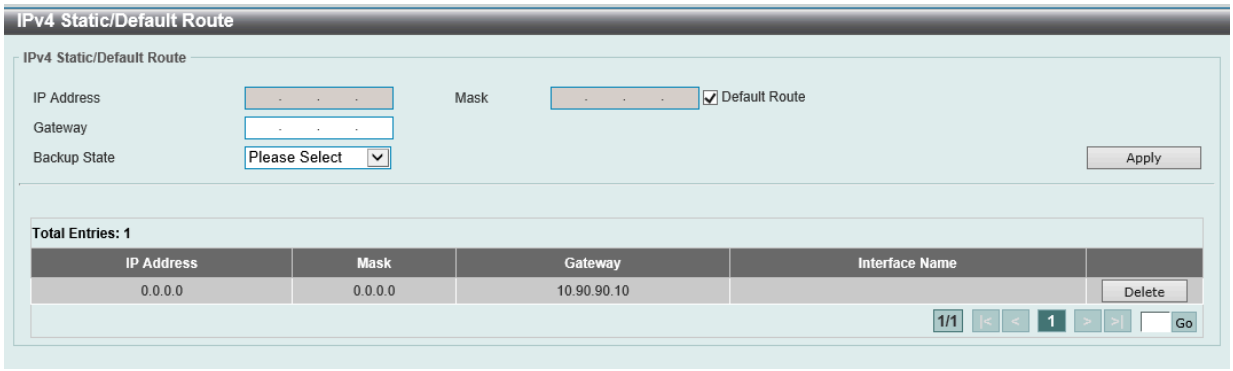


図 9-15　IPv4 Static/Default Route 画面

画面に表示される項目：

項目	説明
IP Address	スタティックルートに割り当てる IPv4 アドレスを入力します。 「Default Route」をチェックすると、IPv4 アドレスとしてデフォルトルートを使用します。
Mask	このルートのサブネットマスクを入力します。
Gateway	このルートのゲートウェイ IP アドレスを入力します。
Backup State	バックアップオプションを選択します。 • 「Primary」- 宛先へのプライマリルートとしてルートを指定します。 • 「Backup」- 宛先へのバックアップルートとしてルートを指定します。

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

IPv4 Route Table（IPv4 ルートテーブル）

IPv4 ルートテーブルの設定を行います。

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

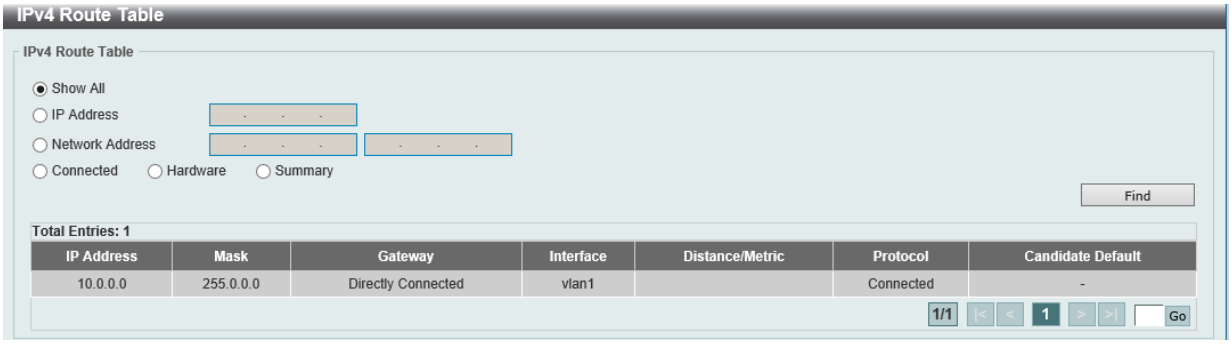


図 9-16　IPv4 Route Table 画面

画面に表示される項目：

項目	説明
Show All	すべての IPv4 ルートを表示します。
IP Address	表示するルートの宛先 IP アドレスを指定します。
Network Address	表示するルートの宛先ネットワークアドレスを指定します。 1 つ目の入力欄にネットワークプレフィックス、2 つ目の入力欄にネットワークマスクを入力します。
Connected	接続されたルートのみを表示します。
Hardware	ハードウェアチップに記録されたルートのみ表示されます。
Summary	スイッチに設定されているルートソースの概要と数が表示されます。

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

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

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

IPv6 スタティック / デフォルトルートを表示、設定します。

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

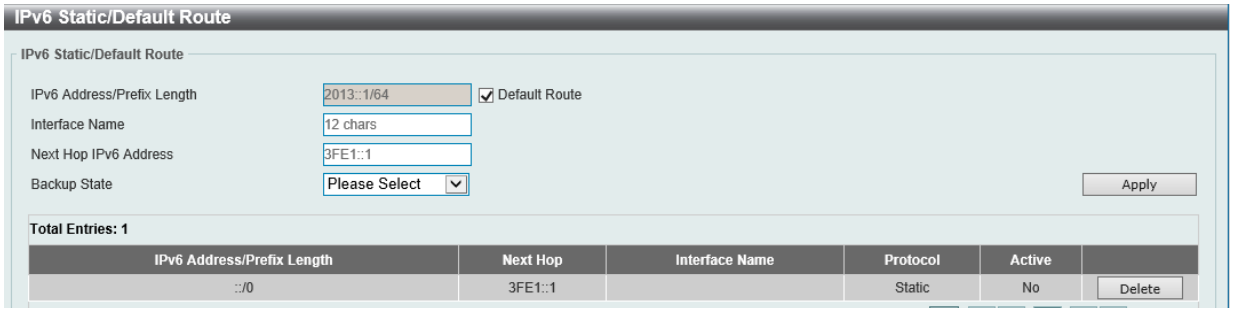


図 9-17　IPv6 Static/Default Route 画面

画面に表示される項目：

項目	説明
IPv6 Address/Prefix Length	ルートの IP アドレスとプレフィックス長を入力します。デフォルトルートを IPv6 アドレスとして使用するには、「Default Route」オプションを選択します。
Interface Name	このルートに関連付けるインタフェース名を入力します。
Next Hop IPv6 Address	ネクストホップ IPv6 アドレスを入力します。
Backup State	バックアップオプションを選択します。 • 「Primary」- 宛先へのプライマリルートとして設定されます。 • 「Backup」- 宛先へのバックアップルートとして設定されます。

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

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

IPv6 Route Table（IPv6 ルートテーブル）

現在の IPv6 ルーティングテーブルを表示します。

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

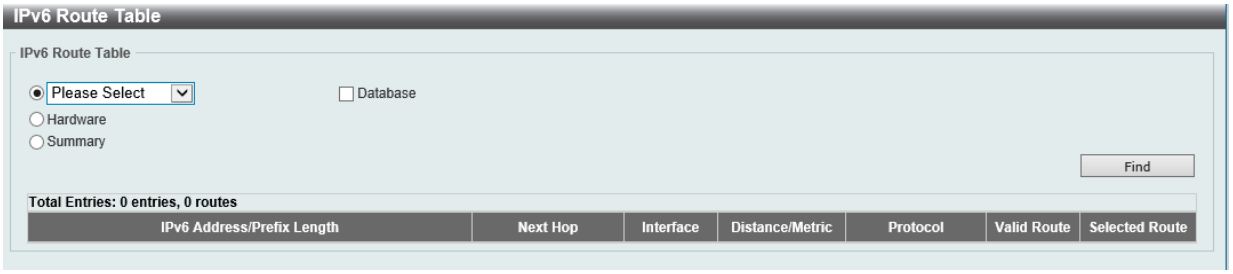


図 9-18　IPv6 Route Table 画面

画面に表示される項目：

項目	説明
IPv6 Address	プルダウンメニューから本項目を選択し、表示する IPv6 アドレスを入力します。
IPv6 Address/Prefix Length	プルダウンメニューから本項目を選択し、IPv6 アドレスとプレフィックス長を入力します。 「Longer Prefixes」を選択すると、指定プレフィックス長より長いすべての IPv6 ルートを表示します。
Interface VLAN	プルダウンメニューから本項目を選択し、表示するインタフェース VLAN を入力します。
Connected	プルダウンメニューから本項目を選択し、接続されたルートのみ表示します。
Database	チェックボックスにチェックを入れると、ルーティングデータベースのエントリをすべて表示します。
Hardware	ハードウェアルートのみを表示するにはこのオプションを選択します。 ハードウェアルートは、ハードウェアチップに書き込まれているルートです。
Summary	チェックボックスにチェックを入れると、このスイッチで設定されたルートソースの概要と数を表示します。

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

IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル設定）

L3 Features > IP Multicast Routing Protocol
IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）の設定を行います。

IPMC（IPMC 設定）

IP Multicast Routing Forwarding Cache Table（IP マルチキャストルーティングフォワーディングキャッシュテーブル）

IP Multicast Forwarding Cache（IP マルチキャストフォワーディングキャッシュ）データベースの表示、設定を行います。

L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Routing Forwarding Cache Table の順にメニューをクリックして、以下の画面を表示します。

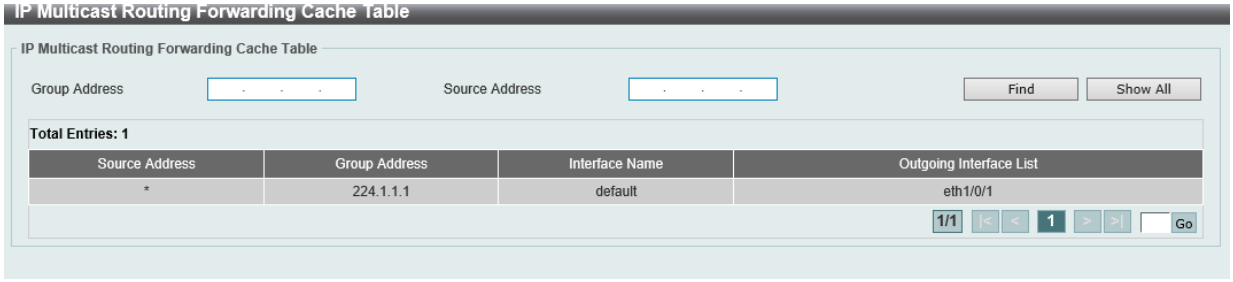


図 9-19　IP Multicast Routing Forwarding Cache Table 画面

画面に表示される項目：

項目	説明
Group Address	マルチキャストグループ IP アドレスを指定します。
Source Address	マルチキャストソース IP アドレスを指定します。

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

IPv6MC（IPv6MC 設定）

IPv6 Multicast Routing Forwarding Cache Table（IPv6 マルチキャストルーティングフォワーディングキャッシュテーブル）

IPv6 Multicast Forwarding Cache（IPv6 マルチキャストフォワーディングキャッシュ）データベースを表示します。

L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Forwarding Cache Table の順にメニューをクリックして、以下の画面を表示します。

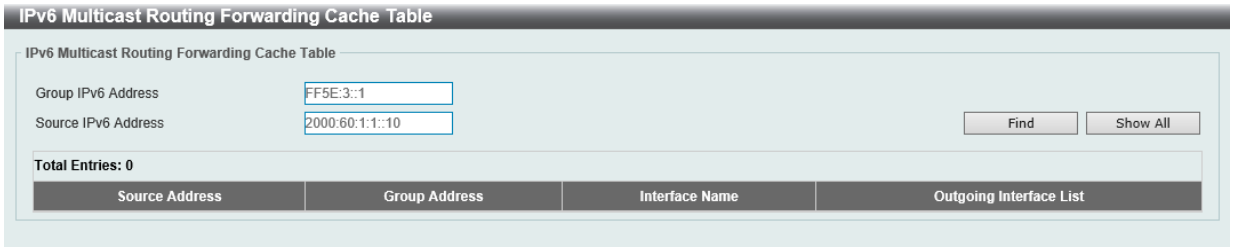


図 9-20　IPv6 Multicast Routing Forwarding Cache Table 画面

画面に表示される項目：

項目	説明
Group IPv6 Address	マルチキャストグループ IPv6 アドレスを指定します。
Source IPv6 Address	ソース IPv6 アドレスを指定します。

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

第 10 章　QoS（QoS 機能の設定）

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

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

サブメニュー	説明
Basic Settings（基本設定）	QoS の Basic Settings（基本設定）を行います。
Advanced Settings（詳細設定）	QoS の Advanced Settings（詳細設定）を行います。

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。

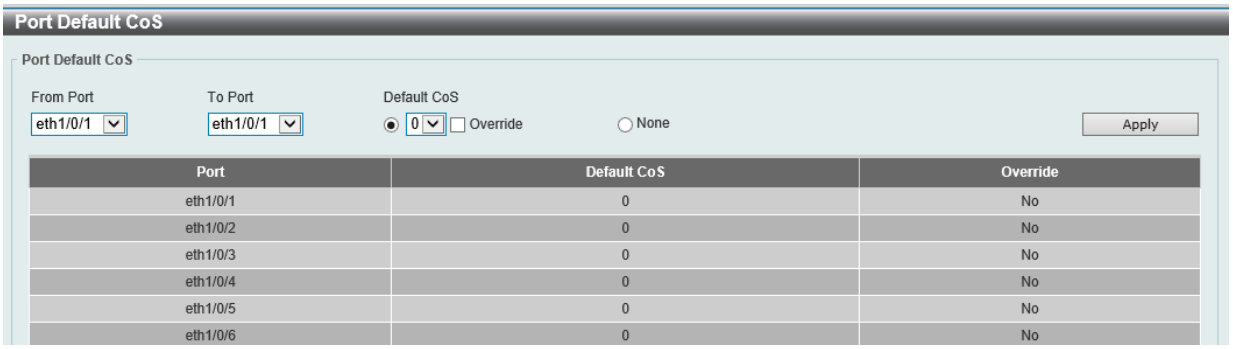


図 10-1　Port Default CoS 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Default CoS	ポートのデフォルト CoS を指定します。「Override」にチェックを入れると、パケットの CoS を上書きします。デフォルト CoS は、ポートで受信した全てのパケット（タグ付き / タグなしの両方）に適用されます。「None」を選択すると、タグ付きパケットの場合はパケットの CoS を使用し、タグなしパケットの場合はポートデフォルト CoS となります。 • 設定可能範囲：0-7

「Apply」をクリックして、設定内容を適用します。

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

ポートスケジューラメソッドを設定します。

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

図 10-2　Port Scheduler Method 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Scheduler Method	指定ポートに対するスケジューリングの方法を設定します。 • 「SP」- すべてのキューは Strict Priority（絶対優先）スケジューリングを使用します。最も高い CoS 優先度のキューから絶対優先で送信されます。 • 「RR」- すべてのキューは Round-Robin スケジューリングを使用します。キューを順番に見ながら、均等な比率でパケットが処理されます。 • 「WRR」- Round-Robin 方式でパケットをキューに送出します。最初に、各キューは可変の重みをセットします。CoS キューからパケットが送信される度に、重み（Weight）の値から「1」が差し引かれ、次の CoS 優先度キューが処理されます。重みが「0」になると、重みが補充されるまでそのキューの処理は停止します。すべての CoS キューの重みが「0」に到達すると、キューの重みが補充されます。（初期値） • 「WDRR」- Round-Robin 方式で送信キューに蓄積された未処理のクレジットを処理します。最初に、各キューはクレジットカウンタを可変の数値にセットします。CoS キューからパケットが送信される度に、クレジットカウンタからパケットサイズが差し引かれ、次の CoS 優先度キューが処理されます。クレジットカウンタが「0」になると、クレジットが補充されるまでそのキューの処理は停止します。すべての CoS キューのクレジットカウンタが「0」に到達すると、クレジットカウンタが補充されます。クレジットカウンタが 0 またはマイナスになり、最後のパケット送信が完了するまで処理が行われます。その後、クレジットは補充されます。クレジットが補充されると、各 CoS キューのクレジットカウンタにクレジットのクオンタムが補充されます。各キューのクオンタムはユーザ定義により異なる場合があります。 特定の CoS キューを SP モードに設定する場合、それより優先度の高い CoS キューについても SP モードである必要があります。

「Apply」をクリックして、設定内容を適用します。

Queue Settings（QoS 設定）

キューを設定、表示します。

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

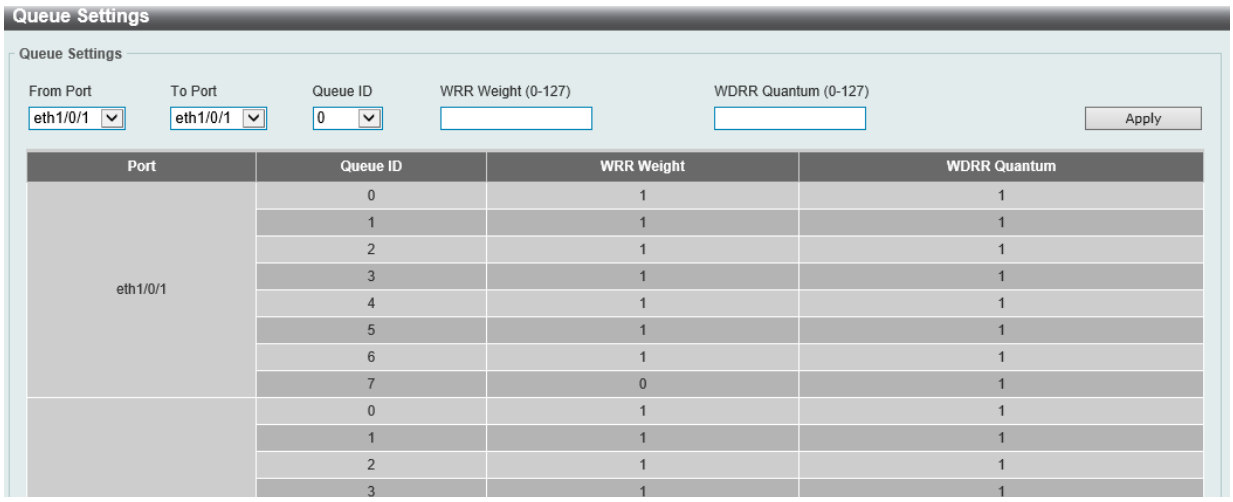


図 10-3　Queue Settings 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Queue ID	キュー ID を指定します。 • 設定可能範囲：0-7
WRR Weight	WRR の値を入力します。 「Expedited Forwarding」(EF) の動作要件を満たすには、最も優先度の高いキューが常に「Per-hop Behavior」(PHB) により選択され、キューのスケジュールモードが Strict プライオリティである必要があります。そのため、「Differentiate Service」がサポートされている場合、最後のキューの重みは 0 に設定する必要があります。 • 設定可能範囲：0-127
WDRR Quantum	「WDRR Quantum」の値を入力します。 • 設定可能範囲：0-127

「Apply」をクリックして、設定内容を適用します。

CoS to Queue Mapping（CoS キューマッピング設定）

CoS-to-Queue マッピングの表示、設定を行います。

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

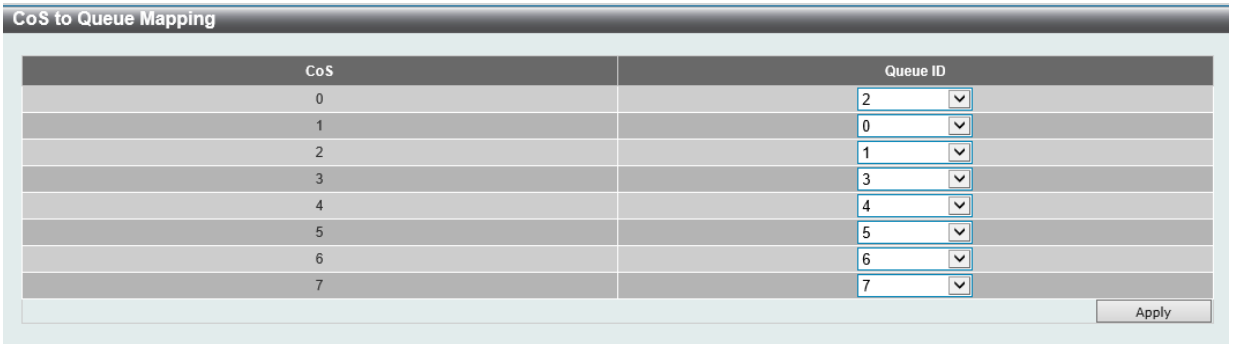


図 10-4　CoS to Queue Mapping 画面

画面に表示される項目：

項目	説明
Queue ID	各 CoS 値にマッピングされるキュー ID を指定します。 • 選択肢：0-7

「Apply」をクリックして、設定内容を適用します。

Port Rate Limiting（ポートレート制限設定）

ポートレート制限の設定を行います。

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

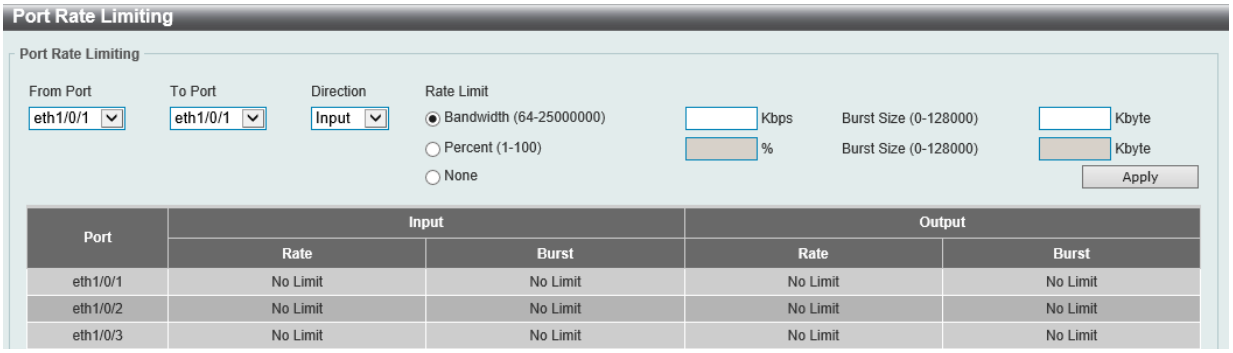


図 10-5　Port Rate Limiting 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Direction	レート制限の対象を指定します。 • 「Input」- イングレスパケットに対してレート制限を行います。 • 「Output」- イーグレスパケットに対してレート制限を行います。
Rate Limit	レート制限の値を指定します。 指定された制限は、指定インタフェースの最大速度を超えることはできません。受信帯域幅制限の場合、受信トラフィックが制限を超えたときに、受信側は PAUSE フレームまたはフロー制御フレームを送信します。 • 「Bandwidth」- 受信 / 送信の帯域幅の値を入力欄に入力します。 - 設定可能範囲：64-25000000（Kbps） - 「Burst Size」：0-128000（Kbytes） • 「Percent」- 受信 / 送信の帯域幅パーセンテージを入力欄に入力します。 - 設定可能範囲：1-100（%） - 「Burst Size」：0-128000（Kbytes） • 「None」- 指定ポートのレート制限を削除します。

「Apply」をクリックして、設定内容を適用します。

注意　「Bandwidth」の「Burst Size」を「0」に設定した場合、レート制限は行われません。

Queue Rate Limiting（キューレート制限設定）

キューレートの制限設定をします。

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

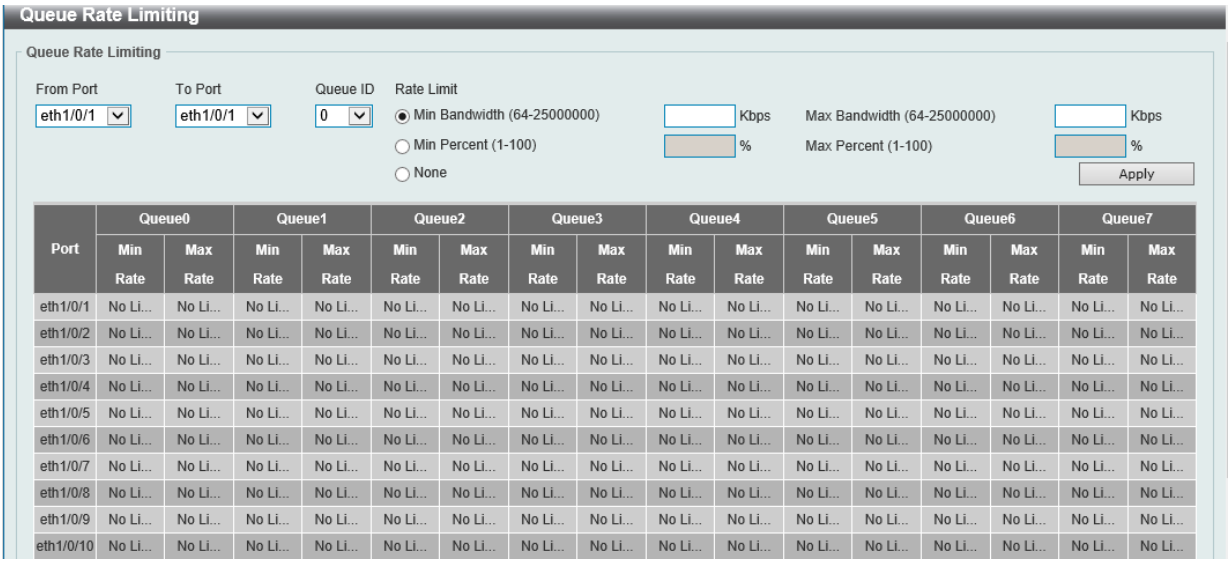


図 10-6　Queue Rate Limiting 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Queue ID	キュー ID を指定します。 • 選択肢：0-7
Rate Limit	キューレート制限の設定を行います。 • 「Min Bandwidth / Max Bandwidth」- 最小 / 最大のレート制限帯域値を入力します。 　- 設定可能範囲：64-25000000（Kbps） • 「Min Percent / Max Percent」- 最小 / 最大のレート制限パーセンテージを入力します。 　- 設定可能範囲：1-100（%） • 「None」- 指定ポートのレート制限を「なし」に設定します。 最小帯域の値により、キューから送信されるパケットが保証されます。また、帯域幅に余裕がある場合でも、キューからの送信パケットは最大帯域幅を超えることはありません。 各キューの最小帯域幅が保証されるようにするために、最小帯域幅の合計はインタフェース帯域幅の 75% 未満である必要があります。最も優先度の高い Strict プライオリティキューに対しては、最低保証帯域幅を設定する必要はありません。これは、すべてのキューの最小帯域幅が一杯である場合にはこのキューのトラフィックが最初に処理されるためです。 本設定は 1 つの物理ポートに対してのみ設定可能で、ポートチャネルに対しては設定できません。1 つの CoS における最小保証帯域は、複数の物理ポートにまたがって使用することはできないためです。

「Apply」をクリックして、設定内容を適用します。

Advanced Settings（詳細設定）

DSCP Mutation Map（DSCP 変更マップ設定）

本項目では「Differentiated Services Code Point」(DSCP) 変更マップ設定を行います。
インタフェースでパケットを受信すると、QoS 関連の処理の前に、DSCP 変更マップに基づき受信 DSCP が他の DSCP に変更されます。DSCP 変更機能は、異なる DSCP 割り当てを持つドメインを統合する場合に役に立ちます。DSCP-CoS マップと DSCP-color マップはパケット本来の DSCP に基づいて動作します。後続のすべての動作は変更 DSCP に基づいて行われます。

QoS > Advanced Settings > DSCP Mutation Map の順にクリックし、以下の画面を表示します。

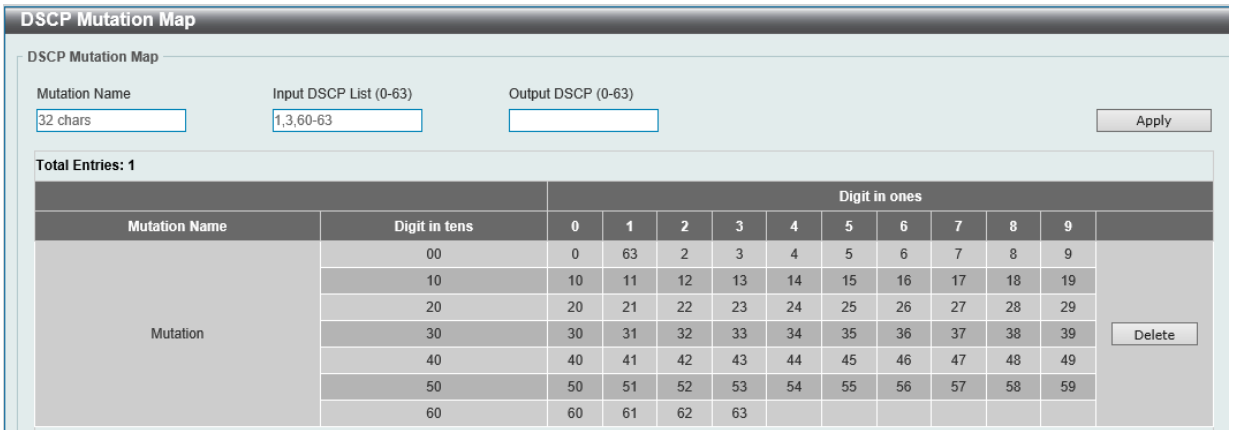


図 10-7　DSCP Mutation Map 画面

画面に表示される項目：

項目	説明
Mutation Name	DSCP 変更マップ名を指定します。（32 文字以内）
Input DSCP List	インプット DSCP リストの値を入力します。 ・ 設定可能範囲：0-63
Output DSCP	アウトプット DSCP リストの値を入力します。 ・ 設定可能範囲：0-63

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

Port Trust State and Mutation Binding（ポートトラスト設定 & 変更マップバインディング）

ポートトラスト設定、変更マップのバインディング設定を行います。

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

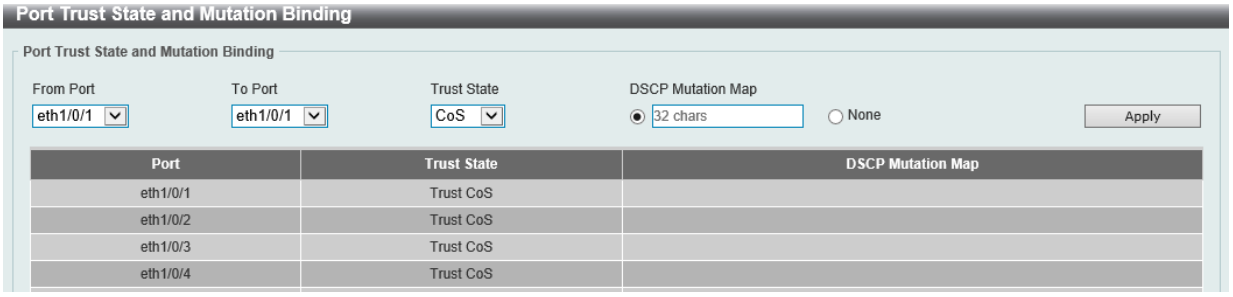


図 10-8　Port Trust State and Mutation Binding 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Trust State	ポートトラストのオプションを指定します。 ・ 選択肢：「CoS」「DSCP」
DSCP Mutation Map	DSCP 変更マップ名を入力します。（32 文字以内） 「None」を選択すると、DSCP 変更マップがポートに割り当てられません。

「Apply」をクリックして、設定内容を適用します。

DSCP CoS Mapping（DSCP CoS マップ設定）

本スイッチにおける DSCP CoS マップの設定と表示を行います。

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

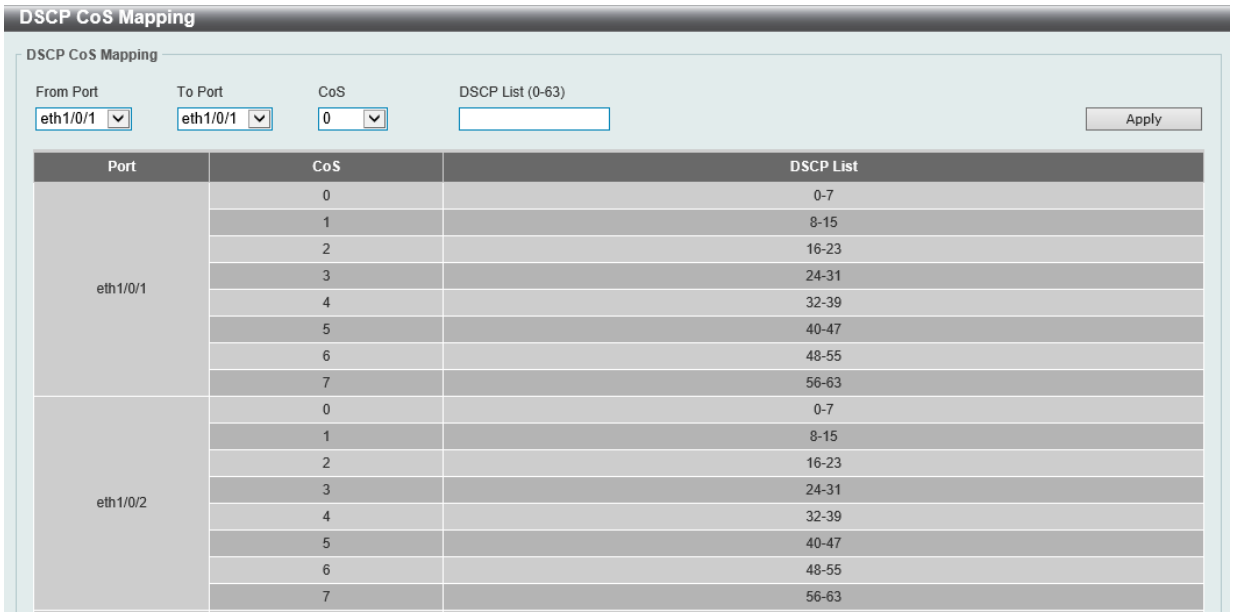


図 10-9　DSCP CoS Mapping 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
CoS	DSCP リストにマッピングする CoS 値を指定します。 • 設定可能範囲：0-7
DSCP List	CoS 値をマッピングする DSCP リストの値を入力します。 • 設定可能範囲：0-63

「Apply」をクリックして、設定内容を適用します。

Class Map（クラスマップ設定）

本スイッチにおけるクラスマップの設定と表示を行います。

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

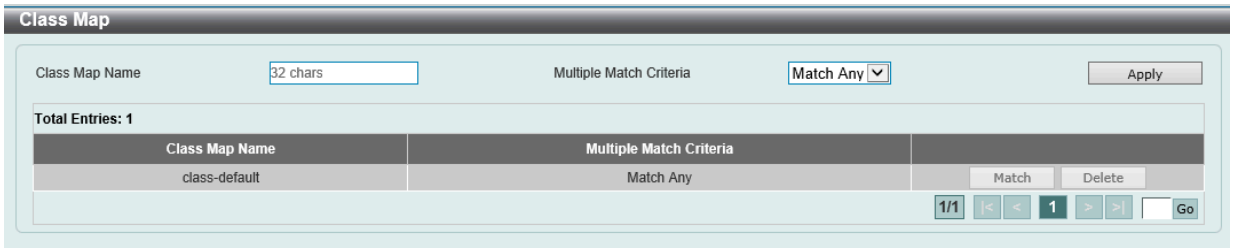


図 10-10　Class Map 画面

画面に表示される項目：

項目	説明
Class Map Name	クラスマップ名を指定します。（32 文字以内）
Multiple Match Criteria	一致条件の種類を指定します。 • 選択肢：「Match All」（すべて一致）、「Match Any」（いずれかに一致）

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

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

エントリの設定

「Match」をクリックすると下記の画面が表示されます。

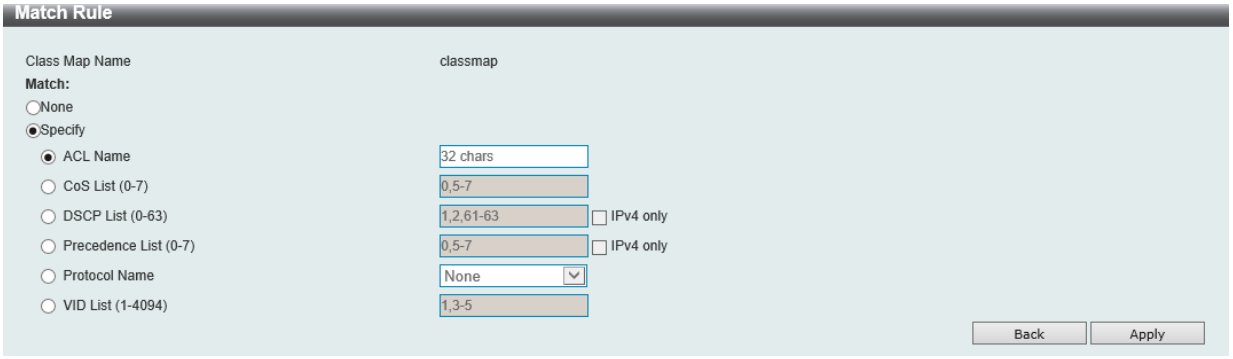


図 10-11　Class Map - Match Rule 画面

画面に表示される項目：

項目	説明
None	このクラスマップでは照合を行いません。
Specify	このクラスマップでは下記のいずれかのオプションで照合を行います • 「ACL Name」- クラスマップで照合するアクセスリスト名を指定します。（32 文字以内） • 「CoS List」- クラスマップで照合する CoS リスト値を指定します。「Inner」を指定すると、レイヤ 2 CoS マーキングの QinQ パケット内のインナモースト CoS を照合します。 - 設定可能範囲：0-7 • 「DSCP List」- クラスマップで照合する DSCP リスト値を指定します。「IPv4 only」にチェックを入れると、IPv4 パケットのみ照合します。チェックを入れない場合、IPv4/v6 両方のパケットを照合します。 - 設定可能範囲：0-63 • 「Precedence List」- クラスマップで照合する Precedence リスト値を指定します。「IPv4 only」にチェックを入れると、IPv4 パケットのみ照合します。チェックを入れない場合、IPv4/v6 両方のパケットを照合します。IPv6 パケットの場合、IPv6 ヘッダに含まれるトラフィッククラスの上位 3 ビットが Precedence になります。 - 設定可能範囲：0-7 • 「Protocol Name」- クラスマップで照合するプロトコル名を指定します。 - 選択肢：「None」「ARP」「BGP」「DHCP」「DNS」「EGP」「FTP」「IPv4」「IPv6」「NetBIOS」「NFS」「NTP」「OSPF」「PPPOE」「RIP」「RTSP」「SSH」「Telnet」「TFTP」 • 「VID List」- クラスマップで照合する VLAN リスト値を指定します。 - 設定可能範囲：1-4094

「Apply」をクリックして、設定内容を適用します。

「Back」をクリックすると前のページに戻ります

Policy Map（ポリシーマップ設定）

本スイッチにおけるポリシーマップの設定と表示を行います。

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

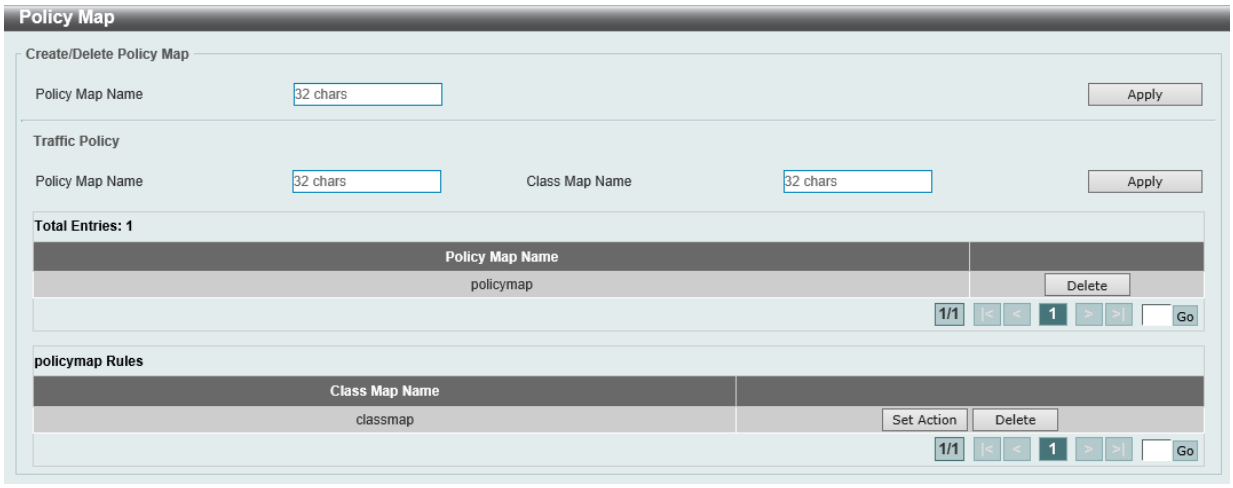


図 10-12　Policy Map 画面

画面に表示される項目：

項目	説明
Create/Delete Policy Map	
Policy Map Name	ポリシーマップ名を指定します。（32 文字以内）
Traffic Policy	
Policy Map Name	ポリシーマップ名を指定します。（32 文字以内）
Class Map Name	クラスマップ名を指定します。（32 文字以内）

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

Class Map の編集

「Set Action」をクリックし、アクション設定を行います。

ポリシーマップのエントリをクリックすると、画面下部にクラスマップが表示されます。「Set Action」をクリックし、以下の画面を表示します。

図 10-13　Set Action 画面

画面に表示される項目：

項目	説明
None	アクションを実行しません。
Specify	設定に基づきアクションを実行します。 • 「New Precedence」- 新しい Precedence 値を選択します。「IPv4 only」にチェックを入れると、IPv4 Precedence のみマークされます。チェックを入れない場合、IPv4/v6 両方の Precedence がマークされます。IPv6 パケットの場合、IPv6 ヘッダに含まれるトラフィッククラスの上位 3 ビットが Precedence になります。Precedence の設定は CoS キュー選択には影響しません。 - 設定可能範囲：0-7 • 「New DSCP」- パケットの新しい DSCP 値を指定します。「IPv4 only」にチェックを入れると、IPv4 DSCP のみマークされます。チェックを入れない場合、IPv4/v6 両方の DSCP がマークされます。DSCP の設定は CoS キュー選択には影響しません。 - 設定可能範囲：0-63 • 「New CoS」- パケットの新しい CoS 値を指定します。入力インタフェースにポリシーマップが適用されている場合、CoS 値の設定は CoS キュー選択に影響します。 - 設定可能範囲：0-7 • 「New CoS Queue」- パケットの新しい CoS キュー値を指定します。元の CoS キュー選択は上書きされます。インタフェースの出力フローにポリシーマップが適用されている場合、CoS 値の設定は影響しません。 - 設定可能範囲：0-7

「Apply」をクリックして、設定内容を適用します。

Policy Binding（ポリシーバインディング設定）

ポリシーバインディング設定を行います。

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

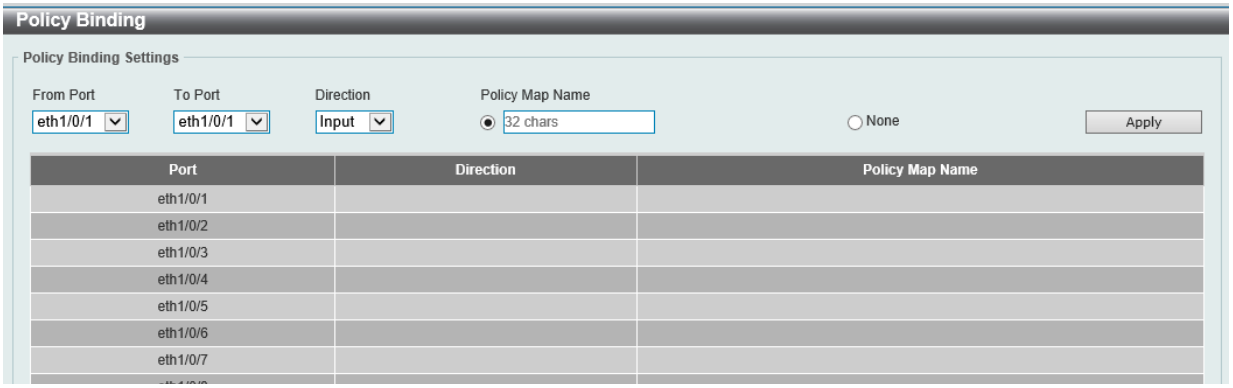


図 10-14　Policy Binding 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Direction	トラフィックの方向を指定します。 • 選択肢「Input」、「Output」
Policy Map Name	ポリシーマップ名を指定します。（32 文字以内） 「None」を選択すると本エントリにポリシーマップは関連付けられません。

「Apply」をクリックして、設定内容を適用します。

第 11 章　ACL（ACL 機能の設定）

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

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

サブメニュー	説明
ACL Configuration Wizard（ACL 設定ウィザード）	ウィザードを使用してアクセスプロファイルとルールを作成します。
ACL Access List（ACL アクセスリスト）	ACL アクセスリストの設定をします。
ACL Interface Access Group（ACL インタフェースアクセスグループ）	ACL インタフェースアクセスグループの設定を行います。

ACL Configuration Wizard（ACL 設定ウィザード）

ACL Configuration Wizard（ACL 設定ウィザードの開始）

ACL 設定ウィザードは、アクセスプロファイルと ACL ルールの編集、新規作成を行います。

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

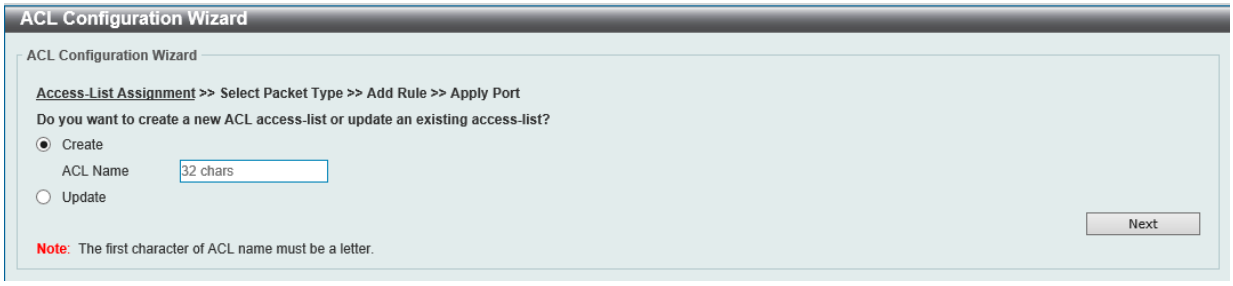


図 11-15　ACL Configuration Wizard 画面（Create）

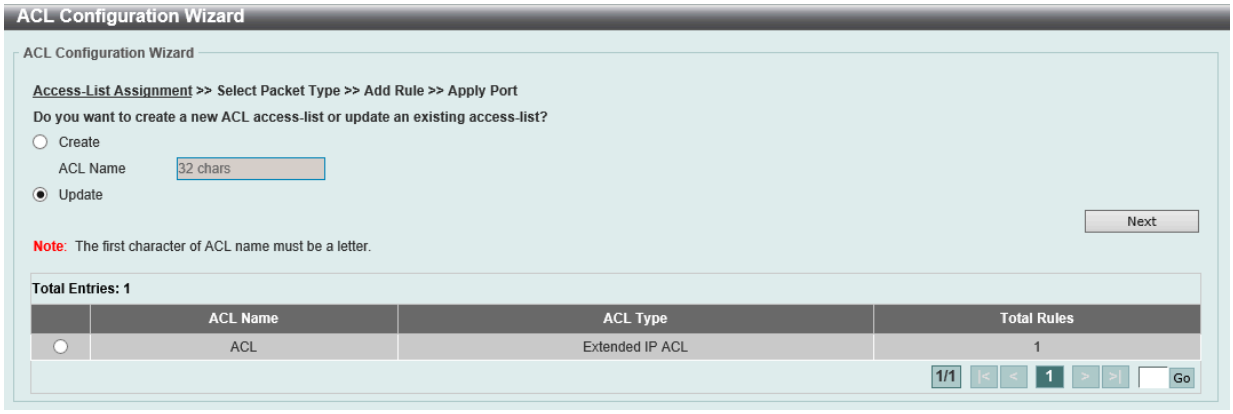


図 11-16　ACL Configuration Wizard 画面（Update）

画面に表示される項目：

項目	説明
Create	新しいアクセスルールを作成する場合は、「Create」を選択します。
ACL Name	作成する ACL 名を指定します。（32 文字以内）
Update	既存の ACL アクセスリストを表示し、エントリを再設定する場合に選択します。

「Next」をクリックし、パケットタイプの選択を行います。

パケットタイプ選択（ACL 設定ウィザード）

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

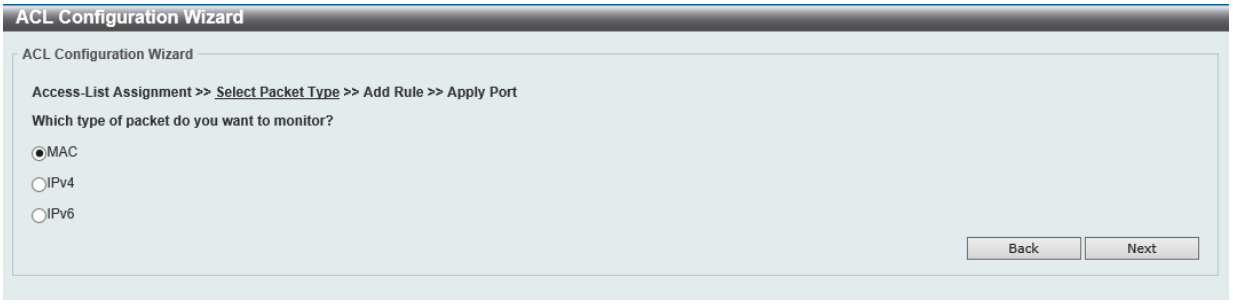


図 11-17　ACL Configuration Wizard（Select Packet Type）画面

画面に表示される項目：

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

「Next」をクリックします。
選択したパケットの種類により、次に表示される画面が異なります。プロファイルの種類に合わせた設定方法に従い設定を行います。

ルール追加（ACL 設定ウィザード）

「ACL Configuration Wizard」にて ACL のパケットタイプを指定した後、各パケットの ACL エントリにおける ACL ルールの追加設定を行います。

MAC ACL の設定

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

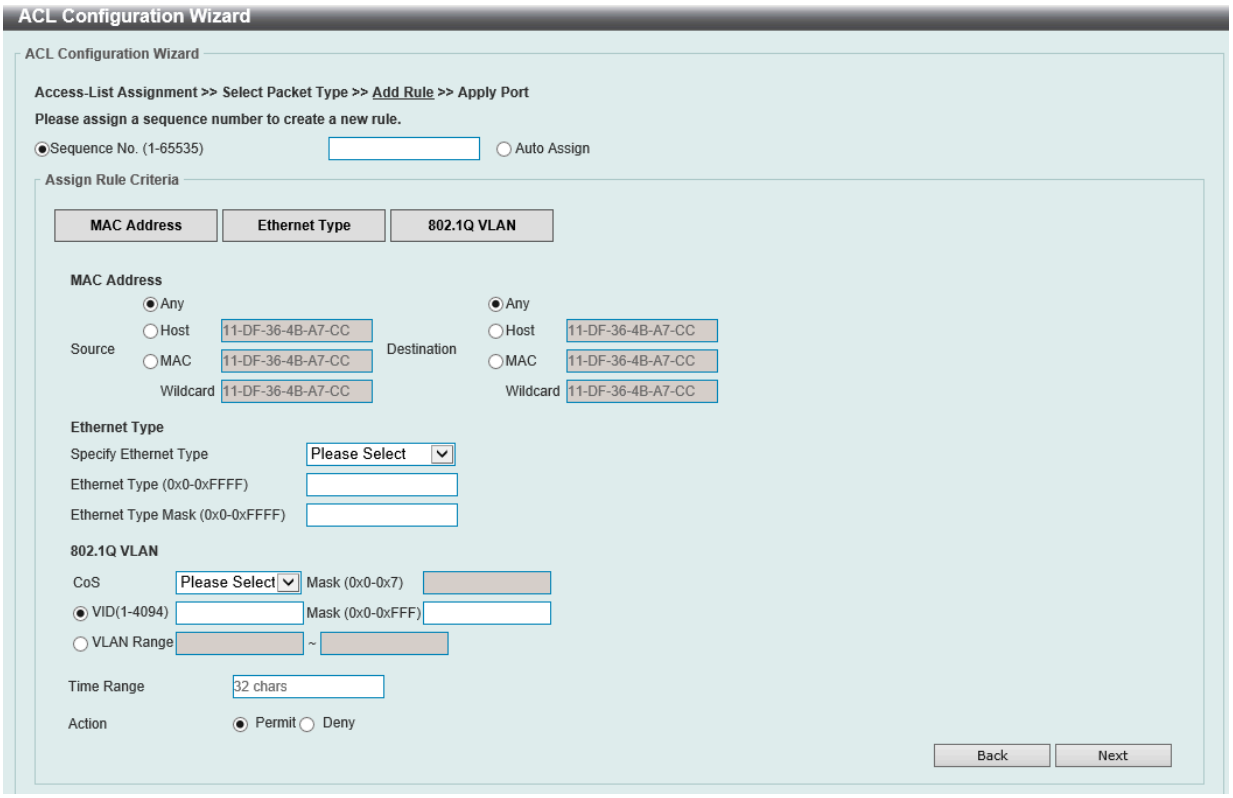


図 11-18　ACL Configuration Wizard 画面（Extended MAC ACL）

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Assign Rule Criteria	
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力することができます。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
Specify Ethernet Type	イーサネットタイプを選択します。 • 選択肢：「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
Ethernet Type	イーサネットタイプの 16 進数値を指定します。 「Specify Ethernet Type」ドロップダウンリストでイーサネットタイププロファイルを選択すると、適切な 16 進数値が自動的に入力されます。 • 設定可能範囲：0x0-0xFFFF
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。 「Specify Ethernet Type」ドロップダウンリストでイーサネットタイププロファイルを選択すると、適切な 16 進数値が自動的に入力されます。 • 設定可能範囲：0x0-0xFFFF
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに適用する VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）
VLAN Range	ACL ルールに紐づける VLAN 範囲（開始 VLAN/ 終了 VLAN）を入力します。 • 設定可能範囲：1-4094
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit」「Deny」

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

IPv4 ACL Rule の設定

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

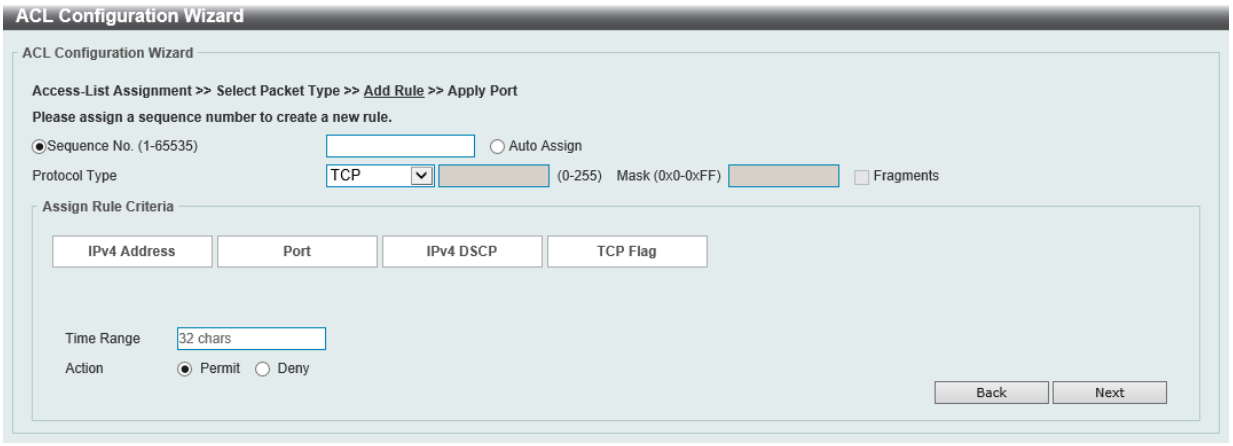


図 11-19　ACL Configuration Wizard 画面（Standard IPv4 ACL）

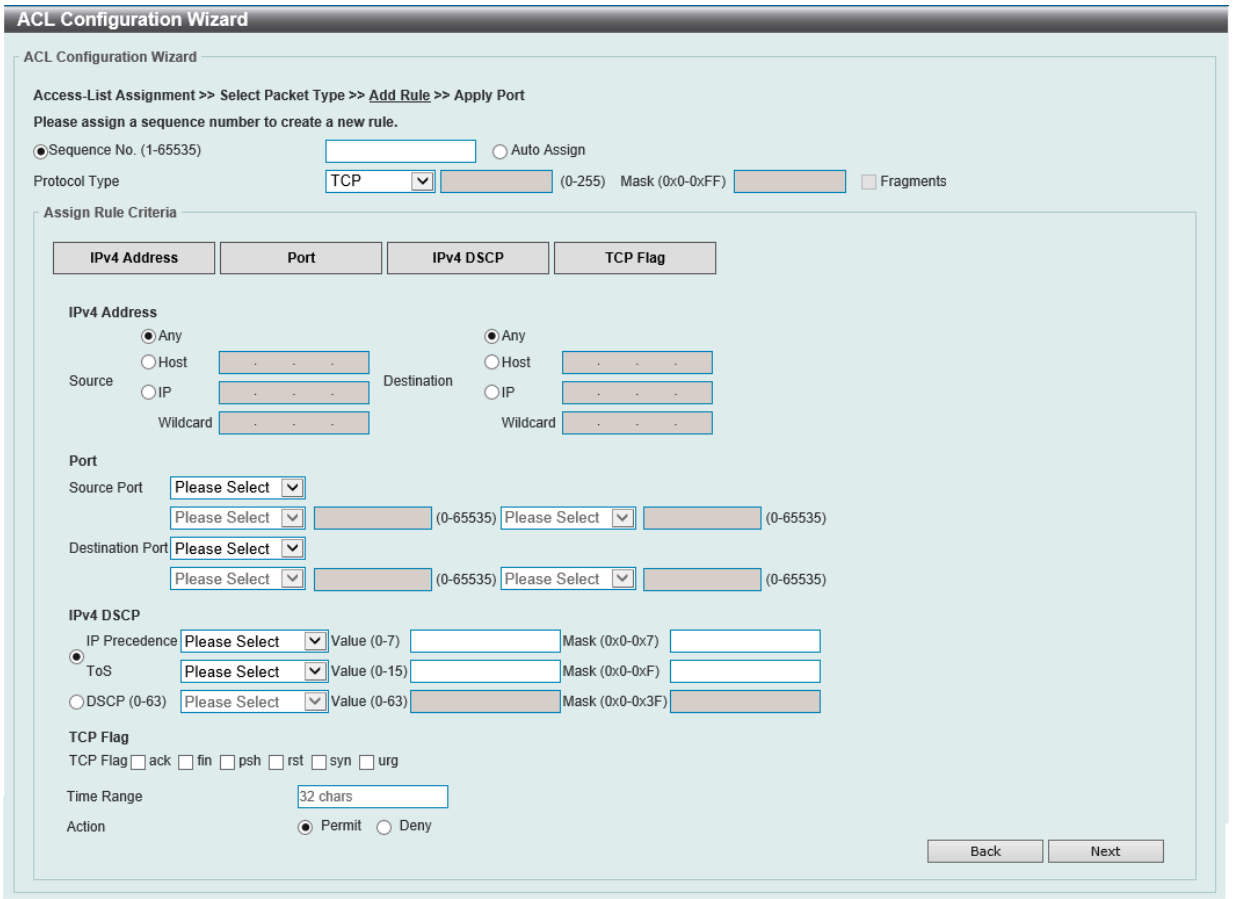


図 11-20　ACL Configuration Wizard 画面（Extended IPv4 ACL）

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Protocol Type	プロトコルの種類を以下から選択します。 • 「TCP」「UDP」「ICMP」「EIGRP (88)」「ESP (50)」「GRE (47)」「IGMP (2)」「OSPF (89)」「PIM (103)」「VRRP (112)」「IP-in-IP(94)」「PCP (108) 」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

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

項目	説明
Source	送信元のアドレスを指定します • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
IP Precedence	IP 優先値を指定します。 • 選択肢：「0（routine）」「1（priority）」「2（immediate）」「3（flash）」「4（flash-override）」「5（critical）」「6（internet）」「7（network）」 - 「Value」- IP 優先値を入力します。（0-7） - 「Mask」- IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」（ToS）の値を以下から指定します。 • 選択肢：「normal (0)」「min-monetary-cost (1)」「max-reliability (2)」「max-throughput (4)」「min-delay (8)」 - 「Value」- ToS 値を入力します。（0-15） - 「Mask」- ToS マスクを入力します。（0x0-0xF）
DSCP	使用する DSCP 値を選択します。 • 「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」- DSCP 値を入力します。（0-63） - 「Mask」- DSCP マスクを入力します。（0x0-0x3F）
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit」「Deny」

「Next」をクリックします。

IPv6 ACL Rule の設定

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

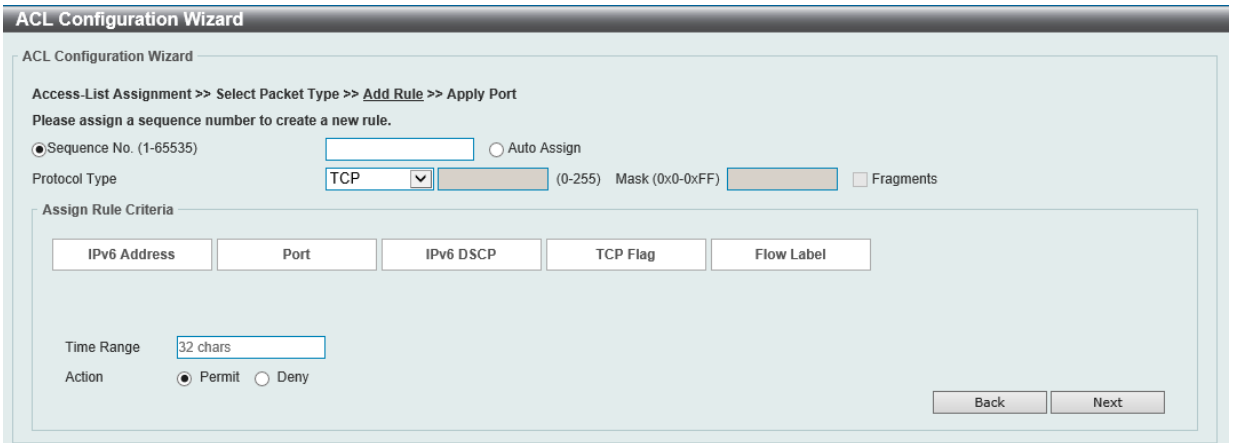


図 11-21　ACL Configuration Wizard 画面（Standard IPv6 ACL）

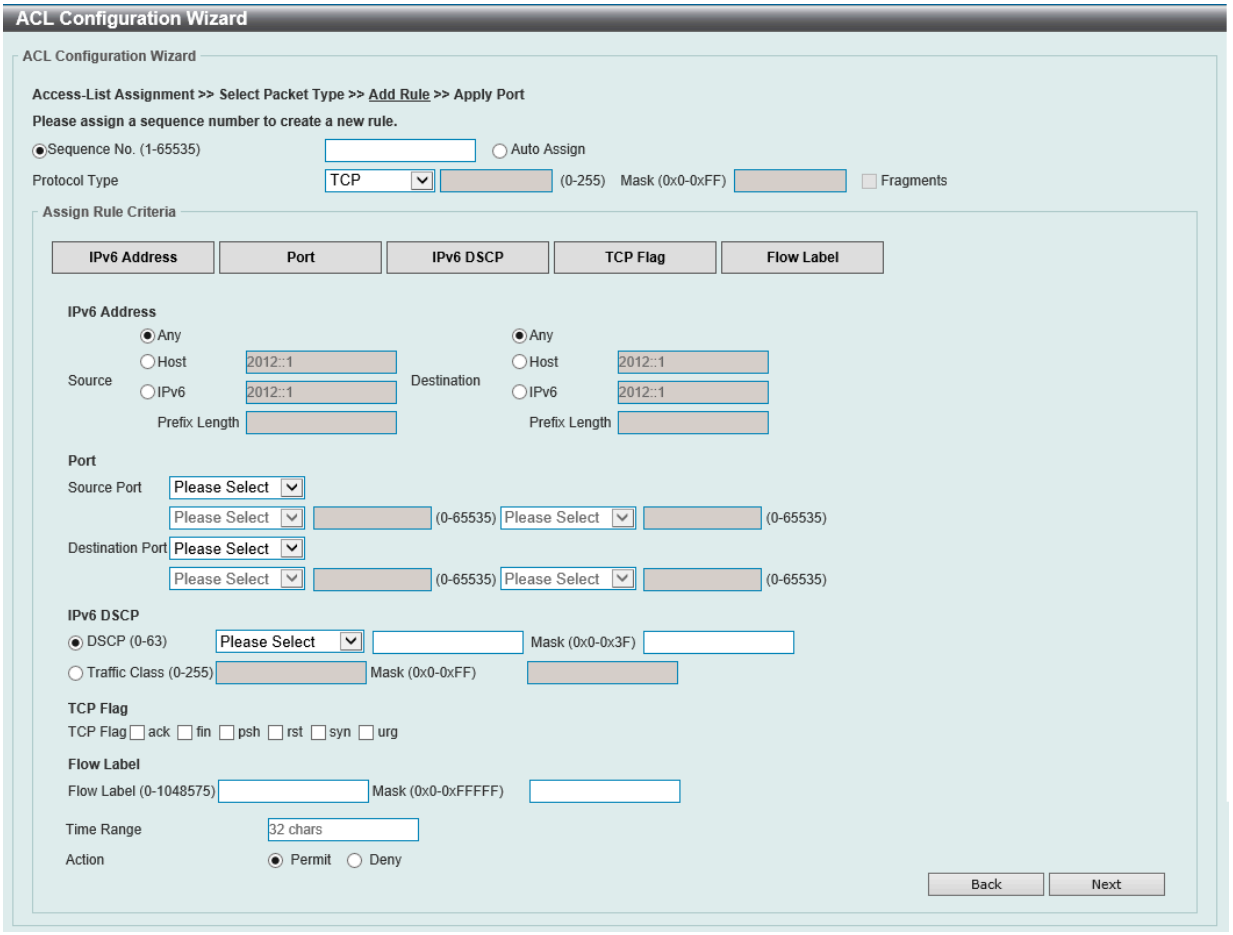


図 11-22　ACL Configuration Wizard 画面（Extended IPv6 ACL）

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。 「Auto Assign」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
Protocol Type	プロトコルの種類を以下から選択します。 • 「TCP」「UDP」「ICMP」「Protocol ID」「ESP(50)」「PCP(108)」「SCTP(132)」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「 Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

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

項目	説明
Source	送信元アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が指定可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が指定可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
DSCP	使用する DSCP 値を選択します。 • 「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」- DSCP 値を入力します。（0-63） - 「Mask」- DSCP マスクを入力します。（0x0-0x3F）
Traffic Class	トラフィッククラス値とトラフィッククラスのマスク値を入力します。 • 設定可能範囲：0-255 • 「Mask」：トラフィッククラスのマスクを入力します。（0x0-0xFF）
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Flow Label	フローラベルの値を入力します。 • 設定可能範囲：0-1048575 • 「Mask」：フローラベルマスクを入力します。（0x0-0xFFFFF）
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit」「Deny」

「Next」をクリックします。

ポート設定（ACL 設定ウィザード）

「ACL Configuration Wizard」にて適用するポートの設定を行います。

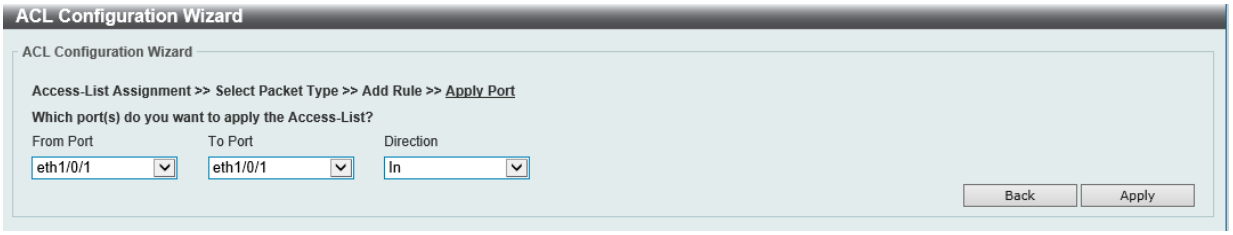


図 11-23　ACL Configuration Wizard 画面（Apply Port）

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

ACL Access List（ACL アクセスリスト）

ACL アクセスリストの設定、表示を行います。
ACL > ACL Access List の順にメニューをクリックし、以下の画面を表示します。

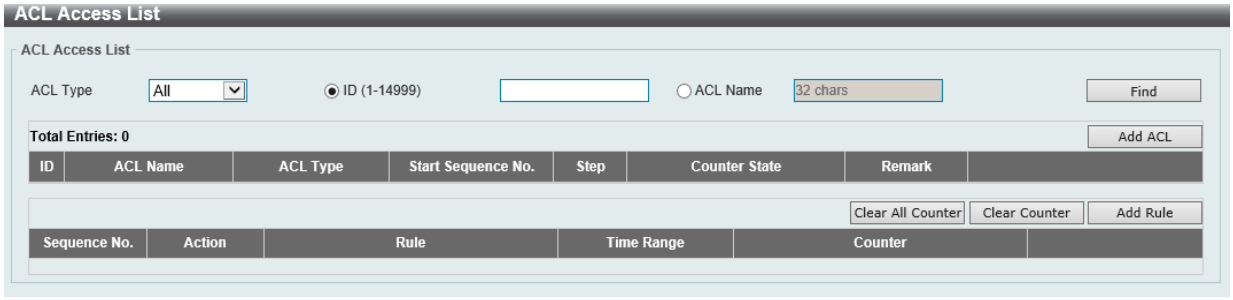


図 11-24　ACL Access List 画面

画面に表示される項目：

項目	説明
ACL Type	ACL プロファイルの種類を選択します。 • 選択肢：「All」「IP ACL」「IPv6 ACL」「MAC ACL」
ID	ACL ID を入力します。 • 設定可能範囲：1-14999
ACL Name	ACL 名を入力します。（32 文字以内）

「Find」をクリックし、入力した情報を基にエントリを検索します。
「Add ACL」をクリックし、新しい ACL プロファイルを作成します。
「Edit」をクリックして、指定エントリの編集を行います。
「Delete」をクリックすると指定のエントリを削除します。

ACL ルールの作成・カウンタの削除
ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」をクリックします。
「Clear All Counter」をクリックし、表示されたすべてのカウンタ情報を消去します。
「Clear Counter」をクリックし、表示された指定ルールのカウンタ情報を消去します。

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

ACL の編集

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

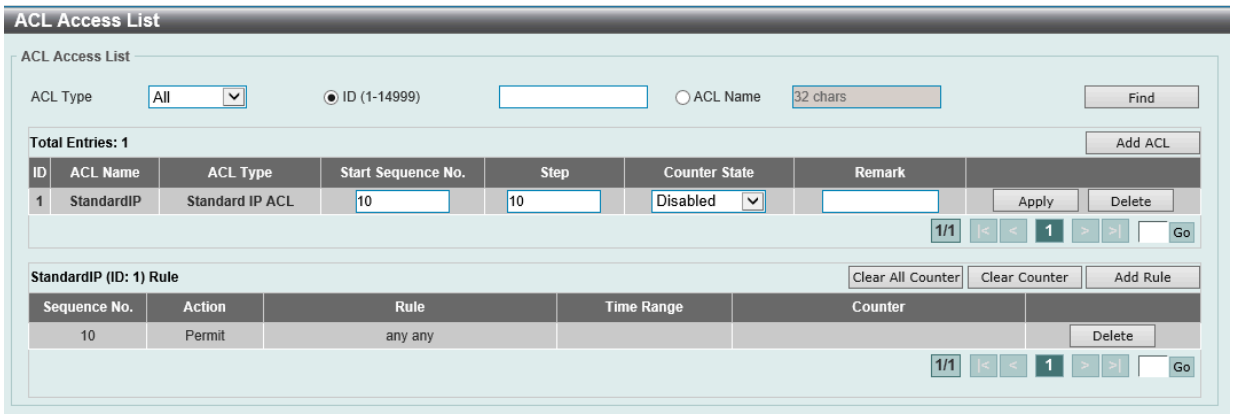


図 11-25　Standard IP ACL（Edit ACL）画面

画面に表示される項目：

項目	説明
Start Sequence No.	シーケンスの開始番号を入力します。
Step	シーケンス番号のステップ（インクリメント）数を入力します。 たとえば、シーケンスの開始番号が 20、ステップ値が 5 の場合、後続のシーケンス番号は 25、30、35、40 となります。 • 設定可能範囲：1-32 • 初期値：10
Counter State	カウンタ状態オプションを有効 / 無効に設定します。
Remark	ACL のオプション注釈を入力します。

「Apply」をクリックし、設定を適用します。

ACL プロファイルの作成

「Add ACL」をクリックすると、以下の画面が表示されます。

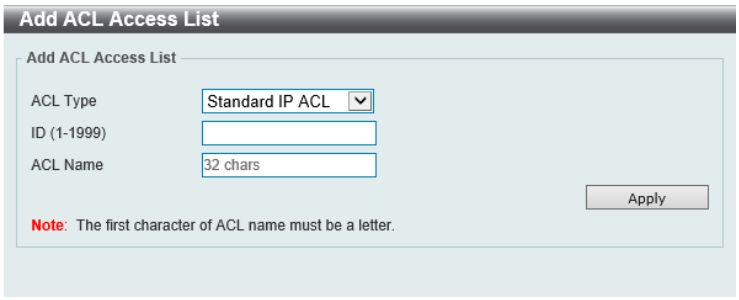


図 11-26　Standard IP ACL（Add ACL Access List）画面

画面に表示される項目：

項目	説明
ACL Type	ACL プロファイルの種類を選択します。 • 選択肢： 「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」
ID	ACL ID を入力します。 • Standard IP ACL の場合：1 - 1999 • Extended IP ACL の場合：2000 - 3999 • Standard IPv6 ACL の場合：11000 - 12999 • Extended IPv6 ACL の場合：13000 - 14999 • Extended MAC ACL の場合：6000 - 7999
ACL Name	ACL 名を入力します。（32 文字以内）

「Apply」をクリックして、設定内容を適用します。

Standard IP ACL（通常 IP ACL）の設定

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

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

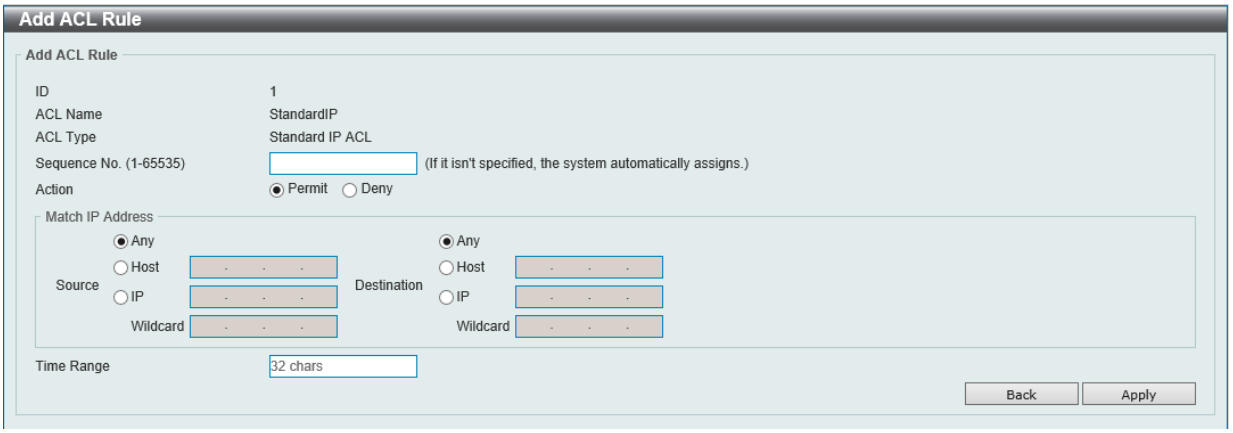


図 11-27　Standard IP ACL（Add Rule）画面

画面に表示される項目：

項目	説明
Sequence No.	ACL ルールのシーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit」「Deny」
Source	送信元のアドレスを指定します • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。

項目	説明
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」をクリックして、設定を適用します。

Extended IP ACL（拡張 IP ACL）の設定

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

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

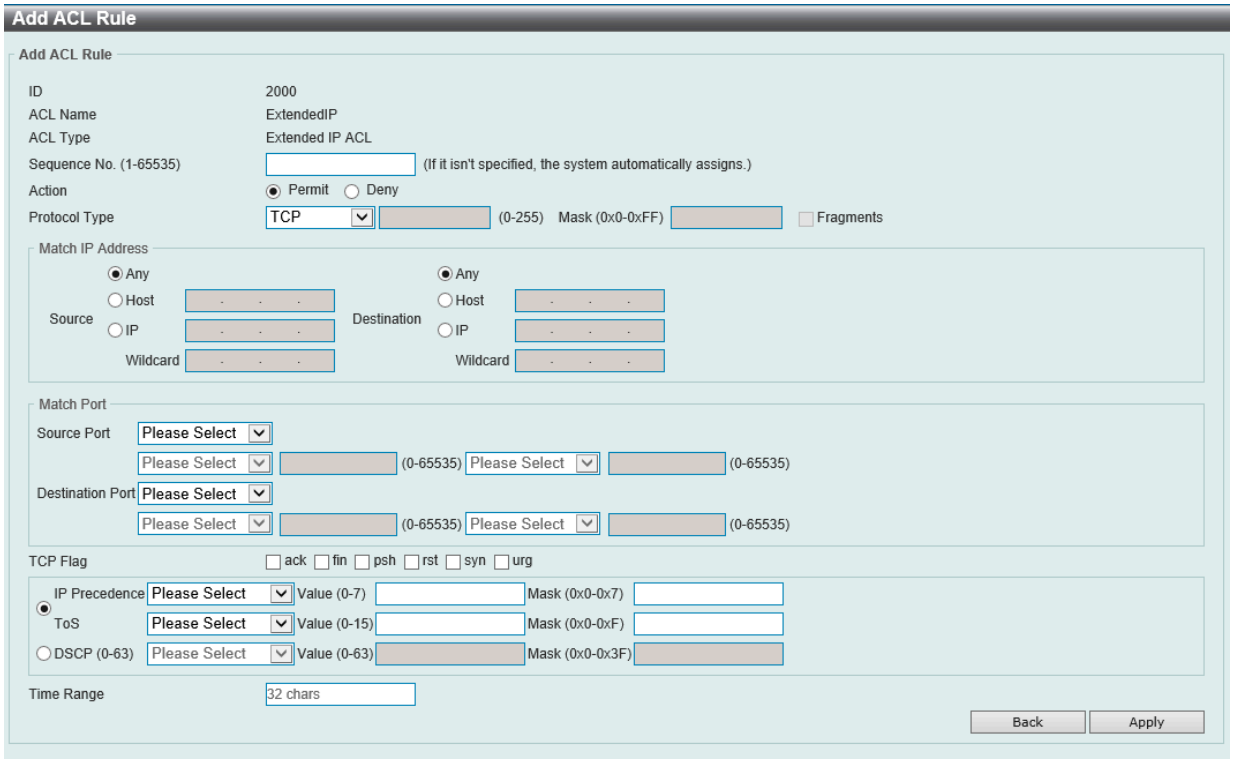


図 11-28　Extended IP ACL（Add Rule）画面

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit」「Deny」
Protocol Type	プロトコルの種類を以下から選択します。 • 「TCP」「UDP」「ICMP」「EIGRP (88)」「ESP (50)」「GRE (47)」「IGMP (2)」「OSPF (89)」「PIM (103)」「VRRP (112)」「IP-in-IP (94)」「PCP (108) 」「Protocol ID」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「 Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

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

画面に表示される項目：

項目	説明
Source	送信元のアドレスを指定します • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「Wildcard」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
IP Precedence	IP 優先値を指定します。 • 選択肢：「0（routine）」「1（priority）」「2（immediate）」「3（flash）」「4（flash-override）」「5（critical）」「6（internet）」「7（network）」 - 「Value」- IP 優先値を入力します。（0-7） - 「Mask」- IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」（ToS）の値を以下から指定します。 • 選択肢：「normal (0)」「min-monetary-cost (1)」「max-reliability (2)」「max-throughput (4)」「min-delay (8)」 - 「Value」- ToS 値を入力します。（0-15） - 「Mask」- ToS マスクを入力します。（0x0-0xF）
DSCP	使用する DSCP 値を選択します。 • 「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」- DSCP 値を入力します。（0-63） - 「Mask」- DSCP マスクを入力します。（0x0-0x3F）
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」をクリックして、設定を適用します。

Standard IPv6 ACL（標準 IPv6 ACL）の設定

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

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

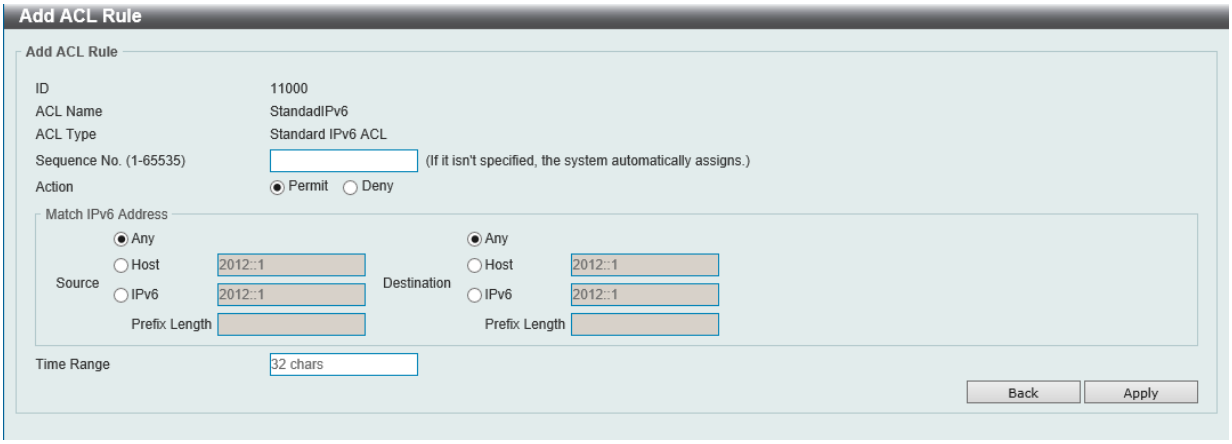


図 11-29　Standard IPv6 ACL（Add Rule）画面

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。 値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit」「Deny」
Source	送信元アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が指定可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「Prefix Length」が指定可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」をクリックして、設定内容を適用します。

Extended IPv6 ACL（拡張 IPv6 ACL）の設定

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

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

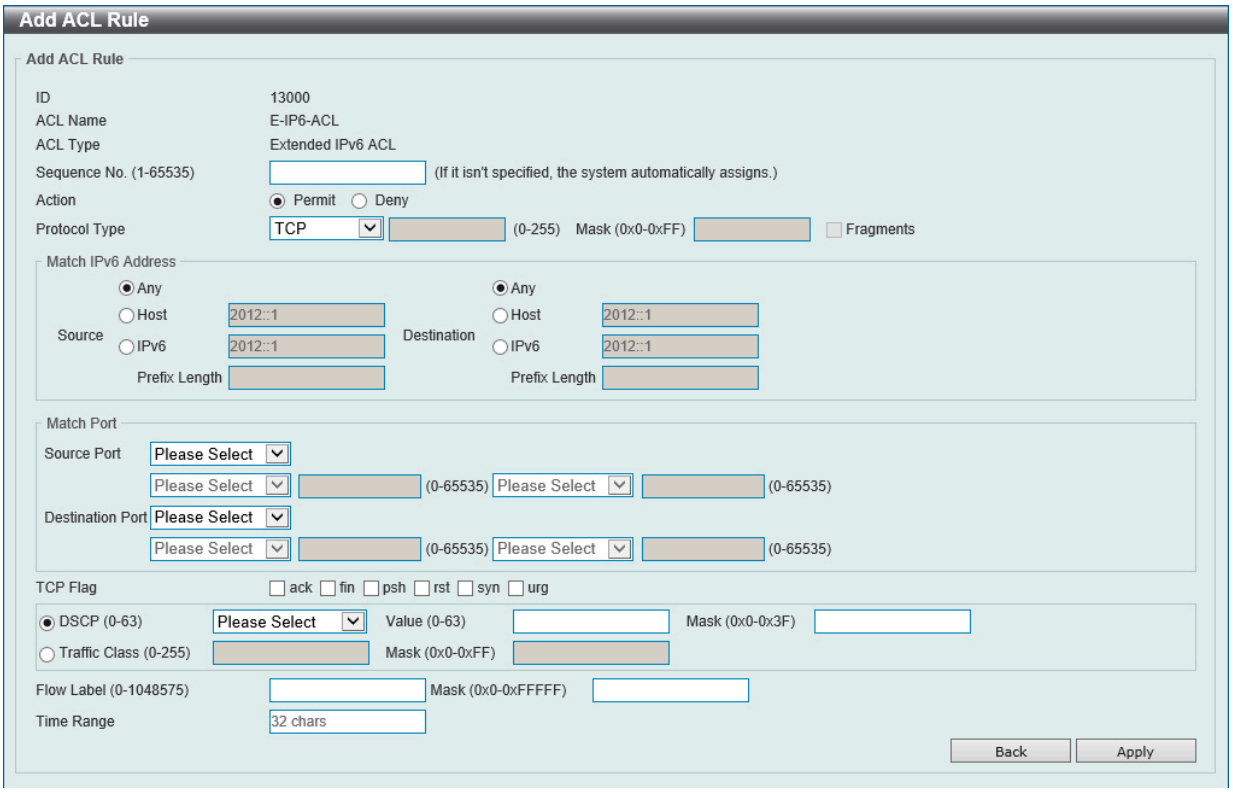


図 11-30　Extended IPv6 ACL（Add Rule）画面

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit」「Deny」
Protocol Type	プロトコルの種類を以下から選択します。 •「TCP」「UDP」「ICMP」「Protocol ID」「ESP (50)」「PCP (108) 」「SCTP (132)」「None」 - 「Value」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「Mask」-「 Protocol ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「Fragments」- パケットフラグメントフィルタを含める場合に指定します。

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

画面に表示される項目：

項目	説明
Source	送信元アドレスを指定します。 •「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 •「Host」- 送信元ホストの IPv6 アドレスを入力します。 •「IPv6」-「Prefix Length」が指定可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
Destination	宛先アドレスを指定します。 •「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 •「Host」- 宛先ホストの IPv6 アドレスを入力します。 •「IPv6」-「Prefix Length」が指定可能になります。宛先 IPv6 アドレスとプレフィックス長を入力します。

項目	説明
Source Port	【TCP/UDP を選択時に表示】送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
Destination Port	【TCP/UDP を選択時に表示】宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「Range」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「Mask」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
TCP Flag	【TCP を選択時に表示】 TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」
Specify ICMP Message Type	【ICMP を選択時に表示】 使用する ICMP メッセージの種類を指定します。
ICMP Message Type	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
Message Code	【ICMP を選択時に表示】 ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
DSCP	使用する DSCP 値を選択します。 • 「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5 (40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「Value」- DSCP 値を入力します。（0-63） - 「Mask」- DSCP マスクを入力します。（0x0-0x3F）
Traffic Class	トラフィッククラス値とトラフィッククラスのマスク値を入力します。 • 設定可能範囲：0-255 • 「Mask」：トラフィッククラスのマスクを入力します。（0x0-0xFF）
Flow Label	フローラベルの値を入力します。 • 設定可能範囲：0-1048575 • 「Mask」：フローラベルマスクを入力します。（0x0-0xFFFFF）
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」をクリックして、設定を適用します。

Extended MAC ACL（拡張 MAC ACL）の設定

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

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

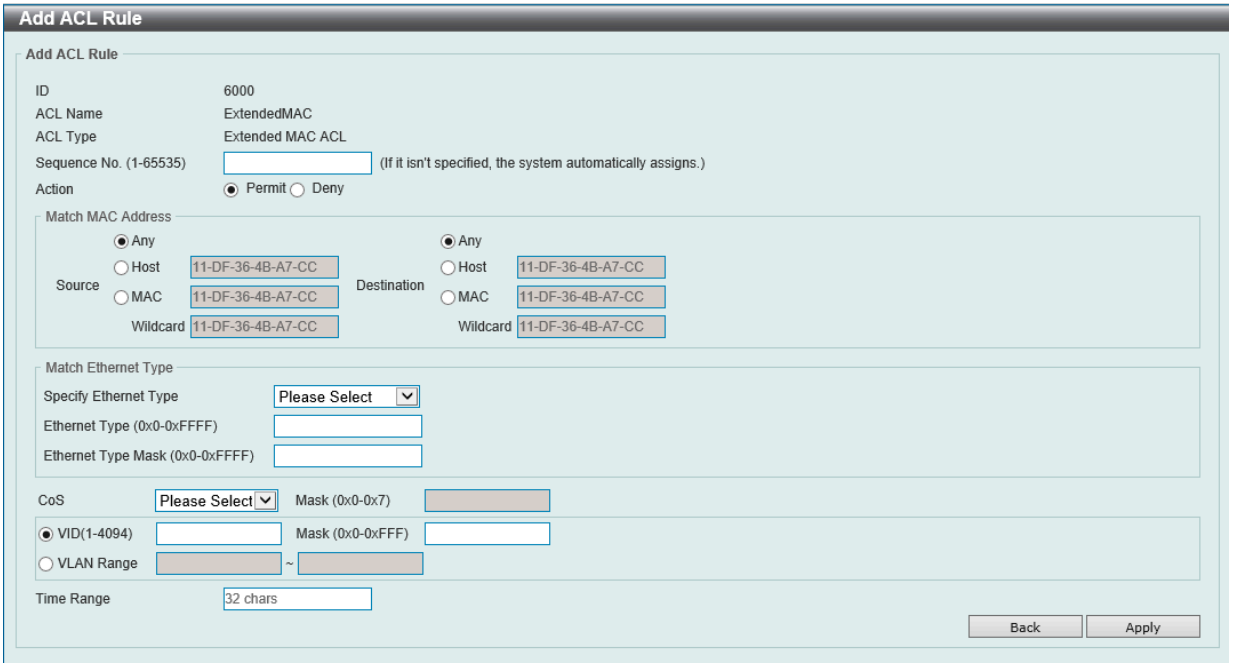


図 11-31　Extended MAC ACL（Add Rule）画面

画面に表示される項目：

項目	説明
Sequence No.	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
Action	本ルールで実行するアクションを選択します。 • 選択肢：「Permit」「Deny」
Source	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「Host」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力することができます。
Destination	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「Host」- 宛先ホストの MAC アドレスを入力します。 • 「MAC」-「Wildcard」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力することができます。
Specify Ethernet Type	イーサネットタイプを選択します。 • 選択肢:「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
Ethernet Type	イーサネットタイプの 16 進数値を 0x0 から 0xFFFF の間で指定します。 「Specify Ethernet Type」で指定したイーサネットタイプに基づき、自動的に適切な値が入力されます。
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。「Specify Ethernet Type」で指定したイーサネットタイプに基づき、自動的に適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 • 「Mask」：CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに適用する VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「Mask」：VLAN ID マスクを入力します。（0x0-0xFFF）
VLAN Range	ACL ルールに紐づける VLAN 範囲（開始 VLAN/ 終了 VLAN）を入力します。 • 設定可能範囲：1-4094
Time Range	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「Apply」をクリックして、設定を適用します。

ACL Interface Access Group（ACL インタフェースアクセスグループ）

ACL インタフェースアクセスグループの設定、表示を行います。

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

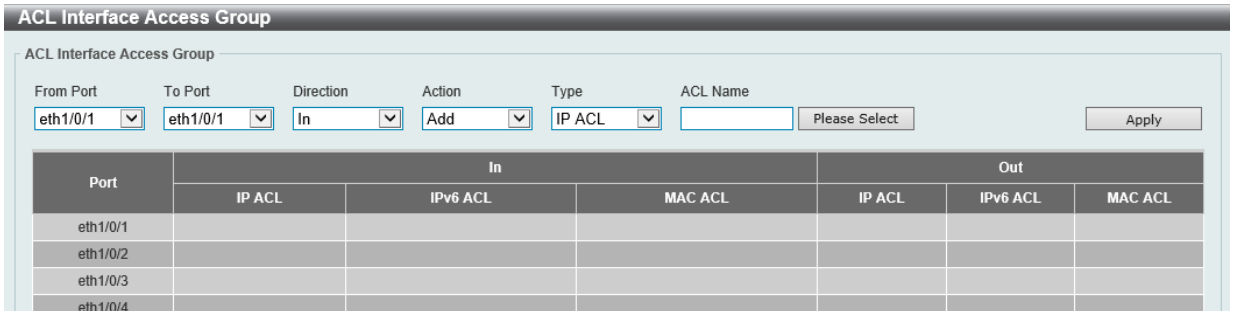


図 11-32　ACL Interface Access Group 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Direction	方向を指定します。 • 選択肢：「In」「Out」
Action	ACL インタフェースアクセスグループを追加 / 削除します。 • 選択肢：「Add」「Delete」
Type	ACL の種類を選択します。 • 選択肢：「IP ACL」「IPv6 ACL」「MAC ACL」
ACL Name	アクセスコントロールリスト名を入力します。 「Please Select」をクリックし、既存の ACL プロファイルを指定することも可能です。

「Apply」をクリックして、設定を適用します。

「Please Select」をクリックし、作成した ACL プロファイルを選択します。

「Please Select」をクリック すると次の画面が表示されます。

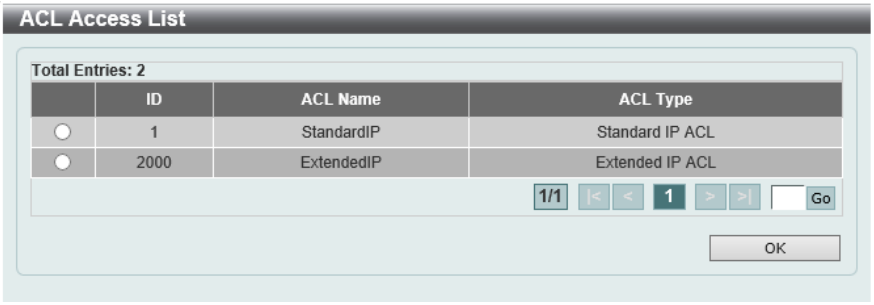


図 11-33　ACL Access List 面

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

第 12 章　Security（セキュリティ機能の設定）

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

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

サブメニュー	説明
Port Security（ポートセキュリティ）	ポートセキュリティの設定を行います。
802.1X（802.1X 認証設定）	802.1X 認証設定を行います。
AAA（AAA 設定）	AAA の設定を行います。
RADIUS（RADIUS 設定）	RADIUS の設定を行います。
IMPB（IP-MAC-Port Binding / IP-MAC ポートバインディング）	IP-MAC ポートバインディングの設定を行います。
DHCP Server Screening（DHCP サーバスクリーニング設定）	DHCP サーバスクリーニングの設定を行います。
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。
Network Access Authentication（ネットワークアクセス認証）	ネットワークアクセス認証設定を行います。
Safeguard Engine（セーフガードエンジン）	セーフガードエンジン設定を行います。
Trusted Host（トラストホスト）	トラストホスト設定を行います。
Traffic Segmentation Settings（トラフィックセグメンテーション設定）	トラフィックセグメンテーション設定を行います。
Storm Control Settings（ストームコントロール設定）	ストームコントロールの設定を行います。
DoS Attack Prevention Settings（DoS 攻撃防止設定）	DoS 攻撃防止設定を行います。
SSH（Secure Shell の設定）	SSH（Secure Shell）の設定を行います。
SSL（Secure Socket Layer）	SSL（Secure Socket Layer）の設定を行います。
Network Protocol Port Protection Settings（ネットワークプロトコルポート保護設定）	ネットワークプロトコルポート保護設定を行います。

Port Security（ポートセキュリティ）

ポートセキュリティの設定を行います。
ポートセキュリティ機能では、送信元 MAC アドレスが未認証であるコンピュータについて、指定ポートからネットワークへアクセスすることを防ぐことができます。

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

ポートセキュリティのグルーバル設定を行います。

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

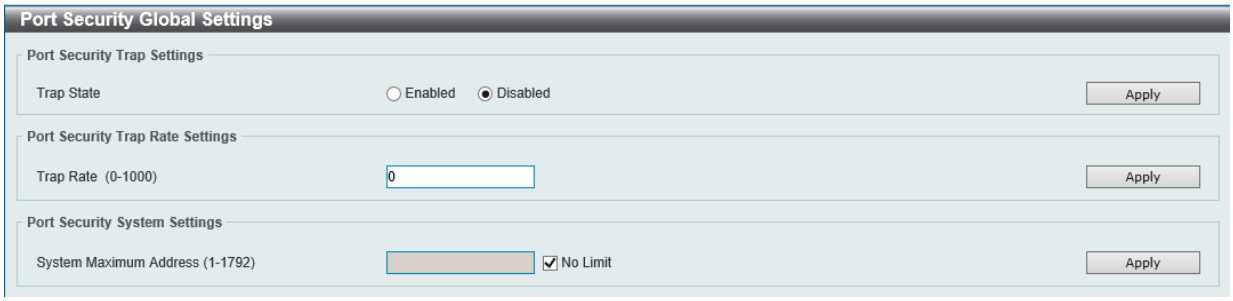


図 12-1　Port Security Global Settings 画面

画面に表示される項目：

項目	説明
Port Security Trap Settings	
Trap State	ポートセキュリティのトラップを有効 / 無効に設定します。
Port Security Trap Rate Settings	
Trap Rate	1 秒あたりのトラップ数を指定します。 • 設定可能範囲：0-1000 • 初期値：0
Port Security System Settings	
System Maximum Address	許可される最大 MAC アドレス数を入力します。初期値では制限なしになります。 「No Limit」オプションにチェックを入れると、セキュアな MAC アドレスの最大数が適用されます。 • 設定可能範囲：1-1792

「Apply」をクリックして、設定内容を適用します。

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

ポートセキュリティのポート設定と設定内容の表示を行います。

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

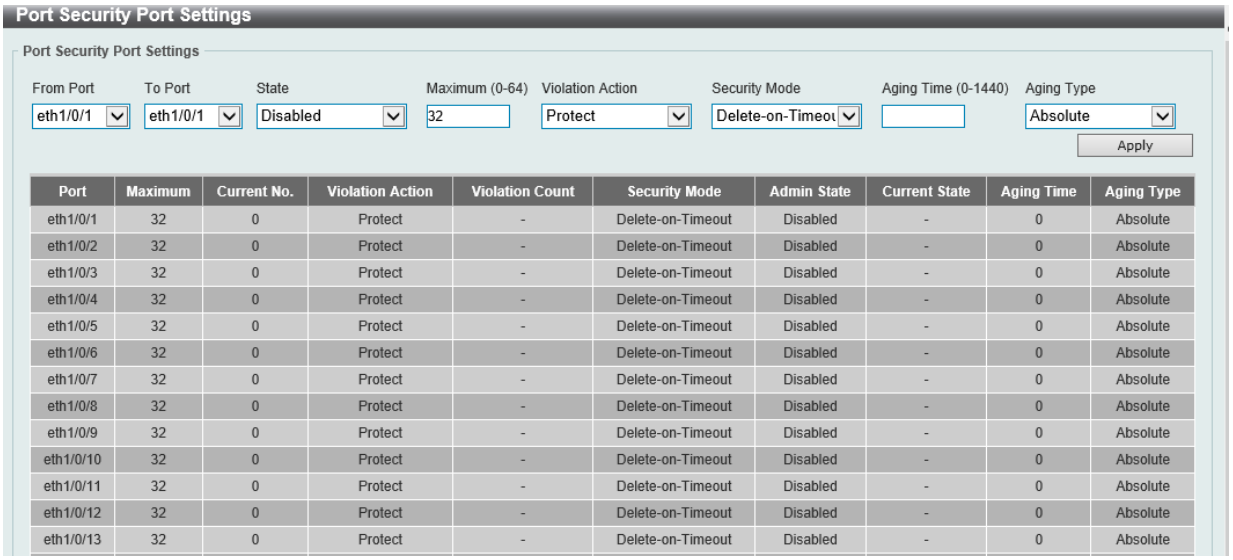


図 12-2　Port Security Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
State	指定ポートにおけるポートセキュリティ機能を有効 / 無効に設定します。
Maximum	指定ポートで許可されるセキュアな MAC アドレスの最大数を指定します。 • 設定可能範囲：0 - 64 • 初期値：32
Violation Action	違反に対して実行するアクションを指定します。 •「Protect」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反としてはカウントされません。 •「Restrict」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントしてシステムログに記録します。 •「Shutdown」- セキュリティ違反がある場合にポートをシャットダウンし、システムログに記録します。
Security Mode	セキュリティモードを選択します。 •「Permanent」- すべての学習した MAC アドレスは手動でエントリを削除しない限り削除されません。 •「Delete-on-Timeout」- すべての学習した MAC アドレスはタイムアウトにより自動的に削除されるか、手動により削除されます。
Aging Time	指定ポートで自動学習された安全なアドレスに使用するエージングタイムを入力します。 • 設定可能範囲：0 - 1440（分）
Aging Type	エージングの種類を指定します。 •「Absolute」- ポート上のすべてのアドレスは、指定された時間を過ぎるとアドレスリストから削除されます。（初期値） •「Inactivity」- ポート上のアドレスは、指定の期間そのアドレスからのトラフィックがない場合にエージアウトします。

「Apply」をクリックして、設定内容を適用します。

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

ポートセキュリティアドレスエントリの設定、表示を行います。

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

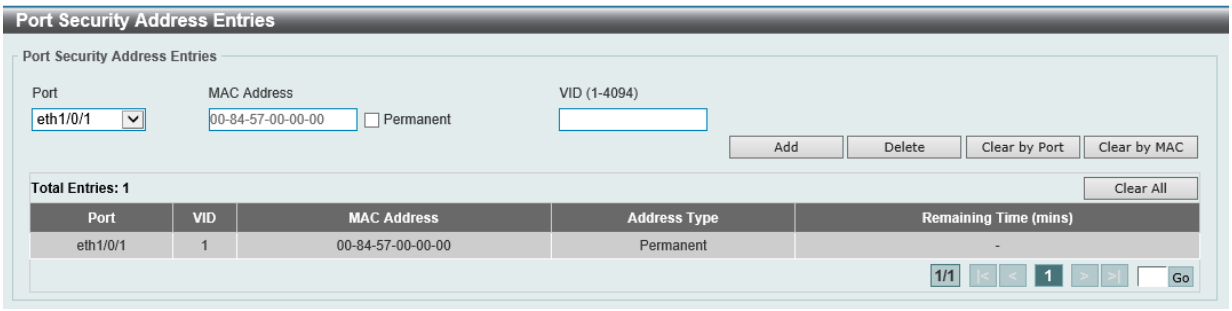


図 12-3　Port Security Address Entries 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
MAC Address	MAC アドレスを入力します。 「Permanent」オプションにチェックを入れると、すべての学習した MAC アドレスは手動でエントリを削除しない限り削除されません。
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094

「Add」をクリックして、入力した情報に基づく新しいエントリを追加します。
「Delete」をクリックして、入力した情報に基づく新しいエントリを削除します。

「Clear by Port」をクリックして、選択したポートに基づく情報を消去します。
「Clear by MAC」をクリックして、選択した MAC アドレスに基づく情報を消去します。
「Clear All」をクリックして、テーブル上のすべての情報を消去します。

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

802.1X（802.1X 認証設定）

802.1X（ポートベースおよびホストベースのアクセスコントロール）

IEEE 802.1X は、ユーザ認証を行うセキュリティの規格です。

クライアント / サーバベースのアクセスコントロールモデルを使用し、特定のローカルエリアネットワーク上の有線 / 無線デバイスへのアクセスを許可および認証するために使用します。この認証方法は、ネットワークへアクセスするユーザの認証に RADIUS サーバを使用し、EAPOL（Extensible Authentication Protocol over LAN）と呼ばれるパケットをクライアント / サーバ間でリレーして実現します。

以下の図は、基本的な EAPOL パケットの構成です。

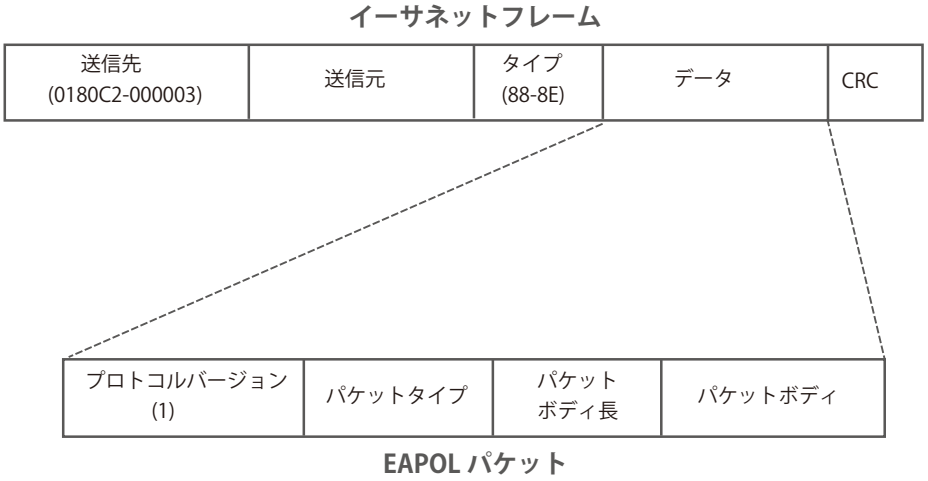


図 12-4　EAPOL パケット

IEEE 802.1X を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。
EAPOL パケットは、承認完了前でも指定ポート経由で送受信できる唯一のトラフィックです。

802.1X アクセスコントロールには認証サーバ、オーセンティケータ、クライアントの 3 つの役割があります。
それぞれがアクセスコントロールセキュリティの作成、状態の維持、動作のために重要です。

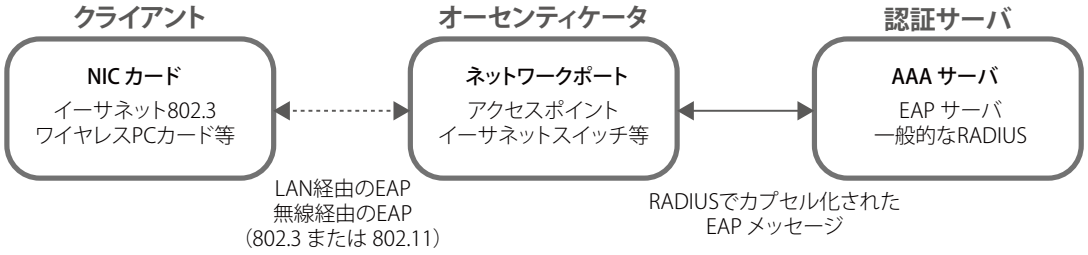


図 12-5　802.1X の 3 つの要素

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

認証サーバ

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

認証サーバ上で RADIUS サーバプログラムが実行され、認証サーバのデータがオーセンティケータ（スイッチ）に正しく登録されている必要があります。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを使用する前に、認証サーバ（RADIUS）によって認証される必要があります。

認証サーバの役割は、ネットワークにアクセスするクライアントの身元を証明することです。認証サーバ（RADIUS）とクライアントの間で EAPOL パケットによるセキュアな情報交換を行い、クライアントが「LAN やスイッチのサービスに対するアクセス許可があるか」をスイッチに通知します。

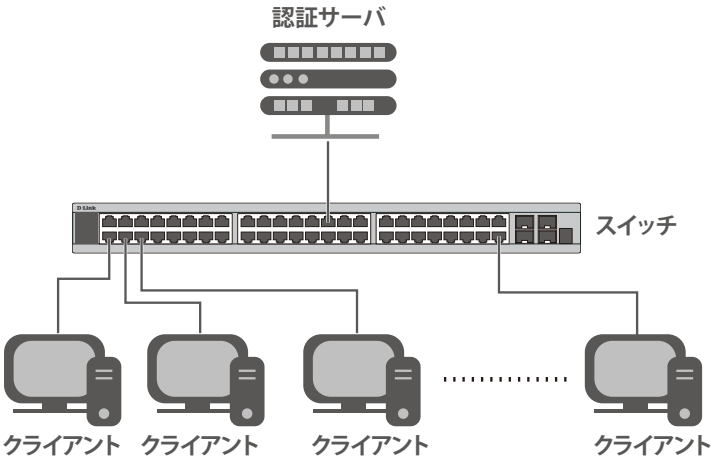


図 12-6　認証サーバ

オーセンティケータ

オーセンティケータ（スイッチ）は、認証サーバとクライアントの間を仲介します。

802.1X を使用する場合、オーセンティケータには 2 つの役割があります。

- 1 つ目の役割：
  クライアントに EAPOL パケットを通して認証情報を提出するよう要求することです。
  EAPOL パケットはクライアントにアクセスが許可される前にオーセンティケータを通過することのできる唯一の情報です。
- 2 つ目の役割：
  クライアントから収集した情報を認証サーバに確認してもらい、その結果をクライアントに伝達することです。

スイッチをオーセンティケータとして設定するには、以下の手順を実行します。

1. スイッチの 802.1X 機能を有効にします。（**Security > 802.1X > 802.1X Global Settings**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Port Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > RADIUS > RADIUS Server Settings**）

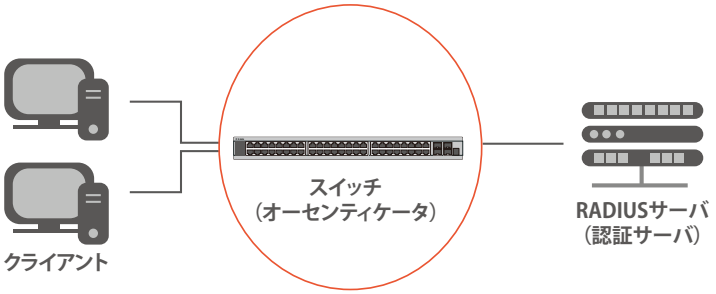


図 12-7　オーセンティケータ

クライアント

クライアントとは、LAN やスイッチが提供するサービスへアクセスしようとする端末です。

クライアントとなる端末では、802.1X プロトコルに準拠したソフトウェアが起動している必要があります。一部の Windows OS のように、OS 内に既にそのソフトウェアが組み込まれている場合がありますが、それ以外の OS をお使いの場合は、802.1X クライアントソフトウェアを別途用意する必要があります。

クライアントは EAPOL パケットを使用して LAN へのアクセスを要求し、スイッチからの要求に応答します。

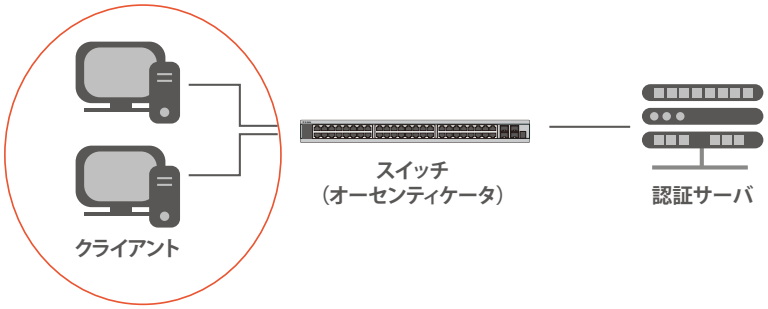


図 12-8　クライアント

認証プロセスについて

前述の「認証サーバ」「オーセンティケータ」「クライアント」により、802.1X プロトコルはネットワークへアクセスするユーザの認証を安定的かつ安全に行います。

認証完了前には EAPOL トラフィックのみが特定のポートの通過を許可されます。このポートは、有効なユーザ名とパスワード（802.1X の設定によっては MAC アドレスも）を持つクライアントがアクセス権を取得してポートのロックが解除されるまで、ロック状態を保ちます。ロックが解除されると、通常のトラフィックがポートを通過できるようになります。

本製品の 802.1X では、以下の 2 種類のアクセスコントロールが選択できます。

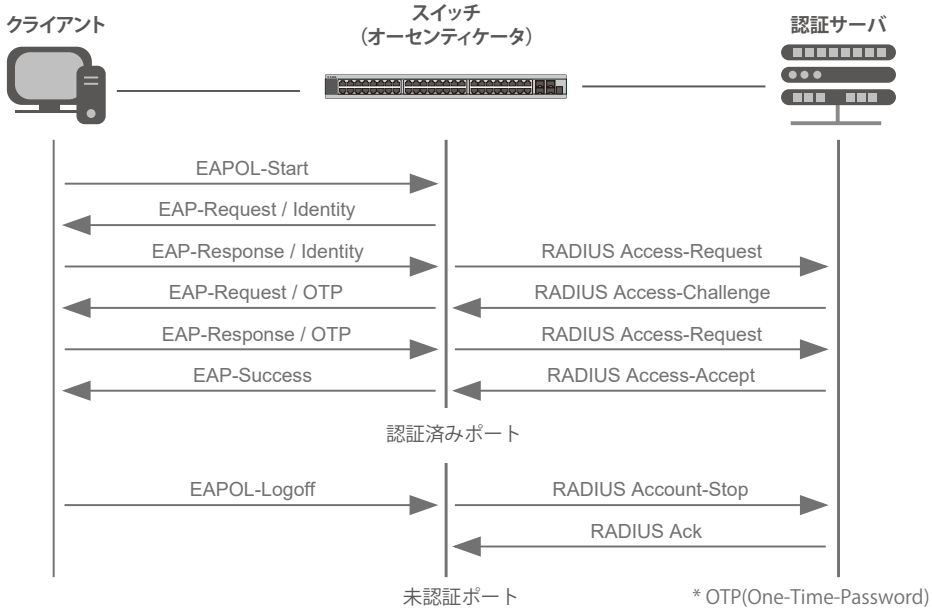


図 12-9　802.1X 認証プロセス

本製品の 802.1X 機能では、以下の 2 つのタイプのアクセスコントロールから選択することができます。

1. **ポートベースのアクセスコントロール**
   本方式では、リモート RADIUS サーバが、ポートごとに 1 人のユーザのみを認証することで、同じポート上の残りのユーザがネットワークにアクセスできるようにします。
2. **ホストベースのアクセスコントロール**
   本方式では、スイッチはポートで最大 448 件までの MAC アドレスを自動的に学習してリストに追加します。
   スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に MAC アドレスごと（ユーザごと）の認証を行います。

ポートベースのネットワークアクセスコントロール

802.1X は、元々は LAN 上で Point to Point プロトコルの特長を活用するために開発されました。

単一の LAN セグメントが 2 台より多くのデバイスを持たない場合、デバイスのどちらかがブリッジポートとなります。
ブリッジポートは、「リンクのリモートエンドにアクティブなデバイスが接続された」「アクティブなデバイスが非アクティブ状態になった」などのイベントを検知します。これらのイベントをポートの認証状態の制御に利用し、ポートの許可がされていない接続デバイスの認証プロセスを開始します。これをポートベースのアクセスコントロールと呼びます。

■ ポートベースネットワークアクセスコントロール

接続デバイスが認証に成功すると、ポートは「Authorized」（認証済み）の状態になります。ポートが未認証になるようなイベントが発生するまで、ポート上のすべてのトラフィックはアクセスコントロール制限の対象になりません。

そのため、ポートが複数のデバイスが所属する共有 LAN セグメントに接続される場合、接続デバイスの 1 つが認証に成功すると共有セグメント上のすべての LAN に対してアクセスを許可することになります。このような場合、ポートベースネットワークアクセスコントロールは脆弱であるといえます。

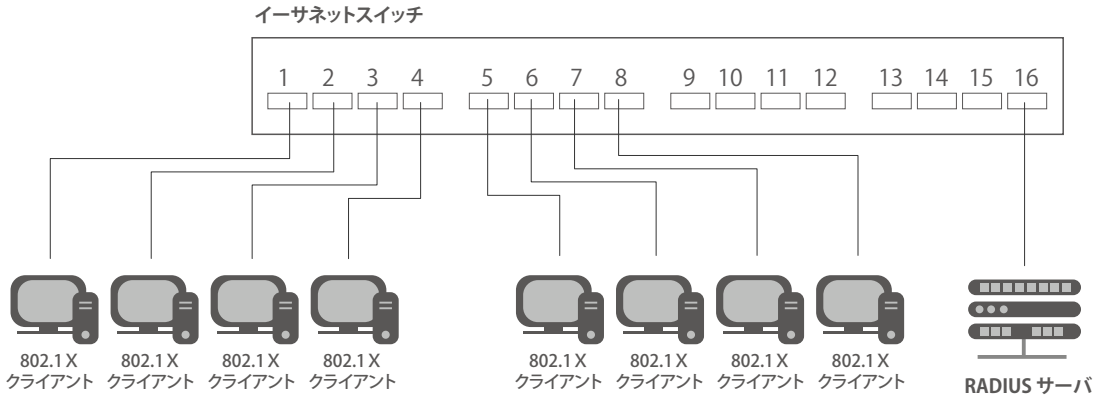


図 12-10　ポートベースアクセスコントロールのネットワーク構成例

■ ホストベースネットワークアクセスコントロール

共有 LAN セグメント内で 802.1X を活用するには、LAN へのアクセスを希望する各デバイスに論理ポートを定義する必要があります。

スイッチは、共有 LAN セグメントに接続する 1 つの物理ポートを異なる論理ポートの集まりであると認識し、それら論理ポートを EAPOL パケット交換と認証状態に基づいて別々に制御します。スイッチは接続する各デバイスの MAC アドレスを学習し、それらのデバイスがスイッチ経由で LAN と通信するための論理ポートを確立します。

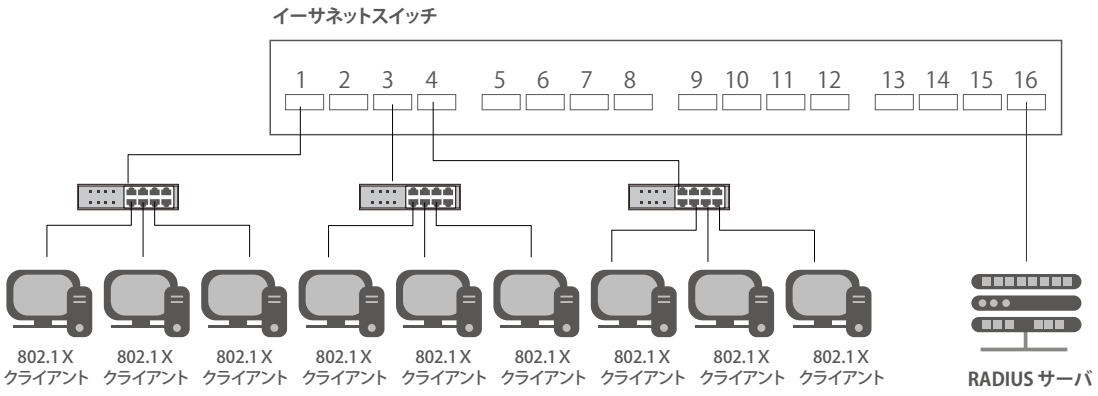


図 12-11　ホストベースアクセスコントロールのネットワーク構成例

802.1X Global Settings（802.1X グローバル設定）

本画面では 802.1X グローバル設定を行います。

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

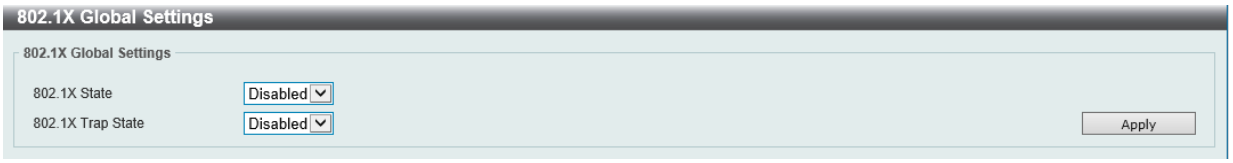


図 12-12　802.1X Global Settings 画面

画面に表示される項目：

項目	説明
802.1X State	802.1X 認証を有効 / 無効に設定します。
802.1X Trap State	802.1X トラップを有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

802.1X Port Settings（802.1X ポート設定）

802.1X 認証ポートを設定します。

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

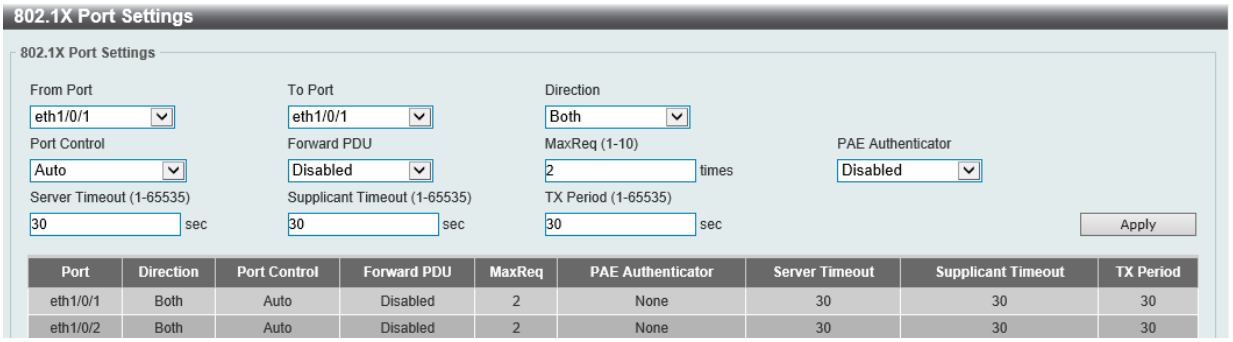


図 12-13　802.1X Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Direction	制御するトラフィックの方向を指定します。 • 「In」- 指定したポートへの入力トラフィックのみ制御対象となります。 • 「Both」- ポートが受信 / 送信する両方向のトラフィックについて処理します。
Port Control	ポートの認証状態を指定します。 • 「ForceAuthorized」（認証強制）- 両方向の通信でポートは制御されません。 • 「Auto」（自動）- 制御対象の方向のポートへのアクセスは認証が必要になります。 • 「ForceUnauthorized」（未認証強制）- 制御対象の方向のポートへのアクセスはブロックされます。
Forward PDU	PDU 転送機能を有効 / 無効に設定します。
MaxReq	バックエンドの認証ステートマシンがクライアントに対して Extensible Authentication Protocol（EAP）リクエストフレームを再送する最大回数を指定します。ここで指定した最大回数の後に、認証プロセスが再開されます。 • 設定可能範囲：1-10 • 初期値：2
PAE Authenticator	PAE Authenticator を有効 / 無効に指定します。 本設定により、特定ポートを IEEE 802.1X Port Access Entity（PAE）オーセンティケータとして指定します。
Server Timeout	サーバのタイムアウト時間を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
Supplicant Timeout	サプリカント（クライアント）のタイムアウト状態となる時間を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
TX Period	送信間隔を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）

「Apply」をクリックして、設定内容を適用します。

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

認証セッションの状態を表示します。

Security > 802.1X > Authentication Session Information の順にメニューをクリックして、以下の画面を表示します。

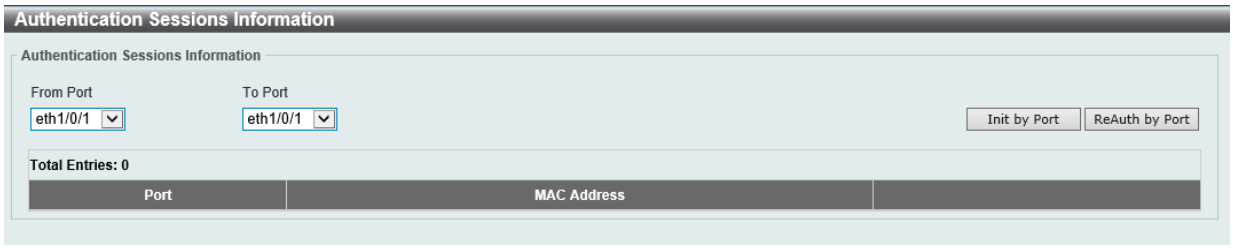


図 12-14　Authentication Session Information 画面

画面に表示される項目：

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

「Init by Port」をクリックして、指定ポートに基づくセッション情報の初期化を実行します。
「ReAuth by Port」をクリックして、指定ポートに基づくセッション情報の再認証（Re-Authenticate）を実行します。

「Init by MAC」をクリックして、指定 MAC アドレスに基づくセッション情報の初期化を実行します。
「ReAuth by MAC」をクリックして、指定 MAC アドレスに基づくセッション情報の再認証（Re-Authenticate）を実行します。

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

Authenticator Statistics（オーセンティケータ統計情報）

オーセンティケータの統計情報を表示します。

Security > 802.1X > Authenticator Statistics の順にメニューをクリックして、以下の画面を表示します。

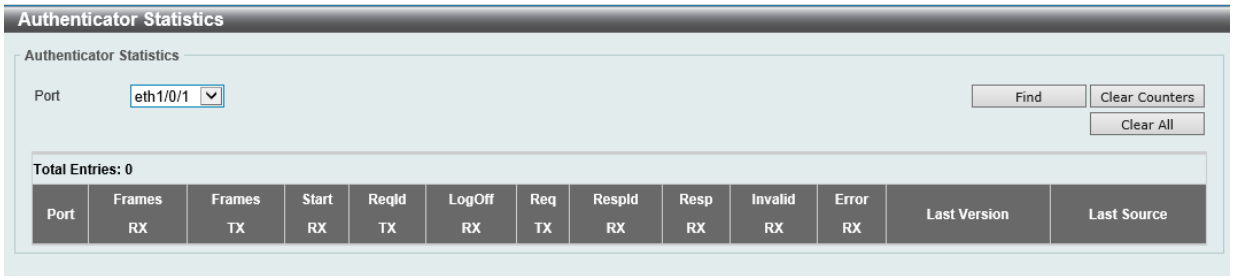


図 12-15　Authenticator Statistics 画面

画面に表示される項目：

項目	説明
Port	統計情報を表示 / クリアするポートを指定します。

「Find」をクリックして、指定した情報に基づくエントリを検出します。
「Clear Counters」をクリックして、選択に基づく情報を消去します。
「Clear All」をクリックして、テーブル上のすべての情報を消去します。

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

Authenticator Session Statistics（オーセンティケータセッション統計情報）

オーセンティケータセッションの統計情報を表示します。

Security > 802.1X > Authenticator Session Statistics の順にメニューをクリックして、以下の画面を表示します。

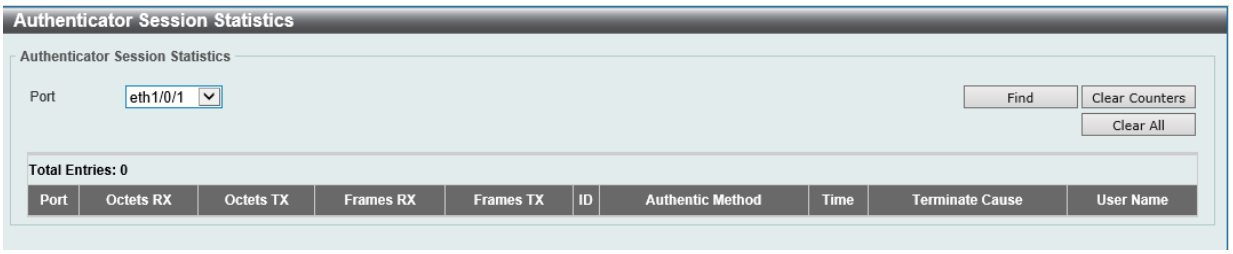


図 12-16　Authenticator Session Statistics 画面

画面に表示される項目：

項目	説明
Port	統計情報を表示 / クリアするポートを指定します。

「Find」をクリックして、指定した情報に基づくエントリを検出します。

「Clear Counters」をクリックして、選択に基づく情報を消去します。
「Clear All」をクリックして、テーブル上のすべての情報を消去します。

Authenticator Diagnostics（オーセンティケータ診断）

オーセンティケータ診断情報を表示します。

Security > 802.1X > Authenticator Diagnostics の順にメニューをクリックして、以下の画面を表示します。

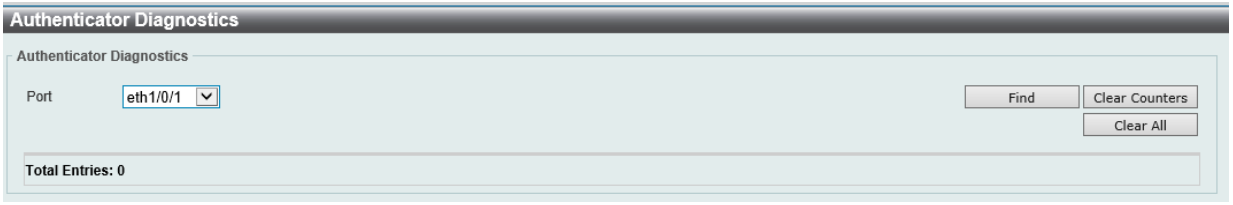


図 12-17　Authenticator Diagnostics 画面

画面に表示される項目：

項目	説明
Port	診断情報を表示 / クリアするポートを指定します。

「Find」をクリックして、指定した情報に基づくエントリを検出します。
「Clear Counters」をクリックして、選択に基づく情報を消去します。
「Clear All」をクリックして、テーブル上のすべての情報を消去します。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

AAA（AAA 設定）

AAA（Authentication、Authorization、Accounting）の設定を行います。

AAA Global Settings（AAA グローバル設定）

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

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

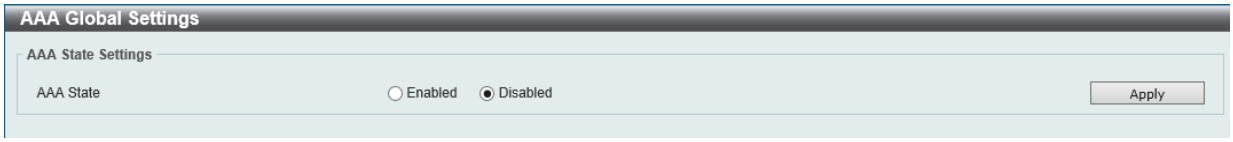


図 12-18　AAA Global Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。

Authentication Settings（認証設定）

AAA ネットワーク認証設定を行います。

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

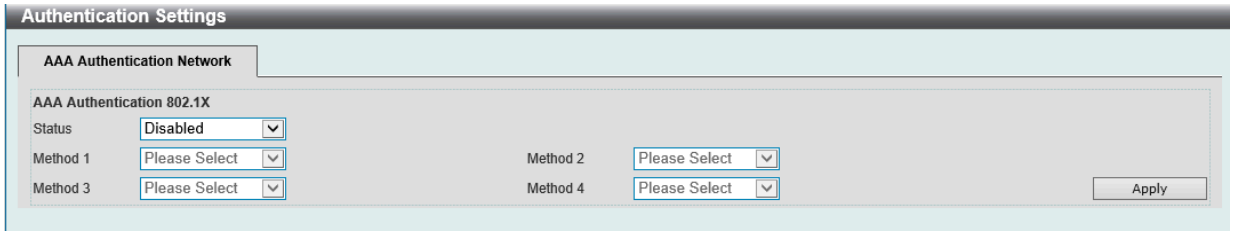


図 12-19　Authentication Settings 画面

画面に表示される項目：

項目	説明
Status	各項目の認証設定の有効 / 無効を設定します。
Method 1 - 4	本設定項目のメソッドリストを選択します。 • 「none」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- 認証にローカルデータベースを使用します。 • 「group」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバ設定で定義されたサーバを使用します。

「Apply」をクリックして、設定内容を適用します。

注意　802.1X の機能において、認証にローカルデータベースを指定した場合、EAP-MD5 のみをサポートします。

RADIUS（RADIUS 設定）

RADIUS サーバの設定を行います。

RADIUS Global Settings（RADIUS グローバル設定）

RADIUS サーバのグローバルステータスを設定します。

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

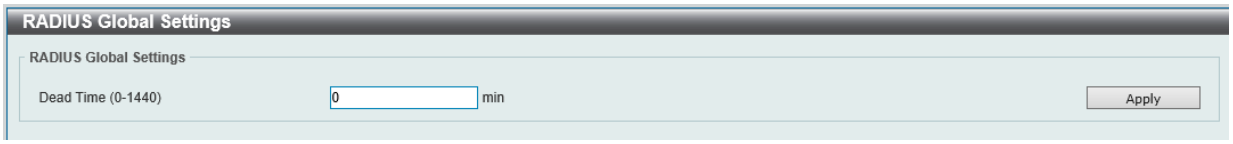


図 12-20　RADIUS Global Settings 画面

画面に表示される項目：

項目	説明
DeadTime	デッドタイムの設定を行います。 0 に設定した場合、応答しないサーバは「Dead」として認識されることはありません。この設定により、応答しないサーバホストのエントリはスキップされ、認証プロセス時間が改善されます。 システムが認証サーバへ認証を行う際、一度に一台のサーバへの認証が試みられます。接続を試みたサーバが応答しない場合、システムは次のサーバに対して接続を試行します。応答しないサーバが検出されると、当該サーバはダウン状態として認識され、「デッドタイム」タイマが開始されます。それ以降のリクエスト認証はデッドタイム時間が経過するまでスキップされます。 • 設定可能範囲：0 - 1440（分） • 初期値：0（分）

「Apply」をクリックして、設定内容を適用します。

RADIUS Server Settings（RADIUS サーバの設定）

RADIUS サーバ設定を行います。

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

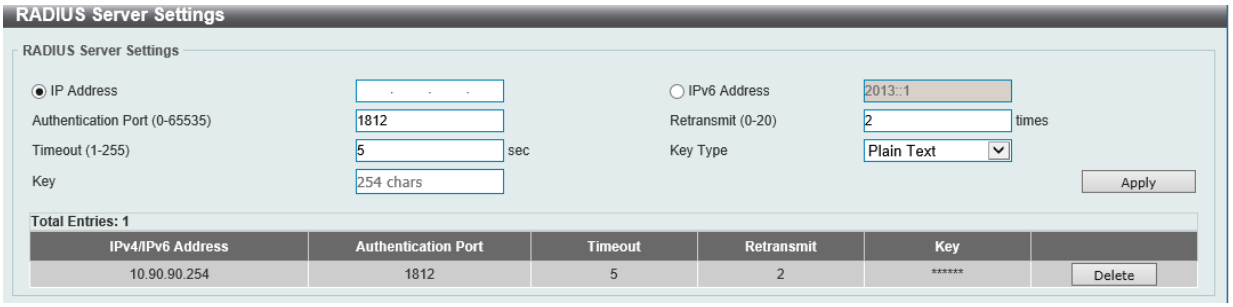


図 12-21　RADIUS Server Settings 画面

画面に表示される項目：

項目	説明
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。
Authentication Port	認証ポート番号を入力します。認証を使用しない場合は「0」を指定します。 • 設定可能範囲：0-65535 • 初期値：1812
Retransmit	再送回数を設定します。このオプションを無効にする場合、「0」を指定します。 • 設定可能範囲：0-20（回） • 初期値：2（回）
Timeout	タイムアウト時間を設定します。 • 設定可能範囲：1-255（秒） • 初期値：5（秒）
Key Type	使用する鍵の種類を選択します。 • 選択肢：「Plain Text」（平文）
Key	RADIUS サーバとの通信で使用する鍵を指定します。（254 文字以内）

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

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

RADIUS グループサーバの表示、設定を行います。

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

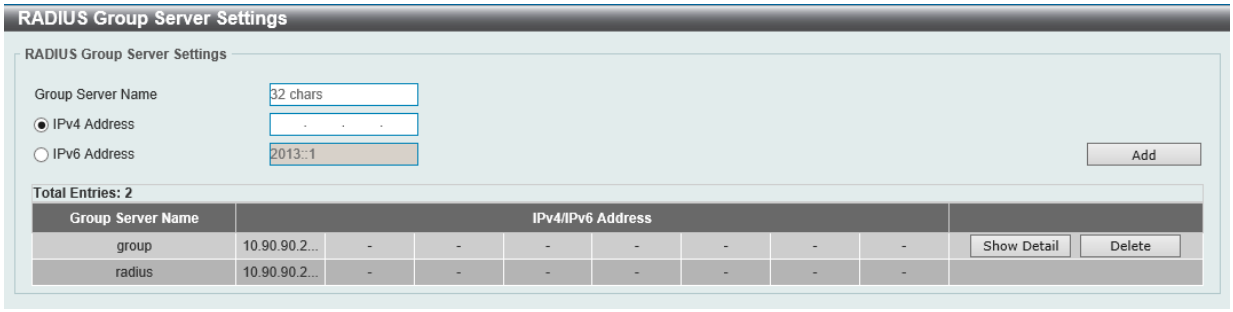


図 12-22　RADIUS Group Server Settings 画面

画面に表示される項目：

項目	説明
Group Server Name	RADIUS グループサーバ名を入力します。（32 文字以内）
IPv4 Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。

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

エントリの詳細を表示

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

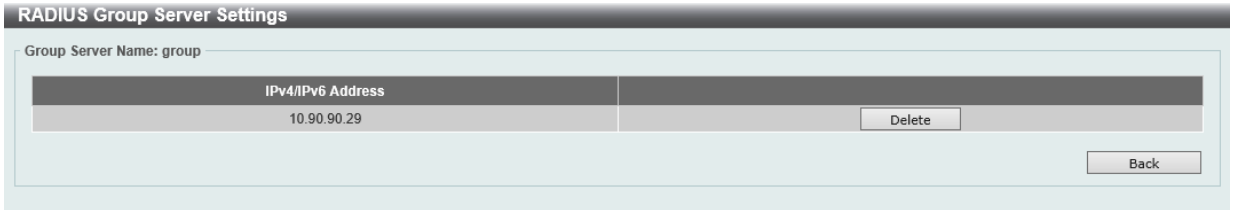


図 12-23　RADIUS Group Server Settings - Detail 画面

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

RADIUS Statistic（RADIUS 統計情報）

RADIUS 統計情報を表示します。

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

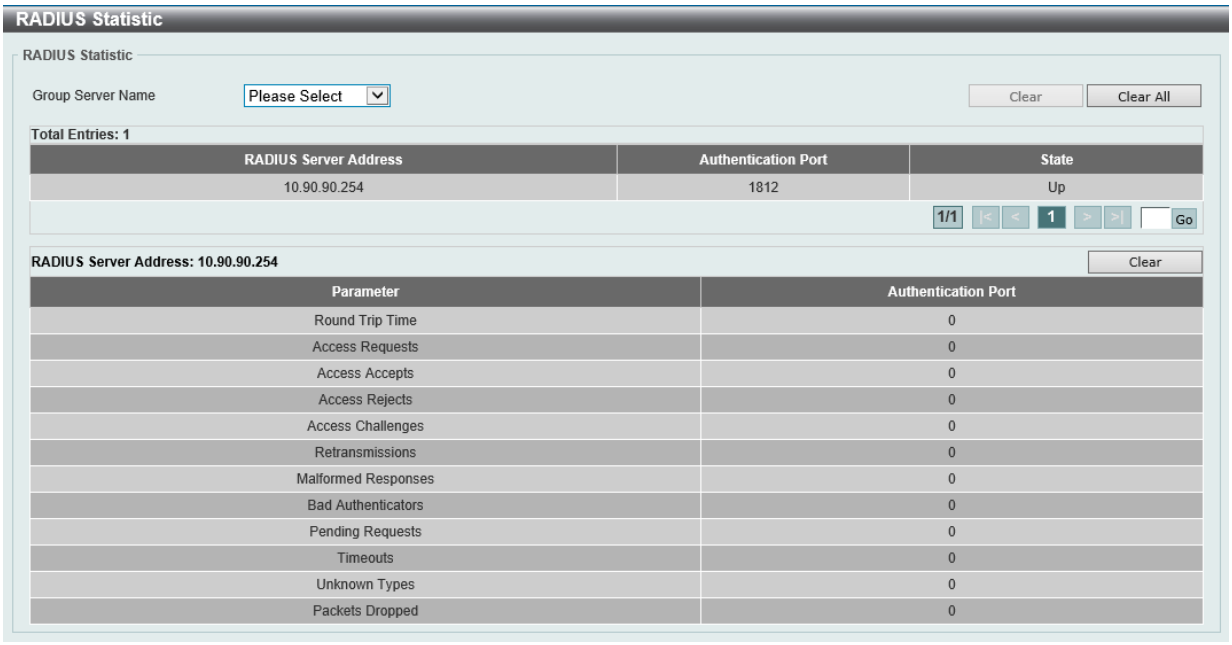


図 12-24　RADIUS Statistic 画面

画面に表示される項目：

項目	説明
Group Server Name	表示する RADIUS グループサーバ名を選択します。

「Clear」をクリックして、選択に基づいて表示した情報を消去します。
「Clear All」をクリックして、テーブル上のすべての情報を消去します。

IMPB（IP-MAC-Port Binding / IP-MAC ポートバインディング）

IMPB（IP-MAC-Port Binding) の設定を行います。

IP ネットワークレイヤ（IP レベル）では 4 バイトのアドレスを使用し、イーサネットリンクレイヤ（データリンクレベル）では 6 バイトの MAC アドレスを使用します。これらの 2 つのアドレスタイプを結びつけることにより、レイヤ間のデータ転送が可能になります。

IP-MAC バインディングの主な目的は、スイッチにアクセスするユーザを制限することです。IP アドレスと MAC アドレスのペアについて、事前に設定したデータベースと比較を行い、認証クライアントのみがスイッチのポートアクセスできるようにします。もしくは DHCP スヌーピングが有効な場合において、スイッチがスヌーピング DHCP パケットから自動的に IP/MAC ペアを学習し、IMPB ホワイトリストに保存することで、認証クライアントのポートアクセスが可能になります。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。本機能はポートベースであるため、ポートごとに本機能を有効 / 無効にすることができます。

IPv4

DHCPv4 Snooping（DHCPv4 スヌーピング）

■ DHCP Snooping Global Settings（DHCP スヌーピンググローバル設定）

DHCP スヌーピングのグローバル設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings の順にクリックし、以下の画面を表示します。

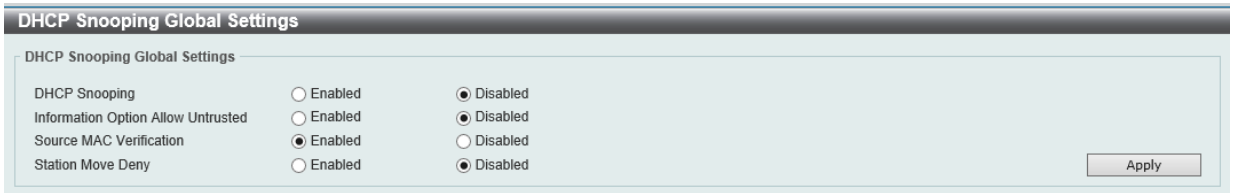


図 12-25　DHCP Snooping Global Settings 画面

画面に表示される項目：

項目	説明
DHCP Snooping	DHCP スヌーピングのグローバルステータスを有効 / 無効に設定します。
Information Option Allow Untrusted	信頼されていないインタフェースにおける、リレーオプション 82 付き DHCP パケット許可のグローバルステータスを有効 / 無効に設定します。
Source MAC Verification	クライアントのハードウェアアドレスと DHCP パケットの送信元 MAC アドレスが一致しているかどうかの検証を有効 / 無効に設定します。
Station Move Deny	DHCP スヌーピングの端末移動拒否（Station Move Deny）を有効 / 無効に設定します。 端末移動を有効（本機能を無効）にすると、指定ポート上で同じ VLAN ID と MAC アドレスを持つダイナミック DHCP バインディングエントリは、新しい DHCP プロセスが同じ VLAN ID と MAC アドレスに属していることを検出した場合、他のポートへ移動することが可能です。

「Apply」をクリックして、設定内容を適用します。

■ DHCP Snooping Port Settings（DHCP スヌーピングポート設定）

DHCP スヌーピングポートの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings の順にクリックし、以下の画面を表示します。

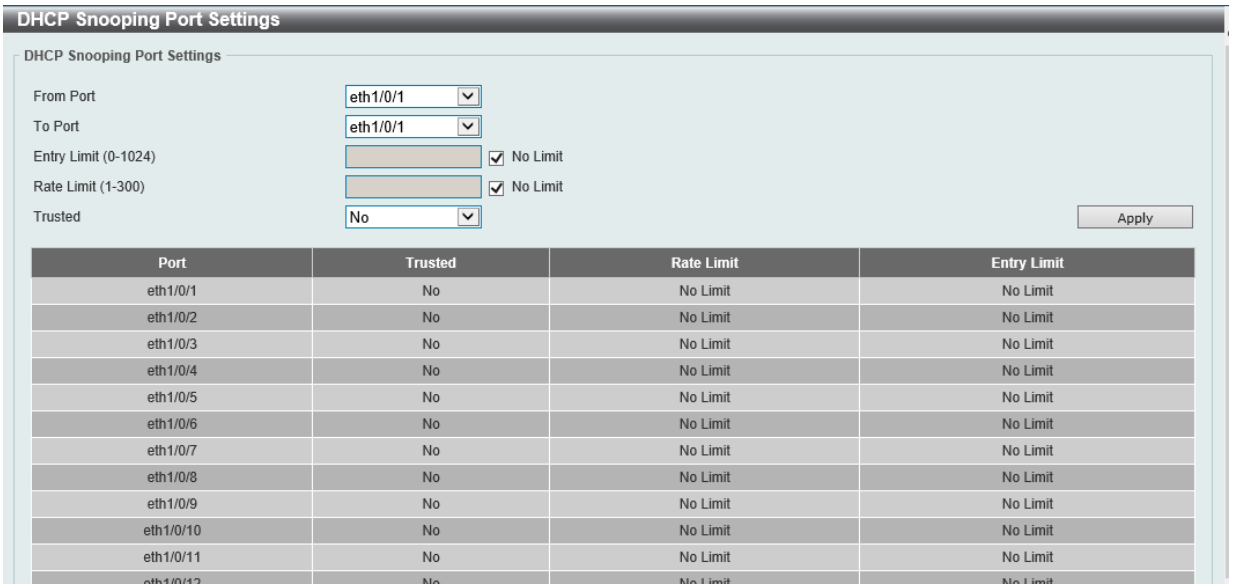


図 12-26　DHCP Snooping Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
Entry Limit	エントリリミットの値を入力します。「No Limit」にチェックをすると、本機能は無効になります。 • 設定可能範囲：0-1024
Rate Limit	レートリミットの値を入力します。「No Limit」にチェックをすると、本機能は無効になります。 • 設定可能範囲：1-300
Trusted	信頼済みオプションを選択します。 DHCP サーバや他のスイッチなどに接続しているポートは信頼済みインタフェースとして設定される必要があります。 DHCP クライアントに接続しているポートは信頼されていないポートとして設定します。 DHCP スヌーピングは、DHCP サーバと信頼されていないインタフェースの間でファイアウォールとして動作します。 • 選択肢：「No」「Yes」

「Apply」をクリックして、設定内容を適用します。

■ DHCP Snooping VLAN Settings（DHCP スヌーピング VLAN 設定）

DHCP スヌーピング VLAN の設定、表示を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings の順にクリックし、以下の画面を表示します。

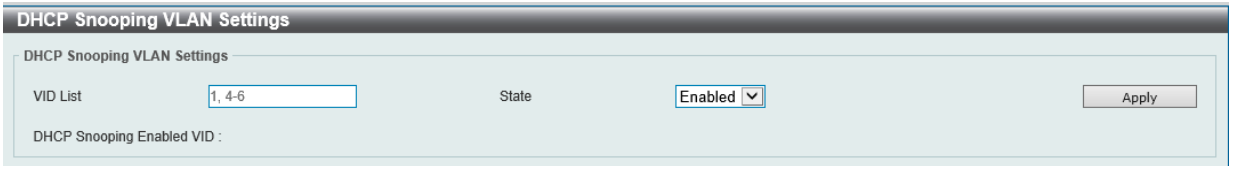


図 12-27　DHCP Snooping VLAN Settings 画面

画面に表示される項目：

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	DHCP スヌーピング VLAN を有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

■ DHCP Snooping Database（DHCP スヌーピングデータベース）

DHCP スヌーピングデータベースの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database の順にクリックし、以下の画面を表示します。

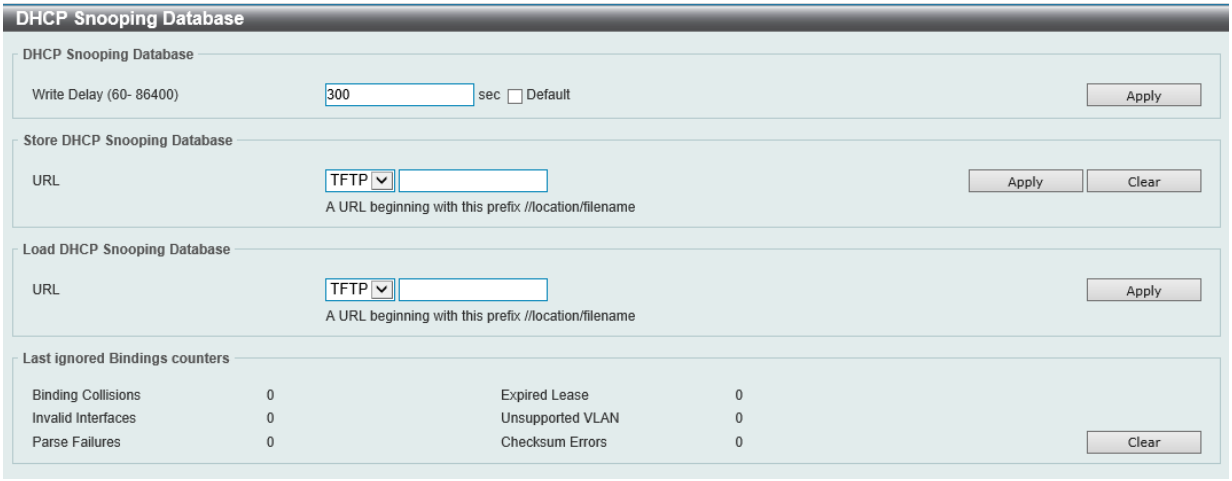


図 12-28　DHCP Snooping Database 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。
「Clear」をクリックするとカウンタ情報が消去されます。

■ DHCP Snooping Binding Entry（DHCP スヌーピングバインディングエントリ設定）

DHCP バインディングポートエントリの表示、設定を行います。

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

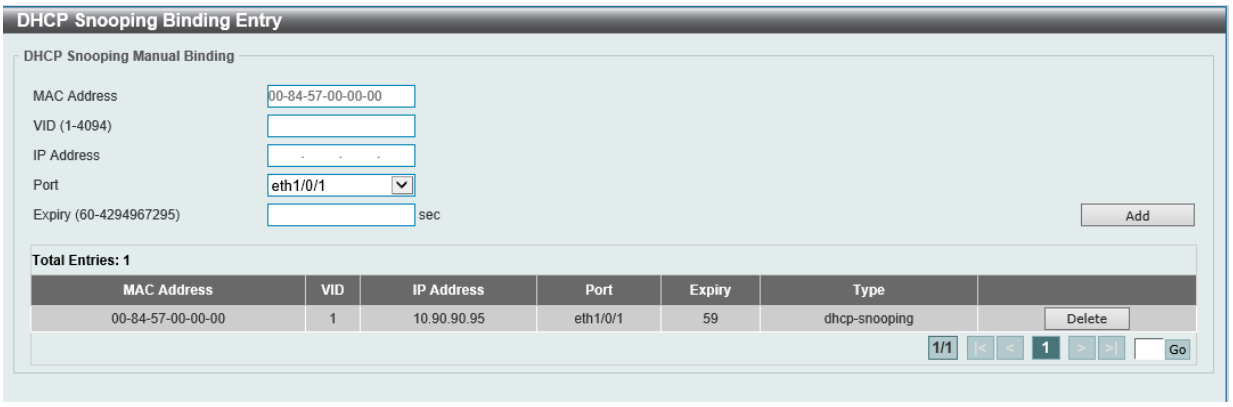


図 12-29　DHCP Snooping Binding Entry 画面

画面に表示される項目：

項目	説明
MAC Address	DHCP スヌーピングバインディングエントリの MAC アドレスを入力します。
VID	DHCP スヌーピングバインディングエントリの VLAN ID を入力します。 • 設定可能範囲：1-4094
IP Address	DHCP スヌーピングバインディングエントリの IP アドレスを入力します。
Port	設定するポートを指定します。
Expiry	有効期限を入力します。 • 設定可能範囲：60 - 4294967295（秒）

「Add」をクリックして入力した情報を基に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして特定のページへ移動します。

Dynamic ARP Inspection（ダイナミック ARP インスペクション）

■ ARP Access List（ARP アクセスリスト）

ARP アクセスリストの設定、表示を行います。

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

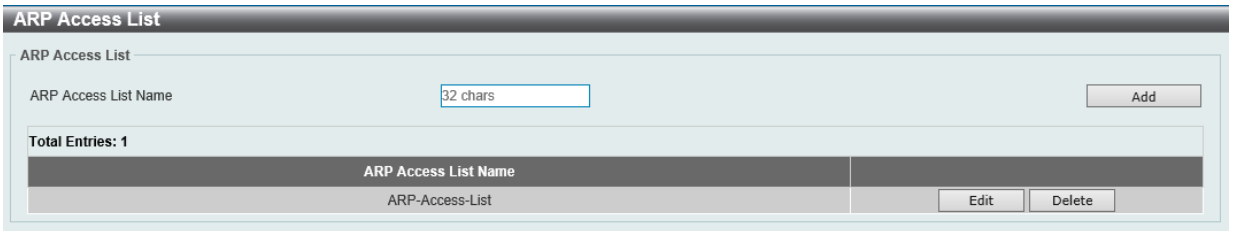


図 12-30　ARP Access List 画面

画面に表示される項目：

項目	説明
ARP Access List Name	ARP アクセスリスト名を入力します。（32 文字以内）

「Add」をクリックして入力した情報を基に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。

エントリの編集

「Edit」をクリックして、指定のエントリを編集します。以下の画面が表示されます。

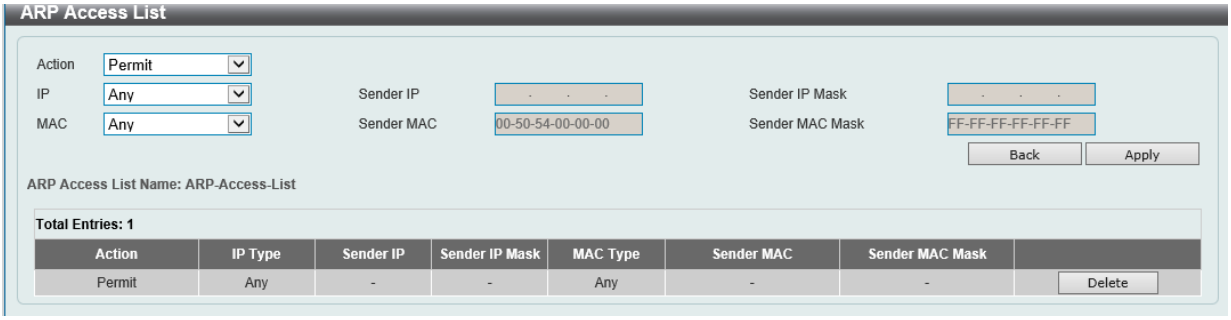


図 12-31　ARP Access List - Edit 画面

画面に表示される項目：

項目	説明
Action	実行するアクションを指定します。 • 選択肢：「Permit」（許可）、「Deny」（拒否）
IP	送信元 IP アドレスの種類を指定します。 • 選択肢：「Any」「Host」「IP with Mask」
Sender IP	送信元 IP アドレスを「Host」または「IP with Mask」に設定した場合、使用する送信元 IP アドレスを入力します。
Sender IP Mask	送信元 IP アドレスを「IP with Mask」に設定した場合、使用する送信元 IP マスクを入力します。
MAC	送信元 MAC アドレスの種類を指定します。 • 選択肢：「Any」「Host」「MAC with Mask」
Sender MAC	送信元 MAC アドレスを「Host」「MAC with Mask」から選択した後、使用する送信元 MAC アドレスを入力します。
Sender MAC Mask	「MAC with Mask」を選択した場合、使用する送信元 MAC マスクを入力します。

「Back」をクリックすると前のページに戻ります。

「Apply」をクリックして、設定内容を適用します。

「Delete」をクリックして指定エントリを削除します。

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

ARP インスペクションの設定、表示を行います。

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

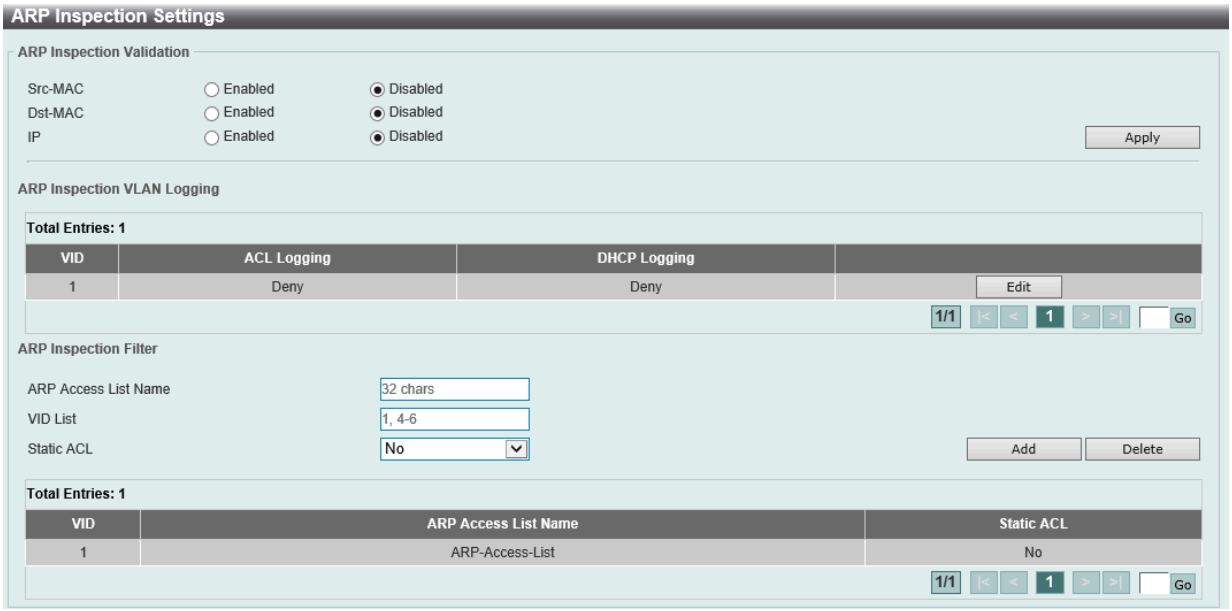


図 12-32　ARP Inspection Settings 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。
「Add」をクリックして入力した情報を基に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。

■ ARP Inspection Port Settings（ARP インスペクションポート設定）

ポートでの ARP インスペクションの設定、表示を行います。

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

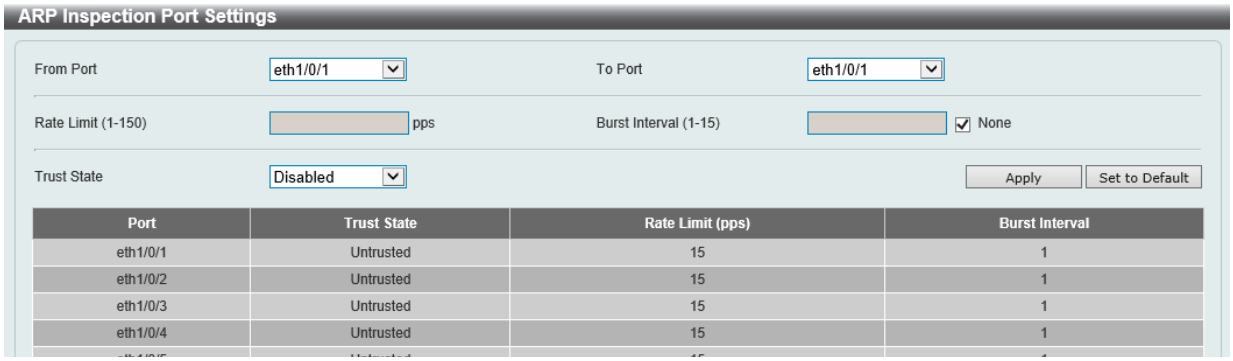


図 12-33　ARP Inspection Port Settings 画面

画面に表示される項目：

項目	説明
From Port/ To Port	設定するポートの範囲を指定します。
Rate Limit	レート制限の値を入力します。 • 設定可能範囲：1 - 150（パケット / 秒）
Burst Interval	バーストインターバルの値を入力します。「None」にチェックをいれるとオプションは無効になります。 • 設定可能範囲：1-15
Trust State	トラストステートを有効 / 無効に設定します。

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

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

VLAN での ARP インスペクションの設定、表示を行います。

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

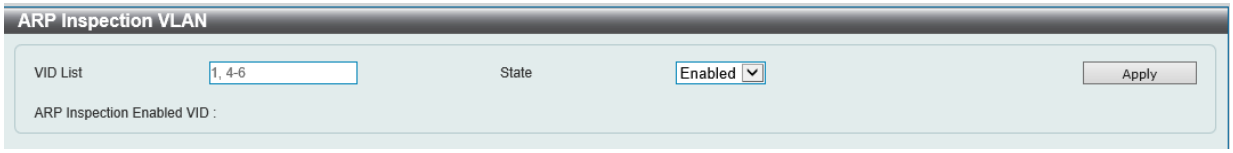


図 12-34　ARP Inspection VLAN 画面

画面に表示される項目：

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	指定 VLAN の ARP インスペクションについて有効 / 無効に設定します。

「Apply」をクリックして、設定内容を適用します。

■ ARP Inspection Statistics（ARP インスペクション統計）

ARP インスペクションの統計情報の表示、消去を行います。

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

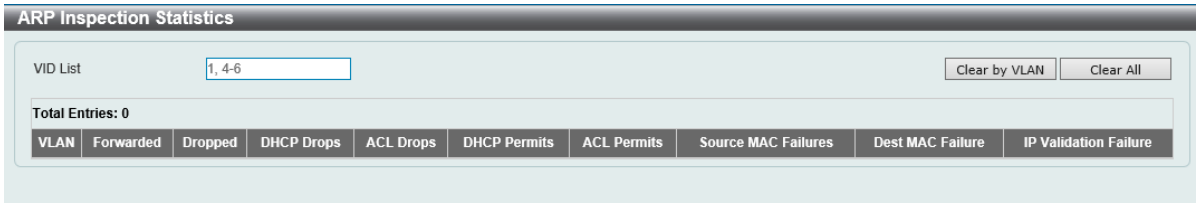


図 12-35　ARP Inspection Statistics 画面

画面に表示される項目：

項目	説明
VID List	統計情報を削除する VLAN ID リストを入力します。

「Clear by VLAN」をクリックして、入力した VLAN ID についての情報を消去します。
「Clear All」をクリックして、テーブルのすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動します。

■ ARP Inspection Log（ARP インスペクションログ）

ARP インスペクションログ情報の表示、消去、設定を行います。

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

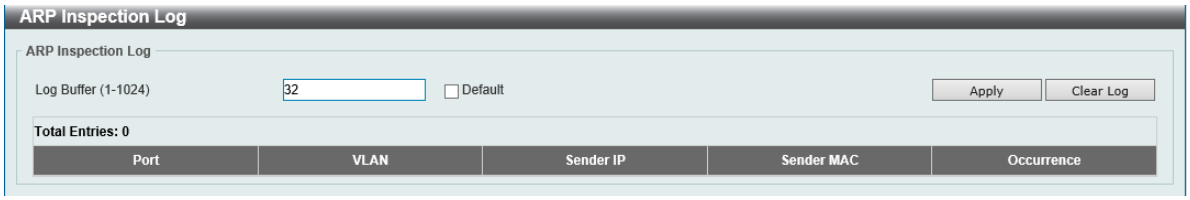


図 12-36　ARP Inspection Log 画面

画面に表示される項目：

項目	説明
Log Buffer	使用するログバッファの値を入力します。 • 設定可能範囲：1 - 1024 • 初期値：32

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

IP Source Guard（IP ソースガード）

■ IP Source Guard Port Settings（IP ソースガードポート設定）

IP ソースガード（IPSG）の表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings の順にクリックし、以下の画面を表示します。

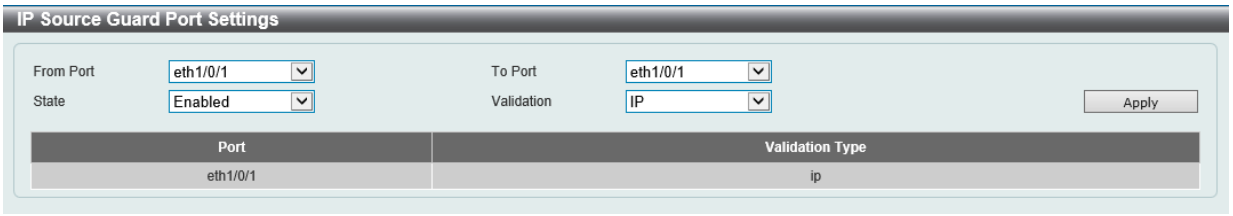


図 12-37　IP Source Guard Port Settings 画面

画面に表示される項目：

項目	説明
From Port/To Port	設定するポートの範囲を指定します。
State	指定ポートの IP ソースガードを有効 / 無効に設定します。
Validation	検証方法を選択します。 • 「IP」- 受信パケットの IP アドレスがチェックされます。 • 「IP-MAC」- 受信パケットの IP アドレスと MAC アドレスがチェックされます。

「Apply」をクリックして、設定内容を適用します。

■ IP Source Guard Binding（IP ソースガードバインディング）

IP ソースガードバインディングの表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding の順にクリックし、以下の画面を表示します。

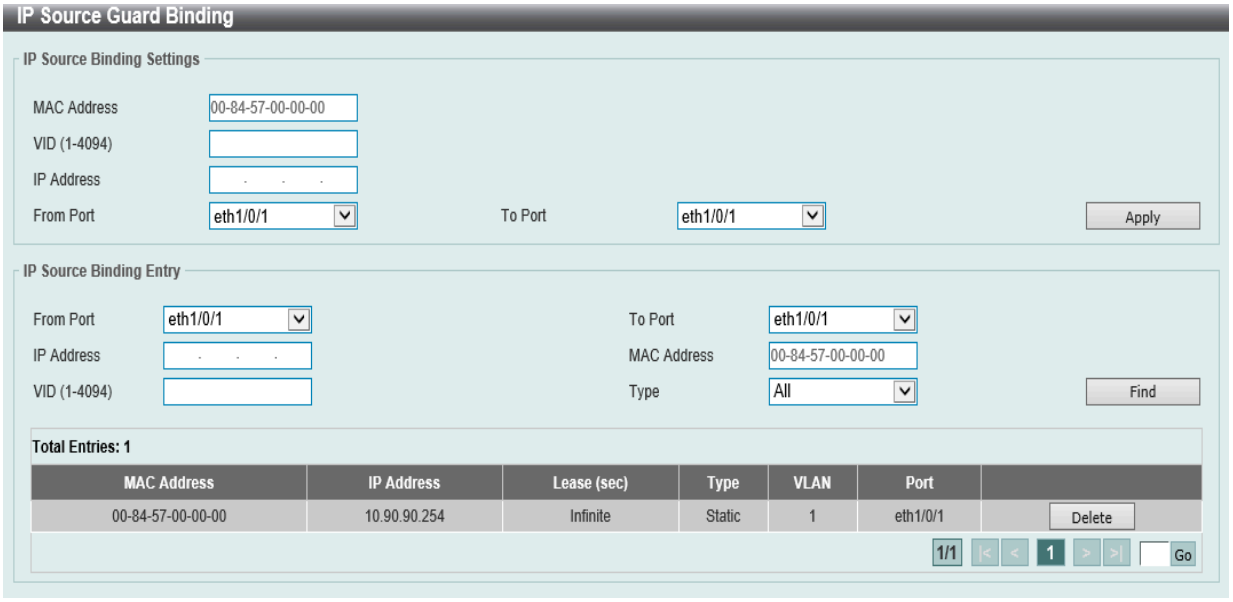


図 12-38　IP Source Guard Binding 画面

画面に表示される項目：

項目	説明
IP Source Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
IP Address	バインディングエントリの IP アドレスを入力します。
From Port/To Port	設定するポートの範囲を指定します。
IP Source Binding Entry	
From Port/To Port	バインディングエントリを検索するポートの範囲を指定します。
IP Address	バインディングエントリの IP アドレスを入力します。
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
Type	バインディングエントリの種類を選択します。 • 「All」- すべての DHCP バインディングエントリが表示されます。 • 「DHCP Snooping」- DHCP バインディングスヌーピングによって学習された IP ソースガードバインディングエントリが表示されます。 • 「Static」- 手動で設定した IP ソースガードバインディングが表示されます。

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、指定エントリを削除します。
「Find」をクリックして、入力した情報を基に指定のエントリを表示します。

■ IP Source Guard HW Entry（IP ソースガードハードウェアエントリ）

IP ソースガードハードウェアエントリの表示を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry の順にクリックし、以下の画面を表示します。

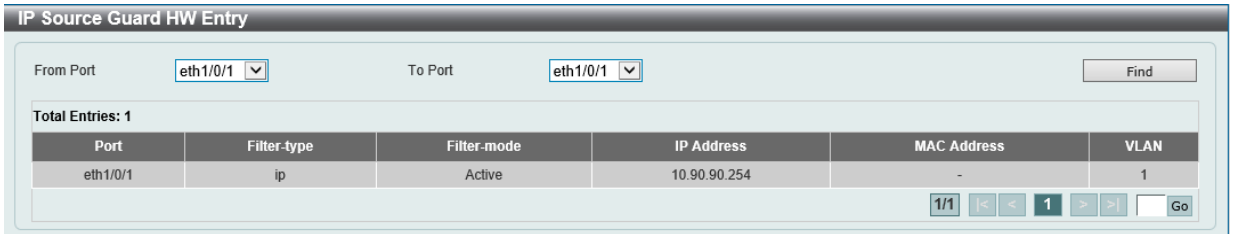


図 12-39　IP Source Guard HW Entry 画面

画面に表示される項目：

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

「Find」をクリックして指定した情報を基に指定のエントリを表示します。
複数ページが存在する場合は、ページ番号を入力後、「Go」をクリックして、特定のページへ移動します。

Advanced Settings（詳細設定）

■ IP-MAC-Port Binding Settings（IP-MAC ポートバインディング設定）

IP-MAC ポートバインディングの設定、表示を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings の順にクリックし、以下の画面を表示します。

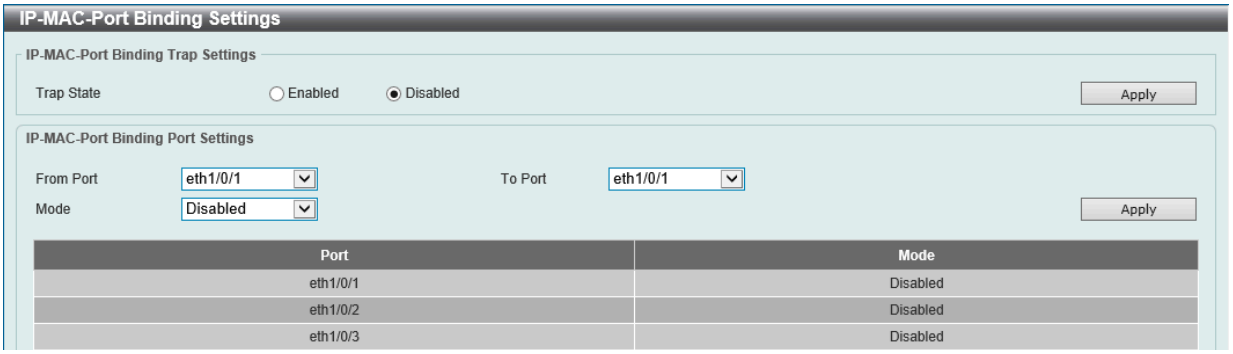


図 12-40　IP-MAC-Port Binding Settings 画面

画面に表示される項目：

項目	説明
IP-MAC-Port Binding Trap Settings	
Trap State	IP-MAC ポートバインディングのトラップ設定を有効 / 無効に指定します。
IP-MAC-Port Binding Port Settings	
From Port/ To Port	設定するポートの範囲を指定します。
Mode	アクセスコントロールのモードを選択します。 • 「Disabled」- 指定ポートで IP-MAC-Port バインディング機能が無効になります。 • 「Strict」- ホストが ARP/IP パケット送信後、それらのパケットがバインディングチェックを通過した場合に、ポートへアクセスできます。バインディングチェックを通過するには、送信元 IP アドレス / 送信元 MAC アドレス /VLAN ID/ 受信ポート番号が、IP ソースガードスタティックバインディングエントリ、または DHCP スヌーピングによって学習されたダイナミックバインディングエントリのいずれかのエントリに一致する必要があります。 • 「Loose」- ホストが ARP/IP パケット送信後、それらのパケットがバインディングチェックを通過しなかった場合にポートへのアクセスが拒否されます。バインディングチェックを通過するには、送信元 IP アドレス / 送信元 MAC アドレス / VLAN ID/ 受信ポート番号が、IP ソースガードスタティックバインディングエントリ、または DHCP スヌーピングによって学習されたダイナミックバインディングエントリのいずれかのエントリに一致する必要があります。

「Apply」をクリックして、設定内容を適用します。

■ IP-MAC-Port Binding Blocked Entry（IP-MAC ポートバインディングブロックエントリ）

IP-MAC ポートバインディングブロックエントリの表示、消去を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry の順にクリックし、以下の画面を表示します。

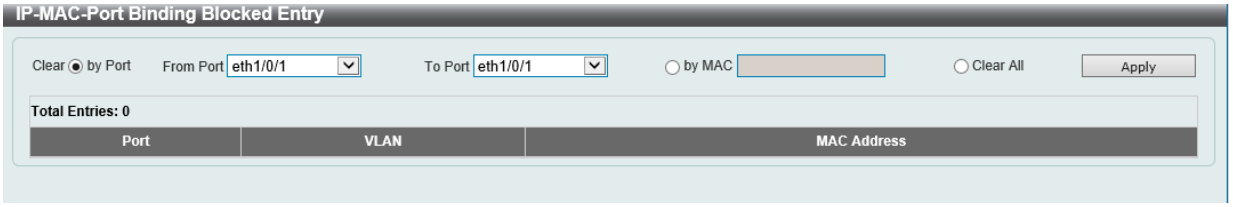


図 12-41　IP-MAC-Port Binding Blocked Entry 画面

画面に表示される項目：

項目	説明
Clear by Port	選択ポートに基づいたエントリテーブルをクリアにします。
From Port/ To Port	設定するポートの範囲を指定します。
Clear by MAC	指定した MAC アドレスに基づきエントリを消去します。項目欄に MAC アドレスを入力します。
Clear All	MAC アドレスを含むすべてのエントリを消去します。

「Apply」をクリックして、設定内容を適用します。

IPv6

IPv6 Snooping（IPv6 スヌーピング）

IPv6 スヌーピングについて表示、設定します。

Security > IMPB > IPv6 > IPv6 Snooping の順にクリックし、以下の画面を表示します。

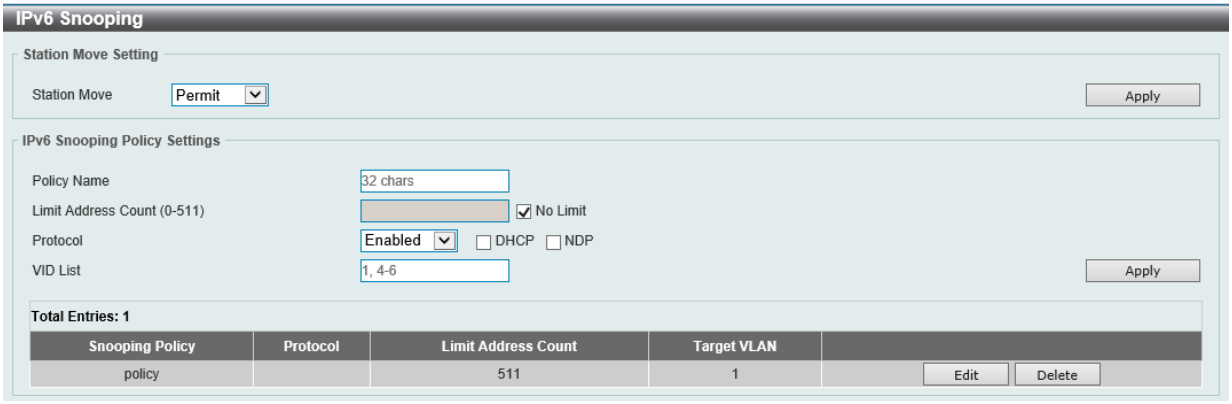


図 12-42　IPv6 Snooping 画面

画面に表示される項目：

項目	説明
	Station Move Setting
Station Move	ステーション移行について設定します。 • 「Permit」（許可）、「Deny」（拒否）
	IPv6 Snooping Policy Settings
Policy Name	IPv6 スヌーピングポリシー名を入力します。（32 文字以内）
Limit Address Count	アドレスカウント制限の値を指定します。「No Limit」を指定するとアドレスカウント制限は無効になります。 • 設定可能範囲：0-511
Protocol	プロトコルステートを有効 / 無効に設定し、本ポリシーに対応するプロトコルを選択します。 • 「DHCP」- DHCPv6 パケットのアドレスがスヌーピングされます。 • 「NDP」- NDP パケットのアドレスがスヌーピングされます。 DHCPv6 スヌーピング： アドレス割り当ての際に DHCPv6 クライアントとサーバ間の DHCPv6 パケットをスヌーピングします。DHCPv6 クライアントが有効な IPv6 アドレスを取得すると、DHCPv6 スヌーピングによってバインディングデータベースが作成されます。 ND スヌーピング： ステートレス自動設定による IPv6 アドレスと手動設定による IPv6 アドレスのための機能です。IPv6 アドレスを割り当てる前に、ホストは「Duplicate Address Detection」（DAD：重複アドレス検出）を実行する必要があります。ND スヌーピングは DAD メッセージ（DAD NS と DAD NA）を受信しバインディングデータベースを構築します。NDP パケット (NS と NA) は、ホストが到達可能かを判断しバインディングを削除するかどうかを決定するためにも使用されます。
VID List	使用する VLAN ID リストを入力します。

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

IPv6 ND Inspection（IPv6 ND インスペクション）

IPv6 ND インスペクションについて表示、設定します。

Security > IMPB > IPv6 > IPv6 ND Inspection の順にクリックし、以下の画面を表示します。

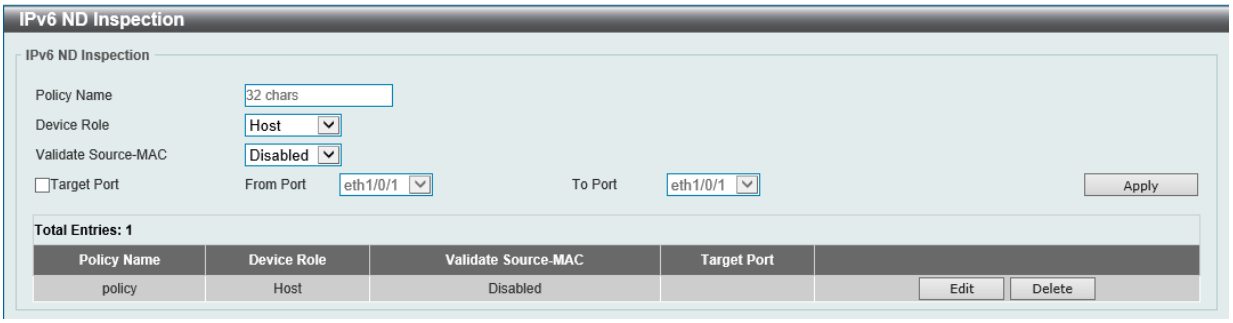


図 12-43　IPv6 ND Inspection 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 • 「Host」- デバイスの役割をホストに設定します。NS/NA メッセージに対するインスペクションが実行されます。（初期値） • 「Router」- デバイスの役割をルータに設定します。NS/NA に対するインスペクションは実行されません。 NS/NA インスペクションを動作させるときは、DHCP もしくは ND プロトコルから学習したダイナミックバインディングテーブルに対しての妥当性の確認が必要です。
Validate Source-MAC	送信元 MAC アドレスオプションの検証を有効 / 無効に設定します。 リンクレイヤアドレスを含む ND メッセージを受信した時に、リンクレイヤアドレスに対して送信元 MAC アドレスがチェックされます。リンクレイヤアドレスと MAC アドレスが異なる場合、パケットは破棄されます。
Target Port	チェックを入れターゲットポートを指定します。
From Port/To Port	設定するポートの範囲を選択します。

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

IPv6 RA Guard（IPv6 RA ガード）

IPv6 RA ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 RA Guard の順にクリックし、以下の画面を表示します。

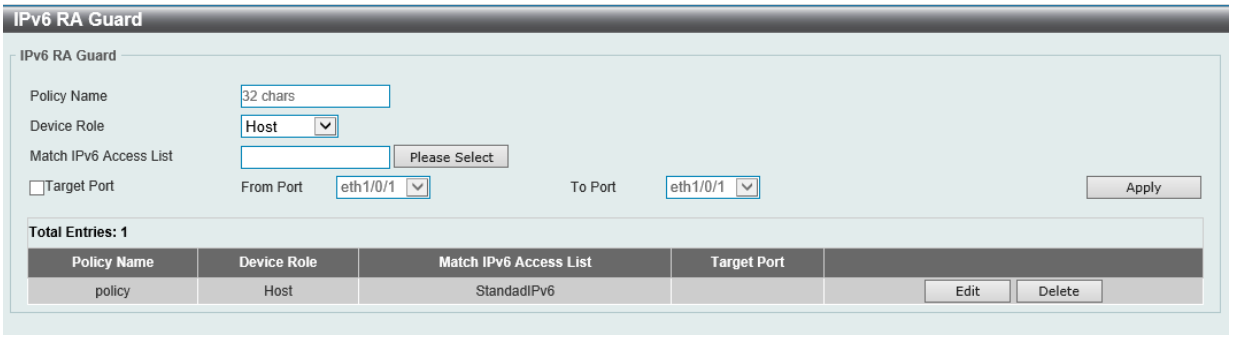


図 12-44　IPv6 RA Guard 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 • 「Host」- デバイスの役割をホストに設定します。RA パケットはすべてブロックされます。（初期値） • 「Router」- デバイスの役割をルータに設定します。RA パケットは、ポートに設定された ACL に従い転送されます。
Match IPv6 Access List	照合を行う IPv6 アクセスリストを入力します。 「Please Select」をクリックすると、既存の ACL を選択できます。
Target Port	チェックを入れ、ターゲットポートを指定します。
From Port/ To Port	設定するポートの範囲を指定します。

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

ACL 選択画面

「Please Select」をクリックすると次の画面が表示されます。

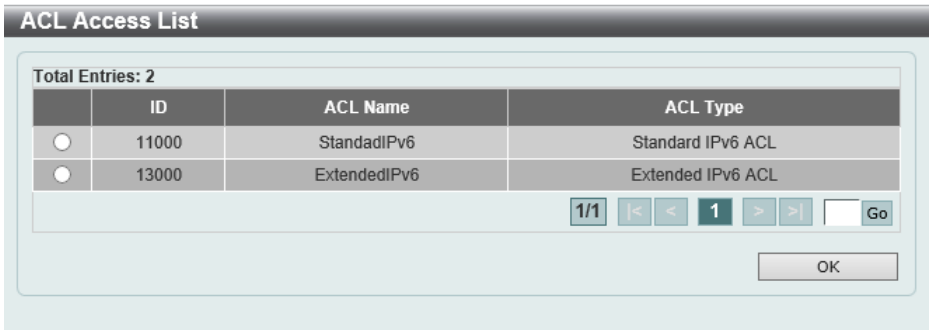


図 12-45　ACL Access List 画面

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

IPv6 DHCP Guard（IPv6 DHCP ガード）

IPv6 DHCP ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 DHCP Guard の順にクリックし、以下の画面を表示します。

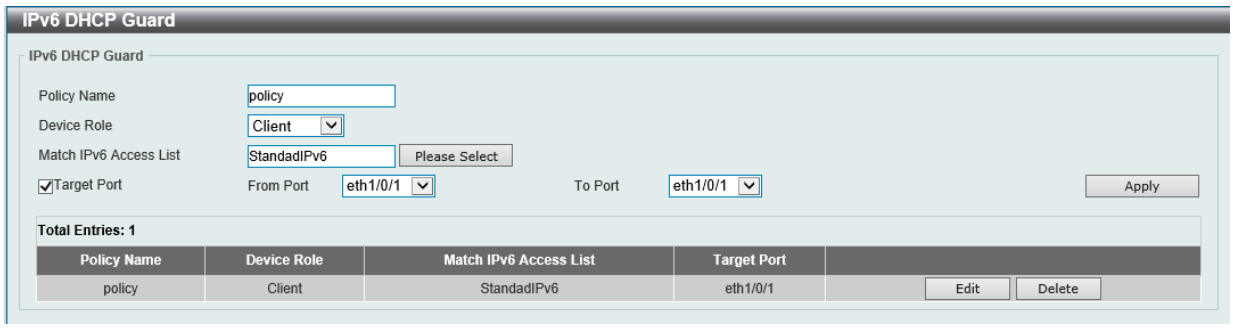


図 12-46　IPv6 DHCP Guard 画面

画面に表示される項目：

項目	説明
Policy Name	ポリシー名を入力します。（32 文字以内）
Device Role	デバイスの役割を選択します。 • 「Client」- DHCPv6 サーバからの DHCPv6 パケットはすべてブロックされます。（初期値） • 「Server」- DHCPv6 サーバパケットはポートに設定された ACL に従い転送されます。
Match IPv6 Access List	照合する IPv6 アクセスリストを入力します。 「Please Select」をクリックすると、既存のエントリから選択することができます。
Target Port	チェックを入れ、ターゲットポートを指定します。
From Port/ To Port	設定するポートの範囲を選択します。

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

ACL 選択画面

「Please Select」をクリックすると次の画面が表示されます。

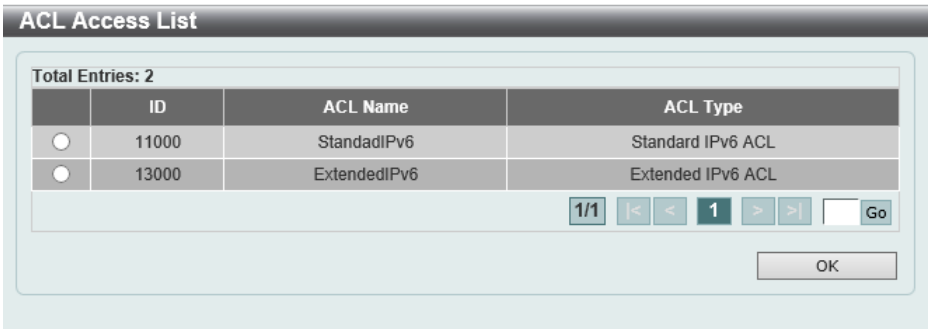


図 12-47　ACL Access List 画面

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

IPv6 Source Guard（IPv6 ソースガード）

■ IPv6 Source Guard Settings（IPv6 ソースガード設定）

IPv6 ソースガードの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings の順にクリックし、以下の画面を表示します。

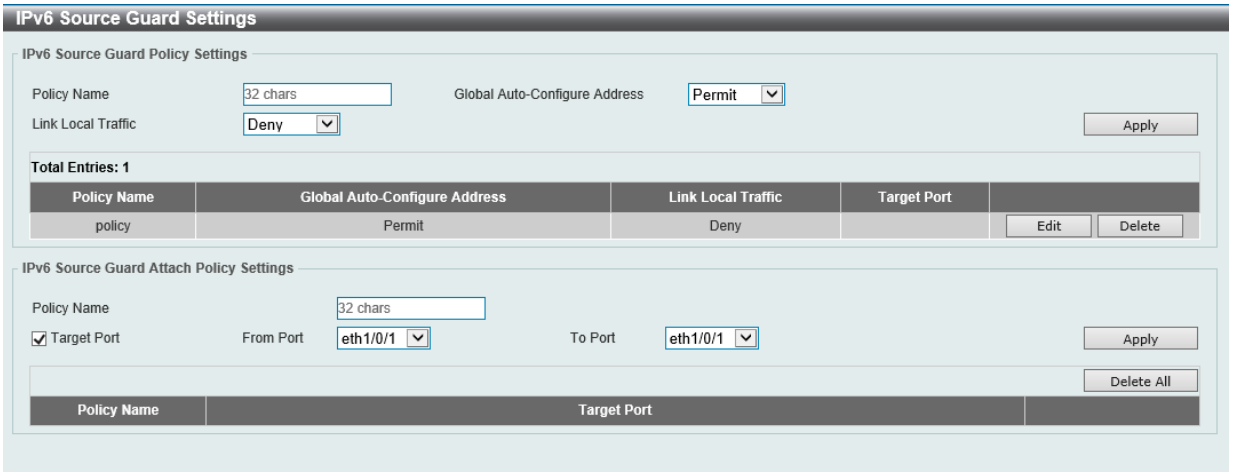


図 12-48　IPv6 Source Guard Settings 画面

画面に表示される項目：

項目	説明
IPv6 Source Guard Policy Settings	
Policy Name	ポリシー名を入力します。（32 文字以内）
Global Auto-Configure Address	自動設定グローバルアドレスからのデータトラフィックの許可 / 拒否を選択します。リンク上のすべてのグローバルアドレスが DHCP によって割り当てられていて、ホスト自身による設定アドレスからのトラフィック送信をブロックしたい場合に役に立ちます。 • 選択肢：「Permit」（許可）、「Deny」（拒否）
Link Local Traffic	ハードウェアによって許可されたリンクローカルアドレスからのデータトラフィックを許可 / 拒否します。 • 選択肢：「Permit」（許可）、「Deny」（拒否）
IPv6 Source Guard Attach Policy Settings	
Policy Name	ポリシー名を入力します。（32 文字以内）
Target Port	ターゲットポートを指定します。
From Port/To Port	設定するポートの範囲を指定します。

「Apply」をクリックして、設定内容を適用します。
「Edit」をクリックして、指定エントリを編集します。

「Delete」をクリックして、指定エントリを削除します。
「Delete All」をクリックして、すべてのエントリを削除します。

■ IPv6 Neighbor Binding（IPv6 ネイババインディング）

IPv6 ネイババインディングの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding の順にクリックし、以下の画面を表示します。

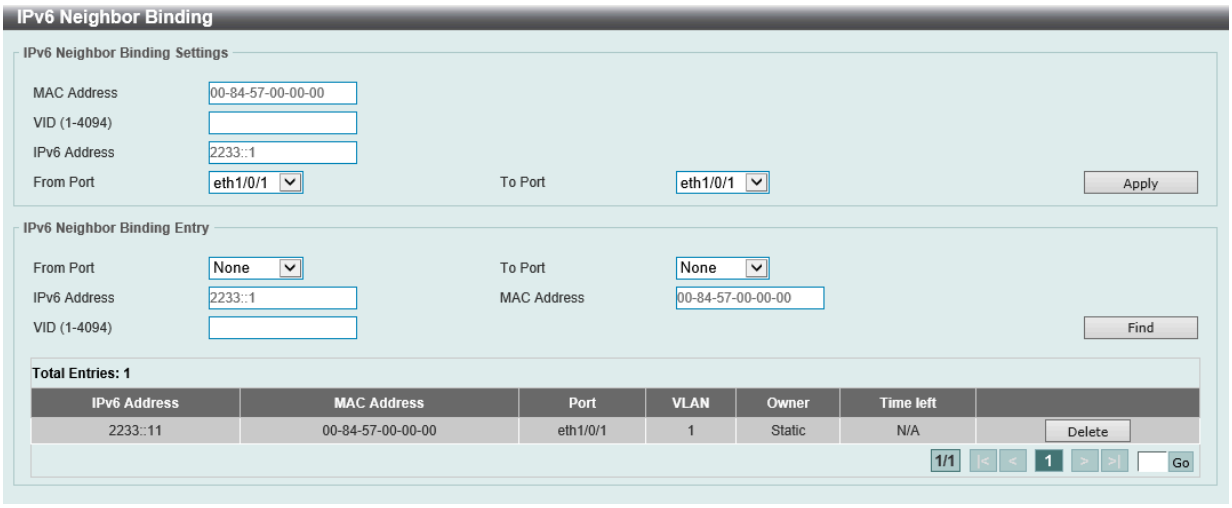


図 12-49　IPv6 Neighbor Binding 画面

画面に表示される項目：

項目	説明
IPv6 Neighbor Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。 • 設定可能範囲：1-4094
IPv6 Address	バインディングエントリの IPv6 アドレスを入力します。
From Port/To Port	設定するポートの範囲を指定します。
IPv6 Neighbor Binding Entry	
From Port/To Port	設定するポートの範囲を指定します。
IPv6 Address	検索する IPv6 アドレスを入力します。
MAC Address	検索する MAC アドレスを入力します。
VID	検索する VLAN ID を入力します。

「Apply」をクリックして、設定内容を適用します。
「Delete」をクリックして、指定エントリを削除します。
「Find」をクリックして、情報を基に指定のエントリを表示します。

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

DHCP Server Screening（DHCP サーバスクリーニング設定）

DHCP サーバパケットの制限や、DHCP クライアントが指定の DHCP サーバパケットを受信するように設定します。複数の DHCP サーバがネットワーク上に存在し、それぞれ異なる個別のクライアントグループに DHCP サービスを提供する場合に役立ちます。

ポートで DHCP サーバスクリーニング機能が有効になっている場合、このポートで受信したすべての DHCP サーバパケットは、ソフトウェアベースのチェックのために CPU にリダイレクトされます。 正当な DHCP サーバパケットは転送され、不正な DHCP サーバパケットは破棄されます。
DHCP サーバスクリーニング機能を有効にすると、すべての DHCP サーバパケットが特定のポートでフィルタリングされます。

DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）

DHCP サーバスクリーニングのグローバル設定を行います。

Security > DHCP Server Screening > DHCP Server Screening Global Settings の順にメニューをクリックして画面を表示します。

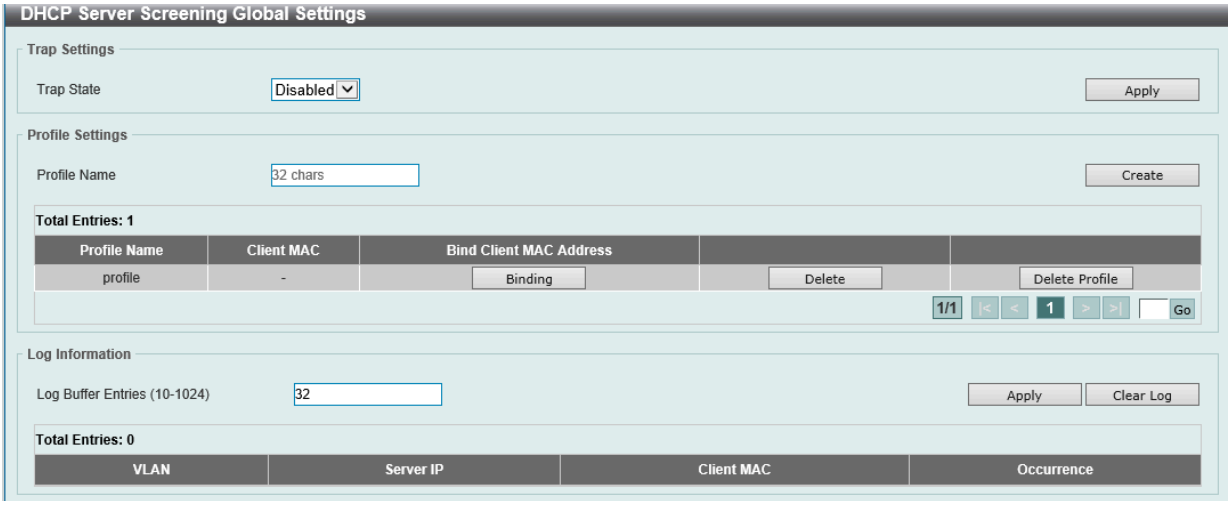


図 12-50　DHCP Server Screening Global Settings 画面

画面に表示される項目：

項目	説明
Trap Settings	
Trap State	DHCP サーバスクリーニングのトラップ機能を有効 / 無効に設定します。
Profile Settings	
Profile Name	DHCP サーバスクリーニングのプロファイル名を入力します。（32 文字以内）
Log Information	
Log Buffer Entries	ログバッファエントリ数を入力します。 • 設定可能範囲：10-1024 • 初期値：32

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

MAC アドレスのバインディング

「Binding」をクリックすると以下の画面が表示されます。

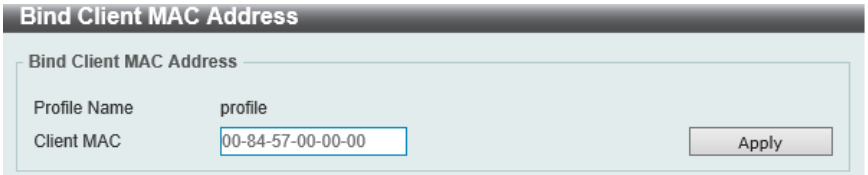


図 12-51　Bind Client MAC Address 画面

画面に表示される項目：

項目	説明
Client MAC	使用する MAC アドレスを指定します。

「Apply」をクリックして、設定内容を適用します。

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

DHCP サーバスクリーニングポートの表示、設定を行います。

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

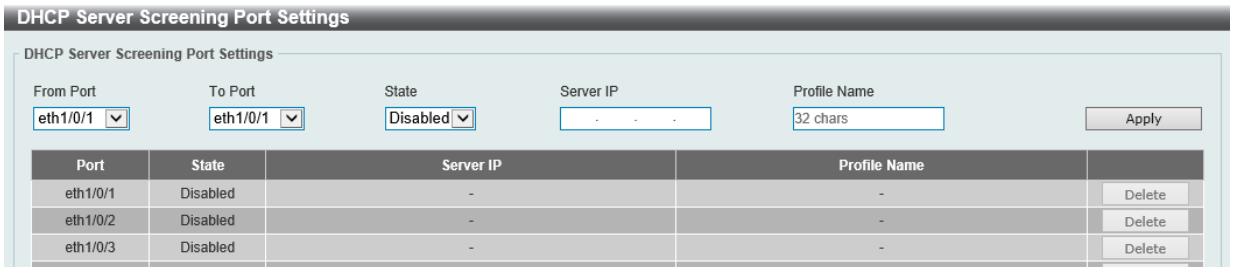


図 12-52　DHCP Server Screening Port Settings 画面

画面に表示される項目：

項目	説明
From Port/ To Port	設定するポートの範囲を指定します。
State	指定ポートでの DHCP サーバスクリーニング機能を有効 / 無効に設定します。
Server IP	DHCP サーバの IP アドレスを入力します。
Profile Name	ポートに設定する DHCP サーバスクリーニングプロファイル名を入力します。

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

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。
エントリが作成されると、送信元 IP アドレスがエントリのゲートウェイ IP アドレスと一致するものの、送信元 MAC アドレスがエントリのゲートウェイ MAC アドレスと一致しない ARP パケットは、システムによって破棄されます。 送信元 IP アドレスがゲートウェイ IP アドレスと一致しない ARP パケットは、ASP によってバイパスされます。

ARP アドレスが設定済みのゲートウェイの IP アドレス、MAC アドレス、およびポートリストと一致する場合、受信ポートが ARP により信頼済みか否かにかかわらず、ダイナミック ARP インスペクション（DAI）チェックをバイパスします。

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

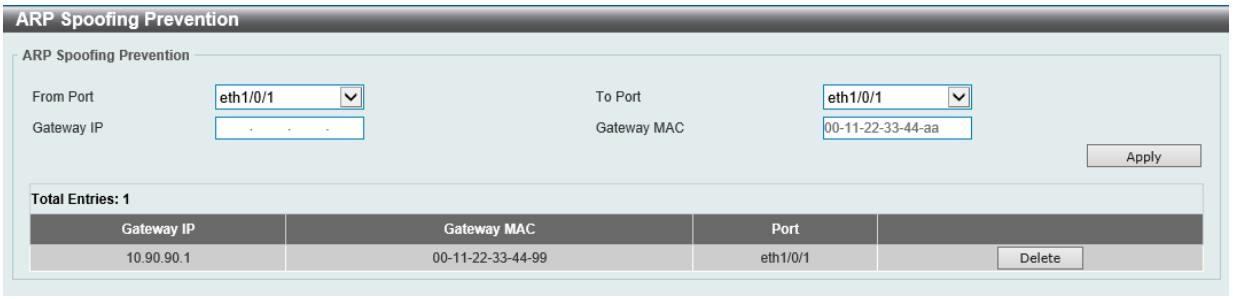


図 12-53　ARP Spoofing Prevention 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
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」をクリックして、変更を適用します。
「Delete」をクリックして、指定エントリを削除します。

補足　設定可能なダイナミック ARP エントリ数は最大 1500 です。

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

Guest VLAN（ゲスト VLAN 設定）

ネットワークアクセス認証のゲスト VLAN の表示、設定を行います。

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

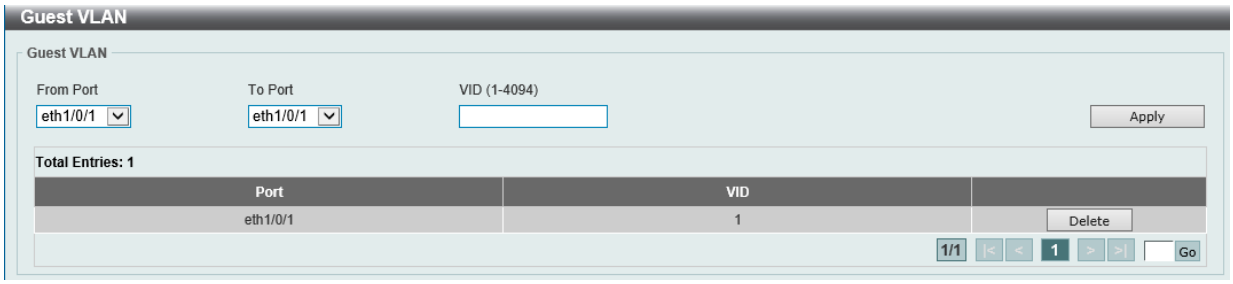


図 12-54　Guest VLAN 画面

画面に表示される項目：

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

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

Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）

ネットワークアクセス認証のグローバルステータスを設定します。

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

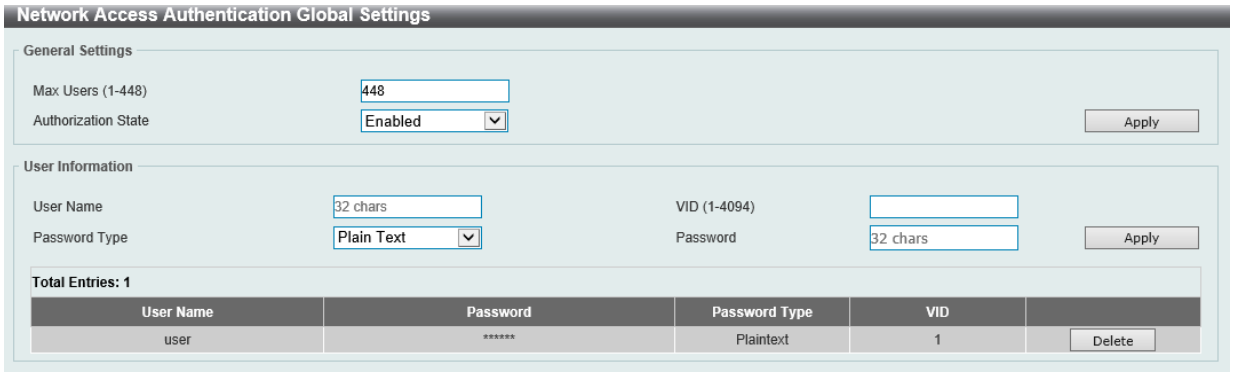


図 12-55　Network Access Authentication Global Settings 画面

画面に表示される項目：

項目	説明
General Settings	
Max Users	許可するユーザの最大数を指定します。 • 設定可能範囲：1-448 • 初期値：448
Authorization State	承認について有効 / 無効に指定します。 本オプションは、認証された設定を承認するかどうかを指定します。認証への承認が有効になると、RADIUS サーバにより付与される権限属性（VLAN など）が許容されます。
User Information	
User Name	ユーザ名を入力します。（32 文字以内）
VID	VLAN ID を入力します。
Password Type	パスワードの種類を選択します。 • 選択肢：「Plain Text」（平文）
Password	パスワードを入力します。（32 文字以内）

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

Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）

ネットワークアクセス認証のポート設定を行います。

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

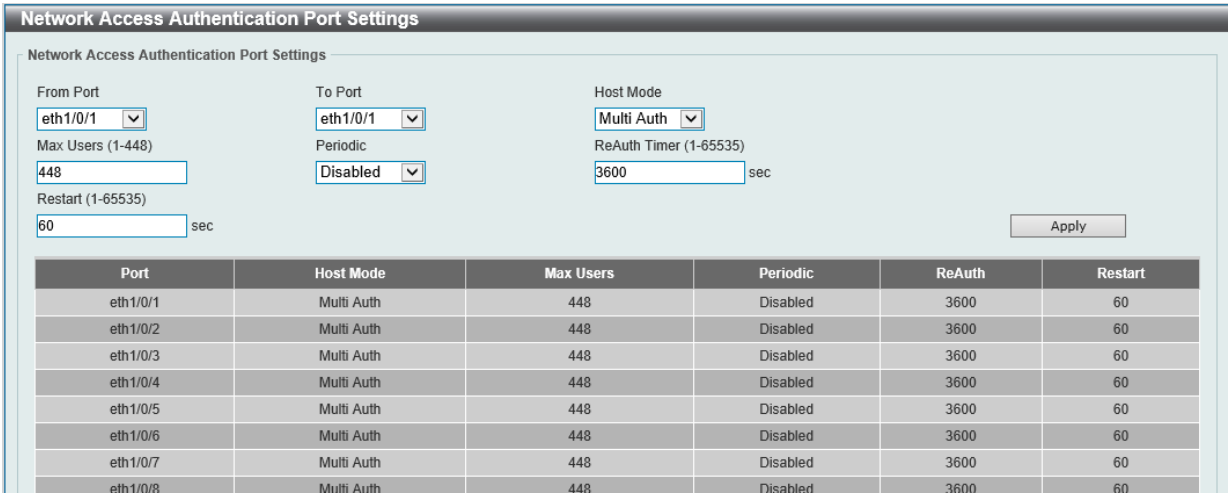


図 12-56　Network Access Authentication Port Settings 画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Host Mode	選択ポートに適用するホストモードを選択します。 • 「Multi Host」- ポートがマルチホストモードで動作している場合、一台のホストが認証されると、他のすべてのホストについてもポートへのアクセスが許可されます。802.1X 認証に従い、再認証失敗や認証ユーザのログオフなどが発生した場合、ポートはしばらくの間ブロックされます。一定の時間が過ぎると、EAPOL パケットの処理を元に戻します。 • 「Multi Auth」- ポートがマルチ認証モードで動作している場合、各ホストに対し、ポートへのアクセスに認証が必要になります。ホストは MAC アドレスによって識別され、認証されたホストのみポートへのアクセスが可能になります。（初期値）
Max Users	最大ユーザ数を指定します。 • 設定可能範囲：1-448
Periodic	選択ポートの定期的な再認証を有効 / 無効に設定します。802.1X プロトコルにのみ影響します。 • 初期値：「Disabled」（無効）
ReAuth Timer	再認証タイマを指定します。 • 設定可能範囲：1 - 65535（秒） • 初期値：3600（秒）
Restart	リスタート時間を入力します。 • 設定可能範囲：1 - 65535（秒） • 初期値：60（秒）

「Apply」をクリックして、設定内容を適用します。

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

ネットワークアクセス認証セッションの情報表示、クリアを行います。

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

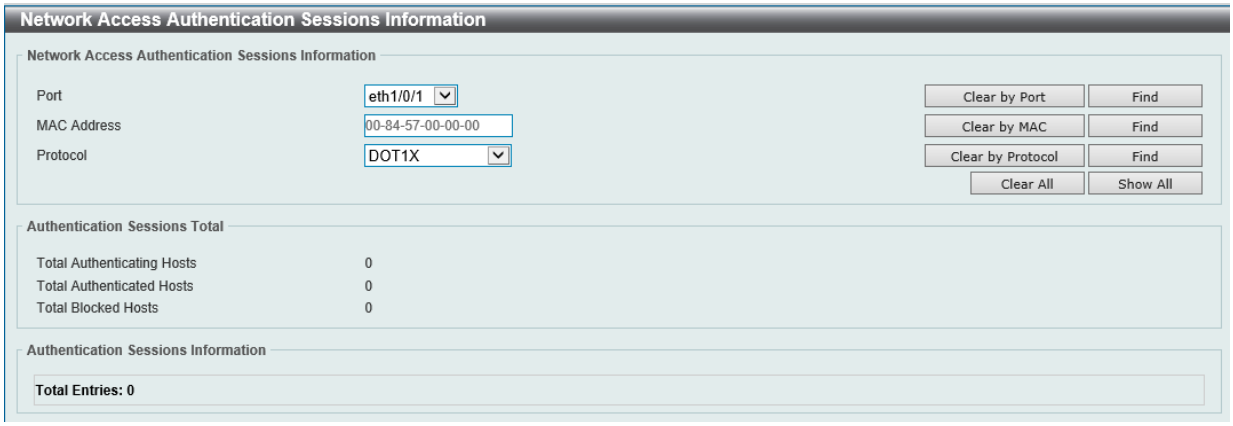


図 12-57　Network Access Authentication Sessions Information 画面

画面に表示される項目：

項目	説明
Port	表示 / クリアするポートを指定します。
MAC Address	表示 / クリアする MAC アドレスを指定します。
Protocol	プロトコルオプションを選択します。 • 選択肢：「DOT1X」

「Apply」をクリックして、設定内容を適用します。

情報の消去

「Clear by Port」をクリックして、選択したポートに基づく情報を消去します。
「Clear by MAC」をクリックして、選択した MAC アドレスに基づく情報を消去します。
「Clear by Protocol」をクリックして、選択したプロトコルに基づく情報を消去します。
「Clear All」をクリックして、テーブル上のすべての情報を消去します。

エントリの検出 / 表示

「Find」をクリックして、入力した情報を基に指定のエントリを検出します。
「Show All」をクリックして、すべてのエントリを表示します。

注意　dot1x の機能において、定期的に EAP Request/Identity を送信する機能はありません。

Safeguard Engine（セーフガードエンジン）

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃により、スイッチの CPU 負荷は対応可能なキャパシティを超えて増大してしまう可能性があります。このような問題を軽減するために、本スイッチにはセーフガードエンジン機能が実装されています。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化してスイッチ全体の操作性を保ち、限られたリソース内で重要なパケットの送受信を可能にします。

CPU 負荷が上昇しきい値を超えると、セーフガードエンジン機能が作動し、スイッチは「Exhausted」モードに入ります。Exhausted モードでは、スイッチは ARP と IP パケットで使用可能な帯域を制限します。CPU 負荷がしきい値を下回った場合、セーフガードエンジンは動作を停止し、スイッチは Exhausted モードを脱却して通常モードへ移行します。

CPU 宛に送信されるパケットは 3 つのグループに分類されます。サブインタフェースとしても知られるこれらのグループは、CPU が特定の種類のトラフィックを識別するために使用する論理的なインタフェースです。この 3 つのグループは「プロトコル」「管理」「ルート」に分類されています。通常、スイッチの CPU が受信パケットを処理する際、「プロトコル」グループが最も高い優先度のパケットを受信し、（スイッチの CPU は基本的にルーティングパケットの処理を行うため）「ルート」グループは最も優先度の低いパケットを受信します。「プロトコル」グループで処理されるパケットは、ルータによって識別されたプロトコルコントロールパケットです。「管理」グループ内では、パケットは Telnet や SSH などの相互通信プロトコルによって、ルータやシステムネットワーク管理インタフェースへ送信されます。「ルート」グループで処理されるパケットは、一般にルータ CPU によって処理される通過ルーティングパケットとして認識されます。

以下の表ではプロトコルと対応するサブインタフェースを表示します。

プロトコル名	サブインタフェース（グループ）	概要
802.1X	Protocol	Port-based Network Access Control（ポートベースアクセスコントロール）
ARP	Protocol	Address resolution Protocol（ARP）
DHCP	Protocol	Dynamic Host Configuration Protocol（DHCP）
DNS	Protocol	Domain Name System（DNS）
GVRP	Protocol	GARP VLAN Registration Protocol（GVRP）
ICMPv4	Protocol	Internet Control Message Protocol（ICMP）
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol（NS/NA/RS/RA）
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol（NS/NA/RS/RA）
IGMP	Protocol	Internet Group Management Protocol（IGMP）
LACP	Protocol	Link Aggregation Control Protocol（LACP）
SNMP	Manage	Simple Network Management Protocol（SNMP）
SSH	Manage	Secure Shell（SSH）
STP	Protocol	Spanning Tree Protocol（STP）
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol（TFTP）
Web	Manage	Hypertext Transfer Protocol（HTTP） Hypertext Transfer Protocol Secure（HTTPS）

カスタマイズされたレートリミット（パケット / 秒）、をセーフガードエンジンのサブインタフェースに対してまとめて割り当て、または管理インタフェースで指定した個々のプロトコルに対して割り当てることが可能です。本機能を使用して個々のプロトコルのレート制限をカスタマイズする場合、不適切なレート制限を設定すると、パケットの処理に異常が発生する場合がありますのでご注意ください。

注意 エンジンガードが有効になっている場合、スイッチは FFP（高速フィルタプロセッサ）メータリングテーブルを使用して、様々なトラフィックフロー（ARP、IP）に帯域幅を割り当て、CPU 使用率とトラフィック制限を制御します。これにより、ネットワーク経由のトラフィックルーティング速度が制限される場合があります。

Safeguard Engine Settings（セーフガードエンジン設定）

スイッチにセーフガードエンジンの設定を行います。

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

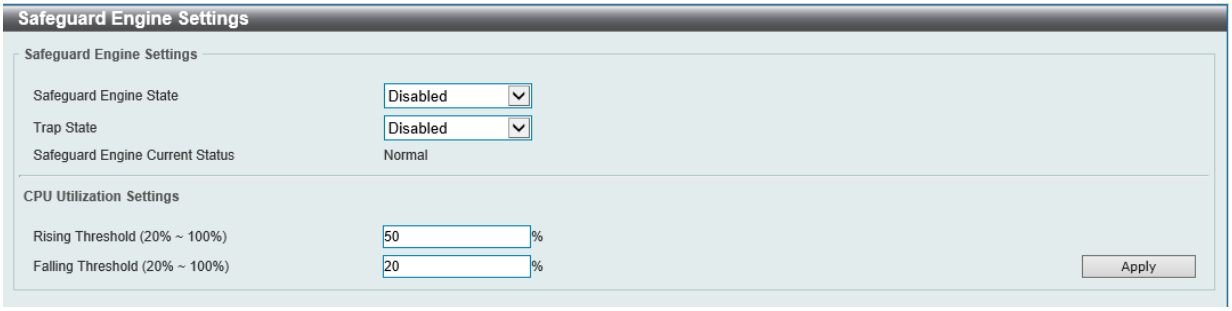


図 12-58　Safeguard Engine Settings 画面

画面に表示される項目：

項目	説明
Safeguard Engine Settings	
Safeguard Engine State	セーフガードエンジン機能を有効 / 無効に設定します。
Trap State	セーフガードエンジンのトラップを有効 / 無効に設定します。
Safeguard Engine Current Status	現在のセーフガードエンジンのステータスを表示します。
CPU Utilization Settings	
Rising Threshold	CPU 使用率の上昇しきい値を設定します。 CPU 使用率がこのしきい値に到達すると、Exhausted モードに入ります。 • 設定可能範囲：20 - 100（%）
Falling Threshold	CPU 使用率の下降しきい値を設定します。 CPU 使用率がこのしきい値を下回ると、セーフガードエンジン状態から Normal モードに戻ります。 • 設定可能範囲：20 - 100（%）

「Apply」をクリックして、設定内容を適用します。

CPU Protect Counters（CPU プロテクトカウンタ）

CPU プロテクションのカウンタ情報を表示、消去します。

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

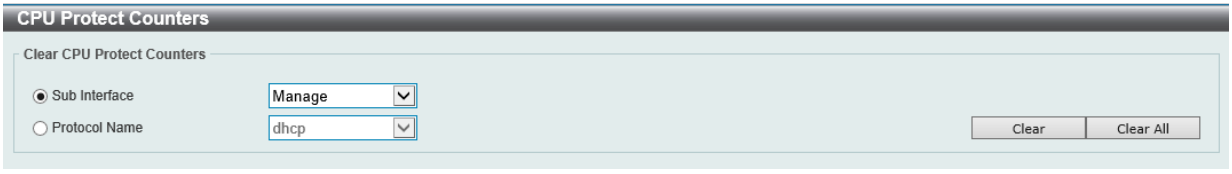


図 12-59　CPU Protect Counters 画面

画面に表示される項目：

項目	説明
Sub Interface	サブインタフェースのオプションを選択します。 指定したサブインタフェースの CPU プロテクトカウンタをクリアします。 • 選択肢：「Manage」「Protocol」「Route」「All」
Protocol Name	プロトコル名のオプションを選択します。

「Clear」をクリックして、設定に基づいた情報を消去します。
「Clear All」をクリックして、すべての情報を消去します。

CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）

CPU プロテクションのサブインタフェースを設定、表示します。

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

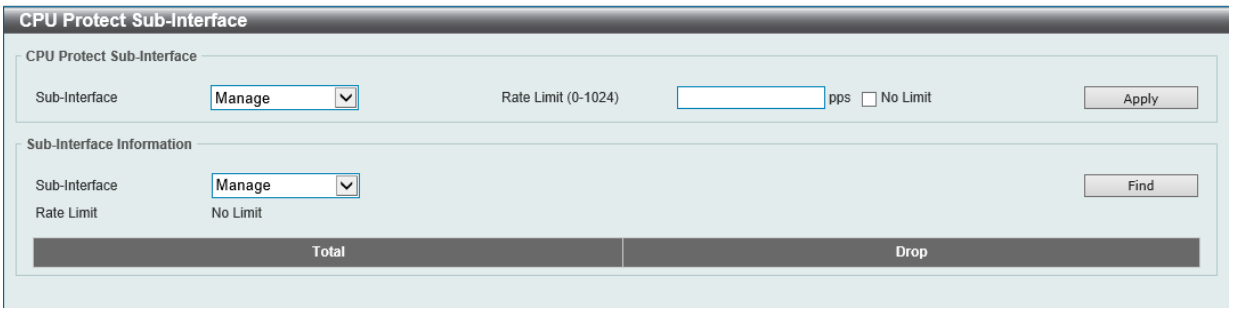


図 12-60　CPU Protect Sub-Interface 画面

画面に表示される項目：

項目	説明
CPU Protect Sub-Interface	
Sub-Interface	サブインタフェースのオプションを選択します。 • 選択肢：「Manage」「Protocol」「Route」
Rate Limit	レートリミットの値を入力します。「No Limit」を指定するとレートリミットを無効にします。 • 設定可能範囲：0-1024（パケット / 秒）
Sub-Interface Information	
Sub-Interface	サブインタフェースのオプションを選択します。 • 選択肢：「Manage」「Protocol」「Route」

「Apply」をクリックして、設定内容を適用します。
「Find」をクリックして、入力した情報を基に指定エントリを検出します。

CPU Protect Type（CPU プロテクトタイプ）

CPU プロテクションの種類を設定します。

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

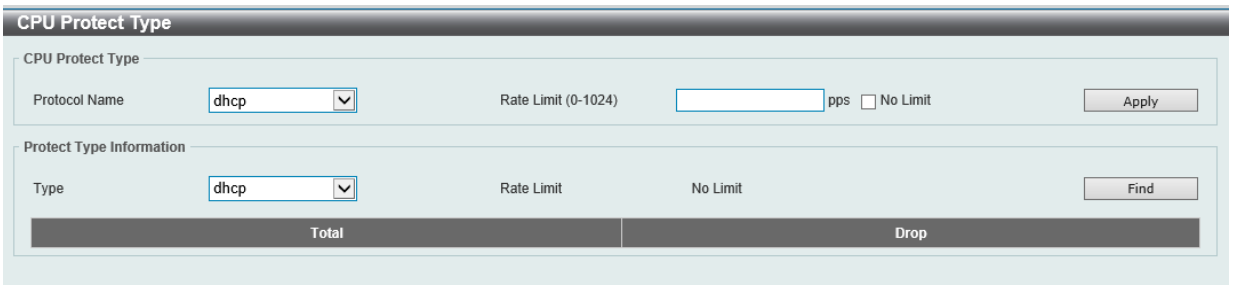


図 12-61　CPU Protect Type 画面

画面に表示される項目：

項目	説明
CPU Protect Type	
Protocol Name	プロトコル名のオプションを選択します。
Rate Limit	レートリミットの値を入力します。「No Limit」を指定するとレートリミットを無効にします。 • 設定可能範囲：0 - 1024（パケット / 秒）
Protect Type Information	
Type	プロトコルタイプを選択します。プロトコルタイプの選択後、レートリミットの値が表示されます。

「Apply」をクリックして、設定内容を適用します。
「Find」をクリックして、入力した情報を基に指定エントリを検出します。

Trusted Host（トラストホスト）

トラストホストの設定、表示を行います。

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

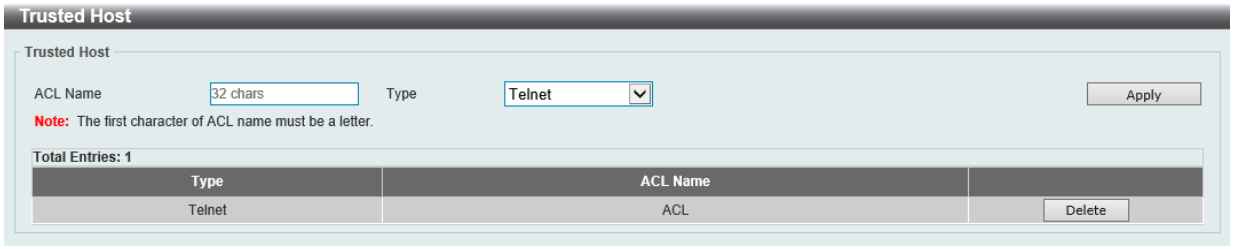


図 12-62　Trusted Host 画面

画面に表示される項目：

項目	説明
ACL Name	使用する ACL 名を入力します。（32 文字以内）
Type	トラストホストの種類を指定します。 • 選択肢：「Telnet」「SSH」「Ping」「HTTP」「HTTPS」

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

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

トラフィックセグメンテーションを設定します。トラフィックセグメンテーション転送ドメインが指定されると、ポートで受信するパケットは、レイヤ 2 パケット転送においてドメイン内のインタフェースに制限されます。ポートの転送ドメインが空の場合、ポートで受信したパケットのレイヤ 2 転送は制限されません。

トラフィックセグメンテーションのメンバリストは、同じ転送ドメインのポートとポートチャネルなど、異なるインタフェースタイプで構成できます。指定されたインタフェースにポートチャネルが含まれている場合、このポートチャネルのすべてのメンバポートが転送ドメインに含まれます。

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

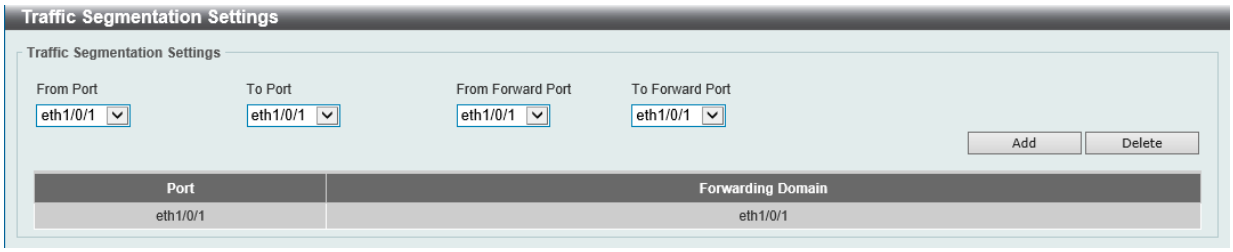


図 12-63　Traffic Segmentation Settings 画面

画面に表示される項目：

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

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

Storm Control Settings（ストームコントロール設定）

ストームコントロールの設定、表示を行います。

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

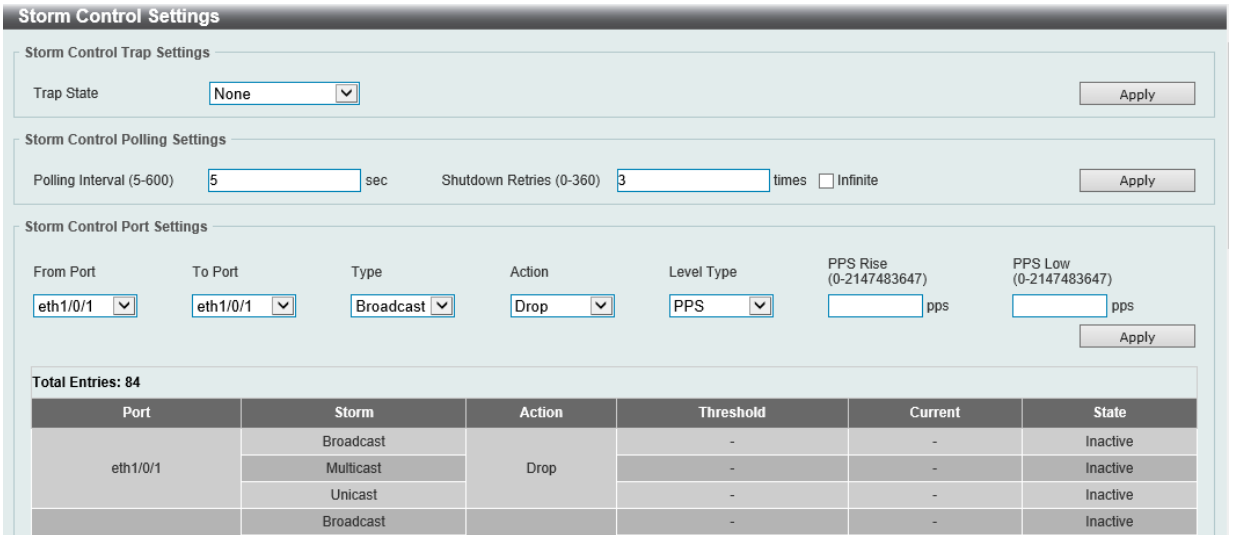


図 12-64　Storm Control Settings 画面

画面に表示される項目：

項目	説明
Storm Control Trap Settings	
Trap State	ストームコントロールトラップのオプションを指定します。 • 「None」- トラップは送信されません。 • 「Storm Occur」- ストームの発生を検出した時点でトラップが通知されます。 • 「Storm Clear」- ストームが解消された時点でトラップが通知されます。 • 「Both」- ストームの発生を検出、またはストームが解消された時点でトラップが通知されます。
Storm Control Polling Settings	
Polling Interval	ポーリング間隔の値を指定します。 • 設定可能範囲：5 - 600（秒） • 初期値：5（秒）
Shutdown Retries	シャットダウンの再試行回数を入力します。「Infinite」にチェックを入れると本機能は無効になります。 • 定可能範囲：0 - 360 • 初期値：3
Storm Control Port Settings	
From Port / To Port	設定するポートの範囲を指定します。
Type	コントロールするストームの種類を選択します。 • 選択肢：「Broadcast」「Multicast」「Unicast」 シャットダウンモードに設定されている場合、ユニキャストは「Known」「Unknown」両方を参照します。 つまり、既知または不明なユニキャストパケットが指定のしきい値に達すると、ポートはシャットダウンします。それ以外の設定では、ユニキャストは「Unknown」パケットのみを参照します。
Action	実行するアクションを指定します。 • 「None」- ストームパケットをフィルタしません。 • 「Shutdown」- 指定したしきい値に達するとポートはシャットダウンされます。 • 「Drop」- 指定したしきい値に達するとパケットは破棄されます。
Level Type	レベルタイプを指定します。 • 選択肢：「PPS」「Kbps」「Level」
PPS Rise	1 秒あたりのパケット量について上限しきい値を指定します。 • 設定可能範囲：0-2147483647（パケット / 秒）
PPS Low	秒あたりのパケット量について下限しきい値を指定します。 • 設定可能範囲：0-2147483647（パケット / 秒） • 初期値：PPS Rise 値の 80%

「Apply」をクリックして、設定内容を適用します。

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

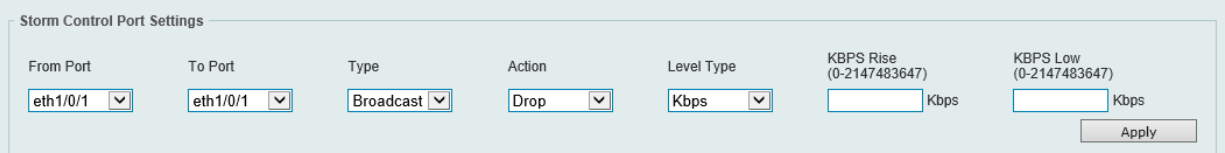


図 12-65　Storm Control（Kbps）画面

画面に表示される項目：

項目	説明
KBPS Rise	上限 KBPS の値を指定します。 ポートで受信するトラフィックの上限しきい値をキロビット / 秒で指定します。 • 設定可能範囲：0 - 2147483647（Kbps）
KBPS Low	下限 KBPS の値を指定します。 ポートで受信するトラフィックの下限しきい値をキロビット / 秒で指定します。 • 設定可能範囲：0 - 2147483647（Kbps） • 初期値：KBPS Rise 値の 80%

「Apply」をクリックして、設定内容を適用します。

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

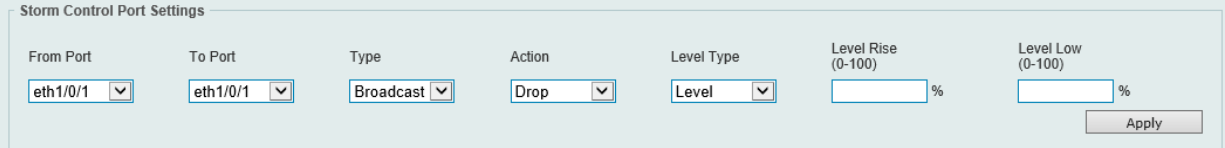


図 12-66　Storm Control（Level）画面

画面に表示される項目：

項目	説明
Level Rise	上限レベルを入力します。 ポートが受信するトラフィックの総帯域のパーセンテージを、上限しきい値として指定します。 • 設定可能範囲：0 - 100（%）
Level Low	下限レベルを入力します。 ポートが受信するトラフィックの総帯域のパーセンテージを、下限しきい値として指定します。 • 設定可能範囲：0 - 100（%） • 初期値：Level Rise 値の 80%

「Apply」をクリックして、設定内容を適用します。

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

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

各 DoS 攻撃に対して防御設定を行います。次のような既知の DoS 攻撃をスイッチで検出することができます。

- Land 攻撃：
  このタイプの攻撃には、送信元アドレスと宛先アドレスがターゲットデバイスのアドレスに設定されている IP パケットが使用されます。ターゲットデバイスが自身に対して継続的に応答してしまう可能性があります。
- Blat 攻撃：
  このタイプの攻撃は、ターゲットデバイスの宛先ポートと同じ TCP / UDP ソースポートでパケットを送信します。ターゲットデバイスが自身に対して応答してしまう可能性があります。
- TCP-Null：
  このタイプの攻撃には、シーケンス番号 0 でフラグを持たない特定のパケットを使用したポートスキャンが使用されます。
- TCP-Xmas：
  このタイプの攻撃には、シーケンス番号 0 で緊急（URG）、プッシュ（PSH）、および FIN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- TCP SYN-FIN：
  このタイプの攻撃には、SYN および FIN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- TCP SYN SrcPort Less 1024：
  このタイプの攻撃には、送信元ポート 0 ～ 1023 と SYN フラグを含む特定のパケットを使用したポートスキャンが使用されます。
- Ping of Death 攻撃：
  Ping of Death 攻撃は、コンピュータに対する攻撃の一種で、不正な形式の Ping または悪意のある Ping をコンピュータに送信します。 Ping のサイズは通常 64 バイトです（多くのコンピュータは、最大 IP パケットサイズである 65535 バイトより大きい Ping を処理できません）。このサイズの ping を送信すると、ターゲットコンピュータがクラッシュする可能性があります。従来、このバグは比較的簡単に悪用されていました。一般に、65536 バイトの Ping パケットを送信することはネットワークプロトコルの規定に違反しますが、断片化されている場合、このサイズのパケットが送信できてしまいます。ターゲットコンピュータがパケットを再構成すると、バッファオーバーフローが発生する可能性があり、システムクラッシュを引き起こすことがあります。
- TCP Tiny Fragment 攻撃：
  Tiny TCP Fragment 攻撃者は、IP フラグメンテーションを使用して非常に小さなフラグメントを作成し、TCP ヘッダ情報をパケットフラグメントに分割してルータのチェック機能を通過させ、攻撃を実行します。
- すべてのタイプ：
  上記のすべてのタイプ

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

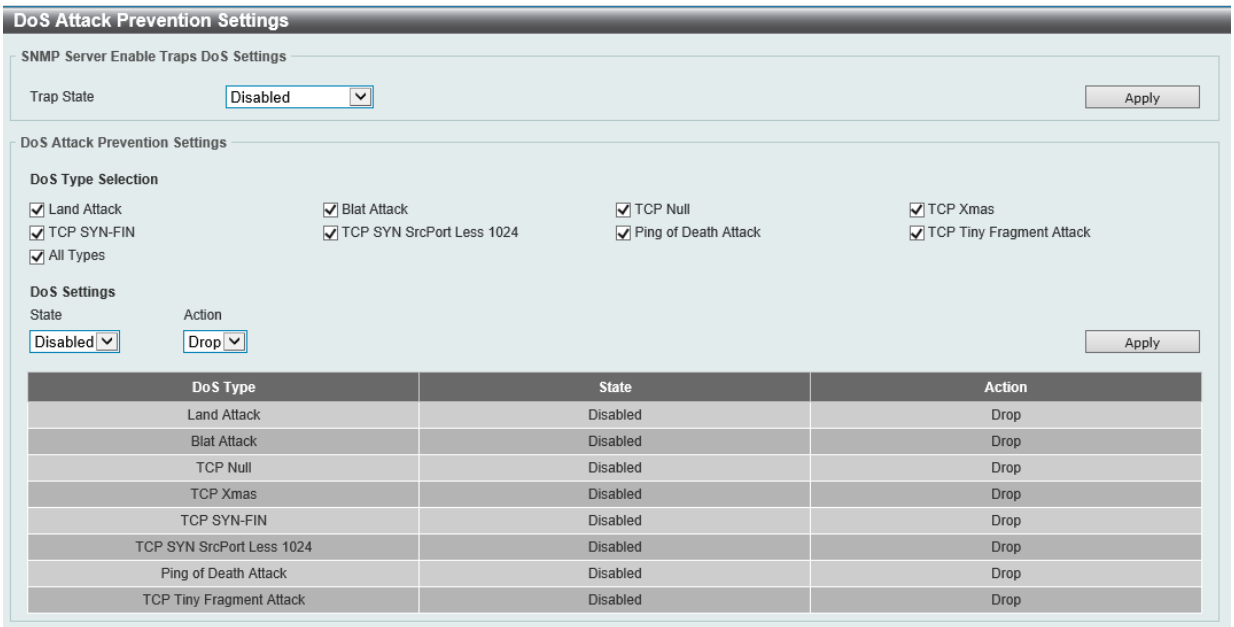


図 12-67　DoS Attack Prevention Settings 画面

画面に表示される項目：

項目	説明
SNMP Server Enable Traps DoS Settings	
Trap State	DoS 攻撃防止のトラップ状態を有効 / 無効に設定します。
DoS Attack Prevention Settings	
DoS Type Selection	適切な DoS 攻撃防御のタイプを選択します。
State	DoS 攻撃防止の状態を有効 / 無効に指定します。
Action	DoS 攻撃を検出したときに実行されるアクションを指定します。 ・「Drop」- 一致する DoS 攻撃パケットをすべて破棄します。

「Apply」をクリックして、設定内容を適用します。

SSH（Secure Shell の設定）

SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。SSH は、リモートのホストコンピュータへの安全なログインや、リモートのエンドノードでの安全なコマンド実行メソッドを可能にし、信頼関係を結んでいないホスト間に暗号化と認証を利用した安全な通信を提供します。高度なセキュリティ機能を備えた SSH は、今日のネットワーク環境に必要不可欠なツールです。ネットワーク通信を脅かす数々のセキュリティハザードに対して、強力な監視者としての役割を担います。

リモート PC（SSH クライアント）とスイッチ（SSH サーバ）間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

1. User Accounts Settings 画面で管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
2. SSH User Settings 画面の「Authentication Method」で使用して、ユーザアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「Host Based」、「Password」、「Public Key」の 3 つがあります。
3. Host Key 画面で、SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。
4. 最後に SSH Global Settings 画面で、SSH を有効にします。

これらの手順が完了後、安全な帯域内の接続でスイッチの管理を行うために、リモート PC 上の SSH クライアントの設定を行います。

SSH Global Settings（SSH グローバル設定）

SSH グローバル設定および設定内容の確認に使用します。

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

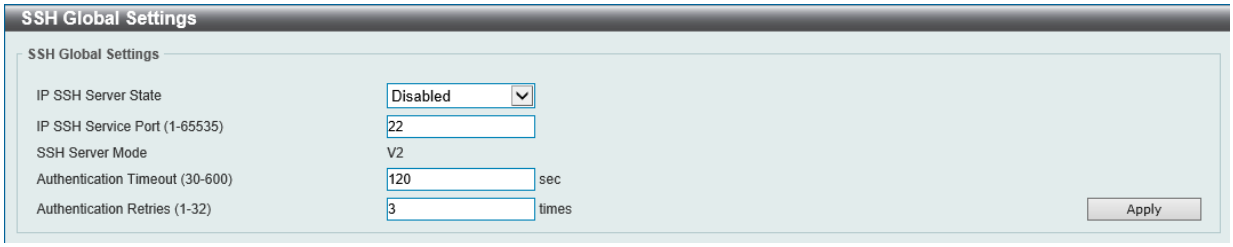


図 12-68　SSH Global Settings 画面

画面に表示される項目：

項目	説明
IP SSH Server State	グローバルに SSH 機能を有効 / 無効にします。
IP SSH Service Port	SSH サービスポート番号を設定します。 • 設定可能範囲：1-65535 • 初期値：22
Authentication Timeout	認証のタイムアウト時間を指定します。 • 設定可能範囲：30 - 600（秒） • 初期値：120（秒）
Authentication Retries	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。 指定した回数を超えるとスイッチは接続を切り、ユーザは再度スイッチに接続する必要があります。 • 設定可能範囲：1 - 32 • 初期値：3

「Apply」をクリックして、設定内容を適用します。

Host Key（Host Key 設定）

SSH ホスト鍵の設定を行います。

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

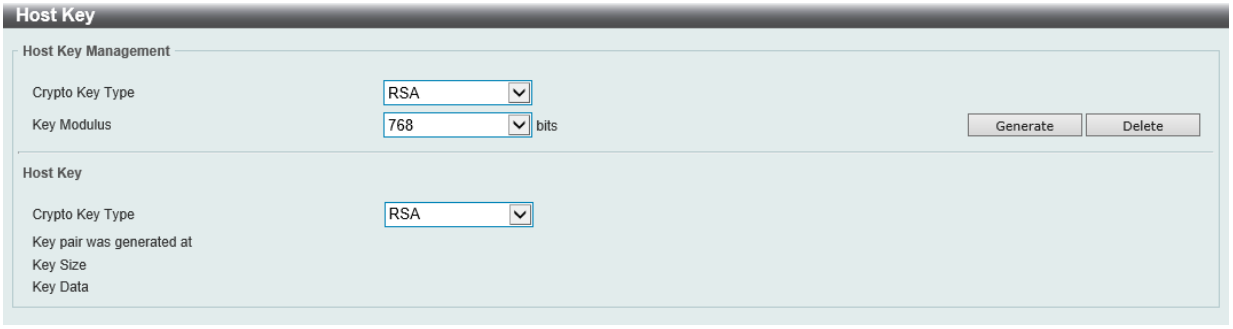


図 12-69　Host Key 画面

画面に表示される項目：

項目	説明
Host Key Management	
Crypto Key Type	暗号鍵の種類を選択します。 • 「Rivest Shamir Adleman（RSA）」「Digital Signature Algorithm（DSA）」
Key Modulus	鍵係数の値を入力します。 • 選択肢：「360」「512」「768」「1024」「2048」（ビット）
Host Key	
Crypto Key Type	暗号鍵の種類を選択します。 • 「Rivest Shamir Adleman（RSA）」「Digital Signature Algorithm（DSA）」

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

「Generate」をクリックすると鍵の生成が開始されます。
鍵の生成が完了すると次の画面が表示されます。

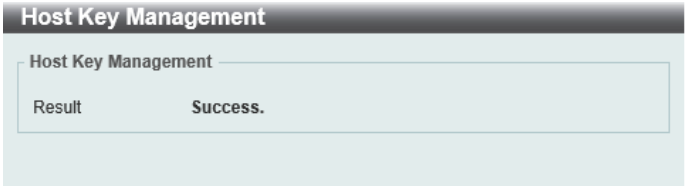


図 12-70　Host Key (Success) 画面

SSH Server Connection（SSH サーバ接続）

SSH サーバ接続テーブルの内容を確認します。

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

図 12-71　SSH Server Connection 画面

表示されるエントリの内容を確認します。

SSH User Settings（SSH ユーザ設定）

SSH ユーザの設定を行います。

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

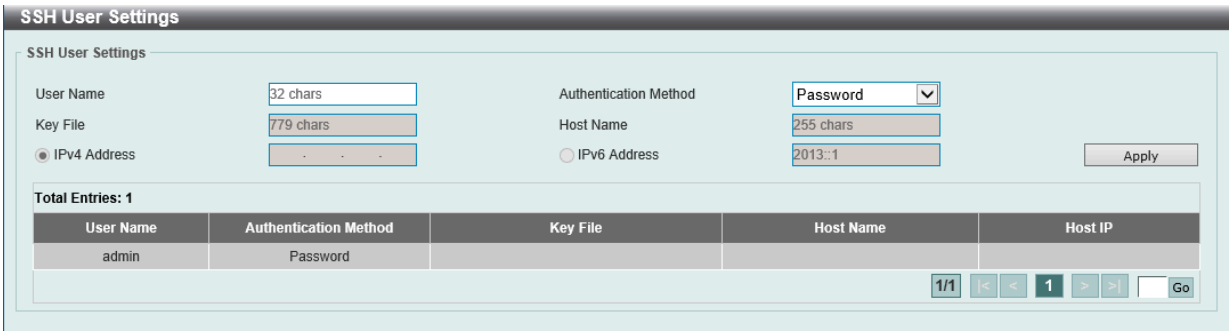


図 12-72　SSH User Settings 画面

画面に表示される項目：

項目	説明
User Name	SSH ユーザを識別するユーザ名を指定します。（32 文字以内）
Authentication Method	スイッチにアクセスを試みるユーザの認証モードを指定します。 • 選択肢：「Password」「Public Key」「Host-based」
Key File	「Public Key」または「Host-based」を選択した場合、公開鍵を入力します。
Host Name	「Host-based」を選択した場合、ホスト名を入力します。
IPv4 Address	「Host-based」を選択した場合、IPv4 アドレスを入力します。
IPv6 Address	「Host-based」を選択した場合、IPv6 アドレスを入力します。

「Apply」をクリックして、設定内容を適用します。

SSL（Secure Socket Layer）

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

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

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

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

これら 3 つのパラメータは、スイッチ上での 11 個の選択肢として独自に組み合わされ、サーバとクライアント間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。また、本スイッチは、TLSv1.0/1.1/1.2 をサポートしています。それ以外のバージョンは本スイッチとは互換性がない恐れがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する可能性があります。

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

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

SSL Global Settings（SSL グローバル設定）

SSL グローバル設定を行います。

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

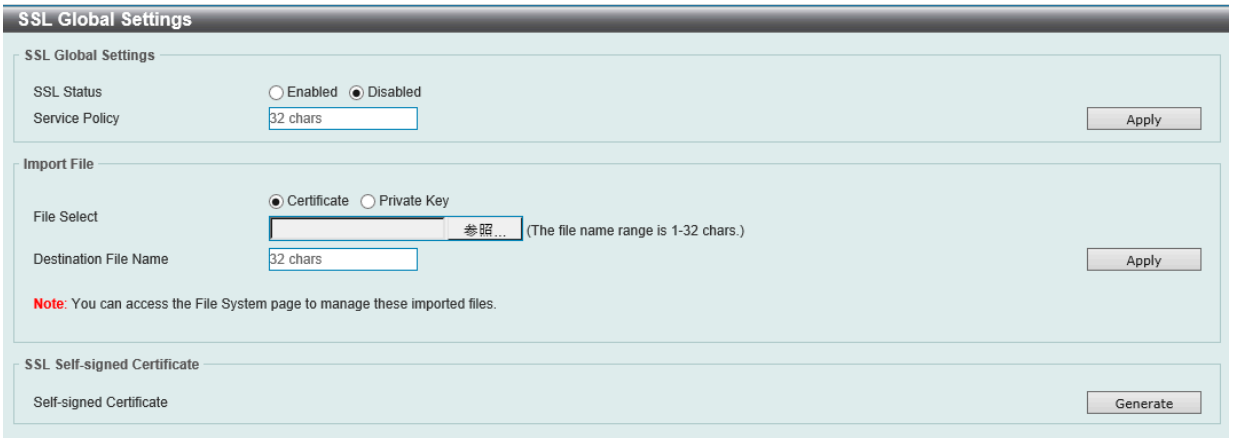


図 12-73　SSL Global Settings 画面

画面に表示される項目：

項目	説明
SSL Global Settings	
SSL Status	SSL のグローバルステータスを有効 / 無効に設定します。
Service Policy	SSL ポリシー名を入力します。（32 文字以内）
Import File	
File Select	ロードされるファイル種類を選択します。 • 選択肢：「Certificate」「Private Key」 ファイル種類を選択した後、「Browse/ 参照」ボタンをクリックし、適切なファイルを選択してローカルコンピュータからロードします。
Destination File Name	宛先ファイル名を指定します。（32 文字以内）
SSL Self-signed Certificate	
Self-signed Certificate	「Generate」を選択すると、組み込みの自己署名証明書の有無に関係なく、新しい自己署名証明書が生成されます。生成された証明書は、ユーザが所有する証明書には影響しません。

「Apply」をクリックして、設定内容を適用します。

注意　SSL 自己署名証明書は、キー長が 2048 ビットの自己署名 RSA 証明書のみをサポートします。

注意　SSL を有効にする場合は、「Service Policy」を適切に設定した後に、「SSL Status」を「Enabled」にしてください。

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

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て、以下の画面を表示します。

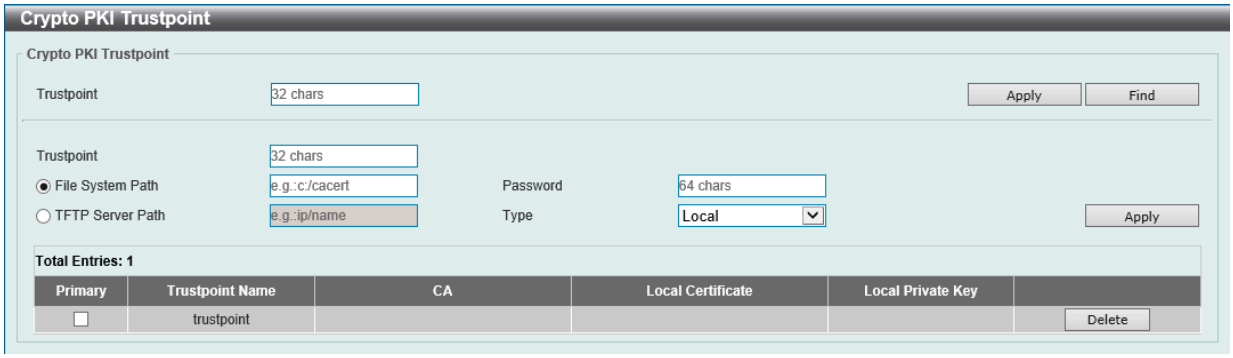


図 12-74　Crypto PKI Trustpoint 画面

画面に表示される項目：

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

「Apply」をクリックして、設定内容を適用します。
「Find」をクリックして、入力した情報に基づいて指定エントリを検出します。
「Delete」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て、以下の画面を表示します。

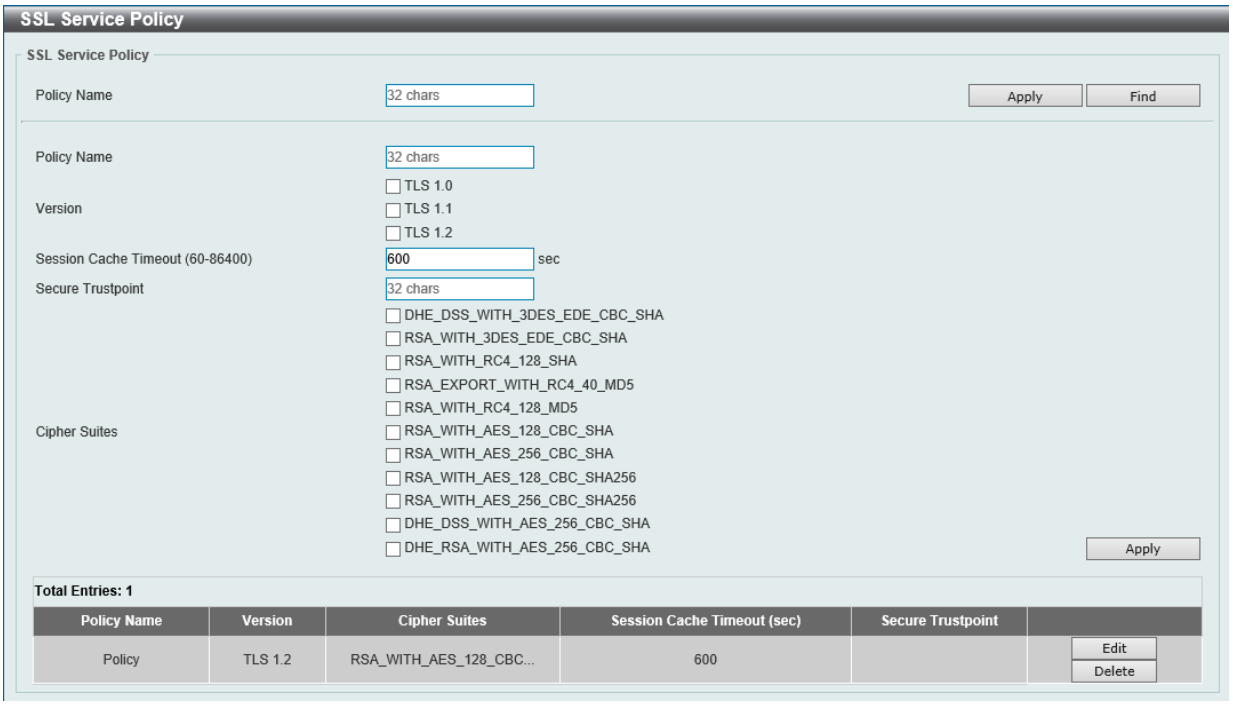


図 12-75　SSL Service Policy 画面

画面に表示される項目：

項目	説明
Policy Name	SSL サービスポリシー名を入力します。（32 文字以内）
Version	「Transport Layer Security」(TLS) のバージョンを指定します。 • 選択肢：「TLS 1.0」「TLS 1.1」「TLS 1.2」
Session Cache Timeout	セッションキャッシュタイムアウトの時間を指定します。 • 設定可能範囲：60-86400（秒） • 初期値：600（秒）
Secure Trustpoint	セキュアなトラストポイントの名前を入力します。（32 文字以内）
Cipher Suites	本プロファイルの暗号スイートを選択します。

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

Network Protocol Port Protection Settings（ネットワークプロトコルポート保護設定）

ネットワークプロトコルポート保護の設定を行います。

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

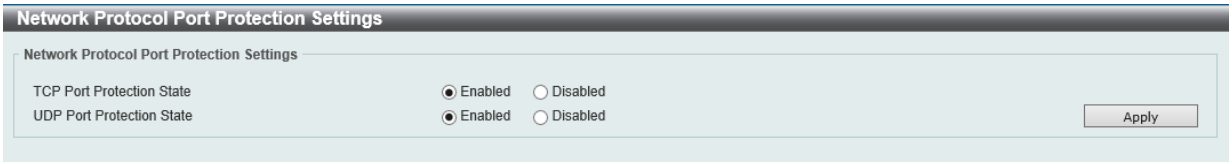


図 12-76　Network Protocol Port Protection Settings 画面

画面に表示される項目：

項目	説明
TCP Port Protect State	TCP ポート保護ステータスを有効 / 無効に指定します。
UDP Port Protect State	UDP ポート保護ステータスを有効 / 無効に指定します。

「Apply」をクリックして、設定内容を適用します。

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

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

サブメニュー	説明
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。

Cable Diagnostics（ケーブル診断機能）

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は UTP ケーブルを簡易的に確認するために設計されています。ケーブルの品質やエラーの種類を診断します。

注意　ケーブル診断機能は簡易機能であり、参考としてご利用ください。正確な検査やテストのためには専用のテスタを使用して行ってください。

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

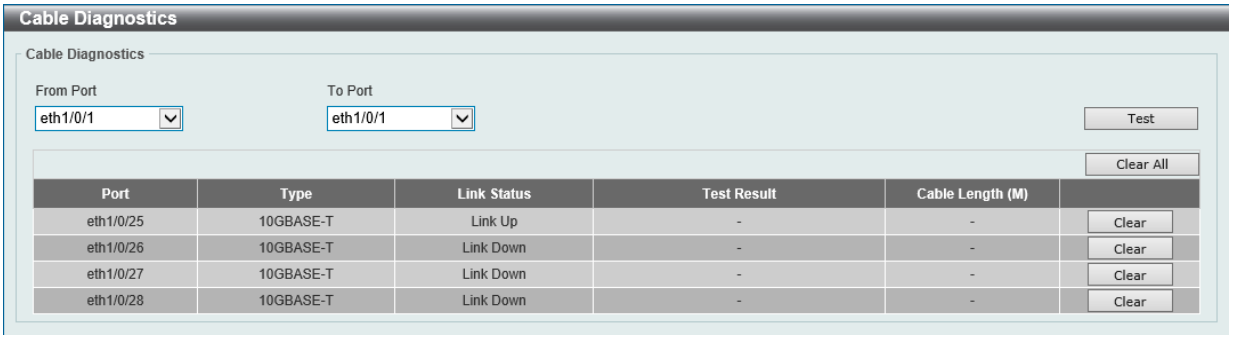


図 13-1　Cable Diagnostics 画面

■ ケーブル診断の手順

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

■ 情報の消去

「Clear」をクリックし、指定ポートの情報を消去します。
「Clear All」をクリックし、テーブル上のすべての情報を消去します。

■ ケーブル診断機能の制限

- GE ポートのみサポート
- 最大対応ケーブル長 120 メートル
- ケーブル長の誤差± 5 メートル
- より正確な結果を得るには、RJ-45 コネクタで TIA/EIA-568B ピンアサインを使用

■ 障害メッセージ

- Open - エラーペアのケーブルが指定された位置に接続されていません。
- Short - エラーペアのケーブルは、指定された位置でショート（短絡）しています。
- Open or Short - ケーブルにオープン（断線）またはショート（短絡）の問題がありますが、PHY にはそれらを区別する機能がありません。
- Crosstalk - エラーペアのケーブルに、指定された位置でクロストークの問題があります。
- Shutdown - リモートパートナーの電源がオフです。
- Unknown - テストのステータスが不明です。
- No cable - ポートには、リモートパートナーへのケーブル接続がありません。

第 14 章　Monitoring（スイッチのモニタリング）

Monitoring メニューを使用し、本スイッチのポート使用率、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
Utilization（利用分析）	ポートの帯域使用率を表示します。
Statistics（統計情報）	パケット統計情報とエラー統計情報を表示します。
Mirror Settings（ミラー設定）	ポートミラーリングの設定を行います。
Device Environment（機器環境確認）	機器環境の表示を行います。

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。

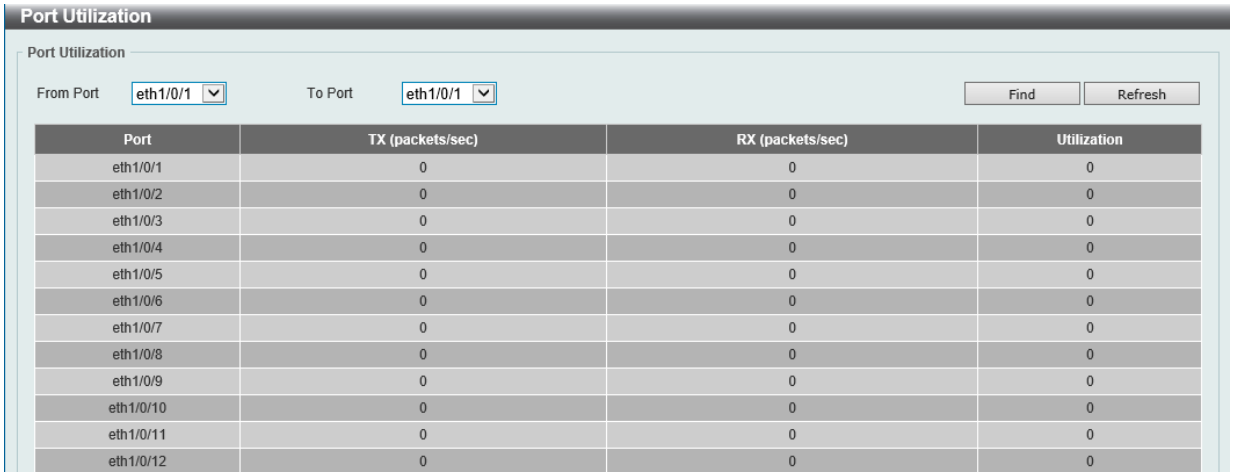


図 14-1　Port Utilization 画面

画面に表示される項目：

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

「Find」をクリックし、入力した情報を基に指定のエントリを検出します。
「Refresh」をクリックし、テーブルを更新します。

Statistics（統計情報）

スイッチの統計情報を表示します。

Port（ポート統計情報）

ポート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。

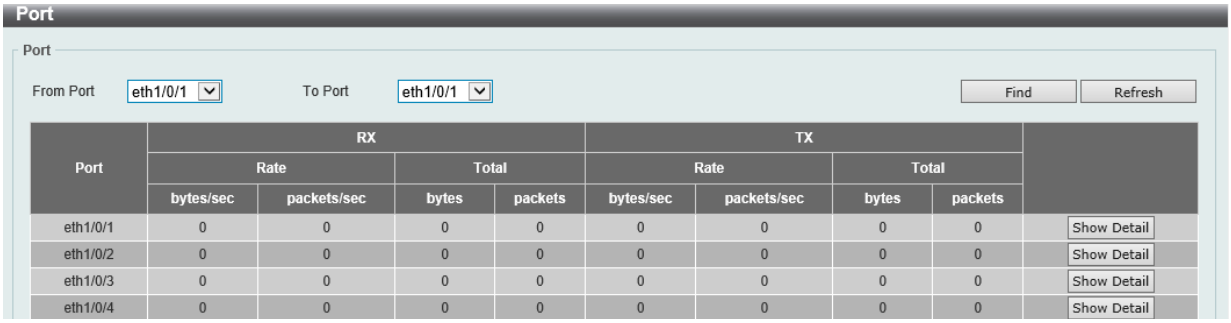


図 14-2　Port 画面

画面に表示される項目：

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

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

「Show Detail」をクリックすると以下の画面が表示されます。

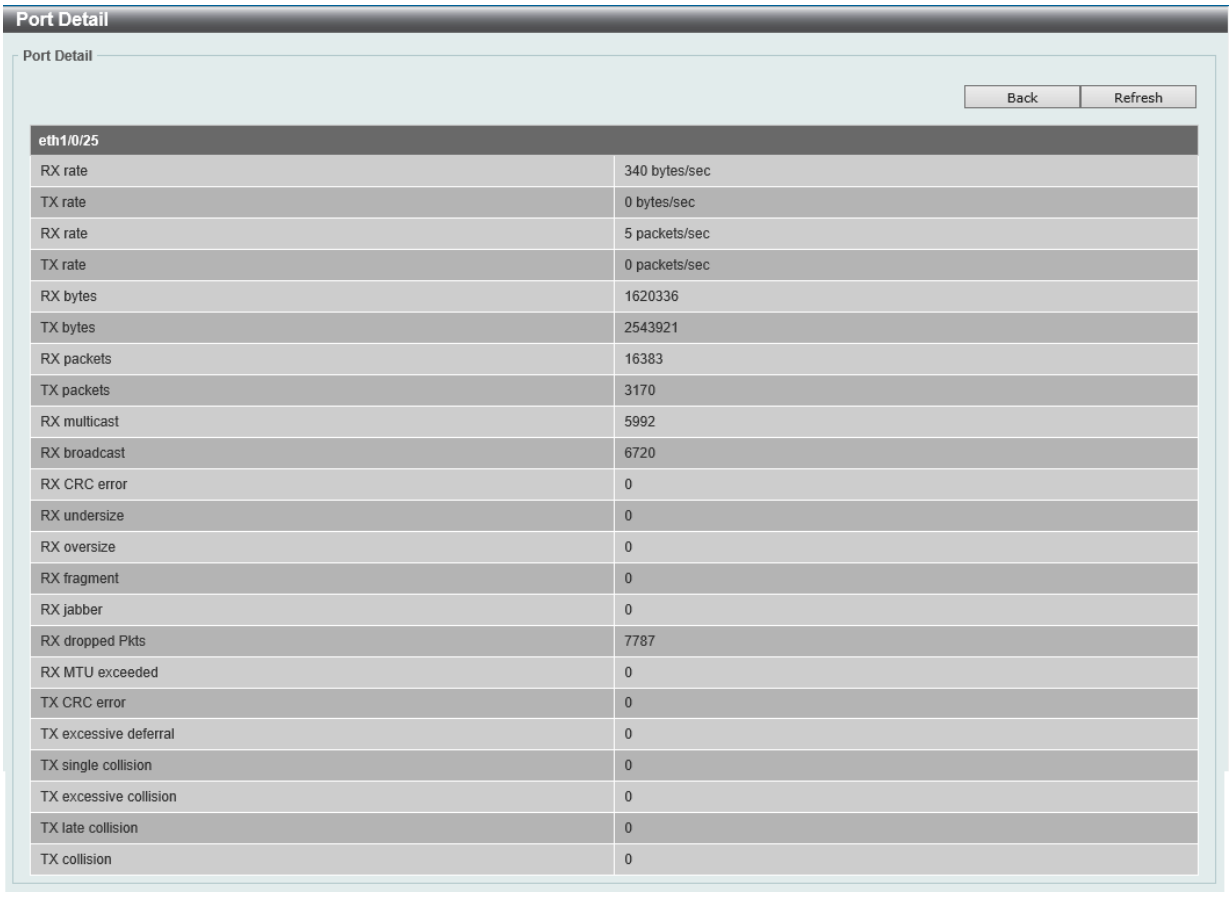


図 14-3　Port Detail 画面

「Refresh」をクリックし、テーブルを更新します。
「Back」をクリックし、前の画面に戻ります。

Interface Counters（インタフェースカウンタ）

インタフェースカウンタ情報について表示します。

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

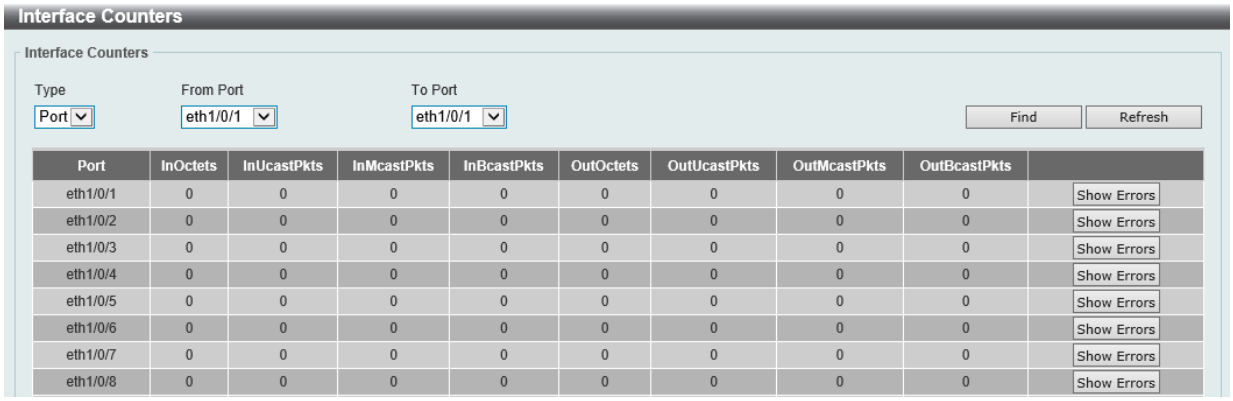


図 14-4　Interface Counters 画面

画面に表示される項目：

項目	説明
Type	表示する情報のタイプを選択します。「Port」のみ選択可能です。
From Port / To Port	表示するポート範囲を指定します。

「Find」をクリックし、入力した情報を基に指定のエントリを検出します。
「Refresh」をクリックし、テーブルを更新します。

「Show Errors」をクリックし、指定ポートのエラー情報について表示します。

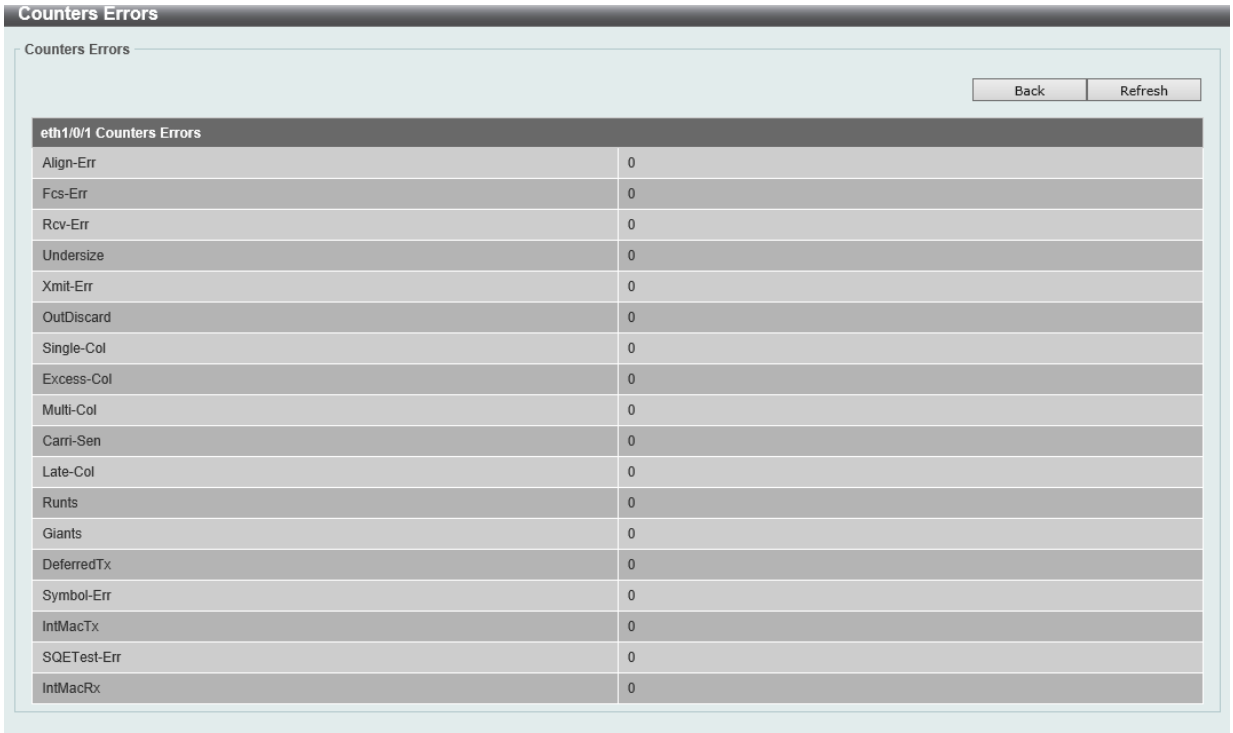


図 14-5　Counters Errors 画面

「Refresh」をクリックし、テーブルを更新します。
「Back」をクリックし、前の画面に戻ります。

Counters（カウンタ）

すべてのポートのカウンタ情報を表示、消去します。

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

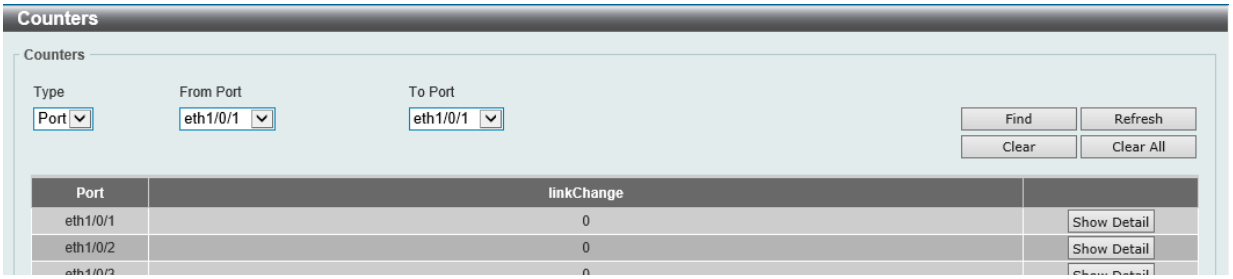


図 14-6　Counters 画面

画面に表示される項目：

項目	説明
Type	タイプに「Port」を選択します。
From Port / To Port	表示するポートの範囲を指定します。

「Find」をクリックし、入力した情報を基に指定のエントリを検出します。
「Refresh」をクリックし、テーブルを更新します。
「Clear」をクリックし、指定ポートの情報を消去します。
「Clear All」をクリックし、テーブル上のすべての情報を消去します。

詳細を表示

「Show Detail」をクリックし、指定ポートの詳細情報について表示します。

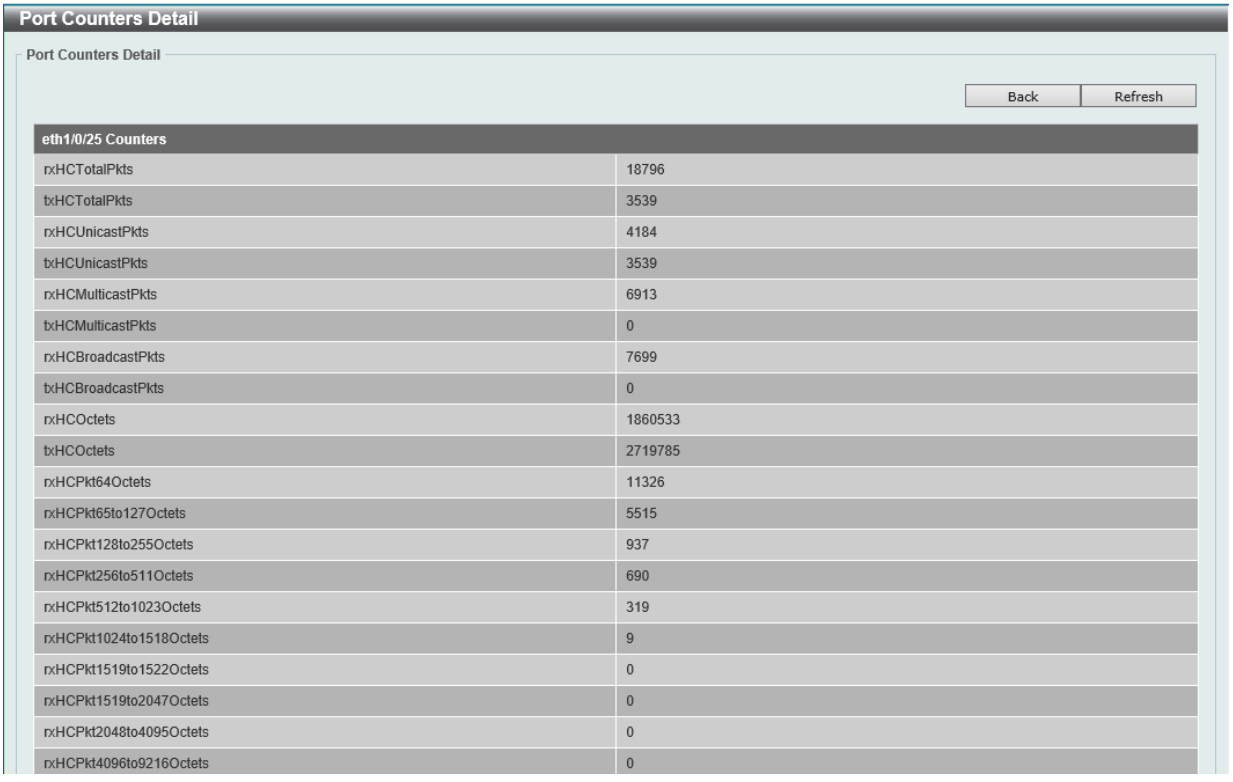


図 14-7　Port Counters Detail 画面

「Refresh」をクリックし、テーブルを更新します。
「Back」をクリックし、前の画面に戻ります。

Mirror Settings（ミラー設定）

ミラーリング機能についての設定、表示を行います。
本スイッチは、対象ポートで送受信するフレームをコピーして、そのコピーしたフレームの出力先を他のポートに変更する機能（ポートミラーリング）を持っています。ミラーリングポートに監視機器（スニファや RMON probe など）を接続し、最初のポートを通したパケットの詳細を確認することができます。トラブルシューティングやネットワーク監視の目的に適しています。

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

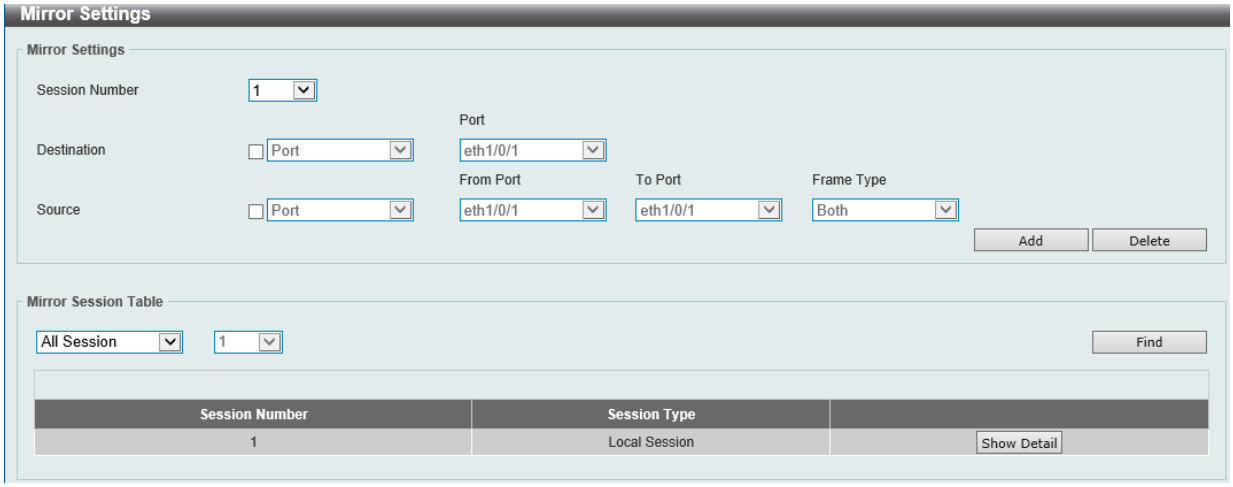


図 14-8　Mirror Settings 画面

画面に表示される項目：

項目	説明
Mirror Settings	
Session Number	このエントリのセッション番号を指定します。 • 設定可能範囲：1-4
Destination	チェックボックスを選択して、ポートミラーエントリの宛先を設定します。 宛先タイプオプションとして「Port」を選択します。 「Port」を選択した後にポート番号を指定します。
Source	チェックボックスを選択して、このポートミラーエントリの送信元を設定します。 • 送信元タイプオプションとして「Port」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「Both」（両方）、「RX」（受信データ）、「TX」（送信データ）から指定します。
Mirror Session Table	
該当エントリのセッション番号を指定します。ドロップダウンメニューから表示される情報のミラーセッションタイプを選択します。 • 「All Session」- テーブル内のすべてのミラーセッションを表示します。 • 「Session Number」- 指定したミラーセッションのみをテーブルします。ミラーセッション番号（1-4）を選択します。	

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

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

「Show Detail」をクリックし、以下の画面を表示します。

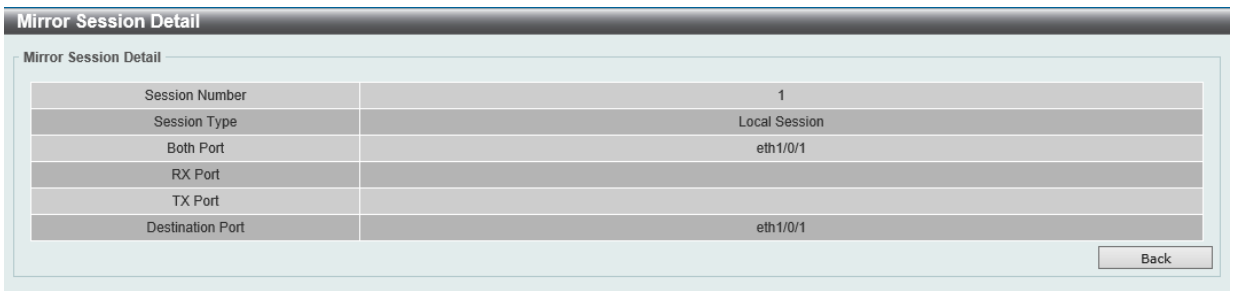


図 14-9　Mirror Settings - Show Detail 画面

「Back」をクリックし、以下の画面を表示します。

Device Environment（機器環境確認）

本画面ではスイッチの内部温度状態を表示します。

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

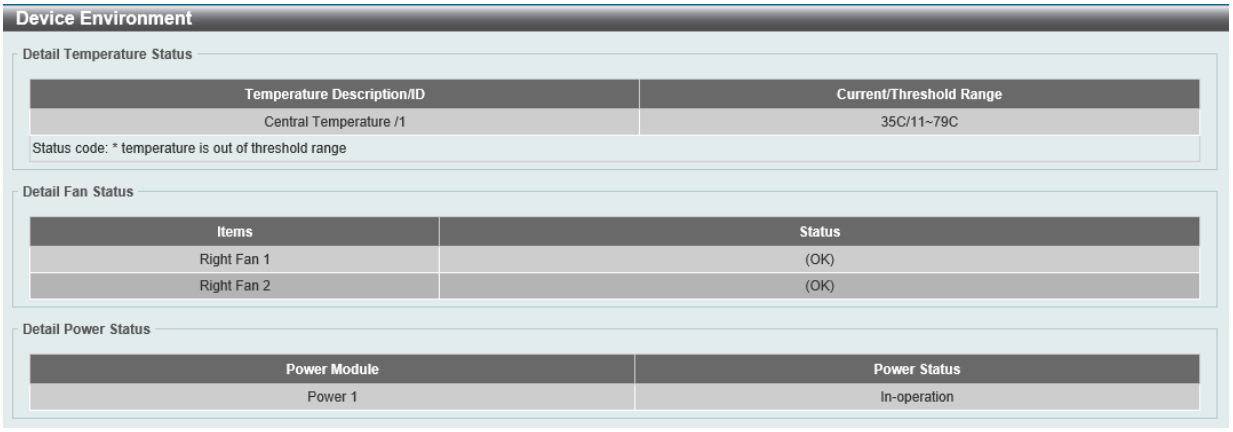


図 14-10　Device Environment 画面

第 15 章　Green（省電力テクノロジー）

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

サブメニュー	説明
Power Saving（省電力）	スイッチの省電力設定を行います。
EEE（Energy Efficient Ethernet/ 省電力イーサネット）	Energy Efficient Ethernet/ 省電力イーサネットの設定を行います。

Power Saving（省電力）

スイッチの省電力機能を設定、表示します。

Green > Power Saving メニューをクリックし、以下の画面を表示します。

■ Power Saving Global Settings タブ

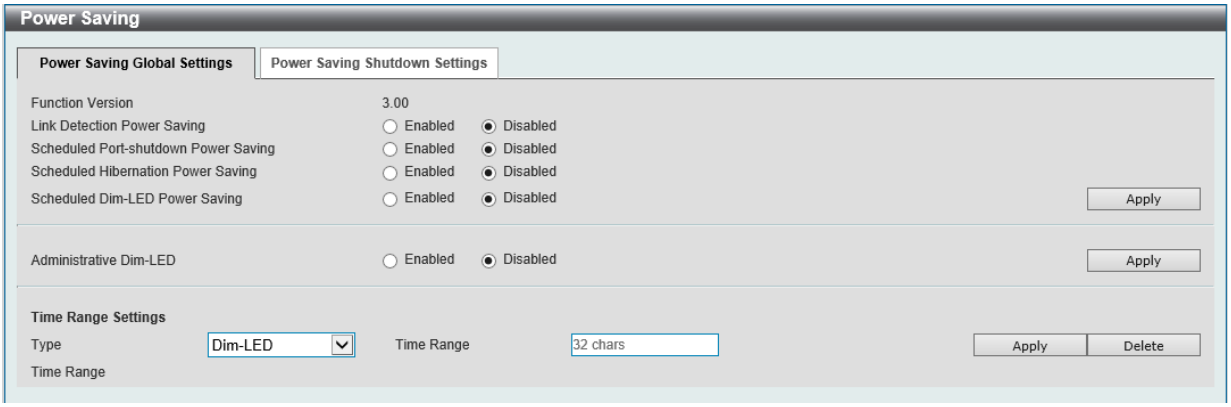


図 15-1　Power Saving - Power Saving Global Settings タブ画面

画面に表示される項目：

項目	説明
Link Detection Power Saving	「リンク検出」を有効 / 無効に設定します。 本設定を有効にすると、リンクダウンしているポートへの電力供給が停止し、スイッチの消費電力を抑えます。リンクアップしているポートへの影響はありません。
Scheduled Port-shutdown Power Saving	スケジュールによるポートシャットダウン機能を有効 / 無効に設定します。
Scheduled Hibernation Power Saving	スケジュールによるシステムスリープ機能を有効 / 無効に設定します。
Scheduled Dim-LED Power Saving	スケジュールによる減光 LED の有効 / 無効を指定します。
Administrative Dim-LED	ポート LED 機能の有効 / 無効を指定します。
Time Range Settings	
Type	省電力モードの種類を指定します。 • 選択肢：「Dim-LED」
Time Range	上記省電力機能に適用するスケジュールを指定します。

「Apply」をクリックし、設定を適用します。
「Delete」をクリックし指定のエントリを削除します。

■ Power Saving Shutdown Settings タブ

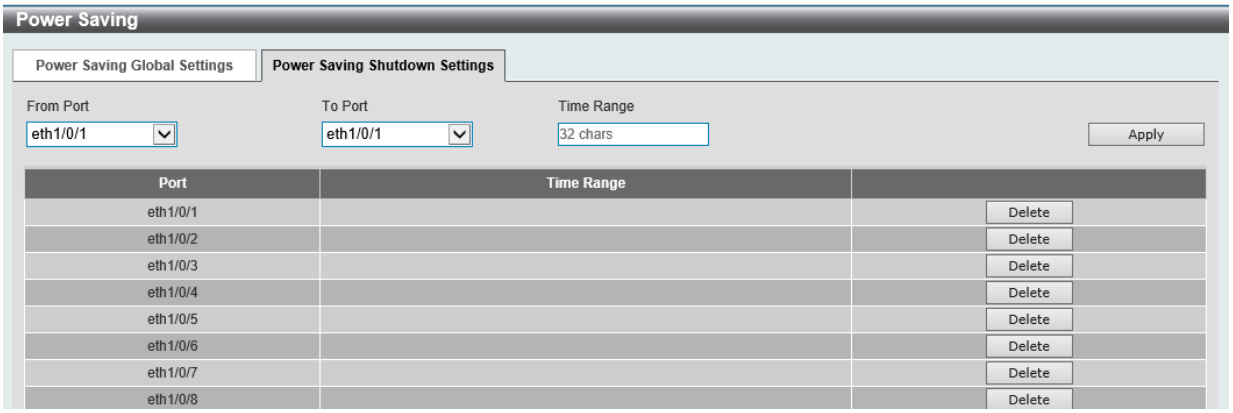


図 15-2　Power Saving - Power Saving Shutdown Settings タブ画面

画面に表示される項目：

項目	説明
From Port / To Port	設定するポートの範囲を指定します。
Time Range	ポートに適用するスケジュール名を指定します。

「Apply」をクリックして、設定内容を適用します。画面は自動的に更新されます。
「Delete」をクリックして、指定のエントリを削除します。

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

「Energy Efficient Ethernet」(EEE/ 省電力イーサネット) は「IEEE 802.3az」によって定義されています。
リンク上でパケットの送受信が発生していない場合、電力消費を抑えることができます。

Green > EEE の順にクリックし、以下の設定画面を表示します。

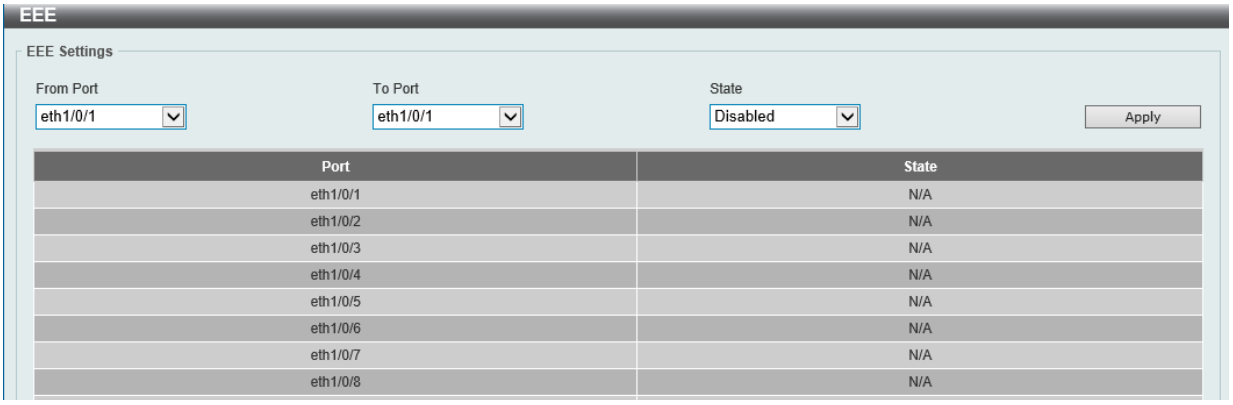


図 15-3　EEE 画面

画面に表示される項目：

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

「Apply」をクリックし、設定を適用します。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 16 章　Toolbar（ツールバー）

Web インタフェース画面上部のツールバーにある「Save」「Tools」「Wizard」「Online Help」「Logout」メニューを使用してスイッチの管理・設定を行います。

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

メニュー	サブメニュー	説明
Save（保存）	—	コンフィグレーションをスイッチに保存します。
Tools（ツール）	Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）	ファームウェアのアップグレードとバックアップを行います。
	Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）	コンフィグレーションのリストアとバックアップを行います。
	Certificate & Key Restore & Backup（証明書と鍵のリストア＆バックアップ）	証明書とキーのリストアとバックアップを行います。
	Log Backup（ログのバックアップ）	ログファイルのバックアップをします。
	Ping	Ping を実行します。
	Language Management（言語管理）	言語設定を行います。
	Reboot System（システム再起動）	システムの再起動を行います。
Wizard（ウィザード）	—	スマートウィザードを開始します。
Online Help（オンラインヘルプ）	D-Link Support Site（D-Link サポート Web サイト（英語））	D-Link サポートサイト（英語版）を表示します
	User Guide（ユーザガイド（英語版））	ユーザガイド（英語版）を表示します。
Surveillance Mode（サーベイランスモードへの変更）	—	スタンダードモードからサーベイランスモードに移行します。
Logout（ログアウト）	—	ログアウトします。

図 16-1　Toolbar

Save（保存）

現在のコンフィグレーションを保存します。

Save Configuration（コンフィグレーションの保存）

Save > Save Configuration をクリックし、以下の画面を表示します。

コンフィグレーションの保存

現在実行中のコンフィグレーションをブートコンフィグとしてスイッチに保存します。
電源が落ちた場合にコンフィグレーションが失われることを防ぎます。

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、「Apply」をクリックします。

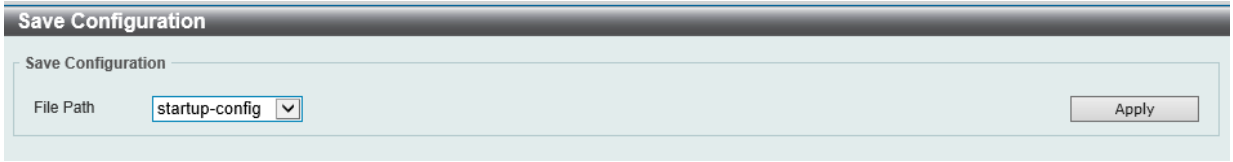


図 16-2　Save Configuration 画面

画面に表示される項目：

項目	説明
File Path	保存先を指定します。 • 選択肢：「startup-config」「Configuration 1」「Configuration 2」

「Apply」をクリックしてコンフィグレーションを保存します。

Tools（ツール）

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

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

HTTP を使用してローカル PC からファームウェアアップグレードを実行します。

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

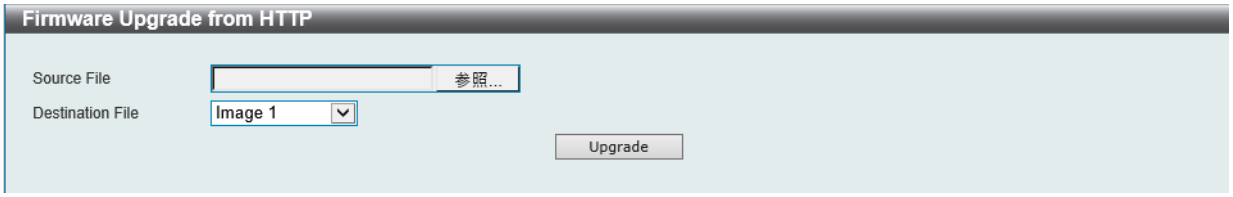


図 16-3　Firmware Upgrade from HTTP 画面

画面に表示される項目：

項目	説明
Source File	「Browse/ 参照」をクリックしてローカル PC 上のファームウェアファイルの場所を指定します。
Destination File	ファームウェアが保存されるスイッチの宛先を指定します。 • 選択肢：「Image 1」「Image 2」

「Upgrade」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 サーバを使用してファームウェアアップグレードを実行します。

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

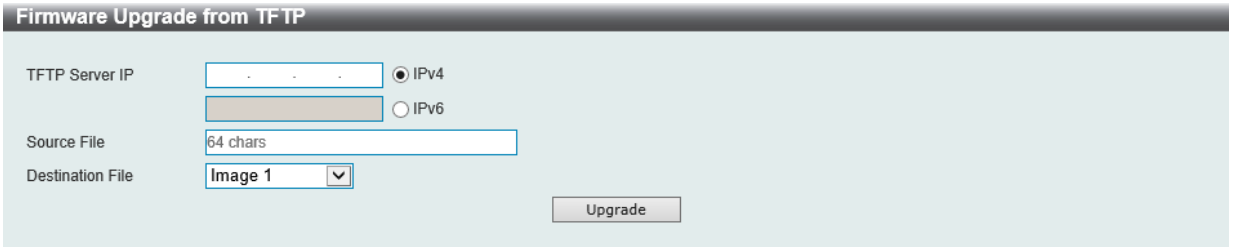


図 16-4　Firmware Upgrade from TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内）
Destination File	ファームウェアが保存されるスイッチの宛先を指定します。 • 選択肢：「Image 1」「Image 2」

「Upgrade」をクリックしてアップグレードを開始します。

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

HTTP を使用して、ローカル PC へファームウェアのバックアップを行います。

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

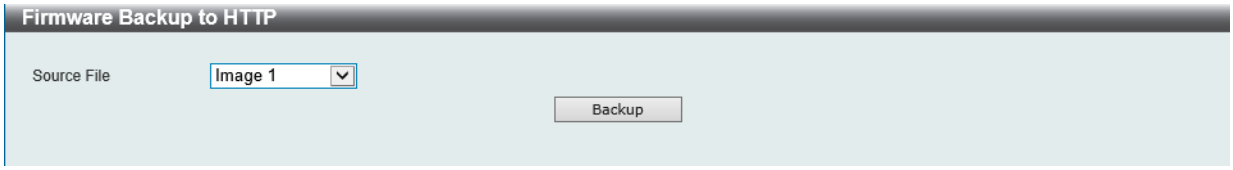


図 16-5　Firmware Backup to HTTP 画面

画面に表示される項目：

項目	説明
Source File	ローカル PC にバックアップするファームウェアを選択します。 • 選択肢：「Image 1」「Image 2」

「Backup」をクリックしてバックアップを開始します。

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

TFTP サーバにファームウェアバックアップを行います。

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

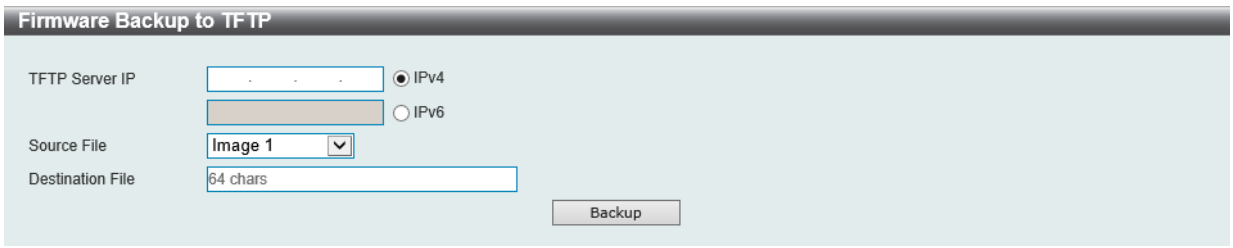


図 16-6　Firmware Backup to TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバにバックアップするファームウェアを選択します。 • 選択肢：「Image 1」「Image 2」
Destination File	ファームウェアがバックアップされる TFTP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「Backup」をクリックしてバックアップを開始します。

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

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

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

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

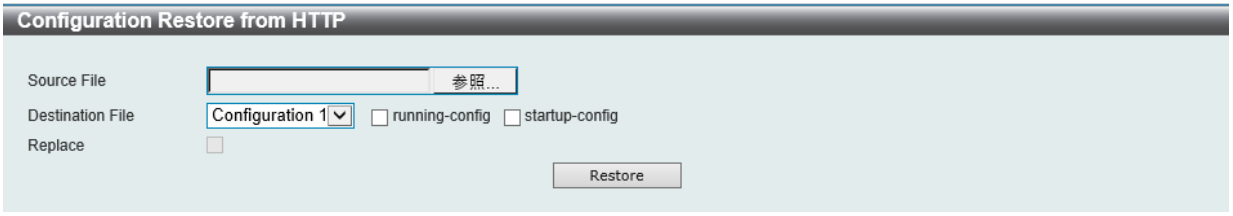


図 16-7　Configuration Restore from HTTP 画面

画面に表示される項目：

項目	説明
Source File	「Browse/ 参照」をクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定します。
Destination File	コンフィグレーションファイルが保存されるスイッチの場所を指定します。 • 「Configuration 1」-「Configuration 1」を指定します。 • 「Configuration 2」-「Configuration 2」を指定します。 • 「running-config」- ランニングコンフィグレーションファイルが上書きされます。 • 「startup-config」- スタートアップコンフィグレーションファイルが上書きされます。
Replace	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

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

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

TFTP サーバからコンフィグレーションをリストアします。

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

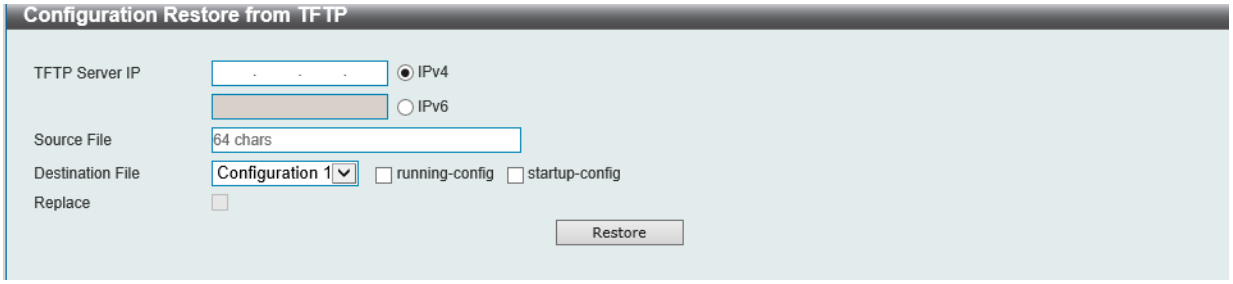


図 16-8　Configuration Restore from TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。（64 文字以内）
Destination File	コンフィグレーションファイルがストアされるスイッチの場所 / ファイル名を指定します。 • 「Configuration 1」-「Configuration 1」を指定します。 • 「Configuration 2」-「Configuration 2」を指定します。 • 「running-config」- ランニングコンフィグレーションファイルが上書きされます。 • 「startup-config」- スタートアップコンフィグレーションファイルが上書きされます。
Replace	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

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

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

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

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

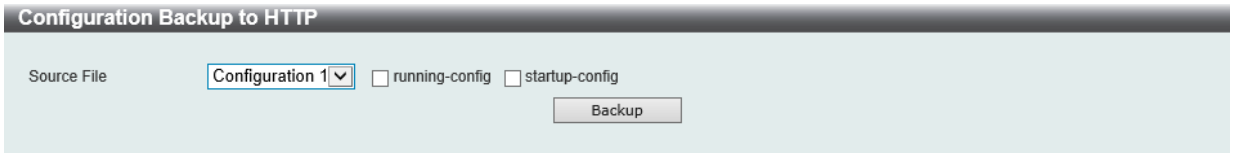


図 16-9　Configuration Backup to HTTP 画面

画面に表示される項目：

項目	説明
Source File	ローカル PC にバックアップするコンフィグレーションファイルを選択します。 • 「Configuration 1」-「Configuration 1」を指定します。 • 「Configuration 2」-「Configuration 2」を指定します。 • 「running-config」- ランニングコンフィグレーションファイルを指定します。 • 「startup-config」- スタートアップコンフィグレーションファイルを指定します。

「Backup」をクリックしてバックアップを開始します。

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

TFTP サーバにコンフィグレーションバックアップを行います。

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

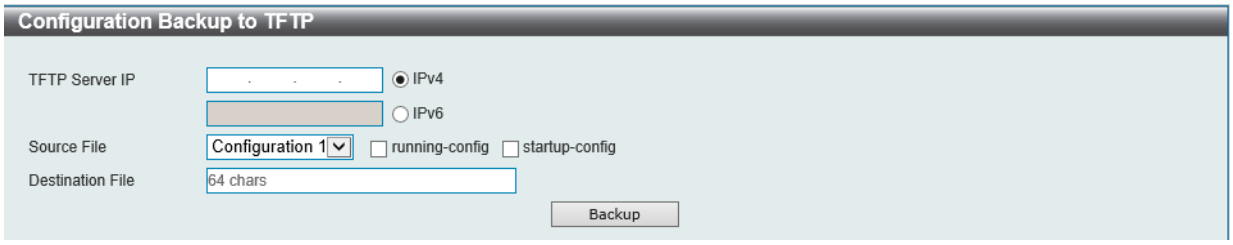


図 16-10　Configuration Backup to TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバにバックアップするコンフィグレーションファイルを選択します。 • 「Configuration 1」-「Configuration 1」を指定します。 • 「Configuration 2」-「Configuration 2」を指定します。 • 「running-config」- ランニングコンフィグレーションファイルを指定します。 • 「startup-config」- スタートアップコンフィグレーションファイルを指定します。
Destination File	コンフィグレーションファイルが保存される TFTP サーバの場所を指定します。（64 文字以内）

「Backup」をクリックしてバックアップを開始します。

Certificate & Key Restore & Backup（証明書と鍵のリストア＆バックアップ）

Certificate & Key Restore from HTTP（HTTP を使用した証明書 / 鍵リストア）

HTTP を使用してローカル PC から証明書 / 鍵のリストアを実行します。

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

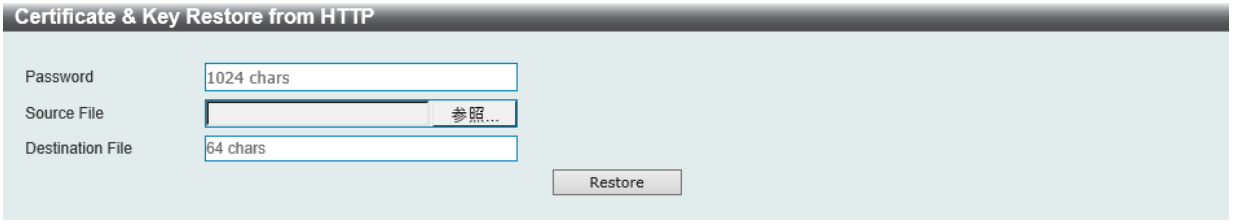


図 16-11　Certificate & Key Restore from HTTP 画面

画面に表示される項目：

項目	説明
Source File	「Browse/ 参照」をクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定します。
Destination File	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「Restore」をクリックしてリストアを開始します。

Certificate & Key Restore from TFTP（TFTP を使用した証明書とキーのリストア）

TFTP サーバから証明書 / 鍵リストアを実行します。

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

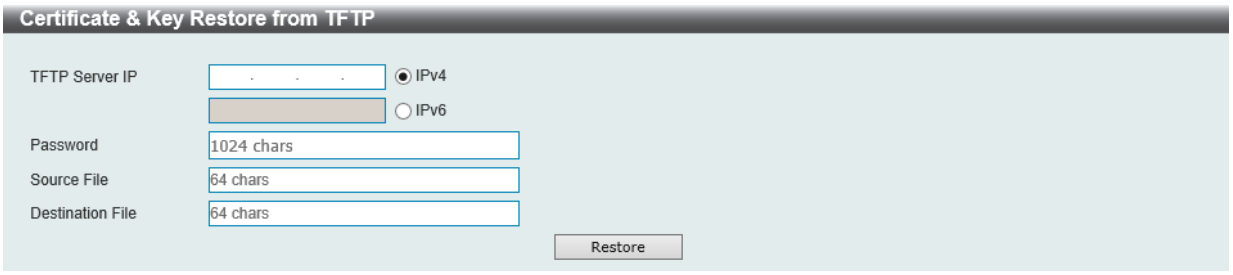


図 16-12　Certificate & Key Restore from TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバ上に保存されている証明書 / 鍵のパスとファイル名を入力します。（64 文字以内）
Destination File	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「Restore」をクリックしてリストアを開始します。

Public Key Backup to HTTP（HTTP を使用した公開鍵バックアップ）

HTTP を使用してローカル PC へ公開鍵のバックアップを行います。

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

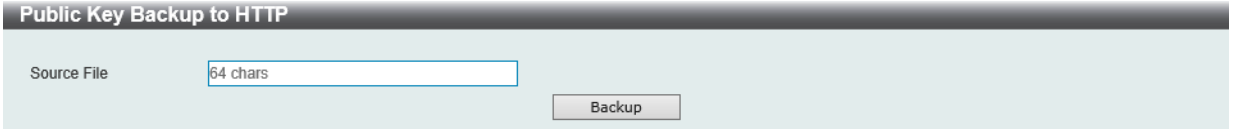


図 16-13　Public Key Backup to HTTP 画面

画面に表示される項目：

項目	説明
Source File	スイッチに保存されている公開鍵ファイルのパスとファイル名を入力します。（64 文字以内）

「Backup」をクリックしてバックアップを開始します。

Public Key Backup to TFTP（TFTP を使用した公開鍵バックアップ）

TFTP サーバに公開鍵バックアップを行います。

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

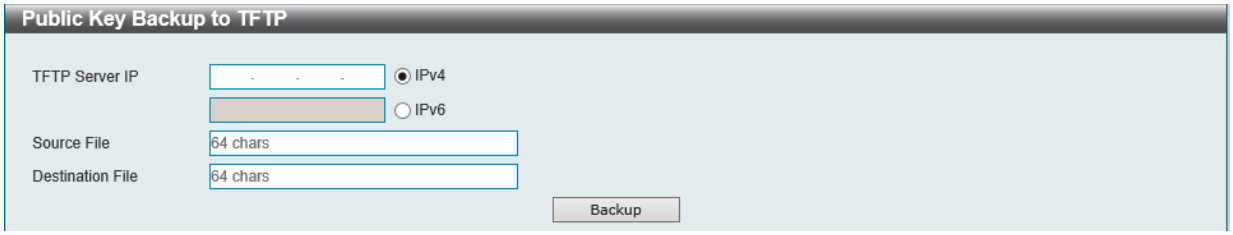


図 16-14　Public Key Backup to TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Source File	スイッチに保存されている公開鍵ファイルのパスとファイル名を入力します。（64 文字以内）
Destination File	公開鍵ファイルをバックアップする TFTP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「Backup」をクリックしてバックアップを開始します。

Log Backup（ログのバックアップ）

Log Backup to HTTP（HTTP を使用したログのバックアップ）

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

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

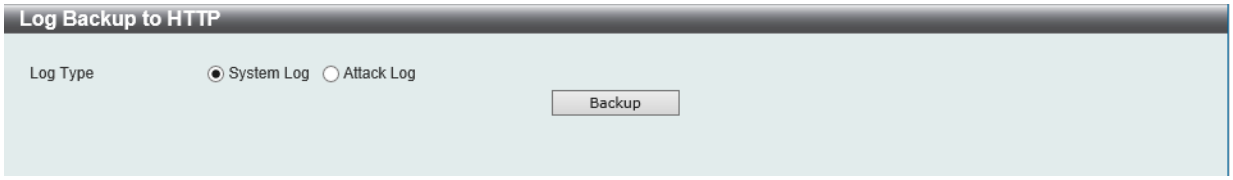


図 16-15　Log Backup to HTTP 画面

画面に表示される項目：

項目	説明
Log Type	HTTP を使用してローカル PC にバックアップするログの種類を選択します。 • 「System Log」- システムログをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「Backup」をクリックしてバックアップを開始します。

Log Backup to TFTP（TFTP を使用したログのバックアップ）

TFTP サーバへのシステムログのバックアップを行います。

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

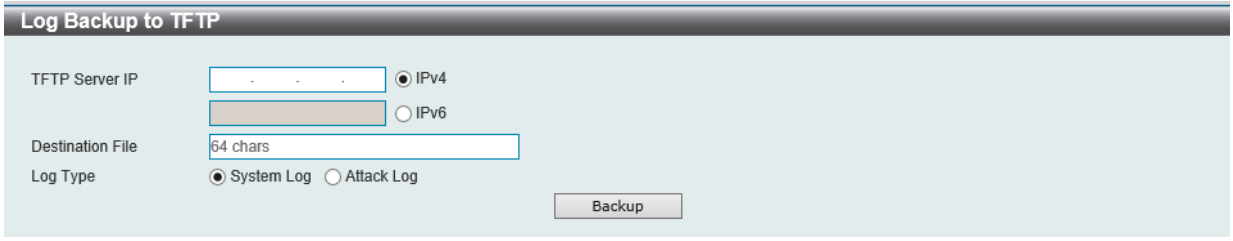


図 16-16　Log Backup to TFTP 画面

画面に表示される項目：

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
Destination File	ログファイルが保存される TFTP サーバの場所を指定します。（64 文字以内）
Log Type	HTTP を使用してローカル PC にバックアップするログの種類を選択します。 • 「System Log」- システムログをバックアップします。 • 「Attack Log」- 攻撃関連のログをバックアップします。

「Backup」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。ネットワーク上のスイッチと機器の接続状況を確認するうえで非常に有効です。

Tools > Ping をクリックし、設定画面を表示します。

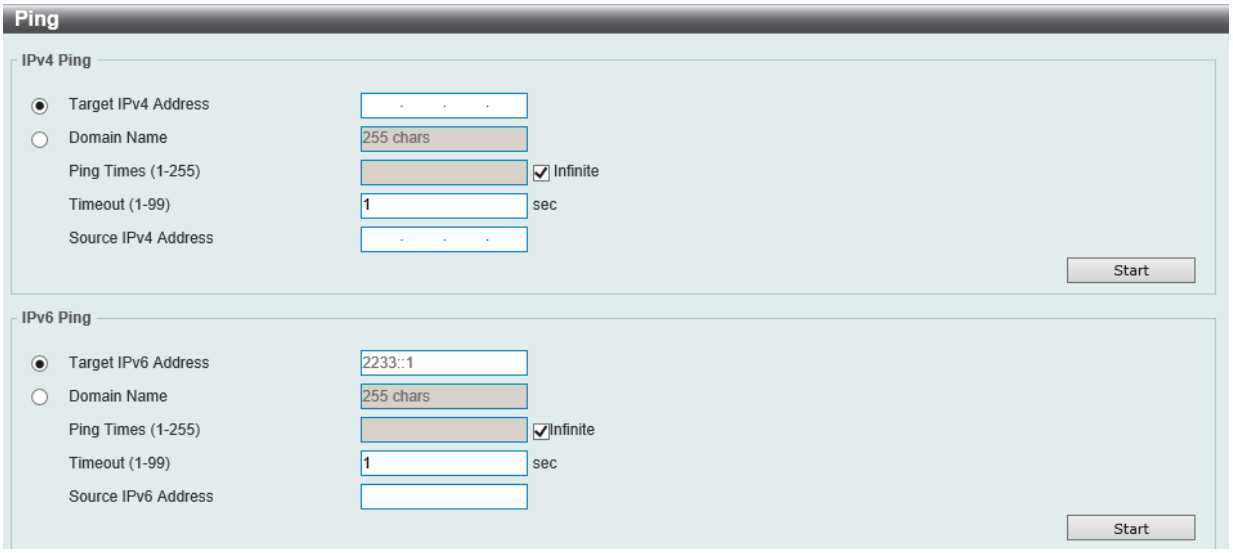


図 16-17　Ping 画面

画面に表示される項目：

項目	説明
IPv4 Ping	
Target IPv4 Address	Ping の送信先となる IPv4 アドレスを入力します。
Domain Name	検出するシステムのドメイン名を入力します。
Ping Times	Ping の試行回数を入力します。 「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。 • 設定可能範囲：1-255
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。 指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。 • 設定可能範囲：1-99（秒）
Source IPv4 Address	送信元 IPv4 アドレスを入力します。 スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。入力した IPv4 アドレスは、リモートホストに送信されるパケットの送信元 IP アドレスまたはプライマリ IP アドレスとして使用されます。
IPv6 Ping	
Target IPv6 Address	Ping の送信先となる IPv6 アドレスを入力します。
Domain Name	Ping の送信先となるドメイン名を入力します。
Ping Times	Ping の試行回数を入力します。 「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。 • 設定可能範囲：1-255
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。 指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。 • 設定可能範囲：1-99（秒）

項目	説明
Source IPv6 Address	送信元 IPv6 アドレスを入力します。 スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。入力した IPv6 アドレスは、リモートホストに送信されるパケットの送信元 IP アドレスまたはプライマリ IP アドレスとして使用されます。

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

以下のように結果が表示されます。

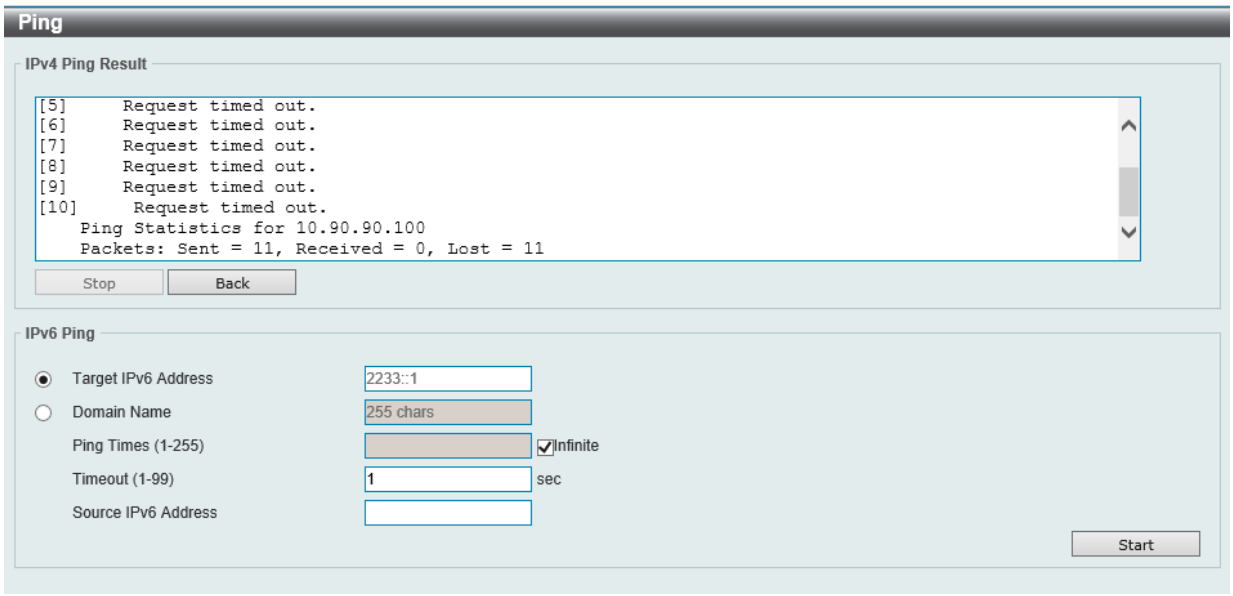


図 16-18　IPv4 Ping Result 画面

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

Language Management（言語管理）

言語ファイルのインストールを行います。

Tools > Language Management をクリックし、設定画面を表示します。

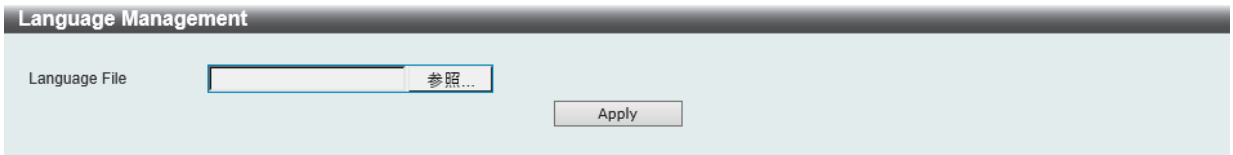


図 16-19　Language Management 画面

画面に表示される項目：

項目	説明
Language File	「Browse/ 参照」をクリックして、ローカル PC の言語ファイルを選択します。

「Apply」をクリックし、言語ファイルをインストールします。

Reset（リセット）

スイッチの設定内容を工場出荷時状態に戻します。

Tools > Reset をクリックし、次の設定画面を表示します。

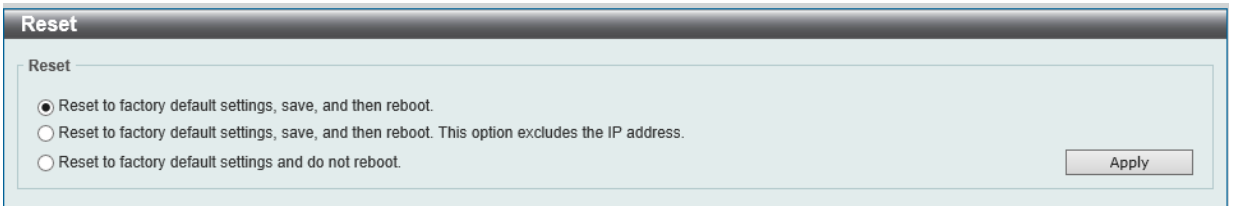


図 16-20　Reset 画面

画面に表示される項目：

項目	説明
Reset to factory default settings, save, and then reboot.	スイッチを工場出荷時設定にリセットして、保存、再起動を実行します。 （IP アドレスを含む）
Reset to factory default settings, save, and then reboot.This option excludes the IP address.	スイッチを工場出荷時の設定に戻し、保存、再起動を実行します。 （IP アドレスは除く）
Reset to factory default settings and do not reboot.	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」をクリックして、リセットを開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

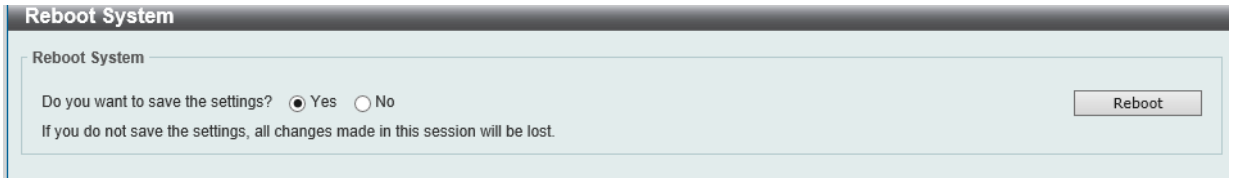


図 16-21　Reboot System 画面

画面に表示される項目：

項目	説明
Yes	スイッチは再起動する前に現在の設定を保存します。
No	スイッチは再起動する前に現在の設定を保存しません。保存していない設定は破棄され、最後に保存した時の設定が使われます。
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。

再起動中は以下の画面が表示されます。

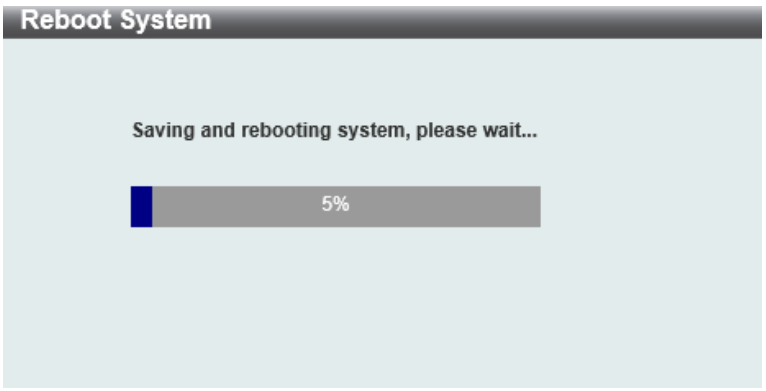


図 16-22　Reboot System（Rebooting）画面

Wizard（ウィザード）

クリックするとスマートウィザードを開始します。詳しくは「Smart Wizard 設定」を参照ください。

Online Help（オンラインヘルプ）

D-Link Support Site（D-Link サポート Web サイト（英語））

クリックすると D-Link のサポート Web サイト（英語）へ接続します。インターネット接続が必要です。

User Guide（ユーザガイド（英語版））

ユーザガイド（英語版）を表示します。インターネット接続が必要です。

Surveillance Mode（サーベイランスモードへの変更）

クリックするとスタンダードモードからサーベイランスモードに移行します。移行に失敗すると警告メッセージが表示されます。

注意 他のユーザセッションが同時にアクセスする場合、同じ Web UI モードの場合にのみアクセスが可能です。
Web モードは実行中のユーザセッションが 1 つの場合のみ変更できます。他のユーザセッションが実行中の場合は、Web モードを変更できません。

「Surveillance Mode」をクリックすると次の画面が表示されます。

図 16-23　Surveillance Mode Confirmation Message 画面

「サーベイランスモードに移行すると、ASV2.0、LBD、SNMP、SNMP トラップがグローバルで有効になります。Safeguard、Syslog が有効になります。また、VLAN メンバポートはアップリンクポートを除いてタグなしポートになります。」という内容です。

サーベイランスモードへ変更する場合は「OK」をクリックします。「Cancel」をクリックするとスタンダードモードへ戻ります。

サーベイランスモードへの変更に成功すると、次のダイアログが表示されます。

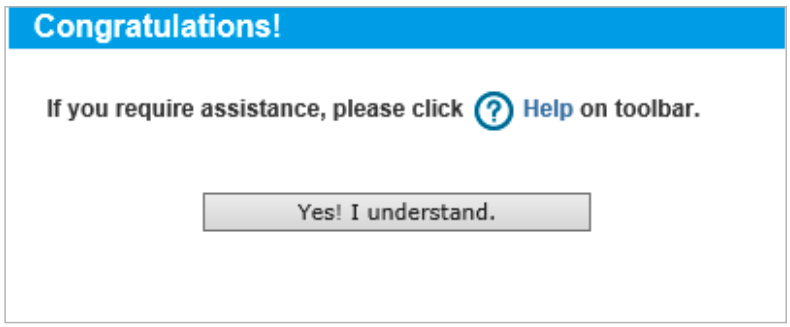


図 16-24　Surveillance Mode 'Congratulations' Message 画面

「Yes! I understand」をクリックしサーベイランスモードへ移行します。詳しくは「第 17 章　サーベイランスモード」を参照ください。

Logout（ログアウト）

クリックするとログアウトします。

第 17 章　サーベイランスモード

本製品シリーズには「Standard Mode（スタンダードモード）」と「Surveillance Mode（サーベイランスモード）」の 2 種類の Web GUI があります。「サーベイランスモード」はネットワーク上の監視デバイス（IP カメラ等）や IP セキュリティデバイスの確認と管理のために特化したインタフェースです。

- Surveillance Overview（サーベイランスモード概要）
- Port Information（ポート情報）
- IP-Camera Information（IP-Camera 情報）
- NVR Information（NVR 情報）
- Management（管理）
- Time（時刻設定）
- Surveillance Settings（サーベイランス設定）
- Surveillance Log（サーベイランスログ）
- Health Diagnostic（正常性診断）
- Toolbar（ツールバー）（サーベイランスモード）

Surveillance Overview（サーベイランスモード概要）

サーベイランスモード画面が表示された場合、メイン画面には「Surveillance Overview（サーベイランスの概要）」が表示されます。
本画面には、「Surveillance Topology」（サーベイランストポロジ）」タブと「Device Information（デバイス情報）」タブが存在します。

Surveillance Topology（サーベイランストポロジ）

「Surveillance Topology」タブでは、スイッチに接続されたデバイスの情報など、サーベイランストポロジ（図）が表示されます。
トポロジに表示されているデバイスのアイコンにカーソルを置くと、デバイスについての情報が表示されます。

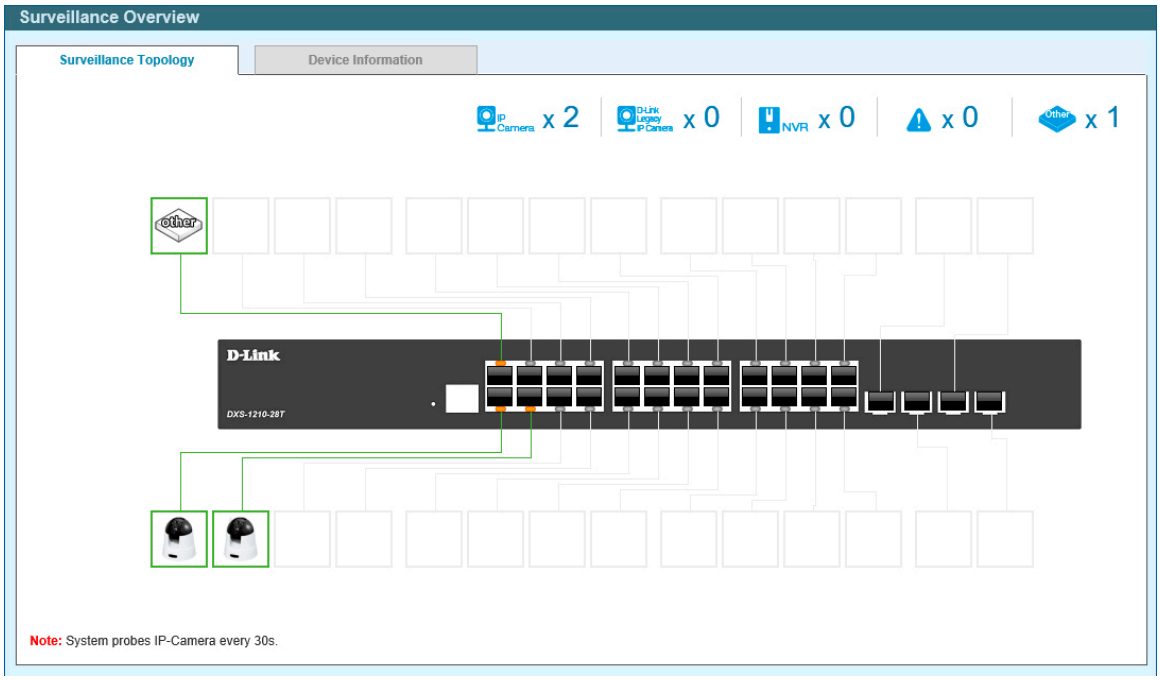


図 17-1　Surveillance Overview 画面

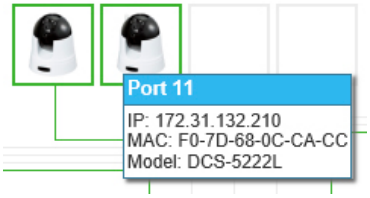
以下の項目が表示されます。

アイコン	説明
上部機器アイコン	
IP Camera	検出された ONVIF IP カメラ数です。
D-Link Legacy IP Camera	検出された D-Link レガシー IP カメラ数です。（ASV 1.0 により検出）
NVR	検出された NVR（Network Video Recorders）数です。
	スイッチで発生している警告の数です。
Other	スイッチに接続している他の機器の数です。

各機器アイコンの PoE 電力需給状況について以下のように表示されます。

アイコン	説明
	スイッチに接続している機器を表示します。緑色の枠で囲まれている機器は PoE 受電機器ではありません。

トポロジに表示されているデバイスのアイコンにカーソルを置くと、デバイスについての情報が表示されます。



注意　スイッチは ONVIF トラフィックをサーベイランス機器のステータスのモニタに使用しますが、他社製機器だと ONVIF 基準に準拠していない場合があります。「検出されない」などの問題が発生した場合、サーベイランス機器の ONVIF 準拠の有無を確認してください。

Device Information（デバイス情報）

デバイスの情報を確認します。

「Device Information」をクリックし、以下の画面を表示します。

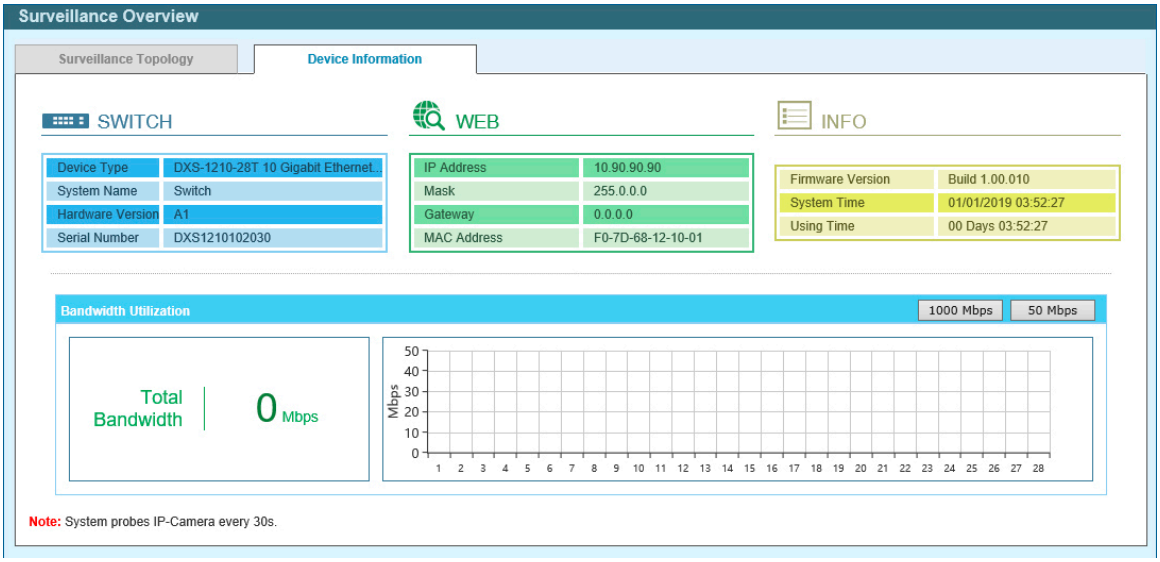


図 17-2　Device Information 画面

「1000 Mbps」をクリックして、帯域幅使用率チャートに表示される最大帯域幅を 1Gbps に変更します。
「50 Mbps」をクリックして、帯域幅使用率チャートに表示される最大帯域幅を 50Mbps に変更します。

Port Information（ポート情報）

各ポートのステータスを表示します。
スループット、ループ検知ステータス、ケーブル長、電力消費、IP カメラ /NVR/ その他のデバイスの接続台数などが表示されます。

「Port Information」をクリックし、以下の画面を表示します。

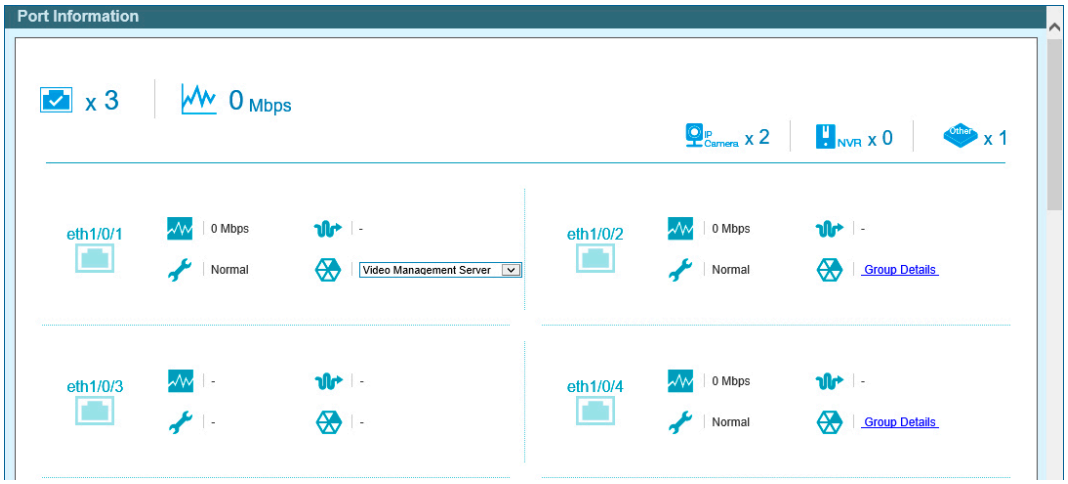


図 17-3　Port Information 画面

以下のアイコン、項目が表示されます。

アイコン	説明
上部機器アイコン	
	スイッチのイーサネットポートに接続したデバイス数です。
	スイッチのイーサネットポートに接続したデバイスによる総インバウンド帯域です。
	検出された ONVIF IP カメラ数です。
	検出された NVR 数です。
	スイッチに接続している他の機器の数です。
各ポート情報	
	ポート番号です。
	対象ポートの総インバウンド帯域（Mbps）です。
	接続しているケーブルのケーブル長です。
	ポートのループバック検出状況について表示します。 • 「Normal」- ネットワークでのループは発生していません。 • 「Loop」- ループが発生しています。「Loop」は「Health Diagnostics」画面へのリンクになります。
	ONVIF 対応機器（IP カメラ /NVR）が対象ポートに検出された場合、アイコンは「Group Details」（グループ詳細）へのリンクになります。

アイコン	説明
Video Management Server	ONVIF 非対応機器が検出された場合、ドロップダウンが表示され、下記から機器の種類を選択することが可能です。 • 「Video Management Server（ビデオマネジメントサーバ）」 • 「VMS Client/Remote Viewer（VMS クライアント / リモートビューワ）」 • 「Video Encoder（ビデオエンコーダ）」 • 「Network Storage（ネットワークストレージ）」 • 「Other IP Surveillance Device（その他サーベイランス機器）」

Group Details（グループ詳細）をクリックすると次の画面が表示されます。

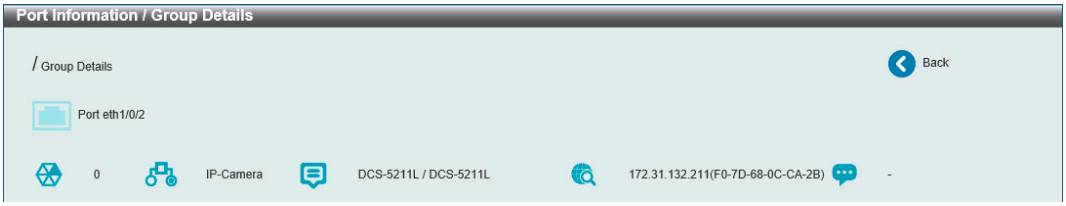


図 17-4　Port Information / Group Details 画面

以下のアイコン、項目が表示されます。

アイコン	説明
Port eth1/0/1	スイッチのポート番号です。
	スイッチのイーサネットポートに接続した IP カメラまたは NVR のグループ ID です。
	スイッチのイーサネットポートに接続した IP カメラまたは NVR の種類です。
	スイッチのイーサネットポートに接続した IP カメラの型番です。
	スイッチのイーサネットポートに接続した IP カメラまたは NVR の IP アドレスと MAC アドレスです。
	スイッチのイーサネットポートに接続したデバイスの概要です。

「Back」をクリックすると前の画面に戻ります。

IP-Camera Information（IP-Camera 情報）

スイッチに接続されているカメラの情報を表示します。

「IP-Camera Information」をクリックし、以下の画面を表示します。

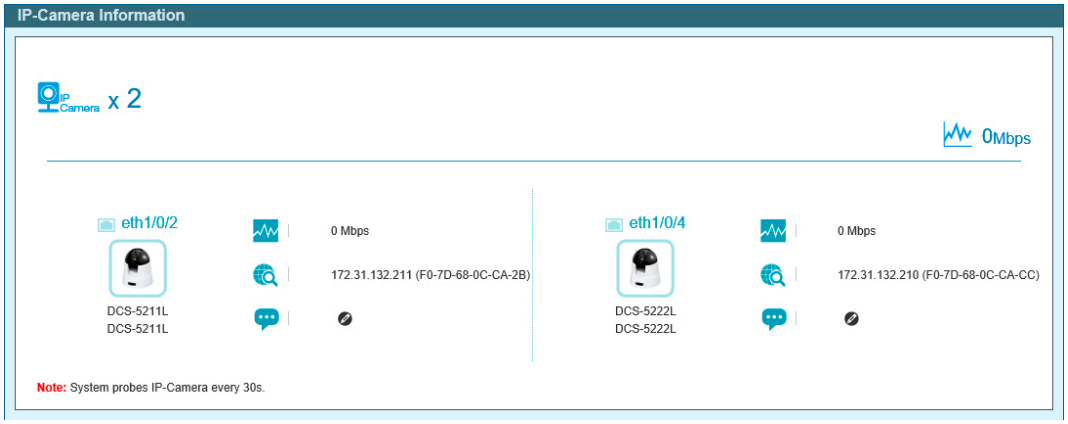
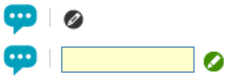


図 17-5　IP-Camera Information 画面

以下のアイコン、項目が表示されます。

アイコン	説明
上部アイコン	
	スイッチのイーサネットポートに接続した検出された ONVIF IP カメラ数です。
	スイッチのイーサネットポートに接続した ONVIF IP カメラにより使用されている総インバウンド帯域量です。
各機器情報	
	ポート番号です。
	機器のアイコンまたは画像が表示されます。 D-Link 以外の ONVIF 対応カメラでは、一般的な画像が表示されます。D-Link カメラの場合、対象機器の画像が表示されます。
	IP カメラにより使用されている総インバウンド帯域量です。
	IP カメラの IP/MAC アドレスです。
	機器の概要を表示します。アイコンをクリックして概要を編集します。 入力完了後、アイコンをクリックして設定を保存します。

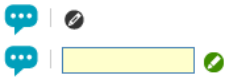
NVR Information（NVR 情報）

スイッチに接続された NVR の情報を表示します。

機能一覧から「NVR Information」をクリックします。

図 17-6　NVR Information 画面

以下のアイコン、項目が表示されます。

アイコン	説明
上部アイコン	
	スイッチのイーサネットポートに接続した NVR 数です。
	スイッチのイーサネットポートに接続した NVR により使用されている総インバウンド帯域量です。
各機器情報	
	ポート番号です。
	NVR 機器のアイコンまたは画像が表示されます。
	NVR により使用されているインバウンド帯域量です。
	NVR の IP/MAC アドレスです。
	NVR の概要を表示します。アイコンをクリックして概要を編集します。入力完了後、アイコンをクリックして設定を保存します。
	NVR のグループ ID です。
	NVR に管理されている ONVIF 対応の IP カメラの数です。
	NVR により管理されている ONVIF IP カメラについての情報が表示されます。

Management（管理）

File System（ファイルシステム）

スイッチのファイルシステムを設定します。

1. **Management > File System** の順にメニューをクリックします。

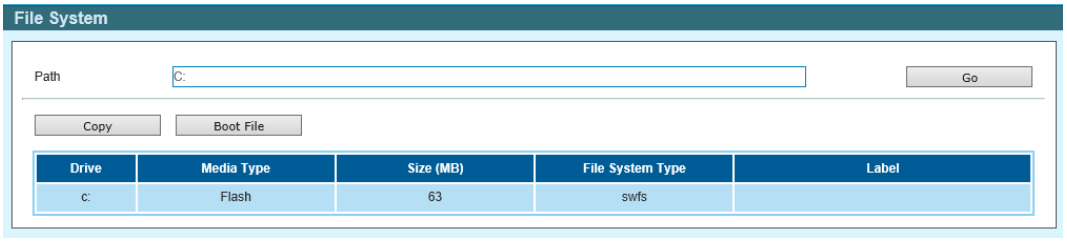


図 17-7　File System 画面

2. 設定したい内容に応じて以下から操作を選択します。

項目	説明
Path	ファイルパスを指定します。

3. 「Go」をクリックして入力したパスを参照します。
4. 「c:」のハイパーリンクをクリックすると C ドライブのファイルシステムを参照します。次の画面が表示されます。

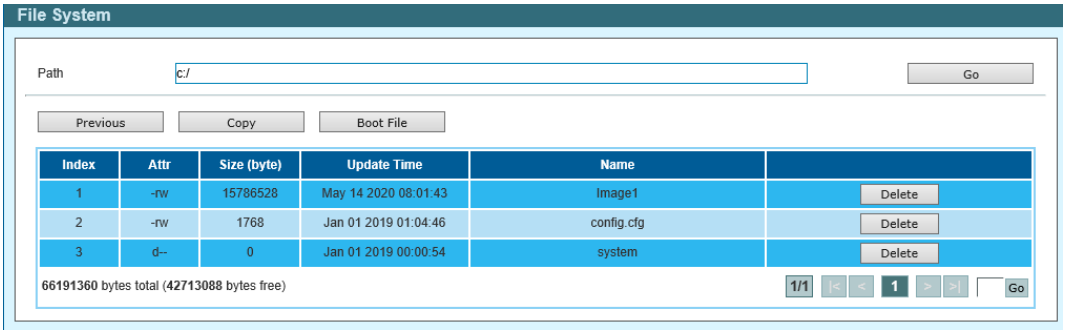


図 17-8　File System（c:）画面

「Previous」：前の画面に戻ります。
「Copy」：ファイルをコピーします。
「Boot File」：ブートアップイメージとブートコンフィグレーションファイルの設定を行います。
「Delete」：ファイルを削除します。

指定ファイルをコピーするには、「Copy」をクリックします。次の画面が表示されます。

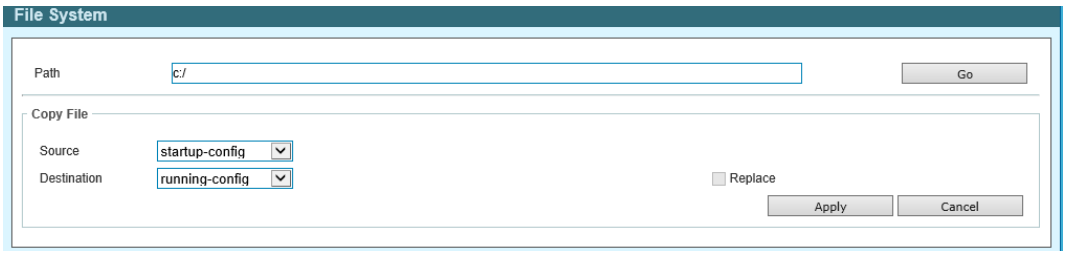


図 17-9　File System（Copy）画面

項目	説明
Source	コピー元のファイルを指定します。 • 「startup-config」- スタートアップコンフィグレーションファイルをコピー元として指定します。 • 「Image 1」-「Image 1」のファームウェアをコピー元として指定します。 • 「Image 2」-「Image 2」のファームウェアをコピー元として指定します。 • 「Configuration 1」-「Configuration 1」をコピー元として指定します。 • 「Configuration 2」-「Configuration 2」をコピー元として指定します。
Destination	コピー先のファイルを指定します。 • 「running-config」- ランニングコンフィグレーションファイルを上書きします。 • 「startup-config」- スタートアップコンフィグレーションファイルを上書きします。 • 「Image 1」-「Image 1」のファームウェアを上書きします。 • 「Image 2」-「Image 2」のファームウェアを上書きします。 • 「Configuration 1」-「Configuration 1」を上書きします。 • 「Configuration 2」-「Configuration 2」を上書きします。
Replace	チェックすると現在実行中のコンフィグレーションと入れ替わります。

「Apply」をクリックして設定を有効にします。

「Cancel」をクリックして設定を破棄します。

Time（時刻設定）

スイッチの時刻や SNTP サーバの設定を行います。

Clock Settings（時刻設定）

スイッチの時刻を設定します。

1. **Time > Clock Settings** の順にメニューをクリックします。

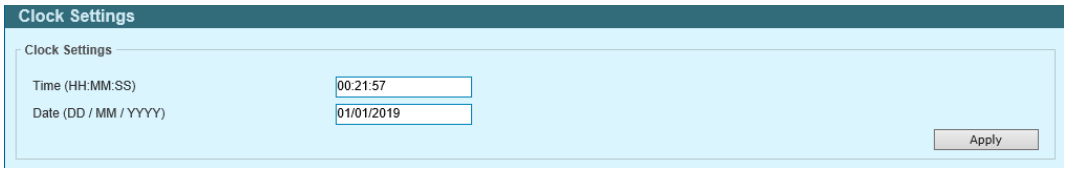


図 17-10　Clock Settings 画面

2. 時刻と日付を設定します。

項目	説明
Time (HH:MM:SS)	システムの時刻を「HH:MM:SS」（時間：分：秒）のフォーマットで設定します。
Date(DD/MM/YYYY)	システムの日付を「DD:MM:YYYY」（日：月：年）のフォーマットで設定します。

3. 「Apply」をクリックして設定を有効にします。

SNTP Settings（SNTP 設定）

Simple Network Time Protocol (SNTP) の設定を行います。

1. **Time > SNTP Settings** の順にメニューをクリックします。

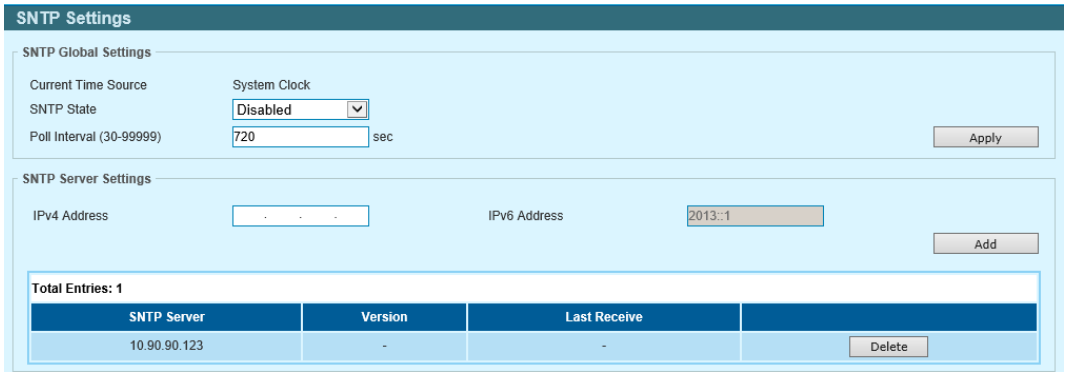


図 17-11　SNTP Settings 画面

2. 「SNTP Global Settings」セクションで、設定したい内容に応じて以下から操作を選択します。

項目	説明
SNTP State	SNTP 機能を有効 / 無効 にします。
Poll Interval	ポーリング間隔を指定します。 • 設定可能範囲：30-99999（秒） • 初期値：720（秒）

3. 「Apply」をクリックして設定を有効にします。

SNTP サーバを設定する場合：

1. 「SNTP Server Settings」セクションで、設定したい内容に応じて以下から操作を選択します。

項目	説明
IPv4 Address	SNTP サーバの IPv4 アドレスを設定します。
IPv6 Address	SNTP サーバの IPv6 アドレスを設定します。

2. 「 Add」をクリックして SNTP サーバを追加します。「Delete」をクリックすると SNTP サーバを削除します。

Surveillance Settings（サーベイランス設定）

サーベイランス VLAN の設定を行います。サーベイランス VLAN は 1 つのみです。
本サーベイランス VLAN は、ONVIF プロトコルを使用して、IP カメラやネットワークビデオレコーダー（NVR）などのサーベイランスデバイスの認識もサポートします。

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

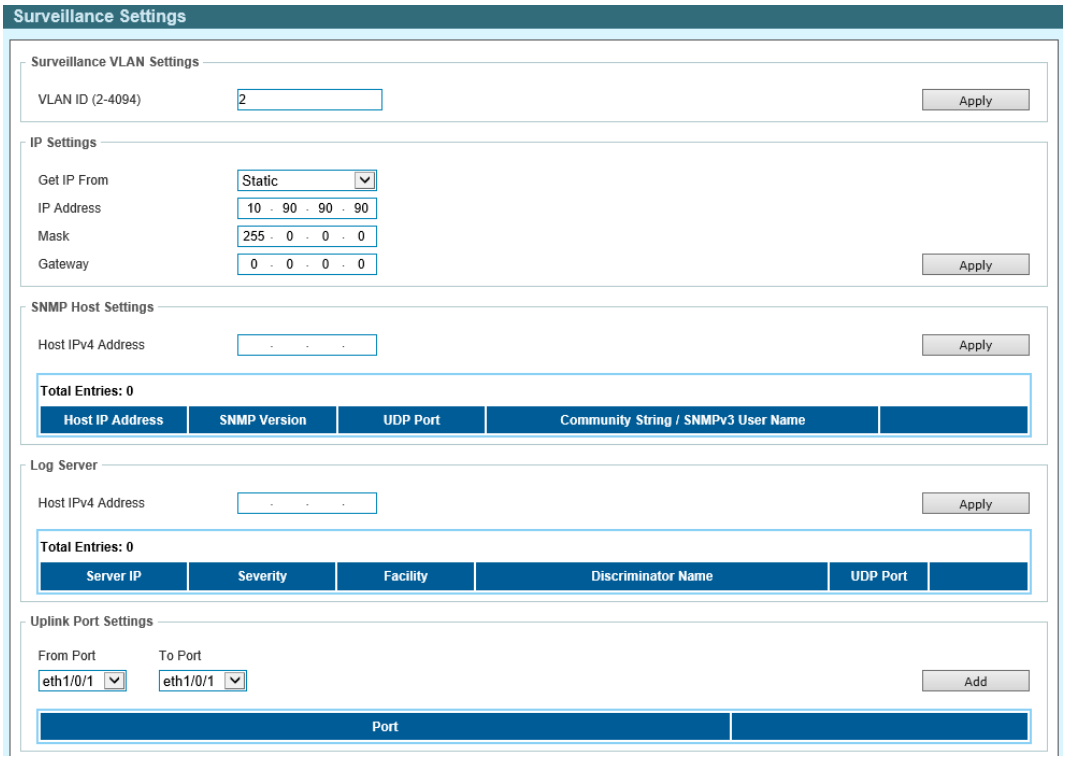


図 17-12　Surveillance Settings 画面

画面に表示される項目：

項目	説明
Surveillance VLAN Settings	
VLAN ID	サーベイランス VLAN の ID を指定します。 • 設定可能範囲：2-4094
IP Settings	
Get IP From	スイッチの IP アドレスの取得方法を選択します。 • 選択肢：「Static」「DHCP」
IP Address	スイッチの IPv4 アドレスを入力します。
Mask	スイッチの IPv4 サブネットマスクを入力します。
Gateway	デフォルトゲートウェイの IPv4 アドレスを入力します。
SNMP Host Settings	
Host IPv4 Address	SNMP ホストの IPv4 アドレスを指定します。
Log Server	
Host IPv4 Address	ログサーバの IPv4 アドレスを指定します。
Uplink Port Settings	
From Port / To Port	ポート範囲を指定します。

各項目で「Apply」をクリックして設定を有効にします。
設定を削除するには「Delete」をクリックします。

Surveillance Log（サーベイランスログ）

スイッチで生成されたサーベイランスログの一覧を表示します。

機能一覧から「Surveillance Log」をクリックします。

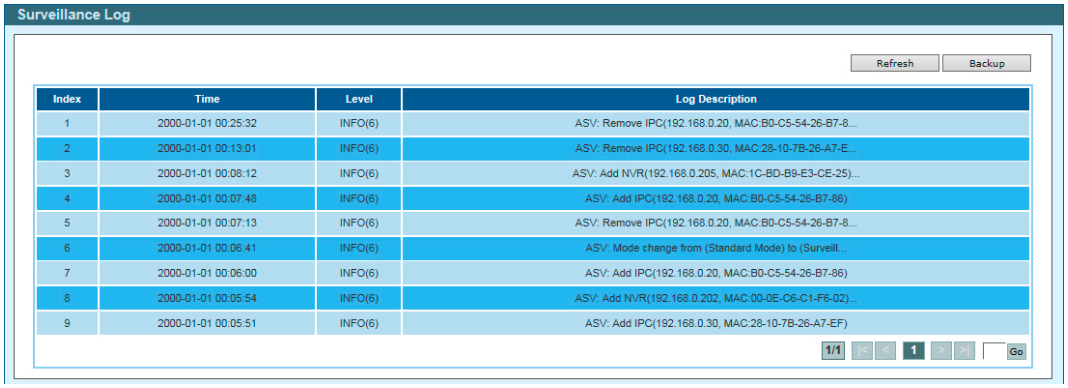


図 17-13　Surveillance Log 画面

テーブルの情報を更新するには「Refresh」をクリックします。
「Backup」をクリックすると、HTTP を使用して、サーベイランスログを PC へアップロードします。
複数のページがある場合、「Go」をクリックしてページを移動します。

Health Diagnostic（正常性診断）

正常性診断の情報、検出された監視デバイス情報、およびスイッチ上のすべてのポートまたは選択されたポートのケーブル距離テストの開始に使用されます。 リンクアップポートごとに、システムはリンクステータス、PoE ステータス、およびエラーカウンタを定期的にチェックします。
このページは 30 秒ごとに更新されます。

機能一覧から「Health Diagnostic」をクリックします。

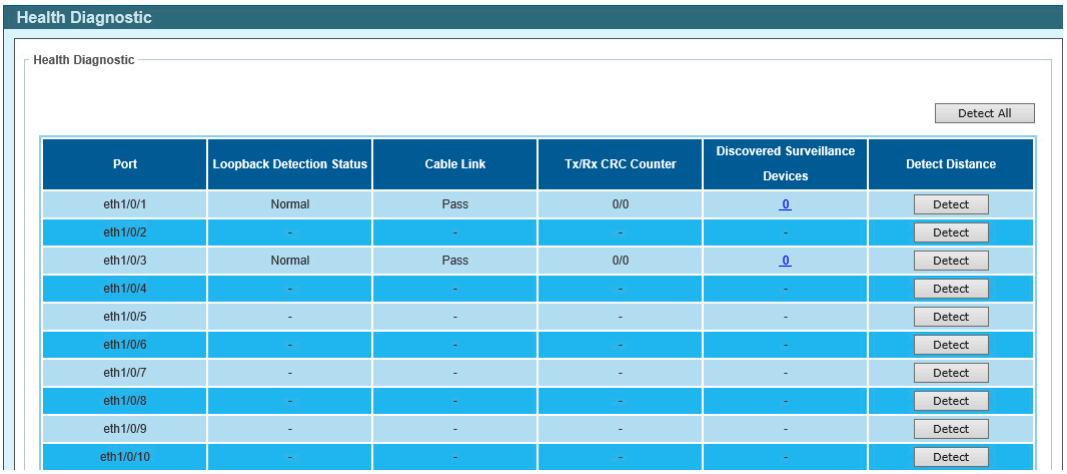


図 17-14　Health Diagnostic 画面

画面に表示される項目：

項目	説明
Port	ポート番号を表示します。
Loopback Detection Status	ポートのループバックを表示します。 • 「Normal」- ループは検出されていません。 • 「Loop」- ループが検出されています。
Cable Link	ケーブルリンクの状態を表示します。 • 「PASS」- 全二重モードでリンクアップしています。
Tx/Rx CRC Counter	TX/RX CRC カウンタについて表示します。
Discovered Surveillance Devices	検出された ONVIF IP カメラ /NVR の数を表示します。 ハイパーリンク（1）をクリックするとポートに接続した IP カメラ /NVR のグループ詳細（Group Details）について表示します。
Detect Distance	「Detect」をクリックすると、指定ポートのケーブル長テストを開始します。

スイッチの全ポートでケーブル長を検出するには「Detect All」をクリックします。

Toolbar（ツールバー）（サーベイランスモード）

Web インタフェース画面上部のツールバーにある「Wizard」「Tools」「Save」「Help」「Online Help」「Standard Mode」「Logout」メニューを使用してスイッチの管理・設定を行います。

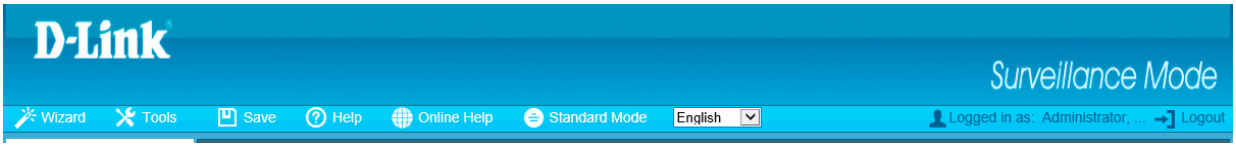


図 17-15　Toolbar（サーベイランスモード）

Wizard（ウィザード）

クリックするとスマートウィザードを開始します。詳しくは Smart Wizard 設定を参照ください。

Tools（ツール）

Firmware Upgrade & Backup（ファームウェアのアップグレードと保存）

ファームウェアのバックアップ、またはファームウェアのアップグレードを行います。

■ 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。

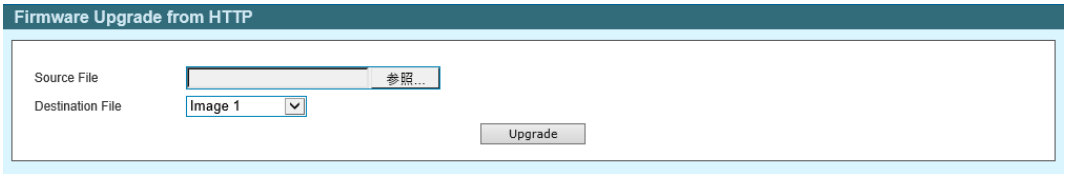


図 17-16　Firmware Upgrade from HTTP 画面

画面に表示される項目：

項目	説明
Source File	「Browse/ 参照」をクリックしてローカル PC 上のファームウェアファイルの場所を指定します。
Destination File	ファームウェアが保存されるスイッチの宛先を指定します。 • 選択肢：「Image 1」「Image 2」

「Upgrade」をクリックしてアップグレードを開始します。

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

HTTP を使用して、ローカル PC へのファームウェアのバックアップを行います。

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

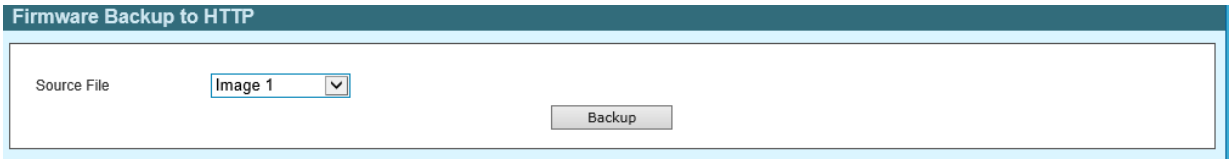


図 17-17　Firmware Backup to HTTP 画面

画面に表示される項目：

項目	説明
Source File	ローカル PC にバックアップするファームウェアを選択します。 • 選択肢：「Image 1」「Image 2」

「Backup」をクリックしてバックアップを開始します。

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

■ Configuration Restore from HTTP（HTTP からのコンフィグレーションリストア）

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

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

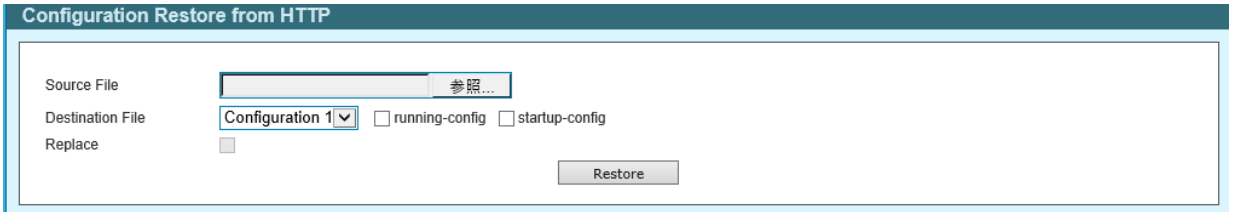


図 17-18　Configuration Restore from HTTP 画面

画面に表示される項目：

項目	説明
Source File	「Browse/ 参照」をクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定します。
Destination File	コンフィグレーションファイルが保存されるスイッチの場所を指定します。 • 「Configuration 1」-「Configuration 1」を指定します。 • 「Configuration 2」-「Configuration 2」を指定します。 • 「running-config」- ランニングコンフィグレーションファイルが上書きされます。 • 「startup-config」- スタートアップコンフィグレーションファイルが上書きされます。
Replace	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

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

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

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

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

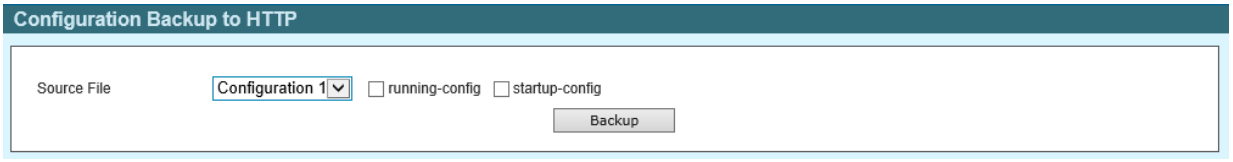


図 17-19　Configuration Backup to HTTP 画面

画面に表示される項目：

項目	説明
Source File	ローカル PC にバックアップするコンフィグレーションファイルを選択します。 • 「Configuration 1」-「Configuration 1」を指定します。 • 「Configuration 2」-「Configuration 2」を指定します。 • 「running-config」- ランニングコンフィグレーションファイルを指定します。 • 「startup-config」- スタートアップコンフィグレーションファイルを指定します。

「Backup」をクリックしてバックアップを開始します。

Language Management（言語管理）

言語ファイルのインストールを行います。

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

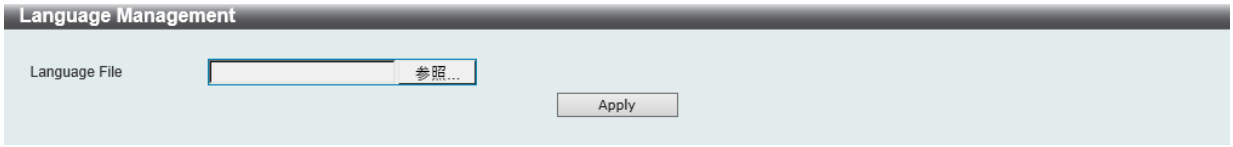


図 17-20　Language Management 画面

画面に表示される項目：

項目	説明
Language File	「Browse/ 参照」をクリックして、ローカル PC の言語ファイルを選択します。

「Apply」をクリックし、言語ファイルをインストールします。

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。

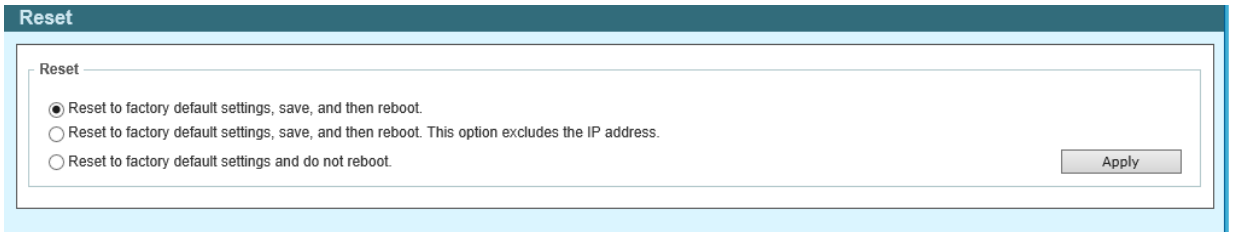


図 17-21　Reset 画面

画面に表示される項目：

項目	説明
Reset to factory default settings, save, and then reboot.	スイッチを工場出荷時設定にリセットして、保存、再起動を実行します。（IP アドレスを含む）
Reset to factory default settings, save, and then reboot.This option excludes the IP address.	スイッチを工場出荷時の設定に戻し、保存、再起動を実行します。（IP アドレスは除く）
Reset to factory default settings and do not reboot.	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」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。

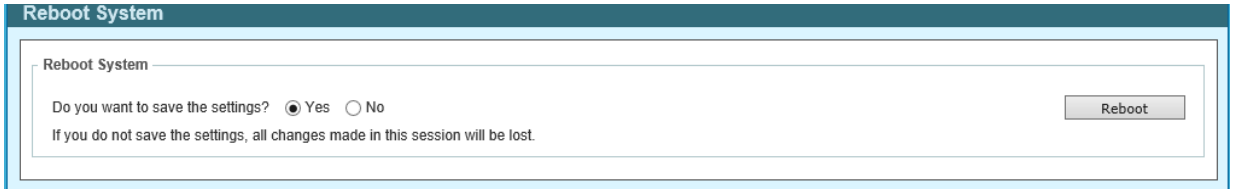


図 17-22　Reboot System 画面

画面に表示される項目：

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。

Save（保存）

Save Configuration（コンフィグレーションの保存）

現在のコンフィグレーションをスイッチに保存します。

Save > Save Configuration をクリックし、以下の画面を表示します。

図 17-23　Save Configuration 画面

画面に表示される項目：

項目	説明
File Path	コンフィグレーションファイルの保存先を選択します。 • 「Configuration 1」-「Configuration 1」を宛先に指定します。 • 「Configuration 2」-「Configuration 2」を宛先に指定します。 • 「startup-config」- スタートアップコンフィグレーションファイルを宛先に指定します。

「Apply」をクリックし、設定を保存します。

Help（ヘルプ画面）

ツールバーの「Help」をクリックすると、以下のヘルプ画面が表示されます。

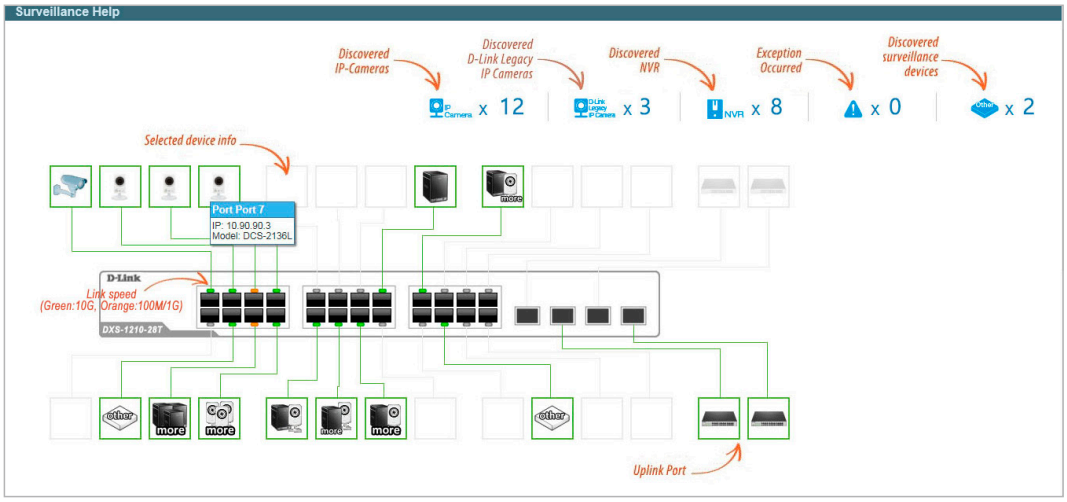


図 17-24　Surveillance Help - Diagram 画面

Device Status

Icon	Description	Icon	Description	Icon	Description
	The device is operational but is not powered by PoE.		The device is operational and is powered by PoE.		The device may malfunction. Some problem detected on this port or device.

IP-Camera/NVR Status

Icon	Description	Icon	Description	Icon	Description
	One D-Link ONVIF IP-Camera discovered on this port. For D-Link IP-Camera, a specific icon will be displayed.		One ONVIF IP-Camera discovered on this port.		Multiple ONVIF IP-Cameras discovered on this port.
	One NVR discovered on this port. Any device connect to IP-Camera via HTTP, HTTPS and RTSP will be recognized as an NVR.		Multiple NVRs discovered on this port.		One ONVIF IP-Camera and one NVR discovered on this port.
	Multiple ONVIF IP-Cameras and one NVR discovered on this port.		One ONVIF IP-Camera and multiple NVRs discovered on this port.		Multiple ONVIF IP-Cameras and multiple NVRs discovered on this port.
	The port is up and no ONVIF IP-Camera, NVR, or other surveillance device has been discovered on this port.		This port is set as uplink port and the port status is up. Uplink port joins all VLANs and surveillance discovery process is disabled on this port.		This port is set as uplink port and the port status is down.

図 17-25　Surveillance Help - Table 画面

Online Help（オンラインヘルプ）

D-Link Support Site（D-Link サポート Web サイト（英語））

クリックすると D-Link のサポート Web サイト（英語）へ接続します。インターネット接続が必要です。

User Guide（ユーザガイド（英語版））

ユーザガイド（英語版）を表示します。インターネット接続が必要です。

Standard Mode（スタンダードモード）

ツールバーの「Standard Mode」をクリックすると、スタンダードモードの Web UI 表示に切り替わります。

注意 セッションが複数実行されている場合、スタンダードモードへの切り替えを行うことはできません。

Logout（ログアウト）

クリックすると Web GUI からログアウトします。

【付録 A】システムログエントリ

スイッチのシステムログに表示される可能性のあるログイベントとそれらの意味を以下に示します。

Critical（重大）、Warning（警告）、Informational（報告）、Critical（重大）、Warning（警告）、Informational（報告）、Notification（通知）

	ログの内容	緊急度	イベントの説明
	802.1X		
1	802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) **パラメータ説明：** • username：認証されているユーザ名 • interface-id：スイッチインタフェース番号 • mac-address：認証されたデバイスの MAC アドレス	Critical	802.1X 認証に失敗しました。 認証失敗には主に以下の原因が考えられます。 (1) user authentication failure. : ユーザ認証失敗 (2) no server(s) responding. : サーバ応答なし (3) no servers configured. : サーバ未設定 (4) no resources. : リソース不足 (5) user timeout expired. : ユーザタイムアウト
2	802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) **パラメータ説明：** • username：認証されたユーザ名 • interface-id：インタフェース名 • mac-address：認証されたデバイスの MAC アドレス	Informational	802.1X 認証に成功しました。
	AAA		
1	AAA is <status> **パラメータ説明：** status：AAA のステータス	Informational	AAA グローバルステートが有効または無効です。
2	Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。（例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。（例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	Informational	ログインに成功しました。
3	Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。 例：Console、Telnet、SSH、Web、Web(SSL) • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	Warning	ログインに失敗しました。
4	RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • vid：RADIUS サーバから認証された VLAN ID 割り当て • interface–id：認証されたクライアントのポート番号 • username：認証されるユーザ名	Informational	RADIUS が有効な VLAN ID 属性を割り当てました。

	ログの内容	緊急度	イベントの説明
	ARP		
1	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <port-num>, Interface: <ipif-name>) **パラメータ説明：** • ipaddr：重複した IP アドレス • macaddr：重複した IP アドレスの MAC アドレス • port-num：デバイスのポート番号 • ipif_name：重複した IP アドレスを持つスイッチのインタフェース名	Warning	Gratuitous ARP は重複した IP を検出しました。
	Auto image		
1	The downloaded firmware was successfully executed by DHCP Auto image update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：TFTP サーバの IP アドレス	Informational	DHCP 自動イメージによるファームウェアダウンロードは成功しました。
2	The downloaded firmware was not successfully executed by DHCP Autoimage update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：TFTP サーバの IP アドレス	Informational	DHCP 自動イメージによるファームウェアダウンロードは失敗しました。
	Auto Save Config		
1	CONFIG-6-DDPSAVECONFIG: Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	DDP の設定情報が自動で保存されました。
	Auto Surveillance VLAN		
1	New surveillance device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface–id：インタフェース名 • mac-address：サーベイランスデバイスの MAC アドレス	Informational	インタフェースで新しい監視デバイスが検出されました。
2	<interface-id> add into surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名 • vid：VLAN ID	Informational	サーベイランス VLAN が有効のインタフェースが自動的にサーベイランス VLAN に追加されました。
3	<interface-id> remove from surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名 • vid：VLAN ID	Informational	インタフェースがサーベイランスVLANから離脱しました。同時に一定の期間内に当該のインタフェースに監視デバイスが検出されず、ログメッセージが送信されました。
4	ASV: Add IPC (<ipaddr>, MAC:<mac-address>) **パラメータ説明：** • ipaddr：IPC の IP アドレス • mac-address：IPC の MAC アドレス	Informational	IPC がサーベイランス VLAN に追加されました。
5	ASV: Remove IPC (<ipaddr>, MAC:<mac-address>) **パラメータ説明：** • ipaddr：IPC の IP アドレス • mac-address：IPC の MAC アドレス	Informational	IPC がサーベイランス VLAN から削除されました。
6	ASV: Add NVR (<ipaddr>, MAC:<mac-address>) **パラメータ説明：** • ipaddr：NVR の IP アドレス • mac-address：NVR の MAC アドレス	Informational	NVR がサーベイランス VLAN に追加されました。

ログの内容		緊急度	イベントの説明
7	ASV: Remove NVR (<ipaddr>, MAC:<mac-address>) **パラメータ説明：** • ipaddr：NVR の IP アドレス • mac-address：NVR の MAC アドレス	Informational	NVR がサーベイランス VLAN から削除されました。
8	ASV: Mode change from <mode> to <mode > **パラメータ説明：** • mode: ASV 2.0 のモード（standard または surveillance）	Informational	Web GUI で ASV2.0 のモードが変更されました。
Configuration/Firmware			
1	Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Informational	ファームウェアのアップグレードに成功しました。
2	Firmware upgraded by <session> unsuccessfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Warning	ファームウェアのアップグレードに失敗しました。
3	Firmware uploaded by <session> successfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Informational	ファームウェアのアップロードに成功しました。
4	Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Warning	ファームウェアのアップロードに失敗しました。
5	Configuration downloaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Informational	コンフィグレーションのダウンロードに成功しました。

ログの内容		緊急度	イベントの説明
6	Configuration downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Warning	コンフィグレーションのダウンロードに失敗しました。
7	Configuration uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Informational	コンフィグレーションのアップロードに成功しました。
8	Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Warning	コンフィグレーションのアップロードに失敗しました。
9	Configuration saved to flash by console (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ名	Informational	コンソールによりコンフィグレーションが Flash に保存されました。
10	Configuration saved to flash (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	リモートによりコンフィグレーションが Flash に保存されました。
11	Log message uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Informational	ログメッセージのアップロードに成功しました。

ログの内容		緊急度	イベントの説明
12	Log message uploaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Warning	ログメッセージのアップロードに失敗しました。
13	Downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) **パラメータ説明：** • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • server-ip：サーバの IP アドレス • pathfile：サーバのパスとファイル名	Warning	未知のタイプのファイルのダウンロードに失敗しました。
DAD			
1	Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages **パラメータ説明：** • ipv6address：NS メッセージの IPv6 アドレス • interface-id：ポートインタフェース ID	Warning	DAD の間に DUT が「Neighbor Solicitation」(NS) メッセージを重複アドレスとともに受信しました。
2	Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages **パラメータ説明：** • ipv6address：NA メッセージの IPv6 アドレス • interface-id：ポートインタフェース ID	Warning	DAD の間に DUT が「Neighbor Advertisement」(NA) メッセージを重複アドレスとともに受信しました。
Dynamic ARP Inspection（DAI）			
1	Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) **パラメータ説明：** • type：ARP パケットの種類。ARP パケットが、「request」か「response」かを示します。 • ip-address：IP アドレス • mac-address：MAC アドレス • vlan-id：VLAN ID • interface-id：インタフェース名	Warning	DAI が無効な ARP パケットを検出しました。
2	Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) **パラメータ説明：** • type：ARP パケットの種類。ARP パケットが、「request」か「response」かを示します。 • ip-address：IP アドレス • mac-address：MAC アドレス • vlan-id：VLAN ID • interface-id：インタフェース名	Informational	DAI が有効な ARP パケットを検出しました。
DHCPv6 Client			
1	DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] **パラメータ説明：** • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 クライアントインタフェース管理者ステートが変更されました。

ログの内容		緊急度	イベントの説明
2	DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name> **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 クライアントが DHCPv6 サーバから ipv6 アドレスを取得しました。
3	The IPv6 address <ipv6address> on interface <ipif-name> starts renewing **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得した IPv6 アドレスが更新を開始します。
4	The IPv6 address <ipv6address> on interface <ipif-name> renews success **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスの更新に成功しました。
5	The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスのリバインドを開始します。
6	The IPv6 address <ipv6address> on interface <ipif-name> rebinds success **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスがリバインドに成功しました。
7	The IPv6 address <ipv6address> on interface <ipif-name> was deleted **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバからの IPv6 アドレスが削除されました。
DHCPv6 Relay			
1	DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] **パラメータ説明：** • <ipif-name>：DHCPv6 リレーエージェントインタフェース名	Informational	特定のインタフェースの管理者ステートの DHCPv6 リレーが変更されました。
DNS Resolver			
1	Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr> **パラメータ説明：** • domain-name：ドメイン名文字列 • ipaddr：スタティック / ダイナミック IP アドレス	Informational	重複するドメイン名キャッシュが追加され、ダイナミックドメイン名キャッシュが削除されました。
DoS Prevention			
1	<dos-type> is dropped from (IP: <ip-address> Port <interface-id>) **パラメータ説明：** • dos-type：DoS 攻撃タイプ • ip-address:：IP アドレス • interface-id:：インタフェース名	Notification	DoS 攻撃を検出しました。
	Interface		
1	Port <port-type><interface-id> link down **パラメータ説明：** • port-type：ポートタイプ • interface-id：インタフェース名	Informational	ポートがリンクダウンしました。

ログの内容		緊急度	イベントの説明
2	Port <port-type><interface-id> link up, <link-speed> **パラメータ説明：** • port-type：ポートタイプ • interface-id：インタフェース名 • link-speed：ポートのリンクスピード	Informational	ポートがリンクアップしました。
IP Source Guard（IPSG）			
1	Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>) **パラメータ説明：** • ipaddr：IP アドレス • macaddr：MAC アドレス • vlan-id：VLAN ID • interface-id：インタフェース ID	Warning	DHCP スヌーピングエントリを ISPG テーブルにセットするに当たり、ハードウェアルールのリソースがない場合、シスログが記録されます。
IPv6 Source Guard			
1	Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlan-id>, Interface <interface-id>) **パラメータ説明：** • ipaddr：IPv6 スヌーピングエントリの IPv6 アドレス • macaddr：IPv6 スヌーピングエントリの MAC アドレス • vlanid：IPv6 スヌーピングエントリの VLAN ID • interface-id：IPv6 スヌーピングエントリのインタフェース	Warning	DHCP スヌーピングエントリを IPv6SG テーブルにセットするに当たり、ハードウェアルールのリソースがない場合、シスログが記録されます。
LACP			
1	Link Aggregation Group <group-id> link up **パラメータ説明：** • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクアップします。
2	Link Aggregation Group <group-id> link down **パラメータ説明：** • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクダウンします。
3	<ifname> attach to Link Aggregation Group <group-id> **パラメータ説明：** • Ifname：アグリゲーショングループにアタッチするポートのインタフェース名 • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループにアタッチします。
4	<ifname> detach from Link Aggregation Group <group-id> **パラメータ説明：** • ifname：アグリゲーショングループにアタッチするポートのインタフェース名 • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループにデタッチします。
LBD（ループバック検知）			
1	<interface-id> LBD loop occurred **パラメータ説明：** • interface-id：ループが検知されたインタフェース	Critical	インタフェースがループを検知しました。
2	<interface-id> VLAN <vlan-id> LBD loop occurred **パラメータ説明：** • interface-id：ループが検知されたインタフェース • vlan-id：ループが検知された VLAN	Critical	インタフェースが VLAN のループを検知しました。
3	<interface-id> LBD loop recovered **パラメータ説明：** • interface-id：ループから回復したインタフェース	Critical	ループバックから回復しました。

ログの内容		緊急度	イベントの説明
4	<interface-id> VLAN <vlan-id> LBD loop recovered **パラメータ説明：** • interface-id：ループから回復したインタフェース • vlan-id：ループから回復した VLAN	Critical	VLAN のインタフェースループが回復しました。
5	Loop VLAN number overflow	Critical	ループバックが発生した VLAN の数が指定の数に達しました。
LLDP-MED			
1	LLDP-MED topology change detected (on port <portNum>. chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notification	LLDP-MED トポロジの変更が検出されました。

	ログの内容	緊急度	イベントの説明
2	Conflict LLDP-MED device type detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notification	LLDP-MED デバイスタイプの重複が検出されました。
3	Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) • chassisID：シャーシ ID • portType：ポート ID サブタイプ 値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) • portID：ポート ID • deviceClass：LLDP-MED デバイスタイプ	Notification	LLDP-MED TLV の非互換性が検出されました。

	ログの内容	緊急度	イベントの説明
	Login/Logout CLI		
1	Successful login through Console (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ	Informational	コンソール経由のログインに成功しました。
2	Login failed through Console (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ	Warning	コンソール経由のログインに失敗しました。
3	Console session timed out (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ	Informational	コンソールのセッションはタイムアウトしました。
4	Logout through Console (Username: <username>) **パラメータ説明：** • username：現在のログインユーザ	Informational	コンソール経由でログアウトしました。
5	Successful login through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由のログインに成功しました。
6	Login failed through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Warning	Telnet 経由のログインに失敗しました。
7	Telnet session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	Telnet のセッションはタイムアウトしました。
8	Logout through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由でログアウトしました。
9	Successful login through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	SSH 経由のログインに成功しました。
10	Login failed through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Critical	SSH 経由のログインに失敗しました。
11	SSH session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	SSH のセッションはタイムアウトしました。
12	Logout through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	SSH 経由でログアウトしました。
	MSTP Debug Enhancement		

ログの内容		緊急度	イベントの説明
1	Spanning Tree Protocol is enabled	Informational	スパニングツリープロトコル有効化
2	Spanning Tree Protocol is disabled	Informational	スパニングツリープロトコル無効化
3	Topology changed (Instance: <instance-id>,<interface-id>, MAC:<macaddr>) **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号 • macaddr：ブリッジの MAC アドレス	Notification	トポロジに変更がありました。
4	[CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority:<priority>) **パラメータ説明：** • Instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。 • macaddr：ブリッジの MAC アドレス • priority：ブリッジの優先値。4096 で割り切れます。	Informational	新しいルートブリッジが選定されました。
5	New root port selected (Instance:<instance-id>, <interface-id>) **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号	Notification	新しいルートポートが選定されました。
6	Spanning Tree port status change (Instance:<instance-id>, <interface-id>) <old-status> -> <new-status> **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号 • old-status：旧ステータス（Disable, Discarding, Learning, Forwarding） • new-status：新ステータス（Disable, Discarding, Learning, Forwarding）	Notification	スパニングツリーポートのステートが変更されました。
7	Spanning Tree port role change (Instance:<instance-id>, <interface-id>) <old-role> -> <new-role> **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。 • interface-id：トポロジ変更情報を検知 / 受信したポート番号 • old-role：旧ロール（DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort.） • new-role：新ロール（DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort.）	Informational	スパニングツリーポートのロールが変更されました。
8	Spanning Tree instance created (Instance:<instance-id>) **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。	Informational	スパニングツリーインスタンスが作成されました。
9	Spanning Tree instance deleted (Instance :< Instance-id >) **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。	Informational	スパニングツリーインスタンスが削除されました。
10	Spanning Tree version change (new version:<new-version>) **パラメータ説明：** • new-version：アクティブな STP バージョン	Informational	スパニングツリーのバージョンが変更されました。

	ログの内容	緊急度	イベントの説明
11	Spanning Tree MST configuration ID name and revision level change (name:<name>, revision level <revision-level>) **パラメータ説明：** • name：指定された MST リージョンの名前 • revision-level：リビジョンレベル	Informational	MST configuration ID で、コンフィグレーション名とリビジョンレベルが変更されました。
12	Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> add vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。 • startvlanid：追加する VLAN 範囲の開始 VID • endvlanid：追加する VLAN 範囲の終了 VID	Informational	VLAN が MST インスタンスにマッピングされました。
13	Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> delete vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。 • startvlanid：削除する VLAN 範囲の開始 VID • endvlanid：削除する VLAN 範囲の終了 VID	Informational	VLAN が MST インスタンスから削除されました。
14	Spanning Tree port role change (Instance:<instance-id>, <interface-id>) to alternate port due to the guard root **パラメータ説明：** • instance-id：MST インスタンス ID。 0 は、デフォルトのインスタンスである CIST を表します。 • interface-id：イベントを検知したポート番号	Informational	ガードルートのためにスパニングツリーポートロールが交代します。
	Peripheral（周辺機器）		
1	<fan-descr> back to normal **パラメータ説明：** • fan-descr：ファンの ID と場所	Critical	ファンが回復しました。
2	<fan-descr> failed **パラメータ説明：** • fan-descr：ファンの ID と場所	Critical	ファンに異常があります。
3	<thermal-sensor-descr> detects abnormal temperature <degree> **パラメータ説明：** • thermal-sensor-descr：センサ ID と場所 • degree：温度	Critical	温度センサがアラーム状態に入りました。
4	<thermal-sensor-descr> temperature back to normal **パラメータ説明：** • thermal-sensor-descr：センサ ID と場所	Critical	温度が通常に戻りました。
5	Factory reset button pressed	Critical	リセットボタンが押されました。
	Port Security		
1	MAC address <macaddr> causes port security violation on <interface-id> **パラメータ説明：** • macaddr：違反 MAC アドレス • interface-id：インタフェース名	Warning	ポート上のアドレスが超過
2	Limit on system entry number has been exceeded	Warning	システム上のアドレスが超過

	ログの内容	緊急度	イベントの説明
	Safeguard		
1	Safeguard Engine enters EXHAUSTED mode	Warning	ホストは「exhausted」モードに移行しました。
2	Safeguard Engine enters NORMAL mode	Informational	ホストは「normal」モードに移行しました。
	SNMP		
1	SNMP request received from <ipaddr> with invalid community string **パラメータ説明：** • ipaddr：IP アドレス	Informational	SNMP リクエストは無効なコミュニティストリングを受信しました。
	SSH		
1	SSH server is enabled	Informational	SSH サーバは有効
2	SSH server is disabled	Informational	SSH サーバは無効
	Storm Control		
1	<Broadcast | Multicast | Unicast> storm is occurring on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Warning	ストームが発生しました。
2	<Broadcast | Multicast | Unicast> storm is cleared on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Informational	ストームが解消されました。
3	<interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Warning	パケットストームによりポートがシャットダウンしました。
	System		
1	System warm start	Critical	システムがウォームスタートしました。
2	System cold start	Critical	システムがコールドスタートしました。
3	System started up	Critical	システムが起動しました。
	Telnet		
1	Successful login through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet クライアントのユーザ名 • ipaddr：Telnet クライアントの IP アドレス	Informational	Telnet 経由のログインに成功しました。
2	Login failed through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet クライアントのユーザ名 • ipaddr：Telnet クライアントの IP アドレス	Warning	Telnet 経由のログインに失敗しました。

ログの内容		緊急度	イベントの説明
3	Logout through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet クライアントのユーザ名 • ipaddr：Telnet クライアントのアドレス	Informational	Telnet からログアウトしました。
4	Telnet session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：Telnet サーバにログインするユーザ名 • ipaddr：Telnet クライアントの IP アドレス	Informational	Telnet セッションがタイムアウトしました。
Voice VLAN			
1	New voice device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface-id：インタフェース名 • mac-address：音声デバイスの MAC アドレス	Informational	インタフェースで音声機器が検出されました。
2	<interface-id> add into voice VLAN <vid> **パラメータ説明：** • interface-id：インタフェース名 • vid：VLAN ID	Informational	自動音声 VLAN モードのインタフェースが音声 VLAN に追加されました。
3	<interface-id> remove from voice VLAN <vid> **パラメータ説明：** • interface-id：インタフェース名 • vid：VLAN ID	Informational	インタフェースが音声 VLAN から離脱し、一定期間内に音声機器がインタフェースに検出されませんでした。ログメッセージが送信されます。
Web			
1	Successful login through Web (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：HTTP クライアントのユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web 経由でのログインに成功しました。
2	Login failed through Web (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：HTTP クライアントのユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Warning	Web 経由でのログインに失敗しました。
3	Web session timed out (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：HTTP クライアントのユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web セッションがタイムアウトしました。
4	Logout through Web (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：HTTP クライアントのユーザ名 • ipaddr：HTTP クライアントの IP アドレス	Informational	Web 経由でログアウトしました。
5	Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：SSL サーバへのログインに使用するユーザ名 • ipaddr：SSL クライアントの IP アドレス	Informational	Web（SSL）経由でのログインに成功しました。
6	Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：SSL サーバへのログインに使用するユーザ名 • ipaddr：SSL クライアントの IP アドレス	Warning	Web（SSL）経由でのログインに失敗しました。

ログの内容		緊急度	イベントの説明
7	Web (SSL) session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：SSL サーバへのログインに使用するユーザ名 • ipaddr：SSL クライアントの IP アドレス	Informational	Web セッションがタイムアウトしました。（SSL）
8	Logout through Web (SSL) (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：SSL サーバへのログインに使用するユーザ名 • ipaddr：SSL クライアントの IP アドレス	Informational	Web（SSL）経由でのログアウトに成功しました。

【付録 B】トラップログエントリ

スイッチにおいて現れる可能性のあるトラップログエントリとそれらの意味を以下に示します。

	トラップ名	説明	OID
802.1X			
1	dDot1xExtLoggedSuccess	ホストが 802.1X 認証に成功したときに送信されます。（ログインに成功） 関連オブジェクト： (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.171.14.30.0.1
2	dDot1xExtLoggedFail	ホストが 802.1X 認証に失敗したときに送信されます。 （ログインに失敗） 関連オブジェクト： (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.171.14.30.0.2
Authentication Fail			
1	authenticationFailure	authenticationFailure トラップは、SNMPv2 エンティティが、エージェントロールで動作し、正しく認証されないプロトコルメッセージを受信したことを表します。SNMPv2 のすべての実装は、このトラップを生成することができる必要がある一方、snmpEnableAuthenTraps オブジェクトは、このトラップが生成されるか否かを示します。	1.3.6.1.6.3.1.1.5.5
DHCP Server Screen Prevention			
1	dDhcpFilterAttackDetected	DHCP サーバスクリーンが有効なとき、スイッチが偽造 DHCP サーバパケットを受信すると、攻撃パケットを受信したイベントをトラップ送信します。 関連オブジェクト： (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.171.14.133.0.1
DoS Prevention			
1	dDosPreveAttackDetectedPacket	DoS アタックを検出したとき送信されます。 関連オブジェクト： (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171.14.59.0.2
ErrDisable			
1	dErrDisNotifyPortDisabledAssert	ポートが error-disabled モードになったときに送信されます。 関連オブジェクト： (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.1
2	dErrDisNotifyPortDisabledClear	インターバル時間後にポートループが再起動したときに送信されます。 関連オブジェクト： (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.2
General Management			
1	dGenMgmtLoginFail	スイッチへのログインに失敗したときに送信されます。 関連オブジェクト： (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171.14.165.0.1

	トラップ名	説明	OID
		Gratuitous ARP	
1	agentGratuitousARPTrap	IP アドレスが重複していた場合に送信されます。 関連オブジェクト : (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.14.75.0.1
		IMPB	
1	dImpbViolationTrap	アドレス違反通知は IP-MAC ポートバインディングアドレス違反が検出された際に生成されます。 関連オブジェクト : (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.171.14.22.0.1
		LACP	
1	linkUp	「linkUp」トラップはエージェント役の SNMP エンティティによって、コミュニケーションリンクの一つが「notPresent」ステート以外の他のステートからダウンステートに移行しようとしている「ifOperStatus」オブジェクトの検出を意味します。他のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	「linkDown」トラップはエージェント役の SNMP エンティティによって、コミュニケーションリンクの一つがダウンステートに残り、「notPresent」ステート以外の他のステートに移行する「ifOperStatus」オブジェクトの検出を意味します。他のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : (1) ifIndex (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3
		LBD	
1	dLbdLoopOccurred	インタフェースにループが発生したときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.1
2	dLbdLoopRestart	間隔時間後、インタフェースのループが再スタートしたときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.2
3	dLbdVlanLoopOccurred	インタフェースに VID ループが発生したときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.3

	トラップ名	説明	OID
4	dLbdVlanLoopRestart	間隔時間後、VID のインタフェースループが再スタートしたときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.4
	LLDP/LLDP-MED Trap Name		
1	lldpRemTablesChange	「lldpRemTablesChange」通知は「lldpStatsRemTableLastChangeTime」変更時に送信されます。 関連オブジェクト : (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2	lldpXMedTopologyChangeDetected	ローカルポートに新しいリモートデバイスがアタッチされた、またはリモートデバイスがポートから切断 / 移動した場合のトポロジの変更を感知するローカルデバイスによって送信されます。 関連オブジェクト : (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1
	MAC Notification		
1	swL2macNotification	アドレステーブルの MAC アドレスに変更があったときに送信されます。 関連オブジェクト : (1) swL2macNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
2	dL2FdbMacNotificationWithVID	アドレステーブルの MAC アドレスに変更があったときに送信されます。 関連オブジェクト : (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.171.14.3.0.2
	MSTP		
1	newRoot	newRoot トラップは、送信側のエージェントがスパニングツリーの新しいルートになったことを示します。トラップは、新しいルートとして選出された後にすぐにブリッジによって送信され、その選出に続いてすぐに Topology Change Timer のアクションの起動などを行います。 本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.1
2	topologyChange	topologyChange トラップは、構成するいずれかのポートが Learning 状態から Forwarding 状態に、Forwarding 状態から Blocking 状態に遷移する場合にブリッジによって送信されます。本トラップは、newRoot トラップが同様の変更に対して送信される場合には送信されません。 本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.2
	Peripheral		
1	dEntityExtFanStatusChg	ファン状態の変更通知 （ファンの不具合 (dEntityExtEnvFanStatus is 'fault') または回復 (dEntityExtEnvFanStatus is 'ok')） 関連オブジェクト : (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.171.14.5.0.1
2	dEntityExtThermalStatusChg	温度状態の変更通知 （温度警告 (dEntityExtEnvTempStatus is 'abnormal') または回復 (dEntityExtEnvTempStatus is 'ok')） 関連オブジェクト : (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.171.14.5.0.2

	トラップ名	説明	OID
		Port	
1	linkUp	ポートがリンクアップしたときに生成されます。 関連オブジェクト : (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	ポートがリンクダウンしたときに生成されます。 関連オブジェクト : (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3
		Port Security	
1	dPortSecMacAddrViolation	ポートセキュリティトラップが有効な場合、事前定義されたポートセキュリティ設定に違反する新しい MAC アドレスがトリガとなり送信されるトラップメッセージです。 関連オブジェクト : (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.171.14.8.0.1
		RMON	
1	risingAlarm	SNMP トラップは、アラームエントリが上昇しきい値を超える時に生成され、SNMP トラップの送信に設定されたイベントを生成します。 関連オブジェクト : (1)alarmIndex (2)alarmVariable (3)alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
2	fallingAlarm	SNMP トラップは、アラームエントリが下降しきい値を下回るときに生成され、SNMP トラップの送信に設定されたイベントを生成します。 関連オブジェクト : (1)alarmIndex (2)alarmVariable (3)alarmSampleType (4)alarmValue (5)alarmFallingThreshold	1.3.6.1.2.1.16.0.2
		Safeguard	
1	dSafeguardChgToExhausted	システムが操作モードをノーマルから exhausted に変更したことを示します。 関連オブジェクト : (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.1
2	dSafeguardChgToNormal	システムが操作モードを exhausted からノーマルに変更したことを示します。 関連オブジェクト : (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.2
		Start	
1	coldStart	coldStart トラップは、SNMPv2 エンティティが、エージェントロールで動作し、自身を再起動し、設定が変更されたかもしれないことを表します。	1.3.6.1.6.3.1.1.5.1
2	warmStart	warmStart トラップは、SNMPv2 エンティティが、エージェントロールで動作し、設定が変更されないような再起動を表します。	1.3.6.1.6.3.1.1.5.2

	トラップ名	説明	OID
Storm Control			
1	dStormCtrlOccurred	「dStormCtrlNotifyEnable」が "stormOccurred" または "both" で、ストームが検出されたときに送信されます。 関連オブジェクト : (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.1
2	dStormCtrlStormCleared	「dStormCtrlNotifyEnable」が "stormCleared" または "both" で、ストームがクリアされたときに送信されます。 関連オブジェクト : (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.2
System File			
1	dsfUploadImage	イメージファイルのアップロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.1
2	dsfDownloadImage	イメージファイルのダウンロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.2
3	dsfUploadCfg	コンフィグレーションファイルのアップロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.3
4	dsfDownloadCfg	コンフィグレーションファイルのダウンロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.4
5	dsfSaveCfg	コンフィグレーションファイルの保存に成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.5

【付録 C】RADIUS 属性の割り当て指定

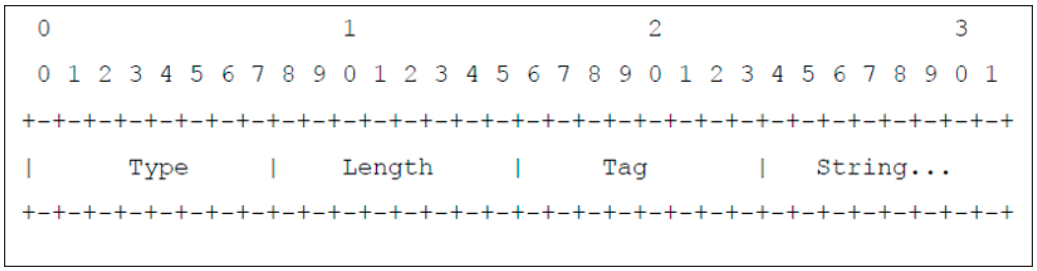
スイッチの RADIUS 属性の割り当ては、802.1X モジュールで使用されます。
次の RADIUS 属性割り当てタイプについて説明します。

- VLAN

RADIUS サーバで Privilege Level（権限レベル）の帯域幅を割り当てるためには、適切なパラメータを RADIUS サーバに設定する必要があります。
VLAN 割り当てを使用するために、RFC3580 は RADIUS パケットで次のトンネル属性を定義します。

RADIUS トンネル属性	説明	値	摘要
Tunnel-Type	本属性はトンネルの開始に使用されるトンネリングプロトコルまたはトンネルの終了に使用されるトンネリングプロトコルを示します。	13 (VLAN)	必須
Tunnel-Medium-Type	本属性は使用されている伝送の媒体を示します。	6 (802)	必須
Tunnel-Private-Group-ID	本属性は特定のトンネルセッションのグループ ID を示します。	String 値（VID）	必須

「Tunnel-Private-Group-ID」属性フォーマットのサマリは次のようになります。



タグフィールドの定義は次の通りです。（RFC 2868 とは違う）

タグフィールド値	文字列フィールドのフォーマット
0x01	VLAN 名 (ASCII)
0x02	VLAN ID (ASCII)
その他 (0x00、0x03 ~ 0x1F、>0x1F)	**1.** スイッチが VLAN 設定の文字列を受信した場合、最初は VLAN ID として認識します。つまりスイッチは既存の VLAN ID をチェックし合致するものがあるか調べます。 **2.** スイッチが合致する VLAN ID を発見した場合、その VLAN へ移動します。 **3.** スイッチが合致する VLAN ID を発見できなかった場合、VLAN 設定の文字列は VLAN 名として認識されます。 **4.** そして合致する VLAN 名を発見します。

注意 0x1F よりも大きいタグフィールドは続くフィールドの最初のオクテットとして認識されます。

ユーザが RADIUS サーバの VLAN 属性（VID 3 など）を設定し、802.1X 認証に成功すると、ポートは VLAN 3 に割り当てられます。
しかし、VLAN 属性を設定せずに認証に成功しても、ポートは元の VLAN に置かれます。RADIUS サーバに設定された VLAN 属性が存在しないと、ポートは要求された VLAN に割り当てられません。

【付録 D】IETF RADIUS 属性のサポート

リモート認証ダイヤルインユーザサービス（RADIUS）属性を使用すると、リクエストや応答の中で認証、承認、情報、設定詳細などをやり取りすることができます。

本付録では、スイッチによりサポートされる RADIUS 属性一覧を記載しています。

RADIUS 属性は、IETF 規格やベンダ特定属性（VSA) によりサポートされます。VSA により、ベンダは固有の RADIUS 属性を定義することができます。D-Link VSA についての詳しい情報は、「【付録 C】RADIUS 属性の割り当て指定」を参照してください。

IETF 規格 RADIUS 属性は、RFC2865 リモート認証ダイヤルインユーザサービス（RADIUS)、RFC2866 RADIUS アカウンティング、RFC2868 トンネルプロトコルに対する RADIUS 属性、RFC2869 RADIUS 拡張で定義されています。
以下のリストは、D-Link スイッチでサポートされている IETF RADIUS 属性です。

1. RADIUS 認証属性

番号	IETF 属性
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

【付録 E】機能設定例

本項では、一般によく使う機能についての設定例を記載します。実際に設定を行う際の参考にしてください。

- Traffic Segmentation（トラフィックセグメンテーション）
- VLAN
- Link Aggregation（リンクアグリゲーション）
- Access List（アクセスリスト）
- Loopback Detection（LBD）（ループ検知）

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DXS-1210-28T
- DXS-1210-28S

Traffic Segmentation（トラフィックセグメンテーション）

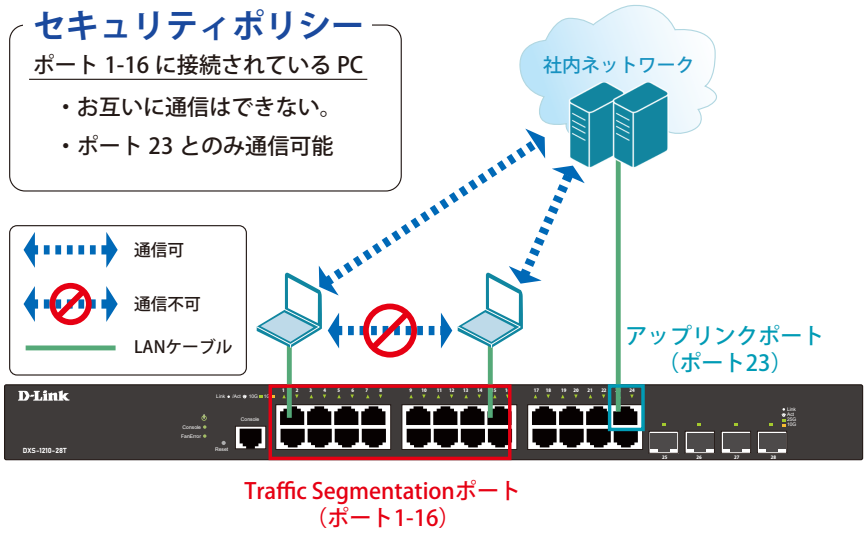


図 18-1　Traffic Segmentation（DXS-1210-28T）

概要

ポート 1 - 16 に対し、トラフィックセグメンテーションを設定します。
1 - 16 のポート間ではお互いに通信ができないようにし、ポート 1 - 16 は、アップリンクポートとして使用するポート 23 とのみ通信ができるようにします。

設定手順

1. ポート（1-16）のセキュリティ設定をします。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#traffic-segmentation forward interface ethernet 1/0/23
Switch(config-if-range)#end
```

2. 情報確認

```
Switch#show traffic-segmentation forward
```

注意 本機能を利用する場合、送信先 MAC アドレスが不明な Unknown ユニキャストについて、スイッチの全ポートにフラッドされます。他ポートへのフラッディングを回避するために、ダウンリンクポートを対象に、ストームコントロール機能を用いて宛先 MAC アドレス不明の unknown ユニキャストパケットをドロップするよう設定を追加します。

3. （必要に応じて）ストームコントロール機能により、Unknown ユニキャストに閾値「0」を設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#storm-control unicast level kbps 0
Switch(config-if-range)#storm-control action drop
Switch(config-if-range)#end
```

4. 設定を保存します。

```
Switch#copy running-config startup-config
```

5. 情報確認（ポート 1-16 の storm-control の unicast の設定と閾値を表示します。）

```
Switch#show storm-control interface ethernet 1/0/1-16 unicast
```

VLAN

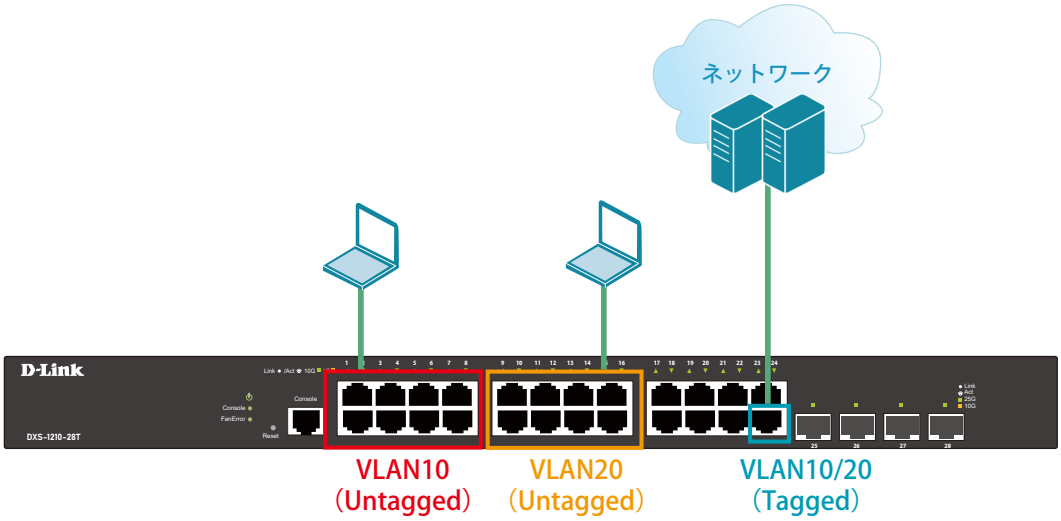


図 18-2　VLAN（DXS-1210-28T）

概要

VLAN を設定します。ポート 1 - 8 に VLAN10 を「Untagged」で割り当て、ポート 9 ～ 16 に VLAN20 を「Untagged」で割り当て、ポート 24 において、VLAN10 と VLAN20 を「Tagged」で割り当てます。

設定手順

1. VLAN10、VLAN20 を作成します。

```
Switch#configure terminal
Switch(config)#vlan 10,20
Switch(config-vlan)#end
```

2. ポート 1-8 に VLAN10、ポート 9-16 に VLAN20 を 割り当てます。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit

Switch#configure terminal
Switch(config)#interface range ethernet 1/0/9-16
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#end
```

3. 上位のネットワークへ接続されているポート 24 に VLAN10、20 の通信を転送することができるように、VLAN を設定します。
   ■設定方法①（hybrid mode を設定する場合）

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add tagged 10,20
Switch(config-if)#end
```

   ■設定方法②（hybrid mode を使用せず、trunk にて同様の設定を行う場合）

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10,20
Switch(config-if)#end
```

4. 設定を保存します。

```
Switch#copy running-config startup-config
```

5. 情報確認

```
Switch#show vlan
```

（作成した VLAN と各ポートに割り当てられている VLAN が表示されます。）

```
Switch#show vlan int ethernet 1/0/xx
```

（ポートに紐づいている VLAN 情報が表示されます。）

Link Aggregation（リンクアグリゲーション）

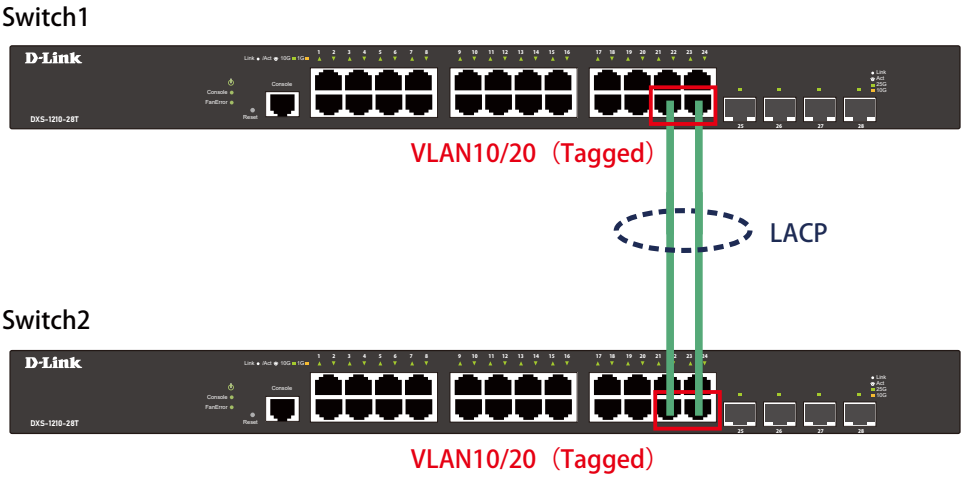


図 18-3　Link Aggregation（DXS-1210-28T）

概要

VLAN10 と 20 の Tagged VLAN を設定したポートにリンクアグリゲーションを設定します。ポート 22 と 24 に VLAN10 と VLAN20 を「Tagged」で割り当て、ポート 22 と 24 をグループ 1 として LACP によるリンクアグリゲーションに設定します。

設定手順（Switch1、Switch2 共通）

1. VLAN10、VLAN20 を作成します。

```
Switch#configure terminal
Switch(config)#vlan 10,20
Switch(config-vlan)#exit
```

2. Link Aggregation（LACP）のグループを作成します。

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/22
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
```

3. Link Aggregation のポートを設定します。

```
Switch(config)#interface port-channel 1
```

4. 作成した port-channel に VLAN を設定します。
   LAG ポートに設定する VLAN は、各物理インタフェース上では設定せず、Port-channel インタフェース上で VLAN の設定を行います。

```
Switch(config)#interface port-channel 1
Switch(config if)#switchport mode trunk
Switch(config if)#switchport trunk native vlan 1
Switch(config if)#switchport trunk allowed vlan 1,10,20
Switch(config if)#exit
Switch(config)#exit
```

5. 設定を保存します。

```
Switch#copy running-config startup-config
```

6. 情報確認
   - Port-channel に設定されている VLAN 情報を表示します。

```
Switch#show vlan interface port-channel 1
```

   - グループ番号とグループで使用されている Protocol を表示します。

```
Switch#show channel-group
```

   - 各グループに所属している Port 番号と、リンクアグリゲーションの状態を表示します。

```
Switch#show channel-group channel 1 detail
```

Access List（アクセスリスト）

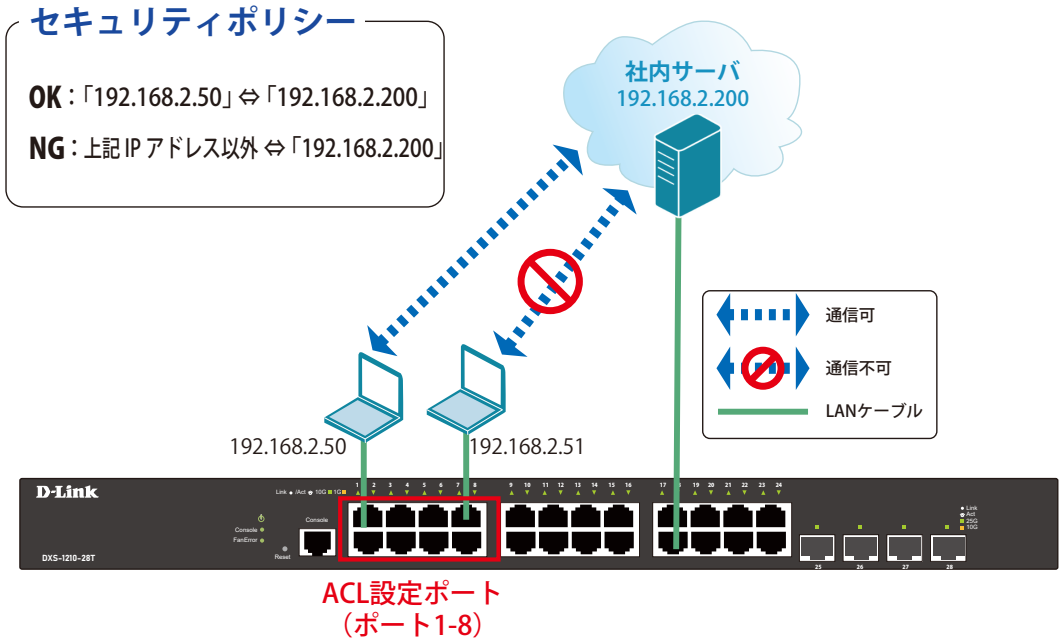


図 18-4　Access List（DXS-1210）

概要

ポート 1 - 8 に対し、アクセスリストを設定します。ポート 1 - 8 に接続される端末の IP の中から、「192.168.2.50」の端末から社内サーバ（192.168.2.200）へのアクセスは許可し、それ以外の端末から社内サーバへのアクセスは禁止するように設定します。

設定手順

1. アクセスリストに名前（extended ACL）を付けて定義します。
   「192.168.2.50 ⇔ 192.168.2.200」間の通信を許可するルールを追加します。
   「192.168.2.200」へのすべての通信を拒否するルールを追加します。

```
Switch#configure terminal
Switch(config)#ip access-list extended ACL
Switch(config-ip-ext-acl)#permit 192.168.2.50 0.0.0.0 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#deny any 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#end
```

2. アクセスリストのルールを、適用対象ポート 1 - 8 へ設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#ip access-group ACL in
Switch(config-if-range)#end
```

3. 設定を保存します。

```
Switch#copy running-config startup-config
```

4. 情報確認

```
Switch#show access-list
Switch#show access-list ip
Switch#show access-group
```

Loopback Detection（LBD）（ループ検知）

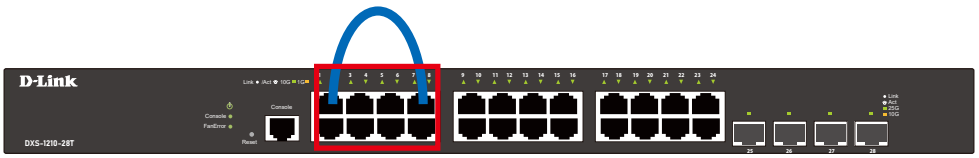


図 18-5　Loopback Detection（DXS-1210）

概要

ポート 1~8 に対しループバック検知を設定します。ポート 1~8 でループを検知した際、ポートをシャットダウンするように設定します。

設定手順

1. ポートベースでループ検知機能を動作させ、ループ検知後はポートをシャットダウンする設定をします。

```
Switch#configure terminal
Switch(config)#loopback-detection
Switch(config)#loopback-detection mode port-based
```

2. ループ発生を確認する間隔を 20 秒に設定します。

```
Switch(config)#loopback-detection interval 20
```

3. （必要に応じて）ループ発生後のループ解消確認間隔を 20 秒に設定し、ループ解消確認後、自動で Port 開放するように設定します。

```
Switch(config)#errdisable recovery cause loopback-detect interval 20
```

注意 この設定をしない場合、永続的にポートが「shutdown」状態となります。ポートを開放する場合、該当のポートに対し、インタフェースモードにて「no shutdown」コマンドを投入する必要があります。

4. ポート 1-8 でループバック検知機能を有効にします。

```
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#spanning-tree state disable
Switch(config-if-range)#loopback-detection
Switch(config-if-range)#end
```

注意 「spanning-tree」が「enable」になっている場合、ループ検知機能を設定できないため、設定するインタフェースの「spanning-tree」の設定をまず「disable」にします。

注意 「spanning-tree」はデフォルトでグローバルでは「disable」に設定されていますが、各インタフェース「enable」となっています。各インタフェースにて「disable」設定が必要となります。

5. show コマンドで「Spanning Tree」が無効になっているかを確認します。

```
Switch#show spanning-tree configuration interface ethernet 1/0/1-8
```

6.「Spanning Tree」がポート単位で「disable」に設定されている場合、ステータスが Disabled と表示されます。

```
Spanning tree state : Disabled
```

7. 設定を保存します。

```
Switch#copy running-config startup-config
```

8. 情報確認

```
Switch#show loopback-detection
```

（ループ検知の有効 / 無効、設定しているモード、対象の VLAN、各ポートのループ状態等を表示します。）

```
Switch#show errdisable recovery
```

（ループ解消後の自動ポート解放設定 有効 / 無効、確認間隔を表示します。）